



## SNMP の設定

---

この章では、Catalyst 3750 スイッチに SNMP（簡易ネットワーク管理プロトコル）を設定する方法について説明します。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。



(注) この章で使用されるコマンドの構文および使用方法の詳細については、このリリースに対応するスイッチのコマンド リファレンス、および『*Cisco IOS Configuration Fundamentals Command Reference*』 Release 12.1 を参照してください。

---

この章で説明する内容は、次のとおりです。

- [SNMP の概要 \(p.27-2\)](#)
- [SNMP の設定 \(p.27-7\)](#)
- [SNMP ステータスの表示 \(p.27-17\)](#)

## SNMP の概要

SNMP はアプリケーション レイヤ プロトコルで、マネージャとエージェント間の通信用メッセージ形式を規定します。SNMP システムは、SNMP マネージャ、SNMP エージェント、および MIB (管理情報ベース) で構成されます。SNMP マネージャは、CiscoWorks などの Network Management System (NMS; ネットワーク管理システム) の一部に組み入れることができます。エージェントおよび MIB はスイッチ上で動作します。スイッチに SNMP を設定するには、マネージャとエージェント間の関係を定義します。

SNMP エージェントは MIB 変数を格納し、SNMP マネージャは、この変数の値を要求または変更できます。マネージャは、エージェントから値を取得したり、エージェントに値を保管することもできます。エージェントは、デバイス パラメータおよびネットワーク データに関する情報の保管場所である MIB からデータを収集します。また、エージェントはマネージャから要求されるデータ取得または設定に対応します。

エージェントは、非送信請求トラップをマネージャに送信します。トラップとは、ネットワーク上のある状態を SNMP マネージャに通知するメッセージです。トラップは、不正なユーザ認証、再起動、リンクのステータス (アップまたはダウン)、MAC (メディア アクセス制御) アドレス追跡、TCP 接続の切断、ネイバとの接続の切断、その他の重要なイベントを表示します。

Catalyst 3750 では、スイッチ スタック全体の SNMP 要求およびトラップがスタック マスターで処理されます。スタック マスターは、すべてのスタック メンバーに関連する要求またはトラップをトランスペアレントに管理します。新しいスタック マスターが選択されると、新しいマスターが以前のスタック マスターの設定に従って SNMP 要求およびトラップの処理を継続します。SNMP 管理ステーションとの IP 接続は、新しいマスターが制御を引き継いだあとも、有効であるとみなされます。

スイッチ スタックの詳細については、[第 5 章「スイッチ スタックの管理」](#)を参照してください。

ここでは、次の内容について説明します。

- [SNMP のバージョン \(p.27-2\)](#)
- [SNMP マネージャの機能 \(p.27-4\)](#)
- [SNMP エージェントの機能 \(p.27-4\)](#)
- [SNMP コミュニティ スtring \(p.27-4\)](#)
- [SNMP による MIB 変数へのアクセス \(p.27-5\)](#)
- [SNMP 通知 \(p.27-5\)](#)
- [SNMP ifIndex MIB オブジェクト値 \(p.27-6\)](#)

## SNMP のバージョン

このソフトウェア リリースでは、次の SNMP バージョンをサポートしています。

- SNMPv1 SNMP、完全インターネット標準 (RFC 1157 に定義)
- SNMPv2C は、SNMPv2Classic のパーティベース管理およびセキュリティ フレームワークを SNMPv2C のコミュニティ スtring ベース管理フレームワークに置き換えるもので、SNMPv2Classic の一括検索を保持しながら、エラー処理が改良されています。SNMPv2C の機能は次のとおりです。
  - SNMPv2 SNMP のバージョン 2、インターネット標準草案 (RFC 1902 ~ 1907 に定義)
  - SNMPv2C SNMPv2 に対応するコミュニティ スtring ベース管理フレームワーク、実験的インターネット プロトコル (RFC 1901 に定義)
- SNMPv3 SNMP のバージョン 3 は、RFC 2273 ~ 2275 に定義された相互運用可能な標準ベース プロトコルです。SNMPv3 はネットワーク経由でパケットの認証および暗号化を行い、デバイスへの安全なアクセスを実現します。以下のセキュリティ機能が組み込まれています。

- メッセージ整合性 パケットが送信中に不正に変更されないようにします。
- 認証 メッセージの送信元が有効かどうかを判別します。
- 暗号化 パッケージの内容をスクランブルし、不正送信元に読み取られないようにします。



(注) 暗号化を選択する場合は、**priv** キーワードを指定します。このキーワードは、暗号化ソフトウェアイメージがインストールされている場合のみ使用できます。

SNMPv1 と SNMPv2C は、ともにコミュニティベース形式のセキュリティを使用します。エージェントの MIB にアクセスできるマネージャのコミュニティは、IP アドレスのアクセス制御リストとパスワードによって定義されています。

SNMPv2C には、一括検索メカニズムと管理ステーションへのより詳細なエラー メッセージ報告機能が組み込まれています。一括検索メカニズムは表や大量の情報を検索し、必要なラウンドトリップ数を最小限にします。SNMPv2C の改良されたエラー処理には、各種のエラー状況を区別する拡張エラー コードが組み込まれています。エラー状況は、SNMPv1 の単一のエラー コードを使用して報告されます。SNMPv2C のエラー リターン コードが、エラー タイプを報告します。

