



# 簡易ネットワーク管理プロトコル (SNMP) の設定

この章では、アクセス ポイントに 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コマンドの構文と使用方法の詳細は、このリリースの『Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges』、およびリリース 12.3 の『Cisco IOS Configuration Fundamentals Command Reference』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 \(P. 17-2\)](#)
- [SNMP の設定 \(P. 17-5\)](#)
- [SNMP の設定 \(P. 17-5\)](#)

## 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 NMS (network management system; 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 MIB (management information base; 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。

エージェントは割り込み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や、再起動、リンク ステータス (起動または停止)、media access control (MAC; メディア アクセス制御) アドレスの追跡、Transmission Control Protocol (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 バージョン \(P. 17-2\)](#)
- [SNMP マネージャの機能 \(P. 17-3\)](#)
- [SNMP エージェントの機能 \(P. 17-4\)](#)
- [SNMP コミュニティ ストリング \(P. 17-4\)](#)
- [SNMP による MIB 変数へのアクセス \(P. 17-4\)](#)

## 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 : 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。SNMPv2C には、次の機能があります。
  - 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。SNMPv3 には、次の機能があります。
  - Secure Hash Algorithm (SHA) および Message Digest 5 (MD5) 認証プロトコルと Data Encryption Standard (DES; データ暗号規格) 56 暗号化のサポート。
  - 3 つのセキュリティ レベル : NoAuthNoPriv (認証なし、プライバシーなし)、AuthNoPriv (認証あり、プライバシーなし)、AuthPriv (認証あり、プライバシーあり)

SNMPv3 は、SNMP 通信における最も可用性の高いセキュリティ レベルをサポートします。SNMPv1 と SNMPv2 のコミュニティ ストリングは、暗号化されずにプレーン テキストとして保存および送信されます。SNMPv3 セキュリティ モデルでは、SNMP ユーザは認証され、ユーザ グループに参加します。システム データへのアクセスは、その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 17-1 は、アクセス ポイントでサポートされる SNMP バージョンとセキュリティ レベルを示しています。

表 17-1 SNMP バージョンとセキュリティ レベル

SNMP 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	Keyed-Hashing for Message Authentication Code-Message Digest 5 (HMAC-MD5) または Keyed-Hashing for Message Authentication Code-Secure Hash Algorithm (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 17-2 に説明する操作を実行します。

表 17-2 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。 <sup>1</sup>
get-bulk-request <sup>2</sup>	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割り込みメッセージです。

- 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 エージェントは割り込み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、NMS のコミュニティ スtring の定義は、アクセス ポイントの 3 つのコミュニティ スtring 定義のうち少なくとも 1 つと一致している必要があります。

コミュニティ スtring には、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。
- 読み取りと書き込み：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の変数を設定し、ネットワーク上のデバイスに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 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（特定のイベントの通知）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 17-1 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 C「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. 17-5)
- SNMP エージェントの有効化 (P. 17-5)
- コミュニティ スtring の設定 (P. 17-5)
- トラップ マネージャの設定とトラップの有効化 (P. 17-7)
- エージェントの連絡先と場所の情報の設定 (P. 17-9)
- `snmp-server view` コマンドの使用 (P. 17-9)
- SNMP の例 (P. 17-10)

### デフォルトの SNMP 設定

表 17-3 は、デフォルトの SNMP 設定を示しています。

表 17-3 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	どのストリングも、デフォルトでは設定されていません。ただし、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 IEEE802dot11 MIB への読み取り専用アクセスで、 <i>public</i> コミュニティを自動的に生成します。
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 `command-line interface` (CLI; コマンドライン インターフェイス) 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、SNMPv1 と SNMPv2 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、ストリング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と書き込み権限、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。

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	<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"> <li><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。</li> <li>(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。</li> <li>(オプション) <code>view mib-view</code> には、<b>ieee802dot11</b> 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 <code>snmp-server view</code> コマンドの使用方法は、「<a href="#">snmp-server view コマンドの使用</a>」の項 (P. 17-9) を参照してください。</li> <li>(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 (<b>ro</b>) を指定し、許可された管理ステーションで MIB オブジェクトを取得し、修正する場合は読み取りと書き込み (<b>rw</b>) 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。</li> </ul> <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> <code>{deny   permit} source [source-wildcard]</code>	(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"> <li><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。</li> <li><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。</li> <li><code>source</code> 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。</li> <li>(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。</li> </ul> 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トリングをス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)。特定のコミュニティストリングを削除する場合は、グローバルコンフィギュレーションコマンド `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と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トリングであり、`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トリングであることを指定する方法を示しています。

