



SNMP の設定

この章では、アクセス ポイントで 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)

この章で使用されるコマンドの構文と使用方法の詳細は、このリリースの『Cisco Aironet アクセス ポイント / ブリッジ Cisco IOS コマンド リファレンス』⁶ および『Cisco IOS Configuration Fundamentals Command Reference for Release 12.3』⁷ を参照してください。

この章の内容は、次のとおりです。

- [SNMP の概要 \(P. 18-2\)](#)
- [SNMP の設定 \(P. 18-5\)](#)
- [SNMP ステータスの表示 \(P. 18-12\)](#)

SNMP の概要

SNMP は、SNMP のマネージャとエージェント間の通信のメッセージ形式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) に組み込まれています。エージェントと Management Information Base (MIB; 管理情報ベース) は、アクセス ポイント上に置かれます。アクセス ポイント上で SNMP を設定する場合、マネージャとエージェント間の関連性を定義します。

SNMP エージェントには、SNMP マネージャが値を要求または変更できる MIB 変数が格納されます。マネージャはエージェントから値を取得し、またエージェントに値を保存します。エージェントは、デバイス パラメータとネットワーク データの情報のリポジトリである 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。

エージェントは要請されていないトラップをマネージャに送信できます。トラップは SNMP マネージャにネットワークの状況を警告するメッセージです。トラップは不適切なユーザ認証、再起動、リンク ステータス (起動または停止)、MAC アドレスの追跡、TCP 接続の終了、近接との接続の損失、またはその他の重要なイベントを表す場合があります。

この項では、次の概念を説明します。

- [SNMP のバージョン \(P. 18-2\)](#)
- [SNMP マネージャの機能 \(P. 18-3\)](#)
- [SNMP エージェントの機能 \(P. 18-3\)](#)
- [SNMP コミュニティ スtring \(P. 18-4\)](#)
- [SNMP による MIB 変数へのアクセス \(P. 18-4\)](#)

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ます。

- SNMPv1 : Simple Network Management Protocol。RFC 1157 で定義される完全なインターネット規格。
- SNMPv2C には、次の種類があります。
 - SNMPv2 : Simple Network Management Protocol のバージョン 2。RFC 1902 ~ 1907 で定義されるドラフト インターネット規格。
 - SNMPv2C : SNMPv2 のコミュニティ ベースの管理フレームワーク。RFC 1901 で定義される試用段階のインターネット プロトコル。
- SNMPv3 には、次の種類があります。
 - SHA および Message Digest (MD) 5 認証プロトコルとデータ暗号規格 56 暗号化。
 - 3 つのセキュリティ レベル。認証なしプライバシーなし (NoAuthNoPriv)、認証ありプライバシーなし (AuthNoPriv) および認証ありプライバシーあり (AuthPriv)。

SNMPv3 は、SNMP 通信に利用できる最高レベルのセキュリティをサポートしています。SNMPv1 と SNMPv2 のコミュニティ スtring は、暗号化なしのプレーン テキストとして格納、転送されます。SNMPv3 セキュリティ モデルでは、SNMP ユーザはユーザ グループの認証と結合を行います。システム データへのアクセスは、グループに基づいて制限されます。

SNMP エージェントは、管理ステーションでサポートされる SNMP のバージョンを使用するように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対話できるため、SNMPv3 プロトコルを使用する管理ステーションや、SNMP v2 または SNMPv1 プロトコルを使用する管理ステーションとの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。

表 18-1 は、アクセス ポイントでサポートされる SNMP のバージョンとセキュリティ レベルを示しています。

表 18-1 SNMP のバージョンとセキュリティ レベル

SNMP のバージョン	セキュリティ レベル	認証	暗号化
v1	NoAuthNoPriv	コミュニティ スtring の一致	なし
v2C	NoAuthNoPriv	コミュニティ スtring の一致	なし
v3	NoAuthNoPriv	ユーザ名の一致	なし
v3	AuthNoPriv	HMAC-MD5 または HMAC-SHA アルゴリズム	なし
v3	AuthPriv	HMAC-MD5 または HMAC-SHA アルゴリズム	データ暗号規格 56 ビット暗号化

SNMPv3 の詳細は、次のリンクをクリックして、Cisco IOS リリース 12.0(3)T の「New Feature Documentation」を参照してください。

