SNMP の設定

この章では、CSS に Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）機能を設定する方法について説明します。また、通信業界で広く使用されるアプリケーション層プロトコルである SNMP の概要についても説明します。この章の内容は、特に指示のない限り、すべての CSS モデルに適用されます。

この章の主な内容は次のとおりです。

SNMP の概要

SNMP は、IP ベースのインターネットワークのネットワーク管理標準規格です。SNMP には、プロトコル、データベース構造規格、および管理データ オブジェクトのセットが含まれます。標準的な SNMP の実装は、1 つ以上の Network Management Systems（NMS; ネットワーク管理システム）で実行する管理アプリケーションと、通常さまざまなネットワーク装置上のファームウェアで実行するエージェント アプリケーションで構成されます。

SNMP には、主な標準リビジョンが 2 つ（SNMPv1 および SNMPv2）あります。CSS では、SNMPv1 および SNMPv2C（SNMP バージョン 2C）、標準の Management Information Base（MIB; 管理情報ベース）（MIB-II）オブジェクト、およびエンタープライズ MIB オブジェクトの拡張セットがサポートされます。MIB については、「MIB の概要」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。

- マネージャとエージェント
- SNMP マネージャとエージェントの通信

（注）　デフォルトでは、SNMP による CSS へのアクセスは、**no restrict snmp** コマンドにより有効になっています。詳細については、「CSS での SNMP 設定の準備」を参照してください。

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*と呼ばれるソフトウェア エンティティを使用してネットワーク装置を管理します。

- *マネージャ*は、ネットワーク内の他の SNMP 管理対象装置（ネットワーク ノード）をすべて監視および制御します。管理対象ネットワークには、SNMP マネージャが最低 1 つ必要です。マネージャは、ネットワーク内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、管理対象装置（ネットワーク ノード）に常駐します。エージェントは、SNMP マネージャから指示を受信し、イベントが起きるたびに管理情報を SNMP マネージャに送信します。エージェントは、ルータ、ブリッジ、ハブ、ワークステーション、またはプリンタに置くことができ、これによって、多くのネットワーク装置を識別できるようになります。

SNMP 管理アプリケーションには、異なるタイプのものが多数ありますが、すべてのアプリケーションで同じ基本タスクが実行されます。つまり、SNMP マネージャはエージェントと通信し、ネットワーク装置を監視および制御し、ネットワーク装置から警告を受信します。どの SNMP 互換 NMS を使用しても、CSS を監視および制御できます。

SNMP マネージャとエージェントの通信

SNMP マネージャとエージェント間の通信には、いくつかの方法があります。

- マネージャで可能な処理は次のとおりです。
  - 値を取得（GET アクション）

    SNMP マネージャでは、エージェント装置にログインしたユーザの数や、エージェント装置におけるクリティカル プロセ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送信します。
  - 指定した変数の次の値を取得（GET-NEXT アクション）

    SNMP マネージャは、MIB から値を取得します。GET-NEXT 機能を使用する場合、検索する MIB オブジェクト インスタンスの正確な名前を知る必要はありません。SNMP マネージャは、指定された変数を取得し、目的の変数を見つけるまで順番に検索します。
  - 複数の値を取得（GET-BULK アクション）

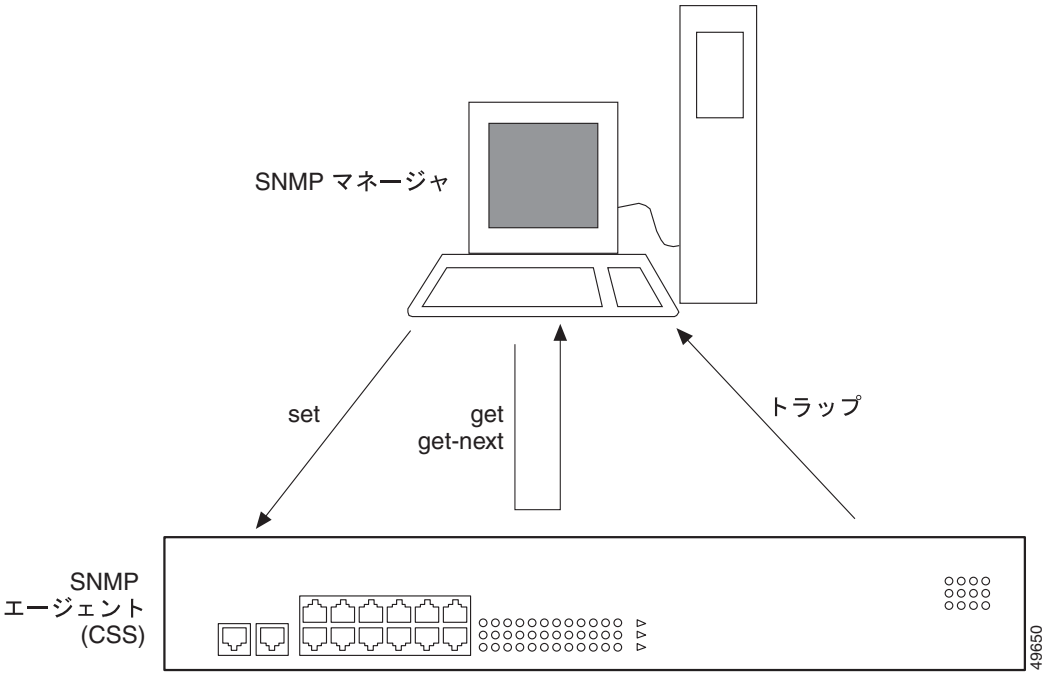
    SNMP マネージャは、指定した GET-NEXT アクションを複数回実行します。
  - エージェントでの設定変更（SET アクション）

    SNMP マネージャは、MIB オブジェクトの値を変更するようにエージェントに要求します。たとえば、SET アクションを使用して、リモート装置上でスクリプトやアプリケーションを実行できます。

- エージェントに事前に決められた重要なイベントが起きると、エージェントは、マネージャに割り込みメッセージをいつでも送信できます。このメッセージを *トラップ* と呼びます。CSS ソフトウェアでサポートされる SNMP トラップ（および関連する MIB オブジェクト）の詳細については、「CSS の SNMP トラップ」を参照してください。

  トラップ状況が発生すると、SNMP エージェントは、*トラップ受信装置* または *トラップ ホスト* として指定された装置に SNMP トラップ メッセージを送信します。SNMP 管理者は、トラップ ホスト（通常は、SNMP 管理ステーション）を、トラップが検出されたときに必要なアクションを実行するように設定します。図 5-1 は、マネージャとエージェントの通信を表しています。

図 5-1　SNMP マネージャとエージェントの間のやり取り



MIB の概要

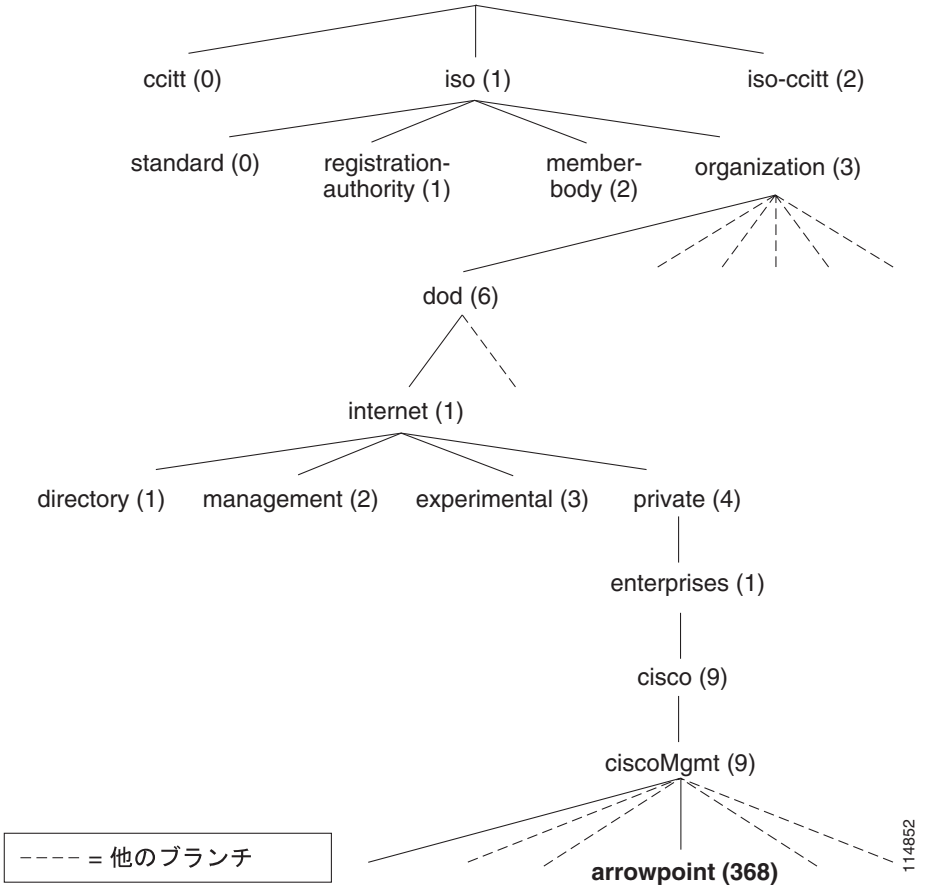
SNMP では、MIB を利用してネットワークから情報を得ます。MIB は、*MIB オブジェクト*と呼ばれるコード ブロックのデータベースです。各 MIB オブジェクトでは、エージェントのポートを利用して転送されるバイト数の計算など、1 つの特定の機能を制御します。MIB オブジェクトは、MIB のオブジェクト名、説明、デフォルト値などを定義する *MIB 変数*で構成されています。

MIB オブジェクトの収集は階層構造になっています。MIB 階層は *MIB ツリー*と呼ばれます。MIB ツリーは、International Standards Organization（ISO; 国際標準化機構）により定義されています。MIB は SNMP マネージャにインストールされ、SNMP ネットワークの各エージェント内にあります。

