SNMP の設定

この章では、モバイル ノードに 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） この章で使用される全構文とその使用方法については、このリリースの『*Cisco IOS Command Reference*』または『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

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 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）に組み込むことができます。エージェントおよび Management Information Base（MIB; 管理情報ベース）は、ネットワーク デバイスに置かれます。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することができます。エージェントは、デバイスのパラメータやネットワーク データの保管場所である 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取得要求または設定要求に応答することもできます。

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 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：RFC 1157 に定められた SNMP（完全なインターネット規格）。
- SNMPv2C には次の機能があります。

  - SNMPv2：RFC 1902 ～ 1907 で規定（ドラフト インターネット規格）。
  - SNMPv2C：RFC 1901 で規定（試用段階のインターネット プロトコル）。
- SNMPv3：RFC 2273 ～ 2275 で規定。SNMPv3 はネットワーク経由でパケットの認証と暗号化を併用して、デバイスへの安全なアクセスを実現します。

SNMPv1 と SNMPv2C は、両方ともコミュニティベースのセキュリティ形式を使用します。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 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、SNMPv2Classic のバルク検索機能と改良エラー処理を維持しながら改善したうえで、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、SNMPv2C のコミュニティ ベースの管理フレームワークに置き換えたものです。

SNMPv2C にはバルク検索メカニズムが組み込まれ、より詳細なエラー メッセージを管理ステーションに報告します。バルク検索メカニズムは、テーブルや大量の情報を検索し、必要な往復回数を最小限に抑えます。SNMPv2C の改良エラー処理には、さまざまなエラー状態を区別するため拡張エラー 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。現在では、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 レベルの両方を備えています。セキュリティ モデルは、ユーザと、ユーザが属するグループに対して作られた認証方針です。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 レベルの組み合わせによって、SNMP パケットの処理時に採用されるセキュリティ メカニズムが決まります。

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 プロトコルを使用する管理ステーションや、SNMPv2 プロトコルを使用する管理ステーションと通信できるように、ソフトウェアを設定することができます。

SNMP マネージャ機能

SNMP マネージャは、MIB 情報を使用して、表 17-1 に示す動作を実行します。

表 17-1　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、小さなデータ ブロックを数多く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。
トラップ	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** コマンドは、SNMPv2 でしか動作しません。

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。トラップ状態の例には、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 トポロジーが変更された場合、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 がブリッジにアクセスするには、NMS のコミュニティ ストリング定義が、ブリッジ上の 3 つのコミュニティ ストリング定義の少なくとも 1 つと一致してい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 3 つのいずれかです。

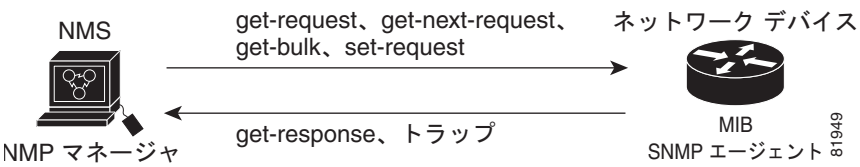
- read-only：許可された管理ステーションに、コミュニティ ストリングを除く MIB 内のすべてのオブジェクトへの読み取りアクセスを許可しますが、書き込みアクセスは許可しません。
- read-write：許可された管理ステーションに、MIB 内のすべてのオブジェクトへの読み書きアクセスを許可しますが、コミュニティ ストリングに対するアクセスは許可しません。

SNMP を使用して MIB 変数にアクセスする方法

NMS の例として、CiscoWorks ネットワーク管理ソフトウェアがあります。CiscoWorks 2000 ソフトウェアは、ブリッジの MIB 変数を使用してデバイス変数を設定し、ネットワーク上のデバイスをポーリングして特定の情報を取得します。ポーリング結果は、グラフ形式で表示されます。この結果を分析して、インターネットワーク関連の問題のトラブルシューティング、ネットワーク パフォーマンスの改善、デバイス設定の確認、トラフィック負荷のモニタなどを行うことができます。

