CHAPTER 27

SNMP の設定

この章では、Cisco Nexus 4001I/4005I Switch Module for IBM BladeCenter 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。

この章で説明する内容は、次のとおりです。

SNMP について

簡易ネットワーク管理プロトコル（SNMP）は、SNMP マネージャとエージェントの間の通信のメッセージ フォーマットを提供するアプリケーション レイヤ プロトコルです。SNMP は、ネットワーク内のデバイスのモニタリングおよび管理に使用する標準フレームワークと共通言語を提供します。

ここでは、次の内容について説明します。

SNMP 機能の概要

SNMP フレームワークは 3 つの部分で構成されます。

- SNMP マネージャ：SNMP を使用してネットワーク デバイスのアクティビティを制御し、モニタリングするシステム
- SNMP エージェント：デバイスのデータを維持し、必要に応じてこれらのデータを管理システムに報告する、管理対象デバイス内のソフトウェア コンポーネント。スイッチはエージェントおよび Management Information Base（MIB; 管理情報ベース）をサポートします。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。
- 管理情報ベース（MIB）：SNMP エージェントの管理対象オブジェクトのコレクション

SNMP は、RFC 3411 ～ 3418 で規定されています。

（注）　Cisco NX-OS は、イーサネット MIB の SNMP セットをサポートしません。

スイッチは、SNMPv1、SNMPv2c、および SNMPv3 をサポートします。SNMPv1 と SNMPv2c は、ともにコミュニティベース形式のセキュリティを使用します。

SNMP 通知

SNMP の重要な機能の 1 つは、SNMP エージェントから通知を生成できることです。これらの通知では、要求を SNMP マネージャから送信する必要はありません。通知は、不正なユーザ認証、再起動、接続の切断、ネイバー ルータとの接続の切断、その他の重要なイベントを表示します。

Cisco NX-OS は、トラップまたはインフォームとして SNMP 通知を生成します。トラップの信頼性はインフォームより低くなります。SNMP マネージャはトラップを受信しても Acknowledgment（ACK; 確認応答）を送信しないからです。このため、トラップが受信されたかどうかをスイッチが判断できません。インフォーム要求を受信する SNMP マネージャは、SNMP 応答 Protocol Data Unit（PDU; プロトコル データ ユニット）でメッセージの受信を確認します。スイッチが応答を受信しない場合、インフォーム要求を再び送信できます。

複数のホスト レシーバーに通知を送信するよう Cisco NX-OS を設定できます。ホスト レシーバーの詳細については、「SNMP 通知レシーバーの設定」（P.27-7）を参照してください。

SNMPv3

SNMPv3 はネットワーク上でフレームの認証および暗号化を組み合わせることによって、デバイスへの安全なアクセスを提供します。SNMPv3 が提供するセキュリティ機能は次のとおりです。

- メッセージの完全性：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：メッセージのソースが有効かどうかを判別します。
- 暗号化：許可されていないソースにより判読されないように、パケットの内容のスクランブルを行います。

SNMPv3 は、セキュリティ モデルとセキュリティ レベルの両方を提供します。セキュリティ モデルは、ユーザおよびユーザが属するロールを設定する認証方式です。セキュリティ レベルはセキュリティ モデル内で許可されたセキュリティのレベルです。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り、SNMP パケット処理中に採用されるセキュリティ メカニズムが決まります。

ここでは、次の内容について説明します。

SNMPv1、SNMPv2、SNMPv3 のセキュリティ モデルおよびセキュリティ レベル

セキュリティ レベルは、SNMP メッセージを開示から保護する必要があるかどうか、およびメッセージを認証するかどうか判断します。セキュリティ モデル内のさまざまなセキュリティ レベルは、次のとおりです。

- noAuthNoPriv：認証または暗号化を実行しないセキュリティ レベル
- authNoPriv：認証は実行するが、暗号化を実行しないセキュリティ レベル
- authPriv：認証と暗号化両方を実行するセキュリティ レベル

SNMPv1、SNMPv2c、および SNMPv3 の 3 つのセキュリティ モデルを使用できます。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り、SNMP メッセージの処理中に適用されるセキュリティ メカニズムが決まります。