SNMPv3 は、セキュリティ モデルとセキュリティ レベルの両方を備えています。セキュリティ モデルは、ユーザおよびそのユーザが所属するグループに対して設定する認証方法です。セキュリティ レベルは、1 つのセキュリティ モデルの中で許可されるセキュリティのレベルを表します。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って、SNMP パケットを処理するとき使用するセキュリティ メカニズムが決まります。使用可能なセキュリティ モデルは SNMPv1、SNMPv2C、および SNMPv3 です。

表 27-1 に、セキュリティ モデルおよびセキュリティ レベルをさまざまに組み合わせた場合の特性を示します。

表 27-1 SNMP セキュリティ モデルおよびレベル

モデル	レベル	認証	暗号化	結果
SNMPv1	noAuthNoPriv	コミュニティ スtring	なし	認証にコミュニティ スtringの照合を使用します。
SNMPv2C	noAuthNoPriv	コミュニティ スtring	なし	認証にコミュニティ スtringの照合を使用します。
SNMPv3	noAuthNoPriv	ユーザ名	なし	認証にユーザ名の照合を使用します。
SNMPv3	authNoPriv	MD5 または SHA	なし	HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証を行います。
SNMPv3	authPriv (暗号ソフトウェアイメージが必要)	MD5 または SHA	DES	HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証を行います。 CBC-DES (DES-56) 標準に基づく認証以外に DES 56 ビット暗号化を行います。

管理ステーションがサポートする SNMP のバージョンを使用するには、SNMP エージェントを設定する必要があります。エージェントは複数のマネージャと通信できるため、SNMPv1、SNMPv2C、および SNMPv3 プロトコルによる通信をサポートするようにソフトウェアを設定できます。

## SNMP マネージャの機能

SNMP マネージャは MIB 情報を使用し、表 27-2 に示す動作を実行します。

表 27-2 SNMP の動作

動作	説明
get-request	特定の変数から値を取得します。
get-next-request	テーブル内の変数から値を取得します。 <sup>1</sup>
get-bulk-request <sup>2</sup>	テーブルの複数行など、大きなデータブロックを取得します。小さなデータブロックを何回も送信する必要はありません。
get-response	NMS から送られる get-request、get-next-request、および set-request に応答します。
set-request	特定の変数に値を格納します。
trap	イベントの発生時に、SNMP エージェントから SNMP マネージャに送られる、非送信請求メッセージです。

1. この動作では、SNMP マネージャに正確な変数名を認識させる必要はありません。テーブル内を順に検索し、必要な変数を検出します。
2. *get-bulk* コマンドが機能するのは SNMPv2 以降に限られます。

## SNMP エージェントの機能

SNMP エージェントは、次のように SNMP マネージャの要求に応答します。

- MIB 変数の取得 SNMP エージェントは、NMS からの要求に応答してこの機能を開始します。エージェントは、要求された MIB 変数の値を取得し、その値で NMS に応答します。
- MIB 変数の設定 SNMP エージェントは、NMS からのメッセージに応答してこの機能を開始します。SNMP エージェントは、MIB 変数の値を NMS から要求された値に変更します。

また、SNMP エージェントは非送信請求トラップメッセージを送信し、エージェントで重要なイベントが発生したことを NMS に通知します。トラップ条件の例には、ポートまたはモジュールが起動または停止した場合、スパンニングツリー トポロジの変更が発生した場合、認証障害が発生した場合などがあります。

## SNMP コミュニティ スtring

SNMP コミュニティ スtring は MIB オブジェクトへのアクセスを認証し、内蔵パスワードとして機能します。NMS がスイッチにアクセスするには、NMS 上のコミュニティ スtring の定義が、スイッチ上の 3 つのコミュニティ スtring の定義と 1 つまたは複数一致する必要があります。

コミュニティ スtring は、次のいずれかの属性を持ちます。

- read-only (RO) 許可した管理ステーションに、コミュニティ スtring を除く MIB 内のオブジェクトすべてに対する読み取りアクセス権を与えます。ただし、書き込みアクセスは許可しません。
- read-write (RW) 許可した管理ステーションに、MIB 内のオブジェクトすべてに対する読み取りおよび書き込みアクセス権を与えます。ただし、コミュニティ スtring へのアクセスは許可しません。
- read-write-all 許可した管理ステーションに、コミュニティ スtring も含めた MIB 内のオブジェクトすべてに対する読み取りおよび書き込みアクセス権を与えます。



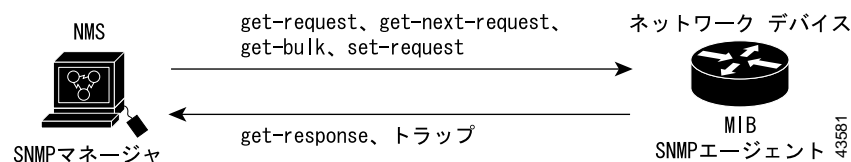
(注) クラスタを作成すると、コマンド スイッチがメンバー スイッチと SNMP アプリケーション間のメッセージ交換を管理します。Cluster Management ソフトウェアは、コマンド スイッチ上で最初に設定された RW および RO コミュニティ スtring にメンバー スイッチ番号 ( *@esN*、*N* はスイッチ番号) を追加し、これらの String をメンバー スイッチに伝達します。詳細については、第 6 章「スイッチのクラスタ設定」を参照してください。

