CHAPTER 33

SNMP の設定

CLI と SNMP は、Cisco MDS 9000 ファミリのすべてのスイッチで共通のロールを使用します。SNMP を使用して CLI で作成したロールを変更したり、その逆を行うことができます。

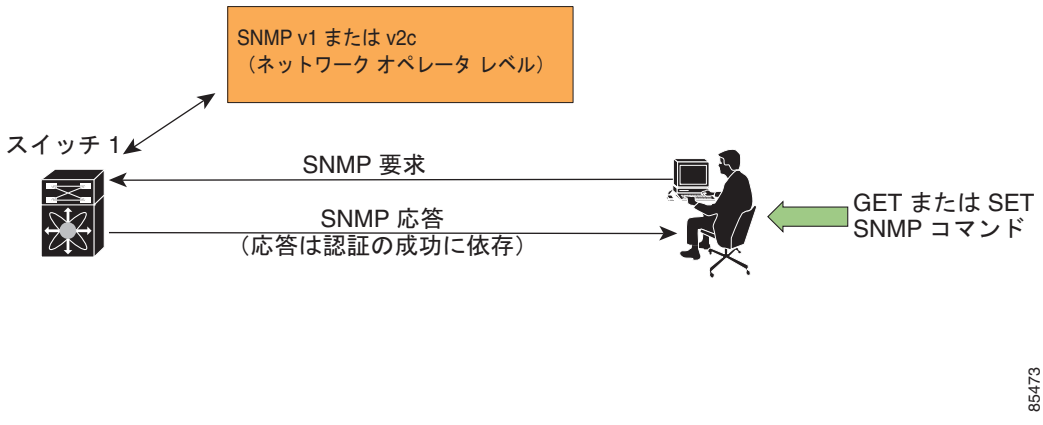
CLI ユーザと SNMP ユーザのユーザ、パスワード、ロールは、すべて同じです。CLI を通じて設定されたユーザは SNMP（たとえば、Fabric Manager や Device Manager）を使用してスイッチにアクセスでき、その逆も可能です。

この章は、次の項で構成されています。

SNMP セキュリティの概要

SNMP は、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション層プロトコルです。すべての Cisco MDS 9000 ファミリ スイッチで、SNMPv1、SNMPv2c、および SNMPv3 の 3 つの SNMP バージョンが使用できます（図 33-1 を参照）。

図 33-1　　SNMP セキュリティ



この項では、次のトピックについて取り上げます。

SNMP バージョン 1 およびバージョン 2c

SNMP バージョン 1（SNMPv1）および SNMP バージョン 2c（SNMPv2c）は、コミュニティ ストリングを使用してユーザ認証を行います。コミュニティ ストリングは、SNMP の初期のバージョンで使用されていた弱いアクセス コントロール方式です。SNMPv3 は、強力な認証を使用することによってアクセス コントロールを大幅に改善しています。したがって、SNMPv3 がサポートされている場合は、SNMPv1 および SNMPv2c に優先して使用してください。

SNMP バージョン 3

SNMP バージョン 3（SNMPv3）は、ネットワーク管理のための相互運用可能な標準ベースのプロトコルです。SNMPv3 は、ネットワーク経由のフレームの認証と暗号化を組み合わせることによって、デバイスへのセキュア アクセスを実現します。SNMPv3 で提供され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 では、セキュリティ モデルとセキュリティ レベルの両方が提供されています。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 レベルとは、セキュリティ モデル内で許可される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。

SNMP スイッチの連絡先情報と場所情報の割り当て

32 文字までの長さで（スペースを含まない）のスイッチ コンタクト情報を指定できます。さらに、スイッチ ロケーションを指定できます。

連絡先および場所の情報を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# snmp-server contact NewUser`	スイッチのコンタクト名を割り当てます。
	`switch(config)# no snmp-server contact NewUser`	スイッチのコンタクト名を削除します。
ステップ 3	`switch(config)# snmp-server location SanJose`	スイッチ ロケーションを割り当てます。
	`switch(config)# no snmp-server location SanJose`	スイッチ ロケーションを削除します。

連絡先および場所の情報を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# snmp-server contact NewUser`	スイッチのコンタクト名を割り当てます。
	`switch(config)# no snmp-server contact NewUser`	スイッチのコンタクト名を削除します。
ステップ 3	`switch(config)# snmp-server location SanJose`	スイッチ ロケーションを割り当てます。
	`switch(config)# no snmp-server location SanJose`	スイッチ ロケーションを削除します。