図 17-1 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（特定イベントの通知）を送信することができ、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 アドレス追跡などのネットワークの状態を SNMP マネージャに通知するメッセージです。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 17-1　　SNMP ネットワーク



サポート対象の MIB の詳細、およびアクセス手順については、第 16 章「MIB のサポート」を参照してください。

SNMP の設定

ここでは、ブリッジで SNMP を設定する手順について説明します。

SNMP のデフォルト設定

表 17-2 に SNMP のデフォルト設定を示します。

表 17-2　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
SNMP コミュニティ ストリング	設定なし
SNMP トラップ レシーバー	設定なし
SNMP トラップ	イネーブルでない

SNMP エージェントのイネーブル化

SNMP をイネーブルにする特定の IOS コマンドは存在しません。SNMPv1 および SNMPv2 は、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 ストリングはパスワードと同様に機能して、ブリッジ上のエージェントへのアクセスを許可します。

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。

- SNMP マネージャの IP アドレスのアクセス リスト。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することが許可された SNMP マネージャが対象です。
- MIB ビュー。特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します。
- コミュニティにアクセスできる 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。

（注） 現在の IOS MIB エージェント実装では、デフォルトのコミュニティ ストリングは、インターネット MIB オブジェクト サブツリーに対するものです。IEEE802dot11 は MIB オブジェクト ツリーの別のブランチのもとにあるので、IEEE802dot11 MIB 上の別のコミュニティ ストリングと表示、あるいは、MIB オブジェクト ツリー内の ISO オブジェクト上の共通の表示とコミュニティ ストリングのいずれかを有効にする必要があります。ISO は、IEEE（IEEE802dot11）およびインターネットの共通の親ノードです。この MIB エージェントの動作は、IOS ソフトウェアを実行していないアクセス ポイントでの MIB エージェントの動作とは異なります。

特権 EXEC モードから、次の手順に従ってブリッジにコミュニティ ストリングを設定します。

	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* [*access-list-number*] [**view** *mib-view*] [**ro** | **rw**]	コミュニティ ストリングを設定します。 • *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）*access-list-number* 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。 • （任意）**view** *mib-view* には、コミュニティがアクセスできる MIB ビューを指定します（**ieee802dot11** など）。**snmp-server view** コマンドを使用して、IEEE ビューで標準 IEEE 802.11 MIB オブジェクトにアクセスする方法については、「snmp-server view コマンドの使用」（P.17-8）を参照してください。 • （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。 **（注）** IEEE802dot11 MIB にアクセスするには、IEEE802dot11 MIB 上の別のコミュニティ ストリングと表示、あるいは、MIB オブジェクト ツリー内の ISO オブジェクト上の共通の表示とコミュニティ ストリングのいずれかを有効にする必要があります。
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。 • *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することが許可された 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 を入れます。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。
ステップ 4	**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 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 ストリングをヌル文字列に設定します（コミュニティ ストリングに値を入力しないで）。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 *open* および *ieee* を SNMP に割り当てて両方に読み書きアクセスを許可し、*open* が IEEE802dot11-MIB 以外のオブジェクトのクエリに対するコミュニティ ストリングで、*ieee* が IEEE802dot11-MIB オブジェクトのクエリに対するコミュニティ ストリングであることを指定する例を示します。

```
bridge(config)# snmp-server view dot11view ieee802dot11 included
bridge(config)# snmp-server community open rw
bridge(config)# snmp-server community ieee view ieee802dot11 rw
```

トラップ マネージャの設定とトラップのイネーブル化

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、トラップは発行されません。

デバイスはトラップ マネージャを無制限に設定できます。任意の長さのコミュニティ ストリングを設定できます。

表 17-3 に、サポートされるブリッジのトラップ（通知タイプ）を説明します。これらのトラップの一部または全部をイネーブルにして、これを受信するようにトラップ マネージャを設定することができます。

