java-trustpoint コマンド～ kill コマンド

java-trustpoint

指定したトラストポイントの場所から PKCS12 証明書およびキー関連情報を使用するように WebVPN Java オブジェクト署名機能を設定設定するには、webvpn コンフィギュレーション モードで **java-trustpoint** コマンドを使用します。Java オブジェクト署名の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。

java-trustpoint *trustpoint*

no java-trustpoint

構文の説明

トラストポイント	**crypto ca import** コマンドによって設定されたトラストポイントの場所を指定します。

デフォルト

デフォルトでは、Java オブジェクト署名のトラストポイントは none に設定されています。

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	トランスペアレント	シングル	コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(2)	このコマンドが追加されました。

使用上のガイドライン

トラストポイントは、認証局（CA）または ID キー ペアを表します。**java-trustpoint** コマンドの場合、指定したトラストポイントにはアプリケーション署名エンティティの X.509 証明書、その証明書に対応する RSA 秘密キー、ルート CA までの認証局チェーンを含める必要があります。そのためには通常、**crypto ca import** コマンドを使用して PKCS12 形式のバンドルをインポートします。PKCS12 バンドルは、信頼できる CA 認証局から入手するか、openssl といったオープン ソース ツールを使用して既存の X.509 証明書と RSA 秘密キーから手動で作成できます。

（注） アップロードされた証明書は、パッケージ（CSD パッケージなど）に組み込まれた Java オブジェクトの署名には使用できません。

例

次に、最初に新しいトラストポイントを設定してから、そのトラストポイントを WebVPN Java オブジェクト署名用に設定する例を示します。

```
ciscoasa(config)# crypto ca import mytrustpoint pkcs12 mypassphrase
Enter the base 64 encoded PKCS12.
End with the word "quit" on a line by itself.
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully.
ciscoasa(config)#
```

次に、WebVPN Java オブジェクトに署名する新しいトラストポイントを設定する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config)# java-trustpoint mytrustpoint
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ca import	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ます。

join-failover-group

コンテキストをフェールオーバー グループに割り当てるには、コンテキスト コンフィギュレーション モードで **join-failover-group** 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。

join-failover-group *group_num*

no join-failover-group *group_num*

構文の説明

group_num	フェールオーバー グループの番号を指定します。

デフォルト

フェールオーバー グループ 1。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

管理コンテキストは、常にフェールオーバー グループ 1 に割り当てられます。フェールオーバー グループとコンテキスト アソシエーションを表示するには、**show context detail** コマンドを使用できます。

コンテキストをフェールオーバー グループに割り当てる前に、**failover group** コマンドを使用して、フェールオーバー グループをシステム コンテキスト内に作成する必要があります。このコマンドは、コンテキストがアクティブ状態になっているユニット上で入力します。デフォルトでは、未割り当てのコンテキストは、フェールオーバー グループ 1 のメンバーになっています。そのため、コンテキストがまだフェールオーバー グループに割り当てられていない場合は、フェールオーバー グループ 1 がアクティブ状態になっているユニット上で、このコマンドを入力する必要があります。

システムからフェールオーバー グループを削除するには、事前に **no join-failover-group** コマンドを使用して、フェールオーバー グループからコンテキストをすべて削除しておく必要があります。

例

次に、ctx1 というコンテキストをフェールオーバー グループ 2 に割り当てる例を示します。

```
ciscoasa(config)# context ctx1
ciscoasa(config-context)# join-failover-group 2
ciscoasa(config-context)# exit
```

関連コマンド

コマンド	説明
コンテキスト	指定したコンテキストのコンテキスト コンフィギュレーション モードを開始します。
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
show context detail	コンテキストの詳細情報（名前、クラス、インターフェイス、フェールオーバー グループ アソシエーション、およびコンフィギュレーション ファイルの URL など）を表示します。

jumbo-frame reservation

ジャンボ フレームをサポート対象のモデルで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 **jumbo-frame reservation** コマンドを使用します。ジャンボ フレームをディセーブルにするには、このコマンドの **no** 形式を使用します。

