
# crypto ca authenticate ～ crypto map set trustpoint コマンド

## crypto ca authenticate

トラストポイントに関連付けられた CA 証明書をインストールして認証するには、グローバル コンフィギュレーション モードで **crypto ca authenticate** コマンドを使用します。CA 証明書を削除するには、このコマンドの **no** 形式を使用します。

**crypto ca authenticate** *trustpoint* [**fingerprint** *hexvalue*] [**nointeractive]**

**no crypto ca authenticate** *trustpoint*

**シンタックスの説明**

| | |
|---|---|
| **fingerprint** | FWSM が CA 証明書の認証に使用する英数字のハッシュ値を指定します。フィンガープリントを指定すると、FWSM は計算された CA 証明書のフィンガープリントと比較し、両方の値が一致する場合に限り、証明書を受け入れます。フィンガープリントを指定しないと、FWSM は計算されたフィンガープリントを表示し、証明書を受け入れるかどうかを確認します。 |
| *hexvalue* | フィンガープリントの 16 進数値を識別します。 |
| **nointeractive** | 非対話モードを使用して、このトラストポイントの CA 証明書を取得します。これを使用するのは、デバイス マネージャだけです。この場合、フィンガープリントを指定しないと、FWSM は質問を表示せずに証明書を受け入れます。 |
| *trustpoint* | CA 証明書の取得先となるトラストポイントを指定します。名前の最大長は、128 文字です。 |

**デフォルト**

このコマンドにはデフォルト動作またはデフォルト値はありません。

**コマンド モード**

次の表に、コマンドを入力できるモードを示します。

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

**コマンド履歴**

| リリース | 変更 |
|---|---|
| 3.1(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**

トラストポイントに SCEP エンロールメントが設定されている場合、CA 証明書は SCEP によりダウンロードされます。設定されていない場合、FWSM は、base-64 形式の CA 証明書を端末にペーストするように要求します。

このコマンドの起動は、実行コンフィギュレーションの一部にはなりません。

**例**

次に、FWSM で CA の証明書を要求する例を示します。CA から証明書が送信されると、FWSM は管理者に対して、CA 証明書のフィンガープリントを調べ、CA の証明書を確認するように要求します。FWSM の管理者は、表示されたフィンガープリントの値が、既知の正しい値と一致しているかどうかを確認する必要があります。FWSM により表示されたフィンガープリントが正しい値と一致していれば、有効な証明書として受け入れます。

```
hostname(config)# crypto ca authenticate myca
Certificate has the following attributes:
Fingerprint: 0123 4567 89AB CDEF 0123
Do you accept this certificate? [yes/no] y#
hostname(config)#
```

次の例では、トラストポイント tp9 に端末ベース（手動）エンロールメントが設定されています。この場合、FWSM は管理者に対し、CA 証明書を端末にペーストするように要求します。証明書のフィンガープリントが表示されたあと、FWSM により、証明書を保持するかの確認プロンプトが表示されます。

```
hostname(config)# crypto ca authenticate tp9
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

MIIDjjCCAvegAwIBAgIQejIaQ3SJRIBMHcvDdgOsKTANBgkqhkiG9w0BAQUFADBA
MQswCQYDVQQGEwJVUzELMAkGA1UECBMCTUExETAPBgNVBAcTCEZyYW5rbGluMREw
DwYDVQQDEwhCcmlhbnNDQTAeFw0wMjEwMTcxODE5MTJaFw0wNjEwMjQxOTU3MDha
MEAxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJNQTERMA8GA1UEBxMIRnJhbmtsaW4x
ETAPBgNVBAMTCEJyaWFuc0NBMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCd
jXEPvNnkZD1bKzahbTHuRot1T8KRUbCP5aWKfqViKJENzI2GnAheArazsAcc4Eaz
LDnpuyyqa0j5LA3MI577MoN1/nll018fbpqOf9eVDPJDkYTvtZ/X3vJgnEjTOWyz
T0pXxhdU1b/jgqVE74OvKBzU7A2yoQ2hMYzwVbGkewIDAQABo4IBhzCCAYMwEwYJ
KwYBBAGCNxQCBAYeBABDAEEwCwYDVR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8w
HQYDVR0OBBYEFBHr3holowFDmniI3FBwKpSEucdtMIIBGwYDVR0fBIIBEjCCAQ4w
gcaggcOggcCGgb1sZGFwOi8vL0NOPUJyaWFuc0NBLENOPWJyaWFuLXcyay1zdnIs
Q049Q0RQLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENO
PUNvbmZpZ3VyYXRpb24sREM9YnJpYW5wZGMsREM9YmRzLERDPWNvbT9jZXJ0aWZp
Y2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Y2xhc3M9Y1JMRGlzdHJpYnV0
aW9uUG9pbnQwQ6BBoD+GPWh0dHA6Ly9icmlhbi13Mmstc3ZyLmJyaWFucGRjLmJk
cy5jb20vQ2VydEVucm9sbC9CcmlhbnNDQS5jcmwwEAYJKwYBBAGCNxUBBAMCAQEw
DQYJKoZIhvcNAQEFBQADgYEAdLhc4Za3AbMjRq66xH1qJWxKUzd4nE9wOrhGgA1r
j4B/Hv2K1gUie34xGqu9OpwqvJgp/vCU12Ciykb1YdSDy/PxN4KtR9Xd1JDQMbu5
f20AYqCG5vpPWavCgmgTLcdwKa3ps1YSWGkhWmScHHSiGg1a3tevYVwhHNPA4mWo
7sQ=

Certificate has the following attributes:
Fingerprint: 21B598D5 4A81F3E5 0B24D12E 3F89C2E4
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
hostname(config)#
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **crypto ca enroll** | CA のエンロールメントを開始します。 |
| **crypto ca import certificate** | 手動エンロールメント要求に対する応答として CA から戻された証明書をインストールします。また、トラストポイントに PKS12 データをインポートします。 |
| **crypto ca trustpoint** | 特定のトラストポイントのトラストポイント サブモードを開始します。 |

# crypto ca certificate chain

指定したトラストポイントの証明書チェーン コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **crypto ca certificate chain** コマンドを使用します。グローバル コンフィギュレーション モードに戻るには、このコマンドの **no** 形式を使用するか、**exit** コマンドを使用します。

**crypto ca certificate chain** *trustpoint*

**[no] crypto ca certificate chain** *trustpoint*

**シンタックスの説明**

| | |
|---|---|
| *trustpoint* | 証明書チェーンを設定するトラストポイントを指定します。 |

**デフォルト**

このコマンドにはデフォルト値はありません。

**コマンド モード**

次の表に、コマンドを入力できるモードを示します。

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

**コマンド履歴**

| リリース | 変更 |
|---|---|
| 3.1(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 CA 証明書チェーン サブモードを開始する例を示します。

```
hostname<config># crypto ca certificate chain central
hostname<config-cert-chain>#
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **clear configure crypto ca trustpoint** | すべてのトラストポイントを削除します。 |

# crypto ca certificate map

CA 証明書マップ モードを開始するには、グローバル コンフィギュレーション モードで、**crypto ca configuration map** コマンドを使用します。このコマンドを実行すると、ca 証明書マップ モードになります。このグループのコマンドを使用して、証明書マッピング ルールの優先順位リストを保守します。シーケンス番号により、マッピング ルールの順序を指定します。

crypto CA コンフィギュレーション マップ ルールを削除するには、このコマンドの **no** 形式を使用します。

**crypto ca certificate map** *sequence-number*

**no crypto ca certificate map** [*sequence-number*]

## シンタックスの説明

| | |
|---|---|
| *sequence-number* | 作成する証明書マップ ルールの番号を指定します。範囲は、1 ～ 65535 です。この番号は、証明書マップ ルールにトンネル グループをマップするトンネル グループ マップの作成時に使用できます。 |

## デフォルト

このコマンドには、デフォルトの動作または値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更 |
|---|---|
| 3.1(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

このコマンドを発行すると、FWSM は CA 証明書マップ コンフィギュレーション モードになり、証明書の発行者およびサブジェクトの Distinguished Name（DN; 識別名）に基づいてルールを設定できます。これらのルールの一般的な形式は、次のとおりです。

*DN match-criteria match-value*

*DN* は、*subject-name* または *issuer-name* です。DN は、ITU-T X.509 標準規格に定義されています。証明書フィールドのリストについては、関連コマンドを参照してください。

*match-criteria* は、次の式または演算子で構成されます。

| | |
|---|---|
| **attr** *tag* | 比較を、Common Name（CN; 一般名称）などの特定の DN 属性に制限します。 |
| **co** | 含まれる |
| **eq** | 等しい |
| **nc** | 含まれない |
| **ne** | 等しくない |

DN 照合の文字列は、大文字と小文字が区別されます。

## 例

次に、シーケンス番号 1（ルール # 1）で CA 証明書マップ モードを開始し、サブジェクト名の CN 属性が pat と一致する必要があることを指定する例を示します。

```
hostname(config)# crypto ca certificate map 1
hostname(ca-certificate-map)# subject-name attr cn eq pat
hostname(ca-certificate-map)#
```

次に、シーケンス番号 1 で CA 証明書マップ モードを開始し、サブジェクト名のどこかに値 cisco が含まれていることを指定する例を示します。

```
hostname(config)# crypto ca certificate map 1
hostname(ca-certificate-map)# subject-name co cisco
hostname(ca-certificate-map)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **issuer-name** | ルール エントリを、IPSec ピア 証明書の発行者 DN に適用します。 |
| **subject-name（crypto ca 証明書マップ）** | ルール エントリを、IPSec ピア 証明書のサブジェクト DN に適用します。 |
| **tunnel-group-map enable** | **crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリにトンネル グループを対応付けます。 |

# crypto ca crl request

指定したトラストポイントの設定パラメータに基づいて CRL を要求するには、crypto ca トラストポイント コンフィギュレーション モードで **crypto ca crl request** コマンドを使用します。

**crypto ca crl request** *trustpoint*

## シンタックスの説明

| | |
|---|---|
| *trustpoint* | トラストポイントを指定します。最大文字数は、128 です。 |

## デフォルト

このコマンドには、デフォルトの動作または値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更 |
|---|---|
| 3.1(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

このコマンドの起動は、実行コンフィギュレーションの一部にはなりません。

## 例

次に、central という名前のトラストポイントに基づいて CRL を要求する例を示します。

```
hostname(config)# crypto ca crl request central
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **crl configure** | crl configure モードを開始します。 |

# crypto ca enroll

CA のエンロールメント プロセスを開始するには、グローバル コンフィギュレーション モードで **crypto ca enroll** コマンドを使用します。このコマンドを正しく実行するには、トラストポイントが正しく設定されている必要があります。

