CHAPTER 16

intercept-dhcp コマンド～ issuer-name コマンド

intercept-dhcp

DHCP 代行受信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 **intercept-dhcp enable** コマンドを使用します。DHCP 代行受信をディセーブルにするには、**intercept-dhcp 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 intercept-dhcp 属性を削除し、ユーザがデフォルトまたはその他のグループ ポリシーから DHCP 代行受信コンフィギュレーションを継承できるようにするには、**no intercept-dhcp** コマンドを使用します。

intercept-dhcp *netmask* {**enable | disable**}

no intercept-dhcp

構文の説明

disable	DHCP 代行受信をディセーブルにします。
enable	DHCP 代行受信をイネーブルにします。
netmask	トンネル IP アドレスのサブネット マスクを提供します。

デフォルト

DHCP 代行受信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	透過	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

スプリット トンネル オプションが 255 バイトを超えていると、Microsoft XP で異常が発生し、ドメイン名が破損します。この問題を回避するには、セキュリティ アプライアンスで送信ルートの数を 27 ～ 40 に制限します。ルートの数はルートのクラスによって異なります。

DHCP 代行受信によって Microsoft XP クライアントは、セキュリティ アプライアンスでスプリット トンネリングを使用できるようになります。セキュリティ アプライアンスは、Microsoft Windows XP クライアント DHCP Inform メッセージに直接応答して、クライアントにトンネル IP アドレス用のサブネット マスク、ドメイン名、およびクラスレス スタティック ルートを提供します。Windows クライアントが XP 以前である場合は、DHCP 代行受信により、ドメイン名およびサブネット マスクが提供されます。これは、DHCP サーバを使用するのが効果的でない環境で役立ちます。

例

次に、FirstGroup というグループ ポリシーに DHCP 代行受信を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# intercept-dhcp enable
```

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。インターフェイス コンフィギュレーション モードでは、インターフェイスのタイプおよびセキュリティ コンテキスト モードに応じて、ハードウェアの設定（物理インターフェイスの場合）、名前の割り当て、VLAN の割り当て、IP アドレスの割り当てをはじめ、数多くの設定を行うことができます。

マルチ コンテキスト モードでは、**allocate-interface** コマンドを使用してマッピング名が割り当てられた場合、そのマッピング名の指定が必要になることがあります。

すべてのモデルで、物理インターフェイスのパラメータを設定できます。

ASA 5505 適応型セキュリティ アプライアンスなど組み込みスイッチを搭載したモデルを除くすべてのモデルで、論理冗長インターフェイスを作成できます。

ASA 5505 適応型セキュリティ アプライアンスなど組み込みスイッチを搭載したモデルを除くすべてのモデルで、VLAN に割り当てられる論理サブインターフェイスを作成できます。組み込みスイッチを搭載したモデルには、VLAN インターフェイスに割り当てることができるスイッチ ポート（このコマンドで物理インターフェイスと呼んでいるもの）を備えているものがあります。この場合、VLAN のサブインターフェイスを作成するのではなく、物理インターフェイスから独立した VLAN インターフェイスを作成します。その後、VLAN インターフェイスに 1 つ以上の物理インターフェイスを割り当てることができます。

冗長インターフェイス、サブインターフェイス、または VLAN 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。物理インターフェイスまたはマッピングされているインターフェイスは削除できません。

物理インターフェイスの場合（全モデルが対象）：

interface *physical_interface*

冗長インターフェイスの場合（組み込みスイッチを搭載したモデルには使用不可）：

interface redundant *number*

no interface redundant *number*

サブインターフェイスの場合（組み込みスイッチを搭載したモデルには使用不可）：

interface {*physical_interface* | **redundant** *number*}**.***subinterface*

no interface {*physical_interface* | **redundant** *number*}**.***subinterface*

VLAN インターフェイスの場合（組み込みスイッチを搭載したモデルが対象）：

interface vlan *number*

no interface vlan *number*

マルチ コンテキスト モードの場合（マッピング名が割り当てられているとき）：

interface *mapped_name*

構文の説明

mapped_name	マルチ コンテキスト モードで、**allocate-interface** コマンドを使用してマッピング名が割り当てられている場合は、マッピング名を指定します。
physical_interface	*type*[*slot*/]*port* という形式で物理インターフェイスのタイプ、スロット、およびポート番号を指定します。タイプとスロット/ポート間のスペースは任意です。 物理インターフェイスのタイプには、次のものがあります。 • **ethernet** • **gigabitethernet** • **management**（ASA 5500 のみ） PIX 500 シリーズ セキュリティ アプライアンスでは、タイプの後ろにポート番号を入力します（**ethernet0** など）。 ASA 5500 シリーズ適応型セキュリティ アプライアンスでは、スロット/ポート（たとえば、**gigabitethernet 0/1**. の前に来るタイプを入力します。シャーシに組み込まれているインターフェイスは、スロット 0 に割り当てられ、4GE SSM（または組み込み 4GE SSM）のインターフェイスはスロット 1 に割り当てられます。 管理インターフェイスは、管理トラフィック専用のファスト イーサネット インターフェイスであり、**management 0/0** のように指定します。ただし、必要に応じて通過トラフィック用に使用することもできます（**management-only** コマンドを参照）。トランスペアレント ファイア ウォール モードでは、通過トラフィックに許可されている 2 つのインターフェイスに加えて、管理インターフェイスを使用できます。また、管理インターフェイスにサブインターフェイスを追加して、マルチ コンテキスト モードの各セキュリティ コンテキストでの管理を実現できます。 インターフェイスのタイプ、スロット、およびポート番号を確認するには、モデルに付属のハードウェア マニュアルを参照してください。
redundant *number*	論理冗長インターフェイスを指定します。*number* には 1 ～ 8 の値を指定します。冗長インターフェイスは、アクティブ物理インターフェイスとスタンバイ物理インターフェイスのペアとなっています（**member-interface** コマンドを参照）。アクティブ インターフェイスで障害が発生すると、スタンバイ インターフェイスがアクティブになって、トラフィックを通過させ始めます。 すべてのセキュリティ アプライアンス コンフィギュレーションは、メンバ物理インターフェイスではなく論理冗長インターフェイスを参照します。 **redundant** と ID 間のスペースは任意です。
subinterface	論理サブインターフェイスに指定されている 1 ～ 4294967293 の整数を指定します。サブインターフェイスの最大数は、セキュリティ アプライアンス モデルによって異なります。サブインターフェイスは、ASA 5505 適応型セキュリティ アプライアンスなど組み込みスイッチを搭載したモデルには使用できません。プラットフォームあたりのサブインターフェイス（または VLAN）の最大数については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。VLAN サブインターフェイスが 1 つ以上あるインターフェイスは、自動的に 802.1Q トランクとして設定されます。
vlan *number*	組み込みスイッチを搭載したモデルの場合、VLAN ID を 1 ～ 4090 の範囲で指定します。

デフォルト

デフォルトでは、セキュリティ アプライアンスはすべての物理インターフェイスを対象に **interface** コマンドを自動的に生成します。

マルチ コンテキスト モードでは、セキュリティ アプライアンスは **allocate-interface** コマンドを使用して、コンテキストに割り当てられているすべてのインターフェイスを対象に **interface** コマンドを自動的に生成します。

インターフェイスのデフォルトの状態は、そのタイプおよびコンテキスト モードによって異なります。

マルチ コンテキスト モードでは、システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。

シングル モードまたはシステム実行スペースでは、インターフェイスのデフォルトの状態は次のとおりです。

- 物理インターフェイス：ディセーブル。
- 冗長インターフェイス：イネーブル。ただし、トラフィックが冗長インターフェイスを通過するためには、メンバ物理インターフェイスもイネーブルになっている必要があります。
- サブインターフェイス：イネーブル。ただし、トラフィックがサブインターフェイスを通過するためには、物理インターフェイスもイネーブルになっている必要があります。

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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、サブインターフェイスの新しい命名規則に対応し、インターフェイス コンフィギュレーション モードでは引数が独立したコマンドとなるように変更されました。
7.2(1)	**interface vlan** コマンドが、ASA 5505 適応型セキュリティ アプライアンスでの組み込みスイッチをサポートするために追加されました。
8.0(2)	**interface redundant** コマンドが追加されました。

使用上のガイドライン

イネーブルになっているインターフェイスでトラフィックを通過させるには、インターフェイス コンフィギュレーション モード コマンドである **nameif** を設定し、ルーテッド モードの場合には **ip address** も設定します。サブインターフェイスの場合は、**vlan** コマンドも設定します。スイッチ物理インターフェイスの場合、**switchport access vlan** コマンドを使用して、物理インターフェイスを VLAN インターフェイスに割り当てます。

インターフェイス設定を変更し、既存接続のタイムアウトを待たずに新しいセキュリティ情報を使用する場合は、**clear local-host** コマンドを使用して接続をクリアできます。

デフォルトのセキュリティ レベル

デフォルトのセキュリティ レベルは 0 です。インターフェイスに「inside」という名前を付け、**security-level** コマンドを使用してセキュリティ レベルを明示的に設定しないと、セキュリティ アプライアンスはセキュリティ レベルを 100 に設定します。

マルチ コンテキスト モードのガイドライン

- 各コンテキスト内からコンテキスト インターフェイスを設定します。
- システム コンフィギュレーションでコンテキストにすでに割り当てたコンテキスト インターフェイスを設定します。それ以外のインターフェイスは使用できません。
- システム コンフィギュレーションでイーサネット設定、冗長インターフェイス、およびサブインターフェイスを設定します。それ以外のコンフィギュレーションは使用できません。フェールオーバー インターフェイスは例外で、システム コンフィギュレーションに設定されます。このコマンドでフェールオーバー インターフェイスを設定しないでください。

トランスペアレント ファイアウォールのガイドライン

トランスペアレント ファイアウォール モードでは、2 つのインターフェイスだけがトラフィックを通過させることができます。ただし、ASA 5510 以降の適応型セキュリティ アプライアンスの場合、Management 0/0 インターフェイス（物理インターフェイスまたはサブインターフェイスのいずれか）を管理トラフィック用に 3 つめのインターフェイスとして使用できます。この場合モードは設定不可となり、常に管理専用にする必要があります。

サブインターフェイスのガイドライン

- 最大サブインターフェイス：プラットフォームに許可するサブインターフェイスの数を決定するには、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』でライセンス情報を参照してください。
- 物理インターフェイスでのタグなしパケットの阻止：サブインターフェイスを使用する場合は、物理インターフェイスでは一般にトラフィックを通過させないようにします。物理インターフェイスではタグなしパケットが通過してしまうためです。この特性は、冗長インターフェイス ペアのアクティブな物理インターフェイスにも当てはまります。サブインターフェイスでトラフィックを通過させるには物理的インターフェイスまたは冗長インターフェイスをイネーブルにする必要があるため、**nameif** コマンドを除外して物理インターフェイスまたは冗長インターフェイスでトラフィックを通過させないようにします。物理インターフェイスまたは冗長インターフェイスでタグなしパケットを通過させる場合は、通常どおり **nameif** コマンドを設定できます。

冗長インターフェイスのガイドライン

- フェールオーバーのガイドライン：
  - フェールオーバーまたはステート リンク用に冗長インターフェイスを使用する場合は、プライマリ ユニットに加えてセカンダリ ユニット上の基本的なコンフィギュレーションの一部として冗長インターフェイスを設定する必要があります。
  - フェールオーバーまたはステート リンク用に冗長インターフェイスを使用する場合は、2 つのユニット間にスイッチまたはハブを配置する必要があります。両ユニットは直接接続できません。スイッチやハブがなくても、プライマリ ユニット上のアクティブ ポートをセカンダリ ユニット上のスタンバイ ポートに直接接続できる場合もあります。
  - **monitor-interface** コマンドを使用して、フェールオーバーの冗長インターフェイスをモニタできます。その際、論理冗長インターフェイス名を参照してください。
  - アクティブ インターフェイスがスタンバイ インターフェイスにフェールオーバーした場合、デバイスレベルのフェールオーバーをモニタしているときには、冗長インターフェイスで障害が発生しているように見えません。冗長インターフェイスで障害が発生しているように見えるのは、両方の物理インターフェイスで障害が発生したときだけです。

- 冗長インターフェイスの MAC アドレス：冗長インターフェイスは、最初に追加した物理インターフェイスの MAC アドレスを使用します。コンフィギュレーションでメンバ インターフェイスの順序を変更すると、MAC アドレスは、リストの最初になったインターフェイスの MAC アドレスと一致するように変更されます。または、メンバー インターフェイスの MAC アドレスとは関係なく使用される MAC アドレスを冗長インターフェイスに割り当てることができます（**mac-address** コマンドまたは **mac-address auto** コマンドを参照）。アクティブ インターフェイスがスタンバイ インターフェイスにフェールオーバーした場合は、同じ MAC アドレスが維持されるため、トラフィックが妨げられることはありません。
- 物理インターフェイスのガイドライン：メンバー インターフェイスを追加するときには、次のガイドラインに従ってください。
  - 両方のメンバ インターフェイスが同じ物理タイプである必要があります。たとえば、両方ともイーサネットにする必要があります。
  - 名前が設定されている場合は、物理インターフェイスを冗長インターフェイスに追加できません。この場合、まず **no nameif** コマンドを使用して名前を削除する必要があります。

注意　コンフィギュレーション内で物理インターフェイスをすでに使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

  - 冗長インターフェイス ペアの一部である物理インターフェイスに使用できるコンフィギュレーションのみが物理パラメータ（**speed** コマンド、**duplex** コマンド、**description** コマンド、**shutdown** コマンドなど）です。また、**default** や **help** などの実行時コマンドを入力することもできます。
  - アクティブ インターフェイスをシャットダウンすると、スタンバイ インターフェイスがアクティブになります。

組み込みスイッチのガイドライン

組み込みスイッチを搭載したモデルの場合、物理インターフェイス専用の物理パラメータおよびスイッチ パラメータ（VLAN 割り当てを含む）を設定します。VLAN インターフェイスにはその他のすべてのパラメータを設定します。

トランスペアレント ファイアウォール モードの ASA 5505 適応型セキュリティ アプライアンスの場合､基本ライセンスで 2 つのアクティブ VLAN と Security Plus ライセンスで 3 つのアクティブ VLAN を設定でき、そのうちの 1 つをフェールオーバー用にする必要があります。ルーテッド モードでは、基本ライセンスで最大 3 つのアクティブ VLAN と Security Plus ライセンスで最大 5 つのアクティブ VLAN を設定できます。アクティブな VLAN とは、**nameif** コマンドが設定された VLAN のことです。VLAN は、アクティブ VLAN の数を制限してライセンスに準拠している限り、必要な数だけ設定できます。基本ライセンスの場合、3 つめの VLAN は他の 1 つの VLAN にのみトラフィックを開始するように設定できます。3 つめの VLAN を制限するには、**no forward interface** コマンドを使用します。Security Plus ライセンスでは、通常のトラフィック用に 3 つの VLAN インターフェイス、フェールオーバー用に 1 つの VLAN インターフェイス、および ISP へのバックアップ リンクとして 1 つの VLAN インターフェイスを設定できます。ただし、フェールオーバー VLAN インターフェイスは、**interface vlan** コマンドでは設定されません。フェールオーバー VLAN ID に物理インターフェイスを割り当てた後、**failover lan** コマンドを使用して VLAN インターフェイスを作成し、設定します。ISP へのバックアップ リンクを識別するには、プライマリ VLAN コンフィギュレーションで **backup interface** コマンドを使用します。このインターフェイスは、プライマリ インターフェイスで障害が発生しない限り、トラフィックを通過させません。詳細については、**backup interface** コマンドを参照してください。

管理専用インターフェイス

ASA 5510 以降の適応型セキュリティ アプライアンスには、Management 0/0 という専用の管理インターフェイスが含まれ、セキュリティ アプライアンスへのトラフィックをサポートするようになっています。ただし、**management-only** コマンドを使用することで、任意のインターフェイスを管理専用インターフェイスとして設定できます。また、Management 0/0 の場合、管理専用モードをディセーブルにできるため、このインターフェイスは他のインターフェイスと同じくトラフィックを通過させることができます。

トランスペアレント ファイアウォール モードでは、2 つのインターフェイスだけがトラフィックを通過させることができます。ただし、ASA 5510 以降の適応型セキュリティ アプライアンスの場合、Management 0/0 インターフェイス（物理インターフェイスまたはサブインターフェイスのいずれか）を管理トラフィック用に 3 つめのインターフェイスとして使用できます。この場合モードは設定不可となり、常に管理専用にする必要があります。

例

次に、シングル モードで物理インターフェイスのパラメータを設定する例を示します。

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

次に、シングル モードでサブインターフェイスのパラメータを設定する例を示します。

