CHAPTER 32

ユーザ ロールおよび共通ロールの設定

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 を使用して作成したロールは CLI を使用して変更でき、その逆も可能です。

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。

- 「ロールベースの認証」（P.32-1）
- 「ロールの配信」（P.32-4）
- 「共通ロールの設定」（P.32-9）
- 「ユーザ アカウントの設定」（P.32-10）
- 「SSH サービスの設定」（P.32-14）
- 「管理者パスワードの回復」（P.32-19）
- 「デフォルト設定」（P.32-21）

ロールベースの認証

Cisco MDS 9000 ファミリ スイッチはロールに基づいた認証を行います。ロールベースの認証は、ユーザをロール（役割）に割り当てることによってスイッチ操作へのアクセスを制限します。この種類の認証では、ユーザに割り当てられたロールに基づいて管理操作が制限されます。

ユーザがコマンドの実行、コマンドの完了、またはコンテキスト ヘルプの取得を行った場合、ユーザにそのコマンドへのアクセス権があると、スイッチ ソフトウェアによって処理の続行が許可されます。

この項では、次のトピックについて取り上げます。

- 「ロールの概要」（P.32-2）
- 「ロールとプロファイルの設定」（P.32-2）
- 「各ロールのルールと機能の設定」（P.32-2）
- 「VSAN ポリシーの設定」（P.32-3）

ロールの概要

ロールごとに複数のユーザを含めることができ、各ユーザは複数のロールに所属できます。たとえば、role1 ユーザにはコンフィギュレーション コマンドへのアクセスだけが、role2 ユーザには **debug** コマンドへのアクセスだけが許可されているとします。この場合、role1 と role2 の両方に所属しているユーザは、コンフィギュレーション コマンドと **debug** コマンドの両方にアクセスできます。

（注） ユーザが複数のロールに所属している場合、各ロールで許可されているすべてのコマンドを実行できます。コマンドへのアクセス権は、コマンドへのアクセス拒否よりも優先されます。たとえば、TechDocs グループに属しているユーザが、コンフィギュレーション コマンドへのアクセスを拒否されているとします。ただし、このユーザはエンジニアリング グループにも属しており、コンフィギュレーション コマンドへのアクセス権を持っています。この場合、このユーザはコンフィギュレーション コマンドにアクセスできます。

ヒント ロールを作成した時点で、必要なコマンドへのアクセスが即時に許可されるわけではありません。管理者が各ロールに適切なルールを設定して、必要なコマンドへのアクセスを許可する必要があります。

ロールとプロファイルの設定

追加ロールの作成または既存ロールのプロファイル修正を行うには、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)# role name techdocs` `switch(config-role)#`	指定したロール（techdocs）のモードを開始します。 **（注）** ロール サブモード プロンプトは、ロールのサブモードを開始したことを示します。このサブモードは techdocs グループに固有です。
	`switch(config)# no role name techdocs`	ロール techdocs を削除します。
ステップ 3	`switch(config-role)# description Entire Tech Docs group`	新しいロールに記述を割り当てます。記述は 1 行に制限され、スペースを含めることができます。
	`switch(config-role)# no description`	Tech Docs グループの記述をリセットします。

（注） network-admin ロールに属するユーザだけがロールを作成できます。

各ロールのルールと機能の設定

各ロールに、最大 16 のルールを設定できます。ルールが適用される順序は、ユーザ指定のルール番号で決まります。たとえば、ルール 1 のあとにルール 2 が適用され、ルール 3 以降が順に適用されます。network-admin ロールに属さないユーザは、ロールに関連したコマンドを実行できません。

たとえば、ユーザ A にすべての **show** コマンドの実行を許可されていても、ユーザ A が network-admin ロールに所属していないかぎり、ユーザ A は **show role** コマンドの出力を表示できません

rule コマンドでは特定のロールで実行できる動作を指定します。ルールを構成する要素は、ルール番号、ルール タイプ（許可または拒否）、コマンド タイプ（**config**、**clear**、**show**、**exec**、**debug** など）、および任意の機能名（FSPF、ゾーン、VSAN、fcping、インターフェイスなど）です。

（注）　この場合、**exec** コマンドでは、**show**、**debug** および **clear** の各コマンドのカテゴリに入らない、EXEC モード内のすべてのコマンドが対象になります。

