CHAPTER 4

ipv6 address コマンド～ ip verify reverse-path コマンド

ipv6 address

IPv6 をイネーブルにし、インターフェイスで IPv6 アドレスを設定（ルーテッド モード）したり、ブリッジ グループまたは管理インターフェイス アドレスの IPv6 アドレスを設定（トランスペアレント モード）したりするには、**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** [**default trust** {**dhcp** | **ignore**}] | **dhcp** [**default**] |
ipv6_address/*prefix_length* [**standby** *ipv6_prefix* | **cluster-pool** *poolname*] |
ipv6_prefix/*prefix_length* **eui-64** | *prefix_name ipv6_address*/*prefix_length* | *ipv6_address*
link-local [**standby** *ipv6_address*]}

no ipv6 address {**autoconfig** [**default trust** {**dhcp** | **ignore**}] | **dhcp** [**default**] |
ipv6_address/*prefix_length* [**standby** *ipv6_address* | **cluster-pool** *poolname*] |
ipv6_prefix/*prefix_length* **eui-64** | *prefix_name ipv6_address*/*prefix_length* | *ipv6_address*
link-local [**standby** *ipv6_address*]}

構文の説明

autoconfig	インターフェイスでステートレスな自動設定をイネーブルにします。インターフェイスでステートレスな自動設定をイネーブルにすると、ルータ アドバタイズメント メッセージで受信したプレフィックスに基づいて IPv6 アドレスが設定されます。ステートレスな自動設定がイネーブルになっている場合、インターフェイスのリンクローカル アドレスは、Modified EUI-64 インターフェイス ID に基づいて自動的に生成されます。トランスペアレント ファイアウォール モードではサポートされません。 （注） RFC 4862 では、ステートレスな自動設定に設定されたホストはルータ アドバタイズメント メッセージを送信しないと規定していますが、ASA はこの場合、ルータ アドバタイズメント メッセージを送信します。メッセージを抑制するには、**ipv6 nd suppress-ra** コマンドを参照してください。

cluster-pool *poolname*	(オプション)ASA クラスタリングの場合に、**ipv6 local pool** コマンドで定義されたアドレスのクラスタ プールを設定します。引数で定義されたメイン クラスタの IP アドレスは、現在のマスター ユニットだけに属します。各クラスタ メンバには、このプールからローカル IP アドレスが割り当てられます。 各ユニットに割り当てられるアドレスを、事前に正確に特定することはできません。各ユニットで使用されているアドレスを表示するには、**show ipv6 local pool** *poolname* コマンドを入力します。各クラスタ メンバには、クラスタに参加したときにメンバ ID が割り当てられます。この ID によって、プールから使用されるローカル IP が決定します。
default	(オプション)ルータ アドバタイズメントからデフォルト ルートを取得します。
default trust	(オプション)ルータ アドバタイズメントからデフォルト ルートをインストールします。
dhcp (autoconfig)	(オプション)信頼できる送信元から(言い換えると、IPv6 アドレスを提供した同じサーバから)取得されたルータ アドバタイズメントからのデフォルト ルートのみを ASA が使用することを指定します。
dhcp	DHCPv6 サーバから IPv6 アドレスを取得します。
ignore	(オプション)別のネットワークからルータ アドバタイズメントを取得できる(よりリスクの高い方法となる可能性がある)ことを指定します。
ipv6_address/prefix_length	インターフェイスにグローバル アドレスを割り当てます。グローバル アドレスを割り当てると、インターフェイスのリンクローカル アドレスが自動的に作成されます。
ipv6_prefix/prefix_length **eui-64**	Modified EUI-64 形式を使用してインターフェイスの MAC アドレスから生成されたインターフェイス ID と、指定されたプレフィックスを結合することによって、インターフェイスにグローバル アドレスを割り当てます。グローバル アドレスを割り当てると、インターフェイスのリンクローカル アドレスが自動的に作成されます。*prefix_length* 引数で指定された値が 64 ビットを超えている場合は、プレフィックス ビットがインターフェイス ID よりも優先されます。指定したアドレスを別のホストが使用している場合は、エラー メッセージが表示されます。 スタンバイ アドレスを指定する必要はありません。インターフェイス ID が自動的に生成されます。 Modified EUI-64 形式のインターフェイス ID は、リンク層アドレスの上位 3 バイト(OUI フィールド)と下位 3 バイト(シリアル番号)の間に 16 進数の FFFE を挿入することで、48 ビット リンク層(MAC)アドレスから導出されます。選択されたアドレスが一意のイーサネット MAC アドレスから生成されることを保証するため、上位バイトの下位から 2 番めのビット(ユニバーサル/ローカル ビット)が反転され、48 ビット アドレスの一意性が示されます。たとえば、MAC アドレス 00E0.B601.3B7A のインターフェイスには、02E0:B6FF:FE01:3B7A の 64 ビット インターフェイス ID が指定されます。

ipv6_address **link-local**	手動でリンクローカル アドレスだけを設定します。このコマンドに指定された *ipv6_address* は、インターフェイス用に自動的に生成されるリンクローカル アドレスを上書きします。リンクローカル アドレスは、リンクローカル プレフィックス FE80::/64 と Modified EUI-64 形式のインターフェイス ID で形成されます。MAC アドレスが 00E0.B601.3B7A のインターフェイスの場合、リンクローカル アドレスは FE80::2E0:B6FF:FE01:3B7A になります。指定したアドレスを別のホストが使用している場合は、エラー メッセージが表示されます。
prefix_name *ipv6_address/prefix_length*	委任されたプレフィックスを使用します。この機能は、ASA インターフェイスに DHCPv6 プレフィクス委任クライアントをイネーブルにさせる（**ipv6 dhcp client pd**）ために必要です。通常、委任されたプレフィクスは /60 以下であるため、複数 /64 ネットワークにサブネット化できます。接続されるクライアント用に SLAAC をサポートする必要がある場合は、/64 がサポートされるサブネット長です。/60 サブネットを補完するアドレス（1:0:0:0:1 など）を指定する必要があります。プレフィックスが /60 未満の場合は、アドレスの前に :: を入力します。たとえば、委任されたプレフィクスが 2001:DB8:1234:5670::/60 である場合、このインターフェイスに割り当てられるグローバル IP アドレスは 2001:DB8:1234:5671::1/64 です。ルータ アドバタイズメントでアドバタイズされるプレフィクスは 2001:DB8:1234:5671::/64 です。この例では、プレフィクスが /60 未満である場合、プレフィックスの残りのビットは、前に配置される :: によって示されるように、0 になります。たとえば、プレフィクスが 2001:DB8:1234::/48 である場合、IPv6 アドレスは 2001:DB8:1234::1:0:0:0:1/64 になります。
standby *ipv6_address*	（任意）フェールオーバー ペアのセカンダリ ユニットまたはフェールオーバー グループで使用されるインターフェイス アドレスを指定します。

デフォルト

IPv6 はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(1)	トランスペアレント ファイアウォール モードのサポートが追加されました。
8.2(2)	スタンバイ アドレスのサポートが追加されました。
8.4(1)	トランスペアレント モード用にブリッジ グループが追加されました。BVI の IP アドレスを設定し、グローバルには設定しません。
9.0(1)	ASA クラスタリングをサポートするために、**cluster-pool** キーワードが追加されました。
9.6(2)	次のオプションが追加されました。 • **autoconfig default trust** {**dhcp** | **ignore**} • **dhcp** [**default**] • *prefix_name ipv6_address/prefix_length*

使用上のガイドライン

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

マルチ コンテキスト モードのガイドライン

シングル コンテキスト ルーテッド ファイアウォール モードでは、各インターフェイス アドレスはそれぞれ固有のサブネットに存在する必要があります。マルチ コンテキスト モードでは、このインターフェイスが共有インターフェイスにある場合、各 IP アドレスはそれぞれ固有であるものの、同じサブネットに存在する必要があります。インターフェイスが固有のものである場合、この IP アドレスを必要に応じて他のコンテキストで使用できます。

DHCPv6 およびプレフィクス委任オプションは、マルチ コンテキスト モードではサポートされていません。

トランスペアレント ファイアウォールのガイドライン

トランスペアレント モードでは、IPv6 アドレスの手動設定のみがサポートされています。トランスペアレント ファイアウォールは、IP ルーティングに参加しません。ASA に必要な唯一の IP コンフィギュレーションは、BVI のアドレスを設定することです。このアドレスが必要になるのは、ASA がシステム メッセージや AAA サーバとの通信など ASA で発信されるトラフィックの送信元アドレスとしてこのアドレスを使用するためです。このアドレスは、リモート管理アクセスにも使用できます。このアドレスは、上流のルータおよび下流のルータと同じサブネットに存在する必要があります。マルチ コンテキスト モードの場合、各コンテキスト内の管理 IP アドレスを設定します。管理インターフェイスを含むモデルの場合は、このインターフェイスの IP アドレスを管理用に設定することもできます。

フェールオーバーのガイドライン

スタンバイ IP アドレスは、メイン IP アドレスと同じサブネットに存在する必要があります。

ASA クラスタリングのガイドライン

個々のインターフェイスのクラスタ プールは、クラスタ インターフェイス モードを個別インターフェイスに設定（**cluster-interface mode individual**）してからでないと設定できません。唯一の例外は管理専用インターフェイスです。

- 管理専用インターフェイスはいつでも、個別インターフェイスとして設定できます(スパンド EtherChannel モードのときでも)。管理インターフェイスは、個別インターフェイスとすることができます(トランスペアレント ファイアウォール モードのときでも)。
- スパンド EtherChannel モードでは、管理インターフェイスを個別インターフェイスとして設定すると、管理インターフェイスに対してダイナミック ルーティングをイネーブルにできません。スタティック ルートを使用する必要があります。

