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た 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*

シンタックスの説明

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提供されている場合、セキュリティ アプライアンスは CA 証明書の計算されたフィンガープリントと比較し、2 つの値が一致した場合のみ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 専用の非対話型モードを使用して、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

このコマンドには、デフォルトの動作も値もありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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、CA 証明書は SCEP 経由でダウンロードされます。トラストポイントが SCEP 登録用に設定されていない場合、セキュリティ アプライアンスは 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

次の例では、セキュリティ アプライアンスが CA の証明書を要求します。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)#
```

次の例では、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、管理者に証明書が保持され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 サブモードに入ります。

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 モードに入るには、グローバル コンフィギュレーション モードで **crypto ca certificate chain** コマンドを使用します。グローバル コンフィギュレーション モードに戻るには、このコマンドの **no** 形式を使用するか、**exit** コマンドを使用します。

crypto ca certificate chain *trustpoint*

シンタックスの説明

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

デフォルト

このコマンドに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(1)	このコマンドが導入されました。

例

次の例では、トラストポイント central の CA 証明書チェーン サブモードに入ります。

```
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 モードに入るには、グローバル コンフィギュレーション モードで **crypto ca configuration map** コマンドを使用します。このコマンドを実行すると、CA 証明書マップ モードに入ります。証明書マッピング規則の優先順位付き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。マッピング規則の順序はシーケンス番号によって決まります。

暗号 CA 証明書マップ規則を削除するには、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*]}

シンタックスの説明

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規則の番号を指定します。範囲は 1 ～ 65535 です。トンネル グループを証明書マップ規則にマッピングする 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(1)	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認定者名（DN）に基づいて規則を設定できます。これらの規則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*	比較を通常名（CN）などの特定の DN アトリビュートに制限します。
co	含む
eq	等しい
nc	含まない
ne	等しくない

DN の一致表現では大文字と小文字が区別されません。

例

次の例は、example-map というマップ名とシーケンス番号 1（規則番号 1）で CA 証明書マップ モードに入り、subject-name という通常名（CN）アトリビュートが Pat と一致する必要があることを指定しています。

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

次の例は、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 モードに入り、subject-name 内のどこかに値 cisco が含まれることを指定しています。

```
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	規則エントリが 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（暗号 CA 証明書マップ）	規則エントリが 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** コマンドで作成された証明書マップ エントリをトンネル グループに関連付けます。

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、暗号 CA トラストポイント コンフィギュレーション モードで **crypto ca crl request** コマンドを使用します。

crypto ca crl request *trustpoint*

シンタックスの説明

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

デフォルト

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
暗号 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(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドの呼び出しは、実行コンフィギュレーションの一部になりません。

例

次の例では、central という名前のトラストポイントに基づいて CRL を要求します。

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

関連コマンド

コマンド	説明
crl configure	crl 設定モードに入ります。

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**]

シンタックスの説明

noconfirm	（オプション）すべてのプロンプトを表示しないようにします。要求されてい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、または他の非対話型で使用するためのものです。
trustpoint	登録に使用するトラストポイントの名前を指定します。最大文字数は 128 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	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 符号化 PKCS10 認証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型のプロンプトを生成します。

例

次の例では、SCEP 登録を使用して、トラストポイント tp1 で ID 証明書を登録します。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 サブモードに入ります。

crypto ca export

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

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

シンタックスの説明

passphrase	エクスポートする PKCS12 ファイルの暗号化に使用するパスフレーズを指定します。
pkcs12	トラストポイント コンフィギュレーションのエクスポートに使用する公開キー暗号化標準を指定します。
trustpoint	証明書とキーをエクスポートするトラストポイントの名前を指定します。エクスポート時にトラストポイントが RSA キーを使用する場合、エクスポートされるキー ペアはトラストポイントと同じ名前を割り当てられます。

デフォルト

このコマンドに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(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドの呼び出しは、アクティブなコンフィギュレーションの一部になりません。PKCS12 データは端末に書き込まれます。

例

次の例では、xxyyzz をパスコードとして使用して、トラストポイント central の PKCS12 データをエクスポートします。

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

Exported pkcs12 follows:

[ PKCS12 data omitted ]

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

hostname (config)#
```

関連コマンド

コマンド	説明
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 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のトラストポイント サブモードに入ります。

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、または 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、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**]

シンタックスの説明

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。最大文字数は 128 です。PKCS12 データをインポートし、トラストポイントが RSA キーを使用する場合、インポートされるキー ペアはトラストポイントと同じ名前を割り当てられます。
certificate	セキュリティ アプライアンスに、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に指示します。
pkcs12	セキュリティ アプライアンスに、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に指示します。
passphrase	PKCS12 データの暗号解除に使用するパスフレーズを指定します。
nointeractive	（オプション）非対話型モードを使用して証明書をインポートします。プロンプトをすべて表示しません。このオプションは、スクリプト、ASDM、または他の非対話型で使用するためのものです。

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(1)	このコマンドが導入されました。

例

次の例では、トラストポイント Main の証明書を手動でインポートします。

```
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)#
```

