da – dg

- description （69 ページ）

database path

ローカル CA サーバー データベースのパスまたは位置を指定するには、CA サーバー コンフィギュレーション モードで **database** コマンドを使用します。フラッシュ メモリへのパスをデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

［ **no** ］ **database path** *mount-name directory-path*

構文の説明

directory-path	CA ファイルが保存される、マウント ポイント上のディレクトリへのパスを指定します。
mount-name	マウント名を指定します。

コマンド デフォルト

デフォルトでは、CA サーバー データベースはフラッシュ メモリに保存されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

データベースに保存されるローカル CA ファイルには、証明書データベース ファイル、ユーザー データベース ファイル、一時 PKCS12 ファイル、および現在の CRL ファイルが含まれます。*mount-name* 引数は、 ASA のファイルシステムを指定するために使用する **mount** コマンドの *name* 引数と同じです。

（注） これらの CA ファイルは内部保存ファイルです。変更しないでください。

例

次に、CA データベースのマウント ポイントを cifs_share として定義し、そのマウント ポイント上のデータベース ファイル ディレクトリを ca_dir/files_dir として定義する例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# database path cifs_share ca_dir/files_dir/
ciscoasa
(config-ca-server)
#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバー コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ユーザーはローカル CA を設定および管理できます。
crypto ca server user-db write	ローカルCAデータベースに設定されているユーザー情報をディスクに書き込みます。
debug crypto ca server	ユーザーがローカルCAサーバーを設定する場合にデバッグ メッセージを表示します。
mount	Common Internet File System（CIFS）および File Transfer Protocol ファイルシステム（FTPFS）の一方または両方を、ASA がアクセスできるようにします。
show crypto ca server	ASA の CA コンフィギュレーションの特性を表示します。
show crypto ca server cert-db	CA サーバーが発行する証明書を表示します。

ddns

ダイナミック DNS（DDNS）アップデート方式のタイプを指定するには、DDNS アップデート方式モードで **ddns** コマンドを使用します。実行コンフィギュレーションから更新方式タイプを削除するには、このコマンドの **no** 形式を使用します。

ddns [**both**]
no ddns [**both**]

構文の説明

both （オプション）DNS の A と PTR の両方のリソース レコード（RR）のアップデートを指定します。

コマンド デフォルト

DNS A RR のみを更新します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
DDNS アップデート方式	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

DDNS は、DNS で保持されている名前/アドレスおよびアドレス/名前のマッピングを更新します。DDNS 更新を実行するための 2 つの方式（RFC 2136 で規定されている IETF 標準、および一般的な HTTP 方式）のうち、ASA のこのリリースでは、IETF 方式をサポートしています。

名前とアドレスのマッピングは、次の 2 タイプの RR に保持されます。

- A リソース レコードには、ドメイン名から IP アドレスへのマッピングが含まれます。
- PTR リソース レコードには、IP アドレスからドメイン名へのマッピングが含まれます。

DDNS アップデートを使用して、DNS の A RR タイプと PTR RR タイプとの間で一貫した情報を保持できます。

DDNS アップデート方式コンフィギュレーション モードで **ddns** コマンドを発行するとき、アップデートを DNS A RR に対してのみ行うか、DNS の A と PTR の両方の RR タイプに対して行うかを定義します。

例

次に、ddns-2 という名前の DDNS アップデート方式に対し DNS の A と PTR の両方の RR のアップデートを設定する例を示します。

```
ciscoasa(config)# ddns update method ddns-2
ciscoasa(DDNS-update-method)# ddns both
```

関連コマンド

コマンド	説明
ddns update	DDNS アップデート方式を ASA のインターフェイスまたは DDNS アップデートホスト名に関連付けます。
ddns update method	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
dhcp-client update dns	DHCP クライアントが DHCP サーバーに渡すアップデート パラメータを設定します。
dhcpd update dns	DHCP サーバーによる DDNS アップデートの実行をイネーブルにします。
interval maximum	DDNS アップデート方式によるアップデート試行の最大間隔を設定します。

ddns update

ダイナミックDNS（DDNS）アップデート方式を、ASAインターフェイスまたはアップデートホスト名に関連付けるには、インターフェイス コンフィギュレーション モードで **ddns update** コマンドを使用します。DDNS 更新方式とインターフェイスまたはホスト名とのアソシエーションを、実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

ddns update [*method-name* | **hostname** *hostname*]
no ddns update [*method-name* | **hostname** *hostname*]

構文の説明

hostname	コマンド文字列内の後続の語をホスト名として指定します。
hostname	更新で使用するホスト名を指定します。
method-name	設定するインターフェイスとのアソシエーションの方式名を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

DDNSアップデート方式を定義した後、DDNSアップデートをトリガーするために、そのDDNSアップデート方式を ASA インターフェイスに関連付ける必要があります。

ホスト名は、完全修飾ドメイン名（FQDN）またはホスト名のみを指定できます。ホスト名のみ指定した場合、ASA は、ドメイン名をホスト名に追加して FQDN を作成します。

例

次に、インターフェイス GigabitEthernet0/2 に ddns-2 という名前の DDNS 更新方式およびホスト名 hostname1.example.com を関連付ける例を示します。

```
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# ddns update ddns-2
ciscoasa(config-if)# ddns update hostname hostname1.example.com
```

関連コマンド

コマンド	説明
ddns	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update method	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
dhcp-client update dns	DHCP クライアントが DHCP サーバーに渡すアップデート パラメータを設定します。
dhcpd update dns	DHCP サーバーによる DDNS アップデートの実行をイネーブルにします。
interval maximum	DDNS アップデート方式によるアップデート試行の最大間隔を設定します。

ddns update method

DNS リソースレコード（RR）を動的に更新する方式を作成するには、グローバル コンフィギュレーション モードで **ddns update method** コマンドを使用します。実行コンフィギュレーションからダイナミック DNS（DDNS）更新方式を削除するには、このコマンドの **no** 形式を使用します。

ddns update method *name* ［ **web** { **reference-identity** *name* | **update-type** { **ipv4** | **ipv6** } | **update-url** *url* }］
no ddns update method *name*

構文の説明

name	ダイナミックにDNSレコードを更新するための方式の名前を指定します。
reference-identity	サーバー ID を検証するための参照 ID 名を指定します。
update-type	送信する更新のタイプ（ipv4 または ipv6）を指定します。
update-url	DDNS 更新の更新 URL 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。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.18(1)	サーバー証明書の ID と一致するように設定されている参照 ID 名を指定するオプションが追加されました。

使用上のガイドライン

DDNS は、DNS で保持されている名前/アドレスおよびアドレス/名前のマッピングを更新します。**ddns update method** コマンドで設定する更新方式により、DDNS 更新の実行方法と実行頻度が決まります。DDNS 更新を実行するための 2 つの方式（RFC 2136 で規定されている IETF 標準、および一般的な HTTP 方式）のうち、ASA のこのリリースでは、IETF 方式をサポートしています。

名前とアドレスのマッピングは、次の 2 タイプのリソース レコード（RR）に保持されます。

- A リソース レコードには、ドメイン名から IP アドレスへのマッピングが含まれます。
- PTR リソース レコードには、IP アドレスからドメイン名へのマッピングが含まれます。

DDNS アップデートを使用して、DNS の A RR タイプと PTR RR タイプとの間で一貫した情報を保持できます。

（注） **ddns update method** コマンドが機能する前に、インターフェイスでドメインルックアップを有効にした状態で、**dns** コマンドを使用して到達可能なデフォルトの DNS サーバーを設定する必要があります。