ツリーの最上層には、ネットワークについての最も広範な情報があります。ツリーの各ブランチおよびサブブランチは、展開が進むにつれて情報が細分化され、ツリーの最下部のブランチには、最も詳細で固有性の高い MIB オブジェクトがあります。リーフには実際のデータが含まれています。ツリーが展開されるにつれ、MIB オブジェクトが詳細化されていく例については、図 5-2 を参照してください。

（注） ISO の規定によって MIB ツリーには MIB-I と MIB-II の 2 つのバージョンがあります。MIB-II には、MIB-I よりも多くの変数があります。MIB-II 標準については、RFC 1213 の Management Information Base for Network Management of TCP/IP-based Internets: MIB-II を参照してください。

図 5-2　MIB ツリーの最上層



ここでは、次の内容について説明します。

- MIB 変数
- 拡張 MIB（エンタープライズ MIB）
- MIB ファイルの更新

MIB 変数

MIB 変数には次の 2 つのタイプがあります。

- スカラ変数：単一表現を持つオブジェクトを定義する変数。つまり、1 つのオブジェクトで全システムの特定の特性を記述します。たとえば、スカラ変数の 1 つとして、CSS のシステム全体を記述する **SysDescr** があります。
- 表変数：複数表現を持つオブジェクトを定義する変数。つまり、オブジェクトが、修飾子に応じて異なる値を持つことが可能です。たとえば、1 つの表オブジェクトで、インターフェイスごとのバイト、ボードごとの温度、またはサービスごとのヒット数を示すことができます。

図 5-2 で示されているように、MIB オブジェクト名には番号が付けられています。この番号は、*object identifier*（*OID; オブジェクト識別子*）と呼ばれ、MIB ツリー内の MIB オブジェクトを固有に識別します。点線は、この箇所での説明に関係のない他のブランチを表します。

たとえば、図 5-2 では、CSS 固有の MIB オブジェクトを含む arrowpoint (368) という MIB オブジェクトは、次のようにラベルが付けられます。

```
iso.organization.dod.internet.private.enterprises.cisco.ciscoMgmt.
arrowpoint
```

または

```
1.3.6.1.4.1.9.9.368
```

拡張 MIB（エンタープライズ MIB）

MIB ツリーには、特定のベンダーが独自の拡張機能を構築するための特別なブランチ セットがあります。この特別なブランチ セットは*エンタープライズ MIB ブランチ*と呼ばれます。CSS の MIB は、CSS ディスクの次のディレクトリと ZIP ファイルに格納されています。

- SNMPv1 MIB：/mibs/v1/cssmibsv1.zip
- SNMPv2C MIB：/mibs/v2/cssmibsv2.zip

CSS のエンタープライズ MIB（図 5-2 で強調表示されている MIB 識別子）は、このブランチの MIB ファイルで構成されています。エンタープライズ MIB ファイルは、機能境界線に沿って分類されています。

CSS エンタープライズ MIB の下の MIB ブランチ一覧については、「CSS MIB」を参照してください。

MIB ファイルの更新

ここでは、管理ステーションで MIB ファイルを更新する手順を説明します。

標準 MIB のロード

管理ステーションに CSS MIB をロードする前に、次の標準 MIB をロードする必要があります。

SNMP v1 の標準 MIB

- RFC-1212
- RFC-1215
- INET-ADDRESS-MIB
- SNMP-FRAMEWORK-MIB
- SNMPv2-TC-v1
- RFC1155-SMI
- SNMPv2-SMI-v1 (RFC 1493)

SNMP v2 の標準 MIB

- SNMPv2-SMI
- SNMPv2-TC
- SNMP-FRAMEWORK-MIB
- SNMPv2-CONF
- INET-ADDRESS-MIB
- BRIDGE-MIB

CSS ソフトウェアのアップグレード後に管理ステーションで標準 MIB を更新するには、次の手順を実行します。

1. 標準 MIB を管理ステーションに転送します。
2. 標準 MIB を管理アプリケーションにロードします。

CSS MIB のロード

CSS ソフトウェアのアップグレード後に CSS エンタープライズ MIB を更新することをお勧めします。CSS MIB は、CSS GZIP ファイルに含まれています。ソフトウェアのアップグレード中に、この MIB が CSS/mibs ディレクトリにロードされます。CSS MIB の詳細については、「CSS MIB」を参照してください。

CSS のアップグレード後に管理ステーションの CSS MIB を更新するには、次の手順を実行します。

1. FTP を使用して、CSS MIB（/v1 または /v2）ディレクリから管理ステーションに CSS MIB を転送します。

（注）　FTP の CSS 実装では、複数のファイル転送に使用する **mget** コマンドを使用できません。

2. CSS MIB を管理アプリケーションにロードします。

（注）　/v2 ディレクトリには、CSS v2 のすべての MIB が格納されます。/v1 ディレクトリには、v1 コンパイラを使用してコンパイルする CSS v1 の MIB だけが格納されます。/v1 ディレクトリに必要な MIB がない場合は、/v2 ディレクトリ内の該当する MIB を使用してください。

SNMP コミュニティ

各 SNMP 装置（メンバー）は、*コミュニティ*の一員です。SNMP コミュニティで、各 SNMP 装置のアクセス権が決定されます。

コミュニティに名前を指定します。コミュニティに名前をつけると、*メンバー*としてこのコミュニティに割り当てられたすべての SNMP 装置には、同じアクセス権が与えられます。CSS がサポートしているアクセス権は、次のとおりです。

- read：コミュニティ内の装置の MIB ツリーへの読み取り専用アクセス
- read-write：コミュニティ内の装置の MIB ツリーへの読み取り / 書き込みアクセス

CSS での SNMP 設定の準備

SNMP 管理アプリケーションを設定すると、CSS で SNMP を設定することができます。CSS では、SNMP 機能の 2 つの基本領域（SNMP 機能および RMON 機能）を設定できます。

（注）　RMON の設定については、第 6 章「RMON の設定」を参照してください。

CSS への SNMP アクセスを制御するには、**no restrict snmp** コマンドと **restrict snmp** コマンドを使用します。デフォルトでは、SNMP によるアクセスが有効になっています。このグローバル設定モード コマンドには、次のオプションがあります。

- **no restrict snmp** : CSS への SNMP アクセスを有効にする（デフォルト設定）。
- **restrict snmp**：CSS への SNMP アクセスを無効にする。

ネットワークに SNMP を設定する前に、SNMP 設定を計画する際は次の点について検討してください。

- SNMP マネージャが必要とする情報の種類を決定する（アプリケーションで SNMP マネージャを使用している場合）。管理ソフトウェアを利用して目的の MIB 変数を選択します。
- 必要なトラップ　ホスト数を決定する。ネットワークの設定によっては、プライマリ トラップ ホストを設定し、別のワークステーションでも冗長用にトラップを受信したい場合があります。また、分散型またはセグメント型ネットワークでは、さらに多くのトラップ ホストを使用したい場合もあります。SNMP エージェントには、エージェントあたり 5 トラップ ホストまで設定できます。つまり、1 つのエージェントで最高 5 つのホストに報告できます。
- 管理ステーション（1 つまたは複数）を決定する。CSS は SNMP ネットワーク体系内の 1 つのエージェントです。このエージェントは、装置のブート時にはすでに CSS に埋め込まれています。したがって、必要なのは、CSS に SNMP パラメータを設定する作業だけです。

SNMP エージェントとしての CSS の定義

ここでは、SNMP エージェントとして CSS を定義する方法について説明します。内容は次のとおりです。

SNMP エージェント設定のクイック スタート

表 5-1 では、CSS を SNMP エージェントとして設定するために必要な手順の概要を説明しています。それぞれの手順に、作業を行うために必要な CLI コマンドも示します。CLI コマンドに関する各機能とすべてのオプションの詳細については、表 5-1 以降の項を参照してください。

表 5-1　CSS の SNMP エージェント定義のクイック スタート

作業とコマンドの例

1. read-only（GET アクション用）と read-write（GET および SET アクション用）の各アクセス タイプについて、SNMP コミュニティ ストリングを定義します。この手順は、CSS で SNMP を使用する場合には必須です。
`(config)# snmp community public read-only`
`(config)# snmp community private read-write`

2. （省略可）SNMP の連絡先名を入力します。 `(config)# snmp contact "fred n mandy"`

表 5-1　CSS の SNMP エージェント定義のクイック スタート（続き）

作業とコマンドの例
3. （省略可）SNMP の連絡先の場所を入力します。 `(config)# snmp location "Operations"`
4. （省略可）SNMP の装置名を入力します。 `(config)# snmp name "arrowpoint.com"`

5. トラップの受信側と SNMP コミュニティ（SNMP トラップを設定する場合に必要）を割り当てます。トラップ ホストは 5 つまで指定できます。デフォルトでは、すべてのトラップは無効になっています。**snmp trap-host** の IP アドレスは、トラップを受信するように設定された SNMP ホストに対応します。**trap-host** コマンドの末尾に入力するコミュニティ情報はトラップ内に入り、管理ステーションが着信トラップをフィルタリングするために使用することができます。
`(config)# snmp trap-host 172.16.3.6 trap`
`(config)# snmp trap-host 172.16.8.4 trap`

6. （省略可）汎用トラップをオンにします。認証失敗トラップを使用する場合は、この手順が必要です。 `(config)# snmp trap-type generic`
7. （省略可）認証失敗トラップをオンにします。この手順を実行するには、汎用トラップをオンにする必要があります。ステップ 6 を参照してください。権限のない SNMP マネージャが、無効な、または誤ったコミュニティ名を SNMP エージェントに送信した場合は、認証が失敗します。認証エラーが起きると、エージェントは認証トラップをトラップ ホスト（複数のトラップ ホストを設定した場合は複数のトラップ ホスト）に送信します。 `(config)# snmp auth-traps`

8. （省略可）グローバル エンタープライズ トラップを有効にします。エンタープライズ トラップを使用する場合は、この手順が必要です。
`(config)# snmp trap-type enterprise`
特定のエンタープライズ トラップ タイプを有効にします。ログインの失敗をトラップ ホストに通知するトラップを設定できます。ログイン失敗トラップで、ログインに失敗したユーザのユーザ名と送信元 IP アドレスがわかります。
`(config)# snmp trap-type enterprise login-failure`

