



## sa ~ shov

---

- [same-security-traffic](#) (4 ページ)
- [sasl-mechanism](#) (6 ページ)
- [saml idp](#) (9 ページ)
- [saml idp-trustpoint](#) (12 ページ)
- [saml identity-provider](#) (14 ページ)
- [sast](#) (15 ページ)
- [scansafe](#) (17 ページ)
- [scansafe general-options](#) (20 ページ)
- [scep-enrollment enable](#) (23 ページ)
- [scep-forwarding-url](#) (25 ページ)
- [secondary](#) (27 ページ)
- [secondary-authentication-server-group](#) (29 ページ)
- [secondary-color](#) (31 ページ)
- [secondary-pre-fill-username](#) (33 ページ)
- [secondary-text-color](#) (36 ページ)
- [secondary-username -from-certificate](#) (38 ページ)
- [secondary-username-from-certificate-choice](#) (42 ページ)
- [secure-unit-authentication](#) (44 ページ)
- [security-group](#) (46 ページ)
- [security-group-tag](#) (48 ページ)
- [security-level](#) (50 ページ)
- [segment-id](#) (53 ページ)
- [send response](#) (56 ページ)
- [seq-past-window](#) (58 ページ)
- [serial-number](#) (60 ページ)
- [server \(POP3、IMAP4、SMTP\) \(廃止\)](#) (61 ページ)
- [server \(ScanSafe 汎用オプション\)](#) (63 ページ)
- [server \(ssh pubkey-chain\)](#) (67 ページ)
- [server authenticate-client](#) (69 ページ)

- server cipher-suite (71 ページ)
- server-port (73 ページ)
- server-separator (POP3、IMAP4、SMTP) (廃止) (75 ページ)
- server trust-point (77 ページ)
- server-type (79 ページ)
- service (CTL プロバイダー) (82 ページ)
- service (グローバル) (84 ページ)
- service (オブジェクト サービス) (87 ページ)
- service call-home (90 ページ)
- service-module (91 ページ)
- service-object (93 ページ)
- service password-recovery (96 ページ)
- service-policy (クラス) (99 ページ)
- service-policy (グローバル) (102 ページ)
- service sw-reset-button (105 ページ)
- service telemetry (107 ページ)
- session (109 ページ)
- session console (111 ページ)
- session do (113 ページ)
- session ip (115 ページ)
- set adaptive-interface cost (117 ページ)
- set as-path (119 ページ)
- set automatic-tag (121 ページ)
- set community (123 ページ)
- set connection (125 ページ)
- set connection advanced-options (130 ページ)
- set connection decrement-ttl (135 ページ)
- set connection timeout (137 ページ)
- set default interface (141 ページ)
- set dscp (143 ページ)
- set ikev1 transform-set (146 ページ)
- set interface (148 ページ)
- set ip df (150 ページ)
- set ip default next-hop (152 ページ)
- set ip next-hop (154 ページ)
- set ip next-hop recursive (156 ページ)
- set ip next-hop verify-availability (158 ページ)
- set local-preference (161 ページ)
- set metric (163 ページ)
- set metric-type (165 ページ)
- set metric-type internal (167 ページ)

- [set origin](#) (169 ページ)
- [set pfs](#) (171 ページ)
- [set security-association lifetime](#) (173 ページ)
- [set trustpoint](#) (175 ページ)
- [setup](#) (177 ページ)
- [set weight](#) (180 ページ)
- [sfr](#) (181 ページ)
- [shape](#) (185 ページ)
- [share-ratio](#) (189 ページ)

## 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。

### コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

### コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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、Cisco Secure Firewall 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л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	<b>same-security-traffic</b> 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 サーバー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 サーバー 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。

認証メカニズムを無効にするには、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 ユーザーにとっては、ASA が LDAP サーバー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

<i>digest-md5</i>	ASA は、ユーザー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ー名とレルムを送信することによって応答します。
<b>server-group-name</b>	最大 64 文字の Kerberos AAA サーバー グループを指定します。

### 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。ASA は、認証パラメータをプレーンテキストで LDAP サーバーに渡します。



(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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AAA サーバー 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 変更内容  
ス

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 サーバー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 サーバーの両方で、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 はサーバーに設定されている SASL メカニズムのリストを取得して、ASA とサーバー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 サーバーと 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 サーバー 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 サーバー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 サーバーとして `kerb-svr1` 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
<b>ldap-over-ssl</b>	SSL が LDAP クライアントとサーバー間の接続を保護することを指定します。
<b>server-type</b>	LDAP サーバー ベンダーに Microsoft または Sun のいずれかを指定します。

コマンド	説明
<b>ldap attribute-map (global configuration mode)</b>	ユーザー定義の属性名を 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 はエンドユーザーを ASA へリダイレクトできます。
clock-skew <value>	NotBefore アサーションと NotOnOrAfterSAML アサーションを許容するクロックスキュー。デフォルトでは clock-skew は無効になっています。clock-skew のデフォルト値は 1 秒です。指定できる範囲は 1 ~ 180 秒です。
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。
signature <value>	シグニチャ (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。  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。  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。  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。

コマンド 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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
webvpn	• 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` : エンドユーザーを 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
認証	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 idp-trustpoint

SAML IdP コンフィギュレーションのトラストポイント IdP 設定を上書きするには、webvpn トンネルグループ コンフィギュレーションモードで **saml idp-trustpoint** コマンドを使用します。IdP トラストポイント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。

**saml idp-trustpoint name**  
**no saml idp-trustpoint name**

### 構文の説明

*name* IdP トラストポイントの名前。

### コマンド デフォルト

有効になっていません

### コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

### コマンド履歴

リリー 変更内容  
 ス

9.17(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

既存の ASA SAML コンフィギュレーションは、設定された SAML IDP ごとに 1 つの IDP トラストポイントのみをサポートします。 **saml idp-trustpoint** コマンドは IdP 設定を上書きして、Microsoft Azure の複数アプリケーションの導入シナリオをサポートします。

IdP トラストポイント設定がトンネルグループに存在する場合、このコマンドはトンネルグループの **saml identity-provider** コマンドで参照される IdP コンフィギュレーションのトラストポイント IdP 設定を上書きします。

### 例

次に、トラストポイント IdP コンフィギュレーションの IdP 設定を上書きする例を示します。

```
ciscoasa(config)# same-security-traffic permit inter-interface
ciscoasa(config-webvpn)# tunnel-group Sales webvpn-attributes
ciscoasa(config-tunnel-webvpn)# saml idp-trustpoint _SmartCallHome_ServerCA
```

