CHAPTER 9

# crypto ca authenticate コマンド～ customization コマンド

# crypto ca authenticate

トラストポイントに関連付けられている CA 証明書をインストールおよび認証するには、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*

## 構文の説明

| | |
|---|---|
| **fingerprint** | セキュリティ アプライアンスが CA 証明書の認証に使用する、英数字で構成されたハッシュ値を指定します。フィンガープリントが指定されている場合、セキュリティ アプライアンスは、そのフィンガープリントを、CA 証明書の計算されたフィンガープリントと比較して、2 つの値が一致した場合にだけその証明書を受け入れます。フィンガープリントがない場合、セキュリティ アプライアンス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尋ねます。 |
| hexvalue | フィンガープリントの 16 進値を指定します。 |
| **nointeractive** | Device Manager 専用の非対話形式モードを使用して、このトラストポイントの CA 証明書を取得します。そのとき、フィンガープリントがない場合、セキュリティ アプライアンスは確認せずに証明書を受け入れます。 |
| *trustpoint* | CA 証明書を取得す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 | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | • | • | • | — |

## コマンド履歴

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

## 使用上のガイドライン

トラストポイントが SCEP 登録用に設定されている場合、CA 証明書は SCEP 経由でダウンロードされます。そうでない場合、セキュリティ アプライアンスは、ユーザに Base-64 形式の CA 証明書を端末に貼り付けるように要求します。

このコマンドの呼び出しは、実行コンフィギュレーションの一部になりません。

## 例

次に、CA 証明書を要求するセキュリティ アプライアンスの例を示します。CA は証明書を送信し、セキュリティ アプライアンスは、管理者に CA 証明書のフィンガープリントをチェックして CA 証明書を確認するように要求します。セキュリティ アプライアンスの管理者は、表示されたフィンガープリントの値を既知の正しい値と照合する必要があります。セキュリティ アプライアンスによって表示されたフィンガープリントが正しい値と一致した場合は、その証明書を有効であるとして受け入れる必要があります。

```
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)#
```

次に、トラストポイント tp9 が端末ベース（手動）の登録用に設定される例を示します。この場合、セキュリティ アプライアンスは、管理者に CA 証明書を端末に貼り付けるように要求します。証明書のフィンガープリントを表示した後、セキュリティ アプライアンスは、管理者に証明書を保持することを確認するように要求します。

```
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 への登録を開始します。 |
| **crypto ca import certificate** | 手動登録要求への応答として CA から受信した証明書をインストールします。また、PKS12 データをトラストポイントにインポートするためにも使用されます。 |
| **crypto ca trustpoint** | 指定したトラストポイントに対してトラストポイント 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 モードに戻る場合は、**exit** コマンドを使用します。

**crypto ca certificate chain** *trustpoint*

## 構文の説明

| | |
|---|---|
| *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

次の表は、このコマンドを入力できるモードを示しています。

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

## コマンド履歴

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

## 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 モードが開始されます。証明書マッピング ルールの優先順位付けされたリストを管理するには、このコマンドのグループを使用します。マッピング ルールの順序はシーケンス番号によって決まります。クリプト 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* | *map-name sequence-number*}

**no crypto ca certificate map** {*sequence-number* | *map-name* [*sequence-number*]}

## 構文の説明

| | |
|---|---|
| *map-name* | certificate-to-group マップの名前を指定します。 |
| *sequence-number* | 作成する証明書マップ ルールの番号を指定します。指定できる範囲は 1 ～ 65535 です。トンネル グループを証明書マップ ルールにマッピングする tunnel-group-map を作成するときに、この番号を使用できます。 |

## デフォルト

sequence-number のデフォルトの動作や値はありません。

*map-name* のデフォルトの値は、DefaultCertificateMap です。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 | このコマンドが導入されました。 |
| 7.2 | *map-name* キーワードが追加されました。 |

## 使用上のガイドライン

このコマンドを発行すると、セキュリティ アプライアンスは CA 証明書マップ コンフィギュレーション モードになります。このモードでは、証明書の発行者名およびサブジェクト Distinguished Name（DN; 認定者名）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* のいずれかです。DN は、ITU-T X.509 標準で定義されています。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、次の表現または演算子で構成されます。

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

DN の一致表現は大文字と小文字が区別されません。

## 例

次に、example-map というマップ名とシーケンス番号 1（ルール番号 1）で CA 証明書マップ モードを開始し、subject-name という Common Name（CN; 一般名）属性が Example1 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 example-map 1
hostname(ca-certificate-map)# subject-name attr cn eq Example1
hostname(ca-certificate-map)#
```

次に、example-map というマップ名とシーケンス番号 1 で CA 証明書マップ モードを開始し、subject-name 内に値 cisco が含まれることを指定する例を示します。

```
hostname(config)# crypto ca certificate map example-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 エントリが IPSec ピア証明書の発行者 DN に適用されることを指定します。 |
| **subject-name（クリプト CA 証明書マップ）** | ルール エントリが IPSec ピア証明書のサブジェクト DN に適用されることを指定します。 |
| **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 エントリをトンネル グループに関連付けます。 |

# crypto ca crl request

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

**crypto ca crl request** *trustpoint*

## 構文の説明

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

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 使用上のガイドライン

このコマンドの呼び出しは、実行コンフィギュレーションの一部になりません。

## 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 コンフィギュレーション モードを開始します。 |

# crypto ca enroll

CA との登録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。このコマンドが正常に実行されるには、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**]

## 構文の説明

| | |
|---|---|
| **noconfirm** | （任意）すべてのプロンプトを表示しないようにします。要求される場合がある登録オプションは、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、または他の非対話形式で使用するためのものです。 |
| *trustpoint* | 登録するトラストポイントの名前を指定します。文字数は最大で 128 です。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

## コマンド履歴

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

## 使用上のガイドライン

トラストポイントが SCEP 登録用に設定されている場合、セキュリティ アプライアンスはただちに CLI プロンプトを表示し、コンソールへのステータス メッセージを非同期的に表示します。トラストポイントが手動登録用に設定されている場合、セキュリティ アプライアンスは Base-64 エンコード PKCS10 証明書要求をコンソールに書き込んでから、CLI プロンプトを表示します。

このコマンドは、参照されるトラストポイントの設定された状態に応じて、異なる対話形式プロンプトを生成します。

## 例

次に、SCEP 登録を使用して、トラストポイント tp1 でアイデンティティ証明書を登録する例を示します。セキュリティ アプライアンスは、トラストポイント コンフィギュレーションで保存されていない情報を要求します。

```
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)#
```

次のコマンドは、CA 証明書の手動登録を示しています。

```
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の CA 証明書を取得します。 |
| **crypto ca import pkcs12** | 手動登録要求への応答として CA から受信した証明書をインストールします。また、PKS12 データをトラストポイントにインポートするためにも使用されます。 |
| **crypto ca trustpoint** | 指定したトラストポイントに対してトラストポイント サブモードを開始します。 |

# crypto ca export

セキュリティ アプライアンスのトラストポイント コンフィギュレーションを、関連付けられているすべてのキーおよび証明書とともに PKCS12 形式でエクスポートするには、またはデバイスのアイデンティティ証明書を PEM 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* **identify-certificate**

## 構文の説明

| | |
|---|---|
| **identify-certificate** | 指定したトラストポイントに関連付けられている登録済み証明書をコンソールに表示することを指定します。 |
| *trustpoint* | 証明書が表示されるトラストポイントの名前を指定します。トラストポイント名の最大文字数は 128 文字です。 |

## 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

次の表は、このコマンドを入力できるモードを示しています。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 | このコマンドが導入されました。 |
| 8.0(2) | このコマンドは、PEM 形式での証明書のエクスポートに対応するために変更されました。 |

## 使用上のガイドライン

このコマンドの呼び出しは、アクティブなコンフィギュレーションには含まれません。PEM データまたは PKCS12 データはコンソールに書き込まれます。

Web ブラウザでは、パスワードベースの対称キーで保護された付属の公開キー証明書とともに秘密キーを格納するために PKCS12 形式を使用しています。セキュリティ デバイスは、トラストポイントに関連付けられている証明書とキーを Base-64 エンコード PKCS12 形式でエクスポートします この機能を使用して、証明書とキーをセキュリティ デバイス間で移動できます。

証明書の PEM エンコーディングは、PEM ヘッダーで囲まれた X.509 証明書の Base-64 エンコーディングです。これは、セキュリティ デバイス間で証明書をテキストベースで転送するための標準的な方法を提供します。セキュリティ デバイスがクライアントとして機能している場合、PEM エンコーディングは、SSL/TLS プロトコル プロキシを利用する *proxy-ldc-issuer* 証明書のエクスポートに使用できます。

**例**

次に、トラストポイント 222 の PEM 形式の証明書をコンソール表示としてエクスポートする例を示します。

```
hostname (config)# crypto ca export 222 identity-certificate

Exported 222 follows:
-----BEGIN CERTIFICATE-----
MIIGDzCCBXigAwIBAgIKFiUgwwAAAAAFPDANBgkqhkiG9w0BAQUFADCBnTEfMB0G
CSqGSIb3DQEJARYQd2Jyb3duQGNpc2NvLmNvbTELMAkGA1UEBhMCVVMxCzAJBgNV
BAgTAk1BMREwDwYDVQQHEwhGcmFua2xpbjEWMBQGA1UEChMNQ2lzY28gU3lzdGVt
czEZMBcGA1UECxMQRnJhbmtsaW4gRGV2VGVzdDEaMBgGA1UEAxMRbXMtcm9vdC1j
YS01LTIwMDQwHhcNMDYxMTAyMjIyNjU3WhcNMjQwNTIwMTMzNDUyWjA2MRQwEgYD
VQQFEwtKTVgwOTQwSzA0TDEeMBwGCSqGSIb3DQEJAhMPQnJpYW4uY2lzY28uY29t
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCvxxIYKcrb7cJpsiFKwwsQUph5
4M5Y3CDVKEVF+98HrD6rhd0n/d6R8VYSfu76aeJC5j9Bbn3xOCx2aY5K2enf3SBW
Y66S3JeZBV88etFmyYJ7rebjUVVQZaFcq79EjoP99IeJ3a89Y7dKvYqq8I3hmYRe
uipm1G6wfKHOrpLZnwIDAQABo4IDujCCA7YwCwYDVR0PBAQDAgWgMBoGA1UdEQQT
MBGCD0JyaWFuLmNpc2NvLmNvbTAdBgNVHQ4EFgQUocM/JeVV3fjZh4wDe0JS74Jm
pvEwgdkGA1UdIwSB0TCBzoAUYZ8t0+V9pox+Y47NtCLk7WxvIQShgaOkgaAwgZ0x
HzAdBgkqhkiG9w0BCQEWEHdicm93bkBjaXNjby5jb20xCzAJBgNVBAYTAlVTMQsw
CQYDVQQIEwJNQTERMA8GA1UEBxMIRnJhbmtsaW4xFjAUBgNVBAoTDUNpc2NvIFN5
c3RlbXMxGTAXBgNVBAsTEEZyYW5rbGluIERldlRlc3QxGjAYBgNVBAMTEW1zLXJv
b3QtY2EtNS0yMDA0ghBaZ5s0Ng4SskMxF2NlIoxgMIIBSAYDVR0fBIIBPzCCATsw
geuggeiggeWGgeJsZGFwOi8vd2luMmstYWQuRlJLLU1TLVBLSS5jaXNjby5jb20v
Q049bXMtcm9vdC1jYS01LTIwMDQsQ049d2luMmstYWQsQ049Q0RQLENOPVB1Ymxp
YyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24s
REM9RlJLLU1TLVBLSSxEQz1jaXNjbyxEQz1jb20/Y2VydGlmaWNhdGVSZXZvY2F0
aW9uTGlzdD9iYXNlP29iamVjdGNsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MEug
SaBHhkVodHRwOi8vd2luMmstYWQuZnJrLW1zLXBraS5jaXNjby5jb20vQ2VydEVu
cm9sbC9tcy1yb290LWNhLTUtMjAwNC5jcmwwggFCBggrBgEFBQcBAQSCATQwggEw
MIG8BggrBgEFBQcwAoaBr2xkYXA6Ly8vQ049bXMtcm9vdC1jYS01LTIwMDQsQ049
QUlBLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNv
bmZpZ3VyYXRpb24sREM9RlJLLU1TLVBLSSxEQz1jaXNjbyxEQz1jb20/Y0FDZXJ0
aWZpY2F0ZT9iYXNlP29iamVjdGNsYXNzPWNlcnRpZmljYXRpb25BdXRob3JpdHkw
bwYIKwYBBQUHMAKGY2h0dHA6Ly93aW4yay1hZC5mcmstbXMtcGtpLmNpc2NvLmNv
bS9DZXJ0RW5yb2xsL3dpbjJrLWFkLkZSSy1NUy1QS0kuY2lzY28uY29tX21zLXJv
b3QtY2EtNS0yMDA0LmNydDANBgkqhkiG9w0BAQUFAAOBgQBlh7maRutcKNpjPbLk
bdcafJfHQ3k4UoWo0s1A0LXzdF4SsBIKQmpbfqEHtlx4EsfvfHXxUQJ6TOab7axt
hxMbNX3m7giebvtPkreqR9OYWGUjZwFUZ16TWnPA/NP3fbqRSsPgOXkC7+/5oUJd
eAeJOF4RQ6fPpXw9LjO5GXSFQA==
-----END CERTIFICATE-----
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の CA 証明書を取得します。 |
| **crypto ca enroll** | CA への登録を開始します。 |
| **crypto ca import** | 手動登録要求への応答として CA から受信した証明書をインストールします。また、PKS12 データをトラストポイントにインポートするためにも使用されます。 |
| **crypto ca trustpoint** | 指定したトラストポイントのトラストポイント コンフィギュレーション モードを開始します。 |

# crypto ca import

手動登録要求への応答で CA から受信した証明書をインストールしたり、PKCS12 データを使用してトラストポイントの証明書とキー ペアをインポートしたりするには、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。セキュリティ アプライアンスは、ユーザに Base-64 形式で端末にテキストを貼り付けるように要求します。

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

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

## 構文の説明

| | |
|---|---|
| *trustpoint* | インポート アクションを関連付けるトラストポイントを指定します。文字数は最大で 128 です。PKCS12 データをインポートし、トラストポイントが RSA キーを使用する場合、インポートされるキー 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** | トラストポイントによって示される CA から証明書をインポートするようセキュリティ アプライアンスに指示します |
| **pkcs12** | PKCS12 形式を使用してトラストポイントの証明書とキー ペアをインポートするようセキュリティ アプライアンスに指示します。 |
| 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）非対話形式モードを使用して証明書をインポートします。すべてのプロンプトを表示しないようにします。このオプションは、スクリプト、ASDM、または対話が必要ないその他の場合に使用するオプションです。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 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
hostname (config)#
```

次に、PKCS12 データをトラストポイント central に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
hostname (config)#
```

## 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とキー ペアを PKCS12 形式でエクスポートします。 |
| **crypto ca authenticate** | トラストポイントの CA 証明書を取得します。 |
| **crypto ca enroll** | CA への登録を開始します。 |
| **crypto ca trustpoint** | 指定したトラストポイントに対してトラストポイント サブモードを開始します。 |

# crypto ca server

セキュリティ アプライアンス上のローカル CA サーバを設定および管理するには、グローバル コンフィギュレーション モードで **crypto ca server** コマンドを使用して設定 ca サーバ コンフィギュレーション モードを開始し、CA コンフィギュレーション コマンドにアクセスします。設定されているローカル CA サーバをセキュリティ アプライアンスから削除するには、このコマンドの **no** 形式を使用します。

**crypto ca server**

**no crypto ca server**

## デフォルト

認証局サーバは、セキュリティ アプライアンス上でイネーブルになっていません。

## 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。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.0(2) | このコマンドが導入されました。 |

## 使用上のガイドライン

セキュリティ アプライアンス上にローカル CA は 1 つしか存在できません。

**crypto ca server** コマンドは CA サーバを設定しますが、イネーブルにはしません。ローカル CA をイネーブルにするには、設定 ca サーバ モードで **shutdown** コマンドの **no** 形式を使用します。

**no shutdown** コマンドで CA サーバをアクティブにすると、CA および LOCAL-CA-SERVER というトラストポイントの RSA キー ペアが確立されて自己署名証明書が保持されます。この新しく生成された自己署名証明書には、「デジタル署名」、「crl 署名」および「証明書の署名」のキー使用設定が常に設定されています。

**注意**　**no crypto ca server** コマンドは、ローカル CA サーバの現在の状態に関係なく、設定済みのローカル CA サーバ、その RSA キー ペア、および関連付けられているトラストポイントを削除します。

## 例

次に、このコマンドを使用して設定 ca サーバ コンフィギュレーション モードを開始し、このモードで使用可能なローカル CA サーバ コマンドをリストするために疑問符を使用する例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# ?

CA Server configuration commands:
  cdp-url               CRL Distribution Point to be included in the issued
```

```
                        certificates
  database              Embedded Certificate Server database location
                        configuration
  enrollment-retrieval  Enrollment-retrieval timeout configuration
  exit                  Exit from Certificate Server entry mode
  help                  Help for crypto ca server configuration commands
  issuer-name           Issuer name
  keysize               Size of keypair in bits to generate for certificate
                        enrollments
  lifetime              Lifetime parameters
  no                    Negate a command or set its defaults
  otp                   One-Time Password configuration options
  renewal-reminder      Enrollment renewal-reminder time configuration
  shutdown              Shutdown the Embedded Certificate Server
  smtp                  SMTP settings for enrollment E-mail notifications
  subject-name-default  Subject name default configuration for issued
                        certificates
```