SNMPv3 CLI のユーザ管理と AAA の統合

Cisco SAN-OS ソフトウェアは RFC 3414 と RFC 3415 を実装しています。これには、ユーザベース セキュリティ モデル（USM）とロール ベースのアクセス コントロールが含まれています。SNMP と CLI のロール管理は共通化されており、同じ証明書とアクセス権限を共有しますが、以前のリリースではローカル ユーザ データベースは同期化されませんでした。

SNMPv3 のユーザ管理を AAA サーバ レベルで一元化できます。ユーザ管理を一元化すると、Cisco MDS スイッチ上で稼働する SNMP エージェントが 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。

この項では、次のトピックについて取り上げます。

- 「CLI および SNMP のユーザ同期」（P.33-3）
- 「スイッチ アクセスの制限」（P.33-4）
- 「グループベースの SNMP アクセス」（P.33-4）

CLI および SNMP のユーザ同期

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。

SNMP または CLI ユーザを作成するには、**username** コマンドまたは **snmp-server user** コマンドを使用します。

- **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として同期されます。
- **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` パスフレーズとして同期されます。

ユーザの同期化は、次のように処理されます。

- いずれかのコマンド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 /暗号化形式で指定すると、パスワードは同期化されません。

- 既存の SNMP ユーザは、特に変更しなくても、引き続き `auth` および `priv` のパスフレーズを維持できます。
- 管理ステーションが usmUserTable 内に SNMP ユーザを作成する場合、対応する CLI ユーザはパスワードなし（ログインは無効）で作成され、network-operator のロールが付与されます。

スイッチ アクセスの制限

IP アクセス コントロール リスト（IP-ACL）を使用して、Cisco MDS 9000 ファミリ スイッチへのアクセスを制限できます。第 35 章「IPv4 および IPv6 のアクセス コントロール リストの設定」を参照してください。

グループベースの SNMP アクセス

（注）　*グループ*が業界全体で使用されている標準 SNMP 用語なので、この SNMP の項では、ロールのことをグループと言います。

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。

ユーザの作成および変更

SNMP または CLI を使用して、ユーザの作成、または既存のユーザの変更を実行できます。

- SNMP：スイッチ上の usmUserTable に存在するユーザのクローンとして、新規のユーザを作成します。ユーザを作成した後、クローンの秘密キーを変更してから、そのユーザをアクティブにします。RFC 2574 を参照してください。
- CLI：**snmp-server user** コマンドを使用して、ユーザの作成または既存のユーザの変更を実行します。

Cisco MDS 9000 ファミリ スイッチ上で使用できるロールは、network-operator および network-admin です。GUI（Fabric Manager および Device Manager）を使用する場合は、default-role もあります。また、Common Roles データベースに設定されているどのロールも利用できます（"User Accounts" section on page 39-10 を参照）。

ヒント　CLI セキュリティ データベースおよび SNMP ユーザ データベースに対する更新はすべて同期化されます。SNMP パスワードを使用して、Fabric Manager または Device Manager のいずれかにログインできます。ただし、CLI パスワードを使用して Fabric Manager または Device Manager にログインした場合、その後のログインには必ず CLI パスワードを使用する必要があります。Cisco MDS SAN-OS

Release 2.0(1b) にアップグレードする前から SNMP データベースと CLI データベースの両方に存在しているユーザの場合、アップグレードすると、そのユーザに割り当てられるロールは両方のロールを結合したものになります。

この項では、次のトピックについて取り上げます。

AES 暗号化ベースのプライバシー

Advanced Encryption Standard（AES）は対称暗号アルゴリズムです。Cisco SAN-OS ソフトウェアは SNMP メッセージ暗号化の機密保全プロトコルの 1 つとして AES を使用し、RFC 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 AAA 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 を指定して、SNMP PDU を暗号化する必要があります。

CLI からの SNMP ユーザの設定

snmp-server user コマンドと **username** コマンドで指定したパスフレーズは同期されます（「SNMPv3 CLI のユーザ管理と AAA の統合」（P.33-3）を参照）。

CLI から SNMP ユーザを作成または変更するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t` `switch(config)#`	コンフィギュレーション モードに入ります。