ユーザベースのセキュリティ モデル

表 27-1 に、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の意味を示します。

表 27-1　SNMP セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	結果
v1	noAuthNoPriv	コミュニティ ストリング	なし	コミュニティ ストリングの照合を使用して認証します。
v2c	noAuthNoPriv	コミュニティ ストリング	なし	コミュニティ ストリングの照合を使用して認証します。
v3	noAuthNoPriv	ユーザ名	なし	ユーザ名の照合を使用して認証します。
v3	authNoPriv	HMAC-MD5 または HMAC-SHA	なし	Hash-Based Message Authentication Code（HMAC）Message Digest 5（MD5; メッセージ ダイジェスト 5）アルゴリズムまたは HMAC Secure Hash Algorithm（SHA）アルゴリズムに基づいて認証します。
v3	authPriv	HMAC-MD5 または HMAC-SHA	DES	HMAC-MD5 アルゴリズムまたは HMAC SHA アルゴリズムに基づいて認証します。Data Encryption Standard（DES; データ暗号規格）の 56 ビット暗号化、および Cipher Block Chaining（CBC; 暗号ブロック連鎖）DES（DES-56）標準に基づいた認証を提供します。

SNMPv3 User-Based Security Model（USM; ユーザベース セキュリティ モデル）は SNMP メッセージ レベルのセキュリティを示し、次のサービスを提供します。

- メッセージの完全性：メッセージが不正な方法で変更または破壊されていないことを保証します。また、データ シーケンスが、通常発生するものよりも高い頻度で変更されていないことを保証します。
- メッセージ発信元の認証：受信データを発信したユーザのアイデンティティが確認されたことを保証します。
- メッセージの機密性：情報が使用不可であること、または不正なユーザ、エンティティ、またはプロセスに開示されないことを保証します。

SNMPv3 は、設定済みユーザによる管理動作のみを許可し、SNMP メッセージを暗号化します。

Cisco NX-OS は、次の 2 つの SNMPv3 認証プロトコルを使用します。

- HMAC-MD5-96 認証プロトコル

- HMAC-SHA-96 認証プロトコル

Cisco NX-OS は、SNMPv3 メッセージ暗号化用のプライバシー プロトコルの 1 つとして Advanced Encryption Standard（AES; 高度暗号化規格）を使用し、Request For Comments（RFC; コメント要求）3826 に準拠しています。

priv オプションで、SNMP セキュリティ暗号化方式として、DES または 128 ビット AES を選択できます。**priv** オプションを **aes-128** トークンと併用すると、プライバシー パスワードは 128 ビット AES キーの生成に使用されます。AES のプライバシー パスワードは最小で 8 文字です。パスフレーズをクリア テキストで指定する場合、最大 64 文字を指定できます。ローカライズド キーを使用する場合は、最大 130 文字を指定できます。

（注） 外部の Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）サーバを使用して SNMPv3 を使う場合、外部 AAA サーバのユーザ設定でプライバシー プロトコルに AES を指定する必要があります。

コマンドライン インターフェイス（CLI）および SNMP ユーザの同期

SNMPv3 ユーザ管理は、認証、許可、アカウンティング（AAA）サーバ レベルで集中化できます。この中央集中型ユーザ管理により、Cisco NX-OS の SNMP エージェントは AAA サーバのユーザ認証サービスを利用できます。ユーザ認証が検証されると、SNMP PDU の処理が進行します。AAA サーバはユーザ グループ名の格納にも使用されます。SNMP はグループ名を使用して、スイッチでローカルに使用できるアクセス ポリシーまたはロール ポリシーを適用します。

ユーザ グループ、ロール、またはパスワードの設定が変更されると、SNMP と AAA の両方のデータベースが同期化されます。

Cisco NX-OS は、次のようにユーザ設定を同期化します。

- **snmp-server user** コマンドで指定された **auth** パスフレーズは、CLI ユーザのパスワードになります。
- **username** コマンドで指定されたパスワードは、SNMP ユーザの **auth** および **priv** パスフレーズになります。
- SNMP または CLI のいずれかを使用してユーザを削除すると、SNMP と CLI の両方の該当ユーザが削除されます。
- ユーザとロールの対応関係の変更は、SNMP と CLI で同期化されます。

（注） パスフレーズ / パスワードをローカライズド キー / 暗号化形式で設定すると、Cisco NX-OS はパスワードを同期化しません。

グループベースの SNMP アクセス

（注） *グループ*は業界全体で使用されている標準的な SNMP 用語なので、SNMP に関する説明では、「ロール」ではなく「グループ」を使用します。

SNMP アクセス権は、グループ別に編成されます。SNMP 内の各グループは、CLI を使用する場合のロールに似ています。各グループは 3 つのアクセス権により定義されます。つまり、読み取りアクセス、書き込みアクセス、および通知アクセスです。それぞれのアクセスを、各グループでイネーブルまたはディセーブルに設定できます。

