



# database path コマンド～ dhcp-server コマ ンド

---

# database path

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

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

## 構文の説明

<i>directory-path</i>	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。
<i>mount-name</i>	マウント名を指定します。

## デフォルト

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

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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 コンフィギュ レーション	• Yes	—	• Yes	—	—

## コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

## 使用上のガイドライン

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



(注)

これらの CA ファイルは内部保存ファイルです。変更しないでください。

## 例

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

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

**関連コマンド**

コマンド	説明
<b>crypto ca server</b>	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ユーザはローカル CA を設定および管理できます。
<b>crypto ca server user-db write</b>	ローカル CA データベースに設定されているユーザ情報をディスクに書き込みます。
<b>debug crypto ca server</b>	ユーザがローカル CA サーバを設定する場合にデバッグ メッセージを表示します。
<b>mount</b>	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。
<b>show crypto ca server</b>	ASA の CA コンフィギュレーション の特性を表示します。
<b>show crypto ca server cert-db</b>	CA サーバが発行する証明書を表示します。

# ddns

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

**ddns [both]**

**no ddns [both]**

## 構文の説明

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

## デフォルト

DNS A RR のみを更新します。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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	• Yes	—	• Yes	• Yes	—

## 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
<b>ddns update</b>	DDNS アップデート方式を ASA インターフェイスまたは DDNS アップデート ホスト名に関連付けます。
<b>ddns update method</b>	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。
<b>dhcp-client update dns</b>	DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。
<b>dhcpcd update dns</b>	DHCP サーバによる DDNS アップデートの実行をイネーブルにします。
<b>interval maximum</b>	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

<b>hostname</b>	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。
<i>hostname</i>	更新で使用するホスト名を指定します。
<i>method-name</i>	設定するインターフェイスとのアソシエーションの方式名を指定します。

## デフォルト

デフォルトの動作や値はありません。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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	• Yes	—	• Yes	• Yes	—

## 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
<b>ddns</b>	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。
<b>ddns update method</b>	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。
<b>dhcp-client update dns</b>	DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。
<b>dhcpcd update dns</b>	DHCP サーバによる DDNS アップデートの実行をイネーブルにします。
<b>interval maximum</b>	DDNS アップデート方式によるアップデート試行の最大間隔を設定します。

# ddns update method

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

**ddns update method** *name*

**no ddns update method** *name*

## 構文の説明

*name*                      ダイナミックに DNS レコードを更新するための方式の名前を指定します。

## デフォルト

デフォルトの動作や値はありません。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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	• Yes	—	• Yes	• Yes	—

## コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

## 使用上のガイドライン

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

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

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

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



(注)

**ddns update method** コマンドを実行する前に、インターフェイスでドメイン ルックアップをイネーブルにした状態で、**dns** コマンドを使用して到達可能なデフォルト DNS サーバを設定する必要があります。



**例**

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

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

**関連コマンド**

コマンド	説明
<b>ddns</b>	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。
<b>ddns update</b>	DDNS アップデート方式を ASA インターフェイスまたは DDNS アップデート ホスト名に関連付けます。
<b>dhcp-client update dns</b>	DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。
<b>dhcpd update dns</b>	DHCP サーバによるダイナミック DNS アップデートの実行をイネーブルにします。
<b>interval maximum</b>	DDNS アップデート方式によるアップデート試行の最大間隔を設定します。

# debug

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

**debug** *feature* [*subfeature*] [*level*]

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

## 構文の説明

<i>level</i>	(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。
<i>feature</i>	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、 <b>debug ?</b> コマンドを使用して CLI ヘルプを表示します。
<i>subfeature</i>	(オプション)機能によっては、1 つ以上のサブ機能のデバッグ メッセージをイネーブルにできます。

## デフォルト

デフォルトのデバッグ レベルは 1 です。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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	• Yes	• Yes	• Yes	• Yes	• Yes

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

## 使用上のガイドライン

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

## 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
```

# default (crl 設定)

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

## default

### 構文の説明

このコマンドには引数またはキーワードはありません。

### デフォルト

デフォルトの動作や値はありません。

### コマンドモード

次の表に、コマンドを入力できるモードを示します。

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	• Yes	—	• Yes	—	—

### コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

### 使用上のガイドライン

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

### 例

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

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

### 関連コマンド

コマンド	説明
<b>crl configure</b>	crl 設定コンフィギュレーションモードを開始します。
<b>crypto ca trustpoint</b>	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。
<b>protocol ldap</b>	CRL の取得方法として LDAP を指定します。

# default(インターフェイス)

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

## default command

### 構文の説明

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

### デフォルト

デフォルトの動作や値はありません。

### コマンドモード

次の表に、コマンドを入力できるモードを示します。

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	• Yes	• Yes	• Yes	• Yes	—

### コマンド履歴

リリース	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
<b>interface</b>	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

<b>area</b>	(オプション)OSPFv3 エリア パラメータを指定します。
<b>auto-cost</b>	(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。
<b>default-information</b>	(オプション)デフォルトの情報を配布します。
<b>default-metric</b>	(オプション)再配布されるルートのもトリックを指定します。
<b>discard-route</b>	(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。
<b>distance</b>	(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。
<b>distribute-list</b>	(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。
<b>ignore</b>	(オプション)特定のイベントを無視します。
<b>log-adjacency-changes</b>	(任意)隣接ステートの変更を記録します。
<b>maximum-paths</b>	(オプション)複数のパスを介してパケットを転送します。
<b>passive-interface</b>	(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。
<b>redistribute</b>	(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。
<b>router-id</b>	(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。
<b>summary-prefix</b>	(オプション)OSPFv3 集約プレフィックスを指定します。
<b>timers</b>	(任意)OSPFv3 タイマーを指定します。

## デフォルト

デフォルトの動作や値はありません。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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	• Yes	—	• Yes	—	—

---

**コマンド履歴**

リリース	変更内容
9.0(1)	このコマンドが追加されました。

---

**使用上のガイドライン**

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

---

**例**

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