## SNMP による MIB 変数へのアクセス

NMS の一例は、CiscoWorks ネットワーク管理ソフトウェアです。CiscoWorks2000 ソフトウェアは、スイッチの MIB 変数を使用してデバイスの変数を設定し、ネットワーク上のデバイスに対するポーリングを実行して特定の情報を入手します。ポーリング結果は、グラフ形式で表示されます。この結果を分析して、インターネットワーキングに関する問題のトラブルシューティング、ネットワークパフォーマンスの改善、デバイスの設定の確認、トラフィック負荷のモニタなどを行うことができます。

図 27-1 に示すように、SNMP エージェントは MIB からデータを収集します。エージェントは SNMP マネージャに対してトラップ (特定イベントの通知) を送信し、SNMP マネージャはトラップを受信してそれを処理します。トラップは、ネットワーク上で発生した不正なユーザ認証、再起動、リンク ステータス (アップまたはダウン)、MAC アドレス追跡などに関する条件を SNMP マネージャに通知します。SNMP エージェントはさらに、SNMP マネージャから *get-request*、*get-next-request*、および *set-request* 形式で送られる MIB 関連のクエリに応答します。

図 27-1 SNMP ネットワーク



サポートされている MIB とそのアクセス方法については、付録 A「サポートされている MIB」を参照してください。

## SNMP 通知

SNMP を使用すると、スイッチは特定のイベントが発生したときに SNMP マネージャに通知を送信できます。SNMP 通知は、トラップまたはインフォーム要求として送信できます。コマンド構文内に、トラップまたはインフォームを選択するオプションが指定されていない場合、キーワード *traps* はトラップまたはインフォーム、あるいはその両方を表します。SNMP 通知をトラップまたはインフォームのどちらで送信するかを指定するには、*snmp-server host* コマンドを使用します。



(注) SNMPv1 はインフォームをサポートしていません。

レシーバはトラップの受信時に確認応答を送信しないため、トラップは信頼性が低く、送信側はトラップが受信されたかどうかを判別できません。SNMP マネージャはインフォーム要求を受信すると、SNMP 応答 Protocol Data Unit (PDU; プロトコル データ ユニット) を使用してメッセージを確認します。送信側が応答を受信しない場合は、インフォーム要求を再送信します。このため、インフォームの方がトラップよりも目的の宛先に到達する可能性が高くなります。

インフォームはトラップよりも信頼性が高いため、スイッチおよびネットワーク内のリソースの消費量も多くなります。送信後すぐに廃棄されるトラップと異なり、インフォーム要求は応答を受信するか、または要求が時間切れになるまでメモリ内に保持されます。トラップの送信は 1 回限りですが、インフォームは何回も再送信されたり、再試行されることがあります。再試行が繰り返されるとトラフィックが増加し、ネットワークのオーバーヘッドが大きくなるため、トラップおよびインフォームを使用する場合は信頼性とリソースのどちらを重視するかの選択が必要となります。SNMP マネージャですべての通知を受信することが重要な場合はインフォーム要求を使用し、ネットワークトラフィックまたはスイッチのメモリが重要で、通知が必要ない場合は、トラップを使用します。

## SNMP ifIndex MIB オブジェクト値

NMS では、IF-MIB によって interface index (ifIndex) オブジェクト値の生成および割り当てが行われます。この値は、物理または論理インターフェイスを識別する 0 より大きな一意の数です。スイッチが再起動するか、スイッチ ソフトウェアがアップグレードされても、スイッチはインターフェイスで同じ値を使用します。たとえば、スイッチがポート 2 に 10003 の ifIndex 値を割り当てた場合、この値はスイッチの再起動後も変わりません。

スイッチはインターフェイスに ifIndex 値を割り当てた場合に、表 27-3 に記載されている値の 1 つを使用します。

表 27-3 ifIndex 値

インターフェイス タイプ	ifIndex 範囲
SVI <sup>1</sup>	1 ~ 4999
EtherChannel	5000 ~ 5012
ループバック	5013 ~ 5077
トンネル	5078 ~ 5142
物理 (ギガビットイーサネットまたは SFP <sup>2</sup> モジュールインターフェイスなど)	10000 ~ 14500
null	14501

1. SVI = Switch Virtual Interface : スイッチ仮想インターフェイス
2. SFP = Small Form-factor Pluggable



(注) スイッチが範囲内の値を順番に使用するとは限りません。

## SNMP の設定

ここでは、スイッチに SNMP を設定する方法について説明します。具体的な設定情報は次のとおりです。

- [SNMP のデフォルト設定 \( p.27-7 \)](#)
- [SNMP 設定時の注意事項 \( p.27-7 \)](#)
- [SNMP エージェントのディセーブル化 \( p.27-8 \)](#)
- [コミュニティ スtring の設定 \( p.27-8 \)](#)
- [SNMP グループおよびユーザの設定 \( p.27-10 \)](#)
- [SNMP 通知の設定 \( p.27-11 \)](#)
- [エージェント コンタクトおよびロケーションの設定 \( p.27-14 \)](#)
- [SNMP 経由で使用する TFTP サーバの制限 \( p.27-15 \)](#)
- [SNMP の例 \( p.27-15 \)](#)

