
# acl-netmask-convert コマンド～ auto-update timeout コマンド

## acl-netmask-convert

RADIUS サーバから受信したダウンロード可能な ACL 内のネットマスクをセキュリティ アプライアンスがどのように扱うかを指定するには、AAA サーバ ホスト モードで **acl-netmask-convert** コマンドを使用します。このモードには、**aaa-server host** コマンドを使用してアクセスできます。コマンドを削除するには、このコマンドの **no** 形式を使用します。

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

**no acl-netmask-convert**

**シンタックスの説明**

| | |
|---|---|
| **auto-detect** | セキュリティ アプライアンスが、使用されているネットマスク表現のタイプを判断するように指定します。セキュリティ アプライアンスは、ワイルドカード ネットマスク表現を検出すると、標準ネットマスク表現に変換します。このキーワードの詳細については、「使用上のガイドライン」を参照してください。 |
| **standard** | セキュリティ アプライアンスが、RADIUS サーバから受信したダウンロード可能な ACL に標準ネットマスク表現だけが含まれていると見なすように指定します。ワイルドカード ネットマスク表現からの変換は行われません。 |
| **wildcard** | セキュリティ アプライアンスが、RADIUS サーバから受信したダウンロード可能な ACL にワイルドカード ネットマスク表現だけが含まれていると見なし、ACL のダウンロード時にその表現をすべて標準ネットマスク表現に変換するように指定します。 |

**デフォルト**

デフォルトでは、ワイルドカード ネットマスク表現からの変換は行われません。

**コマンド モード**

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| AAA サーバ ホスト | • | • | • | • | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(4) | このコマンドが導入されました。 |

## 使用上のガイドライン

RADIUS サーバがワイルドカード形式のネットマスクを含むダウンロード可能な ACL を提供する場合は、wildcard キーワードまたは auto-detect キーワードと共に **acl-netmask-convert** コマンドを使用します。セキュリティ アプライアンスは、ダウンロード可能な ACL に標準ネットマスク表現が含まれていると予想します。一方、Cisco Secure VPN 3000 シリーズ コンセントレータは、ダウンロード可能な ACL に、標準ネットマスク表現とは逆のワイルドカード ネットマスク表現が含まれていると予想します。ワイルドカード マスクでは、無視するビット位置には 1 が、一致する必要のあるビット位置には 0 が置かれます。**acl-netmask-convert** コマンドを使用すると、このような違いが、RADIUS サーバ上でダウンロード可能な ACL を設定する方法に及ぼす影響を最小限に抑えることができます。

**auto-detect** キーワードは、RADIUS サーバがどのように設定されているかわからない場合に役立ちます。ただし、ワイルドカード ネットマスク表現に「穴」があると、その表現が正しく検出されず、変換されません。たとえば、ワイルドカード ネットマスク 0.0.255.0 は、第 3 オクテットがどのような数値であっても許可し、Cisco VPN 3000 シリーズ コンセントレータで有効に使用できますが、セキュリティ アプライアンスはこの表現をワイルドカード ネットマスクとして検出できません。

## 例

次の例では、ホスト「192.168.3.4」に対して「srvgrp1」という名前の RADIUS AAA サーバを設定し、ダウンロード可能な ACL のネットマスク変換をイネーブルにして、タイムアウトを 9 秒に、リトライ間隔を 7 秒に、認証ポートを 1650 に設定しています。

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

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **aaa authentication** | **aaa-server** コマンドで指定したサーバ上での、LOCAL、TACACS+、または RADIUS のユーザ認証、または ASDM ユーザ認証をイネーブルまたはディセーブルにします。 |
| **aaa-server host** | AAA サーバ ホスト コンフィギュレーション モードに入ります。このモードでは、ホストに固有の AAA サーバ パラメータを設定できます。 |
| **clear configure aaa-server** | すべての AAA コマンド文をコンフィギュレーションから削除します。 |
| **show running-config aaa-server** | すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。 |

# action-uri

Web サーバの URI を指定してシングル サインオン認証用のユーザ名とパスワードを受信するには、AAA サーバ ホスト コンフィギュレーション モードで **action-uri** コマンドを使用します。これは HTTP Forms コマンドを使用した SSO です。

URI パラメータ値をリセットするには、このコマンドの **no** 形式を使用します。新しい値を入力するには、**action-uri** コマンドを再度使用します。

**action-uri** *string*

**no action-uri**

（注）　HTTP プロトコルで SSO を適切に設定するには、認証と HTTP プロトコル交換についての十分な実用知識が必要です。

## シンタックスの説明

| | |
|---|---|
| *string* | 認証プログラムの URI。複数の行に入力できます。各行の最大文字数は 255 文字です。URI 全体の最大文字数は 2,048 文字です。 |

## デフォルト

デフォルトの値や動作はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

URI（ユニフォーム リソース識別子）は、インターネット上のコンテンツの位置を特定するコンパクトな文字列です。URI で表されるコンテンツには、テキスト ページ、ビデオ クリップ、サウンド クリップ、静止画、動画、プログラムなどがあります。URI の最も一般的な形式は Web ページ アドレスです。Web ページ アドレスは、URI の特定の形式（つまりサブセット）で、Uniform Resource Locator（URL; ユニフォーム リソース ロケータ）と呼ばれます。

セキュリティ アプライアンスの WebVPN サーバは、POST 要求を使用してシングル サインオン認証要求を認証 Web サーバに送信します。この処理が実行されるようにするには、HTTP POST 要求を使用して認証 Web サーバ上のアクション URI にユーザ名とパスワードを渡すようにセキュリティ アプライアンスを設定します。**action-uri** コマンドは、セキュリティ アプライアンスが POST 要求を送信する先の Web サーバ上の認証プログラムの場所と名前を指定します。

認証 Web サーバ上のアクション URI は、認証 Web サーバのログイン ページにブラウザで直接接続するとわかります。ブラウザに表示されるログイン Web ページの URL が、認証 Web サーバのアクション URI です。

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

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

## 例

次の例では、認証データを受信する URI は次のとおりです。

http://www.example.com/auth/index.html/appdir/authc/forms/MCOlogin.fcc?TYPE=33554433&REALMOID=06-000a1311-a828-1185-ab41-8333b16a0008&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fauth.example.com

AAA サーバ ホスト コンフィギュレーション モードで入力した次の例では、www.example.com の上記の URI を指定しています。

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

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

## 関連コマンド

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

# activation-key

セキュリティ アプライアンスのアクティベーション キーを変更し、セキュリティ アプライアンス上で運用されているアクティベーション キーをセキュリティ アプライアンスのフラッシュ パーティションに隠しファイルとして保存されているアクティベーション キーと比較してチェックするには、グローバル コンフィギュレーション モードで **activation-key** コマンドを使用します。

**activation-key [***activation-key-four-tuple*| *activation-key-five-tuple*]

## シンタックスの説明

| | |
|---|---|
| *activation-key-four-tuple* | アクティベーション キー。形式のガイドラインについては、「使用上のガイドライン」を参照してください。 |
| *activation-key-five-tuple* | アクティベーション キー。形式のガイドラインについては、「使用上のガイドライン」を参照してください。 |

## デフォルト

このコマンドにデフォルト設定はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル 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) | セキュリティ アプライアンスでこのコマンドがサポートされるようになりました。 |

## 使用上のガイドライン

各要素の間にスペースを 1 つ入れて、4 つの要素で構成される 16 進数文字列として *activation-key-four-tuple* を入力します。または、各要素の間にスペースを 1 つ入れて、5 つの要素で構成される 16 進数文字列として、*activation-key-five-tuple* を入力します。次に例を示します。

```
0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

先頭部分の 0x 指定子は省略できます。値は、すべて 16 進数であると見なされます。

キーはコンフィギュレーション ファイルに保存されず、シリアル番号に関連付けられます。

## 例

次の例は、セキュリティ アプライアンスのアクティベーション キーを変更する方法を示しています。

```
hostname(config)# activation-key 0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show activation-key** | アクティベーション キーを表示します。 |

# address-pool

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

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

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

## シンタックスの説明

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

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| トンネル グループ一般アトリビュート 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) | このコマンドが導入されました。 |

## 使用上のガイドライン

このコマンドは、インターフェイスごとに 1 つずつ、複数入力できます。インターフェイスを指定しない場合、このコマンドは、明示的に参照されていないすべてのインターフェイスのデフォルトを指定します。

グループ ポリシーの **address-pools** コマンドによるアドレス プールの設定で、トンネル グループの **address-pool** コマンドによるローカル プールの設定が上書きされます。

プールを指定する順序は重要です。セキュリティ アプライアンスは、このコマンドでプールを指定した順序に従って、それらのプールからアドレスを割り当てます。

## 例

config-general コンフィギュレーション モードに入る次の例では、IPSec リモートアクセス トンネル グループ xyz のリモート クライアントにアドレスを割り当てるためのアドレス プールのリストを指定しています。

```
hostname(config)# tunnel-group xyz
hostname(config)# tunnel-group xyz general
hostname(config-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
hostname(config-general)#
```

**関連コマンド**

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

# address-pools（グループ ポリシー）

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

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

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

**address-pools none**

**no address-pools none**

**シンタックスの説明**

| | |
|---|---|
| *address_pool* | **ip local pool** コマンドで設定したアドレス プールの名前を指定します。最大 6 個のローカル アドレス プールを指定できます。 |
| **none** | アドレス プールが何も設定されていないことを示し、他のグループ ポリシーからの継承をディセーブルにします。 |
| **value** | アドレスの割り当てに使用するアドレス プールを 6 個まで指定します。 |

**デフォルト**

デフォルトでは、アドレス プールのアトリビュートを継承できるようになっています。

**コマンド モード**

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グループ ポリシー アトリビュート 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 |
|---|---|
| 7.2(1) | このコマンドが導入されました。 |

**使用上のガイドライン**

このコマンドのアドレス プールの設定で、グループ内のローカル プールの設定が上書きされます。ローカル アドレスの割り当てに使用するローカル アドレス プールを 6 個まで指定できます。

プールを指定する順序は重要です。セキュリティ アプライアンスは、このコマンドでプールを指定した順序に従って、それらのプールからアドレスを割り当てます。

**address-pools none** コマンドは、このアトリビュートが他のポリシー（DefaultGrpPolicy など）から継承されることをディセーブルにします。**no address pools none** コマンドは、コンフィギュレーションから **address-pools none** コマンドを削除し、デフォルトの値（継承可能）に戻します。

**例**

次のコマンドは、config-general コンフィギュレーション モードで入力しています。この例では、GroupPolicy1 で、リモート クライアントにアドレスを割り当てるために pool 1 と pool20 を使用するように設定しています。

```
hostname(config)# ip local pool pool 192.168.10.1-192.168.10.100 mask 255.255.0.0
hostname(config)# ip local pool pool20 192.168.20.1-192.168.20.200 mask 255.255.0.0
hostname(config)# group-policy GroupPolicy1 attributes
hostname(config-group-policy)# address-pools value pool1 pool20
hostname(config-group-policy)#
```

**関連コマンド**

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

# alias

アドレスを手動で変換し、DNS の応答を変更するには、グローバル コンフィギュレーション モードで **alias** コマンドを使用します。**alias** コマンドを削除するには、このコマンドの **no** 形式を使用します。このコマンドの代わりに、外部 NAT コマンド（**nat** コマンドと **static** コマンドを **dns** キーワードと一緒に使用）を使えるようになっています。**alias** コマンドではなく、外部 NAT コマンドを使用することをお勧めします。

**alias** *interface_name mapped_ip real_ip* [*netmask*]

**[no] alias** *interface_name mapped_ip real_ip* [*netmask*]

## シンタックスの説明

| | |
|---|---|
| *interface_name* | マップされた IP アドレスに向かうトラフィックの入力インターフェイス（またはマップされた IP アドレスからのトラフィックの出力インターフェイス）の名前を指定します。 |
| *mapped_ip* | 実際の IP アドレスの変換先の IP アドレスを指定します。 |
| *real_ip* | 実際の IP アドレスを指定します。 |
| *netmask* | （オプション）両方の IP アドレスのサブネット マスクを指定します。ホストのマスクには、**255.255.255.255** と入力します。 |

## デフォルト

このコマンドにデフォルト設定はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル 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 |
|---|---|
| 既存 | このコマンドは既存のものです。 |

## 使用上のガイドライン

このコマンドで、宛先アドレスを変換することもできます。たとえば、ホストがパケットを 209.165.201.1 に送信する場合は、**alias** コマンドを使用することで、トラフィックを他のアドレス（209.165.201.30 など）にリダイレクトできます。

（注）　***alias*** コマンドを他のアドレスへの変換ではなく DNS の書き換えに使用する場合は、エイリアスがイネーブルなインターフェイス上で ***proxy-arp*** をディセーブルにします。***sysopt noproxyarp*** コマンドを使用して、セキュリティ アプライアンスが一般的な NAT 処理のために ***proxy-arp*** でトラフィックを自分自身にプルしないようにしてください。

**alias** コマンドを変更または削除した後は、**clear xlate** コマンドを使用します。

DNS ゾーン ファイルの中に、**alias** コマンドに含まれている「dnat」アドレスの A（アドレス）レコードが存在している必要があります。

**alias** コマンドには、2 つの使用方法があります。次に、その概要を示します。

- セキュリティ アプライアンスが *mapped_ip* 宛てのパケットを取得した場合、そのパケットを *real_ip* に送信するように **alias** コマンドを設定できる。
- セキュリティ アプライアンスが *real_ip* 宛てに DNS パケットを送信し、そのパケットがセキュリティ アプライアンスに戻ってきた場合、DNS パケットに変更を加えて、宛先ネットワーク アドレスを *mapped_ip* にするように **alias** コマンドを設定できる。

**alias** コマンドは、ネットワーク上の DNS サーバと自動的に対話して、エイリアスが設定された IP アドレスへのドメイン名によるアクセスを透過的に処理します。

*real_ip* IP アドレスと *mapped_ip* IP アドレスにネットワーク アドレスを使用すると、ネット エイリアスを指定できます。たとえば、**alias 192.168.201.0 209.165.201.0 255.255.255.224** コマンドを実行すると、209.165.201.1 ～ 209.165.201.30 の各 IP アドレスのエイリアスが作成されます。

**static** コマンドと **access-list** コマンドで **alias** コマンドの *mapped_ip* アドレスにアクセスするには、**access-list** コマンド内で、許可されるトラフィック送信元アドレスとして *mapped_ip* アドレスを指定します。次に例を示します。

```
hostname(config)# alias (inside) 192.168.201.1 209.165.201.1 255.255.255.255
hostname(config)# static (inside,outside) 209.165.201.1 192.168.201.1 netmask
255.255.255.255
hostname(config)# access-list acl_out permit tcp host 192.168.201.1 host 209.165.201.1
eq ftp-data
hostname(config)# access-group acl_out in interface outside
```

内部アドレス 192.168.201.1 を宛先アドレス 209.165.201.1 にマッピングして、エイリアスを指定しています。

内部ネットワーク クライアント 209.165.201.2 が example.com に接続すると、内部クライアントのクエリーに対する外部 DNS サーバからの DNS 応答は、セキュリティ アプライアンスによって 192.168.201.29 へと変更されます。セキュリティ アプライアンスで 209.165.200.225 ～ 209.165.200.254 をグローバル プール IP アドレスとして使用している場合、パケットはセキュリティ アプライアンスに SRC=209.165.201.2 および DST=192.168.201.29 として送信されます。セキュリティ アプライアンスは、アドレスを外部の SRC=209.165.200.254 および DST=209.165.201.29 に変換します。

## 例

次の例では、内部ネットワークに IP アドレス 209.165.201.29 が含まれています。このアドレスはインターネット上にあり、example.com に属しています。内部のクライアントが example.com にアクセスしても、パケットはセキュリティ　アプライアンスに到達しません。クライアントは、209.165.201.29 がローカルの内部ネットワーク上にあると判断するためです。

この動作を修正するには、**alias** コマンドを次のように使用します。

```
hostname(config)# alias (inside) 192.168.201.0 209.165.201.0 255.255.255.224

hostname(config)# show running-config alias
alias 192.168.201.0 209.165.201.0 255.255.255.224
```