例

次に、ddns-2 という名前の DDNS 更新方式を設定する例を示します。

```
ciscoasa(config)# ddns update method ddns-2
```

参照 ID オブジェクトを使用して DDNS サーバーへの接続を検証するには、**reference-identity** *ref_id_name* を使用します。参照 ID オブジェクトは、一致基準を指定し、**crypto ca reference-identity refidname** を使用して作成されます。参照 ID が設定されている場合、DDNS サーバーに接続を試みる際に、ASA は一致するホスト名でサーバー証明書の ID を検証します。ホストの解決に失敗するか、一致するものが見つからない場合、エラーメッセージが表示されて接続が終了します。

```
asa(config-aaa-server-host)# ddns update method tempddns
asa(DDNS-update-method)# web ?

dynupd-method mode commands/options:
  reference-identity  Enter Reference-identity name to validate server identity
  update-type         Configure the type of update to be sent
  update-url          Configure Update URL for DDNS update
```

設定された参照 ID は、show running-config コマンドで表示されます。

```
asa(DDNS-update-method)# web reference-identity dyndns
asa(DDNS-update-method)# show running-config ddns
ddns update method tempddns
web update-url
pwd@10.x.x.x/update?hostname=<>https://admin:pwd@10.x.x.x/update?hostname=<;h>&myip=<a>
web update-type ipv4
web reference-identity dyndns
interval maximum 0 0 2 0
!
asa(DDNS-update-method)#

asa(DDNS-update-method)# sh ddns update method
Dynamic DNS Update Method: dyndns
Dynamic DNS updated via HTTP(s) protocols
  URL used to update record:
pwd@10.x.x.x/update?hostname=<>https://admin:pwd@10.x.x.x/update?hostname=<;h>&myip=<a>
```

```
  Update type configured: ipv4
  Configured reference-identity name: dyndns
  Maximum update interval: 0 days 0 hours 2 minutes 0 seconds
asa(DDNS-update-method)#
```

関連コマンド

コマンド	説明
ddns	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update	DDNS アップデート方式を ASA のインターフェイスまたは DDNS アップデートホスト名に関連付けます。
dhcp-client update dns	DHCP クライアントが DHCP サーバーに渡すアップデート パラメータを設定します。
dhcpd update dns	DHCP サーバーによるダイナミック DNS アップデートの実行をイネーブルにします。
interval maximum	DDNS アップデート方式によるアップデート試行の最大間隔を設定します。

debug

特定機能のデバッグメッセージを表示するには、特権 EXEC モードで **debug** コマンドを使用します。デバッグ メッセージの表示を無効にするには、このコマンドの **no** 形式を使用します。

debug feature [*subfeature*] [*level*]
no debug *feature* [*subfeature*]

構文の説明

level	（オプション）デバッグ レベルを指定します。このレベルは、一部の機能で使用できない場合があります。
feature	デバッグをイネーブルにする機能を指定します。使用可能な機能を表示するには、**debug ?** コマンドを使用して CLI ヘルプを表示します。
subfeature	（オプション）機能によっては、1 つ以上のサブ機能のデバッグ メッセージをイネーブルにできます。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.13(1)	**debug crypto ca** コマンドが変更され、オプションが少なくなり、デバッグレベルが 14 に制限されました。
9.18(1)	このコマンドは、パスモニタリングのデバッグを含めるように変更されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカルサポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug**コマンドは、ネットワークトラフィックが少なく、ユーザも少ないときに使用することを推奨します。デ

バッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が低くなります。

バージョン 9.13(1) 以降、**debug crypto ca** コマンドに対するオプション、すなわち **debug crypto ca transactions** および **debug crypto ca messages** は、すべての該当するコンテンツを **debug crypto ca** コマンド自体に提供するために統合されています。また、使用可能なデバッグ レベルの数が 14 に削減されました。

例

次に、**debug aaa internal** コマンドの出力例を示します。

```
ciscoasa(config)# debug aaa internal
debug aaa internal enabled at level 1
ciscoasa(config)# uap allocated. remote address: 10.42.15.172, Session_id: 2147483841
uap freed for user . remote address: 10.42.15.172, session id: 2147483841
```

次に、変更された **debug crypto ca** コマンドを示します。

```
(config)# debug crypto ca ?
exec mode commands/options:
  <1-14>                   Specify an optional debug level (default is 1)
  cluster                  debug PKI cluster
  cmp                      debug the CMP transactions
  periodic-authentication  debug PKI peroidic authentication
  <cr>
```

default（crl 設定）

すべてのCRLパラメータをシステムデフォルト値に戻すには、CRL設定コンフィギュレーション モードで **default** コマンドを使用します。

default

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドの呼び出しは、アクティブなコンフィギュレーションには含まれません。crl 設定コンフィギュレーションモードは、暗号CAトラストポイントコンフィギュレーションモードからアクセスできます。これらのパラメータは、LDAPサーバーで必要な場合のみ使用されます。

例

次に、ca-crl コンフィギュレーション モードを開始して、CRL コマンド値をデフォルトに戻す例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# default
ciscoasa(ca-crl)#
```

関連コマンド

コマンド	説明
crl configure	crl 設定コンフィギュレーション モードを開始します。

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。
protocol ldap	CRL の取得方法として LDAP を指定します。

default（インターフェイス）

インターフェイスコマンドをシステムデフォルト値に戻すには、インターフェイス コンフィギュレーション モードで **default** コマンドを使用します。

default*command*

構文の説明

command デフォルトに設定するコマンドを指定します。次に例を示します。

```
default activation key
```

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは実行時のコマンドです。入力しても、アクティブなコンフィギュレーションの一部にはなりません。

例

次に、インターフェイス コンフィギュレーション モードを開始して、セキュリティ レベルをデフォルトに戻す例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# default security-level
```

関連コマンド

コマンド	説明
interface	インターフェイス コンフィギュレーション モードを開始します。

default（IPv6 ルータ OSPF）

OSPFv3 パラメータをデフォルト値に戻すには、IPv6 ルータ OSPF コンフィギュレーション モードで **default** コマンドを使用します。

default [**area** | **auto-cost** | **default-information** | **default-metric** | **discard-route** | **distance** | **distribute-list** | **ignore** | **log-adjacency-changes** | **maximum-paths** | **passive-interface** | **redistribute** | **router-id** | **summary-prefix** | **timers**]

構文の説明

area	（オプション）OSPFv3 エリア パラメータを指定します。
auto-cost	（オプション）帯域幅に従って OSPFv3 インターフェイスのコストを指定します。
default-information	（オプション）デフォルトの情報を配布します。
default-metric	（オプション）再配布されるルートのメトリックを指定します。
discard-route	（オプション）廃棄ルートの導入をイネーブルまたはディセーブルにします。
distance	（オプション）アドミニストレーティブ ディスタンスを指定します。
distribute-list	（オプション）ルーティング アップデートでネットワークをフィルタリングします。
ignore	（オプション）特定のイベントを無視します。
log-adjacency-changes	（任意）隣接ステートの変更を記録します。
maximum-paths	（オプション）複数のパスを介してパケットを転送します。
passive-interface	（オプション）インターフェイス上のルーティング アップデートを抑制します。
redistribute	（オプション）別のルーティング プロトコルからの IPv6 プレフィックスを再配布します。
router-id	（オプション）指定したルーティング プロセスのルータ ID を指定します。
summary-prefix	（オプション）OSPFv3 集約プレフィックスを指定します。
timers	（任意）OSPFv3 タイマーを指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