次に、設定済みでイネーブルになっている CA サーバをセキュリティ アプライアンスから削除するために、設定 ca サーバ モードで **crypto ca server** コマンドの **no** 形式を使用する例を示します。

```
hostname(config-ca-server)#no crypto ca server

Certificate server 'remove server' event has been queued for processing.
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **debug crypto ca server** | ローカル CA サーバを設定するときに、デバッグ メッセージを表示します。 |
| **show crypto ca server** | 設定されている CA サーバのステータスおよびパラメータを表示します。 |
| **show crypto ca server cert-db** | ローカル CA サーバ証明書を表示します。 |

# crypto ca server crl issue

Certificate Revocation List（CRL; 証明書失効リスト）の発行を強制的に行うには、特権 EXEC モードで **crypto ca server crl issue** コマンドを使用します。

**crypto ca server crl issue**

## 構文の説明

このコマンドにはキーワードまたは引数はありません。

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.0(2) | このコマンドが導入されました。 |

## 使用上のガイドライン

このコマンドは失われた CRL の回復に使われますが、ほとんど使用されることはありません。通常、CRL は失効時に既存の CRL に再署名することで自動的に再発行されます。**crypto ca server crl issue** コマンドは、証明書データベースに基づいて CRL を再生成します。また、このコマンドを使用するのは、証明書データベースの内容に基づいて CRL を再生成する必要がある場合だけです。

## 例

次に、ローカル CA サーバによる CRL の発行を強制的に行う例を示します。

```
hostname(config-ca-server)# crypto ca server crl issue
A new CRL has been issued.
hostname(config-ca-server)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **cdp-url** | CA によって発行される証明書に含める証明書失効リスト配布ポイントを指定します。 |

| コマンド | 説明 |
|---|---|
| **crypto ca server** | CA サーバ コンフィギュレーション モードの CLI コマンド セットへのアクセスを提供し、ユーザがローカル CA を設定および管理できるようにします。 |
| **crypto ca server revoke** | ローカル CA サーバが発行した証明書を、証明書データベースと CRL で失効としてマークします。 |
| **show crypto ca server crl** | ローカル CA の現在の CRL を表示します。 |

# crypto ca server revoke

ローカル Certificate Authority（CA; 認証局）サーバによって発行された証明書を証明書データベースと CRL で失効としてマークするには、特権 EXEC モードで **crypto ca server revoke** コマンドを使用します。

**crypto ca server revoke** *cert-serial-no*

## 構文の説明

| | |
|---|---|
| *cert-serial-no* | 失効させる証明書のシリアル番号を指定します。シリアル番号は 16 進形式で入力します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.0(2) | このコマンドが導入されました。 |

## 使用上のガイドライン

セキュリティ アプライアンス上のローカル CA によって発行された特定の証明書を失効させるには、そのセキュリティ アプライアンスで **crypto ca server revoke** コマンドを入力します。証明書は、このコマンドによって CA サーバの証明書データベースと CRL に失効としてマークされると失効します。失効させる証明書を指定するには、証明書のシリアル番号を 16 進形式で入力します。

指定した証明書が失効した後に、CRL が自動的に再生成されます。

## 例

次に、ローカル CA サーバによって発行されたシリアル番号 782ea09f の証明書を失効させる例を示します。

```
hostname(config-ca-server)## crypto ca server revoke 782ea09f
Certificate with the serial number 0x782ea09f has been revoked.A new CRL has been issued.

hostname(config-ca-server)#
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **crypto ca server crl issue** | CRL を強制的に発行します。 |
| **crypto ca server unrevoke** | ローカル CA サーバによって発行され、すでに失効している証明書の失効を取り消します。 |
| **crypto ca server user-db remove** | CA サーバのユーザ データベースからユーザを削除します。 |
| **show crypto ca server crl** | ローカル CA の現在の CRL を表示します。 |
| **show crypto ca server user-db** | CA サーバのユーザ データベースに含まれているユーザを表示します。 |

# crypto ca server unrevoke

ローカル CA サーバによって発行され、すでに失効している証明書の失効を取り消すには、特権 EXEC モードで **crypto ca server unrevoke** コマンドを使用します。

**crypto ca server unrevoke** *cert-serial-no*

## 構文の説明

| | |
|---|---|
| *cert-serial-no* | 失効を取り消す証明書のシリアル番号を指定します。シリアル番号は 16 進形式で入力します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.0(2) | このコマンドが導入されました。 |

## 使用上のガイドライン

セキュリティ アプライアンス上のローカル CA によって発行され、すでに失効している証明書の失効を取り消すには、**crypto ca server unrevoke** コマンドを入力します。証明書は、このコマンドによって証明書が証明書データベースで有効とマークされ、CRL から削除されると、再び有効になります。失効を取り消す証明書を指定するには、証明書のシリアル番号を 16 進形式で入力します。

指定した証明書の失効が取り消された後に、CRL が自動的に再生成されます。

## 例

次に、ローカル CA サーバによって発行されたシリアル番号 782ea09f の証明書の失効を取り消す例を示します。

```
hostname(config-ca-server)# crypto ca server unrevoke 782ea09f
Certificate with the serial number 0x782ea09f has been unrevoked.A new CRL has been
issued.

hostname(config-ca-server)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **crypto ca server** | CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。 |
| **crypto ca server crl issue** | CRL を強制的に発行します。 |
| **crypto ca server revoke** | ローカル CA サーバが発行した証明書を、証明書データベースと CRL で失効としてマークします。 |
| **crypto ca server user-db add** | CA サーバのユーザ データベースにユーザを追加します。 |
| **show crypto ca server cert-db** | ローカル CA サーバ証明書を表示します。 |
| **show crypto ca server user-db** | CA サーバのユーザ データベースに含まれているユーザを表示します。 |

# crypto ca server user-db add

CA サーバのユーザ データベースに新しいユーザを挿入するには、特権 EXEC モードで **crypto ca server user-db add** コマンドを使用します。

**crypto ca server user-db add** *user* [**dn** *dn*] **[email** *e-mail-address*]

## 構文の説明

| | |
|---|---|
| **dn** *dn* | 追加するユーザに対して発行される証明書のサブジェクト名認定者名を指定します。DN ストリングにカンマが含まれる場合、値のストリングを二重引用符で囲みます（たとえば、O="Company, Inc."）。 |
| **email** *e-mail-address* | 新しいユーザの電子メール アドレスを指定します。 |
| *user* | 登録特権の付与対象となる 1 人のユーザを指定します。ユーザ名は、単純なユーザ名または電子メール アドレスです。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.0(2) | このコマンドが導入されました。 |

## 使用上のガイドライン

*user* 引数には単純なユーザ名（jandoe など）または電子メール アドレス（jandoe@example.com など）を指定できます。*username* は、エンド ユーザが登録ページで指定したユーザ名と一致する必要があります。

*username* は、特権のないユーザとしてデータベースに追加されます。登録特権を付与するには、**crypto ca server allow** コマンドを使用する必要があります。

*username* をワンタイム パスワードとともに使用して、登録インターフェイス ページでユーザを登録します。

**（注）** ワンタイム パスワード（OTP）を電子メールで通知するには、*username* フィールドまたは *email-address* フィールドに電子メール アドレスを指定する必要があります。メール送信時に電子メール アドレスが指定されていない場合、エラーが生成されます。

*user* 引数の **email** は、ユーザに登録と更新を忘れないように通知するための電子メール アドレスとしてのみ使用され、発行される証明書には表示されません。

電子メール アドレスを指定すると、質問がある場合にユーザに連絡することができ、また、その電子メール アドレス宛てに、登録に必要なワンタイム パスワードが通知されます。

ユーザにオプションの *dn* が指定されていない場合、サブジェクト名 dn は、*username* と subject-name-default DN 設定を使用して cn=*username*,subject-name-default として形成されます。

## 例

次に、ユーザ名 jandoe@example.com のユーザを完全なサブジェクト名 DN とともにユーザ データベースに追加する例を示します。

```
hostname(config-ca-server)# crypto ca server user-db add dn "cn=Jan Doe, ou=engineering,
o=Example, l=RTP, st=NC, c=US"
hostname(config-ca-server)#
```

次に、jondoe というユーザに登録特権を付与する例を示します。

```
hostname(config-ca-server)# crypto ca server user-db allow jondoe
hostname(config-ca-server)
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **crypto ca server** | CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。 |
| **crypto ca server user-db allow** | CA サーバ データベース内の特定のユーザまたはユーザのサブセットに、CA への登録を許可します。 |
| **crypto ca server user-db remove** | CA サーバ データベースからユーザを削除します。 |
| **crypto ca server user-db write** | **database path** コマンドで指定したファイルに、CA サーバ データベース内のユーザ情報をコピーします。 |
| **database path** | ローカル CA データベースのパスまたは場所を指定します。デフォルトの場所はフラッシュ メモリです。 |

# crypto ca server user-db allow

ユーザまたはユーザのグループにローカル CA サーバ データベースへの登録を許可するには、特権 EXEC モードで **crypto ca server user-db allow** コマンドを使用します。このコマンドには、ワンタイム パスワードを生成および表示したり、ワンタイム パスワードをユーザに電子メールで送信したりするオプションも含まれています。

**crypto ca server user-db allow** {*username* | **all-unenrolled** | **all-certholders**} [**display-otp**] [**email-otp**] [**replace-otp** ]

## 構文の説明

| | |
|---|---|
| **all-certholders** | 証明書が現在有効かどうかに関係なく、証明書が発行されているデータベース内のすべてのユーザに登録特権を付与することを指定します。これは、更新特権の付与と同じです。 |
| **all-unenrolled** | 証明書が発行されていないデータベース内のすべてのユーザに登録特権を付与することを指定します。 |
| **email-otp** | （任意）指定したユーザのワンタイム パスワードを、それらのユーザの設定済み電子メール アドレスに電子メールで送信します。 |
| **replace-otp** | （任意）指定したユーザのうち、有効なワンタイム パスワードを当初は持っていたすべてのユーザに対してワンタイム パスワードを再生成することを指定します。 |
| **display-otp** | （任意）指定したすべてのユーザのワンタイム パスワードをコンソールに表示します。 |
| *username* | 登録特権の付与対象となる 1 人のユーザを指定します。ユーザ名として簡易ユーザ名または電子メール アドレスを指定できます。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.0(2) | このコマンドが導入されました。 |

## 使用上のガイドライン

**replace-otp** キーワードを指定すると、指定したすべてのユーザに対して OTP が生成されます。指定したユーザに対して以前に生成された有効な OTP は、これらの新しい OTP で置き換えられます。

OTP は、セキュリティ デバイスに保存されませんが、ユーザに通知したり、登録時にユーザを認証したりする必要がある場合に生成および再生成されます。

## 例

次に、データベース内のすべての未登録ユーザに登録特権を付与する例を示します。

```
hostname(config-ca-server)# crypto ca server user-db allow all-unenrolled
hostname(config-ca-server)#
```

次に、user1 というユーザに登録特権を付与する例を示します。

```
hostname(config-ca-server)# crypto ca server user-db allow user1
hostname(config-ca-server)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **crypto ca server** | CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。 |
| **crypto ca server user-db add** | CA サーバのユーザ データベースにユーザを追加します。 |
| **crypto ca server user-db write** | **database path** コマンドで指定したファイルに、CA サーバ データベース内のユーザ情報をコピーします。 |
| **enrollment-retrieval** | 登録されたユーザが PKCS12 登録ファイルを取得できる期間を時間単位で指定します。 |
| **show crypto ca server cert-db** | ローカル CA によって発行された証明書をすべて表示します。 |

# crypto ca server user-db email-otp

ローカル CA サーバ データベース内の特定のユーザまたはユーザのサブセットに OTP を電子メールで送信するには、特権 EXEC モードで **crypto ca server user-db email-otp** コマンドを使用します。

**crypto ca server user-db email-otp** {*username* | **all-unenrolled** | **all-certholders**}

## 構文の説明

| | |
|---|---|
| **all-certholders** | 証明書が現在有効かどうかに関係なく、その証明書が発行されているデータベース内のすべてのユーザに OTP を電子メールで送信することを指定します。 |
| **all-unenrolled** | 証明書が一度も発行されていないか、期限が切れた証明書または失効した証明書しか保持していない、データベース内のすべてのユーザに OTP を電子メールで送信することを指定します。 |
| *username* | 1 人のユーザ用の OTP をそのユーザに電子メールで送信することを指定します。ユーザ名として簡易ユーザ名または電子メール アドレスを指定できます。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.0(2) | このコマンドが導入されました。 |

## 例

次に、データベース内のすべての未登録ユーザに OTP を電子メールで送信する例を示します。

```
hostname(config-ca-server)# crypto ca server user-db email-otp all-unenrolled
hostname(config-ca-server)#
```

次に、user1 というユーザに OTP を電子メールで送信する例を示します。

```
hostname(config-ca-server)# crypto ca server user-db email-otp user1
hostname(config-ca-server)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **crypto ca server user-db show-otp** | CA サーバ データベース内の特定のユーザまたはユーザのサブセットのワンタイム パスワードを表示します。 |
| **show crypto ca server cert-db** | ローカル CA によって発行された証明書をすべて表示します。 |
| **show crypto ca server user-db** | CA サーバのユーザ データベースに含まれているユーザを表示します。 |

# crypto ca server user-db remove

ローカル CA サーバのユーザ データベースからユーザを削除するには、特権 EXEC モードで **crypto ca server user-db remove** コマンドを使用します。

**crypto ca server user-db remove** *username*

## 構文の説明

| | |
|---|---|
| *username* | 削除するユーザの名前を、ユーザ名または電子メール アドレスの形式で指定します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.0(2) | このコマンドが導入されました。 |

## 使用上のガイドライン

このコマンドは、CA ユーザ データベースからユーザ名を削除して、ユーザが登録できないようにします。また、このコマンドには、前に発行された有効な証明書を失効させるオプションもあります。

## 例

次に、ユーザ名 user1 のユーザを CA サーバのユーザ データベースから削除する例を示します。

```
hostname(config-ca-server)# crypto ca server user-db remove user1

WARNING: No certificates have been automatically revoked. Certificates issued to user
user1 should be revoked if necessary.

hostname(config-ca-server)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **crypto ca server crl issue** | CRL を強制的に発行します。 |
| **crypto ca server revoke** | ローカル CA サーバが発行した証明書を、証明書データベースと CRL で失効としてマークします。 |

| コマンド | 説明 |
|---|---|
| **show crypto ca server user-db** | CA サーバのユーザ データベースに含まれているユーザを表示します。 |
| **crypto ca server user-db write** | ローカル CA データベースに設定されているユーザ情報を、**database path** コマンドで指定したファイルに書き込みます。 |

# crypto ca server user-db show-otp

ローカル CA サーバ データベース内の特定のユーザまたはユーザのサブセットの OTP を表示するには、特権 EXEC モードで **crypto ca server user-db show-otp** コマンドを使用します。

**crypto ca server user-db show-otp** {*username* | **all-certholders** | **all-unenrolled**}

## 構文の説明

| | |
|---|---|
| **all-certholders** | 証明書が現在有効かどうかに関係なく、その証明書が発行されているデータベース内のすべてのユーザの OTP を表示します。 |
| **all-unenrolled** | 証明書が一度も発行されていないか、期限が切れた証明書または失効した証明書しか保持していない、データベース内のすべてのユーザの OTP を表示します。 |
| *username* | 1 人のユーザの OTP を表示することを指定します。ユーザ名として簡易ユーザ名または電子メール アドレスを指定できます。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.0(2) | このコマンドが導入されました。 |

## 例

次に、有効または無効な証明書を持つデータベース内のすべてのユーザの OTP を表示する例を示します。

```
hostname(config-ca-server)# crypto ca server user-db show-otp all-certholders
hostname(config-ca-server)#
```

次に、user1 というユーザの OTP を表示する例を示します。

```
hostname(config-ca-server)# crypto ca server user-db show-otp user1
hostname(config-ca-server)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **crypto ca server user-db add** | CA サーバのユーザ データベースにユーザを追加します。 |
| **crypto ca server user-db allow** | CA サーバ データベース内の特定のユーザまたはユーザのサブセットに、ローカル CA への登録を許可します。 |
| **crypto ca server user-db email-otp** | CA サーバ データベース内の特定のユーザまたはユーザのサブセットにワンタイム パスワードを電子メールで送信します。 |
| **show crypto ca server cert-db** | ローカル CA によって発行された証明書をすべて表示します。 |

# crypto ca server user-db write

すべてのローカル CA データベース ファイルを保存するディレクトリの場所を設定するには、特権 EXEC モードで **crypto ca server user-db write** コマンドを使用します。

**crypto ca server user-db write**

## 構文の説明

このコマンドにはキーワードまたは引数はありません。

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.0(2) | このコマンドが導入されました。 |

## 使用上のガイドライン

**crypto ca server user-db write** コマンドを使用して、新しいユーザベースのコンフィギュレーション データを、データベース パス コンフィギュレーションで指定した場所に保存します。この情報は、**crypto ca server user-db add** コマンドおよび **crypto ca server user-db allow** コマンドで新しいユーザが追加または許可されると生成されます。

## 例

次に、ローカル CA データベースに設定されているユーザ情報を保存場所に書き込む例を示します。

```
hostname(config-ca-server)# crypto ca server user-db write
hostname(config-ca-server)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **crypto ca server user-db add** | CA サーバのユーザ データベースにユーザを追加します。 |
| **database path** | ローカル CA データベースのパスまたは場所を指定します。デフォルトの場所はフラッシュ メモリです。 |

| コマンド | 説明 |
|---|---|
| **crypto ca server user-db remove** | CA サーバのユーザ データベースからユーザを削除します。 |
| **show crypto ca server cert-db** | ローカル CA によって発行された証明書をすべて表示します。 |
| **show crypto ca server user-db** | CA サーバのユーザ データベースに含まれているユーザを表示します。 |

# crypto ca trustpoint

指定したトラストポイントのトラストポイント 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。

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

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

## 構文の説明

| | |
|---|---|
| **noconfirm** | すべての対話形式プロンプトを非表示にします。 |
| *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

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが導入されました。 |
| 7.2(1) | Online Certificate Status Protocol をサポートするためにサブコマンドが追加されました。これらのサブコマンドには、**match certificate map**、**ocsp disable-nonce**、**ocsp url**、**revocation-check** が含まれます。 |
| 8.0(2) | 証明書の検証をサポートするサブコマンドが追加されました。これらのサブコマンドには、**id-usage** と **validation-policy** が含まれます。**accept-subordinates**、**id-cert-issuer**、および **support-user-cert-validation** は廃止されました。 |
| 8.0(4) | 信頼できるエンタープライズ間（Phone-Proxy と TLS-Proxy 間など）での自己署名証明書の登録をサポートするために、**enrollment self** サブコマンドが追加されました。 |