次の例では、PKCS12 データをトラストポイント central に手動でインポートします。

```
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のトラストポイント サブモードに入ります。

crypto ca trustpoint

指定したトラストポイントのトラストポイント サブモードに入るには、グローバル コンフィギュレーション モードで **crypto ca trustpoint** コマンドを使用します。指定したトラストポイントを削除するには、このコマンドの **no** 形式を使用します。このコマンドはトラストポイント情報を管理します。トラストポイントは、CA によって発行された証明書に基づいて CA の識別情報を表し、また、装置の識別情報を表すことがあります。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 によって発行されるユーザ証明書の認証ポリシーを指定します。

crypto ca trustpoint *trustpoint-name*

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

シンタックスの説明

noconfirm	対話型のプロンプトをすべて表示しません。
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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	Online Certificate Status Protocol（OSCP; オンライン証明書ステータス プロトコル）をサポートするためにサブコマンドが追加されました。**match certificate map**、**ocsp disable-nonce**、**ocsp url**、および **revocation-check** などのコマンドがあります。

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、暗号 CA トラストポイント コンフィギュレーション モードに入ります。

このマニュアルにアルファベット順に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、装置にインストールされていない場合にフェーズ 1 の IKE 交換中に提供されたときに受け入れるかどうかを指定します。
- **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 サブモードに入ります（**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の一部になりません。
- **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**：自動（SCEP）登録のリトライ期間を分単位で指定します。
- **enrollment retry count**：自動（SCEP）登録の許可されるリトライの最大回数を指定します。
- **enrollment terminal**：このトラストポイントを使用したカット 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を使用して登録する自動登録（SCEP）を指定し、登録 URL（*url*）を設定します。
- **exit**：サブモードを終了します。
- **fqdn** *fqdn*：登録中に、指定した完全修飾認定者名（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**：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。
- **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*：公開キーを認証するキー ペアを指定します。
- **match certificate** *map-name* **override ocsp**：証明書マップを OCSP 上書き規則と照合します。
- **ocsp disable-nonce**：ナンス拡張子をディセーブルにします。この拡張子は、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、この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。
- **exit**：サブモードを終了します。
- **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。CA は、通常、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。
- **revocation check**：失効ステータスをチェックする方法（CRL、OCSP、なし）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**：イネーブルにした場合、トラストポイントがリモート証明書を発行した CA に対して認証されていれば、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は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。

例

次の例では、central という名前のトラストポイントを管理するための CA トラストポイント モードに入ります。

```
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	暗号 CA 証明書マップ モードに入ります。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します。

crypto dynamic-map match address

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。

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

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

シンタックスの説明

acl-name	ダイナミック暗号マップ エントリに一致させるアクセス リストを指定します。
dynamic-map-name	ダイナミック暗号マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック暗号マップ エントリに対応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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例では、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 crypto dynamic-map コマンドの使用方法を示します。

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

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto dynamic-map	すべてのダイナミック暗号マップの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 をこの暗号マップ 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。この暗号マップ 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**

シンタックスの説明

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

デフォルト

デフォルト設定はオフです。

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(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

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

例

次のコマンドは、mymap という名前のダイナミック暗号マップの 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暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto dynamic-map	すべてのダイナミック暗号マップの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*

シンタックスの説明

dynamic-map-name	ダイナミック暗号マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック暗号マップ エントリに対応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、ダイナミック暗号マップ 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、ダイナミック暗号マップ 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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例では、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 に設定します。

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

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto dynamic-map	すべてのダイナミック暗号マップの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

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 | group 7]**

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

シンタックスの説明

dynamic-map-name	ダイナミック暗号マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック暗号マップ エントリに対応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。
group7	IPSec が、たとえば movianVPN クライアントで、楕円曲線フィールドのサイズが 163 ビットである group7（ECC）を使用するように指定します。
set pfs	このダイナミック暗号マップ 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、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(1)	このコマンドが変更され、Diffie-Hellman group 7 が追加されました。

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。実行しない場合は、ネゴシエーションに失敗します。ローカル コンフィギュレーション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

次の例では、ダイナミック暗号マップ 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します。指定された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暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto dynamic-map	すべてのダイナミック暗号マップの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**

シンタックスの説明

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

デフォルト

デフォルトでは、このコマンドの値はオフになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル 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

次のコマンドは、mymap という名前のダイナミック暗号マップの 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暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto dynamic-map	すべてのダイナミック暗号マップの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

ダイナミック暗号マップ 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*]

ダイナミック暗号マップ 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*]

すべてのトランスフォーム セットを指定するか、何も指定せずにこのコマンドの **no** 形式を使用すると、ダイナミック暗号マップ エントリが削除されます。

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

シンタックスの説明

dynamic-map-name	ダイナミック暗号マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック暗号マップ エントリに対応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。各暗号マップ 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)	暗号マップ 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

ダイナミック暗号マップは、すべてのパラメータが設定されていない暗号マップです。ポリシーのテンプレートとして機能し、未設定のパラメータは、IPSec ネゴシエーションでピアに必要な条件を照合するときに動的にラーニングされます。セキュリティ アプライアンスは、スタティック暗号マップでピアの IP アドレスが特定されていない場合に、ピアでトンネルをネゴシエートさせるために動的マップを使用します。これは、次のようなピアに当てはまります。

- パブリック IP アドレスが動的に割り当てられる。

  LAN-to-LAN 接続のピアでも、リモート アクセスするピアでも、DHCP を使用してパブリック IP アドレスを取得します。セキュリティ アプライアンスは、このアドレスをトンネルを開始するときだけ使用します。
- プライベート IP アドレスが動的に割り当てられる。

  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 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暗号マップを設定するので、（DHCP または別の方法で）動的に割り当てられた 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ので、IPSec ネゴシエーションを開始するには、ダイナミック暗号マップが必要です。たとえば、ヘッドセットが IKE のネゴシエーション中に Cisco VPN クライアントに 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。

ダイナミック暗号マップを使うと、IPSec の設定が簡単になります。ピアが常に事前に決定されていないネットワークで使用することをお勧めします。Cisco VPN クライアント（モバイル ユーザなど）や IP アドレスを動的に取得するルータがある場合に、ダイナミック暗号マップを使ってください。

ヒント　ダイナミック暗号マップの **permit** エントリに **any** キーワードを使うときは注意してください。マルチキャストやブロードキャストのトラフィックが **permit** エントリの対象となることもあるので、該当するアドレスの範囲について **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 で遮ら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。

ダイナミック暗号マップは、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、ダイナミック暗号マップを使用してリモート ピアと接続を開始することはできません。ダイナミック暗号マップを設定した場合は、発信トラフィックがアクセス リストで許可されていても、対応する SA が存在しないと、セキュリティ アプライアンスがトラフィックをドロップします。

暗号マップ セットには、ダイナミック暗号マップを含めることができます。ただし、ダイナミック暗号マップのセットには、一番低い優先度（優先度の数値が一番大きい）を設定し、セキュリティ アプライアンスがダイナミック暗号マップ以外のマップを先に評価するようにする必要があります。このように設定すると、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、ダイナミック暗号マップのセットを調べます。