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t3/snmp3.htm>

SNMP マネージャの機能

SNMP マネージャは MIB 内の情報を使用して、表 18-2 に表示されている操作を実行します。

表 18-2 SNMP の操作

操作	説明
get-request	特定の変数から値を取得します。
get-next-request	テーブル内の特定の変数から値を 1 つ取得します。 ¹
get-bulk-request ²	テーブル内の複数行など、小さなデータ ブロックを数多く送信するような場合に、大きなブロックでデータを取得します。
get-response	NMS が送信した get-request、get-next-request、set-request 要求に返答します。
set-request	特定の変数に値を保存します。
trap	あるイベントが発生したときに、SNMP エージェントが SNMP マネージャに送信する非要求メッセージ。

- この操作により、SNMP マネージャは正確な変数名を知る必要がなくなります。テーブルから必要な変数を見つけるために、逐次検索が実行されます。
- get-bulk コマンドは、SNMPv2 でのみ機能します。

SNMP エージェントの機能

SNMP エージェントは、SNMP マネージャからの要求に次のように応答します。

- MIB 変数の取得：SNMP エージェントは、NMS からの要求に応じ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、NMS にその値を返します。
- 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じ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 が要求した値に変更します。

また、SNMP エージェントは非要請トラップ メッセージを送信して、エージェントで重要なイベントが発生したことを NMS に伝えます。トラップの状況の例として、ポートまたはモジュールの起動または停止、スパンニングツリー トポロジの変更、認証の失敗などが含まれます。

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 がアクセス ポイントにアクセスするためには、NMS のコミュニティ スtringの定義が少なくともアクセス ポイントの 3 つのコミュニティ スtring定義のうち、1 つと一致している必要があります。

コミュニティ スtringに次の属性のいずれかを指定できます。

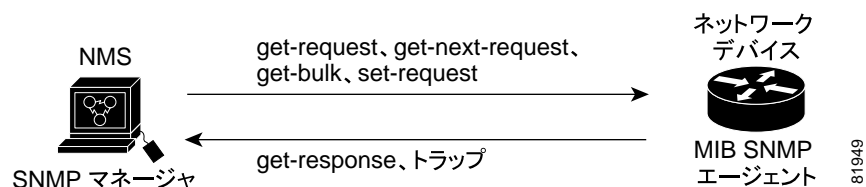
- 読み取り専用：許可された管理ステーションへの読み取りアクセスを、コミュニティ スtringを除く MIB のすべてのオブジェクトに許可しますが、書き込みアクセスは許可しません。
- 読み取り / 書き込み：許可された管理ステーションへの読み取りおよび書き込みアクセスを、MIB のすべてのオブジェクトに許可しますが、コミュニティ スtringには許可しません。

SNMP による MIB 変数へのアクセス

NMS の例として CiscoWorks ネットワーク管理ソフトウェアがあります。CiscoWorks 2000 ソフトウェアは、アクセス ポイントの 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で特定の情報をポーリングします。ポーリングの結果をグラフで表示して、分析し、インターネットワーキング問題のトラブルシューティング、ネットワークのパフォーマンス向上、デバイスの設定の確認、トラフィック負荷の監視などに使用できます。

図 18-1 に示すように、SNMP エージェントは MIB からデータを収集します。エージェントは SNMP マネージャにトラップ（特定のイベントの通知）を送信でき、SNMP マネージャはトラップを受信して処理します。トラップは、不適切なユーザ認証、再起動、リンク ステータス（起動または停止）、MAC アドレスの追跡などの、ネットワーク上の状況を SNMP マネージャに警告するメッセージです。また、SNMP エージェントは、SNMP マネージャが *get-request*、*get-next-request*、および *set-request* の形式で送信する、MIB 関連のクエリーに応答します。

図 18-1 SNMP ネットワーク



サポートされる MIB とそのアクセス方法については、付録 B「サポートされている MIB」を参照してください。

SNMP の設定

この項では、アクセス ポイントで SNMP を設定する方法について説明します。内容は次のとおりです。

- デフォルトの SNMP 設定 (P. 18-5)
- SNMP エージェントの有効化 (P. 18-5)
- コミュニティ スtring の設定 (P. 18-5)
- SNMP サーバグループ名の指定 (P. 18-7)
- SNMP サーバホストの設定 (P. 18-8)
- SNMP サーバユーザの設定 (P. 18-8)
- トラップ マネージャの設定とトラップの有効化 (P. 18-8)
- エージェントの連絡先と場所の情報の設定 (P. 18-10)
- `snmp-server view` コマンドの使用 (P. 18-10)
- SNMP の例 (P. 18-10)