## 関連コマンド

コマンド	説明
identity-provider	ASA内のサードパーティ SAML ID プロバイダー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 が使用するよう設定している SAML Idp の名前。

### コマンドデフォルト

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。

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

### コマンド履歴

リリー 変更内容  
 ス

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。



- (注) SAML ID プロバイダー名を追加しているときに、「ERROR: SAML configuration could not be built」というエラーが表示された場合は、トンネルグループ名をチェックして、トンネルグループ名に特殊文字の &、"、< が含まれていないことを確認してください。トンネルグループ名を追加するには、**tunnel-group webvpn-attributes** コマンドを使用します。

### 関連コマンド

コマンド	説明
認証	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。

### コマンド デフォルト

デフォルトの動作や値はありません。

### コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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
<b>ctl-file (global)</b>	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。
<b>ctl-file (phone-proxy)</b>	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。
<b>phone-proxy</b>	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спек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 サーバーに送信します。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。

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

## コマンド履歴

リリース 変更内容  
ス

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
<b>class-map type inspect scansafe</b>	ホワイトリストに記載されたユーザーとグループのインスペクション クラス マップを作成します。
<b>default user group</b>	ASA に入ってくるユーザーのアイデンティティを ASA が判別できない場合のデフォルトのユーザー名やグループを指定します。
<b>http [s ]</b> (パラメータ)	インスペクションポリシーマップのサービス タイプ (HTTP または HTTPS) を指定します。
<b>inspect scansafe</b>	このクラスのトラフィックに対するクラウド Web セキュリティ インスペクションをイネーブルにします。
<b>license</b>	要求の送信元の組織を示すため、ASA がクラウド Web セキュリティ プロキシ サーバーに送信する認証キーを設定します。
<b>match user group</b>	ユーザーまたはグループをホワイトリストと照合します。
<b>policy-map type inspect scansafe</b>	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。
<b>retry-count</b>	再試行回数値を入力します。この値は、可用性をチェックするために、クラウド Web セキュリティ プロキシ サーバーをポーリングする前に ASA が待機する時間です。
<b>scansafe</b>	マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティ を許可します。
<b>scansafe general-options</b>	汎用クラウド Web セキュリティ サーバー オプションを設定します。

コマンド	説明
<b>server { primary   backup }</b>	プライマリまたはバックアップのクラウド Web セキュリティプロキシサーバーの完全修飾ドメイン名または IP アドレスを設定します。
<b>show conn scansafe</b>	大文字の Z フラグに示されたようにすべてのクラウド Web セキュリティ接続を表示します。
<b>show scansafe server</b>	サーバーが現在のアクティブサーバー、バックアップサーバー、または到達不能のいずれであるか、サーバーのステータスを表示します。
<b>show scansafe statistics</b>	合計と現在の http 接続を表示します。
<b>user-identity monitor</b>	AD エージェントから指定したユーザーまたはグループ情報をダウンロードします。
<b>whitelist</b>	トラフィックのクラスでホワイトリストアクションを実行します。

## scansafe general-options

クラウド Web セキュリティ プロキシ サーバー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。サーバー 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。

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

### コマンド履歴

リリー 変更内容  
 ス

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 サーバーとバックアップ プロキシ サーバーを設定できます。

### 例

次に、プライマリ サーバー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
<b>class-map type inspect scansafe</b>	ホワイトリストに記載されたユーザーとグループのインスペクション クラス マップを作成します。

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

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

## 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。

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

**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。

### コマンドデフォルト

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。

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

### コマンド履歴

リリース 変更内容  
 ス

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 セキュアクライアントのみです。

ASA は、セキュアクライアントとサードパーティ認証局間の SCEP 要求のプロキシとして動作できます。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、ユーザーが 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 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）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セキュアクライアント）はサポートしています。

ASA 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
<code>crypto ikev2 enable</code>	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。
<code>scep-forwarding-url</code>	グループ ポリシー用のSCEP 認証局を登録します。
<code>secondary-pre-fill-username clientless</code>	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。
<code>secondary-authentication-server-group</code>	証明書が使用できないときにはユーザー名を指定します。



# 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。

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

**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。

## コマンドデフォルト

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。

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

## コマンド履歴

リリー 変更内容  
ス

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。

## 例

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ー名を指定します。

# 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。

## コマンドデフォルト

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
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)	以前のバージョンのソフトウェアでは「同時」ブートアップが許可されていたため、フェールオーバーグループを優先ユニットでアクティブにする <b>preempt</b> コマンドは必要ありませんでした。しかし、この機能は、両方のフェールオーバーグループが最初に起動するユニットでアクティブになるように変更されました。

## 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番目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番目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

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
<b>failover group</b>	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。
<b>preempt</b>	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。
<b>primary</b>	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ー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

<i>interface_name</i>	(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。
<b>LOCAL</b>	(任意) 通信障害によりサーバーグループにあるすべてのサーバーが非アクティブになった場合に、ローカルユーザーデータベースに対する認証を要求します。サーバーグループ名が <b>LOCAL</b> または <b>NONE</b> の場合、ここでは <b>LOCAL</b> キーワードを使用しないでください。
<b>none</b>	(任意) サーバーグループ名を <b>NONE</b> と指定して、認証が不要であることを示します。
<i>groupname</i> [ <b>LOCAL</b> ]	事前に設定済みの認証サーバーまたはサーバー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。
<b>use-primary-username</b>	プライマリユーザー名をセカンダリ認証のユーザー名として使用します。

### コマンドデフォルト

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。

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

## コマンド履歴

リリー 変更内容  
ス

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つのユーザー名のみが要求されます。

ユーザー名がデジタル証明書から抽出される場合は、プライマリユーザー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
<b>pre-fill-username</b>	事前入力ユーザー名機能をイネーブルにします。
<b>show running-config tunnel-group</b>	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。
<b>tunnel-group general-attributes</b>	名前付きのトンネル グループの一般属性を指定します。
<b>username-from-certificate</b>	認可時のユーザー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。

- 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。
- 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。
- 名前の最大長は 32 文字です。

