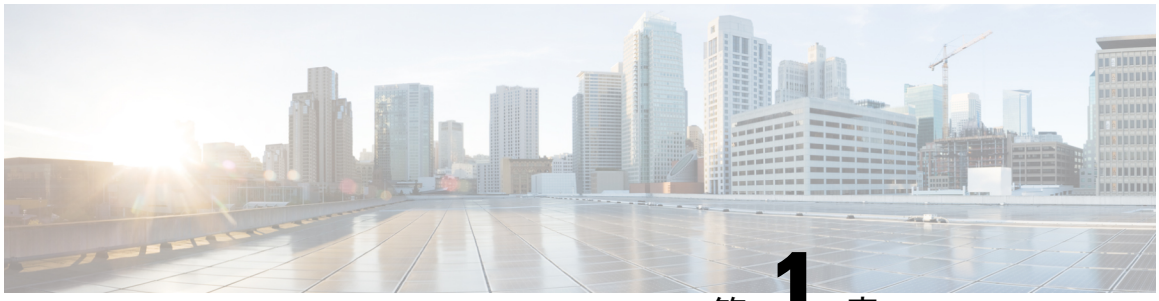
Cisco IOS リリース 15.2(8)E（Catalyst マイクロスイッチ シリーズ）IPv6 コンフィギュレーション ガイド

初版：2021 年 4 月 26 日

最終更新：2021 年 12 月 21 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次



第 1 章

IPv6 ネットワークの管理

HTTP（S）の IPv6 サポート

この機能は、HTTP（S）クライアントとサーバで IPv6 アドレスをサポートするようにします。

Cisco ソフトウェアの HTTP サーバは、IPv6 と IPv4 の両方の HTTP クライアントからの要求を処理できます。HTTP（S）サーバがクライアントからの接続を受け入れると、サーバはそのクライアントが IPv4 であるか IPv6 ホストであるかを決定します。それに応じて、ソケット コールを受け入れる IPv4 または IPv6 のアドレス ファミリが選択されます。リスニング ソケットは、IPv4 と IPv6 の両方の接続を待ち受け続けます。

Cisco ソフトウェアの HTTP クライアントは、IPv4 と IPv6 の両 HTTP サーバへの要求を送信できます。

IPv6 HTTP クライアントを使用すると、実際の IPv6 アドレスの URL は、RFC 2732 のルールを使用してフォーマットする必要があります。

IPv6 デバイスへの HTTP アクセスのディセーブル化

HTTP サーバをイネーブルにし、デバイスに IPv6 アドレスが設定されている場合、IPv6 を介した HTTP アクセスは自動的にイネーブルになります。HTTP サーバが必要でない場合は、ディセーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。

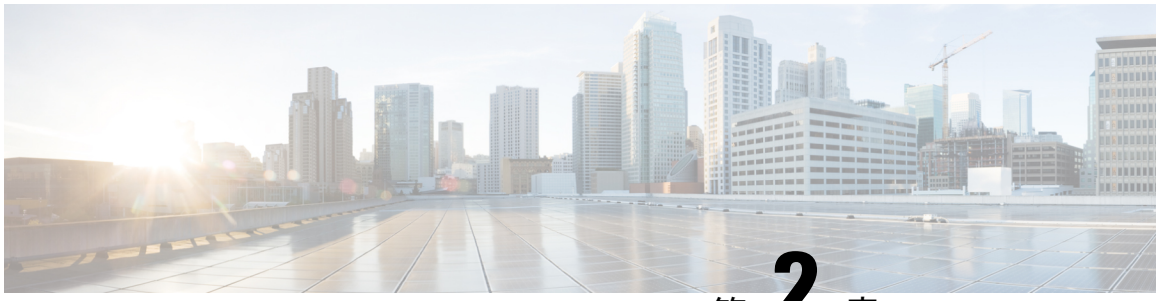
	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no ip http server** 例： `Device(config)# no ip http server`	HTTP アクセスをディセーブルにします。

