CHAPTER 16

interface ～ issuer-name コマンド

interface

コンフィギュレーションにインターフェイスを追加してインターフェイス コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **interface** コマンドを使用します。

interface {*vlan <n>* | *mapped_name*}

シンタックスの説明

vlan <n>	マルチコンテキスト モードで、VLAN 名、セキュリティ レベル、および IP アドレスを設定します。
mapped_name	（任意）マルチ コンテキスト モードの場合、**allocate-interface** コマンドを使用して割り当てられたマッピング名を識別します。

デフォルト

このコマンドには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。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。
2.2(1)	このコマンドが変更されました。
3.1(1)	このコマンドが変更され、インターフェイス コンフィギュレーション モードのコマンドを分離するように引数が変更されました。

使用上のガイドライン

マルチモードのシステムでは、FWSM で追加が可能なコンテキストにインターフェイスを割り当てることができます。この場合、手動でインターフェイスを追加する必要はありません。同様に、フェールオーバーまたはステート リンクに VLAN を割り当てると、**interface** コマンドが自動的に追加されます。

シングル モードでは、パラメータを設定するために、特定の VLAN に interface コマンドを入力する必要があります。

インターフェイス コンフィギュレーション モードでは、名前、VLAN、および IP アドレスを指定し、さらにその他のさまざまな設定値を設定できます。スイッチによって FWSM にまだ割り当てられていない VLAN にインターフェイスを追加した場合、そのインターフェイスはダウン ステートになります。FWSM に VLAN を割り当てた時点で、インターフェイスはアップ ステートに変化します。インターフェイス ステートの詳細については、show interface コマンドを参照してください。

allocate-interface コマンドを使用してコンテキストに VLAN を割り当て、インターフェイスがまだ存在していなかった場合、FWSM によってシステム コンフィギュレーションにそのインターフェイスが自動的に追加されます。たとえば、コンテキストに [VLAN 100] を割り当てると、システム コンフィギュレーションに **interface vlan 100** コマンドが追加されます。

failover lan interface *interface_name* **vlan** *vlan* コマンドでは、各モジュールの動作状態を判別するために、アクティブ モジュールとスタンバイ モジュール間の通信に使用する、インターフェイス名および VLAN を指定します。

failover link *interface_name* [**vlan** *vlan*] コマンドでは、ステートフル フェールオーバー インターフェイスに対応するインターフェイス名および VLAN を指定します。ステートフル フェールオーバーのために、アクティブとスタンバイ間のリンクであらゆるプロトコル ステート情報が受け渡されます。

例

次に、インターフェイス コンフィギュレーション モードを開始する例を示します。

```
fwsm(config-if)# interface vlan22
fwsm(config-if)# shutdown
```

関連コマンド

コマンド	説明
allocate-interface	セキュリティ コンテキストにインターフェイスおよびサブインターフェイスを割り当てます。
clear configure interface	インターフェイスに対応するすべてのコンフィギュレーションを消去します。
clear interface	**show interface** コマンドのカウンタを消去します。
show interface	インターフェイスのランタイム ステータスおよび統計情報を表示します。

interface bvi

ブリッジ グループにブリッジ仮想インターフェイスを設定するには、グローバル コンフィギュレーション モードで **interface bvi** コマンドを使用します。ブリッジ仮想インターフェイスの設定を削除するには、このコマンドの **no** 形式を使用します。このコマンドを使用してインターフェイス コンフィギュレーション モードを開始すると、ブリッジ グループの管理用 IP アドレスを設定できます。

interface bvi *bridge_group_number*

no interface bvi *bridge_group_number*

シンタックスの説明

bridge_group_number	ブリッジ グループ番号を 1 ～ 100 の整数で指定します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(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

トランスペアレント ファイアウォールは、内部インターフェイスと外部インターフェイスとで同一ネットワークを接続します。各インターフェイス ペアはブリッジ グループに属します。ブリッジ グループには管理 IP アドレスを割り当てる必要があります。ブリッジ グループごとに異なるネットワークに接続します。ブリッジ グループのトラフィックは、他のブリッジ グループから切り離されます。したがって、FWSM 内部の別のブリッジ グループにトラフィックがルーティングされることはありません。また、FWSM からいったん出なければ、外部ルータで FWSM 内部の別のブリッジ グループにルーティングすることはできません。

ブリッジ グループに各インターフェイスを割り当てるには、**interface vlan** コマンドを使用してからさらに、**bridge-group** コマンドを使用します。ブリッジ グループの管理 IP アドレスを設定するには、**interface bvi** コマンドを使用し、さらに **ip address** コマンドを使用します。管理 IP アドレスが必要なのは、FWSM がシステム メッセージ、AAA サーバとの通信など、FWSM を起点とするトラフィックの送信元アドレスとして、このアドレスを使用するからです。このアドレスは、リモート管理アクセスにも使用できます。

例

次の例では、ブリッジ グループ 1 に VLAN 300 および 301 を割り当て、さらにブリッジ グループ 1 の管理アドレスおよびスタンバイ アドレスを設定します。

```
hostname(config)# interface vlan 300
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# bridge-group 1
hostname(config-if)# interface vlan 301
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# bridge-group 1
hostname(config-if)# interface bvi 1
hostname(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

関連コマンド

コマンド	説明
bridge-group	トランスペアレント ファイアウォール インターフェイスをブリッジ グループにグループ化します。
clear configure interface bvi	ブリッジ仮想インターフェイスの設定を消去します。
interface	インターフェイスを設定します。
ip address	ブリッジ グループの管理 IP アドレスを設定します。
show running-config interface bvi	ブリッジ仮想インターフェイスの設定を表示します。

interface-policy

インターフェイス障害を検出する際のフェールオーバー ポリシーを指定するには、フェールオーバー グループ コンフィギュレーション モードで **interface-policy** 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。

interface-policy *num*[**%**]

no interface-policy *num*[**%**]

シンタックスの説明

num	1 ～ 100（%）または 1 ～インターフェイスの最大数を指定します。
%	（任意）数値 *num* が監視対象インターフェイスの割合であることを指定します。

デフォルト

failover interface-policy コマンドを装置に設定した場合、**interface-policy** フェールオーバー グループ コマンドのデフォルトはその値になります。それ以外の場合、*num* は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(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

引数 *num* とオプション キーワード **%** の間にスペースはありません。

障害の発生したインターフェイスの数が設定されたポリシーの条件を満たし、もう 1 つの FWSM が正常に機能している場合、FWSM は自身を故障とみなして、フェールオーバーが実行されます（アクティブ FWSM に障害が発生した場合）。**monitor-interface** コマンドでモニタ対象として指定されたインターフェイスだけがポリシーのカウントに含まれます。

例

フェールオーバー グループの設定例（部分）を示します。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# interface-policy 25%
hostname(config-fover-group)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
failover group	アクティブ / アクティブ フェールオーバーを行うフェールオーバー グループを定義します。
failover interface-policy	インターフェイス モニタ ポリシーを設定します。
monitor-interface	フェールオーバーのためにモニタするインターフェイスを指定します。

ip address

インターフェイスの IP アドレス（ルーティング モード）またはブリッジ グループの管理アドレス（トランスペアレント モード）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 **ip address** コマンドを使用します。ルーテッド モードの場合、VLAN ID に対してインターフェイス コンフィギュレーション モードを開始します（**interface** コマンド）。トランスペアレント モードの場合は、ブリッジ グループに対してインターフェイス コンフィギュレーション モードを開始します（**interface bvi** コマンド）。IP アドレスを削除するには、このコマンドの **no** 形式を使用します。このコマンドで、フェールオーバー用のスタンバイ アドレスも設定します。

ip address *ip_address* [*mask*] [***standby*** *ip_address*]

no ip address [*ip_address*]

シンタックスの説明

ip_address	インターフェイスの IP アドレス（ルーテッド モード）またはブリッジ グループの管理 IP アドレス（トランスペアレント モード）を設定します。
mask	（任意）IP アドレスのサブネット マスクを設定します。マスクを設定しなかった場合、FWSM は IP アドレス クラスのデフォルト マスクを使用します。 トランスペアレント ファイアウォールにホスト アドレス（/32 または 255.255.255.255）を割り当てないでください。また、/30　サブネット（255.255.255.252）など、ホスト アドレス数が 3（アップストリーム ルータ、ダウンストリーム ルータ、およびトランスペアレント ファイアウォールに 1 つずつ）に満たないその他のサブネットを使用しないでください。FWSM は、サブネットの先頭アドレスと最終アドレスとの間で送受信されるすべての ARP パケットをドロップします。たとえば、/30 サブネットを使用し、そのサブネットからアップストリーム ルータへの予約アドレスを割り当てた場合、FWSM はダウンストリーム ルータからアップストリーム ルータへの ARP 要求をドロップします。
standby *ip_address*	（任意）フェールオーバー用スタンバイ装置の IP アドレスを設定します。スタンバイ IP アドレスは、メイン IP アドレスと同じサブネット上になければなりません。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
2.2(1)	このコマンドが追加されました。
3.1(1)	このコマンドがグローバル コンフィギュレーション コマン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 コマンドに変更されました。

使用上のガイドライン

シングル コンテキスト ルーテッド ファイアウォール モードでは、各インターフェイス アドレスがそれぞれ固有のサブネットになければなりません。マルチコンテキスト モードでは、このインターフェイスが共有インターフェイス上にある場合、各 IP アドレスは固有でなければなりませんが、同一サブネット上にあってもかまいません。インターフェイスが固有の場合は、必要に応じて他のコンテキスト間でこの IP アドレスを共有できます。

トランスペアレント ファイアウォール モードでは、各インターフェイス ペアはブリッジ グループに属します。ブリッジ グループには管理 IP アドレスを割り当てる必要があります。ブリッジ グループごとに異なるネットワークに接続します。管理 IP アドレスが必要なのは、FWSM がシステム メッセージ、AAA サーバとの通信など、FWSM を起点とするトラフィックの送信元アドレスとして、このアドレスを使用するからです。このアドレスは、リモート管理アクセスにも使用できます。このアドレスは、アップストリーム ルータおよびダウンストリーム ルータと同じサブネット上になければなりません。

例

次に、2 つのインターフェイスの IP アドレスおよびスタンバイ アドレスを設定する例を示します。

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
hostname(config-if)# interface vlan 200
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.2.1 255.255.255.0 standby 10.1.2.2
```

