



簡易ネットワーク管理プロトコルの設定

- [SNMP の前提条件 \(1 ページ\)](#)
- [SNMP の制約事項 \(3 ページ\)](#)
- [SNMP に関する情報 \(4 ページ\)](#)
- [SNMP の設定方法 \(9 ページ\)](#)
- [SNMP ステータスのモニタリング \(25 ページ\)](#)
- [SNMP の例 \(26 ページ\)](#)
- [その他の参考資料 \(27 ページ\)](#)
- [簡易ネットワーク管理プロトコルの機能の履歴と情報 \(28 ページ\)](#)

SNMP の前提条件

サポートされている 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 : 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、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：有効な送信元からのメッセージである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。

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 にはバルク検索機能が組み込まれ、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。バルク検索機能は、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 では、セキュリティモデルとセキュリティレベルの両方が提供されています。セキュリティモデルは、ユーザ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とは、セキュリティモデル内で許可されるセキュリティのレベルです。セキュリティ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方式が決まります。使用可能なセキュリティモデルは、SNMPv1、SNMPv2C、および SNMPv3 です。

次の表では、この特性を識別し、セキュリティモデルとセキュリティレベルの異なる組み合わせを比較します。

表 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	未対応	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	未対応	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	未対応	ユーザ名の照合を使用して認証します。

モデル	レベル	認証	暗号化	結果
SNMPv3	authNoPriv	Message Digest 5 (MD5) または Secure Hash Algorithm (SHA)	未対応	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	MD5 または SHA	データ暗号規格 (DES) または Advanced Encryption Standard (AES)	<p>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。</p> <p>次の暗号化アルゴリズムで、User-based Security Model (USM) を指定できます。</p> <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せん。

SNMP の制約事項

バージョンの制約事項

- SNMPv1 は informs をサポートしていません。

SNMP に関する情報

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、および管理情報ベース (MIB) で構成されます。SNMP マネージャは、Cisco Prime Infrastructure などのネットワーク管理システム (NMS) に統合できます。エージェントおよび MIB は、デバイスに常駐します。デバイス上で 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。

SNMP マネージャ機能

SNMP マネージャは、MIB 情報を使用して、次の表に示す動作を実行します。

表 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。
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。

¹ この動作を使用した場合、SNMP マネージャは厳密な変数名を知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 オブジェクトへのアクセスを認証し、組み込みパスワードとして機能します。NMS がデバイスにアクセスするには、NMS 上のコミュニティストリング定義がデバイス上の3つのコミュニティストリング定義の少なくとも1つと一致しなければなりません。

コミュニティストリングの属性は、次のいずれかです。

- 読み取り専用 (RO)：コミュニティストリングを除き MIB 内のすべてのオブジェクトに、許可された管理ステーションに対する読み取りアクセス権を与えますが、書き込みアクセスは許可しません。
- 読み取り-書き込み (RW)：MIB 内のすべてのオブジェクトに、許可された管理ステーション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、コマンドデバイスがメンバデバイスと SNMP アプリケーション間のメッセージ交換を管理します。Network Assistant ソフトウェアは、コマンドデバイス上で最初に設定された RW および RO コミュニティストリングにメンバデバイス番号 (@esN、N はデバイス番号) を追加し、これらのストリングをメンバデバイスに伝播します。

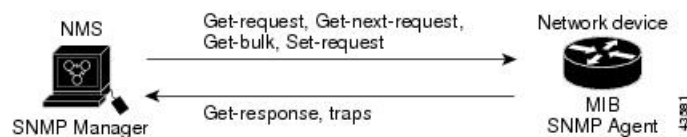
SNMP MIB 変数アクセス

NMS の例として、Cisco Prime Infrastructure ネットワーク管理ソフトウェアがあります。Cisco Prime Infrastructure ソフトウェアは、デバイス 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。

次の図に示すように、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、リンクステータス（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 関連のクエリに応答します。