例：デバイスへの HTTP アクセスのディセーブル化

次の例では、**show running-config** コマンドを使用すると、デバイスで HTTP アクセスがディセーブルになっていることが示されています。

```
Device# show running-config

Building configuration...
!
Current configuration : 1490 bytes
!
version 12.2
!
hostname Device
!
no ip http server
!
line con 0
line aux 0
line vty 0 4
```



第 2 章

IPv6 ACL の設定

IPv6 ACL の設定に関する情報

IP バージョン 6（IPv6）アクセス コントロール リスト（ACL）を作成し、それをインターフェイスに適用することによって、IPv6 トラフィックをフィルタリングできます。これは、IP バージョン 4（IPv4）の名前付き ACL を作成し、適用する方法と同じです。

IPv6 ACL の概要

スイッチイメージは、次のタイプの IPv6 ACL をサポートします。

- IPv6 ポート ACL：レイヤ 2 インターフェイスの着信トラフィックでだけサポートされます。インターフェイスに届くすべての IPv6 パケットに適用されます。

（注） サポートされない IPv6 ACL を設定した場合、エラー メッセージが表示され、その設定は有効になりません。

スイッチは、IPv6 トラフィックの Virtual LAN（VLAN）ACL（VLAN マップ）をサポートしません。

1 つのインターフェイスに、IPv4 ACL および IPv6 ACL の両方を適用できます。

サポートされる ACL 機能

スイッチの IPv6 ACL には、次の特性があります。

- 分割フレーム（IPv4 では fragments キーワード）がサポートされます。
- IPv6 ACL では、IPv4 と同じ統計情報がサポートされます。

- スイッチの Ternary CAM（TCAM）スペースが不足している場合、ACL ラベルに対応付けられたパケットは CPU に転送され、ACL はソフトウェアで適用されます。

IPv6 ACL の制限事項

IPv4 では、番号制の標準 IP ACL および拡張 IP ACL、名前付き IP ACL、および MAC ACL を設定できます。IPv6 がサポートするのは名前付き ACL だけです。

スイッチは Cisco IOS がサポートする IPv6 ACL の大部分をサポートしますが、一部例外もあります。

- スイッチは、**flowlabel**、**routing header**、および **undetermined-transport** というキーワードの照合をサポートしません。
- スイッチは再起 ACL（**reflect** キーワード）をサポートしません。
- このリリースが IPv6 用にサポートしているのは、ポート ACL だけです。IPv6 用のルータ ACL および VLAN ACL（VLAN マップ）はサポートしていません。
- スイッチは IPv6 フレームに MAC ベース ACL を適用しません。
- レイヤ 2 EtherChannel に IPv6 ポート ACL を適用できません。
- スイッチは出力ポート ACL をサポートしません。
- ACL を設定する場合、ACL に入力されるキーワードには、それがプラットフォームでサポートされるかどうかにかかわらず、制限事項はありません。ハードウェア転送が必要なインターフェイス（物理ポート）に ACL を適用する場合、スイッチはインターフェイスで ACL がサポートされるかどうか判別します。サポートされない場合、ACL の付加は拒否されます。
- インターフェイスに適用される ACL に、サポートされないキーワードを持つアクセス コントロールエントリ（ACE）を追加しようとする場合、スイッチは現在インターフェイスに適用されている ACL に ACE が追加されるのを許可しません。

IPv6 ACL の設定

IPv6 トラフィックをフィルタリングする場合は、次の手順を実行します。

手順

ステップ 1 IPv6 ACL を作成し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。

ステップ 2 IPv6 ACL が、トラフィックをブロックする（deny）または通過させる（permit）よう設定します。

ステップ 3 インターフェイスに IPv6 ACL を適用します。

IPv6 ACL のデフォルト設定

デフォルトでは、IPv6 ACL は設定または適用されていません。

他の機能およびスイッチとの相互作用

- ブリッジド フレームがポート ACL によってドロップされる場合、このフレームはブリッジングされません。
- IPv4 ACL および IPv6 ACL の両方を 1 つのスイッチに作成したり、同一インターフェイスに適用できます。各 ACL には一意の名前が必要です。設定済みの名前を使用しようとすると、エラー メッセージが表示されます。