## SNMP のデフォルト設定

表 27-4 に、SNMP のデフォルト設定を示します。

表 27-4 SNMP のデフォルト設定

機能	デフォルト設定
SNMP エージェント	イネーブル
SNMP コミュニティ スtring	Read-Only : パブリック Read-Write : プライベート Read-Write-all : シークレット
SNMP トラップ レシーバ	設定なし
SNMP トラップ	イネーブルなし
SNMP バージョン	<b>version</b> キーワードを指定しない場合、デフォルトはバージョン 1 です。
SNMPv3 認証	キーワードを指定しない場合、デフォルトは <b>noauth</b> ( noAuthNoPriv ) セキュリティ レベルです。
SNMP 通知タイプ	タイプを指定しない場合、すべての通知が送信されます。

## SNMP 設定時の注意事項

SNMP グループは、SNMP ユーザを SNMP ビューにマッピングするテーブルです。SNMP ユーザは、SNMP グループのメンバーです。SNMP ホストは、SNMP トラップ動作の受信側です。SNMP エンジン **ID** は、ローカルまたはリモート SNMP エンジンの名前です。

SNMP を設定する場合の注意事項は、次のとおりです。

- SNMP グループを設定する場合は、通知ビューを指定しないでください。 **snmp-server host** グローバル コンフィギュレーション コマンドを使用すると、ユーザ用の通知ビューが自動生成され、そのユーザに関連付けられたグループに追加されます。グループの通知ビューを変更すると、そのグループに関連付けられたすべてのユーザに影響を与えます。通知ビューを設定する時期については、『 *Cisco IOS Configuration Fundamentals Command Reference* 』 Release 12.1 を参照してください。

- リモート ユーザを設定するには、ユーザが所属するデバイスのリモート SNMP エージェントの IP アドレスまたはポート番号を指定します。
- 特定のエージェントのリモート ユーザを設定する前に、**snmp-server engineID** グローバル コンフィギュレーション コマンドで **remote** オプションを指定し、SNMP エンジン ID を設定してください。リモート エージェントの SNMP エンジン ID およびユーザ パスワードは、認証およびプライバシー ダイジェストを計算するために使用されます。リモート エンジン ID を先に設定しないと、コンフィギュレーション コマンドは失敗します。
- SNMP インフォームを設定する場合は、SNMP データベース内のリモート エージェントの SNMP エンジン ID を設定してから、プロキシ要求またはインフォームを送信する必要があります。
- SNMP エンジン ID の値を変更すると、重大な悪影響を及ぼします。(コマンドラインから入力した)ユーザのパスワードは、パスワードおよびローカル エンジン ID に基づいて MD5 または SHA セキュリティ ダイジェストに変換されます。コマンドライン パスワードはその後、RFC 2274 の要求に従って破棄されます。この破棄が原因で、エンジン ID の値が変更されると、SNMPv3 ユーザのセキュリティ ダイジェストが無効になるので、**snmp-server user username** グローバル コンフィギュレーション コマンドを使用して SNMP ユーザを再設定しなければなりません。同様に、エンジン ID が変更された場合は、コミュニティ ストリングを再設定する必要があります。

## SNMP エージェントのディセーブル化

SNMP エージェントをディセーブルにするには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	説明
ステップ 1	<b>configure terminal</b>	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>no snmp-server</b>	SNMP エージェントの動作をディセーブルにします。
ステップ 3	<b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 4	<b>show running-config</b>	設定を確認します。
ステップ 5	<b>copy running-config startup-config</b>	(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。

**no snmp-server** グローバル コンフィギュレーション コマンドは、デバイス上で実行されているすべてのバージョン (バージョン 1、バージョン 2C、およびバージョン 3) をディセーブルにします。SNMP をイネーブルにする特定の IOS コマンドはありません。最初に入力する **snmp-server** グローバル コンフィギュレーション コマンドによって、SNMP のすべてのバージョンがイネーブルになります。

## コミュニティ ストリングの設定

SNMP マネージャとエージェント間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 ストリングはパスワードと同様に機能し、スイッチのエージェントへのアクセスを許可します。任意で、ストリングに関連付けられた次の特性を 1 つまたは複数指定することができます。

- エージェントへアクセスするコミュニティ ストリングの使用が許可されている、SNMP マネージャの IP アドレスに関するアクセス リスト。
- MIB ビュー。指定のコミュニティがアクセス可能な全 MIB オブジェクトのサブセットを定義します。
- コミュニティがアクセス可能な MIB オブジェクトの読み取りおよび書き込み権限、または読み取り専用権限。

