
# same-security-traffic through share-ratio コマンド

## same-security-traffic

同じセキュリティレベルのインターフェイス間での通信を許可するか、またはトラフィックが同じインターフェイスに入って同じインターフェイスから出ることを許可するには、グローバル コンフィギュレーション モードで **same-security-traffic** コマンドを使用します。同じセキュリティレベルのトラフィックをディセーブルにするには、このコマンドの **no** 形式を使用します。

**same-security-traffic permit** {**inter-interface** | **intra-interface**}

**no same-security-traffic permit** {**inter-interface** | **intra-interface**}

**構文の説明**

| | |
|---|---|
| **inter-interface** | 同じセキュリティ レベルを持つ異なるインターフェイス間での通信を許可します。 |
| **intra-interface** | 同じインターフェイスに入って同じインターフェイスから出る通信を許可します。 |

**デフォルト**

このコマンドは、デフォルトでディセーブルになっています。

**コマンド モード**

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが追加されました。 |
| 7.2(1) | **intra-interface** キーワードを使用すると、IPsec トラフィックだけではなく、すべてのトラフィックが同じインターフェイスに出入りできるようになりました。 |

## 使用上のガイドライン

同じセキュリティ レベルのインターフェイス間での通信を許可すると（**same-security-traffic inter-interface** コマンドを使用してイネーブルにします）、次の利点があります。

- 101 より多い数の通信インターフェイスを設定できます。各インターフェイスで異なるレベルを使用する場合は、レベルごと（0 ～ 100）に 1 つのインターフェイスのみを設定できます。
- アクセス リストなしで、すべての同じセキュリティ レベルのインターフェイス間で自由にトラフィックを送受信できます。

**same-security-traffic intra-interface** コマンドを使用すると、トラフィックが同じインターフェイスに入って同じインターフェイスから出ることができます。この動作は、通常は許可されていません。この機能は、あるインターフェイスに入り、その後同じインターフェイスからルーティングされる VPN トラフィックの場合に役立ちます。この場合、VPN トラフィックは暗号化解除されたり、別の VPN 接続のために再度暗号化されたりする場合があります。たとえば、ハブ アンド スポーク VPN ネットワークがあり、ASA がハブ、リモート VPN ネットワークがスポークの場合、あるスポークが別のスポークと通信するためには、トラフィックは ASA に入ってから他のスポークに再度ルーティングされる必要があります。

（注） **same-security-traffic intra-interface** コマンドによって許可されるすべてのトラフィックには、引き続きファイアウォール ルールが適用されます。リターン トラフィックが ASA を通過できない原因となるため、非対称なルーティング状態にしないよう注意してください。

## 例

次に、同じセキュリティ レベルのインターフェイス間での通信をイネーブルにする例を示します。

```
ciscoasa(config)# same-security-traffic permit inter-interface
```

次に、トラフィックが同じインターフェイスに入って同じインターフェイスから出られるようにする例を示します。

```
ciscoasa(config)# same-security-traffic permit intra-interface
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show running-config same-security-traffic** | **same-security-traffic** コンフィギュレーションを表示します。 |

# sasl-mechanism

LDAP クライアントを LDAP サーバに対して認証するための Simple Authentication and Security Layer（SASL）メカニズムを指定するには、AAA サーバ ホスト コンフィギュレーション モードで **sasl-mechanism** コマンドを使用します。SASL 認証メカニズムのオプションは、**digest-md5** および **kerberos** です。

認証メカニズムをディセーブルにするには、このコマンドの **no** 形式を使用します。

**sasl-mechanism** {**digest-md5** | **kerberos** *server-group-name*}

**no sasl-mechanism** {**digest-md5** | **kerberos** *server-group-name*}

(注) VPN ユーザにとっては、ASA が LDAP サーバへのクライアント プロキシとして動作するため、ここでの LDAP クライアントとは ASA を意味しています。

## 構文の説明

| | |
|---|---|
| **digest-md5** | ASA は、ユーザ名とパスワードから計算された MD5 値を使用して応答します。 |
| **kerberos** | ASA は、Generic Security Services Application Programming Interface（GSSAPI）Kerberos メカニズムを使用してユーザ名とレルムを送信することによって応答します。 |
| *server-group-name* | 最大 64 文字の Kerberos AAA サーバ グループを指定します。 |

## デフォルト

デフォルトの動作や値はありません。ASA は、認証パラメータをプレーン テキストで LDAP サーバに渡します。

(注) SASL を設定していない場合は、**ldap-over-ssl** コマンドを使用して、SSL によって LDAP 通信を保護することを推奨します。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

ASA が SASL メカニズムを使用して LDAP サーバに対する認証を行うよう指定するには、このコマンドを使用します。

ASA と LDAP サーバの両方で、複数の SASL 認証メカニズムをサポートできます。SASL 認証をネゴシエートする場合、ASA はサーバに設定されている SASL メカニズムのリストを取得して、ASA とサーバの両方に設定されているメカニズムのうち最も強力な認証メカニズムを設定します。Kerberos メカニズムは、Digest-MD5 メカニズムよりも強力です。たとえば、LDAP サーバと ASA の両方でこれら 2 つのメカニズムがサポートされている場合、ASA では、より強力な Kerberos メカニズムが選択されます。

各メカニズムは独立して設定されるため、SASL メカニズムをディセーブルにするには、ディセーブルにする各メカニズムに対して別々に **no** コマンドを入力する必要があります。明示的にディセーブルにしないメカニズムは引き続き有効です。たとえば、両方の SASL メカニズムをディセーブルにするには、次の両方のコマンドを入力する必要があります。

**no sasl-mechanism digest-md5**

**no sasl-mechanism kerberos** *server-group-name*

## 例

次に、AAA サーバ ホスト コンフィギュレーション モードで、名前が ldapsvr1、IP アドレスが 10.10.0.1 の LDAP サーバに対する認証のために SASL メカニズムをイネーブルにする例を示します。この例では、SASL digest-md5 認証メカニズムがイネーブルにされています。

```
ciscoasa(config)# aaa-server ldapsvr1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# sasl-mechanism digest-md5
```

次に、SASL Kerberos 認証メカニズムをイネーブルにして、Kerberos AAA サーバとして kerb-servr1 を指定する例を示します。

```
ciscoasa(config)# aaa-server ldapsvr1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# sasl-mechanism kerberos kerbsvr1
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **ldap-over-ssl** | SSL が LDAP クライアントとサーバ間の接続を保護することを指定します。 |
| **server-type** | LDAP サーバ ベンダーに Microsoft または Sun のいずれかを指定します。 |
| **ldap attribute-map**（グローバル コンフィギュレーション モード） | ユーザ定義の属性名を Cisco LDAP 属性名にマッピングするために、LDAP 属性マップを作成して名前を付けます。 |

# saml idp

新しい SAML IdP を追加するには、webvpn コンフィギュレーション モードで **saml idp** コマンドを使用します。SAML IdP を削除するには、このコマンドの **no** 形式を使用します。

**saml idp** *idp-entityID*

**no saml idp** *idp-entityID*

## 構文の説明

| | |
|---|---|
| **base-URL** | クライアントレス VPN のベース URL。サードパーティ製 IdP に提供される SAML メタデータで使用されます。それによって、IdP はエンドユーザを ASA へリダイレクトできます。 |
| **idp-entityID** | ASA が使用するように設定している SAML Idp のエンティティ ID。 |
| **internal** | IdP が内部ネットワーク内にある場合は、このフラグを設定します。 |
| シグニチャ<br>**signature <value>** | SAML 要求内の署名を有効または無効にします。<br>（オプション）署名を有効にし、SAML 要求で特定の方式を使用します。 |
| **timeout assertion** | NotBefore とタイムアウトの合計が NoOnOrAfter より早い場合に、NoOnOrAfter を上書きします。 |
| **timeout-in-seconds** | SAML タイムアウト値（秒単位）。デフォルトでは、SAML タイムアウトは設定されていません。アサーションの NotBefore と NotOnOrAfter は、有効性を判別するために使用されます。 |
| **trustpoint [idp \| sp]** ***<trustpoint-name>*** | トラストポイント idp には、SAML アサーションを検証するための ASA の IdP 証明書が含まれます。<br>trustpoint-name は、既存のトラストポイント名のいずれかになります。<br>トラストポイント sp には、ASA の署名を検証するか、または SAML アサーションを暗号化するための IdP の ASA（SP）証明書が含まれます。 |
| **url [sign-in \| sign-out]** ***<value>*** | URL は、IdP のサインインおよびサインアウト URL です。<br>IdP にサインインするための URL の値。url 値には、4 ～ 2000 文字を含める必要があります。 |

## デフォルト

なし。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.5(2) | このコマンドが追加されました。 |
| 9.7(1) | internal 属性が追加されました。 |
| 9.8(1) | SHA2 サポートと署名方式を指定する機能が SAML 要求に追加されました。 |

## 使用上のガイドライン

このコマンドは、1 つ以上のサードパーティの SAML ID プロバイダーの設定値を設定します。IdP 設定は、それらがトンネル グループに適用されるまで使用されません。

SAML IdP のサインイン URL、サインアウト URL、署名証明書は、ベンダーの Web サイトで確認できます。IdP の署名証明書を保持するためのトラストポイントを作成する必要があります。トラストポイント名はトラストポイント idp によって使用されます。

webvpn モードで Idp を作成すると、saml-idp サブモードに切り替わります。このモードで、この Idp の次の設定値を設定できます。

- url sign-in：Idp にサインインするための URL。
- url sign-out：IdP をサインアウトしたときのリダイレクト先 URL。
- signature：SAML 要求内の署名を有効または無効にします。デフォルトでは、署名は無効になっています。
- signature <value>：署名を有効にし、rsa-sha1、rsa-sha256、rsa-sha384、または rsa-sha512 を方式に指定します。デフォルトでは、署名は無効になっています。
- time-out：SAML タイムアウト値（秒単位）。
- base-url：エンドユーザを ASA にリダイレクトするために、URL がサードパーティ IdP に提供されます。base-url を設定しないと、URL は ASA のホスト名とドメイン名から取得されます。たとえば、ホスト名が「ssl-vpn」で、ドメイン名が「cisco.com」の場合、show saml metadata では、https://ssl-vpn.cisco.com がベース URL として表示されます。base-url またはホスト名/ドメイン名のいずれも設定されていない場合、show saml metadata はエラーを返します。
- trustpoint：ASA の署名を検証するか、または SAML アサーションを暗号化するために、ASA（SP）に基づく既存のトラストポイントまたは IdP が使用できる IDP 証明書を割り当てます。

## 例

次に、Idp を定義し、Idp 設定値を設定する方法の例を示します。

```
ciscoasa(config)# same-security-traffic permit inter-interface
ciscoasa(config-webvpn)# saml idp salesforce_idp
ciscoasa(config-webvpn-saml-idp)# url sign-in
https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
ciscoasa(config-webvpn-saml-idp)# url sign-out
https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
ciscoasa(config-webvpn-saml-idp)# trustpoint idp salesforce_trustpoint
ciscoasa(config-webvpn-saml-idp)# trustpoint sp asa_trustpoint
ciscoasa(config-webvpn)# saml idp feide_idp
ciscoasa(config-webvpn-saml-idp)# url sign-in
http://cisco.feide.no/simplesaml/saml2/idp/SSOService.php
ciscoasa(config-webvpn-saml-idp)# trustpoint idp feide_trustpoint
ciscoasa(config-webvpn-saml-idp)# trustpoint sp asa_trustpoint
ciscoasa(config-webvpn-saml-idp)# signature
ciscoasa(config-webvpn-saml-idp)# timeout assertion 120
ciscoasa(config-webvpn-saml-idp)# base-url https://ssl-vpn.cisco.com
```

関連コマンド

| コマンド | 説明 |
|---|---|
| **authentication** | saml などの、トンネル グループの認証タイプを設定します。 |
| **identity-provider** | ASA 内のサードパーティ SAML ID プロバイダーのこの設定に名前を付けます。 |

# saml identity-provider

config-tunnel-webvpn モードでこの CLI を使用して、SAML IdP をトンネル グループ（接続プロファイル）に割り当てます。

**saml identity-provider** *name*

**no saml identity-provider** *name*

## 構文の説明

| | |
|---|---|
| **name** | ASA が使用するように設定している SAML Idp の名前。 |

## デフォルト

なし。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.5(2) | このコマンドが追加されました。 |

## 使用上のガイドライン

これは、ASA 内のサードパーティ SAML ID プロバイダーのこの設定に名前を付けます。

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **authentication** | saml などの、トンネル グループの認証タイプを設定します。 |
| **idp** | サードパーティ SAML ID プロバイダーの Idp を設定します。 |

# sast

CTL レコードに作成する SAST 証明書の数を指定するには、CTL ファイル コンフィギュレーション モードで **sast** コマンドを使用します。CTL ファイル内の SAST 証明書の数をデフォルト値の 2 に戻すには、このコマンドの **no** 形式を使用します。

**sast** *number_sasts*

**no sast** *number_sasts*

## 構文の説明

| | |
|---|---|
| *number_sasts* | 作成する SAST キーの数を指定します。デフォルトは 2 です。許容最大数は、5 です。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.0(4) | コマンドが追加されました。 |

## 使用上のガイドライン

CTL ファイルは、System Administrator Security Token（SAST; システム管理者セキュリティ トークン）によって署名されます。

電話プロキシは CTL ファイルを生成するため、CTL ファイル自体を署名するための SAST キーを作成する必要があります。このキーは、ASA で生成できます。SAST は、自己署名証明書として作成されます。

通常、CTL ファイルには複数の SAST が含まれています。ある SAST が回復可能でない場合は、後でもう 1 つの SAST を使用してファイルを署名できます。

## 例

次に、**sast** コマンドを使用して、CTL ファイルに 5 つの SAST 証明書を作成する例を示します。

```
ciscoasa(config-ctl-file)# sast 5
```

関連コマンド

| コマンド | 説明 |
|---|---|
| **ctl-file（グローバル）** | Phone Proxy コンフィギュレーション用に作成する CTL ファイル、またはフラッシュ メモリから解析するための CTL ファイルを指定します。 |
| **ctl-file（Phone-Proxy）** | Phone Proxy コンフィギュレーションで使用する CTL ファイルを指定します。 |
| **phone-proxy** | Phone Proxy インスタンスを設定します。 |

# scansafe

コンテキストに対してクラウド Web セキュリティ インスペクションをイネーブルにするには、コンテキスト コンフィギュレーション モードで **scansafe** コマンドを使用します。クラウド Web セキュリティをディセーブルにするには、このコマンドの **no** 形式を使用します。

**scansafe** [**license** *key*]

**no scansafe** [**license** *key*]

## 構文の説明

| | |
|---|---|
| **license** *key* | このコンテキストの認証キーを入力します。キーを指定しない場合は、システム コンフィギュレーションで設定されているライセンスがこのコンテキストで使用されます。ASA は、要求がどの組織からのものかを示すために、認証キーを クラウド Web セキュリティ プロキシ サーバに送信します。認証キーは 16 バイトの 16 進数です。 |

## コマンド デフォルト

デフォルトでは、システム コンフィギュレーションに入力されたライセンスがコンテキストで使用されます。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.0(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可する必要があります。

## 例

次に、デフォルトのライセンスを使用してコンテキスト 1 でクラウド Web セキュリティをイネーブルにし、ライセンス キーの上書きを使用してコンテキスト 2 でクラウド Web セキュリティをイネーブルにする設定の例を示します。

```
! System Context
!
scansafe general-options
server primary ip 180.24.0.62 port 8080
```

```
retry-count 5
license 366C1D3F5CE67D33D3E9ACEC265261E5
!
context one
 allocate-interface GigabitEthernet0/0.1
 allocate-interface GigabitEthernet0/1.1
 allocate-interface GigabitEthernet0/3.1
 scansafe
 config-url disk0:/one_ctx.cfg
!
context two
 allocate-interface GigabitEthernet0/0.2
 allocate-interface GigabitEthernet0/1.2
 allocate-interface GigabitEthernet0/3.2
 scansafe license 366C1D3F5CE67D33D3E9ACEC26789534
 config-url disk0:/two_ctx.cfg
!
```

## 関連コマンド

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

# scansafe general-options

クラウド Web セキュリティ プロキシ サーバとの通信を設定するには、グローバル コンフィギュレーション モードで **scansafe general-options** コマンドを使用します。サーバ コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

**scansafe general-options**

**no scansafe general-options**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## コマンド デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.0(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

クラウド Web セキュリティのプライマリ プロキシ サーバとバックアップ プロキシ サーバを設定できます。

## 例

次に、プライマリ サーバを設定する例を示します。

```
scansafe general-options
 server primary ip 180.24.0.62 port 8080
 retry-count 5
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

関連コマンド

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

# scep-enrollment enable

トンネル グループの Simple Certificate Enrollment Protocol をイネーブルまたはディセーブルにするには、トンネル グループ一般属性モードで **scep-enrollment enable** コマンドを使用します。

このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

**scep-enrollment enable**

**no scep-enrollment enable**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルトでは、このコマンドはトンネル グループ コンフィギュレーションに存在しません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.4(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

この機能がサポートされるのは、リリース 3.0 以降の Cisco AnyConnect Secure Mobility Client のみです。

ASA は、AnyConnect とサードパーティ認証局の間の SCEP 要求のプロキシとして動作することができます。認証局がプロキシとして動作する場合に必要なのは、ASA にアクセス可能であることのみです。ASA のこのサービスが機能するには、ASA が登録要求を送信する前に、ユーザが AAA でサポートされているいずれかの方法を使用して認証されている必要があります。また、ホスト スキャンおよびダイナミック アクセス ポリシーを使用して、登録資格のルールを適用することもできます。

ASA では、AnyConnect SSL または IKEv2 VPN セッションでのみこの機能をサポートしています。これは、IOS CS、Windows Server 2003 CA、および Windows Server 2008 CA を含む、すべての SCEP 準拠認証局をサポートしています。

クライアントレス（ブラウザベース）でのアクセスは SCEP プロキシをサポートしていませんが、WebLaunch（クライアントレス起動 AnyConnect）はサポートしていません。

ASA では、証明書のポーリングはサポートしていません。

ASA はこの機能に対するロード バランシングをサポートしています。

## 例

次に、グローバル コンフィギュレーション モードで、remotegrp というリモート アクセス トンネル グループを作成し、グループ ポリシー用の SCEP をイネーブルにする例を示します。

```
ciscoasa(config)# tunnel-group remotegrp type remote-access
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# scep-enrollment enable
INFO: 'authentication aaa certificate' must be configured to complete setup of this
option.
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **crypto ikev2 enable** | IPsec ピアが通信するインターフェイスで IKEv2 ネゴシエーションをイネーブルにします。 |
| **scep-forwarding-url** | グループ ポリシー用の SCEP 認証局を登録します。 |
| **secondary-pre-fill-username clientless** | 証明書が SCEP プロキシの WebLaunch のサポートに使用できない場合は、共通のセカンダリ パスワードを使用します。 |
| **secondary-authentication-server-group** | 証明書が使用できないときにはユーザ名を指定します。 |

# scep-forwarding-url

グループ ポリシー用の SCEP 認証局を登録するには、グループ ポリシー コンフィギュレーション モードで **scep-forwarding-url** コマンドを使用します。

このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

**scep-forwarding-url** {**none** | **value** [*URL*]}

**no scep-forwarding-url**

## 構文の説明

| | |
|---|---|
| **none** | グループ ポリシーの認証局を指定しません。 |
| *URL* | 認証局の SCEP URL を指定します。 |
| **value** | この機能をクライアントレス接続でイネーブルにします。 |

## デフォルト

デフォルトでは、このコマンドは存在しません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.4(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

このコマンドは、サードパーティのデジタル証明書をサポートするグループ ポリシーごとに 1 回入力します。

## Example

次に、グローバル コンフィギュレーション モードで、FirstGroup という名前のグループ ポリシーを作成し、グループ ポリシーの認証局を登録する例を示します。

```
ciscoasa(config)# group-policy FirstGroup internal
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# scep-forwarding-url value http://ca.example.com:80/
Attempting to retrieve the CA/RA certificate(s) using the URL. Please wait ...
```

関連コマンド

| コマンド | 説明 |
|---|---|
| **crypto ikev2 enable** | IPsec ピアが通信するインターフェイスで IKEv2 ネゴシエーションをイネーブルにします。 |
| **scep-enrollment enable** | トンネル グループに対して Simple Certificate Enrollment Protocol をイネーブルにします。 |
| **secondary-pre-fill-username clientless** | 証明書が SCEP プロキシの WebLaunch のサポートに使用できない場合は、共通のセカンダリ パスワードを使用します。 |
| **secondary-authentication-server-group** | 証明書が使用できないときにはユーザ名を指定します。 |

# secondary

**preempt** コマンドの使用時にフェールオーバー グループの優先ユニットを設定するには、フェールオーバー グループ コンフィギュレーション モードで **secondary** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

**secondary**

**no secondary**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

フェールオーバー グループに **primary** または **secondary** が指定されていない場合は、フェールオーバー グループはデフォルトで **primary** に設定されます。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが追加されました。 |
| 9.0(1) | 早期のソフトウェア バージョンでは、フェールオーバー グループが優先ユニットでアクティブになるために **preempt** コマンドを必要としないように、「同時」ブートアップが許可されていました。ただし、この機能は、現在、両方のフェールオーバー グループがブートアップした最初のユニットでアクティブになるように変更されています。 |

## 使用上のガイドライン

**primary** または **secondary** 優先順位をフェールオーバー グループに割り当てると、**preempt** コマンドが設定されているときに、フェールオーバー グループがどのユニット上でアクティブになるかが指定されます。グループの **primary** または **secondary** の設定にかかわらず、両方のフェールオーバー グループがブートアップした最初のユニットでアクティブになります(それらが同時に起動したように見える場合でも、一方のユニットが最初にアクティブになります)。もう一方のユニットがオンラインになったとき、2 番めのユニットをプライオリティの高いユニットとして所有するフェールオーバー グループは、そのフェールオーバー グループが **preempt** コマンドで設定されているか、**no failover active** コマンドを使用して手動でもう一方のユニットに強制されない限り、2 番めのユニットではアクティブになりません。フェールオーバー グループが **preempt** コマンドで設定される場合、指定されたユニットでフェールオーバー グループが自動的にアクティブになります。

## 例

次の例では、プライマリ装置のフェールオーバー グループ 1 をより高いプライオリティに設定し、セカンダリ装置のフェールオーバー グループ 2 をより高いプライオリティに設定します。どのフェールオーバー グループも **preempt** コマンドを使用して設定されているため、これらのグループは、優先するユニットが使用可能になったときにそのユニット上で自動的にアクティブになります。

```
ciscoasa(config)# failover group 1
ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# exit
ciscoasa(config)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012
ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **failover group** | Active/Active フェールオーバーのためのフェールオーバー グループを定義します。 |
| **preempt** | 優先するユニットが使用可能になったときに、フェールオーバー グループをそのユニット上で強制的にアクティブにします。 |
| **primary** | プライマリ ユニットに、セカンダリ ユニットよりも高いプライオリティを付与します。 |

# secondary-authentication-server-group

二重認証がイネーブルの場合にセッションに関連付けるセカンダリ認証サーバ グループを指定するには、トンネル グループ一般属性モードで **secondary-authentication-server-group** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

**secondary-authentication-server-group** [*interface_name*] {**none** | **LOCAL** | *groupname* [**LOCAL**]} [**use-primary-username**]}

**no secondary-authentication-server-group**

## 構文の説明

| | |
|---|---|
| *interface_name* | (オプション)IPsec トンネルが終端するインターフェイスを指定します。 |
| **LOCAL** | (任意)通信障害によりサーバ グループにあるすべてのサーバが非アクティブになった場合に、ローカル ユーザ データベースに対する認証を要求します。サーバ グループ名が **LOCAL** または **NONE** の場合、ここでは **LOCAL** キーワードを使用しないでください。 |
| **none** | (任意)サーバ グループ名を **NONE** と指定して、認証が不要であることを示します。 |
| *groupname* [**LOCAL**] | 事前に設定済みの認証サーバまたはサーバ グループを指定します。LOCAL グループを指定することもできます。 |
| **use-primary-username** | プライマリ ユーザ名をセカンダリ認証のユーザ名として使用します。 |

## デフォルト

デフォルト値は **none** です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.2(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

このコマンドは、二重認証がイネーブルになっている場合に限り有効です。**secondary-authentication-server-group** コマンドは、セカンダリ AAA サーバ グループを指定します。SDI サーバ グループはセカンダリ サーバ グループにできません。

use-primary-username キーワードが設定されている場合は、ログイン ダイアログボックスで 1 つのユーザ名のみが要求されます。

ユーザ名がデジタル証明書から抽出される場合は、プライマリ ユーザ名だけが認証に使用されます。

## 例

次に、グローバル コンフィギュレーション モードで、remotegrp という名前のリモート アクセス トンネル グループを作成して、接続のプライマリ サーバ グループとしてグループ sdi_server の使用を指定し、セカンダリ認証サーバ グループとしてグループ ldap_server を指定する例を示します。

```
ciscoasa(config)# tunnel-group remotegrp type remote-access
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-webvpn)# authentication-server-group sdi_server
ciscoasa(config-tunnel-webvpn)# secondary-authentication-server-group ldap_server
ciscoasa(config-tunnel-webvpn)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **pre-fill-username** | 事前入力ユーザ名機能をイネーブルにします。 |
| **show running-config tunnel-group** | 指定されたトンネル グループ コンフィギュレーションを表示します。 |
| **tunnel-group general-attributes** | 名前付きのトンネル グループの一般属性を指定します。 |
| **username-from-certificate** | 認可時のユーザ名として使用する証明書内のフィールドを指定します。 |

# secondary-color

WebVPN ログイン、ホームページ、およびファイル アクセス ページのセカンダリ カラーを設定するには、webvpn コンフィギュレーション モードで **secondary-color** コマンドを使用します。色をコンフィギュレーションから削除して、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。

**secondary-color** [*color*]

**no secondary-color**

## 構文の説明

| | |
|---|---|
| *color* | (任意)色を指定します。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。<br>• RGB 形式は 0,0,0 で、各色(赤、緑、青)を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。<br>• HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。<br>• 名前の最大長は 32 文字です。 |

## デフォルト

デフォルトのセカンダリ カラーは HTML の #CCCCFF(薄紫色)です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 使用上のガイドライン

RGB 値を使用する場合、推奨値は 216 です。推奨色は、数学的にあり得る数よりはるかに少なくなります。多くのディスプレイは 256 色しか処理できず、そのうちの 40 色は MAC と PC とでは異なった表示になります。最適な結果を得るために、公開されている RGB テーブルをチェックしてください。RGB テーブルをオンラインで検索するには、検索エンジンで RGB と入力します。

## 例

次に、HTML の色値 #5F9EAO（灰青色）を設定する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# secondary-color #5F9EAO
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **title-color** | ログイン ページ、ホームページ、およびファイル アクセス ページの WebVPN タイトル バーの色を設定します。 |

# secondary-pre-fill-username

クライアントレスまたは AnyConnect 接続の二重認証で使用するクライアント証明書からユーザ名を抽出できるようにするには、トンネル グループ webvpn 属性モードで **secondary-pre-fill-username** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

**secondary-pre-fill-username** {**clientless** | **ssl-client**} [**hide**]

**secondary-pre-fill-username** {**clientless** | **ssl-client**} **hide** [**use-primary-password** | **use-common-password** [*type_num*] *password*]

