



## SNMP の設定

---

この章は、次の項で構成されています。

- [SNMP に関する情報, on page 1](#)
- [SNMP の注意事項および制約事項, on page 6](#)
- [SNMP のデフォルト設定, on page 6](#)
- [SNMP の設定 \(7 ページ\)](#)
- [SNMP ローカル エンジン ID の設定, on page 19](#)
- [SNMP のディセーブル化 \(20 ページ\)](#)
- [SNMP 設定の確認, on page 21](#)

## SNMP に関する情報

簡易ネットワーク管理プロトコル (SNMP) は、SNMP マネージャとエージェント間の通信用メッセージフォーマットを提供する、アプリケーションレイヤプロトコルです。SNMP では、ネットワーク内のデバイスのモニタリングと管理に使用する標準フレームワークと共通言語が提供されます。

## SNMP 機能の概要

SNMP フレームワークは 3 つの部分で構成されます。

- **SNMP マネージャ** : SNMP を使用してネットワークデバイスのアクティビティを制御し、モニタリングするシステム
- **SNMP エージェント** : デバイスのデータを維持し、必要に応じてこれらのデータを管理システムに報告する、管理対象デバイス内のソフトウェア コンポーネント。Cisco Nexus デバイスはエージェントおよび MIB をサポートします。SNMP エージェントをイネーブルにするには、マネージャとエージェントの関係を定義する必要があります。
- **MIB (Management Information Base; 管理情報ベース)** : SNMP エージェントの管理対象オブジェクトの集まり



**Note** Cisco NX-OS は、イーサネット MIB の SNMP セットをサポートしません。

Cisco Nexus デバイスは、SNMPv1、SNMPv2c、および SNMPv3 をサポートします。SNMPv1 および SNMPv2c はどちらも、コミュニティベース形式のセキュリティを使用します。

SNMP は、RFC 3410 (<http://tools.ietf.org/html/rfc3410>)、RFC 3411 (<http://tools.ietf.org/html/rfc3411>)、RFC 3412 (<http://tools.ietf.org/html/rfc3412>)、RFC 3413 (<http://tools.ietf.org/html/rfc3413>)、RFC 3414 (<http://tools.ietf.org/html/rfc3414>)、RFC 3415 (<http://tools.ietf.org/html/rfc3415>)、RFC 3416 (<http://tools.ietf.org/html/rfc3416>)、RFC 3417 (<http://tools.ietf.org/html/rfc3417>)、RFC 3418 (<http://tools.ietf.org/html/rfc3418>)、および RFC 3584 (<http://tools.ietf.org/html/rfc3584>) で定義されています。

## SNMP 通知

SNMP の重要な機能の 1 つは、SNMP エージェントから通知を生成できることです。これらの通知では、要求を SNMP マネージャから送信する必要はありません。通知は、不正なユーザ認証、再起動、接続の切断、隣接ルータとの接続の切断、その他の重要なイベントを表示します。

Cisco NX-OS は、トラップまたはインフォームとして SNMP 通知を生成します。トラップは、エージェントからホスト レシーバテーブルで指定された SNMP マネージャに送信される、非同期の非確認応答メッセージです。インフォームは、SNMP エージェントから SNMP マネージャに送信される非同期メッセージで、マネージャは受信したという確認応答が必要です。

トラップの信頼性はインフォームより低くなります。SNMP マネージャはトラップを受信しても確認応答 (ACK) を送信しないからです。このため、トラップが受信されたかどうかをスイッチが判断できません。インフォーム要求を受信する SNMP マネージャは、SNMP 応答プロトコルデータユニット (PDU) でメッセージの受信を確認応答します。Cisco Nexus デバイスが応答を受信しない場合、インフォーム要求を再び送信できます。

複数のホスト レシーバーに通知を送信するよう Cisco NX-OS を設定できます。

## SNMPv3

SNMPv3 は、ネットワーク経由のフレームの認証と暗号化を組み合わせることによって、デバイスへのセキュアアクセスを実現します。SNMPv3 が提供するセキュリティ機能は次のとおりです。

- メッセージの完全性：パケットが伝送中に改ざんされていないことを保証します。
- 認証：メッセージのソースが有効かどうかを判別します。
- 暗号化：許可されていないソースにより判読されないように、パケットの内容のスクランブルを行います。

SNMPv3 では、セキュリティ モデルとセキュリティ レベルの両方が提供されています。セキュリティ モデルは、ユーザおよびユーザが属するロールを設定する認証方式です。セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティ モデルとセキュリティ レベルの組み合わせにより、SNMP パケット処理中に採用されるセキュリティ メカニズムが決まります。

