



SNMP の設定

この章では、スイッチに 簡易ネットワーク管理プロトコル (SNMP) を設定する方法について説明します。特に明記しない限り、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 スタックを指します。



(注)

この章で使用するコマンドの完全な構文および使用方法の詳細については、Cisco.com ページの次の URL から、このリリースに対応するコマンドリファレンス、および『Cisco IOS Network Management Command Reference, Release 12.4』を参照してください。
http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_book.html

この章の内容は、次のとおりです。

- 「SNMP の概要」 (P.33-1)
- 「SNMP の設定」 (P.33-6)
- 「SNMP ステータスの表示」 (P.33-20)

SNMP の概要

SNMP は、マネージャとエージェント間の通信のメッセージ 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 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) に統合できます。エージェントおよび MIB は、スイッチに常駐します。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せん。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格納したりできます。エージェントは、デバイス パラメータやネットワーク データの保存場所である MIB から値を収集します。また、エージェントはマネージャのデータ取得またはデータ設定の要求に応答できます。

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できます。トラップは、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 ステータス (アップまたはダウン)、MAC アドレス追跡、TCP 接続の終了、ネイバーとの接続の切断などの重要なイベントの発生を意味する場合があります。

スタック マスターでは、スイッチ スタック全体に対する SNMP 要求およびトラップが処理されます。スタック マスターでは、すべてのスタック メンバに関連するすべての要求またはトラップが透過的に管理されます。新しいスタック マスターが選択されると、新しいマスターで制御が開始された後でも SNMP 管理ステーションに対する IP 接続が維持されたままの場合、新しいマスターでは、前のスタック マスターで設定済みの SNMP 要求およびトラップの処理が続行されます。

スイッチ スタックの詳細については、第 7 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、次の概要について説明します。

- 「SNMP バージョン」 (P.33-2)
- 「SNMP マネージャ機能」 (P.33-3)
- 「SNMP エージェント機能」 (P.33-4)
- 「SNMP コミュニティ スtring」 (P.33-4)
- 「SNMP を使用して MIB 変数にアクセスする方法」 (P.33-4)
- 「SNMP 通知」 (P.33-5)
- 「SNMP ifIndex MIB オブジェクト値」 (P.33-6)

SNMP バージョン

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

- SNMPv1 : RFC1157 に規定された SNMP (完全インターネット標準)。
- SNMPv2C は、SNMPv2Classic のバルク検索機能を残し、エラー処理を改善したうえで、SNMPv2Classic のパーティ ベースの管理およびセキュリティ フレームワークをコミュニティ スtring ベースの管理フレームワークに置き換えたものです。次の機能があります。
 - SNMPv2 : RFC 1902 ~ 1907 に規定された SNMP バージョン 2 (ドラフト版インターネット標準)。
 - SNMPv2C : RFC 1901 に規定された SNMPv2 のコミュニティ スtring ベースの管理フレームワーク (試験版インターネットプロトコル)。
- SNMPv3 : RFC 2273 ~ 2275 に定められた SNMP バージョン 3 (相互運用可能な標準ベースのプロトコル) SNMPv3 は、ネットワーク上のパケットを認証、暗号化することでデバイスへのアクセスに対するセキュリティを提供します。SNMPv3 は、次のセキュリティ機能を備えています。
 - メッセージの完全性 : パケットが伝送中に改ざん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ミキシングし、許可されていない送信元に内容が読まれることを防止します。



(注) 暗号化を選択するには、**priv** キーワードを入力します。このキーワードは、暗号化ユニバーサル ソフトウェア イメージがインストールされている場合だけ使用できます。

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が、IP アドレス アクセス コントロール リストおよびパスワードによって定義されます。

SNMPv2C にはバルク検索メカニズムが組み込まれ、より詳細なエラー メッセージを管理ステーションに報告します。バルク検索メカニズムは、テーブルや大量の情報を検索し、必要な往復回数を削減します。SNMPv2C ではエラー処理機能が改善され、さまざまなエラーを区別するための拡張エラーコードが使用されています。これらのエラーは、SNMPv1 では単一のエラー コードで報告されます。SNMPv2 では、エラー リターン コードでエラー タイプが報告されるようになりました。

SNMPv3 は、セキュリティ モデルとセキュリティ レベルの両方を提供します。セキュリティ モデルは、ユーザとユーザが属しているグループ用に設定された認証方式です。セキュリティ レベルは、セキュリティ モデル内で許可されたセキュリティのレベルです。セキュリティ レベルとセキュリティ モデルの組み合わせにより、SNMP パケットを扱うときに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 33-1 に、セキュリティ モデルとセキュリティ レベルのさまざまな組み合わせについて、その特性を示します。

