CHAPTER 16

MIB のサポート

この章では、Cisco 3200 シリーズ モバイル アクセス ルータでサポートされる MIB について説明します。

一般的な MIB

- BRIDGE-MIB
- CISCO-BULK-FILE-MIB
- CISCO-CDP-MIB
- CISCO-CIRCUIT-INTERFACE-MIB
- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-ENVMON-MIB
- CISCO-FLASH-MIB
- CISCO-FTP-CLIENT-MIB
- CISCO-IMAGE-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-NTP-MIB
- CISCO-NBAR-PROTOCOL-DISCOVERY-MIB
- CISCO-PROCESS-MIB
- CISCO-STACKMAKER-MIB
- CISCO-SYSLOG-MIB
- ENTITY-MIB
- IF-MIB
- OLD-CISCO-CHASSIS-MIB
- OLD-CISCO-CPU-MIB
- OLD-CISCO-FLASH-MIB
- OLD-CISCO-INTERFACES-MIB
- OLD-CISCO-MEMORY-MIB

- OLD-CISCO-SYS-MIB
- OLD-CISCO-SYSTEM-MIB
- RFC 1213-MIB（MIBII）
- SNMPv2-MIB

ワイヤレス MIB

- IEEE802dot11-MIB
- Q-BRIDGE-MIB
- P-BRIDGE-MIB
- CISCO-DOT11-IF-MIB
- CISCO-WLAN-VLAN-MIB
- CISCO-IETF-DOT11-QOS-MIB
- CISCO-IETF-DOT11-QOS-EXT-MIB
- CISCO-DOT11-ASSOCIATION-MIB
- CISCO-DDP-IAPP-MIB
- CISCO-IP-PROTOCOLFILTER-MIB
- CISCO-SYSLOG-EVENTEXT-MIB
- CISCO-TBRIDGE-DEV-IFMIB

ルーティングおよびルーテッド プロトコル MIB

- CISCO-MOBILE-IP-MIB
- CISCO-PING-MIB
- CISCO-TCP-MIB
- OLD-CISCO-IP-MIB
- OLD-CISCO-TCP-MIB
- RFC 1253-MIB（OSPF）
- TCP-MIB
- UDP-MIB
- RFC 2006-MIB
- BGP4-MIB
- CISCO-BGP4-MIB

LAN および WAN MIB

- RFC 1398-MIB（イーサネット）
- CISCO-DIAL-CONTROL-MIB
- CISCO-FRAME-RELAY-MIB
- RFC 1315-MIB（フレーム リレー）
- RFC 1381-MIB（LAPB）
- RFC1382-MIB（X.25）
- RS-232-MIB

IP マルチキャスト MIB

- CISCO-IPMROUTE-MIB
- CISCO-PIM-MIB
- IGMP-STD-MIB
- IPMROUTE-MIB
- IPMROUTE-STD-MIB
- MSDP-MIB
- PIM-MIB

IPSEC/VPN MIB

- CISCO-IPSEC-MIB
- CISCO-IPSEC-FLOW-MONITOR-MIB
- CISCO-IPSEC-POLICY-MAP-MIB
- CISCO-VPDN-MGMT-MIB

QOS MIB

- CISCO-CAR-MIB
- CISCO-IP-STAT-MIB
- CISCO-QUEUE-MIB
- INT-SERV-MIB
- INT-SERV-GUARANTEED-MIB
- RSVP-MIB
- CISCO-CLASS-BASED-QOS-MIB
- CISCO-PPPOE-MIB

ネットワーク管理 MIB

- CISCO-RTTMON-MIB

VLAN MIB

- CISCO- VLAN-MEMBERSHIP-MIB
- CISCO-VTP-MIB
- CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB

モバイル IP MIB のサポート

Simple Network Management Protocol（SNMP）機能に対するモバイル IP MIB サポートにより、外部エージェント エンティティとホーム エージェント モバイル IP エンティティのネットワーク監視機能および管理機能を拡張する MIB モジュールが追加されます。モバイル IP SNMP を使用したの管理は、RFC 2006-MIB および CISCO-MOBILE-IP-MIB の 2 つの MIB で定義されます。