図 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、デバイスから 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 応答プロトコルデータユニット (PDU) 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、デバイス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。再送信の回数が増え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高くなる原因にもなります。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デバイスの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。デバイスの再起動またはデバイスソフトウェアのアップグレード時に、デバイスは、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、デバイスのポート2に10003というifIndex値が割り当てられていると、デバイスの再起動後も同じ値が使用されます。

デバイスは、次の表内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 3: ifIndex 値

Interface Type	ifIndex 範囲
SVI ³	1 ~ 4999
EtherChannel	5001 ~ 5048
Tunnel	5078 ~ 5142
タイプ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SFP ⁴ モジュールインターフェイスなど）	10000 ~ 14500
ヌル	14501
ループバックおよびトンネル	24567+

³ SVI = スイッチ仮想インターフェイス

⁴ SFP = Small Form-Factor Pluggable

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 ⁵
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	バージョン 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。

⁵ これは、デバイスが起動し、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

デバイスが起動し、デバイスのスタートアップ 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 グループを設定するときには、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には、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、そのユーザを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。
- 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、デバイスは **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、RFC2274 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 ストリングも再設定する必要があります。

SNMP の設定方法

SNMP エージェントのディセーブル化

no snmp-server グローバル コンフィギュレーション コマンドは、デバイス上で実行している SNMP エージェント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）をディセーブルにします。入力した最初の **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 エージェントのすべてのバージョンを再度イネーブルにします。特に SNMP をイネーブルにするために指定された Cisco IOS コマンドはありません。

SNMP エージェントをディセーブルにするには、次の手順を実行します。

始める前に

SNMP エージェントをディセーブルにする前にイネーブルにする必要があります。デバイス上で入力した最初の **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 エージェントがイネーブルになります。

手順の概要

1. **enable**
2. **configureterminal**
3. **no snmp-server**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	configureterminal 例： Device# 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 3	no snmp-server 例：	SNMP エージェント動作をディセーブルにします。

	コマンドまたはアクション	目的
	Device(config)# no snmp-server	
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 5	show running-config 例： Device# show running-config	入力を確認します。
ステップ 6	copy running-config startup-config 例： Device# 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。

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、デバイス上のエージェントへのアクセスを許可する、パスワードと同様の役割を果たします。ストリング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

デバイス上でコミュニティストリングを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **snmp-server community string [view view-name] [ro | rw] [access-list-number]**
4. **access-list access-list-number {deny | permit} source [source-wildcard]**
5. **end**
6. **show running-config**

7. copy running-config startup-config

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configureterminal 例： Device# 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 3	snmp-server community string [view view-name] [ro rw] [access-list-number] 例： Device(config)# snmp-server community comaccess ro 4	コミュニティストリングを設定します。 (注) コンテキスト情報を区切るには @ 記号を使用します。このコマンドの設定時に SNMP コミュニティストリングの一部として @ 記号を使用しないでください。 <ul style="list-style-type: none"> <i>string</i> 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) <i>view</i> 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)、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) <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。

	コマンドまたはアクション	目的
ステップ 4	access-list access-list-number {deny permit} source [source-wildcard] 例 : Device(config)# access-list 4 deny any	(任意) ステップ 3 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。 <ul style="list-style-type: none"> • access-list-number には、ステップ 3 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、source 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 5	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 6	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 7	copy running-config startup-config 例 : Device# 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。

次のタスク

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tring を削除するには、**no snmp-server** コミュニティ 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。

デバイス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。

SNMP グループおよびユーザの設定

デバイス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。

デバイス上の SNMP グループとユーザを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **snmp-server engineID** { *local engineid-string* | *remote ip-address* [*udp-port port-number*] *engineid-string* }
4. **snmp-server group** *group-name readview writeview notifyview access-list* { *v1* | *v2c* | *v3* { *auth* | *noauth* | *priv* } } [*read*] [*write*] [*notify*] [*access*]
5. **snmp-server user** *username group-name host port access-list access-list access-list auth-passwordpriv password* { *remote* [*udp-port*] } { *v1* [*access*] | *v2c* [*access*] | *v3* [*encrypted*] [*access*] [*auth* {*md5* | *sha*}] } [{*ds* | *3ds* | *as* {*128* | *192* | *256*} }]
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します (要求された場合)。
ステップ 2	configureterminal 例 : Device# 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 3	snmp-server engineID { <i>local engineid-string</i> <i>remote ip-address</i> [<i>udp-port port-number</i>] <i>engineid-string</i> } 例 :	SNMP のローカル コピーまたはリモート コピーに名前を設定します。

