CHAPTER 7

簡易ネットワーク管理プロトコル（SNMP）の設定

この章では、Cisco 4700 Series Application Control Engine（ACE）アプライアンスに 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 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。

この章の内容は、次のとおりです。

SNMP に関する情報

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、認証にコミュニティ ストリング照合が使用されます。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、認証に SNMP ユーザが使用され、強力な認証を使用した高度なアクセス コントロールが可能になります。可能なかぎり、SNMPv1 や SNMPv2c ではなく SNMPv3 を使用してください。

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 では、次のセキュリティ機能が提供されます。

- 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 コンテンツにスクランブルをかけて、権限のない送信元で解読できないようにします。

ここでは、次の内容について説明します。

マネージャとエージェント

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を通して送信されたバイト数のカウントなど、特定の機能だけを制御します。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 マネージャと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、次の操作を実行できます。
  - エージェントから値を取得（**get** 操作）。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** 操作）。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 Object IDentifier（OID; オブジェクト ID）= 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** 操作）。**get-next** 操作では、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** 操作を実行すれば、探している 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、指定された変数を取得して、順次検索で必要な変数を検索します。
- 一連の値を取得（**get-bulk** 操作）。get-bulk 操作では、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 ブロックを伝送する必要があります。SNMP マネージャは、指定した一連の **get-next** 操作を実行します。

- 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** 操作による情報収集）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 と通知」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。応答要求は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、デバイスを一意に識別する clogOriginID と clogOriginIDType の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 4700 Series Application Control Engine Appliance 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 と通知」を参照してください。

SNMPv3 の CLI ユーザ管理と 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、Authentication, Authorization, and Accounting（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 4700 Series Application Control Engine Appliance Security Configuration Guide*』を参照してください）。この集中型ユーザ管理によって、ACE の SNMP エージェントが AAA サーバのユーザ認証サービスを利用できるようになります。

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 グループ名の保存にも使用されます。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。

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 内で同期されます。

（注） セキュリティ暗号化用のローカライズしたキーまたは暗号化形式でパスワードを指定した場合は、パスワードが同期されません。

- **username** コマンドで指定したパスワードは、SNMP ユーザ用の **auth** および **priv** パスワードとして同期されます。
- 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。

username コマンドを使用した CLI ユーザの作成方法については、『*Cisco 4700 Series Application Control Engine Appliance 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。

複数ストリング インデックスに関するガイドライン

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存在している場合は、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 標準によれば、SNMP 要求、応答、またはトラップに対して、128 を超えるサブ ID の使用はできません。次にオブジェクト名を示します。

- 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 7-1 に、複数ストリング インデックスを使用可能なテーブルの一覧を示します。

表 7-1　複数ストリング 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、 cslbxServerFarmProbeTableName
CISCO-SLB-HEALTH-MON-MIB.my	cshMonServerfarmRealProbeStatsTable	cslbxProbeName、 slbServerFarmName、 cshMonServerfarmRealServerName

サポート対象の MIB と通知

表 7-2 に、ACE のサポート対象 MIB を示します。

表 7-2　SNMP MIB サポート

MIB サポート	機能 MIB	説明
アプライアンス MIB		
CISCO-ENTITY-VENDORTYPE-OID-MIB	該当なし	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 値のリストを表示します。 **製品名（PID）/entPhysicalVendorType** **ACE4710-K9** cevChassisACE4710K9 {cevChassis 610} **電源モジュール** cevPowerSupplyAC345 {cevPowerSupply 190} **CPU ファン** cevFanACE4710K9CpuFan {cevFan 91} **DIMM ファン** cevFanACE4710K9DimmFan {cevFan 92} **PCI ファン** cevFanACE4710K9PciFan {cevFan 93}

表 7-2　SNMP MIB サポート （続き）

MIB サポート	機能 MIB	説明
CISCO-ENTITY-VENDORTYPE-OID-MIB *（続き）*	該当なし	**製品名（PID）/entPhysicalVendorType** **電圧センサー** cevSensorPSOutput {cevSensor 39} **CPU ファン センサー** cevSensorCpuFanSpeed {cevSensor 58} **DIMM ファン センサー** cevSensorACE4710K9DimmFanSpeed {cevSensor 59} **PCI ファン センサー** cevSensorACE4710K9PciFanSpeed {cevSensor 60} **CPU 温度センサー** cevSensorACE4710K9 CPUTemp {cevSensor 56} **周囲温度センサー** cevSensorACE4710K9 AmbientTemp {cevSensor 57}
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、ACE アプライアンス シャーシ内部の各モジュール、電源、ファン、およびセンサーに関する詳細を提供します。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す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 7-2　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 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.my	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。
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 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。これらの 2 つのタイプの情報間で、MIB の多対多関係が可能になります。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 7-2　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 キー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。
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 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 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 7-2　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	デバイス内部の AAA サーバ動作および外部サーバとの AAA 通信のステートを反映した設定情報と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-APPLICATION ACCELERATION-MIB	CISCO-APPLICATION-ACCELERATION-CAPABILITY-MIB	ACE 内のアプリケーション アクセラレーション システムを管理します。この MIB には、パフォーマンス統計情報とアプリケーション アクセラレーション システムのコアであるコンデンサのステータスを提供する器具類が含まれます。コンデンサは、複数の最適化技術を適用して Web アプリケーション アクセスを高速化するソフトウェア アクセラレータです。
CISCO-ENHANCED-SLB-MIB	CISCO-ENHANCED-SLB-CAPABILITY	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 • 実サーバの現在のステート（OPERATIONAL、OUT-OF-SERVICE、PROBE-FAILED など） • サーバ ファーム内の実サーバ設定 • 実サーバおよびサーバ ファームのヘルス プローブ設定 • 各実サーバのヘルス プローブ統計情報 • 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。スロット番号値は ACE アプライアンスには適用されないので、slbEntity Index の値は常に 1 になります。 CISCO-ENHANCED-SLB-MIB の cesRServerProbeTable テーブルは、**show probe detail** コマンド出力に表示される実サーバ プローブ統計情報に関する詳細を提供します。 CISCO-ENHANCED-SLB-MIB の cesServerFarmRserverTable および cesRserverTable テーブルは、**show rserver** コマンド出力に表示されるデータに関する詳細を提供します。

表 7-2　SNMP MIB サポート （続き）

MIB サポート	機能 MIB	説明
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。 **（注）** イーサネット データ ポート、イーサネット管理ポート、およびポートチャネル インターフェイスは、管理コンテキストでしか使用できません。この場合、CISCO-IF-EXTENSION-MIB は管理コンテキストのすべてのインターフェイスをサポートし、各ユーザ コンテキストは VLAN および BVI インターフェイスのみをサポートします。
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。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。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。 cippfIpFilterHits は、アクセス コントロール エントリのヒット カウントの合計を提供します。 IP プロトコルは RFC 791 で規定されています。
CISCO-L4L7MODULE-REDUNDANCY-MIB	CISCO-L4L7MODULE-REDUNDANCY-CAPABILITY	アクティブおよびスタンバイの ACE アプライアンス間の冗長性（または耐障害性）を反映した設定情報テーブルと統計情報テーブルを提供します。各ピア アプライアンスは、1 つまたは複数の耐障害性（FT）グループで構成されます。 CISCO-L4L7MODULE-REDUNDANCY-MIB は、FT ステート、IP アドレス、ピア FT ステート、ピア IP アドレス、ソフトウェアの互換性、ライセンスの互換性、ピアが属するグループの数、および送受信されたハートビート メッセージの数などの冗長構成情報を提供します。 CISCO-L4L7MODULE-REDUNDANCY-MIB は、**show ft peer**、**show ft group detail**、および **show ft stats** コマンド出力に表示される耐障害性の統計情報に関する詳細を提供します。

表 7-2　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。 CISCO-L4L7RESOURCE-LIMIT-MIB の ciscoL4L7ResourceLimitTable、ciscoL4L7ResourceRateLimitTable、および ciscoL4L7ResourceUsageSummaryTable は、**show resource usage** コマンド出力に表示される Current、Peak、および Denied の統計情報に関する詳細を提供します。
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。仮想コンテキストは、物理デバイス（ACE）の論理パーティションです。仮想コンテキストは、別々に管理可能な各種サービス タイプを提供します。各仮想コンテキストは、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、Secure Shell（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、仮想コンテキストを作成または削除できます。また、仮想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。
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。 システム プロセス情報は、コンテキスト別ではなく、CPU システム レベル（CPU 使用状況の合計値）で表示されます。
CISCO-PRODUCTS-MIB	該当なし	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** ACE4710-K9 ciscoACE4710K9 {ciscoProducts 824}