スイッチ上でコミュニティ スtring を設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	説明
ステップ 1	<i>configure terminal</i>	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	<i>snmp-server community string</i> [ <i>view view-name</i> ] [ <i>ro</i>   <i>rw</i> ] [ <i>access-list-number</i> ]	<p>コミュニティ スtring を設定します。</p> <ul style="list-style-type: none"> <li><i>string</i> には、パスワードのように機能し、SNMP プロトコルへのアクセスを許可する String を指定します。任意の文字数で、1 つまたは複数のコミュニティ スtring を設定できます。</li> <li>(任意) <i>view</i> には、コミュニティがアクセス可能なビュー レコードを指定します。</li> <li>(任意) 許可した管理ステーションに MIB オブジェクトを検索させる場合は読み取り専用 (<i>ro</i>)、MIB オブジェクトを検索して変更させる場合は読み取り / 書き込み (<i>rw</i>) を指定します。デフォルトでは、コミュニティ スtring はすべてのオブジェクトへの読み取り専用アクセスを許可します。</li> <li>(任意) <i>access-list-number</i> には、1 ~ 99 および 1300 ~ 1999 の範囲で標準の IP アクセス リスト番号を入力します。</li> </ul>
ステップ 3	<i>access-list access-list-number</i> { <i>deny</i>   <i>permit</i> } <i>source</i> [ <i>source-wildcard</i> ]	<p>(任意) ステップ 2 で標準の IP アクセス リスト番号を指定した場合はリストを作成し、必要な回数だけこのコマンドを繰り返します。</p> <ul style="list-style-type: none"> <li><i>access-list-number</i> には、ステップ 2 で指定したアクセス リスト番号を入力します。</li> <li><i>deny</i> キーワードを指定すると、条件が一致した場合にアクセスが拒否されます。<i>permit</i> キーワードを指定すると、条件が一致した場合にアクセスが許可されます。</li> <li><i>source</i> には、エージェントへアクセスするコミュニティ スtring の使用が許可されている SNMP マネージャの IP アドレスを入力します。</li> <li>(任意) <i>source-wildcard</i> を指定する場合は、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置に 1 を配置します。</li> </ul> <p>アクセス リストの末尾には、すべてに適用される暗黙の拒否ステートメントが常に存在することに注意してください。</p>
ステップ 4	<i>end</i>	イネーブル EXEC モードに戻ります。
ステップ 5	<i>show running-config</i>	設定を確認します。
ステップ 6	<i>copy running-config startup-config</i>	(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。



(注) SNMP コミュニティのアクセスをディセーブルにするには、そのコミュニティに対するコミュニティ スtring をヌル String に設定します (コミュニティ スtring に値を入力しない)。

特定のコミュニティ スtring を削除するには、*no snmp-server community string* グローバル コンフィギュレーション コマンドを使用します。


次に、SNMP にストリング **comaccess** を割り当て、読み取り専用アクセスを許可し、IP アクセスリスト 4 がコミュニティ ストリングを使用してスイッチの SNMP エージェントにアクセスするよう指定する方法を示します。

```
Switch(config)# snmp-server community comaccess ro 4
```

## SNMP グループおよびユーザの設定

スイッチ上のローカルまたはリモート SNMP サーバ エンジンに、識別名 (エンジン ID) を指定できます。SNMP ユーザを SNMP ビューにマッピングする SNMP サーバ グループを設定し、SNMP グループに新規ユーザを追加できます。

スイッチ上で SNMP を設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	説明
ステップ 1	<b>configure terminal</b>	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</b> { <i>local engineid-string</i>   <i>remote ip-address</i> [ <i>udp-port port-number</i> ] <i>engineid-string</i> }	SNMP のローカル コピーまたはリモート コピーのいずれかの名前を設定します。 <ul style="list-style-type: none"> <li><b>engineid-string</b> は、SNMP のコピー名を含む 24 文字の ID ストリングです。後続の値がゼロの場合、エンジン ID に 24 文字すべてを指定する必要はありません。後続値がすべてゼロとなる位置まで、エンジン ID の一部を指定します。たとえば、12340000000000000000000000 のエンジン ID を設定する場合は、<b>snmp-server engineID local 1234</b> と入力します。</li> <li><b>remote</b> を選択した場合は、SNMP のリモート コピーが格納されたデバイスの <b>ip-address</b>、および任意でリモート デバイス上の UDP ポートを指定します。デフォルト値は 162 です。</li> </ul>
ステップ 3	<b>snmp-server group groupname</b> { <i>v1</i>   <i>v2c</i> / <i>v3</i> [ <i>auth</i>   <i>noauth</i>   <i>priv</i> ]} [ <i>read readview</i> ] [ <i>write writeview</i> ] [ <i>notify notifyview</i> ] [ <i>access access-list</i> ]	リモート デバイスに新規の SNMP グループを設定します。 <ul style="list-style-type: none"> <li><b>groupname</b> には、グループ名を指定します。</li> <li>セキュリティ モデルを指定します。 <ul style="list-style-type: none"> <li><b>v1</b> は、使用可能なセキュリティ モデルのうち、安全性が最も低いモデルです。</li> <li><b>v2c</b> は、2 番めに安全性が低いモデルです。このモデルを使用すると、インフォームおよび整数を標準の 2 倍の幅で伝送できます。</li> <li><b>v3</b> は最も安全性が高いモデルで、認証レベルを選択する必要があります。</li> </ul> </li> <li><b>auth</b> Message Digest 5 (MD5) および Secure Hash Algorithm (SHA) パケット認証をイネーブルにします。</li> <li><b>noauth</b> noAuthNoPriv セキュリティ レベル。キーワードを指定しない場合は、このレベルがデフォルトです。</li> <li><b>priv</b> Data Encryption Standard (DES; データ暗号化規格) パケット暗号化 (別名 プライバシ) をイネーブルにします。</li> </ul> <p> (注) <b>priv</b> キーワードは、暗号ソフトウェア イメージがインストールされている場合のみ使用できます。</p>