次の例では、内部の 10.1.1.11 にある Web サーバ、および 209.165.201.11 で作成された **static** コマンドを示しています。送信元ホストは、外部のアドレス 209.165.201.7 にあります。外部の DNS サーバには、次に示すとおり、www.example.com のレコードが登録されています。

```
dns-server# www.example.com. IN A 209.165.201.11
```

ドメイン名 www.example.com. の末尾のピリオドは必要です。

次に、**alias** コマンドを使用する例を示します。

```
hostname(config)# alias 10.1.1.11 209.165.201.11 255.255.255.255
```

セキュリティ アプライアンスは、内部クライアント用のネーム サーバ応答を 10.1.1.11 に変更して、Web サーバに直接接続できるようにします。

アクセスを可能にするには、次のコマンドも必要です。

```
hostname(config)# static (inside,outside) 209.165.201.11 10.1.1.11

hostname(config)# access-list acl_grp permit tcp host 209.165.201.7 host
209.165.201.11 eq telnet
hostname(config)# access-list acl_grp permit tcp host 209.165.201.11 eq telnet host
209.165.201.7
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **access-list extended** | アクセス リストを作成します。 |
| **clear configure alias** | すべての **alias** コマンドをコンフィギュレーションから削除します。 |
| **show running-config alias** | コンフィギュレーション内の、デュアル NAT コマンドで使用する重複アドレスを表示します。 |
| **static** | ローカル IP アドレスをグローバル IP アドレスに、またはローカル ポートをグローバル ポートにマッピングすることによって、1 対 1 のアドレス変換規則を設定します。 |

# allocate-interface

セキュリティ コンテキストにインターフェイスを割り当てるには、コンテキスト コンフィギュレーション モードで **allocate-interface** コマンドを使用します。コンテキストからインターフェイスを削除するには、このコマンドの **no** 形式を使用します。

**allocate-interface** *physical_interface* [*map_name*] [***visible*** | ***invisible***]

**no allocate-interface** *physical_interface*

**allocate-interface** *physical_interface.subinterface*[**-***physical_interface.subinterface*]
[*map_name*[**-***map_name*]] [***visible*** | ***invisible***]

**no allocate-interface** *physical_interface.subinterface*[**-***physical_interface.subinterface*]

## シンタックスの説明

| | |
|---|---|
| ***invisible*** | （デフォルト）コンテキスト ユーザが **show interface** コマンドで、マッピング名（設定されている場合）だけを表示できるようにします。 |
| *map_name* | （オプション）マッピング名を設定します。<br><br>*map_name* は、インターフェイス ID ではなく、インターフェイスを示す英数字のエイリアスで、コンテキスト内で使用できます。マッピング名を指定しない場合は、コンテキスト内でインターフェイス ID が使用されます。セキュリティを確保するため、コンテキストによって使用されているインターフェイスをコンテキスト管理者に知らせたくない場合があります。<br><br>マッピング名はアルファベットで始まり、アルファベットまたは数字で終わる必要があります。その間の文字には、アルファベット、数字、または下線だけを使用できます。たとえば、次のような名前を使用できます。<br><br>`int0`<br><br>`inta`<br><br>`int_0`<br><br>サブインターフェイスの場合は、マッピング名の範囲を指定できます。<br><br>範囲の詳細については、「使用上のガイドライン」を参照してください。 |
| *physical_interface* | インターフェイス ID（***gigabit*ethernet0/1** など）を設定します。使用できる値については、**interface** コマンドを参照してください。 |
| *subinterface* | サブインターフェイス番号を設定します。サブインターフェイスの範囲を指定できます。 |
| ***visible*** | （オプション）マッピング名を設定した場合でも、コンテキスト ユーザが **show interface** コマンドで、物理インターフェイスのプロパティを表示できるようにします。 |

## デフォルト

デフォルトでは、マッピング名を設定した場合に **show interface** コマンドの出力にインターフェイス ID は表示されません。

**コマンド モード**　次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| コンテキスト コンフィギュレーション | • | • | — | — | • |

**コマンド履歴**

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが導入されました。 |

**使用上のガイドライン**　このコマンドを複数回入力して、異なる範囲を指定できます。マッピング名または表示の設定を変更するには、所定のインターフェイス ID でこのコマンドを再入力し、新しい値を設定します。**no allocate-interface** コマンドを入力して、最初からやり直す必要はありません。**allocate-interface** コマンドを削除すると、セキュリティ アプライアンスによって、コンテキスト内のインターフェイス関連のコンフィギュレーションがすべて削除されます。

透過ファイアウォール モードでは、2 つのインターフェイスのみがトラフィックを通過させることができます。ただし、ASA 適応型セキュリティ アプライアンスでは、専用の管理インターフェイス Management 0/0（物理インターフェイスまたはサブインターフェイス）を管理トラフィック用の第 3 のインターフェイスとして使用できます。

**（注）**　透過モードの管理インターフェイスは、MAC アドレス テーブルにないパケットをそのインターフェイスを通してフラッドしません。

ルーテッド モードでは、必要に応じて、同じインターフェイスを複数のコンテキストに割り当てることができます。透過モードでは、インターフェイスを共有できません。

サブインターフェイスの範囲を指定する場合は、マッピング名の一致範囲を指定できます。範囲については、次のガイドラインに従ってください。

- マッピング名は、アルファベット部分と、それに続く数値部分で構成される必要がある。範囲の両端で、マッピング名のアルファベット部分が一致する必要があります。たとえば、次のような範囲を入力します。

  ```
  int0-int10
  ```

  たとえば、**gigabitethernet0/1.1-gigabitethernet0/1.5 happy1-sad5** と入力すると、コマンドが失敗します。
- マッピング名の数値部分には、サブインターフェイス範囲と同じ個数の数値が含まれる必要がある。たとえば、次の例では、両方の範囲に 100 個のインターフェイスが含まれています。

  ```
  gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100
  ```

  たとえば、**gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int15** と入力すると、コマンドが失敗します。

## 例

次の例は、gigabitethernet0/1.100、gigabitethernet0/1.200、および gigabitethernet0/2.300 ～ gigabitethernet0/1.305 をコンテキストに割り当てる方法を示しています。マッピング名は、int1 ～ int8 です。

```
hostname(config-ctx)# allocate-interface gigabitethernet0/1.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet0/2.305
int3-int8
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **context** | システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードに入ります。 |
| **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 モードに入ります。 |
| **show context** | コンテキストのリスト（システム実行スペース）または現在のコンテキストに関する情報を表示します。 |
| **show interface** | インターフェイスのランタイム ステータスと統計情報を表示します。 |
| **vlan** | サブインターフェイスに VLAN ID を割り当てます。 |

# apcf

Application Profile Customization Framework プロファイルをイネーブルにするには、webvpn モードで **apcf** コマンドを使用します。特定の APCF スクリプトをディセーブルにするには、このコマンドの **no** 形式を使用します。すべての APCF スクリプトをディセーブルにするには、このコマンドの **no** 形式を引数なしで使用します。

**apcf** URL/filename.ext

**no apcf [**URL/filename.ext]

## シンタックスの説明

| | |
|---|---|
| URL | セキュリティ アプライアンス上にロードして使用する APCF プロファイルの場所を指定します。http://、https://、tftp://、ftp://、flash:/、disk#:/' のいずれかの URL を使用します。<br><br>URL には、サーバ、ポート、およびパスが含まれる場合があります。ファイル名だけを指定した場合、デフォルト URL は flash:/ です。**copy** コマンドを使用して、APCF プロファイルをフラッシュ メモリにコピーできます。 |
| filename.extension | APCF カスタマイゼーション スクリプトの名前を指定します。これらのスクリプトは必ず XML 形式です。拡張子は、.xml、.txt、.doc などです。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| WebVPN モード | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

Application Profile Customization Framework オプションでは、非標準の Web アプリケーションや Web リソースが WebVPN 接続で適切にレンダリングされるように、セキュリティ アプライアンスによってそれらの処理を可能にします。APCF プロファイルには、特定のアプリケーションに関して、いつ（事前、事後）、どこの（ヘッダー、本文、要求、応答）、どのデータを変換するかを指定するスクリプトがあります。

複数の APCF プロファイルをセキュリティ アプライアンス上で使用できます。そのようにした場合、セキュリティ アプライアンスは、それらを古いものから新しいものの順に 1 つずつ適用します。

apcf コマンドは、Cisco TAC のサポートがある場合に限り使用することをお勧めします。

## 例

次の例は、フラッシュ メモリの /apcf にある apcf1 という名前の APCF をイネーブルにする方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# apcf flash:/apcf/apcf1.xml
hostname(config-webvpn)#
```

次の例は、myserver という https サーバのポート 1440（パスは /apcf）にある apcf2.xml という名前の APCF をイネーブルにする方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# apcf https://myserver:1440/apcf/apcf2.xml
hostname(config-webvpn)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **proxy-bypass** | 特定のアプリケーションの最小限のコンテンツ リライトを設定します。 |
| **rewrite** | トラフィックがセキュリティ アプライアンスを通過するかどうかを決定します。 |
| **show running config webvpn apcf** | APCF コンフィギュレーションを表示します。 |

# application-access

認証済みの WebVPN ユーザに表示される WebVPN ホームページの Application Access ボックス、およびそれらのユーザがアプリケーションを選択したときに開く Application Access ウィンドウをカスタマイズするには、webvpn カスタマイゼーション モードで **application-access** コマンドを使用します。

**application-access** {**title** | **message** | **window**} {**text** | **style**} *value*

[**no**] **application-access** {**title** | **message** | **window**} {**text** | **style**} *value*

このコマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

## シンタックスの説明

| | |
|---|---|
| **title** | Application Access ボックスのタイトルを変更することを指定します。 |
| **message** | Application Access ボックスのタイトルの下に表示されるメッセージを変更することを指定します。 |
| **window** | Application Access ウィンドウを変更することを指定します。 |
| **text** | テキストを変更することを指定します。 |
| **style** | スタイルを変更することを指定します。 |
| *value* | 実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。 |

## デフォルト

Application Access ボックスのデフォルトのタイトル テキストは「Application Access」です。

Application Access ボックスのデフォルトのタイトル スタイルは次のとおりです。

background-color:#99CCCC;color:black;font-weight:bold;text-transform:uppercase

Application Access ボックスのデフォルトのメッセージ テキストは「Start Application Client」です。

Application Access ボックスのデフォルトのメッセージ スタイルは次のとおりです。

background-color:#99CCCC;color:maroon;font-size:smaller

Application Access ウィンドウのデフォルトのウィンドウ テキストは次のとおりです。

「Close this window when you finish using Application Access.Please wait for the table to be displayed before starting applications.」

Application Access ウィンドウのデフォルトのウィンドウ スタイルは次のとおりです。

background-color:#99CCCC;color:black;font-weight:bold

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| Webvpn カスタマイゼーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1(1) | このコマンドが導入されました。 |

**使用上のガイドライン**

**style** オプションは、有効な Cascading Style Sheet（CSS）パラメータとして表現されます。このパラメータの説明は、このマニュアルでは取り扱いません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト www.w3.org の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手可能です。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目は青を表しています。

**（注）** WebVPN ページを簡単にカスタマイズするには、ASDM を使用することをお勧めします。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するのに便利な機能があります。

**例**

次の例では、Application Access ボックスの背景色を RGB 16 進値 66FFFF（緑色の一種）にカスタマイズしています。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# application-access title style background-color:#66FFFF
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **application-access hide-details** | Application Access ウィンドウでのアプリケーション詳細の表示をイネーブルまたはディセーブルにします。 |
| **browse-networks** | WebVPN ホームページの Browse Networks ボックスをカスタマイズします。 |
| **file-bookmarks** | WebVPN ホームページの File Bookmarks タイトルまたはリンクをカスタマイズします。 |
| **web-applications** | WebVPN ホームページの Web Application ボックスをカスタマイズします。 |
| **web-bookmarks** | WebVPN ホームページの Web Bookmarks タイトルまたはリンクをカスタマイズします。 |

# application-access hide-details

WebVPN Applications Access ウィンドウに表示されるアプリケーション詳細を非表示にするには、WebVPN カスタマイゼーション モードで **application-access hide-details** コマンドを使用します。

**application-access hide-details** {**enable | disable**}

[**no**] **application-access hide-details** {**enable | disable**}

このコマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

## シンタックスの説明

| | |
|---|---|
| **enable** | Application Access ウィンドウのアプリケーション詳細を非表示にします。 |
| **disable** | Application Access ウィンドウのアプリケーション詳細を非表示にしません。 |

## デフォルト

デフォルトはディセーブルです。アプリケーション詳細は Application Access ウィンドウに表示されます。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| Webvpn カスタマイゼーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1(1) | このコマンドが導入されました。 |

## 例

次の例では、アプリケーション詳細の表示をディセーブルにしています。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# application-access hide-details disable
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **application-access** | WebVPN ホームページの Application Access ボックスをカスタマイズします。 |
| **browse-networks** | WebVPN ホームページの Browse Networks ボックスをカスタマイズします。 |
| **web-applications** | WebVPN ホームページの Web Application ボックスをカスタマイズします。 |

# area

OSPF エリアを作成するには、ルータ コンフィギュレーション モードで **area** コマンドを使用します。エリアを削除するには、このコマンドの **no** 形式を使用します。

**area** *area_id*

**no area** *area_id*

## シンタックスの説明

| | |
|---|---|
| *area_id* | 作成するエリアの ID。10 進数または IP アドレスを使用して ID を指定できます。有効な 10 進値は 0 ～ 4294967295 です。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| ルータ コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 既存 | このコマンドは既存のものです。 |

## 使用上のガイドライン

作成するエリアには、パラメータが設定されていません。関連する area コマンドを使用して、エリア パラメータを設定します。

## 例

次の例は、エリア ID 1 の OSPF エリアを作成する方法を示しています。

```
hostname(config-router)# area 1
hostname(config-router)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **area authentication** | OSPF エリアの認証をイネーブルにします。 |
| **area nssa** | エリアを準スタブ エリアとして定義します。 |
| **area stub** | エリアをスタブ エリアとして定義します。 |
| **router ospf** | ルータ コンフィギュレーション モードに入ります。 |
| **show running-config router** | グローバル ルータ コンフィギュレーション内のコマンドを表示します。 |

# area authentication

OSPF エリアの認証をイネーブルにするには、ルータ コンフィギュレーション モードで **area authentication** コマンドを使用します。エリア認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

**area** *area_id* **authentication** [***message-digest***]

**no area** *area_id* **authentication** [***message-digest***]

## シンタックスの説明

| | |
|---|---|
| *area_id* | 認証をイネーブルにするエリアの ID。10 進数または IP アドレスを使用して ID を指定できます。有効な 10 進値は 0 ～ 4294967295 です。 |
| ***message-digest*** | （オプション）*area_id* によって指定されたエリアでの Message Digest 5（MD5）認証をイネーブルにします。 |

## デフォルト

エリア認証はディセーブルになっています。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| ルータ コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 既存 | このコマンドは既存のものです。 |

## 使用上のガイドライン

指定した OSPF エリアが存在しない場合は、このコマンドの入力時にそのエリアが作成されます。***message-digest*** キーワードを付けずに **area authentication** コマンドを入力すると、簡易パスワード認証がイネーブルになります。***message-digest*** キーワードを付けると、MD5 認証がイネーブルになります。