表 5-1　CSS の SNMP エージェント定義のクイック スタート（続き）

作業とコマンドの例
9. （省略可）リロードが有効になるようにトラップ ホストを設定します。リロードを有効にすることにより、適切な書き込みコミュニティ権限を持つ管理ステーションから CSS を再度ブートできます。 `(config)# **snmp reload-enable 100**`
10. （省略可）システムで Denial of Service（DoS; サービスの拒絶）攻撃があったことをトラップ ホストに通知するための特殊なエンタープライズ トラップしきい値を設定します。たとえば、不正な送信元または宛先のアドレスによる DoS 攻撃をトラップ ホストに通知するように、トラップしきい値を設定することができます。 `(config)# **snmp trap-type enterprise dos-illegal-attack trap-threshold 1**`

次の実行設定例は、表 5-1 のコマンドの入力結果を表しています。

```
!************************** GLOBAL ***************************
  snmp trap-type enterprise

  snmp community techpubs read-write
  snmp contact "fred n mandy"
  snmp location "Operations"
  snmp name "arrowpoint.com"
  snmp trap-host 172.16.3.6 trap
  snmp trap-host 172.16.8.4 trap
  snmp trap-type generic
  snmp auth-traps
  snmp trap-type enterprise login-failure
  snmp reload-enable 100
  snmp trap-type enterprise dos-illegal-attack trap-threshold 1
```

SNMP コミュニティの設定

SNMP コミュニティ名とアクセス権を設定または変更するには、**snmp community** コマンドを使用します。コミュニティ名はいくつでも指定できます。

注意　CSS で SNMP を使用する前に、各アクセス タイプ（read-only または read-write）のコミュニティ ストリングを定義しておく必要があります。read コミュニティ ストリングを指定しないと CSS にアクセスできません。

グローバル設定モードのコマンドのシンタックスは次のとおりです。

snmp community *community_name* [**read-only**|**read-write**]

このコマンドの変数とオプションは次のとおりです。

- *community_name*：システムの SNMP コミュニティ名。スペースを含まない 31 文字以内のテキスト文字列を引用符で囲まずに入力します。
- **read-only**：コミュニティに読み取り専用でアクセスできる。
- **read-write**：コミュニティに読み取りおよび書き込みでアクセスできる。

たとえば、次のように入力します。

```
(config)# snmp community sqa read-write
```

コミュニティ名を削除するには、次のコマンドを入力します。

```
(config)# no snmp community sqa
```

SNMP の連絡先の設定

SNMP システムの連絡先名を設定または変更するには、**snmp contact** コマンドを使用します。設定できる連絡先名は 1 つだけです。このグローバル設定モードのコマンドのシンタックスは次のとおりです。

snmp contact *"contact_name"*

連絡先名には、スペースを含む 255 文字以内のテキスト文字列を、引用符で囲んで入力します。入力文字には、たとえば、電話番号や電子メール アドレスなどの連絡手段の情報を入れることもできます。

たとえば、次のように入力します。

```
(config)# snmp contact "Fred N. Mandy"
```

指定した SNMP 連絡先名を削除して、デフォルトの「Cisco Systems, Content Network Systems」にリセットするには、次のように入力します。

```
(config)# no snmp contact
```

SNMP の場所情報の設定

SNMP システムの場所を設定または変更するには、**snmp location** コマンドを使用します。設定できる場所は 1 つだけです。このグローバル設定モードのコマンドのシンタックスは次のとおりです。

snmp location *"location"*

場所には、システムの実際の場所を入力します。255 文字以内のテキスト文字列を引用符で囲んで入力します。

たとえば、次のように入力します。

```
(config)# snmp location "sqa_lab1"
```

指定した SNMP システムの場所を削除して、デフォルトの「Customer Premises」にリセットするには、次のように入力します。

```
(config)# no snmp location
```

SNMP 名の設定

このシステムの SNMP 名を設定または変更するには、**snmp name** コマンドを使用します。指定できる名前は 1 つだけです。このグローバル設定モードのコマンドのシンタックスは次のとおりです。

snmp name *"name"*

SNMP 名には、管理者がシステムに割り当てた一意の名前を入力します。255 文字以内のテキスト文字列を引用符で囲んで入力します。標準的な名前の表記法は、システムの完全修飾ドメイン名（たとえば、sqa@arrowpoint.com）です。

たとえば、次のように入力します。

```
(config)# snmp name "sqa@arrowpoint.com"
```

システムの SNMP 名を削除して、デフォルトの「Support」にリセットするには、次のように入力します。

```
(config)# no snmp name
```

SNMP トラップ ホストの設定

CSS からトラップを受信する SNMP ホストを設定または変更するには、**snmp trap-host** コマンドを使用します。トラップ ホストは 5 つまで指定できます。このグローバル設定モード コマンドのシンタックスは次のとおりです。

snmp trap-host *ip_or_host community_name* {**snmpv2**}

このコマンドの変数とオプションは次のとおりです。

- *ip_or_host*：トラップを受信するように設定された SNMP ホストの IP アドレスまたはホスト名。ドット付き 10 進表記の IP アドレス（192.168.11.1 など）またはニーモニック ホスト名（myhost.mydomain.com など）を入力します。
- *community_name*：トラップを特定の SNMP ホストに送信する時に使用するコミュニティ名。スペースを含まない 12 文字以内のテキスト文字列を、引用符で囲まずに入力します。
- **snmpv2**：SNMPv2 形式で送信するトラップを指定する。

たとえば、次のように入力します。

```
(config)# snmp trap-host 172.16.3.6 sqalab1 snmpv2
```

特定のトラップ ホストを削除するには、次のコマンドを入力します。

```
(config)# no snmp trap-host 172.16.3.6
```

SNMP トラップ送信元の設定

CSS で生成されたトラップに Agent-Address フィールドを設定するには、**snmp trap-source** コマンドを使用します。このコマンドは SNMPv1 だけに適用され、SNMPv2C には適用されません。このグローバル設定モードのコマンドのシンタックスは次のとおりです。

snmp trap-source [**egress-port**|**management** |**specified** *source_ip_address*]

このコマンドのオプションと変数は次のとおりです。

- **egress-port**：出力ポートに設定されている VLAN 回線 IP アドレスを使用してトラップの Agent-Address フィールドを設定する。IP アドレスは CSS により動的に決定されるので、IP アドレスを入力する必要はありません。
- **management**：イーサネット管理ポート IP アドレスを使用してトラップの Agent-Address フィールドを設定する。このオプションは、Cisco 11500 シリーズ CSS でだけ実行できます。
- **specified** *source_ip address*：トラップの Agent-Address フィールドで使用する IP アドレスを入力できる。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。

たとえば、次のように入力します。

```
(config)# snmp trap-source egress-port
```

SNMP 送信元トラップをデフォルトの管理ポート IP アドレスに戻すには、次のように入力します。

```
(config)# no snmp trap-source
```

SNMP 汎用トラップの設定

デフォルトでは、CSS で SNMP 汎用トラップ タイプは無効になっています。SNMP 汎用トラップ タイプを有効にするには、**snmp trap-type generic** コマンドを使用します。汎用 SNMP トラップは、コールド スタート、ウォーム スタート、リンク ダウン、リンク アップ、および認証失敗からなります。

（注） CSS ソフトウェアの一部としてロードされる SNMP トラップ（および関連する MIB オブジェクト）の詳細については、「CSS の SNMP トラップ」を参照してください。

たとえば、次のように入力します。

```
(config)# snmp trap-type generic
```

汎用トラップを無効にするには、次のコマンドを入力します。

```
(config)# no snmp trap-type generic
```

（注） CSS から送信されるのは、SNMP v1 トラップ タイプだけです。

SNMP 認証トラップの設定

デフォルトでは、CSS で SNMP 認証トラップの生成は無効になっています。SNMP 認証トラップを有効にするには、**snmp auth-traps** コマンドを使用します。SNMP 管理ステーションが無効なコミュニティ名でシステムへのアクセスを試みると、CSS でトラップが生成されます。

（注） **snmp trap-type generic** コマンドで SNMP 汎用トラップを有効にします。このコマンドは、システムが認証トラップを生成できるようになる前に実行する必要があります。詳細については、「SNMP 汎用トラップの設定」を参照してください。

（注）　CSS ソフトウェアの一部としてロードされる SNMP トラップ（および関連する MIB オブジェクト）の詳細については、「CSS の SNMP トラップ」を参照してください。

たとえば、次のコマンドを両方入力します。

```
(config)# snmp trap-type generic
(config)# snmp auth-traps
```

認証トラップの生成を無効にするには、次のコマンドを入力します。

```
(config)# no snmp auth-traps
```

SNMP エンタープライズ トラップの設定

デフォルトでは、CSS の SNMP エンタープライズ トラップ タイプは無効になっています。SNMP エンタープライズ トラップ タイプを有効にするには、**snmp trap-type enterprise** コマンドを使用します。エンタープライズ トラップを有効にすると、次のような場合にエンタープライズ トラップが生成されるように CSS を設定できます。

- サービス拒絶攻撃イベントが発生した場合
- ログインが失敗した場合
- CSS サービス、電源、またはレポータの状態が遷移した場合
- 電源が入っている CSS シャーシにモジュールを挿入した場合
- Inter-Switch Communications（ISC; スイッチ間通信）LifeTick 障害メッセージが生成された場合
- CSS の SSL 証明書が有効期限に達した場合
- CSS ディスクの使用領域が、設定されたしきい値以上になった場合

特定の状態が発生した場合に CSS がトラップを生成しないようにするには、**snmp trap-type enterprise** コマンドの **no** 形式を使用します。

（注）　CSS から送信されるのは、SNMP v1 トラップ タイプだけです。

CSS ソフトウェアの一部としてロードされる SNMP トラップ（および関連する MIB オブジェクト）の詳細については、「CSS の SNMP トラップ」を参照してください。DoS エンタープライズ トラップの設定方法については、「サービス運用妨害（DoS）の設定」を参照してください。

このグローバル設定モードのコマンドのシンタックスは次のとおりです。

snmp trap-type enterprise {*dos_attack_type* {**trap-threshold** *threshold_value*}|
cert-exp|**chmgr-module-transition**
|**chmgr-ps-transition** |**disk-quota** {**interval** *minutes* {**quota-threshold** *percentage*}|**isc-lifetick-failure**|**isc-state-transition**|**login-failure**
|**reload**|**redundancy-transition**|**reporter-transition**
|**service-transition**}