```
hostname(config)# interface gigabitethernet0/1.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# no shutdown
```

次に、システム コンフィギュレーション用にマルチ コンテキスト モードでインターフェイス パラメータを設定し、GigabitEthernet 0/1.1 サブインターフェイスをコンテキスト A に割り当てる例を示します。

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# no shutdown
hostname(config-if)# interface gigabitethernet0/1.1
hostname(config-subif)# vlan 101
hostname(config-subif)# no shutdown
hostname(config-subif)# context contextA
hostname(config-ctx)# ...
hostname(config-ctx)# allocate-interface gigabitethernet0/1.1
```

次に、コンテキスト コンフィギュレーション用にマルチ コンテキスト モードでパラメータを設定する例を示します。

```
hostname/contextA(config)# interface gigabitethernet0/1.1
hostname/contextA(config-if)# nameif inside
hostname/contextA(config-if)# security-level 100
hostname/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
hostname/contextA(config-if)# no shutdown
```

次の例では、3 つの VLAN インターフェイスを設定します。3 つめのホーム インターフェイスは、トラフィックをワーク インターフェイスに転送できません。

```
hostname(config)# interface vlan 100
```

```
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address dhcp
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif work
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# no forward interface vlan 200
hostname(config-if)# nameif home
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

...
```

次に、**failover lan** コマンドを使用して別途設定されるフェールオーバー インターフェイスを含め、5 つの VLAN インターフェイスを設定する例を示します。

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# nameif dmz
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.3.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 400
hostname(config-if)# nameif backup-isp
hostname(config-if)# security-level 50
```

```
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# failover lan faillink vlan500
hostname(config)# failover interface ip faillink 10.4.1.1 255.255.255.0 standby 10.4.1.2
255.255.255.0

hostname(config)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 400
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 500
hostname(config-if)# no shutdown
```

次の例では、2 つの冗長インターフェイスを作成します。

```
hostname(config)# interface redundant 1
hostname(config-if)# member-interface gigabitethernet 0/0
hostname(config-if)# member-interface gigabitethernet 0/1
hostname(config-if)# interface redundant 2
hostname(config-if)# member-interface gigabitethernet 0/2
hostname(config-if)# member-interface gigabitethernet 0/3
```

関連コマンド

コマンド	説明
allocate-interface	インターフェイスおよびサブインターフェイスをセキュリティ コンテキストに割り当てます。
member-interface	インターフェイスを冗長インターフェイスに割り当てます。
clear interface	**show interface** コマンドのカウンタをクリアします。
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。
vlan	サブインターフェイスに VLAN を割り当てます。

interface（vpn ロードバランシング）

VPN ロード バランシングの仮想クラスタで VPN ロード バランシング用にデフォルト以外のパブリック インターフェイスまたはプライベート インターフェイスを指定するには、VPN ロード バランシング モードで **interface** コマンドを使用します。このインターフェイス指定を削除し、デフォルトのインターフェイスに戻すには、このコマンドの **no** 形式を使用します。

interface {**lbprivate** | **lbpublic**} *interface-name*]

no interface {**lbprivate** | **lbpublic**}

構文の説明

interface-name	VPN ロード バランシング クラスタのパブリック インターフェイスまたはプライベート インターフェイスとして設定されるインターフェイスの名前。
lbprivate	このコマンドが VPN ロード バランシングのプライベート インターフェイスを設定することを指定します。
lbpublic	このコマンドが VPN ロード バランシングのパブリック インターフェイスを設定することを指定します。

デフォルト

interface コマンドを省略した場合、**lbprivate** インターフェイスはデフォルトで **inside** に設定され、**lbpublic** インターフェイスはデフォルトで **outside** 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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

まず、**vpn load-balancing** コマンドを使用して、VPN ロード バランシング モードを開始しておく必要があります。

また、あらかじめ **interface**、**ip address**、**nameif** の各コマンドを使用して、このコマンドで指定するインターフェイスを設定し、名前を割り当てておく必要があります。

このコマンドの no 形式は、インターフェイスをデフォルトの状態に戻します。

例

次に、**vpn load-balancing** コマンド シーケンスの一例を示します。この中の **interface** コマンドでは、クラスタのプライベート インターフェイスをデフォルト（inside）に戻す「test」インターフェイスとして、クラスタのパブリック インターフェイスを指定しています。

```
hostname(config)# interface GigabitEthernet 0/1
```

```
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# no interface lbprivate
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロード バランシング モードを開始します。

interface-policy

モニタリングでインターフェイスの障害を検出する際にフェールオーバーの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*[**%**]

構文の説明

num	パーセンテージとして使用するときには 1 ～ 100 の数値を指定し、そうでなければインターフェイスの最大数として 1 を指定します。
%	（任意）*num* の数字が、モニタ対象インターフェイスのパーセンテージであることを指定します。

デフォルト

ユニットに **failover interface-policy** コマンドが設定されている場合は、**interface-policy** フェールオーバー グループ コマンドのデフォルトが設定値であると見なされます。そうでない場合、*num* は 1 となります。

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	透過	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

num 引数とオプションの **%** キーワードの間にはスペースを挿入しません。

障害が発生したインターフェイスの数が設定したポリシーを満たし、他のセキュリティ アプライアンスが正しく機能している場合、セキュリティ アプライアンスが自らを障害発生としてマークし、フェールオーバーが発生することがあります（アクティブなセキュリティ アプライアンスで障害が発生した場合）。ポリシーでカウントされるのは、**monitor-interface** コマンドでモニタ対象として指定したインターフェイスのみです。

例

次の部分的な例では、フェールオーバー グループで可能な設定を示します。

```
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	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
failover interface-policy	インターフェイス モニタリング 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対象にするインターフェイスを指定します。

internal-password

クライアントレス SSL VPN ポータル ページで追加パスワード フィールドを表示するには、webvpn コンフィギュレーション モードで **internal-password** コマンドを使用します。この追加パスワードは、セキュリティ アプライアンスが SSO を許可しているファイル サーバに対してユーザを認証するのに使用されます。

内部パスワードの使用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。

internal-password enable

no internal password

構文の説明

enable	内部パスワードの使用をイネーブルにします。

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。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

イネーブルにした場合、エンド ユーザはクライアントレス SSL VPN セッションにログインするときに 2 つめのパスワードを入力します。クライアントレス SSL VPN サーバは、HTTPS を使用して、ユーザ名やパスワードなどの SSO 認証要求を認証サーバに送信します。認証サーバが認証要求を承認すると、SSO 認証クッキーがクライアントレス SSL VPN サーバに返されます。このクッキーは、ユーザに代わってセキュリティ アプライアンスに保持され、ユーザを認証して SSO サーバによって保護されたドメイン内の Web サイトを保護するのに使用されます。

内部パスワード機能は、内部パスワードを SSL VPN パスワードとは異なるものにする場合に便利です。特に、セキュリティ アプライアンスへの認証にワンタイム パスワードを使用し、内部サイトの認証に別のパスワードを使用できます。

例

次に、内部パスワードをイネーブルにする例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# internal password enable
hostname(config-webvpn)#
```

関連コマンド

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

interval maximum

DDNS 更新方式による更新試行の最大間隔を設定するには、DDNS 更新方式モードで **interval** 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 DDNS 更新方式の間隔を削除するには、このコマンドの **no** 形式を使用します。

interval maximum *days hours minutes seconds*

no interval maximum *days hours minutes seconds*

構文の説明

days	更新試行間の日数を 0 ～ 364 の範囲で指定します。
hours	更新試行間の時間数を 0 ～ 23 の範囲で指定します。
minutes	更新試行間の分数を 0 ～ 59 の範囲で指定します。
seconds	更新試行間の秒数を 0 ～ 59 の範囲で指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

日、時間、分、および秒を足すと、間隔の合計時間になります。

例

次に、3 分 15 秒ごとに更新を試行する方式を ddns-2 という名前で設定する例を示します。

```
hostname(config)# ddns update method ddns-2
hostname(DDNS-update-method)# interval maximum 0 0 3 15
```

関連コマンド

コマンド	説明
ddns（**DDNS 更新方式モード**）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update（**インターフェイス コンフィギュレーション モード**）	Dynamic DNS（DDNS; ダイナミック DNS）アップデート方式を、セキュリティ アプライアンスのインターフェイスまたは DDNS アップデート ホスト名に関連付けます。

コマンド	説明
ddns update method (グローバル コンフィギュレーション モード)	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
dhcp-client update dns	DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。
dhcpd update dns	DHCP サーバによるダイナミック DNS アップデートの実行をイネーブルにします。

invalid-ack

ACK が無効になっているパケットに対するアクションを設定するには、tcp-map コンフィギュレーション モードで **invalid-ack** コマンドを使用します。値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。このコマンドは、**set connection advanced-options** コマンドを使用してイネーブルにされる TCP 正規化ポリシーの一部です。

invalid-ack {**allow** | **drop**}

no invalid-ack

構文の説明

allow	ACK が無効になっているパケットを許可します。
drop	ACK が無効になっているパケットをドロップします。

デフォルト

デフォルト アクションは、ACK が無効になっているパケットをドロップすることです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(4)/8.0(4)	このコマンドが導入されました。

使用上のガイドライン

TCP 正規化をイネーブルにするには、モジュラ ポリシー フレームワークを次のように使用します。

1. **tcp-map**：TCP 正規化アクションを指定します。
   a. **invalid-ack**：tcp-map コンフィギュレーション モードでは、**invalid-ack** コマンドをはじめ多数のコマンドを入力できます。
2. **class-map**：TCP 正規化を実行するトラフィックを指定します。
3. **policy-map**：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. **set connection advanced-options**：作成した TCP マップを指定します。
4. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

次のような場合に無効な ACK が検出される可能性があります。

- TCP 接続が SYN-ACK-received ステータスでは、受信した TCP パケットの ACK 番号が次の TCP パケット送信のシーケンス番号と同じでない場合、その ACK は無効です。

- 受信した TCP パケットの ACK 番号が次の TCP パケット送信のシーケンス番号より大きい場合は常に、その ACK は無効です。

（注）　無効な ACK を含む TCP パケットは、WAAS 接続で自動的に許可されます。

例

次に、ACK が無効になっているパケットを許可するようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# invalid-ack allow
hostname(config)# class-map cmap
hostname(config-cmap)# match any
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
hostname(config)#
```

関連コマンド

コマンド	説明
class-map	サービス ポリシーに対してトラフィックを指定します。
policy-map	サービス ポリシー内でトラフィックに適用するアクションを指定します。
set connection advanced-options	TCP 正規化をイネーブルにします。
service-policy	サービス ポリシーをインターフェイスに適用します。
show running-config tcp-map	TCP マップ コンフィギュレーションを表示します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

ip address

インターフェイス（ルーテッド モード）または管理アドレス（トランスペアレント モード）の IP アドレスを設定するには、**ip address** コマンドを使用します。ルーテッド モードの場合は、インターフェイス コンフィギュレーション モードでこのコマンドを入力します。トランスペアレント モードの場合は、グローバル コンフィギュレーション モードでこのコマンドを入力します。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。このコマンドはこの他、フェールオーバーのスタンバイ アドレスを設定します。

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

no ip address [*ip_address*]

構文の説明

ip_address	インターフェイスの IP アドレス（ルーテッド モード）または管理 IP アドレス（トランスペアレント モード）。
mask	（任意）IP アドレスのサブネット マスク。マスクを設定しない場合、セキュリティ アプライアンスでは IP アドレス クラスのデフォルト マスクが使用されます。
standby *ip_address*	（任意）フェールオーバーのスタンバイ ユニットの IP アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	ルーテッド モードの場合、このコマンドは、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 モードの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 アドレスはそれぞれ固有のサブネットに存在する必要があります。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にある場合、各 IP アドレスはそれぞれ固有であるものの、同じサブネットに存在する必要があります。インターフェイスが固有のものである場合、この IP アドレスを必要に応じて他のコンテキストで使用できます。

トランスペアレント ファイアウォールは、IP ルーティングに参加しません。セキュリティ アプライアンスに必要な唯一の IP コンフィギュレーションは、管理 IP アドレスを設定することです。このアドレスが必要になるのは、セキュリティ アプライアンスがシステム メッセージや AAA サーバとの通信などセキュリティ アプライアンスで発信され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ためです。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、上流のルータおよび下流のルータと同じサブネットに存在する必要があります。マルチ コンテキスト モードの場合、各コンテキスト内の管理 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に存在する必要があります。

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 gigabitethernet0/2
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)# no shutdown
hostname(config-if)# interface gigabitethernet0/3
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
hostname(config-if)# no shutdown
```

次に、トランスペアレント ファイアウォールの管理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)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
```

関連コマンド

コマンド	説明
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	インターフェイスで DHCP サーバから IP アドレスを取得できるように設定します。
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 dhcp

DHCP を使用してインターフェイスの IP アドレスを取得するには、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 dhcp** コマンドを使用します。このインターフェイスの DHCP クライアン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。

ip address dhcp [**setroute**]

no ip address dhcp

構文の説明

setroute	（任意）セキュリティ アプライアンスが DHCP サーバから提供されたデフォルト ルートを使用できるようにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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	変更内容
7.0(1)	このコマンドは、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。このコマンドは、外部インターフェイスだけでなく、任意のインターフェイスもイネーブルにできます。

使用上のガイドライン

DHCP リースをリセットし、新規リースを要求するには、このコマンドを再入力します。

ip address dhcp コマンドを入力する前に、**no shutdown** コマンドを使用してインターフェイスをイネーブルにしなかった場合、DHCP 要求が送信されないことがあります。

（注） セキュリティ アプライアンスは、タイムアウトが 32 秒未満のリースを拒否します。

例

次に、gigabitethernet0/1 インターフェイスで DHCP をイネーブルにする例を示します。

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# no shutdown
hostname(config-if)# ip address dhcp
```

関連コマンド

コマンド	説明
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	インターフェイスの IP アドレス、またはトランスペアレント ファイア ウォールの管理 IP アドレスを設定します。
show ip address dhcp	DHCP サーバから取得された IP アドレスを示します。

ip address pppoe

PPPoE 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 **ip address pppoe** コマンドを使用します。PPPoE 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 [*ip_address* [*mask*]] **pppoe** [**setroute**]

no ip address [*ip_address* [*mask*]] **pppoe**

構文の説明

ip_address	IP アドレスを PPPoE サーバから受信するのではなく手動で設定します。
mask	IP アドレスのサブネット マスクを指定します。マスクを設定しない場合、セキュリティ アプライアンスでは IP アドレス クラスのデフォルト マスクが使用されます。
setroute	セキュリティ アプライアンスが、PPPoE サーバから提供されるデフォルト ルートを使用できるようにします。PPPoE サーバがデフォルト ルートを送信しない場合、セキュリティ アプライアンスはアクセス コンセントレータのアドレスをゲートウェイとするデフォルト ルートを作成します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