## 例

次の例は、エリア 1 の MD5 認証をイネーブルにする方法を示しています。

```
hostname(config-router)# area 1 authentication message-digest
hostname(config-router)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **router ospf** | ルータ コンフィギュレーション モードに入ります。 |
| **show running-config router** | グローバル ルータ コンフィギュレーション内のコマンドを表示します。 |

# area default-cost

スタブまたは NSSA に送信されるデフォルト サマリー ルートのコストを指定するには、ルータ コンフィギュレーション モードで **area default-cost** コマンドを使用します。デフォルトのコスト値に戻すには、このコマンドの **no** 形式を使用します。

**area** *area_id* ***default-cost*** *cost*

**no area** *area_id* ***default-cost***

## シンタックスの説明

| | |
|---|---|
| *area_id* | デフォルト コストを変更するスタブまたは NSSA の ID。10 進数または IP アドレスを使用して ID を指定できます。有効な 10 進値は 0 ～ 4294967295 です。 |
| *cost* | スタブまたは NSSA に使用されるデフォルト サマリー ルートのコストを指定します。有効な値は 0 ～ 65535 です。 |

## デフォルト

*cost* のデフォルト値は 1 です。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| ルータ コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 既存 | このコマンドは既存のものです。 |

## 使用上のガイドライン

指定したエリアが以前に **area** コマンドで定義されていなかった場合は、このコマンドによって、指定したパラメータでそのエリアが作成されます。

## 例

次の例は、スタブまたは NSSA に送信されるサマリー ルートのデフォルト コストを指定する方法を示しています。

```
hostname(config-router)# area 1 default-cost 5
hostname(config-router)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **area nssa** | エリアを準スタブ エリアとして定義します。 |
| **area stub** | エリアをスタブ エリアとして定義します。 |
| **router ospf** | ルータ コンフィギュレーション モードに入ります。 |
| **show running-config router** | グローバル ルータ コンフィギュレーション内のコマンドを表示します。 |

# area filter-list prefix

ABR の OSPF エリア間のタイプ 3 LSA でアドバタイズされたプレフィックスをフィルタリングするには、ルータ コンフィギュレーション モードで **area filter-list prefix** コマンドを使用します。フィルタを変更またはキャンセルするには、このコマンドの **no** 形式を使用します。

**area** *area_id* **filter-list** ***prefix*** *list_name* {***in*** | ***out***}

**no area** *area_id* ***filter-list prefix*** *list_name* {***in*** | ***out***}

## シンタックスの説明

| | |
|---|---|
| *area_id* | フィルタリングを設定するエリアの ID。10 進数または IP アドレスを使用して ID を指定できます。有効な 10 進値は 0 ～ 4294967295 です。 |
| ***in*** | 指定エリアに着信するアドバタイズされたプレフィックスに、設定済みプレフィックス リストを適用します。 |
| *list_name* | プレフィックス リストの名前を指定します。 |
| ***out*** | 指定エリアから発信するアドバタイズされたプレフィックスに、設定済みプレフィックス リストを適用します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| ルータ コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 既存 | このコマンドは既存のものです。 |

## 使用上のガイドライン

指定したエリアが以前に **area** コマンドで定義されていなかった場合は、このコマンドによって、指定したパラメータでそのエリアが作成されます。

タイプ 3 LSA だけをフィルタリングできます。プライベート ネットワークに ASBR が設定されている場合は、ASBR がタイプ 5 LSA（プライベート ネットワークを記述）を送信します。この LSA は、パブリック エリアを含む AS 全体にフラッドされます。

## 例

次の例では、他のすべてのエリアからエリア 1 に送信されるプレフィックスをフィルタリングします。

```
hostname(config-router)# area 1 filter-list prefix-list AREA_1 in
hostname(config-router)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **router ospf** | ルータ コンフィギュレーション モードに入ります。 |
| **show running-config router** | グローバル ルータ コンフィギュレーション内のコマンドを表示します。 |

# area nssa

エリアを NSSA として設定するには、ルータ コンフィギュレーション モードで **area nssa** コマンドを使用します。エリアから NSSA 指定を削除するには、このコマンドの **no** 形式を使用します。

**area** *area_id* **nssa** [***no-redistribution***] [***default-information-originate*** [***metric-type*** {***1*** | ***2***}] [***metric*** *value*]] [***no-summary***]

**no area** *area_id* **nssa** [***no-redistribution***] [***default-information-originate*** [***metric-type*** {***1*** | ***2***}] [***metric*** *value*]] [***no-summary***]

## シンタックスの説明

| | |
|---|---|
| *area_id* | NSSA として指定するエリアの ID。10 進数または IP アドレスを使用して ID を指定できます。有効な 10 進値は 0 ～ 4294967295 です。 |
| ***default-information-originate*** | NSSA エリアでのタイプ 7 デフォルトの生成に使用します。このキーワードは、NSSA ABR 上または NSSA ASBR 上に限り有効です。 |
| **metric** *metric_value* | （オプション）OSPF デフォルト メトリック値を指定します。有効な値は 0 ～ 16777214 です。 |
| ***metric-type*** {***1*** \| ***2***} | （オプション）デフォルト ルートの OSPF メトリック タイプ。有効な値は次のとおりです。<br>• ***1*** : タイプ 1<br>• ***2*** : タイプ 2<br>デフォルト値は 2 です。 |
| ***no-redistribution*** | （オプション）ルータが NSSA ABR である場合に、**redistribute** コマンドで通常エリアだけにルートをインポートし、NSSA エリアにはインポートしないときに使用します。 |
| ***no-summary*** | （オプション）エリアを、サマリー ルートが投入されない準スタブ エリアにします。 |

## デフォルト

デフォルトは次のとおりです。

- NSSA エリアは定義されていません。
- ***metric-type*** は 2 です。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| ルータ コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 既存 | このコマンドは既存のものです。 |

**使用上のガイドライン**

指定したエリアが以前に **area** コマンドで定義されていなかった場合は、このコマンドによって、指定したパラメータでそのエリアが作成されます。

あるオプションをエリアに設定した後、別のオプションを指定すると、両方のオプションが設定されます。たとえば、次の 2 つのコマンドを別々に入力すると、コンフィギュレーション内では、両方のオプションが設定された 1 つのコマンドになります。

```
area 1 nssa no-redistribution
area area_id nssa default-information-originate
```

**例**

次の例は、2 つのオプションを別々に設定すると、コンフィギュレーション内でどのように 1 つのコマンドになるかを示しています。

```
hostname(config-router)# area 1 nssa no-redistribution
hostname(config-router)# area 1 nssa default-information-originate
hostname(config-router)# exit
hostname(config-router)# show running-config router ospf 1
router ospf 1
 area 1 nssa no-redistribution default-information-originate
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **area stub** | エリアをスタブ エリアとして定義します。 |
| **router ospf** | ルータ コンフィギュレーション モードに入ります。 |
| **show running-config router** | グローバル ルータ コンフィギュレーション内のコマンドを表示します。 |

# area range

エリアの境界でルートを統合および集約するには、ルータ コンフィギュレーション モードで **area range** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

**area** *area_id* **range** *address mask* [***advertise*** | ***not-advertise***]

**no area** *area_id* **range** *address mask* [***advertise*** | ***not-advertise***]

## シンタックスの説明

| | |
|---|---|
| *address* | サブネット範囲の IP アドレス。 |
| advertise | （オプション）アドレス範囲ステータスを advertise に設定し、タイプ 3 要約リンクステート アドバタイズメント（LSA）を生成します。 |
| *area_id* | 範囲を設定するエリアの ID。10 進数または IP アドレスを使用して ID を指定できます。有効な 10 進値は 0 ～ 4294967295 です。 |
| *mask* | IP アドレスのサブネット マスク。 |
| not-advertise | （オプション）アドレス範囲ステータスを DoNotAdvertise に設定します。タイプ 3 要約 LSA の表示が抑止され、コンポーネント ネットワークは他のネットワークからは見えないままになります。 |

## デフォルト

アドレス範囲ステータスは advertise に設定されます。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| ルータ コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 既存 | このコマンドは既存のものです。 |

## 使用上のガイドライン

指定したエリアが以前に **area** コマンドで定義されていなかった場合は、このコマンドによって、指定したパラメータでそのエリアが作成されます。

**area range** コマンドは、ABR だけで使用されます。このコマンドによって、エリアのルートが統合または集約されます。その結果、1 つのサマリー ルートが ABR によって他のエリアにアドバタイズされます。エリアの境界でルーティング情報が凝縮されます。エリアの外部では、アドレス範囲ごとに 1 つのルートがアドバタイズされます。この動作は、「経路集約」と呼ばれます。1 つのエリアに複数の **area range** コマンドを設定できます。この設定により、OSPF は、多くの異なるアドレス範囲セットのアドレスを集約できます。

**no area** *area_id* **range** *ip_address netmask* ***not-advertise*** コマンドは、***not-advertise*** オプション キーワードだけを削除します。

## 例

次の例は、ネットワーク 10.0.0.0 上のすべてのサブネット対する 1 つのサマリー ルート、およびネットワーク 192.168.110.0 上のすべてのホストに対する 1 つのサマリー ルートが、ABR によって他のエリアにアドバタイズされるよう指定しています。

```
hostname(config-router)# area 10.0.0.0 range 10.0.0.0 255.0.0.0
hostname(config-router)# area 0 range 192.168.110.0 255.255.255.0
hostname(config-router)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **router ospf** | ルータ コンフィギュレーション モードに入ります。 |
| **show running-config router** | グローバル ルータ コンフィギュレーション内のコマンドを表示します。 |

# area stub

エリアをスタブ エリアとして定義するには、ルータ コンフィギュレーション モードで **area stub** コマンドを使用します。スタブ エリア機能を削除するには、このコマンドの **no** 形式を使用します。

**area** *area_id* [***no-summary***]

**no area** *area_id* [***no-summary***]

## シンタックスの説明

| | |
|---|---|
| *area_id* | スタブ エリアの ID。10 進数または IP アドレスを使用して ID を指定できます。有効な 10 進値は 0 ～ 4294967295 です。 |
| ***no-summary*** | ABR がサマリー リンク アドバタイズメントをスタブ エリアに送信しないようにします。 |

## デフォルト

デフォルトの動作は次のとおりです。

- スタブ エリアが定義されていません。
- サマリー リンク アドバタイズメントがスタブ エリアに送信されます。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| ルータ コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 既存 | このコマンドは既存のものです。 |

## 使用上のガイドライン

このコマンドは、スタブまたは NSSA に接続されている ABR だけで使用できます。

**area stub** と **area default-cost** という 2 つのスタブ エリア ルータ コンフィギュレーション コマンドがあります。スタブ エリアに接続されているすべてのルータおよびアクセス サーバで、**area stub** コマンドを使用して、エリアをスタブ エリアとして設定する必要があります。スタブ エリアに接続されている ABR だけで **area default-cost** コマンドを使用します。**area default-cost** コマンドは、ABR によって生成されるサマリー デフォルト ルートのメトリックをスタブ エリアに提供します。

## 例

次の例では、指定したエリアをスタブ エリアとして設定しています。

```
hostname(config-router)# area 1 stub
hostname(config-router)#
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **area default-cost** | スタブまたはNSSA に送信されるデフォルト サマリー ルートのコストを指定します。 |
| **area nssa** | エリアを準スタブ エリアとして定義します。 |
| **router ospf** | ルータ コンフィギュレーション モードに入ります。 |
| **show running-config router** | グローバル ルータ コンフィギュレーション内のコマンドを表示します。 |

# area virtual-link

OSPF 仮想リンクを定義するには、ルータ コンフィギュレーション モードで **area virtual-link** コマンドを使用します。オプションをリセットする、または仮想リンクを削除するには、このコマンドの **no** 形式を使用します。

**area** *area_id* **virtual-link** *router_id* [***authentication*** [***message-digest*** | ***null***]] [***hello-interval*** *seconds*] [***retransmit-interval*** seconds] [***transmit-delay*** *seconds*] [***dead-interval*** *seconds* [[***authentication-key*** *key*] | [***message-digest-key*** *key_id* ***md5*** *key*]]

**no area** *area_id* **virtual-link** *router_id* [***authentication*** [***message-digest*** | ***null***]] [***hello-interval*** *seconds*] [***retransmit-interval*** seconds] [***transmit-delay*** *seconds*] [***dead-interval*** *seconds* [[***authentication-key*** *key*] | [***message-digest-key*** *key_id* ***md5*** *key*]]

**シンタックスの説明**

| | |
|---|---|
| *area_id* | 仮想リンクの中継エリアのエリア ID。10 進数または IP アドレスを使用して ID を指定できます。有効な 10 進値は 0 ～ 4294967295 です。 |
| ***authentication*** | （オプション）認証タイプを指定します。 |
| ***authentication-key*** *key* | （オプション）隣接ルーティング デバイスで使用するための OSPF 認証パスワードを指定します。 |
| ***dead-interval*** *seconds* | （オプション）hello パケットを 1 つも受信しない場合に、隣接ルーティング デバイスがダウンしたことを宣言する前の間隔を設定します。有効な値は 1 ～ 65535 秒です。 |
| ***hello-interval*** *seconds* | （オプション）インターフェイス上で送信される hello パケット間の間隔を指定します。有効な値は 1 ～ 65535 秒です。 |
| ***md5*** *key* | （オプション）最大 16 バイトの英数字によるキーを指定します。 |
| ***message-digest*** | （オプション）メッセージ ダイジェスト認証を使用することを指定します。 |
| ***message-digest-key*** *key_id* | （オプション）Message Digest 5（MD5）認証をイネーブルにし、認証キー ID 番号を指定します。有効な値は 1 ～ 255 です。 |
| ***null*** | （オプション）認証を使用しないことを指定します。パスワードまたはメッセージ ダイジェスト認証は、OSPF エリアに設定されていれば上書きされます。 |
| ***retransmit-interval*** *seconds* | （オプション）インターフェイスに属する隣接ルータの LSA 再送間隔を指定します。有効な値は 1 ～ 65535 秒です。 |
| *router_id* | 仮想リンク ネイバーに関連付けられているルータ ID。ルータ ID は各ルータによって内部でインターフェイス IP アドレスから生成されます。この値は、IP アドレスの形式で入力する必要があります。デフォルトはありません。 |
| ***transmit-delay*** *seconds* | （オプション）OSPF によるトポロジ変更の受信と最短パス優先（SPF）計算の開始との間の遅延時間（0 ～ 65535 秒）を指定します。デフォルトは 5 秒です。 |

**デフォルト**

デフォルトは次のとおりです。

- *area_id*：エリア ID は事前に定義されていません。
- *router_id*：ルータ ID は事前に定義されていません。
- ***hello-interval*** *seconds*：10 秒。
- ***retransmit-interval*** *seconds*：5 秒。
- ***transmit-delay*** *seconds*：1 秒。
- ***dead-interval*** *seconds*：40 秒。
- ***authentication-key*** *key*：キーは事前に定義されていません。
- ***message-digest-key*** *key_id* ***md5*** *key*：キーは事前に定義されていません。

**コマンド モード**

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| ルータ コンフィギュレーション | • | — | • | — | — |

**コマンド履歴**

| リリース | 変更内容 |
|---|---|
| 既存 | このコマンドは既存のものです。 |

**使用上のガイドライン**

OSPF では、すべてのエリアがバックボーン エリアに接続されている必要があります。バックボーンへの接続が失われた場合、仮想リンクを確立することで接続を修復できます。

hello 間隔を小さくすればするほど、トポロジ変更の検出が速くなりますが、ルーティング トラフィックが増加します。

再送間隔の設定値はあまり小さくしないでください。小さくすると、不要な再送信が行われます。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。

送信遅延の値では、インターフェイスの送信遅延と伝搬遅延を考慮に入れる必要があります。

指定した認証キーは、***area*** *area_id* ***authentication*** コマンドでバックボーンに対して認証がイネーブルにされている場合にだけ使用されます。

簡易テキスト認証と MD5 認証という 2 つの認証方式は、相互排他的です。どちらかを指定するか、または両方とも指定しないでください。***authentication-key*** *key* または ***message-digest-key*** *key_id* ***md5*** *key* の後に指定したキーワードと引数はすべて無視されます。したがって、オプションの引数はすべて、上記のキーワードと引数の組み合せの前に指定します。

インターフェイスに認証タイプが指定されていない場合、インターフェイスはエリアに指定されている認証タイプを使用します。エリアに認証タイプが指定されていない場合、エリアのデフォルトは null 認証です。

**（注）** 仮想リンクを正しく設定するには、各仮想リンク ネイバーに、中継エリア ID および対応する仮想リンク隣接ルータ ID が含まれている必要があります。ルータ ID を表示するには、**show ospf** コマンドを使用します。

