CHAPTER 36

SNMP の設定

この章では、IE 3000 スイッチに Simple Network Management Protocol（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。

（注） この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド 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

SNMP の概要

SNMP は、マネージャとエージェントの間の通信のメッセージのフォーマットを提供する、アプリケーション層のプロトコルです。SNMP システムは、SNMP マネージャ、SNMP エージェント、および Management Information Base（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。エージェントと MIB はスイッチ上に存在します。スイッチで 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格納したりできます。エージェントは、装置パラメータやネットワーク データに関する情報のリポジトリである MIB から値を収集します。エージェントは、マネージャからのデータの取得要求または設定要求に応答することもできます。

また、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、ネットワーク上の特定の状態を 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を意味する場合があります。

ここでは、次の概念情報について説明します。

SNMP のバージョン

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

- SNMPv1：RFC 1157 に規定されている簡易ネットワーク管理プロトコル（完全インターネット標準）。
- SNMPv2C は、SNMPv2Classic のバルク取得機能を引き継ぎ、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トリングベースの管理フレームワークに置き換えたものです。SNMPv2C には次の機能があります。
  - SNMPv2：RFC 1902 ～ 1907 に規定されている簡易ネットワーク管理プロトコルのバージョン 2（ドラフト版インターネット標準）。
  - SNMPv2C：RFC 1901 に規定されている SNMPv2 のコミュニティストリング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：SNMP のバージョン 3 は、RFC 2273 ～ 2275 に規定されている相互運用可能な標準ベース プロトコルです。SNMPv3 は、ネットワーク上のパケットを認証および暗号化することで装置へのセキュアなアクセスを提供します。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：パケットが送信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混合して、許可されていない送信元が読み取ることができないようにします。

（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使用できます。

SNMPv1 と 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。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 アドレスの Access Control List（ACL; アクセス制御リスト）およびパスワードによって定義されます。

SNMPv2C は、バルク取得メカニズムと、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する機能を備えています。バルク取得メカニズムは、テーブルや大量の情報を取得し、必要な往復回数を最小限に抑えます。SNMPv2C では、エラー処理機能が改善され、さまざまな種類のエラー状態を区別する拡張エラー コードが使用されています。これらの状態は、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 パケットを処理するときに使用されるセキュリティ 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 36-1 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 36-1　SNMP のセキュリティ モデルとセキュリティ 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	不可	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	不可	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	不可	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）	不可	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。
SNMPv3	authPriv（暗号化ソフトウェア イメージが必要）	MD5 または SHA	データ暗号化規格（DES）または高度暗号化規格（AES）	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。次の暗号化アルゴリズムを使用する User-based Security Model（USM）を指定できます。 • CBC-DES（DES-56）規格に基づく認証および DES 56 ビット暗号化 • 3DES 168 ビット暗号化 • AES 128 ビット、192 ビット、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ので、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 の情報を使用して、表 36-2 に示す動作を実行します。

表 36-2　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、大きいデータ ブロックを取得します。通常、このようなデータは、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ります。
get-response	NMS から送信される 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 マネージャに送信さ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て、必要な変数を検出します。
2. **get-bulk** コマンドを使用できるのは、SNMPv2 以降だけです。

SNMP エージェント機能

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。

また、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、非送信請求トラップ メッセージを送信します。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 ストリング

SNMP コミュニティ ストリングは、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ためには、NMS のコミュニティ ストリング定義が、スイッチ上の 3 つのコミュニティ ストリング定義の少なくとも 1 つに一致する必要があります。

