CHAPTER 7

SNMP の設定

この章では、Cisco Application Control Engine（ACE）モジュールに Cisco MIB（Management Information Base; 管理情報ベース）を照会し、NMS（Network Management System; ネットワーク管理システム）にイベント通知を送信するように 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。

この章の内容は、次のとおりです。

SNMP の概要

SNMP は NMS、SNMP エージェント、および ACE などの管理対象デバイス間における管理情報の交換を容易にするためのアプリケーション レイヤ プロトコルです。NMS にトラップ（イベント通知）を送信するように ACE を設定できます。または、NMS を使用して、ACE 上の MIB を参照することもできます。

ACE には、ネットワーク モニタリングをサポートする SNMP エージェントがあります。ACE がサポートするのは SNMP Version 1（SNMPv1）、SNMP Version 2c（SNMPv2c）、および SNMP Version 3（SNMPv3）です。

SNMPv1 および SNMPv2c では、コミュニティ ストリングの照合によって認証を行います。コミュニティ ストリングは、強制力の弱いアクセス コントロールです。SNMPv3 では、SNMP ユーザを使用した強力な認証機能により、アクセス コントロールが強化されています。SNMPv1 や SNMPv2c の使用は避け、できるだけ SNMPv3 を使用するようにしてください。

SNMPv3 は、相互運用が可能な、標準型のネットワーク管理プロトコルです。SNMPv3 では、ネットワーク上のフレームの認証と暗号化を組み合わせることにより、デバイスに対するセキュアなアクセスを実現しています。SNMPv3 が提供するセキュリティ機能は、次のとおりです。

- メッセージ整合性 — パケットが伝送中に改ざんされていないことを保証します。
- 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 — パケット コンテンツのスクランブルによって、不正な送信元が認識できないようにします。

ここで説明する内容は、次のとおりです。

マネージャおよびエージェント

SNMP では*マネージャ*および*エージェント*というソフトウェア エンティティを使用して、ネットワーク デバイスを管理します。

- *マネージャ*は、ネットワークにおける他のすべての SNMP 管理対象デバイス（ネットワーク ノード）を監視して制御します。管理対象ネットワークには、SNMP マネージャが最低 1 つは必要です。マネージャはネットワーク上のワークステーションにインストールします。
- *エージェント*は、管理対象デバイス（ネットワーク ノード）に配置します。エージェントは、SNMP マネージャから命令を受け取り、さらにイベント発生時に管理情報を SNMP マネージャへ返り送すソフトウェア モジュールです。エージェントはたとえば、デバイスで送受信されたバイト数、パケット数、送受信されたブロードキャスト メッセージ数などのデータを報告します。

SNMP 管理アプリケーションはさまざまですが、実行する基本作業は同じです。これらのアプリケーションによって、SNMP マネージャはエージェントと通信し、ネットワーク デバイスからのアラートを監視、設定、および受信できます。ACE はトラップおよび SNMP **get** 要求をサポートしますが、デバイス上で値を設定する **set** 要求はサポートしません。SNMP と互換性のある NMS を使用すると、ACE を監視できます。

SNMP では、各変数を*管理対象オブジェクト*と呼んでいます。管理対象オブジェクトとは、エージェントがアクセスでき、NMS に報告できるものです。すべての管理対象オブジェクトは MIB に格納されます。MIB は MIB オブジェクトと呼ばれる管理対象オブジェクトのデータベースです。各 MIB オブジェクトは、エージェントのポートから送信されたバイト数をカウントするなど、特定の 1 つの機能を制御します。MIB オブジェクトは MIB 変数からなり、MIB 変数は MIB オブジェクトの名前、デスクリプション、およびデフォルト値を定義します。ACE は、定義ごとに値のデータベースを維持します。

MIB を検索すると、必然的に NMS から SNMP get 要求を実行することになります。任意の SNMPv3、MIB-II 互換ブラウザを使用して、SNMP トラップを受信したり MIB を参照したりできます。

SNMP マネージャおよびエージェントの通信

SNMP マネージャおよびエージェントは、さまざまな方法で通信できます。PDU（プロトコル データ ユニット）は、SNMP マネージャおよびエージェントが情報の送受信に使用するメッセージ形式です。

- SNMP マネージャは、次の動作を実行できます。
  - エージェントから値を取得（**get** 動作）。SNMP マネージャは、エージェント デバイスにログオンしたユーザ数、そのデバイス上のクリティカル デバイスのステータスなどの情報をエージェントに要求します。エージェントは要求された MIB オブジェクトの値を取得し、マネージャにその値を返します（**get-response** 動作）。変数バインディング（varbind）は、要求を受け取った側に、発信元が知りたがっている内容を知らせる MIB オブジェクトのリストです。変数バインディングはオブジェクト識別情報（OID）= 値のペアです。これによって NMS は、受信側が要求を満たし、応答を返したときに、必要な情報を容易に識別できるようになります。
  - 指定した変数の直後の値を取得（**get-next** 動作）。**get-next** 動作では、一連のコマンドを実行することによって、MIB から値のグループを取得します。**get-next** 動作を実行することによって、対象の MIB オブジェクトの正確なインスタンスを知る必要がなくなります。SNMP マネージャが、指定された変数を使用して、順次検索によって対象の変数を検索するからです。
  - 一連の値を取得（**get-bulk** 動作）。get-bulk 動作では、テーブルの複数の行など、大型のデータ ブロックを取得します。そうでない場合、通常は多数の小さいデータ ブロックを伝送しなければなりません。SNMP マネージャは、指定した一連の **get-next** 動作を実行します。
- エージェントは、既定の重要イベントがエージェントで発生した場合、いつでも SNMP マネージャに割り込みメッセージを送信できます。このメッセージをイベント通知と呼んでいます。SNMP イベント通知（トラップまたは情報要求）は、多数の MIB に組み込まれており、NMS から管理対象デバイスに頻繁にポーリング（**get** 動作による情報収集）を実行しなくてすむようになります。ACE がサポートする MIB オブジェクトおよび SNMP 通知の詳細については、「サポート対象の MIB および通知」を参照してください。

SNMP トラップおよび応答要求

特定のイベントが発生したときに、SNMP マネージャに通知（トラップまたは応答要求）を送信するように ACE を設定できます。トラップは、受信側がトラップを受信しても確認応答を送信しないので、送信側でトラップが受信されたかどうかを調べることができず、信頼性に欠ける場合があります。しかし、応答要求を受信した SNMP マネージャは、SNMP 応答 PDU でメッセージの確認応答を行います。送信側が応答を受信しなかった場合は、通常、応答要求が再送信されます。応答要求の所定の宛先に届く可能性が高くなります。

通知には MIB 変数バインディングのリストが含まれ、通知によってリレーされるステータスが明確になります。通知に関連付けられた変数バインディングのリストは、MIB の通知定義に含まれます。シスコでは標準 MIB に関して、変数バインディングを追加することによって一部の通知を拡張し、通知理由がいっそう明確になるようにしています。

（注）　NMS アプリケーションで、各通知に付加された clogOriginID および clogOriginIDType 変数バインディングを使用することによって、トラップの発信元デバイスを固有のものとして特定できます。**logging device-id** コンフィギュレーション モード コマンドを使用すると、デバイスを固有のものとして特定する clogOriginID および clogOriginIDType 変数バインディングの値を設定できます。**logging device-id** コマンドの詳細については、『*Cisco Application Control Engine Module System Message Guide*』を参照してください。

トラップの宛先および応答要求の詳細を取得するには、SNMP-TARGET-MIB を使用します。

ACE がサポートする SNMP 通知の詳細については、「サポート対象の MIB および通知」を参照してください。

SNMPv3 の CLI によるユーザ管理および AAA 統合

ACE では、メッセージ セキュリティおよびロールベース アクセス コントロールに対応する SNMPv3 USM（ユーザベース セキュリティ モデル）を含んだ RFC 3414 および RFC 3415 を実装しています。SNMPv3 のユーザ管理は、AAA（認

証、認可、アカウンティング）サーバ レベルで中央集中化が可能です。（詳細は『*Cisco Application Control Engine Module Security Configuration Guide*』を参照してください。）この中央集中型のユーザ管理によって、ACE の SNMP エージェントは AAA サーバのユーザ認証サービスを利用できます。ユーザ認証の確認後、SNMP PDU の処理が続けられます。AAA サーバは、ユーザ グループ名の保管にも使用されます。SNMP ではグループ名を使用して、ACE でローカルに使用できるユーザ アクセスおよびロール ポリシーを適用します。

CLI および SNMP ユーザの同期

ユーザ グループ、ロール、またはパスワードの設定を変更すると、SNMP と AAA の両方でデータベースが同期化します。**username** コマンドを使用して CLI ユーザを作成する場合は、『*Cisco Application Control Engine Module Virtualization Configuration Guide*』を参照してください。**snmp-server user** コマンドを使用して SNMP ユーザを作成する場合は、「SNMP ユーザの設定」を参照してください。

ユーザの同期は次のように行われます。

- **no username** コマンドを使用してユーザを削除すると、そのユーザは SNMP と CLI の両方からも削除されます。ただし、**no snmp-server user** コマンドを使用してユーザを削除した場合は、そのユーザは SNMP からだけ削除され、CLI からは削除されません。
- ユーザロール マッピングの変更は、SNMP と CLI で同期します。

（注） セキュリティ暗号化のために、ローカライズした鍵または暗号化形式でパスワードを指定した場合、パスワードは同期しません。

- **username** コマンドで指定したパスワードは、SNMP ユーザの **auth** および **priv** パスワードと同期します。
- 既存の SNMP ユーザは、**auth** および **priv** 情報を変更しないまま維持できます。
- パスワードを指定しないで **username** コマンドを使用して、SNMP データベースに存在しない新規ユーザを作成した場合、その SNMP ユーザは noAuthNoPriv セキュリティ レベルで作成されます。

サポート対象の MIB および通知

表 7-1 に、ACE のサポート対象 MIB を示します。

表 7-1　SNMP MIB サポート

MIB サポート	機能 MIB	説明
スーパーバイザ モジュール MIB		
CISCO-ENTITY-FRU-CONTROL-MIB	CISCO-ENTITY-FRU-CONTROL-CAPABILITY	ENTITY-MIB の拡張版として機能。ACE の動作状態を監視します。CISCO-ENTITY-FRU-CONTROL-MIB のサポートは、管理コンテキストに限られます。
CISCO-ENTITY-VENDORTYPE-OID-MIB	該当せず	各種 ACE コンポーネントに割り当てるオブジェクト識別情報（OID）を定義します。この MIB の OID は、entPhysicalTable の entPhysicalVendorType フィールドの値として、ENTITY-MIB の entPhysicalTable で使用されます。各 OID は、シャーシ、ラインカード、ポート アダプタといった物理エンティティのタイプを一意に特定します。次に entPhysicalVendorType OID 値のリストを示します。 **製品名（PID）　entPhysicalVendorType** ACE10-6500-K9　cevCat6kAce10K9 ACE20-MOD-K9　cevCat6kAce10K9 （cevModuleCat6000Type120） 空気取り入れ口の温度 cevSensorModuleInletTemp （cevSensor 36） 空気吹き出し口の温度 cevSensorModuleOutletTemp （cevSensor 35） その他のデバイス 温度センサー　cevSensorModuleDeviceTemp （cevSensor 31）