**crypto ca enroll** *trustpoint* [**noconfirm**]

## シンタックスの説明

| | |
|---|---|
| **noconfirm** | (任意) すべてのプロンプトを抑制します。プロンプトを表示するエンロールメント オプションは、トラストポイントに事前設定されている必要があります。このオプションは、スクリプト、ASDM、または同様の他の非対話モード用です。 |
| *trustpoint* | エンロールメントを行うトラストポイントの名前を指定します。最大文字数は、128 です。 |

## デフォルト

このコマンドには、デフォルトの動作または値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更 |
|---|---|
| 3.1(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

トラストポイントに SCEP エンロールメントが設定されている場合、FWSM はすぐに CLI プロンプトを表示し、コンソールにはステータス メッセージが非同期で表示されます。トラストポイントに手動エンロールメントが設定されている場合、FWSM は base-64 コード化 PKCS10 証明書要求をコンソールに書き込み、CLI プロンプトを表示します。

このコマンドは対話プロンプトを生成しますが、プロンプトは参照するトラストポイントの設定ステートに応じて異なります。

## 例

次に、SCEP エンロールメントを使用して、トラストポイント tp1 で ID 証明書をエンロールする例を示します。FWSM により、トラストポイント設定に保管されていない情報が要求されます。

```
hostname(config)# crypto ca enroll tp1
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
% password to the CA Administrator in order to revoke your certificate.
% For security reasons your password will not be saved in the configuration.
% Please make a note of it.
Password:
Re-enter password:
% The fully-qualified domain name in the certificate will be: xyz.example.com
% The subject name in the certificate will be: xyz.example.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA [yes/no]: yes
% Certificate request sent to Certificate authority.
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

hostname(config)#
```

次に、CA 証明書の手動エンロールメントのコマンド例を示します。

hostname(config)# **crypto ca enroll tp1**

```
% Start certificate enrollment ..
% The fully-qualified domain name in the certificate will be: xyz.example.com
% The subject name in the certificate will be: wb-2600-3.example.com
if serial number not set in trustpoint, prompt:
% Include the router serial number in the subject name? [yes/no]: no
If ip-address not configured in trustpoint:
% Include an IP address in the subject name? [no]: yes
Enter Interface name or IP Address[]: 1.2.3.4
Display Certificate Request to terminal? [yes/no]: y
Certificate Request follows:
MIIBFTCBwAIBADA6MTgwFAYJKoZIhvcNAQkIEwcxLjIuMy40MCAGCSqGSIb3DQEJ
AhYTd2ItMjYwMC0zLmNpc2NvLmNvbTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQDT
IdvHa4D5wXZ+40sKQV7Uek1E+CC6hm/LRN3p5ULW1KF6bxhA3Q5CQfh4jDxobn+A
Y8GoeceulS2Zb+mvgNvjAgMBAAGgITAfBgkqhkiG9w0BCQ4xEjAQMA4GA1UdDwEB
/wQEAwIFoDANBgkqhkiG9w0BAQQFAANBACDhnrEGBVtltG7hp8x6Wz/dgY+ouWcA
lzy7QpdGhb1du2P81RYn+8pWRA43cikXMTeM4ykEkZhLjDUgv9t+R9c=

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: no
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **crypto ca authenticate** | このトラストポイント用の CA 証明書を取得します。 |
| **crypto ca import pkcs12** | 手動エンロールメント要求に対する応答として CA から戻された証明書をインストールします。また、トラストポイントに PKS12 データをインポートします。 |
| **crypto ca trustpoint** | 特定のトラストポイントのトラストポイント サブモードを開始します。 |

# crypto ca export

トラストポイント設定に関連付けられた鍵および証明書を PKCS12 形式でエクスポートするには、グローバル コンフィギュレーション モードで **crypto ca export** コマンドを使用します。

**crypto ca export** *trustpoint* ***pkcs12*** *passphrase*

## シンタックスの説明

| | |
|---|---|
| *passphrase* | PKCS12 ファイルをエクスポート用に暗号化するために使用するパスフレーズを指定します。 |
| ***pkcs12*** | トラストポイント設定のエクスポートに使用する公開鍵暗号化規格を指定します。 |
| *trustpoint* | 証明書および鍵をエクスポートするトラストポイントの名前を指定します。トラストポイントが RSA 鍵を使用している場合、エクスポートされた鍵のペアには、トラストポイントと同じ名前が割り当てられます。 |

## デフォルト

このコマンドにはデフォルト値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更 |
|---|---|
| 3.1(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

このコマンドの起動は、アクティブ コンフィギュレーションの一部にはなりません。PKCS12 データは、端末に書き込まれます。

## 例

次に、パスコードとして xxyyzz を使用し、トラストポイント central の PKCS12 データをエクスポートする例を示します。

```
hostname(config)# crypto ca export central pkcs12 xxyyzz

Exported pkcs12 follows:

[ PKCS12 data omitted ]

---End - This line not part of the pkcs12---
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **crypto ca import pkcs12** | 手動エンロールメント要求に対する応答として CA から戻された証明書をインストールします。また、トラストポイントに PKS12 データをインポートします。 |
| **crypto ca authenticate** | このトラストポイント用の CA 証明書を取得します。 |
| **crypto ca enroll** | CA のエンロールメントを開始します。 |
| **crypto ca trustpoint** | 特定のトラストポイントのトラストポイント サブモードを開始します。 |

# crypto ca import

手動エンロールメント要求の応答として CA から受信した証明書をインストールするか、PKCS12 データを使用してトラストポイントの証明書および鍵のペアをインポートするには、グローバル コンフィギュレーション モードで **crypto ca import** コマンドを使用します。FWSM は、base-64 形式でテキストを端末にペーストするよう要求します。

**crypto ca import** *trustpoint* **certificate** [ **nointeractive** ]

**crypto ca import** *trustpoint* **pkcs12** *passphrase* [ **nointeractive** ]

**シンタックスの説明**

| | |
|---|---|
| *trustpoint* | インポート処理に関連付けるトラストポイントを指定します。最大文字数は、128 です。PKCS12 データをインポートし、トラストポイントが RSA 鍵を使用している場合、インポートした鍵のペアには、トラストポイントと同じ名前が割り当てられます。 |
| **certificate** | FWSM が、トラストポイントにより提示された CA から証明書をインポートするように指示します。 |
| ***pkcs12*** | FWSM が、PKCS12 形式を使用して、トラストポイントの証明書および鍵のペアをインポートするように指示します。 |
| *passphrase* | PKCS12 データの復号化に使用するパスフレーズを指定します。 |
| **nointeractive** | （任意）証明書を非対話モードでインポートします。すべてのプロンプトが抑制されます。このオプションは、スクリプト、ASDM、または同様の他の非対話モード用です。 |

**デフォルト**

このコマンドには、デフォルトの動作または値はありません。

**コマンド モード**

次の表に、コマンドを入力できるモードを示します。

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

**コマンド履歴**

| リリース | 変更 |
|---|---|
| 3.1(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 Main の証明書を手動でインポートする例を示します。

```
hostname(config)# crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be:
securityappliance.example.com

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
[ certificate data omitted ]
quit
INFO: Certificate successfully imported
```

次に、トラストポイント central に PKCS12 データを手動でインポートする例を示します。

```
hostname(config)# crypto ca import central pkcs12

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **crypto ca export** | トラストポイントの証明書および鍵のペアを、PKCS12 形式でエクスポートします。 |
| **crypto ca authenticate** | トラストポイント用の CA 証明書を取得します。 |
| **crypto ca enroll** | CA のエンロールメントを開始します。 |
| **crypto ca trustpoint** | 特定のトラストポイントのトラストポイント サブモードを開始します。 |

# crypto ca trustpoint

トラストポイントを追加して、トラストポイント コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **crypto ca trustpoint** コマンドを使用します。指定したトラストポイントを削除するには、このコマンドの **no** 形式を使用します。このコマンドは、トラストポイント情報を管理します。トラストポイントは、CA が発行した証明書に基づいて CA 識別情報を提示し、可能な場合にはデバイスの識別情報も提示します。trustpoint コマンドは、FWSM が CA 証明書を取得する方法、FWSM が自己の証明書を CA から取得する方法、および CA が発行するユーザ証明書の認証ポリシーなど、CA 特有の設定パラメータを管理します。

**crypto ca trustpoint** *trustpoint-name*

**no crypto ca trustpoint** *trustpoint-name* [**noconfirm/**

## シンタックスの説明

| | |
|---|---|
| ***noconfirm*** | （任意）すべての対話プロンプトを抑制します。 |
| *trustpoint-name* | 管理するトラストポイントの名前を指定します。名前の最大長は、128 文字です。 |

## デフォルト

このコマンドには、デフォルトの動作または値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更 |
|---|---|
| 3.1(1) | このコマンドのサポートが追加されました。 |

## 使用上のガイドライン

トラストポイントは、CA が発行した証明書に基づいて CA 識別情報を提示し、可能な場合にはデバイスの識別情報も提示します。trustpoint コマンドは、FWSM が CA 証明書を取得する方法、FWSM が自己の証明書を CA から取得する方法、および CA が発行するユーザ証明書の認証ポリシーなど、CA 特有の設定パラメータを管理します。

## 例

次に、トラストポイント central を管理するために CA トラストポイント モードを開始する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure crypto ca trustpoint** | すべてのトラストポイントを削除します。 |
| **crypto ca authenticate** | このトラストポイント用の CA 証明書を取得します。 |
| **crypto ca certificate map** | crypto ca 証明書マップ モードを開始します。証明書ベースの ACL（アクセス制御リスト）を定義します。 |
| **crypto ca crl request** | 指定したトラストポイントの設定パラメータに基づいて、CRL を要求します。 |
| **crypto ca import** | 手動エンロールメント要求に対する応答として CA から戻された証明書をインストールします。また、トラストポイントに PKS12 データをインポートします。 |

# crypto dynamic-map match address

ダイナミック暗号マップ エントリを定義するには、グローバル コンフィギュレーション モードで **crypto dynamic-map match address** コマンドを使用します。暗号マップ エントリからアクセス リストを削除するには、このコマンドの **no** 形式を使用します。このコマンドの追加情報については、crypto map match address コマンドを参照してください。

**crypto dynamic-map** *dynamic-map-name dynamic-seq-num* **match address** *acl_name*

**no crypto dynamic-map** *dynamic-map-name dynamic-seq-num* **match address** *acl_name*

## シンタックスの説明

| | |
|---|---|
| *acl-name* | ダイナミック暗号マップ エントリを照合するアクセス リストを指定します。 |
| *dynamic-map-name* | ダイナミック暗号マップ セットの名前を指定します。 |
| *dynamic-seq-num* | ダイナミック暗号マップ エントリに対応したシーケンス番号を指定します。 |

## デフォルト

このコマンドには、デフォルトの動作または値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更 |
|---|---|
| 1.1(1) | このコマンドが追加されました。 |
| 3.1(1) | このコマンドが、**crypto dynamic-map** コマンドから変更されました。 |

## 例

次に、aclist1 という名前のアクセス リストのアドレスと照合する crypto dynamic-map コマンドの使用例を示します。