### コマンド 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。

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

### コマンド履歴

リリース 変更内容  
 ス

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
<b>title-color</b>	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セキュアクライアント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ー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-pre-fill-username
```

### 構文の説明

<b>clientless</b>	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。
<b>hide</b>	認証に使用するユーザー名を VPN ユーザーに非表示にします。
<i>password</i>	パスワードストリングを入力します。
<b>client</b> <b>ssl-client</b>	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。 9.8(1) 以降では <b>client</b> キーワードを使用してください。
<i>type_num</i>	次のいずれかのオプションを入力します。 <ul style="list-style-type: none"> <li>• 入力するパスワードがプレーンテキストの場合は 0。</li> <li>• 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。</li> </ul>
<b>use-common-password</b>	ユーザー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。
<b>use-primary-password</b>	ユーザー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。

### コマンドデフォルト

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、抽出したユーザー名が VPN ユーザーに表示されます。 **use-primary-password** と **use-common-password** のいずれのキーワードも指定しないと、ユーザー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。

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

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。

9.8(1) **ssl-client** キーワードが **client** に変更されました。

### 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があります。

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ー名を、セカンダリユーザー名またはパスワード認証のユーザー名として使用できるようにします。2 回目の認証で証明書からのユーザー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 番目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、ユーザー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ー体験になります。

**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 ユーザー名として使用して、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、抽出されたユーザー名をユーザーに非表示にします。

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

次の例では、前のコマンドと同じ機能を実行しますが、セキュアクライアント接続だけに適用されます。

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

次の例では、ユーザー名を非表示にして、ユーザー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 client hide
use-primary-password
```

次の例では、ユーザー名を非表示にして、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 client hide use-common-password
*****
```

## 関連コマンド

コマンド	説明
<code>pre-fill-username</code>	事前入力ユーザー名機能をイネーブルにします。
<code>show running-config tunnel-group</code>	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。
<code>tunnel-group general-attributes</code>	名前付きのトンネル グループの一般属性を指定します。
<code>username-from-certificate</code>	認可時のユーザー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。

### コマンド 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。

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

### コマンド履歴

リリー 変更内容  
 ス

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
<b>text-color</b>	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 つ目のユーザー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ー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ー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** Adaptive Security Device Manager (ASDM) によって生成されたスクリプトファイルを使用して、ユーザー名として使用する DN フィールドを証明書から抽出することを指定します。

### コマンド 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。

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

## コマンド履歴

リリー 変更内容  
ス

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ー名として使用する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回目のユーザー名/パスワード認証のための2つ目のユーザー名として使用するよう強制します。

2回目のユーザー名/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ー名の事前充填機能で、取得されたユーザー名を使用するには、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回めのユーザー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)。

属性	定義
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（ユーザー ID）。
UPN	User Principal Name（ユーザープリンシパル名）。
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-username-from-certificate command, only** とともに **secondary-authentication-server-group** コマンドも指定する場合、認証にはプライマリユーザー名が使用されます。

## 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、事前入力ユーザー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	事前入力ユーザー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セキュアクライアント接続において、ユーザー名抽出を有効にします。
username-from-certificate	認可時のユーザー名として使用する証明書内のフィールドを指定します。



コマンド	説明
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。
<b>secondary-authentication-server-group</b>	セカンダリ AAA サーバーグループを指定します。ユーザー名がデジタル証明書から抽出される場合は、プライマリ ユーザー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ー名フィールドにユーザー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ー名を使用するには、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ー名を、セカンダリ認証の事前入力ユーザー名フィールドで使用するよう SSL または IKE で送信するかどうかを指定します。

**second-certificate** ユーザー証明書のユーザー名を、セカンダリ認証の事前入力ユーザー名フィールドで使用するようクライアントから送信するかどうかを指定します。

### コマンド デフォルト

デフォルトでは、事前入力するユーザー名は 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。

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

### コマンド履歴

リリー 変更内容  
ス

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ー両方の証明書認証が可能になります。事前入力ユーザー名フィールドでは、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。事前入力のユーザー名は、常にクライアントから受信した 2 つ目の（ユーザー）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（ユーザー証明書）のどちらかを使用して事前入力ユーザー名フィールドに使用するユーザー名を取得することができます。

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ー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 tgl type remote-access
ciscoasa(config)#tunnel-group tgl 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 tgl 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
<b>username-from-certificate-choice</b>	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。

### コマンド 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。

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

### コマンド履歴

リリー 変更内容  
ス

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 サーバー 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、どのバックアップ サーバーに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ー名/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ー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、ユーザーがユーザー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
<b>ip-phone-bypass</b>	ユーザー認証を行わずに 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。
<b>leap-bypass</b>	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 パケットがユーザー認証の前に 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、ユーザー認証ごとに再度認証を行います。
<b>user-authentication</b>	ハードウェアクライアントの背後にいるユーザーに対して、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

<b>tag sgt##</b>	<p>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。</p> <p>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も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。</p>
<b>name sg_name</b>	<p>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]、[!@#%&amp;()-_{}.] を含めることができます。</p>

### コマンド デフォルト

デフォルトの動作や値はありません。

### コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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 タグからユーザーアイデンティティへのマッピングと、Cisco TrustSec タグからサーバー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、ローカライズされたセキュリティポリシーを持つローカルセキュリティグループを必要とする、グローバルに定義されていないネットワークリソースが ASA によりローカライズされている場合があります。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。ユーザーは、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
<b>object-group security</b>	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 ユーザーデータベース内のユーザー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ー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ーのセキュリティグループタグを設定しません。

**value** セキュリティグループタグ番号を指定します。  
*sgt*

### 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。

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

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グをサポートしています。外部 AAA サーバーを使用するか、または、ローカルユーザーか 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 サーバーが 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、ローカルユーザーが利用したりすることができます。

次は、VPN ユーザーに SGT を割り当てるための一般的なプロセスです。

1. ユーザーは、ISE サーバーを含む AAA サーバー 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、ユーザー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ーを認証し、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 サーバーの属性に、VPN ユーザー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
<b>show asp table cts sgt-map</b>	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。
<b>show cts sgt-map</b>	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。

### コマンド 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。

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

### コマンド履歴

リリース 変更内容  
 ス

7.0(1) このコマンドは、**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спекションエンジン：一部のインспек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спек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спек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спек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 制御：NAT 制御をイネーブルにする場合、低位のセキュリティインターフェイス（外部）上のホストにアクセスする高位のセキュリティインターフェイス（内部）上のホストに 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
<b>clear local-host</b>	すべての接続をリセットします。
<b>interface</b>	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
<b>nameif</b>	インターフェイス名を設定します。
<b>vlan</b>	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。

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

### コマンド履歴

リリース 変更内容  
 ス

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

コマンド	説明
<b>vtep-nve</b>	VNI インターフェイスを VTEP 送信元インターフェイスに関連付けます。
<b>vxlan port</b>	VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。

## 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は無効になっています。

**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。

### コマンド デフォルト

デフォルトの動作や値はありません。

### コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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
<b>inspect radius-accounting</b>	RADIUS アカウンティングのインスペクションを設定します。



コマンド	説明
parameters	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。

### コマンドデフォルト

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
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
<b>class-map</b>	サービス ポリシーに対してトラフィックを指定します。
<b>policy-map</b>	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。
<b>queue-limit</b>	順序が不正なパケットの制限を設定します。
<b>set connection advanced-options</b>	TCP 正規化をイネーブルにします。
<b>service-policy</b>	サービス ポリシーをインターフェイスに適用します。
<b>show running-config tcp-map</b>	TCP マップ コンフィギュレーションを表示します。
<b>tcp-map</b>	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。

### コマンド 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

次の表に、コマンドを入力できるモードを示します。

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

### コマンド履歴

リリー 変更内容  
ス

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
<b>crypto ca trustpoint</b>	トラストポイントコンフィギュレーションモードを開始します。

## 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ーを指定するには、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、ユーザーがサーバー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ーに要求を送信します。デフォルトのサーバーを設定せず、ユーザーもサーバーを指定しない場合、ASA ではエラーが返されます。