プロファイルの変更

既存ロールのプロファイルを変更するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	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)# role name sangroup` `switch(config-role)#`	既存のロール sangroup のロール コンフィギュレーション サブモードを開始します。

ステップ 3	`switch(config-role)# rule 1 permit config`
	`switch(config-role)# rule 2 deny config feature fspf`
	`switch(config-role)# rule 3 permit debug feature zone`
	`switch(config-role)# rule 4 permit exec feature fcping`
		sangroup ロールに属すユーザが、**fspf config** コマンドを除くすべてのコンフィギュレーション コマンドを実行できるようにします。これらのユーザは、**zone debug** コマンドおよび **fcping** EXEC モード コマンドも実行できます。

ステップ 4	`switch(config-role)# no rule 4`	ルール 4 を削除し、sangroup が **fcping** コマンドを実行できないようにします。

ステップ 3 で、ルール 1 が最初に適用され、sangroup ユーザがすべての **config** コマンドにアクセスすることが許可されます。次にルール 2 が適用され、sangroup ユーザには FSPF 設定が拒否されます。結果として、sangroup ユーザは **fspf** コンフィギュレーション コマンドを除く、他のすべての **config** コマンドを実行できます。

（注）　ルールは適用する順序が重要です。これらの 2 つのルールを入れ替え、**deny config feature fspf** ルールを最初に置き、次に **permit config** ルールを置いた場合は、2 番めのルールがグローバルに効果を持って最初のルールに優先するため、sangroup ユーザの全員にすべてのコンフィギュレーション コマンドの実行を許可することになります。

VSAN ポリシーの設定

VSAN ポリシーを設定するには、ENTERPRISE_PKG ライセンスが必要です（第 3 章「ライセンスの入手とインストール」を参照）。

選択した VSAN セットだけにタスクの実行が許可されるように、ロールを設定できます。デフォルトでは、どのロールの VSAN ポリシーも許可に設定されているため、すべての VSAN に対してタスクが実行されます。選択した VSAN セットだけにタスクの実行が許可されるロールを設定できます。1 つのロールに対して選択的に VSAN を許可するには、VSAN ポリシーを拒否に設定し、あとでその設定を許可に設定するか、または適切な VSAN を設定します。

（注）　VSAN ポリシーが拒否に設定されているロールに設定されているユーザは、E ポートの設定を変更できません。これらのユーザが変更できるのは、（ルールの内容に応じて）F ポートまたは FL ポートの設定だけです。これにより、これらのユーザは、ファブリックのコア トポロジに影響する可能性のある設定を変更できなくなります。

ヒント　ロールを使用して、VSAN 管理者を作成できます。設定したルールに応じて、これらの VSAN 管理者は他の VSAN に影響を与えることなく、VSAN に MDS 機能（ゾーン、fcdomain、VSAN プロパティなど）を設定できます。また、ロールが複数の VSAN での処理を許可している場合、VSAN 管理者はこれらの VSAN 間で F ポートまたは FL ポートのメンバーシップを変更できます。

VSAN ポリシーが拒否に設定されているロールに属すユーザのことを、VSAN 制限付きユーザと呼びます。

VSAN ポリシーの変更

（注）　SAN-OS Release 3.x 以前では、VSAN の適用は非 show コマンドに対して実行されますが、すべての show コマンドが適用されるわけではありません。

既存ロールの VSAN ポリシーを変更するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	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)# role name sangroup` `switch(config-role)#`	sangroup ロールのロール コンフィギュレーション サブモードを開始します。
ステップ 3	`switch(config)# vsan policy deny` `switch(config-role-vsan)`	このロールの VSAN ポリシーを **deny** に変更し、VSAN を選択的に許可できるサブモードを開始します。
	`switch(config-role)# no vsan policy deny`	設定されている VSAN ロール ポリシーを削除し、工場出荷時のデフォルト（**permit**）に戻します。
ステップ 4	`switch(config-role-vsan)# permit vsan 10-30`	このロールが、VSAN 10 ～ 30 に許可されたコマンドを実行できるようにします。
	`switch(config-role-vsan)# no permit vsan 15-20`	このロールの権限を、VSAN 15 ～ 20 のコマンドの実行について除外します。したがって、このロールは、VSAN 10 ～ 14、および 21 ～ 30 でコマンドを実行できることになります。