```
hostname(config)# crypto dynamic-map mymap 10 match address aclist1
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure crypto dynamic-map** | すべてのダイナミック暗号マップの全設定をクリアします。 |
| **show running-config crypto dynamic-map** | すべてのダイナミック暗号マップの全設定を表示します。 |

# crypto dynamic-map set peer

ダイナミック暗号マップ エントリを定義するには、グローバル コンフィギュレーション モードで **crypto dynamic-map set peer** コマンドを使用します。暗号マップ エントリからアクセス リストを削除するには、このコマンドの **no** 形式を使用します。このコマンドの追加情報については、**crypto map set peer** コマンドを参照してください。

**crypto dynamic-map** *dynamic-map-name dynamic-seq-num* **set peer** *ip_address* | *hostname*

**no crypto dynamic-map** *dynamic-map-name dynamic-seq-num* **set peer** *ip_address* | *hostname*

## シンタックスの説明

| | |
|---|---|
| *dynamic-map-name* | ダイナミック暗号マップ セットの名前を指定します。 |
| *dynamic-seq-num* | ダイナミック暗号マップ エントリに対応したシーケンス番号を指定します。 |
| *ip_address* | ダイナミック暗号マップ エントリのピアを、**name** コマンドで定義した IP アドレスで指定します。 |
| *hostname* | ダイナミック暗号マップ エントリのピアを、**name** コマンドで定義したホスト名で指定します。 |

## デフォルト

このコマンドには、デフォルトの動作または値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更 |
|---|---|
| 1.1(1) | このコマンドが追加されました。 |
| 3.1(1) | このコマンドが、**crypto dynamic-map** コマンドから変更されました。 |

## 例

次に、IP アドレス 10.0.0.1 を、mymap という名前のダイナミック マップのピアとして設定する例を示します。

```
hostname(config)# crypto dynamic-map mymap 10 set peer 10.0.0.1
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure crypto dynamic-map** | すべてのダイナミック暗号マップの全設定をクリアします。 |
| **show running-config crypto dynamic-map** | すべてのダイナミック暗号マップの全設定を表示します。 |

# crypto dynamic-map set pfs

ダイナミック暗号マップ エントリを定義するには、グローバル コンフィギュレーション モードで **crypto dynamic-map set pfs** コマンドを使用します。暗号マップ エントリからアクセス リストを削除するには、このコマンドの **no** 形式を使用します。このコマンドの追加情報については、**crypto map set pfs** コマンドを参照してください。

**crypto dynamic-map** *dynamic-map-name dynamic-seq-num* **set pfs [group1 | group2 | group5 | group 7]**

**no crypto dynamic-map** *dynamic-map-name dynamic-seq-num* **set pfs [group1 | group2 | group5 | group 7]**

## シンタックスの説明

| | |
|---|---|
| *dynamic-map-name* | ダイナミック暗号マップ セットの名前を指定します。 |
| *dynamic-seq-num* | ダイナミック暗号マップ エントリに対応したシーケンス番号を指定します。 |
| **group1** | 新しい Diffie-Hellman 交換の実行時に、IPSec が 768 ビット Diffie-Hellman プライム モジュラス グループを使用するように指定します。 |
| **group2** | 新しい Diffie-Hellman 交換の実行時に、IPSec が 1024 ビット Diffie-Hellman プライム モジュラス グループを使用するように指定します。 |
| **group5** | 新しい Diffie-Hellman 交換の実行時に、IPSec が 1536 ビット Diffie-Hellman プライム モジュラス グループを使用するように指定します。 |
| **group7** | IPSec が、Movian VPN クライアントなどに対し、楕円曲線フィールドのサイズが 163 ビットである group7（ECC）を使用するように指定します。 |
| **set pfs** | ダイナミック暗号マップ エントリの新しいセキュリティ アソシエーションを要求するとき、または新しいセキュリティ アソシエーションの要求を受信するときに、IPSec が Perfect Forward Secrecy（PFS）を要求するように設定します。 |

## デフォルト

このコマンドには、デフォルトの動作または値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更 |
|---|---|
| 1.1(1) | このコマンドが追加されました。 |
| 3.1(1) | このコマンドが、**crypto dynamic-map** コマンドから変更されました。 |

## 使用上のガイドライン

**match address**、**set peer**、および **set pfs** などの **crypto dynamic-map** コマンドは、**crypto map** コマンドの項目で説明されています。ピアのネゴシエーション開始時にローカル コンフィギュレーションに PFS が指定されている場合、ピアは PFS 交換を実行する必要があります。実行しない場合、ネゴシエーションに失敗します。ローカル コンフィギュレーションにグループが指定されていない場合、FWSM はデフォルトの group2 を使用します。ローカル コンフィギュレーションに PFS が指定されていない場合、ピアからの PFS のオファーはすべて受け入れられます。

Cisco VPN クライアントと通信する場合、FWSM は PFS 値を使用せず、フェーズ 1 の実行中にネゴシエートされた値を使用します。

## 例

次に、mymap 10 というダイナミック暗号マップについて新しいセキュリティ アソシエーションをネゴシエートする場合、必ず PFS を使用するように指定する例を示します。指定グループは、group2 です。

```
hostname(config)# crypto dynamic-map mymap 10 set pfs group2
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure crypto dynamic-map** | すべてのダイナミック暗号マップの全設定をクリアします。 |
| **show running-config crypto dynamic-map** | すべてのダイナミック暗号マップの全設定を表示します。 |

# crypto dynamic-map set reverse route

ダイナミック暗号マップ エントリを定義するには、グローバル コンフィギュレーション モードで **crypto dynamic-map set reverse route** コマンドを使用します。暗号マップ エントリからアクセス リストを削除するには、このコマンドの **no** 形式を使用します。このコマンドの追加情報については、crypto map set reverse-route コマンドを参照してください。

**crypto dynamic-map** *dynamic-map-name dynamic-seq-num* **set reverse route**

**no crypto dynamic-map** *dynamic-map-name dynamic-seq-num* **set reverse route**

## シンタックスの説明

| | |
|---|---|
| *dynamic-map-name* | 暗号マップ セットの名前を指定します。 |
| *dynamic-seq-num* | 暗号マップ エントリに割り当てる番号を指定します。 |

## デフォルト

このコマンドにはデフォルトの値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更 |
|---|---|
| 1.1(1) | このコマンドが追加されました。 |
| 3.1(1) | このコマンドが、**crypto dynamic-map** コマンドから変更されました。 |

## 例

次に、mymap というダイナミック暗号マップの RRI をイネーブルにする例を示します。

```
hostname(config)# crypto dynamic-map mymap 10 set reverse route
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure crypto dynamic-map** | すべてのダイナミック暗号マップの全設定をクリアします。 |
| **show running-config crypto dynamic-map** | すべてのダイナミック暗号マップの全設定を表示します。 |

# crypto dynamic-map set security-association lifetime

ダイナミック暗号マップ エントリを定義するには、グローバル コンフィギュレーション モードで **crypto dynamic-map set security-association lifetime** コマンドを使用します。暗号マップ エントリからアクセス リストを削除するには、このコマンドの **no** 形式を使用します。このコマンドの追加情報については、**crypto map set security-association lifetime** コマンドを参照してください。

**crypto dynamic-map** *dynamic-map-name dynamic-seq-num* **set security-association lifetime seconds** *seconds* | **kilobytes** *kilobytes*

**no crypto dynamic-map** *dynamic-map-name dynamic-seq-num* **set security-association lifetime seconds** *seconds* | **kilobytes** *kilobytes*

## シンタックスの説明

| | |
|---|---|
| *dynamic-map-name* | ダイナミック暗号マップ セットの名前を指定します。 |
| *dynamic-seq-num* | ダイナミック暗号マップ エントリに対応したシーケンス番号を指定します。 |
| *kilobytes* | セキュリティ アソシエーションが期限切れになる前に、そのセキュリティ アソシエーションを使用してピア間で通信できるトラフィック量（キロバイト）を指定します。デフォルトは、4,608,000 KB です。 |
| *seconds* | セキュリティ アソシエーションの有効存続時間を秒数で指定します。デフォルトは、28,800 秒（8 時間）です。 |

## デフォルト

kilobytes のデフォルト値は 4,608,000 KB、seconds のデフォルト値は 28,800 秒です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更 |
|---|---|
| 1.1(1) | このコマンドが追加されました。 |
| 3.1(1) | このコマンドが、**crypto dynamic-map** コマンドから変更されました。 |

## 例

次に、mymap というダイナミック暗号マップのセキュリティ アソシエーションのライフタイムを秒数で指定する例を示します。

```
hostname(config)# crypto dynamic-map mymap 10 set security-association lifetime
seconds 1400
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure crypto dynamic-map** | すべてのダイナミック暗号マップの全設定をクリアします。 |
| **show running-config crypto dynamic-map** | すべてのダイナミック暗号マップの全設定を表示します。 |

# crypto dynamic-map set transform-set

ダイナミック暗号マップ エントリを定義するには、グローバル コンフィギュレーション モードで **crypto dynamic-map set transform-set** コマンドを使用します。暗号マップ エントリからアクセス リストを削除するには、このコマンドの **no** 形式を使用します。このコマンドの追加情報については、**crypto map set transform-set** コマンドを参照してください。

**crypto dynamic-map** *dynamic-map-name dynamic-seq-num* **set transform-set** *transform-set-name1* [*… transform-set-name9*]

**no crypto dynamic-map** *dynamic-map-name dynamic-seq-num* **set transform-set** *transform-set-name1* [*… transform-set-name9*]

## シンタックスの説明

| | |
|---|---|
| *dynamic-map-name* | ダイナミック暗号マップ セットの名前を指定します。 |
| *dynamic-seq-num* | ダイナミック暗号マップ エントリに対応したシーケンス番号を指定します。 |
| *transform-set-name1*<br>*transform-set-name9* | ダイナミック暗号マップ エントリに使用するトランスフォーム セット（**crypto ipsec** コマンドで定義したトランスフォーム セットの名前）を指定します。 |