PPPoE は、イーサネットと PPP という広く受け入れられている 2 つの標準を結合して、IP アドレスをクライアント システムに割り当てる認証方式を提供します。ISP は、既存のリモート アクセス インフラストラクチャを使用して高速ブロードバンド アクセスをサポートするためと、顧客の使い勝手向上のために、PPPoE を配置します。

PPPoE を使用して IP アドレスを設定する前に、**vpdn** コマンドでユーザ名、パスワード、および認証プロトコルを設定します。複数のインターフェイスでこのコマンドをイネーブルにした場合（たとえば、ISP へのバックアップ リンク用）は、**pppoe client vpdn group** コマンドを使用して、必要に応じて各インターフェイスをそれぞれ異なる VPDN グループに割り当てることができます。

最大伝送単位（MTU）サイズは、自動的に 1492 バイトに設定されます。これは、イーサネット フレーム内で PPPoE 伝送を許可する正しい値です。

PPPoE セッションをリセットして再起動するには、このコマンドを再入力します。

このコマンドは、**ip address** コマンドまたは **ip address dhcp** コマンドと同時には設定できません。

例

次に、GigabitEthernet 0/1 インターフェイスで PPPoE をイネーブルにする例を示します。

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address pppoe
hostname(config-if)# no shutdown
```

次に、PPPoE インターフェイスの IP アドレスを手動で設定する例を示します。

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.1.1 255.255.255.0 pppoe
hostname(config-if)# no shutdown
```

関連コマンド

コマンド	説明
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	インターフェイスの IP アドレスを設定します。
pppoe client vpdn group	このインターフェイスを特定の VPDN グループに割り当てます。
show ip address pppoe	PPPoE サーバから取得された IP アドレスを表示します。
vpdn group	～を作成します。

ip-address-privacy

IP アドレスのプライバシー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 **ip-address-privacy** 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。

ip-address-privacy

no ip-address-privacy

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

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。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、SIP インスペクション ポリシー マップで SIP を経由する IP アドレスのプライバシーをイネーブルにする例を示します。

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# ip-address-privacy
```

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。

ip audit attack

攻撃シグニチャに一致するパケットに対してデフォルト アクシ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 **ip audit attack** コマンドを使用します。デフォルト アクションを復元（して接続をリセット）するには、このコマンドの **no** 形式を使用します。アクションは複数指定することも、まったく指定しないこともできます。

ip audit attack [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit attack

構文の説明

action	（任意）一連のデフォルト アクションを定義することを指定します。このキーワードの後に何もアクションを指定しない場合、セキュリティ アプライアンスはアクションを実行しません。**action** キーワードを入力しない場合、セキュリティ アプライアンスではキーワードが入力されたものと見なして、**action** キーワードをコンフィギュレーションに記述します。
alarm	（デフォルト）パケットがシグニチャに一致したことを示すシステム メッセージを生成します。
drop	（任意）パケットをドロップします。
reset	（任意）パケットをドロップし、接続を閉じます。

デフォルト

デフォルト アクションは、送信し、アラームを生成することです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドで設定するアクションは、**ip audit name** コマンドを使用して監査ポリシーを設定すると上書きできます。**ip audit name** コマンドでアクションを指定しない場合は、このコマンドで設定するアクションが使用されます。

シグニチャのリストについては、**ip audit signature** コマンドを参照してください。

例

次に、攻撃シグニチャに一致するパケットに対してアラームを生成し、リセットするデフォルト アクションを設定する例を示します。内部インターフェイスの監査ポリシーはアラームだけを生成するようにこのデフォルトを上書きしますが、外部インターフェイスの監査ポリシーは **ip audit attack** コマンドで設定されたデフォルト設定を使用します。

```
hostname(config)# ip audit attack action alarm reset
hostname(config)# ip audit name insidepolicy attack action alarm
hostname(config)# ip audit name outsidepolicy attack
hostname(config)# ip audit interface inside insidepolicy
hostname(config)# ip audit interface outside outsidepolicy
```

関連コマンド

コマンド	説明
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	監査ポリシーをインターフェイスに割り当てます。
ip audit signature	シグニチャをディセーブルにします。
show running-config ip audit attack	**ip audit attack** コマンドのコンフィギュレーションを表示します。

ip audit info

情報シグニチャに一致するパケットに対してデフォルト アクシ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 **ip audit info** コマンドを使用します。デフォルト アクションを復元（してアラームを生成）するには、このコマンドの **no** 形式を使用します。アクションは複数指定することも、まったく指定しないこともできます。

ip audit info [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit info

構文の説明

action	（任意）一連のデフォルト アクションを定義することを指定します。このキーワードの後に何もアクションを指定しない場合、セキュリティ アプライアンスはアクションを実行しません。**action** キーワードを入力しない場合、セキュリティ アプライアンスではキーワードが入力されたものと見なして、**action** キーワードをコンフィギュレーションに記述します。
alarm	（デフォルト）パケットがシグニチャに一致したことを示すシステム メッセージを生成します。
drop	（任意）パケットをドロップします。
reset	（任意）パケットをドロップし、接続を閉じます。

デフォルト

デフォルト アクションは、アラームを生成することです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドで設定するアクションは、**ip audit name** コマンドを使用して監査ポリシーを設定すると上書きできます。**ip audit name** コマンドでアクションを指定しない場合は、このコマンドで設定するアクションが使用されます。

シグニチャのリストについては、**ip audit signature** コマンドを参照してください。

例

次に、情報シグニチャに一致するパケットに対してアラームを生成し、リセットするデフォルト アクションを設定する例を示します。内部インターフェイスの監査ポリシーはアラームを生成し、ドロップするようにこのデフォルトを上書きしますが、外部インターフェイスの監査ポリシーは **ip audit info** コマンドで設定されたデフォルト設定を使用します。

```
hostname(config)# ip audit info action alarm reset
hostname(config)# ip audit name insidepolicy info action alarm drop
hostname(config)# ip audit name outsidepolicy info
hostname(config)# ip audit interface inside insidepolicy
hostname(config)# ip audit interface outside outsidepolicy
```

関連コマンド

コマンド	説明
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	監査ポリシーをインターフェイスに割り当てます。
ip audit signature	シグニチャをディセーブルにします。
show running-config ip audit info	**ip audit info** コマンドのコンフィギュレーションを表示します。

ip audit interface

監査ポリシーをインターフェイスに割り当てるには、グローバル コンフィギュレーション モードで **ip audit interface** コマンドを使用します。インターフェイスからポリシーを削除するには、このコマンドの **no** 形式を使用します。

ip audit interface *interface_name policy_name*

no ip audit interface *interface_name policy_name*

構文の説明

interface_name	インターフェイス名を指定します。
policy_name	**ip audit name** コマンドで追加したポリシーの名前。各インターフェイスに **info** ポリシーおよび **attack** ポリシーを割り当てることができます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、監査ポリシーを内部インターフェイスおよび外部インターフェイスに適用する例を示します。

```
hostname(config)# ip audit name insidepolicy1 attack action alarm
hostname(config)# ip audit name insidepolicy2 info action alarm
hostname(config)# ip audit name outsidepolicy1 attack action reset
hostname(config)# ip audit name outsidepolicy2 info action alarm
hostname(config)# ip audit interface inside insidepolicy1
hostname(config)# ip audit interface inside insidepolicy2
hostname(config)# ip audit interface outside outsidepolicy1
hostname(config)# ip audit interface outside outsidepolicy2
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。

コマンド	説明
ip audit signature	シグニチャをディセーブルにします。
show running-config ip audit interface	**ip audit interface** コマンドのコンフィギュレーションを表示します。

ip audit name

パケットが定義済みの攻撃シグニチャまたは情報シグニチャに一致したときに実行するアクションを識別する名前付き監査ポリシーを作成するには、グローバル コンフィギュレーション モードで **ip audit name** コマンドを使用します。シグニチャは、既知の攻撃パターンに一致するアクティビティです。たとえば、DoS 攻撃に一致するシグニチャがあります。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

ip audit name *name* {**info** | **attack**} [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit name *name* {**info** | **attack**} [**action** [**alarm**] [**drop**] [**reset**]]

構文の説明

action	（任意）一連のアクションを定義することを指定します。このキーワードの後に何もアクションを指定しない場合、セキュリティ アプライアンスはアクションを実行しません。**action** キーワードを入力しないと、セキュリティ アプライアンスは **ip audit attack** コマンドおよび **ip audit info** コマンドによって設定されたデフォルト アクションを使用します。
alarm	（任意）パケットがシグニチャに一致したことを示すシステム メッセージを生成します。
attack	攻撃シグニチャの監査ポリシーを作成します。パケットは、DoS 攻撃や不正な FTP コマンドなど、ネットワークでの攻撃の一部となる可能性があります。
drop	（任意）パケットをドロップします。
info	情報シグニチャの監査ポリシーを作成します。パケットは、現時点ではネットワークを攻撃していませんが、ポート スイープなど情報収集アクティビティの一部である可能性があります。
name	ポリシーの名前を設定します。
reset	（任意）パケットをドロップし、接続を閉じます。

デフォルト

ip audit attack コマンドおよび **ip audit info** コマンドを使用してデフォルト アクションを変更しなかった場合、攻撃シグニチャおよび情報シグニチャのデフォルト アクションはアラームを生成することです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ポリシーを適用するには、**ip audit interface** コマンドを使用して、そのポリシーをインターフェイスに割り当てます。各インターフェイスに **info** ポリシーおよび **attack** ポリシーを割り当てることができます。

シグニチャのリストについては、**ip audit signature** コマンドを参照してください。

トラフィックがシグニチャに一致し、そのトラフィックに対してアクションを実行する場合は、**shun** コマンドを使用して、問題のホストからの新規接続を拒否し、既存の接続からのパケットの受信を禁止します。

例

次に、内部インターフェイスには攻撃シグニチャおよび情報シグニチャに関するアラームを生成する監査ポリシーを設定し、外部インターフェイスには攻撃に備えて接続をリセットする監査ポリシーを設定する例を示します。

```
hostname(config)# ip audit name insidepolicy1 attack action alarm
hostname(config)# ip audit name insidepolicy2 info action alarm
hostname(config)# ip audit name outsidepolicy1 attack action reset
hostname(config)# ip audit name outsidepolicy2 info action alarm
hostname(config)# ip audit interface inside insidepolicy1
hostname(config)# ip audit interface inside insidepolicy2
hostname(config)# ip audit interface outside outsidepolicy1
hostname(config)# ip audit interface outside outsidepolicy2
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	監査ポリシーをインターフェイスに割り当てます。
ip audit signature	シグニチャをディセーブルにします。
shun	特定の送信元アドレスおよび宛先アドレスでパケットをブロックします。

ip audit signature

監査ポリシーに対してシグニチャ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 **ip audit signature** コマンドを使用します。シグニチャを再び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。正規のトラフィックが頻繁にシグニチャに一致する場合には、シグニチャをディセーブルにしてみてください。リスクが伴うことを承知でシグニチャをディセーブルにすると、多数のアラームを回避できます。

ip audit signature *signature_number* **disable**

no ip audit signature *signature_number*

構文の説明

signature_number	ディセーブルにするシグニチャ番号を指定します。サポートされているシグニチャのリストについては、表 16-1 を参照してください。
disable	シグニチャをディセーブルにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン　表 16-1 に、サポートされているシグニチャおよびメッセージ番号の一覧を示します。

表 16-1　シグニチャ ID とシステム メッセージ番号

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
1000	400000	IP options-Bad Option List	Informational	IP データグラム ヘッダーの IP オプションのリストが不完全であるか、または不正な形式になっている IP データグラムを受信するとトリガーされます。IP オプションのリストには、さまざまなネットワーク管理タスクまたはデバッグ タスクを実行するオプションが 1 つ以上含まれています。
1001	400001	IP options-Record Packet Route	Informational	データグラムの IP オプション リスト中にオプション 7（記録パケット ルート）を含む IP データグラムを受信するとトリガーされます。
1002	400002	IP options-Timestamp	Informational	データグラムの IP オプション リスト中にオプション 4（タイムスタンプ）を含む IP データグラムを受信するとトリガーされます。
1003	400003	IP options-Security	Informational	データグラムの IP オプション リスト中にオプション 2（セキュリティ オプション）を含む IP データグラムを受信するとトリガーされます。
1004	400004	IP options-Loose Source Route	Informational	データグラムの IP オプション リスト中にオプション 3（緩慢な送信元ルート）を含む IP データグラムを受信するとトリガーされます。
1005	400005	IP options-SATNET ID	Informational	データグラムの IP オプション リスト中にオプション 8（SATNET ストリーム ID）を含む IP データグラムを受信するとトリガーされます。
1006	400006	IP options-Strict Source Route	Informational	データグラムの IP オプション リスト中にオプション 2（厳密な送信元ルーティング）を含む IP データグラムを受信するとトリガーされます。
1100	400007	IP Fragment Attack	Attack	オフセット フィールドのオフセット値が 0 より大きく 5 未満になっている IP データグラムを受信するとトリガーされます。
1102	400008	IP Impossible Packet	Attack	送信元と宛先が同じアドレスになっている IP パケットが到着するとトリガーされます。このシグニチャは、いわゆる Land Attack を捕捉します。

表 16-1　シグニチャ ID とシステム メッセージ番号 （続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
1103	400009	IP Overlapping Fragments（Teardrop）	Attack	同じ IP データグラム内に含まれている 2 つのフラグメントのオフセット値が、そのデータグラム内の位置決めを共有していることを示す場合にトリガーされます。これは、フラグメント A がフラグメント B によって完全に上書きされること、またはフラグメント A がフラグメント B によって部分的に上書きされることを意味します。オペレーティング システムによっては、このように重複するフラグメントが正しく処理されず、重複フラグメントを受信すると例外をスローしたり、他の不適切な動作を行ったりします。Teardrop 攻撃では、これにより DoS 状態を引き起こします。
2000	400010	ICMP Echo Reply	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 0（エコー応答）に設定された IP データグラムを受信するとトリガーされます。
2001	400011	ICMP Host Unreachable	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 3（ホスト到達不能）に設定された IP データグラムを受信するとトリガーされます。
2002	400012	ICMP Source Quench	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 4（ソース クエンチ）に設定された IP データグラムを受信するとトリガーされます。
2003	400013	ICMP Redirect	Informational	P ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 5（リダイレクト）に設定された IP データグラムを受信するとトリガーされます。
2004	400014	ICMP Echo Request	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 8（エコー要求）に設定された IP データグラムを受信するとトリガーされます。
2005	400015	ICMP Time Exceeded for a Datagram	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 11（データグラムの超過時間）に設定された IP データグラムを受信するとトリガーされます。

表 16-1　シグニチャ ID とシステム メッセージ番号 （続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
2006	400016	ICMP Parameter Problem on Datagram	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 12（データグラムのパラメータ問題）に設定された IP データグラムを受信するとトリガーされます。
2007	400017	ICMP Timestamp Request	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 13（タイムスタンプ要求）に設定された IP データグラムを受信するとトリガーされます。
2008	400018	ICMP Timestamp Reply	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 14（タイムスタンプ応答）に設定された IP データグラムを受信するとトリガーされます。
2009	400019	ICMP Information Request	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 15（情報要求）に設定された IP データグラムを受信するとトリガーされます。
2010	400020	ICMP Information Reply	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 16（ICMP 情報応答）に設定された IP データグラムを受信するとトリガーされます。
2011	400021	ICMP Address Mask Request	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 17（アドレス マスク要求）に設定された IP データグラムを受信するとトリガーされます。
2012	400022	ICMP Address Mask Reply	Informational	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 18（アドレス マスク応答）に設定された IP データグラムを受信するとトリガーされます。
2150	400023	Fragmented ICMP Traffic	Attack	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、他にも 1（ICMP）に設定されたフラグメント フラグが存在するか、またはオフセット フィールドにオフセット値が指定されている IP データグラムを受信するとトリガーされます。
2151	400024	Large ICMP Traffic	Attack	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、IP 長が 1024 より大きくなっている IP データグラムを受信するとトリガーされます。

表 16-1　シグニチャ ID とシステム メッセージ番号 （続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
2154	400025	Ping of Death Attack	Attack	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、最終フラグメント ビットが設定され、さらに（IP オフセット * 8）+（IP データ長）が 65535 を超えている場合、つまり IP オフセット（このフラグメントの元のパケットでの開始位置を表し、かつ 8 バイト単位であるもの）にパケットの残りを加えた値が、IP パケットの最大サイズを超えている IP データグラムを受信するとトリガーします。
3040	400026	TCP NULL flags	Attack	SYN、FIN、ACK、または RST のいずれのフラグも設定されていない 1 つの TCP パケットが特定のホストに送信されるとトリガーされます。
3041	400027	TCP SYN+FIN flags	Attack	SYN および FIN のフラグが設定されている 1 つの TCP パケットが特定のホストに送信されるとトリガーされます。
3042	400028	TCP FIN only flags	Attack	1 つの孤立 TCP FIN パケットが特定のホストの特権ポート（ポート番号が 1024 未満）に送信されるとトリガーされます。
3153	400029	FTP Improper Address Specified	Informational	要求側ホストと異なるアドレスを指定して port コマンドが発行された場合にトリガーされます。
3154	400030	FTP Improper Port Specified	Informational	1024 未満または 65535 より大きい値のデータ ポートを指定して port コマンドが発行された場合にトリガーされます。
4050	400031	UDP Bomb attack	Attack	指定されている UDP 長が、指定されている IP 長より短い場合にトリガーされます。この不正な形式のパケット タイプは、サービス拒絶攻撃と関連付けられています。
4051	400032	UDP Snork attack	Attack	送信元ポートが 135、7、または 19 のいずれかで、宛先ポートが 135 になっている UDP パケットが検出されるとトリガーされます。
4052	400033	UDP Chargen DoS attack	Attack	このシグニチャは、送信元ポート 7 および宛先ポート 19 において UDP パケットが検出されるとトリガーされます。
6050	400034	DNS HINFO Request	Informational	DNS サーバから HINFO レコードへのアクセスが試みられるとトリガーされます。
6051	400035	DNS Zone Transfer	Informational	送信元ポートが 53 の通常の DNS ゾーン転送が実行されるとトリガーされます。
6052	400036	DNS Zone Transfer from High Port	Informational	送信元ポートが 53 以外のときに不正な DNS ゾーン転送が発生するとトリガーされます。
6053	400037	DNS Request for All Records	Informational	すべてのレコードに対する DNS 要求があるとトリガーされます。

表 16-1　シグニチャ ID とシステム メッセージ番号 （続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
6100	400038	RPC Port Registration	Informational	ターゲット ホストで新しい RPC サービスを登録する試みがあるとトリガーされます。
6101	400039	RPC Port Unregistration	Informational	ターゲット ホストで既存の RPC サービスを登録解除する試みがあるとトリガーされます。
6102	400040	RPC Dump	Informational	ターゲット ホストに対して RPC ダンプ要求が発行されるとトリガーされます。
6103	400041	Proxied RPC Request	Attack	ターゲット ホストのポートマッパーにプロキシ RPC 要求が送信されるとトリガーされます。
6150	400042	ypserv (YP server daemon) Portmap Request	Informational	YP サーバ デーモン（ypserv）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6151	400043	ypbind (YP bind daemon) Portmap Request	Informational	YP バインド デーモン（ypbind）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6152	400044	yppasswdd (YP password daemon) Portmap Request	Informational	YP パスワード デーモン（yppasswdd）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6153	400045	ypupdated (YP update daemon) Portmap Request	Informational	YP 更新デーモン（ypupdated）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6154	400046	ypxfrd (YP transfer daemon) Portmap Request	Informational	YP 転送デーモン（ypxfrd）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6155	400047	mountd (mount daemon) Portmap Request	Informational	マウント デーモン（mountd）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6175	400048	rexd (remote execution daemon) Portmap Request	Informational	リモート実行デーモン（rexd）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6180	400049	rexd (remote execution daemon) Attempt	Informational	rexd プログラムの呼び出しが行われるとトリガーされます。リモート実行デーモンは、プログラムをリモート実行する役割を担うサーバです。rexd プログラムの呼び出しは、システム リソースへの不正アクセスの試みを示唆している場合があります。
6190	400050	statd Buffer Overflow	Attack	サイズの大きな statd 要求が送信されるとトリガーされます。これは、バッファをオーバーフローさせてシステムへアクセスしようとする試みの可能性があります。

例

次に、シグニチャ 6100 をディセーブルにする例を示します。