このコマンドのオプションは次のとおりです。

- **snmp trap-type enterprise**：エンタープライズ トラップを有効にする。エンタープライズ トラップ オプションを設定する前に、エンタープライズ トラップを有効にする必要があります。
- *dos_attack_type*：（省略可）DoS 攻撃の発生時に SNMP エンタープライズ トラップを生成する。1 秒間の攻撃数が、設定した DoS 攻撃タイプのしきい値を超えると、1 秒ごとにトラップが 1 つ生成されます。詳細については、「サービス運用妨害（DoS）の設定」の項を参照してください。
- **trap-threshold** *threshold_value*：（省略可）デフォルトのトラップしきい値をオーバーライドする。*threshold_value* には、1 ～ 65535 の数値を入力します。詳細については、「サービス運用妨害（DoS）の設定」を参照してください。
- **cert-exp**：CSS の SSL 証明書が有効期限に達した場合に SNMP エンタープライズ トラップを生成する。SSL 証明書が事前の警告期間に入ると、トラップが生成されます。デフォルトで、警告期間は有効期限の 30 日前です。トラップには、証明書名、事前の警告値、および、証明書の有効期限までの日数を示す Time To Live（TTL）の値が含まれます。TTL が負の値の場合は、有効期限が過ぎてから何日経過したかを示します。
- **chmgr-module-transition**：電源が入った Cisco 11503 シリーズ CSS や Cisco 11506 シリーズ CSS に対してモジュール（SCM、FEM、GEM など）を着脱した場合に、SNMP エンタープライズ トラップを生成する。
- **chmgr-ps-transition**：Cisco 11503 シリーズ CSS や Cisco 11506 シリーズ CSS の電源状態が変化した場合（電源のオン / オフ、または CSS シャーシからの取り外し）に、SNMP エンタープライズ トラップを生成する。

- **disk-quota**：CSS ディスク上の使用領域が、設定されているしきい値以上になった場合に、SNMP エンタープライズ トラップを有効にする。たとえば、このトラップを有効にするには、次のように入力します。

  ```
  (config)# snmp trap-type enterprise disk-quota
  ```

  ディスク領域の使用率をチェックする間隔は、デフォルトで 720 分ごとになっています。デフォルトの使用率のしきい値は 90 パーセントです。チェック間隔や使用率のしきい値を変更するには、次のオプションを使用します。

  - **interval** *minutes*：（省略可）ディスクの割り当てチェック間隔を、分単位で設定する。ここで指定した間隔で CSS ディスクの使用率がチェックされます。*minutes* 変数には、1 ～ 1440 の整数値を入力します。デフォルト値は 720 です。たとえば、チェック間隔を 1000 分に変更する場合は、次のように入力します。

    ```
    (config)# snmp trap-type enterprise disk-quota interval 1000
    ```

  - **quota-threshold** *percentage*：（省略可）ディスク割り当てのしきい値を設定する。このしきい値は、CSS ディスクの使用バイトの割合です。*percentage* 変数には、10 ～ 99 の整数値を入力します。デフォルト値は 90 です。たとえば、使用率のしきい値を 85 パーセントに変更するには、次のように入力します。

    ```
    (config)# snmp trap-type enterprise disk-quota interval 1000
    quota-threshold 85
    ```

- **isc-lifetick-failure**：Cisco 11500 シリーズ CSS で ISC LifeTick 障害メッセージが生成された場合に、SNMP エンタープライズ トラップを生成する。LifeTick メッセージは、Adaptive Session Redundancy（ASR; 適応型セッション冗長性）を設定したポート間で 1 秒間に 4 回生成されます。ソフトウェアまたはハードウェアの障害により、ポート間で 1 秒以内に LifeTick メッセージを受信できない場合に、ISC LifeTick 障害メッセージが生成されます。
- **isc-state-transition**：デュアル IISC リンクを使用する ASR 設定で、アクティブな ISC リンクがダウンし、スタンバイ リンクがアクティブになったときに、SNMP エンタープライズ トラップを生成する。ASR および ISC の詳細については、『*Cisco Content Services Switch Redundancy Configuration Guide*』を参照してください。
- **login-failure**：CSS ログイン障害の発生時に SNMP エンタープライズ トラップを生成する。CSS では、アラート レベルのログ メッセージも生成されます。
- **reload**：CSS のリブート時に SNMP エンタープライズ トラップを生成する。CSS が SNMP を利用して直接起動された場合にも、トラップが生成されます。

- **redundancy-transition**：CSS 冗長化の状態が変化した場合に、SNMP エンタープライズ トラップを生成する。
- **reporter-transition**：CSS レポータの状態が変化した場合に、SNMP エンタープライズ トラップを生成する。レポータがアクティブになった場合、レポータが一時停止した場合、または、VRID ピアリング仮想ルータや重要な物理インターフェイスの状態が変化した場合に、トラップが生成されます。
- **service-transition**：CSS サービスの状態が変化した場合に、SNMP エンタープライズ トラップを生成する。サービスがダウンしたり、ダウンしたサービスで運用が適切に再開された場合に、トラップが生成されます。

たとえば、CSS ログイン失敗の発生時に SNMP エンタープライズ トラップを有効にするには、次のコマンドを入力します。

```
(config)# snmp trap-type enterprise
(config)# snmp trap-type enterprise login-failure
```

すべてのエンタプライズ トラップを無効にするには、次のコマンドを入力します。

```
(config)# no snmp trap-type enterprise
```

有効になっている特定のエンタープライズ トラップを無効にするには、**snmp trap-type enterprise** コマンドの **no** 形式を使用します。たとえば、電源障害が発生した場合にトラップを生成しないようにするには、次のコマンドを入力します。

```
(config)# no snmp trap-type enterprise chmgr-ps-transition
```

SNMP リロード有効の設定

SNMP を使用して CSS を再度ブートするには、**snmp reload-enable** コマンドを使用します。このグローバル設定モード コマンドのシンタックスとオプションは次のとおりです。

- **snmp reload-enable**：apSnmpExtReloadSet オブジェクトへのすべての SNMP 書き込みに対して、CSS の強制リブートを許可する。このリロード オブジェクト apSnmpExtReloadSet は、1.3.6.1.4.1.9.9.368.1.22.7 に存在します。このオブジェクトは、CSS エンタープライズ MIB の snmpext.mib にあります。

- **snmp reload-enable** *reload_value*：*reload_value* と等しい SNMP 書き込みに対して、CSS の強制リブートを許可する。

（注）　このコマンドを使用するには、まず **snmp trap-type enterprise** コマンドを使用してエンタープライズ トラップを有効にする必要があります。「SNMP エンタープライズ トラップの設定」の項を参照してください。

reload_value には、SNMP ベースで再度ブートできる apSnmpExtReloadSet の制御に使用するオブジェクトを入力します。オブジェクトの設定が 0 の場合、SNMP によるリブートは行えません。オブジェクトの値を 1 ～ 2147483646 に設定すると、この値が apSnmpExtReloadSet オブジェクトに書き込まれて、リブートが行われます。*reload_value* オブジェクトの設定が 2147483647 の場合、apSnmpExtReloadSet にどの値を書き込んでも、リブートが行われる場合があります。セキュリティ保持のため、読み取り時には、このオブジェクトは常に 0 を戻します。

（注）　**snmp reload-enable** コマンドを使用して CSS を再度ブートする場合、実行設定ファイルを保存するように指示するメッセージや、再度ブートするかどうかを確認するメッセージが表示されません。このコマンドを実行する前に、必ず実行設定ファイルへの変更を保存し、CSS を再度ブートするようにしてください。

たとえば、次のように入力します。

```
(config)# snmp reload-enable
```

SNMP による CSS のリブートを行わないようにする（デフォルト動作）には、次のコマンドを入力します。

```
(config)# no snmp reload-enable
```

サービス運用妨害（DoS）の設定

特別なエンタープライズ トラップを設定して、トラップ ホストに、システムへの DoS 攻撃を通知することができます。また、CLI を使用して、DoS 攻撃についての詳しい情報を表示し、CSS の DoS 統計情報を 0 にリセットすることができます。

DoS 攻撃イベントの発生時に、CSS で SNMP エンタープライズ トラップが生成されるように設定するには、**snmp trap-type enterprise** コマンドを使用して SNMP エンタープライズ トラップを有効にしておく必要があります。詳細については、「SNMP エンタープライズ トラップの設定」の項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。

- DoS のクイック スタート
- DoS SNMP トラップ タイプの定義
- DoS 設定の表示

DoS のクイック スタート

表 5-2 は、トラップ ホストにシステムへの DoS 攻撃を通知する特殊なエンタープライズ トラップ設定に必要な手順をまとめた表です。それぞれの手順に、作業を行うために必要な CLI コマンドも示します。CLI コマンドに関する各機能とすべてのオプションの詳細については、表 5-2 以降の項を参照してください。

表 5-2　DoS 設定のクイック スタート

作業とコマンドの例
1. エンタープライズ トラップが有効になっていない場合は、有効にします。 `(config)# snmp trap-type enterprise`
2. トラップ ホストに、不正な送信元または宛先のアドレスを持っている DoS 攻撃を通知するトラップしきい値を設定します。 `(config)# snmp trap-type enterprise dos-illegal-attack trap-threshold 1`

表 5-2　DoS 設定のクイック スタート（続き）

作業とコマンドの例
3. トラップ ホストに DoS LAND 攻撃を通知するトラップしきい値を設定します。 `(config)# snmp trap-type enterprise dos-land-attack trap-threshold 1`
4. トラップ ホストに DoS スマーフ攻撃を通知するトラップしきい値を設定します。 `(config)# snmp trap-type enterprise dos-smurf-attack trap-threshold 1`
5. トラップ ホストに DoS SYN 攻撃を通知するトラップしきい値を設定します。 `(config)# snmp trap-type enterprise dos-syn-attack trap-threshold 10`