ユーザ名が作成され、ユーザのロールが管理者によって設定され、ユーザがそのロールに追加されていれば、そのユーザはエージェントとの通信を開始できます。

設定時の注意事項および制限事項

Cisco NX-OS は、イーサネット MIB への読み取り専用アクセスをサポートします。

SNMP の設定

ここでは、次の内容について説明します。

SNMP ユーザの設定

SNMP のユーザを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal`	コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# snmp-server user` *name* `[auth {md5 | sha} passphrase [auto] [priv [aes-128] passphrase] [engineID id][localizedkey]]`	認証およびプライバシー パラメータのある SNMP ユーザを設定します。
ステップ 3	`switch(config)# show snmp user`	（任意）1 人または複数の SNMP ユーザに関する情報を表示します。
ステップ 4	`switch(config)# copy running-config startup-config`	（任意）この設定の変更を保存します。

SNMP メッセージ暗号化の適用

着信要求に認証または暗号化が必要となるよう SNMP を設定できます。デフォルトでは、SNMP エージェントは、認証と暗号化なしで SNMPv3 メッセージを受け入れます。プライバシーを適用する場合、Cisco NX-OS は、noAuthNoPriv または uthNoPriv のどちらかの securityLevel パラメータを使用しているすべての SNMPv3 PDU 要求に対して、authorization Error で応答します。

グローバル コンフィギュレーション モードで 1 人のユーザに SNMP メッセージ暗号化を適用する手順は、次のとおりです。

コマンド	目的
`switch(config)# snmp-server user name enforcePriv`	このユーザに対して SNMP メッセージ暗号化を適用します。

グローバル コンフィギュレーション モードですべてのユーザに SNMP メッセージ暗号化を適用する手順は、次のとおりです。

コマンド	目的
`switch(config)# snmp-server globalEnforcePriv`	すべてのユーザに対して SNMP メッセージ暗号化を適用します。

SNMPv3 ユーザに対する複数のロールの割り当て

SNMP ユーザを作成した後で、そのユーザに複数のロールを割り当てることができます。

（注）　他のユーザにロールを割り当てることができるのは、network-admin ロールに属するユーザだけです。

グローバル コンフィギュレーション モードで 1 人の SNMP ユーザにロールを割り当てる手順は、次のとおりです。

コマンド	目的
`switch(config)# snmp-server user name group`	この SNMP ユーザと設定されたユーザ ロールをアソシエートします。

SNMP コミュニティの作成

SNMPv1 または SNMPv2c の SNMP コミュニティを作成できます。

グローバル コンフィギュレーション モードで SNMP コミュニティ ストリングを作成する手順は、次のとおりです。

コマンド	目的
`switch(config)# snmp-server community name group {ro | rw}`	SNMP コミュニティ ストリングを作成します。

SNMP 通知レシーバーの設定

複数のホスト レシーバーに対して SNMP 通知を生成するよう Cisco NX-OS を設定できます。

グローバル コンフィギュレーション モードで SNMPv1 トラップのホスト レシーバーを設定する手順は、次のとおりです。

コマンド	目的
`switch(config)# snmp-server host` *ip-address* **traps** {**version 1**] *community* [**udp_port** *number*]	SNMPv1 トラップのホスト レシーバーを設定します。コミュニティは、最大 255 文字の英数字で指定できます。UDP ポート番号の範囲は 0 ～ 65535 です。

グローバル コンフィギュレーション モードで SNMPv2c トラップまたはインフォームのホスト レシーバーを設定する手順は、次のとおりです。

コマンド	目的
`switch(config)# snmp-server host` *ip-address* {**traps** | **informs**} **version 2c** *community* [**udp_port** *number*]	SNMPv2c トラップまたはインフォームのホスト レシーバーを設定します。コミュニティは、最大 255 文字の英数字で指定できます。UDP ポート番号の範囲は 0 ～ 65535 です。

グローバル コンフィギュレーション モードで SNMPv3 トラップまたはインフォームのホスト レシーバーを設定する手順は、次のとおりです。

コマンド	目的
`switch(config)# snmp-server host` *ip-address* {**traps** | **informs**} **version 3** {**auth** | **noauth** | **priv** } *username* [**udp_port** *number*]	SNMPv2c トラップまたはインフォームのホスト レシーバーを設定します。ユーザ名は、最大 255 文字の英数字で指定できます。UDP ポート番号の範囲は 0 ～ 65535 です。