**（注）** ダイナミック暗号マップ エントリには、**crypto map set transform-set** コマンド が必要です。エントリに必要なのは、トランスフォーム セットだけです。

## デフォルト

このコマンドには、デフォルトの動作または値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更 |
|---|---|
| 1.1(1) | このコマンドが追加されました。 |
| 3.1(1) | このコマンドが、**crypto dynamic-map** コマンドから変更されました。 |

## 例

次に、mymap というダイナミック暗号マップに、2 つのトランスフォーム セット（tfset1 および tfset2）を指定する例を示します。

```
hostname(config)# crypto dynamic-map mymap 10 set transform-set tfset1 tfset2
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure crypto dynamic-map** | すべてのダイナミック暗号マップの全設定をクリアします。 |
| **show running-config crypto dynamic-map** | すべてのダイナミック暗号マップの全設定を表示します。 |

# crypto ipsec df-bit

IPSec パケットの Don't Fragment（DF）ビット ポリシーを設定するには、グローバル コンフィギュレーション モードで **crypto ipsec df-bit** コマンドを使用します。

**crypto ipsec df-bit** [**clear-df** | **copy-df** | **set-df**] *interface*

## シンタックスの説明

| | |
|---|---|
| ***clear-df*** | （任意）外側の IP ヘッダーの DF ビットをクリアするように指定します。この場合、FWSM は、パケットを分割して、IPSec カプセル化に追加できます。 |
| ***copy-df*** | （任意）外側の DF ビット設定について、FWSM がオリジナル パケットを調べるように指定します。 |
| ***set-df*** | （任意）外側の IP ヘッダーの DF ビットを設定するように指定します。ただし、元のパケットの DF ビットがクリアされている場合、FWSM はパケットを分割することがあります。 |
| *interface* | インターフェイス名を指定します。 |
| token | ユーザ認証にトークン ベース サーバを使用することを指定します。 |

## デフォルト

このコマンドは、デフォルトではディセーブルです。このコマンドを、設定を指定せずにイネーブルにすると、FWSM は、デフォルトの ***copy-df*** 設定を使用します。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更 |
|---|---|
| 3.1(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

IPSec トンネルを使用した DF ビット機能により、FWSM で、カプセル化されたヘッダーの DF ビットをクリア、設定、またはコピーするかどうかを指定できます。IP ヘッダーの DF ビットは、デバイスによるパケット分割を許可するかどうかを決定します。

グローバル コンフィギュレーション モードで **crypto** ***ipsec df-bit*** コマンドを使用すると、FWSM で、カプセル化ヘッダー内の DF ビットを指定できます。

トンネル モードの IPSec トラフィックをカプセル化する場合には、DF ビットに ***clear-df*** 設定を使用します。この設定により、デバイスが使用可能な MTU（最大伝送ユニット）サイズより大きなパケットを送信できます。また、この設定は、使用可能な MTU サイズが不明な場合にも適しています。

## 例

次に、グローバル コンフィギュレーション モードで、IPSec DF ポリシーを **clear-df** に指定する例を示します。

```
hostname(config)# crypto ipsec df-bit clear-df inside
hostname(config)#
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **crypto ipsec fragmentation** | IPSec パケットのフラグメンテーション ポリシーを設定します。 |
| **show crypto ipsec df-bit** | 指定したインターフェイスの DF ビット ポリシーを表示します。 |
| **show crypto ipsec fragmentation** | 指定したインターフェイスの分割ポリシーを表示します。 |

# crypto ipsec fragmentation

IPSec パケットの分割ポリシーを設定するには、グローバル コンフィギュレーション モードで **crypto ipsec fragmentation** コマンドを使用します。

**crypto ipsec fragmentation** {**after-encryption** | **before-encryption**} *interface*

**シンタックスの説明**

| | |
|---|---|
| ***after-encryption*** | FWSM が、カプセル化の実行後に IPSec パケットを最大 MTU（最大伝送ユニット）サイズに近いサイズに分割するように指定します（事前分割をディセーブルにします）。 |
| ***before-encryption*** | FWSM が、カプセル化の実行前に IPSec パケットを最大 MTU サイズに近いサイズに分割するように指定します（事前分割をイネーブルにします）。 |
| *interface* | インターフェイス名を指定します。 |
| token | ユーザ認証にトークン ベース サーバを使用することを指定します。 |

**デフォルト**

この機能は、デフォルトではディセーブルです。

**コマンド モード**

次の表に、コマンドを入力できるモードを示します。

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

**コマンド履歴**

| リリース | 変更 |
|---|---|
| 3.1(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**

パケットが、暗号化する FWSM の発信リンクの MTU に近いサイズの場合、IPSec ヘッダーを付けてカプセル化すると、発信リンクの MTU サイズを超えることがあります。この場合、暗号化のあとでパケットが分割されるので、複号化するデバイスはプロセス パスを再構成する必要があります。IPSec VPN の事前分割を使用すると、複号化デバイスは、プロセス パスではなく高性能 CEF パスで動作するので、複号化デバイスのパフォーマンスが向上します。

IPSec VPN の事前分割では、暗号化デバイスは、IPSec SA の一部として設定されるトランスフォーム セットの情報から、カプセル化したあとのパケット サイズを事前に判別できます。パケットが出力インターフェイスの MTU を超えると判別した場合、デバイスは、暗号化する前にパケットを分割します。これにより、複号化する前のプロセス レベルの再構成が不要になるので、複号化のパフォーマンスが向上し、IPSec トラフィックの全般的なスループットも向上します。

## 例

次に、グローバル コンフィギュレーション モードで、インターフェイス上の IPSec パケットの事前分割をイネーブルにする例を示します。

```
hostname(config)# crypto ipsec fragmentation before-encryption mgmt
hostname(config)#
```

次に、グローバル コンフィギュレーション モードで、インターフェイス上の IPSec パケットの事前分割をディセーブルにする例を示します。

```
hostname(config)# crypto ipsec fragmentation after-encryption mgmt
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **crypto ipsec df-bit** | IPSec パケットの DF ビット ポリシーを設定します。 |
| **show crypto ipsec fragmentation** | IPSec パケットのフラグメンテーション ポリシーを表示します。 |
| **show crypto ipsec df-bit** | 指定したインターフェイスの DF ビット ポリシーを表示します。 |

# crypto ipsec security-association lifetime

グローバル ライフタイムの値を設定するには、グローバル コンフィギュレーション モードで、**crypto ipsec security-association lifetime** コマンドを使用します。暗号 IPSec エントリのライフタイム値をデフォルト値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。

**crypto ipsec security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}

**no crypto ipsec security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}

## シンタックスの説明

| | |
|---|---|
| *kilobytes* | セキュリティ アソシエーションが期限切れになる前に、そのセキュリティ アソシエーションを使用してピア間で通信できるトラフィック量（キロバイト）を指定します。範囲は、10 ～ 2147483647 KB です。デフォルトは、4,608,000 KB です。 |
| *seconds* | セキュリティ アソシエーションの有効存続時間を秒数で指定します。範囲は、120 ～ 214783647 秒です。デフォルトは、28,800 秒（8 時間）です。 |
| token | ユーザ認証にトークン ベース サーバを使用することを指定します。 |

## デフォルト

kilobytes のデフォルト値は 4,608,000 KB、seconds のデフォルト値は 28,800 秒です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更 |
|---|---|
| 1.1(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

**crypto ipsec security-association lifetime** コマンドでは、IPSec セキュリティ アソシエーションのネゴシエーションに使用するグローバル ライフタイム値を変更します。

IPSec セキュリティ アソシエーションでは、共有秘密鍵を使用します。これらの鍵とセキュリティ アソシエーションは、同時にタイムアウトになります。

特定の暗号マップ エントリにライフタイム値が設定されていない場合、FWSM はネゴシエーション実行中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、ピアへの要求にグローバル ライフタイム値を指定し、こ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。FWSM は、ピアからネゴシエーション要求を受信すると、ピアが指定したライフタイム値またはローカル設定のライフタイム値のうち、どちらか小さい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。

ライフタイムは、2 種類あります。「期間」のライフタイム、および「トラフィック量」のライフタイムです。セキュリティ アソシエーションは、いずれかのライフタイムに到達した時点で期限切れになります。

FWSM では、暗号マップ、ダイナミック マップ、および IPSec 設定を、オンザフライで変更できます。この場合、FWSM は、変更によって影響を受ける接続だけをダウンします。たとえば、アクセス リスト内のエントリを削除して、暗号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。

グローバル期間ライフタイムを変更するには、**crypto ipsec security-association lifetime seconds** コマンドを使用します。期間ライフタイムを使用すると、指定した秒数が経過した時点で、セキュリティ アソシエーションがタイムアウトになります。

グローバル トラフィック量ライフタイムを変更するには、**crypto ipsec security-association lifetime kilobytes** コマンドを使用します。トラフィック量ライフタイムを使用すると、指定したトラフィック量（キロバイト）がセキュリティ アソシエーションの鍵によって保護された時点で、セキュリティ アソシエーションがタイムアウトになります。

ライフタイムが短いほど、同じ鍵で暗号化されるデータ量は少なくなるので、攻撃者による鍵再現攻撃の可能性は低くなります。ただし、ライフタイムを短くするほど、新しいセキュリティ アソシエーションを確立するための CPU 処理時間は長くなります。

セキュリティ アソシエーション（および対応する鍵）は、指定された秒数またはトラフィック量（KB）のどちらかが先に経過した時点で、期限切れになります。

## 例

次に、セキュリティ アソシエーションのグローバル期間ライフタイムを指定する例を示します。

```
hostname(config)# crypto ipsec-security association lifetime seconds 240
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure crypto map** | グローバル ライフタイム、トランスフォーム セットなど、すべての IPSec 設定をクリアします。 |
| **show running-config crypto map** | すべての暗号マップの全設定を表示します。 |

# crypto ipsec transform-set

トランスフォーム セットを定義するには、グローバル コンフィギュレーション モードで、**crypto ipsec transform-set** コマンドを使用します。このコマンドを使用して、トランスフォーム セットが使用する IPSec 暗号化およびハッシュ アルゴリズムを指定します。トランスフォーム セットを削除するには、このコマンドの **no** 形式を使用します。