OSPFv3 パラメータのデフォルト値をリセットするには、このコマンドを使用します。

例

次に、OSPFv3 タイマー パラメータをデフォルト値にリセットする例を示します。

```
ciscoasa(config-router)# d
efault timers spf
```

関連コマンド

コマンド	説明
distance	OSPFv3 ルーティング プロセスのアドミニストレーティブ ディスタンスを指定します。
default-information originate	OSPFv3 ルーティング ドメインへのデフォルトの外部ルートを生成します。
log-adjacency-changes	OSPFv3 ネイバーが起動または停止したときに、ルータが syslog メッセージを送信するように設定します。

default（パラメータ）

IP オプションインスペクション時に特定のアクションを指定しないオプションのデフォルトアクションを定義するには、パラメータ コンフィギュレーション モードで **default** コマンドを使用します。システムのデフォルトに戻すには、このコマンドの **no** 形式を使用します。

default action { **allow** | **clear** }
no default action { **allow** | **clear** }

構文の説明

allow	IP オプション インスペクション ポリシーマップに明示的に指定されていないオプションを含んでいるパケットを許可します。
clear	IP オプション インスペクション ポリシーマップに明示的に指定されていないオプションをパケット ヘッダーから削除してから、パケットを許可します。

コマンド デフォルト

デフォルトでは、IP オプション インスペクションはルータアラート オプションを許可しますが、その他の IP オプションを含んでいるパケットはドロップします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
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、特定の IP オプションを持つどの IP パケットが ASA を通過できるかを制御できます。変更せずにパケットを通過させたり、指定されている IP オプションをクリアしてからパケットを通過させたりできます。

例

次に、IP オプションインスペクションのアクションをポリシーマップで設定する例を示します。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
```

```
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# default action clear
ciscoasa(config-pmap-p)# router-alert action allow
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

default（時間範囲）

absolute コマンドと **periodic** コマンドをデフォルト設定に戻すには、時間範囲コンフィギュレーション モードで **default** コマンドを使用します。

default { **absolute** | **periodic** *days-of-the-week time* **to** [*days-of-the-week*] *time* }

構文の説明

absolute	時間範囲が有効になる絶対時間を定義します。
days-of-the-week	最初の days-of-the-week 引数は、関連付けられている有効時間範囲が開始する日または曜日です。2 番めの days-of-the-week 引数は、関連付けられているステートメントの有効期間が終了する日または曜日です。 この引数は、単一の曜日または曜日の組み合わせです（Monday（月曜日）、Tuesday（火曜日）、Wednesday（水曜日）、Thursday（木曜日）、Friday（金曜日）、Saturday（土曜日）、および Sunday（日曜日））。他に指定できる値は、次のとおりです。 • daily：月曜日～日曜日 • weekdays：月曜日～金曜日 • weekend：土曜日と日曜日 終了の曜日が開始の曜日と同じ場合は、終了の曜日を省略できます。
periodic	時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定します。
time	時刻を HH:MM 形式で指定します。たとえば、午前 8 時は 8:00、午後 8 時は 20:00 とします。
to	「開始時刻から終了時刻まで」の範囲を入力するには、**to** キーワードを入力する必要があります。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

終了の days-of-the-week 値が開始の days-of-the-week 値と同じ場合、終了の days-of-the-week 値を省略できます。

time-range コマンドに **absolute** 値と **periodic** 値の両方が指定されている場合、**periodic** コマンドは absolute start 時刻を経過した後にのみ評価の対象になり、absolute end 時刻を経過した後は評価の対象にはなりません。

時間範囲機能は、ASA のシステムクロックに依存しています。ただし、この機能は NTP 同期を使用すると最適に動作します。

例

次に、**absolute** キーワードの動作をデフォルトに戻す例を示します。

```
ciscoasa(config-time-range)# default absolute
```

関連コマンド

コマンド	説明
absolute	時間範囲が有効になる絶対時間を定義します。
periodic	時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定します。
time-range	時間に基づいて ASA のアクセスコントロールを定義します。

default-acl

ポスチャ検証が失敗したNACフレームワークセッションのデフォルトのACLとして使用されるようにACLを指定するには、nacポリシーnacフレームワーク コンフィギュレーション モードで **default-acl** コマンドを使用します。このコマンドをNACポリシーから削除するには、このコマンドの **no** 形式を使用します。

[**no**] **default-acl** *acl-name*

構文の説明

acl-name	セッションに適用されるアクセス コントロール リストの名前を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.0(2)	コマンド名から「nac-」が削除されました。コマンドが、グループ ポリシー コンフィギュレーション モードからnacポリシーnacフレームワーク コンフィギュレーション モードに移動されました。

使用上のガイドライン

各グループ ポリシーは、ポリシーに一致し、NAC に対して適格なホストに適用されるデフォルト ACL を指しています。ASA は、ポスチャ検証の前に NAC のデフォルト ACL を適用します。ポスチャ検証の後、ASAはデフォルトACLをリモートホストのアクセスコントロールサーバーから取得したACLに置き換えます。ポスチャ確認が失敗した場合は、デフォルト ACL がそのまま使われます。

また、ASA は、クライアントレス認証がイネーブルになっている（デフォルト設定）場合にも、NAC のデフォルト ACL を適用します。

例

次に、ポスチャ検証が成功する前に適用される ACL として acl-1 を指定する例を示します。

```
ciscoasa(config-group-policy)# default-acl acl-1
ciscoasa(config-group-policy)
```

次の例では、デフォルト グループ ポリシーから ACL を継承しています。

```
ciscoasa(config-group-policy)# no default-acl
ciscoasa(config-group-policy)
```

関連コマンド

コマンド	説明
nac-policy	Cisco NAC ポリシーを作成してアクセスし、そのタイプを指定します。
nac-settings	NAC ポリシーをグループ ポリシーに割り当てます。
debug nac	NAC フレームワーク イベントのロギングをイネーブルにします。
show vpn-session_summary.db	IPsec、WebVPN、および NAC セッションの数を表示します。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。

default-domain

グループポリシーのユーザーのデフォルトドメイン名を設定するには、グループ ポリシー コンフィギュレーション モードで **default-domain** コマンドを使用します。ドメイン名を削除するには、このコマンドの **no** 形式を使用します。

default-domain { **value** *domain-name* | **none** }
no default-domain [*domain-name*]

構文の説明

none	デフォルトドメイン名がないことを指定します。デフォルトドメイン名にヌル値を設定して、デフォルトドメイン名を拒否します。デフォルトまたは指定したグループポリシーのデフォルトドメイン名は継承されません。
value *domain-name*	グループのデフォルト ドメイン名を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ユーザーがドメイン名を継承しないようにするには、**default-domain none** コマンドを使用します。

ASA は、ドメインフィールドを省略した DNS クエリに追加するために、AnyConnect クライアント または従来の VPN クライアント（IPsec/IKEv1）にデフォルトドメイン名を渡します。このドメイン名は、トンネルパケットにのみ適用されます。デフォルト ドメイン名がない場合、ユーザーはデフォルト グループ ポリシーのデフォルト ドメイン名を継承します。

