CHAPTER 29

SNMP の設定

この章では、Cisco ME 3400 イーサネット アクセス スイッチで 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） この章で使用す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。URL は次のとおりです。
http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_book.html
MIB（管理情報ベース）一括統計情報データ収集およびプロセス MIB の設定のためのコマンドの詳細については『*Cisco IOS Commands Master List, Release 12.4*』を参照してください。URL は次のとおりです。
http://www.cisco.com/en/US/products/ps6350/products_product_indices_list.html

- 「SNMP の概要」（P.29-1）
- 「SNMP の設定」（P.29-7）
- 「SNMP ステータスの表示」（P.29-24）

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。トラップには、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、ネイバーとの接続の切断、その他重要なイベントがあります。

スイッチは Cisco Data Collection MIB をサポートしませんが、CLI（コマンドライン インターフェイス）を使用して、選択した MIB データを特定の NMS ステーションに定期的に転送できます。このリリース以降では、Cisco Process MIB CPU しきい値テーブルの設定もできます。

ここでは、次の概要について説明します。

- 「SNMP のバージョン」（P.29-2）
- 「SNMP マネージャの機能」（P.29-3）
- 「SNMP エージェントの機能」（P.29-4）
- 「SNMP コミュニティ ストリング」（P.29-4）
- 「SNMP による MIB 変数へのアクセス」（P.29-4）
- 「SNMP 通知」（P.29-5）
- 「SNMP ifIndex MIB オブジェクト値」（P.29-6）
- 「MIB データの収集および転送」（P.29-6）

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（RFC1157 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 ストリング 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。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ドラフト（RFC1902 ～ 1907 に定義）
  - SNMPv2C：SNMPv2 に対応するコミュニティストリング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。次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、キーワード **priv** 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は、IP アドレスの Access Control List（ACL; アクセス コントロール 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 コードを使用してレポートされます。SNMPv2C のエラー リターン コードが、エラー タイプをレポートします。

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 レベルの組み合せによって、SNMP パケットを処理する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 29-1 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せた場合の特性を示します。

表 29-1　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 ストリング	不可	認証にコミュニティ ストリングの照合を使用します。
SNMPv2C	noAuthNoPriv	コミュニティ ストリング	不可	認証にコミュニティ ストリングの照合を使用します。
SNMPv3	noAuthNoPriv	ユーザ名	不可	認証にユーザ名の照合を使用します。
SNMPv3	authNoPriv	MD5（Message Digest 5）または SHA（Secure Hash Algorithm）	不可	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（Data Encryption Standard）または AES（Advanced Encryption Standard）	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。 次の暗号化アルゴリズムで USM（User-based Security Model）を指定できます。 • CBC-DES（DES-56）標準に基づいて、認証に加えて DES（56 ビット）暗号化を提供 • 3DES 168 ビット暗号化 • AES 128 ビット、192 ビット、256 ビット暗号化

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、SNMPv3 のいずれか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 29-2 に示す動作を実行します。

表 29-2　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。

表 29-2　SNMP の動作 （続き）

動作	説明
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 ストリング

SNMP コミュニティ ストリングは 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 ストリングの定義が、スイッチ上の 3 つのコミュニティ ストリングの定義と 1 つまたは複数一致する必要があります。

コミュニティ ストリングは、次のいずれかのアトリビュートを持ちます。

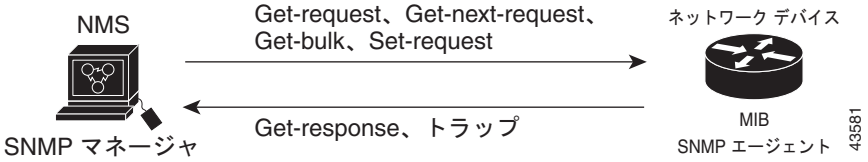
- read-only（RO）: 許可した管理ステーションに、コミュニティ ストリングを除く MIB 内のオブジェクトすべてに対する読み取りアクセス権を与えます。ただし、書き込みアクセスは許可しません。
- read-write（RW）: 許可した管理ステーションに、MIB 内のオブジェクトすべてに対する読み取りおよび書き込みアクセス権を与えます。ただし、コミュニティ ストリングへのアクセスは許可しません。

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。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、ネットワーク間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 29-1 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 関連のクエリーに応答します。