仮想リンクからオプションを削除するには、削除するオプションを付けて、このコマンドの **no** 形式を使用します。仮想リンクを削除するには、**no area** *area_id* ***virtual-link*** コマンドを使用します。

## 例

次の例では、MD5 認証の仮想リンクを確立しています。

```
hostname(config-router)# area 10.0.0.0 virtual-link 10.3.4.5 message-digest-key 3 md5
sa5721bk47
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **area authentication** | OSPF エリアの認証をイネーブルにします。 |
| **router ospf** | ルータ コンフィギュレーション モードに入ります。 |
| **show ospf** | OSPF ルーティング プロセスに関する一般情報を表示します。 |
| **show running-config router** | グローバル ルータ コンフィギュレーション内のコマンドを表示します。 |

# arp

ARP テーブルにスタティック ARP エントリを追加するには、グローバル コンフィギュレーション モードで **arp** コマンドを使用します。スタティック エントリを削除するには、このコマンドの **no** 形式を使用します。スタティック ARP エントリは MAC アドレスを IP アドレスにマッピングし、ホストに到達するまでに通過するインターフェイスを指定します。スタティック ARP エントリはタイムアウトしないため、ネットワーク問題の解決に役立つことがあります。透過ファイアウォール モードでは、ARP 検査でスタティック ARP テーブルが使用されます（**arp-inspection** コマンドを参照）。

**arp** *interface_name ip_address mac_address* [***alias***]

**no arp** *interface_name ip_address mac_address*

## シンタックスの説明

| | |
|---|---|
| ***alias*** | （オプション）このマッピングに対してプロキシ ARP をイネーブルにします。セキュリティ アプライアンスは、このコマンドで指定された IP アドレスに対する ARP 要求を受信すると、セキュリティ アプライアンスの MAC アドレスで応答します。その後、その IP アドレスを持つホスト宛てのトラフィックを受信すると、セキュリティ アプライアンスはこのコマンドで指定されたホスト MAC アドレスにそのトラフィックを転送します。このキーワードは、たとえば、ARP を実行しないデバイスがある場合に役立ちます。<br><br>透過ファイアウォール モードの場合、このキーワードは無視され、セキュリティ アプライアンスはプロキシ ARP を実行しません。 |
| *interface_name* | ホスト ネットワークに接続されているインターフェイス。 |
| *ip_address* | ホストの IP アドレス。 |
| *mac_address* | ホストの MAC アドレス。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル 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 |
|---|---|
| 既存 | このコマンドは既存のものです。 |

**使用上のガイドライン**

ホストは IP アドレスによってパケットの宛先を指定しますが、イーサネット上での実際のパケット配信は、イーサネット MAC アドレスに依存しています。ルータまたはホストは、直接接続されているネットワーク上でパケットを配信する場合、IP アドレスに関連付けられている MAC アドレスを要求する ARP 要求を送信してから、その ARP 応答に従ってパケットを MAC アドレスに配信します。ホストまたはルータは ARP テーブルを保持しているため、配信する必要のあるパケットごとに ARP 要求を送信する必要がありません。ARP テーブルは、ネットワーク上で ARP 応答が送信されるたびに動的にアップデートされます。また、一定期間使用されなかったエントリは、タイムアウトになります。エントリが間違っている場合（たとえば、所定の IP アドレスの MAC アドレスが変更された場合）、アップデートされる前にそのエントリがタイムアウトになります。

**（注）** 透過ファイアウォール モードの場合、セキュリティ アプライアンスとの間のトラフィック（管理トラフィックなど）にはダイナミック ARP エントリが使用されます。

**例**

次の例では、外部インターフェイス上で、10.1.1.1 のスタティック ARP エントリを MAC アドレス 0009.7cbe.2100 で作成しています。

```
hostname(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **arp timeout** | セキュリティ アプライアンスが ARP テーブルを再構築するまでの時間を設定します。 |
| **arp-inspection** | 透過ファイアウォール モードで、ARP パケットを調べて ARP スプーフィングを防止します。 |
| **show arp** | ARP テーブルを表示します。 |
| **show arp statistics** | ARP 統計情報を表示します。 |
| **show running-config arp** | ARP タイムアウトの現在のコンフィギュレーションを表示します。 |

# arp timeout

セキュリティ アプライアンスが ARP テーブルを再構築するまでの時間を設定するには、グローバル コンフィギュレーション モードで **arp timeout** コマンドを使用します。デフォルトのタイムアウトに戻すには、このコマンドの **no** 形式を使用します。ARP テーブルを再構築すると、自動的に、新しいホスト情報にアップデートされ、古いホスト情報が削除されます。ホスト情報が頻繁に変更されるため、タイムアウト値を小さくする必要がある場合もあります。

**arp *timeout*** *seconds*

**no arp *timeout*** *seconds*

## シンタックスの説明

| | |
|---|---|
| *seconds* | ARP テーブルを再構築する間隔の秒数（60 ～ 4294967）。 |

## デフォルト

デフォルト値は 14,400 秒（4 時間）です。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル 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 |
|---|---|
| 既存 | このコマンドは既存のものです。 |

## 例

次の例では、ARP タイムアウトを 5,000 秒に変更します。

```
hostname(config)# arp timeout 5000
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **arp** | スタティック ARP エントリを追加します。 |
| **arp-inspection** | 透過ファイアウォール モードで、ARP パケットを調べて ARP スプーフィングを防止します。 |
| **show arp statistics** | ARP 統計情報を表示します。 |
| **show running-config arp timeout** | ARP タイムアウトの現在のコンフィギュレーションを表示します。 |

# arp-inspection

透過ファイアウォール モードで ARP 検査をイネーブルにするには、グローバル コンフィギュレーション モードで **arp-inspection** コマンドを使用します。ARP 検査をディセーブルにするには、このコマンドの **no** 形式を使用します。ARP 検査では、すべての ARP パケットがスタティック ARP エントリ（**arp** コマンドを参照）と比較され、一致しないパケットがブロックされます。この機能により、ARP スプーフィングを防止できます。

**arp-inspection** *interface_name* ***enable*** [***flood*** | ***no-flood***]

**no arp-inspection** *interface_name* ***enable***

## シンタックスの説明

| | |
|---|---|
| ***enable*** | ARP 検査をイネーブルにします。 |
| ***flood*** | （デフォルト）スタティック ARP エントリのどの要素とも一致しないパケットが、発信元インターフェイスを除くすべてのインターフェイスにフラッドされるように指定します。MAC アドレス、IP アドレス、またはインターフェイス間でミスマッチがある場合、セキュリティ アプライアンスはパケットをドロップします。<br><br>**（注）** 管理専用のインターフェイス（存在する場合）では、このパラメータを flood に設定しても、パケットはフラッドされません。 |
| *interface_name* | ARP 検査をイネーブルにするインターフェイス。 |
| ***no-flood*** | （オプション）スタティック ARP エントリに正確に一致しないパケットがドロップされるように指定します。 |

## デフォルト

デフォルトでは、すべてのインターフェイスで ARP 検査がディセーブルになっています。すべての ARP パケットがセキュリティ アプライアンスを通過できます。ARP 検査をイネーブルにすると、デフォルトでは、まったく一致しない ARP パケットがフラッドされます。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル 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) | このコマンドが導入されました。 |

## 使用上のガイドライン

ARP 検査をイネーブルにするには、事前に **arp** コマンドを使用してスタティック ARP エントリを設定しておく必要があります。

ARP 検査をイネーブルにすると、セキュリティ アプライアンスは、すべての ARP パケット内の MAC アドレス、IP アドレス、および送信元インターフェイスを ARP テーブル内のスタティック エントリと比較して、次のアクションを実行します。

- IP アドレス、MAC アドレス、および送信元インターフェイスが ARP エントリと一致した場合、パケットを通過させます。
- MAC アドレス、IP アドレス、またはインターフェイス間でミスマッチがある場合、セキュリティ アプライアンスはパケットをドロップします。
- ARP パケットのエントリがスタティック ARP テーブル内のどのエントリとも一致しなかった場合、パケットをすべてのインターフェイスに転送（フラッド）するように、またはドロップするように、セキュリティ アプライアンスを設定できます。

（注）　管理専用のインターフェイス（存在する場合）では、このパラメータを flood に設定しても、パケットはフラッドされません。

ARP 検査により、悪意のあるユーザが他のホストまたはルータになりすますこと（ARP スプーフィングと呼ばれる）を防止できます。ARP スプーフィングは、「man-in-the-middle」攻撃をイネーブルにすることができます。たとえば、ホストがゲートウェイ ルータに ARP 要求を送信すると、ゲートウェイ ルータはゲートウェイ ルータの MAC アドレスで応答します。ところが、攻撃者はホストに、ルータの MAC アドレスではなく、攻撃者の MAC アドレスを含む別の ARP 応答を送信します。これで、攻撃者は、ルータに転送する前に、ホストのトラフィックをすべて代行受信できるようになります。

ARP 検査により、正しい MAC アドレスと、それに関連付けられている IP アドレスがスタティック ARP テーブル内にある限り、攻撃者が攻撃者の MAC アドレスで ARP 応答を送信できないことが保証されます。

（注）　透過ファイアウォール モードの場合、セキュリティ アプライアンスとの間のトラフィック（管理トラフィックなど）にはダイナミック ARP エントリが使用されます。

## 例

次の例では、外部インターフェイス上で ARP 検査をイネーブルにし、スタティック ARP エントリに一致しないすべての ARP パケットをドロップするようセキュリティ アプライアンスを設定しています。

```
hostname(config)# arp outside 209.165.200.225 0009.7cbe.2100
hostname(config)# arp-inspection outside enable no-flood
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **arp** | スタティック ARP エントリを追加します。 |
| **clear configure arp-inspection** | ARP 検査のコンフィギュレーションを消去します。 |
| **firewall transparent** | ファイアウォール モードを透過に設定します。 |
| **show arp statistics** | ARP 統計情報を表示します。 |
| **show running-config arp** | ARP タイムアウトの現在のコンフィギュレーションを表示します。 |

# asdm disconnect

アクティブな ASDM セッションを終了するには、特権 EXEC モードで **asdm disconnect** コマンドを使用します。

**asdm disconnect** *session*

## シンタックスの説明

| | |
|---|---|
| *session* | 終了させるアクティブな ASDM セッションのセッション ID。すべてのアクティブな ASDM セッションのセッション ID を表示するには、**show asdm sessions** コマンドを使用します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| 特権 EXEC | • | • | • | • | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | **pdm disconnect** コマンドが **asdm disconnect** コマンドに変更されました。 |

## 使用上のガイドライン

アクティブな ASDM セッションとそれに関連付けられているセッション ID のリストを表示するには、**show asdm sessions** コマンドを使用します。特定のセッションを終了するには、**asdm disconnect** コマンドを使用します。

ASDM セッションを終了しても、残りのすべてのアクティブな ASDM セッションは、関連付けられている ID を保持します。たとえば、3 つのアクティブな ASDM セッションがあり、それぞれのセッション ID が 0、1、2 である場合、セッション 1 を終了しても、残りのアクティブな ASDM セッションはセッション ID 0 および 2 を保持します。この例では、次の新しい ASDM セッションにセッション ID 1 が割り当てられ、その後の新しいセッションには、セッション ID 3 から順番に ID が割り当てられます。

## 例

次の例では、セッション ID 0 の ASDM セッションを終了しています。**asdm disconnect** コマンドの入力前後に、**show asdm sessions** コマンドで、アクティブな ASDM セッションを表示しています。

```
hostname# show asdm sessions

0 192.168.1.1
1 192.168.1.2
hostname# asdm disconnect 0
hostname# show asdm sessions

1 192.168.1.2
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show asdm sessions** | アクティブな ASDM セッションとそれに関連付けられているセッション ID のリストを表示します。 |

# asdm disconnect log_session

アクティブな ASDM ロギング セッションを終了するには、特権 EXEC モードで **asdm disconnect log_session** コマンドを使用します。

**sdm disconnect log_session** *session*

## シンタックスの説明

| | |
|---|---|
| *session* | 終了させるアクティブな ASDM ロギング セッションのセッション ID。すべてのアクティブな ASDM セッションのセッション ID を表示するには、**show asdm log_sessions** コマンドを使用します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| 特権 EXEC | • | • | • | • | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

アクティブな ASDM ロギング セッションとそれに関連付けられているセッション ID のリストを表示するには、**show asdm log_sessions** コマンドを使用します。特定のロギング セッションを終了するには、**asdm disconnect log_session** コマンドを使用します。

アクティブな各 ASDM セッションは、1 つまたは複数の ASDM ロギング セッションと関連付けられています。ASDM は、ロギング セッションを使用して、セキュリティ アプライアンスから syslog メッセージを取得します。ログ セッションを終了すると、アクティブな ASDM セッションに悪影響が及ぶことがあります。不要な ASDM セッションを終了するには、**asdm disconnect** コマンドを使用します。

**（注）** 各 ASDM セッションは、少なくとも 1 つの ASDM ロギング セッションを保持しているため、**show asdm sessions** と **show asdm log_sessions** の出力は同じ内容になることもあります。

ASDM ロギング セッションを終了しても、残りのすべてのアクティブな ASDM ロギング セッションは、関連付けられている ID を保持します。たとえば、3 つのアクティブな ASDM ロギング セッションがあり、それぞれのセッション ID が 0、1、2 である場合、セッション 1 を終了しても、残りのアクティブな ASDM ロギング セッションはセッション ID 0 および 2 を保持します。この例では、次の新しい ASDM ロギング セッションにセッション ID 1 が割り当てられ、その後の新しいロギング セッションには、セッション ID 3 から順番に ID が割り当てられます。

## 例

次の例では、セッション ID 0 の ASDM セッションを終了しています。**asdm disconnect log_sessions** コマンドの入力前後に、**show asdm log_sessions** コマンドで、アクティブな ASDM セッションを表示しています。

```
hostname# show asdm log_sessions

0 192.168.1.1
1 192.168.1.2
hostname# asdm disconnect 0
hostname# show asdm log_sessions

1 192.168.1.2
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show asdm log_sessions** | アクティブな ASDM ロギング セッションとそれに関連付けられているセッション ID のリストを表示します。 |

# asdm group

**注意**　このコマンドを手動で設定しないでください。**asdm group** コマンドは ASDM によって実行コンフィギュレーションに追加され、内部用に使用されます。このコマンドは、情報提供のためだけにこのマニュアルに記載されています。

**asdm group** *real_grp_name real_if_name*

**asdm group** *ref_grp_name ref_if_name* ***reference*** *real_grp_name*

## シンタックスの説明

| | |
|---|---|
| *real_grp_name* | ASDM オブジェクト グループの名前。 |
| *real_if_name* | 指定のオブジェクト グループが関連付けられているインターフェイスの名前。 |
| *ref_grp_name* | *real_grp_name* 引数で指定されたオブジェクト グループの変換された IP アドレスを含むオブジェクト グループの名前。 |
| *ref_if_name* | 着信トラフィックの宛先 IP アドレスが変換される元となるインターフェイスの名前。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル 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) | **pdm group** コマンドが **asdm group** コマンドに変更されました。 |

## 使用上のガイドライン

このコマンドを手動で設定または削除しないでください。

# asdm history enable

ASDM 履歴トラッキングをイネーブルにするには、グローバル コンフィギュレーション モードで **asdm history enable** コマンドを使用します。ASDM 履歴トラッキングをディセーブルにするには、このコマンドの **no** 形式を使用します。

**asdm history enable**

**no asdm history enable**

## シンタックスの説明

このコマンドには、引数もキーワードもありません。

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル 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) | **pdm history enable** コマンドが **asdm history enable** コマンドに変更されました。 |

## 使用上のガイドライン

ASDM 履歴トラッキングをイネーブルにすることによって得られる情報は、ASDM 履歴バッファに格納されます。この情報を表示するには、**show asdm history** コマンドを使用します。この履歴情報は、ASDM によってデバイス モニタリングに使用されます。