表 7-2　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。 CISCO-SLB-MIB の slbVServerInfoTable テーブルは、**show service-policy** コマンド出力に表示されるデータに関する詳細を提供します。 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 アプライアンス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-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。 CISCO-SLB-EXT-MIB の cslbxServerFarmStatsTable テーブルは、**show serverfarm** コマンド出力に表示されるデータに関する詳細を提供します。 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 サーバ ファームは、非アクティブ ステートからアクティブ ステートに、または、アクティブ ステートから非アクティブ ステートに変更できます。アクティブ ステートから非アクティブ ステートに変更する理由は次のとおりです。 • すべての実サーバがダウンしている。 • 1 台以上の実サーバが最大接続ステートまたは最大負荷ステートに到達したか、プローブ障害または ARP 障害が発生したために、1 つのサーバ ファーム内のすべての実サーバが稼動していない。 • サーバ ファームが部分的に限界に達している。

表 7-2　SNMP MIB サポート （続き）

MIB サポート	機能 MIB	説明
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。ACE のヘルス プローブ コンフィギュレーションおよび統計情報のテーブルを提供します。 CISCO-SLB-HEALTH-MON-MIB の cshMonSfarmRealProbeStatsTable および cslbxProbeCfgTable テーブルは、**show probe detail** コマンド出力に表示されるプローブ データに関する詳細を提供します。
CISCO-SSL-PROXY-MIB	CISCO-SSL-PROXY-CAPABILITY	SSL および Transport Layer Security（TLS）トランザクションを終了および加速する SSL プロキシ デバイスを管理します。プロキシ デバイスは、コンフィギュレーションおよびアプリケーションに応じて、SSL サーバまたは SSL クライアントとして動作できます。 この MIB は、プロキシ サービスおよび TCP、SSL、および TLS を含むプロトコルの統計情報を監視するのに使用されます。
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。
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。 **（注）** イーサネット データ ポート、イーサネット管理ポート、およびポートチャネル インターフェイスは、管理コンテキストでしか使用できません。この場合、IF-MIB は管理コンテキストのすべてのインターフェイスをサポートし、各ユーザ コンテキストは VLAN および BVI インターフェイスのみをサポートします。
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。

表 7-2　SNMP MIB サポート （続き）

MIB サポート	機能 MIB	説明
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。
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 7-3 に、ACE で使用される MIB ごとにサポートされている / サポートされていないテーブルとオブジェクトを示します。

表 7-3　MIB テーブルとオブジェクトのサポート

MIB 名	サポートされているテーブルとオブジェクト	サポートされていないテーブルとオブジェクト
SNMPv2-MIB	スカラ オブジェクト： sysDescr sysName sysLocation sysContact sysObjectID sysServices sysORLastChange snmpInPkts snmpOutPkts snmpInBadVersions snmpInBadCommunityNames snmpInBadCommunityUses snmpInASNParseErrs snmpInTooBigs snmpInNoSuchNames snmpInBadValues snmpInReadOnlys snmpInGenErrs snmpInTotalReqVars snmpInTotalSetVars snmpInGetRequests snmpInGetNexts	すべてのテーブルとオブジェクトがサポートされています。

表 7-3　MIB テーブルとオブジェクトのサポート （続き）

MIB 名	サポートされているテーブルとオブジェクト	サポートされていないテーブルとオブジェクト
SNMPv2-MIB *（続き）*	snmpInSetRequests snmpInGetResponses snmpInTraps snmpOutTooBigs snmpOutNoSuchNames snmpOutBadValues snmpOutGenErrs snmpOutGetRequests snmpOutGetNexts snmpOutSetRequests snmpOutGetResponses snmpOutTraps snmpEnableAuthenTraps snmpSilentDrops snmpProxyDrops テーブル： sysORTable	
SNMP-COMMUNITY-MIB	テーブル： snmpCommunityTable snmpTargetAddrExtTable	すべてのテーブルとオブジェクトがサポートされています。
SNMP-MPD-MIB	スカラ オブジェクト： snmpUnknownSecurityModels snmpInvalidMsgs snmpUnknownPDUHandlers	すべてのテーブルとオブジェクトがサポートされています。
SNMP-NOTIFICATION-MIB	テーブル： snmpNotifyTable snmpNotifyFilterProfileTable snmpNotifyFilterTable	すべてのテーブルとオブジェクトがサポートされています。
SNMP-TARGET-MIB	スカラ オブジェクト： snmpUnavailableContexts snmpUnknownContexts テーブル： snmpTargetAddrTable snmpTargetParamsTable	スカラ オブジェクト： snmpTargetSpinLock

表 7-3　MIB テーブルとオブジェクトのサポート （続き）

MIB 名	サポートされているテーブルとオブジェクト	サポートされていないテーブルとオブジェクト
SNMP-USER-BASED-SM-MIB	スカラ オブジェクト： usmStatsUnsupportedSecLevels usmStatsNotInTimeWindows usmStatsUnknownUserNames usmStatsUnknownEngineIDs usmStatsWrongDigests usmStatsDecryptionErrors テーブル： usmUserTable	スカラ オブジェクト： usmUserSpinLock
SNMP-VIEW-BASED-ACM-MIB	テーブル： vacmContextTable vacmSecurityToGroupTable vacmAccessTable	スカラ オブジェクト： vacmViewSpinLock
ENTITY-MIB	テーブル： entPhysicalTable	テーブル： entLogicalTable entLPMappingTable entAliasMappingTable entPhysicalContainsTable オブジェクト： entPhysicalAlias entPhysicalAssetID entPhysicalMfgDate
ENTITY-SENSOR-MIB	entPhySensorTable	すべてのテーブルとオブジェクトがサポートされています。
IF-MIB	スカラ オブジェクト： ifNumber ifTableLastChange テーブル： ifTable ifXTable	テーブル： ifStackTable ifRcvAddressTable ifTestTable オブジェクト： ifStackLastChange

表 7-3　MIB テーブルとオブジェクトのサポート （続き）

MIB 名	サポートされているテーブルとオブジェクト	サポートされていないテーブルとオブジェクト
IP-MIB	スカラ オブジェクト： icmpInMsgs icmpInErrors icmpInDestUnreachs icmpInTimeExcds icmpInParmProbs icmpInSrcQuenchs icmpInRedirects icmpInEchos icmpInEchoReps icmpInTimestamps icmpInTimestampReps icmpInAddrMasks icmpInAddrMaskRepsicmp OutMsg icmpOutErrors icmpOutDestUnreachs icmpOutTimeExcds icmpOutParmProbs icmpOutSrcQuenchs icmpOutRedirects icmpOutEchos icmpOutEchoReps icmpOutTimestamps icmpOutTimestampReps icmpOutAddrMasks icmpOutAddrMaskReps	テーブル： ipNetToMediaTable ipv4InterfaceTable ipv6InterfaceTable ipAddressTable ipAddressPrefixTable ipNetToPhysicalTable ipDefaultRouterTable ipv6RouterAdvertTable ipv6ScopeZoneIndexTable オブジェクト： ipSystemStatsInMcastOctets ipSystemStatsHCInMcastOctet ipSystemStatsOutMcastOctets ipSystemStatsHCOutMcastOctets ipIfStatsInMcastOctets ipIfStatsHCInMcastOctets ipIfStatsOutMcastOctets ipIfStatsHCOutMcastOctets
IP-MIB	テーブル： ipAddrTable ipSystemStatsTable ipIfStatsTable icmpStatsTable icmpMsgStatsTable	

表 7-3　MIB テーブルとオブジェクトのサポート （続き）

MIB 名	サポートされているテーブルとオブジェクト	サポートされていないテーブルとオブジェクト
TCP-MIB	スカラ オブジェクト： tcpRtoAlgorithm tcpRtoMin tcpRtoMax tcpMaxConn tcpActiveOpens tcpPassiveOpens tcpAttemptFails tcpEstabResets tcpCurrEstab tcpInSegs tcpOutSegs tcpRetransSegs tcpInErrs tcpOutRsts	スカラ オブジェクト： tcpHCInSegs tcpHCOutSegs テーブル： tcpConnTable tcpConnectionTable tcpListenerTable
UDP-MIB	スカラ オブジェクト： udpInDatagrams udpNoPorts udpInErrors udpOutDatagrams	スカラ オブジェクト： udpHCInDatagrams udpHCOutDatagrams テーブル： udpTable udpEndpointTable
CISCO-PROCESS-MIB	テーブル： cpmProcessTable cpmCPUTotalTable cpmProcessExtRevTable	テーブル： cpmProcessExtTable cpmCPUThresholdTable cpmCPUHistoryTable cpmCPUProcessHistoryTable スカラ オブジェクト： cpmCPUHistoryThreshold cpmCPUHistorySize オブジェクト： cpmCPUInterruptMonIntervalValue