```
server { ipaddr または 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ーの DNS 名。

*ipaddr* デフォルトの電子メールプロキシサーバーの IP アドレス。

### コマンドデフォルト

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ーはありません。

### コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
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 電子メールサーバー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 サーバーを設定するには、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 { 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

<b>backup</b>	バックアップ サーバーを識別していることを指定します。
<b>ip ip_address</b>	サーバーの IP アドレスを指定します。
<b>fqdn fqdn</b>	サーバーの完全修飾ドメイン名 (FQDN) を指定します。
<b>port port</b>	(任意) デフォルトでは、クラウド Web セキュリティ プロキシ サーバーは 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。
<b>primary</b>	プライマリ サーバー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。

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

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 Cloud Web Security プロキシ サーバーとバックアップ プロキシ サーバーが割り当てられます。これらのサーバーは、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 サーバー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ーから到着しない場合など)、プロキシサーバーは 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、プロキシサーバーが使用不可の場合、サーバー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ー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、サーバーがTCPスリーウェイハンドシェイクを完了できても、サーバー上のクラウド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ー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ーが連続する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ー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ー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。

プロキシサーバーが到達可能でないトラフィック状態	サーバー 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) )	$(30 + ( (5-1) \times (30) )) = 150$ 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) )	$900 + (5 \times (30)) = 1050$ 秒

## 例

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

コマンド	説明
<b>user-identity monitor</b>	ADエージェントから指定したユーザーまたはグループ情報をダウンロードします。
<b>whitelist</b>	トラフィックのクラスでホワイトリストアクションを実行します。

## 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サーバーおよびそのキーを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。サーバー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サーバーの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。

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

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サーバーの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ーとそのキーを追加または削除できます。

各サーバーについて、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にあるサーバー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にあるサーバー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
<b>copy</b>	ASA との間でファイルをコピーします。
<b>key-hash</b>	ハッシュ SSH ホスト キーを入力します。
<b>key-string</b>	公開 SSH ホスト キーを入力します。
<b>ssh pubkey-chain</b>	ASA のデータベースに格納されるサーバーとそのキーを手動で追加または削除します。
<b>ssh stricthostkeycheck</b>	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す。

## コマンド デフォルト

このコマンドは、デフォルトでイネーブルです。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。

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

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
<b>tls-proxy</b>	TLS プロキシインスタンスを設定します。

## server cipher-suite

TLS プロキシサーバー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。

- **3des-sha1**
- **aes128-sha1**
- **aes256-sha1**
- **des-sha1**
- **null-sha1**
- **rc4-sha1**

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、プロキシサーバーは **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。

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

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 サーバー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 サーバー接続に最小 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 サーバー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
<b>tls-proxy</b>	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。
<b>client cipher-list</b>	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 サーバーポートを設定するには、AAA サーバーホストモードで **server-port** コマンドを使用します。指定されているサーバー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。

### コマンドデフォルト

デフォルトのサーバー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。

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

### コマンド履歴

リリース 変更内容  
 ス

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 サーバーでサーバーポート番号 8888 を使用するよう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
<b>aaa-server host</b>	ホスト固有の AAA サーバー パラメータを設定します。
<b>clear configure aaa-server</b>	AAA サーバーのコンフィギュレーションをすべて削除します。
<b>show running-config aaa-server</b>	すべての AAA サーバー、特定のサーバー グループ、特定のグループ内の特定のサーバー、または特定のプロトコルの AAA サーバー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。

電子メールサーバー名および VPN サーバー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** { シンボル }  
**no server-separator**

## 構文の説明

シンボル 電子メールサーバー名および VPN サーバー名を区切る文字。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。

## コマンドデフォルト

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。

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

サーバーの区切り文字には、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 サーバー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
<b>name-separator</b>	電子メールおよびVPNのユーザー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 サーバー 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。

#### コマンド デフォルト

デフォルトの動作や値はありません。

#### コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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、グローバルの **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ー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、サーバー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
<b>client</b> (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。
<b>client trust-point</b>	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。
<b>ssl trust-point</b>	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。
<b>tls-proxy</b>	TLS プロキシインスタンスを設定します。

## server-type

LDAP サーバーモデルを手動で設定するには、AAA サーバー 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、次のサーバー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 サーバー (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

<i>auto-detect</i>	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。
<i>generic</i>	Sun および Microsoft の LDAP ディレクトリ サーバー以外の LDAP v3 準拠のディレクトリ サーバーを指定します。一般的な LDAP サーバーでは、パスワード管理はサポートされません。
<i>microsoft</i>	LDAP サーバーが Microsoft Active Directory であることを指定します。
<i>openldap</i>	LDAP サーバーが OpenLDAP サーバーであることを指定します。
<i>novell</i>	LDAP サーバーが Novell サーバーであることを指定します。
<i>sun</i>	LDAP サーバーが Sun Microsystems JAVA System Directory Server であることを指定します。

### コマンドデフォルト

デフォルトでは、自動検出によってサーバー 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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AAA サーバー 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 サーバー 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ーと互換性があります。