次に、SNMPv3 インフォームのホスト レシーバーを設定する例を示します。

```
switch(config)# snmp-server host 192.0.2.1 informs version 3 auth NMS
```

（注） SNMP マネージャは、SNMPv3 メッセージを認証し暗号解除するため、スイッチの SNMP engineID に基づくユーザ クレデンシャル（authKey/PrivKey）を認識していなければなりません。

通知ターゲット ユーザの設定

SNMPv3 インフォーム通知を通知ホスト レシーバーに送信するには、デバイスに通知ターゲット ユーザを設定する必要があります。

スイッチは、通知ターゲット ユーザのクレデンシャルを使用して、設定した通知ホスト レシーバーへの SNMPv3 インフォーム通知メッセージを暗号化します。

（注）　受信した INFORM PDU を認証し暗号解除するためには、通知ホスト レシーバーが、インフォームを認証し暗号解除する スイッチ内に設定されたクレデンシャルと同じユーザ クレデンシャルを保持している必要があります。

通知ターゲット ユーザを設定するには、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
`switch(config)# snmp-server user` *name* [auth {md5 | sha} *passphrase* [auto] [priv [aes-128] *passphrase*] [engineID *id*]	通知ホスト レシーバーに対応した、指定した engineID を持つ通知ターゲット ユーザを設定します。engineID フォーマットは、コロンで区切られた 12 桁の 16 進数です。

次に、通知ターゲット ユーザを設定する例を示します。

```
switch(config)# snmp-server user NMS auth sha abcd1234 priv abcdefgh enginID
00:00:00:63:00:01:00:a1:ac:15:10:03
```

SNMP 通知のイネーブル化

通知をイネーブルまたはディセーブルにできます。通知名を指定しないと、Cisco NX-OS は通知をすべてイネーブルにします。

（注）　**snmp-server enable traps** CLI コマンドを使用すると、設定通知ホスト レシーバーによっては、トラップとインフォームの両方をイネーブルにできます。

表 27-2 に、Cisco NX-OS MIB の通知をイネーブルにする CLI コマンドを示します。

表 27-2　SNMP 通知のイネーブル化

MIB	関連コマンド
すべての通知	**snmp-server enable traps**
CISCO-AAA-SERVER-MIB	**snmp-server enable traps aaa**
ENTITY-MIB, CISCO-ENTITY-FRU-CONTROL-MIB, CISCO-ENTITY-SENSOR-MIB	**snmp-server enable traps entity** **snmp-server enable traps entity fru**
CISCO-LICENSE-MGR-MIB	**snmp-server enable traps license**
IF-MIB	**snmp-server enable traps link**
SNMPv2-MIB	**snmp-server enable traps snmp** **snmp-server enable traps snmp authentication**

（注）　ライセンス通知は、デフォルトではイネーブルです。他の通知はすべて、デフォルトではディセーブルです。

グローバル コンフィギュレーション モードで指定の通知をイネーブルにするには、次のいずれかの作業を行います。

コマンド	目的
`switch(config)# snmp-server enable traps`	すべての SNMP 通知をイネーブルにします。
`switch(config)# snmp-server enable traps aaa [server-state-change]`	AAA SNMP 通知をイネーブルにします。
`switch(config)# snmp-server enable traps entity [fru]`	ENTITY-MIB SNMP 通知をイネーブルにします。
`switch(config)# snmp-server enable traps license`	ライセンス SNMP 通知をイネーブルにします。
`switch(config)# snmp-server enable traps port-security`	ポート セキュリティ SNMP 通知をイネーブルにします。
`switch(config)# snmp-server enable traps snmp [authentication]`	SNMP エージェント通知をイネーブルにします。

linkUp/linkDown 通知の設定

デバイスに対して、イネーブルにする linkUp/linkDown 通知を設定できます。次のタイプの linkUp/linkDown 通知をイネーブルにできます。

