so ～ st

software authenticity development

開発キー署名付きイメージのロードをイネーブルまたはディセーブルにするには、パラメータ コンフィギュレーション モードで **software authenticity development** コマンドを使用します。パラメータ 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。このオプションは、一度イネーブルにすると、開発キー署名付きイメージのロードをディセーブルにするまで維持されます。

software authenticity development { **enable | disable** }

構文の説明

disable	開発キー署名付きイメージのロードをディセーブルにします。
enable	開発キー署名付きイメージのロードをイネーブルにします。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
パラメータ 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
9.3(2)	このコマンドが追加されました。

例

次に、開発キー署名付きシグニチャのロードをイネーブルにする例を示します。

```
ciscoasa(config)# software authenticity development enable
ciscoasa(config)# show software authenticity development
Loading of development images is enabled
ciscoasa(config)#
```

次に、開発キー署名付きイメージのロードをディセーブルにする例を示します。

```
ciscoasa(config)# software authenticity development disable
ciscoasa(config)# show software authenticity development
Loading of development images is disabled
ciscoasa(config)#
```

関連コマンド

コマンド	説明
show software authenticity keys	開発キーを表示します。
show software authenticity file disk0:asa932-1fbff.SSA	開発キー ファイルの内容を表示します。
show software authenticity running	現在実行中のファイルに関連したデジタル署名情報を表示します。
software authenticity key add special	SPI フラッシュに新しい開発キーを追加します。
software authenticity key revoke special	SPI フラッシュから古い開発キーを削除します。

software authenticity key add special

SPIフラッシュに新しい開発キーを追加するには、パラメータコンフィギュレーションモードで **software authenticity key add special** コマンドを使用します。パラメータ 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。

software authenticity key add special

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。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
パラメータ 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
9.3(2)	このコマンドが追加されました。

例

次に、SPI フラッシュに新しい開発キーを追加する例を示します。

```
ciscoasa(config)# software authenticity key add special
Writing the key to Primary...Success
Writing the key to Backup...Success
Done!
The following example shows what happens if you try to add a new development image to
SPR flash and one already exists:
ciscoasa(config)# software authenticity key add special
Duplicate key found in Primary...Skipping key write
Duplicate key found in Backup...Skipping key write
Done!
```

関連コマンド

コマンド	説明
software authenticity key revoke special	SPI フラッシュから古い開発キーを削除します。
show software authenticity keys	SPI フラッシュの開発キーを表示します。

コマンド	説明
show software authenticity file disk0:asa932-1fbff.SSA	開発キー ファイルの内容を表示します。
show software authenticity running	現在実行中のファイルに関連したデジタル署名情報を表示します。

software authenticity key revoke special

SPIフラッシュから古い開発キーを削除するには、パラメータ コンフィギュレーション モードで **software authenticity key revoke special** コマンドを使用します。パラメータ 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。

software authenticity key revoke special

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。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
パラメータ 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
9.3(2)	このコマンドが追加されました。

例

次に、SPI フラッシュから開発キーを削除する例を示します。

```
ciscoasa(config)# software authenticity key revoke special
Revoking the key with version A...Success
Revoking the key with version A...Success
Done!
```

関連コマンド

コマンド	説明
software authenticity key add special	SPI フラッシュに新しい開発キーを追加します。
show software authenticity keys	SPI フラッシュの開発キーを表示します。
show software authenticity file disk0:asa932-1fbff.SSA	開発キー ファイルの内容を表示します。

コマンド	説明
show software authenticity running	現在実行中のファイルに関連したデジタル署名情報を表示します。

software-version

サーバーまたはエンドポイントのソフトウェアバージョンを表示するサーバーおよびユーザーエージェント ヘッダー フィールドを識別するには、パラメータ コンフィギュレーション モードで **software-version** コマンドを使用します。パラメータ 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。この機能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。

software-version action { **mask | log** } [**log**]

no software-version action { **mask | log** } [**log**]

構文の説明

log	違反が発生した場合、スタンドアロンまたは追加のログを記録することを指定します。
mask	SIP メッセージ内のソフトウェア バージョンをマスクします。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
パラメータ 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
7.2(1)	このコマンドが追加されました。

例

次に、SIP インスペクション ポリシー マップでソフトウェア バージョンを識別する例を示します。

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# software-version action log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。

コマンド	説明
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシーマップ コンフィギュレーションをすべて表示します。

source-interface

VXLAN VTEP インターフェイスの送信元インターフェイス名を指定するには、nve コンフィギュレーション モードで **source-interface** コマンドを使用します。インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

source-interface*interface_name*
no source-interface *interface_name*

構文の説明

interface_name	VTEP送信元インターフェイス名を設定します。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
Nve 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
9.4(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

VTEP送信元インターフェイスは、すべてのVNIインターフェイスに関連付けられる予定の標準の ASA インターフェイス（物理、冗長、EtherChannel、または VLAN）です。ASA/セキュリティ コンテキストごとに 1 つの VTEP 送信元インターフェイスを設定できます。

VTEP 送信元インターフェイスは、VXLAN トラフィック専用にすることができますが、その使用に制限されません。必要に応じて、インターフェイスを通常のトラフィックに使用し、そのトラフィックのインターフェイスにセキュリティポリシーを適用できます。ただし、VXLAN トラフィックの場合は、すべてのセキュリティ ポリシーを VNI インターフェイスに適用する必要があります。VTEP インターフェイスは、物理ポートとしてのみ機能します。

トランスペアレントファイアウォールモードでは、VTEP送信元インターフェイスは、BVIの一部ではないため、そのIPアドレスを設定しません。このインターフェイスは、管理インターフェイスが処理される方法に似ています。

（注） 送信元インターフェイスの MTU が 1554 バイト未満の場合、ASA は自動的に MTU を 1554 バイトに増やします。

例

次に、GigabitEthernet 1/1 インターフェイスを VTEP 送信元インターフェイスとして設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# nve 1
ciscoasa(cfg-nve)# source-interface outside
ciscoasa(cfg-nve)# default-mcast-group 236.0.0.100
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
default-mcast-group	VTEP 送信元インターフェイスに関連付けられているすべての VNI インターフェイスのデフォルトのマルチキャスト グループを指定します。
encapsulation vxlan	NVE インスタンスを VXLAN カプセル化に設定します。
inspect vxlan	標準 VXLAN ヘッダー形式に強制的に準拠させます。
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
mcast-group	VNI インターフェイスのマルチキャスト グループ アドレスを設定します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
nve-only	VXLAN送信元インターフェイスがNVE専用であることを指定します。
peer ip	ピア VTEP の IP アドレスを手動で指定します。
segment-id	VNI インターフェイスの VXLAN セグメント ID を指定します。
show arp vtep-mapping	リモート セグメント ドメインにある IP アドレスとリモート VTEP IP アドレス用の VNI インターフェイスにキャッシュされた MAC アドレスを表示します。
show interface vni	VNIインターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス（設定されている場合）のステータス、ならびに関連付けられている NVE インターフェイスを表示します。

コマンド	説明
show mac-address-table vtep-mapping	リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ2転送テーブル（MACアドレステーブル）を表示します。
show nve	NVEインターフェイスのパラメータ、ステータス、および統計情報とキャリアインターフェイス（送信元インターフェイス）のステータス、このNVEをVXLAN VTEPとして使用するVNI、ならびにこのNVEインターフェイスに関連付けられているピアVTEP IPアドレスを表示します。
show vni vlan-mapping	VNIセグメントIDと、VLANインターフェイスまたはトランスペアレントモードの物理インターフェイス間のマッピングを表示します。
source-interface	VTEP送信元インターフェイスを指定します。
vtep-nve	VNIインターフェイスをVTEP送信元インターフェイスに関連付けます。
vxlan port	VXLAN UDPポートを設定します。デフォルトでは、VTEP送信元インターフェイスはUDPポート4789へのVXLANトラフィックを受け入れます。

speed

インターフェイスの速度を設定するには、インターフェイス コンフィギュレーション モードで **speed** コマンドを使用します。速度設定をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

speed { *speed* | **auto** | **nonegotiate** | **sfp-detect** }
no speed [*speed* | **auto** | **nonegotiate** | **sfp-detect**]

構文の説明

auto	速度を自動検出します。RJ-45 のみ。
nonegotiate	SFP インターフェイス（Cisco Secure Firewall 3100 を除く）の場合、**no speed nonegotiate** を指定すると速度が 1000 Mbps に設定され、フロー制御パラメータとリモート障害情報のリンクネゴシエーションが有効になります。10 Gbps インターフェイスの場合、このオプションを指定すると速度が 1,000 Mbps に設定されます。**nonegotiate** キーワードは、SFP インターフェイスで使用できる唯一のキーワードです。**speed nonegotiate** コマンドは、リンク ネゴシエーションをディセーブルにします。 Cisco Secure Firewall 3100 については、**negotiate-auto** コマンドを参照してください。
speed	速度を特定の設定に設定します。
sfp-detect	（Cisco Secure Firewall 3100 のみ）インストールされている SFP モジュールの速度を検出し、適切な速度を使用します。デュプレックスは常に全二重で、自動ネゴシエーションは常に有効です。このオプションは、後でネットワークモジュールを別のモデルに変更し、速度を自動的に更新する場合に便利です。この設定は、デフォルトです。

コマンド デフォルト

RJ-45 インターフェイスの場合、デフォルトは **speed auto** です。

SFP インターフェイス（Cisco Secure Firewall 3100 を除く）の場合、デフォルトは **no speed nonegotiate** です。

Cisco Secure Firewall 3100 の場合、デフォルトは **sfp-detect** 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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
インターフェイス 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)	このコマンドは、**interface** コマンドのキーワードからインターフェイス コンフィギュレーション モードのコマンドに変更されました。
9.14(1)	Firepower 1000 および 2100 の 1GB ファイバインターフェイスで、**speed nonegotiate** コマンドを使用して速度の自動ネゴシエーションを無効にできるようになりました。
9.17(1)	Cisco Secure Firewall 3100 に sfp-detect キーワードが追加されました。

使用上のガイドライン

速度は物理インターフェイスだけで設定します。

ネットワークで自動検出がサポートされていない場合は、速度を特定の値に設定します。

ASA 5500 シリーズの RJ-45 インターフェイスでは、デフォルトのオートネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX を有効にするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションが無効にされ、Auto-MDI/MDIX も無効になります。

PoE ポートで速度を **auto** 以外に設定する場合（可能な場合）、IEEE 802.3af をサポートしない Cisco IP Phone およびシスコ ワイヤレス アクセス ポイントは検出されず、電力は供給されません。

（注） ファイバインターフェイス搭載の ASA 5500-X または ASA 5585-X に対して **speed** コマンドを設定しないでください。設定すると、リンク障害が発生します。

例

次に、速度を 1000BASE-T に設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# speed 1000
ciscoasa(config-if)# duplex full
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

関連コマンド

コマンド	説明
clear configure interface	インターフェイスのコンフィギュレーションをすべてクリアします。

コマンド	説明
duplex	デュプレックス モードを設定します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。
show running-config interface	インターフェイス コンフィギュレーションを表示します。

spf-interval

最短パス優先（SPF）計算の IS-IS スロットリングをカスタマイズするには、ルータ isis コンフィギュレーション モードで **spf-interval** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

spf-interval ［ **level-1 | level-2** ］ *spf-max-wait* ［ *spf-initial-wait spf-second-wait* ］
no spf-interval ［ **level-1 | level-2** ］ *spf-max-wait* ［ *spf-initial-wait spf-second-wait* ］

構文の説明

level-1	（任意）レベル 1 エリアだけに間隔を適用します。
level-2	（任意）レベル 2 エリアだけに間隔を適用します。
spf-max-wait	連続する 2 つの SPF 計算の最大間隔（秒単位）を示します。指定できる範囲は 1 ～ 120 秒です。デフォルトは 10 秒です。
spf-initial-wait	（任意）トポロジが変更された後の初期 SPF 計算遅延（ミリ秒単位）を示します。有効な範囲は 1 ～ 120000 ミリ秒です。デフォルトは 5500 ミリ秒（5.5 秒）、
spf-second-wait	（任意）最初と 2 番目の SPF 計算の間のホールド タイム（ミリ秒単位）を示します。有効な範囲は 1 ～ 120000 ミリ秒です。デフォルトは 5500 ミリ秒（5.5 秒）、

コマンド デフォルト

spf-max-wait：10 秒

spf-initial-wait：5500 ミリ秒

spf-second-wait：5500 ミリ秒

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ isis 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
9.6(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

SPF計算が実行されるのは、トポロジが変更されたときだけです。外部ルートが変更された場合は実行されません。

spf-intervalコマンドは、ソフトウェアがSPF計算を実行する頻度を制御します。SPF計算は、プロセッサに高い負荷を与えます。そのため、特にエリアが広くトポロジが頻繁に変わる場合には、計算を実行する頻度を制限することが有効です。SPF間隔を大きくすると、ルータのプロセッサ負荷が軽減されますが、コンバージェンスの速度が低下する可能性があります。

次の説明を参照して、このコマンドのデフォルト値を変更するかどうか決定する際の参考にしてください。

- *spf-initial-wait* 引数は、トポロジが変更されてから最初の SPF 計算までの初期の待機時間（ミリ秒単位）を示します。
- *spf-second-wait* 引数は、最初と 2 番目の SPF 計算の間の間隔（ミリ秒単位）を示します。
- 後続の各待機間隔は、指定された *spf-max-wait* 間隔に達するまで、前の待機間隔の 2 倍の長さになります。SPF 計算は、最初と 2 番目の間隔の後にスロットルされるか、スローダウンします。*spf-max-wait* 間隔に達すると、待機間隔はネットワークが安定するまでこの間隔に維持されます。
- ネットワークが安定して、 *spf-max-wait* 間隔の 2 倍の時間内にトリガーがない場合は、高速動作（初期の待機時間）に戻ります。

SPFスロットリングはダンプニングメカニズムではありません。つまり、SPFスロットリングはSPF計算を阻止せず、ルート、インターフェイス、またはルータをダウンとしてマークしません。SPF スロットリングは、SPF 計算の間の間隔を単に長くするに過ぎません。

例

次に、SPF計算、部分的なルート計算（PRC）、およびリンクステートパケット（LSP）生成の間隔を設定する例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# spf-interval 5 10 20
ciscoasa(config-router)# prc-interval 5 10 20
ciscoasa(config-router)# lsp-gen-interval 2 50 100
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルなIS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。

コマンド	説明
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。

コマンド	説明
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。

コマンド	説明
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

split-dns

スプリットトンネルを介して解決されるドメインのリストを入力するには、グループポリシー コンフィギュレーション モードで **split-dns** コマンドを使用します。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。

スプリット トンネリング ドメインのリストをすべて削除するには、**no split-dns** コマンドを引数なしで使用します。これにより、**split-dns none** コマンドを発行して作成されたヌルリストを含め、設定されているスプリット トンネリング ドメインのリストはすべて削除されます。

スプリット トンネリング ドメインのリストがない場合、ユーザーはデフォルトのグループ ポリシー内に存在するリストを継承します。このようなスプリット トンネリング ドメインのリストをユーザーが継承しないようにするには、**split-dns none** コマンドを使用します。

split-dns { **value** *domain-name1 domain-name2 domain-nameN* **| none** }
no split-dns [*domain-name1 domain-name2 domain-nameN*]

構文の説明

value *domain-name*	スプリットトンネルを介して ASA が解決するドメイン名を指定します。
none	スプリット DNS リストがないことを指定します。スプリット DNS リストをヌル値で設定して、スプリット DNS リストを拒否します。デフォルトのグループ ポリシーまたは指定したグループ ポリシーのスプリット DNS リストを継承しません。

コマンド デフォルト

スプリット DNS はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー 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
7.0(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