**no secondary-no pre-fill-username**

## 構文の説明

| | |
|---|---|
| **clientless** | この機能をクライアントレス接続でイネーブルにします。 |
| **hide** | 認証に使用するユーザ名を VPN ユーザに非表示にします。 |
| **password** | パスワード ストリングを入力します。 |
| **ssl-client** | この機能を AnyConnect VPN クライアント接続でイネーブルにします。 |
| **type_num** | 次のいずれかのオプションを入力します。<br>• 入力するパスワードがプレーン テキストの場合は 0。<br>• 入力するパスワードが暗号化されている場合は 8。パスワードは、入力時にアスタリスクで表示されます。 |
| **use-common-password** | ユーザにプロンプトを表示せずに、使用する共通の 2 次認証パスワードを指定します。 |
| **use-primary-password** | ユーザにプロンプトを表示せずに、2 次認証に 1 次認証パスワードを再使用します。 |

## デフォルト

この機能はデフォルトで無効に設定されています。**hide** キーワードを指定せずにこのコマンドを入力すると、抽出したユーザ名が VPN ユーザに表示されます。**use-primary-password** と **use-common-password** のいずれのキーワードも指定しないと、ユーザにはパスワード プロンプトが表示されます。*type_num* のデフォルト値は 8 です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.2(1) | このコマンドが追加されました。 |
| 8.3(2) | [**use-primary-password** \| **use-common-password** [*type_num*] *password*] オプションが追加されました。 |

## 使用上のガイドライン

この機能をイネーブルにするには、トンネル グループ一般属性モードで **secondary-username-from-certificate** コマンドを入力する必要もあります。

このコマンドは、二重認証がイネーブルになっている場合に限り有効です。**secondary-pre-fill-username** コマンドは、**secondary-username-from-certificate** コマンドで指定された証明書フィールドから抽出されたユーザ名を、セカンダリ ユーザ名またはパスワード認証のユーザ名として使用できるようにします。2 回めの認証で証明書からのユーザ名の事前充填機能を使用するには、両方のコマンドを設定する必要があります。

(注) クライアントレス接続と SSL クライアント接続は、相互排他的なオプションではありません。1 つのコマンドラインで指定できるのはいずれか 1 つのみですが、同時に両方をイネーブルにできます。

2 番めの名を非表示にして、プライマリまたは共通のパスワードを使用する場合は、ユーザ体験は単一認証と似ています。プライマリまたは共通のパスワードを使用すると、デバイス証明書を使用したデバイスの認証がシームレスなユーザ体験になります。

**use-primary-password** キーワードは、すべての認証のセカンダリ パスワードとしてプライマリ パスワードを使用することを指定します。

**use-common-password** キーワードは、すべての 2 次認証に共通のセカンダリ パスワードを使用することを指定します。エンドポイントにインストールされているデバイス証明書に BIOS ID またはその他の ID が含まれている場合は、2 次認証要求では、事前に入力された BIOS ID をセカンダリ ユーザ名として使用して、そのトンネル グループでのすべての認証に対して設定された共通のパスワードを使用できます。

## 例

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 グループを作成して、接続がブラウザベースである場合に、エンドポイントのデジタル証明書の名前を、認証または認可クエリーに使用する名前として再使用することを指定します。

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp webvpn-attributes
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username clientless
```

次の例では、前のコマンドと同じ機能を実行しますが、抽出されたユーザ名をユーザに非表示にします。

```
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username clientless hide
```

次の例では、AnyConnect 接続だけに適用される点を除いて、前のコマンドと同じ機能を実行します。

```
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username ssl-client hide
```

次の例では、ユーザ名を非表示にして、ユーザにプロンプトを表示せずに、2 次認証に 1 次認証パスワードを再使用します。

```
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username ssl-client hide
use-primary-password
```

次の例では、ユーザ名を非表示にして、入力するパスワードを 2 次認証に使用します。

```
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username ssl-client hide
use-common-password **********
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **pre-fill-username** | 事前入力ユーザ名機能をイネーブルにします。 |
| **show running-config tunnel-group** | 指定されたトンネル グループ コンフィギュレーションを表示します。 |
| **tunnel-group general-attributes** | 名前付きのトンネル グループの一般属性を指定します。 |
| **username-from-certificate** | 認可時のユーザ名として使用する証明書内のフィールドを指定します。 |

# secondary-text-color

WebVPN ログイン、ホームページ、およびファイル アクセス ページのセカンダリ テキストの色を設定するには、webvpn モードで **secondary-text-color** コマンドを使用します。色をコンフィギュレーションから削除して、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。

**secondary-text-color** [*black* | *white*]

**no secondary-text-color**

## 構文の説明

| | |
|---|---|
| auto | text-color コマンドの設定に基づいて、黒または白が選択されます。つまり、プライマリ カラーが黒の場合、この値は白になります。 |
| black | デフォルトのセカンダリ テキストの色は黒です。 |
| white | テキストの色を白に変更できます。 |

## デフォルト

デフォルトのセカンダリ テキストの色は黒です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 例

次に、セカンダリ テキストの色を白に設定する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# secondary-text-color white
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **text-color** | ログイン ページ、ホームページ、およびファイル アクセス ページの WebVPN タイトル バーのテキストの色を設定します。 |

# secondary-username-from-certificate

クライアントレス接続または AnyConnect（SSL クライアント）接続において、二重認証の 2 つめのユーザ名として使用する証明書のフィールドを指定するには、トンネル グループ一般属性モードで **secondary-username-from-certificate** コマンドを使用します。

属性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。

**secondary-username-from-certificate** {*primary-attr* [*secondary-attr*] | **use-entire-name** | **use-script**}

**no secondary-username-from-certificate**

## 構文の説明

| | |
|---|---|
| *primary-attr* | 証明書から認可クエリーのユーザ名を取得するために使用する属性を指定します。pre-fill-username がイネーブルになっている場合、取得された名前は認証クエリーでも使用できます。 |
| *secondary-attr* | （任意）デジタル証明書から認証または認可クエリーのユーザ名を取得するためにプライマリ属性とともに使用する追加の属性を指定します。pre-fill-username がイネーブルになっている場合、取得された名前は認証クエリーでも使用できます。 |
| **use-entire-name** | ASA では、完全なサブジェクト DN（RFC1779）を使用して、デジタル証明書から認可クエリーの名前を取得する必要があることを指定します。 |
| **use-script** | ASDM によって生成されたスクリプト ファイルを使用して、ユーザ名として使用する DN フィールドを証明書から抽出することを指定します。 |

## デフォルト

この機能はデフォルトでディセーブルであり、二重認証がイネーブルの場合にのみ有効です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.2(1) | このコマンドが追加されました。 |

**使用上のガイドライン**

このコマンドは、二重認証がイネーブルになっている場合に限り有効です。

二重認証が有効になっている場合、このコマンドはユーザ名として使用する 1 つ以上のフィールドを証明書から選択します。**secondary-username-from-certificate** コマンドは、セキュリティアプライアンスに、指定した証明書フィールドを 2 回めのユーザ名/パスワード認証のための 2 つめのユーザ名として使用するように強制します。

2 回めのユーザ名/パスワード認証または認可のために、証明書からのユーザ名の事前充填機能で、取得されたユーザ名を使用するには、トンネル グループ webvpn 属性モードで **pre-fill-username** コマンドおよび **secondary-pre-fill-username** コマンドも設定する必要があります。つまり、2 回めのユーザ名の事前充填機能を使用するには、両方のコマンドを設定する必要があります。

プライマリ属性およびセカンダリ属性の有効値は、次のとおりです。

| 属性 | 定義 |
|---|---|
| C | Country（国名）：2 文字の国名略語。国名コードは、ISO 3166 国名略語に準拠しています。 |
| CN | Common Name（一般名）：人、システム、その他のエンティティの名前。セカンダリ属性としては使用できません。 |
| DNQ | ドメイン名修飾子。 |
| EA | 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）：組織が置かれている市または町。 |
| N | 名前 |
| O | Organization（組織）：会社、団体、機関、連合、その他のエンティティの名前。 |
| OU | Organizational Unit（組織ユニット）：組織（O）内のサブグループ。 |
| SER | Serial Number（シリアル番号）。 |
| SN | Surname（姓）。 |
| 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。 |
| T | Title（タイトル）。 |
| UID | User Identifier（ユーザ ID）。 |
| UPN | User Principal Name（ユーザ プリンシパル名）。 |
| use-entire-name | DN 名全体を使用します。セカンダリ属性としては使用できません。 |
| use-script | ASDM によって生成されたスクリプト ファイルを使用します。 |

**（注）** **secondary-authentication-server-group** コマンドを **secondary-username-from-certificate** コマンドとともに指定した場合は、プライマリ ユーザ名のみが認証に使用されます。

## 例

次に、グローバル コンフィギュレーション モードで、remotegrp という名前のリモート アクセス トンネル グループを作成し、プライマリ属性として CN（一般名）、セカンダリ属性として OU を使用して、デジタル証明書から認可クエリーの名前を取得するように指定する例を示します。

```
ciscoasa(config)# tunnel-group remotegrp type remote-access
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# username-from-certificate CN
ciscoasa(config-tunnel-general)# secondary-username-from-certificate OU
ciscoasa(config-tunnel-general)#
```

次に、トンネル グループ属性を変更し、事前入力ユーザ名を設定する例を示します。

```
username-from-certificate {use-entire-name | use-script | <primary-attr>} [secondary-attr]
secondary-username-from-certificate {use-entire-name | use-script | <primary-attr>}
[secondary-attr] ; used only for double-authentication
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **pre-fill-username** | 事前入力ユーザ名機能をイネーブルにします。 |
| **secondary-pre-fill-username** | クライアントレス接続または AnyConnect クライアント接続において、ユーザ名抽出をイネーブルにします。 |
| **username-from-certificate** | 認可時のユーザ名として使用する証明書内のフィールドを指定します。 |
| **show running-config tunnel-group** | 指定されたトンネル グループ コンフィギュレーションを表示します。 |
| **secondary-authentication-server-group** | セカンダリ AAA サーバ グループを指定します。ユーザ名がデジタル証明書から抽出される場合は、プライマリ ユーザ名だけが認証に使用されます。 |

# secondary-username-from-certificate-choice

セカンダリ認証または許可用として事前入力ユーザ名フィールドにユーザ名を使用する必要がある証明書を選択するには、**secondary-username-from-certificate-choice** コマンドを使用します。このコマンドは tunnel-group general-attributes モードで使用します。デフォルトの証明書で使用されているユーザ名を使用するには、このコマンドの **no** 形式を使用します。

**secondary-username-from-certificate-choice** {**first-certificate** | **second-certificate**}

**no secondary-username-from-certificate-choice** {**first-certificate** | **second-certificate**}

## 構文の説明

| | |
|---|---|
| **first-certificate** | マシン証明書のユーザ名を、セカンダリ認証の事前入力ユーザ名フィールドで使用するように SSL または IKE で送信するかどうかを指定します。 |
| **second-certificate** | ユーザ証明書のユーザ名を、セカンダリ認証の事前入力ユーザ名フィールドで使用するようにクライアントから送信するかどうかを指定します。 |

## デフォルト

デフォルトでは、事前入力するユーザ名は 2 つ目の証明書から取得されます。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.14(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

複数証明書オプションを使用すると、証明書を通じたマシンとユーザ両方の証明書認証が可能になります。事前入力ユーザ名フィールドでは、証明書のフィールドを解析し、AAA および証明書認証済み接続で以降の（プライマリまたはセカンダリ）AAA 認証に使用することができます。事前入力のユーザ名は、常にクライアントから受信した 2 つ目の（ユーザ）証明書から取得されます。

9.14(1) 以降、ASA では、最初の証明書（マシン証明書）または 2 つ目の証明書（ユーザ証明書）のどちらを使用して事前入力ユーザ名フィールドに使用するユーザ名を取得するかを選択できます。

このコマンドは、認証タイプ（AAA、証明書、または複数証明書）に関係なく、任意のトンネルグループに使用および設定できます。ただし、設定は、複数証明書認証（複数証明書または AAA 複数証明書）に対してのみ有効となります。このオプションが複数証明書認証に使用されない場合は、2 つ目の証明書がデフォルトとして認証または許可の目的で使用されます。

## 例

次に、プライマリおよびセカンダリ認証または許可の事前入力ユーザ名に使用する証明書を設定する方法の例を示します。

```
ciscoasa(config)#tunnel-group tg1 type remote-access
ciscoasa(config)#tunnel-group tg1 general-attributes
ciscoasa(config-tunnel-general)# address-pool IPv4
ciscoasa(config-tunnel-general)# secondary-authentication-server-group LOCAL/<Auth-Server>
ciscoasa(config-tunnel-general)# username-from-certificate-choice first-certificate
ciscoasa(config-tunnel-general)# secondary-username-from-certificate-choice
first-certificate

ciscoasa(config)# tunnel-group tg1 webvpn-attributes
ciscoasa(config-tunnel-webvpn)# authentication aaa multiple-certificate
ciscoasa(config-tunnel-webvpn)# pre-fill-username client
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username client
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **username-from-certificate-choice** | プライマリ認証の証明書オプションを指定します。 |

# secure-unit-authentication

セキュア ユニット認証をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **secure-unit-authentication enable** コマンドを使用します。セキュア ユニット認証をディセーブルにするには、**secure-unit-authentication disable** コマンドを使用します。実行コンフィギュレーションからセキュア ユニット認証属性を削除するには、このコマンドの **no** 形式を使用します。**secure-unit-authentication** {**enable** | **disable**}

**no secure-unit-authentication**

## 構文の説明

| | |
|---|---|
| **disable** | セキュア ユニット認証をディセーブルにします。 |
| **enable** | セキュア ユニット認証をイネーブルにします。 |

## デフォルト

セキュア ユニット認証はディセーブルです。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 使用上のガイドライン

セキュア ユニット認証では、ハードウェア クライアントが使用するトンネル グループに認証サーバ グループが設定されている必要があります。

プライマリASA でセキュア ユニット認証が必要な場合は、すべてのバックアップ サーバに対してもセキュア ユニット認証を設定する必要があります。

**no** オプションを指定すると、他のグループ ポリシーからセキュア ユニット認証の値を継承できます。

セキュア ユニット認証では、VPN ハードウェア クライアントがトンネルを開始するたびにクライアントに対してユーザ名/パスワード認証を要求することによって、セキュリティが強化されます。この機能をイネーブルにすると、ハードウェア クライアントではユーザ名とパスワードが保存されません。

**（注）** この機能をイネーブルにした場合に VPN トンネルを確立するには、ユーザがユーザ名とパスワードを入力する必要があります。

## 例

次に、FirstGroup という名前のグループ ポリシーに対して、セキュア ユニット認証をイネーブルにする例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# secure-unit-authentication enable
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **ip-phone-bypass** | ユーザ認証を行わずに IP 電話に接続できるようにします。セキュア ユニット認証は有効なままです。 |
| **leap-bypass** | イネーブルの場合、VPN ハードウェア クライアントの背後にある無線デバイスからの LEAP パケットがユーザ認証の前に VPN トンネルを通過できます。これにより、シスコ ワイヤレス アクセス ポイント デバイスを使用するワークステーションで LEAP 認証を確立できるようになります。その後、ユーザ認証ごとに再度認証を行います。 |
| **user-authentication** | ハードウェア クライアントの背後にいるユーザに対して、接続前に ASA に識別情報を示すように要求します。 |

# security-group

Cisco TrustSec で使用できるようにセキュリティ グループをセキュリティ オブジェクト グループに追加するには、オブジェクトグループ セキュリティ コンフィギュレーション モードで **security-group** コマンドを使用します。セキュリティ グループを削除するには、このコマンドの **no** 形式を使用します。

**security-group** {**tag** *sgt#* | **name** *sg_name*}

**no security-group** {**tag** *sgt#* | **name** *sg_name*}

## 構文の説明

| | |
|---|---|
| **tag** *sgt#* | セキュリティ グループ オブジェクトをインライン タグとして指定します。セキュリティ タイプがタグの場合は、1 ～ 65533 の数字を入力します。<br><br>SGT は、ISE による IEEE 802.1X 認証、Web 認証、または MAC 認証バイパス（MAB）を通してデバイスに割り当てられます。セキュリティ グループの名前は ISE 上で作成され、セキュリティ グループをわかりやすい名前で識別できるようになります。セキュリティ グループ テーブルによって、SGT がセキュリティ グループ名にマッピングされます。 |
| **name** *sg_name* | セキュリティ グループ オブジェクトを名前付きオブジェクトとして指定します。セキュリティ タイプが名前の場合は、32 バイトの文字列を、大文字と小文字を区別して入力します。*sg_name* には、[a-z]、[A-Z]、[0-9]、[!@#$%^&()-_{}. ] を含めることができます。 |

## コマンド デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.0(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

作成したセキュリティ グループ オブジェクト グループは、Cisco TrustSec をサポートする機能で使用できます。そのグループを拡張 ACL に入れると、たとえばアクセス ルールで使用できるようになります。

Cisco TrustSec と統合されているときは、ASA は ISE からセキュリティ グループの情報をダウンロードします。ISE はアイデンティティ リポジトリとしても動作し、Cisco TrustSec タグからユーザ アイデンティティへのマッピングと、Cisco TrustSec タグからサーバ リソースへのマッピングを行います。セキュリティ グループ アクセス リストのプロビジョニングおよび管理は、中央集中型で ISE 上で行います。

ただし、ASA には、グローバルには定義されていない、ローカライズされたネットワーク リソースが存在することがあり、そのようなリソースにはローカル セキュリティ グループとローカライズされたセキュリティ ポリシーが必要です。ローカル セキュリティ グループには、ISE からダウンロードされた、ネストされたセキュリティ グループを含めることができます。ASA は、ローカルと中央のセキュリティ グループを統合します。

ASA 上でローカル セキュリティ グループを作成するには、ローカル セキュリティ オブジェクト グループを作成します。1 つのローカル セキュリティ オブジェクト グループに、1 つ以上のネストされたセキュリティ オブジェクト グループまたはセキュリティ ID またはセキュリティ グループ名を入れることができます。ユーザは、ASA 上に存在しない新しいセキュリティ ID またはセキュリティ グループ名を作成することもできます。

ASA 上で作成したセキュリティ オブジェクト グループは、ネットワーク リソースへのアクセスの制御に使用できます。セキュリティ オブジェクト グループを、アクセス グループやサービス ポリシーの一部として使用できます。

## 例

次に、セキュリティ グループ オブジェクトを設定する例を示します。

```
ciscoasa(config)# object-group security mktg-sg
ciscoasa(config)# security-group name mktg
ciscoasa(config)# security-group tag 1
```

次に、セキュリティ グループ オブジェクトを設定する例を示します。

```
ciscoasa(config)# object-group security mktg-sg-all
ciscoasa(config)# security-group name mktg-managers
ciscoasa(config)# group-object mktg-sg // nested object-group
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **object-group security** | セキュリティ グループ オブジェクトを作成します。 |

# security-group-tag

リモート アクセス VPN グループ ポリシーまたは LOCAL ユーザ データベース内のユーザのセキュリティ グループ タグを設定するには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **security-group-tag value** コマンドを使用します。セキュリティ グループ タグ属性を削除するには、このコマンドの **no** 形式を使用します。

**security-group-tag** {**none** | **value** *sgt*}

**no security-group-tag** {**none** | **value** *sgt*}

## 構文の説明

| | |
|---|---|
| **none** | このグループ ポリシーまたはユーザのセキュリティ グループ タグを設定しません。 |
| **value** *sgt* | セキュリティ グループ タグ番号を指定します。 |

## コマンド デフォルト

デフォルトは **security-group-tag none** です。つまり、この属性に設定されているセキュリティ グループ タグはありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.3(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

ASA は、VPN セッションのセキュリティ グループ タギングをサポートしています。外部 AAA サーバを使用するか、または、ローカル ユーザか VPN グループ ポリシーのセキュリティ グループ タグを設定することで、セキュリティ グループ タグ（SGT）を VPN セッションに割り当てることができます。さらに、レイヤ 2 イーサネット経由で、Cisco TrustSec システムを介してこのタグを伝搬することができます。AAA サーバが SGT を提供できない場合には、セキュリティ グループ タグをグループ ポリシーで利用したり、ローカル ユーザが利用したりすることができます。

次は、VPN ユーザに SGT を割り当てるための一般的なプロセスです。

1. ユーザは、ISE サーバを含む AAA サーバ グループを使用しているリモート アクセス VPN に接続します。
2. ASA が ISE に AAA 情報を要求します。この情報に SGT が含まれている場合があります。ASA は、ユーザのトンネル トラフィックに対する IP アドレスの割り当ても行います。
3. ASA が AAA 情報を使用してユーザを認証し、トンネルを作成します。
4. ASA が AAA 情報から取得した SGT と割り当て済みの IP アドレスを使用して、レイヤ 2 ヘッダー内に SGT を追加します。
5. SGT を含むパケットが Cisco TrustSec ネットワーク内の次のピア デバイスに渡されます。

AAA サーバの属性に、VPN ユーザに割り当てるための SGT が含まれていない場合、ASA はグループ ポリシーの SGT を使用します。グループ ポリシーに SGT が含まれていない場合は、タグ 0x0 が割り当てられます。

## 例

次に、グループ ポリシーの SGT 属性を設定する方法の例を示します。

```
ciscoasa(config-group-policy)# security-group-tag value 101
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show asp table cts sgt-map** | データ パスに保持されている IP アドレス セキュリティ グループのテーブル マップ データベースから IP アドレス セキュリティ グループのテーブル マップ エントリを表示します。 |
| **show cts sgt-map** | 制御パスの IP アドレス セキュリティ グループ テーブル マネージャ エントリを表示します。 |

# security-level

インターフェイスのセキュリティ レベルを設定するには、インターフェイス コンフィギュレーション モードで **security-level** コマンドを使用します。セキュリティ レベルをデフォルトに設定するには、このコマンドの **no** 形式を使用します。セキュリティ レベルを指定すると、高いセキュリティ レベルのネットワークと低いセキュリティ レベルのネットワークとの間の通信に追加の保護が設定され、高いセキュリティ レベルのネットワークが低いセキュリティ レベルのネットワークから保護されます。

**security-level** *number*

**no security-level**

## 構文の説明

| | |
|---|---|
| *number* | 0（最低）～ 100（最高）の整数。 |

## デフォルト

デフォルトのセキュリティ レベルは 0 です。

インターフェイスに「inside」という名前を指定して、明示的にセキュリティ レベルを設定しないと、ASA によってセキュリティ レベルが 100 に設定されます（**nameif** コマンドを参照）。このレベルは必要に応じて変更できます。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが、**nameif** コマンドのキーワードからインターフェイス コンフィギュレーション モードのコマンドに変更されました。 |

## 使用上のガイドライン

レベルによって、次の動作が制御されます。

- ネットワーク アクセス：デフォルトで、高いセキュリティ レベルのインターフェイスから低いセキュリティ レベルのインターフェイスへの通信（発信）は暗黙的に許可されます。高いセキュリティ レベルのインターフェイス上のホストは、低いセキュリティ レベルのインターフェイス上の任意のホストにアクセスできます。インターフェイスにアクセス リストを適用することによって、アクセスを制限できます。

  同じセキュリティ レベルのインターフェイス間では、同じセキュリティ レベル以下の他のインターフェイスへのアクセスが暗黙的に許可されます。

- インスペクション エンジン:一部のインスペクション エンジンは、セキュリティ レベルに依存します。同じセキュリティ レベルのインターフェイス間では、インスペクション エンジンは発信と着信のいずれのトラフィックに対しても適用されます。
  - NetBIOS インスペクション エンジン:発信接続に対してのみ適用されます。
  - OraServ インスペクション エンジン:ホストのペア間に OraServ ポートへの制御接続が存在する場合は、ASA 経由での着信データ接続のみが許可されます。
- フィルタリング:HTTP(S) および FTP フィルタリングは、(高いレベルから低いレベルへの)発信接続にのみ適用されます。

  同じセキュリティ レベルのインターフェイス間では、発信と着信のいずれのトラフィックもフィルタリングできます。
- NAT コントロール:NAT コントロールをイネーブルにする場合、高いセキュリティ レベルのインターフェイス(内部)上のホストから低いセキュリティ レベルのインターフェイス(外部)上のホストにアクセスするときは、内部インターフェイスのホストに NAT を設定する必要があります。

  NAT コントロールをイネーブルにしない場合、または同じセキュリティ レベルのインターフェイス間においては、任意のインターフェイス間で NAT を使用することも、使用しないこともできます。外部インターフェイスに NAT を設定する場合は、特別なキーワードが必要になることがあります。
- **established** コマンド:このコマンドを使用すると、高いレベルのホストから低いレベルのホストへの接続がすでに確立されている場合、低いセキュリティ レベルのホストから高いセキュリティ レベルのホストへの戻り接続が許可されます。

  同じセキュリティ レベルのインターフェイス間では、発信と着信の両方の接続に対して **established** コマンドを設定できます。

通常、同じセキュリティ レベルのインターフェイス間では通信できません。同じセキュリティ レベルのインターフェイス間で通信する場合は、**same-security-traffic** コマンドを参照してください。101 を超える通信インターフェイスを作成する必要がある場合や、2 つのインターフェイス間のトラフィックに同じ保護機能を適用する必要がある場合(同程度のセキュリティが必要な 2 つの部門がある場合など)に、2 つのインターフェイスに同じレベルを割り当てて、それらのインターフェイス間での通信を許可できます。

インターフェイスのセキュリティ レベルを変更する場合、既存の接続がタイムアウトするのを待たずに新しいセキュリティ情報を使用するときは、**clear local-host** コマンドを使用して接続をクリアできます。

## 例

次に、2 つのインターフェイスのセキュリティ レベルを 100 と 0 に設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet0/0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

関連コマンド

| コマンド | 説明 |
|---|---|
| **clear local-host** | すべての接続をリセットします。 |
| **interface** | インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。 |
| **nameif** | インターフェイス名を設定します。 |
| **vlan** | サブインターフェイスに VLAN ID を割り当てます。 |

# segment-id

VNI インターフェイスの VXLAN 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 **segment-id** コマンドを使用します。ID を削除するには、このコマンドの **no** 形式を使用します。

**segment-id** *id*

**no segment-id** *id*

## 構文の説明

| | |
|---|---|
| *id* | 1 ～ 16777215 の範囲で ID を設定します。 |

## コマンド デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.4(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

セグメント ID は VXLAN タギングに使用されます。

## 例

次に、VNI 1 インターフェイスを設定し、1000 のセグメント ID を指定する例を示します。

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# mcast-group 236.0.0.100
```

関連コマンド

| コマンド | 説明 |
|---|---|
| **debug vxlan** | VXLAN トラフィックをデバッグします。 |
| **default-mcast-group** | VTEP 送信元インターフェイスに関連付けられているすべての VNI インターフェイスのデフォルトのマルチキャスト グループを指定します。 |
| **encapsulation vxlan** | NVE インスタンスを VXLAN カプセル化に設定します。 |
| **inspect vxlan** | 標準 VXLAN ヘッダー形式に強制的に準拠させます。 |
| **interface vni** | VXLAN タギング用の VNI インターフェイスを作成します。 |
| **mcast-group** | VNI インターフェイスのマルチキャスト グループ アドレスを設定します。 |
| **nve** | ネットワーク仮想化エンドポイント インスタンスを指定します。 |
| **nve-only** | VXLAN 送信元インターフェイスが NVE 専用であることを指定します。 |
| **peer ip** | ピア VTEP の IP アドレスを手動で指定します。 |
| **show arp vtep-mapping** | リモート セグメント ドメインにある IP アドレスとリモート VTEP IP アドレス用の VNI インターフェイスにキャッシュされた MAC アドレスを表示します。 |
| **show interface vni** | VNI インターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス(設定されている場合)のステータス、ならびに関連付けられている NVE インターフェイスを表示します。 |
| **show mac-address-table vtep-mapping** | リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ 2 転送テーブル(MAC アドレス テーブル)を表示します。 |
| **show nve** | NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリア インターフェイス(送信元インターフェイス)のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。 |
| **show vni vlan-mapping** | VNI セグメント ID と、VLAN インターフェイスまたはトランスペアレント モードの物理インターフェイス間のマッピングを表示します。 |
| **source-interface** | VTEP 送信元インターフェイスを指定します。 |
| **vtep-nve** | VNI インターフェイスを VTEP 送信元インターフェイスに関連付けます。 |
| **vxlan port** | VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。 |

# send response

RADIUS の Accounting-Response Start および Accounting-Response Stop メッセージを RADIUS の Accounting-Request Start および Stop メッセージの送信元に送信するには、RADIUS アカウンティング パラメータ コンフィギュレーション モードで **send response** コマンドを使用します。このモードには、**inspect radius-accounting** コマンドを使用してアクセスします。

このオプションは、デフォルトで無効です。

**send response**

**no send response**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2(1) | このコマンドが追加されました。 |

## 例

次に、RADIUS アカウンティングで応答を送信する例を示します。