(注) Sun : Sun ディレクトリサーバーにアクセスするために ASA に設定されている DN が、サーバー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ー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ー、Sun LDAP ディレクトリサーバー、または一般的な LDAPv3 サーバーのいずれか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 サーバータイプを決定できない場合で、サーバーが Microsoft または Sun のサーバー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、サーバーを Microsoft または Sun Microsystems の LDAP サーバーとして手動で設定できます。

## 例

次に、AAA サーバー 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 サーバー ldapsvr1 のサーバー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 サーバーを設定しています。

```
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ー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
<b>ldap-over-ssl</b>	SSL が LDAP クライアントとサーバー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ー間での SASL 認証を設定します。
<b>ldap attribute-map (global configuration mode)</b>	ユーザー定義の属性名を CiscoLDAP 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 プロバイダー)

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** クライアントにエクスポートする証明書を指定します。  
*listening\_port*

### コマンド 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。

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

### コマンド履歴

リリー 変更内容  
ス

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 サーバー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
client	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ー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。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。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できなかった場合、ASA は拒否されたパケットを何も通知せずに廃棄します。

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 サーバーからの 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。

(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。

**コマンドデフォルト** デフォルトでは、すべてのインターフェイスで **service resetoutbound is** 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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュ レーション	• 対応	• 対応	• 対応	• 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
<b>show running-config service</b>	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

<b>destination operator number</b>	(任意。 <b>tcp</b> 、 <b>udp</b> 、 <b>sctp</b> 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。 <ul style="list-style-type: none"> <li>• <b>eq</b> : ポート番号に等しい。</li> <li>• <b>gt</b> : ポート番号より大きい。</li> <li>• <b>lt</b> : ポート番号より小さい。</li> <li>• <b>neq</b> : ポート番号と等しくない。</li> <li>• <b>range</b> : ポート範囲。2つの番号は、<b>range 1024 4500</b> のようにスペースで区切って指定します。</li> </ul>
<b>{ icmp   icmp6 } [ icmp_type [ icmp_code ] ]</b>	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。
<b>protocol</b>	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。
<b>sctp</b>	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。
<b>source operator number</b>	(任意。 <b>tcp</b> 、 <b>udp</b> 、 <b>sctp</b> 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 <b>destination</b> のものと同じです。
<b>tcp</b>	サービスタイプが TCP 接続用であることを指定します。
<b>udp</b>	サービスタイプが UDP 接続用であることを指定します。

コマンドデフォルト デフォルトの動作や値はありません。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
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
<b>clear configure object</b>	作成されたすべてのオブジェクトをクリアします。
<b>object-group service</b>	サービス オブジェクトを設定します。
<b>show running-config object service</b>	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。

### コマンド 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。

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

### コマンド履歴

リリー 変更内容  
ス

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
<b>call-home (global configuration)</b>	Call Home コンフィギュレーション モードを開始します。
<b>call-home test</b>	Call Home テスト メッセージを手動で送信します。
<b>show call-home</b>	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。

- 最初のスロットのモジュールの場合は **1**。
- 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思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)。

### コマンド 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。

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

### コマンド履歴

リリー 変更内容  
ス

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、通信チャンネルを閉じます。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

<code>destination operator number</code>	(任意。 <code>tcp</code> 、 <code>udp</code> 、 <code>tcp-udp</code> 、 <code>sctp</code> 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。 <ul style="list-style-type: none"> <li>• <code>eq</code> : ポート番号に等しい。</li> <li>• <code>gt</code> : ポート番号より大きい。</li> <li>• <code>lt</code> : ポート番号より小さい。</li> <li>• <code>neq</code> : ポート番号と等しくない。</li> <li>• <code>range</code> : ポート範囲。2つの番号は、<code>range 1024 4500</code> のようにスペースで区切って指定します。</li> </ul>
<code>{ icmp   icmp6 } [ icmp_type [ icmp_code ] ]</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。
<code>object name</code>	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。
<code>protocol</code>	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前のリストについては、CLI ヘルプを参照してください。
<code>sctp</code>	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。
<code>source operator number</code>	(任意。 <code>tcp</code> 、 <code>udp</code> 、 <code>tcp-udp</code> 、 <code>sctp</code> 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 <code>destination</code> のものと同じです。
<code>tcp</code>	サービス タイプが TCP 接続用であることを指定します。

<b>tcp-udp</b>	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。
<b>udp</b>	サービス タイプが UDP 接続用であることを指定します。

コマンド デフォルト      デフォルトの動作や値はありません。

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

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

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** 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
<b>clear configure object-group</b>	すべての <b>object-group</b> コマンドをコンフィギュレーションから削除します。
<b>network-object</b>	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。
<b>object service</b>	サービス オブジェクトを追加します。
<b>object-group</b>	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。
<b>port-object</b>	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。
<b>show running-config object-group</b>	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、不正なユーザー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。

### コマンド 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。

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

### コマンド履歴

リリー 変更内容  
 ス

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 **Escape** 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 **Escape** キーを押して、モニターモードを起動します。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、ユーザーが 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。ユーザーが ROMMON を開始すると、ユーザーは、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。ユーザーは、最初に消去を実行しないと、ROMMON を開始できません。ユーザー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、不正なユーザー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、システムを動作状態に回復するには、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、ユーザーは、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。ユーザーは、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。ユーザー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、不正なユーザー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、システムを動作状態に回復するには、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
<b>config-register</b>	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。
<b>enable password</b>	イネーブルパスワードを設定します。
<b>password</b>	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。

### コマンドデフォルト

デフォルトの動作や値はありません。

### コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

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 TGI-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
TGI-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
```

一  
例

#### 関連コマンド

コマンド	説明
<b>class (policy-map)</b>	ポリシー マップにクラス マップを指定します。
<b>clear configure service-policy</b>	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。
<b>clear service-policy</b>	サービス ポリシーの統計情報をクリアします。

コマンド	説明
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 (グローバル)

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

<b>fail-close</b>	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спек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。
<b>global</b>	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。
<b>interface</b> <i>intf</i>	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。
<i>policymap_name</i>	<b>policy-map</b> 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спекションポリシーマップ ( <b>policy-map type inspect</b> ) は指定できません。

### コマンド デフォルト

デフォルトの動作や値はありません。

### コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

### コマンド履歴

リリース 変更内容  
ス

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。各機能で使用できるコマンドの詳細については、CLI コンフィギュレーション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
<b>clear configure service-policy</b>	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。
<b>clear service-policy</b>	サービスポリシーの統計情報をクリアします。