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

## 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。コミュニティストリングの長さは任意です。

表 17-4 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) について説明しています。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 17-4 通知タイプ

通知タイプ	説明
<b>authenticate-fail</b>	認証の失敗のトラップを有効にします。
<b>config</b>	SNMP 設定変更のトラップを有効にします。
<b>deauthenticate</b>	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。
<b>disassociate</b>	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。
<b>dot11-qos</b>	QoS (Quality Of Service) 変更のトラップを有効にします。
<b>entity</b>	SNMP のエンティティ変更のトラップを有効にします。
<b>rogue-ap</b>	不正アクセス ポイント検出のトラップを有効にします。
<b>snmp</b>	SNMP イベントのトラップを有効にします。
<b>switch-over</b>	切り替えのトラップを有効にします。
<b>syslog</b>	syslog トラップを有効にします。
<b>wlan-wep</b>	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 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 17-4 に示す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 コンフィギュレーション コマンド **snmp-server host** を使用します。

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	<b>configure terminal</b>	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	<b>snmp-server host</b> <i>host-addr</i> { <b>traps</b>   <b>informs</b> } { <b>version</b> {1   2c   3} { <b>auth</b>   <b>noauth</b>   <b>priv</b> }} { <b>community-string</b> [ <b>udp-port</b> <i>port</i> ] <i>notification-type</i> }	<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"> <li><i>host-addr</i> 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。</li> <li>ホストに SNMP トラップを送信する場合は、<b>traps</b> (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、<b>informs</b> を指定します。</li> <li>サポートする SNMP バージョンを指定します。<b>informs</b> 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"> <li><b>auth</b> : 暗号化を行わないパケットの認証を指定します。</li> <li><b>noauth</b> : パケットに認証も暗号化も使用しないことを指定します。</li> <li><b>priv</b> : パケットに認証と暗号化を使用することを指定します。</li> </ul> </li> <li><i>community-string</i> 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 <b>snmp-server host</b> コマンドを使用して設定できますが、シスコでは、<b>snmp-server host</b> コマンドを使用する前に <b>snmp-server community</b> 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。</li> <li><i>notification-type</i> には、表 17-4 (P. 17-8) 内のキーワードを使用します。</li> </ul>



	コマンド	目的
ステップ 3	<b>snmp-server enable traps notification-types</b>	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 17-4 (P. 17-8) 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 <b>snmp-server enable traps</b> コマンドを個別に発行します。
ステップ 4	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show running-config</b>	入力内容を確認します。
ステップ 6	<b>copy running-config startup-config</b>	(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。

特定のホストについてトラップの受信を無効にするには、グローバル コンフィギュレーション 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 コンフィギュレーション 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接点と場所を設定し、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	<b>configure terminal</b>	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	<b>snmp-server contact text</b>	システム接点の文字列を設定します。  例：  <b>snmp-server contact Dial System Operator at beeper 21555.</b>
ステップ 3	<b>snmp-server contact text</b>	システムの場所の文字列を設定します。  例：  <b>snmp-server location Building 3/Room 222</b>
ステップ 4	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show running-config</b>	入力内容を確認します。
ステップ 6	<b>copy running-config startup-config</b>	(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 読み取りと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 読み取りと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 および SNMPv2C 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が許可されます。この設定で、アクセス ポイントからトラップが送信され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と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 ストリングであり、*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 ストリングであることを指定する方法を示しています。

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

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ています。アクセス ポイントはまた 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、*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 のメンバーに対して、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 行目で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 **snmp-server host** コマンドを上書きします。

```
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動作を有効にする方法を示しています。

```
ap(config)# snmp-server enable traps
ap(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、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、リリース 12.3 の『Cisco IOS Configuration Fundamentals Command Reference』を参照してください。