```
hostname(config)# policy-map type inspect radius-accounting ra
ciscoasa(config-pmap)# send response
ciscoasa(config-pmap-p)# send response
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **inspect radius-accounting** | RADIUS アカウンティングのインスペクションを設定します。 |
| **パラメータ** | インスペクション ポリシー マップのパラメータを設定します。 |

# seq-past-window

パストウィンドウ シーケンス番号（TCP 受信ウィンドウの適切な境界を越える受信 TCP パケットのシーケンス番号）を持つパケットに対するアクションを設定するには、tcp マップ コンフィギュレーション モードで **seq-past-window** コマンドを使用します。値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。このコマンドは、**set connection advanced-options** コマンドを使用してイネーブルにされる TCP 正規化ポリシーの一部です。

**seq-past-window** {**allow** | **drop**}

**no seq-past-window**

## 構文の説明

| | |
|---|---|
| **allow** | パストウィンドウ シーケンス番号を持つパケットを許可します。このアクションは、**queue-limit** コマンドが 0（ディセーブル）に設定されている場合に限り許可されます。 |
| **drop** | パストウィンドウ シーケンス番号を持つパケットをドロップします。 |

## デフォルト

デフォルトのアクションでは、パストウィンドウ シーケンス番号を持つパケットはドロップされます。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2(4)/8.0(4) | このコマンドが追加されました。 |

## 使用上のガイドライン

TCP 正規化をイネーブルにするには、モジュラ ポリシー フレームワークを次のように使用します。

1. **tcp-map**：TCP 正規化アクションを指定します。
   a. **seq-past-window**：tcp マップ コンフィギュレーション モードでは、**seq-past-window** コマンドおよびその他数多くのコマンドを入力できます。
2. **class-map**：TCP 正規化を実行するトラフィックを指定します。

3. **policy-map**：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. **set connection advanced-options**：作成した TCP マップを指定します。
4. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

## 例

次に、パストウィンドウ シーケンス番号を持つパケットを許可するように ASA を設定する例を示します。

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# seq-past-window allow
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match any
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **class-map** | サービス ポリシーに対してトラフィックを指定します。 |
| **policy-map** | サービス ポリシー内でトラフィックに適用するアクションを指定します。 |
| **queue-limit** | 順序が不正なパケットの制限を設定します。 |
| **set connection advanced-options** | TCP 正規化をイネーブルにします。 |
| **service-policy** | サービス ポリシーをインターフェイスに適用します。 |
| **show running-config tcp-map** | TCP マップ コンフィギュレーションを表示します。 |
| **tcp-map** | TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。 |

# serial-number

登録時に、ASA のシリアル番号を証明書に含めるには、クリプト CA トラストポイント コンフィギュレーション モードで **serial-number** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**serial-number**

**no serial-number**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルト設定では、シリアル番号は含まれません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

## コマンド履歴

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

## 例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central の登録要求に ASA のシリアル番号を含める例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# serial-number
```

## 関連コマンド

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

# server（POP3、IMAP4、SMTP）（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

デフォルトの電子メール プロキシ サーバを指定するには、該当する電子メール プロキシ コンフィギュレーション モードで **server** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** バージョンを使用します。ASA は、ユーザがサーバを指定せずに電子メール プロキシに接続した場合、デフォルトの電子メール サーバに要求を送信します。デフォルトのサーバを設定せず、ユーザもサーバを指定しない場合、ASA ではエラーが返されます。

**server** {*ipaddr or hostname*}

**no server**

## 構文の説明

| | |
|---|---|
| *hostname* | デフォルトの電子メール プロキシ サーバの DNS 名。 |
| *ipaddr* | デフォルトの電子メール プロキシ サーバの IP アドレス。 |

## デフォルト

デフォルトでは、デフォルトの電子メール プロキシ サーバはありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが追加されました。 |
| 9.5.2 | このコマンドは廃止されました。 |

## 例

次に、IP アドレス 10.1.1.7 を指定してデフォルトの POP3S 電子メール サーバを設定する例を示します。

```
ciscoasa(config)# pop3s
ciscoasa(config-pop3s)# server 10.1.1.7
```

# server（ScanSafe 汎用オプション）

プライマリおよびバックアップ クラウド Web セキュリティ プロキシ サーバを設定するには、ScanSafe 汎用オプション コンフィギュレーション モードで **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。

**server** {**primary** | **backup**} {**ip** *ip_address* | **fqdn** *fqdn*} [**port** *port*]

**no server** {**primary** | **backup**} {**ip** *ip_address* | **fqdn** *fqdn*} [**port** *port*]

## 構文の説明

| | |
|---|---|
| **backup** | バックアップ サーバを識別していることを指定します。 |
| **ip** *ip_address* | サーバの IP アドレスを指定します。 |
| **fqdn** *fqdn* | サーバの完全修飾ドメイン名（FQDN）を指定します。 |
| **port** *port* | （オプション）デフォルトでは、クラウド Web セキュリティ プロキシ サーバは HTTP と HTTPS の両方のトラフィックにポート 8080 を使用します。指示されている場合以外は、この値を変更しないでください。 |
| **primary** | プライマリ サーバを識別していることを指定します。 |

## コマンド デフォルト

デフォルト ポートは 8080 です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.0(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

Cisco Cloud Web Security サービスに登録すると、プライマリ クラウド Web セキュリティ プロキシ サーバとバックアップ プロキシ サーバが割り当てられます。これらのサーバは、アベイラビリティをチェックするために定期的にポーリングされます。ASA がクラウド Web セキュリティ プロキシ サーバに到達することができない場合（SYN/ACK パケットがプロキシ サーバから到着しない場合など）、プロキシ サーバは TCP スリーウェイ ハンドシェイクを介してポーリングされて、アベイラビリティがチェックされます。設定した試行回数（デフォルトは 5）後に、プロキシ サーバが使用不可の場合、サーバは到達不能として宣言され、バックアップ プロキシ サーバがアクティブになります。

(注) クラウド Web セキュリティ アプリケーションの状態をチェックすることで、フェールオーバーをさらに改善することができます。場合によっては、サーバが TCP スリーウェイ ハンドシェイクを完了できても、サーバ上のクラウド Web セキュリティ アプリケーションが正しく機能していないことがあります。アプリケーション健全性チェックを有効にすると、スリーウェイ ハンドシェイクが完了しても、アプリケーション自体が応答しない場合、システムはバックアップ サーバにフェールオーバーできます。これにより、より信頼性の高いフェールオーバー設定が確立されます。この追加のチェックを有効にするには、**health-check application** コマンドを使用します。

継続ポーリングによってプライマリ サーバが連続する 2 回の再試行回数の期間にアクティブであることが示されると、ASA はバックアップ サーバからプライマリ クラウド Web セキュリティ プロキシ サーバに自動的にフォール バックします。このポーリング間隔を変更するには、**retry-count** コマンドを使用します。

| プロキシ サーバが到達可能でないトラフィック状態 | サーバ タイムアウトの計算 | 接続タイムアウトの結果 |
|---|---|---|
| トラフィックが多い | クライアントのハーフ オープンの接続のタイムアウト + ASA TCP 接続タイムアウト | (30 + 30)= 60 秒 |
| 単一接続の失敗 | クライアントのハーフ オープンの接続のタイムアウト + ((再試行しきい値 - 1)x(ASA TCP 接続タイムアウト)) | (30 +((5-1)x(30)))= 150 秒 |
| アイドル:接続は送信されていません。 | 15 分 +((再試行しきい値)x (ASA TCP 接続タイムアウト)) | 900 +(5 x(30))= 1050 秒 |

## 例

次に、プライマリ サーバとバックアップ サーバを設定する例を示します。プライマリ サーバおよびバックアップ サーバに対して個別にコマンドを入力する必要があります。

```
scansafe general-options
 server primary ip 10.24.0.62 port 8080
 server backup ip 10.10.0.7 port 8080
 health-check application
 retry-count 7
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **class-map type inspect scansafe** | ホワイトリストに記載されたユーザとグループのインスペクション クラス マップを作成します。 |
| **default user group** | ASA に入ってくるユーザのアイデンティティを ASA が判別できない場合のデフォルトのユーザ名やグループを指定します。 |
| **health-check application** | フェールオーバーのための、クラウド Web セキュリティのアプリケーション健全性チェックを有効にします。 |
| **http**[**s**](パラメータ) | インスペクション ポリシー マップのサービス タイプ(HTTP または HTTPS)を指定します。 |

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

# server (ssh pubkey-chain)

オンボードのセキュア コピー(SCP)クライアントの SSH サーバおよびそのキーを ASA データベースに対して手動で追加または削除するには、ssh pubkey-chain コンフィギュレーション モードで **server** コマンドを使用します。サーバおよびそのホスト キーを削除するには、このコマンドの **no** 形式を使用します。

**server** *ip_address*

**no server** *ip_address*

## 構文の説明

| | |
|---|---|
| *ip_address* | SSH サーバの IP アドレスを指定します。 |

## コマンド デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.1(5) | このコマンドが追加されました。 |

## 使用上のガイドライン

オンボードの SCP クライアントを使用して、ASA との間でファイルをコピーすることができます。ASA は接続先の各 SCP サーバの SSH ホストキーを保存します。必要に応じて、ASA データベースから手動でサーバとそのキーを追加または削除できます。

各サーバについて、SSH ホストの **key-string**(公開キー) または **key-hash**(ハッシュ値)を指定できます。

## 例

次に、10.86.94.170 にあるサーバのすでにハッシュされているホスト キーを追加する例を示します。

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.86.94.170
ciscoasa(config-ssh-pubkey-server)# key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:
2e:19
```

次に、10.7.8.9 にあるサーバのホスト ストリング キーを追加する例を示します。

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **copy** | ASA との間でファイルをコピーします。 |
| **key-hash** | ハッシュ SSH ホスト キーを入力します。 |
| **key-string** | 公開 SSH ホスト キーを入力します。 |
| **ssh pubkey-chain** | ASA のデータベースに格納されるサーバとそのキーを手動で追加または削除します。 |
| **ssh stricthostkeycheck** | オンボードのセキュア コピー(SCP)クライアントの SSH ホスト キーのチェックをイネーブルにします。 |

# server authenticate-client

TLS ハンドシェイク時における ASA での TLS クライアントの認証をイネーブルにするには、TLS プロキシ コンフィギュレーション モードで **server authenticate-client** コマンドを使用します。

クライアント認証をバイパスするには、このコマンドの **no** 形式を使用します。

**server authenticate-client**

**no server authenticate-client**

## 構文の説明

このコマンドには、引数またはキーワードがありません。

## デフォルト

このコマンドは、デフォルトでイネーブルです。つまり、ASA とのハンドシェイク時に、TLS クライアントは、証明書の提示を要求されます。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.0(4) | このコマンドが追加されました。 |

## 使用上のガイドライン

TLS プロキシ ハンドシェイク時にクライアント認証が必要であるかどうかを制御するには、**server authenticate-client** コマンドを使用します。イネーブルの場合（デフォルト）、セキュリティ アプライアンスは TLS クライアントに証明書要求 TLS ハンドシェイク メッセージを送信し、TLS クライアントは証明書の提示を要求されます。

クライアント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。TLS クライアント認証のディセーブルは、ASA が CUMA クライアントや、Web ブラウザなどのクライアント証明書を送信できないクライアントと相互運用する必要がある場合に適しています。

## 例

次に、クライアント認証をディセーブルにした TLS プロキシ インスタンスを設定する例を示します。

```
ciscoasa(config)# tls-proxy mmp_tls
ciscoasa(config-tlsp)# no server authenticate-client
ciscoasa(config-tlsp)# server trust-point cuma_server_proxy
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **tls-proxy** | TLS プロキシ インスタンスを設定します。 |

# server cipher-suite

TLS プロキシ サーバで使用できる暗号方式を定義するには、tls プロキシ コンフィギュレーション モードで **server cipher suite** コマンドを使用します。グローバルな暗号方式の設定を使用するには、このコマンドの **no** 形式を使用します。

**server cipher-suite** *cipher_list*

**no server cipher-suite** *cipher_list*

## 構文の説明

| | |
|---|---|
| *cipher_list* | 次の任意の組み合わせを含めるように暗号方式を設定します。<br>• **3des-sha1**<br>• **aes128-sha1**<br>• **aes256-sha1**<br>• **des-sha1**<br>• **null-sha1**<br>• **rc4-sha1**<br>複数のオプションはスペースで区切ります。 |

## コマンド デフォルト

TLS プロキシで使用できる暗号方式を定義しないと、プロキシ サーバは **ssl cipher** コマンドによって定義されたグローバル暗号スイートを使用します。デフォルトでは、グローバル暗号方式レベルは medium です。つまり、NULL-SHA、DES-CBC-SHA、および RC4-MD5 を除くすべての暗号方式が使用できます。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.8(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

ASA が TLS プロキシ サーバとして動作している場合は、SSL 暗号スイートを設定できるようになりました。以前は、ASA に グローバル設定を行うには、**ssl cipher** コマンドを使用するしかありませんでした。

ASA で一般的に使用可能なスイート（**ssl cipher** コマンド）以外の別のスイートを使用する場合にのみ、server cipher-suite コマンドを指定します。

ASA 上のすべての SSL サーバ接続に最小 TLS バージョンを設定する場合は、**ssl server-version** コマンドを参照してください。デフォルトは TLS v1.0 です。

## 例

次に、TLS プロキシ サーバ暗号方式を設定する例を示します。

```
ciscoasa(config)# tls-proxy test
ciscoasa(config-tlsp)# server cipher-list aes128-sha1 aes256-sha1
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **tls-proxy** | TLS プロキシ インスタンスを定義し、最大セッション数を設定します。 |
| **client cipher-list** | TLS プロキシ クライアントの暗号スイートを定義します。 |

# server-port

ホストの AAA サーバ ポートを設定するには、AAA サーバ ホスト モードで **server-port** コマンドを使用します。指定されているサーバ ポートを削除するには、このコマンドの **no** 形式を使用します。

**server-port** *port-number*

**no server-port** *port-number*

## 構文の説明

| | |
|---|---|
| *port-number* | 0 ～ 65535 の範囲のポート番号。 |

## デフォルト

デフォルトのサーバ ポートは次のとおりです。

- SDI：5500
- LDAP：389
- Kerberos：88
- NT：139
- TACACS+：49

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 例

次に、srvgrp1 という名前の SDI AAA サーバでサーバ ポート番号 8888 を使用するように設定する例を示します。

```
ciscoasa(config)# aaa-server srvgrp1 protocol sdi
ciscoasa(config-aaa-server-group)# aaa-server srvgrp1 host 192.168.10.10
ciscoasa(config-aaa-server-host)# server-port 8888
```

関連コマンド

| コマンド | 説明 |
|---|---|
| **aaa-server host** | ホスト固有の AAA サーバ パラメータを設定します。 |
| **clear configure aaa-server** | AAA サーバのコンフィギュレーションをすべて削除します。 |
| **show running-config aaa-server** | すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。 |

# server-separator（POP3、IMAP4、SMTP）（廃止）

(注) このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

電子メール サーバ名および VPN サーバ名のデリミタとして文字を指定するには、該当する電子メール プロキシ モードで **server-separator** コマンドを使用します。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。

**server-separator** {*symbol*}

**no server-separator**

## 構文の説明

| | |
|---|---|
| *シンボル* | 電子メール サーバ名および VPN サーバ名を区切る文字。使用できるのは、「@」（アットマーク）、「|」（パイプ）、「:」（コロン）、「#」（番号記号）、「,」（カンマ）、および「;」（セミコロン）です。 |

## デフォルト

デフォルトは「@」（アット マーク）です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | トランスペアレント | シングル | コンテキスト | システム |
| pop3s | • 対応 | — | • 対応 | — | — |
| Imap4s | • 対応 | — | • 対応 | — | — |
| Smtps | • 対応 | — | • 対応 | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが追加されました。 |
| 9.5.2 | このコマンドは廃止されました。 |

## 使用上のガイドライン

サーバの区切り文字には、名前の区切り文字とは異なる文字を使用する必要があります。

## 例

次に、パイプ（|）を IMAP4S サーバの区切り文字として設定する例を示します。

```
ciscoasa(config)# imap4s
ciscoasa(config-imap4s)# server-separator |
```

関連コマンド

| コマンド | 説明 |
|---|---|
| **name-separator** | 電子メールおよび VPN のユーザ名とパスワードを区切ります。 |

# server trust-point

TLS ハンドシェイク時に提示するプロキシ トラストポイント証明書を指定するには、TLS サーバ コンフィギュレーション モードで **server trust-point** コマンドを使用します。

**server trust-point** *proxy_trustpoint*

## 構文の説明

| | |
|---|---|
| *proxy_trustpoint* | **crypto ca trustpoint** コマンドによって定義されるトラストポイントを指定します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.0(4) | このコマンドが追加されました。 |

## 使用上のガイドライン

トラストポイントでは、自己署名証明書、認証局に登録されている証明書、またはインポートされたクレデンシャルの証明書を使用できます。**server trust-point** コマンドは、グローバル **ssl trust-point** コマンドよりも優先されます。

**server trust-point** コマンドは、TLS ハンドシェイク時に提示するプロキシ トラストポイント証明書を指定します。証明書は、ASA が所有している必要があります（ID 証明書）。証明書には、自己署名証明書、認証局に登録されている証明書、またはインポートされたクレデンシャルの証明書を使用できます。

接続を開始できる各エンティティに対して TLS プロキシ インスタンスを作成します。TLS 接続を開始するエンティティは、TLS クライアントのロールを担います。TLS プロキシにはクライアント プロキシとサーバ プロキシが厳密に定義されているため、いずれのエンティティからも接続が開始される可能性がある場合には、2 つの TLS プロキシ インスタンスを定義する必要があります。

**（注）** 電話プロキシとともに使用する TLS プロキシ インスタンスを作成する場合、サーバのトラストポイントは、CTL ファイル インスタンスによって作成される内部電話プロキシ トラストポイントです。トラストポイント名は、*internal_PP_<ctl-file_instance_name> の形式となります。*

## 例

次に、**server trust-point** コマンドを使用して、TLS ハンドシェイク時に提示するプロキシ トラストポイント証明書を指定する例を示します。

```
ciscoasa(config-tlsp)# server trust-point ent_y_proxy
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **client (tls-proxy)** | TLS プロキシ インスタンスのトラストポイント、キー ペア、および暗号スイートを設定します。 |
| **client trust-point** | TLS ハンドシェイク中に提示するプロキシ トラストポイント証明書を指定します。 |
| **ssl trust-point** | インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。 |
| **tls-proxy** | TLS プロキシ インスタンスを設定します。 |

# server-type

LDAP サーバ モデルを手動で設定するには、AAA サーバ ホスト コンフィギュレーション モードで **server-type** コマンドを使用します。ASA では、次のサーバ モデルがサポートされています。

- Microsoft Active Directory
- Sun Microsystems JAVA System Directory Server（以前の Sun ONE Directory Server）
- LDAPv3 に準拠した一般的な LDAP ディレクトリ サーバ（パスワード管理なし）

このコマンドをディセーブルにするには、このコマンドの **no** 形式を使用します。

**server-type** {**auto-detect** | **microsoft** | **sun** | **generic** | **openldap** | **novell**}

**no server-type** {**auto-detect** | **microsoft** | **sun** | **generic** | **openldap** | **novell**}

## 構文の説明

| | |
|---|---|
| **auto-detect** | ASA で自動検出によって LDAP サーバ タイプを決定することを指定します。 |
| **generic** | Sun および Microsoft の LDAP ディレクトリ サーバ以外の LDAP v3 準拠のディレクトリ サーバを指定します。一般的な LDAP サーバでは、パスワード管理はサポートされません。 |
| **microsoft** | LDAP サーバが Microsoft Active Directory であることを指定します。 |
| **openldap** | LDAP サーバが OpenLDAP サーバであることを指定します。 |
| **novell** | LDAP サーバが Novell サーバであることを指定します。 |
| **sun** | LDAP サーバが Sun Microsystems JAVA System Directory Server であることを指定します。 |

## デフォルト

デフォルトでは、自動検出によってサーバ タイプの決定が試みられます。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1(1) | このコマンドが追加されました。 |
| 8.0(2) | OpenLDAP および Novell サーバ タイプのサポートが追加されました。 |

## 使用上のガイドライン

ASA は LDAP バージョン 3 をサポートしており、Sun Microsystems JAVA System Directory Server、Microsoft Active Directory、およびその他の LDAPv3 ディレクトリ サーバと互換性があります。

（注）

- Sun：Sun ディレクトリ サーバにアクセスするために ASA に設定されている DN は、そのサーバ上のデフォルト パスワード ポリシーにアクセスできる必要があります。DN として、ディレクトリ管理者、またはディレクトリ管理者権限を持つユーザを使用することを推奨します。または、デフォルト パスワード ポリシーに ACI を設定できます。
- Microsoft：Microsoft Active Directory でパスワード管理をイネーブルにするには、LDAP over SSL を設定する必要があります。
- Generic：パスワード管理機能はサポートされていません。

デフォルトで、ASA では、Microsoft ディレクトリ サーバ、Sun LDAP ディレクトリ サーバ、または一般的な LDAPv3 サーバのいずれに接続しているかが自動検出されます。ただし、自動検出で LDAP サーバ タイプを決定できない場合で、サーバが Microsoft または Sun のサーバであることが明らかである場合は、**server-type** コマンドを使用して、サーバを Microsoft または Sun Microsystems の LDAP サーバとして手動で設定できます。

## 例

次に、AAA サーバ ホスト コンフィギュレーション モードで、IP アドレス 10.10.0.1 の LDAP サーバ ldapsvr1 のサーバ タイプを設定する例を示します。この最初の例では、Sun Microsystems LDAP サーバを設定しています。

```
ciscoasa(config)# aaa-server ldapsvr1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# server-type sun
```

次に、ASA で自動検出を使用してサーバ タイプを決定することを指定する例を示します。

```
ciscoasa(config)# aaa-server ldapsvr1 protocol LDAP
ciscoasa(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# server-type auto-detect
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **ldap-over-ssl** | SSL が LDAP クライアントとサーバ間の接続を保護することを指定します。 |
| **sasl-mechanism** | LDAP クライアントおよびサーバ間での SASL 認証を設定します。 |
| **ldap attribute-map**（グローバル コンフィギュレーション モード） | ユーザ定義の属性名を Cisco LDAP 属性名にマッピングするために、LDAP 属性マップを作成して名前を付けます。 |

# service (ctl-provider)

証明書信頼リスト プロバイダーがリッスンするポートを指定するには、CTL プロバイダー コンフィギュレーション モードで **service** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

**service port** *listening_port*

**no service port** *listening_port*

## 構文の説明

| | |
|---|---|
| **port** *listening_port* | クライアントにエクスポートする証明書を指定します。 |

## デフォルト

デフォルトのポートは 2444 です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.0(2) | このコマンドが追加されました。 |

## 使用上のガイドライン

CTL プロバイダーがリッスンするポートを指定するには、CTL プロバイダー コンフィギュレーション モードで **service** コマンドを使用します。ポートは、クラスタ内の CallManager サーバによってリッスンされているポートである必要があります（[CallManager administration] ページの [Enterprise Parameters] で設定）。デフォルトのポートは 2444 です。

## 例

次の例は、CTL プロバイダー インスタンスを作成する方法を示しています。

```
ciscoasa(config)# ctl-provider my_ctl
ciscoasa(config-ctl-provider)# client interface inside 172.23.45.1
ciscoasa(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
ciscoasa(config-ctl-provider)# export certificate ccm_proxy
ciscoasa(config-ctl-provider)# ctl install
```

関連コマンド

| コマンド | 説明 |
|---|---|
| クライアント | CTL プロバイダーへの接続が許可されるクライアントを指定し、クライアント認証用のユーザ名とパスワードも指定します。 |
| **ctl** | CTL クライアントの CTL ファイルを解析し、トラストポイントをインストールします。 |
| **ctl-provider** | CTL プロバイダー モードで CTL プロバイダー インスタンスを設定します。 |
| **export** | クライアントにエクスポートする証明書を指定します。 |
| **tls-proxy** | TLS プロキシ インスタンスを定義し、最大セッション数を設定します。 |

# service（グローバル）

拒否された TCP 接続のリセットをイネーブルにするには、グローバル コンフィギュレーション モードで **service** コマンドを使用します。リセットをディセーブルにするには、このコマンドの **no** 形式を使用します。

**service** {**resetinbound** [**interface** *interface_name*] | **resetoutbound** [**interface** *interface_name*] | **resetoutside**}

**no service** {**resetinbound** [**interface** *interface_name*] | **resetoutbound** [**interface** *interface_name*] | **resetoutside**}

## 構文の説明

| | |
|---|---|
| **interface** *interface_name* | 指定したインターフェイスのリセットをイネーブルまたはディセーブルにします。 |
| **resetinbound** | ASA の通過を試み、アクセス リストまたは AAA 設定に基づいて ASA によって拒否されたすべての着信 TCP セッションに TCP リセットを送信します。ASA は、アクセス リストまたは AAA によって許可されても、既存の接続に属しておらず、ステートフル ファイアウォールによって拒否されたパケットのリセットも送信します。同じセキュリティ レベルのインターフェイス間のトラフィックも影響を受けます。このオプションがイネーブルになっていない場合は、ASA は拒否されたパケットを、何も通知せずに廃棄します。インターフェイスを指定しない場合、この設定はすべてのインターフェイスに適用されます。 |
| **resetoutbound** | ASA の通過を試み、アクセス リストまたは AAA 設定に基づいて ASA によって拒否されたすべての発信 TCP セッションに TCP リセットを送信します。ASA は、アクセス リストまたは AAA によって許可されても、既存の接続に属しておらず、ステートフル ファイアウォールによって拒否されたパケットのリセットも送信します。同じセキュリティ レベルのインターフェイス間のトラフィックも影響を受けます。このオプションがイネーブルになっていない場合は、ASA は拒否されたパケットを、何も通知せずに廃棄します。このオプションは、デフォルトで有効です。たとえば、トラフィック ストーム時に CPU の負荷を軽減するためなどに発信リセットをディセーブルにできます。 |
| **resetoutside** | 最もセキュリティ レベルの低いインターフェイスで終端し、アクセス リストまたは AAA 設定に基づいて ASA によって拒否された TCP パケットのリセットをイネーブルにします。ASA は、アクセス リストまたは AAA によって許可されても、既存の接続に属しておらず、ステートフル ファイアウォールによって拒否されたパケットのリセットも送信します。このオプションをイネーブルにしなかった場合、ASA は拒否されたパケットを何も通知せずに廃棄します。<br><br>インターフェイス PAT では、**resetoutside** キーワードを使用することを推奨します。このキーワードを使用すると、外部 SMTP または FTP サーバからの IDENT を ASA で終了できます。これらの接続をアクティブにリセットすることによって、30 秒のタイムアウト遅延を回避できます。<br><br>**（注）** 接続はこのオプションに関係なく、常に BGP と WebVPN（安全性が最低のインターフェイス）にリセットされます。 |

## 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 **service resetoutbound** がイネーブルになっています。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1(1) | **interface** キーワードおよび **resetoutbound** コマンドが追加されました。 |

## 使用上のガイドライン

アイデンティティ要求（IDENT）接続をリセットする必要がある場合は、着信トラフィックに対して明示的にリセットを送信できます。拒否されたホストに TCP RST（TCP ヘッダーのリセットフラグ）を送信すると、RST によって着信 IDENT プロセスが停止されるため、IDENT がタイムアウトするのを待機する必要がなくなります。外部ホストは IDENT がタイムアウトするまで SYN を継続的に再送信するため、IDENT がタイムアウトするのを待機するとトラフィックの速度低下の原因となる可能性があります。そのため、**service resetinbound** コマンドによってパフォーマンスが向上する可能性があります。

## 例

次に、内部インターフェイスを除くすべてのインターフェイスで発信リセットをディセーブルにする例を示します。

