CHAPTER 16

# interface-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。

intercept-dhcp アトリビュートを実行コンフィギュレーションから削除するには、**no intercept-dhcp** コマンドを使用します。このコマンドを使用すると、ユーザは、デフォルト グループ ポリシーまたは他のグループ 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ます。

DHCP 代行受信を使用すると、Microsoft XP クライアントは、セキュリティ アプライアンスに対してスプリット トンネリングを使用できます。セキュリティ アプライアンスは、Microsoft Windows XP クライアントの DHCP Inform メッセージに直接応答し、そのクライアントにトンネル IP アドレスのサブネット 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。XP 以前の Windows クライアントに対しては、DHCP 代行受信は、ドメイン名とサブネット マスクを提供します。この機能は、DHCP サーバを使用することに利点がない環境に有用です。

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

**no intercept-dhcp**

**シンタックスの説明**

| | |
|---|---|
| **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になっています。

**コマンド モード**

次の表は、このコマンドを入力できるモードを示しています。

| | 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 225 バイトを超えていると、Microsoft XP に異常が発生し、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 ルートに制限します。ルートの数は、ルートのクラスによって異なります。

**例**

次の例は、FirstGroup というグループ ポリシーに DHCP 代行受信を設定する方法を示しています。

```
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 モードに入るには、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とセキュリティ コンテキスト モードに応じて、ハードウェア設定値を設定し、名前、VLAN、および IP アドレスを割り当て、その他多数の設定値を設定することができます。

すべてのモデルで、物理インターフェイスに対応したパラメータを設定できます。ASA 5505 適応型セキュリティ アプライアンスといった組み込みスイッチがあるモデルを除いて、すべてのモデルは、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。組み込みスイッチがあるモデルには、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（このコマンドの物理インターフェイスと呼ばれる）が用意されています。この場合、VLAN のサブインターフェイスは作成しませんが、物理インターフェイスとは別に VLAN インターフェイスを作成します。VLAN インターフェイスには、1 つまたは複数の物理インターフェイスを割り当てることができます。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は削除できません。

物理インターフェイスの場合（すべてのモデル）：

**interface** {*physical_interface* | *mapped_name*}

サブインターフェイスの場合（組み込みスイッチがあるモデルには使用できません）：

**interface** {*physical_interface.subinterface* | *mapped_name*}

**no interface** *physical_interface.subinterface*

VLAN インターフェイスの場合（組み込みスイッチのあるモデル）：

**interface vlan** *number*

**no interface vlan** *number*

**シンタックスの説明**

| | |
|---|---|
| *mapped_name* | マルチ コンテキスト モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。 |
| *physical_interface* | 物理インターフェイスのタイプ、スロット、およびポート番号で、*type*[*slot*/]*port* として指定します。タイプとスロット / ポートの間にスペースを入れるかどうかは任意です。<br><br>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。<br><br>• **ethernet**<br>• **gigabitethernet**<br><br>PIX 500 シリーズ セキュリティ アプライアンスの場合は、タイプに続けてポート番号を入力します（たとえば、**ethernet0**）。<br><br>ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合は、タイプに続けてスロット / ポートを入力します（たとえば、**gigabitethernet0/1**）。シャーシに組み込まれたインターフェイスはスロット 0 に割り当てられ、4GE SSM 上のインターフェイス（または組み込まれた 4GE SSM）はスロット 1 に割り当てられます。<br><br>ASA 5510 以降の適応型セキュリティ アプライアンスには、次のタイプもあります。<br><br>• **management**<br><br>管理インターフェイスは、管理トラフィック専用に設計されたファースト イーサネット インターフェイスで、**management0/0** として指定されます。ただし、必要に応じて、通過トラフィックに使用することもできます（**management-only** コマンドを参照）。透過ファイアウォール モードでは、通過トラフィック用の 2 つのインターフェイスのほかに、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 モードのセキュリティ コンテキストごとに管理することができます。<br><br>インターフェイス タイプ、スロット、およびポート番号を特定するには、使用中のモデルに付属しているハードウェア ドキュメントを参照してください。 |
| **subinterface** | （オプション）論理サブインターフェイスを示す 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 アプライアンスの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 アプライアンスといった組み込みスイッチがあるモデルには使用できません。プラットフォームごと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 Security Appliance Command Line Configuration Guide*』を参照してください。1 つまたは複数の VLAN サブインターフェイスを持つ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* | 組み込みスイッチがあるモデルの場合、VLAN ID 番号を 1 ～ 1001 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に対して **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たインターフェイスすべてに対して、**interface** コマンドを自動的に生成します。

物理インターフェイスは、デフォルトではすべてシャットダウンされます。コンフィギュレーションでは、コンテキスト内の割り当て済みインターフェイスはシャットダウンされません。VLAN インターフェイスはデフォルトではシャットダウンされません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | 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、新しいサブインターフェイスの命名規則が適用できるように、また、インターフェイス コンフィギュレーション モードで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。 |

## 使用上のガイドライン

物理インターフェイスは、デフォルトではすべてシャットダウンされます。イネーブルになっているサブインターフェイスをトラフィックが通過できるようにするには、物理インターフェイスを事前にイネーブルにしておく必要があります。マルチ コンテキスト モードの場合、物理インターフェイスまたはサブインターフェイスをコンテキストに割り当てると、インターフェイスはデフォルトではそのコンテキスト内でイネーブルになります。ただし、トラフィックがコンテキスト 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をシステム コンフィギュレーションでもイネーブルにする必要があります。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、そのインターフェイスを共有しているすべてのコンテキストでダウンします。VLAN インターフェイスはデフォルトではイネーブルです。

イネーブルになっているインターフェイスをトラフィックが通過できるようにするには、インターフェイス コンフィギュレーション モードのコマンドである **nameif** および **ip address**（ルーテッド モード用）を設定します。サブインターフェイスの場合は、**vlan** コマンドを設定します。スイッチ物理インターフェイスの場合、**switchport access vlan** コマンド（アクセス ポート用）または **switchport trunk allowed vlan** コマンド（トランク ポート用）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。セキュリティ レベルは、デフォルトでは 0（最低レベル）になっています。インターフェイスのデフォルト レベルについて調べる場合や、インターフェイスの相互通信を可能にするためにデフォルトの 0 から変更する場合は、**security-level** コマンドを参照してください。

マルチ コンテキスト モードでは、物理パラメータ、サブインターフェイス、および VLAN 割り当ては、システム コンフィギュレーションのみに設定します。それ以外のパラメータはすべて、コンテキスト コンフィギュレーションのみに設定します。

組み込みスイッチのあるモデルの場合、物理パラメータとスイッチ パラメータ（VLAN 割り当てを含む）を物理インターフェイスのみに設定できます。その他すべてのパラメータを VLAN インターフェイスに設定できます。

透過ファイアウォール モードでは、ASA 5505 適応型セキュリティ アプライアンスの場合、Base ライセンスでアクティブな VLAN を 2 つまで、Security Plus ライセンスでアクティブな VLAN を 3 つまで設定できます。その内のいずれかは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、Base ライセンスの場合はアクティブな VLAN を 3 つまで、Security Plus ライセンスの場合は 20 まで設定できます。アクティブな VLAN とは、**nameif** コマンドが設定されている VLAN です。Base ライセンスの場合、3 つ目の VLAN のみが別の VLAN へのトラフィックを開始するように設定できます。**no forward interface** コマンドを使用して 3 つめの VLAN を制限します。

ASA 以降の適応型セキュリティ アプライアンスには、Management 0/0 と呼ばれる専用の管理インターフェイスが含まれており、このインターフェイスによってセキュリティ アプライアンスへのトラフィックをサポートします。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 の管理専用モードをディセーブルにして、他のインターフェイスと同様にトラフィックを通過させることもできます。

**（注）** 透過ファイアウォール モードでは、2 つのインターフェイスのみ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 アプライアンスでは、専用の管理インターフェイス（物理インターフェイスまたはサブインターフェイス）を管理トラフィック用の第 3 のインターフェイスとして使用できます。モードはこの場合設定不能であり、常に管理専用にする必要があります。

インターフェイス設定を変更する場合、既存の接続がタイムアウトするのを待たずに新しいセキュリティ情報を使用するときは、**clear local-host** コマンドを使用して接続を消去してもかまいません。

**例**

次の例では、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
```

次の例では、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
```

次の例では、マルチ コンテキスト モードで、システム コンフィギュレーションのインターフェイス パラメータを設定し、gigabitethernet 0/1.1 サブインターフェイスを contextA に割り当てます。

```
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
```

次の例では、マルチ コンテキスト モードで、コンテキスト コンフィギュレーションのパラメータを設定します。

```
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 LAN インターフェイスを設定しています。3 つ目のホーム 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

...
```

次の例では、5 つの VLAN インターフェイス（**failover lan** コマンドを使用して別々に設定されたフェールオーバー インターフェイスを含む）を設定しています。

```
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
```

## 関連コマンド

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

# interface（VPN ロードバランシング）

VPN ロードバランシング仮想クラスタで VPN ロードバランシングのデフォルト以外のパブリック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。インターフェイスの指定を削除して、デフォルト 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**}

## シンタックスの説明

| | |
|---|---|
| *interface-name* | VPN ロードバランシング クラスタのパブリックまたはプライベート インターフェイスとして設定す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ように指定します。 |
| ***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ように指定します。 |

## デフォルト

**interface** コマンドを省略した場合、デフォルトでは、***lbprivate*** インターフェイスは***内部***に、***lbpublic*** インターフェイスは***外部***に設定されます。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | 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 モードに入る必要があります。

また、事前に **interface**、**ip address**、および **nameif** 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 形式を使用すると、インターフェイスがデフォルトに戻ります。

## 例

次に、**vpn load-balancing** コマンド シーケンスの例を示します。このコマンド シーケンスには、クラスタのパブリック インターフェイスを「test」として指定する **interface** コマンドと、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（内部）に戻す interface コマンドが含まれています。

```
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 モードに入ります。 |

# interface-policy

監視中にインターフェイスの障害が検出された場合の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*[**%**]

## シンタックスの説明

| | |
|---|---|
| *num* | 1 ～ 100 の数を指定するか（パーセンテージとして使用する場合）、または 1 からインターフェイスの最大数までの数を指定します。 |
| *%* | （オプション）*num* の数が監視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

装置に対して **failover interface-policy** コマンドが設定されている場合は、その値が **interface-policy** フェールオーバー グループ コマンドのデフォルトと見なされます。設定されていなければ、*num* は 1 になっています。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | 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 **%** キーワードの間にスペースを含めないでください。