ロールの配信

ロールベース設定は、Cisco Fabric Services（CFS）インフラストラクチャを利用して効率的なデータベース管理を可能にし、ファブリック全体に対するシングル ポイントでの設定を提供します（第 7 章「CFS インフラストラクチャの使用」を参照）。

次の設定が配信されます。

- ロール名と説明
- ロールに対するルールのリスト

- VSAN ポリシーと許可されている VSAN のリスト

この項では、次のトピックについて取り上げます。

- 「ロール データベースの概要」（P.32-5）
- 「ファブリックのロック」（P.32-5）
- 「ロールベース設定変更のコミット」（P.32-5）
- 「ロールベース設定変更の廃棄」（P.32-6）
- 「ロールベース設定の配布のイネーブル化」（P.32-6）
- 「セッションのクリア」（P.32-6）
- 「データベース マージに関する注意事項」（P.32-6）
- 「ロールベース情報の表示」（P.32-7）
- 「配信がイネーブルの場合のロールの表示」（P.32-7）

ロール データベースの概要

ロールベース設定は 2 つのデータベースを利用して設定内容の受け取りと実装を行います。

- コンフィギュレーション データベース：ファブリックで現在実行されているデータベースです。
- 保留中のデータベース：以降の設定変更は保留中のデータベースに保存されます。設定を修正した場合は、保留中のデータベースの変更内容をコンフィギュレーション データベースにコミットするかまたは廃棄する必要があります。その間、ファブリックはロックされた状態になります。保留中のデータベースへの変更は、その変更をコミットするまでコンフィギュレーション データベースに反映されません。

ファブリックのロック

データベースを修正する最初のアクションで保留中のデータベースが作成され、ファブリック全体の機能がロックされます。ファブリックがロックされると、次のような状況になります。

- 他のユーザがこの機能の設定に変更を加えることができなくなります。
- コンフィギュレーション データベースの複製が、最初の変更とともに保留中のデータベースになります。

ロールベース設定変更のコミット

保留中のデータベースに行われた変更をコミットすると、その設定はそのファブリック内のすべてのスイッチにコミットされます。コミットが正常に行われると、設定の変更がファブリック全体に適用され、ロックが解除されます。コンフィギュレーション データベースはこれ以降、コミットされた変更を保持し、保留中のデータベースは消去されます。

ロールベースの設定変更をコミットするには、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)# role commit vsan 3`	ロールベースの設定変更をコミットします。

ロールベース設定変更の廃棄

保留中のデータベースに加えられた変更を廃棄（中断）する場合、コンフィギュレーション データベースは影響を受けないまま、ロックが解除されます。

ロールベースの設定変更を廃棄するには、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)# role abort`	ロールベースの設定変更を廃棄し、保留中のコンフィギュレーション データベースをクリアします。

ロールベース設定の配布のイネーブル化

ロールベース設定の配信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)# role distribute`	ロール ベース設定の配信をイネーブルにします。
	`switch(config)# no role distribute`	ロール ベース設定の配信をディセーブルにします（デフォルト）。

セッションのクリア

ファブリック内の既存のロール セッションを強制的にクリアするには、開始されたセッションに参加中のスイッチから **clear role session** コマンドを発行します。

注意　このコマンドを発行すると、保留中のデータベース内のすべての変更が失われます。

```
switch# clear role session
```

データベース マージに関する注意事項

ファブリックのマージではスイッチ上のロール データベースは変更されません。2 つのファブリックをマージし、それらのファブリックが異なるロール データベースを持つ場合は、ソフトウェアがアラート メッセージを発します。

概念の詳細については、「CFS マージのサポート」（P.7-9）を参照してください。

- ファブリック全体のすべてのスイッチでロール データベースが同一であることを確認してください。
- 必ず目的のデータベースになるように任意のスイッチのロール データベースを編集してから、コミットしてください。これによりファブリック内のすべてのスイッチ上のロール データベースの同期が保たれます。

ロールベース情報の表示

スイッチに設定されたルールを表示するには、**show role** コマンドを使用します。ルールはルール番号別、およびそれぞれのロールに基づいて表示されます。ロール名を指定しなかった場合はすべてのロールが表示されます。例 32-1 を参照してください。