	コマンド	目的
ステップ 2	`switch(config)# snmp-server user joe network-admin auth sha abcd1234`	ユーザ（joe）が、network-admin ロールで HMAC-SHA-96 認証パスワード（abcd1234）を使用するように設定を作成または変更します。
	`switch(config)# snmp-server user sam network-admin auth md5 abcdefgh`	ユーザ（sam）が、network-admin ロールで HMAC-MD5-96 認証パスワード（abcdefgh）を使用するように設定を作成または変更します。
	`switch(config)# snmp-server user Bill network-admin auth sha abcd1234 priv abcdefgh`	ユーザ（Bill）が、network-admin ロールで HMAC-SHA-96 認証レベルおよびプライバシー暗号化パラメータを使用するように設定を作成または変更します。
	`switch(config)# no snmp-server user usernameA`	ユーザ（usernameA）およびすべての関連パラメータを削除します。
	`switch(config)# no snmp-server usam role vsan-admin`	vsan-admin ロールから指定のユーザ（usam）を削除します。
	`switch(config)# snmp-server user user1 network-admin auth md5 0xab0211gh priv 0x45abf342 localizedkey`	パスワードをローカライズド キー フォーマット（RFC 2574）で指定します。ローカライズド キーは、16 進表記（たとえば、0xacbdef）で指定します。
	`switch(config)# snmp-server  user user2 auth md5 asdgfsadf priv aes-128 asgfsgkhkj`	MD5 認証プロトコルと AES-128 プライバシー プロトコルを使用して user2 を設定します。
ステップ 3	`switch(config)# snmp-server user joe sangroup`	指定したユーザ（joe）を sangroup ロールに追加します。
	`switch(config)# snmp-server user joe techdocs`	指定したユーザ（joe）を techdocs ロールに追加します。

CLI から SNMP ユーザのパスワードを作成または変更するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# snmp-server user user1 role1 auth md5 0xab0211gh priv 0x45abf342 localizedkey`	セキュリティ暗号化方式に DES オプションを使用して、パスワードをローカライズド キー フォーマットで指定します。
	`switch(config)# snmp-server user user1 role2 auth sha 0xab0211gh priv aes-128 0x45abf342 localizedkey`	セキュリティ暗号化方式に 128-bit AES オプションを使用して、パスワードをローカライズド キー フォーマットで指定します。

注意　CLI から SNMP ユーザを設定する場合は、**localizedkey** オプションを使用することは避けてください。ローカライズド キーにはデバイス エンジン ID 情報が含まれているため、デバイス間で移動可能ではありません。あるデバイスに別のデバイスで生成したコンフィギュレーション ファイルをコピーした場合、パスワードが正しく設定されない可能性があります。コンフィギュレーションをデバイスにコピーした後で、必要なパスワードを明示的に設定します。**localizedkey** オプションで指定されるパスワードは、最大 130 文字に制限されています。

（注）　**snmp-server user** コマンドには、追加パラメータとして engineID を指定できます。engineID は、通知対象ユーザを作成します（「通知対象ユーザの設定」（P.33-13）を参照）。engineID を指定しない場合、ローカル ユーザが作成されます。

SNMPv3 メッセージ暗号化の適用

デフォルトでは、SNMP エージェントは、auth キーと priv キーを使用したユーザ設定の SNMPv3 メッセージ暗号化を使用する。SNMPv3 メッセージの authNoPriv および authPriv の securityLevel パラメータを許可します。

ユーザのメッセージ暗号化を適用するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# snmp-server user testUser enforcePriv`	このユーザを使用して SNMPv3 メッセージにメッセージ暗号化を適用します。 （注）　auth および priv の両方のキーが設定された既存のユーザに対してだけ、このコマンドを使用できます。ユーザがプライバシーを適用するように設定されている場合、SNMP エージェントは、noAuthNoPriv または authNoPriv の securityLevel パラメータを使用している SNMPv3 PDU 要求に、authorizationError で応答します。
	`switch(config)# no snmp-server user testUser enforcePriv`	SNMPv3 メッセージ暗号化の適用をディセーブルにします。

