SNMP の設定

この章では、アクセス ポイントで簡易ネットワーク管理プロトコル（SNMP）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については、このリリースの『*Cisco IOS Command Reference for Cisco Aironet Access Points*』を参照してください。

SNMP の概要

SNMP は、アプリケーション層プロトコルであり、SNMP マネージャと SNMP エージェントとの通信に使用されるメッセージ フォーマットを提供します。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。エージェントと管理情報ベース（MIB）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。

この項では、次の概念を説明します。

SNMP 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：RFC 1157 に規定された SNMP（完全インターネット標準）。
- SNMPv2C には、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：SNMPv2 のコミュニティ ベースの管理フレームワーク。RFC 1901 に規定された試用段階のインターネット プロトコル。
- SNMPv3 には、次の機能があります。
  - SHA および Message Digest 5（MD5; メッセージ ダイジェスト 5）認証プロトコルと DES56 暗号のサポート。
  - 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 通信に利用できる高度な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 ストリングは、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 グループの認証と参加を行います。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、SNMPv2 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ている 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 Version	セキュリティ レベル	認証	暗号化
v1	NoAuthNoPriv	コミュニティ ストリングの一致	なし
v2C	NoAuthNoPriv	コミュニティ ストリングの一致	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（DES）56 ビット暗号

SNMP マネージャ機能

SNMP マネージャは、MIB 情報を使用して、表 18-2 に示す動作を実行します。

表 18-2　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代わりに、大きなブロックでデータを取得します。
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** コマンドは、SNMPv2 に限り機能します。

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 ストリングの定義がアクセス ポイントの 3 つのコミュニティ ストリング定義のうち、少なくとも 1 つと一致している必要があります。

(注)　SNMP コミュニティは、SNMPv1 および SNMPv2c で使用されます。SNMPv3 はコミュニティを使用しません。

コミュニティ ストリングの属性は、次のいずれかです。

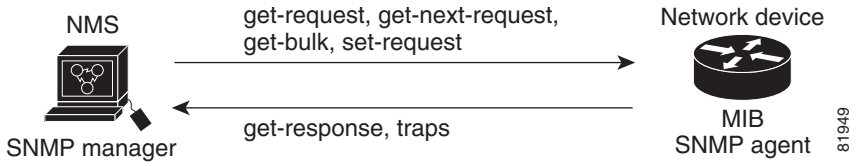
- 読み取り専用：許可された管理ステーションへの読み取りアクセスを、コミュニティ ストリングを除く MIB のすべてのオブジェクトに許可しますが、書き込みアクセスは許可しません。
- 読み取り/書き込み：許可された管理ステーションへの読み取りおよび書き込みアクセスを、MIB のすべてのオブジェクトに許可しますが、コミュニティ ストリングには許可しません。

SNMP を使用して MIB 変数にアクセスする方法

NMS の例として、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、アクセス ポイント 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。ポーリング結果を表示および解析して、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。

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。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 18-1　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、付録 B「サポート対象 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。

SNMP のデフォルト設定

表 18-3 に、SNMP のデフォルト設定を示します。

表 18-3　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	どのストリング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、*public* コミュニティを生成します。
SNMP トラップ レシーバ	未設定
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 コンフィギュレーション 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 ストリングを生成します。

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。

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

(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ため、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。

特権 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	**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、**ieee802dot11** 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 ビューを通じて標準 IEEE 802.11 MIB オブジェクトにアクセスする **snmp-server view** コマンドの使用方法については、「snmp-server view コマンドの使用」セクション（18-10 ページ）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**）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（**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。
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 4	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**show running-config**	入力内容を確認します。
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 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。

次の例は、コミュニティ ストリング *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* がすべてのオブジェクトのクエリに対するコミュニティ ストリングであることを指定する方法を示します。

```
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
snmp-server group [*groupname* {**v1** | **v2c** | **v3** [**auth** | **noauth** | **priv**]}][**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]	新しい SNMP グループの設定、または SNMP ユーザを SNMP ビューにマップするテーブルの設定を行います。

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
snmp-server host *host* [**traps** | **informs**][**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]	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
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*]	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 Release 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 ストリングの長さは任意です。

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全部を有効にして、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 18-4　通知タイプ

通知タイプ	説明
aaa_server	AAA イベントのトラップを有効にします。
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。
cef	cef トラップを許可します
config-copy	SNMP config-copy トラップを許可します
config-ctid	SNMP config-ctid トラップを許可します
cpu	CPU に関連したトラップを許可します
dot11-mibs	dot11 トラップを許可します
entity	SNMP entity トラップを許可します
l2tun-pseudowire-status	SNMP L2 pseudowire status トラップを許可します
l2tun-session	SNMP L2 session トラップを許可します
syslog	SNMP syslog トラップを許可します
tty	TCP connection トラップを許可します
udp-port	通知ホストの UDP ポート番号です
vrfmib	SNMP vrfmib トラップを許可します

udp-port などの一部の通知タイプは、グローバル コンフィギュレーション 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。

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	**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** {**auth** | **noauth** | **priv**}}} *community-string* [**udp-port** *port*] *notification-type*	トラップ メッセージの受信側を指定します。 • *host-addr* 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。 • 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。SNMP 情報をホストに送信するには、**informs** 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 にはバージョン 1 (デフォルト) を使用できません。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。 – **auth**：暗号化なしのパケットの認証を指定します。 – **noauth**：パケットの認証と暗号化をしないように指定します。 – **priv**：パケットの認証と暗号化を指定します。 • *community-string* には、通知動作時に送信するストリングを指定します。この文字列は **snmp-server host** コマンドを使用して設定できますが、**snmp-server community** コマンドでこの文字列を定義してから、**snmp-server host** コマンドを使用することを推奨します。 • *notification-type* には、表 18-4 (18-8 ページ) 内のキーワードを使用します。
ステップ 3	**snmp-server enable traps** *notification-types*	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。トラップのリストは、表 18-4 (18-8 ページ) を参照してください。 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 **snmp-server enable traps** コマンドを個別に発行します。
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**	入力内容を確認します。
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。

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。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 コンタクトおよびロケーション情報の設定

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、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*	システムに関する問い合わせ先を表す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*	システムのロケーションを表す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**	入力内容を確認します。
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 **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 ストリングを通じて、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 ストリング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 での例

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 ストリング *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に対するコミュニティ ストリングであり、*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。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、トラップとともに送信されます。

```
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。

```
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。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* に対する以前の **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こと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、クエリに MD5 認証を使用し、MD5 用のパスワードに *xyz123* を使用し、DES56 データ クエリ暗号を使用し、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、クエリに MD5 認証を使用し、MD5 用の暗号化されたパスワードに *abc789* を使用し、DES56 データ クエリ暗号を使用し、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 設定だけ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 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。この表示のフィールドについては、『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。