図 29-1　　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、トラップまたは情報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。

レシーバー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。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 値を割り当てる場合、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 値を割り当てるときに、表 29-3 に記載されている値の 1 つを使用します。

表 29-3　ifIndex 値

インターフェイス タイプ	ifIndex 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。

MIB データの収集および転送

MIB データをデバイスから特定の NMS に定期的に転送するように設定するには、複数の MIB からのデータをリストにグループ化し、ポーリング インターバルを設定します。リスト内のすべての MIB オブジェクトは特定のインターバルでポーリングされ、データは、設定された転送インターバルで特定の NMS に転送されます。定期的なデータの収集および転送のメカニズムは、*bulk-statistics* 機能と呼ばれます。

一括統計情報を設定するには、bulk-statistics オブジェクト リストを使用して、モニタする SNMP オブジェクト タイプと、収集するオブジェクトのインスタンスを指定する bulk-statistics スキーマを指定します。一連の Object Identifier（OID; オブジェクト ID）を使用して、MIB、MIB テーブル、MIB オブジェクト、およびオブジェクト インデックスを指定できます。

- bulk-statistics オブジェクト リストは、ユーザが指定した名前により識別される同じ MIB インデックスを共有するユーザ指定の一連の MIB オブジェクトです。
- bulk-statistics スキーマは、ユーザが指定した名前により識別され、オブジェクト リストの名前、オブジェクト リスト内のオブジェクトのために取得されるインスタンス、およびポーリング インターバルが含まれています。

収集するデータを設定すると、収集されたすべてのデータにより、1 つの仮想の bulk-statistics ファイルが作成されます。ファイルを NMS（FTP、RCP、または TFTP）に転送する方法、ファイルを転送する頻度（デフォルトは 30 分）、およびセカンダリ宛先（プライマリ NMS が使用できない場合）を指定できます。転送インターバルの時間は、収集インターバルの時間でもあります。収集インターバルが

終了したあと、bulk-statistics ファイルはフリーズされ、新しいローカルの bulk-statistics ファイルが新しいデータを保存するために作成されます。フリーズしたファイルは指定された宛先に転送されたあと、削除されます（ファイルを指定した期間メモリ内に保存するようにデバイスを設定していない場合）。転送が失敗した場合に SNMP 通知を NMS に送信し、ローカル デバイスに Syslog メッセージを入力するように、スイッチを設定できます。

SNMP の設定

- 「SNMP のデフォルト設定」（P.29-7）
- 「SNMP 設定時の注意事項」（P.29-7）
- 「SNMP エージェントのディセーブル化」（P.29-8）
- 「コミュニティ ストリングの設定」（P.29-9）
- 「SNMP グループおよびユーザの設定」（P.29-10）
- 「SNMP 通知の設定」（P.29-12）
- 「エージェント コンタクトおよびロケーションの設定」（P.29-17）
- 「SNMP 経由で使用する TFTP サーバの制限」（P.29-17）
- 「MIB データ収集および転送の設定」（P.29-18）
- 「Cisco Process MIB CPU しきい値テーブルの設定」（P.29-21）
- 「MIB データ収集および転送の設定」（P.29-18）

SNMP のデフォルト設定

表 29-4　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**）を除いてイネーブルなし。
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	キーワードを指定しない場合、デフォルトは **noauth**（noAuthNoPriv）セキュリティ レベルです。
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. スイッチが起動してスタートアップ 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 コマンドがない場合、これがデフォルトです。

SNMP 設定時の注意事項

スイッチが起動して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 コマンドがある場合、SNMP エージェントはイネーブルです。

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 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*』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。
- 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 パスワードはそのあと、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、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）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 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-name or 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します。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、パスワードのように機能し、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。任意の文字数で、1 つまたは複数のコミュニティ ストリングを設定できます。 • （任意）**view** 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。 • （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（**ro**）、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（**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への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 の範囲で標準の 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*]	（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、リストを作成して必要な回数だけこの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。 • キーワード **deny** 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。キーワード **permit** 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。 • *source* には、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 アドレスを入力します。 • （任意）*source-wildcard* 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 を入れます。 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文が常に存在す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）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）。