表 33-1 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
SNMPv1	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
SNMPv2C	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
SNMPv3	noAuthNoPriv	ユーザ名	No	ユーザ名の照合を使用して認証します。
SNMPv3	authNoPriv	Message Digest 5 (MD5) または Secure Hash Algorithm (SHA)	No	HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証します。
SNMPv3	authPriv (暗号化ユニバーサルソフトウェア イメージが必要)	MD5 または SHA	Data Encryption Standard (DES; データ暗号化規格) または Advanced Encryption Standard (AES; 高度暗号化規格)	HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証します。 次の暗号化アルゴリズムで、User-based Security Model (USM) を指定できます。 <ul style="list-style-type: none"> • CBC-DES (DES-56) 規格に基づく認証に加えた DES 56 ビット暗号化。 • 3DES 168 ビット暗号化 • AES 128 ビット暗号化、192 ビット暗号化、または 256 ビット暗号化

管理ステーションでサポートされている SNMP 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 を使用す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 マネージャ機能

SNMP マネージャは、MIB 情報を使用して、表 33-2 に示す動作を実行します。

表 33-2 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。 ¹
get-bulk-request ²	テーブルの複数の行など、通常はサイズの小さい多数のデータ ブロックに分割して送信する必要がある巨大なデータ ブロックを取得します。

表 33-2 SNMP の動作 (続き)

動作	説明
get-response	NMS から送信される get-request、get-next-request、および set-request に対して応答します。
set-request	特定の変数に値を格納します。
trap	SNMP エージェントから SNMP マネージャに送られる、イベントの発生を伝える非送信請求メッセージです。

- 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て、必要な変数を検出します。
- get-bulk コマンドを使用できるのは、SNMPv2 以上に限られます。

SNMP エージェント機能

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

- 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、この値を使用して 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。

エージェントで重要なイベントが発生したことを NMS に通知するために、SNMP エージェントは非送信請求トラップメッセージも送信します。トラップ条件の例には、ポートまたはモジュールがアップまたはダウン状態になった場合、スパンニングツリー トポロジが変更された場合、認証に失敗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 オブジェクトに対するアクセスを認証し、組み込み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 のコミュニティ スtring定義が、スイッチ上の 3 つのコミュニティ スtring定義の少なくとも 1 つと一致していなければなりません。

コミュニティ スtringの属性は、次の 3 つのいずれかです。

- Read-Only (RO)：許可された管理ステーションに、コミュニティ スtringを除く MIB 内のすべてのオブジェクトへの読み取りアクセスを許可しますが、書き込みアクセスは許可しません。
- Read-Write (RW)：許可された管理ステーションに、MIB 内のすべてのオブジェクトへの読み書きアクセスを許可しますが、コミュニティ スtringに対するアクセスは許可しません。

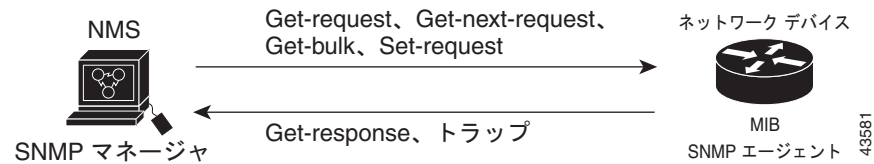
SNMP を使用して MIB 変数にアクセスする方法

NMS の例として、CiscoWorks ネットワーク管理ソフトウェアがあります。CiscoWorks 2000 ソフトウェアは、スイッチの MIB 変数を使用してデバイス変数を設定し、ネットワーク上のデバイスをポーリングして特定の情報を取得します。ポーリング結果は、グラフ形式で表示されます。この結果を解析して、インターネットワーキング関連の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 33-1 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、トラップ (特定イベントの通知) を送信でき、SNMP マネージャはトラップを受信して処理します。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

データス（アップまたはダウン）、MAC アドレス トラッキングなどの状況を 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* 形式で送信される MIB 関連のクエリーに応答します。

図 33-1 SNMP ネットワーク



SNMP 通知

SNMP を使用すると、特定のイベントが発生した場合に、スイッチから SNMP マネージャに通知を送信できます。SNMP 通知は、トラップまたは情報要求として送信できます。コマンド構文では、トラップまたは情報を選択するオプションがコマンドにない限り、キーワード *traps* はトラップ、情報、またはその両方を表します。**snmp-server host** コマンドを使用して、トラップまたは情報として SNMP 通知を送信するかどうかを指定します。



(注) SNMPv1 は *informs* をサポートしていません。

トラップは信頼性に欠けます。受信側はトラップを受信しても確認応答を送信しないので、トラップが受信されたかどうかを送信側にわからないからです。情報要求の場合、受信した SNMP マネージャは SNMP 応答 Protocol Data Unit (PDU; プロトコルデータユニット) でメッセージを確認します。送信側が応答を受信しなかった場合は、再び情報要求を送信できます。再送信できるので、情報の方がトラップより意図した宛先に届く可能性が高くなります。