例 32-1　　すべてのロールに関する情報の表示

```
switch# show role
Role: network-admin
Description: Predefined Network Admin group.This role cannot be modified
Access to all the switch commands

Role: network-operator
Description: Predefined Network Operator group.This role cannot be modified
Access to Show commands and selected Exec commands

Role: svc-admin
Description: Predefined SVC Admin group.This role cannot be modified
Access to all SAN Volume Controller commands

Role: svc-operator
Description: Predefined SVC Operator group.This role cannot be modified
Access to selected SAN Volume Controller commands

[Role]：TechDocs
  vsan policy: permit (default)

Role: sangroup
  Description: SAN management group
  vsan policy: deny
  Permitted vsans: 10-30

  ----------------------------------------------
  Rule    Type    Command-type      Feature
  ----------------------------------------------
    1.   permit    config                  *
    2.     deny    config               fspf
    3.   permit     debug               zone
    4.   permit      exec             fcping
```

配信がイネーブルの場合のロールの表示

コンフィギュレーション データベースを表示するには、**show role** コマンドを使用します。

配信がロール設定に対してイネーブルかどうか、現在のファブリック ステータス（ロックまたはロック解除）、および最後に実行された動作を表示するには、**show role status** コマンドを使用します。例 32-2 を参照してください。

例 32-2　　ロール ステータス情報の表示

```
switch# show role status
Distribution: Enabled
Session State: Locked

Last operation (initiated from this switch): Distribution enable
Last operation status: Success
```

保留中のロール データベースを表示するには、**show role pending** コマンドを使用します。

例 32-3 は、この手順に従って **show role pending** コマンドを実行した出力を示しています。

1. **role name myrole** コマンドを使用して myrole というロールを作成します。
2. **rule 1 permit config feature fspf** コマンドを発行します。
3. **show role pending** コマンドを発行して、出力を表示します。

例 32-3　保留中のロール データベース情報の表示

```
switch# show role pending
Role: network-admin
Description: Predefined Network Admin group.This role cannot be modified
Access to all the switch commands

Role: network-operator
Description: Predefined Network Operator group.This role cannot be modified
Access to Show commands and selected Exec commands

Role: svc-admin
Description: Predefined SVC Admin group.This role cannot be modified
Access to all SAN Volume Controller commands

Role: svc-operator
Description: Predefined SVC Operator group.This role cannot be modified
Access to selected SAN Volume Controller commands

[Role] : TechDocs
  vsan policy: permit (default)

Role: sangroup
  Description: SAN management group
  vsan policy: deny
  Permitted vsans: 10-30

  ----------------------------------------------
  Rule    Type    Command-type      Feature
  ----------------------------------------------
    1.   permit    config                  *
    2.     deny    config               fspf
    3.   permit     debug               zone
    4.   permit      exec             fcping

Role: myrole
  vsan policy: permit (default)
  ----------------------------------------------
  Rule    Type    Command-type      Feature
  ----------------------------------------------
    1.   permit    config               fspf
```

保留中のロール データベースとコンフィギュレーションのロール データベースの相違を表示するには、**show role pending-diff** コマンドを使用します。例 32-4 を参照してください。

例 32-4　2 つのデータベースの相違の表示

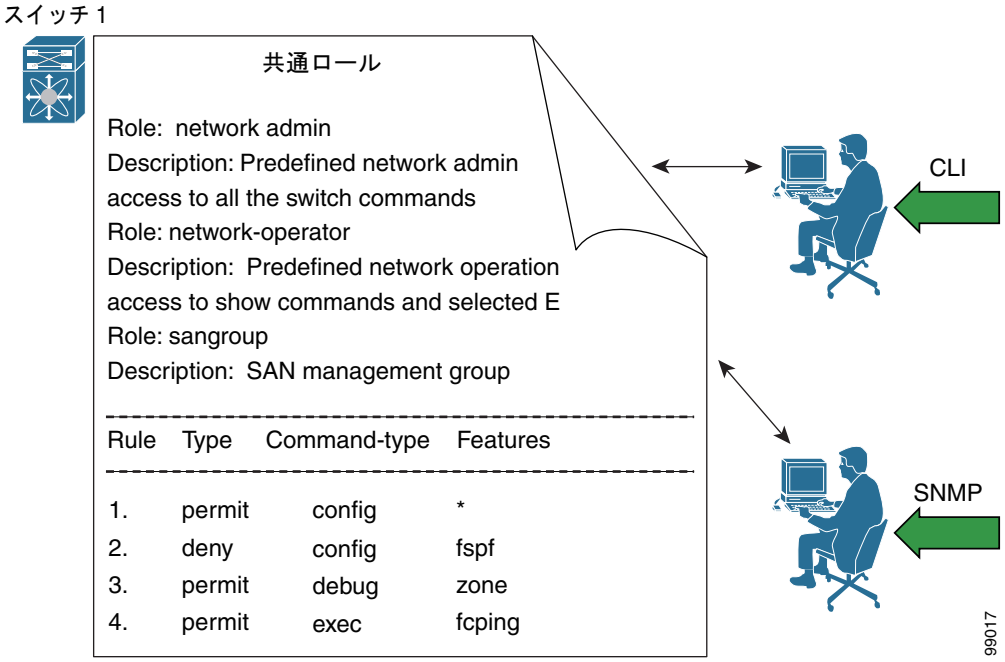
```
switch# show role pending-diff
    +Role: myrole
    +  vsan policy: permit (default)
    +  ----------------------------------------------
    +  Rule    Type    Command-type      Feature
    +  ----------------------------------------------
```

```
    +    1.   permit    config                fspf
```