DHCPv6 およびプレフィクス委任オプションは、クラスタリングではサポートされていません。

例

次に、選択したインターフェイスのグローバル アドレスとして 2001:0DB8:BA98::3210/64 を割り当て、スタンバイ ユニットの対応するインターフェイスのアドレスとして 2001:0DB8:BA98::3211 を割り当てる例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 address 2001:0DB8:BA98::3210/64 standby 2001:0DB8:BA98::3211
```

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

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

次に、IPv6 プレフィックス 2001:0DB8:BA98::/64 を選択したインターフェイスに割り当て、アドレスの下位 64 ビットに EUI-64 インターフェイス ID を指定する例を示します。このデバイスがフェールオーバー ペアの一部である場合は、**standby** キーワードを指定する必要がありません。スタンバイ アドレスは、Modified EUI-64 インターフェイス ID を使用して自動的に作成されます。

```
ciscoasa(config)# interface gigabitethernet 0/2
ciscoasa(onfig-if)# ipv6 address 2001:0DB8:BA98::/64 eui-64
```

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

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# ipv6 address FE80::260:3EFF:FE11:6670 link-local
```

次に、フェールオーバー ペアのプライマリ ユニットで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、セカンダリ ユニットの対応する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:FE11:6671 を割り当てる例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# ipv6 address FE80::260:3EFF:FE11:6670 link-local standby
FE80::260:3EFF:FE11:6671
```

次に、委任されたプレフィクスを補完するためのアドレスとして ::1:0:0:0:1/64 を割り当てる例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/5
ciscoasa(config-if)# ipv6 address Outside-Prefix ::1:0:0:0:1/64
```

関連コマンド

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

ipv6-address-pool

アドレスをリモート クライアントに割り当てるための IPv6 アドレス プール リストを指定するには、トンネル グループ一般属性コンフィギュレーション モードで **ipv6-address-pool** コマンドを使用します。IPv6 アドレス プールを削除するには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

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

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

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

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

プールの指定順序は重要です。ASA では、このコマンドでプールを指定した順序に従って、それらのプールからアドレスが割り当てられます。

例

次に、トンネル グループ一般属性コンフィギュレーション モードを開始し、IPsec リモート アクセス トンネル グループ テスト用に、アドレスをリモート クライアントに割り当てるための IPv6 アドレス プール リストを指定する例を示します。

```
ciscoasa(config)# tunnel-group test type remote-access
ciscoasa(config)# tunnel-group test general-attributes
ciscoasa(config-tunnel-general)# ipv6-address-pool (inside) ipv6addrpool1 ipv6addrpool2
ipv6addrpool3
ciscoasa(config-tunnel-general)#
```

関連コマンド

コマンド	説明
ipv6-address-pools	グループ ポリシーの IPv6 アドレス プール設定を設定します。これらの設定は、トンネル グループの IPv6 アドレス プール設定を上書きします。
ipv6 local pool	VPN リモート アクセス トンネルに使用する IP アドレス プールを設定します。
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group	トンネル グループを設定します。

ipv6-address-pools

アドレスをリモート クライアントに割り当てるための IPv6 アドレス プール リストを最大 6 つ指定するには、グループ ポリシー属性コンフィギュレーション モードで **ipv6-address-pools** コマンドを使用します。グループ ポリシーから属性を削除し、別のグループ ポリシー ソースからの継承をイネーブルにするには、このコマンドの **no** 形式を使用します。

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

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

ipv6-address-pools none

no ipv6-address-pools none

構文の説明

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

デフォルト

デフォルトでは、IPv6 アドレス プールの属性は設定されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グループ ポリシー属性コンフィギュレーション	• Yes	—	• Yes	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

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

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

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

例

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

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

関連コマンド

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

ipv6 dhcp client pd

DHCPv6 プレフィクス委任クライアントをイネーブルにするとともに、インターフェイスで取得されるプレフィックスに名前を付けるには、インターフェイス コンフィギュレーション モードで **ipv6 dhcp client pd** コマンドを使用します。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。

ipv6 dhcp client pd *name*

no ipv6 dhcp client pd *name*

構文の説明

name	このプレフィックスの名前を設定します。名前には最大 200 文字を使用できます。プレフィックス（**ipv6 address** *prefix_name*）を使用してインターフェイスに IP アドレスを割り当てるときに、この名前を使用します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

1 つ以上のインターフェイスで DHCPv6 プレフィクス委任クライアントをイネーブルにします。ASA は、サブネット化して内部ネットワークに割り当てることができる 1 つ以上の IPv6 プレフィックスを取得します。通常、プレフィックス委任クライアントをイネーブルにしたインターフェイスは DHCPv6 アドレス クライアントを使用して IP アドレスを取得し、その他の ASA インターフェイスだけが、委任されたプレフィックスから取得されるアドレスを使用します。

この機能は、クラスタリングではサポートされていません。

この機能は管理専用インターフェイスでは設定できません。

例

次に、GigabitEthernet 0/0 で DHCPv6 アドレスクライアントおよびプレフィックス委任クライアントを設定した後に、アドレスをプレフィックスとともに GigabitEthernet 0/1 および 0/2 に割り当てる例を示します。

```
interface gigabitethernet 0/0
    ipv6 address dhcp setroute default
    ipv6 dhcp client pd Outside-Prefix
    ipv6 dhcp client pd hint ::/60
interface gigabitethernet 0/1
    ipv6 address Outside-Prefix ::1:0:0:0:1/64
interface gigabitethernet 0/2
    ipv6 address Outside-Prefix ::2:0:0:0:1/64
```

関連コマンド

コマンド	説明
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
domain-name	IR メッセージへの応答で SLAAC クライアントに提供されるドメイン名を設定します。
dns-server	IR メッセージへの応答で SLAAC クライアントに提供される DNS サーバを設定します。
import	ASA がプレフィックス委任クライアント インターフェイスで DHCPv6 サーバから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
ipv6 address	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
ipv6 address dhcp	インターフェイスの DHCPv6 を使用してアドレスを取得します。
ipv6 dhcp client pd hint	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
ipv6 dhcp pool	DHCPv6 ステートレス サーバを使用して、特定のインターフェイスで SLAAC クライアントに提供する情報を含むプールを作成します。
ipv6 dhcp server	DHCPv6 ステートレス サーバを有効にします。
network	サーバから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
nis address	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。
nis domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。
show ipv6 dhcp	DHCPv6 情報を表示します。
show ipv6 general-prefix	DHCPv6 プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示します。
sip address	IR メッセージへの応答で SLAAC クライアントに提供される SIP アドレスを設定します。

コマンド	説明
sip domain-name	IR メッセージへの応答で SLAAC クライアントに提供される SIP ドメイン名を設定します。
sntp address	IR メッセージへの応答で SLAAC クライアントに提供される SNTP アドレスを設定します。

ipv6 dhcp client pd hint

受信する委任されたプレフィクスに関する 1 つ以上のヒントを提供するには、インターフェイス コンフィギュレーション モードで **ipv6 dhcp client pd hint** コマンドを使用します。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。

ipv6 dhcp client pd hint *ipv6_prefix/prefix_length*

no ipv6 dhcp client pd hint *ipv6_prefix/prefix_length*

構文の説明

ipv6_prefix/prefix_length	受信する IPv6 プレフィックスとプレフィックス長を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

通常、特定のプレフィクス長（::/60 など）を要求しますが、以前に特定のプレフィックスを受信しており、リースの期限が切れるときにそれを確実に再取得したい場合は、そのプレフィックスの全体をヒントとして入力できます。複数のヒント（異なるプレフィックスまたはプレフィックス長）を入力すると、どのヒントに従うのか、またはそもそもヒントに従うのかどうかが DHCP サーバによって決定されます。

例

次に、GigabitEthernet 0/0 で DHCPv6 アドレスクライアントおよびプレフィックス委任クライアントを設定した後に、アドレスをプレフィックスとともに GigabitEthernet 0/1 および 0/2 に割り当てる例を示します。

```
interface gigabitethernet 0/0
    ipv6 address dhcp setroute default
    ipv6 dhcp client pd Outside-Prefix
    ipv6 dhcp client pd hint ::/60
interface gigabitethernet 0/1
    ipv6 address Outside-Prefix ::1:0:0:0:1/64
interface gigabitethernet 0/2
    ipv6 address Outside-Prefix ::2:0:0:0:1/64
```

関連コマンド

コマンド	説明
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
domain-name	IR メッセージへの応答で SLAAC クライアントに提供されるドメイン名を設定します。
dns-server	IR メッセージへの応答で SLAAC クライアントに提供される DNS サーバを設定します。
import	ASA がプレフィックス委任クライアント インターフェイスで DHCPv6 サーバから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
ipv6 address	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
ipv6 address dhcp	インターフェイスの DHCPv6 を使用してアドレスを取得します。
ipv6 dhcp client pd hint	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
ipv6 dhcp pool	DHCPv6 ステートレス サーバを使用して、特定のインターフェイスで SLAAC クライアントに提供する情報を含むプールを作成します。
ipv6 dhcp server	DHCPv6 ステートレス サーバを有効にします。
network	サーバから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
nis address	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。
nis domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。
show ipv6 dhcp	DHCPv6 情報を表示します。
show ipv6 general-prefix	DHCPv6 プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示します。
sip address	IR メッセージへの応答で SLAAC クライアントに提供される SIP アドレスを設定します。