## 使用上のガイドライン

CA を宣言するには、**crypto ca trustpoint** コマンドを使用します。このコマンドを発行すると、クリプト CA トラストポイント コンフィギュレーション モードが開始されます。

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 が発行する証明書に基づいた CA のアイデンティティとデバイスのアイデンティティを表します。トラストポイント サブモード内のコマンドは、CA 固有のコンフィギュレーション パラメータを制御します。これらのパラメータでは、セキュリティ アプライアンスが CA 証明書を取得する方法、セキュリティ アプライアンスが CA から証明書を取得する方法、および CA が発行するユーザ証明書の認証ポリシーを指定しま

す。

このコマンド リファレンス ガイドにアルファベット順で記載されている次のコマンドを使用して、トラストポイントの特性を指定できます。

- **accept-subordinates**：トラストポイントに関連付けられた CA に従属する CA 証明書がデバイスにインストールされていない場合、フェーズ 1 の IKE 交換中にその CA 証明書が提供されたときに、それを受け入れるかどうかを指定します。
- **client-types**：このトラストポイントを使用して、ユーザ接続に関連付けられた証明書を検証できるクライアント接続タイプを指定します。
- **crl required | optional | nocheck**：CRL コンフィギュレーション オプションを指定します。
- **crl configure**：CRL コンフィギュレーション モードを開始します（**crl** を参照）。
- **default enrollment**：すべての登録パラメータをシステム デフォルト値に戻します。このコマンドの呼び出しは、アクティブなコンフィギュレーションには含まれません。
- **email** *address*：登録中に、指定した電子メール アドレスを証明書のサブジェクト代替名の拡張に含めるかどうかを CA に確認します。
- **enrollment retry period**：SCEP 登録の再試行期間を分単位で指定します。
- **enrollment retry count**：SCEP 登録に許可する最大試行回数を指定します。
- **enrollment self**：自己署名証明書を生成する登録を指定します。
- **enrollment terminal**：このトラストポイントへのカット アンド ペースト登録を指定します。
- **enrollment url** *url*：このトラストポイントに登録する SCEP 登録を指定し、登録 URL（*url*）を設定します。
- **exit**：コンフィギュレーション モードを終了します。
- **fqdn** *fqdn*：登録中に、指定した FQDN を証明書のサブジェクト代替名の拡張に含めるかどうかを CA に確認します。
- **id-cert-issuer**：廃止されました。このトラストポイントに関連付けられた CA によって発行されるピア証明書をシステムが受け入れるかどうかを指定します。
- **id-usage**：トラストポイントの登録済み ID の使用方法を指定します。
- **ignore-ipsec-keyusage**：廃止されました。IPsec クライアント証明書のキー使用チェックを行わないようにします。
- **ignore-ssl-keyusage**：廃止されました。SSL クライアント証明書のキー使用チェックを行わないようにします。
- **ip-addr** *ip-address*：登録中に、セキュリティ アプライアンスの IP アドレスを証明書に含めるかどうかを CA に確認します。
- **keypair** *name*：公開キーが証明対象となるキー ペアを指定します。
- **match certificate** *map-name* **override ocsp**：証明書マップを OCSP 上書きルールと照合します。
- **ocsp disable-nonce**：ナンス拡張子をディセーブルにします。ナンス拡張子は、失効要求と応答を結び付けて暗号化して、リプレイ アタックを回避するためのものです。
- **ocsp url**：この URL の OCSP サーバで、トラストポイントに関連するすべての証明書の失効ステータスをチェックすることを指定します。
- **password** *string*：登録中に CA に登録されるチャレンジ フレーズを指定します。通常、CA はこのフレーズを使用して、その後の失効要求を認証します。
- **proxy-ldc-issuer**：TLS プロキシ ローカル ダイナミック証明書の発行者を指定します。
- **revocation check**：失効をチェックする方法（CRL、OCSP、none）を指定します。

- **serial-number**：登録中に、セキュリティ アプライアンスのシリアル番号を証明書に含めるかどうかを CA に確認します。
- **subject-name** *X.500 name*：登録中に、指定したサブジェクト DN を証明書に含めるかどうかを CA に確認します。
- **support-user-cert-validation**：廃止されました。イネーブルの場合、リモート証明書を発行した CA に対してトラストポイントが認証されていれば、リモート ユーザ証明書を検証するコンフィギュレーション設定をこのトラストポイントから取得できます。このオプションは、サブコマンド **crl required | optional | nocheck** および CRL サブモードのすべての設定に関連付けられたコンフィギュレーション データに適用されます。
- **validation-policy**：廃止されました。ユーザ接続に関連付けられている証明書を検証するためのトラストポイントの条件を指定します。

## 例

次に、central という名前のトラストポイントを管理するために 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の CA 証明書を取得します。 |
| **crypto ca certificate map** | クリプト CA 証明書マップ モードを開始します。証明書ベースの ACL を定義します。 |
| **crypto ca crl request** | 指定したトラストポイントのコンフィギュレーション パラメータに基づいて、CRL を要求します。 |
| **crypto ca import** | 手動登録要求への応答として CA から受信した証明書をインストールします。また、PKS12 データをトラストポイントにインポートするためにも使用されます。 |

# crypto dynamic-map match address

アクセス リストのアドレスをダイナミック クリプト マップ エントリに一致させるには、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。アドレス一致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 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*

## 構文の説明

| | |
|---|---|
| *acl-name* | ダイナミック クリプト マップ エントリに一致させるアクセス リストを指定します。 |
| *dynamic-map-name* | ダイナミック クリプト マップ セットの名前を指定します。 |
| *dynamic-seq-num* | ダイナミック クリプト マップ エントリに対応するシーケンス番号を指定します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 既存 | このコマンドは既存です。 |

## 使用上のガイドライン

このコマンドの詳細については、**crypto map match address** コマンドを参照してください。

## 例

次に、**crypto dynamic-map** コマンドを使用して、aclist1 という名前のアクセス リストのアドレスに一致させる例を示します。

```
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 クリプト マップのすべてのコンフィギュレーションをクリアします。 |
| **show running-config crypto dynamic-map** | すべてのダイナミック クリプト マップのすべてのコンフィギュレーションを表示します。 |

# crypto dynamic-map set nat-t-disable

接続の NAT-T をクリプト マップ エントリに基づいてディセーブルにするには、グローバル コンフィギュレーション モードで **crypto dynamic-map set nat-t-disable** コマンドを使用します。このクリプト マップ エントリの NAT-T をイネーブルにするには、このコマンドの **no** 形式を使用します。

**crypto dynamic-map** *dynamic-map-name dynamic-seq-num* **set nat-t-disable**

**no crypto dynamic-map** *dynamic-map-name dynamic-seq-num* **set nat-t-disable**

## 構文の説明

| | |
|---|---|
| *dynamic-map-name* | ダイナミック クリプト マップ セットの名前を指定します。 |
| *dynamic-seq-num* | ダイナミック クリプト 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オフです。

## 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 | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

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

## 使用上のガイドライン

NAT-T をグローバルにイネーブルにするには、**isakmp nat-traversal** コマンドを使用します。その後、**crypto dynamic-map set nat-t-disable** コマンドを使用して、特定のクリプト マップ エントリの NAT-T をディセーブルにできます。

## 例

次のコマンドでは、mymap という名前のダイナミック クリプト マップの NAT-T をディセーブルにします。

```
hostname(config)# crypto dynamic-map mymap 10 set nat-t-disable
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 クリプト マップのすべてのコンフィギュレーションをクリアします。 |
| **show running-config crypto dynamic-map** | すべてのダイナミック クリプト マップのすべてのコンフィギュレーションを表示します。 |

# crypto dynamic-map set peer

このコマンドの詳細については、**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*

## 構文の説明

| | |
|---|---|
| *dynamic-map-name* | ダイナミック クリプト マップ セットの名前を指定します。 |
| *dynamic-seq-num* | ダイナミック クリプト マップ エントリに対応するシーケンス番号を指定します。 |
| *ip_address* | **name** コマンドで定義されているように、ダイナミック クリプト マップ エントリのピアを IP アドレスで指定します。 |
| *hostname* | **name** コマンドで定義されているように、ダイナミック クリプト マップ エントリのピアをホスト名で指定します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 既存 | このコマンドは既存です。 |

## 例

次に、mymap という名前のダイナミック マップのピアを IP アドレス 10.0.0.1 に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 クリプト マップのすべてのコンフィギュレーションをクリアします。 |
| **show running-config crypto dynamic-map** | すべてのダイナミック クリプト マップのすべてのコンフィギュレーションを表示します。 |

# crypto dynamic-map set pfs

ダイナミック クリプト マップ 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 dynamic-map set pfs** コマンドを使用します。指定したダイナミック クリプト 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。

このコマンドの詳細については、**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]**

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

## 構文の説明

| | |
|---|---|
| *dynamic-map-name* | ダイナミック クリプト マップ セットの名前を指定します。 |
| *dynamic-seq-num* | ダイナミック クリプト マップ エントリに対応するシーケンス番号を指定します。 |
| **group1** | IPSec で新しい Diffie-Hellman 交換を実行するときに、768 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。 |
| **group2** | IPSec で新しい Diffie-Hellman 交換を実行するときに、1024 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。 |
| **group5** | IPSec で新しい Diffie-Hellman 交換を実行するときに、1536 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。 |
| **set pfs** | ダイナミック クリプト マップ エントリ用の新しいセキュリティ アソシエーションの要求時に Perfect Forward Secrecy（PFS; 完全転送秘密）を要求するように IPSec を設定するか、新しいセキュリティ アソシエーションの要求の受信時に PFS を要求するように IPSec を設定します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、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 | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドは変更され Diffie-Hellman グループ 7 が追加されました。 |
| 8.0(4) | **group 7** コマンド オプションは**廃止されました**。グループ 7 を設定しようとするとエラー メッセージが生成され、代わりにグループ 5 が使用されます。 |

## 使用上のガイドライン

**crypto dynamic-map** コマンド（**match address**、**set peer**、**set pfs** など）については、**crypto map** コマンドの項で説明します ピアがネゴシエーションを開始するときに、ローカル コンフィギュレーションで 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、ネゴシエーションは失敗します。ローカル コンフィギュレーションでグループが指定されていない場合、セキュリティ アプライアンスはデフォルトの group2 が指定されているものと見なします。ローカル コンフィギュレーションで PFS が指定されていない場合は、ピアからの PFS のオファーがすべて受け入れられます。

セキュリティ アプライアンスは、Cisco VPN Client と対話するときに PFS 値を使用しません。その代わり、フェーズ 1 でネゴシエートされた値を使用します。

## 例

次に、ダイナミック クリプト マップ mymap 10 用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 を使用するよう指定する例を示します。指定されているグループはグループ 2 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 クリプト マップのすべてのコンフィギュレーションをクリアします。 |
| **show running-config crypto dynamic-map** | すべてのダイナミック クリプト マップのすべてのコンフィギュレーションを表示します。 |

# crypto dynamic-map set reverse route

このコマンドの詳細については、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**

## 構文の説明

| | |
|---|---|
| *dynamic-map-name* | クリプト マップ セットの名前を指定します。 |
| *dynamic-seq-num* | クリプト 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

このコマンドのデフォルト値はオフです。

## 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 | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

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

## 例

次のコマンドでは、mymap という名前のダイナミック クリプト マップの RRI をイネーブルにします。

```
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 クリプト マップのすべてのコンフィギュレーションをクリアします。 |
| **show running-config crypto dynamic-map** | すべてのダイナミック クリプト マップのすべてのコンフィギュレーションを表示します。 |

# crypto dynamic-map set transform-set

ダイナミック クリプト マップ エントリで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 dynamic-map set transform-set** コマンドを使用します。

**crypto dynamic-map** *dynamic-map-name dynamic-seq-num* **set transform-set** *transform-set-name1* [*… transform-set-name11*]

ダイナミック クリプト マップ エントリからトランスフォーム セットを削除するには、このコマンドの **no** 形式で、削除するトランスフォーム セットの名前を指定します。

**no crypto dynamic-map** *dynamic-map-name dynamic-seq-num* **set transform-set** *transform-set-name1* [*… transform-set-name11*]

トランスフォーム セットをすべて指定するかまたは何も指定せずに、このコマンドの **no** 形式を使用すると、ダイナミック クリプト マップ エントリが削除されます。

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

## 構文の説明

| | |
|---|---|
| *dynamic-map-name* | ダイナミック クリプト マップ セットの名前を指定します。 |
| *dynamic-seq-num* | ダイナミック クリプト マップ エントリに対応するシーケンス番号を指定します。 |
| *transform-set-name1* *transform-set-name11* | トランスフォーム セットの名前を 1 つ以上指定します。このコマンドで指定するトランスフォーム セットは、**crypto ipsec transform-set** コマンドで定義されている必要があります。各クリプト マップ エントリは、11 個までのトランスフォーム セットをサポートしています。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 | このコマンドが導入されました。 |
| 7.2(1) | クリプト マップ エントリにおけるトランスフォーム セットの最大数が変更されました。 |

## 使用上のガイドライン

ダイナミック クリプト マップは、いずれのパラメータも設定されていないクリプト マップです。ダイナミック クリプト マップは、欠落しているパラメータが、IPsec ネゴシエーションの結果として、ピアの要件に合うように後でダイナミックに学習されるポリシー テンプレートの役割を果たします。セ

キュリティ アプライアンスは、スタティック クリプト マップでピアの IP アドレスがまだ指定されていない場合、ピアでトンネルをネゴシエートさせるためにダイナミック クリプト マップを適用します。これは、次のタイプのピアで発生します。

- パブリック IP アドレスがダイナミックに割り当てられるピア。

  LAN-to-LAN のピア、およびリモート アクセスするピアは、両方とも DHCP を使用してパブリック IP アドレスを取得できます。セキュリティ アプライアンスは、トンネルを開始するときだけこのアドレスを使用します。

- プライベート IP アドレスがダイナミックに割り当てられるピア。

  通常、リモート アクセスのトンネルを要求するピアは、ヘッドエンドによって割り当てられたプライベート IP アドレスを持っています 一般に、LAN-to-LAN トンネルには、事前に決定済みのプライベート ネットワークのセットがあり、スタティック マップを設定し、IPSec SA を確立するために使用されます。

管理者がスタティック クリプト マップを設定するため、（DHCP または別の方法で）ダイナミックに割り当てられた IP アドレスがわからない場合や、割り当て方法には関係なく他のクライアントのプライベート IP アドレスがわからない場合があります。通常、VPN クライアントは、スタティック IP アドレスを持たないため、IPSec ネゴシエーションを開始するためにダイナミック クリプト マップを必要とします。たとえば、ヘッドエンドが IKE のネゴシエーション中に Cisco VPN Client に IP アドレスを割り当て、クライアントはこのアドレスを IPSec SA のネゴシエーションで使用します。

ダイナミック クリプト マップを使用すると、IPsec のコンフィギュレーションが簡単になります。ダイナミック クリプト マップは、ピアが常に事前に決定されるとは限らないネットワークで使用することを推奨します。ダイナミック クリプト マップは、Cisco VPN Client（モバイル ユーザなど）、およびダイナミックに割り当てられた IP アドレスを取得するルータに対して使用してください。

**ヒント**　ダイナミック クリプト マップの **permit** エントリに **any** キーワードを使用する場合は、注意が必要です。このような **permit** エントリの対象となるトラフィックにマルチキャストやブロードキャストのトラフィックが含まれる場合、該当するアドレス範囲について **deny** エントリをアクセス リストに挿入します。ネットワークとサブネットのブロードキャスト トラフィック、および IPSec で保護されない他のすべてのトラフィックについて **deny** エントリを挿入するようにしてください。

ダイナミック クリプト マップは、接続を開始したリモートのピアと SA をネゴシエートするときだけ機能します。セキュリティ アプライアンスは、ダイナミック クリプト マップを使用してリモート ピアとの接続を開始することはできません。ダイナミック クリプト マップを設定した場合は、発信トラフィックがアクセス リストの permit エントリに一致する場合でも、対応する SA が存在しないと、セキュリティ アプライアンスはそのトラフィックをドロップします。

クリプト マップ セットには、ダイナミック クリプト マップを含めることができます。ダイナミック クリプト マップのセットには、クリプト マップ セットで一番低いプライオリティ（つまり、一番大きいシーケンス番号）を設定し、セキュリティ アプライアンスが他のクリプト マップを先に評価するようにする必要があります。セキュリティ アプライアンスは、他の（スタティック）マップのエントリが一致しない場合にだけ、ダイナミック クリプト マップのセットを調べます。

スタティック クリプト マップ セットと同様に、ダイナミック クリプト マップ セットにも、同じ dynamic-map-name を持つすべてのダイナミック クリプト マップを含めます。dynamic-seq-num によって、セット内のダイナミック クリプト マップが区別されます。ダイナミック クリプト マップを設定する場合は、クリプト アクセス リストに対して IPSec ピアのデータ フローを指定するために許可 ACL を挿入します。このように設定しないと、セキュリティ アプライアンスは、ピアが提示するあらゆるデータ フロー ID を受け入れることになります。

**注意**　ダイナミック クリプト マップ セットを使用して設定されたセキュリティ アプライアンス インターフェイスにトンネリングされるトラフィックに対してスタティック（デフォルト）ルートを割り当てないでください。トンネリングされるトラフィックを指定するには、ダイナミック クリプト マップに ACL を追加します。リモート アクセス トンネルに関連付けられた ACL を設定する場合は、適切なアドレス プールを指定してください。逆ルート注入を使用してルートをインストールするのは、必ずトンネルがアップ状態になった後にしてください。

1 つのクリプト マップ セット内で、スタティック マップ エントリとダイナミック マップ エントリを組み合わせることができます。

## 例

次に、10 個の同じトランスフォーム セットから成る「dynamic0」というダイナミック クリプト マップ エントリを作成する例を示します。「crypto ipsec transform-set（トランスフォーム セットの作成または削除）」の項には、10 個のトランスフォーム セット サンプル コマンドが示されています。