共通ロールの設定

Cisco MDS 9000 ファミリのすべてのスイッチで、CLI と SNMP は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（図 32-1 を参照）。

図 32-1　　共通ロール



SNMP の各ロールは、CLI を通じて作成または変更されたロールと同じです（「ロールベースの認証」（P.32-1）を参照）。

各ロールは、必要に応じて 1 つ以上の VSAN に制限できます。

SNMP または CLI を使用して、新しいロールの作成、または既存のロールの変更を実行できます。

- SNMP：CISCO-COMMON-ROLES-MIB を使用してロールを設定または変更します。詳細については、『*Cisco MDS 9000 Family MIB Quick Reference*』を参照してください。
- CLI：**role name** コマンドを使用します。

CLI オペレーションから SNMP へのマッピング

SNMP では、GET、SET、および NOTIFY の 3 つの操作だけを行うことができます。CLI では、DEBUG、SHOW、CONFIG、CLEAR、および EXEC の 5 つの操作を行うことができます。

（注）　NOTIFY には、CLI の syslog メッセージのような制限はありません。

表 32-1 は、CLI オペレーションが SNMP オペレーションにどのようにマッピングされるかを示します。

表 32-1　CLI オペレーションから SNMP オペレーションへのマッピング

CLI オペレーション	SNMP オペレーション
DEBUG	Ignored
SHOW	GET
CONFIG	SET
CLEAR	SET
EXEC	SET

例 32-5 に、my_role という名前のロールの CLI 操作を SNMP 操作へマッピングする特権およびルールを示します。

例 32-5　CLI 操作から SNMP 操作へのマッピングの表示

```
switch# show role name my_role
Role:my_role
  vsan policy:permit (default)
  ----------------------------------------------
  Rule    Type    Command-type      Feature
  ----------------------------------------------
    1.   permit     clear                 *
    2.     deny     clear                ntp
    3.   permit    config                 *
    4.     deny    config                ntp
    5.   permit     debug                 *
    6.     deny     debug                ntp
    7.   permit      show                 *
    8.     deny      show                ntp
    9.   permit      exec                 *
```

（注） ルール 4 では、CONFIG は NTP では拒否されますが、ルール 9 によって、NTP MIB オブジェクトに対する SET は許可されます。これは、EXEC も SNMP SET 操作にマッピングされているためです。

ユーザ アカウントの設定

Cisco MDS 9000 ファミリ スイッチでは、すべてのユーザのアカウント情報がシステムに保管されます。ユーザの認証情報、ユーザ名、ユーザ パスワード、パスワードの有効期限、およびロール メンバーシップが、そのユーザのユーザ プロファイルに保存されます。

ここで説明するタスクを利用すると、ユーザの作成および既存ユーザのプロファイルの修正を実行できます。これらのタスクは管理者によって定義されている特権ユーザに制限されます。

この項では、次のトピックについて取り上げます。

- 「ユーザの概要」（P.32-11）
- 「強力なパスワードの特性」（P.32-11）
- 「ユーザの設定」（P.32-12）
- 「ユーザのログアウト」（P.32-13）

- 「ユーザ アカウント情報の表示」（P.32-13）

ユーザの概要

snmp-server user オプションで指定したパスフレーズと **username** オプションで指定したパスワードは同期されます（「SNMPv3 CLI のユーザ管理と AAA の統合」（P.33-3）を参照）。