(注) この設定を変更した場合は、ASA のリブートが必要です。

jumbo-frame reservation

no jumbo-frame reservation

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

ジャンボ フレームの予約は、デフォルトではディセーブルになっています。

ASASM では、デフォルトでジャンボ フレームがサポートされます。このコマンドを使用する必要はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.1(1)	このコマンドが ASA 5580 に追加されました。
8.2(5)/8.4(1)	ASA 5585-X のサポートが追加されました。
8.6(1)	ASA 5512-X ～ ASA 5555-X のサポートが追加されました。

使用上のガイドライン

ジャンボ フレームとは、標準的な最大値 1518 バイト（レイヤ 2 ヘッダーおよび VLAN タギングの 18 バイトを含む）より大きく、9216 バイトまでのイーサネット パケットのことです。**mtu** コマンドは*ペイロード*値のみを指定するため、9216 バイトのジャンボ フレームについては MTU が 9198（9216 ～ 18 バイトはヘッダー）になるように設定する必要があります。

ジャンボ フレームをサポートするには追加のメモリが必要となるため、アクセス リストなどの他の機能の最大使用量が制限される可能性があります。

ジャンボ フレームは Management *n*/*n* インターフェイスではサポートされません。

ジャンボ フレームを送信する必要がある各インターフェイスについて、MTU を 1500 より大きい値に設定してください。たとえば、**mtu** コマンドを使用して値を 9198 に設定してください。ASASM では、デフォルトでジャンボ フレームがサポートされるため、**jumbo-frame** reservation コマンドを設定する必要はありません。MTU の値の設定だけ行ってください。

また、ジャンボ フレームを使用する場合は、TCP の最大セグメント サイズ（MSS）の値を設定してください。MSS は、MTU より 120 バイト小さい値に設定する必要があります。たとえば、MTU を 9000 に設定した場合、MSS は 8880 に設定する必要があります。MSS を設定するには、**sysopt connection tcpmss** コマンドを使用できます。

フェールオーバー ペアでジャンボ フレームがサポートされるようにするには、プライマリ ユニットとセカンダリ ユニットの両方をリブートする必要があります。ダウン時間を回避するには、次の手順を実行します。

- アクティブ ユニットでコマンドを発行します。
- アクティブ ユニットで実行コンフィギュレーションを保存します。
- プライマリ ユニットとセカンダリ ユニットを 1 つずつリブートします。

例

次に、ジャンボ フレームの予約をイネーブルにし、コンフィギュレーションを保存して ASA をリロードする例を示します。

```
ciscoasa(config)# jumbo-frame reservation
WARNING: this command will take effect after the running-config is saved
and the system has been rebooted. Command accepted.

ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: 718e3706 4edb11ea 69af58d0 0a6b7cb5

70291 bytes copied in 3.710 secs (23430 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm] Y
```

関連コマンド

コマンド	説明
mtu	インターフェイスの最大伝送単位を指定します。
show jumbo-frame reservation	**jumbo-frame reservation** コマンドの現在のコンフィギュレーションを表示します。

kcd-server

Active Directory ドメインに参加できるように ASA を設定するには、webvpn コンフィギュレーション モードで **kcd-server** コマンドを使用します。ASA の指定した動作を解除するには、このコマンドの **no** 形式を使用します。

kcd-server *aaa-server-group_name* **user** *username* **password** *password*

no kcd-server

構文の説明

user	サービス レベル特権を持つ Active Directory ユーザを指定します。
password	指定したユーザのパスワードを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。

使用上のガイドライン

Active Directory ドメインに参加できるように ASA を設定するには、webvpn コンフィギュレーション モードで **kcd-server** コマンドを使用します。ドメイン コントローラの名前とレルムは **aaa-server-groupname** コマンドで指定します。AAA サーバ グループのタイプは Kerberos サーバにする必要があります。**username** オプションと **password** オプションは、管理者特権を持つユーザには対応しませんが、ドメイン コントローラのサービス レベル特権を持つユーザに対応する必要があります。このコマンドの結果として成功または失敗のステータスが表示されます。この結果は、**show webvpn kcd** コマンドでも確認できます。

ASA 環境の Kerberos 制約付き委任（KCD）は、Kerberos で保護されたすべての Web サービスへのシングル サインオン（SSO）アクセスを WebVPN ユーザに提供します。ユーザの代わりに ASA でクレデンシャル（サービス チケット）を管理し、そのチケットを使用してサービスに対するユーザの認証を行います。

kcd-server コマンドが機能するには、ASA はソース ドメイン（ASA が常駐するドメイン）とターゲットまたはリソース ドメイン（Web サービスが常駐するドメイン）間の信頼関係を確立する必要があります。ASA は、その独自のフォーマットを使用して、サービスにアクセスするリモート アクセス ユーザの代わりに、ソースから宛先ドメインへの認証パスを越えて、必要なチケットを取得します。

このパスのことをクロスレルム認証と呼びます。クロスレルム認証の各フェーズで、ASA は特定のドメインのクレデンシャルおよび後続のドメインとの信頼関係に依存しています。

クロスレルム認証を使用するように ASA を設定するには、**ntp**、**hostname**、**dns domain-lookup**、**dns server-group** の各コマンドを使用して、Active Directory ドメインに参加する必要があります。

例

次に、**kcd-server** コマンドの使用例を示します。

```
ciscoasa(config)# aaa-server kcd-grp protocol kerberos
ciscoasa(config-aaa-server-group)# aaa-server kcd-grp host DC
ciscoasa(config-aaa-server-group)# kerberos-realm EXAMPLE.COM
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# kcd-server kcd-grp user Administrator password Cisco123
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)#
```

次に、クロスレルム認証の設定例を示します。ドメイン コントローラは 10.1.1.10（内部インターフェイスで到達可能）、ドメイン名は PRIVATE.NET です。また、ドメイン コントローラのサービス アカウントのユーザ名は dcuser、パスワードは dcuser123! です。

```
ciscoasa(config)# config t

-----Create an alias for the Domain Controller-------------

ciscoasa(config)# name 10.1.1.10 DC

----Configure the Name server-----------------------------

ciscoasa(config)# ntp server DC

----Enable a DNS lookup by configuring the DNS server and Domain name --------------

ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# name-server DC
ciscoasa(config-dns-server-group)# domain-name private.net

----Configure the AAA server group with Server and Realm------------------------------

ciscoasa(config)# aaa-server KerberosGroup protocol Kerberos
ciscoasa(config-asa-server-group)# aaa-server KerberosGroup (inside) host DC
ciscoasa(config-asa-server-group)# Kerberos-realm PRIVATE.NET

----Configure the Domain Join-----------------------------

ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# kcd-server KerberosGroup username dcuser password dcuser123!
ciscoasa(config)#
```

関連コマンド

コマンド	説明
aaa-server	AAA サーバ コンフィギュレーション モードを開始します。このモードでは、AAA サーバのパラメータを設定できます。
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始します。このモードでは、ホストに固有の AAA サーバ パラメータを設定できます。
clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。
dns	ドメイン ネーム サーバを指定します。
domain-name	サーバのドメイン名を指定します。
hostname	ホスト名を指定します。
ntp	転送プロトコルを指定します。
show aaa-kerberos	すべての Kerberos AAA サーバのサーバ統計情報を表示します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

keepout

(ASA のメンテナンスまたはトラブルシューティングの実行中に)新しいユーザ セッションのログイン ページではなく、管理者定義のメッセージを表示するには、webvpn コンフィギュレーション モードで **keepout** コマンドを使用します。以前に設定された立ち入り禁止ページを削除するには、このコマンドの **no** 形式を使用します。

keepout

no keepout *string*

構文の説明

string	二重引用符で囲んだ英数字ストリング。

デフォルト

立ち入り禁止ページはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドがイネーブルにされると、クライアントレスの WebVPN ポータル ページが使用不可になります。ポータルのログイン ページではなく、ポータルが使用不可であることを通知する管理者定義メッセージが表示されます。クライアントレス アクセスをディセーブルにするが AnyConnect アクセスは許可するには、**keepout** コマンドを使用します。また、このコマンドを使用して、メンテナンス中のためポータルが使用不可であることを示すこともできます。

例

次に、立ち入り禁止ページを設定する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# keepout "The system is unavailable until 7:00 a.m. EST."
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
webvpn	webvpn コンフィギュレーション モードを開始します。このモードではクライアントレス SSL VPN 接続の属性を設定できます。

kerberos-realm

この Kerberos サーバのレルム名を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **kerberos-realm** コマンドを使用します。レルム名を削除するには、このコマンドの **no** 形式を使用します。

kerberos-realm *string*

no kerberos-realm

構文の説明

string	大文字と小文字が区別される最大 64 文字の英数字ストリング。ストリングにスペースは使用できません。 (注) Kerberos レルム名では数字と大文字だけを使用します。ASA では、*string* 引数に小文字のアルファベットを使用できますが、小文字は大文字に変換されません。大文字だけを使用してください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Kerberos サーバに対してのみ有効です。

Microsoft Windows の **set USERDNSDOMAIN** コマンドを Kerberos レルムの Windows 2000 Active Directory サーバ上で実行する場合は、*string* 引数の値をこのコマンドの出力と一致させる必要があります。次の例では、EXAMPLE.COM が Kerberos レルム名です。

```
C:\>set USERDNSDOMAIN
USERDNSDOMAIN=EXAMPLE.COM
```

string 引数には、数字と大文字のアルファベットのみを使用する必要があります。**kerberos-realm** コマンドでは、大文字と小文字が区別されます。また、ASA では、小文字は大文字に変換されません。

例

次のシーケンスは、AAA サーバ ホストの設定に関するコンテキストで Kerberos レルムを「EXAMPLE.COM」に設定するための **kerberos-realm** コマンドを示しています。

```
ciscoasa(config)# aaa-server svrgrp1 protocol kerberos
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション サブモードを開始し、ホスト固有の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

key（AAA サーバ ホスト）

AAA サーバに対して NAS を認証するために使用されるサーバ シークレットの値を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **key** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードには、AAA サーバ プロトコル コンフィギュレーション モードからアクセスできます。キーを削除するには、このコマンドの **no** 形式を使用します。

key *key*

no key

構文の説明

key	最大 127 文字の英数字キーワード。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

key の値は、127 文字までの英数字で構成されているキーワードで、TACACS+ サーバ上のキーと同じ値にします。大文字と小文字は区別されます。127 を超える文字は無視されます。このキーは、クライアントとサーバの間でやり取りするデータを暗号化するために使用されます。キーは、クライアント システムとサーバ システムの両方で同一である必要があります。キーにスペースは使用できませんが、その他の特殊文字は使用できます。キー（サーバ シークレット）の値は、ASA を AAA サーバに対して認証します。

このコマンドは、RADIUS サーバと TACACS+ サーバに対してのみ有効です。

例

次に、ホスト「1.2.3.4」に「srvgrp1」という TACACS+ AAA サーバを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、キーを「myexclusivemumblekey」に設定する例を示します。

```
ciscoasa(config)# aaa-server svrgrp1 protocol tacacs+
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa(config-aaa-server-host)# timeout 9
```

```
ciscoasa(config-aaa-server-host)# retry-interval 7
ciscoasa(config-aaa-server-host)# key myexclusivemumblekey
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始します。このモードでは、ホストに固有の AAA サーバ パラメータを設定できます。
clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。
show running-config aaa-server	AAA サーバの設定を表示します。

key(クラスタ グループ)

クラスタ制御リンクの制御トラフィックの認証キーを設定するには、クラスタ グループ コンフィギュレーション モードで **key** コマンドを使用します。キーを削除するには、このコマンドの **no** 形式を使用します。

key *shared_secret*

no key [*shared_secret*]

構文の説明

shared_secret	共有秘密を 1 ～ 63 文字の ASCII 文字列に設定します。共有秘密は、キーを生成するために使用されます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、データパス トラフィック(接続状態アップデートや転送されるパケットなど)には影響しません。データパス トラフィックは、常にクリア テキストとして送信されます。

例

次に、共有秘密を設定する例を示します。

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

関連コマンド

コマンド	説明
clacp system-mac	スパンド EtherChannel を使用するときは、ASA は cLACP を使用してネイバー スイッチとの間で EtherChannel のネゴシエーションを行います。
cluster group	クラスタに名前を付け、クラスタ コンフィギュレーション モードを開始します。
cluster-interface	クラスタ制御リンク インターフェイスを指定します。
cluster interface-mode	クラスタ インターフェイス モードを設定します。
conn-rebalance	接続の再分散をイネーブルにします。
console-replicate	スレーブ ユニットからマスター ユニットへのコンソール複製をイネーブルにします。
enable(クラスタ グループ)	クラスタリングをイネーブルにします。
health-check	クラスタのヘルス チェック機能(ユニットのヘルス モニタリングおよびインターフェイスのヘルス モニタリングを含む)をイネーブルにします。
local-unit	クラスタ メンバーに名前を付けます。
mtu cluster-interface	クラスタ制御リンク インターフェイスの最大伝送ユニットを指定します。
priority(クラスタ グループ)	マスター ユニット選定のこのユニットのプライオリティを設定します。

key chain

IGP ピアを認証するためのローテーション キーを設定するには、グローバル コンフィギュレーション モードで **key chain** 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。

key chain *key-chain-name* **key** *key-id* **key-string {0 | 8}** *key-string-text* **cryptographic-algorithm** md5 **[accept-lifetime** [*local* | *start-time*] [**duration** {*duration value* | *infinite* | *end-time*}] [**send-lifetime** [*local* | *start-time*] [**duration** {*duration value* | *infinite* | *end-time*}]

no key chain *key-chain-name* **key** *key-id* **key-string {0 | 8}** *key-string-text* **cryptographic-algorithm** md5 [**accept-lifetime** [*local* | *start-time*] [**duration** {*duration value* | *infinite* | *end-time*}] [**send-lifetime** [*local* | *start-time*] [**duration** {*duration value* | *infinite* | *end-time*}]

構文の説明

key-chain-name	OSPFv2 認証用に設定するキー チェーンの名前。
key-id	キー チェーン内の固有識別子。有効な範囲は 1 ～ 255 です。
0	暗号化されていないパスワードが続くことを指定します。
8	暗号化されたパスワードが後に続くことを指定します。
key-string-text	キー id のパスワード。文字列には、プレーン テキストまたは暗号化された値を使用できます。
md5	サポートされている暗号化アルゴリズム。md5 のみがサポートされています。
accept-lifetime	(任意)別のデバイスとのキー交換時にデバイスがそのキーを受け入れる期間。
send-lifetime	(任意)別のデバイスとのキー交換時にデバイスがそのキーを送信する期間。

デフォルト

受け入れまたは送信のライフタイムが指定されていない場合は、デフォルトで常にアクティブになります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.12(1)	このコマンドが追加されました。

使用上のガイドライン

key chain コマンドを使用して、インターフェイスの OSPFv2 認証で使用されるキー チェーンを設定します。**key id**、**key string**、および **cryptographic-algorithm** コマンドを入力する必要があります。受け入れおよび送信のライフタイムを入力して、キーのローテーションをスケジュールします。ライフタイム変数は、セキュアなキー ロールオーバーを処理するのに便利です。デバイスはキーのライフタイムを使用して、特定の期間にキー チェーン内のどのキーがアクティブになるかを判断します。ライフタイムが指定されていない場合、キー チェーン認証は、タイム ラインを使用しない MD5 認証と同様に機能します。キー チェーンの設定を削除するには、**no key chain** を使用します。

例

次の例は、キー チェーンの設定コマンドを示しています。

```
ciscoasa(config)# key chain CHAIN1
ciscoasa(config-keychain)# key 1
ciscoasa(config-keychain-key)# key-string 0 CHAIN1KEY1STRING
ciscoasa(config-keychain-key)# cryptographic-algorithm md5
ciscoasa(config-keychain-key)# accept-lifetime 11:22:33 1 SEP 2018 infinite
ciscoasa(config-keychain-key)#
```

例

次の例は、実行中のキーチェーン設定の出力を示しています。

```
ciscoasa# show running key chain
key chain CHAIN2
 key 1
  key-string KEY1CHAIN2
  cryptographic-algorithm md5
 key 2
  accept-lifetime 11:00:12 Sep 1 2018 11:12:12 Sep 1 2018
  cryptographic-algorithm md5
key chain CHAIN1
 key 1
  key-string CHAIN1KEY1STRING
  accept-lifetime 11:22:33 Sep 1 2018 duration -1
  cryptographic-algorithm md5
ciscoasa# show runing key chain CHAIN1
key chain CHAIN1
 key 1
  key-string CHAIN1KEY1STRING
  accept-lifetime 11:22:33 Sep 1 2018 duration -1
  cryptographic-algorithm md5
ciscoasa#
```

関連コマンド

コマンド	説明
show key chain	設定されたキー チェーンを表示します。
show running key chain	現在アクティブなキー チェーンの詳細を表示します。
clear configure key chain	設定されているキー チェーンを削除します。

key config-key password-encryption

暗号キーの生成に使用するマスター パスフレーズを設定し、プレーン テキストのパスワードを暗号化して安全に保存するには、グローバル コンフィギュレーション モードで **key config-key password-encryption** コマンドを使用します。パスフレーズで暗号化されたパスワードを復号化するには、このコマンドの **no** 形式を使用します。

key config-key password-encryption *passphrase* [*old_passphrase*]

no key config-key password-encryption *passphrase*

構文の説明

passphrase	パスフレーズの長さは、8 ～ 128 文字にする必要があります。パスフレーズには、バックスペースと二重引用符を除くすべての文字を使用できます。コマンドにパスフレーズを入力しないと、入力を求めるプロンプトが表示されます。インタラクティブ プロンプトを使用してパスワードを入力し、パスワードがコマンド履歴バッファに記録されないようにします。
old_passphrase	パスフレーズを変更する場合は、以前のパスフレーズを入力します。

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	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

使用上のガイドライン

マスター パスフレーズを使用する機能としては、次のものがあります。

- OSPF
- EIGRP
- VPN ロード バランシング
- VPN (リモート アクセスおよびサイトツーサイト)
- フェールオーバー

- AAA サーバ
- Logging
- 共有ライセンス

パスワードの暗号化をトリガーするには、**key config-key password-encrypt** コマンドと **password encryption aes** コマンドの両方を任意の順序で入力する必要があります。**write memory** と入力して、暗号化されたパスワードをスタートアップ コンフィギュレーションに保存します。そうしないと、スタートアップ コンフィギュレーション内のパスワードが表示されることがあります。マルチコンテキスト モードでは、システム実行スペースに **write memory all** を使用してすべてのコンテキストの設定を保存します。

このコマンドを実行できるのは、コンソール、SSH、HTTPS 経由の ASDM などによるセキュア セッションにおいてのみです。

暗号化されたパスワードがプレーン テキスト パスワードに変換されるため、**no key config-key password-encrypt** コマンドは注意して使用してください。パスワードの暗号化がサポートされていないソフトウェア バージョンにダウングレードするときは、このコマンドの **no** 形式を使用できる場合があります。

フェールオーバーがイネーブルであっても、フェールオーバー共有キーが設定されていない場合に、マスター パスフレーズを変更すると、エラー メッセージが表示されます。このメッセージには、マスター パスフレーズの変更がプレーン テキストとして送信されないよう、フェールオーバー共有キーを入力する必要があることが示されます。

アクティブ/スタンバイ フェールオーバーでパスワード暗号化をイネーブルにするか、または変更すると、**write standby** が実行され、アクティブな設定をスタンバイ ユニットに複製することになります。この複製がないと、スタンバイ ユニット上の暗号化されたパスワードが、同じパスフレーズを使用していても、異なるものになります。設定の複製によって設定が同じになることが保証されます。アクティブ/アクティブ フェールオーバーの場合は、**write standby** と手動で入力する必要があります。アクティブ/アクティブ モードでは、**write standby** によってトラフィックの中断が発生します。これは、新しい設定が同期される前に、セカンダリ ユニットで設定がクリアされるためです。**failover active group 1** コマンドと **failover active group 2** コマンドを使用してプライマリ ASA のすべてのコンテキストをアクティブにし、**write standby** と入力してから、**no failover active group 2** コマンドを使用してグループ 2 のコンテキストをセカンダリ ユニットに復元します。

write erase コマンドに続いて **reload** コマンドを使用すると、マスターパスフレーズを紛失した場合はそのマスターパスフレーズとすべての設定が削除されます。

例

次に、暗号キーの生成に使用するパスフレーズを設定し、パスワード暗号化をイネーブルにする例を示します。

```
ciscoasa(config)# key config-key password-encryption
    Old key: bumblebee
    New key: haverford
    Confirm key: haverford
ciscoasa(config)# password encryption aes
ciscoasahostname(config)# write memory
```

関連コマンド

コマンド	説明
password encryption aes	パスワードの暗号化をイネーブルにします。
write erase	**reload** コマンドを続いて使用すると、マスター パスフレーズが紛失された場合にパスフレーズを削除します。

key-hash

オンボードのセキュア コピー（SCP）クライアントのサーバのハッシュ SSH ホスト キーを手動で追加するには、サーバ コンフィギュレーション モードで **key-hash** コマンドを使用します。サーバ コンフィギュレーション モードにアクセスするには、先に **ssh pubkey-chain** コマンドを入力します。キーを削除するには、このコマンドの **no** 形式を使用します。

key-hash {**md5** | **sha256**} *fingerprint*

no key-hash {**md5** | **sha256**} *fingerprint*

構文の説明

fingerprint	ハッシュ キーを入力します。
{**md5** | **sha256**}	使用するハッシュのタイプ（MD5 または SHA-256）を設定します。ASA のコンフィギュレーションでは、常に SHA-256 が使用されます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.1(5)	このコマンドが追加されました。

使用上のガイドライン

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

各サーバについて、SSH ホストの **key-string**（公開キー）または **key-hash**（ハッシュ値）を指定できます。**key-hash** では、すでにハッシュされているキーを入力します（MD5 または SHA-256 を使用）。たとえば、**show** コマンドの出力からコピーしたキーなどを入力できます。

例

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

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

関連コマンド

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

keypair

証明する公開キーのキー ペアを指定するには、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 **keypair** 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。

keypair *name*

no keypair *name* **| [rsa modulus 1024|2048|4096|512|768] | [ecdsa elliptic-curve 256|384|521]**

構文の説明

ecdsa	CMP の手動登録と自動登録用の ECDSA キーを生成します。
name	CMP 以外の登録用のキー ペアの名前を指定します。
rsa	CMP の手動登録と自動登録用の RSA キーを生成します。

デフォルト

デフォルト設定では、キー ペアは含まれません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.7(1)	新しい EDCSA と RSA のキーペアが追加されました。

例

次に、central トラストポイントのクリプト CA トラストポイント コンフィギュレーション モードを開始し、central トラストポイント用に証明するキー ペアを指定する例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# keypair exchange
```

関連コマンド

コマンド	説明
crypto ca trustpoint	クリプト CA トラストポイント コンフィギュレーション モードを開始します。
crypto key generate dsa	DSA キーを生成します。
crypto key generate rsa	RSA キーを生成します。
default enrollment	登録パラメータをデフォルト値に戻します。

keysize

ユーザ証明書の登録で、ローカルの認証局（CA）サーバによって生成される公開キーと秘密キーのサイズを指定するには、CA サーバ コンフィギュレーション モードで **keysize** コマンドを使用します。キー サイズをデフォルトの 1024 ビットの長さ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。

keysize *size*

no keysize

構文の説明

size	キーのサイズ（ビット単位）。サイズは次のいずれかになります。 • 512 • 768 • 1024 • 2048 • 4096

デフォルト

デフォルトでは、このキー ペアの各キーの長さは 1024 ビットです。

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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

例

次に、ローカル CA サーバによってユーザ用に生成される、公開キーと秘密キーのすべてのキー ペアのキーのサイズを 2048 ビットに指定する例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server))# keysize 2048
ciscoasa(config-ca-server)#
```

次に、ローカル CA サーバによってユーザ用に生成される、公開キーと秘密キーのすべてのキーペアのキーのサイズを、デフォルトの 1024 ビットの長さにリセットする例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# no keysize
ciscoasa(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 モードのコマンド セットへのアクセスを提供し、ローカル CA の設定と管理ができるようにします。
issuer-name	認証局証明書のサブジェクト名 DN を指定します。
subject-name-default	CA サーバが発行するすべてのユーザ証明書でユーザ名とともに使用される汎用的なサブジェクト名 DN を指定します。

keysize server

ローカルの認証局(CA)サーバによって生成される公開キーと秘密キーのサイズを指定し、CA のキー ペアのサイズを設定するには、CA サーバ コンフィギュレーション モードで **keysize server** コマンドを使用します。キー サイズをデフォルトの 1024 ビットの長さ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。

keysize server *size*

no keysize server

構文の説明

size	キーのサイズ(ビット単位)。サイズは次のいずれかになります。 • 512 • 768 • 1024 • 2048 • 4096

デフォルト

デフォルトでは、このキー ペアの各キーの長さは 1024 ビットです。

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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

例

次に、CA 証明書のキー サイズを 2048 ビットに指定する例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server))# keysize server 2048
ciscoasa(config-ca-server)#
```

次に、CA 証明書のキー サイズをデフォルトの 1024 ビットにリセットする例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# no keysize server
ciscoasa(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 モードのコマンド セットへのアクセスを提供し、ローカル CA の設定と管理ができるようにします。
issuer-name	認証局証明書のサブジェクト名 DN を指定します。
keysize	ユーザ証明書のキー ペアのサイズを指定します。
subject-name-default	CA サーバが発行するすべてのユーザ証明書でユーザ名とともに使用される汎用的なサブジェクト名 DN を指定します。

key-string

オンボードのセキュア コピー(SCP)クライアントのサーバのパブリック SSH ホスト キーを手動で追加するには、サーバ コンフィギュレーション モードで **key-string** コマンドを使用します。サーバ コンフィギュレーション モードにアクセスするには、先に **ssh pubkey-chain** コマンドを入力します。このコマンドを入力すると、キー ストリングを入力するプロンプトが表示されます。ストリングがコンフィギュレーションに保存されると、SHA-256 を使用してハッシュされ、**key-hash** コマンドとして保存されます。したがって、ストリングを削除するときは、**no key-hash** コマンドを使用します。

key-string
key_string

構文の説明

key_string	公開キーを入力します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.1(5)	このコマンドが追加されました。

使用上のガイドライン

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

各サーバについて、SSH ホストの **key-string**(公開キー) または **key-hash**(ハッシュ値)を指定できます。*key_string* はリモート ピアの Base64 で符号化された RSA 公開キーです。オープン SSH クライアントから(言い換えると .ssh/id_rsa.pub ファイルから)公開キー値を取得できます。Base64 で符号化された公開キーを送信した後、SHA-256 によってそのキーがハッシュされます。

例

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

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

次に、保存されたハッシュ キーを表示する例を示します。

```
ciscoasa(config-ssh-pubkey-server)# show running-config ssh
ssh scopy enable
ssh stricthostkeycheck
ssh pubkey-chain
  server 10.7.8.9
    key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:
2e:19
```

関連コマンド

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

kill

Telnet セッションを終了するには、特権 EXEC モードで **kill** コマンドを使用します。

kill *telnet_id*

構文の説明

telnet_id	Telnet セッションの ID を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

kill コマンドを使用すると、Telnet セッションを終了できます。Telnet セッションの ID を表示するには、**who** コマンドを使用します。Telnet セッションを終了すると、ASA は、警告することなく、すべてのアクティブなコマンドを終了して接続をドロップします。

例

次に、ID「2」の Telnet セッションを終了する例を示します。最初に、アクティブな Telnet セッションのリストを表示するため、**who** コマンドを入力します。次に、ID「2」の Telnet セッションを終了するため、**kill 2** コマンドを入力します。

```
ciscoasa# who
2: From 10.10.54.0

ciscoasa# kill 2
```

関連コマンド

コマンド	説明
telnet	ASA への Telnet アクセスを設定します。
who	アクティブな Telnet セッションのリストを表示します。