スタティック暗号マップ セットと同様、ダイナミック暗号マップ セットにも、同じ dynamic-map-name を持つすべてのダイナミック暗号マップを含めます。dynamic-seq-num で、セット内のマップを区別します。ダイナミック暗号マップを設定する場合は、暗号アクセス リストに対して IPSec ピアのデータ フローを指示するために許可用の ACL を挿入してください。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、ピアが提示するデータ フローの ID をすべて受け入れることになります。

注意　ダイナミック暗号マップ 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通じるトラフィックにスタティック ルート（デフォルト）を割り当てないでください。インターフェイスに通じるトラフィックを特定するには、ダイナミック暗号マップに ACL を追加します。リモート アクセス トンネル用の ACL を設定するときは、適切なアドレス プールを指定してください。トンネルがアップの状態になってから、逆ルート注入を使用してルートを指定します。

1 つの暗号マップ セットに、スタティックとダイナミックの両方のマップ エントリを含めることができます。

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、トランスフォーム セットに関するコマンド例を 10 例示しています。次の例では、その同じ 10 例のトランスフォーム セットからなる dynamic0 というダイナミック暗号マップ エントリを作成します。

```
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	暗号マップ 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暗号マップをコンフィギュレーションから消去します。
show running-config crypto dynamic-map	ダイナミック暗号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	暗号マップのコンフィギュレーションを表示します。

crypto ipsec df-bit

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

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

シンタックスの説明

clear-df	（オプション）外部 IP ヘッダーは DF ビットを消去されること、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	（オプション）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	（オプション）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。しかし、元のパケットで DF ビットが消去されている場合、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、デフォルトでは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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

DF ビットを IPSec トンネル機能と共に使用すると、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から Don't Fragment（DF）ビットを消去、設定、またはコピーできるかどうかが指定できます。IP ヘッダー内の DF ビットにより、装置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、装置は使用可能な MTU の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 のサイズが不明な場合にも適しています。

例

グローバル コンフィギュレーション モードで入力した次の例では、IPSec DF ポリシーを **clear-df** に設定しています。

```
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*

シンタックスの説明

after-encryption	暗号化の後で MTU の最大サイズに近い IPSec パケットをフラグメント化するようにセキュリティ アプライアンスに指定します(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 パケットをフラグメント化するようにセキュリティ アプライアンスに指定します(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。
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

この機能はデフォルトでイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

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 のサイズに近い場合、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。MTU のサイズを超えると暗号化の後にパケットがフラグメント化され、このため暗号解除装置がプロセス パスで再組み立てされます。IPSec VPN の事前フラグメント化では、暗号解除装置はプロセス パスではなく高性能な CEF パスで動作するため、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では、暗号化装置は、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。装置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、装置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、暗号解除前のプロセス レベルの再組み立てが回避され、暗号解除のパフォーマンスおよび全体的な IPsec トラフィックのスループットの向上に役立ちます。

例

グローバル コンフィギュレーション モードで入力した次の例では、IPSec パケットの事前フラグメント化を装置上でグローバルにイネーブルにします。

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

グローバル コンフィギュレーション モードで入力した次の例では、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*}

シンタックスの説明

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。範囲は 10 ～ 2,147,483,647 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。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
1.1(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

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、共有秘密鍵を使用します。これらの鍵とセキュリティ アソシエーションは、両方同時にタイムアウトします。

個々の暗号マップ エントリでライフタイム値が設定されていない場合は、セキュリティ アソシエーションの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、セキュリティ アプライアンスは、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。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、期間を指定するものとトラフィック量を指定するものの 2 つがあります。セキュリティ アソシエーションは、いずれかのライフタイムに最初に到達した時点で期限切れになります。

セキュリティ アプライアンスでは、暗号マップ、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。これを行う場合は、変更によって影響を受ける接続だけがセキュリティ 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、暗号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、関連する接続だけ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。

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

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場合は、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時点で、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、攻撃者がキー再現攻撃を成功させることが困難になります。攻撃者にとっては、解析の対象となる、同じキーで暗号化されたデータの量が少なくなるためです。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（およびそれに対応するキー）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、どちらかを超えた時点で有効期限が切れます。

例

次の例では、セキュリティ アソシエーションのグローバル期間ライフタイムを指定します。

```
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）を消去します。
show running-config crypto map	すべての暗号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。この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***]**

シンタックスの説明

authentication	（オプション）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。 **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 **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 **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。 **esp-aes**：128 ビット キーで AES を使用する場合 **esp-aes-192**：192 ビット キーで AES を使用する場合 **esp-aes-256**：256 ビット キーで AES を使用する場合 **esp-des**：56 ビットの DES-CBC を使用する場合 **esp-3des**：トリプル DES アルゴリズムを使用する場合 **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

認証設定のデフォルトは、esp-none（認証しない）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(1)	この項が改訂されました。

使用上のガイドライン

トランスフォーム セットを設定したら、そのセットを暗号マップに割り当てます。1 つの暗号マップにトランスフォーム セットを 6 つまで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際、セキュリティ アプライアンスは、まず各暗号マップのアクセス リストとピアが一致するかどうかを調べます。次に、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、その他の設定を、暗号マップに割り当てられているトランスフォーム セットと照合します。一致する設定が見つかった場合は、セキュリティ アプライアンスは、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。ピアがアクセス リストに一致しない場合や、暗号マップに割り当てられているトランスフォーム セット内に完全に一致するセキュリティ設定が見つからない場合、セキュリティ アプライアンスは 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。また、認証を指定せずに暗号化を指定することもできます。作成してい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。変更しているトランスフォーム セットに認証だけを指定した場合は、現在の暗号化設定がそのまま残ります。

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 の大きなサイズのキーを扱えるように Diffie-Hellman group 5 を割り当てることをお勧めします。

ヒント

暗号マップまたはダイナミック暗号マップにトランスフォーム セットを適用し、後で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 セットに設定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。その後に続く値は、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、暗号化と認証をまったく設定しない場合を除く、すべてのオプションを示しています。

