



Cisco IME での SNMP の設定

SNMP バージョン 3 には、認証（要求が本物の送信元から送られていることの確認）、プライバシー（データの暗号化）、許可（ユーザが要求した操作を許可されていることの確認）、アクセス制御（ユーザが要求したオブジェクトへのアクセス権を所持していることの確認）などのセキュリティ機能が備わっています。ネットワークで SNMP パケットが漏えいしないようにするために、SNMPv3 では暗号化を設定できます。

この章では、ネットワーク管理システムで Cisco IME を監視できるようにするために、SNMP v3 を設定する方法を説明します。この章は、次の内容で構成されています。

- 「SNMP 設定チェックリスト」(P.9-1)
- 「SNMP ユーザ」(P.9-3)
- 「SNMP トラップ通知の宛先」(P.9-4)
- 「MIB2 システム グループ」(P.9-7)

SNMP 設定チェックリスト

表 9-1 に、SNMP を設定するための手順の概要を示します。

表 9-1 SNMP 設定チェックリスト

設定手順	関連する手順と項目
ステップ 1 SNMP NMS をインストールおよび設定します。	NMS をサポートする SNMP 製品ドキュメント
ステップ 2 CLI で、次の SNMP サービスがシステムで開始されたことを確認します。 <ul style="list-style-type: none">• SNMP Master Agent• Native Agent• System Application Agent• Cisco Syslog Agent• MIB2 Agent• Host Resources Agent	Cisco IME コマンドラインで、次のコマンドを入力します。 utils service list
ステップ 3 SNMP ユーザを設定します。	「SNMP ユーザ」(P.9-3)
ステップ 4 トラップまたはインフォームの通知先を設定します。	<ul style="list-style-type: none">• 「SNMP トラップ通知の宛先」(P.9-4)• 「SNMP インフォーム通知の宛先」(P.9-5)

表 9-1 SNMP 設定チェックリスト (続き)

設定手順	関連する手順と項目
ステップ 5 システム接点および MIB2 システム グループのロケーションを設定します。	「MIB2 システム グループ」(P.9-7)
ステップ 6 CISCO-SYSLOG-MIB のトラップ設定を設定します。	次のガイドラインを使用して、システムで CISCO-SYSLOG-MIB トラップ設定を設定します。 <ul style="list-style-type: none"> SNMP Set 操作を使用して <code>clogNotificationEnabled</code> (1.3.6.1.4.1.9.9.41.1.1.2) を true に設定します。たとえば、linux コマンドラインから <code>net-snmp set ユーティリティ</code> を使用して、この OID を true に設定します。以下を使用します：<code>snmpset -c <community string> -v2c <transmitter ipaddress> 1.3.6.1.4.1.9.9.41.1.1.2.0 i 1</code> SNMP Set 操作に対し、その他の SNMP 管理アプリケーションも使用できます。 SNMP Set 操作を使用して <code>clogMaxSeverity</code> (1.3.6.1.4.1.9.9.41.1.1.3) 値を設定します。たとえば、linux コマンドラインから <code>net-snmp set ユーティリティ</code> を使用して、この OID 値を設定します。以下を使用します：<code>snmpset -c public -v2c 1<transmitter ipaddress> 1.3.6.1.4.1.9.9.41.1.1.3.0 i <value></code> <p><value> 設定に対し重大度を示す数値を入力します。重大度値が大きいほど、重大度がより低いことを示します。値 1 (緊急) は最も高い重大度を示し、値 8 (デバッグ) は最も低い重大度を示します。Syslog Agent は、指定した重大度値よりも大きい重大度値のメッセージを無視します。たとえば、すべての syslog メッセージをトラップするには、値 8 を使用します。</p>
ステップ 7 SNMP Master Agent サービスを再起動します (オプション)。 ヒント <code>utils snmp config</code> コマンドを実行した後、システムにより SNMP Master Agent エージェントが自動的に再起動されます。	Cisco IME コマンドラインで、次のコマンドを入力します。 <code>utils service start SNMP Master Agent</code>
ステップ 8 NMS で、Cisco IME トラップパラメータを設定します。	<ul style="list-style-type: none"> 「SNMP Managed Information Base (MIB; 管理情報ベース)」(P.9-9) NMS をサポートする SNMP 製品ドキュメント