```
hostname(config)# ip audit signature 6100 disable
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	監査ポリシーをインターフェイスに割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
show running-config ip audit signature	**ip audit signature** コマンド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。これにより、別のグループ ポリシーの値を継承できます。

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

no ip-comp

構文の説明

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ 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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

データ圧縮をイネーブルにすると、モデムで接続するリモート ダイヤルイン ユーザのデータ伝送レートが向上する場合があります。

注意　データ圧縮を使用すると、各ユーザ セッションのメモリ要件と CPU 使用率が高くなり、その結果セキュリティ アプライアンス全体のスループットが低下します。そのため、データ圧縮はモデムで接続しているリモート ユーザに対してだけ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 ポリシーを設計し、それらのユーザに対してだけ圧縮をイネーブルにします。

例

次に、「FirstGroup」というグループ ポリシーの 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 local pool

VPN リモート アクセス トンネルに使用される 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*

構文の説明

first-address	IP アドレスの範囲における開始アドレスを指定します。
last-address	IP アドレスの範囲における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 プールの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

VPN クライアントに割り当てられた IP アドレスが標準以外のネットワークに属しているときには、マスク値を指定する必要があります。デフォルト マスクを使用した場合には、データが誤ってルーティングされることがあります。典型的な例が、IP ローカル プールに 10.10.10.0/255.255.255.0 アドレスが含まれている場合で、これはデフォルトではクラス A ネットワークです。この結果、VPN クライアントが異なるインターフェイス経由で 10 ネットワーク内の別のサブネットにアクセスする必要がある場合には、ある種のルーティング問題が発生することがあります。たとえば、アドレス 10.10.100.1/255.255.255.0 のプリンタがインターフェイス 2 を介して使用できるようになっているものの、10.10.10.0 ネットワークが VPN トンネルを経由するためインターフェイス 1 で使用できるようになっている場合、VPN クライアントはプリンタ宛てのデータのルーティング先を正確に把握できなくなります。10.10.10.0 と 10.10.100.0 のサブネットは両方とも、10.0.0.0 クラス A ネットワークに分類されるため、プリンタ データが VPN トンネル経由で送信される可能性があります。

例

次に、firstpool という名前で 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、最終アドレスは 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 コンフィギュレーションを表示します。特定の IP アドレス プールを指定するには、その名前をコマンドに含めます。

ip-phone-bypass

IP Phone Bypass 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 Bypass 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 Bypass 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。このオプションにより、別のグループ ポリシーから IP Phone Bypass の値を継承できます。

IP Phone Bypass を使用すると、ハードウェア クライアントの背後にある IP フォンが、ユーザ認証プロセスなしで接続できます。イネーブルの場合、セキュア ユニット認証は有効のままになります。

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

no ip-phone-bypass

構文の説明

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

デフォルト

IP Phone Bypass 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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ 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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

IP Phone Bypass は、ユーザ認証をイネーブルにした場合にだけ設定する必要があります。

例

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

```
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対して、接続前にセキュリティ アプライアンスに識別情報を示すように要求します。

ips

ASA 5500 シリーズ適応型セキュリティ アプライアンスは、AIP SSM をサポートします。これは、プロアクティブでフル機能の侵入防御サービスを提供する高度な IPS ソフトウェアを実行して、ワームやネットワーク ウイルスなど悪意のあるトラフィックを停止し、ネットワークに影響が及ばないようにします。インスペクションのために適応型セキュリティ アプライアンスから AIP SSM にトラフィックを迂回させるには、クラス コンフィギュレーション モードで **ips** コマンドを使用します。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。

ips {**inline** | **promiscuous**} {**fail-close** | **fail-open**} [**sensor** {*sensor_name* | *mapped_name*}]

no ips {**inline** | **promiscuous**} {**fail-close** | **fail-open**} [**sensor** {*sensor_name* | *mapped_name*}]

構文の説明

fail-close	AIP SSM で障害が発生した場合には、トラフィックをブロックします。
fail-open	AIP SSM で障害が発生しても、トラフィックを許可します。
inline	パケットを AIP SSM に向けて送ります。パケットは、IPS が動作した結果、ドロップされる場合があります。
promiscuous	AIP SSM 向けにパケットを複製します。AIP SSM が元のパケットをドロップすることはできません。
sensor {*sensor_name* | *mapped_name*}	このトラフィックの仮想センサー名を設定します。AIP SSM（バージョン 6.0 以降）で仮想センサーを使用する場合は、この引数を使用してセンサー名を指定できます。使用可能なセンサー名を表示するには、**ips ... sensor ?** コマンドを使用します。使用可能なセンサーの一覧が表示されます。また、**show ips** コマンドを使用することもできます。 適応型セキュリティ アプライアンスでマルチ コンテキスト モードを使用する場合は、コンテキストに割り当てたセンサーのみを指定できます（**allocate-ips** コマンドを参照）。コンテキストで設定する場合は、*mapped_name* を使用します。 センサー名を指定しないと、トラフィックはデフォルトのセンサーを使用します。マルチ コンテキスト モードでは、コンテキストのデフォルトのセンサーを指定できます。シングル モードの場合、またはマルチ モードでデフォルトのセンサーを指定しない場合、トラフィックは AIP SSM に設定されているデフォルトのセンサーを使用します。 AIP SSM にまだ存在しない名前を入力した場合は、エラーが発生し、コマンドが拒否されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
8.0(2)	仮想センサーのサポートが追加されました。

使用上のガイドライン

適応型セキュリティ アプライアンスに **ips** コマンドを設定する前または後に、AIP SSM にセキュリティ ポリシーを設定します。適応型セキュリティ アプライアンスから AIP SSM へのセッションを確立できるか（**session** コマンド）、または管理インターフェイスで SSH または Telnet を使用して直接 AIP SSM に接続できます。または、ASDM を使用する方法もあります。AIP SSM の設定の詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*』を参照してください。

ips コマンドを設定するには、先に **class-map** コマンド、**policy-map** コマンド、および **class** コマンドを設定する必要があります。

AIP SSM は、適応型セキュリティ アプライアンスとは別のアプリケーションを実行します。ただし、アプリケーションは適応型セキュリティ アプライアンスのトラフィック フローに統合されています。AIP SSM には、管理インターフェイス以外に外部インターフェイス自体は含まれていません。適応型セキュリティ アプライアンスでトラフィック クラスに対して **ips** コマンドを適用すると、トラフィックは次のように適応型セキュリティ アプライアンスおよび AIP SSM を経由します。

1. トラフィックが適応型セキュリティ アプライアンスに入ります。
2. ファイアウォール ポリシーが適用されます。
3. トラフィックがバックプレーン経由で AIP SSM に送信されます（**inline** キーワードを使用します。トラフィックのコピーを AIP SSM に送信するだけの場合の詳細については、**promiscuous** キーワードを参照してください）。
4. AIP SSM が、セキュリティ ポリシーをトラフィックに適用し、適切なアクションを実行します。
5. 有効なトラフィックがバックプレーン経由で適応型セキュリティ アプライアンスに返送されます。AIP SSM が、セキュリティ ポリシーに従ってトラフィックをブロックすることがあり、そのトラフィックは渡されません。
6. VPN ポリシーが適用されます（設定されている場合）。
7. トラフィックが適応型セキュリティ アプライアンスを終了します。

例

次に、無差別モードですべての IP トラフィックを AIP SSM に迂回させ、何らかの理由で AIP SSM カードで障害が発生した場合にはすべての IP トラフィックをブロックする例を示します。

```
hostname(config)# access-list IPS permit ip any any
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list IPS
hostname(config-cmap)# policy-map my-ips-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips promiscuous fail-close
hostname(config-pmap-c)# service-policy my-ips-policy global
```

次に、インライン モードで 10.1.1.0 ネットワークおよび 10.2.1.0 ネットワーク宛てのすべての IP トラフィックを AIP SSM に迂回させ、何らかの理由で AIP SSM カードで障害が発生してもすべてのトラフィックを許可する例を示します。my-ips-class トラフィックにはセンサー 1 が使用され、my-ips-class2 トラフィックにはセンサー 2 が使用されます。

```
hostname(config)# access-list my-ips-acl permit ip any 10.1.1.0 255.255.255.0
hostname(config)# access-list my-ips-acl2 permit ip any 10.2.1.0 255.255.255.0
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list my-ips-acl
```