デフォルトの SNMP 設定

表 18-3 は、デフォルトの SNMP 設定を示しています。

表 18-3 デフォルトの SNMP 設定

機能	デフォルト設定
SNMP エージェント	無効
SNMP コミュニティ スtring	どの文字列もデフォルトでは設定されていません。しかし、Web ブラウザ インターフェイスを使って SNMP を有効にする場合、アクセス ポイントは自動的に、IEEE802dot11 MIB 読み取り専用アクセスで、 <i>public</i> コミュニティを生成します。
SNMP トラップ レシーバー	設定されていません。
SNMP トラップ	有効なトラップなし。

SNMP エージェントの有効化

SNMP を有効にするための特定の CLI コマンドはありません。最初に入力したグローバル設定コマンド `snmp-server` を使用すると、サポートされているバージョンの SNMP が有効になります。

また、Web ブラウザ インターフェイスの SNMP Properties ページで SNMP を有効にすることもできます。Web ブラウザ インターフェイスで SNMP を有効にする場合、アクセス ポイントは自動的に、IEEE802dot11 MIB 読み取り専用アクセスで、*public* と呼ばれるコミュニティ スtring を生成します。

コミュニティ スtring の設定

SNMP コミュニティ スtring を使用して、SNMP マネージャとエージェント間の関連性を定義します。コミュニティ スtring はパスワードと同様に機能し、アクセス ポイント上のエージェントへのアクセスを許可します。

オプションで、スStringに関連した次の特性の 1 つまたは複数指定できます。

- 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String 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取り / 書き込み権限、または読み取り専用の権限。



(注) 現在の Cisco 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ビュー、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ビュー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、Cisco 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。

イネーブル EXEC モードから、次の手順に従ってアクセスポイント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	<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 2	<code>snmp-server community string</code> [<i>access-list-number</i>][<code>view mib-view</code>] [<code>ro</code> <code>rw</code>]	<p>コミュニティストリングを設定します。</p> <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文字列を指定します。任意の長さの 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。 • (オプション) <i>access-list-number</i> には、1 ~ 99 および 1300 ~ 1999 の標準的な IP アクセスリスト番号を入力します。 • (オプション) <code>view mib-view</code> には、<code>ieee802dot11</code> など、このコミュニティがアクセスできる MIB ビューを指定します。IEEE ビューを使用して標準 IEEE 802.11 MIB オブジェクトにアクセスするコマンド <code>snmp-server view</code> の使用方法については、「snmp-server view コマンドの使用」の項 (P. 18-10) を参照してください。 • (オプション) 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 (<code>ro</code>) を指定し、許可された管理ステーションを使用して MIB オブジェクトを取得し、修正する場合は、読み取り / 書き込み (<code>rw</code>) 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。 <p>(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ビュー、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ビューとコミュニティストリングを有効にする必要があります。</p>

	コマンド	目的
ステップ 3	<code>access-list access-list-number</code> {deny permit} source [source-wildcard]	(オプション) ステップ 2 で IP の標準アクセス リストの番号を指定している場合は、このコマンドを必要な回数だけ繰り返してリストを作成します。 <ul style="list-style-type: none"> <code>access-list-number</code> 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。 <code>deny</code> キーワードは、条件に一致する場合にアクセスを拒否します。<code>permit</code> キーワードは、条件に一致する場合にアクセスを許可します。 <code>source</code> には、コミュニティ スtring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。 (オプション) <code>source-wildcard</code> には、ソース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ワイルドカードを指定します。 アクセス リストは常に、すべてを暗黙的に否定するステートメントで終了することに注意してください。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	入力内容を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

SNMP コミュニティのアクセスを無効にするには、そのコミュニティのコミュニティ スtringをヌル文字列に設定します (コミュニティ スtringに値を入力しない)。特定のコミュニティ スtringを削除する場合は、グローバル設定コマンド `no snmp-server community string` を使用します。

次の例は、コミュニティ スtring `open` と `ieee` を SNMP に割り当てる方法、両方に対する読み取り / 書き込みアクセスを許可する方法、`open` が非 IEEE802dot11-MIB オブジェクトのクエリーに対するコミュニティ スtringであり、`ieee` が IEEE802dot11 MIB オブジェクトのクエリーに対するコミュニティ スtringであることを指定する方法を示します。

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

SNMP サーバ グループ名の指定

新しい SNMP グループ、または SNMP ユーザを SNMP ビューにマップするテーブルを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
<code>snmp-server group [groupname {v1 v2c v3 [auth noauth priv]] [read readview] [write writeview] [notify notifyview] [access access-list]</code>	新しい SNMP グループ、または SNMP ユーザを SNMP ビューにマップするテーブルを設定します。

SNMP サーバホストの設定

SNMP トラップ操作の受信者を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
<code>snmp-server host host [traps informs][version {1 2c 3 [auth noauth priv]}] community-string [udp-port port] [notification-type]</code>	SNMP トラップ操作の受信者を設定します。