表 17-3　通知タイプ

通知タイプ	説明
authenticate-fail	認証の失敗に使用するトラップをイネーブルにします。
config	SNMP 設定の変更に使用するトラップをイネーブルにします。
deauthenticate	クライアント デバイスの認証取り消しに使用するトラップをイネーブルにします。
disassociate	クライアント デバイスの結合解除に使用するトラップをイネーブルにします。
dot11-qos	QoS 変更に使用するトラップをイネーブルにします。
entity	SNMP エンティティの変更に使用するトラップをイネーブルにします。
envmon temperature	無線デバイスの温度を監視するトラップをイネーブルにします。このトラップは、ブリッジ無線デバイスの温度が動作時温度（55℃～-33℃、131 ºF～-27.4 ºF）の上限または下限に達すると送信されます。
linkDown	インターフェイスは DHCP で取得した IP アドレスを保持します。有効な linkDown トラップを受信すると、リンクダウン ホールドダウン タイマーが新しく起動されます。
linkUp	linkUp トラップ イベントが発生すると、DHCP クライアントは現在の IP アドレスを延長するか、またはできるだけ速やかに新しい IP アドレスを取得する必要があります。
snmp	SNMP イベントに使用するトラップをイネーブルにします。
syslog	Syslog トラップをイネーブルにします。
wlan-wep	WEP トラップをイネーブルにします。

snmp-server enable グローバル コンフィギュレーション コマンドでは、**tty** や **udp-port** など、一部の通知タイプを制御できません。これらの通知タイプは常にイネーブルに設定されます。表 17-3 に示す通知タイプを受け取るように、特定のホストに **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ことができます。

特権 EXEC モードから、ホストにトラップを送信するようにブリッジを設定する手順は次のとおりです。

	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 host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} *community-string notification-type*	トラップ メッセージの受信者を指定します。 • *host-addr* には、ホスト（ターゲットの受信者）の名前またはアドレスを指定します。 • ホストに SNMP トラップを送信する場合は、**traps**（デフォルト）を指定します。ホストに SNMP の情報を送信する場合は、**informs** を指定します。 • サポートされる SNMP バージョンを指定します。デフォルトの version 1 は、informs に使用できません。 • *community-string* には、通知操作で送信する文字列を指定します。**snmp-server host** コマンドを使用してこの文字列を設定できますが、**snmp-server host** コマンドを使用する前に、**snmp-server community** コマンドを使用してこの文字列を定義することを推奨します。 • *notification-type* には、表 17-3（P.17-6）に列挙されたキーワードを使用します。
ステップ 3	**snmp-server enable traps** *notification-types*	ブリッジで特定のトラップの送信をイネーブルにします。トラップのリストについては、表 17-3（P.17-6）を参照してください。 複数のタイプのトラップをイネーブルにするには、各トラップのタイプに **snmp-server enable traps** コマンドを個別に発行する必要があります。
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。

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。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。

エージェントの連絡先および場所情報の設定

特権 EXEC モードから、SNMP エージェントのシステムの連絡先を設定する手順は次のとおりです。これらの情報にはコンフィギュレーション ファイルからアクセスできます。

	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*	システムの連絡先の文字列を設定します。 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*	システムの場所の文字列を設定します。 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-server view コマンドの使用

グローバル コンフィギュレーション モードで、IEEE ビューと dot11 読み書きコミュニティ ストリングから標準の IEEE 802.11 MIB オブジェクトにアクセスするには、**snmp-server view** コマンドを使用します。

次に IEEE ビューと dot11 読み書きコミュニティ ストリングをイネーブルにする手順を示します。

```
bridge(config)# snmp-server view ieee ieee802dot11 included
bridge(config)# snmp-server community dot11 view ieee RW
```