障害が発生したインターフェイスの数が設定済みポリシーの基準を満たした場合、他のセキュリティ アプライアンスが正常に機能しているときは、セキュリティ アプライアンスは自身を障害としてマークし、場合によってはフェールオーバーが発生します（アクティブなセキュリティ アプライアンスに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** コマンドで監視対象として指定したインターフェイスのみです。

## 例

次の例（抜粋）は、フェールオーバー グループに対して適用可能なコンフィギュレーションを示しています。

```
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監視対象にするインターフェイスを指定します。 |

# interval maximum

DDNS アップデート方式によるアップデート試行間の最大間隔を設定するには、DDNS アップデート方式モードで **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 アップデート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*

## シンタックスの説明

| | |
|---|---|
| *days* | アップデート試行間の日数を 0 ～ 364 の範囲に指定します。 |
| *hours* | アップデート試行間の時間数を 0 ～ 23 の範囲に指定します。 |
| *minutes* | アップデート試行間の分数を 0 ～ 59 の範囲に指定します。 |
| *seconds* | アップデート試行間の秒数を 0 ～ 59 の範囲に指定します。 |

## 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

次の表は、このコマンドを入力できるモードを示しています。

| | 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 アップデート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

日数、時間数、分数、秒数がまとめて加算されて合計間隔が示されます。

## 例

次の例では 3 分 15 秒ごとにアップデートされる ddns-2 という方式が設定されます。

```
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 アップデート方式モード） | 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） | ダイナミック DNS（DDNS）のアップデート方式を、セキュリティ アプライアンス 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。 |
| **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 レコードを動的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。 |

# ip address

インターフェイスの IP アドレス（ルーテッド モード）または管理アドレスの IP アドレス（透過モード）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。透過モードの場合は、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、また、フェールオーバー用のスタンバイ アドレスを設定します。

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

**no ip address** [*ip_address*]

## シンタックスの説明

| | |
|---|---|
| *ip_address* | インターフェイスの IP アドレス（ルーテッド モード）、または管理 IP アドレス（透過モード）。 |
| *mask* | （オプション）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 アプライアンスは IP アドレス クラスのデフォルト マスクを使用します。 |
| ***standby*** *ip_address* | （オプション）フェールオーバー用のスタンバイ装置の 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

次の表は、このコマンドを入力できるモードを示しています。

| | 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 モードに関して、このコマンドが、グローバル コンフィギュレーション コマンドからインターフェイス コンフィギュレーション モード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 アドレスは一意のサブネット上にある必要があります。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上にある場合、各 IP アドレスは一意で、同じサブネット上にある必要があります。インターフェイスが一意の場合、この IP アドレスは、必要に応じて他のコンテキストで使用することができます。

透過ファイアウォールは、IP ルーティングには参加しません。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な理由は、セキュリティ アプライアンスがセキュリティ アプライアンス上で発信するトラフィック（システム メッセージや AAA サーバとの通信など）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。また、このアドレスは、リモート管理アクセスに使用することもできます。このアドレスは、アップストリーム ルータおよびダウンストリーム ルータと同じサブネット上にある必要があります。マルチ コンテキスト モードの場合は、各コンテキスト内で管理 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上にある必要があります。

## 例

次の例では、2 つのインターフェイスの IP アドレスとスタンバイ アドレスを設定します。

```
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
```

次の例では、透過ファイアウォールの管理アドレスとスタンバイ アドレスを設定します。

```
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 モードに入ります。 |
| **ip address dhcp** | DHCP サーバから IP アドレスを取得するようにインターフェイスを設定します。 |
| **show ip address** | インターフェイスに割り当てられた IP アドレスを表示します。 |

# ip address 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**

## シンタックスの説明

| | |
|---|---|
| ***setroute*** | （オプション）DHCP サーバから提供されるデフォルト ルートをセキュリティ アプライアンスが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

次の表は、このコマンドを入力できるモードを示しています。

| | 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、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。また、このコマンドが、外部インターフェイスだけでなく、すべてのインターフェイス上でイネーブルにできるようになりました。 |

## 使用上のガイドライン

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

**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いで **ip address dhcp** コマンドを入力すると、一部の DHCP 要求が送信されない場合があります。

## 例

次の例では、gigabitethernet0/1 インターフェイス上で DHCP をイネーブルにします。

```
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 モードに入ります。 |
| **ip address** | インターフェイスの IP アドレスを設定します。または、透過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 サーバから取得した IP アドレスを表示します。 |

# 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*]] ***p*pppoe** [***setroute***]

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

## シンタックスの説明

| | |
|---|---|
| *ip_address* | PPPoE サーバからアドレスを受信せずに、IP アドレスを手作業で設定します。 |
| *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 アプライアンスは IP アドレス クラスのデフォルト マスクを使用します。 |
| ***setroute*** | セキュリティ アプライアンスでは、PPPoE サーバから提供されるデフォルト ルートが使用されます。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 アプライアンスはゲートウェイとしてアクセス コンセントレータのアドレスによりデフォルト 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

次の表は、このコマンドを入力できるモードを示しています。

| | 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 では広く普及している規格である Ethernet と PPP を組み合せて、クライアント システムに認証方式で IP アドレスを割り当てます。ISP が PPPoE を導入している理由は、PPPoE が既存のリモート アクセス インフラストラクチャを使用する高速ブロードバンド アクセスをサポートしており、顧客が簡単に使用できるためです。

PPPoE を使用して IP アドレスを設定する前に、**vpdn** コマンドを使用してユーザ名、パスワード、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、たとえば、ISP へのバックアップ リンクとして、このコマンドをイネーブルにする場合、必要に応じて **pppoe client vpdn group** コマンドを使用して、異なるグループに各インターフェイスを割り当てることができます。

Maximum Transmission Unit（MTU; 最大伝送ユニット）サイズは自動的に 1492 バイトに設定されます。この値は、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再起動するには、このコマンドを再度入力します。

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

## 例

次の例では、Gigabitethernet 0/1 インターフェイス上で PPPoE をイネーブルにします。

```
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
```

次の例では、PPPoE インターフェイスに対して IP アドレスを手動で設定します。

```
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 モードに入ります。 |
| **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 サーバから取得した IP アドレスを表示します。 |
| **vpdn group** | |

# 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**

## シンタックスの説明

このコマンドには、引数もキーワードもありません。

## デフォルト

このコマンドは、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

次の表は、このコマンドを入力できるモードを示しています。

| | 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

次の例では、SIP 検査ポリシー マップにおいて、SIP 上での IP アドレスのプライバシーをイネーブルにする方法を示します。

```
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 マップに含めるクラス 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検査クラス 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。 |

# ip audit attack

攻撃シグニチャに一致するパケットに対するデフォルト 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 アクションに戻す（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、一切指定しないこともできます。

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

**no ip audit attack**

## シンタックスの説明

| | |
|---|---|
| ***action*** | （オプション）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 アプライアンスは入力したものと見なして ***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** | （オプション）パケットをドロップします。 |
| **reset** | （オプション）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、アラームの送信です。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | 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のものです。 |

## 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** コマンドに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

次の例では、攻撃シグニチャに一致するパケットに対するデフォルト アクションを、alarm および reset に設定します。内部インターフェイスの監査ポリシーは、このデフォルトを無効にして alarm のみに設定します。一方、外部インターフェイスのポリシーは、**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** | インターフェイスに監査ポリシーを割り当てます。 |
| **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するデフォルト 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 アクションに戻す（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、一切指定しないこともできます。

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

**no ip audit info**

## シンタックスの説明

| | |
|---|---|
| ***action*** | （オプション）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 アプライアンスは入力したものと見なして ***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** | （オプション）パケットをドロップします。 |
| **reset** | （オプション）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、アラームの生成です。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | 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のものです。 |

## 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** コマンドに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

次の例では、情報シグニチャに一致するパケットに対するデフォルト アクションを、alarm および reset に設定します。内部インターフェイスの監査ポリシーは、このデフォルトを無効にして alarm および drop に設定します。一方、外部インターフェイスのポリシーは、**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** | インターフェイスに監査ポリシーを割り当てます。 |
| **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

インターフェイスに監査ポリシーを割り当てるには、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。ポリシーをインターフェイスから削除するには、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*

## シンタックスの説明

| | |
|---|---|
| *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*** ポリシーと ***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

次の表は、このコマンドを入力できるモードを示しています。

| | 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のものです。 |

## 例

次の例では、監査ポリシーを内部インターフェイスと外部インターフェイスに適用します。

```
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。 |
| **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する場合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（サービス拒絶攻撃）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**]]

## シンタックスの説明

| | |
|---|---|
| ***action*** | （オプション）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場合、セキュリティ アプライアンスは、**ip audit attack** コマンドと **ip audit info** コマンドで設定されたデフォルト アクションを使用します。 |
| ***alarm*** | （オプション）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、ネットワークに対する攻撃の一部である可能性があります。 |
| **drop** | （オプション）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、現在のところ、ネットワークを攻撃することはありませんが、ポート スィープなど、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** | （オプション）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** コマンドと **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ていなければ、攻撃シグニチャと情報シグニチャに対するデフォルト アクションは、アラームの生成になっています。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | 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のものです。 |

**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インターフェイスにポリシーを割り当てます。各インターフェイスに ***info*** ポリシーと ***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する場合、そのトラフィックに対してアクションを実行するときは、**shun** コマンドを使用して、攻撃ホストからの新しい接続を防止し、既存の接続からのパケットを拒否します。

**例**

次の例では、攻撃シグニチャと情報シグニチャに対してアラームを生成するように、内部インターフェイスの監査ポリシーを設定します。一方、外部インターフェイスのポリシーでは、攻撃の接続をリセットします。

```
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** | インターフェイスに監査ポリシーを割り当てます。 |
| **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と宛先アドレスが指定されたパケットをブロックします。 |

# ip audit signature

監査ポリシーの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。シグニチャを再度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。正当なトラフィックがシグニチャに継続的に一致する場合、シグニチャをディセーブルにするリスクがあっても多数のアラームを回避することを考えているときは、ディセーブルにしてもかまいません。

**ip audit signature** *signature_number* ***disable***

**no ip audit signature** *signature_number*

## シンタックスの説明

| | |
|---|---|
| *signature_number* | ディセーブルにするシグニチャの番号を指定します。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