コマンド	説明
	<ul style="list-style-type: none"> <li>• (任意) <b>read readview</b> には、エージェントの内容表示のみが可能なビューの名前を示す文字列 (64 文字以下) を指定して、入力します。</li> <li>• (任意) <b>write writeview</b> には、データを入力してエージェントの内容を設定するビューの名前を示す文字列 (64 文字以下) を指定して、入力します。</li> <li>• (任意) <b>notify notifyview</b> には、通知、インフォーム、またはトラップを指定するビューの名前を示す文字列 (64 文字以下) を指定して、入力します。</li> <li>• (任意) <b>access access-list</b> には、アクセス リストの名前を示す文字列 (64 文字以下) を指定して、入力します。</li> </ul>
ステップ 4 <b>snmp-server user username groupname [remote host [udp-port port]] {v1   v2c / v3 [auth {md5   sha} auth-password] [encrypted] [access access-list]}</b>	<p>SNMP グループに新規ユーザを設定します。</p> <ul style="list-style-type: none"> <li>• <b>username</b> は、エージェントに接続されたホスト上のユーザ名です。</li> <li>• <b>groupname</b> は、ユーザが関連付けられているグループの名前です。</li> <li>• (任意) ユーザが属するリモート SNMP エンティティおよびホスト名を指定する場合は、<b>remote</b> を入力します。このエンティティの IP アドレスを指定する場合は、さらにオプションの UDP ポート番号を指定します。デフォルト値は 162 です。</li> <li>• SNMP バージョン番号 (<b>v1</b>、<b>v2c</b>、または <b>v3</b>) を入力します。<b>v3</b> を入力する場合は、次のオプションを使用します。 <ul style="list-style-type: none"> <li>- <b>auth</b> 認証レベル設定セッションです。HMAC-MD5-96 または HMAC-SHA-96 認証レベルのいずれかを指定でき、パスワード文字列 (64 文字以下) が必要となります。</li> <li>- <b>encrypted</b> パスワードが暗号化形式で表示されるように指定します。</li> </ul> </li> <li>• (任意) <b>access access-list</b> には、アクセス リストの名前を示す文字列 (64 文字以下) を指定して、入力します。</li> </ul>
ステップ 5 <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 6 <b>show running-config</b>	設定を確認します。
ステップ 7 <b>copy running-config startup-config</b>	(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。

## SNMP 通知の設定

トラップ マネージャは、トラップを受信して処理する管理ステーションです。トラップは、特定のイベントが発生した場合に、スイッチが生成するシステム アラートです。デフォルトでトラップ マネージャは定義されていないため、トラップは送信されません。IOS リリースが稼働するスイッチでは、無制限にトラップ マネージャを設定できます。



(注) 多くのコマンドは、コマンド構文内でワード **traps** を使用します。トラップまたはインフォームを選択するオプションがコマンド内に指定されていない場合、キーワード **traps** はトラップまたはインフォーム、あるいはその両方を表します。SNMP 通知をトラップまたはインフォームのどちらで送信するかを指定するには、**snmp-server host** グローバル コンフィギュレーション コマンドを使用します。



表 27-5 に、サポートされているスイッチのトラップ (通知タイプ) を示します。これらのトラップの一部または全部をイネーブルにし、トラップ マネージャがトラップを受信するように設定できます。

表 27-5 スイッチの通知タイプ

通知タイプのキーワード	説明
<i>bgp</i>	BGP ステート変更トラップを生成。このオプションは、拡張マルチレイヤ イメージがインストールされている場合のみ使用できます。
<i>bridge</i>	STP ブリッジ MIB トラップを生成
<i>cluster</i>	クラスタ設定の変更時にトラップを生成
<i>config</i>	SNMP 設定の変更時にトラップを生成
<i>config-copy</i>	SNMP コピー設定の変更時にトラップを生成
<i>entity</i>	SNMP エンティティの変更時にトラップを生成
<i>envmon</i>	環境モニタトラップを生成。ファン、シャットダウン、電源装置、温度の環境トラップの一部またはすべてをイネーブルにすることができます。
<i>flash</i>	SNMP FLASH 通知を生成。オプションとして、フラッシュの追加または削除に関する通知をイネーブルにできます。このようにすると、スタックからスイッチを削除するか、またはスタックにスイッチを追加した場合に (物理的な取り外し、電源のオフ / オン、またはリロードの場合に)、トラップが生成されます。
<i>fru-ctrl</i>	エンティティ FRU 制御トラップを生成。Catalyst 3750 スイッチ スタックでは、このトラップはスタックに対するスイッチの追加または削除を意味します。
<i>hsrp</i>	Hot Standby Router Protocol (HSRP) の変更時にトラップを生成
<i>mac-notification</i>	MAC アドレス通知のトラップを生成
<i>port-security</i>	SNMP ポート セキュリティトラップを生成。秒当たりの最大トラップ レートを設定することもできます。指定できる範囲は 0 ~ 1000 です。デフォルトは 0 (レート制限なし) です。
<i>rtr</i>	SNMP Response Time Reporter (RTR) に対してトラップを生成
<i>snmp</i>	認証、コールド スタート、ウォーム スタート、リンク アップ、リンク ダウン時の SNMP タイプ通知のトラップを生成
<i>stp</i>	SNMP STP 拡張 MIB トラップを生成
<i>syslog</i>	SNMP Syslog トラップを生成
<i>tty</i>	TCP 接続時にトラップを生成
<i>vlan-membership</i>	SNMP VLAN メンバーシップの変更時にトラップを生成
<i>vlancreate</i>	SNMP VLAN 作成トラップを生成
<i>vlandelete</i>	SNMP VLAN 削除トラップを生成
<i>vtp</i>	VLAN Trunk Protocol (VTP; VLAN トランク プロトコル) の変更時にトラップを生成

表 27-5 に示す通知タイプを受信する場合は、特定のホストに対して *snmp-server host* グローバル コンフィギュレーション コマンドを実行します。