デフォルト ドメイン名に使用できるのは、英数字、ハイフン（-）、およびピリオド（.）のみです。

例

次に、FirstGroup という名前のグループ ポリシーに対して、FirstDomain のデフォルト ドメイン名を設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# default-domain value FirstDomain
```

関連コマンド

コマンド	説明
split-dns	スプリット トンネルを介して解決されるドメインのリストを提供します。
split-tunnel-network-list	トンネリングが必要なネットワークと不要なネットワークを区別するために、ASA が使用するアクセスリストを指定します。
split-tunnel-policy	IPsec クライアントが条件に応じてパケットを暗号化形式で IPsec トンネルを経由して転送したり、クリア テキスト形式でネットワーク インターフェイスに転送したりできるようにします。

default enrollment

すべての登録パラメータをシステムデフォルト値に戻すには、クリプト CA トラストポイント コンフィギュレーション モードで **default enrollment** コマンドを使用します。

default enrollment

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドの呼び出しは、アクティブなコンフィギュレーションには含まれません。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、すべての登録パラメータをトラストポイント central 内のデフォルト値に戻す例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# default enrollment
ciscoasa(ca-trustpoint)#
```

関連コマンド

コマンド	説明
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。
crl configure	CRL コンフィギュレーション モードを開始します。

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。

default-group-policy（imap4s、pop3s、smtps）（廃止）

（注） このコマンドをサポートする最後のリリースは、7.5(1) でした。

電子メールプロキシ設定でグループポリシーが指定されない場合に使用するグループポリシーの名前を指定するには、さまざまなコンフィギュレーション モードで **default-group-policy** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

default-group-policy*groupname*
nodefault-group-policy

構文の説明

groupname	デフォルト グループ ポリシーとして使用する、設定済みのグループ ポリシーを指定します。**group-policy** コマンドを使用して、グループポリシーを設定します。

コマンド デフォルト

DfltGrpPolicy という名前のデフォルト グループ ポリシーは、常に、に存在します。この **default-group-policy** コマンドを使用すると、作成したグループポリシーを、電子メールプロキシセッション用のデフォルトグループポリシーとして置き換えることができます。または、DfltGrpPolicy を編集することもできます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
Imap4s コンフィギュレーション	• 対応	—	• 対応	—	—
Pop3s コンフィギュレーション	• 対応	—	• 対応	—	—
smtps コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

Version	変更内容
7.0(1)	このコマンドが追加されました。

Version	変更内容
7.5(2)	このコマンドは廃止されました。

使用上のガイドライン

セッション、IMAP4S セッション、POP3S セッション、および SMTPS セッションには、指定されたグループ ポリシーまたはデフォルト グループ ポリシーが必要です。このコマンドは、該当する電子メール プロキシ モードで使用します。

システムの DefaultGroupPolicy は編集できますが、削除はしないでください。DefaultGroupPolicy の AVP は、次のとおりです。

属性	デフォルト値
wins-server	none
dns-server	none
dhcp-network-scope	none
vpn-access-hours	unrestricted
vpn-simultaneous-logins	3
vpn-idle-timeout	30 分
vpn-session-timeout	none
vpn-filter	none
vpn-tunnel-protocol	WebVPN
ip-comp	disable
re-xauth	disable
group-lock	none
pfs	disable
client-access-rules	none
banner	none
password-storage	disabled
ipsec-udp	disabled
ipsec-udp-port	0
backup-servers	keep-client-config
split-tunnel-policy	tunnelall
split-tunnel-network-list	none

属性	デフォルト値
default-domain	none
split-dns	none
intercept-dhcp	disable
client-firewall	none
secure-unit-authentication	disabled
user-authentication	disabled
user-authentication-idle-timeout	none
ip-phone-bypass	disabled
leap-bypass	disabled
nem	disabled

例

次に、pop3s という名前の POP3S のデフォルト グループ ポリシーを指定する例を示します。

```
ciscoasa
(config)#
 pop3s
ciscoasa(config-webvpn)# default-group-policy pop3s
```

default-group-policy（トンネル グループ一般属性）

ユーザーがデフォルトで継承する属性のセットを指定するには、トンネルグループ一般属性コンフィギュレーション モードで **default-group-policy** コマンドを使用します。デフォルトのグループポリシー名を削除するには、このコマンドの **no** 形式を使用します。

default-group-policy*group-name*
no default-group-policy *group-name*

構文の説明

group-name	デフォルト グループの名前を指定します。

コマンド デフォルト

デフォルト グループ名は DfltGrpPolicy です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

Version	変更内容
7.0(1)	このコマンドが追加されました。
7.1(1)	webvpn コンフィギュレーション モードの **default-group-policy** コマンドは廃止されました。このコマンドは、トンネルグループ一般属性モードの **default-group-policy** コマンドに置き換えられます。

使用上のガイドライン

バージョン 7.1(1) では、このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ一般属性モードの同等のコマンドに変換されます。

デフォルトグループポリシー DfltGrpPolicy には、ASA が初期設定されています。この属性は、すべてのトンネル グループ タイプに適用できます。

例

次に、config-general コンフィギュレーション モードを開始し、ユーザーがデフォルトで、「standard-policy」という IPsec LAN-to-LAN トンネル グループの属性セットを継承するように指定する例を示します。このコマンド セットでは、アカウンティング サーバー、認証サーバー、認可サーバー、およびアドレス プールを定義します。

```
ciscoasa(config)# tunnel-group standard-policy type ipsec-ra
ciscoasa(config)# tunnel-group standard-policy general-attributes
ciscoasa(config-tunnel-general)# default-group-policy first-policy
ciscoasa(config-tunnel-general)# accounting-server-group aaa-server123
ciscoasa(config-tunnel-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
ciscoasa(config-tunnel-general)# authentication-server-group aaa-server456
ciscoasa(config-tunnel-general)# authorization-server-group aaa-server78
ciscoasa(config-tunnel-general)#
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
group-policy	グループ ポリシーを作成または編集します。
show running-config tunnel group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。

default-idle-timeout

WebVPN ユーザーのデフォルト アイドル タイムアウト値を設定するには、webvpn コンフィギュレーション モードで **default-idle-timeout** コマンドを使用します。デフォルトのタイムアウト値をコンフィギュレーションから削除し、デフォルトをリセットするには、このコマンドの **no** 形式を使用します。

default-idle-timeout*seconds*
no default-idle-timeout

構文の説明

seconds	アイドル タイムアウトの秒数を指定します。最小値は 60 秒で、最大値は 1 日（86400 秒）です。

コマンド デフォルト

1800 秒（30 分）。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ユーザーのアイドルタイムアウトが定義されていない場合、値が 0 の場合、または値が有効な値の範囲外である場合に、ASA では、ここで設定した値が使用されます。デフォルト アイドル タイムアウトにより、セッションの失効を回避できます。

クッキーがディセーブルに設定されているブラウザ（またはクッキーを求めた後クッキーを拒否するブラウザ）を使用すると、接続されていないユーザーがセッション データベースに出現する可能性があるため、このコマンドは短時間に設定することを推奨します。許可される最大接続数が（**vpn-simultaneous-logins** コマンドを介して）1 に設定されている場合、最大接続数がすでに存在することがデータベースによって示されるため、ユーザーは再ログインすることができません。アイドル タイムアウトを短く設定すると、このようなファントム セッションを迅速に削除し、ユーザーが再ログインできるようにすることができます。

例

次に、デフォルト アイドル タイムアウトを 1200 秒（20 分）に設定する例を示します。