```
hostname(config)# crypto dynamic-map dynamic0 1 set transform-set 3des-md5 3des-sha
56des-md5 56des-sha 128aes-md5 128aes-sha 192aes-md5 192aes-sha 256aes-md5 256aes-sha
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **crypto ipsec transform-set** | トランスフォーム セットを設定します。 |
| **crypto map set transform-set** | クリプト マップ エントリで使用するトランスフォーム セットを指定します。 |
| **clear configure crypto dynamic-map** | すべてのダイナミック クリプト マップをコンフィギュレーションからクリアします。 |
| **show running-config crypto dynamic-map** | ダイナミック クリプト マップのコンフィギュレーションを表示します。 |
| **show running-config crypto map** | クリプト マップの設定内容を表示します。 |

# crypto ipsec df-bit

IPSec パケットの DF-bit 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*

## 構文の説明

| | |
|---|---|
| **clear-df** | （任意）外部 IP ヘッダーで DF ビットがクリアされること、およびセキュリティ アプライアンスはパケットをフラグメント化して IPSec カプセル化を追加する場合があることを指定します。 |
| **copy-df** | （任意）セキュリティ アプライアンスが外部 DF ビット設定を元のパケット内で探すことを指定します。 |
| **set-df** | （任意）外部 IP ヘッダーに DF ビットを設定することを指定します。ただし、元のパケットで DF ビットがクリアされている場合、セキュリティ アプライアンスはパケットをフラグメント化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。 |

## 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。設定を指定せずにこのコマンドをイネーブルにすると、セキュリティ アプライアンスはデフォルトとして **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 | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | • | • | — | — |

## コマンド履歴

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

## 使用上のガイドライン

DF ビットを IPSec トンネル機能とともに使用すると、セキュリティ アプライアンスが、カプセル化されたヘッダーで Don't Fragment（DF）ビットをクリア、設定、またはコピーできるかどうかを指定できます。IP ヘッダー内の DF ビットにより、デバイスがパケットをフラグメント化できるかどうかが決定されます。

カプセル化されたヘッダーに DF ビットを指定するようにセキュリティ アプライアンスを設定するには、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。

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は、DF ビットに **clear-df** 設定を使用します。この設定を使用すると、デバイスは、使用可能な MTU サイズよりも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** に設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フラグメンテーション ポリシーを表示します。 |

# 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*

## 構文の説明

| | |
|---|---|
| **after-encryption** | 暗号化の後で MTU の最大サイズに近い IPSec パケットをセキュリティ アプライアンスがフラグメント化するように指定します（事前フラグメント化をディセーブルにします）。 |
| **before-encryption** | 暗号化の前に MTU の最大サイズに近い IPSec パケットをセキュリティ アプライアンスがフラグメント化するように指定します（事前フラグメント化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。 |

## デフォルト

この機能は、デフォルトでイネーブルにされています。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 使用上のガイドライン

パケットは、暗号化するセキュリティ アプライアンスの発信リンクの MTU サイズに近い場合、IPSec ヘッダーを付けてカプセル化されると、発信リンクの MTU を超える可能性があります。超えた場合は、暗号化の後にパケットがフラグメント化され、復号化デバイスがプロセス パスで再構築することになります。IPSec VPN の事前フラグメント化では、デバイスはプロセス パスではなく高性能な CEF パスで動作するため、復号化時のデバイスのパフォーマンスが向上します。

IPSec VPN の事前フラグメント化により、暗号化デバイスは、IPSec SA の一部として設定されたトランスフォーム セットで使用可能な情報から、カプセル化されたパケット サイズを事前に設定します。デバイスでパケットが出力インターフェイスの MTU を超えることが事前に設定されている場合、デバイスは暗号化する前にそのパケットをフラグメント化します。これにより、復号化前にプロセス レベルでパケットを再構築する必要がなくなるため、復号化のパフォーマンスと IPsec トラフィックの全体的なスループットが向上します。

## 例

次に、グローバル コンフィギュレーション モードで、IPSec パケットの事前フラグメント化をデバイス上でグローバルにイネーブルにする例を示します。

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

```
hostname(config)#
```

次に、グローバル コンフィギュレーション モードで、IPSec パケットの事前フラグメント化をインターフェイス上でディセーブルにする例を示します。

```
hostname(config)# crypto ipsec fragmentation after-encryption inside
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。crypto 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*}

## 構文の説明

| | |
|---|---|
| *kilobytes* | 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。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。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の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 KB 数は 4,608,000 で、デフォルトの秒数は 28,800 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 | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | • | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 既存 | このコマンドは既存です。 |

## 使用上のガイドライン

**crypto ipsec security-association lifetime** コマンドは、IPSec セキュリティ アソシエーションのネゴシエート時に使用されるグローバル 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。

個々のクリプト マップ エントリでライフタイム値が設定されていない場合、セキュリティ アプライアンスは、ネゴシエート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、ピアへの要求の中でグローバル ライフタイム値を指定します。セキュリティ アプライアンスは、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。セキュリティ アプライアンスは、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済みの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。

ライフタイムには、「期間」ライフタイムと、「トラフィック量」ライフタイムの 2 種類があります。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。

セキュリティ アプライアンスでは、クリプト マップ、ダイナミック マップ、および ipsec 設定をオンザフライで変更できます。変更された場合、セキュリティ アプライアンスでは、変更によって影響を受ける接続のみが切断されます。クリプト マップに関連付けられている既存のアクセス リストをユーザが変更した場合（たとえばアクセス リスト内のエントリを削除した場合）、関連する接続のみが切断されます。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。

グローバルな指定時刻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。指定時刻ライフタイムを使用すると、指定した秒数が経過した後にセキュリティ アソシエーションがタイムアウトします。

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、指定した量のトラフィック（KB 単位）がセキュリティ アソシエーション キーによって保護された後に、セキュリティ アソシエーションがタイムアウトします。

ライフタイムを短くするほど、同一キーで暗号化されている解析対象データが少なくなるため、攻撃者はキー回復攻撃を開始することが難しくなります。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 アソシエーションの確立にかかる CPU 処理時間が長くなります。

セキュリティ アソシエーション（および対応するキー）は、指定した秒数または指定したトラフィック量（KB 単位）のうち、いずれかを最初に超えた時点で有効期限が切れます。

## 例

次に、セキュリティ アソシエーションのグローバル指定時刻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** | すべての IPSec コンフィギュレーション（たとえば、グローバル ライフタイムやトランスフォーム セット）をクリアします。 |
| **show running-config crypto map** | すべてのクリプト マップのすべてのコンフィギュレーションを表示します。 |

# crypto ipsec security-association replay

IPSec アンチリプレイ ウィンドウ サイズを設定するには、グローバル コンフィギュレーション モードで **crypto ipsec security-association replay** コマンドを使用します。ウィンドウ サイズ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 replay** {**window-size** *n* | **disable**}

**no crypto ipsec security-association replay** {**window-size** *n* | **disable**}

## 構文の説明

| | |
|---|---|
| *n* | ウィンドウ サイズを設定します。指定できる値は、64、128、256、512、または 1024 です。デフォルト値は 64 です。 |
| **disable** | アンチリプレイ チェックをディセーブルにします。 |

## デフォルト

デフォルトのウィンドウ サイズは 64 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 | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

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

## 使用上のガイドライン

Cisco IPsec 認証では、暗号化されたパケットそれぞれに対して固有のシーケンス番号を割り当てることによって、暗号化されたパケットを複製する攻撃者に対するアンチ リプレイ保護が提供されます（セキュリティ アソシエーションのアンチ リプレイは、受信者が過去のパケットや複製されたパケットを拒否することによりリプレイ アタックを防ぐセキュリティ サービスです）。復号化側では、検知したことのあるシーケンス番号は破棄されます。エンクリプタによって、シーケンス番号が昇順で割り当てられます。すでに検出されている最も高いシーケンス番号である値 X はデクリプタによって記録されます。また、デクリプタによって、X-N+1 ～ X（N はウィンドウ サイズ）までのシーケンス番号を持つパケットが検出されているかどうかも記録されます。シーケンス番号 X-N のパケットはすべて廃棄されます。現在、N は 64 に設定されているため、デクリプタによって追跡できるパケットは 64 までです。

ただし、64 パケット ウィンドウ サイズでは不十分な場合があります。たとえば、QoS はプライオリティが高いパケットを優先しますが、これにより、プライオリティが低いパケットが、デクリプタによって受信された最後の 64 パケットの 1 つであっても、廃棄される場合があります。このイベントにより、誤ったアラームである警告 syslog メッセージが生成される可能性があります。**crypto ipsec security-association replay** コマンドを使用すると、ウィンドウ サイズを拡張して、デクリプタが 64 を超えるパケットを追跡できます。

アンチリプレイ ウィンドウ サイズを増やしても、スループットおよびセキュリティに影響はありません。メモリへの影響は限定的です。デクリプタ上にシーケンス番号を保管するために必要となるのは、着信 IPsec SA ごとに追加の 128 バイトだけであるためです。今後アンチリプレイに関する問題が発生しないように、最大のウィンドウ サイズである 1024 を使用することを推奨します。

## 例

次に、セキュリティ アソシエーションのアンチリプレイ ウィンドウ サイズを指定する例を示します。

```
hostname(config)# crypto ipsec security-association replay window-size 1024
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure crypto map** | すべての IPSec コンフィギュレーション（たとえば、グローバル ライフタイムやトランスフォーム セット）をクリアします。 |
| **shape** | トラフィック シェーピングをイネーブルにします。 |
| **priority** | プライオリティ キューイングをイネーブルにします。 |
| **show running-config crypto map** | すべてのクリプト マップのすべてのコンフィギュレーションを表示します。 |

# crypto ipsec transform-set（トランスフォーム セットの作成または削除）

トランスフォーム セットを作成または削除するには、グローバル コンフィギュレーション モードで **crypto ipsec transform-set** コマンドを使用します。**crypto ipsec transform-set** コマンドを使用すると、トランスフォーム セットで使用される IPSec 暗号化およびハッシュ アルゴリズムを指定できます。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 transform-set** *transform-set-name encryption* **[***authentication***]**

**no crypto ipsec transform-set** *transform-set-name encryption* **[***authentication***]**

## 構文の説明

| | |
|---|---|
| *authentication* | （任意）IPSec のデータ フローの整合性を保証する認証方法を次の中から 1 つ指定します。<br>**esp-md5-hmac**：ハッシュ アルゴリズムとして MD5/HMAC-128 を使用する場合。<br>**esp-sha-hmac**：ハッシュ アルゴリズムとして SHA/HMAC-160 を使用する場合。<br>**esp-none**：HMAC 認証を使用しない場合。 |
| *encryption* | IPSec のデータ フローを保護する暗号化方法を次の中から 1 つ指定します。<br>**esp-aes**：128 ビット キーで AES を使用する場合。<br>**esp-aes-192**：192 ビット キーで AES を使用する場合。<br>**esp-aes-256**：256 ビット キーで AES を使用する場合。<br>**esp-des**：56 ビットの DES-CBC を使用する場合。<br>**esp-3des**：トリプル DES アルゴリズムを使用する場合。<br>**esp-null**：暗号化を使用しない場合。 |
| *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。すでにコンフィギュレーションに存在するトランスフォーム セットを表示するには、**show running-config ipsec** コマンドを入力します。 |

## デフォルト

デフォルトの認証設定は、esp-none（認証しない）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 | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | • | • | — | — |

**コマンド履歴**

| リリース | 変更内容 |
|---|---|
| 7.0 | このコマンドが導入されました。 |
| 7.2(1) | この項は書き換えられました。 |

**使用上のガイドライン**

トランスフォーム セットを設定したら、そのセットをクリプト マップに割り当てます。1 つのクリプト マップに対して最大 6 つのトランスフォーム セットを割り当てることができます。ピアが IPSec セッションを確立しようとすると、セキュリティ アプライアンスは、一致が検出されるまで、各クリプト マップのアクセス リストに照らしてピアを評価します。次に、セキュリティ アプライアンスは、一致が検出されるまで、ピアがネゴシエートするすべてのプロトコル、アルゴリズム、およびその他の設定を、クリプト マップに割り当てられているトランスフォーム セット内の設定に照らして評価します。セキュリティ アプライアンスでは、ピアの IPSec ネゴシエーションとトランスフォーム セット内の設定とが一致すると、IPSec セキュリティ アソシエーションの一部としてその設定を保護されたトラフィックに適用します。セキュリティ アプライアンスは、ピアがアクセス リストに一致しない場合や、クリプト マップに割り当てられているトランスフォーム セット内にピアのセキュリティ設定と完全に一致するセキュリティ設定が見つからない場合、IPSec セッションを終了します。

暗号化と認証のどちらを先に指定してもかまいません。認証を指定せずに暗号化を指定することもできます。作成するトランスフォーム セットに認証を指定する場合は、暗号化も指定する必要があります。変更するトランスフォーム セットに認証だけを指定した場合、トランスフォーム セットでは、現在の暗号化設定が維持されます。

AES 暗号化を指定する場合は、グローバル コンフィギュレーション モードでも **isakmp policy priority group 5** コマンドを使用して、AES で提供される大きなキー サイズに対応できるように Diffie-Hellman グループ 5 を割り当てることを推奨します。

**ヒント**　クリプト マップまたはダイナミック クリプト マップにトランスフォーム セットを適用し、そのマップに割り当てられているトランスフォーム セットを表示する場合は、トランスフォーム セットにコンフィギュレーションの内容を表す名前を付けておくと便利です。たとえば、次に示す最初の例の「3des-md5」は、トランスフォーム セットで使用する暗号化と認証を示しています。この名前の後に続く値は、トランスフォーム セットに割り当てる実際の暗号化と認証の設定です。

**例**

次のコマンドは、使用可能な暗号化と認証のすべてのオプション（暗号化と認証をまったく指定しないオプションは除く）を示しています。

```
hostname(config)# crypto ipsec transform-set 3des-md5 esp-3des esp-md5-hmac
hostname(config)# crypto ipsec transform-set 3des-sha esp-3des esp-sha-hmac
hostname(config)# crypto ipsec transform-set 56des-md5 esp-des esp-md5-hmac
hostname(config)# crypto ipsec transform-set 56des-sha esp-des esp-sha-hmac
hostname(config)# crypto ipsec transform-set 128aes-md5 esp-aes esp-md5-hmac
hostname(config)# crypto ipsec transform-set 128aes-sha esp-aes esp-sha-hmac
hostname(config)# crypto ipsec transform-set 192aes-md5 esp-aes-192 esp-md5-hmac
hostname(config)# crypto ipsec transform-set 192aes-sha esp-aes-192 esp-sha-hmac
hostname(config)# crypto ipsec transform-set 256aes-md5 esp-aes-256 esp-md5-hmac
hostname(config)# crypto ipsec transform-set 256aes-sha esp-aes-256 esp-sha-hmac
hostname(config)#
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **show running-config ipsec** | すべてのトランスフォーム セットのコンフィギュレーションを表示します。 |

| コマンド | 説明 |
|---|---|
| **crypto map set transform-set** | クリプトマップエントリで使用するトランスフォーム セットを指定します。 |
| **crypto dynamic-map set transform-set** | ダイナミック クリプト マップ エントリで使用するトランスフォーム セットを指定します。 |
| **show running-config crypto map** | クリプト マップの設定内容を表示します。 |
| **show running-config crypto dynamic-map** | ダイナミック クリプト マップのコンフィギュレーションを表示します。 |

# crypto isakmp am-disable

アグレッシブ モードの着信接続をディセーブルにするには、グローバル コンフィギュレーション モードで **crypto isakmp am-disable** コマンドを使用します。アグレッシブ モードの着信接続をイネーブルにするには、このコマンドの **no** 形式を使用します。

**crypto isakmp am-disable**

**no crypto isakmp am-disable**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルト値はイネーブルです。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | **isakmp am-disable** コマンドが追加されました。 |
| 7.2.(1) | **isakmp am-disable** コマンドが、**crypto isakmp am-disable** コマンドに置き換えられました。 |

## 例

次に、グローバル コンフィギュレーション モードでの入力で、アグレッシブ モードの着信接続をディセーブルにする例を示します。

```
hostname(config)# crypto isakmp am-disable
```

## 関連コマンド

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

# crypto isakmp disconnect-notify

ピアに対する切断通知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 isakmp disconnect-notify** コマンドを使用します。切断通知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 isakmp disconnect-notify**

**no crypto isakmp disconnect-notify**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルト値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 | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | **isakmp disconnect-notify** コマンドが追加されました。 |
| 7.2.(1) | **isakmp disconnect-notify** コマンドが、**crypto isakmp disconnect-notify** コマンドに置き換えられました。 |

## 例

次の例では、グローバル コンフィギュレーション モードで、ピアに対する切断通知をイネーブルにします。

```
hostname(config)# crypto isakmp disconnect-notify
```

## 関連コマンド

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

# crypto isakmp enable

IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上で ISAKMP ネゴシエーションをイネーブルにするには、グローバル コンフィギュレーション モードで **crypto isakmp enable** コマンドを使用します。インターフェイスで ISAKMP 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 isakmp enable** *interface-name*

**no crypto isakmp enable** *interface-name*

## 構文の説明

| | |
|---|---|
| *interface-name* | ISAKMP ネゴシエーションをイネーブルまたはディセーブルにするインターフェイスの名前を指定します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 既存 | **isakmp enable** コマンドは既存のものです。 |
| 7.2(1) | **isakmp enable** コマンドが、**crypto isakmp enable** コマンドに置き換えられました。 |

## 例

次の例では、グローバル コンフィギュレーション モードで、内部インターフェイス上で ISAKMP をディセーブルにする方法を示しています。