**crypto ipsec** *map-name seq-num* **transform-set** *transform-set-name transform1 [transform2]*

**no crypto ipsec** *map-name seq-num* **transform-set** *transform-set-name*

## シンタックスの説明

| | |
|---|---|
| **esp-aes** | トランスフォームによって保護する IPSec メッセージを、128 ビット鍵の AES を使用して暗号化する場合、このオプションを指定します。 |
| **esp-aes-192** | トランスフォームによって保護する IPSec メッセージを、192 ビット鍵の AES を使用して暗号化する場合、このオプションを指定します。 |
| **esp-aes-256** | トランスフォームによって保護する IPSec メッセージを、256 ビット鍵の AES を使用して暗号化する場合、このオプションを指定します。 |
| **esp-des** | トランスフォームによって保護する IPSec メッセージを、56 ビット DES-CBC を使用して暗号化する場合、このオプションを指定します。 |
| **esp-3des** | トランスフォームによって保護する IPSec メッセージを、3 DES アルゴリズムを使用して暗号化する場合、このオプションを指定します。 |
| esp-none | IPSec メッセージで HMAC 認証を使用しない場合、このオプションを指定します。 |
| **esp-null** | IPSec メッセージを、IPSec セキュリティ プロトコル（ESP）だけを使用して暗号化しない場合、このオプションを指定します。 |
| **esp-md5-hmac** | トランスフォームによって保護する IPSec メッセージで、ハッシュ アルゴリズムとして MD5/HMAC-128 を使用する場合、このオプションを指定します。 |
| **esp-sha-hmac** | トランスフォームによって保護する IPSec メッセージで、ハッシュ アルゴリズムとして SHA/HMAC-160 を使用する場合、このオプションを指定します。 |
| *map-name* | 暗号マップ セットの名前を指定します。 |
| *seq-num* | 暗号マップ エントリに割り当てる番号を指定します。 |
| *transform1*、*transform2* | 1 つまたは 2 つのトランスフォームを指定します。トランスフォームにより、IPSec セキュリティ プロトコルおよびアルゴリズムを定義します。各トランスフォームに、構文に定義されているように、[**esp-aes** \| **esp-aes-192** \| **esp-aes-256** \| **esp-des** \| **esp-3des** \| **esp-null**] または [**esp-md5-hmac** \| **esp-sha-hmac**] のいずれかで、使用する IPSec セキュリティ プロトコル（ESP）およびアルゴリズムを指定します。 |
| *transform-set-name* | 作成または変更するトランスフォーム セットの名前を指定します。 |
| token | ユーザ認証にトークン ベース サーバを使用することを指定します。 |

## デフォルト

デフォルトの暗号化アルゴリズムは、esp-3des（3 DES）です。

**コマンド モード**

次の表に、コマンドを入力できるモードを示します。

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

**コマンド履歴**

| リリース | 変更 |
|---|---|
| 1.1(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**

トランスフォーム セットには、1 つまたは 2 つの IPSec セキュリティ プロトコルと、これらのセキュリティ プロトコルと併用するアルゴリズムを指定します。IPSec セキュリティ アソシエーションのネゴシエーション中に、両ピアは、特定のデータ フローを保護するときに特定のトランスフォーム セットを使用することに同意します。

IPSec メッセージは、128 ビット鍵、192 ビット鍵、または 256 ビット鍵の AES を使用するトランスフォーム セットによって保護できます。

AES により提供される鍵のサイズは大きいので、ISAKMP ネゴシエーションには、group 1 または group 2 ではなく、Diffie-Hellman group 5 を使用すべきです。この設定には、**isakmp policy priority group 5** コマンドを使用します。

複数のトランスフォーム セットを設定すると、暗号マップ エントリに 1 つ以上のトランスフォーム セットを指定できます。IPSec セキュリティ アソシエーションのネゴシエーションでは、暗号マップ エントリに定義されているトランスフォーム セットにより、その暗号マップ エントリのアクセス リストにより指定されたデータ フローが保護されます。ネゴシエーションの実行中に、2 つのピアは、両ピアで一致しているトランスフォーム セットを検索します。同じトランスフォーム セットが検出されると、FWSM は、両ピアの IPSec セキュリティ アソシエーションの一環として、保護されるトラフィックにそのトランスフォーム セットを適用します。

各トランスフォーム セットには、暗号化または認証に使用するアルゴリズムが設定されています。IPSec セキュリティ アソシエーションのネゴシエーション中に特定のトランスフォーム セットを使用する場合には、トランスフォーム セット全体（プロトコル、アルゴリズム、およびその他の設定値の組み合わせ）が、リモート ピアのトランスフォーム セットと一致している必要があります。

トランスフォーム セットには、ESP 暗号化トランスフォームだけ、または ESP 暗号化トランスフォームと ESP 認証トランスフォームの両方を指定できます。

指定できるトランスフォームの組み合わせ例は、次のとおりです。

- **esp-des**
- **esp-des** および **esp-md5-hmac**

既存のトランスフォーム セットに対して、**crypto ipsec transform-set** コマンドで 1 つまたは複数のトランスフォームを指定すると、既存のトランスフォームは、新しく指定したトランスフォームに置き換えられます。

## 例

次に、2 つのトランスフォーム セットを設定する例を示します。暗号化に DES、ハッシュ アルゴリズムとして SHA/HMAC-160 を使用する t1 というトランスフォーム セット、および暗号化に AES 192、ハッシュ アルゴリズムとして MD5/HMAC-128 を使用する standard というトランスフォーム セットです。

```
hostname(config)# crypto ipsec transform-set t1 esp-des esp-sha-hmac
hostname(config)# crypto ipsec transform-set standard esp-aes-192 esp-md5-hmac
hostname(config)
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure crypto** | グローバル ライフタイム、トランスフォーム セットなど、すべての IPSec 設定をクリアします。 |
| **show running-config crypto map** | すべての暗号マップの全設定を表示します。 |

# crypto key generate dsa

ID 証明書用の DSA 鍵のペアを生成するには、グローバル コンフィギュレーション モードで、**crypto key generate dsa** コマンドを使用します。

**crypto key generate dsa** {**label** *key-pair-label*} [**modulus** *size*] [**noconfirm**]

## シンタックスの説明

| | |
|---|---|
| **label** *key-pair-label* | 鍵のペアに関連付ける名前を指定します。ラベルの最大長は、128 文字です。DSA にはラベルが必要です。 |
| **modulus** *size* | （任意）鍵のペアに関連付けるモジュラ サイズ（512、768、1024）を指定します。デフォルトのモジュラス サイズは、1024 です。 |
| **noconfirm** | （任意）すべての対話プロンプトを抑制します。 |

## デフォルト

デフォルトのモジュラス サイズは、1024 です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更 |
|---|---|
| 3.1(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

**crypto key generate dsa** コマンドでは、SSL、SSH、および IPSec 接続をサポートする DSA 鍵のペアを生成します。生成した鍵のペアは、コマンド構文で指定したラベルによって識別されます。ラベルを指定しないと、FWSM によりエラー メッセージが表示されます。

## 例

次に、グローバル コンフィギュレーション モードで、mypubkey というラベルの DSA 鍵のペアを生成する例を示します。

```
hostname(config)# crypto key generate dsa label mypubkey
INFO: The name for the keys will be: mypubkey
hostname(config)#
```

次に、グローバル コンフィギュレーション モードで、mypubkey というラベルの DSA 鍵のペアを重複して生成しようとした場合の例を示します。

```
hostname(config)# crypto key generate dsa label mypubkey
WARNING: You already have dSA keys defined named mypubkey
Do you really want to replace them? [yes/no] no
ERROR: Failed to create new DSA keys named mypubkey
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **crypto key zeroize** | DSA 鍵のペアを削除します。 |
| **show crypto key mypubkey** | DSA 鍵のペアを表示します。 |

# crypto key generate rsa

ID 証明書用の RSA 鍵のペアを生成するには、グローバル コンフィギュレーション モードで、**crypto key generate rsa** コマンドを使用します。

**crypto key generate rsa** [**usage-keys | general-keys**] [**label** *key-pair-label*] [**modulus** *size*] [**noconfirm**]

## シンタックスの説明

| | |
|---|---|
| **general-keys** | （任意）汎用目的の鍵のペアを 1 つ生成します。これは、デフォルトの鍵ペア タイプです。 |
| **label** *key-pair-label* | （任意）鍵のペアに関連付ける名前を指定します。鍵のペアには、固有のラベルが必要です。同じラベルを使用して別の鍵のペアを作成しようとすると、FWSM により警告メッセージが表示されます。鍵の生成時にラベルを指定しないと、鍵のペアには、固定的に <Default-RSA-Key> という名前が指定されます。 |
| **modulus** *size* | （任意）鍵のペアに関連付けるモジュラ サイズ（512、768、1024、2048）を指定します。デフォルトのモジュラス サイズは、1024 です。 |
| **noconfirm** | （任意）すべての対話プロンプトを抑制します。 |
| ***usage-keys*** | （任意）シグニチャ用および暗号化用に 1 つずつ、2 つの鍵のペアを生成します。つまり、対応する ID に 2 つの証明書が必要になります。 |

## デフォルト

デフォルトの鍵ペア タイプは、**general key** です。デフォルトのモジュラス サイズは、1024 です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更 |
|---|---|
| 3.1(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

**crypto key generate rsa** コマンドでは、SSL、SSH、および IPSec 接続をサポートする RSA 鍵のペアを生成します。生成した鍵のペアは、コマンド構文で指定したラベルによって識別されます。鍵のペアを参照しないトラストポイントには、デフォルトの <Default-RSA-Key> を使用できます。SSH 接続は、常にこの鍵を使用します。これは、SSL には影響しません。トラストポイントに設定されていない限り、SSL は独自の証明書 / 鍵をダイナミックに生成するからです。

## 例

次に、グローバル コンフィギュレーション モードで、mypubkey というラベルの RSA 鍵のペアを生成する例を示します。

```
hostname(config)# crypto key generate rsa label mypubkey
INFO: The name for the keys will be: mypubkey
Keypair generation process
hostname(config)#
```

次に、グローバル コンフィギュレーション モードで、mypubkey というラベルの RSA 鍵のペアを重複して生成しようとした場合の例を示します。

```
hostname(config)# crypto key generate rsa label mypubkey
WARNING: You already have RSA keys defined named mypubkey
Do you really want to replace them? [yes/no] no
ERROR: Failed to create new RSA keys named mypubkey
hostname(config)#
```

次に、グローバル コンフィギュレーション モードで、デフォルト ラベルの RSA 鍵のペアを生成する例を示します。

```
hostname(config)# crypto key generate rsa
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **crypto key zeroize** | RSA 鍵のペアを削除します。 |
| **show crypto key mypubkey** | RSA 鍵のペアを表示します。 |

# crypto key zeroize

指定したタイプ（rsa または dsa）の鍵のペアを削除するには、グローバル コンフィギュレーション モードで、**crypto key zeroize** コマンドを使用します。

**crypto key zeroize** {**rsa** | **dsa**} [**label** *key-pair-label*] [**default**] [**noconfirm**]

## シンタックスの説明

| | |
|---|---|
| **default** | （任意）ラベルのない RSA 鍵のペアを削除します。このキーワードは、RSA 鍵のペアに対してのみ有効です。 |
| **dsa** | 鍵タイプとして、DSA を指定します。 |
| **label** *key-pair-label* | （任意）指定したタイプ（rsa または dsa）の鍵のペアを削除します。ラベルを指定しない場合、FWSM は、指定されたタイプのすべての鍵のペアを削除します。 |
| **noconfirm** | （任意）すべての対話プロンプトを抑制します。 |
| **rsa** | 鍵タイプとして、RSA を指定します。 |

## デフォルト

このコマンドには、デフォルトの動作または値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更 |
|---|---|
| 1.1(1) | このコマンドが追加されました。 |

## 例

次に、グローバル コンフィギュレーション モードで、すべての RSA 鍵のペアを削除する例を示します。

```
hostname(config)# crypto key zeroize rsa
WARNING: All RSA keys will be removed.
WARNING: All router certs issued using these keys will also be removed.