ドメインのリスト内の各エントリを区切るには、単一のスペースを使用します。エントリ数に制限はありませんが、ストリング全体の長さは492文字以下にします。英数字、ハイフン（-）、およびピリオド（.）のみを使用できます。

no split-dns コマンドを引数なしで使用すると、**split-dns none** コマンドを発行して作成したヌル値を含め、現在のネットワークリストはすべて削除されます。

バージョン3.0.4235以降、セキュアクライアントはWindowsプラットフォーム向けのトゥルースプリット DNS 機能をサポートしています。

例

次に、FirstGroup という名前のグループ ポリシーに対してスプリット トンネリングを介して解決されるドメイン Domain1、Domain2、Domain3、および Domain4 を設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# split-dns value Domain1 Domain2 Domain3 Domain4
```

関連コマンド

コマンド	説明
default-domain	ドメイン フィールドが除かれた DNS クエリーに IPSec クライアントが使用するデフォルト ドメイン名を指定します。
split-dns	スプリット トンネルを介して解決されるドメインのリストを提供します。
split-tunnel-network-list	トンネリングが必要なネットワークを区別するために、ASA が使用するアクセスリストを指定します。
split-tunnel-policy	IPsec クライアントが、条件に応じてパケットを暗号化形式で IPsec トンネルを経由して転送したり、クリアテキスト形式でネットワーク インターフェイスに転送したりできるようにします。

split-horizon

EIGRP スプリットホライズンを再度イネーブルにするには、インターフェイス コンフィギュレーション モードで **split-horizon** コマンドを使用します。EIGRP スプリットホライズン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。

split-horizon eigrp *as-number*
no split-horizon eigrp *as-number*

構文の説明

as-number	EIGRP ルーティング プロセスの自律システム番号です。

コマンド デフォルト

split-horizon コマンドはイネーブルになります。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
インターフェイス 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
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードはサポートされます。

使用上のガイドライン

X.25 パケットスイッチド ネットワーク上のリンクを含むネットワークでは、**neighbor** コマンドを使用してスプリットホライズン機能を無効にすることができます。代わりに、コンフィギュレーションで **no split-horizon eigrp** コマンドを明示的に指定することもできます。ただし、その場合、そのネットワーク上の関連するマルチキャスト グループ内のすべてのルータおよびアクセス サーバーに対して、同様にスプリット ホライズンをディセーブルにする必要があります。

通常、スプリットホライズンのデフォルトの状態は、ルートを適切にアドバタイズするために変更することがアプリケーションにおいて必要となる場合を除き、変更しないことを推奨します。シリアルインターフェイスでスプリットホライズンがディセーブルであり、そのインターフェイスがパケットスイッチドネットワークに接続されている場合、そのネットワーク上の関

連するマルチキャスト グループ内のすべてのルータおよびアクセス サーバーに対して、スプリット ホライズンをディセーブルにする必要があります。

例

次に、インターフェイス Ethernet0/0 で EIGRP スプリット ホライズンをディセーブルにする例を示します。

```
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# no split-horizon eigrp 100
```

関連コマンド

コマンド	説明
router eigrp	EIGRP ルーティング プロセスを作成し、このプロセスのコンフィギュレーション モードを開始します。

split-tunnel-all-dns

セキュアクライアントがVPNトンネルを経由するすべてのDNSアドレスを解決できるようにするには、グループ ポリシー コンフィギュレーション モードでsplit-tunnel-all-dnsコマンドを使用します。

実行コンフィギュレーションからこのコマンドを削除するには、このコマンドのno形式を使用します。これにより、別のグループ ポリシーの値を継承できます。

split-tunnel-all-dns { **disable | enable** }
no split-tunnel-all-dns [{ **disable | enable** }]

構文の説明

disable (default)	セキュアクライアントは、スプリットトンネルポリシー（すべてのネットワークをトンネリング、ネットワークリストで指定されたネットワークをトンネリング、またはネットワークリストで指定されたネットワークを除外）に従ってトンネル経由でDNSクエリを送信します。
enable	セキュアクライアントは、VPNトンネルを経由するすべてのDNSアドレスを解決します。

コマンド デフォルト

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

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー 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
8.2(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

split-tunnel-all-dns enableコマンドは、SSLプロトコルまたはIPsec/IKEv2プロトコルを使用するVPN接続に適用され、セキュアクライアントに対してVPNトンネルを経由するすべてのDNSアドレスを解決するように指示します。DNS解決に失敗すると、アドレスは未解決のまま残ります。セキュアクライアントは、パブリックDNSサーバー経由でアドレスの解決を試行しません。

デフォルトでは、この機能はディセーブルになっています。クライアントは、スプリット トンネル ポリシーに従ってトンネル経由でDNS クエリーを送信します。ポリシーは、すべてのネットワークをトンネリング、ネットワーク リストで指定されたネットワークをトンネリング、またはネットワーク リストで指定されたネットワークを除外です。

例

次に、セキュアクライアント が VPN トンネルを経由するすべての DNS クエリを解決できるように ASA を設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# split-tunnel-all-dns enable
```

関連コマンド

コマンド	説明
default-domain	ドメイン フィールドが省略された DNS クエリーに対してレガシー IPsec（IKEv1）VPN クライアントまたは AnyConnect VPN Client（SSL）が使用するデフォルトのドメイン名を指定します。
split-dns	スプリット トンネルを介して解決されるドメインのリストを提供します。
split-tunnel-network-list	トンネリングが必要なネットワークと不要なネットワークを区別するために、ASA が使用するアクセスリストを指定します。
split-tunnel-policy	レガシー VPN クライアント（IPsec/IKEv1）または AnyConnect VPN クライアント（SSL）が、条件に応じてパケットを暗号化形式でトンネルを経由して転送したり、クリア テキスト形式でネットワーク インターフェイスに転送したりできるようにします。

split-tunnel-network-list

スプリットトンネリングのネットワークリストを作成するには、グループ ポリシー コンフィギュレーション モードで **split-tunnel-network-list** コマンドを使用します。ネットワーク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。

split-tunnel-network-list { **value** *access-list name* | **none** }
no split-tunnel-network-list value [*access-list name*]

構文の説明

none	スプリットトンネリングのネットワークリストがないことを指定します。ASA によって、すべてのトラフィックがトンネリングされます。 スプリット トンネリング ネットワーク リストをヌル値で設定して、スプリット トンネリングを拒否します。デフォルトのグループ ポリシーまたは指定したグループ ポリシーのデフォルトのスプリット トンネリング ネットワーク リストを継承しません。
value *access-list name*	トンネリングするネットワークまたはトンネリングしないネットワークを列挙するアクセス リストを指定します。

コマンド デフォルト

デフォルトでは、スプリット トンネリング ネットワーク リストはありません。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー 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
7.0(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

ASA では、ネットワークリストに基づいてスプリットトンネリングの判断が行われます。ネットワークリストは、プライベートネットワーク上のアドレスのリストで構成される標準 ACL です。スプリット トンネリング ネットワーク リストによって、トラフィックがトンネルを通過する必要があるネットワークと、トンネリングを必要としないネットワークが区別されます。

スプリット トンネリング ネットワーク リストがない場合、ユーザーはデフォルトのグループ ポリシーまたは指定したグループ ポリシー内に存在するネットワーク リストを継承します。このようなネットワークリストをユーザーが継承しないようにするには、**split-tunnel-network-list none** コマンドを使用します。

スプリット トンネリング ネットワーク リストをすべて削除するには、**no split-tunnel-network-list** コマンドを引数なしで使用します。これにより、**split-tunnel-network-list none** コマンドを発行して作成されたヌルリストを含め、設定されているネットワークリストはすべて削除されます。

（注） バージョン 9.7(1) 以降、最大 1200 のスプリットネットワークを指定できます。それ以前のリリースでは、制限は 200 ネットワークです。

例

次に、FirstGroup という名前のグループ ポリシーに対して FirstList という名前のネットワーク リストを設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# split-tunnel-network-list value FirstList
```

関連コマンド

コマンド	説明
access-list	アクセス リストを作成するか、ダウンロード可能なアクセス リストを使用します。
default-domain	ドメイン フィールドが除かれた DNS クエリーに IPSec クライアントが使用するデフォルト ドメイン名を指定します。
split-dns	スプリット トンネルを介して解決されるドメインのリストを提供します。
split-tunnel-policy	IPSec クライアントが、条件に応じてパケットを暗号化形式で IPSec トンネルを経由して転送したり、クリアテキスト形式でネットワーク インターフェイスに転送したりできるようにします。

split-tunnel-policy

スプリット トンネリング ポリシーを設定するには、グループ ポリシー コンフィギュレーション モードで **split-tunnel-policy** コマンドを使用します。実行コンフィギュレーションから split-tunnel-policy 属性を削除するには、このコマンドの **no** 形式を使用します。

split-tunnel-policy { **tunnelall | tunnelspecified | excludespecified** }
no split-tunnel-policy

構文の説明

excludespecified	トラフィックを暗号化しないで送信する先となるネットワークのリストを定義します。この機能は、社内ネットワークにトンネルを介して接続しながら、ローカル ネットワーク上のデバイス（プリンタなど）にアクセスするリモート ユーザーにとって役立ちます。このオプションは、セキュアクライアント でのみ機能します。
split-tunnel-policy	トラフィックのトンネリングのルールを設定することを指定します。
tunnelall	トラフィックを暗号化しないで送信しないこと、または ASA 以外の宛先に送信しないことを指定します。リモート ユーザーは企業ネットワークを経由してインターネットにアクセスしますが、ローカル ネットワークにはアクセスできません。
tunnelspecified	指定したネットワークから、または指定したネットワークへのすべてのトラフィックをトンネリングします。このオプションによって、スプリットトンネリングが有効になります。トンネリングするアドレスのネットワーク リストを作成できるようになります。その他のすべてのアドレスへのデータは暗号化しないで送信され、リモート ユーザーのインターネット サービス プロバイダーによってルーティングされます。

コマンド デフォルト

スプリットトンネリングは、デフォルト（**tunnelall**）ではディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー 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
7.0(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

スプリット トンネリングは、本来は、セキュリティ機能ではなくトラフィック管理機能です。最適なセキュリティを確保するには、スプリット トンネリングをイネーブルにしないことを推奨します。

これにより、別のグループ ポリシーのスプリット トンネリングの値を継承できます。

スプリット トンネリングを使用すると、リモート アクセス VPN クライアントが、条件に応じて、パケットを暗号化形式で IPsec トンネルまたは SSL トンネルを経由して転送したり、クリアテキスト形式でネットワーク インターフェイスに転送したりできるようになります。スプリット トンネリングをイネーブルにすると、宛先が IPSec または SSL VPN トンネル エンドポイントの反対側ではないパケットでは、暗号化、トンネルを介した送信、復号化、および最終的な宛先へのルーティングは必要なくなります。

例

次に、FirstGroup という名前のグループ ポリシーに対して、指定したネットワークのみをトンネリングするスプリット トンネリング ポリシーを設定する例を示します。

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 split-tunnel-policy tunnelspecified
```

関連コマンド

コマンド	説明
default-domain	ドメイン フィールドが除かれた DNS クエリーに IPSec クライアントが使用するデフォルト ドメイン名を指定します。
split-dns	スプリット トンネルを介して解決されるドメインのリストを提供します。
split-tunnel-network-list none	スプリット トンネリングのアクセス リストがないことを指定します。トラフィックはすべてトンネルを通過します。
split-tunnel-network-list value	トンネリングが必要なネットワークと不要なネットワークを区別するために、ASA が使用するアクセスリストを指定します。

spoof-server

HTTP プロトコルインスペクションのために、サーバーヘッダーフィールドをストリングに置き換えるには、パラメータ コンフィギュレーション モードで **spoof-server** コマンドを使用します。この機能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。

spoof-server*string*
no spoof-server *string*

構文の説明

string サーバー ヘッダー フィールドを置き換えるストリング。最大 82 文字です。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
パラメータ 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
7.2(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

WebVPN ストリームは spoof-server コマンドの対象になりません。

例

次に、HTTP インスペクション ポリシー マップでサーバー ヘッダー フィールドをあるストリングに置き換える例を示します。

```
ciscoasa(config-pmap-p)# spoof-server
string
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。

コマンド	説明
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

sq-period

NAC フレームワークセッションで正常に完了したポスチャ検証と、ホストポスチャの変化を調べる次回のクエリーとの間隔を指定するには、nac ポリシー nac フレームワーク コンフィギュレーション モードで **sq-period** コマンドを使用します。このコマンドを NAC ポリシーから削除するには、このコマンドの **no** 形式を使用します。

sq-period *seconds*
no sq-period [*seconds*]

構文の説明

seconds	正常に完了した各ポスチャ確認の間隔の秒数。指定できる範囲は 30 ～ 1800 です。

コマンド デフォルト

デフォルト値は 300 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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
nac ポリシー nac フレームワーク 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
7.3(0)	コマンド名から「nac-」が削除されました。コマンドが、グループ ポリシー コンフィギュレーション モードから nac ポリシー nac フレームワーク コンフィギュレーション モードに移動されました。
7.2(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

ASA では、正常に実行された各ポスチャ検証とステータスクエリー応答の後に、ステータスクエリータイマーを起動します。このタイマーが切れると、ホストポスチャの変化を調べるクエリー（ステータスクエリーと呼ばれる）がトリガーされます。

例

次に、ステータス クエリー タイマーの値を 1800 秒に変更する例を示します。

```
ciscoasa(config-nac-policy-nac-framework)# sq-period 1800
ciscoasa(config-nac-policy-nac-framework)
```

次に、NAC フレームワーク ポリシーからステータス クエリー タイマーを削除する例を示します。

```
ciscoasa(config-nac-policy-nac-framework)# no sq-period
ciscoasa(config-nac-policy-nac-framework)
```

関連コマンド

コマンド	説明
nac-policy	Cisco NAC ポリシーを作成してアクセスし、そのタイプを指定します。
nac-settings	NAC ポリシーをグループ ポリシーに割り当てます。
eou timeout	NAC フレームワーク コンフィギュレーションで EAP over UDP メッセージをリモート ホストに送信した後に待機する秒数を変更します。
reval-period	NACフレームワークセッションでの成功したポスチャ確認の間隔を指定します。
debug eap	NAC フレームワーク メッセージのデバッグのための拡張認証プロトコル イベントのロギングをイネーブルにします。

srv-id

参照 ID オブジェクトに URI ID を設定するには、ca-reference-identity モードで **uri-id** コマンドを使用します。URI ID を削除するには、このコマンドの **no** 形式を使用します。最初に、**crypto ca reference-identity** コマンドを入力して参照 ID オブジェクトを設定することで、*ca-reference-identity* モードにアクセスできます。

srv-id*value*
no srv-id *value*

構文の説明

value 各参照 ID の値。

srv-id RFC 4985 に定義されている SRVName 形式の名前をもつ、otherName タイプの subjectAltName エントリ。SRV-ID 識別子には、ドメイン名とアプリケーション サービス タイプの両方を含めることができます。たとえば、「_imaps.example.net」の SRV-ID は、DNS ドメイン名部分の「example.net」と、アプリケーション サービス タイプ部分の「imaps」に分けられます。

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。

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

コマンド履歴

リリース	変更内容
9.6(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

参照 ID が作成されると、4 つの ID タイプと関連付けられた値を参照 ID に追加、または参照 ID から削除することができます。

参照 ID には、DNS ドメイン名を特定する情報が含まれている必要があります。また、アプリケーション サービスを特定する情報も含めることができます。

例

次に、syslog サーバーの参照 ID を作成する例を示します。