```
hostname(config)# no crypto isakmp enable inside
```

## 関連コマンド

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

# crypto isakmp identity

フェーズ 2 ID をピアに送信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 isakmp identity** 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。

**crypto isakmp identity {address | hostname | key-id** *key-id-string* | **auto}**

**no crypto isakmp identity {address | hostname | key-id** *key-id-string* | **auto}**

## 構文の説明

| | |
|---|---|
| **address** | ISAKMP の識別情報を交換するホストの IP アドレスを使用します。 |
| **auto** | ISAKMP ネゴシエーションを、接続のタイプ（事前共有キーの IP アドレス、または証明書認証用の証明書 DN）によって判別します。 |
| **hostname** | ISAKMP の識別情報を交換するホストの完全修飾ドメイン名を使用します（デフォルト）。この名前は、ホスト名とドメイン名で構成されます。 |
| **key-id** *key_id_string* | リモート ピアが事前共有キーを検索するために使用するストリングを指定します。 |

## デフォルト

デフォルトの ISAKMP ID は、**crypto isakmp identity auto** 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 | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 既存 | **isakmp identity** コマンドは既存のものです。 |
| 7.2(1) | **isakmp identity** コマンドが、**crypto isakmp identity** コマンドに置き換えられました。 |

## 例

次の例では、グローバル コンフィギュレーション モードで、接続タイプに応じて、IPSec ピアと通信するためのインターフェイス上で ISAKMP ネゴシエーションをイネーブルにします。

```
hostname(config)# crypto isakmp identity auto
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure crypto isakmp** | すべての ISAKMP コンフィギュレーションをクリアします。 |

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

# crypto isakmp ipsec-over-tcp

IPSec over TCP 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 isakmp ipsec-over-tcp** コマンドを使用します。IPSec over TCP 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 isakmp ipsec-over-tcp** [**port** *port1...port10*]

**no crypto isakmp ipsec-over-tcp** [**port** *port1...port10*]

## 構文の説明

| | |
|---|---|
| **port** *port1...port10* | （任意）デバイスが IPSec over TCP 接続を受け入れるポートを指定します。最大 10 のポートを指定できます。ポート番号には 1 ～ 65535 の範囲の数値を指定できます。デフォルトのポート番号は 10000 です。 |

## デフォルト

デフォルト値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 | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | **isakmp ipsec-over-tcp** コマンドが追加されました。 |
| 7.2.(1) | **isakmp ipsec-over-tcp** コマンドが、**crypto isakmp ipsec-over-tcp** コマンドに置き換えられました。 |

## 例

次の例では、グローバル コンフィギュレーション モードで、IPSec over TCP をポート 45 でイネーブルにします。

```
hostname(config)# crypto isakmp ipsec-over-tcp port 45
hostname(config)#
```

## 関連コマンド

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

# crypto isakmp nat-traversal

NAT トラバーサルをグローバルに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 ISAKMP がイネーブルになっていることを確認します（イネーブルにするには **crypto isakmp enable** コマンドを使用します）。NAT トラバーサル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 isakmp nat-traversal** *natkeepalive*

**no crypto isakmp nat-traversal** *natkeepalive*

## 構文の説明

| | |
|---|---|
| *natkeepalive* | NAT キープアライブ間隔を、10 ～ 3600 秒の範囲で設定します。デフォルトは 20 秒です。 |

## デフォルト

デフォルトでは、NAT トラバーサルはイネーブルになっています。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | **isakmp nat-traversal** コマンドは既存のものです。 |
| 7.2.(1) | **isakmp nat-traversal** コマンドが、**crypto isakmp nat-traversal** コマンドに置き換えられました。 |
| 8.0(2) | NAT トラバーサルが、デフォルトでイネーブルになりました。 |

## 使用上のガイドライン

NAT（PAT を含む）は、IPSec も使用されている多くのネットワークで使用されていますが、IPSec パケットが NAT デバイスを正常に通過することを妨げる非互換性が数多くあります。NAT トラバーサルを使用すると、ESP パケットが 1 つ以上の NAT デバイスを通過できるようになります。

セキュリティ アプライアンスは、IETF の「UDP Encapsulation of IPsec Packets」ドラフトのバージョン 2 とバージョン 3（http://www.ietf.org/html.charters/ipsec-charter.html から入手可能）に記述されているとおりに NAT トラバーサルをサポートしています。また、ダイナミック クリプト マップとスタティック クリプト マップの両方で NAT トラバーサルをサポートしています。

このコマンドは、セキュリティ アプライアンス上で NAT-T をグローバルにイネーブルにします。クリプト マップ エントリでディセーブルにするには、**crypto map set nat-t-disable** コマンドを使用します。

## 例

次に、グローバル コンフィギュレーション モードで、ISAKMP をイネーブルにし、NAT トラバーサルのキープアライブ間隔を 30 秒に設定する例を示します。

```
hostname(config)# crypto isakmp enable
hostname(config)# crypto isakmp nat-traversal 30
```

## 関連コマンド

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

# crypto isakmp policy authentication

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

**crypto isakmp policy** *priority* **authentication** {**crack** | **pre-share** | **rsa-sig**}

## 構文の説明

| | |
|---|---|
| **crack** | 認証方式として、IKE CRACK を指定します。 |
| **pre-share** | 認証方式として事前共有キーを指定します。 |
| *priority* | IKE ポリシーを一意に識別し、そのポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。 |
| **rsa-sig** | 認証方式として RSA シグニチャを指定します。<br>RSA シグニチャにより、IKE ネゴシエーションに対して否認防止を実行できます。これは基本的に、ユーザがピアとの IKE ネゴシエーションを行ったかどうかを、第三者に証明できることを意味します。 |

## デフォルト

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

## コマンド モード

次の表に、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 | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | **isakmp policy authentication** コマンドは既存のものです。 |
| 7.2.(1) | **isakmp policy authentication** コマンドが、**crypto isakmp policy authentication** コマンドに置き換えられました。 |

## 使用上のガイドライン

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

## 例

次に、グローバル コンフィギュレーション モードで、**crypto isakmp policy authentication** コマンドを使用する例を示します。この例では、プライオリティ番号 40 の IKE ポリシーで RSA シグニチャの認証方式を使用するように設定します。

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

## 関連コマンド

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

# crypto isakmp policy encryption

IKE ポリシーで使用する暗号化アルゴリズムを指定するには、グローバル コンフィギュレーション モードで **crypto isakmp policy encryption** コマンドを使用します。暗号化アルゴリズムをデフォルト値の **des** 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 isakmp policy** *priority* **encryption** {**aes | aes-192| aes-256 | des | 3des**}

**no crypto isakmp policy** *priority* **encryption** {**aes | aes-192| aes-256 | des | 3des**}

## 構文の説明

| | |
|---|---|
| **3des** | IKE ポリシーで、Triple DES 暗号化アルゴリズムを使用することを指定します。 |
| **aes** | IKE ポリシーで使用する暗号化アルゴリズムが、128 ビット キーを使用する AES であることを指定します。 |
| **aes-192** | IKE ポリシーで使用する暗号化アルゴリズムが、192 ビット キーを使用する AES であることを指定します。 |
| **aes-256** | IKE ポリシーで使用する暗号化アルゴリズムが、256 ビット キーを使用する AES であることを指定します。 |
| **des** | IKE ポリシーで使用する暗号化アルゴリズムが、56 ビット DES-CBC であることを指定します。 |
| *priority* | Internet Key Exchange（IKE; インターネット キー交換）ポリシーを一意に指定し、ポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。 |

## デフォルト

デフォルトの ISAKMP ポリシー暗号化は、**3des** 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 | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | **isakmp policy encryption** コマンドは既存のものです。 |
| 7.2.(1) | **isakmp policy encryption** コマンドが、**crypto isakmp policy encryption** コマンドに置き換えられました。 |

## 例

次に、グローバル コンフィギュレーション モードで、**crypto isakmp policy encryption** コマンドを使用する例を示します。この例では、プライオリティ番号 25 の IKE ポリシーに使用するアルゴリズムとして 128 ビット キーの AES 暗号化を設定します。

```
hostname(config)# crypto isakmp policy 25 encryption aes
```

次に、グローバル コンフィギュレーション モードでの入力で、プライオリティ番号 40 の IKE ポリシー内で 3DES アルゴリズムを使用するように設定する例を示します。

```
hostname(config)# crypto isakmp policy 40 encryption 3des
hostname(config)#
```

## 関連コマンド

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

# crypto isakmp policy group

IKE ポリシーの Diffie-Hellman グループを指定するには、グローバル コンフィギュレーション モードで **crypto isakmp policy group** コマンドを使用します。IKE ポリシーは、IKE ネゴシエーション時に使用するパラメータのセットを定義したものです。Diffie-Hellman グループ識別子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 isakmp policy** *priority* **group** {**1 | 2 | 5**}

**no crypto isakmp policy** *priority* **group**

## 構文の説明

| | |
|---|---|
| **group 1** | IKE ポリシーで、768 ビットの Diffie-Hellman グループを使用することを指定します。768 ビットは、デフォルト値です。 |
| **group 2** | IKE ポリシーで、1024 ビットの Diffie-Hellman グループ 2 を使用することを指定します。 |
| **group 5** | IKE ポリシーで、1536 ビットの Diffie-Hellman グループ 5 を使用することを指定します。 |
| *priority* | Internet Key Exchange（IKE; インターネット キー交換）ポリシーを一意に指定し、ポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。 |

## デフォルト

デフォルトのグループ ポリシーはグループ 2 です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | **isakmp policy group** コマンドが追加されました。 |
| 7.2(1) | **isakmp policy group** コマンドが、**crypto isakmp policy group** コマンドに置き換えられました。 |
| 8.0(4) | **group 7** コマンド オプションは**廃止されました**。グループ 7 を設定しようとするとエラー メッセージが生成され、代わりにグループ 5 が使用されます。 |

## 使用上のガイドライン

グループ オプションには、768 ビット（DH グループ 1）、1024 ビット（DH グループ 2）、および 1536 ビット（DH グループ 5）の 3 つがあります。1024 ビットと 1536 ビットの Diffie-Hellman グループは、セキュリティが高くなりますが、CPU の処理時間は長くなります。

（注）　Cisco VPN Client のバージョン 3.x 以上では、ISAKMP ポリシーで DH グループ 2 を使用する必要があります（DH グループ 1 に設定すると、Cisco VPN Client は接続できません）。

AES は、VPN-3DES のライセンスがあるセキュリティ アプライアンスに限りサポートされます。AES では大きなキー サイズが提供されるため、ISAKMP ネゴシエーションでは Diffie-Hellman（DH）グループ 1 やグループ 2 ではなく、グループ 5 を使用する必要があります。グループ 5 を設定するには、**crypto isakmp policy priority group 5** コマンドを使用します。

## 例

次に、グローバル コンフィギュレーション モードで、**crypto isakmp policy group** コマンドを使用する例を示します。この例では、プライオリティ番号 40 の IKE ポリシーに対し、グループ 2、1024 ビットの Diffie Hellman を使用するように設定しています。

```
hostname(config)# crypto isakmp policy 40 group 2
```

## 関連コマンド

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

# crypto isakmp policy hash

IKE ポリシーのハッシュ アルゴリズムを指定するには、グローバル コンフィギュレーション モードで **crypto isakmp policy hash** コマンドを使用します。IKE ポリシーは、IKE ネゴシエーション時に使用するパラメータのセットを定義したものです。ハッシュ アルゴリズムをデフォルト値の SHA-1 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 isakmp policy** *priority* **hash** {**md5** | **sha**}

**no crypto isakmp policy** *priority* **hash**

## 構文の説明

| | |
|---|---|
| **md5** | IKE ポリシーのハッシュ アルゴリズムとして MD5（HMAC バリアント）を指定します。 |
| *priority* | プライオリティをポリシーに一意に指定および割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。 |
| **sha** | IKE ポリシーのハッシュ アルゴリズムとして SHA-1（HMAC バリアント）を指定します。 |

## デフォルト

デフォルトのハッシュ アルゴリズムは SHA-1（HMAC バリアント）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 | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | **isakmp policy hash** コマンドは既存のものです。 |
| 7.2.(1) | **isakmp policy hash** コマンドが、**crypto isakmp policy hash** コマンドに置き換えられました。 |

## 使用上のガイドライン

ハッシュ アルゴリズムのオプションには、SHA-1 と MD5 の 2 つがあります。MD5 のダイジェストの方が小さく、SHA-1 よりもやや速いと見なされています。

## 例

次に、グローバル コンフィギュレーション モードで、**crypto isakmp policy hash** コマンドを使用する例を示します。この例では、プライオリティ番号 40 の IKE ポリシーに MD5 ハッシュ アルゴリズムを使用することを指定します。

```
hostname(config)# crypto isakmp policy 40 hash md5
```

**関連コマンド**

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

# crypto isakmp policy lifetime

IKE セキュリティ アソシエーションが期限切れになるまでのライフタイムを指定するには、グローバル コンフィギュレーション モードで **crypto isakmp policy lifetime** コマンドを使用します。ピアがライフタイムを提示していない場合は、無限のライフタイムを指定できます。セキュリティ アソシエーションのライフタイムをデフォルト値の 86,400 秒（1 日）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 isakmp policy** *priority* **lifetime** *seconds*

**no crypto isakmp policy** *priority* **lifetime**

## 構文の説明

| | |
|---|---|
| *priority* | Internet Key Exchange（IKE; インターネット キー交換）ポリシーを一意に指定し、ポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。 |
| *seconds* | 各セキュリティ アソシエーションが期限切れになるまでの秒数を指定します。有限のライフタイムを提示するには、120 ～ 2147483647 秒の整数を使用します。無限のライフタイムを提示するには、0 秒を使用します。 |

## デフォルト

デフォルト値は 86,400 秒（1 日）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 | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | **isakmp policy lifetime** コマンドは既存のものです。 |
| 7.2.(1) | **isakmp policy lifetime** コマンドが、**crypto isakmp policy lifetime** コマンドに置き換えられました。 |

## 使用上のガイドライン

IKE は、ネゴシエーションを開始するとき、自身のセッション用のセキュリティ パラメータについて合意しようとします。次に、各ピアのセキュリティ アソシエーションが、合意されたパラメータを参照します。ピアは、ライフタイムが期限切れになるまで、セキュリティ アソシエーションを保持します。セキュリティ アソシエーションは、期限切れになるまで、その後の IKE ネゴシエーションで利用できるため、新しい IPSec セキュリティ アソシエーションを設定するときに時間を節約できます。ピアは、現在のセキュリティ アソシエーションが期限切れになる前に、新しいセキュリティ アソシエーションをネゴシエートします。

ライフタイムを長くするほど、セキュリティ アプライアンスで以降の IPSec セキュリティ アソシエーションを設定する時間が節約されます。暗号化強度は十分なレベルにあるため、キーの再生成間隔を極端に短く（約 2 ～ 3 分ごとに）しなくてもセキュリティは保証されます。デフォルトをそのまま使用することを推奨します。

（注）　IKE セキュリティ アソシエーションのライフタイムが無限に設定されている場合、ピアが有限のライフタイムを提示したときは、ピアからネゴシエートされた有限のライフタイムが使用されます。

## 例

次に、グローバル コンフィギュレーション モードで、プライオリティ番号 40 の IKE ポリシーに IKE セキュリティ アソシエーションのライフタイムを 50,400 秒（14 時間）に設定する例を示します。

```
hostname(config)# crypto isakmp policy 40 lifetime 50400
```

次に、グローバル コンフィギュレーション モードでの入力で、IKE セキュリティ アソシエーションのライフタイムを無限に設定する例を示します。

```
hostname(config)# crypto isakmp policy 40 lifetime 0
```

## 関連コマンド

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

# crypto isakmp reload-wait

すべてのアクティブなセッションが自発的に終了しないとセキュリティ アプライアンスをリブートできないようにするは、グローバル コンフィギュレーション モードで **crypto isakmp reload-wait** コマンドを使用します。アクティブなセッションが終了するのを待たずにセキュリティ アプライアンスをリブートするには、このコマンドの **no** 形式を使用します。

**crypto isakmp reload-wait**

**no crypto isakmp reload-wait**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | **isakmp reload-wait** コマンドが追加されました。 |
| 7.2.(1) | **isakmp reload-wait** コマンドが、**crypto isakmp reload-wait** コマンドに置き換えられました。 |

## 例

次の例では、グローバル コンフィギュレーション モードで、すべてのアクティブなセッションが終了するまで待機してからセキュリティ アプライアンスをリブートするように設定します。

```
hostname(config)# crypto isakmp reload-wait
```

## 関連コマンド

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

# crypto key generate rsa

アイデンティティ証明書用の RSA キー 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**]

## 構文の説明

| | |
|---|---|
| general-keys | 1 つの汎用キー ペアを生成します。これはデフォルトのキー ペア タイプです。 |
| label *key-pair-label* | キー ペアに関連付ける名前を指定します。このキー ペアのラベルは一意である必要があります。同じラベルを使用して別のキー ペアを作成しようとすると、セキュリティ アプライアンスは警告メッセージを表示します。キーの生成時にラベルを指定しない場合、そのキー ペアにはスタティックに <Default-RSA-Key> という名前が付けられます。 |
| modulus *size* | キー ペアのモジュラス サイズ（512、768、1024、および 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 | すべての対話型プロンプトを非表示にします。 |
| **usage-keys** | シグニチャ用と暗号化用の 2 つのキー ペアを生成します。これは、対応する識別用に 2 つの証明書が必要なことを意味します。 |

## デフォルト

デフォルトのキー 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 | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | • | • | • | — |

## コマンド履歴

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

## 使用上のガイドライン

SSL、SSH、および IPSec 接続をサポートするために RSA キー ペアを生成するには、**crypto key generate rsa** コマンドを使用します。生成されたキー ペアは、コマンド構文の一部として指定できるラベルで識別されます。キー ペアを参照しないトラストポイントは、デフォルトの <Default-RSA-Key> を使用できます。SSH 接続では常にこのキーが使用されます。SSL は独自の証明書やキーをダイナミックに生成するため、証明書やキーがトラストポイントに設定されていない限り、このことは SSL に影響を与えません。

