



SNMP 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](#) (10 ページ)
- [SNMP の例](#) (18 ページ)
- [SNMP ステータスのモニタリング](#) (20 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	ユーザー名	未対応	ユーザー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す。

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

ここでは、SNMP の概要について説明します。

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。エージェントと MIB はネットワークデバイス上に存在します。デバイスに SNMP を設定するには、マネージャとエージェントの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 以上に限られます。



(注) パフォーマンスに関連する問題を回避するために、SNMP マネージャで **ciscoFlashFileDate** MIB オブジェクトをクエリから除外することを推奨します。これは、**ciscoFlashFileDate** オブジェクトが MIB で公開されていても、製品ではサポートされていないためです。

SNMP エージェント機能

SNMP エージェントは、1つ以上の SNMP マネージャから要求を受信できます。すべての要求に、NMS の IP アドレス、NMS がエージェントをポーリングした回数、およびポーリングのタイムスタンプが含まれます。この情報は、IPv4 サーバーと IPv6 サーバーの両方で追跡できます。

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。

※ **show snmp stats hosts** コマンドを使用してキュー内の SNMP マネージャ要求のリストを表示し、**clear snmp stats hosts** コマンドを使用してキューをクリアします。

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。

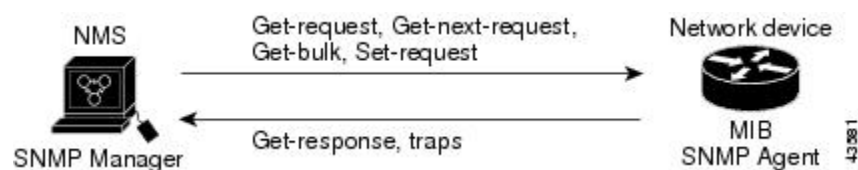
- 読み取り-書き込み (RW) : MIB 内のすべてのオブジェクトに、許可された管理ステーションに対する読み取りおよび書き込みアクセス権を与えますが、コミュニティストリングへのアクセスは許可しません。
- クラスタを作成すると、コマンドデバイスがメンバデバイスと SNMP アプリケーション間のメッセージ交換を管理します。Network Assistant ソフトウェアは、コマンドデバイス上で最初に設定された RW および RO コミュニティストリングにメンバデバイス番号 (@esN、N はデバイス番号) を追加し、これらのストリングをメンバデバイスに伝播します。

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 変数を使用してデバイス変数を設定し、ネットワーク上のデバイスをポーリングして特定の情報を取得します。ポーリング結果は、グラフ形式で表示されます。この結果を解析して、インターネットワーキング関連の問題のトラブルシューティング、ネットワークパフォーマンスの改善、デバイス設定の確認、トラフィック負荷のモニタなどを行うことができます。

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 マネージャから次の形式で送信される MIB 関連のクエリに応答します。 *get-request*、*get-next-request* にダウンロードすると、*set-request* 形式のファイル名を付けてファイルを保存します。

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、トラップまたはインフォームのどちらとして SNMP 通知を送信するかを指定します。



(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

SNMP エージェントの IF-MIB モジュールがリポート後すぐに起動されます。さまざまな物理インターフェイスドライバが IF-MIB モジュールの登録を初期化されているように、「インデックス番号をください」と示します。IF-MIB モジュールが先着順で使用可能な次の ifIndex 番号を割り当てます。つまり、1つのリポートから他のリポートへのドライバの初期化順序のマイナーな違いが、同じ物理インターフェイスにリポートを行う以前のものとは別のインデックス番号を取得する可能性があるということです (インデックス持続が有効化されていない限り)。

SNMP および Syslog Over IPv6

IPv4 と IPv6 の両方をサポートするには、IPv6 のネットワーク管理で IPv4 および IPv6 のトランスポートが必要になります。Syslog over IPv6 は、このトランスポートのアドレスデータタイプをサポートします。

Simple Network Management Protocol (SNMP) と syslog over IPv6 は、次の機能を提供します。

- IPv4 と IPv6 両方のサポート
- SNMP に対する IPv6 トランスポート、および SNMP 変更による IPv6 ホストのトラップのサポート
- IPv6 アドレス指定をサポートするための SNMP および syslog に関連する MIB
- IPv6 ホストをトラップレシーバとして設定

Over IPv6 をサポートするため、SNMP は既存の IP トランスポートマッピングを変更して、IPv4 と IPv6 を同時にサポートします。次の SNMP 動作は、IPv6 トランスポート管理をサポートします。