情報の方がトラップより信頼性が高いのは、スイッチおよびネットワークのリソースを多く消費するという特性にも理由があります。送信と同時に廃棄されるトラップと異なり、情報要求は応答を受信するまで、または要求がタイムアウトになるまで、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、情報は数回にわたって再送信つまり再試行が可能です。再試行によってトラフィックが増え、ネットワークのオーバーヘッドが大きくなる原因になります。したがって、トラップにするか情報にするかは、信頼性を取るかリソースを取るかという選択になります。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、情報要求を使用してください。ネットワークまたはスイッチ メモリ上のトラフィックが問題になる場合で、なおかつ通知が不要な場合は、トラップを使用してください。

SNMP ifIndex MIB オブジェクト値

NMS の IF-MIB は、物理インターフェイスまたは論理インターフェイスを識別する、ゼロより大きい一意の値である `interface index (ifIndex)` オブジェクト値の生成および割り当てを行います。スイッチの再起動またはスイッチのソフトウェアのアップグレード時に、スイッチは、インターフェイスにこれと同じ値を使用します。たとえば、スイッチのポート 2 に 10003 という ifIndex 値が割り当てられていると、スイッチの再起動後も同じ値が使用されます。

スイッチは、表 33-3 のいずれかの値を使用して、インターフェイスに ifIndex 値を割り当てます。

表 33-3 ifIndex 値

インターフェイス タイプ	ifIndex 範囲
SVI ¹	1 ~ 4999
EtherChannel	5001 ~ 5048
種類とポート番号に基づく物理（ギガビットイーサネットまたはモジュールインターフェイスなど）	10000 ~ 14500
ヌル	10501（スタック不可スイッチ）14501（スタック可能スイッチ）
ループバックおよびトンネル	24567 +

1. SVI = Switch Virtual Interface



(注) スイッチは、範囲内の連続した値を使用しない場合があります。

SNMP の設定

ここでは、次の設定について説明します。

- 「SNMP のデフォルト設定」 (P.33-7)
- 「SNMP 設定時の注意事項」 (P.33-7)
- 「SNMP エージェントのディセーブル化」 (P.33-8)
- 「コミュニティ スtring の設定」 (P.33-8)
- 「SNMP グループおよびユーザの設定」 (P.33-10)
- 「SNMP 通知の設定」 (P.33-13)
- 「エージェント コンタクトおよびロケーションの設定」 (P.33-17)
- 「SNMP を通して使用する TFTP サーバの制限」 (P.33-18)
- 「SNMP の例」 (P.33-19)

SNMP のデフォルト設定

表 33-4 に、SNMP のデフォルト設定を示します。

表 33-4 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	ディセーブル ¹ 。
SNMP トラップ レシーバ	未設定。
SNMP トラップ	TCP 接続のトラップ (tty) 以外は、イネーブルではありません。
SNMP バージョン	version キーワードがない場合、デフォルトはバージョン 1 になります。
SNMPv3 認証	キーワードを入力しなかった場合、セキュリティ レベルはデフォルトで noauth (noAuthNoPriv) になります。
SNMP 通知タイプ	タイプが指定されていない場合、すべての通知が送信されます。

1. これは、スイッチが起動し、スタートアップ コンフィギュレーションに **snmp-server** グローバル コンフィギュレーション コマンドが設定されていない場合のデフォルトです。

SNMP 設定時の注意事項

スイッチが起動し、スイッチのスタートアップ コンフィギュレーションに少なくとも 1 つの **snmp-server** グローバル コンフィギュレーション コマンドが設定されている場合、SNMP エージェントはイネーブルになります。

SNMP グループは、SNMP ユーザを SNMP ビューに対応付けるテーブルです。SNMP ユーザは、SNMP グループのメンバです。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 を設定する場合は、以下の注意事項に従ってください。

- SNMP グループを設定するときは、通知ビューを指定しません。 **snmp-server host** グローバル コンフィギュレーション コマンドがユーザの通知ビューを自動生成し、そのユーザに対応するグループに追加します。グループの通知ビューを変更すると、そのグループに対応付けられたすべてのユーザが影響を受けます。通知ビューの設定が必要な状況については、『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*』を参照してください。
- 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 コマンドを **remote** オプションとともに使用して、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を使用して認証およびプライバシー ダイジェストが算出されます。先にリモート エンジン ID を設定しておかないと、コンフィギュレーション コマンドがエラーになります。
- SNMP 情報を設定するときには、プロキシ要求または情報の送信先となるリモートエージェントの SNMP エンジン ID を SNMP データベースに設定しておく必要があります。
- ローカルユーザがリモートホストと関連付けられていない場合、スイッチは **auth** (authNoPriv) および **priv** (authPriv) の認証レベルの情報を送信しません。
- SNMP エンジン ID の値を変更すると、重大な影響が生じます。(コマンドラインで入力された) 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。コマンドラインのパスワードは、RFC 2274 の規定に