表 7-3　MIB テーブルとオブジェクトのサポート （続き）

MIB 名	サポートされているテーブルとオブジェクト	サポートされていないテーブルとオブジェクト
CISCO-SYSLOG-EXT-MIB	スカラ オブジェクト： cseSyslogConsoleEnable cseSyslogConsoleMsgSeverity cseSyslogServerTableMaxEntries cseSyslogTerminalEnable cseSyslogTerminalMsgSeverity テーブル： cseSyslogServerTable	スカラ オブジェクト： cseSyslogLogFileName cseSyslogLogFileMsgSeverity cseSyslogFileLoggingDisable cseSyslogLinecardEnable cseSyslogLinecardMsgSeverity テーブル： cseSyslogMessageControlTable
CISCO-SYSLOG-MIB	スカラ オブジェクト： clogNotificationsSent clogNotificationsEnabled clogMaxSeverity clogMsgIgnores clogMsgDrops clogOriginIDType clogOriginID clogHistTableMaxLength clogHistMsgsFlushed テーブル： clogHistoryTable	スカラ オブジェクト： clogMaxservers テーブル： clogServerConfigTable
CISCO-SYSTEM-MIB	スカラ オブジェクト： csyClockDateAndTime csyClockLostOnReboot csyLocationCountry	スカラ オブジェクト： csySummerTimeStatus csySummerTimeOffset csySummerTimeRecurringStart csySummerTimeRecurringEnd csyScheduledResetTime csyScheduledResetAction csyScheduledResetReason csySnmpAuthFail csySnmpAuthFailAddressType csySnmpAuthFailAddress csyNotificationsEnable

表 7-3　MIB テーブルとオブジェクトのサポート （続き）

MIB 名	サポートされているテーブルとオブジェクト	サポートされていないテーブルとオブジェクト
CISCO-SLB-MIB	スカラ オブジェクト： cSlbVServerStateChangeNotifEnabled テーブル： slbStatsTable slbServerFarmTable slbVServerInfoTable	スカラ オブジェクト： cSlbVirtStateChangeNotifEnabled cSlbRealStateChangeNotifEnabled cSlbRealServerStateChangeNotifEnabled テーブル： slbRealTable slbVirtualServerTable slbVServerTable slbConnectionTable slbVirtualClientTable slbStickyObjectTable slbDfpPasswordTable slbDfpAgentTable slbDfpRealTable slbSaspTable slbSaspAgentTable slbSaspGroupTable slbSaspMemberTable slbSaspStatsTable
CISCO-SLB-MIB		**slbStatsTable** でサポートされていないオブジェクト： slbStatsUnassistedSwitchingPkts slbStatsUnassistedSwitchingHCPks slbStatsAssistedSwitchingPkts slbStatsAssistedSwitchingHCPkts slbStatsZombies slbStatsHCZombies **slbServerFarmTable** でサポートされていないオブジェクト： slbServerFarmPredictor slbServerFarmNat slbServerFarmBindId **slbVServerInfoTable** でサポートされていないオブジェクト： slbVServerL4Decisions slbVServerL7Decisions slbVServerEstablishedConnections

表 7-3　MIB テーブルとオブジェクトのサポート （続き）

MIB 名	サポートされているテーブルとオブジェクト	サポートされていないテーブルとオブジェクト
CISCO-SLB-EXT-MIB	テーブル： cslbxStatsTable cslbxServerFarmTable cslbxServerFarmProbeTable cslbxServerFarmStatsTable	テーブル： cslbxConnTable cslbxRedirectSvrTable cslbxSfarmHttpReturnCodeTable cslbxNatPoolTable cslbxStickyGroupTable cslbxStickyObjectTable cslbxStickyGroupExtTable cslbxMapTable cslbxHttpExpressionTable cslbxHttpReturnCodeTable cslbxPolicyTable cslbxVirtualServerTable cslbxRuleTable cslbxVlanTable cslbxAliasAddrTable cslbxStaticRouteTable cslbxFtTable cslbxXmlConfigTable cslbxOwnerTable cslbxScriptFileTable cslbxScriptTaskTable

表 7-3　MIB テーブルとオブジェクトのサポート （続き）

MIB 名	サポートされているテーブルとオブジェクト	サポートされていないテーブルとオブジェクト
CISCO-SLB-EXT-MIB *（続き）*		**cslbxStatsTable** でサポートされていないオブジェクト： cslbxStatsServerInitConns cslbxStatsServerInitHCConns cslbxStatsCurrServerInitConns cslbxStatsFailedServerInitConns cslbxStatsNoActiveServerRejects **cslbxServerFarmTable** でサポートされていないオブジェクト： cslbxServerFarmClientNatPool cslbxServerFarmHttpReturnCodeMap **cslbxServerFarmStatsTable** でサポートされていないオブジェクト： cslbxServerFarmNumOfTimeFailOvers cslbxServerFarmNumOfTimeBkInServs

表 7-3　MIB テーブルとオブジェクトのサポート （続き）

MIB 名	サポートされているテーブルとオブジェクト	サポートされていないテーブルとオブジェクト
CISCO-SLB-HEALTH-MON-MIB	テーブル： cslbxProbeCfgTable cslbxProbeHeaderCfgTable cslbxProbeHTTPCfgTable cslbxProbeFTPCfgTable cslbxProbeIMAPCfgTable cshMonServerfarmRealProbe StatsTable	cslbxDnsProbeIpTable cslbxProbeSIPCfgTable cslbxProbeTFTPCfgTable cslbxProbeExpectStatusCfgTable cshMonProbeTypeStatsTable **cslbxProbeCfgTable** でサポートされていないオブジェクト： cslbxProbePassword cslbxProbeSocketReuse cslbxProbeSendDataType cslbxProbePriority **cslbxProbeHTTPCfgTable** でサポートされていないオブジェクト： cslbxProbeHTTPCfgPersistence **cshMonServerfarmRealProbeLastProbeTime** でサポートされていないオブジェクト： cshMonServerfarmRealProbeLast ActiveTime cshMonServerfarmRealProbeLast FailedTime cshMonProbeInheritedPortType
CISCO-ENHANCED-SLB-MIB	スカラ オブジェクト： cesRealServerNotifEnable テーブル： cesRserverTable cesServerFarmRserverTable cesRserverProbeTable	**cesServerFarmRserverTable** でサポートされていないオブジェクト： cesServerFarmRserverDroppedConns テーブル： cesRealServerProbeTable

表 7-3　MIB テーブルとオブジェクトのサポート （続き）

MIB 名	サポートされているテーブルとオブジェクト	サポートされていないテーブルとオブジェクト
CISCO-IF-EXTENSION-MIB	テーブル： cieIfNameMappingTable	テーブル： cieIfPacketStatsTable cieIfInterfaceTable cieIfStatusListTable cieIfDot1qCustomEtherTypeTable cieIfUtilTable cieIfDot1dBaseMappingTable
CISCO-IP-PROTOCOL-FILTER-MIB	テーブル： cippfIpProfileTable cippfIpFilterTable cippfIpFilterStatsTable	テーブル： cippfIfIpProfileTable cippfIpFilterExtTable **cippfIpFilterTable** でサポートされていないオブジェクト： cippfIpFilterSrcIPGroupName cippfIpFilterDstIPGroupName cippfIpFilterProtocolGroupName cippfIpFilterSrcServiceGroupName cippfIpFilterDstServiceGroupName cippfIpFilterICMPGroupName
CISCO-MODULE-VIRTUALIZATION-MIB	スカラ オブジェクト： cmVirtContextNotifEnable テーブル： cmVirtualContextTable cmVirtContextIfMapTable	**cmVirtualContextTable** でサポートされていないオブジェクト： cmVirtContextURL
CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB	テーブル： ciscoL4L7ResourceClassTable ciscoL4L7ResourceLimitTable ciscoL4L7ResourceRateLimitTable ciscoL4L7ResourceUsage SummaryTable	スカラ オブジェクト： clrResourceLimitReachedNotifEnabled clrResourceRateLimitReachedNotifEnabled

表 7-3　MIB テーブルとオブジェクトのサポート （続き）

MIB 名	サポートされているテーブルとオブジェクト	サポートされていないテーブルとオブジェクト
CISCO-AAA-SERVER-MIB	テーブル： casConfigTable	スカラ オブジェクト： casServerStateChangeEnable テーブル： casStatisticsTable **casConfigTable** でサポートされていないオブジェクト： casPriority
CISCO-AAA-SERVER-EXT-MIB	スカラ オブジェクト： cAAASvrExtSvrGrpSvrListMaxEnt cAAASvrExtAppToSvrGrpMaxEnt cAAASvrExtClearAccLog cAAALoginAuthTypeMSCHAP テーブル： cAAASvrExtConfigTable cAAASvrExtProtocolParamTable cAAASvrExtSvrGrpConfigTable cAAASvrExtSvrGrpLDAPConfig テーブル cAAASvrExtAppSvrGrpConfig テーブル	スカラ オブジェクト： cAAASvrExtLocalAccLogMaxSize **cAAASvrExtConfigTable** でサポートされていないオブジェクト： cAAAServerDeadTime cAAAServerIdleTime cAAAServerTestUser cAAAServerTestPassword