6. DoS 攻撃についての情報を表示します。
`(config)# show dos summary`
`(config)# show dos`

7. 必要に応じて、CSS の DoS 統計情報を 0 にリセットします。 `(config)# zero dos statistics`

次の実行設定例は、表 5-2 のコマンドの入力結果を表しています。

```
!************************** GLOBAL ***************************
  snmp trap-type enterprise

  snmp community techpubs read-write
  snmp contact "fred n mandy"
  snmp location "Operations"
  snmp name "arrowpoint.com"
  snmp trap-host 172.16.3.6 trap
  snmp trap-host 172.16.8.4 trap
  snmp trap-type generic
  snmp auth-traps
  snmp trap-type enterprise login-failure
  snmp reload-enable 100
  snmp trap-type enterprise dos-illegal-attack trap-threshold 1
  snmp trap-type enterprise dos-land-attack trap-threshold 1
  snmp trap-type enterprise dos-smurf-attack trap-threshold 1
  snmp trap-type enterprise dos-syn-attack trap-threshold 10
  snmp trap-type enterprise dos-illegal-attack trap-threshold 1
```

DoS SNMP トラップ タイプの定義

DoS 攻撃イベントが発生したときに CSS が SNMP エンタープライズ トラップを生成できるようにするには、**snmp trap-type enterprise** コマンドを使用します。1 秒間の攻撃数が、設定した DoS 攻撃タイプのしきい値を超えると、1 秒ごとにトラップが 1 つ生成されます。CSS ソフトウェアの一部としてロードされる SNMP トラップ（および関連する MIB オブジェクト）の詳細については、「CSS の SNMP トラップ」を参照してください。

DoS 攻撃イベントの発生時に、CSS で SNMP エンタープライズ トラップが生成されるように設定するには、**snmp trap-type enterprise** コマンドを使用して SNMP エンタープライズ トラップを有効にしておく必要があります。詳細については、「SNMP エンタープライズ トラップの設定」の項を参照してください。

このグローバル設定モードのコマンドのシンタックスは次のとおりです。

snmp trap-type enterprise *dos_attack_type* {**trap-threshold** *threshold_value*}

dos_attack_type 変数は、トラップする DoS 攻撃イベントのタイプです。オプションは、次のとおりです。

- **dos-illegal-attack**：不正な送信元または宛先のアドレスに対してトラップを生成する。不正アドレスには、ループバック送信元アドレス、ブロードキャスト送信元アドレス、ループバック宛先アドレス、マルチキャスト送信元アドレス、またはユーザが所有する送信元アドレスがあります。このタイプの攻撃のデフォルト トラップしきい値は、1 秒あたり 1 です。
- **dos-land-attack**：送信元と宛先のアドレスが同一のパケットに対してトラップを生成する。このタイプの攻撃のデフォルト トラップしきい値は、1 秒あたり 1 です。
- **dos-smurf-attack**：ブロードキャスト宛先アドレスを持つ PING 数がしきい値を超えると、トラップを生成する。このタイプの攻撃のデフォルト トラップしきい値は、1 秒あたり 1 です。
- **dos-syn-attack**：TCP 接続のうち、送信元によって開始されたが、TCP の 3 方向ハンドシェイクを完了させるための ACK（確認応答）フレームが続かない接続の数がしきい値を超えると、トラップを生成する。このタイプの攻撃のデフォルト トラップしきい値は、1 秒あたり 10 です。

デフォルト トラップしきい値を上書きするには、**trap-threshold** オプションを指定します。*threshold_value* には、1 ～ 65535 の数値を入力します。

たとえば、CSS で、送信元および宛先アドレスが同一のパケットに対してトラップを生成できるようにするには、次のコマンドを入力します。

```
(config)# snmp trap-type enterprise dos-land-attack
```

CSS で DoS 攻撃イベント トラップを生成しないようにするには、次のコマンドを入力します。

```
(config)# no snmp trap-type enterprise dos_attack_type
```

DoS 設定の表示

各 CSS Session Processor（SP; セッション プロセッサ）での DoS 攻撃に関する詳細情報を表示するには、**show dos** コマンドを使用します。**show dos** コマンドを実行すると、次のような情報が表示されます。

- CSS のブート後に発生した攻撃の合計数
- 攻撃のタイプとこれらの攻撃の 1 秒あたりの最大発生数
- その攻撃の最初と最後の発生
- 送信元と宛先の IP アドレス

CSS は、各 SP あたりの最近の攻撃イベントを最大 50 個まで表示できます。たとえば、次のように表示できます。

- 1 つの SP を持つ CSS 11501 は、最大 50 のイベント
- 最大 3 つの SP を持つ CSS 11503 は、最大 150 のイベント
- 最大 6 つの SP を持つ CSS 11506 は、最大 300 のイベント

同じ DoS タイプ、送信元と宛先アドレスで複数の攻撃が発生すると、1 つのイベントにまとめられます。このようにイベントをまとめると、表示イベントの数を削減できます。

DoS 攻撃の要約情報を表示するには、**show dos summary** コマンドを使用します。

たとえば、次のように入力します。

```
(config)# show dos summary
```

表 5-3 では、**show dos** コマンドで表示されるフィールドについて説明します。

表 5-3　show dos コマンドのフィールド

フィールド	説明
Total Attacks	CSS のブート後に検出された DoS 攻撃の合計数。次の攻撃タイプとそれぞれの発生件数が表示されます。 • **SYN Attacks**：送信元によって開始されたが、TCP の 3 方向ハンドシェイクを完了させるための ACK フレームが後に続かない TCP 接続 • **LAND Attacks**：送信元と宛先のアドレスが同一のパケット • **Zero Port Attacks**：送信元または宛先の TCP ポートまたは UDP ポートが 0 のフレーム **（注）** 旧バージョンの SmartBits ソフトウェアでは、送信元または宛先のポートを 0 に設定したフレームが送信されることがあります。CSS では、これらのフレームを DoS 攻撃として記録し、破棄します。 • **Illegal Src Attacks**：不正な送信元アドレス • **Illegal Dst Attacks**：不正な宛先アドレス • **Smurf Attacks**：ブロードキャスト宛先アドレスを持つ PING
First Attack Detected	DoS 攻撃が最初に検出された時刻
Last Attack Detected	DoS 攻撃が最後に検出された時刻

表 5-3　show dos コマンドのフィールド（続き）

フィールド	説明
Maximum per second	秒単位のイベントの最大発生数。1 秒間の最大イベント数は、SNMP トラップのしきい値を設定する場合に使用します。1 秒間の最大イベント数は、SP ごとの最大数です。 • CSS 11506 では SP を 6 台まで使用できるので、1 秒間の最大数は、このフィールドに表示されている値の 6 倍になります。 • CSS 11503 では SP を 3 台まで使用できるので、1 秒間の最大数は、このフィールドに表示されている値の 3 倍になります。
DoS Attack Event	検出された各攻撃イベントの詳細（SP ごとに最大 50 イベントまで）
First Attack	攻撃イベントが最初に発生した時刻
Last Attack	攻撃イベントが最後に発生した時刻
Source/Destination Address	攻撃イベントの送信元および宛先アドレス
Event Type	イベントのタイプ
Total Attacks	イベントで発生した攻撃の合計数

DoS 統計情報のリセット

CSS の DoS 統計情報を 0 にリセットするには、いずれかのモードで **zero dos statistics** コマンドを使用します。このコマンドを実行すると、**show dos** コマンドで表示される DoS 統計情報のフィールドの値が 0 になります。**show dos** コマンドの詳細については、「DoS 設定の表示」の項を参照してください。

SNMP 設定の表示

SNMP の設定を終えたら、SNMP 設定を表示します。たとえば、次のように入力します。

```
(config)# show running-config global
```

show running-config コマンドとその出力については、第 1 章「CSS ソフトウェアの管理」を参照してください。

CSS での SNMP の管理

ここでは、CSS で SNMP を管理するために必要な作業について説明します。内容は次のとおりです。

- SNMP マネージャによる CSS へのアクセスの有効化
- CSS を使用した MIB オブジェクトの検索
- ログの表示
- RMON アラームの設定

SNMP マネージャによる CSS へのアクセスの有効化

デフォルトで、CSS は SNMP がコマンド ベースにアクセスできるようにしています。ただし、CSS で SNMP を使用するには、まず、**snmp community** コマンドを使用してコミュニティ ストリングを作成する必要があります。詳細については、「SNMP コミュニティの設定」の項を参照してください。

（注）　SNMP は、安全なネットワーク環境ではありません。ネットワークを保護するためには、SNMP を単独で使用しないでください。

CSS を使用した MIB オブジェクトの検索

MIB オブジェクト、およびそのオブジェクトを構成する変数を検索するには、次の手順を実行します。

1. 次のコマンドを入力して、グローバル設定モードにアクセスします。

   ```
   # config
   ```

2. 次のコマンドを入力して、RMON アラーム モードにアクセスします。

   ```
   (config)# rmon-alarm index_number
   ```

   index_number には RMON アラーム インデックスを指定します。RMON アラーム インデックスを使用して、CSS へのアラームを識別します。RMON については、第 6 章「RMON の設定」を参照してください。

3. 次のコマンドを入力して、MIB オブジェクトを表示します。

```
(config-rmonalarm[1])# lookup object
```

object には MIB オブジェクト名を指定します。

特定のオブジェクトを検索するか、または目的のオブジェクトを検索するためのワイルドカードとして疑問符（?）を使用することができます。

たとえば、検索する MIB の正確な名前がわからないが、目的の MIB が apFlowMgrExt オブジェクト グループの一部だということはわかっている場合、次のように、**lookup** コマンドで疑問符（**?**）を使用します。

```
(config-rmonalarm[1])# lookup apFlowMgrExt?

apFlowMgrExtDoSAttackEventType
apFlowMgrExtDoSAttackEventCount
apFlowMgrExtDoSAttackIndex
apFlowMgrExtDosTotalSmurfAttacks
apFlowMgrExtDosTotalIllegalSourceAttacks
apFlowMgrExtDosTotalZeroPortAttacks
apFlowMgrExtDosTotalLandAttacks
apFlowMgrExtDosTotalSynAttacks
apFlowMgrExtDosTotalAttacks
apFlowMgrExtIdleTimer
apFlowMgrExtPortIdleValue
apFlowMgrExtPortIdle
apFlowMgrExtReserveCleanTimer
apFlowMgrExtPermanentPort4
apFlowMgrExtPermanentPort3
apFlowMgrExtPermanentPort2
apFlowMgrExtPermanentPort1
apFlowMgrExtFlowTraceDuration
apFlowMgrExtFlowTraceMaxFileSize
apFlowMgrExtFlowTraceState
```