```
ciscoasa(config)# no service resetoutbound
ciscoasa(config)# service resetoutbound interface inside
```

次に、DMZ インターフェイスを除くすべてのインターフェイスで着信リセットをイネーブルにする例を示します。

```
ciscoasa(config)# service resetinbound
ciscoasa(config)# no service resetinbound interface dmz
```

次に、外部インターフェイスが終端となる接続でリセットをイネーブルにする例を示します。

```
ciscoasa(config)# service resetoutside
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show running-config service** | サービス コンフィギュレーションを表示します。 |

# service（オブジェクト サービス）

サービス オブジェクトのプロトコルおよびオプションの属性を定義するには、オブジェクト サービス コンフィギュレーション モードで **service** コマンドを使用します。定義を削除するには、このコマンドの **no** 形式を使用します。

**service** {*protocol* | {**tcp** | **udp** | **sctp**} [**source** *operator number*] [**destination** *operator number*] | {**icmp** | **icmp6**} [*icmp_type* [*icmp_code*]]}

**no service** {*protocol* | {**tcp** | **udp** | **sctp**} [**source** *operator number*] [**destination** *operator number*] | {**icmp** | **icmp6**} [*icmp_type* [*icmp_code*]]}

## 構文の説明

| | |
|---|---|
| **destination** *operator number* | （オプション：**tcp**、**udp**、**sctp** のみ）宛先ポート名または番号（0 ～ 65535）を指定します。サポートされる名前のリストについては、CLI ヘルプを参照してください。演算子は次のとおりです。<br>• **eq**：ポート番号に等しい。<br>• **gt**：ポート番号より大きい。<br>• **lt**：ポート番号より小さい。<br>• **neq**：ポート番号と等しくない。<br>• **range**：ポート範囲。2 つの番号は、**range 1024 4500** のようにスペースで区切って指定します。 |
| {**icmp** \| **icmp6**} [*icmp_type* [*icmp_code*]] | サービス タイプが ICMP または ICMP バージョン 6 接続用であることを指定します。任意で ICMP タイプを名前または番号（0 ～ 255）で指定できます（使用可能なオプションの ICMP タイプ名については、CLI のヘルプを参照してください）。タイプを指定すると、オプションで ICMP コード（1 ～ 255）を含めることができます。 |
| *protocol* | プロトコル名または番号（0 ～ 255）を指定します。サポートされる名前のリストについては、CLI ヘルプを参照してください。 |
| **sctp** | サービス タイプが Stream Control Transmission Protocol（SCTP）接続であることを指定します。 |
| **source** *operator number* | （オプション：**tcp**、**udp**、**sctp** のみ）送信元ポート名または番号（0 ～ 65535）を指定します。サポートされる名前のリストについては、CLI ヘルプを参照してください。演算子は **destination** のものと同じです。 |
| **tcp** | サービス タイプが TCP 接続用であることを指定します。 |
| **udp** | サービス タイプが UDP 接続用であることを指定します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.3(1) | このコマンドが追加されました。 |
| 9.0(1) | ICMP コードのサポートが追加されました。 |
| 9.5(2) | SCTP のサポートが追加されました。 |

## 使用上のガイドライン

ACL（**access-list** コマンド）や NAT（**nat** コマンド）など、コンフィギュレーションの他の部分ではサービス オブジェクトを名前で使用できます。

既存のサービス オブジェクトを別のプロトコルおよびポートを使用して設定した場合、新しいコンフィギュレーションでは既存のプロトコルとポートが新しいプロトコルとポートに置き換わります。

## 例

次に、SSH トラフィックのサービス オブジェクトを作成する例を示します。

```
ciscoasa(config)# object service SSH
ciscoasa(config-service-object)# service tcp destination eq ssh
```

次に、EIGRP トラフィックのサービス オブジェクトを作成する例を示します。

```
ciscoasa(config)# object service EIGRP
ciscoasa(config-service-object)# service eigrp
```

次に、ポート 0 ～ 1024 から HTTPS へのトラフィックに対してサービス オブジェクトを作成する例を示します。

```
ciscoasa(config)# object service HTTPS
ciscoasa(config-service-object)# service tcp source range 0 1024 destination eq https
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure object** | 作成されたすべてのオブジェクトをクリアします。 |
| **object-group service** | サービス オブジェクトを設定します。 |
| **show running-config object service** | 現在のサービス オブジェクト コンフィギュレーションを表示します。 |

# service call-home

Call Home サービス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 **service call-home** コマンドを使用します。Call Home サービスをディセーブルにするには、このコマンドの **no** 形式を使用します。

**service call-home**

**no service call-home**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルトで、サービス Call Home コマンドはディセーブルです。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.2(2) | このコマンドが追加されました。 |

## 例

次に、Call Home サービスをイネーブルにする例を示します。

```
ciscoasa(config)# service call-home
```

次に、Call Home サービスをディセーブルにする例を示します。

```
hostname(config)# no service call-home
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **call-home**（グローバル コンフィギュレーション） | Call Home コンフィギュレーション モードを開始します。 |
| **call-home test** | Call Home テスト メッセージを手動で送信します。 |
| **show call-home** | Call Home コンフィギュレーション情報を表示します。 |

# service-module

サービスモジュールが応答しなくなったことをシステムが判断するまでの時間を調整するには、グローバル コンフィギュレーション モードで **service-module** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**service-module** {*module_id* | **all**} {**keepalive-counter** | **keepalive-timeout**} *value*

**no service-module** {*module_id* | **all**} {**keepalive-counter** | **keepalive-timeout**} *value*

## 構文の説明

| | |
|---|---|
| {*module_id* \| **all**} | キープアライブ値を調整するモジュールを指定します。**all** を指定すると、すべてのモジュールのキープアライブ値を調整します。**?** を使用して、システムに有効なモジュール ID を決定します。ID は通常、次のようになります。<br>• 最初のスロットのモジュールの場合は **1**。<br>• ASA FirePOWER モジュールの場合は **sfr**。 |
| **keepalive-counter** *value* | モジュールがダウンしていると見なされる前に応答なしで送信できるキープアライブの最大数（1 ～ 12）。 |
| **keepalive-timeout** *value* | キープアライブメッセージの送信間隔（4 ～ 16 秒）。 |

## デフォルト

デフォルトのカウントは 6、デフォルトのタイムアウトは 4 です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.12(3) | このコマンドが追加されました。 |

## 使用上のガイドライン

システムでは、コントロールプレーンのキープアライブメッセージを送信することで、サービスモジュールのヘルスステータスを定期的にチェックしています。CPU の使用率が高いために通信の遅延が発生した場合、システムが応答をすぐに受信できず、これによりモジュールから応答を受信しなかったと判断する可能性があります。システムは、モジュールが実際には正常に機能しているにもかかわらず、ダウンしていることを宣言し、通信チャネルを閉じます。ハイアベイラビリティが設定されている場合、システムはサービスカードの障害によりバックアップユニットにフェールオーバーします。これがセットアップ中頻繁に発生する場合は、キープアライブ時間を延長するか、システムがモジュールの障害を宣言するまでの時間を延長してください。

## 例

次の例では、キープアライブ時間およびタイムアウトを変更する方法について示します。

```
ciscoasa(config)# service-module all keepalive-count 10
ciscoasa(config)# service-module all keepalive-timeout 8
```

# service-object

TCP、UDP、または TCP-UDP として事前定義されていないサービスまたはサービス オブジェクトをサービス オブジェクト グループに追加するには、オブジェクトグループ サービス コンフィギュレーション モードで **service-object** コマンドを使用します。サービスを削除するには、このコマンドの **no** 形式を使用します。

**service-object** {*protocol* | {**tcp** | **udp** | **tcp-udp** | **sctp**} [**source** *operator number*] [**destination** *operator number*] | {**icmp** | **icmp6**} [*icmp_type* [*icmp_code*]] | **object** *name*}

**no service-object** {*protocol* | {**tcp** | **udp** | **tcp-udp** | **sctp**} [**source** *operator number*] [**destination** *operator number*] | {**icmp** | **icmp6**} [*icmp_type* [*icmp_code*]] | **object** *name*}

## 構文の説明

| | |
|---|---|
| **destination** *operator number* | (オプション:**tcp**、**udp**、**tcp-udp**、**sctp** のみ)宛先ポート名または番号(0 ～ 65535)を指定します。サポートされる名前のリストについては、CLI ヘルプを参照してください。演算子は次のとおりです。<br>• **eq**:ポート番号に等しい。<br>• **gt**:ポート番号より大きい。<br>• **lt**:ポート番号より小さい。<br>• **neq**:ポート番号と等しくない。<br>• **range**:ポート範囲。2 つの番号は、**range 1024 4500** のようにスペースで区切って指定します。 |
| {**icmp** \| **icmp6**} [*icmp_type* [*icmp_code*]] | サービス タイプが ICMP または ICMP バージョン 6 接続用であることを指定します。任意で ICMP タイプを名前または番号(0 ～ 255)で指定できます(使用可能なオプションの ICMP タイプ名については、CLI のヘルプを参照してください)。タイプを指定すると、オプションで ICMP コード(1 ～ 255)を含めることができます。 |
| **object** *name* | 名前付きオブジェクトまたはグループをオブジェクトに追加します。 |
| *protocol* | プロトコル名または番号(0 ～ 255)を指定します。サポートされる名前のリストについては、CLI ヘルプを参照してください。 |
| **sctp** | サービス タイプが Stream Control Transmission Protocol(SCTP)接続であることを指定します。 |
| **source** *operator number* | (オプション:**tcp**、**udp**、**tcp-udp**、**sctp** のみ)送信元ポート名または番号(0 ～ 65535)を指定します。サポートされる名前のリストについては、CLI ヘルプを参照してください。演算子は **destination** のものと同じです。 |
| **tcp** | サービス タイプが TCP 接続用であることを指定します。 |
| **tcp-udp** | サービス タイプが TCP または UDP 接続用であることを指定します。 |
| **udp** | サービス タイプが UDP 接続用であることを指定します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.0(1) | このコマンドが追加されました。 |
| 8.3(1) | **object** キーワードが、サービス オブジェクト（**object service** コマンド）をサポートするために追加されました。 |
| 9.0(1) | ICMP コードのサポートが追加されました。 |
| 9.5(2) | SCTP のサポートが追加されました。 |

## 使用上のガイドライン

**object-group service** コマンドを使用してサービス オブジェクト グループを作成した場合、グループ全体に対してプロトコル タイプを事前定義していなければ、**service-object** コマンドを使用して、複数のサービスおよびサービス オブジェクト（ポートを含む）をさまざまなプロトコルのグループに追加できます。**object-group service [tcp | udp | tcp-udp]** コマンドを使用して特定のプロトコル タイプに対してサービス オブジェクト グループを作成した場合、**port-object** コマンドを使用してオブジェクト グループに指定できるのは宛先ポートのみです。

## 例

次の例では、TCP と UDP の両方のサービスを同じサービス オブジェクト グループに追加する方法を示します。

```
ciscoasa(config)# object-group service CommonApps
ciscoasa(config-service-object-group)# service-object tcp destination eq ftp
ciscoasa(config-service-object-group)# service-object tcp-udp destination eq www
ciscoasa(config-service-object-group)# service-object tcp destination eq h323
ciscoasa(config-service-object-group)# service-object tcp destination eq https
ciscoasa(config-service-object-group)# service-object udp destination eq ntp
```

次の例では、複数のサービス オブジェクトを同じサービス オブジェクト グループに追加する方法を示します。

```
hostname(config)# service object SSH
hostname(config-service-object)# service tcp destination eq ssh

hostname(config)# service object EIGRP
hostname(config-service-object)# service eigrp

hostname(config)# service object HTTPS
hostname(config-service-object)# service tcp source range 0 1024 destination eq https

ciscoasa(config)# object-group service Group1
ciscoasa(config-service-object-group)# service-object object SSH
ciscoasa(config-service-object-group)# service-object object EIGRP
ciscoasa(config-service-object-group)# service-object object HTTPS
```

関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure object-group** | すべての **object-group** コマンドをコンフィギュレーションから削除します。 |
| **network-object** | ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。 |
| **object service** | サービス オブジェクトを追加します。 |
| **object-group** | コンフィギュレーションを最適化するためのオブジェクト グループを定義します。 |
| **port-object** | サービス オブジェクト グループにポート オブジェクトを追加します。 |
| **show running-config object-group** | 現在のオブジェクト グループを表示します。 |

# service password-recovery

パスワードの回復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 **service password-recovery** コマンドを使用します。パスワードの回復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。パスワードの回復はデフォルトでイネーブルですが、不正なユーザがパスワードの回復メカニズムを使用して ASA を侵害できないようにするためにディセーブルにすることができます。

**service password-recovery**

**no service password-recovery**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

パスワードの回復は、デフォルトでイネーブルです。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 使用上のガイドライン

ASA 5500 シリーズ適応型セキュリティ アプライアンスでは、パスワードを忘れた場合、起動時にプロンプトが表示されたときに端末のキーボードで Esc キーを押して、ROMMON で ASA を起動できます。次に、コンフィギュレーション レジスタを変更することによって、スタートアップ コンフィギュレーションを無視するように ASA を設定します（**config-register** コマンドを参照）。たとえば、コンフィギュレーション レジスタがデフォルトの 0x1 の場合、**confreg 0x41** コマンドを入力して値を 0x41 に変更します。ASA がリロードされると、デフォルトのコンフィギュレーションがロードされ、デフォルトのパスワードを使用して特権 EXEC モードを開始できます。その後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーしてスタートアップ コンフィギュレーションをロードし、パスワードをリセットします。最後に、コンフィギュレーション レジスタを元の設定に戻して、以前と同様に起動するように ASA を設定します。たとえば、グローバル コンフィギュレーション モードで **config-register 0x1** コマンドを入力します。

PIX 500 シリーズ セキュリティ アプライアンスでは、起動時にプロンプトが表示されたときに端末のキーボードで Esc キーを押して、モニタ モードで ASA を起動します。その後、PIX パスワード ツールを ASA にダウンロードして、すべてのパスワードおよび **aaa authentication** コマンドを消去します。

ASA 5500 シリーズ適応型セキュリティ アプライアンスでは、**no service password-recovery** コマンドを使用すると、ユーザが ROMMON を開始することを防止でき、コンフィギュレーションも変更されないままとすることができます。ユーザが ROMMON を開始すると、ユーザは、ASA によって、すべてのフラッシュ ファイル システムを消去するように求められます。ユーザは、最初に消去を実行しないと、ROMMON を開始できません。ユーザがフラッシュ ファイル システムを消去しない場合、ASA はリロードします。パスワードの回復は ROMMON の使用と既存のコンフィギュレーションを維持することに依存しているため、フラッシュ ファイル システムを消去することによってパスワードを回復できなくなります。ただし、パスワードを回復できなくすることで、不正なユーザがコンフィギュレーションを表示したり、別のパスワードを挿入したりすることがなくなります。この場合に、システムを動作ステートに回復するには、新しいイメージとバックアップ コンフィギュレーション ファイル(使用可能な場合)をロードします。**service password-recovery** コマンドは、コンフィギュレーション ファイルに情報提供の目的でのみ表示されます。CLI プロンプトでこのコマンドを入力すると、設定は NVRAM に保存されます。設定を変更する唯一の方法は、CLI プロンプトでコマンドを入力することです。このコマンドの異なるバージョンで新規コンフィギュレーションをロードしても、設定は変更されません。ASA が起動時にスタートアップ コンフィギュレーションを無視するように設定されている場合にパスワードの回復をディセーブルにすると、ASA によって設定が変更され、通常どおりにスタートアップ コンフィギュレーションが起動されます。フェールオーバーを使用し、スタートアップ コンフィギュレーションを無視するようにスタンバイ装置が設定されている場合は、**no service password recovery** コマンドでスタンバイ装置に複製したときにコンフィギュレーション レジスタに同じ変更が加えられます。

PIX 500 シリーズ セキュリティ アプライアンスでは、**no service password-recovery** コマンドを使用すると、ユーザは、PIX パスワード ツールによって、すべてのフラッシュ ファイル システムを消去するように求められます。ユーザは、最初に消去を実行しないと、PIX パスワード ツールを使用できません。ユーザがフラッシュ ファイル システムを消去しない場合、ASA はリロードします。パスワードの回復は既存のコンフィギュレーションを維持することに依存しているため、フラッシュ ファイル システムを消去することによってパスワードを回復できなくなります。ただし、パスワードを回復できなくすることで、不正なユーザがコンフィギュレーションを表示したり、別のパスワードを挿入したりすることがなくなります。この場合に、システムを動作ステートに回復するには、新しいイメージとバックアップ コンフィギュレーション ファイル(使用可能な場合)をロードします。

## 例

次に、ASA 5500 シリーズのパスワードの回復をディセーブルにする例を示します。

```
ciscoasa(config)# no service password-recovery
WARNING: Executing "no service password-recovery" has disabled the password recovery
mechanism and disabled access to ROMMON. The only means of recovering from lost or
forgotten passwords will be for ROMMON to erase all file systems including configuration
files and images. You should make a backup of your configuration and have a mechanism to
restore images from the ROMMON command line.
```

次に、ASA 5500 シリーズで、起動時に ROMMON を開始するタイミングとパスワードの回復操作を完了する例を示します。

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.
```

```
Use ? for help.
rommon #0> confreg

Current Configuration Register: 0x00000001
Configuration Summary:
  boot default image from Flash

Do you wish to change this configuration? y/n [n]: n

rommon #1> confreg 0x41

Update Config Register (0x41) in NVRAM...

rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.


Loading disk0:/ASA_7.0.bin... Booting...
###################
...
Ignoring startup configuration as instructed by configuration register.
Type help or '?' for a list of available commands.
ciscoasa> enable
Password:
ciscoasa# configure terminal
ciscoasa(config)# copy startup-config running-config

Destination filename [running-config]?
Cryptochecksum(unchanged): 7708b94c e0e3f0d5 c94dde05 594fbee9

892 bytes copied in 6.300 secs (148 bytes/sec)
ciscoasa(config)# enable password NewPassword
ciscoasa(config)# config-register 0x1
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **config-register** | リロード時にスタートアップ コンフィギュレーションを無視するように ASA を設定します。 |
| **イネーブル パスワード** | イネーブル パスワードを設定します。 |
| **password** | ログイン パスワードを設定します。 |

# service-policy（クラス）

別のポリシー マップの下に階層型ポリシー マップを適用するには、クラス コンフィギュレーション モードで **service-policy** コマンドを使用します。サービス ポリシーをディセーブルにするには、このコマンドの **no** 形式を使用します。階層型ポリシーは、シェーピングされたトラフィックのサブセットに対してプライオリティ キューイングを実行する場合に QoS トラフィック シェーピングでのみサポートされています。

**service-policy** *policymap_name*

**no service-policy** *policymap_name*

## 構文の説明

| | |
|---|---|
| *policymap_name* | **policy-map** コマンドで設定したポリシー マップ名を指定します。**priority** コマンドを含むレイヤ 3/4 ポリシー マップのみを指定できます。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2(4)/8.0(4) | このコマンドが追加されました。 |

## 使用上のガイドライン

階層型プライオリティ キューイングは、トラフィック シェーピング キューを有効にするインターフェイスで使用します。シェーピングされるトラフィックのサブセットに優先順位を付けることができます。標準プライオリティ キュー（**priority-queue** コマンド）は使用しません。

階層型プライオリティ キューイングでは、モジュラ ポリシー フレームワークを使用して次のタスクを実行します。

1. **class-map**：プライオリティ キューイングを実行するトラフィックを指定します。
2. **policy-map**（プライオリティ キューイングの場合）：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. **priority**：クラス マップのプライオリティ キューイングを有効にします。ポリシー マップを階層的に使用する場合は、このポリシー マップに priority コマンドだけを含めることができます。

3. **policy-map**（トラフィック シェーピングの場合）：**class-default** クラス マップに関連付けるアクションを指定します。
   a. **class class-default**：アクションを実行する **class-default** クラス マップを指定します。
   b. **shape**：トラフィック シェーピングをクラス マップに適用します。
   c. **service-policy**：プライオリティ キューイングをシェーピングされたトラフィックのサブセットに適用できるように、**priority** コマンドを設定したプライオリティ キューイング ポリシー マップを呼び出します。
4. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

## 例

次の例では、外部インターフェイスのすべてのトラフィックでトラフィック シェーピングをイネーブルにして、DSCP ビットが ef に設定された VPN tunnel-grp1 内のトラフィックにプライオリティを付けます。

```
ciscoasa(config)# class-map TG1-voice
ciscoasa(config-cmap)# match tunnel-group tunnel-grp1
ciscoasa(config-cmap)# match dscp ef

ciscoasa(config)# policy-map priority-sub-policy
ciscoasa(config-pmap)# class TG1-voice
ciscoasa(config-pmap-c)# priority

ciscoasa(config-pmap-c)# policy-map shape_policy
ciscoasa(config-pmap)# class class-default
ciscoasa(config-pmap-c)# shape
ciscoasa(config-pmap-c)# service-policy priority-sub-policy

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

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **class**（ポリシー マップ） | ポリシー マップにクラス マップを指定します。 |
| **clear configure service-policy** | サービス ポリシーのコンフィギュレーションをクリアします。 |
| **clear service-policy** | サービス ポリシーの統計情報をクリアします。 |
| **policy-map** | クラス マップに対して実行するアクションを指定します。 |
| **priority** | プライオリティ キューイングをイネーブルにします。 |
| **service-policy (global)** | インターフェイスにポリシー マップを適用します。 |
| **shape** | トラフィック シェーピングをイネーブルにします。 |
| **show running-config service-policy** | 実行コンフィギュレーションに設定されているサービス ポリシーを表示します。 |
| **show service-policy** | サービス ポリシーの統計情報を表示します。 |

# service-policy (global)

すべてのインターフェイスでグローバルに、または特定のインターフェイスでポリシー マップをアクティブにするには、グローバル コンフィギュレーション モードで **service-policy** コマンドを使用します。サービス ポリシーをディセーブルにするには、このコマンドの **no** 形式を使用します。インターフェイスでポリシーのセットをイネーブルにするには、**service-policy** コマンドを使用します。

**service-policy** *policymap_name* [**global** | **interface** *intf* ] [**fail-close**]

**no service-policy** *policymap_name* [**global** | **interface** *intf* ] [**fail-close**]

## 構文の説明

| | |
|---|---|
| **fail-close** | IPv6 トラフィックをサポートしていないアプリケーション インスペクションによってドロップされた IPv6 トラフィックに対して syslog（767001）を生成します。デフォルトでは、syslog が生成されません。 |
| **global** | すべてのインターフェイスにポリシー マップを適用します。 |
| **interface** *intf* | 特定のインターフェイスにポリシー マップを適用します。 |
| *policymap_name* | **policy-map** コマンドで設定したポリシー マップ名を指定します。レイヤ 3/4 ポリシー マップのみを指定できます。インスペクション ポリシー マップ（**policy-map type inspect**）は指定できません。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 使用上のガイドライン

サービス ポリシーをイネーブルにするには、Modular Policy Framework を使用します。

1. **class-map**：プライオリティ キューイングを実行するトラフィックを指定します。
2. **policy-map**：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. *commands for supported features*：特定のクラス マップについて、QoS、アプリケーション インスペクション、CSC または AIP SSM、TCP 接続と UDP 接続の制限とタイムアウト、TCP 正規化など、さまざまな機能の多数のアクションを設定できます。各機能で使用可能なコマンドの詳細については、CLI 設定ガイドを参照してください。
3. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

インターフェイス サービス ポリシーは、特定の機能に対するグローバル サービス ポリシーより優先されます。たとえば、インスペクションのグローバル ポリシーがあり、TCP 正規化のインターフェイス ポリシーがある場合、インターフェイスに対してインスペクションと TCP 正規化の両方が適用されます。ただし、インスペクションのグローバル ポリシーがあり、インスペクションのインターフェイス ポリシーもある場合、そのインターフェイスにはインターフェイス ポリシーのインスペクションのみが適用されます。

デフォルトでは、すべてのデフォルト アプリケーション インスペクション トラフィックに一致するグローバル ポリシーがコンフィギュレーションに含まれ、すべてのインスペクションがトラフィックにグローバルに適用されます。適用できるグローバル ポリシーは 1 つだけなので、グローバル ポリシーを変更する場合は、デフォルトのポリシーを編集するか、デフォルトのポリシーをディセーブルにして新しいポリシーを適用します。

デフォルト サービス ポリシーには、次のコマンドが含まれています。

```
service-policy global_policy global
```

## 例

次に、外部インターフェイスで inbound_policy ポリシー マップをイネーブルにする例を示します。

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

次のコマンドは、デフォルト グローバル ポリシーをディセーブルにし、他のすべての ASA インターフェイスで新しいポリシー new_global_policy をイネーブルにします。

```
ciscoasa(config)# no service-policy global_policy global
ciscoasa(config)# service-policy new_global_policy global
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure service-policy** | サービス ポリシーのコンフィギュレーションをクリアします。 |
| **clear service-policy** | サービス ポリシーの統計情報をクリアします。 |
| **service-policy (class)** | 別のポリシー マップの下に階層型ポリシーを適用します。 |
| **show running-config service-policy** | 実行コンフィギュレーションに設定されているサービス ポリシーを表示します。 |
| **show service-policy** | サービス ポリシーの統計情報を表示します。 |

# service sw-reset-button

ASA 5506-X、5508-X、および 5516-X でリセット ボタンをイネーブルにするには、グローバル コンフィギュレーション モードで **service sw-reset-button** コマンドを使用します。リセット ボタンをディセーブルにするには、このコマンドの **no** 形式を使用します。

**service sw-reset-button**

**no service sw-reset-button**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

**service sw-reset-button** は、デフォルトでイネーブルになっています。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.3(2) | コマンドが追加されました。 |

## 使用上のガイドライン

リセット ボタンは背面パネルにある小さな埋め込み型のボタンです。約 3 秒以上押すと ASA がリセットされ、次のリブート後に「出荷時」のデフォルト状態に戻ります。設定変数が工場出荷時デフォルトにリセットされます。ただし、フラッシュは削除されないため、ファイルは削除されません。

## 例

次に、ソフトウェア リセット ボタンをイネーブルにする例を示します。

```
ciscoasa(config)# service sw-reset-button
ciscoasa(config)# show sw-reset-button

Software Reset Button is configured.
```