コミュニティ ストリングには、次の 3 つの属性のいずれかを指定できます。

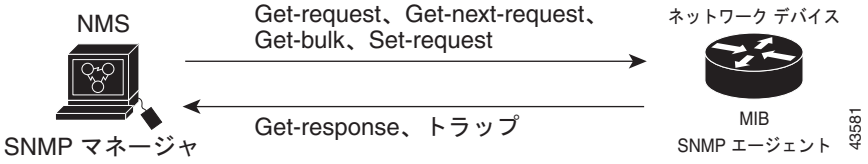
- 読み取り専用（RO）：許可された管理ステーションに対して、コミュニティ ストリングを除く MIB 内のすべてのオブジェクトへの読み取りアクセスを許可しますが、書き込みアクセスは許可しません。
- 読み書き（RW）：許可された管理ステーションに対して、MIB 内のすべてのオブジェクトへの読み書きアクセスを許可しますが、コミュニティ ストリングへのアクセスは許可しません。
- クラスタを作成すると、メンバー スイッチと SNMP アプリケーション間のメッセージ交換がコマンド スイッチによって管理されます。Network Assistant ソフトウェアは、コマンド スイッチ上で最初に設定された RW コミュニティ ストリングと RO コミュニティ ストリングにメンバー スイッチ番号（*@esN*、*N* はスイッチ番号）を追加し、これらのストリングをメンバー スイッチに伝播します。詳細については、第 6 章「スイッチのクラスタ化」および Cisco.com の『*Getting Started with Cisco Network Assistant*』を参照してください。

SNMP による MIB 変数へのアクセス

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 変数を使用して装置変数を設定し、ネットワーク上の装置をポーリングして特定の情報を取得します。ポーリングの結果は、グラフで表示できます。この結果を解析して、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 パフォーマンスの向上、装置の設定確認、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 36-1 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 マネージャにトラップ（特定のイベントの通知）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、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、ネットワーク上の状況を SNMP マネージャに通知します。また、SNMP エージェントは、*get-request*、*get-next-request*、および *set-request* の形式で SNMP マネージャから送信される MIB 関連のクエリーに応答します。

図 36-1　SNMP ネットワーク



サポートされる MIB の詳細、および MIB へのアクセス方法については、付録 A「サポートされる MIB」を参照してください。

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場合、キーワード *traps* はトラップか情報、またはその両方を表します。SNMP 通知をトラップとして送信するか情報として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 は情報をサポートしません。

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送信側にはわからないためです。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）でメッセージに確認応答します。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も意図した宛先に届く可能性が高くなります。

ただし、この特性によって、情報の方がトラップよりも信頼性が高くなる一方で、スイッチおよびネットワークで消費されるリソースが多くなります。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必要がある場合は、情報要求を使用してください。ネットワーク上またはスイッチのメモリ上のトラフィックが問題になる場合で、通知が不要なときは、トラップを使用してください。

SNMP ifIndex MIB オブジェクト値

NMS では、IF-MIB によって、インターフェイス インデックス（ifIndex）オブジェクト値の生成および割り当てを行います。このオブジェクト値は、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、インターフェイスに対してこれと同じ値が使用されます。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場合、スイッチの再起動後も同じ値が使用されます。

スイッチでは、表 36-3 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 36-3　ifIndex 値

インターフェイス タイプ	ifIndex の範囲
SVI[1]	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[2] モジュール インターフェイス）	10000 ～ 14500
ヌル	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（着脱可能小型フォーム ファクタ）

（注）　範囲内の連続した値が使用されるとは限りません。

SNMP の設定

SNMP のデフォルト設定

表 36-4 に、SNMP のデフォルト設定を示します。

表 36-4　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 レシーバー	設定なし。
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. スイッチを起動したときにスタートアップ 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

スイッチを起動したときに、スイッチのスタートアップ 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 コマンドが少なくとも 1 つ設定されていると、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 の設定時は、次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 コマンドによって、ユーザ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ている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ているすべてのユーザが影響を受けます。通知ビューを設定する必要がある場合の詳細については、『*Cisco IOS Network Management Command Reference*』を参照してください。
- リモート ユーザを設定する場合は、ユーザが存在する装置のリモート 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 とユーザ パスワードを使用して、認証およびプライバシ ダイジェストが算出されます。あらかじめリモート 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する必要があります。
- 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）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 のセキュリティ 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 の規定に従って破棄されます。この破棄により、エンジン ID の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 ユーザを再設定する必要があります。同様の理由から、エンジン ID を変更した場合は、コミュニティ ストリング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	**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	**no snmp-server**	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	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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、装置上で稼動し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）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、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。任意で、ストリングに関連付けられる次の特性を 1 つまたは複数指定できます。

- 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 アドレスのアクセス リスト
- 指定のコミュニティが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
- コミュニティがアクセスできる MIB オブジェクトに対する読み書き権限または読み取り専用権限