Do you really want to remove these keys? [yes/no] y
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **crypto key generate dsa** | ID 証明書用の DSA 鍵のペアを生成します。 |
| **crypto key generate rsa** | ID 証明書用の RSA 鍵のペアを生成します。 |

# crypto map interface

定義済みの暗号マップ セットをインターフェイスに適用するには、グローバル コンフィギュレーション モードで、**crypto map interface** コマンドを使用します。インターフェイスから暗号マップ セットを削除するには、このコマンドの **no** 形式を使用します。

**crypto map** *map-name* **interface** *interface-name*

**no crypto map** *map-name* **interface** *interface-name*

## シンタックスの説明

| | |
|---|---|
| *interface-name* | FWSM が VPN ピアとトンネルを確立するために使用するインターフェイスを指定します。ISAKMP がイネーブルで、認証局を使用して証明書を取得している場合には、CA 証明書に指定されているアドレスのインターフェイスを指定する必要があります。 |
| *map-name* | 暗号マップ セットの名前を指定します。 |

## デフォルト

このコマンドには、デフォルトの動作または値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更 |
|---|---|
| 1.1(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

このコマンドは、任意のアクティブな FWSM インターフェイスに、暗号マップ セットを割り当てます。FWSM は、任意またはすべてのアクティブ インターフェイス上で IPSec ターミネーションをサポートします。インターフェイスで IPSec サービスを提供するには、事前にインターフェイスに暗号マップ セットを割り当てる必要があります。

1 つのインターフェイスに割り当てることができる暗号マップ セットは、1 つだけです。*map-name* が同じで、*seq-num* が異なる複数の暗号マップ エントリがある場合、これらのエントリは同じセットに属し、すべてのエントリがインターフェイスに割り当てられます。FWSM は、*seq-num* が最も小さい暗号マップ エントリを最初に評価します。

（注）　FWSM では、暗号マップ、ダイナミック マップ、および IPSec 設定を、オンザフライで変更できます。この場合、FWSM は、変更によって影響を受ける接続だけをダウンします。たとえば、アクセス リスト内のエントリを削除して、暗号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。

スタティックな暗号マップはすべて、アクセス リスト、トランスフォーム セット、および IPSec ピアの 3 つを定義している必要があります。いずれか 1 つが欠落していると、暗号マップは不完全であるとみなされ、FWSM は次のエントリに移動します。ただし、暗号マップがアクセス リストと一致し、他の 2 つの要件のいずれか、または両方と一致しない場合には、FWSM はトラフィックを廃棄します。

すべての暗号マップが完全であるかどうかを確認するには、**show running-config crypto map** コマンドを使用します。不完全な暗号マップを修正するには、その暗号マップを削除し、欠落しているエントリを追加してから、再び割り当てます。

## 例

次に、グローバル コンフィギュレーション モードで、外部インターフェイスに mymap という暗号マップ セットを割り当てる例を示します。FWSM は、この外部インターフェイスを通過するトラフィックを、mymap セット内のすべての暗号マップ エントリに対して評価します。発信トラフィックが、いずれかの mymap 暗号マップ エントリのアクセス リストと一致すると、FWSM は、その暗号マップ エントリの設定を使用してセキュリティ アソシエーションを形成します。

```
hostname(config)# crypto map mymap interface outside
```

次に、最小限必要な暗号マップ コンフィギュレーションの例を示します。

```
hostname(config)# crypto map mymap 10 ipsec-isakmp
hostname(config)# crypto map mymap 10 match address 101
hostname(config)# crypto map mymap set transform-set my_t_set1
hostname(config)# crypto map mymap set peer 10.0.0.1
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure crypto map** | すべての暗号マップの全設定をクリアします。 |
| **show running-config crypto map** | 暗号マップのコンフィギュレーションを表示します。 |

# crypto map ipsec-isakmp dynamic

特定の暗号マップ エントリが、既存のダイナミック暗号マップを参照するように設定するには、グローバル コンフィギュレーション モードで、**crypto map ipsec-isakmp dynamic** コマンドを使用します。クロス リファレンスを削除するには、このコマンドの **no** 形式を使用します。

**[no] crypto map** *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

## シンタックスの説明

| | |
|---|---|
| *dynamic-map-name* | 既存のダイナミック暗号マップを参照する暗号マップ エントリの名前を指定します。 |
| **ipsec-isakmp** | IKE が、この暗号マップ エントリの IPSec セキュリティ アソシエーションを確立するように指定します。 |
| *map-name* | 暗号マップ セットの名前を指定します。 |
| *seq-num* | 暗号マップ エントリに割り当てる番号を指定します。 |

## デフォルト

このコマンドには、デフォルトの動作または値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更 |
|---|---|
| 1.1(1) | このコマンドが追加されました。 |
| 3.1(1) | このコマンドから、**ipsec-manual** キーワードが削除されました。 |

## 使用上のガイドライン

ダイナミック暗号マップ エントリを作成するには、**crypto dynamic-map** コマンドを使用します。ダイナミック暗号マップ セットの作成後に、**crypto map ipsec-isakmp dynamic** コマンドを使用して、ダイナミック暗号マップ セットをスタティック暗号マップに追加します。

暗号マップ エントリを定義したら、**crypto map interface** コマンドを使用して、ダイナミック暗号マップ セットをインターフェイスに割り当てることができます。

ダイナミック暗号マップには、2 つの機能があります。保護対象トラフィックのフィルタリングと分類、およびトラフィックに適用するポリシーの定義です。最初の機能はインターフェイス上のトラフィック フローに影響して、2 つめの機能はトラフィックに対して実行される（IKE による）ネゴシエーションに影響します。

IPSec ダイナミック暗号マップには、次の内容を設定します。

- 保護対象のトラフィック
- セキュリティ アソシエーションを確立する IPSec ピア
- 保護対象トラフィックに適用するトランスフォーム セット
- 鍵およびセキュリティ アソシエーションの使用または管理方法

暗号マップ セットは、マップ名が同じで、シーケンス番号（seq-num）が異なる暗号マップ エントリの集合です。したがって、特定のインターフェイス上で、指定のセキュリティを適用した特定のトラフィックを 1 つのピアに転送し、異なる IPSec セキュリティを適用した他のトラフィックを同じ、または異なるピアに転送できます。これを実行するには、マップ名が同じで、シーケンス番号が異なる 2 つの暗号マップ エントリを作成します。

seq-num 引数に割り当てる番号は、任意の値ではありません。この番号により、暗号マップ セット内の複数の暗号マップ エントリがランク付けされます。暗号マップ エントリは、シーケンス番号が低いものから順番に評価されます。つまり、番号の低いマップ エントリのほうが優先順位が高くなります。

**（注）** ダイナミック暗号マップに暗号マップをリンクする場合には、ダイナミック暗号マップを指定する必要があります。暗号マップは、**crypto dynamic-map** コマンドによって定義された既存のダイナミック暗号マップにリンクされます。変換後に行った暗号マップ エントリの変更は、反映されません。たとえば、ピア設定を変更しても、反映されません。ただし、FWSM がアップのあいだは、変更内容が保管されています。ダイナミック暗号マップを暗号マップに戻すと、変更が反映され、**show running-config crypto map** コマンドの出力に表示されます。これらの設定は、FWSM がリブートされるまで保持されます。

## 例

次に、グローバル コンフィギュレーション モードで、mymap という暗号マップが test というダイナミック暗号マップを参照するように設定する例を示します。

```
hostname(config)# crypto map mymap ipsec-isakmp dynamic test
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure crypto map** | すべての暗号マップの全設定をクリアします。 |
| **show running-config crypto map** | 暗号マップのコンフィギュレーションを表示します。 |

# crypto map match address

暗号マップ エントリにアクセス リストを割り当てるには、グローバル コンフィギュレーション モードで、**crypto map match address** コマンドを使用します。暗号マップ エントリからアクセス リストを削除するには、このコマンドの **no** 形式を使用します。

**crypto map** *map-name seq-num* **match address** *acl_name*

**no crypto map** *map-name seq-num* **match address** *acl_name*

## シンタックスの説明

| | |
|---|---|
| *acl_name* | 暗号化アクセス リストの名前を指定します。この名前は、照合する暗号化アクセス リストの name 引数の名前と一致している必要があります。 |
| *map-name* | 暗号マップ セットの名前を指定します。 |
| *seq-num* | 暗号マップ エントリに割り当てる番号を指定します。 |

## デフォルト

このコマンドには、デフォルトの動作または値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更 |
|---|---|
| 1.1(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

このコマンドは、すべてのスタティック暗号マップ エントリに必要です。**crypto dynamic-map** コマンドを使用してダイナミック暗号マップ エントリを定義する場合には、このコマンドは必須ではありませんが、使用することを強く推奨します。アクセス リストを定義するには、**access-list** コマンドを使用します。

IPSec は、アクセス リストを使用して、IPSec 暗号により保護するトラフィックと、保護が不要なトラフィックとを判別します（アクセスリストにより許可されたトラフィックは、保護されます。アクセス リストにより拒否されたトラフィックは、対応する暗号マップ エントリに関しては保護されません）。

**（注）** 暗号アクセス　リストは、トラフィックのインターフェイス通過を許可するか、拒否するかは判別しません。この判別を行うのは、**access-group** コマンドにより、インターフェイスに直接割り当てるアクセス リストです。

透過モードでは、宛先アドレスは、FWSM の IP アドレス（管理アドレス）でなければなりません。透過モードで許可されるのは、FWSM へのトンネルだけです。

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure crypto map** | すべての暗号マップの全設定をクリアします。 |
| **show running-config crypto map** | 暗号マップのコンフィギュレーションを表示します。 |