```
ciscoasa(config-router)# default timers spf
```

---

**関連コマンド**

コマンド	説明
<b>distance</b>	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。
<b>default-information originate</b>	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。
<b>log-adjacency-changes</b>	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спек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

<b>allow</b>	IP オプション インспек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。
<b>clear</b>	IP オプション インспекション ポリシー マップに明示的に指定されていないオプションをパケット ヘッダーから削除してから、パケットを許可します。

## デフォルト

デフォルトでは、IP オプション インспек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	• Yes	• Yes	• Yes	• Yes	—

## 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спек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спек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спек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
<b>class</b>	ポリシー マップのクラス マップ名を指定します。
<b>class-map type inspect</b>	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。
<b>policy-map</b>	レイヤ 3/4 のポリシー マップを作成します。
<b>show running-config policy-map</b>	現在のポリシー マップ コンフィギュレーションをすべて表示します。



## default (時間範囲)

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

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

### 構文の説明

<b>absolute</b>	時間範囲が有効になる絶対時間を定義します。
<i>days-of-the-week</i>	最初の <i>days-of-the-week</i> 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 番目の <i>days-of-the-week</i> 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。 <ul style="list-style-type: none"> <li>• <b>daily</b>: 月曜日～日曜日</li> <li>• <b>weekdays</b>: 月曜日～金曜日</li> <li>• <b>weekend</b>: 土曜日と日曜日</li> </ul> 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。
<b>periodic</b>	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。
<i>time</i>	時刻を <b>HH:MM</b> 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。
<b>to</b>	「開始時刻から終了時刻まで」の範囲を入力するには、 <b>to</b> キーワードを入力する必要があります。

### デフォルト

デフォルトの動作や値はありません。

### コマンドモード

次の表に、コマンドを入力できるモードを示します。

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
<b>absolute</b>	時間範囲が有効になる絶対時間を定義します。
<b>periodic</b>	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。
<b>time-range</b>	時間に基づいてASAのアクセス コントロールを定義します。

# default-acl

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

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

## 構文の説明

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

## デフォルト

デフォルトの動作や値はありません。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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	• Yes	—	• Yes	—	—

## コマンド履歴

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

## 使用上のガイドライン

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

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

## 例

次に、ポスト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
<b>nac-policy</b>	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。
<b>nac-settings</b>	NAC ポリシーをグループ ポリシーに割り当てます。
<b>debug nac</b>	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。
<b>show vpn-session_summary.db</b>	IPsec、WebVPN、および NAC セッションの数を表示します。
<b>show vpn-session.db</b>	NAC の結果を含む、VPN セッションの情報を表示します。

# default-domain

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

**default-domain** { *value domain-name* | **none** }

**no default-domain** [*domain-name*]

## 構文の説明

<b>none</b>	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。
<b>value domain-name</b>	グループのデフォルト ドメイン名を指定します。

## デフォルト

デフォルトの動作や値はありません。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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	• Yes	—	• Yes	—	—

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

## 使用上のガイドライン

ユーザがドメイン名を継承しないようにするには、**default-domain none** コマンドを使用します。ASAは、ドメイン フィールドを省略した DNS クエリーに追加するために、AnyConnect セキュア モビリティ クライアントまたはレガシーの VPN クライアント (IPsec/IKEv1) にデフォルト ドメイン名を渡します。このドメイン名は、トンネル パケットにのみ適用されます。デフォルト ドメイン名がない場合、ユーザはデフォルト グループ ポリシーのデフォルト ドメイン名を継承します。デフォルト ドメイン名に使用できるのは、英数字、ハイフン(-)、およびピリオド(.)のみです。

## 例

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

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

## 関連コマンド

コマンド	説明
<b>split-dns</b>	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。
<b>split-tunnel-network-list</b>	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。
<b>split-tunnel-policy</b>	IPsec クライアントが条件に応じてパケットを暗号化形式で IPsec トンネルを経由して転送したり、クリア テキスト形式でネットワーク インターフェイスに転送したりできるようにします。

# default enrollment

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

## default enrollment

### 構文の説明

このコマンドには引数またはキーワードはありません。

### デフォルト

デフォルトの動作や値はありません。

### コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

# default-group-policy (imap4s, pop3s, smtps) (廃止)



(注)

このコマンドをサポートする最後のリリースは、7.5(1) でした。

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

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

**no default-group-policy**

## 構文の説明

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

## デフォルト

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

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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	• Yes	—	• Yes	—	—
Pop3s コンフィギュレーション	• Yes	—	• Yes	—	—
smtps コンフィギュレーション	• Yes	—	• Yes	—	—

## コマンド履歴

Version	変更内容
7.0(1)	このコマンドが追加されました。
7.5(2)	このコマンドは廃止されました。



#### 使用上のガイドライン

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

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

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

#### 例

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

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

# default-group-policy (トンネル グループ一般属性)

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

**default-group-policy** *group-name*

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

## 構文の説明

*group-name* デフォルト グループの名前を指定します。

## デフォルト

デフォルト グループ名は DfltGrpPolicy です。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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	• Yes	—	• Yes	—	—

## 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 <b>default-group-policy</b> 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 <b>default-group-policy</b> コマンドに置き換えられています。

## 使用上のガイドライン

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

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

## 例

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

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

---

**関連コマンド**

コマンド	説明
<b>clear-configure tunnel-group</b>	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。
<b>group-policy</b>	グループ ポリシーを作成または編集します。