表 7-3　MIB テーブルとオブジェクトのサポート （続き）

MIB 名	サポートされているテーブルとオブジェクト	サポートされていないテーブルとオブジェクト
CISCO-LICENSE-MGR-MIB	スカラ オブジェクト： clmNotificationsEnable clmNoOfLicenseFilesInstalled clmNoOfLicensedFeatures clmLicenseViolationWarnFlag テーブル： clmLicenseFileContentsTable clmLicenseFeatureUsageTable clmFeatureUsageDetailsTable	スカラ オブジェクト： clmHostId clmLicenseConfigSpinLock clmLicenseFileURI clmLicenseFileTargetName clmLicenseConfigCommand clmLicenseRequestCommandStatus clmLicenseRequestSpinLock clmLicenseRequestFeatureName clmLicenseRequestAppName clmLicenseRequestCommand clmLicenseRequestCommandStatus **clmLicenseFeatureUsageTable** でサポートされていないオブジェクト： clmLicenseGracePeriod clmLicenseEnabled
CISCO-APPLICATION-ACCELERATION-MIB	テーブル： caaStatTable	**caaStatTable** でサポートされていないオブジェクト： caaState caaRequests caaLastRestartedTime caaRequestSize

表 7-3　MIB テーブルとオブジェクトのサポート （続き）

MIB 名	サポートされているテーブルとオブジェクト	サポートされていないテーブルとオブジェクト
CISCO-L4L7MODULE-REDUNDANCY-MIB	テーブル： clrRedundancyInfoTable clrPeerInfoTable clrHAStatsTable	スカラ オブジェクト： clrStateChangeNotifEnabled テーブル： clrRedundancyConfigTable clrPeerConfigTable clrLBStatsTable **clrRedundancyInfoTable** でサポートされていないオブジェクト： clrRedundancyPriority clrRedundancyStateChangeTime clrHAStatsTable でサポートされていないオブジェクト： clrHAStatsMissedHeartBeatMsgs clrHAStatsRxUniDirectionalHeartBeatMsgs clrHAStatsHeartBeatTimeout Mismatches clrHAStatsPeerUpEvents clrHAStatsPeerDownEvents
CISCO-SSL-PROXY-MIB	スカラ オブジェクト： cspTlcFullHandShake cspTlcResumedHandShake cspS3cFullHandShake cspS3cResumedHandShake cspTlcHandShakeFailed cspTlcDataFailed cspS3cHandShakeFailed cspS3cDataFailed cspScActiveSessions cspScConnInHandShake cspScConnInDataPhase cspScConnInReneg	残りのすべてのテーブルとオブジェクトはサポートされていません。

表 7-4 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 7-4 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 7-4　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。
cesRealServerStateUpRev1	CISCO-ENHANCED-SLB-MIB	サーバ ファーム内で構成された実サーバのステートは、ユーザ介入によって稼動中です。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。 • cesRealServerName • cesServerFarmRserverBackupPort • cesServerFarmName • cesServerFarmRserverAdminStatus • cesServerFarmRserverOperStatus • cesRserverIpAddressType • cesRserverIpAddress • cesServerFarmRserverDescr
cesRealServerStateDownRev1	CISCO-ENHANCED-SLB-MIB	サーバ ファーム内で構成された実サーバのステートは、ユーザ介入によって非稼動中です。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。 • cesRealServerName • cesServerFarmRserverBackupPort • cesServerFarmName • cesServerFarmRserverAdminStatus • cesServerFarmRserverOperStatus • cesServerFarmRserverStateDescr • cesRserverIpAddressType • cesRserverIpAddress • cesServerFarmRserverDescr

表 7-4　SNMP トラップ サポート （続き）

通知名	通知の保管場所	説明
cesRealServerStateChangeRev1	CISCO-ENHANCED-SLB-MIB	サーバ ファーム内で構成された実サーバのステートは、ユーザ介入以外のイベントによって、新しいステートに変化しました。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。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。 • cesRealServerName • cesServerFarmRserverBackupPort • cesServerFarmName • cesServerFarmRserverAdminStatus • cesServerFarmRserverOperStatus • cesServerFarmRserverStateDescr • cesRserverIpAddressType • cesRserverIpAddress • cesProbeName • cesServerFarmRserverDescr
cesRserverStateUp	CISCO-ENHANCED-SLB-MIB	グローバル実サーバのステートは、ユーザ介入によって稼動中です。 （注）　この実サーバをリッスンしている実サーバごとに異なる cesRealServerStateUpRev1 通知は送信されません。
cesRserverStateDown	CISCO-ENHANCED-SLB-MIB	グローバル実サーバのステートは、ユーザ介入によって非稼動中です。 （注）　この実サーバをリッスンしている実サーバごとに異なる cesRealServerStateDownRev1 通知は送信されません。
cesRserverStateChange	CISCO-ENHANCED-SLB-MIB	グローバル実サーバのステートは、ユーザ介入以外のイベントによって、新しいステートに変化しました。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）　この実サーバをリッスンしている実サーバごとに異なる cesRealServerStateChangeRev1 通知は送信されません。

表 7-4　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	仮想サーバのステートが変化しました。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 仮想サーバのステートが変化する理由は、インターフェイスへのバインディング、ポリシーからのアクティブ サーバ ファームの削除、Virtual IP Address（VIP; 仮想 IP アドレス）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。
ciscoSlbVServerStateChange	CISCO-SLB-MIB.my	VIP がクラス マップから削除されたことを示す通知。この通知は、仮想サーバのステートが変化した場合にも送信されます。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 ciscoSlbVServerVIPStateChange 通知は、VIP アドレスの設定または関連付けが変化したときに送信されます 。 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。
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。
clmLicenseExpiryWarningNotify	CISCO-LICENSE-MGR-MIB	システムで、インストール済みの機能ライセンスの有効期限がもうすぐ切れることが検出されたことを示す通知。
clmNoLicenseForFeature Notify	CISCO-LICENSE-MGR-MIB	システムで、特定の機能の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ことを示す通知。
cmVirtContextAdded, cmVirtContextRemoved	CISCO-MODULE-VIRTUALIZATION-MIB	仮想コンテキストとも呼ばれる ACE ユーザ コンテキストが作成または削除されたことを示す通知。

表 7-4　SNMP トラップ サポート （続き）

通知名	通知の保管場所	説明
cslbxServerFarmStateChange	CISCO-SLB-EXT-MIB	サーバ ファーム内のすべての実サーバがダウンして、サーバ ファームのステートが変化したことを示す通知。この変数バインディングには、次の詳細が含まれています。 • cslbxServerFarmName • cslbxServerFarmState • cslbxServerFarmStateChangeDescr • cslbxServerFarmNumOfTimeFailOvers • cslbxServerFarmNumOfTimeBkInServs
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。 （注）　イーサネット データ ポート、イーサネット管理ポート、およびポートチャネル インターフェイスは、管理コンテキストでしか使用できません。この場合、linkUp および linkDown 通知は管理コンテキストのすべてのインターフェイスをサポートし、各ユーザ コンテキストは VLAN および BVI インターフェイスのみをサポートします。

SNMP のデフォルト設定

表 7-5 に、SNMP パラメータのデフォルト設定の一覧を示します。

表 7-5　デフォルト SNMP パラメータ

パラメータ	デフォルト
SNMP 通知	どの通知も定義または発行されていません。
linkUp トラップと linkDown トラップの実装	NMS に対する linkUp トラップと linkDown トラップのシスコ実装がイネーブルになっています（Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）標準ベースの実装ではありません）。
管理コンテキストおよびユーザ コンテキストごとの SNMP エンジン ID	エンジン ID は、ACE によって自動的に作成されます。
SNMP-COMMUNITY-MIB の snmpCommunityName OID と snmpCommunitySecurityName OID	これらの OID はデフォルトでマスクされています。

簡易ネットワーク管理プロトコル（SNMP）の設定

ここでは、SNMP の設定方法について説明します。内容は次のとおりです。

SNMP を設定するためのタスク フロー

ACE 上で SNMP を設定するには、次の手順を実行します。

ステップ 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、適切なコンテキストで動作しているかどうかを確認してください。必要に応じて、適切なコンテキストに直接ログインするか、または切り替えてください。

```
host1/Admin# changeto C1
host1/C1#
```

この手順内の残りの例では、特に指定がなければ、管理コンテキストが使用されます。コンテキスト作成の詳細については、『*Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*』を参照してください。