**注意**　1024 ビットを超える RSA キー ペアを持つ ID 証明書を使用している複数の SSL 接続によって、セキュリティ アプライアンスでの CPU 使用率が高くなり、クライアントレス ログインが拒否される可能性があります。

## 例

次に、グローバル コンフィギュレーション モードで、mypubkey というラベルの RSA キー 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 というラベルが重複する RSA キー ペアを誤って生成しようとする例を示します。

```
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 キー 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 キー ペアを削除します。 |
| **show crypto key mypubkey** | RSA キー ペアを表示します。 |

# crypto key zeroize

指定したタイプ（rsa または dsa）のキー 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**]

## 構文の説明

| | |
|---|---|
| **default** | ラベルがない RSA キー ペアを削除します。このキーワードは、RSA キー ペアに限り有効です。 |
| dsa | キー タイプとして DSA を指定します。 |
| label *key-pair-label* | 指定したタイプ（rsa または dsa）のキー ペアを削除します。ラベルを指定しない場合、セキュリティ アプライアンスは、指定したタイプのキー ペアをすべて削除します。 |
| noconfirm | すべての対話型プロンプトを非表示にします。 |
| rsa | キー タイプとして RSA を指定します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 既存 | このコマンドは既存です。 |

## 例

次に、グローバル コンフィギュレーション モードで、すべての RSA キー 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** | アイデンティティ証明書用の DSA キー ペアを生成します。 |
| **crypto key generate rsa** | アイデンティティ証明書用の RSA キー ペアを生成します。 |

# crypto map interface

以前に定義したクリプト 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。このクリプト マップ セットをインターフェイスから削除するには、このコマンドの **no** 形式を使用します。

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

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

## 構文の説明

| | |
|---|---|
| *interface-name* | セキュリティ アプライアンスが VPN ピアとのトンネルの確立に使用するインターフェイスを指定します。ISAKMP がイネーブルになっており、CA を使用して証明書を取得する場合は、CA 証明書で指定されているアドレスを持つインターフェイスにする必要があります。 |
| *map-name* | クリプト マップ セットの名前を指定します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 既存 | このコマンドは既存です。 |

## 使用上のガイドライン

このコマンドを使用して、クリプト マップ セットを任意のアクティブなセキュリティ アプライアンスのインターフェイスに割り当てます。セキュリティ アプライアンスでは、あらゆるアクティブ インターフェイスを IPSec の終端にすることができます。インターフェイスで IPSec サービスを提供するには、そのインターフェイスにまずクリプト マップ セットを割り当てる必要があります。

インターフェイスに割り当てることができるクリプト マップ セットは 1 つだけです。同じ *map-name* で *seq-num* が異なるクリプト マップ エントリが複数ある場合、それらのエントリは同じセットの一部であり、そのインターフェイスにすべて適用されます。セキュリティ アプライアンスは、*seq-num* が最も小さいクリプト マップ エントリを最初に評価します。

（注）　セキュリティ アプライアンスでは、クリプト マップ、ダイナミック マップ、および ipsec 設定を動作中に変更できます。設定を変更する場合、変更によって影響を受ける接続のみがセキュリティ アプライアンスによって停止させられます。特に、アクセス リスト内のエントリを削除することによって、クリプト マップに関連付けられている既存のアクセス リストを変更する場合は、関連する接続のみが停止させられます。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。

すべてのスタティック クリプト マップでは、アクセス リスト、トランスフォーム セット、および IPsec ピアという 3 つの部分を定義する必要があります。これらの 1 つが欠けている場合、そのクリプト マップは不完全であるため、セキュリティ アプライアンスは次のエントリに進みます。ただし、クリプト マップがアクセス リストでは一致するが、他の 2 つの要件のいずれかまたは両方で一致しない場合、セキュリティ アプライアンスはトラフィックをドロップします。

すべてのクリプト マップが完全であることを確認するには、**show running-config crypto map** コマンドを使用します。不完全なクリプト マップを修正するには、クリプト マップを削除し、欠けているエントリを追加してからクリプト マップを再適用します。

## 例

次に、グローバル コンフィギュレーション モードで、mymap という名前のクリプト マップ セットを外部インターフェイスに割り当てる例を示します。トラフィックは、この外部インターフェイスを通過するとき、セキュリティ アプライアンスによって mymap セット内のすべてのクリプト マップ エントリに照らして評価されます。発信トラフィックが、いずれかの mymap クリプト マップ エントリのアクセス リストと一致する場合、セキュリティ アプライアンスはそのクリプト マップ エントリのコンフィギュレーションを使用して、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、必要最小限のクリプト マップ エントリ 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** | すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。 |
| **show running-config crypto map** | クリプト マップの設定内容を表示します。 |

# crypto map ipsec-isakmp dynamic

所定のクリプト マップ エントリで既存のダイナミック クリプト マップを参照させるようにするには、グローバル コンフィギュレーション モードで **crypto map ipsec-isakmp dynamic** コマンドを使用します。相互参照を削除するには、このコマンドの **no** 形式を使用します。

ダイナミック クリプト 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 クリプト マップ セットを作成した後に、**crypto map ipsec-isakmp dynamic** コマンドを使用して、ダイナミック クリプト マップ セットをスタティック クリプト マップに追加します。

**crypto map** *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

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

## 構文の説明

| | |
|---|---|
| *dynamic-map-name* | 既存のダイナミック クリプト マップを参照するクリプト マップ エントリの名前を指定します。 |
| **ipsec-isakmp** | IKE がクリプト 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ことを指定します。 |
| *map-name* | クリプト マップ セットの名前を指定します。 |
| *seq-num* | クリプト 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

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 | このコマンドは、**ipsec-manual** キーワードを削除するように変更されました。 |

## 使用上のガイドライン

クリプト マップ エントリを定義してから、**crypto map interface** コマンドを使用して、ダイナミック クリプト 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 クリプト マップを使用することで、保護の対象となるトラフィックのフィルタリングと分類、そのトラフィックに適用するポリシーの定義という 2 つの機能を利用できます。最初の機能はインターフェイス上のトラフィック フローが対象となり、2 番めの機能はそのトラフィックのために（IKE を通じて）実行されるネゴシエーションが対象となります。

IPSec ダイナミック クリプト マップでは、次のことを指定します。

- 保護するトラフィック
- セキュリティ アソシエーションを確立する IPSec ピア

- 保護対象のトラフィックとともに使用するトランスフォーム セット
- キーおよびセキュリティ アソシエーションの使用方法または管理方法

クリプト マップ セットとは、それぞれ異なるシーケンス番号（seq-num）を持つが、マップ名が同じであるクリプト マップ エントリの集合です。したがって、所定のインターフェイスで、あるトラフィックには指定のセキュリティを適用してピアに転送し、その他のトラフィックには別の IPSec セキュリティを適用して同じまたは別のピアに転送できます。これを行うには、マップ名は同じであるが、シーケンス番号がそれぞれ異なる 2 つのクリプト マップ エントリを作成します。

seq-num 引数として割り当てる番号は、任意に決定しないでください。この番号によって、クリプト マップ セット内の複数のクリプト マップ エントリにランクが付けられます。小さいシーケンス番号のクリプト マップ エントリは、大きいシーケンス番号のマップ エントリよりも先に評価されます。つまり、番号の小さいマップ エントリの方がプライオリティが高くなります。

**（注）** クリプト マップをダイナミック クリプト マップにリンクする場合は、ダイナミック クリプト マップを指定する必要があります。指定すると、**crypto dynamic-map** コマンドを使用して以前に定義した既存のダイナミック クリプト マップにクリプト マップがリンクされます。クリプト マップ エントリが変換された後に加えた変更は、有効になりません。たとえば、set peer 設定への変更は有効になりません。ただし、セキュリティ アプライアンスは起動中に変更を保存します。ダイナミック クリプト マップをクリプト マップに変換して戻す場合、この変更は有効となり、**show running-config crypto map** コマンドの出力に表示されます。セキュリティ アプライアンスは、リブートされるまでこれらの設定を維持します。

## 例

次のコマンドでは、グローバル コンフィギュレーション モードで、test という名前のダイナミック クリプト マップを参照するようにクリプト マップ mymap を設定します。

```
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** | すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。 |
| **show running-config crypto map** | クリプト マップの設定内容を表示します。 |

# crypto map match address

アクセス リストをクリプト マップ エントリに割り当てるには、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。クリプト 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*

## 構文の説明

| | |
|---|---|
| *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、一致対象となる名前付き暗号化アクセス リストの名前引数と一致している必要があります。 |
| *map-name* | クリプト マップ セットの名前を指定します。 |
| *seq-num* | クリプト 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

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 既存 | このコマンドは既存です。 |

## 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 クリプト マップに対して必要です。**crypto dynamic-map** コマンドを使用してダイナミック クリプト マップを定義する場合、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。アクセス リストのヒット カウントは、トンネルが開始されたときにのみ増加します。トンネルがいったんアップ状態になると、ヒット カウントはパケット フローごとには増加しません。トンネルがドロップされてから再開されると、ヒット カウントは増加します。

セキュリティ アプライアンスは、アクセス リストを使用して、IPSec クリプトで保護するトラフィックと保護を必要としないトラフィックとを区別します。また、許可 ACE に一致する発信パケットを保護し、許可 ACE に一致する着信パケットが確実に保護されるようにします。

セキュリティ アプライアンスは、パケットが deny ステートメントと一致すると、クリプト マップ内の残りの ACE に対するパケットの評価を省略して、順番に次のクリプト マップ内の ACE に対するパケットの評価を再開します。*ACL のカスケード処理*には、ACL 内の残りの ACE の評価をバイパスする拒否 ACE の使用、およびクリプト マップ セット内の次のクリプト マップに割り当てられた ACL に対するトラフィックの評価の再開が含まれています。各クリプト マップを異なる IPSec 設定に関連付

けることができるため、拒否 ACE を使用して、対応するクリプト マップの詳細な評価から特別なトラフィックを除外し、その特別なトラフィックを別のクリプト マップの permit ステートメントに一致させることで別のセキュリティを提供または要求できます。

**（注）** クリプト アクセス リストでは、インターフェイスを通過するトラフィックを許可するかどうかは判別されません。このような判別は、**access-group** コマンドを使用してインターフェイスに直接適用されるアクセス リストによって行われます。

トランスペアレント モードでは、宛先アドレスはセキュリティ アプライアンスの IP アドレス、管理アドレスである必要があります。トランスペアレント モードでは、セキュリティ アプライアンスへのトンネルだけが許可されます。

## 関連コマンド

| コマンド | 説明 |
|---|---|
| clear configure crypto map | すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。 |
| show running-config crypto map | クリプト マップの設定内容を表示します。 |

# crypto map set connection-type

クリプト マップ エントリのバックアップ Site-to-Site 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}**

## 構文の説明

| | |
|---|---|
| **answer-only** | ピアが、適切な接続先ピアを決定するための最初の独自の交換中に、まず着信 IKE 接続だけに応答することを指定します。 |
| **bidirectional** | ピアが、クリプト マップ エントリに基づいて接続を受け入れ、発信できることを指定します。これは、すべての Site-to-Site 接続のデフォルトの接続タイプです。 |
| **map-***name* | クリプト マップ セットの名前を指定します。 |
| **originate-only** | ピアが、適切な接続先ピアを決定するために最初の独自の交換を開始することを指定します。 |
| *seq-num* | クリプト マップ エントリに割り当てる番号を指定します。 |
| **set connection-type** | クリプト マップ エントリのバックアップ Site-to-Site 機能の接続タイプを指定します。answer-only、originate-only、および bidirectional の 3 つのタイプの接続があります。 |

## 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 | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

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

## 使用上のガイドライン

**crypto map set connection-type** コマンドは、バックアップ Lan-to-Lan 機能の接続タイプを指定します。接続の一方の側で複数のバックアップ ピアを指定できます。

この機能は、次のプラットフォーム間でのみ使用できます。

- 2 つの Cisco ASA 5500 シリーズ セキュリティ アプライアンス
- Cisco ASA 5500 シリーズ セキュリティ アプライアンスと Cisco VPN 3000 コンセントレータ

- Cisco ASA 5500 シリーズ セキュリティ アプライアンスと、Cisco PIX セキュリティ アプライアンス ソフトウェア v7.0 以上を実行しているセキュリティ アプライアンス

バックアップ Lan-to-Lan 接続を設定するには、接続の一方の側を **originate-only** キーワードを使用して originate-only として設定し、複数のバックアップ ピアがある側を **answer-only** キーワードを使用して answer-only として設定することを推奨します。originate-only 側では、**crypto map set peer** コマンドを使用してピアのプライオリティを指定します。originate-only セキュリティ アプライアンスは、リストの最初のピアとネゴシエートしようとします。ピアが応答しない場合、セキュリティ アプライアンスはピアが応答するか、またはリストにピアがなくなるまで下に向かってリストを検索します。

このように設定した場合、originate-only ピアは、最初に独自のトンネルを確立してピアとネゴシエートしようとします。その後は、いずれかのピアが通常の Lan-to-Lan 接続を確立することができ、いずれかの側からのデータがトンネル接続を開始できます。

トランスペアレント ファイアウォール モードでは、このコマンドは表示されますが、インターフェイスに対応付けられたクリプト マップに含まれるクリプト マップ エントリでは、connection-type 値は answer-only 以外の値に設定できません。

表 9-1 に、サポートされているすべてのコンフィギュレーションを示します。他の組み合わせは、予測不可能なルーティング問題を引き起こす場合があります。

**表 9-1　サポートされているバックアップ LAN-to-LAN 接続タイプ**

| リモート側 | 中央側 |
|---|---|
| Originate-Only | Answer-Only |
| Bi-Directional | Answer-Only |
| Bi-Directional | Bi-Directional |

## 例

次に、グローバル コンフィギュレーション モードで、クリプト マップ mymap を設定し、接続タイプを originate-only に設定する例を示します。

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

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure crypto map** | すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。 |
| **show running-config crypto map** | クリプト マップの設定内容を表示します。 |

# crypto map set inheritance

クリプト マップ エントリ用に生成されるセキュリティ アソシエーションの精度（シングルまたはマルチ）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 **set inheritance** コマンドを使用します。クリプト マップ エントリの継承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。

**crypto map** *map-name seq-num* **set inheritance {data| rule}**

**no crypto map** *map-name seq-num* **set inheritance {data | rule}**

## 構文の説明

| | |
|---|---|
| **data** | ルールで指定されているアドレス範囲内のアドレス ペアごとに 1 つのトンネルを指定します。 |
| *map-name* | クリプト マップ セットの名前を指定します。 |
| **rule** | クリプト マップに関連付けられている各 ACL エントリに 1 つのトンネルを指定します。これがデフォルトです。 |
| *seq-num* | クリプト マップ エントリに割り当てる番号を指定します。 |
| **set inheritance** | 継承のタイプを **data** または **rule** に指定します。継承では、各 Security Policy Database（SPD; セキュリティ ポリシー データベース）ルールに対して 1 つの Security Association（SA; セキュリティ アソシエーション）を生成したり、範囲内の各アドレス ペアに対して複数のセキュリティ SA を生成したりすることができます。 |

## デフォルト

デフォルト値は、**rule** です。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

## コマンド履歴

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

## 使用上のガイドライン

このコマンドは、セキュリティ アプライアンスがトンネルに応答しているときではなく、トンネルを開始しているときにのみ機能します。データ設定を使用すると、多数の IPSec SA が作成される可能性があります。この場合、メモリが消費され、全体としてのトンネルが少なくなります。データ設定は、セキュリティへの依存が非常に高いアプリケーションに対してのみ使用してください。

## 例

次に、グローバル コンフィギュレーション モードで、クリプト マップ mymap を設定し、継承タイプを data に設定する例を示します。

```
hostname(config)# crypto map mymap 10 set inheritance data
```

```
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure crypto map** | すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。 |
| **show running-config crypto map** | クリプト マップの設定内容を表示します。 |

# crypto map set nat-t-disable

接続の NAT-T をクリプト マップ エントリに基づいてディセーブルにするには、グローバル コンフィギュレーション モードで **crypto map set nat-t-disable** コマンドを使用します。このクリプト マップ エントリの NAT-T をイネーブルにするには、このコマンドの **no** 形式を使用します。

**crypto map** *map-name seq-num* **set nat-t-disable**

**no crypto map** *map-name seq-num* **set nat-t-disable**

## 構文の説明

| | |
|---|---|
| *map-name* | クリプト マップ セットの名前を指定します。 |
| *seq-num* | クリプト 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

このコマンドのデフォルト設定はオンではありません（したがって、NAT-T はデフォルトでイネーブルです）。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 使用上のガイドライン

NAT-T をグローバルにイネーブルにするには、**isakmp nat-traversal** コマンドを使用します。その後、**crypto map set nat-t-disable** コマンドを使用して、特定のクリプト マップ エントリの NAT-T をディセーブルにできます。

## 例

次のコマンドでは、グローバル コンフィギュレーション モードで、mymap という名前のクリプト マップ エントリの NAT-T をディセーブルにします。

```
hostname(config)# crypto map mymap 10 set nat-t-disable
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure crypto map** | すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。 |
| **isakmp nat-traversal** | すべての接続の NAT-T をイネーブルにします。 |
| **show running-config crypto map** | クリプト マップの設定内容を表示します。 |

# crypto map set peer

クリプト 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。クリプト 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*}

## 構文の説明

| | |
|---|---|
| *hostname* | ピアを、セキュリティ アプライアンスの **name** コマンドで定義した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* | クリプト マップ セットの名前を指定します。 |
| **peer** | クリプト マップ エントリの IPSec ピアをホスト名または IP アドレスで指定します。 |
| *seq-num* | クリプト 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

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 | このコマンドは、最大 10 個のピア アドレスを許容するように変更されました。 |

## 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 クリプト マップに対して必要です。**crypto dynamic-map** コマンドを使用してダイナミック クリプト マップ エントリを定義する場合、このコマンドは必須ではなく、ほとんど使用しません。これは、ピアが通常は未知のものであるためです。