コマンド	説明
<b>service-policy (class)</b>	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。
<b>show running-config service-policy</b>	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。
<b>show service-policy</b>	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のリセットボタンを有効にするには、グローバルコンフィギュレーションモードで **service sw-reset-button** コマンドを使用します。リセットボタンを無効にするには、このコマンドの **no** 形式を使用します。

**service 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。

### コマンドデフォルト

デフォルトでは **service sw-reset-button** 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。

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

### コマンド履歴

リリース 変更内容  
 ス

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
<b>show running-config service</b>	サービスコンフィギュレーションを表示します。

# service telemetry

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、Secure Firewall eXtensible オペレーティングシステム (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。

## コマンドデフォルト

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。

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

## コマンド履歴

リリース 変更内容  
ス

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。このコマンドは、ブレードごとのテレメトリサポートを制御するために使用されます。シャーシごとのテレメトリサポートを制御するには、FXOS/シャーシマネージャで有効にする必要があります。

## 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
<b>show telemetry</b>	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。

## sessionid

### 構文の説明

*d* モジュール ID を指定します。

- 物理モジュール：1（スロット番号 1 の場合）
- ソフトウェアモジュール、ASA  
FirePOWER：sfr
- ソフトウェアモジュール、IPS：ips
- ソフトウェアモジュール、ASA CX：cxsc

### 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

次の表は、このコマンドを入力できるモードを示しています。

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

### 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、**Ctrl-Shift-6** キーを押してから **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
<b>debug session-command</b>	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。

- ASA FirePOWER モジュール : **sfr**
- IPS モジュール : **ips**
- ASA CX モジュール : **cxsc**
- ASA 5506W-X ワイヤレスアクセスポイント : **wlan**

#### 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

次の表は、このコマンドを入力できるモードを示しています。

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

#### 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** と入力し、**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ー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ー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、代わりにターミナルサーバー プロンプトに戻ります。ASA にターミナルサーバーを再接続すると、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** コマンドを使用してください。

## 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
<b>session</b>	モジュールへの Telnet セッションを開始します。
<b>show module log console</b>	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** コマンド

## 構文の説明

*id* モジュール ID を指定します。

- 物理モジュール : **1** (スロット番号 1 の場合)
- ソフトウェアモジュール、ASA FirePOWER : **sfr**
- ソフトウェアモジュール、IPS : **ips**
- 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。

- **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。
- **get-config** : モジュール設定を取得します。
- **password-reset** : モジュールのパスワードをデフォルトにリセットします。

## 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

次の表は、このコマンドを入力できるモードを示しています。

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

## 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、**Ctrl-Shift-6** キーを押してから **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
<b>debug session-command</b>	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）にログイン 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

<b>id</b>	モジュール ID を指定します。  <ul style="list-style-type: none"> <li>物理モジュール：1（スロット番号 1 の場合）</li> <li>ソフトウェアモジュール、IPS : <b>ips</b></li> </ul>
<b>address address</b>	syslog サーバー アドレスを設定します。
<b>gateway address</b>	ゲートウェイを syslog サーバーに設定します。
<b>mask</b>	サブネットマスクを設定します。

## 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

次の表は、このコマンドを入力できるモードを示しています。

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

## 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 <b>ips</b> 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、**Ctrl-Shift-6**, キーを押してから **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
<b>debug session-command</b>	セッションのデバッグメッセージを表示します。

## set adaptive-interface cost

候補インターフェイスの適応インターフェイスコストに基づいて出力インターフェイスを設定するには、ルート マップ コンフィギュレーション モードで **set adaptive-interface cost** コマンドを使用します。

**set adaptive-interface cost** *interface\_list*

### 構文の説明

*interface\_list* インターフェイス名のスペース区切りのリスト。これらのインターフェイスから出力インターフェイスが選択されます。

### コマンドデフォルト

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。

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

9.17(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

インターフェイスのコストは、インターフェイス コンフィギュレーションで **policy-route cost** コマンドを使用して設定します。デフォルトのコストは0であるため、明示的なコスト値を設定していない場合も適応インターフェイスコストを使用できます。

インターフェイスのコストが同じである場合、アクティブ-アクティブ設定であり、出力インターフェイスでパケットがロードバランシング (ラウンドロビン) されます。コストが異なる場合、コストが最も低いインターフェイスが選択されます。インターフェイスは、アップしている場合にのみ考慮されます。

たとえば、2つの WAN リンクに同じコストを設定すると、これらのリンク間でトラフィックをロードバランシングして、パフォーマンスを向上させることができます。ただし、一方の WAN リンクの帯域幅が他方よりも高い場合は、高帯域幅リンクのコストを1に設定し、低帯域幅リンクを2に設定して、高帯域幅リンクがダウンしている場合にのみ低帯域幅リンクを使用します。

このコマンドを使用してルートマップを設定したら、**policy-route route-map** コマンドを使用して入力インターフェイスに適用する必要があります。

#### 例

次に、output1 と output2 を候補として、それらのコストに基づいて出力インターフェイスを設定する例を示します。

```
ciscoasa(config)# route-map mymap 10
ciscoasa(config-route-map)# match ip address DIA_traffic
ciscoasa(config-route-map)# set adaptive-interface cost output1 output2
```

## 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。

自律システム番号の形式の詳細については、`router bgp` コマンドの説明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。

### コマンド 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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルートマップ 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` が変わり自律システム長を変更できます。`set as-pathprepend` 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
<b>clear bgp</b>	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。
<b>bgp asnotation dot</b>	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、 <code>asplain</code> 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。

### コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

### コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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** 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。**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 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
ciscoasa(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。有効な値の範囲は 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。 <ul style="list-style-type: none"> <li>• internet</li> <li>• local-as</li> <li>• no-advertise</li> <li>• no-export</li> </ul>