コマンド	説明
sip domain-name	IR メッセージへの応答で SLAAC クライアントに提供される SIP ドメイン名を設定します。
sntp address	IR メッセージへの応答で SLAAC クライアントに提供される SNTP アドレスを設定します。

ipv6 dhcp pool

DHCPv6 サーバからステートレス アドレス自動設定（SLAAC）クライアントに提供させる情報を含む IPv6 DHCP プールを設定するには、グローバル コンフィギュレーション モードで **ipv6 dhcp pool** コマンドを使用します。プールを削除するには、このコマンドの **no** 形式を使用します。

ipv6 dhcp pool *pool_name*

no ipv6 dhcp pool *pool_name*

構文の説明

pool_name	プールの名前を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

SLAAC をプレフィックス委任機能とともに使用するクライアントについては、情報要求（IR）パケットを ASA に送信する際に情報（DNS サーバ、ドメイン名など）を提供するように ASA を設定できます。ASA は IR パケットのみを受け入れます。また、アドレスをクライアントに割り当てません。**ipv6 dhcp server** コマンドを使用して DHCPv6 ステートレス サーバを設定します。サーバをイネーブルにする場合は、このプール名を指定します。必要に応じてインターフェイスごとに個別のプールを設定できます。また、複数のインターフェイスで同じプールを使用することもできます。**ipv6 dhcp pool** コマンドを入力した後に、クライアントに提供する 1 つ以上のパラメータを設定できます。

ipv6 dhcp client pd コマンドを使用してプレフィックス委任を設定します。

この機能は、クラスタリングではサポートされていません。

例

次に、2 つの IPv6 DHCP プールを作成して、2 つのインターフェイスで DHCPv6 サーバを有効にする例を示します。

```
ipv6 dhcp pool Eng-Pool
    domain-name eng.example.com
    import dns-server
ipv6 dhcp pool IT-Pool
    domain-name it.example.com
    import dns-server
interface gigabitethernet 0/0
    ipv6 address dhcp setroute default
    ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
    ipv6 address Outside-Prefix ::1:0:0:0:1/64
    ipv6 dhcp server Eng-Pool
    ipv6 nd other-config-flag
interface gigabitethernet 0/2
    ipv6 address Outside-Prefix ::2:0:0:0:1/64
    ipv6 dhcp server IT-Pool
    ipv6 nd other-config-flag
```

関連コマンド

コマンド	説明
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
domain-name	IR メッセージへの応答で SLAAC クライアントに提供されるドメイン名を設定します。
dns-server	IR メッセージへの応答で SLAAC クライアントに提供される DNS サーバを設定します。
import	ASA がプレフィックス委任クライアント インターフェイスで DHCPv6 サーバから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
ipv6 address	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
ipv6 address dhcp	インターフェイスの DHCPv6 を使用してアドレスを取得します。
ipv6 dhcp client pd	委任されたプレフィックスを使用して、インターフェイスのアドレスを設定します。
ipv6 dhcp client pd hint	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
ipv6 dhcp server	DHCPv6 ステートレス サーバを有効にします。
network	サーバから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
nis address	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。
nis domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。

コマンド	説明
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。
show ipv6 dhcp	DHCPv6 情報を表示します。
show ipv6 general-prefix	DHCPv6 プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示します。
sip address	IR メッセージへの応答で SLAAC クライアントに提供される SIP アドレスを設定します。
sip domain-name	IR メッセージへの応答で SLAAC クライアントに提供される SIP ドメイン名を設定します。
sntp address	IR メッセージへの応答で SLAAC クライアントに提供される SNTP アドレスを設定します。

ipv6 dhcprelay enable

インターフェイスで DHCPv6 リレー サービス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 **ipv6 dhcprelay enable** コマンドを使用します。DHCPv6 リレー サービスをディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 dhcprelay enable *interface*

no ipv6 dhcprelay enable *interface*

構文の説明

interface	宛先の出力インターフェイスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、インターフェイスで DHCPv6 リレー サービスをイネーブルにすることができます。このサービスをイネーブルにすると、インターフェイスに対するクライアントからの着信 DHCPv6 メッセージ(他のリレー エージェントでリレーされたメッセージも含む)が、設定されているすべての発信リンクを介してすべての設定済みリレー宛先に転送されます。マルチ コンテキスト モードの場合は、複数のコンテキストで使用されているインターフェイス(つまり、共有インターフェイス)で DHCP リレー サービスをイネーブルにすることはできません。

例

次に、ASA の外部インターフェイスの DHCPv6 サーバ(IP アドレス 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701)に対する DHCPv6 リレー エージェントを設定する例を示します。クライアント要求の送信元は ASA の内部インターフェイスで、バインディングのタイムアウト値は 90 秒です。

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 outside
ciscoasa(config)# ipv6 dhcprelay timeout 90
ciscoasa(config)# ipv6 dhcprelay enable inside
```

関連コマンド

コマンド	説明
ipv6 dhcprelay server	クライアント メッセージの転送先となる IPv6 DHCP サーバの宛先アドレスを指定します。
ipv6 dhcprelay timeout	DHCPv6 サーバからの応答をリレー バインディング構造を通して DHCPv6 クライアントに渡すときに許容する時間の長さを秒単位で設定します。

ipv6 dhcprelay server

クライアント メッセージの転送先となる IPv6 DHCP サーバの宛先アドレスを指定するには、グローバル コンフィギュレーション モードで **ipv6 dhcprelay server** コマンドを使用します。IPv6 DHCP サーバの宛先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 dhcprelay server *ipv6-address* [*interface*]

no ipv6 dhcprelay server *ipv6-address* [*interface*]

構文の説明

interface	(オプション)宛先の出力インターフェイスを指定します。
ipv6-address	リンク スコープのユニキャスト、マルチキャスト、サイト スコープのユニキャスト、またはグローバル IPv6 アドレスを指定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• Yes	—	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、クライアント メッセージの転送先となる IPv6 DHCP サーバの宛先アドレスを指定できます。クライアントのメッセージは、この出力インターフェイスが接続されたリンクを経由して宛先アドレスに転送されます。指定したアドレスがリンク スコープのアドレスである場合は、インターフェイスを指定する必要があります。リレー宛先の指定は必須です。ループバックやノードローカルのマルチキャスト アドレスは指定できません。サーバは 1 つのコンテキストに対して 10 台まで指定できます。

例

次に、ASA の外部インターフェイスの DHCPv6 サーバ（IP アドレス 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701）に対する DHCPv6 リレー エージェントを設定する例を示します。クライアント要求の送信元は ASA の内部インターフェイスで、バインディングのタイムアウト値は 90 秒です。

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 outside
ciscoasa(config)# ipv6 dhcprelay timeout 90
ciscoasa(config)# ipv6 dhcprelay enable inside
```

関連コマンド

コマンド	説明
ipv6 dhcprelay enable	インターフェイスで IPv6 DHCP リレー サービスをイネーブルにします。
ipv6 dhcprelay timeout	DHCPv6 サーバからの応答をリレー バインディング構造を通して DHCPv6 クライアントに渡すときに許容する時間の長さを秒単位で設定します。

ipv6 dhcprelay timeout

DHCPv6 サーバからの応答をリレー バインディング構造を通して DHCPv6 クライアントに渡すときに許容する時間の長さ(秒数)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 dhcprelay timeout** 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。

ipv6 dhcprelay timeout *seconds*

no ipv6 dhcprelay timeout *seconds*

構文の説明

seconds	DHCPv6 リレー アドレス ネゴシエーションの許容時間(秒数)を設定します。有効な値の範囲は、1 ～ 3600 です。

デフォルト

デフォルトは 60 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、DHCPv6 サーバからの応答をリレー バインディング構造を通して DHCPv6 クライアントに渡すときに許容する時間の長さを秒単位で設定できます。

例

次に、ASA の外部インターフェイスの DHCPv6 サーバ(IP アドレス 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701)に対する DHCPv6 リレー エージェントを設定する例を示します。クライアント要求の送信元は ASA の内部インターフェイスで、バインディングのタイムアウト値は 90 秒です。

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 outside
ciscoasa(config)# ipv6 dhcprelay timeout 90
ciscoasa(config)# ipv6 dhcprelay enable inside
```

関連コマンド

コマンド	説明
ipv6 dhcprelay server	クライアント メッセージの転送先となる IPv6 DHCP サーバの宛先アドレスを指定します。
ipv6 dhcprelay enable	クライアント メッセージの転送先となる IPv6 DHCP サーバの宛先アドレスを指定します。

ipv6 dhcp server

ステートレス アドレス自動設定(SLAAC)をプレフィックス委任機能とともに使用するクライアントについては、インターフェイス コンフィギュレーション モードで **ipv6 dhcp server** コマンドを使用して DHCPv6 ステートレス サーバを設定します。DHCP サーバ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 dhcp server *pool_name*

no ipv6 dhcp server *pool_name*

構文の説明

pool_name	**ipv6 dhcp pool** コマンドで設定した IPv6 プールの名前を設定します。このプールには、特定のインターフェイスでクライアントに提供する情報が含まれます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

SLAAC をプレフィックス委任機能とともに使用するクライアントについては、情報要求（IR）パケットを ASA に送信する際に情報（DNS サーバ、ドメイン名など）を提供するように ASA を設定できます。ASA は IR パケットのみを受け入れます。また、アドレスをクライアントに割り当てません。**ipv6 dhcp client pd** コマンドを使用してプレフィックス委任を設定します。

この機能は、クラスタリングではサポートされていません。

例

次に、2 つの IPv6 DHCP プールを作成して、2 つのインターフェイスで DHCPv6 サーバを有効にする例を示します。