ステップ 2　設定モードに入ります。

```
host1/Admin# config
Enter configuration commands, one per line. End with CNTL/Z
host1/Admin(config)#
```

ステップ 3　ACE 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
```

ステップ 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
```

ステップ 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"
```

ステップ 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"
```

ステップ 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
```

ステップ 8　ACE から NMS に SNMP トラップと応答要求を送信できるようにします。

```
host1/Admin(config)# snmp-server enable traps slb
```

ステップ 9　SNMP 管理プロトコルとクライアント送信元 IP アドレスに基づいて、ACE によるネットワーク管理トラフィックの受信を許可するクラス 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)#
```

ステップ 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)#
```

ステップ 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
```

ステップ 12　（オプション）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

ここでは、ACE CLI から SNMP ユーザを設定する方法について説明します。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。

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 コンテキストの SNMP エンジン ID を変更すると、設定済みのすべての SNMP ユーザが無効になります。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 コンテキストの SNMPv3 エンジン ID の設定」を参照してください。

制約事項

このテーマには、次のような制約があります。

- ACE は、コンテキストごとに最大 28 人の SNMP ユーザをサポートします。
- **snmp-server user** コマンドを通したユーザ設定が適用できるのは SNMPv3 だけです。SNMPv1 と 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が認証されます（「SNMP コミュニティの定義」を参照）。

詳細手順

	コマンド	目的
ステップ 1	**config** **例：** host1/host1/Admin# config host1/Admin(config)#	グローバル コンフィギュレーション モードに入ります。
ステップ 2	**snmp-server user** *user_name* [*group_name*] [**auth** {**md5** | **sha**} *password1* [**localizedkey** | **priv** {*password2* | **aes-128** *password2*}]] **例：** host1/Admin(config)# snmp-server user joe Network-Monitor auth sha abcd1234	SNMP ユーザ情報を設定します。 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、引用符で囲まれていない、スペースを含まないテキスト文字列を入力します。 • *group_name*：（オプション）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、引用符で囲まれていない、スペースを含まないテキスト文字列を入力します。SNMP のアクセス権は、グループ別に編成されます。SNMP のグループは、CLI 上で設定されるロールに似ています。*groupname* は、**role configuration mode** コマンドで定義します。詳細は、『*Cisco 4700 Series Application Control Engine Appliance 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 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*』を参照してください。 • **auth**：（オプション）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 Message Digest 5（MD5）暗号化アルゴリズムを指定します。 • **sha**：ユーザ認証に HMAC Secure Hash Algorithm（SHA）暗号化アルゴリズムを指定します。

コマンド	目的
snmp-server user *user_name* [*group_name*] [**auth** {**md5** | **sha**} *password1* [**localizedkey** | **priv** {*password2* | **aes-128** *password2*}]] (continued)	• *password1*：ユーザ認証パスワード。最大 130 文字の英数字からなる、引用符で囲まれていない、スペースを含まないテキスト文字列を入力します。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。ACE は、パスワードで次の特殊文字をサポートしています。 , ./ = + - ^ @ !% ~ # $ * ( ) ACE は、実行コンフィギュレーションでクリア テキスト形式のパスワードを暗号化します。 • **localizedkey**：（オプション）パスワードがセキュリティ暗号化用のローカライズされたキー形式であることを示します。 • **priv :**（オプション）ユーザの暗号化パラメータを指定します。**priv** オプションと **aes-128** オプションは、このプライバシ パスワードが 128 ビット AES キーを生成するためのものであることを示します。 • **aes-128**：プライバシ用の 128 バイト 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。ローカライズしたキー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。ACE は、パスワードで次の特殊文字をサポートしています。 , ./ = + - ^ @ !% ~ # $ * ( ) ACE は、実行コンフィギュレーションでクリア テキスト形式のパスワードを暗号化します。
no snmp-server user *user_name* [*group_name*] [**auth** {**md5** | **sha**} *password1* [**localizedkey** | **priv** {*password2* | **aes-128** *password2*}]] **例：** host1/Admin(config)# no snmp-server user joe Network-Monitor auth sha abcd1234	（オプション）SNMP ユーザ設定をディセーブルにするか、SNMP ユーザを削除します。
ステップ 3　**do copy running-config startup-config** **例：** host1/Admin(config)# do copy running-config startup-config	（オプション）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

下の例は、SNMP ユーザ情報の設定方法を示しています。

```
host1/Admin# config
Enter configuration commands, one per line. End with CNTL/Z
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 コミュニティの定義

ここでは、SNMP コミュニティの名前とアクセス権の作成または変更方法について説明します。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れます。しかし、ユーザによるデータの変更はできません。

注意　管理コンテキストまたはユーザ コンテキストの SNMP エンジン ID を変更すると、設定済みのすべての SNMP コミュニティが削除されます。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 コンテキストの SNMPv3 エンジン ID の設定」を参照してください。

制約事項

このテーマには、次のような制約があります。

- SNMP コミュニティが適用できるのは、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）。
- 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 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*』を参照してください。

詳細手順

	コマンド	目的
ステップ 1	**config** **例：** host1/Admin# config host1/Admin(config)#	グローバル コンフィギュレーション モードに入ります。

	コマンド	目的
ステップ 2	**snmp-server community** *community_name* [**group** *group_name* | **ro**] **例：** host1/Admin(config)# snmp-server community SNMP_Community1 group Network-Monitor	SNMP コミュニティの名前とアクセス権を作成または変更します。 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*：このシステムの SNMP コミュニティ名。最大 32 文字の英数字からなる、引用符で囲まれていない、スペースを含まないテキスト文字列を入力します。 • **group** *group_name*：（オプション）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、引用符で囲まれていない、スペースを含まないテキスト文字列を入力します。 • **ro**：（オプション）このコミュニティに対する読み取り専用アクセスを許可します。
	no snmp-server community *community_name* [**group** *group_name* | **ro**] **例：** host1/Admin(config)# no snmp-server community SNMP_Community1 group Network-Monitor	（オプション）SNMP コミュニティを削除します。
ステップ 3	**do copy running-config startup-config** **例：** host1/Admin(config)# do copy running-config startup-config	（オプション）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

SNMP コンタクトの設定

ここでは、SNMP システムに関するコンタクト情報の指定方法について説明します。

制約事項

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。

詳細手順

	コマンド	目的
ステップ 1	**config** **例：** host1/Admin# config host1/Admin(config)#	グローバル コンフィギュレーション モードに入ります。
ステップ 2	**snmp-server contact** *contact_information* **例：** host1/Admin(config)# snmp-server contact "User1 user1@cisco.com"	SNMP システムに関するコンタクト情報を指定します。 スペースを含めて最大 240 文字の英数字からなるテキスト文字列として、*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。電話番号や E メール アドレスなど、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。

	コマンド	目的
	no snmp-server contact **例：** host1/Admin(config)# snmp-server contact	（オプション）SNMP コンタクト名を削除します。
ステップ 3	**do copy running-config startup-config** **例：** host1/Admin(config)# do copy running-config startup-config	（オプション）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

SNMP ロケーションの設定

ここでは、SNMP システム ロケーションの指定方法について説明します。

制約事項

指定できるロケーションは 1 つだけです。

詳細手順

	コマンド	目的
ステップ 1	**config** **例：** host1/Admin# config host1/Admin(config)#	グローバル コンフィギュレーション モードに入ります。
ステップ 2	**snmp-server location** *location* **例：** host1/Admin(config)# snmp-server location “Boxborough MA”	SNMP システム ロケーションを指定します。 システムの物理的な場所として、*location* 引数を入力します。スペースを含め、最大 240 文字の英数字からなるテキスト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。
	no snmp-server location **例：** host1/Admin(config)# no snmp-server location	SNMP システム ロケーション情報を削除します。
ステップ 3	**do copy running-config startup-config** **例：** host1/Admin(config)# do copy running-config startup-config	（オプション）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

SNMP 通知の設定

ここでは、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 SNMP マネージャに通知として送信するように ACE を設定する方法について説明します。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。

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 と通知」を参照してください。

ここでは、次の内容について説明します。

- 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 標準のイネーブル化

SNMP 通知ホストの設定

ここでは、SNMP 通知を受信するホストの指定方法について説明します。

制約事項

このテーマには、次のような制約があります。

- 通知を送信するには、SNMP 通知を受信する 1 つ以上のホストを指定する必要があります。
- ACE は、コンテキストごとに最大 10 の SNMP ホストをサポートします。

詳細手順

	コマンド	目的
ステップ 1	**config** **例：** host1/Admin# config host1/Admin(config)#	グローバル コンフィギュレーション モードに入ります。
ステップ 2	**snmp-server host** *host_address* {*community-string_username* | **informs** | **traps** | **version** {**1**{**udp-port**} | **2c** {**udp-port**} | **3** [**auth** | **noauth** | **priv**]}} **例：** host1/Admin(config)# snmp-server host 192.168.1.1 traps version 2c SNMP_Community1 udp-port 500	SNMP 通知を受信するホストを指定します。 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。アドレスはドット区切りの 10 進 IP 表記（192.168.11.1 など）で入力します。 • *community-string_username*：通知動作を含む 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、引用符で囲まれていない、スペースを含まないテキスト文字列を入力します。 • **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。このオプションは、SNMP 応答要求と組み合わせての使用はできません。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**：（オプション）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**：（オプション）noAuthNoPriv セキュリティ レベルを指定します。 • **priv**：（オプション）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。

	コマンド	目的
	no snmp-server host *host_address* {*community-string_username* | **informs** | **traps** | **version** {**1**{**udp-port**} | **2c** {**udp-port**} | **3** [**auth** | **noauth** | **priv**]}} **例：** host1/Admin(config)# no snmp-server host 192.168.1.1 traps version 2c SNMP_Community1 udp-port 500	指定されたホストを削除します。
ステップ 3	**do copy running-config startup-config** **例：** host1/Admin(config)# do copy running-config startup-config	（オプション）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

SNMP 通知のイネーブル化

ここでは、ACE から NMS への SNMP 通知トラップと応答要求の送信を可能にする方法について説明します。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、どの SNMP 通知も定義または発行されていません。

制約事項

このテーマには、次のような制約があります。

- 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** コマンドで使用される通知タイプには、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 オブジェクトが関連付けられます。ただし、**snmp-server host** コマンドで使用可能なすべての通知タイプに notificationEnable MIB オブジェクトが含まれているわけではないため、通知タイプによっては、**snmp-server enable** コマンドで制御できない場合があります。

前提条件

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。

詳細手順

	コマンド	目的
ステップ 1	**config** 例： host1/Admin# config host1/Admin(config)#	グローバル コンフィギュレーション モードに入ります。
ステップ 2	**snmp-server enable traps** [*notification_type*] [*notification_option*] 例： host1/Admin(config)# snmp-server enable traps slb real	ACE から NMS に SNMP トラップと応答要求を送信できるようにします。 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*：（オプション）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。 （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。**logging history level** コマンドを使用して、送信するメッセージのレベルを指定します。**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 4700 Series Application Control Engine Appliance 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。

コマンド	目的
snmp-server enable traps [*notification_type*] [*notification_option*] (continued)	• *notification_option*：（オプション）次の SNMP 通知をイネーブルにします。 – **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**、**serverfarm**、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起きた場合に、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）。 サーバ ファーム内のすべての実サーバがダウンしたために、サーバ ファームのステートが変化。 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、外部に面している ACE 内のコンテンツ スイッチの背後にあるサーバを意味し、宛先アドレス（IP アドレスの範囲を使用可能）、プロトコル、宛先ポート、または着信 VLAN の属性からなります。
no snmp-server enable traps [*notification_type*] [*notification_option*] **例：** host1/Admin(config)# no snmp-server enable traps slb real	SNMP サーバ通知をディセーブルにします。
ステップ 3　**do copy running-config startup-config** **例：** host1/Admin(config)# do copy running-config startup-config	（オプション）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

下の例は、コミュニティ ストリングを使用して、ACE から IP アドレスが 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方法を示しています。