複数のピアを設定することは、フォールバック リストを指定することと同じです。トンネルごとに、セキュリティ アプライアンスはリスト内の最初のピアとネゴシエートしようとします。ピアが応答しない場合、セキュリティ アプライアンスはピアが応答するか、またはリストにピアがなくなるまで下に向かってリストを検索します。バックアップ LAN-to-LAN 機能を使用している場合（つまり、クリプト マップ接続タイプが originate-only の場合）にのみ複数のピアを設定できます。詳細については、**crypto map set connection-type** 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、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クリプト マップ コンフィギュレーションの例を示します。この例では、ピア 10.0.0.1 またはピア 10.0.0.2 に対するセキュリティ アソシエーションを設定できます。

```
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** | すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。 |
| **show running-config crypto map** | クリプト マップの設定内容を表示します。 |

# crypto map set pfs

クリプト マップ エントリ用の新しいセキュリティ アソシエーションの要求時に PFS を要求するように IPSec を設定するか、または新しいセキュリティ アソシエーションの要求の受信時に PFS を要求するように IPSec 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 map set pfs** コマンドを使用します。IPSec が PFS を要求しないことを指定するには、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]**

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

## 構文の説明

| | |
|---|---|
| **group1** | IPSec で新しい Diffie-Hellman 交換を実行するときに、768 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。 |
| **group2** | IPSec で新しい Diffie-Hellman 交換を実行するときに、1024 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。 |
| **group5** | IPSec で新しい Diffie-Hellman 交換を実行するときに、1536 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。 |
| *map-name* | クリプト マップ セットの名前を指定します。 |
| *seq-num* | クリプト 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 は設定されません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 | このコマンドは変更され Diffie-Hellman グループ 7 が追加されました。 |
| 8.0(4) | **group 7** コマンド オプションは**廃止されました**。グループ 7 を設定しようとするとエラー メッセージが生成され、代わりにグループ 5 が使用されます。 |

## 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たびに新しい Diffie-Hellman 交換が発生します。この交換によって、処理時間が長くなります。PFS を使用すると、セキュリティがさらに向上します。1 つのキーが攻撃者によってクラックされた場合でも、侵害されるのはそのキーで送信されたデータだけになるためです。

このコマンドを使用すると、クリプト マップ エントリ用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、ネゴシエート中に IPSec が PFS を要求します。**set pfs** ステートメントでグループが指定されていない場合、セキュリティ アプライアンスはデフォルト（グループ 2）を送信します。

ピアがネゴシエーションを開始するときに、ローカル コンフィギュレーションで 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、ネゴシエーションは失敗します。ローカル コンフィギュレーションでグループが指定されていない場合、セキュリティ アプライアンスはデフォルトの group2 が指定されているものと見なします。ローカル コンフィギュレーションでグループ 2 またはグループ 5 が指定されている場合は、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、ネゴシエーションは失敗します。

ネゴシエーションが成功するには、両端に PFS が設定されている必要があります。設定されている場合、グループは完全に一致する必要があります。セキュリティ アプライアンスは、ピアからの PFS のいずれのオファーも受け入れません。

1536 ビットの Diffie-Hellman プライム モジュラス グループであるグループ 5 は、グループ 1 やグループ 2 よりも高いセキュリティを提供します。ただし、他のグループより処理時間が長くなります。

セキュリティ アプライアンスは、Cisco VPN Client と対話するときに PFS 値を使用しません。その代わり、フェーズ 1 で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、クリプト マップ「mymap 10」用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 を使用することを指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** | すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。 |
| **show running-config crypto map** | クリプト マップの設定内容を表示します。 |
| **tunnel-group** | トンネル グループとそのパラメータを設定します。 |

# crypto map set phase1-mode

メインまたはアグレッシブへの接続を開始する場合にフェーズ 1 の IKE モードを指定するには、グローバル コンフィギュレーション モードで **crypto map set phase1 mode** 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。アグレッシブ モードの Diffie-Hellman グループを含めるかどうかは任意です。含めない場合、セキュリティ アプライアンスはグループ 2 を使用します。

**crypto map** *map-name seq-num* **set phase1-mode {main | aggressive [group1 | group2 | group5]}**

**no crypto map** *map-name seq-num* **set phase1-mode {main | aggressive [group1 | group2 | group5]}**

## 構文の説明

| | |
|---|---|
| aggressive | フェーズ 1 IKE ネゴシエーションにアグレッシブ モードを指定します。 |
| **group1** | IPSec で新しい Diffie-Hellman 交換を実行するときに、768 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。 |
| **group2** | IPSec で新しい Diffie-Hellman 交換を実行するときに、1024 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。 |
| **group5** | IPSec で新しい Diffie-Hellman 交換を実行するときに、1536 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。 |
| **main** | フェーズ 1 IKE ネゴシエーションにメイン モードを指定します。 |
| *map-name* | クリプト マップ セットの名前を指定します。 |
| *seq-num* | クリプト 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

フェーズ 1 のデフォルト 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 | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 | このコマンドが導入されました。 |
| 8.0(4) | **group 7** コマンド オプションは**廃止されました**。グループ 7 を設定しようとするとエラー メッセージが生成され、代わりにグループ 5 が使用されます。 |

## 使用上のガイドライン

このコマンドは、発信側モードでのみ機能します。応答側モードでは機能しません。

## 例

次に、グローバル コンフィギュレーション モードで、クリプト マップ mymap を設定し、グループ 2 を使用してフェーズ 1 のモードをアグレッシブに設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** | すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。 |
| **show running-config crypto map** | クリプト マップの設定内容を表示します。 |

# crypto map set reverse-route

クリプト マップ エントリに基づいて任意の接続の 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。クリプト マップ エントリに基づいた任意の接続の逆ルート注入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 s***et reverse-route**

## 構文の説明

| | |
|---|---|
| *map-name* | クリプト マップ セットの名前を指定します。 |
| *seq-num* | クリプト 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

このコマンドのデフォルト設定はオフです。

## 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 | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | • | • | — | — |

## コマンド履歴

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

## 使用上のガイドライン

セキュリティ アプライアンスは、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 を使用してそれらのルートをプライベート ネットワークまたはボーダー 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 という名前のクリプト マップの RRI をイネーブルにする例を示します。

```
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** | すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。 |
| **show running-config crypto map** | クリプト マップの設定内容を表示します。 |

# crypto map set security-association lifetime

特定のクリプト 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されるグローバル 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。クリプト 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*}

## 構文の説明

| | |
|---|---|
| *kilobytes* | 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。<br>デフォルトは 4,608,000 KB です。 |
| *map-name* | クリプト 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期限が切れるまでの存続時間（秒数）を指定します。デフォルトは 28,800 秒（8 時間）です。 |
| *seq-num* | クリプト 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 KB 数は 4,608,000 で、デフォルトの秒数は 28,800 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 | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | • | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 既存 | このコマンドは既存です。 |

## 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、セキュリティ アプライアンスは、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。セキュリティ アプライアンスは、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

ライフタイムには、「期間」ライフタイムと、「トラフィック量」ライフタイムの 2 種類があります。セッション キーとセキュリティ アソシエーションは、いずれかのライフタイムに最初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を指定できます。

**（注）** セキュリティ アプライアンスでは、クリプト マップ、ダイナミック マップ、および ipsec 設定を動作中に変更できます。設定を変更する場合、変更によって影響を受ける接続のみがセキュリティ アプライアンスによって停止させられます。特に、アクセス リスト内のエントリを削除することによって、クリプト マップに関連付けられている既存のアクセス リストを変更する場合は、関連する接続のみが停止させられます。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。

指定時刻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。指定時刻ライフタイムを使用すると、指定した秒数が経過した後にキーおよびセキュリティ アソシエーションがタイムアウトします。

## 例

次のコマンドでは、グローバル コンフィギュレーション モードで、クリプト マップ mymap のセキュリティ アソシエーション ライフタイムを秒単位および KB 単位で指定します。

```
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** | すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。 |
| **show running-config crypto map** | クリプト マップの設定内容を表示します。 |

# crypto map set transform-set

クリプト マップ エントリで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。

**crypto map** *map-name seq-num* **set transform-set** *transform-set-name1*
[*… transform-set-name11*]

クリプト マップ エントリから特定のトランスフォーム セット名を削除するには、トランスフォーム セットの名前を指定してこのコマンドの **no** 形式を使用します。

**no crypto map** *map-name seq-num* **set transform-set** *transform-set-name1*
[*… transform-set-name11*]

トランスフォーム セットをすべて指定するか何も指定せずに、クリプト マップ 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。

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

## 構文の説明

| | |
|---|---|
| *map-name* | クリプト マップ セットの名前を指定します。 |
| *seq-num* | クリプト マップ エントリに対応するシーケンス番号を指定します。 |
| *transform-set-name1*<br>*transform-set-name11* | トランスフォーム セットの名前を 1 つ以上指定します。このコマンドで指定するトランスフォーム セットは、**crypto ipsec transform-set** コマンドで定義されている必要があります。各クリプト マップ エントリは、11 個までのトランスフォーム セットをサポートしています。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 | このコマンドが導入されました。 |
| 7.2(1) | クリプト マップ エントリにおけるトランスフォーム セットの最大数が変更されました。 |

## 使用上のガイドライン

このコマンドは、すべてのクリプト マップ エントリで必要です。

IPSec の開始側とは反対側にあるピアは、最初に一致したトランスフォーム セットをセキュリティ アソシエーションに使用します。ローカルのセキュリティ アプライアンスがネゴシエーションを開始した場合、セキュリティ アプライアンスは、**crypto map** コマンドで指定した順番どおりに、トランス

フォーム セットの内容をピアに提示します。ピアがネゴシエーションを開始すると、ローカルのセキュリティ アプライアンスは、クリプト マップ エントリ内の、ピアから送信された IPSec パラメータと一致する最初のトランスフォーム セットを使用します。

IPSec の開始側とは反対側にあるピアが、一致するトランスフォーム セットの値を見つけられない場合、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ないため、開始側はトラフィックをドロップします。

トランスフォーム セットのリストを変更するには、新しいリストを再度指定して、古いリストと置き換えます。

次のコマンドを使用してクリプト マップを変更すると、セキュリティ アプライアンスは、指定したシーケンス番号と同じ番号のクリプト マップ エントリだけを変更します。たとえば、次のコマンドを入力すると、セキュリティ アプライアンスは、「56des-sha」というトランスフォーム セットをリストの最後に挿入します。

```
hostname(config)# crypto map map1 1 set transform-set 128aes-md5 128aes-sha 192aes-md5
hostname(config)# crypto map map1 1 transform-set 56des-sha
hostname(config)#
```

次のコマンドの応答は、前の 2 つのコマンドで行った変更を合わせたものになります。

```
hostname(config)# show running-config crypto map
crypto map map1 1 set transform-set 128aes-md5 128aes-sha 192aes-md5 56des-sha
hostname(config)#
```

クリプト マップ エントリ内のトランスフォーム セットの順番を再設定するには、エントリを削除し、マップ名とシーケンス番号の両方を指定してから、エントリを再作成します。たとえば、次のコマンドでは、シーケンス番号 3 の map2 というクリプト マップ エントリを再設定します。

```
asa2(config)# no crypto map map2 3 set transform-set
asa2(config)# crypto map map2 3 set transform-set 192aes-sha 192aes-md5 128aes-sha
128aes-md5
asa2(config)#
```

## 例

「crypto ipsec transform-set（トランスフォーム セットの作成または削除）」の項には、10 個のトランスフォーム セット サンプル コマンドが示されています。次に、10 個の同じトランスフォーム セットから成る「map2」というクリプト マップ エントリを作成する例を示します。

```
hostname(config)# crypto map map2 10 set transform-set 3des-md5 3des-sha 56des-md5
56des-sha 128aes-md5 128aes-sha 192aes-md5 192aes-sha 256aes-md5 256aes-sha
hostname(config)#
```

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 アプライアンスが 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場合に最小限必要となるクリプト 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 map2 10 ipsec-isakmp
hostname(config)# crypto map map2 10 match address 101
hostname(config)# crypto map map2 set transform-set 3des-md5
hostname(config)# crypto map map2 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 クリプト マップをコンフィギュレーションからクリアします。 |
| **clear configure crypto map** | コンフィギュレーションから、すべてのクリプト マップをクリアします。 |

| コマンド | 説明 |
|---|---|
| **crypto dynamic-map set transform-set** | ダイナミック クリプト マップ エントリで使用するトランスフォーム セットを指定します。 |
| **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 dynamic-map** | ダイナミック クリプト マップのコンフィギュレーションを表示します。 |
| **show running-config crypto map** | クリプト マップの設定内容を表示します。 |

# crypto map set trustpoint

クリプト マップ エントリのフェーズ 1 ネゴシエーション中に、認証用に送信する証明書を指定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。クリプト 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]**

**no crypto map** *map-name seq-num* **set trustpoint** *trustpoint-name* **[chain]**

## 構文の説明

| | |
|---|---|
| **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、ルート証明書からアイデンティティ証明書まで、証明書の階層内のすべての CA 証明書が含まれています。デフォルト値はディセーブル（チェーンなし）です。 |
| *map-name* | クリプト マップ セットの名前を指定します。 |
| *seq-num* | クリプト 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 ネゴシエーション中に送信する証明書を指定します。デフォルトは none です。 |
| token | ユーザ認証にトークンベースのサーバを使用することを指定します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

## コマンド履歴

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

## 使用上のガイドライン

このクリプト マップ 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、クリプト マップ mymap に tpoint1 という名前のトラストポイントを指定し、証明書の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** | すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。 |
| **show running-config crypto map** | クリプト マップの設定内容を表示します。 |
| **tunnel-group** | トンネル グループを設定します。 |

# csc

セキュリティ アプライアンスがネットワーク トラフィックを CSC SSM に送信できるようにするには、クラス コンフィギュレーション モードで **csc** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。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。

**csc** {**fail-open** | **fail-close**}

**no csc**

## 構文の説明

| | |
|---|---|
| **fail-close** | CSC SSM が失敗した場合、セキュリティ アプライアンスがトラフィックをブロックする必要があることを指定します。これは、クラス マップで選択されたトラフィックにのみ適用されます。CSC SSM に送信されていない他のトラフィックは、CSC SSM 障害による影響を受けません。 |
| **fail-open** | CSC SSM が失敗した場合、セキュリティ アプライアンスがトラフィックを許可する必要があることを指定します。これは、クラス マップで選択されたトラフィックにのみ適用されます。CSC SSM に送信されていない他のトラフィックは、CSC SSM 障害による影響を受けません。 |

## デフォルト

このコマンドは、デフォルトでディセーブルになっています。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 使用上のガイドライン

**csc** コマンドは、該当するクラス マップに一致したすべてのトラフィックを CSC SSM に送信するようにセキュリティ ポリシーを設定します。この設定の後、セキュリティ アプライアンスは、トラフィックが宛先に引き続き送信されるのを許可します。

CSC SSM がトラフィックをスキャンできない場合は、一致しているトラフィックをセキュリティ アプライアンスが処理する方法を指定できます。**fail-open** キーワードは、CSC SSM を使用できない場合でも、トラフィックが宛先に引き続き送信されるのをセキュリティ アプライアンスが許可するように指定します。**fail-close** キーワードは、CSC SSM が使用できない場合、一致しているトラフィックが宛先に引き続き送信されるのをセキュリティ アプライアンスが許可しないように指定します。

CSC SSM は、HTTP、SMTP、POP3、および FTP トラフィックをスキャンできます。接続を要求しているパケットの宛先ポートが、これらのプロトコルにとって既知のポートである場合にのみ、これらのプロトコルがサポートされます。つまり、CSC SSM は、次の接続のみをスキャンできます。

- TCP ポート 21 に対してオープンされている FTP 接続。
- TCP ポート 80 に対してオープンされている HTTP 接続。
- TCP ポート 110 に対してオープンされている POP3 接続。
- TCP ポート 25 に対してオープンされている SMTP 接続。

**csc** コマンドを使用しているポリシーで、これらのポートを他のプロトコルに誤用する接続が選択された場合、セキュリティ アプライアンスはパケットを CSC SSM に渡しますが、CSC SSM はパケットをスキャンせずに渡します。

CSC SSM の効率を最大限にするには、次のように、**csc** コマンドを実装しているポリシーが使用するクラス マップを設定します。

- サポートされているプロトコルのうち、CSC SSM がスキャンするプロトコルだけを選択します。たとえば、HTTP トラフィックをスキャンしない場合は、サービス ポリシーが HTTP トラフィックを CSC SSM に転送しないようにしてください。
- セキュリティ アプライアンスによって保護されている信頼できるホストを危険にさらす接続だけを選択します。これらは、外部ネットワークまたは信頼できないネットワークから内部ネットワークへの接続です。次の接続をスキャンすることを推奨します。
  - 発信 HTTP 接続。
  - セキュリティ アプライアンスの内部のクライアントからセキュリティ アプライアンスの外部のサーバへの FTP 接続。
  - セキュリティ アプライアンスの内部のクライアントからセキュリティ アプライアンスの外部のサーバへの POP3 接続。
  - 内部メール サーバ宛ての着信 SMTP 接続。

### FTP スキャン

CSC SSM は、FTP セッションのプライマリ チャネルが標準ポート（TCP ポート 21）を使用している場合にのみ、FTP ファイル転送のスキャンをサポートします。

FTP インスペクションは、CSC SSM がスキャンする FTP トラフィックに対してイネーブルである必要があります。これは、FTP が、データ転送用にダイナミックに割り当てられたセカンダリ チャネルを使用するためです。セキュリティ アプライアンスは、セカンダリ チャネルに割り当てられるポートを決定し、データ転送の実行を許可するピンホールを開きます。FTP データをスキャンするように CSC SSM が設定されている場合、セキュリティ アプライアンスはデータ トラフィックを CSC SSM に転送します。

FTP インスペクションは、グローバルに、または **csc** コマンドが適用される同じインターフェイスに適用できます。デフォルトでは、FTP インスペクションはグローバルにイネーブルになっています。デフォルトのインスペクション コンフィギュレーションを変更していない場合、CSC SSM による FTP スキャンをイネーブルにするために必要なその他の FTP インスペクション コンフィギュレーションはありません。

FTP インスペクションまたはデフォルトのインスペクション コンフィギュレーションの詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

## 例

内部ネットワーク上のクライアントから HTTP、FTP、および POP3 接続で外部のネットワークに要求されたトラフィック、および外部のホストから DMZ ネットワーク上のメール サーバに着信する SMTP 接続を CSC SSM に転送するように、セキュリティ アプライアンスを設定する必要があります。内部ネットワークから DMZ ネットワーク上の Web サーバへの HTTP 要求は、スキャンされません。

次のコンフィギュレーションでは、2 つのサービス ポリシーを作成します。最初のポリシー csc_out_policy は、内部インターフェイスに適用され、csc_out アクセス リストを使用して、FTP および POP3 に対するすべての発信要求が確実にスキャンされるようにします。csc_out アクセス リストにより、内部から外部インターフェイス上のネットワークへの HTTP 接続が確実にスキャンされるようにもなりますが、このアクセス リストには、内部から DMZ ネットワーク上のサーバへの HTTP 接続を除外する拒否 ACE が含まれています。

2 番めのポリシー csc_in_policy は、外部インターフェイスに適用されます。このポリシーは csc_in アクセス リストを使用して、外部インターフェイスで発信され、DMZ ネットワークを宛先とする SMTP 要求と HTTP 要求が CSC SSM で確実にスキャンされるようにします。HTTP 要求をスキャンすることで、Web サーバは HTTP ファイルのアップロードから保護されます。