## SNMPv1、SNMPv2、SNMPv3 のセキュリティ モデルおよびセキュリティ レベル

セキュリティ レベルは、SNMP メッセージを開示から保護する必要があるかどうか、およびメッセージを認証するかどうか判断します。セキュリティ モデル内のさまざまなセキュリティ レベルは、次のとおりです。

- noAuthNoPriv : 認証または暗号化を実行しないセキュリティ レベル。このレベルは、SNMPv3 ではサポートされていません。
- authNoPriv : 認証は実行するが、暗号化を実行しないセキュリティ レベル。
- authPriv : 認証と暗号化両方を実行するセキュリティ レベル。

SNMPv1、SNMPv2c、および SNMPv3 の 3 つのセキュリティ モデルを使用できます。セキュリティ モデルとセキュリティ レベルの組み合わせにより、SNMP メッセージの処理中に適用されるセキュリティ メカニズムが決まります。

**Table 1: SNMP セキュリティ モデルおよびセキュリティ レベル**

モデル	レベル	認証	暗号化	結果
v1	noAuthNoPriv	コミュニティ ストリング	なし	コミュニティ ストリングの照合を使用して認証します。
v2c	noAuthNoPriv	コミュニティ ストリング	なし	コミュニティ ストリングの照合を使用して認証します。

モデル	レベル	認証	暗号化	結果
v3	authNoPriv	HMAC-MD5 または HMAC-SHA	未対応	Hash-Based Message Authentication Code (HMAC) メッセージダイジェスト 5 (MD5) アルゴリズムまたは HMAC Secure Hash Algorithm (SHA) アルゴリズムに基づいて認証します。
v3	authPriv	HMAC-MD5 または HMAC-SHA	DES	HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムに基づいて認証します。データ暗号規格 (DES) の 56 ビット暗号化、および暗号ブロック連鎖 (CBC) DES (DES-56) 標準に基づいて認証します。

## ユーザベースのセキュリティ モデル

SNMPv3 ユーザーベースセキュリティ モデル (USM) は SNMP メッセージレベルセキュリティを参照し、次のサービスを提供します。

- メッセージの完全性：メッセージが不正な方法で変更または破壊されず、データシーケンスが悪意なく起こり得る範囲を超えて変更されていないことを保証します。
- メッセージの発信元の認証：データを受信したユーザーが提示した ID の発信元を確認します。
- メッセージの機密性：情報が使用不可であること、または不正なユーザ、エンティティ、またはプロセスに開示されないことを保証します。

SNMPv3 は、設定済みユーザによる管理動作のみを許可し、SNMP メッセージを暗号化します。

Cisco NX-OSは、次の 2 つの SNMPv3 認証プロトコルを使用します。

- HMAC-MD5-96 認証プロトコル
- HMAC-SHA-96 認証プロトコル

Cisco NX-OS は、SNMPv3 メッセージ暗号化用プライバシープロトコルの1つとして、Advanced Encryption Standard (AES) を使用し、RFC 3826 に準拠します。

**priv** オプションで、SNMP セキュリティ暗号化方式として、DES または 128 ビット AES 暗号化を選択できます。**priv** オプションと **aes-128** トークンを併用すると、このプライバシーパスワードは 128 ビットの AES キー番号を生成するためのパスワードになります。AES **priv** パスワードは、8 文字以上の長さにできます。パスフレーズをクリアテキストで指定する場合、最大 64 文字を指定できます。ローカライズドキーを使用する場合は、最大 130 文字を指定できます。



---

**Note** 外部の AAA サーバーを使用して SNMPv3 を使う場合、外部 AAA サーバーのユーザー設定でプライバシープロトコルに AES を指定する必要があります。

---

## CLI および SNMP ユーザの同期

SNMPv3 ユーザ管理は、Access Authentication and Accounting (AAA) サーバレベルで集中化できます。この中央集中型ユーザ管理により、Cisco NX-OS の SNMP エージェントは AAA サーバのユーザ認証サービスを利用できます。ユーザ認証が検証されると、SNMP PDU の処理が進行します。AAA サーバはユーザグループ名の格納にも使用されます。SNMP はグループ名を使用して、スイッチでローカルに使用できるアクセスポリシーまたはロールポリシーを適用します。

