



# Cisco 10000 シリーズ ESR MIB の概要

この章では、専用線のコンフィギュレーションに必要な Cisco 10000 シリーズ Edge Services Router (ESR; エッジ サービス ルータ) の拡張管理機能について説明します。具体的な内容は次のとおりです。

- [MIB 拡張機能の利点 \(p.1-1\)](#)
- [SNMP の概要 \(p.1-2\)](#)
- [関連情報およびリンク \(p.1-6\)](#)

## MIB 拡張機能の利点

Cisco 10000 シリーズ ESR の拡張管理機能によって、SNMP (簡易ネットワーク管理プロトコル) を使用してルータを管理できます。また、この機能によって、より多くの Management Information Base (MIB; 管理情報ベース) をルータで使用できます。SNMP および MIB の詳細については、「[SNMP の概要](#)」(p.1-2) を参照してください。

Cisco 10000 シリーズ ESR の拡張管理機能には、次のような利点があります。

- SNMP ベースの Network Management System (NMS; ネットワーク管理システム) を使用して、Cisco 10000 のリソースを管理および監視できます。
- SNMP **set** および **get** 要求を使用して、Cisco 10000 シリーズ ESR MIB の情報にアクセスできます。
- インベントリ管理、バルク データ転送といった機能を実行するために必要な時間およびシステムリソースが節約されます。

そのほかにも次のような利点があります。

- 規格に準拠したテクノロジー (SNMP) によって、ルータの障害およびパフォーマンスを監視できます。
- すべての SNMP バージョン (SNMPv1、SNMPv2c、および SNMPv3) がサポートされています。
- サービスに影響を及ぼす可能性のある障害、アラーム、および状態に関する通知が行われます。
- 複数のエンティティに関する障害およびアラーム情報の集約化が可能です。
- CLI (コマンドラインインターフェイス) 以外の方法で、ルータの情報にアクセスできます。

## SNMP の概要

SNMP は、ネットワーク上の装置を監視および管理するための標準フレームワークおよび共通言語を提供するアプリケーション レイヤ プロトコルです。

SNMP フレームワークには、次の 3 つの部分があります。

- **SNMP マネージャ** — SNMP を使用してネットワーク ホストの活動を制御および監視するシステム。この管理システムは、一般に NMS といいます。NMS は、ネットワーク管理のための専用装置を表す場合も、ネットワーク管理装置上で使用するアプリケーションを表す場合もあります。SNMP と併用できる多くのネットワーク管理アプリケーションがあります。単純なコマンドラインアプリケーションから (CiscoWorks2000 製品ラインのように) 豊富な機能を備えたグラフィカル ユーザ インターフェイスまで、さまざまな機能が提供されています。
- **SNMP エージェント** — 管理対象の装置上で動作するソフトウェア コンポーネントであり、装置に関するデータを維持し、必要に応じてそのデータを管理システムに報告します。エージェントおよび MIB は、ルーティング装置 (ルータ、アクセス サーバ、またはスイッチ) 上に存在します。管理対象の装置で SNMP エージェントをイネーブルにするには、マネージャとエージェントの関係を定義する必要があります ([「SNMP サポートのイネーブル化」](#) [p.2-4] を参照)。
- **MIB**

SNMP では、大量のコマンドを定義する代わりに、`get`、`get-next`、および `set` 要求の形式であらゆる動作を実行します。たとえば、SNMP マネージャは `get` 要求を使用して SNMP エージェントから値を取得し、`set` 要求を使用して SNMP エージェントに値を設定します。

## MIB の説明

MIB は、階層型に編成されたネットワーク管理情報の集合体です。MIB は、ID によって識別される管理オブジェクトの集合で成り立っています。MIB にアクセスするには、SNMP などのネットワーク管理プロトコルを使用します。管理オブジェクトは、管理対象の装置 (ルータなど) に備わっている特性の 1 つであり、MIB オブジェクトまたは単にオブジェクトとも呼ばれます。管理オブジェクトは、1 つまたは複数のオブジェクト インスタンス (本質的には変数) で構成されます。シスコシステムズが実装した SNMP では、RFC 1213 に記述された MIB II 変数の定義が使用されています。

MIB には、次の 2 種類の管理オブジェクトを含めることができます。

- **スカラー オブジェクト** — 単一のオブジェクト インスタンスを定義します (例: IF-MIB の `ifNumber`、BGP4-MIB の `bgpVersion` など)。
- **テーブル オブジェクト** — MIB テーブルにまとめられた、相互に関連性のある複数のオブジェクト インスタンスを定義します (例: IF-MIB の `ifTable` は、ルータ上のインターフェイス エンティティを定義します)。