追加情報

「関連項目」(P.9-12) を参照してください。

SNMP ユーザ

表 9-2 に、Cisco IME サーバで SNMP ユーザを操作するために必要なコマンドを示します。

表 9-2 トレースの CLI コマンド

タスク	コマンド
SNMP ユーザをリストする。	utils snmp config user 3 list
SNMP ユーザを追加する。	utils snmp config user 3 add システムにより、パラメータを要求するプロンプトが表示されます。パラメータの名前と説明については、表 9-3 を参照してください。
SNMP ユーザを更新する。	utils snmp config user 3 update システムにより、パラメータを要求するプロンプトが表示されます。パラメータの名前と説明については、表 9-3 を参照してください。
SNMP ユーザを削除する。	utils snmp config user 3 delete システムにより、パラメータを要求するプロンプトが表示されます。パラメータの名前と説明については、表 9-3 を参照してください。

SNMP ユーザの CLI パラメータ

表 9-3 で、V3 の SNMP ユーザ パラメータの設定について説明します。

表 9-3 V3 の SNMP ユーザ パラメータの設定

フィールド	説明
username	アクセス権を付与するユーザの名前。名前には、最大 32 の文字を指定でき、英数字、ハイフン (-)、およびアンダースコア (_) を任意に組み合わせて指定できます。 ヒント ネットワーク管理システム (NMS) に対して設定したユーザを入力します。
authprotocol	認証プロトコル。HMAC-SHA を指定するには、SHA と入力します。
authpassphrase	認証プロトコルのパスワードを指定します。パスワードは 8 文字以上指定する必要があります。
privprotocol	プライバシー プロトコル (AES128、AES192、または AES256) を指定します。
privpassphrase	プライバシー プロトコルのパスワードを指定します。パスワードは 8 文字以上指定する必要があります。

表 9-3 V3 の SNMP ユーザ パラメータの設定 (続き)

フィールド	説明
accessprivilege	<p>アクセス レベルに関する次のオプションのいずれかを入力します。</p> <ul style="list-style-type: none"> • ReadOnly : ユーザは MIB オブジェクトの値を読み取ることのみできます。 • ReadWrite : ユーザは MIB オブジェクトの値を読み取ること、および書き込むことができます。 • ReadWriteNotify : ユーザは、MIB オブジェクトの値を読み取ること、および書き込むことができ、さらにトラップ メッセージおよびインフォーム メッセージに関する MIB オブジェクト値を送信できます。 • NotifyOnly : ユーザは、トラップ メッセージおよびインフォーム メッセージに関する MIB オブジェクト値を送信することのみできます。 • ReadNotifyOnly : ユーザは、MIB オブジェクトの値を読み取ることができ、さらにトラップ メッセージおよびインフォーム メッセージに関する値を送信できます。 • None : ユーザは、トラップ情報を読み取ること、書き込むこと、および送信することができません。 <p>ヒント トラップ設定パラメータを変更するには、ユーザに NotifyOnly、ReadNotifyOnly、または ReadWriteNotify 特権を設定する必要があります。</p>
ipaddress1	<p>パケットを受け取る送信元の IP アドレスを指定します。デフォルトでは、すべてのホストからのパケットを受け取るように指定されます。</p>
ipaddress2	<p>パケットを受け取る送信元の IP アドレスを指定します。デフォルトでは、すべてのホストからのパケットを受け取るように指定されます。</p>

追加情報

「[関連項目](#)」(P.9-12) を参照してください。

SNMP トラップ通知の宛先

SNMP エージェントは、重要なシステム イベントを示すために、トラップまたはインフォームの形式で NMS に通知を送信します。トラップでは宛先からの確認応答を受信しますが、インフォームでは確認応答は受信しません。

次の項は、SNMP V3 通知宛先設定に適用されます。

表 9-4 に、Cisco IME サーバで SNMP トラップ通知宛先を操作するために必要なコマンドを示します。

表 9-4 SNMP トラップ通知宛先の CLI コマンド

タスク	コマンド
トラップ通知の宛先をリストする。	utils snmp config trap 3 list
設定済みの v3 ユーザ名に関連する v3 トラップ通知宛先を追加する。	utils snmp config trap 3 add システムにより、パラメータを要求するプロンプトが表示されます。パラメータの名前と説明については、表 9-5 を参照してください。
トラップ通知宛先を更新する。	utils snmp config trap 3 update システムにより、パラメータを要求するプロンプトが表示されます。パラメータの名前と説明については、表 9-5 を参照してください。
トラップ通知宛先を削除する。	utils snmp config trap 3 delete システムにより、パラメータを要求するプロンプトが表示されます。パラメータの名前と説明については、表 9-5 を参照してください。