```
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 linkUp および linkDown トラップに関する IETF 標準のイネーブル化

ここでは、linkUp トラップと linkDown トラップのシスコ実装を送信するのではなく、linkUp トラップと linkDown トラップ用の IETF 標準ベースの実装（RFC 2863 を参照）を NMS に送信するように ACE を設定する方法について説明します。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。

（注）　デフォルトでは、シスコ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。

詳細手順

	コマンド	目的
ステップ 1	**config** 例： host1/Admin# config host1/Admin(config)#	グローバル コンフィギュレーション モードに入ります。
ステップ 2	**snmp-server trap link ietf** 例： host1/Admin(config)# snmp-server trap link ietf	linkUp トラップと linkDown トラップ用の IETF 標準ベースの実装を送信するように ACE を設定します。
	no snmp-server trap link ietf 例： host1/Admin(config)# no snmp-server trap link ietf	linkUp トラップと linkDown トラップのシスコ実装に戻します。
ステップ 3	**do copy running-config startup-config** 例： host1/Admin(config)# do copy running-config startup-config	（オプション）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

SNMP コミュニティ名 OID と コミュニティ セキュリティ名 OID のマスク解除

ここでは、SNMP-COMMUNITY-MIB の snmpCommunityName OID と snmpCommunitySecurityName OID のマスク解除方法について説明します。これらの OID はデフォルトでマスクされています。

詳細手順

	コマンド	目的
ステップ 1	**config** 例： host1/Admin# config host1/Admin(config)#	グローバル コンフィギュレーション モードに入ります。
ステップ 2	**snmp-server unmask-community** 例： host1/host1/Admin(config)# snmp-server unmask-community	SNMP-COMMUNITY-MIB の snmpCommunityName OID と snmpCommunitySecurityName OID をマスク解除します。
	no snmp-server unmask-community 例： host1/Admin(config)# no snmp-server unmask-community	（オプション）snmpCommunityName and OID と snmpCommunitySecurityName OID をマスクします。
ステップ 3	**do copy running-config startup-config** 例： host1/Admin(config)# do copy running-config startup-config	（オプション）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

SNMP トラップに対するトラップ送信元インターフェイスの割り当て

ここでは、SNMP v1 トラップ PDU に含まれるトラップ送信元アドレスである VLAN インターフェイスの指定方法について説明します。

制約事項

このテーマには、次のような制約があります。

- **snmp-server trap-source** コマンドを設定しなかった場合は、通知が送信される宛先ホスト アドレスごとの内部ルーティング テーブルから送信元 IP アドレスが取得されます。
- 有効な IP アドレスが設定されていないインターフェイスの VLAN 番号を指定した場合は、SNMP v1 トラップに関する通知が送信されなくなります。
- SNMP v1 トラップ PDU に含まれるトラップ送信元アドレスとして冗長な ACE 間で指定された FT VLAN インターフェイスの VLAN 番号の選択が禁止されます。

詳細手順

	コマンド	目的
ステップ 1	**config** 例： host1/Admin# config host1/Admin(config)#	グローバル コンフィギュレーション モードに入ります。
ステップ 2	**snmp-server trap-source vlan** *number* 例： host1/Admin(config)# snmp-server trap-source vlan 50	SNMP v1 トラップ PDU に含まれるトラップ送信元アドレスである VLAN インターフェイスを指定します。 *number* 引数は、SNMP v1 トラップ PDU に含まれるトラップ送信元アドレスである VLAN インターフェイスの番号を指定します。既存の VLAN インターフェイスに対応する 2 ～ 4094 の値を入力します。
	no snmp-server trap-source vlan *number* 例： host1/Admin(config)# no snmp-server trap-source vlan 50	（オプション）SNMPv1 トラップ PDU に含まれるトラップ送信元アドレスである指定された VLAN インターフェイスを削除します。
ステップ 3	**do copy running-config startup-config** 例： host1/Admin(config)# do copy running-config startup-config	（オプション）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

管理コンテキストの IP アドレスを通した ACE ユーザ コンテキスト データへのアクセス

ここでは、SNMP マネージャで 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する方法について説明します。ACE 管理コンテキストと各 ACE ユーザ コンテキストには、個別の IP アドレスが割り当てられています。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。

管理コンテキストの IP アドレスを使用して、ユーザ コンテキストに関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。

ここでは、次の内容について説明します。

- SNMPv1/v2 使用時のユーザ コンテキスト データへのアクセス
- SNMPv3 の使用時のユーザ コンテキスト データへのアクセス

制約事項

ユーザ コンテキストに関する通知は、管理コンテキストを通して送信できません。

SNMPv1/v2 使用時のユーザ コンテキスト データへのアクセス

ここでは、SNMPv1/v2 を使用して、適切な SNMP バージョン、管理コンテキスト IP アドレス、およびユーザ コンテキストの名前に埋め込まれた管理コンテキスト コミュニティ ストリングを指定することによって、管理コンテキスト IP アドレスを通してユーザ コンテキストに使用可能な MIB にアクセスする方法について説明します。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、管理コンテキストまたは任意の 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。

例

下の例は、管理コンテキストにコミュニティ ストリングの adminCommunity と 10.6.252.63 の IP アドレスが設定されているときに、ユーザ コンテキスト C1 に関するデータを返す方法を示しています。