```
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 セットの設定を表示します。
crypto map set transform-set	暗号マップ 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	ダイナミック暗号マップ 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	暗号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 dynamic-map	ダイナミック暗号マップのコンフィギュレーションを表示します。

crypto ipsec transform-set mode transport

トランスフォーム セットの IPSec トランスポート 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 ipsec transport-set mode transport** コマンドを使用します。トランスフォーム セットから IPSec トランスポート モードを削除するには、このコマンドの **no** 形式を使用します。

crypto ipsec transform-set *transform-set-name* **mode transport**

no crypto ipsec transform-set *transform-set-name* **mode transport**

シンタックスの説明

mode transport	トンネル モード要求に加えて、トランスポート モード要求を受け入れるためのトランスフォーム セットを指定します。
transform-set-name	変更するトランスフォーム セットの名前を指定します。トランスフォーム セットをすでに作成していることを前提としています。
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

デフォルトはトンネル モードです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドは、トランスフォーム セットに対して IPSec トランスポート モードを指定します。Windows 2000 の L2TP/IPSec クライアントは IPSec トランスポート モードを使用するので、このトランスポート セットでトランスポート モードを選択する必要があります。デフォルトはトンネル モードです。

トンネル モードはトランスフォーム セットに対して自動的にイネーブルになります。セキュリティ アプライアンスは、Windows 2000 の L2TP/IPSec クライアントと通信する場合を除き（トランスポート モードを使用）、トンネル モードを使用します。

例

次の例では、暗号化に Triple DES を使用し、ハッシュ アルゴリズムに MD5/HMAC-128 を使用する transet5 という名前のトランスフォーム セットを設定してから、トランスフォーム セット transet5 に IPSec トランスポート モードを指定します。

```
hostname(config)# crypto ipsec transform-set transet5 esp-3des esp-md5-hmac
hostname(config)# crypto ipsec transform-set transet5 mode transport
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto	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）を消去します。
clear configure crypto map	すべての暗号マップを消去します。
show running-config crypto map	すべての暗号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 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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルト値はイネーブルです。

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(1)(1)	**isakmp am-disable** コマンドが導入されました。
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

次の例では、グローバル コンフィギュレーション モードで、アグレッシブ モードの着信接続をディセーブルにします。

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

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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルト値はディセーブルです。

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(1)(1)	**isakmp disconnect-notify** コマンドが導入されました。
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消去します。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear crypto isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

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。インターフェイス上で ISAKMP 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*

シンタックスの説明

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

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}**

シンタックスの説明

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、接続のタイプよって判別します（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）。
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文字列を指定します。

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

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*]

シンタックスの説明

port *port1...port10*	（オプション）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。ポート番号の範囲は 1 ～ 65535 です。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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)(1)	**isakmp ipsec-over-tcp** コマンドが導入されました。
7.2.(1)	**isakmpipsec-over-tcp** コマンドが、**crypto isakmpipsec-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、ポート 45 上で IPSec over TCP を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消去します。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear crypto isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp nat-traversal

NAT Traversal 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（イネーブルにするには **crypto isakmp enable** コマンドを使用します）、次に **crypto isakmp nat-traversal** コマンドを使用します。NAT Traversal がイネーブルのときに、これ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*

シンタックスの説明

natkeepalive	NAT キープアライブ間隔を 10 ～ 3,600 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、NAT Traversal（**crypto isakmp nat-traversal**）はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

使用上のガイドライン

Network Address Translation（NAT; ネットワーク アドレス変換）は、Port Address Translation（PAT; ポート アドレス変換）も含め、IPSec も使用し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 デバイスを問題なく通過することを妨げる非互換性が数多くあります。NAT Traversal を使用すると、ESP パケットが 1 つまたは複数の 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 NAT Traversal をサポートしています。NAT Traversal は、ダイナミックとスタティックの両方の暗号マップでサポートされています。

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。暗号マップ 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

次の例では、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、30 秒間隔で NAT Traversal をイネーブルにします。

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

crypto isakmp policy

IKE 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 isakmp policy** 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*

シンタックスの説明

priority	IKE ポリシーを一意に識別し、そのポリシーに優先順位を割り当てます。1 ～ 65534 の整数を使用します。1 は優先順位が最も高く、65534 が最も低くなります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2.(1)	このコマンドが導入されました。

使用上のガイドライン

crypto isakmp policy コマンドを使用すると、暗号 isakmp ポリシー モードに入って、認証、暗号化、グループ、ハッシュ、およびライフタイムの設定を行うことができます。

例

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

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

関連コマンド

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

crypto isakmp reload-wait

すべてのアクティブなセッションが自主的が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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)(1)	**isakmp reload-wait** コマンドが導入されました。
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リブートするように、セキュリティ アプライアンスに通知します。

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

crypto key generate dsa

ID 証明書用の DSA 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 dsa** コマンドを使用します。

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

シンタックスの説明

label *key-pair-label*	キー ペアに関連付ける名前を指定します。最大ラベル長は 128 文字です。DSA にはラベルが必要です。
modulus *size*	キー ペアのモジュール サイズ 512、768、または 1024 を指定します。デフォルトのモジュール サイズは 1024 です。
noconfirm	対話型のプロンプトをすべて表示しません。

デフォルト

デフォルトの係数サイズは 1024 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(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

SSL、SSH、および IPSec 接続をサポートする DSA キー ペアを生成するには、**crypto key generate dsa** コマンドを使用します。生成されたキー ペアは、コマンド シンタックスの一部として指定したラベルで識別します。ラベルを指定しない場合、セキュリティ アプライアンスはエラー メッセージを表示します。

（注） DSA キーを生成するとき、遅延が発生する場合があります。Cisco PIX 515E Firewall では、この遅延が最大数分にわたることがあります。

例

グローバル コンフィギュレーション モードで入力した次の例では、mypubkey というラベルの DSA キー ペアを生成します。

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

グローバル コンフィギュレーション モードで入力した次の例では、誤って mypubkey というラベルの重複した DSA キー ペアを生成しようとしています。

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

関連コマンド

コマンド	説明
crypto key zeroize	DSA キー ペアを削除します。
show crypto key mypubkey	DSA キー ペアを表示します。

crypto key generate rsa

ID 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**]

シンタックスの説明

general-keys	一組の汎用キーを生成します。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。同じラベルで別のキー 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、キー　ペアはスタティックに <Default-RSA-Key> という名前が付けられます。
modulus *size*	キー ペアのモジュール サイズ 512、768、1024、または 2048 を指定します。デフォルトのモジュール サイズは 1024 です。
noconfirm	対話型のプロンプトをすべて表示しません。
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 通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-keys** です。デフォルトの係数サイズは 1024 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(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

SSL、SSH、および IPSec 接続をサポートする 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 シンタックスの一部として指定できるラベルで識別します。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、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。

例

グローバル コンフィギュレーション モードで入力した次の例では、mypubkey というラベルの RSA キー ペアを生成します。

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

グローバル コンフィギュレーション モードで入力した次の例では、誤って mypubkey というラベルの重複した RSA キー ペアを生成しようとしています。