RFC 2006-MIB は、RFC 2006『*The Definitions of Managed Objects for IP Mobility Support Using SMIv2*』内の定義を使用する MIB モジュールです。Cisco IOS Release 12.2(1)T から、RFC 2006 Set オペレーションと SNMP 通知（トラップ）がサポートされます。Network Management System（NMS; ネットワーク管理システム）から実行する Set オペレーションで、モバイル IP サービスの開始と停止、セキュリティ アソシエーションの修正と削除、アドバタイズ パラメータの修正、および外部エージェントの Care-of Address（CoA; 気付アドレス）の設定に RFC 2006-MIB を使用できます。IOS ソフトウェアを使用するサポート対象ルーティング デバイスでは、セキュリティ違反に関する SNMP 通知もイネーブルにできます。

CISCO-MOBILE-IP-MIB は、RFC 2006-MIB をシスコが企業向けに拡張したものです。CISCO-MOBILE-IP-MIB により、ホーム エージェントのモビリティ バインディング合計数と、外部エージェント ビジターのバインディング合計数を NMS を使用してモニタリングできます。これらのバインディングは、CISCO-MOBILE-IP-MIB ではそれぞれ *cmiHaRegTotalMobilityBindings* および *cmiFaRegTotalVisitors* として定義されています。

このマニュアルの作業は、デバイス上に SNMP とモバイル IP を設定していることを前提にしています。SNMP Set オペレーションを通じて mipAssocTable 内のセキュリティ アソシエーションを修正および削除できるので、SNMPv3 を使用することを強く推奨します。

選択されたプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに対応する MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。

http://tools.cisco.com/ITDIT/MIBS/servlet/index

必要な MIB 情報が Cisco MIB Locator でサポートされていない場合は、次の URL にある Cisco MIB ページからサポート対象 MIB のリストを入手して、MIB をダウンロードすることもできます。

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Cisco MIB Locator にアクセスするには、Cisco.com のアカウントが必要です。アカウント情報を忘れた場合や紛失した場合は、cco-locksmith@cisco.com に空の E メールを送信してください。送信された E メール アドレスが Cisco.com に登録されているかどうかが自動的にチェックされます。チェックに成功すると、アカウントの詳細と新規のランダム パスワードが E メールで通知されます。承認されたユーザは次の URL の指示に従って、Cisco.com のアカウントを設定できます。

http://www.cisco.com/register

モバイル IP MIB のメリット

RFC 2006-MIB は、セキュリティ違反が発生した場合に NMS へ送信されるモバイル IP エンティティ（ホーム エージェントまたは外部エージェント）の通知を定義します。この通知は、侵入元を特定するのに使用できます。

また、RFC 2006-MIB は、モバイル IP エンティティのセキュリティ違反を記録するテーブル（*mipSecViolationTable*）も定義します。このログを NMS から取り出して（Get オペレーションを使用）、システムのセキュリティ違反事例の分析に使用できます。

CISCO-MOBILE-IP-MIB を使用して、ホーム エージェント モビリティ バインディングの合計数をモニタリングできます。これ以降、ホーム エージェントの現在の負荷のスナップショットを表示できます。これはネットワーク内の負荷を任意の時間に測定し、キャパシティ プランニングを追跡するのに重要です。