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

SNMPv3 の使用時のユーザ コンテキスト データへのアクセス

ここでは、SNMPv3 を使用し、管理コンテキスト 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 SNMPv3 パケット内の管理コンテキストでサポートされているユーザ コンテキスト名を使用することによって、管理コンテキスト IP アドレスを通してユーザ コンテキストの MIB にアクセスする方法について説明します。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 コンテキストの SNMPv3 エンジン ID の設定」を参照してください。

例

下の例は、管理コンテキストに SNMP ユーザの snmpuser と 10.6.252.63 の IP アドレスが設定されているときに、ユーザ コンテキスト C2 からデータを返す方法を示しています。

```
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 コンテキスト名フィールドが空の文字列（""）に設定された SNMPv3 要求をユーザ コンテキストの IP アドレスに送信すると、その要求は廃棄されます。

ACE コンテキストの SNMPv3 エンジン ID の設定

ここでは、管理コンテキストまたはユーザ コンテキストの SNMP エンジン ID の設定方法について説明します。ACE では、デフォルトで、管理コンテキストと各ユーザ コンテキストの SNMP エンジン ID が自動的に作成されます。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 コンテキストの SNMP エンジン ID を変更した場合は、設定済みのすべての 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。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 ユーザを再作成し、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する必要があります（「SNMP コミュニティの定義」を参照）。

詳細手順

	コマンド	目的
ステップ 1	**config** 例： host1/Admin# config host1/Admin(config)#	グローバル コンフィギュレーション モードに入ります。
ステップ 2	**snmp-server engineid** *number* 例： host1/Admin(config)# snmp-server engineID 884395734985738888843957349857388	ACE コンテキストの SNMP エンジン ID を設定します。 *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。
	no snmp-server engineid *number* 例： host1/Admin(config)# snmp-server engineID 884395734985738888843957349857388	（オプション）ACE コンテキストのデフォルトのエンジン ID をリセットします。
ステップ 3	**do show snmp engineID** 例： host1/Admin(config)# **do show snmp engineID**	（オプション）コンテキストのエンジン ID を表示します。
ステップ 4	**do copy running-config startup-config** 例： host1/Admin(config)# do copy running-config startup-config	（オプション）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

SNMP 管理トラフィック サービスの設定

ここでは、クラス マップ、ポリシー マップ、およびサービス ポリシーの使用を通して ACE とやり取りする SNMP 管理トラフィックの設定方法について説明します。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、トラフィック ポリシーを 1 つの VLAN インターフェイスに、またはすべての VLAN インターフェイスにグローバルにアタッチします。

ここでは、SNMP アクセス用のクラス マップ、ポリシー マップ、およびサービス ポリシーの作成方法について概要を示します。

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 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*』を参照してください。

ここでは、次の内容について説明します。

- レイヤ 3 およびレイヤ 4 クラス マップの作成と設定
- レイヤ 3 およびレイヤ 4 ポリシー マップの作成
- 同じコンテキスト内のすべての VLAN インターフェイスへのサービス ポリシーのグローバルな適用
- 特定の VLAN インターフェイスへのサービス ポリシーの適用

レイヤ 3 およびレイヤ 4 クラス マップの作成と設定

ここでは、レイヤ 3 およびレイヤ 4 クラス マップを作成して、ACE で受信可能な SNMP 管理トラフィックを分類する方法について説明します。このクラス マップを使用して、ACE で受信可能な着信 IP プロトコルとクライアント送信元ホストの IP アドレスとサブネット マスクを一致条件として特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が受信できるようになります。このクラス マップでは、SNMP などのプロトコルの管理セキュリティとして、許容ネットワーク トラフィックも定義されます。

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。

詳細手順

	コマンド	目的
ステップ 1	**config** **例：** host1/Admin# config host1/Admin#(config)#	グローバル コンフィギュレーション モードに入ります。
ステップ 2	**class-map type management** [**match-all** | **match-any**] *map_name* **例：** host1/Admin(config)# class-map type management match-all SNMP-ALLOW_CLASS host1/Admin(config-cmap-mgmt)#	レイヤ 3 およびレイヤ 4 クラス マップを作成して、ACE で受信可能な SNMP 管理トラフィックを分類します。 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**：（オプション）クラス マップに複数の一致条件が含まれている場合に、ACE でレイヤ 3 およびレイヤ 4 ネットワーク トラフィックを評価する方法を決定します。**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、一致と見なされます。 – **match-all**：（デフォルト）クラス マップで指定された一致条件のすべてがクラス マップ内のネットワーク トラフィック クラスと一致する（通常は、同じタイプの **match** コマンド）。 – **match-any**：クラス マップで指定された一致条件の 1 つがクラス マップ内のネットワーク トラフィック クラスと一致する（通常は、タイプの異なる **match** コマンド）。 • *map_name*：クラス マップに割り当てられた名前。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。 このコマンドによって、クラス マップ管理コンフィギュレーション モードに入ります。
	no class-map type management [**match-all** | **match-any**] *map_name* **例：** host1/Admin(config)# no class-map type management match-all SNMP-ALLOW_CLASS	（オプション）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 マップを削除します。
ステップ 3	**description** *text* **例：** host1/Admin(config-cmap-mgmt)# description Allow SNMP access	レイヤ 3 およびレイヤ 4 リモート管理クラス マップの概要を提供します。 *text* 引数は、入力が必要な説明です。最大 240 文字の英数字からなる、引用符で囲まれていないテキスト文字列を入力します。
	no description **例：** host1/Admin(config-cmap-mgmt)# no description	（オプション）クラス マップから説明を削除します。

	コマンド	目的
ステップ 4	[*line_number*] **match protocol snmp** {**any** | **source-address** *ip_address mask*} **例：** `host1/Admin(config-cmap-mgmt)# match protocol snmp source-address 192.168.10.1 255.255.255.0`	SNMP が ACE で受信可能なことと NMS を指定するためのクラス マップを設定します。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。 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*：（オプション）編集または削除対象の **match** コマンドを特定するための行番号。2 ～ 255 の整数を入力します。**no** *line_number* を入力すると、行全体を入力しなくても、長い **match** コマンドを削除できます。行番号は、match 文のプライオリティまたは順番を示すものではありません。 • **any**：管理トラフィック分類用の任意の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 アドレスとサブネット マスクを指定します。分類の一部として、ACE は暗黙的に、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。 • *mask*：ドット区切りの 10 進表記のクライアントのサブネット マスク（255.255.255.0 など）。
	no match protocol snmp **例：** `host1/Admin(config-cmap-mgmt)# no match protocol snmp`	（オプション）クラス マップから指定された SNMP プロトコル一致条件を選択解除します。
ステップ 5	**do copy running-config startup-config** **例：** `host1/Admin(config-cmap-mgmt)# do copy running-config startup-config`	（オプション）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

レイヤ 3 およびレイヤ 4 ポリシー マップの作成

ここでは、特定の分類と一致する 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するレイヤ 3 およびレイヤ 4 ポリシー マップの作成方法について説明します。

詳細手順

	コマンド	目的

ステップ 1	**config**
	
	例：
	`host1/Admin# config`
	`host1/Admin#(config)#`
		グローバル コンフィギュレーション モードに入ります。

ステップ 2	**policy-map type management first-match** *map_name*
	例：
	`host1/Admin(config)# policy-map type management first-match SNMP-ALLOW_POLICY`
	`host1/Admin(config-pmap-mgmt)#`
		ACE による SNMP 管理プロトコルの受信を許可するレイヤ 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。
		
		map_name 引数は、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。
		
		このコマンドによって、ポリシー マップ管理コンフィギュレーション モードに入ります。

	no policy-map type management first-match *map_name* **例：** `host1/Admin(config)# no policy-map type management first-match SNMP-ALLOW_POLICY`	（オプション）ACE からネットワーク トラフィック管理ポリシー マップを削除します。

	コマンド	目的

ステップ 3	**class** {*name1* [**insert-before** *name2*] | **class-default**}
	例：
	`host1/Admin(config-pmap-mgmt)# class SNMP-ALLOW_CLASS`
	`host1/Admin(config-pmap-mgmt-c)#`
		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ために **class-map** コマンドを使用して作成されたレイヤ 3 およびレイヤ 4 トラフィック クラスを指定します。
		引数、キーワード、およびオプションは次のとおりです。
		• *name1*：トラフィックとトラフィック ポリシーを関連付けるために **class-map** コマンドを使用して設定された、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*：（オプション）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。このクラスの削除または変更はできません。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** 文が含まれており、任意のトラフィック分類との一致に使用されます。
		このコマンドを使用すると、ポリシー マップ管理クラス コンフィギュレーション モードが開始します。

	no class *name1* **例：** `host1/Admin(config-cmap-mgmt)# no class SNMP-ALLOW_CLASS`	（オプション）レイヤ 3 およびレイヤ 4 ポリシー マップからクラス マップを削除します。