```
ipv6 dhcp pool Eng-Pool
    domain-name eng.example.com
    import dns-server
ipv6 dhcp pool IT-Pool
    domain-name it.example.com
    import dns-server
interface gigabitethernet 0/0
    ipv6 address dhcp setroute default
    ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
    ipv6 address Outside-Prefix ::1:0:0:0:1/64
    ipv6 dhcp server Eng-Pool
    ipv6 nd other-config-flag
interface gigabitethernet 0/2
    ipv6 address Outside-Prefix ::2:0:0:0:1/64
    ipv6 dhcp server IT-Pool
    ipv6 nd other-config-flag
```

関連コマンド

コマンド	説明
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
domain-name	IR メッセージへの応答で SLAAC クライアントに提供されるドメイン名を設定します。
dns-server	IR メッセージへの応答で SLAAC クライアントに提供される DNS サーバを設定します。
import	ASA がプレフィックス委任クライアント インターフェイスで DHCPv6 サーバから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
ipv6 address	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
ipv6 address dhcp	インターフェイスの DHCPv6 を使用してアドレスを取得します。
ipv6 dhcp client pd	委任されたプレフィックスを使用して、インターフェイスのアドレスを設定します。
ipv6 dhcp client pd hint	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
ipv6 dhcp pool	DHCPv6 ステートレス サーバを使用して、特定のインターフェイスで SLAAC クライアントに提供する情報を含むプールを作成します。
network	サーバから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
nis address	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。

コマンド	説明
nis domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。
show ipv6 dhcp	DHCPv6 情報を表示します。
show ipv6 general-prefix	DHCPv6 プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示します。
sip address	IR メッセージへの応答で SLAAC クライアントに提供される SIP アドレスを設定します。
sip domain-name	IR メッセージへの応答で SLAAC クライアントに提供される SIP ドメイン名を設定します。
sntp address	IR メッセージへの応答で SLAAC クライアントに提供される SNTP アドレスを設定します。

ipv6 enable

IPv6 処理をイネーブルにする場合に、まだ明示的な IPv6 アドレスを設定していないときには、グローバル コンフィギュレーション モードで **ipv6 enable** コマンドを使用します。明示的な IPv6 アドレスでまだ設定されていないインターフェイスで IPv6 処理をディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 enable

no ipv6 enable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

IPv6 はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• Yes	—	• Yes	• Yes	—
グローバル コンフィギュレーション	—	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(1)	トランスペアレント ファイアウォール モードのサポートが追加されました。

使用上のガイドライン

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

明示的な IPv6 アドレスで設定されているインターフェイスで **no ipv6 enable** コマンドを実行しても、IPv6 処理はディセーブルになりません。

例

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

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

関連コマンド

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

ipv6 enforce-eui64

ローカル リンク上の IPv6 アドレスに Modified EUI-64 形式のインターフェイス ID の使用を適用するには、グローバル コンフィギュレーション モードで **ipv6 enforce-eui64** コマンドを使用します。Modified EUI-64 アドレス形式の適用をディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 enforce-eui64 *if_name*

no ipv6 enforce-eui64 *if_name*

構文の説明

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

デフォルト

Modified EUI-64 形式の適用はディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.2(1)	トランスペアレント ファイアウォール モードのサポートが追加されました。

使用上のガイドライン

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

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

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

48 ビット リンク層（MAC）アドレスから Modified EUI-64 形式のインターフェイス ID を取得するには、リンク層アドレスの上位 3 バイト（OUI フィールド）と下位 3 バイト（シリアル番号）との間に 16 進数 FFFE を挿入します。選択されたアドレスが一意のイーサネット MAC アドレスから生成されることを保証するため、上位バイトの下位から 2 番めのビット（ユニバーサル/ローカル ビット）が反転され、48 ビット アドレスの一意性が示されます。たとえば、MAC アドレス 00E0.B601.3B7A のインターフェイスには、02E0:B6FF:FE01:3B7A の 64 ビット インターフェイス ID が指定されます。

例

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

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

関連コマンド

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

ipv6 icmp

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

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

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

構文の説明

any	IPv6 アドレスを指定するキーワード。IPv6 プレフィックス ::/0 の省略形。
deny	選択したインターフェイスで指定の ICMP トラフィックを阻止します。
host	アドレスが特定のホストを指すよう指定します。

icmp-type	アクセス ルールによってフィルタリングされる ICMP メッセージ タイプを指定します。値は、有効な ICMP タイプ番号（0 ～ 255）、または次の ICMP タイプ リテラルのいずれかを指定できます。 • destination-unreachable • packet-too-big • time-exceeded • parameter-problem • echo-request • echo-reply • membership-query • membership-report • membership-reduction • router-renumbering • router-solicitation • router-advertisement • neighbor-solicitation • neighbor-advertisement • neighbor-redirect
if-name	アクセス ルールが適用されるインターフェイスの名前（**nameif** コマンドで指定した名前）。
ipv6-address	ICMPv6 メッセージをインターフェイスに送信しているホストの IPv6 アドレス。
ipv6-prefix	ICMPv6 メッセージをインターフェイスに送信している IPv6 ネットワーク。
permit	選択したインターフェイスで指定の ICMP トラフィックを許可します。
prefix-length	IPv6 プレフィックスの長さ。この値は、アドレスの高次の連続ビットのうち、プレフィックスのネットワーク部分を構成しているビットの数を示します。プレフィックス長の前にスラッシュ（/）を使用する必要があります。

デフォルト

ICMP アクセス ルールが定義されていない場合、すべての ICMP トラフィックが許可されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(1)	トランスペアレント ファイアウォール モードのサポートが追加されました。

使用上のガイドライン

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

IPv6 対応インターフェイスで許可される最小 MTU は 1280 バイトです。ただし、IPsec がインターフェイスでイネーブルになっている場合、MTU 値は、IPsec 暗号化のオーバーヘッドのために 1380 未満に設定できません。インターフェイスを 1380 バイト未満に設定すると、パケットのドロップが発生する可能性があります。

インターフェイスに対して定義されている ICMP ルールがない場合、すべての IPv6 ICMP トラフィックが許可されます。

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

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

ipv6 icmp コマンドは、ASA インターフェイスで終了する ICMP トラフィックのアクセス ルールを設定します。パススルー ICMP トラフィックのアクセス ルールを設定するには、**ipv6 access-list** コマンドを参照してください。

例

次に、外部インターフェイスですべての ping 要求を拒否し、すべての packet-too-big メッセージを許可する（パス MTU ディスカバリをサポートするため）方法を示します。

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

次に、ホスト 2000:0:0:4::2 またはプレフィックス 2001::/64 上のホストに対して外部インターフェイスへの ping を許可する例を示します。

```
ciscoasa(config)# ipv6 icmp permit host 2000:0:0:4::2 echo-reply outside
ciscoasa(config)# ipv6 icmp permit 2001::/64 echo-reply outside
ciscoasa(config)# ipv6 icmp permit any packet-too-big outside
```

関連コマンド

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

ipv6 local pool

IPv6 アドレス プールを設定するには、グローバル コンフィギュレーション モードで **ipv6 local pool** コマンドを使用します。プールを削除するには、このコマンドの **no** 形式を使用します。

ipv6 local pool *pool_name ipv6_address/prefix_length number_of_addresses*

no ipv6 local pool *pool_name ipv6_address/prefix_length number_of_addresses*

構文の説明

ipv6_address	プールの開始 IPv6 アドレスを指定します。
number_of_addresses	範囲：1 ～ 16384。
pool_name	この IPv6 アドレス プールに割り当てる名前を指定します。
prefix_length	範囲：0 ～ 128。

デフォルト

デフォルトでは、IPv6 ローカル アドレス プールは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	ASA クラスタリングをサポートするために、**ipv6 address** コマンドでクラスタ プールとして IPv6 ローカル プールを指定できるようになりました。

使用上のガイドライン

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

例

次に、アドレスをリモート クライアントに割り当てるために使用する firstipv6pool という名前の IPv6 アドレス プールを設定する例を示します。

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

関連コマンド

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

ipv6 nd dad attempts

重複アドレス検出時にインターフェイスに連続して送信されるネイバー送信要求メッセージの数を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd dad attempts** コマンドを使用します。送信する重複アドレス検出メッセージの数をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd dad attempts *value*

no ipv6 nd dad attempts *value*

構文の説明

value	0 ～ 600 の数値。0 を入力すると、指定したインターフェイスでの重複アドレス検出がディセーブルになります。1 を入力すると、後続の送信なしの単一の送信が設定されます。デフォルト値は 1 メッセージです。

デフォルト

デフォルトの試行回数は 1 回です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(1)	トランスペアレント ファイアウォール モードのサポートが追加されました。

使用上のガイドライン

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

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

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

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

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

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

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

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

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

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

例

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

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

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

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

関連コマンド

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

ipv6 nd managed-config-flag

IPv6 ルータ アドバタイズメント パケットの管理対象アドレス設定フラグを設定するように ASA 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 managed config-flag** 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。

ipv6 nd managed-config-flag

no ipv6 managed-config-flag

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

IPv6 自動設定クライアント ホストでは、このフラグを使用して、取得されるステートレス自動設定アドレスに加えて、ステートフル アドレス設定プロトコル(DHCPv6)に基づいてアドレスを取得する必要があることを示すことができます。

例

次に、インターフェイス GigabitEthernet 0/0 で IPv6 ルータ アドバタイズメント パケットの管理対象アドレス設定フラグを設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd managed config-flag
```

関連コマンド

コマンド	説明
ipv6 nd other-config-flag	IPv6 ルータ アドバタイズメント パケットの他の設定フラグを設定するように ASA を設定します。

ipv6 nd ns-interval

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

ipv6 nd ns-interval *value*

no ipv6 nd ns-interval [*value*]

構文の説明

value	IPv6 ネイバー送信要求メッセージが送信される時間間隔(ミリ秒単位)。有効な値の範囲は、1000 ～ 3600000 ミリ秒です。デフォルト値は 1000 ミリ秒です。

デフォルト

ネイバー送信要求のデフォルトの送信間隔は 1,000 ミリ秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(1)	トランスペアレント ファイアウォール モードのサポートが追加されました。

使用上のガイドライン

この値は、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 での IPv6 ネイバー送信要求の送信間隔を 9000 ミリ秒に設定します。

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

関連コマンド

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

ipv6 nd other-config-flag

IPv6 ルータ アドバタイズメント パケットの他の設定フラグを設定するように ASA 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 other-config-flag** 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。

ipv6 nd other-config-flag

no ipv6 other-config-flag

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

IPv6 自動設定クライアント ホストでは、このフラグを使用して、ステートフル アドレス設定プロトコル（DHCPv6）に基づいて DNS サーバなどの非アドレス設定情報を取得する必要があることを示すことができます。