モバイル IP MIB の制約事項

RFC 2006-MIB のオブジェクトおよびテーブルで Set オペレーションを使用する場合、次の制約事項が課せられます。

- mipEnable オブジェクト：ルータ上でモバイル IP サービスを開始および停止するのに使用できます。このオブジェクトについては、Set サポートの問題はありません。
- faRegistrationRequired オブジェクト：モバイル ノードを外部エージェントに登録するかどうかを制御します。シスコはモバイル IP を実装しているので、CLI（コマンドライン インターフェイス）を使用してこのパラメータをインターフェイス レベルで設定できます。ただし、このオブジェクトは、MIB ではインターフェイス レベルで定義されません。したがって、このオブジェクトでは SNMP オペレーションは実行できません。
- mipSecAssocTable：異なるモバイル IP エンティティ（ホーム エージェント、外部エージェント、およびモバイル ノード）間ですでに設定されているセキュリティ アソシエーションを、管理ステーションで表示/修正できます。このテーブルのインデックス オブジェクトは、エンティティの IP アドレスと Security Parameter Index（SPI）です。SNMP を使用してこのテーブルに新しい行を作成したり、または削除したりするためのオブジェクトはありません。表 16-1 に mipSecAssocTable のオブジェクトの固定値を示します。

表 16-1　RFC 2006-MIB mipSecAssocTable オブジェクトの固定セキュリティ メソッド

オブジェクト	固定セキュリティ メソッド値
mipSecAlgorithmType	MD5
mipSecAlgorithmMod	prefixSuffix
mipSecReplayMethod	タイムスタンプ

Set オペレーションに mipSecKey オブジェクト値を設定した場合、この値は印字可能な ASCII 値を含んでいる場合は ASCII キーとして解釈されます。それ以外では、キーは 16 進数の文字列として解釈されます。

このテーブルには rowStatus オブジェクトがないため、このテーブルの行を削除する場合は mipSecKey オブジェクトを特別な値に設定します。既存のセキュリティ アソシエーションは、mipSecKey オブジェクトをすべて 0 に設定すると削除できます。

- maAdvConfigTable：このテーブルで、モビリティ エージェントのすべてのアドバタイズ インターフェイスのアドバタイズ パラメータを修正できます。このテーブルに rowStatus オブジェクトが存在していても行の作成と削除は行うことができません。新しい行の作成は、ホーム エージェントまたは外部エージェント サービスが新しい行に対応するインターフェイス上で開始することを意味するためです。

  しかし、このテーブル内にはサービス（ホーム エージェントまたは外部エージェント）の開始を指定するオブジェクトはありません。したがって、外部エージェントまたはホーム エージェント サービスがイネーブルになった各インターフェイスには、すでに 1 つの行が対応していることになります。

  maAdvResponseSolicitaionOnly オブジェクトの値が TRUE の場合、このテーブルの maAdvMaxInterval オブジェクト、maAdvMinInterval オブジェクト、および maAdvMaxAdvLifetime オブジェクトはインスタンス生成されません。

  行に対応するインターフェイスが起動していない場合、行は notReady ステートに移行します。

- faCOATable：このテーブルで外部エージェントに CoA を設定できます。このテーブルには、rowStatus オブジェクトとテーブルのインデックスの 2 つのオブジェクトがあります。このテーブルで設定できるオブジェクトは 1 つだけであるため（rowStatus）、createAndWait rowStatus を使用した行の作成はサポートされていません。また、このテーブルの行に対して、notInService ステートはサポートされていません。

  （このテーブルの行で設定された）CoA に対応するインターフェイスが起動していない場合、行のステータスは notReady になります。起動していないインターフェイスに対応する行は新しく作成できません。

モバイル IP MIB 通知の送信

モバイル IP MIB の SNMP 機能のサポートは、ネットワーク管理アプリケーション（通常は外部 NMS で実行する GUI（グラフィカル ユーザ インターフェイス）プログラム）に情報を提供することを目的としています。モバイル IP MIB オブジェクトは、SNMP の Set、Get、Get-next、および Get-bulk オペレーションを使用して NMS から読み込むことができます。通知タイプ *ipmobile* をイネーブルにすると、トラップと情報を NMS に送信することもできます。

モバイル IP トラップまたは情報をホストに送信するようにルータを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# snmp-server enable traps ipmobile`	SNMP で使用するためにモバイル IP 通知（トラップと情報）の送信をイネーブルにします。
`Router(config)# snmp-server host` *host-addr* [**traps** | **informs**][**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] **ipmobile**	モバイル IP のトラップまたは情報の受信者（ホスト）を指定します。