ユーザグループ、ロール、またはパスワードの設定が変更されると、SNMP と AAA の両方のデータベースが同期化されます。

Cisco NX-OS は、次のようにユーザー設定を同期化します。

- **snmp-server user** コマンドで指定された **auth** パスフレーズは、CLI ユーザーのパスワードになります。
- **username** コマンドで指定されたパスワードは、SNMP ユーザーの **auth** および **priv** パスフレーズになります。
- SNMP または CLI を使用してユーザを作成または削除すると、SNMP と CLI の両方でユーザが作成または削除されます。
- ユーザとロールの対応関係の変更は、SNMP と CLI で同期化されます。
- ロール変更 (CLI からの削除または変更) は、SNMP と同期化されます。



---

**Note** パスフレーズまたはパスワードをローカライズしたキーおよび暗号形式で設定した場合、Cisco NX-OS はユーザー情報 (パスワード、ルールなど) を同期させません。

---

## グループベースの SNMP アクセス



**Note** グループは業界全体で使用されている標準的な SNMP 用語なので、SNMP に関する説明では、「ロール」ではなく「グループ」を使用します。

SNMP アクセス権は、グループ別に編成されます。SNMP 内の各グループは、CLI を使用する場合のロールに似ています。各グループは3つのアクセス権により定義されます。つまり、読み取りアクセス、書き込みアクセス、および通知アクセスです。それぞれのアクセスを、各グループでイネーブルまたはディセーブルに設定できます。

ユーザ名が作成され、ユーザのロールが管理者によって設定され、ユーザがそのロールに追加されていれば、そのユーザはエージェントとの通信を開始できます。

## SNMP の注意事項および制約事項

SNMP には、次の注意事項および制限事項があります。

- アクセス コントロール リスト (ACL) は、スイッチに設定されたローカル SNMPv3 ユーザのみに適用できます。ACL は、認証、許可、アカウントティング (AAA) サーバに保存されるリモート SNMPv3 ユーザに適用できません。
- Cisco NX-OS は、イーサネット MIB への読み取り専用アクセスをサポートします。詳細については次の URL <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml> にアクセスして、Cisco NX-OS の MIB サポート リストを参照してください。
- Cisco NX-OS は、SNMPv3 noAuthNoPriv セキュリティ レベルをサポートしていません。
- Cisco NX-OS Release 7.0(3)I6(1) から以前のリリースへの無停止ダウングレードパスを行う場合、ローカル エンジン ID を設定していたなら、ローカル エンジン ID の設定を戻してから、SNMP ユーザとコミュニティ文字列を再設定する必要があります。
- Cisco Nexus 3000 シリーズ スイッチは、要求に対して最大 10000 個のフラッシュ ファイルをサポートします。

## SNMP のデフォルト設定

Table 2: デフォルトの SNMP パラメータ

パラメータ	デフォルト
ライセンス通知	イネーブル
linkUp/Down 通知タイプ	ietf-extended

# SNMP の設定

## SNMP 送信元インターフェイスの設定

特定のインターフェイスを使用するように SNMP を設定できます。

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル設定モードを開始します。
ステップ 2	switch(config)# <b>snmp-server source-interface {inform   trap} type slot/port</b>	すべての SNMP パケットの送信元インターフェイスを設定します。次のリストに、 <i>interface</i> として有効な値を示します。 <ul style="list-style-type: none"> <li>• ethernet</li> <li>• loopback</li> <li>• mgmt</li> <li>• port-channel</li> <li>• vlan</li> </ul>
ステップ 3	switch(config)# <b>show snmp source-interface</b>	設定済みの SNMP 送信元インターフェイスを表示します。

### 例

次に、SNMP 送信元インターフェイスを設定する例を示します。

```
switch(config)# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server source-interface inform ethernet 1/10
switch(config)# snmp-server source-interface trap ethernet 1/10
switch(config)# show snmp source-interface
```

```
-----
Notification                source-interface
-----
trap                        Ethernet1/10
inform                      Ethernet1/10
-----
```

## SNMP ユーザの設定



**Note** Cisco NX-OS で SNMP ユーザーを設定するために使用するコマンドは、Cisco IOS でユーザーを設定するために使用されるものとは異なります。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	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	<pre>switch(config)# snmp-server user name [auth {md5   sha} passphrase [auto] [priv [aes-128] passphrase] [engineID id] [localizedkey]]</pre> <b>Example:</b> <pre>switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh</pre>	認証およびプライバシー パラメータのある SNMP ユーザを設定します。 パスフレーズには最大 64 文字の英数字を使用できます。大文字と小文字が区別されます。 <b>localizedkey</b> キーワードを使用する場合は、パスフレーズに大文字と小文字を区別した英数字を 130 文字まで使用できます。 <b>engineID</b> の形式は、12 桁のコロンで区切った 10 進数字です。
ステップ 3	(Optional) <b>switch# show snmp user</b> <b>Example:</b> <pre>switch(config) # show snmp user</pre>	1 人または複数の SNMP ユーザーに関する情報を表示します。
ステップ 4	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

### Example

次に、SNMP ユーザーを設定する例を示します。

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh
```



## SNMP メッセージ暗号化の適用

着信要求に認証または暗号化が必要となるよう SNMP を設定できます。デフォルトでは、SNMP エージェントは認証および暗号化を行わないでも SNMPv3 メッセージを受け付けます。プライバシーを適用する場合、Cisco NX-OS は、**noAuthNoPriv** または **authNoPriv** のいずれかのセキュリティ レベル パラメータを使用するすべての SNMPv3 PDU 要求に対して、許可エラーで応答します。

SNMP メッセージの暗号化を特定のユーザーに強制するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
switch(config)# <b>snmp-server user name enforcePriv</b>	このユーザーに対して SNMP メッセージ暗号化を適用します。

SNMP メッセージの暗号化をすべてのユーザーに強制するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
switch(config)# <b>snmp-server globalEnforcePriv</b>	すべてのユーザーに対して SNMP メッセージ暗号化を適用します。

## SNMPv3 ユーザに対する複数のロールの割り当て

SNMP ユーザーを作成した後で、そのユーザーに複数のロールを割り当てることができます。



**Note** 他のユーザーにロールを割り当てることができるのは、**network-admin** ロールに属するユーザーだけです。

コマンド	目的
switch(config)# <b>snmp-server user name group</b>	この SNMP ユーザーと設定されたユーザー ロールをアソシエートします。

## SNMP コミュニティの作成

SNMPv1 または SNMPv2c の SNMP コミュニティを作成できます。

コマンド	目的
switch(config)# <b>snmp-server community name group {ro   rw}</b>	SNMP コミュニティ スtring を作成します。

## SNMP 要求のフィルタリング

アクセス コントロール リスト (ACL) をコミュニティに割り当てて、着信 SNMP 要求にフィルタを適用できます。割り当てた ACL により着信要求パケットが許可される場合、SNMP はその要求を処理します。ACL により要求が拒否される場合、SNMP はその要求を廃棄して、システム メッセージを送信します。

ACL は次のパラメータで作成します。

- 送信元 IP アドレス
- 宛先 IP アドレス
- 送信元ポート
- 宛先ポート
- プロトコル (UDP または TCP)

ACL は、UDP および TCP を介する IPv4 および IPv6 の両方に適用されます。ACL を作成したら、ACL を SNMP コミュニティに割り当てます。



**ヒント** ACL の作成の詳細については、使用している Cisco Nexus シリーズ ソフトウェアの NX-OS セキュリティ コンフィギュレーション ガイドを参照してください。

ACL をコミュニティに割り当てて SNMP 要求をフィルタするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
<pre>switch(config)# snmp-server community <i>community name</i> use-acl <i>acl-name</i></pre> <p><b>Example:</b></p> <pre>switch(config)# snmp-server community public use-acl my_acl_for_public</pre>	SNMP コミュニティに IPv4 ACL または IPv6 ACL を割り当てて SNMP 要求をフィルタします。

## SNMP 通知レシーバの設定

複数のホスト レシーバーに対して SNMP 通知を生成するよう Cisco NX-OS を設定できます。

グローバル コンフィギュレーション モードで SNMPv1 トラップのホスト レシーバを設定できます。

コマンド	目的
switch(config)# <b>snmp-server host</b> <i>ip-address</i> <b>traps version 1</b> <i>community</i> [ <b>udp_port number</b> ]	SNMPv1 トラップのホスト レシーバを設定します。 <i>ip-address</i> は IPv4 または IPv6 アドレスを使用できます。 コミュニティは、最大 255 文字の英数字で指定できます。 UDP ポート番号の範囲は 0 ~ 65535 です。

グローバルコンフィギュレーションモードで SNMPv2c トラップまたはインフォームのホストレシーバを設定できます。

コマンド	目的
switch(config)# <b>snmp-server host</b> <i>ip-address</i> { <b>traps</b>   <b>informs</b> } <b>version 2c</b> <i>community</i> [ <b>udp_port number</b> ]	SNMPv2c トラップまたはインフォームのホストレシーバを設定します。 <i>ip-address</i> は IPv4 または IPv6 アドレスを使用できます。 コミュニティは、最大 255 文字の英数字で指定できます。 UDP ポート番号の範囲は 0 ~ 65535 です。

グローバルコンフィギュレーションモードで SNMPv3 トラップまたはインフォームのホストレシーバを設定できます。

コマンド	目的
switch(config)# <b>snmp-server host</b> <i>ip-address</i> { <b>traps</b>   <b>informs</b> } <b>version 3</b> { <b>auth</b>   <b>noauth</b>   <b>priv</b> } <i>username</i> [ <b>udp_port number</b> ]	SNMPv2c トラップまたはインフォームのホストレシーバを設定します。 <i>ip-address</i> は IPv4 または IPv6 アドレスを使用できます。 ユーザー名は、最大 255 文字の英数字で指定できます。 UDP ポート番号の範囲は 0 ~ 65535 です。



**Note** SNMP マネージャは、SNMPv3 メッセージを認証し暗号解除するため、Cisco Nexus デバイスの SNMP engineID に基づくユーザー クレデンシャル (authKey/PrivKey) を認識していなければなりません。

次に、SNMPv1 トラップのホスト レシーバを設定する例を示します。

```
switch(config)# snmp-server host 192.0.2.1 traps version 1 public
```

次に、SNMPv2 インフォームのホスト レシーバを設定する例を示します。

```
switch(config)# snmp-server host 192.0.2.1 informs version 2c public
```

次に、SNMPv3 インフォームのホスト レシーバを設定する例を示します。

```
switch(config)# snmp-server host 192.0.2.1 informs version 3 auth NMS
```

## VRF を使用する SNMP 通知レシーバの設定

設定された VRF をホスト レシーバに接続するように Cisco NX-OS を設定できます。SNMP 通知レシーバの VRF 到達可能性およびフィルタリング オプションを設定すると、SNMP によって CISCO-SNMP-TARGET-EXT-MIB の cExtSnmptargetVrfTable にエントリが追加されます。



(注) VRF 到達可能性またはフィルタリング オプションを設定する前に、ホストを設定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	switch# <b>configure terminal</b>	グローバル設定モードを開始します。
ステップ 2	switch# <b>snmp-server host ip-address use-vrf vrf_name [ udp_port number]</b>	特定の VRF を使用してホスト レシーバと通信するように SNMP を設定します。IP アドレスは、IPv4 または IPv6 アドレスを使用できます。VRF 名には最大 255 の英数字を使用できます。UDP ポート番号の範囲は 0 ~ 65535 です。このコマンドによって、CISCO-SNMP-TARGET-EXT-MB の ExtSnmptargetVrfTable にエントリが追加されます。
ステップ 3	(任意) switch(config)# <b>copy running-config startup-config</b>	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

### 例

次に、IP アドレス 192.0.2.1 の SNMP サーバー ホストを「Blue」という名前の VRF を使用するように設定する例を示します。

```
switch# configuration terminal
switch(config)# snmp-server host 192.0.2.1 use-vrf Blue
switch(config)# copy running-config startup-config
```

## VRF に基づく SNMP 通知のフィルタリング

通知が発生した VRF に基づいて、Cisco NX-OS 通知をフィルタリングするように設定できます。

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル設定モードを開始します。
ステップ 2	switch(config)# <b>snmp-server host</b> <i>ip-address</i> <b>filter-vrf</b> <i>vrf_name</i> [ <b>udp_port</b> <i>number</i> ]	設定された VRF に基づいて、通知ホストレシーバへの通知をフィルタリングします。IP アドレスは、IPv4 または IPv6 アドレスを使用できます。VRF 名には最大 255 の英数字を使用できます。UDP ポート番号の範囲は 0 ~ 65535 です。  このコマンドによって、CISCO-SNMP-TARGET-EXT-MB の ExtSnmptargetVrfTable にエントリが追加されます。
ステップ 3	(任意) switch(config)# <b>copy running-config startup-config</b>	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

## 例

次に、VRF に基づいて SNMP 通知のフィルタリングを設定する例を示します。

```
switch# configuration terminal
switch(config)# snmp-server host 192.0.2.1 filter-vrf Red
switch(config)# copy running-config startup-config
```

## インバンドアクセスのための SNMP の設定

次のものを使用して、インバンドアクセス用に SNMP を設定できます。

- コンテキストのない SNMP v2 の使用：コンテキストにマッピングされたコミュニティを使用できます。この場合、SNMP クライアントはコンテキストについて認識する必要はありません。
- コンテキストのある SNMP v2 の使用：SNMP クライアントはコミュニティ、たとえば、<community>@<context> を指定して、コンテキストを指定する必要があります。
- SNMP v3 の使用：コンテキストを指定できます。

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configuration terminal</b>	グローバル設定モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	<code>switch(config)# snmp-server context context-name vrf vrf-name</code>	管理 VRF またはデフォルト VRF に SNMP コンテキストをマッピングします。カスタム VRF はサポートされません。  名前には最大 32 の英数字を使用できません。
ステップ 3	<code>switch(config)# snmp-server community community-name group group-name</code>	SNMPv2c コミュニティと SNMP コンテキストにマッピングし、コミュニティが属するグループを識別します。名前には最大 32 の英数字を使用できます。
ステップ 4	<code>switch(config)# snmp-server mib community-map community-name context context-name</code>	SNMPv2c コミュニティを SNMP コンテキストにマッピングします。名前には最大 32 の英数字を使用できます。

## 例

次の SNMPv2 の例は、コンテキストに `snmpdefault` という名前のコミュニティをマッピングする方法を示しています。

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server context def vrf default
switch(config)# snmp-server community snmpdefault group network-admin
switch(config)# snmp-server mib community-map snmpdefault context def
switch(config)#
```

次の SNMPv2 の例は、マッピングされていないコミュニティ `comm` を設定し、インバンドアクセスする方法を示しています。

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server context def vrf default
switch(config)# snmp-server community comm group network-admin
switch(config)#
```

次の SNMPv3 の例は、v3 ユーザー名とパスワードを使用する方法を示しています。

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server context def vrf default
switch(config)#
```

## SNMP 通知のイネーブル化

通知をイネーブルまたはディセーブルにできます。通知名を指定しないと、Cisco NX-OSは通知をすべてイネーブルにします。



**Note** **snmp-server enable traps** CLI コマンドを使用すると、設定通知ホスト レシーバによっては、トラップとインフォームの両方をイネーブルにできます。

次の表に、Cisco NX-OS MIB の通知をイネーブルにする CLI コマンドを示します。

**Table 3: SNMP 通知のイネーブル化**

MIB	関連コマンド
すべての通知	<b>snmp-server enable traps</b>
CISCO-ERR-DISABLE-MIB	<b>snmp-server enable traps show interface status</b>
Q-BRIDGE-MIB	<b>snmp-server enable traps show mac address-table</b>
CISCO-SWITCH-QOS-MIB	<b>snmp-server enable traps show hardware internal buffer info pkt-stats</b>
BRIDGE-MIB	<b>snmp-server enable traps bridge newroot</b> <b>snmp-server enable traps bridge topologychange</b>
CISCO-AAA-SERVER-MIB	<b>snmp-server enable traps aaa</b>
ENTITY-MIB、 CISCO-ENTITY-FRU-CONTROL-MIB、 CISCO-ENTITY-SENSOR-MIB	<b>snmp-server enable traps entity</b> <b>snmp-server enable traps entity fru</b>
CISCO-LICENSE-MGR-MIB	<b>snmp-server enable traps license</b>
IF-MIB	<b>snmp-server enable traps link</b>
CISCO-PSM-MIB	<b>snmp-server enable traps port-security</b>
SNMPv2-MIB	<b>snmp-server enable traps snmp</b> <b>snmp-server enable traps snmp authentication</b>
CISCO-FCC-MIB	<b>snmp-server enable traps fcc</b>
CISCO-DM-MIB	<b>snmp-server enable traps fcdomain</b>
CISCO-NS-MIB	<b>snmp-server enable traps fcns</b>
CISCO-FCS-MIB	<b>snmp-server enable traps fcs discovery-complete</b> <b>snmp-server enable traps fcs request-reject</b>
CISCO-FDMI-MIB	<b>snmp-server enable traps fdmi</b>
CISCO-FSPF-MIB	<b>snmp-server enable traps fspf</b>
CISCO-PSM-MIB	<b>snmp-server enable traps port-security</b>

MIB	関連コマンド
CISCO-RSCN-MIB	<b>snmp-server enable traps rscn</b> <b>snmp-server enable traps rscn els</b> <b>snmp-server enable traps rscn ils</b>
CISCO-ZS-MIB	<b>snmp-server enable traps zone</b> <b>snmp-server enable traps zone default-zone-behavior-change</b> <b>snmp-server enable traps zone enhanced-zone-db-change</b> <b>snmp-server enable traps zone merge-failure</b> <b>snmp-server enable traps zone merge-success</b> <b>snmp-server enable traps zone request-reject</b> <b>snmp-server enable traps zone unsupp-mem</b>
CISCO-CONFIG-MAN-MIB  <b>Note</b> ccmCLIRunningConfigChanged 通知を除き、MIB オブジェクトをサポートしていません。	<b>snmp-server enable traps config</b>



**Note** ライセンス通知は、デフォルトではイネーブルです。

グローバル コンフィギュレーション モードで指定の通知をイネーブルにするには、次の作業を行います。

コマンド	目的
switch(config)# <b>snmp-server enable traps</b>	すべての SNMP 通知をイネーブルにします。
switch(config)# <b>snmp-server enable traps aaa [server-state-change]</b>	AAA SNMP 通知をイネーブルにします。
switch(config)# <b>snmp-server enable traps entity [fru]</b>	ENTITY-MIB SNMP 通知をイネーブルにします。
switch(config)# <b>snmp-server enable traps license</b>	ライセンス SNMP 通知をイネーブルにします。
switch(config)# <b>snmp-server enable traps port-security</b>	ポートセキュリティ SNMP 通知をイネーブルにします。
switch(config)# <b>snmp-server enable traps snmp [authentication]</b>	SNMP エージェント通知をイネーブルにします。



## リンクの通知の設定

デバイスに対して、イネーブルにする linkUp/linkDown 通知を設定できます。次のタイプの linkUp/linkDown 通知をイネーブルにできます。

- cieLinkDown : シスコ拡張リンク ステート ダウン通知をイネーブルにします。
- cieLinkUp : シスコ拡張リンク ステート アップ通知をイネーブルにします。
- cisco-xcvr-mon-status-chg : シスコ インターフェイス トランシーバ モニター ステータス変更通知をイネーブルにします。
- delayed-link-state-change : 遅延リンク ステート変更をイネーブルにします。
- extended-linkUp : IETF 拡張リンク ステート アップ通知をイネーブルにします。
- extended-linkDown : IETF 拡張リンク ステート ダウン通知をイネーブルにします。
- linkDown : IETF リンク ステート ダウン通知をイネーブルにします。
- linkUp : IETF リンク ステート アップ通知を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	<b>configure terminal</b> 例 : <pre>switch# configure terminal switch(config)#</pre>	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	<b>snmp-server enable traps link</b> <b>[cieLinkDown   cieLinkUp  </b> <b>cisco-xcvr-mon-status-chg  </b> <b>delayed-link-state-change]  </b> <b>extended-linkUp   extended-linkDown  </b> <b>linkDown   linkUp]</b> 例 : <pre>switch(config)# snmp-server enable traps link cieLinkDown</pre>	リンク SNMP 通知をイネーブルにします。

## インターフェイスでのリンク通知のディセーブル化

個別のインターフェイスで linkUp および linkDown 通知をディセーブルにできます。これにより、フラッピングインターフェイス（アップとダウン間の移行を繰り返しているインターフェイス）に関する通知を制限できます。

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル設定モードを開始します。
ステップ 2	switch(config)# <b>interface</b> <i>type slot/port</i>	変更するインターフェイスを指定します。
ステップ 3	switch(config-if)# <b>no snmp trap link-status</b>	インターフェイスの SNMP リンクステートトラップをディセーブルにします。この機能は、デフォルトでイネーブルにされています。

## TCP での SNMP に対するワンタイム認証のイネーブル化

TCP セッション上で SNMP に対するワンタイム認証をイネーブルにできます。

コマンド	目的
switch(config)# <b>snmp-server tcp-session [auth]</b>	TCP セッション上で SNMP に対するワンタイム認証をイネーブルにします。この機能はデフォルトで無効に設定されています。

## SNMP スイッチの連絡先および場所の情報の割り当て

スイッチの連絡先情報（スペースを含めず、最大 32 文字まで）およびスイッチの場所を割り当てることができます。

## Procedure

	Command or Action	Purpose
ステップ 1	switch# <b>configuration terminal</b>	グローバル設定モードを開始します。
ステップ 2	switch(config)# <b>snmp-server contact</b> <i>name</i>	sysContact (SNMP 担当者名) を設定します。
ステップ 3	switch(config)# <b>snmp-server location</b> <i>name</i>	sysLocation (SNMP ロケーション) を設定します。
ステップ 4	(Optional) switch# <b>show snmp</b>	1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 5	(Optional) switch# <b>copy running-config startup-config</b>	この設定変更を保存します。

## コンテキストとネットワーク エンティティ間のマッピング設定

プロトコルインスタンス、VRF などの論理ネットワーク エンティティに対する SNMP コンテキストのマッピングを設定できます。

### Procedure

	Command or Action	Purpose
ステップ 1	switch# <b>configuration terminal</b>	グローバル設定モードを開始します。
ステップ 2	switch(config)# <b>snmp-server context</b> <i>context-name</i> [ <b>instance</b> <i>instance-name</i> ] [ <b>vrf</b> <i>vrf-name</i> ] [ <b>topology</b> <i>topology-name</i> ]	SNMP コンテキストをプロトコルインスタンス、VRF、またはトポロジにマッピングします。名前には最大 32 の英数字を使用できます。
ステップ 3	switch(config)# <b>snmp-server mib community-map</b> <i>community-name</i> <b>context</b> <i>context-name</i>	SNMPv2c コミュニティを SNMP コンテキストにマッピングします。名前には最大 32 の英数字を使用できます。
ステップ 4	(Optional) switch(config)# <b>no snmp-server context</b> <i>context-name</i> [ <b>instance</b> <i>instance-name</i> ] [ <b>vrf</b> <i>vrf-name</i> ] [ <b>topology</b> <i>topology-name</i> ]	SNMP コンテキストとプロトコルインスタンス、VRF、またはトポロジ間のマッピングを削除します。名前には最大 32 の英数字を使用できます。  <b>Note</b> コンテキストマッピングを削除する目的で、インスタンス、VRF、またはトポロジを入力しないでください。 <b>instance</b> 、 <b>vrf</b> 、または <b>topology</b> キーワードを使用すると、コンテキストとゼロ長ストリング間のマッピングが設定されます。

## SNMP ローカル エンジン ID の設定

Cisco NX-OS リリース 7.0(3)I6(1)以降では、ローカルデバイスにエンジン ID を設定できます。



**Note** SNMP ローカル エンジン ID を設定すると、すべての SNMP ユーザ、V3 ユーザに設定されたホスト、およびコミュニティストリングを再設定する必要があります。Cisco NX-OS リリース 7.0(3)I7(1) 以降では、SNMP ユーザとコミュニティストリングのみを再設定する必要があります。

## Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> switch# configure terminal switch(config)#	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	<b>snmp-server engineID local engineid-string</b> <b>Example:</b> switch(config)# snmp-server engineID local AA:BB:CC:1A:2C:10	ローカル デバイスの SNMP engineID を変更します。  ローカル エンジン ID は、コロンで指定された 16 進数オクテットのリストとして設定する必要があります。ここでは 10 ~ 64 の範囲の偶数 16 進数文字が使用され、2 つの 16 進数文字ごとにコロンで区切られます。たとえば、i80:00:02:b8:04:61:62:63 です。
ステップ 3	<b>show snmp engineID</b> <b>Example:</b> switch(config)# show snmp engineID	設定されている SNMP エンジンの ID を表示します。
ステップ 4	<b>[no] snmp-server engineID local engineid-string</b> <b>Example:</b> switch(config)# no snmp-server engineID local AA:BB:CC:1A:2C:10	ローカル エンジン ID を無効にし、自動生成されたデフォルトのエンジン ID を設定します。
ステップ 5	Required: <b>copy running-config startup-config</b> <b>Example:</b> switch(config)# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

## SNMP のディセーブル化

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> <b>例 :</b> switch# configure terminal switch(config)#	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。

	コマンドまたはアクション	目的
ステップ 2	<pre>switch(config) # no snmp-server protocol enable</pre> <p>例 :</p> <pre>no snmp-server protocol enable</pre>	<p>SNMP をディセーブルにします。</p> <p>SNMP は、デフォルトでディセーブルになっています。</p>

## SNMP 設定の確認

SNMP 設定情報を表示するには、次の作業を行います。

コマンド	目的
<b>show snmp</b>	SNMP ステータスを表示します。
<b>show snmp community</b>	SNMP コミュニティストリングを表示します。
<b>show interface snmp-ifindex</b>	すべてのインターフェイスについて (IF-MIB から) SNMP の ifIndex 値を表示します。
<b>show running-config snmp [all]</b>	SNMP の実行コンフィギュレーションを表示します。
<b>show snmp engineID</b>	SNMP engineID を表示します。
<b>show snmp group</b>	SNMP ロールを表示します。
<b>show snmp sessions</b>	SNMP セッションを表示します。
<b>show snmp context</b>	SNMP コンテキストマッピングを表示します。
<b>show snmp host</b>	設定した SNMP ホストの情報を表示します。
<b>show snmp source-interface</b>	設定した発信元インターフェイスの情報を表示します。
<b>show snmp trap</b>	イネーブルまたはディセーブルである SNMP 通知を表示します。
<b>show snmp user</b>	SNMPv3 ユーザを表示します。



## 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。