システム MIB 変数には、SNMP を通じて次のようにしてアクセスします。

- **MIB 変数へのアクセス** — NMS からの要求に応じて、SNMP エージェントがこの機能を開始します。SNMP エージェントは要求された MIB 変数の値を検索し、その値を NMS に返します。
- **MIB 変数の設定** — NMS からのメッセージに応じて、SNMP エージェントがこの機能を開始します。SNMP エージェントは、MIB 変数の値を NMS が要求した値に変更します。

## SNMP トラップ

SNMP エージェントは、次のような重要なシステム イベントが発生したときに、SNMP マネージャにメッセージを送信することができます。

- インターフェイスまたはカードが動作を開始または停止した場合
- 温度がしきい値を超えた場合
- 認証エラーが発生した場合

エージェントがアラーム状態を検出すると、その発生時刻、タイプ、および重大度に関する情報を記録し、通知メッセージを生成して所定の IP ホストに送信します。SNMP 通知は、トラップまたはインフォームのいずれかで送信できます。Cisco 10000 シリーズ ESR 上でトラップをイネーブルにする方法については、「[SNMP サポートのイネーブル化](#)」(p.2-4)を参照してください。Cisco 10000 シリーズ ESR のトラップについての詳細は、[第 4 章「トラップの監視」](#)を参照してください。

シスコシステムズが実装した SNMP では、RFC 1215 に記述された SNMP トラップの定義が使用されています。

## SNMP バージョン

Cisco IOS ソフトウェアは、次の SNMP バージョンをサポートしています。

- SNMPv1 — SNMP。RFC 1157 に定義された完全版インターネット標準であり、コミュニティ ストリングに基づくセキュリティ機能を提供します。
- SNMPv2c — SNMPv2 用のコミュニティ ストリングに基づく管理フレームワーク。SNMPv2c は、SNMPv2p (SNMPv2 クラシック) のプロトコル動作およびデータ タイプを更新したものであり、SNMPv1 のコミュニティ ベースのセキュリティ モデルを採用しています。
- SNMPv3 — SNMP バージョン 3。SNMPv3 は、次のセキュリティ機能を使用して、装置への安全なアクセスを提供します。
  - メッセージインテグリティ — パケットが送信中に改ざんされないようにします。
  - 認証 — メッセージが有効な送信元から発信されたものであるかどうかを判別します。
  - 暗号化 — パケットの内容をスクランブルし、不正に傍受されないようにします。

### SNMPv1 および SNMPv2c

SNMPv1 および SNMPv2c は、両方ともコミュニティ ベースのセキュリティを使用しています。エージェントの MIB にアクセスできる管理者のコミュニティを、IP アドレスの Access Control List (ACL; アクセス制御リスト) およびパスワードで定義します。

SNMPv2c サポートには、バルク検索メカニズムと、管理ステーションへの詳細なエラー メッセージ レポート機能が含まれています。バルク検索メカニズムは、テーブルおよび大量の情報の検索に対応し、伝送に必要な往復回数を減らします。SNMPv2c で改善されたエラー処理サポートには、さまざまなエラー条件を区別する拡張エラー コードがあります。これらの条件は、SNMPv1 では単一のエラー コードで報告されます。エラー リターン コードでエラーの種類が報告されるようになり、次の 3 種類の例外も報告されます。

- no such object 例外
- no such instance 例外
- end of MIB view 例外

## SNMPv3

SNMPv3 は、複数のセキュリティ モデルおよびセキュリティ レベルを提供しています。セキュリティ モデルは、ユーザおよびそのユーザが所属するグループに対して設定する認証ストラテジーです。セキュリティ レベルは、1つのセキュリティ モデルの中で許可されるセキュリティのレベルを表します。セキュリティ モデルとセキュリティ レベルの組み合わせによって、SNMP パケットを処理するときに使用するセキュリティ メカニズムが決まります。

## SNMP セキュリティ モデルおよびレベル

表 1-1 に、各種の SNMP バージョンで提供されるセキュリティ モデルおよびレベルを示します。

表 1-1 SNMP セキュリティ モデルおよびレベル

モデル	レベル	認証	暗号化	説明
v1	noAuthNoPriv	コミュニティ ストリング	なし	認証にコミュニティ ストリングのマッチングを使用。
v2c	noAuthNoPriv	コミュニティ ストリング	なし	認証にコミュニティ ストリングのマッチングを使用。
v3	noAuthNoPriv	ユーザ名	なし	認証にユーザ名のマッチングを使用。
	authNoPriv	MD5 または SHA	なし	HMAC-MD5 または HMAC-SHA アルゴリズムに基づく認証を提供。
	authPriv	MD5 または SHA	DES	HMAC-MD5 または HMAC-SHA アルゴリズムに基づく認証を提供。CBC-DES (DES-56) 規格に基づく DES 56 ビット暗号化機能も提供。