次の表は、このコマンドを入力できるモードを示しています。

| | 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のものです。 |

## 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とシステム メッセージ番号を示します。

**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 オプション：不良オプション リスト | 情報 | 受信した IP データグラムの IP データグラム ヘッダーにある IP オプションのリストが不完全な場合や変造されている場合にトリガーされます。IP オプションのリストには、種々のネットワーク管理タスクやデバッグ 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 オプション：記録パケット ルート | 情報 | 受信した IP データグラムの IP オプション リストにオプション 7（記録パケット ルート）が含まれている場合にトリガーされます。 |
| 1002 | 400002 | IP オプション：タイムスタンプ | 情報 | 受信した IP データグラムの IP オプション リストにオプション 4（タイムスタンプ）が含まれている場合にトリガーされます。 |

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 |
|---|---|---|---|---|
| 1003 | 400003 | IP オプション：セキュリティ | 情報 | 受信した IP データグラムの IP オプション リストにオプション 2（セキュリティ オプション）が含まれている場合にトリガーされます。 |
| 1004 | 400004 | IP オプション：発信元ルートの損失 | 情報 | 受信した IP データグラムの IP オプション リストにオプション 3（発信元ルートの損失）が含まれている場合にトリガーされます。 |
| 1005 | 400005 | IP オプション：SATNET ID | 情報 | 受信した IP データグラムの IP オプション リストにオプション 8（SATNET ストリーム ID）が含まれている場合にトリガーされます。 |
| 1006 | 400006 | IP オプション：完全発信元ルート | 情報 | 受信した IP データグラムの IP オプション リストにオプション 2（完全発信ルーティング）が含まれている場合にトリガーされます。 |
| 1100 | 400007 | IP フラグメント攻撃 | 攻撃 | 受信した IP データグラムのオフセット フィールドに含まれているオフセット値が 0 より大きく 5 より小さい場合にトリガーされます。 |
| 1102 | 400008 | IP 不可能パケット | 攻撃 | 到着した IP パケットの送信元アドレスと宛先アドレスが一致している場合にトリガーされます。このシグニチャは、いわゆる Land 攻撃を捕捉します。 |
| 1103 | 400009 | IP フラグメント重複（Teardrop） | 攻撃 | 同じ IP データグラムに含まれている 2 つのフラグメントが、データグラム内で両フラグメントが位置決めを共有していることを示すオフセットを持っている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する場合があります。一部のオペレーティング システムは、このように重複するフラグメントを正しく処理しないため、重複フラグメントを受信したときに、例外を投げたり、不適切に動作したりする場合があります。このようにして、Teardrop 攻撃から DoS が引き起こされます。 |
| 2000 | 400010 | ICMP エコー応答 | 情報 | 受信した IP データグラムの 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）に設定されている場合にトリガーされます。 |
| 2001 | 400011 | ICMP ホスト到達不能 | 情報 | 受信した IP データグラムの 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）に設定されている場合にトリガーされます。 |
| 2002 | 400012 | ICMP Source Quench | 情報 | 受信した IP データグラムの 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（Source Quench）に設定されている場合にトリガーされます。 |

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 |
|---|---|---|---|---|
| 2003 | 400013 | ICMP リダイレクト | 情報 | 受信した IP データグラムの 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 5（リダイレクト）に設定されている場合にトリガーされます。 |
| 2004 | 400014 | ICMP エコー要求 | 情報 | 受信した IP データグラムの 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）に設定されている場合にトリガーされます。 |
| 2005 | 400015 | データグラムの ICMP タイム超過 | 情報 | 受信した IP データグラムの 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（データグラムのタイム超過）に設定されている場合にトリガーされます。 |
| 2006 | 400016 | データグラム上の ICMP パラメータ問題 | 情報 | 受信した IP データグラムの 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（データグラム上のパラメータ問題）に設定されている場合にトリガーされます。 |
| 2007 | 400017 | ICMP タイムスタンプ要求 | 情報 | 受信した IP データグラムの 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）に設定されている場合にトリガーされます。 |
| 2008 | 400018 | ICMP タイムスタンプ応答 | 情報 | 受信した IP データグラムの 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）に設定されている場合にトリガーされます。 |
| 2009 | 400019 | ICMP 情報要求 | 情報 | 受信した IP データグラムの 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）に設定されている場合にトリガーされます。 |
| 2010 | 400020 | ICMP 情報応答 | 情報 | 受信した IP データグラムの 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）に設定されている場合にトリガーされます。 |
| 2011 | 400021 | ICMP アドレス マスク要求 | 情報 | 受信した IP データグラムの 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）に設定されている場合にトリガーされます。 |
| 2012 | 400022 | ICMP アドレス マスク応答 | 情報 | 受信した IP データグラムの 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）に設定されている場合にトリガーされます。 |

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 |
|---|---|---|---|---|
| 2150 | 400023 | フラグメント化された ICMP トラフィック | 攻撃 | 受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定されているほか、それ以外にも 1（ICMP）に設定されたフラグメント フラグがあるか、またはオフセット フィールドにオフセットが含まれている場合にトリガーされます。 |
| 2151 | 400024 | 大きい ICMP トラフィック | 攻撃 | 受信した IP データグラムの 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 の長さが 1024 より大きい場合にトリガーされます。 |
| 2154 | 400025 | Ping of Death 攻撃 | 攻撃 | 受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、Last Fragment ビットが設定され、（IP オフセット * 8）+（IP データ長）> 65,535 の式が成り立つ場合にトリガーされます。この式は、IP オフセット（元のパケットにおけるこのフラグメントの開始位置で、8 バイト単位）と残りのパケットの合計が IP パケットの最大サイズを超えていることを意味します。 |
| 3040 | 400026 | TCP NULL フラグ | 攻撃 | SYN、FIN、ACK、または RST フラグがいずれも設定されていない単一の TCP パケットが、特定のホストに送信された場合にトリガーされます。 |
| 3041 | 400027 | TCP SYN+FIN フラグ | 攻撃 | SYN および FIN フラグが設定されている単一の TCP パケットが、特定のホストに送信された場合にトリガーされます。 |
| 3042 | 400028 | TCP FIN のみのフラグ | 攻撃 | 単一の身元不明 TCP FIN パケットが、特定のホスト上の特権ポート（ポート番号は 1024 より小さい）に送信された場合にトリガーされます。 |
| 3153 | 400029 | FTP に誤ったアドレスを指定 | 情報 | ポート コマンドが、要求元ホストとは異なるアドレスを使用して発行された場合にトリガーされます。 |
| 3154 | 400030 | FTP に誤ったポートを指定 | 情報 | ポート コマンドが、1024 未満または 65535 を超えるデータ ポートを指定して発行された場合にトリガーされます。 |
| 4050 | 400031 | UDP Bomb 攻撃 | 攻撃 | 指定された UDP の長さが、指定された IP の長さより小さい場合にトリガーされます。この変造パケット タイプは、DoS 攻撃に関連付けられています。 |
| 4051 | 400032 | UDP Snork 攻撃 | 攻撃 | 検出された UDP パケットの送信元ポートが 135、7、または 19 のいずれかで、宛先ポートが 135 の場合にトリガーされます。 |
| 4052 | 400033 | UDP Chargen DoS 攻撃 | 攻撃 | このシグニチャがトリガーされるのは、検出された UDP パケットの送信元ポートが 7 で、宛先ポートが 19 の場合です。 |
| 6050 | 400034 | DNS HINFO 要求 | 情報 | DNS サーバの HINFO レコードにアクセスする攻撃が発生した場合にトリガーされます。 |
| 6051 | 400035 | DNS ゾーン転送 | 情報 | 通常の DNS ゾーン転送（送信元ポートは 53）が発生した場合にトリガーされます。 |

**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 |
|---|---|---|---|---|
| 6052 | 400036 | ハイ ポートからの DNS ゾーン転送 | 情報 | 不正な DNS ゾーン転送（送信元ポートは 53 以外）が発生した場合にトリガーされます。 |
| 6053 | 400037 | すべての記録の DNS 要求 | 攻撃 | すべての記録の DNS 要求を受信した場合にトリガーされます。 |
| 6100 | 400038 | RPC ポート登録 | 情報 | ターゲット ホストに対して新しい RPC サービスを登録する攻撃が発生した場合にトリガーされます。 |
| 6101 | 400039 | RPC ポート非登録 | 情報 | ターゲット ホストに対して既存の RPC サービスを登録解除する攻撃が発生した場合にトリガーされます。 |
| 6102 | 400040 | RPC Dump | 情報 | ターゲット ホストに RPC ダンプ要求が発行された場合にトリガーされます。 |
| 6103 | 400041 | プロキシの RPC 要求 | 攻撃 | ターゲット ホストのポートマッパーにプロキシの RPC 要求が送信された場合にトリガーされます。 |
| 6150 | 400042 | ypserv（YP サーバ デーモン）Portmap 要求 | 情報 | YP サーバ デーモン（ypserv）ポートのポートマッパーに要求が送信された場合にトリガーされます。 |
| 6151 | 400043 | ypbind（YP バインド デーモン）Portmap 要求 | 情報 | YP バインド デーモン（ypbind）ポートのポートマッパーに要求が送信された場合にトリガーされます。 |
| 6152 | 400044 | yppasswdd（YP パスワード デーモン）Portmap 要求 | 情報 | YP パスワード デーモン（yppasswdd）ポートのポートマッパーに要求が送信された場合にトリガーされます。 |
| 6153 | 400045 | ypupdated（YP アップデート デーモン）Portmap 要求 | 攻撃 | YP アップデート デーモン（ypupdated）ポートのポートマッパーに要求が送信された場合にトリガーされます。 |
| 6154 | 400046 | ypxfrd（YP 転送デーモン）Portmap 要求 | 攻撃 | YP 転送デーモン（ypxfrd）ポートのポートマッパーに要求が送信された場合にトリガーされます。 |
| 6155 | 400047 | mountd（マウント デーモン）Portmap 要求 | 情報 | マウント デーモン（mountd）ポートのポートマッパーに要求が送信された場合にトリガーされます。 |
| 6175 | 400048 | rexd（リモート実行デーモン）Portmap 要求 | 情報 | リモート実行デーモン（rexd）ポートのポートマッパーに要求が送信された場合にトリガーされます。 |
| 6180 | 400049 | rexd（リモート実行デーモン）攻撃 | 情報 | rexd プログラムが呼び出された場合にトリガーされます。リモート実行デーモンは、リモート プログラムの実行を担当するサーバです。これは、システム リソースに不正アクセスする攻撃の兆候である可能性があります。 |
| 6190 | 400050 | statd バッファ オーバーフロー | 攻撃 | 大規模な statd 要求が送信された場合にトリガーされます。これは、バッファをオーバーフローさせ、システム リソースにアクセスする攻撃である可能性があります。 |