- デフォルト設定のユーザーデータグラムプロトコル (UDP) SNMP ソケットを開く

- ※ `SR_IPV6_TRANSPORT` と呼ばれる新しいトランスポート メカニズムを提供
- IPv6 トランスポートによる SNMP 通知の送信
- IPv6 トランスポートの SNMP 名のアクセス リストのサポート
- IPv6 トランスポートを使用した SNMP プロキシ転送のサポート
- SNMP マネージャ機能と IPv6 トランスポートの連動確認

設定手順を含む SNMP over IPv6 の詳細については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Managing Cisco IOS Applications over IPv6」の章を参照してください。

設定手順を含む、syslog over IPv6 については、Cisco.com で『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」の章を参照してください。

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 ³
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。

³ 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

デバイスでは、SNMP UDP ポート 161 および 162 を開き、SNMP エージェントを有効にするために、次のいずれかのグローバル コンフィギュレーション コマンドを設定する必要があります。 **snmp-server host**、または **snmp-server user**、または **snmp-server community**、または **snmp-server manager**に従って構成設定を変更します。

SNMP *group* は、SNMP ユーザーを SNMP ビューに対応付けるテーブルです。SNMP *user* は、SNMP グループのメンバーです。SNMP ホストは、トラップ動作の受信先です。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 コマンドがユーザーの通知ビューを自動生成し、そのユー

ザーに関連付けられてい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にリモートユーザーを設定する前に、SNMP エンジン ID を設定します。設定には、**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** オプションを指定して使用します。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。
- ローカルユーザー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**) の認証レベルのインフォームを送信しません。
- SNMP エンジン ID の値を変更すると、重大な影響が生じます。（コマンドラインで入力された）ユーザのパスワードは、パスワードおよびローカル エンジン ID に基づいて、MD5 または SHA セキュリティ ダイジェストに変換されます。コマンドラインのパスワードは、RFC 2274 の規定に従って廃棄されます。このようにパスワードが廃棄されるため、エンジン ID 値を変更した場合は、SNMPv3 ユーザーのセキュリティ 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 ユーザー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 サーバーホストをデフォルトの UDP ポート（162）で設定すると、**show running-config** コマンドの出力に UDP ポート値が表示されません。デフォルト以外の UDP ポート値を **snmp-server host {host-addr} community-string udp-port value** コマンドを使用して指定する場合は、UDP ポート番号が **show running-config** コマンド出力に表示されます。これを自動または手動で実行するように **snmp-server host** コマンドを、デフォルトの UDP ポート 162 を使用しても使用しなくても設定できます。ただし、両方を同時に設定することはできません。

正しい例を次に示します。

```
Device(config)# snmp-server host 10.10.10.10 community udp-port 163
Device(config)# snmp-server host 10.10.10.10 community
```

```
Device(config)# snmp-server host 10.10.10.10 community udp-port 163
Device(config)# snmp-server host 10.10.10.10 community udp-port 162
```

次の例は正しくありません。

```
Device(config)# snmp-server host 10.10.10.10 community udp-port 163
Device(config)# snmp-server host 10.10.10.10 community
Device(config)# snmp-server host 10.10.10.10 community udp-port 162
```

```
Device(config)# snmp-server host 10.10.10.10 community udp-port 163
Device(config)# snmp-server host 10.10.10.10 community udp-port 162
Device(config)# snmp-server host 10.10.10.10 community
```

SNMP の設定方法

ここでは、SNMP の設定方法について説明します。

SNMP コミュニティ スtring

SNMP コミュニティ スtringは、MIB オブジェクトへのアクセスを認証し、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tring定義がデバイス上の3つのコミュニティ スtring定義の少なくとも1つと一致しなければなりません。

コミュニティ スtring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tring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tring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tring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Stringをメンバデバイスに伝播します。