デフォルトでは、明示的に期限を指定しないかぎり、ユーザ アカウントは無期限に有効です。**expire** オプションを使用すると、ユーザ アカウントをディセーブルにする日付を設定できます。日付は YYYY-MM-DD 形式で指定します。

（注） 1 つのスイッチには、最大 256 ユーザを設定できます。

ヒント bin、daemon、adm、lp、sync、shutdown、halt、mail、news、uucp、operator、games、gopher、ftp、nobody、nscd、mailnull、rpc、rpcuser、xfs、gdm、mtsuser、ftpuser、man、sys は予約語で、ユーザの設定には使用できません。

（注） ユーザ パスワードはスイッチ コンフィギュレーション ファイルに表示されません。

ヒント パスワードが簡潔である場合（短く、解読しやすい場合）、パスワード設定は拒否されます。サンプル設定のように、強力なパスワードを設定してください。パスワードでは大文字と小文字が区別されます。「admin」は Cisco MDS 9000 ファミリ スイッチのデフォルト パスワードではなくなりました。強力なパスワードを明確に設定する必要があります。

注意 TACACS+、RADIUS、またはローカルのいずれで作成されたものであっても、Cisco MDS SAN-OS はすべてが数字のユーザ名はサポートしません。すべて数字の名前を持つローカル ユーザは作成できません。AAA サーバに数字だけのユーザ名が存在する場合、ログイン時に入力しても、そのユーザはログインできません。

ヒント トラブルシューティングのために **internal** キーワードを指定してコマンドを発行するには、network-admin グループのメンバーであるアカウントが必要です。

強力なパスワードの特性

強力なパスワードは、次の特性を持ちます。

- 長さが 8 文字以上である
- 複数の連続する文字（「abcd」など）を含んでいない
- 複数の同じ文字の繰り返し（「aaabbb」など）を含んでいない
- 辞書に載っている単語を含んでいない

- 正しい名前を含んでいない
- 大文字と小文字の両方を含んでいない。
- 数字が含まれている

強力なパスワードの例を次に示します。

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

（注） クリア テキストのパスワードには、アルファベットと数字だけを含めることができます。ドル記号（$）は使用できません。

ユーザの設定

新規ユーザの設定または既存ユーザのプロファイル修正を行うには、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)# username usam password abcd123AAA expire 2003-05-31`	ユーザ アカウント（usam）を作成または更新し、パスワード（abcd123AAA）および有効期限 2003-05-31 を設定します。パスワードは 64 文字に制限されています。 **（注）** ユーザ アカウント名には、数値以外の文字を含める必要があります。
	`switch(config)# username msam password 0 abcd12AAA role network-operator`	ユーザ アカウント（msam）を作成または更新し、クリア テキスト（0 で示される）のパスワード（abcd12AAA）を設定します。パスワードは 64 文字に制限されています。 **（注）** ユーザ アカウント名には、数値以外の文字を含める必要があります。
	`switch(config)# username user1 password 5 !@*asdsfsdfjh!@df`	ユーザ アカウント（user1）に暗号化（5 で指定される）パスワード（!@*asdsfsdfjh!@df）を指定します。
ステップ 3	`switch(config)# username usam role network-admin`	network-admin ロールに指定のユーザ（usam）を追加します。
	`switch(config)# no username usam role vsan-admin`	vsan-admin ロールから指定のユーザ（usam）を削除します。