	コマンドまたはアクション	目的
	<pre>Device(config)# snmp-server engineID local 1234</pre>	<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 を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。手順例では、123400000000000000000000 のエンジン ID を設定します。 • remote 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ユーザデータグラムプロトコル (UDP) ポートを指定します。デフォルトは 162 です。
ステップ 4	<pre>snmp-server group group-name readview writeview notifyview access <i>kv</i> {v1 v2c v3{auth noauth priv}} [read] [write] [notify] [access]</pre> <p>例 :</p> <pre>Device(config)# snmp-server group public v2c access lmnop</pre>	<p>リモート デバイス上で新しい SNMP グループを設定します。</p> <p><i>group-name</i> には、グループの名前を指定します。</p> <p>次のいずれかのセキュリティモデルを指定します。</p> <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 番目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。 • v3 最も安全な場合には、次の認証レベルの 1 つを選択する必要があります。 <p>auth : Message Digest 5 (MD5) およびセキュアハッシュアルゴリズム (SHA) によるパケット認証を可能にします。</p> <p>noauth : noAuthNoPriv セキュリティ レベルを可能にします。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 : データ暗号規格 (DES) によるパケット暗号化 (プライバシーともいう) を可能にします。</p> <p>(任意) read readview 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。</p>

	コマンドまたはアクション	目的
		<p>(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設定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。</p> <p>(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。</p> <p>(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。</p>
<p>ステップ 5</p>	<p>snmp-server user <i>username group-name host port access-list access-list access-list auth-passwordpriv</i> <i>remote</i> <i>ip</i> <i>udp</i> <i>port</i> <i>auth</i> <i>password</i> <i>priv</i> <i>remote</i> <i>ip</i> <i>udp</i> <i>port</i> <i>auth</i> <i>password</i> <i>priv</i></p> <p>例 :</p> <pre>Device(config)# snmp-server user Pat public v2c</pre>	<p>SNMP グループに対して新規ユーザを追加します。</p> <p><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。</p> <p><i>group-name</i> は、ユーザが関連付けられているグループの名前です。</p> <p>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。デフォルトは 162 です。</p> <p>SNMP バージョン番号 (v1、v2c、または v3) を入力します。v3 を入力すると、次のオプションが追加されます。</p> <ul style="list-style-type: none"> • encrypted 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 では、認証レベルを設定します。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ます。また、<i>auth-password</i> でパスワードの文字列を指定する必要があります (最大 64 文字)。 <p>v3 を入力すると、次のキーワードを使用して (64 文字以下)、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 <i>priv-password</i> を設定することもできます。</p> <ul style="list-style-type: none"> • priv ユーザベースセキュリティモデル (USM) を指定します。 • des 56 ビット DES アルゴリズムを使用する場合に指定します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • 3des 168 ビット DES アルゴリズムを使用する場合に指定します。 • aes DES アルゴリズムを使用する場合に指定します。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。 <p>(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。</p>
ステップ 6	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 7	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 8	copy running-config startup-config 例 : Device# 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ときにデバイス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 が稼働しているデバイスでは、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。

グローバルコンフィギュレーションコマンドを **snmp-server host** グローバルコンフィギュレーションコマンドと組み合わせて使用すると、次の表に示す通知タイプを特定のホストで受

信できます。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 4: デバイスの通知タイプ

通知タイプのキーワード	説明
bridge	STP 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。デバイススタックでは、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有効にできます。このようにすると、スタックからデバイスを削除するか、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、電源の再投入、またはリロードの場合に）、トラップが発行されます。
fru-ctrl	エンティティ現場交換可能ユニット (FRU) 制御トラップを生成します。デバイススタックでは、このトラップはスタックにおけるデバイスの挿入/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。
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。