<b>show running-config tunnel group</b>	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。
<b>tunnel-group general-attributes</b>	名前付きのトンネル グループの一般属性を指定します。

# default-idle-timeout

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

**default-idle-timeout** *seconds*

**no default-idle-timeout**

構文の説明	<i>seconds</i>	アイドルタイムアウトの秒数を指定します。最小値は 60 秒で、最大値は 1 日 (86400 秒) です。
-------	----------------	---

デフォルト	1800 秒 (30 分)。
-------	----------------

コマンドモード	次の表に、コマンドを入力できるモードを示します。
---------	--------------------------

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	• Yes	—	• Yes	—	—

コマンド履歴	リリース	変更内容
	7.0(1)	このコマンドが追加されました。

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

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

---

**例**

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

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

---

**関連コマンド**

コマンド	説明
<b>vpn-simultaneous-logins</b>	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

<i>acl-name</i>	(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。
<b>in</b>	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。
<b>out</b>	外部ルーティング情報をアドバタイズするように EIGRP を設定します。

## デフォルト

外部ルートが受け入れられ、送信されます。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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	• Yes	—	• Yes	• Yes	—

## 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
<b>router eigrp</b>	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作成するには、ISIS コンフィギュレーション モードで **default-information originate** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

**default-information originate [route-map map-name]**

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

## 構文の説明

<b>route-map</b>	(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。
<b>map-name</b>	ルート マップ名。

## デフォルト

このコマンドは、デフォルトでディセーブルになっています。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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	• Yes	—	• Yes	• Yes	—

## コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

## 使用上のガイドライン

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

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

ルート マップは次の 2 つの目的で使用できます。

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

**match ip address standard-access-list** コマンドを使用して、ルータが 0/0 をアドバタイズする前に存在しなければならない 1 つ以上の IP ルートを指定することができます。



## 例

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

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

## 関連コマンド

コマンド	説明
<b>advertise passive-only</b>	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。
<b>area-password</b>	IS-IS エリア認証パスワードを設定します。
<b>authentication key</b>	IS-IS の認証をグローバルで有効にします。
<b>authentication mode</b>	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。
<b>authentication send-only</b>	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。
<b>clear isis</b>	IS-IS データ構造をクリアします。
<b>distance</b>	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。
<b>domain-password</b>	IS-IS ドメイン認証パスワードを設定します。
<b>fast-flood</b>	IS-IS LSP がフルになるように設定します。
<b>hello padding</b>	IS-IS hello をフル MTU サイズに設定します。
<b>hostname dynamic</b>	IS-IS ダイナミック ホスト名機能を有効にします。
<b>ignore-lsp-errors</b>	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。
<b>isis adjacency-filter</b>	IS-IS 隣接関係の確立をフィルタ処理します。
<b>isis advertise-prefix</b>	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。
<b>isis authentication key</b>	インターフェイスに対する認証を有効にします。
<b>isis authentication mode</b>	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。
<b>isis authentication send-only</b>	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。
<b>isis circuit-type</b>	IS-IS で使用される隣接関係のタイプを設定します。
<b>isis csnp-interval</b>	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。
<b>isis hello-interval</b>	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。
<b>isis hello-multiplier</b>	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。
<b>isis hello padding</b>	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。

コマンド	説明
<b>isis lsp-interval</b>	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。
<b>isis metric</b>	IS-IS メトリックの値を設定します。
<b>isis password</b>	インターフェイスの認証パスワードを設定します。
<b>isis priority</b>	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。
<b>isis protocol shutdown</b>	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。
<b>isis retransmit-interval</b>	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。
<b>isis retransmit-throttle-interval</b>	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。
<b>isis tag</b>	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。
<b>is-type</b>	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。
<b>log-adjacency-changes</b>	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。
<b>lsp-full suppress</b>	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。
<b>lsp-gen-interval</b>	LSP 生成の IS-IS スロットリングをカスタマイズします。
<b>lsp-refresh-interval</b>	LSP の更新間隔を設定します。
<b>max-area-addresses</b>	IS-IS エリアの追加の手動アドレスを設定します。
<b>max-lsp-lifetime</b>	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。
<b>maximum-paths</b>	IS-IS のマルチパス ロード シェアリングを設定します。
<b>metric</b>	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。
<b>metric-style</b>	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。
<b>net</b>	ルーティング プロセスの NET を指定します。
<b>passive-interface</b>	パッシブ インターフェイスを設定します。
<b>prec-interval</b>	PRC の IS-IS スロットリングをカスタマイズします。
<b>protocol shutdown</b>	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。
<b>redistribute isis</b>	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。
<b>route priority high</b>	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。
<b>router isis</b>	IS-IS ルーティングをイネーブルにします。
<b>set-attached-bit</b>	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。

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

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

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

**default-information originate**

**no default-information originate**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルトの動作や値はありません。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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	• Yes	—	• Yes	• Yes	—

## 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
<b>network</b>	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。
<b>neighbor default-originate</b>	BGP スピーカー (ローカル ルータ) にネイバーへのデフォルト ルート 0.0.0.0 の送信を許可して、このルートがデフォルト ルートとして使用されるようにします。

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

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