	コマンド	目的
ステップ 4	switch(config)# **username admin sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAtjIHrIt/3dDeohix6JcRSIYZ0EOdJ3l5RONWcwSgAuTUSrLk 3a9hdYkzY94fhHmNGQGCjVg+8cbOxyH4Z1jcVFcrDogtQT+Q8dveqts/8XQhqkNAFeGy4u8TJ2Us oreCU6DlibwkpzDafzKTpA5vB6FmHd2TI6Gnse9FUgKD5fs=**	既存のユーザ アカウント（admin）の SSH キーを指定します。
	switch(config)# **no username admin sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAtjIHrIt/3dDeohix6JcRSIYZ0EOdJ3l5RONWcwSgAuTUSrLk 3a9hdYkzY94fhHmNGQGCjVg+8cbOxyH4Z1jcVFcrDogtQT+Q8dveqts/8XQhqkNAFeGy4u8TJ2Us oreCU6DlibwkpzDafzKTpA5vB6FmHd2TI6Gnse9FUgKD5fs=**	ユーザ アカウント（admin）の SSH キーを削除します。
ステップ 5	switch(config)# **username usam ssh-cert-dn usam-dn dsa**	既存のユーザ アカウント（usam）の認証に使用する SSH X.509 証明書の識別名と DSA アルゴリズムを指定します。
	switch(config)# **username user1 ssh-cert-dn user1-dn rsa**	既存のユーザ アカウント（user1）の認証に使用する SSH X.509 証明書の識別名と RSA アルゴリズムを指定します。
	switch(config)# **no username admin ssh-cert-dn admin-dn dsa**	ユーザ アカウント（admin）の SSH X.509 証明書の識別名を削除します。

ユーザのログアウト

スイッチの他のユーザをログアウトするには、**clear user** コマンドを使用します。

次の例では、vsam という名前のユーザが、スイッチからログアウトされます。

```
switch# clear user vsam
```

ログインしているユーザのリストを表示するには、**show users** コマンドを使用します（例 32-6 を参照）。

例 32-6　　ログインしているすべてのユーザの表示

```
switch# show users
admin    pts/7        Jan 12 20:56 (10.77.202.149)
admin    pts/9        Jan 12 23:29 (user.example.com)
admin    pts/10       Jan 13 03:05 (dhcp-10-10-1-1.example.com)
admin    pts/11       Jan 13 01:53 (dhcp-10-10-2-2.example.com)
```

ユーザ アカウント情報の表示

ユーザ アカウントに関して設定されている情報を表示するには、**show user-account** コマンドを使用します。例 32-7 ～ 32-8 を参照してください。

例 32-7　　指定したユーザに関する情報の表示

```
switch# show user-account user1
user:user1
        this user account has no expiry date
        roles:network-operator
no password set.Local login not allowed
```

```
Remote login through RADIUS is possible
```

例 32-8　　すべてのユーザに関する情報の表示

```
switch# show user-account
show user-account
user:admin
        this user account has no expiry date
        roles:network-admin
user:usam
        expires on Sat May 31 00:00:00 2003
        roles:network-admin network-operator
user:msam
        this user account has no expiry date
        roles:network-operator
user:user1
        this user account has no expiry date
        roles:network-operator
no password set.local login not allowed
Remote login through RADIUS is possible
```

SSH サービスの設定

Cisco MDS 9000 ファミリのすべてのスイッチで、Telnet サービスはデフォルトでイネーブルです。SSH サービスをイネーブルにする場合は、事前にサーバ キーペアを生成してください（「SSH サーバ キーペアの生成」（P.32-15）を参照）。

サーバ キーを生成するには、**ssh key** コマンドを使用します。

注意　SSH を使用してスイッチにログインするときに、**aaa authentication login default none** コマンドが発行済みの場合、ログインするには 1 つまたは複数のキー ストロークを入力する必要があります。キー ストロークをまったく入力しないで Enter キーを押すと、ログインが拒否されます。

この項では、次のトピックについて取り上げます。

- 「SSH の概要」（P.32-14）
- 「SSH サーバ キーペアの生成」（P.32-15）
- 「SSH キーの指定」（P.32-15）
- 「生成したキーペアの上書き」（P.32-16）
- 「SSH ホストのクリア」（P.32-17）
- 「SSH または Telnet サービスのイネーブル化」（P.32-18）
- 「SSH プロトコル ステータスの表示」（P.32-18）
- 「デジタル証明書を使用した SSH 認証」（P.32-19）

SSH の概要

SSH は Cisco SAN-OS CLI にセキュアなコミュニケーションを提供します。SSH キーは、次の SSH オプションに使用できます。

- SSH1
- RSA を使用する SSH2
- DSA を使用する SSH2

SSH サーバ キーペアの生成

SSH サービスをイネーブルにする前に、適切なバージョンの SSH サーバ キー ペアを取得してください。使用する SSH クライアントのバージョンに応じた SSH サーバ キー ペアを生成します。各キーペアに指定するビット数は、768 ～ 2048 です。