通知タイプのキーワード	説明
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。 1. snmp-server enable trapsport-security 2. snmp-server enable trapsport-securitytrap-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。

通知タイプのキーワード	説明
vtp	VLAN トランッキングプロトコル (VTP) が変更された場合に、トラップを生成します。

ホストにトラップまたは情報を送信するようにデバイスを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **snmp-server engineID remote ip-address engineid-string**
4. **snmp-server user username group-name host port access-list access-list access-list auth-password {remote [udp-port]} {v1 [access] | v2c [access] | v3 [encrypted] [access] [auth {md5 | sha}]}**
5. **snmp-server group group-name {v1 | v2c | v3 {auth | noauth | priv}} [read readview] [write writeview] [notify notifyview] [access access-list]**
6. **snmp-server host host-addr [informs | traps] [version {1 | 2c | 3 {auth | noauth | priv}}] community-string [notification-type]**
7. **snmp-server enable traps notification-types**
8. **snmp-server trap-source interface-id**
9. **snmp-server queue-length length**
10. **snmp-server trap-timeout seconds**
11. **end**
12. **show running-config**
13. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードをイネーブルにします。 • パスワードを入力します (要求された場合)。
ステップ 2	configureterminal 例： Device# 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 3	snmp-server engineID remote ip-address engineid-string 例： Device (config)# snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b	リモート ホストのエンジン ID を指定します。

	コマンドまたはアクション	目的
ステップ 4	<pre>snmp-server user username group-name host port access-list access-list access-list [hostname] [v1[auth] v2[auth] v3[auth noauth priv]] [access-list] [notification-type]</pre> <p>例 :</p> <pre>Device(config)# snmp-server user Pat public v2c</pre>	<p>SNMP ユーザを設定し、ステップ 3 で作成したリモートホストに関連付けます。</p> <p>(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。</p>
ステップ 5	<pre>snmp-server group group-name {v1 v2c v3 {auth noauth priv}} [read readview] [write writeview] [notify notifyview] [access access-list]</pre> <p>例 :</p> <pre>Device(config)# snmp-server group public v2c access lmnop</pre>	<p>SNMP グループを設定します。</p>
ステップ 6	<pre>snmp-server host host-addr [informs traps] [version {1 2c 3 {auth noauth priv}}] community-string [notification-type]</pre> <p>例 :</p> <pre>Device(config)# snmp-server host 203.0.113.1 comaccess snmp</pre>	<p>SNMP トラップ動作の受信先を指定します。</p> <p><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。</p> <p>(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。</p> <p>(任意) SNMP 情報をホストに送信するには、informs を指定します。</p> <p>(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。</p> <p>(任意) バージョン 3 の場合、認証レベル auth、noauth、または priv を選択します。</p> <p>(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のみ使用可能です。</p> <p><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トリングを入力します。version 3 が指定されている場合、SNMPv3 ユーザ名を入力します。</p> <p>コンテキスト情報を区切るには @ 記号を使用します。このコマンドの設定時に SNMP コミュニティストリングの一部として @ 記号を使用しないでください。</p>

	コマンドまたはアクション	目的
		(任意) <i>notification-type</i> には、上の表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。
ステップ 7	snmp-server enable traps notification-types 例： Device(config)# snmp-server enable traps snmp	デバイスでのトラップまたはインフォームの送信を有効にし、送信する通知の種類を指定します。通知タイプの一覧については、上の表を参照するか、次のコマンドを入力してください。 snmp-server enable traps? 複数のトラップタイプを有効にするには、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。 <ol style="list-style-type: none"> snmp-server enable trapsport-security snmp-server enable trapsport-securitytrap-rate rate
ステップ 8	snmp-server trap-source interface-id 例： Device(config)# snmp-server trap-source GigabitEthernet1/0/1	(任意) 送信元インターフェイスを指定します。このインターフェイスによってトラップメッセージの IP アドレスが提供されます。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 9	snmp-server queue-length length 例： Device(config)# snmp-server queue-length 20	(任意) 各トラップホストのメッセージキューの長さを指定します。指定できる値の範囲は 1～5000 です。デフォルトは 10 です。
ステップ 10	snmp-server trap-timeout seconds 例： Device(config)# snmp-server trap-timeout 60	(任意) トラップメッセージを再送信する頻度を指定します。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 11	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 12	show running-config 例：	入力を確認します。