上記の例では、ワイルドカードとして疑問符（?）を使用した結果、apFlowMgrExt MIB オブジェクトに関する情報が返されています。疑問符を使用せずに目的の MIB を指定して **lookup** コマンドを実行すると、その MIB の詳細を表示できます。たとえば、次のようになります。

```
(config-rmonalarm[1])# lookup apFlowMgrExtDOSAttackEventCount

ASN Name:           apFlowMgrExtDOSAttackEventCount
MIB:                flowmgrext
Object Identifier:  1.3.6.1.4.1.9.9.368.1.36.27.1.6
Argument Type:      Integer
Range:              0-4294967295
Description:
   This is the number of times this DoS attack had occurred.
```

また、次の例のように、**lookup** コマンドに MIB オブジェクト名を指定しないで、すべてのエンタープライズ MIB のリストを表示することもできます。

```
(config-rmonalarm[1])# lookup ?
```

lookup コマンドでは、*string* および *MAC address* のタイプの MIB オブジェクトが省略されます。

有用な MIB 統計情報

表 5-4 に、CSS に関する有用な情報を提供する MIB グループの一部を示します。

表 5-4　CSS の MIB 情報

MIB 名	説明
RFC 1398	イーサネット統計情報
RFC 1493	ブリッジ情報
RFC 1757	RMON 統計情報
svcExt.mib	サービス変数（TCP 接続を含む）
cntExt.mib	コンテンツ ルール変数（フレーム統計情報を含む）
ownExt.mib	所有者統計情報（フレーム数とバイト数を含む）

表 5-4　CSS の MIB 情報（続き）

MIB 名	説明
cntsvcExt.mib	コンテンツ ルールごとのサービスに関する統計情報（フレーム数、バイト数、ヒット数を含む）
chassis MgrExt	CSS シャーシの情報を表示する。また、スロット番号とポート番号を ifIndex 番号に関連付けることができる。

ログの表示

traplog ファイルには、汎用トラップおよびエンタープライズ トラップの両方について、発生したトラップがすべて書き込まれます。ネットワーク装置は、SNMP トラップ設定が有効かどうかを traplog ファイルに書き込みます。

トラップログ ファイルのサイズが最大の大きさ（ハード ディスクを使用する CSS の場合は 50MB、フラッシュ ディスクを使用する CSS の場合は 10MB）に達すると、トラップログ ファイルの名前が traplog.prev に変わります。このファイルは、バックアップ ファイルとして保存され、新しいトラップログ ファイルが作成されます。トラップログ ファイルの名前が変わると、既存のバックアップ トラップログ ファイルは上書きされます。CSS を再度ブートしても、最大サイズに達するまで、既存のトラップログ ファイルが使用されます。

前回の CSS リブート以降のトラップ ログを表示するには、**show log** コマンドを使用します。たとえば、次のように入力します。

```
# show log traplog
```

デフォルトでは、次のイベントで critical-2 レベルのメッセージが生成されます。

- リンク アップ
- リンク ダウン
- コールド スタート
- ウォーム スタート
- サービスの停止
- サービスの一時停止

この他のすべての SNMP トラップでは、デフォルトで notice-5 メッセージが生成されます。

RMON アラームの設定

RMON アラームを使用すると、MIB オブジェクトが目的の遷移状態になっているか監視できます。RMON アラーム モードで使用できるコマンドについては、第 6 章「RMON の設定」を参照してください。

CSS の SNMP トラップ

表 5-5 および 表 5-6 に、CSS でサポートされる SNMP v1 トラップと SNMP v2C トラップの一覧をそれぞれ示します。

表 5-5　SNMP v1 トラップ

MIB 名	エンタープライズ オブジェクト ID（OID）	汎用	固有	パラメータ
coldStart	<sysObjectID>	0	0	----------
warmStart	<sysObjectID	1	0	----------
linkDown	<sysObjectID>	2	0	ifIndex 1.3.6.1.2.1.2.2.1.1 ifOperStatus 1.3.6.1.2.1.2.2.1.8 ifAdminStatus 1.3.6.1.2.1.2.2.1.7
linkUp	<sysObjectID>	3	0	ifIndex 1.3.6.1.2.1.2.2.1.1 ifOperStatus 1.3.6.1.2.1.2.2.1.8 ifAdminStatus 1.3.6.1.2.1.2.2.1.7
authenticationFailure	<sysObjectID>	4	0	----------
egpNeighborLoss	<sysObjectID>	5	0	----------
apFlowMgrExtDosSynTrap (flowMgrExt.mib)	1.3.6.1.4.1.9.9.368.1.36.1	6	1	apFlowMgrExtDOSAttackEventString 1.3.6.1.4.1.9.9.368.1.36.28.1.8 apFlowMgrExtDOSAttackEventIntervalCount 1.3.6.1.4.1.9.9.368.1.36.28.1.9 apFlowMgrExtDOSAttackEventCount 1.3.6.1.4.1.9.9.368.1.36.28.1.6

表 5-5　SNMP v1 トラップ（続き）

MIB 名	エンタープライズ オブジェクト ID（OID）	汎用	固有	パラメータ
apFlowMgrExtDosLandTrap (flowMgrExt.mib)	1.3.6.1.4.1.9.9.368.1.36.1	6	2	apFlowMgrExtDOSAttackEventString 1.3.6.1.4.1.9.9.368.1.36.28.1.8 apFlowMgrExtDOSAttackEventIntervalCount 1.3.6.1.4.1.9.9.368.1.36.28.1.9 apFlowMgrExtDOSAttackEventCount 1.3.6.1.4.1.9.9.368.1.36.28.1.6
apFlowMgrExtDosIllegalTrap (flowMgrExt.mib)	1.3.6.1.4.1.9.9.368.1.36.1	6	3	apFlowMgrExtDOSAttackEventString 1.3.6.1.4.1.9.9.368.1.36.28.1.8 apFlowMgrExtDOSAttackEventIntervalCount 1.3.6.1.4.1.9.9.368.1.36.28.1.9 apFlowMgrExtDOSAttackEventCount 1.3.6.1.4.1.9.9.368.1.36.28.1.6
apFlowMgrExtDosSmurfTrap (flowMgrExt.mib)	1.3.6.1.4.1.9.9.368.1.36.1	6	5	apFlowMgrExtDOSAttackEventString 1.3.6.1.4.1.9.9.368.1.36.28.1.8 apFlowMgrExtDOSAttackEventIntervalCount 1.3.6.1.4.1.9.9.368.1.36.28.1.9 apFlowMgrExtDOSAttackEventCount 1.3.6.1.4.1.9.9.368.1.36.28.1.6
apIpv4RedundancyTrap (apIpv4.mib)	1.3.6.1.4.1.9.9.368.1.9.1.1	6	1	apIpv4TrapEventText 1.3.6.1.4.1.9.9.368.1.9.34.0 apIpv4RedundancyState 1.3.6.1.4.1.9.9.368.1.9.19.0 apIpv4RedundancyIf 1.3.6.1.4.1.9.9.368.1.9.20.0 apIpv4RedundancyMaster 1.3.6.1.4.1.9.9.368.1.9.21.0

表 5-5　SNMP v1 トラップ（続き）

MIB 名	エンタープライズ オブジェクト ID（OID）	汎用	固有	パラメータ
apIpv4RedundancyState Transition (apIpv4Redundancy.mib)	1.3.6.1.4.1.9.9.368.1.9.8.1	6	1	apIpv4RedundancyEventText 1.3.6.1.4.1.9.9.368.1.9.8.9.0 apIpv4RedundancyVRIntAddr 1.3.6.1.4.1.9.9.368.1.9.8.2.1.2 apIpv4RedundancyVRID 1.3.6.1.4.1.9.9.368.1.9.8.2.1.1 apIpv4RedundancyVROperState 1.3.6.1.4.1.9.9.368.1.9.8.2.1.13 apIpv4RedundancyVRFailReason 1.3.6.1.4.1.9.9.368.1.9.8.2.1.14 apIpv4RedundancyVRMasterIP 1.3.6.1.4.1.9.9.368.1.9.8.2.1.8
apSnmpExtReloadTrap (snmpExt.mib)	1.3.6.1.4.1.9.9.368.1.22.1	6	1	apSnmpExtTrapEventText 1.3.6.1.4.1.9.9.368.1.22.27.0
apSnmpExtReporterTraps (snmpExt.mib)	1.3.6.1.4.1.9.9.368.1.68.1	6	1	apReporterTrapEventText 1.3.6.1.4.1.9.9.368.1.68.7.0
apSvcTransitionTrap (svcExt.mib)	1.3.6.1.4.1.9.9.368.1.15.1	6	1	apSvcTrapEventText 1.3.6.1.4.1.9.9.368.1.15.10.0
apTermSessLoginFailureTrap (terminalMgmt.mib)	1.3.6.1.4.1.9.9.368.1.11.1	6	1	apTermSessLoginFailureInfo 1.3.6.1.4.1.9.9.368.1.11.3.0
apChassisMgrExtPsTrap (chassisMgrExt.mib)	1.3.6.1.4.1.9.9.368.1.34.1	6	1	apChassisMgrExtTrapPsEventText 1.3.6.1.4.1.9.9.368.1.34.24.0
apChassisMgrModuleTrap (chassisMgrExt.mib)	1.3.6.1.4.1.9.9.368.1.34.1	6	2	apChassisMgrExtTrapModuleEventText 1.3.6.1.4.1.9.9.368.1.34.25.0

表 5-5　SNMP v1 トラップ（続き）

MIB 名	エンタープライズ オブジェクト ID（OID）	汎用	固有	パラメータ
apEnetISCLifetickTrap (enetExt.mib)	1.3.6.1.4.1.9.9.368.1.39.1	6	1	apEnetISCLifetickEventText 1.3.6.1.4.1.9.9.368.1.39.8.0
apEnetISCStateTransition (enetExt.mib)	1.3.6.1.4.1.9.9.368.1.39.1	6	2	apEnetISCEventText 1.3.6.1.4.1.9.9.368.1.39.13.0 apEnetISCState 1.3.6.1.4.1.9.9.368.1.39.10.0 apEnetISCPortOneFailureReason 1.3.6.1.4.1.9.9.368.1.39.11.0 apEnetISCPortTwoFailureReason 1.3.6.1.4.1.9.9.368.1.39.12.0