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、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、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 コピーのいずれかの名前を設定します。 • *engineid-string* 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、123400000000000000000000 のエンジン ID を設定する場合は、**snmp-server engineID local 1234** と入力します。 • **remote** 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 *ip-address*、および任意でリモート デバイス上でデータの格納に使用する UDP ポートを指定します。デフォルトは 162 です。
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 デバイスに新規の SNMP グループを設定します。 • *groupname* には、グループ名を指定します。 • セキュリティ モデルを指定します。 – **v1** 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。 – **v2c** は、2 番目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。 – **v3** 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。 **auth**：MD5 および SHA パケット認証をイネーブルにします。 **noauth**：noAuthNoPriv 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い場合は、このレベルがデフォルトです。 **priv**：Data Encryption Standard（DES; データ暗号化規格）パケット暗号化（別名 *プライバシー*）をイネーブルにします。 **（注）** キーワード **priv** 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だけ使用できます。 • （任意）**read** *readview* には、エージェントの内容表示だけが可能なビューの名前を示すストリング（64 文字以下）を指定して、入力します。 • （任意）**write** *writeview* 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ストリング（64 文字以下）を指定して、入力します。 • （任意）**notify** *notifyview* 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ストリング（64 文字以下）を指定して、入力します。 • （任意）**access** *access-list* には、アクセス リストの名前を示すストリング（64 文字以下）を指定して、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 グループの新規ユーザを追加します。 • *username* は、エージェントに接続されたホスト上のユーザ名です。 • *groupname* は、ユーザが関連付けられているグループの名前です。 • 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、**remote** 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、次のオプションを使用します。 – **encrypted** は、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。キーワード **v3** を指定している場合だけこのキーワードが使用可能です。 – **auth** は、認証レベル設定セッションです。HMAC-MD5-96（**md5**）または HMAC-SHA-96（**sha**）認証レベルのいずれかを指定でき、パスワード ストリング *auth-password*（64 文字以下）が必要となります。 • **v3** を入力し、スイッチが暗号ソフトウェア イメージを実行している場合、プライベート（**priv**）暗号化アルゴリズムとパスワード ストリング *priv-password*（64 文字以下）も設定できます。 – **priv** は、USM（User-based Security Model）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* には、アクセス リストの名前を示すストリング（64 文字以下）を指定して、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** モード設定の 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）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。スイッチには、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 29-5 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 29-5　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）状態変化トラップを生成。このオプションは、メトロ IP アクセス イメージがインストールされている場合に限り使用できます。
bridge	STP ブリッジ MIB トラップを生成。
bulkstat collection transfer	データ収集またはデータ転送が失敗した場合、または bulkstats ファイルが最大サイズに達した場合にトラップを生成。
config	SNMP 設定の変更時にトラップを生成。
copy-config	SNMP コピー設定の変更時にトラップを生成。
cpu threshold	CPU しきい値超過時にトラップを生成。
entity	SNMP エンティティの変更時にトラップを生成。
envmon	環境モニタ トラップを生成。ファン、シャットダウン、ステータス、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できます。
ethernet	SNMP イーサネット トラップを生成。
flash	SNMP FLASH 通知を生成。
hsrp	Hot Standby Router Protocol（HSRP）の変更時にトラップを生成。
ipmulticast	IP マルチキャスト ルーティングの変更時にトラップを生成。
mac-notification	MAC アドレス通知のトラップを生成。
msdp	Multicast Source Discovery Protocol（MSDP）の変更時にトラップを生成。
ospf	Open Shortest Path First（OSPF）変更時にトラップを生成。シスコ固有のエラー、リンク ステート アドバタイズメント、レート リミット、再送信、状態変化のトラップの一部またはすべてをイネーブルにできます。
pim	Protocol-Independent Multicast（PIM）の変更時にトラップを生成。無効な PIM メッセージ、ネイバーの変更、rendezvous point（RP; ランデブー ポイント）マッピングの変更のトラップの一部またはすべてを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。秒あ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、デフォルトは 0（レート制限なし）です。 （注）　通知タイプ **port-security** を使用してトラップを設定する場合、まずポート セキュリティ トラップを設定し、そのあとポート 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）に対してトラップを生成
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 ダウン時の SNMP タイプ通知のトラップを生成

表 29-5　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
storm-control	SNMP ストーム制御のトラップを生成。分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、デフォルトは 0 です（無制限、発生するたびにトラップを送信）。
stpx	SNMP STP 拡張 MIB トラップを生成。
syslog	SNMP Syslog トラップを生成。
tty	TCP 接続時にトラップを生成。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 メンバシップの変更時にトラップを生成。
vlancreate	SNMP VLAN 作成トラップを生成。
vlandelete	SNMP VLAN 削除トラップを生成。

（注）　**flash insertion**、**flash removal**、**fru-ctrl**、および **vtp** 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。**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、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 コマンドを組み合せて使用します。

表 29-5 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、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 ホストに対応する SNMP ユーザを設定します。 （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。設定しない場合、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。
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。

	コマンド	目的
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。 • （任意）SNMP インフォームをホストに送信する場合は、**informs** を入力します。 • （任意）SNMP トラップをホストに送信する場合は、**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 はインフォームをサポートしていません。 • （任意）バージョン 3 の場合は、認証レベル（**auth**、**noauth**、または **priv**）を選択します。 **（注）** キーワード **priv** 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だけ使用できます。 • *community-string* では、**version 1** または **version 2c** を指定した場合、通知作業で送信されるパスワードと同様のコミュニティ ストリングを入力します。**version 3** を指定した場合、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します。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 29-5（P.29-13）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 29-5（P.29-13）を参照するか、または **snmp-server enable traps ?** を入力します。 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、まずポート セキュリティ トラップを設定し、そのあとポート 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。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 8	**snmp-server queue-length** *length*	（任意）各トラップ ホストのメッセージ キュー長を設定します。指定できる値の範囲は 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 メッセージの再送信間隔を定義します。指定できる値の範囲は 1 ～ 1000 秒で、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。

	コマンド	目的
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。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。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。

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	**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 しきい値通知のタイプと値を設定します。 • **total**：通知タイプを total CPU utilization に設定します。 • **process**：通知タイプを CPU process utilization に設定します。 • **interrupt**：通知タイプを CPU interrupt utilization に設定します。 • **rising** *percentage*：CPU リソースのパーセンテージ（1 ～ 100）。設定されたインターバルを超えると、CPU しきい値通知を送信します。 • **interval** *seconds*：CPU しきい値超過の時間（単位は秒、5 ～ 86400）。条件を満たす場合、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）。使用度合いが設定されたインターバルのレベルを下回ったときに、CPU しきい値通知を送信します。 この値は、**rising** *percentage* 値以下でなければなりません。指定されていない場合、**falling** *fall-percentage* 値は **rising** *percentage* 値と同じです。
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。 （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 EXEC コマンドを入力する必要があります。
ステップ 5	**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。

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	**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 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 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）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、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。 *access-list-number* 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。

	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 リストを作成します。必要な回数だけこの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。 • キーワード **deny** 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。キーワード **permit** 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。 • *source* 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。 • （任意）*source-wildcard* 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 を入れます。 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文が常に存在す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）コンフィギュレーション ファイルに設定を保存します。

MIB データ収集および転送の設定

ここでは、MIB データ収集のための基本的な設定について説明します。詳細については、『*Periodic MIB Data Collection and Transfer Mechanism*』フィーチャ モジュールを参照してください。URL は次のとおりです。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/products_feature_guide09186a008014c77d.html

bulk-statistics オブジェクト リストおよびスキーマ オプションを設定するには、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 mib bulkstat object-list** *list-name*	SNMP bulk-statistics オブジェクト リストを定義し、bulk-statistics object-list コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**add** {*object-name* | *oid*}	bulk-statistics オブジェクト リストに MIB オブジェクトを追加します。 • *object-name* には、リストに追加する MIB オブジェクトの名前を入力します。オブジェクト名は、Interfaces MIB または Cisco Committed Access Rate MIB からだけ入力できます。 • *oid* には、リストに追加する MIB オブジェクトのオブジェクト ID を入力します。 オブジェクト リスト内のすべてのオブジェクトは同じ MIB インデックス内になければなりませんが、同じ MIB テーブルに属している必要はありません。モニタする、すべてのオブジェクトが追加されるまで、このコマンドを繰り返します。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**snmp mib bulkstat schema** *schema-name*	SNMP 一括統計情報スキーマに名前を付け、bulk-statistics スキーマ コンフィギュレーション モードを開始します。
ステップ 6	**object-list** *list-name*	このスキーマに含める bulk-statistics オブジェクト リストを指定します。オブジェクト リストは、スキーマごとに 1 つだけ指定します。複数の **object-list** コマンドが入力された場合、最新のコマンドが以前のコマンドを上書きします。
ステップ 7	**instance** {**exact** | **wild**} {**interface** *interface-id* | **oid** *oid*}	このスキーマ内のオブジェクトにインスタンス情報を指定します。スキーマごとに **instance** コマンドを 1 つだけ入力します。複数の **instance** コマンドが入力された場合、最新のコマンドが以前のコマンドを上書きします。 • オブジェクト リストに付加された特定のインスタンスが完全な OID である場合、**exact** を入力します。 • 指定された OID のすべてのサブインデックスがそのスキーマに属している場合、**wild** を入力します。 • **interface** *interface-id* を入力して、インスタンス OID ではなく、インスタンス ID を指定します。 • **oid***oid* を入力して、スキーマのインスタンス OID を指定します。
ステップ 8	**poll interval** *interval*	スキーマで指定されたオブジェクト インスタンスからのデータ収集のタイム インターバルを分単位で設定します。指定できる範囲は 1 ～ 20000 分で、デフォルトは 5 分です。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**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。

次の例では、bulk-statistics オブジェクト リストおよびスキーマを設定します。

```
Switch(config)# snmp mib bulkstat object-list ifMIB
Switch(config-bulk-objects)# add 1.3.6.1.2.1.2.1.2.2.2.1.11
Switch(config-bulk-objects)# add ifName
Switch(config-bulk-objects)# exit
Switch(config)# snmp mib bulkstat schema testschema
Switch(config-bulk-sc)# object-list ifMIB
Switch(config-bulk-sc)# instance wild oil 1
Switch(config-bulk-sc)# poll-interval 1
Switch(config-bulk-sc)# exit
```

bulk-statistics 転送オプションを設定するには、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 mib bulkstat transfer** *transfer-id*	転送設定を名前で特定し、bulk-statistics 転送コンフィギュレーション モードを開始します。
ステップ 3	**buffer-size** *bytes*	（任意）bulk-statistics データ ファイルの最大サイズ（バイト）を指定します。指定できる範囲は 1024 ～ 2147483647 バイトで、デフォルトは 2048 バイトです。
ステップ 4	**format** {**bulkBinary** | **bulkASCII** | **schemaASCII**}	（任意）bulk-statistics データ ファイルのフォーマットを指定します。デフォルトは **schemaASCII** です。
ステップ 5	**schema** *schema-name*	転送する bulk-statistics スキーマを指定します。必要な数のスキーマに対し、このコマンドを繰り返します。複数のスキーマを転送設定に対応付けることができます。
ステップ 6	**transfer-interval** *minutes*	（任意）転送を試みる前に、システムが MIB データを収集する時間の長さを指定します。有効な範囲は 1 ～ 2147483647 分で、デフォルトは 30 分です。転送インターバルは、収集インターバルと同じです。
ステップ 7	**url primary** *URL*	bulk-statistics ファイルを転送する先の NMS（ホスト）および転送に使用するプロトコル（FTP、RCP、または TFTP）を指定します。オプションで、**url secondary** コマンドを入力して、バックアップの転送先も指定できます。
ステップ 8	**retry** *number*	（任意）再送信の回数を指定します。指定できる範囲は 1 ～ 100 で、デフォルトは 0（再送信しない）です。
ステップ 9	**retain** *minutes*	（任意）bulk-statistics ファイルをシステム メモリに保管する時間を指定します。有効な範囲は 0 ～ 20000 分で、デフォルトは 0（転送が成功するとファイルはすぐに削除される）です。
ステップ 10	**enable**	設定のための bulk-statistics データの収集および転送プロセスを開始します。定期的な収集および転送を開始するには、このコマンドを入力する必要があります。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show mib bulk transfer**	設定を確認します。
ステップ 13	**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。

収集プロセスを停止するには、**no enable** 転送コンフィギュレーション コマンドを入力します。動作を再開するには、再び **enable** コマンドを入力します。**enable** コマンドでプロセスを再開するたびに、データは新しい bulk-statistics ファイルに収集されます。