単純な Set または Get の SNMP 要求を処理するために、システムでモバイル IP 通知をイネーブルにする必要はないことに注意してください。

必要な snmp-server コマンドがコンフィギュレーション ファイル内にあることを確認するには、**more system:running-config** コマンドまたは **show running-config** コマンドを使用します。

モバイル IP のセキュリティ違反通知の設定例

次の例では、モバイル IP のセキュリティ違反の通知が情報としてホスト myhost.cisco.com に送信されています。コミュニティ ストリングは private1 と定義されています。

```
snmp-server enable traps ipmobile
snmp-server host myhost.cisco.com informs version 3 auth private1
```

モバイル IP の Simple Network Management Protocol（SNMP）セキュリティ通知をイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps ipmobile** コマンドを使用します。モバイル IP の SNMP 通知をディセーブルにするには、このコマンドの **no** 形式を使用します。

SNMP モバイル IP の通知をトラップまたは情報要求として送信できます。このコマンドはトラップと情報の両方の要求をイネーブルにします。

snmp-server enable traps ipmobile コマンドは、**snmp-server host** コマンドと併せて使用されます。SNMP の通知を受信するホストを指定する場合は、**snmp-server host** グローバル コンフィギュレーション コマンドを使用します。SNMP の通知を送信する場合は、1 つ以上の **snmp-server host** を設定する必要があります。

SNMP 通知オペレーションの受信者を指定する場合は、グローバル コンフィギュレーション モードで **snmp-server host** コマンドを使用します。指定したホストを削除するには、このコマンドの **no** 形式を使用します。

キーワードを使用せずにこのコマンドを入力すると、デフォルトですべてのトラップ タイプがホストに送信されます。このホストに情報は送信されません。

version キーワードが指定されていなければ、デフォルトはバージョン 1 です。キーワードを何も指定しない **no snmp-server host** コマンドは、ホストに対して、情報ではなくトラップの送信をディセーブルにします。情報をディセーブルにするためには、**no snmp-server host informs** コマンドを使用します。

（注） このコマンドを使用する前に、**snmp-server community** コマンドで*コミュニティ ストリング*が定義されていない場合、**snmp-server community** コマンドのデフォルト形式がコンフィギュレーションに自動的に挿入されます。このような **snmp-server community** の自動設定に使用されるパスワード（*community-string*）は、**snmp-server host** コマンドで指定されるものに等しくなります。これは Cisco IOS Release 12.0(3) 以降のリリースでのデフォルト動作です。

SNMP の通知をトラップ要求または情報要求として送信できます。トラップは、受信側が受領しても確認応答を送信しないため信頼できません。送信側はトラップが受領されたかどうかを判断できません。ただし、情報要求を受け取る SNMP エンティティは、SNMP 応答 PDU でメッセージを確認します。送信側が応答を受け取らなければ、情報要求を再送信できます。このため情報の方が目的の宛先に到着する確率が高くなります。

ただし、情報はエージェントとネットワークでリソースを多く消費します。送信された直後に廃棄されるトラップとは異なり、情報要求は応答が受領されるか要求がタイムアウトになるまでメモリ内に保持する必要があります。またトラップが一度だけ送信されるのに対し、情報は数回再送信を試みることができます。この再試行によってトラフィックが増加し、ネットワーク上のオーバーヘッド増加につながります。

通知を送信するには、**snmp-server host** グローバル コンフィギュレーション コマンドを入力します。SNMP の通知を送信するようにルータを設定する場合は、1 つ以上の **snmp-server host** コマンドを入力する必要があります。キーワードを指定せずにコマンドを入力すると、ホストのすべてのトラップ タイプがイネーブルになります。

複数のホストをイネーブルにする場合は、各ホストに個別に **snmp-server host** コマンドを発行する必要があります。ホストごとにコマンドで複数の通知タイプを指定できます。