従って廃棄されます。このようにパスワードが廃棄されるため、エンジン ID 値を変更した場合は SNMPv3 ユーザのセキュリティ ダイジェストが無効となり、`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 ユーザを再設定する必要があります。エンジン ID を変更した場合は、同様の制限によってコミュニティ スtring も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、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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>no snmp-server</code>	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	<code>end</code>	特権 EXEC モードに戻ります。
ステップ4	<code>show running-config</code>	設定を確認します。
ステップ5	<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。

`no snmp-server` 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、デバイスで稼働中のすべてのバージョン (バージョン 1、バージョン 2C、バージョン 3) がディセーブルになります。SNMP をイネーブルにする特定の Cisco IOS コマンドは存在しません。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tring の設定

SNMP マネージャとエージェントの関係を定義するには、SNMP コミュニティ スtring を使用します。コミュニティ スtring は、スイッチ上のエージェントへのアクセスを許可するパスワードと同様に機能します。スString に対応する次の特性を 1 つまたは複数指定することもできます。

- コミュニティ スtring を使用してエージェントにアクセスできる SNMP マネージャの IP アドレスのアクセス リスト
- 指定のコミュニティにアクセスできるすべての MIB オブジェクトのサブセットを定義する MIB ビュー
- コミュニティにアクセスできる MIB オブジェクトの読み書き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 ストリングを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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 community string [view view-name] [ro rw] [access-list-number]</code>	<p>コミュニティ ストリングを設定します。</p> <ul style="list-style-type: none"> <code>string</code> には、パスワードと同様に機能し、SNMP プロトコルへのアクセスを許可するストリングを指定します。任意の長さのコミュニティ ストリングを 1 つまたは複数設定できます。 (任意) <code>view</code> には、コミュニティがアクセスできるビュー レコードを指定します。 (任意) 許可された管理ステーションで MIB オブジェクトを取得する場合は読み取り専用 (<code>ro</code>)、許可された管理ステーションで MIB オブジェクトを取得および変更する場合は読み書き (<code>rw</code>) を指定します。デフォルトでは、コミュニティ ストリングはすべてのオブジェクトに対する読み取り専用アクセスを許可します。 (任意) <code>access-list-number</code> には、1 ~ 99 および 1300 ~ 1999 の標準 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>	<p>(任意) ステップ 2 で標準 IP アクセス リスト番号を指定してリストを作成した場合は、必要に応じてコマンドを繰り返します。</p> <ul style="list-style-type: none"> <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。 <code>deny</code> キーワードは、条件が一致した場合にアクセスを拒否します。<code>permit</code> キーワードは、条件が一致した場合にアクセスを許可します。 <code>source</code> には、コミュニティ ストリングを使用してエージェントにアクセスできる SNMP マネージャの IP アドレスを入力します。 (任意) <code>source-wildcard</code> には、<code>source</code> 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は 1 を設定します。 <p>アクセス リストの末尾には、すべてに対す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	<code>end</code>	特権 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。



(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、そのコミュニティのコミュニティ ストリングをヌル ストリングに設定します (コミュニティ ストリングに値を入力しないでください)。

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 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、ストリング *comaccess* を SNMP に割り当てて読み取り専用アクセスを許可し、IP アクセス リスト 4 がこのコミュニティ 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できるように指定する例を示します。

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

SNMP グループおよびユーザの設定

スイッチのローカルまたはリモート SNMP サーバ エンジンを表す識別名 (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、新規ユーザを SNMP グループに追加できます。

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

	コマンド	目的
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 {local <i>engineid-string</i> remote <i>ip-address</i> [<i>udp-port port-number</i>] <i>engineid-string</i>}</code>	SNMP のローカル コピーまたはリモート コピーの名前を設定します。 <ul style="list-style-type: none"> <i>engineid-string</i> は、SNMP のコピー名を指定する 24 文字の ID ストリングです。後続ゼロが含まれる場合は、24 文字のエンジン ID すべてを指定する必要はありません。指定するのは、エンジン ID のうちゼロのみが続く箇所を除いた部分だけです。たとえば、123400000000000000000000 というエンジン ID を設定する場合、<code>snmp-server engineID local 1234</code> のように入力できます。 <code>remote</code> を指定した場合、SNMP のリモート コピーが置かれているデバイスの <i>ip-address</i> を指定し、任意でリモートデバイスの UDP ポートを指定します。デフォルト値は 162 です。