```
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)#
```

グローバル コンフィギュレーション モードで入力した次の例では、デフォルト ラベルの RSA キー ペアを生成します。

```
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**]

シンタックスの説明

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	対話型のプロンプトをすべて表示しません。
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のものです。

例

グローバル コンフィギュレーション モードで入力した次の例では、すべての RSA キー ペアを削除します。

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

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

関連コマンド

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

crypto map interface

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

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

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

シンタックスの説明

interface-name	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 をイネーブルにしていて、認証局（CA）を使用して証明書を取得する場合には、CA 証明書内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	暗号マップ 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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドは、暗号マップ セットを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るために使用します。セキュリティ アプライアンスでは、任意のアクティブ インターフェイスを IPSec の終端にできます。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暗号マップ 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暗号マップ セットは 1 つだけです。同じ *map-name* で *seq-num* が異なる暗号マップ 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が適用されます。セキュリティ アプライアンスは、*seq-num* が最も小さい暗号マップ 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、暗号マップ、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。これを行う場合は、変更によって影響を受ける接続だけがセキュリティ 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、暗号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、関連する接続だけ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。

（注）　すべてのスタティック暗号マップは、アクセス リスト、トランスフォーム セット、および IPsec ピアの 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、暗号マップは不完全で、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。しかし、暗号マップがアクセス 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、このセキュリティ アプライアンスはトラフィックをドロップします。

すべての暗号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。不完全な暗号マップを修正するには、暗号マップを削除し、欠けているエントリを追加して再び適用します。

例

グローバル コンフィギュレーション モードで入力した次の例では、mymap という名前の暗号マップ セットを外部インターフェイスに割り当てます。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暗号マップ エントリと対照され、評価されます。発信トラフィックが mymap 暗号マップ エントリの 1 つのアクセス 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暗号マップ 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
```

次の例は、必要な最小限の暗号マップ コンフィギュレーションを示しています。

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

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map ipsec-isakmp dynamic

与えられた暗号マップ エントリに既存のダイナミック暗号マップを参照するように要求するには、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。

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

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*

シンタックスの説明

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

デフォルト

デフォルトの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 **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

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

ダイナミック暗号マップを使用することで、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 番目の機能は（IKE を通じた）そのトラフィックのためのネゴシエーションが対象となります。

IPSec ダイナミック暗号マップは次の 4 つを指定します。

- 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共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

暗号マップ セットは、それぞれ異なるシーケンス番号（seq-num）を持ち、マップ名が共通している暗号マップ エントリの集合です。たとえば、所定のインターフェイスを介して、あるトラフィックには所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個のピアに転送するとします。このような構成をセットアップするには、2 つの暗号マップ エントリを作成します。マップ名は同じ名前にし、シーケンス番号をそれぞれ別の番号にします。

シーケンス番号引数として割り当てる番号は、任意に決定しないようにしてください。この番号は、暗号マップ セットに含まれている複数の暗号マップ エントリにランクを付けます。シーケンス番号の小さい暗号マップ エントリが番号の大きい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 エントリは優先順位が高くなります。

（注）　暗号マップをダイナミック暗号マップにリンクする場合は、ダイナミック暗号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暗号マップに暗号マップがリンクされます。暗号マップ 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。しかし、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。ダイナミック暗号マップを暗号マップに変換して戻す場合、変更は有効で、**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

グローバル コンフィギュレーション モードで入力した次のコマンドでは、暗号マップ mymap を test という名前のダイナミック暗号マップを参照するように設定します。

```
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	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map match address

アクセス リストを暗号マップ 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。暗号マップ エントリからアクセス リストを削除するには、このコマンドの **no** 形式を使用します。

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

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

シンタックスの説明

acl_name	暗号化アクセス リストの名前を指定します。この名前は、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	暗号マップ セットの名前を指定します。
seq-num	暗号マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドは、すべてのスタティック暗号マップに対して指定必須となるコマンドです。**crypto dynamic-map** コマンドでダイナミック暗号マップを定義する場合は、このコマンドは必須ではありませんが、使用することを強く推奨します。

アクセス リストを定義するには、**access-list** コマンドを使用します。

セキュリティ アプライアンスは、アクセ スリストを利用して、IPSec 暗号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保護されるようにします。

セキュリティ アプライアンスがパケットを deny 文と照合する場合、暗号マップ内の残りのアクセス コントロール エントリ（ACE）に対するパケットの評価を省略し、順番に次の暗号マップ内の 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、および暗号マップ セット内の次の暗号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。各暗号マップを別の 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暗号マップの詳細な評価から特別なトラフィックを除外し、特別なトラフィックを別の暗号マップの permit 文と一致させて別のセキュリティを提供または要求できます。

（注）　暗号化用のアクセス　リストは、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を判定しません。このような判定には、**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 リストが使用されます。

（注）　透過モードでは、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。透過モードでは、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	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map set connection-type

この暗号マップ エントリのバックアップ サイトツーサイト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}**