```
default-information originate [always] [metric value] [metric-type {1 | 2}] [route-map map-name]
```

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

## 構文の説明

<b>always</b>	(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。
<b>metric value</b>	(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。
<b>metric-type {1   2}</b>	(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。 <ul style="list-style-type: none"> <li>• 1: タイプ 1 の外部ルート</li> <li>• 2: タイプ 2 の外部ルート</li> </ul>
<b>route-map map-name</b>	(オプション)適用するルート マップの名前を指定します。

## デフォルト

デフォルト値は次のとおりです。

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

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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	• Yes	—	• Yes	—	—
ルータ OSPF コンフィギュレーション	• Yes	—	• Yes	—	—

## コマンド履歴

リリース	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
<b>router ospf</b>	ルータ コンフィギュレーション モードを開始します。
<b>show running-config router</b>	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。
<b>ipv6 router ospf</b>	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。
<b>show running-config ipv6 router</b>	グローバル ルータ コンフィギュレーションの OSPFv3 コマンドを表示します。

# default-information originate (ルータ RIP)

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

**default-information originate** [route-map name]

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

## 構文の説明

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

## デフォルト

このコマンドは、デフォルトでディセーブルになっています。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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	• Yes	—	• Yes	—	—

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



# default-language

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

**default-language** *language*

## 構文の説明

*language* 事前にインポート済みの変換テーブルの名前を指定します。

## デフォルト

デフォルト言語は en-us (米国で使用されている英語) です。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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	• Yes	—	• Yes	—	—

## コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

## 使用上のガイドライン

ASAでは、ブラウザベースのクライアントレス SSL VPN 接続を開始するユーザに表示されるポータルと画面、および AnyConnect VPN クライアント ユーザに表示されるユーザ インターフェイスで使用される言語を変換できます。

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

## 例

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

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

## 関連コマンド

コマンド	説明
<b>import webvpn translation-table</b>	変換テーブルをインポートします。
<b>revert</b>	キャッシュ メモリから変換テーブルを削除します。
<b>show import webvpn translation-table</b>	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-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	• Yes	• Yes	• Yes	—	—

## 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
<b>debug vxlan</b>	VXLAN トラフィックをデバッグします。
<b>default-mcast-group</b>	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。
<b>encapsulation vxlan</b>	NVE インスタンスを VXLAN カプセル化に設定します。
<b>inspect vxlan</b>	標準 VXLAN ヘッダー形式に強制的に準拠させます。
<b>interface vni</b>	VXLAN タギング用の VNI インターフェイスを作成します。
<b>mcast-group</b>	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。
<b>nve</b>	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。
<b>nve-only</b>	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。
<b>peer ip</b>	ピア VTEP の IP アドレスを手動で指定します。
<b>segment-id</b>	VNI インターフェイスの VXLAN セグメント ID を指定します。
<b>show arp vtep-mapping</b>	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。
<b>show interface vni</b>	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。
<b>show mac-address-table vtep-mapping</b>	リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ 2 転送テーブル(MAC アドレス テーブル)を表示します。

コマンド	説明
<b>show nve</b>	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。
<b>show vni vlan-mapping</b>	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。
<b>source-interface</b>	VTEP 送信元インターフェイスを指定します。
<b>vtep-nve</b>	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。
<b>vxlan port</b>	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

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

## デフォルト

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

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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	• Yes	—	• Yes	• Yes	—

## 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
<b>router eigrp</b>	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。
<b>redistribute (EIGRP)</b>	EIGRP ルーティング プロセスにルートを再配布します。

# default user group

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