コマンド	目的
ステップ 3 snmp-server group <i>groupname</i> { v1 v2c v3 { auth noauth priv }} [read <i>readview</i>] [write <i>writeview</i>] [notify <i>notifyview</i>] [access <i>access-list</i>]	<p>リモート デバイスに新規 SNMP グループを設定します。</p> <ul style="list-style-type: none"> • <i>groupname</i> には、グループを指定します。 • セキュリティ モデルを指定します。 <ul style="list-style-type: none"> – v1 は、最も安全性の低いセキュリティ モデルです。 – v2c は、2 番めに安全性の低いセキュリティ モデルです。標準の 2 倍の幅で情報および整数を送送できます。 – 最も安全な v3 の場合、認証レベルを選択する必要があります。 <p>auth : MD5 および SHA によるパケット認証が可能です。</p> <p>noauth : noAuthNoPriv というセキュリティ レベルをイネーブルにします。キーワードを指定しなかった場合、これがデフォルトです。</p> <p>priv : DES によるパケット暗号化をイネーブルにします (<i>privacy</i> と呼ばれます)。</p> <p>(注) priv キーワードは、暗号化ユニバーサル ソフトウェア イメージがインストールされている場合にだけ利用できます。</p> <ul style="list-style-type: none"> • (任意) read <i>readview</i> とともに、エージェントの内容を表示できるビューの名前を表すストリング (64 文字以下) を入力します。 • (任意) write <i>writeview</i> とともに、データを入力し、エージェントの内容を表示できるビューの名前を表すストリング (64 文字以下) を入力します。 • (任意) notify <i>notifyview</i> とともに、通知、情報、またはトラップを指定するビューの名前を表すストリング (64 文字以下) を入力します。 • (任意) access <i>access-list</i> とともに、アクセス リスト名のストリング (64 文字以下) を入力します。

コマンド	目的
ステップ4 <code>snmp-server user username groupname {remote host [udp-port port]} {v1 [access access-list] v2c [access access-list] v3 [encrypted] [access access-list] [auth {md5 sha} auth-password]} [priv {des 3des aes {128 192 256}} priv-password]</code>	SNMP グループに対して新規ユーザを追加します。 <ul style="list-style-type: none"> • <i>username</i> は、エージェントに接続するホスト上のユーザ名です。 • <i>groupname</i> は、ユーザが対応付けられるグループの名前です。 • remote を入力して、ユーザが所属するリモート SNMP エンティティおよびそのエンティティのホスト名または IP アドレスとともに、任意で UDP ポート番号を指定します。デフォルト値は 162 です。 • SNMP バージョン番号 (v1、v2c、または v3) を入力します。v3 を入力する場合は、次のオプションを追加します。 <ul style="list-style-type: none"> – encrypted は、パスワードを暗号化形式で表示するように指定します。このキーワードは、v3 キーワードが指定されている場合のみ使用可能です。 – auth は認証レベル設定セッションで、HMAC-MD5-96 (md5) または HMAC-SHA-96 (sha) 認証レベルを使用できます。パスワードストリング <i>auth-password</i> (64 文字以下) が必要です。 • v3 を入力してスイッチが暗号化ソフトウェア イメージを実行中の場合は、プライベート (priv) 暗号化およびパスワードストリング <i>priv-password</i> (64 文字以下) の設定もできます。 <ul style="list-style-type: none"> – priv は、User-based Security Model (USM) を指定します。 – des は、56 ビット DES アルゴリズムの使用を指定します。 – 3des は、168 ビット DES アルゴリズムの使用を指定します。 – aes は、DES アルゴリズムの使用を指定します。128 ビット暗号化、192 ビット暗号化、または 256 ビット暗号化のいずれかを選択する必要があります。 • (任意) access access-list とともに、アクセスリスト名のストリング (64 文字以下) を入力します。
ステップ5 <code>end</code>	特権 EXEC モードに戻ります。
ステップ6 <code>show running-config</code>	設定を確認します。 (注) auth noauth priv モード設定の SNMPv3 情報を表示するには、 show snmp user 特権コマンドを入力する必要があります。
ステップ7 <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 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ときにスイッチが生成するシステム アラートです。デフォルトでは、トラップ マネージャは定義されず、トラップは送信されません。この Cisco IOS Release が稼働しているスイッチでは、トラップ マネージャを無制限に設定できます。



(注)

コマンド構文で *traps* というワードを使用するコマンドは多数あります。トラップまたは情報を選択するオプションがコマンドにない限り、キーワード **traps** はトラップ、情報のいずれか、またはその両方を表します。**snmp-server host** グローバル コンフィギュレーション コマンドを使用して、トラップまたは情報として SNMP 通知を送信するかどうかを指定します。

表 33-5 に、サポートされているスイッチ 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て、これを受信するようにトラップ マネージャを設定できます。

表 33-5 スwitchの通知タイプ

通知タイプのキーワード	説明
bgp	ボーダー ゲートウェイ プロトコル (BGP) 状態変化トラップを生成します。このオプションは、IP サービス フィーチャ セットがイネーブルになっている場合にだけ使用できます。
bridge	Spanning-Tree Protocol (STP; スパニングツリー プロトコル) ブリッジ MIB トラップを生成します。
cluster	クラスタ設定が変更された場合に、トラップを生成します。
config	SNMP 設定が変更された場合に、トラップを生成します。
copy-config	SNMP コピー設定が変更された場合に、トラップを生成します。
cpu-threshold	CPU に関連したトラップをイネーブルにします。
entity	SNMP エンティティが変更された場合に、トラップを生成します。
envmon	環境モニタ トラップを生成します。ファン (fan)、シャットダウン (shutdown)、ステータス (status)、電源 (supply)、温度 (temperature) の環境トラップのいずれかまたはすべてをイネーブルにできます。
errdisable	ポート VLAN が errdisable ステートになった場合に、トラップを生成します。1 分あたりの最大トラップ速度も設定できます。指定できる範囲は 0 ~ 10000 です。デフォルトは 0 で、レート制限がないという意味です。
flash	SNMP FLASH 通知を生成します。スイッチ スタックでは、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)、トラップが発行されます。
fru-ctrl	エンティティ Field Replaceable Unit (FRU; 現場交換可能ユニット) 制御トラップを生成します。スイッチ スタックでは、このトラップはスタックにおけるスイッチの挿入/取り外しを意味します。
hsrp	ホットスタンバイ ルータ プロトコル (HSRP) が変更された場合に、トラップを生成します。
ipmulticast	IP マルチキャスト ルーティングが変更された場合に、トラップを生成します。

表 33-5 スイッチの通知タイプ (続き)

通知タイプのキーワード	説明
mac-notification	MAC アドレス通知のトラップを生成します。
msdp	Multicast Source Discovery Protocol (MSDP) が変更された場合に、トラップを生成します。
ospf	Open Shortest Path First (OSPF) が変更された場合に、トラップを生成します。シスコ固有、エラー、リンクステート アドバタイズ、レート制限、再送信、ステート変更に関するトラップを任意にイネーブルにできます。
pim	Protocol-Independent Multicast (PIM) が変更された場合に、トラップを生成します。無効な PIM メッセージ、ネイバー変更、およびランデブー ポイント (RP) マッピングの変更に関するトラップを任意にイネーブルにできます。
port-security	SNMP ポートセキュリティトラップを生成します。1 秒あたりの最大トラップ速度も設定できます。指定できる範囲は 0 ~ 1000 秒です。デフォルトは 0 秒で、レート制限がないという意味です。 (注) 通知タイプ port-security を使用してトラップを設定する際に、まずポートセキュリティトラップを設定して、次に以下のポートセキュリティトラップ レートを設定します。 <ul style="list-style-type: none"> • snmp-server enable traps port-security • snmp-server enable traps port-security trap-rate rate
rtr	SNMP Response Time Reporter (RTR) のトラップを生成します。
snmp	認証、コールドスタート、ウォームスタート、リンクアップ、またはリンクダウンについて、SNMP タイプ通知のトラップを生成します。
storm-control	SNMP ストーム制御のトラップを生成します。1 分あたりの最大トラップ速度も設定できます。指定できる範囲は 0 ~ 1000 です。デフォルトは 0 に設定されています (制限なしの状態では、発生ごとにトラップが送信されます)。
stpx	SNMP STP 拡張 MIB トラップを生成します。
syslog	SNMP の Syslog トラップを生成します。
tty	TCP 接続のトラップを生成します。このトラップは、デフォルトでイネーブルに設定されています。
vlan-membership	SNMP VLAN メンバーシップが変更された場合に、トラップを生成します。
vlancreate	SNMP VLAN 作成トラップを生成します。
vlandelete	SNMP VLAN 削除トラップを生成します。
vtp	VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) が変更された場合に、トラップを生成します。



(注)

fru-ctrl、**insertion**、**msdp**、**ospf**、**pim**、および **removal** キーワードは、コマンドラインのヘルプストリングには表示されますが、Catalyst Switch Module 3012 ではサポートされていません。SNMP 情報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て使用します。

表 33-5 に示す通知タイプを受信するには、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情報を送信するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	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	snmp-server engineID remote <i>ip-address engineid-string</i>	リモート ホスト用のエンジン ID を指定します。
ステップ 3	snmp-server user <i>username</i> <i>groupname</i> { remote <i>host</i> [udp-port <i>port</i>]} { v1 [access <i>access-list</i>] v2c [access <i>access-list</i>] v3 [encrypted] [access <i>access-list</i>] [auth { md5 sha } <i>auth-password</i>]}	ステップ 2 で設定したリモート ホストと対応付ける SNMP ユーザを設定します。 (注) アドレスに対応するリモート ユーザを設定するには、先にリモート ホストのエンジン ID を設定しておく必要があります。このようにしないと、エラー メッセージが表示され、コマンドが実行されません。
ステップ 4	snmp-server group <i>groupname</i> { v1 v2c v3 { auth noauth priv }} [read <i>readview</i>] [write <i>writeview</i>] [notify <i>notifyview</i>] [access <i>access-list</i>]	SNMP グループを設定します。
ステップ 5	snmp-server host <i>host-addr</i> [informs traps] [version { 1 2c 3 { auth noauth priv }}] <i>community-string</i> [<i>notification-type</i>]	SNMP トラップ動作の受信側を指定します。 <ul style="list-style-type: none"> <i>host-addr</i> には、ホスト (対象となる受信側) の名前またはインターネット アドレスを指定します。 (任意) SNMP 情報をホストに送信するには、informs を指定します。 (任意) SNMP トラップをホストに送信するには、traps (デフォルト) を指定します。 (任意) SNMP version (1、2c、または 3) を指定します。SNMPv1 は informs をサポートしていません。 (任意) バージョン 3 の場合、認証レベルとして auth、noauth、または priv を選択します。 (注) priv キーワードは、暗号化ユニバーサル ソフトウェア イメージがインストールされている場合にだけ利用できます。 <ul style="list-style-type: none"> <i>community-string</i> には、version 1 または version 2c が指定されている場合、通知動作で送信される、パスワードに類似したコミュニティ スtring を入力します。version 3 が指定されている場合、SNMPv3 ユーザ名を入力します。 (任意) <i>notification-type</i> には、表 33-5 (P.33-13) に記載されているキーワードを使用します。タイプが指定されていない場合、すべての通知が送信されます。

	コマンド	目的
ステップ 6	snmp-server enable traps <i>notification-types</i>	<p>スイッチがトラップまたは情報を送信できるようにし、送信する通知のタイプを指定します。通知タイプの一覧については、表 33-5 (P.33-13) を参照するか、snmp-server enable traps ? 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 snmp-server enable traps コマンドを個別に入力する必要があります。</p> <p>(注) 通知タイプ port-security を使用してトラップを設定する際に、まずポート セキュリティ トラップを設定して、次に以下のポート セキュリティ トラップ レートを設定します。</p> <ul style="list-style-type: none"> • snmp-server enable traps port-security • snmp-server enable traps port-security trap-rate rate
ステップ 7	snmp-server trap-source <i>interface-id</i>	(任意) 送信元インターフェイスを指定します。そこからトラップ メッセージに対応する IP アドレスが取得されます。情報の送信元 IP アドレスも、このコマンドで設定します。
ステップ 8	snmp-server queue-length <i>length</i>	(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 です。デフォルトは 10 です。
ステップ 9	snmp-server trap-timeout <i>seconds</i>	(任意) トラップ メッセージを再送信する間隔を設定します。指定できる範囲は 1 ~ 1000 です。デフォルトは 30 秒です。
ステップ 10	end	特権 EXEC モードに戻ります。
ステップ 11	show running-config	設定を確認します。
ステップ 12	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。

snmp-server host コマンドでは、通知を受信するホストを指定します。**snmp-server enable trap** コマンドによって、指定された通知メカニズム（トラップおよび情報）がグローバルでイネーブルになります。ホストが情報を受信できるようにするには、そのホストに対応する **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情報をグローバルにイネーブルにする必要があります。

指定したホストがトラップを受信しないようにするには、**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。キーワードを指定しないで **no snmp-server host** コマンドを使用すると、ホストへのトラップはディセーブルになりますが、情報はディセーブルになりません。情報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 コマンドを使用してください。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。

CPU しきい値通知のタイプと値の設定

CPU しきい値通知のタイプと値を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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>process cpu threshold type {total process interrupt} rising percentage interval seconds [falling fall-percentage interval seconds]</code>	<p>CPU しきい値通知のタイプと値を設定します。</p> <ul style="list-style-type: none"> total : 通知タイプを CPU 使用率の合計に設定します。 process : 通知タイプを CPU プロセス使用率に設定します。 interrupt : 通知タイプを CPU 割り込み使用率に設定します。 rising percentage : CPU リソースのパーセンテージ (1 ~ 100)。設定された間隔を過ぎると CPU しきい値通知を送信します。 interval seconds : CPU しきい値超過の秒単位の持続時間 (5 ~ 86400)。この条件が満たされると CPU しきい値通知を送信します。 falling fall-percentage : CPU リソースのパーセンテージ (1 ~ 100)。設定された間隔の間、使用率がこのレベルより低下すると、CPU しきい値通知を送信します。 <p>この値は、rising percentage の値以下である必要があります。この値を指定しないと、falling fall-percentage の値は rising percentage の値と同じになります。</p>
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<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。