SNMP サーバユーザの設定

SNMP グループに新しいユーザを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
<code>snmp-server user username [groupname remote ip-address [udp-port port] {v1 v2c v3 [encrypted] [auth {md5 sha} auth-password [priv des56 priv password]] [access access-list]</code>	SNMP グループに新しいユーザを設定します。

トラップ マネージャの設定とトラップの有効化

トラップ マネージャは、トラップを受信し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アクセス ポイント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ておらず、トラップは発行されません。

この Cisco IOS リリースを実行するアクセス ポイントには、トラップ マネージャを無制限に設定できます。コミュニティ スtring の長さは任意です。

表 18-4 は、サポートされるアクセス ポイントのトラップ（通知タイプ）を示しています。これらのトラップの一部またはすべてを有効にして、そのトラップを受信するようにトラップ マネージャを設定できます。

表 18-4 通知タイプ

通知タイプ	説明
authenticate-fail	認証の失敗のトラップを有効にします。
config	SNMP 設定変更のトラップを有効にします。
deauthenticate	クライアント デバイスの認証取り消しのトラップを有効にします。
disassociate	クライアント デバイスのアソシエーション解除のトラップを有効にします。
dot11-qos	QoS 変更のトラップを有効にします。
entity	SNMP のエンティティ変更のトラップを有効にします。
rogue-ap	不正なアクセス ポイントの検出のトラップを有効にします。
snmp	SNMP イベントのトラップを有効にします。
switch-over	切り替えのトラップを有効にします。
syslog	syslog トラップを有効にします。
wlan-wep	WEP トラップを有効にします。

tty や udp-port などの一部の通知タイプは、グローバル設定コマンド `snmp-server enable` で制御できません。これらの通知タイプは、常に有効です。表 18-4 に記載された通知タイプを受信する場合は、特定のホストにグローバル設定コマンド `snmp-server host` を使用できます。

特権 EXEC モードから、次の手順に従ってホストにトラップを送信するようにアクセス ポイントを設定します。

	コマンド	目的
ステップ 1	<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 2	<code>snmp-server host host-addr {traps informs} {version {1 2c 3 {auth noauth priv}}} community-string [udp-port port] notification-type</code>	<p>トラップ メッセージの受信者を指定します。</p> <ul style="list-style-type: none"> <code>host-addr</code> には、(ターゲットの受信者)ホスト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、<code>traps</code> (デフォルト) を指定します。ホストに SNMP 情報を送信する場合は、<code>informs</code> を指定します。 サポートする SNMP バージョンを指定します。informs を指定した場合は、デフォルトのバージョン 1 は使用できません。バージョン 3 には、次の 3 つのセキュリティ レベルがあります。 <ul style="list-style-type: none"> <code>auth</code> : 暗号化なしのパケットの認証を指定します。 <code>noauth</code> : パケットの認証と暗号化をしないように指定します。 <code>priv</code> : パケットの認証と暗号化を指定します。 <code>community-string</code> には、通知操作で送信する文字列を指定します。この文字列は <code>snmp-server host</code> コマンドを使用して設定できませんが、<code>snmp-server host</code> コマンドを使用する前に、<code>snmp-server community</code> コマンドを使用してこの文字列を定義することをお勧めします。 <code>notification-type</code> には、表 18-4 (P.18-8) に記載されたキーワードを使用します。
ステップ 3	<code>snmp-server enable traps notification-types</code>	<p>アクセス ポイントで特定のトラップの送信を有効にします。トラップのリストについては、表 18-4 (P.18-8) を参照してください。</p> <p>複数のタイプのトラップを有効にする場合、各トラップタイプに <code>snmp-server enable traps</code> コマンドを個別に発行します。</p>
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	入力内容を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

特定のホストに対し、トラップの受信を無効にするには、グローバル設定コマンド `no snmp-server host host` を使用します。特定のトラップ タイプを無効にするには、グローバル設定コマンド `no snmp-server enable traps notification-types` を使用します。

エージェントの連絡先と場所の情報の設定

特権 EXEC モードから、次の手順に従って SNMP エージェントのシステムの連絡先と場所を設定し、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します。

	コマンド	目的
ステップ 1	<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 2	<code>snmp-server contact <i>text</i></code>	システムの連絡先文字列を設定します。 例： <code>snmp-server contact Dial System Operator at beeper 21555.</code>
ステップ 3	<code>snmp-server location <i>text</i></code>	システムの場所の文字列を設定します。 例： <code>snmp-server location Building 3/Room 222</code>
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	入力内容を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