SNMP エージェントは、管理ステーションがサポートしている SNMP バージョンを使用するように設定する必要があります。1つのエージェントが複数のマネージャと通信する場合があります。この理由から、ある管理ステーションとの通信には SNMPv1 プロトコルを使用し、別の管理ステーションとの通信には SNMPv2c、あるいは SNMPv3 を使用するように Cisco IOS ソフトウェアを設定することができます。

## RFC

MIB モジュールは、SNMP MIB モジュール言語で記述され、通常、Internet Engineering Task Force (IETF) に提出される Request For Comments (RFC) 文書で定義されています。RFC は、インターネット ソサエティおよびインターネット コミュニティ全体で検討されることを目的として、個人またはグループが作成します。RFC ステータスに達する前に、Internet Draft (I-D) として草案が公開されます。推奨される水準に達した RFC には、Standard (STD) というラベルが付けられます。詳細については、インターネット ソサエティおよび IETF の Web サイト (<http://www.isoc.org> および <http://www.ietf.org>) を参照してください。

シスコシステムズでは、システムごとに固有の MIB 拡張機能を提供しています。シスコのエンタープライズ MIB は、このマニュアルで特に明記しないかぎり、該当する RFC に記述されているガイドラインに準拠しています。

## オブジェクト ID

Object Identifier (OID; オブジェクト ID) は、管理対象のネットワーク装置上の MIB オブジェクトを一意に識別します。OID は、MIB 階層構造における MIB オブジェクトの場所を示し、複数の管理対象の装置からなるネットワーク上で MIB オブジェクトにアクセスするための手段になります。上位の MIB OID は、ISO、ITU などの標準化機関によって割り当てられていますが、下位の OID については、Cisco Assigned Numbers Authority (CANA) などの関連組織が割り当てを行います。

OID 中の数字は、MIB 階層構造のレベルに対応しています。たとえば 1.3.6.1.4.1.9.9.xyz-MIB という OID は、MIB 階層の中で次の場所にある xyz-MIB を表します。( ) 内の数字は、MIB 階層構造との対応を示すために併記しているに過ぎません。実際に使用する OID は数値だけで表記されます。

iso (1) .org (3) .dod (6) .internet (1) .private (4) .enterprises (1) .cisco (9) .ciscoMgt (9) .mn-MIB 管理オブジェクト (IF-MIB の ifNumber など) は、オブジェクト名 (iso.org.dod.internet.mgmt.enterprises.interfaces.ifNumber) または OID (1.3.6.1.2.1.2.1) によって一意に識別することができます。

MIB オブジェクトに割り当てられた OID の一覧は、次の URL を参照してください。

<ftp://ftp.cisco.com/pub/mibs/oid/>

## 関連情報およびリンク

次の URL にアクセスすると、Cisco MIB の全般的な情報を入手することができます。このページにあるリンクを利用して、MIB をダウンロードしたり、関連情報（アプリケーションノート、OID 一覧など）にアクセスしたりすることができます。

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

## TAC に関する情報および FAQ

次の URL にアクセスすると、シスコシステムズの Technical Assistance Center (TAC) が作成した SNMP に関する情報を入手することができます。

- <http://www.cisco.com/warp/public/477/SNMP/index.html> : SNMP に関する Cisco TAC のページです。SNMP に関する一般的な情報へのリンクと、SNMP によるデータ収集のヒントが記載されています。
- [http://www.cisco.com/warp/public/477/SNMP/mibs\\_9226.shtml](http://www.cisco.com/warp/public/477/SNMP/mibs_9226.shtml) : Cisco MIB に関する Frequently Asked Questions (FAQ; よくある質問) のリストです。

## SNMP の設定情報

次の URL にアクセスすると、SNMP の設定情報を入手することができます。

- [http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/cfun\\_vcg.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/cfun_vcg.htm) : SNMP サポートを設定するための手順を紹介しています。『Cisco IOS Configuration Fundamentals Configuration Guide』の一部を転載したものです。
- [http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/fun\\_r/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/fun_r/index.htm) : SNMP コマンドについて説明しています。『Cisco IOS Configuration Fundamentals Command Reference』の一部を転載したものです。