表 5-6　SNMP v2C トラップ

MIB 名	エンタープライズ オブジェクト ID （OID）	パラメータ
coldStart	1.3.6.1.6.3.1.1.5.1	————————
warmStart	1.3.6.1.6.3.1.1.5.2	————————
linkDown	1.3.6.1.6.3.1.1.5.3	ifIndex 1.3.6.1.2.1.2.2.1.1 ifOperStatus 1.3.6.1.2.1.2.2.1.8 ifAdminStatus 1.3.6.1.2.1.2.2.1.7
linkUp	1.3.6.1.6.3.1.1.5.4	ifIndex 1.3.6.1.2.1.2.2.1.1 ifOperStatus 1.3.6.1.2.1.2.2.1.8 ifAdminStatus 1.3.6.1.2.1.2.2.1.7

表 5-6　SNMP v2C トラップ（続き）

MIB 名	エンタープライズ オブジェクト ID （OID）	パラメータ
authenticationFailure	1.3.6.1.6.3.1.1.5.5	————————
egpNeighborLoss	1.3.6.1.6.3.1.1.5.6	————————
apFlowMgrExtDosSynTrap (flowMgrExt.mib)	1.3.6.1.4.1.9.9.368.1.36.1.0.1	apFlowMgrExtDOSAttackEventString 1.3.6.1.4.1.9.9.368.1.36.28.1.8 apFlowMgrExtDOSAttackEventIntervalCount 1.3.6.1.4.1.9.9.368.1.36.28.1.9 apFlowMgrExtDOSAttackEventCount 1.3.6.1.4.1.9.9.368.1.36.28.1.6
apFlowMgrExtDosLandTrap (flowMgrExt.mib)	1.3.6.1.4.1.9.9.368.1.36.1.0.2	apFlowMgrExtDOSAttackEventString 1.3.6.1.4.1.9.9.368.1.36.28.1.8 apFlowMgrExtDOSAttackEventIntervalCount 1.3.6.1.4.1.9.9.368.1.36.28.1.9 apFlowMgrExtDOSAttackEventCount 1.3.6.1.4.1.9.9.368.1.36.28.1.6
apFlowMgrExtDosIllegalTrap (flowMgrExt.mib)	1.3.6.1.4.1.9.9.368.1.36.1.0.3	apFlowMgrExtDOSAttackEventString 1.3.6.1.4.1.9.9.368.1.36.28.1.8 apFlowMgrExtDOSAttackEventIntervalCount 1.3.6.1.4.1.9.9.368.1.36.28.1.9 apFlowMgrExtDOSAttackEventCount 1.3.6.1.4.1.9.9.368.1.36.28.1.6
apFlowMgrExtDosSmurfTrap (flowMgrExt.mib)	1.3.6.1.4.1.9.9.368.1.36.1.0.5	apFlowMgrExtDOSAttackEventString 1.3.6.1.4.1.9.9.368.1.36.28.1.8 apFlowMgrExtDOSAttackEventIntervalCount 1.3.6.1.4.1.9.9.368.1.36.28.1.9 apFlowMgrExtDOSAttackEventCount 1.3.6.1.4.1.9.9.368.1.36.28.1.6

表 5-6　SNMP v2C トラップ（続き）

MIB 名	エンタープライズ オブジェクト ID （OID）	パラメータ
apIpv4RedundancyTrap (apIpv4.mib)	1.3.6.1.4.1.9.9.368.1.9.1.1.0.1	apIpv4TrapEventText 1.3.6.1.4.1.9.9.368.1.9.34.0 apIpv4RedundancyState 1.3.6.1.4.1.9.9.368.1.9.19.0 apIpv4RedundancyIf 1.3.6.1.4.1.9.9.368.1.9.20.0 apIpv4RedundancyMaster 1.3.6.1.4.1.9.9.368.1.9.21.0
apIpv4RedundancyStateTransition (apIpv4Redundancy.mib)	1.3.6.1.4.1.9.9.368.1.9.8.1.0.1	apIpv4RedundancyEventText 1.3.6.1.4.1.9.9.368.1.9.8.9.0 apIpv4RedundancyVRIntAddr 1.3.6.1.4.1.9.9.368.1.9.8.2.1.2 apIpv4RedundancyVRID 1.3.6.1.4.1.9.9.368.1.9.8.2.1.1 apIpv4RedundancyVROperState 1.3.6.1.4.1.9.9.368.1.9.8.2.1.13 apIpv4RedundancyVRFailReason 1.3.6.1.4.1.9.9.368.1.9.8.2.1.14 apIpv4RedundancyVRMasterIP 1.3.6.1.4.1.9.9.368.1.9.8.2.1.8
apSnmpExtReloadTrap (snmpExt.mib)	1.3.6.1.4.1.9.9.368.1.22.1.0.1	apSnmpExtTrapEventText 1.3.6.1.4.1.9.9.368.1.22.27.0
apSnmpExtReporterTraps (snmpExt.mib)	1.3.6.1.4.1.9.9.368.1.68.1.0.1	apReporterTrapEventText 1.3.6.1.4.1.9.9.368.1.68.7.0
apSvcTransitionTrap (svcExt.mib)	1.3.6.1.4.1.9.9.368.1.15.1.0.1	apSvcTrapEventText 1.3.6.1.4.1.9.9.368.1.15.10.0
apTermSessLoginFailureTrap (terminalMgmt.mib)	1.3.6.1.4.1.9.9.368.1.11.1.0.1	apTermSessLoginFailureInfo 1.3.6.1.4.1.9.9.368.1.11.3.0

表 5-6　SNMP v2C トラップ（続き）

MIB 名	エンタープライズ オブジェクト ID （OID）	パラメータ
apChassisMgrExtPsTrap (chassisMgrExt.mib)	1.3.6.1.4.1.9.9.368.1.34.1.0.1	apChassisMgrExtTrapPsEventText 1.3.6.1.4.1.9.9.368.1.34.24.0
apChassisMgrModuleTrap (chassisMgrExt.mib)	1.3.6.1.4.1.9.9.368.1.34.1.0.2	apChassisMgrExtTrapModuleEventText 1.3.6.1.4.1.9.9.368.1.34.25.0
apEnetISCLifetickTrap (enetExt.mib)	1.3.6.1.4.1.9.9.368.1.39.1.0.1	apEnetISCLifetickEventText 1.3.6.1.4.1.9.9.368.1.39.8.0
apEnetISCStateTransition (enetExt.mib)	1.3.6.1.4.1.9.9.368.1.39.1.0.2	apEnetISCEventText 1.3.6.1.4.1.9.9.368.1.39.13.0 apEnetISCState 1.3.6.1.4.1.9.9.368.1.39.10.0 apEnetISCPortOneFailureReason 1.3.6.1.4.1.9.9.368.1.39.11.0 apEnetISCPortTwoFailureReason 1.3.6.1.4.1.9.9.368.1.39.12.0

CSS MIB

表 5-7 は、CSS エンタープライズ MIB（オブジェクト識別子 1.3.6.1.4.1.9.9.368）のすぐ下にある CSS MIB オブジェクトの説明です。この表の MIB は、CSS コンテンツ固有の MIB オブジェクトです。オブジェクト情報の検索方法については、「CSS を使用した MIB オブジェクトの検索」を参照してください。

表 5-7　CSS エンタープライズ MIB の下にある MIB ブランチ

MIB ファイル名	MIB モジュールの説明	関連する CLI コマンド
aclExt.mib (OID 1.3.6.1.4.1.9.9.368.1.23)	CSS ACL 句のテーブル	`(config-acl)# ?`

ap64Stats.mib
(OID 1.3.6.1.4.1.9.9.368.1.44)
	RMON（RFC 1757）、MIB-II（RFC 1213）および EtherErrors（RFC 1398）の 64 ビット統計情報集計	`# show rmon ?`
		`# show mibii ?`
		`# show ether-errors ?`

cisco-apent.mib (OID 1.3.6.1.4.1.9.9.368.1)	CSS エンタープライズ MIB ブランチ階層	――――――――――
apIpv4.mib (OID 1.3.6.1.4.1.9.9.368.1.9.1)	IPv4 グローバル情報の MIB サポート（ボックスツーボックス冗長設定）	`(config)# ip ?`
apIpv4Arp.mib (OID 1.3.6.1.4.1.9.9.368.1.9.4)	IPv4 ARP の MIB サポート	`(config)# arp ?`
apIpv4Dns.mib (OID 1.3.6.1.4.1.9.9.368.1.9.7)	IPv4 DNS リゾルバ設定の MIB サポート	`(config)# dns ?`
apIpv4Host.mib (OID 1.3.6.1.4.1.9.9.368.1.9.6)	IPv4 ホストテーブルの MIB サポート	`(config)# host ?`
apIpv4Interface.mib (OID 1.3.6.1.4.1.9.9.368.1.9.2)	IPv4 インターフェイス用の MIB サポート（ボックスツーボックス冗長設定）	`(config-ip)# ?`
apIpv4Ospf.mib (OID 1.3.6.1.4.1.9.9.368.1.9.3.2)	Open Shortest Path First（OSPF）プロトコルの MIB サポート	`(config)# ospf ?`
apIpv4Redundancy.mib (OID 1.3.6.1.4.1.9.9.368.1.9.8)	IPv4 冗長性の MIB サポート	`(config-ip)# redundancy ?`