```
hostname(config)# class-map my-ips-class2
hostname(config-cmap)# match access-list my-ips-acl2
hostname(config-cmap)# policy-map my-ips-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips inline fail-open sensor sensor1
hostname(config-pmap)# class my-ips-class2
hostname(config-pmap-c)# ips inline fail-open sensor sensor2
hostname(config-pmap-c)# service-policy my-ips-policy interface outside
```

関連コマンド

コマンド	説明
allocate-ips	セキュリティ コンテキストに仮想センサーを割り当てます。
class	トラフィック分類に使用するクラス マップを指定します。
class-map	ポリシー マップ用にトラフィックを識別します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
show running-config policy-map	現在のすべての**ポリシー マップ** コンフィギュレーションを表示します。

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。これにより、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 through NAT とも呼ばれる IPSec over UDP を使用すると、Cisco VPN Client またはハードウェア クライアントは NAT を実行しているセキュリティ アプライアンスに UDP 経由で接続できます。

ipsec-udp {enable | disable}

no ipsec-udp

構文の説明

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ 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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

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。

さらに、IPSec over UDP を使用するように Cisco VPN Client を設定する必要があります（デフォルトで使用するように設定されています）。VPN 3002 では、IPSec over UDP を使用するためのコンフィギュレーションが必要ありません。

IPSec over UDP は独自仕様で、リモート アクセス接続にだけ適用され、モード コンフィギュレーションが必要です。つまり、セキュリティ アプライアンスは SA のネゴシエーション中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 パフォーマンスが若干低下します。

例

次に、FirstGroup というグループ ポリシーの 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	セキュリティ アプライアンスが UDP トラフィックを受信するポートを指定します。

ipsec-udp-port

IPSec over UDP の 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。これにより、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 ネゴシエーションでは、セキュリティ アプライアンスは設定されたポートで待ち受け、他のフィルタ ルールによって UDP トラフィックがドロップされた場合でも、そのポート宛てに UDP トラフィックを転送します。

ipsec-udp-port *port*

no ipsec-udp-port

構文の説明

port	4001 ～ 49151 の範囲内の整数を使用して、UDP ポート番号を識別します。

デフォルト

デフォルトのポートは 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	透過	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

この機能をイネーブルにすると、複数のグループ ポリシーを設定し、各グループ ポリシーでそれぞれ別のポート番号を使用できます。

例

次に、FirstGroup というグループ ポリシーの IPSec UDP ポートをポート 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	Cisco VPN Client またはハードウェア クライアントは、NAT を実行しているセキュリティ アプライアンスに UDP 経由で接続できるようにします。

ip verify reverse-path

ユニキャスト 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。Unicast RPF は、ルーティング テーブルに従い、すべてのパケットが正しい発信元インターフェイスと一致する送信元 IP アドレスを持っていることを確認して、IP スプーフィング（パケットが不正な送信元 IP アドレスを使用し、実際の送信元を隠蔽すること）から保護します。

ip verify reverse-path interface *interface_name*

no ip verify reverse-path interface *interface_name*

構文の説明

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。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

通常、セキュリティ アプライアンスは、パケットの転送先を判定するときに宛先アドレスだけを調べます。Unicast RPF は、送信元アドレスも調べるようにセキュリティ アプライアンスに指示します。そのため、逆経路転送（Reverse Path Forwarding）と呼ばれます。セキュリティ アプライアンスの通過を許可するすべてのトラフィックについて、送信元アドレスに戻るルートをセキュリティ アプライアンスのルーティング テーブルに含める必要があります。詳細については、RFC 2267 を参照してください。

たとえば、外部トラフィックの場合、セキュリティ アプライアンスはデフォルト ルートを使用して Unicast RPF 保護の条件を満たすことができます。トラフィックが外部インターフェイスから入り、送信元アドレスがルーティング テーブルにない場合、セキュリティ アプライアンスはデフォルト ルートを使用して、外部インターフェイスを発信元インターフェイスとして正しく識別します。

ルーティング テーブルにあ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入り、このアドレスが内部インターフェイスに関連付けられている場合、セキュリティ アプライアンスはパケットをドロップします。同様に、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入った場合は、一致するルート（デフォルト ルート）が外部インターフェイスを示しているため、セキュリティ アプライアンスはパケットをドロップします。

Unicast 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ないため、個々のパケットはチェックされません。
- UDP と TCP にはセッションがあるため、最初のパケットは逆ルート ルックアップが必要です。セッション中に到着する後続のパケットは、セッションの一部として保持されている既存の状態を使用してチェックされます。最初のパケット以外のパケットは、最初のパケットと同じインターフェイスに到着したことを保証するためにチェックされます。

例

次に、外部インターフェイスでユニキャスト 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** コンフィギュレーションをクリアします。
clear ip verify statistics	ユニキャスト RPF の統計情報をクリアします。
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** コンフィギュレーションを表示します。

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 リストには、セキュリティ アプライアンスが通過を許可またはブロックす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**]]

構文の説明

any	IPv6 プレフィックス ::/0 の省略形で、任意の IPv6 アドレスを示します。
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	条件に一致する場合、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 メッセージングをディセーブルにします。
host	アドレスが特定のホストを指すよう指定します。
icmp6	セキュリティ アプライアンスを通過する ICMPv6 トラフィックにアクセス ルールを適用することを指定します。

icmp_type	アクセス ルールによってフィルタリングされる ICMP メッセージ 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 リテラルのいずれかを指定できます。 • 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* 引数を省略すると、すべての ICMP タイプを指定したことになります。
icmp_type_obj_grp_id	（任意）オブジェクト グループ 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）106100 syslog メッセージを生成する時間間隔を指定します。有効な値は、1 ～ 600 秒です。デフォルトの interval は 300 秒です。この値は、非アクティブなフローを削除するための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 の 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（情報）です。
line *line-num*	（任意）アクセス ルールの挿入先となるリスト内の行番号。行番号を指定しなかった場合は、アクセス リストの末尾に ACE が追加されます。
log	（任意）ACE に対するロギング アクションを指定します。**log** キーワードを指定しないか、または **log default** キーワードを指定した場合、ACE によってパケットが拒否されると、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、レベルまたは間隔とともに指定した場合、ACE によってパケットが拒否されると、メッセージ 106100 が生成されます。アクセス リストの末尾にある暗黙的な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 で明示的にパケットを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 アドレスを宛先 IP アドレスと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 ポートまたは宛先 IP アドレス ポートを比較するためのものです。有効なオペランドには、より小さいを表す **lt**、より大きいを表す **gt**、一致を表す **eq**、不一致を表す **neq**、包含範囲を表す **range** があります。演算子およびポートを指定せずに **ipv6 access-list** コマンドを使用すると、デフォルトではすべてのポートを指定したことになります。
permit	条件が一致した場合に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。*port* 引数を入力する際、0 ～ 65535 の範囲の番号でポートを指定できます。また、*protocol* が **tcp** または **udp** である場合には、リテラル名を使用できます。 許可される TCP 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。 許可される UDP 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	アドレスの高次の連続ビットのうち、何個が IPv6 プレフィックス（IPv6 アドレスのネットワーク部分）を構成しているかを指定します。
protocol	IP プロトコルの名前または番号。有効な値は、**icmp**、**ip**、**tcp**、**udp**、または IP プロトコル番号を表す 1 ～ 254 の範囲の整数です。
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 トラフィックの送信元である 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（情報）です。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ipv6 access-list コマンドを使用すると、IPv6 アドレスにポートまたはプロトコルへのアクセスを許可するのか拒否するのかを指定できます。各コマンドは ACE と呼ばれます。同じアクセス リスト名を持つ 1 つまたは複数の ACE はアクセス リストと呼ばれます。**access-group** コマンドを使用して、インターフェイスにアクセス リストを適用します。

セキュリティ アプライアンスは、アクセス リストを使用して明示的にアクセスを許可しない限り、外部インターフェイスから内部インターフェイスへのパケットをすべて拒否します。内部インターフェイスから外部インターフェイスへのパケットは、明示的にアクセスを拒否しない限り、デフォルトですべて許可されます。

ipv6 access-list コマンドは、IPv6 固有である点を除いて、**access-list** コマンドに似ています。アクセス リストの詳細については、**access-list extended** コマンドを参照してください。

ipv6 access-list icmp コマンドは、セキュリティ アプライアンスを通過する ICMPv6 メッセージをフィルタリングするために使用されます。特定のインターフェイスでの発信および終端が許可される 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 グループを設定する方法については、**object-group** コマンドを参照してください。

例

次に、ホストが TCP を使用して 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
```

次の例では、**eq** とポートを使用して、FTP へのアクセスだけを拒否します。

```
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
```

次の例では、**lt** を使用して、2025 より小さいすべてのポートへのアクセスを許可します。これにより、予約済みポート（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	アクセス リストをインターフェイスに割り当てます。
ipv6 icmp	セキュリティ アプライアンスのインターフェイスで終了する ICMP メッセージに対するアクセス 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 webtype

クライアントレス SSL VPN に対するフィルタリングをサポートする設定に追加できる IPv6 アクセス リストを作成するには、グローバル コンフィギュレーション モードで **access-list webtype** コマンドを使用します。アクセス リストを削除するには、このコマンドの **no** 形式を使用し、構文ストリング全体をコンフィギュレーションにあるとおりに指定します。

ipv6 access-list *id* **webtype** {**deny** | **permit**} **url** [**url_string** | **any**]

no ipv6 access-list *id* **webtype** {**deny** | **permit**} **url** [**url_string** | **any**]

構文の説明

id	アクセス リストの名前または番号。
any	すべての対象へのアクセスを指定します。
deny	条件に一致する場合、アクセスを拒否します。
permit	条件に合致している場合、アクセスを許可します。
url	フィルタリングに URL を使用することを指定します。
url_string	（任意）フィルタリングする URL を指定します。

デフォルト

デフォルトの設定は次のとおりです。

- 特にアクセスを許可しない限り、適応型セキュリティ アプライアンスによって、発信元インターフェイス上のすべてのパケットが拒否されます。
- ACL ロギングでは、拒否されたパケットについてシステム ログ メッセージ 106023 が生成されます。拒否されたパケットをログに記録するには、パケットを明示的に拒否する必要があります。

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

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが導入されました。

使用上のガイドライン

次のワイルドカード文字を使用すると、Webtype アクセス リスト エントリに複数のワイルドカードを定義できます。

- 0 個以上の任意の数の文字に一致させるには、アスタリスク「*」を入力します。
- 任意の 1 文字に正確に一致させるには、疑問符「?」を入力します。
- 範囲内の任意の 1 文字に一致する範囲演算子を作成するには、角カッコ「[ ]」を入力します。

例

この項の例では、IPv6 Webtype アクセス リストでのワイルドカードの使用方法を示します。

- 次に、http://www.cisco.com/ や http://wwz.caco.com/ などの URL に一致させる例を示します。

```
ipv6 access-list test webtype permit url http://ww?.c*co*/
```

- 次に、http://www.cisco.com や ftp://wwz.carrier.com などの URL に一致させる例を示します。

```
ipv6 access-list test webtype permit url *://ww?.c*co*/
```

- 次の例は、http://www.cisco.com:80 や https://www.cisco.com:81 などの URL に一致します。

```
ipv6 access-list test webtype permit url *://ww?.c*co*:8[01]/
```

上記の例に示した range 演算子「[]」は、文字 0 または 1 が出現可能であることを指定します。

- 次に、http://www.google.com や http://www.boogie.com などの URL に一致させる例を示します。

```
ipv6 access-list test webtype permit url http://www.[a-z]oo?*/
```

上記の例に示した range 演算子「[]」は、a ～ z の範囲内の任意の 1 文字が出現可能であることを指定します。

- 次の例は、http://www.cisco.com/anything/crazy/url/ddtscgiz などの URL に一致します。

```
ipv6 access-list test webtype permit url htt*://*/*cgi?*
```

（注） 任意の http URL に一致させるには、http://* を入力するというこれまでの方法ではなく、http://*/* を入力する必要があります。

関連コマンド

コマンド	説明
access-group	コンフィギュレーションの最適化に使用できるオブジェクト グループを定義します。
access-list ethertype	EtherType に基づいてトラフィックを制御するアクセス リストを設定します。
access-list extended	アクセス リストをコンフィギュレーションに追加し、適応型セキュリティ アプライアンスを通過する IP トラフィック用のポリシーを設定します。
clear access-group	アクセス リスト カウンタをクリアします。
show running-config access-list	適応型セキュリティ アプライアンスで実行されているアクセス リスト コンフィギュレーションを表示します。

ipv6 address

IPv6 をイネーブルにし、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**}

構文の説明

autoconfig	インターフェイスでステートレス自動設定を使用して、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 ビットにインターフェイス ID を指定します。
ipv6-address	インターフェイスに割り当てられた 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られた 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	アドレスの高次の連続ビットのうち、何個が IPv6 プレフィックス（IPv6 アドレスのネットワーク部分）を構成しているかを指定します。

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	透過	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイスに 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。IPv6 アドレスを指定した後で **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てインターフェイスで IPv6 アドレスの自動設定をイネーブルにするために使用されます。アドレスは、ルータ アドバタイズメント メッセージで受信したプレフィッ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ければ、アドレスはこのインターフェイス用に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には、エラー メッセージが表示されます。

ipv6 address eui-64 コマンドは、インターフェイスの IPv6 アドレスを設定するために使用されます。任意の **eui-64** を指定した場合、アドレスの下位 64 ビットに EUI-64 インターフェイス ID が使用されます。*prefix-length* 引数に指定されている値が 64 ビットを超えている場合は、プレフィックス ビットがインターフェイス ID よりも優先されます。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。

Modified EUI-64 形式のインターフェイス ID は、リンク層アドレスの上位 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 進数の FFFE を挿入することで、48 ビット リンク層（MAC）アドレスから導出されます。選択されたアドレスが一意のイーサネット MAC アドレスから生成されることを保証するため、上位バイトの下位から 2 番めのビット（ユニバーサル/ローカル ビット）が反転され、48 ビット アドレスの一意性が示されます。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 の 64 ビット インターフェイス ID が指定されます。

ipv6 address link-local コマンドは、インターフェイスの IPv6 リンクローカル アドレスを設定するために使用されます。このコマンドに指定された *ipv6-address* は、インターフェイス用に自動的に生成されるリンクローカル アドレスを上書きします。リンクローカル アドレスは、リンクローカル プレフィックス 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 アドレスが 00E0.B601.3B7A のインターフェイスの場合、リンクローカル アドレスは FE80::2E0:B6FF:FE01:3B7A になります。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 gigabitethernet 0/0
hostname(config-if)# ipv6 address 3ffe:c00:0:1::576/64
```

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

```
hostname(config)# interface gigabitethernet 0/1
hostname(config-if)# ipv6 address autoconfig
```

次の例では、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、アドバイザーの下位 64 ビットに EUI-64 インターフェイス ID を指定します。

```
hostname(config)# interface gigabitethernet 0/2
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 gigabitethernet 0/3
hostname(config-if)# 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 用に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 アドレスが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 アドレスでまだ設定されていないインターフェイスで 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

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

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	透過	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ipv6 enable コマンドは、インターフェイスに IPv6 リンクローカル ユニキャスト アドレスを自動的に設定し、さらにインターフェイスを IPv6 処理用にイネーブルにします。

明示的な IPv6 アドレスで設定されているインターフェイスで **no ipv6 enable** コマンドを実行しても、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で IPv6 処理をイネーブルにする例を示します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 enable
```

関連コマンド

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

ipv6 enforce-eui64

ローカル リンク上の IPv6 アドレスに Modified EUI-64 形式のインターフェイス ID の使用を適用するには、グローバル コンフィギュレーション モードで **ipv6 enforce-eui64** コマンドを使用します。Modified EUI-64 アドレス形式の適用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 enforce-eui64 *if_name*

no ipv6 enforce-eui64 *if_name*

構文の説明

if_name	Modified EUI-64 アドレス形式の適用をイネーブルにするインターフェイスの名前を **nameif** コマンドで指定されているとおりに指定します。

デフォルト

Modified EUI-64 形式の適用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。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドがインターフェイスでイネーブルになっていると、そのインターフェイス ID が Modified EUI-64 形式を採用していることを確認するために、インターフェイスで受信した IPv6 パケットの送信元アドレスが送信元 MAC アドレスに照らして確認されます。IPv6 パケットがインターフェイス ID に Modified EUI-64 形式を採用していない場合、パケットはドロップされ、次のシステム ログ メッセージが生成されます。

```
%PIX|ASA-3-325003: EUI-64 source address check failed.
```

アドレス形式の確認は、フローが作成される場合にのみ実行されます。既存のフローからのパケットは確認されません。また、アドレスの確認はローカル リンク上のホストに対してのみ実行できます。ルータの背後にあるホストから受信したパケットは、アドレス形式の検証に失敗してドロップされます。これは、その送信元 MAC アドレスがルータの MAC アドレスであり、ホストの MAC アドレスではないためです。

48 ビット リンク層（MAC）アドレスから Modified EUI-64 形式のインターフェイス ID を取得するには、リンク層アドレスの上位 3 バイト（OUI フィールド）と下位 3 バイト（シリアル番号）との間に 16 進数 FFFE を挿入します。選択されたアドレスが一意のイーサネット MAC アドレスから生成され

ることを保証するため、上位バイトの下位から 2 番めのビット（ユニバーサル/ローカル ビット）が反転され、48 ビット アドレスの一意性が示されます。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 の 64 ビット インターフェイス ID が指定されます。

例

次に、内部インターフェイスで受信した IPv6 アドレスに対して Modified EUI-64 形式の適用をイネーブルにする例を示します。