```
ciscoasa
(config)#
 webvpn
ciscoasa(config-webvpn)# default-idle-timeout 1200
```

関連コマンド

コマンド	説明
vpn-simultaneous-logins	許可される同時 VPN セッションの最大数を設定します。

default-information

EIGRP ルーティングプロセスのデフォルトルート情報候補を制御するには、ルータ EIGRP コンフィギュレーション モードで **default-information** コマンドを使用します。着信更新または発信更新で EIGRP デフォルトルート情報候補を非表示にするには、このコマンドの **no** 形式を使用します。

default-information { **in** | **out** } [*acl-name*]
no default-information { **in** | **out** }

構文の説明

acl-name	（オプション）名前付きの標準アクセス リストを指定します。
in	外部のデフォルトルーティング情報を受け入れるように EIGRP を設定します。
out	外部ルーティング情報をアドバタイズするように EIGRP を設定します。

コマンド デフォルト

外部ルートが受け入れられ、送信されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

アクセスリストが指定されたこのコマンドまたは **default-information** コマンドの **no** 形式のみが実行コンフィギュレーションに表示されます。これは、デフォルトルーティング情報候補がデフォルトで受け入れられ、送信されるためです。このコマンドの **no** 形式には、*acl-name* 引数はありません。

例

次に、外部デフォルト ルート情報またはデフォルト ルート情報候補の受領をディセーブルにする例を示します。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# no default-information in
```

関連コマンド

コマンド	説明
router eigrp	EIGRP ルーティング プロセスを作成し、このプロセスのコンフィギュレーション モードを開始します。

default-information originate

IS-IS ルーティング ドメインへのデフォルト ルートを生成するには、ISIS コンフィギュレーション モードで **default-information originate** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

default-information originate ［ **route-map** *map-name* ］
no default-information originate ［ **route-map** *map-name* ］

構文の説明

route-map	（任意）ルーティング プロセスは、ルート マップが満たされている場合にデフォルト ルートを生成します。
map-name	ルート マップ名。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用して設定されたルータがルーティング テーブルに 0.0.0.0 へのルートを持っている場合、IS-IS は LSP で 0.0.0.0 に対するアドバタイズメントを発信します。

ルート マップが存在しない場合、デフォルトではレベル 2 LSP だけでアドバタイズされます。レベル 1 ルーティングでデフォルト ルートを発見するメカニズムには、最も近いレベル 1 またはレベル 2 ルータを探すというものがあります。最も近いレベル 1 またはレベル 2 ルータは、レベル 1 LSP で Attach ビット（ATT）を調べることにより検出できます。

ルート マップは次の 2 つの目的で使用できます。

- ASA にレベル 1 LSP でデフォルトを生成させます。
- 条件に従って 0/0 をアドバタイズします。

match ip address standard-access-list コマンドを使用することで、ルータが 0/0 をアドバタイズする前に存在している必要がある 1 つ以上の IP ルートを指定できます。

例

次に示す例は、ソフトウェアにデフォルト外部ルートを IS-IS ドメイン内に生成させる例を示します。

```
router isis
! ISIS routes will be distributed into IS-IS
redistribute isis 120 metric
! access list 2 is applied to outgoing routing updates
default-information originate
! access list 2 defined as giving access to network 10.105.0.0
access-list 2 permit 10.105.0.0 0.0.255.255
```

関連コマンド

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

コマンド	説明
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。

コマンド	説明
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。

コマンド	説明
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

default-information originate（アドレス ファミリ）

デフォルトルート（ネットワーク 0.0.0.0）を配布するように Border Gateway Protocol（BGP）ルーティングプロセスを設定するには、アドレス ファミリ コンフィギュレーション モードで default-information originate コマンドを使用します。デフォルトルートのアドバタイズメントをディセーブルにするには、このコマンドの no 形式を使用します。

default-informationoriginate
no default-information originate

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

default-information originate コマンドは、デフォルトルート（ネットワーク 0.0.0.0）をアドバタイズするように BGP ルーティングプロセスを設定するために使用されます。再配布ステートメントも、この設定を完了するように設定されている必要があります。そうでない場合、デフォルト ルートはアドバタイズされません。

BGP の default-information originate コマンドの設定は、network (BGP) コマンドの設定に似ています。ただし、default-information originate コマンドは、ルート 0.0.0.0 の明示的な再配布が必要です。network コマンドでは、ルート 0.0.0.0 が内部ゲートウェイプロトコル（IGP）のルーティングテーブルに存在することのみが必要です。したがって、network コマンドが優先されます。

（注） default-information originate コマンドは、同じルータで neighbor default-originate コマンドとともに設定しないでください。どちらか一方を設定する必要があります。

例

次の例では、ルータは BGP ルーティング プロセスに OSPF からデフォルト ルートを再配布するように設定されます。

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# default-information originate
ciscoasa(config-router-af)# redistribute ospf 100
```

関連コマンド

コマンド	説明
network	Border Gateway Protocol（BGP）およびマルチプロトコル BGP ルーティング プロセスによってアドバタイズされるネットワークを指定します。
neighbor default-originate	BGP スピーカー（ローカル ルータ）にネイバーへのデフォルト ルート 0.0.0.0 の送信を許可して、このルートがデフォルト ルートとして使用されるようにします。

default-information originate（IPv6 ルータ OSPF、ルータ OSPF）

OSPFv2 または OSPFv3 ルーティングドメインへのデフォルトの外部ルートを生成するには、ルータ コンフィギュレーション モードまたは IPv6 ルータ コンフィギュレーション モードで **default-information originate** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

default-information originate [**always**] [**metric** *value*] [**metric-type** { **1** | **2** }] [**route-map** *map-name*]
no default-information originate [**always**] [**metric** *value*] [**metric-type** { **1** | **2** }] [**route-map** *map-name*]

構文の説明

always	（オプション）ソフトウェアにデフォルト ルートがあるかどうかにかかわらず、常に、デフォルト ルートをアドバタイズします。
metric *value*	（オプション）OSPF のデフォルト メトリック値を、0 ～ 16777214 の範囲で指定します。
metric-type {**1** | **2**}	（任意）OSPF ルーティング ドメインにアドバタイズされるデフォルトのルートに関連付けられる外部リンク タイプを指定します。有効な値は、次のとおりです。 • **1**：タイプ 1 外部ルート。 • **2**：タイプ 2 外部ルート。
route-map *map -name*	（オプション）適用するルート マップの名前を指定します。

コマンド デフォルト

デフォルト値は次のとおりです。

- **metric** *value* は 10 です。
- **metric-type** は 2 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
IPv6 ルータ OSPF コンフィギュレーション	• 対応	—	• 対応	—	—
ルータ OSPF コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	OSPFv3 のサポートが追加されました。

使用上のガイドライン

このコマンドの **no** 形式をオプションのキーワードおよび引数とともに使用すると、コマンドからオプションの情報のみが削除されます。たとえば、**no default-information originate metric** *3* コマンドを入力すると、実行コンフィギュレーションのコマンドから **metric** *3* オプションが削除されます。コマンド全体を実行コンフィギュレーションから削除するには、このコマンドの **no** 形式をオプションなしで使用します（**no default-information originate**）。

例

次に、オプションのメトリックおよびメトリックタイプとともに **default-information originate** コマンドを使用する例を示します。

```
ciscoasa(config-rtr)# default-information originate always metric 3 metric-type 2
ciscoasa(config-rtr)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションの OSPFv2 コマンドを表示します。
ipv6 router ospf	IPv6 のルータ コンフィギュレーション モードを開始します。
show running-config ipv6 router	グローバル ルータ コンフィギュレーションの OSPFv3 コマンドを表示します。

default-information originate（ルータ RIP）

RIP へのデフォルトルートを生成するには、ルータ コンフィギュレーション モードで **default-information originate** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

default-information originate ［ **route-map** *name* ］
no default-information originate ［ **route-map** *name* ］

構文の説明

route-map *name*	（任意）適用するルート マップ名。ルート マップが一致すると、ルーティング プロセスによってデフォルト ルートが生成されます。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

default-information originate コマンドで参照されるルートマップは拡張アクセスリストを使用できません。標準のアクセスリストのみを使用できます。