または、次のコマンドを使用して、SNMPv3 メッセージ暗号化をすべてのユーザに対してグローバルに適用することもできます。

	コマンド	目的
ステップ 1	`switch# config t` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# snmp-server globalEnforcePriv`	スイッチ上のすべてのユーザに SNMPv3 メッセージ暗号化を適用します。
	`switch(config)# no snmp-server globalEnforcePriv`	グローバルな SNMPv3 メッセージ暗号化の適用をディセーブルにします。

SNMPv3 ユーザの複数のロールへの割り当て

SNMP サーバのユーザ設定が強化され、SNMPv3 ユーザに複数のロール（グループ）を割り当てることが可能になっています。最初に SNMPv3 ユーザを作成した後で、そのユーザにロールを追加できます。

（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。

CLI から SNMPv3 ユーザに複数のロールを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# snmp-server user NewUser role1`	role1 ロールの SNMPv3 ユーザ（NewUser）の設定を作成または変更します。
	`switch(config)# snmp-server user NewUser role2`	role2 ロールの SNMPv3 ユーザ（NewUser）の設定を作成または変更します。
	`switch(config)# no snmp-server user User5 role2`	指定されたユーザ（User5）の role2 を削除します。

コミュニティの追加または削除

SNMPv1 および SNMPv2 のユーザの場合は、読み取り専用または読み取り / 書き込みアクセスを設定できます。RFC 2576 を参照してください。

SNMPv1 または SNMPv2c のコミュニティを作成するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# snmp-server community snmp_Community ro`	指定した SNMP コミュニティに読み取り専用アクセスを追加します。
	`switch(config)# snmp-server community snmp_Community rw`	指定した SNMP コミュニティに読み取りと書き込みのアクセスを追加します。
	`switch(config)# no snmp-server community snmp_Community`	指定した SNMP コミュニティのアクセスを削除します（デフォルト）。

SNMP トラップとインフォーム通知

特定のイベントが発生したときに SNMP マネージャに通知を送信するように Cisco MDS スイッチを設定できます。

（注）　通知をトラップまたはインフォームとして送信する宛先の詳細情報を入手するには、SNMP-TARGET-MIB を使用します。詳細については、『*Cisco MDS 9000 Family MIB Quick Reference*』を参照してください。

この項では、次のトピックについて取り上げます。

- 「SNMP セキュリティ情報の表示」（P.33-16）

ヒント　SNMPv1 オプションは、**snmp-server host** *ip-address* **informs** コマンドでは使用できません。

SNMPv2c 通知の設定

IPv4 を使用する SNMPv2c 通知を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# **config t** switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **snmp-server host 171.71.187.101 traps version 2c private udp-port 1163**	指定したホストが SNMPv2c コミュニティ ストリング（private）を使用して SNMPv2c トラップを受信するように設定します。
	switch(config)# **no snmp-server host 171.71.187.101 traps version 2c private udp-port 2162**	指定したホストが SNMPv2c コミュニティ ストリング（private）を使用して設定済みの UDP ポートの SNMPv2c トラップを受信できないようにします。
ステップ 3	switch(config)# **snmp-server host 171.71.187.101 informs version 2c private udp-port 1163**	指定したホストが SNMPv2c コミュニティ ストリング（private）を使用して SNMPv2c インフォームを受信するように設定します。
	switch(config)# **no snmp-server host 171.71.187.101 informs version 2c private udp-port 2162**	指定したホストが SNMPv2c コミュニティ ストリング（private）を使用して設定済みの UDP ポートの SNMPv2c インフォームを受信できないようにします。

IPv6 を使用する SNMPv2c 通知を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# **config t** switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **snmp-server host 2001:0DB8:800:200C::417A traps version 2c private udp-port 1163**	指定したホストが SNMPv2c コミュニティ ストリング（private）を使用して SNMPv2c トラップを受信するように設定します。
	switch(config)# **no snmp-server host 2001:0DB8:800:200C::417A traps version 2c private udp-port 2162**	指定したホストが SNMPv2c コミュニティ ストリング（private）を使用して設定済みの UDP ポートの SNMPv2c トラップを受信できないようにします。
ステップ 3	switch(config)# **snmp-server host 2001:0DB8:800:200C::417A informs version 2c private udp-port 1163**	指定したホストが SNMPv2c コミュニティ ストリング（private）を使用して SNMPv2c インフォームを受信するように設定します。
	switch(config)# **no snmp-server host 2001:0DB8:800:200C::417A informs version 2c private udp-port 2162**	指定したホストが SNMPv2c コミュニティ ストリング（private）を使用して設定済みの UDP ポートの SNMPv2c インフォームを受信できないようにします。