ホストにトラップまたはインフォームを送信するようにスイッチを設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	説明
ステップ 1	<code>configure terminal</code>	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	<code>snmp-server engineID remote ip-address engineid-string</code>	リモート ホストのエンジン ID を指定します。
ステップ 3	<code>snmp-server user username groupname remote host [udp-port port] {v1   v2c / v3 [auth {md5   sha} auth-password] [encrypted] [access access-list]}</code>	<p>ステップ 2 で作成したリモート ホストに対応する SNMP ユーザを設定します。</p> <p> (注) アドレスに対してリモート ユーザを設定する場合は、最初にそのリモート ホストのエンジン ID を設定する必要があります。リモート エンジン ID を設定する前にユーザを設定しようとすると、エラー メッセージが表示され、コマンドは実行されません。</p>
ステップ 4	<code>snmp-server host host-addr [traps / informs] [version {1   2c / 3} [auth   noauth   priv]] community-string [udp-port port] [notification-type]</code>	<p>SNMP トラップ動作の受信側を指定します。</p> <ul style="list-style-type: none"> <li><code>host-addr</code> には、ホスト (対象となる受信デバイス) の名前またはインターネット アドレスを指定します。</li> <li>(任意) SNMP トラップをホストに送信する場合は、<code>traps</code> (デフォルト) を入力します。</li> <li>(任意) SNMP インフォームをホストに送信する場合は、<code>informs</code> を入力します。</li> <li>(任意) SNMP バージョン <code>version</code> (<code>1</code>、<code>2c</code>、または <code>3</code>) を指定します。SNMPv1 はインフォームをサポートしていません。</li> <li>(任意) バージョン 3 の場合は、認証レベル (<code>auth</code>、<code>noauth</code>、または <code>priv</code>) を選択します。</li> </ul> <p> (注) <code>priv</code> キーワードは、暗号ソフトウェア イメージがインストールされている場合のみ使用できます。</p> <ul style="list-style-type: none"> <li><code>community-string</code> には、通知動作によって送信されたパスワードと同様のコミュニティ スtring を入力します。</li> <li>(任意) <code>udp-port port</code> には、リモート デバイスの UDP ポートを入力します。</li> <li>(任意) <code>notification-type</code> には、表 27-5 (p.27-12) に示されているキーワードを使用します。タイプを指定しない場合、すべての通知が送信されます。</li> </ul>
ステップ 5	<code>snmp-server enable traps notification-types</code>	<p>トラップまたはインフォームを送信するスイッチをイネーブルにし、送信する通知タイプを指定します。通知タイプの一覧については、表 27-5 (p.27-12) を参照するか、または <code>snmp-server enable traps ?</code> と入力してください。</p> <p>複数のトラップ タイプをイネーブルにするには、トラップ タイプごとに <code>snmp-server enable traps</code> コマンドを個別に入力する必要があります。</p>
ステップ 6	<code>snmp-server trap-source interface-id</code>	(任意) 送信元インターフェイスを指定します。これにより、トラップ メッセージ用の IP アドレスが設定されます。このコマンドを実行すると、インフォーム用の送信元 IP アドレスも設定されます。
ステップ 7	<code>snmp-server queue-length length</code>	(任意) 各トラップ ホストのメッセージ キュー長を設定します。指定できる範囲は 1 ~ 1000 で、デフォルトは 10 です。

	コマンド	説明
ステップ 8	<b><i>snmp-server trap-timeout seconds</i></b>	(任意)トラップ メッセージの再送信間隔を定義します。指定できる範囲は 1 ~ 1000 秒で、デフォルトは 30 秒です。
ステップ 9	<b><i>end</i></b>	イネーブル EXEC モードに戻ります。
ステップ 10	<b><i>show running-config</i></b>	設定を確認します。
ステップ 11	<b><i>copy running-config startup-config</i></b>	(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。

***snmp-server host*** コマンドは、通知を受信するホストを指定します。***snmp-server enable trap*** コマンドは、指定された通知 (トラップまたはインフォーム用) のメカニズムをグローバルにイネーブルにします。インフォームを受信するホストをイネーブルにするには、ホストに対して ***snmp-server host informs*** コマンドを設定し、***snmp-server enable traps*** コマンドを使用してインフォームをグローバルにイネーブルにする必要があります。

トラップを受信するように指定されたホストを削除する場合は、***no snmp-server host host*** グローバル コンフィギュレーション コマンドを使用します。***no snmp-server host*** コマンドにキーワードを指定しないで使用すると、ホストに対して、トラップはディセーブルになりますが、インフォームはディセーブルになりません。インフォームをディセーブルにするには、***no snmp-server host informs*** グローバル コンフィギュレーション コマンドを使用します。特定のトラップ タイプをディセーブルにするには、***no snmp-server enable traps notification-types*** グローバル コンフィギュレーション コマンドを使用します。

## エージェント コンタクトおよびロケーションの設定

SNMP エージェントのシステム コンタクトおよびロケーションを設定して、コンフィギュレーション ファイルからこれらの記述にアクセスできるようにするには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	説明
ステップ 1	<b><i>configure terminal</i></b>	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><i>snmp-server contact text</i></b>	システム コンタクト スtring を設定します。 次に例を示します。 <code>snmp-server contact Dial System Operator at beeper 21555.</code>
ステップ 3	<b><i>snmp-server location text</i></b>	システム ロケーション スtring を設定します。 次に例を示します。 <code>snmp-server location Building 3/Room 222</code>
ステップ 4	<b><i>end</i></b>	イネーブル EXEC モードに戻ります。
ステップ 5	<b><i>show running-config</i></b>	設定を確認します。
ステップ 6	<b><i>copy running-config startup-config</i></b>	(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。