  IPv4 ACL と IPv6 ACL の作成、および同一のレイヤ 2 インターフェイス インターフェイスへの IPv4 ACL または IPv6 ACL の適用には、異なるコマンドを使用します。ACL を付加するのに誤ったコマンドを使用すると（例えば、IPv6 ACL の付加に IPv4 コマンドを使用するなど）、エラー メッセージが表示されます。
- MAC ACL を使用して、IPv6 フレームをフィルタリングできません。MAC ACL は非 IP フレームだけをフィルタリングできます。
- ハードウェアメモリが満杯の場合、設定済みの ACL を追加すると、パケットは CPU に転送され、ACL はソフトウェアで適用されます。ハードウェアが一杯になると、ACL がアンロードされたことを示すメッセージがコンソールに出力され、パケットはソフトウェアで処理されます。

  注 追加できなかった ACL と同じタイプのパケットのみ（ipv4、ipv6、MAC）がソフトウェアで処理されます。
- TCAM が満杯の場合、設定済みの ACL を追加すると、パケットは CPU に転送され、ACL はソフトウェアで適用されます。

IPv6 ACL の作成

IPv6 ACL を作成するには、次の手順に従ってください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6access-list***access-list-name* 例： `ipv6 access-list access-list-name`	IPv6 アクセス リスト名を定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ステップ 4	**{deny|permit} protocol** 例： `{deny | permit} protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length | any |host destination-ipv6-address} [operator [port-number]][dscp value] [fragments][log] [log-input] [routing][sequence value] [time-range name]`	条件が一致した場合にパケットを拒否する場合は deny、許可する場合は permit を指定します。次に、条件について説明します。 • protocol には、インターネット プロトコルの名前または番号を入力します。ahp、esp、icmp、ipv6、pcp、stcp、tcp、udp、または IPv6 プロトコル番号を表す 0 ～ 255 の整数を使用できます。 • source-ipv6-prefix/prefix-length または destination-ipv6-prefix/ prefix-length は、拒否条件または許可条件を設定する送信元または宛先 IPv6 ネットワークあるいはネットワーク クラスで、コロン区切りの 16 ビット値を使用した 16 進形式で指定します（RFC 2373 を参照）。 • IPv6 プレフィックス ::/0 の短縮形として、any を入力します。 • host source-ipv6-address または destination-ipv6-address には、拒否条件または許可条件を設定する送信元または宛先 IPv6 ホスト アドレスを入力します。アドレスはコロン区切りの 16 ビット値を使用した 16 進形式で指定します。 •（任意）operator には、指定のプロトコルの送信元ポートまたは宛先ポートを比較するオペランドを指

	コマンドまたはアクション	目的
		定します。オペランドには、lt（より小さい）、gt（より大きい）、eq（等しい）、neq（等しくない）、range（包含範囲）があります。 source-ipv6-prefix/prefix-length 引数のあとの operator は、送信元ポートに一致する必要があります。destination-ipv6-prefix/prefix-length 引数のあとの operator は、宛先ポートに一致する必要があります。 • （任意）port-number は、0 ～ 65535 の 10 進数または TCP あるいは UDP ポートの名前です。TCP ポート名を使用できるのは、TCP のフィルタリング時だけです。UDP ポート名を使用できるのは、UDP のフィルタリング時だけです。 • （任意）dscp value を入力して、各 IPv6 パケット ヘッダーの Traffic Class フィールド内のトラフィック クラス値と DiffServ コード ポイント値を照合します。指定できる範囲は 0 ～ 63 です。 • （任意）fragments を入力して、先頭ではないフラグメントを確認します。このキーワードが表示されるのは、プロトコルが ipv6 の場合だけです。 • （任意）log を指定すると、エントリと一致するパケットに関するログ メッセージがコンソールに送信されます。log-input を指定すると、ログエントリに入力インターフェイスが追加されます。ロギングはルータ ACL でだけサポートされます。 • （任意）routing を入力して、IPv6 パケットのルーティングを指定します。