（注）　スイッチは、イベント（SNMP トラップおよびインフォーム）を、最大 10 件の宛先に転送できます。

SNMPv3 通知の設定

IPv4 を使用する SNMPv3 通知を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# **config t** switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **snmp-server host 16.20.11.14 traps version 3 noauth testuser udp-port 1163**	指定したホストが SNMPv3 ユーザ（testuser）および noAuthNoPriv の securityLevel を使用して SNMPv3 トラップを受信するように設定します。
	switch(config)# **snmp-server host 16.20.11.14 informs version 3 auth testuser udp-port 1163**	指定したホストが SNMPv3 ユーザ（testuser）および AuthNoPriv の securityLevel を使用して SNMPv3 インフォームを受信するように設定します。
	switch(config)# **snmp-server host 16.20.11.14 informs version 3 priv testuser udp-port 1163**	指定したホストが SNMPv3 ユーザ（testuser）および AuthPriv の securityLevel を使用して SNMPv3 インフォームを受信するように設定します。
	switch(config)# **no snmp-server host 172.18.2.247 informs version 3 testuser noauth udp-port 2162**	指定したホストが SNMPv3 インフォームを受信できないようにします。

IPv6 を使用する SNMPv3 通知を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# **config t** switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **snmp-server host 2001:0DB8:800:200C::417A traps version 3 noauth testuser udp-port 1163**	指定したホストが SNMPv3 ユーザ（testuser）および noAuthNoPriv の securityLevel を使用して SNMPv3 トラップを受信するように設定します。
	switch(config)# **snmp-server host 2001:0DB8:800:200C::417A informs version 3 auth testuser udp-port 1163**	指定したホストが SNMPv3 ユーザ（testuser）および AuthNoPriv の securityLevel を使用して SNMPv3 インフォームを受信するように設定します。
	switch(config)# **snmp-server host 2001:0DB8:800:200C::417A informs version 3 priv testuser udp-port 1163**	指定したホストが SNMPv3 ユーザ（testuser）および AuthPriv の securityLevel を使用して SNMPv3 インフォームを受信するように設定します。
	switch(config)# **no snmp-server host 2001:0DB8:800:200C::417A informs version 3 testuser noauth udp-port 2162**	指定したホストが SNMPv3 インフォームを受信できないようにします。

（注）　SNMPv3 通知の場合、SNMP マネージャは、SNMP メッセージを認証および復号化するために、スイッチの engineID に基づくユーザ資格情報（authKey/PrivKey）を知っていることが期待されます。

SNMP 通知のイネーブル化

通知（トラップおよびインフォーム）は、特定のイベントが発生したときにスイッチによって生成されるシステム アラートです。通知をイネーブルまたはディセーブルにできます。デフォルトでは、通知は 1 つも定義されておらず、通知が生成されることはありません。通知名を指定しないと、すべての通知が無効または有効になります。

表 33-1 に、Cisco MDS MIB の通知をイネーブルにする CLI コマンドを示します。

（注）　**snmp-server enable traps** CLI コマンドを使用すると、設定方法に応じて、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。**snmp-server host** CLI コマンドによる通知を参照してください。

表 33-1　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**
ENITY-MIB、 CISCO-ENTITY-FRU-CONTROL-MIB、 CISCO-ENTITY-SENSOR-MIB	**snmp-server enable traps entity** **snmp-server enable traps entity fru**
CISCO-FCC-MIB	**snmp-server enable traps fcc**
CISCO-DM-MIB	**snmp-server enable traps fcdomain**
CISCO-NS-MIB	**snmp-server enable traps fcns**
CISCO-FCS-MIB	**snmp-server enable traps fcs discovery-complete** **snmp-server enable traps fcs request-reject**
CISCO-FDMI-MIB	**snmp-server enable traps fdmi**
CISCO-FSPF-MIB	**snmp-server enable traps fspf**
CISCO-LICENSE-MGR-MIB	**snmp-server enable traps license**
IF-MIB	snmp-server enable traps link
CISCO-PSM-MIB	**snmp-server enable traps port-security**
CISCO-RSCN-MIB	**snmp-server enable traps rscn** **snmp-server enable traps rscn els** **snmp-server enable traps rscn ils**
SNMPv2-MIB	**snmp-server enable traps snmp** **snmp-server enable traps snmp authentication**