トラップ通知宛先のパラメータの設定

表 9-5 で、V3 のトラップ通知宛先パラメータの設定について説明します。

表 9-5 V3 のトラップ通知宛先パラメータの設定

フィールド	説明
ipaddress	通知宛先のホスト IP アドレス。
portno	宛先サーバの通知受信ポート番号。
oldportno	現在設定されている宛先サーバの通知受信ポート番号。
newportno	トラップ通知宛先の更新時に使用する宛先サーバの通知受信ポート番号。
username	通知宛先に関連する SNMP ユーザを指定します。

追加情報

「関連項目」(P.9-12) を参照してください。

SNMP インフォーム通知の宛先

SNMP エージェントは、重要なシステム イベントを示すために、トラップまたはインフォームの形式で NMS に通知を送信します。トラップでは宛先からの確認応答を受信しますが、インフォームでは確認応答は受信しません。

表 9-6 で、V3 のインフォーム通知宛先の設定について説明します。

表 9-6 SNMP インフォーム通知宛先の CLI コマンド

タスク	コマンド
インフォーム通知の宛先をリストする。	utils snmp config inform 3 list
v3 インフォーム通知の宛先を追加する。	utils snmp config inform 3 add システムにより、パラメータを要求するプロンプトが表示されます。パラメータの名前と説明については、表 9-7 を参照してください。
インフォーム通知の宛先を更新する。	utils snmp config inform 3 update システムにより、パラメータを要求するプロンプトが表示されます。パラメータの名前と説明については、表 9-7 を参照してください。
インフォーム通知の宛先を削除する。	utils snmp config inform 3 delete システムにより、パラメータを要求するプロンプトが表示されます。パラメータの名前と説明については、表 9-7 を参照してください。

インフォーム通知宛先のパラメータの設定

表 9-7 V3 のインフォーム通知宛先パラメータの設定

フィールド	説明
ipaddress	通知宛先のホスト IP アドレス。
portno	宛先サーバの通知受信ポート番号。
oldportno	現在設定されている宛先サーバの通知受信ポート番号。
newportno	インフォーム通知宛先の更新時に使用する宛先サーバの通知受信ポート番号。
username	通知宛先に関連する SNMP ユーザを指定します。
oldusername	インフォームに現在関連付けられている v3 ユーザ名を指定します。
newusername	インフォームに関連付ける v3 ユーザ名を指定します。
deleteuserconf	Y または N を使用して、古いユーザの削除を確定するかどうか指定します。
authprotocol	認証プロトコル。HMAC-SHA を指定するには、SHA と入力します。
authpassphrase	認証プロトコルのパスワードを指定します。パスワードは 8 文字以上指定する必要があります。
privprotocol	プライバシー プロトコル (AES128、AES192、または AES256) を指定します。
privpassphrase	プライバシー プロトコルのパスワードを指定します。パスワードは 8 文字以上指定する必要があります。

表 9-7 V3 のインフォーム通知宛先パラメータの設定 (続き)

フィールド	説明
accessprivilege	<p>アクセス レベルに関する次のオプションのいずれかを入力します。</p> <ul style="list-style-type: none"> • ReadWriteNotify : ユーザは、MIB オブジェクトの値を読み取ること、および書き込むことができ、さらにトラップ メッセージおよびインフォーム メッセージに関する MIB オブジェクト値を送信できます。 • NotifyOnly : ユーザは、トラップ メッセージおよびインフォーム メッセージに関する MIB オブジェクト値を送信することのみできます。 • ReadNotifyOnly : ユーザは、MIB オブジェクトの値を読み取ることができ、さらにトラップ メッセージおよびインフォーム メッセージに関する値を送信できます。
engineId	インフォーム メッセージを送信する先のサーバのリモートエンジン ID を指定します。

追加情報

「[関連項目](#)」(P.9-12) を参照してください。

MIB2 システム グループ

CLI を使用して、MIB-II システム グループのシステム接点およびシステム ロケーション オブジェクトを設定できます。たとえば、システム接点として Administrator, 555-121-6633 と入力すること、およびシステム ロケーションとして San Jose, Bldg 23, 2nd floor と入力することができます。

表 9-8 に、Cisco IME サーバで MIB2 システム グループを操作するために必要なコマンドを示します。

表 9-8 MIB2 の CLI コマンド

タスク	コマンド
MIB2 システム グループ設定をリストする。	utils snmp config mib2 list
MIB2 システム グループを追加する。	utils snmp config mib2 add システムにより、パラメータを要求するプロンプトが表示されます。パラメータの名前と説明については、表 9-9 を参照してください。
MIB2 システム グループを更新する。	utils snmp config mib2 update システムにより、パラメータを要求するプロンプトが表示されます。パラメータの名前と説明については、表 9-9 を参照してください。
MIB2 システム グループを削除する。	utils snmp config mib2 delete システムにより、パラメータを要求するプロンプトが表示されます。パラメータの名前と説明については、表 9-9 を参照してください。

