



## SNMP コマンド

---

この章は、次の項で構成されています。

- [snmp-server community](#) (2 ページ)
- [snmp-server community-group](#) (4 ページ)
- [snmp-server server](#) (6 ページ)
- [snmp-server source-interface](#) (7 ページ)
- [snmp-server source-interface-ipv6](#) (9 ページ)
- [snmp-server view](#) (11 ページ)
- [snmp-server group](#) (13 ページ)
- [show snmp views](#) (15 ページ)
- [show snmp groups](#) (16 ページ)
- [snmp-server user](#) (18 ページ)
- [show snmp users](#) (20 ページ)
- [snmp-server filter](#) (22 ページ)
- [show snmp filters](#) (23 ページ)
- [snmp-server host](#) (24 ページ)
- [snmp-server engineID local](#) (26 ページ)
- [snmp-server engineID remote](#) (28 ページ)
- [show snmp engineID](#) (29 ページ)
- [snmp-server enable traps](#) (30 ページ)
- [snmp-server trap authentication](#) (31 ページ)
- [snmp-server contact](#) (32 ページ)
- [snmp-server location](#) (33 ページ)
- [snmp-server set](#) (34 ページ)
- [snmp trap link-status](#) (35 ページ)
- [show snmp](#) (36 ページ)

## snmp-server community

SNMP コマンド (v1 および v2) へのアクセスを許可するコミュニティ アクセス スtring (パスワード) を設定するには、**snmp-server community** グローバル コンフィギュレーション モード コマンドを使用します。これは、GET や SET などの SNMP コマンドに使用されます。

このコマンドは、SNMP v1 および v2 の両方を設定します。

指定したコミュニティ スtring を削除するには、このコマンドの **no** 形式を使用します。

### 構文

```
snmp-server community community-string [ro | rw | su] [ip-address / ipv6-address] [mask mask | prefix prefix-length] [view view-name] [type {router | oob}]
```

```
no snmp-server community community-string [ip-address] [type {router | oob}]
```

### パラメータ

- **community-string** : SNMP プロトコルへのアクセスを許可するパスワードを定義します。  
(範囲 : 1 ~ 20 文字)。
- **ro** : (任意) 読み取り専用アクセスを指定します (デフォルト)。
- **rw** : (任意) 読み取りと書き込みアクセスを指定します。
- **su** : (任意) SNMP 管理者アクセス権を指定します。
- **ip-address** : (任意) 管理ステーション IP アドレス。デフォルトは、すべての IP アドレスです。IPv4、IPv6 または IPv6z アドレスを使用できます。
- **mask** : (任意) IPv4 アドレスのマスクを指定します。これはネットワーク マスクではありませんが、設定されている IP アドレスと比較するパケットの発信元アドレスのビットを定義するマスクです。指定しない場合、デフォルトで 255.255.255.255 に設定されます。IPv4 アドレスなしでマスクを指定した場合、コマンドはエラーを返します。
- **prefix-length** : (任意) IPv4 アドレスプレフィックスを構成するビット数を指定します。指定しない場合、デフォルトで 32 になります。IPv4 アドレスなしでプレフィックス長を指定した場合、コマンドはエラーを返します。
- **view view-name** : (任意) **snmp-server view** (11 ページ) コマンドを使用して設定されたビューの名前を指定します (コマンド設定において特定の順序をユーザが意識する必要はありません)。ビューには、コミュニティで使用できるオブジェクトが定義されています。これは **su** には該当しません。MIB 全体にアクセスできるからです。指定しないと、コミュニティテーブル、SNMPv3 ユーザテーブル、アクセステーブルを除き、すべてのオブジェクトを使用できます。(範囲 : 1 ~ 30 文字)
- **type router** : (任意) IP アドレスがアウトオブバンド ネットワーク上にあるかインバンド ネットワーク上にあるかを示します。

## デフォルト設定

コミュニティは定義されていません

## コマンドモード

グローバル コンフィギュレーション モード

## 使用上のガイドライン

コマンドの論理キーはペア (community, ip-address) です。ip-address を省略した場合、キーは (community, All-IPs) です。つまり、2つのコマンドに同じ community, ip-address ペアを指定することはできません。

*view-name* は、コミュニティストリングのアクセス権を制限するために使用します。view-name を指定すると、ソフトウェアは次のことを行います。

- 内部セキュリティ名を生成します。
- SNMPv1 および SNMPv2 セキュリティ モデルの内部セキュリティ名を内部グループ名にマップします。
- SNMPv1 および SNMPv2 セキュリティ モデルの内部グループ名を view-name にマップします (読み取りビューと通知ビューには常にマップし、rw を指定している場合は書き込みビューにもマップします)。

## 例

IP アドレス 1.1.1.121 およびマスク 255.0.0.0 にある管理ステーションへの管理者アクセス権のパスワードを定義します。

```
switchxxxxxx(config)# snmp-server community abcd su 1.1.1.121 mask 255.0.0.0
```

## snmp-server community-group

ユーザグループにアクセス権を設定するには、**snmp-server community-group** を使用します。アクセス権を指定するためには、グループが存在している必要があります。このコマンドは、SNMP v1 および v2 の両方を設定します。

### 構文

```
snmp-server community-group community-string group-name [ip-address | ipv6-address] [mask mask / prefix prefix-length] [type {router | oob}]
```

### パラメータ

- **community-string** : SNMP プロトコルへのアクセスを許可するパスワードを定義します。  
(範囲 : 1 ~ 20 文字)。
- **group-name** : これは、**snmp-server group** (13 ページ) に v1 または v2 を指定して設定したグループの名前です (2つのコマンド設定において特定の順序をユーザが意識する必要はありません)。グループには、コミュニティで使用できるオブジェクトが定義されています。(範囲 : 1 ~ 30 文字)
- **ip-address** : (任意) 管理ステーション IP アドレス。デフォルトは、すべての IP アドレスです。IPv4、IPv6 または IPv6z アドレスを使用できます。
- **mask** : (任意) IPv4 アドレスのマスクを指定します。これはネットワーク マスクではありませんが、設定されている IP アドレスと比較するパケットの発信元アドレスのビットを定義するマスクです。指定しない場合、デフォルトで 255.255.255.255 に設定されます。IPv4 アドレスなしでマスクを指定した場合、コマンドはエラーを返します。
- **prefix-length** : (任意) IPv4 アドレスプレフィックスを構成するビット数を指定します。指定しない場合、デフォルトで 32 になります。IPv4 アドレスなしでプレフィックス長を指定した場合、コマンドはエラーを返します。
- **type router** : (任意) IP アドレスがアウトオブバンドネットワーク上にあるかインバンドネットワーク上にあるかを示します。

### デフォルト設定

コミュニティは定義されていません

### コマンドモード

グローバル コンフィギュレーション モード

### 使用上のガイドライン

*group-name* は、コミュニティストリングのアクセス権を制限するために使用します。*group-name* を指定すると、ソフトウェアは次のことを行います。

- 内部セキュリティ名を生成します。
- SNMPv1 および SNMPv2 セキュリティ モデルの内部セキュリティ名をグループ名にマップします。

#### 例

グループ *abcd* に対してパスワード *tom* を定義して、このグループがプレフィックス 8 の管理ステーション 1.1.1.121 にアクセスできるようにします。

```
switchxxxxxx(config)# snmp-server community-group tom abcd 1.1.1.122 prefix 8
```

## snmp-server server

SNMP プロトコルでデバイスを設定できるようにするには、**snmp-server server** グローバル コンフィギュレーション モード 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。

### 構文

**snmp-server server**

**no snmp-server server**

### パラメータ

このコマンドには引数またはキーワードはありません。

### デフォルト設定

無効

### コマンドモード

グローバル コンフィギュレーション モード

### 例

```
switchxxxxxx(config)# snmp-server server
```

# snmp-server source-interface

簡易ネットワーク管理プロトコル（SNMP）トラップがインフォームやトラップの送信元とするインターフェイスを指定するには、グローバルコンフィギュレーションモードで **snmp-server source-interface** コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

## 構文

```
snmp-server source-interface {traps | informs} interface-id
```

```
no snmp-server source-interface [traps | informs]
```

## パラメータ

- **traps** : SNMP トラップ インターフェイスを指定します。
- **informs** : SNMP インフォームを指定します。
- **interface-id** : 送信元インターフェイスを指定します。

## デフォルト設定

送信元 IPv4 アドレスは、発信インターフェイスで定義され、ネクスト ホップ IPv4 サブネットに属する IPv4 アドレスです。

**no snmp-server source-interface** でパラメータが指定されていない場合、デフォルトは両方 traps、および informs です。

## コマンドモード

グローバル コンフィギュレーション モード

## 使用上のガイドライン

送信元インターフェイスが発信インターフェイスの場合は、ネクスト ホップ IPv4 サブネットに属するインターフェイス IP アドレスが適用されます。

送信元インターフェイスが発信インターフェイスでない場合は、送信元インターフェイスで定義された最小 IPv4 アドレスが適用されます。

使用できる IPv4 送信元アドレスがない場合は、SNMP トラップまたは SNMP インフォームを送信しようとする、Syslog メッセージが発行されます。

SNMP トラップの送信元インターフェイスを削除するには、**no snmp-server source-interface traps** コマンドを使用します。

SNMP インフォームの送信元インターフェイスを削除するには、**no snmp-server source-interface informs** コマンドを使用します。

SNMP トラップおよび SNMP インフォームの送信元インターフェイスを削除するには、**no snmp-server source-interface** コマンドを使用します。

#### 例

次に、VLAN 10 をトラップの送信元インターフェイスとして設定する例を示します。

```
switchxxxxxx(config)# snmp-server source-interface traps vlan 100
```



## snmp-server source-interface-ipv6

簡易ネットワーク管理プロトコル（SNMP）トラップがインフォームやトラップの送信元とするインターフェイスを指定するには、グローバルコンフィギュレーションモードで **snmp-server source-interface** コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

### 構文

```
snmp-server source-interface-ipv6 {traps | informs} interface-id
```

```
no snmp-server source-interface-ipv6 [traps | informs]
```

### パラメータ

- **traps** : SNMP トラップ インターフェイスを指定します。
- **informs** : SNMP トラップ インフォームを指定します。
- **interface-id** : 送信元インターフェイスを指定します。

### デフォルト設定

IPv6 送信元アドレスは、発信インターフェイスの IPv6 アドレスであり、RFC6724 に従って選択されます。

**no snmp-server source-interface** でパラメータが指定されていない場合、デフォルトは両方 traps、および informs です。

### コマンドモード

グローバル コンフィギュレーション モード

### 使用上のガイドライン

送信元インターフェイスが発信インターフェイスである場合は、インターフェイスで定義され、RFC 6724 に従って選択された IPv6 アドレスです。

送信元インターフェイスが発信インターフェイスでない場合は、送信元インターフェイス上で宛先 IPv6 アドレスの範囲で定義された最小 IPv6 アドレスが適用されます。

使用できる IPv6 送信元アドレスがない場合は、SNMP トラップまたは SNMP インフォームを送信しようとする、Syslog メッセージが発行されます。

SNMP トラップの送信元 IPv6 インターフェイスを削除するには、**no snmp-server source-interface-ipv6 traps** コマンドを使用します。

SNMP インフォームの送信元 IPv6 インターフェイスを削除するには、**no snmp-server source-interface-ipv6 informs** コマンドを使用します。

SNMP トラップおよび SNMP インフォームの送信元 IPv6 インターフェイスを削除するには、**no snmp-server source-interface-ipv6** コマンドを使用します。

#### 例

次の例では、VLAN 10 を送信元インターフェイスとして設定します。

```
switchxxxxxx(config)# snmp-server source-interface-ipv6 traps vlan 100
```

## snmp-server view

SNMP ビューを作成または更新するには、**snmp-server view** グローバル コンフィギュレーションモード コマンドを使用します。SNMP ビューを削除するには、このコマンドの **no** 形式を使用します。

### 構文

```
snmp-server view view-name oid-tree {included | excluded}
```

```
no snmp-server view view-name [oid-tree]
```

### パラメータ

- **view-name** : 作成または更新しているビューの名前を指定します。(長さ: 1 ~ 30 文字)
- **included** : ビュータイプが含まれることを指定します。
- **excluded** : ビュータイプが除外されることを指定します。
- **oid-tree** : (任意) ビューに含める、またはビューから除外する ASN.1 サブツリーオブジェクト識別子を指定します。サブツリーを識別するには、数字 (1.3.6.2.4 など) や単語 (System など) や一連の番号 (任意) で構成されるテキスト文字列を指定します。サブツリーファミリを指定するには、サブ ID の 1 文字をアスタリスク (\*) ワイルドカードに変えます。たとえば、1.3.\*.4 です。このパラメータは、指定している MIB によって異なります。

### デフォルト設定

次のビューがデフォルトで作成されます。

- **Default** : SNMP パラメータ自体を設定するものを除きすべての MIB を含みます。
- **DefaultSuper** : すべての MIB を含みます。

### コマンドモード

グローバル コンフィギュレーションモード

### 使用上のガイドライン

このコマンドは、同じビューに対して複数回入力できます。

コマンドの論理キーはペア (**view-name**, **oid-tree**) です。このため、2つのコマンドに同じ **view-name** と **oid-tree** を指定することはできません。

ビューの数は 64 に制限されています。

Default ビューおよび DefaultSuper ビューは、内部ソフトウェア用に予約されており、削除も変更もできません。

## 例

次の例では、sysServices（システム 7）を除くすべてのオブジェクトが MIB-II システム グループに含まれ、インターフェイス 1 のすべてのオブジェクトが MIB-II インターフェイス グループに含まれているビューを作成しています（この形式は、ifEntry に指定されているパラメータで指定します）。

```
switchxxxxxx(config)# snmp-server view user-view system included  
switchxxxxxx(config)# snmp-server view user-view system.7 excluded  
switchxxxxxx(config)# snmp-server view user-view ifEntry.*.1 included
```

## snmp-server group

SNMP グループを設定するには、**snmp-server group** グローバル コンフィギュレーション モード コマンドを使用します。グループは、SNMP ユーザを SNMP ビューにマップするために使用します。SNMP グループを削除するには、このコマンドの **no** 形式を使用します。

### 構文

```
snmp-server group groupname {v1 / v2 / v3 [noauth / auth / priv] [notify notifyview]} [read readview] [write writeview]
```

```
no snmp-server group groupname {v1 / v2 / v3 [noauth / auth / priv]}
```

### パラメータ

- **group** *groupname* : グループ名を指定します。(長さ : 1 ~ 30 文字)
- **v1** : SNMP バージョン 1 のセキュリティ モデルを指定します。
- **v2** : SNMP バージョン 2 のセキュリティ モデルを指定します。
- **v3** : SNMP バージョン 3 のセキュリティ モデルを指定します。
- **noauth** : パケット認証が実行されないことを指定します。SNMP バージョン 3 のセキュリティ モデルにのみ適用されます。
- **auth** : パケット認証が暗号化なしで実行されることを指定します。SNMP バージョン 3 のセキュリティ モデルにのみ適用されます。
- **priv** : パケット認証が暗号化ありで実行されることを指定します。SNMP バージョン 3 のセキュリティ モデルにのみ適用されます。認証とプライバシーの両方による SNMPv3 ユーザの作成は、GUI で行う必要があることに注意してください。他のすべてのユーザは、CLI で作成できます。
- **notify** *notifyview* : (任意) インフォームまたはトラップを生成できるビュー名を指定します。inform は確認が必要なトラップです。SNMP バージョン 3 のセキュリティ モデルにのみ適用されます。(長さ : 1 ~ 32 文字)
- **read** *readview* : (任意) 表示のみできるビュー名を指定します。(長さ : 1 ~ 32 文字)
- **write** *writeview* : (任意) エージェントを設定できるビュー名を指定します。(長さ : 1 ~ 32 文字)

### デフォルト設定

グループ エントリは存在しません。

*notifyview* を指定しないと、通知ビューは定義されません。

*readview* を指定しないと、コミュニティ テーブル、SNMPv3 ユーザ テーブル、アクセス テーブルを除き、すべてのオブジェクトを取得できます。

*writeview* を指定しないと、書き込みビューは定義されません。

## コマンド モード

グローバル コンフィギュレーション モード

## 使用上のガイドライン

このコマンドに定義されているグループは、ユーザをグループにマップするために [snmp-server user](#) (18 ページ) コマンドで使用します。これらのユーザは、このコマンドに定義されているビューに自動的にマップされます。

コマンドの論理キーは (**groupname, snmp-version, security-level**) です。snmp-version v1/v2 の場合、security-level は常に **noauth** です。

## 例

次の例では、*user-group* というグループを SNMPv3 にアタッチし、暗号化されたセキュリティレベルをグループに割り当て、*user-view* というビューのアクセス権を読み取り専用に制限しています。次に、*user-group* にユーザ *tom* を割り当てています。そのため、ユーザ *tom* には *user-view* で権利が割り当てられます。

```
switchxxxxxxx(config)# snmp-server group user-group v3 priv read user-view  
switchxxxxxxx(config)# snmp-server user tom user-group v3
```

# show snmp views

SNMP ビューを表示するには、**show snmp views** 特権 EXEC モード コマンドを使用します。

## 構文

**show snmp views** [*viewname*]

## パラメータ

**viewname** : (任意) ビュー名を指定します。(長さ : 1 ~ 30 文字)

## デフォルト設定

*viewname* を指定しないと、すべてのビューが表示されます。

## コマンドモード

特権 EXEC モード

## 例

次に、設定した SNMP ビューを表示する例を示します。

switchxxxxxx# show snmp views		
Name	OID Tree	Type
-----	-----	-----
Default	iso	Included
Default	snmpNotificationMIB	Excluded
DefaultSuper	iso	Included

# show snmp groups

設定した SNMP グループを表示するには、**show snmp groups** 特権 EXEC モード コマンドを使用します。

## 構文

**show snmp groups** [groupname]

## パラメータ

**groupname** : (任意) グループ名を指定します。(長さ : 1 ~ 30 文字)

## デフォルト設定

すべてのグループを表示します。

## コマンドモード

特権 EXEC モード

## 例

次に、設定した SNMP グループを表示する例を示します。

switchxxxxxxx# show snmp groups							
Name		Security				Views	
-----	Model		Level		Read	Write	Notify
user-group	-----		----		-----	-----	-----
managers-group	V2		no_auth		Default	""	""
	V2		no_auth		Default	Default	""

次の表では、上記の重要なフィールドについて説明します。

フィールド		説明
[名前 (Name) ]		グループ名。
Security	Model	使用中の SNMP モデル (v1、v2 または v3) 。
Security	Level	パケットセキュリティ。SNMP v3 セキュリティにのみ適用できます。



フィールド		説明
Views	Read	エージェントの内容を表示できるビュー名。指定しないと、コミュニティテーブル、SNMPv3 ユーザテーブル、アクセステーブルを除き、すべてのオブジェクトを使用できます。
	Write	データを入力し、エージェントの内容を管理できるビュー名。
	Notify	インフォームまたはトラップを指定できるビュー名。

## snmp-server user

新しい SNMP ユーザを設定するには、**snmp-server user** グローバル コンフィギュレーション モード コマンドを使用します。ユーザを削除するには、このコマンドの **no** 形式を使用します。認証およびプライバシー パスワードを暗号化形式（SSD を参照）で入力するには、このコマンドの暗号化形式を使用します。

### 構文

```
snmp-server user username groupname {v1 | v2c | [remote host] v3} [auth { sha | sha224 | sha256 | sha384 | sha512 } auth-password [priv priv-password]]
```

```
encrypted snmp-server user username groupname {v1 | v2c | [remote host] v3} [auth { sha | sha224 | sha256 | sha384 | sha512 } encrypted-auth-password [priv encrypted-priv-password]]
```

```
no snmp-server user username {v1 | v2c | [remote host] v3}
```

### パラメータ

- **username** : エージェントに接続するホストのユーザ名を定義します。（範囲：最大 20 文字）。
- **groupname** : ユーザが属するグループの名前。グループは、[snmp-server group](#)（13 ページ）コマンドに v1 または v2c パラメータを指定して設定する必要があります（2つのコマンド設定において特定の順序をユーザが意識する必要はありません）。（範囲：最大 30 文字）
- **v1** : ユーザが v1 ユーザであることを指定します。
- **v2c** : ユーザが v2c ユーザであることを指定します。
- **v3** : ユーザが v3 ユーザであることを指定します。
- **remote host** : （任意）リモート SNMP ホストの IP アドレス（IPv4、IPv6 または IPv6z）またはホスト名。
- **auth** : （任意）どの認証レベルを使用するかを指定します。
  - Sha** : （任意）HMAC-SHA-96 認証レベルを指定します。
  - Sha224** : （任意）HMAC-SHA-224-128 認証レベルを指定します。
  - Sha256** : （任意）HMAC-SHA-256-192 認証レベルを指定します。
  - Sha384** : （任意）HMAC-SHA-384-256 認証レベルを指定します。
  - Sha512** : （任意）HMAC-SHA-512-384 認証レベルを指定します。
- **auth-password** : （任意）認証パスワードを指定します。範囲：32 文字以内。
- **encrypted-auth-password** : （任意）認証パスワードを暗号化形式で指定します。
- **priv priv-password** : （任意）プライベート（priv）暗号化とプライバシーパスワードを指定します（範囲：最大 32 文字）。使用する暗号化アルゴリズムは、128 ビットの暗号キー

を使用する暗号フィードバックモード (CFB : Cipher Feedback Mode) の高度暗号化規格 (AES) アルゴリズムです。

- **encrypted-priv-password** : (任意) プライバシー パスワードを暗号化形式で指定します。

## デフォルト設定

グループ エントリは存在しません。

## コマンドモード

グローバル コンフィギュレーション モード

## 使用上のガイドライン

SNMP v1 および v2 に対して、このコマンドは `snmp-server community-group` と同じ操作を実行します。ただし、`snmp-server community-group` は v1 と v2 の両方を同時に設定する点が異なります。このコマンドでは、v1 と v2 に対して 1 回ずつ実行する必要があります。

デバイスに SNMPv3 ユーザを追加するには、ローカル SNMP エンジン ID を定義する必要があります。リモートホストユーザの場合、リモート SNMP エンジン ID も必要です。

**snmpEngineID** の値を変更または削除すると、SNMPv3 ユーザのデータベースが削除されます。

このコマンドの論理キーは `username` です。

インフォームは確認応答を必要とするトラップです。そのため、リモートホストにインフォームを送信するには、そのリモートホストを設定する必要があります。設定したリモートホストは (インフォームの取得以外に) デバイスを管理することもできます。

リモートユーザを設定する場合は、ユーザが存在するデバイスのリモート SNMP エージェントに対応する IP アドレスを指定します。また、特定のエージェントにリモートユーザを設定する前に、`snmp-server engineID remote` (28 ページ) コマンドを使用して SNMP エンジン ID を設定します。リモートエージェントの SNMP エンジン ID は、パスワードから認証とプライバシーダイジェストを計算する際に必要です。最初にリモートエンジン ID が設定されていない場合、コンフィギュレーション コマンドは失敗します。

異なるバージョンやアクセス レベル (`noauth`、`auth` または `auth & priv`) のたびに、同じグループを複数回定義できるため、ユーザを定義するときにグループ名を指定するだけでは不十分です。そうではなく、このユーザからのパケットを処理する方法を完全に決定するためには、グループ名、バージョンおよびアクセス レベルを指定する必要があります。

## 例

この例では、SNMP v1 および v2c を使用して、ユーザ `tom` をグループ `abcd` に割り当てています。ユーザ `jerry` が SNMP v3 を使用してグループ `efgh` に割り当てられます。

```
switchxxxxxx(config)# snmp-server user tom acbd v1
switchxxxxxx(config)# snmp-server user tom acbd v2c
switchxxxxxx(config)# snmp-server user jerry efgh v3 auth sha pass1234
```

# show snmp users

設定した SNMP ユーザを表示するには、**show snmp users** 特権 EXEC モード コマンドを使用します。

## 構文

**show snmp users** [*username*]

## パラメータ

**username** : (任意) ユーザ名を指定します。(長さ : 1 ~ 30 文字)

## デフォルト設定

すべてのユーザを表示します。

## コマンドモード

特権 EXEC モード

## 例

次に、設定した SNMP ユーザを表示する例を示します。

```
switchxxxxx# show snmp users
User name           : ulrem
  Group name        : group1
  Authentication Method : None
  Privacy Method    : None
  Remote            : 11223344556677
  Auth Password     :
  Priv Password     :
User name           : qqg
  Group name        : www
  Authentication Method : SHA256
  Privacy Method    : None
  Remote            :
  Auth Password     : helloworld1234567890987665
  Priv Password     :
User name           : hello
  Group name        : world
  Authentication Method : SHA256
  Privacy Method    : AES-128
  Remote            :
  Auth Password (encrypted) : Z/tC3UF5j0pYfmXm8xeMvcIOQ6LQ4GOACCGYLRdAgOE6XQKTC
                                qMlrnpWuHraRlZj
  Priv Password (encrypted) : kN1ZHsSLo6WWx1kuZVzhLOolgI5waaNf7Vq6yLBpJds4N68tL
                                1tbTRSz2H4c4Q4o
User name           : ulnoAuth
  Group name        : group1
  Authentication Method : None
  Privacy Method    : None
  Remote            :
  Auth Password (encrypted) :
  Priv Password (encrypted) :
```

```
User name                : u1OnlyAuth
Group name               : group1
Authentication Method    : SHA1
Privacy Method           : None
Remote                   :
Auth Password (encrypted): 8nPzy2hzuba9pG3iiC/q0451RynUn7kq94L9WORFrRM=
Priv Password (encrypted):
```

## snmp-server filter

SNMP サーバ通知フィルタを作成または更新するには、**snmp-server filter** グローバルコンフィギュレーション モード コマンドを使用します。通知フィルタを削除するには、このコマンドの **no** 形式を使用します。

### 構文

```
snmp-server filter filter-name oid-tree {included | excluded}
```

```
no snmp-server filter filter-name [oid-tree]
```

### パラメータ

- **filter-name** : 更新または作成しているフィルタレコードのラベルを指定します。名前は、他のコマンドでそのフィルタを参照するために使用します。(長さ: 1 ~ 30 文字)
- **oid-tree** : ビューに含めるまたはビューから除外する ASN.1 サブツリーのオブジェクト識別子を指定します。サブツリーを識別するために、1.3.6.2.4 などの数字や **system** などの単語で構成されるテキスト文字列を指定します。サブツリーファミリを指定するには、サブ ID の 1 文字をアスタリスク (\*) ワイルドカードに変えます。たとえば、1.3.\*.4 です。
- **included** : フィルタタイプが含まれることを指定します。
- **excluded** : フィルタタイプが除外されることを指定します。

### デフォルト設定

ビュー エントリは存在しません。

### コマンドモード

グローバル コンフィギュレーション モード

### 使用上のガイドライン

このコマンドは、同じフィルタに対して複数回入力できます。オブジェクト識別子が複数の行に含まれている場合、後の行が優先されます。コマンドの論理キーはペア (*filter-name*, *oid-tree*) です。

### 例

次に、sysServices (System 7) と MIB-II インターフェイスグループ内のインターフェイス 1 のすべてのオブジェクトを除く、MIB-II システムグループのすべてのオブジェクトを含むフィルタを作成する例を示します (この形式は *ifEntry* で指定したパラメータによって異なります)。

```
switchxxxxxxx(config)# snmp-server filter f1 system included
switchxxxxxxx(config)# snmp-server filter f2 system.7 excluded
switchxxxxxxx(config)# snmp-server filter f3 ifEntry.*.1 included
```

## show snmp filters

定義した SNMP フィルタを表示するには、**show snmp filters** 特権 EXEC モード コマンドを使用します。

### 構文

**show snmp filters** [*filtername*]

### パラメータ

**filtername** : フィルタ名を指定します。（長さ : 1 ~ 30 文字）

### デフォルト設定

フィルタ名を定義しないと、すべてのフィルタが表示されます。

### コマンドモード

特権 EXEC モード

### 例

次に、設定した SNMP フィルタを表示する例を示します。

<pre>switchxxxxxx# show snmp filters user-filter</pre>		
Name	OID Tree	Type
-----	-----	-----
user-filter	1.3.6.1.2.1.1	Included
user-filter	1.3.6.1.2.1.1.7	Excluded
user-filter	1.3.6.1.2.1.2.2.1.*.1	Included

## snmp-server host

SNMP 通知（トラップ/インフォーム）用にホストを設定するには、**snmp-server host** グローバル コンフィギュレーション モード コマンドを使用します。このコマンドの **no** 形式を使用すると、指定したホストを削除します。

### 構文

```
snmp-server host {host-ip | hostname} [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}]
community-string [udp-port port] [filter filtername] [timeout seconds] [retries retries]
```

```
no snmp-server host {ip-address | hostname} [traps | informs] [version {1 | 2c | 3}]
```

### パラメータ

- **host-ip** : ホスト（ターゲットとなる受信側）の IP アドレス。デフォルトは、すべての IP アドレスです。IPv4、IPv6 または IPv6z アドレスを使用できます。
- **hostname** : ホスト（ターゲットとなる受信側）のホスト名。（範囲：1～158 文字。ホスト名の各部分の最大ラベルサイズ：63）。
- **trap** : （任意）このホストに SNMP トラップを送信します（デフォルト）。
- **informs** : （任意）このホストに SNMP インフォームを送信します。伝達は、確認応答を必要とするトラップです。SNMPv1 には適用できません。
- **version 1** : （任意）SNMPv1 トラップが使用されます。
- **version 2c** : （任意）SNMPv2 トラップまたはインフォームが使用されます。
- **version 3** : （任意）SNMPv2 トラップまたはインフォームが使用されます。
- 認証オプションは、SNMP v3 のみに使用できます。次のオプションを使用できます。
  - noauth** : （任意）パケットを認証しないことを指定します。
  - auth** : （任意）暗号化なしでパケットを認証することを指定します。
  - priv** : （任意）暗号化ありでパケットを認証することを指定します。
- **community-string** : 通知操作により送信されるパスワードのようなコミュニティストリング。（範囲：1～20 文字）。v1 および v2 の場合、コミュニティストリングをここに入力できます。v3 の場合、コミュニティストリングは v3 の **snmp-server user** (ISCLI) コマンドに定義されているユーザ名に一致する必要があります。
- **udp-port port** : （任意）使用するホストの UDP ポート。デフォルトは 162 です。（範囲：1～65535）
- **filter filtername** : （任意）このホストのフィルタ。指定しないと、何もフィルタ処理されません。フィルタを定義するには、**snmp-server filter** を使用します（コマンドの特定の順序をユーザが意識する必要はありません）。（範囲：最大 30 文字）



- **timeout seconds** : (任意) (インフォームのみ) インフォームを再送信するまでに確認応答を待機する秒数。デフォルトは 15 秒です。(範囲 : 1 ~ 300)
- **retries retries** : (任意) (インフォームのみ) 生成したメッセージに対する応答を受信しない場合に、インフォーム要求を再送信する最大回数。デフォルトは 3 です。(範囲 : 0 ~ 255)

### デフォルト設定

バージョン : SNMP V1

通知のタイプ : トラップ

udp-port : 162

インフォームを指定した場合、デフォルトの再試行回数は 3 です。

タイムアウト : 15

### コマンドモード

グローバル コンフィギュレーション モード

### 使用上のガイドライン

このコマンドの論理キーは一覧 (ip-address/hostname, traps/informs, version) です。

SNMPv1 または v2 通知の受信者を設定すると、すべての MIB に対してその受信者の通知ビューが自動的に生成されます。

SNMPv3 の場合、ユーザまたは通知ビューは自動的に作成されません。

ユーザまたはグループを作成するには、`snmp-server user (ISCLI)` および `snmp-server group` コマンドを使用します。

### 例

次に、表示された IP アドレスでホストを定義する例を示します。

```
switchxxxxxx(config)# snmp-server host 1.1.1.121 abc
```

## snmp-server engineID local

SNMP v3 のローカル デバイスで SNMP engineID を指定するには、**snmp-server engineID local** グローバル コンフィギュレーション モード コマンドを使用します。このエンジン ID を削除するには、このコマンドの **no** 形式を使用します。

### 構文

**snmp-server engineID local** {*engineid-string* | *default*}

**no snmp-server engineID local**

### パラメータ

- **engineid-string** : エンジン ID を識別する連結 16 進数文字を指定します。16 進数文字列の各バイトは、2 桁の 16 進数です。バイトは、ピリオドまたはコロンで区切られます。16 進数の奇数を入力すると、その文字列にプレフィックスとして数字 0 が自動的に付与されます。（長さ：5 ~ 32 文字、9 ~ 64 16 進数）
- **default** : デバイスの MAC アドレスに基づいてエンジン ID が自動的に作成されることを指定します。

### デフォルト設定

デフォルトのエンジン ID は、規格に従って次のように定義されています。

- 最初の 4 オクテット : 最初のビット = 1、残りの部分は割り当てられた IANA エンタープライズ番号。
- 5 番目のオクテット : 後に MAC アドレスが続くことを示すために 3 に設定されます。
- 最後 6 番目のオクテット : デバイスの MAC アドレス。

### コマンドモード

グローバル コンフィギュレーション モード

### 使用上のガイドライン

SNMPv3 を使用するには、デバイスにエンジン ID を指定する必要があります。任意の ID を指定したり、デフォルトの文字列（デバイスの MAC アドレスを使用して生成されたもの）を使用したりできます。

エンジン ID は管理ドメイン内で一意である必要があるため、次のガイドラインが推奨されます。

- デフォルト以外の EngineID を設定し、管理ドメイン内で一意であることを確認します。
- **snmpEngineID** の値を変更または削除すると、SNMPv3 ユーザデータベースが削除されません。

- SNMP エンジン ID は、すべて 0x0 やすべて 0xF や 0x00000001 にすることはできません。

#### 例

次の例では、デバイスで SNMPv3 を有効にし、デバイスのローカルエンジン ID をデフォルト値に設定しています。

```
switchxxxxxx(config)# snmp-server engineid local default
The engine-id must be unique within your administrative domain.
Do you wish to continue? [Y/N]Y
The SNMPv3 database will be erased. Do you wish to continue? [Y/N]Y
```

## snmp-server engineID remote

リモート SNMP デバイスの SNMP エンジン ID を指定するには、**snmp-server engineID remote** グローバル コンフィギュレーション モード コマンドを使用します。設定したエンジン ID を削除するには、このコマンドの **no** 形式を使用します。

### 構文

**snmp-server engineID remote** *ip-address engineid-string*

**no snmp-server engineID remote** *ip-address*

### パラメータ

- **ip-address** : リモート デバイスの IPv4、IPv6 または IPv6z アドレス。
- **engineid-string** : エンジン ID を識別する文字列。エンジン ID は、連結した 16 進文字列です。16 進数文字列の各バイトは、2 桁の 16 進数です。各バイトは、ピリオドまたはコロンで区切ることができます。ユーザが 16 進数の奇数を入力すると、16 進文字列に自動的にプレフィックスとして 0 が付与されます。（範囲 : engineid-string : 5 ~ 32 文字。9 ~ 64 16 進数）

### デフォルト設定

リモート エンジン ID は、デフォルトでは設定されません。

### コマンドモード

グローバル コンフィギュレーション モード

### 使用上のガイドライン

リモート エンジン ID は、SNMP バージョン 3 インフォームが設定されている場合に必要です。リモート エンジン ID は、リモート ホスト上のユーザに送信されるパケットを認証して暗号化するためのセキュリティ ダイジェストを計算する場合に使用します。

### 例

```
switchxxxxxx(config)# snmp-server engineID remote 1.1.1.1 11:AB:01:CD:23:44
```

# show snmp engineID

ローカル SNMP エンジン ID を表示するには、**show snmp engineID** 特権 EXEC モード コマンドを使用します。

## 構文

**show snmp engineID**

## パラメータ

このコマンドには引数またはキーワードはありません。

## コマンドモード

特権 EXEC モード

## 例

次に、SNMP エンジン ID を表示する例を示します。

```
switchxxxxxx# show snmp engineID
```

```
Local SNMP engineID: 08009009020C0B099C075878
```

```
IP address Remote SNMP engineID
```

```
-----
```

```
172.16.1.1 08009009020C0B099C075879
```

## snmp-server enable traps

デバイスが SNMP トラップを送信できるようにするには、**snmp-server enable traps** グローバルコンフィギュレーションモードコマンドを使用します。すべての SNMP トラップを無効にするには、このコマンドの **no** 形式を使用します。

### 構文

**snmp-server enable traps**

**no snmp-server enable traps**

### デフォルト設定

SNMP トラップは有効になっています。

### コマンドモード

グローバル コンフィギュレーション モード

### 使用上のガイドライン

**no snmp-server enable traps** を入力した場合、例に示すように、[snmp-server trap authentication \(31 ページ\)](#) を使用して失敗トラップを有効にすることができます。

### 例

次の例では、SNMP 失敗トラップを除き、SNMP トラップを有効にしています。

```
switchxxxxxxx(config)# snmp-server enable traps  
switchxxxxxxx(config)# no snmp-server trap authentication
```

# snmp-server trap authentication

認証が失敗したときにデバイスが SNMP トラップを送信できるようにするには、**snmp-server trap authentication** グローバル コンフィギュレーション モード コマンドを使用します。SNMP 失敗認証トラップを無効にするには、このコマンドの **no** 形式を使用します。