表 33-1　SNMP 通知のイネーブル化 （続き）

MIB	関連コマンド
VRRP-MIB, CISCO-IETF-VRRP-MIB	**snmp-server enable traps vrrp**
CISCO-ZS-MIB	**snmp-server enable traps zone** **snmp-server enable traps zone default-zone-behavior-change** **snmp-server enable traps zone merge-failure** **snmp-server enable traps zone merge-success** **snmp-server enable traps zone request-reject** **snmp-server enable traps zone unsupp-mem**

次の通知はデフォルトでイネーブルになっています。

- entity fru
- license
- link ietf-extended

他の通知はすべて、デフォルトではディセーブルです。

個々の通知をイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# snmp-server enable traps fcdomain`	指定した SNMP（fcdomain）通知をイネーブルにします。
	`switch(config)# no snmp-server enable traps`	指定した SNMP 通知をディセーブルにします。通知名を指定しないと、すべての通知がディセーブルになります。

すべての通知とそのステータスを表示するには、**show snmp trap** コマンドを使用します。

```
switch# show snmp trap
Trap type                              Enabled
---------                              -------
entity fru                              Yes
fcc                                     No
fcdomain                                No
fcns                                    No
fcs request-reject                      No
fcs discovery-complete                  No
fdmi                                    No
fspf                                    No
license                                 Yes
port-security                           No
rscn els                                No
rscn ils                                No
snmp authentication                     No
vrrp                                    Yes
zone unsupported member                 No
zone request-reject                     No
zone merge-failure                      No
zone merge-success                      No
zone default-zone-behavior-change       No
```

通知対象ユーザの設定

SNMPv3 インフォーム通知を SNMP マネージャに送信するには、スイッチ上で通知対象ユーザを設定する必要があります。

通知対象ユーザを設定するには、次のコマンドを使用します。

	コマンド	目的
ステップ 1	`switch# config t` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# snmp-server user testusr auth md5 xyub20gh priv xyub20gh engineID 00:00:00:63:00:01:00:a1:ac:15:10:03`	指定したエンジン ID の SNMP マネージャに対応する、指定した資格情報を持つ通知対象ユーザを設定します。
	`switch(config)# no snmp-server user testusr auth md5 xyub20gh priv xyub20gh engineID 00:00:00:63:00:01:00:a1:ac:15:10:03`	通知対象ユーザを削除します。

通知対象ユーザの資格情報は、設定した SNMP マネージャへの SNMPv3 インフォーム通知メッセージの暗号化に使用されます（**snmp-server host** コマンドに従って）。

（注）　SNMP マネージャは、受信した INFORM PDU を認証および復号化するために、同じユーザ資格情報をユーザのローカル設定データ ストアに持っている必要があります。

スイッチの linkUp/linkDown 通知の設定

スイッチに対して、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：インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルになっている場合、そのインターフェイスについて CISCO-IF-EXTENSION-MIB.my で定義された通知（cieLinkUp、cieLinkDown）のみが送信されます。
- IETF：インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルになっている場合、そのインターフェイスについて IF-MIB で定義された通知（linkUp、linkDown）のみが送信されます。通知定義で定義された変数バインドのみが、それらの通知とともに送信されます。
- IEFT extended：インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルになっている場合、そのインターフェイスについて IF-MIB で定義された通知（linkUp、linkDown）のみが送信されます。通知定義で定義された変数バインドに加え、シスコの実装に固有の IF-MIB で定義された変数バインドも送信されます。これがデフォルト設定です。
- IEFT Cisco：インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルになっている場合、そのインターフェイスについて IF-MIB で定義された通知（linkUp、linkDown）および CISCO-IF-EXTENSION-MIB.my で定義された通知（cieLinkUp、cieLinkDown）のみが送信されます。通知定義で定義された変数バインドのみが、linkUp 通知や linkDown 通知とともに送信されます。
- IEFT extended Cisco：インターフェイスに対して ifLinkUpDownTrapEnable（IF-MIB で定義）がイネーブルになっている場合、そのインターフェイスについて IF-MIB で定義された通知（linkUp、linkDown）および CISCO-IF-EXTENSION-MIB.my で定義された通知（cieLinkUp、

cieLinkDown）のみが送信されます。linkUp と linkDown の通知定義で定義された変数バインドに加え、シスコの実装に固有の IF-MIB で定義された変数バインドも linkUp 通知や linkDown 通知とともに送信されます。