# crypto map set connection-type

暗号マップ エントリの Backup Site-to-Site（サイト間バックアップ）機能の接続タイプを指定するには、グローバル コンフィギュレーション モードで、**crypto map set connection-type** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

**crypto map** *map-name seq-num* **set connection-type {answer-only | originate-only | bidirectional}**

**no crypto map** *map-name seq-num* **set connection-type {answer-only | originate-only | bidirectional}**

## シンタックスの説明

| | |
|---|---|
| **answer-only** | ピアが、暗号マップ エントリに基づくサイト間接続について、着信 IKE 接続への応答だけを実行するように指定します。ピアから、接続要求を発信することはできません。このキーワードを使用できるのは、トランスペアレント ファイアウォール モードの場合だけです。 |
| **bidirectional** | ピアが、暗号マップ エントリに基づく接続を受け入れ、かつ接続を開始できるように指定します。これは、すべてのサイト間接続のデフォルトの接続タイプです。このキーワードは、トランスペアレント ファイアウォール モードには使用できません。 |
| **map-***name* | 暗号マップ セットの名前を指定します。 |
| **originate-only** | ピアが、暗号マップ エントリに基づく接続の開始だけを実行するように指定します。着信接続を受け入れることはできません。このキーワードは、トランスペアレント ファイアウォール モードには使用できません。 |
| *seq-num* | 暗号マップ エントリに割り当てる番号を指定します。 |

## デフォルト

デフォルトの設定は、bidirectional です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更 |
|---|---|
| 3.1(1) | このコマンドが追加されました。 |

## 例

次に、グローバル コンフィギュレーション モードで、mymap という暗号マップを設定して接続タイプを双方向に設定する例を示します。

```
hostname(config)# crypto map mymap 10 set connection-type bidirectional
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure crypto map** | すべての暗号マップの全設定をクリアします。 |
| **show running-config crypto map** | 暗号マップのコンフィギュレーションを表示します。 |

# crypto map set peer

暗号マップ エントリの IPSec ピアを指定するには、グローバル コンフィギュレーション モードで、**crypto map set peer** コマンドを使用します。暗号マップ エントリから IPSec ピアを削除するには、このコマンドの **no** 形式を使用します。

**crypto map** *map-name seq-num* **set peer** {*ip_address* | *hostname*} {*...ip_address* | *hostname10*}

**no crypto map** *map-name seq-num* **set peer** {*ip_address* | *hostname*} {*...ip_address* | *hostname10*}

## シンタックスの説明

| | |
|---|---|
| *hostname* | FWSM **name** コマンドで定義したように、ピアをホスト名で指定します。 |
| *ip_address* | ピアを、IP アドレスで指定します。 |
| *map-name* | 暗号マップ セットの名前を指定します。 |
| **peer** | 暗号マップ エントリの IPSec ピアを、ホスト名または IP アドレスのいずれかで指定します。 |
| *seq-num* | 暗号マップ エントリに割り当てる番号を指定します。 |

## デフォルト

このコマンドには、デフォルトの動作または値はありません。

## コマンド モード

次の表に、このコマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更 |
|---|---|
| 1.1(1) | このコマンドが追加されました。 |
| 3.1(1) | このコマンドに、最大 10 のピア アドレスを指定できるようになりました。 |

## 使用上のガイドライン

このコマンドは、すべてのスタティック暗号マップに必要です。**crypto dynamic-map** コマンドを使用してダイナミック暗号マップを定義する場合には、このコマンドは必須ではありません。通常、ピアは不明なので、ほとんどの場合、このコマンドを使用しません。

LAN と LAN を接続する場合には、originator-only 接続タイプに限り、複数のピアを指定できます。複数ピアを設定することは、フォールバック リストを提供することと同じです。各トンネルについて、FWSM は、リストの最初のピアとネゴシエーションを試みます。そのピアが応答しない場合、FWSM は、いずれかのピアが応答するか、リストの最後のピアに到達するまで、リストされている順序でピアとのネゴシエーションを試みます。複数のピアを設定できるのは、LAN-to-LAN バックアップ機能（originate-only タイプの暗号マップ）を使用する場合だけです。

## 例

次に、グローバル コンフィギュレーション モードで、セキュリティ アソシエーションの確立に IKE を使用し、暗号マップを設定する例を示します。この例では、ピア 10.0.0.1 またはピア 10.0.0.2 のどちらかと、セキュリティ アソシエーションを確立できます。

```
hostname(config)# crypto map mymap 10 ipsec-isakmp
hostname(config)# crypto map mymap 10 match address 101
hostname(config)# crypto map mymap 10 set transform-set my_t_set1
hostname(config)# crypto map mymap 10 set peer 10.0.0.1 10.0.0.2
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **clear configure crypto map** | すべての暗号マップの全設定をクリアします。 |
| **show running-config crypto map** | 暗号マップのコンフィギュレーションを表示します。 |

# crypto map set pfs

暗号マップ エントリの新しいセキュリティ アソシエーションを要求する場合、または新しいセキュリティ アソシエーションの要求を受信する場合に、IPSec が Perfect Forward Secrecy（PFS）を要求するように設定するには、グローバル コンフィギュレーション モードで、**crypto map set pfs** コマンドを使用します。IPSec が PFS を要求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。

**crypto map** *map-name seq-num* **set pfs [group1 | group2 | group5 | group7]**

**no crypto map** *map-name seq-num* **set pfs [group1 | group2 | group5 | group7]**

**シンタックスの説明**

| | |
|---|---|
| **group1** | 新しい Diffie-Hellman 交換の実行時に、IPSec が 768 ビット Diffie-Hellman プライム モジュラス グループを使用するように指定します。 |
| **group2** | 新しい Diffie-Hellman 交換の実行時に、IPSec が 1024 ビット Diffie-Hellman プライム モジュラス グループを使用するように指定します。 |
| **group5** | 新しい Diffie-Hellman 交換の実行時に、IPSec が 1536 ビット Diffie-Hellman プライム モジュラス グループを使用するように指定します。 |
| **group7** | IPSec が、Movian VPN クライアントなどに対し、楕円曲線フィールドのサイズが 163 ビットである group7（ECC）を使用するように指定します。 |
| *map-name* | 暗号マップ セットの名前を指定します。 |
| *seq-num* | 暗号マップ エントリに割り当てる番号を指定します。 |

**デフォルト**

デフォルトでは、PFS は設定されていません。

**コマンド モード**

次の表に、このコマンドを入力できるモードを示します。:

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

**コマンド履歴**

| リリース | 変更 |
|---|---|
| 1.1(1) | このコマンドが追加されました。 |
| 3.1(1) | このコマンドに、Diffie-Hellman group7 が追加されました。 |

**使用上のガイドライン**

PFS を使用すると、新しいセキュリティ アソシエーションをネゴシエートするごとに新しい Diffie-Hellman 交換が実行されるので、処理時間が長くなります。また、PFS を使用すると、1 つの鍵が攻撃者によって破壊されても、影響を受けるのは、その鍵によって送信されたデータだけなので、セキュリティ レベルが高くなります。

このコマンドを使用すると、ネゴシエーションの実行中、暗号マップ エントリの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、IPSec は PFS を要求します。**set pfs** ステートメントにグループを指定しない場合、FWSM は、デフォルトの group2 を使用します。

ピアのネゴシエーション開始時にローカル コンフィギュレーションに PFS が指定されている場合、ピアは PFS 交換を実行する必要があります。実行しない場合、ネゴシエーションに失敗します。ローカル コンフィギュレーションにグループが指定されていない場合、FWSM はデフォルトの group2 を使用します。ローカル コンフィギュレーションに group2、group5、group7 が指定されている場合、そのグループがピアのオファーに含まれている必要があります。含まれていない場合、ネゴシエーションに失敗します。

ネゴシエーションを成功させるには、両端に PFS が設定されている必要があります。また、設定されている場合、グループが正確に一致している必要があります。FWSM は、ピアからの PFS オファーをすべて受け入れるわけではありません。

1536 ビット Diffie-Hellman プライム モジュラス グループ（group5）は、group1 または group2 よりも高いセキュリティを提供しますが、処理時間は他のグループよりも長くなります。

Diffie-Hellman Group7 は、楕円曲線フィールドのサイズが 163 ビットの IPSec SA 鍵を生成します。このオプションは、任意の暗号化アルゴリズムと併用できます。このオプションは、movian VPN クライアントを対象としたものですが、Group7（ECC）をサポートする任意のピアを併用できます。

Cisco VPN クライアントと通信する場合、FWSM は PFS 値を使用せず、フェーズ 1 の実行中にネゴシエートされた値を使用します。

**例**

次に、グローバル コンフィギュレーション モードで、暗号マップ mymap 10 の新しいセキュリティ アソシエーションをネゴシエートするときに、必ず PFS を使用するように設定する例を示します。

```
hostname(config)# crypto map mymap 10 ipsec-isakmp
hostname(config)# crypto map mymap 10 set pfs group2
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **clear isakmp sa** | アクティブな IKE セキュリティ アソシエーションを削除します。 |
| **clear configure crypto map** | すべての暗号マップの全設定をクリアします。 |
| **show running-config crypto map** | 暗号マップのコンフィギュレーションを表示します。 |
| **tunnel-group** | トンネル グループおよびパラメータを設定します。 |

# crypto map set phase1 mode

接続開始時のフェーズ 1 の IKE モードを main または aggressive のどちらかに指定するには、グローバル コンフィギュレーション モードで、**crypto map set phase1mode** コマンドを使用します。フェーズ 1 IKE ネゴシエーション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。aggressive モードでの Diffie-Hellman グループの指定は、任意です。指定しない場合、FWSM は group2 を使用します。

**crypto map** *map-name seq-num* **set phase1mode {main | aggressive [group1 | group2 | group5 | group7]}**

**no crypto map** *map-name seq-num* **set phase1mode {main | aggressive [group1 | group2 | group5 | group7]}**

## シンタックスの説明

| | |
|---|---|
| aggressive | フェーズ 1 IKE ネゴシエーションに aggressive モードを指定します。 |
| **group1** | 新しい Diffie-Hellman 交換の実行時に、IPSec が 768 ビット Diffie-Hellman プライム モジュラス グループを使用するように指定します。 |
| **group2** | 新しい Diffie-Hellman 交換の実行時に、IPSec が 1024 ビット Diffie-Hellman プライム モジュラス グループを使用するように指定します。 |
| **group5** | 新しい Diffie-Hellman 交換の実行時に、IPSec が 1536 ビット Diffie-Hellman プライム モジュラス グループを使用するように指定します。 |
| **group7** | IPSec が、Movian VPN クライアントなどに対し、楕円曲線フィールドのサイズが 163 ビットである group7（ECC）を使用するように指定します。 |
| **main** | フェーズ 1 IKE ネゴシエーションに main モードを指定します。 |
| *map-name* | 暗号マップ セットの名前を指定します。 |
| *seq-num* | 暗号マップ エントリに割り当てる番号を指定します。 |

## デフォルト

デフォルトのフェーズ 1 モードは、**main** です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更 |
|---|---|
| 3.1(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

このコマンドを使用できるのは、initiator モードだけで、responder モードには使用できません。

## 例

次に、グローバル コンフィギュレーション モードで、暗号マップ mymap のフェーズ 1 モードを aggressive に設定し、group2 を使用するように指定する例を示します。