例

次に、インターフェイス GigabitEthernet 0/0 で IPv6 ルータ アドバタイズメント パケットの他の設定フラグを設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd other-config-flag
```

関連コマンド

コマンド	説明
ipv6 nd managed-config-flag	IPv6 ルータ アドバタイズメント パケットの管理対象アドレス設定フラグを設定するように ASA を設定します。

ipv nd 6-prefix

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

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

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

構文の説明

at *valid-date preferred-date*	ライフタイムおよびプリファレンスが期限切れになる日付と時刻。プレフィックスは、この指定された日付と時刻に達するまで有効です。日付は *date-valid-expire month-valid-expire hh:mm-valid-expire date-prefer-expire month-prefer-expire hh:mm-prefer-expire* の形式で表されます。
default	デフォルト値が使用されます。
infinite	（任意）有効なライフタイムが期限切れになりません。
ipv6-prefix	ルータ アドバタイズメントに含まれる IPv6 ネットワーク番号。 この引数は、RFC 2373 に記述されている形式である必要があります。RFC 2373 では、コロンで区切った 16 ビット値を使用して 16 進数形式でアドレスを指定します。
no-advertise	（任意）ローカルリンク上のホストでは、指定されたプレフィックスが IPv6 自動設定に使用されないことを示します。

no-autoconfig	(任意)ローカルリンク上のホストでは、指定されたプレフィックスがIPv6 自動設定に使用できないことを示します。
off-link	(任意)指定されたプレフィックスがオンリンクの判別に使用されないことを示します。
preferred-lifetime	指定された IPv6 プレフィックスが優先プレフィックスとしてアドバタイズされる時間(秒単位)。有効値の範囲は 0 ～ 4294967295 秒です。最大値は無限ですが、これは **infinite** キーワードを使用して指定もできます。デフォルトは 604800(7 日間)です。
prefix-length	IPv6 プレフィックスの長さ。この値は、アドレスの高次の連続ビットのうち、プレフィックスのネットワーク部分を構成しているビットの数を示します。プレフィックス長の前にスラッシュ(/)を使用する必要があります。
valid-lifetime	指定された IPv6 プレフィックスが有効プレフィックスとしてアドバタイズされる時間。有効値の範囲は 0 ～ 4294967295 秒です。最大値は無限ですが、これは **infinite** キーワードを使用して指定もできます。デフォルトは 2592000(30 日間)です。

デフォルト

IPv6 ルータ アドバタイズメントを発信するインターフェイスに設定されているすべてのプレフィックスが、有効ライフタイム 2592000 秒(30 日)および優先ライフタイム 604800 秒(7 日)でアドバタイズされます。どちらのライフタイムにも「onlink」フラグと「autoconfig」フラグが設定されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、プレフィックスをアドバタイズするかどうかなど、プレフィックスごとに個々のパラメータを制御できます。

デフォルトでは、**ipv6 address** コマンドを使用してインターフェイスにアドレスとして設定されるプレフィックスは、ルータ アドバタイズメントでアドバタイズされます。**ipv6 nd prefix** コマンドを使用してアドバタイズメント用にプレフィックスを設定した場合は、そのプレフィックスだけがアドバタイズされます。

default キーワードを使用すると、すべてのプレフィックスのデフォルト パラメータを設定できます。

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

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

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

例

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

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

関連コマンド

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

ipv6 nd ra-interval

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

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

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

構文の説明

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

デフォルト

200 秒。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• Yes	—	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン　**ipv6 nd ra-lifetime** コマンドを使用して ASA がデフォルト ルータとして設定されている場合、送信間隔は IPv6 ルータ アドバタイズメントのライフタイム以下にする必要があります。他の IPv6 ノードとの同期を防止するには、実際に使用される値を指定値の 20 % 以内でランダムに調整します。

例　次に、選択したインターフェイスで IPv6 ルータ アドバタイズメントの間隔を 201 秒に設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd ra-interval 201
```

関連コマンド

コマンド	説明
ipv6 nd ra-lifetime	IPv6 ルータ アドバタイズメントのライフタイムを設定します。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 nd ra-lifetime

インターフェイスの IPv6 ルータ アドバタイズメントの「ルータ ライフタイム」の値を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd ra-lifetime** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd ra-lifetime *seconds*

no ipv6 nd ra-lifetime [*seconds*]

構文の説明

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

デフォルト

1800 秒。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• Yes	—	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

「ルータ ライフタイム」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。値は、ASA がこのインターフェイス上でデフォルト ルータとして有効であることを示します。

値をゼロ以外の値に設定すると、ASA がこのインターフェイス上でデフォルト ルータであると見なされます。「ルータ ライフタイム」の値としてゼロ以外の値を設定する場合は、その値がルータ アドバタイズメント間隔以上でなければなりません。

値を 0 に設定すると、ASA がこのインターフェイス上でデフォルト ルータであると見なされません。

例

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

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

関連コマンド

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

ipv6 nd reachable-time

到達可能性確認イベントが発生した後でリモート IPv6 ノードが到達可能であると見なされる時間を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd reachable-time** コマンドを使用します。デフォルトの時間に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd reachable-time *value*

no ipv6 nd reachable-time [*value*]

構文の説明

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

デフォルト

0 ミリ秒。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(1)	トランスペアレント ファイアウォール モードのサポートが追加されました。

使用上のガイドライン

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

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

例

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

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

関連コマンド

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

ipv6 nd suppress-ra

LAN インターフェイスで IPv6 ルータ アドバタイズメントの送信を抑制するには、インターフェイス コンフィギュレーション モードで **ipv6 nd suppress-ra** コマンドを使用します。LAN インターフェイスで IPv6 ルータ アドバタイズメントの送信を再びイネーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

IPv6 ユニキャスト ルーティングがイネーブルになっている場合、ルータ アドバタイズメントは LAN インターフェイスで自動的に送信されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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

例

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

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

関連コマンド

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

ipv6 neighbor

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

ipv6 neighbor *ipv6_address if_name mac_address*

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

構文の説明

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

デフォルト

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

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(1)	トランスペアレント ファイアウォール モードのサポートが追加されました。

使用上のガイドライン

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

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

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

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

例

次に、IPv6 アドレスを 3001:1::45A、MAC アドレスを 0002.7D1A.9472 にして、内部ホスト用のスタティック エントリをネイバー探索キャッシュに追加する例を示します。

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

関連コマンド

コマンド	説明
clear ipv6 neighbors	スタティック エントリを除く、IPv6 ネイバー探索キャッシュ内のすべてのエントリを削除します。
show ipv6 neighbor	IPv6 ネイバー キャッシュ情報を表示します。

ipv6 ospf

IPv6 の OSPFv3 インターフェイスのコンフィギュレ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 **ipv6 ospf** コマンドを使用します。IPv6 の OSPFv3 インターフェイスのコンフィギュレーションをディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 ospf [*process-id*] [**cost** | **database-filter** | **dead-interval** *seconds* | **flood-reduction** | **hello-interval** *seconds* | **mtu-ignore** | **neighbor** | **network** | **priority** | **retransmit-interval** *seconds* | **transmit-delay** *seconds*]

no ipv6 ospf [*process-id*] [**cost** | **database-filter** | **dead-interval** *seconds* | **flood-reduction** | **hello-interval** *seconds* | **mtu-ignore** | **neighbor** | **network** | **priority** | **retransmit-interval** *seconds* | **transmit-delay** *seconds*]

構文の説明

cost	インターフェイス上でパケットを送信するコストを明示的に指定します。
database-filter	OSPFv3 インターフェイスへの発信 LSA をフィルタリングします。
dead-interval *seconds*	秒単位で設定する期間内に hello パケットが確認されないと、当該ルータがダウンしていることがネイバーによって示されます。この値はネットワーク上のすべてのノードで同じにする必要があります。値の範囲は、1 ～ 65535 です。デフォルト値は、**ipv6 ospf hello-interval** コマンドで設定された間隔の 4 倍です。
flood-reduction	インターフェイスに LSA のフラッディング削減を指定します。
hello-interval *seconds*	インターフェイス上で送信される hello パケット間の間隔(秒数)を指定します。この値は特定のネットワーク上のすべてのノードで同じにする必要があります。値の範囲は、1 ～ 65535 です。デフォルトの間隔は、イーサネット インターフェイスで 10 秒、非ブロードキャスト インターフェイスで 30 秒です。
mtu-ignore	DBD パケットを受信した場合の OSPF MTU 不一致検出をディセーブルにします。OSPF MTU 不一致検出は、デフォルトでイネーブルになっています。
neighbor	非ブロードキャスト ネットワークへの OSPFv3 ルータの相互接続を設定します。
network	ネットワーク タイプに依存するデフォルト以外のタイプに OSPF ネットワーク タイプを設定します。
priority	ルータ プライオリティを設定します。これは、ネットワークにおける指定ルータの特定に役立ちます。有効値の範囲は 0 ～ 255 です。
process-id	イネーブルにする OSPFv3 プロセスを指定します。有効値の範囲は 1 ～ 65535 です。
retransmit-interval *seconds*	インターフェイスに属する隣接関係の LSA 再送信間の時間を秒単位で指定します。接続ネットワーク上の任意の 2 台のルータ間で想定される往復遅延より大きな値にする必要があります。有効値の範囲は、1 ～ 65535 秒です。デフォルトは 5 秒です。
transmit-delay *seconds*	インターフェイス上でリンクステート更新パケットを送信する時間を秒単位で設定します。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 1 秒です。