	コマンドまたはアクション	目的
		• （任意）sequence value を入力して、アクセス リスト ステートメントのシーケンス番号を指定します。指定できる範囲は 1 ～ 4294967295 です。 • （任意）time-range name を入力して、拒否または許可ステートメントに適用される時間の範囲を指定します。
ステップ 5	**{deny|permit} tcp** 例： `{deny | permit} tcp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length | any |hostdestination-ipv6-address} [operator [port-number]][ack] [dscp value][established] [fin] [log][log-input] [neq {port |protocol}] [psh] [range{port | protocol}] [rst][routing] [sequence value] [syn] [time-range name][urg]`	（任意）TCP アクセス リストおよびアクセス条件を定義します。 TCP の場合は tcp を入力します。パラメータはステップ 3 で説明されているパラメータと同じですが、次に示すオプションのパラメータが追加されています。 • ack：確認応答（ACK）ビット セット • established：確立された接続。TCP データグラムに ACK または RST ビットが設定されている場合、照合が行われます。 • fin：終了ビット セット。送信元からのデータはそれ以上ありません。 • neq {port | protocol}：所定のポート番号上にないパケットだけを照合します。 • psh：プッシュ機能ビット セット • range {port | protocol}：ポート番号の範囲内のパケットだけを照合します。 • rst：リセット ビット セット • syn：同期ビット セット • urg：緊急ポインタ ビット セット

	コマンドまたはアクション	目的
ステップ 6	**{deny|permit} udp** 例： `{deny | permit} udp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length | any | hostdestination-ipv6-address} [operator [port-number]][dscp value] [log][log-input] [neq {port |protocol}] [range {port |protocol}] [routing][sequence value][time-range name]`	（任意）UDP アクセス リストおよびアクセス条件を定義します。 ユーザ データグラム プロトコルの場合は、udp を入力します。UDP パラメータは TCP に関して説明されているパラメータと同じです。ただし、[operator [port]] のポート番号またはポート名は、UDP ポートの番号または名前でなければなりません。UDP の場合、established パラメータは無効です。
ステップ 7	**{deny|permit} icmp** 例： `{deny | permit} icmp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length | any | hostdestination-ipv6-address} [operator [port-number]][icmp-type [icmp-code] |icmp-message] [dscpvalue] [log] [log-input] [sequence value][time-range name]`	（任意）ICMP アクセス リストおよびアクセス条件を定義します。 インターネット制御メッセージ プロトコルの場合は、icmp を入力します。ICMP パラメータはステップ 3a の IP プロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージ タイプおよびコード パラメータが追加されています。オプションのキーワードの意味は次のとおりです。 • icmp-type：ICMP メッセージ タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • icmp-code：ICMP パケットを ICMP メッセージ コード タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • icmp-message：ICMP パケットを ICMP メッセージ タイプ名または ICMP メッセージ タイプとコード名でフィルタリングする場合に入力します。ICMP メッセージのタイプ名およびコード名のリストについては、? キーを使用するか、またはこのリリースのコマンド リファレンスを参照してください。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show ipv6 access-list** 例： `Device# show ipv6 access-list`	アクセス リストの設定を確認します。
ステップ 10	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 11	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

インターフェイスへの IPv6 ACL の適用

ここでは、ネットワーク インターフェイスに IPv6 ACL を適用する手順について説明します。レイヤ 3 インターフェイスで 着信トラフィックに ACL を適用できます。

インターフェイスへのアクセスを制御する管理には、特権EXECモードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface interface_id** 例： `Device# interface interface-id`	アクセスリストを適用するレイヤ2インターフェイス（ポート ACL 用）を特定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 traffic-filter** *access-list-name* 例： `Device# ipv6 traffic-filter access-list-name in`	インターフェイスの着信トラフィックまたは発信トラフィックにアクセス リストを適用します。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	アクセス リストの設定を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IPv6 ACL の表示

IPv6 ACL を表示するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**show access-list** 例： `Device(config)# show access-lists`	デバイスに設定されたすべてのアクセス リストを表示します。
ステップ 4	**show ipv6 access-list** *acl_name* 例： `Device(config)# show ipv6 access-list [access-list-name]`	設定済みのすべての IPv6 アクセス リストまたは名前付けされたアクセス リストを表示します。