```
hostname(config)# crypto map mymap 10 set phase1mode aggressive group2
hostname(config)#
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **clear isakmp sa** | アクティブな IKE セキュリティ アソシエーションを削除します。 |
| **clear configure crypto map** | すべての暗号マップの全設定をクリアします。 |
| **show running-config crypto map** | 暗号マップのコンフィギュレーションを表示します。 |

# crypto map set reverse-route

暗号マップ エントリに基づくすべての接続に対して、Reverse Route Injection（RRI）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、**crypto map set reverse-route** コマンドを使用します。暗号マップ エントリに基づくすべての接続について、RRI 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。

**crypto map** *map-name seq-num* ***set reverse-route***

**no crypto map** *map-name seq-num* ***set reverse-route***

**シンタックスの説明**

| | |
|---|---|
| *map-name* | 暗号マップ セットの名前を指定します。 |
| *seq-num* | 暗号マップ エントリに割り当てる番号を指定します。 |

**デフォルト**

このコマンドの設定は、デフォルトではオフになっています。

**コマンド モード**

次の表に、コマンドを入力できるモードを示します。

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

**コマンド履歴**

| リリース | 変更 |
|---|---|
| 3.1(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**

FWSM では、ルーティング テーブルにスタティック ルートを自動的に追加し、OSPF を使用して、これらのルートをプライベート ネットワークまたは境界ルータに通知できます。

**例**

次に、グローバル コンフィギュレーション モードで、mymap という暗号マップの RRI をイネーブルに設定する例を示します。

```
hostname(config)# crypto map mymap 10 set reverse-route
hostname(config)#
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **clear configure crypto map** | すべての暗号マップの全設定をクリアします。 |
| **show running-config crypto map** | 暗号マップのコンフィギュレーションを表示します。 |

# crypto map set security-association lifetime

（特定の暗号マップ エントリについて）IPSec セキュリティ アソシエーションをネゴシエートするときに使用するグローバル ライフタイム値を上書きするには、グローバル コンフィギュレーション モードで **crypto map set security-association lifetime** コマンドを使用します。暗号マップ エントリのライフタイム値をグローバル値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。

**crypto map** *map-name seq-num* **set security-association lifetime {seconds** *seconds* | **kilobytes** *kilobytes*}

**no crypto map** *map-name seq-num* **set security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}

## シンタックスの説明

| | |
|---|---|
| *kilobytes* | セキュリティ アソシエーションが期限切れになる前に、そのセキュリティ アソシエーションを使用してピア間で通信できるトラフィック量（キロバイト）を指定します。<br>デフォルトは、4,608,000 KB です。 |
| *map-name* | 暗号マップ セットの名前を指定します。 |
| *seconds* | セキュリティ アソシエーションの有効存続時間を秒数で指定します。デフォルトは、28,800 秒（ 8 時間）です。 |
| *seq-num* | 暗号マップ エントリに割り当てる番号を指定します。 |

## デフォルト

キロバイトのデフォルト値は 4,608,000 KB、秒のデフォルト値は 28,800 秒です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更 |
|---|---|
| 1.1(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

暗号マップのセキュリティ アソシエーションは、グローバル ライフタイム値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、共有秘密鍵を使用します。これらの鍵とセキュリティ アソシエーションは、同時にタイムアウトになります。

特定の暗号マップ エントリにライフタイム値が設定されている場合、FWSM は、セキュリティ アソシエーションのネゴシエーション中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、ピアへの要求にその暗号マップのライフタイム値を指定し、こ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。FWSM は、ピアからネゴシエーション要求を受信すると、ピアが指定したライフタイム値またはローカル設定のライフタイム値のうち、どちらか小さい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。

ライフタイムは、2 種類あります。「期間」のライフタイム、および「トラフィック量」のライフタイムです。セッション鍵およびセキュリティ アソシエーションは、どちらかのライフタイムが先に到達した時点で期限切れになります。1 つのコマンドで、両方のライフタイムを指定できます。

（注）　FWSM では、暗号マップ、ダイナミック マップ、および IPSec 設定を、オンザフライで変更できます。この場合、FWSM は、変更によって影響を受ける接続だけをダウンします。たとえば、アクセス リスト内のエントリを削除して、暗号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。

期間ライフタイムを変更するには、**crypto map set security-association lifetime seconds** コマンドを使用します。期間ライフタイムを使用すると、指定した秒数が経過した時点で、鍵およびセキュリティ アソシエーションがタイムアウトになります。

## 例

次に、グローバル コンフィギュレーション モードで、暗号マップ mymap のセキュリティ アソシエーション ライフタイムを秒数およびキロバイトで指定する例を示します。

```
hostname(config)# crypto map mymap 10 set security-association lifetime seconds 1400
kilobytes 3000000
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure crypto map** | すべての暗号マップの全設定をクリアします。 |
| **show running-config crypto map** | 暗号マップのコンフィギュレーションを表示します。 |

# crypto map set transform-set

暗号マップ エントリに使用するトランスフォーム セットを指定するには、グローバル コンフィギュレーション モードで、**crypto map set transform-set** コマンドを使用します。指定したトランスフォーム セットを暗号マップ エントリから削除するには、このコマンドの **no** 形式を使用します。

**crypto map** *map-name seq-num* **set transform-set** *transform-set-name1* [*… transform-set-name9*]

**no crypto map** *map-name seq-num* **set transform-set** *transform-set-name1* [*… transform-set-name9*]

## シンタックスの説明

| | |
|---|---|
| *map-name* | 暗号マップ セットの名前を指定します。 |
| *seq-num* | 暗号マップ エントリに割り当てる番号を指定します。 |
| *transform-set-name1*<br>*transform-set-name9* | 暗号マップに使用するトランスフォーム セットを、**crypto ipsec transform-set** コマンドで定義した名前で指定します。ipsec-isakmp またはダイナミック暗号マップ エントリには、最大 9 のトランスフォーム セットを指定できます。 |

## デフォルト

このコマンドには、デフォルトの動作または値はありません。

## コマンド モード

次の表に、このコマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更 |
|---|---|
| 1.1(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

このコマンドは、すべての暗号マップ エントリに必要です。

ローカル FWSM がネゴシエーションを開始する場合、トランスフォーム セットは **crypto map** コマンド ステートメントで指定した順序でピアに提示されます。ピアがネゴシエーションを開始する場合、ローカル FWSM は、暗号マップ エントリに指定されているトランスフォーム セットのいずれかに最初に一致したトランスフォーム セットを受け入れます。

両方のピアで最初に一致したトランスフォーム セットが、セキュリティ アソシエーションに使用されます。一致するトランスフォーム セットがない場合、IPSec はセキュリティ アソシエーションを確立しません。トラフィックを保護するセキュリティ アソシエーションが存在しないので、トラフィックは廃棄されます。

トランスフォーム セットのリストを変更する場合には、新しいトランスフォーム セットのリストを再指定し、既存のリストを置換します。変更が適用されるのは、そのトランスフォーム セットを参照する **crypto map** コマンド ステートメントだけです。

**crypto map** コマンド ステートメントに含めるトランスフォーム セットはすべて、**crypto ipsec transform-set** コマンドを使用して事前に定義しておく必要があります。

## 例

次に、グローバル コンフィギュレーション モードで、暗号マップ mymap に 2 つのトランスフォーム セット（tfset1 および tfset2）を指定する例を示します。

```
hostname(config)# crypto map mymap 10 set transform-set tfset1 tfset2
hostname(config)#
```

次に、グローバル コンフィギュレーション モードを開始して、FWSM が IKE を使用してセキュリティ アソシエーションを確立するときに最小限必要な暗号マップ コンフィギュレーションを示します。

```
hostname(config)# crypto map mymap 10 ipsec-isakmp
hostname(config)# crypto map mymap 10 match address 101
hostname(config)# crypto map mymap set transform-set my_t_set1
hostname(config)# crypto map mymap set peer 10.0.0.1
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure crypto map** | すべての暗号マップの全設定をクリアします。 |
| **crypto ipsec transform-set** | トランスフォーム セットを設定します。 |
| **show running-config crypto map** | 暗号マップのコンフィギュレーションを表示します。 |

# crypto map set trustpoint

暗号マップ エントリのフェーズ 1 ネゴシエーションの実行中に、認証用として送信する証明書を識別するトラストポイントを指定するには、グローバル コンフィギュレーション モードで、**crypto map set trustpoint** コマンドを使用します。暗号マップ エントリからトラストポイントを削除するには、このコマンドの **no** 形式を使用します。

**crypto map** *map-name seq-num* **set trustpoint** *trustpoint-name* **[chain]**

**nocrypto map** *map-name seq-num* **set trustpoint** *trustpoint-name* **[chain]**

## シンタックスの説明

| | |
|---|---|
| **chain** | （任意）証明書チェーンを送信します。CA 証明書チェーンには、ルート証明書から ID 証明書までの証明書階層における、すべての CA 証明書が含まれます。デフォルトの値はディセーブル（チェーンなし）です。 |
| *map-name* | 暗号マップ セットの名前を指定します。 |
| *seq-num* | 暗号マップ エントリに割り当てる番号を指定します。 |
| *trustpoint-name* | フェーズ 1 ネゴシエーションの実行中に送信する証明書を識別します。デフォルトの値はありません。 |

## デフォルト

デフォルトの値はありません。

## コマンド モード

次の表に、このコマンドを入力できるモードを示します。:

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

## コマンド履歴

| リリース | 変更 |
|---|---|
| 3.1(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

この crypto map コマンドは、接続の開始に対してのみ有効です。応答側の情報については、**tunnel-group** コマンドを参照してください。

## 例

次に、グローバル コンフィギュレーション モードで、暗号マップ mymap にトラストポイント tpoint 1 を指定し、証明書チェーンを含める例を示します。

```
hostname(config)# crypto map mymap 10 set trustpoint tpoint1 chain
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure crypto map** | すべての暗号マップの全設定をクリアします。 |
| **show running-config crypto map** | 暗号マップのコンフィギュレーションを表示します。 |
| **tunnel-group** | トンネル グループを設定します。 |