## 例

次の例では、ASDM 履歴トラッキングをイネーブルにしています。

```
hostname(config)# asdm history enable
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show asdm history** | ASDM 履歴バッファの内容を表示します。 |

# asdm image

フラッシュ メモリ内の ASDM ソフトウェア イメージの場所を指定するには、グローバル コンフィギュレーション モードで **asdm image** コマンドを使用します。イメージの場所の指定を削除するには、このコマンドの **no** 形式を使用します。

**asdm image** *url*

**no asdm image** [*url*]

## シンタックスの説明

*url*　フラッシュ メモリ内の ASDM イメージの場所を設定します。次の URL シンタックスを参照してください。

- ***disk0:/*[*path/*]*filename***

  ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合、この URL は内蔵フラッシュ メモリを指します。***disk0*** ではなく ***flash*** を使用することもできます。これらは、エイリアス関係にあります。
- ***disk1:/*[*path/*]*filename***

  ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合、この URL は外部フラッシュ メモリ カードを指します。
- ***flash:/*[*path/*]*filename***

  この URL は内蔵フラッシュ メモリを指します。

## デフォルト

このコマンドをスタートアップ コンフィギュレーションに含めない場合、セキュリティ アプライアンスは最初に検出した ASDM イメージを起動時に使用します。内蔵フラッシュ メモリのルート ディレクトリ内を検索し、次に外部フラッシュ メモリを検索します。イメージを検出した場合、セキュリティ アプライアンスは **asdm image** コマンドを実行コンフィギュレーションに挿入します。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル 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) | このコマンドが導入されました。 |

## 使用上のガイドライン

フラッシュ メモリに複数の ASDM ソフトウェア イメージを格納できます。アクティブな ASDM セッションのある間に、**asdm image** コマンドを入力して新しい ASDM ソフトウェア イメージを指定しても、アクティブなセッションは中断しません。アクティブな ASDM セッションは、セッションを開始した ASDM ソフトウェア イメージを引き続き使用します。新しい ASDM セッションは、新しいソフトウェア イメージを使用します。**no asdm image** コマンドを入力すると、コンフィギュレーションからコマンドが削除されます。ただし、最後に設定したイメージの場所を使用して、セキュリティ アプライアンスから ASDM にアクセスできます。

このコマンドをスタートアップ コンフィギュレーションに含めない場合、セキュリティ アプライアンスは最初に検出した ASDM イメージを起動時に使用します。内蔵フラッシュ メモリのルート ディレクトリ内を検索し、次に外部フラッシュ メモリを検索します。イメージを検出した場合、セキュリティ アプライアンスは **asdm image** コマンドを実行コンフィギュレーションに挿入します。必ず **write memory** コマンドを使用して、実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存してください。**asdm image** コマンドをスタートアップ コンフィギュレーションに保存しておかないと、再起動するたびにセキュリティ アプライアンスが ASDM イメージを探し、**asdm image** コマンドを実行コンフィギュレーションに挿入します。Auto Update を使用している場合は、起動時にこのコマンドが自動的に追加され、セキュリティ アプライアンスにあるコンフィギュレーションが Auto Update Server にあるコンフィギュレーションと一致しなくなります。そのため、セキュリティ アプライアンスは Auto Update Server からコンフィギュレーションをダウンロードします。この不必要な動作を防ぐには、**asdm image** コマンドをスタートアップ コンフィギュレーションに保存しておきます。

## 例

次の例では、ASDM イメージを asdm.bin に設定しています。

```
hostname(config)# asdm image flash:/asdm.bin
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show asdm image** | 現在の ASDM イメージ ファイルを表示します。 |
| **boot** | ソフトウェア イメージ ファイルとスタートアップ コンフィギュレーション ファイルを設定します。 |

# asdm location

**注意**　このコマンドを手動で設定しないでください。**asdm location** コマンドは ASDM によって実行コンフィギュレーションに追加され、内部通信に使用されます。このコマンドは、情報提供のためだけにこのマニュアルに記載されています。

**asdm location** *ip_addr netmask if_name*

**asdm location** *ipv6_addr/prefix if_name*

## シンタックスの説明

| | |
|---|---|
| *ip_addr* | ネットワーク トポロジを定義するために ASDM によって内部で使用される IP アドレス。 |
| *netmask* | *ip_addr* のサブネット マスク。 |
| *if_name* | ASDM にアクセスするときに通過するインターフェイスの名前。 |
| *ipv6_addr/prefix* | ネットワーク トポロジを定義するために ASDM によって内部で使用される IPv6 アドレスおよびプレフィックス。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル 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) | **pdm location** コマンドが **asdm location** コマンドに変更されました。 |

## 使用上のガイドライン

このコマンドを手動で設定または削除しないでください。

# asr-group

非対称ルーティング インターフェイス グループ ID を指定するには、インターフェイス コンフィギュレーション モードで **asr-group** コマンドを使用します。この ID を削除するには、このコマンドの **no** 形式を使用します。

**asr-group** *group_id*

**no asr-group** *group_id*

## シンタックスの説明

| | |
|---|---|
| *group_id* | 非対称ルーティング グループ ID。有効な値は 1 ～ 32 です。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| インターフェイス コンフィギュレーション | • | • | — | • | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(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

Active/Active フェールオーバーがイネーブルである場合、ロードバランシングのために、発信接続のリターン トラフィックがピア装置上のアクティブなコンテキストを介してルーティングされることがあります。このピア装置上で、発信接続のコンテキストはスタンバイ グループ内にあります。

**asr-group** コマンドでは、着信インターフェイスによるフローが見つからない場合、同じ asr グループのインターフェイスで着信パケットが再分類されます。再分類により、別のインターフェイスによるフローが見つかり、関連付けられているコンテキストがスタンバイ状態である場合、パケットは処理のためにアクティブ装置に転送されます。

このコマンドを有効にするには、ステートフル フェールオーバーがイネーブルである必要があります。

ASR 統計情報を表示するには、**show interface detail** コマンドを使用します。この統計情報には、インターフェイス上で送信、受信、およびドロップされた ASR パケットの数が含まれています。

## 例

次の例では、選択したインターフェイスを非対称ルーティング グループ 1 に割り当てています。

コンテキスト ctx1 のコンフィギュレーション

```
hostname/ctx1(config)# interface e2
hostname/ctx1(config-if)# nameif outside
hostname/ctx1(config-if)# ip address 192.168.1.11 255.255.255.0 standby 192.168.1.21
hostname/ctx1(config-if)# asr-group 1
```

コンテキスト ctx2 のコンフィギュレーション

```
hostname/ctx2(config)# interface e3
hostname/ctx2(config-if)# nameif outside
hostname/ctx2(config-if)# ip address 192.168.1.31 255.255.255.0 standby 192.168.1.41
hostname/ctx2(config-if)# asr-group 1
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **interface** | インターフェイス コンフィギュレーション モードに入ります。 |
| **show interface** | インターフェイス統計情報を表示します。 |

# auth-cookie-name

認証クッキーの名前を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **auth-cookie-name** コマンドを使用します。これは HTTP Forms コマンドを使用した SSO です。

**auth-cookie-name**

## シンタックスの説明

| | |
|---|---|
| *name* | 認証クッキーの名前。最大長は 128 文字です。 |

## デフォルト

デフォルトの値や動作はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

セキュリティ アプライアンスの WebVPN サーバは、HTTP POST 要求を使用してシングル サインオン認証要求を SSO サーバに送信します。認証が成功した場合、認証 Web サーバは、クライアント ブラウザに認証クッキーを返します。クライアント ブラウザは、その認証クッキーを提示することで、SSO ドメイン内の他の Web サーバに対して認証を行います。**auth-cookie-name** コマンドは、セキュリティ アプライアンスによって SSO で使用される認証クッキーの名前を設定します。

一般的な認証クッキーの形式は、Set-Cookie: < クッキー名 >=< クッキー値 > ［;< クッキー アトリビュート >］です。次の認証クッキーの例では、SMSESSION が **auth-cookie-name** コマンドで設定される名前です。

```
Set-Cookie:
SMSESSION=yN4Yp5hHVNDgs4FT8dn7+Rwev41hsE49XlKc+1twie0gqnjbhkTkUnR8XWP3hvDH6PZPbHIHtWLD
KTa8ngDB/lbYTjIxrbDx8WPWwaG3CxVa3adOxHFR8yjD55GevK3ZF4ujgU1lhO6fta0dSSOSepWvnsCb7IFxCw
+MGiw0o88uHa2t4l+SillqfJvcpuXfiIAO06D/dapWriHjNoi4llJOgCst33wEhxFxcWy2UWxs4EZSjsI5GyBn
efSQTPVfma5dc/emWor9vWr0HnTQaHP5rg5dTNqunkDEdMIHfbeP3F90cZejVzihM6igiS6P/CEJAjE;Domain
=.example.com;Path=/
```

AAA サーバ ホスト コンフィギュレーション モードで入力された次の例では、example.com という名前の Web サーバから受信した認証クッキーの認証クッキー名として SMSESSION を指定しています。

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# auth-cookie-name SMSESSION
hostname(config-aaa-server-host)#
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **action-uri** | シングル サインオン認証用のユーザ名とパスワードを受信する Web サーバ URI を指定します。 |
| **hidden-parameter** | 認証 Web サーバとの交換に使用する非表示パラメータを作成します。 |
| **password-parameter** | SSO 認証用にユーザ パスワードを送信する必要がある HTTP POST 要求のパラメータの名前を指定します。 |
| **start-url** | 事前ログイン クッキーの取得先 URL を指定します。 |
| **user-parameter** | SSO 認証で使用される HTTP POST 要求の一部としてユーザ名パラメータが送信される必要があることを指定します。 |

# authentication

WebVPN または電子メール プロキシの認証方式を設定するには、**authentication** コマンドを使用します。WebVPN の場合、このコマンドは webvpn モードで使用します。電子メール プロキシ（IMAP4S、POP3S、SMTPS）の場合、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。デフォルトの AAA に戻すには、このコマンドの **no** 形式を使用します。

セキュリティ アプライアンスは、ユーザを認証して、ユーザのアイデンティティを確認します。

**authentication** {**aaa** | **certificate** | **mailhost** | **piggyback**}

**no authentication**

**シンタックスの説明**

| | |
|---|---|
| **aaa** | セキュリティ アプライアンスが設定済み AAA サーバに対してチェックするユーザ名とパスワードを提供します。 |
| **certificate** | SSL ネゴシエーション中に証明書を提供します。 |
| **mailhost** | リモート メール サーバを介した認証。mailhost を設定できるのは SMTPS だけです。IMAP4S および POP3S の場合、メールホスト認証は必須であり、設定可能なオプションとして表示されません。 |
| **piggyback** | HTTPS WebVPN セッションがすでに存在する必要があります。ピギーバック認証は、電子メール プロキシだけで使用できます。 |

**デフォルト**

次の表は、WebVPN および電子メール プロキシのデフォルトの認証方式を示しています。

| プロトコル | デフォルトの認証方式 |
|---|---|
| WebVPN | AAA |
| IMAP4S | メールホスト（必須） |
| POP3S | メールホスト（必須） |
| SMTPS | AAA |

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| Webvpn | • | — | • | — | — |
| Imap4s | • | — | • | — | — |
| Pop3s | • | — | • | — | — |
| SMTPS | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが導入されました。 |
| 7.1(1) | このコマンドは、webvpn モードでは廃止され、トンネル グループ webvpn アトリビュート モードに置き換えられました。 |

## 使用上のガイドライン

リリース 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 webvpn アトリビュート モードの同等のコマンドに変換されます。

WebVPN の場合、AAA 認証と証明書認証の両方を要求できます。その場合、ユーザは証明書およびユーザ名とパスワードを提供する必要があります。

電子メール プロキシ認証の場合、複数の認証方式を要求できます。

このコマンドを再び指定すると、現在のコンフィギュレーションが上書きされます。

## 例

次の例は、WebVPN ユーザに対して認証のために証明書の提供を要求する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# authentication certificate
```

# authentication（暗号 isakmp ポリシー コンフィギュレーション モード）

IKE ポリシー内の認証方式を指定するには、暗号 isakmp ポリシー コンフィギュレーション モードで **authentication** コマンドを使用します。IKE ポリシーは、IKE ネゴシエーション用のパラメータのセットを定義したものです。ISAKMP 認証方式を削除するには、関連する **clear configure** コマンドを使用します。

**authentication** {**crack** | **pre-share** | **rsa-sig**}

## シンタックスの説明

| | |
|---|---|
| **crack** | 認証方式として、IKE Challenge/Response for Authenticated Cryptographic Keys（CRACK）を指定します。 |
| **pre-share** | 認証方式として、事前共有キーを指定します。 |
| *priority* | IKE ポリシーを一意に識別し、そのポリシーに優先順位を割り当てます。1 ～ 65534 の整数を使用します。1 は優先順位が最も高く、65534 が最も低くなります。 |
| **rsa-sig** | 認証方式として、RSA シグニチャを指定します。<br><br>RSA シグニチャは、IKE ネゴシエーションに対する否認防止ができます。これは、基本的にユーザがピアとの IKE ネゴシエーションを行ったかどうかを、第三者に証明できることを意味します。 |

## デフォルト

デフォルトの ISAKMP ポリシー認証は、**pre-share** です。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| 暗号 isakmp ポリシー 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)(1) | **isakmp policy authentication** コマンドは既存のものです。 |
| 7.2.(1) | **isakmp policy authentication** コマンドが、**authentication** コマンドに置き換えられました。 |

## 使用上のガイドライン

RSA シグニチャを指定する場合は、認証局（CA）から証明書を取得するようにセキュリティ アプライアンスとそのピアを設定する必要があります。事前共有キーを指定する場合は、セキュリティ アプライアンスとそのピアに、事前共有キーを別々に設定する必要があります。

## 例

次の例は、グローバル コンフィギュレーション モードで、**authentication** コマンドを使用する方法を示しています。この例では、優先順位番号 40 の IKE ポリシーで RSA シグニチャの認証方式を使用するように設定します。

```
hostname(config)# crypto isakmp policy 40
hostname(config-isakmp-policy)# authentication rsa-sig
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure crypto isakmp** | すべての ISAKMP コンフィギュレーションを消去します。 |
| **clear configure crypto isakmp policy** | ISAKMP ポリシー コンフィギュレーションをすべて消去します。 |
| **clear crypto isakmp sa** | IKE ランタイム SA データベースを消去します。 |
| **show running-config crypto isakmp** | アクティブなコンフィギュレーションをすべて表示します。 |

# authentication（トンネル グループ webvpn コンフィギュレーション モード）

トンネル グループの認証方式を指定するには、トンネル グループ webvpn コンフィギュレーション モードで **authentication** コマンドを使用します。

**authentication aaa** [**certificate**]

**authentication certificate** [**aaa**]

## シンタックスの説明

| | |
|---|---|
| **aaa** | このトンネル グループの認証にユーザ名とパスワードを使用することを指定します。 |
| **certificate** | 認証にデジタル証明書を使用することを指定します。 |

## デフォルト

デフォルトの認証方式は AAA です。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| トンネル グループ webvpn コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1(1) | このコマンドは、webvpn コンフィギュレーション モードから、トンネル グループの webvpn アトリビュート コンフィギュレーション モードに移動しました。 |

## 使用上のガイドライン

認証方式は、少なくとも 1 つ必要です。AAA 認証、証明書認証、またはその両方を指定できます。これらは、どちらを先に指定してもかまいません。このコマンドを省略した場合、セキュリティ アプライアンスはデフォルトの認証方式である AAA を使用します。

WebVPN 証明書認証では、HTTPS ユーザ証明書を各インターフェイスに求める必要があります。つまり、この選択が機能するためには、証明書認証を指定する前に、**http authentication-certificate** コマンドでインターフェイスを指定しておく必要があります。

リリース 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 webvpn アトリビュート モードの同等のコマンドに変換されます。

## 例

次の例は、トンネル グループ webvpn コンフィギュレーション モードの **authentication** コマンドを示しています。トンネル グループ「test」のメンバーに対して、認証にユーザ名とパスワードを使用する必要があることを指定しています。