次に、ソフトウェア リセット ボタンを無効にする例を示します。

```
ciscoasa(config)# no service sw-reset-button
ciscoasa(config)# show sw-reset-button

Software Reset Button is not configured.
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show running-config service** | サービス コンフィギュレーションを表示します。 |

# サービス テレメトリ

テレメトリ データ サービスが有効になっている場合、デバイス情報、CPU/メモリ/ディスク/帯域幅の使用率、ライセンスの使用状況、設定済み機能リスト、クラスタ/フェールオーバー情報、およびお客様の ASA デバイスに関する同様の情報が、FXOS を介して Cisco Security Services Exchange（SSE）に送信されます。サービスを有効にするには、グローバル コンフィギュレーション モードで **service telemetry** コマンドを使用します。テレメトリ サービスを無効にするには、このコマンドの **no** 形式を使用します。

**service telemetry**

**no service telemetry**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルトでは、サービス テレメトリ コマンドは有効になっています。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.13(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

ASA テレメトリ サービスは、ASA アプリケーションを実行している SSPXRU（FP9300 および FP4100）プラットフォームでサポートされています。

## 例

次に、テレメトリ サービスを有効化する例を示します。

```
ciscoasa(config)# service telemetry
```

次に、テレメトリ サービスを無効化する例を示します。

```
hostname(config)# no service telemetry
```

関連コマンド

| コマンド | 説明 |
| --- | --- |
| **show telemetry** | テレメトリの設定とアクティビティに関連する過去 100 のイベントを表示します。また、最後に送信されたテレメトリ データとサンプルが JSON 形式で表示されます。 |

# session

ASA からモジュール（IPS SSP や CSC SSM など）への Telnet セッションを確立して、モジュール CLI にアクセスするには、特権 EXEC モードで **session** コマンドを使用します。

**session** *id*

## 構文の説明

| | |
|---|---|
| *id* | モジュール ID を指定します。<br>• 物理モジュール：**1**（スロット番号 1 の場合）<br>• ソフトウェア モジュール、ASA FirePOWER：**sfr**<br>• ソフトウェア モジュール、IPS：**ips**<br>• ソフトウェア モジュール、ASA CX：**cxsc** |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが追加されました。 |
| 8.6(1) | IPS SSP ソフトウェア モジュールに対して **ips** モジュール ID が追加されました。 |
| 9.1(1) | ASA CX モジュールのサポートが追加されました（**cxsc** キーワード）。 |
| 9.2(1) | ASA FirePOWER モジュールのサポートが追加されました（**sfr** キーワード）。 |

## 使用上のガイドライン

このコマンドは、モジュールがアップ状態である場合にのみ使用できます。ステート情報については、**show module** コマンドを参照してください。

セッションを終了するには、**exit** と入力するか、または Ctrl+Shift+6 を押してから x キーを押します。

次のハードウェア モジュールでは **session 1** コマンドを使用できないことに注意してください。

- ASA CX
- ASA FirePOWER

## 例

次に、スロット 1 のモジュールへのセッションを確立する例を示します。

```
ciscoasa# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **debug session-command** | セッションのデバッグ メッセージを表示します。 |

# session console

ASA からソフトウェア モジュール（IPS SSP ソフトウェア モジュールなど）への仮想コンソール セッションを確立するには、特権 EXEC モードで **session console** コマンドを使用します。このコマンドは、コントロール プレーンがダウンしているために **session** コマンドを使用して Telnet セッションを確立できない場合に便利です。

**session** *id* **console**

## 構文の説明

| | |
|---|---|
| *id* | モジュール ID を指定します。<br>• ASA FirePOWER モジュール：**sfr**<br>• IPS モジュール：**ips**<br>• ASA CX モジュール：**cxsc**<br>• ASA 5506W-X ワイヤレス アクセス ポイント：**wlan** |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.6(1) | このコマンドが追加されました。 |
| 9.1(1) | ASA CX モジュールのサポートが追加されました（**cxsc** キーワード）。 |
| 9.2(1) | ASA FirePOWER モジュールのサポートが追加されました（**sfr** キーワード）。 |
| 9.4(1) | ASA 5506W-X ワイヤレス アクセス ポイント（**wlan** キーワード）のサポートが追加されました。 |

## 使用上のガイドライン

セッションを終了するには、**Ctrl-Shift-6** を押してから x キーを押します。

このコマンドは、**Ctrl+Shift+6**、x がターミナル サーバのプロンプトに戻るエスケープ シーケンスであるターミナル サーバとともに使用しないでください。**Ctrl+Shift+6**、x は、モジュール コンソールをエスケープし ASA プロンプトに戻るシーケンスでもあります。したがって、この状況でモジュール コンソールを終了しようとすると、代わりにターミナル サーバ プロンプトに戻ります。ASA にターミナル サーバを再接続すると、モジュール コンソール セッションがまだアクティブなままであり、ASA プロンプトに戻ることができません。ASA プロンプトにコンソールを戻すには、直接シリアル接続を使用する必要があります。

代わりに **session** コマンドを使用します。

## 例

次に、IPS モジュールへのコンソール セッションを作成する例を示します。

```
ciscoasa# session ips console

Establishing console session with slot 1
Opening console session with module ips.
Connected to module ips. Escape character sequence is 'CTRL-SHIFT-6 then x'.

sensor login: service
Password: test
```

次に、ワイヤレス アクセス ポイントへのコンソール セッションを作成する例を示します。

```
ciscoasa# session wlan console
opening console session with module wlan
connected to module wlan. Escape character sequence is ‘CTRL-^X’

ap>
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **session** | モジュールへの Telnet セッションを開始します。 |
| **show module log console** | コンソール ログ情報を表示します。 |

# session do

ASA からモジュールへの Telnet セッションを確立し、コマンドを実行するには、特権 EXEC モードで **session do** コマンドを使用します。

**session** *id* **do** *command*

## 構文の説明

| | |
|---|---|
| *id* | モジュール ID を指定します。<br>• 物理モジュール：**1**（スロット番号 1 の場合）<br>• ソフトウェア モジュール、ASA FirePOWER：**sfr**<br>• ソフトウェア モジュール、IPS：**ips**<br>• ソフトウェア モジュール、ASA CX：**cxsc** |
| *command* | モジュールでコマンドを実行します。サポートされるコマンドは次のとおりです。<br>• **setup host ip** *ip_address*/*mask*,*gateway_ip*：管理 IP アドレスおよびゲートウェイを設定します。<br>• **get-config**：モジュール コンフィギュレーションを取得します。<br>• **password-reset**：モジュール パスワードをデフォルトにリセットします。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1(1) | このコマンドが追加されました。 |
| 8.6(1) | IPS SSP ソフトウェア モジュールに対して **ips** モジュール ID が追加されました。 |
| 8.4(4.1) | ASA CX モジュールのサポートが追加されました。 |
| 9.2(1) | **sfr** キーワードを含め、ASA FirePOWER モジュールのサポートが追加されました。 |

## 使用上のガイドライン

このコマンドは、モジュールがアップ状態である場合にのみ使用できます。ステート情報については、**show module** コマンドを参照してください。

セッションを終了するには、**exit** と入力するか、または **Ctrl+Shift+6** を押してから X キーを押します。

## 例

次に、管理 IP アドレスを 10.1.1.2/24 に、デフォルト ゲートウェイを 10.1.1.1 に設定する例を示します。

```
ciscoasa# session 1 do setup host ip 10.1.1.2/24,10.1.1.1
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **debug session-command** | セッションのデバッグ メッセージを表示します。 |

# session ip

モジュール（IPS SSP や CSC SSM など）にロギング IP アドレスを設定するには、特権 EXEC モードで **session ip** コマンドを使用します。

**session** *id* **ip** {**address** *address mask* | **gateway** *address*}

## 構文の説明

| | |
|---|---|
| *id* | モジュール ID を指定します。<br>• 物理モジュール：**1**（スロット番号 1 の場合）<br>• ソフトウェア モジュール、IPS：**ips** |
| **address** *address* | syslog サーバ アドレスを設定します。 |
| **gateway** *address* | ゲートウェイを syslog サーバに設定します。 |
| *mask* | サブネット マスクを設定します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1(1) | このコマンドが追加されました。 |
| 8.4(4.1) | ASA CX モジュールのサポートが追加されました。 |
| 8.6(1) | IPS SSP ソフトウェア モジュールに対して **ips** モジュール ID が追加されました。 |

## 使用上のガイドライン

このコマンドは、モジュールがアップ状態である場合にのみ使用できます。ステート情報については、**show module** コマンドを参照してください。

セッションを終了するには、**exit** と入力するか、または **Ctrl+Shift+6** を押してから X キーを押します。

## 例

次に、スロット 1 のモジュールへのセッションを確立する例を示します。

```
ciscoasa# session 1 ip address
```

関連コマンド

| コマンド | 説明 |
| --- | --- |
| **debug session-command** | セッションのデバッグ メッセージを表示します。 |

# set as-path

BGP ルートの自律システム パスを変更するには、ルートマップ コンフィギュレーション モードで **set as-path** コマンドを使用します。自律システム パスを変更しないようにするには、このコマンドの **no** 形式を使用します。

**set as-path** {**tag** | **prepend** *as-path-string*}

**no set as-path** {**tag** | **prepend** *as-path-string*}

## 構文の説明

| | |
|---|---|
| *as-path-string* | AS_PATH 属性に付加する自律システムの番号。この引数の値の範囲は、1 ～ 65535 の有効な自律システム番号です。複数の値を入力できます。最大 10 個の AS 番号を入力できます。<br>自律システムの番号形式の詳細については、**router bgp** コマンドを参照してください。 |
| **prepend** | ルート マップにより照合されたルートの自律システム パスに、キーワード **prepend** に続いて文字列を付加します。BGP のインバウンド ルート マップおよびアウトバウンド ルート マップに適用します。 |
| **tag** | ルートのタグを自律システム パスに変換します。BGP にルートを再配布するときのみ適用されます。 |

## デフォルト

自律システム パスは変更されません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.2(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

最適なパス選択に影響を与える唯一のグローバル BGP メトリックは、自律システム パス長です。自律システム パスの長さを変えることで、BGP スピーカーは遠くのピアによる最適なパス選択に影響を与えます。

タグを自律システム パスに変換することで、このコマンドの **set as-path tag** のバリエーションにより、自律システム長を変更できます。**set as-path prepend** のバリエーションを使用すれば、任意の自律システム パス文字列を BGP ルートに「付加」できます。通常、ローカルな自律システム番号は複数回追加され、AS パス長が増します。

シスコが採用している 4 バイト自律システム番号では、自律システム番号の正規表現のマッチングおよび出力表示のデフォルトの形式として asplain（たとえば、65538）を使用していますが、RFC 5396 で定義されているとおり、4 バイト自律システム番号を asplain 形式および asdot 形式の両方で設定できます。4 バイト自律システム番号の正規表現マッチングと出力表示のデフォルトを asdot 形式に変更するには、**bgp asnotation dot** コマンドに続けて、**clear bgp *** コマンドを実行し、現在の BGP セッションをすべてハード リセットします。

## 例

次に、再配布されたルートのタグを自律システム パスに変換する例を示します。

```
ciscoasa(config)# route-map set-as-path-from-tag
ciscoasa(config-route-map)# set as-path tag
ciscoasa(config-route-map)# router bgp 100
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# redistribute ospf 109 route-map set-as-path-from-tag
```

次に、10.108.1.1 にアドバタイズされたすべてのルートに 100 100 100 を付加する例を示します。

```
ciscoasa(config)# route-map set-as-path
ciscoasa(config-route-map)# match as-path 1
ciscoasa(config-route-map)# set as-path prepend 100 100 100
ciscoasa(config-route-map)# router bgp 100
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.108.1.1 route-map set-as-path out
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear bgp** | ハードまたはソフトの再設定を使用して BGP 接続をリセットします。 |
| **bgp asnotation dot** | デフォルトの表示を変更し、ボーダー ゲートウェイ プロトコル（BGP）4 バイト自律システム番号の正規表現一致形式を、asplain 形式（10 進数の値）からドット付き表記にします。 |

# set automatic-tag

自動的にタグ値を計算するには、ルートマップ コンフィギュレーション モードで set automatic-tag コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

**set automatic-tag**

**no set automatic-tag**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

このコマンドは、デフォルトでディセーブルになっています。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.2(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

タグを設定する場合は、match 句を使用する必要があります（permit everything を指している場合でも）。

あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義するには、**route-map** グローバル コンフィギュレーション コマンドと、match および set **route-map** コンフィギュレーション コマンドを使用します。**route-map** コマンドごとに、それに関連した match および set コマンドのリストがあります。match コマンドは、一致基準、つまり現在の **route-map** コマンドに再配布が許可される条件を指定します。set コマンドは、set 処理、つまり match コマンドで指定した基準を満たしている場合に実行する特定の再配布アクションを指定します。**no route-map** コマンドは、ルート マップを削除します。

set **route-map** コンフィギュレーション コマンドを使用すると、ルート マップのすべての一致基準が満たされたときに実行される再配布 set 処理を指定します。すべての一致基準を満たすと、すべての set 処理が実行されます。

## 例

次に、ボーダー ゲートウェイ プロトコル（BGP）で学習されたルートのタグ値が自動的に計算されるように Cisco ASA ソフトウェアを設定する例を示します。

```
ciscoasa(config-route-map)# route-map tag
ciscoasa(config-route-map)# match as-path 10
iscoasa(config-route-map)# set automatic-tag
ciscoasa(config-route-map)# router bgp 100
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# table-map tag
```

# set community

BGP コミュニティ属性を設定するには、**set community** ルート マップ コンフィギュレーション コマンドを使用します。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。

**set community** {*community-number* [**additive**] | [*well-known-community*] [**additive**] | **none**}

**no set community**

## 構文の説明

| | |
|---|---|
| **additive** | (オプション)既存のコミュニティにコミュニティを追加します。 |
| *community-number* | そのコミュニティ番号を指定します。有効な値は、1 ～ 4294967200、**no-export**、または **no-advertise** です。 |
| **none** | (オプション)ルート マップを渡すプレフィックスからコミュニティ属性を削除します。 |
| *well-known-community* | (オプション)次のキーワードを使用することにより、ウェルノウン コミュニティを指定できます。<br>• **internet**<br>• **local-as**<br>• **no-advertise**<br>• **no-export** |

## デフォルト

BGP コミュニティ属性は存在しません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.2(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

タグを設定する場合は、match 句を使用する必要があります(「permit everything」リストを指している場合でも)。

あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義するには、route-map グローバル コンフィギュレーション コマンドと、**match** および **set** route-map コンフィギュレーション コマンドを使用します。**route-map** コマンドごとに、それに関連した **match** および **set** コマンドのリストがあります。**match** コマンドは、*一致基準*(現在の **route-map** コマンドで再配布が許可される条件)を指定します。**set** コマンドは、*set 処理*(**match** コマンドによって強制される基準が満たされた場合に実行される特定の再配布アクション)を指定します。**no route-map** コマンドは、ルート マップを削除します。

**set** ルート マップ コンフィギュレーション コマンドは、ルート マップのすべての一致基準が満たされたときに実行される再配布 *set 処理*を指定します。すべての一致基準を満たすと、すべての set 処理が実行されます。

## 例

次の例では、自律システム パス アクセス リスト 1 を通過するルートのコミュニティが 109 に設定されます。自律システム パス アクセス リスト 2 を通過するルートのコミュニティは、no-export(これらのルートがどの eBGP ピアにもアドバタイズされない)に設定されます。

```
ciscoasa(config-route-map)# set community 10
ciscoasa(config-route-map)# match as-path 1
ciscoasa(config-route-map)# set community 109
ciscoasa(config-route-map)# set community 20
ciscoasa(config-route-map)# match as-path 2
ciscoasa(config-route-map)# set community no-export
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **match as-path** | アクセス リストで指定されている BGP 自律システム パスを照合します。 |

# set connection

ポリシー マップ内のトラフィック クラスに対して接続制限を指定するには、クラス コンフィギュレーション モードで **set connection** コマンドを使用します。これらの指定を削除して、無制限の接続数を許可するには、このコマンドの **no** 形式を使用します。

**set connection** {[**conn-max** *n*] [**embryonic-conn-max** *n*] [**per-client-embryonic-max** *n*] [**per-client-max** *n*] [**random-sequence-number** {**enable** | **disable**}]}

**no set connection** {[**conn-max** *n*] [**embryonic-conn-max** *n*] [**per-client-embryonic-max** *n*] [**per-client-max** *n*] [**random-sequence-number** {**enable** | **disable**}]}

## 構文の説明

| | |
|---|---|
| **conn-max** *n* | （TCP、UDP、SCTP）。許可する同時接続の最大数を 0 ～ 2000000 の範囲で設定します。デフォルトは 0 で、この場合は接続数が制限されません。たとえば、同時接続を許可するように 2 つのサーバが設定されている場合、接続制限数は、設定されている各サーバに別々に適用されます。TCP 接続の場合、確立された接続のみに適用されます。<br><br>クラスに設定された場合、この引数では、クラス全体で許可される同時接続最大数が制限されます。この場合、1 つの攻撃ホストがすべての接続を使い果たし、クラスにおいてアクセス リストに一致する他のホストが使用できる接続がなくなる可能性があります。 |
| **embryonic-conn-max** *n* | 許可する同時 TCP 初期接続の最大数を 0 ～ 2000000 の範囲で設定します。デフォルトは 0 で、この場合は接続数が制限されません。 |
| **per-client-embryonic-max** *n* | クライアントごとに許可する同時 TCP 初期接続の最大数を 0 ～ 2000000 の範囲で設定します。クライアントは、ASA から（新規接続を作成する）接続の初期パケットを送信するホストとして定義されます。<br><br>**access-list** が **class-map** とともに使用され、この機能のトラフィックが照合される場合、初期接続制限は、アクセス リストに一致するすべてのクライアントの累積初期接続数ではなく、ホストごとに適用されます。デフォルトは 0 で、この場合は接続数が制限されません。このキーワードは、管理クラス マップでは使用できません。 |
| **per-client-max** *n* | （TCP、UDP、SCTP）。クライアントごとに許可する同時接続最大数を 0 ～ 2000000 の範囲で設定します。クライアントは、ASA から（新規接続を作成する）接続の初期パケットを送信するホストとして定義されます。TCP 接続の場合、これには確立済み接続、ハーフオープン接続、ハーフクローズ接続が含まれます。<br><br>**access-list** が **class-map** とともに使用され、この機能のトラフィックが照合される場合、接続制限は、アクセス リストに一致するすべてのクライアントの累積接続数ではなく、ホストごとに適用されます。デフォルトは 0 で、この場合は接続数が制限されません。<br><br>このキーワードは、管理クラス マップでは使用できません。クラスに設定された場合、このキーワードでは、クラスにおいてアクセス リストに一致する各ホストに許可される同時接続最大数が制限されます。 |

| | |
|---|---|
| **random-sequence-number {enable \| disable}** | TCP シーケンス番号ランダム化をイネーブルまたはディセーブルにします。このキーワードは、管理クラス マップでは使用できません。詳細については、「使用上のガイドライン」を参照してください。 |

## デフォルト

**conn-max**、**embryonic-conn-max**、**per-client-embryonic-max**、および **per-client-max** の各パラメータの *n* のデフォルト値は、0（接続数の制限なし）です。

シーケンス番号ランダム化は、デフォルトでイネーブルです。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが追加されました。 |
| 7.1(1) | **per-client-embryonic-max** キーワードおよび **per-client-max** キーワードが追加されました。 |
| 8.0(2) | このコマンドが、ASA への管理トラフィックにおいて、レイヤ 3/4 管理クラス マップでも使用できるようになりました。**conn-max** キーワードおよび **embryonic-conn-max** キーワードだけが使用可能です。 |
| 9.0(1) | 最大接続数が 65535 から 2000000 に増えました。 |
| 9.5(2) | **conn-max** キーワードと **per-client-max** キーワードが SCTP、TCP および UDP に適用されるようになりました。 |

## 使用上のガイドライン

モジュラ ポリシー フレームワークを使用してこのコマンドを設定します。最初に、**class-map** コマンド（通過トラフィック）または **class-map type management** コマンド（管理トラフィック）を使用して、タイムアウトを適用するトラフィックを定義します。次に、**policy-map** コマンドを入力してポリシーを定義し、**class** コマンドを入力してクラス マップを参照します。クラス コンフィギュレーション モードで、**set connection** コマンドを入力できます。最後に、**service-policy** コマンドを使用して、インターフェイスにポリシー マップを適用します。モジュラ ポリシー フレームワークの仕組みの詳細については、CLI 設定ガイドを参照してください。

(注) ASA モデル上の CPU コア数によっては、同時接続および初期接続の最大数が、各コアによる接続の管理方法が原因で、設定されている数を超える場合があります。最悪の場合、ASA は最大 *n*-1 の追加接続および初期接続を許可します。ここで、*n* はコアの数です。たとえば、モデルに 4 つのコアがあり、6 つの同時接続および 4 つの初期接続を設定した場合は、各タイプで 3 つの追加接続を使用できます。ご使用のモデルのコア数を確認するには、**show cpu core** コマンドを入力します。

### TCP 代行受信の概要

初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。ASA では、クライアントあたりの制限値と初期接続の制限を利用して TCP 代行受信を開始します。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。TCP 代行受信では、SYN クッキー アルゴリズムを使用して TCP SYN フラッディング攻撃を防ぎます。SYN フラッディング攻撃は、通常はスプーフィングされた IP アドレスから送信されてくる一連の SYN パケットで構成されています。SYN パケットのフラッディングが定常的に生じると、SYN キューが一杯になる状況が続き、接続要求に対してサービスを提供できなくなります。接続の初期接続しきい値を超えると、ASA はサーバのプロキシとして動作し、クライアント SYN 要求に対する SYN-ACK 応答を生成します。ASA がクライアントから ACK を受信すると、クライアントを認証し、サーバへの接続を許可できます。

### TCP シーケンスのランダム化

それぞれの TCP 接続には 2 つの ISN が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。ASA は、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。

保護対象のホストの ISN をランダム化することにより、攻撃者が新しい接続に使用される次の ISN を予測して新しいセッションをハイジャックするのを阻止します。

TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。

- 別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。
- ASA で eBGP マルチホップを使用しており、eBGP ピアで MD5 を使用している場合。ランダム化により、MD5 チェックサムは分解されます。
- ASA で接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。

## 例

次に、**set connection** コマンドを使用して、同時接続最大数を 256 に設定し、TCP シーケンス番号ランダム化をディセーブルにする例を示します。

```
ciscoasa(config)# policy-map localpolicy1
ciscoasa(config-pmap)# class local_server
ciscoasa(config-pmap-c)# set connection conn-max 256 random-sequence-number disable
ciscoasa(config-pmap-c)#
```

複数のパラメータを指定してこのコマンドを入力することも、各パラメータを個別のコマンドとして入力することもできます。ASA は、コマンドを実行コンフィギュレーション内で 1 行に結合します。たとえば、クラス コンフィギュレーション モードで次の 2 つのコマンドを入力するとします。

```
ciscoasa(config-pmap-c)# set connection conn-max 600
ciscoasa(config-pmap-c)# set connection embryonic-conn-max 50
```

**show running-config policy-map** コマンドの出力には、2 つのコマンドの結果が単一の結合コマンドとして表示されます。

```
set connection conn-max 600 embryonic-conn-max 50
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **class** | トラフィックの分類に使用するクラス マップを指定します。 |
| **clear configure policy-map** | すべてのポリシー マップ コンフィギュレーションを削除します。ただし、例外として、ポリシー マップが service-policy コマンドで使用されている場合、そのポリシー マップは削除されません。 |
| **policy-map** | ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。 |
| **show running-config policy-map** | 現在のすべてのポリシー マップ コンフィギュレーションを表示します。 |
| **show service-policy** | サービス ポリシー設定を表示します。**set connection** コマンドを含むポリシーを表示するには、**set connection** キーワードを使用します。 |

# set connection advanced-options

接続の詳細設定を行うには、クラス コンフィギュレーション モードで **set connection advanced-options** コマンドを使用します。オプションを削除するには、このコマンドの **no** 形式を使用します。

**set connection advanced-options** {*tcp_mapname* | **tcp-state-bypass** | **sctp-state-bypass** | **flow-offload**}

**no set connection advanced-options** {*tcp_mapname* | **tcp-state-bypass** | **sctp-state-bypass** | **flow-offload**}

## 構文の説明

| | |
|---|---|
| **flow-offload** | ASA からオフロードし、直接 NIC に切り替える対象として、一致するフローを指定します。これにより、データセンターにおける大量のデータ フローのパフォーマンスが向上します。フロー オフロードは、FXOS 1.1.3 以上を稼働する Firepower 9300 シリーズまたは FXOS 1.1.4 以上を稼働する Firepower 4100 シリーズで使用可能です。<br>このオプションを動作させるには、事前にフロー オフロードを有効にしておく必要があります。**flow-offload enable** コマンドを使用します。 |
| **sctp-state-bypass** | SCTP ステート バイパスを実装して、SCTP ステートフル インスペクションを無効にします。SCTP トラフィックはプロトコル準拠かどうかを検証されません。 |
| *tcp_mapname* | **tcp-map** コマンドで作成された TCP マップの名前。TCP 正規化をカスタマイズするには、このオプションを使用します。 |
| **tcp-state-bypass** | ネットワーク内で非対称ルーティングを使用している場合は、TCP ステート チェックをバイパスします。TCP ステート バイパスの使用方法の詳細およびガイドラインについては、後述の「使用上のガイドライン」を参照してください。 |

## デフォルト

デフォルトの動作や値はありません。すべての TCP 正規化オプション（TCP マップ内）にデフォルト設定がありますが、デフォルトで有効になっているオプションはありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが追加されました。 |
| 8.2(1) | **tcp-state-bypass** キーワードが追加されました。 |
| 9.5(2) | **sctp-state-bypass** キーワードが追加されました。 |
| 9.5(2) | **flow-offload** キーワードが追加されました。オプションには、Firepower eXtensible Operating System 1.1.3 以上が必要です。オプションは、Firepower 9300 シリーズで使用可能です。 |
| 9.6(1) | FXOS 1.1.4 以上を稼働する Firepower 4100 シリーズでフロー オフロードのサポートが追加されました。 |

## 使用上のガイドライン

TCP マップを使用して TCP 正規化をカスタマイズするには、モジュラ ポリシー フレームワークを使用します。

1. **tcp-map**：変更する場合は、対象の TCP 正規化アクションを指定します。
2. **class-map**：TCP 正規化アクションを実行するトラフィックを指定します。
3. **policy-map**：クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. **set connection advanced options**：TCP マップまたは別のオプションをクラス マップに適用します。
4. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

### TCP ステート バイパス：個別のデバイスを通過するアウトバウンド フローおよびインバンド フローを許可する

デフォルトで、ASA を通過するすべてのトラフィックは、適応型セキュリティ アルゴリズムを使用して検査され、セキュリティ ポリシーに基づいて許可またはドロップされます。ASA では、各パケットの状態（新規接続であるか、または確立済み接続であるか）がチェックされ、そのパケットをセッション管理パス（新規接続の SYN パケット）、ファスト パス（確立済みの接続）、またはコントロール プレーン パス（高度なインスペクション）に割り当てることによって、ファイアウォールのパフォーマンスが最大化されます。

高速パスの既存の接続に一致する TCP パケットは、セキュリティ ポリシーのあらゆる面の再検査を受けることなく ASA を通過できます。この機能によってパフォーマンスは最大になります。ただし、SYN パケットを使用してファスト パスにセッションを確立する方法、およびファスト パスで行われるチェック（TCP シーケンス番号など）が、非対称ルーティング ソリューションの障害となる場合があります。これは、接続の発信フローと着信フローの両方が同じ ASA を通過する必要があるためです。

たとえば、ある新しい接続が ASA 1 に開始されるとします。SYN パケットはセッション管理パスを通過し、接続のエントリが高速パス テーブルに追加されます。この接続の後続のパケットが ASA 1 を通過する場合、パケットは高速パスのエントリと一致して、通過します。しかし、後続のパケットが ASA 2 に到着すると、SYN パケットがセッション管理パスを通過していないために、高速パスにはその接続のエントリがなく、パケットはドロップされます。

アップストリーム ルータに非対称ルーティングが設定されており、トラフィックが 2 つの ASA を通過することがある場合は、特定のトラフィックに対して TCP ステート バイパスを設定できます。TCP ステート バイパスは、高速パスでのセッションの確立方法を変更し、高速パスのインスペクションをディセーブルにします。この機能では、UDP 接続の処理と同様の方法で TCP トラフィックが処理されます。指定されたネットワークと一致した非 SYN パケットが ASA に入った時点で高速パス エントリが存在しない場合、高速パスで接続を確立するために、そのパケットはセッション管理パスを通過します。いったん高速パスに入ると、トラフィックは高速パスのインスペクションをバイパスします。

### TCP ステート バイパスでサポートされていない機能

TCP ステート バイパスを使用するときは、次の機能はサポートされません。

- アプリケーション検査:アプリケーション検査では、着信および発信トラフィックの両方が同じ ASA を通過する必要があるため、TCP ステート バイパスではアプリケーション検査はサポートされません。
- AAA 認証セッション:ユーザがある ASA で認証される場合、他の ASA 経由で戻るトラフィックは、その ASA でユーザが認証されていないため、拒否されます。
- TCP 代行受信、最大初期接続制限、TCP シーケンス番号ランダム化:ASA では接続の状態が追跡されないため、これらの機能は適用されません。
- TCP 正規化:TCP ノーマライザはディセーブルです。
- SSM 機能:TCP ステート バイパスと、IPS や CSC などの SSM 上で実行されるアプリケーションを使用することはできません。

### TCP ステート バイパスの NAT のガイドライン

変換セッションは ASA ごとに個別に確立されるので、TCP ステート バイパス トラフィック用に両方の ASA でスタティック NAT を設定してください。ダイナミック NAT を使用すると、ASA 1 でのセッションに選択されるアドレスが、ASA 2 でのセッションに選択されるアドレスと異なります。

### TCP ステート バイパスの接続タイムアウトのガイドライン

リリース 9.10(1) 以降、特定の接続に 2 分間トラフィックがない場合、接続はタイムアウトします。このデフォルトは、**set connection timeout idle** コマンドを使用して上書きできます。通常の TCP 接続は、デフォルトで 60 分後にタイムアウトします。9.10(1) よりも前のリリースでは、TCP ステートバイパス接続で 60 分間のグローバルタイムアウト値を使用します。

## 例

次に、**set connection advanced-options** コマンドを使用して、localmap という名前の TCP マップの使用を指定する例を示します。