```
default {[user username] [group groupname]}
```

```
no default [user username] [group groupname]
```

## 構文の説明

<i>username</i>	デフォルトのユーザ名を指定します。
<i>groupname</i>	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	• Yes	• Yes	• Yes	• Yes	—

## コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

## 使用上のガイドライン

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

## 例

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

```
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# http
ciscoasa(config-pmap-p)# default name Boulder group Cisco
```

## 関連コマンド

コマンド	説明
<b>class-map type inspect scansafe</b>	ホワイトリストに記載されたユーザとグループのインスペクション クラス マップを作成します。
<b>http[s]</b> (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。
<b>inspect scansafe</b>	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спекションをイネーブルにします。
<b>license</b>	要求の送信元の組織を示すため、ASAがクラウド Web セキュリティ プロキシ サーバに送信する認証キーを設定します。
<b>match user group</b>	ユーザまたはグループをホワイトリストと照合します。
<b>policy-map type inspect scansafe</b>	インспек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。
<b>retry-count</b>	再試行回数値を入力します。この値は、可用性をチェックするために、クラウド Web セキュリティ プロキシ サーバをポーリングする前に ASA が待機する時間です。
<b>scansafe</b>	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。
<b>scansafe general-options</b>	汎用クラウド Web セキュリティ サーバ オプションを設定します。
<b>server {primary   backup}</b>	プライマリまたはバックアップのクラウド Web セキュリティ プロキシ サーバの完全修飾ドメイン名または IP アドレスを設定します。
<b>show conn scansafe</b>	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。
<b>show scansafe server</b>	サーバが現在のアクティブ サーバ、バックアップ サーバ、または到達不能のいずれであるか、サーバのステータスを表示します。
<b>show scansafe statistics</b>	合計と現在の http 接続を表示します。
<b>user-identity monitor</b>	AD エージェントから指定したユーザまたはグループ情報をダウンロードします。
<b>whitelist</b>	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。

## デフォルト

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

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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	• Yes	—	• Yes	• Yes	—

## コマンド履歴

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

## 使用上のガイドライン

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

## 例

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

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

```
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# show interface Ethernet0/0

Interface Ethernet0/0 "outside", is up, line protocol is up
Hardware is i82546GB rev03, BW 100 Mbps, DLY 1000 usec
```

```
Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
MAC address 0013.c480.7e16, MTU 1500
IP address 10.86.194.224, subnet mask 255.255.254.0
! Remainder of the output removed
```

```
ciscoasa(config-if)# delay 200
ciscoasa(config-if)# show interface Ethernet0/0
```

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

---

#### 関連コマンド

---

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

---

# delete

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

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

## 構文の説明

<b>/noconfirm</b>	(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。
<b>/recursive</b>	(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。
<b>/replicate</b>	(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。
<b>disk0:</b>	(オプション)内部のフラッシュ メモリを指定します。
<b>disk1:</b>	(オプション)外部フラッシュ メモリ カードを指定します。
<b>filename</b>	削除するファイルの名前を指定します。
<b>flash:</b>	(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、 <b>disk0</b> と同じです。
<b>path/</b>	(任意)ファイルのパスに指定します。

## デフォルト

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

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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	• Yes	• Yes	• Yes	• Yes	• Yes

## コマンド履歴

リリース	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
<b>cd</b>	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。
<b>rmdir</b>	ファイルまたはディレクトリを削除します。
<b>show file</b>	指定されたファイルを表示します。

# deny-message

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

**deny-message value** *string*

**no deny-message value**

## 構文の説明

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

## デフォルト

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

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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 <code>webvpn</code> コンフィ ギュレーション	• Yes	—	• Yes	—	—

## コマンド履歴

リリース	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 <code>webvpn</code> コンフィギュレーション モードからグループ <code>webvpn</code> コンフィギュレーション モードに変更されました。

## 使用上のガイドライン

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

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

**deny-message value** コマンドへのストリングの入力時は、コマンドがラップしている場合でも引き続き入力します。

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

## 例

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

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

## 関連コマンド

コマンド	説明
<b>clear configure group-policy</b>	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。
<b>group-policy</b>	グループ ポリシーを作成します。
<b>group-policy attributes</b>	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。
<b>show running-config group-policy</b>	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。
<b>webvpn</b>	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

<i>version</i>	ASAがドロップする SNMP トラフィックのバージョンを指定します。使用可能な値は、 <b>1</b> 、 <b>2</b> 、 <b>2c</b> 、および <b>3</b> です。
----------------	---

## デフォルト

デフォルトの動作や値はありません。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

## 使用上のガイドライン

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

## 例

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

```
ciscoasa(config)# access-list snmp-acl permit tcp any any eq 161
ciscoasa(config)# access-list snmp-acl permit tcp any any eq 162
ciscoasa(config)# class-map snmp-port
ciscoasa(config-cmap)# match access-list snmp-acl
ciscoasa(config-cmap)# exit
ciscoasa(config)# snmp-map inbound_snmp
ciscoasa(config-snmp-map)# deny version 1
```