シンタックスの説明

answer-only	このピアが、適切な接続先ピアを決定するための初期の専用交換中に、最初は着信 IKE 接続だけに応答することを指定します。
bidirectional	このピアが、この暗号マップ 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。これはすべてのサイトツーサイト接続のデフォルトの接続タイプです。
map-*name*	暗号マップ セットの名前を指定します。
originate-only	このピアが、適切な接続先ピアを決定するための最初の専用交換を開始することを指定します。
seq-num	暗号マップ エントリに割り当てる番号を指定します。
set connection-type	この暗号マップ エントリのバックアップ サイトツーサイト機能の接続タイプを指定します。answer-only、originate-only、および bidirectional の 3 タイプの接続があります。

デフォルト

デフォルト設定は bidirectional 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	•	—	•	—	—

* 透過ファイアウォール 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暗号マップに含まれる暗号マップ エントリでは、connection-type 値は answer-only 以外の値に設定できません。

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

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 ピアを指定することができます。

この機能は、次のプラットフォーム間のみで動作します。

- 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 ピアのある側を **answer-only** キーワードを使用して answer-only として設定することをお勧めします。originate-only 側では、**crypto map set peer** コマンドを使用してピアの優先順位を指定します。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、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 ピアは専用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。

表 9-1 に、サポートされるすべての設定を示します。これら以外の組み合せでは、予測できないルーティング問題が生じることがあります。

表 9-1　サポートされるバックアップ LAN-to-LAN 接続タイプ

リモート側	中央側
originate-only	answer-only
bidirectional	answer-only
bidirectional	bidirectional

例

グローバル コンフィギュレーション モードで入力した次の例では、暗号マップ mymap を設定し、接続タイプを originate-only に設定します。

```
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	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map set inheritance

この暗号マップ 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。この暗号マップ 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}**

シンタックスの説明

data	規則で指定されているアドレス範囲内のすべてのアドレス ペアに 1 つのトンネルを指定します。
map-name	暗号マップ セットの名前を指定します。
rule	この暗号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。これはデフォルトの値です。
seq-num	暗号マップ エントリに割り当てる番号を指定します。
set inheritance	継承のタイプを **data** または **rule** に指定します。継承では、各セキュリティ ポリシー データベース（SPD）規則に対して 1 つのセキュリティ アソシエーション（SA）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(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、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のみ動作します。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、全体的なトンネルが少なくなります。データ設定は、セキュリティ依存型のアプリケーションに対してのみ使用する必要があります。

例

グローバル コンフィギュレーション モードで入力した次の例では、暗号マップ mymap を設定し、継承タイプを data に設定します。

```
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	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map set nat-t-disable

接続の NAT-T をこの暗号マップ 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。この暗号マップ 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***

シンタックスの説明

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

デフォルト

このコマンドの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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

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

例

グローバル コンフィギュレーション モードで入力した次のコマンドは、mymap という名前の暗号マップ 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	すべての暗号マップのすべてのコンフィギュレーションを消去します。
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	暗号マップのコンフィギュレーションを表示します。

crypto map set peer

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

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

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

シンタックスの説明

hostname	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	暗号マップ セットの名前を指定します。
peer	暗号マップ エントリの IPSec ピアをホスト名または IP アドレスで指定します。
seq-num	暗号マップ エントリに割り当てる番号を指定します。

デフォルト

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、最大 10 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暗号マップに対して指定必須となるコマンドです。**crypto dynamic-map** コマンドでダイナミック暗号マップ エントリを定義する場合には、このコマンドは必須ではなく、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、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（つまり暗号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

グローバル コンフィギュレーション モードで入力した次の例は、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暗号マップ コンフィギュレーションを示します。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セットアップできます。

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

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map set pfs

この暗号マップ 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完全転送秘密（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 | group7]**

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

シンタックスの説明

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。
group7	IPSec が、たとえば movianVPN クライアントで、楕円曲線フィールドのサイズが 163 ビットである group7（ECC）を使用するように指定します。
map-name	暗号マップ セットの名前を指定します。
seq-num	暗号マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトでは、PFS は設定されません。

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	このコマンドが変更され、Diffie-Hellman group 7 が追加されました。

使用上のガイドライン

PFS を使用すると、新しいセキュリティ アソシエーションをネゴシエートするたびに新しい Diffie-Hellman 交換が発生します。この交換によって、処理にかかる時間が長くなります。PFS を使用すると、セキュリティがいっそう向上します。1 つのキーが攻撃者によってクラックされた場合でも、信頼性が損なわ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、暗号マップ 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** 文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（group2）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。実行しない場合は、ネゴシエーションに失敗します。ローカル コンフィギュレーション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 group2、group5、または group7 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は、ネゴシエーションに失敗します。

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 のオファーをすべて受け入れません。

1536 ビットの Diffie-Hellman プライム モジュラス グループ group5 は、group1 や group2 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。

楕円曲線フィールドのサイズが 163 ビットである Diffie-Hellman Group 7 では、IPSec SA キーが生成されます。このオプションは、任意の暗号化アルゴリズムと共に使用できます。これは、movianVPN クライアントで使用するためのオプションですが、Group 7（ECC）をサポートしている任意のピアで使用できます。

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

グローバル コンフィギュレーション モードで入力した次の例では、暗号マップ「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します。

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

関連コマンド

コマンド	説明
clear isakmp sa	アクティブな IKE セキュリティ アソシエーションを削除します。
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。
tunnel-group	トンネル グループ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 phase1mode** コマンドを使用します。フェーズ 1 IKE ネゴシエーションの設定を削除するには、このコマンドの **no** 形式を使用します。アグレッシブ モードの Diffie-Hellman グループを含めることはオプションです。含めない場合、セキュリティ アプライアンスは group 2 を使用します。

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

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

シンタックスの説明

aggressive	フェーズ 1 IKE ネゴシエーションにアグレッシブ 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。
group7	IPSec が、たとえば movianVPN クライアントで、楕円曲線フィールドのサイズが 163 ビットである group7（ECC）を使用するように指定します。
main	フェーズ 1 IKE ネゴシエーションにメイン モードを指定します。
map-name	暗号マップ セットの名前を指定します。
seq-num	暗号マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトのフェーズ 1 のモードは、**main** 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(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、発信側モードでのみ動作します。応答側モードでは動作しません。