```
ciscoasa(config)# access-list http-server permit tcp any host 10.1.1.1
ciscoasa(config)# class-map http-server
ciscoasa(config-cmap)# match access-list http-server
ciscoasa(config-cmap)# exit
ciscoasa(config)# tcp-map localmap
ciscoasa(config)# policy-map global_policy global
ciscoasa(config-pmap)# description This policy map defines a policy concerning connection
to http server.
ciscoasa(config-pmap)# class http-server
ciscoasa(config-pmap-c)# set connection advanced-options localmap
ciscoasa(config-pmap-c)#
```

次に、TCP ステート バイパスのコンフィギュレーション例を示します。

```
ciscoasa(config)# access-list tcp_bypass extended permit tcp 10.1.1.0 255.255.255.224 any

ciscoasa(config)# class-map tcp_bypass
ciscoasa(config-cmap)# description "TCP traffic that bypasses stateful firewall"
ciscoasa(config-cmap)# match access-list tcp_bypass

ciscoasa(config-cmap)# policy-map tcp_bypass_policy
ciscoasa(config-pmap)# class tcp_bypass
ciscoasa(config-pmap-c)# set connection advanced-options tcp-state-bypass

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

次に、SCTP ステート バイパスの設定例を示します。

```
ciscoasa(config)# access-list sctp_bypass extended permit sctp
10.1.1.0 255.255.255.224 any

ciscoasa(config)# class-map sctp_bypass
ciscoasa(config-cmap)# description "SCTP traffic that bypasses stateful inspection"
ciscoasa(config-cmap)# match access-list sctp_bypass

ciscoasa(config-cmap)# policy-map sctp_bypass_policy
ciscoasa(config-pmap)# class sctp_bypass
ciscoasa(config-pmap-c)# set connection advanced-options sctp-state-bypass

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

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **class** | ポリシー マップにクラス マップを指定します。 |
| **class-map** | サービス ポリシーで使用するクラス マップを作成します。 |
| **flow-offload** | フロー オフロードを有効にします。 |
| **policy-map** | クラス マップと 1 つ以上のアクションを関連付けるポリシー マップを設定します。 |
| **service-policy** | インターフェイスにポリシー マップを割り当てます。 |
| **set connection timeout** | 接続タイムアウトを設定します。 |
| **show running-config policy-map** | 現在のポリシー マップ コンフィギュレーションをすべて表示します。 |
| **tcp-map** | TCP マップを作成します。 |

# set connection decrement-ttl

ポリシー マップ内のトラフィック クラスにおいて存続可能時間の値をデクリメントするには、クラス コンフィギュレーション モードで **set connection decrement-ttl** コマンドを使用します。存続可能時間をデクリメントしない場合は、このコマンドの **no** 形式を使用します。

**set connection decrement-ttl**

**no set connection decrement-ttl**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルトで、ASA では、存続可能時間はデクリメントされません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2(2) | このコマンドが追加されました。 |

## 使用上のガイドライン

このコマンド、および **icmp unreachable** コマンドは、ASA をホップの 1 つとして表示する ASA 経由の traceroute を可能とするために必要です。

パケット存続時間（TTL）をデクリメントすると、TTL が 1 のパケットはドロップされますが、接続に TTL がより大きいパケットを含むと想定されるセッションでは、接続が開かれます。OSPF hello パケットなどの一部のパケットは TTL = 1 で送信されるため、パケット存続時間（TTL）をデクリメントすると、予期しない結果が発生する可能性があります。

## 例

次の例では、存続時間のデクリメントをイネーブルにして、ICMP 到達不能レート制限を設定します。

```
ciscoasa(config)# policy-map localpolicy1
ciscoasa(config-pmap)# class local_server
ciscoasa(config-pmap-c)# set connection decrement-ttl
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# icmp unreachable rate-limit 50 burst-size 6
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **class** | トラフィック分類に使用するクラス マップを指定します。 |
| **icmp unreachable** | ICMP 到達不能メッセージが ASA を通過可能なレートを制御します。 |
| **policy-map** | ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。 |
| **show running-config policy-map** | 現在のポリシー マップ コンフィギュレーションをすべて表示します。 |
| **show service-policy** | サービス ポリシー設定を表示します。 |

# set connection timeout

ポリシー マップ内のトラフィック クラスに対して接続タイムアウトを指定するには、クラス コンフィギュレーション モードで **set connection timeout** コマンドを使用します。タイムアウトを削除するには、このコマンドの **no** 形式を使用します。

**set connection timeout** {[**embryonic** *hh*:*mm*:*ss*] [**idle** *hh*:*mm*:*ss* [**reset**]] [**half-closed** *hh*:*mm*:*ss*] [**dcd** [*retry_interval* [*max_retries*]]]}

**no set connection timeout** {[**embryonic** *hh*:*mm*:*ss*] [**idle** *hh*:*mm*:*ss* [**reset**]] [**half-closed** *hh*:*mm*:*ss*] [**dcd** [*retry_interval* [*max_retries*]]]}

## 構文の説明

| | |
|---|---|
| **dcd** [*retry_interval* [*max_retries*]] | デッド接続検出（DCD）をイネーブルにします。DCD では、デッド接続を検出して、トラフィックをまだ処理できる接続を期限切れにすることなく、そのデッド接続を期限切れにすることができます。DCD は、アイドル状態でも有効な接続を維持する場合に設定します。TCP 接続がタイムアウトすると、ASA は、エンドホストに DCD プローブを送信して接続の有効性を判断します。最大再試行回数を超えてもエンドホストの一方が応答しない場合、ASA はその接続を解放します。両方のエンドホストが応答して接続の有効性が確認されると、ASA はアクティビティ タイムアウトを現在時刻に更新し、それに応じてアイドル タイムアウトを再スケジュールします。<br><br>トランスペアレント ファイアウォール モードで動作している場合、エンドポイントにスタティック ルートを設定する必要があります。バージョン 9.13(1) 以前では、クラスタ内で DCD を使用できません。<br><br>次のオプション値を設定できます。<br><br>• *retry_interval*：DCD プローブに応答がない場合に次のプローブを送信するまでの *hh*:*mm*:*ss* 形式の間隔を 0:0:1 ～ 24:0:0 の範囲で指定します。デフォルト値は 0:0:15 です。<br><br>クラスタまたは高可用性構成で動作しているシステムでは、間隔を 1 分（0:1:0）未満に設定しないことを推奨します。接続をシステム間で移動する必要がある場合、必要な変更には 30 秒以上かかり、変更が行われる前に接続が削除される場合があります。<br><br>• *max_retries*：接続が無活動状態であると宣言するまでに失敗する DCD の連続再試行回数を設定します。最小値は 1、最大値は 255 です。デフォルトは 5 分です。 |
| **embryonic** *hh*:*mm*:*ss* | TCP 初期（ハーフオープン）接続が閉じられるまでのタイムアウト期間を 0:0:5 ～ 1193:0:0 の範囲で設定します。デフォルト値は 0:0:30 です。値を 0 に設定することもできます。これは、接続がタイムアウトになることはないことを意味します。初期接続とは、スリーウェイ ハンドシェイクが完了していない TCP 接続です。 |
| **half-closed** *hh*:*mm*:*ss* | ハーフクローズ接続が閉じられるまでのアイドル タイムアウト期間を、9.1(1) 以前の場合は 0:5:0 ～ 1193:0:0 の範囲、9.1(2) 以降の場合は 0:0:30 ～ 1193:0: 0 の範囲で設定します。デフォルト値は 0:10:0 です。値を 0 に設定することもできます。これは、接続がタイムアウトになることはないことを意味します。ハーフクローズの接続は DCD の影響を受けません。また、ASA は、ハーフクローズ接続を切断するときにリセット パケットを送信しません。 |

| | |
|---|---|
| **idle** *hh*:*mm*:*ss* | 任意のプロトコルの確立済み接続が閉じられるまでのアイドル タイムアウト期間を設定します。有効な範囲は 0:0:1 ～ 1193:0:0 です。 |
| **reset** | TCP トラフィックに対してのみ、アイドル接続が削除された後に両方のエンド システムに対して TCP RST パケットを送信します。 |

## デフォルト

timeout コマンドを使用してデフォルトをグローバルに変更していない場合、デフォルトは次のとおりです。

- デフォルトの **embryonic** タイムアウトは 30 秒です。
- デフォルトの **half-closed** アイドル タイムアウトは 10 分です。
- デフォルトの **dcd** *max_retries* の値は 5 です。
- デフォルトの **dcd** *retry_interval* の値は 15 秒です。
- デフォルトの **idle** タイムアウトは 1 時間です。
- デフォルトの **udp** アイドル タイムアウトは 2 分です。
- デフォルトの **icmp** アイドル タイムアウトは 2 秒です。
- デフォルトの **esp** および **ha** アイドル タイムアウトは 30 秒です。
- その他すべてのプロトコルでは、デフォルトのアイドル タイムアウトは 2 分です。
- タイムアウトにならないようにするには、0:0:0 を入力します。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが追加されました。 |
| 7.2(1) | DCD のサポートが追加されました。 |
| 8.2(2) | **tcp** キーワードが、すべてのプロトコルのアイドル タイムアウトを制御する **idle** に代わって廃止されました。 |
| 9.1(2) | 最小 **half-closed** 値が 30 秒(0:0:30)に引き下げられました。 |
| 9.13(1) | DCD の設定は、クラスタで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

モジュラ ポリシー フレームワークを使用してこのコマンドを設定します。最初に、**class-map** コマンドを使用して、タイムアウトを適用するトラフィックを定義します。次に、**policy-map** コマンドを入力してポリシーを定義し、**class** コマンドを入力してクラス マップを参照します。クラス コンフィギュレーション モードで、**set connection timeout** コマンドを入力できます。最後に、**service-policy** コマンドを使用して、インターフェイスにポリシー マップを適用します。モジュラ ポリシー フレームワークの仕組みの詳細については、CLI 設定ガイドを参照してください。

**show service-policy** コマンドには、DCD からのアクティビティ量を示すためのカウンタが含まれます。

## 例

次に、すべてのトラフィックの接続タイムアウトを設定する例を示します。

```
ciscoasa(config)# class-map CONNS
ciscoasa(config-cmap)# match any
ciscoasa(config-cmap)# policy-map CONNS
ciscoasa(config-pmap)# class CONNS
ciscoasa(config-pmap-c)# set connection timeout idle 2:0:0 embryonic 0:40:0 half-closed
0:20:0 dcd
ciscoasa(config-pmap-c)# service-policy CONNS interface outside
```

複数のパラメータを使用して **set connection** コマンドを入力するか、各パラメータを別々のコマンドとして入力できます。ASA は、コマンドを実行コンフィギュレーション内で 1 行に結合します。たとえば、クラス コンフィギュレーション モードで次の 2 つのコマンドを入力するとします。

```
ciscoasa(config-pmap-c)# set connection timeout idle 2:0:0
ciscoasa(config-pmap-c)# set connection timeout embryonic 0:40:0
```

この場合、**show running-config policy-map** コマンドの出力には、2 つのコマンドの結果が次の単一の結合コマンドとして表示されます。

```
set connection timeout idle 2:0:0 embryonic 0:40:0
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **class** | トラフィックの分類に使用するクラス マップを指定します。 |
| **clear configure policy-map** | すべてのポリシー マップ コンフィギュレーションを削除します。ただし、ポリシー マップが service-policy コマンド内で使用されている場合、そのポリシー マップは削除されません。 |
| **policy-map** | ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。 |
| **set connection** | 接続の値を設定します。 |
| **show running-config policy-map** | 現在のポリシー マップ コンフィギュレーションをすべて表示します。 |
| **show service-policy** | DCD およびその他のサービス アクティビティのカウンタを表示します。 |

# set default interface

**set interface** コマンドを **default** オプションとともに使用した場合、一致するトラフィックをルーティングするための最初の試行は、明示ルートをルックアップすることで、通常のルートルックアップを介して実行されなければなりません。通常のルートルックアップに失敗した場合のみ、PBR が指定されたインターフェイスを使用してトラフィックを転送します。その後、「デフォルト」でトリガーされたルックアップと、インターフェイス オプションでトリガーされたルックアップはどちらも、宛先への明示ルートの存在に依存します。「デフォルト」ルックアップは常に成功します。「デフォルト」ルックアップが失敗した場合は、宛先への明示ルートがないことを意味しています。そのため、インターフェイス アクションは適用できません。「set default interface」が設定されている場合は、「Null0」のみをインターフェイスとして設定できます。このオプションが設定されており、通常のルート ルックアップで宛先への明示ルート（デフォルト以外のルート）が判明しない場合、トラフィックはドロップされます。

**set default interface Null0**

**no set default interface Null0**

## 構文の説明

| | |
|---|---|
| *interface* | パケットの転送先インターフェイス。 |

## デフォルト

このコマンドにはデフォルトはありません。set 処理として、Null0 インターフェイスが指定されている必要があります。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.4(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

このコマンドを使用すると、特定のユーザに異なるデフォルト ルートを提供します。Cisco ASA が宛先への明示ルートを持たない場合、パケットはこのインターフェイスにルーティングされます。set default interface コマンドでアップとして指定された最初のインターフェイスが使用されます。オプションで指定されたインターフェイスは、次に試行されます。

ポリシー ルーティング パケットに関する条件を定義するには、**ip policy route-map** インターフェイス コンフィギュレーション コマンド、**route-map** グローバル コンフィギュレーション コマンド、match および set route-map コンフィギュレーション コマンドを使用します。**ip policy route-map** コマンドは、名前でルート マップを識別します。route-map コマンドごとに、それに関連した match および set コマンドのリストがあります。**match** コマンドは、一致基準（ポリシー ルーティングが発生する条件）を指定します。**set** コマンドは、set 処理（match コマンドによって強制される基準が満たされた場合に実行される特定のルーティング アクション）を指定します。

IPv6 対応の PBR で、ポリシー ルーティング パケットに関する条件を定義するには、match および set route-map コンフィギュレーション コマンドとともに、**ipv6 policy route-map** または **ipv6 local policy route-map** コマンドを使用します。

set 句は互いに組み合わせて使用できます。set 句は次の順で評価されます。

1. set ip next-hop
2. set interface
3. set ip default next-hop
4. set default interface

## 例

```
(config)# route-map testmap
(config-route-map)# set default interface Null0
(config)# show run route-map
!
route-map testmap permit 10
  set default interface Null0
!
(config)# show route-map testmap
route-map testmap, permit, sequence 10
   Match clauses:
   Set clauses:
                default interface Null0
```

# set dscp

**set dscp** コマンドは、一致する IP パケットの QoS ビットを設定するために使用されます。

**set ip dscp {0-63 | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef }**

**no set ip dscp**

**set ipv6 dscp {0-63 | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef }**

**no set ipv6 dscp**

## 構文の説明

| | |
|---|---|
| 0 ～ 63 | DSCP 値の数値範囲。 |
| af | 相対的優先転送クラス |
| ef | 緊急転送 |
| デフォルト | |
| cs | |

## デフォルト

ToS バイトの DSCP 値は設定されません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.4(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

DSCP ビットを設定すると、他の Quality of Service（QoS）機能がビット設定で動作するようになります。

### 相互に排他的な DSCP と precedence

set dscp コマンドを set precedence コマンドとともに使用して同じパケットをマークすることはできません。2 つの値（DSCP および precedence）は相互に排他的です。パケットにはどちらか一方の値を設定でき、両方を設定することはできません。

### precedence の値とキューイング

マーキングされたトラフィックには、ネットワークによってプライオリティ（または緊急処理のタイプ）が設定されます。通常は、ネットワーク エッジ（または管理ドメイン）で Precedence 値を設定します。データは、precedence に従ってキューイングされます。重み付け均等化キューイング（WFQ）で、輻輳ポイントでの優先順位の高いトラフィックの処理を高速化できます。Weighted Random Early Detection（WRED; 重み付けランダム早期検出）により、輻輳時の優先順位の高いトラフィックの損失率を他のトラフィックより確実に小さくできます。

### 「from-field」パケットマーキング カテゴリの使用

このコマンドを、拡張パケット マーキング機能の一部として使用すると、DSCP 値のマッピングと設定に使用される「from-field」パケットマーキング カテゴリを指定できます。「from-field」パケットマーキング カテゴリは次のとおりです。

- サービス クラス（CoS）
- QoS group

「from-field」カテゴリを指定したが、table キーワードと適用可能な table-map-name 引数を指定していない場合、デフォルト アクションは、「from-field」カテゴリに関連付けられた値を DSCP 値としてコピーすることです。たとえば、set dscp cos コマンドを設定する場合、CoS 値がコピーされ、DSCP 値として使用されます。

（注） CoS フィールドは 3 ビット フィールドで、DSCP フィールドは 6 ビット フィールドです。set dscp cos コマンドを設定する場合、CoS フィールドの 3 ビットのみが使用されます。

**set dscp qos-group** コマンドを設定する場合、QoS グループ値がコピーされ、DSCP 値として使用されます。

DSCP の有効値の範囲は 0 ～ 63 の数字です。QoS グループの有効値の範囲は 0 ～ 99 です。したがって、set dscp qos-group コマンドを設定する場合、次の点に注意してください。

- QoS グループの値が両方の値の範囲（たとえば、44）にある場合、packet-marking 値がコピーされ、パケットがマーク付けされます。
- QoS グループの値が DSCP の範囲を超える場合（たとえば、77）、packet-marking 値はコピーされず、パケットはマーク付けされません。アクションは実行されません。

### IPv6 環境での DSCP 値の設定

このコマンドを IPv6 環境で使用すると、デフォルトで IP パケットと IPv6 パケットの両方が照合されます。ただし、この機能によって設定される実際のパケットは、この機能を含むクラスマップの一致基準に合致するパケットのみです。

### IPv6 パケットのみに対する DSCP 値の設定

IPv6 値のみの DSCP 値を設定するには、match protocol ipv6 コマンドを使用する必要があります。このコマンドがない場合、precedence 一致では、デフォルトで、IPv4 パケットと IPv6 パケットの両方で一致が発生します。

### IPv4 パケットのみに対する DSCP 値の設定

IPv4 値のみの DSCP 値を設定するには、適切な match ip コマンドを使用する必要があります。このコマンドを使用しないと、他の一致基準に応じて、クラス マップが IPv6 パケットと IPv4 パケットの両方に合致し、DSCP 値が両方のタイプのパケットで機能することがあります。

## 例

```
(config)# route-map testmapv4
(config-route-map)# set ip dscp af22
(config)# show run route-map
!
route-map testmapv4 permit 10
  set ip dscp af22
!
(config)# show route-map testmapv4
route-map testmapv4, permit, sequence 10
   Match clauses:
   Set clauses:
                ip dscp af22
(config)# route-map testmapv6
(config-route-map)# set ipv6 dscp cs6
(config)# show run route-map
!
route-map testmapv6 permit 10
  set ipv6 dscp cs6
!
(config)# show route-map testmap
route-map testmap, permit, sequence 10
   Match clauses:
   Set clauses:
                ipv6 dscp cs6
```

# set ikev1 transform-set

IPsec プロファイルに IPsec IKEv1 プロポーザルを指定するには、IPsec プロファイル コンフィギュレーション モードで **set ikev1 transform-set** コマンドを使用します。IPsec IKEv1 プロポーザルを削除するには、このコマンドの **no** 形式を使用します。

**set ikev1 transform-set** *transform-set name*

**no set ikev1 transform-set** *transform-set name*

## 構文の説明

| | |
|---|---|
| *transform-set name* | IPsec IKEv1 プロポーザルの名前を指定します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | トランスペアレント | シングル | コンテキスト | システム |
| IPsec プロファイル設定 | • あり | • なし | • あり | • なし | • - |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.7(1) | このコマンドが追加されました。 |

## 例

次に、IPsec プロファイルに IKEv1 プロポーザルを指定する例を示します。

```
ciscoasa(config)# crypto ipsec profile VTIipsec
ciscoasa(config-ipsec-profile)# set ikev1 transform-set
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **crypto ipsec profile** | 新しい IPsec プロファイルを作成します。 |
| **responder-only** | VTI トンネル インターフェイスをレスポンダ専用モードに設定します。 |
| **set pfs** | PFS グループを IPsec プロファイル設定に使用するように指定します。 |
| **set security-association lifetime** | IPsec プロファイル設定でのセキュリティ アソシエーションの期間を指定します。これは、キロバイト単位か秒単位、またはその両方で指定します。 |
| **set trustpoint** | VTI トンネル接続の開始時に使用する証明書を定義するトラストポイントを指定します。 |

# set interface

**set interface** コマンドは、一致するトラフィックを転送する際に経由する必要があるインターフェイスを設定するために使用されます。パケットの転送先として有効な稼働中のインターフェイスが見つかるまで、指定された順序でインターフェイスが評価される場合は、複数のインターフェイスを設定できます。インターフェイス名を Null0 として指定すると、ルート マップに一致するトラフィックはすべてドロップされます。

**set interface [...***interface***]**

**no set interface [...***interface***]**

## 構文の説明

| | |
|---|---|
| *interface* | パケットの転送先インターフェイス。 |

## デフォルト

コマンドのデフォルト値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.4(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

ポリシー ルーティング パケットに関する条件を定義するには、**ip policy route-map** インターフェイス コンフィギュレーション コマンド、route-map グローバル コンフィギュレーション コマンド、match および set route-map コンフィギュレーション コマンドを使用します。**ip policy route-map** コマンドは、名前でルート マップを識別します。route-map コマンドごとに、それに関連した match および set コマンドのリストがあります。match コマンドは、一致基準（ポリシー ルーティングが発生する条件）を指定します。set コマンドは、set 処理（match コマンドによって強制される基準が満たされた場合に実行される特定のルーティング アクション）を指定します。

IPv6 対応の PBR で、ポリシー ルーティング パケットに関する条件を定義するには、match および **set route-map** コンフィギュレーション コマンドとともに、**ipv6 policy route-map** または **ipv6 local policy route-map** コマンドを使用します。

set interface コマンドで指定された最初のインターフェイスがダウン状態になると、オプションで指定されたインターフェイスが順番に試行されます。

set 句は互いに組み合わせて使用できます。set 句は次の順で評価されます。

1. set ip next-hop
2. set interface
3. set ip default next-hop
4. set default interface

有用なネクスト ホップはインターフェイスで暗黙指定されます。ネクスト ホップとインターフェイスが見つかるとすぐに、そのパケットがルーティングされます。

## 例

```
ciscoasa(config)# route-map testmap
ciscoasa(config-route-map)# set interface outside
ciscoasa(config)# show run route-map
!
route-map testmap permit 10
  set interface outside
!
ciscoasa(config)# show route-map testmap
route-map testmap, permit, sequence 10
   Match clauses:
   Set clauses:
                interface outside
```

# set ip df

**set ip df** コマンドは、一致する IP パケットに df（do-not-fragment）ビットを設定するために使用されます。

**set ip df [0|1]**

**no set ip df**

## 構文の説明

| | |
|---|---|
| 0 | df ビットを 0 に設定（df ビットをクリア）して、パケット フラグメンテーションを許可します。 |
| 1 | df ビットを 1 に設定して、パケット フラグメンテーションを禁止します。 |

## デフォルト

このコマンドにはデフォルトはありません。set 処理で、0 または 1 のいずれかを df ビットとして指定する必要があります。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.4(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

パス MTU 検出（PMTUD）を使用して、フラグメンテーションを回避する IP パケットの MTU 値を決定できます。ICMP メッセージがルータによってブロックされると、パス MTU は破棄され、df ビットが設定されたパケットは廃棄されます。set ip df コマンドを使用して df ビットをクリアし、パケットのフラグメンテーションと送信を許可します。フラグメンテーションによって、ネットワーク上のパケット転送速度が低下する場合がありますが、アクセス リストを使用して、df ビットがクリアされるパケット数を制限できます。

**（注）** df ビットが設定されている場合、一部の IP トランスミッタ（特に Linux のいくつかのバージョン）が、IP ヘッダーの ID フィールド（IPid）をゼロに設定することがあります。ルータがこのようなパケットの df ビットをクリアする場合やそのパケットがその後フラグメント化される場合には、IP レシーバは、おそらく元の IP パケットに正常にリアセンブルすることができません。

## 例

```
(config)# route-map testmap
(config-route-map)# set ip df 1
(config)# show run route-map
!
route-map testmap permit 10
  set ip df 1
!
(config)# show route-map testmap
route-map testmap, permit, sequence 10
   Match clauses:
   Set clauses:
                ip df 1
```

# set ip default next-hop

**set ip next-hop** コマンドを **default** オプションとともに使用した場合、一致するトラフィックをルーティングするための最初の試行は、明示ルートをルックアップすることで、通常のルートルックアップを介して実行されなければなりません。通常のルートルックアップが失敗した場合のみ、ポリシー ベース ルーティング（PBR）は、指定されたネクスト ホップ IP アドレスを使用してトラフィックを転送します。