## 構文

**snmp-server trap authentication**

**no snmp-server trap authentication**

## パラメータ

このコマンドには引数またはキーワードはありません。

## デフォルト設定

SNMP 失敗認証トラップは有効になっています。

## コマンドモード

グローバル コンフィギュレーション モード

## 例

次の例では、すべての SNMP トラップを無効にし、失敗認証トラップのみを有効にしています。

```
switchxxxxxx(config)# no snmp-server enable traps  
switchxxxxxx(config)# snmp-server trap authentication
```

## snmp-server contact

システム接点 (sysContact) 文字列の値を設定するには、**snmp-server contact** グローバル コンフィギュレーション モード コマンドを使用します。システム接点情報を削除するには、このコマンドの **no** 形式を使用します。

### 構文

**snmp-server contact** *text*

**no snmp-server contact**

### パラメータ

**text** : システム接点情報を指定します。(長さ : 1 ~ 160 文字)

### デフォルト設定

なし

### コマンドモード

グローバル コンフィギュレーション モード

### 例

次の例では、システム接点情報を `Technical_Support` に設定しています。

```
switchxxxxxx(config)# snmp-server contact Technical_Support
```



## snmp-server location

システム ロケーション スtring の値を設定するには、**snmp-server location** グローバル コンフィギュレーション モード コマンドを使用します。位置の String を削除するには、このコマンドの **no** 形式を使用します。

### 構文

**snmp-server location** *text*

**no snmp-server location**

### パラメータ

**text** : システムのロケーション情報を指定します。(長さ : 1 ~ 160 文字)

### デフォルト設定

なし

### コマンドモード

グローバル コンフィギュレーション モード

### 例

次の例では、デバイス ロケーションを `New_York` に設定しています。

```
switchxxxxxx(config)# snmp-server location New_York
```

## snmp-server set

対応する CLI コマンドがないアクションを MIB が実行する場合にコンフィギュレーションファイルに SNMP MIB コマンドを定義するには、**snmp-server set** グローバルコンフィギュレーションモードコマンドを使用します。

### 構文

**snmp-server set** *variable-name name value [name2 value2...]*

### パラメータ

- **variable-name** : SNMP MIB 変数名を指定します。これは、有効な文字列である必要があります。
- **name value** : 名前と値のペアの一覧を指定します。それぞれの名前と値は、有効な文字列である必要があります。スカラー MIB の場合、単一の名前と値のペアのみが存在します。テーブルのエントリの場合、名前と値のペアが 1 つ以上あり、その後には 1 つ以上のフィールドが続きます。

### コマンドモード

グローバル コンフィギュレーション モード

### 使用上のガイドライン

CLI では必要に応じてどのような設定でも設定できますが、同等の CLI コマンドがない MIB 変数を SNMP ユーザが設定するという場合もあります。

### 例

次の例では、スカラー MIB `sysName` を値 `TechSupp` で設定しています。

```
switchxxxxxx(config)# snmp-server set sysName sysname TechSupp
```

## snmp trap link-status

SNMP トラップのリンク ステータス生成を有効にするには、**snmp trap link-status** インターフェイス コンフィギュレーションモード コマンドを使用します。SNMP トラップのリンク ステータス生成を無効にするには、このコマンドの **no** 形式を使用します。

### 構文

**snmp trap link-status**

**no snmp trap link-status**

### パラメータ

このコマンドには引数またはキーワードはありません。

### デフォルト設定

SNMP リンク ステータス トラップの生成は有効になっています。

### コマンドモード

インターフェイス コンフィギュレーションモード

### 例

次の例では、SNMP リンク ステータス トラップの生成を無効にしています。

```
switchxxxxxx(config)# interface gil/0/1  
switchxxxxxx(config-if)# # no snmp trap link-status
```

# show snmp

SNMP ステータスを表示するには、**show snmp** 特権 EXEC モード コマンドを使用します。

## 構文

**show snmp**

## パラメータ

このコマンドには、引数またはキーワードはありません。

## デフォルト設定

なし

## コマンドモード

特権 EXEC モード

## 例

次に、SNMP 通信ステータスを表示する例を示します。

```
switchxxxxxx# show snmp
SNMP is enabled
SNMP traps Source IPv4 interface: vlan 1
SNMP informs Source IPv4 interface: vlan 11
SNMP traps Source IPv6 interface: vlan 10
SNMP informs Source IPv6 interface:
```

Community-String -----	Community-Access -----	View name -----	IP Address -----	Mask ----
public	read only	user-view	All	
private	read write	Default	172.16.1.1/10	
private	su	DefaultSuper	172.16.1.1	

  

Community-string -----	Group name -----	IP Address -----	Mask	Type -----
public	user-group	All		Router

```
Traps are enabled.
Authentication trap is enabled.
Version 1,2 notifications
```

Target Address -----	Type ----	Community -----	Version -----	UDP Port ----	Filter Name -----	TO Sec ---	Retries -----
192.122.173.42	Trap	public	2	----	-----	---	3
192.122.173.42	Inform	public	2	162 162	-----	15 15	3

```
Version 3 notifications
```

Target Address	Type	Username	Security Level	UDP Port	Filter name	TO Sec	Retries
----- 192.122.173.42	---- Inform	----- Bob	----- Priv	---- 162	-----	--- 15	----- 3
System Contact: Robert System Location: Marketing							

次の表に、この出力で表示される重要なフィールドの説明を示します。

フィールド	説明
Community-string	SNMP へのアクセスを許可するコミュニティ アクセス ストリング。
Community-access	許可されているアクセス タイプ：読み取り専用、読み取り/書き込み、スーパー アクセス。
IP Address	管理ステーション IP アドレス。
Target Address	ターゲットとなる受信側の IP アドレス。
Version	送信されたトラップの SNMP バージョン。



## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。