```
ciscoasa(config)# crypto ca reference-identity syslogServer
```

```
ciscoasa(config-ca-ref-identity)# dns-id syslog1-bxb.cisco.com
ciscoasa(config-ca-ref-identity)# cn-id syslog1-bxb.cisco.com
```

関連コマンド

コマンド	説明
crypto ca reference-identity	参照 ID オブジェクトを設定します。
cn-id	参照 ID オブジェクトのコモン ネーム ID を設定します。
dns-id	参照 ID オブジェクトの DNS ドメイン名 ID を設定します。
uri-id	参照 ID オブジェクトの URI ID を設定します。
logging host	セキュアな接続のために参照 ID オブジェクトを使用できるロギング サーバーを設定します。
call-home profile destination address http	安全な接続のために参照 ID オブジェクトを使用できる Smart Call Home サーバーを設定します。

ss7 variant

M3UAインスペクション用にネットワーク内で使用されているSS7バリエーションを特定するには、パラメータ コンフィギュレーション モードで **ss7 variant** コマンドを使用します。パラメータ コンフィギュレーション モードにアクセスするには、まず **policy-map type inspect m3ua** コマンドを入力します。デフォルトの SS7 バリエーションに戻すには、このコマンドの **no** 形式を使用します。

ss7 variant { **ITU | ANSI | Japan | China** }
no ss7 variant { **ITU | ANSI | Japan | China** }

構文の説明

ITU	ITU のバリエーション。これはデフォルトです。
ANSI	ANSI のバリエーション。
Japan	日本のバリエーション。
China	中国のバリエーション。

コマンド デフォルト

デフォルトは、ITU SS7 バリエーションです。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
パラメータ 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
9.6(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

このコマンドを使用して、ネットワーク内で使用されているSS7バリエーションを特定できます。オプションを設定して、M3UAポリシーを導入した後は、最初にポリシーを削除しないかぎり、ポリシーを変更することはできません。

バリエーションによって、M3UA メッセージで使用されるポイント コードの形式が決まります。

- ITU：ポイント コードは 14 ビットで 3-8-3 形式です。値の範囲は、[0-7]-[0-255]-[0-7] です。これは、デフォルトの SS7 バリエーションです。
- ANSI：ポイント コードは 24 ビットで 8-8-8 形式です。値の範囲は、[0-255]-[0-255]-[0-255] です。
- Japan：ポイント コードは 16 ビットで 5-4-7 形式です。値の範囲は、[0-31]-[0-15]-[0-127] です。
- China：ポイント コードは 24 ビットで 8-8-8 形式です。値の範囲は、[0-255]-[0-255]-[0-255] です。

例

次に、SS7 バリエーションを ITU に設定する例を示します。

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# ss7 variant ITU
```

関連コマンド

コマンド	説明
inspect m3ua	M3UA インスペクションをイネーブルにします。
match dpc	M3UA 宛先ポイント コードと一致させます。
match opc	M3UA 発信ポイント コードと一致させます。
policy-map type inspect	インスペクション ポリシー マップを作成します。

ssh

ASA に SSH アクセスを追加するには、グローバル コンフィギュレーション モードで **ssh** コマンドを使用します。ASA への SSH アクセス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。

ssh { *ip_address mask* | *ipv6_address/prefix* } *interface*
no ssh { *ip_address mask* | *ipv6_address/prefix* } *interface*

構文の説明

interface	SSH をイネーブルにする ASA インターフェイス。名前付きインターフェイスを指定します。ブリッジ グループの場合、ブリッジ グループ メンバ インターフェイスを指定します。VPN 管理アクセスのみ（**management-access** コマンドを参照）の場合、名前付き BVI インターフェイスを指定します。
ip_address	ASA への SSH 接続を開始することを認可されるホストまたはネットワークの IPv4 アドレス。
ipv6_address/prefix	ASA への SSH 接続を開始することを認可されるホストまたはネットワークの IPv6 アドレスとプレフィックス。
mask	*ip_address* のネットワーク マスク。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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
7.0(1)	このコマンドが追加されました。

リリース	変更内容
8.4(2)	**pix** または **asa** ユーザー名とログインパスワードで SSH を使用して ASA に接続することができなくなりました。SSH を使用するには、**aaa authentication ssh console LOCAL** コマンド（CLI）または **Configuration > Device Management > Users/AAA > AAA Access > Authentication**（ASDM）を使用して AAA 認証を設定し、**username** コマンド（CLI）を入力するか **Configuration > Device Management > Users/AAA > User Accounts**（ASDM）を選択してローカルユーザーを定義する必要があります。ローカル データベースの代わりに AAA サーバーを認証に使用する場合、ローカル認証もバックアップの手段として設定しておくことをお勧めします。
8.4(4.1)、9.1(2)	**ssh authentication** コマンドを使用すると、ユーザー単位で、ASA への SSH 接続の公開キー認証を有効にすることができます。
9.1(2)	ASA での SSH サーバーの実装が、AES-CTR モードの暗号化をサポートするようになりました。
9.1(7)/9.4(3)/9.5(3)/9.6(1)	**ssh cipher encryption** コマンドおよび **ssh cipher integrity** コマンドを使用して、SSH アクセスの暗号化と整合性の方式を設定できます。
9.6(2)	**ssh authentication** には **aaa authentication ssh console LOCAL** コマンドが必要です。バージョン 9.6(2) 以降では、パスワードを定義せずに **username** を作成できるため、公開キー認証のみが必要となります。
9.7(1)	直接接続された SSH 管理ステーションがある場合、ASA およびホストの /31 サブネットを使用してポイントツーポイント接続を作成できます。
9.6(3)/9.8(1)	SSH 公開キー認証を使用するユーザーの認証とパスワードを使用するユーザーの認証を区別します。AAA SSH 認証（**aaa authentication ssh console)**）を明示的にイネーブルにする必要がなくなりました。ユーザーに **ssh authentication** コマンドを設定すると、このタイプの認証を使用するユーザーのローカル認証がデフォルトでイネーブルになります。さらに、明示的に AAA SSH 認証を設定すると、パスワードを持つユーザー名のみにこの認証が適用されます。また、AAA サーバータイプを使用できます。
9.9(2)	仮想インターフェイスが指定可能になりました。

使用上のガイドライン

ssh *ip_address* コマンドでは、ASA への SSH 接続を開始することを認可されるホストまたはネットワークを指定します。複数の **ssh** コマンドをコンフィギュレーションに含めることができます。

ASA への SSH の使用を開始する前に、**crypto key generate rsa** コマンドを使用してデフォルトの RSA キーを生成する必要があります。

また、ASA インターフェイスに SSH アクセスの目的でアクセスするために、ホスト IP アドレスを許可するアクセス ルールは必要ありません。このセクションの手順に従って、SSH アクセスを設定する必要があるだけです。

ASA への通過ルートとなるインターフェイス以外のインターフェイスへの SSH アクセスはサポートされません。たとえば、SSH ホストが外部インターフェイスにある場合、外部インターフェイスへの直接管理接続のみ開始できます。このルールの例外は、VPN 接続を介した場合のみです（**management-access** コマンドを参照）。

ASA は、コンテキスト/単一のモードあたり最大 5 つの同時 SSH 接続と、すべてのコンテキストにまたがり分散された最大 100 の接続を許容します。

ASA は SSH バージョン 2 で提供されている SSH リモート シェル機能をサポートし、DES 暗号方式および 3DES 暗号方式をサポートします。

次の SSH バージョン 2 機能は、ASA でサポートされていません。

- X11 転送。
- ポート フォワーディング。
- SFTP サポート。
- Kerberos と AFS のチケット引き渡し
- データ圧縮

ユーザー名およびパスワードとともに SSH を使用するには、 **aaa authentication ssh console LOCAL** コマンドを使用して AAA 認証を設定し、**username** コマンドを入力してローカルユーザーを定義する必要があります。ローカル データベースの代わりに AAA サーバーを認証に使用する場合、ローカル認証もバックアップの手段として設定しておくことをお勧めします。

ローカル **username** および公開キー認証とともに SSH を使用するには、**ssh authentication** コマンドを設定します。ローカル データベースのみがサポートされます。

バージョン 9.6(2) および 9.7(1) では、**ssh authentication** には **aaa authentication ssh console LOCAL** コマンドが必要です。バージョン 9.6(2) 以降では、パスワードを定義せずに **username** を作成できるため、公開キー認証のみが必要となります。

（注） パスワードとともにユーザー名を作成する必要を回避するために、**username** コマンドの **nopassword** オプションを使用しないでください。**nopassword** オプションでは任意のパスワードを入力できます。「パスワードなし」ではありません。**aaa** コマンドを設定する場合、**nopassword** オプションによってセキュリティ問題が生じます。

9.6(1) 以前および 9.6(3)/9.8(1) 以降では、 **aaa authentication ssh console LOCAL** コマンドを設定する必要はありません。このコマンドは、パスワードを持つユーザーのみに適用されます。また、LOCAL だけでなく、任意のサーバータイプを指定できます。たとえば、一部のユーザーはローカル データベースを使用して公開キー認証を使用し、他のユーザーは RADIUS でパス

ワードを使用できます。**aaa authentication ssh console LOCAL** コマンドを設定すると、**username** パスワードと秘密キーのうちのどちらをログインに使用するかを選択できます。

例

次の例は、RSA キーを生成し、アドレスが 192.168.1.2 の内部インターフェイス上のホストで ASA にアクセスする方法を示しています。

```
ciscoasa(config)# crypto key generate rsa modulus 1024
ciscoasa(config)# write memory
ciscoasa(config)# aaa authentication ssh console LOCAL

WARNING: local database is empty! Use 'username' command to define local users.
ciscoasa(config)# username exampleuser1 password examplepassword1 privilege 15
ciscoasa(config)# ssh 192.168.1.2 255.255.255.255 inside
ciscoasa(config)# ssh timeout 30
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドをクリアします。
crypto key generate rsa	アイデンティティ証明書用の RSA キー ペアを生成します。
debug ssh	SSH コマンドのデバッグ情報とエラー メッセージを表示します。
show running-config ssh	実行コンフィギュレーションの現在の SSH コマンドを表示します。
ssh scopy enable	ASA でセキュアコピーサーバーをイネーブルにします。
ssh version	SSH バージョン 1 と SSH バージョン 2 のいずれかを使用するよう、ASA を制限します。

ssh authentication

SSH公開キー認証をユーザー単位で有効にするには、ユーザー名属性モードで **ssh authentication** コマンドを使用します。公開キー認証をユーザー単位で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。

ssh authentication { **pkf | publickey** [**nointeractive**] *key* [**hashed**] }
no ssh authentication { **pkf | publickey** [**nointeractive**] *key* [**hashed**] }

構文の説明

hashed	**show running-config username** コマンドを使用して ASA 上でキーを表示した場合、キーは、SHA-256 ハッシュを使用して暗号化されます。キーを **pkf** として入力した場合でも、ASA はキーをハッシュし、ハッシュ化された **publickey** として表示します。 **show** の出力からキーをコピーする必要がある場合、 **hashed** キーワードを使って、 **publickey** タイプを指定します。
キー	key 引数の値は次のいずれかになります。 • key 引数が指定され、ハッシュされたタグが指定されていない場合、キーの値は、ssh-rsa、ecdsa-sha2-nistp、または ssh-ed25519 の未処理キーを生成することのできる SSH キー生成ソフトウェアによって生成される Base 64 で符号化された公開キーである必要があります（つまり、証明書は使用しません）。Base 64 エンコード公開キーを送信すると、そのキーは SHA-256 によりハッシュ化され、それ以降のすべての比較では対応する 32 バイト ハッシュが使用されます。 • key 引数が指定され、ハッシュされたタグを指定した場合は、キーの値は、SHA-256 で事前にハッシュされている必要があります。長さは 32 バイトで、各バイトはコロンで区切られている必要があります（解析のため）。
nointeractive	**nointeractive** オプションは、SSH 公開キーファイル形式のキーをインポートするときにすべてのプロンプトを抑制します。この非インタラクティブ データ入力モードは ASDM での使用のみを目的としています。

pkf	**pkf** キーの場合、PKF でフォーマットされたキーを最大 4096 ビット貼り付けるよう求められます。Base64 形式では大きすぎてインラインで貼り付けることができないキーにはこのフォーマットを使用します。たとえば、ssh keygen を使って 4096 ビットのキーを生成してから PKF に変換し、そのキーに対して **pkf** キーワードが求められるようにすることができます。 （注） フェールオーバーで **pkf** オプションを使用できますが、PKF キーは、スタンバイシステムに自動的に複製されません。PKF キーを同期するには、 **write standby** コマンドを入力する必要があります。
publickey	**publickey** の場合、*key* は Base64 でエンコードされた公開キーです。SSH-RSA raw キー（証明書なし）を生成可能な任意の SSH キー生成ソフトウェア（ssh keygen など）を使用して、キーを生成できます。

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。

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

コマンド履歴

リリース	変更内容
8.4(4.1)、9.1(2)	このコマンドが追加されました。 この機能は、*8.5*（*1*）、*8.6*（*1*）、*8.7*（*1*）、*9.0*（*1*）、*9.0(2)*、*9.1(1)* では、利用できません。
9.1(2)	**pkf** キーワードと最大 4096 ビットのキーのサポートが追加されました。
9.6(2)	**ssh authentication** には **aaa authentication ssh console LOCAL** コマンドが必要です。バージョン 9.6(2) 以降では、パスワードを定義せずに **username** を作成できるため、公開キー認証のみが必要となります。

リリース	変更内容
9.6(3)/9.8(1)	SSH公開キー認証を使用するユーザーの認証とパスワードを使用するユーザーの認証を区別します。AAA SSH 認証（**aaa authentication ssh console)**）を明示的にイネーブルにする必要がなくなりました。ユーザーに **ssh authentication** コマンドを設定すると、このタイプの認証を使用するユーザーのローカル認証がデフォルトでイネーブルになります。さらに、明示的にAAA SSH 認証を設定すると、パスワードを持つユーザー名のみにこの認証が適用されます。また、AAA サーバー タイプを使用できます。
9.16(1)	EdDSA および ECDSA キーのサポートが追加されました。

使用上のガイドライン

ローカル **username** の場合、パスワード認証の代わりに公開キー認証を有効にすることができます。ssh-rsa、ecdsa-sha2-nistp、または ssh-ed25519 raw キー（証明書なし）を生成可能な任意の SSH キー生成ソフトウェア（ssh keygen など）を使用して、公開キー/秘密キーのペアを生成できます。Y **ssh authentication** コマンドを使用して、ASA で公開キーを入力します。その後、SSHクライアントは秘密キー（およびキーペアを作成するために使用したパスフレーズ）を使用して ASA に接続します。

ローカル データベースのみがサポートされます。

設定を保存すると、ハッシュされたキー値はコンフィギュレーションに保存され、ASA のリブート時に使用されます。

バージョン 9.6(2) および 9.7(1) では、 **ssh authentication** には **aaa authentication ssh console LOCAL** コマンドが必要です。バージョン 9.6(2) 以降では、パスワードを定義せずに **username** を作成できるため、公開キー認証のみが必要となります。

（注） パスワードとともにユーザー名を作成する必要を回避するために、 **username** コマンドの **nopassword** オプションを使用しないでください。 **nopassword** オプションでは任意のパスワードを入力できます。「パスワードなし」ではありません。 **aaa** コマンドを設定する場合、 **nopassword** オプションによってセキュリティ問題が生じます。

9.6(1) 以前および 9.6(3)/9.8(1) 以降では、 **aaa authentication ssh console LOCAL** コマンドを設定する必要はありません。このコマンドは、パスワードを持つユーザーのみに適用されます。また、LOCALだけでなく、任意のサーバータイプを指定できます。たとえば、一部のユーザーはローカル データベースを使用して公開キー認証を使用し、他のユーザーは RADIUS でパスワードを使用できます。 **aaa authentication ssh console LOCAL** コマンドを設定すると、 **username** パスワードと秘密キーのうちのどちらをログインに使用するかを選択できます。

例

次に、PKF 形式のキーを使用して認証する例を示します。