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. **configure terminal**
3. **snmp-server engineID** {local engineid-string | remote ip-address [udp-port port-number] engineid-string}
4. **snmp-server group** group-name {v1 | v2c | v3 {auth | noauth | priv}} [read readview] [write writeview] [notify notifyview] [access access-list]
5. **snmp-server user** username group-name {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]
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> <code>enable</code>	特権 EXEC モードを有効にします。 <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# <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 3	snmp-server engineID {local engineid-string remote ip-address [udp-port port-number] engineid-string} 例： Device(config)# <code>snmp-server engineID local 1234</code>	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。 <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tring です。後続ゼロが含まれる場合は、24 文字のエンジン ID すべてを指定する必要はありません。指定するのは、エンジン ID のうちゼロのみが続く箇所を除いた部分だけです。手順例では、12340000000000000000000000 のエンジン ID を設定します。 • ※ remote を選択した場合、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ー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	snmp-server group group-name {v1 v2c v3 {auth noauth priv}} [read readview] [write writeview] [notify notifyview] [access access-list] 例： Device(config)# <code>snmp-server group public v2c access lmnop</code>	リモート デバイス上で新しい SNMP グループを設定します。 ※ <i>group-name</i> には、グループの名前を指定します。次のいずれかのセキュリティモデルを指定します。 <ul style="list-style-type: none"> • v1 は、最も安全性の低いセキュリティモデルです。 • v2c は、2 番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。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • 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のみを表示できるビュー名を表す文字列 (64 文字以内) を入力します。</p> <p>(任意) write writeview 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名を表す文字列 (64 文字以内) を入力します。</p> <p>(任意) notify notifyview とともに、通知、インフォーム、またはトラップを指定するビュー名を表す文字列 (64 文字以内) を入力します。</p> <p>(任意) access access-list とともに、アクセスリスト名の文字列 (64 文字以内) を入力します。</p>
ステップ 5	<pre>snmp-server user username group-name {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]</pre> <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>The <i>username</i> は、エージェントに接続する、ホスト上のユーザーの名前です。</p> <p><i>group-name</i> は、ユーザーが対応付けられるグループの名前です。</p> <p>Enter remote を入力して、ユーザー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 を押します)。永続タイマーとして v3 を入力した場合は、次の追加オプションがあります。</p> <ul style="list-style-type: none"> • encrypted は、パスワードを暗号化形式で表示するように指定します。このキーワードは、v3 キーワードを指定した場合のみ使用できます。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • auth は認証レベル設定セッションであり、HMAC-MD5-96 (md5) または HMAC-SHA-96 (sha) 認証レベルを使用できます。 <i>auth-password</i> パスワード文字列 が必要です。(64 文字以下)。 <p>永続タイマーとして 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文字列 <i>priv-password</i> を設定することもできます。</p> <ul style="list-style-type: none"> • priv は、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。 • 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文字列 (64 文字以内) 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

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、トラップまたはインフォームのどちらとしてSNMP通知を送信するかを指定します。



(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。

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. `configure terminal`
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： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	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 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. **configure terminal**
3. **snmp-server tftp-server-list 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 モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	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 {deny permit} source [source-wildcard] 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、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 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) を無効にして、SNMP プロセスをシャットダウンします。グローバル コンフィギュレーション モードで、**snmp-server host**、または **snmp-server user**、または **snmp-server community**、または **snmp-server manager** のいずれかのコマンドを入力して、SNMP エージェントのすべてのバージョンを再度有効にします。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。SNMP エージェントは、デバイスに入力された最初の **snmp-server** グローバル コンフィギュレーション コマンドによって有効になります。

手順の概要

1. **enable**
2. **configure terminal**
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 モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	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	no snmp-server 例： Device(config)# no snmp-server	SNMP エージェント動作をディセーブルにします。
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。

SNMP の例

次に、SNMP の全バージョンをイネーブルにする例を示します。この設定では、任意の SNMP マネージャがコミュニティストリング *public* を使用して、読み取り専用権限ですべてのオブジェクトにアクセスできます。この設定では、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 のメンバーに、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 認証失敗トラップは、SNMPv2C
がコミュニティストリング *cisco.com* を使用してホスト *cisco.com* に送信します。 *public* をクリッ
クします。

```
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 行目で、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、**snmp-server** ホスト *cisco.com* に対する以前の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
```

次の例では、すべてのトラップをホスト *myhost.cisco.com* *myhost.cisco.com* に送信するよう
にコミュニティストリング *public* を使用して、デバイスをイネーブルにする方法を示します。

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

次の例では、ユーザーがグローバル コンフィギュレーション モードを開始したときに、ユー
ザーをリモートホストに関連付け、**auth** (*authNoPriv*) 認証レベルインフォームを送信する方
法を示しています。

```
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
```

次に、SNMP エージェントにポーリングされた SNMP マネージャのエントリを表示する例を示
します。

```
Device# show snmp stats host
```

Request Count	Last Timestamp	Address
2	00:00:01 ago	3.3.3.3
1	1w2d ago	2.2.2.2

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 3: 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 エンジンおよびモートエンジンに関する情報を表示します。
show snmp group	ネットワーク上の各 SNMP グループに関する情報を表示します。
show snmp pending	保留中の SNMP 要求の情報を表示します。
show snmp sessions	現在の SNMP セッションの情報を表示します。
show snmp user	SNMP ユーザ テーブルの各 SNMP ユーザ名に関する情報を表示します。 (注) このコマンドは、 auth noauth priv モードの SNMP 情報を表示する際に使用する必要があります。この情報は running-config 出力には表示されません。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。