スイッチでコミュニティ 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	**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 community** *string* [**view** *view-name*] [**ro** | **rw**] [*access-list-number*]	コミュニティ ストリングを設定します。 **（注）** @ 記号は、コンテキスト情報を区切る場合に使用されます。このコマンドを設定するとき、@ 記号を SNMP コミュニティ ストリングの一部として使用しないでください。 • *string* 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）**view** 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（**ro**）を指定し、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（**rw**）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）*access-list-number* には、1 ～ 99 および 1300 ～ 1999 までの標準 IP アクセス リスト番号を入力します。
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	（任意）ステップ 2 で標準 IP アクセス リスト番号を指定し、そのあとにリストを作成する場合は、必要に応じてコマンドを繰り返します。 • *access-list-number* 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。 • *source* 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）*source-wildcard* には、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は 1 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

（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、読み取り専用アクセスを許可して、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の 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、その SNMP グループに新しいユーザを追加することができます。

スイッチで 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	**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** {**local** *engineid-string* | **remote** *ip-address* [**udp-port** *port-number*] *engineid-string*}	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。 • *engineid-string* は、SNMP のコピーの名前を指定する 24 文字の ID ストリングです。後続ゼロがある場合は、24 文字のエンジン ID 全体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、末尾までゼロだけ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、次のように入力できます。 **snmp-server engineID local 1234** • **remote** を指定した場合は、SNMP のリモート コピーが置かれている装置の *ip-address* を指定し、任意でリモート装置の User Datagram Protocol（UDP; ユーザ データグラム プロトコル）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** *groupname* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]	リモート装置に新しい SNMP グループを設定します。 • *groupname* には、グループの名前を指定します。 • セキュリティ モデルを指定します。 – **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伝送できます。 – **v3** は最も安全なセキュリティ モデルで、認証レベルを選択する必要があります。 **auth**：Message Digest 5（MD5）および Secure Hash Algorithm（SHA）によるパケット認証をイネーブルにします。 **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、この値がデフォルトになります。 **priv**：Data Encryption Standard（DES; データ暗号化規格）によるパケット暗号化（別名、*プライバシ*）をイネーブルにします。 **（注）** **priv** 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にだけ使用できます。 • （任意）**read** *readview* とともに、エージェントの内容の表示だけ可能な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** *writeview* とともに、データの入力とエージェントの内容の設定を行う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** *notifyview* 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** *access-list* とともに、アクセス リストの名前を表すストリング（64 文字以下）を入力します。

	コマンド	目的
ステップ 4	**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*]	SNMP グループの新しいユーザを追加します。 • *username* は、エージェントに接続するホスト上のユーザの名前です。 • *groupname* は、ユーザを関連付けるグループの名前です。 • **remote** を入力して、ユーザが属するリモート SNMP エンティティ、そのエンティティのホスト名または IP アドレス、さらに任意で 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。 – **encrypted** は、パスワードを暗号化形式で表示することを指定します。このキーワードは、**v3** キーワードが指定されている場合にだけ使用できます。 – **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**）認証レベルを指定できます。このオプションにはパスワード ストリング *auth-password*（64 文字以下）が必要です。 • **v3** を入力する場合、スイッチで暗号化ソフトウェア イメージが実行されているときは、プライベート（**priv**）暗号化アルゴリズムおよびパスワード ストリング *priv-password*（64 文字以下）を設定することもできます。 – **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、192 ビット、または 256 ビットの暗号化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 リストの名前を表すストリング（64 文字以下）を入力します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。 **（注）** **auth** | **noauth** | **priv** のモード設定に関する SNMPv3 情報を表示するには、**show snmp user** 特権 EXEC コマンドを入力する必要があります。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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で生成されるシステム 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ておらず、トラップは送信されません。この Cisco IOS リリースが稼動しているスイッチでは、設定できるトラップ マネージャの数に制限はありません。

（注）　コマンド構文で *traps* という単語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場合、キーワード **traps** はトラップか情報、またはその両方を表します。SNMP 通知をトラップとして送信するか情報として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 36-5 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いずれかまたはすべてをイネーブルにして、そのトラップを受信するようにトラップ マネージャを設定できます。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 36-5　スイッチの通知タイプ