**set ip default next-hop** *ip-address* [*... ip-address*]

**no set ip default next-hop** *ip-address* [*... ip-address*]

**set default ipv6next-hop** *ip-address* [**...** *ip-address*]

**no set default ipv6 next-hop** *ip-address* [**...** *ip-address*]

## 構文の説明

| | |
|---|---|
| *ip-address* | パケットが出力される出力先ネクスト ホップの IP アドレス。隣接ルータである必要はありません。 |
| *ipv6-address* | パケットが出力されるネクスト ホップの IPv6 アドレス。隣接ルータである必要はありません。 |

## デフォルト

このコマンドはデフォルトでは無効になっています。set 処理には、1 つ以上のネクストホップ IP アドレスを指定する必要があります。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.4(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

このコマンドを使用すると、特定のユーザに異なるデフォルト ルートを提供します。ソフトウェアがパケットの宛先への明示ルートを持たない場合、パケットは次のネクスト ホップにルーティングされます。**set ip default next-hop** コマンドで指定された最初のネクスト ホップはルータに隣接している必要があります。次に、オプションの IP アドレスが使用されます。

ポリシー ルーティング パケットに関する条件を定義するには、ip policy route-map インターフェイス コンフィギュレーション コマンド、route-map グローバル コンフィギュレーション コマンド、match および set route-map コンフィギュレーション コマンドを使用します。ip policy route-map コマンドは、名前でルート マップを識別します。route-map コマンドごとに、それに関連した match および set コマンドのリストがあります。match コマンドは、一致基準（ポリシー ルーティングが発生する条件）を指定します。set コマンドは、set 処理（match コマンドによって強制される基準が満たされた場合に実行される特定のルーティング アクション）を指定します。

**set next-hop** コマンドで指定された最初のネクスト ホップがダウン状態になると、任意で指定された IP アドレスが使用されます。

set 句は互いに組み合わせて使用できます。set 句は次の順で評価されます。

1. **set next-hop**
2. **set interface**
3. **set default next-hop**
4. **set default interface**

（注） set ip next-hop と set ip default next-hop は類似のコマンドですが、操作順が異なります。set ip next-hop コマンドを設定すると、最初にポリシー ルーティングを使用してからルーティング テーブルを使用します。set ip default next-hop コマンドを設定すると、最初にルーティング テーブルを使用してから指定のネクスト ホップをポリシー ルーティングします。

## 例

```
(config)# route-map testmapv4
(config-route-map)# set ip default next-hop 1.1.1.1
(config)# show run route-map
!
route-map testmapv4 permit 10
  set ip default next-hop 1.1.1.1
!
(config)# show route-map testmapv4
route-map testmapv4, permit, sequence 10
Match clauses:
Set clauses:
ip default next-hop 1.1.1.1
(config)# route-map testmapv6
(config-route-map)# set ipv6 default next-hop 2001::1
(config)# show run route-map
!
route-map testmapv6 permit 10
  set ipv6 default next-hop 2001::1
!
(config)# show route-map testmapv6
route-map testmapv6, permit, sequence 10
Match clauses:
Set clauses:
ipv6 default next-hop 2001::1
```

# set ip next-hop

ポリシー ルーティングにおいてルート マップの match 句を通過するパケットの出力先を示すには、ルートマップ コンフィギュレーション モードで **set ip next-hop** コマンドを使用します。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。

**set ip next-hop** *ip-address* [*... ip-address*] [**peer-address**]

**no set ip next-hop** *ip-address* [**...** *ip-address*] [**peer-address**]

**set ipv6 next-hop**

## 構文の説明

| | |
|---|---|
| *ip-address* | パケットが出力される出力先ネクスト ホップの IP アドレス。隣接ルータである必要はありません。 |
| **peer-address** | （オプション）ネクスト ホップを BGP ピア アドレスに設定します。 |

## デフォルト

このコマンドは、デフォルトでディセーブルになっています。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.2(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

コマンド構文の省略記号（...）は、コマンド入力で *ip-address* 引数に複数の値を含めることができることを示します。

ポリシー ルーティング パケットに関する条件を定義するには、**ip policy route-map** インターフェイス コンフィギュレーション コマンド、**route-map** グローバル コンフィギュレーション コマンド、**match** および **set** コンフィギュレーション コマンドを使用します。**ip policy route-map** コマンドは、名前でルート マップを識別します。**route-map** コマンドごとに、それに関連した **match** および **set** コマンドのリストがあります。**match** コマンドは、*一致基準*（ポリシー ルーティングが発生する条件）を指定します。**set** コマンドは、*set 処理*（**match** コマンドによって強制される基準が満たされた場合に実行される特定のルーティング アクション）を指定します。

**set next-hop** コマンドで指定された最初のネクスト ホップがダウン状態になると、任意で指定された IP アドレスが使用されます。

BGP ピアのインバウンド ルート マップで **peer-address** キーワードを指定し、**set next-hop command** コマンドを使用すると、受信した一致するルートのネクスト ホップをネイバー ピア アドレスに設定し、サードパーティのネクスト ホップを上書きします。したがって、同じルート マップを複数の BGP ピアに適用すると、サードパーティのネクストホップを上書きできます。

BGP ピアのアウトバウンド ルート マップで **peer-address** キーワードを指定し、**set next-hop** コマンドを使用すると、アドバタイズされた一致するルートのネクスト ホップをローカル ルータのピア アドレスに設定し、ネクスト ホップ計算をディセーブルにします。他のルートではなく、一部のルートにネクスト ホップを設定できるので、**set next-hop** コマンドは、（ネイバー単位の）**neighbor next-hop-self** コマンドよりも詳細に設定できます。**neighbor next-hop-self** コマンドは、そのネイバーに送信されたすべてのルートにネクスト ホップを設定します。

set 句は互いに組み合わせて使用できます。set 句は次の順で評価されます。

1. **set next-hop**
2. **set interface**
3. **set default next-hop**
4. **set default interface**

（注） 反映されたルートの一般的な設定エラーを回避するために、BGP ルート リフレクタ クライアントに適用するルート マップで **set next-hop** コマンドを使用しないでください。

## 例

次の例では、3 台のルータが同じ LAN 上にあります（IP アドレス 10.1.1.1, 10.1.1.2 および 10.1.1.3）。それぞれが異なる自律システム（AS）です。**set ip next-hop peer-address** コマンドは、ルート マップと一致する、リモート自律システム 100 内のルータ（10.1.1.3）からリモート自律システム 300 内のルータ（10.1.1.1）へのトラフィックが、LAN への相互接続上で自律システム 100 内のルータ（10.1.1.1）に直接送信されるのではなく、ルータ bgp 200 を通過するように指定します。

```
ciscoasa(config)# router bgp 200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.1.1.3 remote-as 300
ciscoasa(config-router-af)# neighbor 10.1.1.3 route-map set-peer-address out
ciscoasa(config-router-af)# neighbor 10.1.1.1 remote-as 100
ciscoasa(config-route-af)# route-map set-peer-address permit 10
ciscoasa(config-route-map)# set ip next-hop peer-address
```

# set ip next-hop recursive

**set ip next-hop** と **set ip default next-hop** はどちらも、ネクストホップが直接接続されたサブネット上に存在している必要があります。**set ip next-hop recursive** では、ネクストホップ アドレスが直接接続されている必要はありません。代わりにネクストホップ アドレスで再帰ルックアップが実行され、一致するトラフィックは、ルータで使用されているルーティング パスに従って、そのルート エントリで使用されているネクストホップに転送されます。

ネクストホップの再帰ルックアップは、IPv6 に対して、またはデフォルト キーワードが指定されている場合には、適用できません。

**set ip next-hop recursive** [*ipv4-address*]

**no set ip next-hop recursive** [*ipv4-address*]

## 構文の説明

| | |
|---|---|
| *ipv4-address* | パケットが出力される出力先ネクスト ホップの IP アドレス。隣接ルータである必要はありません。 |

## デフォルト

このコマンドは、デフォルトでディセーブルになっています。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.4(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

ポリシー ルーティング パケットに関する条件を定義するには、**ip policy route-map** インターフェイス コンフィギュレーション コマンド、route-map グローバル コンフィギュレーション コマンド、match および set route-map コンフィギュレーション コマンドを使用します。ip policy route-map コマンドは、名前でルート マップを識別します。route-map コマンドごとに、それに関連した match および set コマンドのリストがあります。match コマンドは、一致基準（ポリシー ルーティングが発生する条件）を指定します。set コマンドは、set 処理（match コマンドによって強制される基準が満たされた場合に実行される特定のルーティング アクション）を指定します。

set ip next-hop コマンドで指定された最初のネクスト ホップに関連付けられたインターフェイスがダウン状態になると、オプションで指定された IP アドレスが順番に試行されます。

set 句は互いに組み合わせて使用できます。set 句は次の順で評価されます。

1. set ip next-hop
2. set interface
3. set ip default next-hop
4. set default interface

（注） **set ip next-hop** と **set ip default next-hop** は類似のコマンドですが、操作順が異なります。set ip next-hop コマンドを設定すると、最初にポリシー ルーティングを使用してからルーティング テーブルを使用します。set ip default next-hop コマンドを設定すると、最初にルーティング テーブルを使用してから指定のネクスト ホップをポリシー ルーティングします。

例

```
(config)# route-map testmapv4
(config-route-map)# set ip next-hop recursive 1.1.1.1
(config)# show run route-map
!
route-map testmapv4 permit 10
  set ip next-hop recursive 1.1.1.1
!
(config)# show route-map testmapv4
route-map testmapv4, permit, sequence 10
   Match clauses:
   Set clauses:
                ip next-hop recursive 1.1.1.1
```

# set ip next-hop verify-availability

**set ip next-hop verify-availability** は、ネクストホップの到達可能性を確認するために、SLA モニタ トラッキング オブジェクトとともに設定できます。複数のネクストホップの可用性を確認するために、複数の **set ip next-hop verify-availability** コマンドを異なるシーケンス番号と異なるトラッキング オブジェクトで設定できます。

**set ip next-hop verify-availability** [*sequence number*] **track** [*tracked-object-number*]

**no set ip next-hop verify-availability** [*sequence number*] **track** [*tracked-object-number*]

## 構文の説明

| | |
|---|---|
| *sequence-number* | ネクスト ホップのシーケンス。指定できる範囲は 1 ～ 65535 です。 |
| **track** | トラッキング方式はトラックです。 |
| *tracked-object-number* | トラッキング サブシステムが追跡しているオブジェクト数。指定できる範囲は 1 ～ 500 です。 |

## デフォルト

コマンドのデフォルト値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.4(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

set ip next-hop verify-availability コマンドは、次の 2 とおりの方法で使用できます。

- ネクスト ホップの到達可能性を確認するための Cisco Discovery Protocol（CDP）を使用したポリシーベース ルーティング（PBR）。
- リモート デバイスが到達可能であるかどうか確認するために Internet Control Message Protocol（ICMP）ping または HTTP GET リクエストを使用してオブジェクト トラッキングをサポートするオプションの引数。

### CDP 検証の使用方法

このコマンドは、ルータがポリシー ルーティングを試みる前に、ネクスト ホップが到達可能であることを確認するために使用されます。このコマンドには次のような特長があります。

- パフォーマンスが若干低下します。
- CDP がインターフェイスに設定されている必要があります。
- ネクスト ホップは、CDP が有効なシスコ デバイスである必要があります。
- プロセス スイッチングと Cisco Express Forwarding（CEF）ポリシー ルーティングでサポートされていますが、CDP ネイバー データベースの依存関係のため、分散型 CEF（dCEF）では利用できません。

ルータがパケットをネクスト ホップにポリシー ルーティングしていて、ネクスト ホップがダウンしている場合、ルータがネクスト ホップ（ダウン中）に対して Address Resolution Protocol（ARP）を使用しようとして失敗します。この動作はいつまでも続きます。この状況の発生を防ぐには、set ip next-hop verify-availability コマンドを使用して、そのネクスト ホップにルーティングする前に、ルート マップのネクスト ホップが CDP ネイバーであることを確認するようにルータを設定します。

いくつかのメディアまたはカプセル化は CDP をサポートしていない、またはルータにトラフィックを送信しているのがシスコ デバイスではない場合があるため、このコマンドはオプションです。

このコマンドが設定され、ネクスト ホップが CDP ネイバーではない場合、ルータは次のネクスト ホップ（存在する場合）を検索します。ネクスト ホップがない場合は、パケットはポリシー ルーティングされません。

このコマンドが設定されていない場合、パケットは正常にポリシー ルーティングされるか、または永続的にルーティングされないままになります。

いくつかのネクストホップのみの可用性を選択的に確認する場合、異なる基準（アクセス リストの照合またはパケット サイズの照合を使用）で異なるルート マップ エントリ（同じルート マップ名）を設定してから、選択的に set ip next-hop verify-availability コマンドを使用することもできます。

### オブジェクト トラッキングの使用方法

オブジェクト トラッキングをサポートするオプションの引数とともに、このコマンドを使用すると、PBR は次の基準に基づいて決定を下すことができます。

- リモート デバイスへの ICMP ping の到達可能性。
- リモート デバイスで稼働中のアプリケーション（たとえば、デバイスが HTTP GET リクエストに応答する）。
- ルーティング情報ベース（RIB）に存在するルート（たとえば、10.2.2.0/24 が RIB に存在する場合のみ、ポリシー ルーティングする）。
- インターフェイスの状態（たとえば、E0 で受信されたパケットは E2 がダウンしている場合のみ、E1 にポリシー ルーティングする必要がある）。

オブジェクト トラッキングは次のように機能します。PBR は、特定のオブジェクトのトラッキングを対象としていることをトラッキング プロセスに通知します。トラッキング プロセスは、そのオブジェクトの状態が変化したときに、それを PBR に通知します。この通知はレジストリを介して行われ、イベント駆動型です。

トラッキング サブシステムは、オブジェクトの状態をトラッキングする役割を担います。オブジェクトには、トラッキング プロセスによって定期的に ping が実行される IP アドレスを指定できます。オブジェクトの状態（アップまたはダウン）は、トラック レポート データ構造に保存されます。トラッキング プロセスは、トラッキング オブジェクト レポートを作成します。次に、ルート マップを設定している exec プロセスが、所定のオブジェクトが存在するかどうかを判別するために、トラッキング プロセスにクエリできます。オブジェクトが存在する場合、トラッキング サブシステムはトラッキングを開始し、オブジェクトの初期状態を読み取ります。オブジェクトの状態が変化すると、トラッキング プロセスはオブジェクトの状態が変わったことを、このプロセスをトラッキングしているすべてのクライアントに通知します。そのため、PBR が使用しているルート マップ構造は、トラック レポート内のオブジェクトの現在の状態を反映して更新できます。このプロセス間通信は、レジストリと共有トラック レポートを使用して実行されます。

**（注）** CDP およびオブジェクト トラッキング コマンドを混在させると、トラッキングされているネクスト ホップが最初に試行されます。

## 例

```
ciscoasa(config)# sla monitor 1
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 1.1.1.1 interface outside
ciscoasa(config)# sla monitor schedule 1 life forever start-time now
ciscoasa(config)# track 1 rtr 1 reachability
ciscoasa(config)#
ciscoasa(config)# route-map testmapv4
ciscoasa(config-route-map)# set ip next-hop verify-availability 1.1.1.1 10 track 1
ciscoasa(config)# show run route-map
!
route-map testmapv4 permit 10
  set ip next-hop verify-availability 1.1.1.1 10 track 1
!
ciscoasa(config)# show route-map testmap
route-map testmapv4, permit, sequence 10
   Match clauses:
   Set clauses:
               ip next-hop verify-availability 1.1.1.1 10 track 1
```

# set local-preference

自律システム パスのプリファレンス値を指定するには、ルートマップ コンフィギュレーション モードで set local-preference コマンドを使用します。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。

**set local-preference** *number-value*

**no set local-preference** *number-value*

## 構文の説明

| | |
|---|---|
| *number-value* | プリファレンス値。0 ～ 4294967295 の整数。 |

## デフォルト

プリファレンス値は 100 です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.2(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

プリファレンスは、ローカル自律システム内のすべてのルータにのみ送信されます。

あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義するには、**route-map** グローバル コンフィギュレーション コマンドと、match および set **route-map** コンフィギュレーション コマンドを使用します。**route-map** コマンドごとに、それに関連した match および set コマンドのリストがあります。match コマンドは、一致基準、つまり現在の **route-map** コマンドに再配布が許可される条件を指定します。set コマンドは、set 処理、つまり match コマンドで指定した基準を満たしている場合に実行する特定の再配布アクションを指定します。**no route-map** コマンドは、ルート マップを削除します。

set **route-map** コンフィギュレーション コマンドを使用すると、ルート マップのすべての一致基準が満たされたときに実行される再配布 set 処理を指定します。すべての一致基準を満たすと、すべての set 処理が実行されます。

**bgp default local-preference** コマンドを使用して、デフォルトのプリファレンス値を変更できます。

## 例

次に、アクセス リスト 1 に含まれるすべてのルートに対して、ローカル プリファレンスを 100 に設定する例を示します。

```
ciscoasa(config-route-map)# route-map map-preference
ciscoasa(config-route-map)# match as-path 1
ciscoasa(config-route-map)# set local-preference 100
```

# set metric

ルート マップ内の OSPF およびその他のダイナミック ルーティング プロトコルのルートのメトリック値を設定するには、ルートマップ コンフィギュレーション モードで **set metric** コマンドを使用します。OSPF およびその他のダイナミック ルーティング プロトコルのメトリック値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

**set metric** *metric-value* | [***bandwidth delay reliability loading mtu***]

**no set metric** *metric-value* | [***bandwidth delay reliability loading mtu***]

## 構文の説明

| | |
|---|---|
| *帯域幅* | ルートの EIGRP 帯域幅（kbps）。有効値の範囲は、0 ～ 4294967295 です。 |
| *delay* | EIGRP ルート遅延（10 マイクロ秒単位）。有効値の範囲は、0 ～ 4294967295 です。 |
| *loading* | 0 ～ 255 の数値で表される、ルートの有効な EIGRP 帯域幅。値 255 は、100 % のロードを意味します。 |
| *metric-value* | 数値で表される、OSPF およびその他のダイナミック ルーティング プロトコル（EIGRP 以外）のルートのメトリック値。有効値の範囲は、0 ～ 4294967295 です。 |
| *mtu* | EIGRP のルートの最小 MTU サイズ（バイト単位）。有効値の範囲は、0 ～ 4294967295 です。 |
| *信頼性* | 0 ～ 255 の数値で表される、EIGRP のパケット伝送の成功確率。値 255 は 100 % の信頼性を意味し、0 は信頼性がないことを意味します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが追加されました。 |
| 8.2(5) | ルート マップで EIGRP をサポートするために、*bandwidth*、*delay*、*reliability*、*loading*、および *mtu* 引数が追加されました。 |
| 9.0(1) | マルチ コンテキスト モードのサポートが追加されました。 |

## 使用上のガイドライン

**no set metric** コマンドを使用すると、OSPF およびその他のダイナミック ルーティング プロトコルのメトリック値をデフォルトに戻すことができます。このコンテキストでは、*metric-value* 引数は 0 ～ 4294967295 の整数です。

## 例

次に、OSPF ルーティングのルート マップを設定する例を示します。

```
ciscoasa(config)# route-map maptag1 permit 8
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# match metric 5
ciscoasa(config-route-map)# show route-map
route-map maptag1 permit 8
set metric 5
match metric 5
```

次に、ルート マップ内の EIGRP のメトリック値を設定する例を示します。

```
ciscoasa(config)# access-list route-out line 1 standard permit 10.1.1.0 255.255.255.0
ciscoasa(config)# route-map rmap permit 10
ciscoasa(config-route-map)# set metric 10000 60 100 1 1500
ciscoasa(config-route-map)# show route-map rmap
route-map rmap, permit, sequence 10
  Match clauses:
    ip address (access-lists): route-out
  Set clauses:
    metric 10000 60 100 1 1500
ciscoasa(config-route-map)# show running-config route-map
route-map rmap permit 10
 match ip address route-out
 set metric 10000 60 100 1 1500
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **match interface** | 指定したいずれかのインターフェイスの外部にネクスト ホップを持つルートを配布します。 |
| **match ip next-hop** | 指定したアクセス リストのいずれかによって渡されるネクスト ホップ ルータ アドレスを持つルートを配布します。 |
| **route-map** | あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義します。 |

# set metric-type

OSPF メトリック ルートのタイプを指定するには、ルート マップ コンフィギュレーション モードで **set metric-type** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**set metric-type**{**type-1** | **type-2**}

**no set metric-type**

## 構文の説明

| | |
|---|---|
| **type-1** | 指定された自律システムの外部にある OSPF メトリック ルートのタイプを指定します。 |
| **type-2** | 指定された自律システムの外部にある OSPF メトリック ルートのタイプを指定します。 |

## デフォルト

デフォルトは、**type-2** です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが追加されました。 |
| 9.0(1) | マルチ コンテキスト モードのサポートが追加されました。 |

## 例

次に、OSPF ルーティングのルート マップを設定する例を示します。

```
ciscoasa(config)# route-map maptag1 permit 8
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# match metric 5
ciscoasa(config-route-map)# set metric-type type-2
ciscoasa(config-route-map)# show route-map
route-map maptag1 permit 8
  set metric 5
  set metric-type type-2
  match metric 5
ciscoasa(config-route-map)# exit
ciscoasa(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **match interface** | 指定したいずれかのインターフェイスの外部にネクスト ホップを持つ、すべてのルートを配布します。 |
| **route-map** | あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義します。 |
| **set metric** | ルート マップの宛先ルーティング プロトコルのメトリック値を指定します。 |

# set metric-type internal

ネクスト ホップの内部ゲートウェイ プロトコル（IGP）のメトリックと照合するために外部 BGP（eBGP）ネイバーにアドバタイズされたプレフィックスに Multi Exit Discriminator（MED）を設定するには、ルートマップ コンフィギュレーション モードで **set metric-type internal** コマンドを使用します。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。

**set metric-type internal**

**no set metric-type internal**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.2(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

このコマンドを指定すると、BGP はルートのネクスト ホップと関連付けられた IGP メトリックに対応する MED 値をアドバタイズします。このコマンドは、生成された内部 BGP（iBGP）生成ルートおよび eBGP 生成ルートに適用されます。

このコマンドを使用すると、共通の自律システム内の複数の BGP スピーカーが 1 つの特定のプレフィックスに対して異なる MED 値をアドバタイズできます。また、IGP メトリックが変更された場合、BGP によって 10 分ごとにルートが再アドバタイズされることに注意してください。

あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義するには、**route-map** グローバル コンフィギュレーション コマンドと、**match** および **set** route-map コンフィギュレーション コマンドを使用します。**route-map** コマンドごとに、それに関連した **match** および **set** コマンドのリストがあります。**match** コマンドは、*一致基準*（現在の **route-map** コマンドで再配布が許可される条件）を指定します。**set** コマンドは、*set 処理*（**match** コマンドによって強制される基準が満たされた場合に実行される特定の再配布アクション）を指定します。**no route-map** コマンドは、ルート マップを削除します。

**set** route-map コンフィギュレーション コマンドは、ルート マップのすべての一致基準が満たされたときに実行される再配布 *set 処理*を指定します。すべての一致基準を満たすと、すべての set 処理が実行されます。

(注) このコマンドは、ボーダー ゲートウェイ プロトコル（BGP）へのルートの再配布ではサポートされていません。

## 例

次に、ネイバー 172.16.2.3 へのすべてのアドバタイズ済みルートの MED 値を、ネクスト ホップの対応する IGP メトリックに設定する例を示します。

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 172.16.0.0
ciscoasa(config-router-af)# neighbor 172.16.2.3 remote-as 200
ciscoasa(config-router-af)# neighbor 172.16.2.3 route-map setMED out
ciscoasa(config-route-map)# route-map setMED permit 10
ciscoasa(config-route-map)# match as-path as-path-acl
ciscoasa(config-route-map)# set metric-type internal
ciscoasa(config-route-map)# ip as-path access-list as-path-acl permit .*
```

# set origin

BGP 送信元コードを設定するには、ルートマップ コンフィギュレーション モードで **set origin** コマンドを使用します。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。

**set origin** {**igp** | **egp** *autonomous-system-number* | **incomplete**}

**no set origin** {**igp** | **egp** *autonomous-system-number* | **incomplete**}

## 構文の説明

| | |
|---|---|
| *autonomous-system-number* | リモート自律システム番号。この引数の値の範囲は、1 ～ 65535 の有効な自律システム番号です。 |
| **egp** | 外部ゲートウェイ プロトコル(EGP)のローカル システム。 |
| **igp** | 内部ゲートウェイ プロトコル(IGP)のリモート システム。 |
| **incomplete** | 不明な継承。 |

## デフォルト

ルートの起点は、メイン IP ルーティング テーブルのルートのパス情報に基づいています。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.2(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

ルートの起点を設定する場合は、match 句を使用する必要があります(「permit everything」リストを指している場合でも)。ルートを BGP に再配布するときの特定の起点を設定するには、このコマンドを使用します。ルートが再配布されると、通常、起点は incomplete として記録され、BGP テーブルでは ? で示されます。

あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義するには、**route-map** グローバル コンフィギュレーション コマンドと、**match** および **set** route-map コンフィギュレーション コマンドを使用します。**route-map** コマンドごとに、それに関連した **match** および **set** コマンドのリストがあります。**match** コマンドは、*一致基準*(現在の **route-map** コマンドで再配布が許可される条件)を指定します。**set** コマンドは、*set 処理*(**match** コマンドによって強制される基準が満たされた場合に実行される特定の再配布アクション)を指定します。**no route-map** コマンドは、ルート マップを削除します。

**set** route-map コンフィギュレーション コマンドは、ルート マップのすべての一致基準が満たされたときに実行される再配布 *set 処理*を指定します。すべての一致基準を満たすと、すべての set 処理が実行されます。

## 例

次に、ルート マップを IGP に送信するルートの発信を設定する例を示します。

```
ciscoasa(config-route-map)# route-map set_origin
ciscoasa(config-route-map)# match as-path 10
ciscoasa(config-route-map)# set origin igp
```

# set pfs

IPsec プロファイルに PFS グループを指定するには、IPsec プロファイル コンフィギュレーション モードで **set pfs** コマンドを使用します。PFS グループを削除するには、このコマンドの **no** 形式を使用します。

**set pfs** *Diffie-Hellman group* [**group14**]

**no set pfs** *Diffie-Hellman group* [**group14**]

## 構文の説明

| | |
|---|---|
| *Diffie-Hellman グループ* | *Diffie-Hellman group (dh group)* の名前を指定します。 |
| **group14** | IPsec で新しい Diffie-Hellman 交換を実行するときに、2048 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | トランスペアレント | シングル | コンテキスト | システム |
| IPsec プロファイル設定 | • あり | • なし | • あり | • なし | • - |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.7(1) | このコマンドが追加されました。 |
| 9.13(1) | グループ 14 のサポートが追加されました。**group2** および **group5** コマンド オプションは廃止され、以降のリリースで削除されます。 |

## 例

次に、group14 を pfs として設定する例を示します。