```
hostname(config)# ipv6 enforce-eui64 inside
```

関連コマンド

コマンド	説明
ipv6 address	インターフェイスで IPv6 アドレスを設定します。
ipv6 enable	インターフェイス上で IPv6 をイネーブルにします。

ipv6 icmp

インターフェイスの 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*

構文の説明

any	IPv6 アドレスを指定するキーワード。IPv6 プレフィックス ::/0 の省略形。
deny	選択したインターフェイスで指定の ICMP トラフィックを阻止します。
host	アドレスが特定のホストを指すよう指定します。
icmp-type	アクセス ルールによってフィルタリングされる ICMP メッセージ 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 リテラルのいずれかを指定できます。 • 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
if-name	アクセス ルールが適用されるインターフェイスの名前（**nameif** コマンドで指定した名前）。
ipv6-address	ICMPv6 メッセージをインターフェイスに送信しているホストの IPv6 アドレス。
ipv6-prefix	ICMPv6 メッセージをインターフェイスに送信している IPv6 ネットワーク。
permit	選択したインターフェイスで指定の ICMP トラフィックを許可します。
prefix-length	IPv6 プレフィックスの長さ。この値は、アドレスの高次の連続ビットのうち、プレフィックスのネットワーク部分を構成しているビットの数を示します。プレフィックス長の前にスラッシュ（/）を使用する必要があります。

デフォルト

ICMP アクセス ルールが定義されていない場合、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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

IPv6 の ICMP は、IPv4 の ICMP と同じ働きをします。ICMPv6 によって、ICMP 宛先到達不能メッセージなどのエラー メッセージや、ICMP エコー要求および応答メッセージのような情報メッセージが生成されます。さらに、IPv6 の ICMP パケットは IPv6 ネイバー探索プロセスおよびパス MTU ディスカバリに使用されます。

インターフェイスに対して定義されている ICMP ルールがない場合、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対して定義されている ICMP ルールが複数ある場合は、最初に一致したルールから順に処理され、その後暗黙のすべて拒否ルールが続きます。たとえば、最初に一致したルールが許可ルールである場合、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である場合、または ICMP パケットがそのインターフェイスのどのルールにも一致しなかった場合、セキュリティ アプライアンスは ICMP パケットを廃棄し、syslog メッセージを生成します。

そのため、ICMP ルールを入力する順序が重要になります。特定のネットワークからの ICMP トラフィックをすべて拒否するルールを入力し、その後にそのネットワーク上の特定のホストからの ICMP トラフィックを許可するルールが続く場合、ホストのルールはいっさい処理されません。ICMP トラフィックは、ネットワークのルールによってブロックされます。ただし、ホストのルールを先に入力し、その後にネットワークのルールを続けた場合、そのホストからの ICMP トラフィックは許可され、そのネットワークからのそれ以外の ICMP トラフィックはブロックされます。

ipv6 icmp コマンドは、セキュリティ アプライアンス インターフェイスで終了する 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 ルールを設定するには、**ipv6 access-list** コマンド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 ディスカバリをサポートするため）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 またはプレフィックス 2001::/64 上のホストに対して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
hostname(config)# ipv6 icmp permit any packet-too-big 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 local pool

アドレスをリモート クライアントに割り当てるための IPv6 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 **ipv6 local pool** コマンドを使用します。コンフィギュレーションから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。

ipv6 local pool *pool_name ipv6_address/prefix_length number_of_addresses*

no ipv6 local pool *pool_name ipv6_address/prefix_length number_of_addresses*

構文の説明

pool_name	この IPv6 アドレス プールに割り当てる名前を指定します。
ipv6_address	設定する IPv6 アドレス プールを指定します。形式は x:x:x:: です。
number_of_addresses	範囲：1 ～ 16384
prefix_length	範囲：0 ～ 128

デフォルト

デフォルトでは、IPv6 ローカル アドレス プールは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

IPv6 ローカル プールを割り当てるには、トンネル グループで **ipv6-local-pool** コマンドを使用するか、またはグループ ポリシーで **ipv6-address-pools**（末尾の「s」に注意）コマンドを使用します。グループ ポリシーの ipv6-address-pools 設定は、トンネル グループの ipv6-address-pool 設定を上書きします。

例

次に、設定一般コンフィギュレーション モードを開始し、アドレスをリモート クライアントに割り当てるために使用される IPv6 アドレス プールを firstipv6pool という名前で設定する例を示します。

```
hostname(config)# ipv6 local pool firstipv6pool 2001:DB8::1001/32 100
hostname(config)#
```

関連コマンド

コマンド	説明
ipv6-address-pool	IPv6 アドレス プールを VPN トンネル グループ ポリシーに関連付けます。
ipv6-address-pools	IPv6 アドレス プールを VPN グループ ポリシーに関連付けます。
clear configure ipv6 local pool	設定済みのすべての IPv6 ローカル プールをクリアします。
show running-config ipv6	IPv6 のコンフィギュレーションを表示します。

ipv6 nd dad attempts

重複アドレス検出時にインターフェイスに連続して送信されるネイバー送信要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値に戻すには、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*]

構文の説明

value	0 ～ 600 までの数字。0 を入力すると、指定したインターフェイスでの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、後続の送信なしの単一の送信が設定されます。デフォルト値は 1 メッセージです。

デフォルト

デフォルトの試行回数は 1 回です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

アドレスがインターフェイスに割り当てられる前に、重複アドレス検出によって、新しいユニキャスト IPv6 アドレスの一意性が確認されます（重複アドレス検出の実行中、新しいアドレスは一時的な状態になります）。重複アドレス検出では、ネイバー送信要求メッセージを使用して、ユニキャスト IPv6 アドレスの一意性を確認します。ネイバー送信要求メッセージの送信頻度を設定するには、**ipv6 nd ns-interval** コマンドを使用します。

重複アドレス検出は、管理上ダウンしているインターフェイスでは停止します。インターフェイスが管理上ダウンしている間、そのインターフェイスに割り当てられたユニキャスト IPv6 アドレスは保留状態に設定されます。

インターフェイスが管理上アップ状態に戻ると、そのインターフェイスで重複アドレス検出が自動的に再起動されます。管理上アップ状態に戻っているインターフェイスでは、インターフェイス上のすべてのユニキャスト IPv6 アドレスを対象に重複アドレス検出が再起動されます。

（注）　インターフェイスのリンクローカル アドレスで重複アドレス検出が実行されている間、他の IPv6 アドレスの状態は仮承諾に設定されたままとなります。リンクローカル アドレスで重複アドレス検出が完了すると、残りの IPv6 アドレスで重複アドレス検出が実行されます。

重複アドレス検出によって重複アドレスが特定された場合、そのアドレスの状態は DUPLICATE に設定され、アドレスは使用されなくなります。重複アドレスがインターフェイスのリンクローカル アドレスの場合は、そのインターフェイス上で IPv6 パケットの処理がディセーブルになり、次のようなエラー メッセージが発行されます。

```
%PIX-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 アドレスである場合、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。

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

アドレスの状態が DUPLICATE に設定されている間、重複アドレスに関連付けられたコンフィギュレーション コマンドはすべて設定済みのままとなります。

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た場合、新しいリンクローカル アドレスで重複アドレス検出が実行され、インターフェイスに関連付けられた他のすべての IPv6 アドレスが再生成されます（重複アドレス検出は新規のリンクローカル アドレスでのみ実行されます）。

例

次に、重複アドレス検出がインターフェイスの仮承諾のユニキャスト IPv6 アドレスで実行された場合に、5 つ連続して送信されるネイバー送信要求メッセージを設定する例を示します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# 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 gigabitethernet 0/1
hostname(config-if)# ipv6 nd dad attempts 0
```

関連コマンド

コマンド	説明
ipv6 nd ns-interval	インターフェイスで IPv6 ネイバー送信要求メッセージが送信される時間間隔を設定します。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 nd ns-interval

インターフェイスで IPv6 ネイバー送信要求メッセージが再送信される時間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*]

構文の説明

value	IPv6 ネイバー送信要求メッセージが送信される時間間隔（ミリ秒単位）。有効な値の範囲は、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

ネイバー送信要求メッセージが送信される時間間隔は 1000 ミリ秒です。

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	透過	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

この値は、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 アドバタイズメントに含まれます。

例

次に、GigabitEthernet 0/0 の IPv6 ネイバー送信要求送信間隔を 9000 ミリ秒に設定する例を示します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd ns-interval 9000
```

関連コマンド

コマンド	説明
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 nd prefix

IPv6 ルータ アドバタイズメントにどの IPv6 プレフィックスを含めるかを設定するには、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。プレフィッ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**]

構文の説明

at *valid-date preferred-date*	ライフタイムおよびプリファレンスが期限切れになる日付と時刻。プレフィックスは、この指定された日付と時刻に達するまで有効です。日付は *date-valid-expire month-valid-expire hh:mm-valid-expire date-prefer-expire month-prefer-expire hh:mm-prefer-expire* の形式で表されます。
default	デフォルト値が使用されます。
infinite	（任意）有効なライフタイムが期限切れになりません。
ipv6-prefix	ルータ アドバタイズメントに含まれる IPv6 ネットワーク番号。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
no-advertise	（任意）ローカル リンク上のホストでは、指定されたプレフィックスが IPv6 自動設定に使用されないことを示します。
no-autoconfig	（任意）ローカル リンク上のホストでは、指定されたプレフィックスが IPv6 自動設定に使用できないことを示します。
off-link	（任意）指定されたプレフィックスがオンリンクの判別に使用されないことを示します。
preferred-lifetime	指定された IPv6 プレフィックスが優先プレフィックスとしてアドバタイズされる時間（秒単位）。有効値の範囲は 0 ～ 4294967295 秒です。最大値は無限ですが、これは infinite を使用して指定もできます。デフォルトは 604800（7 日間）です。
prefix-length	IPv6 プレフィックスの長さ。この値は、アドレスの高次の連続ビットのうち、プレフィックスのネットワーク部分を構成しているビットの数を示します。プレフィックス長の前にスラッシュ（/）を使用する必要があります。
valid-lifetime	指定された IPv6 プレフィックスが有効プレフィックスとしてアドバタイズされる時間。有効値の範囲は 0 ～ 4294967295 秒です。最大値は無限を表します。**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 アドバタイズメントを発信するインターフェイスに設定されているすべてのプレフィックスが、有効ライフタイム 2592000 秒（30 日）および優先ライフタイム 604800 秒（7 日）でアドバタイズされます。どちらのライフタイムにも「onlink」フラグと「autoconfig」フラグが設定されます。

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。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン　このコマンドを使用すると、プレフィックスをアドバタイズするかどうかなど、プレフィックスごとに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にアドレスとして設定されるプレフィックスは、ルータ アドバタイズメントでアドバタイズされます。**ipv6 nd prefix** コマンドを使用してアドバタイズメント用にプレフィックスを設定した場合は、そのプレフィッ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、すべてのプレフィックスのデフォルト パラメータを設定できます。

プレフィックスの有効期限を指定するための日付を設定できます。有効な推奨ライフタイムは、リアルタイムでカウントダウンされます。有効期限に達すると、プレフィックスはアドバタイズされなくなります。

onlink が「on」（デフォルト）である場合、指定されたプレフィックスがそのリンクに割り当てられます。指定されたプレフィックスを含むそのようなアドレスにトラフィックを送信するノードは、宛先がリンク上でローカルに到達可能であると見なします。

autoconfig が「on」（デフォルト）である場合、ローカル リンク上のホストに対して、指定されたプレフィックスが IPv6 自動設定に使用できることを示します。

例　次に、有効ライフタイムを 1000 秒、優先ライフタイムを 900 秒にして、指定したインターフェイスから送信されるルータ アドバタイズメントに IPv6 プレフィックス 2001:200::/35 を含める例を示します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd prefix 2001:200::/35 1000 900
```

関連コマンド

コマンド	説明
ipv6 address	IPv6 アドレスを設定し、インターフェイスで IPv6 処理をイネーブルにします。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 nd ra-interval

インターフェイス上で IPv6 ルータ アドバタイズメント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*]

構文の説明

msec	（任意）指定される値がミリ秒単位であることを示します。このキーワードが指定されていない場合、指定される値は秒単位となります。
value	IPv6 ルータ アドバタイズメントの送信間隔。有効な値の範囲は、3 ～ 1800 秒であるか、**msec** キーワードが指定されている場合には 500 ～ 1800000 ミリ秒です。デフォルトは 200 秒です。

デフォルト

200 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	透過	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ipv6 nd ra-lifetime コマンドを使用してセキュリティ アプライアンスがデフォルト ルータとして設定されている場合、送信間隔は IPv6 ルータ アドバタイズメントのライフタイム以下にする必要があります。他の IPv6 ノードとの同期を防止するには、実際に使用される値を指定値の 20 % 以内で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で IPv6 ルータ アドバタイズメントの間隔を 201 秒に設定する例を示します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# 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 アドバタイズメントのライフタイムを設定します。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 nd ra-lifetime

インターフェイス上で IPv6 ルータ アドバタイズメントに「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*]

構文の説明

seconds	セキュリティ アプライアンスがこのインターフェイスでデフォルト ルータであることの有効性。有効な値の範囲は、0 ～ 9000 秒です。デフォルトは 1,800 秒です。0 は、セキュリティ アプライアンスを、選択したインターフェイス上のデフォルト ルータと見なしてはならないことを示します。

デフォルト

1800 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	透過	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

「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 アドバタイズメントに含まれます。値は、セキュリティ アプライアンスがこのインターフェイス上でデフォルト ルータとして有効であることを示します。

値をゼロ以外の値に設定すると、セキュリティ アプライアンスがこのインターフェイス上でデフォルト ルータであると見なされます。「ルータ ライフタイム」値をゼロ以外の値にする場合、ルータ アドバタイズメント間隔を下回る値にはしないでください。

値を 0 に設定すると、セキュリティ アプライアンスがこのインターフェイス上でデフォルト ルータであると見なされません。

例

次に、選択したインターフェイス上で IPv6 ルータ アドバタイズメントのライフタイムを 1801 秒に設定する例を示します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd ra-lifetime 1801
```

関連コマンド

コマンド	説明
ipv6 nd ra-interval	インターフェイスで IPv6 Router Advertisement（RA; ルータ アドバタイズメント）メッセージが送信される時間間隔を設定します。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 nd reachable-time

到達可能性確認イベントが発生した後でリモート IPv6 ノードが到達可能であると見なされる時間を設定するには、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*]

構文の説明

value	リモート IPv6 ノードが到達可能であると見なされる時間（ミリ秒単位）。有効な値の範囲は、0 ～ 3600000 ミリ秒です。デフォルト値は 0 です *value* に 0 を使用すると、到達可能時間が未定のまま送信されます。到達可能時間の値を設定し、追跡するのは、受信デバイスの役割です。

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	透過	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

時間を設定すると、使用不可能なネイバーの検出がイネーブルになります。設定時間を短くすると、使用不可能なネイバーをさらに迅速に検出できます。ただし、時間を短くすると、すべての IPv6 ネットワーク デバイスで IPv6 ネットワーク帯域幅および処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。

このコマンドが 0 に設定されている際の実際の値を含め、セキュリティ アプライアンスで使用されている到達可能時間を参照するには、**show ipv6 interface** コマンドを使用して、使用されている ND 到達可能時間など IPv6 インターフェイスに関する情報を表示します。

例

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

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd reachable-time 1700000
```

関連コマンド

コマンド	説明
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 nd suppress-ra

LAN インターフェイスで IPv6 ルータ アドバタイズメント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 アドバタイズメントの送信を再び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。

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

IPv6 ユニキャスト ルーティングがイネーブルになっている場合、ルータ アドバタイズメントは LAN インターフェイスで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	透過	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	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

LAN 以外のインターフェイス タイプ（たとえばシリアル インターフェイスやトンネル インターフェイス）で IPv6 ルータ アドバタイズメントの送信をイネーブルにするには、**no ipv6 nd suppress-ra** コマンドを使用します。

例

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

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd suppress-ra
```

