aaa accounting command through accounting-server-group コマンド

aaa accounting command

CLI で **show** コマンド以外のコマンドを入力したときに TACACS+ アカウンティング サーバにアカウンティング メッセージを送信するには、グローバル コンフィギュレーション モードで **aaa accounting command** コマンドを入力します。コマンド アカウンティングのサポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting command [**privilege** *level*] *tacacs+-server-tag*

no aaa accounting command [**privilege** *level*] *tacacs+-server-tag*

構文の説明

privilege *level*	**privilege** コマンドを使用してコマンドの特権レベルをカスタマイズする場合、最小特権レベルを指定することによって、ASA で処理の対象とするコマンドを制限できます。最小特権レベルよりも下のコマンドは、ASA で処理の対象となりません。 (注) 廃止されたコマンドを入力して **privilege** キーワードをイネーブルにした場合、廃止されたコマンドのアカウンティング情報は ASA によって送信されません。廃止されたコマンドを処理の対象とするには、**privilege** キーワードをディセーブルにします。CLI では数多くの廃止されたコマンドがまだ受け入れられています。これらのコマンドは、現在受け入れられるコマンドに CLI で変換される場合もあります。廃止されたコマンドは、CLI のヘルプまたはこのマニュアルには記載されていません。
tacacs+-server-tag	**aaa-server protocol** コマンドで指定するように、アカウンティング レコードの送信先の TACACS+ サーバまたはサーバのグループを指定します。

デフォルト

デフォルトの特権レベルは 0 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

aaa accounting command コマンドを設定すると、管理者が入力する **show** コマンド以外の各コマンドが記録され、アカウンティング サーバに送信されます。

例

次に、サポート対象のコマンドについてアカウンティング レコードが生成され、それらのレコードが adminserver という名前のグループからサーバに送信されることを指定する例を示します。

```
ciscoasa(config)# aaa accounting command adminserver
```

関連コマンド

コマンド	説明
aaa accounting	TACACS+ または RADIUS ユーザ アカウンティングをイネーブルまたはディセーブルにします（**aaa-server** コマンドで指定したサーバで）。
clear configure aaa	設定した AAA アカウンティングの値を削除またはリセットします。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa accounting console

管理者アクセスの AAA アカウンティングのサポートをイネーブルにするには、グローバル コンフィギュレーション モードで **aaa accounting console** コマンドを使用します。管理者アクセスの AAA アカウンティングのサポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting {**serial** | **telnet** | **ssh** | **enable**} **console** *server-tag*

no aaa accounting {**serial** | **telnet** | **ssh** | **enable**} **console** *server-tag*

構文の説明

enable	特権 EXEC モードの開始と終了を示すアカウンティング レコードの生成をイネーブルにします。
serial	シリアル コンソール インターフェイスを介して確立される admin セッションの確立と終了を示すアカウンティング レコードの生成をイネーブルにします。
server-tag	**aaa-server protocol** コマンドで定義された、アカウンティング レコードの送信先のサーバ グループを指定します。有効なサーバ グループ プロトコルは RADIUS と TACACS+ です。
ssh	SSH で作成される admin セッションの確立と終了を示すアカウンティング レコードの生成をイネーブルにします。
telnet	Telnet で作成される admin セッションの確立と終了を示すアカウンティング レコードの生成をイネーブルにします。

デフォルト

デフォルトでは、管理アクセス用の AAA アカウンティングはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

aaa-server コマンドで指定済みのサーバ グループの名前を指定する必要があります。

例

次に、イネーブル アクセスについてアカウンティング レコードが生成され、それらのレコードが adminserver という名前のサーバに送信されることを指定する例を示します。

```
ciscoasa(config)# aaa accounting enable console adminserver
```

関連コマンド

コマンド	説明
aaa accounting match	TACACS+ または RADIUS ユーザ アカウンティングをイネーブルまたはディセーブルにします(**aaa-server** コマンドで指定したサーバで)。
aaa accoungting command	管理者/ユーザが入力する各コマンド(または、指定した特権レベル以上のコマンド)が記録され、アカウンティング サーバに送信されることを指定します。
clear configure aaa	設定した AAA アカウンティングの値を削除またはリセットします。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa accounting include、exclude

ASA を介した TCP または UDP 接続のアカウンティングをイネーブルにするには、グローバル コンフィギュレーション モードで **aaa accounting include** コマンドを使用します。アカウンティングからアドレスを除外するには、**aaa accounting exclude** コマンドを使用します。アカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting {**include** | **exclude**} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

no aaa accounting {**include** | **exclude**} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

構文の説明

exclude	サービスおよびアドレスが **include** コマンドによってすでに指定されている場合に、指定したサービスおよびアドレスをアカウンティングから除外します。
include	アカウンティングが必要なサービスおよび IP アドレスを指定します。**include** ステートメントで指定されないトラフィックは処理されません。
inside_ip	セキュリティの高い側のインターフェイスの IP アドレスを指定します。このアドレスは、このコマンドを適用するインターフェイスによって、送信元アドレスまたは宛先アドレスであることがあります。セキュリティの低い側のインターフェイスにコマンドを適用する場合、このアドレスは宛先アドレスです。セキュリティの高い側のインターフェイスにコマンドを適用する場合、このアドレスは送信元アドレスです。すべてのホストを指定するには、0 を指定します。
inside_mask	内部 IP アドレスのネットワークマスクを指定します。IP アドレスが 0 の場合は 0 を使用します。ホストには 255.255.255.255 を指定します。
interface_name	ユーザがアカウンティングを要求するインターフェイスの名前を指定します。
outside_ip	(任意)セキュリティの低い側のインターフェイスの IP アドレスを指定します。このアドレスは、このコマンドを適用するインターフェイスによって、送信元アドレスまたは宛先アドレスであることがあります。セキュリティの低い側のインターフェイスにコマンドを適用する場合、このアドレスは送信元アドレスです。セキュリティの高い側のインターフェイスにコマンドを適用する場合、このアドレスは宛先アドレスです。すべてのホストを指定するには、0 を指定します。
outside_mask	(任意)外部 IP アドレスのネットワークマスクを指定します。IP アドレスが 0 の場合は 0 を使用します。ホストには 255.255.255.255 を指定します。

server_tag	**aaa-server host** コマンドで定義した AAA サーバグループを指定します。
service	アカウンティングが必要なサービスを指定します。次のいずれかの値を指定できます。 • **any** または **tcp/0**（すべての TCP トラフィックを指定します） • **FTP** • **http** • **https** • **ssh** • **telnet** • **tcp/***port* • **udp/***port*

デフォルト

デフォルトでは、管理アクセス用の AAA アカウンティングはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASA は、ASA を通過する任意の TCP トラフィックまたは UDP トラフィックについてのアカウンティング情報を RADIUS サーバまたは TACACS+ サーバに送信できます。そのトラフィックも認証されている場合、AAA サーバはユーザ名でアカウンティング情報を保持できます。トラフィックが認証済みでない場合、AAA サーバは IP アドレスによってアカウンティング情報を保持できます。アカウンティング情報には、セッションの開始時刻と終了時刻、ユーザ名、ASA を通過するセッションのバイト数、使用されたサービス、および各セッションの継続時間などの情報が含まれます。

このコマンドを使用する前に、**aaa-server** コマンドで AAA サーバを最初に指定する必要があります。

ACL で指定されているトラフィックのアカウンティングをイネーブルにするには、**aaa accounting match** コマンドを使用します。**match** コマンドは、**include** コマンドおよび **exclude** コマンドと同じコンフィギュレーションで使用できません。**include** コマンドおよび **exclude** コマンドの代わりに **match** コマンドを使用することを推奨します。**include** コマンドおよび **exclude** コマンドは ASDM によってサポートされていません。

セキュリティが同じインターフェイス間で **aaa accounting include** および **exclude** コマンドを使用することはできません。その場合は、**aaa accounting match** コマンドを使用する必要があります。

例

次に、すべての TCP 接続でアカウンティングをイネーブルにする例を示します。

```
ciscoasa(config)# aaa-server mygroup protocol tacacs+
ciscoasa(config)# aaa-server mygroup (inside) host 192.168.10.10 thekey timeout 20
ciscoasa(config)# aaa accounting include any inside 0 0 0 0 mygroup
```

関連コマンド

コマンド	説明
aaa accounting match	ACL で指定されているトラフィックのアカウンティングをイネーブルにします。
aaa accoungting command	管理者アクセスのアカウンティングをイネーブルにします。
aaa-server host	AAA サーバを設定します。
clear configure aaa	AAA コンフィギュレーションをクリアします。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa accounting match

ASA を介した TCP および UDP 接続のアカウンティングをイネーブルにするには、グローバル コンフィギュレーション モードで **aaa accounting match** コマンドを使用します。トラフィックのアカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting match *acl_name interface_name server_tag*

no aaa accounting match *acl_name interface_name server_tag*

構文の説明

acl_name	ACL 名の一致によるアカウンティングが必要なトラフィックを指定します。ACL 内の permit エントリはアカウンティングの対象となり、deny エントリはアカウンティングから免除されます。このコマンドは、TCP トラフィックおよび UDP トラフィックについてのみサポートされます。このコマンドを入力し、他のプロトコルを許可する ACL をこのコマンドが参照している場合、警告メッセージが表示されます。
interface_name	ユーザがアカウンティングを要求するインターフェイスの名前を指定します。
server_tag	**aaa-server** コマンドによって定義される AAA サーバ グループ タグを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASA は、ASA を通過する任意の TCP トラフィックまたは UDP トラフィックについてのアカウンティング情報を RADIUS サーバまたは TACACS+ サーバに送信できます。そのトラフィックも認証されている場合、AAA サーバはユーザ名でアカウンティング情報を保持できます。トラフィックが認証済みでない場合、AAA サーバは IP アドレスによってアカウンティング情報を保持できます。アカウンティング情報には、セッションの開始時刻と終了時刻、ユーザ名、ASA を通過するセッションのバイト数、使用されたサービス、および各セッションの継続時間などの情報が含まれます。

このコマンドを使用する前に、**aaa-server** コマンドで AAA サーバを最初に指定する必要があります。

AAA サーバ プロトコル コンフィギュレーション モードで **accounting-mode** コマンドを使用して同時アカウンティングをイネーブルにしない限り、アカウンティング情報はサーバ グループ内のアクティブなサーバにのみ送信されます。

aaa accounting match コマンドは、**aaa accounting include** および **exclude** コマンドと同じコンフィギュレーションの中では使用できません。**include** コマンドおよび **exclude** コマンドの代わりに **match** コマンドを使用することを推奨します。**include** コマンドおよび **exclude** コマンドは ASDM によってサポートされていません。

例

次に、特定の ACL acl2 と一致するトラフィックのアカウンティングをイネーブルにする例を示します。

```
ciscoasa(config)# access-list acl12 extended permit tcp any any
ciscoasa(config)# aaa accounting match acl2 outside radserver1
```

関連コマンド

コマンド	説明
aaa accounting include、exclude	コマンドで IP アドレスを直接指定することによって、アカウンティングをイネーブルにします。
access-list extended	ACL を作成します。
clear configure aaa	AAA コンフィギュレーションを削除します。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa authentication console

シリアル、SSH、HTTPS（ASDM）、または Telnet 接続で ASA CLI にアクセスするユーザを認証するか、**enable** コマンドを使用して特権 EXEC モードにアクセスするユーザを認証するには、グローバル コンフィギュレーション モードで **aaa authentication console** コマンドを使用します。認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authentication {**serial** | **enable** | **telnet** | **ssh** | **http**} **console** {**LOCAL** | *server_group* [**LOCAL**]}

no aaa authentication {**serial** | **enable** | **telnet** | **ssh** | **http**} **console** {**LOCAL** | *server_group* [**LOCAL**]}

構文の説明

enable	**enable** コマンドを使用して特権 EXEC モードにアクセスするユーザを認証します。
http	HTTPS で ASA にアクセスする ASDM ユーザを認証します。デフォルトでは、ASDM は空白のユーザ名とイネーブル パスワードを受け入れ、このコマンドを設定しなくても認証にローカル データベースを使用することもできます。このコマンドは、空白のユーザ名とイネーブル パスワードによるログインを許可しません。 **aaa** コマンドが定義されているが、HTTPS 認証によってタイムアウトが要求される場合（AAA サーバがダウンしているか使用できないことを意味する）は、空白のユーザ名とイネーブル パスワードを使用して、ASA にアクセスできます。デフォルトでは、イネーブル パスワードは設定されていません。

LOCAL	認証にローカル データベースを使用します。**LOCAL** キーワードは大文字と小文字が区別されます。ローカル データベースが空の場合、次の警告メッセージが表示されます。
	
	`Warning:local database is empty! Use 'username' command to define local users.`
	
	コンフィギュレーション内にまだ **LOCAL** キーワードがあるときにローカル データベースが空になった場合、次の警告メッセージが表示されます。
	
	`Warning:Local user database is empty and there are still commands using 'LOCAL' for authentication.`

server-tag [**LOCAL**]	**aaa-server** コマンドによって定義される AAA サーバ グループ タグを指定します。HTTPS 管理認証では AAA サーバ グループ用に SDI プロトコルがサポートされません。 *server-tag* 引数に加えて **LOCAL** キーワードを使用すると、AAA サーバを使用できない場合に、フォールバック方式としてローカル データベースを使用するように ASA を設定できます。**LOCAL** キーワードは大文字と小文字が区別されます。ローカル データベースでは AAA サーバと同じユーザ名およびパスワードを使用することを推奨します。これは、ASA のプロンプトでは、いずれの方式が使用されているかが示されないためです。
serial	シリアル コンソール ポートを使用して ASA にアクセスするユーザを認証します。

ssh	SSH を使用して ASA にアクセスするパスワードを持つユーザを認証します。ローカル **ユーザ名**の場合、**ssh authentication** コマンドを使用したパスワード認証の代わりに、公開キー認証を有効にすることができます。バージョン 9.6(2) および 9.7(1) では、**ssh authentication** には、**aaa authentication ssh console LOCAL** コマンドが必須です。 9.6(1) 以前および 9.6(3)/9.8(1) 以降では、**aaa authentication ssh console LOCAL** コマンドを公開キー認証用に設定する必要はありません。このコマンドはパスワードを持つユーザにのみ適用され、LOCAL だけでなく任意のサーバ タイプを指定できます。たとえば、ローカル データベースを使用し、公開キー認証を利用できるユーザもいれば、RADIUS とともにパスワードを使用できるユーザもいます。
telnet	Telnet を使用して ASA にアクセスするユーザを認証します。**aaa authentication telnet console** コマンドが定義されていない場合は、ASA のログイン パスワード（**password** コマンドで設定）で、ASA CLI にアクセスできます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(2)	**pix** または **asa** ユーザ名とログイン パスワードで SSH を使用して ASA に接続することができなくなりました。SSH を使用するには、**aaa authentication ssh console LOCAL** コマンド（CLI）または [Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication (ASDM)] を使用して AAA 認証を設定してから、ローカル ユーザを定義する必要があります。ローカル ユーザを定義するには、**username** コマンド（CLI）を入力するか、[Configuration] > [Device Management] > [Users/AAA] > [User Accounts (ASDM)] を選択します。ローカル データベースの代わりに AAA サーバを認証に使用する場合、ローカル認証もバックアップの手段として設定しておくことをお勧めします。

リリース	変更内容
9.6(2)	**ssh authentication** には、**aaa authentication ssh console LOCAL** コマンドが必須です。バージョン 9.6(2) 以降では、パスワードを定義せずに**ユーザ名**を作成できるため、公開キー認証のみが必要となります。
9.6(3)/9.8(1)	SSH 公開キー認証を使用するユーザの認証とパスワードを使用するユーザの認証を区別します。AAA SSH 認証（**aaa authentication ssh console**）を明示的にイネーブルにする必要がなくなりました。ユーザに **ssh authentication** コマンドを設定すると、このタイプの認証を使用するユーザのローカル認証がデフォルトでイネーブルになります。さらに、明示的に AAA SSH 認証を設定すると、パスワードを持つユーザ名のみにこの認証が適用されます。また、AAA サーバ タイプを使用できます。

使用上のガイドライン

ASA で Telnet、SSH、または HTTPS ユーザを認証する前に、**telnet** コマンド、**ssh** コマンド、または **http** コマンドを使用して ASA へのアクセスを設定する必要があります。これらのコマンドでは、ASA との通信を許可する IP アドレスを指定します。

ASA へのログイン

ASA に接続した後、ログインしてユーザ EXEC モードにアクセスします。

- シリアル アクセスの認証を有効にしていない場合は、ユーザ名またはパスワードを入力しません。
- Telnet の認証をイネーブルにしていない場合は、ユーザ名を入力しません。ログイン パスワード（**password** コマンドで設定）を入力します。
- このコマンドを使用して Telnet または SSH 認証をイネーブルにした場合は、AAA サーバまたはローカル ユーザ データベースで定義されているユーザ名とパスワードを入力します。

特権 EXEC モードへのアクセス

特権 EXEC モードを開始するには、**enable** コマンドまたは **login** コマンドを入力します（ローカル データベースのみを使用している場合）。

- enable 認証を設定していない場合は、**enable** コマンドを入力するときにシステム イネーブル パスワード（**enable password** コマンドで設定）を入力します。ただし、enable 認証を使用しない場合、**enable** コマンドを入力した後は、特定のユーザとしてログインしていません。ユーザ名を維持するには、enable 認証を使用してください。
- enable 認証を設定している場合、ASA によってユーザ名とパスワードの入力が求められます。

ローカル データベースを使用する認証の場合、**login** コマンドを使用できます。このコマンドでは、ユーザ名は維持されますが、認証をオンにするコンフィギュレーションは必要ありません。

ASDM へのアクセス

デフォルトでは、ブランクのユーザ名と **enable password** コマンドによって設定されたイネーブル パスワードを使用して ASDM にログインできます。ただし、ログイン画面で（ユーザ名をブランクのままにしないで）ユーザ名とパスワードを入力した場合は、ASDM によってローカル データベースで一致がチェックされます。

HTTPS 認証では AAA サーバ グループ用の SDI プロトコルがサポートされません。HTTPS 認証のユーザ名プロンプトの最大長は 30 文字です。パスワードの最大長は 16 文字です。

システム実行スペースでの AAA コマンドのサポートなし

マルチ コンテキスト モードでは、システム コンフィギュレーションで AAA コマンドを設定できません。

許可されるログイン試行の回数

次の表に示すように、**aaa authentication console** コマンドで選択するオプションによって、ASA CLI への認証されたアクセスに対するプロンプトのアクションは異なります。

オプション	許可されるログイン試行の回数
enable	3 回失敗するとアクセスが拒否される。
serial	成功するまで何回も試行できる。
ssh	3 回失敗するとアクセスが拒否される。
telnet	成功するまで何回も試行できる。
http	成功するまで何回も試行できる。

例

次に、「radius」というサーバ タグの RADIUS サーバへの Telnet 接続で、**aaa authentication console** コマンドを使用する例を示します。

```
ciscoasa(config)# aaa authentication telnet console radius
```

次に、サーバ グループ「AuthIn」を enable 認証用に指定する例を示します。

```
ciscoasa(config)# aaa authentication enable console AuthIn
```

次に、**aaa authentication console** コマンドを使用して、グループ「svrgrp1」内のすべてのサーバが利用できない場合に LOCAL ユーザ データベースにフォールバックさせる例を示します。

```
ciscoasa(config)# aaa-server svrgrp1 protocol tacacs
ciscoasa(config)# aaa authentication ssh console svrgrp1 LOCAL
```

関連コマンド

コマンド	説明
aaa authentication	ユーザ認証をイネーブルまたはディセーブルにします。
aaa-server host	ユーザ認証に使用する AAA サーバを指定します。
clear configure aaa	設定した AAA アカウンティングの値を削除またはリセットします。
ldap map-attributes	LDAP 属性を、ASA で認識できる RADIUS 属性にマッピングします。
service-type	ローカル ユーザの CLI アクセスを制限します。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa authentication include、exclude

ASA を経由する接続の認証をイネーブルにするには、グローバル コンフィギュレーション モードで **aaa authentication include** コマンドを使用します。認証をディセーブルにするには、このコマンドの **no** 形式を使用します。認証からアドレスを除外するには、**aaa authentication exclude** コマンドを使用します。認証からアドレスを除外しないようにするには、このコマンドの **no** 形式を使用します。

aaa authentication {include | exclude} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] {*server_tag* | **LOCAL**}

no aaa authentication {include | exclude} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] {*server_tag* | **LOCAL**}

構文の説明

exclude	サービスおよびアドレスが **include** コマンドによってすでに指定されている場合に、指定したサービスおよびアドレスを認証から除外します。
include	認証が必要なサービスおよび IP アドレスを指定します。**include** ステートメントで指定されないトラフィックは処理されません。
inside_ip	セキュリティの高い側のインターフェイスの IP アドレスを指定します。このアドレスは、このコマンドを適用するインターフェイスによって、送信元アドレスまたは宛先アドレスであることがあります。セキュリティの低い側のインターフェイスにコマンドを適用する場合、このアドレスは宛先アドレスです。セキュリティの高い側のインターフェイスにコマンドを適用する場合、このアドレスは送信元アドレスです。すべてのホストを指定するには、0 を指定します。
inside_mask	内部 IP アドレスのネットワーク マスクを指定します。IP アドレスが 0 の場合は 0 を使用します。ホストには 255.255.255.255 を指定します。
interface_name	ユーザが認証を要求するインターフェイスの名前を指定します。
LOCAL	ローカル ユーザ データベースを指定します。
outside_ip	(任意)セキュリティの低い側のインターフェイスの IP アドレスを指定します。このアドレスは、このコマンドを適用するインターフェイスによって、送信元アドレスまたは宛先アドレスであることがあります。セキュリティの低い側のインターフェイスにコマンドを適用する場合、このアドレスは送信元アドレスです。セキュリティの高い側のインターフェイスにコマンドを適用する場合、このアドレスは宛先アドレスです。すべてのホストを指定するには、0 を指定します。
outside_mask	(任意)外部 IP アドレスのネットワーク マスクを指定します。IP アドレスが 0 の場合は 0 を使用します。ホストには 255.255.255.255 を指定します。

server_tag	**aaa-server** コマンドによって定義される AAA サーバ グループを指定します。
service	認証が必要なサービスを指定します。次のいずれかの値を指定できます。 • **any** または **tcp/0**（すべての TCP トラフィックを指定します） • **FTP** • **http** • **https** • **ssh** • **telnet** • **tcp/***port*[**-***port*] • **udp/***port*[**-***port*] • **icmp/***type* • *protocol*[**/***port*[**-***port*]] プロトコルまたはサービスへのネットワーク アクセス認証を要求するように ASA を設定することは、すべてのプロトコルまたはサービスについて可能ですが、ユーザが直接認証を受けることができるのは、HTTP、HTTPS、Telnet、または FTP だけです。ユーザがこれらのサービスのいずれかの認証を受けないと、ASA は認証が必要な他のトラフィックを許可しません。詳細については、「使用上のガイドライン」を参照してください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ACL で指定されているトラフィックの認証をイネーブルにするには、**aaa authentication match** コマンドを使用します。**match** コマンドは、**include** コマンドおよび **exclude** コマンドと同じコンフィギュレーションで使用できません。**include** コマンドおよび **exclude** コマンドの代わりに **match** コマンドを使用することを推奨します。**include** コマンドおよび **exclude** コマンドは ASDM によってサポートされていません。

セキュリティが同じインターフェイス間で **aaa authentication include** および **exclude** コマンドを使用することはできません。その場合は、**aaa authentication match** コマンドを使用する必要があります。

TCP セッションのシーケンス番号は、シーケンス ランダム化をディセーブルにした場合でもランダム化されることがあります。この現象は、AAA サーバが TCP セッションを代行処理してユーザを認証し、アクセスを許可する場合に発生します。

一度だけの認証

所定の IP アドレスのユーザは、認証セッションが期限切れになるまで、すべてのルールおよびタイプに対して一度だけ認証を受ける必要があります(タイムアウト値については、**timeout uauth** コマンドを参照してください)。たとえば、ASA に Telnet と FTP の認証を設定した場合、最初に Telnet の認証に成功したユーザは、その認証セッションが存在する限り、FTP の認証を受ける必要がありません。

HTTP 認証または HTTPS 認証では、**timeout uauth** コマンドが非常に小さな値に設定されている場合でも、一度認証されたユーザの再認証が必要になることはありません。これは、ブラウザが「Basic=Uuhjksdkfhk==」文字列をキャッシュして、当該サイトへの後続の接続すべてに使用するためです。このストリングがクリアされるのは、ユーザが Web ブラウザのインスタンスをすべて終了し、再起動したときだけです。キャッシュをフラッシュしても意味がありません。

認証確認を受けるために必要なアプリケーション

プロトコルまたはサービスへのネットワーク アクセス認証を要求するように ASA を設定することは、すべてのプロトコルまたはサービスについて可能ですが、ユーザが直接認証を受けることができるのは、HTTP、HTTPS、Telnet、または FTP だけです。ユーザがこれらのサービスのいずれかの認証を受けないと、ASA は認証が必要な他のトラフィックを許可しません。

ASA が AAA 用にサポートしている認証ポートは固定値です。

- ポート 21 は FTP 用
- ポート 23 は Telnet 用
- ポート 80 は HTTP 用
- ポート 443 は HTTPS 用

ASA 認証プロンプト

Telnet および FTP の場合、ASA は認証プロンプトを生成します。

HTTP の場合、ASA はデフォルトで基本 HTTP 認証を使用し、認証プロンプトを提供します。ユーザがユーザ名とパスワードを入力できる内部 Web ページにユーザをリダイレクトするように ASA を設定することもできます(**aaa authentication listener** コマンドで設定します)。

HTTPS の場合、ASA はカスタム ログイン画面を生成します。ユーザがユーザ名とパスワードを入力できる内部 Web ページにユーザをリダイレクトするように ASA を設定することもできます(**aaa authentication listener** コマンドで設定します)。

リダイレクションは、基本方式を強化したものです。これは、認証時に向上したユーザ エクスペリエンスが提供されると同時に、Easy VPN でもファイアウォール モードでも、HTTP および HTTPS と同じユーザ エクスペリエンスが提供されるためです。また、ASA での直接認証もサポートしています。

基本 HTTP 認証を使用し続けた方がよい場合もあります。ASA でリスニング ポートを開く必要がない場合や、ルータ上の NAT を使用しているため、ASA で提供される Web ページの変換ルールを作成する必要がない場合、あるいは基本 HTTP 認証の方がネットワークで効果的に機能する場合です。たとえば、電子メールに URL が埋め込まれている場合などのように、ブラウザ以外のアプリケーションでは基本認証の方が適していることがあります。

正常に認証されると、ASA により元の宛先にリダイレクトされます。宛先サーバにも独自の認証がある場合、ユーザは別のユーザ名とパスワードを入力します。基本 HTTP 認証を使用していて、宛先サーバ用に別のユーザ名とパスワードを入力する必要がある場合は、**virtual http** コマンドを設定する必要があります。

(注) **aaa authentication secure-http-client** コマンドを使用しないまま HTTP 認証を使用すると、ユーザ名とパスワードはクリア テキストでクライアントから ASA に送信されます。HTTP 認証をイネーブルにする場合は、必ず **aaa authentication secure-http-client** コマンドを使用することを推奨します。

FTP の場合、ASA ユーザ名、アット マーク（@）、FTP ユーザ名（name1@name2）を入力するオプションがあります。パスワードには、ASA パスワード、アット マーク（@）、FTP パスワード（password1@password2）を入力します。たとえば、次のテキストを入力します。

```
name> asa1@partreq
password> letmein@he110
```

この機能は、複数のログインを必要とするファイアウォールをカスケード接続している場合に有用です。複数の名前およびパスワードは、複数のアット マーク（@）で区切ることができます。

許可されるログイン試行の回数は、サポートされているプロトコルによって次のように異なります。

プロトコル	許可されるログイン試行の回数
FTP	間違ったパスワードを入力すると、接続がただちにドロップされる。
HTTP HTTPS	ログインが成功するまで、プロンプトが何回も再表示される。
Telnet	4 回失敗すると接続がドロップされる。

スタティック PAT および HTTP

HTTP 認証では、スタティック PAT が設定されている場合、ASA は実際のポートをチェックします。ASA は、マッピング ポートにかかわらず、実際のポート 80 を宛先とするトラフィックを検出した場合、HTTP 接続を代行受信し、認証を実行します。

たとえば、次のように、外部 TCP ポート 889 がポート 80（www）に変換され、関係するすべての ACL でこのトラフィックが許可されるとします。

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 www netmask 255.255.255.255
```

この場合、ユーザはポート 889 で 10.48.66.155 にアクセスを試み、ASA はそのトラフィックを代行受信して、HTTP 認証を実行します。ASA が HTTP 接続の完了を許可する前に、ユーザの Web ブラウザには HTTP 認証ページが表示されます。

次の例のように、ローカル ポートがポート 80 ではないとします。

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 111 netmask 255.255.255.255
```

この場合、ユーザには認証ページは表示されません。代わりに、ASA は Web ブラウザにエラーメッセージを送信して、要求されたサービスを使用する前にユーザが認証を受ける必要があることを通知します。

ASA での直接認証

HTTP、HTTPS、Telnet、または FTP が ASA を通過することを許可せず、他のタイプのトラフィックに対しては認証を課す場合、**aaa authentication listener** コマンドを設定することで、HTTP または HTTPS を使用して ASA で直接認証できます。

インターフェイスの AAA をイネーブルにすると、次の URL で ASA の直接認証を受けることができます。

http://*interface_ip*[**:***port*]**/netaccess/connstatus.html**
https://*interface_ip*[**:***port*]**/netaccess/connstatus.html**

または、仮想 Telnet を設定する方法もあります（**virtual telnet** コマンドを使用）。仮想 Telnet を設定した場合、ユーザは ASA 上で設定された所定の IP アドレスに Telnet で接続し、ASA が Telnet プロンプトを表示します。

例

次に、外部インターフェイスで TCP トラフィックを認証に含める例を示します。内部 IP アドレス 192.168.0.0 およびネットマスク 255.255.0.0、すべてのホストの外部 IP アドレスを指定し、tacacs+ という名前のサーバ グループを使用します。2 番めのコマンドラインでは、外部インターフェイスで Telnet トラフィックを除外します。内部アドレス 192.168.38.0、すべてのホストの外部 IP アドレスを指定します。

```
ciscoasa(config)# aaa authentication include tcp/0 outside 192.168.0.0 255.255.0.0 0 0
tacacs+
ciscoasa(config)# aaa authentication exclude telnet outside 192.168.38.0 255.255.255.0 0 0
tacacs+
```

次に、*interface-name* パラメータの使用方法を示す例を示します。ASA には、内部ネットワーク 192.168.1.0、外部ネットワーク 209.165.201.0（サブネット マスク 255.255.255.224）、および境界ネットワーク 209.165.202.128（サブネット マスク 255.255.255.224）があります。

次の例では、内部ネットワークから外部ネットワークへの接続の認証をイネーブルにします。

```
ciscoasa(config)# aaa authentication include tcp/0 inside 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224 tacacs+
```

次の例では、内部ネットワークから境界ネットワークへの接続の認証をイネーブルにします。

```
ciscoasa(config)#aaa authentication include tcp/0 inside 192.168.1.0 255.255.255.0
209.165.202.128 255.255.255.224 tacacs+
```

次の例では、外部ネットワークから内部ネットワークへの接続の認証をイネーブルにします。

```
ciscoasa(config)# aaa authentication include tcp/0 outside 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224 tacacs+
```

次の例では、外部ネットワークから境界ネットワークへの接続の認証をイネーブルにします。

```
ciscoasa(config)# aaa authentication include tcp/0 outside 209.165.202.128 255.255.255.224
209.165.201.0 255.255.255.224 tacacs+
```

次の例では、境界ネットワークから外部ネットワークへの接続の認証をイネーブルにします。

```
ciscoasa(config)#aaa authentication include tcp/0 perimeter 209.165.202.128
255.255.255.224 209.165.201.0 255.255.255.224 tacacs+
```

関連コマンド

コマンド	説明
aaa authentication console	管理アクセスの認証をイネーブルにします。
aaa authentication match	通過トラフィックのユーザ認証をイネーブルにします。
aaa authentication secure-http-client	HTTP 要求が ASA を通過するのを許可する前に、ASA に対してセキュアなユーザ認証方式を提供します。
aaa-server	グループ関連のサーバ属性を設定します。
aaa-server host	ホスト関連の属性を設定します。

aaa authentication listener

HTTP/HTTPS リスニング ポートでネットワーク ユーザを認証できるようにするには、グローバル コンフィギュレーション モードで **aaa authentication listener** コマンドを使用します。リスニング ポートをイネーブルにすると、ASA では直接接続に対して、およびオプションで通過トラフィックに対して認証ページを提供します。リスナーをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authentication listener {**http** | **https**} *interface_name* [**port** *portnum*] [**redirect**]

no aaa authentication listener {**http** | **https**} *interface_name* [**port** *portnum*] [**redirect**]

構文の説明

{**http** | **https**}	リッスンするプロトコル（HTTP または HTTPS）を指定します。このコマンドは、プロトコルごとに別々に入力します。
interface_name	リスナーをイネーブルにするインターフェイスを指定します。
port *portnum*	ASA で直接トラフィックまたはリダイレクトされたトラフィックをリッスンするポート番号を指定します。デフォルトは 80（HTTP）および 443（HTTPS）です。任意のポート番号を使用して同じ機能を保持できますが、直接認証ユーザがそのポート番号を認識している必要があります。これは、リダイレクトされたトラフィックは正しいポート番号に自動的に送信されますが、直接認証するユーザは、ポート番号を手動で指定する必要があるためです。
redirect	ASA によって提供される認証 Web ページに通過トラフィックをリダイレクトします。このキーワードを指定しないと、ASA インターフェイスへのトラフィックだけが認証 Web ページにアクセスできます。

デフォルト

デフォルトでは、リスナー サービスはディセーブルであり、HTTP 接続では基本 HTTP 認証が使用されます。リスナーをイネーブルにした場合、デフォルトのポートは 80（HTTP）および 443（HTTPS）です。

7.2(1) からアップグレードする場合、リスナーはポート 1080（HTTP）および 1443（HTTPS）でイネーブルになります。**redirect** オプションもイネーブルになります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(2)	このコマンドが追加されました。

使用上のガイドライン

aaa authentication listener コマンドを使用しないと、**aaa authentication match** または **aaa authentication include** コマンドの設定後に HTTP/HTTPS ユーザが ASA で認証する必要があるときに、ASA では基本 HTTP 認証が使用されます。HTTPS の場合、ASA はカスタム ログイン画面を生成します。

aaa authentication listener コマンドを **redirect** キーワードを指定して設定すると、ASA により、すべての HTTP/HTTPS 認証要求は ASA によって提供される Web ページにリダイレクトされます。

リダイレクションは、基本方式を強化したものです。これは、認証時に向上したユーザ エクスペリエンスが提供されると同時に、Easy VPN でもファイアウォール モードでも、HTTP および HTTPS と同じユーザ エクスペリエンスが提供されるためです。また、ASA での直接認証もサポートしています。

基本 HTTP 認証を使用し続けた方がよい場合もあります。ASA でリスニング ポートを開く必要がない場合や、ルータ上の NAT を使用しているため、ASA で提供される Web ページの変換ルールを作成する必要がない場合、あるいは基本 HTTP 認証の方がネットワークで効果的に機能する場合です。たとえば、電子メールに URL が埋め込まれている場合などのように、ブラウザ以外のアプリケーションでは基本認証の方が適していることがあります。

aaa authentication listener コマンドを **redirect** オプションを*指定しない*で入力した場合、ASA での直接認証のみがイネーブルとなり、通過トラフィックでは基本 HTTP 認証が使用されます。**redirect** オプションによって、直接認証と通過トラフィック認証の両方がイネーブルになります。直接認証は、認証チャレンジをサポートしないトラフィック タイプを認証するときに役立ちます。他のサービスを使用する前に、各ユーザを ASA で直接認証できます。

(注) **redirect** オプションをイネーブルにした場合、インターフェイスの IP アドレスを変換する同じインターフェイス、およびリスナー用に使用される同じポートに対して、スタティック PAT も設定することはできません。NAT は成功しますが、認証は失敗します。たとえば、次のコンフィギュレーションはサポートされません。

```
ciscoasa(config)# static (inside,outside) tcp interface www 192.168.0.50 www netmask
255.255.255.255
ciscoasa(config)# aaa authentication listener http outside redirect
```

次のコンフィギュレーションはサポートされます。リスナーによって、ポートはデフォルトの 80 ではなく 1080 が使用されます。

```
ciscoasa(config)# static (inside,outside) tcp interface www 192.168.0.50 www netmask
255.255.255.255
ciscoasa(config)# aaa authentication listener http outside port 1080 redirect
```

例

次に、HTTP および HTTPS 接続をデフォルトのポートにリダイレクトするように ASA を設定する例を示します。

```
ciscoasa(config)# aaa authentication listener http inside redirect
ciscoasa(config)# aaa authentication listener https inside redirect
```

次に、ASA への直接認証要求を許可する例を示します。通過トラフィックによって基本 HTTP 認証が使用されます。

```
ciscoasa(config)# aaa authentication listener http inside
ciscoasa(config)# aaa authentication listener https inside
```

次に、HTTP および HTTPS 接続をデフォルト以外のポートにリダイレクトするように ASA を設定する例を示します。

```
ciscoasa(config)# aaa authentication listener http inside port 1100 redirect
ciscoasa(config)# aaa authentication listener https inside port 1400 redirect
```

関連コマンド

コマンド	説明
aaa authentication listener no-logout-button	カットスルー プロキシのログイン ページからログアウト ボタンを削除します。
aaa authentication match	通過トラフィックのユーザ認証を設定します。
aaa authentication secure-http-client	SSL をイネーブルにし、HTTP クライアントと ASA の間のユーザ名とパスワードのセキュアな交換をイネーブルにします。
clear configure aaa	設定済みの AAA コンフィギュレーションを削除します。
show running-config aaa	AAA コンフィギュレーションを表示します。
virtual http	基本 HTTP 認証による HTTP 認証のカスケードをサポートします。

aaa authentication listener no-logout-button

カットスルー プロキシのポータル ページからログアウト ボタンを削除するには、グローバル コンフィギュレーション モードで **aaa authenticationlistener no-logout-button** コマンドを使用します。ログアウト ボタンを復元する場合は、このコマンドの **no** 形式を入力します。

aaa authentication listener no-logout-button *interface_name*

no aaa authentication listener no-logout-button *interface_name*

構文の説明

interface_name	認証リスナーを有効にするインターフェイスを指定します。

デフォルト

デフォルトでは、ポータル ページにログアウト ボタンがあります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.10(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、カットスルー プロキシのポータル ページ（/netaccess/connstatus.html）には、接続ホストに対してカットスルー プロキシ セッションがすでにアクティブになっているときにアクセスされた場合、セッション情報とログアウト ボタンが表示されます。このコマンドを使用してログアウト ボタンを削除できます。

これは、ユーザが NAT デバイスの背後から接続し、IP アドレスで識別できない場合に便利です。1 人のユーザがログアウトすると、その IP アドレスのすべてのユーザがログアウトされます。

例

次の例では、内部インターフェイスで HTTP および HTTPS リスナーを有効にし、認証が必要なすべての HTTP/HTTPS トラフィックをリダイレクトするように ASA を設定しています。

```
ciscoasa(config)# aaa authentication listener http inside redirect
ciscoasa(config)# aaa authentication listener https inside redirect
ciscoasa(config)# aaa authentication listener no-logout-button inside
```

関連コマンド

コマンド	説明
aaa authentication listener http/https	HTTP/HTTPS リスニング ポートでネットワーク ユーザを認証できるようにします。

aaa authentication login-history

ログイン履歴の期間を設定するには、グローバル コンフィギュレーション モードで **aaa authentication login-history** コマンドを使用します。ログイン履歴をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authentication login-history duration *days*

no aaa authentication login-history [**duration** *days*]

構文の説明

duration *days*	1 ～ 365 の範囲で日数を設定します。デフォルトは 90 です。

コマンド デフォルト

デフォルトは、90 日です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.8(1)	このコマンドが追加されました。

使用上のガイドライン

1 つ以上の CLI 管理方式（SSH、Telnet、シリアル コンソール）でローカル AAA 認証をイネーブルにした場合、AAA サーバのユーザ名またはローカル データベースのユーザ名にこの機能が適用されます。

ASDM のログインは履歴に保存されません。

ログイン履歴はユニット（装置）ごとに保存されます。フェールオーバーおよびクラスタリング環境では、各ユニットが自身のログイン履歴のみを保持します。

ログインの履歴データは、リロードされると保持されなくなります。

ログイン履歴を表示するには、**show aaa login-history** コマンドを使用します。

例

次に、ログイン履歴を 365 日に設定する例を示します。

```
ciscoasa(config)# aaa authentication login-history duration 365
```

ユーザがログインすると、以下の SSH の例のように、自身のログイン履歴が表示されます。

```
cugel@10.86.194.108's password:
User cugel logged in to ciscoasa at 21:04:10 UTC Dec 14 2016
Last login: 21:01:44 UTC Dec 14 2016 from ciscoasa console
Successful logins over the last 90 days: 6
Authentication failures since the last login: 0
Type help or '?' for a list of available commands.
ciscoasa>
```

関連コマンド

コマンド	説明
password-history	直前の **username** パスワードを保存します。ユーザはこのコマンドを設定できません。
password-policy reuse-interval	**username** パスワードの再利用を禁止します。
password-policy username-check	**username** の名前と一致するパスワードを禁止します。
show aaa login-history	ローカル **username** のログイン履歴を表示します。
username	ローカル ユーザを設定します。

aaa authentication match

ASA を通じた接続の認証をイネーブルにするには、グローバル コンフィギュレーション モードで **aaa authentication match** コマンドを使用します。認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authentication match *acl_name interface_name* {*server_tag* | **LOCAL**} **user-identity**

no aaa authentication match *acl_name interface_name* {*server_tag* | **LOCAL**} **user-identity**

構文の説明

acl_name	拡張 ACL 名を指定します。
interface_name	ユーザを認証するインターフェイスの名前を指定します。
LOCAL	ローカル ユーザ データベースを指定します。
server_tag	**aaa-server** コマンドによって定義される AAA サーバ グループ タグを指定します。
user-identity	アイデンティティ ファイアウォールにマッピングされるユーザ アイデンティティを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	**user-identity** キーワードが追加されました。

使用上のガイドライン

aaa authentication match コマンドは、**include** コマンドおよび **exclude** コマンドと同じコンフィギュレーションでは使用できません。**include** コマンドおよび **exclude** コマンドの代わりに **match** コマンドを使用することを推奨します。**include** コマンドおよび **exclude** コマンドは ASDM によってサポートされていません。

TCP セッションのシーケンス番号は、シーケンス ランダム化をディセーブルにした場合でもランダム化されることがあります。この現象は、AAA サーバが TCP セッションを代行処理してユーザを認証し、アクセスを許可する場合に発生します。

One-Time 認証

所定の IP アドレスのユーザは、認証セッションが期限切れになるまで、すべてのルールおよびタイプに対して一度だけ認証を受ける必要があります（タイムアウト値については、**timeout uauth** コマンドを参照してください）。たとえば、ASA に Telnet と FTP の認証を設定した場合、最初に Telnet の認証に成功したユーザは、その認証セッションが存在する限り、FTP の認証を受ける必要がありません。

HTTP 認証または HTTPS 認証では、**timeout uauth** コマンドが非常に小さな値に設定されている場合でも、一度認証されたユーザの再認証が必要になることはありません。これは、ブラウザが「Basic=Uuhjksdkfhk==」文字列をキャッシュして、当該サイトへの後続の接続すべてに使用するためです。このストリングがクリアされるのは、ユーザが Web ブラウザのインスタンスをすべて終了し、再起動したときだけです。キャッシュをフラッシュしても意味がありません。

認証チャレンジの受信に必要なアプリケーション

プロトコルまたはサービスへのネットワーク アクセス認証を要求するように ASA を設定することは、すべてのプロトコルまたはサービスについて可能ですが、ユーザが直接認証を受けることができるのは、HTTP、HTTPS、Telnet、または FTP だけです。ユーザがこれらのサービスのいずれかの認証を受けないと、ASA は認証が必要な他のトラフィックを許可しません。

ASA が AAA 用にサポートしている認証ポートは固定値です。

- ポート 21 は FTP 用
- ポート 23 は Telnet 用
- ポート 80 は HTTP 用
- HTTPS の場合はポート 443（**aaa authentication listener** コマンドが必要）

ASA 認証プロンプト

Telnet および FTP の場合、ASA は認証プロンプトを生成します。

HTTP の場合、ASA はデフォルトで基本 HTTP 認証を使用し、認証プロンプトを提供します。ユーザがユーザ名とパスワードを入力できる内部 Web ページにユーザをリダイレクトするように ASA を設定することもできます（**aaa authentication listener** コマンドで設定します）。

HTTPS の場合、ASA はカスタム ログイン画面を生成します。ユーザがユーザ名とパスワードを入力できる内部 Web ページにユーザをリダイレクトするように ASA を設定することもできます（**aaa authentication listener** コマンドで設定します）。

リダイレクションは、基本方式を強化したものです。これは、認証時に向上したユーザ エクスペリエンスが提供されると同時に、Easy VPN でもファイアウォール モードでも、HTTP および HTTPS と同じユーザ エクスペリエンスが提供されるためです。また、ASA での直接認証もサポートしています。

基本 HTTP 認証を使用し続けた方がよい場合もあります。ASA でリスニング ポートを開く必要がない場合や、ルータ上の NAT を使用しているため、ASA で提供される Web ページの変換ルールを作成する必要がない場合、あるいは基本 HTTP 認証の方がネットワークで効果的に機能する場合です。たとえば、電子メールに URL が埋め込まれている場合などのように、ブラウザ以外のアプリケーションでは基本認証の方が適していることがあります。

正常に認証されると、ASA により元の宛先にリダイレクトされます。宛先サーバにも独自の認証がある場合、ユーザは別のユーザ名とパスワードを入力します。基本 HTTP 認証を使用していて、宛先サーバ用に別のユーザ名とパスワードを入力する必要がある場合は、**virtual http** コマンドを設定する必要があります。

(注) **aaa authentication secure-http-client** コマンドを使用しないまま HTTP 認証を使用すると、ユーザ名とパスワードはクリア テキストでクライアントから ASA に送信されます。HTTP 認証をイネーブルにする場合は、必ず **aaa authentication secure-http-client** コマンドを使用することを推奨します。

FTP の場合、ASA ユーザ名、アット マーク（@）、FTP ユーザ名（name1@name2）を入力するオプションがあります。パスワードには、ASA パスワード、アット マーク（@）、FTP パスワード（password1@password2）を入力します。たとえば、次のテキストを入力します。

```
name> asa1@partreq
password> letmein@he110
```

この機能は、複数のログインを必要とするファイアウォールをカスケード接続している場合に有用です。複数の名前およびパスワードは、複数のアット マーク（@）で区切ることができます。

許可されるログイン試行の回数は、サポートされているプロトコルによって次のように異なります。

プロトコル	許可されるログイン試行の回数
FTP	間違ったパスワードを入力すると、接続がただちにドロップされる。
HTTP HTTPS	ログインが成功するまで、プロンプトが何回も再表示される。
Telnet	4 回失敗すると接続がドロップされます。

スタティック PAT と HTTP

HTTP 認証では、スタティック PAT が設定されている場合、ASA は実際のポートをチェックします。ASA は、マッピング ポートにかかわらず、実際のポート 80 を宛先とするトラフィックを検出した場合、HTTP 接続を代行受信し、認証を実行します。

たとえば、次のように、外部 TCP ポート 889 がポート 80（www）に変換され、関係するすべての ACL でこのトラフィックが許可されるとします。

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 www netmask 255.255.255.255
```

この場合、ユーザはポート 889 で 10.48.66.155 にアクセスを試み、ASA はそのトラフィックを代行受信して、HTTP 認証を実行します。ASA が HTTP 接続の完了を許可する前に、ユーザの Web ブラウザには HTTP 認証ページが表示されます。

次の例のように、ローカル ポートがポート 80 ではないとします。

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 111 netmask 255.255.255.255
```

この場合、ユーザには認証ページは表示されません。代わりに、ASA は Web ブラウザにエラー メッセージを送信して、要求されたサービスを使用する前にユーザが認証を受ける必要があることを通知します。

ASA での直接認証

HTTP、HTTPS、Telnet、または FTP が ASA を通過することを許可せず、他のタイプのトラフィックに対しては認証を課す場合、**aaa authentication listener** コマンドを設定することで、HTTP または HTTPS を使用して ASA で直接認証できます。

インターフェイスの AAA をイネーブルにすると、次の URL で ASA の直接認証を受けることができます。

http://*interface_ip*[**:***port*]**/netaccess/connstatus.html**
https://*interface_ip*[**:***port*]**/netaccess/connstatus.html**

または、仮想 Telnet を設定する方法もあります（**virtual telnet** コマンドを使用）。仮想 Telnet を設定した場合、ユーザは ASA 上で設定された所定の IP アドレスに Telnet で接続し、ASA が Telnet プロンプトを表示します。

例

次に、**aaa authentication match** コマンドを使用する例を示します。

```
ciscoasa(config)# show access-list
access-list mylist permit tcp 10.0.0.0 255.255.255.0 192.168.2.0 255.255.255.0 (hitcnt=0)
access-list yourlist permit tcp any any (hitcnt=0)

ciscoasa(config)# show running-config aaa
aaa authentication match mylist outbound TACACS+
```

このコンテキストでは、次のコマンドは

```
ciscoasa(config)# aaa authentication match yourlist outbound tacacs
```

次のコマンドと同じです。

```
ciscoasa(config)# aaa authentication include TCP/0 outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 tacacs
```

aaa コマンド ステートメントのリストでは、**access-list** コマンド ステートメント間の順序に依存します。たとえば、次のコマンドを入力します。

```
ciscoasa(config)# aaa authentication match mylist outbound TACACS+
```

その後で、次のコマンドを入力します。

```
ciscoasa(config)# aaa authentication match yourlist outbound tacacs
```

ASA は、まず **mylist** 内の **access-list** コマンド ステートメント グループに一致があるか確かめ、次に **yourlist** 内の **access-list** コマンド ステートメント グループに一致があるかを確かめます。

ASA を介した接続の認証をイネーブルにして、アイデンティティ ファイアウォール機能と照合するには、次のコマンドを入力してください。

```
ciscoasa(config)# aaa authenticate match access_list_name inside user-identity
```

関連コマンド

コマンド	説明
aaa authorization	ユーザ認可サービスをイネーブルにします。
access-list extended	ACL を作成します。
clear configure aaa	設定済みの AAA コンフィギュレーションを削除します。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa authentication secure-http-client

SSL をイネーブルにし、HTTP クライアントと ASA の間のユーザ名とパスワードのセキュアな交換をイネーブルにするには、グローバル コンフィギュレーション モードで **aaa authentication secure-http-client** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authentication secure-http-client

no aaa authentication secure-http-client

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

aaa authentication secure-http-client コマンドによって、ユーザの HTTP ベース Web 要求が ASA を通過するのを許可する前に、ASA に対するセキュアなユーザ認証方式が提供されます。このコマンドは、SSL による HTTP カットスルー プロキシ認証に使用されます。

aaa authentication secure-http-client コマンドには、次の制限があります。

- 実行時に、最大で 64 個の HTTPS 認証プロセスが許可されます。64 個の HTTPS 認証プロセスすべてが実行されている場合、認証を必要とする 65 番目の新しい HTTPS 接続は許可されません。
- **uauth timeout 0** が設定されると（**uauth timeout** が 0 に設定される）、HTTPS 認証は機能しない場合があります。HTTPS 認証を受けた後、ブラウザが複数の TCP 接続を開始して Web ページのロードを試みると、最初の接続はそのまま許可されますが、後続の接続に対しては認証が発生します。その結果、ユーザが認証ページに正しいユーザ名とパスワードを毎回入力しても、繰り返し認証ページが表示されます。この状況を回避するには、**timeout uauth 0:0:1** コマンドで **uauth timeout** を 1 秒に設定します。ただし、この回避策では、同じ送信元 IP アドレスからアクセスした認証されていないユーザがファイアウォールを通過できる期間が 1 秒間発生します。

- HTTPS 認証は SSL ポート 443 で行われるため、HTTP クライアントから HTTP サーバ ポート 443 へのトラフィックをブロックするように、**access-list** コマンド ステートメントを設定しないでください。また、ポート 80 上の Web トラフィックに対してスタティック PAT を設定する場合は、SSL ポートに対してもスタティック PAT を設定する必要があります。次の例では、最初の行でスタティック PAT が Web トラフィックに対して設定されるため、HTTPS 認証コンフィギュレーションをサポートするために 2 番めの行を追加する必要があります。

```
static (inside,outside) tcp 10.132.16.200 www 10.130.16.10 www
static (inside,outside) tcp 10.132.16.200 443 10.130.16.10 443
```

例

次に、HTTP トラフィックがセキュアに認証されるように設定する例を示します。

```
ciscoasa(config)# aaa authentication secure-http-client
ciscoasa(config)# aaa authentication include http...
```

「...」は、*authen_service if_name local_ip local_mask* [*foreign_ip foreign_mask*] *server_tag* の値を表します。

次に、HTTPS トラフィックがセキュアに認証されるように設定するコマンドを示します。

```
ciscoasa (config)# aaa authentication include https...
```

「...」は、*authentication -service interface-name local-ip local-mask* [*foreign-ip foreign-mask*] *server-tag* の値を表します。

(注) **aaa authentication secure-https-client** コマンドは、HTTPS トラフィックには必要ありません。

関連コマンド

コマンド	説明
aaa authentication	**aaa-server** コマンドで指定したサーバ上での、LOCAL、TACACS+、または RADIUS のユーザ認証をイネーブルにします。
virtual telnet	ASA 仮想サーバにアクセスします。

aaa authorization command

コマンド認可をイネーブルにするには、グローバル コンフィギュレーション モードで **aaa authorization command** コマンドを使用します。コマンド認可をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authorization command {**LOCAL** | *tacacs+ server_tag* [**LOCAL**]}

no aaa authorization command {**LOCAL** | *tacacs+ server_tag* [**LOCAL**]}

構文の説明

LOCAL	**privilege** コマンドによって設定されるローカル コマンド特権レベルをイネーブルにします。ローカル ユーザ、RADIUS ユーザ、または LDAP ユーザ（LDAP 属性を RADIUS 属性にマッピングする場合）を CLI アクセスについて認証する場合、ASA はそのユーザをローカル データベース、RADIUS、または LDAP サーバで定義されている特権レベルに所属させます。ユーザは、ユーザ特権レベル以下のコマンドにアクセスできます。 TACACS+ サーバ グループ タグの後に **LOCAL** を指定した場合、TACACS+ サーバ グループが使用できないときにフォールバックとしてのみ、ローカル ユーザ データベースがコマンド認可に使用されます。
tacacs+ server_tag	TACACS+ 認可サーバの定義済みのサーバ グループ タグを指定します。**aaa-server** コマンドで定義した AAA サーバ グループ タグです。

デフォルト

認可のためのローカル データベースへのフォールバックはデフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	TACACS+ サーバ グループが一時的に使用できないときの LOCAL 認可へのフォールバックのサポートが追加されました。
8.0(2)	RADIUS サーバまたは LDAP サーバで定義される特権レベルのサポートが追加されました。

使用上のガイドライン

aaa authorization command コマンドでは、CLI でのコマンド実行が認可の対象かどうかを指定します。デフォルトでは、ログインするとユーザ EXEC モードにアクセスでき、最低限のコマンドだけが提供されます。**enable** コマンド（または、ローカル データベースを使用するときは **login** コマンド）を入力すると、特権 EXEC モードおよびコンフィギュレーション コマンドを含む高度なコマンドにアクセスできます。コマンドへのアクセスを制御する場合には、ASA にコマンド許可を設定し、各ユーザに許可するコマンドを制限します。

サポートされるコマンド許可方式

次の 2 つのコマンド許可方式のいずれかを使用できます。

- ローカル特権レベル：ASA でコマンド特権レベルを設定します。ローカル ユーザ、RADIUS ユーザ、または LDAP ユーザ（LDAP 属性を RADIUS 属性にマッピングする場合）を CLI アクセスについて認証する場合、ASA はそのユーザをローカル データベース、RADIUS、または LDAP サーバで定義されている特権レベルに所属させます。ユーザは、ユーザ特権レベル以下のコマンドにアクセスできます。すべてのユーザは、初めてログインするときに、ユーザ EXEC モード（レベル 0 または 1 のコマンド）にアクセスします。ユーザは、特権 EXEC モード（レベル 2 以上のコマンド）にアクセスするために再び **enable** コマンドで認証するか、**login** コマンドでログイン（ローカル データベースに限る）できます。

（注） ローカル コマンド認可は、ローカル データベース内にユーザがなくても、CLI または enable 認証がなくても使用できます。代わりに、**enable** コマンドを入力するときにシステム イネーブル パスワードを入力すると、ASA によってレベル 15 に置かれます。次に、すべてのレベルのイネーブル パスワードを作成します。これにより、**enable** *n*（2 ～ 15）を入力したときに、ASA によってレベル *n* に置かれるようになります。これらのレベルは、ローカル コマンド認可をオンにしない限り使用されません（詳細については、**enable** コマンドを参照してください）。

- TACACS+ サーバ特権レベル：TACACS+ サーバで、ユーザまたはグループが CLI アクセスについて認証した後で使用できるコマンドを設定します。CLI でユーザが入力するすべてのコマンドは、TACACS+ サーバでチェックされます。

セキュリティ コンテキストとコマンド許可

マルチ セキュリティ コンテキストでコマンド許可を実装する場合の重要な考慮点を次に示します。

- AAA 設定はコンテキストごとに個別であり、コンテキスト間で共有されません。

  コマンド許可を設定する場合は、各セキュリティ コンテキストを別々に設定する必要があります。これにより、異なるセキュリティ コンテキストに対して異なるコマンド認可を実行できます。

  セキュリティ コンテキストを切り替える場合、管理者は、ログイン時に指定したユーザ名で許可されるコマンドが新しいコンテキスト セッションでは異なる可能性があることや、新しいコンテキストではコマンド許可がまったく設定されていない可能性があることを念頭に置いてください。コマンド許可がセキュリティ コンテキストによって異なる場合があることを管理者が理解していないと、混乱が生じる可能性があります。この動作は、次の仕組みによってさらに複雑になります。

- **changeto** コマンドによって開始された新しいコンテキスト セッションでは、前のコンテキスト セッションで使用されたユーザ名に関係なく、管理者 ID として常にデフォルトの「enable_15」ユーザ名が使用されます。これにより、enable_15 ユーザに対してコマンド許可が設定されていない場合や、enable_15 ユーザの認可が前のコンテキスト セッションでのユーザの認可と異なる場合に、混乱が生じる可能性があります。

これは、発行される各コマンドを特定の管理者に正確に関連付けることができる場合に限り有効となる、コマンド アカウンティングにも影響します。**changeto** コマンドの使用が許可されているすべての管理者は enable_15 ユーザ名を他のコンテキストで使用できるため、enable_15 ユーザ名でログインしたユーザをコマンド アカウンティング レコードで簡単に特定できるとは限りません。コンテキストごとに異なるアカウンティング サーバを使用する場合は、enable_15 ユーザ名を使用していたユーザを追跡するために数台のサーバのデータを相関させる必要が生じます。

コマンド許可を設定する場合は、次の点を考慮します。

- **changeto** コマンドの使用が許可されている管理者は、実質的に、他のコンテキストそれぞれで enable_15 ユーザに許可されているすべてのコマンドを使用する許可を持ちます。
- コンテキストごとに別々にコマンドを認可する場合は、**changeto** コマンドの使用を許可されている管理者に対して拒否されるコマンドについて、enable_15 ユーザ名でも同様に使用を拒否されることを、各コンテキストで確認してください。

セキュリティ コンテキストを切り替える場合、管理者は特権 EXEC モードを終了し、再度 **enable** コマンドを入力して必要なユーザ名を使用できます。

(注) システム実行スペースでは **aaa** コマンドはサポートされません。したがって、システム実行スペースではコマンド認可は使用できません。

ローカル コマンド認可の前提条件

- **aaa authentication enable console** コマンドを使用して、ローカル、RADIUS、または LDAP 認証の enable 認証を設定します。

  enable 認証は、ユーザが **enable** コマンドにアクセスした後にユーザ名を維持するために必要です。

  または、コンフィギュレーションが不要な **login** コマンド（認証を伴う **enable** コマンドと同じ）を使用できます。enable 認証ほどセキュアではないため、このオプションは推奨しません。

  CLI 認証（**aaa authentication {ssh | telnet | serial} console**）を使用することもできますが、必須ではありません。

- RADIUS が認証に使用されている場合、**aaa authorization exec** コマンドを使用して、RADIUS からの管理ユーザ特権レベルのサポートをイネーブルにすることができますが、必須ではありません。このコマンドは、ローカル、RADIUS、LDAP（マッピング済み）、および TACACS+ の各ユーザの管理認可もイネーブルにします。
- 次に示すユーザ タイプごとの前提条件を確認してください。
  - ローカル データベース ユーザ：**username** コマンドを使用して、ローカル データベース内のユーザを特権レベル 0 ～ 15 で設定します。
  - RADIUS ユーザ：ユーザの Cisco VSA CVPN3000-Privilege-Level を、0 ～ 15 の値で設定します。
  - LDAP ユーザ：ユーザを特権レベル 0 ～ 15 を使用して設定し、**ldap map-attributes** コマンドを使用して LDAP 属性を Cisco VAS CVPN3000-Privilege-Level にマッピングします。
- コマンド特権レベルの設定については、**privilege** コマンドを参照してください。

TACACS+ コマンド認可

TACACS+ コマンド許可をイネーブルにし、ユーザが CLI でコマンドを入力すると、ASA はそのコマンドとユーザ名を TACACS+ サーバに送信し、コマンドが認可されているかどうかを判別します。

TACACS+ サーバによるコマンド認可を設定するときは、意図したとおりに機能することが確認できるまで、コンフィギュレーションを保存しないでください。間違いによりロック アウトされた場合、通常は ASA を再起動することによってアクセスを回復できます。

TACACS+ システムが完全に安定して信頼できることを確認します。必要な信頼性レベルについて、通常は、完全冗長 TACACS+ サーバ システムと ASA への完全冗長接続が必要です。たとえば、TACACS+ サーバ プールに、インターフェイス 1 に接続された 1 つのサーバとインターフェイス 2 に接続された別のサーバを含めます。TACACS+ サーバが使用できない場合にフォールバック方式としてローカル コマンド許可を設定することもできます。この場合、ローカル ユーザおよびコマンド特権レベルを設定する必要があります。

TACACS+ サーバの設定については、CLI 設定ガイドを参照してください。

TACACS+ コマンド認可の前提条件

- **aaa authentication {ssh | telnet | serial} console** コマンドを使用して、CLI 認証を設定します。
- **aaa authentication enable console** コマンドを使用して、**enable** 認証を設定します。

例

次に、tplus1 という名前の TACACS+ サーバ グループを使用してコマンド認可をイネーブルにする例を示します。

```
ciscoasa(config)# aaa authorization command tplus1
```

次に、tplus1 サーバ グループ内のすべてのサーバが使用できない場合に、ローカル ユーザ データベースへのフォールバックをサポートする管理認可を設定する例を示します。

```
ciscoasa(config)# aaa authorization command tplus1 LOCAL
```

関連コマンド

コマンド	説明
aaa authentication console	CLI、ASDM、および enable 認証をイネーブルにします。
aaa authorization exec	RADIUS からの管理ユーザ特権レベルのサポートをイネーブルにします。
aaa-server host	ホスト関連の属性を設定します。
aaa-server	グループ関連のサーバ属性を設定します。
enable	特権 EXEC モードを開始します。
ldap map-attributes	LDAP 属性を、ASA で使用できる RADIUS 属性にマッピングします。
login	ローカル データベースを認証に使用して特権 EXEC モードを開始します。
service-type	ローカル データベース ユーザの CLI、ASDM、およびイネーブル アクセスを制限します。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa authorization exec

管理認可をイネーブルにするには、グローバル コンフィギュレーション モードで **aaa authorization exec** コマンドを使用します。管理認可をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authorization exec {**authentication-server** | **LOCAL**} [**auto-enable**]

no aaa authorization exec {**authentication-server** | **LOCAL**} [**auto-enable**]

構文の説明

authentication-server	ユーザの認証に使用されたサーバから認可属性が取得されることを指定します。
auto-enable	十分な認可特権を持つ管理者が認証クレデンシャルを一度入力すると、特権 EXEC モードを開始できるようにします。
LOCAL	認証方法に関係なく、認可属性が ASA のローカル ユーザ データベースから取得されることを示します。

デフォルト

デフォルトでは、このコマンドはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.2(2)	**LOCAL** オプションが追加されました。
9.2(1)	**auto-enable** オプションが追加されました。
9.4(1)	この CLI は HTTP 以外の管理セッションにだけ適用されます。

使用上のガイドライン

aaa authorization exec コマンドを使用すると、ユーザの service-type クレデンシャルはコンソール アクセスの許可の前に検査されます。

no aaa authorization exec コマンドによる管理認可をディセーブルにする場合、次の点に注意してください。

- コンソール アクセスの許可の前に、ユーザの service-type クレデンシャルはチェックされません。
- コマンド認可が設定されている場合、RADIUS、LDAP、および TACACS+ ユーザについて AAA サーバで特権レベル属性が見つかると、特権レベル属性が引き続き適用されます。

ユーザが CLI、ASDM、または **enable** コマンドにアクセスするときにユーザを認証するように **aaa authentication console** コマンドを設定すると、ユーザ コンフィギュレーションに応じて **aaa authorization exec** コマンドで管理アクセスを制限できます。

(注) シリアルアクセスは管理認可に含まれていないため、**aaa authentication serial console** を設定すると、認証を行うすべてのユーザがコンソールポートにアクセスできます。コマンド認可を設定した場合、コンソールユーザにはコマンドの使用について引き続き制限が適用されます。

ユーザを管理認証対象に設定するには、次の各 AAA サーバ タイプまたはローカル ユーザの要件を参照してください。

- LDAP マッピング済みユーザ：LDAP 属性をマッピングするには、**ldap attribute-map** コマンドを参照してください。
- RADIUS ユーザ：次の値のいずれかにマッピングする IETF RADIUS numeric **service-type** 属性を使用します。
  - Service-Type 5（発信）は、管理アクセスを拒否します。ユーザは **aaa authentication console** コマンドで指定されたサービスを使用できません（**serial** キーワードを除きます。シリアル アクセスは許可されます）。リモート アクセス（IPsec および SSL）ユーザは、引き続き自身のリモート アクセス セッションを認証および終了できます。
  - Service-Type 6（管理）は、**aaa authentication console** コマンドで指定されたサービスへのフル アクセスを許可します。
  - Service-Type 7（NAS プロンプト）は、**aaa authentication {telnet | ssh} console** コマンドを設定した場合は CLI へのアクセスを許可しますが、**aaa authentication http console** コマンドを設定した場合は ASDM コンフィギュレーション アクセスを拒否します。ASDM モニタリング アクセスは許可します。**aaa authentication enable console** コマンドでイネーブル認証を設定している場合、ユーザは **enable** コマンドを使用して特権 EXEC モードにアクセスできません。

(注) 認識される service-type は、ログイン（1）、フレーム化（2）、管理（6）、および NAS プロンプト（7）のみです。その他の service-type を使用すると、アクセスは拒否されます。

- TACACS+ ユーザ:「service=shell」エントリで認可を要求し、サーバは次のように PASS または FAIL で応答します。
  - PASS、特権レベル 1 は、**aaa authentication console** コマンドで指定されたサービスへのフル アクセスを許可します。
  - PASS、特権レベル 2 以上は、**aaa authentication {telnet | ssh} console** コマンドを設定した場合は CLI へのアクセスを許可しますが、**aaa authentication http console** コマンドを設定した場合は ASDM コンフィギュレーション アクセスを拒否します。ASDM モニタリング アクセスは許可します。**aaa authentication enable console** コマンドでイネーブル認証を設定している場合、ユーザは **enable** コマンドを使用して特権 EXEC モードにアクセスできません。
  - FAIL は、管理アクセスを拒否します。ユーザは **aaa authentication console** コマンドで指定されたサービスを使用できません(**serial** キーワードを除きます。シリアル アクセスは許可されます)。
- ローカル ユーザ:**service-type** コマンドを設定します。これは、**username** コマンドのユーザ名コンフィギュレーション モードです。デフォルトの **service-type** は **admin** で、**aaa authentication console** コマンドで指定されたサービスへのフル アクセスを許可します。

例

次に、ローカル データベースを使用して管理認可をイネーブルにする例を示します。

```
ciscoasa(config)# aaa authorization exec LOCAL
```

関連コマンド

コマンド	説明
aaa authentication console	コンソール認証をイネーブルにします。
ldap attribute-map	LDAP 属性をマッピングします。
service-type	ローカル ユーザの制限 CLI アクセス。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa authorization http

ASDM の認可をイネーブルにするには、**aaa authorization http** コマンドを使用します。ASDM のユーザ名の認可をディセーブルにするには、このコマンドの no 形式を使用します。

aaa authorization http console LOCAL | <aaa-server-group>

[no] aaa authorization http console LOCAL | <aaa-server-group>

構文の説明

aaa-server-group	aaa サーバ　グループに対してすでに定義され、設定されたプロトコルは、LDAP、RADIUS、または TACACS+ である必要があります。プロトコルが LDAP、RADIUS、または TACACS+ でない場合は、コマンドに効力はありません。
console	管理認可用のサーバ グループを識別するには、このキーワードを指定します。
LOCAL	AAA プロトコル「local」に事前に定義されたサーバ タグです。

デフォルト

ASDM のユーザ名認証はデフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、webvpn（ASA 1000v）をサポートしないプラットフォームや、No Payload Encryption（NPE）がイネーブルになっているプラットフォームでは使用できません。

例

```
5520-1(config)# aaa ?

configure mode commands/options:
  accounting      Configure user accounting parameters
  authentication  Configure user authentication parameters
  authorization   Configure user authorization parameters
  local           AAA Local method options
  mac-exempt      Configure MAC Exempt parameters
```

```
  proxy-limit     Configure number of concurrent proxy connections allowed per
                  user
5520-1(config)# aaa authorization ?

configure mode commands/options:
  command  Specify this keyword to allow command authorization to be configured
           for all administrators on all consoles
  exclude  Exclude the service, local and foreign network which needs to be
           authenticated, authorized, and accounted
  exec     Perform administrative authorization for console connections(ssh,
           telnet and enable) configured for authentication to RADIUS,
           LDAP, TACACS or LOCAL authentication servers.
  include  Include the service, local and foreign network which needs to be
           authenticated, authorized, and accounted
  match    Specify this keyword to configure an ACL to match
  http     Perform administrative authorization for http connections

5520-1(config)# aaa authorization http ?

configure mode commands/options:
  console  Specify this keyword to identify a server group for administrative
           authorization
5520-1(config)# aaa authorization http console ?

configure mode commands/options:
  LOCAL  Predefined server tag for AAA protocol 'local'
  WORD   Name of RADIUS,LDAP or TACACS+ aaa-server group for administrative
         authorization
```

aaa authorization include、exclude

ASA を介した接続の認可をイネーブルにするには、グローバル コンフィギュレーション モードで **aaa authorization include** コマンドを使用します。認可をディセーブルにするには、このコマンドの **no** 形式を使用します。認可からアドレスを除外するには、**aaa authorization exclude** コマンドを使用します。認可からアドレスを除外しないようにするには、このコマンドの **no** 形式を使用します。

aaa authorization {include | exclude} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

no aaa authorization {include | exclude} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

構文の説明

exclude	サービスおよびアドレスが **include** コマンドによってすでに指定されている場合に、指定したサービスおよびアドレスを認可から除外します。
include	認可が必要なサービスおよび IP アドレスを指定します。**include** ステートメントで指定されないトラフィックは処理されません。
inside_ip	セキュリティの高い側のインターフェイスの IP アドレスを指定します。このアドレスは、このコマンドを適用するインターフェイスによって、送信元アドレスまたは宛先アドレスであることがあります。セキュリティの低い側のインターフェイスにコマンドを適用する場合、このアドレスは宛先アドレスです。セキュリティの高い側のインターフェイスにコマンドを適用する場合、このアドレスは送信元アドレスです。すべてのホストを指定するには、0 を指定します。
inside_mask	内部 IP アドレスのネットワーク マスクを指定します。IP アドレスが 0 の場合は 0 を使用します。ホストには 255.255.255.255 を指定します。
interface_name	ユーザが認可を要求するインターフェイスの名前を指定します。
outside_ip	(任意)セキュリティの低い側のインターフェイスの IP アドレスを指定します。このアドレスは、このコマンドを適用するインターフェイスによって、送信元アドレスまたは宛先アドレスであることがあります。セキュリティの低い側のインターフェイスにコマンドを適用する場合、このアドレスは送信元アドレスです。セキュリティの高い側のインターフェイスにコマンドを適用する場合、このアドレスは宛先アドレスです。すべてのホストを指定するには、0 を指定します。
outside_mask	(任意)外部 IP アドレスのネットワーク マスクを指定します。IP アドレスが 0 の場合は 0 を使用します。ホストには 255.255.255.255 を指定します。

server_tag	**aaa-server** コマンドによって定義される AAA サーバ グループを指定します。
service	認可が必要なサービスを指定します。次のいずれかの値を指定できます。 • **any** または **tcp/0**（すべての TCP トラフィックを指定します） • **FTP** • **http** • **https** • **ssh** • **telnet** • **tcp/***port*[**-***port*] • **udp/***port*[**-***port*] • **icmp/***type* • *protocol*[**/***port*[**-***port*]] **（注）** ポート範囲を指定すると、予期できない結果が認可サーバで生じる可能性があります。ASA では、サーバがストリングを解析してポート範囲に変換できることを前提としており、ポート範囲をストリングとしてサーバに送信します。すべてのサーバがこのような変換を実行するとは限りません。また、ユーザに対して特定のサービスだけを認可する場合もありますが、範囲が受け入れられると、このような認可は行われません。

デフォルト

IP アドレス **0** は、「すべてのホスト」を意味します。ローカル IP アドレスを **0** に設定すると、認可されるホストを認可サーバによって決定できます。

認可のためのローカル データベースへのフォールバックはデフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	**exclude** パラメータを使用すると、ユーザは特定のホストに対して除外するポートを指定できます。

使用上のガイドライン

ACL で指定されているトラフィックの認可をイネーブルにするには、**aaa authorization match** コマンドを使用します。**match** コマンドは、**include** コマンドおよび **exclude** コマンドと同じコンフィギュレーションで使用できません。**include** コマンドおよび **exclude** コマンドの代わりに **match** コマンドを使用することを推奨します。**include** コマンドおよび **exclude** コマンドは ASDM によってサポートされていません。

セキュリティが同じインターフェイス間で **aaa authorization include** および **exclude** コマンドを使用することはできません。その場合は、**aaa authorization match** コマンドを使用する必要があります。

TACACS+ でネットワーク アクセス認可を実行するように、ASA を設定できます。認証ステートメントと認可ステートメントは互いに独立しています。ただし、認証されていないトラフィックは、認可ステートメントに一致した場合でも拒否されます。ユーザが認可を受けるには、まず ASA に認証される必要があります。認証セッションが期限切れになっていない場合、所定の IP アドレスを持つユーザが認証を受ける必要があるのは、すべてのルールおよびタイプで 1 回だけです。このため、トラフィックが認証ステートメントに一致した場合でも認可が発生する可能性があります。

ユーザの認証が完了すると、ASA は、一致するトラフィックの認可ルールをチェックします。トラフィックが認可ステートメントに一致した場合、ASA はユーザ名を TACACS+ サーバに送信します。TACACS+ サーバは ASA に応答し、ユーザ プロファイルに基づいてそのトラフィックの許可または拒否を示します。ASA は、その応答内の認可ルールを実施します。

ユーザに対するネットワーク アクセス認可の設定については、ご使用の TACACS+ サーバのマニュアルを参照してください。

IP アドレスごとに 1 つの **aaa authorization include** コマンドが許可されます。

最初の認可試行が失敗し、2 番めの試行でタイムアウトが発生した場合は、認可されなかったクライアントを **service resetinbound** コマンドを使用してリセットし、そのクライアントが接続の再送信を行わないようにします。次の例は、Telnet の認可タイムアウト メッセージです。

```
Unable to connect to remote host: Connection timed out
```

（注） ポート範囲を指定すると、予期できない結果が認可サーバで生じる可能性があります。ASA では、サーバがストリングを解析してポート範囲に変換できることを前提としており、ポート範囲をストリングとしてサーバに送信します。すべてのサーバがこのような変換を実行するとは限りません。また、ユーザに対して特定のサービスだけを認可する場合もありますが、範囲が受け入れられると、このような認可は行われません。

例

次に、TACACS+ プロトコルを使用する例を示します。

```
ciscoasa(config)# aaa-server tplus1 protocol tacacs+
ciscoasa(config)# aaa-server tplus1 (inside) host 10.1.1.10 thekey timeout 20
ciscoasa(config)# aaa authentication include any inside 0 0 0 0 tplus1
ciscoasa(config)# aaa authorization include any inside 0 0 0 0
ciscoasa(config)# aaa accounting include any inside 0 0 0 0 tplus1
ciscoasa(config)# aaa authentication ssh console tplus1
```

この例では、最初のコマンド ステートメントで tplus1 という名前のサーバ グループを作成し、このグループで使用する TACACS+ プロトコルを指定しています。2 番めのコマンドでは、IP アドレス 10.1.1.10 の認証サーバが内部インターフェイス上にあること、および tplus1 サーバ グループに含まれていることを指定しています。次の 3 つのコマンド ステートメントで指定しているのは、外部インターフェイス経由で外部ホストへの接続を開始するすべてのユーザを tplus1 サーバ グループを使用して認証すること、正常に認証されたユーザに対してはすべてのサービスの使用を認可すること、およびすべての発信接続情報をアカウンティング データベースに記録することです。最後のコマンド ステートメントでは、ASA のコンソールへの SSH アクセスには、tplus1 サーバ グループからの認証が必要であることを指定しています。

次に、外部インターフェイスからの DNS ルックアップに対する認可をイネーブルにする例を示します。

```
ciscoasa(config)# aaa authorization include udp/53 outside 0.0.0.0 0.0.0.0
```

次に、内部ホストから内部インターフェイスに到着する ICMP echo-reply パケットの認可をイネーブルにする例を示します。

```
ciscoasa(config)# aaa authorization include 1/0 inside 0.0.0.0 0.0.0.0
```

これは、ユーザが Telnet、HTTP、または FTP を使用して認証されていない場合は外部ホストを ping できないことを意味します。

次に、内部ホストから inside インターフェイスに到着する ICMP エコー（ping）についてのみ認可をイネーブルにする例を示します。

```
ciscoasa(config)# aaa authorization include 1/8 inside 0.0.0.0 0.0.0.0
```

関連コマンド

コマンド	説明
aaa authorization command	コマンドの実行が認可の対象かどうかを指定します。または、指定したサーバ グループ内のすべてのサーバがディセーブルである場合に、ローカル ユーザ データベースへのフォールバックをサポートするように管理認可を設定します。
aaa authorization match	特定の access-list コマンド名に対して LOCAL または TACACS+ ユーザ認可サービスをイネーブルまたはディセーブルにします。
clear configure aaa	設定した AAA アカウンティングの値を削除またはリセットします。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa authorization match

ASA を通じた接続の許可をイネーブルにするには、グローバル コンフィギュレーション モードで **aaa authorization match** マンドを使用します。認可をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authorization match *acl_name interface_name server_tag*

no aaa authorization match *acl_name interface_name server_tag*

構文の説明

acl_name	拡張 ACL 名を指定します。**access-list extended** コマンドを参照してください。**許可** ACE は、一致したトラフィックを認可するようにマークします。一方、**拒否**エントリは、一致したトラフィックを認可から除外します。
interface_name	ユーザが認証を要求するインターフェイスの名前を指定します。
server_tag	**aaa-server** コマンドで定義した AAA サーバ グループ タグを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

aaa authorization match コマンドは、**include** コマンドおよび **exclude** コマンドと同じコンフィギュレーションでは使用できません。**include** コマンドおよび **exclude** コマンドの代わりに **match** コマンドを使用することを推奨します。**include** コマンドおよび **exclude** コマンドは ASDM によってサポートされていません。

TACACS+ でネットワーク アクセス認可を実行するように、ASA を設定できます。**aaa authorization match** コマンドによる RADIUS 認可では、ASA への VPN 管理接続の認可のみがサポートされます。

認証ステートメントと認可ステートメントは互いに独立しています。ただし、認証されていないトラフィックは、認可ステートメントに一致した場合でも拒否されます。ユーザが認可を受けるには、まず ASA に認証される必要があります。認証セッションが期限切れになっていない場合、所定の IP アドレスを持つユーザが認証を受ける必要があるのは、すべてのルールおよびタイプで 1 回だけです。このため、トラフィックが認証ステートメントに一致した場合でも認可が発生する可能性があります。

ユーザの認証が完了すると、ASA は、一致するトラフィックの認可ルールをチェックします。トラフィックが認可ステートメントに一致した場合、ASA はユーザ名を TACACS+ サーバに送信します。TACACS+ サーバは ASA に応答し、ユーザ プロファイルに基づいてそのトラフィックの許可または拒否を示します。ASA は、その応答内の認可ルールを実施します。

ユーザに対するネットワーク アクセス認可の設定については、ご使用の TACACS+ サーバのマニュアルを参照してください。

最初の認可試行が失敗し、2 番めの試行でタイムアウトが発生した場合は、認可されなかったクライアントを **service resetinbound** コマンドを使用してリセットし、そのクライアントが接続の再送信を行わないようにします。次の例は、Telnet の認可タイムアウト メッセージです。

```
Unable to connect to remote host: Connection timed out
```

(注) ポート範囲を指定すると、予期できない結果が認可サーバで生じる可能性があります。ASA では、サーバがストリングを解析してポート範囲に変換できることを前提としており、ポート範囲をストリングとしてサーバに送信します。すべてのサーバがこのような変換を実行するとは限りません。また、ユーザに対して特定のサービスだけを認可する場合もありますが、範囲が受け入れられると、このような認可は行われません。

例

次に、**aaa** コマンドで tplus1 サーバ グループを使用する例を示します。

```
ciscoasa(config)# aaa-server tplus1 protocol tacacs+
ciscoasa(config)# aaa-server tplus1 (inside) host 10.1.1.10 thekey timeout 20
ciscoasa(config)# aaa authentication include any inside 0 0 0 0 tplus1
ciscoasa(config)# aaa accounting include any inside 0 0 0 0 tplus1
ciscoasa(config)# aaa authorization match myacl inside tplus1
```

この例では、最初のコマンド ステートメントで tplus1 サーバ グループを TACACS+ グループとして定義しています。2 番めのコマンドでは、IP アドレス 10.1.1.10 の認証サーバが内部インターフェイス上にあること、および tplus1 サーバ グループに含まれていることを指定しています。次の 2 つのコマンド ステートメントでは、内部インターフェイスを通過する、任意の外部ホストへの接続が tplus1 サーバ グループを使用して認証され、これらのすべての接続がアカウンティング データベースに記録されることを指定しています。最後のコマンド ステートメントでは、myacl 内の ACE に一致する接続が tplus1 サーバ グループ内の AAA サーバによって認可されることを指定しています。

関連コマンド

コマンド	説明
aaa authorization	ユーザ許可をイネーブルまたはディセーブルにします。
clear configure aaa	すべての AAA コンフィギュレーションのパラメータをデフォルト値にリセットします。
clear uauth	ある特定のユーザまたはすべてのユーザの AAA 許可および認証キャッシュを削除します。次回接続を作成するときには再認証の必要が生じます。

コマンド	説明
show running-config aaa	AAA コンフィギュレーションを表示します。
show uauth	認証および許可の目的で許可サーバに提供されているユーザ名、ユーザ名がバインドされている IP アドレス、およびユーザが認証されただけであるか、キャッシュされたサービスを持っているかを表示します。

aaa kerberos import-keytab

Kerberos キータブファイルをインポートして、Kerberos サーバの認証に使用できるようにするには、グローバル コンフィギュレーション モードで **aaa kerberos import-keytab** コマンドを使用します。インポートされたキータブファイルを削除するには、**clear aaa kerberos keytab** コマンドを使用します。

aaa kerberos import-keytab *file*

構文の説明

url	インポートするファイルのロケーションまたは URL。ファイルをインポートするためにサポートされているロケーションは次のとおりです。ロケーションに応じた完全なパスとファイル名を指定します。 • disk0: • disk1: • flash: • ftp:// • http:// • https:// • scp:// • smb:// • tftp://

デフォルト

デフォルト値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.8(4)	このコマンドが追加されました。

使用上のガイドライン

validate-kdc コマンドを使用して、グループ内のサーバを認証するように Kerberos AAA サーバグループを設定できます。認証を実行するには、Kerberos キー発行局（KDC）からエクスポートしたキータブファイルもインポートする必要があります。KDC を検証することにより、攻撃者が KDC をスプーフィングして、ユーザクレデンシャルが攻撃者の Kerberos サーバに対して認証されるようにする攻撃を防ぐことができます。

KDC の検証を有効にすると、チケット認可チケット（TGT）を取得してユーザを検証した後、システムは **ホスト/***ASA_hostname* のユーザに代わってサービスチケットも要求します。次にシステムは、返されたサービスチケットを KDC の秘密鍵に対して検証します。これは、KDC から生成され、ASA にアップロードされたキータブファイルに保存されます。KDC 認証に失敗すると、サーバは信頼できないと見なされ、ユーザは認証されません。

KDC 認証を完了するには、次の手順を実行する必要があります。

1. （KDC 上。）ASA の Microsoft Active Directory でユーザアカウントを作成します（[Start] > [Programs] > [Administrative Tools] > [Active Directory Users and Computers] に移動します）。たとえば、ASA の完全修飾ドメイン名（FQDN）が asahost.example.com の場合は、asahost という名前のユーザを作成します。
2. （KDC 上。）FQDN とユーザアカウントを使用して、ASA のホストサービスプリンシパル名（SPN）を作成します。

   ```
   C:> setspn -A HOST/asahost.example.com asahost
   ```

3. （KDC 上。）ASA の キータブファイルを作成します（わかりやすくするために改行を追加）。

   ```
   C:\Users\Administrator> ktpass /out new.keytab +rndPass
   /princ host/asahost@EXAMPLE.COM
   /mapuser asahost@example.com
   /ptype KRB5_NT_SRV_HST
   /mapop set
   ```

4. （ASA 上。）**aaa kerberos import-keytab** コマンドを使用して、キータブ（この例では new.keytab）を ASA にインポートします。
5. （ASA 上。）Kerberos AAA サーバグループ設定に **validate-kdc** コマンドを追加します。キータブファイルは、このコマンドが含まれているサーバグループでのみ使用されます。

（注） Kerberos 制約付き委任（KCD）とともに KDC 検証を使用することはできません。サーバグループが KCD に使用されている場合、**validate-kdc** コマンドは無視されます。

例

次に、FTP サーバ上に存在する new.keytab というキータブをインポートし、Kerberos AAA サーバグループで KDC 検証を有効にする例を示します。

```
ciscoasa(config)# aaa kerberos import-keytab ftp://ftpserver.example.com/new.keytab
ftp://ftpserver.example.com/new.keytab imported successfully
ciscoasa(config)# aaa-server svrgrp1 protocol kerberos
ciscoasa(config-aaa-server-group)# validate-kdc
```

関連コマンド

コマンド	説明
clear aaa kerberos keytab	インポートされた Kerberos キータブファイルをクリアします。
show aaa kerberos keytab	Kerberos キータブファイルに関する情報を表示します。
validate-kdc	Kerberos キー発行局（KDC）検証を実行するように Kerberos AAA サーバグループを設定します。

aaa local authentication attempts max-fail

ASA で特定のユーザ アカウントに対して許可されるローカル ログイン試行の連続失敗回数を制限するには(特権レベル 15 のユーザを除きます。この機能はレベル 15 のユーザには影響しません)、グローバル コンフィギュレーション モードで **aaa local authentication attempts max-fail** コマンドを使用します。この機能をディセーブルにし、ローカル ログイン試行の連続失敗回数を無制限に許可するには、このコマンドの **no** 形式を使用します。

aaa local authentication attempts max-fail *number*

構文の説明

number	ユーザがロック アウトされるまでに間違ったパスワードを入力できる最大回数。この数の範囲は、1 ～ 16 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、ローカル ユーザ データベースによる認証だけに影響します。このコマンドを省略すると、ユーザが間違ったパスワードを入力できる回数に制限は設けられません。

間違ったパスワードを入力した試行回数が設定回数に達すると、ユーザはロック アウトされ、管理者がユーザ名をアンロックするまで、ユーザは正常にログインできません。ユーザ名のロックまたはアンロックにより、syslog メッセージが生成されます。

特権レベル 15 のユーザはこのコマンドの影響を受けず、ロック アウトされることはありません。

ユーザが正常に認証されるか、ASA がリブートされると、失敗試行回数は 0 にリセットされ、ロックアウト ステータスは No にリセットされます。

例

次に、**aaa local authentication attempts max-limits** コマンドを使用して、許可される失敗試行の最大回数を 2 に設定する例を示します。

```
ciscoasa(config)# aaa local authentication attempts max-limits 2
```

関連コマンド

コマンド	説明
clear aaa local user lockout	指定したユーザのロックアウト ステータスをクリアし、失敗試行カウンタを 0 に設定します。
clear aaa local user fail-attempts	ユーザのロックアウト ステータスを変更することなく、ユーザ認証試行の失敗回数をゼロにリセットします。
show aaa local user	現在ロックされているユーザ名のリストを表示します。

aaa mac-exempt

認証および認可から免除する MAC アドレスの定義済みリストの使用を指定するには、グローバル コンフィギュレーション モードで **aaa mac-exempt** コマンドを使用します。MAC アドレスのリストの使用をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa mac-exempt match *id*

no aaa mac-exempt match *id*

構文の説明

id	**mac-list** コマンドで設定した MAC リスト番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

追加できる **aaa mac-exempt** コマンドは 1 つだけです。**aaa mac-exempt** コマンドを使用する前に、**mac-list** コマンドを使用して MAC リスト番号を設定します。MAC リスト内の permit エントリによって MAC アドレスは認証および認可から免除され、deny エントリによって MAC アドレスの認証および認可が要求されます（認証および認可がイネーブルの場合）。追加できる **aaa mac-exempt** コマンドのインスタンスは 1 つだけであるため、免除するすべての MAC アドレスを MAC リストに含めてください。

例

次の例では、1 個の MAC アドレスに対する認証をバイパスします。

```
ciscoasa(config)# mac-list abc permit 00a0.c95d.0282 ffff.ffff.ffff
ciscoasa(config)# aaa mac-exempt match abc
```

次のエントリでは、ハードウェア ID が 0003.E3 であるすべての Cisco IP Phone について、認証をバイパスします。

```
ciscoasa(config)# mac-list acd permit 0003.E300.0000 FFFF.FF00.0000
ciscoasa(config)# aaa mac-exempt match acd
```

次に、00a0.c95d.02b2 を除く MAC アドレスのグループの認証をバイパスする例を示します。

```
ciscoasa(config)# mac-list 1 deny 00a0.c95d.0282 ffff.ffff.ffff
ciscoasa(config)# mac-list 1 permit 00a0.c95d.0000 ffff.ffff.0000
ciscoasa(config)# aaa mac-exempt match 1
```

関連コマンド

コマンド	説明
aaa authentication	ユーザ認証をイネーブルにします。
aaa authorization	ユーザ認可サービスをイネーブルにします。
aaa mac-exempt	MAC アドレスのリストを認証と認可の対象から免除します。
show running-config mac-list	**mac-list** コマンドで以前指定された MAC アドレスのリストを表示します。
mac-list	認証および認可から MAC アドレスを免除するために使用する MAC アドレスのリストを指定します。

aaa proxy-limit

特定の IP アドレスの同時認証試行数を制限するには、グローバル コンフィギュレーション モードで **aaa proxy-limit** コマンドを使用します。デフォルトのプロキシ制限値に戻すには、このコマンドの **no** 形式を使用します。

aaa proxy-limit *proxy_limit*

aaa proxy-limit disable

no aaa proxy-limit

構文の説明

disable	プロキシを許可しないことを指定します。
proxy_limit	ユーザごとに許可される同時プロキシ接続数(1 ～ 128)を指定します。

デフォルト

デフォルトのプロキシ制限値は 16 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

送信元アドレスがプロキシ サーバである場合は、この IP アドレスを認証から除外するか、許容される未処理 AAA 要求の数を増やすことを検討してください。

たとえば、ターミナル サーバに接続しているなどの理由で、同じ IP アドレスを使用する 2 人のユーザがブラウザまたは接続を開き、正確に同時に認証を開始しようとした場合、1 人のみが許可され、2 人目はブロックされます。

その IP アドレスからの最初のセッションは代行処理されて認証要求が送信され、もう 1 つのセッションはタイムアウトします。このことは、単一ユーザ名の接続数とは関係ありません。

例

次に、特定の IP アドレスについて未処理認証試行の最大数(同時)を設定する例を示します。

```
ciscoasa(config)# aaa proxy-limit 6
```

関連コマンド

コマンド	説明
aaa authentication	**aaa-server** コマンドで指定されたサーバ上で、LOCAL、TACACS+、または RADIUS ユーザ認証をイネーブルまたはディセーブルに設定したり、表示したりします。または ASDM ユーザ認証をイネーブルまたはディセーブルにしたり、表示したりします。
aaa authorization	LOCAL または TACACS+ ユーザ認可サービスをイネーブルまたはディセーブルにします。
aaa-server host	AAA サーバを指定します。
clear configure aaa	設定した AAA アカウンティングの値を削除またはリセットします。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa sdi import-node-secret

RSA Authentication Manager からエクスポートしたノードシークレットファイルを SDI AAA サーバグループで使用するためにインポートするには、グローバル コンフィギュレーション モードで **aaa sdi import-node-secret** コマンドを使用します。インポートしたノードシークレットファイルを削除するには、**clear aaa sdi node-secret** コマンドを使用します。

aaa sdi import-node-secret *filepath rsa_server_address password*

構文の説明

filepath	RSA Authentication Manager からエクスポートして解凍されたノードシークレットファイルへの完全なパス。ファイルをインポートするためにサポートされているロケーションは次のとおりです。ロケーションに応じた完全なパスとファイル名を指定します。 • disk0: • disk1: • flash: • ftp:// • http:// • https:// • scp:// • smb:// • tftp://
rsa_server_address	ノードシークレットが属する RSA Authentication Manager サーバの IP アドレスまたは完全修飾ホスト名。
password	エクスポート時にファイルを保護するために使用されるパスワード。

デフォルト

デフォルト値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.15(1)	このコマンドが追加されました。

使用上のガイドライン

RSA Authentication Manager（SecurID）サーバによって生成されたノードシークレットファイルを手動でインポートできます。

RSA Authentication Manager サーバからノードシークレットファイルをエクスポートする必要があります。詳細については、RSA Authentication Manager のドキュメントを参照してください。次に、解凍したファイルを ASA にアップロードするか、このコマンドを使用してインポートできるサーバに配置します。

例

次に、rsaam.example.com サーバの nodesecret.rec ファイルをインポートする例を示します。パスワードは mysecret です。

```
ciscoasa# aaa sdi import-node-secret nodesecret.rec rsaam.example.com mysecret
nodesecret.rec imported successfully
ciscoasa#
```

関連コマンド

コマンド	説明
clear aaa sdi node-secret	インポートされた SDI ノードシークレットファイルをクリアします。
show aaa sdi node-secrets	インポートされたノードシークレットファイルがある SecurID サーバに関する情報を表示します。

aaa-server

AAA サーバ グループを作成し、すべてのグループ ホストに対してグループ固有かつ共通の AAA サーバ パラメータを設定するには、グローバル コンフィギュレーション モードで **aaa-server** コマンドを使用します。指定したグループを削除するには、このコマンドの **no** 形式を使用します。

aaa-server *server-tag* **protocol** *server-protocol*

no aaa-server *server-tag* **protocol** *server-protocol*

構文の説明

protocol *server-protocol*	グループ内のサーバによってサポートされる AAA プロトコルを指定します。 • **http-form** • **kerberos** • **ldap** • **nt**（このオプションは、9.3(1) リリース以降は使用できないことに注意してください） • **radius** • **sdi**（認証およびサーバ管理プロトコル（ACE）を使用する RSA SecurID） • **tacacs+**
server-tag	サーバグループ名を指定します。**aaa-server host** コマンドで指定した名前と同じにします。他の AAA コマンドで、この AAA サーバグループ名を参照します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.1(1)	**http-form** プロトコルが追加されました。
8.2(2)	AAA サーバ グループの最大数が、シングル モードで 15 から 100 に増やされました。
8.4(2)	AAA サーバ グループ コンフィギュレーション モードで、**ad-agent-mode** オプションが追加されました。
9.3(1)	**nt** オプションが使用できなくなりました。Windows NT ドメイン認証のサポートが廃止されました。
9.13(1)	許可されるサーバ グループ数の制限は、シングル モードでは 100 から 200 に、マルチ モードでは 4 から 8 に増加しました。また、グループ内のサーバ数の制限は、マルチ モードで 4 から 8 に増加しました。シングル モードでのグループごとのサーバ数の制限は 16 であり、変更されていません。

使用上のガイドライン

シングル モードで最大 100 個のサーバ グループ、またはマルチ モードでコンテキストごとに 4 つのサーバ グループを持つことができます。9.13(1) 以降では、制限はシングルモードでは 200 グループ、マルチモードでは 8 グループに増加しています。

各グループには、シングル モードで最大 16 台、マルチ モードで最大 4 台のサーバを含めることができます。9.13(1) 以降では、マルチモードの制限はグループあたり 8 台のサーバです。ユーザがログインすると、コンフィギュレーション内で指定されている最初のサーバから順に、サーバが応答するまでこれらのサーバが 1 つずつアクセスされます。

aaa-server コマンドで AAA サーバ グループ プロトコルを定義することによって AAA サーバ コンフィギュレーションを制御し、次に **aaa-server host** コマンドを使用してサーバをグループに追加します。**aaa-server protocol** コマンドを入力する場合は、コンフィギュレーション モードを開始します。

RADIUS プロトコルを使用する場合、AAA サーバ グループ コンフィギュレーション モードでは、次のことに注意してください。

- クライアントレス SSL および AnyConnect セッションについてマルチセッション アカウンティングをイネーブルにするには、**interim-accounting-update** オプションを入力します。このオプションを選択すると、開始レコードと終了レコード以外に中間アカウンティング レコードが RADIUS サーバに送信されます。
- ASA と AD エージェントとの間の共有秘密を指定し、RADIUS サーバ グループにフル機能の RADIUS サーバではない AD エージェントを含めることを示すには、**ad-agent-mode** オプションを入力します。ユーザ アイデンティティに関連付けることができるのは、このオプションを使用して設定された RADIUS サーバ グループのみです。結果として、**ad-agent-mode** オプションを使用して設定されていない RADIUS サーバ グループを指定すると **test aaa-server** {**authentication** | **authorization**} *aaa-server-group* コマンドが使用できなくなります。

例

次に、**aaa-server** コマンドを使用して、TACACS+ サーバ グループ コンフィギュレーションの詳細を変更する例を示します。

```
ciscoasa(config)# aaa-server svrgrp1 protocol tacacs+
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
ciscoasa(config-aaa-server-group)# reactivation mode timed
ciscoasa(config-aaa-server-group)# max-failed attempts 2
```

関連コマンド

コマンド	説明
accounting-mode	アカウンティング メッセージが単一のサーバに送信されるか(シングル モード)、グループ内のすべてのサーバに送信されるか(同時モード)を指定します。
reactivation-mode	障害の発生したサーバを再度アクティブにする方式を指定します。
max-failed-attempts	サーバ グループ内の所定のサーバが非アクティブ化されるまでに、そのサーバで許容される接続試行の失敗数を指定します。
clear configure aaa-server	AAA サーバのコンフィギュレーションをすべて削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

aaa-server active、fail

障害とマークされた AAA サーバを再度アクティブにするには、特権 EXEC モードで **aaa-server active** コマンドを使用します。アクティブなサーバを障害状態にするには、特権 EXEC モードで **aaa-server fail** コマンドを使用します。

aaa-server *server_tag* [**active | fail**] **host** {*server_ip* | *name*}

構文の説明

active	サーバをアクティブ状態に設定します。
fail	サーバを障害状態に設定します。
ホスト	ホストの IP アドレス名または IP アドレスを指定します。
name	**name** コマンドを使用してローカルで割り当てた名前か、DNS 名を使用してサーバ名を指定します。DNS 名の最大文字数は 128 文字で、**name** コマンドを使用して割り当てた名前は 63 文字です。
server_ip	AAA サーバの IP アドレスを指定します。
server_tag	サーバ グループのシンボリック名を指定します。この名前は、**aaa-server** コマンドによって指定された名前と照合されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用しないと、グループ内の障害が発生したサーバは、グループ内のすべてのサーバに障害が発生するまで障害状態のままになります。グループ内のすべてのサーバに障害が発生した後に、サーバはすべて再度アクティブにされます。

例

次に、サーバ 192.168.125.60 の状態を表示し、手動で再度アクティブにする例を示します。

```
ciscoasa# show aaa-server group1 host 192.68.125.60
Server Group:  group1
Server Protocol: RADIUS
Server Address:  192.68.125.60
```

```
Server port:  1645
Server status: FAILED. Server disabled at 11:10:08 UTC  Fri Aug 22
...
ciscoasa# aaa-server active host 192.168.125.60
ciscoasa# show aaa-server group1 host 192.68.125.60
Server Group:  group1
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: ACTIVE (admin initiated). Last Transaction at 11:40:09 UTC  Fri Aug 22
...
```

関連コマンド

コマンド	説明
aaa-server	AAA サーバ グループを作成および変更します。
clear configure aaa-server	AAA サーバのコンフィギュレーションをすべて削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

aaa-server host

AAA サーバを AAA サーバ グループの一部として設定し、ホスト固有の AAA サーバ パラメータを設定するには、グローバル コンフィギュレーション モードで **aaa-server host** コマンドを使用します。ホスト コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

aaa-server *server-tag* [(*interface-name*)] **host** {*server-ip* | *name*} [*key*] [**timeout** *seconds*]

no aaa-server *server-tag* [(*interface-name*)] **host** {*server-ip* | *name*} [*key*] [**timeout** *seconds*]

構文の説明

(*interface-name*)	(任意)認証サーバが配置されているネットワーク インターフェイスを指定します。このパラメータにはカッコが必要です。インターフェイスを指定しない場合、デフォルトは **inside** です(使用可能な場合)。
key	(任意)127 文字までの大文字と小文字が区別される英数字のキーワードを指定します。RADIUS サーバまたは TACACS+ サーバ上のキーと同じ値です。127 文字を超えて入力された文字があれば無視されます。このキーは ASA とサーバ間でデータを暗号化するために使われ、ASA とサーバの両方のシステムで同じである必要があります。キーにスペースは使用できませんが、その他の特殊文字は使用できます。ホスト モードで **key** コマンドを使用して、キーを追加または変更できます。
name	**name** コマンドを使用してローカルで割り当てた名前か、DNS 名を使用してサーバ名を指定します。DNS 名の最大文字数は 128 文字で、**name** コマンドを使用して割り当てた名前は 63 文字です。
server-ip	AAA サーバの IP アドレスを指定します。
server-tag	サーバ グループのシンボリック名を指定します。この名前は、**aaa-server** コマンドによって指定された名前と照合されます。
timeout *seconds*	(任意)要求のタイムアウト間隔。この時間を超えると、ASA はプライマリ AAA サーバへの要求を断念します。スタンバイ AAA サーバが存在する場合、ASA は要求をそのバックアップ サーバに送信します。ホスト コンフィギュレーション モードで **timeout** コマンドを使用して、タイムアウト間隔を変更できます。

デフォルト

デフォルトのタイムアウト値は 10 秒です。

デフォルトのインターフェイスは、inside です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	DNS 名のサポートが追加されました。
9.0(1)	ユーザ アイデンティティのサポートが追加されました。
9.9(2)	Radius サーバの IPv6 アドレッシングおよび Radius サーバへの接続のサポートが追加されました。
9.13(1)	許可されるサーバ グループ数の制限は、シングル モードでは 100 から 200 に、マルチ モードでは 4 から 8 に増加しました。また、グループ内のサーバ数の制限は、マルチ モードで 4 から 8 に増加しました。シングル モードでのグループごとのサーバ数の制限は 16 であり、変更されていません。

使用上のガイドライン

aaa-server コマンドで AAA サーバ グループを定義することによって AAA サーバ コンフィギュレーションを制御し、次に **aaa-server host** コマンドを使用してサーバをグループに追加します。**aaa-server host** コマンドを使用すると、AAA サーバ ホスト コンフィギュレーション モードが開始されます。このモードから、ホスト固有の AAA サーバ接続データを指定および管理できます。

各グループには、シングル モードで最大 16 台、マルチ モードで最大 4 台のサーバを含めることができます。9.13(1) 以降では、マルチモードの制限はグループあたり 8 台のサーバです。ユーザがログインすると、コンフィギュレーション内で指定されている最初のサーバから順に、サーバが応答するまでこれらのサーバが 1 つずつアクセスされます。

例

次に、「watchdogs」という名前の Kerberos AAA サーバ グループを設定し、そのグループに AAA サーバを追加し、そのサーバの Kerberos レルムを定義する例を示します。

(注) Kerberos 領域名では数字と大文字だけを使用します。ASA は領域名に小文字を受け入れますが、小文字を大文字に変換しません。大文字だけを使用してください。

```
ciscoasa(config)# aaa-server watchdogs protocol kerberos
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server watchdogs host 192.168.3.4
ciscoasa(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
```

次に、「svrgrp1」という名前の SDI AAA サーバ グループを設定し、そのグループに AAA サーバを追加し、タイムアウト間隔を 6 秒に、再試行間隔を 7 秒に、SDI バージョンをバージョン 5 に設定する例を示します。

```
ciscoasa(config)# aaa-server svrgrp1 protocol sdi
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server svrgrp1 host 192.168.3.4
ciscoasa(config-aaa-server-host)# timeout 6
ciscoasa(config-aaa-server-host)# retry-interval 7
ciscoasa(config-aaa-server-host)# sdi-version sdi-5
```

次の例では、LDAP 検索に **aaa-server** *aaa_server_group_tag* コマンドを使用する際に、検索パスをターゲット グループに絞り込む方法を示しています。

```
ciscoasa(config)# aaa-server CISCO_AD_SERVER protocol ldap
ciscoasa(config)# aaa-server CISCO_AD_SERVER host 10.1.1.1
ciscoasa(config-aaa-server-host)# server-port 636
ciscoasa(config-aaa-server-host)# ldap-base-dn DC=cisco,DC=com
ciscoasa(config-aaa-server-host)# ldap-group-base-dn OU=Cisco Groups,DC=cisco,DC=com
ciscoasa(config-aaa-server-host)# ldap-scope subtree
```

```
ciscoasa(config-aaa-server-host)# ldap-login-password *
ciscoasa(config-aaa-server-host)# ldap-login-dn CISCO\username1
ciscoasa(config-aaa-server-host)# ldap-over-ssl enable
ciscoasa(config-aaa-server-host)# server-type microsoft
```

(注) **ldap-group-base-dn** コマンドが指定されている場合、すべてのグループが LDAP ディレクトリ階層内のこのレベルの下に存在する必要があり、このパスの外部にグループが存在することはできません。

ldap-group-base-dn コマンドは、アクティブな user-identity ベースのポリシーが少なくとも 1 つ存在する場合にのみ有効です。

server-type microsoft コマンドはデフォルトではありませんが、設定する必要があります。

最初の **aaa-server** *aaa_server_group_tag* **host** コマンドは、LDAP 操作に使用されます。

関連コマンド

コマンド	説明
aaa-server	AAA サーバ グループを作成および変更します。
clear configure aaa-server	AAA サーバのコンフィギュレーションをすべて削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

absolute

時間範囲が有効である場合に絶対時間を定義するには、時間範囲コンフィギュレーション モードで **absolute** コマンドを使用します。時間範囲に時間を指定しない場合は、このコマンドの **no** 形式を使用します。

absolute [**end** *time date*] [**start** *time date*]

no absolute

構文の説明

date	（オプション）日付を day month year 形式で指定します（たとえば、1 January 2006）。年の有効な範囲は、1993 ～ 2035 です。
end	（任意）時間範囲の終了日時を指定します。
start	（任意）時間範囲の開始日時を指定します。
time	（任意）時刻を HH:MM 形式で指定します。たとえば、午前 8 時は 8:00、午後 8 時は 20:00 とします。

デフォルト

開始時刻および日付を指定しない場合、permit ステートメントまたは deny ステートメントはただちに有効になり、常にオンです。同様に、最大終了時刻は 23:59 31 December 2035 です。終了時刻および日付を指定しない場合、関連付けられている permit ステートメントまたは deny ステートメントは無期限に有効です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
時間範囲コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

時間ベース ACL を実装するには、**time-range** コマンドを使用して、週および 1 日の中の特定の時刻を定義します。次に、**access-list extended time-range** コマンドを使用して、時間範囲を ACL にバインドします。

例

次に、ACL を 2006 年 1 月 1 日の午前 8 時にアクティブにする例を示します。

```
ciscoasa(config-time-range)# absolute start 8:00 1 January 2006

Because no end time and date are specified, the associated ACL is in effect indefinitely.
```

関連コマンド

コマンド	説明
access-list extended	ASA 経由の IP トラフィックを許可または拒否するためのポリシーを設定します。
default	**time-range** コマンドの **absolute** キーワードと **periodic** キーワードをデフォルト設定に戻します。
periodic	時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定します。
time-range	時間に基づいて ASA のアクセス コントロールを定義します。

accept-subordinates

デバイスにインストールされていない下位 CA 証明書がフェーズ 1 の IKE 交換で提供されたときに、その証明書を受け入れるように ASA を設定するには、クリプト CA トラストポイント コンフィギュレーション モードで **accept-subordinates** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

accept-subordinates

no accept-subordinates

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルト設定はオンです（下位証明書は受け入れられます）。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

フェーズ 1 の処理中に、IKE ピアによって下位証明書とアイデンティティ証明書の両方が渡される場合があります。下位証明書は ASA にインストールされない場合があります。このコマンドを使用すると、管理者はデバイス上にトラストポイントとして設定されていない下位 CA 証明書をサポートできます。確立されたすべてのトラストポイントのすべての下位 CA 証明書が受け入れ可能である必要はありません。つまり、このコマンドを使用すると、デバイスで、証明書チェーン全体をローカルにインストールすることなく、その証明書チェーンを認証できます。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、ASA でトラストポイント central の下位証明書を受け入れることができるようにする例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# accept-subordinates
ciscoasa(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。

access-group

拡張 ACL または EtherType ACL を 1 つのインターフェイスにバインドするには、グローバル コンフィギュレーション モードで **access-group** コマンドを使用します。ACL をインターフェイスからアンバインドするには、このコマンドの **no** 形式を使用します。

access-group *access_list* {**in** | **out**} **interface** *interface_name* [**per-user-override** | **control-plane**]

no access-group *access_list* {**in** | **out**} **interface** *interface_name*

1 組のグローバル拡張ルールを 1 つのコマンドですべてのインターフェイスに適用するには、グローバル コンフィギュレーション モードで **access-group global** コマンドを使用します。設定済みのすべてのインターフェイスからグローバル ルールを削除するには、このコマンドの **no** 形式を使用します。

access-group *access_list* [**global**]

no access-group *access_list* [**global**]

構文の説明

access_list	拡張 ACL の名前。ブリッジ グループ メンバー インターフェイスの場合は、Ethertype ACL を指定することもできます。
control-plane	（オプション）ACL が to-the-box トラフィック用であるかどうかを指定します。たとえば、このオプションを使用し、ISAKMP をブロックすることによって、特定のリモート IP アドレスが ASA への VPN セッションを開始できないようにすることができます。to-the-box 管理トラフィック用のアクセス ルール（**http**、**ssh**、**telnet** などのコマンドで定義）は、**control-plane** オプションで適用される ACL よりも優先されます。したがって、このような許可された管理トラフィックは、to-the-box ACL で明示的に拒否されている場合でも着信が許可されます。このオプションは、**in** 方向にのみ使用可能です。
global	すべてのインターフェイスのすべてのトラフィックに ACL を適用します。
in	指定されたインターフェイスでインバウンド方向に ACL を適用します。
interface *interface_name*	ネットワーク インターフェイスの名前。 ルーテッド モードでは、ブリッジ仮想インターフェイス（BVI）とそのメンバー インターフェイスの両方に拡張 ACL を適用できます。トランスペアレント モードでは、メンバー インターフェイスにのみ拡張 ACL を適用できます。両方のモードでは、メンバー インターフェイスにのみ Ethertype ACL を適用できます。
out	指定されたインターフェイスでアウトバウンド方向に ACL を適用します。
per-user-override	（オプション）ダウンロード可能なユーザ ACL によって、インターフェイスに適用されている ACL を上書きできます。このオプションは、**in** 方向にのみ使用可能です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.3(1)	このコマンドは、グローバル ポリシーをサポートするように変更されました。
9.7(1)	このコマンドは、ルーテッド モードで、BVI に拡張アクセス グループを適用し、ブリッジ グループ メンバー インターフェイスに Ethertype ACL を適用できるように変更されました。

使用上のガイドライン

インターフェイス固有のアクセス グループ ルールがグローバル ルールに優先されるため、パケットの分類時はインターフェイス固有のルールがグローバル ルールの前に処理されます。

ルーテッド モードでは、BVI とそのメンバー インターフェイスの両方にアクセス グループを適用した場合、優先順位は方向によって異なります。インバウンドでは、メンバー インターフェイスのアクセス グループが最初にチェックされ、次に BVI アクセス グループ、最後にグローバル グループがチェックされます。アウトバウンドでは、BVI アクセス グループが最初にチェックされ、次にメンバー インターフェイスのアクセス グループがチェックされます。

インターフェイス固有ルールの使用上のガイドライン

access-group コマンドは、インターフェイスに拡張 ACL をバインドします。ACL を作成するには、最初に **access-list extended** コマンドを使用する必要があります。

インターフェイスに対して着信または発信するトラフィックに ACL を適用できます。**access-list** コマンド ステートメントで **permit** オプションを入力すると、ASA によってパケットの処理は続行されます。**access-list** コマンド ステートメントで **deny** オプションを入力すると、ASA によってパケットが廃棄され、syslog message 106023（または、デフォルト以外のロギングを使用する ACE の場合には 106100）が生成されます。

インバウンド ACL の場合、**per-user-override** オプションを使用すると、ダウンロードされた ACL によって、インターフェイスに適用されている ACL を上書きできます。**per-user-override** オプションを指定しないと、ASA は既存のフィルタリング動作を維持します。**per-user-override** を指定すると、ASA により、ユーザに関連付けられているユーザごとのアクセス リスト（ダウンロードされた場合）の **permit** または **deny** ステータスで、**access-group** コマンドに関連付けられている ACL の permit または deny ステータスを上書きできるようになります。さらに、次のルールが適用されます。

- パケットが到着した時点で、そのパケットに関連付けられているユーザごとの ACL がない場合、インターフェイス ACL が適用されます。
- ユーザごとの ACL は、**timeout** コマンドの **uauth** オプションで指定されたタイムアウト値によって管理されますが、このタイムアウト値は、ユーザごとの AAA セッション タイムアウト値によって上書きできます。
- 既存の ACL ログ動作は同じです。たとえば、ユーザごとの ACL が原因でユーザ トラフィックが拒否された場合、syslog メッセージ 109025 が記録されます。ユーザ トラフィックが許可された場合、syslog メッセージは生成されません。ユーザごとのアクセス リストのログ オプションは、影響を及ぼしません。

デフォルトでは、VPN リモート アクセス トラフィックはインターフェイス ACL と照合されません。ただし、**no sysopt connection permit-vpn** コマンドを使用してこのバイパスをオフにする場合、動作は、グループ ポリシーに適用される **vpn-filter** があるかどうか、および **per-user-override** オプションを設定するかどうかによって異なります。

- **per-user-override** なし、**vpn-filter** なし: トラフィックはインターフェイス ACL と照合されます。
- **per-user-override** なし、**vpn-filter**: トラフィックはまずインターフェイス ACL と照合され、次に VPN フィルタと照合されます。
- **per-user-override**、**vpn-filter**: トラフィックは VPN フィルタのみと照合されます。

(注) 1 つ以上の **access-group** コマンドによって参照される ACL から、すべての機能エントリ(permit ステートメントおよび deny ステートメント)を削除すると、**access-group** コマンドはコンフィギュレーションから自動的に削除されます。**access-group** コマンドは、空の ACL またはコメントのみを含む ACL を参照できません。

グローバル ルールの使用上のガイドライン

access-group global コマンドは、ASA でトラフィックが到着するインターフェイスにかかわらず、すべてのトラフィックに対して 1 組のグローバル ルールを適用します。

すべてのグローバル ルールは、入力(着信)方向のトラフィックにのみ適用されます。グローバル ルールは出力(発信)トラフィックには適用されません。グローバル ルールが着信インターフェイス アクセス ルールと組み合わせて設定された場合、インターフェイス アクセス ルール(特定のルール)がグローバル アクセス ルール(一般のルール)よりも前に処理されます。

例

次に、**access-group global** コマンドを使用して、設定済みのすべてのインターフェイスに ACL を適用する例を示します。

```
ciscoasa(config)# access-list acl-1 extended permit ip host 10.1.2.2 host 10.2.2.2
ciscoasa(config)# access-list acl-2 extended deny ip any any

ciscoasa(config)# access-group acl-1 in interface outside
ciscoasa(config)# access-group acl-2 global
```

上記のルールでは、出力インターフェイスで 10.1.2.2 から 10.2.2.2 にトラフィックを通過させ、10.1.1.10 から 10.2.2.20 へのトラフィックはグローバル拒否ルールによりドロップします。この access-group コンフィギュレーションによって、分類テーブルに次のルールが追加されます(**show asp table classify** コマンドからの出力)。

```
in  id=0xb1f90068, priority=13, domain=permit, deny=false
        hits=0, user_data=0xaece1ac0, cs_id=0x0, flags=0x0, protocol=0
        src ip=10.1.2.2, mask=255.255.255.255, port=0
        dst ip=10.2.2.2, mask=255.255.255.255, port=0, dscp=0x0
```

```
        input_ifc=outside, output_ifc=any
in  id=0xb1f2a250, priority=12, domain=permit, deny=true
        hits=0, user_data=0xaece1b40, cs_id=0x0, flags=0x0, protocol=0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=any, output_ifc=any
in  id=0xb1f90100, priority=11, domain=permit, deny=true
        hits=0, user_data=0x5, cs_id=0x0, flags=0x0, protocol=0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=outside, output_ifc=any
in  id=0xb1f2a3f8, priority=11, domain=permit, deny=true
        hits=0, user_data=0x5, cs_id=0x0, flags=0x0, protocol=0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
        input_ifc=any, output_ifc=any
```

次に、任意のアドレスから DMZ 内の HTTP サーバ（IP アドレス 10.2.2.2）へのグローバル アクセスを許可する例を示します。

```
ciscoasa(config)# access-list global_acl permit tcp any host 10.2.2.2 eq 80
ciscoasa(config)# access-group global_acl global
```

上記のルールは、外部ホスト 10.1.2.2 からホスト 10.2.2.2 への HTTP 接続を許可し、内部ホスト 192.168.0.0 からホスト 10.2.2.2 への HTTP 接続を許可します。

次に、グローバル ポリシーとインターフェイス ポリシーを一緒に使用する方法の例を示します。この例では、任意の内部ホストからサーバ（IP アドレス 10.2.2.2）へのアクセスは許可しますが、他のホストからサーバへのアクセスを拒否します。インターフェイス ポリシーが優先されます。

```
ciscoasa(config)# access-list inside_acl permit tcp any host 10.2.2.2 eq 23
ciscoasa(config)# access-list global_acl deny ip any host 10.2.2.2
ciscoasa(config)# access-group inside_acl in interface inside
ciscoasa(config)# access-group global_acl global
```

上記のルールは、外部ホスト 10.1.2.2 からホスト 10.2.2.2 への SSH 接続を拒否し、内部ホスト 192.168.0.0 からホスト 10.2.2.2 への SSH 接続を許可します。

次に、NAT とグローバル アクセス コントロール ポリシーを一緒に機能させる方法の例を示します。この例では、外部ホスト 10.1.2.2 からホスト 10.2.2.2 への 1 つの HTTP 接続を許可し、内部ホスト 192.168.0.0 からホスト 10.2.2.2 への別の HTTP 接続を許可し、外部ホスト 10.255.255.255 からホスト 172.31.255.255 への 1 つの HTTP 接続を（暗黙ルールによって）拒否します。

```
ciscoasa(config)# object network dmz-server host 10.1.1.2
ciscoasa(config)# nat (any, any) static 10.2.2.2
ciscoasa(config)# access-list global_acl permit tcp any host 10.2.2.2 eq 80
ciscoasa(config)# access-group global_acl global
```

次に、NAT とグローバル アクセス コントロール ポリシーを一緒に機能させる方法の例を示します。この例では、ホスト 10.1.1.1 からホスト 192.168.0.0, への 1 つの HTTP 接続を許可し、ホスト 209.165.200.225 からホスト 172.16.0.0 への別の HTTP 接続を許可し、ホスト 10.1.1.1 からホスト 172.16.0.0 への 1 つの HTTP 接続を拒否します。

```
ciscoasa(config)# object network 10.1.1.1 host 10.1.1.1
ciscoasa(config)# object network 172.16.0.0 host 172.16.0.0
ciscoasa(config)# object network 192.168.0.0 host 192.168.0.0
ciscoasa(config)# nat (inside, any) source static 10.1.1.1 10.1.1.1 destination static
                  192.168.0.0 172.16.0.0
ciscoasa(config)# access-list global_acl permit ip object 10.1.1.1 object 172.16.0.0
ciscoasa(config)# access-list global_acl permit ip host 209.165.200.225 object 172.16.0.0
ciscoasa(config)# access-list global_acl deny ip any 172.16.0.0
ciscoasa(config)# access-group global_acl global
```

関連コマンド

コマンド	説明
access-list extended	拡張 ACL を作成します。
clear configure access-group	すべてのインターフェイスからアクセス グループを削除します。
show running-config access-group	インターフェイスにバインドされている現在の ACL を表示します。

access-list alert-interval

拒否フローの最大数メッセージの時間間隔を指定するには、グローバル コンフィギュレーション モードで **access-list alert-interval** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

access-list alert-interval *secs*

no access-list alert-interval

構文の説明

secs	拒否フローの最大数メッセージの生成の時間間隔。有効な値は、1 ～ 3600 秒です。デフォルト値は 300 秒です。

デフォルト

デフォルトは 300 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ACL deny ステートメントに **log** オプションを設定している場合、トラフィック フローが ACL ステートメントと一致すると、アプライアンスによってフロー情報がキャッシュされます。キャッシュの過負荷を避けるために、syslog メッセージ 106100 で示される統計情報のために保持されるキャッシュ拒否フローの最大数が設定されています。106100 が発行されてキャッシュがリセットされる前に最大数に達した場合は、拒否フローの最大数を超過したことを示す syslog メッセージ 106101 が発行されます。

access-list alert-interval コマンドは、syslog メッセージ 106101 を生成する時間間隔を設定します。拒否フローの最大数に達した場合、最後の syslog メッセージ 106101 が生成されてから *secs* 秒以上が経過すると、別の syslog メッセージ 106101 が生成されます。

拒否フローの最大数メッセージの生成については、**access-list deny-flow-max** コマンドを参照してください。

例

次に、拒否フローの最大数メッセージの時間間隔を指定する例を示します。

```
ciscoasa(config)# access-list alert-interval 30
```

関連コマンド

コマンド	説明
access-list deny-flow-max	作成できる同時拒否フローの最大数を指定します。
access-list extended	ACL をコンフィギュレーションに追加し、ASA を通過する IP トラフィックのポリシーを設定するために使用します。
clear access-group	ACL カウンタをクリアします。
clear configure access-list	実行コンフィギュレーションから ACL をクリアします。
show access-list	ACL エントリを番号で表示します。

access-list deny-flow-max

メッセージ 106100 の統計情報を計算するためにキャッシュできる同時拒否フローの最大数を指定するには、グローバル コンフィギュレーション モードで **access-list deny-flow-max** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

access-list deny-flow-max *number*

no access-list deny-flow-max *number*

構文の説明

number	syslog メッセージ 106100 の統計情報を計算するためにキャッシュする拒否フローの最大数。値は 1 ～ 4096 です。デフォルトは 4096 です。

デフォルト

デフォルトは 4096 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASA でキャッシュ拒否フローの最大数に達すると、syslog メッセージ 106101 が生成されます。

例

次に、キャッシュできる同時拒否フローの最大数を指定する例を示します。

```
ciscoasa(config)# access-list deny-flow-max 256
```

関連コマンド

コマンド	説明
access-list alert-interval	メッセージ 106101 を発行する間隔を設定します。
access-list extended	ACL をコンフィギュレーションに追加し、ASA を通過する IP トラフィックのポリシーを設定するために使用します。
clear access-group	ACL カウンタをクリアします。
clear configure access-list	実行コンフィギュレーションから ACL をクリアします。
show access-list	ACL エントリを番号で表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

access-list ethertype

EtherType に基づいてトラフィックを制御する ACL を設定するには、グローバル コンフィギュレーション モードで **access-list ethertype** コマンドを使用します。ACL を削除するには、このコマンドの **no** 形式を使用します。

access-list *id* **ethertype** {**deny** | **permit**} {**any** | **bpdu** | **dsap** {*hex_address* | **bpdu** | **ipx** | **isis** | **raw-ipx**} | **eii-ipx** | **ipx** | **isis** | **mpls-unicast** | **mpls-multicast** | *hex_number*}

no access-list *id* **ethertype** {**deny** | **permit**} {**any** | **bpdu** | **dsap** {*hex_address* | **bpdu** | **ipx** | **isis** | **raw-ipx**} | **eii-ipx** | **ipx** | **isis** | **mpls-unicast** | **mpls-multicast** | *hex_number*}

構文の説明

任意	すべてのトラフィックを許可または拒否します。
bpdu	ブリッジ プロトコル データ ユニットを許可または拒否します。 9.6(2) 以降では、このキーワードを使用しても意図した結果を得られません。代わりに、**dsap 0x42** 用のルールを書き込みます。 必要なサポートが含まれる 9.9(1) および 9.6 以降のメンテナンス リリースでは、**bpdu** および **dsap 0x42** は **dsap bpdu** ルールに変換されます。
deny	トラフィックを拒否します。
dsap {*hex_address* | **bpdu** | **ipx** | **isis** | **raw-ipx**}	IEEE 802.2 論理リンク制御パケットの宛先サービス アクセス ポイントのアドレス。ユーザが許可または拒否するアドレスを 16 進数（0x01 ～ 0xff）で含めます。 よく使用される値には、以下のキーワードも使用できます。 • **bpdu**：0x42（ブリッジ プロトコル データ ユニット）の場合。 • **ipx**：0xe0（Internet Packet Exchange（IPX）802.2 LLC）の場合。 • **isis**：0xfe（Intermediate System to Intermediate System（IS-IS））の場合。 • **raw-ipx**：0xff（Raw IPX 802.3 形式）の場合。
hex_number	0x600 以上の 16 ビットの 16 進数値として指定された特定の EtherType を含むトラフィックを許可または拒否します。
id	ACL の名前または番号を指定します。
eii-ipx	イーサネット II IPX 形式、EtherType 0x8137 を許可または拒否します。
ipx	IPX を許可または拒否します。 必要なサポートが含まれる 9.9(1) および 9.6 以降のメンテナンス リリースでは、**ipx** は、**dsap ipx**、**dsap raw-ipx**、および **eii-ipx** に対して 3 つの異なるルールを設定するためのショートカットです。
isis	Intermediate System to Intermediate System（IS-IS）を許可または拒否します。 必要なサポートが含まれる 9.9(1) および 9.6 以降のメンテナンス リリースでは、**isis** は **dsap isis** ルールに変換されます。
mpls-multicast	MPLS マルチキャストを許可または拒否します。
mpls-unicast	MPLS ユニキャストを許可または拒否します。
permit	トラフィックを許可します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(5)、9.1(2)	**isis** キーワードが追加されました。
9.6(2)	**dsap** *hex_address* キーワードが追加されました。**bpdu** キーワードは意図したトラフィックを照合しなくなりました。代わりに **dsap 0x42** を使用してください。
9.7(1)	ルーテッド モードのブリッジ グループ メンバー インターフェイスに Ethertype ACL を設定できるようになりました。
9.9(1)	次の点が変更されました。 • **dsap** キーワードに、よく使用されるプロトコルのための次の キーワードが追加されました：**dsap {bpdu | ipx | isis | raw-ipx}**。 • **bpdu** キーワードは **dsap bpdu** キーワードに自動的に変換されます。 • **isis** キーワードは **dsap isis** キーワードに自動的に変換されます。 • **eii-ipx** キーワードが追加されました。 • **ipx** キーワードは、**dsap ipx**、**dsap raw-ipx**、および **eii-ipx** のための 3 つのルールに自動的に変換されます。

使用上のガイドライン

EtherType ACL は、EtherType を指定する 1 つまたは複数のアクセス コントロール エントリ（ACE）で構成されます。EtherType ルールは、16 ビットの 16 進数値で指定されるすべての EtherType および選択されたトラフィック タイプを制御します。

（注） EtherType ACL の場合、ACL の末尾にある暗黙的な拒否は、IP トラフィックや ARP には影響しません。たとえば、EtherType 8037 を許可する場合、ACL の末尾にある暗黙的な拒否によって、拡張 ACL で以前許可（または高位のセキュリティ インターフェイスから低位のセキュリティ インターフェイスへ暗黙的に許可）した IP トラフィックがブロックされることはありません。ただし、EtherType ACE のすべてのトラフィックを明示的に拒否する場合、IP と ARP のトラフィックは拒否され、オート ネゴシエーションなどの物理プロトコル トラフィックだけが引き続き許可されます。

サポートされている EtherType およびその他のトラフィック

EtherType ルールは次を制御します。

- 一般的なタイプの IPX および MPLS ユニキャストまたはマルチキャストを含む、16 ビットの 16 進数値で示された EtherType。
- イーサネット V2 フレーム。
- デフォルトで許可される BPDU。BPDU は、SNAP でカプセル化されており、ASA は特別に BPDU を処理するように設計されています。
- トランク ポート（シスコ専用）BPDU。トランク BPDU のペイロードには VLAN 情報が含まれるため、BPDU を許可すると、ASA により、発信 VLAN を使用してペイロードが修正されます。
- Intermediate System to Intermediate System（IS-IS）。
- IEEE 802.2 論理リンク制御パケット。宛先サービス アクセス ポイントのアドレスに基づいてアクセスを制御できます。

次のタイプのトラフィックはサポートされていません。

- 802.3 形式フレーム：type フィールドではなく length フィールドが使用されるため、ルールでは処理されません。

リターン トラフィックに対するアクセス ルール

EtherType はコネクションレス型であるため、トラフィックを両方向に通過させる場合は、着信インターフェイスと発信インターフェイスの両方にルールを適用する必要があります。

MPLS の許可

MPLS を許可する場合は、Label Distribution Protocol および Tag Distribution Protocol の TCP 接続が ASA を経由して確立されるようにしてください。これには、ASA インターフェイス上の IP アドレスを LDP セッションまたは TDP セッションの router-id として使用するように、ASA に接続されている両方の MPLS ルータを設定します（LDP および TDP を使用することにより、MPLS ルータは、転送するパケットに使用するラベル（アドレス）をネゴシエートできるようになります）。

Cisco IOS ルータで、使用プロトコル（LDP または TDP）に適したコマンドを入力します。interface は、ASA に接続されているインターフェイスです。

```
ciscoasa(config)# mpls ldp router-id interface force
```

または

```
ciscoasa(config)# tag-switching tdp router-id interface force
```

例

次に、EtherType ACL を追加する例を示します。

```
ciscoasa(config)# access-list ETHER ethertype permit ipx
ciscoasa(config)# access-list ETHER ethertype permit bpdu
ciscoasa(config)# access-list ETHER ethertype permit dsap 0x42
ciscoasa(config)# access-list ETHER ethertype permit mpls-unicast
ciscoasa(config)# access-group ETHER in interface inside
```

必要なサポートが含まれる 9.9(1) および 9.6 以降のメンテナンス リリースでは、上記の例は次のように実行されます。

```
ciscoasa(config)# access-list ETHER ethertype permit ipx
INFO: ethertype ipx is saved to config as ethertype eii-ipx
INFO: ethertype ipx is saved to config as ethertype dsap ipx
INFO: ethertype ipx is saved to config as ethertype dsap raw-ipx
```

```
ciscoasa(config)# access-list ETHER ethertype permit bpdu
INFO: ethertype bpdu is saved to config as ethertype dsap bpdu

ciscoasa(config)# access-list ETHER ethertype permit mpls-unicast

ciscoasa(config)# show access-list ETHER
access-list ETHER; 5 elements
access-list ETHER ethertype permit eii-ipx (hitcount=0)
access-list ETHER ethertype permit dsap ipx(hitcount=0)
access-list ETHER ethertype permit dsap raw-ipx(hitcount=0)
access-list ETHER ethertype permit dsap bpdu(hitcount=0)
access-list ETHER ethertype permit mpls-unicast (hitcount=0)

ciscoasa(config)# access-group ETHER in interface inside
```

関連コマンド

コマンド	説明
access-group	ACL をインターフェイスにバインドします。
clear access-group	ACL カウンタをクリアします。
clear configure access-list	実行コンフィギュレーションから ACL をクリアします。
show access-list	ACL エントリを番号で表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

access-list extended

拡張 ACL にアクセス コントロール エントリ（ACE）を追加するには、グローバル コンフィギュレーション モードで **access-list extended** コマンドを使用します。ACE を削除するには、このコマンドの **no** 形式を使用します。

すべてのタイプのトラフィック、ポートなし：

access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} *protocol_argument* [*user_argument*] [*security_group_argument*] *source_address_argument* [*security_group_argument*] *dest_address_argument* [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

no access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} *protocol_argument* [*user_argument*] [*security_group_argument*] *source_address_argument* [*security_group_argument*] *dest_address_argument* [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

ポートベースのトラフィックの場合：

access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} {**tcp** | **udp** | **sctp**} [*user_argument*] [*security_group_argument*] *source_address_argument* [*port_argument*] [*security_group_argument*] *dest_address_argument* [*port_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

no access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} {**tcp** | **udp** | **sctp**} [*user_argument*] [*security_group_argument*] *source_address_argument* [*port_argument*] [*security_group_argument*] *dest_address_argument* [*port_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

ICMP トラフィック、**ICMP** タイプ：

access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} {**icmp** | **icmp6**}[*user_argument*] [*security_group_argument*] *source_address_argument* [*security_group_argument*] *dest_address_argument* [*icmp_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

no access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} {**icmp** | **icmp6**} [*user_argument*] [*security_group_argument*] *source_address_argument* [*security_group_argument*] *dest_address_argument* [*icmp_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time-range** *time_range_name*] [**inactive**]

構文の説明

access_list_name	ACL ID を最大 241 文字の文字列または整数として指定します。ID は、大文字と小文字が区別されます。 ヒント　コンフィギュレーションで ACL ID を見やすくするには、すべて大文字を使用します。
deny	条件に合致している場合、パケットを拒否します。ネットワーク アクセスの場合（**access-group** コマンド）、このキーワードによって、パケットが ASA を通過しないようにします。クラス マップにアプリケーション インスペクションを適用する場合（**class-map** コマンドおよび **inspect** コマンド）、このキーワードによってトラフィックがインスペクションから免除されます。一部の機能では deny ACE の使用は許可されません。詳細については、ACL を使用する各機能のコマンド マニュアルを参照してください。
dest_address_argument	パケットの送信先の IP アドレスまたは FQDN を指定します。使用可能な引数は次のとおりです。 • **host** *ip_address*：IPv4 ホスト アドレスを指定します。 • *ip_address mask*：IPv4 ネットワーク アドレスおよびサブネット マスクを指定します。ネットワーク マスクを指定するときは、指定方法が Cisco IOS ソフトウェアの **access-list** コマンドとは異なることに注意してください。ASA では、ネットワーク マスク（たとえば、Class C マスクの 255.255.255.0）が使用されます。Cisco IOS マスクでは、ワイルドカード ビット（たとえば、0.0.0.255）が使用されます。 • *ipv6-address*/*prefix-length*：IPv6 ホストまたはネットワーク アドレスとプレフィックスを指定します。 • **any**、**any4**、および **any6**：**any** は IPv4 と IPv6 トラフィックの両方を指定します。**any4** は IPv4 トラフィックのみを指定し、**any6** は IPv6 トラフィックのみを指定します。 • **interface** *interface_name* - ASA インターフェイスの名前を指定します。IP アドレスではなくインターフェイス名を使用して、トラフィックの送信元または宛先のインターフェイスに基づいてトラフィックを照合します。トラフィックの送信元がデバイス インターフェイスである場合、ACL に実際の IP アドレスを指定する代わりに interface キーワードを指定する必要があります。たとえば、このオプションを使用し、ISAKMP をブロックすることによって、特定のリモート IP アドレスが ASA への VPN セッションを開始できないようにすることができます。ASA を送信元または宛先とするすべてのトラフィック自体では、**access-group** コマンドを **control-plane** キーワードを指定して使用することが必要となります。 • **object** *nw_obj_id*：**object network** コマンドを使用して作成されたネットワーク オブジェクトを指定します。 • **object-group** *nw_grp_id*：**object-group network** コマンドを使用して作成されたネットワーク オブジェクト グループを指定します。

icmp_argument	(オプション)ICMP のタイプとコードを指定します。 • *icmp_type* [*icmp_code*]:ICMP タイプを名前または番号で指定し、そのタイプの ICMP コード(省略可能)を指定します。コードを指定しない場合は、すべてのコードが使用されます。 • **object-group** *icmp_grp_id*:**object-group service** コマンドまたは(非推奨)**object-group icmp** コマンドを使用して作成された ICMP/ICMP6 用のネットワーク オブジェクト グループを指定します。
inactive	(任意)ACE をディセーブルにします。再度イネーブルにするには、**inactive** キーワードを使用せずに ACE 全体を入力します。この機能を使用すると、非アクティブな ACE のレコードをコンフィギュレーション内に保持して、再度イネーブルにしやすくすることができます。
line *line-num*	(任意)ACE を挿入する行番号を指定します。行番号を指定しなかった場合は、ACL の末尾に ACE が追加されます。行番号はコンフィギュレーションに保存されません。ACE の挿入場所を指定するだけです。
log [[*level*] [**interval** *secs*] | **disable** | **default**]	(オプション)ネットワーク アクセスに関して ACE に一致するパケットが見つかったとき(**access-group** コマンドで ACL が適用されます)のロギング オプションを設定します。引数を指定せずに **log** キーワードを入力すると、デフォルト レベル(6)とデフォルト間隔(300 秒)でシステム ログ メッセージ 106100 が有効になります。**log** キーワードを入力しないと、拒否されたパケットに対して、デフォルトのシステム ログ メッセージ 106023 が生成されます。ログ オプションは次のとおりです。 • *level*:0 ～ 7 の重大度。デフォルトは 6(情報)です。アクティブな ACE に対してこのレベルを変更する場合、新しいレベルは新規接続に適用され、既存の接続は引き続き前のレベルでロギングされます。 • **interval** *secs*:syslog メッセージ間の時間間隔(秒)。1 ～ 600 で指定します。デフォルトは 300 です。この値は、ドロップ統計情報の収集に使用するキャッシュから非アクティブなフローを削除するためのタイムアウト値としても使用されます。 • **disable**:すべての ACE ロギングをディセーブルにします。 • **default**:メッセージ 106023 のロギングをイネーブルにします。この設定は、**log** オプションを含めないことと同じです。
permit	条件に合致している場合、パケットを許可します。ネットワーク アクセスの場合(**access-group** コマンド)、このキーワードによって、パケットが ASA を通過するようにします。クラス マップにアプリケーション インスペクションを適用する場合(**class-map** コマンドおよび **inspect** コマンド)、このキーワードによってインスペクションがパケットに適用されます。

port_argument	(任意:**tcp**、**udp**、**sctp** のみ)送信元ポートまたは宛先ポートを指定します。ポートを指定しなかった場合は、すべてのポートが照合されます。また、この引数を使用するのではなく、*protocol_argument* に指定するサービス オブジェクトのポートも指定できます。 使用可能な引数は次のとおりです。 • *operator port*:ポートの名前または番号(0 ～ 65535)。サポートされる名前のリストについては、CLI ヘルプを参照してください。演算子は次のとおりです。 – **lt**:より小さい – **gt**:より大きい – **eq**:等しい – **neq**:等しくない – **range**:値の包括的な範囲。この演算子を使用するときは、ポート番号を 2 つ指定します。たとえば、次のように指定します。 `range 100 200` DNS、Discard、Echo、Ident、NTP、RPC、SUNRPC、および Talk は、それぞれに TCP の定義と UDP の定義の両方が必要です。TACACS+ では、ポート 49 に対して 1 つの TCP 定義が必要です。 • **object-group** *service_grp_id*:**object-group service** {**tcp** | **udp** | **tcp-udp**} コマンドを使用して作成されたサービス オブジェクト グループを指定します。これらのオブジェクト タイプは推奨されなくなりました。 ポート引数としてプロトコルおよびポートがオブジェクト内で定義されている場合は、推奨される一般的なサービス オブジェクトは指定できません。これらのオブジェクトはプロトコル引数の一部として指定します。
protocol_argument	IP プロトコルを指定します。使用可能な引数は次のとおりです。 • *name* または *number*:プロトコルの名前または番号を指定します。たとえば、UDP は 17、TCP は 6、EGP は 47 です。**ip** を指定すると、すべてのプロトコルに適用されます。使用可能なオプションについては、CLI ヘルプを参照してください。 • **object-group** *protocol_grp_id*:**object-group protocol** コマンドを使用して作成されたプロトコル オブジェクト グループを指定します。 • **object** *service_obj_id*:**object service** コマンドを使用して作成されたサービス オブジェクトを指定します。TCP、UDP、SCTP、または ICMP サービス オブジェクトには、トラフィックを ACE と照合する際に使用するプロトコル、送信元ポートと宛先ポートの両方またはいずれか、あるいは ICMP のタイプとコードを含めることができます。ACE でポートとタイプを個別に設定する必要はありません。 • **object-group** *service_grp_id*:**object-group service** コマンドを使用して作成されたサービス オブジェクト グループを指定します。
sctp	SCTP にプロトコルを設定します。

security_group_argument	TrustSec 機能とともに使用し、送信元や宛先のアドレスに加えて、トラフィックを検出する条件となるセキュリティ グループを指定します。使用可能な引数は次のとおりです。 • **object-group-security** *security_obj_grp_id*:**object-group security** コマンドを使用して作成されたセキュリティ オブジェクト グループを指定します。 • **security-group** {**name** *security_grp_id* | **tag** *security_grp_tag*}:セキュリティ グループの名前またはタグを指定します。
source_address_argument	パケットの送信元の IP アドレスまたは FQDN を指定します。使用可能な引数は、*dest_address_argument* の説明にある引数と同じです。
tcp	TCP にプロトコルを設定します。
time-range *time_range_name*	(オプション)ACE をアクティブにする曜日と時刻を決定する時間範囲オブジェクトを指定します。時間範囲を含めない場合、ACE は常にアクティブです。時間範囲の定義については、**time-range** コマンドを参照してください。
udp	UDP にプロトコルを設定します。
user_argument	アイデンティティ ファイアウォール機能とともに使用し、送信元アドレスに加えて、トラフィックを検出する条件となるグループまたはユーザを指定します。使用可能な引数は次のとおりです。 • **object-group-user** *user_obj_grp_id*:**object-group user** コマンドを使用して作成されたユーザ オブジェクト グループを指定します。 • **user** {[*domain_nickname*\]*name* | **any** | **none**}:ユーザ名を指定します。ユーザ クレデンシャルを含むすべてのユーザを照合するには **any** を指定し、ユーザ名にマッピングされていないアドレスを照合するには **none** を指定してください。これらのオプションが特に役立つのは、**access-group** と **aaa authentication match** のポリシーを結合する場合です。 • **user-group** [*domain_nickname*\\]*user_group_name*:ユーザ グループ名を指定します。\\ はドメインとグループ名の区切りです。

デフォルト

- deny ACE のデフォルトのロギングは、拒否されたパケットについてのみシステム ログ メッセージ 106023 を生成します。
- **log** キーワードが指定されている場合、システム ログ メッセージ 106100 のデフォルトの重大度は 6(情報)で、デフォルトの間隔は 300 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.3(1)	NAT または PAT を使用するときは、さまざまな機能で、ACL でのマッピング アドレスおよびポートの使用が不要になります。これらの機能については、必ず変換されていない実際のアドレスとポートを使用する必要があります。実際のアドレスとポートが使用されるので、NAT コンフィギュレーションが変更されても ACL を変更する必要はなくなります。詳細については、「実際の IP アドレスを使用する機能」セクション（1-91 ページ）を参照してください。
8.4(2)	送信元または宛先 IP アドレスに加えて、送信元と宛先に、アイデンティティ ファイアウォールのユーザおよびグループを使用できるようになりました。送信元と宛先に、**user**、**user-group**、および **object-group-user** のサポートが追加されました。
9.0(1)	送信元または宛先 IP アドレスに加えて、送信元と宛先に、TrustSec セキュリティ グループを使用できるようになりました。送信元または宛先に、**security-group** および **object-group-security** のサポートが追加されました。
9.0(1)	IPv6 のサポートが追加されました。any キーワードは、IPv4 および IPv6 トラフィックを表すように変更されました。IPv4 のみのトラフィックを表す any4 キーワードと、IPv6 のみのトラフィックを表す any6 キーワードが追加されました。送信元および宛先に対して IPv4 および IPv6 アドレスの組み合わせを指定できます。IPv4 と IPv6 間の変換に NAT を使用する場合、実際のパケットには、IPv4 アドレスと IPv6 アドレスの組み合わせは含まれません。ただし、多くの機能において、ACL では常に実際の IP アドレスが使用され、NAT マッピング アドレスは考慮されません。IPv6 固有の ACL は非推奨です。既存の IPv6 ACL は拡張 ACL に移行されます。移行の詳細については、リリース ノートを参照してください。ACL の移行については、9.0 のリリース ノートを参照してください。
9.0(1)	ICMP コードのサポートが追加されました。プロトコルとして **icmp** を指定すると、*icmp_type* [*icmp_code*] を入力できます。
9.5(2)	**sctp** キーワードが追加されました。

使用上のガイドライン

1 つの ACL は、同じ ACL ID を持つ 1 つまたは複数の ACE で構成されます。ACL は、ネットワーク アクセスを制御したり、さまざまな機能を適用するトラフィックを指定したりするために使用されます。特定の ACL 名に対して入力した各 ACE は、ACE で行番号を指定しない限り、その ACL の最後に追加されます。ACL 全体を削除するには、**clear configure access-list** コマンドを使用します。

ACE の順序

ACE の順序は重要です。ASA がパケットを転送するかドロップするかを決定する際、ASA は、エントリがリストされている順番で各 ACE を使用してパケットをテストします。一致が見つかると、ACE はそれ以上チェックされません。たとえば、すべてのトラフィックを明示的に許可する ACE を ACL の先頭に作成した場合は、残りのステートメントはチェックされません。

実際の IP アドレスを使用する機能

次のコマンドと機能では、実際の IP アドレスが ACL の中で使用されます。

- **access-group** コマンド
- モジュラ ポリシー フレームワークの **match access-list** コマンド
- ボットネット トラフィック フィルタの **dynamic-filter enable classify-list** コマンド
- AAA の **aaa ... match** コマンド
- WCCP の **wccp redirect-list group-list** コマンド

マッピング IP アドレスを使用する機能

次の機能は、ACL を使用しますが、これらの ACL は、インターフェイス上で認識されるマッピングされた値を使用します。

- IPsec ACL
- capture コマンドの ACL
- ユーザ単位 ACL
- ルーティング プロトコルの ACL
- 他のすべての機能の ACL

アイデンティティ ファイアウォール、FQDN、および TrustSec の ACL をサポートしない機能

次の機能は ACL を使用しますが、アイデンティティ ファイアウォール（ユーザ名またはグループ名を指定）、FQDN（完全修飾ドメイン名）、または TrustSec 値を含む ACL は使用できません。

- **route-map** コマンド
- VPN の crypto map コマンド
- VPN の group-policy コマンド、ただし、vpn-filter を除く
- WCCP
- DAP

例

次に示す ACL は ASA を通るすべてのホスト（ACL を適用するインターフェイス上の）を許可します。

```
ciscoasa(config)# access-list ACL_IN extended permit ip any any
```

次の ACL の例では、192.168.1.0/24 のホストが 209.165.201.0/27 のネットワークにアクセスすることを拒否します。その他のアドレスはすべて許可されます。

```
ciscoasa(config)# access-list ACL_IN extended deny tcp 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
ciscoasa(config)# access-list ACL_IN extended permit ip any any
```

一部のホストのみにアクセスを制限する場合は、制限された **permit ACE** を入力します。デフォルトでは、明示的に許可しない限り、他のトラフィックはすべて拒否されます。

```
ciscoasa(config)# access-list ACL_IN extended permit ip 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
```

次の ACL では、すべてのホスト（この ACL を適用するインターフェイス上の）からアドレス 209.165.201.29 の Web サイトへのアクセスを禁止しています。他のトラフィックはすべて許可されます。

```
ciscoasa(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
ciscoasa(config)# access-list ACL_IN extended permit ip any any
```

オブジェクト グループを使用する次の ACL では、内部ネットワーク上のさまざまなホストについて、さまざまな Web サーバへのアクセスを禁止しています。他のトラフィックはすべて許可されます。

```
ciscoasa(config-network)# access-list ACL_IN extended deny tcp object-group denied
object-group web eq www
ciscoasa(config)# access-list ACL_IN extended permit ip any any
ciscoasa(config)# access-group ACL_IN in interface inside
```

ネットワーク オブジェクトの 1 つのグループ（A）からネットワーク オブジェクトの別のグループ（B）へのトラフィックを許可する ACL を一時的にディセーブルにするには、次のコマンドを使用します。

```
ciscoasa(config)# access-list 104 permit ip host object-group A object-group B inactive
```

時間ベース ACL を実装するには、**time-range** コマンドを使用して、週および 1 日の中の特定の時刻を定義します。次に、**access-list extended** コマンドを使用して、時間範囲を ACL にバインドします。次に、ACL「Sales」を時間範囲「New_York_Minute」にバインドする例を示します。

```
ciscoasa(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host
209.165.201.1 time-range New_York_Minute
```

時間範囲の定義方法の詳細については、**time-range** コマンドを参照してください。

次の ACL は、すべての ICMP トラフィックを許可します。

```
ciscoasa(config)# access-list abc extended permit icmp any any
```

次の ACL は、オブジェクト グループ「obj_icmp_1」のすべての ICMP トラフィックを許可します。

```
ciscoasa(config)# access-list abc extended permit icmp any any object-group obj_icmp_1
```

次の ACL は、ICMP タイプが 3、および ICMP コードが 4 の送信元ホスト 10.0.0.0 から宛先ホスト 10.1.1.1 への ICMP トラフィックを許可します。その他のタイプの ICMP トラフィックはすべて許可されません。

```
ciscoasa(config)# access-list abc extended permit icmp host 10.0.0.0 host 10.1.1.1 3 4
```

次の ACL は、ICMP タイプが 3、および ICMP コードが任意の送信元ホスト 10.0.0.0 から宛先ホスト 10.1.1.1 への ICMP トラフィックを許可します。その他のタイプの ICMP トラフィックはすべて許可されません。

```
ciscoasa(config)# access-list abc extended permit icmp host 10.0.0.0 host 10.1.1.1 3
```

関連コマンド

コマンド	説明
access-group	ACL をインターフェイスにバインドします。
clear access-group	ACL カウンタをクリアします。
clear configure access-list	実行コンフィギュレーションから ACL をクリアします。

コマンド	説明
show access-list	ACE を番号別に表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

access-list remark

拡張、EtherType、または標準アクセス コントロール エントリの前後にコメントのテキストを指定するには、グローバル コンフィギュレーション モードで **access-list remark** コマンドを使用します。コメントを削除するには、このコマンドの **no** 形式を使用します。

access-list *id* [**line** *line-num*] **remark** *text*

no access-list *id* [**line** *line-num*] **remark** *text*

構文の説明

id	ACL の名前
line *line-num*	(任意)コメントを挿入するライン番号
remark text	コメントのテキスト。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

コメント テキストには、スペース以外の文字を少なくとも 1 つ含める必要があります。空のコメントは許可されません。コメント テキストは、スペースや句読点を含め、最大 100 文字です。

コメントのみを含む ACL では **access-group** コマンドは使用できません。

例

次に、ACL の末尾にコメント テキストを指定する例を示します。

```
ciscoasa(config)# access-list MY_ACL remark checklist
```

関連コマンド

コマンド	説明
access-list extended	ACL をコンフィギュレーションに追加し、ASA を通過する IP トラフィックのポリシーを設定するために使用します。
clear access-group	ACL カウンタをクリアします。
clear configure access-list	実行コンフィギュレーションから ACL をクリアします。
show access-list	ACL エントリを番号で表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

access-list rename

ACL の名前を変更するには、グローバル コンフィギュレーション モードで **access-list rename** コマンドを使用します。

access-list *id* **rename** *new_acl_id*

構文の説明

id	既存の ACL の名前。
rename *new_acl_id*	新しい ACL ID を最大 241 文字の文字列または整数として指定します。ID は、大文字と小文字が区別されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

ACL が同じ名前に変更されると、ASA は、通知なしでこのコマンドを無視します。

例

次に、ACL の名前を TEST から OUTSIDE に変更する例を示します。

```
ciscoasa(config)# access-list TEST rename OUTSIDE
```

関連コマンド

コマンド	説明
access-list extended	ACL をコンフィギュレーションに追加し、ASA を通過する IP トラフィックのポリシーを設定するために使用します。
clear access-group	ACL カウンタをクリアします。
clear configure access-list	実行コンフィギュレーションから ACL をクリアします。

コマンド	説明
show access-list	ACL エントリを番号で表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

access-list standard

標準 ACL にアクセス コントロール エントリ（ACE）を追加するには、グローバル コンフィギュレーション モードで **access-list standard** コマンドを使用します。ACE を削除するには、このコマンドの **no** 形式を使用します。

access-list *id* **standard** {**deny** | **permit**} {**any4** | **host** *ip_address* | *ip_address subnet_mask*}

no access-list *id* **standard** {**deny** | **permit**} {**any4** | **host** *ip_address* | *ip_address subnet_mask*}

構文の説明

any4	任意の IPv4 アドレスに一致させます。
deny	条件に一致する場合、パケットを拒否または免除します
host *ip_address*	IPv4 ホスト アドレスを指定します（つまり、サブネット マスクは 255.255.255.255 です）。
id	ACL の名前または番号。
ip_address subnet_mask	IPv4 ネットワーク アドレスおよびサブネット マスクを指定します。
permit	条件に一致する場合、パケットを許可するか、または含みます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

標準 ACL は、ACL ID または名前が同じすべての ACE で構成されます。標準 ACL は、ルート マップや VPN フィルタなどの限られた数の機能に使用されます。標準 ACL では、IPv4 アドレスのみを使用して、宛先アドレスのみを定義します。

例

次に、標準 ACL にルールを追加する例を示します。

```
ciscoasa(config)# access-list OSPF standard permit 192.168.1.0 255.255.255.0
```

関連コマンド

コマンド	説明
clear configure access-list	実行コンフィギュレーションから ACL をクリアします。
show access-list	ACL エントリを番号で表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

access-list webtype

クライアントレス SSL VPN 接続をフィルタする Web タイプ ACL にアクセス コントロール エントリ（ACE）を追加するには、グローバル コンフィギュレーション モードで **access-list webtype** コマンドを使用します。ACE を削除するには、このコマンドの **no** 形式を使用します。

access-list *id* **webtype** {**deny** | **permit**} **url** {*url_string* | **any**} [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time_range** *name*] [**inactive**]

no access-list *id* **webtype** {**deny** | **permit**} **url** {*url_string* | **any**} [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time_range** *name*] [**inactive**]

access-list *id* **webtype** {**deny** | **permit**} **tcp** *dest_address_argument* [*operator port*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time_range** *name*] [**inactive**]

no **access-list** *id* **webtype** {**deny** | **permit**} **tcp** *dest_address_argument* [*operator port*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**time_range** *name*] [**inactive**]

構文の説明

deny	条件に一致する場合、アクセスを拒否します。
dest_address_argument	パケットの送信先 IP アドレスを指定します。宛先アドレス オプションは次のとおりです。 • **host** *ip_address*：IPv4 ホスト アドレスを指定します。 • *dest_ip_address mask*：10.100.10.0 255.255.255.0 など、IPv4 ネットワーク アドレスおよびサブネット マスクを指定します。 • *ipv6-address*/*prefix-length*：IPv6 ホストまたはネットワーク アドレスとプレフィックスを指定します。 • **any**、**any4**、および **any6**：**any** は IPv4 と IPv6 トラフィックの両方を指定します。**any4** は IPv4 トラフィックのみを指定し、**any6** は IPv6 トラフィックのみを指定します。
id	ACL の名前または番号を指定します。
inactive	（任意）ACE をディセーブルにします。再度イネーブルにするには、**inactive** キーワードを使用せずに ACE 全体を入力します。この機能を使用すると、非アクティブな ACE のレコードをコンフィギュレーション内に保持して、再度イネーブルにしやすくすることができます。

log [[*level*] [**interval** *secs*] | **disable** | **default**]	(オプション)ACE に一致するパケットが見つかったときのロギング オプションを設定します。引数を指定せずに **log** キーワードを入力すると、デフォルト レベル(6)とデフォルト間隔(300 秒)で VPN フィルタのシステム ログ メッセージ 106102 がイネーブルになります。**log** キーワードを入力しないと、デフォルトの VPN フィルタのシステム ログ メッセージ 106103 が生成されます。ログ オプションは次のとおりです。 • *level*:0 ～ 7 の重大度。デフォルトは 6(情報)です。 • **interval** *secs*:syslog メッセージ間の時間間隔(秒)。1 ～ 600 で指定します。デフォルトは 300 です。この値は、ドロップ統計情報の収集に使用するキャッシュから非アクティブなフローを削除するためのタイムアウト値としても使用されます。 • **disable**:すべての ACE ロギングをディセーブルにします。 • **default**:メッセージ 106103 のロギングをイネーブルにします。この設定は、**log** オプションを指定しないのと同じです。
operator port	(オプション)**tcp** を指定する場合は、宛先ポート。ポートを指定しなかった場合は、すべてのポートが照合されます。*operator* は次のいずれかになります。 • **lt**:より小さい • **gt**:より大きい • **eq**:等しい • **neq**:等しくない • **range**:値の包括的な範囲。この演算子を使用するときは、ポート番号を 2 つ指定します。たとえば、次のように指定します。 `range 100 200` *port* には、TCP ポートの番号(整数)または名前を指定できます。
permit	条件が一致した場合にアクセスを許可します。
time_range *name*	(オプション)ACE をアクティブにする曜日と時刻を決定する時間範囲オブジェクトを指定します。時間範囲を含めない場合、ACE は常にアクティブです。時間範囲の定義については、**time-range** コマンドを参照してください。
url {*url_string* | **any**}	照合する URL を指定します。すべての URL ベースのトラフィックに一致させるには、**url any** を使用します。そうでない場合は、URL 文字列を入力します。URL 文字列には、ワイルドカードを含めることができます。URL 文字列については、使用上のガイドラインを参照してください。

デフォルト

デフォルトの設定は次のとおりです。

- ACL ロギングによって、拒否されたパケットに対して syslog メッセージ 106103 が生成されます。
- オプションの **log** キーワードを指定した場合、syslog メッセージ 106102 のデフォルト レベルは 6(情報)です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• —	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

access-list webtype コマンドは、クライアントレス SSL VPN フィルタリングを設定するために使用されます。

以下では、URL の指定に関するヒントと制限事項をいくつか示します。

すべての URL を照合する場合は、**any** を選択します。

- 「Permit url any」と指定すると、「プロトコル://サーバ IP/パス」の形式の URL はすべて許可され、このパターンに一致しないトラフィック（ポート転送など）はブロックされます。暗黙的な拒否が発生しないよう、必要なポート（Citrix の場合はポート 1494）への接続を許可する ACE を使用してください。
- スマート トンネルと ica プラグインは、smart-tunnel:// と ica:// のタイプにのみ一致するため、「permit url any」を使用した ACL によって影響を受けることはありません。
- 使用できるプロトコルは、cifs://、citrix://、citrixs://、ftp://、http://、https://、imap4://、nfs://、pop3://、smart-tunnel://、および smtp:// です。プロトコルでワイルドカードを使用することもできます。たとえば、htt* は http および https に一致し、アスタリスク * はすべてのプロトコルに一致します。たとえば、*://*.example.com は、example.com ネットワークへのすべてのタイプの URL ベース トラフィックに一致します。
- smart-tunnel:// URL を指定すると、サーバ名だけを含めることができます。URL にパスを含めることはできません。たとえば、smart-tunnel://www.example.com は受け入れ可能ですが、smart-tunnel://www.example.com/index.html は受け入れ不可です。
- アスタリスク（*）：空の文字列を含む任意の文字列に一致します。すべての http URL に一致させるには、http://*/* と入力します。
- 疑問符 ? は任意の 1 文字に一致します。
- 角カッコ（[]）：文字の範囲を指定する際に使用する演算子です。角カッコ内に指定された範囲に属する任意の 1 文字に一致します。たとえば、http://www.cisco.com:80/ と http://www.cisco.com:81/ の両方に一致させるには、「**http://www.cisco.com:8[01]/**」と入力します。

例

次の例は、特定の企業の URL へのアクセスを拒否する方法を示しています。

```
ciscoasa(config)# access-list acl_company webtype deny url http://*.example.com
```

次の例は、特定の Web ページへのアクセスを拒否する方法を示しています。

```
ciscoasa(config)# access-list acl_file webtype deny url
https://www.example.com/dir/file.html
```

次の例は、特定サーバ上にある任意の URL へのポート 8080 経由の HTTP アクセスを拒否する方法を示しています。

```
ciscoasa(config)# access-list acl_company webtype deny url http://my-server:8080/*
```

関連コマンド

コマンド	説明
clear configure access-list	実行コンフィギュレーションから ACL をクリアします。
show access-list	ACL エントリを番号で表示します。
show running-config access-list	ASA で稼働中のアクセス リストのコンフィギュレーションを表示します。

accounting-mode

アカウンティング メッセージが単一のサーバに送信されるか(シングル モード)、グループ内のすべてのサーバに送信されるか(同時モード)を指定するには、AAA サーバ コンフィギュレーション モードで **accounting-mode** コマンドを使用します。アカウンティング モードの指定を削除するには、このコマンドの **no** 形式を使用します。

accounting-mode {**simultaneous** | **single**}

構文の説明

simultaneous	グループ内のすべてのサーバにアカウンティング メッセージを送信します。
single	単一のサーバにアカウンティング メッセージを送信します。

デフォルト

デフォルト値はシングル モードです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
AAA サーバ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

単一のサーバにアカウンティング メッセージを送信するには、**single** キーワードを使用します。サーバ グループ内のすべてのサーバにアカウンティング メッセージを送信するには、**simultaneous** キーワードを使用します。

このコマンドは、アカウンティング(RADIUS または TACACS+)にサーバ グループが使用されている場合にのみ有効です。

例

次に、**accounting-mode** コマンドを使用して、グループ内のすべてのサーバにアカウンティング メッセージを送信する例を示します。

```
ciscoasa(config)# aaa-server svrgrp1 protocol tacacs+
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)#
```

関連コマンド

コマンド	説明
aaa accounting	アカウンティング サービスをイネーブルまたはディセーブルにします。
aaa-server protocol	AAA サーバ グループ コンフィギュレーション モードを開始し、グループ内のすべてのホストに対してグループ固有かつ共通の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	AAA サーバ コンフィギュレーションをすべて削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

accounting-port

このホストの RADIUS アカウンティングに使用されるポート番号を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **accounting-port** コマンドを使用します。認証ポートの指定を削除するには、このコマンドの **no** 形式を使用します。

accounting-port *port*

no accounting-port

構文の説明

port	RADIUS アカウンティング用のポート番号。有効な値の範囲は 1 ～ 65535 です。

デフォルト

デフォルトでは、デバイスはアカウンティングのためにポート 1646 で RADIUS をリッスンします（RFC 2058 に準拠）。ポートを指定しない場合は、RADIUS アカウンティングのデフォルトのポート番号（1646）が使用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドでは、アカウンティング レコードの送信先となる、リモート RADIUS サーバ ホストの宛先 TCP/UDP ポート番号を指定します。RADIUS アカウンティング サーバで 1646 以外のポートを使用する場合は、**aaa-server** コマンドで RADIUS サービスを開始する前に、適切なポートに対して ASA を設定する必要があります。

このコマンドは、RADIUS 用に設定されているサーバ グループに限り有効です。

例

次に、ホスト「1.2.3.4」に「srvgrp1」という名前の RADIUS AAA サーバを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、アカウンティング ポートを 2222 に設定する例を示します。

```
ciscoasa(config)# aaa-server svrgrp1 protocol radius
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry-interval 7
ciscoasa(config-aaa-server-host)# accountinq-port 2222
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

関連コマンド

コマンド	説明
aaa accounting	ユーザがいずれのネットワーク サービスにアクセスしたかに関するレコードを保持します。
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始します。このモードでは、ホストに固有の AAA サーバ パラメータを設定できます。
clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

accounting-server-group

アカウンティング レコード送信用の AAA サーバ グループを指定するには、さまざまなモードで **accounting-server-group** コマンドを使用します。アカウンティング サーバをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

accounting-server-group *group_tag*

no accounting-server-group [*group_tag*]

構文の説明

group_tag	設定済みのアカウンティング サーバまたはサーバ グループを指定します。アカウンティング サーバを設定するには、**aaa-server** コマンドを使用します。

デフォルト

デフォルトでは、アカウンティング サーバは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
imap4s コンフィギュレーション（廃止）	• 対応	—	• 対応	—	—
pop3s コンフィギュレーション（廃止）	• 対応	—	• 対応	—	—
smtps コンフィギュレーション（廃止）	• 対応	—	• 対応	—	—
トンネル グループ一般属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードではなく、トンネル グループ一般属性コンフィギュレーション モードで使用できます。
9.5(2)	このコマンドは、imap4s モード、pop3s モード、および smtps モードについては廃止されました。
9.8(1)	このコマンドは、IPSec LAN-to-LAN（IPSec-12L）トンネル グループでは使用できなくなりました。実際、IPSec LAN-to-LAN ではサポートされていませんでした。

使用上のガイドライン

ASA では、アカウンティングを使用して、ユーザがアクセスするネットワーク リソースを追跡します。このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ一般属性コンフィギュレーション モードの同等のコマンドに変換されます。

例

次に、トンネル グループ一般属性コンフィギュレーション モードで、リモート アクセス トンネル グループ「xyz」に対して「aaa-server123」という名前のアカウンティング サーバ グループを設定する例を示します。

```
ciscoasa(config)# tunnel-group xyz type remote-access
ciscoasa(config)# tunnel-group xyz general-attributes
ciscoasa(config-tunnel-general)# accounting-server-group aaa-server123
ciscoasa(config-tunnel-general)#
```

関連コマンド

コマンド	説明
aaa-server	認証、許可、およびアカウンティング サーバを設定します。

CHAPTER 2

acl-netmask-convert コマンド～ application-access hide-details コマンド

acl-netmask-convert

aaa-server host コマンドを使用してアクセスする RADIUS サーバからダウンロード可能な ACL に受信したネットマスクを ASA でどのように処理するかを指定するには、AAA サーバ ホスト コンフィギュレーション モードで **acl-netmask-convert** コマンドを使用します。ASA の指定した動作を解除するには、このコマンドの **no** 形式を使用します。

acl-netmask-convert {**auto-detect** | **standard** | **wildcard**}

no acl-netmask-convert

構文の説明

auto-detect	ASA は、使用されているネットマスク表現のタイプを判断しようとします。ASA は、ワイルドカード ネットマスク表現を検出した場合、標準ネットマスク表現に変換します。このキーワードの詳細については、「使用上のガイドライン」を参照してください。
standard	ASA は、RADIUS サーバから受信したダウンロード可能な ACL に標準ネットマスク表現のみが含まれていると見なします。ワイルドカード ネットマスク表現からの変換は実行されません。
wildcard	ASA は、RADIUS サーバから受信したダウンロード可能な ACL にワイルドカード ネットマスク表現のみが含まれていると見なし、ACL のダウンロード時にそれらのすべてを標準ネットマスク表現に変換します。

デフォルト

デフォルトでは、ワイルドカード ネットマスク表現からの変換は実行されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが追加されました。

使用上のガイドライン

RADIUS サーバから提供されるダウンロード可能な ACL にワイルドカード形式のネットマスクが含まれている場合は、wildcard または auto-detect キーワードを指定して **acl-netmask-convert** コマンドを使用します。ASA は、ダウンロード可能な ACL に標準ネットマスク表現が含まれていると想定します。一方、Cisco VPN 3000 シリーズ コンセントレータは、ダウンロード可能な ACL に、標準ネットマスク表現とは逆のワイルドカード ネットマスク表現が含まれていると想定します。ワイルドカード マスクでは、無視するビット位置に 1、照合するビット位置に 0 が配置されます。**acl-netmask-convert** コマンドを使用すると、このような相違が RADIUS サーバ上のダウンロード可能な ACL の設定方法に与える影響を最小限に抑えることができます。

RADIUS サーバの設定方法が不明な場合は、**auto-detect** キーワードが役立ちます。ただし、「穴」があるワイルドカード ネットマスク表現は、正しく検出および変換できません。たとえば、ワイルドカード ネットマスク 0.0.255.0 は、第 3 オクテットに任意の値を許可し、Cisco VPN 3000 シリーズ コンセントレータでは有効に使用できます。ただし、ASA では、この表現をワイルドカード ネットマスクとして検出できません。

例

次に、ホスト「192.168.3.4」に「srvgrp1」という名前の RADIUS AAA サーバを設定し、ダウンロード可能な ACL のネットマスクの変換をイネーブルにして、タイムアウトを 9 秒、再試行間隔を 7 秒、認証ポートを 1650 に設定する例を示します。

```
ciscoasa(config)# aaa-server svrgrp1 protocol radius
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
ciscoasa(config-aaa-server-host)# acl-netmask-convert wildcard
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry-interval 7
ciscoasa(config-aaa-server-host)# authentication-port 1650
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

関連コマンド

コマンド	説明
aaa authentication	**aaa-server** コマンドまたは ASDM ユーザ認証により指定されたサーバ上の LOCAL、TACACS+、または RADIUS ユーザ認証をイネーブルまたはディセーブルにします。
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始します。このモードでは、ホストに固有の AAA サーバパラメータを設定できます。
clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

アクション

アクセス ポリシーをセッションに適用するか、またはセッションを終了するには、ダイナミック アクセス ポリシー レコード コンフィギュレーション モードで **action** コマンドを使用します。セッションをリセットしてアクセス ポリシーをセッションに適用するには、このコマンドの **no** 形式を使用します。

action {continue | terminate}

no action {continue | terminate}

構文の説明

continue	アクセス ポリシーをセッションに適用します。
terminate	接続を切断します。

デフォルト

デフォルト値は continue です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ダイナミック アクセス ポリシー レコード コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

選択したすべての DAP レコードでセッションにアクセス ポリシーを適用するには、**continue** キーワードを使用します。選択した DAP レコードのいずれかで接続を切断するには、**terminate** キーワードを使用します。

例

次に、Finance という DAP ポリシーのセッションを切断する例を示します。

```
ciscoasa (config)# config-dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)# action terminate
ciscoasa(config-dynamic-access-policy-record)#
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
show running-config dynamic-access-policy-record	すべての DAP レコードまたは指定した DAP レコードの実行コンフィギュレーションを表示します。

action cli command

イベント マネージャ アプレットでアクションを設定するには、イベント マネージャ アプレット コンフィギュレーション モードで **action cli command** コマンドを使用します。設定したアクションを削除するには、**no action** *n* コマンドを入力します。

action *n* **cli command** "*command*"

no action *n*

構文の説明

"*command*"	コマンド名を指定します。*command* オプションの値は、引用符で囲む必要があります。引用符で囲んでいない場合、コマンドが 2 つ以上の単語で構成されているとエラーが発生します。このコマンドは、特権レベル 15（最高）を持つユーザとして、グローバル コンフィギュレーション モードで実行されます。ディセーブルになっているため、このコマンドは入力を受け付けない場合があります。**noconfirm** オプションは、コマンドで使用できる場合に使用します。
n	アクション ID を指定します。有効な ID の範囲は 0 ～ 42947295 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
イベント マネージャ アプレット コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

イベント マネージャ アプレットでアクションを設定するには、このコマンドを使用します。

例

次に、イベント マネージャ アプレットでアクションを設定する例を示します。

```
hostname (config-applet)# action 1 cli command "show version"
```

関連コマンド

コマンド	説明
description	アプレットについて説明します。
event manager run	イベント マネージャ アプレットを実行します。
show event manager	設定された各イベント マネージャ アプレットの統計情報を表示します。
debug event manager	イベント マネージャのデバッグ トレースを管理します。

action-uri

Web サーバの URI を指定して、シングル サインオン（SSO）認証用のユーザ名とパスワードを受信するには、AAA サーバ ホスト コンフィギュレーション モードで **action-uri** コマンドを使用します。URI パラメータ値をリセットするには、このコマンドの **no** 形式を使用します。

action-uri *string*

no action-uri

（注） HTTP プロトコルを使用して SSO を正しく設定するには、認証と HTTP プロトコル交換についての詳しい実務知識が必要です。

構文の説明

string	認証プログラムの URI。複数行に入力できます。各行の最大文字数は 255 です。URI 全体の最大文字数は、2048 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

これは HTTP フォームのコマンドを使用した SSO です。URI（ユニフォーム リソース識別子）は、インターネット上のコンテンツの位置を特定するコンパクトな文字列です。これらのコンテンツには、テキスト ページ、ビデオ クリップ、サウンド クリップ、静止画、動画、ソフトウェア プログラムなどがあります。URI の最も一般的な形式は、Web ページ アドレスです。Web ページ アドレスは、URI の特定の形式またはサブセットで、URL と呼ばれます。

ASA の WebVPN サーバでは、POST 要求を使用して、認証 Web サーバに SSO 認証要求を送信できます。これを行うには、HTTP POST 要求を使用して、認証 Web サーバ上のアクション URI にユーザ名とパスワードを渡すように ASA を設定します。**action-uri** コマンドでは、ASA が POST 要求を送信する Web サーバ上の認証プログラムの場所と名前を指定します。

認証 Web サーバ上のアクション URI を見つけるには、ブラウザで直接 Web サーバのログイン ページに接続します。ブラウザに表示されるログイン Web ページの URL が、認証 Web サーバのアクション URI です。

入力しやすいように、URI は連続する複数の行に入力できるようになっています。各行は入力と同時に ASA によって連結され、URI が構成されます。action-uri 行の 1 行あたりの最大文字数は 255 文字ですが、それよりも少ない文字を各行に入力できます。

(注) ストリングに疑問符を含める場合は、疑問符の前に Ctrl+V のエスケープ シーケンスを使用する必要があります。

例

次に、www.example.com の URI を指定する例を示します。

http://www.example.com/auth/index.html/appdir/authc/forms/MCOlogin.fcc?TYPE=33554433&REALMOID=06-000a1311-a828-1185-ab41-8333b16a0008&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=SM5FZmjnk3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fauth.example.com

```
ciscoasa(config)# aaa-server testgrp1 host www.example.com
ciscoasa(config-aaa-server-host)# action-uri http://www.example.com/auth/index.htm
ciscoasa(config-aaa-server-host)# action-uri l/appdir/authc/forms/MCOlogin.fcc?TYP
ciscoasa(config-aaa-server-host)# action-uri 554433&REALMOID=06-000a1311-a828-1185
ciscoasa(config-aaa-server-host)# action-uri -ab41-8333b16a0008&GUID=&SMAUTHREASON
ciscoasa(config-aaa-server-host)# action-uri =0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk
ciscoasa(config-aaa-server-host)# action-uri 3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6r
ciscoasa(config-aaa-server-host)# action-uri B1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F
ciscoasa(config-aaa-server-host)# action-uri %2Fauth.example.com
ciscoasa(config-aaa-server-host)#
```

(注) アクション URI にホスト名とプロトコルを含める必要があります。上記の例では、これらは URI の最初にある http://www.example.com に含まれています。

関連コマンド

コマンド	説明
auth-cookie-name	認証クッキーの名前を指定します。
hidden-parameter	SSO サーバとの交換に使用する非表示パラメータを作成します。
password-parameter	SSO 認証用にユーザ パスワードを送信する必要がある HTTP POST 要求パラメータの名前を指定します。
start-url	プリログイン クッキーを取得する URL を指定します。
user-parameter	SSO 認証用にユーザ名を送信する必要がある HTTP POST 要求のパラメータの名前を指定します。

activate-tunnel-group-script

このコマンドは、tunnel-group sub-mode で username-from-certificate が設定されている場合に、ASDM によって生成されたスクリプト ファイルをリロードするために内部で使用されます。

（注） このコマンドは、ASA CLI では使用しないでください。

activation-key

ASA にライセンス アクティベーション キーを入力するには、特権 EXEC モードで **activation-key** コマンドを使用します。

activation-key [**noconfirm**] *activation_key* [**activate** | **deactivate**]

構文の説明

activate	時間ベースのアクティベーション キーをアクティブ化します。**activate** がデフォルト値です。特定の機能に対して最後にアクティブ化した時間ベース キーがアクティブになります。
activation_key	アクティベーション キーを ASA に適用します。*activation_key* は、各要素の間にスペースを 1 つ入れた 5 つの要素から構成される 16 進数のストリングです。先頭の 0x 指定子は任意です。すべての値が 16 進数と見なされます。 1 つの永続キーおよび複数の時間ベース キーをインストールできます。新しい永続キーを入力した場合、すでにインストール済みのキーが上書きされます。
deactivate	時間ベースのアクティベーション キーを非アクティブ化します。非アクティブ化した場合でも、アクティベーション キーは ASA にインストールされたままです。後で **activate** キーワードを使用してアクティブ化できます。キーの初回入力時で、**deactivate** を指定した場合、キーは ASA に非アクティブ ステートでインストールされます。
noconfirm	(オプション)確認を求めるプロンプトを表示せずにアクティベーション キーを入力します。

デフォルト

デフォルトでは、ASA は、ライセンスがすでにインストールされた状態で出荷されます。このライセンスは、注文した内容およびベンダーがインストールした内容に応じて、ライセンスを追加できる基本ライセンスの場合と、すべてのライセンスがすでにインストールされている場合があります。インストールされているライセンスを確認するには、**show activation-key** コマンドを使用します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	•

コマンド履歴

リリース	変更内容
7.0(5)	次の制限値が増加されました。 • ASA5510 Base ライセンス接続は 32000 から 5000 に、VLAN は 0 から 10 に増加。 • ASA5510 Security Plus ライセンス接続は 64000 から 130000 に、VLAN は 10 から 25 に増加。 • ASA5520 接続は 130000 から 280000 に、VLAN は 25 から 100 に増加。 • ASA5540 接続は 280000 から 400000 に、VLAN は 100 から 200 に増加。
7.1(1)	SSL VPN ライセンスが追加されました。
7.2(1)	5000 ユーザの SSL VPN ライセンスが ASA 5550 以降に対して追加されました。
7.2(2)	• ASA 5505 ASA上の Security Plus ライセンスに対する VLAN 最大数が、5(3 つのフル機能インターフェイス、1 つのフェールオーバー インターフェイス、1 つのバックアップ インターフェイスに制限されるインターフェイス)から 20 のフル機能インターフェイスに増加されました。また、トランク ポート数も 1 から 8 に増加されました。 • VLAN の制限値が変更されました。ASA 5510 の基本ライセンスでは 10 から 50 に、Security Plus ライセンスでは 25 から 100 に、ASA 5520 では 100 から 150 に、ASA 5550 では 200 から 250 に増えています。
7.2(3)	ASA 5510 は、GE(ギガビット イーサネット)を Security Plus ライセンスのあるポート 0 および 1 でサポートします。ライセンスを Base から Security Plus にアップグレードした場合、外部 Ethernet 0/0 および Ethernet 0/1 ポートの容量は、元の FE(ファスト イーサネット)の 100 Mbps から GE の 1000 Mbps に増加します。インターフェイス名は Ethernet 0/0 および Ethernet 0/1 のままです。**speed** コマンドを使用してインターフェイスの速度を変更します。また、**show interface** コマンドを使用して各インターフェイスの現在の設定速度を確認します。
8.0(2)	• Advanced Endpoint Assessment ライセンスが追加されました。 • VPN ロードバランシングが ASA 5510 Security Plus ライセンスでサポートされます。
8.0(3)	AnyConnect for Mobile ライセンスが追加されました。
8.0(4)/8.1(2)	時間ベース ライセンスが追加されました。
8.1(2)	ASA 5580 上でサポートされる VLAN 数が 100 から 250 に増加されました。
8.0(4)	UC Proxy セッション ライセンスが追加されました。
8.2(1)	• ボットネット トラフィック フィルタ ライセンスが追加されました。 • AnyConnect Essentials ライセンスが追加されました。デフォルトで、ASA は AnyConnect Essentials ライセンスを使用します。これをディセーブルにして他のライセンスを使用するには、**no anyconnect-essentials** コマンドを使用します。 • SSL VPN の共有ライセンスが追加されました。
8.2(2)	モビリティ プロキシに UC Proxy ライセンスが必要なくなりました。

リリース	変更内容
8.3(1)	• フェールオーバー ライセンスが各ユニット上で同一である必要がなくなりました。両方のユニットで使用するライセンスは、プライマリ ユニットおよびセカンダリ ユニットからの結合されたライセンスです。 • 時間ベース ライセンスがスタッカブルになりました。 • IME ライセンスが追加されました。 • 時間ベース ライセンスを複数インストールできるようになり、同時に機能ごとに 1 つのアクティブなライセンスを保持できます。 • **activate** キーワードまたは **deactivate** キーワードを使用して、時間ベース ライセンスをアクティブ化または非アクティブ化できます。
8.4(1)	• ASA 5550 および ASA 5585-X（SSP-10）では、コンテキストの最大数が 50 から 100 に引き上げられました。ASA 5580 および 5585-X（SSP-20）以降では、コンテキストの最大数が 50 から 250 に引き上げられました。 • ASA 5580 および ASA 5585-X では、VLAN の最大数が 250 から 1024 に引き上げられました。 • ファイアウォール接続の最大数が次のように引き上げられました。 – ASA 5580-20：1,000 K から 2,000 K へ – ASA 5580-40：2,000 K から 4,000 K へ – ASA 5585-X（SSP-10 搭載）：750 K から 1,000 K へ – ASA 5585-X（SSP-20 搭載）：1,000 K から 2,000 K へ – ASA 5585-X（SSP-40 搭載）：2,000 K から 4,000 K へ – ASA 5585-X（SSP-60 搭載）：2,000 K から 10,000 K へ • ASA 5580 の場合、AnyConnect VPN セッションの制限が 5,000 から 10,000 に引き上げられました。 • ASA 5580 の場合、その他の VPN セッションの制限が 5,000 から 10,000 に引き上げられました。 • AnyConnect Essentials ライセンスおよび AnyConnect Premium ライセンスに IKEv2 を使用した IPsec リモート アクセス VPN が追加されました。 • Other VPN ライセンス（以前の IPsec VPN）にはサイトツーサイト セッションが追加されました。 • ペイロード暗号化機能のないモデルでは（ASA 5585-X など）、ASA ソフトウェアは ASA で特定の国にエクスポートできるようにして、Unified Communications と VPN 機能をディセーブルにします。

使用上のガイドライン

アクティベーション キーの取得

アクティベーション キーを取得するには、シスコの代理店から購入できる Product Authorization Key が必要になります。機能ライセンスごとに個別の製品アクティベーション キーを購入する必要があります。たとえば、基本ライセンスがある場合は、Advanced Endpoint Assessment 用と追加の SSL VPN セッション用に別々のキーを購入する必要があります。

製品認証キーを取得した後、次のいずれかの URL の Cisco.com でキーを登録する必要があります。

- Cisco.com の登録済みユーザの場合は、次の Web サイトを使用します。

  http://www.cisco.com/go/license

- Cisco.com の登録済みユーザではない場合は、次の Web サイトを使用します。

  http://www.cisco.com/go/license/public

コンテキスト モードのガイドライン

- マルチ コンテキスト モードでシステム実行スペース内にアクティベーション キーを適用します。
- 共有ライセンスは、マルチ コンテキスト モードではサポートされていません。

フェールオーバーのガイドライン

- 共有ライセンスは、アクティブ/アクティブ モードではサポートされていません。
- フェールオーバー ユニットは、各ユニット上で同一のライセンスを必要としません。

  旧バージョンの ASA ソフトウェアは、各ユニット上のライセンスが一致する必要がありました。バージョン 8.3(1) から、同一のライセンスをインストールする必要がなくなりました。通常、ライセンスをプライマリ ユニット専用に購入します。アクティブ/スタンバイ フェールオーバーでは、セカンダリ ユニットがアクティブになるとプライマリ ライセンスを継承します。両方のユニット上にライセンスがある場合、これらのライセンスは単一の実行フェールオーバー クラスタ ライセンスに結合されます。

- ASA 5505 および 5510 では、両方の装置に Security Plus ライセンスが必要です。基本ライセンスはフェールオーバーをサポートしないため、基本ライセンスのみを保持するスタンバイ装置ではフェールオーバーをイネーブルにできません。

アップグレードとダウングレードのガイドライン

任意の旧バージョンから最新バージョンにアップグレードした場合、アクティベーション キーの互換性は存続します。ただし、ダウングレード機能の維持には問題が生じる場合があります。

- バージョン 8.1 以前にダウングレードする場合:アップグレード後に、*8.2 より前*に追加された機能のライセンスを追加でアクティブ化すると、ダウングレードした場合でも旧バージョンに対するアクティベーション キーの互換性は存続します。ただし、*8.2 以降*に追加された機能ライセンスをアクティブ化した場合は、アクティベーション キーの下位互換性がなくなります。互換性のないライセンス キーがある場合は、次のガイドラインを参照してください。
  - 旧バージョンでアクティベーション キーを入力した場合は、そのキーが ASA で使用されます(バージョン 8.2 以降でアクティブ化した新しいライセンスがない場合)。
  - 新しいシステムで、以前のアクティベーション キーがない場合は、旧バージョンと互換性のある新しいアクティベーション キーを要求する必要があります。

- バージョン 8.2 以前にダウングレードする場合：バージョン 8.3 では、より堅牢な時間ベース キーの使用およびフェールオーバー ライセンスの変更が次のとおり追加されました。
  - 複数の時間ベースのアクティベーション キーがアクティブな場合、ダウングレード時には一番最近アクティブ化された時間ベース キーのみがアクティブになれます。他のキーはすべて非アクティブ化されます。
  - フェールオーバー ペアに不一致のライセンスがある場合、ダウングレードによりフェールオーバーはディセーブルになります。キーが一致した場合でも、使用するライセンスは、結合されたライセンスではなくなります。

その他のガイドラインと制限事項

- アクティベーション キーは、コンフィギュレーション ファイルには保存されません。隠しファイルとしてフラッシュ メモリに保存されます。
- アクティベーション キーは、デバイスのシリアル番号に関連付けられます。機能ライセンスは、デバイス間で転送できません（ハードウェア障害の発生時を除く）。ハードウェア障害が発生したためにデバイスを交換する必要がある場合は、シスコのライセンス チームに連絡して、既存のライセンスを新しいシリアル番号に転送するよう依頼してください。シスコのライセンス チームから、製品認証キーの参照番号と既存のシリアル番号を求められます。
- 購入後に、返金またはアップグレードしたライセンスのためにライセンスを返却できません。
- すべてのライセンス タイプをアクティブ化できますが、たとえば、マルチ コンテキスト モードおよび VPN など一部の機能には相互互換性がありません。AnyConnect Essentials ライセンスの場合、次のライセンスとは互換性がありません。SSL VPN フル ライセンス、SSL VPN 共有ライセンス、および Advanced Endpoint Assessment ライセンス。デフォルトでは、AnyConnect Essentials ライセンスがこれらのライセンスの代わりに使用されます。設定の AnyConnect Essentials ライセンスをディセーブルにして他のライセンスを使用するように復元するには、**no anyconnect-essentials** コマンドを使用します。
- 一部の永続ライセンスでは、アクティブ化後に ASA をリロードする必要があります。表 2-1 に、リロードが必要なライセンスを示します。

表 2-1　永続ライセンスのリロード要件

モデル	リロードが必要なライセンス アクション
ASA 5505 および ASA 5510	基本ライセンスと Security Plus ライセンスの切り替え
すべてのモデル	暗号化ライセンスの変更
すべてのモデル	永続ライセンスのダウングレード（たとえば、10 個のコンテキストから 2 個のコンテキストへ）。

例

次に、ASA のアクティベーション キーを変更する例を示します。

```
ciscoasa# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

次に、**activation-key** コマンドの出力例を示します。ここでは、新しいアクティベーション キーが古いアクティベーション キーと異なる場合のフェールオーバーに対する出力が示されています。

```
ciscoasa# activation-key 0xyadayada 0xyadayada 0xyadayada 0xyadayada 0xyadayada

Validating activation key. This may take a few minutes...
The following features available in the running permanent activation key are NOT available
in the new activation key:
```

```
Failover is different.
   running permanent activation key: Restricted (R)
   new activation key: Unrestricted (UR)
WARNING: The running activation key was not updated with the requested key.
Proceed with updating flash activation key? [y]
Flash permanent activation key was updated with the requested key.
```

次に、ライセンス ファイルの出力例を示します。

```
Serial Number Entered: 123456789ja
Number of Virtual Firewalls Selected: 10
Formula One device: ASA 5520

Failover                        : Enabled
VPN-DES                         : Enabled
VPN-3DES-AES                    : Enabled
Security Contexts               : 10
GTP/GPRS                        : Disabled
SSL VPN Peers                   : Default
Total VPN Peers                 : 750
Advanced Endpoint Assessment    : Disabled
AnyConnect for Mobile           : Enabled
AnyConnect for Cisco VPN Phone  : Disabled
Shared License                  : Disabled
UC Phone Proxy Sessions         : Default
Total UC Proxy Sessions         : Default
AnyConnect Essentials           : Disabled
Botnet Traffic Filter           : Disabled
Intercompany Media Engine       : Enabled

----------------------------------------
THE FOLLOWING ACTIVATION KEY IS VALID FOR:
ASA SOFTWARE RELEASE 8.2+ ONLY.

Platform = asa

123456789JA:yadayda1 yadayda1 yadayda1 yadayda1 yadayda1
----------------------------------------
THE FOLLOWING ACTIVATION KEY IS VALID FOR:
ALL ASA SOFTWARE RELEASES, BUT EXCLUDES ANY
8.2+ FEATURES FOR BACKWARDS COMPATIBILITY.

Platform = asa

123456789JA:yadayda2 yadayda2 yadayda2 yadayda2 yadayda2
```

関連コマンド

コマンド	説明
anyconnect-essentials	AnyConnect Essentials ライセンスをイネーブルまたはディセーブルにします。
show activation-key	アクティベーション キーを表示します。
show version	ソフトウェア バージョンおよびアクティベーション キーを表示します。

activex-relay

クライアントレス ポータルに ActiveX を必要とするアプリケーションを埋め込むには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで **activex-relay** コマンドを使用します。デフォルトのグループ ポリシーから **activex-relay** コマンドを継承するには、このコマンドの **no** 形式を使用します。

activex-relay {**enable** | **disable**}

no activex-relay

構文の説明

enable	WebVPN セッションの ActiveX をイネーブルにします。
disable	WebVPN セッションの ActiveX をディセーブルにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

オブジェクト タグがある HTML コンテンツ（画像、オーディオ、ビデオ、Java アプレット、ActiveX、PDF、またはフラッシュなど）に対する ActiveX をユーザが WebVPN ブラウザから起動できるようにするには、**activex-relay enable** コマンドを使用します。これらのアプリケーションでは、WebVPN セッションを使用して ActiveX コントロールをダウンロードおよびアップロードします。ActiveX リレーは、WebVPN セッションが閉じるまで有効です。Microsoft OWA 2007 などを使用する場合は、ActiveX をディセーブルにする必要があります。

（注） これらには同じ機能があるため、スマート トンネルをディセーブルにしても、**activex-relay enable** コマンドによってスマート トンネルのログが生成されます。

次に、特定のグループ ポリシーに関連付けられている WebVPN セッションの ActiveX コントロールをイネーブルにする例を示します。

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# activex-relay enable
```

次に、特定のユーザ名に関連付けられている WebVPN セッションの ActiveX コントロールをディセーブルにする例を示します。

```
ciscoasa(config-username-policy)# webvpn
ciscoasa(config-username-webvpn)# activex-relay disable
```

ad-agent-mode

Cisco アイデンティティ ファイアウォール インスタンスの Active Directory エージェントを設定できるように AD エージェント モードをイネーブルにするには、グローバル コンフィギュレーション モードで **ad-agent-mode** コマンドを使用します。

ad-agent-mode

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

アイデンティティ ファイアウォールに対して Active Directory エージェントを設定するには、**aaa-server** コマンドのサブモードである **ad-agent-mode** コマンドを入力します。**ad-agent-mode** コマンドを入力すると、AAA サーバ グループ コンフィギュレーション モードが開始されます。

AD エージェントは、定期的に、または要求に応じて、WMI を介して Active Directory サーバのセキュリティ イベント ログ ファイルをモニタし、ユーザのログインおよびログオフ イベントを調べます。AD エージェントは、ユーザ ID および IP アドレス マッピングのキャッシュを保持し、ASA に変更を通知します。

AD エージェント サーバ グループのプライマリ AD エージェントとセカンダリ AD エージェントを設定します。プライマリ AD エージェントが応答していないことを ASA が検出し、セカンダリ AD エージェントが指定されている場合、ASA はセカンダリ AD エージェントに切り替えます。AD エージェントの Active Directory サーバは、通信プロトコルとして RADIUS を使用します。そのため、ASA と AD エージェントとの共有秘密のキー属性を指定する必要があります。

例

次に、アイデンティティ ファイアウォールの Active Directory エージェントを設定するときに、**ad-agent-mode** をイネーブルにする例を示します。

```
ciscoasa(config)# aaa-server adagent protocol radius
ciscoasa(config)# ad-agent-mode
ciscoasa(config-aaa-server-group)# aaa-server adagent (inside) host 192.168.1.101
ciscoasa(config-aaa-server-host)# key mysecret
ciscoasa(config-aaa-server-hostkey)# user-identity ad-agent aaa-server adagent
ciscoasa(config-aaa-server-host)# test aaa-server ad-agent
```

関連コマンド

コマンド	説明
aaa-server	AAA サーバ グループを作成し、グループ固有の AAA サーバ パラメータとすべてのグループ ホストに共通の AAA サーバ パラメータを設定します。
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。

address（ダイナミック フィルタ ブラックリスト、ホワイトリスト）

IP アドレスをボットネット トラフィック フィルタのブラックリストまたはホワイトリストに追加するには、ダイナミック フィルタ ブラックリストまたはホワイトリスト コンフィギュレーション モードで **address** コマンドを使用します。アドレスを削除するには、このコマンドの **no** 形式を使用します。

address *ip_address mask*

no address *ip_address mask*

構文の説明

ip_address	ブラックリストに IP アドレスを追加します。
mask	IP アドレスのサブネット マスクを定義します。*mask* には、単一ホストまたはサブネットのマスクを指定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ダイナミック フィルタ ブラックリストまたはホワイトリスト コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

スタティック データベースを使用すると、ホワイトリストまたはブラックリストに追加するドメイン名または IP アドレスでダイナミック データベースを増強できます。ダイナミック フィルタ ホワイトリストまたはブラックリスト コンフィギュレーション モードを開始した後、**address** コマンドおよび **name** コマンドを使用して、適切な名前としてホワイトリストに、または不適切な名前としてブラックリストにタグ付けするドメイン名または IP アドレス（ホストまたはサブネット）を手動で入力できます。

このコマンドを複数回入力して、複数のエントリを追加できます。最大 1000 個のブラックリスト エントリと、最大 1000 個のホワイトリスト エントリを追加できます。

例

次に、ブラックリストおよびホワイトリストのエントリを作成する例を示します。

```
ciscoasa(config)# dynamic-filter blacklist
ciscoasa(config-llist)# name bad1.example.com
ciscoasa(config-llist)# name bad2.example.com
ciscoasa(config-llist)# address 10.1.1.1 255.255.255.0
ciscoasa(config-llist)# dynamic-filter whitelist
ciscoasa(config-llist)# name good.example.com
ciscoasa(config-llist)# name great.example.com
ciscoasa(config-llist)# name awesome.example.com
ciscoasa(config-llist)# address 10.1.1.2 255.255.255.255
```

関連コマンド

コマンド	説明
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。

コマンド	説明
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

address（media-termination）（廃止）

電話プロキシ機能へのメディア接続に使用するメディア ターミネーション インスタンスのアドレスを指定するには、メディア ターミネーション コンフィギュレーション モードで **address** コマンドを使用します。メディア ターミネーション コンフィギュレーションからアドレスを削除するには、このコマンドの **no** 形式を使用します。

address *ip_address* [**interface** *intf_name*]

no address *ip_address* [**interface** *intf_name*]

構文の説明

interface *intf_name*	メディア ターミネーション アドレスを使用するインターフェイスの名前を指定します。1 つのインターフェイスに設定できるメディア ターミネーション アドレスは 1 つだけです。
ip_address	メディア ターミネーション インスタンスに使用する IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
メディア ターミネーション コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。
9.4(1)	このコマンドは、すべての **phone-proxy** および **uc-ime** コマンドとともに廃止されました。

使用上のガイドライン

ASA では、次の基準を満たすメディア ターミネーションの IP アドレスが設定されている必要があります。

- メディア ターミネーション インスタンスでは、すべてのインターフェイスに対してグローバルなメディア ターミネーション アドレスを設定することも、インターフェイスごとにメディア ターミネーション アドレスを設定することもできます。しかし、グローバルなメディア ターミネーション アドレスと、インターフェイスごとに設定するメディア ターミネーション アドレスは同時に使用できません。
- 複数のインターフェイスに対してメディア ターミネーション アドレスを設定する場合、IP 電話との通信時に ASA で使用するアドレスを、インターフェイスごとに設定する必要があります。
- IP アドレスは、そのインターフェイスのアドレス範囲内で使用されていない、パブリックにルーティング可能な IP アドレスです。

例

次に、media-termination address コマンドを使用して、メディア接続に使用する IP アドレスを指定する例を示します。

```
ciscoasa(config)# media-termination mediaterm1
ciscoasa(config-media-termination)# address 192.0.2.25 interface inside
ciscoasa(config-media-termination)# address 10.10.0.25 interface outside
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。
media-termination	電話プロキシ インスタンスに適用するメディア ターミネーション インスタンスを設定します。

address-family ipv4

標準 IP Version 4（IPv4）アドレス プレフィックスを使用してルーティング セッションを設定するためのアドレス ファミリを入力するには、ルータ コンフィギュレーション モードで **address-family ipv4** コマンドを使用します。アドレス ファミリ コンフィギュレーション モードを終了し、実行コンフィギュレーションから IPv4 アドレス ファミリ コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

address-family ipv4

no address-family ipv4

デフォルト

IPv4 アドレス プレフィックスはイネーブルではありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ モード コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

address-family ipv4 コマンドは、コンテキスト ルータをアドレス ファミリ コンフィギュレーション モードにします。このルータから、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定できます。アドレス ファミリ コンフィギュレーション モードを終了し、ルータ コンフィギュレーション モードに戻るには、**exit** と入力します。

（注） アドレス ファミリ IPv4 のルーティング情報が、**neighbor remote-as** コマンドを使用して設定した各 BGP ルーティング セッションにデフォルトでアドバタイズされます。ただし、**neighbor remote-as** コマンドを設定する前に **no bgp default ipv4-unicast** コマンドを入力している場合は除きます。

例

次に、ルータを IPv4 アドレス ファミリのアドレス ファミリ コンフィギュレーション モードにする例を示します。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)#
```

関連コマンド

コマンド	説明
bgp default ipv4-unicast	BGP ピアリング セッションのデフォルトとして IP Version 4（IPv4）ユニキャスト アドレス ファミリを設定します。
neighbor remote-as	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。

address-family ipv6

標準 IP Version 6（IPv6）アドレス プレフィックスを使用してルーティング セッション（BGP など）を設定するためのアドレス ファミリを入力するには、ルータ コンフィギュレーション モードで **address-family ipv6** コマンドを使用します。アドレス ファミリ コンフィギュレーション モードを終了し、実行コンフィギュレーションから IPv6 アドレス ファミリ コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

address-family ipv6 [unicast]

no address-family ipv6

構文の説明

unicast	（オプション）IPv6 ユニキャスト アドレス プレフィックスを指定します。

デフォルト

IPv6 アドレス プレフィックスはイネーブルではありません。IPv6 アドレス プレフィックスが設定されている場合は、ユニキャスト アドレス プレフィックスがデフォルトです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ モード コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

使用上のガイドライン

address-family ipv6 コマンドは、コンテキスト ルータをアドレス ファミリ コンフィギュレーション モードにします。このルータから、標準 IPv6 アドレス プレフィックスを使用するルーティング セッションを設定できます。アドレス ファミリ コンフィギュレーション モードを終了し、ルータ コンフィギュレーション モードに戻るには、**exit** と入力します。

例

次に、ルータを IPv4 アドレス ファミリのアドレス ファミリ コンフィギュレーション モードにする例を示します。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv6
ciscoasa(config-router-af)#
```

関連コマンド

コマンド	説明
neighbor ipv6-address activate	BGP ネイバーとの情報交換をイネーブルにします。

address-pool

アドレスをリモート クライアントに割り当てるためのアドレス プールのリストを指定するには、トンネル グループ一般属性コンフィギュレーション モードで **address-pool** コマンドを使用します。アドレス プールを削除するには、このコマンドの **no** 形式を使用します。

address-pool [(*interface name*)] *address_pool1* [*...address_pool6*]

no address-pool [(*interface name*)] *address_pool1* [*...address_pool6*]

構文の説明

address_pool	**ip local pool** コマンドで設定したアドレス プールの名前を指定します。最大 6 個のローカル アドレス プールを指定できます。
interface name	（任意）アドレス プールに使用するインターフェイスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

これらのコマンドは、インターフェイスごとに 1 つずつ、複数入力できます。インターフェイスが指定されていない場合、コマンドは明示的に参照されていないインターフェイスすべてに対してデフォルトを指定します。

グループ ポリシーの **address-pools** コマンドによるアドレス プール設定は、トンネル グループの **address-pool** コマンドによるローカル プール設定を上書きします。

プールの指定順序は重要です。ASA では、このコマンドでプールを指定した順序に従って、それらのプールからアドレスが割り当てられます。

例

次に、設定トンネル一般コンフィギュレーション モードで、IPsec リモート アクセス トンネル グループ テスト用にアドレスをリモート クライアントに割り当てるためのアドレス プールのリストを指定する例を示します。

```
ciscoasa(config)# tunnel-group test type remote-access
ciscoasa(config)# tunnel-group test general
ciscoasa(config-tunnel-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
ciscoasa(config-tunnel-general)#
```

関連コマンド

コマンド	説明
ip local pool	VPN リモート アクセス トンネルに使用する IP アドレス プールを設定します。
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group-map default-group	**crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリをトンネル グループに関連付けます。

address-pools

アドレスをリモート クライアントに割り当てるためのアドレス プールのリストを指定するには、グループ ポリシー属性コンフィギュレーション モードで **address-pools** コマンドを使用します。グループ ポリシーから属性を削除し、別のグループ ポリシー ソースからの継承をイネーブルにするには、このコマンドの **no** 形式を使用します。

address-pools value *address_pool1* [*...address_pool6*]

no address-pools value *address_pool1* [*...address_pool6*]

address-pools none

no address-pools none

構文の説明

address_pool	**ip local pool** コマンドで設定したアドレス プールの名前を指定します。最大 6 個のローカル アドレス プールを指定できます。
none	アドレス プールを設定しないことを指定し、他のグループ ポリシーからの継承をディセーブルにします。
value	アドレスの割り当てに使用する最大 6 個のアドレス プールのリストを指定します。

デフォルト

デフォルトでは、アドレス プールの属性は継承を許可します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドによるアドレス プール設定は、グループ内のローカル プール設定を上書きします。ローカル アドレスの割り当てに使用する最大 6 個のローカル アドレス プールのリストを指定できます。

プールの指定順序は重要です。ASA では、このコマンドでプールを指定した順序に従って、それらのプールからアドレスが割り当てられます。

address-pools none コマンドは、この属性が他のポリシー（DefaultGrpPolicy など）から継承されないようにします。**no address pools none** コマンドは、**address-pools none** コマンドをコンフィギュレーションから削除して、デフォルト値（継承の許可）に戻します。

例

次に、GroupPolicy1 の設定一般コンフィギュレーション モードで、アドレスをリモート クライアントに割り当てるために使用するアドレス プールのリストとして pool_1 および pool_20 を設定する例を示します。

```
ciscoasa(config)# ip local pool pool_1 192.168.10.1-192.168.10.100 mask 255.255.0.0
ciscoasa(config)# ip local pool pool_20 192.168.20.1-192.168.20.200 mask 255.255.0.0
ciscoasa(config)# group-policy GroupPolicy1 attributes
ciscoasa(config-group-policy)# address-pools value pool_1 pool_20
ciscoasa(config-group-policy)#
```

関連コマンド

コマンド	説明
ip local pool	VPN グループ ポリシーで使用する IP アドレス プールを設定します。
clear configure group-policy	設定されているすべてのグループ ポリシーをクリアします。
show running-config group-policy	すべてのグループ ポリシーまたは特定のグループ ポリシーのコンフィギュレーションを表示します。

admin-context

システム コンフィギュレーションの管理コンテキストを設定するには、グローバル コンフィギュレーション モードで **admin-context** コマンドを使用します。

admin-context *name*

構文の説明

name	名前を最大 32 文字のストリングで設定します。コンテキストをまだ定義していない場合は、まずこのコマンドで管理コンテキスト名を指定します。次に、**context** コマンドを使用して最初に追加するコンテキストを、指定した管理コンテキスト名にする必要があります。 この名前では大文字と小文字が区別されるため、たとえば、「customerA」および「CustomerA」という 2 つのコンテキストを保持できます。文字、数字、またはハイフンを使用できますが、名前の先頭または末尾にハイフンは使用できません。 「System」および「Null」（大文字と小文字の両方）は予約されている名前であり、使用できません。

デフォルト

マルチ コンテキスト モードの新しい ASA の場合、管理コンテキスト名は「admin」です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

コンテキスト コンフィギュレーションが内部フラッシュ メモリにある限り、任意のコンテキストを管理コンテキストに設定できます。

現在の管理コンテキストを削除するには、**clear configure context** コマンドを使用してすべてのコンテキストを削除する必要があります。

システム コンフィギュレーションには、システム自体のネットワーク インターフェイスまたはネットワーク設定は含まれません。代わりに、システムは、ネットワーク リソースにアクセスする必要がある場合に（ASA ソフトウェアをダウンロードしたり、管理者に対してリモート アクセスを許可する場合など）、管理コンテキストとして指定されたコンテキストのいずれかを使用します。

例

次に、管理コンテキストを「administrator」に設定する例を示します。

```
ciscoasa(config)# admin-context administrator
```

関連コマンド

コマンド	説明
clear configure context	システム コンフィギュレーションからすべてのコンテキストを削除します。
context	システム コンフィギュレーションにコンテキストを設定し、コンテキスト コンフィギュレーション モードを開始します。
show admin-context	現在の管理コンテキスト名を表示します。

advertise passive-only

パッシブ インターフェイスに属するプレフィックスだけをアドバタイズするように IS-IS を設定するには、ルータ コンフィギュレーション モードで **advertise passive-only** コマンドを使用します。制限を削除するには、このコマンドの **no** 形式を使用します。

advertise passive-only

no advertise passive-only

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルトの動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ isis コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、リンクステート パケット（LSP）アドバタイズメントから、接続されたネットワークの IP プレフィックスを除外し、IS-IS コンバージェンス時間を削減するための IS-IS メカニズムです。

IS-IS インスタンスごとにこのコマンドを設定すると、ルータの非疑似ノード LSP でアドバタイズされるプレフィックスの数が少なくなるため、IS-IS コンバージェンス時間の削減という課題をスケーラブルに解決することができます。

このコマンドは、「ループバック インターフェイスで IS-IS をイネーブルにする場合、通常、ループバックを受動に設定する」という事実に依存しています。この設定は、ループバックの背後にネイバーが見つかる可能性はないため、ループバックを通じて、必要のない Hello パケットの送信を防ぐために行われます。したがって、アドバタイズする必要があるものがループバックだけで、このループバックがすでに受動に設定されている場合、IS-IS インスタンスごとに **advertise passive-only** コマンドを設定することにより、ルーティング テーブルのデータ過剰を防ぐことができます。

このコマンドの代わりは **no isis advertise-prefix** コマンドです。**no isis advertise-prefix** コマンドは、インターフェイスごとに設定される、規模の小さいソリューションです。

例

次に、**advertise passive-only** コマンドを使用する例を示します。このコマンドは、IS-IS インスタンスに作用し、イーサネット インターフェイス 0 の IP ネットワークのアドバタイズを阻止します。ループバック インターフェイス 0 の IP アドレスだけがアドバタイズされます。

```
!
!
!
interface Gi0/0
 ip address 192.168.20.1 255.255.255.0
router isis
!.
int gi0/1
  ip add 171.1.1.1 255.255.255.0
   router isis
!.
router isis
 passive-interface outside
 net 47.0004.004d.0001.0001.0c11.1111.00
 advertise-passive-only
 log-adjacency-changes
!
```

関連コマンド

コマンド	説明
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。

コマンド	説明
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト(TLV)を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。

コマンド	説明
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

aggregate-address

Border Gateway Protocol（BGP）データベース内に集約エントリを作成するには、アドレス ファミリ コンフィギュレーション モードで **aggregate-address** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

aggregate-address *address mask* [**as-set**] [**summary-only] [suppress-map** *map-name*]**[advertise-map** *map-name*] [**attribute-map** *map-name*]

no aggregate-address *address mask* [**as-set**] [**summary-only] [suppress-map** *map-name*]**[advertise-map** *map-name*] [**attribute-map** *map-name*]

構文の説明

address	集約アドレス。
mask	集約マスク。
as-set	（オプション）自律システム設定パス情報を生成します。
summary-only	（任意）アップデートからのすべてのより具体的なルートをフィルタ処理します。
suppress-map *map-name*	（オプション）抑制するルートの選択に使用されるルート マップの名前を指定します。
advertise-map *map-name*	（オプション）AS_SET 送信元コミュニティを作成するルートの選択に使用されるルート マップの名前を指定します。
attribute-map *map-name*	（オプション）集約ルートの属性を設定するために使用されるルート マップの名前を指定します。

デフォルト

アトミック集約属性は、**as-set** キーワードが指定されない限り、このコマンドによって集約ルートが作成されるときに自動的に設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
コンテキスト コンフィギュレーション、アドレス ファミリ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	このコマンドは、アドレス ファミリ ipv6 サブモードでサポートされるように変更されました。

使用上のガイドライン

集約ルートを BGP またはマルチプロトコル BGP（mBGP）に再配布するか、条件付きの集約ルーティング機能を使用することにより、BGP および mBGP に集約ルーティングを実装できます。

キーワードなしで **aggregate-address** コマンドを使用すると、指定された範囲内にあるより具体的な BGP または mBGP ルートが使用できる場合、BGP または mBGP ルーティング テーブルに集約エントリが作成されます（集約に一致する長いプレフィックスは、ルーティング情報ベース（RIB）に存在する必要があります）。集約ルートは自律システムからのルートとしてアドバタイズされます。また、この集約ルートには、情報が失われている可能性を示すために、アトミック集約属性が設定されます（アトミック集約属性は、**as-set** キーワードを指定しない限りデフォルトで設定されます）。

as-set キーワードを使用すると、コマンドがこのキーワードなしで従う同じルールを使用する集約エントリが作成されますが、このルートにアドバタイズされるパスは、集約されているすべてのパス内に含まれるすべての要素で構成される AS_SET になります。このルートは集約されたルート変更に関する自律システム パス到着可能性情報として継続的に削除してアップデートする必要があるため、多くのパスを集約する際に **aggregate-address** コマンドのこの形式を使用しないでください。

summary-only キーワードを使用すると、集約ルート（192.*.*.* など）が作成されるだけでなく、すべてのネイバーへのより具体的なルートのアドバタイズメントが抑制されます。特定のネイバーへのアドバタイズメントのみを抑制したい場合、**neighbor distribute-list** コマンドを使用できますが、慎重に使用すべきです。より具体的なルートがリークした場合、すべての BGP または mBGP ルータは、生成中の具体的でない集約よりもこのルートを優先します（最長一致ルーティングによる）。

suppress-map キーワードを使用すると、集約ルートは作成されますが、指定されたルートのアドバタイズメントが抑制されます。ルート マップの **match** 句を使用して、集約のより具体的な一部のルートを選択的に抑制し、他のルートを抑制しないでおくことができます。IP アクセス リストと自律システム パス アクセス リストの一致句がサポートされています。

advertise-map キーワードを使用すると、集約ルートの異なるコンポーネント（AS_SET やコミュニティなど）を構築するために使用する特定のルートが選択されます。集約のコンポーネントが別々の自律システムにあり、AS_SET で集約を作成して同じ自律システムの一部にアドバタイズしたい場合、**aggregate-address** コマンドのこの形式が役立ちます。AS_SET から特定の自律システム番号を省略し、集約が受信ルータの BGP ループ検出メカニズムによってドロップされるのを防ぐことを忘れてはなりません。IP アクセス リストと自律システム パス アクセス リストの **match** 句がサポートされています。

attribute-map キーワードを使用すると、集約ルートの属性を変更できます。AS_SET を構成するルートの 1 つが community no-export 属性（集約ルートがエクスポートされるのを防ぐ）などの属性で設定されている場合、**aggregate-address** コマンドのこの形式が役立ちます。属性マップ ルート マップを作成し、集約の属性を変更することができます。

例

次に、集約ルートを作成し、すべてのネイバーへのより具体的なルートのアドバタイズメントを抑制する例を示します。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router)# aggregate-address 10.0.0.0 255.0.0.0 summary-only
```

関連コマンド

コマンド	説明
address-family ipv4	アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 を使用するルーティング セッションを設定します。

alarm contact description

ISA 3000 でアラーム入力の説明を入力するには、グローバル コンフィギュレーション モードで **alarm contact description** コマンドを使用します。デフォルトの説明を対応するコンタクト番号に設定するには、このコマンドの no 形式を使用します。

alarm contact {**1** | **2**} **description** *string*

no alarm contact {**1** | **2**} **description**

構文の説明

1	**2** 説明が設定されているアラーム コンタクトを指定します。1 または 2 を入力します。
string	説明を指定します。説明には最大 80 文字の英数字を使用でき、syslog メッセージに含められます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

例

次に、アラーム コンタクト 1 の説明を指定する例を示します。

```
ciscoasa(config)# alarm contact 1 description Door Open
```

関連コマンド

コマンド	説明
alarm contact severity	ISA 3000 の LED 状態に順に影響を与えるアラームの重大度を指定します。
alarm contact trigger	1 つまたはすべてのアラーム入力のトリガーを指定します。

コマンド	説明
alarm facility input-alarm	アラーム入力のロギング オプションと通知オプションを指定します。
alarm facility power-supply rps	電源アラームを設定します。
alarm facility temperature	温度アラームを設定します。
alarm facility temperature（上限および下限のしきい値）	温度しきい値の下限または上限を設定します。
show alarm settings	すべてのグローバル アラーム設定を表示します。
show environment alarm-contact	すべての外部アラーム設定を表示します。
show facility-alarm relay	アクティブ化された状態のリレーを表示します。
show facility-alarm status	トリガーされたすべてのアラームを表示するか、または指定された重大度に基づいてアラームを表示します。
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。

alarm contact severity

ISA 3000 でアラームの重大度を指定するには、グローバル コンフィギュレーション モードで **alarm contact severity** コマンドを使用します。デフォルトの重大度に戻すには、このコマンドの **no** 形式を使用します。

alarm contact {**1** | **2** | **all**} **severity** {**major** | **minor** | **none**}

no alarm contact {**1** | **2** | **all**} **severity**

構文の説明

{**1** | **2** | **all**}	重大度を設定するアラーム コンタクトを指定します。1、2、または all を入力します。
severity {**major** | **minor** | **none**}	このアラーム コンタクトによってトリガーされたアラームの重大度。この重大度でアラームをラベル付けするほか、この重大度により、コンタクトに関連付けられた LED の動作が制御されます。 • **major**：LED が赤色で点滅します。 • **minor**：LED が赤色で点灯します。これはデフォルトです。 • **none**：LED が消灯します。

コマンド デフォルト

デフォルトでは、重大度はマイナーになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

例

次に、アラーム コンタクト 1 の重大度を指定する例を示します。

```
ciscoasa(config)# alarm contact 1 severity major
```

関連コマンド

コマンド	説明
alarm contact description	アラーム入力の説明を指定します。
alarm contact trigger	1 つまたはすべてのアラーム入力のトリガーを指定します。
alarm facility input-alarm	アラーム入力のロギング オプションと通知オプションを指定します。
alarm facility power-supply rps	電源アラームを設定します。
alarm facility temperature	温度アラームを設定します。
alarm facility temperature（上限および下限のしきい値）	温度しきい値の下限または上限を設定します。
show alarm settings	すべてのグローバル アラーム設定を表示します。
show environment alarm-contact	すべての外部アラーム設定を表示します。
show facility-alarm relay	アクティブ化された状態のリレーを表示します。
show facility-alarm status	トリガーされたすべてのアラームを表示するか、または指定された重大度に基づいてアラームを表示します。
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。

alarm contact trigger

ISA 3000 で 1 つまたはすべてのアラーム入力にトリガーを指定するには、グローバル コンフィギュレーション モードで **alarm contact trigger** コマンドを使用します。デフォルトのトリガーに戻すには、このコマンドの **no** 形式を使用します。

alarm contact {**1** | **2** | **all**} **trigger** {**open** | **closed**}

alarm contact {**1** | **2** | **all**} **trigger**

構文の説明

{**1** | **2** | **all**}	トリガーを設定するアラーム コンタクトを指定します。1、2、または all を入力します。
trigger {**open** | **closed**}	トリガーは、アラート信号を発する電気条件を決定します。 • **open**: コンタクトの通常状態はクローズです。つまり、コンタクトに電流が流れています。コンタクトがオープンになる、つまり電流が停止するとアラートがトリガーされます。 • **closed**: コンタクトの通常状態はオープンです。つまり、コンタクトに電流は流れていません。コンタクトがクローズになる、つまり電流がコンタクトを流れ始めるとアラートがトリガーされます。これはデフォルトです。

コマンド デフォルト

デフォルトでは、クローズ状態がトリガーです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

例

次に、アラーム コンタクト 1 にトリガーを設定する例を示します。

```
ciscoasa(config)# alarm contact 1 trigger open
```

関連コマンド

コマンド	説明
alarm contact description	アラーム入力の説明を指定します。
alarm contact severity	アラームの重大度を指定します。
alarm facility input-alarm	アラーム入力のロギング オプションと通知オプションを指定します。
alarm facility power-supply rps	電源アラームを設定します。
alarm facility temperature	温度アラームを設定します。
alarm facility temperature（上限および下限のしきい値）	温度しきい値の下限または上限を設定します。
show alarm settings	すべてのグローバル アラーム設定を表示します。
show environment alarm-contact	すべての外部アラーム設定を表示します。
show facility-alarm relay	アクティブ化された状態のリレーを表示します。
show facility-alarm status	トリガーされたすべてのアラームを表示するか、または指定された重大度に基づいてアラームを表示します。
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。

alarm facility input-alarm

ISA 3000 でアラーム入力のロギングおよび通知オプションを指定するには、グローバル コンフィギュレーション モードで **alarm facility input-alarm** コマンドを使用します。ロギングおよび通知オプションを削除するには、このコマンドの **no** 形式を使用します。

alarm facility input-alarm {**1** | **2**} {**notifies** | **relay** | **syslog**}

no alarm facility input-alarm {**1** | **2**} {**notifies** | **relay** | **syslog**}

構文の説明

{**1** | **2**}	アラーム コンタクト(1 または 2)を指定します。
notifies	アラームがトリガーされたときに SNMP トラップの送信を有効にします。
relay	アラームがトリガーされたときにハードウェア出力リレーを有効にします。これにより、接続されている外部アラームがアクティブになります。
syslog	アラームがトリガーされたとき、およびアラーム条件が終了したときに syslog メッセージの送信を有効にします。

コマンド デフォルト

デフォルトでは、syslog は有効になっていますが、その他のオプションは無効になっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

例

次に、アラーム入力 1 にロギングおよび通知オプションを指定する例を示します。

```
ciscoasa(config)# alarm facility input-alarm 1 notifies
ciscoasa(config)# alarm facility input-alarm 1 relay
ciscoasa(config)# alarm facility input-alarm 1 syslog
```

関連コマンド

コマンド	説明
alarm contact description	アラーム入力の説明を指定します。
alarm contact severity	アラームの重大度を指定します。
alarm contact trigger	1 つまたはすべてのアラーム入力のトリガーを指定します。
alarm facility power-supply rps	電源アラームを設定します。
alarm facility temperature	温度アラームを設定します。
alarm facility temperature（上限および下限のしきい値）	温度しきい値の下限または上限を設定します。
show alarm settings	すべてのグローバル アラーム設定を表示します。
show environment alarm-contact	すべての外部アラーム設定を表示します。
show facility-alarm relay	アクティブ化された状態のリレーを表示します。
show facility-alarm status	トリガーされたすべてのアラームを表示するか、または指定された重大度に基づいてアラームを表示します。
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。

alarm facility power-supply rps

ISA 3000 で電源アラームを設定するには、グローバル コンフィギュレーション モードで **alarm facility power-supply rps** コマンドを使用します。電源アラーム、リレー、SNMP トラップおよび syslog を無効にするには、**alarm facility power-supply rps disable** コマンドまたは **no** バージョンを使用します。

alarm facility power-supply rps {**disable** | **notifies** | **relay** | **syslog**}

no alarm facility power-supply rps {**disable** | **notifies** | **relay** | **syslog**}

構文の説明

disable	電源アラーム、リレー、SNMP トラップおよび syslog を無効にします。
notifies	アラームがトリガーされたときに SNMP トラップの送信を有効にします。
relay	アラームがトリガーされたときにハードウェア出力リレーを有効にします。これにより、接続されている外部アラームがアクティブになります。
syslog	アラームがトリガーされたとき、およびアラーム条件が終了したときに syslog メッセージの送信を有効にします。

コマンド デフォルト

デフォルトでは、**syslog** が有効で、**リレー**および**通知**は無効になっています。このアラームは、デフォルトで有効になっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

ISA 3000 には、電源装置が 2 台搭載されています。デフォルトでは、システムはシングル電源モードで稼働しています。ただし、デュアルモードでシステムを稼働するよう設定できます。その場合、プライマリ電源が故障すると 2 つ目の電源が自動的に電力を供給します。デュアル モードを有効にすると、電源アラームが自動的に有効になって syslog アラートが送信されますが、アラートを無効にしたり、SNMP トラップまたはアラーム ハードウェア リレーを有効にすることもできます。

alarm facility power-supply rps disable コマンドを使用すると、電源アラーム、リレー、トラップおよび syslog が無効になります。**no alarm facility power-supply rps disable** コマンドを使用すると、電源アラームのみが有効になります。リレー、SNMP トラップ、および syslog を個別に有効にする必要があります。

また、デュアル モードを有効にするには、**power-supply dual** コマンドも設定する必要があります。このアラームは、デュアル モードで自動的に有効になります。

例

次に、デュアル電源モードを有効にし、すべてのアラート オプションを設定する例を示します。

```
ciscoasa(config)# power-supply dual
ciscoasa(config)# alarm facility power-supply rps relay
ciscoasa(config)# alarm facility power-supply rps syslog
ciscoasa(config)# alarm facility power-supply rps notifies
```

次に、デュアル電源アラームを無効にする例を示します。

```
ciscoasa(config)# alarm facility power-supply rps disable
```

関連コマンド

コマンド	説明
alarm contact description	アラーム入力の説明を指定します。
alarm contact severity	アラームの重大度を指定します。
alarm contact trigger	1 つまたはすべてのアラーム入力のトリガーを指定します。
alarm facility input-alarm	アラーム入力のロギング オプションと通知オプションを指定します。
alarm facility temperature	温度アラームを設定します。
alarm facility temperature（上限および下限のしきい値）	温度しきい値の下限または上限を設定します。
show alarm settings	すべてのグローバル アラーム設定を表示します。
show environment alarm-contact	すべての外部アラーム設定を表示します。
show facility-alarm relay	アクティブ化された状態のリレーを表示します。
show facility-alarm status	トリガーされたすべてのアラームを表示するか、または指定された重大度に基づいてアラームを表示します。
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。

alarm facility temperature（アクション）

ISA 3000 で温度アラームを設定するには、グローバル コンフィギュレーション モードで **alarm facility temperature** コマンドを使用します。温度アラームを無効にするには、このコマンドの **no** 形式を使用します。

alarm facility temperature {**primary** | **secondary**} {**notifies** | **relay** | **syslog**}

no alarm facility temperature {**primary** | **secondary**} {**notifies** | **relay** | **syslog**}

構文の説明

primary	プライマリ温度アラームを設定します。
secondary	セカンダリ温度アラームを設定します。
notifies	アラームがトリガーされたときに SNMP トラップの送信を有効にします。
relay	アラームがトリガーされたときにハードウェア出力リレーを有効にします。これにより、接続されている外部アラームがアクティブになります。
syslog	アラームがトリガーされたとき、およびアラーム条件が終了したときに syslog メッセージの送信を有効にします。

コマンド デフォルト

プライマリ温度アラームは、すべてのアラーム アクションに対して有効になっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

デバイスの CPU カードの温度に基づいてアラームを設定できます。

alarm facility temperature コマンドで **high** および **low** キーワードを使用して、プライマリとセカンダリの温度範囲を設定できます。温度が下限しきい値以下になるか上限しきい値以上になると、アラームがトリガーされます。

プライマリ温度アラームは、すべてのアラームアクション（出力リレー、syslog、および SNMP）についてデフォルトで有効になっています。プライマリ温度範囲のデフォルト設定値は -40 °C ～ 92 °C です。

セカンダリ温度アラームはデフォルトでディセーブルになっています。セカンダリ温度は、-35 °C ～ 85 °C の範囲で設定できます。

セカンダリ温度範囲はプライマリ範囲よりも制限されているため、セカンダリの低温または高温のいずれかを設定すると、プライマリ設定にデフォルト以外の値を設定していたとしても、対応するプライマリ設定はこの設定によって無効になります。2 つの異なる高温アラームと 2 つの異なる低温アラームを有効にすることはできません。

したがって、実際には、プライマリのみまたはセカンダリのみの高温値および低温値を設定する必要があります。

例

次の例では、セカンダリ アラームの高温値および低温値を設定し、すべてのアラート アクションを有効にしています。

```
ciscoasa(config)# alarm facility temperature secondary low -20
ciscoasa(config)# alarm facility temperature secondary high 80
ciscoasa(config)# alarm facility temperature secondary notifies
ciscoasa(config)# alarm facility temperature secondary relay
ciscoasa(config)# alarm facility temperature secondary syslog
```

関連コマンド

コマンド	説明
alarm contact description	アラーム入力の説明を指定します。
alarm contact severity	アラームの重大度を指定します。
alarm contact trigger	1 つまたはすべてのアラーム入力のトリガーを指定します。
alarm facility input-alarm	アラーム入力のロギング オプションと通知オプションを指定します。
alarm facility power-supply rps	電源アラームを設定します。
alarm facility temperature（上限および下限のしきい値）	温度しきい値の下限または上限を設定します。
show alarm settings	すべてのグローバル アラーム設定を表示します。
show environment alarm-contact	すべての外部アラーム設定を表示します。
show facility-alarm relay	アクティブ化された状態のリレーを表示します。
show facility-alarm status	トリガーされたすべてのアラームを表示するか、または指定された重大度に基づいてアラームを表示します。
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。

alarm facility temperature（上限および下限しきい値）

ISA 3000 で上限および下限の温度しきい値を設定するには、グローバル コンフィギュレーション モードで **alarm facility temperature** {**low** | **high**} コマンドを使用します。しきい値を削除するか、プライマリの値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

alarm facility temperature {**primary** | **secondary**} {**high** | **low**} *threshold*

no alarm facility temperature {**primary** | **secondary**} {**high** | **low**} *threshold*

構文の説明

primary	プライマリ温度アラームを設定します。
secondary	セカンダリ温度アラームを設定します。
high *threshold*	上限しきい値を摂氏で設定します。プライマリの最大値は 92 です。セカンダリの最大値は 85 です。
low *threshold*	下限しきい値を摂氏で設定します。プライマリの最小値は -40 です。セカンダリの最小値は -35 です。

コマンド デフォルト

デフォルトのプライマリ高温値は 92 °C、低温値は -40 °C です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

デバイスの CPU カードの温度に基づいてアラームを設定できます。

alarm facility temperature コマンドで **high** および **low** キーワードを使用して、プライマリとセカンダリの温度範囲を設定できます。温度が下限しきい値以下になるか上限しきい値以上になると、アラームがトリガーされます。

プライマリ温度アラームは、すべてのアラームアクション（出力リレー、syslog、および SNMP）についてデフォルトで有効になっています。プライマリ温度範囲のデフォルト設定値は -40 °C ～ 92 °C です。

セカンダリ温度アラームはデフォルトでディセーブルになっています。セカンダリ温度は、-35 °C ～ 85 °C の範囲で設定できます。

セカンダリ温度範囲はプライマリ範囲よりも制限されているため、セカンダリの低温または高温のいずれかを設定すると、プライマリ設定にデフォルト以外の値を設定していたとしても、対応するプライマリ設定はこの設定によって無効になります。2 つの異なる高温アラームと 2 つの異なる低温アラームを有効にすることはできません。

したがって、実際には、プライマリのみまたはセカンダリのみの高温値および低温値を設定する必要があります。

例

次の例では、セカンダリ アラームの高温値および低温値を設定し、すべてのアラート アクションを有効にしています。

```
ciscoasa(config)# alarm facility temperature secondary low -20
ciscoasa(config)# alarm facility temperature secondary high 80
ciscoasa(config)# alarm facility temperature secondary notifies
ciscoasa(config)# alarm facility temperature secondary relay
ciscoasa(config)# alarm facility temperature secondary syslog
```

関連コマンド

コマンド	説明
alarm contact description	アラーム入力の説明を指定します。
alarm contact severity	アラームの重大度を指定します。
alarm contact trigger	1 つまたはすべてのアラーム入力のトリガーを指定します。
alarm facility input-alarm	アラーム入力のロギング オプションと通知オプションを指定します。
alarm facility power-supply rps	電源アラームを設定します。
alarm facility temperature	温度アラームを設定します。
show alarm settings	すべてのグローバル アラーム設定を表示します。
show environment alarm-contact	すべての外部アラーム設定を表示します。
show facility-alarm relay	アクティブ化された状態のリレーを表示します。
show facility-alarm status	トリガーされたすべてのアラームを表示するか、または指定された重大度に基づいてアラームを表示します。
clear facility-alarm output	出力リレーの電源を切り、LED のアラーム状態をクリアします。

allocate-interface

インターフェイスをセキュリティ コンテキストに割り当てるには、コンテキスト コンフィギュレーション モードで **allocate-interface** コマンドを使用します。インターフェイスをコンテキストから削除するには、このコマンドの **no** 形式を使用します。

allocate-interface *physical_interface* [*map_name*] [**visible** | **invisible**]

no allocate-interface *physical_interface*

allocate-interface *physical_interface*.*subinterface*[-*physical_interface*.*subinterface*] [*map_name*[-*map_name*]] [**visible** | **invisible**]

no allocate-interface *physical_interface*.*subinterface*[-*physical_interface*.*subinterface*]

構文の説明

invisible	（デフォルト）コンテキスト ユーザが **show interface** コマンドでマッピング名（設定されている場合）だけを表示できるようにします。
map_name	（任意）マッピング名を設定します。 *map_name* は、インターフェイス ID の代わりにコンテキスト内で使用できるインターフェイスの英数字のエイリアスです。マッピング名を指定しない場合、インターフェイス ID がコンテキスト内で使用されます。セキュリティのために、コンテキストで使用されているインターフェイスをコンテキスト管理者に知らせない場合があります。 マッピング名はアルファベットで始まり、アルファベットまたは数字で終わる必要があります。その間の文字には、アルファベット、数字、または下線のみを使用できます。たとえば、次の名前を使用できます。 **int0** **inta** **int_0** サブインターフェイスの場合は、マッピング名の範囲を指定できます。 範囲の詳細については、「使用上のガイドライン」を参照してください。
physical_interface	**gigabitethernet0/1** などのインターフェイス ID を設定します。有効値については、**interface** コマンドを参照してください。インターフェイス タイプとポート番号の間にスペースを含めないでください。
subinterface	サブインターフェイス番号を設定します。サブインターフェイスの範囲を指定できます。
visible	（任意）マッピング名を設定した場合でも、コンテキスト ユーザが **show interface** コマンドで物理インターフェイスのプロパティを表示できるようにします。

デフォルト

マッピング名を設定した場合、デフォルトでは、**show interface** コマンドの出力にインターフェイス ID は表示されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
コンテキスト コンフィギュレーション	• 対応	• 対応	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを複数回入力して、異なる範囲を指定できます。マッピング名または表示設定を変更するには、特定のインターフェイス ID に対してコマンドを再入力し、新しい値を設定します。**no allocate-interface** コマンドを入力して最初からやり直す必要はありません。**allocate-interface** コマンドを削除すると、ASA によって、コンテキスト内のインターフェイス関連のコンフィギュレーションがすべて削除されます。

トランスペアレント ファイアウォール モードでは、2 つのインターフェイスのみがトラフィックを通過させることができます。ただし、ASA では、専用の管理インターフェイス Management 0/0（物理インターフェイスまたはサブインターフェイス）を管理トラフィック用の第 3 のインターフェイスとして使用できます。

（注） トランスペアレント モードの管理インターフェイスは、MAC アドレス テーブルにないパケットをインターフェイスにフラッディングしません。

ルーテッド モードでは、必要に応じて同じインターフェイスを複数のコンテキストに割り当てることができます。トランスペアレント モードでは、インターフェイスを共有できません。

サブインターフェイスの範囲を指定する場合は、マッピング名の一致範囲を指定できます。範囲については、次のガイドラインに従ってください。

- マッピング名は、アルファベット部分と、それに続く数値部分で構成する必要があります。マッピング名のアルファベット部分は、範囲の両端で一致している必要があります。たとえば、次のような範囲を入力します。

  ```
  int0-int10
  ```

  たとえば、**gigabitethernet0/1.1-gigabitethernet0/1.5 happy1-sad5** と入力した場合、コマンドは失敗します。

- マッピング名の数値部分には、サブインターフェイスの範囲と同じ個数の数値を含める必要があります。たとえば、次の例では、両方の範囲に 100 個のインターフェイスが含まれています。

  ```
  gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100
  ```

  たとえば、**gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int15** と入力した場合、コマンドは失敗します。

例

次に、gigabitethernet0/1.100、gigabitethernet0/1.200、および gigabitethernet0/2.300 ～ gigabitethernet0/1.305 をコンテキストに割り当てる例を示します。マッピング名は、int1 ～ int8 です。

```
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet0/2.305
int3-int8
```

関連コマンド

コマンド	説明
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show context	コンテキストのリスト(システム実行スペース)または現在のコンテキストに関する情報を表示します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。
vlan	サブインターフェイスに VLAN ID を割り当てます。

allocate-ips

IPS 仮想センサーをセキュリティ コンテキストに割り当てるには、AIP SSM がインストールされている場合には、コンテキスト コンフィギュレーション モードで **allocate-ips** コマンドを使用します。仮想センサーをコンテキストから削除するには、このコマンドの **no** 形式を使用します。

allocate-ips *sensor_name* [*mapped_name*] [**default**]

no allocate-ips *sensor_name* [*mapped_name*] [**default**]

構文の説明

default	(任意) コンテキストごとに 1 つのセンサーをデフォルト センサーとして設定します。コンテキスト コンフィギュレーションでセンサー名が指定されていない場合は、コンテキストでこのデフォルト センサーが使用されます。コンテキストごとに設定できるデフォルト センサーは 1 つのみです。デフォルト センサーを変更する場合は、**no allocate-ips** コマンドを入力して現在のデフォルト センサーを削除してから、新しいデフォルト センサーを割り当てます。センサーをデフォルトとして指定せず、コンテキスト コンフィギュレーションにセンサー名が含まれていない場合、トラフィックは AIP SSM のデフォルト センサーを使用します。
mapped_name	(任意) コンテキスト内で実際のセンサー名の代わりに使用できるセンサー名のエイリアスとして、マッピング名を設定します。マッピング名を指定しない場合、センサー名がコンテキスト内で使用されます。セキュリティのために、コンテキストで使用されているセンサーをコンテキスト管理者に知らせない場合があります。または、コンテキスト コンフィギュレーションを一般化する場合もあります。たとえば、すべてのコンテキストで「sensor1」および「sensor2」というセンサーを使用する場合、コンテキスト A の sensor1 と sensor2 に「highsec」センサーと「lowsec」センサーをマッピングし、コンテキスト B の sensor1 と sensor2 に「medsec」センサーと「lowsec」センサーをマッピングできます。
sensor_name	AIP SSM に設定されているセンサー名を設定します。AIP SSM に設定されているセンサーを表示するには、**allocate-ips ?** と入力します。使用可能なすべてのセンサーが表示されます。**show ips** コマンドを入力することもできます。システム実行スペースで **show ips** コマンドを入力すると、使用可能なすべてのセンサーが表示されます。このコマンドをコンテキストで入力すると、そのコンテキストにすでに割り当てられているセンサーが表示されます。AIP SSM にまだ存在しないセンサー名を指定した場合は、エラーが表示されますが、**allocate-ips** コマンドはそのまま入力されます。AIP SSM にその名前のセンサーが作成されるまで、コンテキストはそのセンサーがダウンしていると見なします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
コンテキスト コンフィギュレーション	• 対応	• 対応	—	—	•

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

各コンテキストに 1 つ以上の IPS 仮想センサーを割り当てることができます。その後、**ips** コマンドを使用して AIP SSM にトラフィックを送信するようにコンテキストを設定するときに、コンテキストに割り当てられているセンサーを指定できます。コンテキストに割り当てられていないセンサーは指定できません。コンテキストにセンサーが割り当てられていない場合は、AIP SSM に設定されているデフォルト センサーが使用されます。同じセンサーを複数のコンテキストに割り当てることができます。

(注) 仮想センサーを使用するためにマルチ コンテキスト モードを開始する必要はありません。シングル モードでトラフィック フローごとに異なるセンサーを使用できます。

例

次に、sensor1 と sensor2 をコンテキスト A に、sensor1 と sensor3 をコンテキスト B に割り当てる例を示します。どちらのコンテキストもセンサー名を「ips1」と「ips2」にマップします。コンテキスト A では sensor1 をデフォルト センサーとして設定しますが、コンテキスト B ではデフォルトを設定しないため、AIP SSM に設定されているデフォルトが使用されます。

```
ciscoasa(config-ctx)# context A
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# allocate-ips sensor1 ips1 default
ciscoasa(config-ctx)# allocate-ips sensor2 ips2
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold

ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# allocate-ips sensor1 ips1
ciscoasa(config-ctx)# allocate-ips sensor3 ips2
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member silver
```

関連コマンド

コマンド	説明
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。
ips	トラフィックをインスペクションのために AIP SSM に転送します。
show context	コンテキストのリスト(システム実行スペース)または現在のコンテキストに関する情報を表示します。
show ips	AIP SSM に設定されている仮想センサーを表示します。

allowed-eid

IP アドレスに基づいて検査対象 EID を制限するための LISP インスペクション マップを設定するには、パラメータ コンフィギュレーション モードで **allowed-eid** コマンドを使用します。パラメータ コンフィギュレーション モードにアクセスするには、まず **policy-map type inspect lisp** コマンドを入力します。すべての EID を許可するには、このコマンドの **no** 形式を使用します。

allowed-eid access-list *eid_acl_name*

no allowed-eid access-list *eid_acl_name*

構文の説明

access-list *eid_acl_name*	宛先 IP アドレスのみが EID 組み込みアドレスと照合される拡張 ACL を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

IP アドレスに基づいて検査対象 EID を制限するための LISP インスペクション マップを設定します。

クラスタ フロー モビリティの LISP インスペクションについて

ASA は、場所の変更について LISP トラフィックを検査し、シームレスなクラスタリング操作のためにこの情報を使用します。LISP の統合により、ASA クラスタ メンバーは、最初のホップ ルータと ETR または ITR との間で渡される LISP トラフィックを検査し、その後、フローの所有者を新しいサイトへ変更できます。

クラスタ フロー モビリティには複数の相互に関連する設定が含まれています。

1. (オプション)ホストまたはサーバの IP アドレスに基づく検査される EID の限定:最初のホップ ルータは、ASA クラスタが関与していないホストまたはネットワークに関する EID 通知メッセージを送信することがあるため、EID をクラスタに関連するサーバまたはネットワークのみに限定することができます。たとえば、クラスタが 2 つのサイトのみに関連しているが、LISP は 3 つのサイトで稼働している場合は、クラスタに関連する 2 つのサイトの EID のみを含めます。**policy-map type inspect lisp**、**allowed-eid** および **validate-key** コマンドを参照してください。
2. LISP トラフィックのインスペクション:ASA は、最初のホップ ルータと ITR または ETR 間で送信された EID 通知メッセージに関して LISP トラフィックを検査します。ASA は EID とサイト ID を相関付ける EID テーブルを維持します。たとえば、最初のホップ ルータの送信元 IP アドレスと ITR または ETR の宛先アドレスをもつ LISP トラフィックを検査する必要があります。**inspect lisp** コマンドを参照してください。
3. 指定されたトラフィックでのフロー モビリティを有効にするサービス ポリシー:ビジネスクリティカルなトラフィックでフロー モビリティを有効にする必要があります。たとえば、フロー モビリティを、HTTPS トラフィックのみに制限したり、特定のサーバとの間でやり取りされるトラフィックのみに制限したりできます。**cluster flow-mobility lisp** コマンドを参照してください。
4. サイト ID:ASA は各クラスタ ユニットのサイト ID を使用して、新しい所有者を判別します。**site-id** コマンドを参照してください。
5. フロー モビリティを有効にするクラスタレベルの設定:クラスタ レベルでもフロー モビリティを有効にする必要があります。このオン/オフの切り替えを使用することで、特定のクラスのトラフィックまたはアプリケーションに対してフロー モビリティを簡単に有効または無効にできます。**flow-mobility lisp** コマンドを参照してください。

例

次に、EID を 10.10.10.0/24 ネットワーク上の EID に制限する例を示します。

```
ciscoasa(config)# access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0
255.255.255.0
ciscoasa(config)# policy-map type inspect lisp LISP_EID_INSPECT
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# allowed-eid access-list TRACKED_EID_LISP
ciscoasa(config-pmap-p)# validate-key MadMaxShinyandChrome
```

関連コマンド

コマンド	説明
clear cluster info flow-mobility counters	フロー モビリティ カウンタをクリアします。
clear lisp eid	ASA EID テーブルから EID を削除します。
cluster flow-mobility lisp	サービス ポリシーのフロー モビリティを有効にします。
flow-mobility lisp	クラスタのフロー モビリティを有効にします。
inspect lisp	LISP トラフィックを検査します。
policy-map type inspect lisp	LISP 検査をカスタマイズします。
site-id	クラスタ シャーシのサイト ID を設定します。

コマンド	説明
show asp table classify domain inspect-lisp	LISP 検査用の ASP テーブルを表示します。
show cluster info flow-mobility counters	フロー モビリティ カウンタを表示します。
show conn	LISP フロー モビリティの対象となるトラフィックを表示します。
show lisp eid	ASA EID テーブルを表示します。
show service-policy	サービス ポリシーを表示します。
validate-key	LISP メッセージを検証するための事前共有キーを入力します。

allow-ssc-mgmt

ASA 5505 のインターフェイスを SSC 管理インターフェイスとして設定するには、インターフェイス コンフィギュレーション モードで **allow-ssc-mgmt** コマンドを使用します。インターフェイスの割り当てを解除するには、このコマンドの **no** 形式を使用します。

allow-ssc-mgmt

no allow-ssc-mgmt

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

このコマンドは、VLAN 1 用の出荷時のデフォルトのコンフィギュレーションでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

SSC に外部インターフェイスはありません。管理 VLAN として VLAN を設定し、バックプレーン経由での内部 IP 管理アドレスへのアクセスを許可できます。デフォルトでは、VLAN 1 は SSC 管理アドレスでイネーブルになります。SSC 管理 VLAN として割り当てることができるのは 1 つの VLAN だけです。

ASDM を使用してアクセスする場合は、管理アドレス用に NAT を設定しないでください。ASDM の初期セットアップでは、実際のアドレスにアクセスする必要があります。初期セットアップ後（SSC でパスワードを設定した後）は、NAT を設定し、SSC にアクセスするときの変換アドレスを ASDM に提供できます。

例

次に、管理アクセスを VLAN 1 でディセーブルにし、VLAN 2 でイネーブルにする例を示します。

```
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# no allow-ssc-mgmt
ciscoasa(config-if)# interface vlan 2
ciscoasa(config-if)# allow-ssc-mgmt
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定します。
ip address	ブリッジ グループの管理 IP アドレスを設定します。
nameif	インターフェイス名を設定します。
security-level	インターフェイスのセキュリティ レベルを設定します。
hw-module module ip	SSC の管理 IP アドレスを設定します。
hw-module module allow-ip	管理 IP アドレスにアクセスできるホストを設定します。

allow-tls

TLS セッションを許可または禁止するように ESMTP インスペクションを設定するには、パラメータ コンフィギュレーション モードで **allow-tls** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

allow-tls [**action log**]

no allow-tls

構文の説明

action log	暗号化された接続をログに記録するかどうか。

コマンド デフォルト

allow-tls コマンドが ESMTP インスペクションのデフォルトです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(3)	このコマンドが追加されました。
9.4(1)	デフォルトが **no allow-tls** から **allow-tls** に変更されました。ただし、このデフォルトは新しい、または再イメージングされたシステムに適用されます。**no allow-tls** を含むシステムをアップグレードする場合は、このコマンドは変更されません。

使用上のガイドライン

ESMTP インスペクションでは、暗号化された接続を検査できません。すべての ESMTP セッションの検査を強制するには、**no allow-tls** コマンドを使用します。TLS を無効にすると、STARTTLS インジケータが接続要求から削除され、強制的にクライアントとサーバがクリア テキスト接続をネゴシエートします。

クライアントとサーバが暗号化された接続をネゴシエートできるようにする場合は、ESMTP インスペクション ポリシー マップのパラメータ セクションに **allow-tls** コマンドを含め、マップを ESMTP インスペクション サービス ポリシーに接続します。また、_default_esmtp_map（これは独自のマップを適用しない場合に適用されます）を編集することもできます。

例

次に、ESMTP インスペクションをバイパスする暗号化された ESMTP セッションを許可する方法の例を示します。

```
ciscoasa(config)# policy-map type inspect esmtp esmtp_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# allow-tls
```

関連コマンド

コマンド	説明
policy-map type inspect esmtp	インスペクションの ESMTP ポリシー マップを設定します。

always-on-vpn

AnyConnect Always-On-VPN 機能の動作を設定するには、グループ ポリシー コンフィギュレーション モードで **always-on-vpn** コマンドを使用します。

always-on-vpn [**profile-setting** | **disable**]

構文の説明

disable	Always-On-VPN 機能をオフにします。
profile-setting	AnyConnect プロファイルに設定された **always-on-vpn** 設定を使用します。

コマンド デフォルト

Always-On-VPN 機能は、デフォルトでオンになっています。

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

使用上のガイドライン

AnyConnect ユーザのために Always-On-VPN 機能をイネーブルにするには、プロファイル エディタで AnyConnect プロファイルを設定します。次に、適切なポリシーのグループ ポリシー属性を設定します。

例

次の例では、設定されたグループ ポリシーに対して Always-On 機能を有効にしています。

```
ciscoasa(config)# group-policy <group policy> attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# always-on-vpn profile-setting
```

関連コマンド

コマンド	説明
webvpn	WebVPN のグループ ポリシーを設定します。

anti-replay

GTP-U メッセージ シーケンス番号のアンチリプレイを有効にするには、GTP インスペクション ポリシー マップのパラメータ コンフィギュレーション モードで **anti-replay** コマンドを使用します。アンチリプレイを無効にするには、このコマンドの **no** 形式を使用します。

anti-replay [*window_size*]

no anti-replay [*window_size*]

構文の説明

window_size	スライディング ウィンドウのサイズはメッセージの数です。ウィンドウのサイズは、128、256、512、または 1024 になります。値を入力しない場合は、デフォルトの 512 になります。

デフォルト

デフォルトでは、アンチリプレイは無効になっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション モード	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.10(1)	このコマンドが導入されました。

使用上のガイドライン

GTP-U メッセージのスライディング ウィンドウを指定することによって、アンチリプレイを有効にできます。

スライディング ウィンドウのサイズはメッセージの数であり、128、256、512、または 1024 になります。有効なメッセージが表示されると、ウィンドウは新しいシーケンス番号に移行します。シーケンス番号は 0 ～ 65535 の範囲であり、最大値に達するとラッピングされます。また、これらは PDP コンテキストごとに一意です。メッセージは、シーケンス番号がウィンドウ内であれば有効と見なされます。

アンチリプレイは、ハッカーが GTP データ パケットをキャプチャし、それらをリプレイするときに発生する可能性があるセッション ハイジャックや DoS 攻撃を防ぐのに役立ちます。

例

次の例では、ウィンドウ サイズ 512 のアンチリプレイを有効にしています。

```
ciscoasa(config)# policy-map type inspect gtp gtp-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# anti-replay 512
```

関連コマンド

コマンド	説明
inspect gtp	GTP アプリケーション インスペクションをイネーブルにします。
policy-map type inspect gtp	GTP インスペクション ポリシー マップを作成または編集します。
show service-policy inspect gtp	GTP 設定および統計情報を表示します。

anyconnect ask

ASA がリモート SSL VPN クライアント ユーザに対してクライアントのダウンロードを要求するには、グループ ポリシー webvpn またはユーザ名 webvpn コンフィギュレーション モードで **anyconnect ask** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

anyconnect ask {**none** | **enable** [**default** {**webvpn** | **anyconnect**} **timeout** *value*]}

no anyconnect ask none [**default** {**webvpn** | **anyconnect**}]

構文の説明

default anyconnect timeout *value*	リモート ユーザにクライアントのダウンロードを要求するか、クライアントレス接続のポータル ページに移動して、*value* の時間待機してから、デフォルト アクション(クライアントのダウンロード)を実行します。
default webvpn timeout *value*	リモート ユーザにクライアントのダウンロードを要求するか、クライアントレス接続のポータル ページに移動して、*value* の時間待機してから、デフォルト アクション(WebVPN ポータル ページの表示)を実行します。
enable	リモート ユーザにクライアントのダウンロードを要求するか、クライアントレス接続のポータル ページに移動してユーザ応答を無期限に待機します。
none	デフォルト アクションをただちに実行します。

デフォルト

このコマンドのデフォルトは、**anyconnect ask none default webvpn** です。ASA によって、クライアントレス接続のポータル ページがただちに表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

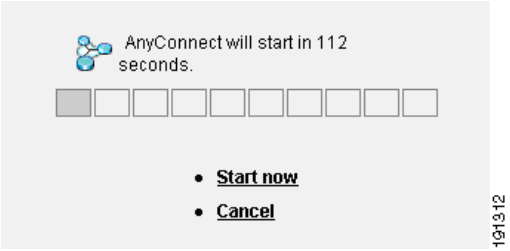
コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.4(1)	**svc ask** コマンドが **anyconnect ask** コマンドに置き換えられました。

使用上のガイドライン

図 2-1 に、**default anyconnect timeout** *value* コマンドまたは **default webvpn timeout** *value* コマンドが設定された場合にリモート ユーザに表示されるプロンプトを示します。

図 2-1　SSL VPN Client のダウンロードに関してリモート ユーザに表示されるプロンプト



例

次に、ASA を設定して、リモート ユーザにクライアントのダウンロードを要求するか、ポータル ページに移動して、ユーザの応答を 10 秒待機してからクライアントをダウンロードするように設定する例を示します。

```
ciscoasa(config-group-webvpn)# anyconnect ask enable default svc timeout 10
```

関連コマンド

コマンド	説明
show webvpn anyconnect	インストールされている SSL VPN クライアントに関する情報を表示します。
anyconnect	特定のグループまたはユーザに対して SSL VPN クライアントをイネーブルまたは必須にします。
anyconnect image	リモート PC へのダウンロードのために ASA がキャッシュ メモリで展開するクライアント パッケージ ファイルを指定します。

anyconnect-custom（バージョン 9.0 から 9.2 まで）

カスタム属性の値を設定または更新するには、AnyConnect カスタム属性コンフィギュレーション モードで **anyconnect-custom** コマンドを使用します。カスタム属性の値を削除するには、このコマンドの **no** 形式を使用します。

anyconnect-custom *attr-name* **value** *attr-value*

anyconnect-custom *attr-name* **none**

no anyconnect-custom *attr-name*

構文の説明

attr-name	**anyconnnect-custom-attr** コマンドで定義された、現在のグループ ポリシーでの属性の名前。
none	デフォルト アクションをただちに実行します。
value *attr-value*	属性値を含む文字列。値は、属性名に関連付けられ、接続の確立時にクライアントに渡されます。450 文字以内で指定します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
AnyConnect カスタム属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、グループ ポリシーにカスタム属性の値を設定します。『*AnyConnect Administrator's Guide*』に、そのリリースに適用されるカスタム属性の有効な値を示します。カスタム属性は、**anyconnect-custom-attr** コマンドで作成します。

属性のマルチライン値を作成するために、このコマンドの複数のインスタンスがサポートされています。特定の属性名に関連付けられたすべてのデータが、CLI で入力された順序に従ってクライアントに提供されます。マルチライン値の個別の行は削除できません。

このコマンドの **no** 形式では、**value** キーワードおよび **none** キーワードは使用できません。

属性名に関連付けられたデータを複数の CLI 行に入力した場合、そのデータは改行文字（\n）で区切られた単一の連結文字列としてエンドポイントに送信されます。

例

次に、AnyConnect 遅延アップデートのカスタム属性を設定する例を示します。

```
ciscoasa(config-group-policy)# anyconnect-custom DeferredUpdateAllowed true
```

関連コマンド

コマンド	説明
show run webvpn	**anyconnect** コマンドを含む、WebVPN に関するコンフィギュレーション情報を表示します。
show run group-policy	現在のグループ ポリシーに関する設定情報を表示します。
anyconnect-custom-attr	カスタム属性を作成します。

anyconnect-custom（バージョン 9.3 以降）

カスタム属性の値を設定または更新するには、グループ ポリシーまたはダイナミック アクセス ポリシー レコード コンフィギュレーション モードで **anyconnect-custom** コマンドを使用します。カスタム属性を削除するには、このコマンドの **no** 形式を使用します。

anyconnect-custom *attr-type* **value** *attr-name*

anyconnect-custom *attr-type* **none**

no anyconnect-custom *attr-type*

構文の説明

attr-type	**anyconnnect-custom-attr** コマンドで定義されたカスタム属性のタイプ。
none	このカスタム属性は、ポリシーから明示的に除外されます。
value *attr-name*	**anyconnect-custom-data** コマンドで定義されたカスタム属性値の名前。 カスタム属性のタイプと名前付き値は、接続の確立時にクライアントに渡されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシーまたはダイナミック アクセス ポリシー レコード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが再定義されました。

使用上のガイドライン

このコマンドは、グループ ポリシーまたは DAP にカスタム属性の値を設定します。

『*AnyConnect Administrator's Guide*』に、そのリリースに適用されるカスタム属性の有効な値を示します。カスタム属性は、**anyconnect-custom-attr** コマンドおよび **anyconnect-custom-data** コマンドで作成します。

このコマンドの **no** 形式では、**none** キーワードは使用できません。

例

次に、AnyConnect 遅延アップデートのカスタム属性を設定する例を示します。

```
ciscoasa(config-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed
ciscoasa(config-webvpn)# exit
ciscoasa(config)# anyconnect-custom-data DeferredUpdateAllowed def-allowed true
ciscoasa(config-group-policy)# anyconnect-custom DeferredUpdateAllowed def-allowed
```

関連コマンド

コマンド	説明
show run webvpn	**anyconnect** コマンドを含む、WebVPN に関するコンフィギュレーション情報を表示します。
show run group-policy	現在のグループ ポリシーに関する設定情報を表示します。
show running-config dynamic-access-policy-record	DAP ポリシーで使用されるカスタム属性を表示します。
anyconnect-custom-attr	このコマンドで使用されるカスタム属性のタイプを作成します。
anyconnect-custom-data	このコマンドで使用されるカスタム属性の名前付き値を作成します。

anyconnect-custom-attr（バージョン 9.0 から 9.2 まで）

カスタム属性を作成するには、AnyConnect カスタム属性コンフィギュレーション モードで **anyconnect-custom-attr** コマンドを使用します。カスタム属性を削除するには、このコマンドの **no** 形式を使用します。

[no] anyconnect-custom-attr *attr-name* **[description** *description***]**

構文の説明

attr-name	属性の名前。この名前は、グループ ポリシー構文および集約認証プロトコル メッセージで参照されます。最大長は 32 文字です。
description *description*	属性の使用方法の自由形式の説明。このテキストは、カスタム属性がグループ ポリシー属性コンフィギュレーション モードから参照された場合に、コマンド ヘルプで表示されます。最大長は 128 文字です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
AnyConnect カスタム属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、AnyConnect の特殊機能をサポートするカスタム属性を作成します。特定の機能に対してカスタム属性を作成した後、それらをグループ ポリシーに追加して、機能が VPN クライアントに適用されるようにします。このコマンドでは、定義されたすべての属性名が一意であることが保証されます。

一部のバージョンの AnyConnect では、機能の設定にカスタム属性が使用されます。各バージョンのリリース ノートおよび『*AnyConnect Administrator's Guide*』に、カスタム属性を必要とするすべての機能を示します。

グループ ポリシーで使用される属性の定義を削除しようとすると、エラー メッセージが表示され、操作は失敗します。ユーザが既存の属性をカスタム属性として追加しようとすると、説明への変更は組み込まれますが、それ以外についてはコマンドは無視されます。

属性のマルチライン値を作成するために、このコマンドの複数のインスタンスがサポートされています。特定の属性名に関連付けられたすべてのデータが、CLI で入力された順序に従ってクライアントに提供されます。マルチライン値の個別の行は削除できません。

例

次に、AnyConnect 遅延アップデートのカスタム属性を設定する例を示します。

```
ciscoasa(config-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed description
Indicates if the deferred update feature is enabled or not
```

関連コマンド

コマンド	説明
show run webvpn	**anyconnect** コマンドを含む、WebVPN に関するコンフィギュレーション情報を表示します。
show run group-policy	現在のグループ ポリシーに関する設定情報を表示します。
anyconnect-custom	カスタム属性のタイプおよび名前付き値をグループ ポリシーまたはダイナミック アクセス ポリシーに関連付けます。

anyconnect-custom-attr（バージョン 9.3 以降）

カスタム属性のタイプを作成するには、config-webvpn コンフィギュレーション モードで **anyconnect-custom-attr** コマンドを使用します。カスタム属性を削除するには、このコマンドの **no** 形式を使用します。

[no] anyconnect-custom-attr *attr-type* **[description** *description***]**

構文の説明

attr-type	属性のタイプ。このタイプは、グループ ポリシー構文、DAP ポリシー構文、および集約認証プロトコル メッセージで参照されます。最大長は 32 文字です。
description *description*	属性の使用方法の自由形式の説明。このテキストは、カスタム属性がグループ ポリシー属性コンフィギュレーション モードから参照された場合に、コマンド ヘルプで表示されます。最大長は文字です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
config-webvpn	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが再定義されました。

使用上のガイドライン

このコマンドは、AnyConnect の特殊機能をサポートするカスタム属性を作成します。特定の機能に対してカスタム属性を作成した後、その属性の値を定義し、その属性をグループ ポリシーに追加して、対応する機能が VPN クライアントに適用されるようにします。このコマンドでは、定義されたすべての属性名が一意であることが保証されます。

一部のバージョンの AnyConnect では、機能の設定にカスタム属性が使用されます。各バージョンのリリース ノートおよび『*AnyConnect Administrator's Guide*』に、カスタム属性を必要とするすべての機能を示します。

グループ ポリシーで使用される属性の定義を削除しようとすると、エラー メッセージが表示され、操作は失敗します。ユーザが既存の属性をカスタム属性として追加しようとすると、説明への変更は組み込まれますが、それ以外についてはコマンドは無視されます。

例

次に、AnyConnect 遅延アップデートのカスタム属性を設定する例を示します。

```
ciscoasa(config-webvpn)# anyconnect-custom-attr DeferredUpdateAllowed description
Indicates if the deferred update feature is enabled or not
ciscoasa(config)# anyconnect-custom-data DeferredUpdateAllowed def-allowed true
```

関連コマンド

コマンド	説明
show run webvpn	**anyconnect** コマンドを含む、WebVPN に関するコンフィギュレーション情報を表示します。
show run group-policy	現在のグループ ポリシーに関する設定情報を表示します。
show running-config dynamic-access-policy-record	DAP ポリシーで使用されるカスタム属性を表示します。
anyconnect-custom	ポリシーで使用するためのカスタム属性の値を設定します。
anyconnect-custom-data	カスタム属性の名前付き値を作成します。

anyconnect-custom-data

カスタム属性の名前付き値を作成するには、グローバル コンフィギュレーション モードで **anyconnect-custom-data** コマンドを使用します。カスタム属性を削除するには、このコマンドの **no** 形式を使用します。

anyconnect-custom-data *attr-type attr-name attr-value*

no anyconnect-custom-data *attr-type attr-name*

構文の説明

attr-type	**anyconnect-custom-attr** を使用して以前に定義された属性のタイプ。
attr-name	指定した値を持つ属性の名前。これは、グループ ポリシーおよびダイナミック アクセス ポリシー レコード コンフィギュレーション モードで参照できます。
attr-value	属性値を含む文字列。 最大 420 文字です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、AnyConnect の特殊機能をサポートするカスタム属性の名前付き値を定義します。特定の機能に対してカスタム属性を作成した後、その属性の値を定義し、その属性を DAP またはグループ ポリシーに追加して、対応する機能が VPN クライアントに適用されるようにします。

一部のバージョンの AnyConnect では、機能の設定にカスタム属性が使用されます。各バージョンのリリース ノートおよび『*AnyConnect Administrator's Guide*』に、カスタム属性を必要とするすべての機能を示します。

グループ ポリシーで使用される属性の名前付き値を削除しようとすると、エラー メッセージが表示され、操作は失敗します。

属性のマルチライン値を作成するために、このコマンドの複数のインスタンスがサポートされています。特定の属性名に関連付けられたすべてのデータが、CLI で入力された順序に従ってクライアントに提供されます。マルチライン値の個別の行は削除できません。

例

次に、AnyConnect 遅延アップデートのカスタム属性を設定する例を示します。

```
ciscoasa(config)# anyconnect-custom-data DeferredUpdateAllowed def-allowed true
```

関連コマンド

コマンド	説明
show run webvpn	**anyconnect** コマンドを含む、WebVPN に関するコンフィギュレーション情報を表示します。
show run group-policy	現在のグループ ポリシーに関する設定情報を表示します。
show running-config dynamic-access-policy-record	DAP ポリシーで使用されるカスタム属性を表示します。
show run anyconnect-custom-data	定義されているすべてのカスタム属性の名前付き値を表示します。
anyconnect-custom	カスタム属性のタイプおよび値をグループ ポリシーまたは DAP に関連付けます。
anyconnect-custom-attr	カスタム属性を作成します。

anyconnect df-bit-ignore

フラグメンテーションが必要なパケットの DF ビットを無視するには、グループ ポリシー webvpn コンフィギュレーション モードで **anyconnect-df-bit-ignore** コマンドを使用します。フラグメンテーションが必要な DF ビットを許可するには、このコマンドの **no** 形式を使用します。

anyconnect df-bit-ignore {enable | none}

no anyconnect df-bit-ignore {enable | none}

構文の説明

enable	AnyConnect クライアントで DF ビットの無視をイネーブルにします。
none	AnyConnect クライアントで DF ビットをディセーブルにします。

デフォルト

デフォルトでは、このオプションはイネーブルになっていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(2)	**svc df-bit-ignore** コマンドが追加されました。
8.4(3)	**svc df-bit-ignore** コマンドが **anyconnect df-bit-ignore** コマンドに置き換えられました。

例

```
vmb-5520(config-group-webvpn)# anyconnect routing-filtering-ignore ?

config-group-webvpn mode commands/options:
  enable  Enable Routing/Filtering for AnyConnect Client
  none    Disable Routing/Filtering for AnyConnect Client
```

anyconnect dpd-interval

デッド ピア検出（DPD）を ASA でイネーブルにし、リモート クライアントと ASA のいずれかで SSL VPN 接続を介した DPD を実行する頻度を設定するには、グループ ポリシー webvpn またはユーザ名 webvpn コンフィギュレーション モードで **anyconnect dpd-interval** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

anyconnect dpd-interval {[**gateway** {*seconds* | **none**}] | [**client** {*seconds* | **none**}]}

no anyconnect dpd-interval {[**gateway** {*seconds* | **none**}] | [**client** {*seconds* | **none**}]}

構文の説明

client none	クライアントで実行される DPD をディセーブルにします。
client *seconds*	クライアントで DPD が実行される頻度（30 ～ 3600 秒）を指定します。
gateway none	ASA で実行される DPD テストをディセーブルにします。
gateway *seconds*	ASA で DPD が実行される頻度（30 ～ 3600 秒）を指定します。値 300 が推奨されます。

デフォルト

デフォルトでは、DPD はイネーブルであり、ASA（ゲートウェイ）とクライアントの両方で 30 秒に設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
8.0(3)	デフォルト設定が、ディセーブルから、ASA（ゲートウェイ）とクライアントの両方で 30 秒に変更されました。
8.4(1)	**svc dpd-interval** コマンドが **anyconnect dpd-interval** コマンドに置き換えられました。

使用上のガイドライン

gateway は、ASA のことです。DPD をイネーブルにし、ASA がクライアントからのパケットを待機する間隔を指定します。その間隔内にパケットが受信されない場合、ASA は同じ間隔で DPD テストを 3 回試行します。クライアントからの応答を受信しない場合、ASA は TLS/DTLS トンネルを切断します。

（注） ASA の DPD プロセスは、TLS/DTLS トンネルを介してクライアントに送信するパケットが ASA にある場合にのみトリガーされます。

例

次に、既存のグループ ポリシー *sales* について、ASA（ゲートウェイ）で実行される DPD の頻度を 3000 秒に設定し、クライアントで実行される DPD の頻度を 1000 秒に設定する例を示します。

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect dpd-interval gateway 3000
ciscoasa(config-group-webvpn)# anyconnect dpd-interval client 1000
```

anyconnect dtls compression

特定のグループまたはユーザに対して低帯域幅リンクの圧縮をイネーブルにするには、グループ ポリシー webvpn またはユーザ名 webvpn コンフィギュレーション モードで **anyconnect dtls compression** コマンドを使用します。グループからコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

anyconnect dtls compression {lzs | none}

no anyconnect dtls compression {lzs | none}

構文の説明

lzs	ステートレス圧縮アルゴリズムをイネーブルにします。
none	圧縮をディセーブルにします。

デフォルト

デフォルトでは、AnyConnect 圧縮はイネーブルではありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

例

次に、圧縮をディセーブルにするシーケンスの例を示します。

```
asa# config terminal
asa(config)# group-policy DfltGrpPolicy attributes
asa(config-group-policy)# webvpn
asa(config-group-webvpn)# anyconnect ssl compression none
asa(config-group-webvpn)# anyconnect dtls compression none
```

anyconnect enable

ASA が AnyConnect クライアントをリモート コンピュータにダウンロードしたり、SSL または IKEv2 搭載の AnyConnect クライアントを使用して ASA に接続したりできるようにするには、webvpn コンフィギュレーション モードで **anyconnect enable** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

anyconnect enable

no anyconnect enable

デフォルト

このコマンドのデフォルトはディセーブルです。ASA はクライアントをダウンロードしません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが **svc enable** として追加されました。
8.4(1)	**svc enable** コマンドが **anyconnect enable** コマンドに置き換えられました。

使用上のガイドライン

no anyconnect enable コマンドを入力しても、アクティブなセッションは終了しません。

anyconnect enable コマンドは、**anyconnect image xyz** コマンドで AnyConnect イメージを設定した後に発行する必要があります。AnyConnect クライアントまたは AnyConnect WebLaunch を使用するには、**anyconnect enable** が必要です。**anyconnect enable** コマンドを SSL または IKEv2 とともに発行しないと、AnyConnect は想定どおりに動作せず、IPsec VPN 接続終了エラーでタイムアウトします。この結果、**show webvpn svc** コマンドは SSL VPN クライアントがイネーブルであると見なさず、インストールされた AnyConnect パッケージをリストしません。

例

次に、ASA でクライアントをダウンロードできるようにする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# anyconnect enable
```

関連コマンド

コマンド	説明
anyconnect image	リモート PC へのダウンロードのために ASA がキャッシュ メモリで展開する AnyConnect SSL VPN クライアント パッケージ ファイルを指定します。
anyconnect modules	AnyConnect SSL VPN Client でオプション機能に必要なモジュールの名前を指定します。
anyconnect profiles	ASA によって Cisco AnyConnect SSL VPN Client にダウンロードされるプロファイルを保管するために使用するファイルの名前を指定します。
show webvpn anyconnect	ASA にインストールされ、リモート PC へのダウンロード用にキャッシュ メモリにロードされた SSL VPN クライアントの情報を表示します。
anyconnect localization	Cisco AnyConnect VPN Client にダウンロードされたローカリゼーション ファイルを保管するために使用するパッケージ ファイルを指定します。

anyconnect-essentials

ASA の AnyConnect Essentials をイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードで **anyconnect-essentials** コマンドを使用します。AnyConnect Essentials の使用をディセーブルにし、代わりにプレミアム AnyConnect クライアントをイネーブルにするには、このコマンドの **no** 形式を使用します。

anyconnect-essentials

no anyconnect-essentials

デフォルト

AnyConnect Essentials は、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドでは、完全な AnyConnect クライアント ライセンスがインストールされていることを前提として、AnyConnect SSL VPN Client 全体の使用と AnyConnect Essentials SSL VPN Client の使用を切り替えます。AnyConnect Essentials は、個別にライセンス供与される SSL VPN クライアントで、すべて ASA 上に設定されます。プレミアム AnyConnect の機能を提供しますが、次の例外があります。

- CSD を使用できない（HostScan/Vault/Cache Cleaner を含む）
- クライアントレス SSL VPN 非対応

AnyConnect Essentials クライアントは、Microsoft Windows Vista、Windows Mobile、Windows XP、Windows 2000、Linux、または Macintosh OS X を実行しているリモート エンド ユーザに Cisco SSL VPN Client の利点をもたらします。

AnyConnect Essentials ライセンスは、**anyconnect-essentials** コマンドを使用してイネーブルまたはディセーブルにします。このコマンドは、AnyConnect Essentials ライセンスが ASA にインストールされている場合にのみ有効です。このライセンスがない場合は、このコマンドを実行すると次のエラー メッセージが表示されます。

```
ERROR: Command requires AnyConnect Essentials license
```

(注) このコマンドは、AnyConnect Essentials の使用をイネーブルまたはディセーブルにするだけです。AnyConnect Essentials *ライセンス*自体は、**anyconnect-essentials** コマンドの設定の影響を受けません。

AnyConnect Essentials ライセンスがイネーブルの場合、AnyConnect クライアントは Essentials モードを使用し、クライアントレス SSL VPN アクセスはディセーブルになります。AnyConnect Essentials ライセンスがディセーブルの場合、AnyConnect クライアントは完全な AnyConnect SSL VPN Client ライセンスを使用します。

(注) このコマンドは、ASAv ではサポートされません。詳細については、ライセンスのマニュアルを参照してください。

アクティブなクライアントレス SSL VPN 接続がある場合に AnyConnect Essentials ライセンスをイネーブルにすると、すべての接続がログオフするため、接続を再確立する必要があります。

例

次に、ユーザが webvpn コンフィギュレーション モードを開始して AnyConnect Essentials VPN Client をイネーブルにする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# anyconnect-essentials
```

anyconnect firewall-rule

パブリックまたはプライベートの ACL ファイアウォールを確立するには、グループ ポリシー webvpn またはユーザ名 webvpn コンフィギュレーション モードで **AnyConnect firewall-rule** コマンドを使用します。

anyconnect firewall-rule client interface {public | private} *ACL*

構文の説明

ACL	アクセス コントロール リストを指定します。
client interface	クライアント インターフェイスを指定します。
private	プライベート インターフェイス ルールを設定します。
public	パブリック インターフェイス ルールを設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.3(1)	この **svc firewall-rule** コマンドが追加されました。
8.4(1)	**svc firewall-rule** コマンドが **anyconnect firewall-rule** コマンドに置き換えられました。
9.0(1)	コマンドの ACL を、IPv4 アドレスと IPv6 アドレスの両方を指定できるユニファイド アクセス コントロール ルールにすることができるようになりました。

使用上のガイドライン

このコマンドを想定どおりに機能させるためには、AnyConnect セキュア モビリティ クライアントの AnyConnect Secure Mobility ライセンス サポートを提供する AsyncOS for Web バージョン 7.0 のリリースが必要です。また、AnyConnect Secure Mobility、ASA 8.3、ASDM 6.3 をサポートする AnyConnect リリースも必要です。

ここに記載したのは、AnyConnect クライアントではファイアウォールがどのように使用されるかについての注意事項です。

- ファイアウォール ルールには送信元 IP は使用されません。クライアントでは、ASA から送信されたファイアウォール ルール内の送信元 IP 情報は無視されます。送信元 IP は、ルールがパブリックかプライベートかに応じてクライアントが特定します。パブリック ルールは、クライアント上のすべてのインターフェイスに適用されます。プライベート ルールは、仮想アダプタに適用されます。
- ASA は、ACL ルールに対して数多くのプロトコルをサポートしています。ただし、AnyConnect のファイアウォール機能でサポートされているのは、TCP、UDP、ICMP、および IP のみです。クライアントでは、異なるプロトコルでルールが受信された場合、そのルールは無効なファイアウォール ルールとして処理され、さらにセキュリティ上の理由からスプリット トンネリングが無効となり、フル トンネリングが使用されます。

ただし次のように、オペレーティング システムによって動作が異なるため注意が必要です。

- Windows コンピュータの場合、Windows Firewall では拒否ルールが許可ルールに優先します。ASA により許可ルールが AnyConnect クライアントへプッシュされても、ユーザがカスタムの拒否ルールを作成していれば、AnyConnect ルールは適用されません。
- Windows Vista では、ファイアウォール ルールが作成されると、ポート番号の範囲がカンマ区切りの文字列として認識されます（たとえば、1 ～ 300 や 5000 ～ 5300）。許可されているポートの最大数は 300 です。指定した数が 300 ポートを超える場合は、最初の 300 ポートに対してのみファイアウォール ルールが適用されます。
- ファイアウォール サービスが AnyConnect クライアントにより開始される必要がある（システムにより自動的に開始されない）Windows ユーザは、VPN 接続の確立にかなりの時間を要する場合があります。
- Mac コンピュータの場合、AnyConnect クライアントでは、ASA で適用されたのと同じ順序でルールが適用されます。グローバル ルールは必ず最後になるようにしてください。
- サードパーティ ファイアウォールの場合、AnyConnect クライアント ファイアウォールとサードパーティ ファイアウォールの双方で許可されたタイプのトラフィックのみ通過できます。AnyConnect クライアントで許可されているタイプのトラフィックであっても、サードパーティ ファイアウォールによってブロックされれば、そのトラフィックはクライアントでもブロックされます。

ローカル印刷およびテザー デバイス サポートに関する ACL ルールの例を含め、AnyConnect クライアント ファイアウォールの詳細については、『*AnyConnect Administrator's Guide*』を参照してください。

例

次に、*ACL AnyConnect_Client_Local_Print* をパブリック ファイアウォールとしてイネーブルにする例を示します。

```
ciscoasa(config)# group-policy example_group attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect firewall-rule client-interface public value
AnyConnect_Client_Local_Print
```

関連コマンド

コマンド	説明
show webvpn anyconnect	インストールされている SSL VPN クライアントに関する情報を表示します。
anyconnect	特定のグループまたはユーザに対して SSL VPN クライアントをイネーブルまたは必須にします。
anyconnect image	リモート PC へのダウンロードのために ASA がキャッシュ メモリで展開するクライアント パッケージ ファイルを指定します。

anyconnect image

AnyConnect 配布パッケージをインストールまたはアップグレードして、実行コンフィギュレーションに追加するには、webvpn コンフィギュレーション モードで **AnyConnect image** コマンドを使用します。AnyConnect 配布パッケージを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

anyconnect image *path order* [**regex** *expression*]

no anyconnect image *path order* [**regex** *expression*]

構文の説明

order	クライアント パッケージ ファイルが複数である場合は、パッケージ ファイルの順序（1 ～ 65535）を指定します。ASA では、オペレーティング システムと一致するまで、指定した順序に従って、各クライアントの一部をリモート PC にダウンロードします。
path	AnyConnect パッケージのパスおよびファイル名を 255 文字以内で指定します。
regex *expression*	ブラウザから渡される user-agent 文字列と照合するために ASA によって使用される文字列を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが **svc image** として追加されました。
8.0(1)	**regex** キーワードが追加されました。
8.4(1)	**svc image** コマンドが **anyconnect image** コマンドに置き換えられました。

使用上のガイドライン

パッケージ ファイルの番号付けにより、ASA が、オペレーティング システムと一致するまで、パッケージ ファイルの一部をリモート PC にダウンロードする順序が確立されます。最も番号の小さいパッケージ ファイルが最初にダウンロードされます。したがって、リモート PC で最も一般的に使用されるオペレーティング システムと一致するパッケージ ファイルに、最も小さい番号を割り当てる必要があります。

デフォルトの順序は 1 です。*order* 引数を指定しない場合は、**svc image** コマンドを入力するたびに、以前に番号 1 と見なされたイメージに上書きします。

クライアント パッケージ ファイルごとに任意の順序で **anyconnect image** コマンドを入力できます。たとえば、2 番目（*order* 2）にダウンロードされるパッケージ ファイルを指定してから、最初（*order* 1）にダウンロードされるパッケージ ファイルを指定する **anyconnect image** コマンドを入力できます。

モバイル ユーザの場合、**regex** keyword を使用して、モバイル デバイスの接続時間を短縮できます。ブラウザが ASA に接続するとき、user-agent 文字列が HTTP ヘッダーに含められます。ASA によってストリングが受信され、そのストリングがあるイメージ用に設定された式と一致すると、そのイメージがただちにダウンロードされます。この場合、他のクライアント イメージはテストされません。

（注） スタンドアロン クライアントを使用している場合、**regex** コマンドは無視されます。また、パフォーマンス向上のため Web ブラウザでのみ使用され、正規表現文字列はスタンドアロン クライアントから提供されるユーザまたはエージェントと照合されません。

ASA では、AnyConnect クライアントと Cisco Secure Desktop（CSD）の両方のパッケージ ファイルがキャッシュ メモリに展開されます。ASA でパッケージ ファイルを正常に展開するには、パッケージ ファイルのイメージとファイルを保管するのに十分なキャッシュ メモリが必要です。

パッケージの展開に十分なキャッシュ メモリがないことを ASA が検出した場合、コンソールにエラー メッセージが表示されます。次に、**svc image** コマンドを使用してパッケージ ファイルをインストールしようとした後でレポートされるエラー メッセージの例を示します。

```
ciscoasa(config-webvpn)# anyconnect image disk0:/anyconnect-win-3.0.0520-k9.pkg
ERROR: File write error (check disk space)
ERROR: Unable to load SVC image - extraction failed
```

これがパッケージ ファイルのインストール試行中に発生した場合、グローバル コンフィギュレーション モードから **dir cache:/** コマンドを使用して、キャッシュ メモリの残りとこれまでにインストールされたパッケージのサイズを確認します。

（注） ASA にデフォルトの内部フラッシュ メモリ サイズまたはデフォルトの DRAM サイズ（キャッシュ メモリ用）だけがある場合、ASA 上で複数の AnyConnect クライアント パッケージを保存およびロードすると、問題が発生することがあります。フラッシュ メモリにパッケージ ファイルに十分な容量がある場合でも、クライアントの unzip とロードのときに ASA のキャッシュ メモリが不足する場合があります。AnyConnect を使用する場合の ASA のメモリ要件について、および ASA で行えるメモリ アップグレードの詳細については、Cisco ASA 5500 シリーズの最新のリリース ノートを参照してください。

例

次に、Windows、MAC、Linux 用の AnyConnect クライアント パッケージ ファイルをこの順序でロードする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# anyconnect image disk0:/anyconnect-win-3.0.0527-k9.pkg 1
ciscoasa(config-webvpn)# anyconnect image disk0:/anyconnect-macosx-i386-3.0.0414-k9.pkg 2
ciscoasa(config-webvpn)# anyconnect image disk0:/anyconnect-linux-3.0.0414-k9.pkg 3
ciscoasa(config-webvpn)
```

次に、ロードされた AnyConnect クライアント パッケージとその順序を表示する、**show webvpn anyconnect** コマンドの出力例を示します。

```
ciscoasa(config-webvpn)# show webvpn anyconnect
1. disk0:/anyconnect-win-3.0.0527-k9.pkg 1 dyn-regex=/Windows NT/
  CISCO STC win2k+
  3,0,0527
  Hostscan Version 3.0.0527
  Tue 10/19/2010 16:16:56.25

2. disk0:/anyconnect-macosx-i386-3.0.0414-k9.pkg 2 dyn-regex=/Intel Mac OS X/
  CISCO STC Darwin_i386
  3.0.0414
  Wed Oct 20 20:39:53 MDT 2010

3. disk0:/anyconnect-linux-3.0.0414-k9.pkg 3 dyn-regex=/Linux i[1-9]86/
  CISCO STC Linux
  3.0.0414
  Wed Oct 20 20:42:02 MDT 2010

3 AnyConnect Client(s) installed
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
anyconnect modules	AnyConnect SSL VPN Client でオプション機能に必要なモジュールの名前を指定します。
anyconnect profiles	ASA によって Cisco AnyConnect SSL VPN Client にダウンロードされるプロファイルを保管するために使用するファイルの名前を指定します。
show webvpn anyconnect	ASA にインストールされ、リモート PC へのダウンロード用にキャッシュ メモリにロードされた SSL VPN クライアントの情報を表示します。
anyconnect localization	Cisco AnyConnect VPN Client にダウンロードされたローカリゼーション ファイルを保管するために使用するパッケージ ファイルを指定します。

anyconnect keep-installer

(注) このコマンドは、2.5 より後の AnyConnect バージョンには適用されませんが、下位互換性のため引き続き使用可能です。**anyconnect keep-installer** コマンドを設定しても、AnyConnect 3.0 以降には影響しません。

リモート PC への SSL VPN クライアントの永続インストールをイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**AnyConnect keep-installer** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

anyconnect keep-installer {**installed** | **none**}

no anyconnect keep-installer {**installed** | **none**}

構文の説明

installed	クライアントの自動アンインストール機能をディセーブルにします。クライアントは、今後の接続のためにリモート PC 上にインストールされたままになります。
none	アクティブな接続の終了後にクライアントがリモート コンピュータからアンインストールされることを指定します。

デフォルト

デフォルトでは、クライアントの永続インストールがイネーブルです。セッションの終了時に、クライアントはリモート コンピュータ上に残ります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	**svc keep-installer** コマンドが追加されました。
8.4(1)	**svc keep-installer** コマンドが **anyconnect keep-installer** コマンドに置き換えられました。

例

次の例では、ユーザはグループ ポリシー webvpn コンフィギュレーション モードを開始し、セッションの終了時にクライアントを削除するようにグループ ポリシーを設定します。

```
ciscoasa(config-group-policy)#webvpn
ciscoasa(config-group-webvpn)# anyconnect keep-installer none
ciscoasa(config-group-webvpn)#
```

関連コマンド

コマンド	説明
show webvpn anyconnect	ASA にインストールされ、リモート PC へのダウンロード用にキャッシュ メモリにロードされた AnyConnect PCs クライアントの情報を表示します。
anyconnect	特定のグループまたはユーザに対して SSL VPN クライアントをイネーブルまたは必須にします。
anyconnect enable	ASA によって AnyConnect PCs クライアント ファイルをリモート PC にダウンロードできるようにします。
anyconnect image	リモート PC へのダウンロード用に ASA によってキャッシュ メモリに展開されている AnyConnect クライアント パッケージ ファイルを指定します。

anyconnect modules

オプション機能のために AnyConnect SSL VPN Client で必要となるモジュールの名前を指定するには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**anyconnect modules** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

anyconnect modules {**none** | **value** *string*}

no anyconnect modules {**none** | **value** *string*}

構文の説明

string	オプション モジュールの名前（最大 256 文字）。複数のストリングを指定する場合は、カンマで区切ります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	**svc modules** コマンドが追加されました。
8.4(1)	**svc modules** コマンドが **anyconnect modules** コマンドに置き換えられました。

使用上のガイドライン

ダウンロード時間を最小にするために、クライアントでは、サポートする各機能に必要なモジュールのダウンロード（ASA から）のみを要求します。**anyconnect modules** コマンドにより、ASA でこれらのモジュールをダウンロードできます。

次の表に、AnyConnect モジュールを表す文字列値を示します。

AnyConnect モジュールを表す文字列	AnyConnect モジュール名
dart	AnyConnect DART（診断およびレポート ツール）
nam	AnyConnect ネットワーク アクセス マネージャ
vpngina	AnyConnect SBL（ログイン前の起動）
websecurity	AnyConnect Web セキュリティ モジュール
telemetry	AnyConnect テレメトリ モジュール
posture	AnyConnect ポスチャ モジュール
none	**none** を選択すると、ASA によって基本的なファイルがダウンロードされ、オプションのモジュールはダウンロードされません。既存のモジュールはグループ ポリシーから削除されます。

例

次の例では、ユーザはグループ ポリシー *PostureModuleGroup* のグループ ポリシー属性モードを開始し、そのグループ ポリシーの webvpn コンフィギュレーション モードを開始しています。さらに、ASA に接続すると AnyConnect ポスチャ モジュールおよび AnyConnect テレメトリ モジュールがエンドポイントにダウンロードされるように、文字列 *posture* および *telemetry* を指定しています。

```
ciscoasa> en
Password:
ciscoasa# config t
ciscoasa(config)# group-policy PostureModuleGroup attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect modules value posture,telemetry
ciscoasa(config-group-webvpn)# write mem
Building configuration...
Cryptochecksum: 40975338 b918425d 083b391f 9e5a5c69

22055 bytes copied in 3.440 secs (7351 bytes/sec)
[OK]
ciscoasa(config-group-webvpn)#
```

グループ ポリシーからモジュールを削除するには、保持するモジュールの値だけを指定したコマンドを再送信します。たとえば、このコマンドはテレメトリ モジュールを削除します。

```
ciscoasa(config-group-webvpn)# anyconnect modules value posture
```

関連コマンド

コマンド	説明
show webvpn anyconnect	ASA のキャッシュ メモリにロードされていてダウンロード可能な AnyConnect パッケージについての情報を表示します。
anyconnect enable	特定のグループまたはユーザに対して、AnyConnect クライアントをイネーブルにします。
anyconnect image	リモート PC へのダウンロード用に ASA によってキャッシュ メモリに展開されている AnyConnect クライアント パッケージ ファイルを指定します。

anyconnect mtu

Cisco AnyConnect VPN Client によって確立された VPN 接続の MTU サイズを調整するには、グループポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**anyconnect mtu** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

anyconnect mtu *size*

no anyconnect mtu *size*

構文の説明

size	MTU サイズ（バイト単位）。576 ～ 1406 バイトです。

デフォルト

デフォルトのサイズは 1406 バイトです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	**svc mtu** コマンドが追加されました。
8.4(1)	**svc mtu** コマンドが **anyconnect mtu** コマンドに置き換えられました。

使用上のガイドライン

このコマンドは、AnyConnect クライアントのみに影響します。VPN Client は、異なる MTU サイズに調整できません。

デフォルトのグループ ポリシーでのこのコマンドのデフォルトは、**no svc mtu** です。MTU サイズは、接続で使用されているインターフェイスの MTU に基づき、IP/UDP/DTLS のオーバーヘッドを差し引いて、自動的に調整されます。

IPv6 対応インターフェイスで許可される最小 MTU は 1280 バイトです。ただし、IPsec がインターフェイスでイネーブルになっている場合、MTU 値は、IPsec 暗号化のオーバーヘッドのために 1380 未満に設定できません。インターフェイスを 1380 バイト未満に設定すると、パケットのドロップが発生する可能性があります。

例

次に、グループ ポリシー *telecommuters* について、MTU サイズを 500 バイトに設定する例を示します。

```
ciscoasa(config)# group-policy telecommuters attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect mtu 500
```

関連コマンド

コマンド	説明
anyconnect keep-installer	クライアントの自動アンインストール機能をディセーブルにします。初期ダウンロード後、接続が終了した後もクライアントはリモート PC 上に残ります。
anyconnect ssl dtls	SSL VPN 接続を確立する CVC に対して DTLS をイネーブルにします。
show run webvpn	**anyconnect** コマンドを含む、WebVPN に関するコンフィギュレーション情報を表示します。

anyconnect profiles（グループ ポリシー属性 > webvpn、ユーザ名属性 > webvpn）

Cisco AnyConnect VPN Client（CVC）ユーザにダウンロードされる CVC プロファイル パッケージを指定するには、webvpn またはコンフィギュレーション モードで **anyconnect profiles** コマンドを使用します。webvpn コンフィギュレーション モードにアクセスするには、最初にグループ ポリシー属性コマンドまたはユーザ名属性を入力します。コンフィギュレーションからこのコマンドを削除し、値を継承するには、コマンドの **no** 形式を使用します。

anyconnect profiles {**value** *profile* | **none**}

no anyconnect profiles {**value** *profile* | **none** } **[type** *type*]

構文の説明

value *profile*	プロファイル名。
none	ASA によってプロファイルはダウンロードされません。
type *type*	標準 AnyConnect プロファイルまたは任意の英数字値に一致するユーザ。

デフォルト

デフォルトは none です。ASA によってプロファイルはダウンロードされません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	**svc profiles** コマンドが追加されました。
8.3(1)	オプションのタイプ **value** が追加されました。
8.4(1)	**svc profiles** コマンドが **anyconnect profiles** コマンドに置き換えられました。

使用上のガイドライン

このコマンドをグループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名属性 webvpn コンフィギュレーション モードで入力すると、ASA によってグループ ポリシーまたはユーザ名に基づいてプロファイルを CVC ユーザにダウンロードできます。CVC プロファイルをすべての CVC ユーザにダウンロードするには、このコマンドを webvpn コンフィギュレーション モードで使用します。

CVC プロファイルとは、CVC ユーザ インターフェイスに表示される接続エントリを設定するために CVC が使用するコンフィギュレーション パラメータのグループで、ホスト コンピュータの名前とアドレスが含まれます。CVC ユーザ インターフェイスを使用して、プロファイルを作成および保存できます。また、テキスト エディタでこのファイルを編集し、ユーザ インターフェイスからは設定できないパラメータの詳細を設定することもできます。

CVC のインストレーションには、他のプロファイル ファイルを編集し、作成するための基礎として使用できる、1 つのプロファイル テンプレート（cvcprofile.xml）が含まれています。CVC プロファイルの編集の詳細については、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。

例

次の例では、ユーザは使用可能なプロファイルを表示する **anyconnect profiles value** コマンドを入力します。

```
ciscoasa(config-group-webvpn)# anyconnect profiles value ?

config-group-webvpn mode commands/options:
Available configured profile packages:
  engineering
  sales
```

次に、ユーザは CVC プロファイル sales を使用するようにグループ ポリシーを設定します。

```
ciscoasa(config-group-webvpn)# anyconnect profiles sales
```

関連コマンド

コマンド	説明
show webvpn anyconnect	インストールされている AnyConnect クライアントに関する情報を表示します。
anyconnect	特定のグループまたはユーザに SSL VPN クライアントをイネーブルにします。または、要求します。
anyconnect image	リモート PC へのダウンロード用に ASA によってキャッシュ メモリに展開されている AnyConnect クライアント パッケージ ファイルを指定します。

anyconnect profiles（webvpn）

ASA によってキャッシュ メモリにロードされて、Cisco AnyConnect VPN Client（CVC）ユーザのグループ ポリシーおよびユーザ名属性で使用可能となるプロファイル パッケージとしてファイルを指定するには、webvpn コンフィギュレーション モードで **anyconnect profiles** コマンドを使用します。コンフィギュレーションからこのコマンドを削除し、ASA によってパッケージ ファイルがキャッシュ メモリからアンロードされるようにするには、このコマンドの **no** 形式を使用します。

anyconnect profiles {*profile path*}

no anyconnect profiles {*profile path*}

構文の説明

path	ASA のフラッシュ メモリ内のプロファイル ファイルのパスおよびファイル名。
profile	キャッシュ メモリ内に作成するプロファイルの名前。

デフォルト

デフォルトは none です。プロファイル パッケージは ASA によってキャッシュ メモリにロードされません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	**svc profiles** コマンドが追加されました。
8.4(1)	**svc profiles** コマンドが **anyconnect profiles** コマンドに置き換えられました。

使用上のガイドライン

CVC プロファイルとは、CVC ユーザ インターフェイスに表示される接続エントリを設定するために CVC が使用するコンフィギュレーション パラメータのグループで、ホスト コンピュータの名前とアドレスが含まれます。CVC ユーザ インターフェイスを使用して、プロファイルを作成および保存できます。

また、テキスト エディタでこのファイルを編集し、ユーザ インターフェイスからは設定できないパラメータの詳細を設定することもできます。CVC のインストレーションには、他のプロファイル ファイルを編集し、作成するための基礎として使用できる、1 つのプロファイル テンプレート（cvcprofile.xml）が含まれています。CVC プロファイルの編集の詳細については、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。

新しい CVC プロファイルを作成してフラッシュ メモリにアップロードした後、webvpn コンフィギュレーション モードで **anyconnect profiles** コマンドを使用して、ASA に対して XML ファイルをプロファイルとして指定します。このコマンドを入力すると、ファイルは ASA のキャッシュ メモリにロードされます。次に、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名属性コンフィギュレーション モードで **anyconnect profiles** コマンドを使用して、グループまたはユーザのプロファイルを指定できます。

例

次の例では、ユーザは、以前に CVC のインストールで提供された cvcprofile.xml ファイルから 2 つの新しいプロファイル ファイル（sales_hosts.xml および engineering_hosts.xml）を作成し、ASA のフラッシュ メモリにアップロードしています。

さらに、ユーザはそれらのファイルを CVC のプロファイルとして ASA に指定し、*sales* と *engineering* という名前を指定しています。

```
ciscoasa(config-webvpn)# anyconnect profiles sales disk0:sales_hosts.xml
ciscoasa(config-webvpn)# anyconnect profiles engineering disk0:engineering_hosts.xml
```

dir cache:stc/profiles コマンドを入力すると、キャッシュ メモリにロードされているプロファイルが表示されます。

```
ciscoasa(config-webvpn)# dir cache:stc/profiles

Directory of cache:stc/profiles/

0      ----  774         11:54:41 Nov 22 2006  engineering.pkg
0      ----  774         11:54:29 Nov 22 2006  sales.pkg

2428928 bytes total (18219008 bytes free)
ciscoasa(config-webvpn)#
```

これらのプロトコルは、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名属性コンフィギュレーション モードでの **svc profiles** コマンドで使用できます。

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect profiles value ?

config-group-webvpn mode commands/options:
Available configured profile packages:
  engineering
  sales
```

関連コマンド

コマンド	説明
show webvpn anyconnect	インストールされている AnyConnect クライアントに関する情報を表示します。
anyconnect	特定のグループまたはユーザに対して SSL VPN クライアントをイネーブルまたは必須にします。
anyconnect image	ASA がリモート PC にダウンロードするためにキャッシュ メモリに展開する AnyConnect パッケージ ファイルを指定します。

anyconnect ssl compression

特定のグループまたはユーザについて、SSL VPN 接続での http データの圧縮をイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**anyconnect ssl compression** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

anyconnect ssl compression {**deflate** | **lzs** | **none**}

no anyconnect ssl compression {**deflate** | **lzs** | **none**}

構文の説明

deflate	デフレート圧縮アルゴリズムをイネーブルにします。
lzs	ステートレス圧縮アルゴリズムをイネーブルにします。
none	圧縮をディセーブルにします。

デフォルト

デフォルトでは、圧縮は none（ディセーブル）に設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	**anyconnect compression** コマンドが追加されました。

使用上のガイドライン

SSL VPN 接続の場合、webvpn コンフィギュレーション モードで設定された **compression** コマンドによって、グループ ポリシー webvpn モードおよびユーザ名 webvpn モードで設定された **anyconnect ssl compression** コマンドは上書きされます。

例

次の例では、グループ ポリシー sales に対して SVC 圧縮はディセーブルです。

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect ssl compression none
```

関連コマンド

コマンド	説明
anyconnect	特定のグループまたはユーザに対して SSL VPN クライアントをイネーブルまたは必須にします。
anyconnect keepalive	リモート コンピュータ上のクライアントから ASA にキープアライブ メッセージが SSL VPN 接続で送信される頻度を指定します。
anyconnect keep-installer	クライアントの自動アンインストール機能をディセーブルにします。クライアントは、今後の接続のためにリモート PC 上にインストールされたままになります。
anyconnect rekey	SSL VPN 接続でクライアントがキーの再生成を実行できるようにします。
compression	すべての SSL、WebVPN、および IPsec VPN 接続で、圧縮をイネーブルにします。
show webvpn anyconnect	インストールされている SSL VPN クライアントに関する情報を表示します。

anyconnect ssl df-bit-ignore

特定のグループまたはユーザについて SSL VPN 接続でパケットを強制的にフラグメント化できるようにする（トンネルを通過できるようにする）には、グループ ポリシー webvpn またはユーザ名 webvpn コンフィギュレーション モードで **anyconnect ssl df-bit-ignore** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

anyconnect ssl df-bit-ignore {enable | disable}

no anyconnect ssl df-bit-ignore

構文の説明

enable	SSL 搭載の AnyConnect で DF ビットの無視をイネーブルにします。
disable	SSL 搭載の AnyConnect で DF ビットをディセーブルにします。

デフォルト

DF ビットの無視は、*ディセーブルに設定されています。*

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(1)	**svc df-bit-ignore** コマンドが **anyconnect ssl df-bit-ignore** コマンドに置き換えられました。

使用上のガイドライン

この機能では、DF ビットが設定されているパケットを強制的にフラグメント化して、トンネルを通過させることができます。使用例として、TCP MSS ネゴシエーションに適切に応答しないネットワークのサーバに対する使用などがあります。

例

次の例では、グループ ポリシー sales に対して DF ビットの無視がイネーブルになっています。

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect ssl df-bit-ignore enable
```

関連コマンド

コマンド	説明
anyconnect	特定のグループまたはユーザに対して SSL VPN クライアントをイネーブルまたは必須にします。
anyconnect keepalive	リモート コンピュータ上のクライアントから ASA にキープアライブ メッセージが SSL VPN 接続で送信される頻度を指定します。
anyconnect keep-installer	クライアントの自動アンインストール機能をディセーブルにします。クライアントは、今後の接続のためにリモート PC 上にインストールされたままになります。
anyconnect rekey	SSL VPN 接続でクライアントがキーの再生成を実行できるようにします。

anyconnect ssl dtls enable

Cisco AnyConnect VPN Client との SSL VPN 接続を確立している特定のグループまたはユーザのインターフェイスで Datagram Transport Layer Security（DTLS）接続をイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名属性 webvpn コンフィギュレーション モードで **anyconnect ssl dtls enable** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

anyconnect ssl dtls enable *interface*

no anyconnect ssl dtls enable *interface*

構文の説明

interface	インターフェイスの名前。

デフォルト

デフォルトではイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	**svc dtls** コマンドが追加されました。
8.4(1)	**svc dtls** コマンドが **anyconnect ssl dtls** コマンドに置き換えられました。

使用上のガイドライン

DTLS をイネーブルにすると、SSL VPN 接続を確立している AnyConnect クライアントで、2 つの同時トンネル（SSL トンネルと DTLS トンネル）を使用できます。DTLS によって、一部の SSL 接続に関連する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

DTLS をイネーブルにしない場合、SSL VPN 接続を確立している AnyConnect クライアント ユーザは SSL トンネルのみで接続します。

このコマンドでは、特定のグループまたはユーザについて DTLS をイネーブルにします。すべての AnyConnect クライアント ユーザについて DTLS をイネーブルにするには、webvpn コンフィギュレーション モードで **anyconnect ssl dtls enable** コマンドを使用します。

例

次に、グループ ポリシー *sales* のグループ ポリシー webvpn コンフィギュレーション モードを開始し、DTLS をイネーブルにする例を示します。

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect ssl dtls enable
```

関連コマンド

コマンド	説明
dtls port	DTLS の UDP ポートを指定します。
anyconnect dtls	SSL VPN 接続を確立するグループまたはユーザに対して、DTLS をイネーブルにします。
vpn-tunnel-protocol	ASA がリモート アクセス用に許可する VPN プロトコル（SSL を含む）を指定します。

anyconnect ssl keepalive

SSL VPN 接続でリモート クライアントから ASA に送信されるキープアライブ メッセージの頻度を設定するには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで、**anyconnect ssl keepalive** コマンドを使用します。コンフィギュレーションからこのコマンドを削除し、値を継承するには、コマンドの **no** 形式を使用します。

anyconnect ssl keepalive {**none** | *seconds*}

no anyconnect ssl keepalive {**none** | *seconds*}

構文の説明

none	キープアライブ メッセージをディセーブルにします。
seconds	キープアライブ メッセージをイネーブルにし、メッセージの頻度（15 ～ 600 秒）を指定します。

デフォルト

デフォルトは 20 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	**svc keepalive** コマンドが追加されました。
8.0(3)	デフォルト設定がディセーブルから 20 秒に変更されました。
8.4(1)	**svc keepalive** コマンドが **anyconnect ssl keepalive** コマンドに置き換えられました。

使用上のガイドライン

Cisco SSL VPN Client（SVC）と Cisco AnyConnect VPN Client の両方で、ASA への SSL VPN 接続を確立するときにキープアライブ メッセージを送信できます。

接続をアイドル状態で維持できる時間がデバイスによって制限されている場合も、プロキシ、ファイアウォール、または NAT デバイスを経由した SSL VPN 接続が確実に開いたままで保たれるように、キープアライブ メッセージの頻度を調整できます（*seconds* で指定）。

また、頻度を調整すると、リモート ユーザが Microsoft Outlook または Microsoft Internet Explorer などのソケット ベース アプリケーションをアクティブに実行していない場合でも、クライアントは切断および再接続されません。

(注) キープアライブはデフォルトでイネーブルになっています。キープアライブをディセーブルにすると、フェールオーバー イベントの際に、SSL VPN クライアント セッションはスタンバイ デバイスに引き継がれません。

例

次の例では、ユーザは、*sales* という名前の既存のグループ ポリシーについて、ASA を設定し、クライアントがキープアライブ メッセージを 300 秒(5 分)の頻度で送信できるようにします。

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anyconnect ssl keepalive 300
```

関連コマンド

コマンド	説明
anyconnect	特定のグループまたはユーザに SSL VPN クライアントをイネーブルにします。または、要求します。
anyconnect dpd-interval	ASA でデッド ピア検出(DPD)をイネーブルにし、クライアントまたは ASA によって DPD が実行される頻度を設定します。
anyconnect keep-installer	クライアントの自動アンインストール機能をディセーブルにします。クライアントは、今後の接続のためにリモート PC 上にインストールされたままになります。
anyconnect ssl rekey	セッションでクライアントがキーの再生成を実行できるようにします。

anyconnect ssl rekey

SSL VPN 接続でリモート クライアントがキーの再生成を実行できるようにするには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで **anyconnect ssl rekey** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

anyconnect ssl rekey {**method** {**ssl** | **new-tunnel**} | **time** *minutes* | **none**}

no anyconnect ssl rekey {**method** {**ssl** | **new-tunnel**} | **time** *minutes* | **none**}

構文の説明

method ssl	キーの再生成中にクライアントによって新しいトンネルが確立されることを指定します。
method new-tunnel	キーの再生成中にクライアントによって新しいトンネルが確立されることを指定します。
method none	キーの再生成をディセーブルにします。
time *minutes*	セッションの開始からキーの再生成が発生するまでの時間（分）を指定します。4 ～ 10080（1 週間）の範囲です。

デフォルト

デフォルトは none（ディセーブル）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	**svc rekey** コマンドが追加されました。
8.0(2)	「中間者」攻撃の可能性を防ぐため、**svc rekey method ssl** コマンドの動作が **svc rekey method new-tunnel** コマンドの動作に変更されました。
8.4(1)	**svc rekey** コマンドが **anyconnect ssl rekey** コマンドに置き換えられました。

使用上のガイドライン

Cisco AnyConnect Secure Mobility Client は、ASA への SSL VPN 接続でキーの再生成を実行できます。キーの再生成方法を **ssl** または **new-tunnel** に設定すると、キー再生成時に SSL 再ネゴシエーションが行われず、クライアントがキー再生成時に新規トンネルを確立することが指定されます。

例

次の例では、ユーザは、グループ ポリシー *sales* に属するリモート クライアントがキーの再生成時に SSL と再ネゴシエートし、セッションの開始後 30 分でキーの再生成が発生することを指定します。

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# anycoanynnect ssl rekey method ssl
ciscoasa(config-group-webvpn)# anyconnect ssl rekey time 30
```

関連コマンド

コマンド	説明
anyconnect enable	特定のグループまたはユーザに対して AnyConnect Secure Mobility Client をイネーブルまたは必須にします。
anyconnect dpd-interval	ASA でデッド ピア検出（DPD）をイネーブルにし、AnyConnect Secure Mobility Client または ASA によって DPD が実行される頻度を設定します。
anyconnect keepalive	リモート コンピュータ上の AnyConnect Secure Mobility Client から ASA にキープアライブ メッセージが送信される頻度を指定します。
anyconnect keep-installer	リモート コンピュータへの AnyConnect Secure Mobility Client の永続インストールをイネーブルにします。

apcf

Application Profile Customization Framework プロファイルをイネーブルにするには、webvpn コンフィギュレーション モードで **apcf** コマンドを使用します。特定の APCF スクリプトをディセーブルにするには、このコマンドの **no** 形式を使用します。すべての APCF スクリプトをディセーブルにするには、このコマンドの **no** 形式を引数なしで使用します。

apcf URL/filename.ext

no apcf [URL/filename.ext]

構文の説明

filename.extension	APCF カスタマイゼーション スクリプトの名前を指定します。これらのスクリプトは、常に XML 形式です。拡張子は、.xml、.txt、.doc などです。
URL	ASA でロードして使用する APCF プロファイルの場所を指定します。http://、https://、tftp://、ftp://、flash:/、disk#:/' のいずれかの URL を使用します。 URL には、サーバ、ポート、およびパスを含めることができます。ファイル名のみを指定した場合、デフォルトの URL は flash:/ です。**copy** コマンドを使用して、APCF プロファイルをフラッシュ メモリにコピーできます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力するモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

apcf コマンドを使用すると、ASA は非標準の Web アプリケーションと Web リソースを WebVPN 接続で正しくレンダリングされるように処理できます。APCF プロファイルには、特定のアプリケーションに関して、いつ(事前、事後)、どこの(ヘッダー、本文、要求、応答)、どのデータを変換するかを指定するスクリプトがあります。

ASA で複数の APCF プロファイルを使用できます。その場合、ASA は、それらのプロファイルを古いものから新しいものの順に 1 つずつ適用します。

APCF コマンドは、Cisco TAC のサポートがある場合にのみ使用することを推奨します。

例

次に、フラッシュ メモリの /apcf にある apcf1 という名前の APCF をイネーブルにする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# apcf flash:/apcf/apcf1.xml
ciscoasa(config-webvpn)#
```

次に、myserver という名前の HTTPS サーバ（ポート 1440）のパス /apcf にある apcf2.xml という名前の APCF をイネーブルにする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# apcf https://myserver:1440/apcf/apcf2.xml
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
proxy-bypass	特定のアプリケーションに対してコンテンツの最低限の書き換えを設定します。
rewrite	トラフィックが ASA を通過するかどうかを決定します。
show running config webvpn apcf	APCF 設定を表示します。

app-agent heartbeat

ASA で実行されている app-agent（アプリケーション エージェント）のハートビート メッセージ間隔を設定して、Firepower シャーシの健全性をチェックするには、グローバル コンフィギュレーション モードで **app-agent heartbeat** コマンドを使用します。

app-agent heartbeat [**interval** *ms*] [**retry-count** *number*]

（注） Firepower シャーシでのみサポートされています。

構文の説明

interval *ms*	ハートビートの時間間隔を 100 ～ 6000 ms の範囲の 100 の倍数単位で設定します。デフォルトは 1000 ms です。
retry-count *number*	再試行の回数を 1 ～ 30 の間で設定します。デフォルトの試行回数は 3 回です。

コマンド デフォルト

デフォルトの間隔は 1000 ms です。

デフォルトの再試行回数は 3 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.6(2)	コマンドが追加されました。
9.9(1)	最小インターフェイスが 300 ms から 100 ms に変更されました。

使用上のガイドライン

ASA はホストの Firepower シャーシとのバックプレーンを介して通信できるかどうかをチェックします。

Firepower 4100/9300 の場合、最小の結合時間（*interval* x *retry-count*）は、600 ミリ秒未満にすることはできません。たとえば、間隔を 100 に、再試行回数を 3 に設定した場合、合計結合時間は 300 ミリ秒になりますが、これはサポートされていません。たとえば、間隔を 100 に設定し、再試行回数を 6 に設定して最小時間（600 ms）を満たすことができます。

例

次に、間隔を 300 ms に設定する例を示します。

```
ciscoasa(config)# app-agent heartbeat interval 300
```

関連コマンド

コマンド	説明
health-check	クラスタ ヘルス チェックのパラメータを設定します。

appl-acl

セッションに適用する設定済みの Web タイプ ACL を指定するには、DAP webvpn コンフィギュレーション モードで **appl-acl** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。すべての Web タイプ ACL を削除するには、このコマンドの **no** 形式を引数なしで使用します。

appl-acl [*identifier***]**

no appl-acl [*identifier***]**

構文の説明

identifier	以前に設定した Web タイプ ACL の名前。最大長は 240 文字です。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
DAP webvpn コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

Web タイプ ACL を設定するには、グローバル コンフィギュレーション モードで **access-list webtype** コマンドを使用します。

appl-acl コマンドを複数回使用して、複数の Web タイプ ACL を DAP ポリシーに適用できます。

例

次に、newacl という名前の設定済みの Web タイプ ACL をダイナミック アクセス ポリシーに適用する例を示します。

```
ciscoasa (config)# config-dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)# webvpn
ciscoasa(config-dynamic-access-policy-record)# appl-acl newacl
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
access-list_webtype	Web タイプ ACL を作成します。

application-access

認証された WebVPN ユーザに表示される WebVPN ホームページの [Application Access] フィールド、およびユーザがアプリケーションを選択したときに表示される [Application Access] ウィンドウをカスタマイズするには、カスタマイゼーション コンフィギュレーション モードで **application-access** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

application-access {**title** | **message** | **window**} {**text** | **style**} *value*

no application-access {**title** | **message** | **window**} {**text** | **style**} *value*

構文の説明

message	[Application Access] フィールドのタイトルの下に表示されるメッセージを変更します。
style	[Application Access] フィールドのスタイルを変更します。
text	[Application Access] フィールドのテキストを変更します。
title	[Application Access] フィールドのタイトルを変更します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）。
window	[Application Access] ウィンドウを変更します。

デフォルト

[Application Access] フィールドのデフォルトのタイトル テキストは「Application Access」です。

[Application Access] フィールドのデフォルトのタイトル スタイルは次のとおりです。

background-color:#99CCCC;color:black;font-weight:bold;text-transform:uppercase

[Application Access] フィールドのデフォルトのメッセージ テキストは「Start Application Client」です。

[Application Access] フィールドのデフォルトのメッセージ スタイルは次のとおりです。

background-color:#99CCCC;color:maroon;font-size:smaller.

[Application Access] ウィンドウのデフォルトのウィンドウ テキストは次のとおりです。

「Close this window when you finish using Application Access. Please wait for the table to be displayed before starting applications.」

[Application Access] ウィンドウのデフォルトのウィンドウ スタイルは次のとおりです。

background-color:#99CCCC;color:black;font-weight:bold

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
カスタマイゼーション コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、**webvpn** コマンドまたは **tunnel-group webvpn-attributes** コマンドを使用してアクセスします。

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

次に、WebVPN ページに対する変更で最もよく行われるページ配色の変更に役立つヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、[Application Access] フィールドの背景色を RGB 16 進値 66FFFF（緑色の一種）にカスタマイズする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# application-access title style background-color:#66FFFF
```

関連コマンド

コマンド	説明
application-access hide-details	[Application Access] ウィンドウのアプリケーション詳細の表示をイネーブルまたはディセーブルにします。
browse-networks	WebVPN ホームページの [Browse Networks] フィールドをカスタマイズします。
file-bookmarks	WebVPN ホームページの [File Bookmarks] タイトルまたはリンクをカスタマイズします。
web-applications	WebVPN ホームページの [Web Application] フィールドをカスタマイズします。
web-bookmarks	WebVPN ホームページの [Web Bookmarks] タイトルまたはリンクをカスタマイズします。

application-access hide-details

WebVPN の [Application Access] ウィンドウに表示されるアプリケーション詳細を非表示にするには、カスタマイゼーション コンフィギュレーション モードで **application-access hide-details** コマンドを使用します。このモードには、**webvpn** コマンドまたは **tunnel-group webvpn-attributes** コマンドを使用してアクセスします。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

application-access hide-details {**enable** | **disable**}

no application-access [**hide-details** {**enable** | **disable**}]

構文の説明

disable	[Application Access] ウィンドウにアプリケーション詳細を表示します。
enable	[Application Access] ウィンドウのアプリケーション詳細を非表示にします。

デフォルト

デフォルトではディセーブルになっています。[Application Access] ウィンドウにアプリケーション詳細が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
カスタマイゼーション コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

例

次に、アプリケーション詳細の表示をディセーブルにする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# application-access hide-details disable
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの [Application Access] フィールドをカスタマイズします。
browse-networks	WebVPN ホームページの [Browse Networks] フィールドをカスタマイズします。
web-applications	WebVPN ホームページの [Web Application] フィールドをカスタマイズします。

CHAPTER 3

area コマンド～ auto-update timeout コマンド

area

OSPFv2 エリアまたは OSPFv3 エリアを作成するには、ルータ コンフィギュレーション モードで **area** コマンドを使用します。エリアを削除するには、このコマンドの **no** 形式を使用します。

area *area_id*

no area *area_id*

構文の説明

area_id	作成するエリアの ID。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	—	—
IPv6 ルータ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	OSPFv3 のサポートが追加されました。

使用上のガイドライン

作成したエリアには、パラメータが設定されていません。関連する **area** コマンドを使用してエリア パラメータを設定します。

例

次に、エリア ID が 1 の OSPF エリアを作成する例を示します。

```
ciscoasa(config-router)# area 1
ciscoasa(config-router)#
```

関連コマンド

コマンド	説明
area nssa	(任意)エリアを Not-So-Stubby Area として定義します。
area stub	エリアをスタブ エリアとして定義します。
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area authentication

OSPFv2 エリアの認証をイネーブルにするには、ルータ コンフィギュレーション モードで **area authentication** コマンドを使用します。エリア認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

area *area_id* **authentication** [**message-digest**]

no area *area_id* **authentication** [**message-digest**]

構文の説明

area_id	認証をイネーブルにするエリアの ID。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
message-digest	（オプション）*area_id* で指定したエリアに対する Message Digest 5（MD5）認証をイネーブルにします。

デフォルト

エリア認証はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードはサポートされます。

使用上のガイドライン

指定した OSPFv2 エリアが存在しない場合は、このコマンドを入力すると作成されます。**message-digest** キーワードを指定せずに **area authentication** コマンドを入力した場合は、簡易パスワード認証がイネーブルになります。**message-digest** キーワードを指定すると、MD5 認証がイネーブルになります。

例

次に、エリア 1 に対して MD5 認証をイネーブルにする例を示します。

```
ciscoasa(config-router)# area 1 authentication message-digest
ciscoasa(config-router)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area default-cost

スタブまたは NSSA に送信されるデフォルト集約ルートのコストを指定するには、ルータ コンフィギュレーション モードまたは IPv6 ルータ コンフィギュレーション モードで **area default-cost** コマンドを使用します。デフォルトのコスト値に戻すには、このコマンドの **no** 形式を使用します。

area *area_id* **default-cost** *cost*

no area *area_id* **default-cost** *cost*

構文の説明

area_id	デフォルト コストを変更するスタブまたは NSSA の ID。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
cost	スタブまたは NSSA に使用されるデフォルト集約ルートのコストを指定します。有効な値の範囲は、0 ～ 65535 です。

デフォルト

cost のデフォルト値は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—
IPv6 ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードおよび OSPFv3 がサポートされています。

使用上のガイドライン

指定したエリアが **area** コマンドを使用して過去に定義されていない場合は、指定したパラメータでこのコマンドがエリアを作成します。

例

次に、スタブまたは NSSA に送信される集約ルートのデフォルト コストを指定する例を示します。

```
ciscoasa(config-router)# area 1 default-cost 5
ciscoasa(config-router)#
```

関連コマンド

コマンド	説明
area nssa	(任意)エリアを Not-So-Stubby Area として定義します。
area stub	エリアをスタブ エリアとして定義します。
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area filter-list prefix

ABR の OSPFv2 エリア間のタイプ 3 LSA でアドバタイズされたプレフィックスをフィルタリングするには、ルータ コンフィギュレーション モードで **area filter-list prefix** コマンドを使用します。フィルタを変更またはキャンセルするには、このコマンドの **no** 形式を使用します。

area *area_id* **filter-list prefix** *list_name* {**in** | **out**}

no area *area_id* **filter-list prefix** *list_name* {**in** | **out**}

構文の説明

area_id	フィルタリングを設定するエリアを識別します。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
in	指定したエリアに着信するアドバタイズされたプレフィックスに、設定済みプレフィックス リストを適用します。
list_name	プレフィックス リストの名前を指定します。
out	指定したエリアから発信されるアドバタイズされたプレフィックスに、設定済みプレフィックス リストを適用します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードはサポートされます。

使用上のガイドライン

指定したエリアが **area** コマンドを使用して過去に定義されていない場合は、指定したパラメータでこのコマンドがエリアを作成します。

フィルタリングできるのはタイプ 3 LSA だけです。プライベート ネットワークに ASBR が設定されている場合、ASBR はプライベート ネットワークを記述するタイプ 5 LSA を送信します。この LSA は、パブリック エリアを含む AS 全体にフラッディングされます。

例

次に、他のすべてのエリアからエリア 1 に送信されるプレフィックスをフィルタリングする例を示します。

```
ciscoasa(config-router)# area 1 filter-list prefix-list AREA_1 in
ciscoasa(config-router)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area nssa

エリアを NSSA として設定するには、ルータ コンフィギュレーション モードまたは IPv6 ルータ コンフィギュレーション モードで **area nssa** コマンドを使用します。NSSA 指定をエリアから削除するには、このコマンドの **no** 形式を使用します。

area *area_id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric-type** {**1** | **2**}] [**metric** *value*]] [**no-summary**]

no area *area_id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric-type** {**1** | **2**}] [**metric** *value*]] [**no-summary**]

構文の説明

area_id	NSSA として指定するエリアを識別します。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
default-information-originate	NSSA エリアでのタイプ 7 デフォルトの生成に使用します。このキーワードは、NSSA ABR または NSSA ASBR でのみ有効です。
metric *metric_value*	（任意）OSPF デフォルト メトリック値を指定します。有効値の範囲は 0 ～ 16777214 です。
metric-type {**1** | **2**}	（任意）デフォルト ルートの OSPF メトリック タイプ。有効な値は次のとおりです。 • **1**: タイプ 1 • **2**: タイプ 2 デフォルト値は 2 です。
no-redistribution	（任意）ルータが NSSA ABR の場合、**redistribute** コマンドを使用して、ルートを NSSA エリアでなく通常のエリアにのみ取り込む場合に使用します。
no-summary	（任意）エリアを Not-So-Stubby Area（NSSA）とし、集約ルートが挿入されないようにします。

デフォルト

デフォルトの設定は次のとおりです。

- NSSA エリアは未定義です。
- **metric-type** は 2 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—
IPv6 ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードおよび OSPFv3 がサポートされています。

使用上のガイドライン

指定したエリアが **area** コマンドを使用して過去に定義されていない場合は、指定したパラメータでこのコマンドがエリアを作成します。

エリアに 1 つのオプションを設定し、後で別のオプションを指定した場合、両方のオプションが設定されます。たとえば、次の 2 のコマンドを別々に入力した場合、コンフィギュレーションには、両方のオプションを指定した 1 つのコマンドが設定されます。

```
ciscoasa(config-rtr)# area 1 nssa no-redistribution
ciscoasa(config-rtr)# area area_id nssa default-information-originate
```

例

次に、2 つのオプションを別々に設定すると、1 つのコマンドがコンフィギュレーションに設定される例を示します。

```
ciscoasa(config-rtr)# area 1 nssa no-redistribution
ciscoasa(config-rtr)# area 1 nssa default-information-originate
ciscoasa(config-rtr)# exit
ciscoasa(config-rtr)# show running-config router ospf 1
router ospf 1
 area 1 nssa no-redistribution default-information-originate
```

関連コマンド

コマンド	説明
area stub	エリアをスタブ エリアとして定義します。
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area-password

IS-IS エリア認証パスワードを設定するには、ルータ ISIS コンフィギュレーション モードで、**area-password** コマンドを使用します。パスワードをディセーブルにするには、このコマンドの **no** 形式を使用します。

area-password *password* [**authenticate snp** {**validate** | **send-only**}]

no area-password [*password*]

構文の説明

password	割り当てるパスワード。
authenticate snp	（任意）これを指定すると、システムはシーケンス番号 PDUS（SNP）にパスワードを挿入するようになります。
validate	これを指定すると、システムはパスワードを SNP に挿入し、受け取ったパスワードを SNP で確認するようになります。
send-only	これを指定すると、システムは SNP へのパスワードの挿入だけは行うようになりますが、SNP での受け取ったパスワードの確認は行われません。このキーワードは、ソフトウェアのアップグレード中、移行をスムーズに行うために使用します。

デフォルト

エリア パスワードは定義されていません。また、エリア パスワードの認証はディセーブルにされています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ isis コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

あるエリアに存在するすべてのルータで **area-password** コマンドを使用することにより、不正ルータによる、リンクステート データベースへの誤ったルーティング情報の挿入を阻止できます。

このパスワードはプレーン テキストとしてやり取りされるため、この機能が提供するセキュリティは限定されています。

このパスワードは、レベル 1（ステーション ルータ レベル）の PDU リンクステート パケット（LSP）、Complete Sequence Number PDU（CSNP）、および Partial Sequence Number PDU（PSNP）に挿入されます。

authenticate snp キーワードを指定して、**validate** または **send-only** キーワードを指定しなかった場合、IS-IS ルーティング プロトコルは SNP にパスワードを挿入しません。

例

次に、エリア認証パスワードを割り当て、このパスワードを SNP に挿入し、システムが受け取った SNP で確認するように指定する例を示します。

```
ciscoasa(config-router)# router isis
ciscoasa(config-router)# area-password track authenticate snp validate
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。

コマンド	説明
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト(TLV)を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。

コマンド	説明
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

area range（IPv6 ルータ OSPF）

エリア境界で OSPFv3 ルートを統合および集約するには、IPv6 ルータ OSPF コンフィギュレーション モードで **area range** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

area *area_id* **range** *ipv6-prefix/prefix-length* [**advertise** | **not-advertise**] [**cost** *cost*]

no area *area_id* **range** *ipv6-prefix/prefix-length* [**advertise** | **not-advertise**] [**cost** *cost*]

構文の説明

advertise	（オプション）Type 3 サマリー LSA をアドバタイズおよび生成するように、範囲ステータスを設定します。
area_id	ルートを要約するエリアの ID を指定します。10 進数または IPv6 プレフィックスのいずれかを使用して ID を指定できます。
cost *cost*	（オプション）このサマリー ルートのメトリックまたはコストを指定します。宛先への最短パスを決定するための OSPF SPF 計算で使用します。有効値の範囲は 0 ～ 16777215 です。
ipv6-prefix	IPv6 プレフィックスを指定します。
not-advertise	（オプション）範囲ステータスを DoNotAdvertise に設定します。Type 3 サマリー LSA は抑制され、コンポーネント ネットワークは他のネットワークから隠された状態のままです。
prefix-length	IPv6 プレフィックス長を指定します。

デフォルト

範囲ステータスはデフォルトで advertise に設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
IPv6 ルータ OSPF コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

指定したエリアが **area** コマンドを使用して過去に定義されていない場合は、指定したパラメータでこのコマンドがエリアを作成します。

area range コマンドは、ABR でのみ使用されます。このコマンドによって、エリアのルートが統合または集約されます。その結果、1 つの集約ルートが ABR によって他のエリアにアドバタイズされます。ルーティング情報は、エリア境界でまとめられます。エリアの外部では、IPv6 プレフィックスおよびプレフィックス長ごとに 1 つのルートがアドバタイズされます。この動作は *ルート集約*と呼ばれます。1 つのエリアに複数の **area range** コマンドを設定できます。このように、OSPFv3 は多くの異なる IPv6 プレフィックスおよびプレフィックス長セットのルートを集約できます。

例

次に、IPv6 プレフィックスが 2000:0:0:4::2 でプレフィックス長が 2001::/64 の他のエリアに ABR によってアドバタイズされる 1 つの集約ルートを指定する例を示します。

```
ciscoasa(config-router)# area 1 range 2000:0:0:4::2/2001::/64
ciscoasa(config-router)#
```

関連コマンド

コマンド	説明
ipv6 router ospf	OSPFv3 の IPv6 ルータ コンフィギュレーション モードを開始します。
show running-config ipv6 router	グローバル ルータ コンフィギュレーションの IPv6 コマンドを表示します。

area range（ルータ OSPF）

エリア境界で ルートを統合および集約するには、ルータ OSPF コンフィギュレーション モードで **area range** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

area *area_id* **range** *address mask* [**advertise** | **not-advertise**]

no area *area_id* **range** *address mask* [**advertise** | **not-advertise**]

構文の説明

address	サブネット範囲の IP アドレス。
advertise	（任意）Type 3 サマリー LSA をアドバタイズおよび生成するように、アドレス範囲ステータスを設定します。
area_id	範囲を設定するエリアを識別します。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
mask	IP アドレスのサブネット マスク。
not-advertise	（任意）アドレス範囲ステータスを DoNotAdvertise に設定します。Type 3 サマリー LSA は抑制され、コンポーネント ネットワークは他のネットワークから隠された状態のままです。

デフォルト

アドレス範囲ステータスは advertise に設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ OSPF コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードはサポートされます。

使用上のガイドライン

指定したエリアが **area** コマンドを使用して過去に定義されていない場合は、指定したパラメータでこのコマンドがエリアを作成します。

area range コマンドは、エリアのルートを統合または集約するために ABR でのみ使用します。その結果、1 つの集約ルートが ABR によって他のエリアにアドバタイズされます。ルーティング情報は、エリア境界でまとめられます。エリアの外部では、アドレス範囲ごとに 1 つのルートがアドバタイズされます。この動作は*ルート集約*と呼ばれます。1 つのエリアに複数の **area range** コマンドを設定できます。このように、OSPF は多くの異なるアドレス範囲セットのアドレスを集約できます。

no area *area_id* **range** *ip_address netmask* **not-advertise** コマンドは、**not-advertise** オプション キーワードのみを削除します。

例

次に、ネットワーク 10.0.0.0 上のすべてのサブネットおよびネットワーク 192.168.110.0 上のすべてのホストに対する 1 つの集約ルートを、ABR によって他のエリアにアドバタイズするように指定する例を示します。

```
ciscoasa(config-router)# area 10.0.0.0 range 10.0.0.0 255.0.0.0
ciscoasa(config-router)# area 0 range 192.168.110.0 255.255.255.0
ciscoasa(config-router)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area stub

エリアをスタブ エリアとして定義するには、ルータ コンフィギュレーション モードまたは IPv6 ルータ コンフィギュレーション モードで **area stub** コマンドを使用します。スタブ エリアを削除するには、このコマンドの **no** 形式を使用します。

area *area_id* **stub** [**no-summary**]

no area *area_id* **stub** [**no-summary**]

構文の説明

area_id	スタブ エリアを識別します。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
no-summary	ABR がサマリー リンク アドバタイズメントをスタブ エリアに送信しないようにします。

デフォルト

デフォルトの動作は次のとおりです。

- スタブ エリアは定義されません。
- サマリー リンク アドバタイズメントはスタブ エリアに送信されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	—	—
IPv6 ルータ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	OSPFv3 のサポートが追加されました。

使用上のガイドライン

このコマンドは、スタブまたは NSSA に接続された ABR でのみ使用されます。

スタブ エリア ルータ コンフィギュレーション コマンドには、**area stub** および **area default-cost** という 2 つのコマンドがあります。スタブ エリアに接続されているすべてのルータおよびアクセス サーバで、**area stub** コマンドを使用して、エリアをスタブ エリアとして設定する必要があります。スタブ エリアに接続された ABR でのみ **area default-cost** コマンドを使用します。**area default-cost** コマンドは、ABR によって生成される集約デフォルト ルートのメトリックをスタブ エリアに提供します。

例

次に、指定したエリアをスタブ エリアとして設定する例を示します。

```
ciscoasa(config-rtr)# area 1 stub
ciscoasa(config-rtr)#
```

関連コマンド

コマンド	説明
area default-cost	スタブまたは NSSA に送信されるデフォルト サマリー ルートのコストを指定します。
area nssa	(任意)エリアを Not-So-Stubby Area として定義します。
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

area virtual-link（IPv6 ルータ OSPF）

OSPFv3 仮想リンクを定義するには、IPv6 ルータ OSPF コンフィギュレーション モードで **area virtual-link** コマンドを使用します。オプションをリセットするか、または仮想リンクを削除するには、このコマンドの **no** 形式を使用します。

area *area_id* **virtual-link** *router_id* [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] [**ttl-security hops** *hop-count*]

no area *area_id* **virtual-link** *router_id* [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] [**ttl-security hops** *hop-count*]

構文の説明

area_id	仮想リンクの中継エリアのエリア ID を指定します。10 進数または有効な IPv6 プレフィックスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
hello-interval *seconds*	（オプション）ASA がインターフェイスで送信する hello パケットの間隔を秒単位で指定します。hello 間隔は、hello パケットでアドバタイズされる符号なし整数値です。この値は、共通のネットワークに接続されているすべてのルータおよびアクセス サーバで同じであることが必要です。有効な値の範囲は、1 ～ 8192 秒です。
retransmit-interval *seconds*	（オプション）インターフェイスに属する隣接ルータの LSA 再送信間の時間を秒単位で指定します。再送信間隔は、接続されているネットワーク上の任意の 2 台のルータ間の予想されるラウンドトリップ遅延です。この値は、予想されるラウンドトリップ遅延よりも大きいことが必要です。有効な値の範囲は、1 ～ 8192 秒です。
router_id	仮想リンク ネイバーに関連付けられているルータ ID を指定します。ルータ ID は、**show ipv6 ospf** コマンドまたは **show ipv6 display** コマンドで表示されます。
transmit-delay *seconds*	（オプション）インターフェイス上でリンクステート アップデート パケットを送信するために必要な推定される時間を秒単位で指定します。ゼロよりも大きい整数値を指定します。アップデート パケット内の LSA の経過時間は、転送前にこの値の分だけ増分されます。有効な値の範囲は、1 ～ 8192 秒です。
dead-interval *seconds*	（オプション）hello パケットがどれだけの時間（秒単位）届かなかった場合にネイバーがルータのダウンを示すかを指定します。デッド インターバルは符号なし整数値です。hello 間隔と同様に、この値は、共通のネットワークに接続されているすべてのルータとアクセス サーバで同じでなければなりません。有効値の範囲は 1 ～ 8192 秒です。
ttl-security hops *hop-count*	（オプション）仮想リンク上で存続可能時間（TTL）セキュリティを設定します。ホップ カウントの有効な値の範囲は 1 ～ 254 です。

（注） 1 桁のパスワードおよび先頭の数字の後に空白が続くパスワードはサポートされなくなりました。

デフォルト

デフォルトの設定は次のとおりです。

- *area_id*:エリア ID は事前に定義されていません。
- *router_id*:ルータ ID は事前に定義されていません。
- **hello-interval**:10 秒です。
- **retransmit-interval**:5 秒です。
- **transmit-delay**:1 秒です。
- **dead-interval**:40 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
IPv6 ルータ OSPF コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

OSPFv3 では、すべてのエリアはバックボーン エリアに接続している必要があります。バックボーンへの接続が失われた場合は、仮想リンクを確立して修復できます。

hello パケットの間隔が短い場合、トポロジ変化の検出が速くなりますが、ルーティング トラフィックが多くなります。

再送信間隔の設定値はあまり小さくしないでください。小さくすると、不要な再送信が行われます。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。

送信遅延の値では、インターフェイスの送信遅延と伝搬遅延を考慮に入れる必要があります。

(注) 仮想リンクを正しく設定するには、各仮想リンク ネイバーに、中継エリア ID および対応する仮想リンク隣接ルータ ID が含まれている必要があります。ルータ ID を取得するには、**show ipv6 ospf** コマンドを使用します。

例

次に、OSPFv3 で仮想リンクを確立する例を示します。

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# log-adjacency-changes
ciscoasa(config-rtr)# area 1 virtual-link 192.168.255.1 hello interval 5
```

area virtual-link（ルータ OSPF）

OSPF 仮想リンクを定義するには、ルータ OSPF コンフィギュレーション モードで **area virtual-link** コマンドを使用します。オプションをリセットするか、または仮想リンクを削除するには、このコマンドの **no** 形式を使用します。

area *area_id* **virtual-link** *router_id* [**authentication** [**key-chain** *key-chain-name* | **message-digest** | **null**]] [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds* [[[[**authentication-key[0 | 8]** *key*] | [**message-digest-key** *key_id* **md5 [0 | 8]** *key*]]]]

no area *area_id* **virtual-link** *router_id* [**authentication** [**key-chain** *key-chain-name* | **message-digest** | **null**]] [**hello-interval** *seconds*] [**retransmit-interval** seconds] [**transmit-delay** *seconds*] [**dead-interval** *seconds* [[[[**authentication-key [0 | 8]** *key*] | [**message-digest-key** *key_id* **md5 [0 | 8]** *key*]]]]

構文の説明

area_id	仮想リンクの中継エリアのエリア ID。10 進数または IP アドレスのいずれかを使用して ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
authentication	（任意）認証タイプを指定します。
key-chain ***key-chain-name***	（任意）認証に使用するキー チェーンを指定します。key-name 引数には最大 63 文字の英数字を指定できます。
authentication-key [0 | 8]*key*	（任意）ネイバー ルーティング デバイスで使用する OSPF 認証パスワードを指定します。
dead-interval *seconds*	（任意）hello パケットを受信しない場合に、ネイバー ルーティング デバイスがダウンしたことを宣言するまでの間隔を指定します。有効な値は、1 ～ 65535 秒です。
hello-interval *seconds*	（任意）インターフェイスで送信される hello パケット間の間隔を指定します。有効な値は、1 ～ 65535 秒です。
md5 [0 | 8] *key*	（任意）最大 16 バイトの英数字のキーを指定します。
message-digest	（任意）メッセージ ダイジェスト認証を使用することを指定します。
message-digest-key *key_id*	（任意）Message Digest 5（MD5）認証をイネーブルにし、認証キー ID 番号を指定します。有効な値は、1 ～ 255 です。
0	暗号化されていないパスワードが続くことを指定します。
8	暗号化されたパスワードが後に続くことを指定します。
null	（任意）認証を使用しないことを指定します。パスワードまたはメッセージ ダイジェスト認証は、OSPF エリアに設定されている場合、上書きされます。
retransmit-interval *seconds*	（任意）インターフェイスに属している隣接ルータの LSA 再送信の間隔を指定します。有効な値は、1 ～ 65535 秒です。
router_id	仮想リンク ネイバーに関連付けられているルータ ID。ルータ ID は、各ルータによって内部でインターフェイス IP アドレスから生成されます。この値は、IP アドレスの形式で入力する必要があります。デフォルトはありません。
transmit-delay *seconds*	（任意）OSPF がトポロジ変更を受信してから、Shortest Path First（SPF）計算を開始するまでの遅延時間を 0 ～ 65535 秒で指定します。デフォルトは 5 秒です。

(注) 1 桁のパスワードおよび先頭の数字の後に空白が続くパスワードはサポートされなくなりました。

デフォルト

デフォルトの設定は次のとおりです。

- *area_id*:エリア ID は事前に定義されていません。
- *router_id*:ルータ ID は事前に定義されていません。
- **hello-interval** *seconds*:10 秒。
- **retransmit-interval** *seconds*:5 秒。
- **transmit-delay** *seconds*:1 秒。
- **dead-interval** *seconds*:40 秒。
- **authentication-key [0 | 8]** *key*:キーは事前に定義されていません。
- **message-digest-key** *key_id* **md5 [0 | 8]** *key*:キーは事前に定義されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ OSPF コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.12(1)	OSPF 認証のローテーション キーをサポートするためにキー チェーン機能が追加されました。

使用上のガイドライン

OSPF では、すべてのエリアがバックボーン エリアに接続されている必要があります。バックボーンへの接続が失われた場合は、仮想リンクを確立して修復できます。

hello 間隔を小さくすればするほど、トポロジ変更の検出が速くなりますが、ルーティング トラフィックが増加します。

再送信間隔の設定値はあまり小さくしないでください。小さくすると、不要な再送信が行われます。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。

送信遅延の値では、インターフェイスの送信遅延と伝搬遅延を考慮に入れる必要があります。

指定した認証キーは、**area** *area_id* **authentication** コマンドでバックボーンに対して認証がイネーブルにされている場合にのみ使用されます。

簡易テキスト認証と MD5 認証という 2 つの認証方式は、相互排他的です。どちらか一方を指定するか、または両方とも指定しないでください。**authentication-key [0 | 8]** *key* または **message-digest-key** *key_id* **md5[0 | 8]** *key* の後に指定したキーワードと引数はすべて無視されます。したがって、オプションの引数は、これらのキーワードと引数の組み合わせの前に指定します。

インターフェイスに認証タイプが指定されていない場合、インターフェイスでは、エリアに指定されている認証タイプが使用されます。エリアに認証タイプが指定されていない場合、エリアのデフォルトはヌル認証です。

(注) 仮想リンクを正しく設定するには、各仮想リンク ネイバーに、中継エリア ID および対応する仮想リンク ネイバー ルータ ID が含まれている必要があります。ルータ ID を表示するには、**show ospf** コマンドを使用します。

例

次に、MD5 認証の仮想リンクを確立する例を示します。

```
ciscoasa(config-rtr)# area 10.0.0.0 virtual-link 10.3.4.5 message-digest-key 3 md5 8
sa5721bk47
```

次に、ローテーション キー認証で仮想リンクを確立する例を示します。

```
ciscoasa(config-rtr)# area 10.0.0.0 virtual-link 10.3.4.5 authentication key-chain
CHAIN-RTR-OSPFKEYS
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show ospf	OSPF ルーティング プロセスに関する一般情報を表示します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

関連コマンド

コマンド	説明
ipv6 router ospf	OSPFv3 のルータ コンフィギュレーション モードを開始します。
show ipv6 ospf	OSPFv3 ルーティング プロセスに関する一般情報を表示します。
show running-config ipv6 router	グローバル ルータ コンフィギュレーションの IPv6 コマンドを表示します。

arp

スタティック ARP エントリを ARP テーブルに追加するには、グローバル コンフィギュレーション モードで **arp** コマンドを使用します。スタティック エントリを削除するには、このコマンドの **no** 形式を使用します。

arp *interface_name ip_address mac_address* [**alias**]

no arp *interface_name ip_address mac_address*

構文の説明

alias	(任意)このマッピングに対してプロキシ ARP をイネーブルにします。ASA は、指定された IP アドレスに対する ARP 要求を受信すると、ASA の MAC アドレスで応答します。その IP アドレスを持つホスト宛てのトラフィックを ASA が受信すると、ASA は、トラフィックをこのコマンドで指定されたホスト MAC アドレスに転送します。このキーワードは、ARP を実行しないデバイスがある場合などに役立ちます。 トランスペアレント ファイアウォール モードでは、このキーワードは無視され、ASA でプロキシ ARP は実行されません。
interface_name	ホスト ネットワークに接続されているインターフェイス。
ip_address	ホストの IP アドレス。
mac_address	ホストの MAC アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ホストは IP アドレスでパケットの宛先を識別しますが、イーサネットにおける実際のパケット配信は、イーサネット MAC アドレスに依存します。ルータまたはホストは、直接接続されたネットワークでパケットを配信する必要がある場合、IP アドレスに関連付けられた MAC アドレスを要求する ARP 要求を送信し、ARP 応答に従ってパケットを MAC アドレスに配信します。ホストまたはルータには ARP テーブルが保管されるため、配信が必要なパケットごとに ARP 要求を送信する必要はありません。ARP テーブルは、ARP 応答がネットワーク上で送信されるたびにダイナミックに更新されます。一定期間使用されなかったエントリは、タイムアウトします。エントリが正しくない場合（たとえば、所定の IP アドレスの MAC アドレスが変更された場合など）、エントリは更新される前にタイムアウトします。

スタティック ARP エントリは、MAC アドレスを IP アドレスにマッピングし、ホストに到達するまでに通過するインターフェイスを指定します。スタティック ARP エントリはタイムアウトせず、ネットワーク問題の解決に役立つ場合があります。トランスペアレント ファイアウォール モードでは、ARP インスペクションでスタティック ARP テーブルが使用されます（**arp-inspection** コマンドを参照）。

（注） トランスペアレント ファイアウォール モードでは、ダイナミック ARP エントリが ASA との間のトラフィック（管理トラフィックなど）に使用されます。

例

次に、外部インターフェイス上の 10.1.1.1 と MAC アドレス 0009.7cbe.2100 のスタティック ARP エントリを作成する例を示します。

```
ciscoasa(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

関連コマンド

コマンド	説明
arp timeout	ASA が ARP テーブルを再構築するまでの時間を設定します。
arp-inspection	トランスペアレント ファイアウォール モードで、ARP パケットを調査し、ARP スプーフィングを防止します。
show arp	ARP テーブルを表示します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

arp-inspection

トランスペアレント ファイアウォール モードでの ARP インスペクションをイネーブルにするには、グローバル コンフィギュレーション モードで **arp-inspection** コマンドを使用します。ARP インスペクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

arp-inspection *interface_name* **enable** [**flood** | **no-flood**]

no arp-inspection *interface_name* **enable**

構文の説明

enable	ARP インスペクションをイネーブルにします。
flood	(デフォルト)スタティック ARP エントリのどの要素とも一致しないパケットをすべてのインターフェイス(発信元インターフェイスを除く)にフラッディングすることを指定します。MAC アドレス、IP アドレス、またはインターフェイス間で不一致がある場合、ASA はパケットをドロップします。 (注) 管理専用のインターフェイス(存在する場合)は、このパラメータが flood に設定されている場合でもパケットをフラッディングしません。
interface_name	ARP インスペクションをイネーブルにするブリッジ グループ メンバー インターフェイス。
no-flood	(任意)スタティック ARP エントリと正確には一致しないパケットをドロップすることを指定します。

デフォルト

デフォルトでは、ARP インスペクションはすべてのインターフェイスでディセーブルになっています。すべての ARP パケットは ASA を通過できます。ARP インスペクションをイネーブルにすると、一致しない ARP パケットはデフォルトでフラッディングされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.7(1)	Integrated Routing and Bridging(IRB; 統合ルーティングおよびブリッジング)を使用するときに、ルーテッド モードでこのコマンドを設定できるようになりました。

使用上のガイドライン

ARP インスペクションをイネーブルにする前に、**arp** コマンドを使用してスタティック ARP エントリを設定します。

ARP インスペクションでは、すべての ARP パケットをスタティック ARP エントリと照合し（**arp** コマンドを参照）、一致しないパケットをブロックします。この機能により、ARP スプーフィングが防止されます。

ARP インスペクションをイネーブルにすると、ASA は、すべての ARP パケット内の MAC アドレス、IP アドレス、および送信元インターフェイスを ARP テーブル内のスタティック エントリと比較し、次のアクションを実行します。

- IP アドレス、MAC アドレス、および送信元インターフェイスが ARP エントリと一致する場合、パケットを通過させます。
- MAC アドレス、IP アドレス、またはインターフェイス間で不一致がある場合、ASA はパケットをドロップします。
- ARP パケットがスタティック ARP テーブル内のどのエントリとも一致しない場合、パケットをすべてのインターフェイスに転送（フラッディング）するか、またはドロップするように ASA を設定できます。

（注） 専用の管理インターフェイス（存在する場合）は、このパラメータが flood に設定されている場合でもパケットをフラッディングしません。

ARP インスペクションによって、悪意のあるユーザが他のホストやルータになりすます（ARP スプーフィングと呼ばれる）のを防止できます。ARP スプーフィングが許可されていると、「中間者」攻撃を受けることがあります。たとえば、ホストが ARP 要求をゲートウェイ ルータに送信すると、ゲートウェイ ルータはゲートウェイ ルータの MAC アドレスで応答します。ただし、攻撃者は、ルータの MAC アドレスではなく攻撃者の MAC アドレスで別の ARP 応答をホストに送信します。これで、攻撃者は、すべてのホスト トラフィックを代行受信してルータに転送できるようになります。

ARP インスペクションを使用すると、正しい MAC アドレスとそれに関連付けられた IP アドレスがスタティック ARP テーブル内にある場合、攻撃者は攻撃者の MAC アドレスで ARP 応答を送信できなくなります。

（注） トランスペアレント ファイアウォール モードでは、ダイナミック ARP エントリが ASA との間のトラフィック（管理トラフィックなど）に使用されます。

例

次に、外部インターフェイスにおける ARP インスペクションをイネーブルにし、スタティック ARP エントリに一致しない ARP パケットをドロップするように ASA を設定する例を示します。

```
ciscoasa(config)# arp outside 209.165.200.225 0009.7cbe.2100
ciscoasa(config)# arp-inspection outside enable no-flood
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
clear configure arp-inspection	ARP インスペクション コンフィギュレーションをクリアします。
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。

コマンド	説明
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

arp permit-nonconnected

非直接接続サブネットも含まれるように ARP キャッシュをイネーブルにするには、グローバル コンフィギュレーション モードで **arp permit-nonconnected** コマンドを使用します。非直接接続サブネットをディセーブルにするには、このコマンドの **no** 形式を使用します。

arp permit-nonconnected

no arp permit-nonconnected

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.4(5)、9.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASA ARP キャッシュには、直接接続されたサブネットからのエントリだけがデフォルトで含まれています。**no arp permit-nonconnected** コマンドがあり（デフォルト動作）、受信した ARP パケットが接続されているインターフェイスとは別のサブネットに存在する場合は、ASA によって着信 ARP 要求も ARP 応答も拒否されます。

最初のケース（デフォルト動作）では、PAT が ASA で設定され、PAT の仮想 IP アドレス（マップ済み）が接続されているインターフェイスとは別のサブネットに存在する場合に障害が発生します。

また、セキュリティ リスクを認識していない場合は、この機能をイネーブルにすることは推奨しません。この機能は、ASA に対するサービス拒否（DoS）攻撃を助長する場合があります。任意のインターフェイスのユーザが大量の ARP 応答を送信して、偽エントリで ASA ARP テーブルがあふれる可能性があります。

次の機能を使用する場合は、この機能を使用する必要がある可能性があります。

- セカンデリ サブネット。
- トラフィック転送の隣接ルートのプロキシ ARP。

例

次に、非接続サブネットをイネーブルにする例を示します。

```
ciscoasa(config)# arp permit non-connected
```

デフォルトの動作は、ASA の **debug arp** コマンドの出力で次のように確認できます。

着信 ARP 要求の場合:

```
- larp-in: request at outside from 10.10.2.1 0013.8083.0bb1 for 10.10.2.2 0000.0000.0000
having smac 0013.8083.0bb1 dmac ffff.ffff.ffff\narp-in: Arp packet received from 10.10.2.1
which is in different subnet than the connected interface 10.10.1.2/255.255.255.0
```

着信 ARP 応答の場合:

次に、非接続サブネットをイネーブルにする例を示します。

```
ciscoasa(config)# arp permit non-connected
- arp-in: response at outside from 10.10.2.1 0013.8083.0bb1 for 10.10.1.2 0016.4687.9f43
having smac 0013.8083.0bb1 dmac 0016.4687.9f43\narp-in: Arp packet received from 10.10.2.1
which is in different subnet than the connected interface 10.10.1.2/255.255.255.0
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。

arp rate-limit

ARP レート制限を設定して 1 秒あたりの ARP パケット数を制御するには、グローバル コンフィギュレーション モードで **arp rate-limit** コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

arp rate-limit *seconds*

no arp rate-limit

構文の説明

seconds	秒数を 10 ～ 32768 の間で指定します。デフォルト値は ASA モデルによって異なります。

コマンド デフォルト

デフォルト値は ASA モデルによって異なります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

この値は ARP ストーム攻撃を防ぐためにカスタマイズできます。

例

次に、ARP レートを 1 秒あたり 10000 に設定する例を示します。

```
ciscoasa(config)# arp rate-limit 10000
```

関連コマンド

コマンド	説明
show arp rate-limit	ARP レート制限を表示します。

arp timeout

ASA が ARP テーブルを再構築するまでの時間を設定するには、グローバル コンフィギュレーション モードで **arp timeout** コマンドを使用します。デフォルトのタイムアウトに戻すには、このコマンドの **no** 形式を使用します。

arp timeout *seconds*

no arp timeout *seconds*

構文の説明

seconds	ARP テーブルを再構築する間隔の秒数（60 ～ 4294967）。

デフォルト

デフォルト値は 14,400 秒（4 時間）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ARP テーブルを再構築すると、自動的に新しいホスト情報が更新され、古いホスト情報が削除されます。ホスト情報は頻繁に変更されるため、タイムアウトを短くすることが必要になる場合があります。

例

次に、ARP タイムアウトを 5,000 秒に変更する例を示します。

```
ciscoasa(config)# arp timeout 5000
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	トランスペアレント ファイアウォール モードで、ARP パケットを調査し、ARP スプーフィングを防止します。

コマンド	説明
show arp statistics	ARP 統計情報を表示します。
show running-config arp timeout	ARP タイムアウトの現在のコンフィギュレーションを表示します。

asdm disconnect

アクティブな ASDM セッションを終了するには、特権 EXEC モードで **asdm disconnect** コマンドを使用します。

asdm disconnect *session*

構文の説明

session	終了するアクティブな ASDM セッションのセッション ID。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	**pdm disconnect** コマンドが **asdm disconnect** コマンドに変更されました。

使用上のガイドライン

アクティブな ASDM セッションとそれに関連付けられているセッション ID のリストを表示するには、**show asdm sessions** コマンドを使用します。特定のセッションを終了するには、**asdm disconnect** コマンドを使用します。

ASDM セッションを終了しても、残りのアクティブな ASDM セッションは、関連付けられているセッション ID を保持します。たとえば、3 つのアクティブな ASDM セッションがあり、それぞれのセッション ID が 0、1、および 2 の場合、セッション 1 を終了すると、残りのアクティブな ASDM セッションはそれぞれセッション ID 0 と 2 を保持します。この例で、次の新しい ASDM セッションにはセッション ID 1 が割り当てられ、その後の新しいセッションにはセッション ID 3 から順に ID が割り当てられます。

例

次に、セッション ID 0 の ASDM セッションを終了する例を示します。**asdm disconnect** コマンドの入力の前後に、**show asdm sessions** コマンドを使用して、アクティブな ASDM セッションを表示しています。

```
ciscoasa# show asdm sessions

0 192.168.1.1
1 192.168.1.2
ciscoasa# asdm disconnect 0
```

```
ciscoasa# show asdm sessions

1 192.168.1.2
```

関連コマンド

コマンド	説明
show asdm sessions	アクティブな ASDM セッションとそれに関連付けられているセッション ID のリストを表示します。

asdm disconnect log_session

アクティブな ASDM ロギング セッションを終了するには、特権 EXEC モードで **asdm disconnect log_session** コマンドを使用します。

asdm disconnect log_session *session*

構文の説明

session	終了するアクティブな ASDM ロギング セッションのセッション ID。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

アクティブな ASDM ロギング セッションとそれに関連付けられているセッション ID のリストを表示するには、**show asdm log_sessions** コマンドを使用します。特定のロギング セッションを終了するには、**asdm disconnect log_session** コマンドを使用します。

それぞれのアクティブな ASDM セッションには、1 つ以上の関連する ASDM ロギング セッションがあります。ASDM は、ロギング セッションを使用して、ASA から Syslog メッセージを取得します。ログ セッションを終了すると、アクティブな ASDM セッションに悪影響が及ぶ場合があります。不要な ASDM セッションを終了するには、**asdm disconnect** コマンドを使用します。

（注） 各 ASDM セッションには少なくとも 1 つの ASDM ロギング セッションがあるため、**show asdm sessions** および **show asdm log_sessions** の出力は同じように見えることがあります。

ASDM ロギング セッションを終了しても、残りのアクティブな ASDM ロギング セッションは、関連付けられているセッション ID を保持します。たとえば、3 つのアクティブな ASDM ロギング セッションがあり、それぞれのセッション ID が 0、1、および 2 の場合、セッション 1 を終了すると、残りのアクティブな ASDM ロギング セッションはそれぞれセッション ID 0 と 2 を保持します。この例で、次の新しい ASDM ロギング セッションにはセッション ID 1 が割り当てられ、その後の新しいロギング セッションにはセッション ID 3 から順に ID が割り当てられます。

例

次に、セッション ID 0 の ASDM セッションを終了する例を示します。**asdm disconnect log_sessions** コマンドの入力の前後に、**show asdm log_sessions** コマンドを使用して、アクティブな ASDM セッションを表示しています。

```
ciscoasa# show asdm log_sessions

0 192.168.1.1
1 192.168.1.2
ciscoasa# asdm disconnect 0
ciscoasa# show asdm log_sessions

1 192.168.1.2
```

関連コマンド

コマンド	説明
show asdm log_sessions	アクティブな ASDM ロギング セッションとそれに関連付けられているセッション ID のリストを表示します。

asdm history enable

ASDM 履歴トラッキングをイネーブルにするには、グローバル コンフィギュレーション モードで **asdm history enable** コマンドを使用します。ASDM 履歴トラッキングをディセーブルにするには、このコマンドの **no** 形式を使用します。

asdm history enable

no asdm history enable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	**pdm history enable** コマンドが **asdm history enable** コマンドに変更されました。

使用上のガイドライン

ASDM 履歴トラッキングをイネーブルにすることによって取得された情報は、ASDM 履歴バッファに保存されます。この情報は、**show asdm history** コマンドを使用して表示できます。履歴情報は、ASDM によってデバイス モニタリングに使用されます。

例

次に、ASDM 履歴トラッキングをイネーブルにする例を示します。

```
ciscoasa(config)# asdm history enable
ciscoasa(config)#
```

関連コマンド

コマンド	説明
show asdm history	ASDM 履歴バッファの内容を表示します。

asdm image

フラッシュ メモリ内の ASDM ソフトウェア イメージの場所を指定するには、グローバル コンフィギュレーション モードで **asdm image** コマンドを使用します。イメージの場所を削除するには、このコマンドの **no** 形式を使用します。

asdm image *url*

no asdm image [*url*]

構文の説明

url	フラッシュ メモリ内の ASDM イメージの場所を設定します。次の URL 構文を参照してください。 • **disk0:/**[*path*/]*filename* ASA 5500 シリーズでは、この URL は内部フラッシュ メモリを示します。**disk0** ではなく **flash** を使用することもできます。これらはエイリアスになっています。 • **disk1:/**[*path*/]*filename* ASA 5500 シリーズでは、この URL は外部フラッシュ メモリ カードを示します。 • **flash:/**[*path*/]*filename* この URL は内部フラッシュ メモリを示します。

デフォルト

このコマンドをスタートアップ コンフィギュレーションに含めない場合、ASA は起動時に最初に検出した ASDM イメージを使用します。内部フラッシュ メモリのルート ディレクトリ内を検索した後で、外部フラッシュ メモリを検索します。ASA はイメージを検出した場合は、**asdm image** コマンドを実行コンフィギュレーションに挿入します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

フラッシュ メモリに複数の ASDM ソフトウェア イメージを保存できます。アクティブな ASDM セッションがある状態で **asdm image** コマンドを入力して新しい ASDM ソフトウェア イメージを指定した場合、アクティブな ASDM セッションは中断されず、そのセッションを開始した ASDM ソフトウェア イメージを引き続き使用します。新しい ASDM セッションは、新しいソフトウェア イメージを使用します。**no asdm image** コマンドを入力すると、コンフィギュレーションからコマンドが削除されます。ただし、最後に設定したイメージの場所を使用して、ASA から引き続き ASDM にアクセスできます。

このコマンドをスタートアップ コンフィギュレーションに含めない場合、ASA は起動時に最初に検出した ASDM イメージを使用します。内部フラッシュ メモリのルート ディレクトリ内を検索した後で、外部フラッシュ メモリを検索します。ASA はイメージを検出した場合は、**asdm image** コマンドを実行コンフィギュレーションに挿入します。**write memory** コマンドを使用して、実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存してください。**asdm image** コマンドをスタートアップ コンフィギュレーションに保存しない場合、リブートのたびに ASA は ASDM イメージを検索し、**asdm image** コマンドを実行コンフィギュレーションに挿入します。Auto Update を使用する場合は、起動時にこのコマンドが自動的に追加されるため、ASA 上のコンフィギュレーションは Auto Update Server 上のコンフィギュレーションと一致しなくなります。このような不一致が発生すると、ASA はコンフィギュレーションを Auto Update Server からダウンロードします。不要な Auto Update アクティビティを回避するには、**asdm image** コマンドをスタートアップ コンフィギュレーションに保存します。

例

次に、ASDM イメージを asdm.bin に設定する例を示します。

```
ciscoasa(config)# asdm image flash:/asdm.bin
ciscoasa(config)#
```

関連コマンド

コマンド	説明
show asdm image	現在の ASDM イメージ ファイルを表示します。
boot	ソフトウェア イメージとスタートアップ コンフィギュレーション ファイルを設定します。

asdm location

注意 このコマンドを手動で設定しないでください。**asdm location** コマンドは ASDM によって実行コンフィギュレーションに追加され、内部通信に使用されます。このコマンドは、情報提供のためだけにこのマニュアルに記載されています。

asdm location *ip_addr netmask if_name*

asdm location *ipv6_addr/prefix if_name*

構文の説明

if_name	最もセキュリティの高いインターフェイスの名前。最もセキュリティの高いインターフェイスが複数ある場合は、任意にインターフェイス名が選択されます。このインターフェイス名は使用されませんが、必須パラメータです。
ip_addr	ネットワーク トポロジを定義するために ASDM によって内部で使用される IP アドレス。
ipv6_addr/prefix	ネットワーク トポロジを定義するために ASDM によって内部で使用される IPv6 アドレスとプレフィックス。
netmask	*ip_addr* のサブネット マスク。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	**pdm location** コマンドが **asdm location** コマンドに変更されました。

使用上のガイドライン

このコマンドを手動で設定または削除しないでください。

as-path access-list

正規表現を使用して自律システム パス フィルタを設定するには、グローバル コンフィギュレーション モードで **as-path access-list** コマンドを使用します。自律システム パス フィルタを削除し、これを実行コンフィギュレーション ファイルから削除するには、このコマンドの **no** 形式を使用します。

as-path access-list *acl-name* {**permit** | **deny**} *regexp*

no as-path access-list *acl-name*

構文の説明

acl-name	AS パス アクセス リストを指定する名前。
permit	一致条件に基づいてアドバタイズメントを許可します。
deny	一致条件に基づいてアドバタイズメントを拒否します。
regexp	AS パス フィルタを定義する正規表現。自律システム番号は 1 ～ 65535 の範囲で表します。 自律システムの番号形式の詳細については、**router bgp** コマンドの説明を参照してください。 **（注）** 正規表現の設定の詳細については、『*Cisco IOS Terminal Services Configuration Guide*』の付録「Regular Expressions」を参照してください。

デフォルト

自律システム パス フィルタは作成されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

自律システム パス フィルタを設定するには、**as-path access-list** コマンドを使用します。着信と発信の両方の BGP パスに自律システム パス フィルタを適用できます。各フィルタは正規表現で定義されます。正規表現が、ルートの自律システム パスの ASCII 文字列表現と一致した場合、**許可**または**拒否**の条件が適用されます。自律システム パスにはローカル自律システム番号を含めないでください。

シスコが採用している 4 バイト自律システム番号は、自律システム番号の正規表現のマッチングおよび出力表示形式のデフォルトとして asplain（たとえば、65538）を使用していますが、RFC 5396 に記載されているとおり、4 バイト自律システム番号を asplain 形式および asdot 形式の両方で設定できます。4 バイト自律システム番号の正規表現マッチングと出力表示のデフォルトを asdot 形式に変更するには、**bgp asnotation dot** コマンドを使用します。デフォルトで asdot 形式がイネーブルにされている場合、正規表現の 4 バイト自律システム番号のマッチングには、すべて asdot 形式を使用する必要があり、使用しない場合正規表現によるマッチングは失敗します。

例

次の例では、自律システム パス アクセス リスト（番号 500）を定義し、自律システム 65535 から、またはこの自律システムを経由して、10.20.2.2 ネイバーにパスをアドバタイズしないように ASA を設定しています。

```
ciscoasa(config)# as-path access-list as-path-acl deny _65535_
ciscoasa(config)# as-path access-list as-path-acl deny ^65535$
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-fmaily ipv4
ciscoasa(config-router-af)# neighbor 192.168.1.1 remote-as 65535
ciscoasa(config-router-af)# neighbor 10.20.2.2 remote-as 40000
ciscoasa(config-router-af)# neighbor 10.20.2.2 filter-list as-path-acl out
```

asp load-balance per-packet

マルチコア ASA の場合、ロード バランシングの動作をパケット単位に変更するには、グローバル コンフィギュレーション モードで **asp load-balance per-packet** コマンドを使用します。デフォルトのロード バランシング メカニズムに戻すには、このコマンドの **no** 形式を使用します。

asp load-balance per-packet [**auto**]

no asp load-balance per-packet

構文の説明

[auto]	ネットワークの状況に応じて、各インターフェイスの受信リングでパケット単位のロードバランシングを自動的に有効または無効にします。

コマンド デフォルト

パケット単位のロードバランシングはデフォルトで無効になっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.1(1)	このコマンドが追加されました。
9.3(1)	**auto** オプションが追加されました。
9.8(1)	**auto** オプションが ASAv で使用できるようになりました。

使用上のガイドライン

ロード バランサのジョブは、パケットを CPU コアに配布し、パケットの順序を維持することです。デフォルトでは、接続は一度に 1 つのコアでしか処理できません。この動作により、使用中のインターフェイス/RX リングの数がコアの数に比べて少ない場合、コアは十分に活用されません。たとえば、ASA で 2 つのギガビット イーサネット インターフェイスしか使用されていない場合は、2 つのコアだけが使用されます。(10 ギガビット イーサネット インターフェイスには 4 つの RX リングと、1 つの RX リングとしてギガビット イーサネット インターフェイスがあります)。パケット単位のロード バランシングを有効にして、より多くのコアを使用できるようにすることで、ロード バランサを最適化することができます。

デフォルトのロードバランシング動作では、多数のインターフェイスが使用されている場合にシステム全体のパフォーマンスが最適化され、パケット単位のロード バランサでは、アクティブなインターフェイスの数が少ない場合にシステム全体のパフォーマンスが最適化されます。

パケット単位のロード バランシングを有効にすると、1 つのコアがインターフェイスからのパケットを処理する場合に、別のコアが同じインターフェイスからの次のパケットを受信して処理できます。したがって、すべてのコアが同じインターフェイスからのパケットを同時に処理することが可能です。

パケット単位のロード バランシングにより、次の場合にパフォーマンスが向上します。

- システムがパケットをドロップする
- **show cpu** コマンドで、CPU 使用率が 100 % を大きく下回っていることが示される：CPU 使用率は、使用されているコアの数を示す効果的な指標です。たとえば、8 コア システムで、2 つのコアが使用されている場合、**show cpu** は 25 % を示します。4 つのコアの場合は 50 %、6 つのコアの場合は 75 % を示します。
- 使用中のインターフェイスの数が少ない

(注) 通常、ASA に 64 未満の同時フローがある場合、パケット単位のロード バランシングを有効にすると、そのメリットよりもオーバーヘッドが大きくなります。

auto オプションを指定すると、ASA は非対称トラフィックが追加されたかどうかを検出できます。ロード バランシングが必要な場合、インターフェイス受信リングとコアとの 1 対 1 のロックは解放されます。パケット単位のロード バランシングは、すべてのインターフェイス受信リングではなく、高負荷のインターフェイス受信リングでのみ有効になります。この適応型ロード バランス メカニズムは、次の問題の回避に役立ちます。

- フロー上での突発的なトラフィックの増加によって発生するオーバーラン
- 特定のインターフェイス受信リングをオーバーサブスクライブするバルク フローによるオーバーラン
- 比較的高過負荷のインターフェイス受信リングによるオーバーラン（シングル コアでは負荷を維持できません）

auto オプションは、9.7 以前の ASAv では使用できません。

例

次に、デフォルトのロード バランシング動作を変更する例を示します。

```
ciscoasa(config)# asp load-balance per-packet
```

次に、パケットごとのロード バランシングのオンとオフの自動切り替えをイネーブルにする例を示します。

```
ciscoasa(config)# asp load-balance per-packet auto
```

関連コマンド

コマンド	説明
clear asp load-balance history	パケットごとの ASP ロード バランシングの履歴統計情報をクリアし、リセットします。
show asp load-balance	ロード バランサのキュー サイズのヒストグラムを表示します。

コマンド	説明
show asp load-balance per-packet	現在のステータス、最高水準点と最低水準点、およびグローバルなしきい値を表示します。
show asp load-balance per-packet history	現在のステータス、最高水準点と最低水準点、グローバルなしきい値、最後のリセット以降のパケットごとの ASP ロード バランシングのオンとオフの切り替え回数、タイム スタンプ付きのパケットごとの ASP ロード バランシングの履歴、およびオンとオフを切り替えた理由を表示します。

asp rule-engine transactional-commit

ルール エンジンのトランザクション コミット モデルをイネーブルまたはディセーブルにするには、**asp rule-engine transactional-commit** コマンドを使用します。

asp rule-engine transactional-commit *option*

no asp rule-engine transactional-commit *option*

構文の説明

option	選択したポリシー用のルール エンジンのトランザクション コミット モデルをイネーブルにします。次のオプションがあります。 • **access-group**：グローバルに、またはインターフェイスに適用されるアクセス ルール。 • **nat**：ネットワーク アドレス変換ルール。

コマンド デフォルト

デフォルトでは、トランザクション コミット モデルはディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.1(5)	このコマンドが追加されました。
9.3(1)	**nat** キーワードが追加されました。

使用上のガイドライン

デフォルトでは、ルール ベースのポリシー（アクセス ルールなど）を変更した場合、変更はただちに有効になります。ただし、この即時性にはパフォーマンスにわずかなコストがかかります。パフォーマンス コストは、1 秒あたりの接続数が多い環境で大量のルール リストがある場合に顕著です。たとえば、ASA が 1 秒あたり 18,000 個の接続を処理しながら、25,000 個のルールがあるポリシーを変更する場合などです。

パフォーマンスに影響するのは、ルール検索を高速化するためにルール エンジンがルールをコンパイルするためです。デフォルトでは、新しいルールを適用できるように、接続試行を評価するときに未コンパイルのルールも検索されます。新しいルールはコンパイルされていないため、検索に時間がかかります。

ルール変更を実装するときにルール エンジンがトランザクション モデルを使用するように、この動作を変更できます。これにより、新しいルールがコンパイルされ、使用できるようになるまで、引き続き古いルールが使用されます。トランザクション モデルを使用すると、ルールのコンパイル中、パフォーマンスは低下しないはずです。次の表に、その動作の違いを示します。

モデル	コンパイル前	コンパイル中	コンパイル後
デフォルト	古いルールと照合します。	新しいルールと照合します。 (接続数/秒が削減されます)	新しいルールと照合します。
トランザクション	古いルールと照合します。	古いルールと照合します。 (接続数/秒は影響を受けません)	新しいルールと照合します。

トランザクション モデルのメリットにはこのほか、インターフェイスで ACL を置き換える際、古い ACL の削除と新しいポリシーの適用との間にギャップが生じないことがあります。これにより、動作中に許容可能な接続がドロップされる確率が減少します。

ヒント ルール タイプのトランザクション モデルをイネーブルにした場合、コンパイルの先頭と末尾をマークする syslog メッセージが存在します。これらのメッセージには、780001 以降の番号が付けられます。

例

次に、アクセス グループのトランザクション コミット モデルをイネーブルにする例を示します。

```
ciscoasa(config)# asp rule-engine transactional-commit access-group
```

関連コマンド

コマンド	説明
clear conf asp rule-engine transactional-commit	ルール エンジンのトランザクション コミット設定をクリアします。
show run asp rule-engine transactional-commit	ルール エンジンの実行コンフィギュレーションを表示します。

asr-group

非対称ルーティング インターフェイス グループ ID を指定するには、インターフェイス コンフィギュレーション モードで **asr-group** コマンドを使用します。ID を削除するには、このコマンドの **no** 形式を使用します。

asr-group *group_id*

no asr-group *group_id*

構文の説明

group_id	非対称ルーティング グループ ID。有効な値は、1 ～ 32 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	• 対応	—	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

Active/Active フェールオーバーがイネーブルの場合、ロード バランシングにより、発信接続のリターン トラフィックがピア ユニット上のアクティブなコンテキストを介してルーティングされることがあります。このピア ユニットでは、発信接続のコンテキストはスタンバイ グループ内にあります。

asr-group コマンドを使用すると、着信インターフェイスのフローが見つからない場合に、着信パケットが同じ ASR グループのインターフェイスで再分類されます。再分類により別のインターフェイスのフローが見つかり、関連付けられているコンテキストがスタンバイ状態の場合、パケットは処理のためにアクティブなユニットに転送されます。

このコマンドを有効にするには、ステートフル フェールオーバーをイネーブルにする必要があります。

ASR 統計情報は、**show interface detail** コマンドを使用して表示できます。この統計情報には、インターフェイス上で送信、受信、およびドロップされた ASR パケットの数が含まれます。

(注) 同じコンテキスト内の 2 個のインターフェイスを、同じ ASR グループ内で設定してはなりません。

例

次に、選択したインターフェイスを非対称ルーティング グループ 1 に割り当てる例を示します。

コンテキスト ctx1 のコンフィギュレーション:

```
ciscoasa/ctx1(config)# interface Ethernet2
ciscoasa/ctx1(config-if)# nameif outside
ciscoasa/ctx1(config-if)# ip address 192.168.1.11 255.255.255.0 standby 192.168.1.21
ciscoasa/ctx1(config-if)# asr-group 1
```

コンテキスト ctx2 のコンフィギュレーション:

```
ciscoasa/ctx2(config)# interface Ethernet3
ciscoasa/ctx2(config-if)# nameif outside
ciscoasa/ctx2(config-if)# ip address 192.168.1.31 255.255.255.0 standby 192.168.1.41
ciscoasa/ctx2(config-if)# asr-group 1
```

関連コマンド

コマンド	説明
interface	インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイス統計情報を表示します。

assertion-consumer-url（廃止）

(注) このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

セキュリティ デバイスがアサーション コンシューマ サービスに接続するためにアクセスする URL を指定するには、webvpn コンフィギュレーション モードで、特定の SAML-type SSO サーバに対して **assertion-consumer-url** コマンドを使用します。この URL をアサーションから削除するには、このコマンドの **no** 形式を使用します。

assertion-consumer-url *url*

no assertion-consumer-url [*url*]

構文の説明

url	SAML-type SSO サーバで使用するアサーション コンシューマ サービスの URL を指定します。URL は http:// または https:// で始まり、255 文字未満の英数字である必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.5(2)	このコマンドは、SAML 2.0 のサポートの導入に伴って廃止されました。

使用上のガイドライン

シングル サインオン（SSO）は、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。ASA は現在、SAML POST-type の SSO サーバと SiteMinder-type の SSO サーバをサポートしています。

このコマンドは、SAML-type の SSO サーバのみに適用されます。

URL が HTTPS で始まる場合は、アサーション コンシューマ サービス SSL 証明書のルート証明書をインストールする必要があります。

例

次に、SAML-type の SSO サーバのアサーション コンシューマ URL を指定する例を示します。

```
ciscoasa(config-webvpn)# sso server myhostname type saml-v1.1-post
ciscoasa(config-webvpn-sso-saml# assertion-consumer-url https://saml-server/postconsumer
ciscoasa(config-webvpn-sso-saml#
```

関連コマンド

コマンド	説明
issuer	SAML-type の SSO サーバのセキュリティ デバイス名を指定します。
request-timeout	SSO 認証の試行に失敗したときにタイムアウトになるまでの秒数を指定します。
show webvpn sso-server	セキュリティ デバイスに設定されているすべての SSO サーバの運用統計情報を表示します。
sso-server	WebVPN SSO サーバを作成します。
trustpoint	SAML-type のブラウザ アサーションへの署名に使用する証明書を含むトラストポイント名を指定します。

attribute bind

属性ベースのネットワーク オブジェクトの IP-to-attribute バインディングを変更するには、EXEC モードで **attribute bind** コマンドを使用します。

attribute bind *agent-name* **binding** *ip-address* **type** *attribute-type* **value** *attribute-value*

構文の説明

agent-name	属性をモニタする VM 属性エージェントの名前を指定します。
ip-address	管理対象の属性ベースのネットワーク オブジェクトの IP アドレスを指定します。
attribute-type	更新する属性タイプを識別する文字列を指定します。
attribute-value	属性タイプに割り当てる新しい値を識別する文字列を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC モード	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

例

次に、SAML-type の SSO サーバのアサーション コンシューマ URL を指定する例を示します。

```
ciscoasa(config)# attribute bind VMAgent binding 10.10.1.19 type custom.location value global
```

関連コマンド

コマンド	説明
attribute source-group	VM 属性エージェントを設定します。
object network attribute	属性ベースのネットワーク オブジェクトを設定します。
show attribute object-map	object-to-attribute バインディングを示します。
show attribute host-map	host-to-attribute バインディングのマップを示します。

attribute source-group

VMware vCenter または単一の ESXi ホストと通信するように VM 属性エージェントを設定するには、EXEC モードで **attribute source-group** コマンドを使用します。エージェントを削除するには、このコマンドの **no** 形式を使用します。

attribute source-group *agent-name* **type** *agent-type*

no attribute source-group *agent-name*

構文の説明

agent-name	VM 属性エージェントの名前を指定します。
agent-type	属性エージェントのタイプを指定します。現在、サポートされるエージェント タイプは ESXi のみです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC モード	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

例

次に、VM 属性エージェントを設定する例を示します。

```
ciscoasa(config)# attribute source-group VMAgent type esxi
```

関連コマンド

コマンド	説明
object network attribute	属性ベースのネットワーク オブジェクトを設定します。
show attribute source-group	設定した属性エージェントに関する情報を表示します。
show attribute object-map	object-to-attribute バインディングを示します。
show attribute host-map	host-to-attribute バインディングのマップを示します。

attribute source-group host

VM 属性エージェントが vCenter または単一の ESXi ホストと通信できるように VMware vCenter ホスト クレデンシャルを設定するには、属性エージェント コンフィギュレーション モードで **attribute source-group host** コマンドを使用します。ホスト クレデンシャルを削除するには、このコマンドの **no** 形式を使用します。

host *ip-address* **username** *ESXi-username* **password** *ESXi-password*

no host *ip-address*

構文の説明

ip-address	VM 属性エージェントの名前を指定します。
ESXi-username	vCenter ホストのユーザ名を指定します。
ESXi-password	vCenter ホストのパスワードを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
属性エージェント コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

属性エージェントを設定または変更した後に、このコマンドを使用します。

例

次に、属性エージェントにホスト クレデンシャルを設定する例を示します。

```
ciscoasa(config)# attribute source-group VMAgent
ciscoasa(config-attr)# host 10.122.202.217 user admin password Cisco123
```

関連コマンド

コマンド	説明
attribute source-group	VM 属性エージェントを設定します。
object network attribute	属性ベースのネットワーク オブジェクトを設定します。
show attribute source-group	設定した属性エージェントに関する情報を表示します。
show attribute object-map	object-to-attribute バインディングを示します。
show attribute host-map	host-to-attribute バインディングのマップを示します。

attribute source-group keepalive

VMware vCenter 通信のキープアライブ設定を構成するには、属性エージェント コンフィギュレーション モードで **attribute source-group keepalive** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

keepalive retry-interval *interval* **retry-count** *count*

no keepalive

構文の説明

間隔	属性エージェントから vCenter へのキープアライブ メッセージの間隔を指定します。キープアライブ メッセージが送信元からの応答を受信するたびに、エージェントは送信元との接続が有効になっているとみなされ、そのエージェントのキープアライブ タイマーが再起動されます。デフォルトは 30 秒です。
count	キープアライブ メッセージが受信されなかった場合の再試行回数を指定します。タイマーがキープアライブを受信せずに期限切れになるたびに、そのエージェントの再試行回数が増分されます。再試行回数が設定されたしきい値に達すると、エージェントは送信元との接触が失われたことを宣言します。デフォルトは 3 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
属性エージェント コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

属性エージェントを設定または変更した後に、このコマンドを使用します。

例

次に、SAML-type の SSO サーバのアサーション コンシューマ URL を指定する例を示します。

```
ciscoasa(config)# attribute source-group VMAgent
ciscoasa(config-attr)# keepalive retry-timer 100 retry-count 5
```

関連コマンド

コマンド	説明
attribute source-group	VM 属性エージェントを設定します。
object network attribute	属性ベースのネットワーク オブジェクトを設定します。
show attribute source-group	設定した属性エージェントに関する情報を表示します。
show attribute object-map	object-to-attribute バインディングを示します。
show attribute host-map	host-to-attribute バインディングのマップを示します。

属性

ASA が DAP 属性データベースに書き込む属性値ペアを指定するには、DAP テスト属性モードで **attributes** コマンドを入力します。

attributes *name value*

構文の説明

name	ウェルノウン属性名、または「label」タグを組み込む属性を指定します。label タグは、DAP レコード内のファイル、レジストリ、プロセス、アンチウイルス、アンチスパイウェア、およびパーソナル ファイアウォールのエンドポイント属性に対して設定するエンドポイント ID に対応します。
value	AAA 属性に割り当てられた値。

コマンド デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
DAP 属性コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

複数の属性値ペアを入力するには、このコマンドを複数回使用します。

通常、ASA は AAA サーバからユーザ認可属性を取得し、Cisco Secure Desktop、Host Scan、CNA または NAC からエンドポイント属性を取得します。test コマンドの場合、ユーザ認可属性とエンドポイント属性をこの属性モードで指定します。ASA は、これらの属性を、DAP サブシステムが DAP レコードの AAA 選択属性およびエンドポイント選択属性を評価するときに参照する属性データベースに書き込みます。

例

次の例では、認証されたユーザが SAP グループのメンバーで、エンドポイント システムにアンチウイルス ソフトウェアがインストールされている場合に、ASA が 2 つの DAP レコードを選択することを前提としています。アンチウイルス ソフトウェアのエンドポイント ルールのエンドポイント ID は *nav* です。

DAP レコードには、次のポリシー属性があります。

DAP レコード 1	DAP レコード 2
action = continue	action = continue
port-forward = enable hostlist1	url-list = links2
—	url-entry = enable

```
ciscoasa # test dynamic-access-policy attributes
ciscoasa(config-dap-test-attr)# attributes aaa.ldap.memberof SAP
ciscoasa(config-dap-test-attr)# attributes endpoint.av.nav.exists true
ciscoasa(config-dap-test-attr)# exit

ciscoasa # test dynamic-access-policy execute
Policy Attributes:
action = continue
port-forward = enable hostlist1
url-list = links2
url-entry = enable

ciscoasa #
```

関連コマンドI

コマンド	説明
display	現在の属性リストを表示します。
dynamic-access-policy-record	DAP レコードを作成します。
test dynamic-access-policy attributes	属性を入力します。
test dynamic-access-policy execute	DAP を生成するロジックを実行し、生成されたアクセスポリシーをコンソールに表示します。

auth-cookie-name

認証クッキーの名前を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **auth-cookie-name** コマンドを使用します。これは HTTP フォームのコマンドを使用した SSO です。

auth-cookie-name

構文の説明

name	認証クッキーの名前。名前の最大の長さは 128 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

ASA の WebVPN サーバは、シングル サインオン（SSO）サーバにシングル サインオン認証要求を送信することに HTTP POST 要求を使用します。認証が成功すると、認証 Web サーバは、認証クッキーをクライアント ブラウザに戻します。クライアント ブラウザは、その認証クッキーを提示して、SSO ドメイン内の他の Web サーバの認証を受けます。**auth-cookie-name** コマンドは、ASA によって SSO に使用される認証クッキーの名前を設定します。

一般的な認証クッキーの形式は、Set-Cookie: *cookie name=cookie value* [;*cookie attributes*] です。次の認証クッキーの例では、SMSESSION が **auth-cookie-name** コマンドで設定される名前です。

```
Set-Cookie:
SMSESSION=yN4Yp5hHVNDgs4FT8dn7+Rwev41hsE49XlKc+1twie0gqnjbhkTkUnR8XWP3hvDH6PZPbHIHtWLDKTa8
ngDB/lbYTjIxrbDx8WPWwaG3CxVa3adOxHFR8yjD55GevK3ZF4ujgU1lhO6fta0dSSOSepWvnsCb7IFxCw+MGiw0o
88uHa2t4l+SillqfJvcpuXfiIAO06D/dapWriHjNoi4llJOgCst33wEhxFxcWy2UWxs4EZSjsI5GyBnefSQTPVfma
5dc/emWor9vWr0HnTQaHP5rg5dTNqunkDEdMIHfbeP3F90cZejVzihM6igiS6P/CEJAjE;Domain=.example.com;
Path=/
```

例

次に、example.com という名前の Web サーバから受信した認証クッキーに認証クッキー名 SMSESSION を指定する例を示します。

```
ciscoasa(config)# aaa-server testgrp1 host example.com
ciscoasa(config-aaa-server-host)# auth-cookie-name SMSESSION
ciscoasa(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
action-uri	シングル サインオン認証用のユーザ名およびパスワードを受信するための Web サーバ URI を指定します。
hidden-parameter	認証 Web サーバと交換するための非表示パラメータを作成します。
password-parameter	SSO 認証用にユーザ パスワードを送信する必要がある HTTP POST 要求パラメータの名前を指定します。
start-url	プリログイン クッキーを取得する URL を指定します。
user-parameter	ユーザ名パラメータを SSO 認証に使用される HTTP POST 要求の一部として送信する必要があることを指定します。

authenticated-session-username

二重認証がイネーブルになっている場合に、セッションに関連付ける認証ユーザ名を指定するには、トンネル グループ一般属性モードで **authenticated-session-username** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

authenticated-session-username {**primary** | **secondary**}

no authenticated-session-username

構文の説明

プライマリ	プライマリ認証サーバからのユーザ名を使用します。
secondary	セカンダリ認証サーバからのユーザ名を使用します。

デフォルト

デフォルト値は **primary** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、二重認証がイネーブルになっている場合に限り有効です。**authenticated-session-username** コマンドは、ASA がセッションに関連付けるユーザ名を抽出する認証サーバを選択します。

例

次に、グローバル コンフィギュレーション モードで、remotegrp という名前の IPsec リモート アクセス トンネル グループを作成し、接続にセカンダリ認証サーバからのユーザ名を使用することを指定する例を示します。

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-webvpn)# authenticated-session-username secondary
ciscoasa(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
pre-fill-username	ユーザ名の事前入力機能をイネーブルにします。
show running-config tunnel-group	指定されたトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。
username-from-certificate	認可時のユーザ名として使用する証明書内のフィールドを指定します。

authentication（bfd-template）

シングルホップおよびマルチホップ セッション用の BFD テンプレートで認証を設定するには、BFD コンフィギュレーション モードで **authentication** コマンドを使用します。シングルホップまたはマルチホップ セッション用の BFD テンプレートで認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

authentication *authentication-type* **[0|8]** *key-string* **key-id** *id*

構文の説明

authentication-type	認証タイプを指定します。有効な値は、**md5**、**meticulous-md5**、**meticulous-sha-1**、および **sha-1** です。
0|8	0:暗号化されていないパスワードが後に続くことを示します。8:暗号化されたパスワードが後に続くことを示します。
key-string	認証されるルーティング プロトコルを使用してパケットで送信および受信される必要のある認証文字列を指定します。有効な範囲は、1 ～ 17 文字の大文字と小文字の英数字です。ただし、最初の文字は数字にはできません。
id	キー文字列に一致する共有キー ID を指定します。

デフォルト

このコマンドにデフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
BFD コンフィギュレーション	• 対応	• —	• 対応	• 対応	• —

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、BFD シングルホップおよびマルチホップ テンプレートで認証を設定するために使用します。セキュリティを強化するために認証を設定することをお勧めします。

認証は、BFD の送信元と宛先のペアごとに設定する必要があり、認証パラメータは両方のデバイスで同じである必要があります。

例

次に、シングルホップ BFD テンプレートで認証を設定する例を示します。

```
ciscoasa(config)# bfd single-hop sh-template
ciscoasa(config-bfd)# authentication sha-1 0 cisco key-id 10
```

次に、マルチホップ BFD テンプレートで認証を設定する例を示します。

```
ciscoasa(config)# bfd multi-hop mh-template
ciscoasa(config-bfd)# authentication shat-1 0 cisco key-id 10
```

関連コマンド

コマンド	説明
authentication	シングルホップ セッションとマルチホップ セッションの BFD テンプレートに認証を設定します。
bfd echo	インターフェイスで BFD エコー モードを有効にします。
bfd interval	インターフェイスにベースライン BFD パラメータを設定します。
bfd map	アドレスとマルチホップ テンプレートを関連付ける BFD マップを設定します。
bfd slow-timers	BFD スロー タイマー値を設定します。
bfd template	シングルホップ BFD テンプレートをインターフェイスにバインドします。
bfd-template single-hop | multi-hop	BFD テンプレートを設定し、BFD コンフィギュレーション モードを開始します。
clear bfd counters	BFD カウンタをクリアします。
echo	BFD シングルホップ テンプレートにエコーを設定します。
neighbor	BGP が登録され、BFD から転送パス検出失敗メッセージを受信できるように、BGP の BFD サポートを設定します。
show bfd drops	BFD でドロップされたパケットの数を表示します。
show bfd map	設定済みの BFD マップを表示します。
show bfd neighbors	既存の BFD 隣接関係の詳細なリストを表示します。
show bfd summary	BFD のサマリー情報を表示します。

認証

WebVPN と電子メール プロキシの認証方式を設定するには、各モードで **authentication** コマンドを使用します。デフォルトの方式に戻すには、このコマンドの **no** 形式を使用します。ASA は、ユーザを認証してユーザ ID を確認します。

authentication {[aaa] [certificate] [multiple certificate] [saml] [mailhost] [piggyback]}

no authentication [**aaa**] [**certificate**] **[multiple certificate] [saml]** [**mailhost**] [**piggyback]**

構文の説明

aaa	ASA が設定済みの AAA サーバと照合するユーザ名およびパスワードを指定します。
certificate	SSL ネゴシエーション時の証明書を指定します。
mailhost	SMTPS の場合のみ、リモート メール サーバで認証します。IMAP4S および POP3S の場合、メールホスト認証は必須であり、設定可能なオプションとして表示されません。
multiple certificate	SSL ネゴシエーション時の複数証明書オプションを指定します。
piggyback	HTTPS WebVPN セッションがすでに存在している必要があります。ピギーバック認証は、電子メール プロキシでのみ使用できます。
saml	SAML 認証方式は相互に排他的です。

デフォルト

次の表に、WebVPN および電子メール プロキシのデフォルトの認証方式を示します。

プロトコル	デフォルトの認証方式
IMAP4S	メールホスト（必須）
POP3S	メールホスト（必須）
SMTPS	AAA
WebVPN	AAA

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
Imap4s コンフィギュレーション	• 対応	—	• 対応	—	—
Pop3s コンフィギュレーション	• 対応	—	• 対応	—	—
smtps コンフィギュレーション	• 対応	—	• 対応	—	—
webvpn コンフィギュレーション	• 対応		• 対応		

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、WebVPN 用のトンネル グループ webvpn 属性コンフィギュレーション モードに置き換えられました。
8.0(2)	このコマンドは、証明書認証要件の変更を反映するように変更されました。
9.5(2)	このコマンドは、SAML 2.0 のサポートを反映して変更されました。
9.7(1)	既存の認証属性は、複数証明書認証のオプションを含めるように変更されます。

使用上のガイドライン

少なくとも 1 つの認証方式が必要です。たとえば、WebVPN の場合、AAA 認証と証明書認証のいずれか一方または両方を指定できます。任意の順序でこれらのコマンドを入力できます。

WebVPN 証明書認証では、それぞれのインターフェイスに対して HTTPS ユーザ証明書を要求する必要があります。つまり、この選択が機能するには、証明書認証を指定する前に、**authentication-certificate** コマンドでインターフェイスを指定しておく必要があります。

このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ webvpn 属性コンフィギュレーション モードの同等のコマンドに変換されます。

WebVPN の場合、AAA 認証と証明書認証の両方を要求できます。この場合、ユーザは証明書とユーザ名/パスワードの両方を指定する必要があります。電子メール プロキシ認証の場合、複数の認証方式を要求できます。このコマンドを再び指定すると、現在のコンフィギュレーションが上書きされます。

例

次に、WebVPN ユーザに認証のための証明書を要求する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# authentication certificate
```

関連コマンド

コマンド	説明
authentication-certificate	接続を確立する WebVPN クライアントからの証明書を要求します。
show running-config	現在のトンネル グループ コンフィギュレーションを表示します。
clear configure aaa	設定した AAA の値を削除またはリセットします。
show running-config aaa	AAA コンフィギュレーションを表示します。

authentication eap-proxy

L2TP over IPsec 接続に対して EAP をイネーブルにし、ASA が PPP 認証プロセスを外部の RADIUS 認証サーバにプロキシできるようにするには、トンネル グループ ppp 属性コンフィギュレーション モードで **authentication eap-proxy** コマンドを使用します。コマンドをデフォルト設定に戻すには（CHAP および MS-CHAP を許可）、このコマンドの **no** 形式を使用します。

authentication eap-proxy

no authentication eap-proxy

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトでは、EAP は認証プロトコルとして許可されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
トンネル グループ PPP 属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

この属性は、L2TP または IPsec トンネル グループ タイプのみに適用できます。

例

次に、設定 ppp コンフィギュレーション モードで、ppremotegrp という名前のトンネル グループの PPP 接続に対して EAP を許可する例を示します。

```
ciscoasa(config)# tunnel-group ppremotegrp type IPSec/IPSec
ciscoasa(config)# tunnel-group ppremotegrp ppp-attributes
ciscoasa(config-ppp)# authentication eap
ciscoasa(config-ppp)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	指定した証明書マップ エントリを表示します。
tunnel-group-map default-group	**crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリをトンネル グループに関連付けます。

認証キー

IS-IS での認証をイネーブルにするには、ルータ ISIS コンフィギュレーション モードで **authentication key** コマンドを使用します。このような認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

authentication key [0 | 8] *password* **[level-1 | level-2]**

no authentication key [0 | 8] *password* **[level-1 | level-2]**

構文の説明

password	認証をイネーブルにし、キーを指定します。
level-1	（任意）レベル 1 パケットについてだけ認証をイネーブルにします。
level-2	（任意）レベル 2 パケットについてだけ認証をイネーブルにします。

デフォルト

ルータ レベルでは、IS-IS パケットにキー認証は適用されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ isis コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

key コマンドで設定されたパスワードが存在しない場合、キー認証は行われません。

キー認証は、クリア テキスト認証または MD5 認証に適用できます。モードは authentication mode コマンドで設定されます。

IS-IS に一度に適用できる認証キーは 1 つだけです。つまり、2 番めの authentication key コマンドを設定すると、最初のコマンドは上書きされます。

キーワード **level-1** および **level-2** のいずれも設定されていない場合、パスワードは両方のレベルに適用されます。

isis authentication key コマンドを使用することにより、個々の IS-IS インターフェイスに認証を指定できます。

(注) IS-IS では、**authentication key-chain** コマンドを使用してグローバルに設定されたキー チェーンの有効期限を選択します。ASA のキー チェーン インフラストラクチャが存在しないため、このコマンドとともにキーを提供します。

例

次に、site1 という名前のキー チェーンに属する任意のキーを受け入れ、送信するように IS-IS を設定する例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0101.0101.0101.00
ciscoasa(config-router)# is-type level-1
ciscoasa(config-router)# authentication mode md5 level-1
ciscoasa(config-router)# authentication key 0 site1 level-1
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。

コマンド	説明
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が ASA のデータベースに更新されずに存在する最長時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト(TLV)を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。

コマンド	説明
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

authentication key eigrp

EIGRP パケットの認証をイネーブルにし、認証キーを指定するには、インターフェイス コンフィギュレーション モードで **authentication key eigrp** コマンドを使用します。EIGRP 認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

authentication key eigrp *as-number key* **key-id** *key-id*

no authentication key eigrp *as-number*

構文の説明

as-number	認証する EIGRP プロセスの自律システム番号。これは、EIGRP ルーティング プロセスに設定されている値と同じにする必要があります。
key	EIGRP 更新を認証するキー。このキーには、最大 16 文字を含めることができます。
key-id *key-id*	キー ID 値。有効な値の範囲は 1 ～ 255 です。

デフォルト

EIGRP 認証はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードはサポートされます。

使用上のガイドライン

EIGRP メッセージ認証をイネーブルにするには、**authentication mode eigrp** および **authentication key eigrp** コマンドの両方をインターフェイスに設定する必要があります。インターフェイスに設定された **authentication** コマンドを表示するには、**show running-config interface** コマンドを使用します。

例

次に、インターフェイス GigabitEthernet0/3 に設定された EIGRP 認証の例を示します。

```
ciscoasa(config)# interface Gigabit0/3
ciscoasa(config-if)# authentication mode eigrp md5
ciscoasa(config-if)# authentication key eigrp 100 thisismykey key_id 5
```

関連コマンド

コマンド	説明
authentication mode eigrp	EIGRP 認証に使用する認証のタイプを指定します。

authentication mode

IS-IS インスタンスに対する IS-IS パケットで使用される認証のタイプを指定するには、ルータ ISIS コンフィギュレーション モードで **authentication mode** コマンドを使用します。クリア テキスト認証に戻すには、このコマンドの **no** 形式を使用します。

authentication mode {**md5** | **text**} [**level-1** | **level-2**]

no authentication mode

構文の説明

md5	Message Digest 5（MD5）認証。
text	平文認証
level-1	（任意）レベル 1 パケットについてだけ、指定された認証をイネーブルにします。
level-2	（任意）レベル 2 パケットについてだけ、指定された認証をイネーブルにします。

デフォルト

クリア テキスト（プレーン テキスト）認証は **area-password** コマンドや **domain-password** コマンドなど、その他の方法でも設定できますが、このコマンドを使用すると、ルータ レベルでは IS-IS パケットに対する認証は提供されません。

コマンド モード

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ isis コンフィギュレーション	• 対応	—	• 対応	• 対応	—

使用上のガイドライン

キーワード **level-1** および **level-2** のいずれも設定されていない場合、モードは両方のレベルに適用されます。

isis authentication mode コマンドを使用することにより、IS-IS インスタンスごとにではなく、1 つの IS-IS インターフェイスに適用される認証のタイプとレベルを指定できます。

area-password または **domain-password** コマンドを使用してクリア テキスト認証が設定されている場合、これらのコマンドよりも authentication mode コマンドが優先されます。

authentication mode コマンドを設定した後で、**area-password** または **domain-password** コマンドを設定しようとしてもできません。**area-password** または **domain-password** コマンドを使用してクリア テキスト認証を設定しなければならない場合は、まず、**no authentication mode** コマンドを使用する必要があります。

例

次に、レベル 1 パケットに対する IS-IS インスタンスの MD5 認証を設定する例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0101.0101.0101.00
ciscoasa(config-router)# is-type level-1
ciscoasa(config-router)# authentication mode md5 level-1
ciscoasa(config-router)# authentication key 0 site1 level-1
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。

コマンド	説明
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト(TLV)を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

authentication ms-chap-v1

L2TP over IPsec 接続に対して PPP の Microsoft CHAP Version 1 認証をイネーブルにするには、トンネル グループ ppp 属性コンフィギュレーション モードで **authentication ms-chap-v1** コマンドを使用します。コマンドをデフォルト設定に戻すには（CHAP および MS-CHAP を許可）、このコマンドの **no** 形式を使用します。Microsoft CHAP Version 1 をディセーブルにするには、このコマンドの **no** 形式を使用します。

authentication ms-chap-v1

no authentication ms-chap-v1

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
トンネル グループ PPP 属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

この属性は、L2TP または IPsec トンネル グループ タイプのみに適用できます。このプロトコルは CHAP と類似していますが、CHAP のようなクリアテキスト パスワードではなく、暗号化されたパスワードのみをサーバが格納して比較するために、よりセキュアです。また、このプロトコルはデータ暗号化のためのキーを MPPE によって生成します。

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体または指定されたトンネル グループだけをクリアします。
show running-config tunnel-group	指定されたトンネル グループまたはすべてのトンネル グループの現在実行されているトンネル グループ コンフィギュレーションを表示します。
tunnel-group	IPsec および WebVPN トンネルの接続固有レコードのデータベースを作成および管理します。

authentication ms-chap-v2

L2TP over IPsec 接続に対して PPP の Microsoft CHAP Version 2 認証をイネーブルにするには、トンネル グループ ppp 属性コンフィギュレーション モードで **authentication ms-chap-v1** コマンドを使用します。コマンドをデフォルト設定に戻すには（CHAP および MS-CHAP を許可）、このコマンドの **no** 形式を使用します。

authentication ms-chap-v2

no authentication ms-chap-v2

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
トンネル グループ PPP 属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

この属性は、L2TP または IPsec トンネル グループ タイプのみに適用できます。

このプロトコルは CHAP と類似していますが、CHAP のようなクリアテキスト パスワードではなく、暗号化されたパスワードのみをサーバが格納して比較するために、よりセキュアです。また、このプロトコルはデータ暗号化のためのキーを MPPE によって生成します。

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体または指定されたトンネル グループだけをクリアします。
show running-config tunnel-group	指定されたトンネル グループまたはすべてのトンネル グループの現在実行されているトンネル グループ コンフィギュレーションを表示します。
tunnel-group	IPsec および WebVPN トンネルの接続固有レコードのデータベースを作成および管理します。

authentication pap

L2TP over IPsec 接続に対して PPP の PAP 認証を許可するには、トンネル グループ ppp 属性コンフィギュレーション モードで **authentication pap** コマンドを使用します。コマンドをデフォルト設定に戻すには（CHAP および MS-CHAP を許可）、このコマンドの **no** 形式を使用します。

authentication pap

no authentication pap

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトでは、PAP は認証プロトコルとして許可されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
トンネル グループ PPP 属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

この属性は、L2TP または IPsec トンネル グループ タイプのみに適用できます。

このプロトコルは、認証時にクリアテキストのユーザ名とパスワードを渡すため、安全ではありません。

例

次に、設定 ppp コンフィギュレーション モードで、ppremotegrp という名前のトンネル グループの PPP 接続に対して PAP を許可する例を示します。

```
ciscoasa(config)# tunnel-group ppremotegrp type IPSec/IPSec
ciscoasa(config)# tunnel-group ppremotegrp ppp-attributes
ciscoasa(config-ppp)# authentication pap
ciscoasa(config-ppp)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	指定した証明書マップ エントリを表示します。
tunnel-group-map default-group	**crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリをトンネル グループに関連付けます。

authentication send-only

IS-IS インスタンスについて、受信ではなく送信される IS-IS パケットに対してのみ認証が実行されるように指定するには、ルータ ISIS コンフィギュレーション モードで **authentication send-only** コマンドを使用します。送信および受信されるパケットに対して認証が実行されるように設定するには、このコマンドの **no** 形式を使用します。

authentication send-only [**level-1** | **level-2**]

no authentication send-only

構文の説明

level-1	（任意）認証は受信ではなく、送信されるレベル 1 パケットだけに実行されます。
level-2	（任意）認証は受信ではなく、送信されるレベル 2 パケットだけに実行されます。

デフォルト

認証がルータ レベルで設定されている場合、その認証が送信と受信の IS-IS パケットに適用されます。

コマンド モード

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ isis コンフィギュレーション	• 対応	—	• 対応	• 対応	—

使用上のガイドライン

このコマンドは、認証モードおよび認証キー チェーンを設定する前に使用します。これにより、認証の実装がスムーズに進むようになります。送信されるパケットだけに認証が挿入され、受信されるパケットではチェックされない場合、各ルータでキーの設定に費やせる時間が長くなります。このコマンドを使用して、通信を必要とするルータすべてを設定した後で、ルータごとに、認証モードとキー チェーンをイネーブルにします。その後、**no authentication send-only** コマンドを指定して、send-only 機能をディセーブルにします。

キーワード **level-1** および **level-2** のいずれも設定されていない場合、send-only 機能は両方のレベルに適用されます。

このコマンドは、クリア テキスト認証または MD5 認証に適用できます。モードは、**authentication mode** コマンドにより決定されます。

例

次に、受信ではなく送信されるパケットでクリア テキスト認証が使用されるように IS-IS レベル 1 パケットを設定する例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0101.0101.0101.00
ciscoasa(config-router)# is-type level-1
ciscoasa(config-router)# authentication send-only level-1
ciscoasa(config-router)# authentication key-chain site1 level-1
```

関連コマンド

authentication-attr-from-server

二重認証がイネーブルになっている場合に、接続に適用する認証サーバの認可属性を指定するには、トンネル グループ一般属性モードで **authentication-attr-from-server** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

authentication-attr-from-server {**primary** | **secondary**}

no authentication-attr-from-server

構文の説明

プライマリ	プライマリ認証サーバを使用します。
secondary	セカンダリ認証サーバを使用します。

デフォルト

デフォルト値は **primary** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、二重認証がイネーブルになっている場合に限り有効です。**authentication-attr-from-server** コマンドは、ASA が接続に適用する認可属性を抽出する認証サーバを選択します。

例

次に、グローバル コンフィギュレーション モードで、remotegrp という名前の IPsec リモート アクセス トンネル グループを作成し、接続に適用する認可属性をセカンダリ認証サーバから入手する必要があることを指定する例を示します。

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-webvpn)# authentication-attr-from-server secondary
ciscoasa(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
pre-fill-username	ユーザ名の事前入力機能をイネーブルにします。
show running-config tunnel-group	指定されたトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。
username-from-certificate	認可時のユーザ名として使用する証明書内のフィールドを指定します。

authentication-certificate

接続を確立している WebVPN クライアントから証明書を要求するには、webvpn コンフィギュレーション モードで **authentication-certificate** コマンドを使用します。クライアント証明書の要求をキャンセルするには、このコマンドの **no** 形式を使用します。

authentication-certificate *interface-name*

no authentication-certificate [*interface-name*]

構文の説明

interface-name	接続を確立するために使用するインターフェイスの名前。使用可能なインターフェイス名は、次のとおりです。 • **inside** インターフェイス GigabitEthernet 0/1 の名前 • **outside** インターフェイス GigabitEthernet 0/0 の名前

デフォルト

authentication-certificate コマンドを省略すると、クライアント証明書認証はディセーブルになります。インターフェイス名を **authentication-certificate** コマンドで指定しない場合、デフォルトのインターフェイス名は **inside** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを有効にするには、WebVPN が対応するインターフェイスですでにイネーブルになっている必要があります。インターフェイスを設定して名前を付けるには、**interface**、**IP address**、および **nameif** コマンドを使用します。

このコマンドは、WebVPN クライアント接続にのみ適用されます。ただし、管理接続のクライアント証明書認証を **http authentication-certificate** コマンドを使用して指定することは、WebVPN をサポートしないものも含めてすべてのプラットフォームで可能です。

ASA は、PKI トラストポイントを使用して証明書を検証します。証明書が検証に合格しない場合、次のいずれかのアクションが実行されます。

条件	実行されるアクション
ASA に組み込まれているローカル CA がイネーブルでない場合。	ASA は SSL 接続を閉じます。
ローカル CA はイネーブルであるが、AAA 認証がイネーブルでない場合。	ASA は証明書を取得するために、クライアントをローカル CA の証明書登録ページにリダイレクトします。
ローカル CA と AAA 認証の両方がイネーブルの場合。	クライアントは AAA 認証ページにリダイレクトされます。設定されている場合、ローカル CA の登録ページのリンクもクライアントに表示します。

例

次に、外部インターフェイスの WebVPN ユーザ接続の証明書認証を設定する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# authentication-certificate outside
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
authentication (tunnel-group webvpn configuration mode)	トンネル グループのメンバーが認証にデジタル証明書を使用する必要があることを指定します。
http authentication-certificate	ASA への ASDM 管理接続に証明書による認証を指定します。
interface	接続を確立するために使用するインターフェイスを設定します
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
ssl trust-point	SSL 証明書トラストポイントを設定します。

authentication-exclude

エンド ユーザがクライアントレス SSL VPN にログインせずに設定済みリンクを参照できるようにするには、webvpn コンフィギュレーション モードで **authentication-exclude** コマンドを使用します。複数のサイトへのアクセスを許可するには、このコマンドを複数回使用します。

authentication-exclude *url-fnmatch*

構文の説明

url-fnmatch	クライアントレス SSL VPN へのログインの要件を免除するリンクを指定します。

コマンド デフォルト

ディセーブル

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

この機能は、一部の内部リソースを SSL VPN 経由で一般利用できるようにする場合に便利です。

リンクに関する情報を、SSL VPN マングリングした形式でエンド ユーザに配布する必要があります。たとえば、SSL VPN を使用してこれらのリソースを参照し、配布するリンクに関する情報に結果の URL をコピーします。

例

次に、2 つのサイトに対して認証要件を免除する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# authentication-exclude http://www.example.com/public/*
ciscoasa(config-webvpn)# authentication-exclude *example.html
ciscoasa(config-webvpn)# ciscoasa #
```

authentication-port

特定のホストの RADIUS 認証に使用するポート番号を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **authentication-port** コマンドを使用します。認証ポートの指定を削除するには、このコマンドの **no** 形式を使用します。

authentication-port *port*

no authentication-port

構文の説明

port	RADIUS 認証用のポート番号(1 ～ 65535)。

デフォルト

デフォルトでは、デバイスはポート 1645 で RADIUS をリッスンします(RFC 2058 に準拠)。ポートが指定されていない場合、RADIUS 認証のデフォルト ポート番号 1645 が使用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドのセマンティックが変更され、RADIUS サーバを含むサーバ グループでホストごとにサーバ ポートを指定できるようになりました。

使用上のガイドライン

このコマンドは、認証機能の割り当て先となるリモート RADIUS サーバ ホストの宛先 TCP/UDP ポート番号を指定します。RADIUS 認証サーバで 1645 以外のポートが使用されている場合は、**aaa-server** コマンドで RADIUS サービスを開始する前に、適切なポートを ASA に設定する必要があります。

このコマンドは、RADIUS 用に設定されているサーバ グループに限り有効です。

例

次に、ホスト「1.2.3.4」に「srvgrp1」という RADIUS AAA サーバを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、さらに認証ポートを 1650 に設定する例を示します。

```
ciscoasa(config)# aaa-server svrgrp1 protocol radius
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry-interval 7
ciscoasa(config-aaa-server-host)# authentication-port 1650
```

```
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

関連コマンド

コマンド	説明
aaa authentication	**aaa-server** コマンドまたは ASDM ユーザ認証により指定されたサーバ上の LOCAL、TACACS+、または RADIUS ユーザ認証をイネーブルまたはディセーブルにします。
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始します。このモードでは、ホストに固有の AAA サーバパラメータを設定できます。
clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

authentication-server-group（imap4s、pop3s、smtps）（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

電子メール プロキシに使用する認証サーバのセットを指定するには、各モードで **authentication-server-group** コマンドを使用します。認証サーバをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

authentication-server-group *group_tag*

no authentication-server-group

構文の説明

group_tag	事前に設定済みの認証サーバまたはサーバ グループを指定します。

デフォルト

デフォルトでは、認証サーバは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
Imap4s コンフィギュレーション	• 対応	—	• 対応	—	—
Pop3s コンフィギュレーション	• 対応	—	• 対応	—	—
smtps コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.5(2)	このコマンドは廃止されました。

使用上のガイドライン

ASA は、ユーザを認証してユーザ ID を確認します。

AAA 認証を設定する場合は、この属性も設定する必要があります。設定しないと、認証は常に失敗します。

認証サーバを設定するには、**aaa-server** コマンドを使用します。

例

次に、「IMAP4SSVRS」という名前の認証サーバのセットを使用するように IMAP4S 電子メール プロキシを設定する例を示します。

```
ciscoasa(config)# imap4s
ciscoasa(config-imap4s)# authentication-server-group IMAP4SSVRS
```

関連コマンド

コマンド	説明
aaa-server host	認証、許可、およびアカウンティング サーバを設定します。

authentication-server-group（トンネル グループ一般属性）

トンネル グループでユーザ認証に使用する AAA サーバ グループを指定するには、トンネル グループ一般属性コンフィギュレーション モードで **authentication-server-group** コマンドを使用します。この属性をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

authentication-server-group [(*interface_name*)] *server_group* [**LOCAL**]

no authentication-server-group [(*interface_name*)] *server_group*

構文の説明

interface_name	（オプション）IPsec トンネルが終端するインターフェイスを指定します。
LOCAL	（オプション）通信障害によりサーバ グループにあるすべてのサーバが非アクティブになった場合に、ローカル ユーザ データベースを使用した認証を要求します。
server_group	事前に設定済みの認証サーバまたはサーバ グループを指定します。

デフォルト

このコマンドのサーバ グループのデフォルト設定は **LOCAL** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般属性コンフィギュレーション モードに移動されました。
8.0(2)	このコマンドは、インターフェイス単位で IPsec 接続の認証を行えるように拡張されました。

使用上のガイドライン

この属性は、すべてのトンネル グループ タイプに適用できます。

認証サーバを設定するには **aaa-server** コマンドを使用し、設定済みの AAA サーバ グループにサーバを追加するには **aaa-server-host** コマンドを使用します。

例

次に、設定一般コンフィギュレーション モードで、remotegrp という名前の IPsec リモート アクセス トンネル グループに aaa-server456 という名前の認証サーバ グループを設定する例を示します。

```
ciscoasa(config)# tunnel-group remotegrp type ipsec-ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# authentication-server-group aaa-server456
ciscoasa(config-tunnel-general)#
```

関連コマンド

コマンド	説明
aaa-server	AAA サーバ グループを作成し、グループ固有の AAA サーバ パラメータとすべてのグループ ホストに共通の AAA サーバ パラメータを設定します。
aaa-server host	設定済みの AAA サーバ グループにサーバを追加し、ホスト固有の AAA サーバ パラメータを設定します。
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。

authorization-required

接続前にユーザが正常に認可されることを求めるには、各モードで **authorization-required** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

authorization-required

no authorization-required

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
Imap4s コンフィギュレーション	• 対応	—	• 対応	—	—
Pop3s コンフィギュレーション	• 対応	—	• 対応	—	—
smtps コンフィギュレーション	• 対応	—	• 対応	—	—
トンネル グループ一般属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般属性コンフィギュレーション モードに移動されました。
7.2(1)	webvpn コンフィギュレーション モードが imap4s、pop3s、および smtps コンフィギュレーション モードに置き換えられました。
9.5(2)	このコマンドは、imap4s モード、pop3s モード、および smtps モードについては廃止されました。

例

次に、remotegrp という名前のリモート アクセス トンネル グループを介して接続するユーザに、完全な DN に基づく認可を要求する例を示します。最初のコマンドでは、remotegrp という名前のリモート グループのトンネル グループ タイプを ipsec_ra（IPsec リモート アクセス）と設定しています。2 番目のコマンドで、指定したトンネル グループのトンネル グループ一般属性コンフィギュレーション モードを開始し、最後のコマンドで、指定したトンネル グループに認可が必要であることを指定しています。

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# authorization-required
ciscoasa(config-tunnel-general)#
```

関連コマンド

コマンド	説明
authorization-dn-attributes	認可用のユーザ名として使用するプライマリおよびセカンダリ サブジェクト DN フィールドを指定します。
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	指定した証明書マップ エントリを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。

authorization-server-group（imap4s、pop3s、smtps）（廃止）

(注) このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

すべてのリモート アクセス VPN のトンネル グループに使用する認可サーバのセットを指定するには、各モードで **authorization-server-group** コマンドを使用します。認可サーバをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

authorization-server-group *group_tag*

no authorization-server-group

構文の説明

group_tag	設定済みの認可サーバまたはサーバ グループを指定します。認可サーバを設定するには、**aaa-server** コマンドを使用します。

デフォルト

デフォルトでは、認可サーバは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
Imap4s コンフィギュレーション	• 対応	—	• 対応	—	—
Pop3s コンフィギュレーション	• 対応	—	• 対応	—	—
smtps コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般属性コンフィギュレーション モードに移動されました。
9.5(2)	このコマンドは廃止されました。

使用上のガイドライン

ASA では、認可を使用して、ユーザに許可されているネットワーク リソースへのアクセス レベルを確認します。**aaa-server** コマンドで使用する認可用のサーバ設定を使用します。

このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ一般属性モードの同等のコマンドに変換されます。

VPN 認可が LOCAL と定義されている場合、デフォルト グループ ポリシー DfltGrpPolicy に設定されている属性が適用されます。

例

次に、「POP3Spermit」という名前の許可サーバのセットを使用するように POP3S 電子メール プロキシを設定する例を示します。

```
ciscoasa(config)# pop3s
ciscoasa(config-pop3s)# authorization-server-group POP3Spermit
```

関連コマンド

コマンド	説明
aaa-server host	認証、許可、およびアカウンティング サーバを設定します。
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。

authorization-server-group（トンネル グループ一般属性）

すべてのリモート アクセス VPN のトンネル グループに使用する認可サーバのセットを指定するには、各モードで **authorization-server-group** コマンドを使用します。認可サーバをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

authorization-server-group [(*if_name*)] *group_tag*

no authorization-server-group

構文の説明

group_tag	設定済みの認可サーバまたはサーバ グループを指定します。認可サーバを設定するには、**aaa-server** コマンドを使用します。
(*if_name*)	（任意）トンネルが終了するインターフェイスの名前。カッコを含める必要があります。

デフォルト

デフォルトでは、認可サーバは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般属性コンフィギュレーション モードに移動されました。

使用上のガイドライン

ASA では、認可を使用して、ユーザに許可されているネットワーク リソースへのアクセス レベルを確認します。aaa-server コマンドで使用する認可用のサーバ設定を使用します。

このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ一般属性モードの同等のコマンドに変換されます。

VPN 認可が LOCAL と定義されている場合、デフォルト グループ ポリシー DfltGrpPolicy に設定されている属性が適用されます。

例

次に、トンネル一般コンフィギュレーション モードで、「remotegrp」という名前の IPsec リモート アクセス トンネル グループに「aaa-server78」という名前の認可サーバ グループを設定する例を示します。

```
ciscoasa(config)# tunnel-group remotegrp type ipsec-ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# authorization-server-group aaa-server78
ciscoasa(config-tunnel-general)#
```

関連コマンド

コマンド	説明
aaa-server host	認証、許可、およびアカウンティング サーバを設定します。
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。

authorize-only

RADIUS AAA サーバ グループに対して authorize-only モードをイネーブルにするには、AAA サーバ グループ コンフィギュレーション モードで **authorize-only** コマンドを使用します。authorize-only モードをディセーブルにするには、このコマンドの **no** 形式を使用します。

authorize-only

no authorize-only

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

authorize-only モードはイネーブルになっていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
aaa サーバ グループ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、ISE 認可変更（CoA）のために RADIUS サーバ グループを authorize-only モードで設定するために使用します。authorize-only モードを使用すると、RADIUS ホスト用に設定された RADIUS 共通パスワードはすべて無視されます。

ISE Change of Authorization（CoA）機能は、認証、認可、およびアカウンティング（AAA）セッションの属性を、セッション確立後に変更するためのメカニズムを提供します。AAA のユーザまたはユーザ グループのポリシーを変更すると、ISE から ASA へ CoA パケットを直接送信して認証を再初期化し、新しいポリシーを適用できます。インライン ポスチャ実施ポイント（IPEP）で、ASA と確立された各 VPN セッションのアクセス コントロール リスト（ACL）を適用する必要がなくなりました。

エンド ユーザが VPN 接続を要求すると、ASA はユーザに対して ISE 認証を実行し、ネットワークへの制限付きアクセスを提供する ACL を受領します。アカウンティング開始メッセージが ISE に送信され、セッションが登録されます。ポスチャ アセスメントが NAC エージェントと ISE 間で直接行われます。このプロセスは、ASA に透過的です。ISE が CoA の「ポリシー プッシュ」を介して ASA にポリシーの更新を送信します。これにより、ネットワーク アクセス権限を高める新しいユーザ ACL が識別されます。後続の CoA 更新を介し、接続のライフタイム中に追加のポリシー評価が ASA に透過的に行われる場合があります。

例

次に、ISE でローカル証明書の検証と認可用のトンネル グループを設定する例を示します。サーバ グループは認証用に使用されないため、**authorize-only** コマンドをサーバ グループ コンフィギュレーションに組み込みます。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

関連コマンド

コマンド	説明
dynamic-authorization	RADIUS サーバ グループ用のダイナミック認可をイネーブルにします。
interim-accounting-update	RADIUS 中間アカウンティング アップデート メッセージの生成をイネーブルにします。
without-csd	特定のトンネル グループに行われる接続のホストスキャン処理をオフに切り替えます。

auth-prompt

ASA を介したユーザ セッションの AAA チャレンジ テキストを指定または変更するには、グローバル コンフィギュレーション モードで **auth-prompt** コマンドを使用します。認証チャレンジ テキストを削除するには、このコマンドの **no** 形式を使用します。

auth-prompt prompt [**prompt** | **accept** | **reject**] *string*

no auth-prompt prompt [**prompt** | **accept** | **reject**]

構文の説明

accept	Telnet 経由のユーザ認証を受け入れる場合、プロンプトとして *string* を表示します。
prompt	このキーワードの後に AAA チャレンジ プロンプトのストリングを入力します。
reject	Telnet 経由のユーザ認証を拒否する場合、プロンプトとして *string* を表示します。
string	最大 235 文字の英数字または 31 単語のストリング。最初に達した、いずれかの最大数により制限されます。特殊文字、スペース、および句読点を使用できます。疑問符を入力するか、または **Enter** キーを押すと、ストリングが終了します（疑問符はストリングに含まれます）。

デフォルト

認証プロンプトを指定しない場合は、次のようになります。

- FTP ユーザには `FTP authentication` が表示されます。
- HTTP ユーザには `HTTP Authentication` が表示されます。
- Telnet ユーザにはチャレンジ テキストが表示されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	セマンティックに小さな変更が加えられました。

使用上のガイドライン

auth-prompt コマンドを使用すると、TACACS+ サーバまたは RADIUS サーバからのユーザ認証が必要な場合に、ASA 経由の HTTP、FTP、および Telnet アクセス用の AAA チャレンジ テキストを指定できます。このテキストは飾りのようなもので、ユーザのログイン時に、ユーザ名プロンプトとパスワード プロンプトの上に表示されます。

Telnet からのユーザ認証が行われる場合、**accept** オプションと **reject** オプションを使用して、認証試行が AAA サーバによって受け入れられたか拒否されたかを示す各ステータス プロンプトを表示できます。

AAA サーバがユーザを認証すると、ASA は **auth-prompt accept** テキスト（指定されている場合）をユーザに表示します。ユーザが認証されない場合は、**reject** テキスト（指定されている場合）を表示します。HTTP セッションおよび FTP セッションの認証では、プロンプトにチャレンジ テキストのみが表示されます。**accept** および **reject** テキストは表示されません。

（注） Microsoft Internet Explorer では、認証プロンプトに最大 37 文字表示されます。Telnet および FTP では、認証プロンプトに最大 235 文字表示されます。

例

次に、認証プロンプトを「Please enter your username and password」という文字列に設定する例を示します。

```
ciscoasa(config)# auth-prompt prompt Please enter your username and password
```

このストリングがコンフィギュレーションに追加されると、ユーザには次のように表示されます。

```
Please enter your username and password
User Name:
Password:
```

Telnet ユーザに対しては、ASA が認証試行を受け入れたときに表示されるメッセージと拒否したときに表示されるメッセージを別々に指定できます。次に例を示します。

```
ciscoasa(config)# auth-prompt reject Authentication failed. Try again.
ciscoasa(config)# auth-prompt accept Authentication succeeded.
```

次に、認証に成功した場合の認証プロンプトを「You're OK.」という文字列に設定する例を示します。

```
ciscoasa(config)# auth-prompt accept You’re OK.
```

認証に成功すると、ユーザには次のメッセージが表示されます。

```
You’re OK.
```

関連コマンド

コマンド	説明
clear configure auth-prompt	指定済みの認証プロンプト チャレンジ テキスト（ある場合）を削除し、デフォルト値に戻します。
show running-config auth-prompt	現在の認証プロンプト チャレンジ テキストを表示します。

auto-signon

クライアントレス SSL VPN 接続用のユーザ ログイン クレデンシャルを内部サーバに自動的に渡すように ASA を設定するには、webvpn コンフィギュレーション モード、webvpn グループ コンフィギュレーション モード、または webvpn ユーザ名コンフィギュレーション モードのいずれかのモードで **auto-signon** コマンドを使用します。特定のサーバへの自動サインオンをディセーブルにするには、元の **ip**、**uri**、および **auth-type** 引数を指定して、このコマンドの **no** 形式を使用します。すべてのサーバへの自動サインオンをディセーブルにするには、このコマンドの **no** 形式を引数なしで使用します。

auto-signon allow {**ip** *ip-address ip-mask* | **uri** *resource-mask*} **auth-type** {**basic** | **ftp** | **ntlm** | **all**}

no auto-signon [**allow** {**ip** *ip-address ip-mask* | **uri** *resource-mask*} **auth-type** {**basic** | **ftp** | **ntlm** | **all**}]

構文の説明

all	NTLM と HTTP 基本認証の両方の方式を指定します。
allow	特定のサーバに対する認証をイネーブルにします。
auth-type	認証方式の選択をイネーブルにします。
basic	HTTP 基本認証方式を指定します。
FTP	FTP および CIFS 認証タイプ。
ip	IP アドレスとマスクで認証先のサーバを特定することを指定します。
ip-address	*ip-mask* とともに使用して、認証先のサーバの IP アドレス範囲を特定します。
ip-mask	*ip-address* とともに使用して、認証先のサーバの IP アドレス範囲を特定します。
ntlm	NTLMv1 認証方式を指定します。
resource-mask	認証先のサーバの URI マスクを指定します。
uri	URI マスクで認証先のサーバを特定することを指定します。

デフォルト

デフォルトでは、この機能はすべてのサーバでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション(グローバル)	• 対応	—	• 対応	—	—
webvpn グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—
WebVPN ユーザ名コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
8.0(1)	NTLMv2 のサポートが追加されました。**ntlm** キーワードには、NTLMv1 と NTLMv2 の両方が含まれます。

使用上のガイドライン

auto-signon コマンドは、クライアントレス SSL VPN ユーザのためのシングル サインオン方式です。この方式では、ログイン クレデンシャル（ユーザ名とパスワード）を NTLM 認証と HTTP 基本認証のいずれか一方または両方を使用する認証用の内部サーバに渡します。複数の auto-signon コマンドを入力でき、それらのコマンドは入力順に処理されます（先に入力したコマンドが優先されます）。

auto-signon 機能は、webvpn コンフィギュレーション グループ ポリシー モード、webvpn コンフィギュレーション モード、または webvpn ユーザ名コンフィギュレーション モードの 3 つのモードで使用できます。一般的な優先動作が適用されます。つまり、グループよりもユーザ名が優先され、グローバルよりもグループが優先されます。モードは、認証の目的範囲に基づいて選択します。

モード	スコープ
webvpn コンフィギュレーション	すべての WebVPN ユーザ（グローバル）
webvpn グループ コンフィギュレーション	グループ ポリシーで定義される WebVPN ユーザのサブセット
WebVPN ユーザ名コンフィギュレーション	個々の WebVPN ユーザ

例

次に、NTLM 認証を使用して、すべてのクライアントレス ユーザに自動サインオンを設定する例を示します。認証先のサーバの IP アドレス範囲は、10.1.1.0 ～ 10.1.1.255 です。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type ntlm
```

次に、HTTP 基本認証を使用して、すべてのクライアントレス ユーザに自動サインオンを設定する例を示します。認証先のサーバは、URI マスク https://*.example.com/* で定義されています。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# auto-signon allow uri https://*.example.com/* auth-type basic
```

次に、HTTP 基本認証または NTLM 認証を使用して、クライアントレス ユーザの ExamplePolicy グループ ポリシーに自動サインオンを設定する例を示します。認証先のサーバは、URI マスク https://*.example.com/* で定義されています。

```
ciscoasa(config)# group-policy ExamplePolicy attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# auto-signon allow uri https://*.example.com/* auth-type all
```

次に、HTTP 基本認証を使用して、Anyuser という名前のユーザに自動サインオンを設定する例を示します。認証先のサーバの IP アドレス範囲は、10.1.1.0 ～ 10.1.1.255 です。

```
ciscoasa(config)# username Anyuser attributes
ciscoasa(config-username)# webvpn
ciscoasa(config-username-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type
basic
```

関連コマンド

コマンド	説明
show running-config webvpn auto-signon	実行コンフィギュレーションの自動サインオンの割り当てを表示します。

auto-summary

ネットワークレベル ルートへのサブネット ルートの自動集約をイネーブルにするには、ルータ コンフィギュレーション モードで **auto-summary** コマンドを使用します。ルート集約をディセーブルにするには、このコマンドの **no** 形式を使用します。

auto-summary

no auto-summary

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

ルート集約は、RIP バージョン 1、RIP バージョン 2、および EIGRP でイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.0(2)	EIGRP のサポートが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

ルート集約により、ルーティング テーブルにおけるルーティング情報の量が少なくなります。

RIP バージョン 1 では、常に自動集約が使用されます。RIP バージョン 1 に対して自動集約をディセーブルにすることはできません。

RIP バージョン 2 を使用している場合は、**no auto-summary** コマンドを指定して、自動集約をオフにすることができます。切断されているサブネット間のルーティングを実行する必要がある場合は、自動サマライズをディセーブルにします。自動サマライズをディセーブルにすると、サブネットがアドバタイズされます。

EIGRP 集約ルートには、アドミニストレーティブ ディスタンス値 5 が割り当てられます。この値は設定できません。

実行コンフィギュレーションではこのコマンドの **no** 形式のみが表示されます。

例

次に、RIP ルート集約をディセーブルにする例を示します。

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# version 2
ciscoasa(config-router)# no auto-summary
```

次に、自動 EIGRP ルート集約をディセーブルにする例を示します。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# no auto-summary
```

関連コマンド

コマンド	説明
clear configure router	実行コンフィギュレーションからすべての **router** コマンドとルータ コンフィギュレーション モード コマンドをクリアします。
router eigrp	EIGRP ルーティング プロセスをイネーブルにし、EIGRP ルータ コンフィギュレーション モードを開始します。
router rip	RIP ルーティング プロセスをイネーブルにし、RIP ルータ コンフィギュレーション モードを開始します。
show running-config router	実行コンフィギュレーション内の **router** コマンドとルータ コンフィギュレーション モード コマンドを表示します。

auto-update device-id

Auto Update Server で使用する ASA のデバイス ID を設定するには、グローバル コンフィギュレーション モードで **auto-update device-id** コマンドを使用します。デバイス ID を削除するには、このコマンドの **no** 形式を使用します。

auto-update device-id [**hardware-serial** | **hostname** | **ipaddress** [*if_name*] | **mac-address** [*if_name*] | **string** *text*]

no auto-update device-id [**hardware-serial** | **hostname** | **ipaddress** [*if_name*] | **mac-address** [*if_name*] | **string** *text*]

構文の説明

hardware-serial	ASA のハードウェア シリアル番号を使用して、デバイスを一意に識別します。
hostname	ASA のホスト名を使用して、デバイスを一意に識別します。
ipaddress [*if_name*]	ASA の IP アドレスを使用して、ASA を一意に識別します。デフォルトでは、ASA は Auto Update Server との通信に使用するインターフェイスを使用します。別の IP アドレスを使用する場合は、*if_name* オプションを指定します。
mac-address [*if_name*]	ASA の MAC アドレスを使用して、ASA を一意に識別します。デフォルトでは、ASA は Auto Update Server との通信に使用するインターフェイスの MAC アドレスを使用します。別の MAC アドレスを使用する場合は、*if_name* オプションを指定します。
string *text*	テキスト ストリングを指定して、デバイスを Auto Update Server に対して一意に識別します。

デフォルト

デフォルト ID はホスト名です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、デバイス ID をシリアル番号に設定する例を示します。

```
ciscoasa(config)# auto-update device-id hardware-serial
```

関連コマンド

auto-update poll-period	Auto Update Server からのアップデートを ASA が確認する頻度を設定します。
auto-update server	Auto Update Server を指定します。
auto-update timeout	タイムアウト期間内に Auto Update Server に接続されない場合、ASA を通過するトラフィックを停止します。
clear configure auto-update	Auto Update Server コンフィギュレーションをクリアします。
show running-config auto-update	Auto Update Server コンフィギュレーションを表示します。

auto-update poll-at

ASA が Auto Update Server をポーリングする特定の日時をスケジューリングするには、グローバル コンフィギュレーション モードで **auto-update poll-at** コマンドを使用します。ASA が Auto Update Server をポーリングするようにスケジューリングした日時のうち、指定した日時をすべて削除するには、このコマンドの **no** 形式を使用します。

auto-update poll-at *days-of-the-week time* [**randomize** *minutes*] [*retry_count* [*retry_period*]]

no auto-update poll-at *days-of-the-week time* [**randomize** *minutes*] [*retry_count* [*retry_period*]]

構文の説明

days-of-the-week	任意の 1 つの曜日（Monday、Tuesday、Wednesday、Thursday、Friday、Saturday、および Sunday）または曜日の組み合わせ。その他の指定可能な値は、daily（月曜日から日曜日まで）、weekdays（月曜日から金曜日まで）、および weekend（土曜日と日曜日）です。
randomize *minutes*	指定した開始日時の後に、不定期にポーリングする期間を 1 ～ 1,439 分で指定します。
retry_count	Auto Update Server への接続の初回試行が失敗した場合に、再接続を何回試行するかを指定します。デフォルトは 0 です。
retry_period	接続試行の間隔を指定します。デフォルトは 5 分です。指定できる範囲は 1 ～ 35791 分です。
時刻	ポーリングを開始する時刻を HH:MM 形式で指定します。たとえば、8:00 は午前 8 時で、20:00 は午後 8 時です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

auto-update poll-at コマンドでは、アップデートをポーリングする時刻を指定します。**randomize** オプションをイネーブルにすると、最初の *time* オプションの時刻から指定した期間（分単位）内に、ポーリングが不定期に実行されます。**auto-update poll-at** および **auto-update poll-period** コマンドは、同時に使用できません。いずれか 1 つのみを設定できます。

例

次の例では、ASA は、毎週金曜日と土曜日の午後 10 時から午後 11 時までの間、不定期に Auto Update Server をポーリングします。ASA がサーバに接続できない場合は、10 分おきにさらに 2 回、接続を試行します。

```
ciscoasa(config)# auto-update poll-at Friday Saturday 22:00 randomize 60 2 10
ciscoasa(config)# auto-update server http://192.168.1.114/aus/autoupdate.asp
```

関連コマンド

auto-update device-id	Auto Update Server で使用するための ASA デバイス ID を設定します。
auto-update poll-period	Auto Update Server からのアップデートを ASA が確認する頻度を設定します。
auto-update timeout	タイムアウト期間内に Auto Update Server に接続されない場合、ASA を通過するトラフィックを停止します。
clear configure auto-update	Auto Update Server コンフィギュレーションをクリアします。
management-access	ASA の内部管理インターフェイスへのアクセスをイネーブルにします。
show running-config auto-update	Auto Update Server コンフィギュレーションを表示します。

auto-update poll-period

ASA が Auto Update Server からのアップデートを確認する頻度を設定するには、グローバル コンフィギュレーション モードで **auto-update poll-period** コマンドを使用します。パラメータをデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]

no auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]

構文の説明

poll_period	Auto Update Server をポーリングする頻度を分単位（1 ～ 35791）で指定します。デフォルトは 720 分（12 時間）です。
retry_count	Auto Update Server への接続の初回試行が失敗した場合に、再接続を何回試行するかを指定します。デフォルトは 0 です。
retry_period	接続試行の間隔を分単位（1 ～ 35791）で指定します。デフォルトは 5 分です。

デフォルト

デフォルトのポーリング期間は、720 分（12 時間）です。

Auto Update Server への最初の接続試行に失敗した場合に再接続を試行するデフォルトの回数は 0 です。

接続試行のデフォルト間隔は 5 分です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

auto-update poll-at および **auto-update poll-period** コマンドは、同時に使用できません。いずれか 1 つのみを設定できます。

例

次に、ポーリング期間を 360 分に、再試行回数を 1 回に、再試行間隔を 3 分に設定する例を示します。

```
ciscoasa(config)# auto-update poll-period 360 1 3
```

関連コマンド

auto-update device-id	Auto Update Server で使用するための ASA デバイス ID を設定します。
auto-update server	Auto Update Server を指定します。
auto-update timeout	タイムアウト期間内に Auto Update Server に接続されない場合、ASA を通過するトラフィックを停止します。
clear configure auto-update	Auto Update Server コンフィギュレーションをクリアします。
show running-config auto-update	Auto Update Server コンフィギュレーションを表示します。

auto-update server

Auto Update Server を指定するには、グローバル コンフィギュレーション モードで **auto-update server** コマンドを使用します。サーバを削除するには、このコマンドの **no** 形式を使用します。

auto-update server *url* [**source** *interface*] {**verify-certificate** | **no-verification**}

no auto-update server *url* [**source** *interface*] {**verify-certificate** | **no-verification**}

構文の説明

no-verification	Auto Update Server 証明書を確認しません。
source *interface*	要求を Auto Update Server に送信するときに使用するインターフェイスを指定します。**management-access** コマンドで指定したインターフェイスと同じインターフェイスを指定すると、Auto Update 要求は管理アクセスに使用されるのと同じ IPsec VPN トンネルを通過します。
url	次の構文を使用して、Auto Update Server の場所を指定します。 **http**[**s**]**:**[[*user:password*@]*location* [:*port*]] **/** *pathname*
verify-certificate	HTTPS の場合、Auto Update Server から返された証明書を確認します。この設定は、デフォルトです。

デフォルト

9.1 以前：証明書の確認はディセーブルになっています。

9.2(1) 以降：**verify-certificate** オプションはデフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	複数のサーバをサポートできるようにコマンドが変更されました。
9.2(1)	Auto Update Server 証明書の確認がデフォルトでイネーブルになりました。**no-verification** キーワードが追加されました。

使用上のガイドライン

ASA は、定期的に Auto Update Server にアクセスして、コンフィギュレーション、オペレーティング システム、および ASDM の更新がないか調べます。

自動アップデート用に複数のサーバを設定できます。アップデートを確認するときに、最初のサーバに接続しますが、接続に失敗した場合は、次のサーバに接続します。このプロセスは、すべてのサーバを試行するまで続行されます。どのサーバにも接続できなかった場合は、auto-update poll-period が接続を再試行するように設定されていれば、最初のサーバから順に接続が再試行されます。

自動アップデート機能を正しく動作させるには、**boot system configuration** コマンドを使用して、有効なブート イメージを指定する必要があります。また、ASDM ソフトウェア イメージを更新するには、auto-update とともに **asdm image** コマンドを使用する必要があります。

source *interface* 引数で指定されたインターフェイスが **management-access** コマンドで指定されたインターフェイスと同じである場合、Auto Update Server への要求は VPN トンネルを介して送信されます。

9.2(1) 以降：Auto Update Server 証明書の確認がデフォルトでイネーブルになりました。新しい設定の場合、証明書の確認を明示的にディセーブルにする必要があります。証明書の確認をイネーブルにしていなかった場合に、以前のリリースからアップグレードしようとすると、証明書の確認はイネーブルではなく、次の警告が表示されます。

```
WARNING: The certificate provided by the auto-update servers will not be verified. In
order to verify this certificate please use the verify-certificate option.
```

設定を移行する場合は、次のように確認なしを明示的に設定します。

auto-update server no-verification

例

次に、Auto Update Server の URL を設定し、インターフェイスを outside として指定する例を示します。

```
ciscoasa(config)# auto-update server http://10.1.1.1:1741/ source outside
verify-certificate
```

関連コマンド

auto-update device-id	Auto Update Server で使用するための ASA デバイス ID を設定します。
auto-update poll-period	Auto Update Server からのアップデートを ASA が確認する頻度を設定します。
auto-update timeout	タイムアウト期間内に Auto Update Server に接続されない場合、ASA を通過するトラフィックを停止します。
clear configure auto-update	Auto Update Server コンフィギュレーションをクリアします。
management-access	ASA の内部管理インターフェイスへのアクセスをイネーブルにします。
show running-config auto-update	Auto Update Server コンフィギュレーションを表示します。

auto-update timeout

Auto Update Server へのアクセスのタイムアウト期間を設定するには、グローバル コンフィギュレーション モードで **auto-update timeout** コマンドを使用します。タイムアウトを削除するには、このコマンドの **no** 形式を使用します。

auto-update timeout [*period*]

no auto-update timeout [*period*]

構文の説明

period	タイムアウト期間を分単位（1 ～ 35791）で指定します。デフォルトは 0 で、タイムアウトがないことを意味します。タイムアウトを 0 に設定することはできません。タイムアウトを 0 にリセットするには、このコマンドの **no** 形式を使用します。

デフォルト

デフォルトのタイムアウトは 0 で、ASA はタイムアウトしないように設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

タイムアウト状態は、syslog メッセージ 201008 でレポートされます。

タイムアウト期間内に Auto Update Server へのアクセスが行われなかった場合、ASA はそれを通過するすべてのトラフィックを停止します。タイムアウトを設定すると、ASA に最新のイメージとコンフィギュレーションが保持されます。

例

次に、タイムアウトを 24 時間に設定する例を示します。

```
ciscoasa(config)# auto-update timeout 1440
```

関連コマンド

auto-update device-id	Auto Update Server で使用するための ASA デバイス ID を設定します。
auto-update poll-period	Auto Update Server からのアップデートを ASA が確認する頻度を設定します。
auto-update server	Auto Update Server を指定します。
clear configure auto-update	Auto Update Server コンフィギュレーションをクリアします。
show running-config auto-update	Auto Update Server コンフィギュレーションを表示します。

CHAPTER 4

backup コマンド～ browse-networks コマンド

backup

ASA のコンフィギュレーション、証明書、キー、およびイメージをバックアップするには、特権 EXEC モードで **backup** コマンドを使用します。

backup [**/noconfirm**] [**context** *ctx-name*] [**interface** *name*] [**passphrase** *value*] [**location** *path*]

構文の説明

/noconfirm	**location** パラメータと **cert-passphrase** パラメータの入力を要求しないように指定します。警告およびエラー メッセージをバイパスしてバックアップを続行できるようにします。
context *ctx-name*	システム実行スペースからのマルチ コンテキスト モードで、**context** キーワードを入力して、指定したコンテキストをバックアップします。各コンテキストを個別にバックアップする必要があります。つまり、各ファイルに対して **backup** コマンドをもう一度入力します。
interface *name*	(任意)バックアップをコピーするインターフェイスの名前を指定します。インターフェイスを指定しなかった場合、ASA は管理専用ルーティング テーブルを確認し、一致するものが見つからなければ、データのルーティング テーブルを確認します。
location *path*	バックアップの **location** にはローカル ディスクまたはリモート URL を指定できます。location を指定しない場合は、次のデフォルト名が使用されます。 • シングル モード: disk0:*hostname*.backup.*timestamp*.tar.gz • マルチ モード: disk0:*hostname*.context-*ctx-name*.backup.*timestamp*.tar.gz
passphrase *value*	VPN 証明書および事前共有キーのバックアップ中、証明書を符号化するために、**cert-passphrase** キーワードで指定された秘密キーが必要です。PKCS12 形式の証明書を符号化および復号化するために使用するパスフレーズを入力する必要があります。バックアップに含まれるのは証明書に関連する RSA キー ペアだけであり、スタンドアロン証明書は除外されます。

デフォルト

location を指定しない場合は、次のデフォルト名が使用されます。

- シングル モード：disk0:*hostname*.backup.*timestamp*.tar.gz
- マルチ モード：disk0:*hostname*.context-*ctx-name*.backup.*timestamp*.tar.gz

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。
9.5(1)	**interface** *name* 引数が追加されました。

使用上のガイドライン

次のガイドラインを参照してください。

- バックアップを開始する前に、バックアップ場所に 300 MB 以上のディスク領域が使用可能である必要があります。
- バックアップ中またはバックアップ後にコンフィギュレーションを変更した場合、その変更内容はバックアップに含められません。バックアップの実行後にコンフィギュレーションを変更してから復元を実行した場合、このコンフィギュレーションの変更は上書きされます。その結果、ASA が異なる動作をする可能性があります。
- バックアップは一度に 1 つだけ開始できます。
- コンフィギュレーションは、元のバックアップを実行したときと同じ ASA バージョンにのみ復元できます。復元ツールを使用して、ASA の異なるバージョン間でコンフィギュレーションを移行することはできません。コンフィギュレーションの移行が必要な場合、新しい ASA OS のロード時に、ASA によって常駐スタートアップ コンフィギュレーションが自動的にアップグレードされます。
- クラスタリングを使用する場合、バックアップできるのは、スタートアップ コンフィギュレーション、実行コンフィギュレーション、およびアイデンティティ証明書のみです。ユニットごとに別々にバックアップを作成および復元する必要があります。
- フェールオーバーを使用する場合、バックアップの作成および復元は、アクティブ ユニットとスタンバイ ユニットに対して別々に行う必要があります。
- ASA にマスター パスフレーズを設定している場合は、この手順で作成したバックアップ コンフィギュレーションの復元時にそのマスター パスフレーズが必要となります。ASA のマスター パスフレーズが不明な場合は、CLI 設定ガイドを参照して、バックアップを続行する前に、マスター パスフレーズをリセットする方法を確認してください。

- PKCS12 データをインポート（**crypto ca trustpoint** コマンドを使用）する際にトラストポイントが RSA キーを使用している場合、インポートされたキー ペアにはトラストポイントと同じ名前が割り当てられます。この制約のため、ASDM コンフィギュレーションを復元した後でトラストポイントおよびそのキー ペアに別の名前を指定した場合、スタートアップ コンフィギュレーションは元のコンフィギュレーションと同じになるのに、実行コンフィギュレーションには異なるキー ペア名が含まれることになります。つまり、キー ペアとトラストポイントに別の名前を使用した場合は、元のコンフィギュレーションを復元できないということです。この問題を回避するため、トラストポイントとそのキー ペアには必ず同じ名前を使用してください。
- インターフェイスを指定しなかった場合、ASA は管理専用ルーティング テーブルを確認し、一致するものが見つからなければ、データのルーティング テーブルを確認します。管理専用インターフェイスを経由するデフォルト ルートがある場合は、すべての**バックアップ** トラフィックがそのルートに一致するため、データ ルーティング テーブルが確認されることはありません。このシナリオでは、データ インターフェイスを経由してバックアップする必要がある場合は常にインターフェイスを指定します。
- CLI を使用してバックアップしてから ASDM を使用して復元したり、その逆を行うことはできません。
- backup location コマンドを発行する場合、ディレクトリパスに二重スラッシュ「//」を使用してください。次に例を示します。

  ```
  ciscoasa# backup location disk0://sample-backup
  ```

- 各バックアップ ファイルに含まれる内容は次のとおりです。
  - 実行コンフィギュレーション
  - スタートアップ コンフィギュレーション
  - すべてのセキュリティ イメージ

    Cisco Secure Desktop およびホスト スキャンのイメージ

    Cisco Secure Desktop およびホスト スキャンの設定

    AnyConnect（SVC）クライアントのイメージおよびプロファイル

    AnyConnect（SVC）のカスタマイズおよびトランスフォーム
  - アイデンティティ証明書（アイデンティティ証明書に関連付けられた RSA キー ペアは含まれるが、スタンドアロン キーは除外される）
  - VPN 事前共有キー
  - SSL VPN コンフィギュレーション
  - アプリケーション プロファイルのカスタム フレームワーク（APCF）
  - ブックマーク
  - カスタマイゼーション
  - ダイナミック アクセス ポリシー（DAP）
  - プラグイン
  - 接続プロファイル用の事前入力スクリプト
  - プロキシ自動設定
  - 変換テーブル
  - Web コンテンツ
  - バージョン情報

例

次に、バックアップを作成する例を示します。

```
ciscoasa# backup location disk0://sample-backup
Backup location [disk0://sample-backup]?

Begin backup…
Backing up [ASA version] … Done!
Backing up [Running Config] … Done!
Backing up [Startup Config]  … Done!

Enter a passphrase to encrypt identity certificates. The default is cisco. You will be
required to enter the same passphrase while doing a restore: cisco
Backing up [Identity Certificates] … Done!

IMPORTANT: This device uses master passphrase encryption. If this backup file is used to
restore to a device with a different master passphrase, you will need to provide the
current master passphrase during restore.
Backing up [VPN Pre-shared keys] … Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] … Done!
Backing up [SSL VPN Configurations: Bookmarks]… Done!
Backing up [SSL VPN Configurations: Customization] … Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] … Done!
Backing up [SSL VPN Configurations: Plug-in] … Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] … Done!
Backing up [SSL VPN Configurations: Proxy auto-config] … Done!
Backing up [SSL VPN Configurations: Translation table] … Done!
Backing up [SSL VPN Configurations: Web Content] … Done!
Backing up [Anyconnect(SVC) client images and profiles] … Done!
Backing up [Anyconnect(SVC) customizations and transforms] … Done!
Backing up [Cisco Secure Desktop and Host Scan images] … Done!
Backing up [UC-IME tickets] … Done!
Compressing the backup directory ... Done!
Copying Backup ... Done!
Cleaning up ... Done!
Backup finished!
```

関連コマンド

コマンド	説明
restore	バックアップ ファイルから ASA のコンフィギュレーション、キー、証明書、およびイメージを復元します。

backup interface

ASA 5505 など、組み込みスイッチを搭載したモデルの場合、インターフェイス コンフィギュレーション モードで **backup interface** コマンドを使用して、ISP などへのバックアップ インターフェイスとして VLAN インターフェイスを指定します。通常の動作に戻すには、このコマンドの **no** 形式を使用します。

backup interface vlan *number*

no backup interface vlan *number*

構文の説明

vlan *number*	バックアップ インターフェイスの VLAN ID を指定します。

デフォルト

デフォルトでは、**backup interface** コマンドはディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
7.2(2)	Security Plus ライセンスでは、VLAN インターフェイス数の制限（通常のトラフィック用は 3 つ、バックアップ インターフェイス用は 1 つ、フェールオーバー用は 1 つ）がなくなり、最大 20 のインターフェイスを設定できるようになりました（最大数以外の制限はありません）。したがって、4 つ以上のインターフェイスをイネーブルにするために **backup interface** コマンドを使用する必要はありません。

使用上のガイドライン

このコマンドを入力できるのは、VLAN インターフェイスのインターフェイス コンフィギュレーション モードだけです。このコマンドは、プライマリ インターフェイスを経由するデフォルト ルートがダウンしない限り、指定したバックアップ インターフェイスを通過しようとするトラフィックをすべてブロックします。

backup interface コマンドで Easy VPN を設定した場合は、バックアップ インターフェイスがプライマリになると、ASA は VPN ルールを新しいプライマリ インターフェイスに移動します。バックアップ インターフェイスの状態を表示する方法については、**show interface** コマンドを参照してください。

必ずプライマリ インターフェイスとバックアップ インターフェイスの両方にデフォルト ルートを設定して、プライマリ インターフェイスに障害が発生した場合にバックアップ インターフェイスを使用できるようにしてください。たとえば、2 つのデフォルト ルートを設定して、1 つはアドミニストレーティブ ディスタンスが低いプライマリ インターフェイス用とし、もう 1 つはアドミニストレーティブ ディスタンスが高いバックアップ インターフェイス用とすることができます。DHCP サーバから取得したデフォルト ルートのアドミニストレーティブ ディスタンスを上書きする方法については、**dhcp client route distance** コマンドを参照してください。デュアル ISP サポートの設定の詳細については、**sla monitor** コマンドおよび **track rtr** コマンドを参照してください。

management-only コマンドをすでに設定しているインターフェイスをバックアップ インターフェイスに設定することはできません。

例

次に、4 つの VLAN インターフェイスを設定する例を示します。backup-isp インターフェイスは、プライマリ インターフェイスがダウンしている場合に限り、通過トラフィックを許可します。**route** コマンドでは、プライマリ インターフェイスとバックアップ インターフェイスのデフォルト ルートを作成し、バックアップ ルートには低いアドミニストレーティブ ディスタンスを設定しています。

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# backup interface vlan 400
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 200
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 300
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.3.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 400
ciscoasa(config-if)# nameif backup-isp
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 400
ciscoasa(config-if)# no shutdown
```

```
ciscoasa(config-if)# route outside 0 0 10.1.1.2 1
ciscoasa(config)# route backup-isp 0 0 10.1.2.2 2
```

関連コマンド

コマンド	説明
forward interface	インターフェイスが別のインターフェイスへのトラフィックを開始することを制限します。
interface vlan	VLAN インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
dhcp client route distance	DHCP サーバから取得したデフォルト ルートのアドミニストレーティブ ディスタンスを上書きします。
sla monitor	スタティック ルートのトラッキングの SLA モニタリング動作を作成します。
track rtr	SLA モニタリング動作の状態を追跡します。

backup-package auto

Cisco ISA 3000 で自動バックアップと復元の操作を設定するには、特権 EXEC モードで **backup-package auto** コマンドを使用します。自動バックアップまたは復元を無効にするには、このコマンドの **no** 形式を使用します。

backup-package {**backup** | **restore**} **auto**

no backup-package {**backup** | **restore**} **auto**

構文の説明

バックアップ	自動バックアップを設定していることを示します。
restore	自動復元を設定していることを示します。

デフォルト

デフォルトのバックアップと復元のモードは手動です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

バックアップと復元のモードは独立しており、個別に設定できます。

自動バックアップと復元の操作にバックアップと復元の設定パラメータを指定するには、**backup-package location** コマンドを使用します。

例

次に、**backup-package** コマンドを使用して自動バックアップを設定する例を示します。

```
ciscoasa# backup-package backup auto
```

関連コマンド

コマンド	説明
show backup-package summary	バックアップと復元のパッケージ パラメータのサマリーを表示します。

backup-package location

Cisco ISA 3000 で後続のバックアップおよび復元の操作に使用するバックアップおよび復元の場所を設定するには、特権 EXEC モードで **backup-package location** コマンドを使用します。バックアップまたは復元の場所をデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

backup-package {**backup** | **restore**} [**interface** *name*] **location disk***n***:** [**passphrase** *string*]

no backup-package {**backup** | **restore**} **location**

構文の説明

backup	バックアップ パラメータを定義していることを示します。
interface *name*	(任意)バックアップまたは復元の通信に使用するインターフェイスの名前。
location disk*n***:**	バックアップ パッケージ情報が保存されるストレージ メディアの場所。
passphrase *string*	(任意)バックアップ情報の暗号化、またはバックアップされた情報の取得に使用するパスフレーズ。
restore	復元パラメータを定義していることを示します。

デフォルト

デフォルトの場所は **disk3:** で、SD カードが含まれています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

バックアップと復元の操作は独立しており、個別に設定できます。

一般に、**backup-package** 情報の設定は、追加のパラメーターを指定しなくても後で手動でデバイス構成をバックアップおよび復元できるようにするための 1 回限りの操作です。

例

次に、**backup-package location** コマンドを使用して、暗号化パスフレーズとして「cisco」を使用してバックアップ パラメータを設定する例を示します。

```
ciscoasa# backup-package backup location disk3: passphrase cisco
```

関連コマンド

コマンド	説明
show backup-package status	バックアップまたは復元用のパッケージ情報を表示します。
show backup-package summary	バックアップと復元のパッケージ パラメータのサマリーを表示します。

backup-servers

バックアップ サーバを設定するには、グループ ポリシー コンフィギュレーション モードで **backup-servers** コマンドを使用します。バックアップ サーバを削除するには、このコマンドの **no** 形式を使用します。

backup-servers {*server1 server2. . . . server10* | **clear-client-config** | **keep-client-config**}

no backup-servers [*server1 server2. . . . server10* | **clear-client-config** | **keep-client-config**]

構文の説明

clear-client-config	クライアントがバックアップ サーバを使用しないことを指定します。ASA は、ヌルのサーバ リストをプッシュします。
keep-client-config	ASA がバックアップ サーバ情報をクライアントに送信しないことを指定します。クライアントは、独自のバックアップ サーバ リストを使用します(設定されている場合)。
server1 server 2.... server10	プライマリ ASA が利用できない場合に VPN クライアントが使用するサーバのリストを指定します。各サーバをスペースで区切り、プライオリティの高い順に並べます。サーバは、IP アドレスまたはホスト名で指定します。リストには 500 文字まで入力できますが、10 個のエントリのみを含めることができます。

デフォルト

クライアント上またはプライマリ ASA 上にバックアップ サーバを設定しない限り、バックアップ サーバは存在しません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

実行コンフィギュレーションから backup-servers 属性を削除するには、このコマンドの **no** 形式を引数なしで使用します。これにより、バックアップ サーバの値を別のグループ ポリシーから継承できます。

IPsec バックアップ サーバにより、VPN クライアントは、プライマリ ASA が利用できない場合でもセントラル サイトに接続できます。バックアップ サーバを設定すると、IPsec トンネルが確立されるときに ASA がクライアントにサーバ リストをプッシュします。

バックアップ サーバは、クライアント上またはプライマリ ASA 上に設定します。ASA 上にバックアップ サーバを設定すると、適応型セキュリティ アプライアンスは、バックアップ サーバ ポリシーをグループ内のクライアントにプッシュして、クライアント上にバックアップ サーバ リストが設定されている場合、そのリストを置き換えます。

（注） ホスト名を使用する場合は、バックアップ DNS サーバおよびバックアップ WINS サーバを、プライマリ DNS サーバおよびプライマリ WINS サーバとは別のネットワーク上に配置することを推奨します。このようにしないと、ハードウェア クライアントの背後のクライアントが DHCP を介してハードウェア クライアントから DNS 情報および WINS 情報を取得している場合、プライマリ サーバとの接続が失われ、バックアップ サーバに異なる DNS 情報と WINS 情報があると、DHCP リースが期限切れになるまでクライアントを更新できなくなります。また、ホスト名を使用している場合に DNS サーバが使用不可になると、大幅な遅延が発生するおそれがあります。

例

次に、「FirstGroup」という名前のグループ ポリシーに、IP アドレスが 10.10.10.1 と 192.168.10.14 であるバックアップ サーバを設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# backup-servers 10.10.10.1 192.168.10.14
```

banner（グローバル）

ASDM バナー、セッション バナー、ログイン バナー、または Message-of-The-Day バナーを設定するには、グローバル コンフィギュレーション モードで banner コマンドを使用します。指定されたバナー キーワード（**exec**、**login**、あるいは **motd**）からすべての行を削除するには、このコマンドの **no** 形式を使用します。

banner {**asdm** | **exec** | **login** | **motd** *text*}

[no] banner {**asdm** | **exec** | **login** | **motd** [*text*]}

構文の説明

asdm	ASDM へのログインに成功した後にバナーを表示するようにシステムを設定します。続行してログインを完了するか、または切断するかを確認するプロンプトがユーザに表示されます。このオプションを使用すると、接続の前に、書面によるポリシー条件の受け入れをユーザに求めることができます。
exec	イネーブル プロンプトを表示する前に、バナーを表示するようにシステムを設定します。
login	Telnet またはシリアル コンソールを使用して ASA にアクセスする場合、パスワード ログイン プロンプトを表示する前にバナーを表示するようにシステムを設定します。
motd	初めて接続したときに Message-of-The-Day バナーを表示するようにシステムを設定します。
text	表示するメッセージ テキスト行。

デフォルト

デフォルトでは、バナーは表示されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.2(4)/8.0(3)	**asdm** キーワードが追加されました。
9.0(1)	**banner login** コマンドは、シリアル コンソール接続をサポートします。

使用上のガイドライン

banner コマンドは、指定したキーワードに対応して表示されるようにバナーを設定します。*text* ストリングは、最初の空白（スペース）の後に続く、行末（復帰または改行（LF））までのすべての文字で構成されます。テキスト内のスペースは維持されます。ただし、CLI ではタブを入力できません。

最初に既存のバナーをクリアしない限り、後続の *text* エントリは既存のバナーの末尾に追加されていきます。

（注） $(domain) トークンと $(hostname) トークンは、ASA のドメイン名とホスト名にそれぞれ置き換えられます。コンテキスト コンフィギュレーションで $(system) トークンを入力すると、このコンテキストでは、システム コンフィギュレーションで設定されているバナーが使用されます。

バナーを複数行にするには、追加する行ごとに banner コマンドを新たに入力します。これにより、既存のバナーの末尾に各行が追加されます。

（注） バナーの認可プロンプトの最大長は、235 文字または 31 単語（最初に制限に達した方）です。

Telnet または SSH を介して ASA にアクセスする場合は、バナー メッセージの処理に必要なシステム メモリが十分ないか、または TCP 書き込みエラーが発生すると、セッションが閉じます。**exec** および **motd** バナーだけが、SSH を介した ASA へのアクセスをサポートしています。ログイン バナーは、初期接続の一部としてユーザ名を渡さない SSHv1 クライアントまたは SSH クライアントをサポートしていません。

バナーを置き換えるには、**no banner** コマンドを使用してから、新しい行を追加します。

指定したバナー キーワードのすべての行を削除するには、**no banner {exec | login | motd}** コマンドを使用します。

no banner コマンドでは、テキスト ストリングを選択して削除することはできません。そのため、**no banner** コマンドの末尾に入力したテキストはすべて無視されます。

例

次に、**asdm**、**exec**、**login**、および **motd** の各バナーを設定する例を示します。

```
ciscoasa(config)#  banner asdm You successfully logged in to ASDM
ciscoasa(config)#  banner motd Think on These Things
ciscoasa(config)#  banner exec Enter your password carefully
ciscoasa(config)#  banner login Enter your password to log in
ciscoasa(config)# show running-config banner
asdm:
You successfully logged in to ASDM

exec:
Enter your password carefully

login:
Enter your password to log in

motd:
Think on These Things
```

次に、**motd** バナーに 2 行目を追加する例を示します。

```
ciscoasa(config)# banner motd and Enjoy Today
ciscoasa(config)# show running-config banner motd
Think on These Things and Enjoy Today
```

関連コマンド

コマンド	説明
clear configure	すべてのバナーを削除します。
show running-config	すべてのバナーを表示します。

banner（グループ ポリシー）

リモート クライアントの接続時にリモート クライアント上でバナーまたはウェルカム テキストを表示するには、グループ ポリシー コンフィギュレーション モードで **banner** コマンドを使用します。バナーを削除するには、このコマンドの **no** 形式を使用します。

banner {**value** *_string* | **none**}

no banner

(注) VPN グループ ポリシーで複数のバナーを設定し、いずれかのバナーを削除すると、すべてのバナーが削除されます。

構文の説明

none	バナーにヌル値を設定して、バナーを禁止します。デフォルトまたは指定したグループ ポリシーのバナーを継承しません。
value *banner_string*	バナー テキストを設定します。ログイン後バナーの最大文字列サイズは 4,000 文字です。復帰改行を挿入するには、「\n」シーケンスを使用します。クライアントやブラウザは各行の表示制限近辺でラッピングを行うため、行ごとに 80 ～ 100 文字を設定することを推奨します。

デフォルト

デフォルトのバナーはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.5(1)	ログイン後バナー長の値を 4,000 に拡大しました。

使用上のガイドライン

バナーは ASA 上にローカルで設定されるため、ユーザはログイン後バナーに対して [Accept] または [Disconnect] をクリックする必要があります。

（注） IKEv1 や AnyConnect バージョン 3 などの古いアーキテクチャでの動作はエラーを発生させずにサポートされています。

バナーを継承しないようにするには、**banner none** コマンドを使用します。

IPsec VPN クライアントは、バナー用の完全な HTML をサポートしています。ただし、クライアントレス ポータルおよび AnyConnect クライアントは部分的な HTML をサポートしています。バナーがリモート ユーザに正しく表示されるようにするには、次のガイドラインに従います。

- IPsec クライアント ユーザの場合は、/n タグを使用します。
- AnyConnect クライアント ユーザの場合は、
 タグを使用します。
- クライアントレス ユーザの場合は、
 タグを使用します。

例

次に、「FirstGroup」という名前のグループ ポリシーにバナーを作成する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# banner value Welcome to Cisco Systems 7.0.
```

base-url

(任意)クライアントレス VPN のベース URL を設定します。この URL は、サードパーティ IdP に提供される SAML メタデータで使用されます。これにより IdP は ASA にエンドポイント ユーザをリダイレクトできるようになります。

この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

base-url {value *_string*}

no base-url

構文の説明

base-url	カウントレス VPN の URL

デフォルト

なし。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

- base-url が設定されている場合、これは AssertionConsumerService と SingleLogoutService のベース URL であり、**show saml metadata** で表示されます。
- base-url が設定されていない場合、ベース URL は ASA の hostname と domain-name から作成されます。たとえば、hostname 名が「ssl-vpn」、domain-name 名が「cisco.com」である場合、**show saml metadata** で表示されるベース URL は **https://ssl-vpn.cisco.com** です。
- base-url、または hostname と domain-name のいずれも設定されていない場合、**show saml metadata** はエラーを表示します。

例

次に、base-url を設定する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# saml idp myIdp
ciscoasa(config-webvpn-saml-idp)# base url https://ClientlessVPN.com
```

関連コマンド

コマンド	説明
signature	SAML 要求のシグニチャをイネーブルまたはディセーブルにします。デフォルトでは、シグニチャはディセーブルです。
timeout	SAML IdP タイムアウトを設定します。
trustpoint	saml-idp サブモードでトラストポイントを設定します。
url	SAML IdP URL を設定します。

basic-mapping-rule

マッピングアドレスおよびポート(MAP)ドメイン内の基本マッピングルールを設定するには、MAP ドメインのコンフィギュレーション モードで **basic-mapping-rule** コマンドを使用します。基本マッピングルールを削除するには、このコマンドの **no** 形式を使用します。

basic-mapping-rule

no basic-mapping-rule

デフォルト

デフォルト設定はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
MAP ドメイン コンフィギュレーション モード	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.13(1)	このコマンドが導入されました。

使用上のガイドライン

カスタマーエッジ(CE)デバイスは、基本マッピングルールを使用して、専用 IPv4 アドレッシングまたは共有アドレスとポート セットの割り当てを決定します。CE デバイスは最初に、システムの IPv4 アドレスをプールのプレフィックスおよびポート範囲内の IPv4 アドレスおよびポート(NAT44 を使用)に変換し、次にルールの IPv6 プレフィックスによって定義されたプール内の IPv6 アドレスに、新しい IPv4 アドレスを変換します。その後、パケットはサービスプロバイダーの IPv6 専用ネットワークを介してボーダーリレー(BR)デバイスに送信されるようになります。

basic-mapping-rule コマンドを入力すると、MAP ドメインの基本マッピング ルール コンフィギュレーション モードが開始されます。ここでは、ルールの IPv4、IPv6、およびポートのプロパティを設定できます。

例

次の例では、1 という名前の MAP-T ドメインを作成して、ドメインの変換ルールを設定しています。

```
ciscoasa(config)# map-domain 1
ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64
ciscoasa(config-map-domain)# basic-mapping-rule
ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
ciscoasa(config-map-domain-bmr)# start-port 1024
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

関連コマンド

コマンド	説明
basic-mapping-rule	MAP ドメインの基本マッピング ルールを設定します。
default-mapping-rule	MAP ドメインのデフォルト マッピング ルールを設定します。
ipv4-prefix	MAP ドメインの基本マッピング ルールの IPv4 プレフィックスを設定します。
ipv6-prefix	MAP ドメインの基本マッピング ルールの IPv6 プレフィックスを設定します。
map-domain	マッピング アドレスおよびポート(MAP)ドメインを設定します。
share-ratio	MAP ドメインの基本マッピング ルールのポート数を設定します。
show map-domain	マッピング アドレスおよびポート(MAP)ドメインに関する情報を表示します。
start-port	MAP ドメインの基本マッピング ルールの開始ポートを設定します。

basic-security

IP オプション インスペクションが設定されたパケット ヘッダーでセキュリティ(SEC)オプションが発生したときのアクションを定義するには、パラメータ コンフィギュレーション モードで **basic-security** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

basic-security action {allow | clear}

no basic-security action {allow | clear}

構文の説明

allow	セキュリティ IP オプションを含むパケットを許可します。
clear	セキュリティ オプションをパケット ヘッダーから削除してから、パケットを許可します。

デフォルト

デフォルトでは、IP オプション インスペクションは、セキュリティ IP オプションを含むパケットをドロップします。

IP オプション インスペクション ポリシー マップで **default** コマンドを使用するとデフォルト値を変更できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IP オプション インスペクション ポリシー マップで設定できます。

IP オプション インスペクションを設定して、どの IP パケットが所定の IP オプションを持ち、ASA を通過できるかを制御できます。変更せずにパケットを通過させたり、指定されている IP オプションをクリアしてからパケットを通過させたりできます。

例

次に、IP オプション インスペクションのアクションをポリシー マップで設定する例を示します。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# basic-security action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

bfd echo

インターフェイスで BFD エコー モードをイネーブルにするには、インターフェイス コンフィギュレーション モードで **bfd echo** コマンドを使用します。BFD エコー モードをディセーブルにするには、このコマンドの **no** 形式を使用します。

bfd echo

no bfd echo

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

BFD エコー モードは、BFD IPv4 セッションではデフォルトディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• —	• 対応	• 対応	• —

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

エコー モードはデフォルトでイネーブルになっていますが、BFD IPv6 セッションではサポートされていません。キーワードを指定せずに **no bfd echo** コマンドを入力すると、エコー パケットの送信がオフになり、ASA が BFD ネイバー ルータから受信したエコー パケットを転送しないことを示します。

エコー モードをイネーブルにすると、最小エコー送信間隔と必要最短送信間隔の値が **bfd interval milliseconds min_rx milliseconds** パラメータから取得されます。

CPU 使用率の上昇を避けるために、BFD エコー モードを使用する前に、**no ip redirects** コマンドを入力して、インターネット制御メッセージ プロトコル(ICMP)リダイレクト メッセージの送信をディセーブルにする必要があります。

例

次に、BFD マップに BFD テンプレートを関連付ける例を示します。

```
(config)# interface gigabitethernet 0/0
(config-if)# bfd echo
```

関連コマンド

コマンド	説明
authentication	シングルホップ セッションとマルチホップ セッションの BFD テンプレートに認証を設定します。
bfd interval	インターフェイスにベースライン BFD パラメータを設定します。
bfd map	アドレスとマルチホップ テンプレートを関連付ける BFD マップを設定します。
bfd slow-timers	BFD スロー タイマー値を設定します。
bfd template	シングルホップ BFD テンプレートをインターフェイスにバインドします。
bfd-template single-hop | multi-hop	BFD テンプレートを設定し、BFD コンフィギュレーション モードを開始します。
clear bfd counters	BFD カウンタをクリアします。
echo	BFD シングルホップ テンプレートにエコーを設定します。
neighbor	BGP が登録され、BFD から転送パス検出失敗メッセージを受信できるように、BGP の BFD サポートを設定します。
show bfd drops	BFD でドロップされたパケットの数を表示します。
show bfd map	設定済みの BFD マップを表示します。
show bfd neighbors	既存の BFD 隣接関係の詳細なリストを表示します。
show bfd summary	BFD のサマリー情報を表示します。

bfd interval

インターフェイスで基準 BFD パラメータを設定するには、インターフェイス コンフィギュレーション モードで **bfd** コマンドを使用します。ベースライン BFD セッション パラメータを削除するには、このコマンドの **no** 形式を使用します。

bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

no bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

構文の説明

interval	BFD 制御パケットが BFD ピアに送信される速度を指定します。有効値は 50 ～ 999 ミリ秒です。
min_rx	BFD 制御パケットが BFD ピアから受信されるときに期待される速度を指定します。有効値は 50 ～ 999 ミリ秒です。
multiplier	BFD ピアから紛失してよい BFD 制御パケットのレートを指定します。このレートに達すると、BFD はそのピアが利用不可になっていることを宣言し、レイヤ 3 BFD ピアに障害が伝えられます。指定できる範囲は 3 ～ 50 です。
milliseconds	この値はミリ秒単位です。
multiplier-value	乗数の値。

デフォルト

このコマンドにデフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• —	• 対応	• 対応	• —

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

例

次に、BFD マップに BFD テンプレートを関連付ける例を示します。

```
(config)# interface gigabitethernet 0/0
(config-if)# bfd interval 50 min_rx 50 multiplier 3
```

関連コマンド

コマンド	説明
authentication	シングルホップ セッションとマルチホップ セッションの BFD テンプレートに認証を設定します。
bfd echo	インターフェイスで BFD エコー モードを有効にします。
bfd map	アドレスとマルチホップ テンプレートを関連付ける BFD マップを設定します。
bfd slow-timers	BFD スロー タイマー値を設定します。
bfd template	シングルホップ BFD テンプレートをインターフェイスにバインドします。
bfd-template single-hop | multi-hop	BFD テンプレートを設定し、BFD コンフィギュレーション モードを開始します。
clear bfd counters	BFD カウンタをクリアします。
echo	BFD シングルホップ テンプレートにエコーを設定します。
neighbor	BGP が登録され、BFD から転送パス検出失敗メッセージを受信できるように、BGP の BFD サポートを設定します。
show bfd drops	BFD でドロップされたパケットの数を表示します。
show bfd map	設定済みの BFD マップを表示します。
show bfd neighbors	既存の BFD 隣接関係の詳細なリストを表示します。
show bfd summary	BFD のサマリー情報を表示します。

bfd map

アドレスをマルチホップ テンプレートに関連付ける BFD マップを設定するには、グローバル コンフィギュレーション モードで、**bfd map** コマンドを使用します。BFD マップを削除するには、このコマンドの **no** 形式を使用します。

bfd map {ipv4 | ipv6} *destination/cdir source/cdir template-name*

no bfd map

構文の説明

ipv4	IPv4 アドレスを設定します。
ipv6	IPv6 アドレスを設定します。
destination/cdir	宛先プレフィクス/長さです。
source/cdir	送信元プレフィクス/長さです。
template-name	BFD マップに関連付ける BFD テンプレートの名前です。

デフォルト

このコマンドにデフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• —	• 対応	• 対応	• —

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

例

次に、BFD マップに BFD テンプレートを関連付ける例を示します。

```
ciscoasa(config)# bfd map ipv4 10.11.11.0/24 10.36.42.5/32 multihop-template1
```

関連コマンド

コマンド	説明
authentication	シングルホップ セッションとマルチホップ セッションの BFD テンプレートに認証を設定します。
bfd echo	インターフェイスで BFD エコー モードを有効にします。
bfd interval	インターフェイスにベースライン BFD パラメータを設定します。

コマンド	説明
bfd slow-timers	BFD スロー タイマー値を設定します。
bfd template	シングルホップ BFD テンプレートをインターフェイスにバインドします。
bfd-template single-hop | multi-hop	BFD テンプレートを設定し、BFD コンフィギュレーション モードを開始します。
clear bfd counters	BFD カウンタをクリアします。
echo	BFD シングルホップ テンプレートにエコーを設定します。
neighbor	BGP が登録され、BFD から転送パス検出失敗メッセージを受信できるように、BGP の BFD サポートを設定します。
show bfd drops	BFD でドロップされたパケットの数を表示します。
show bfd map	設定済みの BFD マップを表示します。
show bfd neighbors	既存の BFD 隣接関係の詳細なリストを表示します。
show bfd summary	BFD のサマリー情報を表示します。

bfd slow-timers

BFD スロー タイマー値を設定するには、グローバル コンフィギュレーション モードで **bfd slow-timers** コマンドを使用します。

bgp slow-timers *[milliseconds]*

構文の説明

milliseconds	（任意）BFD スロー タイマー値（ミリ秒）です。指定できる範囲は 1000 ～ 30,000 です。デフォルトは 1000 です。

デフォルト

BFD スロー タイマーのデフォルト値は 1,000 ミリ秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• —	• 対応	• 対応	• —

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

例

次に、14,000 ミリ秒の BFD スロー タイマーを設定する例を示します。

```
ciscoasa(config)# bfd slow-timers 14000
```

関連コマンド

コマンド	説明
authentication	シングルホップ セッションとマルチホップ セッションの BFD テンプレートに認証を設定します。
bfd echo	インターフェイスで BFD エコー モードを有効にします。
bfd interval	インターフェイスにベースライン BFD パラメータを設定します。
bfd map	アドレスとマルチホップ テンプレートを関連付ける BFD マップを設定します。
bfd template	シングルホップ BFD テンプレートをインターフェイスにバインドします。
bfd-template single-hop | multi-hop	BFD テンプレートを設定し、BFD コンフィギュレーション モードを開始します。

コマンド	説明
clear bfd counters	BFD カウンタをクリアします。
echo	BFD シングルホップ テンプレートにエコーを設定します。
neighbor	BGP が登録され、BFD から転送パス検出失敗メッセージを受信できるように、BGP の BFD サポートを設定します。
show bfd drops	BFD でドロップされたパケットの数を表示します。
show bfd map	設定済みの BFD マップを表示します。
show bfd neighbors	既存の BFD 隣接関係の詳細なリストを表示します。
show bfd summary	BFD のサマリー情報を表示します。

bfd template

シングルホップ BFD テンプレートをインターフェイスにバインドするには、インターフェイス コンフィギュレーション モードで **bfd template** コマンドを使用します。シングルホップ BFD テンプレートをインターフェイスからアンバインドするには、このコマンドの **no** 形式を使用します。

bfd template *template-name*

no bfd template *template-name*

構文の説明

template-name	BFD テンプレートの名前。

デフォルト

このコマンドにデフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• —	• 対応	• 対応	• —

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

bfd-template コマンドを使用してテンプレートを作成していない場合でも、インターフェイスでテンプレート名を設定できますが、テンプレートを定義するまでテンプレートは無効と見なされます。テンプレート名を再設定する必要はありません。名前は自動的に有効になります。

例

次に、インターフェイスにシングル ホップ BFD テンプレートをバインドする例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# bfd template template-1
```

関連コマンド

コマンド	説明
authentication	シングルホップ セッションとマルチホップ セッションの BFD テンプレートに認証を設定します。
bfd echo	インターフェイスで BFD エコー モードを有効にします。
bfd interval	インターフェイスにベースライン BFD パラメータを設定します。
bfd map	アドレスとマルチホップ テンプレートを関連付ける BFD マップを設定します。
bfd slow-timers	BFD スロー タイマー値を設定します。
bfd-template single-hop | multi-hop	BFD テンプレートを設定し、BFD コンフィギュレーション モードを開始します。
clear bfd counters	BFD カウンタをクリアします。
echo	BFD シングルホップ テンプレートにエコーを設定します。
neighbor	BGP が登録され、BFD から転送パス検出失敗メッセージを受信できるように、BGP の BFD サポートを設定します。
show bfd drops	BFD でドロップされたパケットの数を表示します。
show bfd map	設定済みの BFD マップを表示します。
show bfd neighbors	既存の BFD 隣接関係の詳細なリストを表示します。
show bfd summary	BFD のサマリー情報を表示します。

bfd-template

BFD テンプレートを設定し、BFD コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **bfd-template** コマンドを使用します。BFD テンプレートをディセーブルにするには、このコマンドの **no** 形式を使用します。

bfd-template [single-hop | multi-hop] *template-name*

no bfd-template [single-hop | multi-hop] *template-name*

構文の説明

single-hop	シングルホップ BFD テンプレートを指定します。
multi-hop	マルチホップ BFD テンプレートを指定します。
template-name	BFD テンプレートの名前。

デフォルト

このコマンドにデフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• —	• 対応	• 対応	• —

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、BFD テンプレートを作成し、BFD コンフィギュレーション モードを開始するために使用します。また、テンプレートで一連の BFD 間隔値を指定できます。BFD テンプレートの一部として指定される BFD 間隔値は、1 つのインターフェイスに限定されるものではありません。

例

次に、シングルホップ BFD テンプレートを設定する例を示します。

```
ciscoasa(config)# bfd single-hop node1
ciscoasa(config-bfd)# interval min-tx 100 min-rx 100 mulitplier 3
```

次に、マルチホップ BFD テンプレートを設定する例を示します。

```
ciscoasa(config)# bfd multi-hop mh-template
ciscoasa(config-bfd)# interval min-tx 100 min-rx 100 mulitplier 3
```