```
hostname(config)# tunnel-group test type webvpn
hostname(config)# tunnel-group test webvpn-attributes
hostname(config-webvpn)# authentication aaa
```

次の例は、**authentication** コマンドを示しています。トンネル グループ「docs」のメンバーに対して、認証にデジタル証明書を使用する必要があることを指定しています。

```
hostname(config)# tunnel-group docs type webvpn
hostname(config)# tunnel-group docs webvpn-attributes
hostname(config-webvpn)# authentication certificate
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure tunnel-group** | すべてのトンネル グループのコンフィギュレーションを削除します。 |
| **show running-config tunnel-group** | 現在のトンネル グループ コンフィギュレーションを表示します。 |
| **tunnel-group webvpn-attributes** | WebVPN トンネル グループ アトリビュートを設定する config-webvpn モードに入ります。 |

# authentication eap-proxy

L2TP over IPSec 接続で EAP をイネーブルにし、セキュリティ アプライアンスの PPP の認証プロセスを外部の RADIUS 認証サーバに代理させるには、トンネル グループの ppp アトリビュート コンフィギュレーション モードで **authentication eap-proxy** コマンドを使用します。

コマンドをデフォルト設定（CHAP および MS-CHAP を許可）に戻すには、このコマンドの ***no*** 形式を使用します。

**authentication eap-proxy**

**no authentication eap-proxy**

## シンタックスの説明

このコマンドには、キーワードも引数もありません。

## デフォルト

デフォルトでは、EAP は認証プロトコルとして許可されていません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| トンネル グループ PPP アトリビュート 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 |
|---|---|
| 7.2(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

このアトリビュートは、L2TP/IPSec トンネル グループ タイプだけに適用できます。

## 例

次のコマンドは、config-ppp コンフィギュレーション モードで入力しています。この例では、ppremotegrp というトンネル グループの PPP 接続の EAP による認証を許可しています。

```
hostname(config)# tunnel-group ppremotegrp type IPSec/IPSec
hostname(config)# tunnel-group ppremotegrp ppp-attributes
hostname(config-ppp)# authentication eap
hostname(config-ppp)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure tunnel-group** | 設定されているすべてのトンネル グループを消去します。 |
| **show running-config tunnel-group** | 指定した証明書マップ エントリを表示します。 |
| **tunnel-group-map default-group** | **crypto ca certificate map** コマンドで作成された証明書マップ エントリをトンネル グループに関連付けます。 |

# authentication ms-chap-v1

IPSec 接続を使用した L2TP において、PPP の Microsoft CHAP バージョン 1 認証をイネーブルにするには、トンネル グループ PPP アトリビュート コンフィギュレーション モードで **authentication ms-chap-v1** コマンドを使用します。このプロトコルは CHAP と類似していますが、CHAP のようにサーバがクリアテキスト パスワードを格納および比較するのではなく、暗号化されたパスワードのみを格納および比較するため、セキュリティが高くなります。また、このプロトコルはデータ暗号化のためのキーを MPPE によって生成します。

コマンドをデフォルト設定（CHAP および MS-CHAP を許可）に戻すには、このコマンドの ***no*** 形式を使用します。

Microsoft CHAP バージョン 1 をディセーブルにするには、このコマンドの **no** 形式を使用します。

***authentication ms-chap-v1***

**no authentication ms-chap-v1**

## シンタックスの説明

このコマンドには、引数もキーワードもありません。

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| トンネル グループ PPP アトリビュート | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

このアトリビュートは、L2TP/IPSec トンネル グループ タイプだけに適用できます。

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure tunnel-group** | トンネル グループ データベース全体、または特定のトンネル グループのみを消去します。 |
| **show running-config tunnel-group** | 指定したトンネル グループまたはすべてのトンネル グループの現在の実行トンネル グループ コンフィギュレーションを表示します。 |
| **tunnel-group** | IPSec および WebVPN トンネルの接続に固有なレコードのデータベースを作成および管理します。 |

# authentication ms-chap-v2

IPSec 接続を使用した L2TP において、PPP の Microsoft CHAP バージョン 2 認証をイネーブルにするには、トンネル グループ PPP アトリビュート コンフィギュレーション モードで **authentication ms-chap-v1** コマンドを使用します。このプロトコルは CHAP と類似していますが、CHAP のようにサーバがクリアテキスト パスワードを格納および比較するのではなく、暗号化されたパスワードのみを格納および比較するため、セキュリティが高くなります。また、このプロトコルはデータ暗号化のためのキーを MPPE によって生成します。

コマンドをデフォルト設定（CHAP および MS-CHAP を許可）に戻すには、このコマンドの ***no*** 形式を使用します。

Microsoft CHAP バージョン 2 をディセーブルにするには、このコマンドの **no** 形式を使用します。

***authentication ms-chap-v1***

**no authentication ms-chap-v1**

## シンタックスの説明

このコマンドには、引数もキーワードもありません。

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| トンネル グループ PPP アトリビュート | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

このアトリビュートは、L2TP/IPSec トンネル グループ タイプだけに適用できます。

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure tunnel-group** | トンネル グループ データベース全体、または特定のトンネル グループのみを消去します。 |
| **show running-config tunnel-group** | 指定したトンネル グループまたはすべてのトンネル グループの現在の実行トンネル グループ コンフィギュレーションを表示します。 |
| **tunnel-group** | IPSec および WebVPN トンネルの接続に固有なレコードのデータベースを作成および管理します。 |

# authentication pap

L2TP over IPSec 接続で PPP の PAP による認証を許可するには、トンネル グループの ppp アトリビュート コンフィギュレーション モードで **authentication pap** コマンドを使用します。このプロトコルは、認証中にクリアテキストのユーザ名とパスワードを渡すので安全ではありません。

コマンドをデフォルト設定（CHAP および MS-CHAP を許可）に戻すには、このコマンドの ***no*** 形式を使用します。

**authentication pap**

**no authentication pap**

## シンタックスの説明

このコマンドには、キーワードも引数もありません。

## デフォルト

デフォルトでは、PAP は認証プロトコルとして許可されていません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| トンネル グループ PPP アトリビュート 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 |
|---|---|
| 7.2(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

このアトリビュートは、L2TP/IPSec トンネル グループ タイプだけに適用できます。

## 例

次のコマンドは、config-ppp コンフィギュレーション モードで入力しています。この例では、ppremotegrps というトンネル グループの PPP 接続の PAP による認証を許可しています。

```
hostname(config)# tunnel-group ppremotegrp type IPSec/IPSec
hostname(config)# tunnel-group ppremotegrp ppp-attributes
hostname(config-ppp)# authentication pap
hostname(config-ppp)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure tunnel-group** | 設定されているすべてのトンネル グループを消去します。 |
| **show running-config tunnel-group** | 指定した証明書マップ エントリを表示します。 |
| **tunnel-group-map default-group** | **crypto ca certificate map** コマンドで作成された証明書マップ エントリをトンネル グループに関連付けます。 |

# authentication-port

特定のホストの RADIUS 認証に使用するポート番号を指定するには、AAA サーバ ホスト モードで **authentication-port** コマンドを使用します。認証ポートの指定を削除するには、このコマンドの **no** 形式を使用します。このコマンドは、認証機能の割り当て先となる、リモート RADIUS サーバ ホストの宛先 TCP/UDP ポート番号を指定するものです。

**authentication-port** *port*

**no authentication-port**

## シンタックスの説明

| | |
|---|---|
| *port* | RADIUS 認証用のポート番号（1 ～ 65535）。 |

## デフォルト

デフォルトでは、デバイスはポート 1645 で RADIUS をリッスンします（RFC 2058 に準拠）。ポートを指定しない場合は、RADIUS 認証のデフォルト ポート番号（1645）が使用されます。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| AAA サーバ ホスト | • | • | • | • | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドのセマンティックが変更され、RADIUS サーバを含むサーバ グループでホストごとにサーバ ポートを指定できるようになりました。 |

## 使用上のガイドライン

RADIUS 認証サーバが 1645 以外のポートを使用する場合は、**aaa-server** コマンドで RADIUS サービスを開始する前に、セキュリティ アプライアンスに適切なポートを設定する必要があります。

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

## 例

次の例では、ホスト「1.2.3.4」に対して「srvgrp1」という名前の RADIUS AAA サーバを設定し、タイムアウトを 9 秒に、リトライ間隔を 7 秒に、認証ポートを 1650 に設定しています。

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# authentication-port 1650
hostname(config-aaa-server-host)# exit
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **aaa authentication** | **aaa-server** コマンドで指定したサーバ上での、LOCAL、TACACS+、または RADIUS のユーザ認証、または ASDM ユーザ認証をイネーブルまたはディセーブルにします。 |
| **aaa-server host** | AAA サーバ ホスト コンフィギュレーション モードに入ります。このモードでは、ホストに固有の AAA サーバ パラメータを設定できます。 |
| **clear configure aaa-server** | すべての AAA コマンド文をコンフィギュレーションから削除します。 |
| **show running-config aaa-server** | すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。 |

# authentication-server-group

ユーザの認証で使用する AAA サーバ グループを指定するには、トンネル グループ一般アトリビュート モードで **authentication-server-group** コマンドを使用します。このアトリビュートをデフォルトに戻すには、このコマンドの ***no*** 形式を使用します。

**authentication-server-group** [(*interface_name*)] *server_group* [***LOCAL*** | ***NONE***]

**no authentication-server-group** [(*interface_name*)] *server_group*

## シンタックスの説明

| | |
|---|---|
| *interface_name* | （オプション）IPSec トンネルの終点となるインターフェイスを指定します。 |
| ***LOCAL*** | （オプション）通信障害によってサーバ グループにあるすべてのサーバがアクティブでなくなった場合に、ローカル ユーザ データベースを使用して認証することを指定します。サーバ グループの名前が ***LOCAL*** か ***NONE*** の場合は、ここで ***LOCAL*** キーワードを使用しないでください。 |
| ***NONE*** | （オプション）サーバ グループの名前を none に指定します。認証する必要がないことを示すには、***NONE*** キーワードをサーバ グループ名として使用します。 |
| *server_group* | すでに設定済みの AAA サーバ グループの名前を指定します。 |

## デフォルト

このコマンドのサーバ グループのデフォルト設定は、***LOCAL*** です。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| トンネル グループ一般アトリビュート | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが導入されました。 |
| 7.1(1) | このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般アトリビュート モードに移動しました。 |

## 使用上のガイドライン

認証サーバを設定するには、**aaa-server** コマンドを使用します。サーバ グループ名の最大長は 16 文字です。

このコマンドを入力する前に、AAA サーバ グループを設定しておく必要があります。

リリース 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 グループ一般アトリビュート モードの同等のコマンドに変換されます。すべてのタイプのトンネル グループに、このアトリビュートを適用できるようになりました。

## 例

次のコマンドは、config-general コンフィギュレーション モードで入力しています。この例では、「remotegrp」という IPSec リモートアクセス トンネル グループ用に「aaa-server456」という認証サーバ グループを設定しています。

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# authentication-server-group aaa-server456
hostname(config-tunnel-general)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **aaa-server host** | AAA サーバのパラメータを設定します。 |
| **clear configure tunnel-group** | 設定されているすべてのトンネル グループを消去します。 |
| **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。 |

# authentication-server-group（webvpn）

WebVPN またはいずれかの電子メール プロキシで使用する認証サーバ グループを指定するには、**authentication-server-group** コマンドを使用します。WebVPN の場合、このコマンドは webvpn モードで使用します。電子メール プロキシ（IMAP4S、POP3S、SMTPS）の場合、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。コンフィギュレーションから認証サーバを削除するには、このコマンドの **no** 形式を使用します。

セキュリティ アプライアンスは、ユーザを認証して、ユーザのアイデンティティを確認します。

**authentication-server-group** *group_tag*

**no authentication-server-group**

## シンタックスの説明

| | |
|---|---|
| *group_tag* | 設定済みの認証サーバまたはサーバ グループを指定します。認証サーバを設定するには、**aaa-server** コマンドを使用します。グループ タグの最大長は 16 文字です。 |

## デフォルト

デフォルトでは、認証サーバは設定されていません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| Webvpn | • | — | • | — | — |
| Imap4s | • | — | • | — | — |
| Pop3s | • | — | • | — | — |
| SMTPS | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1)(1) | このコマンドが導入されました。 |
| 7.1(1) | このコマンドがトンネル グループ一般アトリビュート 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

AAA 認証を設定する場合は、このアトリビュートも設定する必要があります。設定しないと、認証が必ず失敗します。

リリース 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 グループ一般アトリビュート モードの同等のコマンドに変換されます。

## 例

次の例は、「WEBVPNAUTH」という名前の認証サーバ グループを使用するように WebVPN サービスを設定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# authentication-server-group WEBVPNAUTH
```

次の例は、「IMAP4SSVRS」という名前の認証サーバ グループを使用するように IMAP4S 電子メール プロキシを設定する方法を示しています。

```
hostname(config)# imap4s
hostname(config-imap4s)# authentication-server-group IMAP4SSVRS
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **aaa-server host** | 認証、認可、アカウンティング サーバを設定します。 |

# authorization-dn-attributes（トンネル グループ一般アトリビュート モード）

サブジェクト DN フィールドのどの部分を認可用のユーザ名として使用するかを指定するには、トンネル グループ一般アトリビュート コンフィギュレーション モードで **authorization-dn-attributes** コマンドを使用します。これらのアトリビュートをデフォルト値に戻すには、このコマンドの ***no*** 形式を使用します。

**authorization-dn-attributes** {*primary-attr* [*secondary-attr*] | ***use-entire-name***}

**no authorization-dn-attributes**

**シンタックスの説明**

| | |
|---|---|
| *primary-attr* | 証明書から認可クエリー用の名前を生成するときに使用するアトリビュートを指定します。 |
| *secondary-attr* | （オプション）プライマリ アトリビュートが存在しない場合に、証明書から認可クエリー用の名前を生成するときに使用する追加のアトリビュートを指定します。 |
| ***use-entire-name*** | セキュリティ アプライアンスがサブジェクト DN（RFC1779）全体を使用して名前を生成するように指定します。 |

**デフォルト**

プライマリ アトリビュートのデフォルト値は CN（Common Name; 通常名）です。

セカンダリ アトリビュートのデフォルト値は OU（Organization Unit; 組織ユニット）です。

**コマンド モード**

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| トンネル グループ一般アトリビュート 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 |
|---|---|
| 7.1(1) | このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般アトリビュート コンフィギュレーション モードに置き換えられました。 |

## 使用上のガイドライン

リリース 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 グループ一般アトリビュート モードの同等のコマンドに変換されます。

プライマリ アトリビュートとセカンダリ アトリビュートには、次のようなものがあります。

| アトリビュート | 定義 |
|---|---|
| CN | Common Name（通常名）：個人、システムなどの名前。 |
| OU | Organizational Unit（組織ユニット）：組織（O）内のサブグループ。 |
| O | Organization（組織）：会社、団体、機関、連合などの名前。 |
| L | Locality（地名）：組織が置かれている市または町。 |
| SP | State/Province（州または都道府県）：組織が置かれている州または都道府県。 |
| C | Country（国または地域）：国または地域を示す 2 文字の短縮形。このコードは、ISO 3166 の国または地域の短縮形に準拠しています。 |
| EA | E-mail address（電子メール アドレス） |
| T | Title（タイトル） |
| N | Name（名前） |
| GN | Given Name（名） |
| SN | Surname（姓） |
| I | Initials（イニシャル） |
| GENQ | Generational Qualifier（世代修飾子） |
| DNQ | Domain Name Qualifier（ドメイン名修飾子） |
| UID | User Identifier（ユーザ識別子） |
| UPN | User Principal Name（ユーザ プリンシパル名） |
| SER | Serial Number（シリアル番号） |
| use-entire-name | DN 名全体を使用 |

