



SNMP over IPv6

- [SNMP over IPv6](#) (1 ページ)
- [SNMP over an IPv6 Transport](#) (1 ページ)
- [IPv6 を介した SNMP 通知サーバの設定](#) (1 ページ)
- [例：IPv6 を介した SNMP 通知サーバの設定](#) (3 ページ)

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 <i>string</i> [view <i>view-name</i>] [ro rw] [ipv6 nacl] [<i>access-list-number</i>] 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 { <i>ipv4-ip-address</i> <i>ipv6-address</i> } [udp-port <i>udp-port-number</i>] [vrf <i>vrf-name</i>] <i>engineid-string</i> 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 <i>group-name</i> { v1 v2c v3 { auth noauth priv }} [context <i>context-name</i>] [read <i>read-view</i>] [write <i>write-view</i>] [notify <i>notify-view</i>] [access [ipv6 <i>named-access-list</i>] { <i>acl-number</i> <i>acl-name</i> }] 例：	(任意) 新しい SNMP グループ、または SNMP ユーザを SNMP ビューにマップ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、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
```