```
ciscoasa(config)# crypto key generate eddsa edwards-curve ed25519
```

```
ciscoasa(config)# write memory
ciscoasa(config)# username deanwinchester password examplepassword1 privilege 15
ciscoasa(config)# username deanwinchester attributes
ciscoasa(config-username)# ssh authentication pkf
Enter an SSH public key formatted file.
End with the word "quit" on a line by itself:
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "256-bit ED25519, converted by dean@dwinchester-mac from "
AAAAC3NzaC1lZDI1NTE5AAAAIDmIeTNfEOnuH0094p1MKX80fW2O216g4trnf7gwWe5Q
---- END SSH2 PUBLIC KEY ----
quit
INFO: Import of an SSH public key formatted file SUCCEEDED.
ciscoasa(config-username)# aaa authentication ssh console LOCAL
ciscoasa(config)# ssh 192.168.1.2 255.255.255.255 inside
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドをクリアします。
debug ssh	SSH コマンドのデバッグ情報とエラー メッセージを表示します。
show running-config ssh	実行コンフィギュレーションの現在の SSH コマンドを表示します。
ssh version	SSH バージョン 1 と SSH バージョン 2 のいずれかを使用するよう、ASA を制限します。

ssh cipher encryption

SSHアクセスの設定時に、暗号化および整合性のアルゴリズムを選択できます。SSH暗号の暗号化アルゴリズムを綿密に制御するには、グローバル コンフィギュレーション モードで **ssh cipher encryption** コマンドを使用します。アルゴリズムの特定のセットに対応する定義済みのレベルを利用できます。また、複数のアルゴリズムをコロンで区切って指定することで、カスタム リストを定義できます。デフォルトに戻す場合は、このコマンドの **no** 形式を使用します。

ssh cipher encryption { **all | fips | high | low | medium | custom** *encryption_1* [**:** *encryption_2* [**:** *...encryption_n*]] }
no ssh cipher encryption { **all | fips | high | low | medium | custom** *encryption_1* [**:** *encryption_2* [**:** *...encryption_n*]] }

構文の説明

all	すべての暗号化アルゴリズムを受け入れるように指定します。
custom *encryption_1* [**:** *encryption_2* [**:** *... encryption_n*]]	暗号化アルゴリズムのカスタム セットを指定します。 **show ssh ciphers** コマンドを入力すると、使用可能なすべての暗号化アルゴリズムを表示できます。次に例を示します。 **custom 3des-cbc:aes192-cbc:aes256-ctr**
fips	FIPS 準拠の暗号化アルゴリズムのみを指定します。
high	高強度の暗号化アルゴリズムのみを指定します。
low	低、中、および高強度の暗号化アルゴリズムを指定します。
medium	中および高強度の暗号化アルゴリズムを指定します。

コマンド デフォルト

medium がデフォルトです。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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
9.1(7)/9.4(3)/9.5(3)/9.6(1)	このコマンドが追加されました。
9.16(1)	**chacha20-poly1305@openssh.com** および **aes128-gcm@openssh.com** アルゴリズムが追加されました。

使用上のガイドライン

このコマンドは、 **ssh cipher integrity** コマンドと一緒に使用されます。暗号化アルゴリズムについては、次の値を指定できます。

- all：3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes128-gcm@openssh.com chacha20-poly1305@openssh.com aes192-ctr aes256-ctr
- fips：aes128-cbc aes256-cbc aes128-gcm@openssh.com
- high：aes256-cbc aes128-gcm@openssh.com chacha20-poly1305@openssh.com aes256-ctr
- low：3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr
- medium：3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr

（注） FIPS モードが有効な場合は、FIPS 暗号化および整合性アルゴリズムのみが許可されます。

オプションで、アルゴリズムの一部を選択解除できます。FIPSモードが有効な場合、現在設定されているアルゴリズムと FIPS 準拠のアルゴリズムの共通部分が計算されます。NULL 以外の場合に、結果の構成が使用されます。NULL の場合は、デフォルトの FIPS 準拠のアルゴリズムが使用されます。

セキュア コピーのパフォーマンスは、使用する暗号化アルゴリズムにある程度依存します。medium の暗号セットを選択した場合、ASA は 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr の順にアルゴリズムをネゴシエートします。提示された最初のアルゴリズム（3des-cbc）が選択された場合、aes128-cbc などの一層効率的なアルゴリズムが選択された場合よりも大幅にパフォーマンスが低下します。提示された暗号方式に変更するには、 **ssh cipher encryption** コマンドを使用します（例： **ssh cipher encryption custom aes128-cbc** ）。

例

次に、いくつかのカスタム SSH 暗号化アルゴリズムの構成の例を示します。

```
ciscoasa(config)# ssh cipher encryption custom 3des-cbc:aes128-cbc:aes192-cbc
```

関連コマンド

コマンド	説明
show ssh	設定されている暗号方式を表示します。
show ssh ciphers	使用可能な暗号アルゴリズムを表示します。
ssh cipher integrity	設定されている SSH暗号の整合性アルゴリズムを指定します。

ssh cipher integrity

SSHアクセスの設定時に、暗号化および整合性方式のモードを選択できます。SSH暗号の整合性アルゴリズムを綿密に制御するには、グローバルコンフィギュレーションモードで**ssh cipher integrity**コマンドを使用します。アルゴリズムの特定のセットに対応する定義済みのレベルを利用できます。また、コロンで区切って複数のアルゴリズムを指定して、カスタムリストを定義できます。デフォルトに戻す場合は、このコマンドの **no** 形式を使用します。

ssh cipher integrity { **all | fips | high | low | medium | custom** *algorithm_1* [**:** *algorithm_2* [**:** *...algorithm_n*]] }
no ssh cipher integrity { **all | fips | high | low | medium | custom** *algorithm_1* [**:** *algorithm_2* [**:** *...algorithm_n*]] }

構文の説明

all	すべての整合性アルゴリズムを受け入れるように指定します。
custom *algorithm_1*[**:***algorithm_2*[**:***...algorithm_n*]]	整合性アルゴリズムのカスタムセットを指定します。**show ssh ciphers** コマンドを入力すると、使用可能なすべての整合性アルゴリズムを表示できます。次に例を示します。 **custom hmac-sha1:hmac-sha1-96:hmac-md5-96**
fips	FIPS 準拠の整合性アルゴリズムを指定します。
high	高強度の整合性アルゴリズムのみを指定します。
low	低、中、および高強度の整合性アルゴリズムを指定します。
medium	中および高強度の整合性アルゴリズムを指定します。

コマンド デフォルト

（9.12 以降）High がデフォルトです。

（9.10 以前）Medium がデフォルトです。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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
9.1(7)/9.4(3)/9.5(3)/9.6(1)	このコマンドが追加されました。
9.12(1)	HMAC-SHA256整合性暗号のサポートが追加されました。デフォルトは、高セキュリティの暗号セット（hmac-sha1およびhmac-sha2-256）になりました。以前のデフォルトは中程度のセットでした。
9.13(1)	次の整合性アルゴリズムの値は、安全ではないと見なされ、廃止されます。 • all：hmac-sha1-96、hmac-md5、hmac-md5-96、hmac-sha2-256 • low：hmac-sha1-96、hmac-md5、hmac-md5-96、hmac-sha2-256 • medium：hmac-sha1-96 上記の値は、以降のリリースから削除されます。

使用上のガイドライン

このコマンドは、**ssh cipher encryption** コマンドと一緒に使用されます。整合性アルゴリズムについては、次の値を指定できます。

- all：hmac-sha1、hmac-sha1-96 (廃止)、hmac-md5 (廃止)、hmac-md5-96 (廃止)、hmac-sha2-256 (廃止)
- fips：hmac-sha1, hmac-sha2-256
- high：hmac-sha1, hmac-sha2-256
- low：hmac-sha1、hmac-sha1-96 (廃止)、hmac-md5 (廃止)、hmac-md5-96 (廃止)、hmac-sha2-256 (廃止)
- medium：hmac-sha1、hmac-sha1-96 (廃止)、hmac-md5、hmac-md5-96、hmac-sha2-256

（注） FIPS モードが有効な場合は、FIPS 暗号化および整合性アルゴリズムのみが許可されます。

オプションで、アルゴリズムの一部を選択解除できます。FIPSモードが有効な場合、現在設定されているアルゴリズムと FIPS 準拠のアルゴリズムの共通部分が計算されます。NULL 以外の場合に、結果の構成が使用されます。NULL の場合は、デフォルトの FIPS 準拠のアルゴリズムが使用されます。

例

次に、いくつかのカスタム SSH 整合性アルゴリズムの構成の例を示します。

```
ciscoasa(config)# ssh cipher integrity custom hmac-sha1-96:hmac-md5
```

関連コマンド

コマンド	説明
show ssh	設定されている暗号方式を表示します。
show ssh ciphers	使用可能な暗号アルゴリズムを表示します。
ssh cipher encryption	設定されているSSH暗号の暗号化アルゴリズムを指定します。

ssh disconnect

アクティブな SSH セッションを切断するには、特権 EXEC モードで **ssh disconnect** コマンドを使用します。

ssh disconnect *session_id*

構文の説明

session_id	ID 番号で指定した SSH セッションを切断します。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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

セッション ID を指定する必要があります。切断する SSH セッションの ID を取得するには、**show ssh sessions** コマンドを使用します。

例

次に、切断される SSH セッションの例を示します。

```
ciscoasa# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.39    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
2   172.69.39.29    1.99    IN   3des-cbc   sha1     SessionStarted  pat
                            OUT  3des-cbc   sha1     SessionStarted  pat
ciscoasa# ssh disconnect 2
ciscoasa# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.29    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
```

関連コマンド

コマンド	説明
show ssh sessions	ASA とのアクティブ SSH セッションに関する情報を表示します。
ssh timeout	アイドル状態の SSH セッションのタイムアウト値を設定します。

ssh key-exchange group

SSH キー交換方式を設定するには、グローバル コンフィギュレーション モードで **ssh key-exchange group** コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を使用します。

ssh key-exchange group { **curve25519-sha256** | **dh-group14-sha1** | **dh-group14-sha256** | **ecdh-sha2-nistp256** }
no ssh key-exchange group

構文の説明

curve25519-sha256	キー交換に Elliptic Curve 25519 SHA256 を使用します。
dh-group14-sha1	キー交換に Diffie-Hellman グループ 14 SHA1 を使用します。
dh-group14-sha256	（任意）キー交換に Diffie-Hellman グループ 14 SHA256 を使用します。
ecdh-sha2-nistp256	キー交換に Elliptic Curve Diffie-Hellman（ECDH）SHA2 NIST P-256 を使用します。

コマンド デフォルト

（9.12 以降）デフォルトでは、 **dh-group14-sha256** が使用されます。

（9.10 以前）デフォルトでは、 **dh-group1-sha1** が使用されます。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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 （管理コンテキストのみ）	—

コマンド履歴

リリース	変更内容
9.16(1)	**curve25519-sha256** および **ecdh-sha2-nistp256** オプションが追加されました。
9.13(1)	**dh-group1-sha1** オプションは廃止され、今後のリリースでは削除される予定です。
9.12(2)	SSH キー交換モードの設定は、マルチコンテキストモードでは管理コンテキストに限定されています。

リリース	変更内容
9.12(1)	**dh-group14-sha256** オプションが追加され、これがデフォルトになりました。
8.4(4.1)、9.1(2)	このコマンドが追加されました。 この機能は、*8.5*（*1*）、*8.6*（*1*）、*8.7*（*1*）、*9.0*（*1*）、*9.0(2)*、*9.1(1)* では、利用できません。

使用上のガイドライン

Diffie-Hellman（DH）のようなキー交換は、いずれかの当事者単独では決定できない共有秘密を提供します。キー交換を署名およびホストキーと組み合わせることで、ホスト認証が実現します。このキー交換方式により、明示的なサーバ認証が可能となります。DH キー交換の使用方法の詳細については、RFC 4253 を参照してください。

管理コンテキストでは SSH キー交換を設定する必要があります。この設定は、他のすべてのコンテキストによって継承されます。

例

次に、DH グループ 14 SHA1 のキー交換方式を使用してキーを交換する例を示します。

```
ciscoasa(config)# ssh key-exchange group dh-group-14-sha1
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドをクリアします。
crypto key generate rsa	アイデンティティ証明書用の RSA キー ペアを生成します。
debug ssh	SSH コマンドのデバッグ情報とエラー メッセージを表示します。
show running-config ssh	実行コンフィギュレーションの現在の SSH コマンドを表示します。
ssh scopy enable	ASA でセキュアコピーサーバーをイネーブルにします。
ssh version	SSH バージョン 1 と SSH バージョン 2 のいずれかを使用するよう、ASA を制限します。

ssh key-exchange hostkey

デフォルトのキー順序（EdDSA、ECDSA、RSA）を使用しない場合は、グローバル コンフィギュレーション モードで **ssh key-exchange hostkey** コマンドを使用して、使用するキーペアを指定します。デフォルトに戻す場合は、このコマンドの **no** 形式を使用します。

ssh key-exchange hostkey { **rsa** | **ecdsa** | **eddsa** }
no ssh key-exchange hostname

構文の説明

ecdsa	ECDSA キーのみを使用します。
eddsa	EdDSA キーのみを使用します。
rsa	RSA キーのみを使用します。2048 以上のキーサイズを使用する必要があります。RSA キーのサポートは将来のリリースで削除される予定であるため、代わりに、サポートされている他のキータイプを使用することをお勧めします。

コマンド デフォルト

デフォルトでは、このコマンドは無効になっており、キーは EdDSA、ECDSA、RSA の順に試みられます。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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 （管理コンテキストのみ）	—

コマンド履歴

リリース	変更内容
9.16(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

SSH は EdDSA、ECDSA、RSA の順にキーを試みます。**show crypto key mypubkey** {**eddsa** | **ecdsa** | **rsa**} コマンドを使用してキーを表示します。SSH によって使用されるキーは<Default-*type*-Key>と呼ばれます。**ssh key-exchange hostkey rsa** コマンドでキーの順序を上書きする場合は、2048 以上のキーサイズを使用する必要があります。アップグレードの互換性のために、これより小さいキーは、デフォルトのキー順序を使用する場合にのみサポートされます。RSA キーのサポートは将来のリリースで削除される予定であるため、代わりに、サポートされている他のキータイプを使用することをお勧めします。

例

次の例では、EdDSA キーのみを強制的に使用します。

```
ciscoasa(config)# ssh key-exchange hostkey eddsa
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドをクリアします。
crypto key generate rsa	アイデンティティ証明書用の RSA キー ペアを生成します。
debug ssh	SSH コマンドのデバッグ情報とエラー メッセージを表示します。
show running-config ssh	実行コンフィギュレーションの現在の SSH コマンドを表示します。
ssh key-exchange group	SSH キー交換方式を設定します。
ssh scopy enable	ASA でセキュアコピーサーバーをイネーブルにします。

ssh pubkey-chain

オンボードのセキュアコピー（SCP）クライアントのSSHサーバーおよびそのキーをASAデータベースに対して手動で追加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 **ssh pubkey-chain** コマンドを使用します。すべてのホスト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。単一のサーバーキーだけを削除するには、**server** コマンドを参照してください。

ssh pubkey-chain
no ssh pubkey-chain

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。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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
9.1(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 サーバーの 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ーとそのキーを追加または削除できます。

サーバーごとに（**server** コマンドを参照）、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。

例

次に、10.86.94.170 にあるサーバー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
```

次に、10.7.8.9 にあるサーバーのホスト 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
```

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。
server	SSH サーバーとホストキーを ASA データベースに追加します。
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。

ssh scopy enable

ASA でセキュアコピー（SCP）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 **ssh scopy enable** コマンドを使用します。SCP 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。

ssh scopy enable
no ssh scopy enable

構文の説明

このコマンドには引数またはキーワードはありません。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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
7.0(1)	このコマンドが追加されました。
9.1(7)/9.4(3)/9.5(3)/9.6(1)	**ssh cipher encryption** コマンドおよび **ssh cipher integrity** コマンドを使用して、SSH アクセスの暗号化と整合性の方式を設定できます。