### コマンドデフォルト

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。

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

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` 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。`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
<code>match as-path</code>	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 ] [ syn-cookie-mss 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 ] [ syn-cookie-mss n ] [ random-sequence-number { enable | disable } ] }
```

### 構文の説明

<b>conn-max n</b>	(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 つのサーバー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ー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。  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。
<b>embryonic-conn-max n</b>	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。
<b>per-client-embryonic-max n</b>	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。  <b>access-list</b> が <b>class-map</b> 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ています。

**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。

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。

**syn-cookie-mss** *n* 初期接続制限に達したときに初期接続のSYN cookieを生成するためのサーバーの最大セグメントサイズ（MSS）を48～65535の範囲で設定します。デフォルトは1380です。この設定は、**set connection embryonic-conn-max** または **per-client-embryonic-max** を設定する場合にのみ有効です。

#### コマンド デフォルト

**conn-max**、**embryonic-conn-max**、**per-client-embryonic-max**、および **per-client-max** パラメータについては、*n* のデフォルト値は0です。この場合、無制限の接続が許可されます。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。

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

7.0(1) このコマンドが追加されました。

リリース	変更内容
7.1(1)	<b>per-client-embryonic-max</b> および <b>per-client-max</b> 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。 <b>conn-max</b> キーワードと <b>embryonic-conn-max</b> キーワードだけを使用できます。
9.0(1)	最大接続数が 65535 から 2000000 に増えました。
9.5(2)	<b>conn-max</b> キーワードと <b>per-client-max</b> 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。
9.16(1)	<b>syn-cookie-mss</b> キーワードが追加されました。

## 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する手順は次のとおりです。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動作の詳細については、CLI コンフィギュレーション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ドする 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 フラッド攻撃を防ぎます。SYN フラッド攻撃は、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 パケットのフラッド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 はサーバー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、サーバーへの接続を許可できます。

### TCP シーケンスのランダム化

各 TCP 接続には、クライアントで生成される ISN とサーバーで生成される ISN の 2 つの ISN があります。ASA は、着信と発信の両方向で通過する TCP SYN 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
<b>class</b>	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。



コマンド	説明
<b>clear configure policy-map</b>	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 <b>service-policy</b> 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。
<b>policy-map</b>	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。
<b>show running-config policy-map</b>	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。
<b>show service-policy</b>	サービスポリシー設定を表示します。 <b>set connection</b> コマンドを含むポリシーを表示するには、 <b>set connection</b> 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

<b>flow-offload</b>	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、FXOS 1.1.4 以上を稼働する Firepower 4100 シリーズ、または Cisco Secure Firewall 3100 シリーズで使用可能です。  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。 <b>flow-offload enable</b> コマンドを使用します。
<b>sctp-state-bypass</b>	SCTP ステートバイパスを実装して、SCTP ステートフル インспек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。
<i>tcp_mapname</i>	<b>tcp-map</b> 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。
<b>tcp-state-bypass</b>	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。

### 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。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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス 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)	<b>tcp-state-bypass</b> キーワードが追加されました。
	9.5(2)	<b>sctp-state-bypass</b> キーワードが追加されました。
	9.5(2)	<b>flow-offload</b> キーワードが追加されました。オプションには、FXOS 1.1.3 以上も必要です。オプションは、Firepower 9300 シリーズで使用できます。
	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。
	9.19(1)	Cisco Secure Firewall 3100 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

デフォルトでは、ASA を通過するトラフィックはすべて、アダプティブ 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、通過を許可されるか、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 に到達するとします。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：ユーザーがある 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 でユーザー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
<b>class</b>	ポリシー マップにクラス マップを指定します。
<b>class-map</b>	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。
<b>flow-offload</b>	フロー オフロードを有効にします。
<b>policy-map</b>	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。
<b>service-policy</b>	インターフェイスにポリシー マップを割り当てます。
<b>set connection timeout</b>	接続タイムアウトを設定します。
<b>show running-config policy-map</b>	現在のポリシーマップ コンフィギュレーションをすべて表示します。

コマンド	説明
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。

### コマンドデフォルト

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。

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

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、接続が開かれず。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
<b>class</b>	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。
<b>icmp unreachable</b>	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。
<b>policy-map</b>	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。
<b>show running-config policy-map</b>	現在のポリシーマップ コンフィギュレーションをすべて表示します。
<b>show service-policy</b>	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。

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。

次のオプション値を設定できます。

- *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。

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。

- *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** 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) : mm : ss 以前の 경우는 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を送信しません。

**idle hh : mm** : 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 : ss 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。

## コマンド 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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス 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)	<b>tcp</b> 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 <b>idle</b> キーワードに代わって廃止されました。
	9.1(2)	<b>half-closed</b> の最小値が 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する手順は次のとおりです。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動作の詳細については、**CLI コンフィギュレーションガイド**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
<b>class</b>	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。
<b>clear configure policy-map</b>	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 <b>service-policy</b> 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。
<b>policy-map</b>	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。
<b>set connection</b>	接続の値を設定します。
<b>show running-config policy-map</b>	現在のポリシー マップ コンフィギュレーションをすべて表示します。
<b>show service-policy</b>	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。

### コマンドデフォルト

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルートマップ 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 変更内容  
ス

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、特定のユーザーに異なるデフォルトルートを提供します。宛先への明示ルートが ASA に設定されていない場合、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 packets 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、名前でも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 packets 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 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
```

## 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	
ト	
cs	

## コマンドデフォルト

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。

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

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。

### 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

次の表は、このコマンドを入力できるモードを示しています。

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

### コマンド履歴

リリース 変更内容  
 ス

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
<b>crypto ipsec profile</b>	新しい IPsec プロファイルを作成します。
<b>responder-only</b>	VTI トンネルインターフェイスをレスポンド専用モードに設定します。
<b>set pfs</b>	PFS グループを IPsec プロファイル設定に使用するよう指定します。

コマンド	説明
<b>set security-association lifetime</b>	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。

### コマンド 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。

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

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、名前でも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うちに、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。

### コマンド 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。

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

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 ipv6next-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。

### コマンド 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。

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

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、特定のユーザー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、名前でも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。

### コマンドデフォルト

このコマンドは、デフォルトでディセーブルになっています。

### コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

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 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、名前ですべての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 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 コマンドを使用すると、ネクストホップをネイバーに送信されたすべてのルートに設定します。

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。

### コマンドデフォルト

このコマンドは、デフォルトでディセーブルになっています。

### コマンドモード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルートマップ 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 変更内容  
ス

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 packets 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、名前でも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 モニター 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** [ シーケンス番号 ] **track** [ tracked-object-number ]

**no set ip next-hop verify-availability** [ シーケンス番号 ] **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。

### コマンド 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。

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

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。

### コマンドデフォルト

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。

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

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（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。
<i>delay</i>	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。
<i>loading</i>	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。
<i>metric-value</i>	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。
<i>mtu</i>	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。

## コマンドデフォルト

デフォルトの動作や値はありません。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

7.0(1) このコマンドが追加されました。

---

**リリース** 変更内容
 

---

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
<b>match interface</b>	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。
<b>match ip next-hop</b>	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。
<b>route-map</b>	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。