MIB2 システム グループの CLI パラメータ

表 9-9 で、MIB2 システム グループのパラメータの設定について説明します。

表 9-9 MIB2 システム グループのパラメータの設定

フィールド	説明
Server	接点を設定する対象のサーバ。
SysContact	問題発生時に通知するユーザを指定します。
SysLocation	システム接点として指定するユーザのロケーションを指定します。

追加情報

「[関連項目](#)」(P.9-12) を参照してください。

SNMP Managed Information Base (MIB; 管理情報ベース)

SNMP では、Managed Information Base (MIB; 管理情報ベース) にアクセスできます。MIB は、階層的に編成された情報の集合です。MIB は、オブジェクト ID で識別される管理対象オブジェクトにより構成されます。管理対象デバイスの特定の特性が格納される MIB オブジェクトは、1 つ以上のオブジェクト インスタンス (変数) で構成されます。

SNMP インターフェイスは、次の Cisco 標準 MIB を提供しています。

- CISCO-CDP-MIB
- CISCO-SYSLOG-MIB

Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) 拡張エージェントは、サーバに常駐し、CISCO-CCM-MIB を公開します。CISCO-CCM-MIB は、サーバが認識しているデバイスに関する詳細情報を提供します。クラスタ構成の場合、SNMP 拡張エージェントはクラスタ内の各サーバに常駐します。CISCO-CCM-MIB は、サーバのデバイス登録ステータス、IP アドレス、説明、モデル タイプなど、デバイス情報を提供します (クラスタをサポートする構成でも、クラスタではなくサーバの情報が提供されます)。

SNMP インターフェイスは、次の業界標準 MIB も提供しています。

- SYSAPPL-MIB
- MIB-II (RFC 1213)
- HOST-RESOURCES-MIB

ベンダーが固有にサポートしているハードウェア MIB については、「[ベンダー固有の MIB](#)」項を参照してください。

Cisco IME SNMP インターフェイスは、次の MIB をサポートしています。

CISCO-CDP-MIB

Cisco Discovery Protocol MIB、CISCO-CDP-MIB を読み取るには、Cisco Unified Communications Manager CDP サブエージェントを使用します。この MIB により、Cisco IME はそれ自体をネットワーク上の他のシスコ デバイスにアダプタイズできます。

CDP サブエージェントは CDP-MIB を実装しています。CDP-MIB には、次のオブジェクトが含まれます。

- cdpInterfaceIfIndex
- cdpInterfaceMessageInterval
- cdpInterfaceEnable
- cdpInterfaceGroup
- cdpInterfacePort
- cdpGlobalRun
- cdpGlobalMessageInterval
- cdpGlobalHoldTime
- cdpGlobalLastChange
- cdpGlobalDeviceId
- cdpGlobalDeviceIdFormat
- cdpGlobalDeviceIdFormatCpd

SYSAPPL-MIB

インストールされているアプリケーション、アプリケーション コンポーネント、システムで実行されているプロセスなどの情報を SYSAPPL-MIB から取得するには、System Application Agent を使用します。

System Application Agent は、SYSAPPL-MIB の次のオブジェクト グループをサポートしています。

- sysApplInstallPkg
- sysApplRun
- sysApplMap
- sysApplInstallElmt
- sysApplElmtRun

MIB-II

MIB-II から情報を取得するには、MIB2 エージェントを使用します。MIB2 エージェントは、インターフェイス、IP など、RFC 1213 で定義されている変数へのアクセスを提供します。MIB2 エージェントは、次のオブジェクト グループをサポートしています。

- system
- interfaces
- at
- ip
- icmp
- tcp
- udp
- snmp

HOST-RESOURCES MIB

HOST-RESOURCES-MIB から値を取得するには、Host Resources Agent を使用します。Host Resources Agent は、ストレージ リソース、プロセス テーブル、デバイス情報、インストールされているソフトウェア ベースなど、ホスト情報への SNMP アクセスを提供します。Host Resources Agent は、次のオブジェクト グループをサポートしています。

- hrSystem
- hrStorage
- hrDevice
- hrSWRun
- hrSWRunPerf
- hrSWInstalled

CISCO-SYSLOG-MIB

Syslog は、情報メッセージから重要メッセージまで、すべてのシステム メッセージを追跡し、ログに記録します。この MIB を使用すると、ネットワーク管理アプリケーションで SNMP トラップとして syslog メッセージを受信できます。