```
ciscoasa(config)# crypto ipsec profile VTIipsec
ciscoasa(config-ipsec-profile)# set pfs group14
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **crypto ipsec profile** | 新しい IPsec プロファイルを作成します。 |
| **responder-only** | VTI トンネル インターフェイスをレスポンダ専用モードに設定します。 |
| **set ikev1 transform-set** | IKEv1 変換セットを IPsec プロファイル設定に使用するように指定します。 |

| コマンド | 説明 |
|---|---|
| **set security-association lifetime** | IPsec プロファイル設定でのセキュリティ アソシエーションの期間を指定します。これは、キロバイト単位か秒単位、またはその両方で指定します。 |
| **set trustpoint** | VTI トンネル接続の開始時に使用する証明書を定義するトラストポイントを指定します。 |

# set security-association lifetime

IPsec プロファイル設定でセキュリティ アソシエーションの期間を指定するには、IPsec プロファイル コンフィギュレーション モードで **set security-association lifetime** コマンドを使用します。これは、キロバイト単位か秒単位、またはその両方で指定します。セキュリティ アソシエーションのライフタイム設定を削除するには、このコマンドの **no** 形式を使用します。

**set security-association lifetime** {**seconds** *number* | **kilobytes** {*number* | **unlimited**}}

**no set security-association lifetime** {**seconds** *number* | **kilobytes** {*number* | **unlimited**}}

## 構文の説明

| | |
|---|---|
| **kilobytes** {*number* \| **unlimited**} | 所定のセキュリティ アソシエーションの有効期限が切れるまでに、そのセキュリティ アソシエーションを使用してピア間を通過できるトラフィックの量を KB 単位で指定します。指定できる範囲は 10 ～ 2147483647 KB です。グローバル デフォルトは 4,608,000 キロバイトです。<br>この設定は、リモート アクセス VPN 接続には適用されません。サイト間 VPN のみに適用されます。 |
| **seconds** *number* | セキュリティ アソシエーションの有効期限が切れるまでの存続時間（秒数）を指定します。指定できる範囲は 120 ～ 214783647 秒です。グローバルのデフォルトは 28,800 秒（8 時間）です。<br>この設定は、リモート アクセスとサイト間 VPN の両方に適用されます。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | トランスペアレント | シングル | コンテキスト | システム |
| IPsec プロファイル設定 | • あり | • なし | • あり | • なし | • - |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.7(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

クリプト マップのセキュリティ アソシエーションは、グローバル ライフタイムに基づいてネゴシエートされます。

IPsec セキュリティ アソシエーションでは、共有秘密キーが使用されます。これらのキーとセキュリティ アソシエーションは、両方同時にタイムアウトになります。

特定のクリプト マップ エントリでライフタイム値が設定されている場合、ASA は、セキュリティ アソシエーションのネゴシエート時に新しいセキュリティ アソシエーションを要求するときに、ピアへの要求でクリプト マップ ライフタイム値を指定し、これらの値を新しいセキュリティ アソシエーションのライフタイムとして使用します。ASA は、ピアからネゴシエーション要求を受信すると、ピアが指定するライフタイム値またはローカルに設定されたライフタイム値のうち、小さい方を新しいセキュリティ アソシエーションのライフタイムとして使用します

サイト間 VPN 接続の場合、「時間指定」と「トラフィック量」の 2 つのライフタイムがあります。これらのライフタイムのいずれかに最初に到達すると、セキュリティ アソシエーションが期限切れになります。リモート アクセス VPN セッションでは、指定時刻ライフタイムのみが適用されます。

(注) ASA では、クリプト マップ、ダイナミック マップ、および IPsec 設定を動作中に変更できます。設定を変更する場合、変更によって影響を受ける接続のみが ASA によって停止させられます。たとえば、アクセス リスト内のエントリを削除して、クリプト マップに関連付けられた既存のアクセス リストを変更した場合、関連する接続だけがダウンします。アクセス リスト内の他のエントリに基づく接続は、影響を受けません。

## 例

次に、セキュリティ アソシエーションの有効期間の値を設定する例を示します。

```
ciscoasa(config)# crypto ipsec profile VTIipsec
ciscoasa(config-ipsec-profile)# set security-association lifetime seconds 120 kilobytes
10000
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **crypto ipsec profile** | 新しい IPsec プロファイルを作成します。 |
| **responder-only** | VTI トンネル インターフェイスをレスポンダ専用モードに設定します。 |
| **set ikev1 transform-set** | IKEv1 変換セットを IPsec プロファイル設定に使用するように指定します。 |
| **set pfs** | PFS グループを IPsec プロファイル設定に使用するように指定します。 |
| **set trustpoint** | VTI トンネル接続の開始時に使用する証明書を定義するトラストポイントを指定します。 |

# set trustpoint

VTI トンネル接続の開始時に使用する証明書を定義するトラストポイントを指定するには、IPsec プロファイル コンフィギュレーション モードで **set trustpoint** コマンドを使用します。トラストポイントの設定を削除するには、このコマンドの **no** 形式を使用します。

**set trustpoint** *name* **chain**

**no set trustpoint** *name* **chain**

## 構文の説明

| | |
|---|---|
| *name* | トラストポイントの名前を指定します。 |
| **chain** | 証明書チェーンの送信を有効にします。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | トランスペアレント | シングル | コンテキスト | システム |
| IPsec プロファイル設定 | • あり | • なし | • あり | • なし | • - |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.8(1) | このコマンドが追加されました。 |

## 例

次に、セキュリティ アソシエーションの有効期間の値を設定する例を示します。

```
ciscoasa(config)# crypto ipsec profile VTIipsec
ciscoasa(config-ipsec-profile)# set trustpoint TPVTI chain
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **crypto ipsec profile** | 新しい IPsec プロファイルを作成します。 |
| **responder-only** | VTI トンネル インターフェイスをレスポンダ専用モードに設定します。 |
| **set ikev1 transform-set** | IKEv1 変換セットを IPsec プロファイル設定に使用するように指定します。 |
| **set pfs** | PFS グループを IPsec プロファイル設定に使用するように指定します。 |

# setup

対話形式のプロンプトを使用して ASA の最小限度のコンフィギュレーションを設定するには、グローバル コンフィギュレーション モードで **setup** コマンドを入力します。

セットアップ

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが追加されました。 |
| 8.4(1) | ASA 5510 以降のルーテッド モードでは、設定されたインターフェイスは、「inside」インターフェイスではなく管理*スロット/ポート*インターフェイスになりました。ASA 5505 の場合、設定されたインターフェイスは「inside」インターフェイスではなく VLAN 1 インターフェイスです。 |
| 9.0(1) | デフォルト コンフィギュレーション プロンプトが変更され、セットアップ プロセスを終了するための Ctrl + Z がイネーブルになりました。 |

## 使用上のガイドライン

フラッシュ メモリにスタートアップ コンフィギュレーションがない場合は、起動時にセットアップ プロンプトが自動的に表示されます。

**setup** コマンドによって、ASDM 接続を確立するための最小コンフィギュレーションが順を追って示されます。このコマンドは、コンフィギュレーションがないか、コンフィギュレーションが部分的にしかないユニット向けに設計されたものです。工場出荷時のコンフィギュレーションをサポートするモデルを使用している場合は、**setup** コマンドではなく工場出荷時のコンフィギュレーションを使用することを推奨します(デフォルトのコンフィギュレーションに戻すには、**configure factory-default** コマンドを使用します)。

**setup** コマンドには、「management」という名前が付けられたインターフェイスが必要です。

**setup** コマンドを入力すると、表 1-1 の情報の入力を求められます。表示されたパラメータにコンフィギュレーションがすでに存在する場合は、そのコンフィギュレーションが角カッコで囲まれて表示されるため、その値をデフォルトとして受け入れるか、または新しい値を入力してその値を上書きできます。使用可能なプロンプトは、モデルによって異なる場合があります。システムの **setup** コマンドには、これらのプロンプトのサブセットが含まれています。

*表 1-1　設定プロンプト*

| プロンプト | 説明 |
|---|---|
| `Pre-configure Firewall now through interactive prompts [yes]?` | **yes** または **no** を入力します。**yes** と入力すると、セットアップが続行されます。**no** を入力すると、セットアップが停止し、グローバル コンフィギュレーション プロンプト（ciscoasa(config)#）が表示されます。 |
| `Firewall Mode [Routed]:` | **routed** または **transparent** を入力します。 |
| `Enable password:` | イネーブル パスワードを入力します（パスワードは、3 文字以上である必要があります）。 |
| `Allow password recovery [yes]?` | **yes** または **no** を入力します。 |
| `Clock (UTC):` | このフィールドには何も入力できません。UTC 時間がデフォルトで使用されます。 |
| `Year:` | 4 桁の年（2005 など）を入力します。年の範囲は 1993 ～ 2035 です。 |
| `Month:` | 月名の先頭の 3 文字（9 月の場合は **Sep** など）を使用して月を入力します。 |
| `Day:` | 日付（1 ～ 31）を入力します。 |
| `Time:` | 時間、分、および秒を 24 時間形式で入力します。たとえば、午後 8 時 54 分 44 秒の場合は、**20:54:44** と入力します。 |
| `Host name:` | コマンドライン プロンプトに表示するホスト名を入力します。 |
| `Domain name:` | ASA を稼働するネットワークのドメイン名を入力します。 |
| `IP address of host running Device Manager:` | ASDM にアクセスする必要があるホストの IP アドレスを入力します。 |
| `Use this configuration and save to flash (yes)?` | **yes** または **no** を入力します。**yes** を入力すると、内部インターフェイスがイネーブルになり、要求されたコンフィギュレーションがフラッシュ パーティションに書き込まれます。<br>**no** を入力すると、セットアップ プロンプトが、最初の質問から繰り返されます。<br>`Pre-configure Firewall now through interactive prompts [yes]?`<br>セットアップを終了する場合は **Ctrl + Z** を入力し、プロンプトを繰り返す場合は **yes** を入力します。 |

## 例

次に、**setup** コマンドを完了する例を示します。

```
ciscoasa(config)# setup
Pre-configure Firewall now through interactive prompts [yes]? yes
Firewall Mode [Routed]: routed
Enable password [<use current password>]: writer
Allow password recovery [yes]? yes
```

```
Clock (UTC):
   Year: 2005
   Month: Nov
   Day: 15
   Time: 10:0:0
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: tech_pubs
Domain name: example.com
IP address of host running Device Manager: 10.1.1.1

The following configuration will be used:
Enable password: writer
Allow password recovery: yes
Clock (UTC): 20:54:44 Sep 17 2005
Firewall Mode: Routed
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: tech_pubs
Domain name: example.com
IP address of host running Device Manager: 10.1.1.1

Use this configuration and write to flash? yes
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **configure factory-default** | デフォルトのコンフィギュレーションに戻します。 |

# set weight

ルーティング テーブルの BGP 重みを指定するには、ルートマップ コンフィギュレーション モードで **set weight** コマンドを使用します。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。

**set weight** *number*

**no set weight** *number*

## 構文の説明

| | |
|---|---|
| *number* | 重み値。0 ～ 65535 の範囲の整数に設定できます。 |

## デフォルト

重みは指定のルート マップによって変更されません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.2(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

実行された重みは、最初に一致した自律システム（AS）パスに基づいています。自律システム パスが一致したときに表示された重みは、グローバルな **neighbor** コマンドによって割り当てられた重みを上書きします。つまり、**set weight** route-map コンフィギュレーション コマンドで割り当てられた重みは、**neighbor weight** コマンドを使用して割り当てられた重みを上書きします。

## 例

次に、自律システム パス アクセス リストと一致するルートの BGP 重みを 200 に設定する例を示します。

```
ciscoasa(config-route-map)# route-map set-weight
ciscoasa(config-route-map)# match as-path as_path_acl
iscoasa(config-route-map)# set weight 200
```

# sfr

トラフィックを ASA FirePOWER モジュールにリダイレクトするには、クラス コンフィギュレーション モードで **sfr** コマンドを使用します。リダイレクトを削除するには、このコマンドの **no** 形式を使用します。

**sfr** {**fail-close** | **fail-open**} [**monitor-only**]

**no sfr** {**fail-close** | **fail-open**} [**monitor-only**]

## 構文の説明

| | |
|---|---|
| **fail-close** | モジュールが使用できない場合にトラフィックをブロックするように ASA を設定します。 |
| **fail-open** | モジュールが使用できない場合に、ASA ポリシーのみを適用してトラフィックの通過を許可するように ASA を設定します。 |
| **monitor-only** | トラフィックの読み取り専用コピーをモジュールに送信します(パッシブ モード)。キーワードを指定しない場合、トラフィックはインライン モードで送信されます。 |

## コマンド デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.2(1) | このコマンドが追加されました。 |

## 使用上のガイドライン

クラス コンフィギュレーション モードにアクセスするには、policy-map コマンドを入力します。

ASA に **sfr** コマンドを設定する前または後に、Firepower Management Centerを使用してモジュールにセキュリティ ポリシーを設定します。

**sfr** コマンドを設定するには、まず、**class-map** コマンド、**policy-map** コマンド、および **class** コマンドを設定する必要があります。

### トラフィック フロー

ASA FirePOWER モジュールは、ASA から個別のアプリケーションを実行します。ただし、そのアプリケーションは ASA のトラフィック フローに統合されます。ASA でトラフィックのクラスに対して **sfr** コマンドを適用すると、次のように、トラフィックは ASA およびモジュールを経由します。

1. トラフィックは ASA に入ります。
2. 着信 VPN トラフィックが復号化されます。
3. ファイアウォール ポリシーが適用されます。
4. バックプレーンを介して ASA FirePOWER モジュールにトラフィックが送信されます。
5. モジュールはそのセキュリティ ポリシーをトラフィックに適用し、適切なアクションを実行します。
6. インライン モードでは、有効なトラフィックがバックプレーンを介して ASA に返送されます。ASA FirePOWER モジュールがセキュリティ ポリシーに従ってトラフィックをブロックすることがあり、そのトラフィックは渡されません。パッシブ モードではトラフィックが戻されず、モジュールはトラフィックをブロックできません。
7. 発信 VPN トラフィックが暗号化されます。
8. トラフィックが ASA から出ます。

### ASA の機能との互換性

ASA には、HTTP インスペクションを含む、多数の高度なアプリケーション インスペクション機能があります。ただし、ASA FirePOWER モジュールには ASA よりも高度な HTTP インスペクション機能があり、その他のアプリケーションについても機能が追加されています。たとえば、アプリケーション使用状況のモニタリングおよび制御機能です。

ASA FirePOWER モジュールの機能を最大限に活用するには、ASA FirePOWER モジュールに送信するトラフィックに関する次のガイドラインを参照してください。

- HTTP トラフィックに対して ASA インスペクションを設定しないでください。
- クラウド Web セキュリティ（ScanSafe）インスペクションを設定しないでください。ASA FirePOWER インスペクションと Cloud Web Security のインスペクションの両方を同じトラフィックに設定すると、ASA では ASA FirePOWER インスペクションのみが実行されます。
- ASA 上の他のアプリケーション インスペクションは ASA FirePOWER モジュールと互換性があり、これにはデフォルト インスペクションも含まれます。
- Mobile User Security（MUS）サーバをイネーブルにしないでください。これは、ASA FirePOWER モジュールとの間に互換性がありません。
- フェールオーバーをイネーブルにしている場合、ASA がフェールオーバーすると、既存の ASA FirePOWER フローは新しい ASA に転送されます。新しい ASA の ASA FirePOWER モジュールがその時点からトラフィックのインスペクションを開始します。古いインスペクションの状態は転送されません。

### モニタ専用モード

モニタ専用モードのトラフィック フローは、インライン モードのトラフィック フローと同じです。ただし、ASA FirePOWER モジュールではトラフィックを ASA に戻さない点のみが異なります。代わりに、モジュールはトラフィックにセキュリティ ポリシーを適用し、インライン モードで動作していたらどのようになっていたかをユーザに通知します。たとえば、トラフィックが「ドロップされていたことが予想される」とマークされる場合があります。この情報をトラフィック分析に使用し、インライン モードが望ましいかどうかを判断するのに役立てることができます。

(注) ASA 上でモニタ専用モードと通常のインライン モードの両方を同時に設定できません。セキュリティ ポリシーの 1 つのタイプのみが許可されます。マルチ コンテキスト モードでは、一部のコンテキストに対してモニタ専用モードを設定し、残りのコンテキストに対して通常のインライン モードを設定することはできません。

## 例

次に、すべての HTTP トラフィックを ASA FirePOWER モジュールに迂回させ、何らかの理由でモジュールで障害が発生した場合にはすべての HTTP トラフィックをブロックする例を示します。

```
ciscoasa(config)# access-list ASASFR permit tcp any any eq port 80
ciscoasa(config)# class-map my-sfr-class
ciscoasa(config-cmap)# match access-list ASASFR
ciscoasa(config-cmap)# policy-map my-sfr-policy
ciscoasa(config-pmap)# class my-sfr-class
ciscoasa(config-pmap-c)# sfr fail-close
ciscoasa(config-pmap-c)# service-policy my-cx-policy global
```

次に、10.1.1.0 ネットワークおよび 10.2.1.0 ネットワーク宛てのすべての IP トラフィックを ASA FirePOWER モジュールに迂回させ、何らかの理由でモジュールに障害が発生してもすべてのトラフィックを許可する例を示します。

```
ciscoasa(config)# access-list my-sfr-acl permit ip any 10.1.1.0 255.255.255.0
ciscoasa(config)# access-list my-sfr-acl2 permit ip any 10.2.1.0 255.255.255.0
ciscoasa(config)# class-map my-sfr-class
ciscoasa(config-cmap)# match access-list my-sfr-acl
ciscoasa(config)# class-map my-sfr-class2
ciscoasa(config-cmap)# match access-list my-sfr-acl2
ciscoasa(config-cmap)# policy-map my-sfr-policy
ciscoasa(config-pmap)# class my-sfr-class
ciscoasa(config-pmap-c)# sfr fail-open
ciscoasa(config-pmap)# class my-sfr-class2
ciscoasa(config-pmap-c)# sfr fail-open
ciscoasa(config-pmap-c)# service-policy my-sfr-policy interface outside
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **class** | トラフィック分類に使用するクラス マップを指定します。 |
| **class-map** | ポリシー マップ用にトラフィックを識別します。 |
| **hw-module module reload** | モジュールをリロードします。 |
| **hw-module module reset** | リセットを実行してから、モジュールをリロードします。 |
| **hw-module module shutdown** | モジュールをシャットダウンします。 |
| **policy-map** | ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。 |
| **show asp table classify domain sfr** | トラフィックを ASA FirePOWER モジュールに送信するために作成された NP ルールを表示します。 |
| **show module** | モジュールのステータスを表示します。 |
| **show running-config policy-map** | 現在のすべてのポリシー マップ コンフィギュレーションを表示します。 |
| **show service-policy** | サービス ポリシーの統計情報を表示します。 |
| **sw-module module sfr reload** | ソフトウェア モジュールをリロードします。 |

| コマンド | 説明 |
|---|---|
| **sw-module module sfr reset** | ソフトウェア モジュールをリセットします。 |
| **sw-module module sfr recover** | ソフトウェア モジュール ブート イメージをインストールします。 |
| **sw-module module sfr shutdown** | ソフトウェア モジュールをシャットダウンします。 |

# shape

QoS トラフィック シェーピングをイネーブルにするには、クラス コンフィギュレーション モードで **shape** コマンドを使用します。ASA などの、ファスト イーサネットを使用してパケットを高速に送信するデバイスが存在し、そのデバイスがケーブル モデムなどの低速デバイスに接続されている場合、ケーブル モデムがボトルネックとなり、ケーブル モデムでパケットが頻繁にドロップされます。さまざまな回線速度を持つネットワークを管理するために、低い固定レートでパケットを送信するように ASA を設定できます。これを *トラフィック シェーピング*と呼びます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

(注) トラフィック シェーピングは、ASA 5505、5510、5520、5540、および 5550 のみでサポートされます。(ASA 5500-X などの)マルチコア モデルでは、シェーピングをサポートしていません。

**shape average** *rate* [*burst_size*]

**no shape average** *rate* [*burst_size*]

## 構文の説明

| | |
|---|---|
| **average** *rate* | 一定期間におけるトラフィックの平均レート(ビット/秒)を 64000 ～ 154400000 の範囲で設定します。8000 の倍数の値を指定します。期間の計算方法の詳細については、「使用上のガイドライン」の項を参照してください。 |
| *burst_size* | 一定期間において送信可能な平均バースト サイズ(ビット単位)を 2048 ～ 154400000 の範囲で設定します。128 の倍数の値を指定します。*burst_size* を指定しない場合、デフォルト値は指定した平均レートでの 4 ミリ秒のトラフィックに相当する値になります。たとえば、平均レートが 1000000 ビット/秒の場合、4 ミリ秒では 1000000 * 4/1000 = 4000 になります。 |

## デフォルト

*burst_size* を指定しない場合、デフォルト値は指定した平均レートでの 4 ミリ秒のトラフィックに相当する値になります。たとえば、平均レートが 1000000 ビット/秒の場合、4 ミリ秒では 1000000 * 4/1000 = 4000 になります。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2(4)/8.0(4) | このコマンドが追加されました。 |

## 使用上のガイドライン

トラフィック シェーピングをイネーブルにするには、Modular Policy Framework を使用します。

1. **policy-map**:**class-default** クラス マップに関連付けるアクションを指定します。
   a. **class class-default**:アクションを実行する **class-default** クラス マップを指定します。
   b. **shape**:トラフィック シェーピングをクラス マップに適用します。
   c. （任意）**service-policy**:シェーピングされたトラフィックのサブセットに対してプライオリティ キューイングを適用できるように、**priority** コマンドを設定した異なるポリシー マップを呼び出します。
2. **service-policy**:ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

### トラフィック シェーピングの概要

トラフィック シェーピングは、デバイスとリンクの速度を一致させることで、ジッタや遅延の原因になる可能性のあるパケット損失、可変遅延、およびリンク飽和を制御するために使用されます。

- トラフィック シェーピングは、物理インターフェイスのすべての発信トラフィック、または ASA 5505 の場合は VLAN 上のすべての発信トラフィックに適用する必要があります。特定のタイプのトラフィックにはトラフィック シェーピングを設定できません。
- トラフィック シェーピングは、パケットがインターフェイスで送信する準備ができている場合に実装されます。そのため、レートの計算は、IPSec ヘッダーや L2 ヘッダーなどの潜在的なすべてのオーバーヘッドを含む、送信されるパケットの実際のサイズに基づいて実行されます。
- シェーピングされるトラフィックには、through-the-box トラフィックと from-the-box トラフィックの両方が含まれます。
- シェープ レートの計算は、標準トークン バケット アルゴリズムに基づいて行われます。トークン バケット サイズは、バースト サイズ値の 2 倍です。トークン バケットの詳細については、CLI 設定ガイドを参照してください。
- バースト性のトラフィックが指定されたシェープ レートを超えると、パケットはキューに入れられて、後で送信されます。次に、シェーピング キューのいくつかの特性について説明します（階層型プライオリティ キューイングの詳細については、**priority** コマンドを参照してください）。
  - キューのサイズは、シェープ レートに基づいて計算されます。キューは、1500 バイトのパケットとして 200 ミリ秒に相当するシェープ レート トラフィックを保持できます。最小キュー サイズは 64 です。
  - キューの制限に達すると、パケットはキューの末尾からドロップされます。
  - OSPF Hello パケットなどの一部の重要なキープアライブ パケットは、ドロップされません。
  - 時間間隔は、*time_interval = burst_size / average_rate* によって求められます。時間間隔が長くなるほど、シェープ トラフィックのバースト性は高くなり、リンクのアイドル状態が長くなる可能性があります。この効果は、次のような誇張した例を使うとよく理解できます。

平均レート = 1000000

バースト サイズ = 1000000

この例では、時間間隔は 1 秒であり、これは、100 Mbps の FE リンクでは 1 Mbps のトラフィックを時間間隔 1 秒の最初の 10 ミリ秒内にバースト送信できることを意味し、残りの 990 ミリ秒間はアイドル状態になって、次の時間間隔になるまでパケットを送信できません。したがって、音声トラフィックのように遅延が問題になるトラフィックがある場合は、バースト サイズを平均レートと比較して小さくし、時間間隔を短くする必要があります。

### QoS 機能の相互作用のしくみ

ASA で必要な場合は、個々の QoS 機能を単独で設定できます。ただし、普通は、たとえば一部のトラフィックを優先させて、他のトラフィックによって帯域幅の問題が発生しないようにするために、複数の QoS 機能を ASA に設定します。

次に、インターフェイスごとにサポートされる機能の組み合わせを示します。

- 標準プライオリティ キューイング（特定のトラフィックについて）+ ポリシング（その他のトラフィックについて）

  同じトラフィックのセットに対して、プライオリティ キューイングとポリシングを両方設定することはできません。

- トラフィック シェーピング（1 つのインターフェイス上のすべてのトラフィック）+ 階層型プライオリティ キューイング（トラフィックのサブセット）。

同じインターフェイスに対して、トラフィック シェーピングと標準プライオリティ キューイングを設定することはできません。階層型プライオリティ キューイングのみを設定できます。たとえば、グローバル ポリシーに標準プライオリティ キューイングを設定して、特定のインターフェイスにトラフィック シェーピングを設定する場合、最後に設定した機能は拒否されます。これは、グローバル ポリシーがインターフェイス ポリシーと重複するためです。

通常、トラフィック シェーピングをイネーブルにした場合、同じトラフィックに対してはポリシングをイネーブルにしません。ただし、このような設定は ASA では制限されていません。

## 例

次の例では、外部インターフェイスのすべてのトラフィックでトラフィック シェーピングをイネーブルにして、DSCP ビットが ef に設定された VPN tunnel-grp1 内のトラフィックにプライオリティを付けます。

```
ciscoasa(config)# class-map TG1-voice
ciscoasa(config-cmap)# match tunnel-group tunnel-grp1
ciscoasa(config-cmap)# match dscp ef

ciscoasa(config)# policy-map priority-sub-policy
ciscoasa(config-pmap)# class TG1-voice
ciscoasa(config-pmap-c)# priority

ciscoasa(config-pmap-c)# policy-map shape_policy
ciscoasa(config-pmap)# class class-default
ciscoasa(config-pmap-c)# shape
ciscoasa(config-pmap-c)# service-policy priority-sub-policy

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

関連コマンド

| コマンド | 説明 |
|---|---|
| **class** | ポリシー マップ内でアクションを実行するクラス マップを指定します。 |
| **police** | QoS ポリシングをイネーブルにします。 |
| **policy-map** | サービス ポリシーのトラフィックに適用するアクションを指定します。 |
| **priority** | QoS プライオリティ キューイングを有効にします。 |
| **service-policy**（クラス） | 階層型ポリシー マップを適用します。 |
| **service-policy**（グローバル） | サービス ポリシーをインターフェイスに適用します。 |
| **show service-policy** | QoS 統計情報を表示します。 |

# share-ratio

マッピングアドレスおよびポート(MAP)ドメイン内の基本マッピングルールでポートルールのポート数を決定するポート比率を設定するには、MAP ドメインの基本マッピング ルール コンフィギュレーション モードで **share-ratio** コマンドを使用します。比率を削除するには、このコマンドの **no** 形式を使用します。

**share-ratio** *number*

**no share-ratio** *number*

## 構文の説明

| | |
|---|---|
| *number* | プール内に存在する必要があるポートの数。ポート数は 1～65536 の範囲内とし、2 の累乗にする必要があります(1、2、4、8 など)。 |

## デフォルト

デフォルト設定はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 9.13(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

基本マッピングルールの **start-port** コマンドおよび **share-ratio** コマンドによって、MAP ドメイン内のアドレス変換に使用されるプールの開始ポートとポート数が決まります。

## 例

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

```
ciscoasa(config)# map-domain 1
ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64
ciscoasa(config-map-domain)# basic-mapping-rule
ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
ciscoasa(config-map-domain-bmr)# start-port 1024
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

関連コマンド

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