表 7-1　SNMP MIB サポート（続き）

MIB サポート	機能 MIB	説明
ENTITY-MIB	CISCO-ENTITY-CAPABILITY	ネットワーク デバイス内の物理エンティティおよび論理エンティティの基本管理および識別を行います。ENTITY-MIB のソフトウェア サポートは、ACE 内の物理エンティティが中心です。この MIB は、スイッチ シャーシ内部の各モジュール、電源モジュール、およびファン トレイの詳細情報を提供します。ACE 内に組み込まれているこれらのエンティティを正確にマッピングし、シャーシ ビューを作成できるだけの十分な情報が得られます。 ENTITY-MIB のサポートは、管理コンテキストに限られます。 ENTITY-MIB は RFC 4133 で規定されています。
ENTITY-SENSOR-MIB	CISCO-ENTITY-SENSOR-RFC-CAPABILITY	entitySensorValueGroup というグループが 1 つだけ含まれます。このグループによって、オブジェクトは物理センサーの現在値および状態を通知することができます。entitySensorValueGroup には、entPhySensorTable というテーブルが 1 つだけ含まれます。このテーブルでは、センサーのデータ ユニットのタイプ、スケール係数、精度、現在値、および動作状態を特定する、少数の読み取り専用オブジェクトが提供されます。 ENTITY-SENSOR-MIB のサポートは、管理コンテキストに限られます。 ENTITY-SENSOR-MIB は RFC 3433 で規定されています。

表 7-1　SNMP MIB サポート（続き）

MIB サポート	機能 MIB	説明
SNMPv3 エージェント MIB		
SNMP-COMMUNITY-MIB	CISCO-SNMP-COMMUNITY-CAPABILITY	コミュニティ ストリングとバージョンに依存しない SNMP メッセージ パラメータ間のマッピングに関するオブジェクトが含まれます。この MIB はさらに、受信した要求の送信元アドレスを検証し、発信する通知のターゲット アドレスに基づいてコミュニティ ストリングを選択するメカニズムを提供します。 SNMP-COMMUNITY-MIB は RFC 3584 で規定されています。 （注）　SNMP コミュニティが適用されるのは、SNMPv1 と SNMPv2c だけです。SNMPv3 では、ユーザが所属するロール グループ、ユーザの認証パラメータ、認証パスワード、メッセージ暗号化パラメータの指定などのユーザ設定情報が必要です。
SNMP-FRAMEWORK-MIB	CISCO-SNMP-FRAMEWORK-CAPABILITY	SNMP エンジン、アクセス コントロール サブシステムを含め、SNMP 管理フレームワークの要素を定義します。 SNMP-FRAMEWORK-MIB は RFC 3411 で規定されています。
SNMP-MPD-MIB	CISCO-SNMP-MPD-CAPABILITY	SNMP のメッセージ プロセッシング サブシステムおよびディスパッチャを規定します。SNMP エンジンのディスパッチャは、SNMP メッセージを送受信します。さらに、SNMP アプリケーションに SNMP PDU をディスパッチします。メッセージ プロセッシング モデルは、SNMP のバージョン固有メッセージを処理し、セキュリティ サブシステムとの対話を調整することによって、取り扱う SNMP メッセージに適切なセキュリティが適用されるようにします。 SNMP-MPD-MIB は RFC 3412 で規定されています。

表 7-1　SNMP MIB サポート（続き）

MIB サポート	機能 MIB	説明
SNMP-NOTIFICATION-MIB	CISCO-SNMP-NOTIFICATION-CAPABILITY	通知を生成する目的で SNMP エンティティに使用させるパラメータのリモート設定用メカニズムを提供する、MIB オブジェクトを定義します。 SNMP-NOTIFICATION-MIB は RFC 3413 で規定されています。
SNMP-TARGET-MIB	CISCO-SNMP-TARGET-CAPABILITY	管理ターゲット メッセージの宛先情報および SNMP パラメータに関するテーブルが含まれます。複数のトランスポート エンド ポイントを特定の SNMP パラメータ セットに、または特定のトランスポート エンド ポイントを複数の SNMP パラメータ セットに関連付けることができます。 SNMP-TARGET-MIB は RFC 3413 で規定されています。

表 7-1　SNMP MIB サポート（続き）

MIB サポート	機能 MIB	説明
SNMP-USER-BASED-SM-MIB	CISCO-SNMP-USM-CAPABILITY	SNMPv3 の USM（ユーザベース セキュリティ モデル）に対応する管理情報定義を提供します。SNMPv3 アーキテクチャでは、メッセージのセキュリティを確保するために USM が採用されています。 USM モジュールは、着信メッセージを復号化します。さらに認証データを検証し、PDU を作成します。発信メッセージに関しては、USM モジュールは PDU を暗号化し、認証データを生成します。さらに、メッセージ プロセッサに PDU を引き渡し、メッセージ プロセッサがディスパッチャを呼び出します。 USM モジュールで実装される SNMP-USER-BASED-SM-MIB によって、SNMP マネージャは、ユーザとセキュリティ鍵を管理するコマンドを発行できます。この MIB はさらに、要求側ユーザが存在し、適切な認証情報があることをエージェントが確認できるようにします。認証後、エージェントにより要求が実行されます。 SNMP-USER-BASED-SM-MIB は RFC 3414 で規定されています。 （注）　ユーザ設定が適用されるのは、SNMPv3 だけです。SNMPv1 および SNMPv2c では、コミュニティ ストリングの照合によってユーザを認証します。

表 7-1　SNMP MIB サポート（続き）

MIB サポート	機能 MIB	説明
SNMP-VIEW-BASED-ACM-MIB	CISCO-SNMP-VACM-CAPABILITY	SNMPv3 の VACM（ビューベース アクセス コントロール モデル）を提供します。SNMPv3 アーキテクチャでは、アクセス コントロールに VACM が採用されています。 SNMP-VIEW-BASED-ACM-MIB では、SNMP エージェントからアクセス可能なすべての MIB データへのアクセスを制御するために必要なオブジェクトを規定します。VACM モジュールは初期化時に、エージェント インフラストラクチャにアクセス コントロール モジュールとして登録されます。VACM モジュールは、SNMP メッセージの複数のパラメータに基づいて、アクセス コントロール チェックを実行します。 SNMP-VIEW-BASED-ACM-MIB は RFC 3415 で規定されています。
その他の MIB		
CISCO-AAA-SERVER-EXT-MIB	CISCO-AAA-SERVER-EXT-CAPABILITY	CISCO-AAA-SERVER-MIB の拡張版として機能。他のタイプのサーバ アドレスが含まれるように、CISCO-AAA-SERVER-MIB の casConfigTable を拡張します。CISCO-AAA-SERVER-EXT-MIB は、次の設定機能を管理します。 • 認証およびアカウンティング　モジュールに適用される一般設定 • コンフィギュレーションの設定（この MIB の 1 つのインスタンスで用意されているすべての AAA サーバの設定値） • AAA サーバ グループの設定 • アプリケーション、AAA 機能、サーバ グループ間のマッピングの設定

表 7-1　SNMP MIB サポート（続き）

MIB サポート	機能 MIB	説明
CISCO-AAA-SERVER-MIB	CISCO-AAA-SERVER-CAPABILITY	デバイス内の AAA サーバ動作状態および外部サーバとの AAA 通信を示す、コンフィギュレーションおよび統計情報を提供します。CISCO-AAA-SERVER-MIB が提供する情報は、次のとおりです。 • AAA サーバ設定用のテーブル • 外部 AAA サーバのアイデンティティ • 各 AAA 機能の統計情報 • AAA 機能を提供するサーバのステータス サーバは、任意の AAA 機能を提供する論理エンティティとして定義されます。ACE では、Remote Access Dial-In User Service（RADIUS）、Terminal Access Controller Access Control System Plus（TACACS+）、または Lightweight Directory Access Protocol（v3）（LDAP）プロトコルを使用して、リモート認証を行い、アクセス権を指定できます。
CISCO-ENHANCED-SLB-MIB	CISCO-ENHANCED-SLB-CAPABILITY	CISCO-SLB-MIB および CISCO-SLB-EXT-MIB で定義されたテーブルを拡張し、次のサーバ ロード バランシング機能をサポートします。 • 名前で指定した実サーバによる実サーバ設定。cesRserverTable が実サーバ情報を提供します。 • サーバ ファーム内の実サーバ設定 • 実サーバのヘルス プローブ設定 • HTTP ヘッダー、HTTP クッキー、クライアント IP アドレス、および SSL のスティッキ設定 テーブルで使用する slbEntity Index は ACE のスロット番号です。
CISCO-IF-EXTENSION-MIB	CISCO-IF-EXTENSION-CAPABILITY	インターフェイスに ifIndex を割り当てるために、ifName から ifIndex へのマッピングを返すテーブルを提供します。 CISCO-IF-EXTENSION-MIB は RFC 2863 で規定されています。

表 7-1　SNMP MIB サポート（続き）

MIB サポート	機能 MIB	説明
CISCO-IP-PROTOCOL-FILTER-MIB	CISCO-IP-PROTOCOL-FILTER-CAPABILITY	IP プロトコルのパケット フィルタリングをサポートするための情報を管理します（RFC 791）。 ユーザは cippfIpProfileTable を使用することで、フィルタ プロファイルの情報を作成、削除、および取得できます。フィルタ プロファイルは、プロファイル名で一意に特定されます。フィルタ プロファイルは、簡易使用タイプまたは拡張使用タイプのどちらにでもできます。作成後の使用タイプ変更はできません。cippfIfIpProfileTable は、IP を実行するデバイス インターフェイスにフィルタリング プロファイルを適用します。フィルタ プロファイルは複数のインターフェイスに適用可能です。 cippfIpFilterTable には、すべてのフィルタリング プロファイルに対応する IP フィルタの順序付きリストが含まれます。フィルタおよびプロファイルは、同じフィルタ プロファイル名が与えられている場合に関連付けられます。フィルタを作成できるのは、関連付けられたフィルタ プロファイルが cippfIpProfileTable にすでに存在している場合だけです。同じプロファイル名のフィルタは、共通プロファイルに属します。 他のテーブルに依存しない情報を指定して、インターフェイスベースの cippfIfIpProfileTable を設定できます。ただし、このテーブルのプロファイル名が cippfIpProfileTable のいずれかのプロファイル名および cippfIpFilterTable のいずれかのフィルタ エントリのプロファイル名と一致した場合、プロファイルがアクティブになり、接続デバイス インターフェイスを通過する IP トラフィックにそのフィルタ エントリが適用されます。cippfIpFilterTable のフィルタまたは cippfIpProfileTable のプロファイルを変更すると、すべての接続インターフェイスが影響を受けます。 IP プロトコルは RFC 791 で規定されています。

表 7-1　SNMP MIB サポート（続き）

MIB サポート	機能 MIB	説明
CISCO-L4L7RESOURCE-LIMIT-MIB	CISCO-L4L7MODULE-RESOURCE-LIMIT-CAPABILITY	リソース クラスおよび各種リソースへの最小 / 最大限度設定を管理します。この MIB で参照されるリソースは、他の MIB で使用できるリソース情報への追加ということになります。この MIB は、中央集中方式によるリソース限度管理をサポートする、レイヤ 4 ～ 7 のモジュールに適用されます。設定するリソースには、TCP/IP 接続、MAC アドレス、Syslog バッファ、ACL メモリ、NAT 変換などのカテゴリが含まれます。 entPhysicalIndex の値は常に 1 になります。
CISCO-MODULE-VIRTUALIZATION-MIB	CISCO-MODULE-VIRTUALIZATION-CAPABILITY	ACE ユーザ コンテキスト（仮想コンテキストともいう）の作成、管理方法を提供します。ユーザ コンテキストは、物理デバイス（ACE）の論理パーティションです。ユーザ コンテキストは、別々に管理可能な各種サービス タイプを提供します。各ユーザ コンテキストは、専用のコンフィギュレーションが与えられた、独立したエンティティです。ユーザが作成したコンテキストは、管理コンテキスト（デフォルトの ACE コンテキスト）で設定できるオプションの大部分をサポートします。コンテキストごとに、別々の管理 IP アドレスを与えることができます。この管理 IP アドレスにより、SSH（セキュア シェル）または Telnet プロトコルを使用して ACE とのリモート接続を確立し、その他の要求（SNMP、FTP など）を送信できます。 この MIB に含まれるテーブルを使用すると、ACE ユーザ コンテキストを作成または削除できます。また、ユーザ コンテキストにインターフェイスとインターフェイス範囲を割り当てることができます。

表 7-1　SNMP MIB サポート（続き）

MIB サポート	機能 MIB	説明
CISCO-PROCESS-MIB	CISCO-PROCESS-CAPABILITY	シスコ製デバイスのメモリおよびプロセス CPU 使用率を表示します。この情報はあくまでも推定値です。cpmCPUTotalPhysicalIndex の値は常に 1 になります。 表示されるシステム プロセス情報は、CPU システム レベルのものであり（総 CPU 使用率）、コンテキスト単位のレベルではありません。
CISCO-PRODUCTS-MIB	該当せず	SNMPv2-MIB の sysObjectID オブジェクトで報告可能な OID が含まれます。sysObjectID OID の値は次のとおりです。 **製品名（PID）　sysObjectID** ACE10-6500-K9/ ACE20-MOD-K9　ciscoACE10K9（ciscoProducts 730）
CISCO-SLB-EXT-MIB	CISCO-SLB-EXT-CAPABILITY	Cisco サーバ ロード バランシング MIB（CISCO-SLB-MIB）の拡張版として機能。スティッキ設定用のテーブルを提供します。 ACE に対応する次の MIB オブジェクトには、SLB に関連しない接続も含まれます。 • cslbxStatsCurrConnections • cslbxStatsTimedOutConnections
CISCO-SLB-HEALTH-MON-MIB	CISCO-SLB-HEALTH-MON-CAPABILITY	Cisco サーバ ロード バランシング MIB（CISCO-SLB-MIB）の拡張版として機能。プローブ設定用のテーブルを提供します。

表 7-1　SNMP MIB サポート（続き）

MIB サポート	機能 MIB	説明
CISCO-SLB-MIB	CISCO-SLB-CAPABILITY	サーバ ロード バランシング（SLB）マネージャ（複数可）を管理します。この MIB は、SLB 接続統計情報、サーバ ファーム、実サーバ、VIP ステータス、VIP 統計情報などを監視します。 テーブルで使用する slbEntity Index は ACE のスロット番号です。スロット番号値は ACE モジュールには適用されないので、slbEntity Index の値は常に 1 になります。 ACE に対応する次の MIB オブジェクトには、SLB に関連しない接続も含まれます。 • slbStatsCreatedConnections • slbStatsCreatedHCConnections • slbStatsEstablishedConnections • slbStatsEstablishedHCConnetions • slbStatsDestroyedConnections • slbStatsDestroyedHCConnections • slbStatsReassignedConnections
CISCO-SYSLOG-EXT-MIB	CISCO-SYSLOG-EXT-CAPABILITY	CISCO-SLB-MIB を拡張し、追加のサーバ ファーム設定パラメータ（cslbxServerFarmTable）を提供し、ACE 用のシステム ログ（Syslog）管理パラメータを設定して監視します。この MIB は、Syslog サーバを設定し、ロギング重大度を設定する場合に使用します。 Syslog は RFC 3164 で規定されています。

表 7-1　SNMP MIB サポート（続き）

MIB サポート	機能 MIB	説明
CISCO-SYSLOG-MIB	CISCO-SYSLOG-CAPABILITY	ACE によって生成されたシステム メッセージ（Syslog メッセージ）を記述して保管します。 CISCO-SYSLOG-MIB は、SNMP を使用して Syslog メッセージにアクセスできるようにします。この MIB には、Syslog 通知の送信をイネーブルまたはディセーブルにする、Syslog メッセージおよびオブジェクトの履歴も含まれます。 （注）　この MIB は、CLI からのデバッグ コマンドによって生成されたメッセージは追跡しません。 Syslog は RFC 3164 で規定されています。
IF-MIB	CISCO-IF-CAPABILITY	インターフェイスの一般情報（VLAN など）を報告します。 IF-MIB は RFC 2863 で規定されています。
IP-MIB	CISCO-IP-CAPABILITY	IP および対応する ICMP（インターネット制御メッセージ プロトコル）の実装管理に対して管理対象オブジェクトを定義しますが、IP ルートの管理は除外されます。 IP-MIB は RFC 4293 で規定されています。
SNMPv2-MIB	CISCO-SNMPv2-CAPABILITY	SNMPv2 用の MIB を提供します。管理プロトコル SNMPv2 は、エージェントと管理ステーション間で管理情報を通知するメッセージ交換を規定します。 SNMPv2-MIB は RFC 3418 で規定されています。
TCP-MIB	CISCO-TCP-STD-CAPABILITY	TCP の実装管理に対して、管理対象オブジェクトを定義します。 TCP-MIB は RFC 4022 で規定されています。

表 7-1　SNMP MIB サポート（続き）

MIB サポート	機能 MIB	説明
UDP-MIB	CISCO-UDP-STD-CAPABILITY	UDP（ユーザ データグラム プロトコル）の実装管理に対して、管理対象オブジェクトを定義します。 UDP-MIB は RFC 4113 で規定されています。

表 7-2 に、ACE のサポート対象 SNMP 通知（トラップ）を示します。

（注） イベント トラップの発生元であるシャーシ、スロット、およびコンテキストのコンビネーションを特定できるように、表 7-2 の各通知に clogOrigin ID および clogOriginIDType 変数バインディングが付加されます。

表 7-2　SNMP トラップ サポート

通知名	通知の保管場所	説明
authenticationFailure	SNMPv2-MIB	NMS が有効なコミュニティ ストリングを使用して認証を行わなかったので、SNMP 要求は失敗します。
cesRealServerStateUp	CISCO-ENHANCED-SLB-MIB	サーバ ファームで設定されている実サーバの状態は、ユーザの介入によりアップです。
cesRealServerStateDown	CISCO-ENHANCED-SLB-MIB	サーバ ファームで設定されている実サーバの状態は、ユーザの介入によりダウンです。
cesRealServerStateChange	CISCO-ENHANCED-SLB-MIB	サーバ ファームで設定されている実サーバの状態は、ユーザ介入以外のイベントにより、新しい状態に変化しました。この通知は、ARP 障害、プローブ障害などの状況で送信されます。

表 7-2　SNMP トラップ サポート（続き）

通知名	通知の保管場所	説明
cesRserverStateUp	CISCO-ENHANCED-SLB-MIB	グローバル実サーバの状態は、ユーザ介入によりアップです。 （注）　この実サーバで受信する実サーバごとに、別個の cesRealServerStateUp 通知が送信されることはありません。
cesRserverStateDown	CISCO-ENHANCED-SLB-MIB	グローバル実サーバの状態は、ユーザ介入によりダウンです。 （注）　この実サーバで受信する実サーバごとに、別個の cesRealServerStateDown 通知が送信されることはありません。
cesRserverStateChange	CISCO-ENHANCED-SLB-MIB	グローバル実サーバの状態は、ユーザ介入以外のイベントにより、新しい状態に変化しました。この通知は、ARP 障害、プローブ障害などの状況で送信されます。 （注）　この実サーバで受信する実サーバごとに、別個の cesRealServerStateChange 通知が送信されることはありません。

表 7-2　SNMP トラップ サポート（続き）

通知名	通知の保管場所	説明
ciscoSlbVServerVIPState Change	CISCO-SLB-MIB.my	仮想サーバの状態が変化しています。この通知は、次の変数バインディングとともに送信されます。 • slbVServerState • slbVServerStateChangeDescr • slbVServerClassMap • slbVServerPolicyMap • slbVServerIpAddressType • slbVServerIpAddress • slbVServerProtocol 仮想サーバの状態が変化する理由は、インターフェイスとのバインディング、ポリシーからのアクティブ サーバ ファームの削除、仮想 IP アドレス（VIP）とクラス マップの関連付けなど、さまざまです。 ciscoSlbVServerVIPStateChange は CISCO-SLB-MIB で規定されています。
ciscoSlbVServerState Change	CISCO-SLB-MIB.my	クラス マップから VIP が削除されたという通知。この通知は、次の変数バインディングとともに送信されます。 • slbVServerState • slbVServerStateChangeDescr • slbVServerClassMap • slbVServerPolicyMap ciscoSlbVServerStateChange は CISCO-SLB-MIB で規定されています。
clogMessageGenerated	CISCO-SYSLOG-MIB	ACE が 1 つまたは複数の Syslog メッセージを生成しました。

表 7-2　SNMP トラップ サポート（続き）

通知名	通知の保管場所	説明
clmLicenseExpiryNotify	CISCO-LICENSE-MGR-MIB	インストールされている機能のライセンスが期限切れになったという通知。
clmLicenseFileMissing Notify	CISCO-LICENSE-MGR-MIB	インストールされているはずの 1 つまたは複数のライセンス ファイルの欠落が検出されたという通知。
clmLicenseExpiryWarning Notify	CISCO-LICENSE-MGR-MIB	インストールされている機能のライセンスの期限切れが近いことが検出されたという通知。
clmNoLicenseForFeature Notify	CISCO-LICENSE-MGR-MIB	特定の機能について、ライセンスがインストールされていないことが検出されたという通知。
cmVirtContextAdded, cmVirtContextRemoved	CISCO-MODULE-VIRTUALIZATION-MIB	ユーザが ACE ユーザ コンテキスト（仮想コンテキストともいう）を作成または削除したという通知。
coldStart	SNMPv2-MIB	ACE のコールド リスタート（全面的な電源再投入）後に SNMP エージェントが起動しました。
linkUp, linkDown	SNMPv2-MIB	VLAN インターフェイスはアップまたはダウンです。VLAN インターフェイスがダウンになるのは、**shut** コマンドに続いて **no shut** コマンドを指定した場合、またはスイッチの設定で VLAN が削除された場合などです。

SNMP の制限事項

SNMP MIB テーブルに、48 文字を超えるストリング インデックスが複数ある場合、SNMP ウォークの実行時にインデックスが MIB テーブルに表示されないことがあります。SNMP の規格に従い、SNMP 要求、応答、またはトラップに 128 を超えるサブ ID を使用することはできません。次にオブジェクト名のリストを示します。

- コンテキスト名
- 実サーバ名
- サーバ ファーム名
- プローブ名

- HTTP ヘッダー名
- ACL 名
- クラス マップ名
- ポリシー マップ名
- リソース クラス名

表 7-3 に、複数のストリング インデックスを使用できるテーブルを示します。

表 7-3　複数のストリング インデックスを使用できる SNMP MIB テーブル

MIB 名	テーブル	ストリング インデックス
CISCO-ENHANCED-SLB-MIB.my	cesRserverProbeTable	cesRserverName, cesRserverProbeName
CISCO-ENHANCED-SLB-MIB.my	cesServerFarmRserverTable	slbServerFarmName, cesRserverName
CISCO-SLB-EXT-MIB.my	cslbxServerFarmProbeFarmName	cslbxServerFarmProbeFarmName, cslbxServerFarmProbeProbeName
CISCO-SLB-HEALTH-MON-MIB.my	cslbxProbeHeaderCfgTable	cslbxProbeHeaderProbeName, cslbxProbeHeaderFieldName

SNMP コンフィギュレーション クイック スタート

表 7-4 に、ACE 上で SNMP を設定するために必要な手順の概要を示します。各手順には、作業に必要な CLI コマンドが含まれています。

表 7-4　SNMP 管理コンフィギュレーション クイック スタート

作業およびコマンド例

1. 複数のコンテキストで動作する場合は、CLI プロンプトを観察して、正しいコンテキストで動作していることを確認してください。必要に応じて、正しいコンテキストに直接ログインするか、変更してください。
`host1/Admin# changeto C1`
`host1/C1#`
この表の例ではこれ以降、特に指定しないかぎり管理コンテキストを使用します。コンテキスト作成の詳細については、『*Cisco Application Control Engine Module Virtualization Configuration Guide*』を参照してください。

2. コンフィギュレーション モードを開始します。
`host1/Admin# config`
`Enter configuration commands, one per line. End with CNTL/Z`
`host1/Admin(config)#`

3. ACE の CLI から 1 つまたは複数の SNMP ユーザを設定します。
`host1/Admin(config)# snmp-server user joe Network-Monitor auth sha abcd1234`
`host1/Admin(config)# snmp-server user sam Network-Monitor auth md5 abcdefgh`
`host1/Admin(config)# snmp-server user Bill Network-Monitor auth sha abcd1234 priv abcdefgh`

4. SNMP コミュニティを作成し、アクセス権限を指定します。 `host1/Admin(config)# snmp-server community SNMP_Community1 group Network-Monitor`
5. SNMP システムのコンタクト名を指定します。 `host1/Admin(config)# snmp-server contact "User1 user1@cisco.com"`
6. SNMP システムのロケーションを指定します。 `host1/Admin(config)# snmp-server location "Boxborough MA"`

表 7-4　SNMP 管理コンフィギュレーション クイック スタート（続き）

作業およびコマンド例
7. SNMP 通知を受信するホストを指定します。 `host1/Admin(config)# snmp-server host 192.168.1.1 traps version 2c SNMP_Community1 udp-port 500`
8. ACE から NMS に SNMP トラップおよび応答要求を送信できるようにします。 `host1/Admin(config)# snmp-server enable traps slb`

9. SNMP 管理プロトコルおよびクライアントの送信元 IP アドレスに基づいて、ACE がネットワーク管理トラフィックを受信することを許可するクラス マップを作成します。
`host1/Admin(config)# class-map type management match-all SNMP-ALLOW_CLASS`
`host1/Admin(config-cmap-mgmt)# match protocol snmp source-address 172.16.10.0 255.255.255.254`
`host1/Admin(config-cmap-mgmt)# exit`
`host1/Admin(config)#`

10. SNMP 管理プロトコル分類をアクティブにするポリシー マップを設定します。
`host1/Admin(config)# policy-map type management first-match SNMP-ALLOW_POLICY`
`host1/Admin(config-pmap-mgmt)# class SNMP-ALLOW_CLASS`
`host1/Admin(config-pmap-mgmt-c)# permit`
`host1/Admin(config-pmap-mgmt-c)# exit`
`host1/Admin(config-pmap-mgmt)# exit`
`host1/Admin(config)#`

11. 単一 VLAN インターフェイスにトラフィック ポリシーを接続するか、または同じコンテキスト内のすべての VLAN インターフェイスにグローバルに接続します。インターフェイス VLAN を指定して、その VLAN に SNMP 管理ポリシー マップを適用する例を示します。
`host1/Admin(config)# interface vlan 50`
`host1/Admin(config-if)# ip address 172.16.10.0 255.255.255.254`
`host1/Admin(config-if)# service-policy input SNMP-ALLOW_POLICY`
`host1/Admin(config-if)# exit`

12.（任意）フラッシュ メモリに設定変更を保存します。
`host1/Admin(config)# exit`
`host1/Admin# copy running-config startup-config`

SNMP ユーザの設定

SNMP ユーザは ACE の CLI から設定します。ユーザ設定には、ユーザが所属するロール グループ、ユーザの認証パラメータ、認証パスワード、メッセージ暗号化パラメータの指定などの情報が含まれます。SNMP ユーザ情報を設定するには、コンフィギュレーション モードで **snmp-server user** コマンドを使用します。

（注）　**snmp-server user** コマンドによるユーザ設定が適用されるのは、SNMPv3 の場合だけです。SNMPv1 および SNMPv2c では、コミュニティ ストリングの照合を使用してユーザを認証します（「SNMP コミュニティの定義」を参照）。

ACE は、**username** コマンドによって作成されたユーザと **snmp-server user** コマンドによって作成されたユーザ間の対話を同期させます。したがって、ACE CLI からのユーザ アップデートは、SNMP サーバに自動的に反映されます。ユーザを削除すると、SNMP と CLI の両方でユーザが自動的に削除されます。さらに、ユーザロール マッピングの変更が SNMP に反映されます。

注意　管理コンテキストまたはユーザ コンテキストに対応する SNMP エンジン ID を変更すると、設定されているすべての SNMP ユーザが無効になります。その場合、コンフィギュレーション モードで **snmp-server user** コマンドを使用し、すべての SNMP ユーザを再び作成する必要があります。SNMPv3 エンジン ID の詳細については、「ACE コンテキストに対応する SNMPv3 エンジン ID の設定」を参照してください。

snmp-server user コマンドの構文は次のとおりです。

snmp-server user *user_name* [*group_name*] [**auth** {**md5** | **sha**} *password1* [**localizedkey** | **priv** {*password2* | **aes-128** *password2*}]]

キーワード、引数、およびオプションは次のとおりです。

- *user_name* — ユーザ名。最大 24 文字の英数字からなる文字列を、引用符なしで入力します。スペースは使用しません。

- *group_name* —（任意）ユーザが所属するユーザ ロール グループ。最大 32 文字の英数字からなる文字列を、引用符なしで入力します。スペースは使用しません。SNMP のアクセス権は、グループ別に編成されます。SNMP における各グループは、CLI で設定するロールに類似しています。*groupname* は、**ロール** コンフィギュレーション モードで定義します。詳細は、『*Cisco Application Control Engine Module Virtualization Configuration Guide*』を参照してください。ユーザに複数のロールを割り当てる場合は、複数の **snmp-server user** コマンドを入力します。

（注） ACE の SNMP でサポートされるのは、ネットワーク モニタリング動作だけです。この場合、すべての SNMP ユーザに、システム定義のデフォルト グループ Network-Monitor が自動的に割り当てられます。ユーザ作成の詳細については、『*Cisco Application Control Engine Module Virtualization Configuration Guide*』を参照してください。

- **auth** —（任意）ユーザの認証パラメータを設定します。認証によって、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。
- **md5** — ユーザ認証に HMAC MD5（メッセージ ダイジェスト 5）暗号化アルゴリズムを指定します。
- **sha —** ユーザ認証に HMAC SHA 暗号化アルゴリズムを指定します。
- *password1* — ユーザ認証パスワード。最大 130 文字の英数字からなる文字列を、引用符なしで入力します。スペースは使用しません。ACE は、SNMP 認証パスワードを CLI ユーザのパスワードと自動的に同期させます。
- **localizedkey** —（任意）パスワードをセキュリティのためにローカライズされた暗号化鍵形式に指定します。
- **priv** —（任意）ユーザの暗号化パラメータを指定します。**priv** オプションおよび **aes-128** オプションは、128 ビットの AES 鍵を生成するためのプライバシ パスワードであることを示します。
- **aes-128** — プライバシを確保するために 128 バイトの AES（高度暗号化規格）アルゴリズムを指定します。AES は対称暗号アルゴリズムであり、SNMP メッセージ暗号化に対応するプライバシ プロトコルの 1 つです。これは RFC 3826 に準拠しています。

（注）　外部 AAA サーバを使用して SNMPv3 を動作させる場合、このサーバ上のユーザ設定に SNMP PDU 暗号化に対応する AES が必要です。

- *password2* — ユーザの暗号化パスワード。AES **priv** パスワードは、8 文字以上にします。パスフレーズをクリア テキストで指定する場合は、最大 64 文字の英数字を使用できます。ローカライズした鍵を使用する場合は最大 130 文字の英数字を指定できます。スペースは使用できません。

ユーザ情報の入力例を示します。

```
host1/Admin# config
Enter configuration commands, one per line. End with CNTL/Z
host1/Admin(config)# snmp-server user joe Network-Monitor auth sha
abcd1234
host1/Admin(config)# snmp-server user sam Network-Monitor auth md5
abcdefgh
host1/Admin(config)# snmp-server user Bill Network-Monitor auth sha
abcd1234 priv abcdefgh
```

SNMP ユーザ設定をディセーブルにする場合、または SNMP ユーザを削除する場合は、このコマンドの **no** 形式を使用します。以下に入力例を示します。

```
host1/Admin(config)# no snmp-server user Bill Network-Monitor auth sha
abcd1234 priv abcdefgh
```

SNMP コミュニティの定義

各 SNMP デバイスまたはメンバは、コミュニティに属します。SNMP コミュニティによって、各 SNMP デバイスのアクセス権が決まります。SNMP ではコミュニティを使用して、マネージャとエージェント間の信頼関係を確立します。

コミュニティにはユーザが名前を指定します。その後は、そのコミュニティにメンバとして割り当てられたすべての SNMP デバイスに、同じアクセス権が与えられます（RFC 2576 で規定）。ACE では、このコミュニティに含まれるデバイスの MIB ツリーに対して、読み取り専用アクセスを許可します。読み取り専用コミュニティ ストリングを使用することによって、ユーザはデータ値を読み取ることができます。しかし、ユーザがデータを変更することはできません。

SNMP コミュニティ名およびアクセス権を作成したり変更したりするには、コンフィギュレーション モードで **snmp-server community** コマンドを使用します。

（注） SNMP コミュニティが適用されるのは、SNMPv1 および SNMPv2c だけです。SNMPv3 では、ユーザが所属するロール グループ、ユーザの認証パラメータ、認証パスワード、メッセージ暗号化パスワードを指定するなど、ユーザ設定情報が必要です（「SNMP ユーザの設定」を参照）。

注意 管理コンテキストまたはユーザ コンテキストに対応する SNMP エンジン ID を変更すると、設定されているすべての SNMP コミュニティが削除されます。その場合、コンフィギュレーション モードで **snmp-server community** コマンドを使用し、すべての SNMP コミュニティを再作成する必要があります。SNMPv3 エンジン ID の詳細については、「ACE コンテキストに対応する SNMPv3 エンジン ID の設定」を参照してください。

このコマンドの構文は、次のとおりです。

snmp-server community *community_name* [**group** *group_name* | **ro**]

キーワード、引数、およびオプションは次のとおりです。

- *community_name* — このシステムに対応する SNMP コミュニティ名。最大 32 文字の英数字からなる文字列を引用符で囲まずに入力します。スペースは使用しません。
- **group** *group_name* —（任意）ユーザが所属するロール グループを指定します。最大 32 文字の英数字からなる文字列を引用符で囲まずに入力します。スペースは使用しません。

（注） ACE の SNMP でサポートされるのは、ネットワーク モニタリング動作だけです。この場合、すべての SNMP ユーザに、システム定義のデフォルト グループ Network-Monitor が自動的に割り当てられます。ユーザ作成の詳細については、『*Cisco Application Control Engine Module Virtualization Configuration Guide*』を参照してください。

- **ro** —（任意）このコミュニティに読み取り専用アクセスを認めます。

たとえば、Network-Monitor グループのメンバとして SNMP_Community1 という SNMP コミュニティを指定し、読み取り専用アクセス権を与える場合は、次のように入力します。

```
host1/Admin(config)# snmp-server community SNMP_Community1 group
Network-Monitor
```

SNMP コミュニティを削除する場合は、次のように入力します。

```
host1/Admin(config)# no snmp-server community SNMP_Community1 group
Network-Monitor
```

SNMP コンタクトの設定

SNMP システムのコンタクト情報を指定するには、コンフィギュレーション モードで **snmp-server contact** コマンドを使用します。情報を指定できるのは、1 つのコンタクト名に限られます。このコマンドの構文は、次のとおりです。

snmp-server contact *contact_information*

スペースを含めて最大 240 文字の英数字からなる文字列として、*contact_information* 引数を入力します。文字列に複数の単語が含まれる場合は、文字列を引用符（“ ”）で囲みます。電話番号または E メール アドレスを指定するなど、担当者への連絡方法に関する情報を含めることができます。

SNMP システム コンタクト情報を指定する場合の入力例を示します。

```
host1/Admin(config-context)# snmp-server contact “User1
user1@cisco.com”
```

特定の SNMP コンタクト名を削除する場合は、次のように入力します。

```
host1/Admin(config)# no snmp-server contact
```

SNMP ロケーションの設定

SNMP システムのロケーションを指定するには、コンフィギュレーション モードで **snmp-server location** コマンドを使用します。指定できるロケーションは 1 つだけです。このコマンドの構文は、次のとおりです。

snmp-server location *location*

location はシステムの物理的な位置として入力します。スペースを含め、最大 240 文字の英数字からなる文字列を入力します。文字列に複数の単語が含まれる場合は、文字列を引用符（“ ”）で囲みます。

SNMP システム ロケーション情報を指定する場合の入力例を示します。

```
host1/Admin(config)# snmp-server location “Boxborough MA”
```

特定の SNMP システム ロケーション情報を削除する場合の入力例を示します。

```
host1/Admin(config)# no snmp-server location
```

SNMP 通知の設定

特定のイベントが発生した場合に、トラップまたは応答要求を通知として SNMP マネージャに送信するように ACE を設定できます。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、トラップは信頼性に欠ける場合があります。送信側では、トラップが受信されたかどうかを判断できません。しかし、応答要求を受信した SNMP マネージャは、SNMP 応答 PDU でメッセージの確認応答を行います。送信側が応答を受信しなかった場合は、通常、応答要求が再送信されます。応答要求は所定の宛先に届く可能性が高くなります。

（注） トラップまたは SNMP 応答要求として通知を送信する宛先の詳細情報を取得するには、SNMP-TARGET-MIB を使用します。詳細については、「サポート対象の MIB および通知」を参照してください。

ここで説明する内容は、次のとおりです。

- SNMP 通知ホストの設定
- SNMP 通知のイネーブル化
- SNMP linkUp および linkDown トラップに関する IETF 規格のイネーブル化

SNMP 通知ホストの設定

SNMP 通知を受信するホストを指定するには、コンフィギュレーション モードで **snmp-server host** コマンドを使用します。通知を送信するには、最低限 1 つは **snmp-server host** コマンドを設定する必要があります。

このコマンドの構文は、次のとおりです。

snmp-server host *host_address* {*community-string_username* | **informs** | **traps** | **version** {**1**{**udp-port**} | **2c** {**udp-port**} | **3** [**auth** | **noauth** | **priv**]}}

キーワード、引数、およびオプションは次のとおりです。

- *host_address* — ホスト（ターゲットとなる受信側）の IP アドレス。アドレスはドット付き 10 進 IP 表記（192.168.11.1 など）で入力します。

- *community-string_username* — 通知動作を指定した SNMP コミュニティ ストリングまたはユーザ名。最大 32 文字の英数字からなる文字列を引用符で囲まずに入力します。スペースは使用しません。
- **informs** — 指定されたホストに SNMP 応答要求を送信します。これにより、マネージャ相互間の通信が可能になります。応答要求は、ネットワークで複数の NMS が必要になった場合に有用です。
- **traps** — 指定されたホストに SNMP トラップを送信します。トラップはエージェントにとって、問題が発生したことを NMS に伝える手段です。トラップはエージェントで発生し、エージェント内部で設定されているトラップの宛先に送信されます。トラップの宛先は通常、NMS の IP アドレスです。
- **version** — トラップ送信に使用する SNMP のバージョンを指定します。SNMPv3 が最も安全性の高いモデルです。**priv** キーワードでパケットを暗号化できるからです。
- **1** — SNMPv1 を指定します。このオプションを SNMP 応答要求と組み合わせて使用することはできません。SNMPv1 には、使用するホストの UDP ポートを指定する、オプションのキーワード（**udp-port**）が 1 つあります。デフォルトは 162 です。
- **2c** — SNMPv2C を指定します。SNMPv2C には、使用するホストの UDP ポートを指定する、オプションのキーワード（**udp-port**）が 1 つあります。デフォルトは 162 です。
- **3** — SNMPv3 を指定します。SNMPv3 には 3 種類のオプション キーワードがあります（**auth**、**no auth**、または **priv**）。
- **auth** —（任意）MD5 および SHA によるパケット認証をイネーブルにします。
- **noauth** —（任意）noAuthNoPriv セキュリティ レベルを指定します。
- **priv** —（任意）DES（データ暗号規格）によるパケット暗号化（プライバシ）をイネーブルにします。

たとえば、SNMP 通知の受信側を指定する場合は、次のように入力します。

```
host1/Admin(config)# snmp-server host 192.168.1.1 traps version 2c
SNMP_Community1 udp-port 500
```

特定のホストを削除する場合は、このコマンドの **no** 形式を使用します。入力例を示します。

```
host1/Admin(config)# no snmp-server host 192.168.1.1 traps version 2c
SNMP_Community1 udp-port 500
```

SNMP 通知のイネーブル化

通知トラップおよび応答要求は、特定のイベントが発生したときに ACE が生成するシステム アラートです。SNMP 通知は、トラップまたは応答要求として NMS に送信できます。デフォルトでは、通知は定義されず、発行もされません。ACE が NMS に SNMP トラップおよび応答要求を送信できるようにするには、コンフィギュレーション モードで **snmp-server enable traps** コマンドを使用します。このコマンドによって、指定された通知タイプに関して、トラップと応答要求の両方がイネーブルになります。

SNMP 通知を送信するように ACE を設定するには、最低限 1 つは **snmp-server enable traps** コマンドを指定する必要があります。複数の通知タイプをイネーブルにするには、通知タイプおよび通知オプションごとに、**snmp-server enable traps** コマンドを別々に入力する必要があります。キーワードを指定しないでコマンドを入力した場合、ACE はすべての通知タイプおよびトラップをイネーブルにします。

snmp-server enable traps コマンドは **snmp-server host** コマンドと組み合わせて使用します（「SNMP 通知ホストの設定」を参照）。**snmp-server host** コマンドでは、SNMP 通知を受信するホストを指定します。通知を送信するには、最低限 1 つは SNMP サーバ ホストを設定する必要があります。

（注） **snmp-server enable traps** コマンドで使用した通知タイプには、必ず、グローバルに通知タイプをイネーブルまたはディセーブルにする MIB オブジェクトが対応付けられます。しかし、**snmp-server host** コマンドで使用できるすべての通知タイプに、notificationEnable MIB オブジェクトがあるわけではないので、通知タイプによっては、**snmp-server enable** コマンドでは制御できません。

このコマンドの構文は、次のとおりです。

snmp-server enable traps [*notification_type*] [*notification_option*]

キーワード、引数、およびオプションは次のとおりです。

- *notification_type* — （任意）イネーブルにする通知のタイプ。タイプを指定しなかった場合、ACE はすべての通知を送信します。*notification_type* として、次のキーワードのいずれか 1 つを指定します。

- **license** — SNMP ライセンス マネージャ通知を送信します。このキーワードが表示されるのは、管理コンテキストに限られます。
- **slb** — サーバ ロード バランシング通知を送信します。**slb** キーワードを指定する場合は、*notification_option* 値を指定できます。
- **snmp** — SNMP 通知を送信します。**snmp** キーワードを指定する場合は、*notification_option* 値を指定できます。
- **syslog** — エラー メッセージ通知（Cisco Syslog MIB）を送信します。**logging history level** コマンドで、送信するメッセージのレベルを指定します。

（注） NMS にトラップとしてシステム メッセージを送信できるようにする目的で、**logging history** コマンドを指定できます。**snmp-server enable traps** コマンドで、Syslog トラップをイネーブルにすることも必要です。詳細については、『*Cisco Application Control Engine Module System Message Guide*』を参照してください。

- **virtual-context** — 仮想コンテキスト（ACE ユーザ コンテキスト）変更通知を送信します。このキーワードが表示されるのは、管理コンテキストに限られます。

- *notification_option* —（任意）次の SNMP 通知の 1 つ。
  - **snmp** キーワードを指定した場合は、**authentication**、**coldstart**、**linkdown**、または **linkup** キーワードを指定して、SNMP 通知をイネーブルにします。この選択によって、SNMP 要求で指定されたコミュニティ ストリングが無効だった場合、または VLAN インターフェイスがアップまたはダウンのどちらかの場合に、通知が生成されます。**coldstart** キーワードが表示されるのは、管理コンテキストに限られます。
  - **slb** キーワードを指定した場合は、**real** または **vserver** キーワードを指定して、サーバ ロード バランシング通知をイネーブルにします。この選択によって、次のステート変化が発生した場合に、通知が生成されます。

    ユーザの介入、ARP 障害、またはプローブ障害が原因で、実サーバのステートが変化（アップまたはダウン）。

    仮想サーバのステートが変化（アップまたはダウン）。仮想サーバは外部に対して、ACE のコンテンツ スイッチの背後にあるサーバを代表し、次のアトリビュートからなります。宛先アドレス（IP アドレス範囲を使用可能）、プロトコル、宛先ポート、または着信 VLAN です。

たとえば、コミュニティ ストリング public を使用して、ACE から IP アドレス 192.168.1.1 のホストに、サーバ ロード バランシング トラップを送信できるようにする場合は、次のように入力します。

```
host1/Admin(config)# snmp-server host 192.168.1.1
host1/Admin(config)# snmp-server community SNMP_Community1 group
Network-Monitor
host1/Admin(config)# snmp-server enable traps slb real
```

SNMP サーバ通知をディセーブルにする場合は、このコマンドの **no** 形式を使用します。入力例を示します。

```
host1/Admin(config)# no snmp-server enable traps slb real
```

SNMP linkUp および linkDown トラップに関する IETF 規格のイネーブル化

ACE はデフォルトで、シスコの linkUp および linkDown トラップを NMS に送信します。ACE は Cisco Systems IF-MIB 変数バインディングを送信します。これは ifIndex、ifAdminStatus、ifOperStatus、ifName、ifType、clogOriginID、および clogOriginIDType で構成されます。IETF（インターネット技術特別調査委員会）規格に準拠した linkUp および linkDown トラップ（RFC 2863 で概要を規定）を送信するように、ACE を設定することもできます。**snmp-server trap link ietf** コンフィギュレーション モード コマンドで、ifIndex、ifAdminStatus、および ifOperStatus からなる IETF 規格の IF-MIB（RFC 2863）変数バインディングを使用して、linkUp および linkDown トラップを送信することを ACE に指示します。

（注） デフォルトではシスコの変数バインディングが送信されます。RFC 2863 に準拠したトラップを受信するには、**snmp-server trap link ietf** コマンドを指定する必要があります。

このコマンドの構文は、次のとおりです。

snmp-server trap link ietf

たとえば、RFC 2863 に準拠した linkUp および linkDown トラップを設定する場合は、次のように入力します。

```
host1/Admin(config)# snmp-server trap link ietf
```

シスコの linkUp および linkDown トラップに戻す場合は、次のように入力します。

```
host1/Admin(config)# no snmp-server trap link ietf
```

SNMPv1 トラップのトラップ送信元アドレスとしての VLAN インターフェイス割り当て

ACE はデフォルトで、ACE が通知を送信する宛先ホストのアドレスに応じて、内部ルーティング テーブルのトラップ送信元 IP アドレスを使用します。SNMPv1 トラップ PDU のトラップ送信元アドレスとして、VLAN 上で設定された IP アドレスを使用することを指定するには、コンフィギュレーション モードで **snmp-server trap-source vlan** コマンドを使用します。このコマンドの構文は、次のとおりです。

snmp-server trap-source vlan *number*

number 引数では、設定インターフェイスの VLAN 番号を指定します。既存の VLAN に対応する 2 ～ 4094 の値を入力します。

たとえば、SNMPv1 トラップ PDU の送信元アドレスとしての VLAN インターフェイスに VLAN 50 を指定する場合は、次のように入力します。

```
host1/Admin(config)# snmp-server trap-source vlan 50
```

SNMPv1 トラップ PDU の送信元アドレスとして指定された VLAN を削除し、デフォルトの動作にリセットする場合は、次のように入力します。

```
host1/Admin(config)# no snmp-server trap-source
```

（注） VLAN インターフェイスに有効な IP アドレスが与えられていなかった場合、SNMPv1 トラップ通知は失敗します。

管理コンテキストの IP アドレスから ACE ユーザ コンテキストのデータにアクセスする場合

ACE の管理コンテキストおよび各 ACE ユーザ コンテキストには、専用の IP アドレスがあります。SNMP エージェントはコンテキスト単位で、SNMPv1 および SNMPv2 の場合はコミュニティ ストリング、SNMPv3 の場合はユーザ名をサポートします。SNMP マネージャは、IP アドレスを使用してコンテキストに要求を送信し、そのコンテキストに対応するデータを取得できます。

管理コンテキストに対応する IP アドレスを使用して、ユーザ コンテキストに対応するデータを取得することもできます。管理コンテキストのクレデンシャルでも、パフォーマンス情報、設定情報などのユーザ コンテキスト データにアクセスできます。

（注） ユーザ コンテキスト用の通知を管理コンテキストから送信することはできません。

ここで説明する内容は、次のとおりです。

- SNMPv1/v2 使用時にユーザ コンテキスト データにアクセスする場合
- SNMPv3 使用時にユーザ コンテキスト データにアクセスする場合

SNMPv1/v2 使用時にユーザ コンテキスト データにアクセスする場合

SNMPv1/v2 の場合、ユーザ コンテキスト名とともに適切な SNMP バージョン、管理コンテキストの IP アドレス、および管理コンテキストのコミュニティ ストリングを指定することによって、SNMP マネージャは管理コンテキストの IP アドレスでユーザ コンテキスト用の MIB にアクセスできます。コミュニティ ストリングの形式は、次のとおりです。

admin_community_string@ACE_context_name

ACE_context_name は、任意の ACE ユーザ コンテキストにできます。コンテキスト名を指定しなかった場合は、管理コンテキストに対する要求になります。

たとえば、管理コンテキストにコミュニティ ストリング adminCommunity、IP アドレス 10.6.252.63 が設定されているときに、ユーザ コンテキスト C1 のデータを返す場合は、次のように入力します。

```
snmpget -v2c -c adminCommunity@C1 10.6.252.63 udpDatagrams.0
```

SNMPv3 使用時にユーザ コンテキスト データにアクセスする場合

SNMPv3 の場合、SNMPv3 パケットで管理コンテキストがサポートする管理コンテキストの IP アドレス、適切な SNMP バージョン、管理コンテキスト ユーザ名、およびユーザ コンテキスト名を使用することによって、SNMP マネージャは管理コンテキストの IP アドレスでユーザ コンテキストに対応する MIB にアクセスできます。ACE は、要求の SNMPv3 コンテキスト フィールドに指定されたユーザ コンテキスト名を使用します。

（注） SNMPv3 エンジンは、論理上独立した SNMP エージェントを表します。ACE はコンテキストごとに SNMP エンジン ID を作成しますが、ユーザが設定することもできます。SNMPv3 エンジン ID 設定の詳細については、「ACE コンテキストに対応する SNMPv3 エンジン ID の設定」を参照してください。

たとえば、管理コンテキストに SNMP ユーザ snmpuser、IP アドレス 10.6.252.63 が設定されているときに、ユーザ コンテキスト C2 のデータを返す場合は、次のように入力します。

```
snmpgetnext -v 3 - a MD5 -A cisco123 -u snmpuser -1 authNoPriv
10.6.252.63 system -n C2
```

ACE は、要求の SNMPv3 コンテキスト フィールドの変わりにユーザ コンテキスト C2 を使用します。

（注） SNMPv3 コンテキスト フィールドが空の文字列（“”）に設定されている場合に、ユーザ コンテキストの IP アドレスに要求を送信すると、SNMPv3 要求が廃棄されます。

ACE コンテキストに対応する SNMPv3 エンジン ID の設定

ACE はデフォルトで、管理コンテキストおよび各ユーザ コンテキストの SNMP エンジン ID を自動的に作成します。SNMP エンジンは、論理上独立した SNMP エージェントを表します。ACE コンテキストの IP アドレスでアクセスできるのは、1 つの SNMP エンジン ID だけです。

注意　管理コンテキストまたはユーザ コンテキストに対応する SNMP エンジン ID を変更すると、設定されているすべての SNMP ユーザが無効になり、すべての SNMP コミュニティが削除されます。その場合、コンフィギュレーション モードで **snmp-server user** コマンドを使用して、すべての SNMP ユーザを再作成するとともに、コンフィギュレーション モードで **snmp-server community** コマンドを使用して、すべての SNMP コミュニティを再作成しなければなりません。

ACE の場合、管理コンテキストまたはユーザ コンテキストに対応する SNMP エンジン ID をユーザ側で設定できます。ACE コンテキスト用の SNMP エンジン ID を設定するには、コンテキストに対応するコンフィギュレーション モードで **snmp-server engineid** コマンドを使用します。このコマンドの構文は、次のとおりです。

snmp-server engineid *number*

number 引数は、設定する SNMPv3 エンジン ID です。10 ～ 64 の 16 進数を入力します。

たとえば、管理コンテキスト用のエンジン ID として 884395734985738888843957349857388 を入力する場合は、次のように入力します。

```
host1/Admin(config)# snmp-server engineID
884395734985738888843957349857388
```

管理コンテキストのエンジン ID をデフォルトにリセットする場合は、次のように入力します。

```
host1/Admin(config)# no snmp-server engineID
```

コンテキストのエンジン ID を表示するには、コンテキストに対応する EXEC モードでで **show snmp engineID** コマンドを使用します。たとえば、管理コンテキスト用のエンジン ID を表示する場合は、次のように入力します。

```
host1/Admin# show snmp engineID
```

SNMP 管理トラフィック サービスの設定

クラス マップ、ポリシー マップ、およびサービス ポリシーを使用して、ACE との間で送受信する SNMP 管理トラフィックを設定できます。ACE へのリモート ネットワーク管理アクセスを設定するうえで、各機能が果たす役割を簡単に説明します。

- クラス マップ — SNMP 管理プロトコルおよびクライアント送信元 IP アドレスに基づいて、SNMP 管理トラフィックを許可するリモート ネットワーク トラフィック一致条件を指定します。
- ポリシー マップ — クラス マップで指定された条件と一致するトラフィック分類に対して、リモート ネットワーク管理アクセスを可能にします。
- サービス ポリシー — ポリシー マップをアクティブにして、VLAN インターフェイスにトラフィック ポリシーを接続するか、またはすべての VLAN インターフェイス上でグローバルに接続します。

ACE との SNMP リモート アクセス セッションは、コンテキストに基づいて確立されます。コンテキストおよびユーザ作成の詳細については、『*Cisco Application Control Engine Module Virtualization Configuration Guide*』を参照してください。

ここで説明する内容は、次のとおりです。

レイヤ 3 およびレイヤ 4 クラス マップの作成および設定

ACE で受信できる SNMP 管理トラフィックを分類するために、レイヤ 3 およびレイヤ 4 クラス マップを作成するには、コンフィギュレーション モードで **class-map type management** コマンドを使用します。このコマンドで ACE が受信できる着信 IP プロトコル、さらにクライアント送信元ホストの IP アドレスおよびサブネット マスクを一致条件として指定することによって、ACE でネットワーク管理トラフィックを受信できるようになります。**type management** というクラス マップでは、SNMP などのプロトコル管理セキュリティの形で、許可するネットワーク トラフィックを定義します。

クラス マップには複数の **match** コマンドを指定できます。クラス マップを設定すると、複数の SNMP 管理プロトコルおよび送信元 IP アドレス コマンドをグループとして定義し、さらにトラフィック ポリシーと関連付けることができます。**match-all** および **match-any** キーワードによって、クラス マップに複数の一致条件が存在する場合に、ACE が複数の match 文演算をどのように評価するかが決まります。

このコマンドの構文は、次のとおりです。

class-map type management [**match-all** | **match-any**] *map_name*

キーワード、引数、およびオプションは次のとおりです。

- **match-all** | **match-any** — （任意）クラス マップに複数の一致条件が存在する場合に、ACE がレイヤ 3 およびレイヤ 4 ネットワーク トラフィックをどのように評価するかを決定します。クラス マップは、**match** コマンドが次の条件の 1 つを満たした場合に、一致とみなされます。
  - **match-all** — （デフォルト）クラス マップで指定されているすべての一致条件がクラス マップのネットワーク トラフィック クラスと一致した場合（通常、同じタイプの **match** コマンド）。
  - **match-any** — クラス マップで指定されている一致条件の 1 つがクラス マップのネットワーク トラフィック クラスと一致した場合（通常、タイプの異なる **match** コマンド）。
- *map_name* — クラス マップに割り当てる名前。最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。スペースは使用しません。

class-map type management コマンドを使用するときには、クラス マップ管理コンフィギュレーション モードにアクセスします。このモードを使用すると、クラス マップの説明または一致条件を設定できます。

たとえば、ACE と IP アドレス 192.168.1.1 255.255.255.0 のホスト間で SNMP アクセスを許可する場合は、次のように入力します。

```
host1/Admin(config)# class-map type management match-all
SNMP-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# match protocol snmp source-address
192.168.1.1 255.255.255.0
host1/Admin(config-cmap-mgmt)# exit
```

ACE からレイヤ 3 およびレイヤ 4 SNMP プロトコル管理クラス マップを削除する場合は、次のように入力します。

```
host1/Admin(config)# no class-map type management match-all
SNMP-ALLOW_CLASS
```

クラス マップの説明を指定する場合は、「クラス マップの説明の定義」を参照してください。

ACE が受信したリモート SNMP プロトコル管理トラフィックを分類するには、1 つまたは複数の関連コマンドを組み込み、**match protocol** コマンドを使用して、クラス マップの一致条件を設定します。このコマンドの詳細については、「SNMP プロトコル一致条件の定義」を参照してください。

クラス マップの説明の定義

レイヤ 3 およびレイヤ 4 リモート管理クラス マップの概要を指定するには、クラス マップ管理コンフィギュレーション モードで **description** コマンドを使用します。

このコマンドの構文は、次のとおりです。

description *text*

text 引数は、指定する説明です。最大 240 文字の英数字からなる文字列を引用符で囲まずに入力します。

たとえば、SNMP アクセスを許可するクラス マップであるという説明を指定する場合は、次のように入力します。

```
host1/Admin(config)# class-map type management SNMP-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# description Allow SNMP access
```

クラス マップから説明を削除する場合は、次のように入力します。

```
host1/Admin(config-cmap-mgmt)# no description
```

SNMP プロトコル一致条件の定義

ACE および NMS で SNMP を受信できることを指定するためにクラス マップを設定するには、クラス マップ管理コンフィギュレーション モードで **match protocol snmp** コマンドを使用します。対応するポリシー マップを設定し、ACE への SNMP アクセスを許可します。ネットワーク管理アクセス トラフィック分

類の一部として、クライアント送信元ホストの IP アドレスおよびサブネット マスクも一致条件として指定するか、またはあらゆるクライアント送信元アドレスを管理トラフィック分類で許可するように ACE に指示します。

このコマンドの構文は、次のとおりです。

[*line_number*] **match protocol snmp** {**any** | **source-address** *ip_address mask*}

キーワード、引数、およびオプションは次のとおりです。

- *line_number* — （任意）個々の **match** コマンドを識別する行番号。編集または削除時に役立ちます。2 ～ 255 の整数を入力します。長い **match** コマンドを削除するときには、行全体を入力する代わりに、**no** *line_number* を入力できます。行番号は、match 文のプライオリティまたは順序を示すものではありません。
- **any** — 管理トラフィック分類にあらゆるクライアント送信元アドレスを指定します。
- **source-address** — ネットワーク トラフィック一致条件として、クライアント送信元ホストの IP アドレスおよびサブネット マスクを指定します。分類の一部として、ACE は暗黙で、ポリシー マップが適用されるインターフェイスから宛先 IP アドレスを取得します。
- *ip_address* — クライアントの送信元 IP アドレス。IP アドレスはドット付き 10 進表記（192.168.11.1 など）で入力します。
- *mask* — ドット付き 10 進表記（255.255.255.0 など）で指定したクライアントのサブネット マスク。

たとえば、クラス マップで、送信元アドレス 192.168.10.1 255.255.255.0 から ACE への SNMP アクセスを許可することを指定する場合は、次のように入力します。

```
host1/Admin(config)# class-map type management SNMP-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# match protocol snmp source-address
192.168.10.1 255.255.255.0
```

クラス マップから特定の SNMP プロトコル一致条件を選択解除する場合は、次のように入力します。

```
host1/Admin(config-cmap-mgmt)# no match protocol snmp
```

レイヤ 3 およびレイヤ 4 ポリシー マップの作成

レイヤ 3 およびレイヤ 4 ポリシー マップでは、指定された分類と一致した SNMP ネットワーク管理トラフィックに対して実行するアクションを定義します。ここで説明する内容は、次のとおりです。

- ACE で受信する SNMP ネットワーク管理トラフィック用レイヤ 3 およびレイヤ 4 ポリシー マップの作成
- トラフィック ポリシーでのレイヤ 3 およびレイヤ 4 トラフィック クラスの指定
- レイヤ 3 およびレイヤ 4 ポリシー アクションの指定

ACE で受信する SNMP ネットワーク管理トラフィック用レイヤ 3 およびレイヤ 4 ポリシー マップの作成

SNMP 管理プロトコルの受信を ACE に許可するレイヤ 3 およびレイヤ 4 ポリシー マップを設定するには、コンフィギュレーション モードで **policy-map type management** コマンドを使用します。ACE は、最初に一致した分類に対してアクションを実行します。ACE は、それ以上のアクションは実行しません。

このコマンドの構文は、次のとおりです。

policy-map type management first-match *map_name*

map_name 引数では、レイヤ 3 およびレイヤ 4 ネットワーク管理ポリシー マップに割り当てる名前を指定します。最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。スペースは使用しません。

このコマンドを使用するときには、ポリシー マップ管理コンフィギュレーション モードにアクセスします。

レイヤ 3 およびレイヤ 4 ネットワーク トラフィック管理ポリシー マップを作成する場合の入力例を示します。

```
host1/Admin(config) # policy-map type management first-match
SNMP-ALLOW_POLICY
host1/Admin(config-pmap-mgmt) #
```

ACE からネットワーク トラフィック管理ポリシー マップを削除する場合は、次のように入力します。

```
host1/Admin(config)# no policy-map type management first-match
SNMP-ALLOW_POLICY
```

トラフィック ポリシーでのレイヤ 3 およびレイヤ 4 トラフィック クラスの指定

class-map コマンドでレイヤ 3 およびレイヤ 4 トラフィック クラスを作成し、ネットワーク トラフィックとトラフィック ポリシーを関連付けることを指定するには、**class** コマンドを使用します。このコマンドによって、ポリシー マップ管理クラス コンフィギュレーション モードが開始されます。

このコマンドの構文は、次のとおりです。

class {*name1* [**insert-before** *name2*] | **class-default**}

引数キーワードおよびオプションは次のとおりです。

- *name1* — **class-map** コマンドで設定された、トラフィックとトラフィック ポリシーを関連付ける、定義済みのレイヤ 3 およびレイヤ 4 トラフィック クラスの名前。最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。スペースは使用しません。
- **insert-before** *name2* — （任意）ポリシー マップ コンフィギュレーションの *name2* 引数で指定された、既存のクラス マップまたはインライン一致条件の前に、現在のクラス マップを配置します。ACE では、コンフィギュレーションの一部として順序の並べ替えを保存しません。最大 64 文字の英数字からなる文字列を引用符で囲まずに入力します。スペースは使用しません。
- **class-default** — レイヤ 3 およびレイヤ 4 トラフィック ポリシー用に、class-default クラス マップを指定します。これは、ACE が作成する予約済みのクラス マップです。このクラスを削除したり変更したりすることはできません。指定されたクラス マップの他の一致条件と一致しなかったすべてのネットワーク トラフィックは、デフォルトのトラフィック クラスに割り当てられます。指定された分類がいずれも一致しなかった場合、ACE は **class class-default** コマンドで指定されたアクションと一致させます。class-default クラス マップには、暗黙の **match any** 文があり、これを使用してあらゆるトラフィック分類を一致させます。

たとえば、レイヤ 3 およびレイヤ 4 リモート アクセス ポリシー マップ内で既存のクラス マップを指定する場合は、次のように入力します。

```
host1/Admin(config-pmap-mgmt)# class SNMP-ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)#
```

insert-before コマンドを使用して、ポリシー マップ内での 2 つのクラス マップの順序を定義する場合は、次のように入力します。

```
host1/Admin(config-pmap-mgmt)# class L4_SSH_CLASS insert-before
L4_REMOTE_ACCESS_CLASS
```

レイヤ 3 およびレイヤ 4 トラフィック ポリシーに class-default クラス マップを指定する場合は、次のように入力します。

```
host1/Admin(config-pmap-mgmt)# class class-default
host1/Admin(config-pmap-mgmt-c)#
```

レイヤ 3 およびレイヤ 4 ポリシー マップからクラス マップを削除する場合は、次のように入力します。

```
host1/Admin(config-pmap-mgmt)# no class SNMP-ALLOW_CLASS
```

レイヤ 3 およびレイヤ 4 ポリシー アクションの指定

レイヤ 3 およびレイヤ 4 クラス マップで指定されているネットワーク管理トラフィックを ACE が受信または拒否できるようにするには、次のように、ポリシー マップ クラス コンフィギュレーション モードで **permit** または **deny** コマンドのどちらかを指定します。

- クラス マップで指定されている SNMP 管理プロトコルを ACE に受信させる場合は、ポリシー マップ クラス コンフィギュレーション モードで **permit** コマンドを使用します。
- クラス マップで指定されている SNMP 管理プロトコルの受信を ACE に拒否させる場合は、ポリシー マップ クラス コンフィギュレーション モードで **deny** コマンドを使用します。

レイヤ 3 およびレイヤ 4 ポリシー マップに許可アクションを指定する場合の入力例を示します。

```
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
```

サービス ポリシーの適用

service-policy コマンドを使用すると、次の作業を実行できます。

- 作成済みのポリシー マップを適用します。
- 特定の VLAN インターフェイスにトラフィック ポリシーを接続するか、または同じコンテキスト内のすべての VLAN インターフェイスにグローバルに接続します。
- インターフェイスの入力方向にトラフィック　ポリシーを接続することを指定します。

service-policy コマンドは、コンフィギュレーション モードとインターフェイス コンフィギュレーション モードの両方で使用できます。インターフェイス コンフィギュレーション モードでポリシー マップを指定すると、特定の VLAN インターフェイスにポリシー マップが適用されます。コンフィギュレーション モードでポリシー マップを指定すると、コンテキストに関連付けられているすべての VLAN インターフェイスにポリシーが適用されます。

このコマンドの構文は、次のとおりです。

service-policy input *policy_name*

キーワードおよび引数は次のとおりです。

- **input** — インターフェイスの入力方向にトラフィック　ポリシーを接続することを指定します。トラフィック ポリシーによって、そのインターフェイスで受信されたすべてのトラフィックが評価されます。
- *policy_name* — 作成済みの **policy-map** コマンドで設定された、定義済みポリシー マップの名前。名前は最大 40 文字の英数字です。

たとえば、インターフェイス VLAN を指定して、VLAN に SNMP 管理ポリシー マップを適用する場合は、次のように入力します。

```
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ip address 172.20.1.100 255.255.0.0
host1/Admin(config-if)# service-policy input SNMP_MGMT_ALLOW_POLICY
```

たとえば、コンテキストに関連付けられたすべての VLAN に、SNMP 管理ポリシー マップをグローバルに適用する場合は、次のように入力します。

```
host1/Admin(config)# service-policy input SNMP_MGMT_ALLOW_POLICY
```

インターフェイス VLAN から SNMP 管理ポリシーを切り離す場合は、次のように入力します。

```
host1/Admin(config-if)# no service-policy input SNMP_MGMT_ALLOW_POLICY
```

コンテキストに対応付けられたすべての VLAN から SNMP 管理ポリシーをグローバルに切り離す場合は、次のように入力します。

```
host1/Admin(config)# no service-policy input SNMP_MGMT_ALLOW_POLICY
```

トラフィック ポリシーは、次のいずれかの方法で切り離すことができます。

- サービス ポリシーを最後に適用した VLAN インターフェイスから個別に
- 同じコンテキストのすべての VLAN インターフェイスからグローバルに

ポリシーを切り離すと、ACE は関連するサービス ポリシー統計情報を自動的にリセットし、次回、特定の VLAN インターフェイスに、または同じコンテキストのすべての VLAN インターフェイスにグローバルに、トラフィック ポリシーを接続したときの、サービス ポリシー統計情報の新しい出発点を用意します。

サービス ポリシー作成時の注意事項および制約事項は、次のとおりです。

- コンテキストでグローバルに適用されるポリシー　マップは、コンテキスト内に存在するすべてのインターフェイスに内部的に適用されます。
- インターフェイス上でアクティブになったポリシーは、重複する分類およびアクションに関して、指定されているあらゆるグローバル ポリシーを上書きします。
- ACE　では、インターフェイス上でアクティブにできるのは、特定機能タイプの 1 つのポリシーだけです。

レイヤ 3 およびレイヤ 4 SNMP 管理ポリシー マップのサービス ポリシー統計情報を表示するには、EXEC モードで **show service-policy** コマンドを使用します。

このコマンドの構文は、次のとおりです。

show service-policy *policy_name* [**detail**]

（注） ACE は、該当する接続の終了後、**show service-policy** コマンドによって表示されるカウンタをアップデートします。

キーワード、オプション、および引数は次のとおりです。

- *policy_name* — 現在使用中の（インターフェイスに適用されている）既存ポリシー マップの ID。最大 64 文字の英数字からなる、引用符で囲まれていない文字列です。
- **detail** —（任意）より詳細なポリシー マップ統計およびステータス情報を表示します。

たとえば、SNMP_MGMT_ALLOW_POLICY ポリシー マップのサービス ポリシー統計情報を表示する場合は、次のように入力します。

```
host1/Admin# show service-policy SNMP_MGMT_ALLOW_POLICY
Status     : ACTIVE
Description: Allow mgmt protocols
----------------------------------------
Context Global Policy:
  service-policy: SNMP_MGMT_ALLOW_POLICY
```

サービス ポリシー統計情報を消去するには、**clear service-policy** コマンドを使用します。このコマンドの構文は、次のとおりです。

clear service-policy *policy_name*

policy_name 引数には、現在使用中の（インターフェイスに適用されている）既存ポリシー マップの ID を入力します。

たとえば、現在使用中であるポリシー マップ SNMP_MGMT_ALLOW_POLICY の統計情報を消去する場合は、次のように入力します。

```
host1/Admin# clear service-policy SNMP_MGMT_ALLOW_POLICY
```

SNMP の設定例

次に、SNMP および CLI を使用して、実サーバの現在のステータスを確認する実行コンフィギュレーションの例を示します。このコンフィギュレーションでは、実サーバまたは仮想サーバが動作していないときに、SNMP トラップが送信されたかどうかも確認します。この例から、ACE に接続できるクライアント送信元ホストの IP アドレスを制限できることがわかります。ポリシー マップは、コンテキストに関連付けられているすべての VLAN インターフェイスに適用されます。SNMP の設定部分は、太字で示します。

```
access-list ACL1 line 10 extended permit ip any any

rserver host SERVER1
  ip address 192.168.252.245
  inservice
rserver host SERVER2
  ip address 192.168.252.246
  inservice
rserver host SERVER3
  ip address 192.168.252.247
  inservice

serverfarm host SFARM1
  probe HTTP_PROBE
  rserver SERVER1
    conn-limit max 3 min 2
    inservice
serverfarm host SFARM2
  probe HTTP
  rserver SERVER2
    conn-limit max 500 min 2
    inservice
  rserver SERVER3
    conn-limit max 500 min 2
    inservice

class-map type http loadbalance match-all L7_INDEX-HTML_CLASS
  2 match http url /index.html
class-map match-all L4_MAX-CONN-VIP_105_CLASS
  2 match virtual-address 192.168.120.105 any
class-map type management match-any L4_REMOTE-ACCESS-LOCAL_CLASS
  description Enables SNMP remote management for local users
  1 match protocol snmp source-address 192.168.0.0 255.248.0.0
  2 match protocol snmp source-address 172.16.64.0 255.255.252.0
class-map type http loadbalance match-all L7_URL*_CLASS
  2 match http url .*
```

```
policy-map type management first-match L4_SNMP-REMOTE-MGT_POLICY
  class L4_REMOTE-ACCESS-LOCAL_CLASS
    permit
policy-map type loadbalance first-match L7_LB-SF_MAX-CONN_POLICY
  class L7_INDEX-HTML_CLASS
    serverfarm SFARM1
  class L7_URL*_CLASS
    serverfarm SFARM2
policy-map multi-match L4_VIP_POLICY
  class L4_MAX-CONN-VIP_105_CLASS
    loadbalance vip inservice
    loadbalance policy L7_LB-SF_MAX-CONN_POLICY
    loadbalance vip icmp-reply
    appl-parameter http advanced-options PERSIST-REBALANCE

service-policy input L4_REMOTE-MGT_POLICY

snmp-server user user1 Network-Monitor auth sha "adcd1234"
snmp-server community ACE-public group ro
snmp-server contact "User1 user1@cisco.com"
snmp-server location "San Jose CA"
snmp-server host 192.168.0.236 traps version 2c ACE-public
snmp-server enable traps slb vserver
snmp-server enable traps slb real
snmp-server enable traps syslog
snmp-server enable traps snmp authentication
snmp-server enable traps snmp linkup
snmp-server enable traps snmp linkdown
```

SNMP 統計情報の表示

SNMP の統計情報および設定されている SNMP の情報を表示するには、EXEC モードで **show snmp** コマンドを使用します。デフォルトでは、ACE コンタクト、ACE ロケーション、パケット トラフィック情報、コミュニティ ストリング、およびユーザ情報が表示されます。適切なキーワードを指定することによって、特定の SNMP 情報を表示するように ACE に指示できます。

このコマンドの構文は、次のとおりです。

show snmp [community | engineID | group | host | sessions | user]

キーワードは次のとおりです。

- **community** — （任意）SNMP コミュニティ ストリングを表示します。
- **engineID** — （任意）ACE 上で設定されているローカル SNMP エンジンおよびすべてのリモート エンジンの識別情報を表示します。
- **group** — （任意）ACE 上で設定されているグループの名前、セキュリティ モデル、各種ビューのステータス、および各グループのストレージ タイプを表示します。
- **host** — （オプション）設定されている SNMP 通知の受信ホスト、UDP ポート番号、ユーザ、およびセキュリティ モデルを表示します。
- **sessions** —（任意）トラップまたは応答要求が送信されたターゲットの IP アドレスを表示します。
- **user** — （任意）SNMPv3 ユーザ情報を表示します。

表 7-5 で、**show snmp community** コマンドの出力に含まれる各フィールドについて説明します。

表 7-5　show snmp コマンド出力のフィールド

フィールド	説明
Sys contact	SNMP システムのコンタクト名
Sys location	SNMP システムのロケーション
SNMP packets input	ACE が受信した SNMP パケットの総数
Bad SNMP versions	SNMP バージョンが無効なパケットの数
Unknown community name	未知のコミュニティ名が指定された SNMP パケットの数

表 7-5　show snmp コマンド出力のフィールド（続き）

フィールド	説明
Illegal operation for community name supplied	そのコミュニティには許可されていない動作を要求したパケットの数
Encoding errors	符号化が無効な SNMP パケットの数
Number of requested variables	SNMP マネージャが要求した変数の数
Number of altered variables	SNMP マネージャが変更した変数の数
Get-request PDUs	受信した get 要求の数
Get-next PDUs	受信した get-next 要求の数
Set-request PDUs	受信した set 要求の数
SNMP packets output	ACE が送信した SNMP パケットの総数
Too big errors	最大パケット サイズを超えていた SNMP パケットの数
No such name errors	存在しない MIB オブジェクトが指定されていた SNMP 要求の数
Bad values errors	MIB オブジェクトに無効な値が指定されていた SNMP set 要求の数
General errors	noSuchName エラー、badValue エラー、他の特定のエラーなど、その他のエラーが原因で失敗した SNMP set 要求の数
Community	ACE の SNMP コミュニティ名
Group/Access	コミュニティのアクセス権、読み取り専用
User	SNMP ユーザの名前を特定する文字列
Auth	暗号化を使用しないパケット認証
Priv	暗号化を使用するパケット認証
Group	ユーザが所属するユーザ ロール グループ

表 7-6 で、**show snmp community** コマンドの出力に含まれる各フィールドについて説明します。

表 7-6　show snmp community コマンド出力のフィールド

フィールド	説明
Community	ACE の SNMP コミュニティ名
Group/Access	コミュニティのアクセス権、読み取り専用

表 7-7 で、**show snmp engineID** コマンドの出力に含まれるフィールドについて説明します。

表 7-7　show snmp engineID コマンド出力のフィールド

フィールド	説明
Local SNMP engineID	ACE 上のローカル SNMP エンジンの識別番号

表 7-8 で、**show snmp group** コマンドの出力に含まれる各フィールドについて説明します。

表 7-8　show snmp group コマンド出力のフィールド

フィールド	説明
Group name	共通アクセス ポリシーを使用する SNMP グループまたはユーザ コレクションの名前
Security model	グループが使用するセキュリティ モデル（v1、v2c、または v3）
Security level	グループが使用するセキュリティ レベル
Read view	グループの読み取りビューを特定する文字列
Write view	グループの書き込みビューを特定する文字列
Notify view	グループの通知ビューを特定する文字列

表 7-8　show snmp group コマンド出力のフィールド（続き）

フィールド	説明
Storage-type	設定値がデバイスの揮発性すなわち一時的なメモリに保管されているのか、それともデバイスの電源を切断し、再投入したあとでも有効な不揮発性すなわち永久メモリに保管されているのかを示すステータス
Row status	SNMP グループの Row ステータスがアクティブなのか非アクティブなのか

表 7-9 で、**show snmp host** コマンドの出力に含まれる各フィールドについて説明します。

表 7-9　show snmp host コマンド出力のフィールド

フィールド	説明
Host	ターゲット ホストの IP アドレス
Port	通知の送信先となる UDP ポート番号
Version	トラップ送信に使用する SNMP のバージョン（v1、v2c、または v3）
Level	認証およびプライバシの方式
Type	設定されている通知のタイプ
SecName	ターゲット ホストのスキャン用セキュリティ名

表 7-10 で、**show snmp sessions** コマンドの出力に含まれる各フィールドについて説明します。

表 7-10　show snmp sessions コマンド出力のフィールド

フィールド	説明
Destination	トラップまたは応答要求が送信されたターゲットの IP アドレス

表 7-11 で、**show snmp user** コマンドの出力に含まれる各フィールドについて説明します。

表 7-11　show snmp user コマンド出力のフィールド

フィールド	説明
User	SNMP ユーザの名前を特定する文字列
Auth	暗号化を使用しないパケット認証
Priv	暗号化を使用するパケット認証
Group	ユーザが所属するユーザ ロール グループ