### コマンドデフォルト

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルートマップ 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
<b>match interface</b>	指定したい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。
<b>route-map</b>	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。
<b>set metric</b>	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。デフォルトに戻るには、`no` 形式のコマンドを使用します。

**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。

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

**コマンド 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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルートマップ 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` 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。`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を使用すると、ルートマップのすべての一致基準を満たした場合に実行する再配布 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** グループ [ **group14** ]

**no set pfs Diffie-Hellman** グループ [ **group14** ]

## 構文の説明

*Diffie-Hellman group* *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。

## 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

次の表は、このコマンドを入力できるモードを示しています。

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

## コマンド履歴

リリース 変更内容

9.16(1) **group31** コマンドオプションのサポートが追加されました。

9.15(1) **group2** および **group5** コマンドオプションのサポートが削除されました。

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。

9.7(1) このコマンドが追加されました。

## 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
<b>crypto ipsec profile</b>	新しい IPsec プロファイルを作成します。
<b>responder-only</b>	VTI トンネルインターフェイスをレスポンド専用モードに設定します。
<b>set ikev1 transform-set</b>	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。
<b>set security-association lifetime</b>	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。
<b>set trustpoint</b>	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。

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。

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。

## 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

次の表は、このコマンドを入力できるモードを示しています。

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

## コマンド履歴

リリー 変更内容  
ス

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せん。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
<b>crypto ipsec profile</b>	新しい IPsec プロファイルを作成します。
<b>responder-only</b>	VTI トンネル インターフェイスをレスポンド専用モードに設定します。
<b>set ikev1 transform-set</b>	IKEv1 変換セットを IPsec プロファイル設定に使用するよう指定します。
<b>set pfs</b>	PFS グループを IPsec プロファイル設定に使用するよう指定します。
<b>set trustpoint</b>	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。

## 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

次の表は、このコマンドを入力できるモードを示しています。

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

## コマンド履歴

リリース 変更内容  
 ス

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
<b>crypto ipsec profile</b>	新しい IPsec プロファイルを作成します。
<b>responder-only</b>	VTI トンネルインターフェイスをレスポнда専用モードに設定します。
<b>set ikev1 transform-set</b>	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 pfs	PFS グループを IPsec プロファイル設定に使用するよう指定します。



# 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。

## setup

### 構文の説明

このコマンドには引数またはキーワードはありません。

### コマンドデフォルト

デフォルトの動作や値はありません。

### コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

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、XREF 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: 設定プロンプト

プロンプト	説明
Pre-configure Firewall now through interactive prompts [yes]?	<b>yes</b> または <b>no</b> の入力。 <b>yes</b> と入力すると、セットアップが実行されます。 <b>no</b> 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]:	<b>routed</b> または <b>transparent</b> の入力。
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]?	<b>yes</b> または <b>no</b> の入力。
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 <b>Sep</b> 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、 <b>20:54:44</b> 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。

プロンプト	説明
Use this configuration and save to flash (yes)?	<p><b>yes</b>または<b>no</b>の入力。<b>yes</b>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。</p> <p><b>no</b>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。</p> <p>Pre-configure Firewall now through interactive prompts [yes]?</p> <p>セットアップを終了する場合は <b>Ctrl + Z</b> を入力し、プロンプトを繰り返す場合は <b>yes</b> を入力します。</p>

## 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
<b>configure factory-default</b>	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。

### コマンド 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。

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

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無効にします。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無効にします。

### 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
ciscoasa(config-route-map)# set weight 200
```

# sfr

ASA FirePOWER モジュールにトラフィックを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

<b>fail-close</b>	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。
<b>fail-open</b>	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。
<b>monitor-only</b>	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。

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

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 で **sfr** コマンドを設定する前後に、Secure Firewall Management Center（旧 Firepower Management Center）を使用してモジュールで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 とは別のアプリケーションとして実行します。ただし、AIP SSM/SSC 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の **sfr** コマンドを適用すると、トラフィックは次のように ASA とモジュールを通過します。

1. トラフィックが 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 に返送されません。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 を出ます。

## ASA の機能との互換性

ASA には、HTTP インспекションを含む、多数の高度なアプリケーション インспек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спек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と制御です。

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спек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спекションを設定しないでください。ASA FirePOWER インспекションとクラウド Web セキュリティのインспек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спек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спек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спекションも含まれます。
- Mobile User Security (MUS) サーバーを有効にしないでください。このサーバーは、ASA FirePOWER モジュールとの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、その転送の時点からトラフィックの検査を開始します。古いインспекションのステータスは転送されません。

## モニター専用モード

モニター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ようになっていたかをユーザーに通知します。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 上でモニター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することはできません。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ー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
```

次の例では、10.1.1.0 ネットワークと 10.2.1.0 ネットワーク宛てのすべての IP トラフィックが ASA FirePOWER モジュールに誘導され、何らかの理由でモジュールに障害が発生した場合は、すべてのトラフィックの通過が許可されます。

```
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
<b>class</b>	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。

コマンド	説明
<b>class-map</b>	ポリシー マップ用にトラフィックを識別します。
<b>cxsc</b>	ASA CX モジュールにトラフィックをリダイレクトします。
<b>hw-module module reload</b>	モジュールをリロードします。
<b>hw-module module reset</b>	リセットを実行してから、モジュールをリロードします。
<b>hw-module module shutdown</b>	モジュールをシャットダウンします。
<b>policy-map</b>	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。
<b>show asp table classify domain sfr</b>	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。
<b>show module</b>	モジュールのステータスを表示します。
<b>show running-config policy-map</b>	現在のポリシー マップ コンフィギュレーションをすべて表示します。
<b>show service-policy</b>	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。
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。



- (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。

## コマンドデフォルト

**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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ク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ない場合に実装されます。そのため、レート計算は、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 コンフィギュレーション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せん。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
<b>class</b>	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。
<b>police</b>	QoS ポリシングをイネーブルにします。
<b>policy-map</b>	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。
<b>priority</b>	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。
<b>show service-policy</b>	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）。

## コマンドデフォルト

デフォルト設定はありません。

## コマンドモード

次の表に、コマンドを入力できるモードを示します。

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

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
<b>basic-mapping-rule</b>	MAP ドメインの基本マッピングルールを設定します。
<b>default-mapping-rule</b>	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。
<b>ipv4-prefix</b>	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。
<b>ipv6-prefix</b>	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。
<b>map-domain</b>	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。
<b>share-ratio</b>	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。
<b>show map-domain</b>	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。
<b>start-port</b>	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。

## 翻訳について

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