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 `snmp-server view` コマンドを使用して、IEEE ビューおよび dot11 読み取り / 書き込みコミュニティ スtring を通じて、標準 IEEE 802.11 MIB オブジェクトにアクセスします。

次の例は、IEEE ビューと dot11 読み取り / 書き込みコミュニティ スtring を有効にする方法を示しています。

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

SNMP の例

次の例は、SNMPv1、SNMPv2C、および SNMPv3 を有効にする方法を示しています。この設定により、SNMP マネージャはコミュニティ スtring `public` を使用した読み取り専用権限ですべてのオブジェクトへのアクセスが許可されます。この設定でアクセス ポイントがトラップを送信することはありません。

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

次の例は、コミュニティ スtring `open` と `ieee` を SNMP に割り当てる方法、両方に対する読み取り / 書き込みアクセスを許可する方法、`open` が非 IEEE802dot11-MIB オブジェクトのクエリーに対するコミュニティ スtring であり、`ieee` が IEEE802dot11 MIB オブジェクトのクエリーに対するコミュニティ スtring であることを指定する方法を示します。

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

次の例は、コミュニティ ストリング *public* を使用した読み取り専用権限で、すべてのオブジェクトへのアクセスを SNMP マネージャに許可する方法を示します。また、アクセス ポイントは SNMPv1 を使用してホスト 192.180.1.111 と 192.180.1.33 に、SNMPv2C を使用してホスト 192.180.1.27 に設定トラップを送信します。コミュニティ ストリング *public* はトラップで送信されます。

```
AP(config)# snmp-server community public
AP(config)# snmp-server enable traps config
AP(config)# snmp-server host 192.180.1.27 version 2c public
AP(config)# snmp-server host 192.180.1.111 version 1 public
AP(config)# snmp-server host 192.180.1.33 public
```

次の例は、すべてのオブジェクトが *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方法を示しています。他の SNMP マネージャはオブジェクトにアクセスできません。SNMP 認証失敗トラップはコミュニティ ストリング *public* を使用して、SNMPv2C がホスト *cisco.com* に送信します。

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

次の例は、エンティティ MIB トラップをホスト *cisco.com* に送信する方法を示しています。コミュニティ ストリングは制限されます。最初の行で、アクセス ポイントはそれまでに有効になったトラップ以外にエンティティ MIB トラップを送信できます。2 行目はこれらのトラップの宛先を指定し、ホスト *cisco.com* に対してそれまでに発行されたすべての *snmp-server host* コマンドを無効にします。

```
AP(config)# snmp-server enable traps entity
AP(config)# snmp-server host cisco.com restricted entity
```

次の例は、アクセス ポイントがコミュニティ ストリング *public* を使用して、ホスト *myhost.cisco.com* にすべてのトラップを送信するのを有効にする方法を示します。

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

次の例は、これらの SNMPv3 設定の方法を示しています。

- ビュー名 (*iso*)
- IP アドレス *1.4.74.10* のリモート ホストに対して自身を識別するために、このエージェントが使用する SNMP エンジン ID (*1234567890*)
- プライバシー暗号をサポートする SNMPv3 グループ (*admin*) で、このグループのユーザは全員、(*iso*) ビューで定義されているすべてのオブジェクトに対する読み取りおよび書き込みアクセスが許可されています。
- *admin* グループに属する SNMP ユーザ (*joe*) で、クエリーに MD5 認証を使用し、MD5 用のパスワードに *xyz123* を使用し、データ暗号規格 56 データ クエリー暗号を使用し、暗号キーとして *key007* を使用します。
- *admin* グループに属する SNMP ユーザ (*fred*) で、クエリーに MD5 認証を使用し、MD5 用のパスワードに *abc789* を使用し、データ暗号規格 56 データ クエリー暗号を使用し、暗号キーとして *key99* を使用します。

```
AP(config)# snmp-server view iso iso included
AP(config)# snmp-server engineID remote 1.4.74.10 1234567890
AP(config)# snmp-server group admin v3 priv
AP(config)# snmp-server group admin v3 priv read iso write iso
AP(config)# snmp-server user joe admin v3 auth md5 xyz123 priv des56 key007
AP(config)# snmp-server user fred admin v3 encrypted auth md5 abc789 priv des56 key99
```



(注) この例で最後のコマンドを入力すると、`show running-config` コマンドと `show startup-config` コマンドでは、一部の SNMP 設定のみが表示されるようになります。

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、要求された変数など SNMP の入出力の統計を表示する場合は、`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は、『Cisco IOS Configuration Fundamentals Command Reference for Release 12.3』を参照してください。