同じホストおよび通知の種類（トラップまたは情報）に対して複数の **snmp-server host** コマンドを指定した場合、後続のコマンドによって前のコマンドが上書きされます。最後の **snmp-server host** コマンドのみが有効になります。たとえば、あるホストに **snmp-server host inform** コマンドを入力し、そのあとで同じホストにもう一度 **snmp-server host inform** コマンドを入力すると、最初のコマンドは 2 つ目のコマンドによって置換されます。

snmp-server host コマンドは、**snmp-server enable** グローバル コンフィギュレーション コマンドと併せて使用されます。グローバルに送信する SNMP 通知を指定する場合は、**snmp-server enable** コマンドを使用します。大部分の通知を受信するホストについては、1 つ以上の **snmp-server enable** コマンドおよびそのホストの **snmp-server host** コマンドをイネーブルにする必要があります。

ただし、一部のタイプの通知は **snmp-server enable** コマンドで制御できません。たとえば、いくつかの通知タイプは常にイネーブルです。また別のコマンドによってイネーブルになる通知タイプもあります。たとえば、linkUpDown 通知は **snmp trap link-status** グローバル コンフィギュレーション コマンドによって制御されます。これらの通知タイプは **snmp-server enable** コマンドを要求しません。

通知タイプ オプションのアベイラビリティは、ルータのタイプとそのルータでサポートされる Cisco IOS ソフトウェア機能に依存します。たとえば、**envmon** 通知タイプが使用できるのはシステムに環境モニタが組み込まれている場合のみです。システムで使用できる通知タイプを確認する場合、**snmp-server host** コマンドの最後に **?** コマンドを使用します。

トラップに固有の SNMP コミュニティ ストリングを設定し、SNMP がこのストリングを使用してポーリング アクセスしないようにする場合は、コンフィギュレーションにアクセス リストを組み込む必要があります。次の例では、コミュニティ ストリングの名前は comaccess、アクセス リストの番号は 10 です。

```
snmp-server community comaccess ro 10
snmp-server host 172.20.2.160 comaccess
access-list 10 deny any
```

次の例では、myhost.cisco.com という名前で指定されたホストに RFC 1157 SNMP トラップを送信しています。他のトラップはイネーブルになっていますが、**snmp-server host** コマンドに **snmp** のみが指定されているため、SNMP トラップのみが送信されます。コミュニティ ストリングは comaccess と定義されています。

```
snmp-server enable traps
snmp-server host myhost.cisco.com comaccess snmp
```

次の例では、SNMP およびシスコ環境モニタの企業固有のトラップをアドレス 172.30.2.160 に送信しています。

```
snmp-server enable traps snmp
snmp-server enable traps envmon
snmp-server host 172.30.2.160 public snmp envmon
```

次の例では、コミュニティ ストリング public を使用してルータからホスト myhost.cisco.com にすべてのトラップを送信します。

```
snmp-server enable traps
snmp-server host myhost.cisco.com public
```

次の例では、ホストにトラップが送信されません。BGP トラップはすべてのホストでイネーブルになっていますが、ホストへの送信がイネーブルになっているのは ISDN トラップのみです。

```
snmp-server enable traps bgp
snmp-server host bob public isdn
```

次の例では、コミュニティ ストリング public を使用してルータからホスト myhost.cisco.com にすべての情報要求を送信します。

```
snmp-server enable traps
snmp-server host myhost.cisco.com informs version 2c public
```

次の例では、ホスト myhost.cisco.com に Hot Standby Router Protocol（HSRP）MIB 情報を送信します。コミュニティ ストリングは public として定義されます。

```
snmp-server enable traps hsrp
snmp-server host myhost.cisco.com informs version 2c public hsrp
```

ワークグループ ブリッジ SNMP リンク トラップの例

ワークグループ ブリッジで SNMP リンク トラップを生成するには、ブリッジに次のコマンドを入力する必要があります。

```
snmp-server trap-source Dot11Radio0
snmp-server enable traps snmp linkdown linkup
snmp-server host 1.7.35.35 version
```