関連コマンド

コマンド	説明
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 neighbor

IPv6 ネイバー探索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。ネイバー探索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*]

構文の説明

if_name	**nameif** コマンドで指定された内部インターフェイス名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

スタティック エントリは、IPv6 ネイバー探索キャッシュに設定されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ipv6 neighbor コマンドは、**arp** コマンドに似ています。IPv6 ネイバー探索プロセスによる学習を通して、指定された IPv6 アドレスのエントリがネイバー探索キャッシュにすでに存在する場合、エントリは自動的にスタティック エントリに変換されます。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格納すると、コンフィギュレーションに格納されます。

IPv6 ネイバー探索キャッシュのスタティック エントリを表示するには、**show ipv6 neighbor** コマンドを使用します。

clear ipv6 neighbors コマンドは、スタティック エントリを除いて IPv6 ネイバー探索キャッシュのすべてのエントリを削除します。**no ipv6 neighbor** コマンドは、ネイバー探索キャッシュから指定のスタティック エントリを削除します。ダイナミック エントリ（IPv6 ネイバー探索プロセスから学習したエントリ）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で IPv6 をディセーブルにすると、スタティック エントリを除いて、そのインターフェイス用に設定されたすべての IPv6 ネイバー探索キャッシュ エントリが削除されます（エントリの状態が INCMP [Incomplete] に変更されます）。

IPv6 ネイバー探索キャッシュ内のスタティック エントリがネイバー探索プロセスによって変更されることはありません。

例

次に、IPv6 アドレスを 3001:1::45A、MAC アドレスを 0002.7D1A.9472 にして、内部ホスト用のスタティック エントリをネイバー探索キャッシュに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	スタティック エントリを除く、IPv6 ネイバー探索キャッシュ内のすべてのエントリを削除します。
show ipv6 neighbor	IPv6 ネイバー キャッシュ情報を表示します。

ipv6 route

IPv6 ルートを IPv6 ルーティング テーブルに追加するには、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 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* | **tunneled**]

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

構文の説明

administrative-distance	（任意）ルートのアドミニストレーティブ ディスタンス。デフォルト値は 1 です。この場合、スタティック ルートは接続ルートを除く他のどのタイプのルートよりも優先されます。
if_name	ルートが設定されているインターフェイスの名前。
ipv6-address	指定したネットワークに到達するために使用可能なネクスト 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 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
prefix-length	IPv6 プレフィックスの長さ。この値は、アドレスの高次の連続ビットのうち、プレフィックスのネットワーク部分を構成しているビットの数を示します。プレフィックス長の前にスラッシュ（/）を使用する必要があります。
tunneled	（任意）ルートを VPN トラフィックのデフォルト トンネル ゲートウェイとして指定します。

デフォルト

デフォルトでは、*administrative-distance* 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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

IPv6 ルーティング テーブルの内容を表示するには、**show ipv6 route** コマンドを使用します。

トンネル トラフィックには、標準のデフォルト ルートの他に別のデフォルト ルートを 1 つ定義することができます。**tunneled** オプションを使用してデフォルト ルートを作成すると、セキュリティ アプライアンスに着信するトンネルからのすべてのトラフィックは、学習したルートまたはスタティック ルートを使用してルーティングできない場合、このルートに送信されます。トンネルから出るトラフィックの場合、このルートは、その他の設定または学習されたデフォルト ルートをすべて上書きします。

tunneled オプションを使用したデフォルト ルートには、次の制約事項が適用されます。

- トンネル ルートの出力インターフェイスで、ユニキャスト RPF（**ip verify reverse-path**）をイネーブルにしないでください。トンネル ルートの出力インターフェイスで uRPF をイネーブルにすると、セッションに障害が発生します。
- トンネル ルートの出力インターフェイスで、TCP 代行受信をイネーブルにしないでください。イネーブルにすると、セッションでエラーが発生します。
- VoIP インスペクション エンジン（CTIQBE、H.323、GTP、MGCP、RTSP、SIP、SKINNY）、DNS インスペクション エンジン、または DCE RPC インスペクション エンジンは、トンネル ルートでは使用しないでください。これらのインスペクション エンジンは、トンネル ルートを無視します。

tunneled オプションを使用して複数のデフォルト ルートは定義できません。トンネル トラフィックの ECMP はサポートされていません。

例

次に、アドミニストレーティブ ディスタンスを 110 にして、ネットワーク 7fff::0/32 のパケットを 3FFE:1100:0:CC00::1 にある内部インターフェイス上のネットワーキング デバイスに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。

ipv6-address-pool（トンネル グループ一般属性モード）

アドレスをリモート クライアントに割り当てるための IPv6 アドレス プール リストを指定するには、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 **ipv6-address-pool** コマンドを使用します。IPv6 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。

ipv6-address-pool [(*interface_name*)] *ipv6_address_pool1* [*...ipv6_address_pool6*]

no ipv6-address-pool [(*interface_name*)] *ipv6_address_pool1* [*...ipv6_address_pool6*]

構文の説明

ipv6_address_pool	**ipv6 local pool** コマンドで設定したアドレス プールの名前を指定します。最大 6 個のローカル アドレス プールを指定できます。
interface_name	（任意）アドレス プールに使用するインターフェイスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

これらのコマンドは、インターフェイスごとに 1 つずつ、複数入力できます。インターフェイスが指定されていない場合、コマンドは明示的に参照されていないインターフェイスすべてに対してデフォルトを指定します。

グループ ポリシーの **ipv6-address-pools** コマンドの IPv6 アドレス プール設定は、トンネル グループの **ipv6-address-pool** コマンドの IPv6 アドレス プール設定を上書きします。

プールの指定順序は重要です。セキュリティ アプライアンスでは、このコマンドでプールを指定した順序に従って、それらのプールからアドレスが割り当てられます。

例

次に、設定トンネル一般コンフィギュレーション モードを開始し、IPSec リモート アクセス トンネル グループ テスト用に、アドレスをリモート クライアントに割り当てるための IPv6 アドレス プール リストを指定する例を示します。

```
hostname(config)# tunnel-group test type remote-access
hostname(config)# tunnel-group test general-attributes
```

```
hostname(config-tunnel-general)# ipv6-address-pool (inside) ipv6addrpool1 ipv6addrpool2
ipv6addrpool3
hostname(config-tunnel-general)#
```

関連コマンド

コマンド	説明
ipv6-address-pools	グループ ポリシーの IPv6 アドレス プール設定を設定します。これらの設定は、トンネル グループの IPv6 アドレス プール設定を上書きします。
ipv6 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 プールを設定します。
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。
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	トンネル グループを設定します。

ipv6-address-pools

アドレスをリモート クライアントに割り当てるための IPv6 アドレス プール リストを最大 6 つ指定するには、グループ ポリシー属性コンフィギュレーション モードで **ipv6-address-pools** コマンドを使用します。グループ ポリシーから属性を削除し、別のグループ ポリシー ソースからの継承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。

ipv6-address-pools value *ipv6_address_pool1* [*...ipv6_address_pool6*]

no ipv6-address-pools value *ipv6_address_pool1* [*...ipv6_address_pool6*]

ipv6-address-pools none

no ipv6-address-pools none

構文の説明

ipv6_address_pool	**ipv6 local pool** コマンドで設定した最大 6 つの IPv6 アドレス プールの名前を指定します。各 IPv6 アドレス プール名を区切るには、スペースを使用します。
none	IPv6 アドレス プールが設定されず、他のグループ ポリシーからの継承をディセーブルにすることを指定します。
value	アドレスを割り当てるための IPv6 アドレス プールを最大 6 つ指定します。

デフォルト

デフォルトでは、IPv6 アドレス プールの属性は設定されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

IPv6 アドレス プールを設定するには、**ipv6 local pool** コマンドを使用します。

ipv6-address-pools コマンドにプールを指定する順序は重要です。セキュリティ アプライアンスでは、このコマンドでプールを指定した順序に従って、それらのプールからアドレスが割り当てられます。

ipv6-address-pools none コマンドは、この属性が DefaultGrpPolicy など他のポリシーから継承されることをディセーブルにします。**no ipv6-address-pools none** コマンドは、コンフィギュレーションから **ipv6--address-pools none** コマンドを削除して、デフォルト値に戻します。これにより、継承が許可されます。

例

次に、設定一般コンフィギュレーション モードを開始し、アドレスをリモート クライアントに割り当てるために使用される IPv6 アドレス プールを firstipv6pool という名前で設定し、そのプールを GroupPolicy1 に関連付ける例を示します。

```
hostname(config)# ipv6 local pool firstipv6pool 2001:DB8::1000/32 100
hostname(config)# group-policy GroupPolicy1 attributes
hostname(config-group-policy)# ipv6-address-pools value firstipv6pool
hostname(config-group-policy)#
```

関連コマンド

コマンド	説明
ipv6 local pool	VPN グループ ポリシーに使用される IPv6 アドレス プールを設定します。
clear configure group-policy	設定されているすべてのグループ ポリシーをクリアします。
show running-config group-policy	すべてのグループ ポリシーまたは特定のグループ ポリシーのコンフィギュレーションを表示します。

ipv6-vpn-filter

VPN 接続に使用する ACL の名前を指定するには、グループ ポリシー モードまたはユーザ名モードで **ipv6-vpn-filter** コマンドを使用します。**ipv6-vpn-filter none** コマンドの発行によって作成されるヌル値を含め、ACL を削除するには、このコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。値の継承を防止するには、**ipv6-vpn-filter none** コマンドを使用します。

このユーザまたはグループ ポリシーに対する、さまざまなタイプのトラフィックを許可または拒否するには、ACL を設定します。次に、**ipv6-vpn-filter** コマンドを使用して、その ACL を適用します。

ipv6-vpn-filter {**value** *IPV6-ACL-NAME* | **none**}

no ipv6-vpn-filter

構文の説明

none	アクセス リストがないことを示します。ヌル値を設定して、アクセス リストを使用できないようにします。アクセス リストを他のグループ ポリシーから継承しないようにします。
value *IPV6-ACL-NAME*	事前に設定済みのアクセス リストの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

クライアントレス SSL VPN は、**ipv6-vpn-filter** コマンドに定義されている ACL を使用しません。

例

次に、FirstGroup というグループ ポリシーの ipv6_acl_vpn というアクセス リストを呼び出すフィルタを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipv6-vpn-filter value ipv6_acl_vpn
```

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。

isakmp am-disable

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

isakmp am-disable

no isakmp am-disable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルト値はイネーブルです。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	このコマンドは廃止されました。**crypto isakmp am-disable** コマンドは、それに置き換わるものです。

例

次に、グローバル コンフィギュレーション モードでの入力で、アグレッシブ モードの着信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	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

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

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルト値はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	このコマンドは廃止されました。**crypto isakmp disconnect-notify** コマンドは、それに置き換わるものです。

例

次の例では、グローバル コンフィギュレーション モードで、ピアに対する切断通知をイネーブルにします。

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

関連コマンド

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

isakmp enable

IPSec ピアがセキュリティ アプライアンスと通信しているインターフェイスで 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。インターフェイスで 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*

構文の説明

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

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
7.2(1)	このコマンドは廃止されました。**crypto isakmp enable** コマンドは、それに置き換わるものです。

例

次の例では、グローバル コンフィギュレーション モードで、内部インターフェイス上で ISAKMP をディセーブルにする方法を示しています。

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

関連コマンド

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

isakmp identity

ピアに送信されるフェーズ 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}**

構文の説明

address	ISAKMP の識別情報を交換するホストの IP アドレスを使用します。
auto	接続タイプによって ISKMP ネゴシエーションを決定します。事前共有キーの場合は IP アドレス、証明書認証の場合は証明書 DN となります。
hostname	ISAKMP の識別情報を交換するホストの完全修飾ドメイン名を使用します（デフォルト）。この名前は、ホスト名とドメイン名で構成されます。
key-id *key_id_string*	リモート ピアが事前共有キーを検索するために使用するストリングを指定します。

デフォルト

デフォルトの ISAKMP の識別情報は、**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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
7.2(1)	このコマンドは廃止されました。**crypto isakmp identity** コマンドは、それに置き換わるものです。

例

次の例では、グローバル コンフィギュレーション モードで、接続タイプに応じて、IPSec ピアと通信するためのインターフェイス上で ISAKMP ネゴシエーションをイネーブルにします。

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

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。

コマンド	説明
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp ikev1-user-authentication

IKE 時にハイブリッド認証を設定するには、トンネル グループ ipsec 属性コンフィギュレーション モードで **isakmp ikev1-user-authentication** コマンドを使用します。ハイブリッド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。

isakmp ikev1-user-authentication [*interface*] {**none** | **xauth** | **hybrid**}

no isakmp ikev1-user-authentication [*interface*] {**none** | **xauth** | **hybrid**}

構文の説明

hybrid	IKE 時にハイブリッド XAUTH 認証を指定します。
interface	（任意）ユーザ認証方式が設定されているインターフェイスを指定します。
none	IKE 時にユーザ認証をディセーブルにします。
xauth	拡張ユーザ認証とも呼ばれる XAUTH を指定します。

デフォルト

デフォルトの認証方式は XAUTH、つまり拡張ユーザ認証です。デフォルトの *interface* は、すべてのインターフェイスです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、セキュリティ アプライアンス認証にデジタル証明書を使用し、リモート VPN ユーザ認証に RADIUS、TACACS+、SecurID などの別の従来の方式を使用する必要がある場合に使用します。このコマンドは、IKE のフェーズ 1 をハイブリッド認証と呼ばれる次の 2 つの手順に分けます。

1. セキュリティ アプライアンスは、標準の公開キー技術を使用して、リモート VPN ユーザに対して認証します。これにより、単方向に認証する IKE セキュリティ アソシエーションが確立されます。
2. 次に、XAUTH 交換がリモート VPN ユーザを認証します。この拡張認証では、サポートされている従来のいずれかの認証方式を使用できます。

（注）　認証タイプをハイブリッドに設定するには、事前に認証サーバを設定し、事前共有キーを作成し、トラストポイントを設定する必要があります。

任意の **interface** パラメータを省略すると、コマンドはすべてのインターフェイスに適用され、インターフェイスごとのコマンドが指定されていないときにはバックアップとなります。トンネル グループに指定されている **isakmp ikev1-user-authentication** コマンドが 2 つある場合、1 つは **interface** パラメータを使用し、もう 1 つは使用しません。インターフェイスを指定している方が、その特定のインターフェイスでは優先されます。

例

次に、example-group というトンネル グループの内部インターフェイスでハイブリッド XAUTH をイネーブルにする例を示します。

```
hostname(config)# tunnel-group example-group type ipsec-ra
hostname(config)# tunnel-group example-group ipsec-attributes
hostname(config-tunnel-ipsec)# isakmp ikev1-user-authentication (inside) hybrid
hostname(config-tunnel-ipsec)#
```

関連コマンド

コマンド	説明
aaa-server	AAA サーバを定義します。
pre-shared-key	IKE 接続をサポートするための事前共有キーを作成します。
tunnel-group	IPSec、L2TP/IPSec、および WebVPN 接続の接続固有レコードのデータベースを作成および管理します。

isakmp ipsec-over-tcp

IPSec over TCP をイネーブルにするには、グローバル コンフィギュレーション モードで **isakmp ipsec-over-tcp** コマンドを使用します。IPSec over TCP をディセーブルにするには、このコマンドの **no** 形式を使用します。

isakmp ipsec-over-tcp [**port** *port1...port10*]

no isakmp ipsec-over-tcp [**port** *port1...port10*]

構文の説明

port *port1...port10*	（任意）デバイスが IPSec over TCP 接続を受け入れるポートを指定します。最大 10 のポートを指定できます。ポート番号には 1 ～ 65535 の範囲の数値を指定できます。デフォルトのポート番号は 10000 です。

デフォルト

デフォルト値はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	このコマンドは廃止されました。**crypto isakmp ipsec-over-tcp** コマンドは、それに置き換わるものです。

例

次の例では、グローバル コンフィギュレーション モードで、IPSec over TCP をポート 45 でイネーブルにします。

```
hostname(config)# isakmp ipsec-over-tcp port 45
```

関連コマンド

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

isakmp keepalive

IKE DPD を設定するには、トンネル グループ ipsec 属性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。あらゆるトンネル グループで、IKE キープアライブがデフォルトでイネーブルであり、しきい値と再試行値がデフォルト値になっています。キープアライブ パラメータをデフォルトのしきい値と再試行値でイネーブルの状態に戻すには、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

構文の説明

disable	IKE キープアライブ処理をディセーブルにします。デフォルトではイネーブルになっています。
retry *seconds*	キープアライブ応答を受信しなかったことを受けて再試行する間隔を秒単位で指定します。指定できる範囲は 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せずにピアがアイドル状態でいられ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 グループでは 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 グループのデフォルトは、しきい値が 300 秒、再試行値が 2 秒です。

LAN-to-LAN グループのデフォルトは、しきい値が 10 秒、再試行値が 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	透過	シングル	コンテキスト	システム
トンネル グループ ipsec 属性コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

この属性は、IPSec リモート アクセス タイプおよび IPSec LAN-to-LAN トンネル グループ タイプにのみ適用できます。

例

次に、設定 ipsec コンフィギュレーション モードを開始し、IP アドレスが 209.165.200.225 の IPSec LAN-to-LAN トンネル グループに対して、IKE DPD を設定し、しきい値を 15 にし、再試行間隔を 10 に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-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
hostname(config-tunnel-ipsec)#
```

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。
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 ipsec-attributes	このグループのトンネル グループ ipsec 属性を設定します。

isakmp nat-traversal

NAT トラバーサルをグローバルにイネーブルにするには、ISAKMP がグローバル コンフィギュレーション モードでイネーブルになっていることを確認し（**isakmp enable** コマンドでイネーブルにできます）、次に **isakmp nat-traversal** コマンドを使用します。NAT トラバーサルをイネーブルにした場合、このコマンドの **no** 形式でディセーブルにできます。

isakmp nat-traversal *natkeepalive*

no isakmp nat-traversal *natkeepalive*

構文の説明

natkeepalive	NAT キープアライブ間隔を、10 ～ 3600 秒の範囲で設定します。デフォルトは 20 秒です。

デフォルト

デフォルトでは、NAT トラバーサル（**isakmp nat-traversal**）はディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
7.2(1)	このコマンドは廃止されました。**crypto isakmp nat-traversal** コマンドは、それに置き換わるものです。

使用上のガイドライン

ポート アドレス変換（PAT）を含めネットワーク アドレス変換（NAT）は、IPSec が使用されているものの、IPSec パケットの NAT デバイス通過を阻害する非互換性がいくつもあるネットワークの多くで使用されています。NAT トラバーサルを使用すると、ESP パケットが 1 つ以上の NAT デバイスを通過できるようになります。

セキュリティ アプライアンスは IETF のドラフト「UDP Encapsulation of IPsec Packets」のバージョン 2 およびバージョン 3（http://www.ietf.org/html.charters/ipsec-charter.html から入手可能）に従って NAT トラバーサルをサポートし、NAT トラバーサルはダイナミック クリプト マップとスタティック クリプト マップの両方に対応しています。

このコマンドは、セキュリティ アプライアンス上で NAT-T をグローバルにイネーブルにします。クリプト マップ エントリでディセーブルにするには、**crypto map set nat-t-disable** コマンドを使用します。

例

次の例では、グローバル コンフィギュレーション モードで、ISAKMP をイネーブルにし、30 秒間隔で NAT Traversal をイネーブルにします。

```
hostname(config)# isakmp enable
hostname(config)# isakmp nat-traversal 30
```

関連コマンド

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

isakmp policy authentication

IKE ポリシー内に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 ポリシーは、IKE ネゴシエーション用のパラメータのセットを定義したものです。ISAKMP 認証方式を削除するには、関連する **clear configure** コマンドを使用します。

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

構文の説明

crack	認証方式として IKE Challenge/Response for Authenticated Cryptographic Keys（CRACK）を指定します。
pre-share	認証方式として事前共有キーを指定します。
priority	IKE ポリシーを一意に識別し、その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 はプライオリティが最も高く、65,534 が最も低くなります。
rsa-sig	認証方式として RSA シグニチャを指定します。 RSA シグニチャにより、IKE ネゴシエーションに対して否認防止を実行できます。これは基本的に、ユーザがピアとの 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

デフォルトの ISAKMP ポリシー認証は **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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。7.0 で DSA-Sig 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、Certification Authority（CA; 認証局）から証明書を取得するように、セキュリティ アプライアンスとそのピアを設定する必要があります。事前共有キーを指定する場合は、セキュリティ アプライアンスとそのピアに、事前共有キーを別々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、**isakmp policy authentication** コマンドを使用する例を示します。この例では、使用する RSA シグニチャの認証方式を IKE ポリシー内にプライオリティ番号 40 で設定します。

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

関連コマンド

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

isakmp policy encryption

使用する暗号化アルゴリズムを IKE ポリシー内に指定するには、グローバル コンフィギュレーション モードで **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* **encryption** {**aes | aes-192| aes-256 | des | 3des**}

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

構文の説明

3des	IKE ポリシーで、Triple DES 暗号化アルゴリズムを使用することを指定します。
aes	IKE ポリシーで使用する暗号化アルゴリズムが、128 ビット キーを使用する AES であることを指定します。
aes-192	IKE ポリシーで使用する暗号化アルゴリズムが、192 ビット キーを使用する AES であることを指定します。
aes-256	IKE ポリシーで使用する暗号化アルゴリズムが、256 ビット キーを使用する AES であることを指定します。
des	IKE ポリシーで使用する暗号化アルゴリズムが、56 ビット DES-CBC であることを指定します。
priority	Internet Key Exchange（IKE; インターネット キー交換）ポリシーを一意に指定し、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 はプライオリティが最も高く、65,534 が最も低くなります。

デフォルト

デフォルトの ISAKMP ポリシー暗号化は、**3des** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
7.2(1)	このコマンドは廃止されました。**crypto isakmp policy encryption** コマンドは、それに置き換わるものです。

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、**isakmp policy encryption** コマンドを使用する例を示します。使用するアルゴリズムとして 128 ビット キー AES 暗号化を IKE ポリシー内にプライオリティ番号 25 で設定します。

```
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 モードでの入力で、プライオリティ番号 40 の IKE ポリシー内で 3DES アルゴリズムを使用するように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	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

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 ポリシーは、IKE ネゴシエーション時に使用するパラメータのセットを定義したものです。Diffie-Hellman グループ識別子をデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

isakmp policy *priority* **group** {**1 | 2 | 5**}

no isakmp policy *priority* **group**

構文の説明

group 1	IKE ポリシーで、768 ビットの Diffie-Hellman グループを使用することを指定します。768 ビットは、デフォルト値です。
group 2	IKE ポリシーで、1024 ビットの Diffie-Hellman グループ 2 を使用することを指定します。
group 5	IKE ポリシーで、1536 ビットの Diffie-Hellman グループ 5 を使用することを指定します。
priority	Internet Key Exchange（IKE; インターネット キー交換）ポリシーを一意に指定し、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 はプライオリティが最も高く、65,534 が最も低くなります。

デフォルト

デフォルトはグループ 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	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。グループ 7 が追加されました。
7.2(1)	このコマンドは廃止されました。**crypto isakmp policy group** コマンドは、それに置き換わるものです。
8.0(4)	**group 7** コマンド オプションは**廃止されました**。グループ 7 を設定しようとするとエラー メッセージが生成され、代わりにグループ 5 が使用されます。

使用上のガイドライン

グループ オプションには、768 ビット（DH グループ 1）、1024 ビット（DH グループ 2）、および 1536 ビット（DH グループ 5）の 3 つがあります。1024 ビットと 1536 ビットの Diffie-Hellman グループは、セキュリティが高くなりますが、CPU の処理時間は長くなります。

（注） Cisco VPN Client バージョン 3.x 以降で DH **グループ 2** を設定するには、**isakmp policy** が必要です（DH **グループ 1** を設定した場合、Cisco VPN Client は接続できません）。

AES は、VPN-3DES のライセンスがあるセキュリティ アプライアンスに限りサポートされます。AES では大きなキー サイズが提供されるため、ISAKMP ネゴシエーションでは Diffie-Hellman（DH）**グループ 1** や**グループ 2** ではなく、**グループ 5** を使用する必要があります。このためには、**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、**isakmp policy group** コマンドを使用する例を示します。この例では、プライオリティ番号 40 の IKE ポリシーに対し、グループ 2、1024 ビットの Diffie Hellman を使用するように設定しています。

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

関連コマンド

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

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 ポリシーは、IKE ネゴシエーション時に使用するパラメータのセットを定義したものです。

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**

構文の説明

md5	IKE ポリシーでハッシュ アルゴリズムとして MD5（HMAC バリアント）を使用することを指定します。
priority	Internet Key Exchange（IKE; インターネット キー交換）ポリシーを一意に指定し、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 はプライオリティが最も高く、65,534 が最も低くなります。
sha	IKE ポリシーでハッシュ アルゴリズムとして SHA-1（HMAC バリアント）を使用することを指定します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
7.2(1)	このコマンドは廃止されました。**crypto isakmp policy hash** コマンドは、それに置き換わるものです。

使用上のガイドライン

ハッシュ アルゴリズムのオプションには、SHA-1 と MD5 の 2 つがあります。MD5 のダイジェストの方が小さく、SHA-1 よりもやや速いと見なされています。

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、**isakmp policy hash** コマンドを使用する例を示します。この例では、MD5 ハッシュ アルゴリズムを IKE ポリシー内でプライオリティ番号 40 で使用することを指定します。

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

関連コマンド

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

isakmp policy lifetime

期限切れになるまでの IKE セキュリティ アソシエーション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。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値の 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**

構文の説明

priority	Internet Key Exchange（IKE; インターネット キー交換）ポリシーを一意に指定し、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 はプライオリティが最も高く、65,534 が最も低くなります。
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。有限のライフタイムを提示するには、120 ～ 2147483647 秒の整数を使用します。無限のライフタイムを提示するには、0 秒を使用します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。
7.2(1)	このコマンドは廃止されました。**crypto isakmp policy lifetime** コマンドは、それに置き換わるものです。

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、自身のセッション用のセキュリティ パラメータについて合意しようとします。次に、各ピアのセキュリティ アソシエーションが、合意されたパラメータを参照します。ピアは、ライフタイムが期限切れになるまで、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、期限切れになるまで、その後の IKE ネゴシエーションで利用できるため、新しい IPSec セキュリティ アソシエーションを設定するときに時間を節約できます。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 アソシエーションをネゴシエートします。

ライフタイムを長くするほど、セキュリティ アプライアンスで以降の IPSec セキュリティ アソシエーションを設定する時間が節約されます。暗号化強度は十分なレベルにあるため、キーの再生成間隔を極端に短く（約 2 ～ 3 分ごとに）しなくてもセキュリティは保証されます。デフォルト値の採用を推奨しますが、ピアがライフタイムを提示しない場合には、無限のライフタイムを指定できます。

（注） IKE セキュリティ アソシエーションのライフタイムが無限に設定されている場合、ピアが有限のライフタイムを提示したときは、ピアからネゴシエートされた有限の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 ポリシー内にプライオリティ番号 40 で 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）に設定します。

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、IKE ポリシー内にプライオリティ番号 40 で IKE セキュリティ アソシエーションのライフタイムを 50,4000 秒（14 時間）を設定する例を示します。

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

次に、グローバル コンフィギュレーション モードでの入力で、IKE セキュリティ アソシエーションのライフタイムを無限に設定する例を示します。

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

関連コマンド

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

isakmp reload-wait

すべてのアクティブなセッションが自主的に終了するまで待機してからセキュリティ アプライアンスをリブート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。アクティブなセッションが終了するのを待たずにセキュリティ アプライアンスをリブートするには、このコマンドの **no** 形式を使用します。

isakmp reload-wait

no isakmp reload-wait

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。
7.2(1)	このコマンドは廃止されました。**crypto isakmp reload-wait** コマンドは、それに置き換わるものです。

例

次の例では、グローバル コンフィギュレーション モードで、すべてのアクティブなセッションが終了するまで待機してからセキュリティ アプライアンスをリブートするように設定します。

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

関連コマンド

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

issuer

アサーションを SAML-type SSO サーバに送信するセキュリティ デバイスを指定するには、その特定の SAML タイプの webvpn-sso-saml コンフィギュレーション モードで **issuer** コマンドを使用します。発行者名を削除するには、このコマンドの **no** 形式を使用します。

issuer *identifier*

no issuer [*identifier*]

構文の説明

identifier	セキュリティ デバイス名を指定します。通常は、デバイスのホスト名です。識別情報は、英数字で 65 文字未満にする必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

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、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。セキュリティ アプライアンスは現在、SAML POST-type の SSO サーバと SiteMinder-type の SSO サーバをサポートしています。

このコマンドは、SAML-type の SSO サーバのみに適用されます。

例

次に、asa1.mycompany.com というセキュリティ デバイスの発行者名を指定する例を示します。

```
hostname(config-webvpn)# sso server myhostname type saml-v1.1-post
hostname(config-webvpn-sso-saml# issuer asa1.example.com
hostname(config-webvpn-sso-saml#
```

関連コマンド

コマンド	説明
assertion-consumer-url	セキュリティ デバイスが SAML-type SSO サーバ アサーション コンシューマ サービスに問い合わせる際に使用する URL を指定します。

コマンド	説明
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	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 サーバを作成します。
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。

issuer-name

すべての発行済み証明書の発行者名 DN を指定するには、ローカル Certificate Authority（CA; 認証局）サーバ 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。認証局の証明書からサブジェクト DN 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 *DN-string*

no issuer-name [*DN-string*]

構文の説明

DN-string	自己署名 CA 証明書のサブジェクト名 DN でもある証明書の認定者名を指定します。属性と値のペアを区切るには、カンマを使用します。カンマを含む値は、引用符で囲んでください。発行者名は、英数字で 500 文字未満にする必要があります。

デフォルト

デフォルトの発行者名は cn=*hostame.domain-name* で、たとえば cn=asa.example.com となります。

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

コマンド履歴

リリース	変更内容
7.3(1)	このコマンドが導入されました。
8.0(2)	*DN-string* 値でカンマを保持するため、引用符のサポートが追加されました。

使用上のガイドライン

このコマンドでは、このローカル CA サーバが作成する証明書に表示される発行者名を指定します。この任意のコマンドは、発行者名をデフォルトの CA 名とは異なるものにする場合に使用します。

（注） この発行者名コンフィギュレーションは、いったん CA サーバをイネーブルにし、**no shutdown** コマンドを発行して証明書を生成すると変更できなくなります。

例

次に、証明書認証を設定する例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# issuer-name cn=asa-ca.example.com,ou=Eng,o=Example,c="cisco systems, inc."
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
keysize	証明書登録で生成される公開キーと秘密キーのサイズを指定します。
lifetime	CA 証明書と発行済みの証明書のライフタイムを指定します。
show crypto ca server	ローカル CA の特性を表示します。
show crypto ca server cert-db	ローカル CA サーバ証明書を表示します。