通知タイプのキーワード	説明
bgp	Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）ステート変更トラップを生成します。このオプションは、Enhanced Multilayer Image（EMI）がインストールされ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ときに、トラップを生成します。
config	SNMP 設定が変更されたときに、トラップを生成します。
copy-config	SNMP コピー設定が変更されたときに、トラップを生成します。
entity	SNMP エンティティが変更されたときに、トラップを生成します。
cpu threshold	CPU に関連したトラップを許可します。
envmon	環境モニタ トラップを生成します。ファン、シャットダウン、ステータス、電源、温度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することができます。
errdisable	ポート VLAN が errdisable ステートになったときに、トラップを生成します。1 分あたりの最大トラップ レートも設定できます。指定できる範囲は 0 ～ 10000 です。デフォルト値は 0 で、レート制限がないことを意味します。
flash	SNMP FLASH 通知を生成します。
hsrp	Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）が変更されたときに、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ときに、トラップを生成します。
mac-notification	MAC アドレス通知トラップを生成します。
msdp	Multicast Source Discovery Protocol（MSDP）が変更されたときに、トラップを生成します。
ospf	Open Shortest Path First（OSPF）が変更されたときに、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、ステート変更のトラップのいずれかまたはすべてをイネーブルにすることができます。
pim	Protocol-Independent Multicast（PIM）が変更されたときに、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、Rendezvous Point（RP; ランデブー ポイント）マッピング変更のトラップのいずれかまたはすべてをイネーブルにすることができます。

表 36-5　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
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 レートも設定できます。指定できる範囲は 0 ～ 1000 です。デフォルト値は 0 で、レート制限がないことを意味します。 （注）　通知タイプ **port-security** を使用してトラップを設定する場合は、まずポート セキュリティ トラップを設定し、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。 • **snmp-server enable traps port-security** • **snmp-server enable traps port-security trap-rate** *rate*
rtr	SNMP Response Time Reporter（RTR）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、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 レートも設定できます。指定できる範囲は 0 ～ 1000 です。デフォルト値は 0 です（制限はなく、トラップは発生するたびに送信されます）。
stpx	SNMP STP 拡張 MIB トラップを生成します。
syslog	SNMP 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なっています。
vlan-membership	SNMP VLAN メンバーシップが変更されたときに、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）が変更されたときに、トラップを生成します。

（注）　**fru-ctrl**、**insertion**、および **removal** の各キーワードは、コマンドラインのヘルプ ストリングに表示されますが、サポートされていません。

表 36-5 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 コマンドを使用できます。

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** *ip-address engineid-string*	リモート ホストのエンジン ID を指定します。
ステップ 3	**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*]}	ステップ 2 で作成したリモート ホストに関連付ける 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、あらかじめリモート ホストのエンジン ID を設定しておく必要があります。設定していない場合、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。

	コマンド	目的
ステップ 4	**snmp-server group** *groupname* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]	SNMP グループを設定します。
ステップ 5	**snmp-server host** *host-addr* [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}}] *community-string* [*notification-type*]	SNMP トラップ動作の受信側を指定します。 • *host-addr* 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** を入力します。 • （任意）SNMP トラップをホストに送信するには、**traps**（デフォルト）を入力します。 • （任意）SNMP **version**（**1**、**2c**、または **3**）を指定します。SNMPv1 は情報をサポートしません。 • （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使用できます。 • *community-string* には、**version 1** または **version 2c** を指定した場合は、通知処理で送信されるパスワードと類似したコミュニティ ストリングを入力します。**version 3** を指定した場合は、SNMPv3 ユーザ名を入力します。 **（注）** @ 記号は、コンテキスト情報を区切る場合に使用されます。このコマンドを設定するとき、@ 記号を SNMP コミュニティ ストリングの一部として使用しないでください。 • （任意）*notification-type* には、表 36-5（P.36-13）に示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。
ステップ 6	**snmp-server enable traps** *notification-types*	トラップまたは情報を送信するようにスイッチでイネーブルにし、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 36-5（P.36-13）を参照するか、**snmp-server enable traps ?** と入力してください。 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。 **（注）** 通知タイプ **port-security** を使用してトラップを設定する場合は、まずポート セキュリティ トラップを設定し、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。 • **snmp-server enable traps port-security** • **snmp-server enable traps port-security trap-rate** *rate*
ステップ 7	**snmp-server trap-source** *interface-id*	（任意）送信元インターフェイスを指定します。そのインターフェイスから、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** *length*	（任意）各トラップ ホストのメッセージ キューの長さを設定します。指定できる範囲は 1 ～ 1000 です。デフォルト値は 10 です。
ステップ 9	**snmp-server trap-timeout** *seconds*	（任意）トラップ メッセージを再送信する頻度を設定します。指定できる範囲は 1 ～ 1000 です。デフォルトは 30 秒です。

	コマンド	目的
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。 （注）　**auth** | **noauth** | **priv** のモード設定に関する SNMPv3 情報を表示するには、**show snmp user** 特権 EXEC コマンドを入力する必要があります。
ステップ 12	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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（トラップおよび情報）のメカニズムをグローバルにイネーブルにします。ホストが情報を受信できるようにするには、そのホストについて **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。

CPU スレッシュホールドの通知タイプと値の設定

CPU スレッシュホールドの通知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	**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	**process cpu threshold type** {**total** | **process** | **interrupt**} **rising** *percentage* **interval** *seconds* [**falling** *fall-percentage* **interval** *seconds*]	CPU スレッシュホールドの通知タイプと値を設定します。 • **total**：CPU 総使用率に対する通知タイプを設定します。 • **process**：CPU プロセス使用率に対する通知タイプを設定します。 • **interrupt**：CPU 割り込み率に対する通知タイプを設定します。 • **rising** *percentage*：CPU リソースのパーセント値（1 ～ 100）を指定します。設定した期間この値を上回ると、CPU スレッシュホールドの通知が送信されます。 • **interval** *seconds*：CPU スレッシュホールド超過の期間を秒単位（5 ～ 86400）で指定します。超過期間がこの値に達すると、CPU スレッシュホールドの通知が送信されます。 • **falling** *fall-percentage*：CPU リソースのパーセント値（1 ～ 100）を指定します。設定した期間使用率がこの値を下回ると、CPU スレッシュホールドの通知が送信されます。 この値は、**rising** *percentage* 値以下にする必要があります。**falling** *fall-percentage* 値は、指定しない場合、**rising** *percentage* 値と同じになります。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

エージェント コンタクトおよびロケーションに関する情報の設定

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	**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 contact** *text*	システム コンタクトを表すストリングを設定します。 次に例を示します。 `snmp-server contact Dial System Operator at beeper 21555.`
ステップ 3	**snmp-server location** *text*	システム ロケーションを表すストリングを設定します。 次に例を示します。 `snmp-server location Building 3/Room 222`
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

SNMP を介して使用する TFTP サーバの制限

SNMP を介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 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	**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 tftp-server-list** *access-list-number*	SNMP を介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。 *access-list-number* には、1 ～ 99 および 1300 ～ 1999 までの標準 IP アクセス リスト番号を入力します。

	コマンド	目的
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	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。 • *access-list-number* 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。 • *source* 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）*source-wildcard* には、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は 1 を指定します。 アクセス リストの最後には、すべての要素に対する暗黙の拒否ステートメントが常にあることに注意してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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、任意の SNMP マネージャがコミュニティ ストリング *public* を使用してすべてのオブジェクトに読み取り専用権限でアクセスできます。また、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例を示します。スイッチは、SNMPv1 を使用してホスト 192.180.1.111 とホスト 192.180.1.33 に、SNMPv2C を使用してホスト 192.180.1.27 に 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 のメンバーに対して、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 認証失敗トラップは、コミュニティ ストリング *public* を使用して SNMPv2C からホスト *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ます。1 行目は、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** コマンドを上書きします。

```
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、ユーザをリモート ホストに関連付け、ユーザがグローバル コンフィギュレーション モードになったときに **auth**（authNoPriv）認証レベルの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、要求された変数の数など、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 36-6 に示すその他の特権 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。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 36-6　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]	装置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 要求に関する情報を表示します。
show snmp sessions	現在の SNMP セッションに関する情報を表示します。
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）** **auth | noauth | priv** のモードについて SNMPv3 設定情報を表示するには、このコマンドを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。