デフォルト

デフォルトではすべての IPv6 アドレスが含まれます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

OSPFv3 エリアを作成する前に OSPFv3 ルーティング プロセスをイネーブルにする必要があります。

例

次に、OSPFv3 インターフェイスのコンフィギュレーションをイネーブルにする例を示します。

```
ciscoasa(config)# ipv6 ospf 3
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。
debug ospfv3	OSPFv3 ルーティング プロセスのトラブルシューティング用のデバッグ情報を表示します。

ipv6 ospf area

IPv6 の OSPFv3 エリアを作成するには、グローバル コンフィギュレーション モードで **ipv6 ospf area** コマンドを使用します。IPv6 の OSPFv3 エリアのコンフィギュレーションをディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 ospf area [*area-num*] [**instance**]

no ipv6 ospf area [*area-num*] [**instance**]

構文の説明

area-num	イネーブルにする OSPFv3 エリアを指定します。
instance	インターフェイスに割り当てるエリア インスタンス ID を指定します。

デフォルト

デフォルトではすべての IPv6 アドレスが含まれます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

OSPFv3 ルーティングは、それぞれのインターフェイスについて個別に設定する必要があります。OSPFv3 エリアは各インターフェイスに 1 つだけ設定することができ、ASA の OSPFv3 でサポートされるインスタンスはインターフェイスごとに 1 つだけです。使用されるエリア インスタンス ID はインターフェイスごとに異なります。エリア インスタンス ID は、OSPF パケットの受信にのみ影響し、OSPF の通常のインターフェイスと仮想リンクに適用されます。

例

次に、OSPFv3 インターフェイスのコンフィギュレーションをイネーブルにする例を示します。

```
ciscoasa(config)# ipv6 ospf 3 area 2
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。
debug ospfv3	OSPFv3 ルーティング プロセスのトラブルシューティング用のデバッグ情報を表示します。

ipv6 ospf cost

インターフェイスでパケットを送信するコストを明示的に指定するには、インターフェイス コンフィギュレーション モードで **ipv6 ospf cost** コマンドを使用します。インターフェイスでパケットを送信するコスト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。

ipv6 ospf cost *interface-cost*

no ipv6 ospf cost *interface-cost*

構文の説明

interface-cost	リンクステート メトリックとして表される符号なし整数値を指定します。値の範囲は、1 ～ 65535 です。

デフォルト

デフォルトのコストは帯域幅に基づきます。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン　このコマンドは、インターフェイスのパケット コストを明示的に指定する場合に使用します。

例　次に、パケット コストを 65 に設定する例を示します。

```
ciscoasa(config-if)# ipv6 ospf cost 65
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。
debug ospfv3	OSPFv3 ルーティング プロセスのトラブルシューティング用のデバッグ情報を表示します。

ipv6 ospf database-filter all out

OSPFv3 インターフェイスへの発信 LSA をフィルタリングするには、インターフェイス コンフィギュレーション モードで **ipv6 ospf databse-filter all out** コマンドを使用します。インターフェイスに対する LSA の転送を元に戻すには、このコマンドの **no** 形式を使用します。

ipv6 ospf database-filter all out

no ipv6 ospf database-filter all out

構文の説明　このコマンドには引数またはキーワードはありません。

デフォルト　すべての発信 LSA がインターフェイスにフラッディングされます。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン　このコマンドは、OSPFv3 インターフェイスへの発信 LSA をフィルタリングする場合に使用します。

例　次に、指定したインターフェイスへの発信 LSA をフィルタリングする例を示します。

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf database-filter all out
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。
debug ospfv3	OSPFv3 ルーティング プロセスのトラブルシューティング用のデバッグ情報を表示します。

ipv6 ospf dead-interval

hello パケットを確認できないときにネイバーがルータのダウンを宣言するまでの時間を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 ospf dead-interval** コマンドを使用します。デフォルト時間に戻すには、このコマンドの **no** 形式を使用します。

ipv6 ospf dead-interval *seconds*

no ipv6 ospf dead-interval *seconds*

構文の説明

seconds	間隔を秒単位で指定します。この値はネットワーク上のすべてのノードで同じにする必要があります。有効値の範囲は 1 ～ 65535 です。

デフォルト　デフォルト値は、**ipv6 ospf hello-interval** コマンドで設定された間隔の 4 倍です。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン　このコマンドは、hello パケットを確認できないときにネイバーがルータのダウンを通知するまでの時間を設定する場合に使用します。

例　次に、デッド間隔を 60 に設定する例を示します。

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf dead-interval 60
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。
debug ospfv3	OSPFv3 ルーティング プロセスのトラブルシューティング用のデバッグ情報を表示します。

ipv6 ospf encryption

インターフェイスの暗号化タイプを指定するには、インターフェイス コンフィギュレーション モードで **ipv6 ospf encryption** コマンドを使用します。インターフェイスの暗号化タイプを削除するには、このコマンドの **no** 形式を使用します。

ipv6 ospf encryption {**ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key* | **null**}

no ipv6 ospf encryption {**ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key* | **null**}

構文の説明

authentication-algorithm	使用する暗号化アルゴリズムを指定します。有効な値は次のいずれかです。 • **md5**：Message Digest 5（MD5）をイネーブルにします。 • **sha1**：SHA-1 をイネーブルにします。
encryption-algorithm	ESP で使用する暗号化アルゴリズムを指定します。有効な値は次のとおりです。 • **aes-cdc**：AES-CDC 暗号化をイネーブルにします。 • **3des**：トリプル DES 暗号化をイネーブルにします。 • **des**：DES 暗号化をイネーブルにします。 • **null**：暗号化なしの ESP を指定します。
esp	カプセル化セキュリティ ペイロード（ESP）を指定します。
ipsec	IP セキュリティ プロトコルを指定します。
key	メッセージ ダイジェストの計算で使用される番号を指定します。MD5 認証を使用する場合、キーの長さは 32 桁の 16 進数（16 バイト）である必要があります。SHA-1 認証を使用する場合、キーの長さは 40 桁の 16 進数（20 バイト）である必要があります。
key-encryption-type	（オプション）キー暗号化タイプを指定します。次のいずれかの値を指定できます。 • **0**：キーは暗号化されません。 • **7**：キーは暗号化されます。
null	この設定をエリア認証よりも優先します。
spi *spi*	セキュリティ ポリシー インデックス（SPI）の値を指定します。*spi* の有効な値の範囲は 256 ～ 42949667295 で、10 進数で入力する必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、インターフェイスの暗号化タイプを指定する場合に使用します。

例

次に、インターフェイスで SHA-1 暗号化をイネーブルにする例を示します。

```
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf encryption ipsec spi 1001 esp null sha1
123456789A123456789B123456789C123456789D
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。
debug ospfv3	OSPFv3 ルーティング プロセスのトラブルシューティング用のデバッグ情報を表示します。

ipv6 ospf flood-reduction

インターフェイスへの LSA のフラッディング削減を指定するには、インターフェイス コンフィギュレーション モードで **ipv6 ospf flood-reduction** コマンドを使用します。インターフェイスへの LSA のフラッディング削減を削除するには、このコマンドの **no** 形式を使用します。

ipv6 ospf flood-reduction

no ipv6 ospf flood-reduction

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、インターフェイスへの LSA のフラッディング削減を指定する場合に使用します。

例

次に、インターフェイスへの LSA のフラッディング削減をイネーブルにする例を示します。

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 20.20.200.30 255.255.255.0 standby 20.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf flood reduction
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。
debug ospfv3	OSPFv3 ルーティング プロセスのトラブルシューティング用のデバッグ情報を表示します。

ipv6 ospf hello-interval

hello パケットを確認できないときにネイバーがルータのダウンを宣言するまでの時間を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 ospf dead-interval** コマンドを使用します。デフォルト時間に戻すには、このコマンドの **no** 形式を使用します。

ipv6 ospf dead-interval *seconds*

no ipv6 ospf dead-interval *seconds*

構文の説明

seconds	間隔を秒単位で指定します。この値はネットワーク上のすべてのノードで同じにする必要があります。有効値の範囲は 1 ～ 65535 です。

デフォルト

デフォルトの間隔は、イーサネットを使用する場合は 10 秒、非ブロードキャストを使用する場合は 30 秒です。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン　このコマンドは、hello パケットを確認できないときにネイバーがルータのダウンを通知するまでの時間を設定する場合に使用します。

例　次に、デッド間隔を 60 に設定する例を示します。

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf dead-interval 60
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。
debug ospfv3	OSPFv3 ルーティング プロセスのトラブルシューティング用のデバッグ情報を表示します。

ipv6 ospf mtu-ignore

ASA でデータベース記述子（DBD）パケットを受信した際の OSPFv3 最大伝送単位（MTU）不一致検出をディセーブルにするには、インターフェイス コンフィギュレーション モードで **ipv6 ospf mtu-ignore** コマンドを使用します。ASA で DBD パケットを受信した際の MTU 不一致検出をデフォルトの設定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。

ipv6 ospf mtu-ignore

no ipv6 ospf mtu-ignore

構文の説明　このコマンドには引数またはキーワードはありません。

デフォルト

OSPFv3 MTU 不一致検出は、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、ASA で DBD パケットを受信した際の OSPFv3 MTU 不一致検出をディセーブルにする場合に使用します。

例

次に、ASA で DBD パケットを受信した際の OSPFv3 MTU 不一致検出をディセーブルにする例を示します。

```
ciscoasa(config)# interface serial 0/0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf mtu-ignore
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。
debug ospfv3	OSPFv3 ルーティング プロセスのトラブルシューティング用のデバッグ情報を表示します。

ipv6 ospf neighbor

非ブロードキャスト ネットワークへの OSPFv3 ルータの相互接続を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 ospf neighbor** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter**]

no ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter**]

構文の説明

cost *number*	(オプション)ネイバーに 1 ～ 65535 の整数を使用したコストを割り当てます。コストが具体的に設定されていないネイバーについては、インターフェイスのコストは **ipv6 ospf cost** コマンドに基づいて想定されます。
database-filter	(任意)OSPF ネイバーに送出されるリンクステート アドバタイズメント(LSA)をフィルタリングします。
ipv6-address	ネイバーのリンクローカル IPv6 アドレス。この引数は、RFC 2373 に記述されている形式である必要があります。RFC 2373 では、コロンで区切った 16 ビット値を使用して 16 進数形式でアドレスを指定します。
poll-interval *seconds*	(オプション)ポーリングの時間間隔(秒)を表す数値。RFC 2328 では、この値を hello interval よりずっと大きくすることが推奨されています。デフォルトは 120 秒(2 分)です。このキーワードはポイントツーマルチポイント インターフェイスには適用されません。
priority *number*	(オプション)指定の IPv6 プレフィックスが関連付けられている非ブロードキャスト ネイバーのルータ プライオリティ値を示す数。デフォルトは 0 です。

デフォルト

デフォルトはネットワーク タイプによって異なります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、非ブロードキャスト ネットワークへの OSPFv3 ルータの相互接続を設定する場合に使用します。

例

次に、OSPFv3 ネイバー ルータを設定する例を示します。