例

次に、デフォルト ルートを RIP に生成する例を示します。

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# default-information originate
```

関連コマンド

コマンド	説明
router rip	RIP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。

コマンド	説明
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

default-language

クライアントレス SSL VPN ページに表示されるデフォルト言語を設定するには、webvpn コンフィギュレーション モードで **default-language** コマンドを使用します。

default-language言語

構文の説明

language	事前にインポート済みの変換テーブルの名前を指定します。

コマンド デフォルト

デフォルト言語は en-us（米国で使用されている英語）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

ASA では、ブラウザベースのクライアントレス SSL VPN 接続を開始するユーザーに表示されるポータルと画面、および AnyConnect VPN クライアントユーザーに表示されるユーザーインターフェイスで使用される言語を変換できます。適切なコンプライアンスを実現するために、language パラメータは RFC-1766 で定義されている形式を使用する必要があります。

クライアントレス SSL VPN ユーザーが最初に ASA に接続しログインする前にデフォルトの言語が表示されます。その後は、トンネルグループ設定またはトンネルポリシー設定およびこれらの設定が参照するカスタマイズに基づいて言語が表示されます。

例

次に、Sales という名前を指定して、デフォルト言語を中国語に変更する例を示します。

```
ciscoasa(config-webvpn)# default-language zh
```

関連コマンド

コマンド	説明
import webvpn translation-table	変換テーブルをインポートします。
revert	キャッシュ メモリから変換テーブルを削除します。
show import webvpn translation-table	インポートした変換テーブルに関する情報を表示します。

default-mapping-rule

マッピングアドレスおよびポート（MAP）ドメイン内のデフォルトマッピングルールを設定するには、MAP ドメインのコンフィギュレーション モードで **default-mapping-rule** コマンドを使用します。基本マッピングルールを削除するには、このコマンドの **no** 形式を使用します。

default-mapping-rule *ipv6_prefix / prefix_length*
no default-mapping-rule *ipv6_prefix / prefix_length*

構文の説明

ipv6_prefix/prefix_length	RFC 6052 に従って IPv4 宛先アドレスを埋め込むために使用される IPv6 プレフィックス。通常のプレフィックスの長さは 64 ですが、使用可能な値は 32、40、48、56、64、または 96 です。埋め込み IPv4 アドレスの後の任意の末尾ビットは 0 に設定されます。

コマンド デフォルト

デフォルト設定はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.13(1)	このコマンドが導入されました。

使用上のガイドライン

ボーダーリレー（BR）デバイスはこのルールを使用し、MAP ドメイン外のすべての IPv4 アドレスを、MAP ドメイン内で動作する IPv6 アドレスに変換します。MAP ドメイン内の MAP-T カスタマーエッジ（CE）デバイスは、このルールを使用して IPv4 デフォルトルートをインストールします。

例

次の例では、1 という名前の MAP-T ドメインを作成して、ドメインの変換ルールを設定しています。

```
ciscoasa(config)# map-domain 1

ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64
```

```
ciscoasa(config-map-domain)# basic-mapping-rule
ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
ciscoasa(config-map-domain-bmr)# start-port 1024
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

関連コマンド

コマンド	説明
basic-mapping-rule	MAP ドメインの基本マッピング ルールを設定します。
default-mapping-rule	MAP ドメインのデフォルト マッピング ルールを設定します。
ipv4-prefix	MAP ドメインの基本マッピング ルールの IPv4 プレフィックスを設定します。
ipv6-prefix	MAP ドメインの基本マッピング ルールの IPv6 プレフィックスを設定します。
map-domain	マッピング アドレスおよびポート（MAP）ドメインを設定します。
share-ratio	MAP ドメインの基本マッピング ルールのポート数を設定します。
show map-domain	マッピング アドレスおよびポート（MAP）ドメインに関する情報を表示します。
start-port	MAP ドメインの基本マッピング ルールの開始ポートを設定します。

default-mcast-group

VTEP 送信元インターフェイスに関連付けられているすべての VXLAN VNI インターフェイスにデフォルトのマルチキャストグループを指定するには、NVE コンフィギュレーション モードで **default-mcast-group** コマンドを使用します。デフォルトグループを削除するには、このコマンドの **no** 形式を使用します。

default-mcast-group*mcast_ip*
no default-mcast-group

構文の説明

mcast_ip	デフォルトのマルチキャスト グループの IP アドレスを設定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

ASA がピア VTEP の背後にあるデバイスにパケットを送信する場合、ASA には次の 2 つの重要な情報が必要です。

- リモート デバイスの宛先 MAC アドレス
- ピア VTEP の宛先 IP アドレス

ASA がこの情報を検出するには 2 つの方法あります。

- 単一のピア VTEP IP アドレスを ASA に静的に設定できます。

手動で複数のピアを定義することはできません。

ASA が VXLAN カプセル化 ARP ブロードキャストを VTEP に送信し、エンド ノードの MAC アドレスを取得します。

- マルチキャストグループは、VNI インターフェイスごとに（または **default-mcast-address** コマンドを使用して VTEP 全体に）設定できます。

ASA は、IP マルチキャスト パケット内の VXLAN カプセル化 ARP ブロードキャスト パケットを VTEP 送信元インターフェイスを経由して送信します。この ARP 要求への応答により、ASA はリモート VTEP の IP アドレスと、リモート エンド ノードの宛先 MAC アドレスの両方を取得することができます。

ASA は VNI インターフェイスのリモート VTEP IP アドレスに対する宛先 MAC アドレスのマッピングを維持します。

VNI インターフェイスごとにマルチキャスト グループを設定していない場合は、デフォルトのグループが使用されます。その VNI インターフェイス レベルでグループを設定している場合は、そのグループがこの設定よりも優先されます。

例

次に、GigabitEthernet 1/1 インターフェイスを VTEP 送信元インターフェイスとして設定し、デフォルトのマルチキャスト グループ 236.0.0.100 を指定する例を示します。

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# nve 1
ciscoasa(cfg-nve)# source-interface outside
ciscoasa(cfg-nve)# default-mcast-group 236.0.0.100
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
default-mcast-group	VTEP 送信元インターフェイスに関連付けられているすべての VNI インターフェイスのデフォルトのマルチキャスト グループを指定します。
encapsulation vxlan	NVE インスタンスを VXLAN カプセル化に設定します。
inspect vxlan	標準 VXLAN ヘッダー形式に強制的に準拠させます。
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
mcast-group	VNI インターフェイスのマルチキャスト グループ アドレスを設定します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
nve-only	VXLAN 送信元インターフェイスが NVE 専用であることを指定します。
peer ip	ピア VTEP の IP アドレスを手動で指定します。
segment-id	VNI インターフェイスの VXLAN セグメント ID を指定します。

コマンド	説明
show arp vtep-mapping	リモート セグメント ドメインにある IP アドレスとリモート VTEP IP アドレス用の VNI インターフェイスにキャッシュされた MAC アドレスを表示します。
show interface vni	VNI インターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス（設定されている場合）のステータス、ならびに関連付けられている NVE インターフェイスを表示します。
show mac-address-table vtep-mapping	リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ2転送テーブル（MACアドレステーブル）を表示します。
show nve	NVEインターフェイスのパラメータ、ステータス、および統計情報とキャリアインターフェイス（送信元インターフェイス）のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。
show vni vlan-mapping	VNI セグメント ID と、VLAN インターフェイスまたはトランスペアレント モードの物理インターフェイス間のマッピングを表示します。
source-interface	VTEP 送信元インターフェイスを指定します。
vtep-nve	VNI インターフェイスを VTEP 送信元インターフェイスに関連付けます。
vxlan port	VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。

default-metric

再配布されるルートの EIGRP メトリックを指定するには、ルータ コンフィギュレーション モードで**default-metric** コマンドを使用します。デフォルト値に戻すには、このコマンドの**no** 形式を使用します。

default-metric *bandwidth delay reliability loading mtu*
no default-metric *bandwidth delay reliability loading mtu*