（注）　シスコの実装に固有の IF-MIB で定義される変数バインドの詳細については、『*Cisco MDS 9000 Family MIB Quick Reference*』を参照してください。

スイッチに linkUp/linkDown 通知を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# snmp-server enable traps link`	IETF extended linkUp/linkDown 通知のみをイネーブルにします（デフォルト）。
	`switch(config)# snmp-server enable traps link cisco`	シスコによって定義された cieLinkUp/cieLinkDown 通知のみをイネーブルにします。
	`switch(config)# snmp-server enable traps link ietf`	IETF linkUp/linkDown 通知のみをイネーブルにします。
	`switch(config)# snmp-server enable traps link ietf-extended`	追加の変数バインドを持つ IETF extended linkUp/linkDown 通知のみをイネーブルにします（デフォルト）。
	`switch(config)# snmp-server enable traps link ietf cisco`	IETF（linkUp/linkDown）通知およびシスコによって定義された（cieLinkUp/cieLinkDown）通知をイネーブルにします。
	`switch(config)# snmp-server enable traps link ietf-extended cisco`	追加の変数バインドを持つ IEFT（linkUp/linkDown）通知およびシスコによって定義された（cieLinkUp/cieLinkDown）通知をイネーブルにします。
	`switch(config)# no snmp-server enable traps link`	デフォルト設定（IETF extended）に戻します。

インターフェイスの Up/Down SNMP リンクステート トラップの設定

デフォルトでは、SNMP リンクステート トラップがすべてのインターフェイスに対してイネーブルになっています。リンクの状態が Up と Down の間で切り替わるたびに、SNMP トラップが生成されます。

何百ものインターフェイスを装備したスイッチが多数存在し、それらの多くでリンクの状態をモニタする必要がない場合があります。そのような場合には、リンクステート トラップをディセーブルにすることも選択できます。

特定のインターフェイスに対して SNMP リンクステート トラップをディセーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t` `switch(config)#`	コンフィギュレーション モードに入ります。

	コマンド	目的
ステップ 2	`switch(config)# interface bay 6`	SNMP リンクステート トラップをディセーブルにするインターフェイスを指定します。
	`switch(config-if)# no link-state-trap`	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。
	`switch(config-if)# link-state-trap`	インターフェイスの SNMP リンクステート トラップをイネーブルにします。

インターフェイスに対して SNMP リンクステート トラップをディセーブルにすると、そのコマンドも、システムの実行コンフィギュレーションに追加されます。実行コンフィギュレーションを表示するには、そのインターフェイスに対して **show running-config** コマンドを入力します。

```
switch# show running-config
version 3.1(2)
....
interface bay5
interface bay6
  no link-state-trap <-----インターフェイスの実行コンフィギュレーションにコマンドを追加
interface bay7
...
```

特定のインターフェイスに対する SNMP リンクステート トラップの設定を表示するには、**show interface** コマンドを入力します。

```
switch# show interface bay 6
bay6 is down (Administratively down)
    Hardware is Fibre Channel
    Port WWN is 20:0b:00:05:30:01:70:2c
    Admin port mode is auto, trunk mode is on
    snmp link-state traps are disabled

    Port vsan is 1
    Receive data field Size is 2112
    Beacon is turned off
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
      0 frames input, 0 bytes
        0 discards, 0 errors
        0 CRC,  0 unknown class
        0 too long, 0 too short
      0 frames output, 0 bytes
        0 discards, 0 errors
      0 input OLS, 0 LRR, 0 NOS, 0 loop inits
      0 output OLS, 0 LRR, 0 NOS, 0 loop inits
```

リンクの Up/Down トラップ設定の範囲

インターフェイスに対するリンクの Up/Down トラップ設定は、次の範囲に基づいてトラップを生成します。

スイッチレベルのトラップ設定	インターフェイスレベルのトラップ設定	インターフェイス リンクについて生成されるトラップか？
イネーブル（デフォルト）	有効（デフォルト）	Yes
イネーブル	ディセーブル	No