	コマンドまたはアクション	目的
	Device# <code>show running-config</code>	
ステップ 13	copy running-config startup-config 例 : Device# <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。

次のタスク

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 traps** コマンドによって、指定された通知方式（トラップおよび情報）がグローバルで有効になります。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有効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無効になりますが、情報は無効になりません。情報を無効にするには、**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無効にするには、**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接点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、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **snmp-server contact text**
4. **snmp-server location text**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例 :	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	Device> enable	
ステップ 2	configureterminal 例： Device# 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 3	snmp-server contact text 例： Device(config)# snmp-server contact Dial System Operator at beeper 21555	システムの連絡先文字列を設定します。
ステップ 4	snmp-server location text 例： Device(config)# snmp-server location Building 3/Room 222	システムの場所を表す文字列を設定します。
ステップ 5	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 6	show running-config 例： Device# show running-config	入力を確認します。
ステップ 7	copy running-config startup-config 例： Device# 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 を通して使用する TFTP サーバの制限

SNMP を介したコンフィギュレーションファイルの保存とロードに使用する TFTP サーバを、アクセス リストで指定されたサーバに限定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**

3. `snmp-server tftp-server-list access-list-number`
4. `access-list access-list-number source source-wildcard {deny|permit} []`
5. `end`
6. `show running-config`
7. `copy running-config startup-config`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"> • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# 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 3	snmp-server tftp-server-list access-list-number 例： Device(config)# snmp-server tftp-server-list 44	SNMP を介した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 4	access-list access-list-number source source-wildcard {deny permit} [] 例： Device(config)# access-list 44 permit 10.1.1.2	標準アクセスリストを作成し、コマンドを必要な回数だけ実行します。 <i>access-list-number</i> には、ステップ 3 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、デバイスにアクセスできる 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します。

	コマンドまたはアクション	目的
ステップ 5	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 6	show running-config 例： Device# show running-config	入力を確認します。
ステップ 7	copy running-config startup-config 例： Device# 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 ステータスのモニタリング

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、次の表にリスト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。

表 5: SNMP 情報を表示するためのコマンド

コマンド	目的
show snmp	SNMP 統計情報を表示します。
	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。

コマンド	目的
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。

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、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、デバイスはトラップを送信しません。

```
Device(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。デバイスはさらに、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 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。

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

```
Device(config)# snmp-server community comaccess ro 4
Device(config)# snmp-server enable traps snmp authentication
Device(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行めで、デバイスは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 トラップを送信できるようになります。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** ホストコマンドを無効にします。

```
Device(config)# snmp-server enable traps entity
Device(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* に送信するようにデバイスをイネーブルにする例を示します。

```
Device(config)# snmp-server enable traps
Device(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。

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

その他の参考資料

関連資料

関連項目	マニュアルタイトル
SNMP コマンド	『 <i>Network Management Command Reference, Cisco IOS Release 15.2(2)E</i> 』

エラーメッセージデコーダ

説明	Link
このリリースのシステムエラーメッセージを調査し解決するために、エラーメッセージデコーダツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	Title
なし	-

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	<p>選択したプラットフォーム、Cisco IOS リリース、およびフィッチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。</p> <p>http://www.cisco.com/go/mibs</p>

シスコのテクニカル サポート

説明	Link
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	<p>http://www.cisco.com/support</p>

簡易ネットワーク管理プロトコルの機能の履歴と情報

リリース	変更内容
Cisco IOS Release 15.0(2)EX1	この機能が導入されました。