```
ciscoasa(config)# interface serial 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf 1 area 0
ciscoasa(config-if)# ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。
ipv6 ospf priority	指定したネットワークにおける指定ルータのプライオリティを指定します。

ipv6 ospf network

OSPFv3 ネットワーク タイプをデフォルト以外のタイプに設定するには、インターフェイス コンフィギュレーション モードで **ipv6 ospf network** コマンドを使用します。デフォルトのタイプに戻すには、このコマンドの **no** 形式を使用します。

ipv6 ospf network {**broadcast** | **point-to-point non-broadcast**}

no ipv6 ospf network {**broadcast** | **point-to-point non-broadcast**}

構文の説明

broadcast	ネットワーク タイプをブロードキャストに設定します。
point-to-point non-broadcast	ネットワーク タイプをポイントツーポイントの非ブロードキャストに設定します。

デフォルト

デフォルトはネットワーク タイプによって異なります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、OSPFv3 ネットワーク タイプをデフォルト以外のタイプに設定する場合に使用します。

例

次に、OSPFv3 ネットワークをブロードキャスト ネットワークに設定する例を示します。

```
ciscoasa(config)# interface serial 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf 1 area 0
ciscoasa(config-if)# ipv6 ospf network broadcast
ciscoasa(config-if)# encapsulation frame-relay
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。
ipv6 ospf priority	指定したネットワークにおける指定ルータのプライオリティを指定します。

ipv6 ospf priority

指定したネットワークにおいて指定ルータを特定するためのルータのプライオリティを設定するには、インターフェイス コンフィギュレーション モードで **ipv6 ospf priority** 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 ospf priority *number-value*

no ipv6 ospf priority *number-value*

構文の説明

number-value	ルータのプライオリティを指定する数値を設定します。有効値の範囲は 0 ～ 255 です。

デフォルト

デフォルトのプライオリティは 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン　このコマンドは、ルータのプライオリティを設定する場合に使用します。

例　次に、ルータのプライオリティを 4 に設定する例を示します。

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config-if)# ipv6 ospf priority 4
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。
ipv6 ospf retransmit-interval	インターフェイスに属する隣接関係の LSA 再送信の間隔を指定します。

ipv6 ospf retransmit-interval

インターフェイスに属する隣接関係の LSA 再送信の間隔を指定するには、インターフェイス コンフィギュレーション モードで **ipv6 ospf retransmit-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 ospf retransmit-interval *seconds*

no ipv6 ospf retransmit-interval *seconds*

構文の説明

seconds	再送信の間隔（秒数）を指定します。接続ネットワーク上の任意の 2 台のルータ間で想定される往復遅延より大きな値にする必要があります。有効値の範囲は、1 ～ 65535 秒です。

デフォルト　デフォルトは 5 秒です。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、インターフェイスに属する隣接関係の LSA 再送信の間隔を指定する場合に使用します。

例

次に、再送信間隔を 8 秒に設定する例を示します。

```
ciscoasa(config)# interface ethernet 2
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf retransmit-interval 8
```

関連コマンド

コマンド	説明
ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。
ipv6 ospf priority	指定したネットワークにおける指定ルータのプライオリティを指定します。

ipv6 ospf transmit-delay

インターフェイスでリンクステート更新パケットを送信するために必要とされる時間を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 ospf transmit-delay** 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 ospf transmit-delay *seconds*

no ipv6 ospf transmit-delay *seconds*

構文の説明

seconds	リンクステートの更新を送信するために必要な時間（秒数）を指定します。有効値の範囲は、1 ～ 65535 秒です。

デフォルト

デフォルト値は 1 秒です。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	• Yes	—	• Yes	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン　このコマンドは、インターフェイスでリンクステート更新パケットを送信するために必要とされる時間を設定する場合に使用します。

例　次に、転送遅延を 3 秒に設定する例を示します。

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf transmit-delay 3
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。
ipv6 ospf priority	指定したネットワークにおける指定ルータのプライオリティを指定します。

ipv6 prefix-list

IPv6 プレフィックス リストのエントリを作成するには、グローバル コンフィギュレーション モードで **ipv6 prefix-list** コマンドを使用します。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 prefix-list *list-name* [**seq** *seq-number*]
{**deny** *ipv6-prefix/prefix-length* | **permit** *ipv6-prefix/prefix-length* | **description** *text*} [**ge** *ge-value*] [**le** *le-value*]

no ipv6 prefix-list *list-name*

構文の説明

list-name	プレフィックス リストの名前。 既存のアクセス リストと同じ名前にすることはできません。 (注) 「detail」または「summary」はキーワードであるため、名前に使用できません。
seq *seq-number*	(オプション)設定するプレフィックス リスト エントリのシーケンス番号。
deny	条件に一致するネットワークを拒否します。
permit	条件に一致するネットワークを許可します。
ipv6-prefix	指定したプレフィックス リストに割り当てられている IPv6 ネットワーク。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
prefix-length	IPv6 プレフィックスの長さ。この値は、アドレスの高次の連続ビットのうち、プレフィックスのネットワーク部分を構成しているビットの数を示します。プレフィックス長の前にスラッシュ(/)を使用する必要があります。
description *text*	プレフィックス リストの説明。最大 80 文字です。
ge *ge-value*	(オプション)*ipv6-prefix/prefix-length* 引数の値と等しいかそれよりも長いプレフィックス長を指定します。これは length の範囲の最小値です(長さの範囲の「から」の部分)。
le *le-value*	(オプション)*ipv6-prefix* と等しいかそれよりも短いプレフィックス長を指定します。*/prefix-length* 引数。これは length の範囲の最大値です(長さの範囲の「まで」の部分)。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

関連コマンド

コマンド	説明
show ipv6 prefix-list	IPv6 プレフィックス リストを表示します。
show ipv6 route	IPv6 ルーティング テーブルの現在の内容を表示します。

ipv6 route

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

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

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

構文の説明

administrative-distance	(任意)ルートのアドミニストレーティブ ディスタンス。デフォルト値は 1 です。この場合、スタティック ルートは接続ルートを除く他のどのタイプのルートよりも優先されます。
if_name	ルートを設定するインターフェイスの名前。
ipv6-address	指定したネットワークに到達するために使用可能なネクスト ホップの IPv6 アドレス。
ipv6-prefix	スタティック ルートの宛先となる IPv6 ネットワーク。 この引数は、RFC 2373 に記述されている形式である必要があります。RFC 2373 では、コロンで区切った 16 ビット値を使用して 16 進数形式でアドレスを指定します。
prefix-length	IPv6 プレフィックスの長さ。この値は、アドレスの高次の連続ビットのうち、プレフィックスのネットワーク部分を構成しているビットの数を示します。プレフィックス長の前にスラッシュ(/)を使用する必要があります。
tunneled	(オプション)ルートを VPN トラフィックのデフォルト トンネル ゲートウェイとして指定します。

デフォルト

デフォルトでは、アドミニストレーティブ ディスタンスは 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(1)	トランスペアレント ファイアウォール モードのサポートが追加されました。

使用上のガイドライン

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

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

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

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

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

例

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

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

関連コマンド

コマンド	説明
debug ipv6 route	IPv6 ルーティング テーブルの更新およびルート キャッシュの更新に関するデバッグ メッセージを表示します。
show ipv6 route	IPv6 ルーティング テーブルの現在の内容を表示します。

ipv6 router ospf

OSPFv3 ルーティング プロセスを作成し、IPv6 ルータ コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **ipv6 router ospf** コマンドを使用します。

ipv6 router ospf *process-id*

構文の説明

process-id	ローカルに割り当てられる内部 ID を指定します。有効な値は 1 ～ 65535 の正の整数です。この番号は、IPv6 の OSPFv3 ルーティング プロセスをイネーブルにしたときに管理目的で割り当てられます。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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		
				マルチ	
	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	• Yes	—	• Yes	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン　**ipv6 router ospf** コマンドは、ASA で実行される OSPFv3 ルーティング プロセスのグローバル コンフィギュレーション コマンドです。**ipv6 router ospf** コマンドを入力すると、IPv6 ルータ コンフィギュレーション モードであることを示す (config-rtr)# コマンド プロンプトが表示されます。

no ipv6 router ospf コマンドを使用する場合は、必要な情報を指定する場合を除き、オプションの引数を指定する必要はありません。**no ipv6 router ospf** コマンドは、*process-id* 引数によって指定された OSPFv3 ルーティング プロセスを終了します。*process-id* の値は、ASA においてローカルに割り当てます。OSPFv3 ルーティング プロセスごとに固有の値を割り当てる必要があります。最大 2 つのプロセスが使用できます。

IPv6 ルータ コンフィギュレーション モードの **ipv6 router ospf** コマンドでは、OSPFv3 固有の次のオプションを使用して OSPFv3 ルーティング プロセスを設定できます。

- **area**：OSPFv3 エリア パラメータを設定します。サポートされているパラメータには、0 ～ 4294967295 の 10 進数値のエリア ID、**A.B.C.D** の IP アドレス形式のエリア ID などがあります。
- **default**：コマンドをデフォルト値に設定します。**originate** パラメータはデフォルト ルートを配布します。
- **default-information**：デフォルト情報の配布を制御します。
- **distance**：ルート タイプに基づいて、OSPFv3 ルート アドミニストレーティブ ディスタンスを定義します。サポートされるパラメータには、1 ～ 254 の値のアドミニストレーティブ ディスタンス、OSPF ディスタンスの **ospf** などがあります。
- **exit**：IPv6 ルータ コンフィギュレーション モードを終了します。
- **ignore**：ルータがタイプ 6 Multicast OSPF（MOSPF）パケットのリンクステート アドバタイズメント（LSA）を受信した場合に、**lsa** パラメータが指定されている syslog メッセージの送信を抑止します。
- **log-adjacency-changes**：OSPFv3 ネイバーが起動または停止したときに、ルータが syslog メッセージを送信するように設定します。**detail** パラメータによって、すべての状態変更がログに記録されます。

- **passive-interface**：次のパラメータを使用してインターフェイスでのルーティング更新を抑制します。
  - **GigabitEthernet**：GigabitEthernet IEEE 802.3z インターフェイスを指定します。
  - **Management**：管理インターフェイスを指定します。
  - **Port-channel**：インターフェイスのイーサネット チャネルを指定します。
  - **Redundant**：冗長インターフェイスを指定します。
  - **default**：すべてのインターフェイス上でルーティングが更新されないようにします。
- **redistribute**：次のパラメータに従って、ルーティング ドメイン間でのルートの再配布を設定します。
  - **connected**：接続ルートを指定します。
  - **ospf**：OSPF ルートを指定します。
  - **static**：スタティック ルートを指定します。
- **router-id**：次のパラメータを使用して、指定されたプロセスの固定ルータ ID を作成します。
  - **A.B.C.D**：IP アドレス形式の OSPF ルータ ID を指定します。
  - **cluster-pool**：レイヤ 3 クラスタリングが設定されている場合に、IP アドレス プールを設定します。
- **summary-prefix**：0 ～ 128 の有効な値で IPv6 アドレス サマリーを設定します。**X:X:X:X::X/** パラメータは、IPv6 プレフィックスを指定します。
- **timers**：次のパラメータを使用して、ルーティング タイマーを調整します。
  - **lsa**：OSPF LSA タイマーを指定します。
  - **pacing**：OSPF ペーシング タイマーを指定します。
  - **throttle**：OSPF スロットル タイマーを指定します。

例

次に、OSPFv3 ルーティング プロセスをイネーブルにし、IPv6 ルータ コンフィギュレーション モードを開始する例を示します。

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)#
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。
debug ospfv3	OSPFv3 ルーティング プロセスのトラブルシューティング用のデバッグ情報を表示します。

ipv6-split-tunnel-policy

IPv6 スプリット トンネリング ポリシーを設定するには、グループ ポリシー コンフィギュレーション モードで **ipv6-split-tunnel-policy** コマンドを使用します。実行コンフィギュレーションから ipv6-split-tunnel-policy 属性を削除するには、このコマンドの **no** 形式を使用します。

ipv6-split-tunnel-policy {**tunnelall** | **tunnelspecified** | **excludespecified**}

no ipv6-split-tunnel-policy

構文の説明

excludespecified	トラフィックを暗号化しないで送信する先となるネットワークのリストを定義します。この機能は、社内ネットワークにトンネルを介して接続しながら、ローカル ネットワーク上のデバイス（プリンタなど）にアクセスするリモート ユーザにとって役立ちます。
ipv6-split-tunnel-policy	トラフィックのトンネリングのルールを設定することを指定します。
tunnelall	トラフィックを暗号化しないで送信しないこと、または ASA 以外の宛先に送信しないことを指定します。リモート ユーザは企業ネットワークを経由してインターネットにアクセスしますが、ローカル ネットワークにはアクセスできません。
tunnelspecified	指定したネットワークから、または指定したネットワークへのすべてのトラフィックをトンネリングします。このオプションによって、スプリット トンネリングが有効になります。トンネリングするアドレスのネットワーク リストを作成できるようになります。その他のすべてのアドレスへのデータは暗号化しないで送信され、リモート ユーザのインターネット サービス プロバイダーによってルーティングされます。

デフォルト

IPv6 スプリット トンネリングは、デフォルトではディセーブル（**tunnelall**）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

IPv6 スプリット トンネリングは、本来は、セキュリティ機能ではなくトラフィック管理機能です。最適なセキュリティを確保するには、IPv6 スプリット トンネリングをイネーブルにしないことを推奨します。

これにより、別のグループ ポリシーから IPv6 スプリット トンネリングの値を継承できます。

IPv6 スプリット トンネリングを使用すると、リモートアクセス VPN クライアントは、条件に応じて、パケットを IPsec または SSL IPv6 トンネルを介して暗号化された形式で送信したり、クリア テキスト形式でネットワーク インターフェイスに送信したりできます。IPv6 スプリット トンネリングをイネーブルにすると、宛先が IPsec または SSL VPN トンネル エンドポイントの反対側ではないパケットでは、暗号化、トンネルを介した送信、復号化、および最終的な宛先へのルーティングは必要なくなります。

このコマンドでは、IPv6 スプリット トンネリング ポリシーが特定のネットワークに適用されます。

例

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

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ipv6-split-tunnel-policy tunnelspecified
```