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、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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 contact text</code>	<p>システムに関する問い合わせ先を表すストリングを設定します。</p> <p>次に例を示します。</p> <pre>snmp-server contact Dial System Operator at beeper 21555.</pre>
ステップ 3	<code>snmp-server location text</code>	<p>システムのロケーションを表すストリングを設定します。</p> <p>次に例を示します。</p> <pre>snmp-server location Building 3/Room 222</pre>
ステップ 4	<code>end</code>	特権 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 を通して使用する TFTP サーバの制限

SNMP を通してコンフィギュレーション ファイルを保存およびロードするために使用する TFTP（簡易ファイル転送プロトコル）サーバを、アクセス リストに指定されているサーバに限定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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 を通してコンフィギュレーション ファイルをコピーするために使用する TFTP サーバを、アクセス リスト内のサーバに限定します。 <i>access-list-number</i> には、1 ~ 99 および 1300 ~ 1999 の標準 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、必要な回数だけコマンドを繰り返します。 <ul style="list-style-type: none"> <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。 deny キーワードは、条件が一致した場合にアクセスを拒否します。permit キーワードは、条件が一致した場合にアクセスを許可します。 <i>source</i> には、スイッチにアクセスできる TFTP サーバの IP アドレスを入力します。 (任意) <i>source-wildcard</i> には、<i>source</i> 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は 1 を設定します。 アクセス リストの末尾には、すべてに対す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>	特権 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 の全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、任意の SNMP マネージャがコミュニティストリング *public* を使用して、読み取り専用権限ですべてのオブジェクトにアクセスできます。この設定では、スイッチはトラップを送信しません。

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

次に、任意の SNMP マネージャがコミュニティストリング *public* を使用して、読み取り専用権限ですべてのオブジェクトにアクセスする例を示します。スイッチは、ホスト 192.180.1.111 および 192.180.1.33 (SNMPv1 を使用) や、ホスト 192.180.1.27 (SNMPv2C を使用) へ VTP トラップを送信します。コミュニティストリング *public* は、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、*comaccess* コミュニティストリングを使用するアクセスリスト 4 のメンバに、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する例を示します。その他の SNMP マネージャは、どのオブジェクトにもアクセスできません。SNMP 認証障害トラップは、SNMPv2C がコミュニティストリング *public* を使用してホスト *cisco.com* に送信します。

```
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ます。先頭行は、すでにイネーブルに設定されているトラップに加えて、エンティティ MIB トラップを送信するようにスイッチをイネーブルにします。2 行目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、コミュニティストリング *public* を使用して、すべてのトラップをホスト *myhost.cisco.com* に送信するようにスイッチをイネーブルにする例を示します。

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

次に、ユーザとリモートホストを関連付けて、ユーザがグローバル コンフィギュレーション モードのときに **auth** (authNoPriv) 認証レベルで情報を送信する例を示します。

```
Switch(config)# snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b
Switch(config)# snmp-server group authgroup v3 auth
Switch(config)# snmp-server user authuser authgroup remote 192.180.1.27 v3 auth md5
mypassword
Switch(config)# snmp-server user authuser authgroup v3 auth md5 mypassword
Switch(config)# snmp-server host 192.180.1.27 informs version 3 auth authuser config
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server inform retries 0
```

SNMP ステータスの表示

不正なコミュニティストリング エントリ、エラー、要求変数の数など、SNMP の入出力統計情報を表示するには、**show snmp** 特権 EXEC コマンドを使用します。また、表 33-6 に記載されたその他の特権 EXEC コマンドを使用して、SNMP 情報を表示することもできます。この場合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』を参照してください。

表 33-6 SNMP 情報を表示するためのコマンド

機能	デフォルト設定
show snmp	SNMP 統計情報を表示します。
show snmp engineID [local remote]	デバイス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。
show snmp group	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。
show snmp pending	保留中の SNMP 要求の情報を表示します。
show snmp sessions	現在の SNMP セッションの情報を表示します。
show snmp user	SNMP ユーザ テーブルの各 SNMP ユーザ名に関する情報を表示します。 (注) このコマンドは、 auth noauth priv モードの SNMPv3 設定情報を表示するときに使用する必要があります。この情報は、 show running-config の出力には表示されません。