- Cisco : Cisco NX-OS は、インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルの場合は、シスコ定義の通知（CISCO-IF-EXTENSION-MIB.my の cieLinkUp、cieLinkDown）だけを送信します。
- IETF : Cisco NX-OS は、インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルの場合は、定義されている変数バインドだけを IETF 定義の通知（IF-MIB の linkUp、linkDown）と一緒に送信します。
- IEFT extended : Cisco NX-OS は、インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルの場合は、IETF 定義の通知（IF-MIB の linkUp、linkDown）だけを送信します。Cisco NX-OS は、IF-MIB に定義されている変数バインドに加え、シスコ システムズに固有の変数バインドも送信します。これは、デフォルト設定です。
- IEFT Cisco : Cisco NX-OS は、インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルの場合は、IF-MIB に定義された通知（linkUp、linkDown）および CISCO-IF-EXTENSION-MIB.my に定義された通知（cieLinkUp、cieLinkDown）を送信します。Cisco NX-OS は、linkUp および linkDown 通知に定義された変数バインドだけを送信します。
- IEFT extended Cisco : Cisco NX-OS は、インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルの場合は、IF-MIB に定義された通知（linkUp、linkDown）および CISCO-IF-EXTENSION-MIB.my に定義された通知（cieLinkUp、cieLinkDown）を送信します。Cisco NX-OS は、linkUp および linkDown 通知の IF-MIB に定義されている変数バインドに加え、シスコ システムズに固有の変数バインドも送信します。

グローバル コンフィギュレーション モードで linkUp/linkDown 通知のタイプを設定する手順は、次のとおりです。

コマンド	目的
`switch(config)# snmp-server enable traps link [cisco] [ietf | ietf-extended]`	リンク SNMP 通知をイネーブルにします。

インターフェイスでの Up/Down 通知のディセーブル化

個別のインターフェイスで linkUp および linkDown 通知をディセーブルにできます。フラッピング インターフェイス（Up と Down の間を頻繁に切り替わるインターフェイス）で、この制限通知を使用できます。

インターフェイス コンフィギュレーション モードでインターフェイスの linkUp/linkDown 通知をディセーブルにする手順は、次のとおりです。

コマンド	目的
`switch(config-if)# no snmp trap link-status`	インターフェイスの SNMP リンクステート トラップをディセーブルにします。デフォルトでは、イネーブルです。

TCP での SNMP に対するワンタイム認証のイネーブル化

TCP セッション上で SNMP に対するワンタイム認証をイネーブルにできます。

グローバル コンフィギュレーション モードで、TCP セッション上の SNMP に対するワンタイム認証をイネーブルにする手順は、次のとおりです。

コマンド	目的
`switch(config)# snmp-server tcp-session [auth]`	TCP セッション上で SNMP に対するワンタイム認証をイネーブルにします。デフォルトでは、ディセーブルです。

SNMP スイッチの連絡先および場所の情報の割り当て

スイッチの連絡先情報（スペースを含めず、最大 32 文字まで）およびスイッチの場所を割り当てることができます。情報を割り当てる手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configuration terminal`	コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# snmp-server contact name`	sysContact（SNMP 担当者名）を設定します。
ステップ 3	`switch(config)# snmp-server location name`	sysLocation（SNMP ロケーション）を設定します。
ステップ 4	`switch(config-callhome)# show snmp`	（任意）1 つまたは複数の宛先プロファイルに関する情報を表示します。
ステップ 5	`switch(config)# copy running-config startup-config`	（任意）この設定の変更を保存します。

SNMP の設定の確認

SNMP の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
switch# **show snmp**	SNMP ステータスを表示します。
switch# **show snmp community**	SNMP コミュニティ ストリングを表示します。
switch# **show snmp engineID**	SNMP engineID を表示します。
switch# **show snmp group**	SNMP ロールを表示します。
switch# **show snmp sessions**	SNMP セッションを表示します。
switch# **show snmp trap**	イネーブルまたはディセーブルである SNMP 通知を表示します。
switch# **show snmp user**	SNMPv3 ユーザを表示します。

SNMP の設定例

次の例では、Cisco linkUp/linkDown 通知を 1 つの通知ホスト レシーバーに送信し、2 人の SNMP ユーザ（Admin および NMS）を定義するよう スイッチを設定します。

```
switch # configuration terminal
switch(config)# snmp-server contact Admin@example.com
switch(config)# snmp-server user Admin auth sha A1D2e6te priv W1laT3R9
switch(config)# snmp-server user NMS auth sha A1D2e6te priv W1laT3R9 enginID
00:00:00:63:00:01:00:a1:ac:15:10:03
switch(config)# snmp-server host 192.0.2.1 informs version 3 auth NMS
switch(config)# snmp-server host 192.0.2.1
switch(config)# snmp-server enable traps link
```

デフォルト設定

表 27-3 に、SNMP パラメータのデフォルト設定を示します。

表 27-3　デフォルトの SNMP パラメータ

パラメータ	デフォルト
ライセンス通知	イネーブル
linkUp/Down 通知タイプ	ietf-extended