関連コマンド

コマンド	説明
split-tunnel-network-list none	スプリット トンネリングのアクセス リストがないことを指定します。トラフィックはすべてトンネルを通過します。
split-tunnel-network-list value	トンネリングが必要なネットワークと不要なネットワークを区別するために、ASA が使用するアクセス リストを指定します。

ipv6-vpn-address-assign

IPv6 アドレスをリモート アクセス クライアントに割り当てる方法を指定するには、グローバル コンフィギュレーション モードで **ipv6-vpn-addr-assign** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** バージョンを使用します。設定されている VPN アドレスの割り当て方法を ASA からすべて削除するには、引数なしで、このコマンドの **no** 形式を使用します。

ipv6-vpn-addr-assign {**aaa** | **local** }

no ipv6-vpn-addr-assign {**aaa** | **local** }

構文の説明

aaa	外部または内部（LOCAL）の AAA（認証、認可、アカウンティング）サーバからユーザ単位でアドレスを取得します。IP アドレスが設定された認証サーバを使用している場合は、この方式を使用することをお勧めします。
local	ASA の内部で設定されているアドレス プールから IPv6 アドレスを配布します。

デフォルト

デフォルトでは、AAA とローカルの両方の VPN アドレス割り当てオプションがイネーブルになります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。
9.5(2)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

ASA では、AAA またはローカルのいずれかの方法でリモート アクセス クライアントに IPv6 アドレスを割り当てることができます。複数のアドレス割り当て方法を設定すると、ASA は IPv6 アドレスが見つかるまで各オプションを検索します。

例

次に、アドレス割り当て方法として AAA を設定する例を示します。

例:

```
ciscoasa(config)# ipv6-vpn-addr-assign aaa
```

次に、アドレス割り当て方法としてローカル アドレス プールを使用するように設定する例を示します。

例:

```
ciscoasa(config)# no ipv6-vpn-addr-assign local
```

関連コマンド

コマンド	説明
ipv6 local pool	VPN グループ ポリシーに使用される IPv6 アドレス プールを設定します。
show running-config group-policy	すべてのグループ ポリシーまたは特定のグループ ポリシーのコンフィギュレーションを表示します。
vpn-addr-assign	リモート アクセス クライアントに IPv4 アドレスを割り当てる方法を指定します。

ipv6-vpn-filter

VPN 接続に使用する IPv6 ACL の名前を指定するには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **ipv6-vpn-filter** コマンドを使用します。**ipv6-vpn-filter none** コマンドの発行によって作成されるヌル値を含め、ACL を削除するには、このコマンドの **no** 形式を使用します。

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

no ipv6-vpn-filter

構文の説明

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

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	**ipv6-vpn-filter** コマンドは廃止されました。IPv4 と IPv6 のエントリに対応した統合フィルタを設定するには、**vpn-filter** コマンドを使用してください。この IPv6 フィルタは、**vpn-filter** コマンドによって指定されたアクセス リストに IPv6 エントリがない場合にのみ使用されます。
9.1(4)	**ipv6-vpn-filter** コマンドはディセーブルになっており、「no」形式のみを使用できます。IPv4 と IPv6 のエントリに対応した統合フィルタを設定するには、**vpn-filter** コマンドを使用してください。このコマンドを誤って使用して IPv6 ACL を指定した場合、接続は終了します。

使用上のガイドライン

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

no オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。値の継承を防止するには、**ipv6-vpn-filter none** コマンドを使用します。

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

例

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

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

関連コマンド

コマンド	説明
access-list	アクセス リストを作成するか、ダウンロード可能なアクセス リストを使用します。
vpn-filter	VPN 接続に使用する IPv4 または IPv6 の ACL の名前を指定します。

ip verify reverse-path

ユニキャスト RPF をイネーブルにするには、グローバル コンフィギュレーション モードで **ip verify reverse-path** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip verify reverse-path interface *interface_name*

no ip verify reverse-path interface *interface_name*

構文の説明

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

デフォルト

この機能はデフォルトで無効に設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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

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

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

ルーティング テーブルにあるアドレスから外部インターフェイスにトラフィックが入り、このアドレスが内部インターフェイスに関連付けられている場合、ASA はパケットをドロップします。同様に、未知の送信元アドレスから内部インターフェイスにトラフィックが入った場合は、一致するルート（デフォルト ルート）が外部インターフェイスを示しているため、ASA はパケットをドロップします。

Unicast RPF は、次のように実装されます。

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

例

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

```
ciscoasa(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** コマンドを使用して設定されたコンフィギュレーションをクリアします。
clear ip verify statistics	ユニキャスト RPF の統計情報をクリアします。
show ip verify statistics	ユニキャスト RPF 統計情報を表示します。
show running-config ip verify reverse-path	**ip verify reverse-path** コマンドを使用して設定されたコンフィギュレーションを表示します。