**例**

次の例では、シグニチャ 6100 をディセーブルにします。

```
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** | インターフェイスに監査ポリシーを割り当てます。 |
| **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。

**ip-comp** アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。この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ます。

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

**no ip-comp**

## シンタックスの説明

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

## デフォルト

IP 圧縮はディセーブルになっています。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | 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、モデムで接続しているリモート ダイヤルイン ユーザのデータ伝送速度が向上する場合があります。

**注意**　データ圧縮を行うと、各ユーザ セッションのメモリ要件と CPU 使用率が増加するため、セキュリティ アプライアンスのスループット全体が低下します。このため、データ圧縮は、モデムで接続しているリモート ユーザに対してのみイネーブルにすることをお勧めします。モデム ユーザに固有のグループ ポリシーを設計し、このユーザに対してのみ圧縮をイネーブルにします。

## 例

次の例は、「FirstGroup」というグループ ポリシーに対して IP 圧縮をイネーブルにする方法を示しています。

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

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

**no ip local pool** *poolname*

## シンタックスの説明

| | |
|---|---|
| *first-address* | IP アドレスの範囲の開始アドレスを指定します。 |
| *last-address* | IP アドレスの範囲の最終アドレスを指定します。 |
| ***mask*** *mask* | （オプション）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

次の表は、このコマンドを入力できるモードを示しています。

| | 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

VPN クライアントに割り当てられた IP アドレスが非標準のネットワークに属する場合は、マスク値を指定する必要があります。デフォルト マスクを使用すると、データが誤ってルーティングされる可能性があります。一般的な例として、デフォルトでクラス A ネットワークになっている IP ローカル プールに 10.10.10.0/255.255.255.0 のアドレスが含まれている場合を考えます。この場合、VPN クライアントが複数のインターフェイス上で 10 ネットワーク内の複数のサブネットにアクセスしようとすると、ルーティングの問題が発生する可能性があります。たとえば、アドレス 10.10.100.1/255.255.255.0 のプリンタがインターフェイス 2 経由で使用可能で、10.10.10.0 ネットワークが VPN トンネル上およびインターフェイス 1 経由で使用可能な場合、VPN クライアントでは、プリンタ宛のデータのルーティング先について混乱が生じます。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 ネットワークに該当するため、プリンタのデータは VPN トンネル上で送信される場合があります。

## 例

次の例では、firstpool という IP アドレス プールを設定します。開始アドレスは 10.20.30.40 で、終了アドレスは 10.20.30.50 です。ネットワーク マスクは 255.255.255.0 です。

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

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure ip local pool** | すべての IP ローカル プールを削除します。 |
| **show running-config ip local pool** | ip プール 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。IP phone Bypass アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、IP Phone Bypass の値を別のグループ ポリシーから継承できます。

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 電話を接続するときに、ユーザ認証プロセスが不要になります。イネーブルの場合、Secure Unit Authentication は有効なままになります。

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

**no ip-phone-bypass**

## シンタックスの説明

| | |
|---|---|
| **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

次の表は、このコマンドを入力できるモードを示しています。

| | 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 を設定する必要があるのは、ユーザ認証をイネーブルにした場合のみです。

## 例

次の例は、FirstGroup というグループ ポリシーに対して IP Phone Bypass をイネーブルにする方法を示しています。

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

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **user-authentication** | ハードウェア クライアントの背後にいるユーザに対して、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 をサポートしています。AIP SSM は拡張 IPS ソフトウェアを実行して、インライン モードまたはプロミスキャス モードで詳細なセキュリティ検査を実行します。セキュリティ アプライアンスが AIP SSM にパケットを転送するのは、パケットが出力インターフェイスを通過する直前（または VPN 暗号化が設定されている場合は暗号化が行われる前）と、他のファイアウォール ポリシーが適用された後です。たとえば、アクセス リストによってブロックされたパケットは、AIP SSM に転送されません。

セキュリティ アプライアンスからのトラフィックを AIP SSM に割り当てるには、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***}

**no ips** {***inline*** | ***promiscuous***} {***fail-close*** | ***fail-open***}

## シンタックスの説明

| | |
|---|---|
| **fail-close** | AIP SSM に障害が発生した場合にトラフィックをブロックします。 |
| **fail-open** | AIP SSM に障害が発生した場合にトラフィックを許可します。 |
| ***inline*** | AIP SSM にパケットを転送します。パケットは、IPS 動作の結果としてドロップされる場合があります。 |
| ***promiscuous*** | AIP SSM に対するパケットを複製します。元のパケットを AIP SSM でドロップすることはできません。 |

## 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

次の表は、このコマンドを入力できるモードを示しています。

| | 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。 |

## 使用上のガイドライン

**ips** コマンドを設定するには、最初に、**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 にトラフィックを転送するようにセキュリティ アプライアンスを設定したら、AIP SSM の検査と保護ポリシーを設定します。このポリシーは、トラフィックの検査方法と、進入が検知されたときの処理を決定します。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するか（**session** コマンド）、または管理インターフェイス上で SSH や Telnet を使用して AIP SSM に直接接続することができます。別の方法として、ASDM を使用することもできます。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。

## 例

次の例では、プロミスキャス モードですべての IP トラフィックを AIP SSM に転送し、何らかの理由で AIP SSM カードに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
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **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 マップで使用するトラフィックを指定します。 |
| **clear configure policy-map** | すべての**ポリシー マップ** コンフィギュレーションを削除します。ただし、ポリシー マップが **service-policy** コマンド内で使用されている場合、そのポリシー マップは削除されません。 |
| **policy-map** | ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。 |
| **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。IPSec over UDP アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、IPSec over UDP の値を別のグループ ポリシーから継承できます。

IPSec over UDP（IPSec through NAT と呼ばれる場合もある）を使用すると、Cisco VPN Client またはハードウェア クライアントから、NAT を実行しているセキュリティ アプライアンスに UDP を介して接続できます。

**ipsec-udp {enable | disable}**

**no ipsec-udp**

## シンタックスの説明

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

## デフォルト

IPSec over UDP はディセーブルになっています。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | 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** コマンドを設定する必要もあります。

また、Cisco VPN Client でも、IPSec over UDP を使用するように設定する必要があります（デフォルトでは、使用するように設定されています）。VPN 3002 では、IPSec over UDP を使用するように設定する必要はありません。

IPSec over UDP は独自の方式で、リモートアクセス接続のみに適用され、モード コンフィギュレーションを必要とします。これは、SA のネゴシエート中にセキュリティ アプライアンスがクライアントとコンフィギュレーション パラメータを交換することを意味します。

IPSec over UDP を使用すると、システム パフォーマンスがわずかに低下する場合があります。

## 例

次の例は、FirstGroup というグループ ポリシーに IPSec over UDP を設定する方法を示しています。

```
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 トラフィックをリッスン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。このオプションを使用すると、IPSec over UDP ポートの値を別のグループ ポリシーから継承できます。

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、設定済みのポート上でリッスンし、そのポートに対する UDP トラフィックを転送します。これは、他のフィルタ規則によって UDP トラフィックがドロップされる場合でも同様です。

**ipsec-udp-port** *port*

**no ipsec-udp-port**

**シンタックスの説明**

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

**デフォルト**

デフォルト ポートは 10000 です。

**コマンド モード**

次の表は、このコマンドを入力できるモードを示しています。

| | 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した複数のグループ ポリシーを設定できます。グループ ポリシーごとに、別々のポート番号を使用できます。

**例**

次の例は、FirstGroup というグループ ポリシーの IPSec UDP ポートをポート 4025 に設定する方法を示しています。

```
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 クライアントから、NAT を実行しているセキュリティ アプライアンスに UDP を介して接続できるようにします。 |

# ip verify reverse-path

Unicast 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、IP スプーフィング（パケットが不正な送信元 IP アドレスを使用して実際の送信元を隠す）から保護します。この機能により、すべてのパケットの送信元 IP アドレスが、ルーティング テーブルに従って、正しい送信元インターフェイスに一致することが保証されます。

**ip verify reverse-path interface** *interface_name*

**no ip verify reverse-path interface** *interface_name*

## シンタックスの説明

| | |
|---|---|
| *interface_name* | Unicast 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、デフォルトではディセーブルになっています。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | 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のものです。 |

## 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決定するときは宛先アドレスだけを参照します。Unicast RPF は、送信元アドレスも参照するようにセキュリティ アプライアンスに指示します。この機能が Reverse Path Forwarding（RPF）と呼ばれるのはこのためです。セキュリティ アプライアンスを通過できるように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 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、外部トラフィックについては、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 保護を機能させることができます。外部インターフェイスからトラフィックが着信した場合、送信元アドレスがルーティング テーブルにおいて未知のときは、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送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 テーブルにおいて既知のアドレスから外部インターフェイスにトラフィックが着信した場合、そ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ときは、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着信した場合、一致したルート（デフォルト ルート）は外部インターフェイスを示すため、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

次の例では、外部インターフェイス上で Unicast RPF をイネーブルにします。

```
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消去します。 |
| **clear ip verify statistics** | Unicast RPF の統計情報を消去します。 |
| **show ip verify statistics** | Unicast RPF の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 リストは、セキュリティ アプライアンスが通過させる、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**]]

## シンタックスの説明

| | |
|---|---|
| ***any*** | IPv6 プレフィックス ::/0 の短縮形で、任意の IPv6 アドレスを示します。 |
| **default** | （オプション）ACE 用に syslog メッセージ 106100 が生成されるように指定します。 |
| ***deny*** | 条件に合致している場合、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** | （オプション）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していることを指定します。 |
| ***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規則が適用されるように指定します。 |

| | |
|---|---|
| *icmp_type* | アクセス規則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にできます。<br>• destination-unreachable<br>• packet-too-big<br>• time-exceeded<br>• parameter-problem<br>• echo-request<br>• echo-reply<br>• membership-query<br>• membership-report<br>• membership-reduction<br>• router-renumbering<br>• router-solicitation<br>• router-advertisement<br>• neighbor-solicitation<br>• neighbor-advertisement<br>• neighbor-redirect<br>*icmp_type* 引数を省略すると、すべての ICMP タイプを示します。 |
| *icmp_type_obj_grp_id* | （オプション）オブジェクト グループの ICMP タイプ ID を指定します。 |
| *id* | アクセス リストの名前または番号。 |
| **interval** *secs* | （オプション）syslog メッセージ 106100 を生成する時間間隔を指定します。有効値の範囲は 1 ～ 600 秒です。デフォルトの間隔は 300 秒です。この値は、非アクティブの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* | （オプション）メッセージ 106100 の syslog レベルを指定します。有効値の範囲は 0 ～ 7 です。デフォルト レベルは 6（情報）です。 |
| ***line*** *line-num* | （オプション）アクセス規則を挿入するリスト内の行番号。行番号を指定しない場合、ACE はアクセス リストの末尾に追加されます。 |
| **log** | （オプション）ACE のロギング アクションを指定します。**log** キーワードを指定しない場合や、**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した場合や、レベルまたは間隔と一緒に指定した場合、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るパケットについては、ログに記録されません。ロギングをイネーブルにするには、ACE でパケットを明示的に拒否する必要があります。 |
| *network_obj_grp_id* | 既存のネットワーク オブジェクト グループの ID。 |
| ***object-group*** | （オプション）オブジェクト グループを指定します。 |
| *operator* | （オプション）送信元 IP アドレスを宛先 IP アドレスと比較するための演算子を指定します。*operator* は、送信元 IP アドレスまたは宛先 IP アドレスのポートを比較します。使用できる演算子は、**lt**（小なり）、**gt**（大なり）**eq**（同値）、**neq**（非同値）、および **range**（範囲）です。すべてのポートを含めるには（デフォルト）、演算子およびポートを使用せずに **ipv6 access-list** コマンドを使用します。 |

| | |
|---|---|
| ***permit*** | 条件に合致している場合、アクセスを許可します。 |
| *port* | （オプション）アクセスを許可または拒否するポートを指定します。*port* 引数を入力する場合は、0 ～ 65535 の数を使用するか、*protocol* が ***tcp*** または ***udp*** であればリテラル名を使用して、ポートを指定します。<br><br>使用可能な 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。<br><br>使用可能な 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。有効値は、**icmp**、**ip**、**tcp**、**udp** のいずれか、または IP プロトコル番号を表す 1 ～ 254 までの整数です。 |
| *protocol_obj_grp_id* | 既存のプロトコル オブジェクト グループの ID。 |
| *service_obj_grp_id* | （オプション）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 トラフィックの発信元の 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ときの 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

次の表は、このコマンドを入力できるモードを示しています。

| | 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 アドレスがポートまたはプロトコルにアクセスすることを許可または拒否するかどうかを指定できます。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。アクセス リストをインターフェイスに適用するには、**access-group** コマンドを使用します。

アクセス リストを使用してアクセスを特別に許可しない限り、セキュリティ アプライアンスは、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すべてのパケットは、特にアクセスを拒否しない限り、デフォルトで許可されます。

**ipv6 access-list** コマンドは、IPv6 専用であるという点を除き、**access-list** コマンドと類似しています。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着信を許可する ICMPv6 トラフィックを設定するには、**ipv6 icmp** コマンドを使用します。

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

## 例

次の例では、TCP を使用するすべてのホストが 3001:1::203:A0FF:FED6:162D のサーバにアクセスできるようにします。

```
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 へのアクセスのみを拒否します。

```
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、ポート 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。その結果、既知ポート（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に着信する ICMP メッセージに対して、アクセス規則を設定します。 |
| **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 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***}

## シンタックスの説明

| | |
|---|---|
| ***autoconfig*** | インターフェイス上でステートレス自動設定を使用して、IPv6 アドレスの自動設定をイネーブルにします。 |
| ***eui-64*** | （オプション）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

次の表は、このコマンドを入力できるモードを示しています。

| | 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

インターフェイス上で IPv6 アドレスを設定すると、IPv6 がそのインターフェイス上でイネーブルになります。IPv6 アドレスの指定後に **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、インターフェイス上で 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 メッセージで受信され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、このインターフェイス用に自動的に生成されます。そのリンク ローカル 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。

**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。オプションの **eui-64** が指定されている場合は、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* 引数に指定した値が 64 ビットより大きい場合は、プレフィックス ビットがインターフェイス ID に優先します。指定され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 レイヤ アドレスの上位 3 バイト（OUI フィールド）と下位 3 バイト（シリアル番号）の間に 16 進数の FFFE を挿入することで、48 ビット リンク レイヤ（MAC）アドレスから生成されます。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 番目のビット（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。このコマンドで指定する *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、Modified EUI-64 形式のインターフェイス ID で構成されます。MAC アドレス 00E0.B601.3B7A のインターフェイスには、リンク ローカル アドレス FE80::2E0:B6FF:FE01:3B7A が指定されます。指定され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

次の例では、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 を割り当てます。

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

次の例では、選択したインターフェイスに IPv6 アドレスを自動的に割り当てます。

```
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
```

次の例では、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 インターフェイスに関するデバッグ情報を表示します。 |
| **show ipv6 interface** | IPv6 用に設定し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 アドレスが設定されていないインターフェイス上で IPv6 処理をディセーブルにするには、このコマンドの **no** 形式を使用します。

**ipv6 enable**

**no ipv6 enable**

## シンタックスの説明

このコマンドには、引数もキーワードもありません。

## デフォルト

IPv6 はディセーブルです。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | 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、インターフェイス上で 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、インターフェイスの IPv6 処理をイネーブルにします。

**no ipv6 enable** コマンドは、明示的な IPv6 アドレスが指定されているインターフェイス上では IPv6 処理をディセーブルにしません。

## 例

次の例では、選択したインターフェイス上で IPv6 処理をイネーブルにします。

```
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 処理をイネーブルにします。 |
| **show ipv6 interface** | IPv6 用に設定したインターフェイスのユーザビリティ ステータスを表示します。 |

# ipv6 enforce-eui64

ローカル リンク上で IPv6 アドレスに Modified EUI-64 形式インターフェイス ID 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*

## シンタックスの説明

| | |
|---|---|
| *if_name* | **nameif** コマンドで指定したとおりに、インターフェイスの名前を指定して、Modified EUI-64 アドレス形式の適用をイネーブルにします。 |

## デフォルト

Modified EUI-64 形式の適用はディセーブルです。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | 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

このコマンドがあるインターフェイス上でイネーブルの場合、その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 アドレスと照合され、インターフェイス ID に Modified EUI-64 形式が使用されていることが確認されます。IPv6 パケットがインターフェイス ID に Modified EUI-64 形式を使用していない場合、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、フローが生成された場合に限り行われます。既存のフローからのパケットはチェックされません。その他に、アドレスの確認はローカル リンク上のホストに限り行われます。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確認に失敗し、ドロップされます。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。

Modified EUI-64 形式のインターフェイス ID は、リンク レイヤ アドレスの上位 3 バイト（OUI フィールド）と下位 3 バイト（シリアル番号）の間に 16 進数の FFFE を挿入することで、48 ビット リンク レイヤ（MAC）アドレスから生成されます。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 番目のビット（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

次の例では、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 アクセス規則を設定するには、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 アクセス規則を削除するには、このコマンドの **no** 形式を使用します。

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

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

## シンタックスの説明

| | |
|---|---|
| ***any*** | 任意の IPv6 アドレスを指定するキーワード。IPv6 プレフィックス ::/0 の短縮形。 |
| ***deny*** | 選択したインターフェイス上で、指定した ICMP トラフィックを拒否します。 |
| ***host*** | アドレスが特定のホストを指していることを指定します。 |
| *icmp-type* | アクセス規則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にできます。<br>• destination-unreachable<br>• packet-too-big<br>• time-exceeded<br>• parameter-problem<br>• echo-request<br>• echo-reply<br>• membership-query<br>• membership-report<br>• membership-reduction<br>• router-renumbering<br>• router-solicitation<br>• router-advertisement<br>• neighbor-solicitation<br>• neighbor-advertisement<br>• neighbor-redirect |
| *if-name* | アクセス規則の適用先となるインターフェイスの名前（**nameif** コマンドで指定したもの）。 |
| *ipv6-address* | ICMPv6 メッセージをインターフェイスに送信するホストの 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する IPv6 ネットワーク。 |
| ***permit*** | 選択したインターフェイス上で、指定した 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、何個がプレフィックス（ネットワーク部分）を構成しているかを指定します。プレフィックスの長さ値の前に、スラッシュ（/）を入力する必要があります。 |

## デフォルト

ICMP アクセス規則が定義されていない場合、ICMP トラフィックはすべて許可されます。

**コマンド モード**

次の表は、このコマンドを入力できるモードを示しています。

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

**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 機能の ICMP は、IPv4 の ICMP と同じです。ICMPv6 は、ICMP エコー要求メッセージおよび応答メッセージに類似した ICMP 宛先到達不能メッセージおよび情報メッセージなどのエラーメッセージを生成します。また、IPv6 の ICMP パケットは、IPv6 近隣探索プロセスとパス MTU 探索で使用されます。

インターフェイスに ICMP 規則が定義されていない場合、IPv6 ICMP トラフィックはすべて許可されます。

インターフェイスに ICMP 規則が定義されている場合は、最初に一致した規則が処理され、それ以降の規則はすべて暗黙的に拒否されます。たとえば、最初に一致した規則が許可規則の場合、その ICMP パケットは処理されます。最初に一致した規則が拒否規則の場合や、ICMP パケットがそのインターフェイス上のどの規則にも一致しなかった場合、セキュリティ アプライアンスはその ICMP パケットを廃棄し、syslog メッセージを生成します。

このため、ICMP 規則に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規則を入力してから、そのネットワーク上にある特定のホストからの ICMP トラフィックを許可する規則を入力した場合、そのホスト規則が処理されることはありません。ICMP トラフィックは、ネットワーク規則によってブロックされます。ただし、ホスト規則を入力してから、ネットワーク規則を入力した場合、ホストの ICMP トラフィックは許可されますが、それ以外の当該ネットワークからの ICMP トラフィックはすべてブロックされます。

**ipv6 icmp** コマンドは、セキュリティ アプライアンス インターフェイスに着信する ICMP トラフィックのアクセス規則を設定します。パススルー ICMP トラフィックのアクセス規則を設定するには、**ipv6 access-list** コマンドを参照してください。

**例**

次の例では、外部インターフェイスで、すべての ping 要求を拒否し、すべての Packet Too Big メッセージを許可します（パス MTU 探索をサポートするため）。

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

次の例では、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、外部インターフェイスへの ping を許可します。

```
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 nd dad attempts

重複アドレスの検出中にインターフェイス上で送信される連続的な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。送信される重複アドレス検出メッセージの数をデフォルトに戻すには、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*]

## シンタックスの説明

| | |
|---|---|
| *value* | 0 ～ 600 の数。0 を入力すると、指定されたインターフェイス上で重複アドレス検出がディセーブルになります。1 を入力すると、1 回だけ送信するように設定されます。デフォルト値は 1 つのメッセージです。 |

## デフォルト

デフォルトの試行回数は 1 です。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | 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。

管理上のダウン状態にあるインターフェイスでは、重複アドレス検出は一時停止されます。インターフェイスが管理上のダウン状態にある場合、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のアップ状態に戻ると、インターフェイス上で重複アドレス検出が自動的に再開されます。管理上の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 アドレスに対して重複アドレス検出が再開されます。

**（注）** インターフェイスのリンク ローカル アドレスに対して重複アドレス検出が実行されている間、他の IPv6 アドレスは引き続き一時的な状態に設定されます。リンク ローカル アドレスに対する重複アドレス検出が完了すると、残りの IPv6 アドレスに対して重複アドレス検出が実行されます。

重複アドレス検出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 アドレスの場合、そのアドレスは使用されなくなり、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 3000::4 on outside
```

重複アドレスに関連付けられている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になりますが、アドレスの状態は DUPLICATE に設定されます。

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は、新しいリンク ローカル アドレスに対して重複アドレス検出が実行され、そのインターフェイスに関連付けられている他の IPv6 アドレスがすべて再生成されます（重複アドレス検出は新しいリンク ローカル アドレスに対してのみ実行されます）。

## 例

次の例では、インターフェイスの一時的なユニキャスト IPv6 アドレスに対して重複アドレス検出が実行されている間に 5 つの連続したネイバー送信要求メッセージが送信されるように設定します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd dad attempts 5
```

次の例では、選択したインターフェイス上で重複アドレス検出をディセーブルにします。

```
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** | インターフェイス上でネイバー送信要求メッセージの送信間隔を設定します。 |
| **show ipv6 interface** | IPv6 用に設定したインターフェイスのユーザビリティ ステータスを表示します。 |

# ipv6 nd ns-interval

インターフェイス上で IPv6 ネイバー送信要求メッセージの再送信間隔を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd ns-interval** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

**ipv6 nd ns-interval** *value*

**no ipv6 nd ns-interval** [*value*]

## シンタックスの説明

| | |
|---|---|
| *value* | IPv6 ネイバー送信要求メッセージの送信間隔（ミリ秒単位）。有効となる値の範囲は 1,000 ～ 3,600,000 ミリ秒です。デフォルト値は 1,000 ミリ秒です。 |

## デフォルト

ネイバー送信要求メッセージの送信間隔は 1,000 ミリ秒になっています。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | 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

次の例では、Gigabitethernet 0/0 に対して IPv6 ネイバー送信要求メッセージの送信間隔を 9,000 ミリ秒に設定します。

```
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 用に設定したインターフェイスのユーザビリティ ステータスを表示します。 |

# ipv6 nd prefix

IPv6 ルータ アドバタイズメントに含める IPv6 プレフィックスを設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd prefix** コマンドを使用します。プレフィ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***]

## シンタックスの説明

| | |
|---|---|
| ***at*** *valid-date preferred-date* | ライフタイムと優先順位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到達するまで有効になります。有効期限の形式は、*date-valid-expire month-valid-expire hh:mm-valid-expire date-prefer-expire month-prefer-expire hh:mm-prefer-expire* です。 |
| ***default*** | デフォルト値が使用されます。 |
| ***infinite*** | （オプション）この有効ライフタイムは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める IPv6 ネットワーク番号。<br><br>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*** | （オプション）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 自動設定に使用されないことを示します。 |
| ***no-autoconfig*** | （オプション）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 自動設定に使用不能であることを示します。 |
| ***off-link*** | （オプション）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されたものとしてアドバタイズされる期間（秒単位）。有効となる値の範囲は、0 ～ 4294967295 秒です。最大値は、無限を意味します。infinite で指定することもできます。デフォルトは 604,800（7 日）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、何個がプレフィックス（ネットワーク部分）を構成しているかを指定します。プレフィックスの長さ値の前に、スラッシュ（/）を入力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なものとしてアドバタイズされる期間。有効となる値の範囲は、0 ～ 4294967295 秒です。最大値は、無限を意味します。**infinite** として指定することもできます。デフォルトは 2,592,000（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上で設定されたすべてのプレフィックスがアドバタイズされる場合、有効ライフタイム 2,592,000 秒（30 日）と優先ライフタイム 604,800 秒（7 日）が使用され、「onlink」フラグと「autoconfig」フラグの両方が設定されます。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | 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、個別のパラメータをプレフィックスごとに制御できます。

デフォルトでは、**ipv6 address** コマンドを使用してインターフェイス上のアドレスとして設定されたプレフィックスは、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のプレフィックスを設定すると、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。

日付を設定してプレフィックスの有効期限を指定することができます。有効ライフタイムと優先ライフタイムは、リアルタイムでカウントダウンされます。有効期限に到達すると、プレフィックスはアドバタイズされなくなります。

onlink が「オン」（デフォルト）の場合、指定されたプレフィックスは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アドレスにトラフィックを送信するノードでは、宛先をリンク上でローカルに到達可能なものと見なします。

autoconfig が「オン」（デフォルト）の場合、ローカル リンク上のホストには、指定されたプレフィックスが IPv6 自動設定に使用可能であることが示されます。

## 例

次の例では、指定され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、有効ライフタイム 1,000 秒、および優先ライフタイム 900 秒を含めます。

```
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、インターフェイス上で IPv6 処理をイネーブルにします。 |
| **show ipv6 interface** | IPv6 用に設定したインターフェイスのユーザビリティ ステータスを表示します。 |

# 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*]

## シンタックスの説明

| | |
|---|---|
| ***msec*** | （オプション）指定された値がミリ秒単位であることを示します。このキーワードがない場合、指定された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 ～ 1,800 秒ですが、***msec*** キーワードが指定されている場合は 500 ～ 1,800,000 ミリ秒となります。デフォルトは 200 秒です。 |

## デフォルト

200 秒。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | 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 アプライアンスをデフォルト ルータとして設定した場合、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 ノードと同期させないようにするには、使用する実際の値を、指定された値の 20% 以内でランダムに調整します。

## 例

次の例では、選択したインターフェイスに対して IPv6 ルータ アドバタイズメントの送信間隔を 201 秒に設定します。

```
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 用に設定したインターフェイスのユーザビリティ ステータスを表示します。 |

# 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の「ルータ ライフタイム」を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd ra-lifetime** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

**ipv6 nd ra-lifetime** *seconds*

**no ipv6 nd ra-lifetime** [*seconds*]

## シンタックスの説明

| | |
|---|---|
| *seconds* | このインターフェイスにおけるデフォルト ルータとしてのセキュリティ アプライアンスの有効期間。有効となる値の範囲は、0 ～ 9000 秒です。デフォルトは 1800 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

次の表は、このコマンドを入力できるモードを示しています。

| | 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。この値は、このインターフェイスにおけるデフォルト ルータとしてのセキュリティ アプライアンスの有効期間を示します。

値を 0 以外の値に設定することは、セキュリティ アプライアンスをこのインターフェイス上のデフォルト ルータと見なす必要があることを示します。「ルータ ライフタイム」値を 0 以外の値に設定する場合は、ルータ アドバタイズメントの送信間隔より小さくしないでください。

値を 0 に設定することは、セキュリティ アプライアンスをこの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。

## 例

次の例では、選択したインターフェイスに対して IPv6 ルータ アドバタイズメントのライフタイムを 1,801 秒に設定します。

```
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** | インターフェイス上で IPv6 ルータ アドバタイズメントの送信間隔を設定します。 |
| **show ipv6 interface** | IPv6 用に設定したインターフェイスのユーザビリティ ステータスを表示します。 |

# ipv6 nd reachable-time

到達可能性の確認イベントが発生した後でリモート IPv6 ノードを到達可能と見なす期間を設定するには、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。デフォルト期間に戻すには、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*]

## シンタックスの説明

| | |
|---|---|
| *value* | リモート IPv6 ノードを到達可能と見なす期間（ミリ秒単位）。有効となる値の範囲は 0 ～ 3,600,000 ミリ秒です。デフォルト値は 0 です。<br><br>*value* に 0 を設定した場合、到達可能な時間は不確定として送信されます。受信側のデバイスが、到達可能時間値を設定して追跡します。 |

## デフォルト

0 ミリ秒。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | 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

期間を設定すると、使用不可能なネイバーを検出できます。設定期間を短くすると、使用不可能なネイバーをより迅速に検出できます。ただし、期間を短くするほど、IPv6 ネットワークの帯域幅の消費量と、IPv6 ネットワーク デバイスすべての処理リソースの消費量が増加します。通常の IPv6 動作において、設定期間を大幅に短くすることはお勧めできません。

このコマンドを 0 に設定した場合にセキュリティ アプライアンスで使用される実際の値を含んだ到達可能時間を確認するには、**show ipv6 interface** コマンドを使用して、適用される ND 到達可能時間などの IPv6 インターフェイスの情報を表示します。

## 例

次の例では、選択したインターフェイスに対して IPv6 到達可能期間を 1,700,000 ミリ秒に設定します。

```
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 用に設定したインターフェイスのユーザビリティ ステータスを表示します。 |

# ipv6 nd suppress-ra

LAN インターフェイス上で IPv6 ルータ アドバタイズメントを送信しないようにするには、インターフェイス コンフィギュレーション モードで **ipv6 nd suppress-ra** コマンドを使用します。LAN 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を再度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**

## シンタックスの説明

このコマンドには、引数もキーワードもありません。

## デフォルト

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

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | 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 以外のタイプのインターフェイス（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）上で 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

次の例では、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を送信しないようにします。

```
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 用に設定したインターフェイスのユーザビリティ ステータスを表示します。 |

# ipv6 neighbor

IPv6 近隣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。近隣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*]

## シンタックスの説明

| | |
|---|---|
| *if_name* | **nameif** コマンドによって指定される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* | ローカルのデータリンク アドレスに対応する IPv6 アドレス。 |
| *mac_address* | ローカルのデータライン（ハードウェア MAC）アドレス。 |

## デフォルト

IPv6 近隣探索キャッシュにスタティック エントリは設定されていません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | 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** コマンドと類似しています。指定された IPv6 アドレスのエントリが近隣探索キャッシュにすでに存在する（IPv6 近隣探索プロセスからラーニングされた）場合、そのエントリはスタティック エントリに自動的に変換されます。**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、このエントリがコンフィギュレーションに格納されます。

IPv6 近隣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、IPv6 近隣探索キャッシュのすべてのエントリを、スタティック エントリを除いて削除します。**no ipv6 neighbor** コマンドは、指定したスタティック エントリを近隣探索キャッシュから削除します。このコマンドによってダイナミック エントリ（IPv6 近隣探索プロセスからラーニングされたエントリ）がキャッシュから削除されることはありません。**no ipv6 enable** コマンドを使用してインターフェイス上で IPv6 をディセーブルにすると、そのインターフェイスに設定された IPv6 近隣探索キャッシュのすべてのエントリが、スタティック エントリを除いて削除されます（エントリの状態は INCMP [Incomplete] に変更されます）。

近隣探索プロセスによって IPv6 近隣探索キャッシュのスタティック エントリが変更されることはありません。

## 例

次の例では、IPv6 アドレス 3001:1::45A および MAC アドレス 0002.7D1A.9472 の内部ホストのスタティック エントリを近隣探索キャッシュに追加します。

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

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear ipv6 neighbors** | IPv6 近隣探索キャッシュのすべてのエントリを、スタティック エントリを除いて削除します。 |
| **show ipv6 neighbor** | IPv6 近隣キャッシュ情報を表示します。 |

# ipv6 route

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

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

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

## シンタックスの説明

| | |
|---|---|
| *administrative-distance* | （オプション）ルートの管理ディスタンス。デフォルト値は 1 です。この場合、スタティック ルートは、接続済みルートを除く他のあらゆるタイプのルートに優先します。 |
| *if_name* | ルートの設定対象となるインターフェイスの名前。 |
| *ipv6-address* | 特定のネットワークに到達するために使用できるネクストホップの IPv6 アドレス。 |
| *ipv6-prefix* | スタティック ルートの宛先となる IPv6 ネットワーク。<br><br>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、何個がプレフィックス（ネットワーク部分）を構成しているかを指定します。プレフィックスの長さ値の前に、スラッシュ（/）を入力する必要があります。 |

## デフォルト

デフォルトでは、*administrative-distance* は 1 になっています。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | 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。

## 例

次の例では、ネットワーク 7fff::0/32 に対するパケットを、管理ディスタンス 110 で、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 のルーティング テーブル アップデートおよびルート キャッシュ アップデートに関するデバッグ情報を表示します。 |
| **show ipv6 route** | IPv6 ルーティング テーブルの現在の内容を表示します。 |

# isakmp am-disable

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**

**シンタックスの説明**　このコマンドには、引数もキーワードもありません。

**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**　次の表は、このコマンドを入力できるモードを示しています。

| | 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** コマンドに置き換えられました。 |

**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、アグレッシブ モードの着信接続をディセーブルにします。

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

# isakmp disconnect-notify

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

**isakmp disconnect-notify**

**no isakmp disconnect-notify**

## シンタックスの説明

このコマンドには、引数もキーワードもありません。

## 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

次の表は、このコマンドを入力できるモードを示しています。

| | 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)(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** コマンドに置き換えられました。 |

## 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消去します。 |
| **clear configure isakmp policy** | ISAKMP ポリシー コンフィギュレーションをすべて消去します。 |
| **clear isakmp sa** | IKE ランタイム SA データベースを消去します。 |
| **show running-config isakmp** | アクティブな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するインターフェイス上で ISAKMP ネゴシエーションをイネーブルにするには、グローバル コンフィギュレーション モードで **isakmp enable** コマンドを使用します。インターフェイス上で ISAKMP ディセーブルにするには、このコマンドの **no** 形式を使用します。

**isakmp enable** *interface-name*

**no isakmp enable** *interface-name*

## シンタックスの説明

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

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | 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のものです。 |
| 7.2(1) | このコマンドは廃止されました。**crypto isakmp enable** コマンドに置き換えられました。 |

## 例

次の例は、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消去します。 |
| **clear configure isakmp policy** | ISAKMP ポリシー コンフィギュレーションをすべて消去します。 |
| **clear isakmp sa** | IKE ランタイム SA データベースを消去します。 |
| **show running-config isakmp** | アクティブなコンフィギュレーションをすべて表示します。 |

# isakmp identity

フェーズ 2 ID をピアに送信するように設定するには、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}**

## シンタックスの説明

| | |
|---|---|
| **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** | ISKMP ネゴシエーションを、接続タイプよって判別します（事前共有キーの IP アドレス、または証明書認証用の証明書 DN）。 |
| **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文字列を指定します。 |

## デフォルト

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

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | 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のものです。 |
| 7.2(1) | このコマンドは廃止されました。**crypto isakmp identity** コマンドに置き換えられました。 |

## 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 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、接続タイプに応じて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消去します。 |
| **clear configure isakmp policy** | ISAKMP ポリシー コンフィギュレーションをすべて消去します。 |
| **clear isakmp sa** | IKE ランタイム SA データベースを消去します。 |
| **show running-config isakmp** | アクティブな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 中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 アトリビュート 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**}

## シンタックスの説明

| | |
|---|---|
| **hybrid** | IKE の使用時にハイブリッド XAUTH 認証を指定します。 |
| *interface* | （オプション）ユーザ認証方式を設定するインターフェイスを指定します。 |
| **none** | IKE の使用時にユーザ認証をディセーブルにします。 |
| **xauth** | XAUTH（拡張ユーザ認証とも呼ばれる）を指定します。 |

## デフォルト

デフォルトの認証方式は XAUTH（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

次の表は、このコマンドを入力できるモードを示しています。

| | 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 アトリビュート コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2(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

セキュリティ アプライアンス認証や RADIUS、TACACS+、または SecurID といったリモート VPN ユーザ認証用の従来の手法にデジタル証明書を使用する場合は、このコマンドを使用します。このコマンドは、IKE のフェーズ 1 を次の 2 ステップに分けます。2 つのステップを合せてハイブリッド認証と呼びます。

1. セキュリティ アプライアンスは、リモート VPN ユーザに対して標準の公開キー技術を使用して認証を行います。この認証により単方向で認証される IKE セキュリティ アソシエーションを確立します。
2. そして、XAUTH 交換で、リモート VPN ユーザが認証されます。この拡張認証では、サポートされている従来の認証方式のいずれかが使用されます。

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

オプションの **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にコマンドが指定されていない際にはバックアップとして機能します。トンネル グループに 2 つの **isakmp ikev1-user-authentication** コマンドを指定した場合、1 つは **interface** パラメータを使用し、2 つ目はそれを使用しません。インターフェイスを指定するコマンドはその特定のインターフェイスを優先します。

## 例

次のコマンド例は、example-group と呼ばれるトンネル 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事前共有キーを作成します。 |
| **tunnel-group** | IPSec、L2TP/IPSec、および WebVPN 接続に固有のレコードを含む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*]

## シンタックスの説明

| | |
|---|---|
| **port** *port1...port10* | （オプション）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。ポート番号の範囲は 1 ～ 65535 です。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

次の表は、このコマンドを入力できるモードを示しています。

| | 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)(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** コマンドに置き換えられました。 |

## 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、ポート 45 上で IPSec over TCP を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消去します。 |
| **clear configure isakmp policy** | ISAKMP ポリシー コンフィギュレーションをすべて消去します。 |
| **clear isakmp sa** | IKE ランタイム SA データベースを消去します。 |
| **show running-config isakmp** | アクティブな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 アトリビュート 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。デフォルトでは、すべてのトンネル グループで IKE キープアライブが、デフォルトのしきい値およびリトライ値を使用してイネーブルになっています。キープアライブ パラメータを、デフォルトのしきい値およびリトライ値を使用してイネーブルにした状態に戻すには、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**

## シンタックスの説明

| | |
|---|---|
| ***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が受信されなくなった後のリトライ間の間隔を秒単位で指定します。範囲は 2 ～ 10 秒です。デフォルトは 2 秒です。 |
| ***threshold*** *seconds* | キープアライブのモニタリングを開始するまでピアがアイドル状態を維持できる秒数を指定します。範囲は 10 ～ 3,600 秒です。LAN-to-LAN グループのデフォルトは 10 秒で、リモートアクセス グループのデフォルトは 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 秒で、リトライが 2 秒です。

LAN-to-LAN グループのデフォルトは、しきい値が 10 秒で、リトライが 2 秒です。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | 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 アトリビュート コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが導入されました。 |

## 使用上のガイドライン

このアトリビュートは、IPSec リモートアクセスおよび IPSec LAN-to-LAN トンネル グループ タイプだけに適用できます。

## 例

次の例では、config-ipsec コンフィギュレーション モードで、209.165.200.225 という IP アドレスを持つ 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 に設定し、リトライ間隔を 10 に指定します。

```
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 グループを消去します。 |
| **show running-config tunnel-group** | すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ 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 アトリビュートを設定します。 |

# isakmp nat-traversal

NAT Traversal をグローバルに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 をイネーブルにしたことを確認し（イネーブルにするには **isakmp enable** コマンドを使用します）、次に **isakmp nat-traversal** コマンドを使用します。NAT Traversal がイネーブルのときに、これ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 nat-traversal** *natkeepalive*

**no isakmp nat-traversal** *natkeepalive*

**シンタックスの説明**

| | |
|---|---|
| *natkeepalive* | NAT キープアライブ間隔を 10 ～ 3,600 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、NAT Traversal（**isakmp nat-traversal**）はディセーブルになっています。

**コマンド モード**

次の表は、このコマンドを入力できるモードを示しています。

| | 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のものです。 |
| 7.2(1) | このコマンドは廃止されました。**crypto isakmp nat-traversal** コマンドに置き換えられました。 |

**使用上のガイドライン**

Network Address Translation（NAT; ネットワーク アドレス変換）は、Port Address Translation（PAT; ポート アドレス変換）も含め、IPSec も使用している多くのネットワークで使用されていますが、IPSec パケットが NAT デバイスを問題なく通過することを妨げる非互換性が数多くあります。NAT Traversal を使用すると、ESP パケットが 1 つまたは複数の 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「UDP Encapsulation of IPsec Packets」ドラフトのバージョン 2 とバージョン 3（http://www.ietf.org/html.charters/ipsec-charter.html から入手可能）に記述されているとおり NAT Traversal をサポートしています。NAT Traversal は、ダイナミックとスタティックの両方の暗号マップについてサポートされています。