IPv6 ACL の設定例

例：IPv6 ACL の作成

次に、CISCO と名前が付けられた IPv6 アクセス リストを設定する例を示します。リスト内の最初の拒否エントリは、宛先 TCP ポート番号が 5000 より大きいパケットをすべて拒否します。2 番めの拒否エントリは、送信元 UDP ポート番号が 5000 未満のパケットを拒否します。また、この 2 番めの拒否エントリは、すべての一致をコンソールに表示します。リスト内の最初の許可エントリは、すべての ICMP パケットを許可します。リスト内の 2 番めの許可エントリは、その他のすべてのトラフィックを許可します。すべてのパケットを拒否する暗黙の条件が各 IPv6 アクセス リストの末尾にあるため、この 2 番めの許可エントリが必要となります。

```
Device(config)# ipv6 access-list CISCO
Device(config-ipv6-acl)# deny tcp any any gt 5000
Device (config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Device(config-ipv6-acl)# permit icmp any any
Device(config-ipv6-acl)# permit any any
```

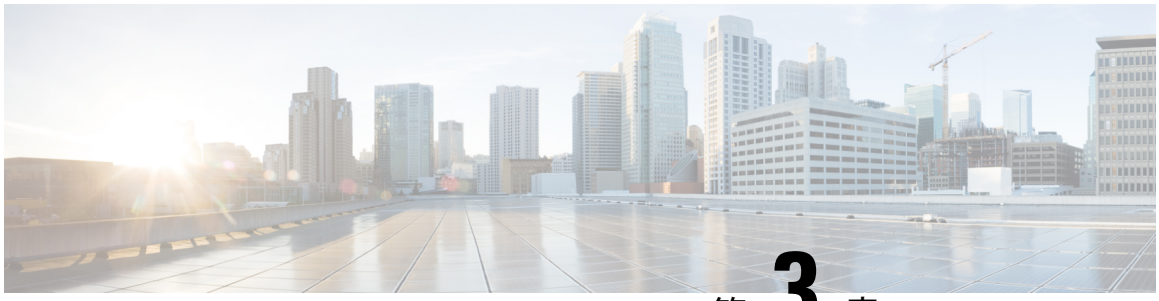
例：IPv6 ACL の表示

次に、**show access-lists** 特権 EXEC コマンドの出力例を示します。出力には、スイッチに設定済みのすべてのアクセス リストが表示されます。

```
Device# show access-lists
Extended IP access list hello
10 permit ip any any
IPv6 access list ipv6
permit ipv6 any any sequence 10
```

次に、**show ipv6 access-lists** 特権 EXEC コマンドの出力例を示します。出力には、スイッチに設定済みの IPv6 アクセス リストだけが表示されます。

```
Device# show ipv6 access-list
IPv6 access list inbound
permit tcp any any eq bgp (8 matches) sequence 10
permit tcp any any eq telnet (15 matches) sequence 20
permit udp any any sequence 30
```



第 3 章

IPv6 組み込み管理コンポーネント

Syslog

IPv6 における Cisco システム メッセージ ロギング（syslog）プロセスを使用すると、ユーザは IPv6 アドレスを指定して syslog メッセージを外部の syslog サーバやホストに記録できます。この実装では、ユーザはホストの IP アドレスを IPv4 形式（たとえば、192.168.0.0）または IPv6 形式（たとえば、2001:DB8:A00:1::1/64）で指定して、IPv4 ベースのロギング ホスト（syslog サーバ）を指定できます。