次のトランスペアレント ファイアウォールの例では、ブリッジ グループ 1 に VLAN 300 および 301 を割り当て、さらにブリッジ グループ 1 の管理アドレスおよびスタンバイ アドレスを設定します。

```
hostname(config)# interface vlan 300
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# bridge-group 1
hostname(config-if)# interface vlan 301
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# bridge-group 1
hostname(config-if)# interface bvi 1
hostname(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

関連コマンド

コマンド	説明
interface bvi	トランスペアレント ファイアウォール ブリッジ グループを設定します。
bridge-group	ブリッジ グループにインターフェイスを割り当てます。
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。
ip address dhcp	DHCP サーバから IP アドレスを取得するように、インターフェイスを設定します。
show ip address	インターフェイスに割り当てられた IP アドレスを表示します。

ip-address

登録時の証明書に FWSM の IP アドレスを含めるには、crypto ca トラストポイント コンフィギュレーション モードで **ip-address** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

ip-address *ip-address*

no ip-address

シンタックスの説明

ip-address	FWSM の IP アドレスを指定します。

デフォルト

IP アドレスを含めないのがデフォルトの設定です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

例

次に、トラストポイント central に対して crypto ca トラストポイント コンフィギュレーション モードを開始し、トラストポイント central に対する登録要求に FWSM の IP アドレスを含める例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# ip-address 209.165.200.225
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルトに戻します。

ip-address-privacy

IP アドレス プライバシ機能をイネーブルにするには、SIP マップ コンフィギュレーション モードで ip-address-privacy コマンドを使用します。IP アドレス プライバシ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。

ip-address-privacy

no ip-address-privacy

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
FWSM 3.1	このコマンドが追加されました。

使用上のガイドライン

IP アドレス プライバシ機能がイネーブルで、なおかつ、IP Phone コールまたはインスタント メッセージング セッションに関与している 2 つの SIP エンド ポイントが同じ内部ファイアウォール インターフェイスを使用して、外部ファイアウォール インターフェイス上の対応する SIP プロキシ サーバと通信する場合、すべての SIP シグナリング メッセージが SIP プロキシ サーバを経由します。

IP アドレス プライバシ機能をイネーブルにできるのは、SIP over TCP または SIP over UDP アプリケーション検査がイネーブルの場合です。デフォルトでは、この機能はディセーブルです。IP アドレス プライバシ機能がイネーブルの場合、FWSM は着信 SIP トラフィックの TCP または UDP ペイロードに組み込まれた内部および外部ホスト IP アドレスを変換しません。これらの IP アドレスに対応する変換規則は無視されます。

例

次に、SIP トラフィックを識別し、SIP マップを定義し、ポリシーを定義して外部インターフェイスに適用する例を示します。

```
hostname(config)# access-list sip-acl permit tcp any any eq 5060
hostname(config)# class-map sip-port
hostname(config-cmap)# match access-list sip-acl
hostname(config-cmap)# sip-map inbound_sip
hostname(config-sip-map)# ip-address-privacy
hostname(config-sip-map)# policy-map S1_policy
hostname(config-pmap)# class sip-port
hostname(config-pmap-c)# inspect sip s1_policy
```

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。
inspect sip	SIP アプリケーション検査をイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを対応付けます。
sip-map	SIP アプリケーション検査 マップを定義します。

ip local pool

VPN リモート アクセス トンネルに使用する IP アドレス プールを設定するには、グローバル コンフィギュレーション モードで **ip local pool** コマンドを使用します。アドレス プールを削除するには、このコマンドの **no** 形式を使用します。

ip local pool *poolname first-address — last-address* [***mask*** *mask*]

no ip local pool *poolname*

シンタックスの説明

first-address	IP アドレス範囲の開始アドレスを指定します。
last-address	IP アドレス範囲の最終アドレスを指定します。
mask *mask*	（任意）アドレス プールのサブネット マスクを指定します。
poolname	IP アドレス プール名を指定します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドのサポートが追加されました。

使用上のガイドライン

非標準ネットワークに所属する VPN クライアントに IP アドレスを割り当てた場合は、マスク値を指定する必要があります。デフォルトのマスクを使用すると、正しくルーティングされない可能性があります。IP ローカル プールに 10.10.10.0/255.255.255.0 のアドレスが含まれている場合が典型的な例です。これはデフォルトでクラス A ネットワークだからです。この場合、VPN クライアントがさまざまなインターフェイスを介して 10 ネットワーク内の異なるサブネットにアクセスしなければならないときに、ある種のルーティング問題が生じる可能性があります。たとえば、アドレス 10.10.100.1/255.255.255.0 のプリンタはインターフェイス 2 を介して使用するが、10.10.10.0 のネットワークは VPN トンネルを介して使用するというインターフェイス 1 の場合、プリンタを宛先とするデータのルーティング先に関して、VPN クライアントに混乱が生じます。10.10.10.0 および 10.10.100.0 のサブネットはどちらも 10.0.0.0 クラス A ネットワークに属すので、プリンタ データを VPN トンネル経由で送信する可能性があります。

例

次に、firstpool という IP アドレス プールを設定する例を示します。開始アドレスは 10.20.30.40 です。終了アドレスは 10.20.30.50 です。ネットワーク マスクは 255.255.255.0 です。

```
hostname(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
```

関連コマンド

コマンド	説明
clear configure ip local pool	すべての IP ローカル プールを削除します。
show running-config ip local pool	IP プールの設定を表示します。特定の IP アドレス プールを指定する場合は、コマンドに名前を含めます。

ip verify reverse-path

ユニキャスト Reverse Path Forwarding（RPF）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 **ip verify reverse-path** 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。ユニキャスト RPF は、ルーティング テーブルに基づいて、すべてのパケットに有効な送信元インターフェイスと一致する送信元 IP アドレスがあることを保証することによって、IP スプーフィング（パケットで不正な送信元 IP アドレスを使用して真の送信元がわからないようにする）から保護します。

ip verify reverse-path interface *interface_name*

no ip verify reverse-path interface *interface_name*

シンタックスの説明

interface_name	ユニキャスト RPF をイネーブルにするインターフェイス

デフォルト

この機能は、デフォルトでディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(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

FWSM は通常、パケットの転送先を判別するときに、宛先アドレスだけを調べます。ユニキャスト RPF は、送信元アドレスも調べるように FWSM に指示します。これが Reverse Path Forwarding と呼ばれる理由です。FWSM を通過させるあらゆるトラフィックに関して、FWSM のルーティング テーブルに送信元アドレスに戻るルートを指定する必要があります。詳細については、RFC 2267 を参照してください。

たとえば、外部トラフィックには、FWSM でデフォルト ルートを使用すると、ユニキャスト RPF 保護が可能になります。外部インターフェイスからトラフィックが届き、ルーティング テーブルに送信元アドレスが指定されていなかった場合、FWSM はデフォルト ルートを使用することによって、外部インターフェイスを送信元インターフェイスとして正しく識別できます。

ルーティング テーブルに指定されているが、内部インターフェイスに対応付けられているアドレスから外部インターフェイスにトラフィックが届いた場合、FWSM はパケットをドロップします。未知の送信元アドレスから内部インターフェイスにトラフィックが届いた場合も同様に、FWSM はパケットをドロップします。対応するルート（デフォルト ルート）が外部インターフェイスを示すからです。

ユニキャスト RPF は次のように実装されます。

- ICMP パケットにはセッションが含まれないため、各パケットがチェックされます。
- UDP および TCP にはセッションが含まれるため、先頭パケットではリバース ルート検索が必要です。セッション中に着信する後続パケットは、セッションの一部として維持される既存のステートを使用してチェックされれます。先頭以外のパケットでは、先頭パケットで使用されたインターフェイスと同じインターフェイスに着信したかどうかが調べられます。

例

次に、外部インターフェイス上でユニキャスト RPF をイネーブルにする例を示します。

```
hostname(config)# ip verify reverse-path interface outside
```

関連コマンド

コマンド	説明
clear configure ip verify reverse-path	**ip verify reverse-path** 設定を消去します。
clear ip verify statistics	ユニキャスト RPF 統計情報を消去します。
show ip verify statistics	ユニキャスト RPF 統計情報を表示します。
show running-config ip verify reverse-path	**ip verify reverse-path** のコンフィギュレーションを表示します。

ip-comp

LZS IP 圧縮をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **ip-comp enable** コマンドを使用します。IP 圧縮をディセーブルにするには、**ip-comp disable** 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 **ip-comp** 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。その結果、別のグループ ポリシーから値を継承できるようになります。

ip-comp {**enable** | **disable**}

no ip-comp

シンタックスの説明

disable	IP 圧縮をディセーブルにします。
enable	IP 圧縮をイネーブルにします。

デフォルト

IP 圧縮はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(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

データ圧縮をイネーブルにすると、モデムに接続するリモート ダイヤルイン ユーザにとって、データ転送速度が上がる可能性があります。

注意　データ圧縮を使用すると、各ユーザ セッションに必要なメモリ容量が増え、CPU 使用率が上がるので、FWSM 全体としてのスループットは下がります。したがって、モデムに接続するリモート ユーザに限定して、データ圧縮をイネーブルにすることを推奨します。モデム ユーザに固有のグループ ポリシーを作成し、モデム ユーザに限定して圧縮をイネーブルにしてください。

例

次に、[FirstGroup] というグループ ポリシーに対して IP 圧縮をイネーブルにする例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ip-comp enable
```

ip-phone-bypass

IP Phone バイパスをイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **ip-phone-bypass enable** コマンドを使用します。IP Phone バイパスをディセーブルにするには、**ip-phone-bypass disable** 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 IP Phone バイパス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。このオプションを使用すると、別のグループ ポリシーから IP Phone バイパスの値を継承できます。

IP Phone バイパス機能を使用すると、ハードウェア クライアントの背後の IP Phone はユーザ認証プロセスをたどらずに接続できます。イネーブルにした場合でも、セキュア ユニット認証は引き続き有効です。

ip-phone-bypass {**enable** | **disable**}

no ip-phone-bypass

シンタックスの説明

disable	IP Phone バイパスをディセーブルにします。
enable	IP Phone バイパスをイネーブルにします。

デフォルト

IP Phone バイパスはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(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

IP Phone バイパスを設定する必要があるのは、ユーザ認証をイネーブルにしている場合だけです。

例

次に、FirstGroup というグループ ポリシーに対して IP Phone バイパスをイネーブルにする例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ip-phone-bypass enable
```

関連コマンド

コマンド	説明
user-authentication	ハードウェア クライアントの背後にいるユーザに、FWSM の認証を受けてから接続することを要求します。

ipsec-udp

IPSec over UDP をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **ipsec-udp enable** コマンドを使用します。IPSec over UDP をディセーブルにするには、**ipsec-udp disable** 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 IPSec over UDP 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。その結果、別のグループ ポリシーから IPSec over UDP の値を継承できるようになります。

IPSec over UDP（別名、IPSec through NAT）を使用すると、シスコ VPN クライアントまたはハードウェア クライアントは、NAT が動作している FWSM に UDP を使用して接続することになります。

ipsec-udp {enable | disable}

no ipsec-udp

シンタックスの説明

disable	IPSec over UDP をディセーブルにします。
enable	IPSec over UDP をイネーブルにします。

デフォルト

IPSec over UDP はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(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

IPSec over UDP を使用するには、**ipsec-udp-port** コマンドも設定する必要があります。

シスコ VPN クライアントも、IPSec over UDP を使用するように設定する必要があります（デフォルトで使用する設定になります）。VPN 3002 の場合、IPSec over UDP を使用する設定は不要です。

IPSec over UDP は独自仕様であり、適用されるのはリモート アクセス接続だけです。また、モードの設定が必要です。すなわち、FWSM は SA のネゴシエーション時に、クライアントとコンフィギュレーション パラメータを交換します。

IPSec over UDP を使用すると、システム パフォーマンスが多少低下する可能性があります。

例

次に、FirstGroup というグループ ポリシーに対して IPSec over UDP を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp enable
```

関連コマンド

コマンド	説明
ipsec-udp-port	FWSM が UDP トラフィックを待ち受けるポートを指定します。

ipsec-udp-port

IPSec over UDP に対応する UDP ポート番号を設定するには、グループ ポリシー コンフィギュレーション モードで **ipsec-udp-port** コマンドを使用します。UDP ポート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。その結果、別のグループ ポリシーから IPSec over UDP ポートの値を継承できるようになります。

IPSec のネゴシエーション時に、FWSM は設定されたポートで待ち受け、他のフィルタ ルールで UDP トラフィックがドロップされる場合であっても、そのポートの UDP トラフィックを転送します。

ipsec-udp-port *port*

no ipsec-udp-port

シンタックスの説明

port	4001 ～ 49151 の整数を使用して、UDP ポート番号を指定します。

デフォルト

デフォルト ポートは 10000 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(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

この機能をイネーブルにして、複数のグループ ポリシーを設定できます。また、グループ ポリシーごとに異なるポート番号を使用できます。

例

次に、FirstGroup というグループ ポリシーに対して IPSec UDP ポートを 4025 に設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp-port 4025
```

関連コマンド

コマンド	説明
ipsec-udp	シスコ VPN クライアントまたはハードウェア クライアントに、UDP を使用して NAT が動作している FWSM に接続させます。

ipv6 access-list

IPv6 アクセス リストを設定するには、グローバル コンフィギュレーション モードで **ipv6 access-list** コマンドを使用します。ACE を削除するには、このコマンドの **no** 形式を使用します。アクセス リストでは、FWSM に通過またはブロックさせるトラフィックを定義します。

ipv6 access-list *id* [***line*** *line-num*] {***deny*** | ***permit***} {*protocol* | ***object-group*** *protocol_obj_grp_id*} {*source-ipv6-prefix*/*prefix-length* | ***any*** | ***host*** *source-ipv6-address* | ***object-group*** *network_obj_grp_id*} [*operator* {*port* [*port*] | ***object-group*** *service_obj_grp_id*}] {*destination-ipv6-prefix*/*prefix-length* | ***any*** | ***host*** *destination-ipv6-address* | ***object-group*** *network_obj_grp_id*} [{*operator port* [*port*] | ***object-group*** *service_obj_grp_id*}] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

no ipv6 access-list *id* [***line*** *line-num*] {***deny*** | ***permit***} {*protocol* | ***object-group*** *protocol_obj_grp_id*} {*source-ipv6-prefix*/*prefix-length* | ***any*** | ***host*** *source-ipv6-address* | ***object-group*** *network_obj_grp_id*} [*operator* {*port* [*port*] | ***object-group*** *service_obj_grp_id*}] {*destination-ipv6-prefix*/*prefix-length* | ***any*** | ***host*** *destination-ipv6-address* | ***object-group*** *network_obj_grp_id*} [{*operator port* [*port*] | ***object-group*** *service_obj_grp_id*}] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

ipv6 access-list *id* [***line*** *line-num*] {***deny*** | ***permit***} ***icmp6*** {*source-ipv6-prefix*/*prefix-length* | ***any*** | ***host*** *source-ipv6-address* | ***object-group*** *network_obj_grp_id*} {*destination-ipv6-prefix*/*prefix-length* | ***any*** | ***host*** *destination-ipv6-address* | ***object-group*** *network_obj_grp_id*} [*icmp_type* | ***object-group*** *icmp_type_obj_grp_id*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

no ipv6 access-list *id* [***line*** *line-num*] {***deny*** | ***permit***} ***icmp6*** {*source-ipv6-prefix*/*prefix-length* | ***any*** | ***host*** *source-ipv6-address* | ***object-group*** *network_obj_grp_id*} {*destination-ipv6-prefix*/*prefix-length* | ***any*** | ***host*** *destination-ipv6-address* | ***object-group*** *network_obj_grp_id*} [*icmp_type* | ***object-group*** *icmp_type_obj_grp_id*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

シンタックスの説明

any	IPv6 のプレフィクス ::/0 の省略形です。あらゆる IPv6 アドレスを意味します。
default	（任意）ACE に対して Syslog メッセージ 106100 を生成することを指定します。
deny	条件に一致した場合、アクセスを拒否します。
destination-ipv6-address	トラフィックを受信するホストの IPv6 アドレス
destination-ipv6-prefix	トラフィックの宛先となる IPv6 ネットワーク アドレス
disable	（任意）Syslog メッセージ生成をディセーブルにします。
host	アドレスが特定のホストを示すことを意味します。
icmp6	FWSM を通過する ICMPv6 トラフィックにアクセス ルールが適用されることを指定します。

icmp_type	アクセス ルールでフィルタリングする ICMP メッセージのタイプを指定します。値は有効な ICMP タイプ番号（0 ～ 255）または次の ICMP タイプ文字表記のいずれか 1 つです。 • destination-unreachable • packet-too-big • time-exceeded • parameter-problem • echo-request • echo-reply • membership-query • membership-report • membership-reduction • router-renumbering • router-solicitation • router-advertisement • neighbor-solicitation • neighbor-advertisement • neighbor-redirect *icmp_type* 引数を指定しなかった場合は、すべての ICMP タイプという意味になります。
icmp_type_obj_grp_id	（任意）オブジェクト グループの ICMP タイプ ID を指定します。
id	アクセス リストの名前または番号
interval *secs*	（任意）Syslog メッセージ 106100 を生成する時間間隔を指定します。有効値は 1 ～ 600 秒です。デフォルトのインターバルは 300 秒です。この値は、非アクティブ フローを削除するタイムアウト値としても使用されます。
level	（任意）メッセージ 106100 に対応する Syslog レベルを指定します。有効な値は 0 ～ 7 です。デフォルトのレベルは 6（通知）です。
line *line-num*	（任意）アクセス ルールを挿入するリストのライン番号。ライン番号を指定しなかった場合、ACE はアクセス リストの末尾に追加されます。
log	（任意）ACE のロギング アクションを指定します。**log** キーワードを指定しなかった場合、または **log default** キーワードを指定した場合は、ACE によってパケットが拒否されたときに、メッセージ 106023 が生成されます。log キーワードを単独で指定するか、level または interval とともに指定した場合は、ACE によってパケットが拒否されたときに、メッセージ 106100 が生成されます。アクセス リストの最後にある暗黙の拒否によって拒否されたパケットはログに記録されません。ロギングをイネーブルにするには、ACE でパケットを明示的に拒否する必要があります。
network_obj_grp_id	既存のネットワーク オブジェクト グループ ID
object-group	（任意）オブジェクト グループを指定します。
operator	（任意）送信元 IP アドレスと宛先 IP アドレスを比較するためのオペランドを指定します。*operator* は、送信元 IP アドレスまたは宛先 IP アドレスのポートを比較します。使用できるオペランドは、**lt**（小なり）、**gt**（大なり）**eq**（同値）、**neq**（非同値）、および **range**（範囲）です。すべてのポートを含めるには（デフォルト）、演算子とポートを指定しないで **ipv6 access-list** コマンドを使用します。

permit	条件に一致した場合、アクセスを許可します。
port	（任意）アクセスを許可または拒否するポートを指定します。*protocol* が ***tcp*** または ***udp*** の場合、*port* 引数を入力するときに、0 ～ 65535 の値またはリテラル名でポートを指定できます。 使用できる TCP のリテラル名は、**aol**、**bgp**、**chargen**、**cifc**、**citrix-ica**、**cmd**、**ctiqbe**、**daytime**、**discard**、**domain**、**echo**、**exec**、**finger**、**ftp**、**ftp-data**、**gopher**、**h323**、**hostname**、**http**、**https**、**ident**、**irc**、**kerberos**、**klogin**、**kshell**、**ldap**、**ldaps**、**login**、**lotusnotes**、**lpd**、**netbios-ssn**、**nntp**、**pop2**、**pop3**、**pptp**、**rsh**、**rtsp**、**smtp**、**sqlnet**、**ssh**、**sunrpc**、**tacacs**、**talk**、**telnet**、**uucp**、**whois**、および **www** です。 使用できる UDP のリテラル名は、**biff**、**bootpc**、**bootps**、**cifs**、**discard**、**dnsix**、**domain**、**echo**、**http**、**isakmp**、**kerberos**、**mobile-ip**、**nameserver**、**netbios-dgm**、**netbios-ns**、**ntp**、**pcanywhere-status**、**pim-auto-rp**、**radius**、**radius-acct**、**rip**、**secureid-udp**、**snmp**、**snmptrap**、**sunrpc**、**syslog**、**tacacs**、**talk**、**tftp**、**time**、**who**、**www**、および **xdmcp** です。
prefix-length	IPv6 プレフィクス（IPv6 アドレスのネットワーク部分）を形成するアドレスの連続する上位ビット数を指定します。
protocol	IP プロトコルの名前または番号。有効値は、**icmp**、**ip**、**tcp**、**udp**、または IP プロトコル番号を表す 1 ～ 254 の整数です。
protocol_obj_grp_id	既存のプロトコル オブジェクト グループ ID
service_obj_grp_id	（任意）オブジェクト グループを指定します。
source-ipv6-address	トラフィックを送信するホストの IPv6 アドレス
source-ipv6-prefix	ネットワーク トラフィックの起点となる IPv6 ネットワーク アドレス

デフォルト

log キーワードを指定した場合、Syslog メッセージ 106100 のデフォルト レベルは 6（通知）になります。

デフォルトのロギング間隔は 300 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(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

ipv6 access-list コマンドを使用すると、IPv6 アドレスがポートまたはプロトコルにアクセスすることを許可するか拒否するかを指定できます。各コマンドを ACE といいます。アクセス リスト名が同じ 1 つ以上の ACE をアクセス リストといいます。アクセス リストをインターフェイスに適用するには、**access-group** コマンドを使用します。

FWSM は、アクセス リストで具体的にアクセスが許可されていないかぎり、外部インターフェイスから内部インターフェイスへのすべてのパケットを拒否します。内部インターフェイスから外部インターフェイスへは、具体的にアクセスが拒否されていないかぎり、デフォルトですべてのパケットが許可されます。

IPv6 に固有であることを除き、**ipv6 access-list** コマンドは **access-list** コマンドと同様です。アクセス リストの詳細については、**access-list extended** コマンドの項を参照してください。

ipv6 access-list icmp コマンドは、FWSM を通過する ICMPv6 メッセージをフィルタリングする場合に使用します。特定のインターフェイスを起点および終点にできる ICMPv6 トラフィックを設定するには、**ipv6 icmp** コマンドを使用します。

オブジェクト グループの設定方法については、**object-group** コマンドの項を参照してください。

例

次に、TCP を使用するあらゆるホストから 3001:1::203:A0FF:FED6:162D サーバにアクセスできるようにする例を示します。

```
hostname(config)# ipv6 access-list acl_grp permit tcp any host
3001:1::203:A0FF:FED6:162D
```

次に、**eq** およびポートを使用して、FTP へのアクセスだけを拒否する例を示します。

```
hostname(config)# ipv6 access-list acl_out deny tcp any host
3001:1::203:A0FF:FED6:162D eq ftp
hostname(config)# access-group acl_out in interface inside
```

次に、**lt** を使用して、ポート番号が 2025 未満のすべてのポートにアクセスできるようにする例を示します。この場合、well-known ポート（1 ～ 1024）へのアクセスが許可されます。

```
hostname(config)# ipv6 access-list acl_dmz1 permit tcp any host
3001:1::203:A0FF:FED6:162D lt 1025
hostname(config)# access-group acl_dmz1 in interface dmz1
```

関連コマンド

コマンド	説明
access-group	インターフェイスにアクセス リストを割り当てます。
ipv6 icmp	FWSM のインターフェイスで終端する ICMP メッセージのアクセス ルールを設定します。
object-group	オブジェクト グループ（アドレス、ICMP タイプ、およびサービス）を作成します。

ipv6 access-list remark

IPv6 アクセス リストにコメントを追加するには、グローバル コンフィギュレーション モードで **ipv6 access-list remark** コマンドを使用します。コメントを削除するには、このコマンドの **no** 形式を使用します。

ipv6 access-list *id* [***line*** *line-num*] **remark** *text*

no ipv6 access-list *id* [***line*** *line-num*] **remark** [*text*]

シンタックスの説明

id	IPv6 アクセス リストの名前
line *line-num*	（任意）コメントを挿入するライン番号
remark text	コメントのテキスト

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(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

コメント テキストは、スペースと句読点を含めて最長 100 文字です。100 文字を超えてコメントを入力した場合、100 番めの文字で切り捨てられます。コメント テキストには、スペース以外の文字を 1 つ以上含める必要があります。空のコメントを入力することはできません。各アクセス リストに複数のコメントを入力できます。

コメントだけからなる ACL には **access-group** コマンドを使用できません。

例

次に、**ipv6 access-list** コマンドの前後に追加するコメント テキストを指定する例を示します。

```
hostname(config)# ipv6 access-list example remark this access list should not be used
```

関連コマンド

コマンド	説明
access-group	インターフェイスにアクセス リストをバインドします。
clear configure ipv6 access-list	実行コンフィギュレーションの IPv6 アクセス リストを消去します。
ipv6 access-list	コンフィギュレーションに IPv6 アクセス リストを追加します。
show ipv6 access-list	IPv6 アクセス リストを表示します。
show running-config ipv6	実行コンフィギュレーションの **ipv6** コマンドを表示します。

ipv6 address

IPv6 をイネーブルにして、インターフェイス上で IPv6 アドレスを設定するには、インターフェイス コンフィギュレーション モードで **ipv6 address** コマンドを使用します。IPv6 アドレスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 address {***autoconfig*** | *ipv6-prefix*/*prefix-length* [***eui-64***] | *ipv6-address* ***link-local***}

no ipv6 address {***autoconfig*** | *ipv6-prefix*/*prefix-length* [***eui-64***] | *ipv6-address* ***link-local***}

シンタックスの説明

autoconfig	インターフェイス上でステートレス自動設定を使用し、IPv6 アドレスの自動設定をイネーブルにします。
eui-64	（任意）IPv6 アドレスの下位 64 ビットでインターフェイス ID を指定します。
ipv6-address	インターフェイスに割り当てる IPv6 リンク ローカル アドレス
ipv6-prefix	インターフェイスに割り当てる IPv6 ネットワーク アドレス
link-local	アドレスがリンク ローカル アドレスであることを指定します。
prefix-length	IPv6 プレフィクス（IPv6 アドレスのネットワーク部分）を形成するアドレスの連続する上位ビット数を指定します。

デフォルト

IPv6 はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(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

インターフェイス上で IPv6 アドレスを設定すると、そのインターフェイスで IPv6 がイネーブルになります。したがって、IPv6 アドレスを指定したあとで、**ipv6 enable** コマンドを使用する必要はありません。

ipv6 address *autoconfig* コマンドは、ステートレス自動設定を使用し、インターフェイス上で IPv6 アドレスの自動設定をイネーブルにする場合に使用します。アドレスは、ルータ アドバタイズ メッセージで受信したプレフィクスに基づいて設定されます。リンク ローカル アドレスが設定されていない場合は、このインターフェイス用のリンク ローカル アドレスが 1 つ自動的に生成されます。別のホストがリンク ローカル アドレスを使用している場合は、エラー メッセージが表示されます。

ipv6 address eui-64 コマンドは、インターフェイスに IPv6 アドレスを設定する場合に使用します。オプションの **eui-64** を指定した場合は、アドレスの下位 64 ビットで EUI-64 インターフェイス ID が使用されます。*prefix-length* 引数に指定した値が 64 ビットを超えている場合は、プレフィクス ビットがインターフェイス ID より優先されます。指定したアドレスを別のホストが使用している場合は、エラー メッセージが表示されます。

リンク レイヤ アドレスの上位 3 バイト（OUI フィールド）と下位 3 バイト（シリアル番号）の間に 16 進数 FFFE を挿入すると、48 ビットのリンク レイヤ（MAC）アドレスから修正 EUI-64 形式のインターフェイス ID が作成されます。選択されたアドレスが固有のイーサネット MAC アドレスによるものであることを保証するために、上位バイトの最下位から 2 番めのビットを倒置させ（ユニバーサル / ローカル ビット）、48 ビット アドレスの固有性を示します。たとえば、MAC アドレス 00E0.B601.3B7A のインターフェイスには、02E0:B6FF:FE01:3B7A という 64 ビット インターフェイス ID が与えられます。

ipv6 address ***link-local*** コマンドは、インターフェイスに IPv6 リンク ローカル アドレスを設定する場合に使用します。このコマンドで指定した *ipv6-address* によって、インターフェイス用に自動生成されたリンク ローカル アドレスが上書きされます。リンク ローカル アドレスは、リンク ローカル プレフィクス FE80::/64 と修正 EUI-64 形式のインターフェイス ID で形成されます。MAC アドレス 00E0.B601.3B7A のインターフェイスには、FE80::2E0:B6FF:FE01:3B7A というリンク ローカル アドレスが与えられます。指定したアドレスを別のホストが使用している場合は、エラー メッセージが表示されます。

例

次に、選択したインターフェイスのグローバル アドレスとして、3FFE:C00:0:1::576/64 を割り当てる例を示します。

```
hostname(config)# interface Vlan101
hostname(config-subif)# ipv6 address 3ffe:c00:0:1::576/64
```

次に、選択したインターフェイスに対して、IPv6 アドレスを自動的に割り当てる例を示します。

```
hostname(config)# interface Vlan101
hostname(config-subif)# ipv6 address autoconfig
```

次に、選択したインターフェイスに IPv6 アドレス 3FFE:C00:0:1::/64 を割り当て、アドレスの下位 64 ビットで EUI-64 インターフェイス ID を指定する例を示します。

```
hostname(config)# interface Vlan101
hostname(onfig-if)# ipv6 address 3FFE:C00:0:1::/64 eui-64
```

次に、選択したインターフェイスのリンク レベル アドレスとして、FE80::260:3EFF:FE11:6670 を割り当てる例を示します。

```
hostname(config)# interface Vlan101
hostname(config-subif)# ipv6 address FE80::260:3EFF:FE11:6670 link-local
```

関連コマンド

コマンド	説明
debug ipv6 interface	IPv6 インターフェイスのデバッグ情報を表示します。
show ipv6 interface	IPv6 として設定されたインターフェイスのステータスを表示します。

ipv6 enable

明示的な IPv6 アドレスを指定して設定されていないインターフェイス上で、IPv6 処理を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 **ipv6 enable** コマンドを使用します。明示的な IPv6 アドレスを指定して設定されていないインターフェイス上で、IPv6 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。

ipv6 enable

no ipv6 enable

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

IPv6 はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(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

ipv6 enable コマンドによって、インターフェイス上で IPv6 リンク ローカル ユニキャスト アドレスが自動的に設定され、同時にインターフェイスでの IPv6 処理もイネーブルになります。

no ipv6 enable コマンドを使用しても、明示的な IPv6 アドレスを指定して設定されたインターフェイス上の IPv6 処理はディセーブルになりません。

例

次に、選択したインターフェイス上で IPv6 処理をイネーブルにする例を示します。

```
hostname(config)# interface Vlan101
hostname(config-subif)# ipv6 enable
```

関連コマンド

コマンド	説明
ipv6 address	インターフェイスに IPv6 アドレスを設定し、そのインターフェイス上で IPv6 処理をイネーブルにします。
show ipv6 interface	IPv6 として設定されたインターフェイスの使用可能状況を表示します。

ipv6 icmp

インターフェイスに ICMP アクセス ルールを設定するには、グローバル コンフィギュレーション モードで **ipv6 icmp** コマンドを使用します。ICMP アクセス ルールを削除するには、このコマンドの **no** 形式を使用します。

ipv6 icmp {***permit*** | ***deny***} {*ipv6-prefix*/*prefix-length* | ***any*** | ***host*** *ipv6-address*} [*icmp-type*] *if-name*

no ipv6 icmp {***permit*** | ***deny***} {*ipv6-prefix*/*prefix-length* | ***any*** | ***host*** *ipv6-address*} [*icmp-type*] *if-name*

シンタックスの説明

any	あらゆる IPv6 アドレスを指定するキーワード。IPv6 プレフィクス ::/0 の省略形
deny	選択されたインターフェイス上で、指定の ICMP トラフィックを禁止します。
host	アドレスが特定のホストを示すことを意味します。
icmp-type	アクセス ルールでフィルタリングする ICMP メッセージのタイプを指定します。値は有効な ICMP タイプ番号（0 ～ 255）または次の ICMP タイプ文字表記のいずれか 1 つです。 • echo • echo-reply（エコー応答） • membership-query • membership-reduction • membership-report • neighbor-advertisement • neighbor-redirect • neighbor-solicitation • destination-unreachable • packet-too-big • parameter-problem • router-advertisement • router-renumbering • router-solicitation • time-exceeded • unreachable（到達不能）
if-name	アクセス ルールを適用するインターフェイスの名前（**nameif** コマンドで指定）
ipv6-address	インターフェイスに ICMPv6 メッセージを送信するホストの IPv6 アドレス
ipv6-prefix	インターフェイスに ICMPv6 メッセージを送信する IPv6 ネットワーク
permit	選択されたインターフェイス上で、指定の ICMP トラフィックを許可します。
prefix-length	IPv6 プレフィクスの長さ。この値は、プレフィクスのネットワーク部分を形成するアドレスの連続する上位ビット数を表します。プレフィクス長の前にスラッシュ（/）を指定する必要があります。

デフォルト

ICMP アクセス ルールを定義しなかった場合、すべての ICMP トラフィックが許可されます。

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。

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

コマンド履歴

リリース	変更
3.1(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

機能に関して、IPv6 の ICMP は IPv4 の ICMP と同じです。ICMPv6 は、ICMP 宛先到達不能メッセージ、ICMP のエコー要求や応答メッセージと同様の通知メッセージなど、エラー メッセージを生成します。さらに、IPv6 ネイバー検出プロセスおよびパス MTU 検出で、IPv6 の ICMP パケットが使用されます。

インターフェイスに ICMP ルールを定義しなかった場合は、すべての IPv6 ICMP トラフィックが許可されます。

インターフェイスに ICMP ルールを定義した場合は、最初に一致したものから順にルールが処理され、さらにすべて拒否する暗黙のルールが続きます。たとえば、最初に一致したルールが許可ルールの場合、ICMP パケットは処理されます。最初に一致したルールが拒否ルールの場合、または ICMP パケットがそのインターフェイスのいずれのルールとも一致しなかった場合は、FWSM によって ICMP パケットが廃棄され、Sylog メッセージが生成されます。

したがって、ICMP ルールは入力順序が重要です。特定のネットワークから着信したすべての ICMP トラフィックを拒否するルールを入力し、次にそのネットワーク上の特定のホストから着信した ICMP トラフィックを許可するルールを入力した場合、ホストのルールが処理されることはありません。ネットワークのルールによって ICMP トラフィックがブロックされるからです。しかし、ホストのルールを先に入力し、次にネットワークのルールを入力した場合は、ホストの ICMP トラフィックは許可され、そのネットワークから送られたそれ以外の ICMP トラフィックはすべてブロックされます。

ipv6 icmp コマンドでは、FWSM インターフェイスで終端する ICMP トラフィックのアクセス ルールを設定します。パススルー ICMP トラフィックのアクセス ルールを設定する場合は、**ipv6 access-list** コマンドの項を参照してください。

例

次に、外部インターフェイスで、すべての ping 要求を拒否し、パス MTU 検出をサポートするためにすべての Packet Too Big メッセージを許可する例を示します。

```
hostname(config)# ipv6 icmp deny any echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

次に、ホスト 2000:0:0:4::2 またはプレフィクス 2001::/64 のホストから外部インターフェイスへの ping を許可する例を示します。

```
hostname(config)# ipv6 icmp permit host 2000:0:0:4::2 echo-reply outside
hostname(config)# ipv6 icmp permit 2001::/64 echo-reply outside
```

関連コマンド

コマンド	説明
ipv6 access-list	アクセス リストを設定します。

ipv6 nd dad attempts

重複アドレスが検出されたときに、インターフェイスから連続して送信するネイバー送信請求メッセージの数を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd dad attempts** コマンドを使用します。送信する重複アドレス検出メッセージの数を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。

ipv6 nd dad attempts *value*

no ipv6 nd dad [**attempts** *value*]

シンタックスの説明

value	0 ～ 600 の値。0 を入力すると、指定したインターフェイス上で重複アドレス検出がディセーブルになります。1 を入力すると、1 回だけの送信になり、追加送信は行われません。デフォルトのメッセージ数は 1 です。

デフォルト

デフォルトの試行回数は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(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

重複アドレス検出では、新しいユニキャスト IPv6 アドレスの固有性が確認されてから、インターフェイスにそれらのアドレスが割り当てられます（重複アドレス検出が実行されている間、新しいアドレスは暫定的なステートのままです）。重複アドレス検出では、ネイバー送信請求メッセージを使用して、ユニキャスト IPv6 アドレスの固有性を確認します。ネイバー送信請求メッセージの送信間隔を設定するには、**ipv6 nd ns-interval** コマンドを使用します。

管理上のダウン状態にあるインターフェイスでは、重複アドレス検出が保留されます。インターフェイスが管理上のダウンになっている間、そのインターフェイスに割り当てたユニキャスト IPv6 アドレスは保留ステートに設定されます。

インターフェイスが管理上のアップに戻ると、そのインターフェイスでの重複アドレス検出が自動的に再開されます。インターフェイスが管理上のアップに戻ると、そのインターフェイス上のすべてのユニキャスト IPv6 アドレスに対して、重複アドレス検出が再開されます。

（注） インターフェイスのリンク ローカル アドレスに対して重複アドレス検出が実行されている間、その他の IPv6 アドレスのステートは引き続き暫定として設定されます。リンク ローカル アドレスに対する重複アドレス検出が完了すると、残りの IPv6 アドレスに対して重複アドレス検出が実行されます。

重複アドレス検出で重複アドレスが識別されると、アドレスのステートが DUPLICATE に設定され、そのアドレスは使用されません。重複アドレスがインターフェイスのリンクローカル アドレスの場合、そのインターフェイスでは IPv6 パケットの処理ができなくなり、次のようなエラー メッセージが発行されます。

```
%fwsm-4-DUPLICATE: Duplicate address FE80::1 on outside
```

重複アドレスがインターフェイスのグローバル アドレスの場合、そのアドレスは使用されず、次のようなエラー メッセージが発行されます。

```
%fwsm-4-DUPLICATE: Duplicate address 3000::4 on outside
```

重複アドレスに対応付られたコンフィギュレーション コマンドはすべて、アドレスのステートが DUPLICATE の間も設定されたままです。

インターフェイスのリンク ローカル アドレスが変更されると、新しいリンクローカル アドレスに対して重複アドレス検出が実行され、そのインターフェイスに対応付けられたその他のすべての IPv6 アドレスが再生成されます（重複アドレス検出が実行されるのは、新しいリンク ローカル アドレスに対してだけです）。

例

次に、インターフェイスの暫定ユニキャスト IPv6 アドレスに対して重複アドレス検出を実行するときに、ネイバー送信請求メッセージを連続して 5 回送信するように設定する例を示します。

```
hostname(config)# interface Vlan101
hostname(config-subif)# ipv6 nd dad attempts 5
```

次に、選択したインターフェイスで重複アドレス検出をディセーブルにする例を示します。

```
hostname(config)# interface Vlan101
hostname(config-subif)# ipv6 nd dad attempts 0
```

関連コマンド

コマンド	説明
ipv6 nd ns-interval	インターフェイスにおける IPv6 ネイバー送信請求の送信間隔を設定します。
show ipv6 interface	IPv6 として設定されたインターフェイスの使用可能状況を表示します。

ipv6 nd ns-interval

インターフェイスにおける IPv6 ネイバー送信請求の再送信間隔を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd ns-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。

ipv6 nd ns-interval *value*

no ipv6 nd ns-interval [*value*]

シンタックスの説明

value	ミリ秒単位で表した IPv6 ネイバー送信請求の送信間隔。有効値は 1000 ～ 3600000 ミリ秒です。デフォルト値は 1000 ミリ秒です。

デフォルト

1000 ミリ秒のネイバー送信請求の送信間隔

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(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

この値は、このインターフェイスから送信されるすべての IPv6 ルータ アドバタイズに組み込まれます。

例

次に、Vlan101 の IPv6 ネイバー送信請求の送信間隔を 9000 ミリ秒に設定する例を示します。

```
hostname(config)# interface Vlan101
hostname(config-subif)# ipv6 nd ns-interval 9000
```

関連コマンド

コマンド	説明
show ipv6 interface	IPv6 として設定されたインターフェイスの使用可能状況を表示します。

ipv6 nd prefix

IPv6 ルータ アドバタイズに含める IPv6 プレフィクスを設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd prefix** コマンドを使用します。プレフィクスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 nd prefix *ipv6-prefix/prefix-length* | ***default*** [[*valid-lifetime preferred-lifetime*] | [***at*** *valid-date preferred-date*] | ***infinite*** | ***no-advertise*** | ***off-link*** | ***no-autoconfig***]

no ipv6 nd prefix *ipv6-prefix/prefix-length* | ***default*** [[*valid-lifetime preferred-lifetime*] | [***at*** *valid-date preferred-date*] | ***infinite*** | ***no-advertise*** | ***off-link*** | ***no-autoconfig***]

シンタックスの説明

at *valid-date preferred-date*	ライフタイムおよびプリファレンスが満了する日時。プレフィクスが有効なのは、指定されたこの日時に達するまでです。日付は *date-valid-expire month-valid-expire hh:mm-valid-expire date-prefer-expire month-prefer-expire hh:mm-prefer-expire* の形式で表します。
default	デフォルト値が使用されます。
infinite	（任意）ライフタイムは無期限に有効です。
ipv6-prefix	ルータ アドバタイズに含める IPv6 ネットワーク番号 この引数は、RFC 2373 で規定された形式にする必要があります。コロンで囲んだ 16 ビット値を使用し、16 進数でアドレスを指定します。
no-advertise	（任意）ローカル リンク上のホストに対して、IPv6 自動設定に指定のプレフィクスを使用しないことを指示します。
no-autoconfig	（任意）ローカル リンク上のホストに対して、IPv6 自動設定に指定のプレフィクスを使用できないことを指示します。
off-link	（任意）オンリンクの決定に指定のプレフィクスを使用しないことを指示します。
preferred-lifetime	指定の IPv6 プレフィクスを優先させるものとしてアドバタイズする時間の長さ（秒数）。有効値は 0 ～ 4294967295 秒です。最大値は無限を意味します。infinite として指定することもできます。デフォルトは 604800（7 日）です。
prefix-length	IPv6 プレフィクスの長さ。この値は、プレフィクスのネットワーク部分を形成するアドレスの連続する上位ビット数を表します。プレフィクス長の前にスラッシュ（/）を指定する必要があります。
valid-lifetime	指定の IPv6 プレフィクスを有効なものとしてアドバタイズする時間の長さ。有効値は 0 ～ 4294967295 秒です。最大値は無限を意味します。**infinite** として指定することもできます。デフォルトは 2592000（30 日）です。

デフォルト

IPv6 ルータ アドバタイズの起点となるインターフェイス上で設定されたすべてのプレフィクスは、有効なライフタイムを 2592000 秒（30 日）、優先ライフタイムを 604800 秒（7 日）として、また、[onlink] フラグと [autoconfig] フラグの両方を設定してアドバタイズされます。

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。

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

コマンド履歴

リリース	変更
3.1(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

このコマンドを使用すると、プレフィクスをアドバタイズするかどうかを含め、プレフィクスに基づいて個々のパラメータを制御できます。

デフォルトでは、**ipv6 address** コマンドを使用してインターフェイス上のアドレスとして設定されたプレフィクスがルータ アドバタイズで伝達されます。**ipv6 nd prefix** コマンドを使用してアドバイズ用のプレフィクスを設定した場合は、これらのプレフィクスだけがアドバタイズされます。

default キーワードを使用すると、すべてのプレフィクスにデフォルトのパラメータが設定されます。

日付を設定すると、プレフィクスの有効期限を指定できます。有効ライフタイムおよび優先ライフタイムのカウント ダウンは、リアルタイムで行われます。満了日に達すると、プレフィクスはアドバタイズされなくなります。

オンリンクが [on]（デフォルト）の場合、指定のプレフィクスがリンクに割り当てられます。指定のプレフィクスが含まれているアドレスにトラフィックを送信するノードは、ローカルでリンクに到達できる宛先を検討します。

autoconfig が [on]（デフォルト）の場合は、ローカル リンク上のホストに対して、IPv6 自動設定に指定のプレフィクスを使用できることを伝えます。

例

次に、有効ライフタイムを 1000 秒、優先ライフタイムを 900 秒として、指定のインターフェイスから送信されるルータ アドバタイズに IPv6 プレフィクス 2001:200::/35 を含める例を示します。

```
hostname(config)# interface Vlan101
hostname(config-subif)# ipv6 nd prefix 2001:200::/35 1000 900
```

関連コマンド

コマンド	説明
ipv6 address	インターフェイス上で IPv6 アドレスを設定し、IPv6 処理をイネーブルにします。
show ipv6 interface	IPv6 として設定されたインターフェイスの使用可能状況を表示します。

ipv6 nd ra-interval

インターフェイスにおける IPv6 ルータ アドバタイズの送信間隔を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd ra-interval** コマンドを使用します。デフォルトの間隔に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd ra-interval [***msec***] *value*

no ipv6 nd ra-interval [[***msec***] *value*]

シンタックスの説明

msec	（任意）ミリ秒単位で指定した値であることを示します。このキーワードを指定しなかった場合、値は秒数を表します。
value	IPv6 ルータ アドバタイズの送信間隔。有効値は 3 ～ 1800 秒、または ***msec*** キーワードが指定されている場合、500 ～ 1800000 ミリ秒です。デフォルトは 200 秒です。

デフォルト

デフォルトの値は、200 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(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

ipv6 nd ra-lifetime コマンドを使用して FWSM をデフォルト ルータとして設定している場合、送信間隔は IPv6 ルータ アドバタイズのライフタイム以下にする必要があります。他の IPv6 ノードと同期しないように、指定値の 20% 以内で実際に使用する値をランダムに調整します。

例

次に、選択したインターフェイスに対して、IPv6 ルータ アドバタイズ間隔を 201 秒に設定する例を示します。

```
hostname(config)# interface Vlan101
hostname(config-subif)# ipv6 nd ra-interval 201
```

関連コマンド

コマンド	説明
ipv6 nd ra-lifetime	IPv6 ルータ アドバタイズのライフタイムを設定します。
show ipv6 interface	IPv6 として設定されたインターフェイスの使用可能状況を表示します。

ipv6 nd ra-lifetime

インターフェイスにおける IPv6 ルータ アドバタイズの「ルータ ライフタイム」値を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd ra-lifetime** 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。

ipv6 nd ra-lifetime *seconds*

no ipv6 nd ra-lifetime [*seconds*]

シンタックスの説明

seconds	このインターフェイスにおける、デフォルト ルータとしての FWSM の有効性。有効値は 0 ～ 9000 秒です。デフォルトは 1800 秒です。0 は、選択したインターフェイス上で FWSM をデフォルト ルータとみなさないことを示します。

デフォルト

デフォルトの値は、1800 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(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

「ルータ ライフタイム」値は、インターフェイスから送信されるすべての IPv6 ルータ アドバタイズに組み込まれます。この値は、このインターフェイスにおける、デフォルト ルータとしての FWSM の有効性を示します。

ゼロ以外の値に設定すると、このインターフェイスでは FWSM をデフォルト ルータとみなすことを意味します。ゼロ以外の「ルータ ライフタイム」値をルータ アドバタイズ間隔より小さくしてはなりません。

値をゼロに設定すると、このインターフェイスでは FWSM をデフォルト ルータとみなさないことを意味します。

例

次に、選択したインターフェイスに対して、IPv6 ルータ アドバタイズのライフタイムを 1801 秒に設定する例を示します。

```
hostname(config)# interface Vlan101
hostname(config-subif)# ipv6 nd ra-lifetime 1801
```

関連コマンド

コマンド	説明
ipv6 nd ra-interval	インターフェイスにおける IPv6 ルータ アドバタイズの送信間隔を設定します。
show ipv6 interface	IPv6 として設定されたインターフェイスの使用可能状況を表示します。

ipv6 nd reachable-time

到達可能性確認イベントの発生後、リモート IPv6 ノードを到達可能とみなす時間の長さを設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd reachable-time** コマンドを使用します。デフォルトの時間長に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd reachable-time *value*

no ipv6 nd reachable-time [*value*]

シンタックスの説明

value	リモート IPv6 ノードを到達可能とみなす時間の長さ（ミリ秒単位）。有効値は 0 ～ 3600000 ミリ秒です。デフォルトの値は、0 です。

デフォルト

0 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。

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

コマンド履歴

リリース	変更
3.1(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

時間を設定すると、使用不能なネイバーを検出できます。設定時間を短くすると、使用不能なネイバーをより迅速に検出できますが、時間が短いほど、すべての IPv6 ネットワーク装置で IPv6 ネットワーク帯域と処理リソースの消費量が増します。通常の IPv6 の運用では、設定時間をあまり短くすることは推奨できません。

例

次に、選択したインターフェイスに対して、IPv6 の到達可能時間を 1700000 秒に設定する例を示します。

```
hostname(config)# interface Vlan101
hostname(config-subif)# ipv6 nd reachable-time 1700000
```

関連コマンド

コマンド	説明
show ipv6 interface	IPv6 として設定されたインターフェイスの使用可能状況を表示します。

ipv6 nd suppress-ra

LAN インターフェイスにおける IPv6 ルータ アドバタイズの送信を抑制するには、インターフェイス コンフィギュレーション モードで **ipv6 nd suppress-ra** コマンドを使用します。LAN インターフェイスで IPv6 ルータ アドバタイズを再び送信できるようにするには、このコマンドの **no** 形式を使用します。

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

IPv6 ユニキャスト ルーティングがイネーブルの場合は、LAN インターフェイス上でルータ アドバタイズが自動的に送信されます。

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。

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

コマンド履歴

リリース	変更
3.1(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

no ipv6 nd suppress-ra コマンドは、非 LAN インターフェイス タイプ（シリアル インターフェイス、トンネル インターフェイスなど）で IPv6 ルータ アドバタイズを送信できるようにする場合に使用します。

例

次に、選択したインターフェイス上で IPv6 ルータ アドバタイズを抑制する例を示します。

```
hostname(config)# interface Vlan101
hostname(config-subif)# ipv6 nd suppress-ra
```

関連コマンド

コマンド	説明
show ipv6 interface	IPv6 として設定されたインターフェイスの使用可能状況を表示します。

ipv6 neighbor

IPv6 ネイバー検出キャッシュにスタティック エントリを設定するには、グローバル コンフィギュレーション モードで **ipv6 neighbor** コマンドを使用します。ネイバー検出キャッシュからスタティック エントリを削除するには、このコマンドの **no** 形式を使用します。

ipv6 neighbor *ipv6_address if_name mac_address*

no ipv6 neighbor *ipv6_address if_name* [*mac_address*]

シンタックスの説明

if_name	**nameif** コマンドで指定された内部または外部インターフェイス名
ipv6_address	ローカル データリンク アドレスに対応する IPv6 アドレス
mac_address	ローカル データ回線（ハードウェア MAC）アドレス

デフォルト

IPv6 ネイバー検出キャッシュにスタティック エントリを設定しません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(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

ipv6 neighbor コマンドは **arp** コマンドに類似しています。指定した IPv6 アドレスのエントリがネイバー検出キャッシュにすでに存在する場合（IPv6 ネイバー検出プロセスで学習した場合）、そのエントリはスタティック エントリに自動的に変換されます。これらのエントリは、**copy** コマンドを使用してコンフィギュレーションを保管するときに、コンフィギュレーションに保管されます。

show ipv6 neighbor コマンドは、IPv6 ネイバー検出キャッシュのスタティック エントリを表示する場合に使用します。

clear ipv6 neighbors コマンドを使用すると、IPv6 ネイバー検出キャッシュのエントリがスタティック エントリを除いてすべて削除されます。**no ipv6 neighbor** コマンドを使用すると、指定したスタティック エントリがネイバー検出キャッシュから削除されます。このコマンドを使用しても、IPv6 ネイバー検出プロセスによって学習したダイナミック エントリはキャッシュから削除されません。**no ipv6 enable** コマンドを使用してインターフェイス上で IPv6 をディセーブルにすると、そのインターフェイスに設定されている IPv6 ネイバー検出キャッシュ エントリがスタティック エントリを除いてすべて削除されます。スタティック エントリのステートは INCMP（Incompleted）に変化します。

IPv6 ネイバー検出キャッシュのスタティック エントリがネイバー検出プロセスによって変更されることはありません。

例

次に、ネイバー検出キャッシュに IP アドレス 3001:1::45A、MAC アドレス 0002.7D1A.9472 の内部ホストに対応するスタティック エントリを追加する例を示します。

```
hostname(config)# ipv6 neighbor 3001:1::45A inside 0002.7D1A.9472
```

関連コマンド

コマンド	説明
clear ipv6 neighbors	IPv6 ネイバー検出キャッシュ内のエントリを、スタティック エントリを除いてすべて削除します。
show ipv6 neighbor	IPv6 ネイバー キャッシュ情報を表示します。

ipv6 route

IPv6 ルーティング テーブルに IPv6 ルートを追加するには、グローバル コンフィギュレーション モードで **ipv6 route** コマンドを使用します。IPv6 のデフォルト ルート を削除するには、このコマンドの **no** 形式を使用します。

ipv6 route *if_name ipv6-prefix*/*prefix-length ipv6-address* [*administrative-distance*]

no ipv6 route *if_name ipv6-prefix*/*prefix-length ipv6-address* [*administrative-distance*]

シンタックスの説明

administrative-distance	（任意）ルートの管理距離。デフォルト値は 1 です。この場合、スタティック ルートは接続済みルートを除く、他のあらゆるタイプのルートより優先されます。
if_name	ルートを設定するインターフェイスの名前
ipv6-address	指定のネットワークに到達するために使用できるネクスト ホップの IPv6 アドレス
ipv6-prefix	スタティック ルートの宛先となる IPv6 ネットワーク この引数は、RFC 2373 で規定された形式にする必要があります。コロンで囲んだ 16 ビット値を使用し、16 進数でアドレスを指定します。
prefix-length	IPv6 プレフィクスの長さ。この値は、プレフィクスのネットワーク部分を形成するアドレスの連続する上位ビット数を表します。プレフィクス長の前にスラッシュ（/）を指定する必要があります。

デフォルト

administrative-distance はデフォルトで 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(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

show ipv6 route コマンドは、IPv6 ルーティング テーブルの内容を表示する場合に使用します。

例

次に、管理上の距離を 110 とするネットワーク装置の内部インターフェイス 3FFE:1100:0:CC00::1 に、ネットワーク 7fff::0/32 へのパケットをルーティングする例を示します。

```
hostname(config)# ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1 110
```

関連コマンド

コマンド	説明
debug ipv6 route	IPv6 ルーティング テーブル アップデートおよびルート キャッシュ アップデートのデバッグ メッセージを表示します。
show ipv6 route	IPv6 ルーティング テーブルの現在の内容を表示します。

isakmp am-disable

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

isakmp am-disable

no isakmp am-disable

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトではイネーブルになります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

例

次に、グローバル コンフィギュレーション モードを開始して、着信アグレッシブ モード接続をディセーブルにする例を示します。

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

関連コマンド

コマンド	説明
clear configure isakmp	ISAKMP 設定をすべて消去します。
clear configure isakmp policy	ISAKMP ポリシー設定をすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config isakmp	アクティブなすべての設定を表示します。

isakmp disconnect-notify

ピアへの切断通知をイネーブルにするには、グローバル コンフィギュレーション モードで **isakmp disconnect-notify** コマンドを使用します。切断通知をディセーブルにするには、このコマンドの **no** 形式を使用します。

isakmp disconnect-notify

no isakmp disconnect-notify

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトではディセーブルになります。

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。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

例

次に、グローバル コンフィギュレーション モードを開始して、ピアへの切断通知をイネーブルにする例を示します。

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

関連コマンド

コマンド	説明
clear configure isakmp	ISAKMP 設定をすべて消去します。
clear configure isakmp policy	ISAKMP ポリシー設定をすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config isakmp	アクティブなすべての設定を表示します。

isakmp enable

IPSec ピアが FWSM と通信するインターフェイス上で、ISAKMP ネゴシエーションをイネーブルにするには、グローバル コンフィギュレーション モードで **isakmp enable** コマンドを使用します。インターフェイス上の ISAKMP をディセーブルにするには、このコマンドの **no** 形式を使用します。

isakmp enable *interface-name*

no isakmp enable *interface-name*

シンタックスの説明

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

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドのサポートが FWSM に追加されました。

例

次に、グローバル コンフィギュレーション モードを開始し、内部インターフェイス上で ISAKMP をディセーブルにする例を示します。

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

関連コマンド

コマンド	説明
clear configure isakmp	ISAKMP 設定をすべて消去します。
clear configure isakmp policy	ISAKMP ポリシー設定をすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config isakmp	アクティブなすべての設定を表示します。

isakmp identity

ピアに送信するフェーズ 2 ID 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 **isakmp identity** 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。

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

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

シンタックスの説明

address	ISAKMP 識別情報を交換するホストの IP アドレスを使用します。
auto	接続タイプに基づく ISKMP ネゴシエーションを決定します。事前共有鍵には IP アドレス、証明書の認証には cert DN です。
hostname	ISAKMP 識別情報を交換するホストの完全修飾ドメイン名を使用します（デフォルト）。この名前はホスト名とドメイン名で形成されます。
key-id *key_id_string*	事前共有鍵の検索でリモート ピアに使用させる文字列を指定します。

デフォルト

デフォルトの ISAKMP ID は **isakmp identity hostname** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

例

次に、グローバル コンフィギュレーション モードを開始して、IPSec ピアと通信するインターフェイス上で、接続タイプに基づく ISAKMP ネゴシエーションをイネーブルにする例を示します。

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

関連コマンド

コマンド	説明
clear configure isakmp	ISAKMP 設定をすべて消去します。
clear configure isakmp policy	ISAKMP ポリシー設定をすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config isakmp	アクティブなすべての設定を表示します。

isakmp keepalive

IKE DPD を設定するには、tunnel-group ipsec-attributes コンフィギュレーション モードで **isakmp keepalive** コマンドを使用します。各トンネル グループでは、IKE キープアライブはデフォルトでイネーブルになり、デフォルトのしきい値と再試行回数が使用されます。デフォルトのしきい値と再試行回数を指定し、キープアライブ パラメータをイネーブルに戻すには、このコマンドの ***no*** 形式を使用します。

isakmp keepalive [***threshold*** *seconds*] [***retry*** *seconds*] [**disable**]

no isakmp keepalive disable

シンタックスの説明

disable	デフォルトでイネーブルになる IKE キープアライブ処理をディセーブルにします。
retry *seconds*	キープアライブ応答を受信しなかった場合の再試行間隔を秒数で指定します。範囲は 2 ～ 10 秒です。デフォルトは 2 秒です。
threshold *seconds*	キープアライブ モニタリングを開始するまでに、ピアをアイドル状態にしておくことのできる秒数を指定します。範囲は 10 ～ 3600 秒です。デフォルトは、LAN-to-LAN グループの場合は 10 秒、リモート アクセス グループでは 300 秒です。

デフォルト

リモート アクセス グループの場合、デフォルトはしきい値が 300 秒、再試行が 2 秒です。

LAN-to-LAN グループの場合、デフォルトはしきい値が 10 秒、再試行が 2 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(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

この属性を適用できるタイプは、IPSec リモート アクセスおよび IPSec LAN-to-LAN トンネル グループだけです。

例

次に、config-ipsec コンフィギュレーション モードを開始し、209.165.200.255 という IPSec LAN-to-LAN トンネル グループに対して IKE DPD を設定し、しきい値として 15、再試行間隔として 10 を指定する例を示します。

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-ipsec)# isakmp keepalive threshold 15 retry 10
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されたトンネル グループをすべて消去します。
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 グループ設定を表示します。
tunnel-group-map default-group	**crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリにトンネル グループを対応付けます。

isakmp policy authentication

IKE ポリシー内部の認証方式を指定するには、グローバル コンフィギュレーション モードで **isakmp policy authentication** コマンドを使用します。IKE ポリシーでは、IKE ネゴシエーション用に一連のパラメータを定義します。認証方式を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。

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

no isakmp policy *priority* **authentication**

シンタックスの説明

dsa-sig	認証方式として DSA シグニチャを指定します。
pre-share	認証方式として 事前共有鍵を指定します。
priority	IKE ポリシーを一意のものとして特定し、ポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 が最高、65,534 が最低のプライオリティです。
rsa-sig	認証方式として RSA シグニチャを指定します。 RSA シグニチャは、拒否されることのない IKE ネゴシエーションを実現します。これは基本的に、ピアと IKE ネゴシエーションを行ったかどうかを第三者に証明できることを意味します。

デフォルト

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

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(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

RSA シグニチャを指定した場合は、認証局（CA）から証明書を取得するように FWSM およびピアを設定する必要があります。事前共有鍵を指定した場合は、FWSM およびピア内でこれらの事前共有鍵を個別に設定する必要があります。

例

次に、グローバル コンフィギュレーション モードを開始して、**isakmp policy authentication** コマンドを使用する例を示します。この例では、IKE ポリシー内で 認証方式として RSA シグニチャを使用し、プライオリティ値を 40 に設定します。

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

関連コマンド

コマンド	説明
clear configure isakmp	ISAKMP 設定をすべて消去します。
clear configure isakmp policy	ISAKMP ポリシー設定をすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config isakmp	アクティブなすべての設定を表示します。

isakmp policy encryption

IKE ポリシー内部で使用する暗号化アルゴリズムを指定するには、グローバル コンフィギュレーション モードで **isakmp policy encryption** コマンドを使用します。暗号化アルゴリズムをデフォルト値の **des** に戻すには、このコマンドの **no** 形式を使用します。

isakmp policy *priority* **encryption** {**aes | aes-192| aes-256 | des | 3des**}

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

シンタックスの説明

3des	IKE ポリシーで使用する暗号化アルゴリズムとして Triple DES を指定します。
aes	IKE ポリシーで使用する暗号化アルゴリズムとして、128 ビット鍵の AES を指定します。
aes-192	IKE ポリシーで使用する暗号化アルゴリズムとして、192 ビット鍵の AES を指定します。
aes-256	IKE ポリシーで使用する暗号化アルゴリズムとして、256 ビット鍵の AES を指定します。
des	IKE ポリシーで使用する暗号化アルゴリズムとして、56 ビット DES-CBC を指定します。
priority	Internet Key Exchange（IKE）ポリシーを一意のものとして特定し、ポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 が最高、65,534 が最低のプライオリティです。

デフォルト

ISAKMP ポリシーの暗号化は、**3des** 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。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

例

次に、グローバル コンフィギュレーション モードを開始し、**isakmp policy encryption** コマンドを使用して、IKE ポリシー内で使用するアルゴリズムを 128 ビット鍵の AES 暗号化に設定し、プライオリティ値として 25 を指定する例を示します。

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

次に、グローバル コンフィギュレーション モードを開始し、IKE ポリシー内で使用するアルゴリズムとして 3DES、プライオリティ値として 40 を設定する例を示します。

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

関連コマンド

コマンド	説明
clear configure isakmp	ISAKMP 設定をすべて消去します。
clear configure isakmp policy	ISAKMP ポリシー設定をすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config isakmp	アクティブなすべての設定を表示します。

isakmp policy group

IKE ポリシーの Diffie-Hellman グループを指定するには、グローバル コンフィギュレーション モードで **isakmp policy group** コマンドを使用します。IKE ポリシーでは、IKE ネゴシエーション時に使用する一連のパラメータを定義します。Diffie-Hellman グループ ID を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。

[no] isakmp policy *priority* **group** {**1** | **2** | **5** | **7**}

シンタックスの説明

group 1	IKE ポリシーで 768 ビット Diffie-Hellman group を使用するように指定します。これがデフォルト値です。
group 2	IKE ポリシーで 1024 ビット Diffie-Hellman group 2 を使用するように指定します。
group 5	IKE ポリシーで 1536 ビット Diffie-Hellman group 5 を使用するように指定します。
group 7	IKE ポリシーで Diffie-Hellman group 7 を使用するように指定します。group 7 では IPSec SA 鍵が生成されます。この場合、楕円曲線フィールドのサイズは 163 ビットです。
priority	Internet Key Exchange（IKE; インターネット キー エクスチェンジ）ポリシーを一意のものとして特定し、ポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 が最高、65,534 が最低のプライオリティです。

デフォルト

デフォルトのグループ ポリシーは group 2 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(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

4 つのグループ オプションがあります。768 ビット（DH group 1）、1024 ビット（DH group 2）、1536 ビット（DH group 5）、および DH group 7 です。1024 ビットおよび 1536 ビット Diffie-Hellman グループはセキュリティを強化できますが、実行に必要な CPU 時間が増します。

（注）

Cisco VPN Client Version 3.x 以降では、**isakmp policy** に DH **group 2** を設定する必要があります（DH **group** 1 が設定されていると、Cisco VPN Client が接続できなくなります）。

AES サポートを利用できるのは、VPN-3DES のライセンスが与えられているセキュリティ アプライアンスに限られます。AES が提供する鍵はサイズが大きいので、ISAKMP ネゴシエーションで、**group 1** または **group 2** ではなく、**group 5** の Diffie-Hellman（DH）を使用する必要があります。この場合、**isakmp policy priority group 5** コマンドを使用します。

例

次に、グローバル コンフィギュレーション モードを開始して、**isakmp policy group** コマンドを使用する例を示します。この例では、IKE ポリシー内で group 2 の 1024 ビット Diffie Hellman を使用し、プライオリティ値を 40 に設定します。

```
hostname(config-if)# isakmp policy 40 group 2
```

関連コマンド

コマンド	説明
clear configure isakmp	ISAKMP 設定をすべて消去します。
clear configure isakmp policy	ISAKMP ポリシー設定をすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config isakmp	アクティブなすべての設定を表示します。

isakmp policy hash

IKE ポリシーの ハッシュ アルゴリズムを指定するには、グローバル コンフィギュレーション モードで **isakmp policy hash** コマンドを使用します。IKE ポリシーでは、IKE ネゴシエーション時に使用する一連のパラメータを定義します。

ハッシュ アルゴリズムをデフォルト値の SHA-1 にリセットするには、このコマンドの **no** 形式を使用します。

isakmp policy *priority* **hash** {**md5 | sha**}

no isakmp policy *priority* **hash**

シンタックスの説明

md5	IKE ポリシーで使用するハッシュ アルゴリズムとして MD5（HMAC バリアント）を指定します。
priority	Internet Key Exchange（IKE）ポリシーを一意のものとして特定し、ポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 が最高、65,534 が最低のプライオリティです。
sha	IKE ポリシーで使用するハッシュ アルゴリズムとして SHA-1（HMAC バリアント）を指定します。

デフォルト

デフォルトのハッシュ アルゴリズムは SHA-1（HMAC バリアント）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(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

2 つのハッシュ アルゴリズム オプションがあります。SHA-1 および MD5 です。MD5 は SHA-1 よりもダイジェストが小さく、わずかながら高速です。

例

次に、グローバル コンフィギュレーション モードを開始して、**isakmp policy hash** コマンドを使用する例を示します。この例では、IKE ポリシー内で MD5 ハッシュ アルゴリズムを使用し、プライオリティ値を 40 に設定します。

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

関連コマンド

コマンド	説明
clear configure isakmp	ISAKMP 設定をすべて消去します。
clear configure isakmp policy	ISAKMP ポリシー設定をすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config isakmp	アクティブなすべての設定を表示します。

isakmp policy lifetime

IKE セキュリティ アソシエーションが期限切れになるまでのライフタイムを指定するには、グローバル コンフィギュレーション モードで **isakmp policy lifetime** コマンドを使用します。ピアからライフタイムの提案がない場合は、無限のライフタイムを指定できます。セキュリティ アソシエーションのライフタイムをデフォルトの 86,400 秒（1 日）にリセットするには、このコマンドの **no** 形式を使用します。

isakmp policy *priority* **lifetime** *seconds*

no isakmp policy *priority* **lifetime**

シンタックスの説明

priority	Internet Key Exchange（IKE）ポリシーを一意のものとして特定し、ポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 が最高、65,534 が最低のプライオリティです。
seconds	各セキュリティ アソシエーションが期限切れになるまでの秒数を指定します。有限ライフタイムを提案する場合は、120 ～ 2147483647（秒数）の整数を使用します。無限のライフタイムには 0 を使用します。

デフォルト

デフォルト値は 86,400 秒（1 日）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(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

IKE はネゴシエーションを開始するときに、独自セッションのセキュリティ パラメータについて合意しようとします。さらに、各ピアのセキュリティ アソシエーションが合意したパラメータを参照します。ピアでは、ライフタイムが満了するまで、セキュリティ アソシエーションを保持します。セキュリティ アソシエーションは、期限が切れる前に、後続の IKE ネゴシエーションで再利用できます。これにより、新しい IPSec セキュリティ アソシエーションを設定する時間を短縮できます。ピアは、現在のセキュリティ アソシエーションが期限切れになる前に、新しいセキュリティ アソシエーションのネゴシエーションを行います。

ライフタイムを長くすると、FWSM は以後の IPSec セキュリティ アソシエーションをさらに短時間で設定します。暗号化の強度は十分であり、数分単位という非常に短い間隔で鍵を再設定しなくても、セキュリティを確保できます。デフォルトを受け入れることを推奨します。

（注）　IKE セキュリティ アソシエーションを無限ライフタイムに設定しても、ピアが有限ライフタイムを設定した場合には、ネゴシエーションによってピアの有限ライフタイムが使用されます。
次に、グローバル コンフィギュレーション モードを開始し、**isakmp policy lifetime** コマンドを使用する例を示します。この例では、IKE ポリシー内部の IKE セキュリティ アソシエーションのライフタイムを 50,400 秒（14 時間）に、プライオリティ値を 40 に設定します。

例

次の例では、グローバル コンフィギュレーション モードを開始し、IKE ポリシー内部の IKE セキュリティ アソシエーションのライフタイムを 50,400 秒（14 時間）に、プライオリティ値を 40 に設定します。

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

次の例では、グローバル コンフィギュレーション モードを開始し、IKE セキュリティ アソシエーションを無限ライフタイムに設定します。

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

関連コマンド

clear configure isakmp	ISAKMP 設定をすべて消去します。
clear configure isakmp policy	ISAKMP ポリシー設定をすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config isakmp	アクティブなすべての設定を表示します。

isakmp reload-wait

FWSM をリブートする前に、すべてのアクティブ セッションが自発的に終了するまで待機できるようにするには、グローバル コンフィギュレーション モードで **isakmp reload-wait** コマンドを使用します。アクティブ セッションの終了を待たずに、FWSM のリブートを開始するには、このコマンドの **no** 形式を使用します。

isakmp reload-wait

no isakmp reload-wait

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

例

次に、グローバル コンフィギュレーション モードを開始し、すべてのアクティブ セッションが終了するまで待機してからリブートすることを FWSM に指示する例を示します。

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

関連コマンド

コマンド	説明
clear configure isakmp	ISAKMP 設定をすべて消去します。
clear configure isakmp policy	ISAKMP ポリシー設定をすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config isakmp	アクティブなすべての設定を表示します。

issuer-name

ルール エントリの文字列と比較する DN を CA の証明書から識別するには、CA 証明書マップ コンフィギュレーション モードで **issuer-name** コマンドを使用します。発行元名を削除するには、このコマンドの **no** 形式を使用します。

issuer-name [**attr** *tag*] {**eq** | **ne** | **co** | **nc**} *string*

no issuer-name [**attr** *tag*] {**eq** | **ne** | **co** | **nc**} *string*

シンタックスの説明

attr tag	証明書の DN 文字列のうち、指定された属性値だけをルール エントリ文字列と比較することを指定します。tag の値は次のとおりです。 DNQ = DN 修飾子 GENQ = 世代修飾子 I = イニシャル GN = 名 N = 名前 SN = 姓 IP = IP アドレス SER = シリアル番号 UNAME = 構造化されていない名前 EA = 電子メール アドレス T = 肩書き O = 組織名 L = 地名 SP = 州 / 県 C = 国 OU = 組織単位 CN = 一般名称
co	DN 文字列または指定されたアトリビュートがルール エントリ文字列に含まれていなければならないことを指定します。
eq	DN 文字列または指定されたアトリビュートがルール文字列全体と一致するように指定します。
nc	DN 文字列または指定されたアトリビュートがルール エントリ文字列のサブストリングであってはならないことを指定します。
ne	DN 文字列または指定されたアトリビュートがルール文字列全体と一致しないよう指定します。
string	ルール エントリ情報を指定します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

例

次に、証明書マップ 4 に対して CA 証明書マップ モードを開始し、発行元名を O = central として設定する例を示します。

```
hostname(config)# crypto ca certificate map 4
hostname(ca-certificate-map)# issuer-name attr o eq central
hostname(ca-certificate-map)# exit
```

関連コマンド

コマンド	説明
crypto ca certificate map	CA 証明書マップ モードを開始します。
subject-name（crypto ca 証明書マップ）	ルール エントリの文字列と比較する CA 証明書の DN を識別します。