表 5-7　CSS エンタープライズ MIB の下にある MIB ブランチ（続き）

MIB ファイル名	MIB モジュールの説明	関連する CLI コマンド
apIpv4Rip.mib (OID 1.3.6.1.4.1.9.9.368.1.9.3.1)	Routing Information Protocol（RIP; ルーティング情報プロトコル）の MIB サポート	(config-ip)# **rip ?**
apIpv4Sntp.mib (OID 1.3.6.1.4.1.9.9.368.1.9.9)	SNTP 用の MIB サポート	(config)# **sntp ?**
apIpv4StaticRoutes.mib (OID 1.3.6.1.4.1.9.9.368.1.9.5)	IPv4 スタティック ルートの MIB サポート	(config)# **ip route ?**
appExt.mib (OID 1.3.6.1.4.1.9.9.368.1.32)	Application Peering Protocol（APP）設定の MIB サポート	(config)# **app ?**
boomClientExt.mib (OID 1.3.6.1.4.1.9.9.368.1.62)	Content Routing Agent（CRA; コンテンツ ルーティング エージェント）パラメータの設定と監視	(config)# **dns-boomerang client ?**
bootExt.mib (OID 1.3.6.1.4.1.9.9.368.1.31)	システム ブート管理の MIB サポート	(config-boot)# **?**
bridgeExt.mib (OID 1.3.6.1.4.1.9.9.368.1.14)	ブリッジ関連パラメータの設定と監視	(config)# **bridge ?**
cappUdpExt.mib (OID 1.3.6.1.4.1.9.9.368.1.52)	Application Peering Protocol-User Datagram Protocol（APP-UDP）グローバル統計情報およびセキュリティ設定	(config)# **app-udp ?**
cctExt.mib (OID 1.3.6.1.4.1.9.9.368.1.29)	CSS 回線情報（ボックスツーボックス冗長設定）	(config)# **circuit ?**
chassisMgrExt.mib (OID 1.3.6.1.4.1.9.9.368.1.34)	CSS シャーシ マネージャ用の MIB	# **show chassis ?**
cntdnsExt.mib (OID 1.3.6.1.4.1.9.9.368.1.41)	コンテンツ ルールの DNS の統計情報	(config)# **dns hotlist ?**
cntExt.mib (OID 1.3.6.1.4.1.9.9.368.1.16)	コンテンツ ルール テーブル	(config-owner-content)# **?**
cnthotExt.mib (OID 1.3.6.1.4.1.9.9.368.1.35)	コンテンツ ルールのホット リスト	(config-owner-content)# **hotlist ?**

表 5-7　CSS エンタープライズ MIB の下にある MIB ブランチ（続き）

MIB ファイル名	MIB モジュールの説明	関連する CLI コマンド
cntLctSvcExt.mib (OID 1.3.6.1.4.1.9.9.368.1.67)	ロケーション クッキーの MIB サポート	(config-owner-content)# **add location-service ?** (config-owner-content)# **remove location-service ?**
cntsvcExt.mib (OID 1.3.6.1.4.1.9.9.368.1.18)	コンテンツ ルールに関連付けられているサービスの監視	(config-owner-content)# **add service ?** (config-owner-content)# **remove service ?**
csaExt.mib (OID 1.3.6.1.4.1.9.9.368.1.59)	CSS への Client Side Accelerator（CSA; クライアント側アクセラレータ）パラメータの設定と監視	(config)# **dns-server ?**
dfpExt.mib (OID 1.3.6.1.4.1.9.9.368.1.65)	Dynamic Feedback Protocol（DFP）の統計情報と設定向けの MIB サポート	(config)# **dfp ?**
dnshotExt.mib (OID 1.3.6.1.4.1.9.9.368.1.48)	DNS ホット リスト	(config)# **domain hotlist ?**
dnsServerExt.mib (OID 1.3.6.1.4.1.9.9.368.1.40)	DNS サーバの MIB サポート	(config)# **dns-server ?**
domainCacheExt.mib (OID 1.3.6.1.4.1.9.9.368.1.60)	CSS の CSA でのドメイン キャッシュの設定管理	(config)# **dns-server domain-cache ?**
dqlExt.mib (OID 1.3.6.1.4.1.9.9.368.1.51)	Domain Qualifier List（DQL; ドメイン修飾子リスト）	(config-dql [name])# **?**
enetExt.mib (OID 1.3.6.1.4.1.9.9.368.1.39)	イーサネット ポートの PHY 状態の設定	(config-interface)# **phy ?**
eqlExt.mib (OID 1.3.6.1.4.1.9.9.368.1.42)	Extension Qualifier List（EQL; 拡張子修飾子リスト）	(config-eql [name])#
fileExt.mib (OID 1.3.6.1.4.1.9.9.368.1.61)	CSS とのネットワーク管理情報の移動をサポートし、既存のファイル構造を検査および修正するためのファイル拡張子	――――――――――

表 5-7　CSS エンタープライズ MIB の下にある MIB ブランチ（続き）

MIB ファイル名	MIB モジュールの説明	関連する CLI コマンド
flowMgrExt.mib (OID 1.3.6.1.4.1.9.9.368.1.36)	フロー マネージャ モジュール用の MIB	(config)# **flow ?**
ftpExt.mib (OID 1.3.6.1.4.1.9.9.368.1.30)	FTP 転送管理レコードの MIB サポート	(config)# **ftp-record ?**
grpExt.mib (OID 1.3.6.1.4.1.9.9.368.1.17)	すべてのグループ関連パラメータの設定	(config-group)# **?**
grpsvcExt.mib (OID 1.3.6.1.4.1.9.9.368.1.19)	サービスに関連するグループ	(config-group)# **add service ?** (config-group)# **remove service ?**
httpExt.mib (OID 1.3.6.1.4.1.9.9.368.1.47)	HTTP 転送管理レコードの MIB サポート	————————
kalExt.mib (OID 1.3.6.1.4.1.9.9.368.1.46)	キープアライブ モードの設定	(config-keepalive)# **?**
logExt.mib (OID 1.3.6.1.4.1.9.9.368.1.20)	CSS ロギング機能	(config)# **logging ?**
nqlExt.mib (OID 1.3.6.1.4.1.9.9.368.1.50)	CSS network qualifier list（NQL; ネットワーク修飾子リスト）の説明	(config-nql [name])# **?**
ownExt.mib (OID 1.3.6.1.4.1.9.9.368.1.25)	Web ホストの所有者情報	(config-owner)# **?**
plucExt.mib (OID 1.3.6.1.4.1.9.9.368.1.56)	プロキシミティ検索クライアント機能	(config)# **proximity cache ?**
probeRttExt.mib (OID 1.3.6.1.4.1.9.9.368.1.55)	階層型プロキシミティ サービス RTT プローブ モジュール機能	(config)# **proximity probe rtt ?**
proxDbExt.mib (OID 1.3.6.1.4.1.9.9.368.1.54)	階層型 Proximity Database（PDB; プロキシミティ データベース）機能で、すべての設定、統計情報、およびメトリック オブジェクトを格納	(config)# **proximity db ?**
publishExt.mib (OID 1.3.6.1.4.1.9.9.368.1.57)	パブリッシャ サービスとサブスクライバ サービス	(config-service)# **publisher ?**

表 5-7　CSS エンタープライズ MIB の下にある MIB ブランチ（続き）

MIB ファイル名	MIB モジュールの説明	関連する CLI コマンド
qosExt.mib (OID 1.3.6.1.4.1.9.9.368.1.28)	CSS MIB モジュールの QoS クラス定義（認識されるコンテンツの QoS クラス）	――――――――
radiusClientExt.mib (OID 1.3.6.1.4.1.9.9.368.1.12)	Remote Access Dial-in User Service（RADIUS）認証プロトコルのクライアント側に対する CSS の拡張機能	(config)# **radius-server ?**
ciscoCssReporter.mib (OID 1.3.6.1.4.1.9.9.368.1.68.1)	CSS レポータ、CSS レポータに関連する重要な物理インターフェイス、および CSS レポータに関連する VRID ピアリング仮想ルータ用の MIB サポート	(config)# **reporter ?** (config-reporter)# **phy ?** (config-reporter)# **vrid ?**
schedExt.mib (OID 1.3.6.1.4.1.9.9.368.1.45)	CLI コマンド スケジューラ レコードの MIB サポート	(config)# **cmd-scheduler ?**
securityMgrExt.mib (OID 1.3.6.1.4.1.9.9.368.1.13)	ネットワーク セキュリティ マネージャの CSS MIB オブジェクト	(config)# **username ?**
snmpExt.mib (OID 1.3.6.1.4.1.9.9.368.1.22)	SNMP トラップと SNMP コミュニティ	(config)# **snmp ?**
sshdExt.mib (OID 1.3.6.1.4.1.9.9.368.1.43)	Secure Shell Daemon（SSHD）サーバの MIB サポート	(config)# **sshd ?**
sslExt.mib (OID 1.3.6.1.4.1.9.9.368.1.63)	Secure Sockets Layer（SSL）アクセラレーション モジュールで SSL の認証とキーを使用するための　SSL ファイル関連付け用 MIB サポート	(config)# **ssl cert ?** (config)# **ssl rsakey ?** (config)# **ssl dakey ?** (config)# **ssl dhparam ?**
ssllExt.mib (OID 1.3.6.1.4.1.9.9.368.1.64)	SSL アクセラレーション モジュールで使用する SSL プロキシ リスト要素と暗号スイート オブジェクト用の MIB サポート	(ssl-proxy-list[name])# **element ?**
subscribeExt.mib (OID 1.3.6.1.4.1.9.9.368.1.58)	CSS エンタープライズの加入者	(config-service)# **subscriber ?**

表 5-7　CSS エンタープライズ MIB の下にある MIB ブランチ（続き）

MIB ファイル名	MIB モジュールの説明	関連する CLI コマンド
svcExt.mib (OID 1.3.6.1.4.1.9.9.368.1.15)	すべてのサービス関連パラメータの設定と監視	(config-service)# ?
tacacsExt.mib (OID 1.3.6.1.4.1.9.9.368.1.66)	Terminal Access Controller Access Control System （TACACS+）認証プロトコルのクライアント側に対する CSS の拡張機能	(config)# **tacacs-server ?**
tagExt.mib (OID 1.3.6.1.4.1.9.9.368.1.53)	コンテンツ タグ リスト	(config)# **header-field-group ?**
terminalMgmt.mib (OID 1.3.6.1.4.1.9.9.368.1.11)	端末オプションの MIB サポート	# **terminal ?** # **restrict ?**
urqlExt.mib (OID 1.3.6.1.4.1.9.9.368.1.49)	Uniform resource locator qualifier list（URQL; URL 修飾子リスト）	(config-urql [name])# ?

以降の内容について

第 6 章「RMON の設定」では、CSS で RMON を設定する方法について説明します。