例

グローバル コンフィギュレーション モードで入力した次の例では、暗号マップ mymap を設定し、group2 を使用してフェーズ 1 のモードをアグレッシブに設定します。

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

関連コマンド

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

crypto map set reverse-route

この暗号マップ 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。この暗号マップ 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* ***set reverse-route***

シンタックスの説明

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

デフォルト

デフォルトでは、このコマンドの設定はオフになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル 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

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境界ルータに通知できます。

例

グローバル コンフィギュレーション モードで入力した次の例では、mymap という名前の暗号マップの RRI をイネーブルにします。

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

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map set security-association lifetime

特定の暗号マップ エントリについて、IPSec セキュリティ アソシエーションをネゴシエートするときに使用されるグローバル 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。暗号マップ エントリのライフタイム値をグローバル値にリセットするには、このコマンドの **no** 形式を使用します。

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

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

シンタックスの説明

kilobytes	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。 デフォルトは 4,608,000 KB です。
map-name	暗号マップ セットの名前を指定します。
seconds	セキュリティ アソシエーションの有効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	暗号マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトの 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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

暗号マップのセキュリティ アソシエーションは、グローバル ライフタイム値に基づいてネゴシエートされます。

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

特定の暗号マップ エントリでライフタイム値が設定されている場合は、セキュリティ アソシエーションの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、セキュリティ アプライアンスは、ピアへの要求の中でこの暗号マップ ライフタイム値を利用します。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、期間を指定するものとトラフィック量を指定するものの 2 つがあります。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、暗号マップ、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。これを行う場合は、変更によって影響を受ける接続だけがセキュリティ 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、暗号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、関連する接続だけ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。

期間ライフタイムを変更するには、**crypto map set security-association lifetime seconds** コマンドを使用します。期間ライフタイムを使用する場合は、指定した秒数が経過した時点で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

グローバル コンフィギュレーション モードで次のコマンドを入力すると、暗号マップ mymap のセキュリティ アソシエーション ライフタイムが秒単位および KB 単位で指定されます。

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

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map set transform-set

暗号マップ エントリ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*]

暗号マップ 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 map *map-name seq-num* **set transform-set** *transform-set-name1* [*… transform-set-name11*]

すべてのトランスフォーム セットを指定するか何も指定せずにこのコマンドの **no** 形式を使用すると、暗号マップ エントリが削除されます。

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

シンタックスの説明

map-name	暗号マップ セットの名前を指定します。
seq-num	暗号マップ エントリの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。各暗号マップ 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)	暗号マップ 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、すべての暗号マップ エントリに対して指定必須となるコマンドです。

IPSec 接続の開始側と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 アソシエーションで使用します。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、暗号マップ エントリの中で、ピアから送られた 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 接続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 セットを見つけられない場合、セキュリティ アソシエーションは確立されません。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ので、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、古いリストの代わりになる新しいリストを指定します。

このコマンドで暗号マップを変更する場合は、指定したシーケンス番号と同じ番号の暗号マップ エントリだけが変更されます。たとえば、次のコマンドを入力した場合、56des-sha というトランスフォーム セットがリストの最後に挿入されます。

```
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、上記の 2 つのコマンドで行った変更を合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)#
```

暗号マップ エントリ内のトランスフォーム セットの順番を変えるには、まずエントリを削除し、マップ名とシーケンス番号の両方を指定してから、エントリを作成し直します。たとえば、次のコマンドは、シーケンス番号 3 の map2 という暗号マップ 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、トランスフォーム セットに関するコマンド例を 10 例示しています。次の例では、その同じ 10 例のトランスフォーム セットからなる暗号マップ エントリ map2 を作成します。

```
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)#
```