構文の説明

bandwidth	ルートの最小帯域幅（KB/秒単位）。有効な値は、1 ～ 4294967295 です。
delay	ルート遅延（10 マイクロ秒単位）。有効な値は、1 ～ 4294967295 です。
loading	ルートの有効な帯域幅。1 ～ 255 の数値で表されます（255 は 100 % のロード）。
mtu	許可する MTU の最小値（バイト単位）。有効値は 1 ～ 65535 です。
reliability	正常なパケット伝送の可能性。0 ～ 255 の数値で表されます。値 255 は 100 % の信頼性を意味し、0 は信頼性がないことを意味します。

コマンド デフォルト

デフォルト メトリックなしで再配布できるのは、接続されているルートのみです。再配布される接続ルートのメトリックは、0 に設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

redistribute コマンドで**metric** キーワードおよび属性を使用しない場合は、デフォルト メトリックを使用して、EIGRP にプロトコルを再配布する必要があります。メトリックのデフォルトは、さまざまなネットワークで機能するよう慎重に設定されています。値を変更する場合は、

最大限の注意を払うようにしてください。スタティック ルートから再配布する場合のみ、同じメトリックを維持できます。

IPv6 対応インターフェイスで許可される最小 MTU は 1280 バイトです。ただし、IPsec がインターフェイスでイネーブルになっている場合、MTU 値は、IPsec 暗号化のオーバーヘッドのために 1380 未満に設定できません。インターフェイスを 1380 バイト未満に設定すると、パケットのドロップが発生する可能性があります。

例

次に、再配布された RIP ルート メトリックが EIGRP メトリックに変換される例を示します。使用する値は、次のとおりです。bandwidth = 1000、delay = 100、reliability = 250、loading = 100、および MTU = 1500。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 172.16.0.0
ciscoasa(config-router)# redistribute rip
ciscoasa(config-router)# default-metric 1000 100 250 100 1500
```

関連コマンド

コマンド	説明
router eigrp	EIGRP ルーティング プロセスを作成して、そのプロセスのルータ コンフィギュレーション モードを開始します。
redistribute (EIGRP)	EIGRP ルーティング プロセスにルートを再配布します。

default user group

クラウド Web セキュリティの場合、ASA に入ってくるユーザーのアイデンティティを ASA が判別できない場合のデフォルトのユーザー名やグループを指定するには、パラメータ コンフィギュレーション モードで **default user group** コマンドを使用します。デフォルトのユーザーまたはグループを削除するには、このコマンドの **no** 形式を使用します。パラメータ コンフィギュレーション モードにアクセスするには、まず **policy-map type inspect scansafe** コマンドを入力します。

default { [**user** *username* [**group** *groupname*]]
no default [**user** *username* [**group** *groupname*]

構文の説明

username	デフォルトのユーザー名を指定します。
groupname	デフォルトのグループ名を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASA に入ってくるユーザーのアイデンティティを ASA が判別できない場合、デフォルトのユーザーやグループが HTTP ヘッダーに含まれています。

例

次に、デフォルト名を「Boulder」、グループ名を「Cisco」として設定する例を示します。

```
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# http
ciscoasa(config-pmap-p)# default name Boulder group Cisco
```

関連コマンド

コマンド	説明
class-map type inspect scansafe	ホワイトリストに記載されたユーザーとグループのインスペクション クラス マップを作成します。
default user group	ASA に入ってくるユーザーのアイデンティティを ASA が判別できない場合のデフォルトのユーザー名やグループを指定します。
http[**s**]（パラメータ）	インスペクション ポリシー マップのサービス タイプ（HTTP または HTTPS）を指定します。
inspect scansafe	このクラスのトラフィックに対するクラウド Web セキュリティ インスペクションをイネーブルにします。
license	要求の送信元の組織を示すため、ASA がクラウド Web セキュリティ プロキシ サーバーに送信する認証キーを設定します。
match user group	ユーザーまたはグループをホワイトリストと照合します。
policy-map type inspect scansafe	インスペクション ポリシー マップを作成すると、ルールのために必要なパラメータを設定し、任意でホワイトリストを識別できます。
retry-count	再試行回数値を入力します。この値は、可用性をチェックするために、クラウド Web セキュリティプロキシサーバーをポーリングする前に ASA が待機する時間です。
scansafe	マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可します。
scansafe general-options	汎用クラウド Web セキュリティ サーバー オプションを設定します。
server {**primary** | **backup**}	プライマリまたはバックアップのクラウド Web セキュリティ プロキシ サーバーの完全修飾ドメイン名または IP アドレスを設定します。
show conn scansafe	大文字の Z フラグに示されたようにすべてのクラウド Web セキュリティ接続を表示します。
show scansafe server	サーバーが現在のアクティブ サーバー、バックアップ サーバー、または到達不能のいずれであるか、サーバーのステータスを表示します。
show scansafe statistics	合計と現在の http 接続を表示します。
user-identity monitor	AD エージェントから指定したユーザーまたはグループ情報をダウンロードします。

コマンド	説明
whitelist	トラフィックのクラスでホワイトリスト アクションを実行します。

delay

インターフェイスの遅延値を設定するには、インターフェイス コンフィギュレーション モードで **delay** コマンドを使用します。デフォルトの遅延値に戻すには、このコマンドの **no** 形式を使用します。

delay*delay-time*
no delay

構文の説明

delay-time	遅延時間（10 マイクロ秒単位）。有効な値は、1 ～ 16777215 です。

コマンド デフォルト

デフォルトの遅延はインターフェイス タイプによって異なります。インターフェイスの遅延値を確認するには、 **show interface** コマンドを使用します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.1(6)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

値は 10 マイクロ秒単位で入力します。**show interface** の出力に表示される遅延値は、マイクロ秒単位です。

例

次に、インターフェイスの遅延をデフォルトの 1000 から 2000 に変更する例を示します。**delay** コマンドの前と後に切り捨てられた **show interface** コマンドの出力が含まれ、このコマンドが遅延値にどのように影響を与えるかを示します。遅延値は、**show interface** の出力の 2 行目、DLY ラベルの後に記載されます。

遅延値を 2000 に変更するために入力するコマンドは、**delay 2000** ではなく **delay 200** です。これは、**delay** コマンドで入力する値が 10 マイクロ秒単位であり、**show interface** の出力ではマイクロ秒単位で表示されるためです。