トラップを受信するデバイスの IP アドレスは、ファスト イーサネット VLAN インターフェイスの IP アドレスではなく、モバイル アクセス ルータ ループバック インターフェイスのスタティック IP アドレスにする必要があります。これは、Dynamic Host Configuration Protocol（DHCP）がイネーブルの場合、ファスト イーサネット インターフェイスの IP アドレスがダイナミックになるためです。

通常モバイル アクセス ルータのファスト イーサネット インターフェイスに送信される SNMP パケットをループバック インターフェイスに強制的に送信するには、次のコマンドを入力します。

arp *1.7.35.35 00ff.ff40.0087* **ARPA BVI1**

ここで、*1.7.35.35 00ff.ff40.0087* はモバイル アクセス ルータのファスト イーサネット インターフェイスの MAC アドレスです。

SNMP パケットおよびインフラストラクチャ モードの VLAN 環境にあるルート デバイスに関連付けられたワークグループ ブリッジで生成された非ネイティブ VLAN トラフィックを転送する場合は、モバイル アクセス ルータのファスト イーサネット インターフェイスで VLAN トランキングをオンにする必要があります。WGB では **wgb vlan** コマンドを使用しないでください。

ワークグループ ブリッジの SNMP マネージャはモバイル アクセス ルータ側にスタティック IP アドレスを必要としているため、ワークグループ ブリッジ上に IP アドレスを持つループバック インターフェイスを追加する必要があります。次に、SNMPv3 の設定例を示します。

ワークグループ ブリッジ

```
interface Loopback0
 ip address 1.2.3.4 255.255.0.0
 no ip route-cache

snmp-server group labgrp v3 noauth
snmp-server user labusr labgrp v3
snmp-server trap-source Loopback0
snmp-server enable traps snmp linkdown linkup
no snmp-server enable traps tty
snmp-server enable traps disassociate
snmp-server enable traps deauthenticate
snmp-server host 1.7.35.35 version 3 noauth labusr
```

モバイル アクセス ルータ

```
snmp-server engineID remote 1.2.3.4 <WGB SNMP engineID>
snmp-server user labusr labgrp remote 1.2.3.4 v3
snmp-server group labgrp v3 noauth
snmp-server manager
snmp-server manager session-timeout <num>
2.authNoPriv:
interface Loopback0
 ip address 1.2.3.4 255.255.0.0
 no ip route-cache

snmp-server group labgrp v3 auth
snmp-server user labusr labgrp v3 auth md5 MD5passwd
snmp-server trap-source Loopback0
snmp-server enable traps snmp linkdown linkup
no snmp-server enable traps tty
snmp-server enable traps disassociate
snmp-server enable traps deauthenticate
snmp-server host 1.7.35.35 version 3 auth labusr
```

モバイル アクセス ルータ

```
snmp-server engineID remote 1.2.3.4 <WGB SNMP engineID>
snmp-server user labusr labgrp remote 1.2.3.4 v3 auth md5 MD5passwd
snmp-server group labgrp v3 auth
snmp-server manager
snmp-server manager session-timeout <num>
```

MIB ファイルの FTP

FTP を使用して個別の MIB ファイルを取得するには、次の手順を実行します。

ステップ 1　FTP を使用してサーバ **ftp.cisco.com** にアクセスします。

ステップ 2　ユーザ名 **anonymous** を使用してログインします。

ステップ 3　パスワードが要求されたら、E メールのユーザ名を入力します。

ステップ 4　`ftp>` プロンプトで、ディレクトリを **/pub/mibs/v1** または **/pub/mibs/v2** に変更します。

ステップ 5　**get** *MIB_filename* コマンドを使用して、MIB ファイルのコピーを入手します。

（注）　次の Cisco Web サイトでも MIB に関する情報にアクセスできます。
http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml