CHAPTER 8

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。

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

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。