```
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# show interface Ethernet0/0
Interface Ethernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 100 Mbps, DLY 1000 usec
        Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
        MAC address 0013.c480.7e16, MTU 1500
        IP address 10.86.194.224, subnet mask 255.255.254.0! Remainder of the output
removedciscoasa(config-if)# delay 200
ciscoasa(config-if)# show interface Ethernet0/0
Interface Ethernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 100 Mbps, DLY 2000 usec
        Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
        MAC address 0013.c480.7e16, MTU 1500
        IP address 10.86.194.224, subnet mask 255.255.254.0! Remainder of the output
removed
```

関連コマンド

コマンド	説明
show interface	インターフェイスの統計情報および設定を表示します。

delete

フラッシュメモリからファイルを削除するには、特権EXECモードで**delete**コマンドを使用します。

delete［ **/noconfirm** ］［ **/replicate** ］［ **disk0:| disk1:| flash:** ］［ *path* /］*filename*

構文の説明

/noconfirm	（任意）確認のためのプロンプトを表示しないように指定します。
/recursive	（任意）すべてのサブディレクトリの指定されたファイルを再帰的に削除します。
/replicate	（オプション）スタンバイ ユニットの指定されたファイルを削除します。
disk0:	（オプション）内部のフラッシュ メモリを指定します。
disk1:	（オプション）外部フラッシュ メモリ カードを指定します。
filename	削除するファイルの名前を指定します。
flash:	（オプション）内部のフラッシュ メモリを指定します。このキーワードは **disk0** と同じです。
path/	（任意）ファイルのパスに指定します。

コマンド デフォルト

ディレクトリを指定しない場合、ディレクトリはデフォルトで現在の作業ディレクトリになります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

パスを指定しない場合は、現在の作業ディレクトリからファイルが削除されます。ファイルの削除では、ワイルドカードがサポートされています。ファイルを削除する場合、ファイル名のプロンプトが表示され、削除を確認する必要があります。

例

次に、現在の作業ディレクトリからtest.cfgという名前のファイルを削除する例を示します。

```
ciscoasa# delete test.cfg
```

関連コマンド

コマンド	説明
cd	現在の作業ディレクトリから、指定したディレクトリに変更します。
rmdir	ファイルまたはディレクトリを削除します。
show file	指定されたファイルを表示します。

deny-message

WebVPN に正常にログインしたが、VPN 特権を持たないリモートユーザーに配信されるメッセージを変更するには、グループ webvpn コンフィギュレーション モードで **deny-message value** コマンドを使用します。文字列を削除して、リモートユーザーがメッセージを受信しないようにするには、このコマンドの **no** 形式を使用します。

deny-message value *string*
no deny-message value

構文の説明

string	491 文字以下の英数字。特殊文字、スペース、および句読点を含みます。

コマンド デフォルト

デフォルトの拒否メッセージは次のとおりです。「Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features. Contact your IT administrator for more information.」

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.1(1)	このコマンドは、トンネル グループ webvpn コンフィギュレーション モードからグループ webvpn コンフィギュレーション モードに変更されました。

使用上のガイドライン

このコマンドを入力する前に、グローバル コンフィギュレーション モードで **group-policy** *name* **attributes** コマンドを入力してから、**webvpn** コマンドを入力する必要があります。（この手順は、ポリシー name が作成済みであることを前提としています）。

no deny-message none コマンドは、グループ webvpn コンフィギュレーションから属性を削除します。ポリシーは属性値を継承します。

deny-message value コマンドに文字列を入力するときは、コマンドがラップする場合でも続けて入力します。

VPNセッションに使用されるトンネルポリシーとは独立して、ログイン時にリモートユーザーのブラウザにテキストが表示されます。

例

次に、group2という名前の内部グループポリシーを作成する最初のコマンドの例を示します。後続のコマンドによって、このポリシーに関連付けられている拒否メッセージを変更します。

```
ciscoasa(config)# group-policy group2 internal
ciscoasa(config)# group-policy group2 attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# deny-message value "Your login credentials are OK. However,
 you have not been granted rights to use the VPN features. Contact your administrator
for more information."
ciscoasa(config-group-webvpn)
```

関連コマンド

コマンド	説明
clear configure group-policy	すべてのグループポリシーコンフィギュレーションを削除します。
group-policy	グループポリシーを作成します。
group-policy attributes	グループポリシー属性コンフィギュレーションモードを開始します。
show running-config group-policy	指定したポリシーの実行グループポリシーコンフィギュレーションが表示されます。
webvpn	グループポリシーwebvpnコンフィギュレーションモードを開始します。

deny version

SNMP トラフィックの特定のバージョンを拒否するには、SNMP マップ コンフィギュレーション モードで **deny version** コマンドを使用します。このコマンドをディセーブルにするには、このコマンドの **no** 形式を使用します。

deny version *version*
no deny version *version*

構文の説明

version ASA がドロップする SNMP トラフィックのバージョンを指定します。有効な値は **1**、**2**、**2c**、および **3** です。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

SNMP トラフィックを特定の SNMP バージョンに制限するには、**deny version** コマンドを使用します。以前のバージョンの SNMP はセキュリティがより低いため、セキュリティ ポリシーで SNMP トラフィックを Version 2 に制限できます。グローバル コンフィギュレーション モードで **snmp-map** コマンドを入力してアクセスできる **snmp-map** コマンドを使用して設定する SNMP マップ内で、**deny version** コマンドを使用します。SNMP マップの作成後に、**inspect snmp** コマンドを使用してこのマップをイネーブルにし、**service-policy** コマンドを使用して 1 つ以上のインターフェイスに適用します。

例

次に、SNMP トラフィックを指定し、SNMP マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイス適用する例を示します。

```
ciscoasa(config)# access-list snmp-acl permit tcp any any eq 161

ciscoasa(config)# access-list snmp-acl permit tcp any any eq 162
```

```
ciscoasa(config)# class-map snmp-port

ciscoasa(config-cmap)# match access-list snmp-acl
ciscoasa(config-cmap)# exit
ciscoasa(config)# snmp-map inbound_snmp
ciscoasa(config-snmp-map)# deny version 1
ciscoasa(config-snmp-map)# exit
ciscoasa(config)# policy-map inbound_policy

ciscoasa(config-pmap)# class snmp-port
ciscoasa(config-pmap-c)# inspect snmp inbound_snmp

ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy inbound_policy interface outside
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
inspect snmp	SNMP アプリケーション インスペクションをイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
snmp-map	SNMP マップを定義し、SNMP マップ コンフィギュレーション モードをイネーブルにします。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

description

指定したコンフィギュレーション ユニット（たとえば、コンテキスト、オブジェクトグループ、またはDAP レコード）に対する説明を追加するには、各コンフィギュレーション モードで **description** コマンドを使用します。説明を削除するには、このコマンドの **no** 形式を使用します。

description*text*
no description

構文の説明

text	説明を最大200文字のテキスト文字列で設定します。説明は、コンフィギュレーションの情報として役立ちます。ダイナミック アクセス ポリシー レコード モードの場合、最大長は 80 文字です。イベント マネージャ アプレットの場合、最大長は 256 文字です。 ストリングに疑問符（?）を含める場合は、不注意からCLIヘルプを呼び出さないように、**Ctrl-V** を入力してから疑問符を入力する必要があります。

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

このコマンドは、さまざまなコンフィギュレーション モードで使用できます。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(2)	ダイナミック アクセス ポリシー レコード コンフィギュレーション モードのサポートが追加されました。
9.2(1)	イベント マネージャ アプレット コンフィギュレーション モードのサポートが追加されました。

例

次に、「管理」コンテキスト コンフィギュレーションに説明を追加する例を示します。

```
ciscoasa(config)# context administrator
ciscoasa(config-context)# description This is the admin context.
ciscoasa(config-context)
# allocate-interface gigabitethernet0/0.1
ciscoasa(config-context)
# allocate-interface gigabitethernet0/1.1
ciscoasa(config-context)
# config-url flash://admin.cfg
```

関連コマンド

コマンド	説明
class-map	**policy-map** コマンドのアクションを適用するトラフィックを指定します。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
object-group	**access-list** コマンドに含めるトラフィックを指定します。
policy-map	**class-map** コマンドで指定したトラフィックに適用するアクションを指定します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。