## SNMP 経由で使用する TFTP サーバの制限

SNMP を経由してコンフィギュレーション ファイルの保存およびロードに使用する Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) サーバを、アクセス リストに指定されたサーバに限定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	説明
ステップ 1	<code>configure terminal</code>	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	<code>snmp-server tftp-server-list access-list-number</code>	SNMP を経由してコンフィギュレーション ファイルのコピーに使用する TFTP サーバを、アクセス リスト内のサーバに限定します。  <code>access-list-number</code> には、1 ~ 99 および 1300 ~ 1999 の範囲で標準の IP アクセス リスト番号を入力します。
ステップ 3	<code>access-list access-list-number { deny   permit } source [source-wildcard]</code>	標準アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。  <ul style="list-style-type: none"> <li><code>access-list-number</code> には、ステップ 2 で指定したアクセス リスト番号を入力します。</li> <li><code>deny</code> キーワードを指定すると、条件が一致した場合にアクセスが拒否されます。<code>permit</code> キーワードを指定すると、条件が一致した場合にアクセスが許可されます。</li> <li><code>source</code> には、スイッチへのアクセスが許可された TFTP サーバの IP アドレスを入力します。</li> <li>(任意) <code>source-wildcard</code> を指定する場合は、送信元に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置に 1 を配置します。</li> </ul> アクセス リストの末尾には、すべてに適用される暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(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。

## SNMP の例

次に、SNMP のすべてのバージョンをイネーブルにする例を示します。この設定では、コミュニティ ストリング `public` を使用してすべてのオブジェクトに読み取り専用権限でアクセスするように SNMP マネージャを許可します。この設定により、スイッチがトラップを送信することはありません。

```
Switch(config)# snmp-server community public
```

次に、コミュニティ ストリング `public` を使用してすべてのオブジェクトに読み取り専用権限でアクセスするように SNMP マネージャを許可する例を示します。このスイッチは、SNMPv1 を使用してホスト 192.180.1.111 および 192.180.1.33 に、SNMPv2C を使用してホスト 192.180.1.27 に、それぞれ VTP トラップを送信します。コミュニティ ストリング `public` がトラップとともに送信されます。

```
Switch(config)# snmp-server community public
Switch(config)# snmp-server enable traps vtp
Switch(config)# snmp-server host 192.180.1.27 version 2c public
Switch(config)# snmp-server host 192.180.1.111 version 1 public
Switch(config)# snmp-server host 192.180.1.33 public
```

次に、コミュニティ ストリング *comaccess* を使用するアクセス リスト 4 のメンバーに、すべてのオブジェクトへの読み取り専用アクセス権を許可する例を示します。その他の SNMP マネージャは、オブジェクトへのアクセス権がありません。コミュニティ ストリング *public* を使用し、SNMPv2C によって SNMP 認証失敗トラップがホスト *cisco.com* に送信されます。

```
Switch(config)# snmp-server community comaccess ro 4
Switch(config)# snmp-server enable traps snmp authentication
Switch(config)# snmp-server host cisco.com version 2c public
```

次に、エンティティ MIB トラップをホスト *cisco.com* に送信する例を示します。コミュニティ ストリングは制限されています。スイッチは最初の行により、すでにイネーブルになっているトラップ以外にエンティティ MIB トラップの送信もイネーブルになります。2 行めはこれらのトラップの宛先を指定し、ホスト *cisco.com* に対する以前の *snmp-server host* コマンドを無効にします。

```
Switch(config)# snmp-server enable traps entity
Switch(config)# snmp-server host cisco.com restricted entity
```

次に、スイッチがコミュニティ ストリング *public* を使用し、すべてのトラップをホスト *myhost.cisco.com* に送信できるように設定する例を示します。

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

## SNMP ステータスの表示

違法なコミュニティ ストリング エントリ、エラー、および要求された変数を含む、SNMP 入出力の統計情報を表示するには、**show snmp** イネーブル EXEC コマンドを使用します。また、SNMP 情報の表示には、表 27-6 に記載されているその他のイネーブル EXEC コマンドも使用できます。この出力に表示されるフィールドの詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』 Release 12.1 を参照してください。

表 27-6 SNMP 情報表示用のコマンド

機能	デフォルト設定
<b>show snmp</b>	SNMP の統計情報を表示します。
<b>show snmp engineID [local / remote]</b>	デバイス上に設定されているローカル SNMP エンジンおよびすべてのリモート エンジンに関する情報を表示します。
<b>show snmp group</b>	ネットワーク上の各 SNMP グループに関する情報を表示します。
<b>show snmp user</b>	SNMP ユーザテーブル内の各 SNMP ユーザ名に関する情報を表示します。



(注)

**snmp-server enable informs** グローバル コンフィギュレーション コマンドはコマンドラインのヘルプ ストリングに表示されていますが、サポートされていません。SNMP インフォーム通知の送信をイネーブルにするには、**snmp-server enable traps** グローバル コンフィギュレーション コマンドと、**snmp-server host host-addr informs** グローバル コンフィギュレーション コマンドを組み合わせで使用します。