## 例

config-ipsec コンフィギュレーション モードに入る次の例では、「remotegrp」という名前のリモート アクセス トンネル グループ（ipsec_ra）を作成し、IPSec グループ アトリビュートを指定して、通常名が認可用のユーザ名として使用されるように定義しています。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# authorization-dn-attributes CN
hostname(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 グループを消去します。 |
| **show running-config tunnel-group** | 指定した証明書マップ エントリを表示します。 |
| **tunnel-group general-attributes** | 名前付きのトンネル グループの一般アトリビュートを指定します。 |

# authorization-dn-attributes（webvpn）

認可用のユーザ名として使用するプライマリ サブジェクト DN フィールドおよびセカンダリ サブジェクト DN フィールドを指定するには、**authorization-dn-attributes** コマンドを使用します。

WebVPN の場合、このコマンドは webvpn モードで使用します。電子メール プロキシ（IMAP4S、POP3S、SMTPS）の場合、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。このアトリビュートをコンフィギュレーションから削除してデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

**authorization-dn-attributes** {*primary-attr*} **[***secondary-attr***] | use-entire-name}**

**no authorization-dn-attributes**

## シンタックスの説明

| | |
|---|---|
| *primary-attr* | デジタル証明書から認可クエリー用の名前を生成するときに使用するアトリビュートを指定します。 |
| *secondary-attr* | （オプション）デジタル証明書から認可クエリー用の名前を生成するときにプライマリ アトリビュートと共に使用する追加のアトリビュートを指定します。 |
| **use-entire-name** | セキュリティ アプライアンスがサブジェクト DN 全体を使用して、デジタル証明書から認可クエリー用の名前を生成するように指定します。 |

## デフォルト

プライマリ アトリビュートのデフォルト値は CN（Common Name; 通常名）です。

セカンダリ アトリビュートのデフォルト値は OU（Organization Unit; 組織ユニット）です。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| Webvpn | • | — | • | — | — |
| Imap4s | • | — | • | — | — |
| Pop3s | • | — | • | — | — |
| SMTPS | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが導入されました。 |
| 7.1(1) | このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般アトリビュート コンフィギュレーション モードに置き換えられました。 |

**使用上のガイドライン**　次の表で、DN フィールドについて説明します。

| DN フィールド | 説明 |
|---|---|
| C | Country（国または地域） |
| CN | Common Name（通常名） |
| DNQ | DN Qualifier（DN 修飾子） |
| EA | E-mail Address（電子メール アドレス） |
| GENQ | Generational Qualifier（世代修飾子） |
| GN | Given Name（名） |
| I | Initials（イニシャル） |
| L | Locality（地名） |
| N | Name（名前） |
| O | Organization（組織） |
| OU | Organizational Unit（組織ユニット） |
| SER | Serial Number（シリアル番号） |
| SN | Surname（姓） |
| SP | State/Province（州または都道府県） |
| T | Title（タイトル） |
| UID | User ID（ユーザ ID） |
| UPN | User Principal Name（ユーザ プリンシパル名） |
| use-entire-name | DN 名全体を使用 |

リリース 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 グループ一般アトリビュート モードの同等のコマンドに変換されます。

**例**　次の例は、WebVPN ユーザが電子メール アドレス（プライマリ アトリビュート）および組織ユニット（セカンダリ アトリビュート）に基づいて認可されるように指定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# authorization-dn-attributes EA OU
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **authorization-required** | ユーザが接続前に正常に認可されることを必須とします。 |

# authorization-required（トンネル グループ一般アトリビュート モード）

ユーザが接続前に正常に認可されることを必須とするには、トンネル グループ一般アトリビュート コンフィギュレーション モードで **authorization-required** コマンドを使用します。このアトリビュート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。

**authorization-required**

**no authorization-required**

## デフォルト

デフォルトでは、このコマンドの設定はディセーブルになっています。

## シンタックスの説明

このコマンドには、引数もキーワードもありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| トンネル グループ一般アトリビュート 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 |
|---|---|
| 7.1(1) | このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般アトリビュート コンフィギュレーション モードに置き換えられました。 |

## 使用上のガイドライン

リリース 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 グループ一般アトリビュート モードの同等のコマンドに変換されます。

## 例

グローバル コンフィギュレーション モードに入る次の例では、「remotegrp」という名前のリモート アクセス トンネル グループを介して接続するユーザが、完全な DN に基づく認可を受けることを必須としています。最初のコマンドでは、「remotegrp」という名前のリモート グループのトンネル グループ タイプを ipsec_ra（IPSec リモートアクセス）と設定しています。2 番目のコマンドで、指定したトンネル グループのトンネル グループ一般アトリビュート コンフィギュレーション モードに入り、最後のコマンドで、指定したトンネル グループで認可が必要となるように指定しています。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# authorization-required
hostname(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 グループを消去します。 |
| **show running-config tunnel-group** | 指定した証明書マップ エントリを表示します。 |
| **tunnel-group general-attributes** | 名前付きのトンネル グループの一般アトリビュートを指定します。 |

# authorization-required（webvpn）

WebVPN ユーザまたは電子メール プロキシ ユーザが接続前に正常に認可されることを必須とするには、**authorization-required** コマンドを使用します。WebVPN の場合、このコマンドは webvpn モードで使用します。電子メール プロキシ（IMAP4S、POP3S、SMTPS）の場合、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。アトリビュートをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

**authorization-required**

**no authorization-required**

## シンタックスの説明

このコマンドには、引数もキーワードもありません。

## デフォルト

デフォルトでは、authorization-required はディセーブルになっています。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| Webvpn | • | — | • | — | — |
| Imap4s | • | — | • | — | — |
| Pop3s | • | — | • | — | — |
| SMTPS | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが導入されました。 |
| 7.1(1) | このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般アトリビュート コンフィギュレーション モードに置き換えられました。 |

## 使用上のガイドライン

リリース 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 グループ一般アトリビュート モードの同等のコマンドに変換されます。

## 例

次の例は、WebVPN ユーザが認可を受けることを必須とする方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# authorization-required
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **authorization-dn-attributes（webvpn）** | 認可用のユーザ名として使用するプライマリ サブジェクト DN フィールドおよびセカンダリ サブジェクト DN フィールドを指定します。 |

# authorization-server-group（トンネル グループ一般アトリビュート モード）

ユーザ認可で使用する AAA サーバ グループ（およびオプションでインターフェイス）を指定するには、トンネル グループ一般アトリビュート モードで **authorization-server-group** 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。

**authorization-server-group** [(*interface-id*)] *server_group*

**no authorization-server-group** [(*interface-id*)]

## シンタックスの説明

| | |
|---|---|
| (*interface-id*) | （オプション）認可を実行するインターフェイスを指定します。このパラメータを指定する場合はカッコが必要です。 |
| *server_group* | 設定済みの認可サーバまたはサーバ グループの名前を指定します。 |

## デフォルト

デフォルトでは、このコマンドの設定は ***no authorization-server-group*** になっています。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| トンネル グループ一般アトリビュート 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) | このコマンドが導入されました。 |
| 7.1(1) | このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般アトリビュート コンフィギュレーション モードに置き換えられました。このコマンドは、すべてのトンネル グループ アトリビュート タイプに使用できるようになりました。 |
| 7.2(2) | インターフェイス単位で IPSec 接続の認可を行えるように機能が拡張されました。 |

## 使用上のガイドライン

VPN 認可が LOCAL と定義されている場合は、デフォルト グループ ポリシー DfltGrpPolicy に設定されているアトリビュートが適用されます。

認可サーバ グループを設定するには **aaa-server** コマンドを使用し、設定済みの aaa サーバ グループにサーバを追加するには **aaa-server-host** コマンドを使用します。

## 例

config-general コンフィギュレーション モードに入る次の例では、「remotegrp」という名前の IPSec リモートアクセス トンネル グループに「aaa-server78」という名前の認可サーバ グループを設定しています。

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# authorization-server-group aaa-server78
hostname(config-tunnel-general)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **aaa-server host** | AAA サーバのパラメータを設定します。 |
| **clear configure tunnel-group** | 設定されているすべてのトンネル グループを消去します。 |
| **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 グループの一般アトリビュートを指定します。 |

# authorization-server-group（webvpn）

WebVPN またはいずれかの電子メール プロキシで使用する認可サーバ グループを指定するには、**authorization-server-group** コマンドを使用します。WebVPN の場合、このコマンドは webvpn モードで使用します。電子メール プロキシ（IMAP4S、POP3S、SMTPS）の場合、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。コンフィギュレーションから認可サーバを削除するには、このコマンドの **no** 形式を使用します。

セキュリティ アプライアンスは、認可を使用して、ユーザがネットワーク リソースに対して許可されるアクセス レベルを確認します。

**authorization-server-group** *group_tag*

**no authorization-server-group**

## シンタックスの説明

| | |
|---|---|
| *group_tag* | 設定済みの認可サーバまたはサーバ グループを指定します。認可サーバを設定するには、**aaa-server** コマンドを使用します。 |

## デフォルト

デフォルトでは、認可サーバは設定されていません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| Webvpn | • | — | • | — | — |
| Imap4s | • | — | • | — | — |
| Pop3s | • | — | • | — | — |
| SMTPS | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが導入されました。 |
| 7.1(1) | このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般アトリビュート コンフィギュレーション モードに置き換えられました。 |

## 使用上のガイドライン

リリース 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 グループ一般アトリビュート モードの同等のコマンドに変換されます。

## 例

次の例は、「WebVPNpermit」という名前の認可サーバ グループを使用するように WebVPN サービスを設定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# authorization-server-group WebVPNpermit
```

次の例は、「POP3Spermit」という名前の認可サーバ グループを使用するように POP3S 電子メール プロキシを設定する方法を示しています。

```
hostname(config)# pop3s
hostname(config-pop3s)# authorization-server-group POP3Spermit
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **aaa-server host** | 認証、認可、アカウンティング サーバを設定します。 |

# auth-prompt

セキュリティ アプライアンスを介したユーザ セッションの AAA チャレンジ テキストを指定または変更するには、グローバル コンフィギュレーション モードで **auth-prompt** コマンドを使用します。認証チャレンジ テキストを削除するには、このコマンドの **no** 形式を使用します。

**auth-prompt prompt** [**prompt** | **accept** | **reject**] *string*

**no auth-prompt prompt** [ **prompt** | **accept** | **reject**]

**シンタックスの説明**

| | |
|---|---|
| **accept** | Telnet 経由のユーザ認証を受け入れる場合に、プロンプトとして *string* を表示します。 |
| **prompt** | このキーワードの後に、AAA チャレンジ プロンプトの文字列を入力します。 |
| **reject** | Telnet 経由のユーザ認証を拒否する場合に、プロンプトとして *string* を表示します。 |
| *string* | 235 文字または 31 単語（どちらか最初に達した方）までの英数字で構成される文字列。特殊文字、スペース、および句読点を使用できます。文字列を終了するには、疑問符を入力するか、**Enter** キーを押します。疑問符は文字列に含まれます。 |

**デフォルト**

認証プロンプトを指定しない場合は、次のようになります。

- FTP ユーザには `FTP authentication` が表示される。
- HTTP ユーザには `HTTP Authentication` が表示される。
- Telnet ユーザにはチャレンジ テキストが表示されない。

**コマンド モード**

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル 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) | セマンティックの小さな変更。 |

## 使用上のガイドライン

**auth-prompt** コマンドを使用すると、TACACS+ サーバまたは RADIUS サーバからのユーザ認証が必要である場合に、セキュリティ アプライアンスを介した HTTP アクセス、FTP アクセス、および Telnet アクセスに対して表示される AAA チャレンジ テキストを指定できます。このテキストは飾りのようなもので、ユーザのログイン時に、ユーザ名プロンプトとパスワード プロンプトの上に表示されます。

ユーザ認証が Telnet から発生する場合は、**accept** オプションと **reject** オプションを使用すると、認証試行が AAA サーバで受け入れられたか拒否されたかを示す異なるステータス プロンプトを表示できます。

AAA サーバがユーザを認証すると、セキュリティ アプライアンスはユーザに **auth-prompt accept** テキストを表示します（指定されている場合）。認証に失敗すると、**reject** テキストを表示します（指定されている場合）。HTTP セッションおよび FTP セッションの認証では、プロンプトにチャレンジ テキストだけが表示されます。**accept** テキストも **reject** テキストも表示されません。

**（注）** Microsoft Internet Explorer では、認証プロンプトに最大 37 文字表示されます。Netscape Navigator では認証プロンプトに最大 120 文字、Telnet および FTP では最大 235 文字表示されます。

## 例

次の例では、認証プロンプトを「Please enter your username and password」という文字列に設定しています。

```
hostname(config)# auth-prompt prompt Please enter your username and password
```

コンフィギュレーションにこの文字列を追加すると、ユーザには次のプロンプトが表示されます。

```
Please enter your username and password
User Name:
Password:
```

Telnet ユーザに対しては、セキュリティ アプライアンスが認証試行を受け入れたときに表示するメッセージと、拒否したときに表示するメッセージを別々に指定することもできます。次に例を示します。

```
hostname(config)# auth-prompt reject Authentication failed. Try again.
hostname(config)# auth-prompt accept Authentication succeeded.
```

次の例では、認証が成功したときの認証プロンプトを「You’re OK.」という文字列に設定しています。

```
hostname(config)# auth-prompt accept You’re OK.
```

正常に認証されたユーザには、次のメッセージが表示されます。

```
You’re OK.
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure auth-prompt** | 指定済みの認証プロンプト チャレンジ テキストがある場合、そのテキストを削除して、デフォルト値に戻します。 |
| **show running-config auth-prompt** | 現在の認証プロンプト チャレンジ テキストを表示します。 |

# auto-signon

WebVPN ユーザ ログイン クレデンシャルを内部サーバに自動的に渡すようにセキュリティ アプライアンスを設定するには、webvpn コンフィギュレーション モード、webvpn グループ コンフィギュレーション モード、または webvpn ユーザ名コンフィギュレーション モードのいずれかのモードで **auto-signon** コマンドを使用します。認証方式は、NTLM（NTLMv1）認証、HTTP Basic 認証、またはその両方が可能です。特定のサーバに対する auto-signon をディセーブルにするには、このコマンドの **no** 形式を元の **ip**、**uri**、および **auth-type** 引数と共に使用します。すべてのサーバに対する auto-signon をディセーブルにするには、このコマンドの **no** 形式を引数なしで指定します。

**auto-signon allow** {**ip** *ip-address ip-mask* | **uri** *resource-mask*} **auth-type** {**basic** | **ntlm** | **all**}

**no auto-signon** [**allow** {**ip** *ip-address ip-mask* | **uri** *resource-mask*} **auth-type** {**basic** | **ntlm** | **all**}]

## シンタックスの説明

| | |
|---|---|
| **all** | NTLM と HTTP Basic の両方の認証方式を指定します。 |
| **allow** | 特定のサーバに対する認証をイネーブルにします。 |
| **auth-type** | 認証方式の選択をイネーブルにします。 |
| **basic** | HTTP Basic 認証方式を指定します。 |
| **ip** | IP アドレスとマスクで認証先のサーバを特定することを指定します。 |
| *ip-address* | *ip-mask* と共に、認証先のサーバの IP アドレス範囲を特定します。 |
| *ip-mask* | *ip-address* と共に、認証先のサーバの IP アドレス範囲を特定します。 |
| **ntlm** | NTLMv1 認証方式を指定します。 |
| *resource-mask* | 認証先のサーバの URI マスクを特定します。 |
| **uri** | URI マスクで認証先のサーバを特定することを指定します。 |

## デフォルト

デフォルトでは、この機能はすべてのサーバに対してディセーブルになっています。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| WebVPN コンフィギュレーション | • | — | • | — | — |
| WebVPN グループ ポリシー コンフィギュレーション | • | — | • | — | — |
| WebVPN ユーザ名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 |
|---|---|
| 7.1.1 | このコマンドが導入されました。 |

## 使用上のガイドライン

**auto-signon** コマンドは、WebVPN ユーザのためのシングル サインオン方式です。このコマンドは、WebVPN ログイン クレデンシャル（ユーザ名とパスワード）を NTLM 認証、HTTP Basic 認証、またはその両方を使用する認証用の内部サーバに渡します。複数の auto-signon コマンドを入力でき、その際にはコマンドは入力順序に従って（最初に入力したコマンドが先に）処理されます。

auto-signon 機能は、webvpn コンフィギュレーション モード、webvpn グループ コンフィギュレーション モード、または webvpn ユーザ名コンフィギュレーション モードの 3 つのモードで使用できます。一般的な優先動作は、ユーザ名がグループに優先する場合、およびグループがグローバルに優先する場合に適用されます。どのモードを選択するかは、必要な認証範囲によって異なります。次の表を参照してください。

| モード | 範囲 |
|---|---|
| WebVPN コンフィギュレーション | すべての WebVPN ユーザ（グローバル） |
| WebVPN グループ コンフィギュレーション | グループ ポリシーで定義されている WebVPN ユーザのサブセット |
| WebVPN ユーザ名コンフィギュレーション | 個々の WebVPN ユーザ |

## 例

次のコマンド例では、すべての WebVPN ユーザに対して、NTLM 認証を使用する auto-signon を設定しています。認証先のサーバの IP アドレスの範囲は、10.1.1.0 ～ 10.1.1.255 です。