グローバル コンフィギュレーション モードで入力した次の例は、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必要となる、最小限の暗号マップ コンフィギュレーションを示しています。

```
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暗号マップをコンフィギュレーションから消去します。
clear configure crypto map	すべての暗号マップをコンフィギュレーションから消去します。
crypto dynamic-map set transform-set	ダイナミック暗号マップ 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	ダイナミック暗号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	暗号マップのコンフィギュレーションを表示します。

crypto map set trustpoint

暗号マップ エントリのフェーズ 1 ネゴシエーション中に、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。暗号マップ エントリからトラストポイントを削除するには、このコマンドの **no** 形式を使用します。

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

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

シンタックスの説明

chain	（オプション）証明書チェーンを送信します。CA 証明書チェーンには、ルート証明書から ID 証明書まで、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	暗号マップ セットの名前を指定します。
seq-num	暗号マップ エントリに割り当てる番号を指定します。
trustpoint- name	フェーズ 1 ネゴシエーション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

デフォルト値は none 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(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

この暗号マップ コマンドは、接続の開始に限り有効です。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

グローバル コンフィギュレーション モードで入力した次の例では、暗号マップ 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指定します。

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

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。
tunnel-group	トンネル グループを設定します。

csc

セキュリティ アプライアンスでネットワーク トラフィックを CSC SSM に送信するのをイネーブルにするには、クラス コンフィギュレーション モードで **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 モードには、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。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

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

no csc

シンタックスの説明

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だけに適用します。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だけに適用します。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、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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 マップによって照合されたトラフィックすべてを 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進み続けるのを許可します。

CSC SSM がトラフィックをスキャンできない場合に、セキュリティ アプライアンスが一致しているトラフィックを取り扱う方法を指定できます。***fail-open*** キーワードは、CSC SSM が利用できない場合でも、トラフィックが宛先に進み続け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に、一致しているトラフィックが宛先に進み続け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。これは、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ものである場合に限りサポートします。つまり、CSC SSM は次の接続に限りスキャンできます。

- 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が、他のプロトコルに対してこれらのポートを間違って使用している接続を選択している場合、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 はそれ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 ポリシーが絶対に 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、外部の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の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限り、FTP ファイル転送のスキャンをサポートします。

FTP 検査は、CSC SSM によりスキャンする 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、データ転送用に動的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空けます。CSC SSM が FTP データをスキャンするように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。

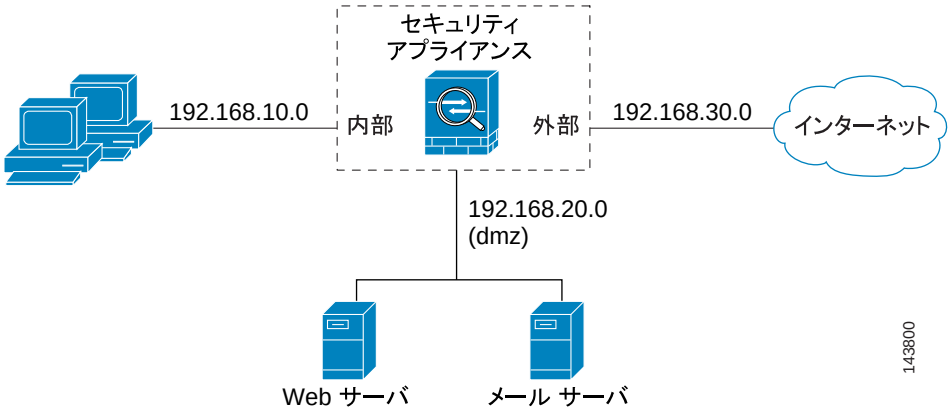
FTP 検査は、グローバル、または **csc** コマンドが適用される同じインターフェイスに適用できます。デフォルトでは、FTP 検査はグローバルにイネーブルにされています。デフォルトの検査コンフィギュレーションを変更していない場合は、CSC SSM により FTP スキャンをイネーブルにする際に、これ以上 FTP 検査コンフィギュレーションが必要になることはありません。

FTP 検査またはデフォルトの検査コンフィギュレーションの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

例

図 9-1 では、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。内部のネットワークから dmz ネットワーク上の Web サーバへの HTTP 要求は、スキャンしないでください。

図 9-1　CSC SSM スキャニングの一般的なネットワーク コンフィギュレーション



次のコンフィギュレーションは、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、内部の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必ずスキャンされるようにします。csc_out アクセス リストは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 接続も必ずスキャンされるようにしますが、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 を含んでいます。

2 番目のポリシーである csc_in_policy は、外部のインターフェイスに適用され、csc_in アクセス リストを使用して、外部インターフェイス上で dmz ネットワーク宛に送信される SMTP および HTTP に対する要求が CSC SSM によって必ず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、HTTP ファイルのアップロードから Web サーバを保護できます。

```
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 検査がイネーブルである必要があります。FTP 検査は、デフォルトでイネーブルです。

関連コマンド

コマンド	説明
class（ポリシー マップ）	トラフィックの分類に使用するクラス マップを指定します。
class-map	ポリシー マップ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 つまたは複数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 つまたは複数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 アクセスに対して 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。CSD 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

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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* コマンドにより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. disk0 上に sdesktop フォルダが存在しない場合は作成します。
3. sdesktop フォルダに data.xml（CSD コンフィギュレーション）ファイルが存在しない場合は挿入します。
4. フラッシュ デバイスから data.xml を実行コンフィギュレーションにロードします。
5. CSD をイネーブルにします。

show webvpn csd コマンドを入力して、CSD がイネーブルかどうかを判断します。

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 CSD をディセーブルにします。CSD 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 CSD 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、CSD をディセーブルにした後、イネーブルにして実行コンフィギュレーションにこのファイルをロードします。

例

次のコマンドの例では、CSD イメージのステータスの表示方法とイネーブルにする方法を示します。

```
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	CSD がイネーブルである場合、そのバージョンを識別します。ディセーブルの場合、CLI は「Secure Desktop is not enabled.」と表示します。
csd image	コマンドで指定された CSD 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、CSD 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 ディストリビューション 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*]

シンタックスの説明

path	CSD 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

次の表は、このコマンドを入力できるモードを示しています。

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

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、CSD 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 CSD 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/cgi-bin/tablebuild.pl/securedesktop から新しい CSD 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既存のイメージをアップグレードします。必ず、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ダウンロードしてください。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、CSD へのリモート ユーザ アクセスの両方を削除します。こ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、CSD ソフトウェアとフラッシュ ドライブ上の CSD 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）　**write memory** コマンドを入力すると、次にセキュリティ アプライアンスをリブートしたときに CSD が使用できることを保証するために、実行コンフィギュレーションを保存します。

例

次のコマンド例は、現在の CSD 配布パッケージの表示方法、フラッシュ ファイル システムの内容の表示方法、および新しい CSD バージョンにアップグレードする方法について示しています。

```
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	CSD がイネーブルである場合、そのバージョンを識別します。ディセーブルの場合、CLI は「Secure Desktop is not enabled.」と表示します。
csd enable	管理およびリモート ユーザ アクセスの CSD をイネーブルにします。

customization

トンネル グループ、グループ、またはユーザ用の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 コンフィギュレーション モード

customization *name*

no customization *name*

グループ ポリシー webvpn コンフィギュレーション モードとユーザ名 webvpn コンフィギュレーション モード

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

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

シンタックスの説明

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ webvpn コンフィギュレーション	•	—	•	—	—
グループ ポリシー WebVPN コンフィギュレーション	•	—	•	—	—
ユーザ名の 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 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** コマンドを使用した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。

モード別のコマンドのオプション

customization コマンドで使用できるキーワードは、モードによって異なります。グループ ポリシー webvpn コンフィギュレーション モードとユーザ名 webvpn コンフィギュレーション モードでは、追加の ***none*** キーワードと ***value*** キーワードがあります。これらのモードでの完全なシンタックスは、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、継承できないようにします。たとえば、ユーザ名 webvpn コンフィギュレーション 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 グループに含まれる値を検索しません。

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

次の例では、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 シーケンスを示します。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)#
```

次の例では、「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方法を示します。グループ ポリシー webvpn コンフィギュレーション モードでは、**customization** コマンドに **value** オプションを追加する必要があ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 アトリビュートを設定する config-webvpn モードに入ります。