Syslog over IPv6 の設定

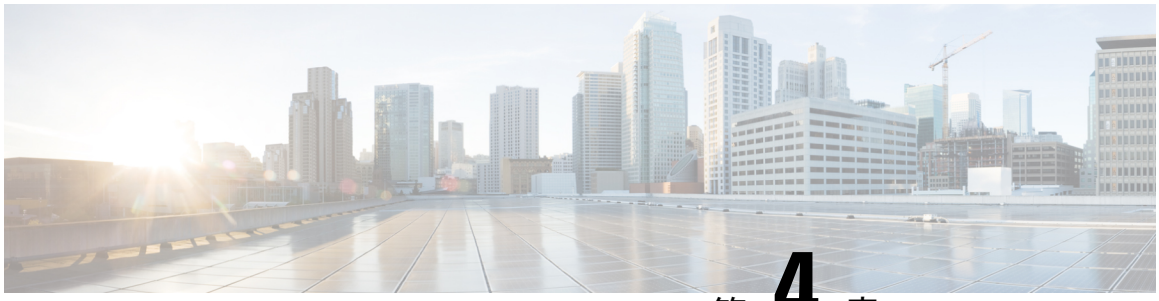
手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**logging host** {{*ip-address* | *hostname*} | {**ipv6** *ipv6-address* | *hostname*}} [**transport** {**udp** [**port** *port-number*] | **tcp** [**port**	リモート ホストへのシステム メッセージおよびデバッグ出力を記録します。

	コマンドまたはアクション	目的
	port-number] [**audit**]}] [**xml** | **filtered** [**stream** *stream-id*]] [**alarm** [*severity*]] 例： `Device(config)# logging host ipv6 AAAA:BBBB:CCCC:DDDD::FFFF`	

例：Syslog over IPv6 の設定

```
Device(config)# logging host ipv6 AAAA:BBBB:CCCC:DDDD::FFFF transport tcp port 1470
```



第 4 章

SNMP over IPv6

SNMP over IPv6

簡易ネットワーク管理プロトコル（SNMP）を IPv6 トランスポート経由で設定し、IPv6 ホストが SNMP クエリーを実行し、IPv6 を実行しているデバイスから SNMP 通知を受信できるようにすることができます。

SNMP over an IPv6 Transport

簡易ネットワーク管理プロトコル（SNMP）を IPv6 トランスポート経由で設定し、IPv6 ホストが SNMP クエリーを実行し、IPv6 ソフトウェアを実行しているデバイスから SNMP 通知を受信できるようにすることができます。SNMP エージェントおよび関連する MIB が拡張され、IPv6 アドレッシングがサポートされるようになりました。この機能は、Data Encryption Standard（3DES）および Advanced Encryption Standard（AES）のメッセージ暗号化規格を使用します。

IPv6 を介した SNMP 通知サーバの設定

SNMP マネージャとエージェントとの関係を定義するには、SNMP コミュニティ ストリングを使用します。コミュニティ ストリングは、デバイス上のエージェントへのアクセスを制御するパスワードのように機能します。ストリングに関連付ける特性を次の中から 1 つ以上指定することもできます。

- エージェントへのアクセスを取得するためにコミュニティ ストリングを使用することを許可された SNMP マネージャの IP アドレスのアクセス リスト
- 特定のコミュニティへのアクセスが可能なすべての MIB オブジェクトのサブセットを定義する MIB ビュー

- コミュニティへのアクセスが可能な MIB オブジェクトに対する読み書きアクセス権または読み取り専用アクセス権

1つ以上のコミュニティストリングを設定できます。特定のコミュニティストリングを削除するには、**no snmp-server community** コマンドを使用します。

snmp-server host コマンドでは、どのホストで SNMP 通知を受信するか、および通知がトラップとインフォーム要求のどちらで送信されるようにするかを指定します。**snmp-server enable traps** コマンドは、指定された通知タイプ（ボーダー ゲートウェイ プロトコル（BGP）トラップ、設定トラップ、エンティティトラップなど）の生成メカニズムをグローバルにイネーブルにします。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [**ipv6** *nacl*] [*access-list-number*] 例： `Device(config)# snmp-server community mgr view restricted rw ipv6 mgr2`	コミュニティ アクセス ストリングを定義します。
ステップ 4	**snmp-server engineID remote** {*ipv4-ip-address* | *ipv6-address*} [**udp-port** *udp-port-number*] [**vrf** *vrf-name*] *engineid-string* 例： `Device(config)# snmp-server engineID remote 3ffe:b00:c18:1::3/127 remotev6`	（任意）リモート SNMP エンジン（または SNMP のコピー）の名前を指定します。
ステップ 5	**snmp-server group** *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context** *context-name*] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** [**ipv6** *named-access-list*] {*acl-number* | *acl-name*}] 例：	（任意）新しい SNMP グループ、または SNMP ユーザを SNMP ビューにマッピングするテーブルを設定します。