```

ciscoasa(config-snmp-map)# exit
ciscoasa(config)# policy-map inbound_policy
ciscoasa(config-pmap)# class snmp-port
ciscoasa(config-pmap-c)# inspect snmp inbound_snmp
ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy inbound_policy interface outside

```

## 関連コマンド

コマンド	説明
<b>class-map</b>	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。
<b>inspect snmp</b>	SNMP アプリケーション インспекションをイネーブルにします。
<b>policy-map</b>	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。
<b>snmp-map</b>	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。
<b>service-policy</b>	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

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

## デフォルト

デフォルトの動作や値はありません。

## コマンドモード

このコマンドは、さまざまなコンフィギュレーション モードで使用できます。

## コマンド履歴

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

## 例

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

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

## 関連コマンド

コマンド	説明
<b>class-map</b>	<b>policy-map</b> 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。
<b>context</b>	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。
<b>interface</b>	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。
<b>object-group</b>	<b>access-list</b> コマンドに含めるトラフィックを指定します。
<b>policy-map</b>	<b>class-map</b> コマンドで指定したトラフィックに適用するアクションを指定します。

# dhcp-client broadcast-flag

ASAによる DHCP クライアント パケットへのブロードキャスト フラグの設定を許可するには、グローバル コンフィギュレーション モードで **dhcp-client broadcast-flag** コマンドを使用します。ブロードキャスト フラグを禁止するには、このコマンドの **no** 形式を使用します。

**dhcp-client broadcast-flag**

**no dhcp-client broadcast-flag**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルトでは、ブロードキャスト フラグはディセーブルになっています。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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	• Yes	• Yes	• Yes	• Yes	—

## コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

## 使用上のガイドライン

**ip address dhcp** コマンドを使用してインターフェイスの DHCP クライアントをイネーブルにすると、DHCP クライアントが検出を送信して IP アドレスを要求するときに、このコマンドを使用して、DHCP パケット ヘッダーでブロードキャスト フラグを 1 に設定できます。DHCP サーバはこのブロードキャスト フラグをリッスンし、フラグが 1 に設定されている場合は応答パケットをブロードキャストします。

**no dhcp-client broadcast-flag** コマンドを入力すると、ブロードキャスト フラグは 0 に設定され、DHCP サーバは応答パケットを提供された IP アドレスのクライアントにユニキャストします。

DHCP クライアントは、DHCP サーバからブロードキャスト オファーとユニキャスト オファーの両方を受信できます。

## 例

次に、ブロードキャスト フラグをイネーブルにする例を示します。

```
ciscoasa(config)# dhcp-client broadcast-flag
```

---

**関連コマンド**

コマンド	説明
<b>ip address dhcp</b>	インターフェイスで DHCP クライアントをイネーブルにします。
<b>interface</b>	IP アドレスを設定するために、インターフェイス コンフィギュレーション モードを開始します。
<b>dhcp-client client-id</b>	DHCP 要求パケット オプション 61 を、インターフェイス MAC アドレスが含まれるように設定します。
<b>dhcp-client update dns</b>	DHCP クライアントで DNS 更新をイネーブルにします。

# dhcp-client client-id

デフォルトの内部生成された文字列ではなく、オプション 61 の DHCP 要求パケットに MAC アドレスが保存されるよう強制するには、グローバル コンフィギュレーション モードで **dhcp-client client-id** コマンドを使用します。MAC アドレスを禁止するには、このコマンドの **no** 形式を使用します。

**dhcp-client client-id interface interface\_name**

**no dhcp-client client-id interface interface\_name**

## 構文の説明

<b>interface interface_name</b>	オプション 61 用に MAC アドレスをイネーブルにするインターフェイスを指定します。
---------------------------------	--

## デフォルト

デフォルトでは、オプション 61 には内部生成 ASCII スtringが使用されます。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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	• Yes	• Yes	• Yes	• Yes	—

## コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

## 使用上のガイドライン

**ip address dhcp** コマンドを使用してインターフェイスの DHCP クライアントをイネーブルにすると、一部の ISP でオプション 61 がインターフェイス MAC アドレスであると見なされます。MAC アドレスが DHCP 要求パケットに含まれていない場合、IP アドレスは割り当てられません。**dhcp-client client-id** コマンドを使用して、オプション 61 用にインターフェイス MAC アドレスを含めます。

## 例

次に、外部インターフェイスのオプション 61 用に MAC アドレスをイネーブルに例を示します。