関連コマンド

コマンド	説明
authentication	シングルホップ セッションとマルチホップ セッションの BFD テンプレートに認証を設定します。
bfd echo	インターフェイスで BFD エコー モードを有効にします。
bfd interval	インターフェイスにベースライン BFD パラメータを設定します。
bfd map	アドレスとマルチホップ テンプレートを関連付ける BFD マップを設定します。
bfd slow-timers	BFD スロー タイマー値を設定します。
bfd template	シングルホップ BFD テンプレートをインターフェイスにバインドします。
clear bfd counters	BFD カウンタをクリアします。
echo	BFD シングルホップ テンプレートにエコーを設定します。
neighbor	BGP が登録され、BFD から転送パス検出失敗メッセージを受信できるように、BGP の BFD サポートを設定します。
show bfd drops	BFD でドロップされたパケットの数を表示します。
show bfd map	設定済みの BFD マップを表示します。
show bfd neighbors	既存の BFD 隣接関係の詳細なリストを表示します。
show bfd summary	BFD のサマリー情報を表示します。

bgp aggregate-timer

BGP ルートが集約される間隔を設定する場合、またはタイマーに基づくルート集約をディセーブルにする場合は、アドレス ファミリ コンフィギュレーション モードで **bgp aggregate-timer** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

bgp aggregate-timer *seconds*

no bgp aggregate-timer

構文の説明

seconds	システムが BGP ルートを集約する間隔（秒単位）。 有効な値は 6 ～ 60 の範囲か、または 0（ゼロ）です。 デフォルト値は 30 です。 値を 0（ゼロ）に設定すると、タイマーに基づく集約をディセーブルにし、集約をただちに開始します。

デフォルト

bgp 集約タイマーのデフォルト値は 30 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
アドレス ファミリ コンフィギュレーション、アドレス ファミリ IPv6 サブモード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	このコマンドは、アドレス ファミリ IPv6 サブモードでサポートされるように変更されました。

使用上のガイドライン

このコマンドは、BGP ルートが集約されるデフォルト間隔を変更するために使用します。

非常に大規模なコンフィギュレーションでは、**aggregate-address summary-only** コマンドを設定した場合でも、より具体的なルートがアドバタイズされ、後で取り消されます。この動作を回避するには、**bgp aggregate-timer** を 0（ゼロ）に設定します。これにより、集約ルートがただちにチェックされ、特定のルートが抑制されます。

例

次に、20 秒間隔で BGP ルート集約を設定する例を示します。

```
ciscoasa(config)# router bgp 50
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp aggregate-timer 20
```

次に、BGP ルート集約をただちに開始する例を示します。

```
ciscoasa(config)# router bgp 50
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# aggregate-address 10.0.0.0 255.0.0.0 summary-only
ciscoasa(config-router-af)# bgp aggregate-timer 20
```

関連コマンド

コマンド	説明
address-family ipv4	アドレス ファミリ コンフィギュレーション モードを開始して、標準 IP バージョン 4（IPv4）アドレス プレフィックスを使用するルーティング セッションを設定します。
aggregate-address	Border Gateway Protocol（BGP）データベース内に集約エントリを作成します。

bgp always-compare-med

異なる自律システムにあるネイバーからのパスの Multi Exit Discriminator（MED）を比較できるようにするには、ルータ コンフィギュレーション モードで **bgp always-compare-med** コマンドを使用します。比較を禁止するには、このコマンドの **no** 形式を使用します。

bgp always-compare-med

no bgp always-compare-med

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドがイネーブルになっていない場合、またはこのコマンドの **no** 形式を入力した場合、ASA ルーティング ソフトウェアは異なる自律システムにあるネイバーからのパスの MED を比較しません。

MED が比較されるのは、比較されるルートの自律システム パスが同じである場合だけです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

MED は、RFC 1771 に記述されているように、オプションの非推移的属性で、4 オクテットの負でない整数です。この属性の値は、BGP の最適パス選択プロセスで、隣接自律システムへの複数の出力点を区別するために使用されることがあります。

MED は、多数のパスの選択肢の中から最適パスを選択するときに考慮されるパラメータの 1 つです。MED が低いパスの方が、MED が高いパスよりも優先されます。最適パス選択プロセス中、MED 比較は、同じ自律システムからのパスに対してだけ行われます。この動作を変更するには、**bgp always-compare-med** コマンドを使用して、受信したパスが属する自律システムに関係なくすべてのパスについて MED 比較を実行します。

bgp deterministic-med コマンドを設定すると、同じ自律システムから受信したすべてのパスについて確定的な MED 値比較を実行できます。

例

次の例では、受信したパスが属する自律システムに関係なくパスの選択肢から MED を比較するように、ローカル BGP ルーティング プロセスを設定しています。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# bgp always-compare-med
```

関連コマンド

コマンド	説明
bgp deterministic-med	同じ自律システムから受信したすべてのパスについて Multi Exit Discriminator（MED）値の確定的な比較を実行します。

bgp asnotation dot

デフォルトの表示を変更し、Border Gateway Protocol（BGP）の 4 バイト自律システム番号の正規表現マッチング形式を asplain 表記（10 進数値）からドット付き表記にするには、ルータ コンフィギュレーション モードで **bgp asnotation dot** コマンドを使用します。デフォルトの 4 バイト自律システム番号の表示と正規表現マッチング形式をリセットして asplain に戻すには、このコマンドの **no** 形式を使用します。

bgp asnotation dot

no bgp asnotation dot

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

BGP 自律システム番号は画面出力に asplain（10 進数値）形式で表示されます。正規表現で 4 バイト自律システム番号とマッチングするデフォルト形式は asplain です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

RFC 4271『*A Border Gateway Protocol 4 (BGP-4)*』に記述されているように、2009 年 1 月まで、企業に割り当てられていた BGP 自律システム番号は 1 ～ 65535 の範囲の 2 オクテットの数値でした。

自律システム番号の要求の増加に伴い、インターネット割り当て番号局（IANA）により割り当てられる自律システム番号は 2009 年 1 月から 65536 ～ 4294967295 の範囲の 4 オクテットの番号になります。RFC 5396『*Textual Representation of Autonomous System (AS) Numbers*』には、自律システム番号を表す 3 つの方式が記述されています。シスコでは、次の 2 つの方式を実装しています。

- asplain：10 進表記方式。2 バイトおよび 4 バイト自律システム番号をその 10 進数値で表します。たとえば、65526 は 2 バイト自律システム番号、234567 は 4 バイト自律システム番号になります。
- asdot：自律システム ドット付き表記。2 バイト自律システム番号は 10 進数で、4 バイト自律システム番号はドット付き表記で表されます。たとえば、65526 は 2 バイト自律システム番号、1.169031（10 進表記の 234567 をドット付き表記にしたもの）は 4 バイト自律システム番号になります。

シスコが採用している 4 バイト自律システム番号では、自律システム番号のデフォルト表示形式として asplain が使用されますが、4 バイト自律システム番号を asplain と asdot の両方の形式で設定できます。また、正規表現で 4 バイト自律システム番号とマッチングするためのデフォルト形式は asplain であるため、4 バイト自律システム番号とマッチングする正規表現はすべて、asplain 形式で記述する必要があります。デフォルトの **show** コマンド出力で、4 バイト自律システム番号が asdot 形式で表示されるように変更する場合は、ルータ コンフィギュレーション モードで **bgp asnotation dot** コマンドを使用します。デフォルトで asdot 形式がイネーブルにされている場合、正規表現の 4 バイト自律システム番号のマッチングには、すべて asdot 形式を使用する必要があり、使用しない場合正規表現によるマッチングは失敗します。次の表に示すように、4 バイト自律システム番号は asplain と asdot のどちらにも設定できますが、**show** コマンド出力と正規表現を使用した 4 バイト自律システム番号のマッチング制御には 1 つの形式だけが使用されます。デフォルトは asplain 形式です。

show コマンド出力の表示と正規表現のマッチング制御で asdot 形式の 4 バイト自律システム番号を使用する場合、**bgp asnotation dot** コマンドを設定する必要があります。**bgp asnotation dot** コマンドをイネーブルにした後で、**clearbgp *** コマンドを入力し、すべての BGP セッションについて、ハード リセットを開始する必要があります。

表4-1　asplain をデフォルトとする 4 バイト自律システム番号形式

書式	設定形式	show コマンド出力および正規表現のマッチング形式
asplain	2 バイト：1 ～ 6553 4 バイト：65536 ～ 4294967295	2 バイト：1 ～ 6553 4 バイト：65536 ～ 4294967295
asdot	2 バイト：1 ～ 6553 4 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 6553 4 バイト：65536 ～ 4294967295

表4-2　asdot を使用する 4 バイト自律システム番号形式

書式	設定形式	show コマンド出力および正規表現のマッチング形式
asplain	2 バイト：1 ～ 65535 4 バイト：65536 ～ 4294967295	2 バイト：1 ～ 65535 4 バイト：1.0 ～ 65535.65535
asdot	2 バイト：1 ～ 65535 4 バイト：1.0 ～ 65535.65535	2 バイト：1 ～ 65535 4 バイト：1.0 ～ 65535.65535

例

次の **show bgp summary** コマンドの出力は、4 バイト自律システム番号のデフォルト asplain 形式を示しています。ここで、asplain 形式で表された 4 バイト自律システム番号 65536 および 65550 に注意してください。

```
ciscoasa(config-router)# show bgp summary

BGP router identifier 172.17.1.99, local AS number 65538
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4        65536       7       7        1    0    0 00:03:04       0
192.168.3.2     4        65550       4       4        1    0    0 00:00:15       0
```

次のコンフィギュレーションは、デフォルトの出力形式を asdot 表記形式に変更するために実行されます。

```
ciscoasa# configure terminal
ciscoasa(config)# router bgp 65538
ciscoasa(config-router)# bgp asnotation dot
```

コンフィギュレーションの実行後、次の **show bgp summary** コマンド出力に示すように、出力が asdot 表記形式に変換されます。asdot 形式で表された 4 バイト自律システム番号 1.0 および 1.14 に注意してください（これらは自律システム番号 65536 と 65550 を asdot 変換したものです）。

```
ciscoasa(config-router)# show bgp summary

BGP router identifier 172.17.1.99, local AS number 1.2
BGP table version is 1, main routing table version 1

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4          1.0       9       9        1    0    0 00:04:13       0
192.168.3.2     4         1.14       6       6        1    0    0 00:01:24       0
```

bgp asnotation dot コマンドを設定すると、4 バイト自律システム パスの正規表現マッチング形式が asdot 表記形式に変更されます。4 バイト自律システム番号は、asplain 形式または asdot 形式のいずれかを使用して、正規表現で設定できますが、現在のデフォルト形式を使用して設定された 4 バイト自律システム番号だけがマッチングされます。1 つ目の例では、**show bgp regexp** コマンドは、asplain 形式で表された 4 バイト自律システム番号を使用して設定されています。現在のデフォルト形式は asdot 形式なのでマッチングは失敗し、何も出力されません。asdot 形式を使用した 2 番目の例では、マッチングは成功し、4 バイトの自律システム パスに関する情報が asdot 表記法を使って表示されます。

```
ciscoasa(config-router)# show bgp regexp ^65536$
ciscoasa(config-router)# show bgp regexp ^1\.0$

BGP table version is 2, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 1.0 i
```

（注） この asdot 表記法で使用されているピリオドは、シスコの正規表現では特殊文字です。特殊な意味を取り除くには、ピリオドの前にバックスラッシュをつけます。

関連コマンド

コマンド	説明
show bgp summary	すべての Border Gateway Protocol（BGP）接続のステータスを表示します。
show bgp regexp	自律システム パスの正規表現と一致するルートを表示します。

bgp bestpath compare-routerid

最適パス選択プロセス中に異なる外部ピアから受信された同一ルートを比較し、最適パスとして最も小さいルータ ID を持つルートを選択するように、Border Gateway Protocol（BGP）ルーティング プロセスを設定するには、ルータ コンフィギュレーション モードで **bgp bestpath compare-routerid** コマンドを使用します。

BGP ルーティング プロセスをデフォルトの動作に戻すには、このコマンドの **no** 形式を使用します。

bgp bestpath compare-routerid

no bgp bestpath compare-routerid

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドの動作はデフォルトでディセーブルであり、同一の属性を持つ 2 つのルートが受信されたとき、BGP は最初に受信されたルートを選択します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

bgp bestpath compare-routerid コマンドは、2 つの異なるピア（ルータ ID を除くすべての属性が同じ）から 2 つの同一のルートが受信されたときに最適パス選択のタイ ブレーカーとしてルータ ID を使用するように BGP ルーティング プロセスを設定するために使用します。このコマンドがイネーブルになっている場合、その他の属性がすべてが等しければ、最も小さいルータ ID が最適パスとして選択されます。

例

次の例では、異なるピアから同一のパスが受信されたときに、パスを比較し、最適パス選択のタイ ブレーカーとしてルータ ID を使用するように、BGP ルーティング プロセスを設定しています。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# bgp bestpath compare-routerid
```

bgp bestpath med missing-as-worst

Multi Exit Discriminator（MED）属性がないルートに無限の値を割り当てる（MED 値のないパスを最も不適切なパスとする）ように Border Gateway Protocol（BGP）ルーティング プロセスを設定するには、ルータ コンフィギュレーション モードで **bgp bestpath med missing-as-worst** コマンドを使用します。ルータをデフォルトの動作に戻す（MED のないルートに 0 の値を割り当てる）には、このコマンドの **no** 形式を使用します。

bgp bestpath med missing-as-worst

no bgp bestpath med missing-as-worst

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

ASA ソフトウェアは、MED 属性のないルートに 0 の値を割り当てるため、MED 属性がないルートを最適パスと見なします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

例

次の例では、MED 属性がないルートを無限の値（4294967294）を持つルートと見なし、このパスを最も不適切なパスとするように BGP ルータ プロセスを設定しています。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# bgp bestpath med missing-as-worst
```

bgp-community new-format

コミュニティを AA:NN 形式（自律システム番号:コミュニティ番号/4 バイトの数値）で表示するように BGP を設定するには、グローバル コンフィギュレーション モードで **bgp-community new-format** コマンドを使用します。コミュニティを 32 ビットの数値として表示するように BGP を設定するには、このコマンドの **no** 形式を使用します。

bgp-community new-format

no bgp-community new-format

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドがイネーブルになっていない場合、または **no** 形式を入力した場合、BGP コミュニティは（AA:NN 形式で入力したときも）32 ビットの数値として表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

bgp-community new-format コマンドは、BGP コミュニティを RFC-1997 準拠の AA:NN 形式で表示するようにローカル ルータを設定するために使用します。

このコマンドは、BGP コミュニティが表示される形式のみに影響を与え、コミュニティやコミュニティの交換には影響を与えません。ただし、32 ビットの数値でなく AA:NN 形式でマッチングを行うように、ローカルに設定された正規表現と一致する拡張 IP コミュニティ リストを更新する必要がある場合があります。

RFC 1997『*BGP Communities Attribute*』には、BGP コミュニティがそれぞれ 2 バイト長の 2 つの部分で構成されると規定されています。1 つ目の部分は自律システム番号で、2 つ目の部分はネットワーク オペレータによって定義された 2 バイトの数値です。

例

次の例では、32 ビットの数値のコミュニティ形式を使用するルータを、AA:NN 形式を使用するようにアップグレードしています。

```
ciscoasa(config)# bgp-community new-format
ciscoasa(config-router)# no bgp transport path-mtu-discovery
```

次の出力例は、**bgp-community new-format** コマンドがイネーブルになっている場合に BGP コミュニティ番号がどのように表示されるかを示しています。

```
ciscoasa(router)# show bgp 10.0.0.0

BGP routing table entry for 10.0.0.0/8, version 4
Paths: (2 available, best #2, table Default-IP-Routing-Table)
Advertised to non peer-group peers:
10.0.33.35
35
10.0.33.35 from 10.0.33.35 (192.168.3.3)
Origin incomplete, metric 10, localpref 100, valid, external
Community: 1:1
Local
0.0.0.0 from 0.0.0.0 (10.0.33.34)
Origin incomplete, metric 0, localpref 100, weight 32768, valid, sourced, best
```

bgp default local-preference

デフォルトのローカル プリファレンス値を変更するには、ルータ コンフィギュレーション モードで **bgp default local-preference** コマンドを使用します。ローカル プリファレンス値をデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

bgp default local-preference *number*

no bgp default local-preference *number*

構文の説明

number	0 ～ 4294967295 の範囲のローカル プリファレンス値。

デフォルト

このコマンドがイネーブルになっていない場合、またはこのコマンドの **no** 形式を入力した場合、ASA ソフトウェアはローカル プリファレンス値 100 を適用します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

ローカル プリファレンス属性は、BGP の最適パス選択プロセス中にプリファレンス レベルをルートに適用するために使用される任意の属性です。この属性は iBGP ピア間だけで交換され、ローカル ポリシーを決定するために使用されます。ローカル プリファレンス値が最大のルートが優先されます。

例

次の例では、ローカル優先順位値は 200 に設定されます。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# bgp default local-preference 200
```

bgp deterministic-med

同じ自律システムから受信されたすべてのパスについて Multi Exit Discriminator（MED）値の確定的な比較を実行するには、ルータ コンフィギュレーション モードで **bgp deterministic-med** コマンドを使用します。必要な MED 比較をディセーブルにするには、このコマンドの **no** 形式を使用します。

bgp deterministic-med

no bgp deterministic-med

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

ASA ソフトウェアは、同じ自律システムから受信されたすべてのパスについて MED 変数の確定的な比較を実行しません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

bgp always-compare-med コマンドは、異なる自律システムにあるネイバーからのパスの Multi Exit Discriminator（MED）の比較をイネーブルにするために使用します。**bgp always-compare-med** コマンドの設定後、同じ自律システムにある異なるネイバーから受信された同じプレフィックスのパスはすべてグループ化され、昇順の MED 値でソートされます（受信専用のパスは無視され、グループ化もソートもされません）。

次に、最適パス選択アルゴリズムにより、既存のルールを使用して最適パスが選択されます。比較は、ネイバーの自律システムごとに行われ、続いてグローバルに行われます。パスのグループ化およびソートは、このコマンドを入力するとただちに行われます。正しい結果を得るには、ローカル自律システム内のすべてのルータでこのコマンドがイネーブル（またはディセーブル）になっている必要があります。

例

次の例では、1 つの連合内の同じサブ自律システムによってアドバタイズされたルートのパス選択中に MED を比較するように BGP を設定しています。

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# bgp deterministic-med
```

次の **show bgp** コマンド出力例は、**bgp deterministic-med** コマンドのコンフィギュレーションによってルート選択がどのように影響を受けるかを示しています。**bgp deterministic-med** コマンドがイネーブルになっていない場合、ルートの受信順序によって最適パス選択でどのようにルートが選択されるかが決まります。次の **show bgp** コマンドの出力例は、同じプレフィックス（10.100.0.0）に対して受信された 3 つのパスを示しています。**bgp deterministic-med** コマンドはイネーブルになっていません。

```
ciscoasa(router)# show bgp 10.100.0.0

BGP routing table entry for 10.100.0.0/16, version 40
Paths: (3 available, best #3, advertised over IBGP, EBGP)
109
   192.168.43.10 from 192.168.43.10 (192.168.43.1)
     Origin IGP, metric 0, localpref 100, valid, internal
 2051
   192.168.43.22 from 192.168.43.22 (192.168.43.2)
     Origin IGP, metric 20, localpref 100, valid, internal
 2051
   192.168.43.3 from 192.168.43.3 (10.4.1.1)
     Origin IGP, metric 30, valid, external, best
```

ルータで bgp deterministic-med 機能がイネーブルになっていない場合、ルートの受信順序によってルート選択が影響を受けることがあります。次のシナリオで、1 つのルータが同じプレフィックスに対して 3 つのパスを受信した場合を考えてみます。

ローカル ルーティング テーブルのすべてのルートをクリアするために、**clear bgp *** コマンドを入力します。

```
ciscoasa(router)# clear bgp *
```

ルーティング テーブルへの再書き込みが行われた後、**show bgp** コマンドを再度発行します。BGP セッションをクリアした後、パスの順序が変わることに注意してください。2 番目のセッションではパスの受信順序が異なっていたため、選択アルゴリズムの結果も変わっています。

```
ciscoasa(router)# show bgp 10.100.0.0

BGP routing table entry for 10.100.0.0/16, version 2
Paths: (3 available, best #3, advertised over EBGP)
 109 192.168.43.10 from 192.168.43.10 (192.168.43.1)
     Origin IGP, metric 0, localpref 100, valid, internal
 2051
   192.168.43.3 from 192.168.43.3 (10.4.1.1)
     Origin IGP, metric 30, valid, external
 2051
   192.168.43.22 from 192.168.43.22 (192.168.43.2)
     Origin IGP, metric 20, localpref 100, valid, internal, best
```

bgp deterministic-med コマンドがイネーブルになっている場合、ローカル ルータがパスを受信した順序に関係なく、選択アルゴリズムの結果は常に同じになります。このシナリオでは、ローカル ルータで **bgp deterministic-med** コマンドを入力した場合、常に次の出力が生成されます。

```
ciscoasa(router)# show bgp 10.100.0.0

BGP routing table entry for 10.100.0.0/16, version 15
```

```
Paths: (3 available, best #1, advertised over EBGP)
 109
   192.168.43.10 from 192.168.43.10 (192.168.43.1)
     Origin IGP, metric 0, localpref 100, valid, internal, best 3
   192.168.43.22 from 192.168.43.22 (192.168.43.2)
      Origin IGP, metric 20, localpref 100, valid, internal 3
   192.168.43.3 from 192.168.43.3 (10.4.1.1)
     Origin IGP, metric 30, valid, external
```

関連コマンド

コマンド	説明
bgp always compare-med	異なる自律システムにあるネイバーからのパスの Multi Exit Discriminator（MED）の比較をイネーブルにします。
clear bgp	ハードまたはソフト再構成を使用して BGP 接続をリセットします。
show bgp	Border Gateway Protocol（BGP）ルーティング テーブル内のエントリを表示します。

bgp enforce-first-as

着信アップデート内の AS_PATH の先頭に自律システム番号が示されていない外部 BGP（eBGP）ピアから受信したアップデートを拒否するように ASA を設定するには、ルータ コンフィギュレーション モードで **bgp enforce-first-as** コマンドを使用します。この動作をディセーブルにするには、このコマンドの **no** 形式を使用します。

bgp enforce-first-as

no bgp enforce-first-as

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドの動作は、デフォルトでイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

bgp enforce-first-as コマンドは、AS_PATH 属性内の最初のセグメントとして自律システム番号が示されていない eBGP ピアから受信した着信アップデートを拒否するために使用します。このコマンドをイネーブルにすると、間違った設定のピアや権限のないピアが、別の自律システムからのルートであるかのようにルートをアドバタイズすることによってトラフィックを誤った宛先に送信する（ローカル ルータをスプーフィングする）ことを回避できます。

例

次に、BGP ピアからのすべての着信アップデートを調べて、AS_PATH 内の最初の自律システム番号が送信側ピアのローカル AS 番号であることを確認する例を示します。次の例では、最初の AS 番号が 65001 でなければ、ピア 10.100.0.1 からのアップデートは廃棄されます。

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# bgp enforce-first-as
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.100.0.1 remote-as 65001
```

関連コマンド

コマンド	説明
address-family ipv4	アドレス ファミリ コンフィギュレーション モードを開始します。
neighbor remote-as	BGP またはマルチプロトコル BGP ルーティング テーブルにエントリを追加します。

bgp fast-external-fallover

これらのピアにアクセスするためのリンクがダウンした場合に外部 BGP ピアリング セッションをただちにリセットするように Border Gateway Protocol（BGP）ルーティング プロセスを設定するには、ルータ コンフィギュレーション モードで **bgp fast-external-fallover** コマンドを使用します。BGP 高速外部フォールオーバーをディセーブルにするには、このコマンドの **no** 形式を使用します。

bgp fast-external-fallover

no bgp fast-external-fallover

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

BGP 高速外部フォールオーバーはデフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

bgp fast-external-fallover コマンドは、直接接続されている外部ピアとの BGP ピアリング セッションにおける高速外部フォールオーバーをディセーブルまたはイネーブルにするために使用します。リンクがダウンするとセッションは即座にリセットされます。直接接続されているピアのみサポートされます。BGP 高速外部フォールオーバーがディセーブルの場合、BGP ルーティング プロセスはデフォルトのホールド タイマーの期限（3 回のキープアライブ）が切れるまで待ってピアリング セッションをリセットします。また、**ip bgp fast-external-fallover** インターフェイス コンフィギュレーション コマンドを使用して、BGP 高速外部フォールオーバーをインターフェイス単位で設定することもできます。

例

次に、BGP 高速外部フォールオーバー機能をディセーブルにする例を示します。このセッションを伝送するリンクがフラップしても、接続はリセットされません。

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# no bgp fast-external-fallover
```

関連コマンド

コマンド	説明
ip bgp fast-external-fallover	インターフェイス単位で高速外部フォールオーバーを設定します。

bgp graceful-restart

ノンストップ転送設定でグレースフル リスタートの Border Gateway Protocol（BGP）ルーティング プロセスを設定するには、ルータ コンフィギュレーション モードで **bgp graceful-restart** コマンドを使用します。BGP グレースフル リスタートをディセーブルにするには、このコマンドの **no** 形式を使用します。

bgp graceful-restart [**restart-time** *seconds* | **stalepath-time** *seconds*]

no bgp graceful-restart [**restart-time** *seconds* | **stalepath-time** *seconds*]

構文の説明

restart-time *seconds*	リスタート イベントが発生した後、グレースフル リスタート対応ネイバーが通常の動作に戻るまでシステムが待機する最大時間（秒）。デフォルトは 120 秒です。値は 1 ～ 3600 秒です。
stalepath-time *seconds*	リスタートしているピアの古いパスをシステムが保持する最大時間（秒）。すべての古いパスは、このタイマーが期限切れになった後に削除されます。デフォルト値は 360 秒です。値は 1 ～ 3600 秒です。

デフォルト

BGP グレースフル リスタートはデフォルトでディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが追加されました。

使用上のガイドライン

ノンストップ転送のグレースフル リスタートを有効にするには、このコマンドを使用します。グレースフル リスタートを使用すると、システムは、再起動中にアドレス グループのフォワーディング ステートを維持する機能をアドバタイズできます。各 BGP ネイバー ルータの再起動機能を設定するには、**neighbor ha-mode graceful-restart** コマンドを使用します。

例

次に、デフォルトのタイマーを使用してグレースフル リスタートをグローバルにイネーブルにする例を示します。

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# bgp graceful-restart
```

関連コマンド

コマンド	説明
neighbor ha-mode graceful-restart	BGP ネイバーの Border Gateway Protocol（BGP）グレースフル リスタート機能を設定します。

bgp inject-map

より具体的なルートを Border Gateway Protocol（BGP）ルーティング テーブルに挿入するように条件付きルート注入を設定するには、アドレス ファミリ コンフィギュレーション モードで **bgp inject-map** コマンドを使用します。条件付きルート注入の設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

bgp inject-map *inject-map* **exist-map** *exist-map* [**copy-attributes**]

no bgp inject-map *inject-map* **exist-map** *exist-map*

構文の説明

inject-map	ローカル BGP ルーティング テーブルに注入するプレフィックスを指定するルート マップの名前。
exist-map *exist-map*	BGP スピーカーが追跡するプレフィックスを含むルート マップの名前を指定します。
copy-attributes	（オプション）注入されたルートが集約ルートの属性を継承するように設定します。

デフォルト

特定のルートが BGP ルーティング テーブルに注入されることはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
アドレス ファミリ コンフィギュレーション、アドレス ファミリ IPv6 サブモード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	このコマンドは、アドレス ファミリ IPv6 サブモードでサポートされるように変更されました。

使用上のガイドライン

bgp inject-map コマンドは、条件付きルート注入を設定するために使用します。条件付きルート注入により、一致するものがなくても、より具体的なプレフィックスを BGP ルーティング テーブルにすることができます。2 つのルート マップ（*exist-map* および *inject-map*）をグローバル コンフィギュレーション モードで設定してから、アドレス ファミリ コンフィギュレーション モードの **bgp inject-map** コマンドで指定します。

exist-map 引数は、BGP スピーカーが追跡するプレフィックスを定義するルート マップを指定します。このルート マップには、集約プレフィックスを指定するための **match ip address prefix-list** コマンド ステートメントと、ルート ソースを指定するための **match ip route-source prefix-list** コマンド ステートメントが含まれる必要があります。

inject-map は、ルーティング テーブルで作成され、このテーブルに格納されるプレフィックスを定義します。注入されたプレフィックスは、ローカル BGP RIB に格納されます。有効な親ルートが存在する必要があります。集約ルート（既存プレフィックス）と同じかそれより具体的なプレフィックスのみを注入できます。

オプションのキーワード **copy-attributes** は、注入されたプレフィックスが集約ルートと同じ属性を継承するように任意で設定するために使用します。このキーワードを入力しない場合、注入されたプレフィックスは、ローカルで生成されたルートのデフォルト属性を使用します。

例

次の例では、条件付きルート注入を設定しています。注入されたプレフィックスは、集約（親）ルートの属性を継承します。

```
ciscoasa(config)# ip prefix-list ROUTE permit 10.1.1.0/24
ciscoasa(config)# ip prefix-list ROUTE_SOURCE permit 10.2.1.1/32
ciscoasa(config)# ip prefix-list ORIGINATED_ROUTES permit 10.1.1.0/25
ciscoasa(config)# ip prefix-list ORIGINATED_ROUTES permit 10.1.1.128/25
ciscoasa(config)# route-map LEARNED_PATH permit 10
ciscoasa(config-route-map)# match ip address prefix-list ROUTE
ciscoasa(config-route-map)# match ip route-source prefix-list ROUTE_SOURCE
ciscoasa(config-route-map)# exit
ciscoasa(config)# route-map ORIGINATE permit 10
ciscoasa(config-route-map)# set ip address prefix-list ORIGINATED_ROUTES
ciscoasa(config-route-map)# set community 14616:555 additive
ciscoasa(config-route-map)# exit
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp inject-map ORIGINATE exist-map LEARNED_PATH
copy-attributes
```

関連コマンド

コマンド	説明
ip prefix-list	プレフィックス リストを作成するか、プレフィックス リスト エントリを追加します。
set community	BGP コミュニティ属性を設定します。
address-family ipv4	アドレス ファミリ コンフィギュレーション モードを開始します。

bgp log-neighbor-changes

BGP ネイバー リセットのロギングをイネーブルにするには、ルータ コンフィギュレーション モードで **bgp log-neighbor-changes** コマンドを使用します。BGP ネイバーとの隣接関係の変化に関するロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

bgp log-neighbor-changes

no bgp log-neighbor-changes

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

BGP ネイバーのロギングはイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

bgp log-neighbor-changes コマンドは、BGP ネイバー ステータスの変化（アップまたはダウン）およびリセットに関するロギングをイネーブルにします。ログはネットワークの接続問題のトラブルシューティングおよびネットワークの安定性の評価に使用します。ネイバーが突然リセットする場合は、ネットワークのエラー率の高いことやパケット損失の多いことが考えられるので、調査するようにしてください。

ステータスの変化に関するメッセージをロギングするために **bgp log-neighbor-changes** コマンドを使用しても、BGP アップデート デバッグを有効にする場合などと異なり、パフォーマンスに大きな影響を与えることはありません。

bgp log-neighbor-changes コマンドがイネーブルでない場合、ネイバー ステータスの変化に関するメッセージは、**show bgp neighbors** コマンドの出力として常に使用可能なリセットの理由を除いて、追跡されません。

eigrp log-neighbor-changes コマンドは、Enhanced Interior Gateway Routing Protocol（EIGRP）ネイバーとの隣接関係のロギングをイネーブルにしますが、BGP ネイバーに関するメッセージは **bgp log-neighbor-changes** コマンドで明確にイネーブルにされた場合にのみ記録されます。

BGP ネイバーの変化に関するログを表示するには、**show logging** コマンドを使用します。

例

次に、ルータ コンフィギュレーション モードで BGP のネイバーの変化をログする例を示します。

```
ciscoasa(config)# bgp router 40000
ciscoasa(config-router)# bgp log-neighbor-changes
```

関連コマンド

コマンド	説明
show BGP neighbors	ネイバーへの BGP 接続に関する情報を表示します。

bgp maxas-limit

AS パス内の自律システム番号が指定した値を超えるルートを廃棄するように Border Gateway Protocol（BGP）を設定するには、ルータ コンフィギュレーション モードで **bgp maxas-limit** コマンドを使用します。ルータをデフォルト動作に戻すには、このコマンドの **no** 形式を使用します。

bgp max-as limit *number*

no bgp max-as limit

構文の説明

number	BGP アップデート メッセージ内の AS パス属性にある自律システム番号の最大数（1 ～ 254）。このコマンドは、AS パス セグメント内の自律システム番号の数に制限を設定するだけでなく、AS パス セグメントの数を 10 に制限します。10 個の AS パス セグメントを許可する動作が、**bgp maxas-limit** コマンドに組み込まれています。

デフォルト

ルートは廃棄されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

bgp maxas-limit コマンドは、着信ルートで許可される AS パス属性内の自律システム番号の数を制限するために使用します。設定した制限を超える AS パス セグメントを持つルートが受信されると、BGP ルーティング プロセスでこのルートが廃棄されます。

例

次に、AS パス属性内の自律システム番号の最大数を 30 に設定する例を示します。

```
ciscoasa(config)# router bgp 4000
ciscoasa(config)# bgp maxas-limit 30
```

bgp nexthop

Border Gateway Protocol（BGP）のネクストホップ アドレス トラッキングを設定するには、アドレス ファミリ コンフィギュレーション モードまたはルータ コンフィギュレーション モードで **bgp nexthop** コマンドを使用します。BGP ネクストホップ アドレス トラッキングをディセーブルにするには、このコマンドの **no** 形式を使用します。

bgp nexthop {**trigger** {**delay** *seconds* | **enable**} | **route-map** *map-name*}

no bgp nexthop {**trigger** {**delay** *seconds* | **enable**} | **route-map** *map-name*}

構文の説明

トリガー	BGP ネクストホップ アドレス トラッキングの使用を指定します。ネクストホップ トラッキング遅延を変更するには、このキーワードを **delay** キーワードとともに使用します。ネクストホップ アドレス トラッキングをイネーブルにするには、このキーワードを **enable** キーワードとともに使用します。
delay	ルーティング テーブルに格納された更新済みのネクストホップ ルートに対するチェックの遅延間隔を変更します。
seconds	遅延に指定する秒数。有効な値は 0 ～ 100 です。デフォルトは 5 です。
enable	BGP ネクストホップ アドレス トラッキングをイネーブルにします。
route-map	BGP プレフィックスのネクストホップ ルートとして割り当てられたルーティング テーブル内のルートに適用されるルート マップの使用を指定します。
map-name	ルート マップの名前。

デフォルト

IPv4 では、BGP ネクストホップ アドレス トラッキングはデフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
アドレスファミリ コンフィギュレーション アドレス ファミリ IPv6 サブモード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	このコマンドは、アドレス ファミリ IPv6 サブモードでサポートされるように変更されました。

使用上のガイドライン

BGP ネクストホップ アドレス トラッキングはイベント ドリブンです。BGP プレフィックスは、ピアリング セッションの確立時に自動的にトラッキングされます。ネクストホップの変更は、ルーティング情報ベース（RIB）で更新されると BGP に迅速に報告されます。この最適化によって、RIB にインストールされているルートのネクストホップの変更に対する応答時間が短縮されることで、全体的な BGP コンバージェンスが改善されます。BGP スキャナ サイクル間に最適パス計算が実行されると、変更内容だけが処理および追跡されます。

（注）

- BGP ネクストホップ アドレス トラッキングによって、BGP 応答時間を大幅に短縮できます。ただし、不安定な内部ゲートウェイ プロトコル（IGP）ピアにより、BGP が不安定になることがあります。BGP への影響の可能性を軽減するために、不安定な IGP ピアリング セッションを積極的にダンプニングさせることを推奨します。
- IPv6 アドレス ファミリでは、BGP ネクストホップ アドレス トラッキングはサポートされていません。

BGP ネクストホップ アドレス トラッキングのルーティング テーブル ウォーク間の遅延間隔を変更するには、**trigger** キーワードを **delay** キーワードおよび *seconds* 引数とともに使用します。すべてのルーティング テーブル ウォーク間の遅延間隔を調整して IGP の調整パラメータと一致させることで、BGP ネクストホップ アドレス トラッキングのパフォーマンスを向上させることができます。デフォルトの遅延間隔は 5 秒であり、高速で調整される IGP の場合はこれが最適な値です。よりゆっくり収束する IGP の場合は、IGP コンバージェンス時間に応じて遅延間隔を 20 秒以上に変更できます。

BGP ネクストホップ アドレス トラッキングをイネーブルにするには、**trigger** キーワードを **enable** キーワードとともに使用します。BGP ネクストホップ アドレス トラッキングは、デフォルトでイネーブルになっています。

ルート マップを使用できるようにするには、**route-map** キーワードおよび *map-name* 引数を使用します。このルート マップは BGP 最適パス計算中に使用され、BGP プレフィックスの Next_Hop 属性に対応するルーティング テーブル内のルートに適用されます。ネクストホップ ルートがルート マップの評価に失敗した場合、ネクストホップ ルートは到達不能とマークされます。このコマンドはアドレス ファミリ単位で実行されるため、異なるアドレス ファミリ内のネクストホップ ルートでは別のルート マップを適用できます。

（注）ルート マップでサポートされるコマンドは、**match ip address** コマンドだけです。**set** コマンドやその他の **match** コマンドはサポートされません。

例

次に、IPv4 アドレス ファミリ セッションによって 20 秒ごとに発生する BGP ネクストホップ アドレス トラッキングのルーティング テーブル ウォーク間の遅延間隔を変更する例を示します。

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# bgp nexthop trigger delay 20
```

次に、IPv4 アドレス ファミリのネクストホップ アドレス トラッキングをディセーブルにする例を示します。

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# no bgp nexthop trigger enable
```

次に、アドレス マスクの長さが 25 を超える場合にのみルートをネクストホップ ルートと見なすことを許可するルート マップを設定する例を示します。このコンフィギュレーションによって、プレフィックスの集約がネクストホップ ルートと見なされることを回避できます。

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# bgp nexthop route-map CHECK-NEXTHOP
ciscoasa(config-router-af)# exit-address-family
ciscoasa(config-router)# exit
ciscoasa(config)# ip prefix-list FILTER25 seq 5 permit 0.0.0.0/0 ge 25
ciscoasa(config)# route-map CHECK-NEXTHOP permit 10
ciscoasa(config)# match ip address prefix-list FILTER25
```

bgp redistribute-internal

EIGRP や OSPF などの内部ゲートウェイ プロトコル（IGP）への iBGP 再配布を設定するには、アドレス ファミリ コンフィギュレーション モードで **bgp redistribute-internal** コマンドを使用します。ルータをデフォルトの動作に戻し、IGP への iBGP 再配布を停止するには、このコマンドの **no** 形式を使用します。

bgp redistribute-internal

no bgp redistribute-internal

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

IBGP ルートが IGP に再配布されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
アドレスファミリ コンフィギュレーション アドレス ファミリ IPv6 サブモード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	このコマンドは、アドレス ファミリ IPv6 サブモードでサポートされるように変更されました。

使用上のガイドライン

bgp redistribute-internal コマンドは、IGP への iBGP の再配布を設定するために使用します。このコマンドの設定後に、BGP 接続をリセットするために **clear bgp** コマンドを入力する必要があります。

BGP を IGP に再配布する際は、必ず、再配布されるプレフィックスの数を制限するために IP prefix-list ステートメントおよび route-map ステートメントを使用してください。

注意 iBGP を IGP に再配布する際は、慎重に行ってください。再配布されるプレフィックスの数を制限するために IP prefix-list ステートメントおよび route-map ステートメントを使用します。フィルタリングされていない BGP ルーティング テーブルを IGP に再配布すると、通常の IGP ネットワーク動作に影響を及ぼす可能性があります。

例

次の例では、BGP から OSPF へのルート再配布をイネーブルにしています。

```
ciscoasa(config)# router ospf 300
ciscoasa(config-router)# redistribute bgp 200
ciscoasa(config-router)# exit
ciscoasa(config)# router bgp 200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp redistribute-internal
```

bgp router-id

Border Gateway Protocol（BGP）のローカル ルーティング プロセスの固定ルータ ID を設定するには、アドレス ファミリ ルータ コンフィギュレーション モードで **bgp router-id** コマンドを使用します。固定ルータ ID を実行コンフィギュレーション ファイルから削除し、デフォルト ルータ ID の選択に戻すには、このコマンドの **no** 形式を使用します。

bgp router-id *ip-address*

no bgp router-id

構文の説明

ip-address	IP アドレス形式のルータ ID。

デフォルト

このコマンドがイネーブルになっていない場合、ルータ ID は物理インターフェイスの最上位の IP アドレスに設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
アドレス ファミリ コンフィギュレーション ルータ コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	このコマンドが変更されました。

使用上のガイドライン

ローカル BGP ルーティング プロセスの固定ルータ ID を設定するには、**bgp router-id** コマンドを使用します。ルータ ID は IP アドレス形式で入力します。任意の有効な IP アドレスを使用できます。ルータでローカルに設定されていないアドレスでもかまいません。ルータ ID が変更されると、ピアリング セッションが自動的にリセットされます。コンテキストごとに個別のルータ ID を設定できます。

例

次に、固定 BGP ルータ ID が 192.168.254.254 であるローカル ルータを設定する例を示します。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 19.168.254.254
```

bgp scan-time

ネクスト ホップ検証用に Border Gateway Protocol（BGP）のスキャン間隔を設定するには、アドレス ファミリ コンフィギュレーション モードで **bgp scan-time** コマンドを使用します。ルータのスキャン間隔をデフォルトのスキャン間隔（60 秒）に戻すには、このコマンドの **no** 形式を使用します。

bgp scan-time *scanner-interval*

no bgp scan-time *scanner-interval*

構文の説明

scanner-interval	BGP ルーティング情報のスキャン間隔。 有効な値は 15 ～ 60 秒です。デフォルトは 60 秒です。

デフォルト

デフォルトのスキャン間隔は 60 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
アドレス ファミリ コンフィギュレーション	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドの **no** 形式を入力しても、スキャンはディセーブルになりませんが、**show running-config** コマンドの出力からは削除されます。

アドレス ファミリに対して **BGP ネクストホップ** アドレス トラッキング（NHT）がイネーブルになっている場合、そのアドレス ファミリで **bgp scan-time** コマンドは受け入れられず、デフォルト値の 60 秒は変更されません。ルータ モードまたはアドレス ファミリ モードで **bgp scan-time** コマンドを使用する場合は、あらかじめ NHT をディセーブルにしておく必要があります。

例

次のルータ コンフィギュレーションの例では、BGP ルーティング テーブルの IPv4 ユニキャスト ルートのネクスト ホップ検証のスキャン間隔を 20 秒に設定しています。

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4
```

```
ciscoasa(config-router-af)# no synchronization
ciscoasa(config-router-af)# bgp scan-time 20
```

関連コマンド

コマンド	説明
show running-config	ASA で現在表示されているコンフィギュレーションを表示します。
bgp nexthop	BGP ネクストホップ アドレス トラッキングを設定します。

bgp suppress-inactive

ルーティング情報ベース（RIB）に導入されていないルートのアドバタイズメントを抑制するには、アドレス ファミリ モードまたはルータ コンフィギュレーション モードで **bgp suppress-inactive** コマンドを使用します。

bgp suppress-inactive

no bgp suppress-inactive

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

ルートは抑制されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
アドレス ファミリ コンフィギュレーション アドレス ファミリ IPv6 サブモード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	このコマンドは、アドレス ファミリ IPv6 サブモードでサポートされるように変更されました。

使用上のガイドライン

bgp suppress-inactive コマンドは、RIB（非アクティブなルート）に導入されていないルートがピアにアドバタイズされないようにするために使用します。この機能がイネーブルになっていない場合、またはこのコマンドの **no** 形式を使用した場合、Border Gateway Protocol（BGP）によって非アクティブなルートがアドバタイズされます。

（注） BGP は、RIB に導入されていないルートに RIB 失敗フラグを付けます。このフラグは、**show bgp** コマンドの出力にも、Rib-Failure (17) のように表示されます。このフラグは、ルートまたは RIB に関するエラーや問題を示しておらず、このコマンドのコンフィギュレーションによっては、このフラグがあってもルートをアドバタイズできる場合もあります。非アクティブなルートに関する情報を表示するには、**show bgp rib-failure** コマンドを入力します。

例

次の例では、RIB に導入されていないルートをアドバタイズしないように BGP ルーティング プロセスを設定しています。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp suppress-inactive
```

関連コマンド

コマンド	説明
show bgp	BGP ルーティング テーブル内のエントリを表示します。
show bgp rib-failure	ルーティング情報ベース(RIB)テーブルにインストールできなかった BGP ルートを表示します。

bgp transport

Border Gateway Protocol（BGP）のすべてのセッションに対してグローバルに TCP トランスポート セッション パラメータをイネーブルにするには、ルータ コンフィギュレーション モードで **bgp transport** コマンドを使用します。すべての BGP セッションに対してグローバルに TCP トランスポート セッション パラメータをディセーブルにするには、このコマンドの **no** 形式を使用します。

bgp transport path-mtu-discovery

no bgp transport path-mtu-discovery

構文の説明

path-mtu-discovery	トランスポート パスの最大伝送ユニット（MTU）検出をイネーブルにします。

デフォルト

TCP パスの MTU 検出は、すべての BGP セッションに対してデフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると BGP セッションでより大きな MTU リンクを活用できるようになり、これは内部 BGP（iBGP）セッションに非常に重要となることがあるため、このコマンドはデフォルトでイネーブルになっています。TCP パスの MTU 検出がイネーブルになっていることを確認するには、**show bgp neighbors** コマンドを使用します。

例

次に、すべての BGP セッションに対して TCP パスの MTU 検出をディセーブルにする例を示します。

```
ciscoasa(config)# router bgp 4500
ciscoasa(config-router)# no bgp transport path-mtu-discovery
```

次に、すべての BGP セッションに対して TCP パスの MTU 検出をイネーブルにする例を示します。

```
iscoasa(config)# router bgp 4500
ciscoasa(config-router)# bgp transport path-mtu-discovery
```

関連コマンド

コマンド	説明
show bgp neighbors	ネイバーへの BGP 接続に関する情報を表示します。

blocks

ブロック診断（**show blocks** コマンドで表示）に追加のメモリを割り当てるには、特権 EXEC モードで **blocks** コマンドを使用します。値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

blocks queue history enable [*memory_size*]

no blocks queue history enable [*memory_size*]

構文の説明

memory_sizes	（任意）ダイナミックな値を適用するのではなく、ブロック診断用のメモリ サイズをバイト単位で設定します。この値が空きメモリよりも大きい場合は、エラー メッセージが表示され、値は受け入れられません。この値が空きメモリの 50 % を超える場合は、警告メッセージが表示されますが、値は受け入れられます。

デフォルト

ブロック診断の追跡に割り当てられるデフォルト メモリは、2136 バイトです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

現在割り当てられているメモリを表示するには、**show blocks queue history** コマンドを入力します。

ASA をリロードすると、メモリ割り当てがデフォルトに戻ります。

割り当てられるメモリ量は最大 150 KB ですが、空きメモリの 50 % を超えることはありません。必要に応じて、メモリ サイズを手動で指定できます。

例

次に、ブロック診断用のメモリ サイズを増やす例を示します。

```
ciscoasa# blocks queue history enable
```

次に、メモリ サイズを 3000 バイトに増やす例を示します。

```
ciscoasa# blocks queue history enable 3000
```

次に、メモリ サイズを 3000 バイトに増やすことを試みるものの、この値が使用可能な空きメモリを超えている例を示します。

```
ciscoasa# blocks queue history enable 3000
ERROR: memory size exceeds current free memory
```

次に、メモリ サイズを 3000 バイトに増やすものの、この値が空きメモリの 50 % を超えている例を示します。

```
ciscoasa# blocks queue history enable 3000
WARNING: memory size exceeds 50% of current free memory
```

関連コマンド

コマンド	説明
clear blocks	システム バッファの統計情報をクリアします。
show blocks	システム バッファの使用状況を表示します。

boot

システムが次回のリロードで使用するイメージ、およびシステムが起動時に使用するコンフィギュレーション ファイルを指定するには、グローバル コンフィギュレーション モードで **boot** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

boot {**config** | **system**} *url*

no boot {**config** | **system**} *url*

構文の説明

config	システムがロードされるときに使用するコンフィギュレーション ファイルを指定します。
system	システムがロードされるときに使用するシステム イメージ ファイルを指定します。
url	イメージまたはコンフィギュレーションの場所を設定します。マルチ コンテキスト モードでは、管理コンテキストですべてのリモート URL にアクセスできる必要があります。次の URL 構文を参照してください。 • **disk0:/**[*path*/]*filename* ASA では、この URL は内部フラッシュ メモリを示します。**disk0** ではなく **flash** を使用することもできます。これらはエイリアスになっています。 • **disk1:/**[*path*/]*filename* ASA では、この URL は外部フラッシュ メモリ カードを示します。このオプションは、ASA サービス モジュールでは使用できません。 • **flash:/**[*path*/]*filename* この URL は内部フラッシュ メモリを示します。 • **tftp://**[*user*[**:***password*]@]*server*[:*port*]**/**[*path*/]*filename*[**;int=***interface_name*] サーバ アドレスへのルートを上書きする場合は、インターフェイス名を指定します。 このオプションは、ASA 5500 シリーズの **boot system** コマンドだけで使用できます。**boot config** コマンドを使用するには、スタートアップ コンフィギュレーションがフラッシュ メモリに存在している必要があります。 **boot system tftp:** コマンドは、1 つのみ設定でき、かつ最初に設定する必要があります。

デフォルト

- ASA イメージ:
  - Firepower 1000 およびアプライアンス モードの Firepower 2100:以前実行していたブート イメージをブートします。
  - その他の物理 ASA:内部フラッシュ メモリ内で見つかった最初のアプリケーション イメージをブートします。
  - ASAv:最初に展開したときに作成された、読み取り専用の boot:/ パーティションにあるイメージをブートします。
  - Firepower 4100/9300 シャーシ:FXOS システムによってブートする ASA イメージが決定されます。この手順を使用して ASA イメージを設定することはできません。
  - プラットフォーム モードの Firepower 2100: どの ASA/FXOS パッケージをブートするかは FXOS システムによって決定されます。この手順を使用して ASA イメージを設定することはできません。
- スタートアップ コンフィギュレーション:デフォルトでは、ASA は、隠しファイルであるスタートアップ コンフィギュレーションからブートします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.13(1)	このコマンドはアプライアンスモードのサポートで Firepower 1000 および 2100 を追加しました。

使用上のガイドライン

複数の ASA または ASDM イメージがある場合は、ブートするイメージを指定する必要があります。イメージを設定しない場合はデフォルトのブート イメージが使用され、そのイメージは意図されたものではない可能性があります。スタートアップ コンフィギュレーションでは、コンフィギュレーション ファイルを任意で指定できます。

次のモデルのガイドラインを参照してください。

- Firepower 4100/9300 シャーシ：ASA のアップグレードは FXOS によって管理されます。ASA オペレーティングシステム内で ASA をアップグレードすることはできません。したがって、このコマンドを ASA イメージに使用しないでください。ASA と FXOS を別々にアップグレードすることができ、FXOS ディレクトリ リストに別々にリストされます。ASA パッケージには常に ASDM が含まれています。
- プラットフォーム モードの Firepower 2100：ASA、ASDM、および FXOS のイメージは 1 つのパッケージに一緒にバンドルされています。パッケージ更新は FXOS によって管理されます。ASA オペレーティングシステム内で ASA をアップグレードすることはできません。したがって、このコマンドを ASA イメージに使用しないでください。ASA と FXOS を個別にアップグレードすることはできません。常にバンドルされています。
- アプライアンス モードの Firepower 1000 および 2100：ASA、ASDM、および FXOS のイメージは 1 つのパッケージに一緒にバンドルされています。パッケージの更新は、次のコマンドを使用して ASA によって管理されます。これらのプラットフォームでは、ブートするイメージを識別するために ASA が使用されますが、基盤となるメカニズムはレガシー ASA とは異なります。
- ASAv：初期展開の ASAv パッケージでは、ASA イメージが読み取り専用 boot:/ パーティションに配置されます。ASAv をアップグレードするときは、フラッシュ メモリに別のイメージを指定します。後でコンフィギュレーションをクリアすると（**clear configure all**）、ASAv は元の展開のイメージをロードするようになることに注意してください。初期展開の ASAv パッケージには、フラッシュ メモリに配置される ASDM イメージも含まれています。ASDM イメージを個別にアップグレードできます。

boot config コマンドを、**write memory** コマンドを使用してスタートアップ コンフィギュレーションに保存すると、CONFIG_FILE 環境変数にも設定が保存されます。ASA は、これらの環境変数を使用して、再起動時にブートするスタートアップ コンフィギュレーションを決定します。

現在の実行コンフィギュレーションとは異なる、新しい場所にあるスタートアップ コンフィギュレーション ファイルを使用する場合は、実行コンフィギュレーションを保存した後に、必ず、スタートアップ コンフィギュレーション ファイルを新しい場所にコピーしてください。このようにしないと、実行コンフィギュレーションの保存時に、実行コンフィギュレーションによって新しいスタートアップ コンフィギュレーションが上書きされます。

ヒント　ASDM イメージ ファイルは、**asdm image** コマンドで指定します。

アプライアンスモードの Firepower 1000 および 2100 のブートシステム

boot system コマンドは 1 つだけ入力できます。新しいイメージにアップグレードする場合は、**no boot system** を入力して、以前に設定したイメージを削除する必要があります。

設定に **boot system** コマンドが存在しない場合があることに注意してください。たとえば、ROMMON からイメージをインストールした場合、新しいデバイスがある場合、またはコマンドを手動で削除した場合などです。

boot system コマンドは、入力時にアクションを実行します。システムはイメージを検証して解凍し、ブート場所（FXOS によって管理される disk0 の内部ロケーション）にコピーします。ASA をリロードすると、新しいイメージがロードされます。リロードの前に気が変わった場合は、**no boot system** コマンドを入力してブート場所から新しいイメージを削除し、現在のイメージを引き続き実行することができます。このコマンドを入力した後で ASA フラッシュメモリから元のイメージ ファイルを削除することもできます。その場合、ASA はブート場所から正しく起動します。

他のモデルとは異なり、スタートアップ コンフィギュレーション内のこのコマンドは、ブート イメージに影響しません（本質的に表面的なものです）。リロード時には、最後にロードされたブート イメージが常に実行されます。このコマンドを入力した後で設定を保存しない場合、リロードすると、新しいイメージが起動された場合でも、古いコマンドが設定に出現します。設定を保存することにより、設定の同期を維持する必要があります。

Cisco ダウンロード サイトからロードできるのは、元のファイル名のイメージのみです。ファイル名を変更した場合はロードされません。Firepower Threat Defense（FTD）イメージをロードすることによって、FTD に再イメージ化することもできます。この場合は、すぐにリロードするように求められます。

他のモデルのブートシステム

最大 4 つの **boot system** コマンドエントリを入力して、複数のイメージをブートする順番に指定することができます。ASA は、最初に検出に成功したイメージをブートします。**boot system** コマンドを入力すると、エントリがリストの最後に追加されます。ブートエントリの順序を変更するには、**clear configure boot system** コマンドを使用してすべてのエントリを削除してから、エントリを目的の順序で再入力する必要があります。設定できる **boot system tftp** コマンドは 1 つだけです。これは、最初に設定する必要があります。

boot system コマンドを、**write memory** コマンドを使用してスタートアップ コンフィギュレーションに保存すると、BOOT 環境変数にも設定が保存されます。ASA は、これらの環境変数を使用して、再起動時にブートするスタートアップ コンフィギュレーションを決定します。

例

次に、起動時に ASA が configuration.txt という名前のコンフィギュレーション ファイルをロードするように指定する例を示します。

```
ciscoasa(config)# boot config disk0:/configuration.txt
```

関連コマンド

コマンド	説明
asdm image	ASDM ソフトウェア イメージを指定します。
show bootvar	ブート ファイルおよびコンフィギュレーションの環境変数を表示します。

border style

認証された WebVPN ユーザに表示される WebVPN ホームページの境界線をカスタマイズするには、カスタマイゼーション コンフィギュレーション モードで **border style** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

border style *value*

no border style *value*

構文の説明

value	使用する Cascading Style Sheet（CSS）パラメータを指定します。許容最大文字数は 256 文字です。

デフォルト

境界線のデフォルト スタイルは background-color:#669999;color:white です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
カスタマイゼーション コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進数値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

(注) WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、境界線の背景色を RGB カラー #66FFFF（緑色の一種）にカスタマイズする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# border style background-color:66FFFF
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの [Application Access] ボックスをカスタマイズします。
browse-networks	WebVPN ホームページの [Browse Networks] ボックスをカスタマイズします。
web-bookmarks	WebVPN ホームページの [Web Bookmarks] タイトルまたはリンクをカスタマイズします。
file-bookmarks	WebVPN ホームページの [File Bookmarks] タイトルまたはリンクをカスタマイズします。

bridge-group

トランスペアレント ファイアウォール モードのブリッジ グループにインターフェイスを割り当てるには、インターフェイス コンフィギュレーション モードで **bridge-group** コマンドを使用します。インターフェイスの割り当てを解除するには、このコマンドの **no** 形式を使用します。トランスペアレント ファイアウォールは、そのインターフェイスで同じネットワークを接続します。1 つのブリッジ グループに最大 4 つのインターフェイスが属することができます。9.6(2) 以降では、ブリッジ グループに最大 64 個のインターフェイスを追加できます。

bridge-group *number*

no bridge-group *number*

構文の説明

number	1 ～ 100 の整数を指定します。9.3(1) 以降、範囲が 1 ～ 250 に拡大されました。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	—	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.3(1)	250 BVI をサポートするために数値の範囲が 1 ～ 250 に増加しました。
9.6(2)	ブリッジ グループあたりのインターフェイスの最大数が 4 から 64 に拡張されました。

使用上のガイドライン

9.2 以前では、シングル モードまたはマルチ モードのコンテキストごとに最大 8 個のブリッジ グループを設定できます。9.3(1) 以降では、最大 250 個のブリッジ グループを設定できます。各ブリッジ グループには、最大 4 つのインターフェイスを含めることができます。同一インターフェイスを複数のブリッジ グループに割り当てることはできません。少なくとも 1 つのブリッジ グループを使用し、データ インターフェイスがブリッジ グループに属している必要があることに注意してください。

(注) ASA 5505 に複数のブリッジ グループを設定できますが、ASA 5505 のトランスペアレント モードのデータ インターフェイスは 2 つという制限は、実質的にブリッジ グループを 1 つだけ使用できることを意味します。

interface bvi コマンドの後に **ip address** コマンドを使用して、ブリッジ グループに管理 IP アドレスを割り当てます。

各ブリッジ グループは、別々のネットワークに接続します。ブリッジ グループのトラフィックは他のブリッジ グループから隔離され、トラフィックは ASA 内の他のブリッジ グループにはルーティングされません。また、トラフィックは外部ルータから ASA 内の他のブリッジ グループにルーティングされる前に、ASA から出る必要があります。

セキュリティ コンテキストのオーバーヘッドを防ぐ場合、またはセキュリティ コンテキストの使用を最小限に抑える場合、複数のブリッジ グループを使用することがあります。ブリッジング機能はブリッジ グループごとに分かれていますが、その他の多くの機能はすべてのブリッジ グループ間で共有されます。たとえば、syslog サーバまたは AAA サーバの設定は、すべてのブリッジ グループで共有されます。セキュリティ ポリシーを完全に分離するには、各コンテキスト内に 1 つのブリッジ グループにして、セキュリティ コンテキストを使用します。

例

次に、ブリッジ グループ 1 に GigabitEthernet 1/1 を割り当てる例を示します。

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# bridge-group 1
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定します。
interface bvi	管理 IP アドレスを設定できるように、ブリッジ グループについてインターフェイス コンフィギュレーション モードを開始します。
ip address	ブリッジ グループの管理 IP アドレスを設定します。
nameif	インターフェイス名を設定します。
security-level	インターフェイスのセキュリティ レベルを設定します。

browse-networks

認証された WebVPN ユーザに表示される WebVPN ホームページの [Browse Networks] ボックスをカスタマイズするには、webvpn カスタマイゼーション コンフィギュレーション モードで **browse-networks** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

browse-networks {**title** | **message** | **dropdown**} {**text** | **style**} *value*

no browse-networks [{**title** | **message** | **dropdown**} {**text** | **style**} *value*]

構文の説明

dropdown	ドロップダウン リストへの変更を指定します。
message	タイトルの下に表示されるメッセージへの変更を指定します。
style	スタイルへの変更を指定します。
text	テキストへの変更を指定します。
title	タイトルへの変更を指定します。
value	表示される実際のテキストを示します。許容最大文字数は 256 文字です。この値は、Cascading Style Sheet（CSS）パラメータにも適用されます。

デフォルト

デフォルトのタイトル テキストは「Browse Networks」です。

デフォルトのタイトル スタイルは、次のとおりです。

background-color:#99CCCC;color:black;font-weight:bold;text-transform:uppercase

デフォルトのメッセージ テキストは「Enter Network Path」です。

メッセージのデフォルト スタイルは次のとおりです。

background-color:#99CCCC;color:maroon;font-size:smaller.

デフォルトのドロップダウン テキストは「File Folder Bookmarks」です。

ドロップダウンのデフォルト スタイルは次のとおりです。

border:1px solid black;font-weight:bold;color:black;font-size:80%.

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn カスタマイゼーション コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、タイトルを「Browse Corporate Networks」に変更し、スタイル内のテキストを青色に変更する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# browse-networks title text Browse Corporate Networks
ciscoasa(config-webvpn-custom)# browse-networks title style color:blue
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの [Application Access] ボックスをカスタマイズします。
file-bookmarks	WebVPN ホームページの [File Bookmarks] タイトルまたはリンクをカスタマイズします。
web-applications	WebVPN ホームページの [Web Application] ボックスをカスタマイズします。
web-bookmarks	WebVPN ホームページの [Web Bookmarks] タイトルまたはリンクをカスタマイズします。

CHAPTER 5

cache コマンド～ clear compression コマンド

cache

キャッシュ モードを開始し、キャッシング属性の値を設定するには、webvpn コンフィギュレーション モードで **cache** コマンドを入力します。コンフィギュレーションからキャッシュ関連のコマンドをすべて削除し、これらをデフォルト値にリセットするには、このコマンドの **no** 形式を入力します。

cache

no cache

デフォルト

ディセーブル

コマンド モード

次の表は、このコマンドを入力するモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
9.5(2)	デフォルトがイネーブルからディセーブルに変更されました。

使用上のガイドライン

キャッシングによって頻繁に再利用されるオブジェクトはシステム キャッシュに保存され、コンテンツを繰り返しリライトしたり圧縮したりする必要性を減らすことができます。これにより、WebVPN とリモート サーバおよびエンド ユーザのブラウザの両方の間のトラフィックが削減されて、多くのアプリケーションの実行効率が大幅に向上します。

(注) コンテンツ キャッシングをイネーブルにすると、一部のシステムの信頼性が低下します。コンテンツ キャッシングをイネーブルにした後、ランダムにクラッシュが発生する場合は、この機能をディセーブルにしてください。

次に、キャッシュ モードを開始する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# cache
hostname(config-webvpn-cache)#
```

関連コマンド

コマンド	説明
cache-static-content	書き換えの対象でないコンテンツをキャッシュします。
disable	キャッシュをディセーブルにします。
expiry-time	オブジェクトを再検証せずにキャッシュする有効期限を設定します。
lmfactor	最終変更時刻のタイムスタンプだけを持つオブジェクトのキャッシュに関する再確認ポリシーを設定します。
max-object-size	キャッシュするオブジェクトの最大サイズを定義します。
min-object-size	キャッシュするオブジェクトの最小サイズを定義します。

ca-check

基本制約の拡張を設定し、トラストポイント証明書に CA フラグを設定するには、crypto ca トラストポイント コンフィギュレーション モードで **ca-check** コマンドを使用します。基本制約の拡張と CA フラグを設定しない場合は、このコマンドの **no** 形式を使用します。

ca-check

no ca-check

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、基本制約の拡張と CA フラグが設定されます。これらを無効にするには、**no** 形式を使用する必要があります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

基本制約の拡張によって、証明書のサブジェクトが認証局（CA）かどうかが識別されます。この場合、証明書を使用して他の証明書に署名することができます。CA フラグは、この拡張の一部です。これらの項目が証明書に存在することは、証明書の公開キーを使用して証明書の署名を検証できることを示します。

例

次に、CA フラグと基本制約の拡張を無効にする例を示します。

```
ciscoasa(config)# crypto ca trustpoint newtrust
ciscoasa(config-ca-trustpoint)# no ca-check
ciscoasa(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	クリプト CA トラストポイント コンフィギュレーション モードを開始します。このコマンドは、グローバル コンフィギュレーション モードで使用します。

cache-static-content

クライアントレス SSL VPN 接続に使用するすべての静的コンテンツをキャッシュするには、webvpn キャッシュ コンフィギュレーション モードで **cache-static-content** コマンドを入力します。静的コンテンツのキャッシングをディセーブルにするには、このコマンドの **no** 形式を入力します。

cache-static-content enable

no cache-static-content enable

構文の説明

enable	すべての静的コンテンツのキャッシュ メモリへのロードをイネーブルにします。

デフォルト

ディセーブル

コマンド モード

次の表は、このコマンドを入力するモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn キャッシュ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

キャッシュ可能なすべての静的コンテンツがアプライアンス キャッシュに保存されるようセキュリティ アプライアンスを設定すると、バックエンド SSL VPN 接続のパフォーマンスが向上します。静的コンテンツには、PDF ファイルやイメージなど、セキュリティ アプライアンスによってデータの書き換えが行われないオブジェクトが含まれています。

例

次に、静的コンテンツのキャッシングをイネーブルにする例を示します。

```
ciscoasa(config-webvpn-cache)# cache-static-content enable
```

関連コマンド

コマンド	説明
disable	キャッシュをディセーブルにします。
expiry-time	オブジェクトを再検証せずにキャッシュする有効期限を設定します。

cache-time

CRL を失効と見なす前にキャッシュ内に残す時間を分単位で指定するには、ca-crl コンフィギュレーション モードで **cache-time** コマンドを使用します。このモードには、クリプト CA トラストポイント コンフィギュレーション モードからアクセスできます。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

cache-time *refresh-time*

no cache-time

構文の説明

refresh-time	CRL をキャッシュ内に残す時間を分単位で指定します。指定できる範囲は 1 ～ 1440 分です。CRL に NextUpdate フィールドがない場合、CRL はキャッシュされません。

デフォルト

デフォルトの設定は 60 分です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ca-crl コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、ca-crl コンフィギュレーション モードを開始し、トラストポイント central でキャッシュ時間のリフレッシュ値を 10 分に指定する例を示します。

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# cache-time 10
ciscoasa(ca-crl)#
```

関連コマンド

コマンド	説明
crl configure	CRL コンフィギュレーション モードを開始します。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
enforcenextupdate	証明書で NextUpdate CRL フィールドを処理する方法を指定します。

call-agent

コール エージェントのグループを指定するには、MGCP マップ コンフィギュレーション モードで **call-agent** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

call-agent *ip_address group_id*

no call-agent *ip_address group_id*

構文の説明

group_id	コール エージェント グループの ID（0 ～ 2147483647）。
ip_address	ゲートウェイの IP アドレス。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
MGCP マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

1 つ以上のゲートウェイを管理できるコール エージェントのグループを指定するには、**call-agent** コマンドを使用します。コール エージェントのグループ情報は、どのコール エージェントも応答を送信できるように、グループ内の（ゲートウェイがコマンドを送信する先以外の）コール エージェントに接続を開くために使用されます。同じ *group_id* を持つコール エージェントは、同じグループに属します。1 つのコール エージェントは複数のグループに所属できます。

例

次に、コール エージェント 10.10.11.5 および 10.10.11.6 にゲートウェイ 10.10.10.115 の制御を許可し、コール エージェント 10.10.11.7 および 10.10.11.8 にゲートウェイ 10.10.10.116 および 10.10.10.117 の制御を許可する例を示します。

```
ciscoasa(config)# mgcp-map mgcp_inbound
ciscoasa(config-mgcp-map)# call-agent 10.10.11.5 101
ciscoasa(config-mgcp-map)# call-agent 10.10.11.6 101
ciscoasa(config-mgcp-map)# call-agent 10.10.11.7 102
ciscoasa(config-mgcp-map)# call-agent 10.10.11.8 102
ciscoasa(config-mgcp-map)# gateway 10.10.10.115 101
```

```
ciscoasa(config-mgcp-map)# gateway 10.10.10.116 102
ciscoasa(config-mgcp-map)# gateway 10.10.10.117 102
```

関連コマンド

コマンド	説明
debug mgcp	MGCP のデバッグ情報の表示をイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。
show mgcp	MGCP のコンフィギュレーションおよびセッションの情報を表示します。

call-duration-limit

H.323 コールのコール継続時間を設定するには、パラメータ コンフィギュレーション モードで **call-duration-limit** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

call-duration-limit *hh:mm:ss*

no call-duration-limit *hh:mm:ss*

構文の説明

hh:mm:ss	継続時間を時、分、および秒で指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、H.323 コールのコール継続時間を設定する例を示します。

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# call-duration-limit 0:1:0
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3 またはレイヤ 4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

call-party-numbers

H.323 コールの設定時に発信側の番号の送信を強制するには、パラメータ コンフィギュレーション モードで **call-party-numbers** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

call-party-numbers

no call-party-numbers

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、H.323 コールのコール設定時に発信側の番号を適用する例を示します。

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# call-party-numbers
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3 またはレイヤ 4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

call-home

Call Home コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **call-home** コマンドを使用します。

call-home

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが追加されました。

使用上のガイドライン

call-home コマンドを入力すると、プロンプトが hostname (cfg-call-home)# に変更され、次の Call Home コンフィギュレーション コマンドを利用できます。

- [**no**] **alert-group** {**group name** | **all**}：Smart Call Home グループをイネーブルまたはディセーブルにします。デフォルトでは、すべてのアラート グループに対してイネーブルになっています。
  group name：syslog、診断、環境、インベントリ、コンフィギュレーション、スナップショット、脅威、テレメトリ、テスト。
- [**no**] **contact-e-mail-addr e-mail-address**：カスタマーの連絡先電子メール アドレスを指定します。このフィールドは必須です。
  e-mail-address：最大 127 文字のカスタマーの電子メール アドレス。
- [**no**] **contact-name contact name**：カスタマーの名前を指定します。
  e-mail-address：最大 127 文字のカスタマーの名前。
- [**no**] **contract-id contract-id-string**：カスタマーの契約 ID を指定します。
  contract-id-string：最大 128 文字の ID 番号。スペースを使用できますが、スペースが含まれる場合はストリングの前後に引用符を付ける必要があります。

- **copy profile src-profile-name dest-profile-name**：既存のプロファイル（**src-profile-name**）の内容を新しいプロファイル（**dest-profile-name**）にコピーします。
  src-profile-name：23 文字までの既存プロファイルの名前。
  dest-profile-name：23 文字までの新規プロファイルの名前。
- **rename profile src-profile-name dest-profile-name**：既存のプロファイルの名前を変更します。
  src-profile-name：23 文字までの既存プロファイルの名前。
  dest-profile-name：23 文字までの新規プロファイルの名前。
- **no configuration all**：Smart Call-home コンフィギュレーションをクリアします。
  [**no**] **customer-id customer-id-string**：カスタマー ID を指定します。
  customer-id-string：最大 64 文字のカスタマー ID。このフィールドは、XML 形式のメッセージでは必須です。
- [**no**] **event-queue-size queue_size**：イベント キュー サイズを指定します。
  queue-size：5 ～ 60 でイベント数を示します。デフォルトは 10 です。
- [**no**] **mail-server ip-address | name priority 1-100 all**：SMTP メール サーバを指定します。顧客は、最大 5 つのメール サーバを指定できます。Smart Call Home メッセージに電子メール転送を使用するには、少なくとも 1 つのメール サーバが必要です。
  ip-address：メール サーバの IPv4 アドレスまたは IPv6 アドレス。
  name：メール サーバのホスト名。
  1-100：メール サーバのプライオリティ。値が小さいほど、プライオリティが高くなります。
- [**no**] **phone-number phone-number-string**：カスタマーの電話番号を指定します。このフィールドは任意です。
  phone-number-string：電話番号。
- [**no**] **rate-limit msg-count**：Smart Call Home が 1 分間に送信できるメッセージの数を指定します。
  msg-count：1 分間に送信できるメッセージ数。デフォルトは 10 です。
- [**no**] **sender** {**from e-mail-address | reply-to e-mail-address**}：電子メール メッセージの from および reply-to の電子メール アドレスを指定します。このフィールドは任意です。
  e-mail-address：発信元または応答先の電子メール アドレス。
- [**no**] **site-id site-id-string**：カスタマー サイト ID を指定します。このフィールドは任意です。
  site-id-string：カスタマーの場所を識別するサイト ID。
- [**no**] **street-address street-address**：カスタマーの住所を指定します。このフィールドは任意です。
  street-address：最大 255 文字の自由形式の文字列。
- [**no**] **alert-group-config environment**：環境グループ コンフィギュレーション モードを開始します。
  [**no**] **threshold** {**cpu | memory**} **low-high**：環境リソースしきい値を指定します。
  low、**high**：有効な値は 0 ～ 100 です。デフォルトは 85 ～ 90 です。
- [**no**] **alert-group-config snapshot**：スナップショット グループ コンフィギュレーション モードを開始します。
  system、**user**：システム コンテキストまたはユーザ コンテキスト（マルチ モードでのみ使用可）で CLI を実行します。
- [**no**] **add-command “cli command”** [{**system | user**}]：スナップショット グループにキャプチャする CLI コマンドを指定します。
  cli command：入力する CLI コマンド。
  system、**user**：CLI をシステム コンテキストまたはユーザ コンテキストで実行します（マルチ モードだけで使用可能）。システムもユーザも指定しないと、CLI はシステム コンテキストとユーザ コンテキストの両方で実行されます。デフォルトは、ユーザ コンテキストです。

（注） Call-Home HTTPS メッセージは、ここで説明する **vrf** コマンドとは別に、**ip http client source-interface** コマンドを使用して、指定した VRF 上の送信元インターフェイスを介してだけ送信できます。

例

次に、連絡先情報を設定する例を示します。

```
hostname(config)# call-home
hostname(cfg-call-home)# contact-e-mail-addr username@example.com
hostname(cfg-call-home)# customer-id Customer1234
hostname(cfg-call-home)# phone-number +1-800-555-0199
hostname(cfg-call-home)# site-id Site1
hostname(cfg-call-home)# street-address "1234 Any Street, Any city, Any state, 12345"
```

次に、Call Home メッセージのレート制限しきい値を設定する例を示します。

```
hostname(config)# call-home
hostname(cfg-call-home)# rate-limit 50
```

次に、Call Home メッセージのレート制限しきい値をデフォルト設定にする例を示します。

```
hostname(config)# call-home
hostname(cfg-call-home)# default rate-limit
```

次に、既存のプロファイルと同じコンフィギュレーション設定の新しい宛先プロファイルを作成する例を示します。

```
hostname(config)# call-home
hostname(cfg-call-home)# copy profile profile1 profile1a
```

次に、一般的な電子メール パラメータ(プライマリ電子メール サーバ、セカンダリ電子メール サーバなど)を設定する例を示します。

```
hostname(config)# call-home
hostname(cfg-call-home)# mail-server smtp.example.com priority 1
hostname(cfg-call-home)# mail-server 192.168.0.1 priority 2
hostname(cfg-call-home)# sender from username@example.com
hostname(cfg-call-home)# sender reply-to username@example.com
```

関連コマンド

コマンド	説明
alert-group	アラート グループをイネーブルにします。
profile	Call Home プロファイル コンフィギュレーション モードを開始します。
show call-home	Call Home コンフィギュレーション情報を表示します。

call-home send

CLI コマンドを実行し、指定されたアドレスにコマンド出力を電子メールで送信するには、特権 EXEC モードで **call-home send** コマンドを使用します。

call-home send cli command [**email** *email*] [**service-number** *service number*]

構文の説明

cli-command	実行する CLI コマンドを指定します。コマンド出力は電子メールで送信されます。
email *email*	CLI コマンド出力の送信先の電子メール アドレスを指定します。電子メール アドレスを指定していない場合、コマンド出力は Cisco TAC（attach@cisco.com）に送信されます。
service-number *service number*	コマンド出力が関係するアクティブな TAC ケース番号を指定します。この番号は、電子メール アドレス（または TAC 電子メール アドレス）が指定されていない場合にのみ必要で、電子メールの件名行に表示されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、指定した CLI コマンドがシステム上で実行されます。指定する CLI コマンドは、引用符（""）で囲む必要があります。また、任意の **run** コマンドまたは **show** コマンド（すべてのモジュール用のコマンドを含む）を指定できます。

その後、コマンド出力は、電子メールで指定の電子メール アドレスに送信されます。電子メール アドレスを指定していない場合、コマンド出力は Cisco TAC（attach@cisco.com）に送信されます。電子メールは、件名行にサービス番号を付けて（指定した場合）ロング テキスト形式で送信されます。

例

次に、CLI コマンドを送信し、コマンド出力を電子メールで送信する例を示します。

```
hostname# call-home send "show diagnostic result module all" email support@example.com
```

関連コマンド

call-home	Call Home コンフィギュレーション モードを開始します。
call-home test	定義した Call Home テスト メッセージを送信します。
service call-home	Call Home をイネーブルまたはディセーブルにします。
show call-home	Call Home コンフィギュレーション情報を表示します。

call-home send alert-group

特定のアラート グループ メッセージを送信するには、特権 EXEC モードで **call-home send alert-group** コマンドを使用します。

call-home send alert-group {**configuration** | **telemetry** | **inventory** | **group snapshot**} [**profile** *profile-name*]

構文の説明

設定	コンフィギュレーション アラート グループ メッセージを宛先プロファイルに送信します。
group snapshot	スナップショット グループを送信します。
インベントリ	インベントリ call-home メッセージを送信します。
profile *profile-name*	(任意)宛先プロファイルの名前を指定します。
Telemetry	特定のモジュール、スロット/サブスロット、またはスロット/ベイ番号に関する診断アラート グループ メッセージを宛先プロファイルに送信します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが追加されました。

使用上のガイドライン

profile *profile-name* を指定しない場合は、サブスクライブ対象のすべての宛先プロファイルにメッセージが送信されます。

手動で送信できるのは、コンフィギュレーション、診断、およびインベントリ アラート グループだけです。宛先プロファイルは、アラート グループにサブスクライブされる必要はありません。

例

次に、コンフィギュレーション アラート グループ メッセージを宛先プロファイルに送信する例を示します。

```
hostname# call-home send alert-group configuration
```

次に、特定のモジュール、スロット/サブスロット、またはスロット/ベイ番号に関する診断アラート グループ メッセージを宛先プロファイルに送信する例を示します。

```
hostname# call-home send alert-group diagnostic module 3 5/2
```

次に、特定のモジュール、スロット/サブスロット、またはスロット/ベイ番号に関する診断アラート グループ メッセージをすべての宛先プロファイルに送信する例を示します。

```
hostname# call-home send alert-group diagnostic module 3 5/2 profile Ciscotac1
```

次に、インベントリ call-home メッセージを送信する例を示します。

```
hostname# call-home send alert-group inventory
```

関連コマンド

call-home	Call Home コンフィギュレーション モードを開始します。
call-home test	定義した Call Home テスト メッセージを送信します。
service call-home	Call Home をイネーブルまたはディセーブルにします。
show call-home	Call Home コンフィギュレーション情報を表示します。

call-home test

プロファイルのコンフィギュレーションを使用して Call Home テスト メッセージを手動で送信するには、特権 EXEC モードで **call-home test** コマンドを使用します。

call-home test [“*test-message*”] **profile** *profile-name*

構文の説明

profile *profile-name*	宛先プロファイルの名前を指定します。
“*test-message*”	（任意）テスト メッセージ テキスト。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、テスト メッセージが指定の宛先プロファイルに送信されます。テスト メッセージ テキストを入力する場合、テキストにスペースが含まれている場合は、このテキストを引用符（""）で囲む必要があります。メッセージを入力しない場合、デフォルト メッセージが送信されます。

例

次に、Call Home テスト メッセージを手動で送信する例を示します。

```
hostname# call-home test “test of the day” profile Ciscotac1
```

関連コマンド

call-home	Call Home コンフィギュレーション モードを開始します。
call-home send alert-group	特定のアラート グループ メッセージを送信します。
service call-home	Call Home をイネーブルまたはディセーブルにします。
show call-home	Call Home コンフィギュレーション情報を表示します。

capability lls

LLS 機能はデフォルトでイネーブルです。送信される OSPF パケットのリンクローカル シグナリング（LLS）データ ブロックの使用を明示的にイネーブルにし、OSPF NSF 認識を再度イネーブルにするには、ルータ コンフィギュレーション モードで **capability lls** コマンドを使用します。LLS と OSPF NSF 認識をディセーブルにするには、このコマンドの no 形式を使用します。

capability lls

no capability lls

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

LLS 機能はデフォルトでイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが導入されました。

使用上のガイドライン

送信される OSPF パケットの LLS データ ブロックの使用をディセーブルにすることで、NSF 認識をディセーブルにすることが必要な場合があります。また、LLS を使用するアプリケーションがルータで動作していない場合に、NSF 認識をディセーブルにすることが必要な場合があります。

NSF が設定されている状態で LLS をディセーブルにしようとすると、「OSPF Non-Stop Forwarding (NSF) must be disabled first」というエラー メッセージが表示されます。

LLS がディセーブルになっている状態で、NSF を設定しようとすると、「OSPF Link-Local Signaling (LLS) capability must be enabled first」というエラー メッセージが表示されます。

例

次に、LLS のサポートと OSPF 認識をイネーブルにする例を示します。

```
ciscoasa(config)# router ospf 2
ciscoasa(config-router)# capability lls
```

関連コマンド		
	capability opaque	Opaque LSA を使用して MPLS TE 情報をネットワークにフラッディングできるようにします。

capability opaque

マルチプロトコル ラベル スイッチング トラフィック エンジニアリング（MPLS TE）トポロジ情報を Opaque LSA を介してネットワークにフラッディングできるようにするには、ルータ コンフィギュレーション モードで **capability opaque** コマンドを使用します。MPLS TE トポロジ情報が Opaque LSA を介してネットワークにフラッディングされないようにするには、このコマンドの no 形式を使用します。

capability opaque

no capability opaque

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

Opaque LSA はデフォルトでイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが導入されました。

使用上のガイドライン

capability opaque コマンドは、すべての範囲（タイプ 9、10、11）の Opaque LSA を介して MPLS TE 情報（タイプ 1 および 4）をフラッディングします。

Opaque LSA サポート機能の制御は、MPLS TE をサポートするために OSPF でイネーブルにする必要があります。

MPLS TE トポロジ情報は、デフォルトで、Opaque LSA を介してエリアにフラッディングされます。

例

次に、Opaque 機能をイネーブルにする例を示します。

```
ciscoasa(config)# router ospf 2
ciscoasa(config-router)# capability opaque
```

関連コマンド		
	capability lls	送信される OSPF パケットの LLS データ ブロックの使用をイネーブルにし、OSPF NSF 認識をイネーブルにします。

captive-portal

ASA FirePOWER モジュールのキャプティブ ポータルをイネーブルにするには、グローバル コンフィギュレーション モードで **captive-portal** コマンドを使用します。キャプティブ ポータルをディセーブルにするには、このコマンドの **no** 形式を使用します。

captive-portal {**global** | **interface** *name*} [**port** *number*]

no captive-portal {**global** | **interface** *name*} [**port** *number*]

構文の説明

global	すべてのインターフェイスでキャプティブ ポータルをグローバルにイネーブルにします。
interface *name*	指定したインターフェイスのみでキャプティブ ポータルをイネーブルにします。コマンドを複数入力して複数のインターフェイスでイネーブルにできます。この方法は、一部のインターフェイスのみのトラフィックを ASA FirePOWER モジュールにリダイレクトする場合に使用します。
port *number*	（任意）認証プロキシ ポートを 1025 以上に設定します。デフォルト ポートである 885 を設定する場合は、このキーワードを指定しないでください。

コマンド デフォルト

デフォルト ポートは 885（TCP）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

キャプティブ ポータルは、ASA FirePOWER モジュールで定義されたアイデンティティ ポリシーと連携して動作します。

HTTP/HTTPS 接続については、アクティブな認証を通じてユーザ ID を収集するアイデンティティ ルールを定義できます。アクティブな認証アイデンティティ ルールを実装する場合は、認証プロキシ ポートとして機能するように ASA でキャプティブ ポータルを設定する必要があります。接続がアクティブ認証を要求するアイデンティティ ルールに一致すると、ASA FirePOWER モジュールは、認証要求を ASA インターフェイスの IP アドレス/キャプティブ ポータルにリダイレクトします。デフォルト ポートは 885 ですが、これは変更可能です。

認証プロキシのキャプティブ ポータルをイネーブルにしない場合は、パッシブ認証のみを使用できます。

例

次に、デフォルト ポート 885 でキャプティブ ポータルをグローバルにイネーブルにする例を示します。

```
ciscoasa(config)# captive-portal global
ciscoasa(config)#
```

関連コマンド

コマンド	説明
sfr	ASA FirePOWER モジュールにトラフィックをリダイレクトします。
show running-config captive-portal	キャプティブ ポータル コンフィギュレーションを表示します。
show service-policy	サービス ポリシーの統計情報を表示します。

capture

パケットスニッフィングおよびネットワーク障害の切り分けのために、パケットキャプチャ機能をイネーブルにするには、特権 EXEC モードで **capture** コマンドを使用します。パケットキャプチャ機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

ネットワークトラフィックをキャプチャします。

capture *capture_name* [**type** {**asp-drop** [**all** | *drop-code*] | **tls-proxy** | **raw-data** | **isakmp** [**ikev1** | **ikev2**] | **inline-tag** [*tag*] | **webvpn user** *webvpn-user*}] [**access-list** *access_list_name*] {**interface** {*interface_name* | **asa_dataplane** | **asa_mgmt_plane** | **cplane**} } [**buffer** *buf_size*] [**ethernet-type** *type*] [**reeinject-hide**] [**packet-length** *bytes*] [**circular-buffer**] [**trace** [**trace-count** *number*]] [**real-time** [**dump**] [**detail**]] [**match** *protocol* {**host** *source-ip* | *source-ip mask* | **any** | **any4** | **any6**} [*operator src_port*] {**host** *dest_ip* |*dest_ip mask* | **any** | **any4** | **any6**} [*operator dest_port*]] [**switch**] [**offload**] [**ivlan** *number*] [**ovlan** *number*]

クラスタ制御リンクトラフィックをキャプチャします。

capture *capture_name* {**type lacp interface** *interface_id* [**buffer** *buf_size*] [**packet-length** *bytes*] [**circular-buffer**] [**real-time** [**dump**] [**detail**]]

capture *capture_name* **interface cluster** [**buffer** *buf_size*] [**ethernet-type** *type*] [**packet-length** *bytes*] [**circular-buffer**] [**cp-cluster**] [**trace** [**trace-count** *number*]] [**real-time** [**dump**] [**detail**]] [**trace**] [**match** *protocol* {**host** *source-ip* | *source-ip mask* | **any** | **any4** | **any6**} [*operator src_port*] {**host** *dest_ip* |*dest_ip mask* | **any** | **any4** | **any6**} [*operator dest_port*]]

クラスタ全体のパケットをキャプチャします。

cluster exec capture *capture_name* [**persist**] [**include-decrypted**]

永続的なパケットトレースクラスタ全体をクリアします。

cluster exec clear packet-trace

パケットキャプチャを削除します。

no capture *capture_name* [*arguments*]

パケットキャプチャを手動で開始または停止します。

capture *capture_name* **stop**

no capture *capture_name* **stop**

構文の説明

access-list *access_list_name*	(任意)アクセス リストと一致するトラフィックをキャプチャします。マルチ コンテキスト モードでは、1 つのコンテキスト内でのみこのコマンドを使用できます。
any	すべての IPv4 トラフィックを指定します。
any4	すべての IPv4 トラフィックを指定します。
any6	すべての IPv6 トラフィックを指定します。
all	高速セキュリティ パスでドロップされるすべてのパケットをキャプチャします。

asa_dataplane	ASA とバックプレーンを使用するモジュール（ASA FirePOWER モジュールなど）の間を通過する ASA バックプレーンのパケットをキャプチャします。
asp-drop *drop-code*	（任意）高速セキュリティ パスでドロップされるパケットをキャプチャします。*drop-code* は、高速セキュリティ パスでドロップされるトラフィックのタイプを指定します。ドロップ コードのリストについては、**show asp drop frame** コマンドを参照してください。このキーワードは、**packet-length**、**circular-buffer**、および **buffer** の各キーワードとともに入力できますが、**interface** キーワードや **ethernet-type** キーワードとともに入力することはできません。クラスタでは、ドロップされた、ユニット間の転送データ パケットもキャプチャされます。マルチ コンテキスト モードでは、このオプションがシステム実行スペースで発行されると、すべてのドロップされたデータ パケットがキャプチャされます。このオプションがコンテキストで発行されたときは、ドロップされたデータ パケットのうち、そのコンテキストに属するインターフェイスから入ったものだけがキャプチャされます。
buffer *buf_size*	（任意）パケットの保存に使用するバッファのサイズをバイト単位で定義します。このバイト数のバッファがいっぱいになると、パケット キャプチャは停止します。クラスタ内で使用されるときは、これはユニットあたりのサイズです（全ユニットの合計ではありません）。
capture_name	パケット キャプチャの名前を指定します。複数のタイプのトラフィックをキャプチャするには、複数の **capture** ステートメントで同じ名前を使用します。**show capture** コマンドを使用してキャプチャのコンフィギュレーションを表示すると、すべてのオプションが 1 行にまとめられます。
circular-buffer	（任意）バッファがいっぱいになったとき、バッファを先頭から上書きします。
cp-cluster	（任意）クラスタ インターフェイスで制御パケットをキャプチャします。
ethernet-type *type*	（任意）キャプチャするイーサネット タイプを選択します。サポートされるイーサネット タイプには、8021Q、ARP、IP、IP6、LACP、PPPOED、PPPOES、RARP、および VLAN などがあります。802.1Q タイプと VLAN タイプでは例外が発生します。802.1Q タグは自動的にスキップされ、照合には内部イーサネット タイプが使用されます。
host *ip*	パケット送信先ホストの単一の IP アドレスを指定します。
include-decrypted	（オプション）ファイアウォールデバイスに入った時点で、通常のトラフィックと復号化されたトラフィックの両方を含む復号化された IPsec パケットをキャプチャします。
inline-tag *tag*	特定の SGT 値のタグを指定するか、または未指定のままにしてすべての SGT 値のタグ付きパケットをキャプチャします。
interface *interface_name*	パケット キャプチャを使用するインターフェイスの名前を設定します。**type asp-drop** を除いて、パケットをキャプチャするにはインターフェイスを設定する必要があります。複数の **capture** コマンドで同じ名前を使用して、複数のインターフェイスを設定できます。ASA のデータプレーン、管理プレーン、またはコントロール プレーンでパケットをキャプチャするには、**interface** キーワードを **asa_dataplane**、**asa_mgmt_plane**、または **cplane** とともにインターフェイス名として指定できます。インターフェイス名として **cluster** を指定すると、クラスタ制御リンク インターフェイスでトラフィックをキャプチャできます。キャプチャのタイプとして **lacp** が設定されている場合は、インターフェイス名は物理名です。
ikev1 または **ikev2**	IKEv1 または IKEv2 プロトコル情報だけをキャプチャします。

isakmp	(オプション)VPN 接続の ISAKMP トラフィックをキャプチャします。ISAKMP サブシステムは、上位層プロトコルにアクセスできません。このキャプチャは、PCAP パーサーを満足させるために物理、IP、および UDP の各レイヤを 1 つにまとめた疑似キャプチャです。このピア アドレスは、SA 交換から取得され、IP レイヤに保存されます。
lacp	(オプション)LACP トラフィックをキャプチャします。設定されている場合は、インターフェイス名は物理インターフェイス名です。
mask	IP アドレスのサブネット マスク。ネットワーク マスクを指定する場合に使用する方式は、Cisco IOS ソフトウェア **access-list** コマンドの方式と異なります。ASA では、ネットワーク マスク(たとえば、Class C マスクの 255.255.255.0)が使用されます。Cisco IOS マスクでは、ワイルドカード ビット(たとえば、0.0.0.255)が使用されます。
match *protocol*	5 タプルが一致するパケットを指定し、キャプチャされるこれらのパケットのフィルタリングを許可します。1 行に最大 3 回このキーワードを使用できます。
operator	(任意)送信元または宛先で使用されるポート番号を照合します。使用できる演算子は、次のとおりです。 • **lt**:より小さい • **gt**:より大きい • **eq**:等しい • **neq**:等しくない • **range**:範囲
packet-length *bytes*	(任意)キャプチャ バッファに保存する各パケットの最大バイト数を設定します。
persit	(オプション)クラスタユニットで永続的なパケットをキャプチャします。
port	(任意)プロトコルを **tcp** または **udp** に設定する場合、TCP ポートまたは UDP ポートの番号(整数)か名前を指定します。
raw-data	(任意)着信パケットおよび発信パケットを 1 つ以上のインターフェイスでキャプチャします。
real-time	キャプチャしたパケットをリアルタイムで継続的に表示します。リアルタイム パケット キャプチャを終了するには、**Ctrl + c** を入力します。キャプチャを完全に削除するには、このコマンドの **no** 形式を使用します。このオプションは、**raw-data** キャプチャおよび **asp-drop** キャプチャにだけ適用されます。このオプションは、**cluster exec capture** コマンドを使用するときはサポートされません。
reinject-hide	(オプション)再注入されたパケットがキャプチャされないことを指定します。クラスタリング環境でだけ適用されます。
stop	(任意)手動でキャプチャを削除せずに停止します。キャプチャを開始するには、このコマンドの **no** 形式を使用します。
tls-proxy	(オプション)復号化された着信データおよび発信データを 1 つ以上のインターフェイス上の TLS プロキシからキャプチャします。
trace *trace_count*	(任意)パケット トレース情報、およびキャプチャするパケット数をキャプチャします。このオプションをアクセス リストとともに使用すると、トレース パケットがデータ パスに挿入されるので、パケットが想定どおりに処理されているかどうかを判別できます。
type	(任意)キャプチャされるデータのタイプを指定します。

user *webvpn-user*	(任意)WebVPN キャプチャのユーザ名を指定します。
webvpn	(任意)特定の WebVPN 接続の WebVPN データをキャプチャします。

デフォルト

デフォルトの設定は次のとおりです。

- デフォルトの **type** は **raw-data** です。
- デフォルトの**buffer** *size* は 512 KB です。
- デフォルトのイーサネット タイプは IP パケットです。
- デフォルトの **packet-length** は 1518 バイトです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
6.2(1)	このコマンドが追加されました。
7.0(1)	キーワード **type asp-drop**、**type isakmp**、**type raw-data**、および **type webvpn** を含むように変更されました。
7.0(8)	ASA がドロップするパケットをすべてキャプチャするように、**all** オプションが追加されました。
7.2(1)	オプション **trace** *trace_count*、**match** *prot*、**real-time**、**host** *ip*、**any**、*mask*、および *operator* を含むように変更されました。
8.0(2)	キャプチャした内容にパスを更新するように変更されました。
8.4(1)	新しい **type** キーワードの **ikev1** と **ikev2** が追加されました。
8.4(2)	IDS の出力に追加の詳細が追加されました。
8.4(4.1)	バックプレーン経由の ASA CX モジュールへのトラフィックをサポートするために **asa_dataplane** オプションが追加されました。
9.0(1)	**cluster**、**cluster exec**、および **reinject-hide** キーワードが追加されました。新しい **type** オプションの **lacp** が追加されました。ISAKMP についてマルチ コンテキスト モードのサポートが追加されました。
9.1(3)	ASA CX バックプレーンでキャプチャされたパケットのフィルタリングが **asa_dataplane** オプションによってサポートされるようになりました。
9.2(1)	ASA FirePOWER モジュールをサポートするように **asa_dataplane** オプションが拡張されました。
9.3(1)	SGT およびイーサネット タギング機能をサポートするために **inline-tag** *tag* のキーワードと引数のペアが追加されました。

リリース	変更内容
9.6(2)	**type asp-drop** のパケット キャプチャは、ACL と一致フィルタリングをサポートします。
9.7(1)	パケット キャプチャを手動で停止したり開始したりするために、**stop** キーワードを追加しました。
9.8(1)	このコマンドは、ボックス クラッシュ時にすべてのアクティブなキャプチャの内容をフラッシュまたはディスク上のファイルに保存するように更新されました。
9.9(1)	クラスタリングの永続的トレースおよび復号化されたパケットのキャプチャがサポートされるようになりました。新しいオプションとして **persist** および **include-decrypted** が追加されました。 また、IPX は 3 つの異なるイーサネット タイプに対応するため、**ethernet-type ipx** が削除されました。代わりに、キャプチャする IPX タイプの 16 進数値を使用します。
9.10(1)	**match** オプションで IPv4 と IPv6 のネットワーク トラフィックをそれぞれキャプチャするために、**any4** および **any6** キーワードを追加しました。
9.12(1)	クラスタ インターフェイスで制御パケットをキャプチャするために、**cp-cluster** を追加しました。

使用上のガイドライン

パケット キャプチャは、接続の問題のトラブルシューティングまたは不審なアクティビティのモニタリングを行うときに役立ちます。複数のキャプチャを作成できます。**capture** コマンドは、実行コンフィギュレーションには保存されません。また、フェールオーバー時にスタンバイ ユニットにコピーされません。

ASA では、通過するすべての IP トラフィックを追跡でき、すべての管理トラフィック（SSH トラフィック、Telnet トラフィックなど）を含む、着信するすべての IP トラフィックをキャプチャできます。

ASA のアーキテクチャは、パケット処理のための異なる 3 セットのプロセッサで構成されています。このアーキテクチャに起因して、キャプチャ機能の性能に一定の制限が加わります。通常は、ASA のパケット転送機能の大部分が 2 個のフロントエンド ネットワーク プロセッサで処理され、アプリケーション インスペクションが必要なパケットに限り、コントロール プレーン汎用プロセッサに送信されます。パケットがセッション管理パス ネットワーク プロセッサに送信されるのは、高速パス プロセッサで処理されないセッションがある場合だけです。

ASA によって転送またはドロップされるすべてのパケットがこの 2 つのフロントエンド ネットワーク プロセッサを通るため、パケット キャプチャ機能はこれらのネットワーク プロセッサに実装されています。したがって、該当するトラフィック インターフェイス用の適切なキャプチャが設定されていれば、ASA を通過するすべてのパケットをこれらのフロントエンド プロセッサでキャプチャできます。入力側では、ASA インターフェイスに到着した時点でパケットがキャプチャされ、出力側では、ネットワークに送信される直前でパケットがキャプチャされます。

（注） WebVPN キャプチャをイネーブルにすると、ASA のパフォーマンスに影響します。トラブルシューティングに必要なキャプチャ ファイルを生成した後、必ずキャプチャをディセーブルにしてください。

キャプチャの保存

ASA 上のすべてのアクティブなキャプチャの内容は、ボックスがクラッシュしたときに保存されます。

トラブルシューティング プロセスの一部としてキャプチャをアクティブ化する場合は、次の点に注意する必要があります。

- 使用するキャプチャ バッファのサイズ、およびフラッシュまたはディスクに十分なスペースがあるかどうか。
- キャプチャされたパケットがクラッシュ前の最新のものになるように、キャプチャ バッファはすべての使用例で円形としてマークする必要があります。

アクティブなキャプチャの内容を保存するファイルの名前は、次の形式となります。

[<context_name>.]<capture_name>.pcap

context_name は、マルチコンテキスト モードでキャプチャがアクティブになっているユーザ コンテキストの名前を示します。シングル コンテキスト モードでは、*context_name* は適用されません。

capture_name は、アクティブ化されたキャプチャの名前を示します。

キャプチャの保存は、コンソールまたはクラッシュ ダンプの前に行われます。これにより、33 MB のキャプチャ バッファでクラッシュのダウンタイムが約 5 秒増加します。キャプチャしたコンテンツをファイルにコピーするのは簡単なプロセスなので、ネストされたクラッシュのリスクは最小限です。

キャプチャの表示

パケット キャプチャを表示するには、**show capture** *name* コマンドを使用します。キャプチャをファイルに保存するには、**copy capture** コマンドを使用します。パケット キャプチャ情報を Web ブラウザで表示するには、**https://***ASA-ip-address***/***admin***/capture/***capture_name***[/pcap]** コマンドを使用します。オプションの **pcap** キーワードを指定すると、libpcap 形式のファイルが Web ブラウザにダウンロードされ、Web ブラウザを使用してこのファイルを保存できます（libcap ファイルは、TCPDUMP または Ethereal で表示できます）。

バッファの内容を TFTP サーバに ASCII 形式でコピーする場合、パケットの詳細および 16 進ダンプは表示されず、ヘッダーだけが表示されます。詳細および 16 進ダンプを表示するには、バッファを PCAP 形式で転送し、TCPDUMP または Ethereal で読み取る必要があります。

キャプチャの停止と開始

パケットをバッファから削除することなく、パケット キャプチャを停止することができます。キャプチャ停止のステータスが表示されます。キャプチャされたパケットは、バッファ内に保持されます。

パケット キャプチャを手動で停止するには、次のコマンドを使用します。

capture *name* **stop**

パケット キャプチャを開始するには、次のコマンドを使用します。

no capture *name* **stop**

キャプチャの削除

キーワードを指定せずに **no capture** を入力すると、キャプチャが削除されます。キャプチャを保持するには、**access-list** または **interface** キーワードを指定します。キャプチャは指定した ACL またはインターフェイスから分離されて保持されます。

リアルタイム操作

リアルタイム表示の進行中には、キャプチャに関するあらゆる操作を実行できません。低速のコンソール接続で **real-time** キーワードを使用すると、パフォーマンスが考慮されて、多数のパケットが非表示になる場合があります。バッファの固定の制限は、1000 パケットです。バッファがいっぱいになると、カウンタはキャプチャしたパケットで維持されます。別のセッションを開く場合、**no capture real-time** コマンドを入力して、リアルタイム表示をディセーブルにできます。

クラスタ

capture コマンドの前に **cluster exec** を指定すると、あるユニットで **capture** コマンドを発行し、そのコマンドを他のすべてのユニットで同時に実行できます。クラスタ全体のキャプチャを実行した後、同じキャプチャ ファイルをクラスタ内のすべてのユニットから同時に TFTP サーバにコピーするには、マスター ユニットで **cluster exec copy** コマンドを入力します。

```
ciscoasa# cluster exec capture capture_name arguments
ciscoasa# cluster exec copy /pcap capture: cap_name tftp://location/path/filename.pcap
```

複数の PCAP ファイル（各ユニットから 1 つずつ）が TFTP サーバにコピーされます。宛先のキャプチャ ファイル名には自動的にユニット名が付加され、filename_A.pcap、filename_B.pcap などとなります。この例では、A と B がクラスタ ユニット名です。

トレースをクラスタ ユニットでキャプチャする場合、トレースは、バッファから手動でクリアされるまで、各クラスタ ノードに永続します。復号化された IPsec パケットは、ASA に入るとキャプチャされます。キャプチャされたパケットには、通常のトラフィックとカプセル化解除されたトラフィックの両方が含まれます。

（注） ファイル名の末尾にユニット名を追加すると、別の宛先名が生成されます。

制限事項

次に、キャプチャ機能の制限の一部を示します。制限の大部分は、ASA のアーキテクチャが本質的に分散型であることと、ASA で使用するハードウェア アクセラレータを原因としています。

- コンテキスト内のクラスタ制御リンクでキャプチャを設定できます。この場合、そのクラスタ制御リンクで送信されるコンテキストに関連付けられているパケットだけがキャプチャされます。
- 共有 VLAN には、次のガイドラインが適用されます。
  - VLAN ごとに設定できるキャプチャは 1 つだけです。共有 VLAN の複数のコンテキストでキャプチャを設定した場合は、最後に設定したキャプチャだけが使用されます。
  - 最後に設定した（アクティブ）キャプチャを削除した場合は、別のコンテキストで事前に設定したキャプチャがあっても、アクティブになるキャプチャはありません。キャプチャをアクティブにするには、キャプチャを削除して追加し直す必要があります。
  - キャプチャを指定したインターフェイス（キャプチャ アクセス リストと一致するインターフェイス）に着信するすべてのトラフィックがキャプチャされます。これには、共有 VLAN の他のコンテキストへのトラフィックが含まれます。
  - したがって、ある VLAN のコンテキスト A でのキャプチャをイネーブルにしたときに、その VLAN がコンテキスト B でも使用される場合は、コンテキスト A とコンテキスト B の両方の入力トラフィックがキャプチャされます。
- 出力トラフィックの場合は、アクティブ キャプチャのあるコンテキストのトラフィックだけがキャプチャされます。唯一の例外は、ICMP 検査をイネーブルにしない（したがって、ICMP トラフィックのセッションが高速パスにない）場合です。この場合は、共有 VLAN のすべてのコンテキストで入力と出力の ICMP トラフィックがキャプチャされます。

- キャプチャを設定する場合、通常は、キャプチャする必要のあるトラフィックを照合するアクセス リストを設定します。トラフィック パターンを照合するアクセス リストの設定が終われば、キャプチャを定義し、キャプチャを設定するインターフェイスとともに、このアクセス リストをキャプチャに関連付ける必要があります。キャプチャは、アクセス リストおよびインターフェイスと、IPv4 トラフィックをキャプチャするためのキャプチャを関連付けた場合に限り機能することに注意してください。IPv6 トラフィックの場合、アクセス リストは不要です。
- ASA CX モジュール トラフィックの場合、キャプチャされたパケットに含まれている追加 AFBP ヘッダーを、PCAP ビューアが認識しないことがあります。このようなパケットを表示するには、適切なプラグインを使用してください。
- インライン SGT タグ付きパケットの場合、キャプチャされたパケットに含まれている追加 CMD ヘッダーを、PCAP ビューアが認識しないことがあります。
- 受信側インターフェイスがないためグローバル インターフェイスがない場合、バックプレーン上で送信されるパケットは、システム コンテキストの制御パケットとして扱われます。これらのパケットはアクセス リスト チェックをバイパスし、常にキャプチャされます。この動作は、シングル モードとマルチ コンテキスト モードの両方に適用されます。
- 特定の asp-drop をキャプチャする場合に適切な理由を表示するには、**show capture** コマンドを使用します。ただし、**show capture** コマンドは、すべての asp-drop をキャプチャする場合は適切な理由を表示しません。

例

パケットをキャプチャするには、次のコマンドを入力します。

```
ciscoasa# capture captest interface inside
ciscoasa# capture captest interface outside
```

Web ブラウザで、発行した「captest」という名前の **capture** コマンドの内容を表示できます。次の場所にあります。

```
https://171.69.38.95/admin/capture/captest
```

libpcap ファイル（Web ブラウザが使用）をローカル マシンにダウンロードするには、次のコマンドを入力します。

```
https://171.69.38.95/capture/http/pcap
```

次に、ASA ボックスがクラッシュしたときにシングルモードでパケットをキャプチャする例を示します。

```
ciscoasa# capture 123 interface inside
```

キャプチャ「123」のコンテンツは、*123.pcap* ファイルとして保存されます。

次に、ASA ボックスがクラッシュしたときにマルチモードでパケットをキャプチャする例を示します。

```
ciscoasa# capture 456 interface inside
```

「管理」コンテキスト内のキャプチャ「456」のコンテンツは、*admin.456.pcap* ファイルとして保存されます。

次に、外部ホスト 171.71.69.234 から内部 HTTP サーバにトラフィックがキャプチャされる例を示します。

```
ciscoasa# access-list http permit tcp host 10.120.56.15 eq http host 171.71.69.234
ciscoasa# access-list http permit tcp host 171.71.69.234 host 10.120.56.15 eq http
ciscoasa# capture http access-list http packet-length 74 interface inside
```

次に、ARP パケットをキャプチャする例を示します。

```
ciscoasa# capture arp ethernet-type arp interface outside
```

次に、5 つのトレース パケットをデータ ストリームに挿入する例を示します。ここで、*access-list 101* は、TCP プロトコル FTP と一致するトラフィックを定義します。

```
hostname# capture ftptrace interface outside access-list 101 trace 5
```

トレースされたパケットおよびパケット処理に関する情報をわかりやすく表示するには、**show capture ftptrace** コマンドを使用します。

次の例では、キャプチャされたパケットをリアルタイムで表示する方法を示します。

```
ciscoasa# capture test interface outside real-time
Warning: Using this option with a slow console connection may result in an excess amount
of non-displayed packets due to performance limitations.
Use ctrl-c to terminate real-time capture.

10 packets displayed
12 packets not displayed due to performance limitations
```

次の例では、キャプチャする必要のある IPv4 トラフィックを照合する拡張アクセス リストを設定する方法を示します。

```
ciscoasa (config)# access-list capture extended permit ip any any
```

次の例では、キャプチャを設定する方法を示します。

```
ciscoasa (config)# capture name access-list acl_name interface interface_name
```

デフォルトでは、キャプチャを設定すると、512 KB のサイズのリニア キャプチャ バッファが作成されます。オプションで循環バッファを設定できます。デフォルトでは、パケットの 68 バイトだけがバッファにキャプチャされます。オプションでこの値を変更できます。

次に、事前に設定されたキャプチャ アクセス リストを使用し、outside インターフェイスに適用される「ip-capture」というキャプチャを作成する例を示します。

```
ciscoasa (config)# capture ip-capture access-list capture interface outside
```

次の例では、キャプチャを表示する方法を示します。

```
ciscoasa (config)# show capture name
```

次の例では、キャプチャを終了する一方でバッファを保持する方法を示します。

```
ciscoasa (config)# no capture name access-list acl_name interface interface_name
```

次の例では、キャプチャを終了し、バッファを削除する方法を示します。

```
ciscoasa (config)# no capture name
```

次の例では、シングル モードでバックプレーンでキャプチャされたトラフィックをフィルタリングする方法を示します。

```
ciscoasa# capture x interface asa_dataplane access-list any4
ciscoasa# capture y interface asa_dataplane match ip any any
```

（注） 制御パケットは、アクセス リストを指定した場合にも、シングル モードでキャプチャされます。

次の例では、マルチ コンテキスト モードでバックプレーンでキャプチャされたトラフィックをフィルタリングする方法を示します。

ユーザ コンテキストでの使用方法:

```
ciscoasa (contextA)# capture x interface asa_dataplane access-list any4
ciscoasa (contextA)# capture y interface asa_dataplane match ip any any
```

システム コンテキストでの使用方法:

```
ciscoasa# capture z interface asa_dataplane
```

(注) マルチ コンテキスト モードでは、**access-list** オプションと **match** オプションはシステム コンテキストで使用できません。

クラスタリングでのキャプチャ

クラスタ内のすべてのユニットでのキャプチャをイネーブルにするには、これらの各コマンドの前に **cluster exec** キーワードを追加します。

次の例では、クラスタリング環境の LACP キャプチャを作成する方法を示します。

```
ciscoasa (config)# capture lacp type lacp interface gigabitEthernet0/0
```

次の例では、クラスタリング リンクでの制御パス パケットのキャプチャを作成する方法を示します。

```
ciscoasa (config)# cap cp interface cluster match udp any eq 49495 any
ciscoasa (config)# cap cp interface cluster match udp any any eq 49495
```

次の例では、クラスタリング リンクでのデータ パス パケットのキャプチャを作成する方法を示します。

```
ciscoasa (config)# access-list cc1 extended permit udp any any eq 4193
ciscoasa (config)# access-list cc1 extended permit udp any eq 4193 any
ciscoasa (config)# capture dp interface cluster access-list cc1
```

次の例では、クラスタを通過するデータ パス トラフィックをキャプチャする方法を示します。

```
ciscoasa (config)# capture abc interface inside match tcp host 1.1.1.1 host 2.2.2.2 eq www
ciscoasa (config)# capture abc interface inside match dup host 1.1.1.1 any
ciscoasa (config)# capture abc interface inside access-list xxx
```

次の例では、指定した実際の発信元から実際の宛先へのフローに対する論理アップデート メッセージをキャプチャし、指定した実際の発信元から実際の宛先へ CCL を介して転送されるパケットをキャプチャする方法を示します。

```
ciscoasa (config)# access-list dp permit real src real dst
```

次の例では、特定タイプのデータ プレーン メッセージ(たとえば ICMP エコー要求/応答)のうち、ある ASA から別の ASA に転送されたものを、メッセージ タイプに応じた **match** キーワードまたはアクセス リストを使用してキャプチャする方法を示します。

```
ciscoasa (config)# capture capture_name interface cluster access-list match icmp any any
```

次の例では、クラスタリング環境内のクラスタ制御リンク上でアクセス リスト 103 を使用してキャプチャを作成する方法を示します。

```
ciscoasa (config)# access-list 103 permit ip A B
ciscoasa (config)# capture example1 interface cluster
```

前の例で、A と B が CCL インターフェイスの IP アドレスである場合は、この 2 つのユニット間で送信されるパケットだけがキャプチャされます。

A および B が、デバイスを通過するトラフィックの IP アドレスである場合は、次のことが当てはまります。

- 転送されたパケットは、通常どおりにキャプチャされます。ただし、送信元および宛先の IP アドレスがアクセス リストに一致することが条件です。
- データ パス ロジック アップデート メッセージがキャプチャされるのは、そのメッセージが A と B の間のフローに対するものであるか、特定のアクセス リスト（たとえば、access-list 103）に対するものである場合です。埋め込まれたフローの 5 タプルが一致するものがキャプチャされます。
- UDP パケットの送信元と宛先のアドレスは CCL のアドレスですが、このパケットがフローを更新するためのものであり、そのフローにアドレス A および B が関連付けられている場合は、このパケットもキャプチャされます。つまり、パケットに埋め込まれているアドレス A および B が一致している限り、そのパケットもキャプチャされます。

次の例では、persistent オプションを使用してキャプチャを設定する方法を示します。

```
cluster2-asa5585a(config)# cluster exec capture test interface outside trace persist
  a(LOCAL):*******************************************************
  cluster2-asa5585a(config)#
```

これで、トラフィックを送信できるようになりました。

```
cluster2-asa5585a(config)# cluster exec show packet-tracer
  a(LOCAL):*******************************************************
  tracer 29/25 (allocate/freed), handle 29/25 (allocated/freed), error 0
  =======  Tracer origin-id a:23, hop 0 =======
  packet-id: Protocol: 0 src-port: 0 dst-port: 0

  Phase: 1
  Type: CAPTURE
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  MAC Access list

  Phase: 2
  Type: ACCESS-LIST
  Subtype:
  Result: DROP
  Config:
  Implicit Rule
  Additional Information:
  MAC Access list

  Result:
  input-interface: outside
  input-status: up
  input-line-status: up
  Action: drop
  Drop-reason: (l2_acl) FP L2 rule drop
```

次の例では、メモリの一部を開放するためには、キャプチャされた永続的なトレースをボックスからクリアする必要があることが示されています。

```
ciscoasa# cluster exec clear packet-trace
```

次に、include-decrypted オプションを使用してキャプチャを設定する例を示します。

```
cluster2-asa5585a(config)# cluster exec show capture
  a(LOCAL):**************************************************************
  capture in type raw-data trace interface outside include-decrypted [Capturing – 588
bytes]
  capture out type raw-data trace interface outside include-decrypted [Capturing - 420
bytes]
  cluster2-asa5585a(config)#
```

これで、IPSec トンネルを介して ICMP トラフィックを送信できるようになりました。説明したとおり、キャプチャ コマンドは復号化された ICMP パケットを取得します。

```
cluster2-asa5585a(config)# cluster exec show capture in | i icmp
  a(LOCAL):**************************************************************
  b:**********************************************************************
  cluster2-asa5585a(config)# cluster exec show capture out | i icmp
  a(LOCAL):**************************************************************
  b:**********************************************************************
  cluster2-asa5585a(config)# cluster exec show capture in | i icmp
  a(LOCAL):**************************************************************
     8: 07:22:57.065014       802.1Q vlan#212 P0 211.1.1.1 > 213.1.1.2: icmp: echo request
  b:**********************************************************************
  cluster2-asa5585a(config)# cluster exec show capture out | i icmp
  a(LOCAL):**************************************************************
    10: 07:22:57.068004       802.1Q vlan#214 P0 213.1.1.2 > 211.1.1.1: icmp: echo reply
  b:**********************************************************************
  cluster2-asa5585a(config)#
```

関連コマンド

コマンド	説明
clear capture	キャプチャ バッファをクリアします。
copy capture	キャプチャ ファイルをサーバにコピーします。
show capture	オプションが指定されていない場合は、キャプチャ コンフィギュレーションを表示します。

cd

現在の作業ディレクトリから指定したディレクトリに変更するには、特権 EXEC モードで **cd** コマンドを使用します。

cd [**disk0: | disk1: | flash:**] [*path*]

構文の説明

disk0:	内部フラッシュ メモリを指定し、続けてコロンを入力します。
disk1:	取り外し可能な外部フラッシュ メモリ カードを指定し、続けてコロンを入力します。
flash:	内部フラッシュ メモリを指定し、続けてコロンを入力します。ASA 5500 シリーズでは、**flash** キーワードは **disk0** のエイリアスです。
path	（任意）移動先ディレクトリの絶対パス。

デフォルト

ディレクトリを指定しないと、ルート ディレクトリに移動します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、「config」ディレクトリに変更する例を示します。

```
ciscoasa# cd flash:/config/
```

関連コマンド

コマンド	説明
pwd	現在の作業ディレクトリを表示します。

cdp-url

ローカル CA によって発行された証明書に含める CDP を指定するには、CA サーバ コンフィギュレーション モードで **cdp-url** コマンドを使用します。デフォルトの CDP に戻すには、このコマンドの **no** 形式を使用します。

[no] cdp-url *url*

構文の説明

url	ローカル CA によって発行された証明書の失効ステータスを検証側が取得する URL を指定します。URL は、英数字 500 文字未満である必要があります。

デフォルト

デフォルトの CDP URL は、ローカル CA が含まれる ASA の CDP URL です。デフォルトの URL の形式は、http://hostname.domain/+CSCOCA+/asa_ca.crl です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

CDP は、発行された証明書に含めることができる拡張であり、証明書の失効ステータスを検証側が取得できる場所を指定できます。一度に設定できる CDP は 1 つだけです。

(注) CDP URL が指定された場合、管理者はその場所から現在の CRL にアクセスできるように管理する必要があります。

例

次に、ローカル CA サーバが発行した証明書に対して、10.10.10.12 の CDP を設定する例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# cdp-url http://10.10.10.12/ca/crl
ciscoasa(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
crypto ca server crl issue	CRL を強制的に発行します。
crypto ca server revoke	証明書データベースおよび CRL で、ローカル CA サーバによって発行された証明書を失効とマークします。
crypto ca server unrevoke	ローカル CA サーバによって発行され、以前に失効した証明書の失効を取り消します。
lifetime crl	証明書失効リストのライフタイムを指定します。

証明書

指定した証明書を追加するには、crypto ca 証明書チェーン コンフィギュレーション モードで **certificate** コマンドを使用します。証明書を削除するには、このコマンドの **no** 形式を使用します。

certificate [**ca** | **ra-encrypt** | **ra-sign** | **ra-general**] *certificate-serial-number*

no certificate *certificate-serial-number*

構文の説明

ca	証明書が CA 発行の証明書であることを示します。
certificate-serial-number	証明書のシリアル番号を 16 進形式で指定し、末尾に「quit」という語を指定します。
ra-encrypt	証明書が SCEP で使用される RA キー暗号化証明書であることを示します。
ra-general	証明書が SCEP メッセージングのデジタル署名およびキー暗号化に使用される RA 証明書であることを示します。
ra-sign	証明書が SCEP メッセージングで使用される RA デジタル署名証明書であることを示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クリプト CA 証明書チェーン コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを発行する場合、ASA は、コマンドに含まれているデータを 16 進形式の証明書として解釈します。**quit** ストリングは、証明書の末尾を示します。

CA は、メッセージ暗号化のためのセキュリティ クレデンシャルおよび公開キーの発行および管理を行うネットワーク内の組織です。公開キー インフラストラクチャの一部である CA は、RA と連携して、デジタル証明書の要求者から取得した情報を確認します。RA が要求者の情報を確認すると、CA から証明書が発行されます。

例

次に、シリアル番号 29573D5FF010FE25B45 の CA 証明書を追加する例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crypto ca certificate chain central
ciscoasa(ca-cert-chain)# certificate ca 29573D5FF010FE25B45
  30820345 308202EF A0030201 02021029 572A3FF2 96EF854F D0D6732F E25B4530
  0D06092A 864886F7 0D010105 05003081 8F311630 1406092A 864886F7 0D010901
  16076140 622E636F 6D310B30 09060355 04061302 55533116 30140603 55040813
  0D6D6173 73616368 75736574 74733111 300F0603 55040713 08667261 6E6B6C69
  6E310E30 0C060355 040A1305 63697363 6F310F30 0D060355 040B1306 726F6F74
  6F75311C 301A0603 55040313 136D732D 726F6F74 2D736861 2D30362D 32303031
  301E170D 30313036 32363134 31313430 5A170D32 32303630 34313430 3133305A
  30818F31 16301406 092A8648 86F70D01 09011607 6140622E 636F6D31 0B300906
  03550406 13025553 31163014 06035504 08130D6D 61737361 63687573 65747473
  3111300F 06035504 07130866 72616E6B 6C696E31 0E300C06 0355040A 13056369
  73636F31 0F300D06 0355040B 1306726F 6F746F75 311C301A 06035504 0313136D
  732D726F 6F742D73 68612D30 362D3230 3031305C 300D0609 2A864886 F70D0101
  01050003 4B003048 024100AA 3EB9859B 8670A6FB 5E7D2223 5C11BCFE 48E6D3A8
  181643ED CF7E75EE E77D83DF 26E51876 97D8281E 9F58E4B0 353FDA41 29FC791B
  1E14219C 847D19F4 A51B7B02 03010001 A3820123 3082011F 300B0603 551D0F04
  04030201 C6300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604
  14E0D412 3ACC96C2 FBF651F3 3F66C0CE A62AB63B 323081CD 0603551D 1F0481C5
  3081C230 3EA03CA0 3A86386C 6461703A 2F2F7732 6B616476 616E6365 64737276
  2F436572 74456E72 6F6C6C2F 6D732D72 6F6F742D 7368612D 30362D32 3030312E
  63726C30 3EA03CA0 3A863868 7474703A 2F2F7732 6B616476 616E6365 64737276
  2F436572 74456E72 6F6C6C2F 6D732D72 6F6F742D 7368612D 30362D32 3030312E
  63726C30 40A03EA0 3C863A66 696C653A 2F2F5C5C 77326B61 6476616E 63656473
  72765C43 65727445 6E726F6C 6C5C6D73 2D726F6F 742D7368 612D3036 2D323030
  312E6372 6C301006 092B0601 04018237 15010403 02010130 0D06092A 864886F7
  0D010105 05000341 0056221E 03F377B9 E6900BF7 BCB3568E ADBA146F 3B8A71F3
  DF9EB96C BB1873B2 B6268B7C 0229D8D0 FFB40433 C8B3CB41 0E4D212B 2AEECD77
  BEA3C1FE 5EE2AB6D 91
  quit
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto map	クリプト マップの設定内容を表示します。
crypto ca certificate chain	証明書クリプト CA 証明書チェーン モードを開始します。
crypto ca trustpoint	CA トラストポイント モードを開始します。
show running-config crypto map	すべてのクリプト マップのすべてのコンフィギュレーションを表示します。

certificate-group-map

証明書マップのルール エントリをトンネル グループに関連付けるには、webvpn コンフィギュレーション モードで **certificate-group-map** コマンドを使用します。現在のトンネル グループ マップの関連付けをクリアするには、このコマンドの **no** 形式を使用します。

certificate-group-map *certificate_map_name index tunnel_group_name*

no certificate-group-map

構文の説明

certificate_map_name	証明書マップの名前。
index	証明書マップのマップ エントリの数値識別子。index の値の範囲は、1 ～ 65535 です。
tunnel_group_name	マップ エントリが証明書と一致する場合に選択されるトンネル グループの名前。*tunnel-group name* はすでに存在している必要があります。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

certificate-group-map コマンドが有効な状態で、WebVPN クライアントから受信した証明書がマップ エントリに対応する場合、結果として得られるトンネル グループは、接続に関連付けられ、ユーザが選択したトンネル グループを上書きします。

certificate-group-map コマンドの複数のインスタンスを使用すると、複数のマッピングが可能です。

例

次に、tgl という名前のトンネル グループにルール 6 を関連付ける例を示します。

```
ciscoasa(config)# webvpn
hostname(config-webvpn)# certificate-group-map map1 6 tg1
hostname(config-webvpn)#
```

関連コマンド

コマンド	説明
crypto ca certificate map	証明書の発行者名とサブジェクト名の識別名(DN)に基づいて、ルールを設定するために CA 証明書マップ コンフィギュレーション モードを開始します。
tunnel-group-map	証明書ベースの IKE セッションをトンネル グループにマップするときのポリシーおよびルールを設定します。

chain

証明書チェーンの送信をイネーブルにするには、トンネル グループ ipsec 属性コンフィギュレーション モードで **chain** コマンドを使用します。このコマンドをデフォルトに戻すには、このコマンドの **no** 形式を使用します。

chain

no chain

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドのデフォルト設定は、ディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
トンネル グループ ipsec 属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

この属性は、すべての IPsec トンネル グループ タイプに適用できます。

このコマンドの入力には、ルート証明書および送信内のすべての下位 CA 証明書が含まれます。

例

次に、トンネル グループ ipsec 属性コンフィギュレーション モードを開始し、IPSec LAN-to-LAN トンネル グループのチェーンを IP アドレス 209.165.200.225 で送信することをイネーブルにする例を示します。このアクションには、ルート証明書およびすべての下位 CA 証明書が含まれます。

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# chain
ciscoasa(config-tunnel-ipsec)#
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	現在のトンネル グループ コンフィギュレーションを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ ipsec 属性を設定します。

change-password

ユーザが自分のアカウント パスワードを変更できるようにするには、特権 EXEC モードで **change-password** コマンドを使用します。

change-password [**/silent**] [**old-password** *old-password* [**new-password** *new-password*]]

構文の説明

new-password *new-password*	新しいパスワードを指定します。
old-password *old-password*	ユーザを再認証します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	—	—	• 対応
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.4(4.1)	このコマンドが追加されました。

使用上のガイドライン

ユーザがパスワードを省略すると、ASA から入力を求めるプロンプトが表示されます。ユーザが **change-password** コマンドを入力すると、実行コンフィギュレーションを保存するように求められます。ユーザが正常にパスワードを変更した後、ユーザに設定変更を保存するように再通知するメッセージが表示されます。

例

次に、ユーザ アカウントのパスワードを変更する例を示します。

```
ciscoasa# change-password old-password myoldpassword000 new password mynewpassword123
```

関連コマンド

コマンド	説明
show run password-policy	現在のコンテキストのパスワード ポリシーを表示します。
clear configure password-policy	現在のコンテキストのパスワード ポリシーをデフォルト値にリセットします。
clear configure username	ユーザ アカウントからユーザ名を削除します。

changeto

セキュリティ コンテキストとシステムの間で切り替えを行うには、特権 EXEC モードで **changeto** コマンドを使用します。

changeto {**system** | **context** *name*}

構文の説明

context *name*	指定した名前のコンテキストに切り替えます。
system	システム実行スペースに切り替えます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	—	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

システム実行スペースまたは管理コンテキストにログインしている場合、コンテキスト間で切り替えを行うことができ、各コンテキスト内でコンフィギュレーションおよびタスクのモニタリングを実行できます。コンフィギュレーション モードで編集したか、あるいは **copy** または **write** コマンドで使用した「実行」コンフィギュレーションは、その時点での実行スペースによって異なります。現在の実行スペースがシステム実行スペースの場合、実行コンフィギュレーションは、システム コンフィギュレーションのみで構成されます。コンテキスト実行スペースの場合、実行コンフィギュレーションは、そのコンテキストのみで構成されます。たとえば、**show running-config** コマンドを入力しても、すべての実行コンフィギュレーション（システムおよびすべてのコンテキスト）を表示することはできません。現在のコンフィギュレーションだけが表示されます。

例

次に、特権 EXEC モードでコンテキストとシステムの間で切り替えを行う例を示します。

```
ciscoasa/admin# changeto system
ciscoasa# changeto context customerA
ciscoasa/customerA#
```

次に、インターフェイス コンフィギュレーション モードでシステムと管理コンテキストの間で切り替えを行う例を示します。実行スペースを変更するときにコンフィギュレーション モードを開始している場合、モードは新しい実行スペースのグローバル コンフィギュレーション モードに変わります。

```
ciscoasa(config-if)# changeto context admin
ciscoasa/admin(config)#
```

関連コマンド

コマンド	説明
admin-context	コンテキストを管理コンテキストに設定します。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。
show context	コンテキストのリスト(システム実行スペース)または現在のコンテキストに関する情報を表示します。

channel-group

EtherChannel に物理インターフェイスを割り当てるには、インターフェイス コンフィギュレーション モードで **channel-group** コマンドを使用します。インターフェイスの割り当てを解除するには、このコマンドの **no** 形式を使用します。

channel-group *channel_id* **mode** {**active** | **passive** | **on**} [**vss-id** {**1** | **2**}]

no channel-group *channel_id*

構文の説明

channel_id	このインターフェイスに割り当てる EtherChannel を 1 ～ 48 の範囲で指定します。
vss-id {**1** | **2**}	（オプション）クラスタリングでは、VSS または vPC の 2 台のスイッチに ASA を接続する場合は、このインターフェイスをどのスイッチに接続するかを指定するために **vss-id** キーワードを設定します（1 または 2）。また、**port-channel span-cluster vss-load-balance** コマンドをポートチャネル インターフェイスに対して使用する必要があります。
mode {**active** | **passive** | **on**}	EtherChannel 内の各物理インターフェイスを次のように設定できます。 • アクティブ：Link Aggregation Control Protocol（LACP）アップデートを送受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。 • パッシブ：LACP アップデートを受信します。パッシブ EtherChannel は、アクティブ EtherChannel のみと接続を確立できます。 • オン：EtherChannel は常にオンであり、LACP は使用されません。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	ASA クラスタリングおよびスパンド EtherChannel をサポートするために **vss-id** キーワードが追加されました。

使用上のガイドライン

チャネル グループ 1 つにつき 8 個のインターフェイスをアクティブにすることができます。1 つのチャネル グループに最大 16 個のインターフェイスを割り当てることができます。アクティブにできるインターフェイスは 8 個のみですが、残りのインターフェイスはインターフェイスに障害が発生した場合のスタンバイ リンクとして動作できます。

チャネル グループのすべてのインターフェイスは、同じタイプと速度である必要があります。チャネル グループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。

このチャネル ID のポートチャネル インターフェイスがコンフィギュレーションにまだ存在しない場合、ポートチャネル インターフェイスが作成されます。

interface port-channel *channel_id*

リンク集約制御プロトコル（LACP）では、2 つのネットワーク デバイス間でリンク集約制御プロトコル データ ユニット（LACPDU）を交換することによって、インターフェイスが集約されます。LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバ インターフェイスの両端が正しいチャネル グループに接続されていることがチェックされます。「オン」モードではインターフェイスがダウンしたときにチャネル グループ内のスタンバイ インターフェイスを使用できず、接続とコンフィギュレーションはチェックされません。

ASA クラスタリング

1 つの ASA につき複数のインターフェイスを、スパンド EtherChannel に入れることができます。1 つの ASA につき複数のインターフェイスが特に役立つのは、VSS または vPC の両方のスイッチに接続するときです。ASA を VSS または vPC の 2 台のスイッチに接続する場合は、**vss-load-balance** キーワードを使用して VSS ロード バランシングをイネーブルにする必要があります。この機能を使用すると、ASA と VSS（または vPC）ペアとの間の物理リンク接続の負荷が確実に分散されます。ロード バランシングをイネーブルにする前に、各メンバー インターフェイスに対して **channel-group** コマンドの **vss-id** キーワードを設定する必要があります。

例

次に、チャネル グループ 1 にインターフェイスを割り当てる例を示します。

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/2
ciscoasa(config-if)# channel-group 1 mode passive
```

関連コマンド

コマンド	説明
interface port-channel	EtherChannel を設定します。
lacp max-bundle	チャネル グループで許可されるアクティブ インターフェイスの最大数を指定します。

コマンド	説明
lacp port-priority	チャネル グループの物理インターフェイスのプライオリティを設定します。
lacp system-priority	LACP システム プライオリティを設定します。
port-channel load-balance	ロード バランシング アルゴリズムを設定します。
port-channel min-bundle	ポートチャネル インターフェイスがアクティブになるために必要な、アクティブ インターフェイスの最小数を指定します。
show lacp	LACP 情報（トラフィック統計情報、システム ID、ネイバーの詳細など）が表示されます。
show port-channel	EtherChannel 情報が、詳細に 1 行のサマリー形式で表示されます。このコマンドは、ポートとポートチャネルの情報も表示します。
show port-channel load-balance	ポートチャネル負荷分散情報が、指定のパラメータ セットに対するハッシュ結果および選択されたメンバー インターフェイスとともに表示されます。

character-encoding

WebVPN ポータル ページでグローバルな文字エンコーディングを指定するには、webvpn コンフィギュレーション モードで **character-encoding** コマンドを使用します。character-encoding 属性の値を削除するには、このコマンドの **no** 形式を使用します。

character-encoding *charset*

no character-encoding *charset*

構文の説明

charset	最大 40 文字から成るストリングで、http://www.iana.org/assignments/character-sets で特定されている有効な文字セットのいずれかに相当するもの。このページに示されている文字セットの名前またはエイリアスのいずれかを使用できます。たとえば、iso-8859-1、shift_jis、ibm850 などです。 この文字列は、大文字と小文字が区別されません。ASA 設定内では、コマンド インタープリタによって大文字が小文字に変換されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

*文字エンコーディング*は「文字コード」や「文字セット」とも呼ばれ、raw データ（0 や 1 など）を文字と組み合わせ、データを表します。使用する文字エンコード方式は、言語によって決まります。ある言語では同じ方式を使用していても、別の言語でも同じとはかぎりません。通常、ブラウザで使用されるデフォルトのエンコーディング方式は地域によって決まりますが、ユーザはこの方式を変更できます。ブラウザはページに指定されたエンコードを検出することもでき、そのエンコードに従ってドキュメントを表示します。character-encoding 属性を使用すると、ユーザは、文字エンコーディング方式の値を WebVPN ポータル ページに指定し、ブラウザを使用している地域やブラウザに対して行われたあらゆる変更に関係なく、ブラウザでこのページを正しく処理できます。

character-encoding 属性は、デフォルトでは、すべての WebVPN ポータル ページに継承されるグローバルな設定です。ただし、ユーザは、character-encoding 属性の値と異なる文字エンコーディングを使用する Common Internet File System（CIFS）サーバの file-encoding 属性を上書きできます。異なる文字エンコーディングが必要な CIFS サーバには異なるファイル エンコーディング値を使用します。

CIFS サーバから WebVPN ユーザにダウンロードされた WebVPN ポータル ページは、サーバを識別する WebVPN file-encoding 属性の値を符号化します。符号化が行われなかった場合は、character-encoding 属性の値を継承します。リモート ユーザのブラウザでは、ブラウザの文字エンコード セットのエントリにこの値がマップされ、使用する適切な文字セットが決定されます。WebVPN コンフィギュレーションで CIFS サーバ用の file-encoding エントリが指定されず、character-encoding 属性も設定されていない場合、WebVPN ポータル ページは値を指定しません。WebVPN ポータル ページが文字エンコーディングを指定しない場合、またはブラウザがサポートしていない文字エンコーディング値を指定した場合、リモート ブラウザはブラウザ自体のデフォルト エンコーディングを使用します。

CIFS サーバに適切な文字エンコーディングを、広域的には webvpn character-encoding 属性によって、個別的には file-encoding の上書きによってマッピングすることで、ページと同様にファイル名やディレクトリ パスを正しくレンダリングすることが必要な場合には、CIFS ページの正確な処理と表示が可能になります。

（注） character-encoding の値および file-encoding の値は、ブラウザによって使用されるフォント ファミリを排除するものではありません。Shift_JIS 文字エンコーディングを使用している場合、次の例に示すように webvpn カスタマイゼーション コマンド モードで **page style** コマンドを使用して、これらの値の 1 つの設定を補完して、フォント ファミリを置き換える必要があります。あるいは、webvpn カスタマイゼーション コマンド モードで **no page style** コマンドを入力して、このフォント ファミリを削除する必要があります。

この属性に値が含まれていない場合、WebVPN ポータル ページの文字セットは、リモート ブラウザに設定されているエンコーディング タイプによって決まります。

例

次に、日本語 Shift_JIS 文字をサポートする character-encoding 属性を設定し、フォント ファミリを削除し、デフォルトの背景色を保持する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# character-encoding shift_jis
ciscoasa(config-webvpn)# customization DfltCustomization
ciscoasa(config-webvpn-custom)# page style background-color:white
ciscoasa(config-webvpn-custom)#
```

関連コマンド

コマンド	説明
debug webvpn cifs	CIFS サーバに関するデバッギング メッセージを表示します。
file-encoding	CIFS サーバおよび関連する文字エンコーディングを指定し、この属性の値を上書きします。
show running-config [all] webvpn	WebVPN の実行コンフィギュレーションを表示します。デフォルト コンフィギュレーションを組み込むには **all** キーワードを使用します。

checkheaps

checkheaps 検証の間隔を設定するには、グローバル コンフィギュレーション モードで **checkheaps** コマンドを使用します。この値をデフォルトに設定するには、このコマンドの **no** 形式を使用します。

checkheaps {check-interval | validate-checksum} *seconds*

no checkheaps {check-interval | validate-checksum} [*seconds*]

構文の説明

check-interval	バッファ検証の間隔を設定します。バッファ検証プロセスでは、ヒープ(割り当てられ、解放されたメモリ バッファ)の健全性がチェックされます。このプロセスの各呼び出しの間、ASA はヒープ全体をチェックし、各メモリ バッファを検証します。不一致がある場合、ASA は、「バッファ割り当てエラー」または「バッファ解放エラー」を発行します。エラーがある場合、ASA は可能であればトレースバック情報をダンプし、リロードします。
seconds	1 ～ 2147483 の間隔を秒単位で設定します。
validate-checksum	コード スペースのチェックサム検証間隔を設定します。最初に ASA を起動するときに、ASA はコード全体のハッシュを計算します。その後、ASA は、定期チェックの間に新しいハッシュを生成し、元のハッシュと比較します。不一致がある場合、ASA は「テキスト チェックサム チェックヒープ エラー」を発行します。エラーがある場合、ASA は可能であればトレースバック情報をダンプし、リロードします。

デフォルト

デフォルトの間隔はそれぞれ 60 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

チェックヒープは、ヒープ メモリ バッファの正常性およびコード領域の完全性を検証する定期的なプロセスです(ダイナミック メモリはシステム ヒープ メモリ領域から割り当てられます)。

例

次に、バッファ割り当て間隔を 200 秒、コード スペースのチェックサムの間隔を 500 秒に設定する例を示します。

```
ciscoasa(config)# checkheaps check-interval 200
ciscoasa(config)# checkheaps validate-checksum 500
```

関連コマンド

コマンド	説明
show checkheaps	checkheaps 統計情報を表示します。

check-retransmission

TCP 再送信スタイルの攻撃を防止するには、tcp マップ コンフィギュレーション モードで **check-retransmission** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

check-retransmission

no check-retransmission

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
TCP マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

tcp-map コマンドはモジュラ ポリシー フレームワーク インフラストラクチャと一緒に使用されます。**class-map** コマンドを使用してトラフィックのクラスを定義し、**tcp-map** コマンドで TCP インスペクションをカスタマイズします。**policy-map** コマンドを使用して、新しい TCP マップを適用します。**service-policy** コマンドで、TCP インスペクションをアクティブにします。

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。矛盾する再送信をエンド システムが解釈する際に生じる TCP 再送信スタイルの攻撃を防止するには、tcp マップ コンフィギュレーション モードで **check-retransmission** コマンドを使用します。

ASA は、再送信のデータが元のデータと同じかどうかを確認しようとします。データが一致しない場合、接続が ASA によってドロップされます。この機能がイネーブルの場合、TCP 接続上のパケットは順序どおりにのみ許可されます。詳細については、**queue-limit** コマンドを参照してください。

例

次に、すべての TCP フローで TCP チェック再送信機能をイネーブルにする例を示します。

```
ciscoasa(config)# access-list TCP extended permit tcp any any
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# check-retransmission
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match access-list TCP
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
help	**policy-map** コマンド、**class** コマンド、および **description** コマンドの構文ヘルプを表示します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection	接続値を設定します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

checksum-verification

TCP チェックサムの検証をイネーブルまたはディセーブルにするには、tcp マップ コンフィギュレーション モードで **checksum-verification** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

checksum-verification

no checksum-verification

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

チェックサムの検証は、デフォルトでディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
TCP マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

tcp-map コマンドはモジュラ ポリシー フレームワーク インフラストラクチャと一緒に使用されます。**class-map** コマンドを使用してトラフィックのクラスを定義し、**tcp-map** コマンドで TCP インスペクションをカスタマイズします。**policy-map** コマンドを使用して、新しい TCP マップを適用します。**service-policy** コマンドで、TCP インスペクションをアクティブにします。

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。tcp マップ コンフィギュレーション モードで **checksum-verification** コマンドを使用して、TCP チェックサムの検証をイネーブルにします。このチェックに失敗すると、パケットはドロップされます。

例

次に、10.0.0.0 ～ 20.0.0.0 の TCP 接続で TCP チェックサムの検証をイネーブルにする例を示します。

```
ciscoasa(config)# access-list TCP1 extended permit tcp 10.0.0.0 255.0.0.0 20.0.0.0
255.0.0.0
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# checksum-verification
```

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match access-list TCP1

ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap

ciscoasa(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
help	**policy-map** コマンド、**class** コマンド、および **description** コマンドの構文ヘルプを表示します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection	接続値を設定します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

cipc security-mode authenticated（廃止）

Cisco IP Communicator（CIPC）Softphone を音声 VLAN シナリオまたはデータ VLAN シナリオに導入する場合に、強制的に CIPC Softphone を認証済みモードで動作させるには、電話プロキシ コンフィギュレーション モードで **cipc security-mode authenticated** コマンドを使用します。CIPC Softphone が暗号化をサポートしている場合に、このコマンドをオフにするには、このコマンドの **no** 形式を使用します。

cipc security-mode authenticated

no cipc security-mode authenticated

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、このコマンドは、no 形式によってディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
Phone-Proxy コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(4)	コマンドが追加されました。
9.4(1)	このコマンドは、すべての **phone-proxy** モード コマンドとともに廃止されました。

使用上のガイドライン

データ VLAN に影響を及ぼそうとするセキュリティ上の脅威から音声ストリームを守るために、複数の VLAN を使用して音声とデータのトラフィックを分離することがセキュリティ上のベスト プラクティスです。ただし、Cisco IP Communicator（CIPC）Softphone アプリケーションは、それぞれの IP Phone に接続する必要があります。IP Phone は、音声 VLAN に常駐しています。この要件により、音声 VLAN とデータ VLAN を分離することが問題になります。これは、SIP プロトコルおよび SCCP プロトコルが広範囲のポートで RTP ポートおよび RTCP ポートをダイナミックにネゴシエートするためです。このダイナミック ネゴシエーションでは、特定の範囲のポートを 2 つの VLAN の間で開く必要があります。

（注） 認証済みモードをサポートしていない旧バージョンの CIPC は、電話プロキシではサポートされていません。

データ VLAN と音声 VLAN の間でのアクセスを広範囲のポートで行わずに、データ VLAN 上の CIPC Softphone を音声 VLAN 上の該当する IP Phone と接続するには、**cipc security-mode authenticated** コマンドを使用して電話プロキシを設定します。

このコマンドを使用すると、電話プロキシが CIPC コンフィギュレーション ファイルを参照し、CIPC ソフトフォンが強制的に（暗号化済みモードではなく）認証済みモードになります。これは、現在のバージョンの CIPC が暗号化済みモードをサポートしていないためです。

このコマンドがイネーブルの場合、電話プロキシは、電話コンフィギュレーション ファイルを解析し、電話が CIPC Softphone かどうかを判別し、セキュリティ モードを認証済みに変更します。またデフォルトでは、電話プロキシがすべての電話を強制的に暗号化済みモードにしている間だけ、CIPC Softphone は認証済みモードをサポートします。

例

次に、**cipc security-mode authenticated** コマンドを使用して、音声 VLAN シナリオまたはデータ VLAN シナリオに Cisco IP Communicator（CIPC）Softphone を導入するときに CIPC Softphone を強制的に認証済みモードで動作させる例を示します。

```
ciscoasa(config)# phone-proxy asa_phone_proxy
ciscoasa(config-phone-proxy)#cipc security-mode authenticated
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。

clacp static-port-priority

クラスタリング スパンド EtherChannel の LACP でダイナミック ポート プライオリティをディセーブルにするには、グローバル コンフィギュレーション モードで **clacp static-port-priority** コマンドを使用します。これは、アクティブ EtherChannel メンバーが 8 を超過する場合に必要となります。ダイナミック ポート プライオリティをイネーブルにするには、このコマンドの **no** 形式を使用します。

clacp static-port-priority

no clacp static-port-priority

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

このコマンドはデフォルトでディセーブルです。ダイナミック ポート プライオリティはイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

一部のスイッチはダイナミック ポート プライオリティをサポートしていないため、このコマンドはスイッチの互換性を高めます。さらに、このコマンドは、9 ～ 32 のアクティブ スパンド EtherChannel メンバーのサポートをイネーブルにします。このコマンドを使用しないと、サポートされるのは 8 個のアクティブ メンバと 8 個のスタンバイ メンバのみです。

ASA EtherChannel は、最大 16 のアクティブ リンクをサポートします。スパンド EtherChannel では、vPC の 2 台のスイッチとともに使用し、**clacp static-port-priority** コマンドによってダイナミック ポート プライオリティをディセーブルにした場合、この機能はクラスタ全体で最大 32 のアクティブ リンクをサポートするように拡張されます。スイッチは、16 のアクティブ リンクを持つ EtherChannel をサポートする必要があります（Nexus 7000 の F2 シリーズ 10 ギガビット イーサネット モジュールなど）。

8 つのアクティブ リンクをサポートする VSS または vPC のスイッチの場合、スパンド EtherChannel に 16 のアクティブ リンクを設定できます（各スイッチに 8 つ接続）。

(注) スパンド EtherChannel で 8 つを超えるアクティブ リンクを使用する場合は、スタンバイ リンクも使用することはできません。9 ～ 32 のアクティブ リンクのサポートでは、スタンバイ リンクを使用できる cLACP ダイナミック ポート プライオリティをディセーブルにする必要があります。

例

次に、ダイナミック ポート プライオリティをディセーブルにする例を示します。

```
ciscoasa(config)# clacp static-port-priority
```

関連コマンド

コマンド	説明
clacp system-mac	cLACP システム ID を設定します。

clacp system-mac

ASA クラスタのマスター ユニットで cLACP システム ID を手動で設定する場合、クラスタ グループ コンフィギュレーション モードで **clacp system-mac** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

clacp system-mac {*mac_address* | **auto**} [**system-priority** *number*]

no clacp system-mac {*mac_address* | **auto**} [**system-priority** *number*]

構文の説明

mac_address	システム ID を *H.H.H* の形式で手動で設定します。H は 16 ビットの 16 進数の 1 桁です。たとえば、MAC アドレス 00-0A-00-00-AA-AA は、000A.0000.AAAA と入力します。
[auto]	システム ID を自動生成します。
system-priority *number*	システム プライオリティを 1 ～ 65535 の範囲で設定します。優先度はどのユニットがバンドルの決定を行うかを決定するため使用されます。デフォルトでは、ASA はプライオリティ 1（最高のプライオリティ）を使用します。このプライオリティは、スイッチのプライオリティよりも高いことが必要です。

コマンド デフォルト

デフォルトでは、システム MAC は自動生成されます（**auto**）。

デフォルトでは、system-priority は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラスタ グループ コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

スパンド EtherChannel を使用するときは、ASA は cLACP を使用してネイバー スイッチとの間で EtherChannel のネゴシエーションを行います。cLACP ネゴシエーションのときに、同じクラスタ内の ASA は互いに連携し、スイッチに対して全体で 1 つの（仮想）デバイスであるかのように見せます。cLACP ネゴシエーションのパラメータの 1 つであるシステム ID は、MAC アドレスの形式をとります。すべての ASA で同じシステム ID が使用されます。システム ID は、マスター ユニットによって自動生成され（デフォルト）、すべてのスレーブに複製されるか、このコマンドに手動で指定します。トラブルシューティングの目的で、たとえば、識別が容易な MAC アドレスを使用できるように、手動で MAC アドレスを設定することがあります。一般的には、自動生成された MAC アドレスを使用します。

このコマンドは、ブートストラップ コンフィギュレーションの一部ではなく、マスター ユニットからスレーブ ユニットに複製されます。ただし、クラスタリングをイネーブルにした後は、この値は変更できません。

例

次に、システム ID を手動で設定する例を示します。

```
cluster group pod1
    local-unit unit1
    cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
    priority 1
    key chuntheunavoidable
    health-check
    clacp system-mac 000a.0000.aaaa
    enable noconfirm
```

関連コマンド

コマンド	説明
cluster group	クラスタ パラメータを設定します。

class（グローバル）

セキュリティ コンテキストの割り当て先のリソース クラスを作成するには、グローバル コンフィギュレーション モードで **class** コマンドを使用します。クラスを削除するには、このコマンドの **no** 形式を使用します。

class *name*

no class *name*

構文の説明

name	20 文字までの文字列で名前を指定します。デフォルト クラスに関する制限を設定するには、**default** という名前を入力します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、コンテキストごとの上限値が適用されていない限り、すべてのセキュリティ コンテキストが ASA のリソースに無制限にアクセスできます。ただし、1 つ以上のコンテキストがリソースを大量に使用しており、他のコンテキストが接続を拒否されている場合は、リソース管理を設定してコンテキストごとのリソースの使用を制限できます。

ASA では、リソース クラスにコンテキストを割り当てることによって、リソースを管理します。各コンテキストでは、クラスによって設定されたリソース制限が使用されます。

クラスを作成すると、ASA は、クラスに割り当てられる各コンテキストに対してリソースの一部を確保しなくなります。その代わりに、ASA は、コンテキストの上限を設定します。リソースをオーバーサブスクライブする場合、または一部のリソースを無制限にする場合は、少数のコンテキストがこれらのリソースを「使い果たし」、他のコンテキストへのサービスに影響する可能性があります。クラス用のリソースを設定するには、**limit-resource** コマンドを参照してください。

すべてのコンテキストは、別のクラスに割り当てられていない場合はデフォルト クラスに属します。コンテキストをデフォルト クラスに積極的に割り当てる必要はありません。

コンテキストがデフォルト クラス以外のクラスに属する場合、それらのクラス設定は常にデフォルト クラス設定を上書きします。ただし、他のクラスに定義されていない設定がある場合、メンバ コンテキストはそれらの制限にデフォルト クラスを使用します。たとえば、すべての同時接続に 2 % の制限を設定したがその他の制限を設定せずにクラスを作成した場合、他のすべての制限はデフォルト クラスから継承されます。逆に、すべてのリソースに対する制限を設定してクラスを作成した場合、そのクラスはデフォルト クラスの設定を使用しません。

デフォルトでは、デフォルト クラスは、すべてのコンテキストにリソースへのアクセスを無制限に提供します。ただし、次の制限が適用されます(この制限は、デフォルトではコンテキストあたりの最大許容値が設定されます)。

- Telnet セッション:5 セッション。
- SSH セッション:5 セッション。
- MAC アドレス:65,535 エントリ。

例

次に、接続のデフォルト クラスの制限に、無制限ではなく 10 % を設定する例を示します。

```
ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
```

他のリソースはすべて無制限のままです。

gold というクラスを追加するには、次のコマンドを入力します。

```
ciscoasa(config)# class gold
ciscoasa(config-class)# limit-resource mac-addresses 10000
ciscoasa(config-class)# limit-resource conns 15%
ciscoasa(config-class)# limit-resource rate conns 1000
ciscoasa(config-class)# limit-resource rate inspects 500
ciscoasa(config-class)# limit-resource hosts 9000
ciscoasa(config-class)# limit-resource asdm 5
ciscoasa(config-class)# limit-resource ssh 5
ciscoasa(config-class)# limit-resource rate syslogs 5000
ciscoasa(config-class)# limit-resource telnet 5
ciscoasa(config-class)# limit-resource xlates 36000
ciscoasa(config-class)# limit-resource routes 5000
```

関連コマンド

コマンド	説明
clear configure class	クラス コンフィギュレーションをクリアします。
context	セキュリティ コンテキストを設定します。
limit-resource	クラスのリソース制限を設定します。
member	コンテキストをリソース クラスに割り当てます。
show class	クラスに割り当てられているコンテキストを表示します。

class（ポリシー マップ）

クラス マップ トラフィックにアクションを割り当てることができるポリシー マップにクラス マップを割り当てるには、ポリシー マップ コンフィギュレーション モードで **class** コマンドを使用します。ポリシー マップからクラス マップを削除するには、このコマンドの **no** 形式を使用します。

class *classmap_name*

no class *classmap_name*

構文の説明

classmap_name	クラス マップの名前を指定します。レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）の場合、レイヤ 3/4 クラス マップ名（**class-map** コマンドまたは **class-map type management** コマンド）を指定する必要があります。インスペクション ポリシー マップ（**policy-map type inspect** コマンド）の場合、インスペクション クラス マップ名（**class-map type inspect** コマンド）を指定する必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

class コマンドを使用するには、Modular Policy Framework を使用します。レイヤ 3/4 ポリシー マップでクラスを使用するには、次のコマンドを入力します。

1. **class-map**：アクションを実行するトラフィックを識別します。
2. **policy-map**：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. *commands for supported features*：特定のクラス マップについて、QoS、アプリケーション インスペクション、CSC または AIP SSM、TCP 接続と UDP 接続の制限とタイムアウト、TCP 正規化など、さまざまな機能の多数のアクションを設定できます。各機能で使用可能なコマンドの詳細については、CLI 設定ガイドを参照してください。

3. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

インスペクション ポリシー マップでクラスを使用するには、次のコマンドを入力します。

1. **class-map type inspect**：アクションを実行するトラフィックを指定します。
2. **policy-map type inspect**：各クラス マップに関連付けられているアクションを指定します。
   a. **class**：アクションを実行するインスペクション クラス マップを指定します。
   b. *アプリケーション タイプのコマンド*：各アプリケーション タイプで使用可能なコマンドについては、CLI 設定ガイドを参照してください。インスペクション ポリシー マップのクラス コンフィギュレーション モードでサポートされているアクションには、次のものが含まれます。
   - パケットのドロップ
   - 接続のドロップ
   - 接続のリセット
   - ロギング
   - メッセージのレートの制限
   - コンテンツのマスキング

   c. **parameters**：インスペクション エンジンに影響を及ぼすパラメータを設定します。CLI はパラメータ コンフィギュレーション モードに移行します。使用可能なコマンドについては、CLI 設定ガイドを参照してください。
3. **class-map**：アクションを実行するトラフィックを識別します。
4. **policy-map**：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するレイヤ 3/4 クラス マップを指定します。
   b. **inspect** *application inspect_policy_map*：アプリケーション インスペクションをイネーブルにし、特別なアクションを実行するインスペクション ポリシー マップを呼び出します。
5. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

このコンフィギュレーションには、すべてのトラフィックと一致する、**class-default** と呼ばれるクラス マップが必ず含まれています。各レイヤ 3/4 ポリシー マップの末尾には、アクションが定義されていない **class-default** クラス マップがコンフィギュレーションに含まれています。すべてのトラフィックと照合するが、別のクラス マップを作成しない場合、このクラス マップをオプションで使用できます。実際、一部の機能は、**class-default** クラス マップ用にのみ設定できます（**shape** コマンドなど）。

class-default クラス マップを含めて、最大 63 個の **class** コマンドおよび **match** コマンドをポリシー マップに設定できます。

例

次に、**class** コマンドを含む、接続ポリシーの **policy-map** コマンドの例を示します。このコマンドは、Web サーバ 10.1.1.1 への接続許可数を制限します。

```
ciscoasa(config)# access-list http-server permit tcp any host 10.1.1.1
ciscoasa(config)# class-map http-server
ciscoasa(config-cmap)# match access-list http-server

ciscoasa(config)# policy-map global-policy
ciscoasa(config-pmap)# description This policy map defines a policy concerning connection
to http server.
```

```
ciscoasa(config-pmap)# class http-server
ciscoasa(config-pmap-c)# set connection conn-max 256
```

次の例は、ポリシー マップでの複数の照合の動作を示しています。

```
ciscoasa(config)# class-map inspection_default
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config)# class-map http_traffic
ciscoasa(config-cmap)# match port tcp eq 80

ciscoasa(config)# policy-map outside_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect http http_map
ciscoasa(config-pmap-c)# inspect sip
ciscoasa(config-pmap)# class http_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:10:0
```

次の例は、トラフィックが最初の利用可能なクラス マップと一致した場合に、同じ機能ドメインのアクションが指定されている後続のクラス マップと照合されないことを示しています。

```
ciscoasa(config)# class-map telnet_traffic
ciscoasa(config-cmap)# match port tcp eq 23
ciscoasa(config)# class-map ftp_traffic
ciscoasa(config-cmap)# match port tcp eq 21
ciscoasa(config)# class-map tcp_traffic
ciscoasa(config-cmap)# match port tcp range 1 65535
ciscoasa(config)# class-map udp_traffic
ciscoasa(config-cmap)# match port udp range 0 65535
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class telnet_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:0:0
ciscoasa(config-pmap-c)# set connection conn-max 100
ciscoasa(config-pmap)# class ftp_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:5:0
ciscoasa(config-pmap-c)# set connection conn-max 50
ciscoasa(config-pmap)# class tcp_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 2:0:0
ciscoasa(config-pmap-c)# set connection conn-max 2000
```

Telnet 接続は、開始時に **class telnet_traffic** と一致します。同様に FTP 接続は、開始時に **class ftp_traffic** と一致します。Telnet および FTP 以外の TCP 接続の場合は、**class tcp_traffic** と一致します。Telnet 接続または FTP 接続は **class tcp_traffic** と一致しますが、すでに他のクラスと一致しているため、ASA はこの照合を行いません。

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
class-map type management	管理トラフィック用のレイヤ 3/4 クラス マップを作成します。
clear configure policy-map	**service-policy** コマンドで使用中のポリシー マップを除く、すべてのポリシー マップ コンフィギュレーションを削除します。
match	トラフィック照合パラメータを定義します。
policy-map	ポリシー（それぞれが 1 つ以上のアクションを持つ 1 つ以上のトラフィック クラスの関連付け）を設定します。

class-map

モジュラ ポリシー フレームワークを使用するとき、グローバル コンフィギュレーション モードで **class-map** コマンド（**type** キーワードは指定しない）を使用して、アクションを適用するレイヤ 3 またはレイヤ 4 のトラフィックを指定します。クラス マップを削除するには、このコマンドの **no** 形式を使用します。

class-map *class_map_name*

no class-map *class_map_name*

構文の説明

class_map_name	40 文字までの長さのクラス マップ名を指定します。名前「class-default」と、「_internal」または「_default」で始まるすべての名前は予約されています。クラス マップのすべてのタイプで同じネーム スペースを使用するため、すでに別のクラス マップ タイプで使用されている名前は再利用できません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このタイプのクラス マップは、レイヤ 3/4 通過トラフィック専用です。ASA 宛ての管理トラフィックについては、**class-map type management** コマンドを参照してください。

レイヤ 3/4 クラス マップにより、アクションを適用するレイヤ 3 および 4 のトラフィックを特定します。1 つのレイヤ 3/4 ポリシー マップに複数のレイヤ 3/4 クラス マップを作成できます。

デフォルトのクラス マップ

コンフィギュレーションには、デフォルト グローバル ポリシーで ASA が使用するデフォルトのレイヤ 3/4 クラス マップが含まれます。これは、**inspection_default** と呼ばれ、デフォルト インスペクション トラフィックと一致します。

```
class-map inspection_default
 match default-inspection-traffic
```

デフォルトのコンフィギュレーションに存在する別のクラス マップは、class-default と呼ばれ、これはすべてのトラフィックと一致します。

```
class-map class-default
 match any
```

このクラス マップは、すべてのレイヤ 3/4 ポリシー マップの最後に表示され、原則的に、他のすべてのトラフィックでどんなアクションも実行しないように ASA に通知します。独自の **match any** クラス マップを作成するのではなく、必要に応じて class-default クラス マップを使用できます。実際のところ、class-default で使用可能な機能は、QoS トラフィック シェーピングなどの一部の機能だけです。

最大クラス マップ

すべてのタイプのクラス マップの最大数は、シングル モードでは 255 個、マルチ モードではコンテキストごとに 255 個です。クラス マップには、次のタイプがあります。

- **class-map**
- **class-map type management**
- **class-map type inspection**
- **class-map type regex**
- ポリシー マップ タイプの **match** コマンドでは、コンフィギュレーション モードを検査します。

この制限にはすべてのタイプのデフォルト クラス マップも含まれます。

コンフィギュレーションの概要

モジュラ ポリシー フレームワークの設定手順は、次の 4 つの作業で構成されます。

1. **class-map** コマンドまたは **class-map type management** コマンドを使用して、アクションの適用対象となるレイヤ 3 と 4 のトラフィックを指定します。
2. （アプリケーション インスペクションのみ）**policy-map type inspect** コマンドを使用して、アプリケーション インスペクション トラフィックの特別なアクションを定義します。
3. **policy-map** コマンドを使用して、レイヤ 3 と 4 のトラフィックにアクションを適用します。
4. **service-policy** コマンドを使用して、インターフェイスでのアクションをアクティブにします。

class-map コマンドを使用して、クラス マップ コンフィギュレーション モードを開始します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。レイヤ 3/4 クラス マップには、クラス マップに含まれているトラフィックを指定する、**match** コマンド（**match tunnel-group** コマンドおよび **match default-inspection-traffic** コマンドを除く）が 1 つだけ含まれています。

例

次に、4 つのレイヤ 3/4 クラス マップを作成する例を示します。

```
ciscoasa(config)# access-list udp permit udp any any
ciscoasa(config)# access-list tcp permit tcp any any
ciscoasa(config)# access-list host_foo permit ip any 10.1.1.1 255.255.255.255

ciscoasa(config)# class-map all_udp
ciscoasa(config-cmap)# description "This class-map matches all UDP traffic"
ciscoasa(config-cmap)# match access-list udp

ciscoasa(config-cmap)# class-map all_tcp
ciscoasa(config-cmap)# description "This class-map matches all TCP traffic"
ciscoasa(config-cmap)# match access-list tcp

ciscoasa(config-cmap)# class-map all_http
ciscoasa(config-cmap)# description "This class-map matches all HTTP traffic"
ciscoasa(config-cmap)# match port tcp eq http

ciscoasa(config-cmap)# class-map to_server
ciscoasa(config-cmap)# description "This class-map matches all traffic to server 10.1.1.1"
ciscoasa(config-cmap)# match access-list host_foo
```

関連コマンド

コマンド	説明
class-map type management	ASA へのトラフィック用のクラス マップを作成します。
policy-map	トラフィック クラスを 1 つ以上のアクションと関連付けることによって、ポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
service-policy	ポリシー マップを 1 つ以上のインターフェイスと関連付けることによって、セキュリティ ポリシーを作成します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

class-map type inspect

モジュラ ポリシー フレームワーク を使用するときに、グローバル コンフィギュレーション モードで **class-map type inspect** コマンドを使用して検査アプリケーションに固有の基準と一致を確認します。インスペクション クラス マップを削除するには、このコマンドの **no** 形式を使用します。

class-map type inspect *application* [**match-all | match-any**] *class_map_name*

no class-map [**type inspect** *application* [**match-all | match-any**]] *class_map_name*

構文の説明

application	照合するアプリケーション トラフィックのタイプを指定します。利用可能なタイプは次のとおりです。 • **dcerpc** • **diameter** • **dns** • **FTP** • **h323** • **http** • **im** • **rtsp** • **scansafe** • **sip**
class_map_name	40 文字までの長さのクラス マップ名を指定します。名前「class-default」と、「_internal」または「_default」で始まるすべての名前は予約されています。クラス マップのすべてのタイプで同じネーム スペースを使用するため、すでに別のクラス マップ タイプで使用されている名前は再利用できません。
match-all	(任意)トラフィックがクラス マップと一致するには、すべての基準と一致する必要があることを指定します。オプションを指定しない場合、**match-all** がデフォルトです。
match-any	(任意)トラフィックがクラス マップと一致するには、1 つ以上の基準と一致する必要があることを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.0(2)	**match-any** キーワードが追加されました。
9.0(1)	**scansafe** キーワードが追加されました。
9.5(2)	**dcerpc** および **diameter** キーワードが追加されました。

使用上のガイドライン

モジュラ ポリシー フレームワークを使用すると、多くのアプリケーション インスペクションに対して特別なアクションを設定できます。レイヤ 3/4 ポリシー マップでインスペクション エンジンをイネーブルにするときは、*インスペクション ポリシー マップ*で定義されているアクションを必要に応じてイネーブルにすることもできます（**policy-map type inspect** コマンドを参照）。

インスペクション ポリシー マップでは、インスペクション クラス マップを作成して、対象とするトラフィックを指定できます。このクラス マップには、1 つ以上の **match** コマンドが含まれます（あるいは、単一の基準とアクションをペアにする場合は、インスペクション ポリシー マップで **match** コマンドを直接使用できます）。アプリケーション固有の基準を照合できます。たとえば DNS トラフィックの場合は、DNS クエリー内のドメイン名と照合可能です。

クラス マップは、複数のトラフィック照合をグループ化します（match-all クラス マップ）。あるいはクラス マップで、照合リストのいずれかを照合できます（match-any クラス マップ）。クラス マップを作成することと、インスペクション ポリシー マップ内で直接トラフィック照合を定義することの違いは、クラス マップを使用して複数の match コマンドをグループ化できる点と、クラス マップを再使用できる点です。このクラス マップで指定するトラフィックに対しては、インスペクション ポリシー マップで、接続のドロップ、リセット、またはロギングなどのアクションを指定できます。

すべてのタイプのクラス マップの最大数は、シングル モードでは 255 個、マルチ モードではコンテキストごとに 255 個です。クラス マップには、次のタイプがあります。

- **class-map**
- **class-map type management**
- **class-map type inspection**
- **class-map type regex**
- ポリシー マップ タイプの **match** コマンドでは、コンフィギュレーション モードを検査します。

この制限にはすべてのタイプのデフォルト クラス マップも含まれます。詳細については、**class-map** コマンドを参照してください。

例

次の例では、すべての基準に一致する必要がある HTTP クラス マップを作成します。

```
ciscoasa(config-cmap)# class-map type inspect http match-all http-traffic
ciscoasa(config-cmap)# match req-resp content-type mismatch
ciscoasa(config-cmap)# match request body length gt 1000
ciscoasa(config-cmap)# match not request uri regex class URLs
```

次の例では、基準のいずれかに一致する必要がある HTTP クラス マップを作成します。

```
ciscoasa(config-cmap)# class-map type inspect http match-any monitor-http
ciscoasa(config-cmap)# match request method get
ciscoasa(config-cmap)# match request method put
ciscoasa(config-cmap)# match request method post
```

関連コマンド

コマンド	説明
class-map	通過トラフィック用のレイヤ 3/4 クラス マップを作成します。
policy-map	トラフィック クラスを 1 つ以上のアクションと関連付けることによって、ポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
service-policy	ポリシー マップを 1 つ以上のインターフェイスと関連付けることによって、セキュリティ ポリシーを作成します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

class-map type management

モジュラ ポリシー フレームワーク を使用するとき、グローバル コンフィギュレーション モードで **class-map type management** コマンドを使用して、アクションを適用する ASA 宛ての、レイヤ 3 またはレイヤ 4 の管理トラフィックを指定します。クラス マップを削除するには、このコマンドの **no** 形式を使用します。

class-map type management *class_map_name*

no class-map type management *class_map_name*

構文の説明

class_map_name	40 文字までの長さのクラス マップ名を指定します。名前「class-default」と、「_internal」または「_default」で始まるすべての名前は予約されています。クラス マップのすべてのタイプで同じネーム スペースを使用するため、すでに別のクラス マップ タイプで使用されている名前は再利用できません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.0(2)	ASA に向かう管理トラフィックの場合、レイヤ 3/4 管理クラス マップに **set connection** コマンドが使用できるようになりました。**conn-max** キーワードおよび **embryonic-conn-max** キーワードだけが使用可能です。

使用上のガイドライン

このタイプのクラス マップは、管理トラフィック専用です。通過トラフィックについては、**class-map** コマンド（**type** キーワードは指定しない）を参照してください。

ASA への管理トラフィックに対して、この種類のトラフィックに特有のアクションの実行が必要になる場合があります。ポリシー マップの管理クラス マップで設定可能なアクションのタイプは、管理トラフィック専用です。たとえば、このタイプのクラス マップでは、RADIUS アカウンティング トラフィックをインスペクトして、接続制限を設定できます。

レイヤ 3/4 クラス マップにより、アクションを適用するレイヤ 3 および 4 のトラフィックを特定します。すべてのタイプのクラス マップの最大数は、シングル モードでは 255 個、マルチ モードではコンテキストごとに 255 個です。

レイヤ 3/4 ポリシー マップそれぞれに、複数のレイヤ 3/4 クラス マップ（管理トラフィックまたは通過トラフィック）を作成できます。

モジュラ ポリシー フレームワークの設定手順は、次の 4 つの作業で構成されます。

1. **class-map** コマンドおよび **class-map type management** コマンドを使用して、アクションを適用するレイヤ 3 およびレイヤ 4 のトラフィックを識別します。
2. （アプリケーション インスペクションのみ）**policy-map type inspect** コマンドを使用して、アプリケーション インスペクション トラフィックの特別なアクションを定義します。
3. **policy-map** コマンドを使用して、レイヤ 3 と 4 のトラフィックにアクションを適用します。
4. **service-policy** コマンドを使用して、インターフェイスでのアクションをアクティブにします。

class-map type management コマンドを使用して、クラス マップ コンフィギュレーション モードを開始します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。管理クラス マップを指定して、アクセス リストまたは TCP や UDP のポートと照合できます。レイヤ 3/4 クラス マップには、クラス マップに含まれるトラフィックを指定する **match** コマンドが 1 つだけが含まれています。

すべてのタイプのクラス マップの最大数は、シングル モードでは 255 個、マルチ モードではコンテキストごとに 255 個です。クラス マップには、次のタイプがあります。

- **class-map**
- **class-map type management**
- **class-map type inspection**
- **class-map type regex**
- ポリシー マップ タイプの **match** コマンドでは、コンフィギュレーション モードを検査します。

この制限にはすべてのタイプのデフォルト クラス マップも含まれます。詳細については、**class-map** コマンドを参照してください。

例

次に、レイヤ 3/4 管理クラス マップを作成する例を示します。

```
ciscoasa(config)# class-map type management radius_acct
ciscoasa(config-cmap)# match port tcp eq 10000
```

関連コマンド

コマンド	説明
class-map	通過トラフィック用のレイヤ 3/4 クラス マップを作成します。
policy-map	トラフィック クラスを 1 つ以上のアクションと関連付けることによって、ポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
service-policy	ポリシー マップを 1 つ以上のインターフェイスと関連付けることによって、セキュリティ ポリシーを作成します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

class-map type regex

モジュラ ポリシー フレームワーク を使用するときに、グローバル コンフィギュレーション モードで **class-map type regex** コマンドを使用して、一致テキストで利用する正規表現をグループ化します。正規表現クラス マップを削除するには、このコマンドの **no** 形式を使用します。

class-map type regex match-any *class_map_name*

no class-map [**type regex match-any**] *class_map_name*

構文の説明

class_map_name	40 文字までの長さのクラス マップ名を指定します。名前「class-default」と、「_internal」または「_default」で始まるすべての名前は予約されています。クラス マップのすべてのタイプで同じネーム スペースを使用するため、すでに別のクラス マップ タイプで使用されている名前は再利用できません。
match-any	トラフィックが正規表現のいずれかとだけ一致する場合でも、このトラフィックがクラス マップと一致しているとすることを指定します。**match-any** が唯一のオプションです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

モジュラ ポリシー フレームワークを使用すると、多くのアプリケーション インスペクションに対して特別なアクションを設定できます。レイヤ 3/4 ポリシー マップでインスペクション エンジンをイネーブルにするときは、*インスペクション ポリシー マップ*で定義されているアクションを必要に応じてイネーブルにすることもできます（**policy-map type inspect** コマンドを参照）。

インスペクション ポリシー マップでは、1 つ以上の **match** コマンドを含んだインスペクション クラス マップを作成することで、アクションの実行対象となるトラフィックを識別できます。または、**match** コマンドをインスペクション ポリシー マップ内で直接使用することもできます。一部の **match** コマンドでは、パケット内のテキストを正規表現を使用して識別できます。たとえば、HTTP パケット内の URL 文字列を照合できます。正規表現クラス マップで正規表現をグループ化できます。

正規表現クラス マップを作成する前に、**regex** コマンドを使用して、正規表現を作成します。次に、**match regex** コマンドを使用して、クラス マップ コンフィギュレーション モードで名前を付けられた正規表現を指定します。

すべてのタイプのクラス マップの最大数は、シングル モードでは 255 個、マルチ モードではコンテキストごとに 255 個です。クラス マップには、次のタイプがあります。

- **class-map**
- **class-map type management**
- **class-map type inspection**
- **class-map type regex**
- ポリシー マップ タイプの **match** コマンドでは、コンフィギュレーション モードを検査します。

この制限にはすべてのタイプのデフォルト クラス マップも含まれます。詳細については、**class-map** コマンドを参照してください。

例

次に、2 つの正規表現を作成し、これを正規表現クラス マップに追加する例を示します。トラフィックに文字列「example.com」または「example2.com」が含まれる場合、トラフィックはクラス マップと一致します。

```
ciscoasa(config)# regex url_example example\.com
ciscoasa(config)# regex url_example2 example2\.com
ciscoasa(config)# class-map type regex match-any URLs
ciscoasa(config-cmap)# match regex url_example
ciscoasa(config-cmap)# match regex url_example2
```

関連コマンド

コマンド	説明
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	トラフィック クラスを 1 つ以上のアクションと関連付けることによって、ポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
service-policy	ポリシー マップを 1 つ以上のインターフェイスと関連付けることによって、セキュリティ ポリシーを作成します。
regex	正規表現を作成します。

clear aaa kerberos

Kerberos 情報をクリアするには、特権 EXEC モードで **clear aaa kerberos** コマンドを使用します。

clear aaa kerberos {**tickets** [**username** *user*] | **keytab**}

構文の説明

keytab	Kerberos キータブファイルをクリアします。
tickets [**username** *user*]	Kerberos チケット情報をクリアします。チケットをクリアするユーザを指定する username キーワードを含めない限り、すべてのチケットがクリアされます。

デフォルト

デフォルト設定はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.8(4)	**keytab** キーワードが追加されました。

例

次に、すべての Kerberos チケットをクリアする例を示します。

```
ciscoasa# clear aaa kerberos tickets
Proceed with deleting kerberos tickets? [confirm] y
```

次に、Kerberos キータブファイルを表示した後にクリアする例を示します。

```
ciscoasa# show aaa kerberos keytab
Principal:   host/asa2@BXB-WIN2016.EXAMPLE.COM
Key version: 10
Key type:    arcfour (23)
ciscoasa# clear aaa kerberos keytab
ciscoasa# show aaa kerberos keytab
No keys found
ciscoasa#
```

関連コマンド

コマンド	説明
show aaa kerberos	システム上のキャッシュされたすべての Kerberos チケット、またはキータブファイルを表示します。

clear aaa local user

ユーザをロック解除したり、ユーザの失敗した認証試行回数をゼロにリセットしたりするには、特権 EXEC モードで **clear aaa local user** コマンドを使用します。

clear aaa local user {**fail-attempts** | **lockout**} {**username** *name* | **all**}

構文の説明

all	ロックアウトされたすべてのユーザをロック解除するか、すべてのユーザについて、失敗試行カウンタを 0 にリセットします。
failed-attempts	指定したユーザまたはすべてのユーザについて、失敗試行カウンタを 0 にリセットします。
lockout	現在ロックアウトされているユーザをロック解除し、ユーザの失敗試行カウンタを 0 にリセットします。このオプションは、ロックアウトされていないユーザには影響を与えません。 管理者をデバイスからロックアウトすることはできません。
username *name*	ロック解除するか、失敗試行カウンタを 0 にリセットする特定のユーザ名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ユーザが認証試行を何回か失敗した後に、ユーザ認証を失敗にするには、このコマンドを使用します。

設定された認証試行の失敗数に達すると、ユーザは、システムからロック アウトされ、システム管理者がこのユーザ名のロックを解除するか、またはシステムをリブートするまで、正常にログインできません。ユーザが正常に認証されるか、またはシステムをリブートすると、失敗試行数が 0 にリセットされ、ロックアウト ステータスが No にリセットされます。また、コンフィギュレーションが変更されると、システムがカウンタを 0 にリセットします。

ユーザ名のロックまたはアンロックにより、システム ログ メッセージが生成されます。特権レベル 15 のシステム管理者は、ロック アウトされません。

例

次に、ユーザ名 anyuser の失敗試行カウンタを 0 にリセットする例を示します。

```
ciscoasa# clear aaa local user fail-attempts username anyuser
ciscoasa#
```

次に、すべてのユーザの失敗試行カウンタを 0 にリセットする例を示します。

```
ciscoasa# clear aaa local user fail-attempts all
ciscoasa#
```

次に、ユーザ名 anyuser のロックアウト状態をクリアし、失敗試行カウンタを 0 にリセットする例を示します。

```
ciscoasa# clear aaa local user lockout username anyuser
ciscoasa#
```

関連コマンド

コマンド	説明
aaa local authentication attempts max-fail	許可される失敗ユーザ認証試行の回数制限を設定します。
show aaa local user	試行失敗カウンタおよびロックアウト ステータスを持つユーザ名のリストを表示します。

clear aaa sdi node-secret

RSA SecurID サーバのノードシークレットファイルを削除するには、特権 EXEC モードで **clear aaa sdi node-secret** コマンドを使用します。

clear aaa sdi node-secret *rsa_server_address*

構文の説明

rsa_server_address	ノードシークレットファイルを削除する RSA SecurID/Authentication Manager サーバの IP アドレスまたは完全修飾ホスト名。

デフォルト

デフォルト設定はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.15(1)	このコマンドが追加されました。

例

次に、ノードシークレットファイルのリストを表示し、その 1 つを削除する例を示します。必要に応じて、aaa sdi import-node-secret コマンドを使用して、サーバの新しいノードシークレットファイルをインポートしてください。

```
ciscoasa# show aaa sdi node-secrets
Last update                    SecurID server
--------------------           --------------------
15:16:13 Jun 24 2020           rsaam.example.com
15:20:07 Jun 24 2020           10.11.12.13
ciscoasa# clear aaa sdi node-secret rsaam.example.com
```

関連コマンド

コマンド	説明
aaa sdi import-node-secret	RSA SecurID Authentication Manager ノードシークレットファイルをインポートします。
show aaa sdi node-secrets	すべての SecurID ノードシークレットファイルを表示します。

clear aaa-server statistics

AAA サーバの統計情報をリセットするには、特権 EXEC モードで **clear aaa-server statistics** コマンドを使用します。

clear aaa-server statistics [**LOCAL** | *groupname* [**host** *hostname*] | **protocol** *protocol*]

構文の説明

groupname	(任意) グループ内のサーバの統計情報をクリアします。
host *hostname*	(任意) グループ内の特定のサーバの統計情報をクリアします。
LOCAL	(任意) LOCAL ユーザ データベースの統計情報をクリアします。
protocol *protocol*	(任意) 指定するプロトコルのサーバの統計情報をクリアします。 • **kerberos** • **ldap** • **nt** • **radius** • **sdi** • **tacacs+**

デフォルト

すべてのグループのすべての AAA サーバの統計情報を削除します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	CLI ガイドラインに沿うように、このコマンドが変更されました。プロトコルの値において、以前の **nt-domain** から **nt** に、以前の **rsa-ace** から **sdi** に置き換えられました。

例

次に、グループ内の特定のサーバの AAA 統計情報をリセットする例を示します。

```
ciscoasa(config)# clear aaa-server statistics svrgrp1 host 1.2.3.4
```

次に、サーバ グループ全体の AAA 統計情報をリセットする例を示します。

```
ciscoasa(config)# clear aaa-server statistics svrgrp1
```

次に、すべてのサーバ グループの AAA 統計情報をリセットする例を示します。

```
ciscoasa(config)# clear aaa-server statistics
```

次に、特定のプロトコル（この場合は TACACS+）の AAA 統計情報をリセットする例を示します。

```
ciscoasa(config)# clear aaa-server statistics protocol tacacs+
```

関連コマンド

コマンド	説明
aaa-server protocol	AAA サーバ接続データのグループ化の指定および管理を行います。
clear configure aaa-server	デフォルト以外のすべての AAA サーバ グループを削除するか、または指定したグループをクリアします。
show aaa-server	AAA サーバの統計情報を表示します。
show running-config aaa-server	現在の AAA サーバ コンフィギュレーションの値を表示します。

clear access-list

アクセス リスト カウンタをクリアするには、グローバル コンフィギュレーション モードで **clear access-list** コマンドを使用します。

clear access-list *id* **counters**

構文の説明

counters	アクセス リストのカウンタをクリアします。
id	アクセス リストの名前または番号。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

clear access-list コマンドを入力したら、カウンタをクリアするアクセス リストの *ID* を指定します。

例

次に、特定のアクセス リスト カウンタをクリアする例を示します。

```
ciscoasa# clear access-list inbound counters
```

関連コマンド

コマンド	説明
access-list extended	アクセス リストをコンフィギュレーションに追加し、ファイアウォールを通過する IP トラフィック用のポリシーを設定します。
access-list standard	OSPF ルートの宛先 IP アドレスを識別するアクセス リストを追加します。このアクセス リストは、OSPF 再配布のルート マップで使用できます。

コマンド	説明
clear configure access-list	実行コンフィギュレーションからアクセス リストをクリアします。
show access-list	アクセス リスト エントリを番号で表示します。
show running-config access-list	適応型セキュリティ アプライアンスで実行中のアクセス リスト コンフィギュレーションを表示します。

clear arp

ダイナミック ARP エントリまたは ARP 統計情報をクリアするには、特権 EXEC モードで **clear arp** コマンドを使用します。

clear arp [**statistics**]

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、すべての ARP 統計情報をクリアする例を示します。

```
ciscoasa# clear arp statistics
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	トランスペアレント ファイアウォール モードで、ARP パケットを調査し、ARP スプーフィングを防止します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

clear asp

高速セキュリティ パス(ASP)の統計情報をクリアするには、**clear asp** コマンドを使用します。

clear asp {**cluster counter** | **drop** [**flow** | **frame**] | **event dp-cp** | **queue-exhaustion** [**snapshot** *number*] | **load-balance history** | **overhead** | **table** [**arp** | **classify** | **filter** [**access-list** *acl_name*]]}

構文の説明

access-list *acl_name*	(任意)指定したアクセス リストのヒット カウンタだけをクリアします。
arp	(任意)ASP ARP テーブルのみでヒット カウンタをクリアします。
classify	(任意)ASP 分類テーブルのみでヒット カウンタをクリアします。
cluster counter	クラスタ カウンタをクリアします。
event	データ パスからコントロール プレーンへのイベントの統計情報をクリアします。
filter	(任意)ASP フィルタ テーブルのみでヒット カウンタをクリアします。
flow	(任意)ドロップされたフロー統計情報をクリアします。
frame	(任意)ドロップされたフレーム/パケット統計情報をクリアします。
load-balance history	パケット単位の ASP ロード バランシングの履歴をクリアし、自動切り替えが発生した回数をリセットします。
overhead	すべての ASP マルチプロセッサ オーバーヘッドの統計情報をクリアします。
queue-exhaustion	データ パス インスペクションの Snort キュー スナップショットをクリアします。
snapshot *number*	(任意)スナップショット ID 別にキューの枯渇をクリアします。
table	ASP ARP テーブルおよび ASP 分類テーブルのヒット カウンタをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(4)	**table** キーワードが追加されました。
8.2(2)	**filter** キーワードが追加されました。
9.3(1)	**load-balance history** キーワードが追加されました。

例

次に、すべての ASP テーブルの統計情報をクリアする例を示します。

```
ciscoasa# clear asp table

Warning: hits counters in asp arp and classify tables are cleared, which might impact the
hits statistic of other modules and output of other "show" commands!ciscoasa#clear asp
table arp
```

```
Warning: hits counters in asp arp table are cleared, which might impact the hits statistic
of other modules and output of other "show" commands!ciscoasa#clear asp table classify
Warning: hits counters in classify tables are cleared, which might impact the hits
statistic of other modules and output of other "show" commands!ciscoasa(config)# clear asp
table
Warning: hits counters in asp tables are cleared, which might impact the hits statistics
of other modules and output of other "show" commands!ciscoasa# sh asp table arp

Context: single_vf, Interface: inside 10.1.1.11 Active 00e0.8146.5212 hits 0

Context: single_vf, Interface: identity :: Active 0000.0000.0000 hits 0 0.0.0.0 Active
0000.0000.0000 hits 0
```

関連コマンド

コマンド	説明
asp load-balance per-packet	ロード バランシング動作を変更します。
show asp load-balance	ロード バランサのキュー サイズのヒストグラムを表示します。
show asp load-balance per-packet	現在のステータス、最高水準点と最低水準点、およびグローバルなしきい値を表示します。
show asp load-balance per-packet history	現在のステータス、最高水準点と最低水準点、グローバルなしきい値、最後のリセット以降のパケットごとの ASP ロード バランシングのオンとオフの切り替え回数、タイム スタンプ付きのパケットごとの ASP ロード バランシングの履歴、およびオンとオフを切り替えた理由を表示します。
show asp	ASP 統計情報を表示します。

clear bfd counters

BFD カウンタをクリアするには、特権 EXEC モードで **clear bfd counters** コマンドを使用します。

clear bfd counters [ld *local_discr* **|** *interface_name* **| ipv4** *ip-address* **| ipv6** *ipv6-address***]**

構文の説明

ld *local_discr*	（任意）指定したローカル識別子の BFD カウンタをクリアします（1 - 4294967295）。
interface_name	（任意）指定したインターフェイスの BFD カウンタをクリアします。
ipv4 *ip_address*	（任意）指定したネイバー IP アドレスの BFD カウンタをクリアします。
ipv6 *ip_address*	（任意）指定したネイバー IPv6 アドレスの BFD カウンタをクリアします。

デフォルト

このコマンドは、すべての BFD カウンタをクリアします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• —	• 対応	• 対応	• —

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

例

次に、すべての BFD カウンタをクリアする例を示します。

```
ciscoasa# clear bfd counters
```

関連コマンド

コマンド	説明
authentication	シングルホップ セッションとマルチホップ セッションの BFD テンプレートに認証を設定します。
bfd echo	インターフェイスで BFD エコー モードを有効にします。
bfd interval	インターフェイスにベースライン BFD パラメータを設定します。
bfd map	アドレスとマルチホップ テンプレートを関連付ける BFD マップを設定します。
bfd slow-timers	BFD スロー タイマー値を設定します。

コマンド	説明
bfd template	シングルホップ BFD テンプレートをインターフェイスにバインドします。
bfd-template single-hop | multi-hop	BFD テンプレートを設定し、BFD コンフィギュレーション モードを開始します。
echo	BFD シングルホップ テンプレートにエコーを設定します。
neighbor	BGP が登録され、BFD から転送パス検出失敗メッセージを受信できるように、BGP の BFD サポートを設定します。
show bfd drops	BFD でドロップされたパケットの数を表示します。
show bfd map	設定済みの BFD マップを表示します。
show bfd neighbors	既存の BFD 隣接関係の詳細なリストを表示します。
show bfd summary	BFD のサマリー情報を表示します。

clear bgp

ハードまたはソフト再構成を使用して Border Gateway Protocol（BGP）接続をリセットするには、特権 EXEC モードで **clear bgp** コマンドを使用します。

clear bgp {[***** | **external**] [**ipv4 unicast** [*as_number* | *neighbor_address* | **table-map**] | **ipv6 unicast** [*as_number* | *neighbor_address*]] [**soft**] [**in** | **out**] | *as_number* [**soft**] [**in** | **out**] | *neighbor_address* [**soft**] [**in** | **out**] | **table-map**}

構文の説明

*****	現在のすべての BGP セッションをリセットすることを指定します。
as_number	（任意）すべての BGP ピア セッションがリセットされる自律システムの番号。
external	外部のすべての BGP セッションをリセットすることを指定します。
in	（オプション）インバウンド再構成を開始します。**in** と **out** のどちらのキーワードも指定しない場合は、インバウンドとアウトバウンドの両方のセッションがリセットされます。
ipv4 unicast	IPv4 アドレス ファミリ セッションのハードまたはソフト再構成を使用して BGP 接続をリセットします。
ipv6 unicast	IPv6 アドレス ファミリ セッションのハードまたはソフト再構成を使用して BGP 接続をリセットします。
neighbor_address	（任意）指定された BGP ネイバーのみをリセットすることを指定します。この引数の値には、IPv4 アドレスまたは IPv6 アドレスを指定できます。
out	（オプション）インバウンド再構成またはアウトバウンド再構成を開始します。**in** と **out** のどちらのキーワードも指定しない場合は、インバウンドとアウトバウンドの両方のセッションがリセットされます。
soft	（任意）低速ピアのステータスを強制的にクリアして、元のアップデート グループに移します。
table-map	BGP ルーティング テーブルの table-map 設定情報をクリアします。このコマンドを使用して、BGP ポリシー アカウンティング機能で設定されたトラフィック インデックス情報をクリアできます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが導入されました。

使用上のガイドライン

clear bgp コマンドを使用して、ハード リセットまたはソフト再構成を開始できます。ハード リセットは、指定されたピアリング セッションを切断して再構築し、BGP ルーティング テーブルを再構築します。ソフト再構成は、保存されたプレフィックス情報を使用し、既存のピアリング セッションを切断せずに BGP ルーティング テーブルの再構成とアクティブ化を行います。ソフト再構成では、保存されているアップデート情報が使用されます。アップデートを保存するために追加のメモリが必要になりますが、ネットワークを中断せずに、新しい BGP ポリシーを適用することができます。ソフト再構成は、インバウンド セッション、またはアウトバウンド セッションに対して設定できます。

マルチ コンテキスト モードでは、**clear bgp *** コマンドだけがシステム実行スペースで使用可能です。

例

次の例では、システム実行スペースで **clear bgp** コマンドが指定されたときに、すべてのコンテキストですべての BGP セッションがリセットされます。このコマンドはすべての BGP セッションをリセットするため、アクションを確認する警告が表示されます。

```
ciscoasa# clear bgp *

This command will reset BGP in ALL contexts.
Are you sure you want to continue? [no]:
```

次の例では、すべての BGP セッションが、シングル モードまたはマルチ コンテキスト モードのコンテキストでリセットされます。

```
ciscoasa# clear bgp *
```

次の例では、ネイバー 10.100.0.1 とのインバウンド セッションに対してソフト再構成が開始され、アウトバウンド セッションは影響を受けません。

```
ciscoasa# clear bgp 10.100.0.1 soft in
```

次の例では、ルート リフレッシュ機能が BGP ネイバー ルータでイネーブルになっており、ネイバー 172.16.10.2 とのインバウンド セッションに対してソフト再構成が開始され、アウトバウンド セッションは影響を受けません。

```
ciscoasa# clear bgp 172.16.10.2 in
```

次の例では、自律システム番号 35700 のすべてのルータとのセッションに対してハード リセットが開始されます。

```
ciscoasa# clear bgp 35700
```

次の例では、すべてのインバウンド eBGP ピアリング セッションに対してソフト再構成が設定されます。

```
ciscoasa# clear bgp external soft in
```

次の例では、すべてのアウトバウンド アドレス ファミリ IPv4 マルチキャスト eBGP ピアリング セッションがクリアされます。

```
ciscoasa# clear bgp external ipv4 multicast out
```

次の例では、自律システム 65400 の IPv4 ユニキャスト アドレス ファミリ セッションで BGP ネイバーのインバウンド セッションに対してソフト再構成が開始され、アウトバウンド セッションは影響を受けません。

```
ciscoasa# clear bgp ipv4 unicast 65400 soft in
```

次の例では、asplain 表記の 4 バイトの自律システム番号 65538 の IPv4 ユニキャスト アドレス ファミリ セッションで BGP ネイバーに対してハード リセットが開始されます。

```
ciscoasa# clear bgp ipv4 unicast 65538
```

次の例では、asdot 表記の 4 バイトの自律システム番号 1.2 の IPv4 ユニキャスト アドレス ファミリ セッションで BGP ネイバーに対してハード リセットが開始されます。

```
ciscoasa# clear bgp ipv4 unicast 1.2
```

次の例は、IPv4 ユニキャスト ピアリング セッションのテーブル マップをクリアします。

```
ciscoasa# clear bgp ipv4 unicast table-map
```

clear blocks

枯渇状態や履歴情報などのパケット バッファ カウンタをリセットするには、特権 EXEC モードで **clear blocks** コマンドを使用します。

clear blocks [**exhaustion** {**history** | **snapshot**} | **export-failed** | **queue** [**history** [**core-local** [*number*]]]]

構文の説明

core-local [*number*]	（任意）すべてのコア、またはコア番号を指定する場合は特定のコアに対し、アプリケーションによってキューに入れられたシステム バッファをクリアします。
exhaustion	（任意）枯渇状態をクリアします。
export-failed	（任意）エクスポート失敗カウンタをクリアします。
history	（任意）履歴をクリアします。
queue	（任意）キューに入れられたブロックをクリアします。
snapshot	（任意）スナップショット情報をクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.1(5)	**history** および **snapshot** オプションが追加されました。

使用上のガイドライン

最低水準点カウンタを各プール内で現在使用可能なブロックにリセットします。また、このコマンドは、前回のバッファ割り当ての失敗時に保存された履歴情報をクリアします。

例

次に、ブロックをクリアする例を示します。

```
ciscoasa# clear blocks
```

関連コマンド

コマンド	説明
blocks	ブロック診断に割り当てるメモリを増やします。
show blocks	システム バッファの使用状況を表示します。

clear-button

WebVPN ユーザが ASA に接続したときに表示される WebVPN ページ ログイン フィールドの [Clear] ボタンをカスタマイズするには、カスタマイゼーション コンフィギュレーション モードで **clear-button** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

clear-button {**text** | **style**} *value*

no clear-button [{**text** | **style**}] *value*

構文の説明

style	スタイルを変更することを指定します。
text	テキストを変更することを指定します。
value	実際に表示するテキストまたは Cascading Style Sheet（CSS）パラメータ（それぞれ許容最大文字数は 256 です）。

デフォルト

デフォルトのテキストは「Clear」です。

デフォルトのスタイルは、border:1px solid black;background-color:white;font-weight:bold;font-size:80% です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
カスタマイゼーション コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、[Clear] ボタンのデフォルトの背景色を黒から青に変更する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# clear-button style background-color:blue
```

関連コマンド

コマンド	説明
group-prompt	WebVPN ページの Login フィールドのグループ プロンプトをカスタマイズします。
login-button	WebVPN ページの Login フィールドのログイン ボタンをカスタマイズします。
login-title	WebVPN ページの Login フィールドのタイトルをカスタマイズします。
password-prompt	WebVPN ページの Login フィールドのパスワード プロンプトをカスタマイズします。
username-prompt	WebVPN ページの Login フィールドのユーザ名プロンプトをカスタマイズします。

clear capture

キャプチャ バッファをクリアするには、特権 EXEC コンフィギュレーション モードで **clear capture** コマンドを使用します。

clear capture {**/all** | *capture_name*}

構文の説明

/all	すべてのインターフェイス上のパケットをクリアします。
capture_name	パケット キャプチャの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

誤ってすべてのパケット キャプチャを破棄することを防止するために、**clear capture** の短縮形（たとえば、**cl cap** や **clear cap**）は、サポートされていません。

例

次に、キャプチャ バッファ「example」のキャプチャ バッファをクリアする例を示します。

```
ciscoasa(config)# clear capture example
```

関連コマンド

コマンド	説明
capture	パケット スニッフィングおよびネットワーク障害の切り分けのためにパケット キャプチャ機能をイネーブルにします。
show capture	オプションが指定されていない場合は、キャプチャ コンフィギュレーションを表示します。

clear clns cache

Connectionless Network Service（CLNS）ルーティング キャッシュをクリアして再初期化するには、clear clns cache EXEC コマンドを使用します。

clear clns cache

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

使用上のガイドライン

ルーティング キャッシュ情報をクリアするには、**clear clns cache** コマンドを使用します。

例

次に、CLNS ルーティング キャッシュをクリアする例を示します。

```
ciscoasa# clear clns cache
```

関連コマンド

コマンド	説明
show clns cache	clns ルーティング キャッシュを表示します。

clear clns is-neighbors

隣接データベースから IS ネイバー情報を削除するには、clear clns is-neighbors EXEC コマンドを使用します。

clear clns is-neighbors

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドデフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

使用上のガイドライン

隣接データベースから IS ネイバー情報をクリアするには、**clear clns is-neighbors** コマンドを使用します。

例

次に、CLNS es-neighbor をクリアする例を示します。

```
ciscoasa# clear clns is-neighbors
```

関連コマンド

コマンド	説明
clear clns neighbors	clns ネイバー情報を削除します。
show clns is-neighbors	clns がネイバー情報であることを示します。

clear clns neighbors

隣接データベースから CLNS ネイバー情報を削除するには、clear clns neighbors EXEC コマンドを使用します。

clear clns neighbors

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドデフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

使用上のガイドライン

隣接データベースからネイバー情報をクリアするには、**clear clns neighbors** コマンドを使用します。

例

次に、隣接データベースから CLNS ネイバー情報を削除する例を示します。

```
ciscoasa# clear clns neighbors
```

関連コマンド

コマンド	説明
clear clns is-neighbors	clns is-neighbor 情報を削除します。
show clns neighbors	clns ネイバー情報を表示します。

clear clns route

動的に導出されたすべての CLNS ルーティング情報を削除するには、clear clns route EXEC コマンドを使用します。

clear clns route

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

使用上のガイドライン

ルーティング情報をクリアするには、**clear clns is-neighbors** コマンドを使用します。

例

次に、動的に導出されたすべての CLNS ルーティング情報を削除する例を示します。

```
ciscoasa# clear clns route
```

関連コマンド

コマンド	説明
show clns route	clns ルート情報を表示します。

clear cluster info

クラスタ統計情報をクリアするには、特権 EXEC モードで **clear cluster info** コマンドを使用します。

clear cluster info {flow-mobility counters | health details | trace | transport}

構文の説明

flow-mobility counters	クラスタ フローモビリティ カウンタをクリアします。
health details	クラスタ ヘルス情報をクリアします。
trace	クラスタ イベント トレース情報をクリアします。
transport	クラスタ転送統計情報をクリアします。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.5(2)	**flow-mobility counters** キーワードが追加されました。
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

クラスタ統計情報を表示するには、**show cluster info** コマンドを使用します。

例

次に、クラスタ イベント トレース情報をクリアする例を示します。

```
ciscoasa# clear cluster info trace
```

関連コマンド

コマンド	説明
show cluster info	クラスタ統計情報を表示します。

clear compression

すべての SVC および WebVPN の接続の圧縮統計情報をクリアするには、特権 EXEC モードで **clear compression** コマンドを使用します。

clear compression {**all** | **anyconnect-ssl** | **http-comp**}

構文の説明

all	すべての圧縮統計情報をクリアします。
http-comp	HTTP-COMP 統計情報をクリアします。
anyconnect-ssl	AnyConnect SSL 圧縮統計情報をクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
8.4(1)	SVC は AnyConnect SSL に置き換えられました。
9.5(2)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、ユーザの圧縮コンフィギュレーションをクリアする例を示します。

```
hostname# clear configure compression
```

関連コマンド

コマンド	説明
compression	すべての SVC 接続および WebVPN 接続の圧縮をイネーブルにします。
svc compression	特定のグループまたはユーザに対して、SVC 接続経由でのデータの圧縮をイネーブルにします。

CHAPTER 6

clear configuration session through clear isis コマンド

clear configuration session

コンフィギュレーション セッションを削除するには、グローバル コンフィギュレーション モードで **clear configuration session** コマンドを使用します。

clear configuration session [*session_name*]

構文の説明

session_name	既存のコンフィギュレーション セッションの名前。現在のセッションのリストを表示するには、**show configuration session** コマンドを使用します。このパラメータを省略した場合は、既存のすべてのセッションが削除されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、ACL やその他のオブジェクトを編集するために隔離されたセッションを作成する、**configure session** コマンドとともに使用します。作成したセッションが必要でなくなり、かつそのセッションで定義した変更をコミットしない場合は、このコマンドを使用してセッションおよび含まれている変更を削除します。

セッションは削除しないで、セッションで加えた変更をクリアするのみの場合は、このコマンドではなく **clear session** コマンドを使用します。

例

次に、old-session という名前のセッションを削除する例を示します。

```
ciscoasa(config)# clear configuration session old-session
```

関連コマンド

コマンド	説明
clear session	コンフィギュレーション セッションの内容をクリアするか、そのアクセス フラグをリセットします。
configure session	セッションを作成するか、開きます。
show configuration session	現在の各セッションで行われた変更を表示します。

clear configure

実行コンフィギュレーションをクリアするには、グローバル コンフィギュレーション モードで **clear configure** コマンドを使用します。

clear configure {**primary** | **secondary** | **all** | *command*}

構文の説明

all	実行コンフィギュレーション全体をクリアします。
command	指定したコマンドのコンフィギュレーションをクリアします。使用可能なコマンドについては、**clear configure ?** コマンドを使用して CLI ヘルプを確認してください。
primary	フェールオーバー ペアの場合に、プライマリ ユニットのコンフィギュレーションをクリアします。
secondary	フェールオーバー ペアの場合に、セカンダリ ユニットのコンフィギュレーションをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドをセキュリティ コンテキストで入力すると、コンテキスト コンフィギュレーションだけがクリアされます。このコマンドをシステム実行スペースで入力すると、システム実行コンフィギュレーションと、すべてのコンテキスト実行コンフィギュレーションがクリアされます。システム コンフィギュレーション内のすべてのコンテキスト エントリがクリアされるため（**context** コマンドを参照）、コンテキストは実行されなくなり、コンテキスト実行スペースに移動できなくなります。

コンフィギュレーションをクリアする前に、（スタートアップ コンフィギュレーションの場所を指定する）**boot config** コマンドへのすべての変更をスタートアップ コンフィギュレーションに必ず保存してください。スタートアップ コンフィギュレーションの場所を実行コンフィギュレーション内だけで変更した場合、再起動時にコンフィギュレーションはデフォルトの場所からロードされます。

（注） **clear configure all** コマンドを入力した場合、パスワードの暗号化で使用されるマスター パス フレーズは削除されません。マスター パス フレーズの詳細については、**config key password-encryption** コマンドを参照してください。

例

次に、実行コンフィギュレーション全体をクリアする例を示します。

```
ciscoasa(config)# clear configure all
```

次に、AAA コンフィギュレーションをクリアする例を示します。

```
ciscoasa(config)# clear configure aaa
```

関連コマンド

コマンド	説明
show running-config	実行コンフィギュレーションを表示します。

clear conn

特定の接続または複数の接続をクリアするには、特権 EXEC モードで **clear conn** コマンドを使用します。

clear conn [**all**] [**protocol** {**tcp** | **udp** | **sctp**}] [**address** *src_ip*[**-***src_ip*] [**netmask** *mask*]] [**port** *src_port*[**-***src_port*]] [**address** *dest_ip*[**-***dest_ip*] [**netmask** *mask*]] [**port** *dest_port*[**-***dest_port*] [**user** [*domain_nickname*\\]*user_name* | **user-group** [*domain_nickname*\\]*user_group_name*] | **zone** [*zone_name*]] [**data-rate**]

構文の説明

address	(任意)指定された送信元または宛先の IP アドレスとの接続をクリアします。
all	(任意)to-the-box 接続を含む、すべての接続をクリアします。**all** キーワードを指定しない場合は、through-the-box 接続だけがクリアされます。
dest_ip	(任意)宛先 IP アドレス(IPv4 または IPv6)を指定します。範囲を指定するには、IP アドレスをダッシュ(-)で区切ります。次に例を示します。 `10.1.1.1-10.1.1.5`
dest_port	(任意)宛先ポート番号を指定します。範囲を指定するには、ポート番号をダッシュ(-)で区切ります。次に例を示します。 `1000-2000`
netmask *mask*	(任意)指定された IP アドレスで使用するサブネット マスクを指定します。
port	(任意)指定された送信元または宛先のポートとの接続をクリアします。
protocol {tcp | udp | sctp}	(任意)指定されたプロトコルを持つ接続をクリアします。
src_ip	(任意)送信元 IP アドレス(IPv4 または IPv6)を指定します。範囲を指定するには、IP アドレスをダッシュ(-)で区切ります。次に例を示します。 `10.1.1.1-10.1.1.5`
src_port	(任意)送信元ポートの番号を指定します。範囲を指定するには、ポート番号をダッシュ(-)で区切ります。次に例を示します。 `1000-2000`
user [*domain_nickname*\\]*user_name*	(オプション)指定したユーザに所属する接続をクリアします。*domain_nickname* 引数を含めない場合、ASA はデフォルト ドメイン内のユーザの接続をクリアします。
user-group [*domain_nickname*\\]*user_group_name*	(オプション)指定したユーザ グループに所属する接続をクリアします。*domain_nickname* 引数を含めない場合、ASA はデフォルト ドメイン内のユーザ グループの接続をクリアします。
zone [*zone_name*]	トラフィック ゾーンに所属する接続をクリアします。
data-rate	(任意)保存されている現在の最大データレートをクリアします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(8)/7.2(4)/8.0(4)	このコマンドが追加されました。
8.4(2)	アイデンティティ ファイアウォールをサポートするための **user** および **user-group** キーワードが追加されました。
9.3(2)	**zone** キーワードが追加されました。
9.5(2)	**protocol sctp** キーワードが追加されました。
9.14(1)	**data-rate** keyword キーワードが追加されました。

使用上のガイドライン

このコマンドは IPv4 および IPv6 のアドレスをサポートします。

コンフィギュレーションに対してセキュリティ ポリシーの変更を加えた場合は、すべての*新しい*接続で新しいセキュリティ ポリシーが使用されます。既存の接続では、その接続が確立された時点で設定されていたポリシーの使用が続行されます。すべての接続で新しいポリシーが確実に使用されるようにするには、**clear conn** コマンドを使用して、現在の接続を切断し、新しいポリシーを使用して再接続できるようにする必要があります。または、ホスト単位で接続をクリアするための **clear local-host** コマンドを使用したり、ダイナミック NAT を使用する接続用の **clear xlate** コマンドを使用したりできます。

ASA が、セカンダリ接続を許可するためのピンホールを作成している場合には、これが **show conn** コマンドの出力に不完全な接続として表示されます。この不完全な接続をクリアするには、**clear conn** コマンドを使用します。

例

次に、すべての接続を表示し、10.10.10.108:4168 と 10.0.8.112:22 の間の管理接続をクリアする例を示します。

```
ciscoasa# show conn all
TCP mgmt 10.10.10.108:4168 NP Identity Ifc 10.0.8.112:22, idle 0:00:00, bytes 3084, flags
UOB

ciscoasa# clear conn address 10.10.10.108 port 4168 address 10.0.8.112 port 22
```

次の例では、拡張メモリに保存されている接続の最大データレートをクリアする方法について示します。

```
ciscoasa# clear conn data-rate
Released conn extension memory for 10 connection(s)
```

関連コマンド

コマンド	説明
clear local-host	特定のローカル ホストまたはすべてのローカル ホストによるすべての接続をクリアします。
clear xlate	ダイナミック NAT セッションおよび NAT を使用しているすべての接続をクリアします。
show conn	接続情報を表示します。
show local-host	ローカル ホストのネットワーク状態を表示します。
show xlate	NAT セッションを表示します。

clear console-output

現在キャプチャされているコンソール出力を削除するには、特権 EXEC モードで **clear console-output** コマンドを使用します。

clear console-output

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、現在キャプチャされているコンソール出力を削除する例を示します。

```
ciscoasa# clear console-output
```

関連コマンド

コマンド	説明
console timeout	ASA に対するコンソール接続のアイドル タイムアウトを設定します。
show console-output	キャプチャされているコンソール出力を表示します。
show running-config console timeout	ASA に対するコンソール接続のアイドル タイムアウトを表示します。

clear coredump

コアダンプ ログをクリアするには、グローバル コンフィギュレーション モードで **clear coredump** コマンドを使用します。

clear coredump

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトでは、コアダンプはイネーブルではありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	

(注) 4100/9300 プラットフォームで動作している ASA の場合は、ブートストラップ CLI モードを使用してコアダンプを処理します。

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、コアダンプ ファイル システムの内容およびコアダンプ ログを削除します。コアダンプ ファイル システムは、元の状態のままです。現在のコアダンプ コンフィギュレーションは変更されないままです。

例

次に、コアダンプ ファイル システムの内容およびコアダンプ ログを削除する例を示します。

```
ciscoasa(config)# clear coredump
Proceed with removing the contents of the coredump filesystem on 'disk0:' [confirm]
```

関連コマンド

コマンド	説明
coredump enable	コアダンプ機能をイネーブルにします。
clear configure coredump	コアダンプ ファイル システムとコアダンプ ファイル システムの内容をシステムから削除します。
show coredump filesystem	コアダンプ ファイル システム上のファイルを表示します。
show coredump log	コアダンプ ログを表示します。

clear counters

プロトコル スタック カウンタをクリアするには、グローバル コンフィギュレーション モードで **clear counters** コマンドを使用します。

clear counters [all | context *context-name* **| summary | top** *n* **] [detail] [protocol** *protocol_name* [*counter_name*]] [**threshold** *n*]

構文の説明

all	(任意)すべてのフィルタ詳細をクリアします。
context *context-name*	(任意)コンテキスト名を指定します。
counter_name	(任意)名前でカウンタを指定します。どのカウンタが使用可能かを確認するには、**show counters protocol** コマンドを使用します。
detail	(任意)カウンタの詳細情報をクリアします。
protocol *protocol_name*	(任意)指定したプロトコルのカウンタをクリアします。
summary	(任意)カウンタの要約をクリアします。
threshold *n*	(任意)指定されたしきい値以上になっているカウンタをクリアします。指定できる範囲は 1 ～ 4294967295 です。
top *n*	(任意)指定されたしきい値以上になっているカウンタをクリアします。指定できる範囲は 1 ～ 4294967295 です。

デフォルト

clear counters summary detail コマンドがデフォルトです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、プロトコル スタック カウンタをクリアする例を示します。

```
ciscoasa(config)# clear counters
```

関連コマンド

コマンド	説明
show counters	プロトコル スタック カウンタを表示します。

clear cpu profile

CPU プロファイリングの統計情報をクリアするには、特権 EXEC モードで **clear cpu profile** コマンドを使用します。

clear cpu profile

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、クラッシュ ファイルを削除する例を示します。

```
ciscoasa# clear cpu profile
```

関連コマンド

show cpu	CPU に関する情報を表示します。
show cpu profile	CPU プロファイリング データを表示します。

clear crashinfo

フラッシュ メモリに保存されたすべてのクラッシュ情報ファイルを削除するには、特権 EXEC モードで **clear crashinfo** コマンドを使用します。

clear crashinfo [**module** {**0** | **1**}]

構文の説明

module {**0** | **1**}	（任意）スロット 0 または 1 のモジュールのクラッシュ ファイルをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.7(1)	フラッシュ メモリに書き込まれたすべてのクラッシュ情報ファイルを削除するように出力が更新されました。

例

次に、クラッシュ ファイルを削除する例を示します。

```
ciscoasa# clear crashinfo
```

関連コマンド

crashinfo force	ASA を強制的にクラッシュさせます。
crashinfo save disable	クラッシュ情報のフラッシュ メモリへの書き込みをディセーブルにします。
crashinfo test	ASA でフラッシュ メモリ内のファイルにクラッシュ情報を保存できるかどうかをテストします。
show crashinfo	フラッシュ メモリに格納されている最新のクラッシュ情報ファイルの内容を表示します。
show crashinfo files	最後の 5 つのクラッシュ情報ファイルを日付とタイムスタンプに基づいて表示します。

clear crypto accelerator statistics

クリプト アクセラレータ MIB からグローバルな統計情報およびアクセラレータ固有の統計情報をクリアするには、特権 EXEC モードで **clear crypto accelerator statistics** コマンドを使用します。

clear crypto accelerator statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、グローバル コンフィギュレーション モードで、クリプト アクセラレータの統計情報を表示する例を示します。

```
ciscoasa(config)# clear crypto accelerator statistics
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear crypto protocol statistics	暗号アクセラレータ MIB にあるプロトコル固有の統計情報をクリアします。
show crypto accelerator statistics	暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報を表示します。
show crypto protocol statistics	暗号アクセラレータ MIB からプロトコル固有の統計情報を表示します。

clear crypto ca crls

指定したトラストポイントに関連付けられたすべての CRL キャッシュをクリアするか、trustpool に関連付けられたすべての CRL をキャッシュからクリアするか、またはすべての CRL のキャッシュをクリアするには、特権 EXEC モードで **clear crypto ca crls** コマンドを使用します。

clear crypto ca crls [**trustpool** | **trustpoint** *trust_point_name*]

構文の説明

trustpoint *trust_point_name*	トラストポイントの名前。名前を指定しない場合、このコマンドはシステム上のキャッシュされた CRL をすべてクリアします。*trust_point_name* を指定せず trustpoint キーワードを指定した場合、コマンドは失敗します。
trustpool	trustpool 内の証明書に関連付けられた CRL にのみアクションが適用されることを示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

例

次に、特権 EXEC コンフィギュレーション モードで、ASA からすべての trustpool CRL を削除する例、trustpoint123 に関連付けられた CLR を削除する例、およびすべての CRL を削除する例を個別に示します。

```
ciscoasa# clear crypto ca crl trustpool
ciscoasa# clear crypto ca crl trustpoint trustpoint123
ciscoasa# clear crypto ca crl
```

関連コマンド

コマンド	説明
crypto ca crl request	トラストポイントの CRL コンフィギュレーションに基づいて CRL をダウンロードします。
show crypto ca crl	キャッシュされたすべての CRL、または指定したトラストポイントのキャッシュされた CRL を表示します。

clear crypto ca trustpool

trustpool からすべての証明書を削除するには、特権 EXEC モードで **clear crypto ca trustpool** コマンドを使用します。

clear crypto ca trustpool [**noconfirm**]

構文の説明

noconfirm	（任意）ユーザ確認プロンプトを抑制し、コマンドが要求どおりに処理されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応		—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

ユーザは、このアクションを実行する前に確認を求められます。

例

次に、すべての証明書をクリアする例を示します。

```
ciscoasa# clear crypto ca trustpool
You are about to clear the trusted certificate pool. Do you want to continue? (y/n) y
ciscoasa#
```

関連コマンド

コマンド	説明
crypto ca trustpool export	PKI trustpool を構成する証明書をエクスポートします。
crypto ca trustpool import	PKI trustpool を構成する証明書をインポートします。
crypto ca trustpool remove	指定された 1 つの証明書を trustpool から削除します。

clear crypto ikev1

IPsec IKEv1 の SA または統計情報を削除するには、特権 EXEC モードで **clear crypto ikev1** コマンドを使用します。すべての IKEv1 SA をクリアするには、このコマンドを引数なしで使用します。

clear crypto ikev1 {**sa** *ip_address* | **stats**}

構文の説明

sa *ip_address*	SA をクリアします。
stats	IKEv1 統計情報をクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

すべての IPsec IKEv1 SA をクリアするには、このコマンドを引数なしで使用します。

例

次に、ASA からすべての IPsec IKEv1 統計情報を削除する例を示します。

```
ciscoasa# clear crypto ikev1 stats
ciscoasa#
```

次に、10.86.1.1 のピア IP アドレスを持つ SA を削除する例を示します。

```
ciscoasa# clear crypto ikev1 sa peer 10.86.1.1
ciscoasa#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてまたは指定されたクリプト マップをコンフィギュレーションからクリアします。
clear configure isakmp	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
show ipsec sa	カウンタ、エントリ、マップ名、ピア IP アドレス、ホスト名などの IPSec SA に関する情報を表示します。
show running-config crypto	IPsec、クリプト マップ、ダイナミック クリプト マップ、ISAKMP など、暗号コンフィギュレーション全体を表示します。

clear crypto ikev2

IPsec IKEv2 の SA または統計情報を削除するには、特権 EXEC モードで **clear crypto ikev2** コマンドを使用します。すべての IKEv2 SA をクリアするには、このコマンドを引数なしで使用します。

clear crypto ikev2 {**sa** *ip_address* | **stats**}

構文の説明

sa *ip_address*	SA をクリアします。
stats	IKEv2 統計情報をクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

すべての IPsec IKEv2 SA をクリアするには、このコマンドを引数なしで使用します。

例

次に、ASA からすべての IPsec IKEv2 統計情報を削除する例を示します。

```
ciscoasa# clear crypto ikev2 stats
ciscoasa#
```

次に、10.86.1.1 のピア IP アドレスを持つ SA を削除する例を示します。

```
ciscoasa# clear crypto ikev2 sa peer 10.86.1.1
ciscoasa#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてまたは指定されたクリプト マップをコンフィギュレーションからクリアします。
clear configure isakmp	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
show ipsec sa	カウンタ、エントリ、マップ名、ピア IP アドレス、ホスト名などの IPsec SA に関する情報を表示します。
show running-config crypto	IPsec、クリプト マップ、ダイナミック クリプト マップ、ISAKMP など、暗号コンフィギュレーション全体を表示します。

clear crypto ipsec sa

IPsec SA のカウンタ、エントリ、クリプト マップ、またはピア接続を削除するには、特権 EXEC モードで **clear crypto ipsec sa** コマンドを使用します。すべての IPsec SA をクリアするには、このコマンドを引数なしで使用します。

clear crypto ipsec sa [counters | entry *ip_address* **{esp | ah}** *spi* **| map** *map name* **| peer** *ip_address***]**

構文の説明

ah	認証ヘッダー。
counters	各 SA 統計情報のすべての IPsec をクリアします。
entry *ip_address*	指定した IP アドレス、ホスト名、プロトコル、および SPI 値に一致するトンネルを削除します。
esp	暗号化セキュリティ プロトコル。
map *map name*	マップ名で識別される、指定したクリプト マップに関連付けられているすべてのトンネルを削除します。
peer *ip_address*	指定したホスト名または IP アドレスで識別されるピアへのすべての IPsec SA を削除します。
spi	セキュリティ パラメータ インデックス（16 進数）を指定します。受信 SPI である必要があります。このコマンドは、送信 SPI ではサポートされていません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

すべての IPsec SA をクリアするには、このコマンドを引数なしで使用します。

例

次に、ASA からすべての IPsec SA を削除する例を示します。

```
ciscoasa# clear crypto ipsec sa
ciscoasa#
```

次に、10.86.1.1 のピア IP アドレスを持つ SA を削除する例を示します。

```
ciscoasa# clear crypto ipsec peer 10.86.1.1
ciscoasa#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてまたは指定されたクリプト マップをコンフィギュレーションからクリアします。
clear configure isakmp	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
show ipsec sa	カウンタ、エントリ、マップ名、ピア IP アドレス、ホスト名などの IPsec SA に関する情報を表示します。
show running-config crypto	IPsec、クリプト マップ、ダイナミック クリプト マップ、ISAKMP など、暗号コンフィギュレーション全体を表示します。

clear crypto isakmp

ISAKMP SA または統計情報をクリアするには、特権 EXEC モードで **clear crypto isakmp** コマンドを使用します。

clear crypto isakmp [**sa** | **stats**]

構文の説明

sa	IKEv1 および IKEv2 SA をクリアします。
stats	IKEv1 および IKEv2 統計情報をクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

すべての ISAKMP 運用データをクリアするには、このコマンドを引数なしで使用します。

例

次に、すべての ISAKMP SA を削除する例を示します。

```
ciscoasa# clear crypto isakmp sa
ciscoasa#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてまたは指定されたクリプト マップをコンフィギュレーションからクリアします。
clear configure isakmp	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。

コマンド	説明
show isakmp	ISAKMP 運用データに関する情報を表示します。
show running-config crypto	IPsec、クリプト マップ、ダイナミック クリプト マップ、ISAKMP など、暗号コンフィギュレーション全体を表示します。

clear crypto protocol statistics

クリプト アクセラレータ MIB 内のプロトコル固有の統計情報をクリアするには、特権 EXEC モードで **clear crypto protocol statistics** コマンドを使用します。

clear crypto protocol statistics *protocol*

構文の説明

protocol	統計情報をクリアするプロトコルの名前を指定します。プロトコルの選択肢は次のとおりです。 • **all**：現在サポートされているすべてのプロトコル。 • **ikev1**：インターネット キー エクスチェンジ（IKE）バージョン 1 • **ikev2**：インターネット キー エクスチェンジ（IKE）バージョン 2 • **ipsec-client**：IP Security（IPsec）フェーズ 2 プロトコル • **other**：新規プロトコル用に予約済み。 • **srtp**：RTP（SRTP）プロトコル • **ssh**：セキュア シェル（SSH）プロトコル • **ssl-client**：セキュア ソケット レイヤ（SSL）プロトコル

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(1)	**ikev1** および **ikev2** キーワードが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、すべての暗号化アクセラレータ統計情報をクリアする例を示します。

```
ciscoasa# clear crypto protocol statistics all
ciscoasa#
```

関連コマンド

コマンド	説明
clear crypto accelerator statistics	暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報をクリアします。
show crypto accelerator statistics	暗号アクセラレータ MIB からグローバルおよびアクセラレータ固有の統計情報を表示します。
show crypto protocol statistics	クリプト アクセラレータ MIB のプロトコル固有の統計情報を表示します。

clear crypto ssl

SSL 情報をクリアするには、特権 EXEC モードで **clear crypto ssl** コマンドを使用します。

clear crypto ssl {**cache** [**all**] | **errors** | **mib** | **objects**}

構文の説明

cache	SSL セッション キャッシュ内の期限切れセッションをクリアします。
all	(任意)SSL セッション キャッシュ内のすべてのセッションおよび統計情報をクリアします。
errors	SSL エラーをクリアします。
mib	SSL MIB 統計情報をクリアします。
objects	SSL オブジェクト統計情報をクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、すべての SSL キャッシュ セッションおよび統計情報をクリアする例を示します。

```
ciscoasa# clear crypto ssl cache all
ciscoasa#
```

関連コマンド

コマンド	説明
show crypto ssl	SSL 情報を表示します。

clear cts

Cisco TrustSec と統合したときに ASA によって使用されたデータをクリアするには、グローバル コンフィギュレーション モードで **clear cts** コマンドを使用します。

clear cts {**environment-data** | **pac**} [**noconfirm**]

構文の説明

noconfirm	確認を求めずにデータをクリアします。
environment-data	Cisco ISE からダウンロードされたすべての CTS 環境データをクリアします。
pac	NVRAM に保存されている CTS PAC 情報をクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

環境データをクリアすると、次回の環境データの更新を手動でトリガーできます。また、リフレッシュ タイマーが期限切れになると、システムによってデータが更新されます。環境データをクリアしても、Cisco TrustSec PAC はシステムから削除されませんが、トラフィック ポリシーに影響を与えます。

保存された PAC をクリアする前に、システムでは、PAC を使用しないと、Cisco TrustSec 環境データをダウンロードできないことを理解してください。ただし、システムにすでに存在する環境データが引き続き使用されます。**clear cts pac** コマンドを実行すると、システムが環境データのアップデートを取得できなります。

クラスタでは、このコマンドはマスター ユニットのみで使用できます。アクティブ/スタンバイ ハイ アベイラビリティ（フェールオーバー）では、このコマンドはアクティブ ユニットのみで使用できます。

例

次に、システムから CTS データをクリアする例を示します。

```
ciscoasa# clear cts pac
Are you sure you want to delete the cts PAC? (y/n) y

ciscoasa# clear cts environment-data
Are you sure you want to delete the cts environment data? (y/n) y
```

関連コマンド

コマンド	説明
clear configure cts	ASA と Cisco TrustSec を統合するためのコンフィギュレーションをクリアします。
cts sxp enable	ASA で SXP プロトコルをイネーブルにします。
show cts	Cisco TrustSec（CTS）情報を表示します。

clear dhcpd

DHCP サーバのバインディングおよび統計情報をクリアするには、特権 EXEC モードで **clear dhcp** コマンドを使用します。

clear dhcpd {**binding** [**all** | *ip_address*] | **statistics**}

構文の説明

all	（任意）すべての dhcpd バインディングをクリアします。
binding	クライアント アドレスのすべてのバインディングをクリアします。
ip_address	（任意）指定した IP アドレスのバインディングをクリアします。
statistics	統計情報カウンタをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

オプションの IP アドレスを **clear dhcpd binding** コマンドに含めた場合は、その IP アドレスのバインディングだけがクリアされます。

すべての DHCP サーバ コマンドをクリアするには、**clear configure dhcpd** コマンドを使用します。

例

次に、**dhcpd** 統計情報をクリアする例を示します。

```
ciscoasa# clear dhcpd statistics
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
show dhcpd	DHCP のバインディング、統計情報、または状態情報を表示します。

clear dhcprelay statistics

DHCP リレー統計情報カウンタをクリアするには、特権 EXEC モードで **clear dhcprelay statistics** コマンドを使用します。

clear dhcprelay statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

clear dhcprelay statistics コマンドは、DHCP リレー統計情報カウンタだけをクリアします。DHCP リレー コンフィギュレーション全体をクリアするには、**clear configure dhcprelay** コマンドを使用します。

例

次に、DHCP リレー統計情報をクリアする例を示します。

```
ciscoasa# clear dhcprelay statistics
ciscoasa#
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
debug dhcprelay	DHCP リレー エージェントのデバッグ情報を表示します。
show dhcprelay statistics	DHCP リレー エージェントの統計情報を表示します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

clear dns

指定された完全修飾ドメイン名（FQDN）ホストに関連付けられたすべての IP アドレスをクリアするには、特権 EXEC モードで **clear dns** コマンドを使用します。

clear dns [**host** *fqdn_name*]

構文の説明

fqdn_name	（オプション）選択されたホストの完全修飾ドメイン名を指定します。
host	（オプション）指定したホストの IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

例

次に、指定した FQDN ホストに関連付けられた IP アドレスをクリアする例を示します。

```
ciscoasa# clear dns 10.1.1.2 www.example.com
```

（注） **dns expire-entry** キーワードの設定は、このコマンドでは無視されます。新しい DNS クエリーは、アクティブ化された各 FQDN ホストに送信されます。

関連コマンド

コマンド	説明
dns domain-lookup	ASA によるネーム ルックアップの実行をイネーブルにします。
dns name-server	DNS サーバ アドレスを設定します。
dns retries	ASA が応答を受信しないときに、DNS サーバのリストを再試行する回数を指定します。
dns timeout	次の DNS サーバを試行するまでに待機する時間を指定します。
show dns-hosts	DNS キャッシュを表示します。

clear dns-hosts cache

DNS キャッシュをクリアするには、特権 EXEC モードで **clear dns-hosts cache** コマンドを使用します。

clear dns-hosts cache

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、**name** コマンドで追加したスタティック エントリをクリアしません。

例

次に、DNS キャッシュをクリアする例を示します。

```
ciscoasa# clear dns-hosts cache
```

関連コマンド

コマンド	説明
dns domain-lookup	ASA によるネーム ルックアップの実行をイネーブルにします。
dns name-server	DNS サーバ アドレスを設定します。
dns retries	ASA が応答を受信しないときに、DNS サーバのリストを再試行する回数を指定します。
dns timeout	次の DNS サーバを試行するまでに待機する時間を指定します。
show dns-hosts	DNS キャッシュを表示します。

clear dynamic-filter dns-snoop

ボットネット トラフィック フィルタの DNS スヌーピング データをクリアするには、特権 EXEC モードで **clear dynamic-filter dns-snoop** コマンドを使用します。

clear dynamic-filter dns-snoop

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

例

次に、ボットネット トラフィック フィルタの DNS スヌーピング データをすべてクリアする例を示します。

```
ciscoasa# clear dynamic-filter dns-snoop
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。

コマンド	説明
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。

コマンド	説明
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

clear dynamic-filter reports

ボットネット トラフィック フィルタのレポート データをクリアするには、特権 EXEC モードで **clear dynamic-filter reports** コマンドを使用します。

clear dynamic-filter reports {**top** [**malware-sites** | **malware-ports** | **infected-hosts**] | **infected-hosts**}

構文の説明

malware-ports	(任意) 上位 10 のマルウェア ポートのレポート データをクリアします。
malware-sites	(任意) 上位 10 のマルウェア サイトのレポート データをクリアします。
infected-hosts (**top**)	(任意) 上位 10 の感染したホストのレポート データをクリアします。
top	上位 10 のマルウェア サイト、ポート、および感染したホストのレポート データをクリアします。
infected-hosts	感染したホストのレポート データをクリアします。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。
8.2(2)	**botnet-sites** キーワードおよび **botnet-ports** キーワードは **malware-sites** および **malware-ports** に変更されました。**top** キーワードが、上位 10 のレポートのクリアを、感染したホストに関する新しいレポートのクリアと区別するために追加されました。**infected-hosts** キーワードが追加されました (**top** なし)。

例

次に、すべてのボットネット トラフィック フィルタの上位 10 のレポート データをクリアする例を示します。

```
ciscoasa# clear dynamic-filter reports top
```

次に、上位 10 のマルウェア サイトのレポート データだけをクリアする例を示します。

```
ciscoasa# clear dynamic-filter reports top malware-sites
```

次に、感染したホストのすべてのレポート データをクリアする例を示します。

```
ciscoasa# clear dynamic-filter reports infected-hosts
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。

コマンド	説明
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter reports infected-hosts	感染ホストのレポートを生成します。
show dynamic-filter reports top	マルウェア サイト、ポート、および感染ホストの上位 10 件のレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

clear dynamic-filter statistics

ボットネット トラフィック フィルタの統計情報をクリアするには、特権 EXEC モードで **clear dynamic-filter statistics** コマンドを使用します。

clear dynamic-filter statistics [**interface** *name*]

構文の説明

interface *name*	（任意）特定のインターフェイスの統計情報をクリアします。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

例

次に、ボットネット トラフィック フィルタの DNS 統計情報をすべてクリアする例を示します。

```
ciscoasa# clear dynamic-filter statistics
```

関連コマンド

コマンド	説明
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。

コマンド	説明
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter reports infected-hosts	感染ホストのレポートを生成します。
show dynamic-filter reports top	マルウェア サイト、ポート、および感染ホストの上位 10 件のレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

clear eigrp events

EIGRP イベント ログをクリアするには、特権 EXEC モードで **clear eigrp events** コマンドを使用します。

clear eigrp [*as-number*] **events**

構文の説明

as-number	（任意）イベント ログをクリアする EIGRP プロセスの自律システム番号を指定します。ASA でサポートされる EIGRP ルーティング プロセスは 1 つだけであるため、自律システム番号（プロセス ID）を指定する必要はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードはサポートされます。

使用上のガイドライン

show eigrp events コマンドを使用して、EIGRP イベント ログを表示できます。

例

次に、EIGRP イベント ログをクリアする例を示します。

```
ciscoasa# clear eigrp events
```

関連コマンド

コマンド	説明
show eigrp events	EIGRP イベント ログを表示します。

clear eigrp neighbors

EIGRP ネイバー テーブルからエントリを削除するには、特権 EXEC モードで **clear eigrp neighbors** コマンドを使用します。

clear eigrp [*as-number*] **neighbors** [*ip-addr* | *if-name*] [**soft**]

構文の説明

as-number	（任意）ネイバー エントリを削除する EIGRP プロセスの自律システム番号を指定します。ASA でサポートされる EIGRP ルーティング プロセスは 1 つだけであるため、自律システム番号（AS）（プロセス ID）を指定する必要はありません。
if-name	（任意）**nameif** コマンドで指定されたインターフェイスの名前。インターフェイス名を指定すると、このインターフェイスを介して学習されたすべてのネイバー テーブル エントリが削除されます。
ip-addr	（任意）ネイバー テーブルから削除するネイバーの IP アドレス。
soft	ASA は、隣接関係をリセットすることなくネイバーと再同期されます。

デフォルト

ネイバー IP アドレスまたはインターフェイス名を指定しない場合は、すべてのダイナミック エントリがネイバー テーブルから削除されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

clear eigrp neighbors コマンドは、**neighbor** コマンドを使用して定義されたネイバーをネイバー テーブルから削除しません。ダイナミックに検出されたネイバーだけが削除されます。

show eigrp neighbors コマンドを使用して、EIGRP ネイバー テーブルを表示できます。

例

次に、EIGRP ネイバー テーブルからすべてのエントリを削除する例を示します。

```
ciscoasa# clear eigrp neighbors
```

次に、「outside」という名前のインターフェイスを介して学習されたすべてのエントリを EIGRP ネイバー テーブルから削除する例を示します。

```
ciscoasa# clear eigrp neighbors outside
```

関連コマンド

コマンド	説明
debug eigrp neighbors	EIGRP ネイバーのデバッグ情報を表示します。
debug ip eigrp	EIGRP プロトコル パケットのデバッグ情報を表示します。
show eigrp neighbors	EIGRP ネイバー テーブルを表示します。

clear eigrp topology

EIGRP トポロジ テーブルからエントリを削除するには、特権 EXEC モードで **clear eigrp topology** コマンドを使用します。

clear eigrp [*as-number*] **topology** *ip-addr* [*mask*]

構文の説明

as-number	(任意)EIGRP プロセスの自律システム番号を指定します。ASA でサポートされる EIGRP ルーティング プロセスは 1 つだけであるため、自律システム番号(AS)(プロセス ID)を指定する必要はありません。
ip-addr	トポロジ テーブルからクリアする IP アドレス。
mask	(任意)*ip-addr* 引数に適用するネットワーク マスク。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

このコマンドは、EIGRP トポロジ テーブルから既存の EIGRP エントリをクリアします。**show eigrp topology** コマンドを使用して、トポロジ テーブルのエントリを表示できます。

例

次に、EIGRP トポロジ テーブルから 192.168.1.0 ネットワークのエントリを削除する例を示します。

```
ciscoasa# clear eigrp topology 192.168.1.0 255.255.255.0
```

関連コマンド

コマンド	説明
show eigrp topology	EIGRP トポロジ テーブルを表示します。

clear facility-alarm output

ISA 3000 で出力リレーの電源を切って、LED のアラーム状態をクリアするには、特権 EXEC モードで **clear facility-alarm output** コマンドを使用します。

clear facility-alarm output

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、出力リレーの電源を切り、出力 LED のアラーム状態をクリアします。これにより、外部アラームがオフになります。ただし、このコマンドを実行しても、外部アラームをトリガーしたアラーム条件は修正されません。問題を解決する必要があります。現在のアラーム条件を確認するには、**show facility-alarm status** コマンドを使用します。

例

次に、出力リレーの電源を切り、出力 LED のアラーム状態をクリアする例を示します。

```
ciscoasa(config)# clear facility-alarm output
```

関連コマンド

コマンド	説明
alarm contact description	アラーム入力の説明を指定します。
alarm contact severity	アラームの重大度を指定します。
alarm contact trigger	1 つまたはすべてのアラーム入力のトリガーを指定します。

コマンド	説明
alarm facility input-alarm	アラーム入力のロギング オプションと通知オプションを指定します。
alarm facility power-supply rps	電源アラームを設定します。
alarm facility temperature	温度アラームを設定します。
alarm facility temperature（上限および下限のしきい値）	温度しきい値の下限または上限を設定します。
show alarm settings	すべてのグローバル アラーム設定を表示します。
show environment alarm-contact	すべての外部アラーム設定を表示します。
show facility-alarm relay	アクティブ化された状態のリレーを表示します。
show facility-alarm status	トリガーされたすべてのアラームを表示するか、または指定された重大度に基づいてアラームを表示します。

clear failover statistics

フェールオーバー統計情報カウンタをクリアするには、特権 EXEC モードで **clear failover statistics** コマンドを使用します。

clear failover statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、**show failover statistics** コマンドで表示される統計情報、および **show failover** コマンド出力の Stateful Failover Logical Update Statistics セクションのカウンタをクリアします。フェールオーバー コンフィギュレーションを削除するには、**clear configure failover** コマンドを使用します。

例

次に、フェールオーバー統計情報カウンタをクリアする例を示します。

```
ciscoasa# clear failover statistics
ciscoasa#
```

関連コマンド

コマンド	説明
debug fover	フェールオーバーのデバッグ情報を表示します。
show failover	フェールオーバー コンフィギュレーションおよび動作統計に関する情報を表示します。

clear flow-export counters

NetFlow 統計情報とエラー データのランタイム カウンタを 0 にリセットするには、特権 EXEC モードで **clear flow-export counters** コマンドを使用します。

clear flow-export counters

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.1(1)	このコマンドが追加されました。

例

次に、NetFlow のランタイム カウンタをリセットする例を示します。

```
ciscoasa# clear flow-export counters
```

関連コマンド

コマンド	説明
flow-export destination	NetFlow コレクタの IP アドレスまたはホスト名と、NetFlow コレクタがリッスンする UDP ポートを指定します。
flow-export template timeout-rate	テンプレート情報が NetFlow コレクタに送信される間隔を制御します。
logging flow-export-syslogs enable	**logging flow-export-syslogs disable** コマンドを入力した後に、syslog メッセージをイネーブルにし、さらに NetFlow データに関連付けられた syslog メッセージをイネーブルにします。
show flow-export counters	NetFlow のすべてのランタイム カウンタを表示します。

clear flow-offload

オフロードされたフローの統計情報またはオフロードされたフローをクリアするには、特権 EXEC モードで **clear flow-offload** コマンドを使用します。

clear flow-offload {**statistics** | **flow all**}

構文の説明

statistics	オフロードされたフローの統計情報をクリアします。
flow all	オフロードされたフローをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが導入されました。

使用上のガイドライン

clear flow-offload statistics コマンドは、オフロードされたフローの統計情報をゼロにリセットします。

clear flow-offload flow all を使用してオフロードされたフローを削除すると、それらのフローの後続パケットは ASA に送信されます。ASA は、フローを再度オフロードします。このため、クリアしたフローの統計情報が不正確になります。このコマンドは、デバッグのためだけに使用します。

例

次に、統計情報をクリアする例を示します。

```
ciscoasa# clear flow-offload statistics
```

関連コマンド

コマンド	説明
flow-offload	フロー オフロードを有効にします。
set-connection advanced-options flow-offload	オフロードの対象としてトラフィック フローを指定します。
show flow-offload	オフロードするフローに関する情報を表示します。

clear fragment

IP フラグメント再構築モジュールの動作データをクリアするには、特権 EXEC モードで **clear fragment** コマンドを入力します。

clear fragment {**queue** | **statistics** [*interface_name*]}

構文の説明

interface_name	（任意）ASA のインターフェイスを指定します。
queue	IP フラグメント再構築キューをクリアします。
statistics	IP フラグメント再構築統計情報をクリアします。

デフォルト

interface_name が指定されていない場合、このコマンドはすべてのインターフェイスに適用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、コンフィギュレーション データのクリアを動作データのクリアと区別するために、**clear fragment** および **clear configure fragment** という 2 つのコマンドに分けられました。

使用上のガイドライン

このコマンドは、現在キューに入っている再構築待機中のフラグメント（**queue** キーワードが入力されている場合）、またはすべての IP フラグメント再構築統計情報（**statistics** キーワードが入力されている場合）のいずれかをクリアします。統計情報は、再構築に成功したフラグメント チェーンの数、再構築に失敗したチェーンの数、および最大サイズの超過によってバッファ オーバーフローが発生した回数を示すカウンタです。

例

次に、IP フラグメント再構成モジュールの運用データをクリアする例を示します。

```
ciscoasa# clear fragment queue
```

関連コマンド

コマンド	説明
clear configure fragment	IP フラグメント再構成コンフィギュレーションをクリアし、デフォルトにリセットします。
fragment	パケット フラグメンテーションを詳細に管理できるようにし、NFS との互換性を高めます。
show fragment	IP フラグメント再構成モジュールの動作データを表示します。
show running-config fragment	IP フラグメント再構成コンフィギュレーションを表示します。

clear gc

ガーベッジ コレクション(GC)プロセスの統計情報を削除するには、特権 EXEC モードで **clear gc** コマンドを使用します。

clear gc

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、GC プロセスの統計情報を削除する例を示します。

```
ciscoasa# clear gc
```

関連コマンド

コマンド	説明
show gc	GC のプロセスの統計情報を表示します。

clear igmp counters

すべての IGMP カウンタをクリアするには、特権 EXEC モードで **clear igmp counters** コマンドを使用します。

clear igmp counters [*if_name*]

構文の説明

if_name	**nameif** コマンドで指定されたインターフェイス名。このコマンドにインターフェイス名を含めると、指定したインターフェイスのカウンタだけがクリアされます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、IGMP 統計情報カウンタをクリアする例を示します。

```
ciscoasa# clear igmp counters
```

関連コマンド

コマンド	説明
clear igmp group	IGMP グループ キャッシュから、検出されたグループをクリアします。
clear igmp traffic	IGMP トラフィック カウンタをクリアします。

clear igmp group

検出されたグループを IGMP グループ キャッシュからクリアするには、特権 EXEC モードで **clear igmp** コマンドを使用します。

clear igmp group [*group* | **interface** *name*]

構文の説明

group	IGMP グループ アドレス。特定のグループを指定すると、そのグループがキャッシュから削除されます。
interface *name*	**namif** コマンドで指定されたインターフェイス名。指定した場合は、そのインターフェイスに関連付けられたすべてのグループが削除されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

グループまたはインターフェイスを指定しない場合は、すべてのインターフェイスからすべてのグループがクリアされます。グループを指定した場合は、そのグループのエントリだけがクリアされます。インターフェイスを指定した場合は、そのインターフェイスのすべてのグループがクリアされます。グループとインターフェイスの両方を指定した場合は、指定したインターフェイスの指定したグループだけがクリアされます。

このコマンドは、スタティックに設定されたグループをクリアしません。

例

次に、検出されたすべての IGMP グループを IGMP グループ キャッシュからクリアする例を示します。

```
ciscoasa# clear igmp group
```

関連コマンド

コマンド	説明
clear igmp counters	すべての IGMP カウンタをクリアします。
clear igmp traffic	IGMP トラフィック カウンタをクリアします。

clear igmp traffic

IGMP トラフィック カウンタをクリアするには、特権 EXEC モードで **clear igmp traffic** コマンドを使用します。

clear igmp traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、IGMP 統計情報トラフィック カウンタをクリアする例を示します。

```
ciscoasa# clear igmp traffic
```

関連コマンド

コマンド	説明
clear igmp group	IGMP グループ キャッシュから、検出されたグループをクリアします。
clear igmp counters	すべての IGMP カウンタをクリアします。

clear ikev1

IPsec IKEv1 SA または統計情報を削除するには、特権 EXEC モードで **clear ikev1** コマンドを使用します。すべての IKEv1 SA をクリアするには、このコマンドを引数なしで使用します。

clear ikev1 {**sa** *ip_address* | **stats**}

構文の説明

sa *ip_address*	SA をクリアします。
stats	IKEv1 統計情報をクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

すべての IPsec IKEv1 SA をクリアするには、このコマンドを引数なしで使用します。

例

次に、ASA からすべての IPsec IKEv1 統計情報を削除する例を示します。

```
ciscoasa# clear ikev1 stats
ciscoasa#
```

次に、10.86.1.1 のピア IP アドレスを持つ SA を削除する例を示します。

```
ciscoasa# clear ikev1 sa peer 10.86.1.1
ciscoasa#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてまたは指定されたクリプト マップをコンフィギュレーションからクリアします。
clear configure isakmp	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
show ipsec sa	カウンタ、エントリ、マップ名、ピア IP アドレス、ホスト名などの IPSec SA に関する情報を表示します。
show running-config crypto	IPsec、クリプト マップ、ダイナミック クリプト マップ、ISAKMP など、暗号コンフィギュレーション全体を表示します。

clear ikev2

IPsec IKEv2 SA または統計情報を削除するには、特権 EXEC モードで **clear ikev2** コマンドを使用します。すべての IKEv2 SA をクリアするには、このコマンドを引数なしで使用します。

clear ikev2 {**sa** *ip_address* | **stats**}

構文の説明

sa *ip_address*	SA をクリアします。
stats	IKEv2 統計情報をクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

すべての IPsec IKEv2 SA をクリアするには、このコマンドを引数なしで使用します。

例

次に、ASA からすべての IPsec IKEv2 統計情報を削除する例を示します。

```
ciscoasa# clear ikev2 stats
ciscoasa#
```

次に、10.86.1.1 のピア IP アドレスを持つ SA を削除する例を示します。

```
ciscoasa# clear ikev2 sa peer 10.86.1.1
ciscoasa#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてまたは指定されたクリプト マップをコンフィギュレーションからクリアします。
clear configure isakmp	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
show ipsec sa	カウンタ、エントリ、マップ名、ピア IP アドレス、ホスト名などの IPsec SA に関する情報を表示します。
show running-config crypto	IPsec、クリプト マップ、ダイナミック クリプト マップ、ISAKMP など、暗号コンフィギュレーション全体を表示します。

clear interface

インターフェイス統計情報をクリアするには、特権 EXEC モードで **clear interface** コマンドを使用します。

clear interface [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*]

構文の説明

interface_name	（任意）**nameif** コマンド内にインターフェイス名のセットを指定します。
mapped_name	（任意）**allocate-interface** コマンドを使用してマッピング名を割り当てた場合、マルチ コンテキスト モードでその名前を指定します。
physical_interface	（任意）**gigabiternet0/1** などのインターフェイス ID を指定します。有効値については、**interface** コマンドを参照してください。
subinterface	（任意）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

デフォルト

デフォルトでは、このコマンドはすべてのインターフェイス統計情報をクリアします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

インターフェイスがコンテキスト間で共有されている場合にコンテキスト内でこのコマンドを入力すると、ASA は現在のコンテキストの統計情報だけをクリアします。システム実行スペースでこのコマンドを入力した場合、ASA は結合された統計情報をクリアします。

インターフェイス名は、システム実行スペースでは使用できません。これは、**nameif** コマンドはコンテキスト内だけで使用できるためです。同様に、**allocate-interface** コマンドを使用してインターフェイス ID をマッピング名にマッピングした場合、そのマッピング名はコンテキスト内だけで使用できます。

例

次に、すべてのインターフェイス統計情報をクリアする例を示します。

```
ciscoasa# clear interface
```

関連コマンド

コマンド	説明
clear configure interface	インターフェイス コンフィギュレーションをクリアします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。
show running-config interface	インターフェイスの設定を表示します。

clear ip audit count

監査ポリシーのシグニチャ一致の数をクリアするには、特権 EXEC モードで **clear ip audit count** コマンドを使用します。

clear ip audit count [**global** | **interface** *interface_name*]

構文の説明

global	(デフォルト)すべてのインターフェイスの一致数をクリアします。
interface *interface_name*	(任意)指定したインターフェイスの一致数をクリアします。

デフォルト

キーワードを指定しない場合、このコマンドはすべてのインターフェイスの一致をクリアします(**global**)。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、すべてのインターフェイスの数をクリアする例を示します。

```
ciscoasa# clear ip audit count
```

関連コマンド

コマンド	説明
ip audit interface	監査ポリシーをインターフェイスに割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
show ip audit count	監査ポリシーのシグニチャ一致の数を表示します。
show running-config ip audit attack	**ip audit attack** コマンドのコンフィギュレーションを表示します。

clear ipsec sa

IPsec SA を完全にクリアするには、または指定したパラメータに基づいてクリアするには、特権 EXEC モードで **clear ipsec sa** コマンドを使用します。

clear ipsec sa [**counters** | **entry** *peer-addr protocol spi* | **peer** *peer-addr* | **map** *map-name*]

構文の説明

counters	(任意)すべてのカウンタをクリアします。
entry	(オプション)指定した IPsec ピア、プロトコル、および SPI の IPsec SA をクリアします。
inactive	(オプション)トラフィックを渡すことができない IPsec SA をクリアします。
map *map-name*	(オプション)指定したクリプト マップの IPsec SA をクリアします。
peer	(オプション)指定したピアの IPsec SA をクリアします。
peer-addr	IPsec ピアの IP アドレスを指定します。
protocol	IPsec プロトコル **esp** または **ah** を指定します。
spi	IPsec SPI を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

同じ機能を実行するために、このコマンドの別の形式である **clear crypto ipsec sa** を使用できます。

例

次に、グローバル コンフィギュレーション モードで、すべての IPsec SA カウンタをクリアする例を示します。

```
ciscoasa# clear ipsec sa counters
ciscoasa#
```

関連コマンド

コマンド	説明
show ipsec sa	指定されたパラメータに基づいて IPsec SA を表示します。
show ipsec stats	IPsec フロー MIB のグローバル IPsec 統計情報を表示します。

clear ipv6 access-list counters（廃止）

IPv6 アクセス リスト統計情報カウンタをクリアするには、特権 EXEC モードで **clear ipv6 access-list counters** コマンドを使用します。

clear ipv6 access-list *id* **counters**

構文の説明

id	IPv6 アクセス リストの識別子。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	このコマンドは廃止されました。

例

次に、IPv6 アクセス リスト 2 の統計情報データをクリアする例を示します。

```
ciscoasa# clear ipv6 access-list 2 counters
ciscoasa#
```

関連コマンド

コマンド	説明
clear configure ipv6	現在のコンフィギュレーションから **ipv6 access-list** コマンドをクリアします。
ipv6 access-list	IPv6 アクセス リストを設定します。
show ipv6 access-list	現在のコンフィギュレーション内の **ipv6 access-list** コマンドを表示します。

clear ipv6 dhcprelay

IPv6 DHCP リレー バインディング エントリおよび統計情報をクリアするには、特権 EXEC モードで **clear ipv6 dhcprelay** コマンドを使用します。

clear ipv6 dhcprelay {**binding** [*ip_address*] | **statistics**}

構文の説明

binding	IPv6 DHCP リレー バインディング エントリをクリアします。
ip_address	(オプション)DHCP リレー バインディングの IPv6 アドレスを指定します。IP アドレスを指定した場合、その IP アドレスに関連付けられたリレー バインディング エントリだけがクリアされます。
statistics	IPv6 DHCP リレー エージェントの統計情報をクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

例

次に、IPv6 DHCP リレー バインディングの統計情報データをクリアする例を示します。

```
ciscoasa# clear ipv6 dhcprelay binding
ciscoasa#
```

関連コマンド

コマンド	説明
show ipv6 dhcprelay binding	リレー エージェントによって作成されたリレー バインディング エントリを表示します。
show ipv6 dhcprelay statistics	IPv6 DHCP リレー エージェントの情報を表示します。

clear ipv6 dhcp statistics

DHCPv6 クライアントとプレフィックス委任クライアントの統計情報をクリアするには、特権 EXEC モードで **clear ipv6 dhcp client statistics** コマンドを使用します。

clear ipv6 dhcp {**client** [**pd**] | **interface** *interface_name* | **server**} **statistics**

構文の説明

client	DHCPv6 クライアントの統計情報をクリアします。
interface *interface_name*	指定したインターフェイスの DHCPv6 統計情報をクリアします。
pd	プレフィックス委任クライアントの統計情報をクリアします。
server	DHCPv6 サーバの統計情報をクリアします。

コマンドデフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォールモード		セキュリティ コンテキスト		
				マルチ	
コマンドモード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、DHCPv6 クライアントの統計情報をクリアします。

例

次に、DHCPv6 クライアントの統計情報をクリアする例を示します。

```
ciscoasa# clear ipv6 dhcp client statistics
```

次に、DHCPv6 プレフィックス委任クライアントの統計情報をクリアする例を示します。

```
ciscoasa# clear ipv6 dhcp client pd statistics
```

次に、外部インターフェイスで統計情報をクリアする例を示します。

```
ciscoasa# clear ipv6 dhcp interface outside statistics
```

次に、DHCPv6 サーバの統計情報をクリアする例を示します。

```
ciscoasa# clear ipv6 dhcp server statistics
```

関連コマンド

コマンド	説明
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
domain-name	IR メッセージへの応答で SLAAC クライアントに提供されるドメイン名を設定します。
dns-server	IR メッセージへの応答で SLAAC クライアントに提供される DNS サーバを設定します。
import	ASA がプレフィックス委任クライアント インターフェイスで DHCPv6 サーバから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
ipv6 address	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
ipv6 address dhcp	インターフェイスの DHCPv6 を使用してアドレスを取得します。
ipv6 dhcp client pd	委任されたプレフィックスを使用して、インターフェイスのアドレスを設定します。
ipv6 dhcp client pd hint	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
ipv6 dhcp pool	DHCPv6 ステートレス サーバを使用して、特定のインターフェイスで SLAAC クライアントに提供する情報を含むプールを作成します。
ipv6 dhcp server	DHCPv6 ステートレス サーバを有効にします。
network	サーバから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
nis address	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。
nis domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。
show ipv6 dhcp	DHCPv6 情報を表示します。
show ipv6 general-prefix	DHCPv6 プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示します。
sip address	IR メッセージへの応答で SLAAC クライアントに提供される SIP アドレスを設定します。
sip domain-name	IR メッセージへの応答で SLAAC クライアントに提供される SIP ドメイン名を設定します。
sntp address	IR メッセージへの応答で SLAAC クライアントに提供される SNTP アドレスを設定します。

clear ipv6 mld traffic

IPv6 Multicast Listener Discovery（MLD; マルチキャスト リスナー検出）トラフィック カウンタをクリアするには、特権 EXEC モードで **clear ipv6 mld traffic** コマンドを使用します。

clear ipv6 mld traffic

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(4)	このコマンドが追加されました。

使用上のガイドライン

clear ipv6 mld traffic コマンドを使用すると、すべての MLD トラフィック カウンタをリセットできます。

例

次に、IPv6 MLD のトラフィック カウンタをクリアする例を示します。

```
ciscoasa# clear ipv6 mld traffic
ciscoasa#
```

関連コマンド

コマンド	説明
debug ipv6 mld	MLD のすべてのデバッグ メッセージを表示します。
show debug ipv6 mld	現在のコンフィギュレーション内の IPv6 に対する MLD コマンドを表示します。

clear ipv6 neighbors

IPv6 ネイバー探索キャッシュをクリアするには、特権 EXEC モードで **clear ipv6 neighbors** コマンドを使用します。

clear ipv6 neighbors

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、検出されたすべての IPv6 ネイバーをキャッシュから削除します。スタティック エントリは削除しません。

例

次に、IPv6 ネイバー探索キャッシュのすべてのエントリ（スタティック エントリは除く）を削除する例を示します。

```
ciscoasa# clear ipv6 neighbors
ciscoasa#
```

関連コマンド

コマンド	説明
ipv6 neighbor	IPv6 ネイバー探索キャッシュのスタティック エントリを設定します。
show ipv6 neighbor	IPv6 ネイバー キャッシュ情報を表示します。

clear ipv6 ospf

OSPFv3 ルーティング パラメータをクリアするには、特権 EXEC モードで **clear ipv6 ospf** コマンドを使用します。

clear ipv6 [*process_id*] [**counters**] [**events**] [**force-spf**] [**process**] [**redistribution**] [**traffic**]

構文の説明

counters	OSPF プロセス カウンタをリセットします。
events	OSPF イベント ログをクリアします。
force-ospf	OSPF プロセスの SPF をクリアします。
process	OSPFv3 プロセスをリセットします。
process_id	プロセス ID の番号をクリアします。有効値の範囲は 1 ～ 65535 です。
redistribution	OSPFv3 ルート再配布をクリアします。
traffic	トラフィック関連の統計情報をクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、すべての OSPFv3 ルーティング パラメータを削除します。

例

次に、すべての OSPFv3 ルート再配布をクリアする例を示します。

```
ciscoasa# clear ipv6 ospf redistribution
ciscoasa#
```

関連コマンド

コマンド	説明
show running-config ipv6 router	OSPFv3 プロセスの実行コンフィギュレーションを表示します。
clear configure ipv6 router	OSPFv3 ルーティング プロセスをクリアします。

clear ipv6 prefix-list

ルーティング プレフィックス リストをクリアするには、特権 EXEC モードで **clear ipv6 prefix-list** コマンドを使用します。

clear ipv6 prefix-list [*name*]

構文の説明

name	**ipv6 prefix-list** コマンドによって作成された名前付きプレフィックス リストをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IPv6 プレフィックス リストを削除します。

例

次に、list1 IPv6 プレフィックス リストをクリアする例を示します。

```
ciscoasa# clear ipv6 prefix-list list1
ciscoasa#
```

関連コマンド

コマンド	説明
show running-config ipv6 prefix-list	IPv6 プレフィックス リストの実行コンフィギュレーションを表示します。
clear configure ipv6 prefix-list	IPv6 プレフィックス損失コンフィギュレーションをクリアします。

clear ipv6 route

IPv6 ルーティング テーブルからルートを削除するには、特権 EXEC モードで **clear ipv6 route** コマンドを使用します。

clear ipv6 route [**management-only**] {**all** | *ipv6-prefix*/*prefix-length*}

構文の説明

management-only	IPv6 管理ルーティング テーブルのみをクリアします。
ipv6-prefix/*prefix-length*	IPv6 プレフィックス用のルーテッドをクリアします。
all	すべての IPv6 ルートをクリアします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(1)	このコマンドが追加されました。

使用上のガイドライン

clear ipv6 route コマンドは、IPv6 に固有であることを除き、**clear ip route** コマンドと類似しています。

宛先ごとの最大伝送ユニット（MTU）キャッシュもクリアされます。

例

次に、2001:0DB8::/35 用の IPv6 ルートを削除する例を示します。

```
ciscoasa# clear ipv6 route 2001:0DB8::/35
```

関連コマンド

コマンド	説明
show ipv6 route	IPv6 ルートを表示します。

clear ipv6 traffic

IPv6 トラフィック カウンタをリセットするには、特権 EXEC モードで **clear ipv6 traffic** コマンドを使用します。

clear ipv6 traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、**show ipv6 traffic** コマンドの出力内のカウンタがリセットされます。

例

次に、IPv6 トラフィック カウンタをリセットする例を示します。**ipv6 traffic** コマンドの出力には、カウンタがリセットされたことが示されています。

```
ciscoasa# clear ipv6 traffic
ciscoasa# show ipv6 traffic
IPv6 statistics:
  Rcvd:  1 total, 1 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  1 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 0 received, 0 sent

ICMP statistics:
```

```
  Rcvd: 1 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 1 neighbor advert
  Sent: 1 output
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 1 neighbor advert

UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 0 output

TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```

関連コマンド

コマンド	説明
show ipv6 traffic	IPv6 トラフィックの統計情報を表示します。

clear ip verify statistics

ユニキャスト RPF 統計情報をクリアするには、特権 EXEC モードで **clear ip verify statistics** コマンドを使用します。

clear ip verify statistics [**interface** *interface_name*]

構文の説明

interface *interface_name*	ユニキャスト RPF 統計情報をクリアするインターフェイスを設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ユニキャスト RPF をイネーブルにする方法については、**ip verify reverse-path** コマンドを参照してください。

例

次に、ユニキャスト RPF 統計情報をクリアする例を示します。

```
ciscoasa# clear ip verify statistics
```

関連コマンド

コマンド	説明
clear configure ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションをクリアします。
ip verify reverse-path	ユニキャスト RPF 機能をイネーブルにして、IP スプーフィングを防ぎます。
show ip verify statistics	ユニキャスト RPF 統計情報を表示します。
show running-config ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションを表示します。

clear isakmp sa

IKEv1 および IKEv2 ランタイム SA データベースをすべて削除するには、特権 EXEC モードで **clear isakmp sa** コマンドを使用します。

clear isakmp sa

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	**clear isakmp sa** コマンドが、**clear crypto isakmp sa** に変更されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、コンフィギュレーションから IKE ランタイム SA データベースを削除する例を示します。

```
ciscoasa# clear isakmp sa
ciscoasa#
```

関連コマンド

コマンド	説明
clear isakmp	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPsec ピアが ASA と通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp stats	実行時統計情報を表示します。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

clear isis

IS-IS データ構造をクリアするには、**clear isis** コマンドを使用します。

clear isis {***** | **lspfull** | **rib redistribution** [**level-1** | **level-2**] [*network_prefix*] [*network_mask*]}

構文の説明

*****	すべての IS-IS データ構造をクリアします。
level-1	（任意）再配布キャッシュから、レベル 1 IS-IS 再配布プレフィックスをクリアします。
level-2	（任意）再配布キャッシュから、レベル 2 IS-IS 再配布プレフィックスをクリアします。
lspfull	IS-IS LSPFULL 状態をクリアします。
network_mask	（任意）RIB からクリアするネットワーク プレフィックスのネットワーク マスクのネットワーク ID を A.B.C.D 形式で表したもの。プレフィックスに対するネットワーク マスクを指定しなかった場合、ネットワーク マスクには、プレフィックスのメジャー ネットが使用されます。
network_prefix	（任意）再配布ルーティング情報ベース（RIB）からクリアするネットワーク プレフィックスのネットワーク ID を A.B.C.D 形式で表したもの。プレフィックスに対するネットワーク マスクを指定しなかった場合、ネットワーク マスクには、プレフィックスのメジャー ネットが使用されます。
rib redistribution	IS-IS 再配布キャッシュ内のプレフィックスをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

再配布されたルートが多すぎて、リンクステート PDU（LSP）がいっぱいになってしまった場合は、問題の解決後、**clear isis lspfull** コマンドを使用して、この状態をクリアします。

clear isis rib コマンドは、Cisco Technical Assistance Center の担当者がソフトウェア エラーの後で実行を依頼したときに、トラブルシューティングのためにだけ使用することをお勧めします。

例

次に、LSPFULL 状態をクリアする例を示します。

```
ciscoasa# clear isis lspfull
```

次に、IP ローカル再配布キャッシュからネットワーク プレフィックス 10.1.0.0 をクリアする例を示します。

```
ciscoasa# clear isis rib redistribution 10.1.0.0 255.255.0.0
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。

コマンド	説明
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト(TLV)を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。

コマンド	説明
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

clear lisp eid コマンド ～ clear xlate コマンド

clear lisp eid

ASA EID テーブルをクリアするには、特権 EXEC モードで **clear lisp eid** コマンドを使用します。

clear lisp eid [*ip_address*]

構文の説明

ip_address	指定した IP アドレスを EID テーブルから削除します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

ASA は EID とサイト ID を相関付ける EID テーブルを維持します。**clear lisp eid** コマンドは、テーブルの EID エントリをクリアします。

クラスタ フロー モビリティの LISP インスペクションについて

ASA は、場所の変更について LISP トラフィックを検査し、シームレスなクラスタリング操作のためにこの情報を使用します。LISP の統合により、ASA クラスタ メンバーは、最初のホップ ルータと ETR または ITR との間で渡される LISP トラフィックを検査し、その後、フローの所有者を新しいサイトへ変更できます。

クラスタ フロー モビリティには複数の相互に関連する設定が含まれています。

1. （オプション）ホストまたはサーバの IP アドレスに基づく検査される EID の限定：最初のホップ ルータは、ASA クラスタが関与していないホストまたはネットワークに関する EID 通知メッセージを送信することがあるため、EID をクラスタに関連するサーバまたはネットワークのみに限定することができます。たとえば、クラスタが 2 つのサイトのみに関連しているが、LISP は 3 つのサイトで稼働している場合は、クラスタに関連する 2 つのサイトの EID のみを含めます。**policy-map type inspect lisp**、**allowed-eid** および **validate-key** コマンドを参照してください。
2. LISP トラフィックのインスペクション：ASA は、最初のホップ ルータと ITR または ETR 間で送信された EID 通知メッセージに関して LISP トラフィックを検査します。ASA は EID とサイト ID を相関付ける EID テーブルを維持します。たとえば、最初のホップ ルータの送信元 IP アドレスと ITR または ETR の宛先アドレスをもつ LISP トラフィックを検査する必要があります。**inspect lisp** コマンドを参照してください。
3. 指定されたトラフィックでのフロー モビリティを有効にするサービス ポリシー：ビジネスクリティカルなトラフィックでフロー モビリティを有効にする必要があります。たとえば、フロー モビリティを、HTTPS トラフィックのみに制限したり、特定のサーバとの間でやり取りされるトラフィックのみに制限したりできます。**cluster flow-mobility lisp** コマンドを参照してください。
4. サイト ID：ASA は各クラスタ ユニットのサイト ID を使用して、新しい所有者を判別します。**site-id** コマンドを参照してください。
5. フロー モビリティを有効にするクラスタレベルの設定：クラスタ レベルでもフロー モビリティを有効にする必要があります。このオン/オフの切り替えを使用することで、特定のクラスのトラフィックまたはアプリケーションに対してフロー モビリティを簡単に有効または無効にできます。**flow-mobility lisp** コマンドを参照してください。

関連コマンド

コマンド	説明
allowed-eids	IP アドレスに基づいて検査される EID を限定します。
clear cluster info flow-mobility counters	フロー モビリティ カウンタをクリアします。
cluster flow-mobility lisp	サービス ポリシーのフロー モビリティを有効にします。
flow-mobility lisp	クラスタのフロー モビリティを有効にします。
inspect lisp	LISP トラフィックを検査します。
policy-map type inspect lisp	LISP 検査をカスタマイズします。
site-id	クラスタ シャーシのサイト ID を設定します。
show asp table classify domain inspect-lisp	LISP 検査用の ASP テーブルを表示します。
show cluster info flow-mobility counters	フロー モビリティ カウンタを表示します。

コマンド	説明
show conn	LISP フロー モビリティの対象となるトラフィックを表示します。
show lisp eid	ASA EID テーブルを表示します。
show service-policy	サービス ポリシーを表示します。
validate-key	LISP メッセージを検証するための事前共有キーを入力します。

clear local-host

接続制限や初期接続制限など、クライアントごとの実行時状態を再初期化するには、特権 EXEC モードで **clear local-host** コマンドを使用します。

clear local-host [*ip_address*] [**all**] [**zone** [*zone_name*]]

構文の説明

all	(任意)to-the-box トラフィックを含む、すべての接続をクリアします。**all** キーワードを指定しない場合は、through-the-box トラフィックだけがクリアされます。
ip_address	(任意)ローカル ホストの IP アドレスを指定します。
zone [*zone_name*]	(オプション)ゾーン接続を指定します。

デフォルト

すべての through-the-box 実行時状態をクリアします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.3(2)	**zone** キーワードが追加されました。

使用上のガイドライン

コンフィギュレーションに対してセキュリティ ポリシーの変更を加えた場合は、すべての*新しい*接続で新しいセキュリティ ポリシーが使用されます。既存の接続では、その接続が確立された時点で設定されていたポリシーの使用が続行されます。すべての接続で新しいポリシーが確実に使用されるようにするには、**clear local-host** コマンドを使用して、現在の接続を切断し、新しいポリシーを使用して再接続できるようにする必要があります。さらにきめ細かく接続をクリアするための **clear conn** コマンドや、ダイナミック NAT を使用する接続用の **clear xlate** コマンドを代わりに使用することもできます。

clear local-host コマンドは、ホスト ライセンス制限からホストを解放します。ライセンス制限にカウントされているホストの数は、**show local-host** コマンドを入力して表示できます。

例

次に、10.1.1.15 のホストの実行時状態および関連する接続をクリアする例を示します。

```
ciscoasa# clear local-host 10.1.1.15
```

関連コマンド

コマンド	説明
clear conn	あらゆる状態の接続を切断します。
clear xlate	ダイナミック NAT セッションおよび NAT を使用しているすべての接続をクリアします。
show local-host	ローカル ホストのネットワーク状態を表示します。

clear logging asdm

ASDM ロギング バッファをクリアするには、特権 EXEC モードで **clear logging asdm** コマンドを使用します。

clear logging asdm

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**clear pdm logging** コマンドから **clear asdm log** コマンドに変更されました。

使用上のガイドライン

ASDM システム ログ メッセージは、ASA のシステム ログ メッセージとは別のバッファに格納されます。ASDM ロギング バッファをクリアすると、ASDM システム ログ メッセージだけがクリアされます。ASA のシステム ログ メッセージはクリアされません。ASDM システム ログ メッセージを表示するには、**show asdm log** コマンドを使用します。

例

次に、ASDM ロギング バッファをクリアする例を示します。

```
ciscoasa(config)# clear logging asdm
ciscoasa(config)#
```

関連コマンド

コマンド	説明
show asdm log_sessions	ASDM ロギング バッファの内容を表示します。

clear logging buffer

ログ バッファをクリアするには、特権 EXEC モードで **clear logging buffer** コマンドを使用します。

clear logging buffer

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次の例では、ログ バッファの内容をクリアする方法を示します。

```
ciscoasa# clear logging buffer
```

関連コマンド

コマンド	説明
logging buffered	ログ バッファを設定します。
show logging	ロギング情報を表示します。

clear logging counter

ログに記録されたカウンタと統計情報をクリアするには、特権 EXEC モードで **clear logging counter** コマンドを使用します。

clear logging counter { all | console | monitor | buffer | trap | asdm | mail}

構文の説明

counter	指定されたロギングの宛先に対するカウンタと統計情報をクリアします。すべてのロギングの宛先に対する統計情報をクリアするには、**all** を指定します。オプションで、**console**、**monitor**、**buffer**、**trap**、**asdm**、**mail** の統計情報をクリアする宛先を指定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.14(1)	このコマンドが追加されました。

使用上のガイドライン

show logging コマンドは、ASA で設定された各ロギングカテゴリについてログに記録されたメッセージの統計情報を提供します。これらの統計情報/カウンタをクリアするには、**clear logging counter** コマンドを使用します。

例

次の例では、ログに記録されたメッセージのカウンタをクリアする方法について示します。

```
ciscoasa# clear logging counter all
```

関連コマンド

コマンド	説明
show logging	ロギング情報を表示します。

clear logging queue bufferwrap

保存されたログ バッファ（ASDM、内部、FTP、およびフラッシュ）をクリアするには、特権 EXEC モードで **clear logging queue bufferwrap** コマンドを使用します。

clear logging queue bufferwrap

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

例

次に、保存されているログ バッファの内容をクリアする例を示します。

```
ciscoasa# clear logging queue bufferwrap
```

関連コマンド

コマンド	説明
logging buffered	ログ バッファを設定します。
show logging	ロギング情報を表示します。

clear mac-address-table

ダイナミック MAC アドレス テーブル エントリをクリアするには、特権 EXEC モードで **clear mac-address-table** コマンドを使用します。

clear mac-address-table [*interface_name*]

構文の説明

interface_name	（任意）選択したインターフェイスの MAC アドレス テーブル エントリをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	—	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、ダイナミック MAC アドレス テーブルのエントリをクリアする例を示します。

```
ciscoasa# clear mac-address-table
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
mac-address-table aging-time	ダイナミック MAC アドレス エントリのタイムアウトを設定します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show mac-address-table	MAC アドレス テーブルのエントリを表示します。

clear memory appcache-threshold

memory appcache-threshold のヒット カウントをクリアするには、特権 EXEC モードで **clear memory appcache-threshold** コマンドを使用します。

clear memory appcache-threshold

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.10(1)	このコマンドが導入されました。

使用上のガイドライン

アプリケーション キャッシュのしきい値に達するたびに、カウンタは 1 ずつ増加します。**clear memory appcache-threshold** コマンドは、メモリ アプリケーション キャッシュのしきい値のヒット カウントをクリアし、0 にリセットします。

例

次に、memory appcache-threshold のヒット カウントをクリアする例を示します。

```
ciscoasa# clear memory appcache-threshold
```

関連コマンド

コマンド	説明
memory appcache-threshold enable	特定のメモリしきい値に達した後のアプリケーション キャッシュの割り当てを制限するには、memory appcache-threshold を有効にします。
show memory appcache-threshold	メモリ appcache しきい値のステータスとヒット数を表示します。

clear memory delayed-free-poisoner

delayed free-memory poisoner ツールのキューと統計情報をクリアするには、特権 EXEC モードで **clear memory delayed-free-poisoner** コマンドを使用します。

clear memory delayed-free-poisoner

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

clear memory delayed-free-poisoner コマンドは、delayed free-memory poisoner ツールのキューで保持されているすべてのメモリを検証なしでシステムに戻し、関連する統計情報カウンタをクリアします。

例

次に、delayed free-memory poisoner ツールのキューと統計情報をクリアする例を示します。

```
ciscoasa# clear memory delayed-free-poisoner
```

関連コマンド

コマンド	説明
memory delayed-free-poisoner enable	delayed free-memory poisoner ツールをイネーブルにします。
memory delayed-free-poisoner validate	delayed free-memory poisoner ツールのキューを検証します。
show memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューの使用状況に関する要約を表示します。

clear memory profile

メモリ プロファイリング機能によって保持されるメモリ バッファをクリアするには、特権 EXEC モードで **clear memory profile** コマンドを使用します。

clear memory profile [peak]

構文の説明

peak	（任意）ピーク メモリ バッファの内容をクリアします。

デフォルト

デフォルトでは、現在「使用されている」プロファイル バッファをクリアします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	—	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

clear memory profile コマンドは、プロファイリング機能によって保持されているメモリ バッファを解放します。したがって、プロファイリングは、クリアされる前に停止している必要があります。

例

次に、プロファイリング機能によって保持されているメモリ バッファをクリアする例を示します。

```
ciscoasa# clear memory profile
```

関連コマンド

コマンド	説明
memory profile enable	メモリ使用状況（メモリ プロファイリング）のモニタリングをイネーブルにします。
memory profile text	プロファイルするメモリのテキスト範囲を設定します。
show memory profile	ASA のメモリ使用状況（プロファイリング）に関する情報を表示します。

clear mfib counters

MFIB ルータ パケット カウンタをクリアするには、特権 EXEC モードで **clear mfib counters** コマンドを使用します。

clear mfib counters [*group* [*source*]]

構文の説明

group	（任意）マルチキャスト グループの IP アドレスです。
source	（任意）マルチキャスト ルート送信元の IP アドレスです。これは、4 分割ドット付き 10 進表記のユニキャスト IP アドレスです。

デフォルト

このコマンドを引数なしで使用した場合、すべてのルートのルート カウンタがクリアされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、すべての MFIB ルータ パケット カウンタをクリアする例を示します。

```
ciscoasa# clear mfib counters
```

関連コマンド

コマンド	説明
show mfib count	MFIB ルートおよびパケット カウント データを表示します。

clear module

ASA 上の SSM に関する情報、ASA 5505 上の SSC に関する情報、ASA 5585-X にインストールされた SSP に関する情報、ASA 5585-X にインストールされた IPS SSP に関する情報、ASA サービス モジュールに関する情報、およびシステム情報をクリアするには、特権 EXEC モードで **clear module** コマンドを使用します。

clear module [*mod_id* | *slot*] [**all** | [**details** | **recover** | **log** [**console**]]]

構文の説明

all	(デフォルト)すべての SSM 情報をクリアします。
console	(オプション)モジュールのコンソール ログ情報をクリアします。
details	(オプション)SSM(たとえば ASA-SSM-*x*0 など)のリモート管理コンフィギュレーションを含め、追加情報をクリアします。
log	(オプション)モジュールのログ情報をクリアします。
mod_id	IPS などのソフトウェア モジュールで使用されるモジュール名をクリアします。
recover	(オプション)SSM について、**hw-module module recover** コマンドの設定をクリアします。 (注) **recover** キーワードが有効になるのは、**hw-module module recover** コマンドに **configure** キーワードを使用して SSM のリカバリ コンフィギュレーションを作成した場合のみです。 (オプション)ASA 5512-X、5515-X、5525-X、5545-X、または 5555-X にインストールされた IPS モジュールについて、**sw-module module** *mod_id* **recover configure image** *image_location* コマンドの設定をクリアします。
slot	モジュールのスロット番号を指定します。0 または 1 のいずれかになります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(1)	SSC のサポートが追加されました。
8.2(5)	ASA 5585-X と ASA 5585-X 上の IPS SSP のサポートが追加されました。
8.4(2)	デュアル SSP インストールのサポートが追加されました。
8.5(1)	ASASM のサポートが追加されました。
8.6(1)	ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X のサポートが追加されました。

使用上のガイドライン

このコマンドは、SSC、SSM、ASASM、IPS SSP、デバイス インターフェイス、および組み込みインターフェイスに関する情報をクリアします。

例

次に、SSM のリカバリ設定をクリアする例を示します。

```
ciscoasa# clear module 1 recover
```

関連コマンド

コマンド	説明
hw-module module recover	リカバリ イメージを TFTP サーバからロードして、SSM を回復します。
hw-module module reset	SSM をシャットダウンし、ハードウェア リセットを実行します。
hw-module module reload	SSM ソフトウェアをリロードします。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切る準備をして、SSM ソフトウェアをシャットダウンします。
show module	SSM 情報を表示します。

clear nac-policy

NAC ポリシーの使用状況の統計情報をリセットするには、グローバル コンフィギュレーション モードで **clear nac-policy** コマンドを使用します。

clear nac-policy [*nac-policy-name*]

構文の説明

nac-policy-name	(任意)使用状況の統計情報をリセットする NAC ポリシーの名前。

デフォルト

名前を指定しない場合、CLI は、すべての NAC ポリシーに関する使用状況の統計情報をリセットします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

例

次に、framework1 という名前の NAC ポリシーの使用状況の統計情報をリセットする例を示します。

```
ciscoasa(config)# clear nac-policy framework1
```

次に、NAC ポリシーの使用状況の統計情報をすべてリセットする例を示します。

```
ciscoasa(config)# clear nac-policy
```

関連コマンド

コマンド	説明
show nac-policy	ASA での NAC ポリシー使用状況の統計情報を表示します。
show vpn-session_summary.db	IPsec、WebVPN、および NAC セッションの数を表示します。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。

clear nat counters

NAT ポリシー カウンタをクリアするには、グローバル コンフィギュレーション モードで **clear nat counters** コマンドを使用します。

clear nat counters [*src_ifc* [*src_ip* [*src_mask*]] [*dst_ifc* [*dst_ip* [*dst_mask*]]]]

構文の説明

dst_ifc	（任意）フィルタリングする宛先インターフェイスを指定します。
dst_ip	（任意）フィルタリングする宛先 IP アドレスを指定します。
dst_mask	（任意）宛先 IP アドレスのマスクを指定します。
src_ifc	（任意）フィルタリングする送信元インターフェイスを指定します。
src_ip	（オプション）フィルタリングする送信元 IP アドレスを指定します。
src_mask	（オプション）送信元 IP アドレスのマスクを指定します。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0 (4)	このコマンドが追加されました。

例

次に、NAT ポリシー カウンタをクリアする例を示します。

```
ciscoasa(config)# clear nat counters
```

関連コマンド

コマンド	説明
nat	別のインターフェイス上にあるマップ済みアドレスに変換する、インターフェイス上のアドレスを識別します。
nat-control	NAT 設定要件をイネーブルまたはディセーブルにします。
show nat counters	プロトコル スタック カウンタを表示します。

clear nve

NVE 送信元インターフェイス統計情報をクリアするには、特権 EXEC モードで **clear nve** コマンドを使用します。

clear nve 1

構文の説明

1	NVE インスタンスを指定します（常に 1）。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリア インターフェイスのステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスをクリアします。

例

次に、NVE インターフェイスの統計情報をクリアする例を示します。

```
ciscoasa# clear nve 1
```

関連コマンド

コマンド	説明
show nve	NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリア インターフェイス（送信元インターフェイス）のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。

clear object-group

ネットワーク オブジェクト グループのオブジェクトのヒット カウントをクリアするには、特権 EXEC モードで **clear object-group** コマンドを使用します。

clear object-group *obj-name* **counters**

構文の説明

counters	ネットワーク オブジェクト グループのカウンタを指定します。
obj-name	既存のネットワーク オブジェクト グループを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

使用上のガイドライン

単一のネットワーク オブジェクト グループにあるオブジェクトのヒット カウントだけをクリアするには、このコマンドを使用します。

例

次に、「Anet」という名前のネットワーク オブジェクト グループのネットワーク オブジェクト ヒット カウントをクリアする例を示します。

```
ciscoasa# clear object-group Anet counters
```

関連コマンド

コマンド	説明
show object-group	指定したオブジェクト グループがネットワーク オブジェクト グループ タイプである場合に、オブジェクト グループ情報およびヒット カウントを表示します。

clear ospf

OSPF プロセス情報をクリアするには、特権 EXEC モードで **clear ospf** コマンドを使用します。

clear ospf [*pid*] {**process** | **counters**}

構文の説明

counters	OSPF カウンタをクリアします。
pid	（任意）OSPF ルーティング プロセスの内部使用の ID パラメータ。有効な値は、1 ～ 65535 です。
process	OSPF ルーティング プロセスを再起動します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

このコマンドは、コンフィギュレーションのいずれの部分も削除しません。コンフィギュレーションから特定のコマンドをクリアするには、このコンフィギュレーション コマンドの **no** 形式を使用します。または、コンフィギュレーションからすべてのグローバル OSPF コマンドを削除するには、**clear configure router ospf** コマンドを使用します。

（注） **clear configure router ospf** コマンドは、インターフェイス コンフィギュレーション モードで入力された OSPF コマンドをクリアしません。

例

次に、OSPF ネイバー カウンタをクリアする例を示します。

```
ciscoasa# clear ospf counters
```

関連コマンド

コマンド	説明
clear configure router	実行コンフィギュレーションからすべてのグローバル ルータ コマンドをクリアします。

clear pclu

PC 論理更新統計情報をクリアするには、特権 EXEC モードで **clear pclu** コマンドを使用します。

clear pclu

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、PC 情報をクリアする例を示します。

```
ciscoasa# clear pclu
```

clear phone-proxy secure-phones

電話プロキシ データベース内のセキュア フォン エントリをクリアするには、特権 EXEC モードで **clear phone-proxy secure-phones** コマンドを使用します。

clear phone-proxy secure-phones [*mac_address* | **noconfirm]**

構文の説明

mac_address	電話プロキシ データベースから、指定した MAC アドレスを持つ IP フォンを削除します。
noconfirm	確認プロンプトなしで、電話プロキシ データベース内のすべてのセキュア フォン エントリを削除します。**noconfirm** キーワードを指定しない場合は、すべてのセキュア フォン エントリを削除するかどうかを確認するプロンプトが表示されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

セキュア フォンによって起動時に必ず CTL ファイルが要求されるため、電話プロキシは、電話をセキュアとしてマークするデータベースを作成します。セキュア フォン データベースのエントリは、設定された指定タイムアウト後に（**timeout secure-phones** コマンドを介して）削除されます。または、**clear phone-proxy secure-phones** コマンドを使用すると、設定済みのタイムアウトが経過する前に電話プロキシ データベースをクリアできます。

例

次に、電話プロキシ データベース内のセキュア エントリをクリアする例を示します。

```
ciscoasa# clear phone-proxy secure-phones 001c.587a.4000
```

関連コマンド

コマンド	説明
timeout secure-phones	アイドル タイムアウトを設定します。この時間を経過すると、電話プロキシ データベースからセキュア フォン エントリが削除されます。

clear pim counters

PIM トラフィック カウンタをクリアするには、特権 EXEC モードで **clear pim counters** コマンドを使用します。

clear pim counters

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、トラフィック カウンタだけをクリアします。PIM トポロジ テーブルをクリアするには、**clear pim topology** コマンドを使用します。

例

次に、PIM トラフィック カウンタをクリアする例を示します。

```
ciscoasa# clear pim counters
```

関連コマンド

コマンド	説明
clear pim reset	リセット時の MRIB 同期を必須にします。
clear pim topology	PIM トポロジ テーブルをクリアします。
show pim traffic	PIM トラフィック カウンタを表示します。

clear pim group-map

グループからのランデブー ポイント(RP)へのマッピング エントリを RP マッピング キャッシュから削除するには、**clear pim group-map** コマンドを使用します。

clear pim group-map [*rp-address*]

構文の説明

rp-address	ランデブー ポイントのマッピング アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが導入されました。

例

次に、RP アドレス 23.23.23.2 のグループから RP へのマッピングのエントリを削除する例を示します。

```
ciscoasa(config)# sh pim group-map
Group Range         Proto Client Groups RP address      Info

224.0.1.39/32*      DM    static 0      0.0.0.0
224.0.1.40/32*      DM    static 0      0.0.0.0
224.0.0.0/24*       L-Localstatic 1      0.0.0.0
232.0.0.0/8*        SSM   config 0      0.0.0.0
224.0.0.0/4*        SM    config 0      9.9.9.9         RPF: ,0.0.0.0
224.0.0.0/4         SM    BSR    0      23.23.23.2      RPF: Gi0/3,23.23.23.2

ciscoasa(config)# clear pim group-map 23.23.23.2
ciscoasa(config)# sh pim group-map
Group Range         Proto Client Groups RP address      Info

224.0.1.39/32*      DM    static 0      0.0.0.0
224.0.1.40/32*      DM    static 0      0.0.0.0
224.0.0.0/24*       L-Localstatic 1      0.0.0.0
232.0.0.0/8*        SSM   config 0      0.0.0.0
224.0.0.0/4*        SM    config 0      9.9.9.9         RPF: ,0.0.0.0
224.0.0.0/4         SM    static 0      0.0.0.0         RPF: ,0.0.0.0
```

関連コマンド

コマンド	説明
clear pim counters	PIM カウンタおよび統計情報をクリアします。
clear pim topology	PIM トポロジ テーブルをクリアします。
clear pim counters	PIM トラフィック カウンタをクリアします。

clear pim reset

リセットによって MRIB 同期を強制するには、特権 EXEC モードで **clear pim reset** コマンドを使用します。

clear pim reset

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

トポロジ テーブルのすべての情報がクリアされ、MRIB 接続がリセットされます。このコマンドは、PIM トポロジ テーブルと MRIB データベース間の状態を同期するために使用できます。

例

次に、トポロジ テーブルをクリアし、MRIB 接続をリセットする例を示します。

```
ciscoasa# clear pim reset
```

関連コマンド

コマンド	説明
clear pim counters	PIM カウンタおよび統計情報をクリアします。
clear pim topology	PIM トポロジ テーブルをクリアします。
clear pim counters	PIM トラフィック カウンタをクリアします。

clear pim topology

PIM トポロジ テーブルをクリアするには、特権 EXEC モードで **clear pim topology** コマンドを使用します。

clear pim topology [*group*]

構文の説明

group	（任意）トポロジ テーブルから削除するマルチキャスト グループのアドレスまたは名前を指定します。

デフォルト

オプションの *group* 引数を指定しない場合、トポロジ テーブルからすべてのエントリがクリアされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、PIM トポロジ テーブルから既存の PIM ルートをクリアします。IGMP ローカル メンバーシップなど、MRIB テーブルから取得した情報は保持されます。マルチキャスト グループを指定した場合は、それらのグループ エントリだけがクリアされます。

例

次に、PIM トポロジ テーブルをクリアする例を示します。

```
ciscoasa# clear pim topology
```

関連コマンド

コマンド	説明
clear pim counters	PIM カウンタおよび統計情報をクリアします。
clear pim reset	リセット時の MRIB 同期を必須にします。
clear pim counters	PIM トラフィック カウンタをクリアします。

clear priority-queue statistics

任意のインターフェイスまたは設定されたすべてのインターフェイスのプライオリティ キュー統計情報カウンタをクリアするには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **clear priority-queue statistics** コマンドを使用します。

clear priority-queue statistics [*interface-name*]

構文の説明

interface-name	(任意)ベストエフォート キューおよび低遅延キューの詳細を表示するインターフェイスの名前を指定します。

デフォルト

インターフェイス名を省略した場合、このコマンドは設定されたすべてのインターフェイスのプライオリティ キュー統計情報をクリアします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、特権 EXEC モードで **clear priority-queue statistics** コマンドを使用して、「test」という名前のインターフェイスのプライオリティ キュー統計情報を削除する例を示します。

```
ciscoasa# clear priority-queue statistics test
ciscoasa#
```

関連コマンド

コマンド	説明
clear configure priority queue	指定されたインターフェイスからプライオリティ キュー コンフィギュレーションを削除します。
priority-queue	インターフェイスにプライオリティ キューイングを設定します。

コマンド	説明
show priority-queue statistics	指定したインターフェイスまたはすべてのインターフェイスのプライオリティ キュー統計情報を表示します。
show running-config priority-queue	指定したインターフェイスの現在のプライオリティ キュー コンフィギュレーションを表示します。

clear process

ASA 上で実行されている特定のプロセスの統計情報をクリアするには、特権 EXEC モードで **clear process** コマンドを使用します。

clear process [**cpu-hog** | **internals**]

構文の説明

cpu-hog	高 CPU 負荷統計情報をクリアします。
internals	プロセス内部統計情報をクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、高 CPU 負荷統計情報をクリアする例を示します。

```
ciscoasa# clear process cpu-hog
ciscoasa#
```

関連コマンド

コマンド	説明
cpu hog granular-detection	リアルタイム高 CPU 負荷検出情報をトリガーします。
show processes	ASA で動作しているプロセスのリストを表示します。

clear resource usage

リソース使用状況の統計情報をクリアするには、特権 EXEC モードで **clear resource usage** コマンドを使用します。

clear resource usage [**context** *context_name* | **all** | **summary** | **system**] [**resource** {[**rate**] *resource_name* | **all**}]

構文の説明

context *context_name*	(マルチ モードのみ)統計情報をクリアするコンテキスト名を指定します。すべてのコンテキストを対象にする場合は、**all**(デフォルト)を指定します。
resource [**rate**] *resource_name*	特定のリソースの使用状況をクリアします。すべてのリソースを対象にするには、**all**(デフォルト)を指定します。リソース使用状況のレートをクリアする場合は、**rate** を指定します。比率で測定されるリソースには、**conns**、**inspects**、および **syslogs** があります。これらのリソース タイプを指定する場合は、**rate** キーワードを指定する必要があります。conns リソースは、同時接続としても測定されます。1 秒あたりの接続を表示するには、**rate** キーワードのみを使用します。 リソースには、次のタイプがあります。 • **asdm**:ASDM 管理セッション。 • **conns**:1 つのホストと複数のその他のホスト間の接続を含む 2 つのホスト間の TCP または UDP 接続。 • **inspects**:アプリケーション インスペクション。 • **hosts**:ASA を通じて接続可能なホスト。 • **mac-addresses**:トランスペアレント ファイアウォール モードで、MAC アドレス テーブルに含められる MAC アドレスの数。 • **ssh**:SSH セッション。 • **syslogs**:syslogs メッセージ。 • **telnet**:Telnet セッション。 • (マルチ モードのみ)**VPN Other**:サイト間 VPN セッション。 • (マルチ モードのみ)**VPN Burst Other**:サイト間 VPN バースト セッション。 • **xlates**:NAT 変換。
summary	(マルチ モードのみ)結合されたコンテキスト統計情報をクリアします。
system	(マルチ モードのみ)システム全体(グローバル)の使用状況の統計情報をクリアします。

デフォルト

マルチ コンテキスト モードの場合、デフォルトのコンテキストは **all** で、これにより、すべてのコンテキストのリソース使用状況がクリアされます。シングル モードの場合、コンテキスト名は無視され、すべてのリソース統計情報がクリアされます。

デフォルトのリソース名は **all** で、これにより、すべてのリソース タイプがクリアされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、すべてのコンテキストの、すべてのリソース使用状況の統計情報（システム全体の使用状況の統計情報は除く）をクリアする例を示します。

```
ciscoasa# clear resource usage
```

次に、システム全体の使用状況の統計情報をクリアする例を示します。

```
ciscoasa# clear resource usage system
```

関連コマンド

コマンド	説明
context	セキュリティ コンテキストを追加します。
show resource types	リソース タイプのリストを表示します。
show resource usage	ASA のリソース使用状況を表示します。

clear route all

ダイナミックに学習されたルートをコンフィギュレーションから削除するには、特権 EXEC モードで **clear route all** コマンドを使用します。

clear route all

デフォルト

デフォルトの動作や値はありません。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

欠落したルートを回復するには、**clear route all** コマンドを使用します。このコマンドを実行すると、グローバル RIB からのすべてのルートが削除されます。すべてのルート（ダイナミックまたはスタティック）がそれぞれのモジュール（プロトコル）によってグローバル RIB にプッシュされます。

一方、最適なルートがグローバル RIB にインストールされている場合は、同じルートがピアと NP テーブルに再配布されます。このプロセスは、複数のスレッドで順番に実行されます。このサイクルが完了するまでにかかる時間は、グローバル RIB のルートの数によって異なります。

したがって、**clear route all** コマンドを連続して使用する場合は、最小時間間隔を 30 秒、最大時間間隔を 120 秒にしてください。推奨される時間間隔に従わずにこのコマンドを複数回実行すると、配布されたルートが削除され、RIB からのルートが失われる可能性があります。

例

次に、ダイナミックに学習されたルートを削除する例を示します。

```
ciscoasa# clear route all
```

関連コマンド

コマンド	説明
clear route *network* **<***mask***>**	指定された宛先ルートを除外します。
show route	ルート情報を表示します。
show running-config route	設定されているルートを表示します。

clear route management-only

指定された宛先ルートを削除するには、特権 EXEC モードで **clear route** ***network <mask>*** コマンドを使用します。管理専用キーワードによって IPv4 管理ルーティング テーブルのみがクリアされます。

clear route management-only [*ip_address ip_mask*]

構文の説明

ip_address ip_mask	除外する宛先 IP アドレスおよびサブネット マスクを指定します。
management-only	IPv4 管理ルーティング テーブルをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.5(1)	管理 VRF インターフェイスのサポートが追加されました。

例

次に、ダイナミックに学習されたルートを削除する例を示します。

```
ciscoasa# clear route 10.118.86.3
```

関連コマンド

コマンド	説明
clear route all	すべてのルートを除外し、リフレッシュします。
show route	ルート情報を表示します。
show running-config route	設定されているルートを表示します。

clear service-policy

イネーブルになっているポリシーの動作データまたは統計情報(存在する場合)をクリアするには、特権 EXEC モードで **clear service-policy** コマンドを使用します。

clear service-policy [**global** | **interface** *intf*] [**user-statistics**]

構文の説明

global	(任意)グローバル サービス ポリシーの統計情報をクリアします。
interface *intf*	(任意)特定のインターフェイスのサービス ポリシーの統計情報をクリアします。
user-statistics	(オプション)ユーザ統計情報のグローバル カウンタはクリアしますが、ユーザごとの統計情報はクリアしません。ユーザごとまたはユーザ グループごとの統計情報は、**show user-identity statistics** コマンドを使用して引き続き確認できます。 **user-statistics** コマンドに **accounting** キーワードを指定すると、送信パケット、受信パケット、および送信ドロップ パケットのすべてのグローバル カウンタがクリアされます。**user-statistics** コマンドに **scanning** キーワードを指定すると、送信ドロップ パケットのグローバル カウンタがクリアされます。 ASA でこれらのユーザ統計情報を収集するには、ユーザ統計情報を収集するようにポリシー マップを設定する必要があります。このガイドの **user-statistics** コマンドを参照してください。

デフォルト

デフォルトでは、このコマンドは、すべてのイネーブルなサービス ポリシーのすべての統計情報をクリアします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

一部のインスペクション エンジンでは、統計情報を選択してクリアできます。**clear service-policy inspect** コマンドを参照してください。

例

次に、外部インターフェイスのサービス ポリシー統計情報をクリアする方法の例を示します。

```
ciscoasa# clear service-policy interface outside
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	GTP インスペクション エンジンのサービス ポリシーの統計情報をクリアします。
clear service-policy inspect radius-accounting	RADIUS アカウンティング インスペクション エンジンのサービス ポリシーの統計情報をクリアします。
show service-policy	サービス ポリシーを表示します。
show running-config service-policy	実行コンフィギュレーションに設定されているサービス ポリシーを表示します。
clear configure service-policy	サービス ポリシーのコンフィギュレーションをクリアします。
service-policy	サービス ポリシーを設定します。

clear service-policy inspect gtp

GTP インスペクション統計情報をクリアするには、特権 EXEC モードで **clear service-policy inspect gtp** コマンドを使用します。

clear service-policy inspect gtp {**pdp-context** {**all** | **apn** *ap_name* | **imsi** *IMSI_value* | **ms-addr** *IP_address* | **tid** *tunnel_ID* | **version** *version_num*} | **requests** [*name* | **map** *name* | **version** *version_num*] | **statistics** [**gsn** *IP_address* | *IP_address*]}

構文の説明。

pdp-context {**all** | **apn** *ap_name* | **imsi** *IMSI_value* | **ms-addr** *IP_address* | **tid** *tunnel_ID* | **version** *version_num*}	パケット データ プロトコル（PDP）またはベアラー コンテキスト情報をクリアします。次のキーワードを使用して、クリアするコンテキストを指定できます。 • **all**：すべてのコンテキストをクリアします。 • **apn** *ap_name*：指定されたアクセス ポイントの名前のコンテキストをクリアします。 • **imsi** *IMSI_value*：指定された IMSI 16 進数のコンテキストをクリアします。 • **ms-addr** *IP_address*：指定されたモバイル サブスクライバ（MS）の IP アドレスのコンテキストをクリアします。 • **tid** *tunnel_ID*：指定された GTP トンネル ID（16 進数）のコンテキストをクリアします。 • **version** *version_num*：指定された GTP バージョン（0 ～ 255）のコンテキストをクリアします。
requests [*name* | **map** *name* | **version** *version_num*]	GTP 要求をクリアします。次のパラメータを使用して、クリアする要求を任意で制限できます。 • *name*：指定された GTP インスペクション ポリシー マップに関連付けられている要求をクリアします。このオプションは、9.5(1) 以降では使用できません。 • **map** *name*：（9.5(1)+）指定された GTP インスペクション ポリシー マップに関連付けられている要求をクリアします。 • **version** *version_num*：（9.5(1)+）指定された GTP バージョン（0 ～ 255）の要求をクリアします。
statistics [**gsn** *IP_address* | *IP_address*]	**inspect gtp** コマンドの GTP 統計情報をクリアします。 **gsn** キーワードにエンドポイントのアドレスを指定すると、特定のエンドポイントの統計情報をクリアできます。9.5(1) 以降はアドレスのみを指定し、**gsn** キーワードは含めないでください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.5(1)	次の点が変更されました。 • **statistics** オプションの **gsn** キーワードが削除されました。エンドポイントの統計情報をクリアするには、そのエンドポイントの IP アドレスのみを指定します。 • **requests** オプションに **version** キーワードが追加されました。**requests** オプションの後ろにマップ名を直接入力する機能に代わり、**map** キーワードがポリシー マップ名に追加されました。 • IPv6 アドレスのサポート。

使用上のガイドライン

GTP インスペクションから統計情報をクリアするには、このコマンドを使用します。統計情報を表示するには、このコマンドの **show** バージョンを使用します。

例

次に、GTP 統計情報をクリアする例を示します。

```
ciscoasa# clear service-policy inspect gtp statistics
```

関連コマンド

コマンド	説明
inspect gtp	GTP インスペクションをイネーブルにします。
show service-policy inspect gtp	GTP 統計情報を表示します。

clear service-policy inspect m3ua

M3UA インスペクション統計情報をクリアするには、特権 EXEC モードで **clear service-policy inspect m3ua** コマンドを使用します。

clear service-policy inspect m3ua {**drops** | **endpoint** [*ip_address*] | **session** [**assocID** *hex_number*]}

構文の説明

drops	M3UA ドロップの統計情報をクリアします。
endpoint [*ip_address*]	M3UA エンドポイントの統計情報をクリアします。必要に応じて、エンドポイントの IP アドレスを指定して、そのエンドポイントの統計情報のみをクリアできます。
session [**assocID** *hex_number*]	厳密なアプリケーション サーバ プロセス（ASP）状態検証をイネーブルにした場合に追跡される、すべての M3UA セッションをクリアします。 特定のセクションをクリアするには、**assocID** キーワードと 16 進数のセッション番号を追加します。現在のセッションとそのアソシエーション ID を表示するには、**show service-policy inspect m3ua session** コマンドを使用します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。
9.7(1)	**session** キーワードが追加されました。

使用上のガイドライン

M3UA インスペクションから統計情報またはセッションをクリアするには、このコマンドを使用します。統計情報とセッションを表示するには、このコマンドの **show** バージョンを使用します。

例

次に、M3UA エンドポイントの統計情報をクリアする例を示します。

```
ciscoasa# clear service-policy inspect m3ua endpoint
```

次のに、特定の M3UA セッションをクリアする例を示します。

```
ciscoasa(config)# show service-policy inspect m3ua session
1 in use, 1 most used
Flags: d - double exchange      , s - single exchange
AssocID: c0bbe629 in Down state, idle:0:00:06, timeout:0:30:00, s
ciscoasa(config)# clear service-policy inspect m3ua session assocID c0bbe629
```

関連コマンド

コマンド	説明
inspect m3ua	M3UA インスペクションをイネーブルにします。
show service-policy inspect m3ua	M3UA 統計情報を表示します。
strict-asp-state	厳密な M3UA ASP 状態検証をイネーブルにします。

clear service-policy inspect radius-accounting

RADIUS アカウンティング ユーザをクリアするには、特権 EXEC モードで **clear service-policy inspect radius-accounting** コマンドを使用します。

clear service-policy inspect radius-accounting users {**all** | *ip_address* | *policy_map*}

構文の説明

all	すべてのユーザをクリアします。
ip_address	この IP アドレスのユーザをクリアします。
policy_map	このポリシー マップに関連付けられているユーザをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、すべての RADIUS アカウンティング ユーザをクリアする例を示します。

```
ciscoasa# clear service-policy inspect radius-accounting users all
```

clear session

コンフィギュレーション セッションの内容を削除したり、そのアクセス フラグをリセットしたりするには、グローバル コンフィギュレーション モードで **clear session** コマンドを使用します。

clear session *session_name* {**access** | **configuration**}

構文の説明

session_name	既存のコンフィギュレーション セッションの名前。現在のセッションのリストを表示するには、**show configuration session** コマンドを使用します。
access	アクセス フラグをクリアします。このフラグは、セッションが編集中であることを示します。編集セッションが破棄されたことを知っていて、変更を完了するにはセッションを開始する必要がある場合に限り、このフラグをクリアします。
configuration	セッションを削除することなく、セッション内で加えた設定変更をクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、ACL やその他のオブジェクトを編集するために隔離されたセッションを作成する、**configure session** コマンドとともに使用します。

このコマンドの主な用途は、アクセス フラグをリセットすることです。セッションを開くと、このフラグにより、セッションが編集中であることが示されます。その後、セッションをクリーンに終了することなく ASA への接続を解除した場合、フラグは設定されたままになり、そのためにセッションを再度開くことができなくなることがあります。実際には誰もセッションを編集していないことが確実にわかっている場合は、フラグをリセットしてアクセスし直すことができます。

また、このコマンドを使用すると、セッションを削除しないで、変更のセッションを空にすることもできます。作成したセッションが不要になり、セッションで定義した変更をコミットしない場合は、**clear configuration session** コマンドを使用して、セッションおよびセッションに含まれている変更を削除します。

例

次に、my-session のアクセス フラグをリセットする例を示します。

```
ciscoasa(config)# clear session my-session access
```

関連コマンド

コマンド	説明
clear configuration session	コンフィギュレーション セッションとその内容を削除します。
configure session	セッションを作成するか、開きます。
show configuration session	現在の各セッションで行われた変更を表示します。

clear shared license

共有ライセンス統計情報、共有ライセンス クライアント統計情報、および共有ライセンス バックアップ サーバ統計情報を 0 にリセットするには、特権 EXEC モードで **clear shared license** コマンドを使用します。

clear shared license [**all** | **backup** | **client** [*hostname*]]

構文の説明

all	(任意)すべての統計情報をクリアします。これがデフォルト設定です。
backup	(任意)バックアップ サーバの統計情報をクリアします。
client	(任意)すべての参加ユニットの統計情報をクリアします。
hostname	(任意)特定の参加ユニットの統計情報をクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

共有ライセンス カウンタには統計データとエラー データが含まれます。

例

次に、すべての共有ライセンス カウンタをリセットする例を示します。

```
ciscoasa# clear shared license all
```

関連コマンド

コマンド	説明
activation-key	ライセンス アクティベーション キーを入力します。
clear configure license-server	共有ライセンス サーバ コンフィギュレーションをクリアします。

コマンド	説明
license-server address	共有ライセンス サーバの IP アドレスと参加者の共有秘密を指定します。
license-server backup address	参加者の共有ライセンス バックアップ サーバを指定します。
license-server backup backup-id	メインの共有ライセンス サーバのバックアップ サーバの IP アドレスおよびシリアル番号を指定します。
license-server backup enable	共有ライセンス バックアップ サーバになるユニットをイネーブルにします。
license-server enable	共有ライセンス サーバになるユニットをイネーブルにします。
license-server port	サーバが参加者からの SSL 接続をリッスンするポートを設定します。
license-server refresh-interval	サーバと通信する頻度を設定するために参加者に提供される更新間隔を設定します。
license-server secret	共有秘密を共有ライセンス サーバに設定します。
show activation-key	インストールされている現在のライセンスを表示します。
show running-config license-server	共有ライセンス サーバ コンフィギュレーションを表示します。
show shared license	共有ライセンス統計情報を表示します。
show vpn-sessiondb	VPN セッションのライセンス情報を表示します。

clear shun

現在イネーブルであるすべての shun をディセーブルにして、shun 統計情報をクリアするには、特権 EXEC モードで **clear shun** コマンドを使用します。

clear shun [*statistics*]

構文の説明

statistics	（任意）インターフェイス カウンタだけをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、現在イネーブルになっているすべての shun をディセーブルにして、shun 統計情報をクリアする例を示します。

```
ciscoasa(config)# clear shun
```

関連コマンド

コマンド	説明
shun	新規接続を抑制し、既存のすべての接続からのパケットを不許可にすることにより、攻撃元ホストへのダイナミック応答をイネーブルにします。
show shun	回避についての情報を表示します。

clear snmp-server statistics

SNMP サーバ統計情報（SNMP パケットの入力カウンタと出力カウンタ）をクリアするには、特権 EXEC モードで **clear snmp-server statistics** コマンドを使用します。

clear snmp-server statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、SNMP サーバ統計情報をクリアする例を示します。

```
ciscoasa# clear snmp-server statistics
```

関連コマンド

コマンド	説明
clear configure snmp-server	SNMP サーバ コンフィギュレーションをクリアします。
show snmp-server statistics	SNMP サーバ コンフィギュレーション情報を表示します。

clear ssl

デバッグ目的で SSL 情報をクリアするには、特権 EXEC モードで **clear ssl** コマンドを使用します。

clear ssl {cache [**all**] | errors | mib | objects}

構文の説明

all	SSL セッション キャッシュ内のすべてのセッションおよび統計情報をクリアします。
cache	SSL セッション キャッシュ内の期限切れセッションをクリアします。
errors	ssl エラーをクリアします。
mib	SSL MIB 統計情報をクリアします。
objects	SSL オブジェクト統計情報をクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.5(2)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

AnyConnect 機能に影響するため、DTLS キャッシュがクリアされることはありません。

例

次に、SSL キャッシュをクリアし、SSL セッション キャッシュ内のすべてのセッションおよび統計情報をクリアする例を示します。

```
ciscoasa# clear ssl cache
SSL session cache cleared: 2
No SSL VPNLB session cache
No SSLDEV session cache
DLTS caches are not cleared

ciscoasa# clear ssl cache all
```

```
Clearing all sessions and statistics
SSL session cache cleared: 5
No SSL VPNLB session cache
No SSLDEV session cache
DLTS caches are not cleared
```

clear startup-config errors

メモリからコンフィギュレーション エラー メッセージをクリアするには、特権 EXEC モードで **clear startup-config errors** コマンドを使用します。

clear startup-config errors

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASA がスタートアップ コンフィギュレーションをロードしたときに生成されたコンフィギュレーション エラーを表示するには、**show startup-config errors** コマンドを使用します。

例

次に、メモリからすべてのコンフィギュレーション エラーをクリアする例を示します。

```
ciscoasa# clear startup-config errors
```

関連コマンド

コマンド	説明
show startup-config errors	ASA がスタートアップ コンフィギュレーションをロードしたときに生成されたコンフィギュレーション エラーを表示します。

clear sunrpc-server active

Sun RPC アプリケーション インスペクションによって開けられたピンホールをクリアするには、特権 EXEC モードで **clear sunrpc-server active** コマンドを使用します。

clear sunrpc-server active

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

Sun RPC アプリケーション インスペクションによって開けられた、NFS や NIS などのサービス トラフィックが ASA を通過できるようにするピンホールをクリアするには、**clear sunrpc-server active** コマンドを使用します。

例

次に、SunRPC サービス テーブルをクリアする例を示します。

```
ciscoasa# clear sunrpc-server
```

関連コマンド

コマンド	説明
clear configure sunrpc-server	ASA からの Sun リモート プロセッサ コール サービスをクリアします。
inspect sunrpc	Sun RPC アプリケーション インスペクションをイネーブルまたはディセーブルにし、使用されるポートを設定します。
show running-config sunrpc-server	SunRPC サービス コンフィギュレーションに関する情報を表示します。
show sunrpc-server active	アクティブな Sun RPC サービスに関する情報を表示します。

clear terminal

現在の CLI セッションの端末設定をクリアして、デフォルトを使用するには、特権 EXEC モードで **clear terminal** コマンドを使用します。

clear terminal {**interactive** | **pager** [[**lines**] *number*]}

構文の説明

interactive	インタラクティブなヘルプの設定をクリアします(CLI で **?** を入力したときの)。デフォルトではイネーブルになっています。
pager [[**lines**] *number*]]	「---more---」プロンプトが表示されるまでの 1 ページあたりの行数の設定をクリアします。デフォルトは 24 です。

コマンド デフォルト

デフォルトの端末動作は次のとおりです。

- **interactive**:有効
- **pager**:24 回線

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、ポケットベルの設定をクリアする例を示します。

```
ciscoasa# clear terminal pager
```

関連コマンド

コマンド	説明
terminal pager	「---More---」プロンプトが表示されるまでの 1 ページあたりの行数を設定します。
terminal interactive	CLI に ? と入力した場合にヘルプをイネーブルまたはディセーブルにします。

clear threat-detection rate

threat-detection basic-threat コマンドを使用して基本的な脅威の検出をイネーブルにしたときに統計情報をクリアするには、特権 EXEC モードで **clear threat detection rate** コマンドを使用します。

clear threat-detection rate

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

例

次に、レート統計情報をクリアする例を示します。

```
ciscoasa# clear threat-detection rate
```

関連コマンド

コマンド	説明
show running-config all threat-detection	脅威検出コンフィギュレーションを表示します。個別にレート設定をしていない場合はデフォルトのレート設定も表示されます。
show threat-detection rate	基本脅威検出の統計情報を表示します。
threat-detection basic-threat	基本脅威検出をイネーブルにします。
threat-detection rate	イベント タイプごとの脅威検出レート制限を設定します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

clear threat-detection scanning-threat

threat-detection scanning-threat コマンドを使用して脅威検出のスキャンをイネーブルにした後で攻撃者と攻撃対象をクリアするには、特権 EXEC モードで **clear threat-detection scanning-threat** コマンドを使用します。

clear threat-detection scanning-threat [attacker [*ip_address* [*mask*]] | **target** [*ip_address* [*mask*]]

構文の説明

attacker	（任意）攻撃者だけをクリアします。
ip_address	（オプション）特定の IP アドレスをクリアします。
mask	（任意）サブネット マスクを設定します。
target	（任意）攻撃対象だけをクリアします。

デフォルト

IP アドレスを指定しなかった場合は、すべてのホストが解放されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

現在の攻撃者および攻撃対象を表示するには、**show threat-detection scanning-threat** コマンドを使用します。

例

次に、**show threat-detection scanning-threat** コマンドで攻撃対象と攻撃者を表示し、次にすべての攻撃対象をクリアする例を示します。

```
ciscoasa# show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0
    192.168.1.249
   Latest Attacker Host & Subnet List:
    192.168.10.234
    192.168.10.0
    192.168.10.2
    192.168.10.3
```

```
    192.168.10.4
    192.168.10.5
    192.168.10.6
    192.168.10.7
    192.168.10.8
    192.168.10.9
ciscoasa# clear threat-detection scanning-threat target
```

関連コマンド

コマンド	説明
show threat-detection shun	現在回避されているホストを表示します。
show threat-detection statistics host	ホストの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

clear threat-detection shun

threat-detection scanning-threat コマンドを使用して脅威検出のスキャンをイネーブルにし、さらに攻撃元ホストの自動回避もイネーブルにした後で、現在回避されているホストを解放するには、特権 EXEC モードで **clear threat-detection shun** コマンドを使用します。

clear threat-detection shun [*ip_address* [*mask*]]

構文の説明

ip_address	（任意）特定の IP アドレスの回避を解除します。
mask	（任意）回避されているホストの IP アドレスのサブネット マスクを設定します。

デフォルト

IP アドレスを指定しなかった場合は、すべてのホストが解放されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

現在回避されているホストを表示するには、**show threat-detection shun** コマンドを使用します。

例

次に、**show threat-detection shun** コマンドで現在回避されているホストを表示し、ホスト 10.1.1.6 を回避状態から解放する例を示します。

```
ciscoasa# show threat-detection shun
Shunned Host List:
10.1.1.6
198.1.6.7
ciscoasa# clear threat-detection shun 10.1.1.6 255.255.255.255
```

関連コマンド

コマンド	説明
show threat-detection shun	現在回避されているホストを表示します。
show threat-detection statistics host	ホストの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

clear threat-detection statistics

threat-detection statistics tcp-intercept コマンドを使用して TCP 代行受信の統計情報をイネーブルにした後で統計情報をクリアするには、特権 EXEC モードで **clear threat-detection scanning-threat** コマンドを使用します。

clear threat-detection statistics [**tcp-intercept**]

構文の説明

tcp-intercept	（任意）TCP 代行受信の統計情報をクリアします。

デフォルト

TCP 代行受信の統計情報をクリアします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

TCP 代行受信の統計情報を表示するには、**show threat-detection statistics top** コマンドを入力します。

例

次に、**show threat-detection statistics top tcp-intercept** コマンドで TCP 代行受信の統計情報を表示し、次にすべての統計情報をクリアする例を示します。

```
ciscoasa# show threat-detection statistics top tcp-intercept

Top 10 Protected Servers under Attack (sorted by average rate)
Monitoring Window Size: 30 mins    Sampling Interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
--------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3    192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4    192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5    192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6    192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7    192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8    192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
```

```
9    192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10   192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)

ciscoasa# clear threat-detection statistics
```

関連コマンド

コマンド	説明
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
threat-detection statistics	脅威の検出の統計情報をイネーブルにします。

clear traffic

送信アクティビティおよび受信アクティビティのカウンタをリセットするには、特権 EXEC モードで **clear traffic** コマンドを使用します。

clear traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

clear traffic コマンドは、**show traffic** コマンドで表示される送信アクティビティと受信アクティビティのカウンタをリセットします。これらのカウンタは、最後に clear traffic コマンドが入力されてから、または ASA がオンラインになってからの、各インターフェイスを通過したパケット数およびバイト数を示します。また、秒数は、ASA が最後にリブートされてからオンラインである継続時間を示します。

例

次に、**clear traffic** コマンドの例を示します。

```
ciscoasa# clear traffic
```

関連コマンド

コマンド	説明
show traffic	送信アクティビティおよび受信アクティビティのカウンタを表示します。

clear uauth

1 人のユーザまたはすべてのユーザのキャッシュされた認証および認可情報をすべて削除するには、特権 EXEC モードで **clear uauth** コマンドを使用します。

clear uauth [*username*]

構文の説明

username	（オプション）削除するユーザ認証情報をユーザ名で指定します。

デフォルト

username 引数を省略すると、すべてのユーザの認証および認可情報が削除されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

clear uauth コマンドは、1 人のユーザまたはすべてのユーザの AAA 認可および認証のキャッシュを削除します。これにより、これらのユーザは、次回接続を作成するときに、再認証を強制されるようになります。

このコマンドは、**timeout** コマンドとともに使用します。

各ユーザ ホストの IP アドレスには、認可キャッシュが付加されます。正しいホストからキャッシュされているサービスにユーザがアクセスしようとした場合、ASA ではそのアクセスが事前に許可されていると見なし、その接続を即座に代理します。ある Web サイトへのアクセスを一度認可されると、たとえば、イメージを読み込むときに、イメージごとに認可サーバと通信しません（イメージが同じ IP アドレスからであると想定されます）。この処理により、パフォーマンスが大幅に向上され、認可サーバの負荷が削減されます。

このキャッシュでは、ユーザ ホストごとに 16 個までのアドレスとサービスのペアが許可されます。

(注) Xauth をイネーブルにすると、クライアントに割り当てられている IP アドレスのエントリが uauth テーブル(**show uauth** コマンドで表示できます)に追加されます。ただし、ネットワーク拡張モードで Easy VPN Remote 機能とともに Xauth を使用すると、ネットワーク間に IPsec トンネルが作成されるため、ファイアウォールの向こう側にいるユーザを 1 つの IP アドレスに関連付けることができません。したがって、Xauth の完了時に uauth エントリが作成されません。AAA 認可またはアカウンティング サービスが必要となる場合は、AAA 認証プロキシをイネーブルにして、ファイアウォールの向こう側にいるユーザを認証します。AAA 認証プロキシの詳細については、AAA コマンドを参照してください。

ユーザの接続がアイドルになった後にキャッシュを保持する期間を指定するには、**timeout uauth** コマンドを使用します。すべてのユーザのすべての認可キャッシュを削除するには、**clear uauth** コマンドを使用します。次回接続を作成するときには再認証される必要が生じます。

例

次に、ユーザの再認証を実行する例を示します。

```
ciscoasa(config)# clear uauth user
```

関連コマンド

コマンド	説明
aaa authentication	**aaa-server** コマンドで指定されたサーバ上の LOCAL、TACACS+、または RADIUS のユーザ認証をイネーブル化、ディセーブル化、または表示します。
aaa authorization	**aaa-server** コマンドで指定されたサーバ上の TACACS+ または RADIUS のユーザ認可をイネーブル化、ディセーブル化、または表示します。
show uauth	現在のユーザの認証情報と認可情報を表示します。
timeout	アイドル時間の最大継続期間を設定します。

clear uc-ime

Cisco Intercompany Media Engine プロキシに関する統計情報を表示するために使用されるカウンタをクリアするには、特権 EXEC モードで **clear uc-ime** コマンドを使用します。

clear uc-ime [[**mapping-service-sessions** | **signaling-sessions** | **fallback-notification**] **statistics**]

構文の説明

fallback-notification	(任意)フォールバック通知の統計情報のカウンタをクリアします。
mapping-service-sessions	(任意)マッピング サービス セッションの統計情報のカウンタをクリアします。
signaling-sessions	(任意)シグナリング セッションの統計情報のカウンタをクリアします。
statistics	(任意)クリアする Cisco Intercompany Media Engine プロキシのカウンタを設定するキーワードです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

例

次に、シグナリング セッションの統計情報を表示するために使用されるカウンタをクリアする例を示します。

```
ciscoasa# clear configure signaling-sessions statistics
```

関連コマンド

コマンド	説明
clear configure uc-ime	ASA 上の Cisco Intercompany Media Engine プロキシの実行コンフィギュレーションをクリアします。
show running-config uc-ime	Cisco Intercompany Media Engine プロキシの実行コンフィギュレーションを表示します。

コマンド	説明
show uc-ime	フォールバック通知、マッピング サービス セッション、およびシグナリング セッションに関する統計情報または詳細情報を表示します。
uc-imc	Cisco Intercompany Media Engine プロキシ インスタンスを ASA に作成します。

clear url-block block statistics

ブロック バッファ使用状況カウンタをクリアするには、特権 EXEC モードで **clear url-block block statistics** コマンドを使用します。

clear url-block block statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

clear url-block block statistics コマンドは、ブロック バッファ使用状況カウンタ（Current number of packets held (global) カウンタは除く）をクリアします。

例

次に、URL ブロック統計情報をクリアし、クリア後のカウンタのステータスを表示する例を示します。

```
ciscoasa# clear url-block block statistics
ciscoasa# show url-block block statistics

URL Pending Packet Buffer Stats with max block  0
-----------------------------------------------------
Cumulative number of packets held: | 0
Maximum number of packets held (per URL): | 0
Current number of packets held (global): | 38
Packets dropped due to
| exceeding url-block buffer limit: | 0
| HTTP server retransmission: | 0
Number of packets released back to client: | 0
```

関連コマンド

コマンド	説明
filter url	トラフィックを URL フィルタリング サーバに送ります。
show url-block	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-block	Web サーバ応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

clear url-cache statistics

コンフィギュレーションから **url-cache** コマンド ステートメントを削除するには、特権 EXEC モードで **clear url-cache** コマンドを使用します。

clear url-cache statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

clear url-cache コマンドは、コンフィギュレーションから URL キャッシュ統計情報を削除します。

URL キャッシュを使用しても、Websense プロトコル バージョン 1 の Websense アカウンティング ログはアップデートされません。Websense プロトコル バージョン 1 を使用している場合は、Websense を実行してログを記録し、Websense アカウンティング情報を表示できるようにします。目的のセキュリティ要求を満たす使用状況プロファイルを取得したら **url-cache** コマンドを入力してスループットを増大させます。Websense プロトコル バージョン 4 および N2H2 URL フィルタリングでは、**url-cache** コマンドの使用時にアカウンティング ログが更新されます。

例

次に、URL キャッシュ統計情報をクリアする例を示します。

```
ciscoasa# clear url-cache statistics
```

関連コマンド

コマンド	説明
filter url	トラフィックを URL フィルタリング サーバに送ります。
show url-cache statistics	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

clear url-server

URL フィルタリング サーバの統計情報をクリアするには、特権 EXEC モードで **clear url-server** コマンドを使用します。

clear url-server statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

clear url-server コマンドは、コンフィギュレーションから URL フィルタリング サーバの統計情報を削除します。

例

次に、URL サーバの統計情報をクリアする例を示します。

```
ciscoasa# clear url-server statistics
```

関連コマンド

コマンド	説明
filter url	トラフィックを URL フィルタリング サーバに送ります。
show url-server	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。

コマンド	説明
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

clear user-identity active-user-database

アイデンティティ ファイアウォールのために特定のユーザのステータスをログアウトに設定するには、特権 EXEC モードで **clear user-identity active-user-database** コマンドを使用します。

clear user-identity active-user-database [**user** [*domain_nickname*\]*use_rname*] | **user-group** [*domain_nickname*\\]*user_group_name*]

構文の説明

*domain_nickname**user_group_name*	統計情報をクリアする対象のユーザ グループを指定します。 *group_name* には、[a-z]、[A-Z]、[0-9]、[!@#$%^&()-_{}.] など、あらゆる文字を使用できます。*domain_NetBIOS_name**group_name* にスペースを含める場合は、ドメイン名とユーザ名を引用符で囲む必要があります。
*domain_nickname**use_rname*	統計情報をクリアする対象のユーザを指定します。 *user_name* には、[a-z]、[A-Z]、[0-9]、[!@#$%^&()-_{}.] など、あらゆる文字を使用できます。*domain_NetBIOS_name**user_name* にスペースを含める場合は、ドメイン名とユーザ名を引用符で囲む必要があります。
user	ユーザの統計情報をクリアすることを指定します。
user-group	ユーザ グループの統計情報をクリアすることを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、指定したユーザ、指定したユーザ グループに属するすべてのユーザ、またはすべてのユーザのステータスをログアウトに設定します。

user-group キーワードを指定すると、指定したユーザ グループに属するすべてのユーザのステータスがログアウトに設定されます。**user-group** キーワードとともに *domain_nickname* 引数を指定しない場合、デフォルト ドメイン内の *user_group_name* というグループに属するユーザのステータスがログアウトに設定されます。

user キーワードを指定すると、指定したユーザのステータスがログアウトに設定されます。**user** キーワードとともに *domain_nickname* 引数を指定しない場合、デフォルト ドメイン内の *user_name* というユーザのステータスがログアウトに設定されます。

user キーワードも **user-group** キーワードも指定しない場合、すべてのユーザのステータスがログアウトに設定されます。

例

次に、SAMPLE ドメインのユーザ グループ users1 に属するすべてのユーザのステータスをログアウトに設定する例を示します。

```
ciscoasa# clear user-identity active-user-database user-group SAMPLE\users1
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。
show user-identity user active	アイデンティティ ファイアウォールのアクティブ ユーザを表示します。

clear user-identity ad-agent statistics

アイデンティティ ファイアウォールの AD エージェント統計情報をクリアするには、特権 EXEC モードで **clear user-identity ad-agent statistics** コマンドを使用します。

clear user-identity ad-agent statistics

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

ASA は、プライマリ AD エージェントおよびセカンダリ AD エージェントに関する次の情報を保持します。

- AD エージェントのステータス
- ドメインのステータス
- AD エージェントの統計情報

AD エージェントの統計データをクリアするには、**clear user-identity ad-agent statistics** コマンドを使用します。

例

次に、アイデンティティ ファイアウォールの AD エージェント統計情報をクリアする例を示します。

```
ciscoasa# clear user-identity ad-agent statistics
ciscoasa# show user-identity ad-agent statistics

    Primary AD Agent                Total  Last Activity
    ------------------------  ----------  ------------------------
    Input packets:                     0  N/A
    Output packets:                    0  N/A
    Send updates:                      0  N/A
```

```
Recv updates:                        0  N/A
Keepalive failed:                    0  N/A
Send update failed:                  0  N/A
Query failed:                        0  N/A

Secondary AD Agent              Total  Last Activity
------------------------  ----------  ------------------------
Input packets:                       0  N/A
Output packets:                      0  N/A
Send updates:                        0  N/A
Recv updates:                        0  N/A
Keepalive failed:                    0  N/A
Send update failed:                  0  N/A
Query failed:                        0  N/A
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。
show user-identity ad-agent [**statistics**]	アイデンティティ ファイアウォールの AD エージェントに関する統計情報を表示します。

clear user-identity statistics

アイデンティティ ファイアウォールに関する統計情報を表示するために使用されるカウンタをクリアするには、特権 EXEC モードで **clear user-identity statistics** コマンドを使用します。

clear user-identity statistics [**user** [*domain_nickname*\\]*use_rname*] | **user-group** [*domain_nickname*\\]*user_group_name*]

構文の説明

*domain_nickname**user_group_name*	統計情報をクリアする対象のユーザ グループを指定します。 *group_name* には、[a-z]、[A-Z]、[0-9]、[!@#$%^&()-_{}.] など、あらゆる文字を使用できます。*domain_NetBIOS_name**group_name* にスペースを含める場合は、ドメイン名とユーザ名を引用符で囲む必要があります。
*domain_nickname**use_rname*	統計情報をクリアする対象のユーザを指定します。 *user_name* には、[a-z]、[A-Z]、[0-9]、[!@#$%^&()-_{}.] など、あらゆる文字を使用できます。*domain_NetBIOS_name**user_name* にスペースを含める場合は、ドメイン名とユーザ名を引用符で囲む必要があります。
user	ユーザの統計情報をクリアすることを指定します。
user-group	ユーザ グループの統計情報をクリアすることを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

domain_nickname が *user_group_name* よりも前に指定されていない場合、ASA はデフォルト ドメイン内の *user_group_name* というグループのアイデンティティ ファイアウォール統計情報を削除します。

domain_nickname が *user_name* よりも前に指定されていない場合、ASA はデフォルト ドメイン内の *user_name* というユーザのアイデンティティ ファイアウォール統計情報を削除します。

例

次に、ユーザ グループの統計情報を表示するために使用されるカウンタをクリアする例を示します。

```
ciscoasa# clear user-identity statistics user-group SAMPLE\users1
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。
show user-identity statistics	アイデンティティ ファイアウォールのユーザまたはユーザ グループの統計情報を表示します。

clear user-identity user-not-found

アイデンティティ ファイアウォールの ASA ローカル user-not-found データベースをクリアするには、特権 EXEC モードで **clear user-identity user-not-found** コマンドを使用します。

clear user-identity user-not-found

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

ASA は、Microsoft Active Directory で見つからない IP アドレスのローカル user-not-found データベースを保持します。ASA は、データベースのリスト全体ではなく、user-not-found リストの最後の 1024 パケットのみを保持します（同じ送信元 IP アドレスからの連続するパケットは 1 つのパケットとして扱われます）。

ASA 上のローカル データベースをクリアするには、**clear user-identity user-not-found** コマンドを使用します。

ヒント Microsoft Active Directory で見つからないユーザの IP アドレスを表示するには、**show user-identity user-not-found** コマンドを使用します。

例

次に、アイデンティティ ファイアウォールのローカル user-not-found データベースをクリアする例を示します。

```
ciscoasa# show user-identity user-not-found
172.13.1.2
171.1.45.5
169.1.1.2
172.13.12
ciscoasa# clear user-identity user-not-found
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。
show user-identity user-not-found	ASA user-not-found データベースで見つからない Active Directory ユーザの IP アドレスを表示します。

clear user-identity user no-policy-activated

アイデンティティ ファイアウォール用にアクティブ化されていないユーザの ASA でローカル レコードをクリアするには、特権 EXEC モードで **clear user-identity user no-policy-activated** コマンドを使用します。

clear user-identity user no-policy-activated

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

どのセキュリティ ポリシーでもアクティブ化されていないユーザ、つまり、アクティブ化されたユーザ グループに属していないか、アクセス リストまたはサービス ポリシー コンフィギュレーションで参照されていないユーザのローカル レコードをクリアするには、**clear user-identity user no-policy-activated** を使用します。

また、**clear user-identity user no-policy-activated** コマンドは、アクティブであるもののまだアクティブ化されていないユーザの IP アドレスもクリアします。

アイデンティティ ファイアウォールのユーザ グループを作成する場合、そのグループをアクティブ化する必要があります。つまり、グループはインポート ユーザ グループ(アクセス リストまたはサービス ポリシー コンフィギュレーションでユーザ グループとして定義)またはローカル ユーザ グループ(オブジェクト グループ ユーザで定義)です。

例

次に、アクティブ化されていないユーザの ASA 上でローカル レコードをクリアする例を示します。

```
ciscoasa# clear user-identity user no-policy-activated
```

関連コマンド

コマンド	説明
clear configure user-identity	アイデンティティ ファイアウォール機能の設定をクリアします。
show user-identity group	アイデンティティ ファイアウォールのアクティブ化されたユーザ グループのリストを表示します。

clear vpn cluster stats internal

VPN クラスタリングの内部カウンタをクリアするには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで次のコマンドを使用します。

clear vpn cluster stats internal

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.9(1)	コマンドが追加されました。

関連コマンド

コマンド	説明
show vpn cluster stats internal	すべての VPN クラスタ カウンタを表示します。

clear vpn-sessiondb statistics

すべての統計情報、特定のセッション、特定のプロトコルなど VPN セッションに関する情報をクリアするには、特権 EXEC モードで **clear vpn-sessiondb statistics** コマンドを使用します。

clear vpn-sessiondb {**all** | **anyconnect** | **failover** | **email-proxy** | **global** | **index** *index_number* | **ipaddress** *IPaddr* | **l2l** | **name** *username* | **protocol** *protocol* | **ra-ikev1-ipsec** | **ra-ikev2-ipsec** | **tunnel-group** *name* | **vpn-lb** | **webvpn**}

構文の説明

all	すべてのセッションの統計情報をクリアします。
anyconnect	AnyConnect VPN クライアント セッションの統計情報をクリアします。
failover	フェールオーバー IPsec セッションの統計情報をクリアします。
email-proxy	(廃止)電子メール プロキシ セッションの統計情報をクリアします。
global	グローバル セッション データの統計情報をクリアします。
index *indexnumber*	インデックス番号を指定して単一のセッションの統計情報をクリアします。**show vpn-sessiondb detail** コマンドの出力には、セッションごとにインデックス番号が表示されます。
ipaddress *IPaddr*	指定した IP アドレスのセッションの統計情報をクリアします。
l2l	VPN LAN-to-LAN セッションの統計情報をクリアします。
protocol *protocol*	次のプロトコルの統計情報をクリアします。 • ikev1:IKEv1 プロトコルを使用したセッション。 • ikev2:IKEv2 プロトコルを使用したセッション。 • ipsec:IKEv1 または IKEv2 を使用した IPsec セッション。 • ipseclan2lan:IPsec LAN-to-LAN セッション。 • ipseclan2lanovernatt:IPsec LAN-to-LAN over NAT-T セッション。 • ipsecovernatt:IPsec over NAT-T セッション。 • ipsecovertcp:IPsec over TCP セッション。 • ipsecoverudp:IPsec over UDP セッション。 • l2tpOverIpSec:L2TP over IPsec セッション。 • l2tpOverIpsecOverNatT:NAT-T を介した L2TP over IPsec セッション。 • ospfv3:OSPFv3 over IPsec セッション。 • webvpn:クライアントレス SSL VPN セッション。 • imap4s:IMAP4 セッション。 • pop3s:POP3 セッション。 • smtps:SMTP セッション。 • anyconnectParent:セッションに使用されるプロトコルに関係なく、AnyConnect クライアント セッション(AnyConnect IPsec IKEv2 セッションおよび SSL セッションを終了します)。 • ssltunnel:SSL を使用した AnyConnect セッションやクライアントレス SSL VPN セッションを含めた、SSL VPN セッション。 • dtlstunnel:DTLS がイネーブルになっている AnyConnect クライアント セッション。

ra-ikev1-ipsec	IPsec IKEv1 セッションおよび L2TP セッションに関する統計情報をクリアします。
ra-ikev2-ipsec	IPsec IKEv2 セッションの統計情報をクリアします。
tunnel-group *groupname*	指定したトンネル グループ(接続プロファイル)のセッションの統計情報をクリアします。
vpn-lb	VPN ロード バランシング管理セッションの統計情報をクリアします。
webvpn	クライアントレス SSL VPN セッションの統計情報をクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.3(2)	**ra-ikev2-ipsec** キーワードが追加されました。
9.8(1)	**email-proxy** オプションが廃止されました。

clear wccp

WCCP 情報をリセットするには、特権 EXEC モードで **clear wccp** コマンドを使用します。

clear wccp [**web-cache** | *service_number*]

構文の説明

web-cache	Web キャッシュ サービスを指定します。
service-number	ダイナミック サービス ID。このサービスの定義は、キャッシュによって示されます。ダイナミック サービス番号は 0 ～ 255 の範囲で指定できます。**web-cache** キーワードで指定される Web キャッシュ サービスを含めると、許可される最大数は 256 個です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、Web キャッシュ サービスの WCCP 情報をリセットする例を示します。

```
ciscoasa# clear wccp web-cache
```

関連コマンド

コマンド	説明
show wccp	WCCP コンフィギュレーションを表示します。
wccp redirect	WCCP リダイレクションのサポートをイネーブルにします。

clear webvpn sso-server statistics

WebVPN シングル サインオン（SSO）サーバの統計情報をリセットするには、特権 EXEC モードで **clear webvpn sso-server statistics** コマンドを使用します。

clear webvpn sso-server statistics *servername*

構文の説明

servername	リセットする SSO サーバの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、「保留要求」の統計情報をリセットしません。

例

次に、暗号アクセラレータ統計情報を表示する例を示します。

```
ciscoasa # clear webvpn sso-server statistics
ciscoasa #
```

関連コマンド

コマンド	説明
clear crypto accelerator statistics	暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報をクリアします。
clear crypto protocol statistics	暗号アクセラレータ MIB にあるプロトコル固有の統計情報をクリアします。
show crypto accelerator statistics	暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報を表示します。
show crypto protocol statistics	暗号アクセラレータ MIB からプロトコル固有の統計情報を表示します。

clear xlate

現在のダイナミック変換および接続情報をクリアするには、特権 EXEC モードで **clear xlate** コマンドを使用します。

clear xlate [**global** *ip1*[**-***ip2*] [**netmask** *mask*]] [**local** *ip1*[**-***ip2*] [**netmask** *mask*]]
[**gport** *port1*[**-***port2*]] [**lport** *port1*[**-***port2*]] [**interface** *if_name*] [**state** *state*]

構文の説明

global *ip1*[**-***ip2*]	(任意)グローバル IP アドレスまたはアドレスの範囲を指定して、アクティブな変換をクリアします。
gport *port1*[*-port2*]	(任意)グローバル ポートまたはポートの範囲を指定して、アクティブな変換をクリアします。
interface *if_name*	(任意)アクティブな変換をインターフェイス別に表示します。
local *ip1*[**-***ip2*]	(任意)ローカル IP アドレスまたはアドレスの範囲を指定して、アクティブな変換をクリアします。
lport *port1*[*-port2*]	(任意)ローカル ポートまたはポートの範囲を指定して、アクティブな変換をクリアします。
netmask *mask*	(任意)グローバル IP アドレスまたはローカル IP アドレスを限定するネットワーク マスクを指定します。
state *state*	(任意)状態を指定して、アクティブな変換をクリアします。次の 1 つ以上の状態を入力できます。 • **static**:スタティック変換を指定します。 • **portmap**:PAT グローバル変換を指定します。 • **norandomseq**:**norondomseq** 設定での **nat** または**スタティック**変換を指定します。 • **identity**:**nat 0** 識別アドレス変換を指定します。 複数の状態を指定する場合は、状態をスペースで区切ってください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

clear xlate コマンドは、変換スロットの内容をクリアします(「xlate」は変換スロットを意味します)。変換スロットは、キーの変更が行われた後でも存続できます。**clear xlate** コマンドは、コンフィギュレーション内の **global** コマンドまたは **nat** コマンドを追加、変更、または削除した後に必ず使用してください。

xlate は、NAT または PAT セッションについて記述します。これらのセッションは、**detail** オプションを指定した **show xlate** コマンドで表示できます。xlate には、スタティックとダイナミックという 2 つのタイプがあります。

スタティック xlate は、**static** コマンドを使用して作成される永続的な xlate です。**clear xlate** コマンドは、スタティック エントリ内のホストをクリアしません。スタティック xlate は、コンフィギュレーションから **static** コマンドを削除することによってのみ削除できます。**clear xlate** コマンドは、スタティック変換ルールを削除しません。コンフィギュレーションから static コマンドを削除しても、スタティック ルールを使用する既存の接続はトラフィックを引き続き転送できます。これらの接続を無効にするには、**clear local-host** コマンドまたは **clear conn** コマンドを使用します。

ダイナミック xlate は、**nat** コマンドまたは **global** コマンドを介したトラフィック処理で必要に応じて作成される xlate です。**clear xlate** コマンドを実行すると、ダイナミック xlate および関連付けられた接続が削除されます。また、**clear local-host** コマンドまたは **clear conn** コマンドを使用して、xlate および関連する接続をクリアすることもできます。コンフィギュレーションから **nat** コマンドまたは **global** コマンドを削除した場合、ダイナミック xlate および関連する接続がアクティブのまま残る場合があります。これらの接続を削除するには、**clear xlate** コマンドを使用します。

例

次に、現在の変換および接続スロット情報をクリアする例を示します。

```
ciscoasa# clear xlate global
```

関連コマンド

コマンド	説明
clear local-host	ローカル ホストのネットワーク情報をクリアします。
clear uauth	キャッシュされたユーザ認証および認可情報をクリアします。
show conn	すべてのアクティブ接続を表示します。
show local-host	ローカル ホスト ネットワーク情報を表示します。
show xlate	現在の変換情報を表示します。

client コマンド ～ crl enforcenextupdate コマンド

client（CTL プロバイダー）

証明書信頼リスト プロバイダーへの接続が許可されるクライアントを指定するか、またはクライアント認証用のユーザ名とパスワードを指定するには、CTL プロバイダー コンフィギュレーション モードで **client** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

client {[**interface** *if_name*] *ipv4_addr* | **username** *user_name* **password** *password* [**encrypted**]}

no client {[**interface** *if_name*] *ipv4_addr* | **username** *user_name* **password** *password* [**encrypted**]}

構文の説明

encrypted	パスワードの暗号化を指定します。
interface *if_name*	接続が許可されるインターフェイスを指定します。
ipv4_addr	クライアントの IP アドレスを指定します。
password *password*	クライアント認証用のパスワードを指定します。
username *user_name*	クライアント認証用のユーザ名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
Ctl プロバイダー コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

CTL プロバイダーへの接続を許可されるクライアントを指定し、クライアント認証用のユーザ名とパスワードを設定するには、CTL プロバイダー コンフィギュレーション モードで **client** コマンドを使用します。複数のコマンドを発行して、複数のクライアントを定義できます。ユーザ名とパスワードは、CallManager クラスタ用の CCM 管理者のユーザ名およびパスワードと一致する必要があります。

例

次の例は、CTL プロバイダー インスタンスを作成する方法を示しています。

```
ciscoasa(config)# ctl-provider my_ctl
ciscoasa(config-ctl-provider)# client interface inside 172.23.45.1
ciscoasa(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
ciscoasa(config-ctl-provider)# export certificate ccm_proxy
ciscoasa(config-ctl-provider)# ctl install
```

関連コマンド

コマンド	説明
ctl	CTL クライアントの CTL ファイルを解析し、トラストポイントをインストールします。
ctl-provider	CTL プロバイダー コンフィギュレーション モードで CTL プロバイダー インスタンスを設定します。
export	クライアントにエクスポートする証明書を指定します。
service	CTL プロバイダーがリッスンするポートを指定します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

client（TLS プロキシ）

TLS プロキシのトラストポイント、キー ペア、および暗号スイートを設定するには、TLS プロキシ コンフィギュレーション モードで **client** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

client {**cipher-suite** *cipher_list* | **ldc** {**issuer** *ca_tp_name* | **key-pair** *key_label*} | **trust-point** *proxy_trustpoint* | **clear-text**}

no client {**cipher-suite** *cipher_list* | **ldc** {**issuer** *ca_tp_name* | **key-pair** *key_label*} | **trust-point** *proxy_trustpoint* | **clear-text**}

構文の説明

cipher-suite *cipher_list*	暗号スイートを指定します。プラットフォームで使用可能なオプションを表示するには、暗号化リストに ? と入力します。
clear-text	ASA と TLS サーバ間の通信がクリア テキストで行われることを指定します（暗号化なし）。
ldc issuer *ca_tp_name*	クライアントのローカル ダイナミック証明書を発行するローカル CA トラストポイントを指定します。
ldc keypair *key_label*	クライアントのローカル ダイナミック証明書で使用する RSA キー ペアを指定します。
trust-point *proxy_trustpoint*	ローカル ダイナミック証明書の発行ではなく、スタティック証明書を使用するトラストポイントを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
TLS プロキシ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.0(4)	**trust-point** キーワードが追加されました。
9.6(1)	**clear-text** キーワードが追加されました。

使用上のガイドライン

いくつかのプロトコル検査エンジンでは、検査に必要である暗号化されたトラフィックの復号に TLS プロキシを使用します。検査の後、トラフィックはこのプロキシにより再度暗号化して宛先へ送信されます。

TLS プロキシで TLS クライアント ロールとして動作する場合、ASA の TLS ハンドシェイク パラメータを制御するには、TLS プロキシ コンフィギュレーション モードで **client** コマンドを使用します。

クライアント トラストポイントには次のオプションがあります。

- ローカル ダイナミック証明書の発行者を識別するには、**client ldc** コマンドを使用します。クライアントごとに一意の証明書が必要な場合は、このオプションを使用します。たとえば、SIP/SCCP インスペクション時の Cisco IP Phone の場合などです。クライアントの（**crypto ca trustpoint** コマンドで定義された）ダイナミック証明書を発行するローカル CA を識別するには、**ldc issuer** コマンドを使用します。トラストポイントには、**proxy-ldc-issuer** コマンドが設定されているか、デフォルトのローカル CA サーバ（LOCAL-CA-SERVER）が必要です。

  crypto key generate コマンドで生成されたキーペアを識別するには、**ldc key-pair** コマンドを使用します。

- スタティック証明書を使用するトラストポイントを識別するには、**client trust-point** コマンドを使用します。たとえば、SIP/SCCP インスペクション時の Cisco Unified Presence Server（CUPS）の場合です。この証明書は ASA が所有する必要があります（アイデンティティ証明書）。証明書には、自己署名証明書、認証局に登録されている証明書、またはインポートされたクレデンシャルの証明書を使用できます。

- TLS サーバとの非暗号化通信を使用するには、**client clear-text** コマンドを使用します。このオプションは、ASA および TLS サーバが同じであるデータセンターに配置されており、通信の安全性を確信できる場合に使用できます。この設定は、Diameter インスペクションを目的としています。

また、**client cipher-suite** を使用して TLS プロキシに別の暗号スイートを設定することもできます。TLS プロキシが使用可能な暗号方式を定義しなかった場合、プロキシは **ssl encryption** コマンドによって定義された暗号スイートを使用します。このコマンドが定義されていない場合は、使用可能なすべての暗号方式が使用されます。ASA で一般に使用可能なものとは異なるスイートを使用する場合にのみ、このコマンドを指定します。このコマンドでは、2 つの TLS セッション間で異なる暗号方式を設定できます。CallManager サーバでは、AES 暗号を使用する必要があります。

例

次に、ローカル ダイナミック証明書の発行者を使用して TLS プロキシを作成する例を示します。

```
ciscoasa(config)# tls-proxy my_proxy
ciscoasa(config-tlsp)# server trust-point ccm_proxy
ciscoasa(config-tlsp)# client ldc issuer ldc_server
ciscoasa(config-tlsp)# client ldc keypair phone_common
```

次に、トラストポイントとスタティック証明書を使用して TLS プロキシを作成する例を示します。

```
ciscoasa(config)# tls-proxy my_proxy
ciscoasa(config-tlsp)# server trust-point ccm_proxy
ciscoasa(config-tlsp)# client trust-point ent_y_proxy
```

次に、ASA と Diameter サーバ間でクリア テキスト通信を使用する Diameter インスペクション用の TLS プロキシを作成する例を示します。

```
ciscoasa(config)# tls-proxy diameter-tls-offload-proxy
ciscoasa(config-tlsp)# server trust-point tls-proxy-server-tp
ciscoasa(config-tlsp)# client clear-text
```

関連コマンド

コマンド	説明
ctl-provider	CTL プロバイダー インスタンスを定義し、CTL プロバイダー コンフィギュレーション モードを開始します。
server trust-point	TLS ハンドシェイク中に提示するプロキシ トラストポイント証明書を指定します。
show tls-proxy	TLS プロキシを表示します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

client-access-rule

ASA を通して IPsec 経由で接続できるリモート アクセス クライアントのタイプとバージョンを制限するルールを設定するには、グループ ポリシー コンフィギュレーション モードで **client-access-rule** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

client-access-rule *priority* {**permit** | **deny**} **type** *type* **version** *version* | **none**

no client-access-rule *priority* [{**permit** | **deny**} **type** *type* **version** *version*]

構文の説明

deny	特定のタイプとバージョンのデバイスの接続を拒否します。
none	クライアント アクセス ルールを許可しません。**client-access-rule** をヌル値に設定します。これにより制限が許可されなくなります。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。
permit	特定のタイプとバージョンのデバイスの接続を許可します。
priority	ルールのプライオリティを決定します。最小の整数値を持つルールは、プライオリティが最も高くなります。したがって、クライアントのタイプとバージョン(またはこのいずれか)に一致する最も小さい整数のルールが、適用されるルールとなります。プライオリティの低いルールに矛盾がある場合、ASA はそのルールを無視します。
type *type*	VPN 3002 などの自由形式のストリングを使用して、デバイス タイプを指定します。文字列は、* 文字をワイルドカードとして使用できる点を除き、**show vpn-sessiondb remote** コマンド出力で表示される値と完全に一致する必要があります。
version *version*	7.0 などの自由形式のストリングを使用して、デバイス バージョンを指定します。文字列は、* 文字をワイルドカードとして使用できる点を除き、**show vpn-sessiondb remote** コマンド出力で表示される値と完全に一致する必要があります。

デフォルト

デフォルトでは、アクセス ルールはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

すべてのルールを削除するには、*priority* 引数だけを指定して **no client-access-rule** コマンドを使用します。これにより、**client-access-rule none** コマンドを発行して作成されたヌル ルールを含む、設定済みのすべてのルールが削除されます。

クライアント アクセス ルールがない場合、ユーザはデフォルトのグループ ポリシー内に存在するすべてのルールを継承します。ユーザがクライアント アクセス ルールを継承しないようにするには、**client-access-rule none** コマンドを使用します。これにより、すべてのクライアント タイプおよびバージョンが接続できるようになります。

次の注意に従ってルールを作成します。

- ルールを定義しない場合、ASA はすべての接続タイプを許可します。
- クライアントがいずれのルールにも一致しない場合、ASA は接続を拒否します。つまり、拒否ルールを定義する場合は、許可ルールも 1 つ以上定義する必要があります。許可ルールを定義しないと、ASA はすべての接続を拒否します。
- ソフトウェア クライアントとハードウェア クライアントの両方について、タイプおよびバージョンが **show vpn-sessiondb remote** コマンド出力で表示される値と完全に一致する必要があります。
- * 文字はワイルドカードであり、各ルールで複数回使用できます。たとえば、**client-access-rule 3 deny type * version 3.*** は、リリース バージョン 3.x ソフトウェアを実行しているすべてのクライアント タイプを拒否する、プライオリティ 3 のクライアント アクセス ルールを作成します。
- 1 つのグループ ポリシーにつき最大 25 のルールを作成できます。
- ルール セット全体に対して 255 文字の制限があります。
- クライアントのタイプとバージョンを送信しないクライアントに対して n/a を使用できます。

例

次に、FirstGroup という名前のグループ ポリシーのクライアント アクセス ルールを作成する例を示します。これらのルールは、ソフトウェア バージョン 4.1 を実行している VPN クライアントを許可する一方で、すべての VPN 3002 ハードウェア クライアントを拒否します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# client-access-rule 1 d t VPN3002 v *
ciscoasa(config-group-policy)# client-access-rule 2 p * v 4.1
```

client-bypass-protocol

ASA が IPv6 トラフィックだけを予期しているときの IPv4 トラフィックの管理方法や、IPv4 トラフィックだけを予期しているときの IPv6 トラフィックの管理方法を設定するには、グループ ポリシー コンフィギュレーション モードで **client-bypass-protocol** コマンドを使用します。クライアント バイパス プロトコル設定をクリアするには、このコマンドの **no** 形式を使用します。

client-bypass-protocol {**enable** | **disable**}

no client-bypass-protocol {**enable** | **disable**}

構文の説明

enable	クライアント バイパス プロトコルがイネーブルの場合、ASA が IP アドレスのタイプを割り当てなかった IP トラフィックは、クライアントからクリア テキストとして送信されます。
disable	クライアント バイパス プロトコルがディセーブルの場合、ASA が IP アドレスのタイプを割り当てなかった IPv6 トラフィックはドロップされます。

デフォルト

クライアント バイパス プロトコルは、DfltGrpPolicy でデフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

Client Bypass Protocol 機能を使用すると、ASA が IPv6 トラフィックだけを予期しているときの IPv4 トラフィックの管理方法や、IPv4 トラフィックだけを予期しているときの IPv6 トラフィックの管理方法を設定することができます。

AnyConnect クライアントが ASA に VPN 接続するときに、ASA は IPv4 と IPv6 の一方または両方のアドレスを割り当てます。ASA が AnyConnect 接続に IPv4 アドレスまたは IPv6 アドレスだけを割り当てた場合に、ASA が IP アドレスを割り当てなかったネットワーク トラフィックについて、クライアント プロトコル バイパスによってそのトラフィックをドロップさせるか、または ASA をバイパスしてクライアントからの暗号化なし、つまり「クリア テキスト」としての送信を許可するかを設定できるようになりました。

たとえば、IPv4 アドレスのみ AnyConnect 接続に割り当てられ、エンドポイントがデュアル スタックされていると想定してください。このエンドポイントが IPv6 アドレスへの到達を試みたときに、クライアント バイパス プロトコル機能がディセーブルの場合は、IPv6 トラフィックがドロップされますが、クライアント バイパス プロトコルがイネーブルの場合は、IPv6 トラフィックはクライアントからクリア テキストとして送信されます。

例

次に、クライアント バイパス プロトコルをイネーブルにする例を示します。

```
hostname(config-group-policy)# client-bypass-protocol enable
hostname(config-group-policy)#
```

次に、クライアント バイパス プロトコルをデイセーブルにする例を示します。

```
hostname(config-group-policy)# client-bypass-protocol disable
hostname(config-group-policy)#
```

次に、クライアント バイパス プロトコル設定をクリアする例を示します。

```
hostname(config-group-policy)# no client-bypass-protocol enable
hostname(config-group-policy)#
```

client-firewall

IKE トンネルのネゴシエーション時に ASA が VPN クライアントにプッシュするパーソナル ファイアウォール ポリシーを設定するには、グループ ポリシー コンフィギュレーション モードで **client-firewall** コマンドを使用します。ファイアウォール ポリシーを削除するには、このコマンドの **no** 形式を使用します。

client-firewall none

no client-firewall {**opt** | **req**} **custom vendor-id** *num* **product-id** *num* **policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl*} [**description** *string*]

client-firewall {**opt** | **req**} **zonelabs-integrity**

(注) ファイアウォールのタイプを **zonelabs-integrity** にする場合は、引数を指定しないでください。ポリシーは、Zone Labs Integrity サーバによって決められます。

client-firewall {**opt** | **req**} **zonelabs-zonealarm policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl*}

client-firewall {**opt** | **req**} **zonelabs-zonealarmorpro policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl*}

client-firewall {**opt** | **req**} **zonelabs-zonealarmpro policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl*}

client-firewall {**opt** | **req**} **cisco-integrated acl-in** *acl* **acl-out** *acl*}

client-firewall {**opt** | **req**} **sygate-personal**

client-firewall {**opt** | **req**} **sygate-personal-pro**

client-firewall {**opt** | **req**} **sygate-personal-agent**

client-firewall {**opt** | **req**} **networkice-blackice**

client-firewall {**opt** | **req**} **cisco-security-agent**

構文の説明

acl-in *acl*	クライアントが着信トラフィックに使用するポリシーを指定します。
acl-out *acl*	クライアントが発信トラフィックに使用するポリシーを指定します。
AYT	クライアント PC のファイアウォール アプリケーションがファイアウォール ポリシーを制御することを指定します。ASA は、ファイアウォールが実行されていることを確認するためのチェックを行います。「Are You There?」という確認メッセージが表示されます。応答がない場合は、ASA によってトンネルが切断されます。
cisco-integrated	Cisco Integrated ファイアウォール タイプを指定します。
cisco-security-agent	Cisco Intrusion Prevention Security Agent ファイアウォール タイプを指定します。
CPP	VPN クライアント ファイアウォール ポリシーのソースとしてプッシュされるポリシーを指定します。

custom	カスタム ファイアウォール タイプを指定します。
description *string*	ファイアウォールの説明を示します。
networkice-blackice	Network ICE Black ICE ファイアウォール タイプを指定します。
none	クライアント ファイアウォール ポリシーがないことを指定します。ファイアウォール ポリシーをヌル値に設定します。これによりファイアウォール ポリシーが禁止されます。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーからファイアウォール ポリシーを継承しないようにします。
opt	オプションのファイアウォール タイプを指定します。
product-id	ファイアウォール製品を指定します。
req	必要なファイアウォール タイプを指定します。
sygate-personal	Sygate Personal ファイアウォール タイプを指定します。
sygate-personal-pro	Sygate Personal Pro ファイアウォール タイプを指定します。
sygate-security-agent	Sygate Security Agent ファイアウォール タイプを指定します。
vendor-id	ファイアウォールのベンダーを指定します。
zonelabs-integrity	Zone Labs Integrity サーバ ファイアウォール タイプを指定します。
zonelabs-zonealarm	Zone Labs Zone Alarm ファイアウォール タイプを指定します。
zonelabs-zonealarmorpro policy	Zone Labs Zone Alarm または Pro ファイアウォール タイプを指定します。
zonelabs-zonealarmpro policy	Zone Labs Zone Alarm Pro ファイアウォール タイプを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	**zonelabs-integrity** ファイアウォール タイプが追加されました。

使用上のガイドライン

設定できるのは、このコマンドの 1 つのインスタンスのみです。

すべてのファイアウォール ポリシーを削除するには、引数を指定せずに **no client-firewall** コマンドを使用します。このコマンドは、**client-firewall none** コマンドを発行して作成したヌル ポリシーを含め、すべての設定済みファイアウォール ポリシーを削除します。

ファイアウォール ポリシーがなくなると、ユーザはデフォルトまたはその他のグループ ポリシー内に存在するファイアウォール ポリシーを継承します。ユーザがそれらのファイアウォール ポリシーを継承しないようにするには、**client-firewall none** コマンドを使用します。

例

次に、FirstGroup という名前のグループ ポリシーについて、Cisco Intrusion Prevention Security Agent を必要とするクライアント ファイアウォール ポリシーを設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# client-firewall req cisco-security-agent
```

client-types（クリプト CA トラストポイント）

ユーザ接続に関連付けられた証明書の検証にこのトラストポイントを使用できるクライアント接続タイプを指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **client-types** コマンドを使用します。

[no] client-types {ssl | ipsec}

構文の説明

ipsec	トラストポイントと関連付けられている認証局（CA）証明書およびポリシーを IPsec 接続の検証に使用できることを指定します。
ssl	トラストポイントと関連付けられている認証局（CA）証明書およびポリシーを SSL 接続の検証に使用できることを指定します。

コマンド デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

同じ CA 証明書に関連付けられているトラストポイントが複数ある場合、特定のクライアント タイプに設定できるのは 1 つのトラストポイントだけです。ただし、1 つのトラストポイントを 1 つのクライアント タイプに設定し、別のトラストポイントを別のクライアント タイプに設定することができます。

同じ CA 証明書に関連付けられているトラストポイントがあり、これがすでに 1 つのクライアント タイプに設定されている場合は、この同じクライアント タイプ設定に新しいトラストポイントを設定することはできません。このコマンドの no 形式を使用して設定をクリアして、トラストポイントがいずれのクライアント検証にも使用できないようにすることができます。

リモート アクセス VPN では、導入要件に応じて、セキュア ソケット レイヤ（SSL）VPN、IP Security（IPsec）、またはこの両方を使用して、事実上すべてのネットワーク アプリケーションまたはリソースにアクセスを許可できます。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、このトラストポイントを SSL トラストポイントとして指定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(config-ca-trustpoint)# client-types ssl
hostname(config-ca-trustpoint)#
```

次に、トラストポイント checkin 1 のクリプト CA トラストポイント コンフィギュレーション モードを開始して、このトラストポイントを IPsec トラストポイントとして指定する例を示します。

```
hostname(config)# crypto ca trustpoint checkin1
hostname(config-ca-trustpoint)# client-types ipsec
hostname(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
id-usage	トラストポイントの登録された ID の使用方法を指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

client-update

すべてのトンネル グループまたは特定のトンネル グループで、アクティブなすべてのリモート VPN ソフトウェア クライアントとハードウェア クライアント、および Auto Update クライアントとして設定されている ASA 用のクライアント更新を発行するには、特権 EXEC モードで **client-update** コマンドを使用します。

クライアント更新のパラメータをグローバル レベル（VPN ソフトウェア クライアントとハードウェア クライアント、および Auto Update クライアントとして設定されている ASA を含む）で設定および変更するには、グローバル コンフィギュレーション モードで **client-update** コマンドを使用します。

VPN ソフトウェア クライアントとハードウェア クライアント用のクライアント アップデート トンネル グループ IPsec 属性パラメータを設定および変更するには、トンネル グループ ipsec 属性コンフィギュレーション モードで **client-update** コマンドを使用します。

クライアント更新をディセーブルにするには、このコマンドの **no** 形式を使用します。

グローバル コンフィギュレーション モードのコマンドは、次のとおりです。

client-update {**enable** | **component** {**asdm** | **image**} | **device-id** *dev_string* | **family** *family_name* | **type** *type*} **url** *url-string* **rev-nums** *rev-nums*}

no client-update {**enable** | **component** {**asdm** | **image**} | **device-id** *dev_string* | **family** *family_name* | **type** *type*} **url** *url-string* **rev-nums** *rev-nums*}

トンネル グループ ipsec 属性コンフィギュレーション モードのコマンドは、次のとおりです。

client-update type *type* **url** *url-string* **rev-nums** *rev-nums*

no client-update type *type* **url** *url-string* **rev-nums** *rev-nums*

特権 EXEC モードのコマンドは、次のとおりです。

client-update {**all** | *tunnel-group*}

no client-update *tunnel-group*

構文の説明

all	（特権 EXEC モードでのみ使用可能）すべてのトンネル グループのすべてのアクティブ リモート クライアントにアクションを適用します。キーワード **all** をこのコマンドの **no** 形式で使用することはできません。
component {**asdm** | **image**}	Auto Update クライアントとして設定されている ASA のソフトウェア コンポーネント。
device-id *dev_string*	固有のストリングで自身を識別するように Auto Update クライアントが設定されている場合は、クライアントが使用するのと同じストリングを指定します。最大で 63 文字です。
enable	（グローバル コンフィギュレーション モードでのみ使用可能）リモート クライアントのソフトウェア更新をイネーブルにします。
family *family_name*	デバイス ファミリで自身を識別するように Auto Update クライアントが設定されている場合は、クライアントが使用するのと同じデバイス ファミリを指定します。これは、asa、pix、または最大 7 文字のテキスト ストリングです。

rev-nums *rev-nums*	(特権 EXEC モードでは使用不可)このクライアントのソフトウェアまたはファームウェア イメージを指定します。Windows、WIN9X、WinNT、および VPN3002 の各クライアントは、任意の順番で 4 つまで、カンマで区切って指定できます。ASA の場合は、1 つしか指定できません。ストリングの最大長は 127 文字です。
tunnel-group	(特権 EXEC モードでのみ使用可能)リモート クライアント アップデートの有効なトンネル グループの名前を指定します。
type *type*	(特権 EXEC モードでは使用不可)クライアント アップデートを通知するために、リモート PC のオペレーティング システム、または Auto Update クライアントとして設定されている ASA のタイプを指定します。リストは次のとおりです。 • asa5505:Cisco 5505 適応型セキュリティ アプライアンス • asa5510:Cisco 5510 適応型セキュリティ アプライアンス • asa5520:Cisco 5520 適応型セキュリティ アプライアンス • asa5540:Cisco 5540 適応型セキュリティ アプライアンス • linux:Linux クライアント • mac:MAC OS X クライアント • pix-515:Cisco PIX 515 Firewall • pix-515e:Cisco PIX 515E Firewall • pix-525:Cisco PIX 525 Firewall • pix-535:Cisco PIX 535 Firewall • Windows:Windows ベースのすべてのプラットフォーム • WIN9X:Windows 95、Windows 98、および Windows ME プラットフォーム • WinNT:Windows NT 4.0、Windows 2000、および Windows XP プラットフォーム • vpn3002:VPN 3002 ハードウェア クライアント • 最大 15 文字のテキスト ストリング
url *url-string*	(特権 EXEC モードでは使用不可)ソフトウェア/ファームウェア イメージの URL を指定します。この URL は、クライアントに適合するファイルを指している必要があります。ストリングの最大長は 255 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
トンネル グループ ipsec 属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.1(1)	トンネル グループ ipsec 属性コンフィギュレーション モードが追加されました。
7.2(1)	Auto Update サーバとして設定された ASA をサポートするために、**component**、**device-id**、および **family** キーワードとその引数が追加されました。

使用上のガイドライン

トンネル グループ ipsec 属性コンフィギュレーション モードでは、この属性を IPsec リモート アクセス トンネル グループ タイプのみに適用できます。

client-update コマンドを使用すると、更新のイネーブル化、更新の適用先となるクライアントのタイプとリビジョン番号の指定、更新の取得元となる URL または IP アドレスの指定を実行できます。また、Windows クライアントの場合は、VPN クライアント バージョンを更新する必要があることを任意でユーザに通知できます。リビジョン番号のリストにあるソフトウェア バージョンをすでに実行しているクライアントの場合は、ソフトウェアを更新する必要はありません。リストにあるソフトウェア バージョンを実行していないクライアントの場合は、ソフトウェアを更新する必要があります。

Windows クライアントに対しては、更新を実行するメカニズムをユーザに提供できます。VPN 3002 ハードウェア クライアント ユーザの場合、アップデートは通知せずに自動的に行われます。クライアントのタイプが別の ASA である場合は、この ASA が Auto Update サーバとして機能します。

(注) すべての Windows クライアントと Auto Update クライアントで、URL のプレフィックスとして、「http://」または「https://」プロトコルを使用する必要があります。VPN 3002 ハードウェア クライアントの場合、代わりに「tftp://」にプロトコルを指定する必要があります。

また、Windows クライアントと VPN3002 ハードウェア クライアントでは、特定のタイプのすべてのクライアントではなく、個々のトンネル グループだけのクライアント アップデートを設定することもできます。

(注) URL の末尾にアプリケーション名を含めることで（例：https://support/updates/vpnclient.exe）、アプリケーションを自動的に起動するようにブラウザを設定できます。

クライアント アップデートをイネーブルにした後に、特定の IPsec リモート アクセス トンネル グループの一連のクライアント アップデートのパラメータを定義できます。これを行うには、トンネル グループ ipsec 属性モードで、トンネル グループの名前とタイプ、および更新されたイメージの取得元となる URL または IP アドレスを指定します。また、リビジョン番号も指定する必要があります。ユーザのクライアント リビジョン番号が、指定したリビジョン番号のいずれかと一致する場合、そのクライアントを更新する必要はありません。たとえば、すべての Windows クライアント用のクライアント アップデートを発行する必要はありません。

任意で、古い Windows クライアントを使用しているアクティブ ユーザに、VPN クライアントの更新が必要であることを知らせる通知を送信できます。これらのユーザに対しては、ダイアログ ボックスが表示されます。ユーザはこのダイアログ ボックスからブラウザを起動して、URL で指定されているサイトから、更新されたソフトウェアをダウンロードできます。このメッセージで設定可能な部分は URL だけですアクティブでないユーザは、次回のログイン時に通知メッセージを受け取ります。この通知は、すべてのトンネル グループのすべてのアクティブ クライアントに送信するか、または特定のトンネル グループのクライアントに送信できます。

ユーザのクライアント リビジョン番号が、指定したリビジョン番号のいずれかと一致する場合、そのクライアントを更新する必要はありません。また、ユーザは通知メッセージを受信しません。VPN 3002 クライアントはユーザの介入なしで更新され、ユーザは通知メッセージを受信しません。

(注) クライアント アップデートのタイプを **windows**（Windows ベースのすべてのプラットフォーム）に指定し、その後、同じエンティティに **win9x** または **winnt** のクライアント アップデート タイプを入力する必要が生じた場合は、まずこのコマンドの **no** 形式で windows クライアント タイプを削除してから、新しい **client-update** コマンドを使用して新しいクライアント タイプを指定します。

例

次に、グローバル コンフィギュレーション モードで、すべてのトンネル グループのすべてのアクティブ リモート クライアントに対してクライアント更新をイネーブルにする例を示します。

```
ciscoasa(config)# client-update enable
ciscoasa#
```

次の例は、Windows（Win9x、WinNT）だけに適用されます。グローバル コンフィギュレーション モードで、リビジョン番号 4.7、およびアップデートを取得するための URL（https://support/updates）を含む、すべての Windows ベースのクライアントのクライアント アップデート パラメータを設定します。

```
ciscoasa(config)# client-update type windows url https://support/updates/ rev-nums 4.7
ciscoasa(config)#
```

次の例は、VPN 3002 ハードウェア クライアントだけに適用されます。トンネル グループ ipsec 属性コンフィギュレーション モードを開始すると、IPsec リモート アクセス トンネル グループ「salesgrp」用のクライアント アップデート パラメータが設定されます。リビジョン番号 4.7 を指定し、TFTP プロトコルを使用して、更新されたソフトウェアを IP アドレス 192.168.1.1 のサイトから取得します。

```
ciscoasa(config)# tunnel-group salesgrp type ipsec-ra
ciscoasa(config)# tunnel-group salesgrp ipsec-attributes
ciscoasa(config-tunnel-ipsec)# client-update type vpn3002
```

```
url tftp:192.168.1.1 rev-nums 4.7
ciscoasa(config-tunnel-ipsec)#
```

次に、Auto Update クライアントとして設定されている Cisco 5520 ASA であるクライアントのクライアント アップデートを発行する例を示します。

```
ciscoasa(config)# client-update type asa5520 component asdm url
http://192.168.1.114/aus/asdm501.bin rev-nums 7.2(1)
```

次に、特権 EXEC モードで、クライアント ソフトウェアを更新する必要があるトンネル グループ「remotegrp」内の、接続中のすべてのリモート クライアントにクライアント アップデート通知を送信する例を示します。他のグループのクライアントは、アップデート通知を受け取りません。

```
ciscoasa# client-update remotegrp
ciscoasa#
```

次に、特権 EXEC モードで、すべてのトンネル グループのすべてのアクティブ クライアントに通知する例を示します。

```
ciscoasa# client-update all
ciscoasa#
```

関連コマンド

コマンド	説明
clear configure client-update	クライアントアップデート コンフィギュレーション全体をクリアします。
show running-config client-update	現在のクライアント アップデート コンフィギュレーションを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ ipsec 属性を設定します。

clock set

ASA のクロックを手動で設定するには、特権 EXEC モードで **clock set** コマンドを使用します。

clock set *hh*:*mm*:*ss* {*month day* | *day month*} *year*

構文の説明

day	1 ～ 31 の日付を設定します。標準の日付形式に応じて、月日を **april 1** または **1 april** のように入力できます。
hh:*mm*:*ss*	時、分、秒を 24 時間形式で設定します。たとえば、午後 8 時 54 分は **20:54:00** のように設定します。
month	月を設定します。標準の日付形式に応じて、月日を **april 1** または **1 april** のように入力できます。
year	たとえば、**2004** など、4 桁で年を設定します。年の範囲は 1993 ～ 2035 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

clock コンフィギュレーション コマンドを入力していない場合、**clock set** コマンドのデフォルトの時間帯は UTC です。**clock timezone** コマンドを使用して **clock set** コマンドを入力した後に時間帯を変更した場合、時間は自動的に新しい時間帯に調整されます。ただし、**clock timezone** コマンドを使用して時間帯を設定した後に **clock set** コマンドを入力した場合は、UTC ではなく、新しい時間帯に応じた時間を入力します。同様に、**clock set** コマンドの後に **clock summer-time** コマンドを入力した場合、時間は夏時間に調整されます。**clock summer-time** コマンドの後に **clock set** コマンドを入力した場合は、夏時間の正しい時間を入力します。

このコマンドはハードウェア チップ内の時間を設定しますが、コンフィギュレーション ファイル内の時間は保存しません。この時間はリブート後も保持されます。他の **clock** コマンドとは異なり、このコマンドは特権 EXEC コマンドです。クロックをリセットするには、**clock set** コマンドの新しい時刻を設定する必要があります。

例

次に、時間帯を MST に設定し、夏時間を米国のデフォルト期間に設定し、MDT の現在の時間を 2004 年 7 月 27 日の午後 1 時 15 分に設定する例を示します。

```
ciscoasa(config)# clock timezone MST -7
ciscoasa(config)# clock summer-time MDT recurring
ciscoasa(config)# exit
ciscoasa# clock set 13:15:0 jul 27 2004
ciscoasa# show clock
13:15:00.652 MDT Tue Jul 27 2004
```

次に、クロックを UTC 時間帯で 2004 年 7 月 27 日の 8 時 15 分に設定し、その後時間帯を MST に設定し、夏時間を米国のデフォルト期間に設定する例を示します。終了時刻（MDT の 1 時 15 分）は前の例と同じです。

```
ciscoasa# clock set 20:15:0 jul 27 2004
ciscoasa# configure terminal
ciscoasa(config)# clock timezone MST -7
ciscoasa(config)# clock summer-time MDT recurring
ciscoasa# show clock
13:15:00.652 MDT Tue Jul 27 2004
```

関連コマンド

コマンド	説明
clock summer-time	夏時間を表示する日付の範囲を設定します。
clock timezone	時間帯を設定します。
show clock	現在時刻を表示します。

clock summer-time

ASA の時間の表示に夏時間の日付範囲を設定するには、グローバル コンフィギュレーション モードで **clock summer-time** コマンドを使用します。夏時間の日付をディセーブルにするには、このコマンドの **no** 形式を使用します。

clock summer-time *zone* **recurring** [*week weekday month hh*:*mm week weekday month hh*:*mm*] [*offset*]

no clock summer-time [*zone* **recurring** [*week weekday month hh*:*mm week weekday month hh*:*mm*] [*offset*]]

clock summer-time *zone* **date** {*day month* | *month day*} *year hh*:*mm* {*day month* | *month day*} *year hh*:*mm* [*offset*]

no clock summer-time [*zone* **date** {*day month* | *month day*} *year hh*:*mm* {*day month* | *month day*} *year hh*:*mm* [*offset*]]

(注) このコマンドは、アプライアンスモードの Firepower 1000 または Firepower 2100 ではサポートされていません。

構文の説明

date	夏時間の開始日と終了日を、特定の年の特定の日付として指定します。このキーワードを使用する場合は、日付を毎年リセットする必要があります。
day	1 ～ 31 の日付を設定します。標準の日付形式に応じて、月日を **April 1** または **1 April** のように入力できます。
hh:mm	時間と分を 24 時間形式で設定します。
month	月をストリングで設定します。**date** コマンドでは、たとえば、標準の日付形式に応じて、月日を **April 1** または **1 April** のように入力できます。
offset	(任意)夏時間の時間を変更する分数を設定します。デフォルト値は 60 分です。
recurring	夏時間の開始日と終了日を、年の特定の日付ではなく、月の日時の形式で指定します。このキーワードを使用すると、定期的な日付範囲を設定できるため、毎年変更する必要がありません。日付を指定しない場合、ASA は、米国のデフォルトの日付範囲(3 月の第 2 日曜日の午前 2 時～ 11 月の第 1 日曜日の午前 2 時)を使用します。
week	(任意)週を 1 ～ 4 の整数で指定するか、**first** や **last** の語で指定します。たとえば、日付が 5 週目に当たる場合は、**last** を指定します。
weekday	(任意)**Monday**、**Tuesday**、**Wednesday** などの曜日を指定します。
year	たとえば、**2004** など、4 桁で年を設定します。年の範囲は 1993 ～ 2035 です。
zone	太平洋夏時間の時間帯をストリング(**PDT** など)で指定します。このコマンドで設定した日付範囲に従って ASA が夏時間を表示する場合、時間帯はここで設定した値に変更されます。基本の時間帯を UTC 以外の時間帯に設定するには、**clock timezone** コマンドを参照してください。

デフォルト

デフォルトのオフセットは 60 分です

デフォルトの定期的な日付範囲は、3 月の第 2 日曜日の午前 2 時 ～ 11 月の第 1 日曜日の午前 2 時です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.0(2)	デフォルトの定期的な日付範囲が、3 月の第 2 日曜日の午前 2 時 ～ 11 月の第 1 日曜日の午前 2 時に変更されました。

使用上のガイドライン

南半球の場合、ASA は、開始月が終了月よりも後に来る（10 月 ～ 3 月など）ことを受け入れます。

例

次に、オーストラリアの夏時間の日付範囲を設定する例を示します。

```
ciscoasa(config)# clock summer-time PDT recurring last Sunday October 2:00 last Sunday
March 2:00
```

国によっては、夏時間が特定の日付に開始されます。次に、夏時間を 2008 年 4 月 1 日午前 3 時に開始し、2008 年 10 月 1 日午前 4 時に終了するように設定する例を示します。

```
ciscoasa(config)# clock summer-time UTC date 1 April 2008 3:00 1 October 2008 4:00
```

関連コマンド

コマンド	説明
clock set	ASA のクロックを手動で設定します。
clock timezone	時間帯を設定します。
ntp server	NTP サーバを指定します。
show clock	現在時刻を表示します。

clock timezone

ASA のクロックの時間帯を設定するには、グローバル コンフィギュレーション モードで **clock timezone** コマンドを使用します。時間帯をデフォルトの UTC に戻すには、このコマンドの **no** 形式を使用します。

アプライアンスモードの Firepower 1000 および 2100 の場合:

clock timezone *zone*

no clock timezone [*zone*]

他のすべてのモデルの場合:

clock timezone *zone* [**-**]*hours* [*minutes*]

no clock timezone [*zone* [**-**]*hours* [*minutes*]]

構文の説明

[**-**]*hours*	UTC からのオフセットの時間数を設定します。たとえば、PST は -8 時間です。
minutes	(任意)UTC からのオフセットの分数を設定します。
zone	太平洋標準時間の時間帯を文字列(PST など)で指定します。アプライアンスモードの Firepower 1000 および 2100 では、**clock timezone ?** コマンドを入力し、使用可能なタイムゾーン名のリストを表示します。

デフォルト

デフォルトの時間帯は UTC です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.13(1)	このコマンドは、アプライアンスモードの Firepower 1000 および 2100 に対して更新されました。

使用上のガイドライン

夏時間を設定するには、**clock summer-time** コマンド（Firepower 1000 または 2100 ではサポート対象外）を参照してください。

clock set コマンド、または NTP サーバから生成された時間は、時間を UTC で設定します。このコマンドを使用して、時間帯を UTC のオフセットとして設定する必要があります。

例

アプライアンスモードの Firepower 1000 および 2100 の場合、タイムゾーンを山地標準時に設定する例を次に示します。

```
ciscoasa(config)# clock timezone ?
Available timezones:
CET
CST6CDT
Cuba
EET
Egypt
Eire
EST
EST5EDT
Factory
GB
GB-Eire
GMT
GMT0
GMT-0
GMT+0
Greenwich
Hongkong
HST
Iceland
Iran
Israel
Jamaica
Japan
[...]
ciscoasa(config)# clock timezone US/?

configure mode commands/options:
  US/Alaska          US/Aleutian    US/Arizona    US/Central
  US/East-Indiana    US/Eastern     US/Hawaii     US/Indiana-Starke
  US/Michigan        US/Mountain    US/Pacific
ciscoasa(config)# clock timezone US/Mountain
```

次に、時間帯を太平洋標準時間（UTC から -8 時間）に設定する例を示します。

```
ciscoasa(config)# clock timezone PST -8
```

関連コマンド

コマンド	説明
clock set	ASA のクロックを手動で設定します。
clock summer-time	夏時間を表示する日付の範囲を設定します。
ntp server	NTP サーバを指定します。
show clock	現在時刻を表示します。

cluster-ctl-file（廃止）

フラッシュ メモリに格納されている既存の CTL ファイルから、すでに作成されているトラストポイントを使用するには、CTL ファイル コンフィギュレーション モードで **cluster-ctl-file** コマンドを使用します。CTL ファイルのコンフィギュレーションを削除して、新しい CTL ファイルを作成できるようにするには、このコマンドの **no** 形式を使用します。

cluster-ctl-file *filename_path*

no cluster-ctl-file *filename_path*

構文の説明

filename_path	ディスクまたはフラッシュ メモリに格納されている CTL ファイルのパスおよびファイル名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ctl ファイル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(4)	コマンドが追加されました。
9.4(1)	このコマンドは、すべての **phone-proxy** モード コマンドとともに廃止されました。

使用上のガイドライン

このコマンドが設定されている場合、電話プロキシは、フラッシュ メモリに格納されている CTL ファイルを解析し、その CTL ファイルからのトラストポイントをインストールし、フラッシュのそのファイルを使用して新しい CTL ファイルを作成します。

例

次に、フラッシュ メモリに格納されている CTL ファイルからトラストポイントをインストールするために、CTL ファイルを解析する例を示します。

```
ciscoasa(config-ctl-file)# cluster-ctl-file disk0:/old_ctlfile.tlv
```

関連コマンド

コマンド	説明
ctl-file（グローバル）	電話プロキシ コンフィギュレーション用に作成する CTL ファイル、またはフラッシュ メモリから解析するための CTL ファイルを指定します。
ctl-file（Phone-Proxy）	Phone Proxy コンフィギュレーションで使用する CTL ファイルを指定します。
phone-proxy	Phone Proxy インスタンスを設定します。

cluster encryption

仮想ロード バランシング クラスタ上で交換されるメッセージの暗号化をイネーブルにするには、VPN ロード バランシング コンフィギュレーション モードで **cluster encryption** コマンドを使用します。暗号化をディセーブルにするには、このコマンドの **no** 形式を使用します。

cluster encryption

no cluster encryption

(注) VPN ロード バランシングには、アクティブな 3DES または AES ライセンスが必要です。ASA は、ロード バランシングをイネーブルにする前に、この暗号化ライセンスの存在をチェックします。アクティブな 3DES または AES ライセンスを検出できない場合、ASA は、ロード バランシングのイネーブル化を回避し、さらにライセンスがこの使用を許可していない限り、ロード バランシング システムによる 3DES の内部コンフィギュレーションを回避します。

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

暗号化は、デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
VPN ロード バランシング コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、仮想ロード バランシング クラスタ上で交換されるメッセージの暗号化のオンとオフを切り替えます。

cluster encryption コマンドを設定する前に、まず **vpn load-balancing** コマンドを使用して VPN ロード バランシング コンフィギュレーション モードを開始する必要があります。また、クラスタの暗号化をイネーブルにする前に、**cluster key** コマンドを使用してクラスタ共有秘密キーを設定する必要があります。

(注) 暗号化を使用する場合は、最初にコマンド **isakmp enable** *inside* を設定する必要があります。ここで、*inside* は、ロード バランシングの内部インターフェイスを示します。ISAKMP がロード バランシング内部インターフェイスでイネーブルになっていない場合、クラスタの暗号化を設定しようとするとエラー メッセージが表示されます。

例

次に、仮想ロード バランシング クラスタの暗号化をイネーブルにする **cluster encryption** コマンドを含む VPN ロード バランシング コマンド シーケンスの例を示します。

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# cluster key 123456789
ciscoasa(config-load-balancing)# cluster encryption
ciscoasa(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
cluster key	クラスタの共有秘密キーを指定します。
vpn load-balancing	VPN ロード バランシング コンフィギュレーション モードを開始します。

cluster exec

クラスタ内のすべてのユニット、または特定のメンバーに対してコマンドを実行するには、特権 EXEC モードで **cluster exec** コマンドを使用します。

cluster exec [**unit** *unit_name*] *command*

構文の説明

unit *unit_name*	（オプション）特定のユニットに対してコマンドを実行します。メンバー名を一覧表示するには、**cluster exec unit ?**（現在のユニットを除くすべての名前が表示される）と入力するか、**show cluster info** コマンドを入力します。
command	実行するコマンドを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

show コマンドをすべてのメンバに送信すると、すべての出力が収集されて現在のユニットのコンソールに表示されます。その他のコマンド、たとえば **capture** や **copy** も、クラスタ全体での実行を活用できます。

例

同じキャプチャ ファイルをクラスタ内のすべてのユニットから同時に TFTP サーバにコピーするには、マスター ユニットで次のコマンドを入力します。

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

複数の PCAP ファイル（各ユニットから 1 つずつ）が TFTP サーバにコピーされます。宛先のキャプチャ ファイル名には自動的にユニット名が付加され、capture1_asa1.pcap、capture1_asa2.pcap などとなります。この例では、asa1 および asa2 がクラスタ ユニット名です。

次の例では、**cluster exec show port-channel summary** コマンドの出力に、クラスタの各メンバーの EtherChannel 情報が表示されています。

```
ciscoasa# cluster exec show port-channel summary
primary(LOCAL):*************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster  Ports
------+-------------+-----------+-----------------------------------------------
1         Po1              LACP      Yes  Gi0/0(P)
2         Po2              LACP      Yes  Gi0/1(P)
 secondary:*********************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster   Ports
------+-------------+-----------+-----------------------------------------------
1         Po1              LACP      Yes   Gi0/0(P)
2         Po2              LACP      Yes   Gi0/1(P)
```

関連コマンド

コマンド	説明
cluster group	クラスタ グループ コンフィギュレーション モードを開始します。
show cluster info	クラスタ情報を表示します。

cluster flow-mobility lisp

トラフィック クラスのフロー モビリティをイネーブルにするには、クラス コンフィギュレーション モードで **cluster flow-mobility lisp** コマンドを使用します。クラス コンフィギュレーション モードにアクセスするには、**policy-map** コマンドを入力します。フロー モビリティをディセーブルにするには、このコマンドの **no** 形式を使用します。

cluster flow-mobility lisp

no cluster flow-mobility lisp

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

フロー モビリティは、ビジネス クリティカルなトラフィックに対してイネーブルにする必要があります。たとえば、フロー モビリティを HTTPS トラフィックのみ、または特定のサーバへのトラフィックのみに制限できます。

クラスタ フロー モビリティの LISP インスペクションについて

ASA は、場所の変更について LISP トラフィックを検査し、シームレスなクラスタリング操作のためにこの情報を使用します。LISP の統合により、ASA クラスタ メンバーは、最初のホップ ルータと ETR または ITR との間で渡される LISP トラフィックを検査し、その後、フローの所有者を新しいサイトへ変更できます。

クラスタ フロー モビリティには複数の相互に関連する設定が含まれています。

1. (オプション)ホストまたはサーバの IP アドレスに基づく検査される EID の限定:最初のホップ ルータは、ASA クラスタが関与していないホストまたはネットワークに関する EID 通知メッセージを送信することがあるため、EID をクラスタに関連するサーバまたはネットワークのみに限定することができます。たとえば、クラスタが 2 つのサイトのみに関連しているが、LISP は 3 つのサイトで稼働している場合は、クラスタに関連する 2 つのサイトの EID のみを含めます。**policy-map type inspect lisp**、**allowed-eid** および **validate-key** コマンドを参照してください。
2. LISP トラフィックのインスペクション:ASA は、最初のホップ ルータと ITR または ETR 間で送信された EID 通知メッセージに関して LISP トラフィックを検査します。ASA は EID とサイト ID を相関付ける EID テーブルを維持します。たとえば、最初のホップ ルータの送信元 IP アドレスと ITR または ETR の宛先アドレスをもつ LISP トラフィックを検査する必要があります。**inspect lisp** コマンドを参照してください。
3. 指定されたトラフィックでのフロー モビリティを有効にするサービス ポリシー:ビジネスクリティカルなトラフィックでフロー モビリティを有効にする必要があります。たとえば、フロー モビリティを、HTTPS トラフィックのみに制限したり、特定のサーバとの間でやり取りされるトラフィックのみに制限したりできます。**cluster flow-mobility lisp** コマンドを参照してください。
4. サイト ID:ASA は各クラスタ ユニットのサイト ID を使用して、新しい所有者を判別します。**site-id** コマンドを参照してください。
5. フロー モビリティを有効にするクラスタレベルの設定:クラスタ レベルでもフロー モビリティを有効にする必要があります。このオン/オフの切り替えを使用することで、特定のクラスのトラフィックまたはアプリケーションに対してフロー モビリティを簡単に有効または無効にできます。**flow-mobility lisp** コマンドを参照してください。

例

次に、HTTPS を使用して 10.10.10.0/24 のサーバに送信されるすべての内部トラフィックに対してフロー モビリティをイネーブルにする例を示します。

```
ciscoasa(config)# access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0
255.255.255.0 eq https
ciscoasa(config)# class-map IMPORTANT-FLOWS-MAP
ciscoasa(config)# match access-list IMPORTANT-FLOWS
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class IMPORTANT-FLOWS-MAP
ciscoasa(config-pmap-c)# cluster flow-mobility lisp
```

関連コマンド

コマンド	説明
allowed-eids	IP アドレスに基づいて検査される EID を限定します。
clear cluster info flow-mobility counters	フロー モビリティ カウンタをクリアします。
clear lisp eid	ASA EID テーブルから EID を削除します。
flow-mobility lisp	クラスタのフロー モビリティを有効にします。
inspect lisp	LISP トラフィックを検査します。
policy-map type inspect lisp	LISP 検査をカスタマイズします。
site-id	クラスタ シャーシのサイト ID を設定します。

コマンド	説明
show asp table classify domain inspect-lisp	LISP 検査用の ASP テーブルを表示します。
show cluster info flow-mobility counters	フロー モビリティ カウンタを表示します。
show conn	LISP フロー モビリティの対象となるトラフィックを表示します。
show lisp eid	ASA EID テーブルを表示します。
show service-policy	サービス ポリシーを表示します。
validate-key	LISP メッセージを検証するための事前共有キーを入力します。

cluster group

クラスタ ブートストラップのパラメータやその他のクラスタ設定を設定するには、グローバル コンフィギュレーション モードで **cluster group** を使用します。クラスタ設定をクリアするには、このコマンドの **no** 形式を使用します。

cluster group *name*

no cluster group *name*

構文の説明

name	1 ～ 38 文字の ASCII 文字列としてクラスタ名を指定します。クラスタ グループはユニットあたり 1 つしか設定できません。クラスタのすべてのメンバが同じ名前を使用する必要があります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

クラスタ内の各ユニットがクラスタに参加するには、ブートストラップ コンフィギュレーションが必要です。一般的には、クラスタに参加するように最初に設定したユニットがマスター ユニットとなります。クラスタリングをイネーブルにした後で、選定期間が経過すると、クラスタのマスター ユニットが選定されます。最初はクラスタ内のユニットが 1 つだけであるため、そのユニットがマスター ユニットになります。それ以降クラスタに追加されるユニットは、スレーブ ユニットとなります。

クラスタリングを設定する前に、**cluster interface-mode** コマンドを使用してクラスタ インターフェイス モードを設定する必要があります。

クラスタリングをイネーブルまたはディセーブルにするには、コンソール ポートまたは ASDM を使用する必要があります。Telnet または SSH を使用することはできません。

例

次の例では、管理インターフェイスを設定し、クラスタ制御リンク用のデバイス ローカル EtherChannel を設定し、ヘルス チェックをディセーブルにし（一時的に）、その後で、「unit1」という名前の ASA のクラスタリングをイネーブルにします。これは最初にクラスタに追加されるユニットであるため、マスター ユニットになります。

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/32 8

interface management 0/0
    nameif management
    ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
    ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
    security-level 100
    management-only
    no shutdown

interface tengigabitethernet 0/6
    channel-group 1 mode active
    no shutdown

interface tengigabitethernet 0/7
    channel-group 1 mode active
    no shutdown

cluster group pod1
    local-unit unit1
    cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
    priority 1
    key chuntheunavoidable
    no health-check
    enable noconfirm
```

次の例には、スレーブ ユニット unit2 のコンフィギュレーションが含まれています。

```
interface tengigabitethernet 0/6
    channel-group 1 mode active
    no shutdown

interface tengigabitethernet 0/7
    channel-group 1 mode active
    no shutdown

cluster group pod1
    local-unit unit2
    cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
    priority 2
    key chuntheunavoidable
    no health-check
    enable as-slave
```

関連コマンド

コマンド	説明
clacp system-mac	スパンド EtherChannel を使用するときは、ASA は cLACP を使用してネイバー スイッチとの間で EtherChannel のネゴシエーションを行います。
cluster-interface	クラスタ制御リンク インターフェイスを指定します。
cluster interface-mode	クラスタ インターフェイス モードを設定します。
conn-rebalance	接続の再分散をイネーブルにします。

コマンド	説明
console-replicate	スレーブ ユニットからマスター ユニットへのコンソール複製をイネーブルにします。
enable(クラスタ グループ)	クラスタリングをイネーブルにします。
health-check	クラスタのヘルス チェック機能(ユニットのヘルス モニタリングおよびインターフェイスのヘルス モニタリングを含む)をイネーブルにします。
health-check auto-rejoin	ヘルス チェック失敗後の自動再結合クラスタ設定をカスタマイズします。
key	クラスタ制御リンクの制御トラフィックの認証キーを設定します。
local-unit	クラスタ メンバーに名前を付けます。
mtu cluster-interface	クラスタ制御リンク インターフェイスの最大伝送ユニットを指定します。
priority(クラスタ グループ)	マスター ユニット選定のこのユニットのプライオリティを設定します。
site-id	サイト間クラスタリングでの MAC アドレスのフラッピングを回避するようにサイト ID を設定します。

cluster-interface

クラスタ制御リンクの物理インターフェイスおよび IP アドレスを指定するには、クラスタ グループ コンフィギュレーション モードで **cluster-interface** コマンドを使用します。クラスタ インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

cluster-interface *interface_id* **ip** *ip_address mask*

no cluster-interface [*interface_id* **ip** *ip_address mask*]

構文の説明

interface_id	EtherChannel という物理インターフェイス、または冗長インターフェイスを指定します。サブインターフェイスと管理インターフェイスは許可されません。このインターフェイスには、**nameif** を設定することはできません。IPS モジュール搭載 ASA 5585-X では、IPS モジュール インターフェイスをクラスタ制御リンクに使用することはできません。
ip *ip_address mask*	IP アドレスには IPv4 アドレスを指定します。IPv6 は、このインターフェイスではサポートされません。ユニットごとに、同じネットワークにある別の IP アドレスを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラスタ グループ コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

クラスタに参加する前に、クラスタ制御リンク インターフェイスをイネーブルにする必要があります。

十分な数のインターフェイスがある場合は、複数のクラスタ制御リンク インターフェイスを結合して 1 つの EtherChannel とすることを推奨します。この EtherChannel は ASA に対してローカルであり、スパンド EtherChannel ではありません。クラスタ制御リンクには、10 ギガビット イーサネット インターフェイスを使用することを推奨します。クラスタ制御リンクでの不要なトラフィックを削減できるように、EtherChannel メンバー インターフェイスに対しては On モードを使用することを推奨します。クラスタ制御リンクは LACP トラフィックのオーバーヘッドを必要としません。これは隔離された、安定したネットワークであるからです。

クラスタ制御リンク インターフェイス コンフィギュレーションは、マスター ユニットからスレーブ ユニットには複製されませんが、同じコンフィギュレーションを各ユニットで使用する必要があります。このコンフィギュレーションは複製されないため、クラスタ制御リンク インターフェイスの設定は各ユニットで個別に行う必要があります。

クラスタ制御リンクの詳細については、設定ガイドを参照してください。

例

次に、Port-channel 2 という EtherChannel を、TenGigabitEthernet 0/6 および TenGigabitEthernet 0/7 のために作成し、このポート チャネルをクラスタ制御リンクとして割り当てる例を示します。ポートチャネル インターフェイスは、チャネル グループにインターフェイスを割り当てたときに自動的に作成されます。

```
interface tengigabitethernet 0/6
    channel-group 2 mode on
    no shutdown

interface tengigabitethernet 0/7
    channel-group 2 mode on
    no shutdown

cluster group cluster1
    cluster-interface port-channel2 ip 10.1.1.1 255.255.255.0
```

関連コマンド

コマンド	説明
clacp system-mac	スパンド EtherChannel を使用するときは、ASA は cLACP を使用してネイバー スイッチとの間で EtherChannel のネゴシエーションを行います。
cluster group	クラスタに名前を付け、クラスタ コンフィギュレーション モードを開始します。
cluster interface-mode	クラスタ インターフェイス モードを設定します。
conn-rebalance	接続の再分散をイネーブルにします。
console-replicate	スレーブ ユニットからマスター ユニットへのコンソール複製をイネーブルにします。
enable(クラスタ グループ)	クラスタリングをイネーブルにします。
health-check	クラスタのヘルス チェック機能(ユニットのヘルス モニタリングおよびインターフェイスのヘルス モニタリングを含む)をイネーブルにします。
key	クラスタ制御リンクの制御トラフィックの認証キーを設定します。
local-unit	クラスタ メンバーに名前を付けます。
mtu cluster-interface	クラスタ制御リンク インターフェイスの最大伝送ユニットを指定します。
priority(クラスタ グループ)	マスター ユニット選定のこのユニットのプライオリティを設定します。

cluster interface-mode

各クラスタ ユニットでクラスタ インターフェイス モードを指定するには、グローバル コンフィギュレーション モードで **cluster interface-mode** コマンドを使用します。クラスタ インターフェイス モードを無効にするには、このコマンドの **no** 形式を入力します。

cluster interface-mode {**individual** | **spanned**} [**check-details** | **force**]

no cluster-interface [*interface_id* **ip** *ip_address mask*]

構文の説明

individual	モードを個別インターフェイス モードに設定します(ルーテッド モード。ASA ハードウェア モデルのみ)。
spanned	モードをスパンド EtherChannel モードに設定します。
check-details	互換性のない設定を表示し、強制的にインターフェイス モードにして後で設定を修正できるようにします。このコマンドではモードは変更されません。
force	互換性のない設定の検査は行わずにモードを変更します。コンフィギュレーションの問題がある場合は、モードを変更した後に手動で解決する必要があります。インターフェイス コンフィギュレーションの修正ができるのはモードの設定後に限られるので、**force** オプションを使用することを推奨します。このようにすれば、最低でも、既存のコンフィギュレーションの状態から開始できます。さらにガイダンスが必要な場合は、モードを設定した後で **check-details** オプションを再実行します。 **force** オプションを指定しないと、互換性のないコンフィギュレーションがある場合は、コンフィギュレーションをクリアしてリロードするように求められるので、コンソール ポートに接続して管理アクセスを再設定する必要があります。コンフィギュレーションに互換性の問題がない場合は(まれなケース)、モードが変更され、コンフィギュレーションは維持されます。コンフィギュレーションをクリアしたくない場合は、**n** を入力してコマンドを終了します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

クラスタリング用に設定できるインターフェイスのタイプは、スパンド EtherChannel と個別インターフェイスのいずれか一方のみです。1 つのクラスタ内でインターフェイス タイプを混在させることはできません。モードを設定していない場合は、クラスタリングをイネーブルにできません。モードを設定した後、クラスタリングを有効にしていない場合でも、インターフェイスはクラスタリング インターフェイスの要件に準拠する必要があります。

次のガイドラインを参照してください。

- モードの設定は、クラスタに追加する各 ASA で個別に行う必要があります。
- 管理専用インターフェイスはいつでも、個別インターフェイス(推奨)として設定できます(スパンド EtherChannel モードのときでも)。管理インターフェイスは、個別インターフェイスとすることができます(トランスペアレント ファイアウォール モードのときでも)。
- スパンド EtherChannel モードでは、管理インターフェイスを個別インターフェイスとして設定すると、管理インターフェイスに対してダイナミック ルーティングをイネーブルにできません。スタティック ルートを使用する必要があります。
- マルチ コンテキスト モードでは、すべてのコンテキストに対して 1 つのインターフェイス タイプを選択する必要があります。たとえば、トランスペアレント モードとルーテッド モードのコンテキストが混在している場合は、すべてのコンテキストにスパンド EtherChannel モードを使用する必要があります。これが、トランスペアレント モードで許可される唯一のインターフェイス タイプであるからです。

例

次に、スパンド EtherChannel モードの現在のインターフェイスの互換性をチェックする例を示します。

```
ciscoasa(config)# cluster interface-mode spanned check-details
ERROR: Please modify the following configuration elements that are incompatible with
'spanned' interface-mode.
 - Interface vni1 is not a span-cluster port-channel interface, vni1(vni1) cannot be used
as data interface when cluster interface-mode is 'spanned'.
 - Interface Gi0/0 is not a span-cluster port-channel interface, Gi0/0(inside) cannot be
used as data interface when cluster interface-mode is 'spanned'.
 - Interface Gi0/1 is not a span-cluster port-channel interface, Gi0/1(test) cannot be
used as data interface when cluster interface-mode is 'spanned'.
 - Interface Gi0/1 is not a span-cluster port-channel interface, Gi0/1.1(vlan100) cannot
be used as data interface when cluster interface-mode is 'spanned'.
 - Interface Gi0/2 is not a span-cluster port-channel interface, Gi0/2(outside) cannot be
used as data interface when cluster interface-mode is 'spanned'.
 - Interface Gi0/5 is not a span-cluster port-channel interface, Gi0/5(bgmember1) cannot
be used as data interface when cluster interface-mode is 'spanned'.
 - Interface Gi0/5 is not a span-cluster port-channel interface, Gi0/5.2(vlan200) cannot
be used as data interface when cluster interface-mode is 'spanned'.
 - Interface BV1 is not a span-cluster port-channel interface, BV1(bvi1) cannot be used as
data interface when cluster interface-mode is 'spanned'.

ciscoasa(config)#
```

次に、モードをスパンド EtherChannel モードに設定し、互換性のない設定をクリアしない例を示します。

```
ciscoasa(config)# cluster interface-mode spanned force
```

関連コマンド

コマンド	説明
clacp system-mac	スパンド EtherChannel を使用するときは、ASA は cLACP を使用してネイバー スイッチとの間で EtherChannel のネゴシエーションを行います。
cluster group	クラスタに名前を付け、クラスタ コンフィギュレーション モードを開始します。
cluster-interface	クラスタ制御リンク インターフェイスを指定します。
conn-rebalance	接続の再分散をイネーブルにします。
console-replicate	スレーブ ユニットからマスター ユニットへのコンソール複製をイネーブルにします。
enable(クラスタ グループ)	クラスタリングをイネーブルにします。
health-check	クラスタのヘルス チェック機能(ユニットのヘルス モニタリングおよびインターフェイスのヘルス モニタリングを含む)をイネーブルにします。
key	クラスタ制御リンクの制御トラフィックの認証キーを設定します。
local-unit	クラスタ メンバーに名前を付けます。
mtu cluster-interface	クラスタ制御リンク インターフェイスの最大伝送ユニットを指定します。
priority(クラスタ グループ)	マスター ユニット選定のこのユニットのプライオリティを設定します。

cluster ip address

仮想ロード バランシング クラスタの IP アドレスを設定するには、VPN ロード バランシング コンフィギュレーション モードで **cluster ip address** コマンドを使用します。IP アドレスの指定を削除するには、このコマンドの **no** 形式を使用します。

cluster ip address *ip-address*

no cluster ip address [*ip-address*]

構文の説明

ip-address	仮想ロード バランシング クラスタに割り当てる IP アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
VPN ロード バランシング コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

最初に、**vpn load-balancing** コマンドを使用して VPN ロード バランシング コンフィギュレーション モードを開始し、仮想クラスタ IP アドレスが指すインターフェイスを設定する必要があります。

このクラスタ IP アドレスは、仮想クラスタを設定するインターフェイスと同じサブネット上にある必要があります。

このコマンドの **no** 形式では、任意の *ip-address* 値を指定した場合、**no cluster ip address** コマンドを実行するには、その値が既存のクラスタの IP アドレスと一致する必要があります。

例

次に、仮想ロード バランシング クラスタの IP アドレスを 209.165.202.224 に設定する **cluster ip address** コマンドを含む VPN ロード バランシング コマンド シーケンスの例を示します。

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
```

```
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
interface	デバイスのインターフェイスを設定します。
nameif	インターフェイスに名前を割り当てます。
vpn load-balancing	VPN ロード バランシング コンフィギュレーション モードを開始します。

cluster key

仮想ロード バランシング クラスタ上で交換される IPsec サイト間トンネルの共有秘密を設定するには、VPN ロード バランシング コンフィギュレーション モードで **cluster key** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

cluster key *shared-secret*

no cluster key [*shared-secret*]

構文の説明

shared-secret	VPN ロード バランシング クラスタの共有秘密を定義する 3 ～ 17 文字の文字列。ストリングに特殊文字を含めることはできますが、スペースを含めることはできません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
VPN ロード バランシング コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

まず、**vpn load-balancing** コマンドを使用して、VPN ロード バランシング コンフィギュレーション モードを開始する必要があります。クラスタの暗号化には、**cluster key** コマンドで定義された共有秘密も使用されます。

共有秘密を設定するには、クラスタの暗号化をイネーブルにする前に **cluster key** コマンドを使用する必要があります。

このコマンドの **no cluster key** 形式で *shared-secret* の値を指定した場合、共有秘密の値は既存のコンフィギュレーションと一致する必要があります。

例

次に、仮想ロード バランシング クラスタの共有秘密を 123456789 に設定する **cluster key** コマンドを含む VPN ロード バランシング コマンド シーケンスの例を示します。

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# cluster key 123456789
ciscoasa(config-load-balancing)# cluster encryption
ciscoasa(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロード バランシング コンフィギュレーション モードを開始します。

cluster master unit

新しいユニットを ASA クラスタのマスター ユニットとして設定するには、特権 EXEC モードで **cluster master unit** コマンドを使用します。

cluster master unit *unit_name*

注意 マスター ユニットを変更する最適な方法は、マスター ユニットでクラスタリングを無効にし（**no enable**（クラスタ グループ）コマンドを参照）、新しいマスター の選定を待機してから、クラスタリングを再び無効にすることです。マスターにする特定のユニットを指定する必要がある場合は、**cluster master unit** コマンドを使用します。ただし、中央集中型機能については、このコマンドを使用してマスター ユニット変更を強制すると、すべての接続がドロップされるので、新しいマスター ユニット上で接続を再確立する必要があります。

構文の説明

unit_name	新しいマスター ユニットとなるローカル ユニット名を指定します。メンバ名を一覧表示するには、**cluster master unit ?**（現在のユニットを除くすべての名前が表示される）と入力するか、**show cluster info** コマンドを入力します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

メイン クラスタ IP アドレスへの再接続が必要になります。

例

次に、新しいマスター ユニットとして asa2 を設定する例を示します。

```
ciscoasa# cluster master unit asa2
```

関連コマンド

コマンド	説明
cluster exec	すべてのクラスタ メンバーにコマンドを送信します。
cluster group	クラスタを設定します。
cluster remove unit	ユニットをクラスタから削除します。

cluster-mode（廃止）

クラスタのセキュリティ モードを指定するには、電話プロキシ コンフィギュレーション モードで **cluster-mode** コマンドを使用します。クラスタのセキュリティ モードをデフォルト モードに設定するには、このコマンドの **no** 形式を使用します。

cluster-mode [**mixed** | **nonsecure**]

no cluster-mode [**mixed** | **nonsecure**]

構文の説明

mixed	電話プロキシ機能の設定時に、クラスタ モードを混合モードとすることを指定します。
nonsecure	電話プロキシ機能の設定時に、クラスタ モードを非セキュア モードとすることを指定します。

デフォルト

デフォルトのクラスタ モードは非セキュアです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
Phone-Proxy コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(4)	コマンドが追加されました。
9.4(1)	このコマンドは、すべての **phone-proxy** モード コマンドとともに廃止されました。

使用上のガイドライン

電話プロキシを混合モード クラスタ（セキュア モードと非セキュア モードの両方）で実行するように設定する場合は、一部の電話が認証または暗号化モードで設定されている場合に備えて LDC 発行元も設定する必要があります。

```
hostname(config)# crypto key generate rsa label ldc_signer_key modulus 1024
hostname(config)# crypto key generate rsa label phone_common modulus 1024
hostname(config)# tls-proxy my_proxy
hostname(config-tlsp)# server trust-point internal_PP_myctl
hostname(config-tlsp)# client ldc issuer ldc_server
hostname(config-tlsp)# client ldc keypair phone_common
```

例

次に、電話プロキシのセキュリティ モードを混合モードに設定する例を示します(IP 電話はセキュア モードと非セキュア モードで動作します)。

```
ciscoasa(config-phone-proxy)# cluster-mode mixed
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。
tls-proxy	TLS プロキシ インスタンスを設定します。

cluster port

仮想ロード バランシング クラスタの UDP ポートを設定するには、VPN ロード バランシング コンフィギュレーション モードで **cluster port** コマンドを使用します。ポートの指定を削除するには、このコマンドの **no** 形式を使用します。

cluster port *port*

no cluster port [*port*]

構文の説明

port	仮想ロード バランシング クラスタに割り当てる UDP ポート。

デフォルト

デフォルトのクラスタ ポートは 9023 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
VPN ロード バランシング コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

まず、**vpn load-balancing** コマンドを使用して、VPN ロード バランシング コンフィギュレーション モードを開始する必要があります。

任意の有効な UDP ポート番号を指定できます。範囲は 1 ～ 65535 です。

このコマンドの **no cluster port** 形式で *port* の値を指定した場合、指定したポート番号は既存の設定済みポート番号と一致する必要があります。

例

次に、仮想ロード バランシング クラスタの UDP ポートを 9023 に設定する例を示します。

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# interface lbpublic test
```

```
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# cluster port 9023
ciscoasa(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロード バランシング コンフィギュレーション モードを開始します。

cluster redistribute vpn-sessiondb

分散型 VPN クラスタ上でアクティブなセッションを再分散するには、特権 EXEC モードで次のコマンドを使用します。

cluster redistribute vpn-sessiondb

構文の説明

このコマンドには、引数はありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.9(1)	コマンドが追加されました。

使用上のガイドライン

このコマンドはバックグラウンドで実行され、CLI に戻ります。操作の完了時に、ユーザに向けてコンソール メッセージが表示されることはありません。

進行状況をモニタするには、**show cluster vpn-sessiondb distribution** コマンドを使用するか、syslogs を有効にします。

ASR 操作は、VPN セッションのオーケストレータであるマスター ノードで実行する必要があります。オーケストレータは、どのセッションがどこへ移動するかを計算します。オーケストレータ自体も、アクティブなセッションを自身から他のノードに移動させることができます。

この操作中のクラスタへの負荷を軽減してタイムリーな応答時間を確保するには、一度に最大 100 セッションを移動させることが要求されます。計算された移動が 1 ノードに対して 1000 セッションの場合、その計算には 10 件の個別の要求があると考えられます。

オーケストレータは、すべてのセッションが移動した時点で、あるいはオーナー メンバーが要求された数のセッションを移動させることができない場合に、ノードに対する移動要求が完了したものとみなします。

再分散操作は、ノードが移動要求に応答できない場合や、クラスタ トポロジの変更（メンバーの参加/脱退）があった場合などに中断されます。

再分散操作はベストエフォート型の操作です。操作の完了後に分散が完璧な状態になるという保証はありません。ノード上のセッション数が平均を 20 % も上回るまたは下回る場合もあります。

例

たとえば、cluster vpn-sessiondb distribution コマンドの実行結果が次のとおりであったとします。

```
Member 0 (unit-1-1): active: 229; backups at: 1(120), 2(109)
Member 1 (unit-1-3): active: 224; backups at: 0(117), 2(107)
Member 2 (unit-1-2): active: 0

After the ASR operation, the result looks like:

Member 0 (unit-1-1): active: 151; backups at: 1(120), 2(31)
Member 1 (unit-1-3): active: 151; backups at: 0(117), 2(34)
Member 2 (unit-1-2): active: 151; backups at: 0(72), 1(79)


Example of a successful initiation:
ciscoasa/master# cluster redistribute vpn-sessiondb
Session redistribution initiated.
Use 'show cluster vpn-sessiondb distribution' to view distribution.

Initiation when redistribution is already in progress:
ciscoasa/master# cluster redistribute vpn-sessiondb
Redistribution already in progress
Use 'show cluster vpn-sessiondb distribution' to view distribution.

When executed on a slave node

ciscoasa/slave# cluster redistribute vpn-sessiondb
ERROR: This command is only allowed on the cluster master
```

関連コマンド

コマンド	説明
vpn-mode	分散型 VPN を有効にします

cluster remove unit

ASA クラスタからユニットを削除するには、特権 EXEC モードで cluster remove unit コマンドを使用します。

cluster remove unit *unit_name*

構文の説明

unit_name	クラスタから削除するローカル ユニット名を指定します。メンバー名を一覧表示するには、**cluster remove unit ?** と入力するか、**show cluster info** コマンドを入力します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

ブートストラップ コンフィギュレーションは変更されず、マスター ユニットから最後に同期されたコンフィギュレーションもそのままであるので、コンフィギュレーションを失わずに後でそのユニットを再度追加できます。マスター ユニットを削除するためにスレーブ ユニットでこのコマンドを入力した場合は、新しいマスター ユニットが選定されます。

例

次に、ユニット名を確認してから、asa2 をクラスタから削除する例を示します。

```
ciscoasa(config)# cluster remove unit ?

Current active units in the cluster:
asa2

ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

関連コマンド

コマンド	説明
cluster exec	すべてのクラスタ メンバーにコマンドを送信します。
cluster group	クラスタを設定します。
cluster master unit	新しいユニットを ASA クラスタのマスター ユニットとして設定します。

cluster replication delay

TCP 接続 のクラスタ レプリケーション遅延をイネーブルにするには、クラスタ グループ コンフィギュレーション モードで **cluster replication delay** コマンドを使用します。遅延をディセーブルにするには、このコマンドの **no** 形式を使用します。

cluster replication delay *seconds* {**http** | **match tcp** {**host** *ip_address* | *ip_address mask* | **any** | **any4** | **any6**} [{**eq** | **lt** | **gt**} *port*] {**host** *ip_address* | *ip_address mask* | **any** | **any4** | **any6**} [{**eq** | **lt** | **gt**} *port*]}

no cluster replication delay *seconds* {**http** | **match tcp** {**host** *ip_address* | *ip_address mask* | **any** | **any4** | **any6**} [{**eq** | **lt** | **gt**} *port*] {**host** *ip_address* | *ip_address mask* | **any** | **any4** | **any6**} [{**eq** | **lt** | **gt**} *port*]}

構文の説明

seconds	遅延を 1 ～ 15 秒で設定します。
http	すべての HTTP トラフィックの遅延を設定します。**http** 遅延はデフォルトにより 5 秒間イネーブルになります。

コマンド デフォルト

http 遅延はデフォルトにより 5 秒間イネーブルになります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.4(1.152)	このコマンドが追加されました。

使用上のガイドライン

この機能で、ディレクタ/バックアップ フロー作成の遅延による存続期間が短いフローに関連する「不要な作業」を排除できます。

例

次に、FTP 遅延を 15 秒に設定し、HTTP 遅延を 15 秒に設定する例を示します。

```
ciscoasa(config)# cluster replication delay 15 match tcp any any eq ftp
ciscoasa(config)# cluster replication delay 15 http
```

関連コマンド

コマンド	説明
cluster group	クラスタ グループの設定を行います。

cn-id

参照 ID オブジェクトで cn-id を設定するには、*ca-reference-identity* モードで **cn-id** コマンドを使用します。cn-id を削除するには、このコマンドの **no** 形式を使用します。*ca-reference-identity* モードにアクセスするには、参照 ID オブジェクトを設定するための **crypto ca reference-identity** コマンドを入力します。

cn-id *value*

no cn-id *value*

構文の説明

value	各参照 ID の値。
cn-id	一般名（CN）。この値は、ドメイン名の全体的な形式に一致します。CN 値は自由形式のテキストにすることはできません。CN-ID 参照 ID では、アプリケーション サービスは特定されません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ca-reference-identity	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

参照 ID が作成されると、4 つの ID タイプと関連付けられた値を参照 ID に追加、または参照 ID から削除することができます。

参照 ID の **cn ID** と **dns ID** には、アプリケーション サービスを特定する情報を含めることができず、DNS ドメイン名を特定する情報が含まれている必要があります。

例

次に、syslog サーバの参照 ID を作成する例を示します。

```
ciscoasa(config)# crypto ca reference-identity syslogServer
ciscoasa(config-ca-ref-identity)# dns-id syslog1-bxb.cisco.com
ciscoasa(config-ca-ref-identity)# cn-id syslog1-bxb.cisco.com
```

関連コマンド

コマンド	説明
crypto ca reference-identity	参照 ID オブジェクトを設定します。
dns-id	参照 ID オブジェクトの DNS ドメイン名 ID を設定します。
srv-id	参照 ID オブジェクトで SRV-ID 識別子を設定します。
uri-id	参照 ID オブジェクトの URI ID を設定します。
logging host	セキュアな接続のために参照 ID オブジェクトを使用できるロギングサーバを設定します。
call-home profile destination address http	安全な接続のために参照 ID オブジェクトを使用できる Smart Call Home サーバを設定します。

command-alias

コマンドのエイリアスを作成するには、グローバル コンフィギュレーション モードで **command-alias** コマンドを使用します。エイリアスを削除するには、このコマンドの **no** 形式を使用します。

command-alias *mode command_alias original_command*

no command-alias *mode command_alias original_command*

構文の説明

command_alias	既存のコマンドに付ける新しい名前を指定します。
mode	**exec**（ユーザ EXEC モードおよび特権 EXEC モード）、**configure**、**interface** など、コマンド エイリアスを作成するコマンド モードを指定します。
original_command	コマンド エイリアスを作成する既存のコマンドまたはキーワードがあるコマンドを指定します。

デフォルト

デフォルトでは、次のユーザ EXEC モード エイリアスが設定されます。

- **help** の場合は **h**
- **logout** の場合は **lo**
- **ping** の場合は **p**
- **show** の場合は **s**

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

コマンド エイリアスを入力すると、元のコマンドが呼び出されます。たとえば、コマンド エイリアスを作成して、長いコマンドのショートカットにすることができます。

任意のコマンドの最初の部分のエイリアスを作成し、さらに通常どおり追加のキーワードと引数を入力できます。

CLI ヘルプを使用する場合、コマンド エイリアスはアスタリスク(*)で示され、次の形式で表示されます。

```
*command-alias=original-command
```

たとえば、**lo** コマンド エイリアスは、次のように、「lo」で始まる他の特権 EXEC モードのコマンドとともに表示されます。

```
ciscoasa# lo?
*lo=logout login logout
```

同じエイリアスをさまざまなモードで使用できます。たとえば、次のように、特権 EXEC モードおよびコンフィギュレーション モードで、「happy」を異なる複数のコマンドのエイリアスとして使用できます。

```
ciscoasa(config)# happy?

configure mode commands/options:
*happy="username employee1 password test"

exec mode commands/options:
*happy=enable
```

コマンドだけを表示し、エイリアスを省略するには、入力行の先頭にスペースを入力します。また、コマンド エイリアスを回避するには、コマンドを入力する前にスペースを使用します。次の例では、**happy?** コマンドの前にスペースがあるため、「happy」というエイリアスが表示されていません。

```
ciscoasa(config)# alias exec test enable
ciscoasa(config)# exit
ciscoasa#   happy?
ERROR: % Unrecognized command
```

コマンドの場合と同様に、CLI ヘルプを使用して、コマンド エイリアスの後に続く引数およびキーワードを表示できます。

完全なコマンド エイリアスを入力する必要があります。短縮されたエイリアスは使用できません。次の例では、パーサーは、**hap** コマンドが「happy」というエイリアスを示しているとは認識しません。

```
ciscoasa# hap
% Ambiguous command: "hap"
```

例

次に、**copy running-config startup-config** コマンドに対して「save」という名前のコマンド エイリアスを作成する例を示します。

```
ciscoasa(config)# command-alias exec save copy running-config startup-config
ciscoasa(config)# exit
ciscoasa# save

Source filename [running-config]?
Cryptochecksum: 50d131d9 8626c515 0c698f7f 613ae54e

2209 bytes copied in 0.210 secs
ciscoasa#
```

関連コマンド

コマンド	説明
clear configure command-alias	デフォルト以外のすべてのコマンド エイリアスをクリアします。
show running-config command-alias	設定されているデフォルト以外のすべてのコマンド エイリアスを表示します。

command-queue

応答を待つ間キューに入れられる MGCP コマンドの最大数を指定するには、MGCP マップ コンフィギュレーション モードで **command-queue** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

command-queue *limit*

no command-queue *limit*

構文の説明

limit	キューに入れるコマンドの最大数（1 ～ 2147483647）を指定します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

MGCP コマンド キューのデフォルトは 200 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
MGCP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

応答を待つ間キューに入れられる MGCP コマンドの最大数を指定するには **command-queue** コマンドを使用します。許可されている値の範囲は、1 ～ 4294967295 です。デフォルトは 200 です。制限値に達した状態で新しいコマンドが着信すると、最も長時間キューに入っているコマンドが削除されます。

例

次に、MGCP コマンドのキューを 150 コマンドに制限する例を示します。

```
ciscoasa(config)# mgcp-map mgcp_policy
ciscoasa(config-mgcp-map)#command-queue 150
```

関連コマンド

コマンド	説明
debug mgcp	MGCP のデバッグ情報の表示をイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。
show mgcp	MGCP のコンフィギュレーションおよびセッションの情報を表示します。
timeout	アイドル タイムアウトを設定します。タイムアウト後に、MGCP メディア接続または MGCP PAT xlate 接続が閉じられます。

commercial-security

IP オプション インスペクションが設定されたパケット ヘッダーで商用セキュリティ（CIPSO）オプションが発生したときに実行するアクションを定義するには、パラメータ コンフィギュレーション モードで **commercial-security** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

commercial-security action {allow | clear}

no commercial-security action {allow | clear}

構文の説明

allow	商用セキュリティ IP オプションを含むパケットを許可します。
clear	商用セキュリティ オプションをパケット ヘッダーから削除して、パケットを許可します。

デフォルト

デフォルトで、IP オプション インスペクションは、商用セキュリティ IP オプションを含むパケットをドロップします。

IP オプション インスペクション ポリシー マップで **default** コマンドを使用するとデフォルト値を変更できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IP オプション インスペクション ポリシー マップで設定できます。

IP オプション インスペクションを設定して、どの IP パケットが所定の IP オプションを持ち、ASA を通過できるかを制御できます。変更せずにパケットを通過させたり、指定されている IP オプションをクリアしてからパケットを通過させたりできます。

例

次に、IP オプション インスペクションのアクションをポリシー マップで設定する例を示します。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# commercial-security action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

community-list

Border Gateway Protocol（BGP）コミュニティ リストを作成または設定し、そのリストへのアクセスを制御するには、グローバル コンフィギュレーション モードで **community-list** コマンドを使用します。コミュニティ リストを削除するには、このコマンドの **no** 形式を使用します。

標準コミュニティ リスト

community-list {*standard* | **standard** *list-name*} {**deny** | **permit**} [*community-number*] [*AA*:*NN*] [**internet**] [**local-AS**] [**no-advertise**] [**no-export**]

no community-list {*standard* | **standard** *list-name*}

拡張コミュニティ リスト

community-list {*expanded* | **expanded** *list-name*} {**deny** | **permit**} *regexp*

no community-list {*expanded* | **expanded** *list-name*}

構文の説明

standard	コミュニティの 1 つ以上の許可または拒否グループを識別する 1 ～ 99 までの番号を使用して、標準コミュニティ リストを設定します。
standard *list-name*	標準コミュニティ リストを設定します。
permit	一致した条件へのアクセスを許可します。
deny	一致した条件へのアクセスを拒否します。
community-number	（オプション）1 ～ 4294967200 までの 32 ビットの番号としてコミュニティを指定します。1 つのコミュニティ、または複数のコミュニティをそれぞれスペースで区切って入力できます。
AA:NN	（任意）4 バイトの新コミュニティ形式で入力する自律システム番号およびネットワーク番号。この値は、コロンで区切られた 2 バイトの数 2 つで設定されます。2 バイトの数ごとに 1 ～ 65535 の数を入力できます。1 つのコミュニティ、または複数のコミュニティをそれぞれスペースで区切って入力できます。
internet	（任意）インターネット コミュニティを指定します。このコミュニティのルートは、すべてのピア（内部および外部）にアドバタイズされます。
no-export	（任意）no-export コミュニティを指定します。このコミュニティのあるルートは、同じ自律システム内のピアへのみ、または連合内の他のサブ自律システムへのみアドバタイズされます。これらのルートは外部ピアにはアドバタイズされません。
local-AS	（任意）local-as コミュニティを指定します。コミュニティのあるルートは、ローカル自律システムの一部であるピアへのみ、または連合のサブ自律システム内のピアへのみアドバタイズされます。これらのルートは、外部ピアや、連合内の他のサブ自律システムにはアドバタイズされません。
no-advertise	（任意）no-advertise コミュニティを指定します。このコミュニティのあるルートはピア（内部または外部）にはアドバタイズされません。
Expanded	コミュニティの 1 つ以上の許可または拒否グループを識別する 100 ～ 500 までの拡張コミュニティ リスト番号を設定します。

expanded *list-name*	拡張コミュニティ リストを設定します。
regexp	入力文字列との照合パターンの指定に使用される正規表現を設定します。 **（注）** 正規表現を使用できるのは拡張コミュニティ リストだけです。

デフォルト

BGP コミュニティの交換はデフォルトではイネーブルになりません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル設定	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

BGP コミュニティ フィルタリングを設定するには、**community-list** コマンドを使用します。BGP コミュニティ値は 32 ビット数値（古い形式）または 4 バイト数値（新しい形式）として設定されます。新しいコミュニティ形式は、**bgp-community new-format** コマンドをグローバル コンフィギュレーション モードで入力した場合に、イネーブルになります。新しいコミュニティ形式は、4 バイト値で構成されます。

先頭の 2 バイトは自律システム番号を表し、末尾の 2 バイトはユーザ定義のネットワーク番号を表します。名前付きおよび番号付きコミュニティ リストがサポートされます。BGP ピア間の BGP コミュニティ属性交換は、**neighbor send-community** コマンドが、指定されたネイバー用に設定されている場合にイネーブルになります。BGP コミュニティ属性は、RFC 1997 および RFC 1998 に定義されています。

BGP コミュニティの交換はデフォルトではイネーブルになりません。これは、**neighbor send-community** コマンドを使用してネイバー単位でイネーブルになります。このコマンドまたは **set community** コマンドで他のコミュニティ値が設定されるまで、デフォルトではすべてのルートまたはプレフィックスにインターネット コミュニティが適用されます。

特定のコミュニティ セットと照合するように許容値が設定されている場合は、デフォルトで、コミュニティ リストが他のすべてのコミュニティ値に対して暗黙拒否に設定されます。

標準コミュニティ リスト

標準コミュニティ リストは、既知のコミュニティや特定のコミュニティ番号の設定に使用されます。標準コミュニティ リストでは、最大 16 のコミュニティを設定できます。16 を超えるコミュニティを設定しようとすると、制限数を超えた後続のコミュニティは処理されないか、または実行コンフィギュレーション ファイルに保存されます。

拡張コミュニティ リスト

拡張コミュニティ リストは正規表現によるフィルタ コミュニティに使用されます。正規表現は、コミュニティ属性の照合パターンの設定に使用されます。* または + の文字を使用した照合の順序は、最長のコンストラクトが最初になります。入れ子のコンストラクトは外側から内側へと照合されます。連結コンストラクトは左側から順に照合されます。ある正規表現が、1 つの入力ストリングの異なる 2 つの部分と一致する可能性がある場合、早く入力された部分が最初に一致します。正規表現の設定の詳細については、『*Cisco IOS Terminal Services Configuration Guide*』の付録「Regular Expressions」を参照してください。

コミュニティ リストの処理

同じコミュニティ リスト文に複数の値を設定すると、論理 AND 条件が作成されます。AND 条件を満たすためにはすべてのコミュニティ値が一致しなければなりません。別のコミュニティ リスト文に複数の値を設定すると、論理 OR 条件が作成されます。条件に一致する最初のリストが処理されます。

例

次の例では、標準コミュニティ リストが、自律システム 50000 のネットワーク 10 からのルートを許可するように設定されます。

```
ciscoasa(config)#  community-list 1 permit 50000:10
```

次の例では、同じ自律システムのピアか、同じ連合内のサブ自律システムのピアからのルートのみを許可するように、標準コミュニティ リストが設定されます。

```
ciscoasa(config)#  community-list 1 permit no-export
```

次の例では、標準コミュニティ リストが、自律システム 65534 内のネットワーク 40 からのコミュニティと自律システム 65412 内のネットワーク 60 からのコミュニティを搬送するルートを拒否するように設定されます。この例は、論理 AND 条件を示しています。すべてのコミュニティ値が一致しないとリストが処理されません。

```
ciscoasa(config)#  community-list 2 deny 65534:40 65412:60
```

次の例では、名前付き標準コミュニティ リストが、ローカル自律システム内のすべてのルートを許可する、または、自律システム 40000 内のネットワーク 20 からのルートを許可するように設定されます。この例は、論理 OR 条件を示しています。最初の一致が処理されます。

```
ciscoasa(config)#  community-list standard RED permit local-AS
ciscoasa(config)#  community-list standard RED permit 40000:20
```

次の例では、プライベート自律システムからのコミュニティを持つルートを拒否するような拡張コミュニティ リストが設定されます。

```
ciscoasa(config)#  community-list 500 deny _64[6-9][0-9][0-9]_|_65[0-9][0-9][0-9]_
```

次の例では、自律システム 50000 のネットワーク 1 から 99 からのルートを拒否するような名前方式の拡張コミュニティ リストが設定されます。

```
ciscoasa(config)#  community-list expanded BLUE deny 50000:[0-9][0-9]_
```

関連コマンド

コマンド	説明
bgp-community-new format	コミュニティを AA:NN（自律システム:コミュニティ番号/4 バイトの番号）形式で表示するように BGP を設定します。
neighbor send-community	コミュニティ属性が BGP ネイバーに送信されるように指定します。
set community	BGP コミュニティ属性を設定します。

compatible rfc1583

RFC 1583 に従った集約ルート コストの計算に使用した方式に戻すには、ルータ コンフィギュレーション モードで **compatible rfc1583** コマンドを使用します。RFC 1583 互換性をディセーブルにするには、このコマンドの **no** 形式を使用します。

compatible rfc1583

no compatible rfc1583

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

コンフィギュレーションには、このコマンドの **no** 形式だけが記述されます。

例

次に、RFC 1583 互換のルート集約コスト計算をディセーブルにする例を示します。

```
ciscoasa(config-router)# no compatible rfc1583
ciscoasa(config-router)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

compression

anyconnect-ssl 接続および WebVPN 接続で圧縮を有効にするには、グローバル コンフィギュレーション モードで **compression** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

compression {**all** | **anyconnect-ssl**| **http-comp**}

no compression {**all** | **anyconnect-ssl**| **http-comp**}

all	使用可能なすべての圧縮技術をイネーブルにすることを指定します。
anyconnect-ssl	anyconnect-ssl 接続での圧縮を指定します。
http-comp	WebVPN 接続に対する圧縮を指定します。

デフォルト

デフォルトは、*all* です。使用可能なボックス全体の圧縮技術がすべて有効になっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応		—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

グローバル コンフィギュレーション モードで設定した **compression** コマンドにより、グループ ポリシー webvpn モードおよびユーザ名 webvpn モードで設定した **compression** anyconnect-ssl コマンドは上書きされます。

たとえば、グループ ポリシー webvpn コンフィギュレーション モードで特定のグループに対する **anyconnect-ssl compression** コマンドを入力し、次にグローバル コンフィギュレーション モードで **no compression** コマンドを入力した場合、そのグループに対して設定した **anyconnect-ssl compression** コマンドの設定は上書きされます。

逆に、グローバル コンフィギュレーション モードで **compression** コマンドを使用して圧縮をオンに戻した場合は、グループ設定が有効となり、圧縮動作は最終的にグループ設定によって決定されます。

no compression コマンドを使用して圧縮をディセーブルにした場合、新しい接続だけが影響を受けます。アクティブな接続は影響を受けません。

例

次に、anyconnect-ssl 接続で圧縮をオンにする例を示します。

```
hostname(config)# compression anyconnect-ssl
```

次に、anyconnect-ssl 接続および WebVPN 接続で圧縮を無効にする例を示します。

```
hostname(config)# no compression anyconnect-ssl http-comp
```

関連コマンド

コマンド	説明
show webvpn anyconnect-ssl	anyconnect-ssl インストールに関する情報を表示します。
anyconnect-ssl enable	特定のグループまたはユーザに対して anyconnect-ssl を有効または必須にします。
anyconnect-ssl compression	特定のグループまたはユーザに対して anyconnect-ssl 接続を介する HTTP データの圧縮を有効にします。

config-register

次回 ASA をリロードするときに使用されるコンフィギュレーション レジスタ値を設定するには、グローバル コンフィギュレーション モードで **config-register** コマンドを使用します。値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

config-register *hex_value*

no config-register

構文の説明

hex_value	コンフィギュレーション レジスタ値を 0x0 ～ 0xFFFFFFFF の 16 進数値に設定します。この数は 32 ビットを表し、各 16 進文字は 4 ビットを表します。それぞれのビットが異なる特性を制御します。ただし、ビット 32 ～ 20 は将来の使用のために予約されており、ユーザが設定できないか、または現在 ASA で使用されていません。したがって、これらのビットを表す 3 つの文字は常に 0 に設定されているため、無視できます。関連するビットは、5 桁の 16 進文字（0x*nnnnn*）で表されます。 文字の前の 0 は含める必要はありません。後続の 0 は含める必要があります。たとえば、0x2001 は 0x02001 と同じですが、0x10000 の 0 はすべて必要です。関連するビットに使用できる値の詳細については、表 8-1 を参照してください。

デフォルト

デフォルト値は 0x1 であり、ローカル イメージおよびスタートアップ コンフィギュレーションからブートします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、ASA 5500 シリーズでのみサポートされます。コンフィギュレーション レジスタ値は、ブート元のイメージおよび他のブート パラメータを決定します。

5 つの文字には、右から左への方向で 0 ～ 4 の番号が付けられます。これは、16 進数および 2 進数の場合には標準的です。各文字に対して 1 つの値を選択したり、必要に応じて値を組み合わせて一致させたりすることができます。たとえば、文字番号 3 に対して 0 または 2 を選択できます。他の値との競合が生じる場合、一部の値が優先されます。たとえば、ASA を TFTP サーバとローカル イメージの両方からブートするように設定する 0x2011 を設定した場合、ASA は TFTP サーバからブートします。この値は、TFTP のブートが失敗した場合、ASA が直接 ROMMON でブートすることも定めているため、デフォルト イメージからブートすることを指定したアクションは無視されます。

0 の値は、他に指定されていなければ、アクションを実行しないことを意味します。

表 8-1 に、各 16 進文字に関連付けられたアクションを示します。各文字に対して 1 つの値を選択します。

表 8-1　コンフィギュレーション レジスタ値

プレフィックス	16 進数文字番号 4、3、2、1、および 0				
0x	0	0	0[1]	0[2]	0
	1 起動中に 10 秒の ROMMON のカウントダウンをディセーブルにします。通常は、カウントダウン中に Escape キーを押して ROMMON を開始できます。	2 TFTP サーバからブートするように ASA を設定している場合、ブートが失敗すると、この値は直接 ROMMON でブートします。		1 ROMMON ブート パラメータ（存在する場合は、**boot system tftp** コマンドと同じ）で指定されたように TFTP サーバ イメージからブートします。この値は、文字 1 に設定された値よりも優先されます。	1 最初の **boot system** *local_flash* コマンドで指定されたイメージをブートします。そのイメージがロードされない場合、ASA は、正常にブートするまで後続の **boot system** コマンドで指定された各イメージのブートを試行します。
					2、4、6、8 特定の **boot system** *local_flash* コマンドで指定されたイメージをブートします。値 3 を指定すると最初の **boot system** コマンドで指定されたイメージが、値 5 を指定すると 2 つめのイメージが起動されます。以降同様に起動されます。 イメージが正常にブートしない場合、ASA は他の **boot system** コマンド イメージに戻ることを試行しません（この点が値 1 と値 3 の使用における違いです）。ただし、ASA には、ブートが失敗した場合に内部フラッシュ メモリのルート ディレクトリ内で検出された任意のイメージからブートを試行するフェールセーフ機能があります。フェールセーフ機能を有効にしない場合は、ルート以外のディレクトリにイメージを保存します。
				4[3] スタートアップ コンフィギュレーションを無視してデフォルトのコンフィギュレーションをロードします。	3、5、7、9 ROMMON で、**boot** コマンドを引数なしで入力した場合、ASA は特定の **boot system** *local_flash* コマンドで指定されたイメージをブートします。値 3 を指定すると最初の **boot system** コマンドで指定されたイメージが、値 5 を指定すると 2 つめのイメージが起動されます。以降同様に起動されます。この値はイメージを自動的にブートしません。
				5 上記の両方のアクションを実行します。	

1. 将来的な使用のために予約されています。
2. 文字番号 0 および 1 が、イメージを自動的にブートするように設定されていない場合、ASA は直接 ROMMON でブートします。
3. **service password-recovery** コマンドを使用してパスワード回復をディセーブルにした場合は、スタートアップ コンフィギュレーションを無視するようにコンフィギュレーション レジスタを設定することはできません。

コンフィギュレーション レジスタ値はスタンバイ ユニットに複製されませんが、アクティブ ユニットにコンフィギュレーション レジスタを設定すると、次の警告が表示されます。

```
WARNING The configuration register is not synchronized with the standby, their values may
not match.
```

confreg コマンドを使用して、コンフィギュレーション レジスタ値を ROMMON で設定することもできます。

例

次に、デフォルト イメージからブートするようにコンフィギュレーション レジスタを設定する例を示します。

```
ciscoasa(config)# config-register 0x1
```

関連コマンド

コマンド	説明
boot	ブート イメージおよびスタートアップ コンフィギュレーションを設定します。
service password-recovery	パスワードの回復をイネーブルまたはディセーブルにします。

config-replicate-parallel

スレーブユニットでの設定変更を順番にではなく並列に同期するには、クラスタ コンフィギュレーション モードで **config-replicate-parallel** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

config-replicate-parallel

no config-replicate-parallel

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラスタ構成	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.14(1)	コマンドが追加されました。

使用上のガイドライン

設定の並列同期は、順次同期よりもパフォーマンスが向上します。

例

次の例では、並列同期をディセーブルにします。

```
ciscoasa(config)# cluster cluster1
ciscoasa(cfg-cluster)# no config-replicate-parallel
```

関連コマンド

コマンド	説明
クラスタ	クラスタ コンフィギュレーション モードを開始します

configure factory-default

コンフィギュレーションを出荷時のデフォルトに戻すには、グローバル コンフィギュレーション モードで **configure factory-default** コマンドを使用します。

configure factory-default [*ip_address* [*mask*]]

構文の説明

ip_address	デフォルトのアドレス 192.168.1.1 を使用する代わりに、管理インターフェイスまたは内部インターフェイスの IP アドレスを設定します。各モデルで設定されるインターフェイスの詳細については、「使用上のガイドライン」を参照してください。
mask	インターフェイスのサブネット マスクを設定します。マスクを設定しない場合、ASA は IP アドレス クラスに適したマスクを使用します。

デフォルト

デフォルトの IP アドレスとマスクは 192.168.1.1 および 255.255.255.0 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	出荷時のデフォルトのコンフィギュレーションが ASA 5505 に追加されました。

使用上のガイドライン

工場出荷時のデフォルトのコンフィギュレーションは、シスコによって新しい ASA に適用される設定です。このコマンドは PIX 525 および PIX 535 ASA を除き、すべてのプラットフォームでサポートされています。

PIX 515/515E および ASA 5510 以上の ASA では、出荷時のデフォルトのコンフィギュレーションによって、管理インターフェイスが自動的に設定されるため、ASDM を使用してそのインターフェイスに接続し、残りの設定を実行できます。ASA 5505 では、出荷時のデフォルトのコンフィギュレーションによって、ASA をネットワークですぐに使用できるように、インターフェイスと NAT が自動的に設定されます。

このコマンドは、ルーテッド ファイアウォール モードでのみ使用可能です。トランスペアレント モードはインターフェイスの IP アドレスをサポートしていません。インターフェイス IP アドレスの設定は、このコマンドが行うアクションの 1 つです。また、このコマンドはシングル コンテキスト モードでのみ使用できます。コンフィギュレーションをクリアされた ASA には、このコマンドを使用して自動的に設定される定義済みのコンテキストはありません。

このコマンドは現在の実行コンフィギュレーションをクリアしてから、複数のコマンドを設定します。

configure factory-default コマンドで IP アドレスを設定した場合、**http** コマンドは、ユーザが指定したサブネットを使用します。同様に、**dhcpd address** コマンドの範囲は、指定したサブネット内のアドレスで構成されます。

出荷時のデフォルトのコンフィギュレーションに戻した後に、**write memory** コマンドを使用してこのコンフィギュレーションを内部フラッシュ メモリに保存します。**write memory** コマンドは、前に **boot config** コマンドで別の場所を設定している場合でも、その設定をクリアしたときにパスもクリアされているので、スタートアップ コンフィギュレーション用のデフォルトの場所に実行コンフィギュレーションを保存します。

(注) このコマンドは、**boot system** コマンド（存在する場合）も、他のコンフィギュレーションとともにクリアします。**boot system** を使用すると、外部フラッシュ メモリ カードのイメージを含む特定のイメージからブートできます。出荷時のコンフィギュレーションに戻した後、次回 ASA をリロードすると、ASA は、内部フラッシュ メモリの最初のイメージからブートします。内部フラッシュ メモリにイメージがない場合、はブートしません。

完全なコンフィギュレーションに有用な追加の設定を行うには、**setup** コマンドを参照してください。

ASA 5505 のコンフィギュレーション

ASA 5505 の工場出荷時のデフォルト設定は、次のとおりです。

- イーサネット 0/1 ～ 0/7 スイッチ ポートを含む内部 VLAN 1 インターフェイス。**configure factory-default** コマンドで IP アドレスを設定していない場合、VLAN 1 の IP アドレスとマスクは、それぞれ 192.168.1.1 と 255.255.255.0 になります。
- イーサネット 0/0 スイッチ ポートを含む外部 VLAN 2 インターフェイス。VLAN 2 は、DHCP を使用してその IP アドレスを取得します。
- デフォルトのルートも DHCP から取得されます。
- すべての内部 IP アドレスが、外部にアクセスするときにインターフェイス PAT によって変換されます。
- デフォルトでは、内部ユーザはアクセス リストを使用して外部にアクセスでき、外部ユーザは内部にアクセスできません。
- ASA で DHCP サーバがイネーブルになっているため、VLAN 1 インターフェイスに接続している PC は、192.168.1.2 ～ 192.168.1.254 のアドレスを受け取ります。
- ASDM 用に HTTP サーバがイネーブルにされており、192.168.1.0 ネットワーク上のユーザからアクセスできます。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface Ethernet 0/0
   switchport access vlan 2
   no shutdown
interface Ethernet 0/1
   switchport access vlan 1
   no shutdown
```

```
interface Ethernet 0/2
   switchport access vlan 1
   no shutdown
interface Ethernet 0/3
   switchport access vlan 1
   no shutdown
interface Ethernet 0/4
   switchport access vlan 1
   no shutdown
interface Ethernet 0/5
   switchport access vlan 1
   no shutdown
interface Ethernet 0/6
   switchport access vlan 1
   no shutdown
interface Ethernet 0/7
   switchport access vlan 1
   no shutdown
interface vlan2
   nameif outside
   no shutdown
   ip address dhcp setroute
interface vlan1
   nameif inside
   ip address 192.168.1.1 255.255.255.0
   security-level 100
   no shutdown
global (outside) 1 interface
nat (inside) 1 0 0
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.2-192.168.1.254 inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational
```

ASA 5510 以降のコンフィギュレーション

ASA 5510 以降の工場出荷時のデフォルト設定は、次のとおりです。

- 管理用 Management 0/0 インターフェイス。**configure factory-default** コマンドで IP アドレスを設定しなかった場合、IP アドレスおよびマスクは 192.168.1.1 および 255.255.255.0 です。
- ASA では DHCP サーバがイネーブルにされているため、このインターフェイスに接続する PC には、192.168.1.2 ～ 192.168.1.254 の間のアドレスが割り当てられます。
- ASDM 用に HTTP サーバがイネーブルにされており、192.168.1.0 ネットワーク上のユーザからアクセスできます。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface management 0/0
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

PIX 515/515E セキュリティ アプライアンスのコンフィギュレーション

PIX 515/515E セキュリティ アプライアンスの出荷時のデフォルトのコンフィギュレーションによって、次のように設定されます。

- 内部 Ethernet1 インターフェイス。**configure factory-default** コマンドで IP アドレスを設定しなかった場合、IP アドレスおよびマスクは 192.168.1.1 および 255.255.255.0 です。
- PIX セキュリティ アプライアンスで DHCP サーバがイネーブルになっているため、このインターフェイスに接続する PC には、192.168.1.2 ～ 192.168.1.254 の間のアドレスが割り当てられます。
- ASDM 用に HTTP サーバがイネーブルにされており、192.168.1.0 ネットワーク上のユーザからアクセスできます。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface ethernet 1
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

例

次に、コンフィギュレーションを出荷時のデフォルトにリセットし、IP アドレス 10.1.1.1 をインターフェイスに割り当て、次に新しいコンフィギュレーションをスタートアップ コンフィギュレーションとして保存する例を示します。

```
ciscoasa(config)# configure factory-default 10.1.1.1 255.255.255.0
Based on the inside IP address and mask, the DHCP address
pool size is reduced to 253 from the platform limit 256

WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
...
ciscoasa(config)#
ciscoasa(config)# copy running-config startup-config
```

関連コマンド

コマンド	説明
boot system	ブート元のソフトウェア イメージを設定します。
clear configure	実行コンフィギュレーションをクリアします。
copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

コマンド	説明
setup	ASA の基本設定を設定するよう要求します。
show running-config	実行コンフィギュレーションを表示します。

configure http

HTTP(S) サーバから実行コンフィギュレーションにコンフィギュレーション ファイルをマージするには、グローバル コンフィギュレーション モードで **configure http** コマンドを使用します。

configure [interface *name***] http[s]://[***user***[:***password***]@]***server***[:***port***]/[***path***/]***filename*

構文の説明

:password	（任意）HTTP(S) 認証の場合、パスワードを指定します。
:*port*	（任意）ポートを指定します。HTTP の場合、デフォルトは 80 です。HTTPS の場合、デフォルトは 443 です。
@	（任意）名前とパスワードの両方またはいずれかを入力する場合は、サーバの IP アドレスの前にアットマーク（@）を付けます。
filename	コンフィギュレーション ファイル名を指定します。
http[**s**]	HTTP または HTTPS を指定します。
interface *name*	（任意）コンフィギュレーション ファイルをコピーするインターフェイス名を指定します。インターフェイスを指定しなかった場合、ASA は管理専用ルーティング テーブルを確認し、一致するものが見つからなければ、データのルーティング テーブルを確認します。
path	（任意）ファイル名へのパスを指定します。
server	サーバの IP アドレスまたは名前を指定します。IPv6 サーバ アドレスでポートを指定する場合は、IP アドレス内のコロンがポート番号の前のコロンと間違われないように、IP アドレスをカッコで囲む必要があります。たとえば、アドレスとポートを次のように入力します。 `[fe80::2e0:b6ff:fe01:3b7a]:8080`
user	（任意）HTTP(S) 認証の場合、ユーザ名を指定します。

デフォルト

HTTP の場合、デフォルト ポートは 80 です。HTTPS の場合、デフォルト ポートは 443 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.5(1)	**interface** *name* 引数が追加されました。

使用上のガイドライン

このコマンドは IPv4 および IPv6 のアドレスをサポートします。マージでは、新しいコンフィギュレーションから実行コンフィギュレーションにすべてのコマンドが追加され、競合するすべてのコマンドが新しいバージョンで上書きされます。たとえば、複数インスタンスが許可されるコマンドの場合は、新しいコマンドが実行コンフィギュレーションの既存のコマンドに追加されます。単一インスタンスだけが許可されるコマンドの場合は、新しいコマンドで実行コンフィギュレーション内のコマンドが上書きされます。実行コンフィギュレーション内に存在するが、新しいコンフィギュレーションには設定されていないコマンドは、マージによって削除されません。

このコマンドは、**copy http running-config** コマンドと同じです。マルチ コンテキスト モードの場合、このコマンドはシステム実行スペースでのみ使用できるため、**configure http** コマンドはコンテキスト内で使用するための代替です。

インターフェイスを指定しなかった場合、ASA は管理専用ルーティング テーブルを確認し、一致するものが見つからなければ、データのルーティング テーブルを確認します。管理専用インターフェイスを経由するデフォルト ルートがある場合は、すべての **configure** トラフィックがそのルートに一致するため、データ ルーティング テーブルを確認することはありません。このシナリオでは、データ インターフェイスからコピーする必要がある場合にそのインターフェイスを指定します。

例

次に、コンフィギュレーション ファイルを HTTPS サーバから実行コンフィギュレーションにコピーする例を示します。

```
ciscoasa(config)# configure https://user1:pa$$w0rd@10.1.1.1/configs/newconfig.cfg
```

関連コマンド

コマンド	説明
clear configure	実行コンフィギュレーションをクリアします。
configure memory	スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージします。
configure net	指定した TFTP URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
configure factory-default	CLI で入力するコマンドを実行コンフィギュレーションに追加します。
show running-config	実行コンフィギュレーションを表示します。

configure memory

スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージするには、グローバル コンフィギュレーション モードで **configure memory** コマンドを使用します。

configure memory

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

マージでは、新しいコンフィギュレーションから実行コンフィギュレーションにすべてのコマンドが追加され、競合するすべてのコマンドが新しいバージョンで上書きされます。たとえば、複数インスタンスが許可されるコマンドの場合は、新しいコマンドが実行コンフィギュレーションの既存のコマンドに追加されます。単一インスタンスだけが許可されるコマンドの場合は、新しいコマンドで実行コンフィギュレーション内のコマンドが上書きされます。実行コンフィギュレーション内に存在するが、新しいコンフィギュレーションには設定されていないコマンドは、マージによって削除されません。

コンフィギュレーションをマージしない場合は、ASA を経由する通信を妨げる実行コンフィギュレーションをクリアしてから、**configure memory** コマンドを入力して新しいコンフィギュレーションをロードできます。

このコマンドは、**copy startup-config running-config** コマンドと同じです。

マルチ コンテキスト モードの場合、コンテキストのスタートアップ コンフィギュレーションは、**config-url** コマンドで指定した場所にあります。

例

次に、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーする例を示します。

```
ciscoasa(config)# configure memory
```

関連コマンド

コマンド	説明
clear configure	実行コンフィギュレーションをクリアします。
configure http	指定した HTTP(S) URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
configure net	指定した TFTP URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
configure factory-default	CLI で入力するコマンドを実行コンフィギュレーションに追加します。
show running-config	実行コンフィギュレーションを表示します。

configure net

TFTP サーバのコンフィギュレーション ファイルを実行コンフィギュレーションにマージするには、グローバル コンフィギュレーション モードで **configure net** コマンドを使用します。

configure net [**interface** *name*] [*server*:[*filename*] | :*filename*]

構文の説明

:*filename*	パスとファイル名を指定します。**tftp-server** コマンドを使用してすでにファイル名を設定してある場合、この引数はオプションです。 このコマンドでファイル名を指定し、**tftp-server** コマンドで名前を指定する場合、ASA は **tftp-server** コマンド ファイル名をディレクトリとして扱い、**configure net** コマンド ファイル名をディレクトリの下のファイルとして追加します。 **tftp-server** コマンドの値を上書きするには、パスとファイル名の前にスラッシュを入力します。スラッシュは、パスが tftpboot ディレクトリに対する相対パスではなく、絶対パスであることを示します。このファイル用に生成される URL には、ファイル名パスの前にダブル スラッシュ(//)が含まれます。必要なファイルが tftpboot ディレクトリにある場合は、ファイル名パスに tftpboot ディレクトリへのパスを含めることができます。 **tftp-server** コマンドを使用して TFTP サーバのアドレスを指定した場合は、コロン(:)の後にファイル名だけを入力できます。
interface *name*	(任意)コンフィギュレーション ファイルをコピーするインターフェイス名を指定します。インターフェイスを指定しなかった場合、ASA は管理専用ルーティング テーブルを確認し、一致するものが見つからなければ、データのルーティング テーブルを確認します。
server:	TFTP サーバの IP アドレスまたは名前を設定します。**tftp-server** コマンドで設定したアドレスがあっても、このアドレスが優先されます。IPv6 サーバ アドレスの場合、IP アドレス内のコロンがファイル名の前のコロンと間違われないように、IP アドレスをカッコで囲む必要があります。たとえば、アドレスを次のように入力します。 [fe80::2e0:b6ff:fe01:3b7a] デフォルトのゲートウェイ インターフェイスは最もセキュリティが高いインターフェイスですが、**tftp-server** コマンドを使用して別のインターフェイス名を設定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.5(1)	**interface** *name* 引数が追加されました。

使用上のガイドライン

このコマンドは IPv4 および IPv6 のアドレスをサポートします。マージでは、新しいコンフィギュレーションから実行コンフィギュレーションにすべてのコマンドが追加され、競合するすべてのコマンドが新しいバージョンで上書きされます。たとえば、複数インスタンスが許可されるコマンドの場合は、新しいコマンドが実行コンフィギュレーションの既存のコマンドに追加されます。単一インスタンスだけが許可されるコマンドの場合は、新しいコマンドで実行コンフィギュレーション内のコマンドが上書きされます。実行コンフィギュレーション内に存在するが、新しいコンフィギュレーションには設定されていないコマンドは、マージによって削除されません。

このコマンドは、**copy tftp running-config** コマンドと同じです。マルチ コンテキスト モードの場合、このコマンドはシステム実行スペースでのみ使用できるため、**configure net** コマンドはコンテキスト内で使用するための代替です。

インターフェイスを指定しなかった場合、ASA は管理専用ルーティング テーブルを確認し、一致するものが見つからなければ、データのルーティング テーブルを確認します。管理専用インターフェイスを経由するデフォルト ルートがある場合は、すべての **configure** トラフィックがそのルートに一致するため、データ ルーティング テーブルを確認することはありません。このシナリオでは、データ インターフェイスからコピーする必要がある場合にそのインターフェイスを指定します。

例

次に、**tftp-server** コマンドにサーバとファイル名を設定してから、**configure net** コマンドを使用してサーバを上書きする例を示します。同じファイル名が使用されています。

```
ciscoasa(config)# tftp-server inside 10.1.1.1 configs/config1
ciscoasa(config)# configure net 10.2.2.2:
```

次に、サーバおよびファイル名を上書きする例を示します。ファイル名へのデフォルト パスは /tftpboot/configs/config1 です。ファイル名をスラッシュ (/) で始めない場合、パスの /tftpboot/ 部分がデフォルトで含まれます。このパスを上書きし、ファイルも tftpboot にある場合は、tftpboot パスを **configure net** コマンドに含めます。

```
ciscoasa(config)# tftp-server inside 10.1.1.1 configs/config1
ciscoasa(config)# configure net 10.2.2.2:/tftpboot/oldconfigs/config1
```

次に、サーバだけを **tftp-server** コマンドに設定する例を示します。**configure net** コマンドはファイル名だけを指定します。

```
ciscoasa(config)# tftp-server inside 10.1.1.1
ciscoasa(config)# configure net :configs/config1
```

関連コマンド

コマンド	説明
configure http	指定した HTTP(S) URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
configure memory	スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージします。
show running-config	実行コンフィギュレーションを表示します。
tftp-server	他のコマンドで使用するためのデフォルトの TFTP サーバおよびパスを設定します。
write net	実行コンフィギュレーションを TFTP サーバにコピーします。

configure session

ACL やオブジェクトを隔離して編集できるコンフィギュレーション セッションを作成または開くには、特権 EXEC モードで **configure session** コマンドを使用します。

configure session *session_name*

構文の説明

session_name	コンフィギュレーション セッションの名前。セッションがすでに存在する場合は、そのセッションを開きます。そうでない場合は、新しいセッションを作成します。 現在のセッションのリストを表示するには、**show configuration session** コマンドを使用します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

使用上のガイドライン

アクセス ルールまたは他の目的に使用する ACL を編集すると、その変更はすぐに実装され、トラフィックに影響を与えます。新しいルールがアクティブになるのはルールのコンパイルが完了した後のみとし、そのコンパイルは各 ACE を編集した後に発生することを、トランザクション コミット モデルによって保証するために、アクセス ルールを使用できます。

ACL 編集の影響をさらに分離するには、「コンフィギュレーション セッション」で変更を行うことができます。このセッションは、変更内容を明示的にコミットする前に、複数の ACE やオブジェクトを編集できる隔離されたモードです。このため、デバイスの動作を変更する前に、目的のすべての変更が完了したことを確認できます。

新しいセッションを作成するか、または既存のセッションを開くには、**configure session** コマンドを使用します。他のユーザが編集のためにセッションをすでに開いている場合は、そのセッションを開くことはできません。セッションが実際には編集されていないと判断した場合は、**clear session** *session_name* **access** コマンドを使用してアクセス フラグをリセットしてから、そのセッションを開くことができます。

一度に最大 3 つのセッションを定義できます。

1 つのセッション内で、次のコマンドを使用できます。

- コンフィギュレーション コマンド:コミットされていないセッションでは、任意のパラメータを指定して次の基本コマンドを使用できます。
  - **access-list**
  - **object**
  - **object-group**
- セッション管理コマンド:使用できるコマンドは、そのセッションを以前コミットしたかどうかによって異なります。使用できる可能性があるコマンドは次のとおりです。
  - **exit**:セッションを単に終了し、変更のコミットや廃棄は行わないため、後で戻ることができます。
  - **commit** [**noconfirm** [**revert-save** | **config-save**]]:(コミットされていないセッションのみ)変更を保存します。セッションを保存するかどうか尋ねられます。リバート セッションを保存(**revert-save**)しておくと、**revert** コマンドで変更を元に戻すことができます。また、コンフィギュレーション セッションを保存(**config-save**)しておくと、そのセッションで変更したすべての内容を、必要に応じて再度コミットできます。リバート セッションまたはコンフィギュレーション セッションを保存した場合は、変更はコミットされますが、セッションはアクティブのままになります。セッションを開いて、変更を元に戻したり同じ変更を再コミットしたりできます。**noconfirm** オプションと任意の適切な save オプションを指定すると、プロンプトが表示されないようにすることができます。
  - **abort**:(コミットされていないセッションのみ)変更を破棄し、セッションを削除します。セッションを保持する場合は、セッションを終了して **clear session** *session_name* **configuration** コマンドを使用します。このコマンドは、セッションを削除せずに空にします。
  - **revert**:(コミットされたセッションのみ)変更を元に戻し、セッションをコミットする前のコンフィギュレーションに戻して、そのセッションを削除します。
  - **show configuration session** [*session_name*]:セッションで行った変更を表示します。

例

次に、my-session を開く例を示します。

```
ciscoasa# configure session my-session access
ciscoasa(config-s)#
```

関連コマンド

コマンド	説明
clear configuration session	コンフィギュレーション セッションとその内容を削除します。
clear session	コンフィギュレーション セッションの内容をクリアするか、そのアクセス フラグをリセットします。
forward-reference	ACE のオブジェクトや ACL、またはアクセス グループが存在する前に、それらを参照できます。
show configuration session	現在の各セッションで行われた変更を表示します。

configure terminal

実行コンフィギュレーションをコマンドラインで設定するには、特権 EXEC モードで **configure terminal** コマンドを使用します。

configure terminal

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、コンフィギュレーションを変更するコマンドを入力できるグローバル コンフィギュレーション モードを開始します。

例

次に、グローバル コンフィギュレーション モードを開始する例を示します。

```
ciscoasa# configure terminal
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure	実行コンフィギュレーションをクリアします。
configure http	指定した HTTP(S) URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
configure memory	スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージします。
configure net	指定した TFTP URL のコンフィギュレーション ファイルを実行コンフィギュレーションにマージします。
show running-config	実行コンフィギュレーションを表示します。

config-url

システムがコンテキスト コンフィギュレーションをダウンロードする URL を指定するには、コンテキスト コンフィギュレーション モードで **config-url** コマンドを使用します。

config-url *url*

構文の説明

url	コンテキスト コンフィギュレーションの URL を設定します。すべてのリモート URL は、管理コンテキストからアクセスできる必要があります。次の URL 構文を参照してください。 • **disk0:/**[*path*/]*filename* ASA 5500 シリーズでは、この URL は内部フラッシュ メモリを示します。**disk0** コマンドではなく **flash** コマンドを使用することもできます。これらはエイリアスになっています。 • **disk1:/**[*path*/]*filename* ASA 5500 シリーズでは、この URL は外部フラッシュ メモリ カードを示します。 • **flash:/**[*path*/]*filename* この URL は内部フラッシュ メモリを示します。 • **ftp://**[*user*[**:***password*]@]*server*[:*port*]**/**[*path*/]*filename*[**;type=***xx*] **type** には次のキーワードのいずれかを指定できます。 – **ap**：ASCII 受動モード – **an**：ASCII 通常モード – **ip**：（デフォルト）バイナリ受動モード – **in**：バイナリ通常モード • **http**[**s**]**://**[*user*[**:***password*]@]*server*[:*port*]**/**[*path*/]*filename* • **tftp://**[*user*[**:***password*]@]*server*[:*port*]**/**[*path*/]*filename*[**;int=***interface_name*] サーバ アドレスへのルートを上書きする場合は、インターフェイス名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
コンテキスト コンフィギュレーション	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン　コンテキスト URL を追加すると、システムはただちにコンテキストをロードし、実行中になります。

(注)　**config-url** コマンドを入力する前に、**allocate-interface** コマンドを入力します。ASA は、コンテキスト コンフィギュレーションをロードする前に、コンテキストにインターフェイスを割り当てる必要があります。コンテキスト コンフィギュレーションには、インターフェイス（**interface**、**nat**、**global** など）を示すコマンドが含まれている場合があります。最初に **config-url** コマンドを入力した場合、ASA はただちにコンテキスト コンフィギュレーションをロードします。インターフェイスを示すコマンドがコンテキストに含まれている場合、それらのコマンドは失敗します。

ファイル名にファイル拡張子は必要ありませんが、「.cfg」を使用することを推奨します。

管理コンテキスト ファイルは、内部フラッシュ メモリに保存する必要があります。

HTTP または HTTPS サーバからコンテキスト コンフィギュレーションをダウンロードした場合、**copy running-config startup-config** コマンドを使用してこれらのサーバに変更内容を戻して保存することはできません。ただし、**copy tftp** コマンドを使用して実行コンフィギュレーションを TFTP サーバにコピーできます。

システムは、サーバが利用できない、またはファイルがまだ存在しないためにコンテキスト コンフィギュレーション ファイルを取得できない場合、コマンドライン インターフェイスですぐに設定できるブランクのコンテキストを作成します。

URL を変更するには、新しい URL で **config-url** コマンドを再入力します。

ASA は、新しいコンフィギュレーションを現在の実行コンフィギュレーションにマージします。同じ URL を再入力した場合でも、保存されたコンフィギュレーションが実行コンフィギュレーションにマージされます。マージによって、新しいコンフィギュレーションから実行コンフィギュレーションに新しいコマンドが追加されます。コンフィギュレーションが同じ場合、変更は発生しません。コマンドが衝突する場合、またはコマンドがコンテキストの実行に影響を与える場合、マージの結果はコマンドによって異なります。エラーが発生することも、予期できない結果が生じることもあります。実行コンフィギュレーションが空白の場合（たとえば、サーバが使用不可でコンフィギュレーションがダウンロードされなかった場合）は、新しいコンフィギュレーションが使用されます。コンフィギュレーションをマージしない場合は、コンテキストを経由する通信を妨げる実行コンフィギュレーションをクリアしてから、新しい URL からコンフィギュレーションをリロードすることができます。

例

次に、管理コンテキストを「administrator」に設定し、内部フラッシュ メモリに「administrator」というコンテキストを作成してから、FTP サーバから 2 つのコンテキストを追加する例を示します。

```
ciscoasa(config)# admin-context administrator
ciscoasa(config)# context administrator
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url flash:/admin.cfg

ciscoasa(config-ctx)# context test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg

ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
```

関連コマンド

コマンド	説明
allocate-interface	コンテキストにインターフェイスを割り当てます。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。
show context	コンテキストのリスト(システム実行スペース)または現在のコンテキストに関する情報を表示します。

connect fxos

Firepower 1000 または 2100 で ASA CLI から FXOS に接続するには、特権 EXEC モードで **connect fxos** コマンドを入力します。

connect fxos [**admin**]

構文の説明

admin	（オプション）アプライアンスモードの Firepower 1000 または Firepower 2100 では、管理者レベルのアクセスに **admin** を指定します。このオプションを指定しないと、ユーザのアクセス権は読み取り専用アクセスになります。管理者モードであっても、コンフィギュレーション コマンドは使用できないことに注意してください。 このキーワードは、プラットフォームモードの Firepower 2100 では使用できません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.8(2)	このコマンドが追加されました。
9.13(1)	**admin** キーワードが追加されました。

使用上のガイドライン

アプライアンスモードの Firepower 1000 および 2100

Firepower 1000 および 2100 アプライアンス モードのコンソール ポートは、ASA CLI に接続します（FXOS CLI に接続する Firepower 2100 プラットフォーム モードのコンソールとは異なります）。ASA CLI から、トラブルシューティングのために Telnet を使用して FXOS CLI に接続できます。

ユーザはクレデンシャルの入力を求められません。現在の ASA ユーザ名が FXOS に渡されるため、追加のログインは必要ありません。ASA CLI に戻るには、**exit** と入力するか、または **Ctrl-Shift-6**、**x** と入力します。

FXOS 内で、**scope security/show audit-logs** コマンドを使用してユーザアクティビティを表示できます。

プラットフォームモードの Firepower 2100

ASA への接続に SSH または Telnet を使用している場合は、このコマンドを使用して FXOS CLI に接続します。FXOS への認証を求められます。デフォルトのユーザ名：**admin** およびパスワード：**Admin123** を使用します。ASA CLI に戻るには、**exit** と入力するか、または **Ctrl-Shift-6**、**x** と入力します。

初期接続が（コンソール ポートなどでの）FXOS への接続である場合は、**connect asa** コマンドを使用すると、ASA CLI に接続できます。当初の接続 CLI に戻るには、**connect** コマンドは使用できません。接続を終了させる必要があります。

例

次に、アプライアンスモードの Firepower 1000 または 2100 で FXOS CLI に接続する例を示します。

```
ciscoasa# connect fxos admin
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
firepower#
firepower# exit
Connection with FXOS terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

次に、プラットフォームモードの Firepower 2100 で FXOS CLI に接続する例を示します。

```
ciscoasa# connect fxos
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
FXOS 2.2(2.32) kp2110
kp2110 login: admin
Password: Admin123
Last login: Sat Jan 23 16:20:16 UTC 2017 on pts/1
Successful login attempts for user 'admin' : 4
Cisco Firepower Extensible Operating System (FX-OS) Software
[…]
kp2110#
kp2110# exit
Remote card closed command session. Press any key to continue.
Connection with fxos terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

関連コマンド

コマンド	説明
fxos permit	ASA データ インターフェイスでの FXOS 管理アクセスを許可します。
fxos port	FXOS 管理アクセス ポートを設定します。
ip-client	FXOS 管理トラフィックを ASA データ インターフェイスに出力することを許可します。

conn data-rate

負荷の大きいデータを渡すデバイス上の接続を表示するには、特権 EXEC モードで **conn data-rate** コマンドを使用します。このコマンドには、フローごとのデータレートが既存の接続情報とともに表示されます。データレート別に接続の収集をディセーブルにするには、このコマンドの **no** 形式を使用します。

conn data-rate

no conn data-rate

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

この機能はデフォルトで無効に設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.14(1)	このコマンドが追加されました。

使用上のガイドライン

conn data-rate コマンドは、デバイスの全体的な負荷に最も関係している可能性がある接続やユーザを特定する際に最も役立ちます。

イネーブルにすると、conn data-rate 機能によってすべての接続に対し次の 2 つの統計情報が追跡されます。

- 接続の順方向および逆方向の現在の(1 秒)データレート。
- 接続の順方向および逆方向の最大(1 秒)データレート。

例

次の例では、接続データレート収集をイネーブルにする方法について示します。

```
ciscoasa(config)#conn data-rate
ciscoasa(config)#
```

関連コマンド

コマンド	説明
show conn data-rate	接続データレートトラッキングの現在の状態を表示します。
show conn detail	データレート値によってフィルタ処理された接続を表示します。
clear conn data-rate	現在の最大データレート値をクリアします。

conn-rebalance

クラスタのメンバー間の接続再分散をイネーブルにするには、クラスタ グループ コンフィギュレーション モードで **conn-rebalance** コマンドを使用します。接続再分散をディセーブルにするには、このコマンドの **no** 形式を使用します。

conn-rebalance [**frequency** *seconds*]

no conn-rebalance [**frequency** *seconds*]

構文の説明

frequency *seconds*	（任意）負荷情報を交換する間隔を 1 ～ 360 秒の範囲内で指定します。デフォルトは 5 秒です。

コマンド デフォルト

接続再分散は、デフォルトではディセーブルです。

イネーブルの場合、デフォルトの頻度は、5 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラスタ グループ コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

アップストリームまたはダウンストリーム ルータによるロード バランシングの結果として、フロー分散に偏りが生じた場合は、新しいフローを過負荷のユニットから他のユニットにリダイレクトするように設定できます。既存のフローは他のユニットには移動されません。イネーブルの場合は、ASA は負荷情報を定期的に交換し、新しい接続の負荷を高負荷のデバイスから低負荷のデバイスに移動します。

このコマンドは、ブートストラップ コンフィギュレーションの一部ではなく、マスター ユニットからスレーブ ユニットに複製されます。

例

次に、接続再分散の頻度を 60 秒に設定する例を示します。

```
ciscoasa(cfg-cluster)# conn-rebalance frequency 60
```

関連コマンド

コマンド	説明
clacp system-mac	スパンド EtherChannel を使用するときは、ASA は cLACP を使用してネイバー スイッチとの間で EtherChannel のネゴシエーションを行います。
cluster group	クラスタに名前を付け、クラスタ コンフィギュレーション モードを開始します。
cluster-interface	クラスタ制御リンク インターフェイスを指定します。
cluster interface-mode	クラスタ インターフェイス モードを設定します。
console-replicate	スレーブ ユニットからマスター ユニットへのコンソール複製をイネーブルにします。
enable(クラスタ グループ)	クラスタリングをイネーブルにします。
health-check	クラスタのヘルス チェック機能(ユニットのヘルス モニタリングおよびインターフェイスのヘルス モニタリングを含む)をイネーブルにします。
key	クラスタ制御リンクの制御トラフィックの認証キーを設定します。
local-unit	クラスタ メンバーに名前を付けます。
mtu cluster-interface	クラスタ制御リンク インターフェイスの最大伝送ユニットを指定します。
priority(クラスタ グループ)	マスター ユニット選定のこのユニットのプライオリティを設定します。

console-replicate

ASA クラスタ内でスレーブ ユニットからマスター ユニットへのコンソール複製をイネーブルにするには、クラスタ グループ コンフィギュレーション モードで **console-replicate** コマンドを使用します。コンソール複製をディセーブルにするには、このコマンドの **no** 形式を使用します。

console-replicate

no console-replicate

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

コンソール複製はデフォルトでディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラスタ グループ コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASA は、特定の重大イベントが発生したときに、メッセージを直接コンソールに出力します。コンソール複製をイネーブルにすると、スレーブ ユニットからマスター ユニットにコンソール メッセージが送信されるので、モニタが必要になるのはクラスタのコンソール ポート 1 つだけとなります。

このコマンドは、ブートストラップ コンフィギュレーションの一部ではなく、マスター ユニットからスレーブ ユニットに複製されます。

例

次に、コンソール複製をイネーブルにする例を示します。

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# console-replicate
```

関連コマンド

コマンド	説明
clacp system-mac	スパンド EtherChannel を使用するときは、ASA は cLACP を使用してネイバー スイッチとの間で EtherChannel のネゴシエーションを行います。
cluster group	クラスタに名前を付け、クラスタ コンフィギュレーション モードを開始します。
cluster-interface	クラスタ制御リンク インターフェイスを指定します。
cluster interface-mode	クラスタ インターフェイス モードを設定します。
conn-rebalance	接続の再分散をイネーブルにします。
enable(クラスタ グループ)	クラスタリングをイネーブルにします。
health-check	クラスタのヘルス チェック機能(ユニットのヘルス モニタリングおよびインターフェイスのヘルス モニタリングを含む)をイネーブルにします。
key	クラスタ制御リンクの制御トラフィックの認証キーを設定します。
local-unit	クラスタ メンバーに名前を付けます。
mtu cluster-interface	クラスタ制御リンク インターフェイスの最大伝送ユニットを指定します。
priority(クラスタ グループ)	マスター ユニット選定のこのユニットのプライオリティを設定します。

console timeout

認証済みシリアル コンソール セッション（**aaa authentication serial console**）に対する非アクティブ タイムアウトを設定して、タイムアウト後にユーザがコンソールからログアウトされるようにするには、または認証済みイネーブル セッション（**aaa authentication serial console**）に対する非アクティブ タイムアウトを設定して、タイムアウト後にユーザが特権 EXEC モードを終了し、ユーザ EXEC モードに戻るようにするには、グローバル コンフィギュレーション モードで **console timeout** コマンドを使用します。認証済みシリアル コンソール セッションに対する非アクティブ タイムアウトをディセーブルにするには、このコマンドの **no** 形式を使用します。

console timeout [*number*]

no console timeout [*number*]

構文の説明

number	コンソール セッションが終了するまでのアイドル時間を分単位（0 ～ 60）で指定します。0 はコンソールがタイムアウトしないことを意味します。

デフォルト

デフォルトのタイムアウトは 0 であり、コンソール セッションがタイムアウトしないことを示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

console timeout コマンドは、認証済みのシリアル接続またはイネーブル接続だけに適用されます。このコマンドは、Telnet、SSH、または HTTP のタイムアウトを変更しません。これらのアクセス方式では、独自のタイムアウト値が維持されます。このコマンドは、認証されていないコンソール接続には影響しません。

no console timeout コマンドは、コンソール タイムアウト値をデフォルトのタイムアウトである 0 にリセットします。この値は、コンソールがタイムアウトしないことを意味します。

例

次に、コンソール タイムアウトを 15 分に設定する例を示します。

```
ciscoasa(config)# console timeout 15
```

関連コマンド

コマンド	説明
clear configure console	デフォルトのコンソール接続設定に戻します。
clear configure timeout	コンフィギュレーションのアイドル時間継続時間をデフォルトに戻します。
show running-config console timeout	ASA に対するコンソール接続のアイドル タイムアウトを表示します。

content-length

HTTP メッセージ本文の長さに基づいて HTTP トラフィックを制限するには、HTTP マップ コンフィギュレーション モードで **content-length** コマンドを使用します。このコマンドを削除するには、このコマンドの **no** 形式を使用します。

content-length { **min** *bytes* [**max** *bytes*] | **max** *bytes*] } **action** {**allow** | **reset** | **drop**} [**log**]

no content-length { **min** *bytes* [**max** *bytes*] | **max** *bytes*] } **action** {**allow** | **reset** | **drop**} [**log**]

構文の説明

action	メッセージがこのインスペクションに合格しなかったときに実行するアクションを指定します。
allow	メッセージを許可します。
bytes	バイト数を指定します。許容される範囲は、**min** オプションでは 1 ～ 65535、**max** オプションでは 1 ～ 50000000 です。
drop	接続を閉じます。
max	（任意）syslog を生成します。
max	（任意）許容される内容の最大長を指定します。
min	（任意）許容される内容の最小長を指定します。
reset	TCP リセット メッセージをクライアントおよびサーバに送信します。

デフォルト

デフォルトでは、このコマンドはディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
HTTP マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

content-length コマンドをイネーブルにすると、ASA は、設定された範囲内のメッセージだけを許可し、範囲外の場合は指定されたアクションを実行します。ASA に TCP 接続をリセットさせて、Syslog エントリを作成させるには、**action** キーワードを使用します。

例

次に、HTTP トラフィックを 100 バイト以上 2000 バイト以下のメッセージに制限する例を示します。メッセージがこの範囲外の場合、ASA は TCP 接続をリセットし、syslog エントリを作成します。

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# content-length min 100 max 2000 action reset log
ciscoasa(config-http-map)# exit
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
http-map	拡張 HTTP インスペクションを設定するための HTTP マップを定義します。
debug appfw	拡張 HTTP インスペクションに関連するトラフィックの詳細情報を表示します。
inspect http	アプリケーション インスペクション用に特定の HTTP マップを適用します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

context

システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **context** コマンドを使用します。コンテキストを削除するには、このコマンドの **no** 形式を使用します。

context *name*

no context *name* [**noconfirm**]

構文の説明

name	名前を最大 32 文字のストリングで設定します。この名前では大文字と小文字が区別されるため、たとえば、「customerA」および「CustomerA」という 2 つのコンテキストを保持できます。文字、数字、またはハイフンを使用できますが、名前の先頭または末尾にハイフンは使用できません。 「System」および「Null」（大文字と小文字の両方）は予約されている名前であり、使用できません。
noconfirm	（任意）確認を求めるプロンプトを表示せずにコンテキストを削除します。このオプションは自動スクリプトで役立ちます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

コンテキスト コンフィギュレーション モードでは、コンテキストで使用できる、コンフィギュレーション ファイルの URL とインターフェイスを指定できます。管理コンテキストがない場合（たとえば、コンフィギュレーションをクリアした場合）、追加する最初のコンテキストは管理コンテキストである必要があります。管理コンテキストを追加するには、**admin-context** コマンドを参照してください。管理コンテキストを指定した後、**context** コマンドを入力して管理コンテキストを設定します。

コンテキストは、システム コンフィギュレーションを編集することによってのみ削除できます。現在の管理コンテキストはこのコマンドの **no** 形式を使用して削除することはできません。**clear configure context** コマンドを使用してすべてのコンテキストを削除した場合にのみ削除できます。

例

次に、管理コンテキストを「administrator」に設定し、内部フラッシュ メモリに「administrator」というコンテキストを作成してから、FTP サーバから 2 つのコンテキストを追加する例を示します。

```
ciscoasa(config)# admin-context administrator
ciscoasa(config)# context administrator
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url flash:/admin.cfg

ciscoasa(config-ctx)# context test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg

ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
```

関連コマンド

コマンド	説明
allocate-interface	コンテキストにインターフェイスを割り当てます。
changeto	コンテキストとシステム実行スペースの間を切り替えます。
config-url	コンテキスト コンフィギュレーションの場所を指定します。
join-failover-group	コンテキストをフェールオーバー グループに割り当てます。
show context	コンテキスト情報を表示します。

copy

ファイルを ASA フラッシュ メモリとの間でコピーするには、特権 EXEC モードで **copy** コマンドを使用します。

copy [**/noconfirm** | **/noverify**] [**/pcap**] [*interface_name*] {*url* | **running-config** | **startup-config**} {**running-config** | **startup-config** | *url*}

構文の説明

/noconfirm	(オプション)確認のプロンプトを表示しないでファイルをコピーします。
interface_name	(任意)ファイルをコピーするインターフェイス名を指定します。インターフェイスを指定しなかった場合、ASA は管理専用ルーティング テーブルを確認し、一致するものが見つからなければ、データのルーティング テーブルを確認します。
/pcap	(オプション)**capture** コマンドの未加工のパケット キャプチャ ダンプを指定します。
/noverify	(オプション)開発キー署名済みイメージをコピーするときに署名検証をスキップします。
running-config	システム メモリに格納されている実行コンフィギュレーションを指定します。
startup-config	フラッシュ メモリに格納されているスタートアップ コンフィギュレーションを指定します。シングル モードのスタートアップ コンフィギュレーション、またはマルチ コンテキスト モードのシステムのスタートアップ コンフィギュレーションは、フラッシュ メモリ内の非表示のファイルです。スタートアップ コンフィギュレーションの場所は、コンテキスト内から **config-url** コマンドで指定します。たとえば、**config-url** コマンドで HTTP サーバを指定し、**copy startup-config running-config** コマンドを入力した場合、ASA は管理コンテキスト インターフェイスを使用して、HTTP サーバからスタートアップ コンフィギュレーションをコピーします。

url	ローカル ロケーションとリモート ロケーション間でコピーするコピー元ファイルまたは宛先ファイルを指定します。(リモート サーバから別のリモート サーバにコピーできません)。コンテキスト内では、コンテキスト インターフェイスを使用して、実行コンフィギュレーションまたはスタートアップ コンフィギュレーションを TFTP サーバまたは FTP サーバにコピーできますが、サーバから実行コンフィギュレーションまたはスタートアップ コンフィギュレーションにコピーすることはできません。他のオプションについては、**startup-config** キーワードを参照してください。TFTP サーバから実行コンテキスト コンフィギュレーションにダウンロードするには、**configure net** コマンドを使用します。一部の URL は、送信元または宛先としてのみ使用できます。正確な使い方については、CLI ヘルプを参照してください。このコマンドでは、次の URL 構文を使用します。 • **cache:/**[[*path*/]*filename*]:ファイル システム内のキャッシュ メモリを示します。 • **capture:/**[[*context_name*/]*buffer_name*]:キャプチャ バッファ内の出力を示します。 • **cluster_trace**:クラスタ トレース ファイル システムを示します。 • **cluster:/**[[*path*/]*filename*]:クラスタ ファイル システムを示します。 • **disk0:/**[[*path*/]*filename*] または **flash:/**[[*path*/]*filename*]:**flash** と **disk0** の両方が内部フラッシュ メモリを示します。いずれのオプションも使用できます。 • **disk1:/**[[*path*/]*filename*]:外部メモリを示します。 • **smb:/**[[*path*/]*filename*]:UNIX サーバのローカル ファイル システムを示します。サーバ メッセージ ブロック ファイル システム プロトコルは、データをパッケージ化し、他のシステムと情報を交換するために、LAN マネージャおよび類似のネットワーク システムで使用されます。 • **ftp://**[[*user*[**:***password*]@]*server*[:*port*]**/**[*path*/]*filename*[**;type=***xx*]]:**type** は次のいずれかのキーワードになります。**ap**(ASCII パッシブ モード)、**an**(ASCII 通常モード)、**ip**(デフォルト:バイナリ パッシブ モード)、**in**(バイナリ通常モード)。 • **http**[**s**]**://**[[*user*[**:***password*]@]*server*[**:***port*]**/**[*path*/]*filename*] • **scp://**[[*user*[**:***password*]@]*server*[**/***path*]**/***filename*[**;int=***interface_name*]]:**;int=***interface* オプションはルート ルックアップをバイパスし、常に指定したインターフェイスを使用してセキュア コピー(SCP)サーバに到達します。 • **system:/**[[*path*/]*filename*]:システム メモリを表します。 • **system:text**:主要な ASA プロセスを分析用に ASA からコピーできるテキストとして表します。 • **tftp://**[[*user*[**:***password*]@]*server*[**:***port*]**/**[*path*/]*filename*[**;int=***interface_name*]] パス名にスペースを含めることはできません。パス名がスペースを含む場合は、**copy tftp** コマンドの代わりに **tftp-server** コマンドでパスを設定します。**;int=***interface* オプションは、ルート ルックアップをバイパスし、常に指定したインターフェイスを使用して TFTP サーバに到達します。

デフォルト　デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応[1]	• 対応

1. コンテキスト内では、実行コンフィギュレーションまたはスタートアップ コンフィギュレーションのみを外部 URL にコピーできます。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	DNS 名のサポートが追加されました。
8.0(2)	**smb** オプションが追加されました。
9.1(5)	**scp** オプションが追加されました。
9.3(2)	**/noverify** オプションが追加されました。
9.5(1)	*interface_name* 引数が追加されました。
9.6(2)	**system:text** キーワードが追加されました。

使用上のガイドライン

- コンフィギュレーションを実行コンフィギュレーションにコピーするには、2 つのコンフィギュレーションをマージします。マージによって、新しいコンフィギュレーションから実行コンフィギュレーションに新しいコマンドが追加されます。コンフィギュレーションが同じ場合、変更は発生しません。コマンドが衝突する場合、またはコマンドがコンテキストの実行に影響を与える場合、マージの結果はコマンドによって異なります。エラーが発生することも、予期できない結果が生じることもあります。
- RSA キーを NVRAM に保存できない場合は、次のエラー メッセージが表示されます。

  ```
  ERROR: NV RAM does not have enough space to save keypair keypair name
  ```

- クラスタ全体のキャプチャを実行後、マスター ユニットで次のコマンドを入力して、クラスタ内のすべてのユニットから同じキャプチャ ファイルを TFTP サーバに同時にコピーできます。

  ```
  hostname (config-cluster)# cluster exec copy /pcap capture: cap_name
  tftp://location/path/filename.pcap
  ```

  複数の PCAP ファイル(各ユニットから 1 つずつ)が TFTP サーバにコピーされます。宛先のキャプチャ ファイル名には自動的にユニット名が付加され、filename_A.pcap、filename_B.pcap などとなります。ここで、A および B はクラスタ ユニット名です。

  (注) ファイル名の末尾にユニット名を追加すると、別の宛先名が生成されます。

  パケットキャプチャをディスクにコピーすることもできます。ただし、コピー操作が成功するためには、キャプチャ名を 63 文字未満にしてください。

- インターフェイスを指定しなかった場合、ASA は管理専用ルーティング テーブルを確認し、一致するものが見つからなければ、データのルーティング テーブルを確認します。管理専用インターフェイスを経由するデフォルト ルートがある場合は、すべての **copy** トラフィックがそのルートに一致するため、データ ルーティング テーブルを確認することはありません。このシナリオでは、データ インターフェイスからコピーする必要がある場合にそのインターフェイスを指定します。

例

次に、システム実行スペースでファイルをディスクから TFTP サーバにコピーする例を示します。

```
ciscoasa(config)# copy disk0:my_context/my_context.cfg
tftp://10.7.0.80/my_context/my_context.cfg
```

次に、ファイルをディスク上のある場所からディスク上の別の場所にコピーする例を示します。宛先ファイルの名前は、コピー元のファイルの名前にすることも、別の名前にすることもできます。

```
ciscoasa(config)# copy disk0:my_context.cfg disk:my_context/my_context.cfg
```

次に、ASDM ファイルを TFTP サーバから内部フラッシュ メモリにコピーする例を示します。

```
ciscoasa(config)# copy tftp://10.7.0.80/asdm700.bin disk0:asdm700.bin
```

次に、コンテキスト内の実行コンフィギュレーションを TFTP サーバにコピーする例を示します。

```
ciscoasa(config)# copy running-config tftp://10.7.0.80/my_context/my_context.cfg
```

copy コマンドでは、IP アドレス（上の例の場合）だけでなく、次に示すように DNS 名もサポートされています。

```
ciscoasa(config)# copy running-config tftp://www.example.com/my_context/my_context.cfg
```

次に、フル パスを指定せずに **copy capture** コマンドを入力した場合に表示されるプロンプトの例を示します。

```
ciscoasa(config)# copy capture:abc tftp
Address or name of remote host [209.165.200.224]?
Source file name [username/cdisk]?
copying capture to tftp://209.165.200.224/username/cdisk:
[yes|no|again]? y
!!!!!!!!!!!!!
```

次のようにフル パスを指定できます。

```
ciscoasa(config)# copy capture:abc tftp:209.165.200.224/tftpboot/abc.cap
```

TFTP サーバをすでに設定している場合は、次のようにファイルの位置や名前を省略できます。

```
ciscoasa(config)# tftp-server outside 209.165.200.224 tftp/cdisk
ciscoasa(config)# copy capture:abc tftp:/tftp/abc.cap
```

次に、開発キー署名済みイメージを検証せずにコピーする例を示します。

```
ciscoasa(config)# copy /noverify lfbff.SSA exa_lfbff.SSA

Source filename [lfbff.SSA]?

Destination filename [exa_lfbff.SSA]?

Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Writing file disk0:/exa_lfbff.SSA...
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Digital Signature was not verified
124125968 bytes copied in 61.740 secs (2034851 bytes/sec)
```

関連コマンド

コマンド	説明
configure net	ファイルを TFTP サーバから実行コンフィギュレーションにコピーします。
copy capture	キャプチャ ファイルを TFTP サーバにコピーします。
tftp-server	デフォルトの TFTP サーバを設定します。
write memory	実行中の設定をスタートアップ コンフィギュレーションに保存します。
write net	実行コンフィギュレーションを TFTP サーバにコピーします。

cpu hog granular-detection

リアルタイムの占有検出を行い、短期間での CPU 占有しきい値を設定するには、特権 EXEC モードで **cpu hog granular-detection** コマンドを使用します。

cpu hog granular-detection [**count** *number*] [**threshold** *value*]

構文の説明

count *number*	実行されるコード実行割り込みの数を指定します。有効な値は、1 ～ 10000000 です。デフォルト値および推奨値は 1000 です。
threshold *value*	範囲は 1 ～ 100 です。設定されていない場合はデフォルトが使用されます。デフォルトはプラットフォームによって異なります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

cpu hog granular-detection コマンドでは、現在のコード実行に 10 ミリ秒ごとに割り込み、割り込みの総数がカウントされます。割り込みによって CPU 占有がチェックされます。存在する場合は、ログに記録されます。このコマンドによって、データ パスでの CPU 占有検出の精度が低下します。

各スケジューラ ベースの占有は、最大 5 つの割り込みベースの占有エントリに関連付けられます。各エントリには最大 3 つのトレースバックが含まれる場合があります。割り込みベースの占有は上書きできません。空き領域がない場合は、新しい占有が廃棄されます。スケジューラ ベースの占有は、LRU ポリシーに従って引き続き再利用され、関連付けられている割り込みベースの占有はそのときにクリアされます。

(注) UDP パケットが小さい ASA 5585-X では、パフォーマンスが影響を受ける可能性があります。

例

次に、CPU 占有検出をトリガーする例を示します。

```
ciscoasa# cpu hog granular-detection count 1000 threshold 10
Average time spent on 1000 detections is 10 seconds, and it may take longer
under heavy traffic.
Please leave time for it to finish and use show process cpu-hog to check results.
```

関連コマンド

コマンド	説明
show process cpu-hog	CPU を占有しているプロセスを表示します。
clear process cpu-hog	CPU を占有しているプロセスをクリアします。

cpu profile activate

CPU プロファイリングを開始するには、特権 EXEC モードで **cpu profile activate** コマンドを使用します。

cpu profile activate *n-samples* [**sample-process** *process-name*] [**trigger cpu-usage** *cpu %* [*process-name*]]

構文の説明

n-samples	サンプル数 *n* を保存するためのメモリを割り当てます。有効値は 1 ～ 100,000 です。
sample-process *process-name*	特定のプロセスのみをサンプリングします。
trigger cpu-usage *cpu %*	グローバルな CPU 使用率である 5 秒を超えるまでプロファイラを開始しないようにし、CPU 使用率がこの値を下回った場合はプロファイラを停止します。
trigger cpu-usage *cpu % process-name*	CPU 使用率が 5 秒のプロセスをトリガーとして使用します。

デフォルト

n-samples のデフォルト値は 1000 です。

cpu % のデフォルト値は 0 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.1(2)	**sample-process** *process-name*、**trigger cpu-usage** *cpu %*、および **trigger cpu-usage** *cpu % process-name* オプションが追加されました。出力形式が更新されました。

使用上のガイドライン

CPU プロファイラは、CPU 使用率が高いプロセスの特定に役立ちます。CPU のプロファイリングでは、タイマー割り込みが発生したときに CPU で動作していたプロセスのアドレスをキャプチャします。このプロファイリングは、CPU の負荷に関係なく、10 ミリ秒ごとに発生します。たとえば、5000 のサンプルを取得する場合、プロファイリングが完了するまで正確に 50 秒かかります。CPU プロファイラが使用する CPU 時間が比較的少ない場合は、サンプルの収集に時間がかかります。CPU プロファイル レコードは、別のバッファでサンプリングされます。

show cpu profile コマンドを **cpu profile activate** コマンドとともに使用して、ユーザが収集できる情報、および TAC が CPU の問題のトラブルシューティングに使用できる情報を表示します。**show cpu profile dump** コマンドの出力は、16 進形式です。

CPU プロファイラが開始条件の発生を待機している場合、**show cpu profile** コマンドは次の出力を表示します。

```
CPU profiling started: 12:45:57.209 UTC Wed Nov 14 2012
CPU Profiling waiting on starting condition.
Core 0: 0 out of 10 samples collected.
Core 1: 0 out of 10 samples collected.
Core 2: 0 out of 10 samples collected.
Core 3: 0 out of 10 samples collected.
CP
0 out of 10 samples collected.
```

例

次の例では、プロファイラをアクティブ化して、1000 個のサンプルを格納するように指示します。

```
hostname# cpu profile activate
Activated CPU profiling for 1000 samples.
Use "show cpu profile" to display the progress or "show cpu profile dump"
to interrupt profiling and display the incomplete results.
```

次に、プロファイリングのステータス（進行中および完了済み）を表示する例を示します。

```
hostname# show cpu profile
CPU profiling started: 13:45:10.400 PST Fri Nov 16 2012
CPU profiling currently in progress:
Core 0: 209 out of 1000 samples collected.
Use "show cpu profile dump" to see the results after it is complete
or to interrupt profiling and display the incomplete results.

hostname# show cpu profile dump
Cisco Adaptive Security Appliance Software Version 9.1(2)
Hardware:   ASA5555
CPU profiling started: 09:13:32.079 UTC Wed Jan 30 2013
No CPU profiling process specified.
No CPU profiling trigger specified.
cores: 2

Process virtual address map:
----------------------------
…
----------------------------
End of process map
Samples for core 0 - stopped
{0x00000000007eadb6,0x000000000211ee7e} ...
```

関連コマンド

コマンド	説明
show cpu profile	CPU プロファイリングの進行状況を表示します。
show cpu profile dump	プロファイリングに関して、完了していない結果または完了した結果を表示します。

coredump enable

コアダンプ機能をイネーブルにするには、**coredump enable** コマンドを入力します。このコマンドをディセーブルにするには、このコマンドの **no** 形式を使用します。

coredump enable [**filesystem disk***n***:** [**size** [**default** | *size*]]

no coredump enable [**filesystem disk***n***:** [**size** [**default** | *size*]]

構文の説明

default	ASA で必要な値が計算されるため、このデフォルト値の使用が推奨されることを指定します。
filesystem disk*n***:**	コアダンプ ファイルが保存されるディスクを指定します。
size	ASA のフラッシュ上のコアダンプ ファイル システム イメージに割り当てる合計サイズを定義します。コアダンプを設定するとき、十分な領域が使用可能でない場合は、エラー メッセージが表示されます。**size** オプションをコンテナとして考えると役立ちます。つまり、生成されたコアダンプではこのサイズを超えてディスク領域を消費できません。
size	ASA がデフォルト値を上書きし、コアダンプ ファイル システムの指定された値（MB 単位）を割り当てることを指定します（領域が使用可能な場合）。

デフォルト

デフォルトでは、コアダンプはイネーブルではありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

(注) 4100/9300 プラットフォームで動作している ASA の場合は、ブートストラップ CLI モードを使用してコアダンプを処理します。

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

この機能をイネーブルにすると、重要なトラブルシューティング情報が提供されます。この機能をディセーブルにすると、システムのクラッシュ時にすべてのコンポーネントのコアダンプ ファイルが生成されなくなります。また、この機能をディセーブルにしても、前のコアダンプ ファイル システム イメージやコアダンプ ファイル システム イメージの内容は削除されません。コアダンプをイネーブルにすると、コアダンプ ファイル システムの作成を許可するように求めるプロンプトが表示されます。このプロンプトは確認であり、作成されるコアダンプ ファイル システムのサイズ(MB 単位)が含まれます。コアダンプをイネーブルまたはディセーブルにした後に、コンフィギュレーションを保存することが重要です。

コアダンプを有効にする前に、ASA デバイスで現在使用可能なディスク領域を認識しておく必要があります。ASA に十分なディスク領域がある場合にのみ、コアダンプを有効にします。コアダンプに割り当てられているディスク領域の容量は、現在 ASA プラットフォームとその標準メモリの次のような構成に基づいています。

- ASA5505、ASA5510、ASA552 の場合は 60 MB
- ASA5540 の場合は 100 MB
- ASA5550、ASA5580 の場合は 200 MB
- ASA5585 の場合は 300 MB

デフォルトのコアダンプが大きすぎて使用可能なフラッシュメモリに保存できない場合、ASA はエラーをスローします。

コアダンプをイネーブルにすると、次のファイル要素が作成されます。これらのファイル要素を明示的に操作しないでください。

- coredumpfsys:コアダンプ イメージが含まれるディレクトリ
- coredumpfsysimage.bin:コアダンプの管理に使用されるコアダンプ ファイル システム イメージ
- coredumpinfo:コアダンプ ログが含まれるディレクトリ

(注) コアダンプをディセーブルにしても、crashinfo ファイルの生成には影響がありません。

ASA でのアプリケーションまたはシステムのクラッシュをトラブルシューティングするために、コアダンプ機能をイネーブルにすることを Cisco TAC が依頼する場合があります。

(注) 後続のコアダンプで、現在のコアダンプを格納するために前のコアダンプが削除される場合があるため、コアダンプ ファイルを必ずアーカイブしてください。コアダンプ ファイルは、設定されたファイル システム(たとえば、「disk0:/coredumpfsys」や「disk1:/coredumpfsys」)に配置され、ASA から削除できます。

コアダンプをイネーブルにするには、次の手順を実行します。

1. **/** ルート ディレクトリになっていることを確認します。コンソールのディレクトリの場所を確認するには、**pwd** コマンドを入力します。
2. 必要に応じて、**cd disk0:/** または **cd disk1:/** コマンドを入力して、ディレクトリを変更します。
3. **coredump enable** コマンドを入力します。

coredump コマンドを使用して ASA 上のクラッシュをトラブルシューティングするときに、クラッシュ後にコアダンプ ファイルが保存されないことがあります。このことは、コアダンプ機能がイネーブルになっており、かつ事前に割り当てられたディスク領域を使用してコアダンプ ファイル システムが作成されている場合に発生する可能性があります。この状態は、通常、数週間ビジーな状態が継続した ASA で大量の RAM が割り当てられ、その後に発生したクラッシュをトラブルシューティングする場合に発生します。

show coredump コマンドの出力に、次のような内容が示されます。

```
Coredump Aborted as the complete coredump could not be written to flash
Filesystem full on 'disk0', current coredump size <size> bytes too big
   for allocated filesystem
```

この問題の発生を抑制するには、フル メモリを格納できるだけの十分な容量があるコアダンプ ファイル システム カードを使用し、対応する領域をコアダンプ ファイル システムに割り当てる必要があります。

例

次の例の各！は、書き込まれる 1 MB のコアダンプ ファイル システムを表しています。

次に、デフォルト値および **disk0:** を使用して、コアダンプ ファイル システムを作成する例を示します。

```
hostname(config)# coredump enable
Warning: Enabling coredump on an ASA5505 platform will delay the
reload of the system in the event of software forced reload.
The exact time depends on the size of the coredump generated.
Proceed with coredump filesystem allocation of 60 MB on 'disk0:'
(Note this may take a while) [confirm]
Making coredump file system
image!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

次に、**disk1:** 上に 120 MB のコアダンプ ファイル システムを作成して、ファイル システムおよびサイズを指定する例を示します。

```
hostname(config)# coredump enable filesystem disk1: size 120
WARNING: Enabling coredump on an ASA5540 platform will delay
the reload of the system in the event of software forced reload.
The exact time depends on the size of the coredump generated.
Proceed with coredump filesystem allocation of 120 MB
on 'disk1:' (Note this may take a while) ? [confirm]
Making coredump file system image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

次に、コアダンプ ファイル システムのサイズを 120 MB から 100 MB に変更する例を示します。

(注) 120 MB のコアダンプ ファイル システムの内容は保持されないため、変更する前に、前のコアダンプを必ずアーカイブしてください。

```
hostname(config)# coredump enable filesystem disk1: size 100
WARNING: Enabling coredump on an ASA5540 platform will delay
the reload of the system in the event of software forced reload.
The exact time depends on the size of the coredump generated.
Proceeding with resizing to 100 MB results in
deletion of current 120 MB coredump filesystem and
its contents on 'disk1:', proceed ? [confirm]
Making coredump file system
image!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
```

次に、**disk0:** 上で最初にコアダンプをイネーブルにし、次に **disk1:** 上でイネーブルにする例を示します。**default** キーワードを使用していることにも注意してください。

(注) 2 つのアクティブなコアダンプ ファイル システムは許可されないため、先に進む前に、前のコアダンプ ファイル システムを削除する必要があります。

```
hostname(config)# coredump enable filesystem disk1: size default
WARNING: Enabling coredump on an ASA5540 platform will delay
the reload of the system in the event of software forced reload.
The exact time depends on the size of the coredump generated.
Coredump is currently configured on 'disk0:', upon successful
configuration on 'disk1:', the coredump filesystem will be
deleted on 'disk0:', proceed ? [confirm]
Proceed with coredump filesystem allocation of 100 MB
on 'disk1:' (Note this may take a while) ? [confirm]
Making coredump file system
image!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!
```

次に、コアダンプ ファイル システムをディセーブルにする例を示します。ただし、現在のコアダンプ ファイル システム イメージおよびその内容は影響を受けません。

```
hostname(config)# no coredump enable
```

コアダンプを再度イネーブルにするには、コアダンプ ファイル システムを設定するために最初に使用したコマンドを再入力します。

次に、コアダンプをディセーブルにし、再度イネーブルにする例を示します。

- デフォルト値を使用する場合:

```
hostname(config)# coredump enable
hostname(config)# no coredump enable
hostname(config)# coredump enable
```

- 明示的な値を使用する場合:

```
hostname(config)# coredump enable filesystem disk1: size 200
hostname(config)# no coredump enable
hostname(config)# coredump enable filesystem disk1: size 200
```

関連コマンド

コマンド	説明
clear configure coredump	コアダンプ ファイル システムとその内容をシステムから削除します。コアダンプ ログもクリアします。
clear coredump	コアダンプ ファイルシステムに現在保存されているコアダンプをすべて削除し、コアダンプ ログをクリアします。
show coredump filesystem	コアダンプ ファイル システムのファイルを表示し、その使用率を示します。
show coredump log	コアダンプ ログを表示します。

crashinfo console disable

コンソールへのクラッシュ情報の出力を抑制するには、グローバル コンフィギュレーション モードで **crashinfo console disable** コマンドを使用します。

crashinfo console disable

no crashinfo console disable

構文の説明

disable	クラッシュが発生した場合にコンソール出力を抑制します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、コンソールへのクラッシュ情報の出力を抑制できます。クラッシュ情報には、デバイスに接続しているすべてのユーザに表示するのは適切でない機密情報が含まれている場合があります。このコマンドとともに、クラッシュ情報がフラッシュに書き込まれていることも確認する必要があります。これはデバイスのリブート後に確認できます。このコマンドは、クラッシュ情報および checkheaps の出力に影響を与えます。この出力はフラッシュに保存され、トラブルシューティングに十分に役立ちます。

例

次に、コンソールへのクラッシュ情報の出力を抑制する例を示します。

```
hostname(config)# crashinfo console disable
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に保存されているシステムまたはモジュールの FIPS コンフィギュレーション情報をクリアします。
fips enable	システムまたはモジュールで FIPS 準拠を強制するためのポリシー チェックをイネーブルまたはディセーブルにします。
fips self-test poweron	電源投入時自己診断テストを実行します。
show crashinfo console	フラッシュへのクラッシュ情報出力の読み取り、書き込み、および設定を行います。
show running-config fips	ASA で実行されている FIPS コンフィギュレーションを表示します。

crashinfo force

ASA を強制的にクラッシュするには、特権 EXEC モードで **crashinfo force** コマンドを使用します。

crashinfo force [**page-fault** | **watchdog** | **dump** [**process** *name*]]

構文の説明

page-fault	（任意）ページ フォールトを利用して、ASA を強制的にクラッシュさせます。
watchdog	（任意）ウォッチドッグを利用して、ASA を強制的にクラッシュさせます。
dump	（任意）主要な ASA プロセス（「lina」）コア ダンプを収集し、システムをクラッシュします。
process *name*	（任意）指定されたプロセス コア ダンプを収集し、システムをクラッシュします。使用可能なプロセスを表示するには、**show kernel process** コマンドを使用します。特定のプロセスが強制終了不能なプロセスである場合、ASA は適切なエラー メッセージを発行し、そのプロセスを強制終了しません。

デフォルト

デフォルトでは、ASA はフラッシュ メモリにクラッシュ情報ファイルを保存します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

crashinfo force コマンドを使用して、クラッシュ出力の生成をテストできます。クラッシュ出力では、本物のクラッシュを、**crashinfo force page-fault** コマンドまたは **crashinfo force watchdog** コマンドによって発生したクラッシュと区別できません。これは、これらのコマンドによって実際にクラッシュが発生しているためです。ASA は、クラッシュのダンプが完了するとリロードします。

注意 実働環境では **crashinfo force** コマンドを使用しないでください。**crashinfo force** コマンドは ASA をクラッシュさせて、強制的にリロードを実行します。

例

次に、**crashinfo force page-fault** コマンドを入力したときに表示される警告の例を示します。

```
ciscoasa# crashinfo force page-fault
WARNING: This command will force the XXX to crash and reboot.
    Do you wish to proceed? [confirm]:
```

キーボードの Return キーまたは Enter キーを押して復帰改行を入力するか、"Y" または "y" を入力すると、ASA がクラッシュしてリロードが実行されます。これらのすべての応答は、確認として解釈されます。その他の文字はすべて no と解釈され、ASA はコマンドライン プロンプトに戻ります。

関連コマンド

clear crashinfo	クラッシュ情報ファイルの内容をクリアします。
crashinfo save disable	クラッシュ情報のフラッシュ メモリへの書き込みをディセーブルにします。
crashinfo test	ASA でフラッシュ メモリ内のファイルにクラッシュ情報を保存できるかどうかをテストします。
show crashinfo	クラッシュ情報ファイルの内容を表示します。

crashinfo save disable

フラッシュ メモリへのクラッシュ情報の書き込みをディセーブルにするには、グローバル コンフィギュレーション モードで **crashinfo save** コマンドを使用します。フラッシュ メモリへのクラッシュ情報の書き込みを許可し、デフォルトの動作に戻すには、このコマンドの **no** 形式を使用します。

crashinfo save disable

no crashinfo save disable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、ASA はフラッシュ メモリにクラッシュ情報ファイルを保存します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	**crashinfo save enable** コマンドは廃止されました。代わりに、**no crashinfo save disable** コマンドを使用します。

使用上のガイドライン

クラッシュ情報は、まずフラッシュ メモリに書き込まれ、次にコンソールに書き込まれます。

(注) ASA が起動中にクラッシュした場合、クラッシュ情報ファイルは保存されません。ASA は、完全に初期化され、動作を開始した後に、クラッシュ情報をフラッシュ メモリに保存できます。

フラッシュ メモリへのクラッシュ情報の保存をもう一度イネーブルにするには、**no crashinfo save disable** コマンドを使用します。

例

次に、フラッシュ メモリへのクラッシュ情報の書き込みをディセーブルにする例を示します。

```
ciscoasa(config)# crashinfo save disable
```

関連コマンド

clear crashinfo	クラッシュ ファイルの内容をクリアします。
crashinfo force	ASA を強制的にクラッシュさせます。
crashinfo test	ASA でフラッシュ メモリ内のファイルにクラッシュ情報を保存できるかどうかをテストします。
show crashinfo	クラッシュ ファイルの内容を表示します。

crashinfo test

フラッシュ メモリのファイルにクラッシュ情報を保存する ASA の機能をテストするには、特権 EXEC モードで **crashinfo test** コマンドを使用します。

crashinfo test

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.7(1)	ユーザが使用可能なクラッシュ情報ファイルが新しい形式で表示されるように、出力が更新されました。

使用上のガイドライン

ユーザが使用可能なクラッシュ情報ファイルは、*crashinfo-test_YYYYMMDD_HHMMSS_UTC* 形式で保存されます。コマンド出力には、実際のクラッシュ情報は表示されません。フラッシュ メモリ内に以前のクラッシュ情報ファイルがすでに存在する場合、そのファイルは上書きされます。

(注) **crashinfo test** コマンドを入力しても ASA はクラッシュしません。

例

次に、クラッシュ情報ファイル テストの出力例を示します。

```
ciscoasa# crashinfo test
```

関連コマンド

clear crashinfo	すべてのクラッシュ情報ファイル、クラッシュ ファイルの内容を削除します。
crashinfo force	ASA を強制的にクラッシュさせます。

crashinfo save disable	クラッシュ情報のフラッシュ メモリへの書き込みをディセーブルにします。
show crashinfo	最新のクラッシュ情報ファイルの内容を表示します。
show crashinfo files	最後の 5 つのクラッシュ情報ファイルを日付とタイムスタンプに基づいて表示します。

crl（廃止）

CRL コンフィギュレーション オプションを指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **crl** コマンドを使用します。

crl {**required** | **optional** | **nocheck**}

構文の説明

nocheck	CRL チェックを実行しないよう ASA に指示します。
optional	必須の CRL が使用できない場合にも、ASA はピア証明書を受け入れることができます。
required	ピア証明書の検証に必要な CRL が使用可能である必要があります。

デフォルト

デフォルト値は **nocheck** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	このコマンドは廃止されました。次の形式の **revocation-check** コマンドに置き換わりました。 • **crl optional** は **revocation-check crl none** に置き換えられました。 • **crl required** は **revocation-check crl** に置き換えられました。 • **crl nocheck** は **revocation-check none** に置き換えられました。
9.13(1)	このコマンドは削除されました。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、このトラストポイントに対してピア証明書を検証する場合に CRL を必須とする例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl required
ciscoasa(ca-trustpoint)#
```

関連コマンド

コマンド	説明
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。
crypto ca trustpoint	クリプト CA トラストポイント コンフィギュレーション モードを開始します。
crl configure	CRL コンフィギュレーション モードを開始します。
url	CRL 取得用の URL を指定します。

crl cache-time

ASA によってリフレッシュされる前に trustpool CRL を CRL キャッシュ内に残す時間(分)を設定するには、CA trustpool コンフィギュレーション モードで **crl cache-time** コマンドを使用します。デフォルト値の 60 分をそのまま使用するには、このコマンドの **no** 形式を使用します。

crl cache-time

no crl cache-time

構文の説明

cache-time	分単位の値(1 ～ 1440)。

デフォルト

デフォルト値は **60** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
Ca trustpool コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、トラストポイント コンフィギュレーション モードでサポートされているこのコマンドのバージョンと整合性があります。

例

```
ciscoasa(ca-trustpool)# crl cache-time 30
```

関連コマンド

コマンド	説明
crl enforcenextupdate	NextUpdate CRL フィールドを処理する方法を指定します。

crl configure

CRL コンフィギュレーション モードを開始するには、クリプト CA トラストポイント コンフィギュレーション モードで **crl configure** コマンドを使用します。

crl configure

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、トラストポイント central の CRL コンフィギュレーション モードを開始する例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)#
```

crl enforcenextupdate

CRL の NextUpdate フィールドの処理方法を指定するには、CA trustpool コンフィギュレーション モードで **crl enforcenextupdate** コマンドを使用します。イネーブルの場合は、期限が切れていない NextUpdate フィールドが CRL に存在する必要があります。この制限を適用しないようにするには、このコマンドの **no** 形式を使用します。

crl enforcenextupdate

no crl enforcenextupdate

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトではイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
Ca trustpool コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

イネーブルの場合は、期限が切れていない NextUpdate フィールドが CRL に存在する必要があります。このコマンドは、トラストポイント コンフィギュレーション モードでサポートされているこのコマンドのバージョンと整合性があります。

関連コマンド

コマンド	説明
crl cache-time	ASA によってリフレッシュされる前に CRL を CRL キャッシュに残す時間を設定します。

CHAPTER 9

crypto am-disable コマンド ～ crypto ipsec security-association replay コマンド

crypto am-disable

アグレッシブ モードの IPsec IKEv1 着信接続をディセーブルにするには、グローバル コンフィギュレーション モードで **crypto ikev1 am-disable** コマンドを使用します。アグレッシブ モードの着信接続をイネーブルにするには、このコマンドの **no** 形式を使用します。

crypto ikev1 am-disable

no crypto ikev1 am-disable

構文の説明　このコマンドには引数またはキーワードはありません。

デフォルト　デフォルト値はイネーブルです。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**isakmp am-disable** コマンドが追加されました。
7.2.(1)	**isakmp am-disable** コマンドが、**crypto isakmp am-disable** コマンドに置き換えられました。
8.4(1)	コマンド名が **crypto isakmp am-disable** から **crypto ikev1 am-disable** に変更されました。

例

次に、グローバル コンフィギュレーション モードでの入力で、アグレッシブ モードの着信接続をディセーブルにする例を示します。

```
ciscoasa(config)# crypto ikev1 am-disable
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブな設定を表示します。

crypto ca alerts expiration

インストールされているすべての証明書の有効期限チェックは **crypto ca alerts expiration** コマンドによりデフォルトでイネーブルになっています。有効期限チェックをディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto ca alerts expiration [begin <days before expiration>] [repeat <days>]

[no] crypto ca alerts expiration [begin <days before expiration>] [repeat <days>]

構文の説明

begin <*days before expiration*>	最初のアラートが発行される有効期限までの日数を設定し、リマインダが送信される間隔を設定します。指定できる範囲は 1 ～ 90 日です。
repeat <*days*>	証明書が更新されない場合のアラート頻度を設定します。範囲は 1 ～ 14 日です。

デフォルト

インストールされたすべての証明書の有効期限チェックはデフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

リマインダは syslog メッセージであるため、無効にする必要はないと考えています。このコマンドが確認されるのは、1 日 1 回だけであるため、パフォーマンスにほとんど影響を与えません。デフォルトでは、最初のアラートは有効期限の 60 日前に送信され、その後は証明書が更新または削除されるまで毎週 1 回送信されます。さらに、有効期限が切れる日にアラートが送信され、その後は毎日 1 回送信されます。アラートの設定に関係なく、有効期限の直前の週はリマインダが毎日送信されます。

例

```
100(config)# crypto ca ?

configure mode commands/options:
  alerts        Configure alerts

100(config)# crypto ca alerts ?
```

```
configure mode commands/options:
  expiration  Configure an alert for certificates nearing expiration
100(config)# crypto ca alerts expiration ?

configure mode commands/options:
  begin   Begin alert
  repeat  Repeat alert
  <cr>100(config)# crypto ca alerts expiration begin ?

configure mode commands/options:
  <1-90>  Days prior to expiration at which the first alert should be sent

100(config)# crypto ca alerts expiration begin 10 ?

configure mode commands/options:
  repeat  Repeat alert
  <cr>
100(config)# crypto ca alerts expiration begin 10 repeat ?

configure mode commands/options:
  <1-14>  Number of days at which the alert should be repeated after the prior
           alert

100(config)# crypto ca alerts expiration begin 10 repeat 1

100(config)# show run crypto ca ?

exec mode commands/options:
  alerts       Show alerts
       certificate  Show certificate map entries

    server         Show local certificate server configuration
    trustpoint   Show trustpoints
     trustpool    Show trustpool
  |             Output modifiers
  <cr>
100(config)# show run crypto ca alerts
crypto ca alerts expiration begin 10 repeat 1

100(config)# clear conf crypto ca ?

configure mode commands/options:
  alerts       Clear alerts
  certificate  Clear certificate map entries
  server       Clear Local CA server
  trustpoint   Clear trustpoints
  trustpool    Clear trustpool

100(config)# clear conf crypto ca alerts
```

関連コマンド

コマンド	説明
clear conf crypto ca alerts	設定済みの暗号 CA アラートをクリアします。
show run crypto ca alerts	設定済みの暗号 CA アラートを表示します。

crypto ca authenticate

トラストポイントに関連付けられている CA 証明書をインストールおよび認証するには、グローバル コンフィギュレーション モードで **crypto ca authenticate** コマンドを使用します。

crypto ca authenticate *trustpoint* [**fingerprint** *hexvalue*] [**nointeractive]**

構文の説明

fingerprint	ASA が CA 証明書の認証に使用する、英数字で構成されたハッシュ値を指定します。フィンガープリントが指定されている場合、ASA は、そのフィンガープリントを、CA 証明書の計算されたフィンガープリントと比較して、2 つの値が一致した場合にだけその証明書を受け入れます。フィンガープリントがない場合、ASA は計算されたフィンガープリントを表示し、証明書を受け入れるかどうかを尋ねます。
hexvalue	フィンガープリントの 16 進数値を指定します。
nointeractive	Device Manager 専用の非対話形式モードを使用して、このトラストポイントの CA 証明書を取得します。そのとき、フィンガープリントがない場合、ASA は確認せずに証明書を受け入れます。
trustpoint	CA 証明書を取得するトラストポイントを指定します。名前の最大長は 128 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

トラストポイントが SCEP 登録用に設定されている場合、CA 証明書は SCEP 経由でダウンロードされます。そうでない場合、ASA は、ユーザに Base 64 形式の CA 証明書を端末に貼り付けるように要求します。

このコマンドの呼び出しは、実行コンフィギュレーションの一部になりません。

例

次に、CA 証明書を要求する ASA の例を示します。CA は証明書を送信し、ASA は、管理者に CA 証明書のフィンガープリントをチェックして CA 証明書を確認するように要求します。ASA の管理者は、表示されたフィンガープリントの値を既知の正しい値と照合する必要があります。ASA によって表示されたフィンガープリントが正しい値と一致した場合は、その証明書を有効であるとして受け入れる必要があります。

```
ciscoasa(config)# crypto ca authenticate myca
Certificate has the following attributes:
Fingerprint: 0123 4567 89AB CDEF 0123
Do you accept this certificate? [yes/no] y#
ciscoasa(config)#
```

次に、トラストポイント tp9 が、端末ベース（手動）の登録用に設定される例を示します。ASA は、管理者に CA 証明書を端末に貼り付けるように要求します。証明書のフィンガープリントを表示した後、ASA は、管理者に証明書を保持することを確認するように要求します。

```
ciscoasa(config)# crypto ca authenticate tp9
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

MIIDjjCCAvegAwIBAgIQejIaQ3SJRIBMHcvDdgOsKTANBgkqhkiG9w0BAQUFADBA
MQswCQYDVQQGEwJVUzELMAkGA1UECBMCTUExETAPBgNVBAcTCEZyYW5rbGluMREw
DwYDVQQDEwhCcmlhbnNDQTAeFw0wMjEwMTcxODE5MTJaFw0wNjEwMjQxOTU3MDha
MEAxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJNQTERMA8GA1UEBxMIRnJhbmtsaW4x
ETAPBgNVBAMTCEJyaWFuc0NBMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCd
jXEPvNnkZD1bKzahbTHuRot1T8KRUbCP5aWKfqViKJENzI2GnAheArazsAcc4Eaz
LDnpuyyqa0j5LA3MI577MoN1/nll018fbpqOf9eVDPJDkYTvtZ/X3vJgnEjTOWyz
T0pXxhdU1b/jgqVE74OvKBzU7A2yoQ2hMYzwVbGkewIDAQABo4IBhzCCAYMwEwYJ
KwYBBAGCNxQCBAYeBABDAEEwCwYDVR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8w
HQYDVR0OBBYEFBHr3holowFDmniI3FBwKpSEucdtMIIBGwYDVR0fBIIBEjCCAQ4w
gcaggcOggcCGgb1sZGFwOi8vL0NOPUJyaWFuc0NBLENOPWJyaWFuLXcyay1zdnIs
Q049Q0RQLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENO
PUNvbmZpZ3VyYXRpb24sREM9YnJpYW5wZGMsREM9YmRzLERDPWNvbT9jZXJ0aWZp
Y2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Y2xhc3M9Y1JMRGlzdHJpYnV0
aW9uUG9pbnQwQ6BBoD+GPWh0dHA6Ly9icmlhbi13Mmstc3ZyLmJyaWFucGRjLmJk
cy5jb20vQ2VydEVucm9sbC9CcmlhbnNDQS5jcmwwEAYJKwYBBAGCNxUBBAMCAQEw
DQYJKoZIhvcNAQEFBQADgYEAdLhc4Za3AbMjRq66xH1qJWxKUzd4nE9wOrhGgA1r
j4B/Hv2K1gUie34xGqu9OpwqvJgp/vCU12Ciykb1YdSDy/PxN4KtR9Xd1JDQMbu5
f20AYqCG5vpPWavCgmgTLcdwKa3ps1YSWGkhWmScHHSiGg1a3tevYVwhHNPA4mWo
7sQ=

Certificate has the following attributes:
Fingerprint: 21B598D5 4A81F3E5 0B24D12E 3F89C2E4
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ca enroll	CA への登録を開始します。
crypto ca import certificate	手動登録要求への応答として CA から受信した証明書をインストールします。
crypto ca trustpoint	指定したトラストポイントのクリプト CA トラストポイント コンフィギュレーション モードを開始します。

crypto ca certificate chain

指定したトラストポイントの証明書チェーン コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **crypto ca certificate chain** コマンドを使用します。

crypto ca certificate chain *trustpoint*

構文の説明

trustpoint	証明書チェーンを設定するトラストポイントを指定します。

デフォルト

デフォルトの値または動作はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、トラストポイント central の証明書チェーン コンフィギュレーション モードを開始する例を示します。

```
ciscoasa(config)# crypto ca certificate chain central
ciscoasa(config-cert-chain)#
```

関連コマンド

コマンド	説明
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。

crypto ca certificate map

証明書マッピング ルールの優先順位付けされたリストを管理するには、グローバル コンフィギュレーション モードで **crypto ca certificate map** コマンドを使用します。クリプト CA コンフィギュレーション マップ ルールを削除するには、このコマンドの **no** 形式を使用します。

crypto ca certificate map {*sequence-number* | *map-name sequence-number*}

no crypto ca certificate map {*sequence-number* | *map-name* [*sequence-number*]}

構文の説明

map-name	certificate-to-group マップの名前を指定します。
sequence-number	作成する証明書マップルールの番号を指定します。指定できる範囲は 1 ～ 65535 です。トンネル グループを証明書マップ ルールにマッピングするトンネル グループ マップを作成するときに、この番号を使用できます。

デフォルト

map-name のデフォルトの値は、DefaultCertificateMap です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	*map-name* オプションが追加されました。

使用上のガイドライン

このコマンドを発行すると、ASA は CA 証明書マップ コンフィギュレーション モードになり、証明書の発行者およびサブジェクトの識別名（DN）に基づいてルールを設定できます。マッピング ルールの順序はシーケンス番号によって決まります。これらのルールの一般的な形式は次のとおりです。

- *DN match-criteria match-value*
- *DN* は、*subject-name* または *issuer-name* のいずれかです。DN は、ITU-T X.509 標準で定義されています。
- *match-criteria* は、次の表現または演算子で構成されます。

attr *tag*	比較を一般名（CN）などの特定の DN 属性に制限します。
co	含む
eq	等しい
nc	含まない
ne	等しくない

DN の一致表現は大文字と小文字が区別されません。

例

次に、example-map というマップ名とシーケンス番号 1（ルール番号 1）で CA 証明書マップ モードを開始し、subject-name という一般名（CN）属性が Example1 と一致する必要があることを指定する例を示します。

```
ciscoasa(config)# crypto ca certificate map example-map 1
ciscoasa(ca-certificate-map)# subject-name attr cn eq Example1
ciscoasa(ca-certificate-map)#
```

次に、example-map というマップ名とシーケンス番号 1 で CA 証明書マップ モードを開始して、subject-name 内に値 cisco が含まれることを指定する例を示します。

```
ciscoasa(config)# crypto ca certificate map example-map 1
ciscoasa(ca-certificate-map)# subject-name co cisco
ciscoasa(ca-certificate-map)#
```

関連コマンド

コマンド	説明
issuer-name	ルール エントリが IPsec ピア証明書の発行者 DN に適用されることを指定します。
subject-name（クリプト CA 証明書マップ）	ルール エントリが IPsec ピア証明書のサブジェクト DN に適用されることを指定します。
tunnel-group-map enable	**crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリをトンネル グループに関連付けます。

crypto ca crl request

指定したトラストポイントのコンフィギュレーション パラメータに基づいて CRL を要求するには、クリプト CA トラストポイント コンフィギュレーション モードで **crypto ca crl request** コマンドを使用します。

crypto ca crl request *trustpoint*

構文の説明

trustpoint	トラストポイントを指定します。許容最大文字数は 128 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドの呼び出しは、実行コンフィギュレーションの一部になりません。

例

次に、central という名前のトラストポイントに基づいて CRL を要求する例を示します。

```
ciscoasa(config)# crypto ca crl request central
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crl configure	CRL コンフィギュレーション モードを開始します。

crypto ca enroll

CA との登録プロセスを開始するには、グローバル コンフィギュレーション モードで **crypto ca enroll** コマンドを使用します。

crypto ca enroll *trustpoint* **[regenerate] [shared-secret <value> | signing-certificate <value>** [**noconfirm**]

構文の説明

noconfirm	(任意)すべてのプロンプトを表示しないようにします。要求される場合がある登録オプションは、トラストポイントに事前設定されている必要があります。このオプションは、スクリプト、ASDM、または他の非インタラクティブ形式で使用するためのものです。
regenerate	登録要求を作成する前に、新しいキー ペアを生成すべきかどうかを示します。
shared-secret	ASA と交換されるメッセージの信頼性と整合性を確認するために使用される、CA によるアウトオブバンド指定値。
signing-certificate	cmp 登録要求に署名するために使用された、以前の発行済みデバイス証明書を持つトラストポイントの名前。
トラストポイント	登録するトラストポイントの名前を指定します。許容最大文字数は 128 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.7(1)	再生成するオプションが追加され、共有秘密キーワードと署名証明書キーワードが追加されました。

使用上のガイドライン

トラストポイントが SCEP 登録用に設定されている場合、ASA はただちに CLI プロンプトを表示し、ステータス メッセージがコンソールに非同期的に表示されます。トラストポイントが手動登録用に設定されている場合、ASA が Base 64 エンコードの PKCS10 証明書要求をコンソールに書き込んでから、CLI プロンプトが表示されます。

このコマンドは、参照されるトラストポイントの設定された状態に応じて、異なるインタラクティブ プロンプトを生成します。このコマンドが正常に実行されるには、トラストポイントが正しく設定されている必要があります。

トラストポイントが CMP 用に設定されている場合、共有秘密値(ir)またはリクエストに署名する証明書を含むトラストポイントの名前(cr)のどちらかを指定できますが、両方を指定することはできません。共有秘密または署名証明書のキーワードは、トラストポイント登録プロトコルが CMP に設定されている場合にのみ使用できます。

例

次に、SCEP 登録を使用して、トラストポイント tp1 でアイデンティティ証明書の登録を要求する例を示します。ASA は、トラストポイント コンフィギュレーションで保存されていない情報を要求します。

```
ciscoasa(config)# crypto ca enroll tp1
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
% password to the CA Administrator in order to revoke your certificate.
% For security reasons your password will not be saved in the configuration.
% Please make a note of it.
Password:
Re-enter password:
% The fully-qualified domain name in the certificate will be: xyz.example.com
% The subject name in the certificate will be: xyz.example.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA [yes/no]: yes
% Certificate request sent to Certificate authority.
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

ciscoasa(config)#
```

次に、CA 証明書の手動登録の例を示します。

```
ciscoasa(config)# crypto ca enroll tp1

% Start certificate enrollment ..
% The fully-qualified domain name in the certificate will be: xyz.example.com
% The subject name in the certificate will be: wb-2600-3.example.com
if serial number not set in trustpoint, prompt:
% Include the router serial number in the subject name? [yes/no]: no
If ip-address not configured in trustpoint:
% Include an IP address in the subject name? [no]: yes
Enter Interface name or IP Address[]: 1.2.3.4
Display Certificate Request to terminal? [yes/no]: y
Certificate Request follows:
MIIBFTCBwAIBADA6MTgwFAYJKoZIhvcNAQkIEwcxLjIuMy40MCAGCSqGSIb3DQEJ
AhYTd2ItMjYwMC0zLmNpc2NvLmNvbTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQDT
IdvHa4D5wXZ+40sKQV7Uek1E+CC6hm/LRN3p5ULW1KF6bxhA3Q5CQfh4jDxobn+A
Y8GoeceulS2Zb+mvgNvjAgMBAAGgITAfBgkqhkiG9w0BCQ4xEjAQMA4GA1UdDwEB
/wQEAwIFoDANBgkqhkiG9w0BAQQFAANBACDhnrEGBVtltG7hp8x6Wz/dgY+ouWcA
lzy7QpdGhb1du2P81RYn+8pWRA43cikXMTeM4ykEkZhLjDUgv9t+R9c=

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: no
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ca aunticate	このトラストポイントの CA 証明書を取得します。
crypto ca import pkcs12	手動登録要求への応答として CA から受信した証明書をインストールします。
crypto ca trustpoint	指定したトラストポイントのクリプト CA トラストポイント コンフィギュレーション モードを開始します。

crypto ca export

ASA のトラストポイント コンフィギュレーションを、関連付けられているすべてのキーおよび証明書とともに PKCS12 形式でエクスポートするには、またはデバイスのアイデンティティ証明書を PEM 形式でエクスポートするには、グローバル コンフィギュレーション モードで **crypto ca export** コマンドを使用します。

crypto ca export *trustpoint* **identity-certificate**

構文の説明

identity-certificate	指定したトラストポイントに関連付けられている登録済み証明書をコンソールに表示することを指定します。
trustpoint	証明書が表示されるトラストポイントの名前を指定します。トラストポイント名の許容最大文字数は 128 文字です。

デフォルト

デフォルトの値または動作はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(2)	このコマンドは、PEM 形式での証明書のエクスポートに対応するために変更されました。

使用上のガイドライン

このコマンドの呼び出しは、アクティブなコンフィギュレーションには含まれません。PEM データまたは PKCS12 データはコンソールに書き込まれます。

Web ブラウザでは、パスワードベースの対称キーで保護された付属の公開キー証明書とともに秘密キーを格納するために PKCS12 形式を使用しています。ASA は、トラストポイントに関連付けられている証明書とキーを Base 64 エンコードの PKCS12 形式でエクスポートします。この機能を使用して、証明書とキーを ASA 間で移動できます。

証明書の PEM エンコーディングは、PEM ヘッダーで囲まれた X.509 証明書の Base-64 エンコーディングです。このエンコーディングは、証明書を ASA 間でテキストベースで転送するための標準的なメソッドです。ASA がクライアントとして動作している場合は、SSL/TLS プロトコルを使用した *proxy-ldc-issuer* 証明書のエクスポートに PEM エンコーディングを使用できます。

例

次に、トラストポイント 222 の PEM 形式の証明書をコンソール表示としてエクスポートする例を示します。

```
ciscoasa (config)# crypto ca export 222 identity-certificate

Exported 222 follows:
-----BEGIN CERTIFICATE-----
MIIGDzCCBXigAwIBAgIKFiUgwwAAAAAFPDANBgkqhkiG9w0BAQUFADCBnTEfMB0G
CSqGSIb3DQEJARYQd2Jyb3duQGNpc2NvLmNvbTELMAkGA1UEBhMCVVMxCzAJBgNV
BAgTAk1BMREwDwYDVQQHEwhGcmFua2xpbjEWMBQGA1UEChMNQ2lzY28gU3lzdGVt
czEZMBcGA1UECxMQRnJhbmtsaW4gRGV2VGVzdDEaMBgGA1UEAxMRbXMtcm9vdC1j
YS01LTIwMDQwHhcNMDYxMTAyMjIyNjU3WhcNMjQwNTIwMTMzNDUyWjA2MRQwEgYD
VQQFEwtKTVgwOTQwSzA0TDEeMBwGCSqGSIb3DQEJAhMPQnJpYW4uY2lzY28uY29t
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCvxxIYKcrb7cJpsiFKwwsQUph5
4M5Y3CDVKEVF+98HrD6rhd0n/d6R8VYSfu76aeJC5j9Bbn3xOCx2aY5K2enf3SBW
Y66S3JeZBV88etFmyYJ7rebjUVVQZaFcq79EjoP99IeJ3a89Y7dKvYqq8I3hmYRe
uipm1G6wfKHOrpLZnwIDAQABo4IDujCCA7YwCwYDVR0PBAQDAgWgMBoGA1UdEQQT
MBGCD0JyaWFuLmNpc2NvLmNvbTAdBgNVHQ4EFgQUocM/JeVV3fjZh4wDe0JS74Jm
pvEwgdkGA1UdIwSB0TCBzoAUYZ8t0+V9pox+Y47NtCLk7WxvIQShgaOkgaAwgZ0x
HzAdBgkqhkiG9w0BCQEWEHdicm93bkBjaXNjby5jb20xCzAJBgNVBAYTAlVTMQsw
CQYDVQQIEwJNQTERMA8GA1UEBxMIRnJhbmtsaW4xFjAUBgNVBAoTDUNpc2NvIFN5
c3RlbXMxGTAXBgNVBAsTEEZyYW5rbGluIERldlRlc3QxGjAYBgNVBAMTEW1zLXJv
b3QtY2EtNS0yMDA0ghBaZ5s0Ng4SskMxF2NlIoxgMIIBSAYDVR0fBIIBPzCCATsw
geuggeiggeWGgeJsZGFwOi8vd2luMmstYWQuRlJLLU1TLVBLSS5jaXNjby5jb20v
Q049bXMtcm9vdC1jYS01LTIwMDQsQ049d2luMmstYWQsQ049Q0RQLENOPVB1Ymxp
YyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24s
REM9RlJLLU1TLVBLSSxEQz1jaXNjbyxEQz1jb20/Y2VydGlmaWNhdGVSZXZvY2F0
aW9uTGlzdD9iYXNlP29iamVjdGNsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MEug
SaBHhkVodHRwOi8vd2luMmstYWQuZnJrLW1zLXBraS5jaXNjby5jb20vQ2VydEVu
cm9sbC9tcy1yb290LWNhLTUtMjAwNC5jcmwwggFCBggrBgEFBQcBAQSCATQwggEw
MIG8BggrBgEFBQcwAoaBr2xkYXA6Ly8vQ049bXMtcm9vdC1jYS01LTIwMDQsQ049
QUlBLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNv
bmZpZ3VyYXRpb24sREM9RlJLLU1TLVBLSSxEQz1jaXNjbyxEQz1jb20/Y0FDZXJ0
aWZpY2F0ZT9iYXNlP29iamVjdGNsYXNzPWNlcnRpZmljYXRpb25BdXRob3JpdHkw
bwYIKwYBBQUHMAKGY2h0dHA6Ly93aW4yay1hZC5mcmstbXMtcGtpLmNpc2NvLmNv
bS9DZXJ0RW5yb2xsL3dpbjJrLWFkLkZSSy1NUy1QS0kuY2lzY28uY29tX21zLXJv
b3QtY2EtNS0yMDA0LmNydDANBgkqhkiG9w0BAQUFAAOBgQBlh7maRutcKNpjPbLk
bdcafJfHQ3k4UoWo0s1A0LXzdF4SsBIKQmpbfqEHtlx4EsfvfHXxUQJ6TOab7axt
hxMbNX3m7giebvtPkreqR9OYWGUjZwFUZ16TWnPA/NP3fbqRSsPgOXkC7+/5oUJd
eAeJOF4RQ6fPpXw9LjO5GXSFQA==
-----END CERTIFICATE-----
ciscoasa (config)#
```

関連コマンド

コマンド	説明
crypto ca aunticate	このトラストポイントの CA 証明書を取得します。
crypto ca enroll	CA への登録を開始します。

コマンド	説明
crypto ca import	手動登録要求への応答として CA から受信した証明書をインストールします。
crypto ca trustpoint	指定したトラストポイントのクリプト CA トラストポイント コンフィギュレーション モードを開始します。

crypto ca import

手動登録要求への応答で CA から受信した証明書をインストールしたり、PKCS12 データを使用してトラストポイントの証明書とキー ペアをインポートしたりするには、グローバル コンフィギュレーション モードで **crypto ca import** コマンドを使用します。

crypto ca import *trustpoint* **certificate** [**nointeractive**]

crypto ca import *trustpoint* **pkcs12** *passphrase* [**nointeractive**]

構文の説明

certificate	トラストポイントによって示される CA から証明書をインポートするよう ASA に指示します。
nointeractive	(オプション)非インタラクティブ モードを使用して証明書をインポートします。すべてのプロンプトが抑制されます。このオプションは、スクリプト、ASDM、または他の非インタラクティブ形式で使用するためのものです。
passphrase	PKCS12 データの復号化に使用するパスフレーズを指定します。
pkcs12	PKCS12 形式を使用してトラストポイントの証明書とキー ペアをインポートするよう ASA に指示します。
trustpoint	インポート アクションを関連付けるトラストポイントを指定します。許容最大文字数は 128 文字です。PKCS12 データをインポートし、トラストポイントが RSA キーを使用する場合、インポートされるキー ペアにはトラストポイントと同じ名前が割り当てられます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、トラストポイント Main の証明書を手動でインポートする例を示します。

```
ciscoasa (config)# crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be:
securityappliance.example.com
```

```
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
[ certificate data omitted ]
quit
INFO: Certificate successfully imported
ciscoasa (config)#
```

次に、PKCS12 データをトラストポイント central に手動でインポートする例を示します。

```
ciscoasa (config)# crypto ca import central pkcs12

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully
ciscoasa (config)#
```

グローバル コンフィギュレーション モードで入力された次の例では、RSA キーペアを保存する十分なスペースが NVRAM にないため、警告メッセージが生成されています。

```
ciscoasa(config)# crypto ca import central pkcs12 mod 2048
INFO: The name for the keys will be: central
Keypair generation process begin. Please wait...
NV RAM will not have enough space to save keypair central. Remove any unnecessary keypairs
and save the running config before using this keypair.
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ca export	トラストポイントの証明書とキー ペアを PKCS12 形式でエクスポートします。
crypto ca aunticate	トラストポイントの CA 証明書を取得します。
crypto ca enroll	CA への登録を開始します。
crypto ca trustpoint	指定したトラストポイントのクリプト CA トラストポイント コンフィギュレーション モードを開始します。

crypto ca reference-identity

参照 ID オブジェクトを設定するには、コンフィギュレーション モードで **crypto ca reference-identity** コマンドを使用します。参照 ID オブジェクトを削除するには、このコマンドの **no** 形式を使用します。

crypto ca reference-identity *reference_identity_name*

no crypto ca reference-identity *reference_identity_name*

ASA を *ca-reference-identity* モードにするには、グローバル コンフィギュレーション モードで **crypto ca reference-identity** コマンドを入力します。*ca-reference-identity* モードで、次の参照 ID を入力します。任意のタイプの参照 ID を複数追加することができます。参照 ID を削除するには、各コマンドの **no** 形式を使用します。

[**no**] **cn-id** *value*

[**no**] **dns-id** *value*

[**no**] **srv-id** *value*

[**no**] **uri-id** *value*

構文の説明

reference-identity-name	参照 ID オブジェクトの名前。
value	各参照 ID の値。
cn-id	一般名（CN）。この値は、ドメイン名の全体的な形式に一致します。CN 値は自由形式のテキストにすることはできません。CN-ID 参照 ID では、アプリケーション サービスは特定されません。
dns-id	タイプ dNSName の subjectAltName エントリ。これは DNS ドメイン名です。DNS-ID 参照 ID では、アプリケーション サービスは特定されません。
srv-id	RFC 4985 に定義されている SRVName 形式の名前をもつ、otherName タイプの subjectAltName エントリ。SRV-ID 識別子には、ドメイン名とアプリケーション サービス タイプの両方を含めることができます。たとえば、「_imaps.example.net」の SRV-ID は、DNS ドメイン名部分の「example.net」と、アプリケーション サービス タイプ部分の「imaps」に分けられます。
uri-id	タイプ uniformResourceIdentifier の subjectAltName エントリです。この値には、「scheme」コンポーネントと、RFC 3986 に定義されている「reg-name」ルールに一致する「host」コンポーネント（またはこれに相当するコンポーネント）の両方が含まれます。URI-ID 識別子には、IP アドレスではなく、およびホスト名だけではなく、DNS ドメイン名を含める必要があります。たとえば、「sip:voice.example.edu」という URI-ID は、DNS ドメイン名の「voice.example.edu」とアプリケーション サービス タイプの「sip」に分割できます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

ASA を *ca-reference-identity* モードにするには、グローバル コンフィギュレーション モードで **crypto ca reference-identity** コマンドを入力します。*ca-reference-identity* モードで、参照 ID（cn-id、dns-id、srv-id、または uri-id）を入力します。任意のタイプの参照 ID を複数追加することができます。参照 ID を削除するには、各コマンドの **no** 形式を使用します。

参照 ID は、未使用の名前を設定すると作成されます。参照 ID が作成されると、4 つの ID タイプと関連付けられた値を参照 ID に追加、または参照 ID から削除することができます。

複数のエントリが使用されている場合、証明書に srv-id、uri-id、または dns-id の少なくとも 1 つのインスタンスが含まれていると、次の動作が予想されます。

- 証明書内の uri-id のいずれかのインスタンスが、名前付き参照 id の uri-id の任意のインスタンスと一致する場合、証明書は参照 ID と一致します。
- 証明書内の srv-id のいずれかのインスタンスが、名前付き参照 id の srv-id の任意のインスタンスと一致する場合、証明書は参照 ID と一致します。
- 証明書内の dns-id のいずれかのインスタンスが、名前付き参照 id の dns-id の任意のインスタンスと一致する場合、証明書は参照 ID と一致します。
- これらのシナリオが存在しない場合、証明書は参照 ID と一致しません。

複数のエントリが使用されている場合、証明書に srv-id、uri-id、または dns-id の少なくとも 1 つのインスタンスが含まれていないが、少なくとも 1 つの cn-id が含まれていると、次の動作が予想されます。

- 証明書内の cn-id のいずれかのインスタンスが、名前付き参照 id の cn-id の任意のインスタンスと一致する場合、証明書は参照 ID と一致します。それ以外の場合、証明書は参照 ID と一致しません。
- 証明書に srv-id、uri-id、dns-id、または cn-id の少なくとも 1 つのインスタンスが含まれていない場合、証明書は参照 ID と一致しません。

ASA が TLS クライアントとして動作する場合、ASA は RFC 6125 で定義されているアプリケーション サーバの ID の検証ルールをサポートします。ASA で設定される参照 ID は、接続の確立中にサーバ証明書で提示される ID と比較されます。これらの ID は、RFC 6125 で定義されている 4 つの ID タイプの特定のインスタンスです。

参照 ID の **cn ID** と **dns ID** には、アプリケーション サービスを特定する情報を含めることができず、DNS ドメイン名を特定する情報が含まれている必要があります。

例

次に、syslog サーバの参照 ID を作成する例を示します。

```
ciscoasa(config)# crypto ca reference-identity syslogServer
ciscoasa(config-ca-ref-identity)# dns-id syslog1-bxb.cisco.com
ciscoasa(config-ca-ref-identity)# cn-id syslog1-bxb.cisco.com
```

関連コマンド

コマンド	説明
cn-id	参照 ID オブジェクトのコモン ネーム ID を設定します。
dns-id	参照 ID オブジェクトの DNS ドメイン名 ID を設定します。
srv-id	参照 ID オブジェクトで SRV-ID 識別子を設定します。
uri-id	参照 ID オブジェクトの URI ID を設定します。
logging host	セキュアな接続のために参照 ID オブジェクトを使用できるロギング サーバを設定します。
call-home profile destination address http	安全な接続のために参照 ID オブジェクトを使用できる Smart Call Home サーバを設定します。

crypto ca server（廃止）

ASA 上のローカル CA サーバを設定および管理するには、グローバル コンフィギュレーション モードで **crypto ca server** コマンドを使用します。設定されているローカル CA サーバを ASA から削除するには、このコマンドの **no** 形式を使用します。

crypto ca server

no crypto ca server

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

認証局サーバは、ASA 上でイネーブルになっていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.12(1)	**smtp** コマンドで、登録 URL のユーザの FQDN を設定するためのプロビジョニング。設定されていない場合、デフォルトで ASA の FQDN が使用されます。 このコマンドは廃止予定で、将来のリリースでは削除されます。
9.13(1)	このコマンドは削除されました。

使用上のガイドライン

ASA 上にローカル CA は 1 つしか存在できません。

crypto ca server コマンドは CA サーバを設定しますが、イネーブルにはしません。ローカル CA をイネーブルにするには、CA サーバ コンフィギュレーション モードで **shutdown** コマンドの **no** 形式を使用します。

no shutdown コマンドで CA サーバをアクティブにすると、CA および LOCAL-CA-SERVER というトラストポイントの RSA キー ペアが確立されて自己署名証明書が保持されます。この新しく生成された自己署名証明書には、デジタル署名、CRL 署名、および証明書署名キーの使用法の設定が常に含まれます。

バージョン 9.12(1) 以降では、ASA を使用して登録 URL の FQDN を設定できます。通常、ユーザは、内部 DNS を ASA FQDN として設定し、外部 DNS を登録電子メールに含まれる FQDN で設定します。ユーザは **fqdn** コマンドを使用して、ASA の FQDN ではなく、登録 URL の FQDN を設定できます。設定されていない場合、ASA はデフォルトでその FQDN を使用します。

注意 **no crypto ca server** コマンドは、ローカル CA サーバの現在の状態に関係なく、設定されているローカル CA サーバ、その RSA キー ペア、および関連付けられているトラストポイントを削除します。

例

次に、CA サーバ コンフィギュレーション モードを開始して、このモードで使用可能なローカル CA サーバ コマンドをリストする例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# ?

CA Server configuration commands:
  cdp-url               CRL Distribution Point to be included in the issued
                        certificates
  database              Embedded Certificate Server database location
                        configuration
  enrollment-retrieval  Enrollment-retrieval timeout configuration
  exit                  Exit from Certificate Server entry mode
  help                  Help for crypto ca server configuration commands
  issuer-name           Issuer name
  keysize               Size of keypair in bits to generate for certificate
                        enrollments
  lifetime              Lifetime parameters
  no                    Negate a command or set its defaults
  otp                   One-Time Password configuration options
  renewal-reminder      Enrollment renewal-reminder time configuration
  shutdown              Shutdown the Embedded Certificate Server
  smtp                  SMTP settings for enrollment E-mail notifications
  subject-name-default  Subject name default configuration for issued
                        certificates
```

次に、**smtp** コマンドでユーザの *fqdn* を設定し、出力を検証する例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# smtp fqdn asa1-localCA.server.amazon.com
ciscoasa(config-ca-server)# show run crypto ca server

crypto ca server
    smtp fqdn asa1-localCA.server.amazon.com
```

次に、設定済みでイネーブルになっている CA サーバを ASA から削除するために、CA サーバ コンフィギュレーション モードで **crypto ca server** コマンドの **no** 形式を使用する例を示します。

```
ciscoasa(config-ca-server)# no crypto ca server

Certificate server 'remove server' event has been queued for processing.
ciscoasa(config)#
```

関連コマンド

コマンド	説明
debug crypto ca server	ローカル CA サーバを設定するときに、デバッグ メッセージを表示します。
show crypto ca server	設定されている CA サーバのステータスおよびパラメータを表示します。
show crypto ca server cert-db	ローカル CA サーバ証明書を表示します。

crypto ca server crl issue

証明書失効リスト(CRL)の発行を強制的に行うには、特権 EXEC モードで **crypto ca server crl issue** コマンドを使用します。

crypto ca server crl issue

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	• 対応	—	• 対応	—	—
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

失われた CRL を回復するには、このコマンドを使用します。通常、CRL は失効時に既存の CRL に再署名することで自動的に再発行されます。**crypto ca server crl issue** コマンドは、証明書データベースに基づいて CRL を再生成します。また、このコマンドを使用するのは、証明書データベースの内容に基づいて CRL を再生成する必要がある場合だけです。

例

次に、ローカル CA サーバによる CRL の発行を強制的に行う例を示します。

```
ciscoasa(config-ca-server)# crypto ca server crl issue
A new CRL has been issued.
ciscoasa(config-ca-server)#
```

関連コマンド

コマンド	説明
cdp-url	CA によって発行される証明書に含める証明書失効リスト配布ポイントを指定します。
crypto ca server	CA サーバ コンフィギュレーション モードのコマンド セットにアクセスできるようにします。これらのコマンド セットを使用することで、ローカル CA を設定および管理できます。
crypto ca server revoke	ローカル CA サーバが発行した証明書を、証明書データベースと CRL で失効としてマークします。
show crypto ca server crl	ローカル CA の現在の CRL を表示します。

crypto ca server revoke

ローカル認証局（CA）サーバによって発行された証明書を証明書データベースと CRL で失効としてマークするには、特権 EXEC モードで **crypto ca server revoke** コマンドを使用します。

crypto ca server revoke *cert-serial-no*

構文の説明

cert-serial-no	失効させる証明書のシリアル番号を指定します。16 進形式で指定する必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	• 対応	—	• 対応	—	—
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

ASA 上のローカル CA によって発行された特定の証明書を失効させるには、その ASA で **crypto ca server revoke** コマンドを入力します。証明書は、このコマンドによって CA サーバの証明書データベースと CRL に失効としてマークされると失効します。失効させる証明書を指定するには、証明書のシリアル番号を 16 進形式で入力します。

指定した証明書が失効した後に、CRL が自動的に再生成されます。

例

次に、ローカル CA サーバによって発行されたシリアル番号 782ea09f の証明書を失効させる例を示します。

```
ciscoasa(config-ca-server)## crypto ca server revoke 782ea09f
Certificate with the serial number 0x782ea09f has been revoked. A new CRL has been issued.
ciscoasa(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server crl issue	CRL を強制的に発行します。
crypto ca server unrevoke	ローカル CA サーバによって発行され、失効した証明書の失効を取り消します。
crypto ca server user-db remove	CA サーバのユーザ データベースからユーザを削除します。
show crypto ca server crl	ローカル CA の現在の CRL を表示します。
show crypto ca server user-db	CA サーバのユーザ データベースに含まれているユーザを表示します。

crypto ca server unrevoke

ローカル CA サーバによって発行され、失効した証明書の失効を取り消すには、特権 EXEC モードで **crypto ca server unrevoke** コマンドを使用します。

crypto ca server unrevoke *cert-serial-no*

構文の説明

cert-serial-no	失効を取り消す証明書のシリアル番号を指定します。16 進形式で指定する必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	• 対応	—	• 対応	—	—
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

ASA 上のローカル CA によって発行され、失効した証明書の失効を取り消すには、**crypto ca server unrevoke** コマンドを入力します。証明書は、このコマンドによって証明書が証明書データベースで有効とマークされ、CRL から削除されると、再び有効になります。失効を取り消す証明書を指定するには、証明書のシリアル番号を 16 進形式で入力します。

指定した証明書の失効が取り消された後に、CRL が再生成されます。

例

次に、ローカル CA サーバによって発行されたシリアル番号 782ea09f の証明書の失効を取り消す例を示します。

```
ciscoasa(config-ca-server)# crypto ca server unrevoke 782ea09f
Certificate with the serial number 0x782ea09f has been unrevoked. A new CRL has been
issued.
ciscoasa(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードのコマンド セットにアクセスできるようにします。これらのコマンド セットを使用することで、ローカル CA を設定および管理できます。
crypto ca server crl issue	CRL を強制的に発行します。
crypto ca server revoke	ローカル CA サーバが発行した証明書を、証明書データベースと CRL で失効としてマークします。
crypto ca server user-db add	CA サーバのユーザ データベースにユーザを追加します。
show crypto ca server cert-db	ローカル CA サーバ証明書を表示します。
show crypto ca server user-db	CA サーバのユーザ データベースに含まれているユーザを表示します。

crypto ca server user-db add

CA サーバのユーザ データベースに新しいユーザを挿入するには、特権 EXEC モードで **crypto ca server user-db add** コマンドを使用します。

crypto ca server user-db add *user* [**dn** *dn*] [**email** *e-mail-address*]

構文の説明

dn *dn*	追加するユーザに対して発行される証明書のサブジェクト名認定者名を指定します。DN ストリングにスペースが含まれている場合は、値を二重引用符で囲みます。カンマは、DN 属性を区切るためにのみ使用できます（「OU=Service, O=Company, Inc.」など）。
email *e-mail-address*	新しいユーザの電子メール アドレスを指定します。
user	登録特権の付与対象となる 1 人のユーザを指定します。ユーザ名は、単純なユーザ名または電子メール アドレスです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	• 対応	—	• 対応	—	—
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

user 引数には単純なユーザ名（user1 など）または電子メール アドレス（user1@example.com など）を指定できます。*username* は、エンド ユーザが登録ページで指定したユーザ名と一致する必要があります。

username は、特権のないユーザとしてデータベースに追加されます。登録特権を付与するには、**crypto ca server allow** コマンドを使用する必要があります。

username 引数をワンタイム パスワードとともに使用して、登録インターフェイス ページでユーザを登録します。

(注) ワンタイム パスワード(OTP)を電子メールで通知するには、*username* 引数または *email-address* 引数に電子メール アドレスを指定する必要があります。メール送信時に電子メール アドレスが指定されていない場合、エラーが生成されます。

email *e-mail-address* のキーワードと引数のペアは、ユーザに登録と更新を忘れないように通知するための電子メール アドレスとしてのみ使用され、発行される証明書には表示されません。

電子メール アドレスを指定すると、質問がある場合にユーザに連絡することができ、また、その電子メール アドレス宛てに、登録に必要なワンタイム パスワードが通知されます。

ユーザにオプションの DN が指定されていない場合、サブジェクト名 DN は、*username* と subject-name-default DN 設定を使用して cn=*username*, subject-name-default として形成されます。

例

次に、ユーザ名 user1@example.com のユーザを完全なサブジェクト名 DN とともにユーザ データベースに追加する例を示します。

```
ciscoasa(config-ca-server)# crypto ca server user-db add dn "cn=Jane Doe, ou=engineering,
o=Example, l=RTP, st=NC, c=US"
ciscoasa(config-ca-server)#
```

次に、user2 というユーザに登録特権を付与する例を示します。

```
ciscoasa(config-ca-server)# crypto ca server user-db allow user2
ciscoasa(config-ca-server)
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードのコマンド セットにアクセスできるようにします。これらのコマンド セットを使用することで、ローカル CA を設定および管理できます。
crypto ca server user-db allow	CA サーバ データベース内の特定のユーザまたはユーザのサブセットに、CA への登録を許可します。
crypto ca server user-db remove	CA サーバ データベースからユーザを削除します。
crypto ca server user-db write	**database path** コマンドで指定したファイルに、CA サーバ データベース内のユーザ情報をコピーします。
database path	ローカル CA データベースのパスまたは場所を指定します。デフォルトの場所はフラッシュ メモリです。

crypto ca server user-db allow

ユーザまたはユーザのグループにローカル CA サーバ データベースへの登録を許可するには、特権 EXEC モードで **crypto ca server user-db allow** コマンドを使用します。このコマンドには、ワンタイム パスワードを生成および表示したり、ワンタイム パスワードをユーザに電子メールで送信したりするオプションも含まれています。

crypto ca server user-db allow {*username* | **all-unenrolled** | **all-certholders**} [**display-otp**] [**email-otp**] [**replace-otp**]

構文の説明

all-certholders	証明書が有効かどうかに関係なく、証明書が発行されているデータベース内のすべてのユーザに登録特権を付与することを指定します。これは、更新特権の付与と同じです。
all-unenrolled	証明書が発行されていないデータベース内のすべてのユーザに登録特権を付与することを指定します。
email-otp	(任意)指定したユーザのワンタイム パスワードを、それらのユーザの設定済み電子メール アドレスに電子メールで送信します。
replace-otp	(任意)指定したユーザのうち、有効なワンタイム パスワードを当初は持っていたすべてのユーザに対してワンタイム パスワードを再生成することを指定します。
display-otp	(オプション)指定したすべてのユーザのワンタイム パスワードをコンソールに表示します。
username	登録特権の付与対象となる 1 人のユーザを指定します。ユーザ名として簡易ユーザ名または電子メール アドレスを指定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	• 対応	—	• 対応	—	—
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

replace-otp キーワードを指定すると、指定したすべてのユーザに対して OTP が生成されます。指定したユーザに対して生成された有効な OTP は、これらの新しい OTP で置き換えられます。

OTP は、ASA に保存されませんが、ユーザに通知したり、登録時にユーザを認証したりする必要がある場合に生成および再生成されます。

例

次に、データベース内のすべての未登録ユーザに登録特権を付与する例を示します。

```
ciscoasa(config-ca-server)# crypto ca server user-db allow all-unenrolled
ciscoasa(config-ca-server)#
```

次に、user1 というユーザに登録特権を付与する例を示します。

```
ciscoasa(config-ca-server)# crypto ca server user-db allow user1
ciscoasa(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードのコマンド セットにアクセスできるようにします。これらのコマンド セットを使用することで、ローカル CA を設定および管理できます。
crypto ca server user-db add	CA サーバのユーザ データベースにユーザを追加します。
crypto ca server user-db write	**database path** コマンドで指定したファイルに、CA サーバ データベース内のユーザ情報をコピーします。
enrollment-retrieval	登録されたユーザが PKCS12 登録ファイルを取得できる期間を時間単位で指定します。
show crypto ca server cert-db	ローカル CA によって発行された証明書をすべて表示します。

crypto ca server user-db email-otp

ローカル CA サーバ データベース内の特定のユーザまたはユーザのサブセットに OTP を電子メールで送信するには、特権 EXEC モードで **crypto ca server user-db email-otp** コマンドを使用します。

crypto ca server user-db email-otp {*username* | **all-unenrolled** | **all-certholders**}

構文の説明

all-certholders	証明書が有効かどうかに関係なく、その証明書が発行されているデータベース内のすべてのユーザに OTP を電子メールで送信することを指定します。
all-unenrolled	証明書が一度も発行されていないか、期限が切れた証明書または失効した証明書しか保持していない、データベース内のすべてのユーザに OTP を電子メールで送信することを指定します。
username	1 人のユーザ用の OTP をそのユーザに電子メールで送信することを指定します。ユーザ名として、ユーザ名または電子メール アドレスを使用できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	• 対応	—	• 対応	—	—
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

例

次に、データベース内のすべての未登録ユーザに OTP を電子メールで送信する例を示します。

```
ciscoasa(config-ca-server)# crypto ca server user-db email-otp all-unenrolled
ciscoasa(config-ca-server)#
```

次に、user1 というユーザに OTP を電子メールで送信する例を示します。

```
ciscoasa(config-ca-server)# crypto ca server user-db email-otp user1
ciscoasa(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server user-db show-otp	CA サーバ データベース内の特定のユーザまたはユーザのサブセットのワンタイム パスワードを表示します。
show crypto ca server cert-db	ローカル CA によって発行された証明書をすべて表示します。
show crypto ca server user-db	CA サーバのユーザ データベースに含まれているユーザを表示します。

crypto ca server user-db remove

ローカル CA サーバのユーザ データベースからユーザを削除するには、特権 EXEC モードで **crypto ca server user-db remove** コマンドを使用します。

crypto ca server user-db remove *username*

構文の説明

username	削除するユーザの名前を、ユーザ名または電子メール アドレスの形式で指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	• 対応	—	• 対応	—	—
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、CA ユーザ データベースからユーザ名を削除して、ユーザが登録できないようにします。また、このコマンドには、前に発行された有効な証明書を失効させるオプションもあります。

例

次に、ユーザ名 user1 のユーザを CA サーバのユーザ データベースから削除する例を示します。

```
ciscoasa(config-ca-server)# crypto ca server user-db remove user1

WARNING: No certificates have been automatically revoked. Certificates issued to user
user1 should be revoked if necessary.

ciscoasa(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server crl issue	CRL を強制的に発行します。
crypto ca server revoke	ローカル CA サーバが発行した証明書を、証明書データベースと CRL で失効としてマークします。
show crypto ca server user-db	CA サーバのユーザ データベースに含まれているユーザを表示します。
crypto ca server user-db write	ローカル CA データベースに設定されているユーザ情報を、**database path** コマンドで指定したファイルに書き込みます。

crypto ca server user-db show-otp

ローカル CA サーバ データベース内の特定のユーザまたはユーザのサブセットの OTP を表示するには、特権 EXEC モードで **crypto ca server user-db show-otp** コマンドを使用します。

crypto ca server user-db show-otp {*username* | **all-certholders** | **all-unenrolled**}

構文の説明

all-certholders	証明書が現在有効かどうかに関係なく、その証明書が発行されているデータベース内のすべてのユーザの OTP を表示します。
all-unenrolled	証明書が一度も発行されていないか、期限が切れた証明書または失効した証明書しか保持していない、データベース内のすべてのユーザの OTP を表示します。
username	1 人のユーザの OTP を表示することを指定します。*ユーザ名*として、ユーザ名または電子メール アドレスを使用できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	• 対応	—	• 対応	—	—
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

例

次に、有効または無効な証明書を持つデータベース内のすべてのユーザの OTP を表示する例を示します。

```
ciscoasa(config-ca-server)# crypto ca server user-db show-otp all-certholders
ciscoasa(config-ca-server)#
```

次に、user1 というユーザの OTP を表示する例を示します。

```
ciscoasa(config-ca-server)# crypto ca server user-db show-otp user1
ciscoasa(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server user-db add	CA サーバのユーザ データベースにユーザを追加します。
crypto ca server user-db allow	CA サーバ データベース内の特定のユーザまたはユーザのサブセットに、ローカル CA への登録を許可します。
crypto ca server user-db email-otp	CA サーバ データベース内の特定のユーザまたはユーザのサブセットにワンタイム パスワードを電子メールで送信します。
show crypto ca server cert-db	ローカル CA によって発行された証明書をすべて表示します。

crypto ca server user-db write

すべてのローカル CA データベース ファイルを保存するディレクトリの場所を設定するには、特権 EXEC モードで **crypto ca server user-db write** コマンドを使用します。

crypto ca server user-db write

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	• 対応	—	• 対応	—	—
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

crypto ca server user-db write コマンドを使用して、新しいユーザベースのコンフィギュレーション データを、データベース パス コンフィギュレーションで指定したストレージに保存します。この情報は、**crypto ca server user-db add** コマンドおよび **crypto ca server user-db allow** コマンドで新しいユーザが追加または許可されると生成されます。

例

次に、ローカル CA データベースに設定されているユーザ情報を保存場所に書き込む例を示します。

```
ciscoasa(config-ca-server)# crypto ca server user-db write
ciscoasa(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server user-db add	CA サーバのユーザ データベースにユーザを追加します。
database path	ローカル CA データベースのパスまたは場所を指定します。デフォルトの場所はフラッシュ メモリです。
crypto ca server user-db remove	CA サーバのユーザ データベースからユーザを削除します。
show crypto ca server cert-db	ローカル CA によって発行された証明書をすべて表示します。
show crypto ca server user-db	CA サーバのユーザ データベースに含まれているユーザを表示します。

crypto ca trustpoint

指定したトラストポイントのクリプト CA トラストポイント コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **crypto ca trustpoint** コマンドを使用します。指定したトラストポイントを削除するには、このコマンドの **no** 形式を使用します。

crypto ca trustpoint *trustpoint-name*

no crypto ca trustpoint *trustpoint-name* [**noconfirm**]

構文の説明

noconfirm	すべての対話形式プロンプトを非表示にします。
trustpoint-name	管理するトラストポイントの名前を指定します。許容される名前の最大長は 128 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	OCSP をサポートするためにオプションが追加されました。これらのサブコマンドには、**match certificate map**、**ocsp disable-nonce**、**ocsp url**、**revocation-check** が含まれます。
8.0(2)	証明書の検証をサポートするためにオプションが追加されました。これらのサブコマンドには、**id-usage** と **validation-policy** が含まれます。**accept-subordinates**、**id-cert-issuer**、および **support-user-cert-validation** は廃止されました。
8.0(4)	信頼できるエンタープライズ間（電話プロキシと TLS プロキシ間など）での自己署名証明書の登録をサポートするために、**enrollment self** オプションが追加されました。
9.13(1)	The **crl required | optional | nocheck** オプションは削除されました。 **match certificate** オプションが変更され、**ovreride CDP** 設定が含まれるようになりました。

使用上のガイドライン

CA を宣言するには、**crypto ca trustpoint** コマンドを使用します。このコマンドを発行すると、クリプト CA トラストポイント コンフィギュレーション モードが開始されます。

このコマンドは、トラストポイント情報を管理します。トラストポイントは、CA が発行する証明書に基づいた CA のアイデンティティとデバイスのアイデンティティを表します。トラストポイント モード内のコマンドは、CA 固有のコンフィギュレーション パラメータを制御します。これらのパラメータでは、ASA が CA 証明書を取得する方法、ASA が CA から証明書を取得する方法、および CA が発行するユーザ証明書の認証ポリシーを指定します。

トラストポイントの特性を指定するには、次のコマンドを入力します。

- **accept-subordinates**：廃止されました。トラストポイントに関連付けられた CA に従属する CA 証明書が ASA にインストールされていない場合、フェーズ 1 の IKE 交換中にその CA 証明書が提供されたときに、それを受け入れるかどうかを指定します。
- **auto-enroll**：CMPv2 自動更新の使用/不使用、トリガーのタイミング、および新しいキーペアの生成/不生成をパラメータで設定します。ライフタイムの後に自動登録を要求する、証明書の絶対ライフタイムの割合を入力します。次に、証明書を更新する際に新しいキーを生成するかどうかを指定します：**[no] auto-enroll [<percent>] [regenerate]**
- **crl required | optional | nocheck**：CRL コンフィギュレーション オプションを指定します。ASA 9.13(1) で削除されました。
- **crl configure**：crl コンフィギュレーション モードを開始します（**crl** コマンドを参照）。
- **default enrollment**：すべての登録パラメータをシステム デフォルト値に戻します。このコマンドの呼び出しは、アクティブなコンフィギュレーションには含まれません。
- **email** *address*：登録中に、指定した電子メール アドレスを証明書のサブジェクト代替名の拡張に含めるかどうかを CA に確認します。
- **enrollment protocol cmp|scep** *url*：このトラストポイントに登録する CMP または SCEP 登録を指定し、登録 URL（*url*）を設定します。
- **enrollment retry period**：SCEP 登録の再試行期間を分単位で指定します。
- **enrollment retry count**：SCEP 登録に許可する最大試行回数を指定します。
- **enrollment terminal**：このトラストポイントへのカット アンド ペースト登録を指定します。
- **enrollment self**：自己署名証明書を生成する登録を指定します。
- **enrollment url**：このトラストポイントに登録する SCEP 登録を指定し、登録 URL（*url*）を設定します。
- **exit**：コンフィギュレーション モードを終了します。
- **fqdn** *fqdn*：登録中に、指定した FQDN を証明書のサブジェクト代替名の拡張に含めるかどうかを CA に確認します。
- **id-cert-issuer**：廃止されました。このトラストポイントに関連付けられた CA によって発行されるピア証明書をシステムが受け入れるかどうかを指定します。
- **id-usage**：トラストポイントの登録済み ID の使用方法を指定します。
- **ip-addr** *ip-address*：登録中に、ASA の IP アドレスを証明書に含めるかどうかを CA に確認します。
- **keypair** *name*：公開キーが証明対象となるキー ペアを指定します。
- keypair [<name>]：RSA または ECDSA のいずれかとして、公開キーを認証するキーペアと、そのモジュラス ビットまたは楕円曲線ビットを指定します。
- **match certificate** *map-name* **override ocsp | override cdp**：証明書マップを OCSP 上書きルールまたは CDP 上書きルールと照合します。

- **ocsp disable-nonce**：ナンス拡張子をディセーブルにします。ナンス拡張子は、失効要求と応答を結び付けて暗号化して、リプレイ アタックを回避するためのものです。
- **ocsp url**：この URL の OCSP サーバで、トラストポイントに関連するすべての証明書の失効ステータスをチェックすることを指定します。
- **exit**：コンフィギュレーション モードを終了します。
- **password** *string*：登録中に CA に登録されるチャレンジ フレーズを指定します。通常、CA はこのフレーズを使用して、その後の失効要求を認証します。
- **revocation check**：失効をチェックする方法（CRL、OCSP、なし）を指定します。
- **serial-number**：登録時に、ASA のシリアル番号を証明書に含めるように CA に要求します。
- **subject-name** *X.500 name*：登録中に、指定したサブジェクト DN を証明書に含めるかどうかを CA に確認します。DN ストリングにカンマが含まれる場合、値のストリングを二重引用符で囲みます（たとえば、O="Company, Inc."）。
- **support-user-cert-validation**：廃止されました。イネーブルの場合、リモート証明書を発行した CA に対してトラストポイントが認証されていれば、リモート ユーザ証明書を検証するコンフィギュレーション設定をこのトラストポイントから取得できます。このオプションは、サブコマンド **crl required | optional | nocheck** および CRL モードのすべての設定に関連付けられたコンフィギュレーション データに適用されます。
- **validation-policy**：ユーザ接続に関連付けられている証明書を検証するためのトラストポイントの条件を指定します。

（注） 接続しようとすると、トラストポイントからの ID 証明書の取得の試行時にそのトラストポイントに ID 証明書が含まれていないことを示す警告が表示されます。

例

次に、central という名前のトラストポイントを管理するために CA トラストポイント コンフィギュレーション モードを開始する例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)#
```

関連コマンド

コマンド	説明
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。
crypto ca aunticate	このトラストポイントの CA 証明書を取得します。
crypto ca certificate map	クリプト CA 証明書マップ コンフィギュレーション モードを開始します。証明書ベースの ACL を定義します。
crypto ca crl request	指定されたトラストポイントのコンフィギュレーション パラメータに基づいて CRL を要求します。
crypto ca import	手動登録要求への応答として CA から受信した証明書をインストールします。

crypto ca trustpool export

PKI trustpool を構成する証明書をエクスポートするには、特権 EXEC コンフィギュレーション モードで **crypto ca trustpool export** コマンドを使用します。

crypto ca trustpool export *filename*

構文の説明

filename	エクスポートされた trustpool 証明書を保存するファイル。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、アクティブな trustpool の内容全体を、指定されたファイルパスに pem コード形式でコピーします。

例

```
ciscoasa# crypto ca trustpool export disk0:/exportfile.pem
Trustpool certificates exported to disk0:/exportfile.pem
ciscoasa#
ciscoasa# more exportfile.pem
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEb
MBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDAdTYWxmb3JkMRow
GAYDVQQKDBFDb21vZG8gQ0EgTGltaXRlZDEhMB8GA1UEAwwYQUFBIENlcnRpZmlj
YXRlIFNlcnZpY2VzMB4XDTA0MDEwMTAwMDAwMFoXDTI4MTIzMTIzNTk1OVowezEL
MAkGA1UEBhMCR0IxGzAZBgNVBAgMEkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4GA1UE

<More>
```

関連コマンド

コマンド	説明
crypto ca trustpool import	PKI trustpool を構成する証明書をインポートします。

crypto ca trustpool import

PKI trustpool を構成する証明書をインポートするには、グローバル コンフィギュレーション モードで **crypto ca trustpool import** コマンドを使用します。

crypto ca trustpool import [clean] url *url* [**noconfirm** [**signature-required**]]

構文の説明

clean	インポート前にダウンロードされたすべての trustpool 証明書を削除します。
noconfirm	すべてのインタラクティブ プロンプトを抑制します。
signature-required	署名されたファイルのみを受け入れることを指定します。
url	インポートする trustpool ファイルの場所。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。
9.12(1)	ASA のデフォルトの信頼できる CA リストを使用するオプションが削除されました。

使用上のガイドライン

このコマンドを使用すると、trustpool バンドルを cisco.com からダウンロードするときに、ファイルのシグネチャを検証できます。バンドルを他のソースからダウンロードする場合や、シグネチャをサポートしていない形式でダウンロードする場合は、有効なシグネチャは必須ではありません。ユーザにはシグネチャのステータスが通知され、バンドルを受け入れるかどうかを選択できます。

表示される可能性のあるインタラクティブな警告は、次のとおりです。

- 無効なシグネチャを持つシスコ バンドル形式
- シスコ以外のバンドル形式
- 有効なシグネチャを持つシスコ バンドル形式

signature-required キーワードは、**noconfirm** オプションを選択した場合にだけ使用できます。**signature-required** キーワードが含まれている場合に、シグネチャが存在しないか確認できないと、インポートが失敗します。

(注) ファイルのシグネチャを確認できない場合は、その他の方法によって正規のファイルであることを確認していない限り、証明書をインストールしないでください。

次に、インタラクティブ プロンプトを抑制し、シグネチャを要求する場合の **crypto ca trustpool import** コマンドの動作の例を示します。

```
ciscoasa(config)# crypto ca trustpool import url ?

configure mode commands/options:
disk0: Import from disk0: file system
disk1: Import from disk1: file system
flash: Import from flash: file system
ftp: Import from ftp: file system
http: Import from http: file system
https: Import from https: file system
smb: Import from smb: file system
system: Import from system: file system
tftp: Import from tftp: file system

ciscoasa(config)# crypto ca trustpool import url http://mycompany.com ?
exec mode commands/options:
noconfirm Specify this keyword to suppress all interactive prompting.

ciscoasa(config)# crypto ca trustpool import url http://mycompany.com noconfirm ?
exec mode commands/options:
signature-required Indicate that only signed files will be accepted
```

関連コマンド

コマンド	説明
crypto ca trustpool export	PKI trustpool を構成する証明書をエクスポートします。

crypto ca trustpool policy

trustpool ポリシーを定義するコマンドを提供するサブモードを開始するには、グローバル コンフィギュレーション モードで **crypto ca trustpool policy** コマンドを使用します。trustpool 証明書バンドルの自動インポートを設定するには、バンドルをダウンロードしてインポートするために ASA が使用する URL を指定します。

crypto ca trustpool policy

構文の説明

このコマンドには引数またはキーワードはありません。

auto-import	trustpool 証明書の自動インポートを設定します。
auto-import [time <H:M:S>] [url <URL address>]	オフピーク時などの便利な時間帯にダウンロードをスケジュールする必要がある場合は、trustpool に証明書をダウンロードする時間と URL を設定します。
auto-import time	ダウンロード時刻を、時、分、秒で指定します。24 時間ごとに指定した時刻にダウンロードが試行されます。指定しない場合は、デフォルト時刻の 22:00 が使用されます。
auto-import url	trustpool 証明書の自動インポートを指定します。指定しない場合は、デフォルトのシスコ URL が使用されます。

デフォルト

デフォルトの動作や値はありません。

自動インポート オブジェクトは、デフォルトでオフになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—
オブジェクト コンフィギュレーション	• 対応	—	—	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。
9.5(2)	auto-import コマンド オプションが追加されました。

例

```
ciscoasa(config)# crypto ca trustpool ?

configure mode commands/options:
policy Define trustpool policy

ciscoasa(config)# crypto ca trustpool policy
ciscoasa(config-ca-trustpool)# ?

CA Trustpool configuration commands:
crl               CRL options
exit              Exit from certificate authority trustpool entry mode
match             Match a certificate map
no                Negate a command or set its defaults
revocation-check  Revocation checking options

auto-import Configure automatic import of trustpool certificates
ciscoasa(config-ca-trustpool)#

ciscoasa(config-ca-trustpool)# auto-import?

crypto-ca-trustpool mode commands/options:

time Specify the auto import time in hours, minutes, and seconds
Default is 22:00:00. An attempt is made every 24 hours at the specified time.
url Specify the HTTP based URL address for automatic import of trustpool certificates

<cr>

ciscoasa(config-ca-trustpool)#

ciscoasa(config-ca-trustpool)# auto-import url ?

crypto-ca-trustpool mode commands/options:
LINE  URL for automatic import
ciscoasa(config-ca-trustpool)#

ciscoasa(config-ca-trustpool)# auto-import time ?
H:M:S    Specify the auto import time in hours, minutes & seconds. E.g. 18:00:00 (attempt
to import is made at every 24 hours at 6PM)
ciscoasa(config-ca-trustpool)#
```

関連コマンド

コマンド	説明
show crypto ca trustpool policy	設定された trustpool ポリシーを表示します。

crypto ca trustpool remove

PKI trustpool から 1 つの指定された証明書を削除するには、特権 EXEC コンフィギュレーション モードで **crypto ca trustpool remove** コマンドを使用します。

crypto ca trustpool remove *cert fingerprint* **[noconfirm]**

構文の説明

cert fingerprint	16 進データ。
noconfirm	すべてのインタラクティブ プロンプトを抑制するには、このキーワードを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは信頼できるルート証明書の内容に対する変更をコミットするため、インタラクティブなユーザはアクションを確認することを求められます。

例

```
ciscoasa# crypto ca trustpool remove ?

  Hex-data Certificate fingerprint
ciscoasa# crypto ca trustpool remove 497904b0eb8719ac47b0bc11519b74d0 ?
noconfirm Specify this keyword to suppress all interactive prompting.
```

関連コマンド

コマンド	説明
clear crypto ca trustpool	trustpool からすべての証明書を削除します。
crypto ca trustpool export	PKI trustpool を構成する証明書をエクスポートします。
crypto ca trustpool import	PKI trustpool を構成する証明書をインポートします。

crypto dynamic-map match address

アクセス リストのアドレスをダイナミック クリプト マップ エントリに一致させるには、グローバル コンフィギュレーション モードで **crypto dynamic-map match address** コマンドを使用します。アドレス一致をディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **match address** *acl_name*

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **match address** *acl_name*

構文の説明

acl-name	ダイナミック クリプト マップ エントリを照合するアクセス リストを指定します。
dynamic-map-name	ダイナミック クリプト マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック クリプト マップ エントリに対応するシーケンス番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

このコマンドの詳細については、**crypto map match address** コマンドを参照してください。

例

次に、**crypto dynamic-map** コマンドを使用して、aclist1 という名前のアクセス リストのアドレスに一致させる例を示します。

```
ciscoasa(config)# crypto dynamic-map mymap 10 match address aclist1
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック クリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto dynamic-map	すべてのダイナミック クリプト マップのすべてのコンフィギュレーションを表示します。

crypto dynamic-map set df-bit

per-signature algorithm（SA）do-not-fragment（DF）ポリシーを設定するには、グローバル コンフィギュレーション モードで **crypto dynamic-map set df-bit** コマンドを使用します。DF ポリシーをディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto dynamic-map *name priority* **set df-bit** [**clear-df** | **copy-df** | **set-df**]

no crypto dynamic-map *name priority* **set df-bit** [**clear-df** | **copy-df** | **set-df**]

構文の説明

name	ダイナミック クリプト マップ セットの名前を指定します。
priority	ダイナミック クリプト マップ エントリに割り当てるプライオリティを指定します。

デフォルト

デフォルトの設定はオフです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

元の DF ポリシー コマンドが保持され、インターフェイスのグローバル ポリシー設定として機能しますが、SA については **crypto map** コマンドが優先されます。

crypto dynamic-map set ikev1 transform-set

ダイナミック クリプト マップ エントリで使用する IKEv1 トランスフォーム セットを指定するには、グローバル コンフィギュレーション モードで **crypto dynamic-map set ikev1 transform-set** コマンドを使用します。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set ikev1 transform-set** *transform-set-name1* [*… transform-set-name11*]

ダイナミック クリプト マップ エントリからトランスフォーム セットを削除するには、このコマンドの **no** 形式でトランスフォーム セット名を指定します。

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set ikev1 transform-set** *transform-set-name1* [*… transform-set-name*11]

ダイナミック クリプト マップ エントリを削除するには、このコマンドの **no** 形式を使用し、トランスフォーム セットすべて指定するか何も指定ません。

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set ikev1 transform-set**

構文の説明

dynamic-map-name	ダイナミック クリプト マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック クリプト マップ エントリに対応するシーケンス番号を指定します。
transform-set-name1 *transform-set-name11*	トランスフォーム セットの名前を 1 つ以上指定します。このコマンドで指定するトランスフォーム セットはすべて、**crypto ipsec ikev1 transform-set** コマンドで定義されている必要があります。各クリプト マップ エントリは、11 個までのトランスフォーム セットをサポートしています。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが追加されました。
7.2(1)	クリプト マップ エントリにおけるトランスフォーム セットの最大数が変更されました。
8.4(1)	**ikev1** キーワードが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

ダイナミック クリプト マップは、いずれのパラメータも設定されていないクリプト マップです。ダイナミック クリプト マップは、不足しているパラメータが、ピアの要件に合うように後でダイナミックに取得される（IPsec ネゴシエーションの結果として）ポリシー テンプレートの役割を果たします。ASA は、スタティック クリプト マップでピアの IP アドレスがまだ指定されていない場合、ピアでトンネルをネゴシエートさせるためにダイナミック クリプト マップを適用します。これは、次のタイプのピアで発生します。

- パブリック IP アドレスがダイナミックに割り当てられるピア。

  LAN-to-LAN のピア、およびリモート アクセスするピアは、両方とも DHCP を使用してパブリック IP アドレスを取得できます。ASA は、トンネルを開始するときだけこのアドレスを使用します。

- プライベート IP アドレスがダイナミックに割り当てられるピア。

  通常、リモート アクセスのトンネルを要求するピアは、ヘッドエンドによって割り当てられたプライベート IP アドレスを持っています一般に、LAN-to-LAN トンネルには事前に決定されたプライベート ネットワークのセットがあります。これがスタティック マップの設定に使用されるので、結果として IPsec SA の確立にも使用されます。

管理者がスタティック クリプト マップを設定するため、（DHCP または別の方法で）ダイナミックに割り当てられた IP アドレスがわからない場合や、割り当て方法には関係なく他のクライアントのプライベート IP アドレスがわからない場合があります。通常、VPN クライアントには、スタティック IP アドレスがなく、IPsec ネゴシエーションを発生させるためのダイナミック クリプト マップが必要です。たとえば、ヘッドエンドは IKE ネゴシエーション中に IP アドレスを Cisco VPN Client に割り当て、クライアントはこのアドレスを使用して IPsec SA をネゴシエートします。

ダイナミック クリプト マップは、IPsec コンフィギュレーションを容易にするので、ピアが必ずしも事前設定されていないネットワークで使用するのに適しています。ダイナミック クリプト マップは、Cisco VPN Client（モバイル ユーザなど）、およびダイナミックに割り当てられた IP アドレスを取得するルータに対して使用してください。

ヒント ダイナミック クリプト マップの **permit** エントリに **any** キーワードを使用する場合は、注意が必要です。このような **permit** エントリの対象となるトラフィックにマルチキャストやブロードキャストのトラフィックが含まれる場合、該当するアドレス範囲について **deny** エントリをアクセス リストに挿入します。ネットワークとサブネット ブロードキャスト トラフィックに対して、また IPsec で保護しないその他のトラフィックに対しては、必ず **deny** エントリを挿入してください。

ダイナミック クリプト マップは、接続を開始したリモートのピアと SA をネゴシエートするときだけ機能します。ASA は、ダイナミック クリプト マップを使用してリモート ピアとの接続を開始することはできません。ダイナミック クリプト マップを設定した場合は、発信トラフィックがアクセス リストの permit エントリに一致する場合でも、対応する SA が存在しないと、ASA はそのトラフィックをドロップします。

クリプト マップ セットには、ダイナミック クリプト マップを含めることができます。ダイナミック暗号マップのセットには、暗号マップ セットで一番低いプライオリティ（つまり、一番大きいシーケンス番号）を設定し、ASA が他の暗号マップを先に評価するようにする必要があります。セキュリティ アプライアンスは、他の（スタティック）マップのエントリが一致しない場合にだけ、ダイナミック クリプト マップのセットを調べます。

スタティック クリプト マップ セットと同様に、ダイナミック クリプト マップ セットにも、同じダイナミック マップ名を持つすべてのダイナミック クリプト マップを含めます。ダイナミック シーケンス番号によって、セット内のダイナミック クリプト マップが区別されます。ダイナミック クリプト マップを設定する場合は、IPsec ピアのデータ フローを暗号アクセス リストで識別するために、ACL の許可を挿入します。このように設定しないと、ASA は、ピアが提示するあらゆるデータ フロー ID を受け入れることになります。

注意 ダイナミック クリプト マップ セットを使用して設定された ASA インターフェイスにトンネリングされるトラフィックに対してスタティック（デフォルト）ルートを割り当てないでください。トンネリングされるトラフィックを指定するには、ダイナミック クリプト マップに ACL を追加します。リモート アクセス トンネルに関連付けられた ACL を設定する場合は、適切なアドレス プールを指定してください。逆ルート注入を使用してルートをインストールするのは、必ずトンネルがアップ状態になった後にしてください。

1 つのクリプト マップ セット内で、スタティック マップ エントリとダイナミック マップ エントリを組み合わせることができます。

例

次に、10 個の同じトランスフォーム セットで構成された「dynamic0」というダイナミック クリプト マップ エントリを作成する例を示します。

```
ciscoasa(config)# crypto dynamic-map dynamic0 1 set ikev1 transform-set 3des-md5 3des-sha
56des-md5 56des-sha 128aes-md5 128aes-sha 192aes-md5 192aes-sha 256aes-md5 256aes-sha
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ipsec ikev1 transform-set	IKEv1 トランスフォーム セットを設定します。
crypto map set transform-set	クリプト マップ エントリで使用するトランスフォーム セットを指定します。
clear configure crypto dynamic-map	すべてのダイナミック クリプト マップをコンフィギュレーションからクリアします。
show running-config crypto dynamic-map	ダイナミック クリプト マップのコンフィギュレーションを表示します。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto dynamic-map set ikev2 ipsec-proposal

ダイナミック クリプト マップ エントリで使用する IKEv2 の IPsec プロポーザルを指定するには、グローバル コンフィギュレーション モードで **crypto dynamic-map set ikev2 ipsec-proposal** コマンドを使用します。ダイナミック クリプト マップ エントリからトランスフォーム セットの名前を削除するには、このコマンドの **no** 形式を使用します。

crypto dynamic-map *dynamic-map-name* **set ikev2 ipsec-proposal** *transform-set-name1* [*… transform-set-name11*]

no crypto dynamic-map *dynamic-map-name* **set ikev2 ipsec-proposal** *transform-set-name1* [*… transform-set-name11*]

構文の説明

dynamic-map-name	ダイナミック クリプト マップ セットの名前を指定します。
transform-set-name1 *transform-set-name11*	トランスフォーム セットの名前を 1 つ以上指定します。このコマンドで指定するトランスフォーム セットは、**crypto ipsec ikev2 transform-set** コマンドで定義されている必要があります。各クリプト マップ エントリは、11 個までのトランスフォーム セットをサポートしています。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

crypto dynamic-map set nat-t-disable

接続の NAT-T をクリプト マップ エントリに基づいてディセーブルにするには、グローバル コンフィギュレーション モードで **crypto dynamic-map set nat-t-disable** コマンドを使用します。この暗号マップ エントリの NAT-T をイネーブルにするには、このコマンドの **no** 形式を使用します。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set nat-t-disable**

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set nat-t-disable**

構文の説明

dynamic-map-name	ダイナミック クリプト マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトの設定はオフです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

isakmp nat-traversal コマンドを使用して NAT-T をグローバルにイネーブルにします。次に、**crypto dynamic-map set nat-t-disable** コマンドを使用して特定のクリプト マップ エントリの NAT-T をディセーブルにします。

例

次のコマンドでは、mymap という名前のダイナミック クリプト マップの NAT-T をディセーブルにします。

```
ciscoasa(config)# crypto dynamic-map mymap 10 set nat-t-disable
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック クリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto dynamic-map	すべてのダイナミック クリプト マップのすべてのコンフィギュレーションを表示します。

crypto dynamic-map set peer

このコマンドの詳細については、**crypto map set peer** コマンドを参照してください。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set peer** *ip_address* | *hostname*

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set peer** *ip_address* | *hostname*

構文の説明

dynamic-map-name	ダイナミック クリプト マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック クリプト マップ エントリに対応するシーケンス番号を指定します。
hostname	**name** コマンドで定義されているように、ダイナミック クリプト マップ エントリのピアをホスト名で指定します。
ip_address	**name** コマンドで定義されているように、ダイナミック クリプト マップ エントリのピアを IP アドレスで指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、IP アドレス 10.0.0.1 を、mymap という名前のダイナミック マップのピアとして設定する例を示します。

```
ciscoasa(config)# crypto dynamic-map mymap 10 set peer 10.0.0.1
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック クリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto dynamic-map	すべてのダイナミック クリプト マップのすべてのコンフィギュレーションを表示します。

crypto dynamic-map set pfs

ダイナミック クリプト マップ エントリ用の新しいセキュリティ アソシエーションの要求時に PFS を要求するように IPsec を設定するか、または新しいセキュリティ アソシエーションの要求の受信時に PFS を要求するように IPsec を設定するには、グローバル コンフィギュレーション モードで **crypto dynamic-map set pfs** コマンドを使用します。IPsec が PFS を要求しないことを指定するには、このコマンドの **no** 形式を使用します。

crypto dynamic-map *map-name map-index* **set pfs** [**group1 | group2 | group5 | group14 | group19 | group20 | group21 | group24**]

no crypto dynamic-map *map-name map-index* **set pfs**[**group1 | group2 | group5 | group14 | group19 | group20 | group21 | group24**]

構文の説明

group14	使用する Diffie-Hellman キー交換グループを指定します。
group15	使用する Diffie-Hellman キー交換グループを指定します。
group16	使用する Diffie-Hellman キー交換グループを指定します。
group19	使用する Diffie-Hellman キー交換グループを指定します。
group20	使用する Diffie-Hellman キー交換グループを指定します。
group21	使用する Diffie-Hellman キー交換グループを指定します。
group24	使用する Diffie-Hellman キー交換グループを指定します。
map-name	クリプト マップ セットの名前を指定します。
map-index	クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトでは、PFS は設定されません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは変更され Diffie-Hellman グループ 7 が追加されました。
8.0(4)	**group 7** コマンド オプションは廃止されました。グループ 7 を設定しようとするとエラー メッセージが生成され、代わりにグループ 5 が使用されます。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

リリース	変更内容
9.13(1)	**group14**、**15**、および **16** コマンドオプションが追加されました。**group 1**、**2**、および **group 5** コマンドは廃止され、以降のリリースで削除されます。
9.15(1)	**グループ 1**、**2**、**5**、および **24** のコマンドオプションは、このリリースでサポートが廃止されました。

PFS を使用すると、新しいセキュリティ アソシエーションをネゴシエートするたびに新しい Diffie-Hellman 交換が発生します。この交換によって、処理時間が長くなります。PFS を使用すると、セキュリティがさらに向上します。1 つのキーが攻撃者によってクラックされた場合でも、侵害されるのはそのキーで送信されたデータだけになるためです。

crypto dynamic-map コマンド（**match address**、**set peer**、**set pfs** など）については、**crypto map** コマンドの項で説明しますピアがネゴシエーションを開始するときに、ローカル コンフィギュレーションで PFS が指定されている場合、ピアは PFS 交換を実行する必要があります。実行しない場合、ネゴシエーションは失敗します。ローカル コンフィギュレーションでグループが指定されていない場合、ASA はデフォルトの group2 が指定されているものと見なします。ローカル コンフィギュレーションで PFS が指定されていない場合は、ピアからの PFS のオファーがすべて受け入れられます。

ASA は、Cisco VPN Client と対話するときに PFS 値を使用しません。その代わり、フェーズ 1 でネゴシエートされた値を使用します。

例

次に、ダイナミック クリプト マップ mymap 10 用の新しいセキュリティ アソシエーションをネゴシエートするときに、必ず PFS を使用するよう指定する例を示します。指定されているグループはグループ 2 です。

```
ciscoasa(config)# crypto dynamic-map mymap 10 set pfs group2
```

次に、group14 のサポートを指定する例を示します。

```
ciscoasa(config)# crypto dynamic-map mymap 10 set pfs groyp14
ciscoasa(config)# crypto dynamic-map mymap 10 set pfs group2 (DEPRECATED)
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック クリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto dynamic-map	すべてのダイナミック クリプト マップのすべてのコンフィギュレーションを表示します。

crypto dynamic-map set reverse route

このコマンドの詳細については、**crypto map set reverse-route** コマンドを参照してください。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set reverse route**

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set reverse route**

構文の説明

dynamic-map-name	クリプト マップ セットの名前を指定します。
dynamic-seq-num	クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

このコマンドのデフォルト値はオフです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次のコマンドでは、mymap という名前のダイナミック クリプト マップの逆ルート注入をイネーブルにします。

```
ciscoasa(config)# crypto dynamic-map mymap 10 set reverse route
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック クリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto dynamic-map	すべてのダイナミック クリプト マップのすべてのコンフィギュレーションを表示します。

crypto dynamic-map set security-association lifetime

特定のダイナミック暗号マップ エントリについて、IPsec セキュリティ アソシエーションをネゴシエートするときに使用されるグローバル ライフタイム値を上書きするには、グローバル コンフィギュレーション モードで **crypto dynamic-map set security-association lifetime** コマンドを使用します。ダイナミック暗号マップ エントリのライフタイム値をグローバル値にリセットするには、このコマンドの **no** 形式を使用します。

crypto dynamic-map *map-name seq-num* **set security-association lifetime** {**seconds** *number* | **kilobytes** {*number* | **unlimited**}}

no crypto dynamic-map *map-name seq-num* **set security-association lifetime** {**seconds** ***number*** | **kilobytes** {***number*** | **unlimited**}}

構文の説明

kilobytes {*number* | **unlimited**}	所定のセキュリティ アソシエーションの有効期限が切れるまでに、そのセキュリティ アソシエーションを使用してピア間を通過できるトラフィックの量を KB 単位で指定します。指定できる範囲は 10 ～ 2147483647 KB です。グローバル デフォルトは 4,608,000 キロバイトです。 この設定は、リモート アクセス VPN 接続には適用されません。サイト間 VPN のみに適用されます。
map-name	クリプト マップ セットの名前を指定します。
seconds *number*	セキュリティ アソシエーションの有効期限が切れるまでの存続時間（秒数）を指定します。指定できる範囲は 120 ～ 214783647 秒です。グローバルのデフォルトは 28,800 秒（8 時間）です。 この設定は、リモート アクセスとサイト間 VPN の両方に適用されます。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトの KB 数は 4,608,000 で、デフォルトの秒数は 28,800 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.1(2)	**unlimited** 引数が追加されました。

使用上のガイドライン

ダイナミック暗号マップのセキュリティ アソシエーションは、グローバル ライフタイムに基づいてネゴシエートされます。

IPsec セキュリティ アソシエーションでは、共有秘密キーが使用されます。これらのキーとセキュリティ アソシエーションは、両方同時にタイムアウトになります。

特定のクリプト マップ エントリでライフタイム値が設定されている場合、ASA は、セキュリティ アソシエーションのネゴシエート時に新しいセキュリティ アソシエーションを要求するときに、ピアへの要求でクリプト マップ ライフタイム値を指定し、これらの値を新しいセキュリティ アソシエーションのライフタイムとして使用します。ASA は、ピアからネゴシエーション要求を受信すると、ピアが指定するライフタイム値またはローカルに設定されたライフタイム値のうち、小さい方を新しいセキュリティ アソシエーションのライフタイムとして使用します

サイト間 VPN 接続の場合、「時間指定」と「トラフィック量」の 2 つのライフタイムがあります。これらのライフタイムのいずれかに最初に到達すると、セキュリティ アソシエーションが期限切れになります。リモート アクセス VPN セッションでは、指定時刻ライフタイムのみが適用されます。

(注) ASA では、クリプト マップ、ダイナミック マップ、および IPsec 設定を動作中に変更できます。設定を変更する場合、変更によって影響を受ける接続のみが ASA によって停止させられます。たとえば、アクセス リスト内のエントリを削除して、クリプト マップに関連付けられた既存のアクセス リストを変更した場合、関連する接続だけがダウンします。アクセス リスト内の他のエントリに基づく接続は、影響を受けません。

指定時刻ライフタイムを変更するには、**crypto dynamic-map set security-association lifetime seconds** コマンドを使用します。指定時刻ライフタイムを使用すると、指定した秒数が経過した後にキーおよびセキュリティ アソシエーションがタイムアウトします。

例

グローバル コンフィギュレーション モードで入力された次のコマンドでは、ダイナミック暗号のダイナミック マップ mymap のセキュリティ アソシエーション ライフタイムを秒単位および KB 単位で指定します。

```
ciscoasa(config)# crypto dynamic-map mymap 10 set security-association
lifetime seconds 1400 kilobytes 3000000
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべての暗号ダイナミック マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto dynamic-map	暗号ダイナミック マップの設定を表示します。

crypto dynamic-map set tfc-packets

IPsec SA でダミーのトラフィック フローの機密性（TFC）パケットをイネーブルにするには、グローバル コンフィギュレーション モードで **crypto dynamic-map set tfc-packets** コマンドを使用します。IPsec SA で TFC パケットをディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto dynamic-map *name priority* **set tfc-packets** [**burst length** | **auto**] [**payload-size bytes** | **auto**] [**timeout second** | **auto**]

no crypto dynamic-map *name priority* **set tfc-packets** [**burst length** | **auto**] [**payload-size bytes** | **auto**] [**timeout second** | **auto**]

構文の説明

name	クリプト マップ セットの名前を指定します。
priority	クリプト マップ エントリに割り当てるプライオリティを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、クリプト マップの既存の DF ポリシー（SA レベルで）を設定します。

crypto dynamic-map set validate-icmp-errors

IPsec トンネルを介して受信した、プライベート ネットワークの内部ホストを宛先とする着信 ICMP エラー メッセージを検証するかどうかを指定するには、グローバル コンフィギュレーション モードで **crypto dynamic-map set validate-icmp-errors** コマンドを使用します。ダイナミック クリプト マップ エントリから着信 ICMP エラー メッセージの検証を削除するには、このコマンドの **no** 形式を使用します。

crypto dynamic-map *name priority* **set validate-icmp-errors**

no crypto dynamic-map *name priority* **set validate-icmp-errors**

構文の説明

name	ダイナミック クリプト マップ セットの名前を指定します。
priority	ダイナミック クリプト マップ エントリに割り当てるプライオリティを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このクリプト マップ コマンドは、着信 ICMP エラー メッセージの検証に対してのみ有効です。

crypto engine accelerator-bias

Symmetric Multi-Processing（SMP）プラットフォームで暗号化コアの割り当てを変更するには、グローバル コンフィギュレーション モードで **crypto engine accelerator-bias** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

crypto engine accelerator-bias [**balanced** | **ipsec** | **ssl**]

no crypto engine accelerator-bias [**balanced** | **ipsec** | **ssl**]

構文の説明

balanced	暗号化ハードウェア リソースを均等に分散します（Admin/SSL および IPsec コア）。
ipsec -client	暗号化ハードウェア リソースを好きな IPsec コアに割り当てます（SRTP 暗号化音声トラフィックを含む）。
ssl-client	暗号化ハードウェア リソースを好きな Admin/SSL コアに割り当てます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

暗号化コアの再分散は、プラットフォーム ASA 5585、5580、5545/5555、ASASM、FP4110、FP4120、FP4140、FP4150、FP9300、SM-24、SM-36、および SM-44 で可能です。

このコマンドを実行すると、暗号化操作を必要とするサービスへのトラフィックが中断されます。このコマンドは、IPsec の障害が設定されていない状態で、メンテナンス期間中に適用する必要があります。

例

次に、crypto engine acccelerator-bias コマンドの設定に使用可能なオプションの例を示します。

```
ciscoasa (config)# crypto engine ?

configure mode commands/options:
accelerator-bias
Specify how to allocate crypto accelerator processors
```

```
ciscoasa (config)# crypto engine accelerator-bias ?
configure mode commands/options
balanced - Equally distribute crypto hardware resources
ipsec-client - Allocate crypto hardware resources to favor IPsec/Encrypted Voice (SRTP)
ssl-client - Allocate crypto hardware resources to favor SSL

ciscoasa (config)# crypto engine accelerator-bias ssl
```

crypto engine large-mod-accel

ラージ モジュラス演算を ASA 5510、5520、5540、または 5550 でソフトウェアからハードウェアに切り替えるには、グローバル コンフィギュレーション モードで **crypto engine large-mod-accel** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

crypto engine large-mod-accel

no crypto engine large-mod-accel

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、ASA は、ソフトウェアでラージ モジュラス演算を実行します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.3(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

このコマンドは、ASA モデル 5510、5520、5540、および 5550 だけで使用可能です。大きなモジュラスの演算をソフトウェアからハードウェアに切り替えます。ハードウェアへの切り替えによって、次のことが高速化されます。

- 2048 ビット RSA 公開キー証明書の処理。
- Diffie Hellman グループ 5（DH5）キーの生成。

このコマンドは、1 秒あたりの接続を向上する必要がある場合に使用することを推奨します。負荷によっては、SSL スループットに限定的なパフォーマンス上の影響がある場合があります。

また、ソフトウェアからハードウェア、またはハードウェアからソフトウェアへの処理の移行時に発生する可能性がある一時的なパケット損失を最小限に抑えるために、使用率が低いとき、またはメンテナンス期間に（いずれかの形式の）このコマンドを使用することを推奨します。

（注） ASA 5580/5500-X プラットフォームには、ラージ モジュラス演算を切り替える機能がすでに統合されています。したがって、**crypto engine** コマンドは、これらのプラットフォームには適用されません。

例

次に、大きなモジュラスの演算をソフトウェアからハードウェアに切り替える例を示します。

```
ciscoasa(config)# crypto engine large-mod-accel
```

次に、前のコマンドをコンフィギュレーションから削除し、大きなモジュラスの演算をソフトウェアに切り替えて戻す例を示します。

```
ciscoasa(config)# no crypto engine large-mod-accel
```

関連コマンド

コマンド	説明
show running-config crypto engine	ラージ モジュラス演算がハードウェアに切り替えられているかどうかを示します。
clear configure crypto engine	ラージ モジュラス演算をソフトウェアに戻します。このコマンドは、**no crypto engine large-mod-accel** コマンドと同等です。

crypto ikev1 enable

IPsec ピアが ASA と通信するインターフェイス上で ISAKMP IKEv1 ネゴシエーションをイネーブルにするには、グローバル コンフィギュレーション モードで **crypto ikev1 enable** コマンドを使用します。ISAKMP IKEv1 をインターフェイスでディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto ikev1 enable *interface-name*

no crypto ikev1 enable *interface-name*

構文の説明

interface-name	ISAKMP IKEv1 ネゴシエーションをイネーブルまたはディセーブルにするインターフェイスの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	この **isakmp enable** コマンドが追加されました。
7.2(1)	**isakmp enable** コマンドが、**crypto isakmp enable** コマンドに置き換えられました。
8.4(1)	IKEv2 機能が追加されたことにより、**crypto isakmp enable** コマンドが **crypto ikev1 enable** コマンドに変更されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次の例では、グローバル コンフィギュレーション モードで、内部インターフェイス上で ISAKMP をディセーブルにする方法を示しています。

```
ciscoasa(config)# no crypto isakmp enable inside
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto ikev1 ipsec-over-tcp

IPsec over TCP をイネーブルにするには、グローバル コンフィギュレーション モードで **crypto ikev1 ipsec-over-tcp** コマンドを使用します。IPsec over TCP をディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto ikev1 ipsec-over-tcp [**port** *port1...port10*]

no crypto ikev1 ipsec-over-tcp [**port** *port1...port10*]

構文の説明

port *port1...port10*	(オプション)デバイスが IPsec over TCP 接続を受け入れるポートを指定します。最大 10 のポートを指定できます。ポート番号には 1 ～ 65535 の範囲の数値を指定できます。デフォルトのポート番号は 10000 です。

デフォルト

デフォルト値は [disabled] です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応		—

コマンド履歴

リリース	変更内容
7.0(1)	**isakmp ipsec-over-tcp** コマンドが追加されました。
7.2.(1)	**isakmp ipsec-over-tcp** コマンドが、**crypto isakmp ipsec-over-tcp** コマンドに置き換えられました。
8.4(1)	コマンド名が **crypto isakmp ipsec-over-tcp** から **crypto ikev1 ipsec-over-tcp** に変更されました。

例

次の例では、グローバル コンフィギュレーション モードで、IPsec over TCP をポート 45 でイネーブルにします。

```
ciscoasa(config)# crypto ikev1 ipsec-over-tcp port 45
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto ikev1 limit max-in-negotiation-sa

ASA の IKEv1 ネゴシエーション中（オープン）SA の数を制限するには、グローバル コンフィギュレーション モードで **crypto ikev1 limit max-in-negotiation-sa** コマンドを使用します。オープン SA の数の制限をディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto ikev1 limit max-in-negotiation-sa *threshold percentage*

no crypto ikev1 limit max-in-negotiation-sa *threshold percentage*

構文の説明

threshold percentage	ASA に対して許容される合計 SA のうち、ネゴシエーション中（オープン）であることが許容されるもののパーセンテージ。しきい値に達すると、追加の接続が拒否されます。範囲は 1 ～ 100 % です。ASA5506/ASA5508（100 %）を除くすべての ASA プラットフォームのデフォルトは 20 % です。

デフォルト

デフォルトは 20 % です。ASA は、ASA5506/ASA5508 を除くオープン SA の数を 20 % に制限します。

使用上のガイドライン

crypto ikev1 limit-max-in-negotiation-sa コマンドは、任意の時点においてネゴシエーション中であることが可能な SA の最大数を制限します。1

crypto ikev1 limit max in-negotiation-sa コマンドは、現在の接続を保護し、クッキー チャレンジ機能が阻止できない可能性があるメモリや CPU の攻撃を防ぐために、以降の接続のネゴシエーションを停止します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.1(2)	このコマンドが追加されました。

例

次に、ネゴシエーション中の IKEv1 接続の数を、許容される最大 IKEv1 接続の 70 % に制限する例を示します。

```
ciscoasa(config)# crypto ikev1 limit max in-negotiation-sa 70
```

関連コマンド

コマンド	説明
crypto ikev1 limit max-sa	ASA での IKEv1 接続数を制限します。
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto ikev1 policy

IPsec 接続の IKEv1 セキュリティ アソシエーション（SA）を作成するには、グローバル コンフィギュレーション モードで **crypto ikev2 policy** コマンドを使用します。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

crypto ikev1 policy *priority*

no crypto ikev1 policy *priority*

構文の説明

priority	ポリシー スイートのプライオリティ。指定できる範囲は 1 ～ 65535 です。1 は最高のプライオリティを、65535 は最低のプライオリティを示します。

デフォルト

デフォルトの動作や値はありません。

使用上のガイドライン

このコマンドは IKEv1 ポリシー コンフィギュレーション モードを開始します。このモードで追加の IKEv1 SA 設定を指定します。IKEv1 SA は、IKEv1 ピアがフェーズ 2 で安全に通信できるようにするためにフェーズ 1 で使用されるキーです。**crypto ikev1 policy** コマンドを入力した後、追加のコマンドを使用して、SA 暗号化アルゴリズム、DH グループ、整合性アルゴリズム、ライフタイム、ハッシュ アルゴリズムを設定できます。

3DES 暗号化方式は廃止されているため、新しく作成された IKE ポリシーと IPsec プロポーザルのデフォルトの暗号化方式は AES-128 になります。これは、新しいポリシーとプロポーザルのみに適用され、既存の設定項目には影響しません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

リリース	変更内容
9.13(1)	• **DH グループ 14、15、および 16** のサポートが追加されました。**groups 1、2**、および **group 5** オプションは、安全でないと見なされます。これらのオプションは廃止され、以降のリリースで削除されます。 • いくつかの整合性および PRF 暗号方式使用する ASA/Lina IKE、IPsec、および SSH モジュールは、安全ではないと見なされます。次の暗号方式は廃止され、以降のリリースで削除されます。 – HMAC-MD5 整合性と PRF 暗号方式 – IPsec での HMAC-MD5 整合性暗号 – HMAC-MD5、HMAC-MD5-96、および HMAC-SHA1-96 整合性暗号 – AES-GMAC、3DES、DES
9.15(1)	• **DH グループ 1、2**、および **5** のオプションは安全でないと見なされ、サポートが廃止されました。 • ASA/Lina IKE、IPsec、および SSH で使用される次の整合性および PRF 暗号は安全でないと見なされ、IKEv1 ポリシー設定から削除されました。 – HMAC-MD5 整合性と PRF 暗号方式 – IPsec での HMAC-MD5 整合性暗号 – HMAC-MD5、HMAC-MD5-96、および HMAC-SHA1-96 整合性暗号 – AES-GMAC、3DES、DES

例

次に、プライオリティ 1 の IKEv1 SA を作成し、IKEv1 ポリシー コンフィギュレーション モードを開始する例を示します。

```
ciscoasa(config)# crypto ikev1 policy 1
ciscoasa(config-ikev1-policy)# authentication rsa-sig
ciscoasa(config-ikev1-policy)# hash md5
ciscoasa(config-ikev1-policy)# group 14
ciscoasa(config-ikev1-policy)# lifetime 300
```

関連コマンド

コマンド	説明
crypto ikev2 cookie-challenge	SA によって開始されたパケットへの応答として、ASA がピア デバイスにクッキー チャレンジを送信できるようにします。
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto ikev2 cookie-challenge

SA によって開始されたパケットへの応答として、ASA がピア デバイスにクッキー チャレンジを送信できるようにするには、グローバル コンフィギュレーション モードで **crypto ikev2 cookie-challenge** コマンドを使用します。クッキー チャレンジをディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto ikev2 cookie-challenge *threshold percentage* | **always** | **never**

no crypto ikev2 cookie-challenge *threshold percentage* | **always** | **never**

構文の説明

threshold percentage	ASA に対して許容される合計 SA のうち、以降の SA ネゴシエーションに対してクッキー チャレンジをトリガーする、ネゴシエーション中のもののパーセンテージ。範囲は 0 ～ 99 % です。デフォルト値は 50 % です。
always	着信 SA に対して常にクッキー チャレンジを行います。
never	着信 SA に対してクッキー チャレンジを行いません。

デフォルト

デフォルトの動作や値はありません。

使用上のガイドライン

ピアに対してクッキー チャレンジを行うことによって、サービス妨害（DoS）攻撃を防止できます。攻撃者は、ピア デバイスが SA によって開始されたパケットを送信し、ASA がその応答を送信しても、ピア デバイスがそれに応答しない場合、DoS 攻撃を開始します。ピア デバイスがこれを継続的に行うと、許可されている数の SA 要求が使い果たされてしまい、最終的に ASA が応答を停止してしまうことがあります。

crypto ikev2 cookie-challenge コマンドを使用してしきい値パーセンテージをイネーブルにすると、オープン SA ネゴシエーションの数を制限できます。たとえば、デフォルト設定の 50% では、許可される SA の 50 % がネゴシエーション中（オープン）のときに、ASA は、それ以降到着した SA 初期パケットに対してクッキー チャレンジを行います。10,000 個の IKEv2 SA が許可される Cisco ASA 5580 では、5000 個の SA がオープンになると、それ以降の着信 SA に対してクッキー チャレンジが行われます。

crypto kev2 limit max in-negotiation-sa コマンドとともに使用する場合は、有効なクロス チェックが行われるように、クッキー チャレンジのしきい値を最大ネゴシエーション中のしきい値よりも低く設定してください。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次の例では、クッキー チャレンジのしきい値が 30 % に設定されます。

```
ciscoasa(config)# crypto ikev2 cookie-challenge 30
```

関連コマンド

コマンド	説明
crypto ikev2 limit max-sa	ASA での IKEv2 接続数を制限します。
crypto ikev2 limit max-in-negotiation-sa	ASA での IKEv2 ネゴシエーション中（オープン）SA の数を制限します。
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto ikev2 enable

IPsec ピアが ASA と通信するインターフェイス上で ISAKMP IKEv2 ネゴシエーションをイネーブルにするには、グローバル コンフィギュレーション モードで **crypto ikev2 enable** コマンドを使用します。ISAKMP IKEv2 をインターフェイスでディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto ikev2 enable *interface-name* [**client-services** [**port** *port*]]

no crypto ikev2 enable *interface-name* [**client-services** [**port** *port*]]

構文の説明

interface-name	ISAKMP IKEv2 ネゴシエーションをイネーブルまたはディセーブルにするインターフェイスの名前を指定します。
client-services	インターフェイスで IKEv2 接続に対してクライアント サービスをイネーブルにします。クライアント サービスには、ソフトウェア アップデート、クライアント プロファイル、GUI のローカリゼーション（翻訳）とカスタマイゼーション、Cisco Secure Desktop、SCEP プロキシなどの拡張 Anyconnect セキュア モビリティ クライアント機能が含まれています。クライアント サービスをディセーブルにしても、AnyConnect クライアントでは IKEv2 との基本的な IPsec 接続が確立されます。
port *port*	IKEv2 接続に対してクライアント サービスをイネーブルにするポートを指定します。範囲は 1 ～ 65535 です。デフォルトはポート 443 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

このコマンドを単独で使用した場合、クライアント サービスはイネーブルになりません。

例

次の例では、グローバル コンフィギュレーション モードで、outside インターフェイス上で IKEv2 をイネーブルにする方法を示しています。

```
ciscoasa(config)# crypto ikev2 enable outside client-services port 443
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto ikev2 fragmentation

IKEv2 のフラグメンテーション設定を構成するには、グローバル コンフィギュレーション モードで **crypto ikev2 fragmentation** コマンドを使用します。

[no] **crypto ikev2 fragmentation** [**mtu** *mtu-size*] | [**preferred-method** [**ietf** | **cisco**]]

no crypto ikev2 fragmentation [**mtu** *mtu-size*] | [**preferred-method** [**ietf** | **cisco**]]

構文の説明

mtu-size	MTU サイズ（68 ～ 1500）。使用する MTU 値には、IPv4/IPv6 ヘッダー + UDP ヘッダーのサイズを含める必要があります。 値を指定すると、IPv4 と IPv6 の両方で同じ値が使用されます。
preferred-method	推奨フラグメンテーション方法：RFC-7383 標準ベースの方法（**ietf**）またはシスコ独自の方法（**cisco**）です。

デフォルト

デフォルトでは、両方の IKEv2 フラグメンテーション方法がイネーブルにされており、MTU は 576（IPv4）または 1280（IPv6）であり、推奨方法は IETF です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、次を実行します。

- IKE パケットがフラグメンテーションを必要とするかどうかを決定するために使用する MTU を設定します。この値を超えたパケットはフラグメント化されます。
- 推奨フラグメンテーション方法を変更します。
- IKE フラグメンテーションをすべてディセーブルにします。

IETF RFC-7383 標準ベースの IKEv2 フラグメンテーション方法は、両方のピアがネゴシエーション中にサポートとプリファレンスを指定したときに使用されます。この方法を使用すると、暗号化はフラグメンテーション後に行われ、各 IKEv2 フラグメント メッセージが個別に保護されます。

シスコ独自のフラグメンテーションは、AnyConnect クライアントなどのピアがこの方法だけを提供する場合、または両方のピアがネゴシエーション中にサポートとプリファレンスを指定した場合に使用されます。この方式を使用すると、暗号化の後にフラグメンテーションが実行されます。受信側のピアは、すべてのフラグメントを受信するまで、メッセージを復号することも認証することもできません。

例

次の例では、グローバル コンフィギュレーション モードで、outside インターフェイス上で IKEv2 をイネーブルにする方法を示しています。

MTU 値を 600 に変更します。

```
ciscoasa(config)# crypto ikev2 fragmentation mtu 600
```

優先するフラグメンテーション方式をシスコ方式に変更する場合:

```
ciscoasa(config)# crypto ikev2 fragmentation preferred-method cisco
```

関連コマンド

コマンド	説明
show crypto ikev2 sa detail	MTU を表示します。
show running-config all crypto ikev2	設定を表示します。

crypto ikev2 limit max-in-negotiation-sa

ASA の IKEv2 ネゴシエーション中（オープン）SA の数を制限するには、グローバル コンフィギュレーション モードで **crypto ikev2 limit max in-negotiation-sa** コマンドを使用します。オープン SA の数の制限をディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto ikev2 limit max in-negotiation-sa *value*

no crypto ikev2 limit max in-negotiation-sa *value*

構文の説明

value	ASA に対して許容される合計 SA のうち、ネゴシエーション中（オープン）であることが許容されるものの数またはしきい値パーセンテージ。しきい値に達すると、追加の接続が拒否されます。範囲は 1 ～ 100 % です。デフォルトは 100 % です。

デフォルト

デフォルトではディセーブルになっています。ASA はオープン SA の数を制限しません。

使用上のガイドライン

crypto ikev2 limit-max-in-negotiation-sa コマンドは、任意の時点においてネゴシエーション中であることが可能な SA の最大数を制限します。**crypto ikev2 cookie-challenge** コマンドとともに使用する場合は、有効なクロス チェックが行われるように、クッキー チャレンジのしきい値をこの制限よりも低く設定してください。

クッキーを使用して着信接続に対してチャレンジを行う **crypto ikev2 cookie-challenge** コマンドとは異なり、**crypto kev2 limit max in-negotiation-sa** コマンドは、現在の接続を保護し、クッキー チャレンジ機能が阻止できない可能性があるメモリや CPU の攻撃を防ぐために、以降の接続のネゴシエーションを停止します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.15(1)	ネゴシエーション中の SA の最大数を絶対値として 15000 まで、または最大デバイスキャパシティから得られる最大値を設定できるようになりました（以前はパーセンテージのみが許可されていました）。

例

次に、ネゴシエーション中の IKEv2 接続の数を、許容される最大 IKEv2 接続の 70% に制限する例を示します。

```
ciscoasa(config)# crypto ikev2 limit max in-negotiation-sa 70
```

関連コマンド

コマンド	説明
crypto ikev2 limit max-sa	ASA での IKEv2 接続数を制限します。
crypto ikev2 cookie-challenge	SA によって開始されたパケットへの応答として、ASA がピア デバイスにクッキー チャレンジを送信できるようにします。
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto ikev2 limit max-sa

ASA での IKEv2 接続数を制限するには、グローバル コンフィギュレーション モードで **crypto ikev2 limit max-sa** コマンドを使用します。接続数の制限をディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto ikev2 limit max-sa *number*

no crypto ikev2 limit max-sa *number*

構文の説明

number	ASA で許可される IKEv2 接続数。制限に達すると、追加の接続が拒否されます。範囲は 1 ～ 10000 です。

デフォルト

デフォルトではディセーブルになっています。ASA は IKEv2 接続数を制限しません。許可される IKEv2 接続の最大数は、ライセンスで指定された接続の最大数になります。

使用上のガイドライン

crypto ikev2 limit max-sa コマンドは、ASA での SA の最大数を制限します。

crypto ikev2 cookie-challenge コマンドとともに使用する場合は、有効なクロス チェックが行われるように、クッキー チャレンジのしきい値をこの制限よりも低く設定してください。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、IKEv2 接続数を 5000 に制限する例を示します。

```
ciscoasa(config)# crypto ikev2 limit max-sa 5000
```

関連コマンド

コマンド	説明
crypto ikev2 cookie-challenge	SA によって開始されたパケットへの応答として、ASA がピア デバイスにクッキー チャレンジを送信できるようにします。
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto ikev2 notify

着信パケットが、SA のトラフィック セレクタと一致しない SA で受信された場合に IKE 通知のピアへの送信を管理者がイネーブルにできるようにするには、**crypto ikev2 notify** コマンドを使用します。この通知の送信をディセーブルにするには、このコマンドの no 形式を使用します。

crypto ikev2 notify invalid-selectors

[no] crypto ikev2 notify invalid-selectors

構文の説明

invalid-selectors	パケットが SA に着信してもトラフィック セレクタと一致しない場合にピアに通知します。
notify	ピアに送信される IKEv2 通知をイネーブルまたはディセーブルにします。

デフォルト

デフォルトでは、この通知はディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

例

```
100/act(config) # crypto ikev2 ?

configure mode commands/options:
    cookie-challenge   Enable and configure IKEv2 cookie challenges based on half-open SAs
    enable             Enable IKEv2 on the specified interface
    limit              Enable limits on IKEv2 SAs
    policy             Set IKEv2 policy suite
    redirect           Set IKEv2 redirect
    remote-access      Configure IKEv2 for Remote Access
    notify             Enable/Disable IKEv2 notifications to be sent to the peer

100/act(config)# crypto ikev2 notify ?

configure mode commands/options:
    invalid-selectors  Notify the peer if a packet is received on an SA but does not match
the traffic selectors
```

crypto ikev2 policy

AnyConnect IPsec 接続の IKEv2 セキュリティ アソシエーション(SA)を作成するには、グローバル コンフィギュレーション モードで **crypto ikev2 policy** コマンドを使用します。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

crypto ikev2 policy *policy_index group <number>*

no crypto ikev2 policy *policy_index group <number>*

構文の説明

group <number>	このポリシーインデックスの Diffie-Hellman グループを 14、15、16、19、20、または 21 として指定します。
policy index	IKEv2 ポリシー コンフィギュレーション モードにアクセスし、ポリシー エントリのプライオリティを指定します。

デフォルト

デフォルトの動作や値はありません。

使用上のガイドライン

IKEv2 SA は、IKEv2 ピアがフェーズ 2 で安全に通信できるようにするためにフェーズ 1 で使用されるキーです。**crypto ikev2 policy** コマンドを入力すると、IKEv2 ポリシー コンフィギュレーション モードが開始され、このモードで追加の IKEv2 SA の設定を指定します。追加のコマンドを使用して、SA 暗号化アルゴリズム、DH グループ、整合性アルゴリズム、ライフタイム、ハッシュ アルゴリズムを設定できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。policy index オプションが追加されました。

リリース	変更内容
9.13(1)	次の整合性、暗号化、および暗号化方式は廃止され、以降のリリースで削除されます。 • md5 • 3des 暗号化 • des 暗号化 • ヌル暗号化 Diffie-Hellman グループ 15 および 16 が追加され、DH グループ 1、2、5、および 24 が廃止されました。
9.15(1)	次の整合性、暗号化、および暗号化方式は、このリリースの強力な暗号化ライセンスモードから削除されました。 • md5 • 3des 暗号化 • des 暗号化 • ヌル暗号化（強力な暗号化と脆弱な暗号化の両方のライセンスモードから削除） DH グループ 1、2、5、および 24 のサポートが廃止されました。

例

次に、プライオリティ 1 の IKEv2 SA を作成し、IKEv2 ポリシー コンフィギュレーション モードを開始する例を示します。

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# integrity md5(DEPRECATED)
ciscoasa(config-ikev2-policy)# integrity sha

ciscoasa(config-ikev2-policy)# prf mad5(DEPRECATED)
ciscoasa(config-ikev2-policy)# prf sha

ciscoasa(config-ikev2-policy)# encryption 3des(DEPRECATED)
ciscoasa(config-ikev2-policy)# encryption des(DEPRECATED)
ciscoasa(config-ikev2-policy)# encryption null(DEPRECATED)
ciscoasa(config-ikev2-policy)# encryption aes
ciscoasa(config-ikev2-policy)# encryption aes-192
```

関連コマンド

コマンド	説明
crypto ikev2 cookie-challenge	SA によって開始されたパケットへの応答として、ASA がピア デバイスにクッキー チャレンジを送信できるようにします。
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto ikev2 redirect

マスターからクラスタ メンバーへのロード バランシング リダイレクションが行われる IKEv2 フェーズを指定するには、グローバル コンフィギュレーション モードで **crypto ikev2 redirect** コマンドを使用します。このコマンドを削除するには、このコマンドの **no** 形式を使用します。

crypto ikev2 redirect {**during-init** | **during-auth**}

no crypto ikev2 redirect {**during-init** | **during-auth**}

構文の説明

during-auth	IKEv2 認証交換中のクラスタ メンバーへのロード バランシング リダイレクションをイネーブルにします。
during-init	IKEv2 SA によって開始された交換中のクラスタ メンバーへのロード バランシング リダイレクションをイネーブルにします。

デフォルト

デフォルトでは、クラスタ メンバーへのロード バランシング リダイレクションは IKEv2 認証交換中に行われます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応		—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。

例

次に、クラスタ メンバーへのロード バランシング リダイレクションが IKEv2 によって開始された交換中に実行されるように設定する例を示します。

```
ciscoasa(config)# crypto ikev2 redirect during-init
```

関連コマンド

コマンド	説明
crypto ikev2 cookie-challenge	SA によって開始されたパケットへの応答として、ASA がピア デバイスにクッキー チャレンジを送信できるようにします。
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。

コマンド	説明
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto ikev2 remote-access trust-point

AnyConnect IKEv2 接続で ASA のアイデンティティ証明書トラストポイントとして参照および使用されるグローバル トラストポイントを指定するには、トンネル グループ コンフィギュレーション モードで **crypto ikev2 remote-access trust-point** コマンドを使用します。設定からコマンドを削除するには、このコマンドの **no** 形式を使用します。

crypto ikev2 remote-access trust-point *name* [*line number*]

no crypto ikev2 remote-access trust-point *name* [*line number*]

構文の説明

name	トラストポイントの名前（最大 65 文字）。
line number	トラストポイントを挿入する行番号の場所を指定します。通常、このオプションは、別の行を削除および再追加しないで一番上にトラストポイントを挿入するために使用されます。行が指定されていない場合、ASA はリストの末尾にトラストポイントを追加します。

デフォルト

デフォルトの動作や値はありません。

使用上のガイドライン

すべての IKEv2 接続で ASA のトラストポイントが AnyConnect クライアントに対して自身を認証するように設定するには、**crypto ikev2 remote-access trust-point** コマンドを使用します。このコマンドを使用すると、AnyConnect クライアントは、ユーザのグループ選択をサポートできます。

2 つのトラストポイントを同時に設定できます。RSA を 2 つ、ECDSA を 2 つ、またはそれぞれ 1 つずつ設定できます。ASA は、設定したトラストポイント リストをスキャンし、クライアントがサポートする最初の 1 つを選択します。ECDSA を使用する場合は、RSA トラストポイントの前に、このトラストポイントを設定する必要があります。

すでに存在するトラストポイントを追加しようとすると、エラーが表示されます。削除するトラストポイント名を指定しないで **no crypto ikev2 remote-access trustpoint** コマンドを使用すると、すべてのトラストポイント コンフィギュレーションが削除されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
トンネル グループ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポート、および 2 つのトラストポイントの設定が追加されました。

例

次に、トラストポイント *cisco_asa_trustpoint* を指定する例を示します。

```
ciscoasa(config)# crypto ikev2 remote-access trust-point cisco_asa_trustpoint
```

crypto ipsec df-bit

IPsec パケットの DF-bit ポリシーを設定するには、グローバル コンフィギュレーション モードで **crypto ipsec df-bit** コマンドを使用します。

crypto ipsec df-bit [**clear-df** | **copy-df** | **set-df**] *interface*

構文の説明

clear-df	(オプション)外部 IP ヘッダーで DF ビットがクリアされること、および ASA はパケットをフラグメント化して IPsec カプセル化を追加する場合があることを指定します。
copy-df	(任意)ASA が外部 DF ビット設定を元のパケット内で探すことを指定します。
set-df	(任意)外部 IP ヘッダーに DF ビットを設定することを指定します。ただし、元のパケットで DF ビットがクリアされている場合、ASA はパケットをフラグメント化することがあります。
interface	インターフェイス名を指定します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。設定を指定せずにこのコマンドをイネーブルにすると、ASA はデフォルトとして **copy-df** 設定を使用します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

DF ビットを IPsec トンネル機能とともに使用すると、ASA が、カプセル化されたヘッダーの Don't Fragment(DF)ビットをクリア、設定、またはコピーできるかどうかを指定できます。IP ヘッダー内の DF ビットにより、デバイスがパケットをフラグメント化できるかどうかが決定されます。

カプセル化されたヘッダーに DF ビットを指定するように ASA を設定するには、グローバル コンフィギュレーション モードで **crypto ipsec df-bit** コマンドを使用します。このコマンドは、クリア テキスト パケットの DF ビット設定を処理し、暗号化が適用されるときに、外部 IPsec ヘッダーに対して DF ビットをクリア、設定、またはコピーします。

トンネル モードの IPsec トラフィックをカプセル化する場合は、DF ビットに **clear-df** 設定を使用します。この設定を使用すると、デバイスは、使用可能な MTU サイズよりも大きなパケットを送信できます。また、この設定は、使用可能な MTU サイズが不明な場合にも適しています。

注意 パケットは、次の矛盾した設定を行うとドロップされます。
crypto ipsec fragmentation after-encryption（フラグメント パケット）
crypto ipsec df-bit set-df outside（DF ビットを設定）

例

次に、グローバル コンフィギュレーション モードで、IPsec DF ポリシーを **clear-df** に設定する例を示します。

```
ciscoasa(config)# crypto ipsec df-bit clear-df outside
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ipsec fragmentation	IPsec パケットのフラグメンテーション ポリシーを設定します。
show crypto ipsec df-bit	指定したインターフェイスの DF ビット ポリシーを表示します。
show crypto ipsec fragmentation	指定したインターフェイスのフラグメンテーション ポリシーを表示します。

crypto ipsec fragmentation

IPsec パケットのフラグメンテーション ポリシーを設定するには、グローバル コンフィギュレーション モードで **crypto ipsec fragmentation** コマンドを使用します。

crypto ipsec fragmentation {**after-encryption** | **before-encryption**} *interface*

構文の説明

after-encryption	暗号化の後で MTU の最大サイズに近い IPsec パケットを ASA がフラグメント化するように指定します(事前フラグメント化をディセーブルにします)。
before-encryption	暗号化の前に MTU の最大サイズに近い IPsec パケットを ASA がフラグメント化するように指定します(事前フラグメント化をイネーブルにします)。
interface	インターフェイス名を指定します。

デフォルト

before-encryption はデフォルトでイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

パケットは、暗号化する ASA の発信リンクの MTU サイズに近い場合、IPsec ヘッダーを付けてカプセル化されると、発信リンクの MTU を超える可能性があります。超えた場合は、暗号化の後にパケットがフラグメント化され、復号化デバイスがプロセス パスで再構築することになります。IPsec VPN の事前フラグメント化では、デバイスはプロセス パスではなく高性能な CEF パスで動作するため、復号化時のデバイスのパフォーマンスが向上します。

IPsec VPN の事前フラグメント化により、暗号化デバイスは、IPsec SA の一部として設定されたトランスフォーム セットで使用可能な情報から、カプセル化されたパケット サイズを事前に設定します。デバイスでパケットが出力インターフェイスの MTU を超えることが事前に設定されている場合、デバイスは暗号化する前にそのパケットをフラグメント化します。これにより、復号化前にプロセス レベルでパケットを再構築する必要がなくなるため、復号化のパフォーマンスと IPsec トラフィックの全体的なスループットが向上します。

IPv6 対応インターフェイスで許可される最小 MTU は 1280 バイトです。ただし、IPsec がインターフェイスでイネーブルになっている場合、MTU 値は、IPsec 暗号化のオーバーヘッドのために 1380 未満に設定できません。インターフェイスを 1380 バイト未満に設定すると、パケットのドロップが発生する可能性があります。

注意 パケットは、次の矛盾した設定を行うとドロップされます。
crypto ipsec fragmentation after-encryption（フラグメント パケット）
crypto ipsec df-bit set-df outside（DF ビットを設定）

例

次に、グローバル コンフィギュレーション モードで、IPsec パケットの事前フラグメント化を内部インターフェイス上だけでイネーブルにする例を示します。

```
ciscoasa(config)# crypto ipsec fragmentation before-encryption inside
ciscoasa(config)#
```

次に、グローバル コンフィギュレーション モードで、IPsec パケットの事前フラグメント化をインターフェイス上でディセーブルにする例を示します。

```
ciscoasa(config)# crypto ipsec fragmentation after-encryption inside
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ipsec df-bit	IPsec パケットの DF ビット ポリシーを設定します。
show crypto ipsec fragmentation	IPsec パケットのフラグメンテーション ポリシーを表示します。
show crypto ipsec df-bit	指定したインターフェイスの DF ビット ポリシーを表示します。

crypto ipsec ikev1 transform-set

IKEv1 トランスフォーム セットを作成または削除するには、グローバル コンフィギュレーション モードで **crypto ipsec ikev1 transform-set** コマンドを使用します。トランスフォームを削除するには、このコマンドの **no** 形式を使用します。

crypto ipsec ikev1 transform-set *transform-set-name encryption* [*authentication*]

no crypto ipsec ikev1 transform-set *transform-set-name encryption* [*authentication*]

構文の説明

authentication	(オプション)IPsec のデータ フローの整合性を保証する認証方法を次の中から 1 つ指定します。 **esp-md5-hmac**:ハッシュ アルゴリズムとして MD5/HMAC-128 を使用する場合。 **esp-sha-hmac**:ハッシュ アルゴリズムとして SHA/HMAC-160 を使用する場合。 **esp-none**:HMAC 認証を使用しない場合。
暗号化	IPsec のデータ フローを保護する暗号化方法を次の中から 1 つ指定します。 **esp-aes**:128 ビット キーで AES を使用する場合。 **esp-aes-192**:192 ビット キーで AES を使用する場合。 **esp-aes-256**:256 ビット キーで AES を使用する場合。 **esp-des**:56 ビットの DES-CBC を使用する場合。 **esp-3des**:トリプル DES アルゴリズムを使用する場合。 **esp-null**:暗号化を使用しない場合。
transform-set-name	作成または変更するトランスフォーム セットの名前。すでにコンフィギュレーションに存在するトランスフォーム セットを表示するには、**show running-config ipsec** コマンドを入力します。

デフォルト

デフォルトの認証設定は、esp-none(認証しない)です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが追加されました。
7.2(1)	この項は書き換えられました。
8.4(1)	**ikev1** キーワードが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.13(1)	次のオプションは廃止され、以降のリリースで削除されます。 • esp-md5-hmac • esp-3des • esp-des
9.15(1)	次のオプションは、このリリースから削除されました。 • esp-md5-hmac • esp-3des • esp-des

使用上のガイドライン

このコマンドでは、トランスフォーム セットが使用する IPsec 暗号化およびハッシュ アルゴリズムを指定します。

トランスフォーム セットを設定したら、そのセットをクリプト マップに割り当てます。1 つのクリプト マップに対して最大 6 つのトランスフォーム セットを割り当てることができます。ピアが IPsec セッションを確立しようとすると、ASA は、一致が検出されるまで、各クリプト マップのアクセス リストを使用してピアを評価します。次に、ASA は、一致が検出されるまで、ピアがネゴシエートするすべてのプロトコル、アルゴリズム、およびその他の設定を、クリプト マップに割り当てられているトランスフォーム セット内の設定を使用して評価します。ASA では、ピアの IPsec ネゴシエーションとトランスフォーム セット内の設定とが一致すると、IPsec セキュリティ アソシエーションの一部としてその設定を保護されたトラフィックに適用します。ASA は、ピアがアクセス リストに一致しない場合や、クリプト マップに割り当てられているトランスフォーム セット内にピアのセキュリティ設定と完全に一致するセキュリティ設定が見つからない場合、IPsec セッションを終了します。

暗号化と認証のどちらを先に指定してもかまいません。認証を指定せずに暗号化を指定することもできます。作成するトランスフォーム セットに認証を指定する場合は、暗号化も指定する必要があります。変更するトランスフォーム セットに認証だけを指定した場合、トランスフォーム セットでは、現在の暗号化設定が維持されます。

AES 暗号化を指定する場合は、グローバル コンフィギュレーション モードでも **isakmp policy priority group 5** コマンドを使用して、AES で提供される大きなキー サイズに対応できるように Diffie-Hellman グループ 5 を割り当てることを推奨します。

ヒント クリプト マップまたはダイナミック クリプト マップにトランスフォーム セットを適用し、そのマップに割り当てられているトランスフォーム セットを表示する場合は、トランスフォーム セットにコンフィギュレーションの内容を表す名前を付けておくと便利です。たとえば、次に示す最初の例の「3des-md5」は、トランスフォーム セットで使用する暗号化と認証を示しています。この名前の後に続く値は、トランスフォーム セットに割り当てる実際の暗号化と認証の設定です。

例

次のコマンドは、使用可能な暗号化と認証のすべてのオプション（暗号化と認証をまったく指定しないオプションは除く）を示しています。

```
ciscoasa(config)# crypto ipsec ikev1 transform-set 3des-md5 esp-3des esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 3des-sha esp-3des esp-sha-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 56des-md5 esp-des esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 56des-sha esp-des esp-sha-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 128aes-md5 esp-aes esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 128aes-sha esp-aes esp-sha-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 192aes-md5 esp-aes-192 esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 192aes-sha esp-aes-192 esp-sha-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 256aes-md5 esp-aes-256 esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 256aes-sha esp-aes-256 esp-sha-hmac

ciscoasa(config)# crypto ipsec ikev1 transform-set esp-des (DEPRECATED)
ciscoasa(config)# crypto ipsec ikev1 transform-set esp-3des(DEPRECATED)
iscoasa(config)# crypto ipsec ikev1 transform-set esp-md5-hmac (DEPRECATED)
```

関連コマンド

コマンド	説明
show running-config ipsec	すべてのトランスフォーム セットのコンフィギュレーションを表示します。
crypto map set transform-set	クリプト マップ エントリで使用するトランスフォーム セットを指定します。
crypto dynamic-map set transform-set	ダイナミック クリプト マップ エントリで使用するトランスフォーム セットを指定します。
show running-config crypto map	クリプト マップの設定内容を表示します。
show running-config crypto dynamic-map	ダイナミック クリプト マップのコンフィギュレーションを表示します。

crypto ipsec ikev1 transform-set mode transport

IPsec IKEv1 接続に対して転送モードを指定するには、グローバル コンフィギュレーション モードで **crypto ipsec ikev1 transform-set mode transport** コマンドを使用します。このコマンドを削除するには、このコマンドの **no** 形式を使用します。

crypto ipsec ikev1 transform-set *transform-set-name* **mode** {**transport**}

no crypto ipsec ikev1 transform-set *transform-set-name* **mode** {**transport**}

構文の説明

transform-set-name	変更するトランスフォーム セットの名前。すでにコンフィギュレーションに存在するトランスフォーム セットを表示するには、**show running-config ipsec** コマンドを入力します。

デフォルト

転送モードのデフォルト設定はディセーブルです。IPsec ではネットワーク トンネル モードが使用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	このコマンドが書き換えられました。
8.4(1)	**ikev1** キーワードが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

デフォルトのネットワーク トンネル モードの代わりに、IPsec にホスト間転送モードを指定するには、**crypto ipsec ikev1 transform-set mode transport** コマンドを使用します。

例

次のコマンドは、使用可能な暗号化と認証のすべてのオプション（暗号化と認証をまったく指定しないオプションは除く）を示しています。

```
ciscoasa(config)# crypto ipsec ikev1 transform-set
ciscoasa(config)#
```

関連コマンド

コマンド	説明
show running-config ipsec	すべてのトランスフォーム セットのコンフィギュレーションを表示します。
crypto map set transform-set	クリプト マップ エントリで使用するトランスフォーム セットを指定します。
crypto dynamic-map set transform-set	ダイナミック クリプト マップ エントリで使用するトランスフォーム セットを指定します。
show running-config crypto map	クリプト マップの設定内容を表示します。
show running-config crypto dynamic-map	ダイナミック クリプト マップのコンフィギュレーションを表示します。

crypto ipsec ikev2 ipsec-proposal

IKEv2 プロポーザルを作成するには、グローバル コンフィギュレーション モードで **crypto ipsec ikev2 ipsec-proposal** コマンドを使用します。プロポーザルを削除するには、このコマンドの **no** 形式を使用します。

crypto ipsec ikev2 ipsec-proposal *proposal tag proposal_name*

no crypto ipsec ikev2 ipsec-proposal *proposal tag proposal_name*

構文の説明

proposal name	IPsec ESP プロポーザル サブモードにアクセスします。
proposal tag	IKEv2 IPsec プロポーザルの名前で、1 ～ 64 文字の文字列です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.13(1)	次の IKEv2/IPsec プロポーザル整合性と暗号化方式は廃止され、以降のリリースで削除されます。 • md5 • 3des • des • aes-gmac • aes-gmac-192 • aes-gmac-256

リリース	変更内容
9.15(1)	次の IKEv2/IPsec プロポーザル整合性と暗号化方式は、このリリースから削除されました。 • md5 • 3des • des • aes-gmac • aes-gmac-192 • aes-gmac-256

使用上のガイドライン

このコマンドは、プロポーザルを作成し、ipsec プロポーザル コンフィギュレーション モードを開始します。このモードで、プロポーザルの複数の暗号化および整合性タイプを指定できます。

例

次に、secure という名前の IPsec プロポーザルを作成し、IPsec プロポーザル コンフィギュレーション モードを開始する例を示します。

```
ciscoasa(config)# crypto ipsec ikev2 ipsec-proposal secure
ciscoasa(config-ipsec-proposal)# protocol esp encryption ?
ciscoasa (config-ipsec-提案) # protocol esp aes
ciscoasa(config-ipsec-proposal)# protocol esp 3des(DEPRECATED)

ciscoasa(config-ipsec-proposal)# protocol esp integrity ?
ciscoasa (config-ipsec-提案) # protocol esp sha
ciscoasa(config-ipsec-proposal)# protocol esp md5(DEPRECATED)
```

関連コマンド

コマンド	説明
show running-config ipsec	すべてのトランスフォーム セットのコンフィギュレーションを表示します。
crypto map set transform-set	クリプト マップ エントリで使用するトランスフォーム セットを指定します。
crypto dynamic-map set transform-set	ダイナミック クリプト マップ エントリで使用するトランスフォーム セットを指定します。
show running-config crypto map	クリプト マップの設定内容を表示します。
show running-config crypto dynamic-map	ダイナミック クリプト マップのコンフィギュレーションを表示します。

crypto ipsec ikev2 sa-strength-enforcement

IKEv2 暗号化暗号の強度が、子 IPsec SA の暗号化暗号の強度よりも確実に高くなるようにします。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto ipsec ikev2 sa-strength-enforcement

no crypto ipsec ikev2 sa-strength-enforcement

デフォルト

適用は、デフォルトで無効になっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.1(2)	このコマンドが追加されました。

使用上のガイドライン

子 SA の暗号化暗号の強度が親 IKEv2 接続の暗号化暗号よりも高い場合、セキュリティは向上しません。セキュリティ対策として、このような状況が発生しないように IPsec を設定することをお勧めします。強度適用の設定は、暗号化暗号にのみ影響します。整合性アルゴリズムやキー交換アルゴリズムは変更されません。IKEv2 システムでは、各子 SA の選択された暗号化暗号の相対的な強度を次のように比較します。

イネーブルの場合、子 SA に設定されている暗号化暗号の強度が親 IKEv2 の暗号化暗号よりも高くないことを確認します。親よりも強力な暗号方式が見つかった場合、子 SA は親の暗号方式を使用するように更新されます。互換性のある暗号方式が見つからない場合、子 SA のネゴシエーションは中断されます。これらのアクションは、syslog およびデバッグ メッセージに記録されます。

次に、サポートされている暗号化暗号を、強度の高い順に示します。同じ行の暗号方式は、このチェックの目的では、同等の強度となります。

- AES-GCM-256、AES-CBC-256
- AES-GCM-192、AES-CBC、192
- AES-GCM-128、AES-CBC-128
- 3DES
- DES
- AES-GMAC（すべてのサイズ）、NULL

関連コマンド

コマンド	説明
show running-config ipsec	イネーブルの場合、crypto ipsec ikev2 sa-strength-enforcement を表示します。

crypto ipsec inner-routing-lookup

IPsec 内部ルーティング ルックアップをイネーブルにするには、コンフィギュレーション モードで **crypto ipsec inner-routing-lookup** コマンドを使用します。IPsec 内部ルーティング ルックアップをディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto ipsec inner-routing-lookup

no crypto ipsec inner-routing-lookup

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

IPsec 内部ルーティング ルックアップはデフォルトでディセーブルにされています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、外部 ESP パケットに対してはパケット単位の隣接関係ルックアップが行われますが、IPSec トンネル経由で送信されるパケットに対してはルックアップが行われません。

一部のネットワーク トポロジでは、ルーティング アップデートによって内部パケットのパスが変更され、ローカル IPsec トンネルが引き続きアップ状態である場合、トンネル経由のパケットは正しくルーティングされず、宛先に到達しません。

これを防止するには、IPSec 内部パケットに対してパケット単位のルーティング ルックアップをイネーブルにします。この機能がデフォルトでディセーブルになっているのは、こうしたルックアップによるパフォーマンスの低下を回避するためです。この機能は、必要な場合にのみイネーブルにしてください。

このコマンドが設定されている場合、非 VTI ベースのトンネルにのみ適用されます。

例

次に、内部ルーティング ルックアップをイネーブルにする例を示します。

```
ciscoasa(config)# crypto ipsec inner-routing-lookup
ciscoasa(config)# show run crypto ipsec
crypto ipsec inner-routing-lookup
```

関連コマンド

コマンド	説明
show run crypto ipsec	実行中の crypto ipsec 設定を表示します。

crypto ipsec profile

新しい IPsec プロファイルを作成するには、グローバル コンフィギュレーション モードで **crypto ipsec profile** コマンドを使用します。IPsec プロファイルを削除するには、このコマンドの **no** 形式を使用します。

crypto ipsec profile *name set pfs <group #>*

no crypto ipsec profile *name set pfs <group #>*

構文の説明

name	新しい IPsec プロファイルの名前を指定します。名前には最大 64 文字を使用できます。
group #	使用する Diffie-Hellman キー交換グループを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル設定	• 対応	• x	• 対応	• 非対応	• -

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドとそのサブモードを導入しました。

例

次の例では、VTIipsec が新しい IPsec プロファイルです。

```
ciscoasa(config)# crypto ipsec profile VTIipsec
```

関連コマンド

コマンド	説明
responder-only	VTI トンネル インターフェイスをレスポンダ専用モードに設定します。
set ikev1 transform-set	IKEv1 変換セットを IPsec プロファイル設定に使用するように指定します。
set pfs	PFS グループを IPsec プロファイル設定に使用するように指定します。
set security-association lifetime	IPsec プロファイル設定でのセキュリティ アソシエーションの期間を指定します。これは、キロバイト単位か秒単位、またはその両方で指定します。
set trustpoint	VTI トンネル接続の開始時に使用する証明書を定義するトラストポイントを指定します。

crypto ipsec security-association lifetime

グローバル ライフタイム値を設定するには、グローバル コンフィギュレーション モードで **crypto ipsec security-association lifetime** コマンドを使用します。グローバル ライフタイム値をデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

crypto ipsec security-association lifetime {**seconds** *number* | **kilobytes** {*number* | **unlimited**}}

no crypto ipsec security-association lifetime {**seconds** *number* | **kilobytes** {*number* | **unlimited**}}

構文の説明

kilobytes {*number* | **unlimited**}	所定のセキュリティ アソシエーションの有効期限が切れるまでに、そのセキュリティ アソシエーションを使用してピア間を通過できるトラフィックの量を KB 単位で指定します。指定できる範囲は 10 ～ 2147483647 KB です。デフォルトは 4,608,000 KB です。 この設定は、リモート アクセス VPN 接続には適用されません。サイト間 VPN のみに適用されます。
seconds *number*	セキュリティ アソシエーションの有効期限が切れるまでの存続時間（秒数）を指定します。指定できる範囲は 120 ～ 214783647 秒です。デフォルトは 28,800 秒（8 時間）です。 この設定は、リモート アクセスとサイト間 VPN の両方に適用されます。
unlimited	ASA がトンネルの発信側である場合に、クイック モードの 1 パケットでキロバイトを送信しません。

デフォルト

デフォルトの KB 数は 4,608,000 で、デフォルトの秒数は 28,800 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.1(2)	**unlimited** 引数が追加されました。

使用上のガイドライン

crypto ipsec security-association lifetime コマンドは、IPsec セキュリティ アソシエーションのネゴシエート時に使用されるグローバル ライフタイム値を変更します。

IPsec セキュリティ アソシエーションでは、共有秘密キーが使用されます。これらのキーとセキュリティ アソシエーションは、両方同時にタイムアウトになります。

個々のクリプト マップ エントリでライフタイム値が設定されていない場合、ASA は、ネゴシエート中に新しいセキュリティ アソシエーションを要求するときに、ピアへの要求の中でグローバル ライフタイム値を指定します。セキュリティ アプライアンスは、この値を新しいセキュリティ アソシエーションのライフタイムとして使用します。ASA は、ピアからネゴシエーション要求を受信すると、ピアが指定するライフタイム値またはローカルに設定されたライフタイム値のうち、小さい方を新しいセキュリティ アソシエーションのライフタイムとして使用します。

サイト間 VPN 接続の場合、「時間指定」と「トラフィック量」の 2 つのライフタイムがあります。これらのライフタイムのいずれかに最初に到達すると、セキュリティ アソシエーションが期限切れになります。リモート アクセス VPN セッションでは、指定時刻ライフタイムのみが適用されます。

ASA では、クリプト マップ、ダイナミック マップ、および IPsec 設定を動作中に変更できます。変更された場合、ASA では、変更によって影響を受ける接続のみが切断されます。クリプト マップに関連付けられている既存のアクセス リストをユーザが変更した場合（たとえばアクセス リスト内のエントリを削除した場合）、関連する接続のみが切断されます。アクセス リスト内の他のエントリに基づく接続は、影響を受けません。

グローバルな指定時刻ライフタイムを変更するには、**crypto ipsec security-association lifetime seconds** コマンドを使用します。指定時刻ライフタイムを使用すると、指定した秒数が経過した後にセキュリティ アソシエーションがタイムアウトします。

グローバル トラフィック量ライフタイムを変更するには、**crypto ipsec security-association lifetime kilobytes** コマンドを使用します。トラフィック量ライフタイムを使用すると、指定した量のトラフィック（KB 単位）がセキュリティ アソシエーション キーによって保護された後に、セキュリティ アソシエーションがタイムアウトします。

ライフタイムを短くするほど、同一キーで暗号化されている解析対象データが少なくなるため、攻撃者はキー回復攻撃を開始することが難しくなります。ただし、ライフタイムを短くするほど、新しいセキュリティ アソシエーションの確立にかかる CPU 処理時間が長くなります。

セキュリティ アソシエーション（および対応するキー）は、指定した秒数または指定したトラフィック量（KB 単位）のうち、いずれかを最初に超えた時点で有効期限が切れます。

例

次に、セキュリティ アソシエーションのグローバル指定時刻ライフタイムを指定する例を示します。

```
ciscoasa(config)# crypto ipsec-security association lifetime seconds 240
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	グローバル ライフタイム、トランスフォーム セットなど、すべての IPsec コンフィギュレーションをクリアします。
show running-config crypto map	すべてのクリプト マップのすべてのコンフィギュレーションを表示します。

crypto ipsec security-association pmtu-aging

パス最大伝送単位（PMTU）のエージングをイネーブルにするには、グローバル コンフィギュレーション モードで **crypto ipsec security-association pmtu-aging** コマンドを使用します。PMTU エージングをディセーブルにするには、このコマンドの no 形式を使用します。

crypto ipsec security-association pmtu-aging *reset-interval*

no crypto ipsec security-association pmtu-aging *reset-interval*

構文の説明

reset-interval	PMTU 値がリセットされる間隔を設定します。

デフォルト

この機能は、デフォルトでイネーブルにされています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

リセット間隔は秒単位で指定します。

crypto ipsec security-association replay

IPsec アンチリプレイ ウィンドウ サイズを設定するには、グローバル コンフィギュレーション モードで **crypto ipsec security-association replay** コマンドを使用します。ウィンドウ サイズをデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

crypto ipsec security-association replay {**window-size** *n* | **disable**}

no crypto ipsec security-association replay {**window-size** *n* | **disable**}

構文の説明

n	ウィンドウ サイズを設定します。指定できる値は、64、128、256、512、または 1024 です。デフォルトは 64 です。
disable	アンチリプレイ チェックをディセーブルにします。

デフォルト

デフォルトのウィンドウ サイズは 64 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(4)/8.0(4)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

Cisco IPsec 認証では、暗号化されたパケットそれぞれに対して固有のシーケンス番号を割り当てることによって、暗号化されたパケットを複製する攻撃者に対するアンチリプレイ保護が提供されます(セキュリティ アソシエーション アンチリプレイは、受信側がリプレイ攻撃から自身を保護するために、古いパケットまたは重複パケットを拒否できるセキュリティ サービスです)。復号機能によって、以前に認識したシーケンス番号が除外されます。エンクリプタによって、シーケンス番号が昇順で割り当てられます。すでに検出されている最も高いシーケンス番号である値 X はデクリプタによって記録されます。また、デクリプタによって、X-N+1 ～ X(N はウィンドウ サイズ)までのシーケンス番号を持つパケットが検出されているかどうかも記録されます。シーケンス番号 X-N を持つすべてのパケットが廃棄されます。現在、N は 64 に設定されているため、デクリプタによって追跡できるパケットは 64 までです。

ただし、64 パケット ウィンドウ サイズでは不十分な場合があります。たとえば、QoS はプライオリティが高いパケットを優先しますが、これにより、プライオリティが低いパケットが、デクリプタによって受信された最後の 64 パケットの 1 つであっても、廃棄される場合があります。このイベントにより、誤ったアラームである警告 syslog メッセージが生成される可能性があります。**crypto ipsec security-association replay** コマンドを使用すると、ウィンドウ サイズを拡張して、デクリプタが 64 を超えるパケットを追跡できます。

アンチリプレイ ウィンドウ サイズを増やしても、スループットおよびセキュリティに影響はありません。メモリへの影響は限定的です。デクリプタ上にシーケンス番号を保管するために必要となるのは、着信 IPsec SA ごとに追加の 128 バイトだけであるためです。今後アンチリプレイに関する問題が発生しないように、最大のウィンドウ サイズである 1024 を使用することを推奨します。

例

次に、セキュリティ アソシエーションのアンチリプレイ ウィンドウ サイズを指定する例を示します。

```
ciscoasa(config)# crypto ipsec security-association replay window-size 1024
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	グローバル ライフタイム、トランスフォーム セットなど、すべての IPsec コンフィギュレーションをクリアします。
shape	トラフィック シェーピングをイネーブルにします。
priority	プライオリティ キューイングをイネーブルにします。
show running-config crypto map	すべてのクリプト マップのすべてのコンフィギュレーションを表示します。

CHAPTER 10

crypto isakmp disconnect-notify コマンド～ cxsc auth-proxy port コマンド

crypto isakmp disconnect-notify

ピアに対する切断通知をイネーブルにするには、グローバル コンフィギュレーション モードで **crypto isakmp disconnect-notify** コマンドを使用します。切断通知をディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto isakmp disconnect-notify

no crypto isakmp disconnect-notify

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルト値は [disabled] です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	**isakmp disconnect-notify** コマンドが追加されました。
7.2.(1)	**isakmp disconnect-notify** コマンドが、**crypto isakmp disconnect-notify** コマンドに置き換えられました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

次の削除理由を使用して、ピアに対する切断通知をイネーブルにできます。

- IKE_DELETE_RESERVED = 0
  無効なコード。送信しません。
- IKE_DELETE_BY_ERROR = 1
  タイムアウトの伝送エラー、またはキープアライブやその他の IKE パケット ACK に対する応答が予期されるときに発生した障害。デフォルトのテキストは「Connectivity to client lost.」です。
- IKE_DELETE_BY_USER_COMMAND = 2
  SA は、ユーザまたは管理者の手動による介入によって削除されました。デフォルトのテキストは「Manually Disconnected by Administrator.」です。
- IKE_DELETE_BY_EXPIRED_LIFETIME = 3
  SA の期限が切れています。デフォルトのテキストは「Maximum Configured Lifetime Exceeded.」です。
- IKE_DELETE_NO_ERROR = 4
  不明なエラーにより削除されました。
- IKE_DELETE_SERVER_SHUTDOWN = 5
  サーバをシャットダウンしています。
- IKE_DELETE_SERVER_IN_FLAMES = 6
  サーバに重大な問題があります。デフォルトのテキストは「Peer is having heat problems.」です。
- IKE_DELETE_MAX_CONNECT_TIME = 7
  アクティブなトンネルの最大許容時間が経過しました。EXPIRED_LIFETIME とは異なり、この理由は、この 1 つの SA だけでなく、IKE ネゴシエート/制御されたトンネル全体が切断されることを示します。デフォルトのテキストは「Maximum Configured Connection Time Exceeded.」です。
- IKE_DELETE_IDLE_TIMEOUT = 8
  トンネルがアイドル状態のまま最大許容時間が経過しました。そのため、この 1 つの SA だけでなく、IKE ネゴシエートされたトンネル全体が切断されます。デフォルトのテキストは「Maximum Idle Time for Session Exceeded.」です。
- IKE_DELETE_SERVER_REBOOT = 9
  サーバを再起動しています。
- IKE_DELETE_P2_PROPOSAL_MISMATCH = 10
  Phase2 プロポーザルの不一致。
- IKE_DELETE_FIREWALL_MISMATCH = 11
  ファイアウォール パラメータの不一致。
- IKE_DELETE_CERT_EXPIRED = 12
  ユーザ認定が必要です。デフォルトのメッセージは「User or Root Certificate has Expired.」です。
- IKE_DELETE_CLIENT_NOT_ALLOWED = 13
  許可されていないクライアント タイプまたはバージョン。
- IKE_DELETE_FW_SERVER_FAIL = 14
  Zone Integrity サーバに接続できませんでした。
- IKE_DELETE_ACL_ERROR = 15
  AAA からダウンロードされた ACL は挿入できません。デフォルトのメッセージは「ACL parsing error.」です。

例

次の例では、グローバル コンフィギュレーション モードで、ピアに対する切断通知をイネーブルにします。

```
ciscoasa(config)# crypto isakmp disconnect-notify
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp identity

フェーズ 1 ID をピアに送信するように設定するには、グローバル コンフィギュレーション モードで **crypto isakmp identity** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

crypto isakmp identity {**address** | **hostname** | **key-id** *key-id-string* | **auto**}

no crypto isakmp identity {**address** | **hostname** | **key-id** *key-id-string* | **auto**}

構文の説明

address	ISAKMP の識別情報を交換するホストの IP アドレスを使用します。
auto	ISAKMP ネゴシエーションを、接続のタイプ（事前共有キーの IP アドレス、または証明書認証用の証明書 DN）によって判別します。
hostname	ISAKMP 識別情報を交換するホストの完全修飾ドメイン名を使用します（デフォルト）。この名前は、ホスト名とドメイン名で構成されます。
key-id *key_id_string*	リモート ピアが事前共有キーを検索するために使用するストリングを指定します。

デフォルト

デフォルトの ISAKMP ID は、**crypto isakmp identity auto** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	**isakmp identity** コマンドが追加されました。
7.2(1)	**isakmp identity** コマンドが、**crypto isakmp identity** コマンドに置き換えられました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次の例では、グローバル コンフィギュレーション モードで、接続タイプに応じて、IPsec ピアと通信するためのインターフェイス上で ISAKMP ネゴシエーションをイネーブルにします。

```
ciscoasa(config)# crypto isakmp identity auto
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp nat-traversal

NAT トラバーサルをグローバルにイネーブルにするには、グローバル コンフィギュレーション モードで ISAKMP がイネーブルになっていることを確認します(イネーブルにするには **crypto isakmp enable** コマンドを使用します)。NAT トラバーサルをディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto isakmp nat-traversal *natkeepalive*

no crypto isakmp nat-traversal *natkeepalive*

構文の説明

natkeepalive	NAT キープアライブ間隔を、10 ～ 3600 秒の範囲で設定します。デフォルトは 20 秒です。

デフォルト

デフォルトでは、NAT トラバーサルはイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	**isakmp nat-traversal** コマンドが追加されました。
7.2.(1)	**isakmp nat-traversal** コマンドが、**crypto isakmpnat-traversal** コマンドに置き換えられました。
8.0(2)	NAT トラバーサルが、デフォルトでイネーブルになりました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

NAT(PAT を含む)は、IPsec も使用されている多くのネットワークで使用されていますが、IPsec パケットが NAT デバイスを正常に通過することを妨げる非互換性が数多くあります。NAT トラバーサルを使用すると、ESP パケットが 1 つ以上の NAT デバイスを通過できるようになります。

ASA は、IETF の「UDP Encapsulation of IPsec Packets」ドラフトのバージョン 2 とバージョン 3 (http://www.ietf.org/html.charters/ipsec-charter.html から入手可能)に記述されているとおりに NAT トラバーサルをサポートしています。また、ダイナミック クリプト マップとスタティック クリプト マップの両方で NAT トラバーサルをサポートしています。

このコマンドは、ASA 上で NAT-T をグローバルにイネーブルにします。クリプト マップ エントリでディセーブルにするには、**crypto map set nat-t-disable** コマンドを使用します。

例

次に、グローバル コンフィギュレーション モードで、ISAKMP をイネーブルにし、NAT トラバーサルのキープアライブ間隔を 30 秒に設定する例を示します。

```
ciscoasa(config)# crypto isakmp enable
ciscoasa(config)# crypto isakmp nat-traversal 30
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp policy authentication

IKE ポリシー内の認証方式を指定するには、グローバル コンフィギュレーション モードで **crypto isakmp policy authentication** コマンドを使用します。ISAKMP 認証方式を削除するには、関連する **clear configure** コマンドを使用します。

crypto isakmp policy *priority* **authentication** {**crack** | **pre-share** | **rsa-sig**}

構文の説明

crack	認証方式として、IKE CRACK を指定します。
pre-share	認証方式として事前共有キーを指定します。
priority	IKE ポリシーを一意に識別し、そのポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。
rsa-sig	認証方式として RSA シグニチャを指定します。 RSA シグニチャにより、IKE ネゴシエーションに対して否認防止を実行できます。これは基本的に、ユーザがピアとの IKE ネゴシエーションを行ったかどうかを、第三者に証明できることを意味します。

デフォルト

デフォルトの ISAKMP ポリシー認証は **pre-share** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**isakmp policy authentication** コマンドが追加されました。
7.2.(1)	**isakmppolicy authentication** コマンドが、**crypto isakmppolicy authentication** コマンドに置き換えられました。

使用上のガイドライン

IKE ポリシーは、IKE ネゴシエーション用のパラメータのセットを定義したものです。

RSA シグニチャを指定する場合は、CA サーバから証明書を取得するように ASA とそのピアを設定する必要があります。事前共有キーを指定する場合は、ASA とそのピアに、事前共有キーを別々に設定する必要があります。

例

次に、グローバル コンフィギュレーション モードで、**crypto isakmp policy authentication** コマンドを使用する例を示します。この例では、プライオリティ番号 40 の IKE ポリシーで RSA シグネチャの認証方式を使用するように設定します。

```
ciscoasa(config)# crypto isakmp policy 40 authentication rsa-sig
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp policy encryption

IKE ポリシーで使用する暗号化アルゴリズムを指定するには、グローバル コンフィギュレーション モードで **crypto isakmp policy encryption** コマンドを使用します。暗号化アルゴリズムをデフォルト値の **des** にリセットするには、このコマンドの **no** 形式を使用します。

crypto isakmp policy *priority* **encryption** {**aes** | **aes-192** | **aes-256** | **des** | **3des**}

no crypto isakmp policy *priority* **encryption** {**aes** | **aes-192** | **aes-256** | **des** | **3des**}

構文の説明

3des	IKE ポリシーで、Triple DES 暗号化アルゴリズムを使用することを指定します。
aes	IKE ポリシーで使用する暗号化アルゴリズムが、128 ビット キーを使用する AES であることを指定します。
aes-192	IKE ポリシーで使用する暗号化アルゴリズムが、192 ビット キーを使用する AES であることを指定します。
aes-256	IKE ポリシーで使用する暗号化アルゴリズムが、256 ビット キーを使用する AES であることを指定します。
des	IKE ポリシーで使用する暗号化アルゴリズムが、56 ビット DES-CBC であることを指定します。
priority	IKE ポリシーを一意に識別し、そのポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。

デフォルト

デフォルトの ISAKMP ポリシー暗号化は、**3des** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**isakmp policy encryption** コマンドが追加されました。
7.2.(1)	**isakmp policy encryption** コマンドが、**crypto isakmp policy encryption** コマンドに置き換えられました。

例

次に、グローバル コンフィギュレーション モードで、**crypto isakmp policy encryption** コマンドを使用する例を示します。この例では、プライオリティ番号 25 の IKE ポリシーに使用するアルゴリズムとして 128 ビット キーの AES 暗号化を設定します。

```
ciscoasa(config)# crypto isakmp policy 25 encryption aes
```

次に、グローバル コンフィギュレーション モードでの入力で、プライオリティ番号 40 の IKE ポリシー内で 3DES アルゴリズムを使用するように設定する例を示します。

```
ciscoasa(config)# crypto isakmp policy 40 encryption 3des
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp policy group

IKE ポリシーに対して Diffie-Hellman グループを指定するには、グローバル コンフィギュレーション モードで **crypto isakmp policy group** コマンドを使用します。Diffie-Hellman グループ ID をデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

crypto isakmp policy *priority* **group** {**1** | **2** | **5**}

no crypto isakmp policy *priority* **group**

構文の説明

group 1	IKE ポリシーで、768 ビットの Diffie-Hellman グループを使用することを指定します。これはデフォルト値です。
group 2	IKE ポリシーで、1024 ビットの Diffie-Hellman グループ 2 を使用することを指定します。
group 5	IKE ポリシーで、1536 ビットの Diffie-Hellman グループ 5 を使用することを指定します。
priority	IIKE ポリシーを一意に識別し、そのポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。

デフォルト

デフォルトのグループ ポリシーはグループ 2 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**isakmp policy group** コマンドが追加されました。
7.2.(1)	**isakmp policy group** コマンドが、**crypto isakmppolicy group** コマンドに置き換えられました。
8.0(4)	**group 7** コマンド オプションは廃止されました。グループ 7 を設定しようとするとエラー メッセージが生成され、代わりにグループ 5 が使用されます。

使用上のガイドライン

IKE ポリシーは、IKE ネゴシエーション時に使用するパラメータのセットを定義したものです。

グループ オプションには、768 ビット（DH グループ 1）、1024 ビット（DH グループ 2）、および 1536 ビット（DH グループ 5）の 3 つがあります。1024 ビットと 1536 ビットの Diffie-Hellman グループは、セキュリティが高くなりますが、CPU の処理時間は長くなります。

（注） Cisco VPN Client のバージョン 3.x 以上では、ISAKMP ポリシーで DH グループ 2 を使用する必要があります（DH グループ 1 に設定すると、Cisco VPN Client は接続できません）。

AES は、VPN-3DES のライセンスがある ASA に限りサポートされます。AES では大きなキー サイズが提供されるため、ISAKMP ネゴシエーションでは Diffie-Hellman（DH）グループ 1 やグループ 2 ではなく、グループ 5 を使用する必要があります。グループ 5 を設定するには、**crypto isakmp policy priority group 5** コマンドを使用します。

例

次に、グローバル コンフィギュレーション モードで、**crypto isakmp policy group** コマンドを使用する例を示します。この例では、プライオリティ番号 40 の IKE ポリシーに対し、グループ 2、1024 ビットの Diffie Hellman を使用するように設定しています。

```
ciscoasa(config)# crypto isakmp policy 40 group 2
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp policy hash

IKE ポリシーのハッシュ アルゴリズムを指定するには、グローバル コンフィギュレーション モードで **crypto isakmp policy hash** コマンドを使用します。ハッシュ アルゴリズムをデフォルト値の SHA-1 にリセットするには、このコマンドの **no** 形式を使用します。

crypto isakmp policy *priority* hash {**md5** | **sha**}

no crypto isakmp policy *priority* **hash**

構文の説明

md5	IKE ポリシーのハッシュ アルゴリズムとして MD5（HMAC バリアント）を指定します。
priority	プライオリティをポリシーに一意に指定および割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。
sha	IKE ポリシーのハッシュ アルゴリズムとして SHA-1（HMAC バリアント）を指定します。

デフォルト

デフォルトのハッシュ アルゴリズムは SHA-1（HMAC バリアント）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**isakmp policy hash** コマンドが追加されました。
7.2.(1)	**isakmp policy hash** コマンドが、**crypto isakmp policy hash** コマンドに置き換えられました。

使用上のガイドライン

IKE ポリシーは、IKE ネゴシエーション時に使用するパラメータのセットを定義したものです。

ハッシュ アルゴリズムのオプションには、SHA-1 と MD5 の 2 つがあります。MD5 のダイジェストの方が小さく、SHA-1 よりもやや速いと見なされています。

例

次に、グローバル コンフィギュレーション モードで、**crypto isakmp policy hash** コマンドを使用する例を示します。この例では、プライオリティ番号 40 の IKE ポリシーに MD5 ハッシュ アルゴリズムを使用することを指定します。

```
ciscoasa(config)# crypto isakmp policy 40 hash md5
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp policy lifetime

IKE セキュリティ アソシエーションが期限切れになるまでのライフタイムを指定するには、グローバル コンフィギュレーション モードで **crypto isakmp policy lifetime** コマンドを使用します。セキュリティ アソシエーションのライフタイムをデフォルト値の 86,400 秒（1 日）にリセットするには、このコマンドの **no** 形式を使用します。

crypto isakmp policy *priority* **lifetime** *seconds*

no crypto isakmp policy *priority* **lifetime**

構文の説明

priority	IKE ポリシーを一意に識別し、そのポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。
seconds	各セキュリティ アソシエーションが期限切れになるまでの秒数を指定します。有限のライフタイムを提示するには、120 ～ 2147483647 秒の整数を使用します。無制限のライフタイムの場合は、0 秒を使用します。

デフォルト

デフォルト値は 86,400 秒（1 日）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**isakmp policy lifetime** コマンドが追加されました。
7.2.(1)	**isakmp policy lifetime** コマンドが、**crypto isakmp policy lifetime** コマンドに置き換えられました。

使用上のガイドライン

IKE は、ネゴシエーションを開始するとき、自身のセッション用のセキュリティ パラメータについて合意しようとします。次に、各ピアのセキュリティ アソシエーションが、合意されたパラメータを参照します。ピアは、ライフタイムが期限切れになるまで、セキュリティ アソシエーションを保持します。ピアがライフタイムを提示していない場合は、無限のライフタイムを指定できます。セキュリティ アソシエーションは、期限切れになるまで、その後の IKE ネゴシエーションで利用できるため、新しい IPsec セキュリティ アソシエーションを設定するときに時間を節約できます。ピアは、現在のセキュリティ アソシエーションが期限切れになる前に、新しいセキュリティ アソシエーションをネゴシエートします。

ライフタイムを長くするほど、ASA は以後の IPSec セキュリティ アソシエーションをより迅速にセットアップします。暗号化強度は十分なレベルにあるため、キーの再生成間隔を極端に短く（約 2 ～ 3 分ごとに）しなくてもセキュリティは保証されます。デフォルトをそのまま使用することを推奨します。

（注） IKE セキュリティ アソシエーションのライフタイムが無限に設定されている場合、ピアが有限のライフタイムを提示したときは、ピアからネゴシエートされた有限のライフタイムが使用されます。

例

次に、グローバル コンフィギュレーション モードで、プライオリティ番号 40 の IKE ポリシーに IKE セキュリティ アソシエーションのライフタイムを 50,400 秒（14 時間）に設定する例を示します。

```
ciscoasa(config)# crypto isakmp policy 40 lifetime 50400
```

次に、グローバル コンフィギュレーション モードでの入力で、IKE セキュリティ アソシエーションのライフタイムを無限に設定する例を示します。

```
ciscoasa(config)# crypto isakmp policy 40 lifetime 0
```

関連コマンド

clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp reload-wait

すべてのアクティブなセッションが自発的に終了しないと ASA をリブートできないようにするは、グローバル コンフィギュレーション モードで **crypto isakmp reload-wait** コマンドを使用します。アクティブなセッションが終了するのを待たずに ASA をリブートするには、このコマンドの **no** 形式を使用します。

crypto isakmp reload-wait

no crypto isakmp reload-wait

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	**isakmp reload-wait** コマンドが追加されました。
7.2.(1)	**isakmp reload-wait** コマンドが、**crypto isakmpreload-wait** コマンドに置き換えられました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、グローバル コンフィギュレーション モードを開始し、すべてのアクティブ セッションが終了するまで待機してからリブートすることを ASA に指示する例を示します。

```
ciscoasa(config)# crypto isakmp reload-wait
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。

コマンド	説明
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto key generate

アイデンティティ証明書用のキー ペアを生成するには、グローバル コンフィギュレーション モードで **crypto key generate** コマンドを使用します。このコマンドは、RSA と楕円曲線署名アルゴリズム（ECDSA）キーによって異なります。

crypto key generate rsa [**usage-keys** | **general-keys**] [**label** *key-pair-label*] [**modulus** *size*] [**noconfirm**]

crypto key generate ecdsa [**label** *key-pair-label*] **elliptic-curve** [**256** | **384** | **521**] [**noconfirm**]

構文の説明

dsa [**label name**]	キー ペアの生成時に Suite-B EDCSA アルゴリズムを使用します。
elliptic-curve [**256** | **384** | **521**]	スイート B EDCSA キー ペアのビット長を指定します。デフォルト値は 384 です。
general-keys	1 つの汎用キー ペアを生成します。これはデフォルトのキー ペア タイプです。
label *key-pair-label*	キー ペアに関連付ける名前を指定します。このキー ペアのラベルは一意である必要があります。ラベルを指定しない場合、キー ペアは静的に Default-RSA-Key または Default-ECDSA-Key という名前になります。
modulus *size*	キー ペアのモジュラス サイズ（512、768、1024、2048、3072 および 4096）を指定します。デフォルトのモジュラス サイズは 2048 です。
noconfirm	すべての対話型プロンプトを非表示にします。
usage-keys	シグニチャ用と暗号化用の 2 つのキー ペアを生成します。これは、対応する識別用に 2 つの証明書が必要なことを意味します。

デフォルト

デフォルトの RSA キー ペアのタイプは、**general key** です。デフォルトのモジュラス サイズは 2048 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	ECDSA キーのサポートが追加されました。
9.9(2)	モジュラス サイズを 3072 に設定できるようになりました。

使用上のガイドライン

SSL、SSH、および IPsec 接続をサポートするためにキー ペアを生成するには、**crypto key generate** コマンドを使用します。生成されたキー ペアは、コマンド構文の一部として指定できるラベルで識別されます。キー ペアを参照しないトラストポイントは、デフォルトの Default-RSA-Key を使用できます。SSH 接続では常にこのキーが使用されます。SSL は独自の証明書やキーをダイナミックに生成するため、証明書やキーがトラストポイントに設定されていない限り、このことは SSL に影響を与えません。

例

次に、ラベル mypubkey を持つ RSA キー ペアを生成する例を示します。

```
ciscoasa(config)# crypto key generate rsa label mypubkey
INFO: The name for the keys will be: mypubkey
Keypair generation process
ciscoasa(config)#
```

次に、デフォルトのラベルを持つ RSA キー ペアを生成する例を示します。

```
ciscoasa(config)# crypto key generate rsa
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
ciscoasa(config)#
```

次に、ECDSA キーを生成する例を示します。RSA キーペアを保存するための十分なスペースがないため警告メッセージが表示されます。

```
ciscoasa(config)# crypto key generate ecdsa label new-ecdsa-key elliptic-curve 521
INFO: The name for the keys will be: new-ecdsa-key
Keypair generation process begin. Please wait...
```

関連コマンド

コマンド	説明
crypto key zeroize	キー ペアを削除します。
show crypto key	キー ペアを表示します。

crypto key zeroize

指定したタイプのキー ペアを削除するには、グローバル コンフィギュレーション モードで **crypto key zeroize** コマンドを使用します。

crypto key zeroize {**rsa** | **ecdsa**} [**label** *key-pair-label*] [**default**] [**noconfirm**]

構文の説明

default	指定されたタイプのデフォルトのキー ペアを削除します。
ecdsa	キー タイプとして ECDSA を指定します。
label *key-pair-label*	削除するキー ペアを識別します。ラベルを指定しない場合、システムは、指定されたタイプのキー ペアをすべて削除します。
noconfirm	すべての対話型プロンプトを非表示にします。
rsa	キー タイプとして RSA を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	ECDSA のサポートが追加されました。

例

次に、グローバル コンフィギュレーション モードで、すべての RSA キー ペアを削除する例を示します。

```
ciscoasa(config)# crypto key zeroize rsa
WARNING: All RSA keys will be removed.
WARNING: All router certs issued using these keys will also be removed.

Do you really want to remove these keys? [yes/no] y
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto key generate	アイデンティティ証明書用のキー ペアを生成します。

crypto large-cert-acceleration enable（廃止）

ASA がハードウェアで 2048 ビットの RSA キー演算を実行できるようにするには、グローバル コンフィギュレーション モードで **crypto large-cert-acceleration enable** コマンドを使用します。ソフトウェアで 2048 ビットの RSA キー演算を実行するには、**no crypto large-cert-acceleration enable** コマンドを使用します。

crypto large-cert-acceleration enable

no crypto large-cert-acceleration enable

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトでは、2048 ビットの RSA キー演算がソフトウェアで実行されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(3)	このコマンドが追加されました。
8.2(5)	このコマンドは廃止されました。**crypto engine large-mod-accel** コマンドに置き換えられました。

使用上のガイドライン

このコマンドは、ASA 5510、ASA 5520、ASA 5540、および ASA 5550 でのみ使用できます。このコマンドは、ASA 5580 では使用できません。

例

次に、2048 ビットの RSA キー演算がハードウェアでイネーブルになっている例を示します。

```
ciscoasa (config)# show running-config crypto large-cert-acceleration
crypto large-cert-acceleration enable
ciscoasa (config)#
```

関連コマンド

コマンド	説明
clear configure crypto	2048 ビットの RSA キー コンフィギュレーションを、残りのクリプト コンフィギュレーションとともにクリアします。
show running-config crypto	2048 ビットの RSA キー コンフィギュレーションを、残りのクリプト コンフィギュレーションとともに表示します。

crypto map interface

以前に定義したクリプト マップ セットをインターフェイスに適用するには、グローバル コンフィギュレーション モードで **crypto map interface** コマンドを使用します。このクリプト マップ セットをインターフェイスから削除するには、このコマンドの **no** 形式を使用します。

crypto map *map-name* **interface** *interface-name* [**ipv6-local-address** *ipv6-address*]

no crypto map *map-name* **interface** *interface-name* [**ipv6-local-address** *ipv6-address*]

構文の説明

interface-name	ASA が VPN ピアとのトンネルの確立に使用するインターフェイスを指定します。ISAKMP がイネーブルになっており、CA を使用して証明書を取得する場合は、CA 証明書で指定されているアドレスを持つインターフェイスにする必要があります。
map-name	クリプト マップ セットの名前を指定します。
ipv6-local-address *ipv6-address*	IPv6 アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.3(1)	**ipv6-local-address** キーワードが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

このコマンドを使用して、クリプト マップ セットを任意のアクティブな ASA のインターフェイスに割り当てます。ASA では、あらゆるアクティブ インターフェイスを IPsec の終端にすることができます。インターフェイスで IPSec サービスを提供するには、事前にそのインターフェイスにクリプト マップ セットを割り当てる必要があります。

インターフェイスに割り当てることができるクリプト マップ セットは 1 つだけです。同じマップ名でシーケンス番号が異なるクリプト マップ エントリが複数ある場合、それらのエントリは同じセットの一部であり、そのインターフェイスにすべて適用されます。ASA は、シーケンス番号が最も小さいクリプト マップ エントリを最初に評価します。

インターフェイスに複数の IPv6 アドレスが設定されており、IPv6 環境で LAN-to-LAN VPN トンネルをサポートするように ASA を設定する場合、**ipv6-local-address** キーワードを使用します。

(注) ASA では、クリプト マップ、ダイナミック マップ、および IPSec 設定を、オンザフライで変更できます。設定を変更する場合、変更によって影響を受ける接続のみが ASA によって停止させられます。たとえば、アクセス リスト内のエントリを削除して、クリプト マップに関連付けられた既存のアクセス リストを変更した場合、関連する接続だけがダウンします。アクセス リスト内の他のエントリに基づく接続は、影響を受けません。

すべてのスタティック クリプトマップでは、アクセス リスト、トランスフォーム セット、および IPsec ピアという 3 つの部分を定義する必要があります。これらの 1 つが欠けている場合、そのクリプト マップは不完全であるため、ASA は次のエントリに進みます。ただし、クリプト マップがアクセス リストと一致し、他の 2 つの要件のいずれか、または両方と一致しない場合には、ASA はトラフィックを廃棄します。

すべてのクリプト マップが完全であることを確認するには、**show running-config crypto map** コマンドを使用します。不完全なクリプト マップを修正するには、クリプト マップを削除し、欠けているエントリを追加してからクリプト マップを再適用します。

例

次に、グローバル コンフィギュレーション モードで、mymap という名前のクリプト マップ セットを外部インターフェイスに割り当てる例を示します。トラフィックは、この outside インターフェイスを通過するとき、ASA によって mymap セット内のすべてのクリプト マップ エントリを使用して評価されます。発信トラフィックが、いずれかの mymap クリプト マップ エントリのアクセス リストと一致する場合、ASA はそのクリプト マップ エントリのコンフィギュレーションを使用して、セキュリティ アソシエーションを形成します。

```
ciscoasa(config)# crypto map mymap interface outside
```

次に、必要最小限のクリプト マップ エントリ コンフィギュレーションの例を示します。

```
ciscoasa(config)# crypto map mymap 10 ipsec-isakmp
ciscoasa(config)# crypto map mymap 10 match address 101
ciscoasa(config)# crypto map mymap set transform-set my_t_set1
ciscoasa(config)# crypto map mymap set peer 10.0.0.1
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map ipsec-isakmp dynamic

所定のクリプト マップ エントリで既存のダイナミック クリプト マップを参照させるようにするには、グローバル コンフィギュレーション モードで **crypto map ipsec-isakmp dynamic** コマンドを使用します。クロス リファレンスを削除するには、このコマンドの **no** 形式を使用します。

ダイナミック クリプト マップ エントリを作成するには、**crypto dynamic-map** コマンドを使用します。ダイナミック クリプト マップ セットを作成した後に、**crypto map ipsec-isakmp dynamic** コマンドを使用して、ダイナミック クリプト マップ セットをスタティック クリプト マップに追加します。

crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

no crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

構文の説明

dynamic-map-name	既存のダイナミック クリプト マップを参照するクリプト マップ エントリの名前を指定します。
ipsec-isakmp	IKE がクリプト マップ エントリの IPsec セキュリティ アソシエーションを確立することを指定します。
map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**ipsec-manual** キーワードを削除するように変更されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

クリプト マップ エントリを定義してから、**crypto map interface** コマンドを使用して、ダイナミック クリプト マップ セットをインターフェイスに割り当てることができます。

ダイナミック クリプト マップを使用することで、保護の対象となるトラフィックのフィルタリングと分類、そのトラフィックに適用するポリシーの定義という 2 つの機能を利用できます。最初の機能はインターフェイス上のトラフィック フローが対象となり、2 番めの機能はそのトラフィックのために（IKE を通じて）実行されるネゴシエーションが対象となります。

IPsec ダイナミック クリプト マップでは、次のことを指定します。

- 保護するトラフィック
- セキュリティ アソシエーションを確立する IPsec ピア
- 保護対象のトラフィックとともに使用するトランスフォーム セット
- キーおよびセキュリティ アソシエーションの使用方法または管理方法

クリプト マップ セットとは、それぞれ異なるシーケンス番号（*seq-num*）を持つが、マップ名が同じであるクリプト マップ エントリの集合です。したがって、所定のインターフェイスで、あるトラフィックには指定のセキュリティを適用してピアに転送し、その他のトラフィックには別の IPsec セキュリティを適用して同じまたは別のピアに転送できます。これを行うには、マップ名は同じであるが、シーケンス番号がそれぞれ異なる 2 つのクリプト マップ エントリを作成します。

seq-num 引数として割り当てる番号は、任意に決定しないでください。この番号によって、クリプト マップ セット内の複数のクリプト マップ エントリにランクが付けられます。小さいシーケンス番号のクリプト マップ エントリは、大きいシーケンス番号のマップ エントリよりも先に評価されます。つまり、番号の小さいマップ エントリの方がプライオリティが高くなります。

（注） クリプト マップをダイナミック クリプト マップにリンクする場合は、ダイナミック クリプト マップを指定する必要があります。指定すると、**crypto dynamic-map** コマンドを使用して以前に定義した既存のダイナミック クリプト マップにクリプト マップがリンクされます。クリプト マップ エントリが変換された後に加えた変更は、有効になりません。たとえば、set peer 設定への変更は有効になりません。ただし、ASA は起動中に変更を保存します。ダイナミック クリプト マップをクリプト マップに変換して戻す場合、この変更は有効となり、**show running-config crypto map** コマンドの出力に表示されます。ASA は、リブートされるまでこれらの設定を維持します。

例

次に、グローバル コンフィギュレーション モードで、mymap というクリプト マップが test というダイナミック クリプト マップを参照するように設定する例を示します。

```
ciscoasa(config)# crypto map mymap ipsec-isakmp dynamic test
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map match address

アクセス リストをクリプト マップ エントリに割り当てるには、グローバル コンフィギュレーション モードで **crypto map match address** コマンドを使用します。クリプト マップ エントリからアクセス リストを削除するには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **match address** *acl_name*

no crypto map *map-name seq-num* **match address** *acl_name*

構文の説明

acl_name	暗号化アクセス リストの名前を指定します。この名前は、一致対象となる名前付き暗号化アクセス リストの名前引数と一致している必要があります。
map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

このコマンドは、すべてのスタティック クリプトマップに対して必要です。**crypto dynamic-map** コマンドを使用してダイナミック クリプト マップを定義する場合、このコマンドは必須ではありませんが、使用することを強く推奨します。

アクセス リストを定義するには、**access-list** コマンドを使用します。アクセス リストのヒット カウントは、トンネルが開始されたときにのみ増加します。トンネルが動作状態になると、パケット単位のフローではヒット カウントは増加しません。トンネルがドロップされてから再開されると、ヒット カウントは増加します。

ASA は、アクセス リストを使用して、IPsec クリプトで保護するトラフィックと保護を必要としないトラフィックとを区別します。また、許可 ACE に一致する発信パケットを保護し、許可 ACE に一致する着信パケットが確実に保護されるようにします。

ASA は、パケットが deny ステートメントと一致すると、クリプト マップ内の残りの ACE を使用したパケットの評価を省略して、順番に次のクリプト マップ内の ACE を使用したパケットの評価を再開します。*ACL のカスケード処理*には、ACL 内の残りの ACE の評価をバイパスする拒否 ACE の使用、およびクリプト マップ セット内の次のクリプト マップに割り当てられた ACL を使用したトラフィックの評価の再開が含まれています。クリプト マップごとに異なる IPsec 設定を関連付けることができるため、拒否 ACE を使用することで、特別なトラフィックを対応するクリプト マップでの以後の評価から除外し、異なるセキュリティを提供する別のクリプト マップ、または異なるセキュリティを必要とする別のクリプト マップの permit 文と特別なトラフィックを照合することができます。

(注) クリプト アクセス リストでは、インターフェイスを通過するトラフィックを許可するかどうかは判別されません。このような判別は、**access-group** コマンドを使用してインターフェイスに直接適用されるアクセス リストによって行われます。

トランスペアレント モードでは、宛先アドレスは ASA の IP アドレス、管理アドレスである必要があります。トランスペアレント モードでは、ASA へのトンネルだけが許可されます。

関連コマンド

コマンド	説明
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map set connection-type

クリプト マップ エントリのバックアップ サイト間機能の接続タイプを指定するには、グローバル コンフィギュレーション モードで **crypto map set connection-type** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set connection-type** {**answer-only** | **originate-only** | **bidirectional**}

no crypto map *map-name seq-num* **set connection-type** {**answer-only** | **originate-only** | **bidirectional**}

構文の説明

answer-only	ピアが、適切な接続先ピアを決定するための最初の独自の交換中に、まず着信 IKE 接続だけに応答することを指定します。
bidirectional	ピアが、クリプト マップ エントリに基づいて接続を受け入れ、発信できることを指定します。これは、すべての Site-to-Site 接続のデフォルトの接続タイプです。
map-name	クリプト マップ セットの名前を指定します。
originate-only	ピアが、適切な接続先ピアを決定するために最初の独自の交換を開始することを指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。
set connection-type	クリプト マップ エントリのバックアップ サイト間機能の接続タイプを指定します。answer-only、originate-only、および bidirectional の 3 つのタイプの接続があります。

デフォルト

デフォルトの設定は bidirectional です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが追加されました。
9.0	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

crypto map set connection-type コマンドは、バックアップ LAN-to-LAN 機能の接続タイプを指定します。接続の一方の側で複数のバックアップ ピアを指定できます。

この機能は、次のプラットフォーム間でのみ使用できます。

- 2 つの Cisco ASA 5500 シリーズ
- Cisco ASA 5500 シリーズと Cisco VPN 3000 コンセントレータ
- Cisco ASA 5500 シリーズと、Cisco PIX セキュリティ アプライアンス ソフトウェア バージョン 7.0 以上を実行しているセキュリティ アプライアンス

バックアップ LAN-to-LAN 接続を設定するには、接続の一方の側を **originate-only** キーワードを使用して originate-only として設定し、複数のバックアップ ピアがある側を **answer-only** キーワードを使用して answer-only として設定することを推奨します。originate-only 側では、**crypto map set peer** コマンドを使用してピアのプライオリティを指定します。originate-only ASA は、リストの最初のピアとネゴシエートしようとします。ピアが応答しない場合、ASA はピアが応答するか、またはリストにピアがなくなるまで下に向かってリストを検索します。

（注） IKEv2 は、サイトからサイトへのバックアップをサポートしていません。これは、発信専用または応答専用のキーワードを使用する場合に設定されます。IKEv2 を使用する場合、暗号マップセット接続タイプは双方向でなければなりません。

このように設定した場合、originate-only ピアは、最初に独自のトンネルを確立してピアとネゴシエートしようとします。その後は、いずれかのピアが通常の LAN-to-LAN 接続を確立することができ、いずれかの側からのデータがトンネル接続を開始できます。

トランスペアレント ファイアウォール モードでは、このコマンドは表示されますが、インターフェイスに対応付けられたクリプト マップに含まれるクリプト マップ エントリでは、connection-type 値は answer-only 以外の値に設定できません。

表10-1 に、サポートされているすべてのコンフィギュレーションを示します。他の組み合わせは、予測不可能なルーティング問題を引き起こす場合があります。

表10-1　サポートされているバックアップ LAN-to-LAN 接続タイプ

リモート側	中央側
Originate-Only	Answer-Only
Bi-Directional	Answer-Only
Bi-Directional	Bi-Directional

例

次に、グローバル コンフィギュレーション モードで、クリプト マップ mymap を設定し、接続タイプを originate-only に設定する例を示します。

```
ciscoasa(config)# crypto map mymap 10 set connection-type originate-only
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map set df-bit

per-signature algorithm（SA）do-not-fragment（DF）ポリシーを設定するには、グローバル コンフィギュレーション モードで **crypto map set df-bit** コマンドを使用します。DF ポリシーをディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto map *name priority* **set df-bit** [**clear-df** | **copy-df** | **set-df**]

no crypto map *name priority* **set df-bit** [**clear-df** | **copy-df** | **set-df**]

構文の説明

name	クリプト マップ セットの名前を指定します。
priority	クリプト マップ エントリに割り当てるプライオリティを指定します。

デフォルト

デフォルトの設定はオフです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

元の DF ポリシー コマンドが保持され、インターフェイスのグローバル ポリシー設定として機能しますが、SA については **crypto map** コマンドが優先されます。

crypto map set ikev1 phase1-mode

メインまたはアグレッシブへの接続を開始する場合にフェーズ 1 の IKEv1 モードを指定するには、グローバル コンフィギュレーション モードで **crypto map set ikev1 phase1-mode** コマンドを使用します。フェーズ 1 IKEv1 ネゴシエーションの設定を削除するには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set ikev1 phase1-mode** {**main** | **aggressive [group1** | **group2** | **group5** | **group14** | **group15** | **group16**| **group19** | **group20** | **group21**]}

no crypto map *map-name seq-num* **set ikev1 phase1-mode** {**main** | **aggressive [group1** | **group2** | **group5** | **group14** | **group15** | **group16** | **group19** | **group20** | **group21**]}

構文の説明

aggressive	フェーズ 1 の IKEv1 ネゴシエーションにアグレッシブ モードを指定します。
group14	IPsec で新しい Diffie-Hellman 交換を実行するときに、2048 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group15	IPsec で新しい Diffie-Hellman 交換を実行するときに、2048 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group16	IPsec で新しい Diffie-Hellman 交換を実行するときに、2048 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group19	IPsec で新しい Diffie-Hellman 交換を実行するときに、2048 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group20	IPsec で新しい Diffie-Hellman 交換を実行するときに、2048 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group21	IPsec で新しい Diffie-Hellman 交換を実行するときに、2048 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
主要	フェーズ 1 の IKEv1 ネゴシエーションにメイン モードを指定します。
map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトのフェーズ 1 モードは **main** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(4)	**group 7** コマンド オプションは廃止されました。グループ 7 を設定しようとするとエラー メッセージが生成され、代わりにグループ 5 が使用されます。
8.4(1)	**ikev1** キーワードが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.13(1)	**DH グループ 14、15、および 16** のサポートが追加され、デフォルトとして設定されています。**グループ 1、2** および**グループ 5** のオプションは廃止され、以降のリリースで削除されます。
9.15(1)	**DH グループ 1、2**、および **5** のサポートは廃止されました。

使用上のガイドライン

このコマンドは、発信側モードでのみ機能します。応答側モードでは機能しません。アグレッシブ モードの Diffie-Hellman グループを含めるかどうかは任意です。含めない場合、ASA はグループ 2 を使用します。

例

次に、グローバル コンフィギュレーション モードで、クリプト マップ mymap を設定し、グループ 2 を使用してフェーズ 1 のモードをアグレッシブに設定する例を示します。

```
ciscoasa(config)# crypto map mymap 10 set ikev1 phase1mode aggressive group2
ciscoasa(config)# crypto map mymap 10 set ikev1 phase1mode aggressive group14
```

関連コマンド

コマンド	説明
clear isakmp sa	アクティブな IKE セキュリティ アソシエーションを削除します。
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map set ikev2 ipsec-proposal

クリプト マップ エントリで使用する IKEv2 プロポーザルを指定するには、グローバル コンフィギュレーション モードで **crypto map set ikev2 ipsec-proposal** コマンドを使用します。クリプト マップ エントリから特定のプロポーザルを削除するには、プロポーザルの名前を指定してこのコマンドの **no** 形式を使用します。プロポーザルをすべて指定するか何も指定せずに、クリプト マップ エントリを削除するには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set ikev2 ipsec-proposal** *propsal-name1*
[*… proposal-name11*]

no crypto map *map-name seq-num* **set ikev2 ipsec-proposal** *propsal-name1*
[*… proposal-name11*]

no crypto map *map-name seq-num* **set ikev2 ipsec-proposal**

構文の説明

map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに対応するシーケンス番号を指定します。
propsal-name1 *proposal-name11*	IKEv2 の IPsec プロポーザルの名前を 1 つ以上指定します。このコマンドで指定するプロポーザルはすべて、**crypto ipsec ikev2 ipsec-proposal** コマンドで定義されている必要があります。各暗号マップ エントリは、最大 11 個のプロポーザルをサポートします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

リリース	変更内容
9.15(1)	次の整合性、暗号化、および暗号化方式は、このリリースから削除されました。 • md5 • 3des • des • aes-gmac • aes-gmac-192 • aes-gmac-256

使用上のガイドライン

すべてのクリプト マップ エントリに、IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルが必要です。

IPsec IKEv2 の開始側とは反対側にあるピアは、最初に一致したプロポーザルをセキュリティ アソシエーションに使用します。ローカルの ASA がネゴシエーションを開始した場合、ASA は、**crypto map** コマンドで指定した順番どおりに、トランスフォーム セットの内容をピアに提示します。ピアがネゴシエーションを開始すると、ローカルの ASA は、クリプト マップ エントリ内の、ピアから送信された IPsec パラメータと一致する最初のプロポーザルを使用します。

IPsec の開始側とは反対側にあるピアが、一致するプロポーザルの値を見つけられない場合、IPsec はセキュリティ アソシエーションを確立しません。トラフィックを保護するセキュリティ アソシエーションがないため、開始側はトラフィックをドロップします。

プロポーザルのリストを変更するには、新しいリストを作成して指定し、古いリストと置き換えます。

次のコマンドを使用してクリプト マップを変更すると、ASA は、指定したシーケンス番号と同じ番号のクリプト マップ エントリだけを変更します。たとえば、次のコマンドを入力すると、ASA は、56des-sha というプロポーザルをリストの最後に挿入します。

```
ciscoasa(config)# crypto map map1 1 set ikev2 ipsec-proposal 128aes-md5 128aes-sha
192aes-md5
ciscoasa(config)# crypto map map1 1 set ikev2 ipsec-proposal 56des-sha
ciscoasa(config)#
```

次のコマンドの応答は、前の 2 つのコマンドで行った変更を合わせたものになります。

```
ciscoasa(config)# show running-config crypto map
crypto map map1 1 set ipsec-proposal 128aes-md5 128aes-sha 192aes-md5 56des-sha
ciscoasa(config)#
```

クリプト マップ エントリ内のプロポーザルの順番を再設定するには、エントリを削除し、マップ名とシーケンス番号の両方を指定してから、エントリを再作成します。たとえば、次のコマンドでは、シーケンス番号 3 の *map2* というクリプト マップ エントリを再設定します。

```
asa2(config)# no crypto map map2 3 set ikev2 ipsec-proposal
asa2(config)# crypto map map2 3 set ikev2 ipsec-proposal 192aes-sha 192aes-md5 128aes-sha
128aes-md5
asa2(config)#
```

例

次に、10 個のプロポーザルで構成された、map2 というクリプト マップ エントリを作成する例を示します。

```
ciscoasa(config)# crypto map map2 10 set ikev2 ipsec-proposal 3des-md5 3des-sha 56des-md5
56des-sha 128aes-md5 128aes-sha 192aes-md5 192aes-sha 256aes-md5 256aes-sha
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック クリプト マップをコンフィギュレーションからクリアします。
clear configure crypto map	コンフィギュレーションから、すべてのクリプト マップをクリアします。
crypto dynamic-map set transform-set	ダイナミック クリプト マップ エントリで使用するトランスフォーム セットを指定します。
crypto ipsec transform-set	トランスフォーム セットを設定します。
show running-config crypto dynamic-map	ダイナミック クリプト マップのコンフィギュレーションを表示します。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map set ikev2 mode

クリプト マップ エントリで使用する IKEv2 モードを指定するには、グローバル コンフィギュレーション モードで **crypto map set ikev2 mode** コマンドを使用します。このモードをリセットするには、コンフィギュレーション モードで このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set ikev2 mode** {**transport** | **transport-require** | **tunnel**}

no crypto map *map-name seq-num* **set ikev2 mode** {**transport** | **transport-require** | **tunnel**}

構文の説明

map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに対応するシーケンス番号を指定します。
transport	transport モードに設定します。
transport-require	transport モードを必須にします。
tunnel	tunnel モード(デフォルト)を設定します。

コマンド デフォルト

モードが設定されていない場合、デフォルトのモードは tunnel です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

IKEv2 では、このモードはトンネルに ESP 暗号化と認証を適用するために指定します。これにより、ESP が適用されるオリジナルの IP パケットの部分が決定されます。

デフォルトは tunnel カプセル化モードです。transport カプセル化モードは、ピアがこのモードをサポートしていない場合に tunnel モードにフォールバックできる転送モードです。transport モードは、リモート アクセス VPN では推奨されません。

- tunnel モード(デフォルト):カプセル化モードは tunnel モードになります。tunnel モードでは、ESP 暗号化と認証が元の IP パケット全体(IP ヘッダーおよびデータ)に適用され、最終的な送信元アドレスと宛先アドレスが非表示になります。元の IP データグラム全体が暗号化され、新しい IP パケットのペイロードになります。

このモードでは、ルータなどのネットワーク デバイスが IPsec のプロキシとして動作できます。つまり、ルータがホストに代わって暗号化を行います。送信元ルータがパケットを暗号化し、IPsec トンネルを使用して転送します。宛先ルータは元の IP データグラムを復号化し、宛先システムに転送します。トンネル モードの大きな利点は、エンド システムを変更しなくても IPsec を利用できるということです。また、トラフィック分析から保護することもできます。トンネル モードを使用すると、攻撃者にはトンネルのエンドポイントしかわからず、トンネリングされたパケットの本来の送信元と宛先はわかりません（これらがトンネルのエンドポイントと同じ場合でも同様）。

- transport モード：カプセル化モードは transport モードになります。ピアがこのモードをサポートしていない場合は tunnel モードにフォールバックできます。transport モードでは IP ペイロードだけが暗号化され、元の IP ヘッダーはそのまま使用されます。

  このモードには、各パケットに数バイトしか追加されず、パブリック ネットワーク上のデバイスに、パケットの最終的な送信元と宛先を認識できるという利点があります。transport モードでは、中間ネットワークでの特別な処理（たとえば QoS）を、IP ヘッダーの情報に基づいて実行できるようになります。ただし、レイヤ 4 ヘッダーが暗号化されるため、パケットの検査が制限されます。

- transport-require：カプセル化モードは transport 専用モードになり、トンネル モードへのフォールバックは許可されません。

カプセル化モードのネゴシエーションは次のとおりです。

- イニシエータが転送モードを提案し、レスポンダがトンネル モードで応答した場合、イニシエータはトンネル モードにフォールバックします。
- 発信側が tunnel モードを提示し、応答側が transport モードで応答した場合、応答側は tunnel モードにフォールバックします。
- 発信側が tunnel モードを提示し、応答側が transport-require モードの場合、応答側はプロポーザルを送信しません。
- 同様に、イニシエータが transport-require モードで、レスポンダがトンネル モードの場合は、レスポンダから NO PROPOSAL CHOSEN が送信されます。

関連コマンド

コマンド	説明
show running-config crypto map	クリプト マップの設定内容を表示します。
clear configure crypto map	コンフィギュレーションから、すべてのクリプト マップをクリアします。

crypto map set ikev2 phase1-mode

メインまたはアグレッシブへの接続を開始する場合にフェーズ 1 の IKEv2 モードを指定するには、グローバル コンフィギュレーション モードで **crypto map set ikev2 phase1-mode** コマンドを使用します。フェーズ 1 IKEv2 ネゴシエーションの設定を削除するには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set ikev2 phase1-mode** {**main** | **aggressive** [**group1** | **group2** | **group5**]}

no crypto map *map-name seq-num* **set ikev2 phase1-mode** {**main** | **aggressive** [**group1** | **group2** | **group5**]}

構文の説明

aggressive	フェーズ 1 の IKEv2 ネゴシエーションにアグレッシブ モードを指定します。
group1	IPsec で新しい Diffie-Hellman 交換を実行するときに、768 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group2	IPsec で新しい Diffie-Hellman 交換を実行するときに、1024 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group5	IPsec で新しい Diffie-Hellman 交換を実行するときに、1536 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
主要	フェーズ 1 の IKEv2 ネゴシエーションにメイン モードを指定します。
map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトのフェーズ 1 モードは **main** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(4)	**group 7** コマンド オプションは廃止されました。グループ 7 を設定しようとするとエラー メッセージが生成され、代わりにグループ 5 が使用されます。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

このコマンドは、発信側モードでのみ機能します。応答側モードでは機能しません。アグレッシブ モードの Diffie-Hellman グループを含めるかどうかは任意です。含めない場合、ASA はグループ 2 を使用します。

例

次に、グローバル コンフィギュレーション モードで、クリプト マップ mymap を設定し、グループ 2 を使用してフェーズ 1 のモードをアグレッシブに設定する例を示します。

```
ciscoasa(config)# crypto map mymap 10 set ikev2 phase1mode aggressive group2
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear isakmp sa	アクティブな IKE セキュリティ アソシエーションを削除します。
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map set ikev2 pre-shared-key

AnyConnect IKEv2 接続の事前共有キーを指定するには、グローバル コンフィギュレーション モードで **crypto map set ikev2 pre-shared-key** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set ikev2 pre-shared-key** *key*

no crypto map *map-name seq-num* **set ikev2 pre-shared-key** *key*

構文の説明

key	1 ～ 128 文字の英数字文字列。
map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、事前共有キー SKTIWHT を設定する例を示します。

```
ciscoasa(config)# crypto map crypto_map_example set ikev2 pre-shared-key SKTIWHT
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map set inheritance

クリプト マップ エントリ用に生成されるセキュリティ アソシエーションの精度（シングルまたはマルチ）を設定するには、グローバル コンフィギュレーション モードで **set inheritance** コマンドを使用します。クリプト マップ エントリの継承の設定を削除するには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set inheritance** {**data** | **rule**}

no crypto map *map-name seq-num* **set inheritance** {**data** | **rule**}

構文の説明

data	ルールで指定されているアドレス範囲内のアドレス ペアごとに 1 つのトンネルを指定します。
map-name	クリプト マップ セットの名前を指定します。
rule	クリプト マップに関連付けられている各 ACL エントリに 1 つのトンネルを指定します。これはデフォルトです。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。
set inheritance	継承のタイプを **data** または **rule** に指定します。継承では、各セキュリティ ポリシー データベース（SPD）ルールに対して 1 つのセキュリティ アソシエーション（SA）を生成したり、範囲内の各アドレス ペアに対して複数のセキュリティ SA を生成したりすることができます。

デフォルト

デフォルト値は **rule** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

このコマンドは、ASA がトンネルに応答しているときではなく、トンネルを開始しているときにのみ機能します。データ設定を使用すると、多数の IPsec SA が作成される可能性があります。この場合、メモリが消費され、全体としてのトンネルが少なくなります。データ設定は、セキュリティへの依存が非常に高いアプリケーションに対してのみ使用してください。

例

次に、グローバル コンフィギュレーション モードで、クリプト マップ mymap を設定し、継承タイプを data に設定する例を示します。

```
ciscoasa(config)# crypto map mymap 10 set inheritance data
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map set nat-t-disable

接続の NAT-T をクリプト マップ エントリに基づいてディセーブルにするには、グローバル コンフィギュレーション モードで **crypto map set nat-t-disable** コマンドを使用します。このクリプト マップ エントリの NAT-T をイネーブルにするには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set nat-t-disable**

no crypto map *map-name seq-num* **set nat-t-disable**

構文の説明

map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

このコマンドのデフォルト設定はオンではありません（したがって、NAT-T はデフォルトでイネーブルです）。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

isakmp nat-traversal コマンドを使用して NAT-T をグローバルにイネーブルにします。その後に、**crypto map set nat-t-disable** コマンドを使用して、特定のクリプト マップ エントリの NAT-T をディセーブルにできます。

例

次のコマンドでは、グローバル コンフィギュレーション モードで、mymap という名前のクリプト マップ エントリの NAT-T をディセーブルにします。

```
ciscoasa(config)# crypto map mymap 10 set nat-t-disable
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
isakmp nat-traversal	すべての接続の NAT-T をイネーブルにします。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map set peer

クリプト マップ エントリの IPsec ピアを指定するには、グローバル コンフィギュレーション モードで **crypto map set peer** コマンドを使用します。クリプト マップ エントリから IPsec ピアを削除するには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set peer** {*ip_address* | *hostname*}{*...ip_address10* | *hostname10*}

no crypto map *map-name seq-num* **set peer** {*ip_address* | *hostname*}{*...ip_address10* | *hostname10*}

構文の説明

hostname	ピアを、ASA **name** コマンドで定義したホスト名で指定します。
ip_address	ピアを IP アドレス（IPv4 または IPv6）で指定します。
map-name	クリプト マップ セットの名前を指定します。
peer	クリプト マップ エントリ内で IPsec ピアをホスト名または IP アドレス（IPv4 または IPv6）で指定します。9.14(1) 以降、IKEv2 でも複数のピアがサポートされています。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、最大 10 個のピア アドレスを許容するように変更されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.14(1)	IKEv2 の複数ピアサポートが追加されました。

使用上のガイドライン

このコマンドは、すべてのスタティッククリプトマップに対して必要です。**crypto dynamic-map** コマンドを使用してダイナミック クリプト マップ エントリを定義する場合、このコマンドは必須ではなく、ほとんど使用しません。これは、ピアが通常は未知のものであるためです。

複数のピアを設定することは、フォールバックリストを指定することと同じです。各トンネルについて、ASA は、リストの最初のピアとネゴシエーションを試みます。ピアが応答しない場合、ASA はピアが応答するか、またはリストにピアがなくなるまで下に向かってリストを検索します。バックアップ LAN-to-LAN 機能を使用している場合（つまり、クリプトマップ接続タイプが originate-only の場合）にのみ複数のピアを設定できます。詳細については、**crypto map set connection-type** コマンドを参照してください。

(注) 9.14(1) 以降、IKEv2 では複数のピアがサポートされています。

例

次に、グローバル コンフィギュレーション モードで、IKE を使用してセキュリティ アソシエーションを確立するクリプト マップ コンフィギュレーションの例を示します。この例では、ピア 10.0.0.1 またはピア 10.0.0.2 のどちらかと、セキュリティ アソシエーションを確立できます。

```
ciscoasa(config)# crypto map mymap 10 ipsec-isakmp
ciscoasa(config)# crypto map mymap 10 match address 101
ciscoasa(config)# crypto map mymap 10 set transform-set my_t_set1
ciscoasa(config)# crypto map mymap 10 set peer 10.0.0.1 10.0.0.2
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map set pfs

クリプト マップ エントリ用の新しいセキュリティ アソシエーションの要求時に PFS を要求するように IPsec を設定するか、または新しいセキュリティ アソシエーションの要求の受信時に PFS を要求するように IPsec を設定するには、グローバル コンフィギュレーション モードで **crypto map set pfs** コマンドを使用します。IPsec が PFS を要求しないことを指定するには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set pfs [group1 | group2 | group5 | group14 | group 15 | group 16 | group19 | group20 | group21 | group24]**

no crypto map *map-name seq-num* **set pfs [group1 | group2 | group5 | group14 | group 15 | group 16 | group19 | group20 | group21 | group24]**

構文の説明

group14	IPsec で新しい Diffie-Hellman 交換を実行するときに、2048 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group15	IPsec で新しい Diffie-Hellman 交換を実行するときに、2048 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group16	IPsec で新しい Diffie-Hellman 交換を実行するときに、2048 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group19	IPsec で新しい Diffie-Hellman 交換を実行するときに、2048 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。IKEv1 ではサポートされていません。
group20	IPsec で新しい Diffie-Hellman 交換を実行するときに、2048 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。IKEv1 ではサポートされていません。
group21	IPsec で新しい Diffie-Hellman 交換を実行するときに、2048 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。IKEv1 ではサポートされていません。
map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトでは、PFS は設定されません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは変更され Diffie-Hellman グループ 7 が追加されました。
8.0(4)	**group 7** コマンド オプションは廃止されました。グループ 7 を設定しようとするとエラー メッセージが生成され、代わりにグループ 5 が使用されます。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.13(1)	DH グループ 14、15、および 16 のサポートが追加されました。DH グループ 1、2、5、および 24 のオプションは廃止され、以降のリリースで削除されます。
9.15(1)	DH グループ 1、2、5、および 24 のオプションは、このリリースでサポートが廃止されました。

使用上のガイドライン

PFS を使用すると、新しいセキュリティ アソシエーションをネゴシエートするたびに新しい Diffie-Hellman 交換が発生します。この交換によって、処理時間が長くなります。PFS を使用すると、セキュリティがさらに向上します。1 つのキーが攻撃者によってクラックされた場合でも、侵害されるのはそのキーで送信されたデータだけになるためです。

このコマンドを使用すると、クリプト マップ エントリ用の新しいセキュリティ アソシエーションを要求するとき、ネゴシエーション中に IPsec が PFS を要求します。**set pfs** ステートメントでグループが指定されていない場合、ASA はデフォルト（グループ 2）を送信します。

ピアがネゴシエーションを開始するときに、ローカル コンフィギュレーションで PFS が指定されている場合、ピアは PFS 交換を実行する必要があります。実行しない場合、ネゴシエーションは失敗します。ローカル コンフィギュレーションでグループが指定されていない場合、ASA はデフォルトの group2 が指定されているものと見なします。ローカル コンフィギュレーションでグループ 2 またはグループ 5 が指定されている場合は、そのグループがピアのオファーに含まれている必要があります。含まれていない場合、ネゴシエーションは失敗します。

ネゴシエーションが成功するには、（Diffie-Hellman グループの有無に関係なく）LAN to LAN トンネルの両端で PFS が設定されている必要があります。設定されている場合、グループは完全一致でなければなりません。ASA はピアからのいずれの PFS のオファーも受け入れません。

1536 ビットの Diffie-Hellman プライム モジュラス グループであるグループ 5 は、グループ 1 やグループ 2 よりも高いセキュリティを提供します。ただし、他のグループより処理時間が長くなります。

ASA は、Cisco VPN Client と対話するときに PFS 値を使用しません。その代わり、フェーズ 1 でネゴシエートされた値を使用します。

例

次に、グローバル コンフィギュレーション モードで、クリプト マップ mymap 10 用の新しいセキュリティ アソシエーションをネゴシエートするときに、必ず PFS を使用することを指定する例を示します。

```
ciscoasa(config)# crypto map mymap 12 set pfs ipsec-isakmp
ciscoasa(config)#crypto map mymap 12 set pfs group2
ciscoasa{config}# crypto map mymap 12 set pfs group14.
```

関連コマンド

コマンド	説明
clear isakmp sa	アクティブな IKE セキュリティ アソシエーションを削除します。
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto map	クリプト マップの設定内容を表示します。
tunnel-group	トンネル グループとそのパラメータを設定します。

crypto map set reverse-route

クリプト マップ エントリに基づいた任意の接続の逆ルート注入をイネーブルにするには、グローバル コンフィギュレーション モードで **crypto map set reverse-route** コマンドを使用します。クリプト マップ エントリに基づいた任意の接続の逆ルート注入をディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set reverse-route [dynamic]**

no crypto map *map-name seq-num s***et reverse-route [dynamic]**

構文の説明

map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。
dynamic	RRI は、IPsec トンネルが作成または破棄されると動的になり、追加または削除されます。

デフォルト

このコマンドのデフォルト設定はオフです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.7(1)	ダイナミック RRI のサポートが追加されました。

使用上のガイドライン

ダイナミックが指定されていない場合:

RRI は設定で行われ、静的とみなされます。設定が変更または削除されるまでそのままになります。ASA は、ルーティング テーブルにスタティック ルートを自動的に追加し、OSPF を使用してそれらのルートをプライベート ネットワークまたはボーダー ルータに通知します。

ダイナミックが指定されている場合:

このアプローチでは、IPsec セキュリティ アソシエーション（SA）の確立が成功するとルートが作成されます。ルートは、ネゴシエートされたセレクタの情報に基づいて追加されます。IPsec SA's が削除されると、このルートは削除されます。また、ダイナミックからスタティックへの設定変更、およびその逆の設定変更により、その暗号マップの既存の IPsec トンネルが破棄されます。

通常、RRI ルートは、ルートが存在せず、トラフィックを暗号化する必要がある場合に、トンネルを開始するために使用されます。ダイナミック RRI がサポートされると、トンネルが確立されるまでルートが存在しません。したがって、ダイナミック RRI が設定された ASA は通常、レスポンダとしてのみ動作します。

ダイナミック RRI は IKEv2 ベースのスタティック暗号マップだけに適用されます。

例

次に、グローバル コンフィギュレーション モードで、mymap という名前のクリプト マップの逆ルート注入をイネーブルにする例を示します。

```
ciscoasa(config)# crypto map mymap 10 set reverse-route
ciscoasa(config)#
```

グローバル コンフィギュレーション モードで入力された次の例では、トンネル確立時にリバース ルート インジェクションが有効になります。

```
ciscoasa(config)#crypto map mymap 1 set reverse-route dynamic
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map set security-association lifetime

特定のクリプト マップ エントリについて、IPsec セキュリティ アソシエーションをネゴシエートするときに使用されるグローバル ライフタイム値を上書きするには、グローバル コンフィギュレーション モードで **crypto map set security-association lifetime** コマンドを使用します。クリプト マップ エントリのライフタイム値をグローバル値にリセットするには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set security-association lifetime** {**seconds** *number* | **kilobytes** {*number* | **unlimited**}}

no crypto map *map-name seq-num* **set security-association lifetime** {**seconds** ***number*** | **kilobytes** {***number*** | **unlimited**}}

構文の説明

kilobytes {*number* | **unlimited**}	所定のセキュリティ アソシエーションの有効期限が切れるまでに、そのセキュリティ アソシエーションを使用してピア間を通過できるトラフィックの量を KB 単位で指定します。指定できる範囲は 10 ～ 2147483647 KB です。グローバル デフォルトは 4,608,000 キロバイトです。 この設定は、リモート アクセス VPN 接続には適用されません。サイト間 VPN のみに適用されます。
map-name	クリプト マップ セットの名前を指定します。
seconds *number*	セキュリティ アソシエーションの有効期限が切れるまでの存続時間（秒数）を指定します。指定できる範囲は 120 ～ 214783647 秒です。グローバルのデフォルトは 28,800 秒（8 時間）です。 この設定は、リモート アクセスとサイト間 VPN の両方に適用されます。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトの KB 数は 4,608,000 で、デフォルトの秒数は 28,800 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.1(2)	unlimited 引数が追加されました。

使用上のガイドライン

クリプト マップのセキュリティ アソシエーションは、グローバル ライフタイムに基づいてネゴシエートされます。

IPsec セキュリティ アソシエーションでは、共有秘密キーが使用されます。これらのキーとセキュリティ アソシエーションは、両方同時にタイムアウトになります。

特定のクリプト マップ エントリでライフタイム値が設定されている場合、ASA は、セキュリティ アソシエーションのネゴシエート時に新しいセキュリティ アソシエーションを要求するときに、ピアへの要求でクリプト マップ ライフタイム値を指定し、これらの値を新しいセキュリティ アソシエーションのライフタイムとして使用します。ASA は、ピアからネゴシエーション要求を受信すると、ピアが指定するライフタイム値またはローカルに設定されたライフタイム値のうち、小さい方を新しいセキュリティ アソシエーションのライフタイムとして使用します

サイト間 VPN 接続の場合、「時間指定」と「トラフィック量」の 2 つのライフタイムがあります。これらのライフタイムのいずれかに最初に到達すると、セキュリティ アソシエーションが期限切れになります。リモート アクセス VPN セッションでは、指定時刻ライフタイムのみが適用されます。

（注） ASA では、クリプト マップ、ダイナミック マップ、および IPsec 設定を動作中に変更できます。設定を変更する場合、変更によって影響を受ける接続のみが ASA によって停止させられます。たとえば、アクセス リスト内のエントリを削除して、クリプト マップに関連付けられた既存のアクセス リストを変更した場合、関連する接続だけがダウンします。アクセス リスト内の他のエントリに基づく接続は、影響を受けません。

指定時刻ライフタイムを変更するには、**crypto map set security-association lifetime seconds** コマンドを使用します。指定時刻ライフタイムを使用すると、指定した秒数が経過した後にキーおよびセキュリティ アソシエーションがタイムアウトします。

例

次のコマンドでは、グローバル コンフィギュレーション モードで、クリプト マップ mymap のセキュリティ アソシエーション ライフタイムを秒単位および KB 単位で指定します。

```
ciscoasa(config)# crypto map mymap 10 set security-association lifetime seconds 1400
kilobytes 3000000
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map set tfc-packets

IPsec SA でダミーのトラフィック フローの機密性(TFC)パケットをイネーブルにするには、グローバル コンフィギュレーション モードで **crypto map set tfc-packets** コマンドを使用します。IPsec SA で TFC パケットをディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto map *name priority* **set tfc-packets** [**burst** *length* | *auto*] [**payload-size** *bytes* | *auto*] [**timeout** *second* | *auto*]

no crypto map *name priority* **set tfc-packets** [**burst** *length* | *auto*] [**payload-size** *bytes* | *auto*] [**timeout** *second* | *auto*]

構文の説明

name	クリプト マップ セットの名前を指定します。
priority	クリプト マップ エントリに割り当てるプライオリティを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、クリプト マップの既存の DF ポリシー(SA レベルで)を設定します。

crypto map set transform-set

クリプト マップ エントリで使用する IKEv1 トランスフォーム セットを指定するには、グローバル コンフィギュレーション モードで **crypto map set transform-set** コマンドを使用します。クリプト マップ エントリから特定のトランスフォーム セット名を削除するには、トランスフォーム セットの名前を指定してこのコマンドの **no** 形式を使用します。トランスフォーム セットをすべて指定するか何も指定せずに、クリプト マップ エントリを削除するには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set transform-set** *transform-set-name1*
[*… transform-set-name11*]

no crypto map *map-name seq-num* **set transform-set** *transform-set-name1*
[*… transform-set-name11*]

no crypto map *map-name seq-num* **set transform-set**

構文の説明

map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに対応するシーケンス番号を指定します。
transform-set-name1 *transform-set-name11*	トランスフォーム セットの名前を 1 つ以上指定します。このコマンドで指定するトランスフォーム セットは、**crypto ipsec transform-set** コマンドで定義されている必要があります。各クリプト マップ エントリは、11 個までのトランスフォーム セットをサポートしています。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	クリプト マップ エントリにおけるトランスフォーム セットの最大数が変更されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

このコマンドは、すべてのクリプト マップ エントリで必要です。

IPsec の開始側とは反対側にあるピアは、最初に一致したトランスフォーム セットをセキュリティ アソシエーションに使用します。ローカルの ASA がネゴシエーションを開始した場合、ASA は、**crypto map** コマンドで指定した順番どおりに、トランスフォーム セットの内容をピアに提示します。ピアがネゴシエーションを開始すると、ローカルの ASA は、クリプト マップ エントリ内の、ピアから送信された IPsec パラメータと一致する最初のトランスフォーム セットを使用します。

IPsec の開始側とは反対側にあるピアが、一致するトランスフォーム セットの値を見つけられない場合、IPsec はセキュリティ アソシエーションを確立しません。トラフィックを保護するセキュリティ アソシエーションがないため、開始側はトラフィックをドロップします。

トランスフォーム セットのリストを変更するには、新しいリストを再度指定して、古いリストと置き換えます。

次のコマンドを使用してクリプト マップを変更すると、ASA は、指定したシーケンス番号と同じ番号のクリプト マップ エントリだけを変更します。たとえば、次のコマンドを入力すると、ASA は、56des-sha というトランスフォーム セットをリストの最後に挿入します。

```
ciscoasa(config)# crypto map map1 1 set transform-set 128aes-md5 128aes-sha 192aes-md5
ciscoasa(config)# crypto map map1 1 transform-set 56des-sha
ciscoasa(config)#
```

次のコマンドの応答は、前の 2 つのコマンドで行った変更を合わせたものになります。

```
ciscoasa(config)# show running-config crypto map
crypto map map1 1 set transform-set 128aes-md5 128aes-sha 192aes-md5 56des-sha
ciscoasa(config)#
```

クリプト マップ エントリ内のトランスフォーム セットの順番を再設定するには、エントリを削除し、マップ名とシーケンス番号の両方を指定してから、エントリを再作成します。たとえば、次のコマンドでは、シーケンス番号 3 の map2 というクリプト マップ エントリを再設定します。

```
asa2(config)# no crypto map map2 3 set transform-set
asa2(config)# crypto map map2 3 set transform-set 192aes-sha 192aes-md5 128aes-sha
128aes-md5
asa2(config)#
```

例

「**crypto ipsec transform-set**（トランスフォーム セットの作成または削除）」の項には、10 個のトランスフォーム セット コマンドが示されています。次に、10 個の同じトランスフォーム セットで構成された、map2 というクリプト マップ エントリを作成する例を示します。

```
ciscoasa(config)# crypto map map2 10 set transform-set 3des-md5 3des-sha 56des-md5
56des-sha 128aes-md5 128aes-sha 192aes-md5 192aes-sha 256aes-md5 256aes-sha
ciscoasa(config)#
```

次に、グローバル コンフィギュレーション モードで、ASA が IKE を使用してセキュリティ アソシエーションを確立する場合に最小限必要となるクリプト マップ コンフィギュレーションの例を示します。

```
ciscoasa(config)# crypto map map2 10 ipsec-isakmp
ciscoasa(config)# crypto map map2 10 match address 101
ciscoasa(config)# crypto map map2 set transform-set 3des-md5
ciscoasa(config)# crypto map map2 set peer 10.0.0.1
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック クリプト マップをコンフィギュレーションからクリアします。
clear configure crypto map	コンフィギュレーションから、すべてのクリプト マップをクリアします。
crypto dynamic-map set transform-set	ダイナミック クリプト マップ エントリで使用するトランスフォーム セットを指定します。
crypto ipsec transform-set	トランスフォーム セットを設定します。
show running-config crypto dynamic-map	ダイナミック クリプト マップのコンフィギュレーションを表示します。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map set trustpoint

クリプト マップ エントリのフェーズ 1 ネゴシエーション中に、認証用に送信する証明書を指定するトラストポイントを指定するには、グローバル コンフィギュレーション モードで **crypto map set trustpoint** コマンドを使用します。クリプト マップ エントリからトラストポイントを削除するには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set trustpoint** *trustpoint-name* [**chain**]

no crypto map *map-name seq-num* **set trustpoint** *trustpoint-name* [**chain**]

構文の説明

chain	(任意)証明書チェーンを送信します。CA 証明書チェーンには、ルート証明書からアイデンティティ証明書まで、証明書の階層内のすべての CA 証明書が含まれています。デフォルト値はディセーブル(チェーンなし)です。
map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。
trustpoint-name	フェーズ 1 ネゴシエーション中に送信する証明書を指定します。デフォルトは none です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

このクリプト マップ コマンドは、接続の開始に対してのみ有効です。応答側の情報については、**tunnel-group** コマンドを参照してください。

例

次に、グローバル コンフィギュレーション モードで、クリプト マップ mymap にトラストポイント tpoint 1 を指定し、証明書チェーンを含める例を示します。

```
ciscoasa(config)# crypto map mymap 10 set trustpoint tpoint1 chain
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto map	クリプト マップの設定内容を表示します。
tunnel-group	トンネル グループを設定します。

crypto map set validate-icmp-errors

IPsec トンネルを介して受信した、プライベート ネットワークの内部ホスト宛ての着信 ICMP エラー メッセージを検証するかどうかを指定するには、グローバル コンフィギュレーション モードで **crypto map set validate-icmp-errors** コマンドを使用します。クリプト マップ エントリからトラストポイントを削除するには、このコマンドの **no** 形式を使用します。

crypto map *name priority* **set validate-icmp-errors**

no crypto map *name priority* **set validate-icmp-errors**

構文の説明

name	クリプト マップ セットの名前を指定します。
priority	クリプト マップ エントリに割り当てるプライオリティを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このクリプト マップ コマンドは、着信 ICMP エラー メッセージの検証に対してのみ有効です。

csc

ASA がネットワーク トラフィックを CSC SSM に送信できるようにするには、クラス コンフィギュレーション モードで **csc** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

csc {**fail-open** | **fail-close**}

no csc

構文の説明

fail-close	CSC SSM が失敗した場合、ASA がトラフィックをブロックする必要があることを指定します。これは、クラス マップで選択されたトラフィックにのみ適用されます。CSC SSM に送信されていない他のトラフィックは、CSC SSM 障害による影響を受けません。
fail-open	CSC SSM が失敗した場合、ASA がトラフィックを許可する必要があることを指定します。これは、クラス マップで選択されたトラフィックにのみ適用されます。CSC SSM に送信されていない他のトラフィックは、CSC SSM 障害による影響を受けません。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。

csc コマンドは、該当するクラス マップに一致したすべてのトラフィックを CSC SSM に送信するようにセキュリティ ポリシーを設定します。この設定の後、ASA は、トラフィックが宛先に引き続き送信されるのを許可します。

CSC SSM がトラフィックをスキャンできない場合は、一致しているトラフィックを ASA が処理する方法を指定できます。**fail-open** キーワードは、CSC SSM を使用できない場合でも、トラフィックが宛先に引き続き送信されるのを ASA が許可するように指定します。**fail-close** キーワードは、CSC SSM が使用できない場合、一致しているトラフィックが宛先に引き続き送信されるのを ASA が許可しないように指定します。

CSC SSM は、HTTP、SMTP、POP3、および FTP トラフィックをスキャンできます。接続を要求しているパケットの宛先ポートが、これらのプロトコルにとって既知のポートである場合にのみ、これらのプロトコルがサポートされます。つまり、CSC SSM は、次の接続のみをスキャンできます。

- TCP ポート 21 に対してオープンされている FTP 接続
- TCP ポート 80 に対してオープンされている HTTP 接続
- TCP ポート 110 に対してオープンされている POP3 接続
- TCP ポート 25 に対してオープンされている SMTP 接続

csc コマンドを使用しているポリシーで、これらのポートを他のプロトコルに誤用する接続が選択された場合、ASA はパケットを CSC SSM に渡しますが、CSC SSM はパケットをスキャンせずに渡します。

CSC SSM の効率を最大限にするには、次のように、**csc** コマンドを実装しているポリシーが使用するクラス マップを設定します。

- サポートされているプロトコルのうち、CSC SSM がスキャンするプロトコルだけを選択します。たとえば、HTTP トラフィックをスキャンしない場合は、サービス ポリシーが HTTP トラフィックを CSC SSM に転送しないようにしてください。
- ASA によって保護されている信頼できるホストを危険にさらす接続だけを選択します。これらは、外部ネットワークまたは信頼できないネットワークから内部ネットワークへの接続です。次の接続をスキャンすることを推奨します。
  - 発信 HTTP 接続
  - ASA の内部のクライアントから ASA の外部のサーバへの FTP 接続
  - ASA の内部のクライアントから ASA の外部サーバへの POP3 接続
  - 内部メール サーバ宛ての着信 SMTP 接続

FTP スキャン

CSC SSM は、FTP セッションのプライマリ チャネルが標準ポート（TCP ポート 21）を使用している場合にのみ、FTP ファイル転送のスキャンをサポートします。

FTP インスペクションは、CSC SSM がスキャンする FTP トラフィックに対してイネーブルである必要があります。これは、FTP が、データ転送用にダイナミックに割り当てられたセカンダリ チャネルを使用するためです。ASA は、セカンダリ チャネルに割り当てられるポートを決定し、データ転送の実行を許可するピンホールを開きます。FTP データをスキャンするように CSC SSM が設定されている場合、ASA はデータ トラフィックを CSC SSM に転送します。

FTP インスペクションは、グローバルに、または **csc** コマンドが適用される同じインターフェイスに適用できます。デフォルトでは、FTP インスペクションはグローバルにイネーブルになっています。デフォルトのインスペクション コンフィギュレーションを変更していない場合、CSC SSM による FTP スキャンをイネーブルにするために必要なその他の FTP インスペクション コンフィギュレーションはありません。

FTP インスペクションまたはデフォルトのインスペクション コンフィギュレーションの詳細については、CLI 設定ガイドを参照してください。

例

内部ネットワーク上のクライアントから HTTP、FTP、および POP3 接続で外部のネットワークに要求されたトラフィック、および外部のホストから DMZ ネットワーク上のメール サーバに着信する SMTP 接続を CSC SSM に転送するように、ASA を設定する必要があります。内部ネットワークから DMZ ネットワーク上の Web サーバへの HTTP 要求は、スキャンされません。

次のコンフィギュレーションでは、2 つのサービス ポリシーを作成します。最初のポリシー csc_out_policy は、内部インターフェイスに適用され、csc_out アクセス リストを使用して、FTP および POP3 に対するすべての発信要求が確実にスキャンされるようにします。csc_out アクセス リストにより、内部から外部インターフェイス上のネットワークへの HTTP 接続が確実にスキャンされるようにもなりますが、このアクセス リストには、内部から DMZ ネットワーク上のサーバへの HTTP 接続を除外する拒否 ACE が含まれています。

2 番めのポリシー csc_in_policy は、外部インターフェイスに適用されます。このポリシーは csc_in アクセス リストを使用して、外部インターフェイスで発信され、DMZ ネットワークを宛先とする SMTP 要求と HTTP 要求が CSC SSM で確実にスキャンされるようにします。HTTP 要求をスキャンすることで、Web サーバは HTTP ファイルのアップロードから保護されます。

```
ciscoasa(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 21
ciscoasa(config)# access-list csc_out deny tcp 192.168.10.0 255.255.255.0 192.168.20.0 255.255.255.0 eq 80
ciscoasa(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 80
ciscoasa(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 110

ciscoasa(config)# class-map csc_outbound_class
ciscoasa(config-cmap)# match access-list csc_out

ciscoasa(config)# policy-map csc_out_policy
ciscoasa(config-pmap)# class csc_outbound_class
ciscoasa(config-pmap-c)# csc fail-close

ciscoasa(config)# service-policy csc_out_policy interface inside

ciscoasa(config)# access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 25
ciscoasa(config)# access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 80

ciscoasa(config)# class-map csc_inbound_class
ciscoasa(config-cmap)# match access-list csc_in

ciscoasa(config)# policy-map csc_in_policy
ciscoasa(config-pmap)# class csc_inbound_class
ciscoasa(config-pmap-c)# csc fail-close

ciscoasa(config)# service-policy csc_in_policy interface outside
```

（注） FTP で転送されるファイルをスキャンするには、CSC SSM に対して FTP 検査がイネーブルになっている必要があります。FTP インスペクションは、デフォルトでイネーブルになっています。

関連コマンド

コマンド	説明
class（ポリシー マップ）	トラフィック分類のクラス マップを指定します。
class-map	ポリシー マップで使用するトラフィック分類マップを作成します。
match port	宛先ポートを使用してトラフィックを照合します。
policy-map	トラフィック クラスを 1 つ以上のアクションと関連付けることによって、ポリシー マップを作成します。
service-policy	ポリシー マップを 1 つ以上のインターフェイスと関連付けることによって、セキュリティ ポリシーを作成します。

csd enable（廃止）

(注) このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

クライアントレス SSL VPN リモート アクセスまたは AnyConnect クライアントを使用したリモート アクセスに対して Cisco Secure Desktop（CSD）をイネーブルにするには、webvpn コンフィギュレーション モードで **csd enable** コマンドを使用します。CSD をディセーブルにするには、このコマンドの **no** 形式を使用します。

csd enable

no csd enable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
9.5(2)	このコマンドは廃止され、**hostscan** コマンドに置き換えられました。

使用上のガイドライン

CSD は、1 つの例外を除いて、ASA へのすべてのリモート アクセス接続試行に対してグローバルにイネーブルまたはディセーブルに設定されます。

csd enable コマンドは、次の処理を実行します。

1. 以前の **csd image** *path* コマンドによって実行されたチェックを補足する有効性チェックを提供します。
2. sdesktop フォルダがまだ存在しない場合は、disk0: 上に作成します。
3. data.xml（Cisco Secure Desktop コンフィギュレーション）ファイルが sdesktop フォルダにまだ存在しない場合は、追加します。

4. フラッシュ デバイスの data.xml を実行コンフィギュレーションにロードします。
5. CSD をイネーブルにします。

（注）
- **show webvpn csd** コマンドを入力して、Cisco Secure Desktop がイネーブルであるかどうかを確認できます。
- **csd enable** コマンドを入力する前に、実行コンフィギュレーション内に **csd image** *path* コマンドが存在する必要があります。
- **no csd enable** コマンドは、実行コンフィギュレーションで CSD をディセーブルにします。CSD がディセーブルの場合、管理者は CSD Manager にアクセスできず、リモート ユーザは CSD を使用できません。
- data.xml ファイルを転送または交換する場合は、このファイルを実行コンフィギュレーションにロードするために、CSD をいったんディセーブルにしてからイネーブルにします。
- CSD は、ASA へのすべてのリモート アクセス接続試行に対してグローバルにイネーブルまたはディセーブルに設定されます。個別の接続プロファイルやグループ ポリシーに対して CSD をイネーブルまたはディセーブルに設定することはできません。

  例外：クライアントレス SSL VPN 接続の接続プロファイルは、コンピュータがグループ URL を使用して ASA への接続を試み、CSD がグローバルにイネーブルの場合、CSD がクライアント コンピュータで実行されないように設定できます。次に例を示します。

```
ciscoasa(config)# tunnel-group group-name webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-url https://www.url-string.com
ciscoasa(config-tunnel-webvpn)# without-csd
```

例

次に、CSD イメージのステータスを表示し、CSD イメージをイネーブルにするためのコマンドを示します。

```
ciscoasa(config-webvpn)# show webvpn csd
Secure Desktop is not enabled.
ciscoasa(config-webvpn)# csd enable
ciscoasa(config-webvpn)# show webvpn csd
Secure Desktop version 3.1.0.25 is currently installed and enabled.
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
csd image	コマンドに指定された CSD イメージを、パスに指定されたフラッシュ ドライブから実行コンフィギュレーションにコピーします。
show webvpn csd	イネーブルの場合、CSD のバージョンを識別します。ディセーブルの場合、CLI に「Secure Desktop is not enabled.」と表示されます。
without-csd	クライアントレス SSL VPN セッションの接続プロファイルを、コンピュータがグループ URL を使用して ASA への接続を試み、CSD がグローバルにイネーブルの場合、CSD がクライアント コンピュータで実行されないように設定します。

csd hostscan image（廃止）

(注) このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

シスコのホスト スキャン配布パッケージをインストールまたはアップグレードし、実行コンフィギュレーションに追加するには、webvpn コンフィギュレーション モードで **csd hostscan image** コマンドを使用します。ホスト スキャン配布パッケージを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

csd hostscan image *path*

no csd hostscan image *path*

構文の説明

path	シスコのホスト スキャン パッケージのパスおよびファイル名を 255 文字以内で指定します。 ホスト スキャン パッケージには、ファイル名の命名規則 hostscan-*version*.pkg を持つスタンドアロンのホスト スキャン パッケージを指定するか、または、Cisco.com からダウンロードでき、ファイル名の命名規則 anyconnect-win-*version*-k9.pkg を持つ完全な AnyConnect セキュア モビリティ クライアント パッケージを指定できます。顧客が AnyConnect セキュア モビリティ クライアントを指定すると、ASA は AnyConnect パッケージからホスト スキャン パッケージを取得してインストールします。 ホスト スキャン パッケージには、ホスト スキャン ソフトウェアおよびホスト スキャン ライブラリとサポート チャートが含まれています。 このコマンドは、CSD イメージをアップロードできません。この操作を行うには、**csd image** コマンドを使用します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.5(2)	このコマンドは廃止されました。このコマンドは **hostscan image** に置き換えられました。

使用上のガイドライン

現在インストールされ、イネーブルになっているホスト スキャン イメージのバージョンを確認するには、**show webvpn csd hostscan** コマンドを入力します。

csd hostscan image コマンドを使用してホスト スキャンをインストールしたら、**csd enable** コマンドを使用してイメージをイネーブルにします。

次回の ASA のリブート時にホスト スキャン イメージを確実に使用できるように、**write memory** コマンドを入力して実行コンフィギュレーションを保存します。

例

次に、シスコのホスト スキャン パッケージをインストールし、イネーブルにして、表示およびフラッシュ ドライブへの設定の保存を行うコマンドを示します。

```
ciscoasa> en
Password: ******
ciscoasa# config t
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# show webvpn csd hostscan
Hostscan is not enabled.
ciscoasa(config-webvpn)# csd hostscan image disk0:/hostscan_3.0.0333-k9.pkg
ciscoasa(config-webvpn)# csd enable
ciscoasa(config-webvpn)# show webvpn csd hostscan
Hostscan version 3.0.0333 is currently installed and enabled
ciscoasa(config-webvpn)# write memory
Building configuration...
Cryptochecksum: 2e7126f7 71214c6b 6f3b28c5 72fa0a1e

22067 bytes copied in 3.460 secs (7355 bytes/sec)
[OK]
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
show webvpn csd hostscan	シスコのホスト スキャンがイネーブルである場合、そのバージョンを示します。ディセーブルの場合、CLI に「Secure Desktop is not enabled.」と表示されます。
csd enable	管理およびリモート ユーザ アクセスの CSD をイネーブルにします。

csd image（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

Cisco Secure Desktop（CSD）配布パッケージを検証して、実行コンフィギュレーションに追加するには、CSD を効率的にインストールし、webvpn コンフィギュレーション モードで **csd image** コマンドを使用します。CSD 配布パッケージを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

csd image *path*

no csd image *path*

構文の説明

path	CSD パッケージのパスおよびファイル名を 255 文字以内で指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
9.5(2)	このコマンドは廃止され、**hostscan image** コマンドに置き換えられました。

使用上のガイドライン

このコマンドを入力する前に、**show webvpn csd** コマンドを入力して、CSD イメージがイネーブルであるかどうかを判断します。CLI は、現在インストールされている CSD イメージがイネーブルである場合、そのバージョンを示します。

新しい Cisco Secure Desktop イメージをコンピュータにダウンロードし、フラッシュ ドライブに転送してから、**csd image** コマンドを使用して、イメージをインストールするか、または既存のイメージをアップグレードします。ダウンロードする場合、使用している ASA に合ったファイルを必ず取得してください。ファイルの形式は、securedesktop_asa_<n>_<n>*.pkg です。

no csd image コマンドを入力すると、CSD Manager への管理アクセスと CSD へのリモート ユーザ アクセスの両方が削除されます。このコマンドを入力しても、ASA は CSD ソフトウェアおよびフラッシュ ドライブの CSD コンフィギュレーションに変更を加えません。

(注) 次回の ASA のリブート時に CSD を確実に使用できるようにするために、**write memory** コマンドを入力して実行コンフィギュレーションを保存します。

例 次に、現在の CSD 配布パッケージを表示し、フラッシュ ファイル システムの内容を表示して、新しいバージョンにアップグレードするためのコマンドを示します。

```
ciscoasa# show webvpn csd
Secure Desktop version 3.1.0.24 is currently installed and enabled.
ciscoasa# config t
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# show disk all
-#- --length-- -----date/time------ path
  6 8543616    Nov 02 2005 08:25:36 PDM
  9 6414336    Nov 02 2005 08:49:50 cdisk.bin
 10 4634       Sep 17 2004 15:32:48 first-backup
 11 4096       Sep 21 2004 10:55:02 fsck-2451
 12 4096       Sep 21 2004 10:55:02 fsck-2505
 13 21601      Nov 23 2004 15:51:46 shirley.cfg
 14 9367       Nov 01 2004 17:15:34 still.jpg
 15 6594064    Nov 04 2005 09:48:14 asdmfile.510106.rls
 16 21601      Dec 17 2004 14:20:40 tftp
 17 21601      Dec 17 2004 14:23:02 bingo.cfg
 18 9625       May 03 2005 11:06:14 wally.cfg
 19 16984      Oct 19 2005 03:48:46 tomm_backup.cfg
 20 319662     Jul 29 2005 09:51:28 sslclient-win-1.0.2.127.pkg
 21 0          Oct 07 2005 17:33:48 sdesktop
 22 5352       Oct 28 2005 15:09:20 sdesktop/data.xml
 23 369182     Oct 10 2005 05:27:58 sslclient-win-1.1.0.133.pkg
 24 1836210    Oct 12 2005 09:32:10 securedesktop_asa_3_1_0_24.pkg
 25 1836392    Oct 26 2005 09:15:26 securedesktop_asa_3_1_0_25.pkg

38600704 bytes available (24281088 bytes used)

******** Flash Card Geometry/Format Info ********

COMPACT FLASH CARD GEOMETRY
   Number of Heads:            4
   Number of Cylinders       978
   Sectors per Cylinder       32
   Sector Size               512
   Total Sectors          125184

COMPACT FLASH CARD FORMAT
   Number of FAT Sectors      61
   Sectors Per Cluster         8
   Number of Clusters      15352
   Number of Data Sectors 122976
   Base Root Sector          123
   Base FAT Sector             1
   Base Data Sector          155
ciscoasa(config-webvpn)# csd image disk0:securedesktop_asa_3_1_0_25.pkg
ciscoasa(config-webvpn)# show webvpn csd
Secure Desktop version 3.1.0.25 is currently installed and enabled.
ciscoasa(config-webvpn)# write memory
Building configuration...
Cryptochecksum: 5e57cfa8 0e9ca4d5 764c3825 2fc4deb6

19566 bytes copied in 3.640 secs (6522 bytes/sec)
[OK]
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
show webvpn csd	イネーブルの場合、CSD のバージョンを識別します。ディセーブルの場合、CLI に「Secure Desktop is not enabled.」と表示されます。
csd enable	管理およびリモート ユーザ アクセスの CSD をイネーブルにします。

ctl

証明書信頼リスト(CTL)プロバイダーをイネーブルにして、CTL クライアントの CTL ファイルを解析し、トラストポイントをインストールするには、ctl プロバイダー コンフィギュレーション モードで **ctl** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

ctl install

no ctl install

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
Ctl プロバイダー コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

CTL プロバイダーをイネーブルにして、CTL クライアントの CTL ファイルを解析し、CTL ファイルのエントリに対するトラストポイントをインストールするには、ctl プロバイダー コンフィギュレーション モードで **ctl** コマンドを使用します。このコマンドでインストールされたトラストポイントには、「_internal_CTL_<ctl_name>」というプレフィックスが付いた名前が設定されます。

このコマンドがディセーブルの場合は、**crypto ca trustpoint** コマンドと **crypto ca certificate chain** コマンドを使用して、各 CallManager サーバと CAPF 証明書を手動でインポートおよびインストールする必要があります。

例

次の例は、CTL プロバイダー インスタンスを作成する方法を示しています。

```
ciscoasa(config)# ctl-provider my_ctl
ciscoasa(config-ctl-provider)# client interface inside 172.23.45.1
ciscoasa(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
```

```
ciscoasa(config-ctl-provider)# export certificate ccm_proxy
ciscoasa(config-ctl-provider)# ctl install
```

関連コマンド

コマンド	説明
ctl-provider	CTL プロバイダー インスタンスを定義し、プロバイダー コンフィギュレーション モードを開始します。
server trust-point	TLS ハンドシェイク中に提示するプロキシ トラストポイント証明書を指定します。
show tls-proxy	TLS プロキシを表示します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

ctl-file（廃止）

電話プロキシ用に作成するための CTL インスタンス、またはフラッシュ メモリに格納されている CTL ファイルを解析するための CTL インスタンスを指定するには、グローバル コンフィギュレーション モードで **ctl-file** コマンドを使用します。電話プロキシの設定時に使用する CTL インスタンスを指定するには、電話プロキシ コンフィギュレーション モードで **ctl-file** コマンドを使用します。CTL インスタンスを削除するには、このコマンドの **no** 形式を使用します。

ctl-file *ctl_name*

no ctl-file *ctl_name* [**noconfirm**]

構文の説明

ctl_name	CTL インスタンスの名前を指定します。
noconfirm	（任意、グローバル モードのみ）**no** コマンドとともに使用して、CTL ファイルの削除時に、トラストポイントの削除に関する警告が ASA コンソールに表示されないようにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
Phone-Proxy コンフィギュレーション					

コマンド履歴

リリース	変更内容
8.0(4)	コマンドが追加されました。
9.4(1)	このコマンドは、すべての **phone-proxy** モード コマンドとともに廃止されました。

使用上のガイドライン

LSC プロビジョニングが必要な電話をユーザが所有している場合は、**ctl-file** コマンドを使用して CTL ファイル インスタンスを設定するときに、CAPF 証明書を CUMC から ASA にインポートする必要もあります。

(注) CTL ファイルを作成するには、ctl ファイル コンフィギュレーション モードで **no shutdown** コマンドを使用します。CTL ファイルのエントリを変更したり CTL ファイルにエントリを追加したりするには、または CTL ファイルを削除するには、**shutdown** コマンドを使用します。

このコマンドの **no** 形式を使用すると、CTL ファイル、および電話プロキシによって内部的に作成されたすべての登録済みトラストポイントが削除されます。また、CTL ファイルを削除すると、関連する認証局から受信したすべての証明書が削除されます。

例

次に、電話プロキシ機能用の CTL ファイルを設定する例を示します。

```
ciscoasa(config)# ctl-file myctl
```

次に、**ctl-file** コマンドを使用して、電話プロキシ モードで電話プロキシ機能用の CTL ファイルを設定する例を示します。

```
ciscoasa(config-phone-proxy)# ctl-file myctl
```

関連コマンド

コマンド	説明
ctl-file（Phone-Proxy）	電話プロキシ インスタンスの設定時に使用する CTL ファイルを指定します。
cluster-ctl-file	フラッシュ メモリに格納されている CTL ファイルからトラストポイントをインストールするために、CTL ファイルを解析します。
phone-proxy	電話プロキシ インスタンスを設定します。
record-entry	CTL ファイルの作成に使用するトラストポイントを指定します。
sast	CTL レコードに作成する SAST 証明書の数を指定します。

ctl-provider

CTL プロバイダー モードで CTL プロバイダー インスタンスを設定するには、グローバル コンフィギュレーション モードで **ctl-provider** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

ctl-provider *ctl_name*

no ctl-provider *ctl_name*

構文の説明

ctl_name	CTL プロバイダー インスタンスの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

CTL プロバイダー コンフィギュレーション モードを開始して CTL プロバイダー インスタンスを作成するには、**ctl-provider** コマンドを使用します。

例

次の例は、CTL プロバイダー インスタンスを作成する方法を示しています。

```
ciscoasa(config)# ctl-provider my_ctl
ciscoasa(config-ctl-provider)# client interface inside 172.23.45.1
ciscoasa(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
ciscoasa(config-ctl-provider)# export certificate ccm_proxy
ciscoasa(config-ctl-provider)# ctl install
```

関連コマンド

コマンド	説明
クライアント	CTL プロバイダーへの接続が許可されるクライアントを指定し、クライアント認証用のユーザ名とパスワードを指定します。
ctl	CTL クライアントの CTL ファイルを解析し、トラストポイントをインストールします。
export	クライアントにエクスポートする証明書を指定します。
service	CTL プロバイダーがリッスンするポートを指定します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

cts import-pac

Cisco ISE から Protected Access Credential（PAC）ファイルをインポートするには、グローバル コンフィギュレーション モードで **cts import-pac** コマンドを使用します。

cts import-pac *filepath* **password** *value*

構文の説明

filepath	次のいずれかの **exec** モード コマンドおよびオプションを指定します。 シングル モード • **disk0**：disk0 のパスおよびファイル名 • **disk1**：disk1 のパスおよびファイル名 • **flash**：フラッシュのパスおよびファイル名 • **ftp**：FTP のパスおよびファイル名 • **http**：HTTP のパスおよびファイル名 • **https**：HTTPS のパスおよびファイル名 • **smb**：SMB のパスおよびファイル名 • **tftp**：TFTP のパスおよびファイル名 マルチ モード • **http**：HTTP のパスおよびファイル名 • **https**：HTTPS のパスおよびファイル名 • **smb**：SMB のパスおよびファイル名 • **tftp**：TFTP のパスおよびファイル名
password *value*	PAC ファイルの暗号化に使用されるパスワードを指定します。このパスワードは、デバイス クレデンシャルの一部として ISE で設定したパスワードとは関係ありません。 パスワードは、PAC ファイルが要求されたときに入力されたパスワードと一致する必要があり、PAC データを復号化するために必要です。このパスワードは、デバイス クレデンシャルの一部として ISE で設定したパスワードとは関係ありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

PAC ファイルを ASA にインポートすると、ISE との接続が確立されます。チャネルが確立されると、ASA は、ISE を使用してセキュア RADIUS トランザクションを開始し、Cisco TrustSec 環境データをダウンロードします。具体的には、ASA は、セキュリティ グループ テーブルをダウンロードします。セキュリティ グループ テーブルによって、SGT がセキュリティ グループ名にマッピングされます。セキュリティ グループの名前は ISE 上で作成され、セキュリティ グループをわかりやすい名前で識別できるようになります。チャネルは RADIUS トランザクションの前には確立されません。ASA は、認証用の PAC を使用して ISE の RADIUS トランザクションを開始します。

ヒント

PAC ファイルには、ASA および ISE がその間で発生する RADIUS トランザクションを保護できる共有キーが含まれています。このキーは、その機密性により、ASA に安全に保存する必要があります。

ファイルの正常なインポート後に、ASA は、ISE で設定されたデバイスのパスワードを要求せずに、ISE から Cisco TrustSec 環境データをダウンロードします。

ASA は、ユーザ インターフェイスからアクセスできない NVRAM の領域に PAC ファイルを保存します。

前提条件

- ASA が PAC ファイルを生成するには、ISE の認識された Cisco TrustSec ネットワーク デバイスとして ASA を設定する必要があります。ASA は、任意の PAC ファイルをインポートできますが、PAC ファイルは、正しく設定された ISE によって生成された場合にのみ ASA で動作します。
- ISE での PAC ファイルの生成時に PAC ファイルを暗号化するために使用されたパスワードを取得します。

  ASA は、PAC ファイルをインポートし、復号化する場合にこのパスワードが必要となります。
- ISE で生成された PAC ファイルにアクセスします。ASA は、フラッシュ、または TFTP、FTP、HTTP、HTTPS、SMB を介してリモート サーバから PAC ファイルをインポートできます（PAC ファイルは、インポート前に ASA フラッシュに配置されている必要はありません）。
- ASA のサーバ グループを設定します。

[Restrictions（機能制限）]

- ASA が HA 設定の一部である場合、プライマリ ASA デバイスに PAC ファイルをインポートする必要があります。
- ASA がクラスタリング設定の一部である場合、マスター デバイスに PAC ファイルをインポートする必要があります。

例

次に、ISE から PAC をインポートする例を示します。

```
ciscoasa(config)# cts import pac disk0:/pac123.pac password hideme
PAC file successfully imported
```

関連コマンド

コマンド	説明
cts refresh environment-data	ASA が Cisco TrustSec と統合されると、ISE からの Cisco TrustSec 環境データをリフレッシュします
cts sxp enable	ASA で SXP プロトコルをイネーブルにします。

cts manual

SGT およびイーサネット タギング（レイヤ 2 SGT インポジションとも呼ばれる）をイネーブルにし、cts manual インターフェイス コンフィギュレーション モードを開始するには、インターフェイス コンフィギュレーション モードで **cts manual** コマンドを使用します。SGT およびイーサネット タギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

cts manual

no cts manual

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、レイヤ 2 SGT インポジションをイネーブルにし、cts manual インターフェイス コンフィギュレーション モードを開始します。

[Restrictions（機能制限）]

- 物理インターフェイス、VLAN インターフェイス、ポート チャネル インターフェイスおよび冗長インターフェイスでのみサポートされます。
- BVI、TVI、VNI などの論理インターフェイスや仮想インターフェイスではサポートされません。
- フェールオーバー リンクはサポートしません。
- クラスタ制御リンクはサポートしません。

例

次に、レイヤ 2 SGT インポジションをイネーブルにし、cts manual インターフェイス コンフィギュレーション モードを開始する例を示します。

```
ciscoasa(config-if)# cts manual
ciscoasa(config-if-cts-manual)#
```

関連コマンド

コマンド	説明
policy static sgt	手動で設定された CTS リンクにポリシーを適用します。
propagate sgt	インターフェイスでのセキュリティ グループ タグ（**sgt** と呼ばれる）の伝播をイネーブルにします。

cts refresh environment-data

ISE からの Cisco TrustSec 環境データをリフレッシュし、調整タイマーを設定されたデフォルト値にリセットするには、グローバル コンフィギュレーション モードで **cts refresh environment-data** コマンドを使用します。

cts refresh environment-data

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASA が Cisco TrustSec と統合されると、ASA は ISE から環境データをダウンロードします。このデータには、セキュリティ グループ タグ(SGT)名テーブルが含まれます。ASA で次のタスクを完了すると、ASA は、ISE から取得した環境データを自動的にリフレッシュします。

- ISE と通信するように AAA サーバを設定します。
- ISE から PAC ファイルをインポートします。
- Cisco TrustSec 環境データを取得するために ASA で使用する AAA サーバ グループを識別します。

通常、ISE からの環境データを手動でリフレッシュする必要はありません。ただし、セキュリティ グループが ISE で変更されることがあります。これらの変更は、ASA セキュリティ グループ テーブルのデータをリフレッシュするまで ASA には反映されません。ASA でデータをリフレッシュして、ISE 上で作成されたセキュリティ グループが ASA に反映されるようにします。

ヒント　メンテナンス時間中に ISE のポリシー設定および ASA での手動データ リフレッシュをスケジュールすることを推奨します。このようにポリシー設定の変更を処理すると、セキュリティ グループ名が解決される可能性が最大化され、セキュリティ ポリシーが ASA で即時にアクティブ化されます。

前提条件

Cisco TrustSec の変更が ASA に適用されるように、ASA は、ISE の認識された Cisco TrustSec ネットワーク デバイスとして設定される必要があり、ASA は PAC ファイルを正常にインポートする必要があります。

[Restrictions（機能制限）]

- ASA が HA 設定の一部である場合、プライマリ ASA デバイスで環境データをリフレッシュする必要があります。
- ASA がクラスタリング設定の一部である場合、マスター デバイスで環境データをリフレッシュする必要があります。

例

次に、ISE から Cisco TrustSec 環境データをダウンロードする例を示します。

```
ciscoasa(config)# cts refresh environment-data
```

関連コマンド

コマンド	説明
cts import-pac	ASA が Cisco TrustSec と統合されると、Cisco ISE から Protected Access Credential（PAC）ファイルをインポートします。
cts sxp enable	ASA で SXP プロトコルをイネーブルにします。

cts role-based sgt-map

IP-SGT バインディングを手動で設定するには、グローバル コンフィギュレーション モードで **cts role-based sgt-map** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

cts role-based sgt-map {*IPv4_addr*[*/mask*] | *IPv6_addr*[*/prefix*]} **sgt** *sgt_value*

no cts role-based sgt-map {*IPv4_addr*[*/mask*] | *IPv6_addr*[*/prefix*]} **sgt** *sgt_value*

構文の説明

IPv4_addr[*/mask*]	使用する IPv4 アドレスを指定します。サブネットのマッピングを作成するために CIDR 形式のサブネット マスクを追加します（10.100.10.0/24 など）。
IPv6_addr[*/prefix*]	使用する IPv6 アドレスを指定します。IPv6 ネットワークのマッピングを作成するためにプレフィックスを追加します。
sgt *sgt_value*	IP アドレスをマッピングする SGT 番号を指定します。有効な値の範囲は 2 ～ 65519 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが追加されました。
9.6(1)	サブネットのマッピングを追加する機能が追加されました。

使用上のガイドライン

このコマンドを使用すると、IP-SGT バインディングを手動で設定することができます。

例

次に、IP-SGT バインディング テーブル エントリを設定する例を示します。

```
ciscoasa(config)# cts role-based sgt-map 10.2.1.2 sgt 50
```

関連コマンド

コマンド	説明
clear configure cts role-based [**sgt-map**]	ユーザ定義の IP-SGT バインディング テーブル エントリを削除します。
show running-config [**all**] **cts role-based [sgt-map]**	ユーザ定義の IP-SGT バインディング テーブル エントリを表示します。

cts server-group

環境データを取得する Cisco TrustSec と統合するために ASA で使用する AAA サーバ グループを識別するには、グローバル コンフィギュレーション モードで **cts server-group** コマンドを使用します。コマンドのサポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

cts server-group *aaa-server-group-name*

no cts server-group [*aaa-server-group-name*]

構文の説明

aaa-server-group-name	既存のローカルで設定された AAA サーバ グループの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

Cisco TrustSec と統合するための ASA の設定の一環として、ISE と通信できるように ASA を設定する必要があります。ASA では、サーバ グループの 1 つのインスタンスだけを Cisco TrustSec 用に設定できます。

前提条件

- 参照先のサーバ グループは、RADIUS プロトコルを使用するように設定する必要があります。ASA に非 RADIUS サーバ グループを追加すると、機能の設定は失敗します。
- ISE もユーザ認証に使用する場合は、ISE に ASA を登録したときに ISE で入力した共有秘密を取得します。この情報が不明な場合は、ISE 管理者にお問い合わせください。

例

次に、ISE 用の AAA サーバ グループを ASA でローカルに設定し、ASA と Cisco TrustSec を統合するためにその AAA サーバ グループを使用するように ASA を設定する例を示します。

```
ciscoasa(config)# aaa-server ISEserver protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ISEserver (inside) host 192.0.2.1
ciscoasa(config-aaa-server-host)# key myexclusivemumblekey
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# cts server-group ISEserver
```

関連コマンド

コマンド	説明
aaa-server *server-tag* **protocol radius**	AAA サーバ グループを作成し、ASA の AAA サーバ パラメータを ISE サーバと通信するように設定します。*server-tag* では、サーバ グループの名前を指定します。
aaa-server *server-tag* (*interface-name*) **host** *server-ip*	AAA サーバを AAA サーバ グループの一部として設定し、ホスト固有の接続データを設定します。(*interface-name*) では、ISE サーバが配置されているネットワーク インターフェイスを指定し、*server-tag* は Cisco TrustSec 統合の AAA サーバ グループの名前です。*server-ip* では、ISE サーバの IP アドレスを指定します。
cts sxp enable	ASA で SXP プロトコルをイネーブルにします。

cts sxp connection peer

SXP ピアへの SXP 接続を設定するには、グローバル コンフィギュレーション モードで **cts sxp connection peer** コマンドを使用します。コマンドのサポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

cts sxp connection peer *peer_ip_address* [**source** *source_ip_address*] **password** {**default** | **mode**} [**mode** {**local** | **peer**}] {**speaker** | **listener**}

no cts sxp connection peer *peer_ip_address* [**source** *source_ip_address*] [**password** {**default** | **none**}] [**mode** {**local** | **peer**}] [**speaker** | **listener**]

構文の説明

default	**password** キーワードとともに使用されます。SXP 接続に設定されたデフォルト パスワードを使用することを指定します。
listener	ASA が SXP 接続でリスナーとして機能することを指定します。これは、ASA がダウンストリーム デバイスから IP-SGT マッピングを受信できることを意味します。SPX 接続について、ASA にスピーカーまたはリスナーの役割が必要であることを指定します。
ローカル	**mode** キーワードとともに使用されます。ローカル SXP デバイスを使用することを指定します。
mode	（オプション）SXP 接続のモードを指定します。
none	**password** キーワードとともに使用されます。SXP 接続にパスワードを使用しないことを指定します。
password	（オプション）SXP 接続に認証キーを使用するかどうかを指定します。
peer	**mode** キーワードとともに使用されます。ピア SXP デバイスを使用することを指定します。
peer_ip_address	SXP ピアの IPv4 アドレスまたは IPv6 アドレスを指定します。ピア IP アドレスは、ASA 発信インターフェイスからアクセスできる必要があります。
source *source_ip_address*	（オプション）SXP 接続のローカル IPv4 または IPv6 アドレスを指定します。
speaker	ASA が SXP 接続でスピーカーとして機能することを指定します。これは、ASA がアップストリーム デバイスに IP-SGT マッピングを転送できることを意味します。SPX 接続について、ASA にスピーカーまたはリスナーの役割が必要であることを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

ピア間の SXP 接続はポイントツーポイントであり、基礎となるトランスポート プロトコルとして TCP を使用します。SXP 接続は IP アドレスごとに設定されます。単一デバイスのペアは複数の SXP 接続に対応できます。

[Restrictions（機能制限）]

- ASA は SXP 接続用の接続ごとのパスワードをサポートしません。
- **cts sxp default password** を使用してデフォルトの SXP パスワードを設定する場合、デフォルトのパスワードを使用するように SXP 接続を設定する必要があります。逆に、デフォルトのパスワードを設定しない場合は、SXP 接続用のデフォルトのパスワードを設定しないでください。この 2 つのガイドラインに従っていない場合、SXP 接続は失敗する可能性があります。
- デフォルトのパスワードを使用する SXP 接続を設定しましたが、ASA にデフォルトのパスワードが設定されていない場合、SXP 接続は失敗します。
- SXP 接続の送信元 IP アドレスを設定する場合は、ASA 発信インターフェイスと同じアドレスを指定する必要があります。送信元 IP アドレスが発信インターフェイスのアドレスと一致しない場合、SXP 接続は失敗します。

  SXP 接続の送信元 IP アドレスが設定されていない場合、ASA は、route/ARP 検索を実行して、SXP 接続用の発信インターフェイスを判別します。SXP 接続の送信元 IP アドレスを設定せずに、ASA が route/ARP 検索を実行して SXP 接続の送信元 IP アドレスを決定できるようにすることを推奨します。
- SXP ピアまたは送信元に対する IPv6 ローカル リンク アドレスの設定はサポートされていません。
- SXP 接続の同一インターフェイスに複数の IPv6 アドレスを設定することはサポートされていません。

例

次に、ASA で SXP 接続を作成する例を示します。

```
ciscoasa(config)# cts sxp connection peer 192.168.1.100
source 192.168.1.1 password default mode peer speaker
```

関連コマンド

コマンド	説明
cts sxp default password	SXP 接続のデフォルト パスワードを指定します。
cts sxp enable	ASA で SXP プロトコルをイネーブルにします。

cts sxp default password

SXP ピアでの TCP MD5 認証のデフォルト パスワードを設定するには、グローバル コンフィギュレーション モードで **cts sxp default password** コマンドを使用します。コマンドのサポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

cts sxp default password [**0** | **8**] *password*

no cts sxp default password [**0** | **8**] [*password*]

構文の説明

0	(オプション)デフォルトのパスワードで暗号化レベルに暗号化されていないクリアテキストを使用することを指定します。デフォルトのパスワードに設定できる暗号化レベルは 1 つだけです。
8	(オプション)デフォルトのパスワードで暗号化レベルに暗号化テキストを使用することを指定します。
password	162 文字までの暗号化された文字列または 80 文字までの ASCII キー文字列を指定します。

デフォルト

デフォルトでは、SXP 接続にパスワードは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトのパスワードを使用する SXP 接続を設定しましたが、ASA にデフォルトのパスワードが設定されていない場合、SXP 接続は失敗します。

[Restrictions(機能制限)]

- ASA は SXP 接続用の接続ごとのパスワードをサポートしません。
- **cts sxp default password** を使用してデフォルトの SXP パスワードを設定する場合、デフォルトのパスワードを使用するように SXP 接続を設定する必要があります。逆に、デフォルトのパスワードを設定しない場合は、SXP 接続用のデフォルトのパスワードを設定しないでください。この 2 つのガイドラインに従っていない場合、SXP 接続は失敗する可能性があります。

例

次に、SXP 接続のデフォルトのパスワードを含む、すべての SXP 接続のデフォルト値を設定する例を示します。

```
ciscoasa(config)# cts sxp enable
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
ciscoasa(config)# cts sxp default password 8 ********
ciscoasa(config)# cts sxp retry period 60
ciscoasa(config)# cts sxp reconcile period 60
```

関連コマンド

コマンド	説明
cts sxp connection peer	ASA と SXP ピアとの SXP 接続を設定します。このコマンドで **password default** キーワードを指定すると、SXP 接続のデフォルトのパスワードを使用できるようになります。
cts sxp enable	ASA で SXP プロトコルをイネーブルにします。

cts sxp default source-ip

SXP 接続のデフォルトのローカル IP アドレスを設定するには、グローバル コンフィギュレーション モードで **cts sxp default source-ip** コマンドを使用します。コマンドのサポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

cts sxp default source-ip *ipaddress*

no cts sxp default source-ip [*ipaddress*]

構文の説明

ipaddress	送信元 IP アドレスの IPv4 または IPv6 アドレスを指定します。

デフォルト

デフォルトでは、デフォルトの送信元 IP アドレスは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

SXP 接続のデフォルトの送信元 IP アドレスを設定する場合は、ASA 発信インターフェイスと同じアドレスを指定する必要があります。送信元 IP アドレスが発信インターフェイスのアドレスと一致しない場合、SXP 接続は失敗します。

SXP 接続の送信元 IP アドレスが設定されていない場合、ASA は、route/ARP 検索を実行して、SXP 接続用の発信インターフェイスを判別します。SXP 接続のデフォルトの送信元 IP アドレスを設定せずに、ASA が route/ARP 検索を実行して SXP 接続の送信元 IP アドレスを決定できるようにすることを推奨します。

例

次に、SXP 接続のデフォルトの送信元 IP アドレスを含む、すべての SXP 接続のデフォルト値を設定する例を示します。

```
ciscoasa(config)# cts sxp enable
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
ciscoasa(config)# cts sxp default password 8 ********
ciscoasa(config)# cts sxp retry period 60
ciscoasa(config)# cts sxp reconcile period 60
```

関連コマンド

コマンド	説明
cts sxp connection peer	ASA の SXP 接続を設定します。このコマンドで **source** *source_ip_address* キーワードおよび引数を指定すると、SXP 接続のデフォルトの送信元 IP アドレスを使用できるようになります。
cts sxp enable	ASA で SXP プロトコルをイネーブルにします。

cts sxp delete-hold-down period

SXP ピアが SXP 接続を終了した後にピアから学習した IP-SGT マッピングに削除ホールド ダウン タイマーを設定するには、グローバル コンフィギュレーション モードで **cts sxp delete-hold-down period** コマンドを使用します。タイマーをデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

cts sxp delete-hold-down period *timervalue*

no cts sxp delete-hold-down period

構文の説明

timervalue	SXP 接続の切断から学習した IP-SGT マッピングが削除されるまで保持する秒数を 120 ～ 64000 の範囲で指定します。

デフォルト

デフォルトでは、*timervalue* は 120 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.8(3)	このコマンドが追加されました。

使用上のガイドライン

各 SXP 接続が削除ホールド ダウン タイマーに関連付けられます。このタイマーは、リスナー側の SXP 接続が切断されたときにトリガーされます。この SXP 接続から学習した IP-SGT マッピングはすぐには削除されません。その代わりに、削除ホールド ダウン タイマーの有効期限が切れるまで保持されます。このタイマーの有効期限が切れると、マッピングが削除されます。

例

次に、削除ホールド ダウン期間を設定する例を示します。

```
ciscoasa(config)# cts sxp delete-hold-down period 240
```

関連コマンド

コマンド	説明
cts sxp connection peer	ASA と SXP ピアとの SXP 接続を設定します。
cts sxp enable	ASA で SXP プロトコルをイネーブルにします。

cts sxp enable

ASA 上の SXP プロトコルをイネーブルにするには、グローバル コンフィギュレーション モードで **cts sxp enable** コマンドを使用します。コマンドのサポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

cts sxp enable

no cts sxp enable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、ASA 上の SXP プロトコルはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

例

次に、ASA 上の SXP プロトコルをイネーブルにする例を示します。

```
ciscoasa(config)# cts sxp enable
```

関連コマンド

コマンド	説明
clear cts	Cisco TrustSec と統合されたときに ASA で使用されるデータをクリアします。
cts sxp connection peer	ASA と SXP ピアとの SXP 接続を設定します。

cts sxp mapping network-map

SXPv2 以前を使用しているピアのスピーカーとして機能している場合、IPv4 サブネット拡張の深さを設定するには、グローバル コンフィギュレーション モードで **cts sxp mapping network-map** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

cts sxp mapping network-map *maximum_hosts*

no cts sxp mapping network-map *maximum_hosts*

構文の説明

maximum_hosts	ネットワーク バインドから拡張できるホスト バインドの最大数（0 ～ 65535）です。デフォルトは 0 です。

デフォルト

デフォルトでは拡張は行われません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

リスナー ピアが SXPv2 以下を使用している場合、ピアは SGT とサブネットのバインドを理解できません。ASA は、個々のホスト バインディングに IPv4 サブネット バインディングを拡張できます（IPv6 バインディングは拡張されません）。このコマンドでは、サブネット バインディングから生成できるホスト バインディングの最大数が指定されます。すべてのリスナー ピアが SXPv3 以降を使用しているか、ASA がリスナーである場合、このコマンドの効果はありません。

例

次に、サブネット マッピングを 1000 ホスト バインドまで拡張できるようにする例を示します。

```
ciscoasa(config)# cts sxp mapping network-map 1000
```

関連コマンド

コマンド	説明
cts sxp connection peer	Trustsec ピアを設定します。

cts sxp reconciliation period

SXP ピアが SXP 接続を終了した後にホールド ダウン タイマーを開始するには、グローバル コンフィギュレーション モードで **cts sxp reconciliation period** コマンドを使用します。コマンドのサポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

cts sxp reconciliation period *timervalue*

no cts sxp reconciliation period [*timervalue*]

構文の説明

timervalue	調整タイマーのデフォルト値を指定します。1 ～ 64000 秒の範囲で秒数を入力します。

デフォルト

デフォルトでは、*timervalue* は 120 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

SXP ピアが SXP 接続を終了すると、ASA はホールド ダウン タイマーを開始します。ホールド ダウン タイマーの実行中に SXP ピアが接続されると、ASA は調整タイマーを開始します。次に、ASA は、SXP マッピング データベースを更新して、最新のマッピングを学習します。

調整タイマーの期限が切れると、ASA は、SXP マッピング データベースをスキャンして、古いマッピング エントリ（前回の接続セッションで学習されたエントリ）を識別します。ASA は、これらの接続を廃止としてマークします。調整タイマーが期限切れになると、ASA は、SXP マッピング データベースから廃止エントリを削除します。

0 を指定すると調整タイマーが開始されないため、このタイマーには 0 を指定できません。調整タイマーを実行できないようにすると、失効する時間の定義がない状態で古いエントリが維持され、ポリシーの適用に対する予期しない結果が発生します。

例

次に、デフォルトの調整タイマーを含む、すべての SXP 接続のデフォルト値を設定する例を示します。

```
ciscoasa(config)# cts sxp enable
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
ciscoasa(config)# cts sxp default password 8 ********
ciscoasa(config)# cts sxp retry period 60
ciscoasa(config)# cts sxp reconcile period 60
```

関連コマンド

コマンド	説明
cts sxp connection peer	ASA と SXP ピアとの SXP 接続を設定します。
cts sxp enable	ASA で SXP プロトコルをイネーブルにします。

cts sxp retry period

ASA が SXP ピア間での新しい SXP 接続の設定を試行するデフォルトの時間間隔を指定するには、グローバル コンフィギュレーション モードで **cts sxp retry period** コマンドを使用します。コマンドのサポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

cts sxp retry period *timervalue*

no cts sxp retry period [*timervalue*]

構文の説明

timervalue	再試行タイマーのデフォルト値を指定します。0 ～ 64000 秒の範囲で秒数を入力します。

デフォルト

デフォルトでは、*timervalue* は 120 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASA が SXP ピア間での新しい SXP 接続の設定を試行するデフォルトの時間間隔を指定します。ASA は、成功した接続が確立されるまで接続を試み続けます。

ASA で確立されていない SXP 接続が存在する限り、再試行タイマーがトリガーされます。

0 秒を指定すると、タイマーの期限が切れず、ASA は SXP ピアへの接続を試行しません。

再試行タイマーが期限切れになると、ASA は接続データベースを順に検索し、データベースに切断されているか、または「保留中」状態の接続が含まれている場合、ASA は、再試行タイマーを再開します。

再試行タイマーは、SXP ピア デバイスとは異なる値に設定することを推奨します。

例

次に、デフォルトの再試行タイマーを含む、すべての SXP 接続のデフォルト値を設定する例を示します。

```
ciscoasa(config)# cts sxp enable
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
ciscoasa(config)# cts sxp default password 8 ********
ciscoasa(config)# cts sxp retry period 60
ciscoasa(config)# cts sxp reconcile period 60
```

関連コマンド

コマンド	説明
cts sxp connection peer	ASA と SXP ピアとの SXP 接続を設定します。
cts sxp enable	ASA で SXP プロトコルをイネーブルにします。

customization

トンネル グループ、グループ、またはユーザに使用するカスタマイゼーションを指定するには、トンネル グループ webvpn 属性コンフィギュレーション モードまたは webvpn コンフィギュレーション モードで **customization** コマンドを使用します。カスタマイゼーションを指定しない場合は、このコマンドの **no** 形式を使用します。

customization *name*

no customization *name*

customization {**none** | **value** *name*}

no customization {**none** | **value** *name*}

構文の説明

name	グループまたはユーザに適用する WebVPN カスタマイゼーションの名前を指定します。
none	グループまたはユーザのカスタマイゼーションをディセーブルにし、カスタマイゼーションが継承されないようにします。
value *name*	グループ ポリシーまたはユーザに適用するカスタマイゼーションの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
トンネル グループ webvpn 属性コンフィギュレーション	• 対応	—	• 対応	—	—
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

トンネル グループ webvpn 属性コンフィギュレーション モードで **customization** コマンドを入力する前に、webvpn コンフィギュレーション モードで **customization** コマンドを使用してカスタマイゼーションの名前を付け、設定する必要があります。

Mode-Dependent コマンド オプション

customization コマンドで使用できるキーワードは使用しているモードによって異なります。グループ ポリシー属性コンフィギュレーション モードおよびユーザ名属性コンフィギュレーション モードでは、追加のキーワード **none** と **value** が表示されます。

たとえば、ユーザ名属性コンフィギュレーション モードで **customization none** コマンドを入力すると、ASA は、グループ ポリシーやトンネル グループ内の値を検索しません。

例

次に、パスワード プロンプトを定義する「123」という名前の WebVPN カスタマイゼーションを最初に確立するコマンド シーケンスの例を示します。この例では、次に「test」という名前の WebVPN トンネル グループを定義し、**customization** コマンドを使用して、「123」という名前の WebVPN カスタマイゼーションを使用することを指定しています。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization 123
ciscoasa(config-webvpn-custom)# password-prompt Enter password
ciscoasa(config-webvpn)# exit
ciscoasa(config)# tunnel-group test type webvpn
ciscoasa(config)# tunnel-group test webvpn-attributes
ciscoasa(config-tunnel-webvpn)# customization 123
ciscoasa(config-tunnel-webvpn)#
```

次に、「cisco」というカスタマイゼーションを「cisco_sales」というグループ ポリシーに適用する例を示します。webvpn コンフィギュレーション モード経由でグループポリシー属性コンフィギュレーション モードになった場合は、**customization** コマンドに追加のコマンド オプション **value** が必要になります。

```
ciscoasa(config)# group-policy cisco_sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# customization value cisco
```

関連コマンド

コマンド	説明
clear configure tunnel-group	すべてのトンネル グループ コンフィギュレーションを削除します。
show running-config tunnel-group	現在のトンネル グループ コンフィギュレーションを表示します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ属性を設定する webvpn コンフィギュレーション モードを開始します。

cxsc

ASA CX モジュールにトラフィックをリダイレクトするには、クラス コンフィギュレーション モードで **cxsc** コマンドを使用します。ASA CX アクションを削除するには、このコマンドの **no** 形式を使用します。

cxsc {**fail-close** | **fail-open**} [**auth-proxy** | **monitor-only**]

no cxsc {**fail-close** | **fail-open**} [**auth-proxy** | **monitor-only**]

構文の説明

auth-proxy	(オプション)アクティブ認証に必要な認証プロキシをイネーブルにします。
fail-close	ASA CX モジュールが使用できない場合、すべてのトラフィックをブロックするように ASA を設定します。
fail-open	ASA CX モジュールが使用できない場合、すべてのトラフィックの通過を検査なしで許可するように ASA を設定します。
monitor-only	デモンストレーションの目的のみで、**monitor-only** を指定して、トラフィックの読み取り専用コピーを ASA CX モジュールに送信します。このオプションを設定すると、次のような警告メッセージが表示されます。 `WARNING: Monitor-only mode should be used for demonstrations and evaluations only. This mode prevents CXSC from denying or altering traffic.`

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(4.1)	このコマンドが追加されました。
9.1(2)	デモンストレーション機能をサポートするために **monitor-only** キーワードが追加されました。
9.1(3)	コンテキストごとの ASA CX ポリシーを設定できるようになりました。

使用上のガイドライン

クラス コンフィギュレーション モードにアクセスするには、policy-map コマンドを入力します。

ASA で **cxsc** コマンドを設定する前または後に、Cisco Prime Security Manager（PRSM）を使用して ASA CX モジュールでセキュリティ ポリシーを設定します。

cxsc コマンドを設定するには、先に **class-map** コマンド、**policy-map** コマンド、および **class** コマンドを設定する必要があります。

トラフィック フロー

ASA CX モジュールは、ASA とは別のアプリケーションを実行します。ただし、そのアプリケーションは ASA のトラフィック フローに統合されます。ASA でトラフィックのクラスの **cxsc** コマンドを適用すると、トラフィックは次のように ASA と ASA CX モジュールを通過します。

1. トラフィックは ASA に入ります。
2. 着信 VPN トラフィックが復号化されます。
3. ファイアウォール ポリシーが適用されます。
4. バックプレーンを介して ASA CX モジュールにトラフィックが送信されます。
5. ASA CX モジュールはセキュリティ ポリシーをトラフィックに適用し、適切なアクションを実行します。
6. 有効なトラフィックがバックプレーンを介して ASA に返送されます。ASA CX モジュールがセキュリティ ポリシーに従ってトラフィックをブロックすることがあり、そのトラフィックは渡されません。
7. 発信 VPN トラフィックが暗号化されます。
8. トラフィックが ASA から出ます。

認証プロキシに関する情報

ASA CX が HTTP ユーザを認証する必要がある場合は（アイデンティティ ポリシーを利用するために）、認証プロキシとして動作するように ASA を設定する必要があります。つまり、ASA CX モジュールは認証要求を ASA インターフェイス IP アドレス/プロキシ ポートにリダイレクトします。デフォルトでは、ポートは 885 です（**cxsc auth-proxy port** コマンドでユーザが設定できます）。この機能は、トラフィックを ASA から ASA CX モジュールに誘導するサービス ポリシーの一部として設定します。認証プロキシをイネーブルにしない場合は、パッシブ認証のみを使用できます。

ASA の機能との互換性

ASA には、HTTP インスペクションを含む、多数の高度なアプリケーション インスペクション機能があります。ただし、ASA CX モジュールには ASA よりも高度な HTTP インスペクション機能があり、その他のアプリケーションについても機能が追加されています。たとえば、アプリケーション使用状況のモニタリングと制御です。

ASA CX モジュールの機能を最大限に活用するには、ASA CX モジュールに送信するトラフィックに関する次のガイドラインを参照してください。

- HTTP トラフィックに対して ASA インスペクションを設定しないでください。
- クラウド Web セキュリティ（ScanSafe）インスペクションを設定しないでください。同じトラフィックに対して ASA CX のアクションとクラウド Web セキュリティ インスペクションの両方が設定されている場合に、ASA が実行するのは ASA CX のアクションのみです。
- ASA 上の他のアプリケーション インスペクションは ASA CX モジュールと互換性があり、これにはデフォルト インスペクションも含まれます。

- Mobile User Security（MUS）サーバをイネーブルにしないでください。これは、ASA CX モジュールとの間に互換性がありません。
- ASA クラスタリングをイネーブルにしないでください。これは、ASA CX モジュールとの間に互換性がありません。
- フェールオーバーをイネーブルにした場合は、ASA がフェールオーバーしたときに、既存の ASA CX フローは新しい ASA に転送されますが、トラフィックは ASA CX モジュールによる処理を受けることなく ASA の通過を許可されます。新しい ASA が受信した新しいフローだけが、ASA CX モジュールによる処理の対象となります。

モニタ専用モード

テストおよびデモンストレーション用に、**monitor-only** キーワードを使用して、ASA CX モジュールに読み取り専用トラフィックの重複ストリームを送信するように ASA を設定できるので、モジュールが ASA トラフィック フローに影響を与えることなく、どのようにトラフィックをインスペクションするかを確認できます。このモードでは、ASA CX モジュールが通常どおりトラフィックをインスペクションし、ポリシーを決定し、イベントを生成します。ただし、パケットが読み取り専用コピーであるため、モジュールのアクションは実際のトラフィックには影響しません。代わりに、モジュールはインスペクション後コピーをドロップします。

次のガイドラインを参照してください。

- ASA 上でモニタ専用モードと通常のインライン モードの両方を同時に設定できません。セキュリティ ポリシーの 1 つのタイプのみが許可されます。
- 次の機能は、モニタ専用モードでサポートされません。
  - 拒否ポリシー
  - アクティブ認証
  - 復号化ポリシー
- ASA CX は、モニタ専用モードでパケット バッファリングを実行せず、イベントはベスト エフォート方式で生成されます。たとえば、長い URL がパケット境界にまたがっている一部のイベントは、バッファリングの欠如の影響を受ける可能性があります。
- ASA ポリシーと ASA CX の両方でモードが一致するように設定する必要があります（両方ともモニタ専用モード、または両方とも通常のインライン モード）。

例

次の例では、すべての HTTP トラフィックが ASA CX モジュールに誘導され、何らかの理由で ASA CX モジュールに障害が発生した場合はすべての HTTP トラフィックがブロックされます。

```
ciscoasa(config)# access-list ASACX permit tcp any any eq port 80
ciscoasa(config)# class-map my-cx-class
ciscoasa(config-cmap)# match access-list ASACX
ciscoasa(config-cmap)# policy-map my-cx-policy
ciscoasa(config-pmap)# class my-cx-class
ciscoasa(config-pmap-c)# cxsc fail-close auth-proxy
ciscoasa(config-pmap-c)# service-policy my-cx-policy global
```

次の例では、10.1.1.0 ネットワークと 10.2.1.0 ネットワーク宛てのすべての IP トラフィックが ASA CX モジュールに誘導され、何らかの理由で ASA CX モジュールに障害が発生した場合は、すべてのトラフィックの通過が許可されます。

```
ciscoasa(config)# access-list my-cx-acl permit ip any 10.1.1.0 255.255.255.0
ciscoasa(config)# access-list my-cx-acl2 permit ip any 10.2.1.0 255.255.255.0
ciscoasa(config)# class-map my-cx-class
ciscoasa(config-cmap)# match access-list my-cx-acl
ciscoasa(config)# class-map my-cx-class2
ciscoasa(config-cmap)# match access-list my-cx-acl2
```

```
ciscoasa(config-cmap)# policy-map my-cx-policy
ciscoasa(config-pmap)# class my-cx-class
ciscoasa(config-pmap-c)# cxsc fail-open auth-proxy
ciscoasa(config-pmap)# class my-cx-class2
ciscoasa(config-pmap-c)# cxsc fail-open auth-proxy
ciscoasa(config-pmap-c)# service-policy my-cx-policy interface outside
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
class-map	ポリシー マップ用にトラフィックを識別します。
cxsc auth-proxy port	認証プロキシのポートを設定します。
debug cxsc	ASA CX デバッグ メッセージをイネーブルにします。
hw-module module password-reset	モジュールのパスワードをデフォルトにリセットします。
hw-module module reload	モジュールをリロードします。
hw-module module reset	リセットを実行してから、モジュールをリロードします。
hw-module module shutdown	モジュールをシャットダウンします。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
session do get-config	モジュール設定を取得します。
session do password-reset	モジュールのパスワードをデフォルトにリセットします。
session do setup host ip	モジュール管理アドレスを設定します。
show asp table classify domain cxsc	トラフィックを ASA CX モジュールに送信するために作成された NP ルールを表示します。
show asp table classify domain cxsc-auth-proxy	ASA CX モジュールの認証プロキシ用に作成された NP ルールを表示します。
show module	モジュールのステータスを表示します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。
show service-policy	サービス ポリシーの統計情報を表示します。

cxsc auth-proxy port

ASA CX モジュール トラフィックの認証プロキシ ポートを設定するには、グローバル コンフィギュレーション モードで **cxsc auth-proxy port** コマンドを使用します。このポートをデフォルトに設定するには、このコマンドの **no** 形式を使用します。

cxsc auth-proxy port *port*

no cxsc auth-proxy port [*port*]

構文の説明

port *port*	認証プロキシのポートを 1024 より大きい値に設定します。デフォルト値は 885 です。

コマンド デフォルト

デフォルト ポートは 885 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(4.1)	このコマンドが追加されました。
9.1(3)	コンテキストごとの ASA CX ポリシーを設定できるようになりました。

使用上のガイドライン

cxsc コマンドの設定時に認証プロキシをイネーブルにする場合は、このコマンドを使用してポートを変更できます。

ASA CX が HTTP ユーザを認証する必要がある場合は（アイデンティティ ポリシーを利用するために）、認証プロキシとして動作するように ASA を設定する必要があります。つまり、ASA CX モジュールは認証要求を ASA インターフェイス IP アドレス/プロキシ ポートにリダイレクトします。デフォルトでは、port は 885 です。この機能は、トラフィックを ASA から ASA CX モジュールに誘導するサービス ポリシーの一部として設定します。認証プロキシをイネーブルにしない場合は、パッシブ認証のみを使用できます。

例

次に、ASA CX トラフィックの認証プロキシをイネーブルにし、ポートを 5000 に変更する例を示します。

```
ciscoasa(config)# access-list ASACX permit tcp any any eq port 80
ciscoasa(config)# class-map my-cx-class
ciscoasa(config-cmap)# match access-list ASACX
ciscoasa(config-cmap)# policy-map my-cx-policy
ciscoasa(config-pmap)# class my-cx-class
ciscoasa(config-pmap-c)# cxsc fail-close auth-proxy
ciscoasa(config-pmap-c)# service-policy my-cx-policy global
ciscoasa(config)# cxsc auth-port 5000
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
class-map	ポリシー マップ用にトラフィックを識別します。
cxsc	ASA CX モジュールにトラフィックをリダイレクトします。
debug cxsc	ASA CX デバッグ メッセージをイネーブルにします。
hw-module module password-reset	モジュールのパスワードをデフォルトにリセットします。
hw-module module reload	モジュールをリロードします。
hw-module module reset	リセットを実行してから、モジュールをリロードします。
hw-module module shutdown	モジュールをシャットダウンします。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
session do get-config	モジュール設定を取得します。
session do password-reset	モジュールのパスワードをデフォルトにリセットします。
session do setup host ip	モジュール管理アドレスを設定します。
show asp table classify domain cxsc	トラフィックを ASA CX モジュールに送信するために作成された NP ルールを表示します。
show asp table classify domain cxsc-auth-proxy	ASA CX モジュールの認証プロキシ用に作成された NP ルールを表示します。
show module	モジュールのステータスを表示します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。
show service-policy	サービス ポリシーの統計情報を表示します。

database path コマンド～ dhcp-server コマンド

database path

ローカル CA サーバ データベースのパスまたは位置を指定するには、CA サーバ コンフィギュレーション モードで **database** コマンドを使用します。フラッシュ メモリへのパスをデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

[no] database path *mount-name directory-path*

構文の説明

directory-path	CA ファイルが保存される、マウント ポイント上のディレクトリへのパスを指定します。
mount-name	マウント名を指定します。

デフォルト

デフォルトでは、CA サーバ データベースはフラッシュ メモリに保存されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

データベースに保存されるローカル CA ファイルには、証明書データベース ファイル、ユーザ データベース ファイル、一時 PKCS12 ファイル、および現在の CRL ファイルが含まれます。*mount-name* 引数は、ASA のファイル システムを指定するために使用する **mount** コマンドの *name* 引数と同じです。

（注） これらの CA ファイルは内部保存ファイルです。変更しないでください。

例

次に、CA データベースのマウント ポイントを cifs_share として定義し、そのマウント ポイント上のデータベース ファイル ディレクトリを ca_dir/files_dir として定義する例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# database path cifs_share ca_dir/files_dir/
ciscoasa(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ユーザはローカル CA を設定および管理できます。
crypto ca server user-db write	ローカル CA データベースに設定されているユーザ情報をディスクに書き込みます。
debug crypto ca server	ユーザがローカル CA サーバを設定する場合にデバッグ メッセージを表示します。
mount	Common Internet File System（CIFS）および File Transfer Protocol ファイル システム（FTPFS）の一方または両方を、ASA がアクセスできるようにします。
show crypto ca server	ASA の CA コンフィギュレーションの特性を表示します。
show crypto ca server cert-db	CA サーバが発行する証明書を表示します。

ddns

ダイナミック DNS（DDNS）アップデート方式のタイプを指定するには、DDNS アップデート方式モードで **ddns** コマンドを使用します。実行コンフィギュレーションから更新方式タイプを削除するには、このコマンドの **no** 形式を使用します。

ddns [**both**]

no ddns [**both**]

構文の説明

both	（オプション）DNS の A と PTR の両方のリソース レコード（RR）のアップデートを指定します。

デフォルト

DNS A RR のみを更新します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
DDNS アップデート方式	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

DDNS は、DNS で保持されている名前/アドレスおよびアドレス/名前のマッピングを更新します。DDNS 更新を実行するための 2 つの方式（RFC 2136 で規定されている IETF 標準、および一般的な HTTP 方式）のうち、ASA のこのリリースでは、IETF 方式をサポートしています。

名前とアドレスのマッピングは、次の 2 タイプの RR に保持されます。

- A リソース レコードには、ドメイン名から IP アドレスへのマッピングが含まれます。
- PTR リソース レコードには、IP アドレスからドメイン名へのマッピングが含まれます。

DDNS アップデートを使用して、DNS の A RR タイプと PTR RR タイプとの間で一貫した情報を保持できます。

DDNS アップデート方式コンフィギュレーション モードで **ddns** コマンドを発行するとき、アップデートを DNS A RR に対してのみ行うか、DNS の A と PTR の両方の RR タイプに対して行うかを定義します。

例

次に、ddns-2 という名前の DDNS アップデート方式に対し DNS の A と PTR の両方の RR のアップデートを設定する例を示します。

```
ciscoasa(config)# ddns update method ddns-2
ciscoasa(DDNS-update-method)# ddns both
```

関連コマンド

コマンド	説明
ddns update	DDNS アップデート方式を ASA インターフェイスまたは DDNS アップデート ホスト名に関連付けます。
ddns update method	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
dhcp-client update dns	DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。
dhcpd update dns	DHCP サーバによる DDNS アップデートの実行をイネーブルにします。
interval maximum	DDNS アップデート方式によるアップデート試行の最大間隔を設定します。

ddns update

ダイナミック DNS（DDNS）アップデート方式を、ASA インターフェイスまたはアップデート ホスト名に関連付けるには、インターフェイス コンフィギュレーション モードで **ddns update** コマンドを使用します。DDNS 更新方式とインターフェイスまたはホスト名とのアソシエーションを、実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

ddns update [*method-name* | **hostname** *hostname*]

no ddns update [*method-name* | **hostname** *hostname*]

構文の説明

hostname	コマンド文字列内の後続の語をホスト名として指定します。
hostname	更新で使用するホスト名を指定します。
method-name	設定するインターフェイスとのアソシエーションの方式名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

DDNS アップデート方式を定義した後、DDNS アップデートをトリガーするために、その DDNS アップデート方式を ASA インターフェイスに関連付ける必要があります。

ホスト名は、完全修飾ドメイン名（FQDN）またはホスト名のみを指定できます。ホスト名のみ指定した場合、ASA は、ドメイン名をホスト名に追加して FQDN を作成します。

例

次に、インターフェイス GigabitEthernet0/2 に ddns-2 という名前の DDNS 更新方式およびホスト名 hostname1.example.com を関連付ける例を示します。

```
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname hostname1.example.com
```

関連コマンド

コマンド	説明
ddns	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update method	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
dhcp-client update dns	DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。
dhcpd update dns	DHCP サーバによる DDNS アップデートの実行をイネーブルにします。
interval maximum	DDNS アップデート方式によるアップデート試行の最大間隔を設定します。

ddns update method

DNS リソース レコード(RR)をダイナミックに更新するための方式を作成するには、グローバル コンフィギュレーション モードで **ddns update method** コマンドを使用します。実行コンフィギュレーションからダイナミック DNS(DDNS)更新方式を削除するには、このコマンドの **no** 形式を使用します。

ddns update method *name*

no ddns update method *name*

構文の説明

name	ダイナミックに DNS レコードを更新するための方式の名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

DDNS は、DNS で保持されている名前/アドレスおよびアドレス/名前のマッピングを更新します。**ddns update method** コマンドで設定するアップデート方式により、DDNS アップデートの実行方法および実行頻度が決まります。DDNS 更新を実行するための 2 つの方式(RFC 2136 で規定されている IETF 標準、および一般的な HTTP 方式)のうち、ASA のこのリリースでは、IETF 方式をサポートしています。

名前とアドレスのマッピングは、次の 2 タイプのリソース レコード(RR)に保持されます。

- A リソース レコードには、ドメイン名から IP アドレスへのマッピングが含まれます。
- PTR リソース レコードには、IP アドレスからドメイン名へのマッピングが含まれます。

DDNS アップデートを使用して、DNS の A RR タイプと PTR RR タイプとの間で一貫した情報を保持できます。

（注） **ddns update method** コマンドを実行する前に、インターフェイスでドメイン ルックアップをイネーブルにした状態で、**dns** コマンドを使用して到達可能なデフォルト DNS サーバを設定する必要があります。

例

次に、ddns-2 という名前の DDNS 更新方式を設定する例を示します。

```
ciscoasa(config)# ddns update method ddns-2
```

関連コマンド

コマンド	説明
ddns	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update	DDNS アップデート方式を ASA インターフェイスまたは DDNS アップデート ホスト名に関連付けます。
dhcp-client update dns	DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。
dhcpd update dns	DHCP サーバによるダイナミック DNS アップデートの実行をイネーブルにします。
interval maximum	DDNS アップデート方式によるアップデート試行の最大間隔を設定します。

debug

特定機能のデバッグ メッセージを表示するには、特権 EXEC モードで **debug** コマンドを使用します。デバッグ メッセージの表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug *feature* [*subfeature*] [*level*]

no debug *feature* [*subfeature*]

構文の説明

level	(オプション)デバッグ レベルを指定します。このレベルは、一部の機能で使用できない場合があります。
feature	デバッグをイネーブルにする機能を指定します。使用できる機能を表示するには、CLI ヘルプの **debug ?** コマンドを使用します。
subfeature	(オプション)機能によっては、1 つ以上のサブ機能のデバッグ メッセージをイネーブルにできます。

デフォルト

デフォルトのデバッグ レベルは 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.13(1)	**debug crypto ca** コマンドが変更され、オプションが少なくなり、デバッグ レベルが 14 に制限されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。

バージョン 9.13(1) 以降では、**debug crypto ca** コマンドのオプション（**debug crypto ca transactions** と **debug crypto ca messages**）が統合され、すべての該当するコンテンツが **debug crypto ca** コマンド自体に提供されます。また、使用可能なデバッグ レベルの数が 14 に削減されました。

例

次に、**debug aaa internal** コマンドの出力例を示します。

```
ciscoasa(config)# debug aaa internal
debug aaa internal enabled at level 1
ciscoasa(config)# uap allocated. remote address: 10.42.15.172, Session_id: 2147483841
uap freed for user . remote address: 10.42.15.172, session id: 2147483841
```

次に、変更された **debug crypto ca** コマンドを示します。

```
(config)# debug crypto ca ?

exec mode commands/options:
  <1-14>                   Specify an optional debug level (default is 1)
  cluster                  debug PKI cluster
  cmp                      debug the CMP transactions
  periodic-authentication  debug PKI peroidic authentication
  <cr>
```

default（crl 設定）

すべての CRL パラメータをシステム デフォルト値に戻すには、crl 設定コンフィギュレーション モードで **default** コマンドを使用します。

default

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
crl 設定コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドの呼び出しは、アクティブなコンフィギュレーションには含まれません。crl 設定コンフィギュレーション モードは、暗号 CA トラストポイント コンフィギュレーション モードからアクセスできます。これらのパラメータは、LDAP サーバで必要な場合のみ使用されます。

例

次に、ca-crl コンフィギュレーション モードを開始して、CRL コマンド値をデフォルトに戻す例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# default
ciscoasa(ca-crl)#
```

関連コマンド

コマンド	説明
crl configure	crl 設定コンフィギュレーション モードを開始します。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
protocol ldap	CRL の取得方法として LDAP を指定します。

default（インターフェイス）

インターフェイス コマンドをシステム デフォルト値に戻すには、インターフェイス コンフィギュレーション モードで **default** コマンドを使用します。

default *command*

構文の説明

command	デフォルトに設定するコマンドを指定します。次に例を示します。 **default activation key**

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは実行時のコマンドです。入力しても、アクティブなコンフィギュレーションの一部にはなりません。

例

次に、インターフェイス コンフィギュレーション モードを開始して、セキュリティ レベルをデフォルトに戻す例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# default security-level
```

関連コマンド

コマンド	説明
interface	インターフェイス コンフィギュレーション モードを開始します。

default（IPv6 ルータ OSPF）

OSPFv3 パラメータをデフォルト値に戻すには、IPv6 ルータ OSPF コンフィギュレーション モードで **default** コマンドを使用します。

default [**area** | **auto-cost** | **default-information** | **default-metric** | **discard-route** | **distance** | **distribute-list** | **ignore** | **log-adjacency-changes** | **maximum-paths** | **passive-interface** | **redistribute** | **router-id** | **summary-prefix** | **timers**]

構文の説明

area	（オプション）OSPFv3 エリア パラメータを指定します。
auto-cost	（オプション）帯域幅に従って OSPFv3 インターフェイスのコストを指定します。
default-information	（オプション）デフォルトの情報を配布します。
default-metric	（オプション）再配布されるルートのメトリックを指定します。
discard-route	（オプション）廃棄ルートの導入をイネーブルまたはディセーブルにします。
distance	（オプション）アドミニストレーティブ ディスタンスを指定します。
distribute-list	（オプション）ルーティング アップデートでネットワークをフィルタリングします。
ignore	（オプション）特定のイベントを無視します。
log-adjacency-changes	（任意）隣接ステートの変更を記録します。
maximum-paths	（オプション）複数のパスを介してパケットを転送します。
passive-interface	（オプション）インターフェイス上のルーティング アップデートを抑制します。
redistribute	（オプション）別のルーティング プロトコルからの IPv6 プレフィックスを再配布します。
router-id	（オプション）指定したルーティング プロセスのルータ ID を指定します。
summary-prefix	（オプション）OSPFv3 集約プレフィックスを指定します。
timers	（任意）OSPFv3 タイマーを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

OSPFv3 パラメータのデフォルト値をリセットするには、このコマンドを使用します。

例

次に、OSPFv3 タイマー パラメータをデフォルト値にリセットする例を示します。

```
ciscoasa(config-router)# default timers spf
```

関連コマンド

コマンド	説明
distance	OSPFv3 ルーティング プロセスのアドミニストレーティブ ディスタンスを指定します。
default-information originate	OSPFv3 ルーティング ドメインへのデフォルトの外部ルートを生成します。
log-adjacency-changes	OSPFv3 ネイバーが起動または停止したときに、ルータが syslog メッセージを送信するように設定します。

default(パラメータ)

IP オプション インスペクション時に特定のアクションを指定しないオプションのデフォルト アクションを定義するには、パラメータ コンフィギュレーション モードで **default** コマンドを使用します。システムのデフォルトに戻すには、このコマンドの **no** 形式を使用します。

default action {allow | clear}

no default action {allow | clear}

構文の説明

allow	IP オプション インスペクション ポリシー マップに明示的に指定されていないオプションを含んでいるパケットを許可します。
clear	IP オプション インスペクション ポリシー マップに明示的に指定されていないオプションをパケット ヘッダーから削除してから、パケットを許可します。

デフォルト

デフォルトでは、IP オプション インスペクションはルータアラート オプションを許可しますが、その他の IP オプションを含んでいるパケットはドロップします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IP オプション インスペクション ポリシー マップで設定できます。

IP オプション インスペクションを設定して、どの IP パケットが所定の IP オプションを持ち、ASA を通過できるかを制御できます。変更せずにパケットを通過させたり、指定されている IP オプションをクリアしてからパケットを通過させたりできます。

例

次に、IP オプション インスペクションのアクションをポリシー マップで設定する例を示します。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# default action clear
ciscoasa(config-pmap-p)# router-alert action allow
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

default（時間範囲）

absolute コマンドおよび **periodic** コマンドの設定をデフォルトに戻すには、時間範囲コンフィギュレーション モードで **default** コマンドを使用します。

default {**absolute** | **periodic** *days-of-the-week time* **to** [*days-of-the-week*] *time*}

構文の説明

absolute	時間範囲が有効になる絶対時間を定義します。
days-of-the-week	最初の days-of-the-week 引数は、関連付けられている有効時間範囲が開始する日または曜日です。2 番めの days-of-the-week 引数は、関連付けられているステートメントの有効期間が終了する日または曜日です。 この引数は、単一の曜日または曜日の組み合わせです（Monday（月曜日）、Tuesday（火曜日）、Wednesday（水曜日）、Thursday（木曜日）、Friday（金曜日）、Saturday（土曜日）、および Sunday（日曜日））。他に指定できる値は、次のとおりです。 • daily：月曜日～日曜日 • weekdays：月曜日～金曜日 • weekend：土曜日と日曜日 終了の曜日が開始の曜日と同じ場合は、終了の曜日を省略できます。
periodic	時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定します。
時刻	時刻を HH:MM 形式で指定します。たとえば、午前 8 時は 8:00、午後 8 時は 20:00 とします。
to	「開始時刻から終了時刻まで」の範囲を入力するには、**to** キーワードを入力する必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
時間範囲コンフィギュレーション	•	•	•	•	

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

終了の days-of-the-week 値が開始の days-of-the-week 値と同じ場合、終了の days-of-the-week 値を省略できます。

time-range コマンドに **absolute** 値と **periodic** 値の両方が指定されている場合、**periodic** コマンドは absolute start 時刻を経過した後にのみ評価の対象になり、absolute end 時刻を経過した後は評価の対象にはなりません。

時間範囲機能は、ASA のシステム クロックに依存しています。ただし、この機能は NTP 同期を使用すると最適に動作します。

例

次に、**absolute** キーワードの動作をデフォルトに戻す例を示します。

```
ciscoasa(config-time-range)# default absolute
```

関連コマンド

コマンド	説明
absolute	時間範囲が有効になる絶対時間を定義します。
periodic	時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定します。
time-range	時間に基づいて ASA のアクセス コントロールを定義します。

default-acl

ポスチャ検証が失敗した NAC フレームワーク セッションのデフォルトの ACL として使用されるように ACL を指定するには、nac ポリシー nac フレームワーク コンフィギュレーション モードで **default-acl** コマンドを使用します。このコマンドを NAC ポリシーから削除するには、このコマンドの **no** 形式を使用します。

[**no**] **default-acl** *acl-name*

構文の説明

acl-name	セッションに適用されるアクセス コントロール リストの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
nac ポリシー nac フレームワーク コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.0(2)	コマンド名から「nac-」が削除されました。コマンドが、グループ ポリシー コンフィギュレーション モードから nac ポリシー nac フレームワーク コンフィギュレーション モードに移動されました。

使用上のガイドライン

各グループ ポリシーは、ポリシーに一致し、NAC に対して適格なホストに適用されるデフォルト ACL を指しています。ASA は、ポスチャ検証の前に NAC のデフォルト ACL を適用します。ポスチャ検証の後、ASA はデフォルト ACL をリモート ホストのアクセス コントロール サーバから取得した ACL に置き換えます。ポスチャ確認が失敗した場合は、デフォルト ACL がそのまま使われます。

また、ASA は、クライアントレス認証がイネーブルになっている（デフォルト設定）場合にも、NAC のデフォルト ACL を適用します。

例

次に、ポスチャ検証が成功する前に適用される ACL として acl-1 を指定する例を示します。

```
ciscoasa(config-group-policy)# default-acl acl-1
ciscoasa(config-group-policy)
```

次の例では、デフォルト グループ ポリシーから ACL を継承しています。

```
ciscoasa(config-group-policy)# no default-acl
ciscoasa(config-group-policy)
```

関連コマンド

コマンド	説明
nac-policy	Cisco NAC ポリシーを作成してアクセスし、そのタイプを指定します。
nac-settings	NAC ポリシーをグループ ポリシーに割り当てます。
debug nac	NAC フレームワーク イベントのロギングをイネーブルにします。
show vpn-session_summary.db	IPsec、WebVPN、および NAC セッションの数を表示します。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。

default-domain

グループ ポリシーのユーザのデフォルト ドメイン名を設定するには、グループ ポリシー コンフィギュレーション モードで **default-domain** コマンドを使用します。ドメイン名を削除するには、このコマンドの **no** 形式を使用します。

default-domain {**value** *domain-name* | **none**}

no default-domain [*domain-name*]

構文の説明

none	デフォルト ドメイン名がないことを指定します。デフォルト ドメイン名にヌル値を設定して、デフォルト ドメイン名を拒否します。デフォルトまたは指定したグループ ポリシーのデフォルト ドメイン名は継承されません。
value *domain-name*	グループのデフォルト ドメイン名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ユーザがドメイン名を継承しないようにするには、**default-domain none** コマンドを使用します。

ASA は、ドメイン フィールドを省略した DNS クエリーに追加するために、AnyConnect セキュア モビリティ クライアントまたはレガシーの VPN クライアント（IPsec/IKEv1）にデフォルト ドメイン名を渡します。このドメイン名は、トンネル パケットにのみ適用されます。デフォルト ドメイン名がない場合、ユーザはデフォルト グループ ポリシーのデフォルト ドメイン名を継承します。

デフォルト ドメイン名に使用できるのは、英数字、ハイフン（-）、およびピリオド（.）のみです。

例

次に、FirstGroup という名前のグループ ポリシーに対して、FirstDomain のデフォルト ドメイン名を設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# default-domain value FirstDomain
```

関連コマンド

コマンド	説明
split-dns	スプリット トンネルを介して解決されるドメインのリストを提供します。
split-tunnel-network-list	トンネリングが必要なネットワークと不要なネットワークを区別するために、ASA が使用するアクセス リストを指定します。
split-tunnel-policy	IPsec クライアントが条件に応じてパケットを暗号化形式で IPsec トンネルを経由して転送したり、クリア テキスト形式でネットワーク インターフェイスに転送したりできるようにします。

default enrollment

すべての登録パラメータをシステム デフォルト値に戻すには、クリプト CA トラストポイント コンフィギュレーション モードで **default enrollment** コマンドを使用します。

default enrollment

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドの呼び出しは、アクティブなコンフィギュレーションには含まれません。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、すべての登録パラメータをトラストポイント central 内のデフォルト値に戻す例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# default enrollment
ciscoasa(ca-trustpoint)#
```

関連コマンド

コマンド	説明
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。
crl configure	CRL コンフィギュレーション モードを開始します。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。

default-group-policy（imap4s、pop3s、smtps）（廃止）

(注) このコマンドをサポートする最後のリリースは、7.5(1) でした。

電子メール プロキシ設定でグループ ポリシーが指定されない場合に使用するグループ ポリシーの名前を指定するには、さまざまなコンフィギュレーション モードで **default-group-policy** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

default-group-policy *groupname*

no default-group-policy

構文の説明

groupname	デフォルト グループ ポリシーとして使用する、設定済みのグループ ポリシーを指定します。**group-policy** コマンドを使用して、グループ ポリシーを設定します。

デフォルト

DfltGrpPolicy という名前のデフォルト グループ ポリシーは、常に、ASA に存在します。この **default-group-policy** コマンドを使用すると、作成したグループ ポリシーを、電子メール プロキシ セッション用のデフォルト グループ ポリシーとして置き換えることができます。または、DfltGrpPolicy を編集することもできます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
Imap4s コンフィギュレーション	• 対応	—	• 対応	—	—
Pop3s コンフィギュレーション	• 対応	—	• 対応	—	—
smtps コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

Version	変更内容
7.0(1)	このコマンドが追加されました。
7.5(2)	このコマンドは廃止されました。

使用上のガイドライン

セッション、IMAP4S セッション、POP3S セッション、および SMTPS セッションには、指定されたグループ ポリシーまたはデフォルト グループ ポリシーが必要です。このコマンドは、該当する電子メール プロキシ モードで使用します。

システムの DefaultGroupPolicy は編集できますが、削除はしないでください。DefaultGroupPolicy の AVP は、次のとおりです。

属性	デフォルト値
wins-server	none
dns-server	none
dhcp-network-scope	none
vpn-access-hours	unrestricted
vpn-simultaneous-logins	3
vpn-idle-timeout	30 分
vpn-session-timeout	none
vpn-filter	none
vpn-tunnel-protocol	WebVPN
ip-comp	disable
re-xauth	disable
group-lock	none
pfs	disable
client-access-rules	none
banner	none
password-storage	disabled
ipsec-udp	disabled
ipsec-udp-port	0
backup-servers	keep-client-config
split-tunnel-policy	tunnelall
split-tunnel-network-list	none
default-domain	none
split-dns	none
intercept-dhcp	disable
client-firewall	none
secure-unit-authentication	disabled
user-authentication	disabled
user-authentication-idle-timeout	none
ip-phone-bypass	disabled
leap-bypass	disabled
nem	disabled

例

次に、pop3s という名前の POP3S のデフォルト グループ ポリシーを指定する例を示します。

```
ciscoasa(config)# pop3s
ciscoasa(config-webvpn)# default-group-policy pop3s
```

default-group-policy（トンネル グループ一般属性）

ユーザがデフォルトで継承する属性のセットを指定するには、トンネル グループ一般属性コンフィギュレーション モードで **default-group-policy** コマンドを使用します。デフォルトのグループ ポリシー名を削除するには、このコマンドの **no** 形式を使用します。

default-group-policy *group-name*

no default-group-policy *group-name*

構文の説明

group-name	デフォルト グループの名前を指定します。

デフォルト

デフォルト グループ名は DfltGrpPolicy です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

Version	変更内容
7.0(1)	このコマンドが追加されました。
7.1(1)	webvpn コンフィギュレーション モードの **default-group-policy** コマンドは廃止されました。このコマンドは、トンネル グループ一般属性モードの **default-group-policy** コマンドに置き換えられています。

使用上のガイドライン

バージョン 7.1(1) では、このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ一般属性モードの同等のコマンドに変換されます。

デフォルト グループ ポリシー DfltGrpPolicy には、ASA が初期設定されています。この属性は、すべてのトンネル グループ タイプに適用できます。

例

次に、config-general コンフィギュレーション モードを開始し、ユーザがデフォルトで、「standard-policy」という IPsec LAN-to-LAN トンネル グループの属性セットを継承するように指定する例を示します。このコマンド セットでは、アカウンティング サーバ、認証サーバ、認可サーバ、およびアドレス プールを定義します。

```
ciscoasa(config)# tunnel-group standard-policy type ipsec-ra
ciscoasa(config)# tunnel-group standard-policy general-attributes
ciscoasa(config-tunnel-general)# default-group-policy first-policy
```

```
ciscoasa(config-tunnel-general)# accounting-server-group aaa-server123
ciscoasa(config-tunnel-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
ciscoasa(config-tunnel-general)# authentication-server-group aaa-server456
ciscoasa(config-tunnel-general)# authorization-server-group aaa-server78
ciscoasa(config-tunnel-general)#
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
group-policy	グループ ポリシーを作成または編集します。
show running-config tunnel group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。

default-idle-timeout

WebVPN ユーザのデフォルト アイドル タイムアウト値を設定するには、webvpn コンフィギュレーション モードで **default-idle-timeout** コマンドを使用します。デフォルトのタイムアウト値をコンフィギュレーションから削除し、デフォルトをリセットするには、このコマンドの **no** 形式を使用します。

default-idle-timeout *seconds*

no default-idle-timeout

構文の説明

seconds	アイドル タイムアウトの秒数を指定します。最小値は 60 秒で、最大値は 1 日（86400 秒）です。

デフォルト

1800 秒（30 分）。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ユーザのアイドル タイムアウトが定義されていない場合、値が 0 の場合、または値が有効な値の範囲外である場合に、ASA では、ここで設定した値が使用されます。デフォルト アイドル タイムアウトにより、セッションの失効を回避できます。

クッキーがディセーブルに設定されているブラウザ（またはクッキーを求めた後クッキーを拒否するブラウザ）を使用すると、接続されていないユーザがセッション データベースに出現する可能性があるため、このコマンドは短時間に設定することを推奨します。許可される最大接続数が（**vpn-simultaneous-logins** コマンドを介して）1 に設定されている場合、最大接続数がすでに存在することがデータベースによって示されるため、ユーザは再ログインすることができません。アイドル タイムアウトを短く設定すると、このようなファントム セッションを迅速に削除し、ユーザが再ログインできるようにすることができます。

例

次に、デフォルト アイドル タイムアウトを 1200 秒（20 分）に設定する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# default-idle-timeout 1200
```

関連コマンド

コマンド	説明
vpn-simultaneous-logins	許可される同時 VPN セッションの最大数を設定します。

default-information

EIGRP ルーティング プロセスのデフォルト ルート情報候補を制御するには、ルータ EIGRP コンフィギュレーション モードで **default-information** コマンドを使用します。着信更新または発信更新で EIGRP デフォルト ルート情報候補を非表示にするには、このコマンドの **no** 形式を使用します。

default-information {**in** | **out**} [*acl-name*]

no default-information {**in** | **out**}

構文の説明

acl-name	(オプション)名前付きの標準アクセス リストを指定します。
in	外部のデフォルト ルーティング情報を受け入れるように EIGRP を設定します。
out	外部ルーティング情報をアドバタイズするように EIGRP を設定します。

デフォルト

外部ルートが受け入れられ、送信されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ EIGRP コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

アクセス リストが指定されたこのコマンドまたは **default-information** コマンドの **no** 形式のみが実行コンフィギュレーションに表示されます。これは、デフォルト ルーティング情報候補がデフォルトで受け入れられ、送信されるためです。このコマンドの **no** 形式には、*acl-name* 引数はありません。

例

次に、外部デフォルト ルート情報またはデフォルト ルート情報候補の受領をディセーブルにする例を示します。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# no default-information in
```

関連コマンド

コマンド	説明
router eigrp	EIGRP ルーティング プロセスを作成し、このプロセスのコンフィギュレーション モードを開始します。

default-information originate

IS-IS ルーティング ドメインへのデフォルト ルートを生成するには、ISIS コンフィギュレーション モードで **default-information originate** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

default-information originate [route-map *map-name***]**

no default-information originate [route-map *map-name***]**

構文の説明

route-map	（任意）ルーティング プロセスは、ルート マップが満たされている場合にデフォルト ルートを生成します。
map-name	ルート マップ名。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ isis コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用して設定されたルータがルーティング テーブルに 0.0.0.0 へのルートを持っている場合、IS-IS は LSP で 0.0.0.0 に対するアドバタイズメントを発信します。

ルート マップが存在しない場合、デフォルトではレベル 2 LSP だけでアドバタイズされます。レベル 1 ルーティングでデフォルト ルートを発見するメカニズムには、最も近いレベル 1 またはレベル 2 ルータを探すというものがあります。最も近いレベル 1 またはレベル 2 ルータは、レベル 1 LSP で Attach ビット（ATT）を調べることにより検出できます。

ルート マップは次の 2 つの目的で使用できます。

- ASA にレベル 1 LSP でデフォルトを生成させます。
- 条件に従って 0/0 をアドバタイズします。

match ip address standard-access-list コマンドを使用して、ルータが 0/0 をアドバタイズする前に存在しなければならない 1 つ以上の IP ルートを指定することができます。

例

次に示す例は、ソフトウェアにデフォルト外部ルートを IS-IS ドメイン内に生成させる例を示します。

```
router isis
! ISIS routes will be distributed into IS-IS
redistribute isis 120 metric
! access list 2 is applied to outgoing routing updates
default-information originate
! access list 2 defined as giving access to network 10.105.0.0
access-list 2 permit 10.105.0.0 0.0.255.255
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。

コマンド	説明
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト(TLV)を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。

コマンド	説明
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

default-information originate（アドレス ファミリ）

デフォルト ルート（ネットワーク 0.0.0.0）を配布するように Border Gateway Protocol（BGP）ルーティング プロセスを設定するには、アドレス ファミリ コンフィギュレーション モードで **default-information originate** コマンドを使用します。デフォルト ルートのアドバタイズメントをディセーブルにするには、このコマンドの **no** 形式を使用します。

default-information originate

no default-information originate

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
アドレス ファミリ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

default-information originate コマンドは、デフォルト ルート（ネットワーク 0.0.0.0）をアドバタイズするように BGP ルーティング プロセスを設定するために使用されます。再配布ステートメントも、この設定を完了するように設定されている必要があります。そうでない場合、デフォルト ルートはアドバタイズされません。

BGP の **default-information originate** コマンドの設定は、**network (BGP)** コマンドの設定に似ています。ただし、**default-information originate** コマンドは、ルート 0.0.0.0 の明示的な再配布が必要です。**network** コマンドでは、ルート 0.0.0.0 が内部ゲートウェイ プロトコル（IGP）のルーティング テーブルに存在することのみが必要です。したがって、**network** コマンドが優先されます。

（注） **default-information originate** コマンドは、同じルータで **neighbor default-originate** コマンドとともに設定しないでください。どちらか一方を設定する必要があります。

例

次の例では、ルータは BGP ルーティング プロセスに OSPF からデフォルト ルートを再配布するように設定されます。

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# default-information originate
ciscoasa(config-router-af)# redistribute ospf 100
```

関連コマンド

コマンド	説明
network	Border Gateway Protocol（BGP）およびマルチプロトコル BGP ルーティング プロセスによってアドバタイズされるネットワークを指定します。
neighbor default-originate	BGP スピーカー（ローカル ルータ）にネイバーへのデフォルト ルート 0.0.0.0 の送信を許可して、このルートがデフォルト ルートとして使用されるようにします。

default-information originate（IPv6 ルータ OSPF、ルータ OSPF）

OSPFv2 または OSPFv3 ルーティング ドメインへのデフォルトの外部ルートを生成するには、ルータ コンフィギュレーション モードまたは IPv6 ルータ コンフィギュレーション モードで **default-information originate** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

default-information originate [**always**] [**metric** *value*] [**metric-type** {**1** | **2**}] [**route-map** *map-name*]

no default-information originate [[**always**] [**metric** *value*] [**metric-type** {**1** | **2**}] [**route-map** *map-name*]]

構文の説明

always	（オプション）ソフトウェアにデフォルト ルートがあるかどうかにかかわらず、常に、デフォルト ルートをアドバタイズします。
metric *value*	（オプション）OSPF のデフォルト メトリック値を、0 ～ 16777214 の範囲で指定します。
metric-type {**1** | **2**}	（任意）OSPF ルーティング ドメインにアドバタイズされるデフォルトのルートに関連付けられる外部リンク タイプを指定します。有効な値は、次のとおりです。 • **1**: タイプ 1 の外部ルート • **2**: タイプ 2 の外部ルート
route-map *map-name*	（オプション）適用するルート マップの名前を指定します。

デフォルト

デフォルト値は次のとおりです。

- **metric** *value* は 10 です。
- **metric-type** は 2 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
IPv6 ルータ OSPF コンフィギュレーション	• 対応	—	• 対応	—	—
ルータ OSPF コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	OSPFv3 のサポートが追加されました。

使用上のガイドライン

このコマンドの **no** 形式をオプションのキーワードおよび引数とともに使用すると、コマンドからオプションの情報のみが削除されます。たとえば、**no default-information originate metric** *3* コマンドを入力すると、実行コンフィギュレーションのコマンドから **metric** *3* オプションが削除されます。コマンド全体を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式をオプションなしで使用します（**no default-information originate**）。

例

次に、オプションのメトリックおよびメトリック タイプとともに **default-information originate** コマンドを使用する例を示します。

```
ciscoasa(config-rtr)# default-information originate always metric 3 metric-type 2
ciscoasa(config-rtr)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションの OSPFv2 コマンドを表示します。
ipv6 router ospf	IPv6 のルータ コンフィギュレーション モードを開始します。
show running-config ipv6 router	グローバル ルータ コンフィギュレーションの OSPFv3 コマンドを表示します。

default-information originate（ルータ RIP）

RIP へのデフォルト ルートを生成するには、ルータ コンフィギュレーション モードで **default-information originate** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

default-information originate [**route-map** *name*]

no default-information originate [**route-map** *name*]

構文の説明

route-map *name*	（任意）適用するルート マップ名。ルート マップが一致すると、ルーティング プロセスによってデフォルト ルートが生成されます。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ RIP コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

default-information originate コマンドで参照されるルート マップは拡張アクセス リストを使用できません。標準のアクセス リストのみを使用できます。

例

次に、デフォルト ルートを RIP に生成する例を示します。

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# default-information originate
```

関連コマンド

コマンド	説明
router rip	RIP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

default-language

クライアントレス SSL VPN ページに表示されるデフォルト言語を設定するには、webvpn コンフィギュレーション モードで **default-language** コマンドを使用します。

default-language *language*

構文の説明

language	事前にインポート済みの変換テーブルの名前を指定します。

デフォルト

デフォルト言語は en-us（米国で使用されている英語）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

ASA では、ブラウザベースのクライアントレス SSL VPN 接続を開始するユーザに表示されるポータルと画面、および AnyConnect VPN クライアント ユーザに表示されるユーザ インターフェイスで使用される言語を変換できます。適切なコンプライアンスを実現するために、language パラメータは RFC-1766 で定義されている形式を使用する必要があります。

クライアントレス SSL VPN ユーザが最初に ASA に接続しログインする前にデフォルトの言語が表示されます。その後は、トンネル グループ設定またはトンネル ポリシー設定およびこれらの設定が参照するカスタマイズに基づいて言語が表示されます。

例

次に、*Sales* という名前を指定して、デフォルト言語を中国語に変更する例を示します。

```
ciscoasa(config-webvpn)# default-language zh
```

関連コマンド

コマンド	説明
import webvpn translation-table	変換テーブルをインポートします。
revert	キャッシュ メモリから変換テーブルを削除します。
show import webvpn translation-table	インポートした変換テーブルに関する情報を表示します。

default-mapping-rule

マッピングアドレスおよびポート(MAP)ドメイン内のデフォルト マッピング ルールを設定するには、MAP ドメインのコンフィギュレーション モードで **default-mapping-rule** コマンドを使用します。基本マッピングルールを削除するには、このコマンドの **no** 形式を使用します。

default-mapping-rule *ipv6_prefix/prefix_length*

no default-mapping-rule *ipv6_prefix/prefix_length*

構文の説明

ipv6_prefix/prefix_length	RFC 6052 に従って IPv4 宛先アドレスを埋め込むために使用される IPv6 プレフィックス。通常のプレフィックスの長さは 64 ですが、使用可能な値は 32、40、48、56、64、または 96 です。埋め込み IPv4 アドレスの後の任意の末尾ビットは 0 に設定されます。

デフォルト

デフォルト設定はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
MAP ドメイン コンフィギュレーション モード	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.13(1)	このコマンドが導入されました。

使用上のガイドライン

ボーダーリレー(BR)デバイスはこのルールを使用し、MAP ドメイン外のすべての IPv4 アドレスを、MAP ドメイン内で動作する IPv6 アドレスに変換します。MAP ドメイン内の MAP-T カスタマーエッジ(CE)デバイスは、このルールを使用して IPv4 デフォルトルートをインストールします。

例

次の例では、1 という名前の MAP-T ドメインを作成して、ドメインの変換ルールを設定しています。

```
ciscoasa(config)# map-domain 1
ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64
ciscoasa(config-map-domain)# basic-mapping-rule
ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
```

```
ciscoasa(config-map-domain-bmr)# start-port 1024
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

関連コマンド

コマンド	説明
basic-mapping-rule	MAP ドメインの基本マッピング ルールを設定します。
default-mapping-rule	MAP ドメインのデフォルト マッピング ルールを設定します。
ipv4-prefix	MAP ドメインの基本マッピング ルールの IPv4 プレフィックスを設定します。
ipv6-prefix	MAP ドメインの基本マッピング ルールの IPv6 プレフィックスを設定します。
map-domain	マッピング アドレスおよびポート(MAP)ドメインを設定します。
share-ratio	MAP ドメインの基本マッピング ルールのポート数を設定します。
show map-domain	マッピング アドレスおよびポート(MAP)ドメインに関する情報を表示します。
start-port	MAP ドメインの基本マッピング ルールの開始ポートを設定します。

default-mcast-group

VTEP 送信元インターフェイスに関連付けられているすべての VXLAN VNI インターフェイスにデフォルトのマルチキャスト グループを指定するには、NVE コンフィギュレーション モードで **default-mcast-group** コマンドを使用します。デフォルト グループを削除するには、このコマンドの **no** 形式を使用します。

default-mcast-group *mcast_ip*

no default-mcast-group

構文の説明

mcast_ip	デフォルトのマルチキャスト グループの IP アドレスを設定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
Nve コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

ASA がピア VTEP の背後にあるデバイスにパケットを送信する場合、ASA には次の 2 つの重要な情報が必要です。

- リモート デバイスの宛先 MAC アドレス
- ピア VTEP の宛先 IP アドレス

ASA がこの情報を検出するには 2 つの方法あります。

- 単一のピア VTEP IP アドレスを ASA に静的に設定できます。

  手動で複数のピアを定義することはできません。

  ASA が VXLAN カプセル化 ARP ブロードキャストを VTEP に送信し、エンド ノードの MAC アドレスを取得します。

- マルチキャスト グループは、VNI インターフェイスごとに（または、**default-mcast-address** コマンドを使用して VTEP 全体に）設定できます。

  ASA は、IP マルチキャスト パケット内の VXLAN カプセル化 ARP ブロードキャスト パケットを VTEP 送信元インターフェイスを経由して送信します。この ARP 要求への応答により、ASA はリモート VTEP の IP アドレスと、リモート エンド ノードの宛先 MAC アドレスの両方を取得することができます。

ASA は VNI インターフェイスのリモート VTEP IP アドレスに対する宛先 MAC アドレスのマッピングを維持します。

VNI インターフェイスごとにマルチキャスト グループを設定していない場合は、デフォルトのグループが使用されます。その VNI インターフェイス レベルでグループを設定している場合は、そのグループがこの設定よりも優先されます。

例

次に、GigabitEthernet 1/1 インターフェイスを VTEP 送信元インターフェイスとして設定し、デフォルトのマルチキャスト グループ 236.0.0.100 を指定する例を示します。

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# nve 1
ciscoasa(cfg-nve)# source-interface outside
ciscoasa(cfg-nve)# default-mcast-group 236.0.0.100
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
default-mcast-group	VTEP 送信元インターフェイスに関連付けられているすべての VNI インターフェイスのデフォルトのマルチキャスト グループを指定します。
encapsulation vxlan	NVE インスタンスを VXLAN カプセル化に設定します。
inspect vxlan	標準 VXLAN ヘッダー形式に強制的に準拠させます。
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
mcast-group	VNI インターフェイスのマルチキャスト グループ アドレスを設定します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
nve-only	VXLAN 送信元インターフェイスが NVE 専用であることを指定します。
peer ip	ピア VTEP の IP アドレスを手動で指定します。
segment-id	VNI インターフェイスの VXLAN セグメント ID を指定します。
show arp vtep-mapping	リモート セグメント ドメインにある IP アドレスとリモート VTEP IP アドレス用の VNI インターフェイスにキャッシュされた MAC アドレスを表示します。
show interface vni	VNI インターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス（設定されている場合）のステータス、ならびに関連付けられている NVE インターフェイスを表示します。
show mac-address-table vtep-mapping	リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ 2 転送テーブル（MAC アドレス テーブル）を表示します。

コマンド	説明
show nve	NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリア インターフェイス（送信元インターフェイス）のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。
show vni vlan-mapping	VNI セグメント ID と、VLAN インターフェイスまたはトランスペアレント モードの物理インターフェイス間のマッピングを表示します。
source-interface	VTEP 送信元インターフェイスを指定します。
vtep-nve	VNI インターフェイスを VTEP 送信元インターフェイスに関連付けます。
vxlan port	VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。

default-metric

再配布されるルートの EIGRP メトリックを指定するには、ルータ コンフィギュレーション モードで **default-metric** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

default-metric *bandwidth delay reliability loading mtu*

no default-metric *bandwidth delay reliability loading mtu*

構文の説明

bandwidth	ルートの最小帯域幅（KB/秒単位）。有効な値は、1 ～ 4294967295 です。
delay	ルート遅延（10 マイクロ秒単位）。有効な値は、1 ～ 4294967295 です。
loading	ルートの有効な帯域幅。1 ～ 255 の数値で表されます（255 は 100 % のロード）。
mtu	許可する MTU の最小値（バイト単位）。有効値は 1 ～ 65535 です。
reliability	正常なパケット伝送の可能性。0 ～ 255 の数値で表されます。値 255 は 100 % の信頼性を意味し、0 は信頼性がないことを意味します。

デフォルト

デフォルト メトリックなしで再配布できるのは、接続されているルートのみです。再配布される接続ルートのメトリックは、0 に設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

redistribute コマンドで **metric** キーワードおよび属性を使用しない場合は、デフォルト メトリックを使用して、EIGRP にプロトコルを再配布する必要があります。メトリックのデフォルトは、さまざまなネットワークで機能するよう慎重に設定されています。値を変更する場合は、最大限の注意を払うようにしてください。スタティック ルートから再配布する場合のみ、同じメトリックを維持できます。

IPv6 対応インターフェイスで許可される最小 MTU は 1280 バイトです。ただし、IPsec がインターフェイスでイネーブルになっている場合、MTU 値は、IPsec 暗号化のオーバーヘッドのために 1380 未満に設定できません。インターフェイスを 1380 バイト未満に設定すると、パケットのドロップが発生する可能性があります。

例

次に、再配布された RIP ルート メトリックが EIGRP メトリックに変換される例を示します。使用する値は、次のとおりです。bandwidth = 1000、delay = 100、reliability = 250、loading = 100、および MTU = 1500。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 172.16.0.0
ciscoasa(config-router)# redistribute rip
ciscoasa(config-router)# default-metric 1000 100 250 100 1500
```

関連コマンド

コマンド	説明
router eigrp	EIGRP ルーティング プロセスを作成して、そのプロセスのルータ コンフィギュレーション モードを開始します。
redistribute（EIGRP）	EIGRP ルーティング プロセスにルートを再配布します。

default user group

クラウド Web セキュリティの場合、ASA に入ってくるユーザのアイデンティティを ASA が判別できない場合のデフォルトのユーザ名やグループを指定するには、パラメータ コンフィギュレーション モードで **default user group** コマンドを使用します。デフォルトのユーザまたはグループを削除するには、このコマンドの **no** 形式を使用します。パラメータ コンフィギュレーション モードにアクセスするには、まず **policy-map type inspect scansafe** コマンドを入力します。

default {[**user** *username*] [**group** *groupname*]}

no default [**user** *username*] [**group** *groupname*]

構文の説明

username	デフォルトのユーザ名を指定します。
groupname	デフォルトのグループ名を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASA に入ってくるユーザのアイデンティティを ASA が判別できない場合、デフォルトのユーザやグループが HTTP ヘッダーに含まれています。

例

次に、デフォルト名を「Boulder」、グループ名を「Cisco」として設定する例を示します。

```
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# http
ciscoasa(config-pmap-p)# default name Boulder group Cisco
```

関連コマンド

コマンド	説明
class-map type inspect scansafe	ホワイトリストに記載されたユーザとグループのインスペクション クラス マップを作成します。
http[s]（パラメータ）	インスペクション ポリシー マップのサービス タイプ（HTTP または HTTPS）を指定します。
inspect scansafe	このクラスのトラフィックに対するクラウド Web セキュリティ インスペクションをイネーブルにします。
license	要求の送信元の組織を示すため、ASA がクラウド Web セキュリティ プロキシ サーバに送信する認証キーを設定します。
match user group	ユーザまたはグループをホワイトリストと照合します。
policy-map type inspect scansafe	インスペクション ポリシー マップを作成すると、ルールのために必要なパラメータを設定し、任意でホワイトリストを識別できます。
retry-count	再試行回数値を入力します。この値は、可用性をチェックするために、クラウド Web セキュリティ プロキシ サーバをポーリングする前に ASA が待機する時間です。
scansafe	マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可します。
scansafe general-options	汎用クラウド Web セキュリティ サーバ オプションを設定します。
server {**primary** | **backup**}	プライマリまたはバックアップのクラウド Web セキュリティ プロキシ サーバの完全修飾ドメイン名または IP アドレスを設定します。
show conn scansafe	大文字の Z フラグに示されたようにすべてのクラウド Web セキュリティ接続を表示します。
show scansafe server	サーバが現在のアクティブ サーバ、バックアップ サーバ、または到達不能のいずれであるか、サーバのステータスを表示します。
show scansafe statistics	合計と現在の http 接続を表示します。
user-identity monitor	AD エージェントから指定したユーザまたはグループ情報をダウンロードします。
whitelist	トラフィックのクラスでホワイトリスト アクションを実行します。

遅延

インターフェイスの遅延値を設定するには、インターフェイス コンフィギュレーション モードで **delay** コマンドを使用します。デフォルトの遅延値に戻すには、このコマンドの **no** 形式を使用します。

delay *delay-time*

no delay

構文の説明

delay-time	遅延時間（10 マイクロ秒単位）。有効な値は、1 ～ 16777215 です。

デフォルト

デフォルトの遅延はインターフェイス タイプによって異なります。インターフェイスのデフォルト値を確認するには、**show interface** コマンドを使用します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.1(6)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

値は 10 マイクロ秒単位で入力します。**show interface** の出力に表示される遅延値は、マイクロ秒単位です。

例

次に、インターフェイスの遅延をデフォルトの 1000 から 2000 に変更する例を示します。**delay** コマンドの前と後に切り捨てられた **show interface** コマンドの出力が含まれ、このコマンドが遅延値にどのように影響を与えるかを示します。遅延値は、**show interface** の出力の 2 行め、DLY ラベルの後に記載されます。

遅延値を 2000 に変更するために入力するコマンドは、**delay 2000** ではなく **delay 200** です。これは、**delay** コマンドで入力する値が 10 マイクロ秒単位であり、**show interface** の出力ではマイクロ秒単位で表示されるためです。

```
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# show interface Ethernet0/0
```

```
Interface Ethernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 100 Mbps, DLY 1000 usec
        Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
        MAC address 0013.c480.7e16, MTU 1500
        IP address 10.86.194.224, subnet mask 255.255.254.0
! Remainder of the output removed

ciscoasa(config-if)# delay 200
ciscoasa(config-if)# show interface Ethernet0/0

Interface Ethernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 100 Mbps, DLY 2000 usec
        Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
        MAC address 0013.c480.7e16, MTU 1500
        IP address 10.86.194.224, subnet mask 255.255.254.0
! Remainder of the output removed
```

関連コマンド

コマンド	説明
show interface	インターフェイスの統計情報および設定を表示します。

delete

フラッシュ メモリからファイルを削除するには、特権 EXEC モードで **delete** コマンドを使用します。

delete [**/noconfirm**] [**/recursive**] [**/replicate**] [**disk0: | disk1: | flash:**] [*path/*] *filename*

構文の説明

/noconfirm	（任意）確認のためのプロンプトを表示しないように指定します。
/recursive	（任意）すべてのサブディレクトリの指定されたファイルを再帰的に削除します。
/replicate	（オプション）スタンバイ ユニットの指定されたファイルを削除します。
disk0:	（オプション）内部のフラッシュ メモリを指定します。
disk1:	（オプション）外部フラッシュ メモリ カードを指定します。
filename	削除するファイルの名前を指定します。
flash:	（オプション）内部のフラッシュ メモリを指定します。このキーワードは、**disk0** と同じです。
path/	（任意）ファイルのパスに指定します。

デフォルト

ディレクトリを指定しない場合、ディレクトリはデフォルトで現在の作業ディレクトリになります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

パスを指定しない場合は、現在の作業ディレクトリからファイルが削除されます。ファイルの削除では、ワイルドカードがサポートされています。ファイルを削除する場合、ファイル名のプロンプトが表示され、削除を確認する必要があります。

例

次に、現在の作業ディレクトリから test.cfg という名前のファイルを削除する例を示します。

```
ciscoasa# delete test.cfg
```

関連コマンド

コマンド	説明
cd	現在の作業ディレクトリから、指定したディレクトリに変更します。
rmdir	ファイルまたはディレクトリを削除します。
show file	指定されたファイルを表示します。

deny-message

WebVPN に正常にログインしたが、VPN 特権を持たないリモート ユーザに配信されるメッセージを変更するには、グループ webvpn コンフィギュレーション モードで **deny-message value** コマンドを使用します。文字列を削除して、リモート ユーザがメッセージを受信しないようにするには、このコマンドの **no** 形式を使用します。

deny-message value *string*

no deny-message value

構文の説明

string	491 文字以下の英数字。特殊文字、スペース、および句読点を含みます。

デフォルト

デフォルトの拒否メッセージは次のとおりです。「Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features. Contact your IT administrator for more information.」

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.1(1)	このコマンドは、トンネル グループ webvpn コンフィギュレーション モードからグループ webvpn コンフィギュレーション モードに変更されました。

使用上のガイドライン

このコマンドを入力する前に、グローバル コンフィギュレーション モードで **group-policy** *name* **attributes** コマンドを入力してから、**webvpn** コマンドを入力する必要があります(この手順は、ポリシー name が作成済みであることを前提としています)。

no deny-message none コマンドは、グループ webvpn コンフィギュレーションから属性を削除します。ポリシーは属性値を継承します。

deny-message value コマンドへのストリングの入力時は、コマンドがラップしている場合でも引き続き入力します。

VPN セッションに使用されるトンネル ポリシーとは独立して、ログイン時にリモート ユーザのブラウザにテキストが表示されます。

例

次に、group2 という名前の内部グループ ポリシーを作成する最初のコマンドの例を示します。後続のコマンドによって、このポリシーに関連付けられている拒否メッセージを変更します。

```
ciscoasa(config)# group-policy group2 internal
ciscoasa(config)# group-policy group2 attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# deny-message value "Your login credentials are OK. However,
you have not been granted rights to use the VPN features. Contact your administrator for
more information."
ciscoasa(config-group-webvpn)
```

関連コマンド

コマンド	説明
clear configure group-policy	すべてのグループ ポリシー コンフィギュレーションを削除します。
group-policy	グループ ポリシーを作成します。
group-policy attributes	グループ ポリシー属性コンフィギュレーション モードを開始します。
show running-config group-policy	指定したポリシーの実行グループ ポリシー コンフィギュレーションが表示されます。
webvpn	グループ ポリシー webvpn コンフィギュレーション モードを開始します。

deny version

SNMP トラフィックの特定のバージョンを拒否するには、SNMP マップ コンフィギュレーション モードで **deny version** コマンドを使用します。このコマンドをディセーブルにするには、このコマンドの **no** 形式を使用します。

deny version *version*

no deny version *version*

構文の説明

version	ASA がドロップする SNMP トラフィックのバージョンを指定します。使用可能な値は、**1**、**2**、**2c**、および **3** です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
SNMP マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

SNMP トラフィックを特定の SNMP バージョンに制限するには、**deny version** コマンドを使用します。以前のバージョンの SNMP はセキュリティがより低いため、セキュリティ ポリシーで SNMP トラフィックを Version 2 に制限できます。グローバル コンフィギュレーション モードで **snmp-map** コマンドを入力してアクセスできる **snmp-map** コマンドを使用して設定する SNMP マップ内で、**deny version** を使用します。SNMP マップの作成後に、**inspect snmp** コマンドを使用してこのマップをイネーブルにし、**service-policy** コマンドを使用して 1 つ以上のインターフェイスに適用します。

例

次に、SNMP トラフィックを指定し、SNMP マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイス適用する例を示します。

```
ciscoasa(config)# access-list snmp-acl permit tcp any any eq 161
ciscoasa(config)# access-list snmp-acl permit tcp any any eq 162
ciscoasa(config)# class-map snmp-port
ciscoasa(config-cmap)# match access-list snmp-acl
```

```
ciscoasa(config-cmap)# exit
ciscoasa(config)# snmp-map inbound_snmp
ciscoasa(config-snmp-map)# deny version 1
ciscoasa(config-snmp-map)# exit
ciscoasa(config)# policy-map inbound_policy
ciscoasa(config-pmap)# class snmp-port
ciscoasa(config-pmap-c)# inspect snmp inbound_snmp
ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy inbound_policy interface outside
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
inspect snmp	SNMP アプリケーション インスペクションをイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
snmp-map	SNMP マップを定義し、SNMP マップ コンフィギュレーション モードをイネーブルにします。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

description

指定したコンフィギュレーション ユニット（たとえば、コンテキスト、オブジェクト グループ、または DAP レコード）に対する説明を追加するには、各コンフィギュレーション モードで **description** コマンドを使用します。説明を削除するには、このコマンドの **no** 形式を使用します。

description *text*

no description

構文の説明

text	説明を最大 200 文字のテキスト文字列で設定します。説明は、コンフィギュレーションの情報として役立ちます。ダイナミック アクセス ポリシー レコード モードの場合、最大長は 80 文字です。イベント マネージャ アプレットの場合、最大長は 256 文字です。 ストリングに疑問符（?）を含める場合は、不注意から CLI ヘルプを呼び出さないように、Ctrl+V を入力してから疑問符を入力する必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

このコマンドは、さまざまなコンフィギュレーション モードで使用できます。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(2)	ダイナミック アクセス ポリシー レコード コンフィギュレーション モードのサポートが追加されました。
9.2(1)	イベント マネージャ アプレット コンフィギュレーション モードのサポートが追加されました。

例

次に、「管理」コンテキスト コンフィギュレーションに説明を追加する例を示します。

```
ciscoasa(config)# context administrator
ciscoasa(config-context)# description This is the admin context.
ciscoasa(config-context)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-context)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-context)# config-url flash://admin.cfg
```

関連コマンド

コマンド	説明
class-map	**policy-map** コマンドのアクションを適用するトラフィックを指定します。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
object-group	**access-list** コマンドに含めるトラフィックを指定します。
policy-map	**class-map** コマンドで指定したトラフィックに適用するアクションを指定します。

dhcp-client broadcast-flag

ASA による DHCP クライアント パケットへのブロードキャスト フラグの設定を許可するには、グローバル コンフィギュレーション モードで **dhcp-client broadcast-flag** コマンドを使用します。ブロードキャスト フラグを禁止するには、このコマンドの **no** 形式を使用します。

dhcp-client broadcast-flag

no dhcp-client broadcast-flag

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、ブロードキャスト フラグはディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

ip address dhcp コマンドを使用してインターフェイスの DHCP クライアントをイネーブルにすると、DHCP クライアントが検出を送信して IP アドレスを要求するときに、このコマンドを使用して、DHCP パケット ヘッダーでブロードキャスト フラグを 1 に設定できます。DHCP サーバはこのブロードキャスト フラグをリッスンし、フラグが 1 に設定されている場合は応答パケットをブロードキャストします。

no dhcp-client broadcast-flag コマンドを入力すると、ブロードキャスト フラグは 0 に設定され、DHCP サーバは応答パケットを提供された IP アドレスのクライアントにユニキャストします。

DHCP クライアントは、DHCP サーバからブロードキャスト オファーとユニキャスト オファーの両方を受信できます。

例

次に、ブロードキャスト フラグをイネーブルにする例を示します。

```
ciscoasa(config)# dhcp-client broadcast-flag
```

関連コマンド

コマンド	説明
ip address dhcp	インターフェイスで DHCP クライアントをイネーブルにします。
interface	IP アドレスを設定するために、インターフェイス コンフィギュレーション モードを開始します。
dhcp-client client-id	DHCP 要求パケット オプション 61 を、インターフェイス MAC アドレスが含まれるように設定します。
dhcp-client update dns	DHCP クライアントで DNS 更新をイネーブルにします。

dhcp-client client-id

デフォルトの内部生成された文字列ではなく、オプション 61 の DHCP 要求パケットに MAC アドレスが保存されるよう強制するには、グローバル コンフィギュレーション モードで **dhcp-client client-id** コマンドを使用します。MAC アドレスを禁止するには、このコマンドの **no** 形式を使用します。

dhcp-client client-id interface *interface_name*

no dhcp-client client-id interface *interface_name*

構文の説明

interface *interface_name*	オプション 61 用に MAC アドレスをイネーブルにするインターフェイスを指定します。

デフォルト

デフォルトでは、オプション 61 には内部生成 ASCII ストリングが使用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

ip address dhcp コマンドを使用してインターフェイスの DHCP クライアントをイネーブルにすると、一部の ISP でオプション 61 がインターフェイス MAC アドレスであると見なされます。MAC アドレスが DHCP 要求パケットに含まれていない場合、IP アドレスは割り当てられません。**dhcp-client client-id** コマンドを使用して、オプション 61 用にインターフェイス MAC アドレスを含めます。

例

次に、外部インターフェイスのオプション 61 用に MAC アドレスをイネーブルに例を示します。

```
ciscoasa(config)# dhcp-client client-id interface outside
```

関連コマンド

コマンド	説明
ip address dhcp	インターフェイスで DHCP クライアントをイネーブルにします。
interface	IP アドレスを設定するために、インターフェイス コンフィギュレーション モードを開始します。
dhcp-client broadcast-flag	DHCP クライアント パケットにブロードキャスト フラグを設定します。
dhcp-client update dns	DHCP クライアントで DNS 更新をイネーブルにします。

dhcp client route distance

DHCP を通じて学習したルートにアドミニストレーティブ ディスタンスを設定するには、インターフェイス コンフィギュレーション モードで **dhcp client route distance** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dhcp client route distance *distance*

no dhcp client route distance *distance*

構文の説明

distance	DHCP を通じて学習したルートに適用するアドミニストレーティブ ディスタンス。有効な値は、1 ～ 255 です。

デフォルト

DHCP を通じて学習したルートには、デフォルトでアドミニストレーティブ ディスタンス 1 が指定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

dhcp client route distance コマンドは、ルートが DHCP を通じて学習された場合にのみチェックされます。ルートが DHCP を通じて学習された後に **dhcp client route distance** コマンドが開始されると、指定したアドミニストレーティブ ディスタンスは、学習された既存のルートに影響を与えません。指定したアドミニストレーティブ ディスタンスが設定されるのは、このコマンドの入力後に学習されたルートだけです。

DHCP でルートを取得するには、**ip address dhcp** コマンドで **setroute** オプションを指定する必要があります。

DHCP を複数のインターフェイスで設定している場合、インストールされたルートの優先度を指定するには、各インターフェイスで **dhcp client route distance** コマンドを使用する必要があります。

例

次に、GigabitEthernet0/2 で DHCP によりデフォルト ルートを取得する例を示します。このルートは、トラッキング エントリ オブジェクト 1 によって追跡されます。SLA 動作によって、outside インターフェイスからの 10.1.1.1 ゲートウェイの可用性がモニタされます。SLA 動作が失敗した場合、GigabitEthernet0/3 で DHCP により取得したバックアップ ルートが使用されます。バックアップ ルートには、アドミニストレーティブ ディスタンスに 254 が割り当てられます。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# dhcp client route track 1
ciscoasa(config-if)# ip address dhcp setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# dhcp client route track 1
ciscoasa(config-if)# dhcp client route distance 254
ciscoasa(config-if)# ip address dhcp setroute
```

関連コマンド

コマンド	説明
dhcp client route track	DHCP を通じて学習したルートをトラッキング エントリ オブジェクトに関連付けます。
ip address dhcp	指定したインターフェイスに DHCP で取得した IP アドレスを設定します。
sla monitor	SLA モニタリング動作を定義します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

dhcp client route track

追加ルートをトラッキング済みの指定オブジェクト番号に関連付けるように DHCP クライアントを設定するには、インターフェイス コンフィギュレーション モードで **dhcp client route track** コマンドを使用します。DHCP クライアントのルート トラッキングをディセーブルにするには、このコマンドの **no** 形式を使用します。

dhcp client route track *number*

no dhcp client route track

構文の説明

number	トラッキング エントリのオブジェクト ID。有効な値は、1 ～ 500 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

dhcp client route track コマンドは、ルートが DHCP を通じて学習された場合にのみチェックされます。ルートが DHCP から学習された後で **dhcp client route track** コマンドを入力すると、学習された既存のルートはトラッキング オブジェクトに関連付けられません。次の 2 つのコマンドを正しい順序で入力する必要があります。常に **dhcp client route track** コマンドを最初に入力し、その後に **ip address dhcp setroute** コマンドを入力してください。**ip address dhcp setroute** コマンドをすでに入力している場合は削除して、前述した順序で再入力します。指定したトラッキング オブジェクトに関連付けられるのは、このコマンドの入力後に学習されたルートだけです。

DHCP でルートを取得するには、**ip address dhcp** コマンドで **setroute** オプションを指定する必要があります。

DHCP を複数のインターフェイスで設定している場合、インストールされたルートの優先度を指定するには、各インターフェイスで **dhcp client route distance** コマンドを使用する必要があります。

例

次に、GigabitEthernet0/2 で DHCP によりデフォルト ルートを取得する例を示します。このルートは、トラッキング エントリ オブジェクト 1 によって追跡されます。SLA 動作によって、outside インターフェイスからの 10.1.1.1 ゲートウェイの可用性がモニタされます。SLA 動作が失敗した場合、GigabitEthernet0/3 で DHCP により取得したバックアップ ルートが使用されます。バックアップ ルートには、アドミニストレーティブ ディスタンスに 254 が割り当てられます。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# dhcp client route track 1
ciscoasa(config-if)# ip address dhcp setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# dhcp client route distance 254
ciscoasa(config-if)# ip address dhcp setroute
```

関連コマンド

コマンド	説明
dhcp client route distance	DHCP を通じて学習したルートにアドミニストレーティブ ディスタンスを割り当てます。
ip address dhcp	指定したインターフェイスに DHCP で取得した IP アドレスを設定します。
sla monitor	SLA モニタリング動作を定義します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

dhcp-client update dns

DHCP クライアントが DHCP サーバに渡す更新パラメータを設定するには、グローバル コンフィギュレーション モードで **dhcp-client update dns** コマンドを使用します。DHCP クライアントが DHCP サーバに渡すパラメータを削除するには、このコマンドの **no** 形式を使用します。

dhcp-client update dns [**server** {**both** | **none**}]

no dhcp-client update dns [**server** {**both** | **none**}]

構文の説明

both	DHCP サーバが DNS A および PTR リソース レコードの両方を更新するクライアント要求。
none	DHCP サーバが DDNS 更新を実行しないクライアント要求。
サーバ	DHCP サーバがクライアント要求を受信するように指定します。

デフォルト

デフォルトでは、ASA は、DHCP サーバが PTR RR 更新のみを実行するよう要求します。クライアントはサーバに FQDN オプションを送信しません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドはインターフェイス コンフィギュレーション モードでも入力できますが、ハイフンは使用しません。**dhcp client update dns** コマンドを参照してください。インターフェイス モードで **dhcp client update dns** コマンドを入力すると、グローバル コンフィギュレーション モードのこのコマンドで設定した設定値が上書きされます。

例

次に、DHCP サーバが A および PTR RR を更新しないことを要求するようクライアントを設定する例を示します。

```
ciscoasa(config)# dhcp-client update dns server none
```

次に、サーバが A および PTR RR を更新することを要求するようクライアントを設定する例を示します。

```
ciscoasa(config)# dhcp-client update dns server both
```

関連コマンド

コマンド	説明
ddns	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update	DDNS アップデート方式を ASA のインターフェイスまたは DDNS アップデート ホスト名に関連付けます。
ddns update method	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
dhcpd update dns	DHCP サーバによる DDNS アップデートの実行をイネーブルにします。
interval maximum	DDNS アップデート方式によるアップデート試行の最大間隔を設定します。

dhcp-network-scope

ASA DHCP サーバが、このグループ ポリシーのユーザにアドレスを割り当てるために使用する必要がある IP アドレスの範囲を指定するには、グループ ポリシー コンフィギュレーション モードで **dhcp-network-scope** コマンドを使用します。実行コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

dhcp-network-scope {*ip_address*} | **none**

no dhcp-network-scope

構文の説明

ip_address	このポリシー グループのユーザに IP アドレスを割り当てるため、DHCP サーバが使用する必要がある IP サブネットワークを指定します。
none	DHCP サブネットワークをヌル値に設定して、IP アドレスが許可されないようにします。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、別のグループ ポリシーの値を継承できます。値を継承できないようにするには、**dhcp-network-scope none** コマンドを使用します。

例

次に、First Group という名前のグループ ポリシーに対して、IP サブネットワーク 10.10.85.1 を設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# dhcp-network-scope 10.10.85.1
```

dhcp-server

VPN トンネルの確立時にクライアントに IP アドレスを割り当てる DHCP サーバのサポートを設定するには、トンネル グループ一般属性コンフィギュレーション モードで **dhcp-server** コマンドを使用します。このコマンドをデフォルトに戻すには、このコマンドの **no** 形式を使用します。

dhcp-server [**link-selection** | **subnet-selection**] **ip1** [**ip2-ip10**]

[**no**] **dhcp-server** [**link-selection** | **subnet-selection**] **ip1** [**ip2-ip10**]

構文の説明

ip1	DHCP サーバのアドレス。
ip2-ip10	(オプション)追加の DHCP サーバのアドレス。1 回のコマンドで最大 10 個まで指定できます。また、複数のコマンドにまたがって指定できます。
link-selection	(オプション)ASA が RFC 3527 で規定されている DHCP サブオプション 5「リレー情報オプション 82 のリンク選択のサブオプション」を送信するかどうかを指定します。この設定は、この RFC をサポートしているサーバのみで使用します。
subnet-selection	(オプション)ASA が RFC 3011 で規定されている DHCP オプション 118「IPv4 サブネット選択オプション」を送信するかどうかを指定します。この設定は、この RFC をサポートしているサーバのみで使用します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(5)	**link-selection** および **subnet-selection** キーワードが追加されました。

使用上のガイドライン

この属性は、リモート アクセス トンネル グループ タイプに対してのみ適用できます。

例

次のコマンドを設定一般コンフィギュレーション モードで入力して、3 つの DHCP サーバ（dhcp1、dhcp2、および dhcp3）を IPsec リモート アクセス トンネル グループ「remotegrp」に追加する例を示します。

```
ciscoasa(config)# tunnel-group remotegrp type remote-access
ciscoasa(config)# tunnel-group remotegrp general
ciscoasa(config-tunnel-general)# default-group-policy remotegrp
ciscoasa(config-tunnel-general)# dhcp-server dhcp1 dhcp2 dhcp3
ciscoasa(config-tunnel-general)
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。

dhcpd address コマンド ～ distribute-list out コマンド

dhcpd address

DHCP サーバで使用される IP アドレス プールを定義するには、グローバル コンフィギュレーション モードで **dhcpd address** コマンドを使用します。既存の DHCP アドレス プールを削除するには、このコマンドの **no** 形式を使用します。

dhcpd address *ip_address1*[*-ip_address2*] *interface_name*

no dhcpd address *interface_name*

構文の説明

interface_name	アドレス プールを割り当てるインターフェイス。トランスペアレント モードでは、ブリッジ グループ メンバー インターフェイスを指定します。ルーテッドモードでは、ルーテッドインターフェイスまたは BVI を指定します。ブリッジ グループ メンバー インターフェイスは指定しないでください。
ip_address1	DHCP アドレス プールの開始アドレス。
ip_address2	DHCP アドレス プールの終了アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.7(1)	Integrated Routing and Bridging（IRB; 統合ルーティングおよびブリッジング）を使用するときに、ルーテッド モードで BVI にこのコマンドを設定できるようになりました。

使用上のガイドライン

DHCP サーバの ASA アドレス プールは、そのアドレス プールが有効な ASA インターフェイスと同じサブネット内にある必要があります。また、*interface_name* を使用して関連する ASA インターフェイスを指定する必要があります。

アドレス プールのサイズは、ASA でプールあたり 256 に制限されています。アドレス プールの範囲が 253 アドレスよりも大きい場合、ASA インターフェイスのネットマスクは、クラス C アドレス（たとえば、255.255.255.0）にはできないため、それよりいくらか大きく、たとえば、255.255.254.0 にする必要があります。

DHCP クライアントは、物理的に ASA DHCP サーバ インターフェイスのサブネットに接続されている必要があります。

dhcpd address コマンドでは、「-」（ダッシュ）文字がオブジェクト名の一部ではなく、範囲指定子と解釈されるため、この文字を含むインターフェイス名は使用できません。

no dhcpd address *interface_name* コマンドは、指定されたインターフェイスに設定されている DHCP サーバ アドレス プールを削除します。

ASA に DHCP サーバ機能を実装する方法の詳細については、CLI 設定ガイドを参照してください。

例

次に、ASA の DMZ インターフェイスに DHCP クライアントのアドレス プールおよび DNS サーバを設定する例を示します。

```
ciscoasa(config)# dhcpd address 10.0.1.100-10.0.1.108 dmz
ciscoasa(config)# dhcpd dns 209.165.200.226
ciscoasa(config)# dhcpd enable dmz
```

次に、内部インターフェイスに DHCP サーバを設定する例を示します。**dhcpd address** コマンドは、そのインターフェイスで DHCP サーバに 10 個の IP アドレスのプールを割り当てます。

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
dhcpd enable	指定したインターフェイスで、DHCP サーバをイネーブルにします。
show dhcpd	DHCP のバインディング情報、統計情報、または状態情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd auto_config

DHCP または PPPoE クライアントを実行しているインターフェイスから取得した値、または VPN サーバから取得した値に基づいて、ASA で DHCP サーバに対して DNS、WINS およびドメイン名の値を自動的に設定できるようにするには、グローバル コンフィギュレーション モードで **dhcpd auto_config** コマンドを使用します。DHCP パラメータの自動設定を解除するには、このコマンドの **no** 形式を使用します。

dhcpd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]

no dhcpd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]

構文の説明

client_if_name	DNS、WINS、およびドメイン名パラメータを提供する DHCP クライアントを実行している、インターフェイスを指定します。
interface *if_name*	アクションが適用されるインターフェイスを指定します。
vpnclient-wins-override	vpnclient パラメータにより、インターフェイス DHCP または PPPoE クライアントの WINS パラメータを上書きします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

CLI コマンドを使用して DNS、WINS、またはドメイン名パラメータを指定した場合、自動設定によって取得されたパラメータは、CLI により設定されたパラメータで上書きされます。

例

次に、内部インターフェイスに DHCP を設定する例を示します。外部インターフェイス上の DHCP クライアントから取得した DNS、WINS、およびドメイン情報を、内部インターフェイス上の DHCP クライアントに渡すには、**dhcpd auto_config** コマンドを使用します。

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd auto_config outside
ciscoasa(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
dhcpd enable	指定したインターフェイスで、DHCP サーバをイネーブルにします。
show ip address dhcp server	DHCP クライアントとして動作するインターフェイスに DHCP サーバから提供される、DHCP オプションに関する詳細情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd dns

DHCP クライアントに対して DNS サーバを定義するには、グローバル コンフィギュレーション モードで **dhcpd dns** コマンドを使用します。定義されたサーバをクリアするには、このコマンドの **no** 形式を使用します。

dhcpd dns *dnsip1* [*dnsip2*] [**interface** *if_name*]

no dhcpd dns *dnsip1* [*dnsip2*] [**interface** *if_name*]

構文の説明

dnsip1	DHCP クライアントに対するプライマリ DNS サーバの IP アドレスを指定します。
dnsip2	（オプション）DHCP クライアントに対する代替 DNS サーバの IP アドレスを指定します。
interface *if_name*	サーバに入力した値を適用するインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

dhcpd dns コマンドは、DHCP クライアントに対する DNS サーバの IP アドレスを 1 つまたは複数指定します。2 つの DNS サーバを指定できます。**no dhcpd dns** コマンドは、コンフィギュレーションから DNS IP アドレスを削除します。

例

次に、ASA の DMZ インターフェイスに DHCP クライアントのアドレス プールおよび DNS サーバを設定する例を示します。

```
ciscoasa(config)# dhcpd address 10.0.1.100-10.0.1.108 dmz
ciscoasa(config)# dhcpd dns 192.168.1.2
ciscoasa(config)# dhcpd enable dmz
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
dhcpd address	指定したインターフェイスの DHCP サーバが使用するアドレス プールを指定します。
dhcpd enable	指定したインターフェイスで、DHCP サーバをイネーブルにします。
dhcpd wins	DHCP クライアントに対して WINS サーバを定義します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd domain

DHCP クライアントに対して DNS ドメイン名を定義するには、グローバル コンフィギュレーション モードで **dhcpd dns** コマンドを使用します。DNS ドメイン名をクリアするには、このコマンドの **no** 形式を使用します。

dhcpd domain *domain_name* [**interface** *if_name*]

no dhcpd domain [*domain_name*] [**interface** *if_name*]

構文の説明

domain_name	DNS ドメイン名（example.com）を指定します。
interface *if_name*	サーバに入力した値を適用するインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

dhcpd domain コマンドは、DHCP クライアントに対する DNS ドメイン名を指定します。**no dhcpd domain** コマンドは、コンフィギュレーションから DNS ドメイン サーバを削除します。

例

次に、ASA で DHCP サーバによって DHCP クライアントに提供されるドメイン名を設定する例を示します。

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd enable

DHCP サーバをイネーブルにするには、グローバル コンフィギュレーション モードで **dhcpd enable** コマンドを使用します。DHCP サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

dhcpd enable *interface*

no dhcpd enable *interface*

構文の説明

interface	DHCP サーバをイネーブルにするインターフェイスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

DHCP サーバは、DHCP クライアントにネットワーク コンフィギュレーション パラメータを提供します。ASA 内で DHCP サーバをサポートすることにより、ASA は DHCP を使用して接続されるクライアントを設定できるようになります。**dhcpd enable** *interface* コマンドを使用すると、DHCP デーモンによる、DHCP 対応のインターフェイス上での DHCP クライアントの要求のリッスンをイネーブルにできます。**no dhcpd enable** コマンドは、指定したインターフェイス上の DHCP サーバ機能をディセーブルにします。

(注) マルチ コンテキスト モードの場合は、複数のコンテキストにより使用されているインターフェイス（共有 VLAN）で DHCP サーバをイネーブルにすることはできません。

ASA が DHCP クライアント要求に応答する場合、要求を受信したインターフェイスの IP アドレスとサブネット マスクを、デフォルト ゲートウェイの IP アドレスとサブネット マスクとして応答で使用します。

（注） ASA DHCP サーバ デーモンは、直接 ASA インターフェイスに接続されていないクライアントはサポートしません。

ASA に DHCP サーバ機能を実装する方法の詳細については、CLI 設定ガイドを参照してください。

例

次に、inside インターフェイスで DHCP サーバをイネーブルにする例を示します。

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
debug dhcpd	DHCP サーバのデバッグ情報を表示します。
dhcpd address	指定したインターフェイスの DHCP サーバが使用するアドレス プールを指定します。
show dhcpd	DHCP のバインディング情報、統計情報、または状態情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd lease

DHCP リース期間を指定するには、グローバル コンフィギュレーション モードで **dhcpd lease** コマンドを使用します。リースのデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

dhcpd lease *lease_length* [**interface** *if_name*]

no dhcpd lease [*lease_length*] [**interface** *if_name*]

構文の説明

interface *if_name*	サーバに入力した値を適用するインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。
lease_length	DHCP サーバから DHCP クライアントに付与される IP アドレス リース期間を秒単位で指定します。有効な値は 300 ～ 1048575 秒です。

デフォルト

lease_length のデフォルト値は 3600 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

dhcpd lease コマンドは、DHCP クライアントに与えるリース期間を秒単位で指定します。このリース期間は、DHCP サーバが割り当てた IP アドレスを DHCP クライアントが使用できる期間を示します。

no dhcpd lease コマンドは、コンフィギュレーションから指定したリース期間を削除して、この値をデフォルト値の 3600 秒に置き換えます。

例

次に、DHCP クライアントに対する DHCP 情報のリース期間を指定する例を示します。

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
```

```
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd option

DHCP オプションを設定するには、グローバル コンフィギュレーション モードで **dhcpd option** コマンドを使用します。オプションをクリアするには、このコマンドの **no** 形式を使用します。

dhcpd option *code* {**ascii** *string*} | {**ip** *IP_address* [*IP_address*]} | {**hex** *hex_string*} [**interface** *if_name*]

no dhcpd option *code* [**interface** *if_name*]

構文の説明

ascii *string*	オプション パラメータがスペースなしの ASCII 文字列であることを指定します。
code	設定する DHCP オプションを表す数字を指定します。有効な値は、0 ～ 255 であり、いくつかの例外があります。サポートされていない DHCP オプション コードのリストについては、「使用上のガイドライン」の項を参照してください。
hex *hex_string*	オプション パラメータが 16 進数の文字列（偶数個の桁数を含み、スペースを含まない）ではないことを指定します。0x プレフィックスを使用する必要はありません。
interface *if_name*	サーバに入力した値を適用するインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。
ip	オプション パラメータが IP アドレスであることを指定します。最大 2 つの IP アドレスを **ip** キーワードに指定できます。
IP_address	ドット付き 10 進表記の IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

dhcpd option コマンドを使用して、TFTP サーバ情報を Cisco IP Phone およびルータに提供することができます。

DHCP オプション要求が ASA DHCP サーバに到着すると、ASA は **dhcpd option** コマンドで指定された値を、クライアントに対する応答に入れます。

dhcpd option 66 コマンドおよび **dhcpd option 150** コマンドは、Cisco IP Phone およびルータがコンフィギュレーション ファイルをダウンロードするときに使用する TFTP サーバを指定します。これらのコマンドは、次のように使用します。

- **dhcpd option 66 ascii** *string*。ここで、*string* は TFTP サーバの IP アドレスまたはホスト名です。オプション 66 には、TFTP サーバを 1 つだけ指定できます。
- **dhcpd option 150 ip** *IP_address* [*IP_address*]。ここで、*IP_address* は TFTP サーバの IP アドレスです。オプション 150 には、最大 2 つの IP アドレスを指定できます。

(注) **dhcpd option 66** コマンドは **ascii** パラメータのみ受け付け、**dhcpd option 150** コマンドは **ip** パラメータのみ受け付けます。

dhcpd option 66 | 150 コマンドに IP アドレスを指定するときには、次のガイドラインに従ってください。

- TFTP サーバが DHCP サーバ インターフェイス上にある場合、TFTP サーバのローカル IP アドレスを使用します。
- TFTP サーバが DHCP サーバ インターフェイスよりもセキュリティが低いインターフェイス上にある場合は、一般の発信ルールが適用されます。DHCP クライアント用の NAT エントリ、グローバル エントリ、およびアクセス リスト エントリを作成し、TFTP サーバの実際の IP アドレスを使用します。
- TFTP サーバがよりセキュリティの高いインターフェイス上にある場合は、一般の着信ルールが適用されます。TFTP サーバ用のスタティック ステートメントとアクセス リスト ステートメントのグループを作成し、TFTP サーバのグローバル IP アドレスを使用します。

その他の DHCP オプションの詳細については、RFC 2132 を参照してください。

(注) ASA は、指定されたオプションのタイプおよび値が、RFC 2132 に定義されているオプション コードに対して期待されているタイプおよび値と一致するかどうかは確認しません。たとえば、**dhcpd option 46 ascii hello** コマンドを入力できます。RFC 2132 では、オプション 46 は 1 桁の 16 進数値として定義されていますが、ASA はこのコンフィギュレーションを受け入れます。

dhcpd option コマンドで次の DHCP オプションは設定できません。

オプション コード	説明
0	DHCPOPT_PAD
1	HCPOPT_SUBNET_MASK
12	DHCPOPT_HOST_NAME
50	DHCPOPT_REQUESTED_ADDRESS
51	DHCPOPT_LEASE_TIME
52	DHCPOPT_OPTION_OVERLOAD

オプション コード	説明
53	DHCPOPT_MESSAGE_TYPE
54	DHCPOPT_SERVER_IDENTIFIER
58	DHCPOPT_RENEWAL_TIME
59	DHCPOPT_REBINDING_TIME
61	DHCPOPT_CLIENT_IDENTIFIER
67	DHCPOPT_BOOT_FILE_NAME
82	DHCPOPT_RELAY_INFORMATION
255	DHCPOPT_END

例

次に、DHCP オプション 66 に TFTP サーバを指定する例を示します。

```
ciscoasa(config)# dhcpd option 66 ascii MyTftpServer
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd ping_timeout

DHCP ping のデフォルト タイムアウトを変更するには、グローバル コンフィギュレーション モードで **dhcpd ping_timeout** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

dhcpd ping_timeout *number* [**interface** *if_name*]

no dhcpd ping_timeout [**interface** *if_name*]

構文の説明

interface *if_name*	サーバに入力した値を適用するインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。
number	ミリ秒単位の ping タイムアウト値。最小値は 10、最大値は 10000 です。デフォルトは 50 です。

デフォルト

number のデフォルトのミリ秒は 50 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

アドレスの競合を避けるため、DHCP サーバは、アドレスを DHCP クライアントに割り当てる前に 2 つの ICMP ping パケットをアドレスに送信します。ASA は、DHCP クライアントに IP アドレスを割り当てる前に、両方の ICMP ping パケットがタイムアウトになるのを待ちます。たとえば、デフォルト値が使用された場合、ASA は IP アドレスを割り当てる前に、1500 ミリ秒（各 ICMP ping パケットに対して 750 ミリ秒）待ちます。

ping のタイムアウト値が長いと、DHCP サーバのパフォーマンスに悪影響を及ぼす場合があります。

例

次に、**dhcpd ping_timeout** コマンドを使用して、DHCP サーバの ping タイムアウト値を変更する例を示します。

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd reserve-address

インターフェイスの DHCP アドレスを予約するには、グローバル コンフィギュレーション モードで **dhcpd reserved-address** コマンドを使用します。既存の DHCP アドレス予約を削除するには、このコマンドの **no** 形式を使用します。

dhcpd reserve-address *ip_address mac_address if_name*

no dhcpd reserve_address *ip_address mac_address if_name*

構文の説明

ip_address	クライアントの MAC アドレスに基づいて DHCP クライアントに割り当てられたアドレスプールの IP アドレス。
mac_address	クライアントの MAC アドレス。
if_name	IP アドレスを予約するインターフェイス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.13(1)	このコマンドが追加されました。

使用上のガイドライン

予約済みアドレスは設定済みのアドレスプールから取得する必要があり、アドレスプールは ASA インターフェイスと同じサブネット上にある必要があります。トランスペアレントモードでは、ブリッジ グループ メンバー インターフェイスを指定します。ルーテッドモードでは、ルーテッドインターフェイスまたは BVI を指定します。ブリッジ グループ メンバー インターフェイスは指定しないでください。

例

次の例では、**dhcpd reserve-address** コマンドを使用して、クライアントの MAC アドレスに基づきアドレスプールからクライアントに特定のアドレスを割り当てる方法について示します。

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd enable inside
ciscoasa(config)# dhcpd reserve-address 10.0.1.109 030c.f142.4cde inside
```

関連コマンド

コマンド	説明
dhcpd address	指定したインターフェイスの DHCP サーバが使用するアドレス プールを指定します。
dhcpd enable	指定したインターフェイスで、DHCP サーバをイネーブルにします。
show dhcpd	DHCP のバインディング情報、統計情報、または状態情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd update dns

DHCP サーバによる DDNS アップデートの実行をイネーブルにするには、グローバル コンフィギュレーション モードで **dhcpd update dns** コマンドを使用します。DHCP サーバによる DDNS をディセーブルにするには、このコマンドの **no** 形式を使用します。

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

no dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

構文の説明

both	DHCP サーバが A と PTR の両方の DNS RR を更新するように指定します。
interface	DDNS 更新が適用される ASA インターフェイスを指定します。
override	DHCP サーバが DHCP クライアント要求を上書きするように指定します。
srv_ifc_name	このオプションを適用するインターフェイスを指定します。

デフォルト

デフォルトでは、DHCP サーバは PTR RR 更新のみを実行します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

DDNS は、DNS で保持されている名前/アドレスおよびアドレス/名前のマッピングを更新します。更新は DHCP サーバと連携して実行されます。**dhcpd update dns** コマンドはサーバによる更新をイネーブルにします。

名前とアドレスのマッピングは、次の 2 タイプの RR に保持されます。

- A リソース レコードには、ドメイン名から IP アドレスへのマッピングが含まれます。
- PTR リソース レコードには、IP アドレスからドメイン名へのマッピングが含まれます。

DDNS アップデートを使用して、A RR タイプと PTR RR タイプとの間で一貫した情報を保持できます。

dhcpd update dns コマンドを使用すると、DHCP サーバが A RR と PRT RR の両方の更新、または PTR RR 更新のみを実行するように設定できます。DHCP クライアントからの更新要求を上書きするように設定することもできます。

例

次に、DDNS サーバが DHCP クライアントからの要求を上書きし、A と PTR の両方のアップデートを実行するよう設定する例を示します。

```
ciscoasa(config)# dhcpd update dns both override
```

関連コマンド

コマンド	説明
ddns	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update	DDNS アップデート方式を ASA インターフェイスまたは DDNS アップデート ホスト名に関連付けます。
ddns update method	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
dhcp-client update dns	DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。
interval maximum	DDNS アップデート方式によるアップデート試行の最大間隔を設定します。

dhcpd wins

DHCP クライアントに対して WINS サーバ IP アドレスを定義するには、グローバル コンフィギュレーション モードで **dhcpd wins** コマンドを使用します。コンフィギュレーションから WINS サーバ IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

dhcpd wins *server1* [*server2*] [**interface** *if_name*]

no dhcpd wins [*server1* [*server2*]] [**interface** *if_name*]

構文の説明

interface *if_name*	サーバに入力した値を適用するインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。
server1	プライマリの Microsoft NetBIOS ネーム サーバ（WINS サーバ）の IP アドレスを指定します。
server2	（任意）代替の Microsoft NetBIOS ネーム サーバ（WINS サーバ）の IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

dhcpd wins コマンドは、DHCP クライアント用の WINS サーバのアドレスを指定します。**no dhcpd wins** コマンドは、コンフィギュレーションから WINS サーバの IP アドレスを削除します。

例

次に、DHCP クライアントに送信される WINS サーバ情報を指定する例を示します。

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
ciscoasa(config)# dhcpd dns 198.162.1.2 198.162.1.3
ciscoasa(config)# dhcpd wins 198.162.1.4
ciscoasa(config)# dhcpd lease 3000
```

```
ciscoasa(config)# dhcpd ping_timeout 1000
ciscoasa(config)# dhcpd domain example.com
ciscoasa(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	すべての DHCP サーバ設定を削除します。
dhcpd address	指定したインターフェイスの DHCP サーバが使用するアドレス プールを指定します。
dhcpd dns	DHCP クライアントに対して DNS サーバを定義します。
show dhcpd	DHCP のバインディング情報、統計情報、または状態情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcprelay enable

DHCP リレー エージェントをイネーブルにするには、グローバル コンフィギュレーション モードで **dhcprelay enable** コマンドを使用します。DHCP リレー エージェントをディセーブルにするには、このコマンドの **no** 形式を使用します。

dhcprelay enable *interface_name*

no dhcprelay enable *interface_name*

構文の説明

interface_name	DHCP リレー エージェントがクライアント要求を受け入れるインターフェイスの名前。

デフォルト

DHCP リレー エージェントはディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

DHCP リレー エージェントでは、指定した ASA インターフェイスから指定した DHCP サーバに DHCP 要求を転送できます。

ASA が **dhcprelay enable** *interface_name* コマンドを使用して DHCP リレー エージェントを開始するには、**dhcprelay server** コマンドがコンフィギュレーションにすでに存在している必要があります。このコマンドがない場合、ASA は次に示すようなエラー メッセージを表示します。

```
DHCPRA: Warning - There are no DHCP servers configured!
        No relaying can be done without a server!
        Use the 'dhcprelay server <server_ip> <server_interface>' command
```

次の条件下では、DHCP リレーをイネーブルにできません。

- 同じインターフェイス上で DHCP リレーと DHCP リレー サーバをイネーブルにすることはできません。
- 同じインターフェイス上で DHCP リレーと DHCP サーバ（**dhcpd enable**）をイネーブルにすることはできません。

- DHCP サーバもイネーブルになっている場合、DHCP リレー エージェントをイネーブルにできません。
- マルチ コンテキスト モードの場合、複数のコンテキストにより使用されているインターフェイス（共有 VLAN）で DHCP リレーをイネーブルにすることはできません。

no dhcprelay enable *interface_name* コマンドは、*interface_name* 引数で指定されたインターフェイスの DHCP リレー エージェント コンフィギュレーションだけを削除します。

例

次に、IP アドレス 10.1.1.1 が設定されている DHCP サーバに対する DHCP リレー エージェントを ASA の外部インターフェイスに設定し、クライアント要求を ASA の内部インターフェイスに設定して、タイムアウト値を 90 秒に設定する例を示します。

```
ciscoasa(config)# dhcprelay server 10.1.1.1 outside
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

次に、DHCP リレー エージェントをディセーブルにする例を示します。

```
ciscoasa(config)# no dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay timeout 90
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
debug dhcp relay	DHCP リレー エージェントのデバッグ情報を表示します。
dhcprelay server	DHCP リレー エージェントが DHCP 要求を転送する DHCP サーバを指定します。
dhcprelay setroute	DHCP リレー エージェントが DHCP 応答でデフォルト ルータ アドレスとして使用する IP アドレスを定義します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

dhcprelay information trust-all

指定されたインターフェイスを信頼できるインターフェイスとして設定するには、グローバル コンフィギュレーション モードで **dhcprelay information trust-all** コマンドを使用します。

dhcprelay information trust-all

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.1(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、特定のインターフェイスを信頼できるインターフェイスとして設定します。インターフェイス固有の信頼できるコンフィギュレーションを表示するには、インターフェイス コンフィギュレーション モードで **show running-config dhcprelay interface** コマンドを使用します。インターフェイス コンフィギュレーション モードで特定のインターフェイスを信頼できるインターフェイスとして設定するには、**dhcprelay information trusted** コマンドを使用します。グローバル コンフィギュレーション モードで特定のインターフェイスを信頼できるインターフェイスとして設定するには、**show running-config dhcprelay** コマンドを使用します。

例

次に、グローバル コンフィギュレーション モードで指定のインターフェイスを信頼できるインターフェイスとして設定する例を示します。

```
ciscoasa(config-if)# interface vlan501
ciscoasa(config-if)# nameif inside
ciscoasa(config)# dhcprelay information trust-all
ciscoasa(config)# show running-config dhcprelay
dhcprelay information trust-all
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
dhcprelay enable	指定したインターフェイスで、DHCP リレー エージェントをイネーブルにします。
dhcprelay setroute	DHCP リレー エージェントが DHCP 応答でデフォルト ルータ アドレスとして使用する IP アドレスを定義します。
dhcprelay timeout	DHCP リレー エージェントのタイムアウト値を指定します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

dhcprelay information trusted

指定されたインターフェイスを信頼できるインターフェイスとして設定するには、インターフェイス コンフィギュレーション モードで **dhcprelay information trusted** コマンドを使用します。

dhcprelay information trusted

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.1(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、特定のインターフェイスを信頼できるインターフェイスとして設定します。インターフェイス固有の信頼できるコンフィギュレーションを表示するには、インターフェイス コンフィギュレーション モードで **show running-config dhcprelay interface** コマンドを使用します。グローバル コンフィギュレーション モードで特定のインターフェイスを信頼できるインターフェイスとして設定するには、**dhcprelay information trust-all** コマンドを使用します。グローバル コンフィギュレーション モードで特定のインターフェイスを信頼できるインターフェイスとして設定するには、**show running-config dhcprelay** コマンドを使用します。

例

次に、指定されたインターフェイスを信頼できるインターフェイスとして設定する例を示します。

```
ciscoasa(config-if)# interface gigabitEthernet 0/0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# dhcprelay information trusted
ciscoasa(config)# show running-config dhcprelay
interface gigabitEthernet 0/0
nameif inside
dhcprelay information trusted
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
dhcprelay enable	指定したインターフェイスで、DHCP リレー エージェントをイネーブルにします。
dhcprelay setroute	DHCP リレー エージェントが DHCP 応答でデフォルト ルータ アドレスとして使用する IP アドレスを定義します。
dhcprelay timeout	DHCP リレー エージェントのタイムアウト値を指定します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

dhcprelay server（グローバル）

DHCP 要求の転送先の DHCP サーバを指定するには、グローバル コンフィギュレーション モードで **dhcpreplay server** コマンドを使用します。DHCP サーバを DHCP リレー コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

dhcprelay server [*interface_name*]

no dhcprelay server [*interface_name*]

構文の説明

interface_name	DHCP サーバが常駐する ASA インターフェイスの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

DHCP リレー エージェントでは、指定した ASA インターフェイスから指定した DHCP サーバに DHCP 要求を転送できます。インターフェイスあたり最大 10 個の DHCP リレー サーバを追加できます。**dhcprelay enable** コマンドを入力する前に、少なくとも 1 つの **dhcprelay server** コマンドを ASA コンフィギュレーションに追加する必要があります。DHCP リレー サーバが設定されているインターフェイス上には、DHCP クライアントを設定できません。

dhcprelay server コマンドは、指定したインターフェイス上で UDP ポート 67 を開き、**dhcprelay enable** コマンドがコンフィギュレーションに追加されるとすぐに DHCP リレー タスクを開始します。

例

次に、IP アドレス 10.1.1.1 が設定されている DHCP サーバに対する DHCP リレー エージェントを ASA の outside インターフェイスに設定し、クライアント要求を ASA の inside インターフェイスに設定して、タイムアウト値を 90 秒に設定する例を示します。

```
ciscoasa(config)# dhcprelay server 10.1.1.1 outside
ciscoasa(config)# dhcprelay timeout 90
```

```
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
dhcprelay enable	指定したインターフェイスで、DHCP リレー エージェントをイネーブルにします。
dhcprelay setroute	DHCP リレー エージェントが DHCP 応答でデフォルト ルータ アドレスとして使用する IP アドレスを定義します。
dhcprelay timeout	DHCP リレー エージェントのタイムアウト値を指定します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

dhcprelay server（インターフェイス）

DHCP 要求の転送先の DHCP リレー インターフェイス サーバを指定するには、インターフェイス コンフィギュレーション モードで **dhcpreplay server** コマンドを使用します。DHCP リレー インターフェイス サーバを DHCP リレー コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

dhcprelay server *ip_address*

no dhcprelay server *ip_address*

構文の説明

ip_address	DHCP リレー エージェントがクライアント DHCP 要求を転送する DHCP リレー インターフェイス サーバの IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.1(2)	このコマンドが追加されました。

使用上のガイドライン

DHCP リレー エージェントでは、指定した ASA インターフェイスから指定した DHCP サーバに DHCP 要求を転送できます。インターフェイスあたり最大 4 つの DHCP リレー サーバを追加できます。**dhcprelay enable** コマンドを入力する前に、少なくとも 1 つの **dhcprelay server** コマンドを ASA コンフィギュレーションに追加する必要があります。DHCP リレー サーバが設定されているインターフェイス上には、DHCP クライアントを設定できません。

dhcprelay server コマンドは、指定したインターフェイス上で UDP ポート 67 を開き、**dhcprelay enable** コマンドがコンフィギュレーションに追加されるとすぐに DHCP リレー タスクを開始します。

インターフェイス コンフィギュレーション モードでは、**dhcprelay server** *ip_address* コマンドを使用して、インターフェイスごとに DHCP リレー サーバ（ヘルパーと呼ばれる）アドレスを設定できます。これは、インターフェイスで DHCP 要求を受信し、ヘルパー アドレスが設定されている場合、その要求はそれらのサーバにのみ転送されることを意味します。

no dhcprelay server *ip_address* コマンドを使用すると、インターフェイスはそのサーバへの DHCP パケットの転送を停止し、*ip_address* 引数で指定されている DHCP サーバの DHCP リレー エージェント コンフィギュレーションを削除します。

このコマンドは、グローバル コンフィギュレーション モードで設定された DHCP リレー サーバより優先されます。つまり、DHCP リレー エージェントは、クライアント検出メッセージを最初に DHCP リレー インターフェイス サーバに、次に DHCP グローバル リレー サーバに転送します。

例

次に、IP アドレス 10.1.1.1 が設定されている DHCP リレー インターフェイス サーバに対する DHCP リレー エージェントを ASA の outside インターフェイスに設定し、クライアント要求を ASA の inside インターフェイスに設定して、タイムアウト値を 90 秒に設定する例を示します。

```
ciscoasa(config)# interface vlan 10
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# dhcprelay server 10.1.1.1
ciscoasa(config-if)# exit
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay enable inside
dhcprelay timeout 90

interface vlan 10
nameif inside
dhcprelay server 10.1.1.1
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
dhcprelay enable	指定したインターフェイスで、DHCP リレー エージェントをイネーブルにします。
dhcprelay setroute	DHCP リレー エージェントが DHCP 応答でデフォルト ルータ アドレスとして使用する IP アドレスを定義します。
dhcprelay timeout	DHCP リレー エージェントのタイムアウト値を指定します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

dhcprelay server (vti tunnel)

VTI トンネルインターフェイスを介して DHCP リレーサーバに到達するには、グローバル コンフィギュレーション モードで **dhcpreplay server** コマンドを使用します。

dhcprelay server *ip_address vti-ifc-name*

構文の説明

ip_address	クライアント DHCP 要求を転送する DHCP リレーサーバの IP アドレスを指定します。
vti-ifc-name	DHCP リレーエージェントが DHCP サーバに DHCP パケットを転送する VTI インターフェイスの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.14(1)	このコマンドが追加されました。

使用上のガイドライン

DHCP リレー エージェントでは、指定した ASA インターフェイスから指定した DHCP サーバに DHCP 要求を転送できます。ただし、リレーエージェントは物理インターフェイスでのみ設定できます。VTI インターフェイスは論理インターフェイスであったため、DHCP リレー要求を転送できませんでした。

ASA 9.14(1) 以降は、このコマンドを使用して、DHCP リレーサーバが VTI トンネルインターフェイスを介してパケットを転送できます。

例

次の例では、DHCP リレーエージェントを VTI トンネルで設定する方法について示します。まず、次のように VTI トンネルを作成します。

```
ciscoasa(config)# interface Tunnel100
ciscoasa(config-if)# nameif vti
ciscoasa(config-if)# ip address 10.1.1.10 255.255.255.0
ciscoasa(config-if)# tunnel source interface outside
ciscoasa(config-if)# tunnel destination 192.168.2.111
```

```
ciscoasa(config-if)# tunnel mode ipsec ipv4
ciscoasa(config-if)# tunnel protection ipsec profile PROFILE1
```

ここで、トンネル名を使用して DHCP リレーサーバを設定します。

```
ciscoasa(config)# dhcprelay server 192.168.3.112 vti
```

dhcprelay setroute

DHCP 応答にデフォルト ゲートウェイ アドレスを設定するには、グローバル コンフィギュレーション モードで **dhcprelay setroute** コマンドを使用します。デフォルト ルータを削除するには、このコマンドの **no** 形式を使用します。

dhcprelay setroute *interface*

no dhcprelay setroute *interface*

構文の説明

interface	最初のデフォルト IP アドレス（DHCP サーバから送信されるパケット内にある）を *interface* のアドレスに変更するように DHCP リレー エージェントを設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、DHCP 応答のデフォルト IP アドレスは、指定された ASA インターフェイスのアドレスに置き換えられます。**dhcprelay setroute** *interface* コマンドを使用すると、DHCP リレー エージェントが最初のデフォルト ルータ アドレス（DHCP サーバから送信されるパケット内にある）を *interface* のアドレスに変更するように設定できます。

パケット内にデフォルトのルータ オプションがない場合、ASA は *interface* アドレスを含むデフォルト ルータを追加します。その結果、クライアントは自分のデフォルト ルートが ASA に向かうように設定できます。

dhcprelay setroute *interface* コマンドを設定しない場合（かつパケット内にデフォルトのルータ オプションがある場合）、パケットは、ルータ アドレスが変更されないまま ASA を通過します。

例

次に、DHCP 応答のデフォルト ゲートウェイを外部 DHCP サーバから ASA の inside インターフェイスに設定する例を示します。

```
ciscoasa(config)# dhcprelay server 10.1.1.1 outside
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay setroute inside
ciscoasa(config)# dhcprelay enable inside
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
dhcprelay enable	指定したインターフェイスで、DHCP リレー エージェントをイネーブルにします。
dhcprelay server	DHCP リレー エージェントが DHCP 要求の転送先にする DHCP サーバを指定します。
dhcprelay timeout	DHCP リレー エージェントのタイムアウト値を指定します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

dhcprelay timeout

DHCP リレー エージェントのタイムアウト値を設定するには、グローバル コンフィギュレーション モードで **dhcprelay timeout** コマンドを使用します。タイムアウト値をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

dhcprelay timeout *seconds*

no dhcprelay timeout

構文の説明

seconds	DHCP リレー アドレス ネゴシエーション用に許可されている時間（秒）を指定します。

デフォルト

DHCP リレー タイムアウトのデフォルト値は 60 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

dhcprelay timeout コマンドは、DHCP サーバからの応答がリレー バインディング構造を通して DHCP クライアントに進むことが許されている時間を秒単位で設定します。

例

次に、IP アドレス 10.1.1.1 が設定されている DHCP サーバに対する DHCP リレー エージェントを ASA の外部インターフェイスに設定し、クライアント要求を ASA の内部インターフェイスに設定して、タイムアウト値を 90 秒に設定する例を示します。

```
ciscoasa(config)# dhcprelay server 10.1.1.1 outside
ciscoasa(config)# dhcprelay timeout 90
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
dhcprelay enable	指定したインターフェイスで、DHCP リレー エージェントをイネーブルにします。
dhcprelay server	DHCP リレー エージェントが DHCP 要求を転送する DHCP サーバを指定します。
dhcprelay setroute	DHCP リレー エージェントが DHCP 応答でデフォルト ルータ アドレスとして使用する IP アドレスを定義します。
show running-config dhcprelay	DHCP リレー エージェントの現在のコンフィギュレーションを表示します。

dialog

WebVPN ユーザに表示されるダイアログボックス メッセージをカスタマイズするには、webvpn カスタマイゼーション コンフィギュレーション モードで **dialog** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

dialog {**title** | **message** | **border**} **style** *value*

no dialog {**title** | **message** | **border**} **style** *value*

構文の説明

border	境界線への変更を指定します。
message	メッセージへの変更を指定します。
style	スタイルへの変更を指定します。
title	タイトルへの変更を指定します。
value	表示する実際のテキストまたは CSS パラメータ（最大 256 文字）。

デフォルト

デフォルトのタイトルのスタイルは background-color:#669999;color:white です。

デフォルトのメッセージのスタイルは background-color:#99CCCC;color:black です。

デフォルトの境界線のスタイルは border:1px solid black;border-collapse:collapse です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn カスタマイゼーション コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

style オプションは、任意の有効な CSS パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進数値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目は青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、ダイアログボックス メッセージの文字表示色を青色に変更するようにカスタマイズする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# dialog message style color:blue
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの [Application Access] ボックスをカスタマイズします。
browse-networks	WebVPN ホームページの [Browse Networks] ボックスをカスタマイズします。
web-bookmarks	WebVPN ホームページの [Web Bookmarks] タイトルまたはリンクをカスタマイズします。
file-bookmarks	WebVPN ホームページの [File Bookmarks] タイトルまたはリンクをカスタマイズします。

diameter

カスタム Diameter 属性値ペア（AVP）を Diameter インスペクション クラスまたはポリシー マップに使用するために作成するには、**diameter** コマンドを使用します。既存のカスタム AVP を削除するには、このコマンドの **no** 形式を使用します。

diameter avp *name* **code** *value* **data-type** *type* [**vendor-id** *id_number*] [**description** *text*]

no diameter avp *name* **code** *value* **data-type** *type* [**vendor-id** *id_number*] [**description** *text*]

構文の説明

name	作成するカスタム AVP の名前（最大 32 文字）。Diameter インスペクション ポリシー マップまたはクラス マップでの **match avp** コマンドでこの名前を参照します。
code *value*	256-4294967295 からのカスタム AVP コード値。システムで定義済みのコードとベンダー ID の組み合わせを入力することはできません。
data-type *type*	AVP のデータ型。次のいずれかの型で AVP を定義できます。新しい AVP が別の型の場合は、その型のカスタム AVP は作成できません。 – **address**：IP アドレスの場合。 – **diameter-identity**：Diameter ID データ。 – **diameter-uri**：Diameter の Uniform Resource Identifier（URI）。 – **float32**：32 ビット浮動小数点。 – **float64**：64 ビット浮動小数点。 – **int32**：32 ビット整数。 – **int64**：64 ビット整数。 – **octetstring**：オクテット文字列。 – **time**：時刻値。 – **uint32**：32 ビット符号なし整数。 – **uint64**：64 ビット符号なし整数。
vendor-id *id_number*	（任意）AVP を定義したベンダーの 0 ～ 4294967295 の ID 番号。たとえば、3GPP ベンダー ID は 10415、IETF は 0。
description *text*	（任意）AVP の説明（最大 80 文字）。スペースを含める場合は、説明を引用符で囲みます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

新しい属性値ペア（AVP）が定義され、登録されると、カスタム Diameter AVP を作成して、Diameter インスペクション ポリシー マップにそれらを定義し、使用することができます。RFC または AVP を定義するその他のソースから AVP の作成に必要な情報を取得します。

カスタム AVP は、AVP 照合用の Diameter インスペクション ポリシー マップまたはクラス マップで使用する場合にのみ、作成します。

例

次に、カスタム AVP の作成方法と、Diameter インスペクション ポリシー マップでの使用方法の例を示します。

```
ciscoasa(config)# diameter avp eg_custom_avp code 9999 data-type int32
ciscoasa(config)# policy-map type inspect diameter avp-filter-pmap
asa3(config-pmap)# match avp eg_custom_avp
```

関連コマンド

コマンド	説明
class-map type inspect diameter	Diameter インスペクション クラス マップを作成します。
match avp	Diameter 属性値ペア（AVP）を照合します。
policy-map type inspect diameter	Diameter インスペクション ポリシー マップを作成します。

dir

ディレクトリの内容を表示するには、特権 EXEC モードで **dir** コマンドを使用します。

dir [/all] [**all-filesystems**] [**/recursive**] [**disk0: | disk1: | flash: | system:**] [*path]*

構文の説明

/all	(任意)すべてのファイルを表示します。
/recursive	(任意)ディレクトリの内容を再帰的に表示します。
all-filesystems	(任意)すべてのファイル システムのファイルを表示します。
disk0:	(任意)内部フラッシュ メモリを指定し、続けてコロンを入力します。
disk1:	(任意)外部フラッシュ メモリ カードを指定し、続けてコロンを入力します。
flash:	(任意)デフォルト フラッシュ パーティションのディレクトリの内容を表示します。
path	(任意)特定のパスを指定します。
system:	(任意)ファイル システムのディレクトリの内容を表示します。

デフォルト

ディレクトリを指定しない場合、ディレクトリはデフォルトで現在の作業ディレクトリになります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

キーワードまたは引数のない **dir** コマンドは、現在のディレクトリの内容を表示します。

例

次に、ディレクトリの内容を表示する例を示します。

```
ciscoasa# dir
Directory of disk0:/

1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

次に、ファイル システム全体の内容を再帰的に表示する例を示します。

```
ciscoasa# dir /recursive disk0:
Directory of disk0:/*
1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

次に、フラッシュ パーティションの内容を表示する例を示します。

```
ciscoasa# dir flash:
Directory of disk0:/*
1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

関連コマンド

コマンド	説明
cd	現在の作業ディレクトリから、指定したディレクトリに変更します。
pwd	現在の作業ディレクトリを表示します。
mkdir	ディレクトリを作成します。
rmdir	ディレクトリを削除します。

director-localization

ディレクタのローカリゼーションを有効にして、データセンターのサイト間クラスタリングのパフォーマンスを向上させ、ラウンドトリップ時間の遅延を減らすには、クラスタ グループ コンフィギュレーション モードで **director-localization** コマンドを使用します。ディレクタのローカリゼーションをディセーブルにするには、このコマンドの **no** 形式を使用します。

director-localization

no director-localization

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラスタ グループ コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

通常、新しい接続は特定のサイト内のクラスタ メンバーによってロード バランスされ、所有されています。ただし、ASA は任意のサイトのメンバーにディレクタ ロールを割り当てます。ディレクタ ローカリゼーションにより、所有者と同じサイトのローカル ディレクタ、どのサイトにも存在可能なグローバル ディレクタという追加のディレクタ ロールが有効になります。所有者とディレクタが同一サイトに存在すると、パフォーマンスが向上します。また、元の所有者が失敗した場合、ローカルなディレクタは同じサイトで新しい接続の所有者を選択します。グローバルなディレクタは、クラスタ メンバーが別のサイトで所有される接続のパケットを受信する場合に使用されます。

ブートストラップ設定でクラスタ メンバーのサイト ID を設定します。

次のトラフィック タイプは、ローカリゼーションをサポートしていません：NAT および PAT トラフィック、SCTP 検査されたトラフィック、フラグメンテーション所有クエリ。

例

次に、cluster1 のディレクタのローカリゼーションをイネーブルにする例を示します。

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# local-unit unit1
ciscoasa(cfg-cluster)# site-id 1
ciscoasa(cfg-cluster)# cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
ciscoasa(cfg-cluster)# priority 1
ciscoasa(cfg-cluster)# key chuntheunavoidable
ciscoasa(cfg-cluster)# director-localization
ciscoasa(cfg-cluster)# enable noconfirm
```

関連コマンド

コマンド	説明
cluster group	クラスタ グループ コンフィギュレーション モードを開始します。
show asp table cluster chash	ローカル cHash テーブルを表示します。
show conn	conn フラグ「l」は、スタブ フローがローカル ディレクタ「Yl」または ローカル バックアップ「yl」であることを示します。
site-id	サイト間クラスタリングで使用するクラスタ ユニットのサイト ID を設定します。

disable（キャッシュ）

WebVPN に対するキャッシングをディセーブルにするには、キャッシュ コンフィギュレーション モードで **disable** コマンドを使用します。キャッシングを再度イネーブルにするには、このコマンドの **no** 形式を使用します。

disable

no disable

デフォルト

キャッシングは、各キャッシュ属性に対するデフォルトの設定でイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力するモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
キャッシュ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

キャッシングによって頻繁に再利用されるオブジェクトはシステム キャッシュに保存され、コンテンツを繰り返しリライトしたり圧縮したりする必要性を減らすことができます。キャッシングにより、WebVPN とリモート サーバおよびエンド ユーザのブラウザの両方の間のトラフィックが削減されて、多くのアプリケーションの実行効率が大幅に向上されます。

例

次に、キャッシングをディセーブルにしてから、それを再度イネーブルにする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# cache
ciscoasa(config-webvpn-cache)# disable
ciscoasa(config-webvpn-cache)# no disable
ciscoasa(config-webvpn-cache)#
```

関連コマンド

コマンド	説明
cache	webvpn キャッシュ コンフィギュレーション モードを開始します。
expiry-time	オブジェクトを再検証せずにキャッシュする有効期限を設定します。

コマンド	説明
lmfactor	最終変更時刻のタイムスタンプだけを持つオブジェクトのキャッシュに関する再確認ポリシーを設定します。
max-object-size	キャッシュするオブジェクトの最大サイズを定義します。
min-object-size	キャッシュするオブジェクトの最小サイズを定義します。

disable（特権 EXEC）

特権 EXEC モードを終了してユーザ EXEC モードに戻るには、特権 EXEC モードで **disable** コマンドを使用します。

disable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• **対応**	• **対応**	• 対応	• 対応	• **対応**

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

enable コマンドを使用して、特権モードを開始します。**disable** コマンドは、特権モードを終了して、ユーザ モードに戻ります。

（注） ユーザ名を使用して ASA にログインしている場合、**disable** と入力するとユーザ ID がデフォルトの enable_1 ユーザ名に変更されます。

例

次の例は、特権モードを開始する方法を示しています。

```
ciscoasa> enable
ciscoasa#
```

次に、特権モードを終了する例を示します。

```
ciscoasa# disable
ciscoasa>
```

関連コマンド

コマンド	説明
enable	特権 EXEC モードを有効にします。

disable service-settings（廃止）

電話プロキシ機能の使用時に IP 電話のサービス設定をディセーブルにするには、電話プロキシ コンフィギュレーション モードで **disable service-settings** コマンドを使用します。IP 電話の設定を保持するには、このコマンドの **no** 形式を使用します。

disable service-settings

no disable service-settings

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

サービス設定はデフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
Phone-Proxy コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。
9.4(1)	このコマンドは、すべての **phone-proxy** モード コマンドとともに廃止されました。

使用上のガイドライン

デフォルトでは、次の設定内容が IP 電話ではディセーブルになります。

- PC Port
- Gratuitous ARP
- Voice VLAN Access
- Web Access
- Span to PC Port

設定されている各 IP フォンの CUCM で設定されている設定を保持するには、**no disable service-settings** コマンドを設定します。

例

次に、ASA で電話プロキシ機能を使用する IP Phone の設定を保持する例を示します。

```
ciscoasa(config-phone-proxy)# no disable service-settings
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。
show phone-proxy	Phone Proxy 固有の情報を表示します。

display

ASA が DAP 属性データベースに書き込む属性値のペアを表示するには、DAP テスト属性モードで **display** コマンドを入力します。

display

コマンド デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
Dap テスト属性	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

通常、ASA は AAA サーバからユーザ認可属性を取得し、Cisco Secure Desktop、Host Scan、CNA または NAC からエンドポイント属性を取得します。test コマンドの場合、ユーザ認可属性とエンドポイント属性をこの属性モードで指定します。ASA は、これらの属性を、DAP サブシステムが DAP レコードの AAA 選択属性およびエンドポイント選択属性を評価するときに参照する属性データベースに書き込みます。**display** コマンドを使用すると、これらの属性をコンソールに表示できます。

関連コマンドl

コマンド	説明
attributes	属性コンフィギュレーション モードを開始します。このモードでは属性値のペアを設定できます。
dynamic-access-policy-record	DAP レコードを作成します。
test dynamic-access-policy attributes	属性サブモードを開始します。
test dynamic-access-policy execute	DAP を生成するロジックを実行し、生成されたアクセスポリシーをコンソールに表示します。

distance

IS-IS プロトコルによって検出されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義するには、ルータ ISIS コンフィギュレーション モードで **distance** コマンドを使用します。コンフィギュレーション ファイルから distance コマンドを削除して、ソフトウェアがディスタンス定義を削除するようにシステムをデフォルト状態に戻すには、このコマンドの **no** 形式を使用します。

distance *weight* **ip**

no distance *weight* **ip**

構文の説明

weight	IS-IS ルートに割り当てるアドミニストレーティブ ディスタンスです。指定できる範囲は 1 ～ 255 です。
ip	IP から取得されるルートに適用する距離です。

デフォルト

デフォルトは 115 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

アドミニストレーティブ ディスタンスは、1 ～ 255 の数値です。通常は、値が大きいほど、信頼性の格付けが下がります。255 のアドミニストレーティブ ディスタンスは、ルーティング情報源がまったく信頼できないため、無視すべきであることを意味します。重み値は主観的に選択します。重み値を選択するための定量的方法はありません。

distance コマンドは、IS-IS ルートがルーティング情報ベース（RIB）に挿入されるときに適用されるアドミニストレーティブ ディスタンスを設定し、他のプロトコルによって検出された同じ宛先アドレスへのルートよりもこれらのルートが優先される可能性に影響を与えるために使用します。

例

次に、すべての IS-IS ルートに距離 20 を割り当てる例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)#distance 20 ip
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。

コマンド	説明
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト(TLV)を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

distance bgp

BGP ルートのアドミニストレーティブ ディスタンスを設定するには、アドレス ファミリ コンフィギュレーション モードで **distance bgp** コマンドを使用します。アドミニストレーティブ ディスタンスをデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

distance bgp *external-distance internal-distance local-distance*

no distance bgp

構文の説明

external-distance	外部 BGP ルートのアドミニストレーティブ ディスタンス。ルートは、外部自律システムから学習された場合は外部になります。この引数の値の範囲は 1 ～ 255 です。
internal-distance	内部 BGP ルートのアドミニストレーティブ ディスタンス。ルートは、ローカル自律システムのピアから学習された場合は内部です。この引数の値の範囲は 1 ～ 255 です。
local-distance	ローカル BGP ルートのアドミニストレーティブ ディスタンス。別のプロセスから再配布されているルータやネットワークの場合、ローカル ルートとは、**network** ルータ コンフィギュレーション コマンドで、通常はバック ドアとして表示されるネットワークです。この引数の値の範囲は 1 ～ 255 です。

デフォルト

このコマンドを設定しない場合、または no 形式を入力した場合は、次の値が使用されます。

external-distance：20
internal-distance：200
local-distance：200

(注) アドミニストレーティブ ディスタンスが 255 のルートはルーティング テーブルに格納されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
アドレスファミリ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

distance bgp コマンドは、個々のルータやルータのグループなど、ルーティング情報送信元の信頼性の格付けを設定するために使用されます。アドミニストレーティブ ディスタンスを数値で表すと、1 ～ 255 の正の整数です。

通常は、値が大きいほど、信頼性の格付けが下がります。アドミニストレーティブ ディスタンスが 255 の場合はルーティング情報の送信元をまったく信頼できないため、無視する必要があります。他のプロトコルが外部 BGP（eBGP）によって実際に学習されたルートよりも良いルートをノードに提供できることがわかっている場合、または一部の内部ルートが BGP によって優先されるべきである場合、このコマンドを使用します。

注意 内部 BGP ルートのアドミニストレーティブ ディスタンスを変更することは危険と見なされており、推奨されません。不適切な設定により、ルーティング テーブルの不整合性やルーティングの中断が発生する可能性があります。

distance mbgp コマンドは、**distance bgp** コマンドに置き換わりました。

例

次の例では、外部ディスタンスを 10、内部ディスタンスを 50、ローカル ディスタンスを 100 に設定しています。

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# neighbor 192.168.6.6 remote-as 123
ciscoasa(config-router-af)# neighbor 172.16.1.1 remote-as 47
ciscoasa(config-router-af)# distance bgp 10 50 100
ciscoasa(config-router-af)# end
```

distance eigrp

内部および外部 EIGRP ルートのアドミニストレーティブ ディスタンスを設定するには、ルータ コンフィギュレーション モードで **distance eigrp** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

distance eigrp *internal-distance external-distance*

no distance eigrp

構文の説明

external-distance	EIGRP 外部ルートのアドミニストレーティブ ディスタンス。外部ルートとは、最適パスを自律システムの外部にあるネイバーから学習するルートです。有効な値は、1 ～ 255 です。
internal-distance	EIGRP 内部ルートのアドミニストレーティブ ディスタンス。内部ルートとは、同じ自律システム内の別のエンティティから学習されるルートです。有効な値は、1 ～ 255 です。

デフォルト

デフォルト値は次のとおりです。

- *external-distance* は 170 です。
- *internal-distance* は 90 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

各ルーティング プロトコルには、他のルーティング プロトコルと異なるアルゴリズムに基づいたメトリックがあるため、異なるルーティング プロトコルによって生成された同じ宛先への 2 つのルートのいずれが「最適パス」であるかは、必ずしも判別できません。アドミニストレーティブ ディスタンスは、2 つの異なるルーティング プロトコルから同じ宛先に複数の異なるルートがある場合に、ASA が最適なパスの選択に使用するルート パラメータです。

ASA で複数のルーティング プロトコルが実行されている場合、**distance eigrp** コマンドを使用して、EIGRP ルーティング プロトコルが検出するルートのデフォルト アドミニストレーティブ ディスタンスを、他のルーティング プロトコルと関連付けて調整できます。表12-1 に、ASA でサポートされているルーティング プロトコルのデフォルトのアドミニストレーティブ ディスタンスを示します。

表12-1　デフォルトのアドミニストレーティブ ディスタンス

ルートの送信元	デフォルトのアドミニストレーティブ ディスタンス
接続されているインターフェイス	0
スタティック ルート	1
EIGRP 集約ルート	5
内部 EIGRP	90
OSPF	110
RIP	120
EIGRP 外部ルート	170
不明（Unknown）	255

このコマンドの **no** 形式はキーワードまたは引数を使用しません。コマンドの **no** 形式を使用すると、内部と外部の両方の EIGRP ルートのアドミニストレーティブ ディスタンスがデフォルトに戻されます。

例

次に、**distance eigrp** コマンドを使用して、すべての EIGRP 内部ルートのアドミニストレーティブ ディスタンスを 80 に、すべての EIGRP 外部ルートのアドミニストレーティブ ディスタンスを 115 に設定する例を示します。EIGRP 外部ルートのアドミニストレーティブ ディスタンスを 115 に設定すると、EIGRP によって検出されたルートが、RIP（OSPF ではなく）によって検出された同じルートを経由する特定の宛先設定に渡されます。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 192.168.7.0
ciscoasa(config-router)# network 172.16.0.0
ciscoasa(config-router)# distance eigrp 90 115
```

関連コマンド

コマンド	説明
router eigrp	EIGRP ルーティング プロセスを作成し、このプロセスのコンフィギュレーション モードを開始します。

distance ospf（IPv6 ルータ OSPF）

ルート タイプに基づいて OSPFv3 ルートのアドミニストレーティブ ディスタンスを定義するには、IPv6 ルータ OSPF コンフィギュレーション モードで **distance** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

distance [**ospf** {**external** | **intra-area** | **inter-area**}] *distance*

no distance [**ospf** {**external** | **intra-area** | **inter-area**}] *distance*

構文の説明

distance	アドミニストレーティブディスタンスを指定します。有効値の範囲は 10 ～ 254 です。
external	（オプション）OSPFv3 ルートに外部タイプ 5 およびタイプ 7 のルートを指定します。
inter-area	（オプション）OSPFv3 ルートにエリア間ルートを指定します。
intra-area	（オプション）OSPFv3 ルートにエリア内ルートを指定します。
ospf	（オプション）OSPFv3 ルートにアドミニストレーティブ ディスタンスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
IPv6 ルータ OSPF コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

OSPFv3 ルートのアドミニストレーティブ ディスタンスを設定するには、このコマンドを使用します。

例

次に、OSPFv3 に対して外部タイプ 5 およびタイプ 7 のルートのアドミニストレーティブ ディスタンスを 200 に設定する例を示します。

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-router)# distance ospf external 200
```

関連コマンド

コマンド	説明
default-information originate	OSPFv3 ルーティング ドメインへのデフォルトの外部ルートを生成します。
redistribute	あるルーティング ドメインから別のルーティング ドメインへ IPv6 ルートを再配布します。

distance ospf（ルータ OSPF）

ルート タイプに基づいて OSPFv2 ルートのアドミニストレーティブ ディスタンスを定義するには、ルータ OSPF コンフィギュレーション モードで **distance ospf** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

distance ospf [**intra-area** *d1*] [**inter-area** *d2*] [**external** *d3*]

no distance ospf

構文の説明

d1、*d2*、*d3*	各ルート タイプの距離を指定します。有効値の範囲は、1 ～ 255 です。
external	（任意）再配布によって取得した他のルーティング ドメインからのルートに距離を設定します。
inter-area	（任意）あるエリアから別のエリアまでのルートすべての距離を設定します。
intra-area	（任意）あるエリア内のすべてのルートの距離を設定します。

デフォルト

d1、*d2*、および *d3* のデフォルト値は 110 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ OSPF コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

少なくとも 1 つのキーワードと引数を指定する必要があります。アドミニストレーティブ ディスタンスのタイプごとにコマンドを個別に入力することができますが、コンフィギュレーションでは 1 つのコマンドとして表示されます。アドミニストレーティブ ディスタンスを再入力する場合、対象ルート タイプのアドミニストレーティブ ディスタンスだけが変更されます。その他のルート タイプのアドミニストレーティブ ディスタンスは影響されません。

このコマンドの **no** 形式はキーワードまたは引数を使用しません。コマンドの **no** 形式を使用すると、すべてのルート タイプのアドミニストレーティブ ディスタンスがデフォルトに戻されます。複数のルート タイプを設定している場合、1 つのルート タイプをデフォルトのアドミニストレーティブ ディスタンスに戻すには、次のいずれかを実行します。

- ルート タイプを、手動でデフォルト値に設定します。
- このコマンドの **no** 形式を使用してコンフィギュレーション全部を削除し、保持するルート タイプに対してコンフィギュレーションを再入力します。

例

次に、外部ルートのアドミニストレーティブ ディスタンスを 150 に設定する例を示します。

```
ciscoasa(config-router)# distance ospf external 105
ciscoasa(config-router)#
```

次に、各ルート タイプに入力した個別のコマンドが、ルータ コンフィギュレーションで 1 つのコマンドとして表示される例を示します。

```
ciscoasa(config-rtr)# distance ospf intra-area 105 inter-area 105
ciscoasa(config-rtr)# distance ospf intra-area 105
ciscoasa(config-rtr)# distance ospf external 105
ciscoasa(config-rtr)# exit
ciscoasa(config)# show running-config router ospf 1
!
router ospf 1
 distance ospf intra-area 105 inter-area 105 external 105
!
ciscoasa(config)#
```

次に、各アドミニストレーティブ ディスタンスを 105 に設定し、次に外部アドミニストレーティブ ディスタンスのみを 150 に変更する例を示します。**show running-config router ospf** コマンドは、外部ルート タイプの値だけが変更され、その他のルート タイプでは以前に設定された値が保持されている状況を示します。

```
ciscoasa(config-rtr)# distance ospf external 105 intra-area 105 inter-area 105
ciscoasa(config-rtr)# distance ospf external 150
ciscoasa(config-rtr)# exit
ciscoasa(config)# show running-config router ospf 1
!
router ospf 1
 distance ospf intra-area 105 inter-area 105 external 150
!
ciscoasa(config)#
```

関連コマンド

コマンド	説明
router ospf	OSPFv2 のルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションの OSPFv2 コマンドを表示します。

distribute-list

Open Shortest Path First（OSPF）アップデートで受信または転送されるネットワークをフィルタリングするには、ルータ OSPF コンフィギュレーション モードで **distribute-list** コマンドを使用します。フィルタを変更またはキャンセルするには、このコマンドの no 形式を使用します。

distribute-list *access-list name* [**in** |**out**] [**interface** *if_name*]

no distribute-list *access-list name* [**in** |**out**]

構文の説明

access-list name	標準 IP アクセス リスト名。このリストは、受信されるネットワークとルーティング アップデートで抑制されるネットワークを定義します。
in	アクセス リストまたはルート ポリシーを着信ルーティング アップデートに適用します。
out	発信ルーティング アップデートにアクセス リストまたはルート ポリシーを適用します。**out** キーワードは、ルータ コンフィギュレーション モードでだけ使用可能です。
interface *if_name*	（オプション）ルーティング アップデートを適用するインターフェイス。インターフェイスを指定すると、アクセス リストは指定されたインターフェイスで受信されたルーティング アップデートにのみ適用されます。

デフォルト

ネットワークはフィルタリングされません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ OSPF コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

インターフェイスが指定されていない場合、アクセス リストはすべての着信更新に適用されます。

例

次に、外部インターフェイスで受信する OSPF ルーティング アップデートをフィルタリングする例を示します。この例では、10.0.0.0 ネットワークのルートを受け入れ、他のすべてのルートを廃棄します。

```
ciscoasa(config)# access-list ospf_filter permit 10.0.0.0 255.0.0.0
ciscoasa(config)# access-list ospf_filter deny any
ciscoasa(config)# router ospf 1
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list ospf_filter in interface outside
```

関連コマンド

コマンド	説明
distribute-list in	着信ルーティング アップデートをフィルタリングします。
router ospf	OSPF ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

distribute-list in（アドレス ファミリ）

Border Gateway Protocol（BGP）の着信アップデートで受信したルートまたはネットワークをフィルタリングするには、アドレスファミリ コンフィギュレーション モードで **distribute-list in** コマンドを使用します。アドレスファミリ コンフィギュレーション モードにアクセスするには、**router bgp** コマンドを入力します。配布リストを削除し、これを実行コンフィギュレーション ファイルから削除するには、このコマンドの **no** 形式を使用します。

distribute-list {*acl-name* | **prefix** *list-name*} **in**

no distribute-list {*acl-name* | **prefix** *list-name*} **in**

構文の説明

acl-name	標準 IP アクセス リスト名。アクセス リストは、ルーティング アップデートで受信されるネットワークと抑制されるネットワークを定義します。
prefix *list-name*	プレフィックス リストの名前。プレフィックス リストは、一致プレフィックスに基づいて、受信されるネットワークとルーティング アップデートで抑制されるネットワークを定義します。

デフォルト

このコマンドが、事前定義済みのアクセス リストまたはプレフィックス リストなしで設定されている場合、配布リストではデフォルトですべてのトラフィックが許可されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
アドレスファミリ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

distribute-list in コマンドは、BGP の着信アップデートをフィルタリングするために使用されます。このコマンドを設定する前に、アクセス リストまたはプレフィックス リストを定義する必要があります。標準アクセス リストおよび拡張アクセス リストがサポートされています。IP プレフィックス リストは、プレフィックス ビット長に基づいたフィルタリングに使用されます。ネットワーク全体、サブネット、スーパーネット、または単一のホスト ルートを指定できます。配布リストを設定する場合は、プレフィックス リストとアクセス リストのコンフィギュレーションは相互に排他的です。配布リストを有効にする前に、**clear bgp** コマンドを使用してセッションをリセットする必要があります。

例

次の例では、プレフィックス リストと配布リストを定義して、ネットワーク 10.1.1.0/24、ネットワーク 192.168.1.0、およびネットワーク 10.108.0.0 からのトラフィックだけを受け入れるように BGP ルーティング プロセスを設定しています。着信ルート リフレッシュが開始され、配布リストがアクティブ化されます。

```
ciscoasa(config)# ip prefix-list RED permit 10.1.1.0/24
ciscoasa(config)# ip prefix-list RED permit 10.108.0.0/16
ciscoasa(config)# ip prefix-list RED permit 192.168.1.0/24
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# distribute-list prefix RED in
ciscoasa(config-router-af)# exit
ciscoasa(config-router)# exit
ciscoasa# clear bgp in
```

次の例では、アクセス リストと配布リストを定義して、ネットワーク 192.168.1.0 およびネットワーク 10.108.0.0 からのトラフィックだけを受け入れるように BGP ルーティング プロセスを設定しています。着信ルート リフレッシュが開始され、配布リストがアクティブ化されます。

```
ciscoasa(config)# access-list distribute-list-acl permit 192.168.1.0 255.255.255.0
ciscoasa(config)# access-list distribute-list-acl permit 10.108.0.0 255.255.0.0
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# distribute-list distribute-list-acl in
ciscoasa(config-router-af)# exit
ciscoasa(config-router)# exit
ciscoasa# clear bgp in
```

関連コマンド

コマンド	説明
clear bgp	ハードまたはソフト再構成を使用して BGP 接続をリセットします。
ip prefix-list	プレフィックス リストを作成したり、プレフィックス リスト エントリを追加したりします。

distribute-list in（ルータ）

着信ルーティング アップデートをフィルタリングするには、ルータ コンフィギュレーション モードで **distribute-list in** コマンドを使用します。フィルタリングを削除するには、このコマンドの **no** 形式のコマンドを使用します。

distribute-list *acl* **in** [**interface** *if_name*]

no distribute-list *acl* **in** [**interface** *if_name*]

構文の説明

acl	標準アクセス リスト名。
interface *if_name*	（オプション）着信ルーティング アップデートを適用するインターフェイス。インターフェイスを指定すると、アクセス リストは指定されたインターフェイスで受信されたルーティング アップデートにのみ適用されます。

デフォルト

着信更新の場合、ネットワークはフィルタリングされません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

インターフェイスが指定されていない場合、アクセス リストはすべての着信更新に適用されます。

例

次に、外部インターフェイスで受信する RIP ルーティング アップデートをフィルタリングする例を示します。この例では、10.0.0.0 ネットワークのルートを受け入れ、他のすべてのルートを廃棄します。

```
ciscoasa(config)# access-list ripfilter permit 10.0.0.0 255.0.0.0
ciscoasa(config)# access-list ripfilter deny any
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list ripfilter in interface outside
```

次に、外部インターフェイスで受信する EIGRP ルーティング アップデートをフィルタリングする例を示します。この例では、10.0.0.0 ネットワークのルートを受け入れ、他のすべてのルートを廃棄します。

```
ciscoasa(config)# access-list eigrp_filter permit 10.0.0.0 255.0.0.0
ciscoasa(config)# access-list eigrp_filter deny any
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list eigrp_filter in interface outside
```

関連コマンド

コマンド	説明
distribute-list out	発信ルーティング アップデートをフィルタリングします。
router eigrp	EIGRP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
router rip	RIP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

distribute-list out（アドレス ファミリ）

Border Gateway Protocol（BGP）の発信アップデートでネットワークがアドバタイズされないように抑制するには、アドレスファミリ コンフィギュレーション モードで **distribute-list out** コマンドを使用します。アドレスファミリ コンフィギュレーション モードにアクセスするには、**router bgp** コマンドを入力します。配布リストを削除し、これを実行コンフィギュレーション ファイルから削除するには、このコマンドの **no** 形式を使用します。

distribute-list {*acl-name* | **prefix** *list-name*} **out** [*protocol process-number* | **connected** | **static**]

no distribute-list {*acl-name* | **prefix** *list-name*} **out** [*protocol process-number* | **connected** | **static**]

構文の説明

acl-name	標準 IP アクセス リスト名。アクセス リストは、ルーティング アップデートで受信されるネットワークと抑制されるネットワークを定義します。
prefix *list-name*	プレフィックス リストの名前。プレフィックス リストは、一致プレフィックスに基づいて、受信されるネットワークとルーティング アップデートで抑制されるネットワークを定義します。
protocol process-number	配布リストに適用するルーティング プロトコルを指定します。BGP、EIGRP、OSPF、および RIP がサポートされています。RIP を除くすべてのルーティング プロトコルについて、プロセス番号を入力します。プロセス番号は、1 ～ 65 までの値です。
connected	接続ルートを通じて学習したピアおよびネットワークを指定します。
static	スタティック ルートを通じて学習したピアおよびネットワークを指定します。

デフォルト

このコマンドが、事前定義済みのアクセス リストまたはプレフィックス リストなしで設定されている場合、配布リストではデフォルトですべてのトラフィックが許可されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
アドレスファミリ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

distribute-list out コマンドは、BGP の発信アップデートをフィルタリングするために使用されます。このコマンドを設定する前に、アクセス リストまたはプレフィックス リストを定義する必要があります。標準アクセス リストだけがサポートされます。

IP プレフィックス リストは、プレフィックス ビット長に基づいたフィルタリングに使用されます。ネットワーク全体、サブネット、スーパーネット、または単一のホスト ルートを指定できます。配布リストを設定する場合は、プレフィックス リストとアクセス リストのコンフィギュレーションは相互に排他的です。配布リストを有効にする前に、**clear bgp** コマンドを使用してセッションをリセットする必要があります。

protocol 引数または *process-number* 引数（あるいはその両方）を入力すると、配布リストは、指定したルーティング プロセスから派生したルートだけに適用されます。distribute-list コマンドで指定されていないアドレスは、配布リストの設定後、発信ルーティング アップデートでアドバタイズされません。

発信アップデートでネットワークまたはルートが受信されないよう抑制するには、**distribute-list in** コマンドを使用します。

例

次の例では、プレフィックス リストと配布リストを定義して、ネットワーク 192.168.0.0 だけをアドバタイズするように BGP ルーティング プロセスを設定しています。アウトバウンド ルート リフレッシュが開始され、配布リストがアクティブ化されます。

```
ciscoasa(config)# ip prefix-list BLUE permit 192.168.0.0/16
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# distribute-list prefix BLUE out
ciscoasa(config-router-af)# exit
ciscoasa(config-router)# exit
ciscoasa# clear bgp out
```

次の例では、アクセス リストと配布リストを定義して、ネットワーク 192.168.0.0 だけをアドバタイズするように BGP ルーティング プロセスを設定しています。アウトバウンド ルート リフレッシュが開始され、配布リストがアクティブ化されます。

```
ciscoasa(config)# access-list distribute-list-acl permit 192.168.0.0 255.255.0.0
ciscoasa(config)# access-list distribute-list-acl deny 0.0.0.0 0.0.0.0
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# distribute-list distribute-list-acl out
ciscoasa(config-router-af)# exit
ciscoasa(config-router)# exit
ciscoasa# clear bgp out
```

関連コマンド

コマンド	説明
clear bgp	ハードまたはソフト再構成を使用して BGP 接続をリセットします。
ip prefix-list	プレフィックス リストを作成したり、プレフィックス リスト エントリを追加したりします。

distribute-list out（ルータ）

発信ルーティング アップデートをフィルタリングするには、ルータ コンフィギュレーション モードで **distribute-list out** コマンドを使用します。フィルタリングを削除するには、このコマンドの **no** 形式のコマンドを使用します。

distribute-list *acl* **out** [**interface** *if_name*] [**eigrp** *as_number* | **rip** | **ospf** *pid* | **static** | **connected**]

no distribute-list *acl* **out** [**interface** *if_name*] [**eigrp** *as_number* | **rip** | **ospf** *pid* | **static** | **connected**]

構文の説明

acl	標準アクセス リスト名。
connected	（任意）接続されたルートのみフィルタリングします。
eigrp *as_number*	（任意）指定した自律システム番号からの EIGRP ルートだけをフィルタリングします。*as_number* 引数は、ASA 上の EIGRP ルーティング プロセスの自律システム番号です。
interface *if_name*	（オプション）発信ルーティング アップデートを適用するインターフェイス。インターフェイスを指定すると、アクセス リストは指定されたインターフェイスで受信されたルーティング アップデートにのみ適用されます。
ospf *pid*	（任意）指定した OSPF プロセスにより検出された OSPF ルートのみフィルタリングします。
rip	（任意）RIP ルートのみフィルタリングします。
static	（任意）スタティック ルートだけをフィルタリングします。

デフォルト

送信更新の場合、ネットワークはフィルタリングされません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.0(2)	**eigrp** キーワードが追加されました。

使用上のガイドライン

インターフェイスが指定されていない場合、アクセス リストはすべての発信更新に適用されます。

例

次に、任意のインターフェイスから送信された RIP 更新で 10.0.0.0 ネットワークがアドバタイズされないようにする例を示します。

```
ciscoasa(config)# access-list ripfilter deny 10.0.0.0 255.0.0.0
ciscoasa(config)# access-list ripfilter permit any
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list ripfilter out
```

次に、EIGRP ルーティング プロセスで外部インターフェイスの 10.0.0.0 ネットワークがアドバタイズされないようにする例を示します。

```
ciscoasa(config)# access-list eigrp_filter deny 10.0.0.0 255.0.0.0
ciscoasa(config)# access-list eigrp_filter permit any
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# distribute-list eigrp_filter out interface outside
```

関連コマンド

コマンド	説明
distribute-list in	着信ルーティング アップデートをフィルタリングします。
router eigrp	EIGRP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
router rip	RIP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

CHAPTER 13

dnscrypt コマンド～ dynamic-filter whitelist コマンド

dnscrypt

DNScrypt がデバイスと Cisco Umbrella 間の接続を暗号化できるようにするには、DNS インスペクション ポリシー マップのパラメータ コンフィギュレーション モードで **dnscrypt** コマンドを使用します。DNScrypt を無効にするには、このコマンドの **no** 形式を使用します。

dnscrypt

no dnscrypt

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

DNScrypt は無効になっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.10(1)	このコマンドが追加されました。

使用上のガイドライン

DNS インスペクション ポリシーマップを設定する際に、次のコマンドを使用します。

DNScrypt を有効にすると、Umbrella リゾルバとのキー交換スレッドが開始されます。キー交換スレッドは、1 時間ごとにリゾルバとのハンドシェイクを実行し、新しい秘密鍵でデバイスを更新します。

DNScrypt では UDP/443 を使用するため、そのポートが DNS インスペクションに使用するクラス マップに含まれていることを確認する必要があります。デフォルトのインスペクション クラスには DNS インスペクションに UDP/443 がすでに含まれています。

例

次の例では、デフォルト ポリシーを使用して Umbrella を有効にし、グローバル DNS インスペクションで使用されるデフォルトのインスペクション ポリシーマップで DNScrypt も有効にします。グローバル DNS インスペクションはすでに UDP/443 に適用されています。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella
ciscoasa(config-pmap-p)# dnscrypt
```

関連コマンド

コマンド	説明
inspect dns	DNS インスペクションをイネーブルにします。
policy-map type inspect dns	DNS インスペクション ポリシー マップを作成します。
public-key	Cisco Umbrella で使用する公開キーを設定します。
token	Cisco Umbrella への登録に必要な API トークンを指定します。
timeout edns	アイドル タイムアウトを設定します。その時間が経過するまでサーバからの応答がない場合、クライアントから Umbrella サーバへの接続は削除されます。
umbrella-global	Cisco Umbrella グローバルパラメータを設定します。
umbrella	DNS インスペクション エンジンで、DNS ルックアップ要求を Cisco Umbrella にリダイレクトできるようにします。

dns domain-lookup

サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信することをイネーブルにするには、グローバル コンフィギュレーション モードで **dns domain-lookup** コマンドを使用します。DNS 要求をディセーブルにするには、このコマンドの **no** 形式を使用します。

(注) ASA では、機能に応じて DNS サーバの使用が限定的にサポートされます。たとえば、ほとんどのコマンドでは、IP アドレスを入力する必要があります。名前を使用できるのは、名前と IP アドレスを関連付けるように **name** コマンドを手動で設定し、**names** コマンドを使用して名前の使用をイネーブルにした場合だけです。

dns domain-lookup *interface_name*

no dns domain-lookup *interface_name*

構文の説明

interface_name	設定されたインターフェイスの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

DNS ルックアップをイネーブルにした後で、**dns server-group DefaultDNS** サーバ グループ コマンド、次に **name-server** コマンドを使用して DNS サーバを指定します。アクティブなサーバ グループは、**dns-group** コマンドを使用して変更できます。PN トンネル グループ用に他の DNS サーバ グループを設定できます。詳細については、**tunnel-group** コマンドを参照してください。

一部の ASA 機能では、ドメイン名で外部サーバにアクセスするために DNS サーバを使用する必要があります。たとえば、ボットネット トラフィック フィルタ機能では、ダイナミック データベース サーバにアクセスして、スタティック データベースのエントリを解決するために DNS サーバが必要です。さらに、Cisco Smart Software Licensing では、ライセンス機関のアドレスの解決に DNS が必要です。他の機能（**ping** コマンドや **traceroute** コマンドなど）では、ping や traceroute を実行する名前を入力できるため、ASA は DNS サーバと通信することで名前を解決できます。名前は、多くの SSL VPN コマンドおよび certificate コマンドでもサポートされます。また、アクセス ルールに完全修飾ドメイン名（FQDN）ネットワーク オブジェクトを使用するために、DNS サーバを設定する必要もあります。

例

次に、管理インターフェイス、内部インターフェイス、および DMZ インターフェイスに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにする例を示します。

```
ciscoasa(config)# dns domain-lookup management
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns domain-lookup dmz
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# name-server 10.1.1.1 management
ciscoasa(config-dns-server-group)# name-server 10.10.1.1 10.20.2.2
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
dns server-group	DNS サーバ グループを設定できる DNS サーバ グループ モードを開始します。
show running-config dns-server group	既存の DNS サーバ グループ コンフィギュレーションを 1 つまたはすべて表示します。

dns expire-entry-timer

TTL が期限切れになった後で解決された FQDN の IP アドレスを削除するには、グローバル コンフィギュレーション モードで **dns expire-entry-timer** コマンドを使用します。タイマーを削除するには、このコマンドの **no** 形式を使用します。

dns expire-entry-timer minutes *minutes*

no dns expire-entry-timer minutes *minutes*

構文の説明

minutes *minutes*	タイマーの時間を分単位で指定します。有効な値の範囲は、1 ～ 65535 分です。

デフォルト

デフォルトでは、DNS expire-entry-timer 値は 1 分です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション モード	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、解決された FQDN の IP アドレスが、その TTL の期限切れ後に削除されるまでの時間を指定します。IP アドレスが削除されると、ASA は tmatch ルックアップ テーブルを再コンパイルします。

このコマンドの指定は、DNS に関連するネットワーク オブジェクトがアクティブ化されている場合にのみ有効です。

デフォルトの DNS expire-entry-timer 値は 1 分です。これは、DNS エントリの TTL の期限が切れた 1 分後に IP アドレスが削除されることを意味します。

(注) 一般的な FQDN ホスト（www.sample.com など）の解決 TTL が短時間である場合、デフォルト設定を使用すると、tmatch ルックアップ テーブルが頻繁に再コンパイルされる可能性があります。セキュリティを確保すると同時に tmatch ルックアップ テーブルの再コンパイル頻度を減らすために、長い DNS expire-entry タイマー値を指定できます。

例

次に、解決されたエントリを 240 分後に削除する例を示します。

```
ciscoasa(config)# dns expire-entry-timer minutes 240
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
dns server-group	DNS サーバ グループを設定できる DNS サーバ グループ モードを開始します。
show running-config dns-server group	既存の DNS サーバ グループ コンフィギュレーションを 1 つまたはすべて表示します。

dns-group

アクティブな DNS グループを指定するには、グローバル コンフィギュレーション モードで **dns-group** コマンドを使用します。トンネル グループごとに DNS サーバ グループを指定するには、トンネル グループ webvpn 属性コンフィギュレーション モードで **dns-group** コマンドを使用します。デフォルトの DNS グループに戻すには、このコマンドの **no** 形式を使用します。

dns-group *name*

no dns-group

構文の説明

name	アクティブな DNS サーバ グループの名前を指定します。

デフォルト

デフォルト値は DefaultDNS です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—
トンネル グループ webvpn 属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

dns server-group コマンドを使用して、DNS グループを設定します。

例

次に、「dnsgroup1」という名前の DNS グループの使用を指定するカスタマイゼーション コマンドの例を示します。

```
ciscoasa(config)# tunnel-group test type webvpn
ciscoasa(config)# tunnel-group test webvpn-attributes
ciscoasa(config-tunnel-webvpn)# dns-group dnsgroup1
ciscoasa(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
dns server-group	DNS サーバ グループを設定できる DNS サーバ グループ モードを開始します。
show running-config dns-server group	既存の DNS サーバ グループ コンフィギュレーションを 1 つまたはすべて表示します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ属性を設定する config-webvpn モードを開始します。

dns-guard

クエリーごとに 1 つの DNS 応答を実行する DNS Guard 機能をイネーブルにするには、パラメータ コンフィギュレーション モードで **dns-guard** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

dns-guard

no dns-guard

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

DNS Guard は、デフォルトでイネーブルになっています。この機能は、**policy-map type inspect dns** コマンドを定義していなくても、**inspect dns** コマンドを設定していれば、イネーブルにできます。ディセーブルにするには、ポリシー マップ コンフィギュレーションで **no dns-guard** コマンドを明示的に指定する必要があります。**inspect dns** コマンドが設定されていない場合、動作は **global dns-guard** コマンドが決定します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

DNS ヘッダーの ID フィールドを使用して、DNS 応答と DNS ヘッダーを一致させます。クエリーごとに 1 つの応答が ASA を介して許可されます。

例

次に、DNS インスペクション ポリシー マップで DNS Guard をイネーブルにする例を示します。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# dns-guard
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

dns name-server

アクティブな DNS サーバ グループの DNS サーバを設定するには、グローバル コンフィギュレーション モードで **dns name-server** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。このコマンドは、**name-server** コマンドと同等です。

(注) ASA では、機能に応じて DNS サーバの使用が限定的にサポートされます。たとえば、ほとんどのコマンドでは、IP アドレスを入力する必要があります。名前を使用できるのは、名前と IP アドレスを関連付けるように **name** コマンドを手動で設定し、**names** コマンドを使用して名前の使用をイネーブルにした場合だけです。

dns name-server *ip_address* [*ip_address2*] [...] [*ip_address6*]

no dns name-server *ip_address* [*ip_address2*] [...] [*ip_address6*]

構文の説明

ip_address	DNS サーバの IPv4 または IPv6 アドレスを指定します。最大で 6 個のアドレスを指定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(2)	このコマンドは、**dns server-group DefaultDNS** サーバ グループに DNS サーバを追加するように変更されました。
9.0(1)	IPv6 アドレスのサポートが追加されました。

使用上のガイドライン

DNS 検索をイネーブルにするには、**dns domain-lookup** コマンドを使用します。DNS ルックアップをイネーブルにしないと、DNS サーバは使用されません。

このコマンドは、アクティブな DNS サーバ グループにサーバを追加します。デフォルトでは、アクティブなグループは **DefaultDNS** と呼ばれます。**dns-group** コマンドを使用してアクティブなグループを変更できます。次に結果の設定を示します。

```
ciscoasa(config)# dns name-server 10.1.1.1
ciscoasa(config)# show running-config dns
dns server-group DefaultDNS
    name-server ip_address
```

一部の ASA 機能では、ドメイン名で外部サーバにアクセスするために DNS サーバを使用する必要があります。たとえば、ボットネット トラフィック フィルタ機能では、ダイナミック データベース サーバにアクセスして、スタティック データベースのエントリを解決するために DNS サーバが必要です。さらに、Cisco Smart Software Licensing では、ライセンス機関のアドレスの解決に DNS が必要です。他の機能（**ping** コマンドや **traceroute** コマンドなど）では、ping や traceroute を実行する名前を入力できるため、ASA は DNS サーバと通信することで名前を解決できます。名前は、多くの SSL VPN コマンドおよび certificate コマンドでもサポートされます。また、アクセス ルールに完全修飾ドメイン名（FQDN）ネットワーク オブジェクトを使用するために、DNS サーバを設定する必要もあります。

例

次に、IPv6 アドレスで DNS サーバを設定する例を示します。

```
ciscoasa(config)# dns domain-lookup
ciscoasa(config)# dns name-server 8080:1:2::2
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
dns server-group	DNS サーバを設定できる DNS サーバ グループ モードを開始します。
show running-config dns-server group	既存の DNS サーバ グループ コンフィギュレーションを 1 つまたはすべて表示します。

dns poll-timer

ネットワーク オブジェクト グループで定義された完全修飾ドメイン名（FQDN）を解決するために、ASA が DNS サーバに照会する期間のタイマーを指定するには、グローバル コンフィギュレーション モードで **dns poll-timer** コマンドを使用します。タイマーを削除するには、このコマンドの **no** 形式を使用します。

dns poll-timer minutes *minutes*

no dns poll-timer minutes *minutes*

構文の説明

minutes *minutes*	タイマーを分単位で指定します。有効な値は、1 ～ 65535 分です。

デフォルト

デフォルトでは、DNS タイマーは 240 分または 4 時間です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、ネットワーク オブジェクト グループで定義された FQDN を解決するために、ASA が DNS サーバに照会する期間のタイマーを指定します。FQDN は、DNS ポーリング タイマーの期限切れ、または、解決された IP エントリの TTL の期限切れのいずれかが発生した時点で解決されます。

このコマンドは、少なくとも 1 つのネットワーク オブジェクト グループがアクティブ化されている場合にのみ有効です。

例

次に、DNS ポーリング タイマーを 240 分に設定する例を示します。

```
ciscoasa(config)# dns poll-timer minutes 240
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
dns server-group	DNS サーバ グループを設定できる DNS サーバ グループ モードを開始します。
show running-config dns-server group	既存の DNS サーバ グループ コンフィギュレーションを 1 つまたはすべて表示します。

dns-server（グループ ポリシー）

プライマリおよびセカンダリの DNS サーバの IP アドレスを設定するには、グループ ポリシー コンフィギュレーション モードで **dns-server** コマンドを使用します。実行コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

dns-server {**value** *ip_address* [*ip_address*] | **none**}

no dns-server

構文の説明

none	**dns-server** コマンドをヌル値に設定して、DNS サーバが許可されないようにします。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。
value *ip_address*	プライマリおよびセカンダリ DNS サーバの IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、別のグループ ポリシーの DNS サーバを継承できます。サーバが継承されないようにするには、**dns-server none** コマンドを使用します。

dns-server コマンドを実行するたびに、既存の設定が上書きされます。たとえば、DNS サーバ x.x.x.x を設定し、次に DNS サーバ y.y.y.y を設定した場合、2 番めのコマンドは最初のコマンドを上書きし、y.y.y.y が唯一の DNS サーバになります。複数のサーバを設定する場合も同様です。以前に設定された DNS サーバを上書きする代わりにサーバを追加するには、このコマンドを入力するときにすべての DNS サーバの IP アドレスを含めます。

例

次の例は、FirstGroup という名前のグループ ポリシーに、IP アドレスが 10.10.10.15 と 10.10.10.45 である DNS サーバを設定する方法を示しています。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# dns-server value 10.10.10.15 10.10.10.45
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
show running-config dns server-group	現在の実行中の DNS サーバ グループ コンフィギュレーションを表示します。

dns-server（IPv6 DHCP プール）

DHCPv6 サーバを設定するときにステートレス アドレス自動設定（SLAAC）クライアントに DNS サーバの IP アドレスを提供するには、IPv6 DHCP プール コンフィギュレーション モードで **dns-server** コマンドを使用します。DNS サーバを削除するには、このコマンドの **no** 形式を使用します。

dns-server *dns_ipv6_address*

no dns-server *dns_ipv6_address*

構文の説明

dns_ipv6_address	DNS サーバの IPv6 アドレスを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
IPv6 DHCP プール コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

プレフィックス委任機能とともに SLAAC を使用しているクライアントの場合は、クライアントが情報要求（IR）パケットを ASA に送信したときに、DNS サーバを含め、**ipv6 dhcp プール**内の情報を提供するように ASA を設定できます。ASA は IR パケットのみを受け付け、アドレスをクライアントに割り当てません。DHCPv6 ステートレス サーバを設定するには、**ipv6 dhcp server** コマンドを使用します。サーバを有効にする場合は、**ipv6 dhcp プール**名を指定します。

プレフィックス委任を設定するには、**ipv6 dhcp client pd** コマンドを使用します。

この機能は、クラスタリングではサポートされていません。

例

次に、2 つの IPv6 DHCP プールを作成して、2 つのインターフェイスで DHCPv6 サーバを有効にする例を示します。

```
ipv6 dhcp pool Eng-Pool
    domain-name eng.example.com
    dns-server 2001:DB8:1::1
ipv6 dhcp pool IT-Pool
    domain-name it.example.com
    dns-server 2001:DB8:1::1
interface gigabitethernet 0/0
    ipv6 address dhcp setroute default
    ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
    ipv6 address Outside-Prefix ::1:0:0:0:1/64
    ipv6 dhcp server Eng-Pool
    ipv6 nd other-config-flag
interface gigabitethernet 0/2
    ipv6 address Outside-Prefix ::2:0:0:0:1/64
    ipv6 dhcp server IT-Pool
    ipv6 nd other-config-flag
```

関連コマンド

コマンド	説明
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
domain-name	IR メッセージへの応答で SLAAC クライアントに提供されるドメイン名を設定します。
import	ASA がプレフィックス委任クライアント インターフェイスで DHCPv6 サーバから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
ipv6 address	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
ipv6 address dhcp	インターフェイスの DHCPv6 を使用してアドレスを取得します。
ipv6 dhcp client pd	委任されたプレフィックスを使用して、インターフェイスのアドレスを設定します。
ipv6 dhcp client pd hint	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
ipv6 dhcp pool	DHCPv6 ステートレス サーバを使用して、特定のインターフェイスで SLAAC クライアントに提供する情報を含むプールを作成します。
ipv6 dhcp server	DHCPv6 ステートレス サーバを有効にします。
network	サーバから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
nis address	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。
nis domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。

コマンド	説明
show ipv6 dhcp	DHCPv6 情報を表示します。
show ipv6 general-prefix	DHCPv6 プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示します。
sip address	IR メッセージへの応答で SLAAC クライアントに提供される SIP アドレスを設定します。
sip domain-name	IR メッセージへの応答で SLAAC クライアントに提供される SIP ドメイン名を設定します。
sntp address	IR メッセージへの応答で SLAAC クライアントに提供される SNTP アドレスを設定します。

dns server-group（グローバル）

DNS サーバ グループを作成して設定するには、グローバル コンフィギュレーション モードで **dns server-group** コマンドを使用します。特定の DNS サーバ グループを削除するには、このコマンドの **no** 形式を使用します。

(注) ASA では、機能に応じて DNS サーバの使用が限定的にサポートされます。たとえば、ほとんどのコマンドでは、IP アドレスを入力する必要があります。名前を使用できるのは、名前と IP アドレスを関連付けるように **name** コマンドを手動で設定し、**names** コマンドを使用して名前の使用をイネーブルにした場合だけです。

dns server -group *name*

no dns server-group

構文の説明

name	DNS サーバ グループの名前を指定します。ASA ルックアップのデフォルトのグループ 名は **DefaultDNS** です。

デフォルト

ASA のデフォルトのアクティブ サーバ グループは DefaultDNS です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

DNS 検索をイネーブルにするには、**dns domain-lookup** コマンドを使用します。DNS ルックアップをイネーブルにしないと、DNS サーバは使用されません。

ASA では、発信要求に **dns server-group DefaultDNS** サーバ グループを使用します。アクティブなサーバ グループは、**dns-group** コマンドを使用して変更できます。VPN トンネル グループ用他の目的のために他の DNS サーバ グループを設定できます。詳細については、**tunnel-group** コマンドを参照してください。

一部の ASA 機能では、ドメイン名で外部サーバにアクセスするために DNS サーバを使用する必要があります。たとえば、ボットネット トラフィック フィルタ機能では、ダイナミック データベース サーバにアクセスして、スタティック データベースのエントリを解決するために DNS サーバが必要です。さらに、Cisco Smart Software Licensing では、ライセンス機関のアドレスの解決に DNS が必要です。他の機能（**ping** コマンドや **traceroute** コマンドなど）では、ping や traceroute を実行する名前を入力できるため、ASA は DNS サーバと通信することで名前を解決できます。名前は、多くの SSL VPN コマンドおよび certificate コマンドでもサポートされます。また、アクセス ルールに完全修飾ドメイン名（FQDN）ネットワーク オブジェクトを使用するために、DNS サーバを設定する必要もあります。

例

次に、「DefaultDNS」という名前の DNS サーバ グループを設定する例を示します。

```
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# domain-name cisco.com
ciscoasa(config-dns-server-group)# name-server 192.168.10.10
ciscoasa(config-dns-server-group)# retries 5
ciscoasa(config-dns-server-group)# timeout 7
ciscoasa(config-dns-server-group)#
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
show running-config dns server-group	現在の実行中の DNS サーバ グループ コンフィギュレーションを表示します。

dns-id

参照 ID オブジェクトで cn-id を設定するには、*ca-reference-identity* モードで **dns-id** コマンドを使用します。dns-id を削除するには、このコマンドの **no** 形式を使用します。*ca-reference-identity* モードにアクセスするには、参照 ID オブジェクトを設定するための **crypto ca reference-identity** コマンドを入力します。

dns-id *value*

no dns-id *value*

構文の説明

value	各参照 ID の値。
dns-id	タイプ dNSName の subjectAltName エントリ。これは DNS ドメイン名です。DNS-ID 参照 ID では、アプリケーション サービスは特定されません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ca-reference-identity	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

参照 ID が作成されると、4 つの ID タイプと関連付けられた値を参照 ID に追加、または参照 ID から削除することができます。

参照 ID の **cn ID** と **dns ID** には、アプリケーション サービスを特定する情報を含めることができず、DNS ドメイン名を特定する情報が含まれている必要があります。

例

次に、syslog サーバの参照 ID を作成する例を示します。

```
ciscoasa(config)# crypto ca reference-identity syslogServer
ciscoasa(config-ca-ref-identity)# dns-id syslog1-bxb.cisco.com
ciscoasa(config-ca-ref-identity)# cn-id syslog1-bxb.cisco.com
```

関連コマンド

コマンド	説明
crypto ca reference-identity	参照 ID オブジェクトを設定します。
cn-id	参照 ID オブジェクトのコモン ネーム ID を設定します。
srv-id	参照 ID オブジェクトで SRV-ID 識別子を設定します。
uri-id	参照 ID オブジェクトの URI ID を設定します。
logging host	セキュアな接続のために参照 ID オブジェクトを使用できるロギング サーバを設定します。
call-home profile destination address http	安全な接続のために参照 ID オブジェクトを使用できる Smart Call Home サーバを設定します。

dns update

DNS ポーリング タイマーの有効期限を待機せずに、指定されたホスト名を解決する DNS ルックアップを開始するには、特権 EXEC モードで **dns update** コマンドを使用します。

dns update [**host** *fqdn_name*] [**timeout seconds** *seconds*]

構文の説明

host *fqdn_name*	DNS アップデートを実行するホストの完全修飾ドメイン名を指定します。
timeout seconds *seconds*	タイムアウトを秒単位で指定します。

デフォルト

デフォルトでは、タイムアウトは 30 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC モード	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、DNS ポーリング タイマーの有効期限を待機しないで、指定されたホスト名を解決する DNS ルックアップをすぐに開始します。オプションを指定せずに DNS アップデートを実行する場合、アクティブ化されたすべてのホスト グループと FQDN ホストが DNS ルックアップ用に選択されます。コマンドの実行が終了すると、ASA のコマンド プロンプトに [Done] と表示され、syslog メッセージが生成されます。

アップデート操作が開始すると、アップデート開始ログが作成されます。アップデート操作が終了するか、またはタイマーが期限切れになってから中断すると、別の syslog メッセージが生成されます。許可される未処理 DNS アップデート操作は 1 つのみです。

例

次に、DNS アップデートを実行する例を示します。

```
ciscoasa# dns update
ciscoasa# …
ciscoasa# [Done] dns update
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
dns server-group	DNS サーバ グループを設定できる DNS サーバ グループ モードを開始します。
show running-config dns-server group	既存の DNS サーバ グループ コンフィギュレーションを 1 つまたはすべて表示します。

domain-name (dns server-group)

未修飾のホスト名に追加するデフォルトのドメイン名を設定するには、dns server-group コンフィギュレーション モードで **domain-name** コマンドを使用します。ドメイン名を削除するには、このコマンドの **no** 形式を使用します。

domain-name *name*

no domain-name [*name*]

構文の説明

name	ドメイン名を最大 63 文字で設定します。

デフォルト

デフォルト ドメイン名は default.domain.invalid です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
DNS サーバ グループ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

ASA は、修飾子を持たない名前のサフィクスとして、ドメイン名を付加します。たとえば、ドメイン名を「example.com」に設定し、syslog サーバとして非修飾名「jupiter」を指定した場合は、ASA によって名前が修飾されて「jupiter.example.com」となります。

例

次に、ドメインを「dnsgroup1」に対して「example.com」に設定する例を示します。

```
ciscoasa(config)# dns server-group dnsgroup1
ciscoasa(config-dns-server-group)# domain-name example.com
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
dns server-group	DNS サーバ グループを設定できる DNS サーバ グループ コンフィギュレーション モードを開始します。

コマンド	説明
domain-name	デフォルトのドメイン名をグローバルに設定します。
show running-config dns-server group	現在の DNS サーバ グループ コンフィギュレーションを 1 つまたはすべて表示します。

domain-name（グローバル）

デフォルトのドメイン名を設定するには、グローバル コンフィギュレーション モードで **domain-name** コマンドを使用します。ドメイン名を削除するには、このコマンドの **no** 形式を使用します。

domain-name *name*

no domain-name [*name*]

構文の説明

name	ドメイン名を最大 63 文字で設定します。

デフォルト

デフォルト ドメイン名は default.domain.invalid です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASA は、修飾子を持たない名前のサフィクスとして、ドメイン名を付加します。たとえば、ドメイン名を「example.com」に設定し、syslog サーバとして非修飾名「jupiter」を指定した場合は、ASA によって名前が修飾されて「jupiter.example.com」となります。マルチ コンテキスト モードでは、システム実行スペース内だけではなく、各コンテキストに対してドメイン名を設定できます。

例

次に、ドメインを example.com に設定する例を示します。

```
ciscoasa(config)# domain-name example.com
```

関連コマンド

コマンド	説明
dns domain-lookup	ASA によるネーム ルックアップの実行をイネーブルにします。
dns name-server	ASA の DNS サーバを指定します。

コマンド	説明
hostname	ASA のホスト名を設定します。
show running-config domain-name	ドメイン名のコンフィギュレーションを表示します。

domain-name（IPv6 DHCP プール）

DHCPv6 サーバを設定するときにステートレス アドレス自動設定（SLAAC）クライアントにドメイン名を提供するには、IPv6 DHCP プール コンフィギュレーション モードで **domain-name** コマンドを使用します。ドメイン名を削除するには、このコマンドの **no** 形式を使用します。

domain-name *domain_name*

no domain-name *domain_name*

構文の説明

domain_name	ドメイン名を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
IPv6 DHCP プール コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

クライアントがプレフィックス委任機能とともに SLAAC を使用する場合、クライアントが情報要求（IR）パケットを ASA に送信するときに **IPv6 DHCP プール**内の情報（ドメイン名など）を提供するように ASA を設定できます。ASA は IR パケットのみを受け付け、アドレスをクライアントに割り当てません。DHCPv6 ステートレス サーバを設定するには、**ipv6 dhcp server** コマンドを使用します。サーバを有効にする場合は、**ipv6 dhcp プール**名を指定します。

プレフィックス委任を設定するには、**ipv6 dhcp client pd** コマンドを使用します。

この機能は、クラスタリングではサポートされていません。

例

次に、2 つの IPv6 DHCP プールを作成して、2 つのインターフェイスで DHCPv6 サーバを有効にする例を示します。

```
ipv6 dhcp pool Eng-Pool
    domain-name eng.example.com
    dns-server 2001:DB8:1::1
```

```
ipv6 dhcp pool IT-Pool
    domain-name it.example.com
    dns-server 2001:DB8:1::1
interface gigabitethernet 0/0
    ipv6 address dhcp setroute default
    ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
    ipv6 address Outside-Prefix ::1:0:0:0:1/64
    ipv6 dhcp server Eng-Pool
    ipv6 nd other-config-flag
interface gigabitethernet 0/2
    ipv6 address Outside-Prefix ::2:0:0:0:1/64
    ipv6 dhcp server IT-Pool
    ipv6 nd other-config-flag
```

関連コマンド

コマンド	説明
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
dns-server	IR メッセージへの応答で SLAAC クライアントに提供される DNS サーバを設定します。
import	ASA がプレフィックス委任クライアントインターフェイスで DHCPv6 サーバから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
ipv6 address	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
ipv6 address dhcp	インターフェイスの DHCPv6 を使用してアドレスを取得します。
ipv6 dhcp client pd	委任されたプレフィックスを使用して、インターフェイスのアドレスを設定します。
ipv6 dhcp client pd hint	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
ipv6 dhcp pool	DHCPv6 ステートレス サーバを使用して、特定のインターフェイスで SLAAC クライアントに提供する情報を含むプールを作成します。
ipv6 dhcp server	DHCPv6 ステートレス サーバを有効にします。
network	サーバから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
nis address	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。
nis domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。
show ipv6 dhcp	DHCPv6 情報を表示します。
show ipv6 general-prefix	DHCPv6 プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示します。

コマンド	説明
sip address	IR メッセージへの応答で SLAAC クライアントに提供される SIP アドレスを設定します。
sip domain-name	IR メッセージへの応答で SLAAC クライアントに提供される SIP ドメイン名を設定します。
sntp address	IR メッセージへの応答で SLAAC クライアントに提供される SNTP アドレスを設定します。

domain-password

IS-IS ルーティング ドメイン認証パスワードを設定するには、ルータ ISIS コンフィギュレーション モードで **domain-password** コマンドを使用します。パスワードをディセーブルにするには、このコマンドの **no** 形式を使用します。

domain-name *password* [**authenticate snp** {**validate** | **send-only**}]

no domain-name *password*

構文の説明

password	割り当てるパスワード。
authenticate snp	(任意) これを指定すると、システムは SNP PDU にパスワードを挿入するようになります。
validate	(任意) これを指定すると、システムはパスワードを SNP に挿入し、受け取ったパスワードを SNP で確認するようになります。
send-only	(任意) これを指定すると、システムは SNP へのパスワードの挿入だけは行うようになりますが、SNP での受け取ったパスワードの確認は行われません。このキーワードは、ソフトウェアのアップグレード中、移行をスムーズに行うために使用します。

デフォルト

ドメイン パスワードは指定されていません。また、レベル 2 ルーティング情報のやり取りを行うための認証はイネーブルにされていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ isis コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

このパスワードはプレーン テキストとしてやり取りされるため、この機能が提供するセキュリティは限定されています。

このパスワードは、レベル 2（エリア ルータ レベル）の PDU リンクステート パケット（LSP）、Complete Sequence Number PDU（CSNP）、および Partial Sequence Number PDU（PSNP）に挿入されます。

authenticate snp キーワードを指定して、**validate** または **send-only** キーワードを指定しなかった場合、IS-IS ルーティング プロトコルは SNP にパスワードを挿入しません。

例

次に、ルーティング ドメインに認証パスワードを割り当て、このパスワードを SNP に挿入し、システムが受け取った SNP で確認するように指定する例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# domain-password users2j45 authenticate snp validate
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。

コマンド	説明
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト(TLV)を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。

コマンド	説明
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

downgrade

ソフトウェア バージョンをダウングレードするには、グローバル コンフィギュレーション モードで **downgrade** コマンドを使用します。

downgrade [**/noconfirm**] *old_image_url old_config_url* [**activation-key** *old_key*]

構文の説明

activation-key *old_key*	（オプション）アクティベーション キーを復元する必要がある場合、古いアクティベーション キーを入力できます。
old_config_url	保存されている移行前のコンフィギュレーションへのパスを指定します（デフォルトでは、disk0 に保存されます）。
old_image_url	disk0、disk1、tftp、または smb で古いイメージへのパスを指定します。
/noconfirm	（任意）プロンプトを出さずにダウングレードします。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、次の機能を完了するためのショートカットです。

1. ブート イメージ コンフィギュレーションのクリア（**clear configure boot**）。
2. 古いイメージへのブート イメージの設定（**boot system**）。
3. （任意）新たなアクティベーション キーの入力（**activation-key**）。
4. 実行コンフィギュレーションのスタートアップ コンフィギュレーションへの保存（**write memory**）。これにより、BOOT 環境変数を古いイメージに設定します。このため、リロードすると古いイメージがロードされます。
5. 古いコンフィギュレーションのスタートアップ コンフィギュレーションへのコピー（**copy** *old_config_url* **startup-config**）。
6. リロード（**reload**）。

例

次に、確認なしでダウングレードする例を示します。

```
ciscoasa(config)# downgrade /noconfirm disk0:/asa821-k8.bin disk0:/8_2_1_0_startup_cfg.sav
```

関連コマンド

コマンド	説明
activation-key	アクティベーション キーを入力します。
boot system	ブートするイメージを設定します。
clear configure boot	ブート イメージ コンフィギュレーションをクリアします。
copy startup-config	コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

download-max-size

(注) **download-max-size** コマンドは機能しません。使用しないでください。ただし、実行コンフィギュレーションでは表示される場合があり、CLI で使用できます。

ダウンロードするオブジェクトの最大許容サイズを指定するには、グループ ポリシー webvpn コンフィギュレーション モードで **download-max-size** コマンドを使用します。このオブジェクトをコンフィギュレーションから削除するには、このコマンドの **no** バージョンを使用します。

download-max-size *size*

no download-max-size

構文の説明

size	ダウンロードするオブジェクトの最大許容サイズを指定します。指定できる範囲は 0 ～ 2147483647 です。

デフォルト

デフォルトのサイズは 2147483647 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

関連コマンド

コマンド	説明
post-max-size	ポストするオブジェクトの最大サイズを指定します。
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。webvpn モードを開始して、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	グローバル コンフィギュレーション モードで使用します。WebVPN のグローバル設定を設定できます。

drop

match コマンドまたは **class** コマンドに一致するすべてのパケットをドロップするには、一致またはクラス コンフィギュレーション モードで、**drop** コマンドを使用します。このアクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

drop [**send-protocol-error**] [**log**]

no drop [**send-protocol-error**] [**log**]

構文の説明

ログ	一致をログに記録します。syslog メッセージの番号は、アプリケーションによって異なります。
send-protocol-error	プロトコル エラー メッセージを送信します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
一致コンフィギュレーションおよびクラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

モジュラ ポリシー フレームワークを使用する場合は、一致またはクラス コンフィギュレーション モードで **drop** コマンドを使用して、**match** コマンドまたはクラス マップと一致するパケットをドロップします。この drop アクションは、アプリケーション トラフィックのインスペクション ポリシー マップ（**policy-map type inspect** コマンド）で有効です。ただし、すべてのアプリケーションでこのアクションが許可されているわけではありません。

インスペクション ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。インスペクション ポリシー マップで使用できる実際のコマンドは、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力してアプリケーション トラフィックを識別（**class** コマンドは **match** コマンドを含む既存の **class-map type inspect** コマンドを指す）した後は、**drop** コマンドを入力して **match** コマンドまたは **class** コマンドと一致するすべてのパケットをドロップできます。

パケットをドロップすると、インスペクション ポリシー マップで以降のアクションは実行されません。たとえば、最初のアクションでパケットをドロップした場合は、それ以降、**match** コマンドまたは **class** コマンドと一致しません。最初のアクションがパケットのロギングである場合は、パケットのドロップなどの別のアクションが発生する可能性があります。同じ **match** コマンドまたは **class** コマンドに対して **drop** アクションと **log** アクションの両方を設定できます。その場合、パケットは所定の一致箇所でドロップされる前にロギングされます。

レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション インスペクションをイネーブルにする場合、このアクションを含むインスペクション ポリシー マップをイネーブルにできます。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map は、インスペクション ポリシー マップの名前です。

例

次に、パケットをドロップし、HTTP トラフィック クラス マップと一致した場合にログを送信する例を示します。同じパケットが 2 番めの **match** コマンドにも一致する場合、そのパケットはすでにドロップされているため、処理されません。

```
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# drop log
ciscoasa(config-pmap-c)# match req-resp content-type mismatch
ciscoasa(config-pmap-c)# reset log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

drop-connection

モジュラ ポリシー フレームワークを使用する場合は、一致またはクラス コンフィギュレーション モードで **drop-connection** コマンドを使用してパケットをドロップし、**match** コマンドまたはクラス マップと一致するトラフィックの接続を閉じます。このアクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

drop-connection [**send-protocol-error**] [**log**]

no drop-connection [**send-protocol-error**] [**log**]

構文の説明

send-protocol-error	プロトコル エラー メッセージを送信します。
ログ	一致をログに記録します。システム ログ メッセージの番号は、アプリケーションによって異なります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
一致コンフィギュレーションおよびクラス コンフィギュレーション	• **対応**	• **対応**	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

接続は、ASA 上の接続データベースから削除されます。接続がドロップされた ASA に入る後続パケットはすべて廃棄されます。この drop-connection アクションは、アプリケーション トラフィックのインスペクション ポリシー マップ（**policy-map type inspect** コマンド）で有効です。ただし、すべてのアプリケーションでこのアクションが許可されているわけではありません。インスペクション ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。インスペクション ポリシー マップで使用できる実際のコマンドは、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力してアプリケーション トラフィックを識別（**class** コマンドは **match** コマンドを含む既存の **class-map type inspect** コマンドを指す）した後は、**drop-connection** コマンドを入力してパケットをドロップし、**match** コマンドまたは **class** コマンドと一致するトラフィックの接続を閉じます。

パケットをドロップするか、または接続を閉じると、インスペクション ポリシー マップで以降のアクションは実行されません。たとえば、最初のアクションがパケットをドロップし接続を閉じることである場合、それ以降は **match** コマンドまたは **class** コマンドに対応しません。最初のアクションがパケットのロギングである場合は、パケットのドロップなどの別のアクションが発生する可能性があります。同じ **match** コマンドまたは **class** コマンドに対して **drop-connection** アクションと **log** アクションの両方を設定できます。その場合、パケットは所定の一致箇所でドロップされる前にロギングされます。

レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション インスペクションをイネーブルにすると、このアクションを含むインスペクション ポリシー マップをイネーブルにできます。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map は、インスペクション ポリシー マップの名前です。

例

次に、パケットをドロップし、接続を閉じて、http-traffic クラス マップと一致した場合にログを送信する例を示します。同じパケットが 2 番めの **match** コマンドにも一致する場合、そのパケットはすでにドロップされているため、処理されません。

```
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# drop-connection log
ciscoasa(config-pmap-c)# match req-resp content-type mismatch
ciscoasa(config-pmap-c)# reset log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

dtls port

DTLS 接続用のポートを指定するには、webvpn コンフィギュレーション モードで **dtls port** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

dtls port *number*

no dtls port *number*

構文の説明

number	UDP ポート番号（1 ～ 65535）。

デフォルト

デフォルトのポート番号は 443 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、DTLS を使用する SSL VPN 接続用の UDP ポートを指定します。

DTLS により、一部の SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

例

次に、webvpn コンフィギュレーション モードを開始し、DTLS 用にポート 444 を指定する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# dtls port 444
```

関連コマンド

コマンド	説明
dtls enable	インターフェイスに対して DTLS をイネーブルにします。
svc dtls	SSL VPN 接続を確立するグループまたはユーザに対して、DTLS をイネーブルにします。
vpn-tunnel-protocol	ASA がリモート アクセス用に許可する VPN プロトコル（SSL を含む）を指定します。

duplex

銅線イーサネット インターフェイス（RJ-45）のデュプレックス方式を設定するには、インターフェイス コンフィギュレーション モードで **duplex** コマンドを使用します。デュプレックス設定をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

duplex {**auto** | **full** | **half**}

no duplex

構文の説明

[auto]	デュプレックス モードを自動検出します。
full	デュプレックス モードを全二重に設定します。
half	デュプレックス モードを半二重に設定します。

デフォルト

デフォルトは auto です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**interface** コマンドのキーワードからインターフェイス コンフィギュレーション モード コマンドに移されました。

使用上のガイドライン

デュプレックス モードは、物理インターフェイス上にだけ設定します。

duplex コマンドは、ファイバ メディアでは使用できません。

ネットワークで自動検出がサポートされていない場合は、デュプレックス モードを特定の値に設定します。

ASA 5500 シリーズの RJ-45 インターフェイスでは、デフォルトのオートネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。

PoE ポート上でデュプレックス方式を **auto** 以外に設定した場合は、IEEE 802.3af をサポートしない Cisco IP Phone およびシスコ ワイヤレス アクセス ポイントは検出されず、電源が供給されません。

例

次に、デュプレックス モードを全二重に設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# speed 1000
ciscoasa(config-if)# duplex full
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

関連コマンド

コマンド	説明
clear configure interface	インターフェイスのコンフィギュレーションをすべてクリアします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。
show running-config interface	インターフェイス コンフィギュレーションを表示します。
speed	インターフェイスの速度を設定します。

dynamic-access-policy-config

DAP レコードとそれに関連付けられたアクセス ポリシー属性を設定するには、グローバル コンフィギュレーション モードで **dynamic-access-policy-config** コマンドを使用します。既存の DAP コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

dynamic-access-policy-config *name* | *activate*

no dynamic-access-policy-config

構文の説明

activate	DAP 選択コンフィギュレーション ファイルをアクティブ化します。
name	DAP レコードの名前を指定します。名前は 64 文字以内で指定できます。スペースを含めることはできません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション(name)	• 対応	• 対応	• 対応	• 対応	—
特権 EXEC(activate)	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

グローバル コンフィギュレーション モードで **dynamic-access-policy-config** コマンドを使用して、1 つまたは複数の DAP レコードを作成します。DAP 選択コンフィギュレーション ファイルをアクティブにするには、*activate* 引数を指定して **dynamic-access-policy-config** コマンドを使用します。

このコマンドを使用するには、ダイナミック アクセス ポリシー レコード モードを開始します。このモードでは、指定した DAP レコードの属性を設定できます。ダイナミック アクセス ポリシー レコード モードで使用できるコマンドは、次のとおりです。

- **アクション**
- **説明**
- **network-acl**

- **priority**
- **user-message**
- **webvpn**

例

次に、user1 という名前の DAP レコードを設定する例を示します。

```
ciscoasa(config)# dynamic-access-policy-config user1
ciscoasa(config-dynamic-access-policy-record)#
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードにアクセス ポリシー属性を入力します。
show running-config dynamic-access-policy-record	すべての DAP レコードまたは指定した DAP レコードの実行コンフィギュレーションを表示します。

dynamic-access-policy-record

DAP レコードを作成してアクセス ポリシー属性を入力するには、グローバル コンフィギュレーション モードで **dynamic-access-policy-record** コマンドを使用します。既存の DAP レコードを削除するには、このコマンドの **no** 形式を使用します。

dynamic-access-policy-record *name*

no dynamic-access-policy-record *name*

構文の説明

name	DAP レコードの名前を指定します。名前は 64 文字以内で指定できます。スペースを含めることはできません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

グローバル コンフィギュレーション モードで **dynamic-access-policy-record** コマンドを使用して、1 つまたは複数の DAP レコードを作成します。このコマンドを使用するには、ダイナミック アクセス ポリシー レコード モードを開始します。このモードでは、指定した DAP レコードの属性を設定できます。ダイナミック アクセス ポリシー レコード モードで使用できるコマンドは、次のとおりです。

- **action**（**continue**、**terminate**、または **quarantine**）
- **説明**
- **network-acl**
- **priority**
- **user-message**
- **webvpn**

例

次に、Finance という名前の DAP レコードを作成する例を示します。

```
ciscoasa(config)# dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)#
```

関連コマンド

コマンド	説明
clear config dynamic-access-policy-record	すべての DAP レコードまたは指定された DAP レコードを削除します。
dynamic-access-policy-config url	DAP 選択コンフィギュレーション ファイルを設定します。
show running-config dynamic-access-policy-record	すべての DAP レコードまたは指定した DAP レコードの実行コンフィギュレーションを表示します。

dynamic-authorization

AAA サーバ グループの RADIUS の動的認可（認可変更）サービスをイネーブルにするには、AAA サーバ グループ コンフィギュレーション モードで **dynamic-authorization** コマンドを使用します。動的認可をディセーブルにするには、このコマンドの **no** 形式を使用します。

dynamic-authorization [**port** *number*]

no dynamic-authorization [**port** *number*]

構文の説明

port *number*	（オプション）ASA で動的認可ポートを指定します。指定できる範囲は、1024 ～ 65535 です。

デフォルト

デフォルトのリスニング ポートは 1700 です。デフォルトでは、dynamic-authorization はイネーブルになりません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
aaa サーバ グループ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、ISE 認可変更（CoA）のために RADIUS サーバ グループを設定するために使用します。定義されると、対応する RADIUS サーバ グループが CoA 通知用に登録され、ASA は ISE からの CoA ポリシー更新用ポートをリッスンします。

ISE Change of Authorization（CoA）機能は、認証、認可、およびアカウンティング（AAA）セッションの属性を、セッション確立後に変更するためのメカニズムを提供します。AAA のユーザまたはユーザ グループのポリシーを変更すると、ISE から ASA へ CoA パケットを直接送信して認証を再初期化し、新しいポリシーを適用できます。インライン ポスチャ実施ポイント（IPEP）で、ASA と確立された各 VPN セッションのアクセス コントロール リスト（ACL）を適用する必要がなくなりました。

エンド ユーザが VPN 接続を要求すると、ASA はユーザに対して ISE 認証を実行し、ネットワークへの制限付きアクセスを提供する ACL を受領します。アカウンティング開始メッセージが ISE に送信され、セッションが登録されます。ポスチャ アセスメントが NAC エージェントと ISE 間で直接行われます。このプロセスは、ASA に透過的です。ISE が CoA の「ポリシー プッシュ」を介して ASA にポリシーの更新を送信します。これにより、ネットワーク アクセス権限を高める新しいユーザ ACL が識別されます。後続の CoA 更新を介し、接続のライフタイム中に追加のポリシー評価が ASA に透過的に行われる場合があります。

例

次の例は、ISE サーバ グループに、動的認可（CoA）のアップデートと時間ごとの定期的なアカウンティングを設定する方法を示しています。ISE によるパスワード認証を設定するトンネル グループ設定が含まれています。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

次に、ISE でローカル証明書の検証と認可用のトンネル グループを設定する例を示します。この場合、サーバ グループは認証用に使用されないため、**authorize-only** コマンドをサーバ グループ コンフィギュレーションに組み込みます。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

関連コマンド

コマンド	説明
authorize-only	RADIUS サーバ グループ用の認可専用モードをイネーブルにします。
interim-accounting-update	RADIUS 中間アカウンティング アップデート メッセージの生成をイネーブルにします。
without-csd	特定のトンネル グループに行われる接続のホストスキャン処理をオフに切り替えます。

dynamic-filter ambiguous-is-black

ボットネット トラフィック フィルタのグレイリストに記載されているトラフィックを、ドロップするためにブラックリストに記載されているトラフィックとして扱うには、グローバル コンフィギュレーション モードで **dynamic-filter ambiguous-is-black** コマンドを使用します。グレイリストに記載されているトラフィックを許可するには、このコマンドの **no** 形式を使用します。

dynamic-filter ambiguous-is-black

no dynamic-filter ambiguous-is-black

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが追加されました。

使用上のガイドライン

dynamic-filter enable コマンドを設定してから **dynamic-filter drop blacklist** コマンドを設定すると、このコマンドでは、グレイリストに記載されているトラフィックが、ドロップするためにブラックリストに記載されているトラフィックとして扱われます。このコマンドをイネーブルにしない場合、グレーリストに記載されているトラフィックはドロップされません。

複数のドメイン名にあいまいなアドレスが関連付けられていますが、これらのドメイン名がすべてブラックリストに記載されてるわけではありません。これらのアドレスはグレーリストに記載されます。

例

次に、外部インターフェイスでポート 80 のすべてのトラフィックをモニタし、ブラックリストおよびグレイリストに記載されているトラフィックを脅威レベル moderate 以上でドロップする例を示します。

```
ciscoasa(config)# access-list dynamic-filter_acl extended permit tcp any any eq 80
ciscoasa(config)# dynamic-filter enable interface outside classify-list dynamic-filter_acl
ciscoasa(config)# dynamic-filter drop blacklist interface outside
ciscoasa(config)# dynamic-filter ambiguous-is-black
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。

コマンド	説明
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

dynamic-filter blacklist

ボットネット トラフィック フィルタのブラックリストを編集するには、グローバル コンフィギュレーション モードで **dynamic-filter blacklist** コマンドを使用します。ブラックリストを削除するには、このコマンドの **no** 形式を使用します。

dynamic-filter blacklist

no dynamic-filter blacklist

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

ダイナミック フィルタ ブラックリスト コンフィギュレーション モードを開始した後に、**address** コマンドおよび **name** コマンドを使用して、ブラックリストで信用できない名前としてタグ付けするドメイン名または IP アドレス（ホストまたはサブネット）を手動で入力できます。また、syslog メッセージおよびレポートで、ダイナミック ブラックリストおよびホワイトリストの両方に記載されている名前または IP アドレスがホワイトリスト アドレスとしてのみ識別されるように、ホワイトリストに名前や IP アドレスを入力できます（**dynamic-filter whitelist** コマンドを参照）。アドレスがダイナミック ブラックリストに記載されていない場合でも、ホワイトリストに記載されたアドレスの syslog メッセージは表示されます。

スタティック ブラックリスト エントリは、常に Very High 脅威レベルに指定されます。

スタティック データベースにドメイン名を追加した場合、ASA は、1 分間待機してからそのドメイン名の DNS 要求を送信し、ドメイン名と IP アドレスの組を *DNS ホスト キャッシュ*に追加します（このアクションはバックグラウンド プロセスで、ASA の設定の続行に影響しません）。ボットネット トラフィック フィルタ スヌーピングによる DNS パケット インスペクションもイネーブルにすることを推奨します（**inspect dns dynamic-filter-snooping** コマンドを参照してください）。次の場合、ASAは、通常の DNS lookup ではなく、ボットネット トラフィック フィルタ スヌーピングを使用してスタティック ブラックリストのドメイン名を解決します。

- ASA DNS サーバが使用できない。
- ASA が通常の DNS 要求を送信する前の 1 分間の待機期間中に接続が開始された。

DNS スヌーピングを使用すると、感染ホストがスタティック データベースに記載されている名前に対する DNS 要求を送信したときに、ASA がドメイン名と関連付けられている IP アドレスを DNS パケット内から検出し、その名前と IP アドレスを DNS 逆ルックアップ キャッシュに追加します。

スタティック データベースを使用すると、ブラックリストに記載するドメイン名または IP アドレスを使用してダイナミック データベースを増強できます。

ボットネット トラフィック フィルタ スヌーピングをイネーブルにせず、上記の状況のいずれかが発生した場合、このトラフィックは、ボットネット トラフィック フィルタでモニタされません。

(注) このコマンドは、ASA が DNS サーバを使用することが必須です。**dns domain-lookup** コマンドおよび **dns server-group** コマンドを参照してください。

例

次に、ブラックリストおよびホワイトリストのエントリを作成する例を示します。

```
ciscoasa(config)# dynamic-filter blacklist
ciscoasa(config-llist)# name bad1.example.com
ciscoasa(config-llist)# name bad2.example.com
ciscoasa(config-llist)# address 10.1.1.1 255.255.255.0

ciscoasa(config-llist)# dynamic-filter whitelist
ciscoasa(config-llist)# name good.example.com
ciscoasa(config-llist)# name great.example.com
ciscoasa(config-llist)# name awesome.example.com
ciscoasa(config-llist)# address 10.1.1.2 255.255.255.255
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。

コマンド	説明
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

dynamic-filter database fetch

ボットネット トラフィック フィルタのダイナミック データベースのダウンロードをテストするには、特権 EXEC モードで **dynamic-filter database fetch** コマンドを使用します。

dynamic-filter database fetch

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

実際のデータベースは ASA で保存されません。ダウンロードされてから廃棄されます。このコマンドは、テスト用にのみ使用してください。

例

次に、ダイナミック データベースのダウンロードをテストする例を示します。

```
ciscoasa# dynamic-filter database fetch
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。

コマンド	説明
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。

コマンド	説明
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

dynamic-filter database find

ボットネット トラフィック フィルタのダイナミック データベースにドメイン名または IP アドレスが含まれているかどうかを確認するには、特権 EXEC モードで **dynamic-filter database find** コマンドを使用します。

dynamic-filter database find *string*

構文の説明

string	*string* には、ドメイン名または IP アドレスのすべてまたは一部を、3 文字以上の検索文字列で指定できます。データベース検索では、正規表現はサポートされません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

一致する項目が複数見つかった場合は、最初の 2 つの項目が表示されます。一致する項目を絞り込むために詳細な検索条件を指定するには、より長い文字列を入力します。

例

次に、文字列「example.com」で検索する例を示します。この例では、一致する項目が 1 つ見つかります。

```
ciscoasa# dynamic-filter database find bad.example.com

   bad.example.com
Found 1 matches
```

次に、文字列「bad」で検索する例を示します。この例では、一致する項目が 3 つ以上見つかります。

```
ciscoasa# dynamic-filter database find bad

   bad.example.com
   bad.example.net
Found more than 2 matches, enter a more specific string to find an exact
match
```

関連コマンド

コマンド	説明
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。

コマンド	説明
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

dynamic-filter database purge

実行メモリからボットネット トラフィック フィルタのダイナミック データベースを手動で削除するには、特権 EXEC モードで **dynamic-filter database purge** コマンドを使用します。

dynamic-filter database purge

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

データベース ファイルは実行メモリに保存されます。フラッシュ メモリには保存されません。データベースを削除する必要がある場合、**dynamic-filter database purge** コマンドを使用します。

データベース ファイルを消去するには、**no dynamic-filter use-database** コマンドを使用して、データベースの使用をディセーブルにしておく必要があります。

例

次に、データベースの使用をディセーブルにしてからデータベースを消去する例を示します。

```
ciscoasa(config)# no dynamic-filter use-database
ciscoasa(config)# dynamic-filter database purge
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。

コマンド	説明
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。

コマンド	説明
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

dynamic-filter drop blacklist

ボットネット トラフィック フィルタを使用して、ブラックリストに記載されたトラフィックを自動的にドロップするには、グローバル コンフィギュレーション モードで **dynamic-filter drop blacklist** コマンドを使用します。自動ドロップをディセーブルにするには、このコマンドの **no** 形式を使用します。

dynamic-filter drop blacklist [**interface** *name*] [**action-classify-list** *subset_access_list*] [**threat-level** {**eq** *level* | **range** *min max*}]

no dynamic-filter drop blacklist [**interface** *name*] [**action-classify-list** *subset_access_list*] [**threat-level** {**eq** *level* | **range** *min max*}]

構文の説明

action-classify-list *sub_access_list*	(任意) ドロップするトラフィックのサブセットを指定します。アクセス リストの作成については、**access-list extended** コマンドを参照してください。 ドロップされるトラフィックは、常に **dynamic-filter enable** コマンドで指定したモニタ トラフィックと同じか、またはモニタ トラフィックのサブセットである必要があります。たとえば、**dynamic-filter enable** コマンドに対してアクセス リストを指定し、このコマンドに対して **action-classify-list** を指定する場合、**dynamic-filter enable** アクセス リストのサブセットになります。
interface *name*	(任意) 特定のインターフェイスへのモニタリングを制限します。ドロップされるトラフィックは、常に **dynamic-filter enable** コマンドで指定したモニタ トラフィックと同じか、またはモニタ トラフィックのサブセットである必要があります。 インターフェイス固有のコマンドは、グローバル コマンドより優先されます。
threat-level {***eq*** *level* | ***range*** *min max*}	(任意) 脅威レベルの設定によってドロップされるトラフィックを制限します。明示的に脅威レベルを設定しない場合、使用されるレベルは、**threat-level range moderate very-high** です。 **(注)** デフォルト設定を変更する確固たる理由がない限り、デフォルト設定を使用することを強くお勧めします。 *level*、*min*、および *max* の各オプションは次のとおりです。 • **very-low** • **low** • **moderate** • **high** • **very-high** **(注)** スタティック ブラックリスト エントリは、常に Very High 脅威レベルに指定されます。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

デフォルトの脅威レベルは **threat-level range moderate very-high** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが追加されました。

使用上のガイドライン

最初に、ドロップするトラフィックに対して **dynamic-filter enable** コマンドを設定するようにしてください。ドロップされるトラフィックは、常に、モニタされるトラフィックと同じであるか、またはこのトラフィックのサブセットである必要があります。

このコマンドは、各インターフェイスおよびグローバル ポリシーに対して複数回入力できます。所定のインターフェイス/グローバル ポリシーに対する複数のコマンドで、重複トラフィックを指定しないでください。コマンド照合順を完全に制御することはできないので、重複トラフィックは、照合されたコマンドを把握できないことになります。たとえば、所定のインターフェイスに対してすべてのトラフィックに一致するコマンド（**action-classify-list** キーワードを使用しない）と **action-classify-list** キーワードを使用するコマンドの両方を指定しないでください。この場合、トラフィックと **action-classify-list** キーワードを使用するコマンドとの照合が行われないことがあります。同様に、**action-classify-list** キーワードを使用する複数のコマンドを指定する場合、アクセス リストが固有であり、ネットワークが重複していないことを確認してください。

例

次に、外部インターフェイスの 80 番ポートのトラフィックをすべてモニタし、脅威レベルが moderate 以上のトラフィックをドロップする例を示します。

```
ciscoasa(config)# access-list dynamic-filter_acl extended permit tcp any any eq 80
ciscoasa(config)# dynamic-filter enable interface outside classify-list dynamic-filter_acl
ciscoasa(config)# dynamic-filter drop blacklist interface outside
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。

コマンド	説明
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

dynamic-filter enable

ボットネット トラフィック フィルタをイネーブルにするには、グローバル コンフィギュレーション モードで **dynamic-filter enable** コマンドを使用します。ボットネット トラフィック フィルタをディセーブルにするには、このコマンドの **no** 形式を使用します。

dynamic-filter enable [**interface** *name*] [**classify-list** *access_list*]

no dynamic-filter enable [**interface** *name*] [**classify-list** *access_list*]

構文の説明

classify-list *access_list*	拡張アクセス リストを使用してモニタするトラフィックを指定します（**access-list extended** コマンドを参照）。アクセス リストを作成しない場合、デフォルトでは、すべてのトラフィックをモニタします。
interface *name*	特定のインターフェイスへのモニタリングを制限します。

デフォルト

デフォルトでは、ボットネット トラフィック フィルタはディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

ボットネット トラフィック フィルタは、各初期接続パケットの送信元 IP アドレスおよび宛先 IP アドレスを、ダイナミック データベース、スタティック データベース、DNS 逆ルックアップ キャッシュ、および DNS ホスト キャッシュの IP アドレスと比較し、syslog メッセージを送信するか、または一致するトラフィックをドロップします。

マルウェアとは、知らないうちにホストにインストールされている悪意のあるソフトウェアです。個人情報（パスワード、クレジット カード番号、キー ストローク、または独自データ）の送信などのネットワーク アクティビティを試みるマルウェアは、マルウェアが既知の不正な IP アドレスへの接続を開始したときにボットネット トラフィック フィルタによって検出できます。Botnet Traffic Filter は、悪意のある既知のドメイン名および IP アドレスを含む動的データベースと、着信接続および発信接続とを照合して、疑わしいアクティビティをすべてログに記録します。また、ローカルの「ブラックリスト」または「ホワイトリスト」に IP アドレスやドメイン名を入力して、スタティック データベースでダイナミック データベースを補完できます。

DNS スヌーピングは個別にイネーブルになります(**inspect dns dynamic-filter-snoop** コマンドを参照)。一般的に、Botnet Traffic Filter を最大限に利用するには、DNS スヌーピングをイネーブルにする必要がありますが、必要に応じて、Botnet Traffic Filter のロギングだけを単独で使用できます。ダイナミック データベースに DNS スヌーピングが設定されていない場合、ボットネット トラフィック フィルタでは、スタティック データベースのエントリとダイナミック データベースの IP アドレスだけが使用されます。ダイナミック データベースのドメイン名は使用されません。

ボットネット トラフィック フィルタのアドレス カテゴリ

ボットネット トラフィック フィルタのモニタ対象のアドレスは次のとおりです。

- 既知のマルウェア アドレス:これらのアドレスは、「ブラックリスト」に記載されます。
- 既知の許可アドレス:これらのアドレスは、「ホワイトリスト」に記載されます。
- あいまいなアドレス:ブラックリストに記載されていないドメイン名を 1 つ以上含む複数のドメイン名に関連付けられているアドレス。これらのアドレスは「グレーリスト」に記載されます。
- リストに記載されていないアドレス:どのリストにも記載されていない不明アドレス。

既知のアドレスに対するボットネット トラフィック フィルタのアクション

dynamic-filter enable コマンドを使用して、不審なアクティビティをロギングするようボットネット トラフィック フィルタを設定できます。また、任意で、**dynamic-filter drop blacklist** コマンドを使用して、不審なトラフィックを自動的にブロックするようボットネット トラフィック フィルタを設定できます。

リストに記載されていないアドレスについては、syslog メッセージは生成されません。ただし、ブラックリスト、ホワイトリスト、およびグレイリストに記載されているアドレスについては、タイプ別の syslog メッセージが生成されます。ボットネット トラフィック フィルタでは、338*nnn* という番号が付いた詳細な syslog メッセージが生成されます。メッセージでは、着信接続と発信接続、ブラックリスト アドレス、ホワイトリスト アドレス、またはグレイリスト アドレス、およびその他の多数の変数が区別されます(グレイリストには、ブラックリストに記載されていないドメイン名を 1 つ以上含む複数のドメイン名に関連付けられているアドレスが含まれています)。

syslog メッセージの詳細については、syslog メッセージ ガイドを参照してください。

デバイス サポート

ボットネット トラフィック フィルタを有効にできるデバイス モデルは次のとおりです。

- ASA 5505
- ASA 5510、5520、5540、5550
- ASA 5512-X、5515-X、5525-X、5545-X、5555-X
- ASA 5580
- ASA 5585-X
- ASASM

例

次に、外部インターフェイスの 80 番ポートのトラフィックをすべてモニタし、脅威レベルが moderate 以上のトラフィックをドロップする例を示します。

```
ciscoasa(config)# access-list dynamic-filter_acl extended permit tcp any any eq 80
ciscoasa(config)# dynamic-filter enable interface outside classify-list dynamic-filter_acl
ciscoasa(config)# dynamic-filter drop blacklist interface outside
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。

コマンド	説明
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

dynamic-filter updater-client enable

ボットネット トラフィック フィルタについて、シスコの更新サーバからのダイナミック データベースのダウンロードをイネーブルにするには、グローバル コンフィギュレーション モードで **dynamic-filter updater-client enable** コマンドを使用します。ダイナミック データベースのダウンロードをディセーブルにするには、このコマンドの **no** 形式を使用します。

dynamic-filter updater-client enable

no dynamic-filter updater-client enable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、ダウンロードはディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

ASA にデータベースをまだインストールしていない場合は、約 2 分後にデータベースが適応型セキュリティ アプライアンスにダウンロードされます。アップデート サーバは、将来のアップデートのために ASA がサーバにポーリングする頻度を決定します（通常は 1 時間ごと）。

ボットネット トラフィック フィルタでは、Cisco アップデート サーバからダイナミック データベースの定期アップデートを受け取ることができます。

このデータベースには、数千もの既知の不正なドメイン名と IP アドレスが含まれています。DNS 応答のドメイン名とダイナミック データベースのドメイン名が一致した場合、ボットネット トラフィック フィルタは、このドメイン名と IP アドレスを *DNS 逆ルックアップ キャッシュ*に追加します。感染したホストがマルウェア サイトの IP アドレスへの接続を開始すると、ASA によって、この不審なアクティビティに関する syslog メッセージ情報が送信されます。

データベースを使用するには、ASA 用のドメイン ネーム サーバを設定して、適応型セキュリティ アプライアンスが URL にアクセスできるようにしてください。ダイナミック データベースでドメイン名を使用するには、DNS パケット インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにする必要があります。ASA は、ドメイン名とそれに関連付けられている IP アドレスを DNS パケット内から検出します。

場合によっては、IP アドレス自体がダイナミック データベースに入力され、ボットネット トラフィック フィルタは DNS 要求を検査せずに、その IP アドレスへのすべてのトラフィックをログに記録します。

データベース ファイルは実行メモリに保存されます。フラッシュ メモリには保存されません。データベースを削除する必要がある場合は、**dynamic-filter database purge** コマンドを使用します。

(注) このコマンドは、ASA が DNS サーバを使用することが必須です。**dns domain-lookup** コマンドおよび **dns server-group** コマンドを参照してください。

例

次のマルチ モードの例では、ダイナミック データベースのダウンロードと、context1 および context2 でのデータベースの使用をイネーブルにします。

```
ciscoasa(config)# dynamic-filter updater-client enable
ciscoasa(config)# changeto context context1
ciscoasa/context1(config)# dynamic-filter use-database
ciscoasa/context1(config)# changeto context context2
ciscoasa/context2(config)# dynamic-filter use-database
```

次のシングル モードの例では、ダイナミック データベースのダウンロードおよび使用をイネーブルにします。

```
ciscoasa(config)# dynamic-filter updater-client enable
ciscoasa(config)# dynamic-filter use-database
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns name-server	ASA の DNS サーバを指定します。
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。

コマンド	説明
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

dynamic-filter use-database

ボットネット トラフィック フィルタのダイナミック データベースの使用をイネーブルにするには、グローバル コンフィギュレーション モードで **dynamic-filter use-database** コマンドを使用します。ダイナミック データベースの使用をディセーブルにするには、このコマンドの **no** 形式を使用します。

dynamic-filter use-database

no dynamic-filter use-database

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、データベースの使用はディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

ダウンロードされたデータベースのディセーブル化は、マルチ コンテキスト モードでデータベースの使用をコンテキストごとに設定できるようにする場合に有用です。ダイナミック データベースのダウンロードのイネーブル化については、**dynamic-filter updater-client enable** コマンドを参照してください。

例

次のマルチ モードの例では、ダイナミック データベースのダウンロードと、context1 および context2 でのデータベースの使用をイネーブルにします。

```
ciscoasa(config)# dynamic-filter updater-client enable
ciscoasa(config)# changeto context context1
ciscoasa/context1(config)# dynamic-filter use-database
ciscoasa/context1(config)# changeto context context2
ciscoasa/context2(config)# dynamic-filter use-database
```

次のシングル モードの例では、ダイナミック データベースのダウンロードおよび使用をイネーブルにします。

```
ciscoasa(config)# dynamic-filter updater-client enable
ciscoasa(config)# dynamic-filter use-database
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。

コマンド	説明
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

dynamic-filter whitelist

ボットネット トラフィック フィルタのホワイトリストを編集するには、グローバル コンフィギュレーション モードで **dynamic-filter whitelist** コマンドを使用します。ホワイトリストを削除するには、このコマンドの **no** 形式を使用します。

dynamic-filter whitelist

no dynamic-filter whitelist

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

スタティック データベースを使用すると、ホワイトリストに記載するドメイン名または IP アドレスを使用してダイナミック データベースを増強できます。ダイナミック フィルタ ホワイトリスト コンフィギュレーション モードを開始した後に、**address** コマンドおよび **name** コマンドを使用して、ホワイトリストで信用できる名前としてタグ付けするドメイン名または IP アドレス（ホストまたはサブネット）を手動で入力できます。ダイナミック ブラックリストとスタティック ホワイトリストの両方に記載された名前やアドレスは、syslog メッセージおよびレポートでは、ホワイトリスト アドレスとしてのみ示されます。アドレスがダイナミック ブラックリストに記載されていない場合でも、ホワイトリストに記載されたアドレスの syslog メッセージは表示されます。スタティック ブラックリストに名前や IP アドレスを入力するには、**dynamic-filter blacklist** コマンドを使用します。

スタティック データベースにドメイン名を追加した場合、ASA は、1 分間待機してからそのドメイン名の DNS 要求を送信し、ドメイン名と IP アドレスの組を *DNS ホスト キャッシュ*に追加します(このアクションはバックグラウンド プロセスで、ASA の設定の続行に影響しません)。ボットネット トラフィック フィルタ スヌーピングによる DNS パケット インスペクションもイネーブルにすることを推奨します(**inspect dns dynamic-filter-snooping** コマンドを参照してください)。次の場合、ASA は、通常の DNS lookup ではなく、ボットネット トラフィック フィルタ スヌーピングを使用してスタティック ブラックリストのドメイン名を解決します。

- ASA DNS サーバが使用できない。
- ASA が通常の DNS 要求を送信する前の 1 分間の待機期間中に接続が開始された。

DNS スヌーピングを使用すると、感染ホストがスタティック データベースに記載されている名前に対する DNS 要求を送信したときに、ASA がドメイン名と関連付けられている IP アドレスを DNS パケット内から検出し、その名前と IP アドレスを DNS 逆ルックアップ キャッシュに追加します。

ボットネット トラフィック フィルタ スヌーピングをイネーブルにせず、上記の状況のいずれかが発生した場合、このトラフィックは、ボットネット トラフィック フィルタでモニタされません。

(注) このコマンドは、ASA が DNS サーバを使用することが必須です。**dns domain-lookup** コマンドおよび **dns server-group** コマンドを参照してください。

例

次に、ブラックリストおよびホワイトリストのエントリを作成する例を示します。

```
ciscoasa(config)# dynamic-filter blacklist
ciscoasa(config-llist)# name bad1.example.com
ciscoasa(config-llist)# name bad2.example.com
ciscoasa(config-llist)# address 10.1.1.1 255.255.255.0

ciscoasa(config-llist)# dynamic-filter whitelist
ciscoasa(config-llist)# name good.example.com
ciscoasa(config-llist)# name great.example.com
ciscoasa(config-llist)# name awesome.example.com
ciscoasa(config-llist)# address 10.1.1.2 255.255.255.255
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバに DNS 要求を送信できるようにします。

コマンド	説明
dns server-group	ASA の DNS サーバを指定します。
dynamic-filter ambiguous-is-black	グレイリストに登録されているトラフィックをブラックリストに登録されているトラフィックと同様のアクションで処理します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter drop blacklist	ブラックリストに登録されているトラフィックを自動でドロップします。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニタされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバの IP アドレス、ASA が次にサーバに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデート サーバに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

echo コマンド ～ extended-security コマンド

echo

BFD シングルホップ テンプレートでエコーを設定するには、BFD テンプレート コンフィギュレーション モードで **echo** コマンドを使用します。シングルホップ セッション用の BFD テンプレートでエコーをディセーブルにするには、このコマンドの **no** 形式を使用します。

echo

no echo

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドにデフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
BFD コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

シングルホップ テンプレートのみでエコー モード機能をイネーブルにするには、このコマンドを使用します。BFD エコーは、IPv6 BFD セッションではサポートされません。

例

次に、シングルホップ BFD テンプレートでエコーを設定する例を示します。

```
ciscoasa(config)# bfd-template single-hop template1
ciscoasa(config-bfd)# echo
```

関連コマンド

コマンド	説明
authentication	シングルホップ セッションとマルチホップ セッションの BFD テンプレートに認証を設定します。
bfd echo	インターフェイスで BFD エコー モードを有効にします。
bfd interval	インターフェイスにベースライン BFD パラメータを設定します。
bfd map	アドレスとマルチホップ テンプレートを関連付ける BFD マップを設定します。
bfd slow-timers	BFD スロー タイマー値を設定します。
bfd template	シングルホップ BFD テンプレートをインターフェイスにバインドします。
bfd-template single-hop | multi-hop	BFD テンプレートを設定し、BFD コンフィギュレーション モードを開始します。
clear bfd counters	BFD カウンタをクリアします。
neighbor	BGP が登録され、BFD から転送パス検出失敗メッセージを受信できるように、BGP の BFD サポートを設定します。
show bfd drops	BFD でドロップされたパケットの数を表示します。
show bfd map	設定済みの BFD マップを表示します。
show bfd neighbors	既存の BFD 隣接関係の詳細なリストを表示します。
show bfd summary	BFD のサマリー情報を表示します。

early-message

H.323 インスペクション中に H.255 SETUP メッセージの前にメッセージを許可するには、パラメータ コンフィギュレーション モードで **early-message** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

early-message *message_type*

no early-message *message_type*

構文の説明

message_type	H.225 SETUP メッセージの前に許可するメッセージのタイプです。次のタイプを入力できます。 • **facility**

デフォルト

このコマンドはディセーブルです。H.225 SETUP メッセージの前にメッセージは許可されず、接続がドロップされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが導入されました。

使用上のガイドライン

H.460.18 では、ネットワーク アドレス変換機能とファイアウォールを越えて H.323 シグナリングを伝送するための方法が定義されています。この方法を使用すると、H.225 FACILITY メッセージを H.225 SETUP メッセージの前に送信できます。H.323/H.225 を使用するときに、接続が完了前に終了するコール セットアップの問題が発生した場合、このコマンドを使用して早期メッセージを許可します。

また、必ず H.323 RAS と H.225 の両方にインスペクションをイネーブルにしてください(デフォルトではどちらもイネーブルになっています)。

例

次に、早期メッセージを許可する例を示します。

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# early-message FACILITY
```

関連コマンド

コマンド	説明
policy-map type inspect	インスペクション ポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

eigrp log-neighbor-changes

EIGRP ネイバーとの隣接関係の変更のロギングをイネーブルにするには、ルータ コンフィギュレーション モードで **eigrp log-neighbor-changes** コマンドを使用します。この機能をオフにするには、このコマンドの **no** 形式を使用します。

eigrp log-neighbor-changes

no eigrp log-neighbor-changes

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

eigrp log-neighbor-changes コマンドはデフォルトでイネーブルです。実行コンフィギュレーションには、コマンドの **no** 形式のみが表示されます。

例

次に、EIGRP ネイバーの変更のロギングをディセーブルにする例を示します。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# no eigrp log-neighbor-changes
```

関連コマンド

コマンド	説明
eigrp log-neighbor-warnings	ネイバー警告メッセージのロギングをイネーブルにします。
router eigrp	EIGRP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

eigrp log-neighbor-warnings

EIGRP ネイバー警告メッセージのロギングをイネーブルにするには、ルータ コンフィギュレーション モードで **eigrp log-neighbor-warnings** コマンドを使用します。この機能をオフにするには、このコマンドの **no** 形式を使用します。

eigrp log-neighbor-warnings [*seconds*]

no eigrp log-neighbor-warnings

構文の説明

seconds	（任意）ネイバー警告メッセージの反復間隔（秒数）。有効値は 1 ～ 65535 です。この間隔内に警告が繰り返し発生した場合、それらの警告はログに記録されません。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。すべてのネイバー警告メッセージがログに記録されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

eigrp log-neighbor-warnings コマンドはデフォルトでイネーブルです。実行コンフィギュレーションには、コマンドの **no** 形式のみが表示されます。

例

次に、EIGRP ネイバーの警告メッセージのロギングをディセーブルにする例を示します。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# no eigrp log-neighbor-warnings
```

次に、EIGRP ネイバー警告メッセージをログに記録し、5 分（300 秒）間隔で警告メッセージを繰り返す例を示します。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# eigrp log-neighbor-warnings 300
```

関連コマンド

コマンド	説明
eigrp log-neighbor-messages	EIGRP ネイバーとの隣接関係に関する変更のロギングをイネーブルにします。
router eigrp	EIGRP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

eigrp router-id

EIGRP ルーティング プロセスによって使用されるルータ ID を指定するには、ルータ コンフィギュレーション モードで **eigrp router-id** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

eigrp router-id *ip-addr*

no eigrp router-id [*ip-addr*]

構文の説明

ip-addr	IP アドレス形式（ドット付き 10 進形式）でのルータ ID。ルータ ID として 0.0.0.0 または 255.255.255.255 を使用することはできません。

デフォルト

指定しない場合、ASA 上で最上位の IP アドレスがルータ ID として使用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

eigrp router-id コマンドが設定されていない場合、EIGRP プロセスが開始されたとき、EIGRP は、ルータ ID として使用するために、ASA 上で最上位の IP アドレスを自動的に選択します。EIGRP プロセスが **no router eigrp** コマンドによって削除されない限り、またはルータ ID が **eigrp router-id** コマンドによって手動で設定されていない限り、ルータ ID は変更されません。

ルータ ID は、外部ルートの発信元ルータを識別するために使用されます。外部ルートがローカルのルータ ID で受信された場合、このルートは廃棄されます。このような事態を回避するには、**eigrp router-id** コマンドを使用して、ルータ ID のグローバル アドレスを指定します。

各 EIGRP ルータには、一意の値を設定する必要があります。

例

次に、EIGRP ルーティング プロセスの固定ルータ ID として 172.16.1.3 を設定する例を示します。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# eigrp router-id 172.16.1.3
```

関連コマンド

コマンド	説明
router eigrp	EIGRP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

eigrp stub

EIGRP ルーティング プロセスをスタブ ルーティング プロセスとして設定するには、ルータ コンフィギュレーション モードで **eigrp stub** コマンドを使用します。EIGRP スタブ ルーティングを削除するには、このコマンドの **no** 形式を使用します。

eigrp stub [**receive-only**] | {[**connected**] [**redistributed**] [**static**] [**summary**]}

no eigrp stub [**receive-only**] | {[**connected**] [**redistributed**] [**static**] [**summary**]}

構文の説明

接続	(任意)接続ルートをアドバタイズします。
receive-only	(任意)ASA を受信専用ネイバーとして設定します。
redistributed	(任意)他のルーティング プロトコルから再配布されたルートをアドバタイズします。
静的	(任意)スタティック ルートをアドバタイズします。
summary	(任意)集約ルートをアドバタイズします。

デフォルト

スタブ ルーティングはイネーブルになっていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

eigrp stub コマンドを使用して、ASA をスタブとして設定します。この場合、ASA では、すべての IP トラフィックがディストリビューション ルータに転送されます。

receive-only キーワードを使用すると、ASA が自律システム内の他のどのルータともルートを共有しないように設定できます。ASA は、EIGRP ネイバーからの更新のみを受信します。**receive-only** キーワードは他のキーワードと組み合わせて使用することはできません。

connected、**static**、**summary**、および **redistributed** の各キーワードは、1 つ以上を組み合わせて指定できます。これらのいずれかのキーワードを指定して **eigrp stub** コマンドを使用した場合、これらの特定のキーワードによって指定されたルート タイプのみが送信されます。

connected キーワードを指定すると、EIGRP スタブ ルーティング プロセスで接続ルートを送信できます。接続ルートが **network** ステートメントで指定されていない場合は、EIGRP プロセスで **redistribute** コマンドを使用して接続ルートの再配布が必要となることがあります。

static キーワードを指定すると、EIGRP スタブ ルーティング プロセスでスタティック ルートを送信できます。このオプションを設定していない場合は、EIGRP は、通常は自動的に再配布される内部スタティック ルートを含め、どのスタティック ルートも送信しません。**redistribute static** コマンドを使用して引き続きスタティック ルートを再配布する必要があります。

summary キーワードを指定すると、EIGRP スタブ ルーティング プロセスで集約ルートを送信できます。集約ルートは、**summary-address eigrp** コマンドを使用して手動で作成することも、**auto-summary** コマンドをイネーブルにして自動的に作成することもできます(このコマンドはデフォルトでイネーブルになっています)。

redistributed キーワードを指定すると、EIGRP スタブ ルーティング プロセスで、他のルーティング プロトコルから EIGRP ルーティング プロセスに再配布されたルートを送信できます。このオプションを設定しない場合、再配布されたルートは EIGRP によってアドバタイズされません。

例

次に、**eigrp stub** コマンドを使用して、接続ルートおよび集約ルートをアドバタイズする EIGRP スタブとして ASA を設定する例を示します。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# eigrp stub connected summary
```

次に、**eigrp stub** コマンドを使用して、接続ルートおよびスタティック ルートをアドバタイズする EIGRP スタブとして ASA を設定する例を示します。集約ルートの送信は許可されません。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# eigrp stub connected static
```

次に、**eigrp stub** コマンドを使用して、EIGRP 更新の受信のみを行う EIGRP スタブとして ASA を設定する例を示します。接続ルート、集約ルート、およびスタティック ルートの情報は送信されません。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0 eigrp
ciscoasa(config-router)# eigrp stub receive-only
```

次に、**eigrp stub** コマンドを使用して、他のルーティング プロトコルから EIGRP に再配布されたルートをアドバタイズする EIGRP スタブとして ASA を設定する例を示します。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# eigrp stub redistributed
```

次に、オプションの引数を指定しないで **eigrp stub** コマンドを使用する例を示します。引数なしで **eigrp stub** コマンドを使用すると、デフォルトで接続ルートおよびスタティック ルートがアドバタイズされます。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# eigrp stub
```

関連コマンド

コマンド	説明
router eigrp	実行コンフィギュレーションから EIGRP ルータ コンフィギュレーション モード コマンドをクリアします。
show running-config router eigrp	実行コンフィギュレーションの EIGRP ルータ コンフィギュレーション モード コマンドを表示します。

eject

ASA の外部コンパクト フラッシュ デバイスの取り外しをサポートするには、ユーザ EXEC モードで **eject** コマンドを使用します。

eject [**/noconfirm**] *disk1:*

構文の説明

disk1:	取り外すデバイスを指定します。
/noconfirm	ASA から外部フラッシュ デバイスを物理的に取り外す前に、デバイスを取り外すかどうかの確認が必要ないことを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

eject コマンドを使用すると、ASA 5500 シリーズからコンパクト フラッシュ デバイスを安全に取り外すことができます。

次に、**eject** コマンドを使用して、デバイスを ASA から物理的に取り外す前に *disk1* を正常にシャットダウンする例を示します。

```
ciscoasa# eject /noconfig disk1:
It is now safe to remove disk1:
ciscoasa# show version
Cisco Adaptive Security Appliance Software Version 8.0(2)34

Compiled on Fri 18-May-07 10:28 by juser System image file is "disk0:/cdisk.asa"
Config file at boot was "startup-config"

wef5520 up 5 hours 36 mins

Hardware:   ASA5520, 512 MB RAM, CPU Pentium 4 Celeron 2000 MHz
Internal ATA Compact Flash, 256MB
Slot 1: Compact Flash has been ejected!
It may be removed and a new device installed.
BIOS Flash M50FW016 @ 0xffe00000, 2048KB
<---More--->
```

関連コマンド

コマンド	説明
show version	オペレーティング システム ソフトウェアに関する情報を表示します。

email

登録時に、指定した電子メール アドレスを証明書のサブジェクト代替名の拡張に含めるには、クリプト CA トラストポイント コンフィギュレーション モードで **email** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

email *address*

no email

構文の説明

address	電子メール アドレスを指定します。最大長は、64 文字です。

デフォルト

デフォルト設定は設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central の登録要求に電子メール アドレス user1@user.net を含める例を示します。

```
ciscoasa(config)# crypto ca-trustpoint central
ciscoasa(ca-trustpoint)# email user1@user.net
ciscoasa(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca-trustpoint	クリプト CA トラストポイント コンフィギュレーション モードを開始します。

enable（クラスタ グループ）

クラスタリングをイネーブルにするには、クラスタ グループ コンフィギュレーション モードで **enable** コマンドを使用します。クラスタリングをディセーブルにするには、このコマンドの **no** 形式を使用します。

enable [**as-slave** | **noconfirm**]

no enable

構文の説明

as-slave	（オプション）互換性のないコマンドの実行コンフィギュレーションを確認せずにクラスタリングをイネーブルにし、クラスタに参加させるスレーブが現在の選択においてマスターとなる可能性をなくします。スレーブのコンフィギュレーションは、マスター ユニットから同期されたコンフィギュレーションによって上書きされます。
noconfirm	（オプション）**enable** コマンドが入力されると、ASA は実行コンフィギュレーションをスキャンして、クラスタリングに対応していない機能の非互換コマンドの有無を調べます。デフォルト コンフィギュレーションにあるコマンドも、これに該当することがあります。互換性のないコマンドを削除するように求められます。応答として **No** を入力した場合は、クラスタリングはイネーブルになりません。確認を省略し、互換性のないコマンドを自動的に削除するには、**noconfirm** キーワードを使用します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラスタ グループ コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

最初にイネーブルにしたユニットについては、マスター ユニット選定が発生します。最初のユニットは、その時点でクラスタの唯一のメンバーであるため、そのユニットがマスター ユニットになります。この期間中にコンフィギュレーション変更を実行しないでください。

すでにマスター ユニットがある場合に、クラスタにスレーブ ユニットを追加するときは、**enable as-slave** コマンドを使用すると、コンフィギュレーションの互換性の問題（主にまだクラスタリング用に設定されていないインターフェイスの存在）を回避できます。

クラスタリングをディセーブルにするには、**no enable** コマンドを入力します。

（注） クラスタリングをディセーブルにした場合は、すべてのデータ インターフェイスがシャットダウンされ、管理インターフェイスだけがアクティブになります。ユニットをクラスタから完全に削除する（その結果としてデータ インターフェイスをアクティブにする）場合は、クラスタ グループ コンフィギュレーション全体を削除する必要があります。

例

次に、クラスタリングをイネーブルにし、互換性のないコンフィギュレーションを削除する例を示します。

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# enable
INFO: Clustering is not compatible with following commands:
policy-map global_policy
 class inspection_default
 inspect skinny
policy-map global_policy
 class inspection_default
  inspect sip
Would you like to remove these commands? [Y]es/[N]o:Y

INFO: Removing incompatible commands from running configuration...
Cryptochecksum (changed): f16b7fc2 a742727e e40bc0b0 cd169999
INFO: Done
```

関連コマンド

コマンド	説明
clacp system-mac	スパンド EtherChannel を使用するときは、ASA は cLACP を使用してネイバー スイッチとの間で EtherChannel のネゴシエーションを行います。
cluster group	クラスタに名前を付け、クラスタ コンフィギュレーション モードを開始します。
cluster-interface	クラスタ制御リンク インターフェイスを指定します。
cluster interface-mode	クラスタ インターフェイス モードを設定します。
conn-rebalance	接続の再分散をイネーブルにします。
console-replicate	スレーブ ユニットからマスター ユニットへのコンソール複製をイネーブルにします。
health-check	クラスタのヘルス チェック機能（ユニットのヘルス モニタリングおよびインターフェイスのヘルス モニタリングを含む）をイネーブルにします。
key	クラスタ制御リンクの制御トラフィックの認証キーを設定します。
local-unit	クラスタ メンバーに名前を付けます。

コマンド	説明
mtu cluster-interface	クラスタ制御リンク インターフェイスの最大伝送ユニットを指定します。
priority（クラスタ グループ）	マスター ユニット選定のこのユニットのプライオリティを設定します。

enable(ユーザ EXEC)

特権 EXEC モードを開始するには、ユーザ EXEC モードで **enable** コマンドを使用します。

enable [*level*]

構文の説明

level	(任意)0 ～ 15 の特権レベル。enable 認証(**aaa authentication enable console** コマンド)では使用されません。

デフォルト

enable 認証(**aaa authentication enable console** コマンドを使用)を使用していない場合は、特権レベル 15 を開始します。enable 認証の場合、デフォルトのレベルは、ユーザ名に設定されているレベルに応じて異なります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトのイネーブル パスワードはブランクです。パスワードの設定については、**enable password** コマンドを参照してください。

enable 認証を使用しない場合は、**enable** コマンドを入力すると、ユーザ名が enable_*level* に変更されます。デフォルトのレベルは 15 です。enable 認証を使用する場合(**aaa authentication enable console** コマンドを使用)、ユーザ名および関連するレベルは維持されます。ユーザ名の維持は、コマンド認可(ローカルまたは TACACS+ を使用した **aaa authorization command** コマンド)で重要です。

レベル 2 以上は特権 EXEC モードを開始します。レベル 0 およびレベル 1 は、ユーザ EXEC モードを開始します。中間のレベルを使用するには、ローカル コマンド認可(**aaa authorization command LOCAL** コマンド)をイネーブルにし、**privilege** コマンドを使用して異なる特権レベルにコマンドを設定します。TACACS+ コマンド認可では、ASA に設定された特権レベルは使用されません。

現在の特権レベルを表示するには、**show curpriv** コマンドを使用します。

特権 EXEC モードを終了するには、**disable** コマンドを入力します。

例

次に、特権 EXEC モードを開始する例を示します。

```
ciscoasa> enable
Password: Pa$$w0rd
ciscoasa#
```

次に、レベル 10 の特権 EXEC モードを開始する例を示します。

```
ciscoasa> enable 10
Password: Pa$$w0rd10
ciscoasa#
```

関連コマンド

コマンド	説明
イネーブル パスワード	イネーブル パスワードを設定します。
disable	特権 EXEC モードを終了します。
aaa authorization command	コマンド認可を設定します。
privilege	ローカル コマンド認可のためのコマンド特権レベルを設定します。
show curpriv	現在ログインしているユーザ名とユーザの特権レベルを表示します。

enable e-mail proxy（廃止）

(注) このコマンドをサポートする最後のリリースは、9.5(1) でした。

以前に設定したインターフェイスで電子メール プロキシ アクセスをイネーブルにするには、**enable** コマンドを使用します。電子メール プロキシ（IMAP4S、POP3S、および SMTPS）の場合は、該当する電子メール プロキシ コンフィギュレーション モードでこのコマンドを使用します。インターフェイス上で電子メール プロキシ アクセスをディセーブルにするには、このコマンドの **no** 形式を使用します。

enable *ifname*

no enable

構文の説明

ifname	以前に設定したインターフェイスを指定します。**nameif** コマンドを使用して、インターフェイスを設定します。

デフォルト

デフォルト値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
Imap4s コンフィギュレーション	• 対応	—	• 対応	—	—
Pop3s コンフィギュレーション	• 対応	—	• 対応	—	—
smtps コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.5(2)	このコマンドは廃止されました。

例

次に、Outside という名前のインターフェイスで POP3S 電子メール プロキシを設定する方法の例を示します。

```
ciscoasa(config)# pop3s
ciscoasa(config-pop3s)# enable Outside
```

enable gprs

RADIUS アカウンティングで GPRS をイネーブルにするには、RADIUS アカウンティング パラメータ コンフィギュレーション モードで **enable gprs** コマンドを使用します。このコマンドをディセーブルにするには、このコマンドの **no** 形式を使用します。

enable gprs

no enable gprs

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
RADIUS アカウンティング パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、**inspect radius-accounting** コマンドを使用してアクセスします。ASA は、セカンダリ PDP コンテキストを適切に処理するために、アカウンティング要求停止メッセージ内に 3GPP VSA 26-10415 があるかどうかをチェックします。このオプションは、デフォルトで無効です。この機能をイネーブルにするには、GTP ライセンスが必要です。

例

次に、RADIUS アカウンティングで GPRS をイネーブルにする例を示します。

```
ciscoasa(config)# policy-map type inspect radius-accounting ra
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# enable gprs
```

関連コマンド

コマンド	説明
inspect radius-accounting	RADIUS アカウンティングのインスペクションを設定します。
パラメータ	インスペクション ポリシー マップのパラメータを設定します。

enable password

特権 EXEC モードのイネーブル パスワードを設定するには、グローバル コンフィギュレーション モードで **enable password** コマンドを使用します。

enable password *password* [**level** *level*] [**pbkdf2** | **encrypted**]

構文の説明

encrypted	(任意)9.6 以前の場合は、32 文字以下のパスワードを暗号化することを指定します。**enable password** コマンドでパスワードを定義すると、ASA はセキュリティのためにそのパスワードをコンフィギュレーションに保存するときに MD5 ハッシュを作成します。**show running-config** コマンドを入力しても、**enable password** コマンドによって実際のパスワードは表示されず、暗号化されたパスワードと、その後に **encrypted** キーワードが表示されます。たとえば、"test" というパスワードを入力した場合、**show running-config** コマンドの出力は次のように表示されます。 `enable password rvEdRh0xPC8bel7s encrypted` CLI で実際に **encrypted** キーワードを入力するのは、コンフィギュレーションを別の ASA にカット アンド ペーストして、同じパスワードを使用する場合だけです。 9.7 以降では、すべての長さのパスワードで PBKDF2 を使用します。
level *level*	(任意)0 ～ 15 の特権レベルのパスワードを設定します。
password	3 ～ 127 文字の英数字および特殊文字から構成されるストリングとしてパスワードを設定します(大文字と小文字は区別されます)。パスワードには、疑問符とスペースを除いて、任意の文字を使用できます。
pbkdf2	(任意)パスワードの暗号化を指定します。9.6 以前の場合、PBKDF2 (パスワードベースのキー派生関数 2)ハッシュは、パスワードの長さが 32 文字を超える場合にのみ使用されます。9.7 以降では、すべてのパスワードで PBKDF2 を使用します。**enable password** コマンドでパスワードを定義すると、ASA はセキュリティのためにそのパスワードをコンフィギュレーションに保存するときに PBKDF2 (Password-Based Key Derivation Function 2)ハッシュを作成します。**show running-config** コマンドを入力しても、**enable password** コマンドによって実際のパスワードは表示されず、暗号化されたパスワードと、その後に **pbkdf2** キーワードが表示されます。たとえば、長いパスワードを入力した場合、**show running-config** コマンドの出力は次のように表示されます。 `username pat password rvEdRh0xPC8bel7s pbkdf2` CLI で実際に **pbkdf2** キーワードを入力するのは、コンフィギュレーションを別の ASA にカット アンド ペーストして、同じパスワードを使用する場合だけです。 新しいパスワードを入力しない限り、既存のパスワードは MD5 ベースのハッシュを使用し続けることに注意してください。

デフォルト

デフォルトのパスワードはブランクです。デフォルトのレベルは 15 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.6(1)	パスワードの長さが 127 文字に増加し、**pbkdf2** キーワードが追加されました。
9.7(1)	すべての長さのパスワードが PBKDF2 ハッシュを使用してコンフィギュレーションに保存されるようになりました。
9.12(1)	**no enable password** コマンドは現在サポートされていません。

使用上のガイドライン

enable レベル 15（デフォルト レベル）のデフォルト パスワードは空白ですが、enable コマンドを最初に入力したときに変更するように求められます。パスワードを空白に設定できません。

CLI で **aaa authorization exec auto-enable** を有効にすると、**enable** コマンド、**login** コマンド（特権レベル 2 以上のユーザ）、または SSH/Telnet セッションを使用して特権 EXEC モードにアクセスできます。これらの方法ではすべて、イネーブル パスワードを設定する必要があります。

このパスワード変更の要件は、ASDM のログインには適用されません。ASDM のデフォルトでは、ユーザ名を使用せず enable パスワードを使用してログインすることができます。

マルチ コンテキスト モードでは、システム コンフィギュレーションおよび各コンテキストに対してイネーブル パスワードを作成できます。

デフォルトの 15 以外の特権レベルを使用するには、ローカル コマンド認可（**aaa authorization command** コマンドを使用して **LOCAL** キーワードを指定）を設定し、**privilege** コマンドを使用して異なる特権レベルにコマンドを設定します。ローカル コマンド認可を設定しない場合、イネーブル レベルは無視されて、設定したレベルにかかわらずレベル 15 へのアクセスが可能になります。現在の特権レベルを表示するには、**show curpriv** コマンドを使用します。

レベル 2 以上は特権 EXEC モードを開始します。レベル 0 およびレベル 1 は、ユーザ EXEC モードを開始します。

例

次に、イネーブル パスワードを Pa$$w0rd に設定する例を示します。

```
ciscoasa(config)# enable password Pa$$w0rd
```

次に、レベル 10 のイネーブル パスワードを Pa$$w0rd10 に設定する例を示します。

```
ciscoasa(config)# enable password Pa$$w0rd10 level 10
```

次に、イネーブル パスワードを、別の ASA からコピーした暗号化されたパスワードに設定する例を示します。

```
ciscoasa(config)# enable password jMorNbK0514fadBh pbkdf2
```

関連コマンド

コマンド	説明
aaa authorization command	コマンド認可を設定します。
enable	特権 EXEC モードを開始します。
privilege	ローカル コマンド認可のためのコマンド特権レベルを設定します。
show curpriv	現在ログインしているユーザ名とユーザの特権レベルを表示します。
show running-config enable	イネーブル パスワードを暗号化された形式で表示します。

webvpn の有効化

以前に設定したインターフェイスで WebVPN アクセスをイネーブルにするには、**enable** コマンドを使用します。このコマンドは、WebVPN コンフィギュレーション モードで使用します。インターフェイスで WebVPN をディセーブルにするには、このコマンドの **no** 形式を使用します。

enable *ifname*

no enable

構文の説明

ifname	以前に設定したインターフェイスを指定します。**nameif** コマンドを使用して、インターフェイスを設定します。

デフォルト

WebVPN は、デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、Outside という名前のインターフェイスで WebVPN をイネーブルにする方法の例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# enable Outside
```

encapsulation-vxlan

VXLAN カプセル化を使用するようにネットワーク仮想化エンドポイント(NVE)インスタンスを設定するには、NVE コンフィギュレーション モードで **encapsulation-vxlan** コマンドを使用します。カプセル化を削除するには、このコマンドの **no** 形式を使用します。

encapsulation-vxlan

no encapsulation-vxlan

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

このコマンドは、**nve** コマンドを入力した場合のデフォルトです。VXLAN のみがカプセル化の対象としてサポートされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
Nve コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

encapsulation vxlan コマンドが NVE インスタンスのデフォルトにより追加されます。明示的に追加する必要はありません。

例

次に、NVE instance 1 を作成し、**encapsulation vxlan** コマンドを自動的に追加する例を示します。

```
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)# show running-config nve
nve 1
 encapsulation vxlan
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
default-mcast-group	VTEP 送信元インターフェイスに関連付けられているすべての VNI インターフェイスのデフォルトのマルチキャスト グループを指定します。
inspect vxlan	標準 VXLAN ヘッダー形式に強制的に準拠させます。
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
mcast-group	VNI インターフェイスのマルチキャスト グループ アドレスを設定します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
nve-only	VXLAN 送信元インターフェイスが NVE 専用であることを指定します。
peer ip	ピア VTEP の IP アドレスを手動で指定します。
segment-id	VNI インターフェイスの VXLAN セグメント ID を指定します。
show arp vtep-mapping	リモート セグメント ドメインにある IP アドレスとリモート VTEP IP アドレス用の VNI インターフェイスにキャッシュされた MAC アドレスを表示します。
show interface vni	VNI インターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス(設定されている場合)のステータス、ならびに関連付けられている NVE インターフェイスを表示します。
show mac-address-table vtep-mapping	リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ 2 転送テーブル(MAC アドレス テーブル)を表示します。
show nve	NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリア インターフェイス(送信元インターフェイス)のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。
show vni vlan-mapping	VNI セグメント ID と、VLAN インターフェイスまたはトランスペアレント モードの物理インターフェイス間のマッピングを表示します。
source-interface	VTEP 送信元インターフェイスを指定します。
vtep-nve	VNI インターフェイスを VTEP 送信元インターフェイスに関連付けます。
vxlan port	VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。

暗号化

AnyConnect IPsec 接続に対して IKEv2 セキュリティ アソシエーション（SA）の暗号化アルゴリズムを指定するには、Ikev2 ポリシー コンフィギュレーション モードで **encryption** コマンドを使用します。コマンドを削除してデフォルト設定を使用するには、このコマンドの **no** 形式を使用します。

encryption [**des** | **3des** | **aes** | **aes-192** | **aes-256** | **aes-gcm** | **aes-gcm-192** | **aes-gcm-256** | **null**]

no encryption [**des** | **3des** | **aes** | **aes-192** | **aes-256** | **aes-gcm** | **aes-gcm-192** | **aes-gcm-256** | **null**]

構文の説明

des	56 ビット DES-CBC 暗号化を ESP に対して指定します。
3des	（デフォルト）トリプル DES 暗号化アルゴリズムを ESP に対して指定します。
aes	AES と 128 ビット キー暗号化を ESP に対して指定します。
aes-192	AES と 192 ビット キー暗号化を ESP に対して指定します。
aes-256	AES と 256 ビット キー暗号化を ESP に対して指定します。
aes-gcm	IKEv2 暗号化の AES-GCM アルゴリズムを指定します。
aes-gcm-192	IKEv2 暗号化の AES-GCM アルゴリズムを指定します。
aes-gcm-256	IKEv2 暗号化の AES-GCM アルゴリズムを指定します。
null	AES-GCM/GMAC が暗号化アルゴリズムとして設定されている場合は、ヌル整合性アルゴリズムを選択します。

デフォルト

デフォルトは 3DES です。

使用上のガイドライン

IKEv2 SA は、IKEv2 ピアがフェーズ 2 で安全に通信できるようにするためにフェーズ 1 で使用されるキーです。**crypto ikev2 policy** コマンドを入力した後、**encryption** コマンドを使用して、SA の暗号化アルゴリズムを設定できます。

OSPFv3 暗号化がインターフェイスでイネーブルの場合、IPsec トンネルを設定している間に隣接関係を確立すると、遅延が発生する可能性があります。基礎となる IPsec トンネルのステータスを判別し、処理が発生していることを確認するには、**show crypto sockets**、**show ipsec policy**、および **show ipsec sa** コマンドを使用します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
Ikev2 ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	IKEv2 暗号化に使用される AES-GCM アルゴリズムが追加されました。

例

次に、Ikev2 ポリシー コンフィギュレーション モードを開始して、暗号化を AES-256 に設定する例を示します。

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# encryption aes-256
```

関連コマンド

コマンド	説明
group	AnyConnect IPsec 接続に対して IKEv2 SA の Diffie-Hellman グループを指定します。
整合性	AnyConnect IPsec 接続に対して IKEv2 SA の ESP 整合性アルゴリズムを指定します。
prf	AnyConnect IPsec 接続に対して IKEv2 SA の疑似乱数関数を指定します。
ライフタイム	AnyConnect IPsec 接続に対して IKEv2 SA の SA ライフタイムを指定します。

エンドポイント

H.323 プロトコル インスペクションの HSI グループにエンドポイントを追加するには、HSI グループ コンフィギュレーション モードで **endpoint** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

endpoint *ip_address if_name*

no endpoint *ip_address if_name*

構文の説明

if_name	エンドポイントが ASA に接続するときに通過するインターフェイス。
ip_address	追加するエンドポイントの IP アドレス。HSI グループあたり最大で 10 のエンドポイントを設定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
hsi グループ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、H.323 インスペクション ポリシー マップの HSI グループにエンドポイントを追加する例を示します。

```
ciscoasa(config-pmap-p)# hsi-group 10
ciscoasa(config-h225-map-hsi-grp)# endpoint 10.3.6.1 inside
ciscoasa(config-h225-map-hsi-grp)# endpoint 10.10.25.5 outside
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
hsi-group	HSI グループを作成します。
hsi	HSI を HSI グループに追加します。

コマンド	説明
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

endpoint-mapper

DCERPC インスペクションのエンドポイント マッパー オプションを設定するには、パラメータ コンフィギュレーション モードで **endpoint-mapper** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

endpoint-mapper [**epm-service-only**] [**lookup-operation** [**timeout** *value*]]

no endpoint-mapper [**epm-service-only**] [**lookup-operation** [**timeout** *value*]]

構文の説明

epm-service-only	バインディング時にエンドポイント マッパー サービスを適用することを指定します。
lookup-operation	エンドポイント マッパー サービスのルックアップ動作をイネーブルにすることを指定します。
timeout *value*	ルックアップ動作におけるピンホールのタイムアウトを指定します。指定できる範囲は 0:0:1 ～ 1193:0:0 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、DCERPC ポリシー マップにエンドポイント マッパーを設定する例を示します。

```
ciscoasa(config)# policy-map type inspect dcerpc dcerpc_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# endpoint-mapper epm-service-only
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

enforcenextupdate

CRL の NextUpdate フィールドの処理方法を指定するには、ca-crl コンフィギュレーション モードで **enforcenextupdate** コマンドを使用します。期限が切れた NextUpdate フィールドがある場合や、NextUpdate フィールドがない場合を許容するには、このコマンドの **no** 形式を使用します。

enforcenextupdate

no enforcenextupdate

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの設定は強制（オン）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ca-crl コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドが設定されている場合は、期限が切れていない NextUpdate フィールドが CRL に存在する必要があります。このコマンドが使用されていない場合、ASA では、CRL に NextUpdate フィールドがない場合や、期限が切れた NextUpdate フィールドがある場合が許容されます。

例

次に、クリプト ca-crl コンフィギュレーション モードを開始して、トラストポイント central に対して、期限が切れていない NextUpdate フィールドが CRL に存在することを必須とする例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# enforcenextupdate
ciscoasa(ca-crl)#
```

関連コマンド]

コマンド	説明
cache-time	キャッシュのリフレッシュ時間を分単位で指定します。
crl configure	ca-crl コンフィギュレーション モードを開始します。
crypto ca trustpoint	クリプト CA トラストポイント コンフィギュレーション モードを開始します。

enrollment protocol scep | cmp url

このトラストポイントの登録に自動登録(SCEP または CMP の場合)を指定して、登録 URL を設定するには、クリプト CA トラストポイント コンフィギュレーション モードで **enrollment protocol scep| cmp url** コマンドを使用します。このコマンドのデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

enrollment protocol scep | smp *url*

no enrollment protocol scep | smp *url*

構文の説明

protocol	SCEP CA URL と CMP CA URL を区別します。

デフォルト

デフォルトの設定はオフです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クリプト CA サーバ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

LTE ワイヤレス ネットワークでセキュリティ ゲートウェイ デバイスとして機能するために、ASA は、SCEP に加えて Certificate Management Protocol(CMPv2)を使用していくつかの証明書管理機能をサポートします。ASA デバイス証明書の登録に CMPv2 を使用することで、CMPv2 が有効な CA からの最初の証明書とセカンダリ証明書を手動登録したり、同じキーペアを使用する以前に発行済みの証明書を差し替えるための証明書を手動更新したりできます。受信した証明書は従来の設定の外部に保存され、証明書が有効になっている IPsec の設定で使用されます。

例

次の例は、登録オプションを示しています。

```
(config)# crypto ca trustpoint new
(config-ca-trustpoint)# enrollment ?
crypto-ca-trustpoint mode commands/options:
    interface  Configure source interface
    protocol   Enrollment protocol
```

```
    retry       Polling parameters
    self        Enrollment will generate a self-signed certificate
    terminal    Enroll via the terminal (cut-and-paste)
asa2(config-ca-trustpoint)# enrollment protocol ?

crypto-ca-trustpoint mode commands/options:
    cmp         Certificate Management Protocol Version 2
    scep        Simple Certificate Enrollment Protocol
asa2(config-ca-trustpoint)# enrollment protocol cmp ?

crypto-ca-trustpoint mode commands/options:
    url         CA server enrollment URL
```

enrollment-retrieval

登録されたユーザが PKCS12 登録ファイルを取得できる期間を時間単位で指定するには、ローカル クリプト CA サーバ コンフィギュレーション モードで **enrollment-retrieval** コマンドを使用します。期間をデフォルトの時間数（24）にリセットするには、このコマンドの **no** 形式を使用します。

enrollment-retrieval *timeout*

no enrollment-retrieval

構文の説明

timeout	何時間以内にユーザがローカル CA 登録 Web ページから発行された証明書を取得しなければならないかを指定します。有効なタイムアウト値の範囲は 1 ～ 720 時間です。

デフォルト

デフォルトでは、PKCS12 登録ファイルは 24 時間保存されて取得できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クリプト CA サーバ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

PKCS12 登録ファイルには、発行された証明書とキー ペアが含まれています。ファイルはローカル CA サーバに保存され、**enrollment-retrieval** コマンドで指定された時間内は登録 Web ページから取得できます。

ユーザが登録可能とマークされている場合、そのユーザは **otp expiration** コマンドで指定した時間内であればそのパスワードを使用して登録できます。ユーザが正常に登録すると、PKCS12 ファイルが生成および保存され、コピーが登録 Web ページを経由して返されます。何らかの理由でファイルのコピーが再度必要になった場合（登録しようとしてダウンロードに失敗した場合など）、ユーザは **enrollment-retrieval** コマンドで指定した時間内であれば新しくコピーを取得できます。

（注） この時間は、OTP の有効期限とは関係ありません。

例

次に、証明書の発行後 48 時間以内は PKCS12 登録ファイルをローカル CA サーバから取得できるように指定する例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# enrollment-retrieval 48
ciscoasa(config-ca-server)#
```

次に、取得可能時間をデフォルトの 24 時間にリセットする例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# no enrollment-retrieval
ciscoasa(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モード コマンドにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
OTP expiration	CA 登録ページ用に発行されたワンタイム パスワードの有効期間を時間単位で指定します。
smtp from-address	CA サーバが生成するすべての電子メールの送信者フィールドに使用する電子メール アドレスを指定します。
smtp subject	ローカル CA サーバが生成するすべての電子メールの件名フィールドに表示されるテキストを指定します。
subject-name-default	CA サーバが発行するすべてのユーザ証明書でユーザ名とともに使用される汎用的なサブジェクト名 DN を指定します。

enrollment retry count

再試行回数を指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **enrollment retry count** コマンドを使用します。デフォルトの再試行回数設定に戻すには、このコマンドの **no** 形式を使用します。

enrollment retry count *number*

no enrollment retry count

構文の説明

number	登録要求の送信を試行する最大回数。有効な値は、0、および 1 ～ 100 の再試行です。

デフォルト

number 引数のデフォルト設定は 0（無制限）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

証明書を要求した後、ASA は CA からの証明書の受信を待ちます。ASA は、設定された再試行間隔内に証明書を受信できない場合、証明書要求を再度送信します。ASA は、応答を受信するか、または設定されている再試行間隔が終了するまで、要求を繰り返し送信します。このコマンドはオプションであり、自動登録を設定している場合のみ適用されます。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central 内の登録再試行回数を 20 回に設定する例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment retry count 20
ciscoasa(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	クリプト CA トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。
enrollment retry period	登録要求を再送信するまでの待機時間を分単位で指定します。

enrollment retry period

再試行間隔を指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **enrollment retry period** コマンドを使用します。デフォルトの再試行間隔設定に戻すには、このコマンドの **no** 形式を使用します。

enrollment retry period *minutes*

no enrollment retry period

構文の説明

minutes	登録要求の送信を試行する間隔（分単位）。有効な範囲は、1 ～ 60 分です。

デフォルト

デフォルトの設定は 1 分です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

証明書を要求した後、ASA は CA からの証明書の受信を待ちます。ASA は、指定された再試行間隔内に証明書を受信できない場合、証明書要求を再度送信します。このコマンドはオプションであり、自動登録を設定している場合のみ適用されます。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central 内の登録再試行間隔を 10 分に設定する例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment retry period 10
ciscoasa(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	クリプト CA トラストポイント コンフィギュレーション モードを開始します。
default enrollment	すべての登録パラメータを、システムのデフォルト値に戻します。
enrollment retry count	登録要求の再試行回数を定義します。

enrollment terminal

このトラストポイントでカット アンド ペースト登録(手動登録とも呼ばれます)を指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **enrollment terminal** コマンドを使用します。このコマンドのデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

enrollment terminal

no enrollment terminal

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの設定はオフです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central の CA 登録にカット アンド ペースト方式を指定する例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment terminal
ciscoasa(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	クリプト CA トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。
enrollment retry count	登録要求の送信を再試行する回数を指定します。

コマンド	説明
enrollment retry period	登録要求を再送信するまでの待機時間を分単位で指定します。
enrollment url	このトラストポイントに対して自動登録（SCEP）を指定して、URL を設定します。

enrollment url（廃止）

このトラストポイントの登録に自動登録（SCEP）を指定して、登録 URL を設定するには、クリプト CA トラストポイント コンフィギュレーション モードで **enrollment url** コマンドを使用します。このコマンドのデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

enrollment url *url*

no enrollment url ***url***

構文の説明

url	自動登録の URL の名前を指定します。最大の長さは 1000 文字です（実質的に無制限です）。

デフォルト

デフォルトの設定はオフです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central に URL https://enrollsite における SCEP 登録を指定する例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment url https://enrollsite
ciscoasa(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	クリプト CA トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。
enrollment retry count	登録要求の送信を再試行する回数を指定します。

コマンド	説明
enrollment retry period	登録要求を再送信するまでの待機時間を分単位で指定します。
enrollment terminal	このトラストポイントを使用したカット アンド ペースト登録を指定します。

eool

IP オプション インスペクションにおいて、パケット ヘッダー内に End of Options List（EOOL）オプションが存在する場合のアクションを定義するには、パラメータ コンフィギュレーション モードで **eool** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

eool action {allow | clear}

no eool action {allow | clear}

構文の説明

allow	End of Options List IP オプションを含むパケットを許可します。
clear	End of Options List オプションをパケットから削除してから、そのパケットを許可します。

デフォルト

デフォルトでは、IP オプション インスペクションは、End of Options List IP オプションを含むパケットをドロップします。

IP オプション インスペクション ポリシー マップで **default** コマンドを使用するとデフォルト値を変更できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IP オプション インスペクション ポリシー マップで設定できます。

IP オプション インスペクションを設定して、どの IP パケットが所定の IP オプションを持ち、ASA を通過できるかを制御できます。変更せずにパケットを通過させたり、指定されている IP オプションをクリアしてからパケットを通過させたりできます。

オプション リストの終端オプションは、1 バイトのゼロのみを含み、すべてのオプションの終端に配置されて、オプションのリストの終端を示します。これは、ヘッダー長に基づくヘッダーの末尾とは一致しない場合があります。

例

次に、IP オプション インスペクションのアクションをポリシー マップで設定する例を示します。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# eool action allow
ciscoasa(config-pmap-p)# nop action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

eou allow（廃止）

(注) このコマンドをサポートする最後のリリースは、Version 9.1(1) でした。

NAC フレームワーク コンフィギュレーションでクライアントレス認証をイネーブルにするには、グローバル コンフィギュレーション モードで **eou allow** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

eou allow {**audit** | **clientless** | **none**}

no eou allow {**audit** | **clientless** | **none**}

構文の説明

監査	クライアントレス認証を実行します。
clientless	クライアントレス認証を実行します。
none	クライアントレス認証をディセーブルにします。

デフォルト

デフォルトのコンフィギュレーションには、**eou allow clientless** コンフィギュレーションが含まれています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.0(2)	**audit** オプションが追加されました。
9.1(2)	このコマンドは廃止されました。

使用上のガイドライン

ASA では、次の両方の条件が満たされている場合にのみこのコマンドが使用されます。

- NAC ポリシー タイプとして NAC フレームワークを使用するようにグループ ポリシーが設定されていること。
- セッションのホストが EAPoUDP 要求に応答しないこと。

例

次に、ACS を使用したクライアントレス認証の実行をイネーブルにする例を示します。

```
ciscoasa(config)# eou allow clientless
ciscoasa(config)#
```

次に、監査サーバを使用してクライアントレス認証を実行するように ASA を設定する例を示します。

```
ciscoasa(config)# eou allow audit
ciscoasa(config)#
```

次に、監査サーバの使用をディセーブルにする例を示します。

```
ciscoasa(config)# no eou allow clientless
ciscoasa(config)#
```

関連コマンド

コマンド	説明
debug eou	EAP over UDP イベントのロギングをイネーブルにして、NAC フレームワーク メッセージをデバッグします。
eou clientless	NAC フレームワーク コンフィギュレーションのクライアントレス認証で ACS に対して送信されるユーザ名およびパスワードを変更します。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。

eou clientless（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.1(1) でした。

NAC フレームワーク コンフィギュレーションにおけるクライアントレス認証でアクセス コントロール サーバに送信するユーザ名とパスワードを変更するには、グローバル コンフィギュレーション モードで **eou clientless** コマンドを使用します。デフォルト値を使用するには、このコマンドの **no** 形式を使用します。

eou clientless username *username* **password** *password*

no eou clientless username *username* **password** *password*

構文の説明

password	EAPoUDP 要求に応答しないリモート ホストのクライアントレス認証を取得するためにアクセス コントロール サーバに送信するパスワードを変更する場合に入力します。
password	クライアントレス ホストをサポートするためにアクセス コントロール サーバに設定されているパスワードを入力します。4 ～ 32 文字の ASCII 文字を入力します。
username	EAPoUDP 要求に応答しないリモート ホストのクライアントレス認証を取得するためにアクセス コントロール サーバに送信するユーザ名を変更する場合に入力します。
username	クライアントレス ホストをサポートするためにアクセス コントロール サーバに設定されているユーザ名を入力します。先頭および末尾のスペース、シャープ記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、山カッコ（< および >）を除く、1 ～ 64 文字の ASCII 文字を入力します。

デフォルト

username 属性と password 属性のデフォルト値は、両方とも clientless です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.1(2)	このコマンドは廃止されました。

使用上のガイドライン

このコマンドは、次の条件をすべて満たしている場合にのみ有効です。

- クライアントレス認証をサポートするために、ネットワーク上にアクセス コントロール サーバが設定されている。
- ASA 上でクライアントレス認証がイネーブルになっている。
- NAC が ASA で設定されている。

このコマンドは Cisco NAC のフレームワーク実装にだけ適用されます。

例

次に、クライアントレス認証のユーザ名を sherlock に変更する例を示します。

```
ciscoasa(config)# eou clientless username sherlock
ciscoasa(config)#
```

次に、クライアントレス認証のユーザ名をデフォルト値である clientless に変更する例を示します。

```
ciscoasa(config)# no eou clientless username
ciscoasa(config)#
```

次に、クライアントレス認証のパスワードを secret に変更する例を示します。

```
ciscoasa(config)# eou clientless password secret
ciscoasa(config)#
```

次に、クライアントレス認証のパスワードをデフォルト値である clientless に変更する例を示します。

```
ciscoasa(config)# no eou clientless password
ciscoasa(config)#
```

関連コマンド

コマンド	説明
eou allow	NAC フレームワーク コンフィギュレーションでクライアントレス認証をイネーブルにします。
debug eou	EAP over UDP イベントのロギングをイネーブルにして、NAC フレームワーク メッセージをデバッグします。
debug nac	NAC フレームワーク イベントのロギングをイネーブルにします。

eou initialize（廃止）

(注) このコマンドをサポートする最後のリリースは、Version 9.1(1) でした。

1 つ以上の NAC フレームワーク セッションに割り当てられているリソースをクリアして、各セッションに対して新しい無条件のポスチャ検証を開始するには、特権 EXEC モードで **eou initialize** コマンドを使用します。

eou initialize {**all** | **group** *tunnel-group* | **ip** *ip-address*}

構文の説明

all	この ASA 上のすべての NAC フレームワーク セッションを再確認します。
group	トンネル グループに割り当てられているすべての NAC フレームワーク セッションを再確認します。
ip	単一の NAC フレームワーク セッションを再確認します。
ip-address	トンネルのリモート ピア側の IP アドレス。
tunnel-group	トンネルをセットアップするパラメータのネゴシエーションに使用されるトンネル グループの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.1(2)	このコマンドは廃止されました。

使用上のガイドライン

リモート ピアのポスチャが変更されたり、割り当てられているアクセス ポリシー（つまりダウンロードされた ACL）が変更されたりしたときに、セッションに割り当てられているリソースをクリアする場合は、このコマンドを使用します。このコマンドを入力すると、ポスチャ検証に使用される EAPoUDP アソシエーションおよびアクセス ポリシーが消去されます。再検証中には NAC のデフォルトの ACL が有効となるため、セッションを初期化するとユーザ トラフィックに影響する場合があります。このコマンドは、ポスチャ確認から免除されているピアには作用しません。

このコマンドは Cisco NAC のフレームワーク実装にだけ適用されます。

例

次に、すべての NAC フレームワーク セッションを初期化する例を示します。

```
ciscoasa# eou initialize all
ciscoasa
```

次に、tg1 というトンネル グループに割り当てられているすべての NAC フレームワーク セッションを初期化する例を示します。

```
ciscoasa# eou initialize group tg1
ciscoasa
```

次に、IP アドレス 209.165. 200.225 を持つエンドポイントの NAC フレームワーク セッションを再検証する例を示します。

```
ciscoasa# eou initialize 209.165.200.225
ciscoasa
```

関連コマンド

コマンド	説明
eou revalidate	1 つ以上の NAC フレームワーク セッションのポスチャ再確認をただちに強制します。
reval-period	NAC フレームワーク セッションでの成功したポスチャ確認の間隔を指定します。
sq-period	NAC フレームワーク セッションで正常に完了したポスチャ確認と、ホスト ポスチャの変化を調べる次回のクエリーとの間隔を指定します。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。
debug nac	NAC フレームワーク イベントのロギングをイネーブルにします。

eou max-retry（廃止）

(注) このコマンドをサポートする最後のリリースは、Version 9.1(1) でした。

ASA が EAP over UDP メッセージをリモート コンピュータに再送信する回数を変更するには、グローバル コンフィギュレーション モードで **eou max-retry** コマンドを使用します。デフォルト値を使用するには、このコマンドの **no** 形式を使用します。

eou max-retry *retries*

no eou max-retry

構文の説明

retries	再送信タイマーが期限切れになった場合に再送信する回数を制限します。1 ～ 3 の範囲の値を入力します。

デフォルト

デフォルト値は 3 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.1(2)	このコマンドは廃止されました。

使用上のガイドライン

このコマンドは、次の条件をすべて満たしている場合にのみ有効です。

- クライアントレス認証をサポートするために、ネットワーク上にアクセス コントロール サーバが設定されている。
- ASA 上でクライアントレス認証がイネーブルになっている。
- NAC が ASA で設定されている。

このコマンドは Cisco NAC のフレームワーク実装にだけ適用されます。

例

次に、EAP over UDP の再送信回数を 1 に制限する例を示します。

```
ciscoasa(config)# eou max-retry 1
ciscoasa(config)#
```

次に、EAP over UDP の再送信回数をデフォルト値である 3 に変更する例を示します。

```
ciscoasa(config)# no eou max-retry
ciscoasa(config)#
```

関連コマンド

eou timeout	NAC フレームワーク コンフィギュレーションで EAP over UDP メッセージをリモート ホストに送信した後に待機する秒数を変更します。
sq-period	NAC フレームワーク セッションで正常に完了したポスチャ確認と、ホスト ポスチャの変化を調べる次回のクエリーとの間隔を指定します。
debug eou	EAP over UDP イベントのロギングをイネーブルにして、NAC フレームワーク メッセージをデバッグします。
debug nac	NAC フレームワーク イベントのロギングをイネーブルにします。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。

eou port（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.1(1) でした。

NAC フレームワーク コンフィギュレーションにおいて、Cisco Trust Agent との EAP over UDP 通信に使用するポート番号を変更するには、グローバル コンフィギュレーション モードで **eou port** コマンドを使用します。デフォルト値を使用するには、このコマンドの **no** 形式を使用します。

eou port *port_number*

no eou port

構文の説明

port_number	EAP over UDP 通信用に指定するクライアント エンドポイントのポート番号。この番号は、Cisco Trust Agent に設定するポート番号です。1024 ～ 65535 の範囲の値を入力します。

デフォルト

デフォルト値は 21862 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.1(2)	このコマンドは廃止されました。

使用上のガイドライン

このコマンドは Cisco NAC のフレームワーク実装にだけ適用されます。

例

次に、EAP over UDP 通信のポート番号を 62445 に変更する例を示します。

```
ciscoasa(config)# eou port 62445
ciscoasa(config)#
```

次に、EAP over UDP 通信のポート番号をデフォルト値に変更する例を示します。

```
ciscoasa(config)# no eou port
ciscoasa(config)#
```

関連コマンド

debug eou	EAP over UDP イベントのロギングをイネーブルにして、NAC フレームワーク メッセージをデバッグします。
eou initialize	1 つ以上の NAC フレームワーク セッションに割り当てられているリソースを消去し、セッションごとに新しい無条件のポスチャ確認を開始します。
eou revalidate	1 つ以上の NAC フレームワーク セッションのポスチャ再確認をただちに強制します。
show vpn-session.db	VLAN マッピングと NAC の結果を含む、VPN セッションの情報を表示します。
show vpn-session_summary.db	VLAN マッピング セッション データを含む、IPsec、Cisco AnyConnect、NAC の各セッションの数を表示します。

eou revalidate（廃止）

(注) このコマンドをサポートする最後のリリースは、Version 9.1(1) でした。

1 つ以上の NAC フレームワーク セッションのポスチャ再検証をただちに実行するには、特権 EXEC モードで **eou revalidate** コマンドを使用します。

eou revalidate {**all** | **group** *tunnel-group* | **ip** *ip-address*}

構文の説明

all	この ASA 上のすべての NAC フレームワーク セッションを再確認します。
group	トンネル グループに割り当てられているすべての NAC フレームワーク セッションを再確認します。
ip	単一の NAC フレームワーク セッションを再確認します。
ip-address	トンネルのリモート ピア側の IP アドレス。
tunnel-group	トンネルをセットアップするパラメータのネゴシエーションに使用されるトンネル グループの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.1(2)	このコマンドは廃止されました。

使用上のガイドライン

ピアのポスチャ、または割り当てられているアクセス ポリシー(つまりダウンロードされた ACL が存在する場合その ACL)が変更された場合にこのコマンドを使用します。このコマンドは、新しい無条件のポスチャ検証を開始します。コマンド入力前に有効であったポスチャ検証および割り当てられているアクセス ポリシーは、新しいポスチャ検証に成功または失敗するまでは引き続き有効となります。このコマンドは、ポスチャ確認から免除されているピアには作用しません。

このコマンドは Cisco NAC のフレームワーク実装にだけ適用されます。

例

次に、すべての NAC フレームワーク セッションを再検証する例を示します。

```
ciscoasa# eou revalidate all
ciscoasa
```

次に、tg-1 というトンネル グループに割り当てられているすべての NAC フレームワーク セッションを再検証する例を示します。

```
ciscoasa# eou revalidate group tg-1
ciscoasa
```

次に、IP アドレス 209.165. 200.225 を持つエンドポイントの NAC フレームワーク セッションを再検証する例を示します。

```
ciscoasa# eou revalidate ip 209.165.200.225
ciscoasa
```

関連コマンド

コマンド	説明
debug eou	EAP over UDP イベントのロギングをイネーブルにして、NAC フレームワーク メッセージをデバッグします。
eou initialize	1 つ以上の NAC フレームワーク セッションに割り当てられているリソースを消去し、セッションごとに新しい無条件のポスチャ確認を開始します。
eou timeout	NAC フレームワーク コンフィギュレーションで EAP over UDP メッセージをリモート ホストに送信した後に待機する秒数を変更します。
reval-period	NAC フレームワーク セッションでの成功したポスチャ確認の間隔を指定します。
sq-period	NAC フレームワーク セッションで正常に完了したポスチャ確認と、ホスト ポスチャの変化を調べる次回のクエリーとの間隔を指定します。

eou timeout（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.1(1) でした。

NAC フレームワーク コンフィギュレーションにおいて、リモート ホストに対して EAP over UDP メッセージを送信した後に待機する秒数を変更するには、グローバル コンフィギュレーション モードで **eou timeout** コマンドを使用します。デフォルト値を使用するには、このコマンドの **no** 形式を使用します。

eou timeout {**hold-period** | **retransmit**} *seconds*

no eou timeout {**hold-period** | **retransmit**}

構文の説明

hold-period	EAPoUDP 再試行回数分の EAPoUDP メッセージを送信した後に待機する最大時間。**eou initialize** コマンドまたは **eou revalidate** コマンドを実行した場合も、このタイマーがクリアされます。このタイマーが期限切れになった場合、ASA はリモート ホストとの新しい EAP over UDP アソシエーションを開始します。
retransmit	1 回の EAPoUDP メッセージ送信後に待機する最大時間。リモート ホストから応答があると、このタイマーはクリアされます。**eou initialize** コマンドまたは **eou revalidate** コマンドを実行した場合も、このタイマーがクリアされます。タイマーが期限切れになると、ASA はリモート ホストに対して EAPoUDP メッセージを再送信します。
seconds	ASA が待機する秒数。hold-period 属性には 60 ～ 86400 の範囲の値を、retransmit 属性には 1 ～ 60 の範囲の値を入力します。

デフォルト

hold-period オプションのデフォルト値は 180 です。

retransmit オプションのデフォルト値は 3 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.1(2)	このコマンドは廃止されました。

使用上のガイドライン

このコマンドは Cisco NAC のフレームワーク実装にだけ適用されます。

例

次に、新しい EAP over UDP アソシエーションを開始するまでの待機時間を 120 秒に変更する例を示します。

```
ciscoasa(config)# eou timeout hold-period 120
ciscoasa(config)#
```

次に、新しい EAP over UDP アソシエーションを開始するまでの待機時間をデフォルト値に変更する例を示します。

```
ciscoasa(config)# no eou timeout hold-period
ciscoasa(config)#
```

次に、再送信タイマーを 6 秒に変更する例を示します。

```
ciscoasa(config)# eou timeout retransmit 6
ciscoasa(config)#
```

次に、再送信タイマーをデフォルト値に変更する例を示します。

```
ciscoasa(config)# no eou timeout retransmit
ciscoasa(config)#
```

関連コマンド

コマンド	説明
debug eou	EAP over UDP イベントのロギングをイネーブルにして、NAC フレームワーク メッセージをデバッグします。
eou max-retry	ASA がリモート コンピュータに対して EAP over UDP メッセージを再送信する回数を変更します。

erase

ファイル システムを消去して再フォーマットするには、特権 EXEC モードで **erase** コマンドを使用します。このコマンドは、非表示のシステム ファイルを含むすべてのファイルを上書きしてファイル システムを消去し、ファイル システムを再インストールします。

erase [**disk0:** | **disk1:** | **flash:**]

構文の説明

disk0:	(任意)内蔵コンパクト フラッシュ メモリ カードを指定し、続けてコロンを入力します。
disk1:	(任意)外部 コンパクト フラッシュ メモリ カード を指定し、続けてコロンを入力します。
flash:	(任意)内部フラッシュ メモリを指定し、続けてコロンを入力します。 ⚠ **注意** フラッシュ メモリを消去すると、フラッシュ メモリに保存されているライセンス情報も削除されます。フラッシュ メモリを消去する前に、ライセンス情報を保存してください。 ASA 5500 シリーズでは、**flash** キーワードは **disk0** のエイリアスです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

erase コマンドは、0xFF パターンを使用してフラッシュメモリ上のすべてのデータを消去し、空のファイルシステム割り当てテーブルをデバイスに書き換えます。

(非表示のシステム ファイルを除く)表示されているすべてのファイルを削除する場合は、**erase** コマンドではなく **delete /recursive** コマンドを入力します。

（注） Cisco ASA 5500 シリーズでは、**erase** コマンドを実行すると、ディスク上のすべてのユーザ データが 0xFF パターンを使用して破棄されます。一方、**format** コマンドはファイル システムの制御構造をリセットするだけです。ロウ ディスク読み取りツールを使用すると、この情報はまだ参照できる可能性があります。

例

次に、ファイル システムを消去して再フォーマットする例を示します。

```
ciscoasa# erase flash:
```

関連コマンド

コマンド	説明
delete	非表示のシステム ファイルを除く表示されているすべてのファイルを削除します。
形式	(非表示のシステム ファイルを含む)すべてのファイルを消去して、ファイル システムをフォーマットします。

esp

IPsec パススルー インスペクションで ESP トンネルおよび AH トンネルのパラメータを指定するには、パラメータ コンフィギュレーション モードで **esp** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

{**esp** | **ah**} [**per-client-max** *num*] [**timeout** *time*]

no {**esp** | **ah**} [**per-client-max** *num*] [**timeout** *time*]

構文の説明

esp	ESP トンネルのパラメータを指定します。
ah	AH トンネルのパラメータを指定します。
per-client-max *num*	1 つのクライアントからの最大トンネル数を指定します。
timeout *time*	ESP トンネルのアイドル タイムアウトを指定します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、UDP 500 のトラフィックを許可する例を示します。

```
ciscoasa(config)# access-list test-udp-acl extended permit udp any any eq 500
ciscoasa(config)# class-map test-udp-class
ciscoasa(config-pmap-c)# match access-list test-udp-acl

ciscoasa(config)# policy-map type inspect ipsec-pass-thru ipsec-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# esp per-client-max 32 timeout 0:06:00
ciscoasa(config-pmap-p)# ah per-client-max 16 timeout 0:05:00

ciscoasa(config)# policy-map test-udp-policy
ciscoasa(config-pmap)# class test-udp-class
ciscoasa(config-pmap-c)# inspect ipsec-pass-thru ipsec-map
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

established

確立された接続に基づく、ポートへの戻り接続を許可するには、グローバル コンフィギュレーション モードで **established** コマンドを使用します。**established** 機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

established *est_protocol dest_port* [*source_port*] [**permitto** *protocol port* [*-port*]] [**permitfrom** *protocol port*[*-port*]]

no established *est_protocol dest_port* [*source_port*] [**permitto** *protocol port* [*-port*]] [**permitfrom** *protocol port*[*-port*]]

構文の説明

est_protocol	確立された接続のルックアップに使用する IP プロトコル（UDP または TCP）を指定します。
dest_port	確立された接続のルックアップに使用する宛先ポートを指定します。
permitfrom	（任意）指定したポートから発信される戻りプロトコル接続を許可します。
permitto	（任意）指定したポートに着信する戻りプロトコル接続を許可します。
port [*-port*]	（任意）戻り接続の（UDP または TCP）宛先ポートを指定します。
protocol	（任意）戻り接続で使用される IP プロトコル（UDP または TCP）。
source_port	（任意）確立された接続のルックアップに使用する送信元ポートを指定します

デフォルト

デフォルトの設定は次のとおりです。

- *dest_port*：0（ワイルドカード）
- *source_port*：0（ワイルドカード）

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード **to** および **from** が CLI から削除されました。代わりにキーワード **permitto** および **permitfrom** を使用します。

使用上のガイドライン

established コマンドを使用すると、ASA 経由の発信接続の戻りアクセスを許可できます。このコマンドは、ネットワークから発信され、ASA によって保護されている元の接続、および外部ホストからの同じ 2 つのデバイス間の着信戻り接続に対して動作します。**established** コマンドでは、接続のルックアップに使用する宛先ポートを指定できます。宛先ポートを指定することによって、コマンドをより細かく制御でき、宛先ポートは既知であるが送信元ポートは不明であるプロトコルをサポートできます。**permitto** および **permitfrom** キーワードでは、リターン インバウンド接続を定義します。

注意 **established** コマンドでは、常に **permitto** キーワードおよび **permitfrom** キーワードを指定することを推奨します。これらのキーワードを指定しないで **established** コマンドを使用すると、外部システムに接続した場合にそれらのシステムから接続に関連する内部ホストに対して無制限に接続が可能となるため、セキュリティのリスクが発生します。このような状況は、内部システムの攻撃に悪用される可能性があります。

例

次に、**established** コマンドを正しく使用しない場合にセキュリティ違反が発生する可能性があることを示すいくつかの例を示します。

次に、内部システムから外部ホストのポート 4000 に TCP 接続を確立した場合に、外部ホストから任意のプロトコルを使用して任意のポートに戻り接続を確立できることを示す例を示します。

```
ciscoasa(config)# established tcp 4000 0
```

プロトコルで使用されるポートが規定されていない場合は、送信元ポートおよび宛先ポートに **0** を指定できます。ワイルドカード ポート(0)は、必要な場合にのみ使用します。

```
ciscoasa(config)# established tcp 0 0
```

(注) **established** コマンドが正しく動作するためには、クライアントは **permitto** キーワードで指定されたポートでリッスンする必要があります。

established コマンドは、**nat 0** コマンドとともに使用できます(**global** コマンドがない場合)。

(注) **established** コマンドは、PAT とともに使用することはできません。

ASA では、**established** コマンドを利用することによって XDMCP がサポートされます。

注意 ASA を通して XWindows システム アプリケーションを使用すると、セキュリティのリスクが発生する可能性があります。

デフォルトで、XDMCP はオンになっていますが、次のように **established** コマンドを入力しないとセッションが完了しません。

```
ciscoasa(config)# established tcp 6000 0 permitto tcp 6000 permitfrom tcp 1024-65535
```

established コマンドを入力すると、内部の XDMCP 実装ホスト（UNIX または Reflection X）から外部の XDMCP 実装 XWindows サーバにアクセスできます。UDP/177 ベースの XDMCP によって TCP ベースの XWindows セッションがネゴシエートされ、後続の TCP 戻り接続が許可されます。リターン トラフィックの送信元ポートは不明であるため、*source_port* フィールドには 0（ワイルドカード）を指定します。*dest_port* は 6000 + *n* となります。*n* は、ローカルのディスプレイ番号を表します。この値を変更するには、次の UNIX コマンドを使用します。

```
ciscoasa(config)# setenv DISPLAY hostname:displaynumber.screennumber
```

（ユーザ対話に基づいて）数多くの TCP 接続が生成され、これらの接続の送信元ポートが不明であるため、**established** コマンドが必要となります。宛先ポートのみがスタティックです。ASA では、XDMCP フィックスアップが透過的に実行されます。コンフィギュレーションは必要ありませんが、TCP セッションを確立できるように **established** コマンドを入力する必要があります。

次に、送信元ポート C からポート B 宛のプロトコル A を使用した 2 つのホスト間の接続の例を示します。ASA 経由でプロトコル D（プロトコル D はプロトコル A とは異なっていてもかまいません）による戻り接続を許可するには、送信元ポートがポート F に、宛先ポートがポート E に対応している必要があります。

```
ciscoasa(config)# established A B C permitto D E permitfrom D F
```

次に、TCP 宛先ポート 6060、および任意の送信元ポートを使用して、内部ホストから外部ホストに接続を開始する例を示します。ASA では、TCP 宛先ポート 6061 および任意の TCP 送信元ポートを使用したホスト間のリターン トラフィックが許可されます。

```
ciscoasa(config)# established tcp 6060 0 permitto tcp 6061 permitfrom tcp 0
```

次に、UDP 宛先ポート 6060、および任意の送信元ポートを使用して、内部ホストから外部ホストに接続を開始する例を示します。ASA では、TCP 宛先ポート 6061 および TCP 送信元ポート 1024 ～ 65535 を使用したホスト間のリターン トラフィックが許可されます。

```
ciscoasa(config)# established udp 6060 0 permitto tcp 6061 permitfrom tcp 1024-65535
```

次に、ローカル ホストから外部ホストにポート 9999 への TCP 接続を開始する例を示します。この例では、外部ホストのポート 4242 からローカル ホストのポート 5454 へのパケットが許可されます。

```
ciscoasa(config)# established tcp 9999 permitto tcp 5454 permitfrom tcp 4242
```

関連コマンド

コマンド	説明
clear configure established	確立されたコマンドをすべて削除します。
show running-config established	確立されている接続に基づく、許可済みの着信接続を表示します。

event crashinfo

ASA でクラッシュが発生した場合にイベント マネージャ アプレットをトリガーするには、イベント マネージャ アプレット コンフィギュレーション モードで **event crashinfo** コマンドを使用します。クラッシュ イベントを削除するには、このコマンドの **no** 形式を使用します。

event crashinfo

no event crashinfo

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
イベント マネージャ アプレット コンフィギュレーション	• 対応	• Yes	• 対応	—	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

output コマンドの値に関係なく、**action** コマンドはクラッシュ情報ファイルに送られます。出力は、**show tech** コマンドの前に生成されます。

(注) ASA がクラッシュした場合、その状態は通常は不明です。一部の CLI コマンドは、この状態のときに実行するのは安全でない場合があります。

例

次に、ASA がクラッシュした場合にアプレットをトリガーする例を示します。

```
ciscoasa(config-applet)# event crashinfo
```

関連コマンド

コマンド	説明
event none	イベント マネージャ アプレットを手動で呼び出します。
event syslog id	イベント マネージャ アプレットに syslog イベントを追加します。
event timer absolute time	絶対イベント タイマーを設定します。
event timer countdown time	カウントダウン タイマー イベントを設定します。
event timer watchdog time	ウォッチドッグ タイマー イベントを設定します。

event manager applet

イベントをアクションや出力とリンクするイベント マネージャ アプレットを作成または編集するには、グローバル コンフィギュレーション モードで event manager applet コマンドを使用します。イベント マネージャ アプレットを削除するには、このコマンドの **no** 形式を使用します。

event manager applet *name*

no event manager applet *name*

構文の説明

name	イベント マネージャ アプレットの名前を指定します。名前には最大 32 文字の長さを使用できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

イベント マネージャ アプレット コンフィギュレーション モードを開始するには、**event manager applet** コマンドを使用します。

例

次に、イベント マネージャ アプレットを作成し、イベント マネージャ アプレット コンフィギュレーション モードを開始する例を示します。

```
ciscoasa(config)# event manager applet appletexample1
ciscoasa(config-applet)#
```

関連コマンド

コマンド	説明
description	アプレットについて説明します。
event manager run	イベント マネージャ アプレットを実行します。

コマンド	説明
show event manager	設定された各イベント マネージャ アプレットの統計情報を表示します。
debug event manager	イベント マネージャのデバッグ トレースを管理します。

event memory-logging-wrap

メモリ ロギングのラップ イベント トリガーを設定するには、イベント マネージャ アプレット コンフィギュレーション モードで **event memory-logging-wrap** コマンドを使用します。

event memory-logging-wrap

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
イベント マネージャ アプレット コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

メモリ ロギングのラップがイネーブルの場合、メモリ ロガーがイベントをイベント マネージャに送信し、設定されたアプレットをトリガーします。

例

次に、すべてのメモリ割り当てを記録するアプレットを示します。

```
ciscoasa(config-applet)# event manager applet memlog
ciscoasa(config-applet)# event memory-logging-wrap
ciscoasa(config-applet)# action 0 cli command "show memory logging wrap"
ciscoasa(config-applet)# output file append disk0:/memlog.log
```

関連コマンド

コマンド	説明
memory logging	メモリ ロギングをイネーブルにします。
show memory logging	メモリ ロギングの結果を表示します。

event none

イベント マネージャ アプレットを手動で呼び出すには、イベント マネージャ アプレット コンフィギュレーション モードで **event none** コマンドを使用します。手動呼び出しを削除するには、このコマンドの **no** 形式を使用します。

event none

no event none

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
イベント マネージャ アプレット コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

event none コマンドを使用して他のイベントを設定できます。

例

次に、イベント マネージャ アプレットを手動で呼び出す例を示します。

```
ciscoasa(config-applet)# event none
```

関連コマンド

コマンド	説明
event crashinfo	ASA でクラッシュが発生した場合にイベント マネージャ アプレットをトリガーします。
event syslog id	イベント マネージャ アプレットに syslog イベントを追加します。
event timer absolute time	絶対イベント タイマーを設定します。

コマンド	説明
event timer countdown time	カウントダウン タイマー イベントを設定します。
event timer watchdog time	ウォッチドッグ タイマー イベントを設定します。

event syslog id

イベント マネージャ アプレットに syslog イベントを追加するには、イベント マネージャ アプレット コンフィギュレーション モードで **event syslog id** コマンドを使用します。イベント マネージャ アプレットから syslog イベントを削除するには、このコマンドの **no** 形式を使用します。

event syslog id *nnnnnn*[*-nnnnnn*] [**occurs** *n*] [**period** *seconds*]

no event syslog id *nnnnnn*[*-nnnnnn*] [**occurs** *n*] [**period** *seconds*]

構文の説明

nnnnnn	syslog メッセージ ID を指定します。
occurs *n*	アプレットを呼び出すために syslog メッセージが発生する必要がある回数を示します。デフォルトは 1 です。有効な値は、1 ～ 4294967295 です。
period *seconds*	イベントが発生する必要がある秒数を示し、アプレットが呼び出される頻度を設定された期間中最大で 1 回に制限します。有効な値は、0 ～ 604800 です。値 0 は、期間が定義されていないことを示しています。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
イベント マネージャ アプレット コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

アプレットをトリガーする単一の syslog メッセージまたは syslog メッセージの範囲を指定するには、**event syslog id** コマンドを使用します。

例

次に、syslog メッセージ 106201 がアプレットをトリガーする例を示します。

```
ciscoasa(config-applet)# event syslog id 106201
```

関連コマンド

コマンド	説明
event crashinfo	ASA でクラッシュが発生した場合にイベント マネージャ アプレットをトリガーします。
event none	イベント マネージャ アプレットを手動で呼び出します。
event timer absolute time	絶対イベント タイマーを設定します。
event timer countdown time	カウントダウン タイマー イベントを設定します。
event timer watchdog time	ウォッチドッグ タイマー イベントを設定します。

event timer

タイマー イベントを設定するには、イベント マネージャ アプレット コンフィギュレーション モードで **event timer** コマンドを使用します。タイマー イベントを削除するには、このコマンドの **no** 形式を使用します。

event timer {watchdog time *seconds* **| countdown time** *seconds* **| absolute time** *hh:mm:ss***}**

no event timer {watchdog time *seconds* **| countdown time** *seconds* **| absolute time** *hh:mm:ss***}**

構文の説明

absolute time	イベントが 1 日 1 回指定した時間に発生し、自動的に再開されることを指定します。
countdown time	イベントが 1 回発生し、そのイベントが削除された後に再度追加されない限り再開されないことを指定します。
hh:mm:ss	時刻形式を指定します。時間範囲は 00:00:00（深夜）～ 23:59:59 です。
seconds	秒数を指定します。有効な値の範囲は 0 ～604800 です。0 の値の場合、このタイマーはディセーブルになります。
watchdog time	イベントが設定された期間ごとに 1 回発生し、自動的に再開されることを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
イベント マネージャ アプレット コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

1 日の指定した時間にイベントが 1 回発生し、自動的に再開されるようにするには、**event timer absolute time** コマンドを使用します。

イベントが 1 回発生し、そのイベントを削除した後に再度追加しない限り再開されないようにするには、**event timer countdown time** コマンドを使用します。

指定した期間ごとにイベントが 1 回発生し、自動的に再開されるようにするには、**event timer watchdog time** コマンドを使用します。

例

次に、1 日の指定した時間が表示された場合にイベントを発生させる例を示します。

```
ciscoasa(config-applet)# event timer absolute time 10:30:20
```

次に、1 日の指定した時間が表示された場合にイベントを発生させる例を示します。

```
ciscoasa(config-applet)# event timer countdown time 10:30:20
```

次に、イベントが 1 日 1 回発生し、自動的に再開されるようにする例を示します。

```
ciscoasa(config-applet)# event timer watchdog time 30
```

関連コマンド

コマンド	説明
event crashinfo	ASA でクラッシュが発生した場合にイベント マネージャ アプレットをトリガーします。
event none	イベント マネージャ アプレットを手動で呼び出します。
event syslog id	イベント マネージャ アプレットに syslog イベントを追加します。
event timer countdown time	カウントダウン タイマー イベントを設定します。
event timer watchdog time	ウォッチドッグ タイマー イベントを設定します。

exceed-mss

3 ウェイ ハンドシェイクでピアによって設定された TCP 最大セグメント サイズ（MSS）を超えるデータ長のパケットを許可またはドロップするには、tcp マップ コンフィギュレーション モードで **exceed-mss** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

exceed-mss {**allow** | **drop**}

no exceed-mss {**allow** | **drop**}

構文の説明

allow	MSS を超えるパケットを許可します。この設定は、デフォルトです。
drop	MSS を超えるパケットをドロップします。

デフォルト

パケットは、デフォルトで許可されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
TCP マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(4)/8.0(4)	デフォルトが **drop** から **allow** に変更されました。

使用上のガイドライン

tcp-map コマンドはモジュラ ポリシー フレームワーク インフラストラクチャと一緒に使用されます。**class-map** コマンドを使用してトラフィックのクラスを定義し、**tcp-map** コマンドで TCP インスペクションをカスタマイズします。**policy-map** コマンドを使用して、新しい TCP マップを適用します。**service-policy** コマンドで、TCP インスペクションをアクティブにします。

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。スリーウェイ ハンドシェイクでピアによって設定された TCP 最大セグメント サイズを超えるデータ長の TCP パケットをドロップするには、tcp マップ コンフィギュレーション モードで **exceed-mss** コマンドを使用します。

例

次に、MSS を超えた場合にポート 21 のフローをドロップする例を示します。

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# exceed-mss drop
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match port tcp eq ftp
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection advanced-options	TCP 正規化を含む、高度な接続機能を設定します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

exempt-list

ポスチャ検証を免除されるリモート コンピュータ タイプのリストにエントリを追加するには、nac ポリシー nac フレームワーク コンフィギュレーション モードで **exempt-list** コマンドを使用します。免除リストからエントリを削除するには、このコマンドの **no** 形式を使用して、削除するエントリのオペレーティング システムおよび ACL を指定します。

exempt-list os "*os-name*" [**disable** | **filter** *acl-name* [**disable**]]

no exempt-list os "*os-name*" [**disable** | **filter** *acl-name* [**disable**]]

構文の説明

acl-name	ASA コンフィギュレーションに存在する ACL の名前。指定する場合は、**filter** キーワードの後に指定する必要があります。
disable	次の 2 つの機能のいずれかを実行します。 • "os-name" の後に入力した場合、ASA は、指定したオペレーティング システムを実行するリモート ホストで免除を行わず、NAC ポスチャ検証を適用します。 • *acl-name* の後に入力した場合、ASA は指定したオペレーティング システムを免除しますが、関連するトラフィックに ACL を割り当てません。
filter	コンピュータのオペレーティング システムが *os name* に一致する場合にトラフィックをフィルタリングするための ACL を適用します。**filter** と *acl-name* のペアは省略可能です。
os	オペレーティング システムをポスチャ検証から免除します。
os name	オペレーティング システム名。名前にスペースが含まれている場合にのみ引用符が必要です（たとえば "Windows XP"）。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
nac ポリシー nac フレームワーク コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.0(2)	コマンド名が **vpn-nac-exempt** から **exempt-list** に変更されました。コマンドが、グループ ポリシー コンフィギュレーション モードから nac ポリシー nac フレームワーク コンフィギュレーション モードに移動されました。

使用上のガイドライン

コマンドでオペレーティング システムを指定しても、例外リストに追加済みのエントリは上書きされません。免除する各オペレーティング システムおよび ACL に対して 1 つずつコマンドを入力します。

no exempt-list コマンドを入力すると、NAC フレームワーク ポリシーからすべての免除が削除されます。エントリを指定してこのコマンドの **no** 形式を発行すると、そのエントリが免除リストから削除されます。

NAC ポリシーに関連付けられている免除リストからすべてのエントリを削除するには、キーワードを指定しないでこのコマンドの **no** 形式を使用します。

例

次に、ポスチャ検証を免除するコンピュータのリストに Windows XP を実行するすべてのホストを追加する例を示します。

```
ciscoasa(config-group-policy)# exempt-list os "Windows XP"
ciscoasa(config-group-policy)
```

次に、Windows XP を実行するすべてのホストを免除して、これらのホストのトラフィックに ACL acl-1 を適用する例を示します。

```
ciscoasa(config-nac-policy-nac-framework)# exempt-list os "Windows XP" filter acl-1
ciscoasa(config-nac-policy-nac-framework)
```

次に、免除リストから上記の例と同じエントリを削除する例を示します。

```
ciscoasa(config-nac-policy-nac-framework)# no exempt-list os "Windows XP" filter acl-1
ciscoasa(config-nac-policy-nac-framework)
```

次に、免除リストからすべてのエントリを削除する例を示します。

```
ciscoasa(config-nac-policy-nac-framework)# no exempt-list
ciscoasa(config-nac-policy-nac-framework)
```

関連コマンド

コマンド	説明
debug nac	NAC フレームワーク イベントのロギングをイネーブルにします。
nac-policy	Cisco NAC ポリシーを作成してアクセスし、そのタイプを指定します。
nac-settings	NAC ポリシーをグループ ポリシーに割り当てます。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。
show vpn-session_summary.db	IPsec、Cisco AnyConnect、および NAC の各セッションの数を表示します。

exit

現在のコンフィギュレーション モードを終了するか、特権 EXEC モードまたはユーザ EXEC モードからログアウトするには、**exit** コマンドを使用します。

exit

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

キー シーケンス Ctrl+Z を使用して、グローバル コンフィギュレーション（および上位の）モードを終了することもできます。このキー シーケンスは、特権 EXEC モードまたはユーザ EXEC モードでは動作しません。

特権 EXEC モードまたはユーザ EXEC モードで **exit** コマンドを入力すると、ASA からログアウトします。特権 EXEC モードからユーザ EXEC モードに戻るには、**disable** コマンドを使用します。

例

次に、**exit** コマンドを使用してグローバル コンフィギュレーション モードを終了し、セッションからログアウトする方法の例を示します。

```
ciscoasa(config)# exit
ciscoasa# exit

Logoff
```

次に、**exit** コマンドを使用してグローバル コンフィギュレーション モードを終了し、その後 **disable** コマンドを使用して特権 EXEC モードを終了する例を示します。

```
ciscoasa(config)# exit
ciscoasa# disable
ciscoasa#
```

関連コマンド

コマンド	説明
quit	コンフィギュレーション モードを終了するか、特権 EXEC モードまたはユーザ EXEC モードからログアウトします。

exp-flow-control

IP オプション インスペクションにおいて、パケット ヘッダー内に実験的フロー制御（FINN）オプションが存在する場合のアクションを定義するには、パラメータ コンフィギュレーション モードで **exp-flow-control** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

exp-flow-control action {allow | clear}

no exp-flow-control action {allow | clear}

構文の説明

allow	実験的フロー制御 IP オプションを含むパケットを許可します。
clear	実験的フロー制御オプションをパケット ヘッダーから削除してから、パケットを許可します。

デフォルト

デフォルトでは、IP オプション インスペクションは、実験的フロー制御 IP オプションを含むパケットをドロップします。

IP オプション インスペクション ポリシー マップで **default** コマンドを使用するとデフォルト値を変更できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IP オプション インスペクション ポリシー マップで設定できます。

IP オプション インスペクションを設定して、どの IP パケットが所定の IP オプションを持ち、ASA を通過できるかを制御できます。変更せずにパケットを通過させたり、指定されている IP オプションをクリアしてからパケットを通過させたりできます。

例

次に、IP オプション インスペクションのアクションをポリシー マップで設定する例を示します。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# exp-flow-control action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

exp-measure

IP オプション インスペクションにおいて、パケット ヘッダー内に実験的測定（ZSU）オプションが存在する場合のアクションを定義するには、パラメータ コンフィギュレーション モードで **exp-measure** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

exp-measure action {allow | clear}

no exp-measure action {allow | clear}

構文の説明

allow	実験的測定 IP オプションを含むパケットを許可します。
clear	実験測定オプションをパケット ヘッダーから削除してから、パケットを許可します。

デフォルト

デフォルトでは、IP オプション インスペクションは、実験的測定 IP オプションを含むパケットをドロップします。

IP オプション インスペクション ポリシー マップで **default** コマンドを使用するとデフォルト値を変更できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IP オプション インスペクション ポリシー マップで設定できます。

IP オプション インスペクションを設定して、どの IP パケットが所定の IP オプションを持ち、ASA を通過できるかを制御できます。変更せずにパケットを通過させたり、指定されている IP オプションをクリアしてからパケットを通過させたりできます。

例

次に、IP オプション インスペクションのアクションをポリシー マップで設定する例を示します。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# exp-measure action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

expiry-time

再検証しないでオブジェクトをキャッシュする有効期限を設定するには、キャッシュ コンフィギュレーション モードで **expiry-time** コマンドを使用します。コンフィギュレーションから有効期限を削除してデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

expiry-time *time*

no expiry-time

構文の説明

時刻	ASA が再検証しないでオブジェクトをキャッシュする時間（分）。

デフォルト

デフォルトは 1 分です。

コマンド モード

次の表は、このコマンドを入力するモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
キャッシュ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

有効期限とは、ASA が再検証しないでオブジェクトをキャッシュする時間（分）を指します。再検証では、内容が再度チェックされます。

例

次に、有効期限を 13 分に設定する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# cache
ciscoasa(config-webvpn-cache)#expiry-time 13
ciscoasa(config-webvpn-cache)#
```

関連コマンド

コマンド	説明
cache	webvpn キャッシュ コンフィギュレーション モードを開始します。
cache-compressed	WebVPN キャッシュの圧縮を設定します。

コマンド	説明
disable	キャッシュをディセーブルにします。
lmfactor	最終変更時刻のタイムスタンプだけを持つオブジェクトのキャッシュに関する再確認ポリシーを設定します。
max-object-size	キャッシュするオブジェクトの最大サイズを定義します。
min-object-size	キャッシュするオブジェクトの最小サイズを定義します。

export

証明書をクライアントにエクスポートすることを指定するには、CTL プロバイダー コンフィギュレーション モードで **export** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

export certificate *trustpoint_name*

no export certificate [*trustpoint_name*]

構文の説明

certificate *trustpoint_name*　クライアントにエクスポートする証明書を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
Ctl プロバイダー コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

CTL プロバイダー コンフィギュレーション モードで **export** コマンドを使用して、証明書をクライアントにエクスポートすることを指定します。トラストポイント名は、**crypto ca trustpoint** コマンドで定義します。証明書は、CTL クライアントで構成された CTL ファイルに追加されます。

例

次の例は、CTL プロバイダー インスタンスを作成する方法を示しています。

```
ciscoasa(config)# ctl-provider my_ctl
ciscoasa(config-ctl-provider)# client interface inside 172.23.45.1
ciscoasa(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
ciscoasa(config-ctl-provider)# export certificate ccm_proxy
ciscoasa(config-ctl-provider)# ctl install
```

関連コマンド

コマンド	説明
ctl	CTL クライアントの CTL ファイルを解析し、トラストポイントをインストールします。
ctl-provider	CTL プロバイダー コンフィギュレーション モードで CTL プロバイダー インスタンスを設定します。
クライアント	CTL プロバイダーへの接続が許可されるクライアントを指定し、クライアント認証用のユーザ名とパスワードを指定します。
service	CTL プロバイダーがリッスンするポートを指定します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

export webvpn AnyConnect-customization

AnyConnect クライアント GUI をカスタマイズするカスタマイゼーション オブジェクトをエクスポートするには、特権 EXEC モードで **export webvpn AnyConnect-customization** コマンドを使用します。

export webvpn AnyConnect-customization type *type* **platform** *platform* **name** *name*

構文の説明

name	カスタマイゼーション オブジェクトを識別する名前。最大数は 64 文字です。
type	カスタマイゼーションのタイプ: • バイナリ:AnyConnect GUI を置き換える実行可能ファイル。 • トランスフォーム:MSI をカスタマイズするトランスフォーム。
url	XML カスタマイゼーション オブジェクトをエクスポートする *URL/filename* 形式のリモート パスとファイル名(最大 255 文字)。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

AnyConnect カスタマイゼーション オブジェクトとは、キャッシュ メモリ内にあり、AnyConnect クライアント ユーザに表示される GUI 画面をカスタマイズする XML ファイルです。カスタマイゼーション オブジェクトをエクスポートすると、XML タグを含む XML ファイルが、指定した URL に作成されます。

カスタマイゼーション オブジェクトによって作成される *Template* という名前の XML ファイルには、空の XML タグが含まれており、新しいカスタマイゼーション オブジェクトを作成するための基礎として利用できます。このオブジェクトは変更したり、キャッシュ メモリから削除したりすることはできませんが、エクスポートし、編集して、新しいカスタマイゼーション オブジェクトとして再度 ASA にインポートできます。

Template の内容は、DfltCustomization オブジェクトの初期状態と同じです。

AnyConnect GUI で使用されるリソース ファイルの完全なリストおよびそれらのファイル名については『*AnyConnect VPN Client Administrator Guide*』を参照してください。

例

次に、AnyConnect GUI で使用されるシスコのロゴをエクスポートする例を示します。

```
ciscoasa# export webvpn AnyConnect-customization type resource company_logo.bmp
tftp://209.165.200.225/dflt_custom
!!!!!!!!!!!!!!!!INFO: Customization object 'DfltCustomization' was exported to
tftp://10.86.240.197/dflt_custom
ciscoasa#
```

関連コマンド

コマンド	説明
import webvpn customization	XML ファイルをカスタマイゼーション オブジェクトとしてキャッシュ メモリにインポートします。
revert webvpn customization	キャッシュ メモリからカスタマイゼーション オブジェクトを削除します。
show import webvpn customization	キャッシュ メモリにあるカスタマイゼーション オブジェクトに関する情報を表示します。

export webvpn customization

クライアントレス SSL VPN ユーザに表示される画面をカスタマイズするカスタマイゼーション オブジェクトをエクスポートするには、特権 EXEC モードで **export webvpn customization** コマンドを使用します。

export webvpn customization *name url*

構文の説明

name	カスタマイゼーション オブジェクトを識別する名前。最大数は 64 文字です。
url	XML カスタマイゼーション オブジェクトをエクスポートする *URL/filename* 形式のリモート パスとファイル名（最大 255 文字）。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

カスタマイゼーション オブジェクトとは、キャッシュ メモリ内にあり、クライアントレス SSL VPN ユーザに表示される画面（ログイン画面、ログアウト画面、ポータル ページ、使用可能な言語など）をカスタマイズする XML ファイルです。カスタマイゼーション オブジェクトをエクスポートすると、XML タグを含む XML ファイルが、指定した URL に作成されます。

カスタマイゼーション オブジェクトによって作成される *Template* という名前の XML ファイルには、空の XML タグが含まれており、新しいカスタマイゼーション オブジェクトを作成するための基礎として利用できます。このオブジェクトは変更したり、キャッシュ メモリから削除したりすることはできませんが、エクスポートし、編集して、新しいカスタマイゼーション オブジェクトとして再度 ASA にインポートできます。

Template の内容は、DfltCustomization オブジェクトの初期状態と同じです。

export webvpn customization コマンドを使用してカスタマイゼーション オブジェクトをエクスポートし、XML タグを変更し、**import webvpn customization** コマンドを使用して新しいオブジェクトとしてファイルをインポートできます。

例

次に、デフォルトのカスタマイゼーション オブジェクト（DfltCustomization）をエクスポートして、dflt_custom という名前の XML ファイルを作成する例を示します。

```
ciscoasa# export webvpn customization DfltCustomization tftp://209.165.200.225/dflt_custom
!!!!!!!!!!!!!!!!INFO: Customization object 'DfltCustomization' was exported to
tftp://10.86.240.197/dflt_custom
ciscoasa#
```

関連コマンド

コマンド	説明
import webvpn customization	XML ファイルをカスタマイゼーション オブジェクトとしてキャッシュ メモリにインポートします。
revert webvpn customization	キャッシュ メモリからカスタマイゼーション オブジェクトを削除します。
show import webvpn customization	キャッシュ メモリにあるカスタマイゼーション オブジェクトに関する情報を表示します。

export webvpn plug-in

ASA のフラッシュ デバイスからプラグインをエクスポートするには、特権 EXEC モードで **export webvpn plug-in** コマンドを入力します。

import webvpn plug-in protocol *protocol URL*

構文の説明

protocol	• **rdp** Remote Desktop Protocol プラグインにより、リモート ユーザは Microsoft Terminal Services が実行するコンピュータに接続できます。シスコでは、変更を加えずにこのプラグインを再配布しています。オリジナルを掲載している Web サイトは、http://properjavardp.sourceforge.net/ です。 • **ssh,telnet** セキュア シェル プラグインにより、リモート ユーザがリモート コンピュータへのセキュア チャネルを確立したり、リモート ユーザが Telnet を使用してリモート コンピュータに接続したりできます。シスコでは、変更を加えずにこのプラグインを再配布しています。オリジナルを掲載している Web サイトは、http://javassh.org/ です。 **注意** **export webvpn plug-in protocol ssh,telnet** *URL* コマンドは、SSH と Telnet の*両方のプラグイン*をエクスポートします。SSH 用と Telnet 用にこのコマンドをそれぞれ入力*しないでください*。**ssh,telnet** ストリングを入力する場合は、両者の間にスペースは挿入*しません*。 • **vnc** Virtual Network Computing プラグインを使用すると、リモート ユーザはリモート デスクトップ共有をオンにしたコンピュータを、モニタ、キーボード、およびマウスを使用して表示および制御できます。シスコでは、変更を加えずにこのプラグインを再配布しています。オリジナルを掲載している Web サイトは、http://www.tightvnc.com/ です。
URL	リモート デバイスへのパス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

プラグインをエクスポートしても、フラッシュから削除されることはありません。エクスポートすると、指定した URL にプラグインのコピーが作成されます。

例

次のコマンドでは、RDP プラグインをエクスポートしています。

```
ciscoasa# export webvpn plug-in protocol rdp tftp://209.165.201.22/plugins/rdp-plugin.jar
```

関連コマンド

コマンド	説明
import webvpn plugin	指定されたプラグインをローカル デバイスから ASA フラッシュにインポートします。
revert webvpn plug-in protocol	ASA のフラッシュ デバイスから指定されたプラグインを削除します。
show import webvpn plug-in	ASA のフラッシュ デバイスに存在するプラグインのリストを示します。

export webvpn mst-translation

AnyConnect インストーラ プログラムを変換する Microsoft トランスフォーム（MST）をエクスポートするには、特権 EXEC モードで **export webvpn mst-translation** コマンドを使用します。

export webvpn mst-translation *component* **language** *language URL*

構文の説明

component	この MST が適用されるコンポーネント。有効な選択肢は AnyConnect のみです。
language	エクスポートされる MST の言語コード。ブラウザで必要とされるのと同じ形式のコードを使用します。
URL	トランスフォームをエクスポートする *URL/filename* 形式のリモート パスとファイル名（最大 255 文字）。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

AnyConnect クライアント GUI と同様に、クライアント インストーラ プログラムに表示されるメッセージを翻訳できます。ASA はトランスフォームを使用して、インストーラに表示されるメッセージを翻訳します。トランスフォームによってインストレーションが変更されますが、元のセキュリティ署名 MSI は変化しません。これらのトランスフォームではインストーラ画面だけが翻訳され、クライアント GUI 画面は翻訳されません。

言語にはそれぞれ独自のトランスフォームがあります。トランスフォームは Orca などのトランスフォーム エディタで編集して、メッセージの文字列を変更できます。その後、トランスフォームを ASA にインポートします。ユーザがクライアントをダウンロードすると、クライアントはコンピュータの目的の言語（オペレーティング システムのインストール時に指定されたロケール）を検出し、該当するトランスフォームを適用します。

現時点では、30 の言語に対応するトランスフォームが用意されています。これらのトランスフォームは、cisco.com の AnyConnect クライアント ソフトウェア ダウンロード ページから、次の .zip ファイルで入手できます。

anyconnect-win-<VERSION>-web-deploy-k9-lang.zip

このファイルの <VERSION> は、AnyConnect のリリース バージョン（2.2.103 など）を表します。

例

次に、英語のトランスフォームを AnyConnect_Installer_English としてエクスポートする例を示します。

```
ciscoasa# export webvpn mst-translation AnyConnect language es
tftp://209.165.200.225/AnyConnect_Installer_English
```

関連コマンド

コマンド	説明
import webvpn customization	XML ファイルをカスタマイゼーション オブジェクトとしてキャッシュ メモリにインポートします。
revert webvpn customization	キャッシュ メモリからカスタマイゼーション オブジェクトを削除します。
show import webvpn customization	キャッシュ メモリにあるカスタマイゼーション オブジェクトに関する情報を表示します。

export webvpn translation-table

SSL VPN 接続を確立するリモート ユーザに表示される用語を変換するために使用される変換テーブルをエクスポートするには、特権 EXEC モードで **export webvpn translation-table** コマンドを使用します。

export webvpn translation-table *translation_domain* {**language** *language* | **template**} *url*

構文の説明

language	事前にインポート済みの変換テーブルの名前を指定します。値は、ブラウザの言語オプションの表現に従って入力します。
translation_domain	機能エリアおよび関連するメッセージです。表14-1 に、使用可能な変換ドメインを示します。
url	オブジェクトの URL を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

ASA では、ブラウザベースのクライアントレス SSL VPN 接続を開始するユーザに表示されるポータルと画面、および AnyConnect VPN クライアント ユーザに表示されるユーザ インターフェイスで使用される言語を変換できます。

リモート ユーザに表示される各機能エリアとそのメッセージには独自の変換ドメインがあります。この変換ドメインは *translation_domain* 引数で指定します。表14-1 に、変換ドメインと変換される機能エリアを示します。

表14-1　変換ドメインと影響を受ける機能エリア

変換ドメイン	変換される機能エリア
AnyConnect	Cisco AnyConnect VPN Client のユーザ インターフェイスに表示されるメッセージ。
バナー	リモート ユーザに表示されるバナーと、VPN アクセスが拒否されたときのメッセージ。
CSD	Cisco Secure Desktop（CSD）のメッセージ。
customization	ログイン ページ、ログアウト ページ、ポータル ページのメッセージ、およびユーザによるカスタマイズが可能なすべてのメッセージ。
plugin-ica	Citrix プラグインのメッセージ。
plugin-rdp	Remote Desktop Protocol プラグインのメッセージ。
plugin-telnet,ssh	Telnet および SSH プラグインのメッセージ。
plugin-vnc	VNC プラグインのメッセージ。
PortForwarder	ポート フォワーディング ユーザに表示されるメッセージ。
url-list	ユーザがポータル ページの URL ブックマークに指定するテキスト。
webvpn	カスタマイズできないすべてのレイヤ 7 メッセージ、AAA メッセージ、およびポータル メッセージ。

変換テンプレートは変換テーブルと同じ形式の XML ファイルですが、変換内容はすべて空です。ASA のソフトウェア イメージ パッケージには、標準機能の一部として各ドメイン用のテンプレートが含まれています。プラグインのテンプレートはプラグインに付属しており、独自の変換ドメインを定義します。クライアントレス ユーザのログインおよびログアウト ページ、ポータル ページ、および URL ブックマークはカスタマイズが可能なため、ASA は customization および url-list 変換ドメイン テンプレートをダイナミックに生成し、テンプレートは変更内容をこれらの機能エリアに自動的に反映させます。

以前にインポートされた変換テーブルをエクスポートすると、URL の場所にそのテーブルの XML ファイルが作成されます。**show import webvpn translation-table** コマンドを使用して、使用可能なテンプレート、およびインポート済みのテーブルのリストを表示できます。

export webvpn translation-table コマンドを使用してテンプレートまたは変換テーブルをダウンロードし、メッセージを変更し、**import webvpn translation-table** コマンドを使用して変換テーブルをインポートします。

例

次に、変換ドメイン *customization* 用のテンプレートをエクスポートする例を示します。このドメインは、クライアントレス SSL VPN 接続を確立するリモート ユーザがカスタマイズおよび表示可能なログイン ページ、ログアウト ページ、ポータル ページ、およびすべてのメッセージを変換するために使用します。ASA は、*Sales* という名前の XML ファイルを作成します。

```
ciscoasa# export webvpn translation-table customization template
tftp://209.165.200.225/Sales
ciscoasa# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

次に、*zh* という名前の、以前にインポートされた中国語用変換テーブルをエクスポートする例を示します。この短縮形 zh は、Microsoft Internet Explorer ブラウザの [インターネット オプション] で中国語に指定されている短縮形に準拠しています。ASAは、*Chinese* という名前の XML ファイルを作成します。

```
ciscoasa# export webvpn translation-table customization language zh
tftp://209.165.200.225/Chinese
ciscoasa# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

関連コマンド

コマンド	説明
import webvpn translation-table	変換テーブルをインポートします。
revert	キャッシュ メモリから変換テーブルを削除します。
show import webvpn translation-table	インポートした変換テーブルに関する情報を表示します。

export webvpn url-list

URL リストをリモートの場所にエクスポートするには、特権 EXEC モードで **export webvpn url-list** コマンドを使用します。

export webvpn url-list *name url*

構文の説明

name	URL リストを識別する名前。最大数は 64 文字です。
url	URL リストのソースへのリモート パス。最大数は 255 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応		—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

WebVPN には、デフォルトで URL リストはありません。

export webvpn url-list コマンドを使用して、Template というオブジェクトをダウンロードできます。Template オブジェクトは変更または削除できません。Template オブジェクトの内容を編集してカスタム URL リストとして保存し、**import webvpn url-list** コマンドを使用してインポートし、カスタム URL リストを追加できます。

インポート済みの URL リストをエクスポートすると、URL の場所にそのリストの XML ファイルが作成されます。**show import webvpn url-list** コマンドを使用して、使用可能なテンプレート、およびインポート済みのテーブルのリストを表示できます。

例

次に、URL リスト *servers* をエクスポートする例を示します。

```
ciscoasa# export webvpn url-list servers2 tftp://209.165.200.225
ciscoasa#
```

関連コマンド

コマンド	説明
import webvpn url-list	URL リストをインポートします。
revert webvpn url-list	キャッシュ メモリから URL リストを削除します。
show import webvpn url-list	インポート済みの URL リストに関する情報を表示します。

export webvpn webcontent

リモートのクライアントレス SSL VPN ユーザに表示される、フラッシュ メモリ内のインポート済みコンテンツをエクスポートするには、特権 EXEC モードで **export webvpn webcontent** コマンドを使用します。

export webvpn webcontent *source url destination url*

構文の説明

destination url	エクスポート先の URL。最大数は 255 文字です。
source url	コンテンツがある ASA のフラッシュ メモリの URL。最大数は 64 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応		—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

webcontent オプションを使用してエクスポートされるコンテンツは、リモートのクライアントレス ユーザに表示されるコンテンツです。これには、クライアントレス ポータルに表示されるインポート済みのヘルプ コンテンツや、カスタマイゼーション オブジェクトによって使用されるロゴなどがあります。

export webvpn webcontent コマンドの後に疑問符（**?**）を入力すると、エクスポート可能なコンテンツのリストを表示できます。次に例を示します。

```
ciscoasa# export webvpn webcontent ?

Select webcontent to export:
  /+CSCOE+/help/en/app-access-hlp.inc
  /+CSCOU+/cisco_logo.gif
```

例

次に、TFTP を使用してファイル *logo.gif* を、*logo_copy.gif* というファイル名で 209.165.200.225 にエクスポートする例を示します。

```
ciscoasa# export webvpn webcontent /+CSCOU+/logo.gif tftp://209.165.200.225/logo_copy.gif
!!!!* Web resource `/+CSCOU+/logo.gif' was successfully initialized
```

関連コマンド

コマンド	説明
import webvpn webcontent	クライアントレス SSL VPN ユーザに表示されるコンテンツをインポートします。
revert webvpn webcontent	コンテンツをフラッシュ メモリから削除します。
show import webvpn webcontent	インポートされたコンテンツに関する情報を表示します。

extended-security

IP オプション インスペクションにおいて、パケット ヘッダー内に拡張セキュリティ(E-SEC)オプションが存在する場合のアクションを定義するには、パラメータ コンフィギュレーション モードで **extended-security** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

extended-security action {allow | clear}

no extended-security action {allow | clear}

構文の説明

allow	拡張セキュリティ IP オプションを含むパケットを許可します。
clear	拡張セキュリティ オプションをパケット ヘッダーから削除してから、パケットを許可します。

デフォルト

デフォルトでは、IP オプション インスペクションは、拡張セキュリティ IP オプションを含むパケットをドロップします。

IP オプション インスペクション ポリシー マップで **default** コマンドを使用するとデフォルト値を変更できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IP オプション インスペクション ポリシー マップで設定できます。

IP オプション インスペクションを設定して、どの IP パケットが所定の IP オプションを持ち、ASA を通過できるかを制御できます。変更せずにパケットを通過させたり、指定されている IP オプションをクリアしてからパケットを通過させたりできます。

例

次に、IP オプション インスペクションのアクションをポリシー マップで設定する例を示します。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# extended-security action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

CHAPTER 15

failover コマンド ～ fast-flood コマンド

failover

フェールオーバーをイネーブルにするには、グローバル コンフィギュレーション モードで **failover** コマンドを使用します。フェールオーバーをディセーブルにするには、このコマンドの **no** 形式を使用します。

フェールオーバー

no failover

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

フェールオーバーはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、コンフィギュレーションでのフェールオーバーのイネーブルまたはディセーブルに限定されました（**failover active** コマンドを参照）。

使用上のガイドライン

フェールオーバーをディセーブルにするには、このコマンドの **no** 形式を使用します。

注意 フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端に ASA を使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになるおそれがあります。ASA を使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

ASA 5505 デバイスでは、ステートレス フェールオーバーのみが、Easy VPN ハードウェア クライアントとして動作していないときにのみ許可されます。

例

次に、フェールオーバーをディセーブルにする例を示します。

```
ciscoasa(config)# no failover
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure failover	**failover** コマンドを実行コンフィギュレーションから消去し、フェールオーバーのデフォルト値に戻します。
failover active	スタンバイ ユニットをアクティブに切り替えます。
show failover	装置のフェールオーバー ステータスに関する情報を表示します。
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。

failover active

スタンバイの ASA またはフェールオーバー グループをアクティブ ステートに切り替えるには、特権 EXEC モードで **failover active** コマンドを使用します。アクティブな ASA またはフェールオーバー グループをスタンバイに切り替えるには、このコマンドの **no** 形式を使用します。

failover active [**group** *group_id*]

no failover active [**group** *group_id*]

構文の説明

group *group_id*	(任意)アクティブにするフェールオーバー グループを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、フェールオーバー グループを含むように変更されました。

使用上のガイドライン

スタンバイ ユニットからのフェールオーバー切り替えを開始するには **failover active** コマンドを使用し、アクティブ ユニットからのフェールオーバー切り替えを開始するには **no failover active** コマンドを使用します。この機能を使用して、障害が発生したユニットを稼働させたり、メンテナンスのためにアクティブ ユニットをオフラインにしたりできます。ステートフル フェールオーバーを使用していない場合、すべてのアクティブ接続がドロップされるため、クライアントはフェールオーバーの発生後、接続を再確立する必要があります。

フェールオーバー グループの切り替えは、Active/Active フェールオーバーでのみ使用できます。Active/Active フェールオーバー ユニットでフェールオーバー グループを指定しないで **failover active** コマンドを入力すると、ユニットのすべてのグループがアクティブになります。

例

次に、スタンバイ グループ 1 をアクティブに切り替える例を示します。

```
ciscoasa# failover active group 1
```

関連コマンド

コマンド	説明
failover reset	ASA を、障害が発生した状態からスタンバイに変更します。

failover cloud authentication

ASAv でサービス プリンシパルを使用した Microsoft Azure への認証ができるようにするには、グローバル コンフィギュレーション モードで **failover cloud authentication** コマンドを使用します。Microsoft Azure 認証を無効にするには、このコマンドの **no** 形式を使用します。

failover cloud authentication {**application-id** *appl-id* | **directory-id** *dir-id* | **key** *secret-key*}

no failover cloud authentication {**application-id** *appl-id* | **directory-id** *dir-id* | **key** *secret-key* [**encrypt**]}

構文の説明

application-id *appl-id*	Azure インフラストラクチャからアクセス キーを要求するときに必要なアプリケーション ID を指定します。
directory-id *dir-id*	Azure インフラストラクチャからアクセス キーを要求するときに必要なディレクトリ ID を指定します。
key *secret-key*	Azure インフラストラクチャからアクセス キーを要求するときに必要な秘密キーを指定します。**encrypt** キーワードが存在する場合、この秘密キーは実行コンフィギュレーションで暗号化されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.8(2)	このコマンドが導入されました。

使用上のガイドライン

自動的に API 呼び出しによって Azure ルート テーブルが変更されるようにするには、ASAv HA ユニットに Azure Active Directory のクレデンシャルが必要です。Azure は、簡単に言えばサービス アカウントであるサービス プリンシパルの概念を採用しています。サービス プリンシパルを使用すると、あらかじめ定義された Azure リソース セット内でタスクを実行するのに十分な権限と範囲のみを持つアカウントをプロビジョニングできます。

Azure リソース（ルート テーブルなど）へのアクセスまたはリソースの変更が必要となるアプリケーションがある場合は、Azure Active Directory（AD）アプリケーションを設定し、必要な権限を割り当てる必要があります。

Azure ポータルに Azure AD アプリケーションを登録すると、アプリケーション オブジェクトとサービス プリンシパル オブジェクトの 2 つのオブジェクトが Azure AD テナントに作成されます。サービス プリンシパル オブジェクトは、特定のテナントでのアプリケーションの使用に関するポリシーと権限を定義し、アプリケーション実行時のセキュリティ プリンシパルの基礎を提供します。

サービス プリンシパルを設定したら、**ディレクトリ ID**、**アプリケーション ID**、および**秘密キー**を取得します。これらは、Azure 認証クレデンシャルを設定するために必要です。

(注) Azure は、『*Azure Resource Manager Documentation*』で Azure AD アプリケーションとサービス プリンシパルを作成する方法について説明しています。

例

次に、パブリック クラウド フェールオーバー コンフィギュレーションに Azure 認証クレデンシャルを追加する例を示します。

```
(config)# failover cloud authentication application-id dfa92ce2-fea4-67b3-ad2a-6931704e420
(config)# failover cloud authentication directory-id 227b0f8f-684d-48fa-9803-c08138b77ae9
(config)# failover cloud authentication key 5yOhH593dtD/O8gzAlWgulrkWz5dH02d2STk3LDbI4c=
(config)#
```

関連コマンド

コマンド	説明
clear configure failover	**failover** コマンドを実行コンフィギュレーションから消去し、フェールオーバーのデフォルト値に戻します。
failover active	スタンバイ ユニットをアクティブに切り替えます。
failover cloud subscription-id	パブリック クラウド フェールオーバー コンフィギュレーションに Azure サブスクリプション ID を追加します。
show failover	装置のフェールオーバー ステータスに関する情報を表示します。
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。

failover cloud peer

パブリック クラウド フェールオーバー ピアを設定するには、グローバル コンフィギュレーション モードで **failover cloud peer** コマンドを使用します。フェールオーバー ピアを無効にするには、このコマンドの **no** 形式を使用します。

failover cloud peer {**ip** *ip-address* | **port** *port-number*}

no failover cloud peer

構文の説明

ip *ip-address*	パブリック クラウド HA ピアへの TCP フェールオーバー制御接続を確立するために使用する IP アドレスを指定します。
port *port-number*	Azure インフラストラクチャからアクセス キーを要求するときに必要なディレクトリ ID を指定します。

デフォルト

デフォルトは、**failover cloud port control** コマンドによって指定されたポート番号（指定されていない場合はデフォルトのポート番号）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.8(2)	このコマンドが導入されました。

使用上のガイドライン

パブリック クラウド HA ピアへの TCP フェールオーバー制御接続を確立するには、IP アドレスが使用されます。すでにアクティブ ユニットである可能性がある HA ピアへのフェールオーバー接続を開こうとする場合は、ポートが使用されます。HA ピア間で NAT が 実行されている場合は、ここでのポートの設定が必要となる場合があります。この設定は、ほとんどの場合不要です。

このコマンドの **no** 形式を使用すると、ピアとなる IP アドレスが削除され、ポート番号がそのデフォルト値に設定されます。ポートが指定されていない場合、ポート番号は、以前にこのコマンドを使用して別の値が設定されていた場合であってもデフォルト値に設定されます。

例

次に、パブリック クラウド フェールオーバー ピアを設定する例を示します。

```
ciscoasa(config)# failover cloud peer ip 10.4.3.5 port 4444
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure failover	**failover** コマンドを実行コンフィギュレーションから消去し、フェールオーバーのデフォルト値に戻します。
failover active	スタンバイ ユニットをアクティブに切り替えます。
show failover	装置のフェールオーバー ステータスに関する情報を表示します。
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。

failover cloud polltime

パブリック クラウドのフェールオーバー ユニットのポーリング タイムおよびホールド タイムを指定するには、グローバル コンフィギュレーション モードで **failover cloud polltime** コマンドを使用します。デフォルトのポーリング期間およびホールド タイムに戻すには、このコマンドの **no** 形式を使用します。

failover cloud polltime *poll_time* [**holdtime** *time*]

no failover cloud polltime

構文の説明

holdtime *time*	(任意)ユニットが制御ポートで hello メッセージを受信する間隔を設定します。この時間を経過すると、ピア ユニットで障害が発生したと見なされます。 有効な値は 3 ～ 60 秒です。装置のポーリング時間の 3 倍に満たない保持時間は入力できません。
polltime *poll_time*	hello メッセージ間の時間を設定します。 有効な値は 1 ～ 15 秒です。

デフォルト

ASAv のデフォルト値は次のとおりです。

- **polltime** *poll_time* は 5 秒です。
- **holdtime** *time* は 15 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.8(2)	このコマンドが導入されました。

使用上のガイドライン

バックアップ ユニットがアクティブ ユニットの存在をモニタするために使用するポーリング間隔を設定するために使用されます。必要に応じ、アクティブ ユニットからの応答がない場合に、バックアップ ユニットがアクティブなロールを取る前に待機する時間（ホールド タイム）も設定できます。ホールド タイムは、強制的にポーリング タイムの 3 倍以上となります。ポーリング間隔を短くすると、ASA で障害を検出し、フェールオーバーをトリガーする速度が速くなります。ただし短時間での検出は、ネットワークが一時的に輻輳した場合に不要な切り替えが行われる原因となります。

例

次に、パブリック クラウド フェールオーバー コンフィギュレーションでフェールオーバー ポーリングを設定する例を示します。

```
ciscoasa(config)# failover cloud polltime 10 holdtime 30
```

関連コマンド

コマンド	説明
clear configure failover	**failover** コマンドを実行コンフィギュレーションから消去し、フェールオーバーのデフォルト値に戻します。
failover active	スタンバイ ユニットをアクティブに切り替えます。
show failover	装置のフェールオーバー ステータスに関する情報を表示します。
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。

failover cloud port

パブリック クラウド フェールオーバーのペアによって使用される 2 つの TCP ポート、2 つのピア間のフェールオーバー通信に使用するポート、および Azure ロード バランサのプローブに使用するポートを指定するには、グローバル コンフィギュレーション モードで **failover cloud port** コマンドを使用します。これらのポートをデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

failover cloud port {**control** *port-number* | **probe** *port-number* [**interface** if-name]}

no failover cloud port {**control** | **probe**}

構文の説明

control *port-number*	(任意)パブリック クラウド HA ピアとの通信に使用する TCP ポートを指定します。
probe *port-number*	(任意)Azure ロード バランサの健全性プローブへの応答に使用する TCP ポートを指定します。
interface if-name	(任意)Azure ロード バランサ プローブを受け入れるプローブ ポート用に設定するインターフェイスを指定します。省略すると、プローブは、プローブによって使用されるよく知られた送信元 IP アドレス(168.63.129.16)に到達するために最適であると、ASAv 内の IP ルーティング機能によって判断されるインターフェイスに受け入れられます。

デフォルト

パブリック クラウド フェールオーバーの TCP 制御ポート番号は 44442 です。

Azure ロード バランサの健全性プローブ ポート番号は 44441 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.8(2)	このコマンドが導入されました。

使用上のガイドライン

デフォルトのポート値に戻すには、このコマンドの **no** 形式を使用します。

物理 ASA および非パブリック クラウドの仮想 ASA では、Gratuitous ARP 要求を使用してフェールオーバー条件を処理しますが、バックアップ ASA は、アクティブな IP アドレスと MAC アドレスに関連付けられていることを示す Gratuitous ARPP を送信します。ほとんどのパブリック クラウド環境では、このようなブロードキャスト トラフィックは許可されていません。このため、パブリック クラウドの HA 設定では、フェールオーバーが発生したときに通信中の接続を再起動する必要があります。

アクティブ装置の状態がバックアップ装置によってモニタされ、所定のフェールオーバー条件に一致しているかどうかが判別されます。所定の条件に一致すると、フェールオーバーが行われます。フェールオーバー時間は、パブリック クラウド インフラストラクチャの応答性に応じて、数秒～ 1 分を超える場合があります。

例

次に、パブリック クラウド フェールオーバー コンフィギュレーションに対し、フェールオーバー通信および Azure ロード バランサ プローブのための TCP ポートを設定する例を示します。

```
ciscoasa(config)# failover cloud port control 4444
ciscoasa(config)# failover cloud port probe 4443
```

関連コマンド

コマンド	説明
clear configure failover	**failover** コマンドを実行コンフィギュレーションから消去し、フェールオーバーのデフォルト値に戻します。
failover active	スタンバイ ユニットをアクティブに切り替えます。
show failover	装置のフェールオーバー ステータスに関する情報を表示します。
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。

failover cloud route-table

内部ルートをアクティブ ユニットに向ける Azure ルート テーブルを設定するには、グローバル コンフィギュレーション モードで **failover cloud route-table** コマンドを使用します。ルート テーブル コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

failover cloud route-table *table-name* [**subscription-id** *sub-id*]

no failover cloud route-table

構文の説明

table-name	ルート テーブルの名前を指定します。
subscription-id *sub-id*	(任意) Azure リソースを変更する際に必要な Azure サブスクリプション ID を指定します。ルート テーブル内にこのパラメータが存在する場合、それは、ルート テーブルを参照する際に使用される Azure サブスクリプションです。省略すると、グローバル コンフィギュレーション モードで設定されているサブスクリプション ID が使用されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.8(2)	このコマンドが導入されました。
9.9(2)	**subscription-id** パラメータが導入されました。

使用上のガイドライン

フェールオーバーでは、内部ルートをアクティブ装置に向ける必要があります。アクティブ装置は、設定されたルート テーブル情報を使用して自動的にルートを自身に向けます。

プライマリ装置とセカンダリ装置の両方でこれらの設定を構成します。プライマリ装置からセカンダリ装置への設定の同期はありません。

2 つ以上の Azure サブスクリプションでユーザ定義のルートを更新するには、オプションの **subscription-id** パラメータを使用します。**route-table** コマンド レベルの **subscription-id** は、グローバル レベルで指定された Azure サブスクリプション ID を上書きします。**subscription-id** を指定せずに **route-table** コマンドを入力すると、グローバル パラメータが使用されます。

ルート テーブル コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

(注) このコマンドを入力すると、ASAv は **cfg-fover-cloud-rt** モードに切り替わります。

例

次の例では、パブリック クラウド フェールオーバーのルート テーブル コンフィギュレーションで cfg-fover-cloud-rt モードを有効にする方法を示します。

```
ciscoasa(config)# failover cloud route-table inside-rt
ciscoasa(cfg-fover-cloud-rt)#

ciscoasa(config)# failover cloud route-table inside-rt subscription-id cd5fe6b4-d2ed-45
ciscoasa(cfg-fover-cloud-rt)#
```

関連コマンド

コマンド	説明
clear configure failover	**failover** コマンドを実行コンフィギュレーションから消去し、フェールオーバーのデフォルト値に戻します。
rg	パブリック クラウド フェールオーバー コンフィギュレーションに Azure リソース グループを追加します。
route-table	パブリック クラウド フェールオーバー コンフィギュレーションに Azure ルート情報を追加します。
show failover	装置のフェールオーバー ステータスに関する情報を表示します。
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。
failover cloud subscription-id	パブリック クラウド フェールオーバー コンフィギュレーションに Azure サブスクリプション ID を追加します。

failover cloud route-table rg

ルート テーブル更新要求に必要な Azure リソース グループを設定するには、cfg-fover-cloud-rt コンフィギュレーション モードで **rg** コマンドを使用します。コンフィギュレーションからリソース グループ情報を削除するには、このコマンドの **no** 形式を使用します。

rg *resource-group*

no rg

構文の説明

resource-group	Azure リソース グループの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
cg-fover-cloud-rt コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.8(2)	このコマンドが導入されました。

使用上のガイドライン

Azure リソース グループは、Azure ソリューション用の関連リソースを保持するコンテナです。リソース グループには、ソリューション用のすべてのリソースを含めるか、またはグループとして管理するリソースのみを含めることができます。リソース グループにリソースを割り当てる方法は、どうすれば組織にとって最も合理的になるかを考慮して決定します。

プライマリ装置とセカンダリ装置の両方でこれらの設定を構成します。プライマリ装置からセカンダリ装置への設定の同期はありません。

コンフィギュレーションからリソース グループ情報を削除するには、このコマンドの **no** 形式を使用します。

(注) Azure は、『*Azure Resource Manager Documentation*』でリソース グループについて説明しています。

例

次に、パブリック クラウド フェールオーバー コンフィギュレーションに Azure リソース グループを追加する例を示します。

```
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)#
```

関連コマンド

コマンド	説明
clear configure failover	**failover** コマンドを実行コンフィギュレーションから消去し、フェールオーバーのデフォルト値に戻します。
rg	パブリック クラウド フェールオーバー コンフィギュレーションに Azure リソース グループを追加します。
show failover	装置のフェールオーバー ステータスに関する情報を表示します。
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。

failover cloud route-table route

フェールオーバー中に更新を必要とするルートを設定するには、cfg-fover-cloud-rt コンフィギュレーション モードで **route** コマンドを使用します。コンフィギュレーションからルート情報を削除するには、このコマンドの **no** 形式を使用します。

route {**name** *route-name* **prefix** *address-prefix* **nexthop** *ip-address*}

no route name *route-name*

構文の説明

route-name	ルートの名前を指定します。
address-prefix	IP アドレス プレフィックス、スラッシュ（「/」）、および数字のネットマスクとして設定されるアドレス プレフィックスを指定します。例: 192.120.0.0/16。
ip-address	ネクスト ホップの IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
cg-fover-cloud-rt コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.8(2)	このコマンドが導入されました。

使用上のガイドライン

フェールオーバーでは、内部ルートをアクティブ装置に向ける必要があります。アクティブ装置は、設定されたルート テーブル情報を使用して自動的にルートを自身に向けます。

プライマリ装置とセカンダリ装置の両方でこれらの設定を構成します。プライマリ装置からセカンダリ装置への設定の同期はありません。

コンフィギュレーションからルート情報を削除するには、このコマンドの **no** 形式を使用します。

(注) Azure は、『*Azure Resource Manager Documentation*』でルーティングの要件について説明しています。

例

次に、パブリック クラウド フェールオーバー コンフィギュレーションに更新が必要なルートを追加する例を示します。

```
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4
ciscoasa(cfg-fover-cloud-rt)#
```

関連コマンド

コマンド	説明
clear configure failover	**failover** コマンドを実行コンフィギュレーションから消去し、フェールオーバーのデフォルト値に戻します。
rg	パブリック クラウド フェールオーバー コンフィギュレーションに Azure リソース グループを追加します。
show failover	装置のフェールオーバー ステータスに関する情報を表示します。
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。

failover cloud subscription-id

Azure サービス プリンシパル用の Azure サブスクリプション ID を設定するには、グローバル コンフィギュレーション モードで **failover cloud subscription-id** コマンドを使用します。このコマンドの **no** 形式は、コンフィギュレーションからサブスクリプション情報を削除します。

failover cloud subscription-id *sub-id*

no failover cloud subscription-id

構文の説明

subscription-id *sub-id*	Azure リソースを変更する際に必要な Azure サブスクリプション ID を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.8(2)	このコマンドが導入されました。

使用上のガイドライン

Azure サブスクリプション ID は、内部ルートをアクティブ ユニットに向ける場合など、Azure ルート テーブルを変更するために必要です。

(注) サブスクリプション ID は、Azure ポータル（https://portal.azure.com）の「サブスクリプション（Subscriptions）」タブで参照できます。

例

次に、パブリック クラウド フェールオーバー コンフィギュレーションに Azure サブスクリプション ID を追加する例を示します。

```
(config)# failover cloud (config)# failover cloud subscription-id ab2fe6b2-c2bd-44
(config)#
```

関連コマンド

コマンド	説明
clear configure failover	**failover** コマンドを実行コンフィギュレーションから消去し、フェールオーバーのデフォルト値に戻します。
failover cloud authentication	パブリック クラウド フェールオーバー コンフィギュレーションに Azure 認証クレデンシャルを追加します。
show failover	装置のフェールオーバー ステータスに関する情報を表示します。
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。

failover cloud unit

パブリック クラウド フェールオーバー コンフィギュレーションで ASAv をプライマリ ユニットまたはセカンダリ ユニットのいずれかに設定するには、グローバル コンフィギュレーション モードで **failover lan unit** コマンドを使用します。ユニットのロールの設定を削除するには、このコマンドの **no** 形式を使用します。

failover cloud unit {**primary** | **secondary**}

no failover cloud unit

構文の説明

プライマリ	ASAv をプライマリ ユニットとして指定します。
secondary	ASAv をセカンダリ ユニットとして指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.8(2)	このコマンドが導入されました。

使用上のガイドライン

冗長性を確保するために、ASAv をアクティブ/バックアップ高可用性（HA）設定でパブリック クラウド環境に展開します。パブリック クラウドでの HA は、アクティブな ASAv の障害がバックアップ ASAv へのシステムの自動フェールオーバーをトリガーするのを許可するステートレスなアクティブ/バックアップ ソリューションを実装します。

アクティブ/バックアップ フェールオーバーを設定する場合、1 つの装置をプライマリとして設定し、もう 1 つの装置をセカンダリとして設定します。この時点で、2 つのユニットは、デバイスとポリシーの設定、およびイベント、ダッシュボード、レポート、ヘルス モニタリングで、2 つの個別のデバイスとして機能します。

フェールオーバー ペアの 2 つの装置の主な相違点は、どちらの装置がアクティブでどちらの装置がバックアップであるか、つまりどちらの装置がアクティブにトラフィックを渡すかということに関連します。両方のユニットがトラフィックを渡すことができますが、プライマリ ユニットだけがロード バランサ プローブに応答し、構成済みのルートをプログラミングしてルートの接続先として使用します。バックアップ装置の主な機能は、プライマリ装置の正常性を監視することです。両方の装置が同時にスタート アップした場合（さらに動作ヘルスが等しい場合）、プライマリ装置が常にアクティブ装置になります。

例

次に、ASAv をパブリック クラウド フェールオーバー コンフィギュレーションにおけるプライマリ ユニットとして設定する例を示します。

```
ciscoasa(config)# failover cloud unit primary
```

関連コマンド

コマンド	説明
clear configure failover	**failover** コマンドを実行コンフィギュレーションから消去し、フェールオーバーのデフォルト値に戻します。
failover active	スタンバイ ユニットをアクティブに切り替えます。
failover cloud peer	パブリック クラウド フェールオーバー ピアの情報を指定します。
show failover	装置のフェールオーバー ステータスに関する情報を表示します。
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。

failover exec

フェールオーバー ペアの特定のユニットに対してコマンドを実行するには、特権 EXEC モードまたはグローバル コンフィギュレーション モードで **failover exec** コマンドを使用します。

failover exec {**active** | **standby** | **mate**} *cmd_string*

構文の説明

active	コマンドをフェールオーバー ペアのアクティブ ユニットまたはフェールオーバー グループに対して実行することを指定します。アクティブ ユニットまたはフェールオーバー グループに対して入力されたコンフィギュレーション コマンドは、スタンバイ ユニットまたはフェールオーバー グループに複製されます。
cmd_string	実行するコマンド。**show** コマンド、コンフィギュレーション コマンド、および EXEC コマンドがサポートされています。
mate	コマンドをフェールオーバー ピアに対して実行することを指定します。
standby	コマンドをフェールオーバー ペアのスタンバイ ユニットまたはフェールオーバー グループに対して実行することを指定します。スタンバイ ユニットまたはフェールオーバー グループに対して実行されたコンフィギュレーション コマンドは、アクティブ ユニットまたはフェールオーバー グループには複製されません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

failover exec コマンドを使用して、フェールオーバー ペアの特定のユニットに対してコマンドを送信できます。

コンフィギュレーション コマンドはアクティブ装置またはコンテキストからスタンバイ装置またはコンテキストに複製されるため、いずれの装置にログインしているかにかかわらず、**failover exec** コマンドを使用して正しい装置にコンフィギュレーション コマンドを入力できます。たとえば、スタンバイ装置にログインしている場合、**failover exec active** コマンドを使用して、コンフィギュレーションの変更をアクティブ装置に送信できます。その後、これらの変更はスタンバイ装置に複製されます。スタンバイ装置またはコンテキストへのコンフィギュレーション コマンドの送信には、**failover exec** コマンドを使用しないでください。これらのコンフィギュレーションの変更はアクティブ装置に複製されないため、2 つのコンフィギュレーションが同期されなくなります。

コンフィギュレーション、exec、および **show** コマンドの出力は、現在のターミナル セッションで表示されます。したがって、**failover exec** コマンドを使用して、ピア装置で **show** コマンドを発行し、その結果を現在のターミナルに表示することができます。

ピア装置でコマンドを実行するには、ローカル装置でコマンドを実行できるだけの十分な権限を持っている必要があります。

コマンド モード

failover exec コマンドは、お使いのターミナル セッションのコマンド モードとは異なるコマンド モード状態を維持します。デフォルトで、**failover exec** のコマンド モードは、指定したデバイスに対するグローバル コンフィギュレーション モードです。このコマンド モードを変更するには、**failover exec** コマンドを使用して適切なコマンド（**interface** コマンドなど）を送信します。

指定されたデバイスの **failover exec** コマンド モードを変更しても、デバイスへのアクセスに使用しているセッションのコマンド モードは変更されません。たとえば、フェールオーバー ペアのアクティブ ユニットにログインしており、グローバル コンフィギュレーション モードで次のコマンドを発行した場合、セッションのコマンド モードはグローバル コンフィギュレーション モードのままですが、**failover exec** コマンドを使用して送信されるすべてのコマンドはインターフェイス コンフィギュレーション モードで実行されます。

```
ciscoasa(config)# failover exec interface GigabitEthernet0/1
ciscoasa(config)#
```

デバイスとの現在のセッションのコマンド モードを変更しても、**failover exec** コマンドで使用されるコマンド モードには影響しません。たとえば、アクティブ ユニットでインターフェイス コンフィギュレーション モードであるときに、**failover exec** のコマンド モードを変更していない場合、次のコマンドはグローバル コンフィギュレーション モードで実行されます。

```
ciscoasa(config-if)# failover exec active router ospf 100
ciscoasa(config-if)#
```

show failover exec コマンドを使用すると、指定したデバイスにコマンド モードが表示されます。**failover exec** コマンドを使用して送信されたコマンドは、このモードで実行されます。

セキュリティに関する注意事項

failover exec コマンドは、フェールオーバー リンクを使用してコマンドをピア装置に送信し、実行されたコマンドの出力をピア装置から受信します。盗聴や中間者攻撃を防止するには、**failover key** コマンドを使用してフェールオーバー リンクを暗号化する必要があります。

制限事項

- ゼロダウンタイム アップグレード手順を使用して 1 台の装置だけをアップグレードする場合は、機能するコマンドとして **failover exec** コマンドをサポートしているソフトウェアが両方の装置で動作している必要があります。
- コマンドの完成およびコンテキスト ヘルプは、*cmd_string* 引数のコマンドでは使用できません。

- マルチ コンテキスト モードでは、ピア装置のピア コンテキストだけにコマンドを送信できます。異なるコンテキストにコマンドを送信するには、まずログインしているユニットでそのコンテキストに変更する必要があります。
- 次のコマンドと **failover exec** コマンドを一緒に使用することはできません。
  - **changeto**
  - **debug**（**undebug**）
- スタンバイ装置が故障状態の場合、故障の原因がサービス カードの不具合であれば、**failover exec** コマンドからのコマンドは受信できます。それ以外の場合、リモート コマンドの実行は失敗します。
- **failover exec** コマンドを使用して、フェールオーバー ピアで特権 EXEC モードをグローバル コンフィギュレーション モードに切り替えることはできません。たとえば、現在のユニットが特権 EXEC モードのときに **failover exec mate configure terminal** コマンドを入力すると、**show failover exec mate** コマンドの出力に、failover exec セッションがグローバル コンフィギュレーション モードであることが示されます。ただし、ピア ユニットで **failover exec** コマンドを使用してコンフィギュレーション コマンドを入力した場合、現在のユニットでグローバル コンフィギュレーション モードを開始しない限り、その処理は失敗します。
- **failover exec mate failover exec mate** *コマンドのような、再帰的な* **failover exec** コマンドは入力できません。
- ユーザの入力または確認が必要なコマンドでは、**/nonconfirm** オプションを使用する必要があります。

例

次に、**failover exec** コマンドを使用して、アクティブ ユニットのフェールオーバー情報を表示する例を示します。コマンドはアクティブ ユニットで実行されるため、コマンドはローカルで実行されます。

```
ciscoasa(config)# failover exec active show failover

Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 3 seconds, holdtime 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 8.0(2), Mate 8.0(2)
Last Failover at: 09:31:50 jst May 2 2004
        This host: Primary - Active
                Active time: 2483 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.101): Normal
                  admin Interface inside (192.168.0.1): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.111): Normal
                  admin Interface inside (192.168.0.11): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)

Stateful Failover Logical Update Statistics
        Link : failover GigabitEthernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         328        0          328        0
        sys cmd         329        0          329        0
```

```
        up time         0           0           0           0
        RPC services    0           0           0           0
        TCP conn        0           0           0           0
        UDP conn        0           0           0           0
        ARP tbl         0           0           0           0
        Xlate_Timeout   0           0           0           0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       329
        Xmit Q:         0       1       329
ciscoasa(config)#
```

次に、**failover exec** コマンドを使用して、ピア ユニットのフェールオーバー ステータスを表示する例を示します。コマンドはアクティブ ユニットであるプライマリ ユニットで実行されるため、セカンダリのスタンバイ ユニットの情報が表示されます。

```
ciscoasa(config)# failover exec mate show failover

Failover On
Failover unit Secondary
Failover LAN Interface: failover GigabitEthernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 3 seconds, holdtime 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 8.0(2), Mate 8.0(2)
Last Failover at: 09:19:59 jst May 2 2004
        This host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.111): Normal
                  admin Interface inside (192.168.0.11): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)
        Other host: Primary - Active
                Active time: 2604 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.101): Normal
                  admin Interface inside (192.168.0.1): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)

Stateful Failover Logical Update Statistics
        Link : failover GigabitEthernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         344        0          344        0
        sys cmd         344        0          344        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       344
        Xmit Q:         0       1       344
```

次に、**failover exec** コマンドを使用して、フェールオーバー ピアのフェールオーバー コンフィギュレーションを表示する例を示します。コマンドはアクティブ ユニットであるプライマリ ユニットで実行されるため、セカンダリのスタンバイ ユニットの情報が表示されます。

```
ciscoasa(config)# failover exec mate show running-config failover

failover
failover lan interface failover GigabitEthernet0/3
failover polltime unit 1 holdtime 3
failover polltime interface 3 holdtime 15
failover link failover GigabitEthernet0/3
failover interface ip failover 10.0.5.1 255.255.255.0 standby 10.0.5.2
ciscoasa(config)#
```

次に、**failover exec** コマンドを使用して、スタンバイ ユニットからアクティブ ユニットにコンテキストを作成する例を示します。コマンドは、アクティブ ユニットからスタンバイ ユニットに複製されます。2 つの「Creating context…」メッセージに注目してください。1 回めは、コンテキスト作成時に **failover exec** コマンドによってピア ユニットから出力されたものであり、2 回めは複製されたコマンドによってローカルにコンテキストが作成されたときにローカル ユニットから出力されたものです。

```
ciscoasa(config)# show context

Context Name      Class      Interfaces           URL
*admin            default    GigabitEthernet0/0,  disk0:/admin.cfg
                             GigabitEthernet0/1

Total active Security Contexts: 1

! The following is executed in the system execution space on the standby unit.

ciscoasa(config)# failover exec active context text

Creating context 'text'... Done. (2)
Creating context 'text'... Done. (3)

ciscoasa(config)# show context
Context Name      Class      Interfaces           URL
*admin            default    GigabitEthernet0/0,  disk0:/admin.cfg
                             GigabitEthernet0/1
 text             default                         (not entered)

Total active Security Contexts: 2
```

次に、**failover exec** コマンドを使用してスタンバイ ステートのフェールオーバー ピアにコンフィギュレーション コマンドを送信したときに警告が返され、その警告が表示される例を示します。

```
ciscoasa# failover exec mate static (inside,outside) 192.168.5.241 192.168.0.241

        **** WARNING ****
        Configuration Replication is NOT performed from Standby unit to Active unit.
        Configurations are no longer synchronized.
ciscoasa(config)#
```

次に、**failover exec** コマンドを使用して、**show interface** コマンドをスタンバイ ユニットに送信する例を示します。

```
ciscoasa(config)# failover exec standby show interface

Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
      MAC address 000b.fcf8.c290, MTU 1500
      IP address 192.168.5.111, subnet mask 255.255.255.0
      216 packets input, 27030 bytes, 0 no buffer
      Received 2 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      284 packets output, 32124 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "outside":
      215 packets input, 23096 bytes
      284 packets output, 26976 bytes
      0 packets dropped
      1 minute input rate 0 pkts/sec,  21 bytes/sec
      1 minute output rate 0 pkts/sec,  23 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  21 bytes/sec
      5 minute output rate 0 pkts/sec,  24 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(10 Mbps)
      MAC address 000b.fcf8.c291, MTU 1500
      IP address 192.168.0.11, subnet mask 255.255.255.0
      214 packets input, 26902 bytes, 0 no buffer
      Received 1 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      215 packets output, 27028 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "inside":
      214 packets input, 23050 bytes
      215 packets output, 23140 bytes
      0 packets dropped
      1 minute input rate 0 pkts/sec,  21 bytes/sec
      1 minute output rate 0 pkts/sec,  21 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  21 bytes/sec
      5 minute output rate 0 pkts/sec,  21 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/2 "failover", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
      Description: LAN/STATE Failover Interface
      MAC address 000b.fcf8.c293, MTU 1500
      IP address 10.0.5.2, subnet mask 255.255.255.0
      1991 packets input, 408734 bytes, 0 no buffer
      Received 1 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      1835 packets output, 254114 bytes, 0 underruns
```

```
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/2) software (0/0)
  Traffic Statistics for "failover":
      1913 packets input, 345310 bytes
      1755 packets output, 212452 bytes
      0 packets dropped
      1 minute input rate 1 pkts/sec,  319 bytes/sec
      1 minute output rate 1 pkts/sec,  194 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 1 pkts/sec,  318 bytes/sec
      5 minute output rate 1 pkts/sec,  192 bytes/sec
      5 minute drop rate, 0 pkts/sec
.
.
.
```

次に、ピア ユニットに対して不正なコマンドを発行したときにエラー メッセージが返され、そのエラー メッセージが表示される例を示します。

```
ciscoasa# failover exec mate bad command

bad command
  ^
ERROR: % Invalid input detected at '^' marker.
```

次に、フェールオーバーがディセーブルの場合に **failover exec** コマンドを使用してエラー メッセージが返され、そのエラー メッセージが表示される例を示します。

```
ciscoasa(config)# failover exec mate show failover

ERROR: Cannot execute command on mate because failover is disabled
```

関連コマンド

コマンド	説明
debug fover	フェールオーバー関連のデバッグ メッセージを表示します。
debug xml	**failover exec** コマンドによって使用される XML パーサーのデバッグ メッセージを表示します。
show failover exec	**failover exec** のコマンド モードを表示します。

failover group

Active/Active フェールオーバー グループを設定するには、グローバル コンフィギュレーション モードで **failover group** コマンドを使用します。フェールオーバー グループを削除するには、このコマンドの **no** 形式を使用します。

failover group *num*

no failover group *num*

構文の説明

num	フェールオーバー グループの番号。有効な値は、1 または 2 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

最大 2 つのフェールオーバー グループを定義できます。**failover group** コマンドは、マルチ コンテキスト モードが設定されたデバイスのシステム コンテキストにのみ追加できます。フェールオーバー グループは、フェールオーバーがディセーブルになっているときに限り作成および削除できます。

このコマンドを入力すると、フェールオーバー グループ コマンド モードが開始されます。フェールオーバー グループ コンフィギュレーション モードでは、**primary**、**secondary**、**preempt**、**replication http**、**interface-policy**、**mac address**、および **polltime interface** コマンドを使用できます。グローバル コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。

(注) **failover polltime interface**、**failover interface-policy**、**failover replication http**、**failover mac address** の各コマンドは、Active/Active フェールオーバー コンフィギュレーションでは何も行いません。これらは、**polltime interface**、**interface-policy**、**replication http**、および **mac address** の各フェールオーバー グループ コンフィギュレーション モード コマンドによって上書きされます。

フェールオーバー グループを削除するときは、フェールオーバー グループ 1 を最後に削除する必要があります。フェールオーバー グループ 1 には、常に管理コンテキストが含まれています。フェールオーバー グループに割り当てられていないすべてのコンテキストは、デフォルトでフェールオーバー グループ 1 に割り当てられます。コンテキストが明示的に割り当てられているフェールオーバー グループは削除できません。

(注) 同じネットワーク上にアクティブ/アクティブ フェールオーバー ペアが複数ある場合は、あるペアのインターフェイスに割り当てられているものと同じデフォルト仮想 MAC アドレスが、他のペアのインターフェイスに割り当てられることがあります。これは、デフォルト仮想 MAC アドレスの決定方法に基づいた動作です。ネットワーク上に重複した MAC アドレスが存在しないようにするには、**mac address** コマンドを使用して、各物理インターフェイスに対して仮想アクティブ MAC アドレスおよび仮想スタンバイ MAC アドレスを割り当てる必要があります。

例

次に、2 つのフェールオーバー グループのコンフィギュレーションの例(抜粋)を示します。

```
ciscoasa(config)# failover group 1
ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# exit
ciscoasa(config)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

関連コマンド

コマンド	説明
asr-group	非対称ルーティング インターフェイス グループ ID を指定します。
interface-policy	モニタリングによってインターフェイスの障害が検出された場合のフェールオーバー ポリシーを指定します。
join-failover-group	コンテキストをフェールオーバー グループに割り当てます。
mac address	フェールオーバー グループ内のコンテキストに対して仮想 MAC アドレスを定義します。
polltime interface	モニタ対象インターフェイスに送信される hello メッセージ間の時間を指定します。
preempt	高いプライオリティを持つユニットが、リブート後にアクティブ ユニットとなることを指定します。
プライマリ	フェールオーバー グループにおいて、プライマリ ユニットに対してより高いプライオリティを指定します。
replication http	選択したフェールオーバー グループに対して、HTTP セッションのレプリケーションを指定します。
secondary	フェールオーバー グループにおいて、セカンダリ ユニットに対してより高いプライオリティを指定します。

failover health-check bfd

ユニット ヘルス モニタリングに Bidirectional Forwarding Detection（BFD）を設定するには、グローバル コンフィギュレーション モードで **failover health-check bfd** コマンドを使用します。BFD をディセーブルにするには、このコマンドの **no** 形式を使用します。

failover health-check bfd *template_name*

no failover health-check bfd *template_name*

構文の説明

template_name	BFD テンプレートの名前。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラスタ グループ コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

CPU の使用率が高い場合、通常のユニットのモニタリングにより誤ってアラームが発生する可能性があります。BFD メソッドは分散されていてるため、CPU の使用率が高い場合でも動作に影響はありません。

最初に、パケット レートを定義するための BFD シングルホップ テンプレートを設定する必要があります。

bfd-template single-hop *template_name*

bfd interval min-tx *milliseconds* **min-rx** *milliseconds* **multiplier** *multiplier_value*

次の制限事項を確認してください。

- FirePOWER 9300 および 4100 のみ
- アクティブ/スタンバイのみ
- ルーテッド モードのみ

例

次に、BFD ユニット ヘルス検出を有効にする例を示します。

```
ciscoasa(config)# bfd template single-hop failover-temp
ciscoasa(config-bfd)# bfd interval min-tx 50 min-rx 50 multiplier 3
ciscoasa(config)# failover health-check bfd failover-temp
```

関連コマンド

コマンド	説明
bfd template	BFD で使用するテンプレートを作成します。
bfd interval	テンプレートのパケット レートを定義します。

failover interface ip

フェールオーバー インターフェイスとステートフル フェールオーバー インターフェイスに対して、IPv4 アドレスとマスク、または IPv6 アドレスとプレフィックスを指定するには、グローバル コンフィギュレーション モードで **failover interface ip** コマンドを使用します。IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

failover interface ip *if_name* [*ip_address mask* **standby** *ip_address* | *ipv6_address*/*prefix* **standby***ipv6_address*]

no failover interface ip *if_name* [*ip_address mask* **standby** *ip_address* | *ipv6_address*/*prefix* **standby***ipv6_address*]

構文の説明

if_name	フェールオーバーまたはステートフル フェールオーバー インターフェイスのインターフェイス名です。
ip_address mask	プライマリ デバイス上のフェールオーバーまたはステートフル フェールオーバー インターフェイスに対して、IP アドレスとマスクを指定します。
ipv6_address	プライマリ デバイス上のフェールオーバーまたはステートフル フェールオーバー インターフェイスに対して、IPv6 アドレスを指定します。
prefix	アドレスの高次の連続ビットのうち、何個が IPv6 プレフィックス（IPv6 アドレスのネットワーク部分）を構成しているかを指定します。
standby *ip_address*	セカンダリ デバイスがプライマリ デバイスとの通信に使用する IP アドレスを指定します。
standby*ipv6_address*	セカンダリ デバイスがプライマリ デバイスとの通信に使用する IPv6 アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(2)	IPv6 アドレスのサポートが追加されました。

使用上のガイドライン

スタンバイ アドレスは、プライマリ アドレスと同じサブネットにある必要があります。

コンフィギュレーションに適用できる **failvover interface ip** コマンドは 1 つだけです。そのため、フェールオーバー インターフェイスには IPv6 アドレスまたは IPv4 アドレスのいずれか 1 つを割り当てることができます。IPv6 アドレスおよび IPv4 アドレスの両方をインターフェイスに割り当てることはできません。

フェールオーバーおよびステートフル フェールオーバー インターフェイスは、ASA がトランスペアレント ファイアウォール モードで稼働し、システムに対してグローバルであっても、レイヤ 3 で動作します。

マルチ コンテキスト モードでは、システム コンテキストにフェールオーバーを設定します（**monitor-interface** コマンドを除く）。

このコマンドは、ASA を LAN フェールオーバー用にブートストラップするときに、コンフィギュレーションの一部である必要があります。

例

次に、フェールオーバー インターフェイスに IPv4 アドレスとマスクを指定する方法の例を示します。

```
ciscoasa(config)# failover interface ip lanlink 172.27.48.1 255.255.255.0 standby
172.27.48.2
```

次に、フェールオーバー インターフェイスに IPv6 アドレスとプレフィックスを指定する方法の例を示します。

```
ciscoasa(config)# failover interface ip lanlink 2001:a0a:b00::a0a:b70/64 standby
2001:a0a:b00::a0a:b71
```

関連コマンド

コマンド	説明
clear configure failover	**failover** コマンドを実行コンフィギュレーションから消去し、フェールオーバーのデフォルト値に戻します。
failover lan interface	フェールオーバー通信に使用するインターフェイスを指定します。
failover link	ステートフル フェールオーバーに使用するインターフェイスを指定します。
monitor-interface	指定したインターフェイスの状態をモニタします。
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。

failover interface-policy

モニタリングによってインターフェイスの障害が検出された場合のフェールオーバーのポリシーを指定するには、グローバル コンフィギュレーション モードで **failover interface-policy** コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

failover interface-policy *num*[**%**]

no failover interface-policy *num*[**%**]

構文の説明

num	パーセンテージとして使用される場合は 1 ～ 100 の数値を、数値として使用される場合は 1 ～インターフェイスの最大数を指定します。
%	(任意)*num* の数字が、モニタ対象インターフェイスのパーセンテージであることを指定します。

デフォルト

デフォルトの設定は次のとおりです。

- *num* は 1 です。
- 物理インターフェイスのモニタリングは、デフォルトでイネーブルになっています。論理インターフェイスのモニタリングは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

num 引数とオプションの **%** キーワードの間にはスペースを挿入しません。

障害が発生したインターフェイスの数が、設定されているポリシーの基準を満たし、他方の ASA が正しく機能している場合、ASA は自身を障害発生状態とマークして、フェールオーバーが行われる可能性があります(アクティブな ASA で障害が発生した場合)。ポリシーでカウントされるのは、**monitor-interface** コマンドでモニタ対象として指定したインターフェイスのみです。

(注) このコマンドが適用されるのは、Active/Standby フェールオーバーのみです。Active/Active フェールオーバーでは、フェールオーバー グループ コンフィギュレーション モードで **interface-policy** コマンドを使用して、各フェールオーバー グループのインターフェイス ポリシーを設定します。

例

次に、2 通りの方法でフェールオーバー ポリシーを指定する例を示します。

```
ciscoasa(config)# failover interface-policy 20%

ciscoasa(config)# failover interface-policy 5
```

関連コマンド

コマンド	説明
failover polltime	ユニットおよびインターフェイスのポーリング タイムを指定します。
failover reset	障害が発生したユニットを障害が発生していない状態に復元します。
monitor-interface	フェールオーバーのためにモニタ対象にするインターフェイスを指定します。
show failover	装置のフェールオーバー状態についての情報を表示します。

failover ipsec pre-shared-key

フェールオーバーの IPsec LAN-to-LAN トンネルと、ユニット間のステート リンクを確立してすべてのフェールオーバー通信を暗号化するには、グローバル コンフィギュレーション モードで **failover ipsec pre-shared-key** コマンドを使用します。キーを削除するには、このコマンドの **no** 形式を使用します。

failover ipsec pre-shared-key *key*

no failover ipsec pre-shared-key

構文の説明

0	暗号化されていないパスワードを指定します。これはデフォルトです。
8	暗号化パスワードを指定します。マスター パスフレーズを使用する場合（**password encryption aes** および **key config-key password-encryption** コマンドを参照）、キーはコンフィギュレーション内で暗号化されています。コンフィギュレーションからコピーする場合（**more system:running-config** 出力からなど）、**8** キーワードを使用してキーの暗号化を指定します。 （注） **show running-config** の出力では、**failover ipsec pre-shared-key** は、***** と表示されます。このマスクされたキーはコピーできません。
key	IKEv2 によるトンネルの確立に使用される、両方のユニットに対するキーを指定します。最大長は 128 文字です。

コマンド デフォルト

0（暗号化なし）がデフォルトです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.1(2)	このコマンドが追加されました。

使用上のガイドライン

フェールオーバー通信をセキュリティ保護しない限り、フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、すべてクリア テキストで送信されます。VPN トンネルの終端に ASA を使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになるおそれがあります。ASA を使用して VPN トンネルを終端する場合は、フェールオーバー通信をセキュリティ保護することをお勧めします。

暗号化方法として、レガシーの **failover key** 方式よりも、**failover ipsec pre-shared-key** 方式を使用することをお勧めします。

IPsec 暗号化とレガシーの **failover key** 暗号化の両方を使用することはできません。両方の方法を設定した場合は、IPsec が使用されます。ただし、マスター パスフレーズを使用する場合は（**password encryption aes** および **key config-key password-encryption** コマンドを参照）、IPsec 暗号化を設定する前に、**no failover key** コマンドを使用してフェールオーバー キーを削除する必要があります。

（注） フェールオーバー LAN-to-LAN トンネルは、IPsec（その他の VPN）ライセンスには適用されません。

例

次に、IPsec 事前共有キーを設定する例を示します。

```
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
```

関連コマンド

コマンド	説明
show running-config failover	実行コンフィギュレーション内のフェールオーバー コマンドを表示します。
show vpn-sessiondb	フェールオーバー IPsec トンネルを含む、VPN トンネルに関する情報を示します。

failover key

フェールオーバー ペアのユニット間での暗号化および認証された通信（フェールオーバー リンクとステート リンクによる）用のキーを指定するには、グローバル コンフィギュレーション モードで **failover key** コマンドを使用します。キーを削除するには、このコマンドの **no** 形式を使用します。

failover key [**0** | **8**] {**hex** *key* | *shared_secret*}

no failover key

構文の説明

0	暗号化されていないパスワードを指定します。これはデフォルトです。
8	暗号化パスワードを指定します。マスター パスフレーズを使用する場合（**password encryption aes** および **key config-key password-encryption** コマンドを参照）、共有秘密はコンフィギュレーション内で暗号化されています。コンフィギュレーションからコピーする場合（**more system:running-config** 出力からなど）、**8** キーワードを使用して共有秘密が暗号化されていることを指定します。 （注） **failover key** の共有秘密は、**show running-config** の出力に ***** と表示されます。このマスクされたキーはコピーできません。
hex *key*	暗号キーの 16 進数値を指定します。キーは、32 文字の 16 進数文字（0 ～ 9、a ～ f）である必要があります。
shared_secret	英数字の共有秘密を指定します。秘密に使用できる文字数は、1 ～ 63 文字です。有効な文字は、数字、文字、または句読点の任意の組み合わせです。共有秘密は、暗号キーを生成するために使用されます。

デフォルト

0（暗号化なし）がデフォルトです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**failover lan key** から **failover key** に変更されました。
7.0(4)	このコマンドが、**hex** *key* キーワードおよび引数を含むように変更されました。
8.3(1)	このコマンドは、**0** および **8** キーワードを使用してマスター パスフレーズをサポートするように変更されました。

使用上のガイドライン

フェールオーバー通信をセキュリティ保護しない限り、フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、すべてクリア テキストで送信されます。VPN トンネルの終端に ASA を使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになるおそれがあります。ASA を使用して VPN トンネルを終端する場合は、フェールオーバー通信をセキュリティ保護することをお勧めします。

暗号化方法として、レガシーの **failover key** 方式よりも、**failover ipsec pre-shared-key** 方式を使用することをお勧めします。

IPsec 暗号化（**failover ipsec pre-shared-key** コマンド）とレガシーの **failover key** 暗号化の両方を使用することはできません。両方の方法を設定した場合は、IPsec が使用されます。ただし、マスター パスフレーズを使用する場合は（**password encryption aes** および **key config-key password-encryption** コマンドを参照）、IPsec 暗号化を設定する前に、**no failover key** コマンドを使用してフェールオーバー キーを削除する必要があります。

例

次に、フェールオーバー ペアのユニット間でフェールオーバー通信をセキュリティ保護するための共有秘密を指定する例を示します。

```
ciscoasa(config)# failover key abcdefg
```

次に、フェールオーバー ペアの 2 つのユニット間でフェールオーバー通信をセキュリティ保護するための 16 進キーを指定する例を示します。

```
ciscoasa(config)# failover key hex 6a1ed228381cf5c68557cb0c32e614dc
```

次に、**more system:running-config** 出力から、暗号化されたパスワードをコピーして貼り付けた例を示します。

```
ciscoasa(config)# failover key 8 TPZCVNgdegLhWMa
```

関連コマンド

コマンド	説明
show running-config failover	実行コンフィギュレーション内のフェールオーバー コマンドを表示します。

failover lan interface

フェールオーバー通信に使用されるインターフェイスを指定するには、グローバル コンフィギュレーション モードで **failover lan interface** コマンドを使用します。フェールオーバー インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

failover lan interface *if_name* {*phy_if*[.*sub_if*] | *vlan_if*}

no failover lan interface [*if_name* {*phy_if*[.*sub_if*] | *vlan_if*}]

構文の説明

if_name	フェールオーバー専用の ASA インターフェイスの名前を指定します。
phy_if	物理インターフェイスを指定します。
sub_if	(任意)サブインターフェイス番号を指定します。
vlan_if	ASASM で、VLAN インターフェイスをフェールオーバー リンクとして指定するために使用されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	*phy_if* 引数が追加されました。
7.2(1)	*vlan_if* 引数が追加されました。
9.5(1)	このコマンドは、ASA 5506H-X の管理インターフェイスを受け入れるように変更されました。

使用上のガイドライン

フェールオーバー ペアの 2 台の装置は、フェールオーバー リンク経由で常に通信して、各装置の動作ステータスを確認しています。

フェールオーバー リンク データ

次の情報がフェールオーバー リンク経由で伝達されています。

- 装置の状態(アクティブまたはスタンバイ)
- hello メッセージ(キープアライブ)

- ネットワーク リンクの状態
- MAC アドレス交換
- コンフィギュレーションの複製および同期

フェールオーバー リンクのインターフェイス

使用されていないデータ インターフェイス（物理、冗長、または EtherChannel）はどれでも、フェールオーバー リンクとして使用できます。ただし、現在名前が設定されているインターフェイスは指定できません。フェールオーバー リンク インターフェイスは、通常のネットワーク インターフェイスとしては設定されません。フェールオーバー通信のためにだけ存在します。このインターフェイスは、フェールオーバー リンク用にのみ使用できます（ステート リンク用としても使用できます）。ASA は、ユーザ データ用とフェールオーバー用に異なるサブインターフェイスが設定されている場合でも、ユーザ データとフェールオーバー リンク間でのインターフェイスの共有はサポートしません。フェールオーバー リンクには、別の物理、EtherChannel、または冗長インターフェイスを使用する必要があります。

フェールオーバー リンクについては、次のガイドラインを参照してください。

- 5506-X ～ 5555-X：管理インターフェイスをフェールオーバー リンクとして使用できません。データ インターフェイスを使用する必要があります。5506H-X は唯一の例外で、フェールオーバー リンクとして管理インターフェイスを使用できます。
- 5506H-X：フェールオーバー リンクとして管理 1/1 インターフェイスを使用できます。フェールオーバー用に設定した場合は、デバイスをリロードして変更を反映させる必要があります。この場合、管理プロセスに管理インターフェイスが必要であるため、ASA Firepower モジュールも使用できません。
- 5585-X：データ インターフェイスとしては使用できますが、管理 0/0 インターフェイスは使用しないでください。この用途で必要とされるパフォーマンスをサポートしていません。
- Firepower 9300 ASA セキュリティ モジュール：管理タイプまたはデータ タイプのどちらかのインターフェイスをフェールオーバー リンクとして使用できます。インターフェイスを節約し、同じシャーシ内のモジュール間でフェールオーバー リンクを共有するには、管理タイプのインターフェイスを使用します。たとえば、それぞれ 3 つのセキュリティ モジュールを備えた 2 台のシャーシがあるとします。シャーシ間で 3 つのフェールオーバー ペアを作成できます。1 つの 10 GigabitEthernet 管理インターフェイスをシャーシ間で使用して、フェールオーバー リンクとして機能させることができます。各モジュール内で一意の VLAN サブインターフェイスを設定するだけです。
- すべてのモデル：1 GB インターフェイスは、フェールオーバーとステート リンクを組み合わせるには十分な大きさです。

フェールオーバー リンクとして使用される冗長インターフェイスについては、冗長性の増強による次の利点を参照してください：

- フェールオーバー ユニットが起動すると、メンバー インターフェイスを交互に実行し、アクティブ ユニットを検出します。
- メンバー インターフェイスの 1 つにあるピアからのキープアライブ メッセージの受信をフェールオーバー ユニットが停止した場合、別のメンバー インターフェイスに切り替えます。

フェールオーバー リンクとして使用される EtherChannel の場合は、順序が不正なパケットを防止するために、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。フェールオーバー リンクとして使用中の EtherChannel の設定は変更できません。

フェールオーバー リンクの接続

フェールオーバー リンクを次の 2 つの方法のいずれかで接続します。

- ASA のフェールオーバー インターフェイスと同じネットワーク セグメント（ブロードキャスト ドメインまたは VLAN）に他の装置のないスイッチを使用する。
- イーサネット ケーブルを使用して装置を直接接続します。外部スイッチは必要ありません。

装置間でスイッチを使用しない場合、インターフェイスに障害が発生すると、リンクは両方のピアでダウンします。このような状況では、障害が発生してリンクがダウンする原因になったインターフェイスがどちらの装置のものかを簡単に特定できないため、トラブルシューティング作業が困難になる場合があります。

ASA は、銅線イーサネット ポートで Auto-MDI/MDIX をサポートしているため、クロスオーバー ケーブルまたはストレート ケーブルのいずれかを使用できます。ストレート ケーブルを使用した場合は、インターフェイスが自動的にケーブルを検出して、送信/受信ペアの 1 つを MDIX にスワップします。

その他のガイドライン

- 接続中のスイッチで VLAN を使用する場合は、フェールオーバー リンク専用の VLAN を使用します。フェールオーバー リンクの VLAN を他の VLAN と共有すると、断続的にトラフィックの問題が発生したり、ping や ARP の障害が発生したりすることがあります。フェールオーバー リンクの接続にスイッチを使用する場合は、スイッチおよび ASA でフェールオーバー リンク専用のインターフェイスを使用します。インターフェイスを、通常のネットワーク トラフィックを伝送するサブインターフェイスと共有しないでください。
- マルチ コンテキスト モードで動作するシステムでは、フェールオーバー リンクはシステム コンテキストにあります。システム コンテキストに設定できるインターフェイスは、このインターフェイス、および使用されている場合はステート リンクのみです。他のインターフェイスは、すべてセキュリティ コンテキストに割り当てられ、セキュリティ コンテキスト内から設定されます。
- フェールオーバー リンクの IP アドレスおよび MAC アドレスは、フェールオーバー時に変更されません。

注意 フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端に ASA を使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになるおそれがあります。ASA を使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

例

次に、共有フェールオーバーおよびステート リンクを含むプライマリ ユニットのフェールオーバー パラメータを設定する例を示します。

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
interface gigabitethernet 0/3
    no shutdown
failover link folink gigabitethernet0/3
failover ipsec pre-shared-key a3rynsun
failover
```

関連コマンド

コマンド	説明
failover lan unit	LAN ベースのフェールオーバーでの、プライマリ装置またはセカンダリ装置を指定します。
failover link	ステートフル フェールオーバー インターフェイスを指定します。

failover lan unit

LAN フェールオーバー設定で ASA をプライマリ装置またはセカンダリ装置のいずれかに設定するには、グローバル コンフィギュレーション モードで **failover lan unit** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

failover lan unit {**primary** | **secondary**}

no failover lan unit {**primary** | **secondary**}

構文の説明

プライマリ	ASA をプライマリ ユニットとして指定します。
secondary	ASA をセカンダリ ユニットとして指定します。

デフォルト

セカンダリ

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

Active/Standby フェールオーバーでは、フェールオーバー ユニットに対するプライマリとセカンダリの指定によって、起動時にどのユニットがアクティブになるかが決まります。次の場合に、起動時にプライマリ ユニットがアクティブ ユニットになります。

- 最初のフェールオーバー ポーリング チェックの間に、プライマリ ユニットとセカンダリ ユニットの両方がブート シーケンスを完了している。
- プライマリ ユニットがセカンダリ ユニットよりも前に起動している。

プライマリ ユニットの起動時にすでにセカンダリ ユニットがアクティブになっている場合、プライマリ ユニットはアクティブにはならずに、スタンバイ ユニットとなります。この場合、プライマリ ユニットを強制的にアクティブ ステータスに戻すには、セカンダリ(アクティブ)ユニットで **no failover active** コマンドを入力する必要があります。

Active/Active フェールオーバーでは、各フェールオーバー グループにプライマリまたはセカンダリのユニット プリファレンスが割り当てられます。このプリファレンスによって、両方のユニットが（フェールオーバー ポーリング期間内に）同時に起動されたときに、起動時にフェールオーバー ペアのどのユニットでフェールオーバー グループのコンテキストがアクティブになるかが決まります。

このコマンドは、ASA を LAN フェールオーバー用にブートストラップするときに、コンフィギュレーションの一部である必要があります。

例

次に、ASA を LAN ベースのフェールオーバーのプライマリ ユニットとして設定する例を示します。

```
ciscoasa(config)# failover lan unit primary
```

関連コマンド

コマンド	説明
failover lan interface	フェールオーバー通信に使用するインターフェイスを指定します。

failover link

ステートフル フェールオーバー インターフェイスを指定し、ステートフル フェールオーバーをイネーブルにするには、グローバル コンフィギュレーション モードで、**failover link** コマンドを使用します。ステートフル フェールオーバー インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

failover link *if_name* [*phy_if*]

no failover link

構文の説明

if_name	ステートフル フェールオーバー専用の ASA インターフェイスの名前を指定します。
phy_if	(任意)物理インターフェイス ポートまたは論理インターフェイス ポートを指定します。ステートフル フェールオーバー インターフェイスが、フェールオーバー通信に割り当てられているインターフェイスを共有しているか、または標準ファイアウォール インターフェイスを共有している場合、この引数は必要ありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	*phy_if* 引数が追加されました。
7.0(4)	このコマンドが、標準ファイアウォール インターフェイスを受け入れるように変更されました。
9.5(1)	このコマンドは、ASA 5506H-X の管理インターフェイスを受け入れるように変更されました。

使用上のガイドライン

ステートフル フェールオーバーを使用するには、接続ステート情報を渡すためのステートフル フェールオーバー リンク（ステート リンクとも呼ばれる）を設定する必要があります。

フェールオーバー リンクの共有

インターフェイスを節約するための最適な方法はフェールオーバー リンクの共有です。このインターフェイスでパフォーマンス上の問題が発生した場合は、別のインターフェイスをステート リンク専用にすることを検討してください。

専用インターフェイス

ステート リンク専用のデータ インターフェイス（物理、冗長、または EtherChannel）を使用できます。ステート リンクとして使用される EtherChannel の場合は、順序が不正なパケットを防止するために、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。

次の 2 つの方法のいずれかで、専用のステート リンクを接続します。

- ASA のフェールオーバー インターフェイスと同じネットワーク セグメント（ブロードキャスト ドメインまたは VLAN）に他の装置のないスイッチを使用する。
- イーサネット ケーブルを使用してアプライアンスを直接接続します。外部スイッチは必要ありません。

装置間でスイッチを使用しない場合、インターフェイスに障害が発生すると、リンクは両方のピアでダウンします。このような状況では、障害が発生してリンクがダウンする原因になったインターフェイスがどちらの装置のものかを簡単に特定できないため、トラブルシューティング作業が困難になる場合があります。

ASA は、銅線イーサネット ポートで Auto-MDI/MDIX をサポートしているため、クロスオーバー ケーブルまたはストレート ケーブルのいずれかを使用できます。ストレート ケーブルを使用した場合は、インターフェイスが自動的にケーブルを検出して、送信/受信ペアの 1 つを MDIX にスワップします。

長距離のフェールオーバーを使用する場合のステート リンクの遅延は、パフォーマンスを最善にするには 10 ミリ秒未満でなければならず、250 ミリ秒を超えないようにする必要があります。遅延が 10 ミリ秒を超えると、フェールオーバー メッセージの再送信により、どうしてもパフォーマンスが低下します。

その他のガイドライン

- マルチ コンテキスト モードでは、ステートフル フェールオーバー リンクはシステム コンテキストに存在します。このインターフェイスとフェールオーバー インターフェイスが、システム コンテキスト内にある唯一のインターフェイスです。他のインターフェイスは、すべてセキュリティ コンテキストに割り当てられ、セキュリティ コンテキスト内から設定されます。
- ステートフル フェールオーバー リンクが通常のデータ インターフェイスに設定されていない限り、ステートフル フェールオーバー リンクの IP アドレスと MAC アドレスは、フェールオーバー時に変更されません。

注意 フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端に ASA を使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになるおそれがあります。ASA を使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

例

次に、共有フェールオーバーおよびステート リンクを含むプライマリ ユニットのフェールオーバー パラメータを設定する例を示します。

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
interface gigabitethernet 0/3
    no shutdown
failover link folink gigabitethernet0/3
failover ipsec pre-shared-key a3rynsun
failover
```

関連コマンド

コマンド	説明
failover interface ip	**failover** コマンドおよびステートフル フェールオーバー インターフェイスの IP アドレスを設定します。
failover lan interface	フェールオーバー通信に使用するインターフェイスを指定します。

failover mac address

物理インターフェイスのフェールオーバー仮想 MAC アドレスを指定するには、グローバル コンフィギュレーション モードで **failover mac address** コマンドを使用します。仮想 MAC アドレスを削除するには、このコマンドの **no** 形式を使用します。

failover mac address *phy_if active_mac standby_mac*

no failover mac address *phy_if active_mac standby_mac*

構文の説明

active_mac	アクティブな ASA の指定したインターフェイスに割り当てられた MAC アドレス。MAC アドレスは h.h.h 形式で入力する必要があります。ここで、h は 16 ビットの 16 進数です。
phy_if	MAC アドレスを設定するインターフェイスの物理名です。
standby_mac	スタンバイの ASA の指定したインターフェイスに割り当てられた MAC アドレス。MAC アドレスは h.h.h 形式で入力する必要があります。ここで、h は 16 ビットの 16 進数です。

デフォルト

設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

failover mac address コマンドを使用すると、Active/Standby フェールオーバー ペアの仮想 MAC アドレスを設定できます。仮想 MAC アドレスが定義されていない場合は、各フェールオーバー ユニットが起動したときに、それらのユニットではインターフェイスのバーンドイン MAC アドレスが使用され、それらのアドレスがフェールオーバー ピアと交換されます。プライマリ ユニットのインターフェイスの MAC アドレスが、アクティブ ユニットのインターフェイスに使用されます。

ただし、両方のユニットが同時にオンラインにならず、セカンダリ ユニットが最初に起動してアクティブになった場合、セカンダリ ユニットは、自身のインターフェイスにバーンドイン MAC アドレスを使用します。その後プライマリ ユニットがオンラインになると、セカンダリ ユニットはプライマリ ユニットから MAC アドレスを取得します。この変更によりネットワーク トラフィックが中断される可能性があります。インターフェイスに仮想 MAC アドレスを設定すると、セカンダリ ユニットがプライマリ ユニットよりも前にオンラインになり、アクティブ ユニットとなった場合でも、正しい MAC アドレスが使用されるようになります。

failover lan interface コマンドでは、フェールオーバーが発生した場合に IP アドレスおよび MAC アドレスが変更されないため、LAN ベースのフェールオーバーに設定されたインターフェイスでは、**failover mac address** コマンドは不要であり、使用できません。このコマンドは、ASA が Active/Active フェールオーバーに設定されている場合には何も行いません。

コンフィギュレーションに **failover mac address** コマンドを追加する場合は、仮想 MAC アドレスを設定し、コンフィギュレーションをフラッシュ メモリに保存して、フェールオーバー ペアをリロードすることを推奨します。アクティブな接続が存在するときに仮想 MAC アドレスを追加すると、これらの接続は停止します。また、仮想 MAC アドレス指定を有効にするには、**failover mac address** コマンドを含むコンフィギュレーション全体を、セカンダリ ASA のフラッシュ メモリに書き込む必要があります。

failover mac address がプライマリ ユニットのコンフィギュレーションに指定されている場合は、セカンダリ ユニットのブートストラップ コンフィギュレーションにも指定する必要があります。

（注） このコマンドが適用されるのは、Active/Standby フェールオーバーのみです。Active/Active フェールオーバーでは、フェールオーバー グループ コンフィギュレーション モードで **mac address** コマンドを使用して、フェールオーバー グループの各インターフェイスの仮想 MAC アドレスを設定します。

他のコマンドまたは方法を使用して MAC アドレスを設定することもできますが、1 つの方法だけを使用することを推奨します。複数の方法を使用して MAC アドレスを設定した場合は、どの MAC アドレスが使用されるかは多くの可変要素によって決まるため、予測できないことがあります。

例

次に、intf2 という名前のインターフェイスのアクティブ MAC アドレスおよびスタンバイ MAC アドレスを設定する例を示します。

```
ciscoasa(config)# failover mac address Ethernet0/2 00a0.c969.87c8 00a0.c918.95d8
```

関連コマンド

コマンド	説明
show interface	インターフェイスのステータス、コンフィギュレーション、および統計情報を表示します。

failover polltime

フェールオーバー ユニットのポーリング タイムおよびホールド タイムを指定するには、グローバル コンフィギュレーション モードで **failover polltime** コマンドを使用します。デフォルトのポーリング期間およびホールド タイムに戻すには、このコマンドの **no** 形式を使用します。

failover polltime [**unit**] [**msec**] *poll_time* [**holdtime** [**msec**] *time*]

no failover polltime [**unit**] [**msec**] *poll_time* [**holdtime** [**msec**] *time*]

構文の説明

holdtime *time*	(任意)ユニットが、フェールオーバー リンクで hello メッセージを受信する間隔を設定します。この時間を経過すると、ピア ユニットで障害が発生したと見なされます。 有効な値は 3 ～ 45 秒です。オプションの **msec** キーワードを使用した場合は、800 ～ 999 ミリ秒です。
msec	(任意)指定する時間がミリ秒単位であることを指定します。
poll_time	hello メッセージ間の時間を設定します。 有効な値は 1 ～ 15 秒です。オプションの **msec** キーワードを使用した場合は、200 ～ 999 ミリ秒です。
unit	(任意)コマンドがユニットのポーリング タイムおよびホールド タイムに使用されていることを示します。 このキーワードをコマンドに追加してもコマンドには影響がありませんが、コンフィギュレーションでこのコマンドを **failover polltime interface** コマンドと区別しやすくなります。

デフォルト

ASA のデフォルト値は次のとおりです。

- *poll_time* は 1 秒です。
- **holdtime** *time* は 15 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**failover poll** コマンドから **failover polltime** コマンドに変更され、**unit** キーワードおよび **holdtime** キーワードが含まれるようになりました。
7.2(1)	**holdtime** キーワードに **msec** キーワードが追加されました。**polltime** の最小値が 500 ミリ秒から 200 ミリ秒に引き下げられました。**holdtime** の最小値が 3 秒から 800 ミリ秒に引き下げられました。

使用上のガイドライン

ユニットのポーリング タイムの 3 倍未満の値を **holdtime** の値として入力することはできません。ポーリング時間が短いほど、ASA は短時間で故障を検出し、フェールオーバーをトリガーできます。ただし、検出が速すぎると、ネットワークが一時的に輻輳したときに不要なスイッチオーバーが発生する可能性があります。

1 回のポーリング期間中に装置がフェールオーバー リンクで hello パケットを受信しなかった場合、残りのインターフェイスで追加テストが実行されます。それでも保持時間内にピア装置から応答がない場合、その装置は故障していると見なされ、故障した装置がアクティブ装置の場合は、スタンバイ装置がアクティブ装置を引き継ぎます。

failover polltime [**unit**] コマンドおよび **failover polltime interface** コマンドの両方をコンフィギュレーションに含めることができます。

(注) フェールオーバー設定で、CTIQBE トラフィックが ASA を通過する場合には、ASA のフェールオーバー ホールド タイムを 30 秒未満に減らす必要があります。CTIQBE キープアライブ タイムアウトは 30 秒であるため、フェールオーバーの状況ではフェールオーバーが発生する前にタイムアウトする可能性があります。CTIQBE がタイムアウトした場合、Cisco CallManager への Cisco IP SoftPhone の接続はドロップされ、IP SoftPhone クライアントは CallManager に再登録する必要があります。

例

次に、ユニットのポーリング タイムの頻度を 3 秒に変更する例を示します。

```
ciscoasa(config)# failover polltime 3
```

次に、200 ミリ秒ごとに hello パケットを送信し、800 ミリ秒以内にフェールオーバー インターフェイスで hello パケットを受信しないとフェールオーバーを実行するように ASA を設定する例を示します。オプションの **unit** キーワードがコマンドに含まれています。

```
ciscoasa(config)# failover polltime unit msec 200 holdtime msec 800
```

関連コマンド

コマンド	説明
failover polltime interface	Active/Standby フェールオーバー コンフィギュレーションのインターフェイス ポーリング期間およびホールド タイムを指定します。
polltime interface	Active/Active フェールオーバー コンフィギュレーションのインターフェイス ポーリング タイムおよびホールド タイムを指定します。
show failover	フェールオーバー コンフィギュレーションの情報を表示します。

failover polltime interface

Active/Standby フェールオーバー コンフィギュレーションのデータ インターフェイスの polltime および holdtime を指定するには、グローバル コンフィギュレーション モードで **failover polltime interface** コマンドを使用します。デフォルトの polltime および holdtime を復元するには、このコマンドの **no** 形式を使用します。

failover polltime interface [**msec**] *polltime* [**holdtime** *time*]

no failover polltime interface [**msec**] *polltime* [**holdtime** *time*]

構文の説明

holdtime *time*	(任意) ピア ユニットからの最後に受信した hello メッセージとインターフェイス テストの開始との間の時間 (計算として) を設定して、インターフェイスの健全性を判断します。また、各インターフェイス テストの期間を *holdtime*/16 として設定します。有効な値は 5 ～ 75 秒です。デフォルトは、*polltime* の 5 倍です。*polltime* の 5 倍よりも短い holdtime 値は入力できません。 インターフェイス テストを開始するまでの時間 (y) を計算するには、次のようにします。 1. x = (*holdtime*/*polltime*)/2、最も近い整数に丸められます。(.4 以下は切り下げ、.5 以上は切り上げ。) 2. y = x**polltime* たとえば、デフォルトの holdtime は 25 で、polltime が 5 の場合は y は 15 秒です。
polltime	hello パケットをピアに送信するまで待機する時間を指定します。有効な値の範囲は、1 ～ 15 秒です。デフォルトは 5 分です。オプションの **msec** キーワードを使用した場合、有効な値は 500 ～ 999 ミリ秒です。
msec	(任意) 指定する時間がミリ秒単位であることを指定します。

デフォルト

デフォルト値は次のとおりです。

- ポーリングの *time* は 5 秒です。
- **holdtime** *time* は、ポーリングの *time* の 5 倍です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**failover poll** コマンドから **failover polltime** コマンドに変更され、**unit** キーワード、**interface** キーワード、および **holdtime** キーワードが含まれるようになりました。
7.2(1)	オプションの **holdtime** *time* と、ミリ秒単位でポーリング タイムを指定する機能が追加されました。

使用上のガイドライン

このコマンドは、Active/Standby フェールオーバーにのみ使用可能です。Active/Active フェールオーバーでは、フェールオーバー グループ コンフィギュレーション モードで **polltime interface** コマンドを使用します。

ポーリング時間が短いほど、ASA は短時間で故障を検出し、フェールオーバーをトリガーできます。ただし短時間での検出は、ネットワークが一時的に輻輳した場合に不要な切り替えが行われる原因となります。

failover polltime unit コマンドと **failover polltime interface** コマンドの両方をコンフィギュレーションに含めることができます。

(注) フェールオーバー設定で、CTIQBE トラフィックが ASA を通過する場合には、ASA のフェールオーバー ホールド タイムを 30 秒未満に減らす必要があります。CTIQBE キープアライブ タイムアウトは 30 秒であるため、フェールオーバーの状況ではフェールオーバーが発生する前にタイムアウトする可能性があります。CTIQBE がタイムアウトした場合、Cisco CallManager への Cisco IP SoftPhone の接続はドロップされ、IP SoftPhone クライアントは CallManager に再登録する必要があります。

例

次に、インターフェイスの polltime の頻度を 15 秒に設定する例を示します。

```
ciscoasa(config)# failover polltime interface 15
```

次に、インターフェイスの polltime の頻度を 500 ミリ秒に、holdtime を 5 秒に設定する例を示します。

```
ciscoasa(config)# failover polltime interface msec 500 holdtime 5
```

関連コマンド

コマンド	説明
failover polltime	装置のフェールオーバー ポーリング期間とホールド タイムを指定します。
polltime interface	Active/Active フェールオーバー コンフィギュレーションのインターフェイス ポーリング タイムを指定します。
show failover	フェールオーバー コンフィギュレーションの情報を表示します。

failover poll-time link-state

インターフェイス リンク ステートのポーリング時間を変更するには、グローバル コンフィギュレーション モードで **failover polltime link-state** コマンドを使用します。リンクステート ポールをディセーブルにするには、このコマンドの **no** 形式を使用します。

failover polltime link-state msec *poll_time*

no failover polltime link-state msec *poll_time*

構文の説明

msec *poll_time*	ポーリング時間を 300 ～ 799 ミリ秒で設定します。

コマンド デフォルト

デフォルトのポーリング時間は 500 ミリ秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、フェールオーバーのペアの ASA では、インターフェイスのリンク ステートが 500 ミリ秒ごとに確認されます。polltime はカスタマイズできます。たとえば、polltime を 300 ミリ秒に設定すると、ASA ではインターフェイスの障害やトリガーのフェールオーバーをより早く検出できるようになります。

アクティブ/アクティブ モードでは、システムに対してこのレートを設定します。フェールオーバー グループごとにこのレートを設定することはできません。

例

次に、リンクステートのポーリング時間を 300 ミリ秒に設定する例を示します。

```
ciscoasa(config)# failover polltime link-state msec 300
```

関連コマンド

コマンド	説明
failover polltime unit	ユニット ヘルス チェックのポーリング時間を設定します。
failover polltime interface	インターフェイス ヘルス チェックのポーリング時間を設定します。

failover reload-standby

スタンバイ ユニットを強制的にリブートするには、特権 EXEC モードで **failover reload-standby** コマンドを使用します。

failover reload-standby

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

フェールオーバー ユニットが同期化されないときにこのコマンドを使用します。スタンバイ ユニットが再起動し、起動終了後にアクティブ ユニットと再同期化されます。

例

次に、アクティブ ユニットで **failover reload-standby** コマンドを使用して、スタンバイ ユニットを強制的にリブートする例を示します。

```
ciscoasa# failover reload-standby
```

関連コマンド

コマンド	説明
write standby	実行コンフィギュレーションをスタンバイ ユニットのメモリに書き込みます。

failover replication http

HTTP（ポート 80）接続のレプリケーションをイネーブルにするには、グローバル コンフィギュレーション モードで **failover replication http** コマンドを使用します。HTTP 接続の複製をディセーブルにするには、このコマンドの **no** 形式を使用します。

failover replication http

no failover replication http

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**failover replicate http** から **failover replication http** に変更されました。

使用上のガイドライン

デフォルトでは、ステートフル フェールオーバーがイネーブルの場合、ASA は HTTP セッション情報を複製しません。HTTP セッションは通常は存続期間が短く、また HTTP クライアントは接続試行が失敗すると通常は再試行するため、HTTP セッションの複製をしないことでシステムのパフォーマンスが向上します。複製をしなくても重要なデータや接続は失われません。**failover replication http** コマンドを使用すると、ステートフル フェールオーバー環境において HTTP セッションのステートフル レプリケーションが可能になりますが、システムのパフォーマンスに悪影響がある可能性があります。

Active/Active フェールオーバー コンフィギュレーションでは、フェールオーバー グループ コンフィギュレーション モードで **replication http** コマンドを使用して、フェールオーバー グループごとに HTTP セッションのレプリケーションを制御します。

例

次に、HTTP 接続のレプリケーションをイネーブルにする例を示します。

```
ciscoasa(config)# failover replication http
```

関連コマンド

コマンド	説明
replication http	特定のフェールオーバー グループに対して、HTTP セッションのレプリケーションをイネーブルにします。
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。

failover replication rate

バルク同期接続レプリケーション レートを設定するには、グローバル コンフィギュレーション モードで **failover replication rate** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

failover replication rate *rate*

no failover replication rate

構文の説明

rate	1 秒あたりの接続数を設定します。値とデフォルト設定はモデルの 1 秒あたりの最大接続数に応じて異なります。

コマンド デフォルト

モデルに応じて異なります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.4(4.1)/8.5(1.7)	このコマンドが追加されました。

使用上のガイドライン

ステートフル フェールオーバーを使用したときの、ASA がスタンバイ ユニットへ接続を複製するレートを設定できます。デフォルトでは、接続は 15 秒間隔でスタンバイ装置に複製されます。ただし、バルク同期が発生すると（たとえば、フェールオーバーを最初にイネーブルにしたときなど）、1 秒あたりの最大接続数の制限のために、大量の接続を同期するのに 15 秒では不十分な場合があります。たとえば、ASASM での最大接続数を 800 万とします。800 万の接続を 15 秒間で複製するということは、1 秒あたり約 53 万 3 千の接続を作成するということです。ただし、1 秒あたりに許可される最大接続数は 30 万です。複製レートが 1 秒あたりの最大接続数以下になるように指定できるようになり、同期期間はすべての接続が同期されるまで調整されます。

例

次に、フェールオーバー レプリケーション レートを 1 秒あたり 20000 接続に設定する例を示します。

```
ciscoasa(config)# failover replication rate 20000
```

関連コマンド

コマンド	説明
failover rate http	HTTP 接続レプリケーションをイネーブルにします。

failover reset

障害が発生した ASA を障害が発生していない状態に復元するには、特権 EXEC モードで **failover reset** コマンドを使用します。

failover reset [**group** *group_id*]

構文の説明

group	（任意）フェールオーバー グループを指定します。**group** キーワードは、Active/Active フェールオーバーに対してのみ適用されます。
group_id	フェールオーバー グループの番号。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、オプションのフェールオーバー グループ ID を追加するように変更されました。

使用上のガイドライン

failover reset コマンドを使用すると、障害が発生したユニットまたはグループを、障害が発生していない状態に変更できます。**failover reset** コマンドはいずれのユニットでも入力できますが、常にアクティブ ユニットでコマンドを入力することを推奨します。アクティブ ユニットで **failover reset** コマンドを入力すると、スタンバイ ユニットが障害が発生していない状態に復元されます。

show failover コマンドまたは **show failover state** コマンドを使用して、ユニットのフェールオーバー ステータスを表示できます。

このコマンドの **no** 形式はありません。

Active/Active フェールオーバーでは、**failover reset** を入力すると、ユニット全体がリセットされます。コマンドにフェールオーバー グループを指定すると、指定したグループのみがリセットされます。

例

次に、障害が発生したユニットを障害が発生していない状態に変更する例を示します。

```
ciscoasa# failover reset
```

関連コマンド

コマンド	説明
failover interface-policy	モニタリングによってインターフェイスの障害が検出された場合のフェールオーバー ポリシーを指定します。
show failover	装置のフェールオーバー ステータスに関する情報を表示します。

failover standby config-lock

フェールオーバー ペアのスタンバイ ユニットまたはスタンバイ コンテキストに対するコンフィギュレーションの変更をロックするには、グローバル コンフィギュレーション モードで **failover standby config-lock** コマンドを使用します。スタンバイ ユニットでのコンフィギュレーションを許可するには、このコマンドの **no** 形式を使用します。

failover standby config-lock

no failover standby config-lock

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトでは、スタンバイ ユニットまたはスタンバイ コンテキストに対するコンフィギュレーションは、警告メッセージ付きで許可されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

使用上のガイドライン

通常のコンフィギュレーション同期以外の変更をスタンバイ ユニットに加えることができないように、スタンバイ ユニット（Active/Standby フェールオーバー）またはスタンバイ コンテキスト（Active/Active フェールオーバー）に対するコンフィギュレーション変更をロックできます。

例

次に、スタンバイ ユニットに対するコンフィギュレーションを許可しない例を示します。

```
ciscoasa(config)# failover standby config-lock
```

関連コマンド

コマンド	説明
clear configure failover	**failover** コマンドを実行コンフィギュレーションから消去し、フェールオーバーのデフォルト値に戻します。
failover active	スタンバイ ユニットをアクティブに切り替えます。
show failover	装置のフェールオーバー ステータスに関する情報を表示します。
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。

failover timeout

非対称ルーテッド セッションのフェールオーバー再接続タイムアウト値を指定するには、グローバル コンフィギュレーション モードで **failover timeout** コマンドを使用します。デフォルトのタイムアウト値に戻すには、このコマンドの **no** 形式を使用します。

failover timeout *hh*[**:***mm*:[**:***ss*]

no failover timeout [*hh*[**:***mm*:[**:***ss*]]

構文の説明

hh	タイムアウト値の時間を指定します。有効な値の範囲は、-1 ～ 1193 です。デフォルトでは、この値は 0 に設定されています。 この値を -1 に設定すると、タイムアウトがディセーブルになり、任意の時間が経過したあとでも接続を再開できます。 この値を 0 に設定し、他のタイムアウト値を指定しないと、コマンドがデフォルト値に設定されて再接続ができなくなります。**no failover timeout** コマンドを入力しても、この値がデフォルト(0)に設定されます。 **(注)** デフォルト値に設定すると、このコマンドは実行コンフィギュレーションに表示されません。
mm	(任意)タイムアウト値の分を指定します。有効な値の範囲は 0 ～ 59 です。デフォルトでは、この値は 0 に設定されています。
ss	(任意)タイムアウト値の秒を指定します。有効な値の範囲は 0 ～ 59 です。デフォルトでは、この値は 0 に設定されています。

デフォルト

デフォルトで、*hh*、*mm*、および *ss* は 0 であり、再接続はできないようになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、コマンド リストに表示されるように変更されました。

使用上のガイドライン

このコマンドは、**nailed** オプションを指定した **static** コマンドとともに使用されます。**nailed** オプションを指定すると、起動後、またはシステムがアクティブになった後、指定した時間内に接続を再確立できます。**failover timeout** コマンドでは、その時間を指定します。設定しない場合は、接続を再確立できません。**failover timeout** コマンドは、**asr-group** コマンドには影響しません。

(注) **nailed** オプションを **static** コマンドに追加すると、その接続で TCP ステート トラッキングとシーケンス チェックがスキップされます。

このコマンドの **no** 形式を使用すると、デフォルト値に戻ります。**failover timeout 0** を入力しても、デフォルト値に戻ります。デフォルト値に設定すると、このコマンドは実行コンフィギュレーションに表示されません。

例

次に、スタンバイ グループ 1 をアクティブに切り替える例を示します。

```
ciscoasa(config)# failover timeout 12:30
ciscoasa(config)# show running-config failover
no failover
failover timeout 12:30:00
```

関連コマンド

コマンド	説明
static	ローカル IP アドレスをグローバル IP アドレスにマッピングすることによって、固定の 1 対 1 のアドレス変換ルールを設定します。

fallback（廃止）

接続の整合性が低下した場合に Cisco Intercompany Media Engine が VoIP から PSTN へフォールバックするために使用するフォールバック タイマーを設定するには、uc-ime コンフィギュレーション モードで **fallback** コマンドを使用します。フォールバックの設定を削除するには、このコマンドの **no** 形式を使用します。

fallback {**sensitivity-file** *filename* | **monitoring timer** *timer_millisec* **hold-down timer** *timer_sec*}

no fallback fallback {**sensitivity-file** *filename* | **monitoring timer** *timer_millisec* **hold-down timer** *timer_sec*}

構文の説明

filename	感度ファイルのファイル名を指定します。.fbs ファイル拡張子が含まれる、ディスクにあるファイルの名前を入力します。ファイル名を指定するときに、ローカル ディスク上のパスを含めることができます（例: `disk0:/file001.fbs`）。
hold-down timer	PSTN にフォールバックするかどうかを Cisco UCM に通知するまでに ASA が待機する時間を設定します。
monitoring timer	インターネットから受信した RTP パケットを ASA でサンプリングする時間間隔を設定します。ASA は、このデータ サンプルを使用して、通話に対して PSTN へのフォールバックが必要かどうか判断します。
sensitivity-file	通話中の PSTN フォールバックに使用するファイルを指定します。感度ファイルは ASA により解析され、RMA ライブラリに入力されます。
timer_millisec	ミリ秒単位でモニタリング タイマーの長さを指定します。10 ～ 600 の範囲で整数を入力します。デフォルトのモニタリング タイマーの長さは 100 ミリ秒です。
timer_sec	ホールドダウン タイマーの長さを秒単位で指定します。10 ～ 360 の範囲で整数を入力します。デフォルトのホールドダウン タイマーの長さは 20 秒です。

デフォルト

デフォルトのモニタリング タイマーの長さは 100 ミリ秒です。ホールドダウン タイマーの長さは 20 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
uc-ime コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.3(1)	コマンドが追加されました。
9.4(1)	このコマンドは、すべての **uc-ime** モード コマンドとともに廃止されました。

使用上のガイドライン

Cisco Intercompany Media Engine のフォールバック タイマーを指定します。

インターネット接続は、時間とともに品質が大幅に変化する可能性があります。そのため、接続の品質が良くてコールが VoIP 上で送信されたとしても、その接続品質は通話中に低下する可能性があります。エンド ユーザに対して全体にわたって良好な通話を保証するために、Cisco Intercompany Media Engine では通話中のフォールバックの実行が試みられます。

通話中のフォールバックを実行するには、インターネットから着信する RTP パケットを ASA でモニタし、情報を RTP Monitoring Algorithm（RMA）API に送信する必要があります。これにより、フォールバックが必要かどうかが ASA に示されます。フォールバックが必要になると、コールを PSTN へフォールバックする必要があることを通知するために、ASA から Cisco UCM に REFER メッセージが送信されます。

（注） SIP インスペクションに対して Cisco Intercompany Media Engine プロキシがイネーブルの場合、フォールバック タイマーは変更できません。フォールバック タイマーを変更する前に、Cisco Intercompany Media Engine プロキシを SIP インスペクションから削除します。

例

次に、フォールバック タイマーを指定するとともに、Cisco Intercompany Media Engine を設定する方法の例を示します。

```
ciscoasa(config)# uc-ime local_uc-ime_proxy
ciscoasa(config-uc-ime)# media-termination ime-media-term
ciscoasa(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure
ciscoasa(config-uc-ime)# ticket epoch 1 password password1234
ciscoasa(config-uc-ime)# fallback monitoring timer 120
ciscoasa(config-uc-ime)# fallback hold-down timer 30
```

次に、感度ファイルを指定するとともに、Cisco Intercompany Media Engine を設定する方法の例を示します。

```
ciscoasa(config)# uc-ime local_uc-ime_proxy
ciscoasa(config-uc-ime)# media-termination ime-media-term
ciscoasa(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure
ciscoasa(config-uc-ime)# ticket epoch 1 password password1234
ciscoasa(config-uc-ime)# fallback sensitivity-file local_uc-ime_fallback_policy
```

関連コマンド

コマンド	説明
show running-config uc-ime	Cisco Intercompany Media Engine プロキシの実行コンフィギュレーションを表示します。
show uc-ime	フォールバック通知、マッピング サービス セッション、およびシグナリング セッションに関する統計情報または詳細情報を表示します。
uc-ime	Cisco Intercompany Media Engine プロキシ インスタンスを ASA に作成します。

fast-flood

IS-IS リンクステート パケット（LSP）をフラッディングするには、ルータ ISIS コンフィギュレーション モードで **fast-flood** コマンドを使用します。高速フラッディングをディセーブルにするには、このコマンドの **no** 形式を使用します。

fast-flood [*lsp-number*]

no fast-flood [*lsp-number*]

構文の説明

lsp-number	（任意）SPF の開始前にフラッディングする LSP の数です。指定できる範囲は 1 ～ 15 です。デフォルトは 5 分です。

デフォルト

高速フラッディングはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ isis コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	コマンドが追加されました。

使用上のガイドライン

fast-flood コマンドでは、指定した数の LSP が ASA から送信されます。LSP 数を指定しない場合、デフォルトとして 5 が使用されます。LSP は、SPF の実行前に SPF を呼び出します。LSP フラッディング プロセスを高速化すると、ネットワークの全体的なコンバージェンス時間が向上します。

ASA は SPF 計算を実行する前に、少なくとも SPF をトリガーした LSP を常にフラッディングする必要があります。

コンバージェンス時間を短縮するために、ASA が SPF 計算を実行する前に、LSP の高速フラッディングをイネーブルにしておくことをお勧めします。

例

次の例では、**fast-flood** コマンドを入力して、SPF 計算が開始される前に、SPF を呼び出す最初の 7 個の LSP をフラッディングするようにルータを設定しています。**show running-configuration** コマンドを入力すると、出力から、ASA で高速フラッディングがイネーブルにされていることがわかります。

```
ciscoasa# clear isis rib redistribution 10.1.0.0 255.255.0.0
ciscoasa> enable
ciscoasa# configure terminal
ciscoasa(config)# router isis
ciscoasa(config-router)# fast-flood 7
ciscoasa(config-router)# end
ciscoasa# show running-config | inc fast-flood

fast-flood 7
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。

コマンド	説明
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト(TLV)を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。

コマンド	説明
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

CHAPTER 16

feature コマンドから fxos port コマンド

feature

スマート ライセンス機能権限付与を要求するには、ライセンス スマート コンフィギュレーション モードで **feature** コマンドを使用します。この機能を削除するには、このコマンドの **no** 形式を使用します。

(注) このコマンドは、ASAv および FirePOWER シャーシでのみサポートされています。

feature {tier standard | strong-encryption | context *number* **| mobile-sp | carrier}**

no feature {tier standard | strong-encryption | context *number* **| mobile-sp | carrier}**

構文の説明

carrier	(FirePOWER 9300/4100 のみ) キャリア (GTP/GPRS、Diameter、SCTP) ライセンスを要求します。このライセンスは、モバイル SP ライセンスを置き換えます。
context *number*	(FirePOWER シャーシのみ) セキュリティ コンテキストのライセンスを要求します。標準ライセンスに含まれるデフォルトのコンテキストの数は差し引いてください。たとえば、ご使用のモデルが 250 のコンテキストをサポートしており、デフォルトのコンテキストの数が 10 の場合、要求するコンテキストの数は 240 までにする必要があります。
mobile-sp	(FirePOWER 9300/4100 のみ) モバイル SP (GTP/GPRS) ライセンスを要求します。このライセンスは、Version 9.5(2) のキャリア ライセンスに置き換えられて廃止されました。
strong-encryption	(FirePOWER シャーシのみ) 高度暗号化 (3DES) ライセンスを要求します。FXOS 1.1.3 以降では、対象となるお客様がデバイスを登録すると、高度暗号化ライセンスが自動的に有効になります。このコマンドを使用する必要があるのは、2.3.0 より前のスマート ソフトウェア マネージャ サテライトのユーザだけです。
tier standard	使用可能なオプションは標準層だけです。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ライセンス スマート コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。
9.4(1.152)	Firepower 9300 ASA セキュリティ モジュールのサポートと、キーワード **strong-encryption**、**mobile-sp**、および **context** が追加されました。
9.5(2)	**mobile-sp** キーワードが **carrier** キーワードに置き換えられました。**strong-encryption** キーワードが廃止されました（2.3.0 より前のスマート ソフトウェア マネージャ サテライトのユーザを除く）。
9.6(1)	Firepower 4100 シリーズのサポートが追加されました。
9.8(2)	Firepower 2100 シリーズのサポートが追加されました。

使用上のガイドライン

ASAv の場合、初めて機能層を要求したときは、変更を有効にするためにライセンス スマート コンフィギュレーション モードを終了する必要があります。シスコ ライセンス認証局で認可された後で機能層を変更した場合、変更を有効にするために ASAv をリロードする必要があります。

例

次に、ASAv 機能層を標準に設定し、スループット レベルを 2G に設定する例を示します。

```
ciscoasa# license smart
ciscoasa(config-smart-lic)# feature tier standard
ciscoasa(config-smart-lic)# throughput level 2G
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

関連コマンド

コマンド	説明
call-home	Smart Call Home を設定します。スマート ライセンスでは、Smart Call Home インフラストラクチャが使用されます。
clear configure license	スマート ライセンス設定をクリアします。
http-proxy	スマート ライセンスおよび Smart Call Home の HTTP(S) プロキシを設定します。
license smart	スマート ライセンスのライセンス権限付与を要求できます。
license smart deregister	ライセンス認証局からデバイスを登録解除します。
license smart register	デバイスをライセンス認証局に登録します。

コマンド	説明
license smart renew	登録またはライセンス権限を更新します。
service call-home	Smart Call Home をイネーブルにします。
show license	スマート ライセンスのステータスを表示します。
show running-config license	スマート ライセンスの設定を表示します。
throughput level	スマート ライセンスのスループット レベルを設定します。

file-bookmarks

認証された WebVPN ユーザに表示される WebVPN ホームページの [File Bookmarks] タイトルまたは [File Bookmarks] リンクをカスタマイズするには、webvpn カスタマイゼーション コンフィギュレーション モードで **file-bookmarks** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

file-bookmarks {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

no file-bookmarks {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

構文の説明

link	リンクへの変更を指定します。
title	タイトルへの変更を指定します。
style	HTML スタイルへの変更を指定します。
text	テキストへの変更を指定します。
value	表示する実際のテキストまたは CSS パラメータ（最大 256 文字）。

デフォルト

デフォルトのリンクのスタイルは color:#669999;border-bottom: 1px solid #669999;text-decoration:none です。

デフォルトのタイトルのスタイルは color:#669999;background-color:#99CCCC;font-weight:bold です。

デフォルトのタイトル テキストは「File Folder Bookmarks」です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn カスタマイゼーション コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

style オプションは、任意の有効な CSS パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、W3C の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進数値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、[File Bookmarks] タイトルを「Corporate File Bookmarks」にカスタマイズする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# file-bookmarks title text Corporate File Bookmarks
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの [Application Access] ボックスをカスタマイズします。
browse-networks	WebVPN ホームページの [Browse Networks] ボックスをカスタマイズします。
web-applications	WebVPN ホームページの [Web Application] ボックスをカスタマイズします。
web-bookmarks	WebVPN ホームページの [Web Bookmarks] タイトルまたはリンクをカスタマイズします。

file-browsing

ファイル サーバまたは共有の CIFS または FTP によるファイル ブラウジングをイネーブルまたはディセーブルにするには、DAP webvpn コンフィギュレーション モードで **file-browsing** コマンドを使用します。

file-browsing enable | disable

構文の説明

enable | disable	ファイル サーバまたは共有のブラウズ機能をイネーブルまたはディセーブルにします。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
DAP webvpn コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

ファイル ブラウジングには、次の使用上の注意事項があります。

- ファイル ブラウジングでは、国際化はサポートされていません。
- ブラウズには、NBNS（マスター ブラウザまたは WINS）が必要です。NBNS に障害が発生した場合や、NBNS が設定されていない場合は、DNS を使用します。

ASA は、さまざまなソースからの属性値を適用できます。次の階層に従って、属性値を適用します。

1. DAP レコード
2. ユーザ名
3. グループ ポリシー
4. トンネル グループのグループ ポリシー
5. デフォルトのグループ ポリシー

したがって、属性の DAP 値は、ユーザ、グループ ポリシー、またはトンネル グループに設定されたものよりも優先順位が高くなります。

DAP レコードの属性をイネーブルまたはディセーブルにすると、ASA はその値を適用して実行します。たとえば、DAP webvpn コンフィギュレーション モードでファイル ブラウジングをディセーブルにした場合、ASA はそれ以上値を検索しません。ディセーブルにする代わりに **file-browsing** コマンドで no の値を設定した場合、属性は DAP レコードには存在しないため、ASA はユーザ名の AAA 属性に移動し、必要に応じてグループ ポリシーにも移動して、適用する値を検索します。

例

次に、Finance という DAP レコードでファイル ブラウジングをイネーブルにする例を示します。

```
ciscoasa (config)# config-dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)# webvpn
ciscoasa(config-dap-webvpn)# file-browsing enable
ciscoasa(config-dap-webvpn)#
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
file-entry	アクセス先のファイル サーバの名前を入力する機能をイ ネーブルまたはディセーブルにします。

file-encoding

Common Internet File System サーバからのページの文字エンコーディングを指定するには、webvpn コンフィギュレーション モードで **file-encoding** コマンドを使用します。file-encoding 属性の値を削除するには、このコマンドの **no** 形式を使用します。

file-encoding {**server-name** | **server-ip-addr**} *charset*

no file-encoding {**server-name** | **server-ip-addr**}

構文の説明

charset	最大 40 文字から成るストリングで、http://www.iana.org/assignments/character-sets で特定されている有効な文字セットのいずれかに相当するもの。このページに示されている文字セットの名前またはエイリアスのいずれかを使用できます。たとえば、iso-8859-1、shift_jis、ibm850 などです。 この文字列は、大文字と小文字が区別されません。ASA 設定内では、コマンド インタープリタによって大文字が小文字に変換されます。
server-ip-addr	文字エンコーディングを指定する CIFS サーバの IP アドレス（ドット付き 10 進表記）。
server-name	文字エンコーディングを指定する CIFS サーバの名前。 ASA では、指定した大文字と小文字の区別が保持されますが、名前をサーバと照合するときには大文字と小文字は区別されません。

デフォルト

WebVPN コンフィギュレーションに明示的な file-encoding エントリがないすべての CIFS サーバからのページでは、character-encoding 属性の文字エンコーディング値が継承されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

webvpn 文字エンコーディング属性の値とは異なる文字エンコーディング エントリが必要なすべての CIFS サーバに対して、ファイル エンコーディング エントリを入力します。

CIFS サーバから WebVPN ユーザにダウンロードされた WebVPN ポータル ページは、サーバを識別する WebVPN ファイル エンコーディング属性の値を符号化します。符号化が行われなかった場合は、文字エンコーディング属性の値を継承します。リモート ユーザのブラウザでは、ブラウザの文字エンコード セットのエントリにこの値がマップされ、使用する正しい文字セットが決定されます。WebVPN コンフィギュレーションで CIFS サーバ用の file-encoding エントリが指定されず、character-encoding 属性も設定されていない場合、WebVPN ポータル ページは値を指定しません。WebVPN ポータル ページが文字エンコーディングを指定しない場合、またはブラウザがサポートしていない文字エンコーディング値を指定した場合、リモート ブラウザはブラウザ自体のデフォルト エンコーディングを使用します。

CIFS サーバに適切な文字エンコーディングを、広域的には webvpn 文字エンコーディング属性によって、個別的にはファイル エンコーディングの上書きによってマッピングすることで、ページと同様にファイル名やディレクトリ パスを正しくレンダリングすることが必要な場合には、CIFS ページの正確な処理と表示が可能になります。

(注) 文字エンコーディングおよびファイル エンコーディングの値は、ブラウザによって使用されるフォント ファミリを排除するものではありません。次の例に示すように日本語の Shift_JIS 文字エンコーディングを使用する場合などは、webvpn カスタマイゼーション コマンド モードで **page style** コマンドを使用してフォント ファミリを置換し、これらの値の 1 つの設定を補足するか、または webvpn カスタマイゼーション コマンド モードで **no page style** コマンドを入力してフォント ファミリを削除する必要があります。

例

次の例では、「CISCO-server-jp」という名前の CIFS サーバが日本語の Shift_JIS 文字をサポートするようにファイル エンコーディング属性を設定し、フォント ファミリを削除して、デフォルトの背景色を保持しています。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# file-encoding CISCO-server-jp shift_jis
ciscoasa(config-webvpn)# customization DfltCustomization
ciscoasa(config-webvpn-custom)# page style background-color:white
ciscoasa(config-webvpn-custom)#
```

次に、CIFS サーバ 10.86.5.174 のファイル エンコーディング属性を設定して、IBM860（エイリアス「CP860」）文字をサポートする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# file-encoding 10.86.5.174 cp860
ciscoasa(config-webvpn)
```

関連コマンド

コマンド	説明
character-encoding	WebVPN コンフィギュレーションのファイル エンコーディング エントリに指定されたサーバのページを除き、すべての WebVPN ポータル ページで使用されるグローバルな文字エンコーディングを指定します。
show running-config webvpn	WebVPN の実行コンフィギュレーションを表示します。デフォルト コンフィギュレーションを組み込むには **all** キーワードを使用します。
debug webvpn cifs	Common Internet File System についてのデバッグ メッセージを表示します。

file-entry

アクセスするファイル サーバ名をユーザが入力できる機能をイネーブルまたはディセーブルにするには、DAP webvpn コンフィギュレーション モードで **file-entry** コマンドを使用します。

file-entry enable | disable

構文の説明

enable | disable	アクセス先のファイル サーバの名前を入力する機能をイ ネーブルまたはディセーブルにします。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
DAP webvpn コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

ASA は、次の階層に従って、さまざまなソースから属性値を適用できます。

1. DAP レコード
2. ユーザ名
3. グループ ポリシー
4. 接続プロファイル(トンネル グループ)のグループ ポリシー
5. デフォルトのグループ ポリシー

属性の DAP 値には、ユーザ、グループ ポリシー、または接続プロファイルよりも高いプライオリティが設定されています。

DAP レコードの属性をイネーブルまたはディセーブルにすると、ASA はその値を適用して実行します。たとえば、DAP webvpn コンフィギュレーション モードでファイル入力をディセーブルにした場合、ASA はそれ以上値を検索しません。ディセーブルにする代わりに **file-entry** コマンドで no の値を設定した場合、属性は DAP レコードには存在しないため、ASA はユーザ名の AAA 属性に移動し、必要に応じてグループ ポリシーにも移動して、適用する値を検索します。

例

次に、Finance という DAP レコードでファイル サーバ名の入力をイネーブルにする例を示します。

```
ciscoasa (config)# config-dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)# webvpn
ciscoasa(config-dap-webvpn)# file-entry enable
ciscoasa(config-dap-webvpn)#
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
file-browsing	ファイル サーバまたは共有のブラウズ機能をイネーブルまたはディセーブルにします。

filter

特定のグループ ポリシーまたはユーザ名の WebVPN 接続で使用するアクセス リストの名前を指定するには、webvpn コンフィギュレーション モードで **filter** コマンドを使用します。アクセス リストを削除するには、このコマンドの **no** 形式を使用します。

filter {**value** *ACLname* | **none**}

no filter

構文の説明

none	WebVPN タイプのアクセス リストがないことを示します。ヌル値を設定して、アクセス リストを使用できないようにします。アクセス リストを他のグループ ポリシーから継承しないようにします。
value *ACLname*	事前に設定済みのアクセス リストの名前を指定します。

デフォルト

WebVPN アクセス リストは、**filter** コマンドを使用してアクセス リストを指定するまでは適用されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

no オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。フィルタ値を継承しないようにするには、**filter value none** コマンドを使用します。

このユーザまたはグループ ポリシーに対する、さまざまなタイプのトラフィックを許可または拒否するには、ACL を設定します。その後、**filter** コマンドを使用して、これらの WebVPN トラフィック用の ACL を適用します。

WebVPN では、**vpn-filter** コマンドで定義された ACL は使用されません。

例

次に、FirstGroup という名前のグループ ポリシーで *acl_in* という名前のアクセス リストを呼び出すフィルタを設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# filter acl_in
```

関連コマンド

コマンド	説明
access-list	アクセス リストを作成するか、ダウンロード可能なアクセス リストを使用します。
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。webvpn コンフィギュレーション モードを開始して、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。

filter activex

ASA を通過する HTTP トラフィック内の ActiveX オブジェクトを削除するには、グローバル コンフィギュレーション モードで **filter activex** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

filter activex *port* [**-***port*] | **except** *local_ip mask foreign_ip foreign_mask*

no filter activex *port* [**-***port*] | **except** *local_ip mask foreign_ip foreign_mask*

構文の説明

except	先行の filter 条件に対する例外を作成します。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。0.0.0.0（短縮形は 0）を使用すると、すべてのホストを指定できます。
foreign_mask	*foreign_ip* 引数のネットワーク マスク。常に特定のマスク値を指定します。0.0.0.0（短縮形は 0）を使用すると、すべてのホストを指定できます。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに 0.0.0.0（短縮形は 0）を設定すると、すべてのホストを指定できます。
mask	*local_ip* 引数のネットワーク マスク。0.0.0.0（短縮形は 0）を使用すると、すべてのホストを指定できます。
port	フィルタリングが適用される TCP ポート。一般的に、これはポート 21 ですが、他の値も受け入れられます。ポート 21 の代わりに、http または url リテラルを使用できます。指定できる値の範囲は、0 ～ 65535 です。
-port	（任意）ポート範囲を指定します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ActiveX オブジェクトには、保護されているネットワーク上のホストやサーバを攻撃することを目的とするコードが含まれている場合があるため、セキュリティのリスクが発生する可能性があります。**filter activex** コマンドを使用して、ActiveX オブジェクトをディセーブルにできます。

ActiveX コントロール（旧称：OLE コントロールまたは OCX コントロール）は、Web ページやその他のアプリケーションに挿入できるコンポーネントです。これらのコントロールにはカスタム フォームやカレンダーなど、情報の収集と表示に使用されるサードパーティ製の多様なフォームが含まれています。ActiveX は、技術的に、ネットワーク クライアントに対して多くの問題を発生させる可能性があります。たとえば、ワークステーションの障害の原因となる、ネットワーク セキュリティ問題を引き起こす、またはサーバへの攻撃に利用される、などのおそれがあります。

filter activex コマンドは、HTML **object** コマンドを、HTML Web ページ内でコメントアウトすることでブロックします。<applet> ～ </applet> タグおよび <object classid> ～ </object> タグを選択的にコメントに置換することによって、HTML ファイルの ActiveX フィルタリングが実行されます。ネストされたタグのフィルタリングは、最上位タグをコメントに変換することによってサポートされています。

注意 <object> タグは、Java アプレット、画像ファイル、およびマルチメディア オブジェクトにも使用されます。この場合、これらもこのコマンドによってブロックされます。

<object> または </object> HTML タグが複数のネットワーク パケットに分割されている場合や、タグ内のコードが MTU のバイト数よりも長い場合は、ASA でタグをブロックできません。

alias コマンドによって参照されている IP アドレスにユーザがアクセスした場合、または WebVPN トラフィックでは、ActiveX ブロッキングは行われません。

例

次に、すべての発信接続で ActiveX オブジェクトをブロックする例を示します。

```
ciscoasa(config)# filter activex 80 0 0 0 0
```

このコマンドは、任意のローカル ホストから任意の外部ホストへの接続において、ポート 80 で Web トラフィックに対して ActiveX オブジェクト ブロッキングを適用することを指定します。

関連コマンド\

コマンド	説明
filter url	トラフィックを URL フィルタリング サーバに送ります。
filter java	ASA を通過する HTTP トラフィックから Java アプレットを削除します。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

filter ftp

Websense サーバまたは N2H2 サーバでフィルタリングする FTP トラフィックを指定するには、グローバル コンフィギュレーション モードで **filter ftp** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

filter ftp *port* [**-***port*] | **except** *local_ip mask foreign_ip foreign_mask* [**allow**] [**interact-block**]

no filter ftp *port* [**-***port*] | **except** *local_ip mask foreign_ip foreign_mask* [**allow**] [**interact-block**]

構文の説明

allow	(任意)サーバが利用できない場合に、フィルタリングなしで発信接続が ASA を通過します。このオプションを省略した場合、および N2H2 サーバまたは Websense サーバがオフラインの場合、ASA は、N2H2 サーバまたは Websense サーバがオンラインに戻るまで、発信ポート 80(Web)トラフィックを停止します。
except	先行の filter 条件に対する例外を作成します。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。0.0.0.0(短縮形は 0)を使用すると、すべてのホストを指定できます。
foreign_mask	*foreign_ip* 引数のネットワーク マスク。常に特定のマスク値を指定します。0.0.0.0(短縮形は 0)を使用すると、すべてのホストを指定できます。
interact-block	(任意)ユーザが対話形式の FTP プログラムを使用して FTP サーバに接続することを禁止します。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに 0.0.0.0(短縮形は 0)を設定すると、すべてのホストを指定できます。
mask	*local_ip* 引数のネットワーク マスク。0.0.0.0(短縮形は 0)を使用すると、すべてのホストを指定できます。
port	フィルタリングが適用される TCP ポート。一般的に、これはポート 21 ですが、他の値も受け入れられます。ポート 80 の代わりに、ftp リテラルを使用できます。
-*port*	(任意)ポート範囲を指定します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

filter ftp コマンドを使用すると、Websense サーバまたは N2H2 サーバでフィルタリングする FTP トラフィックを指定できます。

この機能をイネーブルにした後、ユーザがサーバに対して FTP GET 要求を発行すると、ASA は、FTP サーバ、および Websense サーバまたは N2H2 サーバに対して同時に要求を送信します。Websense サーバまたは N2H2 サーバによって接続が許可されると、ASA は成功の FTP リターン コードを変更しないでそのままユーザに返します。たとえば、成功の戻りコードは「250: CWD command successful.」です。

Websense サーバまたは N2H2 サーバによって接続が拒否されると、ASA は FTP リターン コードを変更して、接続が拒否されたことを示します。たとえば、ASA はコード 250 を「550 Requested file is prohibited by URL filtering policy」に変更します。Websense は FTP PUT コマンドのみをフィルタリングし、PUT コマンドのフィルタリングは行いません。

完全なディレクトリ パスを指定しない対話形式の FTP セッションを禁止するには、**interactive-block** オプションを使用します。対話形式の FTP クライアントを使用すると、ユーザは、完全なパスを入力しないでディレクトリを変更できます。たとえば、ユーザは、**cd /public/files** ではなく、**cd ./files** と入力できます。これらのコマンドを使用する前に、URL フィルタリング サーバを指定してイネーブルにする必要があります。

例

次に、FTP フィルタリングをイネーブルにする例を示します。

```
ciscoasa(config)# url-server (perimeter) host 10.0.1.1
ciscoasa(config)# filter ftp 21 0 0 0 0
ciscoasa(config)# filter ftp except 10.0.2.54 255.255.255.255 0 0
```

関連コマンド

コマンド	説明
filter https	Websense サーバまたは N2H2 サーバによってフィルタリングされる HTTPS トラフィックを指定します。
filter java	ASA を通過する HTTP トラフィックから Java アプレットを削除します。
filter url	トラフィックを URL フィルタリング サーバに送ります。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

filter https

N2H2 サーバまたは Websense サーバでフィルタリングする HTTPS トラフィックを指定するには、グローバル コンフィギュレーション モードで **filter https** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

filter https *port* [**-***port*] | **except** *local_ip mask foreign_ip foreign_mask* [**allow**]

no filter https *port* [**-***port*] | **except** *local_ip mask foreign_ip foreign_mask* [**allow**]

構文の説明

allow	（任意）サーバが利用できない場合に、フィルタリングなしで発信接続が ASA を通過します。このオプションを省略した場合に、N2H2 サーバまたは Websense サーバがオフラインになると、ASA は、N2H2 サーバまたは Websense サーバが再度オンラインになるまで、ポート 443 への発信トラフィックを停止します。
except	（オプション）先行の filter 条件に対する例外を作成します。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。0.0.0.0（短縮形は 0）を使用すると、すべてのホストを指定できます。
foreign_mask	*foreign_ip* 引数のネットワーク マスク。常に特定のマスク値を指定します。0.0.0.0（短縮形は 0）を使用すると、すべてのホストを指定できます。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに 0.0.0.0（短縮形は 0）を設定すると、すべてのホストを指定できます。
mask	*local_ip* 引数のネットワーク マスク。0.0.0.0（短縮形は 0）を使用すると、すべてのホストを指定できます。
port	フィルタリングが適用される TCP ポート。一般的に、これはポート 443 ですが、他の値でも受け入れられます。ポート 443 の代わりに、https リテラルを使用できます。
-port	（任意）ポート範囲を指定します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASA は、外部の Websense または N2H2 フィルタリング サーバを使用した HTTPS サイトおよび FTP サイトのフィルタリングをサポートしています。

サイトが許可されない場合、SSL 接続ネゴシエーションを完了させないことによって、HTTPS フィルタリングが行われます。ブラウザに、「The Page or the content cannot be displayed.」のようなエラー メッセージが表示されます。

HTTPS コンテンツは暗号化されているため、ASA は、ディレクトリおよびファイル名の情報を付けずに URL ルックアップを送信します。

例

次に、10.0.2.54 ホストからの接続を除く、すべての発信 HTTPS 接続をフィルタリングする例を示します。

```
ciscoasa(config)# url-server (perimeter) host 10.0.1.1
ciscoasa(config)# filter https 443 0 0 0 0
ciscoasa(config)# filter https except 10.0.2.54 255.255.255.255 0 0
```

関連コマンド

コマンド	説明
filter activex	ASA を通過する HTTP トラフィックから ActiveX オブジェクトを削除します。
filter java	ASA を通過する HTTP トラフィックから Java アプレットを削除します。
filter url	トラフィックを URL フィルタリング サーバに送ります。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

filter java

ASA を通過する HTTP トラフィックから Java アプレットを削除するには、グローバル コンフィギュレーション モードで **filter java** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

filter java {[*port*[**-***port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*]

no filter java {[*port*[**-***port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*]

構文の説明

except	(オプション)先行の filter 条件に対する例外を作成します。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。0.0.0.0(短縮形は 0)を使用すると、すべてのホストを指定できます。
foreign_mask	*foreign_ip* 引数のネットワーク マスク。常に特定のマスク値を指定します。0.0.0.0(短縮形は 0)を使用すると、すべてのホストを指定できます。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに 0.0.0.0(短縮形は 0)を設定すると、すべてのホストを指定できます。
local_mask	*local_ip* 引数のネットワーク マスク。0.0.0.0(短縮形は 0)を使用すると、すべてのホストを指定できます。
port	フィルタリングが適用される TCP ポート。一般的に、これはポート 80 ですが、他の値でも受け入れられます。ポート 80 には http または url リテラルを使用できます。
*port***-***port*	(任意)ポート範囲を指定します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

Java アプレットは、保護されたネットワーク上のホストとサーバを攻撃するコードを含むことがあるため、セキュリティ リスクを引き起こす可能性があります。Java アプレットは、**filter java** コマンドで取り除くことができます。

filter java コマンドは、発信接続から ASA に返される Java アプレットをフィルタリングします。フィルタリングされてもユーザは HTML ページを受信できますが、アプレットの Web ページ ソースはコメントアウトされているため、アプレットは実行できません。**filter java** コマンドでは、WebVPN トラフィックはフィルタリングされません。

<applet> または </applet> HTML タグが複数のネットワーク パケットに分割されている場合や、タグ内のコードが MTU のバイト数よりも長い場合は、ASA でタグをブロックできません。Java アプレットが <object> タグ内にあることがわかっている場合は、**filter activex** コマンドを使用して削除します。

例

次の例では、すべての発信接続で Java アプレットをブロックすることを指定しています。

```
ciscoasa(config)# filter java 80 0 0 0 0
```

次に、Java アプレット ブロックを、すべてのローカル ホストからポート 80 への Web トラフィック、および外部ホストへの接続の Web トラフィックに適用することを指定する例を示します。

次の例では、保護されたネットワーク上のホストへの Java アプレットのダウンロードをブロックしています。

```
ciscoasa(config)# filter java http 192.168.3.3 255.255.255.255 0 0
```

関連コマンド

コマンド	説明
filter activex	ASA を通過する HTTP トラフィックから ActiveX オブジェクトを削除します。
filter url	トラフィックを URL フィルタリング サーバに送ります。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

filter url

トラフィックを URL フィルタリング サーバに転送するには、グローバル コンフィギュレーション モードで **filter url** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

filter url *port* [**-***port*] | **except** *local_ip local_mask foreign_ip foreign_mask* [**allow**] [**cgi-truncate**] [**longurl-truncate** | **longurl-deny**] [**proxy-block**]

no filter url *port* [**-***port*] | **except** *local_ip mask foreign_ip foreign_mask* [**allow**] [**cgi-truncate**] [**longurl-truncate** | **longurl-deny**] [**proxy-block**]

構文の説明

allow	サーバが利用できない場合、発信接続はフィルタリングなしで ASA を通過します。このオプションを省略した場合に、N2H2 サーバまたは Websense サーバがオフラインになると、ASA は、N2H2 サーバまたは Websense サーバが再度オンラインになるまで、発信ポート 80（Web）トラフィックを停止します。
cgi_truncate	CGI スクリプトのように、URL に疑問符（?）から始まるパラメータ リストがある場合は、フィルタリング サーバに送信する URL から、疑問符を含む疑問符以降のすべての文字を削除します。
except	先行の **filter** 条件に対する例外を作成します。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。0.0.0.0（短縮形は 0）を使用すると、すべてのホストを指定できます。
foreign_mask	*foreign_ip* 引数のネットワーク マスク。常に特定のマスク値を指定します。0.0.0.0（短縮形は 0）を使用すると、すべてのホストを指定できます。
http	ポート 80 を指定します。80 の代わりに http または www と入力してポート 80 を指定することもできます。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに 0.0.0.0（短縮形は 0）を設定すると、すべてのホストを指定できます。
local_mask	*local_ip* 引数のネットワーク マスク。0.0.0.0（短縮形は 0）を使用すると、すべてのホストを指定できます。
longurl-deny	URL が URL バッファ サイズの制限を超える場合や、URL バッファが使用できない場合に URL 要求を拒否します。
longurl-truncate	URL が URL バッファの制限を超える場合は、N2H2 サーバまたは Websense サーバに対して元のホスト名または IP アドレスのみを送信します。
-*port*	（任意）フィルタリングの適用対象となる TCP ポート。一般的に、これはポート 80 ですが、他の値でも受け入れられます。ポート 80 には http または url リテラルを使用できます。ハイフンの後にもう 1 つポートを追加すると、ポートの範囲を指定できます。
proxy-block	ユーザの HTTP プロキシ サーバへの接続を禁止します。
url	ASA 経由で伝送されるデータから URL をフィルタリングします。

デフォルト　このコマンドは、デフォルトでディセーブルになっています。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン　**filter url** コマンドを使用すると、N2H2 または Websense フィルタリング アプリケーションを使用して指定した WWW 上の URL への発信ユーザのアクセスを禁止できます。

(注)　**filter url** コマンドを発行する前に、**url-server** コマンドを設定する必要があります。

filter url コマンドの **allow** オプションは、N2H2 サーバまたは Websense サーバがオフラインになった場合の ASA の動作を決定します。**filter url** コマンドで **allow** オプションを使用し、N2H2 サーバまたは Websense サーバがオフラインになった場合、ポート 80 のトラフィックはフィルタリングなしで ASA を通過します。**allow** オプションを指定しないでこのコマンドを使用し、サーバがオフラインになった場合、ASA では、サーバが再度オンラインになるまでポート 80（Web）への発信トラフィックが停止されるか、または別の URL サーバを使用できる場合は次の URL サーバに制御が渡されます。

(注)　**allow** オプションを設定した場合、ASA では、N2H2 サーバまたは Websense サーバがオフラインになると代替サーバに制御が渡されます。

N2H2 サーバまたは Websense サーバは、ASA と連携して動作し、会社のセキュリティ ポリシーに基づいてユーザの Web サイトへのアクセスを拒否します。

フィルタリング サーバの使用方法

Websense プロトコル バージョン 4 では、ホストと ASA との間でのグループおよびユーザ名認証が可能です。ASA は、ユーザ名ルックアップを実行し、その後 Websense サーバが URL フィルタリングおよびユーザ名のロギングを処理します。

N2H2 サーバは、IFP サーバを実行する Windows ワークステーション（2000、NT、または XP）である必要があります。512 MB 以上の RAM を推奨します。また、N2H2 サービスにおける長い URL のサポートは最大 3 KB までとなっており、Websense における制限よりも短くなっています。

Websense プロトコル バージョン 4 では、次の機能が拡張されました。

- URL フィルタリングによって、ASA では、Websense サーバに定義されているポリシーを使用して発信 URL 要求をチェックできます。
- ユーザ名のロギングによって、Websense サーバでユーザ名、グループ、およびドメイン名が追跡されます。
- ユーザ名ルックアップによって、ASA では、ユーザ認証テーブルを使用して、ホストの IP アドレスをユーザ名にマッピングできます。

Websense についての情報は、次の Web サイトで入手できます。

http://www.websense.com/

設定手順

次の手順を実行して、URL フィルタリングを行います。

1. ベンダー固有の適切な形式の **url-server** コマンドを使用して、N2H2 サーバまたは Websense サーバを指定します。
2. **filter** コマンドを使用して、フィルタリングをイネーブルにします。
3. 必要に応じて **url-cache** コマンドを使用して、スループットを向上させます。ただし、このコマンドは Websense ログを更新しないため、Websense アカウンティング レポートに影響がある可能性があります。**url-cache** コマンドを使用する前に、Websense の実行ログを蓄積します。
4. **show url-cache statistics** コマンドおよび **show perfmon** コマンドを使用して、実行情報を表示します。

長い URL の使用

Websense フィルタリング サーバでは 4 KB まで、N2H2 フィルタリング サーバでは 3 KB までの URL のフィルタリングがサポートされています。

許可されている最大サイズよりも長い URL 要求の処理を許可するには、**longurl-truncate** オプションおよび **cgi-truncate** オプションを使用します。

URL が最大長よりも長く、**longurl-truncate** オプションまたは **longurl-deny** オプションをイネーブルにしない場合、ASA ではパケットがドロップされます。

longurl-truncate オプションを指定すると、ASA は URL が最大許容長よりも長い場合に、URL のホスト名または IP アドレス部分だけを、評価のためにフィルタリング サーバに送信します。**longurl-deny** オプションは、URL が最大許容長よりも長い場合、発信 URL トラフィックを拒否します。

パラメータは含まずに CGI スクリプトの場所とスクリプト名だけを含むよう CGI URL を切り捨てるには、**cgi-truncate** オプションを使用します。長い HTTP 要求のほとんどは、CGI 要求です。パラメータ リストが非常に長い場合、パラメータ リストを含む完全な CGI 要求を待機したり送信したりすると、大量のメモリ リソースが使用され、ASA のパフォーマンスに影響を与える可能性があります。

HTTP 応答のバッファリング

デフォルトで、ユーザが特定の Web サイトに対する接続要求を発行すると、ASA はその要求を Web サーバとフィルタリング サーバに同時に送信します。Web コンテンツ サーバよりも前にフィルタリング サーバが応答しない場合、Web サーバからの応答はドロップされます。このような場合、Web クライアントの観点からは、Web サーバの応答が遅延することになります。

HTTP 応答バッファをイネーブルにすることによって、Web コンテンツ サーバからの応答がバッファリングされ、フィルタリング サーバによって接続が許可された場合にその応答が要求元ユーザに転送されます。これにより、応答バッファをイネーブルにしない場合に発生する遅延を防止できます。

HTTP 応答バッファをイネーブルにするには、次のコマンドを入力します。

```
ciscoasa(config)# url-block block block-buffer-limit
```

block-buffer-limit 引数を、バッファリングする最大ブロック数で置き換えます。1 ～ 128 の値を指定できます。この値は、一度にバッファリング可能な 1550 バイトのブロック数を指定します。

例

次に、10.0.2.54 ホストからの接続を除く、すべての発信 HTTP 接続をフィルタリングする例を示します。

```
ciscoasa(config)# url-server (perimeter) host 10.0.1.1
ciscoasa(config)# filter url 80 0 0 0 0
ciscoasa(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

次に、ポート 8080 でリッスンするプロキシ サーバ宛てのすべての発信 HTTP 接続をブロックする例を示します。

```
ciscoasa(config)# filter url 8080 0 0 0 0 proxy-block
```

関連コマンド

コマンド	説明
filter activex	ASA を通過する HTTP トラフィックから ActiveX オブジェクトを削除します。
filter java	ASA を通過する HTTP トラフィックから Java アプレットを削除します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

fips enable

FIPS 準拠を強制するためのポリシー チェックをイネーブルにするには、グローバル コンフィギュレーション モードで **fips enable** コマンドを使用します。ポリシー チェックをディセーブルにするには、このコマンドの **no** 形式を使用します。

fips enable

no fips enable

構文の説明

enable	FIPS 準拠を強制するためのポリシー チェックをイネーブルまたはディセーブルにします。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• x	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.8(2)	FIPS モードを有効にするには、設定の保存とリロードが必要になりました。また、フェールオーバー ペアの両方のユニットは、同じ FIPS 設定が必要です。

使用上のガイドライン

FIPS 準拠動作モードで実行するには、**fips enable** コマンドを適用し、セキュリティ ポリシーに指定されている正しいコンフィギュレーションを適用する必要があります。内部 API によって、実行時に正しいコンフィギュレーションが適用されるようにデバイスを移行できます。

スタートアップ コンフィギュレーションに FIPS 準拠モードが存在する場合、FIPS POST が実行され、次のコンソール メッセージが出力されます。

```
Copyright (c) 1996-2005 by Cisco Systems, Inc.
Restricted Rights Legend
```

```
Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR
sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

               Cisco Systems, Inc.
               170 West Tasman Drive
               San Jose, California 95134-1706

....
Cryptochecksum (unchanged): 6c6d2f77 ef13898e 682c9f94 9c2d5ba9

INFO: FIPS Power-On Self-Test in process.  Estimated completion in 90 seconds.
.................................................
INFO: FIPS Power-On Self-Test complete.
Type help or '?' for a list of available commands.
sw8-5520>
```

(注) FIPS モードは、クラスタリングモードではサポートされていません。

(注) すべてのインターフェイスがポートチャネルのメンバーとして設定されている場合、FIPS セルフテストは起動時に失敗します。FIPS セルフテストが起動時に成功するには、少なくとも 1 つのインターフェイスを有効にして、ポートチャネルのメンバーとしては設定しないようにする必要があります。

例

次に、システムで FIPS 準拠を強制するためのポリシー チェックを示します。

```
ciscoasa(config)# fips enable
WARNING: FIPS mode change will not take effect until you save configuration and reboot the
device
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に保存されているシステムまたはモジュールの FIPS コンフィギュレーション情報をクリアします。
crashinfo console disable	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、およびコンフィギュレーションをディセーブルにします。
fips self-test poweron	電源投入時自己診断テストを実行します。
show crashinfo console	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行います。
show running-config fips	ASA で実行されている FIPS コンフィギュレーションを表示します。
show fips	FIPS の現在の動作状態を ASA に表示します。

fips self-test poweron

電源投入時自己診断テストを実行するには、特権 EXEC モードで **fips self-test powereon** コマンドを使用します。

fips self-test poweron

構文の説明

poweron	電源投入時自己診断テストを実行します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

このコマンドを入力すると、デバイスで FIPS 140-2 準拠に必要なすべてのセルフテストが実行されます。テストには、暗号化アルゴリズム テスト、ソフトウェア完全性テスト、および重要機能のテストがあります。

例

次に、システムで電源投入時自己診断テストを実行する例を示します。

```
ciscoasa(config)# fips self-test poweron
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に保存されているシステムまたはモジュールの FIPS コンフィギュレーション情報をクリアします。
crashinfo console disable	フラッシュに対するクラッシュ書き込み情報の読み取り、書き込み、およびコンフィギュレーションをディセーブルにします。
fips enable	システムまたはモジュールで FIPS 準拠を強制するためのポリシー チェックをイネーブルまたはディセーブルにします。

コマンド	説明
show crashinfo console	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行います。
show running-config fips	ASA で実行されている FIPS コンフィギュレーションを表示します。

firewall transparent

ファイアウォール モードをトランスペアレント モードに設定するには、グローバル コンフィギュレーション モードで **firewall transparent** コマンドを使用します。ルーテッド モードに戻すには、このコマンドの **no** 形式を使用します。

firewall transparent

no firewall transparent

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、ASA はルーテッド モードです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.5(1)/9.0(1)	マルチ コンテキスト モードでは、コンテキストごとにこれを設定できます。

使用上のガイドライン

トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように動作するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。

マルチ コンテキスト モードでは、コンテキストごとにこのコマンドを設定できます。

多くのコマンドは両方のモードではサポートされていないため、モードを変更した場合は、ASA によってコンフィギュレーションがクリアされます。設定済みのコンフィギュレーションがある場合は、モードを変更する前にコンフィギュレーションをバックアップしてください。新しいコンフィギュレーション作成時の参照としてこのバックアップを使用できます。

firewall transparent コマンドを使用してモードを変更するテキスト コンフィギュレーションを ASA にダウンロードする場合は、このコマンドをコンフィギュレーションの先頭に配置します。先頭に配置することによって、ASA でこのコマンドが読み込まれるとすぐにモードが変更され、その後引き続きダウンロードされたコンフィギュレーションが読み込まれます。コマンドをコンフィギュレーションの後の方に配置すると、コンフィギュレーション内のその位置よりも前にあるすべての行が ASA によってクリアされます。

例

次に、ファイアウォール モードをトランスペアレントに変更する例を示します。

```
ciscoasa(config)# firewall transparent
```

関連コマンド

コマンド	説明
arp-inspection	ARP パケットとスタティック ARP エントリを比較する ARP インスペクションをイネーブルにします。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show firewall	ファイアウォール モードを表示します。
show mac-address-table	ダイナミック エントリおよびスタティック エントリを含む MAC アドレス テーブルを表示します。

flow-export active refresh-interval

flow-update イベント間の間隔を指定するには、グローバル コンフィギュレーション モードで **flow-export active refresh-interval** コマンドを使用します。

flow-export active refresh-interval *value*

構文の説明

value	flow-update イベント間の間隔を分単位で指定します。有効な値は 1 ～ 60 分です。

デフォルト

デフォルト値は 1 分です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.1(2)	このコマンドが追加されました。

使用上のガイドライン

flow-export delay flow-create コマンドを設定した後で、遅延値より 5 秒以上長くはない間隔値を使用して **flow-export active refresh-interval** コマンドを設定した場合、コンソールに次の警告メッセージが表示されます。

```
WARNING: The current delay flow-create value configuration may cause flow-update events to
appear before flow-creation events.
```

flow-export active refresh-interval コマンドを設定した後で、間隔値より 5 秒以上短くはない遅延値を使用して **flow-export delay flow-create** コマンドを設定した場合、コンソールに次の警告メッセージが表示されます。

```
WARNING: The current delay flow-create value configuration may cause flow-update events to
appear before flow-creation events.
```

例

次に、30 分の時間間隔を設定する例を示します。

```
ciscoasa(config)# flow-export active refresh-interval 30
```

関連コマンド

コマンド	説明
clear flow-export counters	NetFlow のランタイム カウンタをすべてゼロにリセットします。
flow-export destination	NetFlow コレクタの IP アドレスまたはホスト名と、NetFlow コレクタがリッスンする UDP ポートを指定します。
flow-export template timeout-rate	テンプレート情報が NetFlow コレクタに送信される間隔を制御します。
logging flow-export-syslogs enable	**logging flow-export-syslogs disable** コマンドを入力した後に、syslog メッセージをイネーブルにし、さらに NetFlow データに関連付けられた syslog メッセージをイネーブルにします。
show flow-export counters	NetFlow のランタイム カウンタのセットを表示します。

flow-export delay flow-create

フロー作成イベントのエクスポートを遅延するには、グローバル コンフィギュレーション モードで **flow-export delay flow-create** コマンドを使用します。遅延なしでフロー作成イベントをエクスポートするには、このコマンドの **no** 形式を使用します。

flow-export delay flow-create *seconds*

no flow-export delay flow-create *seconds*

構文の説明

seconds	フロー作成イベントのエクスポートを遅延する秒数を指定します。有効な値は、1 ～ 180 秒です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.1(2)	このコマンドが追加されました。

使用上のガイドライン

flow-export delay flow-create コマンドが設定されていない場合、フロー作成イベントは遅延なしでエクスポートされます。

設定されている遅延よりも前にフローが切断された場合は、flow-create イベントは送信されません。その代わりに拡張フロー ティアダウン イベントが送信されます。

例

次に、フロー作成イベントのエクスポートを 10 秒間遅延する例を示します。

```
ciscoasa(config)# flow-export delay flow-create 10
```

関連コマンド

コマンド	説明
clear flow-export counters	NetFlow のランタイム カウンタをすべてゼロにリセットします。
flow-export destination	NetFlow コレクタの IP アドレスまたはホスト名と、NetFlow コレクタがリッスンする UDP ポートを指定します。
flow-export template timeout-rate	テンプレート情報が NetFlow コレクタに送信される間隔を制御します。
logging flow-export-syslogs enable	**logging flow-export-syslogs disable** コマンドを入力した後に、syslog メッセージをイネーブルにし、さらに NetFlow データに関連付けられた syslog メッセージをイネーブルにします。
show flow-export counters	NetFlow のランタイム カウンタのセットを表示します。

flow-export destination

NetFlow パケットの送信先のコレクタを設定するには、グローバル コンフィギュレーション モードで **flow-export destination** コマンドを使用します。NetFlow パケットのコレクタを削除するには、このコマンドの **no** 形式を使用します。

flow-export destination *interface-name ipv4-address | hostname udp-port*

no flow-export destination *interface-name ipv4-address | hostname udp-port*

構文の説明

hostname	NetFlow コレクタのホスト名を指定します。
interface-name	宛先に到達可能なインターフェイス名を指定します。
ipv4-address	NetFlow コレクタの IP アドレスを指定します。IPv4 だけがサポートされます。
udp-port	NetFlow コレクタがリッスンしている UDP ポートを指定します。有効な値は、1 ～ 65535 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.1(1)	このコマンドが追加されました。
8.1(2)	フロー エクスポートの宛先の最大数が 5 に増やされました。

使用上のガイドライン

flow-export destination コマンドを使用すると、NetFlow コレクタに NetFlow データをエクスポートするように ASA を設定できます。

(注) セキュリティ コンテキストごとに最大で 5 つのエクスポートの宛先（コレクタ）を入力できます。新しい宛先を入力すると、新たに追加されたコレクタにテンプレート レコードが送信されます。6 つ以上の宛先の追加を試みると、次のエラー メッセージが表示されます。

「ERROR: A maximum of 5 flow-export destinations can be configured.」

ASA が NetFlow データをエクスポートするように設定されている場合、パフォーマンス向上のため、**logging flow-export-syslogs disable** コマンドを入力して（NetFlow でキャプチャされた）冗長な syslog メッセージをディセーブルにすることを推奨します。

例

次に、NetFlow データのコレクタを設定する例を示します。

```
ciscoasa(config)# flow-export destination inside 209.165.200.224 2055
```

関連コマンド

コマンド	説明
clear flow-export counters	NetFlow のランタイム カウンタをすべてゼロにリセットします。
flow-export delay flow-create	指定した時間だけ、フロー作成イベントのエクスポートを遅延します。
flow-export template timeout-rate	テンプレート情報が NetFlow コレクタに送信される間隔を制御します。
logging flow-export-syslogs enable	**logging flow-export-syslogs disable** コマンドを入力した後に、syslog メッセージをイネーブルにし、さらに NetFlow データに関連付けられた syslog メッセージをイネーブルにします。
show flow-export counters	NetFlow のランタイム カウンタのセットを表示します。

flow-export event-type destination

各コレクタにどの NetFlow レコードを送信するかを決定するために NetFlow コレクタおよびフィルタのアドレスを設定するには、ポリシー マップ クラス コンフィギュレーション モードで **flow-export event-type destination** コマンドを使用します。NetFlow コレクタおよびフィルタのアドレスを削除するには、このコマンドの **no** 形式を使用します。

flow-export event-type {**all** | **flow-create** | **flow-denied** | **flow-update** | **flow-teardown**} **destination**

no flow-export event-type {**all** | **flow-create** | **flow-denied** | **flow-update** | **flow-teardown**} **destination**

構文の説明

all	4 つのイベント タイプをすべて指定します。
flow-create	flow-create イベントを指定します。
flow-denied	flow-denied イベントを指定します。
flow-teardown	flow-teardown イベントを指定します。
flow-update	flow-update イベントを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ポリシー マップ クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.1(2)	このコマンドが追加されました。

使用上のガイドライン

NetFlow イベントは、Modular Policy Framework を使用して設定されます。Modular Policy Framework が NetFlow 用に設定されていない場合、イベントはログに記録されません。トラフィックはクラスが設定される順序に基づいて照合されます。一致が検出されると、その他のクラスはチェックされません。NetFlow イベントの場合、コンフィギュレーションの要件は次のとおりです。

- flow-export destination（NetFlow コレクタ）は、その IP アドレスによって一意に識別されます。
- サポートされるイベント タイプは、flow-create、flow-teardown、flow-denied、および all です（前述の 4 つのイベント タイプを含みます）。
- flow-export アクションは、インターフェイス ポリシーでサポートされません。
- flow-export アクションがサポートされるのは、**class-default** コマンド、および **match any** コマンドまたは **match access-list** コマンドで使用されるクラスに限られます。
- NetFlow コレクタが定義されていない場合は、コンフィギュレーション アクションは発生しません。
- NetFlow セキュア イベント ロギングのフィルタリングは、順序に関係なく実行されます。

（注） 有効な NetFlow コンフィギュレーションを作成するには、flow-export destination コンフィギュレーションと flow-export event-type コンフィギュレーションの両方が必要です。flow-export destination コンフィギュレーション単独では何も実行されません。また、flow-export event-type コンフィギュレーションのクラス マップも設定する必要があります。これは、デフォルト クラス マップにすることも、自分で作成したクラス マップにすることもできます。

例

次に、ホスト 10.1.1.1 と 20.1.1.1 の間のすべての NetFlow イベントを送信先 15.1.1.1 にエクスポートする例を示します。

```
ciscoasa(config)# access-list flow_export_acl permit ip host 10.1.1.1 host 20.1.1.1
ciscoasa(config)# class-map flow_export_class
ciscoasa(config-cmap)# match access-list flow_export_acl
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class flow_export_class
ciscoasa(config-pmap-c)# flow-export event-type all destination 15.1.1.1
```

関連コマンド

コマンド	説明
clear flow-export counters	NetFlow のランタイム カウンタをすべてゼロにリセットします。
flow-export delay flow-create	指定した時間だけ、フロー作成イベントのエクスポートを遅延します。
flow-export template timeout-rate	テンプレート情報が NetFlow コレクタに送信される間隔を制御します。
logging flow-export-syslogs enable	**logging flow-export-syslogs disable** コマンドを入力した後に、syslog メッセージをイネーブルにし、さらに NetFlow データに関連付けられた syslog メッセージをイネーブルにします。
show flow-export counters	NetFlow のランタイム カウンタのセットを表示します。

flow-export template timeout-rate

テンプレート情報が NetFlow コレクタに送信される間隔を制御するには、グローバル コンフィギュレーション モードで **flow-export template timeout-rate** コマンドを使用します。テンプレート タイムアウトをデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

flow-export template timeout-rate *minutes*

no flow-export template timeout-rate *minutes*

構文の説明

minutes	間隔を分単位で指定します。有効な値は、1 ～ 3600 分です。
template	テンプレートのエクスポートを設定するための **timeout-rate** キーワードをイネーブルにします。
timeout-rate	テンプレートを最初に送信してから再送信するまでの時間（間隔）を指定します。

デフォルト

間隔のデフォルト値は 30 分です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.1(1)	このコマンドが追加されました。

使用上のガイドライン

使用するコレクタ、およびコレクタにおいて必要となるテンプレート リフレッシュ頻度に基づいて、タイムアウト レートを設定する必要があります。

セキュリティ アプライアンスが NetFlow データをエクスポートするように設定されている場合、パフォーマンス向上のため、**logging flow-export-syslogs disable** コマンドを入力して（NetFlow でキャプチャされた）冗長な syslog メッセージをディセーブルにすることを推奨します。

例

次に、すべてのコレクタに対してテンプレート レコードを 60 分ごとに送信するように NetFlow を設定する例を示します。

```
ciscoasa(config)# flow-export template timeout-rate 60
```

関連コマンド

コマンド	説明
clear flow-export counters	NetFlow データに関連付けられているすべてのランタイム カウンタをリセットします。
flow-export destination	NetFlow コレクタの IP アドレスまたはホスト名と、NetFlow コレクタがリッスンする UDP ポートを指定します。
logging flow-export-syslogs enable	**logging flow-export-syslogs disable** コマンドを入力した後に、syslog メッセージをイネーブルにし、さらに NetFlow データに関連付けられた syslog メッセージをイネーブルにします。
show flow-export counters	NetFlow のランタイム カウンタのセットを表示します。

flow-offload enable

フローのオフロードをイネーブルにするには、グローバル コンフィギュレーション モードで **flow-offload enable** コマンドを使用します。オフロードをディセーブルにするには、このコマンドの **no** 形式を使用します。

flow-offload enable

no flow-offload enable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

フローのオフロードはデフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2.1)	このコマンドが導入されました。このコマンドは FXOS 1.1.3+ を実行している Firepower 9300 シリーズのみで使用できます。
9.6(1)	FXOS 1.1.4+ を実行している Firepower 4100 シリーズのサポートが追加されました。
9.6(2)	トランスペアレント モードのマルチキャスト接続のサポートが追加されました。ただし、ブリッジ グループに 2 つのインターフェイスだけが含まれる場合に限ります。

使用上のガイドライン

データセンターに FirePOWER アプライアンスと ASA セキュリティ モジュールを展開した場合、超高速パスにオフロードするトラフィックを識別して、フローが NIC 自身でスイッチングされるようにできます。オフロードを行うと、大容量ファイルの転送など、データ集約型アプリケーションのパフォーマンスを向上させることができます。

オフロードを行う前に、ASA は接続確立時に通常のセキュリティ処理（アクセス ルールやインスペクションなど）を適用します。ASA はまた、セッションの切断を行います。しかし、接続が確立され、フローがオフロード対象として識別されると、以降の処理は ASA ではなく NIC で発生します。

オフロード中、フローはセキュリティ ポリシー チェックなどのサービスを受け取らないため、システム全体を可能な限り高速に移動できます。オフロードされたフローに対しては、インスペクション、TCP 正規化（設定した場合はチェックサム検証を除く）、QoS、シーケンス番号チェックが行われません。

オフロードできるフローを識別するには、フロー オフロード サービスを適用するサービス ポリシー ルールを作成します。次の条件を満たす場合、一致したフローがオフロードされます。

- IPv4 アドレスのみ。
- TCP、UDP、GRE のみ。
- 標準または 802.1q タグ付きイーサネット フレームのみ。
- （トランスペアレント モードのみ。）インターフェイスを 2 つだけ含むブリッジ グループのマルチキャスト フロー。
- オフロードされるフローに適用できないサービス（インスペクション、復号化、IPSec および VPN フロー、サービス モジュールに送信されるフロー）を受け取らない。

オフロードされるフローのリバース フローもオフロードされます。

フローのオフロードをイネーブルまたはディセーブルにするたびに、システムをリロードする必要があります。

マルチコンテキスト モードでは、フロー オフロードを有効または無効にすると、すべてのコンテキストのフロー オフロードが有効または無効になります。コンテキストごとに異なる設定を使用することはできません。

クラスタまたはフェールオーバー ペアの場合、ヒットレスなモード変更を行うには、次の事項を考慮する必要があります。

- クラスタリング：最初にマスター ユニット上でコマンドを入力しますが、マスター ユニットをすぐにリブートしないでください。代わりに、クラスタの各メンバーを最初にリブートしてから、マスターに戻ってリブートします。その後、マスター ユニットでオフロード サービス ポリシーを設定できます。
- フェールオーバー：最初にアクティブ ユニット上でコマンドを入力しますが、アクティブ ユニットをすぐにリブートしないでください。代わりに、スタンバイ ユニットをリブートしてから、アクティブ ユニットをリブートします。次に、アクティブ ユニット上でオフロード サービス ポリシーを設定します。

（注） デバイス サポートの詳細については、http://www.cisco.com/c/en/us/td/docs/security/firepower/9300/compatibility/fxos-compatibility.html を参照してください。

例

次に、フローのオフロードをイネーブルにし、設定を保存してシステムをリブートする例を示します。

```
ciscoasa(config)# flow-offload enable

WARNING: This command will take effect after the running-config is
saved and the system has been rebooted.

ciscoasahostname(config)# write memory
ciscoasa(config)# reload
```

関連コマンド

コマンド	説明
set-connection advanced-options flow-offload	オフロードの対象としてトラフィック フローを指定します。
show flow-offload	オフロードするフローに関する情報を表示します。

flowcontrol

フロー制御用のポーズ（XOFF）フレームをイネーブルにするには、インターフェイス コンフィギュレーション モードで **flowcontrol** コマンドを使用します。ポーズ フレームをディセーブルにするには、このコマンドの **no** 形式を使用します。

flowcontrol send on [*low_water high_water pause_time*] [**noconfirm**]

no flowcontrol send on [*low_water high_water pause_time*] [**noconfirm**]

構文の説明

high_water	10 GigabitEthernet の最高水準点を 0 ～ 511 KB の範囲で設定し、1 GigabitEthernet の最高水準点を 0 ～ 47 KB の範囲で（4GE-SSM では GigabitEthernet の最高水準点を 0 ～ 11 KB の範囲で）設定します。バッファの使用量が高基準値を超えると、NIC からポーズ フレームが送信されます。
low_water	10 GigabitEthernet の最低水準点を 0 ～ 511 KB の範囲で設定し、1 GigabitEthernet の最低水準点を 0 ～ 47 KB の範囲で（4GE-SSM では GigabitEthernet の最低水準点を 0 ～ 11 KB の範囲で）設定します。Network Interface Controller（NIC; ネットワーク インターフェイス コントローラ）からポーズ フレームが送信された後、バッファの使用量が低基準値を下回ると、NIC から XON フレームが送信されます。リンク パートナーは、XON フレームを受信するとトラフィックを再開できます。
noconfirm	確認なしでコマンドを適用します。このコマンドでは、インターフェイスがリセットされるため、このオプションを指定しない場合は、コンフィギュレーションの変更の確認を求められます。
pause_time	ポーズ リフレッシュのしきい値を 0 ～ 65535 スロットの範囲で設定します。各スロットは 64 バイトを転送するために必要な時間なので、ユニットあたりの時間はリンク速度によって異なります。リンク パートナーは、XON を受信した後、または XOFF の期限が切れた後、トラフィックを再開できます。XOFF の期限は、ポーズ フレーム内のこのタイマー値によって制御されます。バッファの使用量が継続的に最高水準点を超えている場合は、ポーズ リフレッシュのしきい値に指定された間隔でポーズ フレームが繰り返し送信されます。デフォルトは 26624 です。

コマンド デフォルト

ポーズ フレームは、デフォルトではディセーブルになっています。

10 GigabitEthernet の場合は、次のデフォルト設定を参照してください。

- デフォルトの最高水準点は 128 KB です。
- デフォルトの最低水準点は 64 KB です。
- デフォルトのポーズ リフレッシュのしきい値は 26624 スロットです。

1 GigabitEthernet の場合は、次のデフォルト設定を参照してください。

- デフォルトの最高水準点は 24 KB です。
- デフォルトの最低水準点は 16 KB です。
- デフォルトのポーズ リフレッシュのしきい値は 26624 スロットです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.2(2)	ASA 5580 上の 10-GigabitEthernet インターフェイスに対して、このコマンドが追加されました。
8.2(3)	ASA 5585-X のサポートが追加されました。
8.2(5)/8.4(2)	すべてのモードで 1-GigabitEthernet インターフェイスのサポートが追加されました。

使用上のガイドライン

このコマンドは、1-GigabitEthernet および 10-Gigabit Ethernet インターフェイスでサポートされています。このコマンドでは、管理インターフェイスをサポートしていません。

このコマンドは、物理インターフェイスに対して入力します。

トラフィック バーストが発生している場合、バーストが NIC の FIFO バッファまたは受信リング バッファのバッファリング容量を超えると、パケットがドロップされる可能性があります。フロー制御用のポーズ フレームをイネーブルにすると、このような問題の発生を抑制できます。

このコマンドをイネーブルにすると、FIFO バッファの使用量に基づいて、NIC ハードウェアによってポーズ(XOFF)フレームおよび XON フレームが自動的に生成されます。

1. バッファの使用量が最高水準点を超えると、NIC からポーズ フレームが送信されます。
2. ポーズが送信された後、バッファの使用量が最低水準点を下回ると、NIC から XON フレームが送信されます。
3. リンク パートナーは、XON を受信した後、または XOFF の期限が切れた後、トラフィックを再開できます。XOFF の期限は、ポーズ フレーム内のタイマー値によって制御されます。
4. バッファの使用量が継続的に最高水準点を超えている場合は、ポーズ リフレッシュのしきい値に指定された間隔でポーズ フレームが繰り返し送信されます。

このコマンドを使用すると、次の警告メッセージが表示されます。

```
Changing flow-control parameters will reset the interface. Packets may be lost during the
reset.
Proceed with flow-control changes?
```

プロンプトを表示しないでパラメータを変更するには、**noconfirm** キーワードを使用します。

(注) 802.3x に定義されているフロー制御フレームのみがサポートされています。プライオリティベースのフロー制御はサポートされていません。

例

次に、デフォルト設定を使用してポーズ フレームをイネーブルにする例を示します。

```
ciscoasa(config)# interface tengigabitethernet 1/0
ciscoasa(config-if)# flowcontrol send on
Changing flow-control parameters will reset the interface. Packets may be lost during the
reset.
Proceed with flow-control changes?
ciscoasa(config-if)# y
```

関連コマンド

コマンド	説明
interface	インターフェイス コンフィギュレーション モードを開始します。

flow-mobility lisp

クラスタのフロー モビリティをイネーブルにするには、クラス コンフィギュレーション モードで **flow-mobility lisp** コマンドを使用します。フロー モビリティをディセーブルにするには、このコマンドの **no** 形式を使用します。

flow-mobility lisp

no flow-mobility lisp

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラスタ構成	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

このオン/オフ トグルを使用すると、特定のクラスのトラフィックまたはアプリケーションに対してフロー モビリティを簡単にイネーブルまたはディセーブルにできます。

クラスタ フロー モビリティの LISP インスペクションについて

ASA は、場所の変更について LISP トラフィックを検査し、シームレスなクラスタリング操作のためにこの情報を使用します。LISP の統合により、ASA クラスタ メンバーは、最初のホップ ルータと ETR または ITR との間で渡される LISP トラフィックを検査し、その後、フローの所有者を新しいサイトへ変更できます。

クラスタ フロー モビリティには複数の相互に関連する設定が含まれています。

1. （オプション）ホストまたはサーバの IP アドレスに基づく検査される EID の限定：最初のホップ ルータは、ASA クラスタが関与していないホストまたはネットワークに関する EID 通知メッセージを送信することがあるため、EID をクラスタに関連するサーバまたはネットワークのみに限定することができます。たとえば、クラスタが 2 つのサイトのみに関連しているが、LISP は 3 つのサイトで稼働している場合は、クラスタに関連する 2 つのサイトの EID のみを含めます。**policy-map type inspect lisp**、**allowed-eid** および **validate-key** コマンドを参照してください。
2. LISP トラフィックのインスペクション：ASA は、最初のホップ ルータと ITR または ETR 間で送信された EID 通知メッセージに関して LISP トラフィックを検査します。ASA は EID とサイト ID を相関付ける EID テーブルを維持します。たとえば、最初のホップ ルータの送信元 IP アドレスと ITR または ETR の宛先アドレスをもつ LISP トラフィックを検査する必要があります。**inspect lisp** コマンドを参照してください。
3. 指定されたトラフィックでのフロー モビリティを有効にするサービス ポリシー：ビジネスクリティカルなトラフィックでフロー モビリティを有効にする必要があります。たとえば、フロー モビリティを、HTTPS トラフィックのみに制限したり、特定のサーバとの間でやり取りされるトラフィックのみに制限したりできます。**cluster flow-mobility lisp** コマンドを参照してください。
4. サイト ID：ASA は各クラスタ ユニットのサイト ID を使用して、新しい所有者を判別します。**site-id** コマンドを参照してください。
5. フロー モビリティを有効にするクラスタレベルの設定：クラスタ レベルでもフロー モビリティを有効にする必要があります。このオン/オフの切り替えを使用することで、特定のクラスのトラフィックまたはアプリケーションに対してフロー モビリティを簡単に有効または無効にできます。**flow-mobility lisp** コマンドを参照してください。

例

次に、cluster1 のフロー モビリティをイネーブルにする例を示します。

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# flow-mobility lisp
```

関連コマンド

コマンド	説明
allowed-eids	IP アドレスに基づいて検査される EID を限定します。
clear cluster info flow-mobility counters	フロー モビリティ カウンタをクリアします。
clear lisp eid	ASA EID テーブルから EID を削除します。
cluster flow-mobility lisp	サービス ポリシーのフロー モビリティを有効にします。
inspect lisp	LISP トラフィックを検査します。
policy-map type inspect lisp	LISP 検査をカスタマイズします。
site-id	クラスタ シャーシのサイト ID を設定します。
show asp table classify domain inspect-lisp	LISP 検査用の ASP テーブルを表示します。
show cluster info flow-mobility counters	フロー モビリティ カウンタを表示します。

コマンド	説明
show conn	LISP フロー モビリティの対象となるトラフィックを表示します。
show lisp eid	ASA EID テーブルを表示します。
show service-policy	サービス ポリシーを表示します。
validate-key	LISP メッセージを検証するための事前共有キーを入力します。

format

すべてのファイルを消去してファイル システムをフォーマットするには、特権 EXEC モードで **format** コマンドを使用します。

format {**disk0:** | **disk1:** | **flash:**}

構文の説明

disk0*:*	内部フラッシュ メモリを指定し、続けてコロンを入力します。
disk1:	外部フラッシュ メモリ カードを指定し、続けてコロンを入力します。
flash:	内部フラッシュ メモリを指定し、続けてコロンを入力します。ASA 5500 シリーズでは、**flash** キーワードは **disk0** のエイリアスです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

format コマンドは、指定したファイル システム上のすべてのデータを消去して、デバイスに FAT 情報を再書き込みします。

注意 **format** コマンドを使用するのは、必要な場合に、破損したフラッシュ メモリをクリーンアップするためにのみ、慎重に使用してください。

（非表示のシステム ファイルを除く）表示されているすべてのファイルを削除する場合は、**format** コマンドではなく **delete /recursive** コマンドを入力します。

（注） Cisco ASA 5500 シリーズでは、**erase** コマンドを実行すると、ディスク上のすべてのユーザ データが 0xFF パターンを使用して破棄されます。一方、**format** コマンドはファイル システムの制御構造をリセットするだけです。ロウ ディスク読み取りツールを使用すると、この情報はまだ参照できる可能性があります。

破損したファイル システムを修復する場合は、**format** コマンドを入力する前に **fsck** を入力します。

例

次に、フラッシュ メモリをフォーマットする例を示します。

```
ciscoasa# format flash:
```

関連コマンド

コマンド	説明
delete	ユーザに表示されるすべてのファイルを削除します。
erase	すべてのファイルを削除し、フラッシュ メモリをフォーマットします。
fsck	破損したファイル システムを修復します。

forward interface

ASA 5505 など、組み込みスイッチを搭載したモデルの場合、特定の VLAN で他の特定の VLAN への接続の開始を可能にするには、インターフェイス コンフィギュレーション モードで **forward interface** コマンドを使用します。特定の VLAN で他の特定の VLAN への接続が開始されないよう制限するには、このコマンドの **no** 形式を使用します。

forward interface vlan *number*

no forward interface vlan *number*

(注) Firepower 1010 および ASA 5505 でのみサポートされています。

構文の説明

vlan *number*	この VLAN インターフェイスでトラフィックの開始を禁止する先の VLAN ID を指定します。

デフォルト

デフォルトでは、すべてのインターフェイスから他のすべてのインターフェイスにトラフィックを開始できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.13(1)	Firepower 1010 のサポートが追加されました。

使用上のガイドライン

ライセンスでサポートされている VLAN 数に応じて、特定の VLAN の制限が必要となることがあります。

ルーテッド モードでは、ASA 5505 の基本ライセンスで最大 3 つのアクティブ VLAN と Security Plus ライセンスで最大 5 つのアクティブ VLAN を設定できます。アクティブな VLAN とは、**nameif** コマンドが設定された VLAN のことです。いずれのライセンスでも、ASA 5505 では最大 5 つの非アクティブな VLAN を設定できますが、これらをアクティブにする場合は、ライセンスのガイドラインに従う必要があります。

基本ライセンスでは、3 つめの VLAN は **no forward interface** コマンドを使用して設定し、この VLAN から他の特定の VLAN への接続の開始を制限する必要があります。

たとえば、1 つめの VLAN がインターネット アクセス用の外部ネットワークに、2 つめの VLAN が内部の業務用ネットワークに、3 つめの VLAN が家庭用ネットワークにそれぞれ割り当てられているとします。家庭用ネットワークから業務用ネットワークにアクセスする必要はないため、家庭用 VLAN に対して **no forward interface** コマンドを使用できます。業務用ネットワークから家庭用ネットワークにはアクセスできますが、家庭用ネットワークから業務用ネットワークにはアクセスできません。

すでに 2 つの VLAN インターフェイスを **nameif** コマンドで設定している場合は、3 つ目のインターフェイスに対して **nameif** コマンドを使用する前に **no forward interface** コマンドを入力してください。ASA では、ASA 5505 の基本ライセンスで 3 つのフル機能 VLAN インターフェイスを持つことは許可されていません。

例

次の例では、3 つの VLAN インターフェイスを設定します。3 つめの家庭用インターフェイスは、業務用インターフェイスにトラフィックを転送できません。

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address dhcp
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 200
ciscoasa(config-if)# nameif work
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface vlan 300
ciscoasa(config-if)# no forward interface vlan 200
ciscoasa(config-if)# nameif home
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown

ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown

...
```

関連コマンド

コマンド	説明
backup interface	たとえば、ISP へのバックアップ リンクとしてインターフェイスを割り当てます。
clear interface	**show interface** コマンドのカウンタをクリアします。
interface vlan	VLAN インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。
switchport	インターフェイスをスイッチポートモードに設定します。
switchport access vlan	スイッチ ポートを VLAN に割り当てます。

forward-reference

まだ存在しない ACL およびオブジェクトを参照できるようにするには、グローバル コンフィギュレーション モードで **forward-reference** コマンドを使用します。

forward-reference enable

no forward-reference enable

構文の説明

enable	（アクセス グループ内の）ACL の前方参照と（オブジェクトおよび ACL 内の）オブジェクトの前方参照をイネーブルにします。

デフォルト

デフォルトでは、前方参照はディセーブルになっています。アクセス リスト ルール、別のオブジェクト、またはアクセス グループ内で ACL またはオブジェクトを参照するためには、その ACL またはオブジェクトが存在している必要があります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、ACL およびそのオブジェクトを編集するための隔離されたセッションを作成する **configure session** コマンドと組み合わせて使用すると最も役立ちます。たとえば、セッション内で、**access-group** コマンドによって現在参照されている ACL を削除して、同じ名前の新しい ACL を作成できます。セッションをコミットすると、ACL の新しいバージョンがコンパイルされて、コンパイル後にアクセス グループのアクティブ バージョンとなります。

同様に、アクティブなアクセス ルールで使用されているオブジェクトを削除して再作成することもできます。

前方参照は、アクセス ルール ACL で使用できるように設計されています。他の機能（NAT や VPN など）で現在使用されているオブジェクトは削除できません。

前方参照をイネーブルにする際は、慎重に行ってください。デフォルトの動作では、オブジェクト、アクセス リスト、およびアクセス グループの設定時に単純な入力ミスを回避できます。前方参照では、ASA は、入力ミスと、将来作成する何かに対する意図的な参照を区別することはできません。

存在しないオブジェクトまたは ACL を指すルール、アクセス グループ、またはオブジェクトは、処理中に無視されます。欠落している項目を作成するまでは、処理できません。

例

次に、前方参照をイネーブルにする例を示します。

```
ciscoasa(config)# forward-reference enable
```

関連コマンド

コマンド	説明
access-group	ACL をインターフェイスに、またはグローバルに割り当てます。
access-list	ACL ルールを作成します。
configure session	セッションを作成するか、開きます。
object	オブジェクトを作成します。
object-group	オブジェクト グループを作成します。

fqdn（クリプト CA トラストポイント）

登録時に、指定した FQDN を証明書のサブジェクト代替名の拡張に含めるには、クリプト CA トラストポイント コンフィギュレーション モードで **fqdn** コマンドを使用します。FQDN のデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

fqdn [*fqdn* | **none**]

no fqdn

構文の説明

fqdn	FQDN を指定します。最大長は、64 文字です。
none	完全修飾ドメイン名を指定しません。

デフォルト

デフォルトの設定には、FQDN は含まれていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

証明書を使用した Nokia VPN クライアントの認証をサポートするように ASA を設定する場合は、**none** キーワードを使用します。Nokia VPN クライアントの証明書認証のサポートの詳細については、**crypto isakmp identity** コマンドまたは **isakmp identity** コマンドを参照してください。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central の登録要求に FQDN engineering を含める例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)# fqdn engineering
ciscoasa(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	クリプト CA トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。
enrollment retry count	登録要求の送信を再試行する回数を指定します。
enrollment retry period	登録要求の送信を試行するまでの待機時間を分単位で指定します。
enrollment terminal	このトラストポイントを使用したカット アンド ペースト登録を指定します。

fqdn（ネットワーク オブジェクト）

ネットワーク オブジェクトの FQDN を設定するには、オブジェクト コンフィギュレーション モードで **fqdn** コマンドを使用します。このオブジェクトをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

fqdn [**v4** | **v6**] *fqdn*

no fqdn [**v4** | **v6**] *fqdn*

構文の説明

fqdn	ホスト名とドメインを含む FQDN を指定します。FQDN は、数字または文字で始まって終わる必要があります。内部文字として使用できるのは、文字、数字、およびハイフンだけです。ラベルは（www.cisco.com のように）ドットで区切ります。
v4	（オプション）IPv4 ドメイン名を指定します。
v6	（任意）IPv6 ドメイン名を指定します。

デフォルト

デフォルトでは、ドメイン名は IPv4 ドメインです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
オブジェクト ネットワーク コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

別の値を使用して既存のネットワーク オブジェクトを設定すると、新しいコンフィギュレーションが既存のコンフィギュレーションを置き換えます。

例

次に、ネットワーク オブジェクトを作成する例を示します。

```
ciscoasa (config)# object network FQDN_1
ciscoasa (config-network-object)# fqdn example.cisco.com
```

関連コマンド

コマンド	説明
clear configure object	作成されたすべてのオブジェクトをクリアします。
description	ネットワーク オブジェクトに説明を追加します。
fqdn	完全修飾ドメイン名のネットワーク オブジェクトを指定します。
host	ホスト ネットワーク オブジェクトを指定します。
nat	ネットワーク オブジェクトの NAT をイネーブルにします。
object network	ネットワーク オブジェクトを作成します。
object-group network	ネットワーク オブジェクト グループを作成します。
range	ネットワーク オブジェクトのアドレス範囲を指定します。
show running-config object network	ネットワーク オブジェクト コンフィギュレーションを表示します。
subnet	サブネット ネットワーク オブジェクトを指定します。

fragment

パケット フラグメンテーションの付加的な管理を提供して、NFS との互換性を向上させるには、グローバル コンフィギュレーション モードで **fragment** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

fragment reassembly {**full** | **virtual**} {**size** | **chain** | **timeout** *limit*} [*interface*]

no fragment reassembly {**full** | **virtual**} {**size** | **chain** | **timeout** *limit*} [*interface*]

構文の説明

chain *limit*	完全な IP パケットをフラグメント化できる最大フラグメント数を指定します。
interface	（任意）ASA のインターフェイスを指定します。interface が指定されていない場合、このコマンドはすべてのインターフェイスに適用されます。
reassembly full | **virtual**	ASA 経由でルーティングされた IP フラグメントに対して完全再構成または仮想再構成を指定します。ASA で終端する IP フラグメントは、常に完全に再構成されます。
size *limit*	IP 再構築データベース内で再構築を待機可能な最大フラグメント数を設定します。 （注） ASA では、キューのサイズが 2/3 までいっぱいになると、既存のファブリック チェーンの一部ではないすべてのフラグメントが受け入れられなくなります。キューの残りの 1/3 は、すでに部分的にキューイングされている不完全なフラグメント チェーンと送信元 IP アドレス、宛先 IP アドレス、および IP ID 番号が同じであるフラグメントを受け入れるために使用されます。この制限は、フラグメント フラッディング攻撃が行われた場合でも、正規のフラグメント チェーンの再構築を可能にするための DoS 保護メカニズムです。
timeout *limit*	フラグメント化されたパケット全体が到着するまで待機する最大秒数を指定します。タイマーは、パケットの最初のフラグメントが到着したあとに開始します。指定した秒数までに到着しなかったパケット フラグメントがある場合、到着済みのすべてのパケット フラグメントが廃棄されます。

デフォルト

デフォルトの設定は次のとおりです。

- **chain** は 24 パケットです。
- *interface* はすべてのインターフェイスです。
- **size** は 200 です。
- **timeout** は 5 秒です。
- 仮想再構成がイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが変更され、**chain**、**size**、または **timeout** のいずれかのキーワードを選択することが必要になりました。ソフトウェアの以前のリリースでは、これらのキーワードのいずれかを入力しなくても **fragment** コマンドを入力できましたが、これらのキーワードなしでは入力できなくなりました。
8.0(4)	**reassembly full** | **virtual** オプションが追加されました。

使用上のガイドライン

デフォルトで、ASA では、完全な IP パケットを再構築するために最大で 24 のフラグメントを受け入れます。ネットワーク セキュリティ ポリシーに基づいて、各インターフェイスで **fragment chain 1** *interface* コマンドを入力して、フラグメント化されたパケットが ASA を通過しないように ASA を設定することを検討する必要があります。limit を 1 に設定すると、すべてのパケットは完全なものである必要があります。つまり、フラグメント化されていない必要があります。

ASA を通過するネットワーク トラフィックの多くが NFS である場合は、データベースのオーバーフローを回避するために追加の調整が必要となることがあります。

WAN インターフェイスなど、NFS サーバとクライアントとの間の MTU サイズが小さい環境では、**chain** キーワードに追加の調整が必要となる場合があります。この場合、効率性を向上させるために、NFS over TCP を使用することを推奨します。

size *limit* を大きな値に設定すると、ASA がフラグメント フラッディングによる DoS 攻撃を受けやすくなります。**size** *limit* の値は、1550 または 16384 プールの合計ブロック数以上には設定しないでください。

デフォルト値を使用すると、フラグメント フラッディングによる DoS 攻撃が抑制されます。

次のプロセスは、**reassembly** オプションの設定に関係なく実行されます。

- IP フラグメントは、フラグメント セットが作成されるまで、またはタイムアウト間隔が経過するまで収集されます（**timeout** オプションを参照）。
- フラグメント セットが作成されると、セットに対して整合性チェックが実行されます。これらのチェックには、重複、テール オーバーフロー、チェーン オーバーフローはいずれも含まれません（**chain** オプションを参照）。

fragment reassembly virtual コマンドを設定した場合、フラグメント セットはさらなる処理のためにトランスポート層に転送されます。

fragment reassembly full コマンドを設定した場合、フラグメント セットはまず単一の IP パケットに結合されます。この単一の IP パケットは、さらなる処理のためにトランスポート層に転送されます。

例

次に、外部インターフェイスおよび内部インターフェイスにおいてフラグメント化されたパケットの通過を禁止する例を示します。

```
ciscoasa(config)# fragment chain 1 outside
ciscoasa(config)# fragment chain 1 inside
```

引き続き、フラグメント化されたパケットの通過を禁止する追加の各インターフェイスに対して、**fragment chain 1** *interface* コマンドを入力します。

次に、外部インターフェイスのフラグメント データベースを、最大サイズ 2000、最大チェーン長 45、待機時間 10 秒に設定する例を示します。

```
ciscoasa(config)# fragment size 2000 outside
ciscoasa(config)# fragment chain 45 outside
ciscoasa(config)# fragment timeout 10 outside
```

次に、**reassembly virtual** オプションを含む **show fragment** コマンドの出力例を示します。

```
ciscoasa(config)# show fragment
Interface: outside
    Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: inside
    Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
```

関連コマンド

コマンド	説明
clear configure fragment	すべての IP フラグメント再構成コンフィギュレーションを、デフォルトにリセットします。
clear fragment	IP フラグメント再構成モジュールの動作データをクリアします。
show fragment	IP フラグメント再構成モジュールの動作データを表示します。
show running-config fragment	IP フラグメント再構成コンフィギュレーションを表示します。

frequency

選択した SLA 動作の反復間隔を設定するには、SLA モニタ プロトコル コンフィギュレーション モードで **frequency** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

frequency *seconds*

no frequency

構文の説明

seconds	SLA プローブ間の秒数。有効な値は、1 ～ 604800 秒です。この値は、**timeout** の値未満にはできません。

デフォルト

デフォルトの頻度は、60 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
SLA モニタ プロトコル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

SLA 動作は、動作のライフタイム中、指定された頻度で繰り返し実行されます。次に例を示します。

- 60 秒の頻度に設定された **ipIcmpEcho** 動作は、動作のライフタイム中 60 秒ごとにエコー要求パケットを繰り返し送信します。
- エコー動作のデフォルトのパケット数は 1 です。動作が開始されるとこのパケットが送信され、60 秒後に再度送信されます。

個別の SLA 動作において、指定された頻度の値よりも実行に時間がかかる場合は、動作がすぐに繰り返されるのではなく、「busy」という統計情報カウンタが増加します。

frequency コマンドには、**timeout** コマンドに指定された値未満の値は指定できません。

例

次の例では、ID が 123 の SLA 動作を設定し、ID が 1 のトラッキング エントリを作成して、SLA の到達可能性を追跡しています。SLA 動作の頻度が 3 秒に、タイムアウト値が 1000 ミリ秒に設定されています。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
sla monitor	SLA モニタリング動作を定義します。
timeout	SLA 動作が応答を待機する期間を定義します。

fsck

ファイル システムのチェックを実行して、破損を修復するには、特権 EXEC モードで **fsck** コマンドを使用します。

fsck [**/noconfirm**] {**disk0:** | **disk1:** | **flash:**}

構文の説明

/noconfirm	（任意）修復時に確認を求めません。
disk0:	内部フラッシュ メモリを指定し、続けてコロンを入力します。
disk1:	外部フラッシュ メモリ カードを指定し、続けてコロンを入力します。
flash:	内部フラッシュ メモリを指定し、続けてコロンを入力します。**flash** キーワードは、**disk0:** のエイリアスです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

fsck コマンドは、ファイル システムに破損がないかどうかをチェックし、破損があった場合には修復を試みます。より恒久的な手順を試みる前に、このコマンドを使用します。

FSCK ユーティリティで（電源障害や異常なシャットダウンなどによる）ディスクの破損箇所が修復されると、FSCK*xxx*.REC という名前のリカバリ ファイルが作成されます。これらのファイルには、FSCK 実行時に回復されたファイルの一部またはファイル全体が含まれています。まれに、データを回復するためにこれらのファイルを調べる必要がある場合があります。通常、これらのファイルは必要なく、安全に削除できます。

（注） FSCK ユーティリティは起動時に自動的に実行されるため、手動で **fsck** コマンドを入力していない場合でもこれらのリカバリ ファイルが存在する場合があります。

例

次に、フラッシュ メモリのファイル システムをチェックする例を示します。

```
ciscoasa# fsck disk0:
```

関連コマンド

コマンド	説明
delete	ユーザに表示されるすべてのファイルを削除します。
erase	すべてのファイルを削除し、フラッシュ メモリをフォーマットします。
形式	非表示のシステム ファイルを含むファイル システム上のすべてのファイルを消去して、ファイル システムを再インストールします。

ftp mode passive

FTP モードをパッシブに設定するには、グローバル コンフィギュレーション モードで **ftp mode passive** コマンドを使用します。FTP クライアントをアクティブ モードに設定するには、このコマンドの **no** 形式を使用します。

ftp mode passive

no ftp mode passive

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ftp mode passive コマンドは、FTP モードをデフォルトであるパッシブに設定します。ASA では、FTP サーバとの間で、イメージ ファイルやコンフィギュレーション ファイルのアップロードおよびダウンロードを実行できます。**ftp mode passive** コマンドは、ASA 上の FTP クライアントの FTP サーバとの通信方法を制御します。

パッシブ FTP では、クライアントは制御接続およびデータ接続の両方を開始します。パッシブ モードとはサーバの状態を指しており、クライアントが開始する制御接続およびデータ接続の両方をサーバが受動的に受け入れることを意味しています。

パッシブ モードでは、送信元ポートおよび宛先ポートの両方が 1023 よりも大きい一時ポートです。モードはクライアントによって設定されます。クライアントは、**passive** コマンドを発行して、パッシブ データ接続の設定を開始します。パッシブ モードではデータ接続の受け入れ側となるサーバは、今回の特定の接続においてリッスンするポート番号を応答として返します。

例

次に、パッシブ モードを無効にする例を示します。

```
ciscoasa(config)# no ftp mode passive
```

関連コマンド

copy	イメージ ファイルやコンフィギュレーション ファイルを FTP サーバとの間でアップロードまたはダウンロードします。
debug ftp client	FTP クライアントのアクティビティに関する詳細な情報を表示します。
show running-config ftp mode	FTP クライアントのコンフィギュレーションを表示します。

functions（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 8.0(1) でした。

functions コマンドは、リリース 8.0(2) では使用できません。このコマンドは廃止されており、下位互換性の目的でのみこのコマンド リファレンスに記載されています。Web サイトの URL リストの作成、ファイル アクセス、プラグイン、カスタマイゼーション、言語変換には、**import** コマンドおよび **export** コマンドを使用します。

特定のユーザまたはグループ ポリシーに対して、ポート フォワーディング Java アプレットの自動ダウンロード、ファイル アクセス、ファイル ブラウジング、ファイル サーバ名の入力、Web タイプ ACL の適用、HTTP プロキシ、ポート フォワーディング、または WebVPN 上での URL 入力を設定するには、webvpn コンフィギュレーション モードで **functions** コマンドを入力します。設定済みの機能を削除するには、このコマンドの **no** 形式を使用します。

functions {**auto-download** | **citrix** | **file-access** | **file-browsing** | **file-entry** | **filter** | **http-proxy** | **url-entry** | **port-forward** | **none**}

no functions {**auto-download** | **citrix** | **file-access** | **file-browsing** | **file-entry** | **filter** | **http-proxy** | **url-entry** | **port-forward** | **none**}

構文の説明

auto-download	WebVPN ログイン後のポート フォワーディング Java アプレットの自動ダウンロードをイネーブルまたはディセーブルにします。最初に、ポート フォワーディング、Outlook/Exchange プロキシ、または HTTP プロキシをイネーブルにする必要があります。
citrix	リモート ユーザに対して、MetaFrame Application Server からのターミナル サービスのサポートをイネーブルまたはディセーブルにします。このキーワードを指定すると、セキュアな Citrix コンフィギュレーション内で ASA をセキュア ゲートウェイとして使用できます。これらのサービスでは、ユーザは、標準的な Web ブラウザから MetaFrame アプリケーションにアクセスできます。
file-access	ファイル アクセスをイネーブルまたはディセーブルにします。イネーブルの場合、WebVPN ホームページには、サーバ リスト内のファイル サーバが一覧表示されます。ファイル ブラウジングまたはファイル サーバ名の入力をイネーブルにするには、ファイル アクセスをイネーブルにする必要があります。
file-browsing	ファイル サーバおよび共有のブラウジングをイネーブルまたはディセーブルにします。ユーザによるファイル サーバ名の入力を許可するには、ファイル ブラウジングをイネーブルにする必要があります。
file-entry	ユーザによるファイル サーバの名前の入力をイネーブルまたはディセーブルにします。
filter	Web タイプ ACL を適用します。イネーブルの場合、ASA は、WebVPN の **filter** コマンドで定義された Web タイプ ACL を適用します。

http-proxy	リモート ユーザへの HTTP アプレット プロキシの転送をイネーブルまたはディセーブルにします。このプロキシは、Java、ActiveX、フラッシュなどの、適切なマングリングに干渉するテクノロジーに対して有用です。これによって、ASA の使用を継続しながらマングリングを回避できます。転送されたプロキシは、自動的にブラウザの古いプロキシ コンフィギュレーションを変更して、すべての HTTP および HTTPS 要求を新しいプロキシ コンフィギュレーションにリダイレクトします。HTTP アプレット プロキシでは、HTML、CSS、JavaScript、VBScript、ActiveX、Java など、ほとんどすべてのクライアント側テクノロジーがサポートされています。サポートされているブラウザは、Microsoft Internet Explorer だけです。
none	すべての WebVPN functions に対してヌル値を設定します。デフォルトまたは指定したグループ ポリシーから機能を継承しません。
port-forward	ポート フォワーディングをイネーブルにします。イネーブルの場合、ASA は、WebVPN の **port-forward** コマンドで定義されたポート フォワーディング リストを使用します。
url-entry	ユーザによる URL の入力をイネーブルまたはディセーブルにします。イネーブルの場合でも、ASA は引き続き設定されている URL またはネットワーク ACL に基づいて URL を制限します。URL 入力がディセーブルの場合、ASA では、WebVPN ユーザは、ホームページ上の URL に制限されます。

デフォルト

機能は、デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.1(1)	**auto-download** キーワードおよび **citrix** キーワードが追加されました。
8.0(2)	このコマンドは廃止されました。

使用上のガイドライン

functions none コマンドを発行することによって作成されたヌル値を含め、設定されているすべての機能を削除するには、引数を指定しないでこのコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。機能の値を継承しない場合は、**functions none** コマンドを使用します。

例

次に、FirstGroup という名前のグループ ポリシーに対して、ファイル アクセスおよびファイル ブラウジングを設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# functions file-access file-browsing
```

関連コマンド

コマンド	説明
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。webvpn モードを開始して、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。

fxos mode appliance

Firepower 2100 をアプライアンスモードに設定するには、グローバル コンフィギュレーション モードで **fxos mode appliance** コマンドを使用します。このモードをプラットフォームモードに設定するには、このコマンドの **no** 形式を使用します。

fxos mode appliance

no fxos mode appliance

(注) このコマンドは Firepower 2100 のみでサポートされています。

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトでは、モードはアプライアンスモードに設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.13(1)	コマンドが追加されました。

使用上のガイドライン

Firepower 2100 は、Firepower eXtensible Operating System（FXOS）という基礎となるオペレーティング システムを実行します。Firepower 2100 は、次のモードで実行できます。

- アプライアンスモード（デフォルト）：アプライアンスモードでは、ASA のすべての設定を行うことができます。FXOS CLI からは、高度なトラブルシューティング コマンドのみ使用できます。
- プラットフォーム モード：プラットフォーム モードでは、FXOS で、基本的な動作パラメータとハードウェア インターフェイスの設定を行う必要があります。これらの設定には、インターフェイスの有効化、EtherChannels の確立、NTP、イメージ管理などが含まれます。Firepower Chassis Manager Web インターフェイスまたは FXOS CLI を使用できます。その後、ASDM または ASA CLI を使用して ASA オペレーティング システムにセキュリティ ポリシーを設定できます。

モードを変更すると、設定がクリアされ、現在の設定を保存してシステムをリロードする必要があります。デフォルト設定は、リロード時に適用されます。リロードする前に、中断することなく、モードを元の値に戻すことができます。**clear configure all** および **configure factory-default** コマンドは現在のモードをクリアしません。

現在のモードを表示するには、**show fxos mode** を使用します。

例

次に、モードをプラットフォームモードに設定する例を示します。

```
ciscoasa(config)# no fxos mode appliance
Mode set to platform mode
WARNING: This command will take effect after the running-config is saved and the system
has been rebooted. Command accepted.
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: c0532471 648dc7c2 4f2b4175 1f162684

23736 bytes copied in 1.520 secs (23736 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm]
```

関連コマンド

コマンド	説明
connect fxos	FXOS CLI に接続します。
show fxos mode	現在のモード、アプライアンス、またはプラットフォームを表示します。

fxos permit

ASA データ インターフェイスから FirePOWER 2100 で FXOS SSH、HTTPS、または SNMP を使用するには、グローバル コンフィギュレーション モードで **fxos permit** コマンドを使用します。アクセスを無効にするには、このコマンドの **no** 形式を使用します。

fxos {**https** | **ssh** | **snmp**} **permit** {*ipv4_address netmask* | *ipv6_address*/*prefix_length*} *interface_name*

no fxos {**https** | **ssh** | **snmp**} **permit** {*ipv4_address netmask* | *ipv6_address*/*prefix_length*} *interface_name*

構文の説明

https	Firepower Chassis Manager に対し、HTTPS アクセスを許可します。デフォルト ポートは 3443 です。
interface_name	アクセスが許可されている ASA データ インターフェイスを指定します。管理専用インターフェイスは指定できません。
ipv4_address netmask	IPv4 アドレスおよびサブネット マスクを指定します。
ipv6_address/*prefix_length*	IPv6 プレフィックスとプレフィックス長を指定します。
snmp	FXOS への SNMP アクセスを許可します。デフォルト ポートは 3061 です。デバイスからの SNMP トラフィックについては、**ip-client** コマンドも設定する必要があります。
ssh	FXOS への SSH アクセスを許可します。デフォルト ポートは 3022 です。

コマンド デフォルト

次のデフォルトを参照してください。

- HTTPS デフォルト ポート:3443
- SNMP デフォルト ポート:3061
- SSH デフォルト ポート:3022

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.8(2)	このコマンドが追加されました。

使用上のガイドライン

データ インターフェイスから Firepower 2100 の FXOS を管理する場合、SSH、HTTPS、および SNMP アクセスを設定できます。この機能は、デバイスをリモート管理する場合、および管理 1/1 を隔離されたネットワークに維持する場合に役立ちます。継続してローカル アクセスで管理 1/1 を使用できます。1 つのゲートウェイしか指定できないため、ASA データ インターフェイスへのトラフィック転送用に同時に FXOS の管理 1/1 からのリモート アクセスを許可することはできません。デフォルトでは、FXOS 管理ゲートウェイは ASA への内部パスです。

ASA は、FXOS アクセスに非標準ポートを使用します。標準ポートは同じインタ フェースで ASA が使用するため予約されています。ポート値を変更するには、**fxos port** コマンドを使用します。ASA が FXOS にトラフィックを転送するときに、非標準の宛先ポートはプロトコルごとに FXOS ポートに変換されます（FXOS の HTTPS ポートは変更しません）。パケット宛先 IP アドレス（ASA インターフェイス IP アドレス）も、FXOS で使用する内部アドレスに変換されます。送信元アドレスは変更されません。トラフィックを返す場合、ASA は自身のデータ ルーティング テーブルを使用して正しい出力インターフェイスを決定します。管理アプリケーションの ASA データ IP アドレスにアクセスする場合、FXOS ユーザ名を使用してログインする必要があります。ASA ユーザ名は ASA 管理アクセスのみに適用されます。

ip-client コマンドを使用して、ASA データ インターフェイスでの FXOS 管理トラフィックの開始を有効にすることもできます。これは、たとえば、SNMP トラップ、NTP と DNS のサーバ アクセスなどに必要です。

FXOS コンフィギュレーションでは、管理アドレスを許可するため、アクセス リストを設定する必要があります（**ip-block** コマンド）。**fxos permit** コマンドでアドレスを指定している場合、そのアドレスを許可する必要があります。また、デフォルト ゲートウェイが 0.0.0.0 に設定されていることを確認してください。これにより、ASA がゲートウェイとして設定されます。FXOS の **set out-of-band** コマンドを参照してください。

（注） ASA データ インターフェイスに VPN トンネルを使用して、FXOS に直接アクセスすることはできません。SSH の回避策として、ASA に VPN 接続し、ASA CLI にアクセスし、**connect fxos** コマンドを使用して FXOS CLI にアクセスします。SSH、HTTPS、および SNMPv3 は暗号化できるため、データ インターフェイスへの直接接続は安全です。

例

次に、192.168.1.0/24 ネットワークおよび 2001:DB8::34/64 ネットワーク用の内部インターフェイス上で、SSH アクセスおよび HTTPS アクセスを有効にする例を示します。

```
ciscoasa(config)# fxos https permit 192.168.1.0 255.255.155.0 inside
ciscoasa(config)# fxos https permit 2001:DB8::34/64 inside
ciscoasa(config)# fxos ssh permit 192.168.1.0 255.255.155.0 inside
ciscoasa(config)# fxos ssh permit 2001:DB8::34/64 inside
```

関連コマンド

コマンド	説明
connect fxos	ASA CLI から FXOS CLI に接続します。
fxos port	FXOS 管理アクセス ポートを設定します。
ip-client	FXOS 管理トラフィックを ASA データ インターフェイスに出力することを許可します。

fxos port

FirePOWER 2100 ASA データ インターフェイスで FXOS にアクセスするときの SSH ポート、HTTPS ポート、または SNMP ポートを設定するには、グローバル コンフィギュレーション モードで **fxos port** コマンドを使用します。デフォルト ポートを使用するには、このコマンドの **no** 形式を使用します。

fxos {**https** | **ssh** | **snmp**} **port** *port*

no fxos {**https** | **ssh** | **snmp**} **permit** {*ipv4_address netmask* | *ipv6_address*/*prefix_length*} *interface_name*

構文の説明

https	FXOS に対する HTTPS アクセスのためのポートを設定します。デフォルト ポートは 3443 です。
port	ポート番号を指定します。
snmp	FXOS に対する SNMP アクセスのためのポートを設定します。デフォルト ポートは 3061 です。
ssh	FXOS に対する SSH アクセスのためのポートを設定します。デフォルト ポートは 3022 です。

コマンド デフォルト

次のデフォルトを参照してください。

- HTTPS デフォルト ポート:3443
- SNMP デフォルト ポート:3061
- SSH デフォルト ポート:3022

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.8(2)	このコマンドが追加されました。

使用上のガイドライン

fxos permit コマンドを使用して FirePOWER 2100 データ インターフェイスでの FXOS アクセスを許可する場合、使用するポートをアプリケーションごとに設定することができます。ASA は、FXOS アクセスに非標準ポートを使用します。標準ポートは同じインタ フェースで ASA が使用するため予約されています。ASA が FXOS にトラフィックを転送するときに、非標準の宛先ポートはプロトコルごとに FXOS ポートに変換されます（FXOS の HTTPS ポートは変更しません）。

例

次に、SSH アクセスおよび HTTPS アクセスのためのポートを設定する例を示します。

```
ciscoasa(config)# fxos https port 6666
ciscoasa(config)# fxos ssh port 7777
```

関連コマンド

コマンド	説明
connect fxos	ASA CLI から FXOS CLI に接続します。
fxos permit	ASA データ インターフェイスでの FXOS 管理アクセスを許可します。
ip-client	FXOS 管理トラフィックを ASA データ インターフェイスに出力することを許可します。

gateway コマンド～ hw-module module shutdown コマンド

gateway

特定のゲートウェイを管理しているコール エージェントのグループを指定するには、MGCP マップ コンフィギュレーション モードで **gateway** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

gateway *ip_address* [*group_id*]

構文の説明

gateway	特定のゲートウェイを管理するコール エージェント グループ。
group_id	コール エージェント グループの ID（0 ～ 2147483647）。
ip_address	ゲートウェイの IP アドレス。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
MGCP マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

特定のゲートウェイを管理しているコール エージェントのグループを指定するには、**gateway** コマンドを使用します。*ip_address* オプションを使用して、ゲートウェイの IP アドレスを指定します。*group_id* オプションには 0 ～ 4294967295 の数字を指定します。この数字は、ゲートウェイを管理しているコール エージェントの *group_id* に対応している必要があります。1 つのゲートウェイは 1 つのグループだけに所属できます。

例

次に、コール エージェント 10.10.11.5 および 10.10.11.6 にゲートウェイ 10.10.10.115 の制御を許可し、コール エージェント 10.10.11.7 および 10.10.11.8 にゲートウェイ 10.10.10.116 および 10.10.10.117 の制御を許可する例を示します。

```
ciscoasa(config)# mgcp-map mgcp_policy
ciscoasa(config-mgcp-map)# call-agent 10.10.11.5 101
ciscoasa(config-mgcp-map)# call-agent 10.10.11.6 101
ciscoasa(config-mgcp-map)# call-agent 10.10.11.7 102
ciscoasa(config-mgcp-map)# call-agent 10.10.11.8 102
ciscoasa(config-mgcp-map)# gateway 10.10.10.115 101
ciscoasa(config-mgcp-map)# gateway 10.10.10.116 102
ciscoasa(config-mgcp-map)# gateway 10.10.10.117 102
```

関連コマンド

コマンド	説明
debug mgcp	MGCP のデバッグ情報の表示をイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。
show mgcp	MGCP のコンフィギュレーションおよびセッションの情報を表示します。

gateway-fqdn

ASA の FQDN を設定するには、**gateway-fqdn** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

gateway-fqdn value {**FQDN_Name** | **none**}

no gateway-fqdn

構文の説明

fqdn-name	ASA の FQDN を定義して、AnyConnect クライアントにプッシュします。
none	FQDN をヌル値として指定して、FQDN が指定されないようにします。hostname コマンドおよび domain-name コマンドを使用して設定されたグローバル FQDN が使用されます（使用可能な場合）。

デフォルト

デフォルト FQDN 名は、デフォルトのグループ ポリシーで設定されていません。新しいグループ ポリシーは、この値を継承するように設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASA 間にロード バランシングを設定した場合は、VPN セッションの再確立に使用される ASA IP アドレスを解決するために、ASA の FQDN を指定します。この設定は、さまざまな IP プロトコルのネットワーク間のクライアント ローミングをサポートするうえで重要です（IPv4 から IPv6 など）。

AnyConnect プロファイルにある ASA FQDN を使用してローミング後に ASA IP アドレスを取得することはできません。アドレスがロード バランシング シナリオの正しいデバイス（トンネルが確立されているデバイス）と一致しない場合があります。

ASA の FQDN がクライアントにプッシュされない場合、クライアントは、以前にトンネルが確立されている IP アドレスへの再接続を試みます。異なる IP プロトコル（IPv4 から IPv6）のネットワーク間のローミングをサポートするには、AnyConnect は、トンネルの再確立に使用する ASA アドレスを決定できるように、ローミング後にデバイス FQDN の名前解決を行う必要があります。クライアントは、初期接続中にプロファイルに存在する ASA FQDN を使用します。以後のセッション再接続では、使用可能な場合は常に、ASA によってプッシュされた（また、グループ ポリシーで管理者が設定した）デバイス FQDN を使用します。FQDN が設定されていない場合、ASA は、ASDM の [Device Setup] > [Device Name/Password and Domain Name] の設定内容からデバイス FQDN を取得（およびクライアントに送信）します。

デバイス FQDN が ASA によってプッシュされていない場合、クライアントは、異なる IP プロトコルのネットワーク間のローミング後に VPN セッションを再確立できません。

例

次に、ASA の FQDN を ASAName.example.cisco.com として定義する例を示します。

```
ciscoasa(config-group-policy)# gateway-fqdn value ASAName.example.cisco.com
ciscoasa(config-group-policy)#
```

次に、グループ ポリシーから ASA の FQDN を削除する例を示します。グループ ポリシーは、デフォルト グループ ポリシーからこの値を継承します。

```
ciscoasa(config-group-policy)# no gateway-fqdn
ciscoasa(config-group-policy)#
```

次に、FQDN を値なしとして定義する例を示します。ciscoasa コマンドおよび domain-name コマンドを使用して設定されたグローバル FQDN が使用されます（使用可能な場合）。

```
ciscoasa(config-group-policy)# gateway-fqdn none
ciscoasa(config-group-policy)#
```

graceful-restart

NSF 対応 ASA で OSPFv3 のグレースフル リスタートを設定するには、ルータ コンフィギュレーション モードで graceful-restart コマンドを使用します。必要に応じて、**restart-interval** オプションを使用してグレースフル リスタートの間隔を設定します。グレースフル リスタートをディセーブルにするには、このコマンドの **no** 形式を使用します。

graceful-restart [restart-interval *seconds***]**

no graceful-restart

構文の説明

restart-interval *seconds*	（オプション）グレースフル リスタートの間隔を秒数で指定します。有効な範囲は 1 ～ 1800 です。デフォルトは 120 です。 **（注）** 30 秒未満の再起動間隔では、グレースフル リスタートが中断します。

デフォルト

OSPFv3 グレースフル リスタートはデフォルトでディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション モード	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが導入されました。

使用上のガイドライン

graceful-restart コマンドを使用し、OSPFv3 がプロセス再起動によりデータ フォワーディング パスに留まるようにします。

（注） ASA の一般的なリブート サイクルを許可するには、再起動間隔を十分長く設定します。ネットワークが古いルート情報に依存することを回避するために、再起動間隔を過度に長く設定しないでください。

例

次に、OSPFv3 のグレースフル リスタートをイネーブルにする例を示します。

```
ciscoasa(config)# ipv6 router ospf 1
ciscoasa(config-router)# graceful-restart restart-interval 180
```

関連コマンド

コマンド	説明
graceful-restart helper	NSF 認識 ASA で OSPFv3 グレースフル リスタートをイネーブルにします。

graceful-restart helper

NSF 対応の ASA で OSPFv3 のグレースフル リスタートを設定するには、**graceful-restart** を使用します。グレースフル リスタートをディセーブルにするには、このコマンドの **no** 形式を使用します。

graceful-restart helper [**strict-lsa-checking**]

no graceful-restart helper

構文の説明

strict-lsa-checking	(オプション)ヘルパー モードの厳密なリンクステート アドバタイズメント(LSA)をイネーブルにします。

デフォルト

OSPFv3 グレースフル リスタート ヘルパー モードは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション モード	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが導入されました。

使用上のガイドライン

ASA が NSF をイネーブルにしている場合、ASA は NSF 対応であると考えられ、グレースフル リスタート モードで動作します。OSPF プロセスは、ルート プロセッサ(RP)スイッチオーバーのため、ノンストップ フォワーディングの復帰を実行します。デフォルトでは、NSF 対応 ASA に隣接する ASA は NSF 認識となり、NSF ヘルパー モードで動作します。NSF 対応 ASA がグレースフル リスタートを実行しているときは、ヘルパーの ASA はそのノンストップ フォワーディングの復帰プロセスを支援します。再起動するネイバーのノンストップ フォワーディングの復帰を ASA が支援しないようにする場合は、**no nsf ietf helper** コマンドを入力します。

NSF 認識 ASA および NSF 対応 ASA の両方で厳密な LSA チェックをイネーブルにするには、**graceful-restart helper strict-lsa-checking** コマンドを入力します。ただし、グレースフル リスタート プロセス時に ASA がヘルパー ASA になるまでは厳密な LSA チェックは有効になりません。厳密な LSA チェックをイネーブルにすると、ヘルパー ASA は、LSA の変更があるために再起動 ASA にフラッディングされる場合、または、グレースフル リスタート プロセスが開始されたときに再起動 ASA の再送リスト内の LSA に変更があると検出された場合、再起動 ASA のプロセスの支援を終了します。

例

次に、厳密な LSA チェックを行うグレースフル リスタート ヘルパーをイネーブルにする例を示します。

```
ciscoasa(config)# ipv6 router ospf 1
ciscoasa(config-router)# graceful-restart helper strict-lsa-checking
```

関連コマンド

コマンド	説明
graceful-restart	NSF 対応 ASA で OSPFv3 グレースフル リスタートをイネーブルにします。

group

AnyConnect IPSec 接続に対して IKEv2 セキュリティ アソシエーション（SA）の Diffie-Hellman グループを指定するには、ikev2 ポリシー コンフィギュレーション モードで **group** コマンドを使用します。コマンドを削除してデフォルト設定を使用するには、このコマンドの **no** 形式を使用します。

group {**1** | **2** | **5** | **14** | **19** | **20** | **21** | **24**}

no group {**1** | **2** | **5** | **14** | **19** | **20** | **21** | **24**}

構文の説明

1	768 ビット Diffie-Hellman グループ 1 を指定します（FIPS モードではサポートされません）。
2	1024 ビット Diffie-Hellman グループ 2 を指定します。
5	1536 ビット Diffie-Hellman グループ 5 を指定します。
14	ECDH グループを IKEv2 DH キー交換グループとして選択します。
19	ECDH グループを IKEv2 DH キー交換グループとして選択します。
20	ECDH グループを IKEv2 DH キー交換グループとして選択します。
21	ECDH グループを IKEv2 DH キー交換グループとして選択します。
24	ECDH グループを IKEv2 DH キー交換グループとして選択します。

デフォルト

デフォルトの Diffie-Hellman グループはグループ 14 です。

使用上のガイドライン

IKEv2 SA は、IKEv2 ピアがフェーズ 2 で安全に通信できるようにするためにフェーズ 1 で使用されるキーです。**crypto ikev2 policy** コマンドを入力すると、**group** コマンドを使用して SA の Diffie-Hellman グループを設定できます。ASA および AnyConnect クライアントは、グループ ID を使用して、共有秘密を相互に転送することなく共有秘密を取得します。Diffie-Hellman グループ番号が小さいほど、実行に必要な CPU 時間も少なくなります。Diffie-Hellman グループ番号が大きいほど、セキュリティも高くなります。

AnyConnect クライアントが非 FIPS モードで動作している場合、ASA は Diffie-Hellman グループ 1、2、および 5 をサポートします。FIPS モードでは、サポート グループ 2 および 5 をサポートします。したがって、グループ 1 *だけ*を使用するように ASA を設定する場合、FIPS モードの AnyConnect クライアントは接続に失敗します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ikev2 ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	ECDH グループを IKEv2 DH キー交換グループとして選択する機能が追加されました。
9.13.(1)	デフォルト DH グループは **group 14** です。コマンド オプション **group 2**、**group 5**、および **group 24** は廃止され、以降のリリースで削除されます。

例

次に、ikev2 ポリシー コンフィギュレーション モードを開始して、Diffie-Hellman グループをグループ 5 に設定する例を示します。

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# group 5
ciscoasa(config-ikev2-policy) group 2(Deprecated)
ciscoasa(config-ikev2-policy) group 5(Deprecated)
ciscoasa(config-ikev2-policy) group 24(Deprecated)
ciscoasa(config-ikev2-policy) group 14
```

関連コマンド

コマンド	説明
encryption	AnyConnect IPsec 接続に対して IKEv2 SA の暗号化アルゴリズムを指定します。
group	AnyConnect IPsec 接続に対して IKEv2 SA の Diffie-Hellman グループを指定します。
ライフタイム	AnyConnect IPsec 接続に対して IKEv2 SA の SA ライフタイムを指定します。
prf	AnyConnect IPsec 接続に対して IKEv2 SA の疑似乱数関数を指定します。

group-alias

ユーザがトンネル グループの参照に使用する 1 つ以上の変換名を作成するには、トンネル グループ webvpn コンフィギュレーション モードで **group-alias** コマンドを使用します。リストからエイリアスを削除するには、このコマンドの **no** 形式を使用します。

group-alias *name* [**enable** | **disable**]

no group-alias *name*

構文の説明

disable	グループ エイリアスをディセーブルにします。
enable	以前ディセーブルにしたグループ エイリアスをイネーブルにします。
name	トンネル グループ エイリアスの名前を指定します。選択した任意のストリングを指定できます。ただし、スペースを含めることはできません。

デフォルト

デフォルトのグループ エイリアスはありませんが、グループ エイリアスを指定すると、そのエイリアスがデフォルトでイネーブルになります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
トンネル グループ webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

指定したグループ エイリアスが、ログイン ページのドロップダウン リストに表示されます。各グループに複数のエイリアスを指定することも、エイリアスを指定しないことも可能です。このコマンドは、同じグループが「Devtest」や「QA」などの複数の一般名で知られている場合に役立ちます。

例

次に、「devtest」という名前のトンネル グループを設定し、そのグループに対してエイリアス「QA」および「Fra-QA」を確立するコマンドの例を示します。

```
ciscoasa(config)# tunnel-group devtest type webvpn
ciscoasa(config)# tunnel-group devtest webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-alias QA
ciscoasa(config-tunnel-webvpn)# group-alias Fra-QA
ciscoasa(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体または指定したトンネル グループ コンフィギュレーションをクリアします。
show webvpn group-alias	指定したトンネル グループまたはすべてのトンネル グループのエイリアスを表示します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ属性を設定するためのトンネル グループ webvpn コンフィギュレーション モードを開始します。

group-delimiter

グループ名の解析をイネーブルにして、トンネルのネゴシエート時に受信したユーザ名からグループ名を解析する場合に使用するデリミタを指定するには、グローバル コンフィギュレーション モードで **group-delimiter** コマンドを使用します。このグループ名解析をディセーブルにするには、このコマンドの **no** 形式を使用します。

group-delimiter *delimiter*

no group-delimiter

構文の説明

delimiter	グループ名のデリミタとして使用する文字を指定します。有効な値は、**@**、**#**、および **!** です。

デフォルト

デフォルトで、デリミタは指定されていないため、グループ名解析はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

デリミタは、トンネルがネゴシエートされるときに、ユーザ名からトンネル グループ名を解析するために使用されます。デフォルトで、デリミタは指定されていないため、グループ名解析はディセーブルです。

例

次に、グループ デリミタをハッシュ マスク(#)に変更する **group-delimiter** コマンドの例を示します。

```
ciscoasa(config)# group-delimiter #
```

関連コマンド

コマンド	説明
clear configure group-delimiter	設定したグループ デリミタをクリアします。
show running-config group-delimiter	現在のグループ デリミタ値を表示します。
strip-group	グループ除去処理をイネーブルまたはディセーブルにします。

group-lock

リモート ユーザがトンネル グループを介してしかアクセスできないように制限するには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **group-lock** コマンドを発行します。実行コンフィギュレーションから **group-lock** 属性を削除するには、このコマンドの **no** 形式を使用します。

group-lock {value *tunnel-grp-name* **| none}**

no group-lock

構文の説明

none	group-lock をヌル値に設定します。これにより、グループ ロックの制限が許可されなくなります。デフォルトまたは指定したグループ ポリシーの group-lock 値を継承しないようにします。
value *tunnel-grp-name*	ユーザが接続する際に ASA によって要求される既存のトンネル グループの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名コンフィギュレーション	• 対応	—	• 対応	—	—

使用上のガイドライン

グループ ロックをディセーブルにするには、**group-lock none** コマンドを使用します。**no group-lock** コマンドは、別のグループ ポリシーからの値の継承を許可します。

グループロックは、仮想プライベート ネットワーク（VPN）クライアントに設定されているグループが、ユーザが割り当てられたトンネル グループと一致しているかどうかを確認することにより、ユーザを制約します。同一ではなかった場合、ASA はユーザによる接続を禁止します。グループ ロックを設定しなかった場合、ASA は、割り当てられているグループに関係なくユーザを認証します。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、FirstGroup という名前のグループ ポリシーにグループ ロックを設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# group-lock value tunnel group name
```

group-object

オブジェクト グループにグループ オブジェクトを追加するには、オブジェクトの設定時に **group-object** コマンドを使用します。グループ オブジェクトを削除するには、このコマンドの **no** 形式を使用します。

group-object *obj_grp_name*

no group-object *obj_grp_name*

構文の説明

obj_grp_name	オブジェクト グループ（1 ～ 64 文字）を指定します。文字、数字、および「_」、「-」、「.」の組み合わせが使用可能です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
プロトコル、ネットワーク、サービス、ICMP タイプ、セキュリティ グループおよびユーザ オブジェクト グループの各コンフィギュレーション モード	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(2)	オブジェクトグループ ユーザ コンフィギュレーション モードでオブジェクト グループを追加して、アイデンティティ ファイアウォール機能で使用できるようになりました。

使用上のガイドライン

group-object コマンドは、それ自身がオブジェクト グループであるオブジェクトを追加するために、**object-group** コマンドとともに使用します。このサブコマンドを使用すると、同じタイプのオブジェクトを論理グループ化して、構造化されたコンフィギュレーションの階層オブジェクト グループを構築できます。

オブジェクト グループ内でのオブジェクトの重複は、それらのオブジェクトがグループ オブジェクトの場合は許可されます。たとえば、オブジェクト 1 がグループ A とグループ B の両方に存在する場合、A と B の両方を含むグループ C を定義することができます。ただし、グループ階層を循環型にするグループ オブジェクトを含めることはできません。たとえば、グループ A にグループ B を含め、さらにグループ B にグループ A を含めることはできません。

階層オブジェクト グループは 10 レベルまで許可されています。

(注) ASA は、ネストされた IPv6 ネットワーク オブジェクト グループはサポートしません。したがって、IPv6 エントリが含まれるオブジェクトを別の IPv6 オブジェクト グループの下でグループ化することはできません。

例

次に、ホストを重複させる必要性を排除するために **group-object** コマンドを使用する方法の例を示します。

```
ciscoasa(config)# object-group network host_grp_1
ciscoasa(config-network)# network-object host 192.168.1.1
ciscoasa(config-network)# network-object host 192.168.1.2
ciscoasa(config-network)# exit
ciscoasa(config)# object-group network host_grp_2
ciscoasa(config-network)# network-object host 172.23.56.1
ciscoasa(config-network)# network-object host 172.23.56.2
ciscoasa(config-network)# exit
ciscoasa(config)# object-group network all_hosts
ciscoasa(config-network)# group-object host_grp_1
ciscoasa(config-network)# group-object host_grp_2
ciscoasa(config-network)# exit
ciscoasa(config)# access-list grp_1 permit tcp object-group host_grp_1 any eq ftp
ciscoasa(config)# access-list grp_2 permit tcp object-group host_grp_2 any eq smtp
ciscoasa(config)# access-list all permit tcp object-group all-hosts any eq w
```

次に、ローカル ユーザ グループをユーザ グループ オブジェクトに追加するために **group-object** コマンドを使用する方法の例を示します。

```
ciscoasa(config)# object-group user sampleuser1-group
ciscoasa(config-object-group user)# description group members of sampleuser1-group
ciscoasa(config-object-group user)# user-group EXAMPLE\\group.sampleusers-all
ciscoasa(config-object-group user)# user EXAMPLE\user2
ciscoasa(config-object-group user)# exit
ciscoasa(config)# object-group user sampleuser2-group
ciscoasa(config-object-group user)# description group members of sampleuser2-group
ciscoasa(config-object-group user)# group-object sampleuser1-group
ciscoasa(config-object-group user)# user-group EXAMPLE\\group.sampleusers-marketing
ciscoasa(config-object-group user)# user EXAMPLE\user3
```

関連コマンド

コマンド	説明
clear configure object-group	すべての **object-group** コマンドをコンフィギュレーションから削除します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
show running-config object-group	現在のオブジェクト グループを表示します。

group-policy

グループ ポリシーを作成または編集するには、グローバル コンフィギュレーション モードで **group-policy** コマンドを使用します。コンフィギュレーションからグループ ポリシーを削除するには、このコマンドの **no** 形式を使用します。

group-policy *name* {**internal [from** *group-policy_name*] | **external server-group** *server_group* **password** *server_password*}

no group-policy *name*

構文の説明

external server-group *server_group*	グループ ポリシーを外部として指定し、ASA が属性を照会する AAA サーバ グループを識別します。
from *group-policy_name*	この内部グループ ポリシーの属性を、既存のグループ ポリシーの値に初期化します。
internal	グループ ポリシーを内部として識別します。
name	グループ ポリシーの名前を指定します。この名前は最大 64 文字で、スペースを含めることができます。スペースを含むグループ名は、二重引用符で囲む必要があります（"Sales Group" など）。
password *server_password*	外部 AAA サーバ グループから属性を取得する際に使用するパスワードを指定します。パスワードは最大 128 文字です。スペースを含めることはできません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

ASA には、「DefaultGroupPolicy」という名前のデフォルト グループ ポリシーが常に存在しています。ただし、このデフォルト グループ ポリシーは、これを使用するように ASA を設定しない限り、有効ではありません。設定手順については、CLI 設定ガイドを参照してください。

group-policy attributes コマンドを使用してグループ ポリシー コンフィギュレーション モードを開始します。このモードでは、グループ ポリシーのあらゆる属性と値のペアを設定できます。DefaultGroupPolicy には、次の属性と値のペアがあります。

属性	デフォルト値
backup-servers	keep-client-config
バナー	none
client-access-rules	none
client-firewall	none
default-domain	none
dns-server	none
group-lock	none
ip-comp	disable
ip-phone-bypass	disabled
ipsec-udp	disabled
ipsec-udp-port	10000
leap-bypass	disabled
nem	disabled
password-storage	disabled
pfs	disable
re-xauth	disable
secure-unit-authentication	disabled
split-dns	none
split-tunnel-network-list	none
split-tunnel-policy	tunnelall
user-authentication	disabled
user-authentication-idle-timeout	none
vpn-access-hours	unrestricted
vpn-filter	none
vpn-idle-timeout	30 分
vpn-session-timeout	none
vpn-simultaneous-logins	3
vpn-tunnel-protocol	IPsec WebVPN
wins-server	none

また、グループ ポリシー コンフィギュレーション モードで **webvpn** コマンドを入力するか、**group-policy attributes** コマンドを入力してから、グループ webvpn コンフィギュレーション モードで **webvpn** コマンドを入力することで、グループ ポリシーの webvpn コンフィギュレーション モード属性を設定できます。詳細については、**group-policy attributes** コマンドの説明を参照してください。

例

次に、「FirstGroup」という名前の内部グループ ポリシーを作成する例を示します。

```
ciscoasa(config)# group-policy FirstGroup internal
```

次に、AAA サーバ グループに「BostonAAA」、パスワードに「12345678」を指定し、「ExternalGroup」という名前の外部グループ ポリシーを作成する例を示します。

```
ciscoasa(config)# group-policy ExternalGroup external server-group BostonAAA password
12345678
```

関連コマンド

コマンド	説明
clear configure group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーのコンフィギュレーションを削除します。
group-policy attributes	グループ ポリシー コンフィギュレーション モードを開始します。このモードでは、指定したグループ ポリシーの属性と値を設定したり、webvpn コンフィギュレーション モードを開始して、グループの WebVPN 属性を設定したりできます。
show running-config group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーの実行コンフィギュレーションを表示します。
webvpn	webvpn コンフィギュレーション モードを開始し、指定したグループの WebVPN 属性を設定できるようにします。

group-policy attributes

グループ ポリシーコンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで、**group-policy attributes** コマンドを使用します。グループ ポリシーからすべての属性を削除するには、このコマンドの **no** 形式を使用します。

group-policy *name* **attributes**

no group-policy *name* **attributes**

構文の説明

name	グループ ポリシーの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

グループ ポリシー コンフィギュレーション モードでは、指定したグループ ポリシーの属性と値のペアを設定したり、グループ ポリシー webvpn コンフィギュレーション モードを開始してグループの WebVPN 属性を設定したりできます。

属性モードのコマンド構文には、一般的に、次のような特徴があります。

- **no** 形式は実行コンフィギュレーションから属性を削除し、別のグループ ポリシーからの値の継承をイネーブルにします。
- **none** キーワードは実行コンフィギュレーションの属性をヌル値に設定し、これによって継承を禁止します。
- ブール型属性には、イネーブルおよびディセーブルの設定用に明示的な構文があります。

ASA には、DefaultGroupPolicy という名前のデフォルト グループ ポリシーが常に存在しています。ただし、このデフォルト グループ ポリシーは、これを使用するように ASA を設定しない限り、有効ではありません。設定手順については、CLI 設定ガイドを参照してください。

group-policy attributes コマンドを使用してグループ ポリシー コンフィギュレーション モードを開始します。このモードでは、グループ ポリシーのあらゆる属性と値のペアを設定できます。DefaultGroupPolicy には、次の属性と値のペアがあります。

属性	デフォルト値
backup-servers	keep-client-config
バナー	none
client-access-rule	none
client-firewall	none
default-domain	none
dns-server	none
group-lock	none
ip-comp	disable
ip-phone-bypass	disabled
ipsec-udp	disabled
ipsec-udp-port	10000
leap-bypass	disabled
nem	disabled
password-storage	disabled
pfs	disable
re-xauth	disable
secure-unit-authentication	disabled
split-dns	none
split-tunnel-network-list	none
split-tunnel-policy	tunnelall
user-authentication	disabled
user-authentication-idle-timeout	none
vpn-access-hours	unrestricted
vpn-filter	none
vpn-idle-timeout	30 分
vpn-session-timeout	none
vpn-simultaneous-logins	3
vpn-tunnel-protocol	IPsec WebVPN
wins-server	none

また、**group-policy attributes** コマンドを入力してから、グループ ポリシー コンフィギュレーション モードで **webvpn** コマンドを入力することで、グループ ポリシーの webvpn モード属性を設定できます。詳細については、**webvpn** コマンド(グループ ポリシー属性モードおよびユーザ名属性モード)の説明を参照してください。

例

次に、FirstGroup という名前のグループ ポリシーのグループ ポリシー属性モードを開始する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)#
```

関連コマンド

コマンド	説明
clear configure group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーのコンフィギュレーションを削除します。
group-policy	グループ ポリシーを作成、編集、または削除します。
show running-config group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーの実行コンフィギュレーションを表示します。
webvpn	グループ webvpn コンフィギュレーション モードを開始し、指定したグループの WebVPN 属性を設定できるようにします。

group-prompt

WebVPN ユーザが ASA に接続したときに表示される WebVPN ページ ログイン ボックスのグループ プロンプトをカスタマイズするには、webvpn カスタマイゼーション コンフィギュレーション モードで **group-prompt** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

group-prompt {**text** | **style**} *value*

no group-prompt {**text** | **style**} *value*

構文の説明

text	テキストへの変更を指定します。
style	スタイルへの変更を指定します。
value	実際に表示するテキスト、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）。

デフォルト

グループ プロンプトのデフォルト テキストは「GROUP:」です。

グループ プロンプトのデフォルト スタイルは、color:black;font-weight:bold;text-align:right です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn カスタマイゼーション コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

style オプションは、任意の有効な CSS パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進数値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

例

次に、テキストを「Corporate Group:」に変更し、デフォルト スタイルのフォント ウェイトを bolder に変更する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# group-prompt text Corporate Group:
ciscoasa(config-webvpn-custom)# group-prompt style font-weight:bolder
```

関連コマンド

コマンド	説明
password-prompt	WebVPN ページのパスワード プロンプトをカスタマイズします。
username-prompt	WebVPN ページのユーザ名プロンプトをカスタマイズします。

group-search-timeout

show ad-groups コマンドを使用して照会した Active Directory サーバからの応答を待機する最大時間を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **group-search-timeout** コマンドを使用します。コンフィギュレーションからコマンドを削除するには、このコマンドの **no** 形式を使用します。

group-search-timeout *seconds*

no group-search-timeout *seconds*

構文の説明

seconds	Active Directory サーバからの応答を待機する時間（1 ～ 300 秒）。

デフォルト

デフォルトは 10 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

show ad-groups コマンドは LDAP を使用している Active Directory サーバにのみ適用され、Active Directory サーバでリストされているグループが表示されます。**group-search-timeout** コマンドを使用して、サーバからの応答を待機する時間を調整します。

例

次に、タイムアウトを 20 秒に設定する例を示します。

```
ciscoasa(config-aaa-server-host)#group-search-timeout 20
```

関連コマンド

コマンド	説明
ldap-group-base-dn	サーバが、ダイナミック グループ ポリシーで使用されるグループの検索を開始する Active Directory 階層のレベルを指定します。
show ad-groups	Active Directory サーバ上でリストされるグループを表示します。

group-url

グループに対する着信 URL または IP アドレスを指定するには、トンネル グループ webvpn コンフィギュレーション モードで **group-url** コマンドを使用します。リストから URL を削除するには、このコマンドの **no** 形式を使用します。

group-url *url* [**enable** | **disable**]

no group-url *url*

構文の説明

disable	URL をディセーブルにしますが、リストからは削除しません。
enable	URL をイネーブルにします。
url	このトンネル グループの URL または IP アドレスを指定します。

デフォルト

デフォルトの URL または IP アドレスはありませんが、URL または IP アドレスを指定すると、これがデフォルトでイネーブルになります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
トンネル グループ webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

グループの URL または IP アドレスを指定すると、ユーザがログイン時にグループを選択する必要がなくなります。ユーザがログインすると、ASA はトンネル グループ ポリシー テーブル内でユーザの着信 URL/アドレスを検索します。URL/アドレスが見つかり、さらにトンネル グループでこのコマンドがイネーブルになっている場合、ASA は関連するトンネル グループを自動的に選択して、ユーザ名およびパスワード フィールドだけをログイン ウィンドウでユーザに表示します。これによりユーザ インターフェイスが簡素化され、グループ リストがユーザに表示されなくなるという利点が追加されます。ユーザに表示されるログイン ウィンドウでは、そのトンネル グループ用に設定されているカスタマイゼーションが使用されます。

URL/アドレスがディセーブルで、**group-alias** コマンドが設定されている場合は、グループのドロップダウン リストも表示され、ユーザによる選択が必要になります。

1 つのグループに対して複数の URL/アドレスを設定する（または、1 つも設定しない）ことができます。URL/アドレスごとに個別にイネーブルまたはディセーブルに設定できます。指定した URL/アドレスごとに個別の **group-url** コマンドを使用する必要があります。HTTP または HTTPS プロトコルを含めて、URL/アドレス全体を指定する必要があります。

複数のグループに同じ URL/アドレスを関連付けることはできません。ASA では、URL/アドレスの一意性を検証してから、これをトンネル グループに対して受け入れます。

例

次に、「test」という名前の WebVPN トンネル グループを設定し、そのグループに対して 2 つのグループ URL「http://www.cisco.com」および「https://supplier.example.com」を確立するコマンドの例を示します。

```
ciscoasa(config)# tunnel-group test type webvpn
ciscoasa(config)# tunnel-group test webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-url http://www.cisco.com
ciscoasa(config-tunnel-webvpn)# group-url https://supplier.example.com
ciscoasa(config-tunnel-webvpn)#
```

次に、RadiusServer という名前のトンネル グループに対して、グループ URL、http://www.cisco.com および http://192.168.10.10 をイネーブルにする例を示します。

```
ciscoasa(config)# tunnel-group RadiusServer type webvpn
ciscoasa(config)# tunnel-group RadiusServer general-attributes
ciscoasa(config-tunnel-general)# authentication server-group RADIUS
ciscoasa(config-tunnel-general)# accounting-server-group RADIUS
ciscoasa(config-tunnel-general)# tunnel-group RadiusServer webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-alias "Cisco Remote Access" enable
ciscoasa(config-tunnel-webvpn)# group-url http://www.cisco.com enable
ciscoasa(config-tunnel-webvpn)# group-url http://192.168.10.10 enable
ciscoasa(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体または指定したトンネル グループ コンフィギュレーションをクリアします。
show webvpn group-url	指定したトンネル グループまたはすべてのトンネル グループの URL を表示します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ属性を設定する webvpn コンフィギュレーション モードを開始します。

gtp-u-header-check

GTP データ パケットの内部ペイロードが有効な IP パケットであるかどうかを確認し、そうでない場合はドロップします。GTP インスペクション ポリシー マップのパラメータ コンフィギュレーション モードで **gtp-u-header-check** コマンドを使用します。確認を無効にするには、このコマンドの **no** 形式を使用します。

gtp-u-header-check [**anti-spoofing** [**gtpv2-dhcp-bypass** | **gtpv2-dhcp-drop**]]

no gtp-u-header-check [**anti-spoofing** [**gtpv2-dhcp-bypass** | **gtpv2-dhcp-drop**]]

構文の説明

アンチスプーフィング	内部ペイロードの IP ヘッダー内のモバイル ユーザ IP アドレスが、セッション作成応答などの GTP 制御メッセージに割り当てられている IP アドレスと一致するかどうかを確認し、IP アドレスが一致しない場合は GTP-U メッセージをドロップします。このチェックでは、IPv4、IPv6、および IPv4v6 PDN タイプがサポートされています。 モバイル端末が DHCP を使用してそのアドレスを取得する場合、GTPv2 でのエンドユーザの IP アドレスは 0.0.0.0（IPv4）または *prefix*::0（IPv6）になります。その場合、システムは内部パケットで検出した最初の IP アドレスを使用してエンドユーザ IP アドレスを更新します。**gtpv2-dhcp** キーワードを使用して、DHCP で取得したアドレスのデフォルトの動作を変更できます。
gtpv2-dhcp-bypass	0.0.0.0 または *prefix*::0 アドレスを更新しません。その代わりに、エンドユーザの IP アドレスが 0.0.0.0 または *prefix*::0 の場合はパケットを許可します。IP アドレスの取得に DHCP を使用すると、このオプションはアンチスプーフィング チェックをバイパスします。
gtpv2-dhcp-drop	0.0.0.0 または *prefix*::0 アドレスを更新しません。その代わりに、エンドユーザの IP アドレスが 0.0.0.0 または *prefix*::0 の場合はすべてのパケットをドロップします。このオプションは、IP アドレスの取得に DHCP を使用するユーザへのアクセスを防ぎます。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション モード	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.10(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、アンチスプーフィングを実装できます。GTP-C を通じて割り当てたものではない別の IP アドレスを使用してハッカーが別の顧客であるように装う（スプーフィング）可能性があります。アンチスプーフィングは、使用されている GTP-U アドレスが実際に GTP-C を使用して割り当てたものであるかどうかを確認します。

例

次に、デフォルトの動作でアンチスプーフィングを有効にする例を示します。

```
ciscoasa(config)# policy-map type inspect gtp gtp-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# gtp-u-header-check anti-spoofing
```

関連コマンド

コマンド	説明
anti-replay	GTP インスペクションで GTP アンチリプレイを有効にします。
inspect gtp	GTP アプリケーション インスペクションをイネーブルにします。
policy-map type inspect gtp	GTP インスペクション ポリシー マップを作成または編集します。
show service-policy inspect gtp	GTP 設定および統計情報を表示します。

h245-tunnel-block

H.323 で H.245 トンネリングをブロックするには、パラメータ コンフィギュレーション モードで **h245-tunnel-block** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

h245-tunnel-block action [**drop-connection** | **log**]

no h245-tunnel-block action [**drop-connection** | **log**]

構文の説明

drop-connection	H.245 トンネルが検出された場合、コール設定接続をドロップします。
log	H.245 トンネルが検出された場合、ログを発行します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、H.323 コールで H.245 トンネリングをブロックする例を示します。

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# h245-tunnel-block action drop-connection
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

hardware-bypass

Cisco ISA 3000 のハードウェア バイパスをイネーブルにし、停電時もインターフェイス ペア間のトラフィック フローを続行させるには、グローバル コンフィギュレーション モードで **hardware-bypass** コマンドを使用します。ハードウェア バイパスをディセーブルにするには、このコマンドの **no** 形式を使用します。

hardware-bypass GigabitEthernet {**1/1-1/2 | 1/3-1/4**} [**sticky**]

no hardware-bypass GigabitEthernet {**1/1-1/2 | 1/3-1/4**} [**sticky**]

(注) この機能は、Cisco ISA 3000 アプライアンスのみで使用できます。

構文の説明

GigabitEthernet {**1/1-1/2	1/3-1/4**}	サポートされているインターフェイス ペアは、銅線 GigabitEthernet 1/1 と 1/2 および GigabitEthernet 1/3 と 1/4 です。光ファイバ イーサネット モデルがある場合は、銅線イーサネット ペア（GigabitEthernet 1/1 および 1/2）のみがハードウェア バイパスをサポートします。このコマンドは、ペアごとに別々に入力します。
sticky	（任意）電源が回復し、アプライアンスが起動した後は、アプライアンスをハードウェア バイパス モードに保ちます。この場合、**no hardware-bypass manual** コマンドを使用する準備が整った時点でハードウェア バイパスを手動でオフにする必要があります。このオプションを使用すると短時間の割り込みがいつ発生するかを制御できます。

コマンド デフォルト

ハードウェア バイパスは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.4(1.225)	このコマンドが追加されました。

使用上のガイドライン

ハードウェア バイパスがアクティブな場合はファイアウォール機能が設定されていません。したがって、トラフィックの通過を許可しているリスクをご自身が理解していることを確認してください。ハードウェア バイパスを非アクティブ化すると、ASA がフローを引き継ぐため、接続が短時間中断されます。

(注) ISA 3000 への電源が切断され、ハードウェア バイパス モードに移行すると、通信できるのは上記のインターフェイス ペアのみになります。つまり、デフォルトの設定を使用している場合は、inside1 <---> inside2 および outside1 <---> outside2 は通信できなくなります。これらのインターフェイス間の既存の接続がすべて失われます。

例

次に、GigabitEthernet 1/1 および 1/2 のハードウェア バイパスをディセーブルにし、1/3 および 1/4 をイネーブルにする例を示します。

```
ciscoasa(config)# no hardware-bypass GigabitEthernet 1/1-1/2
ciscoasa(config)# hardware-bypass GigabitEthernet 1/3-1/4
```

関連コマンド

コマンド	説明
hardware-bypass boot-delay	ハードウェア バイパスを設定して、ASA FirePOWER が起動するまでアクティブに維持します。
hardware-bypass manual	手動でハードウェア バイパスをアクティブまたは非アクティブにします。

hardware-bypass boot-delay

Cisco ISA 3000 にハードウェア バイパスを設定し、ASA Firepower モジュールが起動するまでアクティブに維持するには、グローバル コンフィギュレーション モードで **hardware-bypass boot-delay** コマンドを使用します。ブート遅延をディセーブルにするには、このコマンドの **no** 形式を使用します。

hardware-bypass boot-delay module-up sfr

no hardware-bypass boot-delay module-up sfr

(注) この機能は、Cisco ISA 3000 アプライアンスのみで使用できます。

構文の説明

module-up sfr	ASA FirePOWER が起動するまでハードウェア バイパスをディセーブルにするのを遅延します。

コマンド デフォルト

ブート遅延はデフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.4(1.225)	このコマンドが追加されました。

使用上のガイドライン

hardware-bypass boot-delay コマンドが動作するようにするには、**sticky** オプションを設定せずに **hardware-bypass** コマンドを使用してハードウェア バイパスをイネーブルにする必要があります。**hardware-bypass boot-delay** を使用しないと、ASA FirePOWER モジュールが起動を完了する前にハードウェア バイパスが非アクティブになる可能性があります。たとえば、モジュールをフェール クローズに設定していた場合、このような状況では、トラフィックがドロップされる可能性があります。

例

次に、(**sticky** オプションを*設定せずに*)ハードウェア バイパスをイネーブルにし、ブート遅延をイネーブルにする例を示します。

```
ciscoasa(config)# hardware-bypass GigabitEthernet 1/1-1/2
ciscoasa(config)# hardware-bypass GigabitEthernet 1/3-1/4
ciscoasa(config)# hardware-bypass boot-delay module-up sfr
```

関連コマンド

コマンド	説明
hardware-bypass	サポートされているインターフェイス ペアのハードウェア バイパスを設定します。
hardware-bypass manual	手動でハードウェア バイパスをアクティブまたは非アクティブにします。

hardware-bypass manual

Cisco ISA 3000 でハードウェア バイパスを手動でアクティブまたは非アクティブにするには、特権 EXEC モードで **hardware-bypass manual** コマンドを使用します

hardware-bypass manual GigabitEthernet {**1/1-1/2 | 1/3-1/4**}

no hardware-bypass manual GigabitEthernet {**1/1-1/2 | 1/3-1/4**}

(注) この機能は、Cisco ISA 3000 アプライアンスのみで使用できます。

構文の説明

GigabitEthernet {**1/1-1/2	1/3-1/4**}	サポートされているインターフェイス ペアは、銅線 GigabitEthernet 1/1 と 1/2 および GigabitEthernet 1/3 と 1/4 です。光ファイバ イーサネット モデルがある場合は、銅線イーサネット ペア（GigabitEthernet 1/1 および 1/2）のみがハードウェア バイパスをサポートします。このコマンドは、ペアごとに別々に入力します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	—	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.4(1.225)	このコマンドが追加されました。

使用上のガイドライン

hardware-bypass コマンドの **sticky** オプションを設定してバイパスをイネーブルに維持する場合は、**hardware-bypass manual** コマンドを使用して電源回復後にハードウェア バイパスを非アクティブ化する必要があります。

このコマンドによって、現在のハードウェア バイパスの状態が変更されます。電源障害が発生した場合は、**hardware-bypass** コンフィギュレーション コマンドのアクションが優先されます。たとえば、**hardware-bypass** がディセーブルに設定されている場合にハードウェア バイパスを手動でイネーブルにした後で電源障害が発生したときは、ハードウェア バイパスは設定に従ってディセーブルになります。

例

次に、手動で GigabitEthernet 1/2 および 1/2 のハードウェア バイパスを非アクティブ化する例を示します。

```
ciscoasa# no hardware-bypass manual GigabitEthernet 1/1-1/2
```

関連コマンド

コマンド	説明
hardware-bypass	サポートされているインターフェイス ペアのハードウェア バイパスを設定します。
hardware-bypass boot-delay	ハードウェア バイパスを設定して、ASA FirePOWER が起動するまでアクティブに維持します。

health-check

クラスタのヘルス チェック機能をイネーブルにするには、クラスタ グループ コンフィギュレーション モードで **health-check** コマンドを使用します。ヘルス チェックをディセーブルにするには、このコマンドの **no** 形式を使用します。

health-check [**holdtime** *timeout*] [**vss-enabled**] [**monitor-interface** {*interface_id* | **service-module** | **debounce-time**}]

no health-check [**holdtime** *timeout*] [**vss-enabled**] [**monitor-interface** {*interface_id* | **service-module** | **debounce-time**}]

構文の説明

holdtime *timeout*	(任意)キープアライブまたはインターフェイス ステータス メッセージの間隔を 3(9.8(1) 以降)または 8(9.7 以前)～ 45 秒の間で決定します。デフォルトは 3 秒です。低い保留時間を設定すると、CCL メッセージングおよび CPU アクティビティが向上します。保留時間を .3 ～ .7 に設定した後に ASA ソフトウェアをダウングレードした場合、新しい設定がサポートされていないので、この設定はデフォルトの 3 秒に戻ります。
monitor-interface {*interface_id* | **service-module** | **debounce-time**}	(任意)このコマンドの **no** 形式を使用すると、インターフェイスまたはハードウェア モジュール(**service-module**)のインターフェイス ヘルス チェックがディセーブルになります。たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルス モニタリングをディセーブルにすることができます。ポートチャネル ID と冗長 ID、または単一の物理インターフェイス ID を指定できます。ヘルス モニタリングは VLAN サブインターフェイス、または VNI や BVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。 ASA が失敗したインターフェイスを削除する前のデバウンス時間を設定するには、**debounce-time** キーワードを使用します。デバウンス時間は 300 ～ 9000 ms の範囲の値を設定します。デフォルトは 500 ms です。値を小さくすると、インターフェイスの障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェイスのステータス更新が発生すると、ASA はインターフェイスを削除するまでに指定されたミリ秒数待機します。EtherChannel がダウン状態からアップ状態に移行する場合(スイッチがリロードされた、スイッチで EtherChannel が有効になったなど)、デバウンス時間がより長くなり、ポートのバンドルにおいて別のクラスタ ユニットの方が高速なため、クラスタ ユニットでインターフェイスの障害が表示されることを妨げることがあります。

vss-enabled	EtherChannel としてクラスタ制御リンクを設定し（推奨）、VSS または vPC ペアに接続している場合、**vss-enabled** オプションをイネーブルにする必要がある場合があります。一部のスイッチでは、VSS/vPC の 1 つのユニットがシャット ダウンまたは起動すると、そのスイッチに接続された EtherChannel メンバー インターフェイスが ASA に対してアップ状態であるように見えますが、これらのインターフェイスはスイッチ側のトラフィックを通していません。ASA holdtime timeout を低い値（0.8 秒など）に設定した場合、ASA が誤ってクラスタから削除される可能性があり、ASA はキープアライブ メッセージをこれらのいずれかの EtherChannel インターフェイスに送信します。**vss-enabled** をイネーブルにすると、ASA はクラスタ制御リンク内のすべての EtherChannel インターフェイス上にキープアライブ メッセージをフラッディングして、少なくとも 1 つのスイッチがこれを受信できるようにします。

コマンド デフォルト

デフォルトでは、ヘルス チェックがイネーブルで、holdtime が 3 秒です。

デフォルトでは、すべてのインターフェイスでインターネット ヘルス モニタリングがイネーブルになっています。

デバウンス時間は 500 ms です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラスタ グループ コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。
9.1(4)	**vss-enabled** キーワードが追加されました。
9.4(1)	**monitor-interface** キーワードが追加されました。
9.5(1)	**service-module** キーワードが追加されました。
9.8(1)	**保留時間**の最小値が 3 秒に下がりました。FirePOWER 4100/9300 に **debounce-time** キーワードが追加されました。
9.9(2)	ASA アプライアンスに **debounce-time** キーワードが追加されました。
9.10(1)	**debounce-time** キーワードは、ダウン状態から稼働状態に変更するインターフェイスに適用されるようになりました。

使用上のガイドライン

何らかのトポロジ変更を行うとき（たとえば、データ インターフェイスの追加または削除、またはスイッチ上のインターフェイスのイネーブル化またはディセーブル化、VSS または vPC を形成するスイッチの追加）は、ヘルス チェック機能をディセーブルにし、ディセーブルにしたインターフェイスのモニタリングもディセーブルにしてください（**no health-check monitor-interface**）。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルス チェック機能を再度イネーブルにできます。

メンバー間のキープアライブ メッセージによって、メンバーのヘルス状態が特定されます。ユニットが holdtime 期間内にピア ユニットからキープアライブ メッセージを受信しない場合は、そのピア ユニットは応答不能またはデッド状態と見なされます。インターフェイス ステータス メッセージによって、リンク障害が検出されます。あるインターフェイスが、特定のユニット上では障害が発生したが、別のユニットではアクティブの場合は、そのユニットはクラスタから削除されます。

（注） 9.8(1) では、ユニット ヘルス チェック メッセージング スキームが、コントロール プレーンの *キープアライブ*からデータ プレーンの *ハートビート*に変更されました。データ プレーンを使用しると、CPU の使用率および信頼性が向上します。

ユニットがホールド時間内にインターフェイス ステータス メッセージを受信しない場合に、ASA がメンバをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのユニットが確立済みメンバであるか、またはクラスタに参加しようとしているかによって異なります。EtherChannel の場合（スパニングかどうかを問わない）は、確立済みメンバーのインターフェイスがダウン状態のときに、ASA はそのメンバーを 9 秒後に削除します。ユニットが新しいメンバーとしてクラスタに参加しようとしているときは、ASA は 45 秒待機してからその新しいユニットを拒否します。非 EtherChannel の場合は、メンバー状態に関係なく、ユニットは 500 ミリ秒後に削除されます。

このコマンドは、ブートストラップ コンフィギュレーションの一部ではなく、マスター ユニットからスレーブ ユニットに複製されます。

例

次に、ヘルス チェックをディセーブルにする例を示します。

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# no health-check
```

関連コマンド

コマンド	説明
clacp system-mac	スパンド EtherChannel を使用するときは、ASA は cLACP を使用してネイバー スイッチとの間で EtherChannel のネゴシエーションを行います。
cluster group	クラスタに名前を付け、クラスタ コンフィギュレーション モードを開始します。
cluster-interface	クラスタ制御リンク インターフェイスを指定します。
cluster interface-mode	クラスタ インターフェイス モードを設定します。
conn-rebalance	接続の再分散をイネーブルにします。
console-replicate	スレーブ ユニットからマスター ユニットへのコンソール複製をイネーブルにします。
enable（クラスタ グループ）	クラスタリングをイネーブルにします。

コマンド	説明
health-check auto-rejoin	ヘルス チェック失敗後の自動再結合クラスタ設定をカスタマイズします。
key	クラスタ制御リンクの制御トラフィックの認証キーを設定します。
local-unit	クラスタ メンバーに名前を付けます。
mtu cluster-interface	クラスタ制御リンク インターフェイスの最大伝送ユニットを指定します。
priority（クラスタ グループ）	マスター ユニット選定のこのユニットのプライオリティを設定します。

health-check application

クラウド Web セキュリティのアプリケーション健全性チェックをイネーブルにするには、ScanSafe 汎用オプション コンフィギュレーション モードで **health-check application** コマンドを使用します。健全性チェックを削除するか、デフォルト タイムアウトに戻すには、このコマンドの **no** 形式を使用します。

health-check application {[**url** *url_string*] | **timeout** *seconds*}

no health-check application {[**url** *url_string*] | **timeout** *seconds*}

構文の説明

url *url_string*	(任意)アプリケーションをポーリングするときに使用する URL を指定します。URL を指定しない場合は、デフォルトの URL が使用されます。デフォルトの URL は、http://gs.scansafe.net/goldStandard?type=text&size=10 です。 URL は、Cisco クラウド Web セキュリティによって指示された場合にのみ指定します。
timeout *seconds*	ASA が健全性チェック URL の GET リクエストを送信してから応答を待機する時間を指定します。ASA は、タイムアウト後にサーバのポーリングに対する再試行制限まで要求を再試行します。その後、サーバがダウンして、フェールオーバーが開始します。デフォルトは 15 秒で、範囲は 5 ～ 120 秒です。

コマンド デフォルト

健全性チェックは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
scansafe 汎用オプション コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

Cisco Cloud Web Security サービスに登録すると、プライマリ クラウド Web セキュリティ プロキシ サーバとバックアップ プロキシ サーバが割り当てられます。これらのサーバは、アベイラビリティをチェックするために定期的にポーリングされます。ASA がクラウド Web セキュリティ プロキシ サーバに到達することができない場合（SYN/ACK パケットがプロキシ サーバから到着しない場合など）、プロキシ サーバは TCP スリーウェイ ハンドシェイクを介してポーリングされて、アベイラビリティがチェックされます。設定した試行回数（デフォルトは 5）後に、プロキシ サーバが使用不可の場合、サーバは到達不能として宣言され、バックアップ プロキシ サーバがアクティブになります。

クラウド Web セキュリティ アプリケーションの状態をチェックすることで、フェールオーバーをさらに改善することができます。場合によっては、サーバが TCP スリーウェイ ハンドシェイクを完了できても、サーバ上のクラウド Web セキュリティ アプリケーションが正しく機能していないことがあります。アプリケーション健全性チェックを有効にすると、スリーウェイ ハンドシェイクが完了しても、アプリケーション自体が応答しない場合、システムはバックアップ サーバにフェールオーバーできます。これにより、より信頼性の高いフェールオーバー設定が確立されます。この追加のチェックを有効にするには、**health-check application** コマンドを使用します。

ヘルス チェックでは、クラウド Web セキュリティ アプリケーションにテストの URL を使用して GET リクエストが送信されます。設定されているタイムアウト期限とリトライ限度内で応答に失敗すると、サーバはダウンとしてマーキングされ、システムはフェールオーバーを開始します。バックアップ サーバもまた、アクティブ サーバとしてマーキングされる前に、正しく機能していることを確認するためにテストされます。フェールオーバーの後、プライマリ サーバのアプリケーションは、オンラインに戻り再度アクティブ サーバとしてマーキングされるまで 30 秒ごとに再テストされます。

継続ポーリングによってプライマリ サーバが連続する 2 回の再試行回数の期間にアクティブであることが示されると、ASA はバックアップ サーバからプライマリ クラウド Web セキュリティ プロキシ サーバに自動的にフォール バックします。このポーリング間隔を変更するには、**retry-count** コマンドを使用します。

例

次に、プライマリ サーバとバックアップ サーバを設定し、デフォルトの URL とタイムアウトを使用して健全性チェックをイネーブルにする例を示します。健全性チェックをイネーブルにし、デフォルト以外のタイムアウトを設定するには、**health-check application** コマンドを別個に入力する必要があります。

```
scansafe general-options
 server primary ip 10.24.0.62 port 8080
 server backup ip 10.10.0.7 port 8080
 health-check application
 retry-count 7
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

関連コマンド

コマンド	説明
class-map type inspect scansafe	ホワイトリストに記載されたユーザとグループのインスペクション クラス マップを作成します。
default user group	ASA に入ってくるユーザのアイデンティティを ASA が判別できない場合のデフォルトのユーザ名やグループを指定します。
http[s]（パラメータ）	インスペクション ポリシー マップのサービス タイプ（HTTP または HTTPS）を指定します。

コマンド	説明
inspect scansafe	このクラスのトラフィックに対するクラウド Web セキュリティ インスペクションをイネーブルにします。
license	要求の送信元の組織を示すため、ASA がクラウド Web セキュリティ プロキシ サーバに送信する認証キーを設定します。
match user group	ユーザまたはグループをホワイトリストと照合します。
policy-map type inspect scansafe	インスペクション ポリシー マップを作成すると、ルールのために必要なパラメータを設定し、任意でホワイトリストを識別できます。
retry-count	再試行回数値を入力します。この値は、可用性をチェックするために、クラウド Web セキュリティ プロキシ サーバをポーリングする前に ASA が待機する時間です。
scansafe	マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可します。
scansafe general-options	汎用クラウド Web セキュリティ サーバ オプションを設定します。
server {**primary** | **backup**}	プライマリまたはバックアップのクラウド Web セキュリティ プロキシ サーバの完全修飾ドメイン名または IP アドレスを設定します。
show conn scansafe	大文字の Z フラグに示されたようにすべてのクラウド Web セキュリティ接続を表示します。
show scansafe server	サーバが現在のアクティブ サーバ、バックアップ サーバ、または到達不能のいずれであるか、サーバのステータスを表示します。
show scansafe statistics	合計と現在の HTTP 接続を表示します。
user-identity monitor	AD エージェントから指定したユーザまたはグループ情報をダウンロードします。
whitelist	トラフィックのクラスでホワイトリスト アクションを実行します。

health-check auto-rejoin

ヘルス チェック失敗後の自動再結合クラスタ設定をカスタマイズするには、クラスタ グループ コンフィギュレーション モードで **health-check auto-rejoin** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

health-check {**data-interface** | **cluster-interface** | **system**} **auto-rejoin** {**unlimited** | *auto_rejoin_max*} [*auto_rejoin_interval* [*auto_rejoin_interval_variation*]]

no health-check {**data-interface** | **cluster-interface** | **system**} **auto-rejoin** [{**unlimited** | *auto_rejoin_max*} [*auto_rejoin_interval* [*auto_rejoin_interval_variation*]]]

構文の説明

auto_rejoin_interval	(任意)再結合試行の間隔を 2 ～ 60 分の範囲で定義します。デフォルト値は **5** 分です。クラスタへの再結合をユニットが試行する最大合計時間は、最後の失敗から 14,400 分に限られています。
auto_rejoin_interval_variation	(任意)間隔を長くするかを 1 ～ 3 の範囲で定義します。 • **1**:変更なし • **2**:2 x 以前の時間 • **3**:3 x 以前の時間 たとえば、間隔の時間を 5 分に設定し、変分を **2** に設定した場合は、最初の試行は 5 分後、2 回目の試行は 10 分後(2 x 5)、3 階目の試行は 20 分後(2 x 10)という具合になります。デフォルト値は、クラスタ インターフェイスの場合は **1**、データ インターフェイスおよびシステムの場合は **2** です。
auto_rejoin_max	クラスタ再結合時の試行回数を 0 ～ 65535 で定義します。**0** は自動再結合を無効にします。デフォルト値は、クラスタ インターフェイスの場合は **unlimited**、データ インターフェイスおよびシステムの場合は **3** です。
cluster-interface	クラスタ制御リンクの自動再結合の設定を行います。
data-interface	データ インターフェイスの自動再結合の設定を行います。
システム	システムにおける内部エラー時の自動再結合の設定を行います。内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーション ステータスなどがあります。
unlimited	クラスタの再結合の試行回数を、クラスタ インターフェイスのデフォルト値である unlimited に設定します。

コマンド デフォルト

- 失敗したクラスタ制御リンクのクラスタ再結合機能が 5 分おきに無制限に試行されます。
- 失敗したデータインターフェイスのクラスタ自動再結合機能は、5 分後と、2 に設定された増加間隔で合計で 3 回試行されます。
- 内部システム エラーの場合のクラスタ自動再結合機能は、5 分後と、2 に設定された増加間隔で、合計で 3 回試行されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
クラスタ グループ コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.9(2)	**system** キーワードが追加されました。
9.5(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドで、ネットワークの状態に合うように自動再結合オプションをカスタマイズできます。

例

次に、両方のインターフェイス タイプについて 10 回の試行を設定する例を示します。データ インターフェイスについては再結合間隔を 10 分、間隔の延長は 3 倍に設定し、クラスタ制御リンクについては再結合間隔を 7 分、間隔の延長は 2 倍に設定します。

```
ciscoasa(config)# cluster group pod1
ciscoasa(cfg-cluster)# local-unit unit1
ciscoasa(cfg-cluster)# cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
ciscoasa(cfg-cluster)# site-id 1
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 10 10 3
ciscoasa(cfg-cluster)# health-check cluster-interface auto-rejoin 10 7 2
ciscoasa(cfg-cluster)# priority 1
ciscoasa(cfg-cluster)# key chuntheunavoidable
ciscoasa(cfg-cluster)# enable noconfirm
```

関連コマンド

コマンド	説明
clacp system-mac	スパンド EtherChannel を使用するときは、ASA は cLACP を使用してネイバー スイッチとの間で EtherChannel のネゴシエーションを行います。
cluster group	クラスタに名前を付け、クラスタ コンフィギュレーション モードを開始します。
cluster-interface	クラスタ制御リンク インターフェイスを指定します。
cluster interface-mode	クラスタ インターフェイス モードを設定します。
conn-rebalance	接続の再分散をイネーブルにします。
console-replicate	スレーブ ユニットからマスター ユニットへのコンソール複製をイネーブルにします。
enable（クラスタ グループ）	クラスタリングをイネーブルにします。

コマンド	説明
health-check	クラスタのヘルス チェック機能(ユニットのヘルス モニタリングおよびインターフェイスのヘルス モニタリングを含む)をイネーブルにします。
key	クラスタ制御リンクの制御トラフィックの認証キーを設定します。
local-unit	クラスタ メンバーに名前を付けます。
mac-address site-id	各サイトのサイト固有の MAC アドレスを設定します。
mtu cluster-interface	クラスタ制御リンク インターフェイスの最大伝送ユニットを指定します。
priority(クラスタ グループ)	マスター ユニット選定のこのユニットのプライオリティを設定します。
site-id	サイト ID を設定して、サイト間クラスタリングでの MAC アドレスのフラッピングを回避します。

hello-interval

インターフェイス上で送信される EIGRP hello パケット間の間隔を指定するには、インターフェイス コンフィギュレーション モードで **hello-interval** コマンドを使用します。hello 間隔をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

hello-interval eigrp *as-number seconds*

no hello-interval eigrp *as-number seconds*

構文の説明

as-number	EIGRP ルーティング プロセスの自律システム番号を指定します。
seconds	インターフェイス上で送信される hello パケット間の間隔を指定します。有効な値は、1 ～ 65535 秒です。

デフォルト

デフォルトは 5 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

hello 間隔を小さくするほど、トポロジの変更が速く検出されますが、より多くのルーティング トラフィックが発生します。この値は、特定のネットワーク上のすべてのルータおよびアクセス サーバで同じにする必要があります。

例

次の例では、EIGRP hello 間隔を 10 秒に、ホールド タイムを 30 秒に設定します。

```
ciscoasa(config-if)# hello-interval eigrp 100 10
ciscoasa(config-if)# hold-time eigrp 100 30
```

関連コマンド

コマンド	説明
hold-time	hello パケットでアドバタイズされる EIGRP ホールド タイムを設定します。

hello padding multi-point

ルータ レベルで IS-IS hello パディングを再度イネーブルにするには、ルータ ISIS コンフィギュレーション モードで、**hello padding multi-point** コマンドを入力します。IS-IS hello パディングをディセーブルにするには、このコマンドの **no** 形式を使用します。

hell padding multi-point

no hello padding multi-point

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

hello パディングは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、最大伝送ユニット（MTU）サイズになるまで IS-IS hello をパディングできます。IS-IS hello をフル MTU に埋め込む利点は、大きなフレームに関連した送信問題によるエラーや隣接インターフェイスの MTU 不一致によるエラーを検出できることです。

両方のインターフェイスの MTU が同じである場合やトランスレーショナル ブリッジングの場合には、ネットワーク帯域幅の無駄を省くため、hello パディングをディセーブルにできます。hello パディングがディセーブルになっても、ASA は、MTU 不一致検出の利点を維持するために、最初の 5 回の IS-IS hello を最大 MTU にパディングして送信します。

IS-IS ルーティング プロセスに関して、ASA 上のすべてのインターフェイスの hello パディングをディセーブルにするには、ルータ コンフィギュレーション モードで **no hello padding** コマンドを入力します。特定のインターフェイスの hello パディングを選択的にディセーブルにするには、インターフェイス コンフィギュレーション モードで **no isis hello padding**コマンドを入力します。

例

次に、**no hello padding** コマンドを使用して、ルータ レベルの hello パディングをオフにする例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# hello padding multi-point
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。

コマンド	説明
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト(TLV)を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

help

指定するコマンドのヘルプ情報を表示するには、ユーザ EXEC モードで **help** コマンドを使用します。

help {*command* | **?**}

構文の説明

?	現在の特権レベルおよびモードで使用可能なすべてのコマンドを表示します。
command	CLI ヘルプを表示するコマンドを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

help コマンドを使用すると、すべてのコマンドのヘルプ情報が表示されます。**help** コマンドの後にコマンド名を入力することによって、個々のコマンドのヘルプを参照できます。コマンド名を指定せず、その代わりに **?** と入力した場合、現在の特権レベルおよびモードで使用可能なすべてのコマンドを表示します。

pager コマンドがイネーブルの場合、24 行表示されると、リスト表示が一時停止して次のプロンプトが表示されます。

```
<--- More --->
```

More プロンプトでは、次のように、UNIX の **more** コマンドに類似した構文が使用されます。

- 次のテキスト画面を表示するには、**Space** バーを押します。
- 次の行を表示するには、**Enter** キーを押します。
- コマンドラインに戻るには、**q** キーを押します。

例

次に、**rename** コマンドのヘルプを表示する例を示します。

```
ciscoasa# help rename

USAGE:

        rename /noconfirm [{disk0:|disk1:|flash:}] <source path> [{disk0:|disk1:
|flash:}] <destination path>

DESCRIPTION:

rename          Rename a file

SYNTAX:

/noconfirm                      No confirmation
{disk0:|disk1:|flash:} Optional parameter that specifies the filesystem
<source path>           Source file path
<destination path>      Destination file path

ciscoasa#
```

次に、コマンド名と疑問符を入力して、ヘルプを表示する例を示します。

```
ciscoasa(config)# enable ?
usage: enable password <pwd> [encrypted]
```

コマンド プロンプトで **?** を入力すると、主要コマンド（**show**、**no**、または **clear** コマンド以外）に関するヘルプが表示されます。

```
ciscoasa(config)# ?
aaa             Enable, disable, or view TACACS+ or RADIUS
                user authentication, authorization and accounting
…
```

関連コマンド

コマンド	説明
show version	オペレーティング システム ソフトウェアに関する情報を表示します。

hidden-parameter

ASA が SSO 認証のために認証 Web サーバに送信する HTTP POST 要求の非表示パラメータを指定するには、AAA サーバ ホスト コンフィギュレーション モードで **hidden-parameter** コマンドを使用します。実行コンフィギュレーションからすべての非表示パラメータを削除するには、このコマンドの **no** 形式を使用します。

hidden-parameter *string*

no hidden-parameter

(注) HTTP プロトコルを使用して SSO を正しく設定するには、認証と HTTP プロトコル交換についての詳しい実務知識が必要です。

構文の説明

string	フォームに組み込まれて SSO サーバに送信される非表示パラメータ。複数行に入力できます。各行の最大文字数は 255 です。すべての行をあわせた（非表示パラメータ全体の）最大文字数は 2048 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

これは HTTP フォームのコマンドを使用した SSO です。

ASA の WebVPN サーバは、認証 Web サーバに SSO 認証要求を送信するときに HTTP POST 要求を使用します。その要求では、ユーザには表示されない SSO HTML フォームの特定の非表示パラメータ（ユーザ名およびパスワード以外）が必要になることがあります。Web サーバから受信したフォームに対して HTTP ヘッダー アナライザを使用することで、Web サーバが POST 要求で想定している非表示パラメータを検出できます。

hidden-parameter コマンドを使用すると、Web サーバが認証 POST 要求で必要としている非表示パラメータを指定できます。ヘッダー アナライザを使用する場合は、エンコーディング済みの URL パラメータを含む非表示パラメータ文字列全体をコピーして貼り付けることができます。

入力を簡単にするために、複数の連続行で非表示パラメータを入力できます。ASA では、その複数行を連結して単一の非表示パラメータにします。非表示パラメータ 1 行ごとの最大文字数は 255 文字ですが、各行にはそれより少ない文字しか入力できません。

(注) 文字列に疑問符を含める場合は、疑問符の前に **Ctrl+V** のエスケープ シーケンスを使用する必要があります。

例

次に、& で区切られた 4 つのフォーム エントリとその値で構成される非表示パラメータの例を示します。POST 要求から抜き出された 4 つのエントリおよびその値は、次のとおりです。

- SMENC、値は ISO-8859-1
- SMLOCALE、値は US-EN
- ターゲット、値は https%3A%2F%2Ftools.cisco.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG
- smauthreason、値は 0

SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Ftools.cisco.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG&smauthreason=0

```
ciscoasa(config)# aaa-server testgrp1 host example.com
ciscoasa(config-aaa-server-host)# hidden-parameter SMENC=ISO-8859-1&SMLOCALE=US-EN&targe
ciscoasa(config-aaa-server-host)# hidden-parameter t=https%3A%2F%2Ftools.cisco.com%2Femc
ciscoasa(config-aaa-server-host)# hidden-parameter o%2Fappdir%2FAreaRoot.do%3FEMCOPageCo
ciscoasa(config-aaa-server-host)# hidden-parameter de%3DENG&smauthreason=0
ciscoasa(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
action-uri	SSO 認証用のユーザ名およびパスワードを受信するための Web サーバ URI を指定します。
auth-cookie-name	認証クッキーの名前を指定します。
password-parameter	SSO 認証用にユーザ パスワードを送信する必要がある HTTP POST 要求パラメータの名前を指定します。
start-url	プリログイン クッキーを取得する URL を指定します。
user-parameter	SSO 認証用にユーザ名を送信する必要がある HTTP POST 要求のパラメータの名前を指定します。

hidden-shares

CIFS ファイルの非表示共有の可視性を制御するには、グループ webvpn コンフィギュレーション モードで **hidden-shares** コマンドを使用します。非表示共有オプションをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

hidden-shares {**none** | **visible**}

[no] hidden-shares {**none** | **visible**}

構文の説明

none	設定済みの非表示共有の表示およびアクセスをユーザが実行できないことを指定します。
visible	非表示共有を表示して、ユーザがアクセスできるようにします。

デフォルト

このコマンドのデフォルト動作は none です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ webvpn コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

非表示共有は、共有名の末尾のドル記号($)で識別されます。たとえば、ドライブ C は C$ として共有されます。非表示共有では、共有フォルダは表示されず、ユーザはこれらの非表示リソースを参照またはアクセスすることを禁止されます。

hidden-shares コマンドの **no** 形式を使用すると、コンフィギュレーションからオプションが削除され、グループ ポリシー属性として非表示共有がディセーブルになります。

例

次に、GroupPolicy2 に関連する WebVPN CIFS 非表示共有を可視にする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-group-policy)# group-policy GroupPolicy2 attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# hidden-shares visible
ciscoasa(config-group-webvpn)#
```

関連コマンド

コマンド	説明
debug webvpn cifs	CIFS に関するデバッグ メッセージを表示します。
group-policy attributes	グループ ポリシー コンフィギュレーション モードを開始します。このモードでは、指定したグループ ポリシーの属性と値を設定したり、webvpn コンフィギュレーション モードを開始して、グループの WebVPN 属性を設定したりできます。
url-list	WebVPN ユーザがアクセスする URL のセットを設定します。
url-list	特定のユーザまたはグループ ポリシーに、WebVPN サーバおよび URL のリストを適用します。

hold-time

ASA が EIGRP hello パケットでアドバタイズするホールド タイムを指定するには、インターフェイス コンフィギュレーション モードで **hold-time** コマンドを使用します。hello 間隔をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

hold-time eigrp *as-number seconds*

no hold-time eigrp *as-number seconds*

構文の説明

as-number	EIGRP ルーティング プロセスの自律システム番号です。
seconds	ホールド タイムを秒数で指定します。有効な値は、1 ～ 65535 秒です。

デフォルト

デフォルトは 15 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

この値は、ASA によって EIGRP hello パケットでアドバタイズされます。そのインターフェイスの EIGRP ネイバーは、この値を使用してASAの可用性を判断します。アドバタイズされたホールド タイム中に ASA から hello パケットを受信しなかった場合、EIGRP ネイバーは ASA が使用不可であると見なします。

非常に混雑した大規模ネットワークでは、一部のルータおよびアクセス サーバが、デフォルト ホールド タイム内にネイバーから hello パケットを受信できない可能性があります。この場合、ホールド タイムを増やすこともできます。

ホールド タイムは、少なくとも hello 間隔の 3 倍にすることを推奨します。指定したホールド タイム内に ASA で hello パケットを受信しなかった場合、このネイバーを通過するルートは使用不可であると見なされます。

ホールド タイムを増やすと、ネットワーク全体のルート収束が遅くなります。

例

次の例では、EIGRP hello 間隔を 10 秒に、ホールド タイムを 30 秒に設定します。

```
ciscoasa(config-if)# hello-interval eigrp 100 10
ciscoasa(config-if)# hold-time eigrp 100 30
```

関連コマンド

コマンド	説明
hello-interval	インターフェイス上で送信される EIGRP hello パケット間の間隔を指定します。

homepage

該当 WebVPN ユーザまたはグループ ポリシーに対して、ログイン時に表示される Web ページの URL を指定するには、webvpn コンフィギュレーション モードで **homepage** コマンドを使用します。設定済みのホームページ（**homepage none** コマンドを発行して作成されたヌル値を含む）を削除するには、このコマンドの **no** 形式を使用します。

homepage {**value** *url-string* | **none**}

no homepage

構文の説明

none	WebVPN ホームページがないことを指定します。ヌル値を設定して、ホームページを拒否します。ホームページを継承しないようにします。
value *url-string*	ホームページの URL を指定します。http:// または https:// のいずれかで始まるストリングにする必要があります。

デフォルト

デフォルトのホームページはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

グループ ポリシーに関連付けられているユーザのホームページ URL を指定するには、このコマンドで URL 文字列値を入力します。デフォルト グローバル ポリシーからホームページを継承するには、このコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。ホームページの継承を禁止するには、**homepage none** コマンドを使用します。

クライアントレス ユーザには、認証の成功後すぐにこのページが表示されます。AnyConnect は、VPN 接続が正常に確立されると、この URL に対してデフォルトの Web ブラウザを起動します。Linux プラットフォームでは、AnyConnect が現在このコマンドをサポートしていないため、コマンドは無視されます。

例

次に、FirstGroup という名前のグループ ポリシーのホームページとして www.example.com を指定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# homepage value http://www.example.com
```

関連コマンド

コマンド	説明
webvpn	webvpn コンフィギュレーション モードを開始して、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。

homepage use-smart-tunnel

クライアントレス SSL VPN の使用時に、グループ ポリシーのホームページがスマート トンネル機能を使用できるようにするには、グループ ポリシー webvpn コンフィギュレーション モードで **homepage use-smart-tunnel** コマンドを使用します。

homepage {**value** *url-string* | **none**}

homepage use-smart-tunnel

構文の説明

none	WebVPN ホームページがないことを指定します。ヌル値を設定して、ホームページを拒否します。ホームページを継承しないようにします。
value *url-string*	ホームページの URL を指定します。http:// または https:// のいずれかで始まるストリングにする必要があります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

使用上のガイドライン

ブラウザ セッションをモニタし、スマート トンネルが WebVPN 接続中に開始されたことを確認するために HTTP キャプチャ ツールを使用できます。ブラウザ キャプチャの表示内容により、要求が制限されることなく Web ページに転送されるかどうか、またスマート トンネルが使用されているかどうかが判断されます。https://172.16.16.23/+CSCOE+portal.html などが表示された場合、*+CSCO** はコンテンツが ASA によって制限されていることを示しています。スマート トンネルが開始されると、+CSCO* がない特定の URL に対する **http get** コマンドが表示されます（GET 200 html http://mypage.example.com など）。

例

ベンダー V がパートナー P に自社内部の在庫サーバ ページへのクライアントレス アクセスを提供する場合を考えます。この場合、ベンダー V の管理者は、次の事項を決定する必要があります。

- ユーザは、クライアントレス SSL VPN にログインした後、クライアントレス ポータルを経由するかどうかに関係なく、在庫ページアクセスできますか。
- ページに Microsoft Silverlight コンポーネントが含まれていますが、アクセスするのにスマート トンネルは適切な選択肢ですか。

- ブラウザがトンネリングされると、すべてのトンネル ポリシーによりすべてのブラウザ トラフィックがベンダー V の ASA を経由するように強制され、パートナー P のユーザは内部リソースにアクセスできなくなりますが、すべてをトンネリングするポリシーは適切ですか。

在庫ページが inv.example.com（10.0.0.0）でホストされると仮定すると、次の例では、1 つのホストだけを含むトンネル ポリシーが作成されます。

```
ciscoasa(config-webvpn)# smart-tunnel network inventory ip 10.0.0.0
ciscoasa(config-webvpn)# smart-tunnel network inventory host inv.example.com
```

次に、トンネル指定トンネル ポリシーをパートナーのグループ ポリシーに適用する例を示します。

```
ciscoasa(config-group-webvpn)# smart-tunnel tunnel-policy tunnelspecified inventory
```

次に、グループ ポリシーのホーム ページを指定し、そこでスマート トンネルをイネーブルにする例を示します。

```
ciscoasa(config-group-webvpn)# homepage value http://inv.example.com
ciscoasa(config-group-webvpn)# homepage use-smart-tunnel
```

host(ネットワーク オブジェクト)

ネットワーク オブジェクトのホストを設定するには、ネットワーク オブジェクト コンフィギュレーション モードで **host** コマンドを使用します。ホストをオブジェクトから削除するには、このコマンドの **no** 形式を使用します。

host *ip_address*

no host *ip_address*

構文の説明

ip_address	オブジェクトのホスト IP アドレス(IPv4 または IPv6)を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
オブジェクト コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

使用上のガイドライン

既存のネットワーク オブジェクトを異なる IP アドレスを使用して設定すると、新しいコンフィギュレーションが既存のコンフィギュレーションに置き換わります。

例

次に、ホスト ネットワーク オブジェクトを作成する例を示します。

```
ciscoasa (config)# object network OBJECT1
ciscoasa (config-network-object)# host 10.1.1.1
```

関連コマンド

コマンド	説明
clear configure object	作成されたすべてのオブジェクトをクリアします。
nat	ネットワーク オブジェクトの NAT をイネーブルにします。
object network	ネットワーク オブジェクトを作成します。

コマンド	説明
object-group network	ネットワーク オブジェクト グループを作成します。
show running-config object network	ネットワーク オブジェクト コンフィギュレーションを表示します。

host(パラメータ)

RADIUS アカウンティングを使用して対話するホストを指定するには、RADIUS アカウンティング パラメータ コンフィギュレーション モードで **host** コマンドを使用します。このモードにアクセスするには、ポリシー マップ タイプ インスペクションの RADIUS アカウンティング サブモードで **parameters** コマンドを使用します。指定したホストをディセーブルにするには、このコマンドの **no** 形式を使用します。

host *address* [**key** *secret*]

no host *address* [**key** *secret*]

構文の説明

ホスト	RADIUS アカウンティング メッセージを送信する単一のエンドポイントを指定します。
address	RADIUS アカウンティング メッセージを送信するクライアントまたはサーバの IP アドレス。
key	アカウンティング メッセージの無償コピーを送信するエンドポイントの秘密キーを指定するオプションのキーワード。
secret	メッセージの検証に使用されるアカウンティング メッセージを送信するエンドポイントの共有秘密キー。最大 128 の英数字を使用できます。

デフォルト

no オプションはデフォルトでディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
RADIUS アカウンティング パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、インスタンスを複数設定できます。

例

次に、RADIUS アカウンティングを使用するホストを指定する例を示します。

```
ciscoasa(config)# policy-map type inspect radius-accounting ra
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# host 209.165.202.128 key cisco123
```

関連コマンド

コマンド	説明
inspect radius-accounting	RADIUS アカウンティングのインスペクションを設定します。
パラメータ	インスペクション ポリシー マップのパラメータを設定します。

hostname

ASA のホスト名を設定するには、グローバル コンフィギュレーション モードで **hostname** コマンドを使用します。デフォルトのホスト名に戻すには、このコマンドの **no** 形式を使用します。

hostname *name*

no hostname [*name*]

構文の説明

name	ホスト名を最大 63 文字で指定します。ホスト名はアルファベットまたは数字で開始および終了する必要があり、間の文字にはアルファベット、数字、またはハイフンのみを使用する必要があります。

デフォルト

デフォルトのホスト名はプラットフォームによって異なります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	英数字以外の文字（ハイフンを除く）は使用できなくなりました。

使用上のガイドライン

ホスト名は、コマンドライン プロンプトとして表示され、複数のデバイスへのセッションを確立している場合に、コマンドを入力している場所を把握するのに役立ちます。マルチ コンテキスト モードでは、システム実行スペースに設定したホスト名がすべてのコンテキストのコマンドライン プロンプトに表示されます。

コンテキスト内に任意で設定したホスト名は、コマンドラインには表示されませんが、**banner** コマンドの **$(hostname)** トークンでは使用できます。

例

次に、ホスト名を firewall1 に設定する例を示します。

```
ciscoasa(config)# hostname firewall1
firewall1(config)#
```

関連コマンド

コマンド	説明
バナー	ログイン バナー、Message-of-The-Day バナー、またはイネーブル バナーを設定します。
domain-name	デフォルトのドメイン名を設定します。

hostname dynamic

ASA で IS-IS ダイナミック ホスト名機能をイネーブルにするには、ルータ ISIS コンフィギュレーション モードで **hostname dynamic** コマンドを使用します。ダイナミック ホスト名機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

hostname dynamic

no hostname dynamic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、ダイナミック ホスト名はイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ルータ isis コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

IS-IS ルーティング ドメインでは、各 ASA はシステム ID により表されます。システム ID は、IS-IS ASA ごと構成されている Network Entity Title（NET）の一部です。たとえば、NET 49.0001.0023.0003.000a.00 が設定されている ASA のシステム ID が 0023.0003.000a であるとします。ネットワーク管理者にとって、ルータでのメンテナンスやトラブルシューティングの間、ルータ名とシステム ID の対応を覚えているのは難しいことです。**show isis hostname** コマンドを入力すると、システム ID に対するルータ名のマッピング テーブルに含まれるエントリが表示されます。

ダイナミック ホスト名メカニズムはリンクステート プロトコル（LSP）フラッディングを使用して、ネットワーク全体にルータ名に対するシステム ID のマッピング情報を配布します。ネットワーク上の ASA はすべて、このシステム ID に対するルータ名のマッピング情報をルーティング テーブルにインストールしようと試みます。

ネットワーク上で、ダイナミック名のタイプ、長さ、値（TLV）をアドバタイズしている ASA が突然アドバタイズメントを停止した場合、最後に受信されたマッピング情報が最大 1 時間、ダイナミック ホスト マッピング テーブルに残るため、ネットワークに問題が発生している間、ネットワーク管理者はマッピング テーブル内のエントリを表示できます。**show isis hostname** コマンドを入力すると、マッピング テーブルに含まれるエントリが表示されます。

例

次に、ホスト名を firewall1 に設定する例を示します。

```
ciscoasa(config)# hostname firewall1
firewall1(config)#
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。

コマンド	説明
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト(TLV)を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

hostscan enable

クライアントレス SSL VPN リモート アクセスまたは AnyConnect クライアントを使用したリモート アクセスに対してホストスキャンをイネーブルにするには、webvpn コンフィギュレーション モードで **hostscan enable** コマンドを使用します。ホストスキャンをディセーブルにするには、このコマンドの **no** 形式を使用します。

hostscan enable

no hostscan enable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

ホストスキャンは、1 つの例外を除いて、ASA へのすべてのリモート アクセス接続試行に対してグローバルにイネーブルまたはディセーブルに設定されます。

hostscan enable コマンドは、次の処理を実行します。

1. 以前の **hostscan image** *path* コマンドによって実行されたチェックを補足する有効性チェックを提供します。
2. sdesktop フォルダがまだ存在しない場合は、disk0: 上に作成します。
3. data.xml（ホストスキャン コンフィギュレーション）ファイルが sdesktop フォルダにまだ存在しない場合は、追加します。
4. フラッシュ デバイスの data.xml を実行コンフィギュレーションにロードします。
5. ホストスキャンをイネーブルにします。

（注）

- **show webvpn hostscan** コマンドを入力して、ホストスキャンがイネーブルであるかどうかを確認できます。
- **hostscan enable** コマンドを入力する前に、実行コンフィギュレーション内に **hostscan image** *path* コマンドが存在する必要があります。
- **no hostscan enable** コマンドは、実行コンフィギュレーションでホストスキャンをディセーブルにします。ホストスキャンがディセーブルの場合、管理者は Hostscan Manager にアクセスできず、リモート ユーザはホストスキャンを使用できません。
- data.xml ファイルを転送または置換する場合は、ホストスキャンをいったんディセーブルにしてからイネーブルにして、このファイルを実行コンフィギュレーションにロードします。
- ホストスキャンは、ASA へのすべてのリモート アクセス接続試行に対してグローバルにイネーブルまたはディセーブルに設定されます。個別の接続プロファイルやグループ ポリシーに対してホストスキャンをイネーブルまたはディセーブルに設定することはできません。

  例外: クライアントレス SSL VPN 接続の接続プロファイルは、コンピュータがグループ URL を使用して ASA への接続を試行し、ホストスキャンがグローバルにイネーブルの場合、ホストスキャンがクライアント コンピュータで実行されないように設定できます。次に例を示します。

```
ciscoasa(config)# tunnel-group group-name webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-url https://www.url-string.com
ciscoasa(config-tunnel-webvpn)# without-Hostscan
```

例

次に、ホストスキャン イメージのステータスを表示し、ホストスキャン イメージをイネーブルにするためのコマンドを示します。

```
ciscoasa(config-webvpn)# show webvpn hostscan
Hostscan is not enabled.
ciscoasa(config-webvpn)# hostscan enable
ciscoasa(config-webvpn)# show webvpn hostscan
Hostscan version 4.1.0.25 is currently installed and enabled.
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
hostscan image	コマンドに指定されたホストスキャン イメージを、パスに指定されたフラッシュ ドライブから実行コンフィギュレーションにコピーします。
show webvpn hostscan	イネーブルの場合、ホストスキャンのバージョンを識別します。ディセーブルの場合、CLI に「Secure Desktop is not enabled.」と表示されます。
without-Hostscan	クライアントレス SSL VPN セッションの接続プロファイルを、コンピュータがグループ URL を使用して ASA への接続を試行し、ホストスキャンがグローバルにイネーブルの場合、ホストスキャンがクライアント コンピュータで実行されないように設定します。

hostscan image

シスコのホスト スキャン配布パッケージをインストールまたはアップグレードし、実行コンフィギュレーションに追加するには、webvpn コンフィギュレーション モードで **hostscan image** コマンドを使用します。ホスト スキャン配布パッケージを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

hostscan image *path*

no hostscan image *path*

構文の説明

path	シスコのホスト スキャン パッケージのパスおよびファイル名を 255 文字以内で指定します。 ホスト スキャン パッケージには、ファイル名の命名規則 hostscan-*version*.pkg を持つスタンドアロンのホスト スキャン パッケージを指定するか、または、Cisco.com からダウンロードでき、ファイル名の命名規則 anyconnect-win-*version*-k9.pkg を持つ完全な AnyConnect セキュア モビリティ クライアント パッケージを指定できます。顧客が AnyConnect セキュア モビリティ クライアントを指定すると、ASA は AnyConnect パッケージからホスト スキャン パッケージを取得してインストールします。 ホスト スキャン パッケージには、ホスト スキャン ソフトウェアおよびホスト スキャン ライブラリとサポート チャートが含まれています。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

現在インストールされ、イネーブルになっているホスト スキャン イメージのバージョンを確認するには、**show webvpn hostscan** コマンドを入力します。

hostscan image コマンドを使用してホスト スキャンをインストールした後に、**enable** コマンドを使用してイメージをイネーブルにします。

次回の ASA のリブート時にホスト スキャン イメージを確実に使用できるように、**write memory** コマンドを入力して実行コンフィギュレーションを保存します。

例

次に、シスコのホスト スキャン パッケージをインストールし、イネーブルにして、表示およびフラッシュ ドライブへの設定の保存を行うコマンドを示します。

```
ciscoasa> en
Password: ******
ciscoasa# config t
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# show webvpn hostscan
Hostscan is not enabled.
ciscoasa(config-webvpn)# hostscan image disk0:/hostscan_3.0.0333-k9.pkg
ciscoasa(config-webvpn)# hostscan enable
ciscoasa(config-webvpn)# show webvpn hostscan
Hostscan version 3.0.0333 is currently installed and enabled
ciscoasa(config-webvpn)# write memory
Building configuration...
Cryptochecksum: 2e7126f7 71214c6b 6f3b28c5 72fa0a1e

22067 bytes copied in 3.460 secs (7355 bytes/sec)
[OK]
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
show webvpn hostscan	シスコのホスト スキャンがイネーブルである場合、そのバージョンを示します。ディセーブルの場合、CLI に「Hostscan is not enabled..」と表示されます。
hostscan enable	管理およびリモート ユーザ アクセスのホストスキャンをイネーブルにします。

hpm topn enable

ASA 経由で接続している上位ホストに関する ASDM のリアルタイム レポートをイネーブルにするには、グローバル コンフィギュレーション モードで **hpm topn enable** コマンドを使用します。ホストのレポート作成をディセーブルにするには、このコマンドの **no** 形式を使用します。

hpm topn enable

no hpm topn enable

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

使用上のガイドライン

システム パフォーマンスを最大にする場合は、このコマンドをディセーブルにすることを推奨します。このコマンドにより、[ASDM Home] > [Firewall Dashboard] > [Top 200 Hosts] ペインに情報が入力されます。

例

次の例では、上位ホストのレポート作成をイネーブルします。

```
ciscoasa(config)# hpm topn enable
```

関連コマンド

コマンド	説明
clear configure hpm	HPM コンフィギュレーションをクリアします。
show running-config hpm	HPM コンフィギュレーションを表示します。

hsi

H.323 プロトコル インスペクションの HSI グループに HSI を追加するには、HSI グループ コンフィギュレーション モードで **hsi** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

hsi *ip_address*

no hsi *ip_address*

構文の説明

ip_address	追加するホストの IP アドレス。HSI グループごとに最大で 5 つの HSI を設定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
HSI グループ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、H.323 インスペクション ポリシー マップで HSI を HSI グループに追加する例を示します。

```
ciscoasa(config-pmap-p)# hsi-group 10
ciscoasa(config-h225-map-hsi-grp)# hsi 10.10.15.11
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
endpoint	HSI グループにエンドポイントを追加します。
hsi-group	HSI グループを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

hsi-group

H.323 プロトコル インスペクション用の HSI グループを定義して、HSI コンフィギュレーション モードを開始するには、パラメータ コンフィギュレーション モードで **hsi-group** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

hsi-group *group_id*

no hsi-group *group_id*

構文の説明

group_id	HSI グループの ID 番号（0 ～ 2147483647）。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、H.323 インスペクション ポリシー マップで HSI グループを設定する例を示します。

```
ciscoasa(config-pmap-p)# hsi-group 10
ciscoasa(config-h225-map-hsi-grp)# hsi 10.10.15.11
ciscoasa(config-h225-map-hsi-grp)# endpoint 10.3.6.1 inside
ciscoasa(config-h225-map-hsi-grp)# endpoint 10.10.25.5 outside
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
endpoint	HSI グループにエンドポイントを追加します。
hsi	HSI を HSI グループに追加します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

hsts enable

ブラウザやその他のユーザ エージェントへの HTTP Strict Transport Security ヘッダーの送信を設定するには、webvpn コンフィギュレーション モードで **hsts enable** コマンドを使用します。コンフィギュレーションからこの設定を削除するには、このコマンドの no 形式を使用します。このコマンドが有効になると、非セキュアな方法でアクセスが試行された場合、準拠しているブラウザおよびユーザ エージェントは HTTPS に切り替えられます。

hsts enable

no hsts enable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、Strict Transport Security ヘッダーは使用されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.8(2)	このコマンドが導入されました。

使用上のガイドライン

HTTP Strict Transport Security（HSTS）は、Web セキュリティ ポリシーのメカニズムであり、プロトコル ダウングレード攻撃および Cookie ハイジャックから Web サイトを保護するのに役立ちます。これにより Web サーバは、Web ブラウザ（またはその他の準拠しているユーザ エージェント）が Web サーバと通信するにはセキュア HTTPS 接続を使用する必要があり、非セキュアな HTTP プロトコルを使用して通信することはできないことを宣言できます。

有効にすると、デフォルトのタイムアウト値である 10,886,400 秒（18 週）が使用されます。これは、**hsts max-age** コマンドを使用して変更できます。

例

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# hsts enable
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
hsts max-age	ASA が HSTS ホストとして扱われ、セキュアな方法でアクセスされる期間の最大値です。
show running-config webvpn hsts	SSL VPN の実行コンフィギュレーションを、HTTP 設定も含めて表示します。

hsts max-age

ブラウザやその他のユーザ エージェントへの HTTP Strict Transport Security ヘッダーの送信が（**hsts enable** コマンドを使用して）設定されている場合、**hsts max-age** を使用すると、ASA が HSTS ホストとして扱われ、セキュアな方法でアクセスされる期間の最大値を設定できます。

hsts max-age *max-value-in-seconds*

構文の説明

max-value-in-seconds	HSTS が有効になる期間（秒数）。範囲は <0 ～ 31536000> 秒です。

デフォルト

デフォルトでは、最大値は 10,886,400（18 週）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.8(2)	このコマンドが導入されました。

使用上のガイドライン

HTTP Strict Transport Security（HSTS）は、Web セキュリティ ポリシーのメカニズムであり、プロトコル ダウングレード攻撃および Cokie ハイジャックから Web サイトを保護するのに役立ちます。これにより Web サーバは、Web ブラウザ（またはその他の準拠しているユーザ エージェント）が Web サーバと通信するにはセキュア HTTPS 接続を使用する必要があり、非セキュアな HTTP プロトコルを使用して通信することはできないことを宣言できます。

有効にすると、デフォルトのタイムアウト値である 10,886,400 秒（18 週）が使用されます。このコマンドは、タイムアウトを変更します。

例

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# hsts max-age 31536000
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
hsts enable	HSTS ヘッダーの送信を有効にします。
show running-config webvpn hsts	SSL VPN の実行コンフィギュレーションを、HTTP 設定も含めて表示します。

html-content-filter

このユーザまたはグループ ポリシーに対して WebVPN セッションの Java、ActiveX、イメージ、スクリプト、およびクッキーをフィルタリングするには、webvpn コンフィギュレーション モードで **html-content-filter** コマンドを使用します。コンテンツ フィルタを削除するには、このコマンドの **no** 形式を使用します。

html-content-filter {**java** | **images** | **scripts** | **cookies** | **none**}

no html-content-filter [**java** | **images** | **scripts** | **cookies** | **none**]

構文の説明

cookies	イメージからクッキーを削除して、限定的な広告フィルタリングとプライバシーを提供します。
イメージ	イメージへの参照を削除します(<IMG> タグを削除します)。
java	Java および ActiveX への参照を削除します(<EMBED>、<APPLET>、および <OBJECT> タグを削除します)。
none	フィルタリングを行わないことを指定します。ヌル値を設定して、フィルタリングを拒否します。フィルタリング値を継承しないようにします。
scripts	スクリプトへの参照を削除します(<SCRIPT> タグを削除します)。

デフォルト

フィルタリングは行われません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

すべてのコンテンツ フィルタ(**html-content-filter none** コマンドを発行して作成されたヌル値を含む)を削除するには、このコマンドの **no** 形式を引数なしで使用します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。HTML コンテンツ フィルタを継承しないようにするには、**html-content-filter none** コマンドを使用します。

次回このコマンドを使用すると、前回までの設定が上書きされます。

例

次に、FirstGroup という名前のグループ ポリシーに対して Java と ActiveX、クッキー、およびイメージのフィルタリングを設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# html-content-filter java cookies images
```

関連コマンド

コマンド	説明
webvpn	webvpn コンフィギュレーション モードを開始して、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。グローバル コンフィギュレーション モードを開始して WebVPN のグローバル設定を設定できるようにします。

http（グローバル）

ASA 内部の HTTP サーバにアクセスできるホストを指定するには、グローバル コンフィギュレーション モードで **http** コマンドを使用します。1 つ以上のホストを削除するには、このコマンドの **no** 形式を使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を引数なしで使用します。

http *ip_address subnet_mask interface_name*

no http

構文の説明

interface_name	ホストが HTTP サーバにアクセスするために通過する ASA のインターフェイスの名前を指定します。物理インターフェイスまたは仮想インターフェイスを指定できます。BVI インターフェイスが指定されている場合、そのインターフェイスに対し **management-access** を設定する必要があります。
ip_address	HTTP サーバにアクセスできるホストの IP アドレスを指定します。
subnet_mask	HTTP サーバにアクセスできるホストのサブネット マスクを指定します。

デフォルト

HTTP サーバにアクセスできるホストはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.7(1)	直接接続された HTTP 管理ステーションがある場合は、ASA とホストで /31 サブネットを使用して、ポイントツーポイント接続を作成できます。
9.9.(2)	仮想インターフェイスが指定可能になりました。

例

次に、IP アドレス 10.10.99.1 とサブネット マスク 255.255.255.255 を持つホストが、外部インターフェイス経由で HTTP サーバにアクセスできるようにする例を示します。

```
ciscoasa(config)# http 10.10.99.1 255.255.255.255 outside
```

次に、任意のホストが、外部インターフェイス経由で HTTP サーバにアクセスできるようにする例を示します。

```
ciscoasa(config)# http 0.0.0.0 0.0.0.0 outside
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。HTTP サーバをディセーブルにし、HTTP サーバにアクセスできるホストを削除します。
http authentication-certificate	ASA への HTTPS 接続を確立するユーザの証明書による認証を要求します。
http redirect	ASA が HTTP 接続を HTTPS にリダイレクトすることを指定します。
http server enable	HTTP サーバをイネーブルにします。
show running-config http	HTTP サーバにアクセスできるホストを表示し、さらに HTTP サーバがイネーブルであるかどうかを表示します。

http[s]（パラメータ）

ScanSafe インスペクション ポリシー マップのサービス タイプを指定するには、パラメータ コンフィギュレーション モードで **http[s]** コマンドを使用します。サービス タイプを削除するには、このコマンドの **no** 形式を使用します。パラメータ コンフィギュレーション モードにアクセスするには、まず **policy-map type inspect scansafe** コマンドを入力します。

{**http** | **https**}

no {**http** | **https**}

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

ScanSafe インスペクション ポリシー マップには、**http** または **https** のいずれか 1 つのサービス タイプのみを指定できます。デフォルトはありません。タイプを指定する必要があります。

例

次に、インスペクション ポリシー マップを作成して、サービス タイプを HTTP に設定する例を示します。

```
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# http
```

関連コマンド

コマンド	説明
class-map type inspect scansafe	ホワイトリストに記載されたユーザとグループのインスペクション クラス マップを作成します。
default user group	ASA に入ってくるユーザのアイデンティティを ASA が判別できない場合のデフォルトのユーザ名やグループを指定します。
inspect scansafe	このクラスのトラフィックに対するクラウド Web セキュリティ インスペクションをイネーブルにします。
license	要求の送信元の組織を示すため、ASA がクラウド Web セキュリティ プロキシ サーバに送信する認証キーを設定します。
match user group	ユーザまたはグループをホワイトリストと照合します。
policy-map type inspect scansafe	インスペクション ポリシー マップを作成すると、ルールのために必要なパラメータを設定し、任意でホワイトリストを識別できます。
retry-count	再試行回数値を入力します。この値は、可用性をチェックするために、クラウド Web セキュリティ プロキシ サーバをポーリングする前に ASA が待機する時間です。
scansafe	マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可します。
scansafe general-options	汎用クラウド Web セキュリティ サーバ オプションを設定します。
server {**primary** | **backup**}	プライマリまたはバックアップのクラウド Web セキュリティ プロキシ サーバの完全修飾ドメイン名または IP アドレスを設定します。
show conn scansafe	大文字の Z フラグに示されたようにすべてのクラウド Web セキュリティ接続を表示します。
show scansafe server	サーバが現在のアクティブ サーバ、バックアップ サーバ、または到達不能のいずれであるか、サーバのステータスを表示します。
show scansafe statistics	合計と現在の http 接続を表示します。
user-identity monitor	AD エージェントから指定したユーザまたはグループ情報をダウンロードします。
whitelist	トラフィックのクラスでホワイトリスト アクションを実行します。

http authentication-certificate

ASDM の HTTPS 接続による認証のために証明書を要求するには、グローバル コンフィギュレーション モードで **http authentication-certificate** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** バージョンを使用します。

http authentication-certificate *interface name* [**match** *certificate_map_name*]

no http authentication-certificate [*interface* [**match** *certificate_map_name*]]

構文の説明

interface	証明書による認証を必要とする ASA でインターフェイスを指定します。
match *certificate_map_name*	証明書は証明書マップと一致する必要があります。マップを設定するには、**crypto ca certificate map** を使用します。

デフォルト

HTTP の証明書認証はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(3)	このコマンドは、**ssl certificate-authentication** コマンドに置き換えられて廃止されました。
8.2.1	このコマンドは、再追加されました。グローバルな **ssl certificate-authentication** コマンドは、下位互換性のために保存されています。
8.4.7, 9.1.3	証明書のみの認証がイネーブルになりました。以前は、このコマンドは、**aaa authentication http console** コマンドをイネーブルにした場合にだけ証明書認証をユーザ認証に追加しました。
9.6(2)	**match** *certificate_map_name* オプションが追加されました。

使用上のガイドライン

AAA 認証の有無にかかわらず証明書認証を必須にできます。証明書認証はインターフェイスごとに設定できます。その結果、信頼できるインターフェイスまたは内部インターフェイス上の接続については証明書の提示が不要になります。コマンドを複数回使用すれば、複数のインターフェイス上で証明書認証をイネーブルにできます。

ASA は、PKI トラスト ポイントと比較して証明書を検証します。証明書が検証に合格しない場合、ASA は SSL 接続を終了します。

例

次に、outside および external というインターフェイスに接続するクライアントに対して、証明書による認証を要求する例を示します。

```
ciscoasa(config)# http authentication-certificate inside
ciscoasa(config)# http authentication-certificate external
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。HTTP サーバをディセーブルにし、HTTP サーバにアクセスできるホストを削除します。
http	IP アドレスとサブネット マスクによって、HTTP サーバにアクセスできるホストを指定します。ホストが HTTP サーバへのアクセスで経由する ASA のインターフェイスを指定します。
http redirect	ASA が HTTP 接続を HTTPS にリダイレクトすることを指定します。
http server enable	HTTP サーバをイネーブルにします。
show running-config http	HTTP サーバにアクセスできるホストを表示し、さらに HTTP サーバがイネーブルであるかどうかを表示します。
ssl authentication-certificate	SSL 接続に証明書を要求します。

http-comp

特定のグループまたはユーザの WebVPN 接続上で HTTP データの圧縮をイネーブルにするには、グループ ポリシー webvpn コンフィギュレーション モードおよびユーザ名 webvpn コンフィギュレーション モードで **http-comp** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

http-comp {**gzip** | **none**}

no http-comp {**gzip** | **none**}

構文の説明

gzip	グループまたはユーザに対して圧縮をイネーブルにすることを指定します。
none	そのグループまたはユーザに対し圧縮がディセーブルにされるよう指示します。

デフォルト

デフォルトでは、圧縮はイネーブルに設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザ名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

WebVPN 接続の場合、グローバル コンフィギュレーション モードで設定された **compression** コマンドによって、グループ ポリシー webvpn コンフィギュレーション モードおよびユーザ名 webvpn コンフィギュレーション モードで設定された **http-comp** コマンドが上書きされます。

例

次の例では、グループ ポリシー sales の圧縮をディセーブルにします。

```
ciscoasa(config)# group-policy sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# http-comp none
```

関連コマンド

コマンド	説明
圧縮	すべての SVC、WebVPN、および IPsec VPN 接続で、圧縮をイネーブルにします。

http connection idle-timeout

ASDM、WebVPN、およびその他のクライアントなど、ASA への HTTPS 接続のアイドルタイムアウトを設定するには、グローバル コンフィギュレーション モードで **http connection idle-timeout** コマンドを使用します。タイムアウトをディセーブルにするには、このコマンドの **no** 形式を使用します。

http connection idle-timeout [*seconds*]

no http connection idle-timeout [*seconds*]

構文の説明no http

seconds	アイドルタイムアウト（10 ? 86400 秒）。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.14(1)	このコマンドが追加されました。

使用上のガイドライン

ASA は、設定した期間アイドル状態の接続を切断します。**http server idle-timeout** コマンドと **http connection idle-timeout** コマンドの両方を設定した場合は、**http connection idle-timeout** コマンドが優先されます。

例

次の例では、HTTPS セッションのアイドルタイムアウトを 600 秒に設定します。

```
ciscoasa(config)# http connections idle-timeout 600
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。HTTP サーバをディセーブルにし、HTTP サーバにアクセスできるホストを削除します。
http	IP アドレスおよびサブネット マスクにより HTTP サーバにアクセスできるホストと、そのホストの HTTP サーバへのアクセスで経由するインターフェイスを指定します。
http authentication-certificate	ASA への HTTPS 接続を確立するユーザの証明書による認証を要求します。
http server enable	ASDM セッション用に HTTP サーバをイネーブルにします。
http server idle-timeout	ASDM アイドルタイムアウトを設定します。
http server session-timeout	ASA に対する ASDM セッションのセッション時間を制限します。
http redirect	ASA が HTTP 接続を HTTPS にリダイレクトすることを指定します。
show running-config http	HTTP サーバにアクセスできるホストを表示し、さらに HTTP サーバがイネーブルであるかどうかを表示します。

http-only-cookie

クライアントレス SSL VPN セッションのクッキーが JavaScript などのクライアント側のスクリプトを介してサードパーティからアクセスされないようにするには、webvpn モードで **http-only-cookie** コマンドを使用します。この制限を削除するには、このコマンドの **no** 形式を使用します。

http-only-cookie

no http-only-cookie

デフォルト

セッション Cookie は、サード パーティによって使用できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.1(7)	このコマンドが追加されました。

使用上のガイドライン

Flash アプリケーションや Java アプレットなどの組み込みオブジェクト、および外部アプリケーションは、通常は既存のセッションのクッキーに依存してサーバと連携しています。これらの組み込みオブジェクトは、初期化時にいくつかの Javascript を使用してブラウザからクッキーを取得します。クライアントレス SSL VPN セッション クッキーに httponly フラグを追加すると、セッション クッキーがブラウザのみで認識され、クライアント側のスクリプトでは認識されなくなり、セッションの共有は不可能になります。

(注) このコマンドは、Cisco TAC から使用を推奨された場合のみ使用してください。このコマンドをイネーブルにすると、次に示すクライアントレス SSL VPN 機能が警告なしで動作しなくなるため、セキュリティ上のリスクが発生します。

• VPN セッションのクッキー設定は、アクティブなクライアントレス SSL VPN セッションがない場合にだけ変更してください。

• クライアントレス SSL VPN セッションのステータスを確認するには、**show vpn-sessiondb webvpn** コマンドを使用します。

• すべてのクライアントレス SSL VPN セッションからログアウトするには、**vpn-sessiondb logoff webvpn** コマンドを使用します。

• 次のクライアントレス SSL VPN 機能は、http-only-cookie コマンドがイネーブルの場合に動作しません。

  – Java プラグイン
  – Java リライタ
  – ポートフォワーディング。
  – ファイルブラウザ
  – デスクトップ アプリケーション（Microsoft Office アプリケーションなど）を必要とする Sharepoint 機能
  – AnyConnect Web 起動
  – Citrix Receiver、XenDesktop、および Xenon
  – その他の非ブラウザ ベース アプリケーションおよびブラウザプラグインベースのアプリケーション

例

```
hostname(config)# webvpn
hostname(config-webvpn)# http-only-cookie
```

http-only-cookie

クライアントレス SSL VPN セッション クッキーの httponly フラグをイネーブルにするには、webvpn コンフィギュレーション モードで **http-only-cookie** コマンドを使用します。このフラグをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

http-only-cookie

no http-only-cookie

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

httponly フラグはデフォルトでディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.2(3)	このコマンドが導入されました。

使用上のガイドライン

Flash アプリケーションや Java アプレットなどの組み込みオブジェクト、および外部アプリケーションは、通常は既存のセッションのクッキーに依存してサーバと連携しています。これらの組み込みオブジェクトは、初期化時にいくつかの Javascript を使用してブラウザからクッキーを取得します。クライアントレス SSL VPN セッション クッキーに httponly フラグを追加すると、セッション クッキーがブラウザのみで認識され、クライアント側のスクリプトでは認識されなくなり、セッションの共有は不可能になります。

VPN セッション クッキー設定の変更は、アクティブなクライアントレス SSL VPN セッションが存在しない場合のみ実行してください。**show vpn-sessiondb webvpn** コマンドを使用して、クライアントレス SSL VPN セッションのステータスを確認します。vpn-sessiondb logoff webvpn コマンドを使用して、すべてのクライアントレス SSL VPN セッションからログアウトします。

次のクライアントレス SSL VPN 機能は、http-only-cookie コマンドがイネーブルの場合に動作しません。

- Java プラグイン
- Java リライタ

- ポートフォワーディング。
- ファイルブラウザ
- デスクトップ アプリケーション（Microsoft Office アプリケーションなど）を必要とする Sharepoint 機能
- AnyConnect Web 起動
- Citrix Receiver、XenDesktop、および Xenon
- その他の非ブラウザ ベース アプリケーションおよびブラウザプラグインベースのアプリケーション

（注） このコマンドは、Cisco TAC から使用を推奨された場合のみ使用してください。このコマンドをイネーブルにすると、セキュリティ上のリスクが発生します。

例

次に、クライアントレス SSL VPN セッション クッキーの httponly フラグをイネーブルにする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# http-only-cookie
ciscoasa(config-webvpn)
```

関連コマンド

コマンド	説明
show running-config webvpn	クライアントレス SSL VPN の実行コンフィギュレーションを表示します。

http-proxy（call-home）

スマート ライセンスおよび Smart Call Home 用に HTTP(S) プロキシを設定するには、Call Home コンフィギュレーション モードで **http-proxy** コマンドを使用します。プロキシを削除するには、このコマンドの **no** 形式を使用します。

http-proxy *ip_address* **port** *port*

no http-proxy [*ip_address* **port** *port*]

構文の説明

ip_address	HTTP プロキシ サーバの IP アドレスを設定します。
port *port*	HTTP プロキシのポート番号を設定します。たとえば、HTTPS サーバに 443 を使用します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
Call Home コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Smart Call Home およびスマート ライセンスに対して HTTP または HTTPS プロキシをグローバルに設定します。

例

次に、HTTP プロキシを設定する例を示します。

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

関連コマンド

コマンド	説明
call-home	Smart Call Home を設定します。スマート ライセンスでは、Smart Call Home インフラストラクチャが使用されます。
clear configure license	スマート ライセンス設定をクリアします。
feature tier	スマート ライセンスの機能層を設定します。
license smart	スマート ライセンスのライセンス権限付与を要求できます。
license smart deregister	ライセンス認証局からデバイスを登録解除します。
license smart register	デバイスをライセンス認証局に登録します。
license smart renew	登録またはライセンス権限を更新します。
service call-home	Smart Call Home をイネーブルにします。
show license	スマート ライセンスのステータスを表示します。
show running-config license	スマート ライセンスの設定を表示します。
throughput level	スマート ライセンスのスループット レベルを設定します。

http-proxy（dap）

HTTP プロキシ ポート フォワーディングをイネーブルまたはディセーブルにするには、DAP webvpn コンフィギュレーション モードで **http-proxy** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

http-proxy {**enable** | **disable** | **auto-start**}

no http-proxy

構文の説明

auto-start	DAP レコードの HTTP プロキシ ポート フォワーディングをイネーブルにし、自動的に開始します。
enable/disable	DAP レコードの HTTP プロキシ ポート フォワーディングをイネーブルまたはディセーブルにします。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
DAP webvpn コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

ASA は、さまざまなソースからの属性値を適用できます。次の階層に従って、属性値を適用します。

1. DAP レコード
2. ユーザ名
3. グループ ポリシー
4. トンネル グループのグループ ポリシー
5. デフォルトのグループ ポリシー

したがって、属性の DAP 値は、ユーザ、グループ ポリシー、またはトンネル グループに設定されたものよりも優先順位が高くなります。

DAP レコードの属性をイネーブルまたはディセーブルにすると、ASA はその値を適用して実行します。たとえば、DAP webvpn コンフィギュレーション モードで HTTP プロキシをディセーブルにすると、ASA はそれ以上値を検索しません。代わりに、**http-proxy** コマンドの **no** 値を使用すると、属性は DAP レコードには存在しないため、ASA は適用する値を見つけるために、ユーザ名および必要に応じてグローバル ポリシーの AAA 属性に移動して検索します。

例

次に、Finance という名前の DAP レコードに対して HTTP プロキシ ポート フォワーディングをイネーブルにする例を示します。

```
ciscoasa (config)# dynamic-access-policy-record Finance
ciscoasa(config-dynamic-access-policy-record)# webvpn
ciscoasa(config-dap-webvpn)# http-proxy enable
ciscoasa(config-dap-webvpn)#
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
show running-config dynamic-access-policy-record	すべての DAP レコードまたは指定した DAP レコードの実行コンフィギュレーションを表示します。

http-proxy（webvpn）

外部プロキシ サーバを使用して HTTP 要求を処理するように ASA を設定するには、webvpn コンフィギュレーション モードで **http-proxy** コマンドを使用します。HTTP プロキシ サーバをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

http-proxy {*host* [*port*] [**exclude** *url*] | **pac** *pacfile*} [**username** *username* {**password** *password*}]

no http-proxy

構文の説明

ホスト	外部 HTTP プロキシ サーバのホスト名または IP アドレス。
pac *pacfile*	1 つ以上のプロキシを指定する JavaScript 関数を含む PAC ファイルを指定します。
password	（オプション。username を指定した場合に限り使用可能）各 HTTP プロキシ要求にパスワードを付加して基本的なプロキシ認証を提供するには、このキーワードを入力します。
password	各 HTTP 要求とともにプロキシ サーバに送信されるパスワード。
port	（任意）HTTP プロキシ サーバによって使用されるポート番号。デフォルト ポートは 80 です。値を指定しなかった場合、ASA はこのポートを使用します。指定できる範囲は 1 ～ 65535 です。
url	プロキシ サーバへの送信が可能な URL から除外する URL を 1 つ、または複数の URL のカンマ区切りのリストを入力します。このストリングには文字数の制限はありませんが、コマンド全体で 512 文字以下となるようにする必要があります。リテラル URL を指定するか、次のワイルドカードを使用できます。 • ***** は、スラッシュ（/）とピリオド（.）を含む任意の文字列と一致します。このワイルドカードは、英数字文字列とともに使用する必要があります。 • **?** は、スラッシュおよびピリオドを含む、任意の 1 文字に一致します。 • [*x*-*y*] は、*x* から *y* の範囲にある任意の 1 文字に一致します。ここで、*x* は ANSI 文字セット内の 1 文字を、*y* は ANSI 文字セット内の別の 1 文字を示します。 • [**!***x*-*y*] は、この範囲内に存在しない任意の 1 文字に一致します。
username	（任意）各 HTTP プロキシ要求にユーザ名を付加して基本的なプロキシ認証を提供するには、このキーワードを入力します。
username	各 HTTP 要求とともにプロキシ サーバに送信されるユーザ名。

デフォルト

デフォルトでは、HTTP プロキシ サーバは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(2)	**exclude**、**username**、および **password** キーワードが追加されました。

使用上のガイドライン

組織が管理するサーバを経由したインターネットへのアクセスを必須にすると、セキュアなインターネット アクセスを確保して管理面の制御を保証するためのフィルタリング導入の別のきっかけにもなります。

ASA でサポートされるのは、**http-proxy** コマンドの 1 つのインスタンスだけです。このコマンドのインスタンスが実行コンフィギュレーションにすでに 1 つ存在する場合、もう 1 つインスタンスを入力すると、CLI は以前のインスタンスを上書きします。**show running-config webvpn** コマンドを入力すると、CLI によって実行コンフィギュレーション内のすべての **http-proxy** コマンドがリストされます。応答に **http-proxy** コマンドがリストされていない場合、このコマンドは存在しません。

(注) プロキシ NTLM 認証は **http-proxy** ではサポートされていません。認証なしのプロキシと基本認証だけがサポートされています。

例

次の例は、次の設定の HTTP プロキシ サーバの使用を設定する方法を示しています。IP アドレスが 209.165. 201.2 で、デフォルト ポートの 443 を使用しています。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# http-proxy 209.165.201.2
ciscoasa(config-webvpn)
```

次に、同じプロキシ サーバを使用して、各 HTTP 要求とともにユーザ名およびパスワードを送信するように設定する例を示します。

```
ciscoasa(config-webvpn)# http-proxy 209.165.201.2 jsmith password mysecretdonttell
ciscoasa(config-webvpn)
```

次も、同じコマンドの例を示しますが、前の例とは異なり、この例では、ASA が HTTP 要求で www.example.com という特定の URL を受信した場合には、プロキシ サーバに渡すのではなく自分自身で要求を解決します。

```
ciscoasa(config-webvpn)# http-proxy 209.165.201.2 exclude www.example.com username jsmith
password mysecretdonttell
ciscoasa(config-webvpn)
```

次に、**exclude** オプションの使用例を示します。

```
ciscoasa(config-webvpn)# http-proxy 10.1.1.1 port 8080 exclude *.com username John pasword
12345678
ciscoasa(config-webvpn)
```

次に、**pac** オプションの使用例を示します。

```
ciscoasa(config-webvpn)# http-proxy pac http://10.1.1.1/pac.js
ciscoasa(config-webvpn)
```

関連コマンド

コマンド	説明
https-proxy	外部プロキシ サーバを使用して HTTPS 要求を処理するように設定します。
show running-config webvpn	SSL VPN の実行コンフィギュレーションを、HTTP および HTTPS のプロキシ サーバをすべて含めて表示します。

http redirect

ASA による HTTP 接続の HTTPS へのリダイレクトを指定するには、グローバル コンフィギュレーション モードで **http redirect** コマンドを使用します。指定した **http redirect** コマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。すべての **http redirect** コマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を引数なしで使用します。

http redirect *interface* [*port*]

no http redirect [*interface*]

構文の説明

interface	ASA で HTTP 要求を HTTPS にリダイレクトする必要があるインターフェイスを識別します。
port	ASA が HTTP 要求をリッスンするポートを識別します。HTTP 要求はリッスン後 HTTPS にリダイレクトされます。デフォルトでは、ポート 80 でリッスンします。

デフォルト

HTTP リダイレクトはディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

インターフェイスには、HTTP を許可するアクセス リストが必要です。アクセス リストがない場合、ASA はポート 80 も HTTP 用に設定した他のどのポートもリッスンしません。

http redirect コマンドが失敗すると、次のメッセージが表示されます。

```
"TCP port <port_number> on interface <interface_name> is in use by another feature. Please choose a different port for the HTTP redirect service"
```

HTTP リダイレクト サービス用に別のポートを使用してください。

例

次に、デフォルト ポート 80 のままで、内部インターフェイスの HTTP リダイレクトを設定する例を示します。

```
ciscoasa(config)# http redirect inside
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。HTTP サーバをディセーブルにし、HTTP サーバにアクセスできるホストを削除します。
http	IP アドレスとサブネット マスクによって、HTTP サーバにアクセスできるホストを指定します。ホストが HTTP サーバへのアクセスで経由する ASA のインターフェイスを指定します。
http authentication-certificate	ASA への HTTPS 接続を確立するユーザの証明書による認証を要求します。
http server enable	HTTP サーバをイネーブルにします。
show running-config http	HTTP サーバにアクセスできるホストを表示し、さらに HTTP サーバがイネーブルであるかどうかを表示します。

http server basic-auth-client

ブラウザベース以外の HTTPS クライアントが ASA 上の HTTPS サービスにアクセスできるようにするには、グローバル コンフィギュレーション モードで **http serverbasic-auth-client** コマンドを使用します。クライアントのサポートを削除するには、このコマンドの **no** 形式を使用します。

http server basic-auth-client *user_agent*

no http server basic-auth-client *user_agent*

構文の説明

user_agent	HTTP 要求の HTTP ヘッダーにあるクライアントの User-Agent 文字列を指定します。完全な文字列または部分文字列を指定できます。部分文字列については、User-Agent 文字列の先頭と一致している必要があります。セキュリティを強化するために完全な文字列をお勧めします。文字列では大文字と小文字が区別されることに注意してください。
	たとえば、**curl** は次の User-Agent 文字列と一致します。
	`curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2`
	curl は、次の User-Agent 文字列とは一致しません。
	`abcd curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2`
	CURL は、次の User-Agent 文字列とは一致しません。
	`curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2`

コマンドデフォルト

デフォルトでは、ASDM、CSM、および REST API が許可されています。

コマンドモード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンドモード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.12(1)	コマンドが追加されました。

使用上のガイドライン

個別のコマンドを使用して、各クライアント文字列を入力します。多くの専門クライアント（python ライブラリ、curl、wget など）は、クロスサイト要求の偽造（CSRF）トークンベースの認証をサポートしていないため、これらのクライアントが ASA 基本認証方式を使用することを明確に許可する必要があります。セキュリティ上の理由から、必要なクライアントのみを許可する必要があります。

例

次に、curl クライアントを許可する例を示します。

```
ciscoasa(config)# http server basic-auth-client curl
```

関連コマンド

コマンド	説明
http server enable	ASA で HTTPS サーバを有効にします。

http server enable

ASA の HTTP サーバをイネーブルにするには、グローバル コンフィギュレーション モードで **http server enable** コマンドを使用します。HTTP サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

http server enable [*port*]

構文の説明no http

port	HTTP 接続に使用するポート。範囲は 1 ～ 65535 です。デフォルトのポートは 443 です。

デフォルト

HTTP サーバはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、HTTP サーバをイネーブルにする例を示します。

```
ciscoasa(config)# http server enable
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。HTTP サーバをディセーブルにし、HTTP サーバにアクセスできるホストを削除します。
http	IP アドレスとサブネット マスクによって、HTTP サーバにアクセスできるホストを指定します。ホストが HTTP サーバへのアクセスで経由する ASA のインターフェイスを指定します。
http authentication-certificate	ASA への HTTPS 接続を確立するユーザの証明書による認証を要求します。

コマンド	説明
http redirect	ASA が HTTP 接続を HTTPS にリダイレクトすることを指定します。
show running-config http	HTTP サーバにアクセスできるホストを表示し、さらに HTTP サーバがイネーブルであるかどうかを表示します。

http server idle-timeout

ASA への ASDM 接続のアイドル タイムアウトを設定するには、グローバル コンフィギュレーション モードで **http server idle-timeout** コマンドを使用します。タイムアウトをディセーブルにするには、このコマンドの **no** 形式を使用します。

http server idle-timeout [*minutes*]

no http server idle-timeout [*minutes*]

構文の説明

minutes	アイドル タイムアウト（1 ～ 1440 分）。

デフォルト

デフォルトの設定は 20 分です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

例

次に、ASDM セッションのアイドル タイムアウトを 500 分に設定する例を示します。

```
ciscoasa(config)# http server idle-timeout 500
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。HTTP サーバをディセーブルにし、HTTP サーバにアクセスできるホストを削除します。
http	IP アドレスおよびサブネット マスクにより HTTP サーバにアクセスできるホストと、そのホストの HTTP サーバへのアクセスで経由するインターフェイスを指定します。
http authentication-certificate	ASA への HTTPS 接続を確立するユーザの証明書による認証を要求します。
http server enable	ASDM セッション用に HTTP サーバをイネーブルにします。

コマンド	説明
http server session-timeout	ASA に対する ASDM セッションのセッション時間を制限します。
http redirect	ASA が HTTP 接続を HTTPS にリダイレクトすることを指定します。
show running-config http	HTTP サーバにアクセスできるホストを表示し、さらに HTTP サーバがイネーブルであるかどうかを表示します。

http server session-timeout

ASA への ASDM 接続のセッション タイムアウトを設定するには、グローバル コンフィギュレーション モードで **http server session-timeout** コマンドを使用します。タイムアウトをディセーブルにするには、このコマンドの **no** 形式を使用します。

http server session-timeout [*minutes*]

no http server session-timeout [*minutes*]

構文の説明no http

minutes	セッション タイムアウト(1 ～ 1440 分)。

デフォルト

セッション タイムアウトはディセーブルです。ASDM 接続にセッション時間の制限はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

例

次に、ASDM 接続のセッション タイムアウトを 1000 分に設定する例を示します。

```
ciscoasa(config)# http server session-timeout 1000
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。HTTP サーバをディセーブルにし、HTTP サーバにアクセスできるホストを削除します。
http	IP アドレスおよびサブネット マスクにより HTTP サーバにアクセスできるホストと、そのホストの HTTP サーバへのアクセスで経由するインターフェイスを指定します。
http authentication-certificate	ASA への HTTPS 接続を確立するユーザの証明書による認証を要求します。
http server enable	ASDM セッション用に HTTP サーバをイネーブルにします。

コマンド	説明
http server idle-timeout	ASA に対する ASDM セッションのアイドル時間を制限します。
http redirect	ASA が HTTP 接続を HTTPS にリダイレクトすることを指定します。
show running-config http	HTTP サーバにアクセスできるホストを表示し、さらに HTTP サーバがイネーブルであるかどうかを表示します。

https-proxy

外部プロキシ サーバを使用して HTTPS 要求を処理するように ASA を設定するには、webvpn コンフィギュレーション モードで **https-proxy** コマンドを使用します。HTTPS プロキシ サーバをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

https-proxy {*host* [*port*] [**exclude** *url*] | [**username** *username* {**password** *password*}]

no https-proxy

構文の説明

ホスト	外部 HTTPS プロキシ サーバのホスト名または IP アドレス。
password	（オプション。username を指定した場合に限り使用可能）各 HTTPS プロキシ要求にパスワードを付加して基本的なプロキシ認証を提供するには、このキーワードを入力します。
password	各 HTTPS 要求とともにプロキシ サーバに送信されるパスワード。
port	（任意）HTTPS プロキシ サーバによって使用されるポート番号。デフォルト ポートは 443 です。値を指定しなかった場合、ASA はこのポートを使用します。指定できる範囲は 1 ～ 65535 です。
url	プロキシ サーバへの送信が可能な URL から除外する URL を 1 つ、または複数の URL のカンマ区切りのリストを入力します。このストリングには文字数の制限はありませんが、コマンド全体で 512 文字以下となるようにする必要があります。リテラル URL を指定するか、次のワイルドカードを使用できます。 • * は、スラッシュ（/）とピリオド（.）を含む任意の文字列と一致します。このワイルドカードは、英数字文字列とともに使用する必要があります。 • ? は、スラッシュおよびピリオドを含む、任意の 1 文字に一致します。 • [*x*-*y*] は、*x* から *y* の範囲にある任意の 1 文字に一致します。ここで、*x* は ANSI 文字セット内の 1 文字を、*y* は ANSI 文字セット内の別の 1 文字を示します。 • [!*x*-*y*] は、この範囲内に存在しない任意の 1 文字に一致します。
username	（任意）各 HTTPS プロキシ要求にユーザ名を付加して基本的なプロキシ認証を提供するには、このキーワードを入力します。
username	各 HTTPS 要求とともにプロキシ サーバに送信されるユーザ名。

デフォルト

デフォルトでは、HTTPS プロキシ サーバは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(2)	**exclude**、**username**、および **password** キーワードが追加されました。

使用上のガイドライン

組織が管理するサーバを経由したインターネットへのアクセスを必須にすると、セキュアなインターネット アクセスを確保して管理面の制御を保証するためのフィルタリング導入の別のきっかけにもなります。

ASA でサポートされるのは、**https-proxy** コマンドの 1 つのインスタンスだけです。このコマンドのインスタンスが実行コンフィギュレーションにすでに 1 つ存在する場合、もう 1 つインスタンスを入力すると、CLI は以前のインスタンスを上書きします。**show running-config webvpn** コマンドを入力すると、CLI によって実行コンフィギュレーション内のすべての **https-proxy** コマンドがリストされます。応答に **https-proxy** コマンドがリストされていない場合、このコマンドは存在しません。

例

次の例は、次の設定の HTTPS プロキシ サーバの使用を設定する方法を示しています:IP アドレスが 209.165. 201.2 で、デフォルト ポートの 443 を使用しています。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# https-proxy 209.165.201.2
ciscoasa(config-webvpn)
```

次に、同じプロキシ サーバを使用して、各 HTTPS 要求とともにユーザ名およびパスワードを送信するように設定する例を示します。

```
ciscoasa(config-webvpn)# https-proxy 209.165.201.2 jsmith password mysecretdonttell
ciscoasa(config-webvpn)
```

次も、同じコマンドの例を示しますが、前の例とは異なり、この例では、ASA が HTTPS 要求で www.example.com という特定の URL を受信した場合には、プロキシ サーバに渡すのではなく自分自身で要求を解決します。

```
ciscoasa(config-webvpn)# https-proxy 209.165.201.2 exclude www.example.com username jsmith
password mysecretdonttell
ciscoasa(config-webvpn)
```

次に、**exclude** オプションの使用例を示します。

```
ciscoasa(config-webvpn)# https-proxy 10.1.1.1 port 8080 exclude *.com username John
pasword 12345678
ciscoasa(config-webvpn)
```

次に、**pac** オプションの使用例を示します。

```
ciscoasa(config-webvpn)# https-proxy pac http://10.1.1.1/pac.js
ciscoasa(config-webvpn)
```

関連コマンド

コマンド	説明
http-proxy	外部プロキシ サーバを使用して HTTP 要求を処理するように設定します。
show running-config webvpn	SSL VPN の実行コンフィギュレーションを、HTTP および HTTPS のプロキシ サーバをすべて含めて表示します。

http username-from-certificate

ASDM の承認または認証を取得する証明書またはルールのフィールドを指定するには、**http username-from-certificate** コマンドを使用します。

http username-from-certificate {<primary-attr> [<secondary-attr>] | use-entire-name | use-script} | pre-fill-username]

構文の説明

pre-fill-username	VPN 接続の場合に同じ目的で機能するトンネルグループ一般属性モードの既存の username-from-certificate コマンドを使用できるようにします。イネーブルの場合、このユーザ名は、ユーザが入力したパスワードとともに認証に使用されます。
primary-attr	ユーザ名の取得に使用する属性を指定します。
secondary-attr	ユーザ名を取得するために、プライマリ属性とともに使用する追加の属性を指定します。
use-entire-name	DN 名全体を使用します。セカンダリ属性としては使用できません。
use-script	ASDM によって生成された LUA スクリプトを使用します。

コマンド デフォルト

このコマンドのデフォルトは、http username-from-certificate CN OU です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

次に、プライマリ属性およびセカンダリ属性の有効値と関連するキーワードの意味を示します。

属性/キーワード	定義
C	Country（国名）:2 文字の国名略語。国名コードは、ISE 3166 国名略語に準拠しています。

属性/キーワード	定義
CN	Common Name（一般名）：人、システム、その他のエンティティの名前。セカンダリ属性としては使用できません。
DNQ	ドメイン名修飾子。
EA	電子メール アドレス
GENQ	世代修飾子
GN	名
I	Initials（イニシャル）。
L	Locality（地名）：組織が置かれている市または町。
N	名前
O	Organization（組織）：会社、団体、機関、連合、その他のエンティティの名前。
OU	組織ユニット：組織内のサブグループ（0）。
SER	Serial Number（シリアル番号）。
SN	Surname（姓）。
SP	州または都道府県：組織が置かれている州または都道府県。
T	Title（タイトル）。
UID	User Identifier（ユーザ ID）。
UPN	User Principal Name（ユーザ プリンシパル名）。

このコマンドは、webvpn をサポートしないプラットフォーム（ASA 1000v）や No Payload Encryption（NPE）がイネーブルになっているプラットフォームでは使用できません。

例

```
100/act(config)# http ?

configure mode commands/options:
  Hostname or A.B.C.D          The IP address of the host and/or network
                               authorized to access the HTTP server
  X:X:X:X::X/<0-128>           IPv6 address/prefix authorized to access the HTTP
                               server
  authentication-certificate   Request a certificate from the HTTPS client when
                               a management connection is being established
  redirect                     Redirect HTTP connections to the security gateway
                               to use HTTPS
  server                       Enable the http server required to run Device
                               Manager
  username-from-certificate    Specify fields from certificate DN to be used for
                               authorization/authentication
100/act(config)# help http

USAGE:

        [no] http {<local_ip>|<hostname>} <mask> <if_name>
        [no] http authentication-certificate <if_name>
        [no] http redirect <if_name> [<port>]
        [no] http server enable [<port>]
        [no] http username-from-certificate {<primary-attr> [<secondary-attr>] | use-
entire-name | use-script } [pre-fill-username]
        show running-config [all] http
        clear configure http
```

```
DESCRIPTION:

http            Configure HTTP server

SYNTAX:

<local_ip>      The ip address of the host and/or network authorized to
                access the device HTTP server.

<hostname>      Hostname of the host authorized to access the device
                HTTP server.

<mask>          The IP netmask to apply to <local_ip>.
                Default is 255.255.255.255.

<if_name>       Network interface name.

<port>          The decimal number or name of a TCP or UDP port.
                Default is "http" (80).
<primary-attr>  The DN from the certificate to be used as the username
<secondary-attr> Optional Secondary DN from the certificate to be used in the username
```

hw-module module allow-ip

ASA 5505 の AIP SSC に対して、管理 IP アドレスにアクセスが許可されたホストを設定するには、特権 EXEC モードで **hw-module module allow-ip** コマンドを使用します。

hw-module module 1 allow-ip *ip_address netmask*

構文の説明

1	スロット番号を指定します。これは常に 1 です。
ip_ address	ホスト IP アドレスを指定します。
netmask	サブネット マスクを指定します。

デフォルト

出荷時のデフォルトのコンフィギュレーションでは、192.168.1.5 ～ 192.168.1.254 のホストが IPS モジュールの管理を許可されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、SSC のステータスがアップ状態にある場合だけ有効です。

これらの設定は、ASA コンフィギュレーションではなく IPS アプリケーション コンフィギュレーションに書き込まれます。これらの設定を ASA から表示するには、**show module details** コマンドを使用します。

または、IPS アプリケーションの **setup** コマンドを使用して、この設定を IPS CLI から設定することもできます。

例

次に、SSC のホスト パラメータを設定する例を示します。

```
ciscoasa# hw-module module 1 allow-ip 209.165.201.29 255.255.255.0
```

関連コマンド

コマンド	説明
hw-module module ip	AIP SSC 管理アドレスを設定します。
show module	モジュールのステータス情報を表示します。

hw-module module ip

ASA 5505 の AIP SSC に対して、管理 IP アドレスを設定するには、特権 EXEC モードで **hw-module module ip** コマンドを使用します。

hw-module module 1 ip *ip_address netmask gateway*

構文の説明

1	スロット番号を指定します。これは常に 1 です。
gateway	ゲートウェイ IP アドレスを指定します。
ip_address	管理 IP アドレスを指定します。
netmask	サブネット マスクを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

このアドレスが ASA VLAN IP アドレスと同じサブネット上にあることを確認します。たとえば、10.1.1.1 を ASA の VLAN に割り当てた場合は、そのネットワーク上の別のアドレス（10.1.1.2 など）を IPS 管理アドレスに割り当てます。

管理ステーションが、直接接続されている ASA ネットワーク上にある場合は、ゲートウェイを、IPS 管理 VLAN に割り当てられた ASA IP アドレスに設定します。上記の例では、10.1.1.1 にゲートウェイを設定します。管理ステーションがリモート ネットワーク上にある場合は、ゲートウェイを、IPS 管理 VLAN のアップストリーム ルータのアドレスに設定します。

（注） これらの設定は、ASA コンフィギュレーションではなく IPS アプリケーション コンフィギュレーションに書き込まれます。これらの設定を ASA から表示するには、**show module details** コマンドを使用します。

または、IPS アプリケーションの **setup** コマンドを使用して、この設定を IPS CLI から設定することもできます。

例

次に、IPS モジュールの管理アドレスを設定する例を示します。

```
ciscoasa# hw-module module 1 ip 209.165.200.254 255.255.255.224 209.165.200.225
```

関連コマンド

コマンド	説明
hw-module module allow-ip	AIP SSC 管理ホストのアドレスを設定します。
show module	モジュールのステータス情報を表示します。

hw-module module password-reset

ハードウェア モジュールのデフォルト管理ユーザのパスワードをデフォルト値にリセットするには、特権 EXEC モードで **hw-module module password-reset** コマンドを使用します。

hw-module module 1 password-reset

構文の説明

1	スロット番号を指定します。これは常に 1 です。

デフォルト

デフォルトのユーザ名とパスワードはモジュールによって異なります。

- IPS モジュール - ユーザ名：**cisco**、パスワード：**cisco**
- CSC モジュール - ユーザ名：**cisco**、パスワード：**cisco**
- ASA CX モジュール - ユーザ名：**admin**、パスワード：**Admin123**

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(2)	このコマンドが追加されました。
8.4(4.1)	ASA CX モジュールのサポートが追加されました。

使用上のガイドライン

このコマンドは、ハードウェア モジュールがアップ状態で、パスワード リセットがサポートされている場合にのみ有効です。IPS の場合、パスワードのリセットは、モジュールが IPS バージョン 6.0 以降を実行している場合にのみサポートされます。パスワードをリセットした後は、モジュール アプリケーションを使用してパスワードを独自の値に変更する必要があります。モジュールのパスワードをリセットすると、モジュールがリブートします。モジュールのリブート中はサービスを使用できません。リブートには数分を要する場合があります。**show module** コマンドを実行すると、モジュールの状態をモニタできます。

コマンドは、必ずプロンプトで確認を要求します。コマンドが成功した場合は、それ以上何も出力されません。コマンドが失敗した場合は、障害が発生した理由を示すエラー メッセージが表示されます。表示される可能性のあるエラー メッセージは、次のとおりです。

```
Unable to reset the password on the module in slot 1

Unable to reset the password on the module in slot 1 - unknown module state

Unable to reset the password on the module in slot 1 - no module installed

Failed to reset the password on the module in slot 1 - module not in Up state

Unable to reset the password on the module in slot 1 - unknown module type

The module in slot 1 does not support password reset

Unable to reset the password on the module in slot 1 - no application found

The SSM application version does not support password reset

Failed to reset the password on the module in slot 1
```

例

次に、スロット 1 のハードウェア モジュールのパスワードをリセットする例を示します。

```
ciscoasa(config)# hw-module module 1 password-reset
Reset the password on module in slot 1? [confirm] y
```

関連コマンド

コマンド	説明
hw-module module recover	TFTP サーバからリカバリ イメージをロードしてモジュールを回復します。
hw-module module reload	モジュール ソフトウェアをリロードします。
hw-module module reset	モジュール ハードウェアをシャット ダウンしてリセットします。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切る準備をして、モジュール ソフトウェアをシャットダウンします。
show module	モジュール情報を表示します。

hw-module module recover

TFTP サーバから取り付けモジュールにリカバリ ソフトウェア イメージをロードしたり、TFTP サーバにアクセスするためのネットワーク設定を行ったりするには、特権 EXEC モードで **hw-module module recover** コマンドを使用します。たとえば、モジュールがローカル イメージをロードできない場合などは、このコマンドを使用したモジュールの回復が必要となる場合があります。

hw-module module 1 recover {**boot** | **stop** | **configure** [**url** *tfp_url* | **ip** *module_address* | **gateway** *gateway_ip_address* | **vlan** *vlan_id*]}

構文の説明

1	スロット番号を指定します。これは常に 1 です。
boot	このモジュールの回復を開始し、**configure** キーワード設定に従ってリカバリ イメージをダウンロードします。ダウンロード後、モジュールは新しいイメージからリブートします。
configure	リカバリ イメージをダウンロードするためのネットワーク パラメータを設定します。**configure** キーワードの後にネットワーク パラメータを入力しなかった場合、すべてのパラメータの入力を求めるプロンプトが表示されます。このコマンドを実行すると、TFTP サーバの URL、管理インターフェイスの IP アドレスとネットマスク、ゲートウェイ アドレス、および VLAN ID の入力を求めるプロンプトが表示されます。これらのネットワーク パラメータは ROMMON で設定されます。モジュール アプリケーション コンフィギュレーションで設定したネットワーク パラメータは ROMMON には使用できないため、ここで別個に設定する必要があります。
gateway *gateway_ip_address*	（任意）SSM 管理インターフェイスを介して TFTP サーバにアクセスするためのゲートウェイ IP アドレス。
ip *module_address*	（オプション）モジュール管理インターフェイスの IP アドレス。
stop	リカバリ アクションを停止し、リカバリ イメージのダウンロードを停止します。モジュールは、元のイメージからブートします。このコマンドは、**hw-module module recover boot** コマンドを使用してリカバリを開始してから 30 ～ 45 秒以内に入力する必要があります。この期間が経過した後で **stop** コマンドを入力すると、モジュールが無応答になるなど、予期しない結果になることがあります。
url *tfp_url*	（任意）TFTP サーバ上のイメージの URL。次の形式で指定します。 **tftp://***server*/[*path*/]*filename*
vlan *vlan_id*	（オプション）管理インターフェイスの VLAN ID を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン　モジュールに障害が発生して、モジュール アプリケーション イメージを実行できない場合は、TFTP サーバからモジュール上に新しいイメージを再インストールできます。

(注)　モジュール ソフトウェア内部では、イメージをインストールするために **upgrade** コマンドを使用しないでください。

指定する TFTP サーバが、最大 60 MB のサイズのファイルを転送できることを確認してください。ネットワークとイメージのサイズに応じて、このプロセスは完了までに約 15 分間かかることがあります。

このコマンドは、モジュールがアップ、ダウン、無応答、または回復のいずれかの状態である場合にのみ使用可能です。ステート情報については、**show module** コマンドを参照してください。

show module 1 recover コマンドを使用してリカバリ コンフィギュレーションを表示できます。

(注)　このコマンドは、ASA CX、ASA FirePOWER モジュールではサポートされていません。

例　次に、TFTP サーバからイメージをダウンロードするようにモジュールを設定する例を示します。

```
ciscoasa# hw-module module 1 recover configure
Image URL [tftp://127.0.0.1/myimage]: tftp://10.1.1.1/ids-newimg
Port IP Address [127.0.0.2]: 10.1.2.10
Port Mask [255.255.255.254]: 255.255.255.0
Gateway IP Address [1.1.2.10]: 10.1.2.254
VLAN ID [0]: 100
```

次に、モジュールを回復する例を示します。

```
ciscoasa# hw-module module 1 recover boot
The module in slot 1 will be recovered. This may
erase all configuration and all data on that device and
attempt to download a new image for it.
Recover module in slot 1? [confirm]
```

関連コマンド

コマンド	説明
debug module-boot	モジュールのブート プロセスに関するデバッグ メッセージを表示します。
hw-module module reset	モジュールをシャットダウンし、ハードウェア リセットを実行します。
hw-module module reload	モジュール ソフトウェアをリロードします。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切る準備をして、モジュール ソフトウェアをシャットダウンします。
show module	モジュール情報を表示します。

hw-module module recover（ASA 5506W-X）

デフォルト設定をロードまたは回復する、あるいは ROMMON にアクセスして新しいイメージを ASA 5506W-X のワイヤレス アクセス ポイントにロードするには、特権 EXEC モードで **hw-module module recover** コマンドを使用します。

hw-module module wlan recover [**configuration** | **image**]

構文の説明

configuration	ワイヤレス アクセス ポイントを工場出荷時のデフォルト設定にリセットします。
image	ROMMON にアクセスし、TFTP アップグレード プロシージャを実行できるモジュール コンソールへのセッション。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

バックプレーン上のアクセス ポイント CLI に対する **image** キーワード セッション。アクセス ポイントをリロードします。アクセス ポイントが起動している場合は、起動プロセスをエスケープして ROMMON にアクセスし、TFTP イメージをダウンロードできます。詳しい手順については、[Reloading the Access Point Image] > [Using the CLI] を参照してください。

例

次に、アクセス ポイント上でイメージを回復する例を示します。

```
ciscoasa# hw-module module wlan recover image
WARNING: Image recovery cannot be carried out via CLI command on this module.
Do you want to reset the module and session into the module console to carry out the image
recovery?[confirm]
Resetting the module and sessioning into the module console
```

関連コマンド

コマンド	説明
hw-module module wlan reset	モジュールをシャットダウンし、ハードウェア リセットを実行します。

hw-module module reload

物理モジュールのモジュール ソフトウェアをリロードするには、特権 EXEC モードで **hw-module module reload** コマンドを使用します。

hw-module module 1 reload

構文の説明

1	スロット番号を指定します。これは常に 1 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(4.1)	ASA CX モジュールのサポートが追加されました。
9.2(1)	ASA FirePOWER モジュールのサポートが追加されました。

使用上のガイドライン

このコマンドは、モジュールをリロードする前にハードウェア リセットを実行する **hw-module module reset** コマンドとは異なります。

このコマンドは、モジュールのステータスがアップ状態にある場合だけ有効です。ステート情報については、**show module** コマンドを参照してください。

例

次に、スロット 1 のモジュールをリロードする例を示します。

```
ciscoasa# hw-module module 1 reload
Reload module in slot 1? [confirm] y
Reload issued for module in slot 1
%XXX-5-505002: Module in slot 1 is reloading. Please wait...
%XXX-5-505006: Module in slot 1 is Up.
```

関連コマンド

コマンド	説明
debug module-boot	モジュールのブート プロセスに関するデバッグ メッセージを表示します。
hw-module module recover	TFTP サーバからリカバリ イメージをロードしてモジュールを回復します。
hw-module module reset	モジュールをシャットダウンし、ハードウェア リセットを実行します。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切る準備をして、モジュール ソフトウェアをシャットダウンします。
show module	モジュール情報を表示します。

hw-module module reset

モジュール ハードウェアをリセットしてからモジュール ソフトウェアをリロードするには、特権 EXEC モードで **hw-module module reset** コマンドを使用します。

hw-module module {1 | wlan} reset

構文の説明

1	スロット番号を指定します。これは常に 1 です。
wlan	ASA 5506W-X の場合は、ワイヤレス アクセス ポイントを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(4.1)	ASA CX モジュールのサポートが追加されました。
9.2(1)	ASA FirePOWER モジュールのサポートが追加されました。
9.4(1)	**wlan** キーワードが追加されました。

使用上のガイドライン

モジュールがアップ状態の場合、**hw-module module reset** コマンドによって、リセットの前にソフトウェアをシャットダウンするように要求されます。

hw-module module recover コマンドを使用してモジュールを回復できます(サポートされている場合)。モジュールが回復状態になっているときに **hw-module module reset** コマンドを入力しても、モジュールは回復プロセスを中断しません。**hw-module module reset** コマンドによって、モジュールのハードウェア リセットが実行され、ハードウェアのリセット後にモジュールのリカバリが続行されます。モジュールがハングした場合は、回復中にモジュールをリセットできます。ハードウェア リセットによって、問題が解決することもあります。

このコマンドは、ソフトウェアのリロードのみを行いハードウェア リセットは行わない **hw-module module reload** コマンドとは異なります。

このコマンドは、モジュールのステータスがアップ、ダウン、無応答、または回復のいずれかの場合にのみ有効です。ステート情報については、**show module** コマンドを参照してください。

例

次に、アップ状態になっているスロット 1 のモジュールをリセットする例を示します。

```
ciscoasa# hw-module module 1 reset
The module in slot 1 should be shut down before
resetting it or loss of configuration may occur.
Reset module in slot 1? [confirm] y
Reset issued for module in slot 1
%XXX-5-505001: Module in slot 1 is shutting down. Please wait...
%XXX-5-505004: Module in slot 1 shutdown is complete.
%XXX-5-505003: Module in slot 1 is resetting. Please wait...
%XXX-5-505006: Module in slot 1 is Up.
```

関連コマンド

コマンド	説明
debug module-boot	モジュールのブート プロセスに関するデバッグ メッセージを表示します。
hw-module module recover	TFTP サーバからリカバリ イメージをロードしてモジュールを回復します。
hw-module module reload	モジュール ソフトウェアをリロードします。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切る準備をして、モジュール ソフトウェアをシャットダウンします。
show module	モジュール情報を表示します。

hw-module module shutdown

モジュール ソフトウェアをシャットダウンするには、特権 EXEC モードで **hw-module module shutdown** コマンドを使用します。

hw-module module 1 shutdown

構文の説明

1	スロット番号を指定します。これは常に 1 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(4.1)	ASA CX モジュールのサポートが追加されました。
9.2(1)	ASA FirePOWER モジュールのサポートが追加されました。

使用上のガイドライン

モジュール ソフトウェアをシャットダウンするのは、コンフィギュレーション データを失うことなく安全にモジュールの電源をオフにできるように準備するためです。

このコマンドは、モジュール ステータスがアップまたは無応答である場合にのみ有効です。ステート情報については、**show module** コマンドを参照してください。

例

次に、スロット 1 のモジュールをシャットダウンする例を示します。

```
ciscoasa# hw-module module 1 shutdown
Shutdown module in slot 1? [confirm] y
Shutdown issued for module in slot 1
ciscoasa#
%XXX-5-505001: Module in slot 1 is shutting down. Please wait...
%XXX-5-505004: Module in slot 1 shutdown is complete.
```

関連コマンド

コマンド	説明
debug module-boot	モジュールのブート プロセスに関するデバッグ メッセージを表示します。
hw-module module recover	TFTP サーバからリカバリ イメージをロードしてモジュールを回復します。
hw-module module reload	モジュール ソフトウェアをリロードします。
hw-module module reset	モジュールをシャットダウンし、ハードウェア リセットを実行します。
show module	モジュール情報を表示します。