Cisco Syslog Agent は、次の MIB オブジェクトについてトラップ機能をサポートしています。

- clogNotificationsSent

- clogNotificationsEnabled
- clogMaxSeverity
- clogMsgIgnores
- clogMsgDrops

ベンダー固有の MIB

各種の Cisco MCS には、ベンダーおよびモデル番号に基づき、次の MIB が含まれます。これらの MIB を照会するために、HP Systems Insight Manager (SIM)、IBM Director Server+Console など、ハードウェアベンダーが開発した標準 MIB ブラウザを使用できます。MIB ブラウザの使用の詳細については、ハードウェアベンダーが提供するドキュメントを参照してください。

ベンダー固有の MIB の情報については、次の表を参照してください。

- [表 9-10](#) : サポートされている IBM MIB について説明しています。
- [表 9-11](#) : サポートされている HP MIB について説明しています。

表 9-10 IBM MIB

MIB	OID	説明
参照専用としてサポート		
IBM-SYSTEM-HEALTH-MIB	1.3.6.1.4.1.2.6.159.1.1.30	温度、電圧、およびファンのステータスを提供します。
IBM-SYSTEM-ASSETID-MIB	1.3.6.1.4.1.2.6.159.1.1.60	ハードウェアコンポーネントのアセットデータを提供します。
IBM-SYSTEM-LMSENSOR-MIB	1.3.6.1.4.1.2.6.159.1.1.80	温度、電圧、およびファンの詳細情報を提供します。
IBM-SYSTEM-NETWORK-MIB	1.3.6.1.4.1.2.6.159.1.1.110	Network Interface Card (NIC; ネットワークインターフェイスカード) のステータスを提供します。
IBM-SYSTEM-MEMORY-MIB	1.3.6.1.4.1.2.6.159.1.1.120	物理メモリの詳細情報を提供します。
IBM-SYSTEM-POWER-MIB	1.3.6.1.4.1.2.6.159.1.1.130	電源の詳細情報を提供します。
IBM-SYSTEM-PROCESSOR-MIB	1.3.6.1.4.1.2.6.159.1.1.140	CPU アセットまたはステータスのデータを提供します。
システムトラップ用としてサポート		
IBM-SYSTEM-TRAP	1.3.6.1.4.1.2.6.159.1.1.0	温度、電圧、ファン、ディスク、NIC、メモリ、電源、および CPU の詳細情報を提供します。
IBM-SYSTEM-RAID-MIB	1.3.6.1.4.1.2.6.167.2	RAID のステータスを提供します。

表 9-11 HP MIB

MIB	OID	説明
参照およびシステムトラップ用としてサポート		
CPQSTDEQ-MIB	1.3.6.1.4.1.232.1	ハードウェア コンポーネントの設定データを提供します。
CPQSINFO-MIB	1.3.6.1.4.1.232.2	ハードウェア コンポーネントのアセット データを提供します。
CPQIDA-MIB	1.3.6.1.4.1.232.3	RAID のステータスおよびイベントを提供します。
CPQHLTH-MIB	1.3.6.1.4.1.232.6	ハードウェア コンポーネントのステータスおよびイベントを提供します。
CPQSTSYS-MIB	1.3.6.1.4.1.232.8	ストレージ (ディスク) システムのステータスおよびイベントを提供します。
CPQSM2-MIB	1.3.6.1.4.1.232.9	iLO のステータスおよびイベントを提供します。
CPQTHRSH-MIB	1.3.6.1.4.1.232.10	アラームしきい値の管理を提供します。
CPQHOST-MIB	1.3.6.1.4.1.232.11	オペレーティング システム情報を提供します。
CPQIDE-MIB	1.3.6.1.4.1.232.14	IDE (CD-ROM) ドライブのステータスおよびイベントを提供します。
CPQNIC-MIB	1.3.6.1.4.1.232.18	Network Interface Card (NIC; ネットワーク インターフェイスカード) のステータスおよびイベントを提供します。

関連項目

- 「SNMP 設定チェックリスト」(P.9-1)
- 「SNMP ユーザ」(P.9-3)
- 「SNMP トラップ通知の宛先」(P.9-4)
- 「SNMP インフォーム通知の宛先」(P.9-5)
- 「MIB2 システム グループ」(P.9-7)
- 「SNMP Managed Information Base (MIB; 管理情報ベース)」(P.9-9)