ステップ 4	**permit** **例：** `host1/Admin(config-pmap-mgmt-c)# permit`	レイヤ 3 およびレイヤ 4 クラス マップで指定されたネットワーク管理トラフィックを ACE で受信可能にします。
	deny **例：** `host1/Admin(config-pmap-mgmt-c)# deny`	（オプション）レイヤ 3 およびレイヤ 4 クラス マップで指定されたネットワーク管理トラフィックを ACE で拒否可能にします。
ステップ 5	**do copy running-config startup-config** **例：** `host1/Admin(config-pmap-mgmt-c)# do copy running-config startup-config`	（オプション）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

下の例は、**insert-before** コマンドを使用して、ポリシー マップ内の 2 つのクラス マップの順序を定義する方法を示しています。

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

同じコンテキスト内のすべての VLAN インターフェイスへのサービス ポリシーのグローバルな適用

ここでは、既存のポリシー マップを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適用する方法について説明します。

サービス ポリシーの適用時は次のガイドラインに注意してください。

- 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。

（注） 特定の VLAN インターフェイスにポリシー マップを適用するには、「特定の VLAN インターフェイスへのサービス ポリシーの適用」を参照してください。

制約事項

ACE では、1 つの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。

詳細手順

	コマンド	目的
ステップ 1	**config** **例：** host1/Admin# config host1/Admin#(config)#	グローバル コンフィギュレーション モードに入ります。
ステップ 2	**service-policy input** *policy_name* **例：** host1/Admin(config)# service-policy input SNMP_MGMT_ALLOW_POLICY	SNMP 管理ポリシー マップを 1 つのコンテキストに関連付けられたすべての VLAN にグローバルに適用します。 キーワードと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 ポリシーをアタッチするように指定します。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 文字の英数字にすることができます。 ポリシー マップを 1 つのコンテキストに関連付けられたすべての VLAN にグローバルに適用する場合

	コマンド	目的
	no service-policy input *policy_name* **例：** host1/Admin(config)# no service-policy input SNMP_MGMT_ALLOW_POLICY	（オプション）1 つのコンテキストに関連付けられたすべての VLAN から SNMP 管理ポリシー マップを削除します。 ポリシーを削除すると、次にトラフィック ポリシーを特定の VLAN インターフェイス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アタッチしたときに、ACE によって自動的に関連するサービス ポリシー統計情報がサービス ポリシー統計情報の新しい開始点を指すようにリセットされます。
ステップ 3	**do copy running-config startup-config** **例：** host1/Admin(config)# do copy running-config startup-config	（オプション）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

特定の VLAN インターフェイスへのサービス ポリシーの適用

ここでは、既存のポリシー マップを特定の VLAN インターフェイスに適用する方法について説明します。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。

（注） ポリシー マップを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適用するには、「同じコンテキスト内のすべての VLAN インターフェイスへのサービス ポリシーのグローバルな適用」を参照してください。

制約事項

ACE では、1 つの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。

詳細手順

	コマンド	目的
ステップ 1	**config** **例：** host1/Admin# config host1/Admin#(config)#	グローバル コンフィギュレーション モードに入ります。
ステップ 2	**interface vlan** *number* **例：** host1/Admin(config)# interface vlan 50 host1/Admin(config-if)#	インターフェイス VLAN を指定します。 *number* 引数は、ACE に割り当てられた VLAN の番号です。 このコマンドによって、VLAN 用のインターフェイス コンフィギュレーション モードに入ります。
ステップ 3	**ip address** *address* **例：** host1/Admin(config-if)# ip address 172.20.1.100 255.255.0.0	VLAN IP アドレスを指定します。

	コマンド	目的
ステップ 4	**service-policy input** *policy_name* 例： host1/Admin(config-if)# service-policy input SNMP_MGMT_ALLOW_POLICY	SNMP 管理ポリシー マップを VLAN に適用します。 キーワードと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 ポリシーをアタッチするように指定します。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 文字の英数字にすることができます。
	no service-policy input *policy_name* 例： host1/Admin(config-if)# no service-policy input SNMP_MGMT_ALLOW_POLICY	（オプション）インターフェイス VLAN から SNMP 管理ポリシーを削除します。 ポリシーを削除すると、次にトラフィック ポリシーを特定の VLAN インターフェイス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アタッチしたときに、ACE によって自動的に関連するサービス ポリシー統計情報がサービス ポリシー統計情報の新しい開始点を指すようにリセットされます。
ステップ 5	**do copy running-config startup-config** 例： host1/Admin(config-if)# do copy running-config startup-config	（オプション）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

SNMP およびサービス ポリシー統計情報の表示またはクリア

ここでは、SNMP およびサービス ポリシー統計情報の表示またはクリア方法について説明します。ここで説明する内容は、次のとおりです。

SNMP およびサービス ポリシー統計情報の表示

ここでは、SNMP 設定と関連するサービス ポリシーに関する設定情報と統計情報を表示する **show** コマンドについて説明します。ここで説明する内容は、次のとおりです。

SNMP 統計情報の表示

SNMP 統計情報と設定済みの SNMP 情報を表示するには、次の **show** コマンドを使用します。

コマンド	目的
show snmp [**community** | **engineID** | **group** | **host** | **sessions** | **user**]	SNMP 統計情報と設定済みの SNMP 情報を表示します。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。 キーワードは次のとおりです。 • **community**：（オプション）SNMP コミュニティ ストリングを表示します。 • **engineID**：（オプション）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**：（オプション）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**：（オプション）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**：（オプション）SNMPv3 ユーザ情報を表示します。

表 7-6 に、**show snmp community** コマンド出力に含まれるフィールドの説明を示します。

表 7-6　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 で受信された 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
Illegal operation for community name supplied	そのコミュニティに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	コミュニティに対するアクセス権、読み取り専用
User	SNMP ユーザの名前を識別する文字列
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 7-7 に、**show snmp community** コマンド出力に含まれるフィールドの説明を示します。

表 7-7　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	コミュニティに対するアクセス権、読み取り専用

表 7-8 に、**show snmp engineID** コマンド出力に含まれるフィールドの説明を示します。

表 7-8　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 7-9 に、**show snmp group** コマンド出力に含まれるフィールドの説明を示します。

表 7-9　show snmp group コマンド出力のフィールド

フィールド	説明
Group name	共通のアクセス ポリシーを使用する SNMP グループまたはユーザ集合の名前
Security model	グループで使用されるセキュリティ モデル（v1、v2c、または v3）
Security level	グループで使用されるセキュリティ レベル
Read view	グループの読み取りビューを識別する文字列
Write view	グループの書き込みビューを識別する文字列
Notify view	グループの通知ビューを識別する文字列
Storage-type	設定値がデバイス上の揮発性メモリまたは一時メモリ内で設定されたのか、デバイスの電源を切断して再投入しても設定が保存される不揮発性メモリまたは永久メモリ内で設定された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か、非アクティブかを示す

表 7-10 に、**show snmp host** コマンド出力に含まれるフィールドの説明を示します。

表 7-10　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	通知の送信先の UDP ポート番号
Version	トラップ送信に使用される SNMP のバージョン（v1、v2c、または v3）
Level	認証とプライバシの手段
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 7-11 に、**show snmp sessions** コマンド出力に含まれるフィールドの説明を示します。

表 7-11　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 7-12 に、**show snmp user** コマンド出力に含まれるフィールドの説明を示します。

表 7-12　show snmp user コマンド出力のフィールド

フィールド	説明
User	SNMP ユーザの名前を識別する文字列
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

SNMP サービス ポリシー統計情報の表示

SNMP 設定に関連付けられたサービス ポリシーの統計情報を表示するには、次の **show** コマンドを使用します。

コマンド	目的
show service-policy *policy_name* [**detail**]	レイヤ 3 およびレイヤ 4 SNMP 管理ポリシー マップに関するサービス ポリシー統計情報を表示します。 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*：最大 64 文字の英数字からなる、引用符で囲まれていないテキスト文字列として現在使用されている（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 • **detail**：（オプション）より詳細なポリシー マップの統計情報とステータス情報を一覧表示します。 **（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。

例

下の例は、SNMP_MGMT_ALLOW_POLICY ポリシー マップに関するサービス ポリシー統計情報の表示方法を示しています。

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

SNMP サービス ポリシー統計情報のクリア

SNMP 設定に関連付けられたサービス ポリシーの統計情報をクリアするには、次の **clear** コマンドを使用します。

コマンド	目的
clear service-policy *policy_name*	サービス ポリシー統計情報をクリアします。 *policy_name* 引数には、現在使用されている（インターフェイスに適用されている）既存のポリシー マップの ID を入力します。

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。この例は、ACE への接続を許可するクライアント送信元ホストの IP アドレスを制限可能なことを示しています。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
```