```
ciscoasa(config)# dhcp-client client-id interface outside
```

---

**関連コマンド**

コマンド	説明
<b>ip address dhcp</b>	インターフェイスで DHCP クライアントをイネーブルにします。
<b>interface</b>	IP アドレスを設定するために、インターフェイス コンフィギュレーションモードを開始します。
<b>dhcp-client broadcast-flag</b>	DHCP クライアント パケットにブロードキャストフラグを設定します。
<b>dhcp-client update dns</b>	DHCP クライアントで DNS 更新をイネーブルにします。

# dhcp client route distance

DHCP を通じて学習したルートにアドミニストレーティブ ディスタンスを設定するには、インターフェイス コンフィギュレーション モードで **dhcp client route distance** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**dhcp client route distance** *distance*

**no dhcp client route distance** *distance*

## 構文の説明

*distance* DHCP を通じて学習したルートに適用するアドミニストレーティブ ディスタンス。有効な値は、1 ~ 255 です。

## デフォルト

DHCP を通じて学習したルートには、デフォルトでアドミニストレーティブ ディスタンス 1 が指定されています。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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	• Yes	—	• Yes	—	—

## コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

## 使用上のガイドライン

**dhcp client route distance** コマンドは、ルートが DHCP を通じて学習された場合にのみチェックされます。ルートが DHCP を通じて学習された後に **dhcp client route distance** コマンドが開始されると、指定したアドミニストレーティブ ディスタンスは、学習された既存のルートに影響を与えません。指定したアドミニストレーティブ ディスタンスが設定されるのは、このコマンドの入力後に学習されたルートだけです。

DHCP でルートを取得するには、**ip address dhcp** コマンドで **setroute** オプションを指定する必要があります。

DHCP を複数のインターフェイスで設定している場合、インストールされたルートの優先度を指定するには、各インターフェイスで **dhcp client route distance** コマンドを使用する必要があります。

## 例

次に、GigabitEthernet0/2 で DHCP によりデフォルトルートを取得する例を示します。このルートは、トラッキング エントリ オブジェクト 1 によって追跡されます。SLA 動作によって、outside インターフェイスからの 10.1.1.1 ゲートウェイの可用性がモニタされます。SLA 動作が失敗した場合、GigabitEthernet0/3 で DHCP により取得したバックアップルートが使用されます。バックアップルートには、アドミニストレーティブ ディスタンスに 254 が割り当てられます。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# dhcp client route track 1
ciscoasa(config-if)# ip address dhcp setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# dhcp client route track 1
ciscoasa(config-if)# dhcp client route distance 254
ciscoasa(config-if)# ip address dhcp setroute
```

## 関連コマンド

コマンド	説明
<b>dhcp client route track</b>	DHCP を通じて学習したルートをトラッキング エントリ オブジェクトに関連付けます。
<b>ip address dhcp</b>	指定したインターフェイスに DHCP で取得した IP アドレスを設定します。
<b>sla monitor</b>	SLA モニタリング動作を定義します。
<b>track rtr</b>	SLA をポーリングするためのトラッキング エントリを作成します。



# dhcp client route track

追加ルートをトラッキング済みの指定オブジェクト番号に関連付けるように DHCP クライアントを設定するには、インターフェイス コンフィギュレーション モードで **dhcp client route track** コマンドを使用します。DHCP クライアントのルート トラッキングをディセーブルにするには、このコマンドの **no** 形式を使用します。

**dhcp client route track** *number*

**no dhcp client route track**

## 構文の説明

<i>number</i>	トラッキング エントリのオブジェクト ID。有効な値は、1 ~ 500 です。
---------------	---

## デフォルト

デフォルトの動作や値はありません。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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	• Yes	—	• Yes	—	—

## コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

## 使用上のガイドライン

**dhcp client route track** コマンドは、ルートが DHCP を通じて学習された場合にのみチェックされます。ルートが DHCP から学習された後で **dhcp client route track** コマンドを入力すると、学習された既存のルートはトラッキング オブジェクトに関連付けられません。次の 2 つのコマンドを正しい順序で入力する必要があります。常に **dhcp client route track** コマンドを最初に入力し、その後に **ip address dhcp setroute** コマンドを入力してください。**ip address dhcp setroute** コマンドをすでに入力している場合は削除して、前述した順序で再入力します。指定したトラッキング オブジェクトに関連付けられるのは、このコマンドの入力後に学習されたルートだけです。

DHCP でルートを取得するには、**ip address dhcp** コマンドで **setroute** オプションを指定する必要があります。

DHCP を複数のインターフェイスで設定している場合、インストールされたルートの優先度を指定するには、各インターフェイスで **dhcp client route distance** コマンドを使用する必要があります。

## 例

次に、GigabitEthernet0/2 で DHCP によりデフォルトルートを取得する例を示します。このルートは、トラッキング エントリ オブジェクト 1 によって追跡されます。SLA 動作によって、outside インターフェイスからの 10.1.1.1 ゲートウェイの可用性がモニタされます。SLA 動作が失敗した場合、GigabitEthernet0/3 で DHCP により取得したバックアップルートが使用されます。バックアップルートには、アドミニストレーティブ ディスタンスに 254 が割り当てられます。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# dhcp client route track 1
ciscoasa(config-if)# ip address dhcp setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# dhcp client route distance 254
ciscoasa(config-if)# ip address dhcp setroute
```

## 関連コマンド

コマンド	説明
<b>dhcp client route distance</b>	DHCP を通じて学習したルートにアドミニストレーティブ ディスタンスを割り当てます。
<b>ip address dhcp</b>	指定したインターフェイスに DHCP で取得した IP アドレスを設定します。
<b>sla monitor</b>	SLA モニタリング動作を定義します。
<b>track rtr</b>	SLA をポーリングするためのトラッキング エントリを作成します。

# dhcp-client update dns

DHCP クライアントが DHCP サーバに渡す更新パラメータを設定するには、グローバル コンフィギュレーション モードで **dhcp-client update dns** コマンドを使用します。DHCP クライアントが DHCP サーバに渡すパラメータを削除するには、このコマンドの **no** 形式を使用します。

**dhcp-client update dns [server {both | none}]**

**no dhcp-client update dns [server {both | none}]**

## 構文の説明

<b>both</b>	DHCP サーバが DNS A および PTR リソース レコードの両方を更新するクライアント要求。
<b>none</b>	DHCP サーバが DDNS 更新を実行しないクライアント要求。
<b>server</b>	DHCP サーバがクライアント要求を受信するように指定します。

## デフォルト

デフォルトでは、ASAは、DHCP サーバが PTR RR 更新のみを実行するよう要求します。クライアントはサーバに FQDN オプションを送信しません。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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	• Yes	—	• Yes	• Yes	—

## コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

## 使用上のガイドライン

このコマンドはインターフェイス コンフィギュレーション モードでも入力できますが、ハイフンは使用しません。**dhcp client update dns** コマンドを参照してください。インターフェイス モードで **dhcp client update dns** コマンドを入力すると、グローバル コンフィギュレーション モードのこのコマンドで設定した設定値が上書きされます。

## 例

次に、DHCP サーバが A および PTR RR を更新しないことを要求するようクライアントを設定する例を示します。