```
hostname(config)# webvpn
hostname(config-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type ntlm
```

次のコマンド例では、すべての WebVPN ユーザに対して、HTTP Basic 認証を使用する auto-signon を設定しています。認証先のサーバは、URI マスク https://*.example.com/* で定義されています。

```
hostname(config)# webvpn
hostname(config-webvpn)# auto-signon allow uri https://*.example.com/* auth-type basic
```

次のコマンド例では、WebVPN ユーザ ExamplePolicy グループに対して、HTTP Basic 認証または NTLM 認証を使用する auto-signon を設定しています。認証先のサーバは、URI マスク https://*.example.com/* で定義されています。

```
hostname(config)# group-policy ExamplePolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# auto-signon allow uri https://*.example.com/* auth-type
all
```

次のコマンド例では、Anyuser という名前のユーザに対して、HTTP Basic 認証を使用する auto-signon を設定しています。認証先のサーバの IP アドレスの範囲は、10.1.1.0 ～ 10.1.1.255 です。

```
hostname(config)# username Anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0
auth-type basic
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show running-config webvpn auto-signon** | 実行コンフィギュレーションの auto-signon 割り当てを表示します。 |

# auto-summary

RIP の経路集約を再度イネーブルにするには、ルータ コンフィギュレーション モードで **auto-summary** コマンドを使用します。RIP の経路集約をディセーブルにするには、このコマンドの **no** 形式を使用します。

**auto-summary**

**no auto-summary**

## シンタックスの説明

このコマンドには、引数もキーワードもありません。

## デフォルト

RIP バージョン 1 と 2 では、経路集約がイネーブルになっています。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| ルータ コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

経路集約によって、ルーティング テーブル内のルーティング情報の量が少なくなります。

RIP バージョン 1 は、常に自動集約を使用します。RIP バージョン 1 の自動集約機能をディセーブルにすることはできません。

RIP バージョン 2 を使用している場合は、**no auto-summary** コマンドを指定して、自動集約をオフにすることができます。接続が切断されているサブネット間でルーティングする必要がある場合は、自動集約をディセーブルにします。自動集約をディセーブルにすると、サブネットがアドバタイズされます。

実行コンフィギュレーションに表示されるのは、このコマンドの **no** 形式のみです。

## 例

次の例では、RIP の経路集約をディセーブルにしています。

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# version 2
hostname(config-router)# no auto-summary
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **clear configure rip** | 実行コンフィギュレーションからすべての RIP コマンドを消去します。 |
| **router rip** | RIP ルーティング プロセスをイネーブルにし、RIP ルータ コンフィギュレーション モードに入ります。 |
| **show running-config rip** | 実行コンフィギュレーション内の RIP コマンドを表示します。 |

# auto-update device-id

Auto Update Server 用のセキュリティ アプライアンス デバイス ID を設定するには、グローバル コンフィギュレーション モードで **auto-update device-id** コマンドを使用します。デバイス ID を削除するには、このコマンドの **no** 形式を使用します。

**auto-update device-id** [**hardware-serial** | **hostname** | **ipaddress** [*if_name*] | **mac-address** [*if_name*] | **string** *text*]

**no auto-update device-id** [**hardware-serial** | **hostname** | **ipaddress** [*if_name*] | **mac-address** [*if_name*] | **string** *text*]

**シンタックスの説明**

| | |
|---|---|
| **hardware-serial** | セキュリティ アプライアンスのハードウェア シリアル番号を使用して、このデバイスを一意に識別します。 |
| **hostname** | セキュリティ アプライアンスのホスト名を使用して、このデバイスを一意に識別します。 |
| **ipaddress** [*if_name*] | セキュリティ アプライアンスの IP アドレスを使用して、セキュリティ アプライアンスを一意に識別します。デフォルトでは、セキュリティ アプライアンスは、Auto Update Server との通信に使用するインターフェイスを使用します。別の IP アドレスを使用する場合は、*if_name* を指定します。 |
| **mac-address** [*if_name*] | セキュリティ アプライアンスの MAC アドレスを使用して、セキュリティ アプライアンスを一意に識別します。デフォルトでは、セキュリティ アプライアンスは、Auto Update Server との通信に使用するインターフェイスの MAC アドレスを使用します。別の MAC アドレスを使用する場合は、*if_name* を指定します。 |
| **string** *text* | デバイスを Auto Update Server に対して一意に識別するためのテキスト文字列を指定します。 |

**コマンド履歴**

| リリース | 変更内容 |
|---|---|
| 7.0 | このコマンドが導入されました。 |

**デフォルト**

デフォルトの ID はホスト名です。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

## 例

次の例では、デバイス ID をシリアル番号に設定しています。

```
hostname(config)# auto-update device-id hardware-serial
```

## 関連コマンド

| | |
|---|---|
| **auto-update poll-period** | セキュリティ アプライアンスが Auto Update Server からのアップデートをチェックする頻度を設定します。 |
| **auto-update server** | Auto Update Server を指定します。 |
| **auto-update timeout** | このタイムアウト期間内に Auto Update Server にアクセスしない場合、セキュリティ アプライアンスを通過するトラフィックを停止します。 |
| **clear configure auto-update** | Auto Update Server のコンフィギュレーションを消去します。 |
| **show running-config auto-update** | Auto Update Server のコンフィギュレーションを表示します。 |

# auto-update poll-at

セキュリティ アプライアンスで Auto Update Server をポーリングする特定の日時を設定するには、グローバル コンフィギュレーション モードで **auto-update poll-at** コマンドを使用します。

**auto-update poll-at** *days-of-the-week time* [**randomize** *minutes*] [*retry_count* [*retry_period*]]

**no auto-update poll-at** *days-of-the-week time* [**randomize** *minutes*] [*retry_count* [*retry_period*]]

## シンタックスの説明

| | |
|---|---|
| *days-of-the-week* | 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）から曜日またはその組み合せを指定します。この他にも、daily（月曜日から日曜日まで）、weekdays（月曜日から金曜日まで）、weekend（土曜日と日曜日）を指定できます。 |
| *time* | ポーリングを開始する時刻を HH:MM 形式で指定します。たとえば、8:00 は午前 8 時を、20:00 は午後 8 時を示します。 |
| **randomize** *minutes* | 指定した開始時刻以後、任意にポーリングする期間（1 ～ 1439 分）を指定します。 |
| *retry_count* | Auto Update Server への最初の接続試行が失敗した後に、再接続を何回試行するかを指定します。デフォルトは 0 です。 |
| *retry_period* | 接続を再試行する間隔を指定します。デフォルトは 5 分です。1 ～ 35791 分に指定できます。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル 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 |
|---|---|
| 7.2(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

**auto-update poll-at** コマンドは、アップデートがあるかどうかを確認するためにポーリングするタイミングを指定します。**randomize** オプションをイネーブルにすると、*time* で指定した開始時刻以後、指定した時間（分単位）内の任意の時刻にポーリングされます。**auto-update poll-at** コマンドと **auto-update poll-period** コマンドは、互いに排他的です。設定できるのは、いずれか一方だけです。

## 例

次の例では、セキュリティ アプライアンスで毎週金曜日と土曜日の午後 10 時から 11 時の間、任意の時刻に Auto Update Server をポーリングするように設定しています。また、接続できなかった場合は、10 分間隔で 2 回再試行します。

```
hostname(config)# auto-update poll-at Friday Saturday 22:00 randomize 60 2 10
hostname(config)# auto-update server http://192.168.1.114/aus/autoupdate.asp
```

## 関連コマンド

| | |
|---|---|
| **auto-update device-id** | Auto Update Server 用のセキュリティ アプライアンス デバイス ID を設定します。 |
| **auto-update poll-period** | セキュリティ アプライアンスが Auto Update Server からのアップデートをチェックする頻度を設定します。 |
| **auto-update timeout** | このタイムアウト期間内に Auto Update Server にアクセスしない場合、セキュリティ アプライアンスを通過するトラフィックを停止します。 |
| **clear configure auto-update** | Auto Update Server のコンフィギュレーションを消去します。 |
| **management-access** | セキュリティ アプライアンス上の内部管理インターフェイスにアクセスできるようにします。 |
| **show running-config auto-update** | Auto Update Server のコンフィギュレーションを表示します。 |

# auto-update poll-period

セキュリティ アプライアンスが Auto Update Server からのアップデートをチェックする頻度を設定するには、グローバル コンフィギュレーション モードで **auto-update poll-period** コマンドを使用します。このパラメータをデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

**auto-update poll-period** *poll_period* [*retry_count* [*retry_period*]]

**no auto-update poll-period** *poll_period* [*retry_count* [*retry_period*]]

## シンタックスの説明

| | |
|---|---|
| *poll_period* | Auto Update Server をポーリングする頻度を分単位で指定します（1 ～ 35791）。デフォルトは 720 分（12 時間）です。 |
| *retry_count* | Auto Update Server への最初の接続試行が失敗した後に、再接続を何回試行するかを指定します。デフォルトは 0 です。 |
| *retry_period* | 接続を試行する間隔を分単位で指定します（1 ～ 35791）。デフォルトは 5 分です。 |

## デフォルト

デフォルトのポーリング間隔は 720 分（12 時間）です。

Auto Update Server への最初の接続試行が失敗した後に再接続を試行する回数は、デフォルトでは 0 です。

接続試行のデフォルト間隔は、5 分です。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル 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 | このコマンドが導入されました。 |

## 使用上のガイドライン

**auto-update poll-at** コマンドと **auto-update poll-period** コマンドは、互いに排他的です。設定できるのは、いずれか一方だけです。

## 例

次の例では、ポーリング間隔を 360 分に、リトライ回数を 1 回に、リトライ間隔を 3 分に設定しています。

```
hostname(config)# auto-update poll-period 360 1 3
```

**関連コマンド**

| | |
|---|---|
| **auto-update device-id** | Auto Update Server 用のセキュリティ アプライアンス デバイス ID を設定します。 |
| **auto-update server** | Auto Update Server を指定します。 |
| **auto-update timeout** | このタイムアウト期間内に Auto Update Server にアクセスしない場合、セキュリティ アプライアンスを通過するトラフィックを停止します。 |
| **clear configure auto-update** | Auto Update Server のコンフィギュレーションを消去します。 |
| **show running-config auto-update** | Auto Update Server のコンフィギュレーションを表示します。 |

# auto-update server

Auto Update Server を指定するには、グローバル コンフィギュレーション モードで **auto-update server** コマンドを使用します。サーバを削除するには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンスは、定期的に Auto Update Server にアクセスして、コンフィギュレーション、オペレーティング システム、および ASDM のアップデートがないか調べます。

**auto-update server** *url* [**source** *interface*] [*verify-certificate*]

**no auto-update server** *url* [**source** *interface*] [*verify-certificate*]

**シンタックスの説明**

| | |
|---|---|
| *url* | Auto Update Server の場所を、シンタックス **http**[**s**]**:**[[*user:password@*]*location* [*:port* ]] / *pathname* を使用して指定します。 |
| *interface* | Auto Update Server に要求を送信する場合に使用するインターフェイスを指定します。 |
| *verify_certificate* | Auto Update Server によって返される証明書を確認します。 |

**デフォルト**

デフォルトの動作や値はありません。

**コマンド モード**

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル 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 | このコマンドが導入されました。 |
| 7.2(1) | 複数のサーバをサポートできるようにコマンドが変更されました。 |

**使用上のガイドライン**

自動アップデート用に複数のサーバを設定できます。アップデートがあるかどうかをチェックするときは、まず 1 台目のサーバに接続しようとし、接続できなかった場合は、2 台目のサーバとの接続を試みます。この要領で、すべてのサーバとの接続が試みられます。どのサーバとも接続できないと、auto-update poll-period コマンドで再試行するように設定している場合は、最初のサーバに戻って再試行されます。

自動アップデート機能を正しく動作させるには、**boot system configuration** コマンドを使用して、有効なブート イメージを指定する必要があります。同様に、ASDM ソフトウェア イメージを自動アップデートするには、**asdm image** コマンドを使用する必要があります。

**source** *interface* 引数に指定したインターフェイスが、**management-access** コマンドで指定したインターフェイスと同じである場合、Auto Update Server への要求は VPN トンネル経由で送信されます。

**例**

次の例では、Auto Update Server の URL を設定し、インターフェイス outside を指定しています。

```
hostname(config)# auto-update server http://10.1.1.1:1741/ source outside
```

**関連コマンド**

| | |
|---|---|
| **auto-update device-id** | Auto Update Server 用のセキュリティ アプライアンス デバイス ID を設定します。 |
| **auto-update poll-period** | セキュリティ アプライアンスが Auto Update Server からのアップデートをチェックする頻度を設定します。 |
| **auto-update timeout** | このタイムアウト期間内に Auto Update Server にアクセスしない場合、セキュリティ アプライアンスを通過するトラフィックを停止します。 |
| **clear configure auto-update** | Auto Update Server のコンフィギュレーションを消去します。 |
| **management-access** | セキュリティ アプライアンス上の内部管理インターフェイスにアクセスできるようにします。 |
| **show running-config auto-update** | Auto Update Server のコンフィギュレーションを表示します。 |

# auto-update timeout

Auto Update Server へのアクセスに関するタイムアウト期間を設定するには、グローバル コンフィギュレーション モードで **auto-update timeout** コマンドを使用します。このタイムアウト期間内に Auto Update Server にアクセスしないと、セキュリティ アプライアンスは、セキュリティ アプライアンスを通過するすべてのトラフィックを停止させます。タイムアウトを設定することで、セキュリティ アプライアンスのイメージとコンフィギュレーションを常に最新の状態に保つことができます。タイムアウトを削除するには、このコマンドの **no** 形式を使用します。

**auto-update timeout** *period*

**no auto-update timeout** [*period*]

## シンタックスの説明

| | |
|---|---|
| *period* | タイムアウト期間を分単位で指定します（1 ～ 35791）。デフォルトは 0 で、タイムアウトはありません。タイムアウトを 0 に設定することはできません。タイムアウトを 0 にリセットするには、このコマンドの **no** 形式を使用します。 |

## デフォルト

デフォルトのタイムアウトは 0 で、セキュリティ アプライアンスはタイムアウトしないように設定されています。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル 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 | このコマンドが導入されました。 |

## 使用上のガイドライン

タイムアウト状態は、システム ログ メッセージ 201008 で報告されます。

## 例

次の例では、タイムアウトを 24 時間に設定しています。

```
hostname(config)# auto-update timeout 1440
```

## 関連コマンド

| | |
|---|---|
| **auto-update device-id** | Auto Update Server 用のセキュリティ アプライアンス デバイス ID を設定します。 |
| **auto-update poll-period** | セキュリティ アプライアンスが Auto Update Server からのアップデートをチェックする頻度を設定します。 |
| **auto-update server** | Auto Update Server を指定します。 |
| **clear configure auto-update** | Auto Update Server のコンフィギュレーションを消去します。 |
| **show running-config auto-update** | Auto Update Server のコンフィギュレーションを表示します。 |