次に、bulk-statistics の転送を設定し、収集プロセスをイネーブルにする例を示します。

```
Switch(config)# snmp mib bulkstat transfer testtransfer
Switch(config-bulk-tr)# format schemaASCII
Switch(config-bulk-tr)# buffer-size 2147483647
Switch(config-bulk-tr)# schema testschema1
Switch(config-bulk-tr)# schema testschema2
Switch(config-bulk-tr)# transfer-interval 1
Switch(config-bulk-tr)# url primary tftp://host/folder/bulkstat1
Switch(config-bulk-tr)# retain 20
Switch(config-bulk-tr)# retry 2
Switch(config-bulk-tr)# enable
Switch(config-bulk-tr)# exit
```

show snmp mib bulk transfer 特権 EXEC コマンドを入力し、設定された転送オプションを表示します。

Cisco Process MIB CPU しきい値テーブルの設定

CLI を使用して、Cisco Process MIB CPU しきい値テーブルを設定できます。

（注）　Cisco Process MIB CPU しきい値テーブルの設定のためのコマンドの詳細については、『*Cisco IOS Commands Master List, Release 12.4*』を参照してください。URL は次のとおりです。
http://www.cisco.com/en/US/products/ps6350/products_product_indices_list.html

CPU しきい値テーブルを設定するには、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 statistics limit entry-percentage** *number* [**size** *seconds*]	プロセス エントリの制限および CPU 使用率の統計情報の履歴テーブルのサイズを設定します。 • **entry-percentage** *number* では、履歴テーブルの一部になるためにプロセスが使用しなければならない CPU 使用率（1 ～ 100%）を入力します。 • （任意）**size** *seconds* では、CPU 統計情報を履歴テーブルに保存する時間を秒単位で設定します。指定できる値の範囲は 5 ～ 86400 秒で、デフォルトは 600 秒です。
ステップ 3	**process cpu threshold type** {**total** | **process** | **interrupt**} **rising** *percentage* **interval** *seconds* [**falling** *percentage* **interval** *seconds*]	CPU しきい値通知のタイプと値を設定します。 • **threshold type** を **total** CPU utilization、CPU **process** utilization、または CPU **interrupt** utilization に設定します。 • **rising** *percentage* では、超過したときに CPU しきい値通知をトリガーする CPU リソースのパーセンテージ（1 ～ 100）を入力します。 • **interval** *seconds* では、CPU しきい値通知をトリガーするために必要な CPU しきい値超過の期間を秒単位（5 ～ 86400）で入力します。デフォルト値は 5 秒です。 • （任意）使用が設定されたインターバルのレベルを下回ったときに、CPU しきい値通知をトリガーする **falling** *percentage* **interval** *seconds* を設定します。パーセンテージは、上限パーセンテージと等しいか、またはそれ以下である必要があります。デフォルトでは、下限パーセンテージは上限パーセンテージと同じ値です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**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 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 MAC 通知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 mac-notification
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
```

次に、ユーザがグローバル コンフィギュレーション モードを開始した際に、ユーザ名とリモート ホストを関連付けて **auth**（authNoPriv）認証レベル インフォーム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
```

次の例では、SNMP 通知をイネーブルにして、定期的な MIB データ収集および転送メカニズムの転送ステータスに関する情報を提供する方法を示します（一括統計情報）。

```
Switch(config)# snmp-server enable traps bulkstat
Switch(config)# snmp-server host 192.180.1.27 informs version 2 public bulkstat
```

次の例では、SNMP 通知をイネーブルにして、Cisco Process MIB CPU しきい値テーブルに関する情報を提供する方法を示します。

```
Switch(config)# snmp-server enable traps cpu threshold
Switch(config)# snmp-server host 192.180.1.27 informs version 2 public cpu
```

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、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** 特権 EXEC コマンドを使用します。また、SNMP 情報の表示には、表 29-6 に記載されているその他の特権 EXEC コマンドも使用できます。この出力内のフィールドについては、『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*』を参照してください。

表 29-6　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 の統計情報を表示します。
show snmp engineID [**local** | **remote**]	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。
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 mib bulk transfer	定期的な MIB データ収集および転送メカニズム（一括統計情報機能）により生成されたファイルの転送ステータスを表示します。
show snmp pending	保留中の SNMP 要求を表示します。
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 テーブル内の各 SNMP ユーザ名に関する情報を表示します。 **（注）** **auth** | **noauth** | **priv** モードの 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** 出力には表示されません。