```
hostname(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 21
hostname(config)# access-list csc_out deny tcp 192.168.10.0 255.255.255.0 192.168.20.0 255.255.255.0 eq 80
hostname(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 80
hostname(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 110

hostname(config)# class-map csc_outbound_class
hostname(config-cmap)# match access-list csc_out

hostname(config)# policy-map csc_out_policy
hostname(config-pmap)# class csc_outbound_class
hostname(config-pmap-c)# csc fail-close

hostname(config)# service-policy csc_out_policy interface inside

hostname(config)# access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 25
hostname(config)# access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 80

hostname(config)# class-map csc_inbound_class
hostname(config-cmap)# match access-list csc_in

hostname(config)# policy-map csc_in_policy
hostname(config-pmap)# class csc_inbound_class
hostname(config-pmap-c)# csc fail-close

hostname(config)# service-policy csc_in_policy interface outside
```

**（注）** FTP により転送されたファイルを CSC SSM がスキャンするには、FTP インスペクションがイネーブルである必要があります。FTP インスペクションは、デフォルトでイネーブルになっています。

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **class（ポリシー マップ）** | トラフィック分類のクラス マップを指定します。 |
| **class-map** | ポリシー マップで使用するトラフィック分類マップを作成します。 |
| **match port** | 宛先ポートを使用してトラフィックを照合します。 |
| **policy-map** | トラフィック クラスを 1 つ以上のアクションと関連付けることによって、ポリシー マップを作成します。 |
| **service-policy** | ポリシー マップを 1 つ以上のインターフェイスと関連付けることによって、セキュリティ ポリシーを作成します。 |

# csd enable

管理およびリモート ユーザ アクセス用に Cisco Secure Desktop をイネーブルにするには、webvpn コンフィギュレーション モードで **csd enable** コマンドを使用します。Cisco Secure Desktop 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。

**csd enable**

**no csd enable**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 使用上のガイドライン

**csd enable** コマンドは、次の処理を実行します。

1. 以前の **csd image** *path* コマンドによって実行されたチェックを補足する有効性チェックを提供します。
2. sdesktop フォルダがまだ存在しない場合は、disk0: 上に作成します。
3. data.xml（Cisco Secure Desktop コンフィギュレーション）ファイルが sdesktop フォルダにまだ存在しない場合は、追加します。
4. フラッシュ デバイスの data.xml を実行コンフィギュレーションにロードします。
5. Cisco Secure Desktop をイネーブルにします。

**show webvpn csd** コマンドを入力して、Cisco Secure Desktop がイネーブルであるかどうかを確認できます。

**csd enable** コマンドを入力する前に、実行コンフィギュレーション内に **csd image** *path* コマンドが存在する必要があります。

**no csd enable** コマンドは、実行コンフィギュレーションで Cisco Secure Desktop をディセーブルにします。Cisco Secure Desktop がディセーブルの場合、ユーザは Cisco Secure Desktop Manager にアクセスできず、リモート ユーザは Cisco Secure Desktop を使用できません。

data.xml ファイルを転送または交換する場合は、このファイルを実行コンフィギュレーションにロードするために、Cisco Secure Desktop をいったんディセーブルにしてからイネーブルにします。

## 例

次に、Cisco Secure Desktop イメージのステータスを表示し、Cisco Secure Desktop イメージをイネーブルにするためのコマンドの使用例を示します。

```
hostname(config-webvpn)# show webvpn csd
Secure Desktop is not enabled.
hostname(config-webvpn)# csd enable
hostname(config-webvpn)# show webvpn csd
Secure Desktop version 3.1.0.25 is currently installed and enabled.
hostname(config-webvpn)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show webvpn csd** | Cisco Secure Desktop がイネーブルである場合、そのバージョンを示します。ディセーブルの場合、CLI に「Secure Desktop is not enabled.」と表示されます。 |
| **csd image** | コマンドで指定された Cisco Secure Desktop イメージを、パスで指定されたフラッシュ ドライブから実行コンフィギュレーションにコピーします。 |

# csd image

Cisco Secure Desktop 配布パッケージを検証して、実行コンフィギュレーションに追加するには、Cisco Secure Desktop を効率的にインストールし、webvpn コンフィギュレーション モードで **csd image** コマンドを使用します。CSD 配布パッケージを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

**csd image** *path*

**no csd image** [*path*]

## 構文の説明

| | |
|---|---|
| *path* | Cisco Secure Desktop パッケージのパスおよびファイル名を 255 文字以内で指定します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 使用上のガイドライン

このコマンドを入力する前に、**show webvpn csd** コマンドを入力して、Cisco Secure Desktop イメージがイネーブルであるかどうかを判断します。CLI は、現在インストールされている Cisco Secure Desktop イメージがイネーブルである場合、そのバージョンを示します。

http://www.cisco.com/cisco/software/navigator.html から新しい Cisco Secure Desktop イメージをコンピュータにダウンロードし、フラッシュ ドライブに転送してから、**csd image** コマンドを使用して、イメージをインストールするか、または既存のイメージをアップグレードします。ダウンロードする場合、使用しているセキュリティ アプライアンスに合ったファイルを必ず取得してください。ファイルの形式は、**securedesktop_asa_**<*n*>**_**<*n*>***.pkg** です。

**no csd image** を入力すると、Cisco Secure Desktop Manager への管理アクセスと、Cisco Secure Desktop へのリモート ユーザ アクセスの両方が削除されます。このコマンドを入力しても、セキュリティ アプライアンスは、Cisco Secure Desktop ソフトウェアおよびフラッシュ ドライブ上の Cisco Secure Desktop コンフィギュレーションに対してどのような変更も行いません。

**（注）** 次回のセキュリティ アプライアンスのリブート時に Cisco Secure Desktop を確実に使用できるようにするために、**write memory** コマンドを入力して実行コンフィギュレーションを保存します。

## 例

次に、現在の Cisco Secure Desktop 配布パッケージを表示し、フラッシュ ファイル システムの内容を表示して、新しいバージョンにアップグレードするためのコマンドの使用例を示します。

```
hostname# show webvpn csd
Secure Desktop version 3.1.0.24 is currently installed and enabled.
hostname# config t
hostname(config)# webvpn
hostname(config-webvpn)# show disk all
-#- --length-- -----date/time------ path
  6 8543616    Nov 02 2005 08:25:36 PDM
  9 6414336    Nov 02 2005 08:49:50 cdisk.bin
 10 4634       Sep 17 2004 15:32:48 first-backup
 11 4096       Sep 21 2004 10:55:02 fsck-2451
 12 4096       Sep 21 2004 10:55:02 fsck-2505
 13 21601      Nov 23 2004 15:51:46 shirley.cfg
 14 9367       Nov 01 2004 17:15:34 still.jpg
 15 6594064    Nov 04 2005 09:48:14 asdmfile.510106.rls
 16 21601      Dec 17 2004 14:20:40 tftp
 17 21601      Dec 17 2004 14:23:02 bingo.cfg
 18 9625       May 03 2005 11:06:14 wally.cfg
 19 16984      Oct 19 2005 03:48:46 tomm_backup.cfg
 20 319662     Jul 29 2005 09:51:28 sslclient-win-1.0.2.127.pkg
 21 0          Oct 07 2005 17:33:48 sdesktop
 22 5352       Oct 28 2005 15:09:20 sdesktop/data.xml
 23 369182     Oct 10 2005 05:27:58 sslclient-win-1.1.0.133.pkg
 24 1836210    Oct 12 2005 09:32:10 securedesktop_asa_3_1_0_24.pkg
 25 1836392    Oct 26 2005 09:15:26 securedesktop_asa_3_1_0_25.pkg

38600704 bytes available (24281088 bytes used)

******** Flash Card Geometry/Format Info ********

COMPACT FLASH CARD GEOMETRY
   Number of Heads:            4
   Number of Cylinders       978
   Sectors per Cylinder       32
   Sector Size               512
   Total Sectors          125184

COMPACT FLASH CARD FORMAT
   Number of FAT Sectors      61
   Sectors Per Cluster         8
   Number of Clusters      15352
   Number of Data Sectors 122976
   Base Root Sector          123
   Base FAT Sector             1
   Base Data Sector          155
hostname(config-webvpn)# csd image disk0:securedesktop_asa_3_1_0_25.pkg
hostname(config-webvpn)# show webvpn csd
Secure Desktop version 3.1.0.25 is currently installed and enabled.
hostname(config-webvpn)# write memory
Building configuration...
Cryptochecksum: 5e57cfa8 0e9ca4d5 764c3825 2fc4deb6

19566 bytes copied in 3.640 secs (6522 bytes/sec)
[OK]
hostname(config-webvpn)#
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **show webvpn csd** | Cisco Secure Desktop がイネーブルである場合、そのバージョンを示します。ディセーブルの場合、CLI に「Secure Desktop is not enabled.」と表示されます。 |
| **csd enable** | 管理およびリモート ユーザ アクセス用に Cisco Secure Desktop をイネーブルにします。 |

# ctl

証明書信頼リスト プロバイダーをイネーブルにして、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 **ctl** 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。

**ctl install**

**no ctl instal**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルトでは、イネーブルです。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.0(2) | このコマンドが導入されました。 |

## 使用上のガイドライン

CTL プロバイダーをイネーブルにして、CTL クライアントの CTL ファイルを解析し、CTL ファイルのエントリに対するトラストポイントをインストールするには、CTL プロバイダー コンフィギュレーション モードで **ctl** コマンドを使用します。このコマンドでインストールされたトラストポイントの名前には「_internal_CTL_<ctl_name>」というプレフィックスが付いています。このコマンドはオプションであり、デフォルトでイネーブルになっています。

このコマンドがディセーブルの場合は、**crypto ca trustpoint** コマンドと **crypto ca certificate chain** コマンドを使用して、各 CallManager サーバと CAPF 証明書を手動でインポートおよびインストールする必要があります。

## 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。

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

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **ctl-provider** | CTL プロバイダー インスタンスを定義し、プロバイダー コンフィギュレーション モードを開始します。 |
| **server trust-point** | TLS ハンドシェイク中に提示するプロキシ トラストポイント証明書を指定します。 |
| **show tls-proxy** | TLS プロキシを表示します。 |
| **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。 |

# ctl-file（グローバル）

電話プロキシ用に作成するための CTL インスタンス、またはフラッシュ メモリに格納されている CTL ファイルを解析するための CTL インスタンスを指定するには、グローバル コンフィギュレーション モードで **ctl-file** コマンドを使用します。CTL インスタ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。

**ctl-file** *ctl_name* **noconfirm**

**no ctl-file** *ctl_name* **noconfirm**

## 構文の説明

| | |
|---|---|
| *ctl_name* | CTL インスタンスの名前を指定します。 |
| **noconfirm** | （任意）**no** コマンドとともに使用して、CTL ファイルが削除されたときにトラストポイントの削除に関する警告がセキュリティ アプライアンスのコンソールに表示されないようにします。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 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

LSC プロビジョニングが必要な電話をユーザが所有している場合は、**ctl-file** コマンドを使用して CTL ファイル インスタンスを設定するときに、CAPF 証明書を CUMC から ASA にインポートする必要もあります。『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

**（注）** CTL ファイルを作成するには、ctl ファイル コンフィギュレーション モードで **no shutdown** コマンドを使用します。CTL ファイルのエントリを変更したり CTL ファイルにエントリを追加したりするには、または CTL ファイルを削除するには、**shutdown** コマンドを使用します。

このコマンドの **no** 形式を使用すると、CTL ファイル、および電話プロキシによって内部的に作成されたすべての登録済みトラストポイントが削除されます。また、CTL ファイルを削除すると、関連する認証局から受信したすべての証明書が破棄されます。

## 例

次に、**ctl-file** コマンドを使用して、Phone Proxy 機能用の CTL ファイルを設定する例を示します。

```
hostname(config)# ctl-file myctl
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **ctl-file（Phone-Proxy）** | 電話プロキシ インスタンスの設定時に使用する CTL ファイルを指定します。 |
| **cluster-ctl-file** | フラッシュ メモリに格納されている CTL ファイルからトラストポイントをインストールするために、CTL ファイルを解析します。 |
| **phone-proxy** | Phone Proxy インスタンスを設定します。 |
| **record-entry** | CTL ファイルの作成に使用するトラストポイントを指定します。 |
| **sast** | CTL レコードに作成する SAST 証明書の数を指定します。 |

# ctl-file（Phone-Proxy）

電話プロキシの設定時に使用する CTL インスタンスを指定するには、電話プロキシ コンフィギュレーション モードで **ctl-file** コマンドを使用します。CTL インスタ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。

**ctl-file** *ctl_name*

**no ctl-file** *ctl_name*

## 構文の説明

| | |
|---|---|
| *ctl_name* | CTL インスタンスの名前を指定します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 例

次に、**ctl-file** コマンドを使用して、Phone Proxy 機能用の CTL ファイルを設定する例を示します。

```
hostname(config-phone-proxy)# ctl-file myctl
```

## 関連コマンド

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

# ctl-provider

CTL プロバイダー モードで証明書信頼リスト プロバイダー インスタンスを設定するには、グローバル コンフィギュレーション モードで **ctl-provider** 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。

**ctl-provider** *ctl_name*

**no ctl-provider** *ctl_name*

## 構文の説明

| | |
|---|---|
| *ctl_name* | CTL プロバイダー インスタンスの名前を指定します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.0(2) | このコマンドが導入されました。 |

## 使用上のガイドライン

CTL プロバイダー コンフィギュレーション モードを開始して CTL プロバイダー インスタンスを作成するには、**ctl-provider** コマンドを使用します。

## 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。

```
hostname(config)# ctl-provider my_ctl
hostname(config-ctl-provider)# client interface inside 172.23.45.1
hostname(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
hostname(config-ctl-provider)# export certificate ccm_proxy
hostname(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。 |
| **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。 |

| コマンド | 説明 |
|---|---|
| **service** | CTL プロバイダーがリッスンするポートを指定します。 |
| **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。 |

# customization

トンネル グループ、グループ、またはユーザに使用するカスタマイゼーションを指定するには、次のモードで **customization** コマンドを使用します。

トンネル グループ webvpn 属性コンフィギュレーション モードと webvpn コンフィギュレーション モードの場合（グローバル コンフィギュレーション モードからアクセス可能）

**customization** *name*

**no customization** *name*

webvpn コンフィギュレーション モードの場合（グループ ポリシー属性コンフィギュレーション モードまたはユーザ名属性コンフィギュレーション モードからアクセス可能）

**customization** {**none** | **value** *name*}

**no customization** {**none** | **value** *name*}

## 構文の説明

| | |
|---|---|
| *name* | 適用する WebVPN カスタマイゼーションの名前を指定します。 |
| **none** | グループまたはユーザのカスタマイゼーションをディセーブルにし、デフォルトの WebVPN ページを表示します。 |
| **value** *name* | グループ ポリシーまたはユーザに適用するカスタマイゼーションの名前を指定します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

## コマンド履歴

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

## 使用上のガイドライン

トンネル グループ webvpn 属性コンフィギュレーション モードで **customization** コマンドを入力する前に、webvpn コンフィギュレーション モードで **customization** コマンドを使用してカスタマイゼーションの名前を付け、設定する必要があります。

### Mode-Dependent コマンド オプション

**customization** コマンドで使用できるキーワードは、現在のモードによって異なります。グループ ポリシー属性 > webvpn コンフィギュレーション モードおよびユーザ名属性 > webvpn コンフィギュレーション モードでは、追加のキーワード **none** と **value** があります。これらのモードでの完全な構文は、次のとおりです。

[**no**] **customization** {**none** | **value** *name*}

**none** は、グループまたはユーザのカスタマイゼーションをディセーブルにし、カスタマイゼーションが継承されないようにします。たとえば、ユーザ名属性 > webvpn モードで **customization none** コマンドを入力すると、セキュリティ アプライアンスは、グループ ポリシーやトンネル グループ内の値を検索しません。

*name* は、グループまたはユーザに適用するカスタマイゼーションの名前です。

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

## 例

次に、パスワード プロンプトを定義する「123」という名前の WebVPN カスタマイゼーションを最初に確立するコマンド シーケンスの例を示します。この例では、次に「test」という WebVPN トンネル グループを定義し、**customization** コマンドを使用して、「123」という WebVPN カスタマイゼーションを使用することを指定しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# customization 123
hostname(config-webvpn-custom)# password-prompt Enter password
hostname(config-webvpn)# exit
hostname(config)# tunnel-group test type webvpn
hostname(config)# tunnel-group test webvpn-attributes
hostname(config-tunnel-webvpn)# customization 123
hostname(config-tunnel-webvpn)#
```

次に、「cisco」というカスタマイゼーションを「cisco_sales」というグループ ポリシーに適用する例を示します。グループ ポリシー属性 > webvpn コンフィギュレーション モードでは、**customization** コマンドに追加のコマンド オプション **value** が必要となることに注意してください。

```
hostname(config)# group-policy cisco_sales attributes
hostname(config-group-policy)#  webvpn
hostname(config-group-webvpn)# customization value cisco
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure tunnel-group** | すべてのトンネル グループのコンフィギュレーションを削除します。 |
| **show running-config tunnel-group** | 現在のトンネル グループ コンフィギュレーションを表示します。 |
| **tunnel-group webvpn-attributes** | WebVPN トンネル グループ属性を設定する設定 webvpn モードを開始します。 |