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。暗号マップ 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消去します。 |
| **clear configure isakmp policy** | ISAKMP ポリシー コンフィギュレーションをすべて消去します。 |
| **clear isakmp sa** | IKE ランタイム SA データベースを消去します。 |
| **show running-config isakmp** | アクティブなコンフィギュレーションをすべて表示します。 |

# isakmp policy authentication

IKE ポリシー内の認証方式を指定するには、グローバル コンフィギュレーション モードで **isakmp policy authentication** コマンドを使用します。IKE ポリシーは、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**}

## シンタックスの説明

| | |
|---|---|
| **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、そのポリシーに優先順位を割り当てます。1 ～ 65534 の整数を使用します。1 は優先順位が最も高く、65534 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。<br>RSA シグニチャは、IKE ネゴシエーションに対する否認防止ができます。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

次の表は、このコマンドを入力できるモードを示しています。

| | 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のものです。DSA-Sig が 7.0 で追加されました。 |

## 使用上のガイドライン

RSA シグニチャを指定する場合は、認証局（CA）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

次の例は、グローバル コンフィギュレーション モードで、**isakmp policy authentication** コマンドを使用する方法を示しています。この例では、優先順位番号 40 の IKE ポリシーに RSA シグニチャの認証方式を使用するように設定します。

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

**関連コマンド**

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

# isakmp policy encryption

IKE ポリシー内の暗号化アルゴリズムを指定するには、グローバル コンフィギュレーション モードで **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**}

**シンタックスの説明**

| | |
|---|---|
| **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）ポリシーを一意に識別し、そのポリシーに優先順位を割り当てます。1 ～ 65534 の整数を使用します。1 は優先順位が最も高く、65534 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**

次の表は、このコマンドを入力できるモードを示しています。

| | 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のものです。 |
| 7.2(1) | このコマンドは廃止されました。**crypto isakmp policy encryption** に置き換えられました。 |

## 例

次の例は、グローバル コンフィギュレーション モードで、**isakmp policy encryption** コマンドを使用する方法を示しています。この例では、優先順位番号 25 の IKE ポリシーに 128 ビット キーの AES 暗号化アルゴリズムを使用するように設定します。

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

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、優先順位番号 40 の IKE ポリシーに 3DES アルゴリズムを使用するように設定します。

```
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消去します。 |
| **clear configure isakmp policy** | ISAKMP ポリシー コンフィギュレーションをすべて消去します。 |
| **clear isakmp sa** | IKE ランタイム SA データベースを消去します。 |
| **show running-config isakmp** | アクティブな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** | **7**}

**no isakmp policy** *priority* **group**

## シンタックスの説明

| | |
|---|---|
| **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 が使用されるように指定します。 |
| **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。 |
| **group 7** | IKE ポリシーで、Diffie-Hellman Group 7 を使用することを指定します。Group 7 は IPSec SA キーを生成します。楕円曲線フィールドのサイズは 163 ビットです。 |
| *priority* | Internet Key Exchange（IKE）ポリシーを一意に識別し、そのポリシーに優先順位を割り当てます。1 ～ 65534 の整数を使用します。1 は優先順位が最も高く、65534 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

次の表は、このコマンドを入力できるモードを示しています。

| | 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のものです。Group 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** コマンドに置き換えられました。 |

## 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 Group 1）、1,024 ビット（DH Group 2）、1,536 ビット（DH Group 5）、および DH Group 7 の 4 つがあります。1,024 ビットと 1,536 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 Version 3.x 以降では、**isakmp policy** で DH **group 2** を設定する必要があります（DH **group 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 が提供するキーはサイズが大きいため、ISAKMP ネゴシエーションには、**group 1** や **group 2** ではなく、Diffie-Hellman（DH）**group 5** を使用する必要があります。この設定には、**isakmp policy priority group 5** コマンドを使用します。

## 例

次の例は、グローバル コンフィギュレーション モードで、**isakmp policy group** コマンドを使用する方法を示しています。この例では、優先順位番号 40 の IKE ポリシーに、グループ 2、1024 ビット Diffie Hellman を使用するように設定します。

```
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消去します。 |
| **clear configure isakmp policy** | ISAKMP ポリシー コンフィギュレーションをすべて消去します。 |
| **clear isakmp sa** | IKE ランタイム SA データベースを消去します。 |
| **show running-config isakmp** | アクティブな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**

## シンタックスの説明

| | |
|---|---|
| **md5** | IKE ポリシーで使用するハッシュ アルゴリズムとして、MD5（HMAC バリアント）を指定します。 |
| *priority* | Internet Key Exchange（IKE）ポリシーを一意に識別し、そのポリシーに優先順位を割り当てます。1 ～ 65534 の整数を使用します。1 は優先順位が最も高く、65534 が最も低くなります。 |
| **sha** | IKE ポリシーで使用するハッシュ アルゴリズムとして、SHA-1（HMAC バリアント）を指定します。 |

## デフォルト

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

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | 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のものです。 |
| 7.2(1) | このコマンドは廃止されました。**crypto isakmp policy hash** コマンドに置き換えられました。 |

## 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 は、SHA-1 よりもダイジェストが小さく、わずかに速いとされています。

## 例

次の例は、グローバル コンフィギュレーション モードで、**isakmp policy hash** コマンドを使用する方法を示しています。この例では、優先順位番号 40 の IKE ポリシーに MD5 ハッシュ アルゴリズムを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消去します。 |
| **clear configure isakmp policy** | ISAKMP ポリシー コンフィギュレーションをすべて消去します。 |
| **clear isakmp sa** | IKE ランタイム SA データベースを消去します。 |
| **show running-config isakmp** | アクティブなコンフィギュレーションをすべて表示します。 |

# isakmp policy lifetime

IKE セキュリティ アソシエーションの期限が満了するまでのライフタイムを指定するには、グローバル コンフィギュレーション モードで **isakmp policy lifetime** コマンドを使用します。ピアがライフタイムを提示していなければ、無限のライフタイムを指定できます。セキュリティ アソシエーションのライフタイムをデフォルト値の 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**

**シンタックスの説明**

| | |
|---|---|
| *priority* | Internet Key Exchange（IKE）ポリシーを一意に識別し、そのポリシーに優先順位を割り当てます。1 ～ 65534 の整数を使用します。1 は優先順位が最も高く、65534 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満了す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 ～ 2,147,483,647 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**

次の表は、このコマンドを入力できるモードを示しています。

| | 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のものです。 |
| 7.2(1) | このコマンドは廃止されました。**crypto isakmp policy lifetime** コマンドに置き換えられました。 |

**使用上のガイドライン**

IKE は、ネゴシエーションを開始するとき、自身のセッション用のセキュリティ パラメータを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満了するまで、セキュリティ アソシエーションを保持します。セキュリティ アソシエーションは、期限満了するまでその後の 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満了する前に、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。デフォルトをそのまま使用することをお勧めします。

**（注）**　IKE セキュリティ アソシエーションが無限のライフタイム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、ピアからの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。
次の例は、グローバル コンフィギュレーション モードで、**isakmp policy lifetime** コマンドを使用する方法を示します。この例では、優先順位番号 40 の IKE ポリシー内に 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**

この例では、グローバル コンフィギュレーション モードで、優先順位番号 40 の IKE ポリシー内に 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。

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

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

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

**関連コマンド**

| | |
|---|---|
| **clear configure isakmp** | すべての ISAKMP コンフィギュレーションを消去します。 |
| **clear configure isakmp policy** | ISAKMP ポリシー コンフィギュレーションをすべて消去します。 |
| **clear isakmp sa** | IKE ランタイム SA データベースを消去します。 |
| **show running-config isakmp** | アクティブな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まで待機しないでセキュリティ アプライアンスのリブートを進めるには、このコマンドの **no** 形式を使用します。

**isakmp reload-wait**

**no isakmp reload-wait**

## シンタックスの説明

このコマンドには、引数もキーワードもありません。

## 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

次の表は、このコマンドを入力できるモードを示しています。

| | 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 reload-wait** コマンドに置き換えられました。 |

## 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リブートするように、セキュリティ アプライアンスに通知します。

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

# issuer-name

規則エントリ文字列との比較対象となる CA 証明書の DN を指定するには、CA 証明書マップ コンフィギュレーション モードで **issuer-name** コマンドを使用します。発行者名を削除するには、コマンドの **no** 形式を使用します。

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

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

## シンタックスの説明

| | |
|---|---|
| ***attr tag*** | 証明書の DN 文字列で、指定されているアトリビュート値だけが規則エントリ文字列と比較されることを示します。タグの値を次に示します。<br><br>DNQ = DN 修飾子<br>GENQ = 世代修飾子<br>I = イニシャル<br>GN = 名<br>N = 名前<br>SN = 姓<br>IP = IP アドレス<br>SER = シリアル番号<br>UNAME = 非構造化名<br>EA = 電子メール アドレス<br>T = 役職<br>O = 組織名<br>L = 地名<br>SP = 州または都道府県<br>C = 国または地域<br>OU = 組織ユニット<br>CN = 通常名 |
| ***co*** | DN 文字列または指定されているアトリビュートが、規則エントリ文字列の部分文字列と一致する必要があることを指定します。 |
| ***eq*** | DN 文字列または指定されているアトリビュートが、規則の文字列全体と一致する必要があることを指定します。 |
| ***nc*** | DN 文字列または指定されているアトリビュートが、規則エントリ文字列の部分文字列と一致しない必要があることを指定します。 |
| ***ne*** | DN 文字列または指定されているアトリビュートが、規則の文字列全体と一致しない必要があることを指定します。 |
| *string* | 規則エントリ情報を指定します。 |

## 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

次の表は、このコマンドを入力できるモードを示しています。

| | 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 |
| 暗号 CA トラストポイント コンフィギュレーション | • | • | • | • | • |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが導入されました。 |

## 例

次の例では、証明書マップ 4 の CA 証明書マップ モードに入り、発行者名を O = central として設定します。

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

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **crypto ca certificate map** | CA 証明書マップ モードに入ります。 |
| **subject-name（暗号 CA 証明書マップ）** | 規則エントリ文字列との比較対象となる、CA 証明書に含まれている DN を指定します。 |