	コマンドまたはアクション	目的
	`Device(config)# snmp-server group public v2c access ipv6 public2`	
ステップ 6	**snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*] 例： `Device(config)# snmp-server host host1.com 2c vrf trap-vrf`	SNMP 通知動作の指定 • SNMP 通知をトラップまたは応答要求として送信するかどうか、使用する SNMP のバージョン、通知のセキュリティ レベル（SNMPv3 の場合）、および通知の受信者（ホスト）を指定します。
ステップ 7	**snmp-server user** *username group-name* [**remote** *host* [**udp-port** *port*]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** [**ipv6** *nacl*] [**priv** {**des** | **3des** | **aes** {**128** | **192** | **256**}} *privpassword*] {*acl-number* | *acl-name*}] 例： `Device(config)# snmp-server user user1 bldg1 remote 3ffe:b00:c18:1::3/127 v2c access ipv6 public2`	（任意）既存の SNMP グループに新しいユーザを設定します。 （注） アドレスのリモート ユーザを設定するには、まずそのリモート ホストのエンジン ID を設定する必要があります。これは、これらのコマンドの設計として課された制限です。ホストよりも前にユーザを設定しようとすると、警告メッセージが表示され、コマンドは実行されません。
ステップ 8	**snmp-server enable traps** [*notification-type*] [**vrrp**] 例： `Device(config)# snmp-server enable traps bgp`	トラップまたはインフォームの送信をイネーブルにして、送信される通知のタイプを指定します。 • *notification-type* 引数が指定されていない場合は、サポートされているすべての通知がデバイスでイネーブルになります。 • デバイスで使用可能な通知を確認するには、 **snmp-server enable traps ?** コマンドを入力します。

例：IPv6 を介した SNMP 通知サーバの設定

次に、コミュニティ ストリング public を使用して、SNMP が読み取り専用アクセス権ですべてのオブジェクトにアクセスすることを許可する例を示します。また、デバイスは、SNMP フ

ラッシュトラップを SNMPv1 を使用して IPv4 ホスト 172.16.1.111 と IPv6 ホスト 3ffe:b00:c18:1::3/127 に送信し、SNMPv2c を使用してホスト 172.16.1.27 に送信します。トラップとともにコミュニティ ストリング public が送信されます。

```
Device(config)# snmp-server community public
Device(config)# snmp-server enable traps flash
Device(config)# snmp-server host 172.16.1.27 version 2c public
Device(config)# snmp-server host 172.16.1.111 version 1 public
Device(config)# snmp-server host 3ffe:b00:c18:1::3/127 public
```

例：SNMP サーバ グループと指定されたビューとの関連付け

次に、SNMP コンテキスト A を SNMPv2c グループ GROUP1 のビューと IPv6 の名前付きアクセス リスト public2 に関連付ける例を示します。

```
Device(config)# snmp-server context A
Device(config)# snmp mib community-map commA context A target-list commAVpn
Device(config)# snmp mib target list commAVpn vrf CustomerA
Device(config)# snmp-server view viewA ciscoPingMIB included
Device(config)# snmp-server view viewA ipForward included
Device(config)# snmp-server group GROUP1 v2c context A read viewA write viewA notify
access ipv6 public2
```

例：SNMP 通知サーバの作成

次に、IPv6 ホストを通知サーバとして設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# snmp-server community mgr view restricted rw ipv6 mgr2
Device(config)# snmp-server engineID remote 3ffe:b00:c18:1::3/127 remotev6
Device(config)# snmp-server group public v2c access ipv6 public2
Device(config)# snmp-server host host1.com 2c vrf trap-vrf
Device(config)# snmp-server user user1 bldg1 remote 3ffe:b00:c18:1::3/127 v2c access
ipv6 public2
Device(config)# snmp-server enable traps bgp
Device(config)# exit
```