```
ciscoasa(config)# dhcp-client update dns server none
```

次に、サーバが A および PTR RR を更新することを要求するようクライアントを設定する例を示します。

```
ciscoasa(config)# dhcp-client update dns server both
```

## 関連コマンド

コマンド	説明
<b>ddns</b>	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。
<b>ddns update</b>	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。
<b>ddns update method</b>	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。
<b>dhcpd update dns</b>	DHCP サーバによる DDNS アップデートの実行をイネーブルにします。
<b>interval maximum</b>	DDNS アップデート方式によるアップデート試行の最大間隔を設定します。

# dhcp-network-scope

ASADHCP サーバが、このグループ ポリシーのユーザにアドレスを割り当てるために使用する必要がある IP アドレスの範囲を指定するには、グループ ポリシー コンフィギュレーション モードで **dhcp-network-scope** コマンドを使用します。実行コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

**dhcp-network-scope** {*ip\_address*} | **none**

**no dhcp-network-scope**

## 構文の説明

<i>ip_address</i>	このポリシー グループのユーザに IP アドレスを割り当てるため、DHCP サーバが使用する必要がある IP サブネットワークを指定します。
<b>none</b>	DHCP サブネットワークをヌル値に設定して、IP アドレスが許可されないようにします。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。

## デフォルト

デフォルトの動作や値はありません。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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	• Yes	—	• Yes	—	—

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

## 使用上のガイドライン

このコマンドを使用すると、別のグループ ポリシーの値を継承できます。値を継承できないようにするには、**dhcp-network-scope none** コマンドを使用します。

## 例

次に、First Group という名前のグループ ポリシーに対して、IP サブネットワーク 10.10.85.1 を設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# dhcp-network-scope 10.10.85.1
```

# dhcp-server

VPN トンネルの確立時にクライアントに IP アドレスを割り当てる DHCP サーバのサポートを設定するには、トンネルグループ一般属性コンフィギュレーションモードで **dhcp-server** コマンドを使用します。このコマンドをデフォルトに戻すには、このコマンドの **no** 形式を使用します。

**dhcp-server** [**link-selection** | **subnet-selection**] **ip1** [**ip2-ip10**]

[**no**] **dhcp-server** [**link-selection** | **subnet-selection**] **ip1** [**ip2-ip10**]

## 構文の説明

<b>ip1</b>	DHCP サーバのアドレス。
<b>ip2-ip10</b>	(オプション)追加の DHCP サーバのアドレス。1 回のコマンドで最大 10 個まで指定できます。また、複数のコマンドにまたがって指定できます。
<b>link-selection</b>	(オプション)ASAが RFC 3527 で規定されている DHCP サブオプション 5「リレー情報オプション 82 のリンク選択のサブオプション」を送信するかどうかを指定します。この設定は、この RFC をサポートしているサーバのみで使用します。
<b>subnet-selection</b>	(オプション)ASAが RFC 3011 で規定されている DHCP オプション 118「IPv4 サブネット選択オプション」を送信するかどうかを指定します。この設定は、この RFC をサポートしているサーバのみで使用します。

## デフォルト

デフォルトの動作や値はありません。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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	• Yes	—	• Yes	—	—

## コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(5)	<b>link-selection</b> および <b>subnet-selection</b> キーワードが追加されました。

## 使用上のガイドライン

この属性は、リモート アクセス トンネルグループタイプに対してのみ適用できます。

**例**

次のコマンドを設定一般コンフィギュレーションモードで入力して、3つのDHCPサーバ(dhcp1、dhcp2、およびdhcp3)をIPsecリモートアクセストンネルグループ「remotegrp」に追加する例を示します。

```
ciscoasa(config)# tunnel-group remotegrp type remote-access
ciscoasa(config)# tunnel-group remotegrp general
ciscoasa(config-tunnel-general)# default-group-policy remotegrp
ciscoasa(config-tunnel-general)# dhcp-server dhcp1 dhcp2 dhcp3
ciscoasa(config-tunnel-general)
```

**関連コマンド**

コマンド	説明
<b>clear-configure tunnel-group</b>	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。
<b>show running-config tunnel group</b>	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。
<b>tunnel-group general-attributes</b>	名前付きのトンネルグループの一般属性を指定します。

