CHAPTER 17

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 証明書と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

trustpoint	**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	透過	シングル	コンテキスト	システム
webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(2)	このコマンドが導入されました。

使用上のガイドライン

トラストポイントは、Certificate Authority（CA; 認証局）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。

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。次のコマンドは、mytrustpoint という新しいトラストポイントを作成します。

```
hostname(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.
hostname(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。

```
hostname(config)# webvpn
hostname(config)# java-trustpoint mytrustpoint
hostname(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	透過	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	•	•	—	•	—

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

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。

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

関連コマンド

コマンド	説明
context	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。

keepout

セキュリティ アプライアンスのメンテナンスまたはトラブルシューティングの実施時に、新しいユーザ セッションのログイン ページではなく、立ち入り禁止の Web ペ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。過去に設定し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** バージョンを使用します。

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	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
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスが使用できないことを通知するには、keepout コマンドを使用します。

例

次に、立ち入り禁止ページを設定する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# keepout "The system is unavailable until 7:00 a.m. EST."
hostname(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 SSLVPN 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 領域名では数字と大文字だけを使用します。セキュリティ アプライアンスでは、*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	透過	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	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このリリースで追加されました。

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、セキュリティ アプライアンスでは、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。

```
hostname(config)# aaa-server svrgrp1 protocol kerberos
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
hostname(config-aaa-server-host)# exit
hostname(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	透過	シングル	コンテキスト	システム
AAA サーバ ホスト	•	•	•	•	—

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

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 文字を超えて入力された文字があれば無視されます。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、セキュリティ アプライアンスを 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。

以前の PIX Firewall のバージョンで使用されていた **aaa-server** コマンドの **key** パラメータは、対応する **key** コマンドに自動的に変換されます。

例

次に、ホスト「1.2.3.4」上で「srvgrp1」という TACACS+ AAA サーバを設定し、タイムアウトを 9 秒に設定し、リトライ間隔を 7 秒に設定し、キーを「myexclusivemumblekey」として設定する例を示します。

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(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、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	AAA サーバのコンフィギュレーションを表示します。

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

構文の説明

name	キー ペアの名前を指定します。

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	透過	シングル	コンテキスト	システム
クリプト CA トラストポイント コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

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。

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

関連コマンド

コマンド	説明
crypto ca trustpoint	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 Certificate Authority（CA; 認証局）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 {**512** | **768** | **1024** | **2048**}

no keysize

構文の説明

512	証明書の登録で生成される公開キーと秘密キーのサイズを 512 ビットに指定します。
768	証明書の登録で生成される公開キーと秘密キーのサイズを 768 ビットに指定します。
1024	証明書の登録で生成される公開キーと秘密キーのサイズを 1024 ビットに指定します。
2048	証明書の登録で生成される公開キーと秘密キーのサイズを 2048 ビットに指定します。

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	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、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。

```
hostname(config)# crypto ca server
hostname(config-ca-server))# keysize 2048
hostname(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。

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

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
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 Certificate Authority（CA; 認証局）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 独自のキー 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 {**512** | **768** | **1024** | **2048**}

no keysize server

構文の説明

512	証明書の登録で生成される公開キーと秘密キーのサイズを 512 ビットに指定します。
768	証明書の登録で生成される公開キーと秘密キーのサイズを 768 ビットに指定します。
1024	証明書の登録で生成される公開キーと秘密キーのサイズを 1024 ビットに指定します。
2048	証明書の登録で生成される公開キーと秘密キーのサイズを 2048 ビットに指定します。

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	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、CA 独自の証明書のキー サイズに 2048 ビットを指定する例を示します。

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

次に、CA 独自の証明書のキー サイズを、デフォルトの 1024 ビットの長さにリセットする例を示します。

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

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
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。

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	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

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、セキュリティ アプライアンスは、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。

```
hostname# who
2: From 10.10.54.0

hostname# kill 2
```

関連コマンド

コマンド	説明
telnet	セキュリティ アプライアンスへの 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。