使用上のガイドライン

SCPはサーバーのみの実装です。SCPのための接続を受け入れて終了できますが、開始することはできません。ASA には次の制約事項があります。

- SCP のこの実装にはディレクトリサポートはないため、ASA の内部ファイルへのリモート クライアント アクセスは制限されます。
- SCP の使用時はバナー サポートはありません。
- SCP ではワイルドカードはサポートされません。
- SSH バージョン 2 接続をサポートするには、ASA のライセンスに VPN-3DES-AES 機能が必要です。

ファイル転送を開始する前に、ASAでは使用可能なフラッシュメモリをチェックします。使用可能なスペースが十分ではない場合、ASA は SCP 接続を終了します。フラッシュメモリ内の

ファイルを上書きする場合でも、ASAにコピーされるファイル用に十分な空きスペースが必要です。SCPプロセスでは、ファイルはまず一時ファイルにコピーされ、置き換えられるファイルに一時ファイルがコピーされます。コピーされるファイルと上書きされるファイルを保持する十分なスペースがフラッシュ内にない場合、ASA は SCP 接続を終了します。

セキュアコピーのパフォーマンスは、使用する暗号化アルゴリズムにある程度依存します。デフォルトで、ASA は 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr の順にアルゴリズムをネゴシエートします。提示された最初のアルゴリズム（3des-cbc）が選択された場合、aes128-cbc などの一層効率的なアルゴリズムが選択された場合よりも大幅にパフォーマンスが低下します。提示された暗号方式に変更するには、**ssh cipher encryption** コマンドを使用します（例：**ssh cipher encryption custom aes128-cbc**）。

例

次の例に、IP アドレスが 10.1.1.1 の管理コンソールからの SSH バージョン 2 接続を受け入れるよう内部インターフェイスを設定する方法を示します。アイドルセッションのタイムアウトは 60 秒に設定され、SCP がイネーブルにされています。

```
ciscoasa(config)# ssh 10.1.1.1 255.255.255.0 inside
ciscoasa(config)# ssh version 2
ciscoasa(config)# ssh scopy enable
ciscoasa(config)# ssh timeout 60
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドをクリアします。
debug ssh	SSH コマンドのデバッグ情報とエラー メッセージを表示します。
show running-config ssh	実行コンフィギュレーションの現在の SSH コマンドを表示します。
ssh	指定したクライアントまたはネットワークから ASA への SSH 接続を許可します。
ssh version	SSH バージョン 1 と SSH バージョン 2 のいずれかを使用するよう、ASA を制限します。

ssh stack ciscossh

CiscoSSH スタックを使用するには、グローバル コンフィギュレーション モードで **ssh stack ciscossh** コマンドを使用します。独自の ASA SSH スタックを使用するには、このコマンドの **no** 形式を使用します。

ssh stack ciscossh
no ssh stack ciscossh

コマンド デフォルト

CiscoSSH スタックはデフォルトで有効になっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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
9.17(1)	このコマンドが追加されました。
9.19(1)	このコマンドは、デフォルトでイネーブルになりました。

使用上のガイドライン

ASA は、SSH 接続用に 2 つの SSH スタック（独自の SSH スタックまたは CiscoSSH スタック）をサポートします。CiscoSSH は OpenSSH をベースとしています。Cisco SSH は次をサポートします。

- FIPS の準拠性
- シスコおよびオープンソースコミュニティからの更新を含む定期的な更新

CiscoSSH スタックは次をサポートしないことに注意してください。

- VPN を介した別のインターフェイスへの SSH（管理アクセス）
- EdDSA キーペア
- FIPS モードの RSA キーペア

これらの機能が必要な場合は、ASA SSH スタックを使用する必要があります。

CiscoSSH スタックでは、SCP 機能に若干の変更があります。ASA **copy** コマンドを使用して SCP サーバとの間でファイルをコピーするには、**ssh** コマンドを使用して、ASA で SCP サーバ サブネット/ホストの SSH アクセスを有効にする必要があります。

例

次に、CiscoSSH スタックを無効にする方法の例を示します。

```
ciscoasa(config)# no ssh stack ciscossh
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドをクリアします。
debug ssh	SSH コマンドのデバッグ情報とエラー メッセージを表示します。
show running-config ssh	実行コンフィギュレーションの現在の SSH コマンドを表示します。
ssh	指定したクライアントまたはネットワークから ASA への SSH 接続を許可します。

ssh stricthostkeycheck

オンボードのセキュアコピー（SCP）クライアントに対するSSHホストキーチェック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 **ssh stricthostkeycheck** コマンドを使用します。ホストキーチェック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。

ssh stricthostkeycheck
no ssh stricthostkeycheck

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。

コマンド デフォルト

このコマンドはデフォルトでイネーブルになります。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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
9.1(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。このオプションがイネーブルになっている場合、ASA にまだ格納されていないホストキーを許可または拒否するように求められます。このオプションがディセーブルになっている場合、ASA は過去に保存されたことがないホストキーを自動的に許可します。

例

次に、SSH ホスト キー チェックをイネーブルにする例を示します。

```
ciscoasa# ssh stricthostkeycheck
ciscoasa# copy x scp://cisco@10.86.95.9/x
The authenticity of host '10.86.95.9 (10.86.95.9)' can't be established.
RSA key fingerprint is dc:2e:b3:e4:e1:b7:21:eb:24:e9:37:81:cf:bb:c3:2a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.86.95.9' (RSA) to the list of known hosts.
Source filename [x]?
Address or name of remote host [10.86.95.9]?
Destination username [cisco]?
```

```
Destination password []? cisco123
Destination filename [x]?
```

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。
server	SSH サーバーとホストキーを ASA データベースに追加します。
ssh pubkey-chain	ASA のデータベースに格納されるサーバーとそのキーを手動で追加または削除します。

ssh timeout

デフォルトの SSH セッション アイドル タイムアウト値を変更するには、グローバル コンフィギュレーション モードで **ssh timeout** コマンドを使用します。デフォルトのタイムアウト値に戻すには、このコマンドの **no** 形式を使用します。

ssh timeout *number*
no ssh timeout

構文の説明

number SSH セッションが切断される前に非アクティブである時間を分単位で指定します。有効な値は、1 ～ 60 分です。

コマンド デフォルト

デフォルトのセッション タイムアウト値は、5 分です。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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
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

ssh timeout コマンドでは、セッションが切断される前にアイドルである時間を分単位で指定します。デフォルトの時間は、5 分です。

例

次に、IP アドレス 10.1.1.1 の管理コンソールからの SSH バージョン 2 接続のみを受け入れるように、内部インターフェイスを設定する例を示します。アイドル セッションのタイムアウトは 60 秒に設定され、SCP がイネーブルにされています。

```
ciscoasa(config)# ssh 10.1.1.1 255.255.255.0 inside
ciscoasa(config)# ssh version 2
ciscoasa(config)# ssh copy enable
ciscoasa(config)# ssh timeout 60
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドをクリアします。
show running-config ssh	実行コンフィギュレーションの現在の SSH コマンドを表示します。
show ssh sessions	ASA とのアクティブ SSH セッションに関する情報を表示します。
ssh disconnect	アクティブな SSH セッションを切断します。

ssh version（廃止）

ASA が受け入れる SSH のバージョンを制限するには、グローバル コンフィギュレーション モードで **ssh version** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。バージョン 2 のみがサポートされます。

ssh version 2
no ssh version 2

構文の説明

2	SSH バージョン 2 接続のみがサポートされることを指定します。

コマンド デフォルト

バージョン 2 がデフォルトです。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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
7.0(1)	このコマンドが追加されました。
9.9(1)	バージョン **1** が廃止されました。**1** キーワードは将来のリリースで削除される予定です。デフォルト設定も **ssh version 1 2** から **ssh version 2** のみに変更されました。
9.16(1)	このコマンドは削除されました。

使用上のガイドライン

SSH バージョンは バージョン 2 にのみ設定する必要があります。

例

次の例に、IP アドレスが 10.1.1.1 の管理コンソールからの SSH バージョン 2 接続を受け入れるよう内部インターフェイスを設定する方法を示します。アイドル セッションのタイムアウトは 60 秒に設定され、SCP がイネーブルにされています。

```
ciscoasa(config)# ssh 10.1.1.1 255.255.255.0 inside
ciscoasa(config)# ssh version 2
ciscoasa(config)# ssh copy enable
ciscoasa(config)# ssh timeout 60
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドをクリアします。
debug ssh	SSH コマンドのデバッグ情報とエラー メッセージを表示します。
show running-config ssh	実行コンフィギュレーションの現在の SSH コマンドを表示します。
ssh	指定したクライアントまたはネットワークから ASA への SSH 接続を許可します。

ssl certificate-authentication

8.2(1) よりも前のバージョンに対する下位互換性のためにクライアント証明書の認証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 **ssl certificate-authentication** コマンドを使用します。ssl 証明書の認証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。

ssl certificate-authentication [**fca-timeout** *timeout-in minutes*] **interface** *interface-name* **port** *port-number*
no ssl certificate-authentication [**fca-timeout** *timeout-in minutes*] **interface** *interface-name* **port** *port-number*

構文の説明

fca-timeout	強制証明書認証タイムアウト値（分単位）。
interface-name	選択したインターフェイスの名前。inside、management、outside などです。
port-number	TCP ポート番号。1 ～ 65535 の範囲の整数です。

コマンド デフォルト

この機能はデフォルトで無効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。

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

コマンド履歴

リリース	変更内容
8.0(3)	このコマンドが追加されました。
8.2(1)	このコマンドは不要になりましたが、以前のバージョンにダウングレードする場合に備えて、ASA で保持されています。

使用上のガイドライン

このコマンドにより、廃止された **http authentication-certificate** コマンドが置き換えられました。

例

次に、SSL 証明書認証機能を使用するように ASA を設定する例を示します。

```
ciscoasa
(config)#
 ssl certificate-authentication interface inside port 330
```

関連コマンド

コマンド	説明
show running-config ssl	現在設定されている一連のSSLコマンドを表示します。

ssl cipher

SSL、DTLS、TLS の各プロトコル用の暗号化アルゴリズムを指定するには、グローバル コンフィギュレーション モードで **ssl cipher** コマンドを使用します。デフォルト（暗号化アルゴリズムの完全なセット）に戻すには、このコマンドの **no** 形式を使用します。

ssl cipher *version* [*level* | **custom** *"string"*]
no ssl cipher *version* [*level* | **custom** *"string"*]

構文の説明

custom 文字列	OpenSSL 暗号定義文字列を使用して暗号スイートの完全な制御権限を付与します。
level	暗号強度を指定し、サポートされる暗号の最低レベルを示します。次に、強度の有効な値を強度の低い順に示します。 • **all**：NULL-SHA を含むすべての暗号が含まれます。 • **low**：NULL-SHA を除くすべての暗号が含まれます。 • **medium**：NULL-SHA、DES-CBC-SHA、および RC4-MD5 を除くすべての暗号が含まれます。 • **fips**：FIPS 準拠の暗号がすべて含まれます（NULL-SHA、DES-CBC-SHA、RC4-MD5、RC4-SHA、および DES-CBC3-SHA を除く）。 • **high**（TLSv1.2 にのみ適用）：SHA-2 暗号を使用する AES-256 のみが含まれます。
version	SSL、DTLS、TLS プロトコルのバージョンを指定します。サポートされているバージョンは次のとおりです。 • **default**：発信接続用の暗号セット。 • **dtlsv1**：DTLSv1 着信接続用の暗号。 • dtlsv1.2：DTLSv1.2 着信接続用の暗号。 • **tlsv1**：TLSv1 着信接続用の暗号。 • **tlsv1.1**：TLSv1.1 着信接続用の暗号。 • **tlsv1.2**：TLSv1.2 着信接続用の暗号。

コマンド デフォルト

すべてのプロトコルバージョンのデフォルトは、**medium** 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。

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

コマンド履歴

リリース	変更内容
9.16(1)	DES は弱い暗号であると見なされるため、強力な暗号ライセンスを有効にする場合の DES 設定のサポートを削除しました。 強力なライセンスが有効になっているときに DES が設定されると、DES が、強力な暗号である AES に変換されます。
9.12(1)	lina で tlv1 でサポートされている暗号から NULL-SHA を削除しました。ssl cipher tlsv1 all および ssl cipher tlsv1 custom NULL-SHA コマンドが廃止され削除されました。
9.10(1)	dtls 1.2 オプションが追加されました。
9.4(1)	すべての SSLv3 設定とサポートが ASA から削除されました。
9.3(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

このコマンドは、ASA バージョン 9.3(2) から **ssl encryption** コマンドに置き換わりました。

推奨設定は [**medium**] です。[**high**] を使用すると、接続が制限されることがあります。**custom** を使用すると、少数の暗号のみが設定されている場合は、機能が制限されることがあります。デフォルトのカスタム値を制限すると、クラスタリングを含めて発信接続が制限されることがあります。

OpenSSL を使用した暗号の詳細については、https://www.openssl.org/docs/apps/ciphers.html を参照してください。

どの暗号がどのバージョンをサポートしているかのリストを表示するには、**show ssl ciphers all** コマンドを使用します。次に例を示します。

```
These are the ciphers for the given cipher level; not all ciphers are supported by all
versions of SSL/TLS.
These names can be used to create a custom cipher list:
  DHE-RSA-AES256-SHA256 (tlsv1.2)
  AES256-SHA256 (tlsv1.2)
  DHE-RSA-AES128-SHA256 (tlsv1.2)
  AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES256-SHA (sslv3, tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
```

```
DHE-RSA-AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
AES128-SHA (sslv3, tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
DES-CBC3-SHA (sslv3, tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
RC4-SHA (sslv3, tlsv1)
RC4-MD5 (sslv3, tlsv1)
DES-CBC-SHA (sslv3, tlsv1)
NULL-SHA (sslv3, tlsv1)
```

ASA によってサポートされる暗号の優先順位は次のとおりです。

TLSv1.2 でサポートされている暗号（1 ～ 9）

1. DHE-RSA-AES256-SHA256
2. AES256-SHA256
3. DHE-RSA-AES128-SHA256
4. AES128-SHA256
5. DHE-RSA-AES256-SHA
6. AES256-SHA
7. DHE-RSA-AES128-SHA
8. AES128-SHA
9. DES-CBC3-SHA

TLSv1.1 または TLSv1.2 でサポートされていない暗号（10 ～ 13）

1. RC4-SHA
2. RC4-MD5
3. DES-CBC-SHA
4. NULL-SHA

例

次に、TLSv1.1 FIPS 準拠の暗号を使用するように ASA を設定する例を示します。

```
ciscoasa
(config)#

ssl cipher tlsv1.1 fips
```

次に、TLSv1 カスタム暗号を使用するように ASA を設定する例を示します。

```
ciscoasa
(config)#
 ssl cipher tlsv1 custom "RC4-SHA:ALL"
```

関連コマンド

コマンド	説明
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。

コマンド	説明
show ssl ciphers	サポートされている暗号のリストを表示します。

ssl-client-certificate

LDAPS の使用時に ASA がクライアント証明書として LDAP サーバーに提示する証明書を指定するには、AAA サーバー ホスト コンフィギュレーション モードで **ssl-client-certificate** コマンドを使用します。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。

ssl-client-certificate *trustpoint_name*
no ssl-client-certificate *trustpoint_name*

構文の説明

trustpoint_name	ASA がクライアント証明書として LDAP サーバーに提示する証明書を保持するトラストポイントの名前。

コマンド デフォルト

デフォルトなし

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。

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

コマンド履歴

リリース	変更内容
9.18(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

この証明書は、クライアント証明書を LDAP サーバーで検証するように設定する場合に必要です。サーバーに対して **ldap-over-ssl** も有効にする必要があります。証明書を設定しないと、ASA は LDAP サーバーから要求されたときに証明書を提示しません。LDAP サーバーがピア証明書を要求するように設定されている場合、セキュア LDAP セッションが完了せず、認証/許可要求が失敗します。

例

次に、2 つの LDAP サーバーでそれぞれ異なるトラストポイントをクライアント認証に使用する例を示します。

```
asa(config)# show running-config aaa-server OPENLDAPS
```

```
aaa-server OPENLDAPS protocol ldap
aaa-server OPENLDAPS (manif) host 10.1.1.2
ldap-base-dn DC=example,DC=com
ldap-scope subtree
ldap-naming-attribute cn
ldap-login-password *****
ldap-login-dn cn=admin,dc=example,dc=com
ldap-over-ssl enable
ssl-client-certificate LDAPS_TP_1
server-type auto-detect
aaa-server OPENLDAPS (manif) host 10.2.2.5
ldap-base-dn DC=example,DC=com
ldap-scope subtree
ldap-naming-attribute cn
ldap-login-password *****
ldap-login-dn cn=admin,dc=example,dc=com
ldap-over-ssl enable
ssl-client-certificate LDAPS_TP_2
server-type auto-detect
```

関連コマンド

コマンド	説明
ldap-over-ssl	LDAP サーバーの通信プロトコルとして LDAPS を設定します。

ssl client-version

ASAがクライアントとして動作する場合のSSL/TLSプロトコルのバージョンを指定するには、グローバル コンフィギュレーション モードで**ssl client-version**コマンドを使用します。デフォルトの設定に戻すには、このコマンドの**no**形式を使用します。

ssl client-version［ **any | sslv3-only | tlsv1-only | sslv3 | tlsv1 | tlsv1.1 | tlsv1.2** ］
no ssl client-version

構文の説明

any	SSLv3 クライアントの hello を送信し、SSLv3（以降）をネゴシエートします。
sslv3	SSLv3 クライアントの hello を送信し、SSLv3（以降）をネゴシエートします。
sslv3-only	SSLv3 クライアントの hello を送信し、SSLv3（以降）をネゴシエートします。 （注） このオプションは、バージョン 9.3(2) で廃止されました。
tlsv1	TLSv1 クライアントの hello を送信し、TLSv1（以降）をネゴシエートします。
tlsv1.1	TLSv1.1 クライアントの hello を送信し、TLSv1.1（以降）をネゴシエートします。
tlsv1.2	TLSv1.2 クライアントの hello を送信し、TLSv1.2（以降）をネゴシエートします。
tlsv1-only	TLSv1 クライアントの hello を送信し、TLSv1（以降）をネゴシエートします。 （注） このオプションは、バージョン 9.3(2) で廃止されました。

コマンド デフォルト

デフォルト値は**tlsv1**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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 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。
9.3(2)	SSLv3 は廃止されました。現在のデフォルトは **any** ではなく **tlsv1** です。**any** キーワードは廃止されました。

使用上のガイドライン

any、**sslv3**、または **sslv3-only** キーワードを使用した場合、次の警告が表示されますが、コマンドは受け入れられます。

```
WARNING: SSLv3 is deprecated. Use of TLSv1 or greater is recommended.
```

ASA の次のメジャー リリースでは、これらのキーワードは ASA から削除されます。

例

次に、SSL クライアントとして動作する場合に SSLv3 プロトコルのバージョンを指定するように ASA を設定する例を示します。

```
ciscoasa
(config)#
 ssl client-version any
```

関連コマンド

コマンド	説明
clear config ssl	コンフィギュレーションからすべての SSL コマンドを削除し、デフォルト値に戻します。
ssl encryption	SSL/TLS プロトコルで使用する暗号化アルゴリズムを指定します。
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
ssl server-version	ASA が SSL/TLS 接続をネゴシエートする最小プロトコル バージョンを指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

ssl dh-group

TLS が使用する DHE-RSA 暗号で Diffie-Hellmann（DH）グループを使用するように指定するには、グローバル コンフィギュレーション モードで **ssl dh-group** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ssl dh-group［ **group1 | group2 | group5 | group14 | group24** ］
no ssl dh-group［ **group1 | group2 | group5 | group14 | group24** ］

構文の説明

group1	DH グループ 1（768 ビット モジュラス）を設定します。
group2	DH グループ 2（1024 ビット モジュラス）を設定します。
group5	DH グループ 5（1536 ビット モジュラス）を設定します。
group14	DH グループ 14（2048 ビット モジュラス、224 ビット素数位数サブグループ）を設定します。
group24	DH グループ 24（2048 ビット モジュラス、256 ビット素数位数サブグループ）を設定します。

コマンド デフォルト

デフォルトは DH グループ 14 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。

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

コマンド履歴

リリース	変更内容
9.16(1)	group2、group5、および group24 コマンドオプションのサポートが削除されました。 group15 コマンドオプションのサポートが追加されました。
9.13(1)	group2 および group 5 コマンド オプションは廃止され、以降のリリースで削除されます。
9.3(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

グループ 1 および 2 は、Java 7 およびそれ以前のバージョンと互換性があります。グループ 5、14、および 24 は、Java 7 と互換性がありません。すべてのグループが Java 8 と互換性があります。グループ 14 と 24 は FIPS 準拠です。

例

次に、特定の DH グループを使用するように ASA を設定する例を示します。

```
ciscoasa
(config)#
 ssl dh-group group14
```

関連コマンド

コマンド	説明
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。

ssl ecdh-group

TLS が使用する ECDHE-ECDSA 暗号でグループを使用するように指定するには、グローバル コンフィギュレーション モードで **ssl ecdh-group** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

ssl ecdh-group［ **group19 | group20 | group21** ］
no ssl ecdh-group［ **group19 | group20 | group21** ］

構文の説明

group19	グループ 19（256 ビット EC）を設定します。
group20	グループ 20（384 ビット EC）を設定します。
group21	グループ 21（521 ビット EC）を設定します。

コマンド デフォルト

デフォルトはグループ 19 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。

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

コマンド履歴

リリース	変更内容
9.4(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

TLSv1.2 では、次の暗号方式のサポートが追加されています。

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256

- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256

（注） 優先度が最も高いのは ECDSA 暗号方式と DHE 暗号方式です。

例

次に、特定の DH グループを使用するように ASA を設定する例を示します。

```
ciscoasa
(config)#
 ssl ecdh-group group21
```

関連コマンド

コマンド	説明
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。

ssl encryption（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.3(1) でした。

SSL、DTLS、TLS の各プロトコル用の暗号化アルゴリズムを指定するには、グローバル コンフィギュレーション モードで **ssl encryption** コマンドを使用します。**.**デフォルト（暗号化アルゴリズムの完全なセット）に戻すには、このコマンドの **no** 形式を使用します。

ssl encryption [**3des-sha1**] [**aes128-sha1**] [**aes256-sha1**] [**des-sha1**] [**null-sha1**] [**rc4-md5**] [**rc4-sha1**] [**dhe-aes256-sha1**] [**dhe-aes128-sha1**]
no ssl encryption

構文の説明

3des-sha1	Secure Hash Algorithm 1 を使用する Triple DES 168 ビット暗号化を指定します（FIPS 準拠）。
aes128-sha1	Secure Hash Algorithm 1 を使用するトリプル AES 128 ビット暗号化を指定します（FIPS 準拠）。
aes256-sha1	Secure Hash Algorithm 1 を使用するトリプル AES 256 ビット暗号化を指定します（FIPS 準拠）。
dhe-aes128-sha1	Transport Layer Security（TLS）用に AES 128 ビット暗号化暗号スイートを指定します（FIPS 準拠）。
dhe-aes256-sha1	Transport Layer Security（TLS）用に AES 256 ビット暗号化暗号スイートを指定します（FIPS 準拠）。
des-sha1	Secure Hash Algorithm 1 を使用する DES 56 ビット暗号化を指定します。
null-sha1	Secure Hash Algorithm 1 で使用するヌル暗号化を指定します。この設定は、機密性なしでメッセージ整合性を強化します。 **注意** null-sha1 を指定すると、データは暗号化されません。
rc4-md5	MD5 ハッシュ関数を使用する RC4 128 ビット暗号化を指定します。
rc4-sha1	Secure Hash Algorithm 1 を使用する RC4 128 ビット暗号化を指定します。

コマンド デフォルト

デフォルトでは、ASA 上の SSL 暗号化リストには次のアルゴリズムが次の順序で含まれています。

1. RC4-SHA1
2. AES128-SHA1（FIPS 準拠）
3. AES256-SHA1（FIPS 準拠）

4. 3DES-SHA1（FIPS 準拠）
5. DHE-AES256-SHA1（FIPS 準拠）
6. DHE-AES128-SHA1（FIPS 準拠）

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 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。
9.1(2)	DHE-AES128-SHA1 アルゴリズムおよび DHE-AES256-SHA1 アルゴリズムを使用した SSL 暗号化のサポートが追加されました。
9.3(2)	このコマンドは廃止され、 **ssl cipher** コマンドに置き換えられました。
9.12(1)	このコマンドは削除されました。

使用上のガイドライン

このコマンドを再度発行すると、前の設定は上書きされます。ASDM のライセンス タブには、設定した値ではなく、ライセンスでサポートされる暗号化の最大レベルが反映されます。

アルゴリズムの使用の優先順位は、アルゴリズムの順序によって決まります。環境のニーズに合わせてアルゴリズムを追加または削除できます。

FIPS 準拠の セキュアクライアント SSL 接続の場合、FIPS 準拠の暗号が SSL 暗号化リストの先頭に指定されていることを確認する必要があります。

アプリケーションによっては DHE がサポートされないものがあるため、他の SSL 暗号化方式を少なくとも 1 つ含めて、暗号スイートが両方に共通するようにします。

http://en.wikipedia.org/wiki/Symmetric-key_algorithm に示すように、暗号化操作では対称キーアルゴリズムが使用されます。

例

次に、3des-sha1 および des-sha1 暗号化アルゴリズムを使用するように ASA を設定する例を示します。

```
ciscoasa
```

```
(config)#
 ssl encryption 3des-sha1 des-sha1
```

ASA バージョン 9.3(2) 以降

次の例では、このコマンドが廃止され、 **ssl cipher** コマンドに置き換えられたことを示します。

ciscoasa (config)# **ssl encryption ?**

```
configure mode commands/options:
This command is DEPRECATED, use 'ssl cipher' instead.
  3des-sha1         Indicate use of 3des-sha1 for ssl encryption
  aes128-sha1       Indicate use of aes128-sha1 for ssl encryption
  aes256-sha1       Indicate use of aes256-sha1 for ssl encryption
  des-sha1          Indicate use of des-sha1 for ssl encryption
  dhe-aes128-sha1   Indicate use of dhe-aes128-sha1 for ssl encryption
  dhe-aes256-sha1   Indicate use of dhe-aes256-sha1 for ssl encryption
  null-sha1         Indicate use of null-sha1 for ssl encryption (NOTE: Data is
                    NOT encrypted if this cipher is chosen)
  rc4-md5           Indicate use of rc4-md5 for ssl encryption
  rc4-sha1          Indicate use of rc4-sha1 for ssl encryption
```

ciscoasa (config)# **ssl encryption rc4-sha1 aes256-sha1 aes128-sha1**

```
WARNING: This command has been deprecated; use 'ssl cipher' instead.
INFO: Converting to: ssl cipher default custom "RC4-SHA:AES256-SHA:AES128-SHA"
INFO: Converting to: ssl cipher sslv3 custom "RC4-SHA:AES256-SHA:AES128-SHA"
INFO: Converting to: ssl cipher tlsv1 custom "RC4-SHA:AES256-SHA:AES128-SHA"
INFO: Converting to: ssl cipher dtlsv1 custom "RC4-SHA:AES256-SHA:AES128-SHA"
```

関連コマンド

コマンド	説明
clear config ssl	コンフィギュレーションからすべての SSL コマンドを削除し、デフォルト値に戻します。
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
ssl client-version	ASA がクライアントとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl server-version	ASA が SSL/TLS 接続をネゴシエートする最小プロトコル バージョンを指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。
ssl cipher	SSL、DTLS、および TLS プロトコルの暗号化アルゴリズムを指定します。 （注） 9.3(2) リリース以降で使用できます。

ssl server-version

ASA が SSL/TLS 接続をネゴシエートする最小プロトコルバージョンを設定するには、グローバル コンフィギュレーション モードで **ssl server-version** コマンドを使用します。デフォルトの any に戻すには、このコマンドの **no** 形式を使用します。

ssl server-version [[**tlsv1 | tlsv1.1 | tlsv1.2**] [**dtlsv1 | dtlsv1.2**]]
no ssl server-version

構文の説明

tlsv1	SSLv2 クライアントの hello を受け入れ、TLSv1（以降）をネゴシエートします。
tlsv1.1	SSLv2 クライアントの hello を受け入れ、TLSv1.1（以降）をネゴシエートします。
tlsv1.2	SSLv2 クライアントの hello を受け入れ、TLSv1.2（以降）をネゴシエートします。
dtlsv1	DTLSv1 クライアントの hello を受け入れ、DTLSv1（以降）をネゴシエートします。
dtlsvv 1.2	DTLSv1.2 クライアントの hello を受け入れ、DTLSv1.2（以降）をネゴシエートします。DTLSv 1.2 トンネルの使用を指定するには、唯一の有効なオプションである TLSv 1.2 トンネルの指定が必要です。

コマンド デフォルト

デフォルト値は **tlsv1** および **dtlsv1** 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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 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。
9.3(2)	SSLv3 は廃止されました。現在のデフォルトは **any** ではなく **tlsv1** です。 **any** キーワードは廃止されました。

リリース	変更内容
9.4(1)	すべての SSLv3 キーワードが ASA コンフィギュレーションから削除され、SSLv3 サポートが ASA から除外されました。SSLv3 がイネーブルになっている場合は、SSLv3 オプションを指定したコマンドからブート時エラーが表示されます。ASA はデフォルトの TLSv1 に戻ります。
9.10(1)	DTLSv 1.2 がサポートされるようになり、DTLS オプションが提供されるようになりました。以前は、DTLS バージョン 1 がデフォルトのままと想定されていました。

例

次に、SSL/TLS 接続をネゴシエートするように ASA を設定する例を示します。

```
ciscoasa
(config)#
 ssl server-version tlsv1
```

次に、set versions のコンフィギュレーションおよび検証の例を示します。

```
ciscoasa (config)# ssl server-version tlsv1.2 dtlsv1.2

ciscoasa (config)# sh run ssl
ssl server-version tlsv1.2 dtlsv1.2
ciscoasa (config)# no ssl server-version
ciscoasa (config)# sh run all ssl
ssl server-version tlsv1 dtlsv1
```

関連コマンド

コマンド	説明
clear config ssl	コンフィギュレーションからすべての SSL コマンドを削除し、デフォルト値に戻します。
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
ssl client-version	ASA がクライアントとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl encryption	SSL/TLS プロトコルで使用する暗号化アルゴリズムを指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

ssl trust-point

インターフェイスの SSL 証明書を表す証明書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 **ssl trust-point** コマンドを *interface* 引数を指定して使用します。インターフェイスを指定しないSSLトラストポイントを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。インターフェイスを指定するエントリを削除するには、このコマンドの **ssl trust-point** *name* [*interface*] 形式を使用します。

ssl trust-point *name*［ *interface*［ **vpnlb-ip** ］ | **domain** *domain-name* ］
no ssl trust-point *name*［ *interface*［ **vpnlb-ip** ］ | **domain** *domain-name* ］

構文の説明

domain *domain-name*	このインターフェイスへのアクセスに使用される特定のドメイン名（たとえば、www.cisco.com）にこのトラストポイントを関連付けます。
interface	トラストポイントが適用されるインターフェイスの名前を指定します。インターフェイスの名前は **nameif** コマンドで定義します。
name	**crypto ca trustpoint** *name* コマンドに設定されているように CA トラストポイントの名前を指定します。
vpnlb-ip	このインター ーフェイスの VPN ロード バランシング クラスタ IP アドレスにこのトラストポイントを関連付けます。インターフェイスにだけ適用されます。

コマンド デフォルト

デフォルトでは、トラストポイント アソシエーションはありません。ASA では、デフォルトの自己生成 RSA キーペア証明書が使用されます。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 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。
9.3(2)	**domain** *domain-name* のキーワードと引数の組み合わせが追加されました。

使用上のガイドライン

インターフェイスまたはドメインを指定しない場合、このエントリは、独自のトラストポイントに関連付けられていない、すべてのインターフェイスで使用されるフォールバック トラストポイントを表します。

ssl trustpoint ? コマンドを入力すると、使用可能な設定済みのトラストポイントが表示されます。 **ssl trust-point** *name* **?** コマンド（たとえば、 **ssl trust-point mysslcert ?** ）を入力した場合、trustpoint-SSL証明書アソシエーションに使用可能な設定済みのインターフェイスが表示されます。

インターフェイス 1 つにつき、最大 16 個のトラストポイントを設定できます。

このコマンドを使用するときは、次のガイドラインに従ってください。

- *trustpoint* の値は、 **crypto ca trustpoint** *name* コマンドで設定された CA トラストポイントの name である必要があります。
- *interface* の値は、あらかじめ設定されたインターフェイスの *nameif* 名である必要があります。
- トラストポイントを削除すると、そのトラストポイントを参照する **ssl trust-point** エントリも削除されます。
- **ssl trust-point** エントリは、インターフェイスごとに 1 つと、インターフェイスを指定しないもの 1 つを保持できます。
- **domain** キーワードで設定したトラストポイントは、複数のインターフェイスに適用されることがあります（接続方法によって異なります）。
- *domain-name* 値ごとに **ssl trust-point** を 1 つだけ設定できます。
- 同じトラストポイントを複数のエントリで再利用できます。
- このコマンドを入力すると、次のエラーが表示される場合があります。

```
error:0B080074:x509 certificate routines:X509_check_private_key:key values
mismatch@x509_cmp.c:339
```

これは、ユーザーが新しい証明書を設定して、以前に設定された証明書と置き換えたことを示しています。特に対処の必要はありません。

- 証明書は次の順序で選択されます。
  - 接続が **domain** キーワードの値に一致した場合、その証明書が最初に選択されます。（ **ssl trust-point** *name* **domain** *domain-name* コマンド）
  - ロードバランシング アドレスへの接続が確立された場合、vpnlb-ip 証明書が選択されます。（ **ssl trust-point** *name* **interface vpnlb-ip** コマンド）
  - インターフェイスに対して設定された証明書。（ **ssl trust-point** *name* **interface** コマンド）
  - インターフェイスに関連付けられていないデフォルトの証明書。（ **ssl trust-point** *name* コマンド）

- ASA の自己署名付き自己生成証明書。

例

次に、inside インターフェイスの FirstTrust という名前の SSL トラストポイントと、インターフェイスが関連付けられない DefaultTrust という名前のトラストポイントを設定する例を示します。

```
ciscoasa
(config)#
 ssl trust-point FirstTrust inside
ciscoasa
(config)#
 ssl trust-point DefaultTrust
```

次に、このコマンドの **no** 形式を使用して、インターフェイスが関連付けられていないトラストポイントを削除する例を示します。

```
ciscoasa
(config)#
 show running-configuration ssl
ssl trust-point FirstTrust inside
ssl trust-point DefaultTrust
ciscoasa(config)# no ssl trust-point
ciscoasa
(config)#
 show running-configuration ssl
ssl trust-point FirstTrust inside
```

次に、インターフェイスが関連付けられているトラストポイントを削除する例を示します。

```
ciscoasa
(config)#
 show running-configuration ssl
ssl trust-point FirstTrust inside
ssl trust-point DefaultTrust
ciscoasa
(config)#
 no ssl trust-point FirstTrust inside
ciscoasa
(config)#
 show running-configuration ssl
ssl trust-point DefaultTrust
```

次に、設定済みのトラストポイントに特定のドメイン名を割り当てる例を示します。

```
ciscoasa
(config)#
 ssl trust-point
            www-cert domain www.example.com
```

関連コマンド

コマンド	説明
clear config ssl	コンフィギュレーションからすべての SSL コマンドを削除し、デフォルト値に戻します。
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
ssl client-version	ASA がクライアントとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl encryption	SSL/TLS プロトコルで使用する暗号化アルゴリズムを指定します。
ssl server-version	ASA が SSL/TLS 接続をネゴシエートする最小プロトコル バージョンを指定します。
show ssl	SSL 設定統計情報を表示します。

sso-server（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

ASA のユーザー認証のためにシングルサインオンサーバーを作成する場合、webvpn コンフィギュレーションモードで **sso-server** コマンドを使用します。このコマンドでは、SSO サーバータイプを指定する必要があります。

SSO サーバーを削除するには、このコマンドの **no** 形式を使用します。

sso-server *name* **type** ［ *siteminder* | *saml-v1.1-post* ］
no sso-server *name*

（注） このコマンドは、SSO 認証用に必要です。

構文の説明

name	SSO サーバーの名前を指定します。最小 4 文字、最大 31 文字です。
saml-v1.1-post	設定する ASA SSO サーバーが、SAML、バージョン 1.1、POST タイプの SSO サーバーであることを指定します。
siteminder	設定する ASA SSO サーバーが、Computer Associates SiteMinder SSO サーバーであることを指定します。
type	SSO サーバーのタイプを指定します。使用できるタイプは、SiteMinder と SAML-V1.1-POST だけです。

コマンド デフォルト

デフォルトの値や動作はありません。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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(1)	このコマンドが追加されました。
9.5(2)	SAML 2.0 がサポートされたため、このコマンドは廃止されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザーはユーザー名とパスワードを一度だけ入力すれば、別のサーバーでさまざまなセキュアなサービスにアクセスできます。 **sso-server** コマンドを使用すると、SSO サーバーを作成できます。

認証では、ASA は SSO サーバーへの WebVPN ユーザーのプロキシとして動作します。ASA は現在、SiteMinder SSO サーバー（以前の Netegrity SiteMinder）と SAML POST タイプの SSO サーバーをサポートしています。現在、type オプションで使用できる引数は *siteminder* または *saml-V1.1-post* に限定されています。

例

次に、webvpn コンフィギュレーション モードで、「example1」という名前の SiteMinder-type の SSO サーバーを作成する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# sso-server example1 type siteminder
ciscoasa(config-webvpn-sso-siteminder)#
```

次に、webvpn コンフィギュレーション モードで、「example2」という名前の SAML、バージョン 1.1、POST-type の SSO サーバーを作成する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# sso-server example2 type saml-v1.1-post
ciscoasa(config-webvpn-sso-saml)#
```

関連コマンド

コマンド	説明
assertion-consumer-url	SAML-type の SSO アサーション コンシューマ サービスの URL を指定します。
issuer	SAML-type の SSO サーバーのセキュリティ デバイス名を指定します。
max-retry-attempts	SSO 認証に失敗した場合に ASA が再試行する回数を設定します。
policy-server-secret	SiteMinder SSO サーバーへの認証要求の暗号化に使用する秘密キーを作成します。
request-timeout	SSO 認証の試行に失敗したときにタイムアウトになるまでの秒数を指定します。
show webvpn sso-server	SSO サーバーの運用統計情報を表示します。
test sso-server	テスト認証要求で SSO サーバーをテストします。

コマンド	説明
trustpoint	SAML-type のブラウザ アサーションへの署名に使用する証明書を含むトラストポイント名を指定します。
web-agent-url	ASA が SiteMinder SSO 認証を要求する SSO サーバーの URL を指定します。

sso-server value（group-policy webvpn）（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

SSO サーバーをグループポリシーに割り当てるには、グループポリシー コンフィギュレーション モードで使用可能な webvpn コンフィギュレーション モードで **sso-server value** コマンドを使用します。

割り当てを削除してデフォルトポリシーを使用するには、このコマンドの **no** 形式を使用します。

デフォルトポリシーが継承されないようにするには、**sso-server none** コマンドを使用します。

sso-server { **value** *name* | **none** }
[**no**] **sso-server value** *name*

構文の説明

name グループポリシーに割り当てる SSO サーバーの名前を指定します。

コマンド デフォルト

グループに割り当てられるデフォルト ポリシーは、DfltGrpPolicy 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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー 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(1)	このコマンドが追加されました。
9.5(2)	SAML 2.0 がサポートされたため、このコマンドは廃止されました。

使用上のガイドライン

グループポリシー webvpn モードで **sso-server value** コマンドを入力すると、SSO サーバーをグループポリシーに割り当てることができます。

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザーはユーザー名とパスワードを一度だけ入力すれば、別のサーバーでさまざまなセキュアなサービスにアクセスできます。ASA は、現在、SiteMinder-type の SSO サーバーと SAML POST-type の SSO サーバーをサポートしています。

このコマンドは SSO サーバーの両タイプに適用されます。

（注） SSO サーバーをユーザーポリシーに割り当てるには、同じコマンド **sso-server value** をユーザー名 webvpn コンフィギュレーション モードで入力します。

例

次に、グループ ポリシー my-sso-grp-pol を作成し、example という名前の SSO サーバーに割り当てるサンプル コマンドを示します。

```
ciscoasa(config)# group-policy my-sso-grp-pol internal
ciscoasa(config)# group-policy my-sso-grp-pol attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# sso-server value example
ciscoasa(config-group-webvpn)#
```

関連コマンド

コマンド	説明
policy-server-secre t	SiteMinder SSO サーバーへの認証要求の暗号化に使用する秘密キーを作成します。
show webvpn sso-server	セキュリティ デバイスに設定されているすべての SSO サーバーの運用統計情報を表示します。
sso-server	シングル サインオン サーバーを作成します。
sso-server value (username webvpn)	SSO サーバーをユーザー ポリシーに割り当てます。
web-agent-url	ASA が、SiteMinder-type の SSO 認証を要求する SSO サーバーの URL を指定します。

sso-server value（username webvpn）（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

SSO サーバーをユーザーポリシーに割り当てるには、ユーザー名コンフィギュレーション モードで使用可能な webvpn コンフィギュレーション モードで **sso-server value** コマンドを使用します。

ユーザーの SSO サーバー割り当てを削除するには、このコマンドの **no** 形式を使用します。

ユーザーポリシーがグループポリシーから不要な SSO サーバー割り当てを継承している場合は、**sso-server none** コマンドを使用して割り当てを削除します。

sso-server { **value** *name* | **none** }
[**no**] **sso-server value** *name*

構文の説明

name ユーザー ポリシーに割り当てる SSO サーバーの名前を指定します。

コマンド デフォルト

デフォルトでは、ユーザー ポリシーはグループ ポリシーの SSO サーバー割り当てを使用します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ユーザー名 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(1)	このコマンドが追加されました。
9.5(2)	SAML 2.0 がサポートされたため、このコマンドは廃止されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザーはユーザー名とパスワードを一度だけ入力すれば、別のサーバーでさまざまなセキュアなサービスに

アクセスできます。ASA は、現在、SiteMinder-type の SSO サーバーと SAML POST-type の SSO サーバーをサポートしています。

このコマンドは SSO サーバーの両タイプに適用されます。

sso-server value コマンドを入力すると、SSO サーバーをユーザーポリシーに割り当てることができます。

（注） SSO サーバーをグループポリシーに割り当てるには、同じコマンド **sso-server value** をグループ webvpn コンフィギュレーション モードで入力します。

例

次に、my-sso-server という名前の SSO サーバーを Anyuser という名前の WebVPN ユーザーのユーザー ポリシーに割り当てるサンプル コマンドを示します。

```
ciscoasa(config)# username Anyuser attributes
ciscoasa(config-username)# webvpn
ciscoasa(config-username-webvpn)# sso-server value my-sso-server
ciscoasa(config-username-webvpn)#
```

関連コマンド

コマンド	説明
policy-server-secret	SiteMinder SSO サーバーへの認証要求の暗号化に使用する秘密キーを作成します。
show webvpn sso-server	セキュリティ デバイスに設定されているすべての SSO サーバーの運用統計情報を表示します。
sso-server	シングル サインオン サーバーを作成します。
sso-server value (config-group-webvpn)	SSO サーバーをグループ ポリシーに割り当てます。
web-agent-url	ASA が SiteMinder SSO 認証を要求する SSO サーバーの URL を指定します。

start-port

マッピングアドレスおよびポート（MAP）ドメイン内の基本マッピングルールでポートプールの開始ポートを設定するには、MAP ドメインの基本マッピング ルール コンフィギュレーション モードで **start-port** コマンドを使用します。比率を削除するには、このコマンドの **no** 形式を使用します。

start-port*number*
no start-port *number*

構文の説明

number 変換されたアドレスのポートプールに表示される最初のポート。指定するポートは 1 ～ 32768 の範囲内とし、2 の累乗にする必要があります（1、2、4、8 など）。既知のポートを除外する場合は、1024 以降から開始します。

コマンド デフォルト

デフォルト設定はありません。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
MAP ドメインの基本マッピング ルール コンフィギュレーション モード。	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.13(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

基本マッピングルールの **start-port** コマンドおよび **share-ratio** コマンドによって、MAP ドメイン内のアドレス変換に使用されるプールの開始ポートとポート数が決まります。

例

次の例では、1 という名前の MAP-T ドメインを作成して、ドメインの変換ルールを設定しています。

```
ciscoasa(config)# map-domain 1

ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64
```

```
ciscoasa(config-map-domain)# basic-mapping-rule
ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
ciscoasa(config-map-domain-bmr)# start-port 1024
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

関連コマンド

コマンド	説明
basic-mapping-rule	MAP ドメインの基本マッピング ルールを設定します。
default-mapping-rule	MAP ドメインのデフォルト マッピング ルールを設定します。
ipv4-prefix	MAP ドメインの基本マッピング ルールの IPv4 プレフィックスを設定します。
ipv6-prefix	MAP ドメインの基本マッピング ルールの IPv6 プレフィックスを設定します。
map-domain	マッピング アドレスおよびポート（MAP）ドメインを設定します。
share-ratio	MAP ドメインの基本マッピング ルールのポート数を設定します。
show map-domain	マッピング アドレスおよびポート（MAP）ドメインに関する情報を表示します。
start-port	MAP ドメインの基本マッピング ルールの開始ポートを設定します。

start-url

オプションの事前ログインクッキーの取得先URLを入力するには、AAAサーバーホストコンフィギュレーション モードで **start-url** コマンドを入力します。これはHTTP フォームのコマンドを使用したSSO です。

start-url *string*

（注） HTTPプロトコルを使用してSSOを正しく設定するには、認証とHTTPプロトコル交換についての詳しい実務知識が必要です。

構文の説明

string	SSO サーバーのURL。URL の最大長は1024 文字です。

コマンド デフォルト

デフォルトの値や動作はありません。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AAA サーバーホスト 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(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

ASA の WebVPN サーバーは、HTTP POST 要求を使用して、シングルサインオン認証要求を認証 Web サーバーに送信できます。認証 Web サーバーは、Set-Cookie ヘッダーをログイン ページのコンテンツとともに送信することによって、事前ログイン シーケンスを実行できます。このことは、認証 Web サーバーのログイン ページにブラウザで直接接続することによって検出できます。ログインページがロードされるときにWebサーバーによってクッキーが設定され、このクッキーがその後のログインセッションに関連する場合、**start-url** コマンドを使用してクッキーの取得先 URL を入力する必要があります。実際のログイン シーケンスは、事前ログイン クッキー シーケンスの後で、認証 Web サーバーへのフォーム送信により開始されます。

（注） **start-url** コマンドは、事前ログインクッキー交換が存在する場合にのみ必要です。

例

次に、AAA サーバー ホスト コンフィギュレーション モードで、事前ログイン クッキーを取得するための URL https://example.com/east/Area.do?Page-Grp1 を指定する例を示します。

```
ciscoasa(config)# aaa-server testgrp1 (inside) host example.com
ciscoasa(config-aaa-server-host)# start-url https://example.com/east/Area.do?Page=Grp1
ciscoasa(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
action-uri	シングルサインオン認証用のユーザー名およびパスワードを受信するための Web サーバー URI を指定します。
auth-cookie-name	認証クッキーの名前を指定します。
hidden-parameter	認証 Web サーバーと交換するための非表示パラメータを作成します。
password-parameter	SSO 認証用にユーザー パスワードを送信する必要がある HTTP POST 要求パラメータの名前を指定します。
user-parameter	SSO認証用にユーザー名を送信する必要があるHTTP POST要求のパラメータの名前を指定します。

state-checking

H.323 の状態チェックを実行するには、パラメータ コンフィギュレーション モードで **state-checking** コマンドを使用します。この機能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。

state-checking［ **h225 | ras** ］
no state-checking［ **h225 | ras** ］

構文の説明

h225	H.225 の状態チェックを実行します。
ras	RAS の状態チェックを実行します。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
パラメータ 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
7.2(1)	このコマンドが追加されました。

例

次に、H.323 コールで RAS の状態チェックを実行する例を示します。

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# state-checking ras
```

関連コマンド

コマンド	説明
policy-map type inspect	インスペクション ポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

storage-url

各コンテキストでフラッシュメモリを使用してVPNパッケージを格納できるようにするには、コンテキスト コンフィギュレーション モードで **storage-url** コマンドを使用します。記憶域を削除するには、このコマンドの **no** 形式を使用します。

storage-url { **private | shared** } [**disk** *n* **:** /] *path* [*context_label*]
no storage-url { **private | shared** } [**disk** *n* **:** /] *path* [*context_label*]

構文の説明

private	プライベート記憶域をコンテキストに割り当てます。private で指定できる専用記憶域は、コンテキストごとに 1 つに限られます。
shared	共有記憶域をコンテキストに割り当てます。shared で指定できる読み取り専用の共有記憶域はコンテキストごとに 1 つですが、共有ディレクトリは複数作成することができます。
[**disk***n***:/**]*path*	記憶域にパスを設定します。ディスク番号を指定しない場合、デフォルトで **disk0** に設定されます。ASA はプライベート記憶域に指定されたパスの下にサブディレクトリを作成し、コンテキストにちなんだ名前を付けます。たとえば、contextA の場合、**disk1:/private-storage** をパスとして指定すると、ASA はこのコンテキストのサブディレクトリを disk1:/private-storage/contextA/ に作成します。この記憶域は複数のコンテキストで共有されるため、ASA は共有記憶域にはコンテキストのサブディレクトリを作成しません。
context_label	（任意）ファイルシステムがコンテキスト管理者に公開されないよう、このパスにコンテキスト内での名前を指定することもできます。それには、*context_label* を使用します。たとえば、*context_label* を **context** として指定すると、コンテキスト内からは、このディレクトリは **context:** と呼ばれます。

コマンド デフォルト

ディスク番号を指定しない場合、デフォルトで **disk0** に設定されます。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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
9.6(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

各コンテキストでフラッシュメモリを使用してセキュアクライアントなどのVPNパッケージを保存できるだけでなく、セキュアクライアントおよびクライアントレスSSL VPNポータルのカスタマイズ用のストレージも提供できます。読み取り専用の共有記憶域だけでなく、コンテキストごとに専用の記憶域も使用できます。注：**mkdir**コマンドを使用して、指定したディスク上にターゲットディレクトリがすでに存在することを確認してください。

privateで指定できる専用記憶域は、コンテキストごとに1つに限られます。コンテキスト内から（およびシステム実行スペースから）、このディレクトリの読み取り/書き込み/削除操作を実行できます。コンテキストごとに許容するディスク容量の大きさを制御するには、**limit-resource storage**コマンドを参照してください。

セキュアクライアントパッケージなど、すべてのコンテキスト間でASAで共有できる共通の大きなファイルの重複を減らすために、共有のストレージスペースを使用できます。共有ディレクトリの書き込みおよび削除操作は、システム実行スペースでのみ実行できます。

例

次に、プライベートディレクトリと共有ディレクトリを作成し、それらを管理コンテキストに割り当てる例を示します。

```
ciscoasa(config)# mkdir disk1:/private-storage
ciscoasa(config)# mkdir disk1:/shared-storage
ciscoasa(config)# context admin
ciscoasa(config-ctx)# storage-url private disk1:/private-storage context
ciscoasa(config-ctx)# storage-url shared disk1:/shared-storage shared
```

関連コマンド

コマンド	説明
limit-resource storage	コンテキストごとに許容するディスク容量の大きさを制御します。

storage-key

セッション間に保管されるデータを保護するストレージキーを指定するには、グループポリシー webvpn コンフィギュレーション モードで **storage-key** コマンドを使用します。このコマンドを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** バージョンを使用します。

storage-key { **none | value** *string* }
nostorage-key

構文の説明

string ストレージ キーの値として使用するストリングを指定します。この文字列は最大 64 文字まで使用できます。

コマンド デフォルト

デフォルトは **none** 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。

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

ストレージキーの値にはスペース以外の任意の文字を使用できますが、標準的な英数字セット（0 ～ 9 および a ～ z）のみを使用することを推奨します。

例

次に、ストレージ キーを値 abc123 に設定する例を示します。

```
ciscoasa
(config)#

group-policy test attributes
ciscoasa
(config-group-policy)#
 webvpn
```

```
ciscoasa
(config-group-webvpn)#
storage-key value abc123
```

関連コマンド

コマンド	説明
storage-objects	セッションとセッションの間に保存されたデータのストレージ オブジェクトを設定します。

storage-objects

セッション間に保管されるデータについて使用するストレージオブジェクトを指定するには、グループポリシー webvpn コンフィギュレーション モードで **storage-objects** コマンドを使用します。このコマンドを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**バージョンを使用します。

storage-objects { **none | value** *string* }
no storage-objects

構文の説明

string ストレージ オブジェクトの名前を指定します。この文字列は最大 64 文字まで使用できます。

コマンド デフォルト

デフォルトは **none** 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。

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

ストレージオブジェクト名にはスペースおよびカンマ以外の任意の文字を使用できますが、標準的な英数字セット（0 ～ 9 および a ～ z）のみを使用することを推奨します。ストリング内でストレージ オブジェクトの名前を区切るには、カンマをスペースなしで使用します。

例

次に、ストレージ オブジェクト名を cookies および xyz456 に設定する例を示します。

```
ciscoasa
(config)#

group-policy test attributes
ciscoasa
(config-group-policy)#
```

```
 webvpn
ciscoasa
(config-group-webvpn)#
storage-object value cookies,xyz456
```

関連コマンド

コマンド	説明
storage-key	セッション間に保管されるデータに対して使用するストレージ キーを設定します。
user-storage	セッション間にユーザー データを保管するための場所を設定します。

strict-asp-state

M3UA アプリケーション サーバー プロセス（ASP）の厳密な状態検証を有効にするには、ポリシー マップ パラメータ コンフィギュレーショ モードで **strict-asp-state** 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。

strict-asp-state
no strict-asp-state

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。

コマンド デフォルト

このコマンドのデフォルト設定は、ディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
パラメータ 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
9.7(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、M3UA インスペクション ポリシー マップを設定する場合に使用します。

アプリケーション サーバー プロセス（ASP）の厳密な状態検証を有効にすると、システムは M3UA セッションの ASP の状態を維持し、検証結果に基づいて ASP メッセージを許可またはドロップします。ASP の厳密な状態検証を無効にすると、すべての ASP メッセージが検査されずに転送されます。

厳密な ASP のステート チェックが必要なのは、ステートフル フェールオーバーが必要な場合、またはクラスタ内での動作が必要な場合です。ただし、厳密な ASP のステート チェックは、上書きモードでのみ動作し、ロードシェアリングまたはブロードキャスト モードで実行している場合は動作しません（RFC 4666 より）。インスペクションは、エンドポイントごとに ASP が 1 つだけあると仮定します。

例

次に、状態およびセッションの厳密なチェックを有効にする例を示します。

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-policy
```

```
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# strict-asp-state
```

関連コマンド

コマンド	説明
inspect m3ua	M3UA インスペクションをイネーブルにします。
policy-map type inspect m3ua	M3UA インスペクション ポリシー マップを作成します。

strict-diameter

Diameter プロトコルの RFC 6733 への厳密な準拠を有効にするには、ポリシー マップ パラメータ コンフィギュレーション モードで **strict-diameter** 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。

strict-diameter { **state | session** }
no strict-diameter { **state | session** }

構文の説明

state	ステート マシンの検証を有効にします。
session	セッション関連のメッセージの検証を有効にします。

コマンド デフォルト

デフォルトでは、インスペクションによって、Diameter フレームの RFC への準拠は確保されますが、状態とセッションのチェックは有効になりません。

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。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
パラメータ 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
9.6(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

Diameter インスペクション ポリシー マップを設定する場合に、このコマンドを使用します。

これらのオプションでは、標準プロトコルの準拠チェックに加え、状態とセッションの厳密なコンプライアンス検証も有効になります。コマンドを2回入力すると、状態とセッションの両方のチェックを有効にすることができます。

例

次に、状態およびセッションの厳密なチェックを有効にする例を示します。

```
ciscoasa(config)# policy-map type inspect diameter diameter-policy
ciscoasa(config-pmap)# parameters
```

```
ciscoasa(config-pmap-p)# strict-diameter state
ciscoasa(config-pmap-p)# strict-diameter session
```

関連コマンド

コマンド	説明
inspect diameter	Diameter インスペクションを有効にします。
policy-map type inspect diameter	Diameter インスペクション ポリシー マップを作成します。

strict-header-validation

RFC 3261 に従って、SIP メッセージのヘッダーフィールドの厳密な検証をイネーブルにするには、パラメータ コンフィギュレーション モードで **strict-header-validation** コマンドを使用します。パラメータ 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。この機能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。

strict-header-validation action { **drop | drop-connection | reset | log** } { **log** }
no strict-header-validation action { **drop | drop-connection | reset | log** } { **log** }

構文の説明

drop	検証発生時にパケットをドロップします。
drop-connection	違反が発生した場合、接続をドロップします。
reset	違反が発生した場合、接続をリセットします。
log	違反が発生した場合、スタンドアロンまたは追加のログを記録することを指定します。任意のアクションと関連付けることができます。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
パラメータ 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
7.2(1)	このコマンドが追加されました。

例

次に、SIP インスペクション ポリシー マップで SIP ヘッダー フィールドの厳密な検証をイネーブルにする例を示します。

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# strict-header-validation action log
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

strict-http

HTTP に準拠していないトラフィックの転送を許可するには、HTTP マップ コンフィギュレーション モードで **strict-http** コマンドを使用します。このモードには **http-map** コマンドを使用してアクセスできます。この機能をデフォルトの動作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。

strict-http action { **allow | reset | drop** } [**log**]
no strict-http action action { **allow | reset | drop** } [**log**]

構文の説明

action	メッセージがこのコマンド インスペクションに合格しなかったときに実行されるアクションです。
allow	メッセージを許可します。
drop	接続を閉じます。
log	（任意）syslog を生成します。
reset	クライアントおよびサーバーに TCP リセット メッセージを送信して接続を閉じます。

コマンド デフォルト

このコマンドは、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

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
HTTP マップ 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

厳密な HTTP インスペクションをディセーブルにすることはできませんが、**strict-http action allow** コマンドを使用すると、HTTP に準拠していないトラフィックの転送が ASA で許可されます。このコマンドによって、デフォルトの動作（HTTP に準拠していないトラフィックの転送を拒否する）が上書きされます。

例

次に、HTTP に準拠していないトラフィックの転送を許可する例を示します。

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# strict-http allow
ciscoasa(config-http-map)#
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug appfw	拡張HTTPインスペクションに関連するトラフィックの詳細情報を表示します。
http-map	拡張 HTTP インスペクションを設定するための HTTP マップを定義します。
inspect http	アプリケーション インスペクション用に特定の HTTP マップを適用します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

strip-group

このコマンドは、user@realm の形式で受信されるユーザー名にのみ適用されます。レルムは、ユーザー名に「@」デリミタが付加された管理ドメインです（juser@abc）。

グループ除去処理をイネーブルまたはディセーブルにするには、トンネルグループ一般属性モードで **strip-group** コマンドを使用します。ASA では、VPN クライアントによって提示されるユーザー名からグループ名を取得して、IPsec 接続のトンネルグループを選択します。グループ除去処理をイネーブルにすると、ASA では、ユーザー名のユーザー部分のみを認可/認証のために送信します。それ以外の場合（ディセーブルの場合）、ASA ではレルムを含むユーザー名全体を送信します。

グループ除去処理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。

strip-group
no strip-group

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。

コマンド デフォルト

このコマンドのデフォルト設定は、ディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ一般属性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
7.0(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

この属性は、IPsec リモート アクセス トンネル タイプだけに適用できます。

（注） MSCHAPv2 の制限により、MSCHAPv2 を PPP 認証に使用すると、トンネル グループのスイッチングを実行できません。MSCHAPv2 中のハッシュ計算はユーザー名の文字列にバインドされます（ユーザー + 区切り + グループなど）。

例

次に、IPsec リモート アクセス タイプの「remotegrp」という名前のリモート アクセス トンネル グループを設定し、一般コンフィギュレーション モードを開始し、「remotegrp」という名前のトンネル グループをデフォルトのグループ ポリシーとして設定して、そのトンネル グループに対してグループ除去をイネーブルにする例を示します。

```
ciscoasa(config)# tunnel-group remotegrp type IPsec_ra
ciscoasa(config)# tunnel-group remotegrp general
ciscoasa(config-tunnel-general)# default-group-policy remotegrp
ciscoasa(config-tunnel-general)# strip-group
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
group-delimiter	グループ名の解析をイネーブルにし、トンネルのネゴシエーション中に受信したユーザー名からグループ名を解析するときに使用するデリミタを指定します。
show running-config tunnel group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。

strip-realm

レルム除去処理をイネーブルまたはディセーブルにするには、トンネルグループ一般属性コンフィギュレーション モードで **strip-realm** コマンドを使用します。レルム除去処理によって、ユーザー名を認証サーバーまたは認可サーバーに送信するときに、ユーザー名からレルムが削除されます。レルムは、@ デリミタを使用してユーザー名に追加される管理ドメインです（username@realm など）。このコマンドをイネーブルにすると、ASA では、ユーザー名のユーザー部分のみを認可/認証のために送信します。それ以外の場合、ASA ではユーザー名全体を送信します。

レルム除去処理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。

strip-realm
no strip-realm

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。

コマンド デフォルト

このコマンドのデフォルト設定は、ディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ一般属性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
7.0.1	このコマンドが追加されました。

使用上のガイドライン

この属性は、IPsec リモート アクセス トンネル タイプだけに適用できます。

例

次に、IPsec リモート アクセス タイプの「remotegrp」という名前のリモート アクセス トンネル グループを設定し、一般コンフィギュレーション モードを開始し、「remotegrp」という名前のトンネル グループをデフォルトのグループ ポリシーとして設定して、そのトンネル グループに対してレルム除去をイネーブルにする例を示します。

```
ciscoasa(config)# tunnel-group remotegrp type IPsec_ra
ciscoasa(config)# tunnel-group remotegrp general
ciscoasa(config-tunnel-general)# default-group-policy remotegrp
ciscoasa(config-tunnel-general)# strip-real
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。