SNMP の例

次に、SNMPv1 と SNMPv2C をイネーブルにする手順を示します。この設定では SNMP マネージャがコミュニティ ストリング *public* を使用して読み出し専用が許可されたすべてのオブジェクトにアクセスするのを許可します。この設定により、ブリッジがトラップを送信することはありません。

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

次に、ストリング *open* および *ieee* を SNMP に割り当てて両方に読み書きアクセスを許可し、*open* が IEEE802dot11-MIB 以外のオブジェクトのクエリに対するコミュニティ ストリングで、*ieee* が IEEE802dot11-MIB オブジェクトのクエリに対するコミュニティ ストリングであることを指定する例を示します。

```
bridge(config)# snmp-server view dot11view ieee802dot11 included
bridge(config)# snmp-server community open rw
bridge(config)# snmp-server community ieee view ieee802dot11 rw
```

次に、任意の SNMP マネージャがコミュニティ ストリング *public* を使用して読み出し専用が許可されたすべてのオブジェクトにアクセスするのを許可する手順を示します。ブリッジは、ホスト 192.180.1.111 および 192.180.1.33（SNMPv1 を使用）や、ホスト 192.180.1.27（SNMPv2C を使用）へ設定トラップを送信します。トラップと一緒にコミュニティ ストリング *public* が送信されます。

```
bridge(config)# snmp-server community public
bridge(config)# snmp-server enable traps config
bridge(config)# snmp-server host 192.180.1.27 version 2c public
bridge(config)# snmp-server host 192.180.1.111 version 1 public
bridge(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出し専用アクセスを許可する手順を示します。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。SNMPv2C はコミュニティ ストリング *public* を使用してホスト *cisco.com* に SNMP Authentication Failure トラップを送信します。

```
bridge(config)# snmp-server community comaccess ro 4
bridge(config)# snmp-server enable traps snmp authentication
bridge(config)# snmp-server host cisco.com version 2c public
```

次に、ホスト *cisco.com* に Entity MIB トラップを送信する手順を示します。コミュニティ ストリングは制限されます。最初の行でそれまでイネーブルにされたすべてのトラップに加えて、ブリッジからの Entity MIB トラップの送信がイネーブルになります。2 行目でこれらのトラップの宛先が指定され、ホスト *cisco.com* に対する以前の **snmp-server host** コマンドがすべて上書きされます。

```
bridge(config)# snmp-server enable traps entity
bridge(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、ブリッジでホスト *myhost.cisco.com* にすべてのトラップを送信するのをイネーブルにする手順を示します。

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

SNMP ステータスの表示

不正なコミュニティ ストリングのエントリ数、エラー数、要求された変数の数など、SNMP の入力および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。この表示のフィールドについての詳細は、『*Cisco IOS Configuration Fundamentals Command Reference for Release* 12.2』を参照してください。

次に、**show snmp** コマンドの出力例を示します。

```
Router# show snmp

Chassis: 01506199
37 SNMP packets input
    0 Bad SNMP version errors
    4 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    24 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    28 Get-next PDUs
    0 Set-request PDUs
78 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
```

```
    0 General errors
    24 Response PDUs
    13 Trap PDUs

SNMP logging: enabled

    Logging to 171.69.58.33.162, 0/10, 13 sent, 0 dropped.

SNMP Manager-role output packets
    4 Get-request PDUs
    4 Get-next PDUs
    6 Get-bulk PDUs
    4 Set-request PDUs
    23 Inform-request PDUs
    30 Timeouts
    0 Drops
SNMP Manager-role input packets
    0 Inform response PDUs
    2 Trap PDUs
    7 Response PDUs
    1 Responses with errors

SNMP informs: enabled
Informs in flight 0/25 (current/max)
Logging to 171.69.217.141.162
4 sent, 0 in-flight, 1 retries, 0 failed, 0 dropped
Logging to 171.69.58.33.162
0 sent, 0 in-flight, 0 retries, 0 failed, 0 dropped
```