スイッチレベルのトラップ設定	インターフェイスレベルのトラップ設定	インターフェイス リンクについて生成されるトラップか？
ディセーブル	イネーブル	No
ディセーブル	ディセーブル	No

SNMP セキュリティ情報の表示

設定済みの SNMP 情報を表示するには、**show snmp** コマンドを使用します（例 33-1 および 33-6 を参照）。

例 33-1　SNMP ユーザの詳細情報の表示

```
switch# show snmp user
_____________________________________________________________________
                   SNMP USERS
_____________________________________________________________________

User                           Auth  Priv(enforce) Groups
____                           ____  ______________ ______
admin                          md5   des(no)        network-admin

testusr                        md5   aes-128(no)    role111
                                                    role222
_____________________________________________________________________
 NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
_____________________________________________________________________
User                           Auth  Priv

____                           ____  ____
testtargetusr                  md5   des
(EngineID 0:0:0:63:0:1:0:0:0:15:10:3)
```

例 33-2　SNMP コミュニティ情報の表示

```
switch# show snmp community
Community                       Access
---------                       ------
private                          rw
public                           ro
v93RACqPNH                       ro
```

例 33-3　SNMP ホスト情報の表示

```
switch# show snmp host
Host                            Port Version  Level  Type   SecName

____                            ____ _______  ______ ____   _______
171.16.126.34                   2162 v2c      noauth trap   public
171.16.75.106                   2162 v2c      noauth trap   public
...
171.31.58.97                    2162 v2c      auth   trap   public
...
```

show snmp コマンドでは、SNMP の連絡先、ロケーション、およびパケット設定に関するカウンタ情報が表示されます。このコマンドで提供される情報は、すべて Cisco MDS 9000 ファミリ Fabric Manager によって使用されます（『*Cisco MDS 9000 Family Fabric Manager Configuration Guide*』を参照）。例 33-4 を参照してください。

例 33-4　SNMP 情報の表示

```
switch# show snmp
sys contact:
sys location:
1631 SNMP packets input
        0 Bad SNMP versions
        0 Unknown community name
        0 Illegal operation for community name supplied
        0 Encoding errors
        64294 Number of requested variables
        1 Number of altered variables
        1628 Get-request PDUs
        0 Get-next PDUs
        1 Set-request PDUs
152725 SNMP packets output
        0 Too big errors
        1 No such name errors
        0 Bad values errors
        0 General errors
Community                       Group / Access
---------                       ------
public                           rw


_____________________________________________________________
                  SNMP USERS
_____________________________________________________________

User                            Auth  Priv(enforce) Groups
____                            ____  _____________ ______
admin                           md5   des(no)       network-admin

testusr                         md5   aes-128(no)   role111
                                                    role222


_____________________________________________________________
 NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
_____________________________________________________________

User                            Auth  Priv
____                            ____  ____
testtargetusr                   md5   des
(EngineID 0:0:0:63:0:1:0:0:0:15:10:3)
```

例 33-5　SNMP エンジン ID の表示

```
switch# show snmp engineID
Local SNMP engineID: 800000090300053000851E
```

例 33-6　SNMP セキュリティ グループ情報の表示

```
switch# show snmp group
groupname: network-admin
security model: any
security level: noAuthNoPriv
readview: network-admin-rd
writeview: network-admin-wr
notifyview: network-admin-rd
storage-type: permanent
row status: active
```

```
groupname: network-admin
security model: any
security level: authNoPriv
readview: network-admin-rd
writeview: network-admin-wr
notifyview: network-admin-rd
storage-type: permanent
row status: active

groupname: network-operator
security model: any
security level: noAuthNoPriv
readview: network-operator-rd
writeview: network-operator-wr
notifyview: network-operator-rd
storage-type: permanent
row status: active

groupname: network-operator
security model: any
security level: authNoPriv
readview: network-operator-rd
writeview: network-operator-wr
notifyview: network-operator-rd
storage-type: permanent
row status: active
```

デフォルト設定

表 33-2 に、すべてのスイッチの SNMP 機能のデフォルト設定を示します。

表 33-2　SNMP のデフォルト設定

パラメータ	デフォルト
ユーザ アカウント	有効期限なし（設定しない場合）
パスワード	なし