SSH サービスでは、SSH バージョン 1 と 2 で使用される 3 種類のキーペアが受け入れられます。

- **rsa1** オプションを使用すると、SSH バージョン 1 プロトコルに対応する RSA1 キーペアが生成されます。
- **dsa** オプションを使用すると、SSH バージョン 2 プロトコルに対応する DSA キーペアが生成されます。
- **rsa** オプションを使用すると、SSH バージョン 2 プロトコルに対応する RSA キーペアが生成されます。

注意　SSH キーをすべて削除した場合、新しい SSH セッションを開始できません。

SSH サーバ キーペアを生成する手順は、次のとおりです。

	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)# ssh key rsa1 1024`
	`generating rsa1 key.....`
	`generated rsa1 key`
		RSA1 サーバ キーペアを生成します。

	`switch(config)# ssh key dsa 1024`
	`generating dsa key.....`
	`generated dsa key`
		DSA サーバ キーペアを生成します。

	`switch(config)# ssh key rsa 1024`
	`generating rsa key.....`
	`generated rsa key`
		RSA サーバ キーペアを生成します。

	`switch(config)# no ssh key rsa 1024` `cleared RSA keys`	RSA サーバ キーペアの設定をクリアします。

SSH キーの指定

SSH キーを指定すると、パスワードを要求されることなく、SSH クライアントを使用してログインできます。SSH キーは次の 3 種類の形式で指定できます。

- Open SSH 形式
- Internet Engineering Task Force（IETF）SECSH 形式
- Privacy Enhanced Mail（PEM）形式の公開キー証明書

指定したユーザの OpenSSH 形式の SSH キーを指定または削除するには、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)# **username admin sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAtjIHrIt/3dDeohix6JcRSIYZ0EOdJ3l5RONWcwSgAuTUSrLk3a9hdYkzY94fhHmNGQGCjVg+8cbOxyH4Z1jcVFcrDogtQT+Q8dveqts/8XQhqkNAFeGy4u8TJ2UsoreCU6DlibwkpzDafzKTpA5vB6FmHd2TI6Gnse9FUgKD5fs=**	ユーザ アカウント（admin）の SSH キーを指定します。
	switch(config)# **no username admin sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAtjIHrIt/3dDeohix6JcRSIYZ0EOdJ3l5RONWcwSgAuTUSrLk3a9hdYkzY94fhHmNGQGCjVg+8cbOxyH4Z1jcVFcrDogtQT+Q8dveqts/8XQhqkNAFeGy4u8TJ2UsoreCU6DlibwkpzDafzKTpA5vB6FmHd2TI6Gnse9FUgKD5fs=**	ユーザ アカウント（admin）の SSH キーを削除します。

指定したユーザの IETF SECSH 形式の SSH キーを指定または削除するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# **copy tftp://10.10.1.1/secsh_file.pub bootflash:secsh_file.pub**	IETF SECSH 形式の SSH キーを含むファイルをダウンロードします。
ステップ 2	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 3	switch(config)# **username admin sshkey file bootflash:secsh_file.pub**	ユーザ アカウント（admin）の SSH キーを指定します。
	switch(config)# **no username admin sshkey file bootflash:secsh_file.pub**	ユーザ アカウント（admin）の SSH キーを削除します。

指定したユーザの PEM フォーマット化された公開キー証明書形式の SSH キーを指定または削除するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# **copy tftp://10.10.1.1/cert.pem bootflash:cert.pem**	PEM フォーマット化された公開キー証明書形式の SSH キーを含むファイルをダウンロードします。
ステップ 2	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 3	switch(config)# **username admin sshkey file bootflash:cert.pem**	ユーザ アカウント（usam）の SSH キーを指定します。
	switch(config)# **no username admin sshkey file bootflash:cert.pem**	ユーザ アカウント（usam）の SSH キーを削除します。

生成したキーペアの上書き

必要なバージョンの SSH キーペア オプションがすでに生成されている場合は、前回生成されたキーペアをスイッチに上書きさせることができます。

前回生成されたキーペアを上書きするには、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)# ssh key dsa 768`
	`ssh key dsa 512`
	`dsa keys already present, use force`
	`option to overwrite them`
	`switch(config)# ssh key dsa 512 force`
	`deleting old dsa key.....`
	`generating dsa key.....`
	`generated dsa key`
		サーバ キーペアの設定を試みます。必要なサーバ キーペアがすでに設定されている場合は、**force** オプションを使用して、そのサーバ キーペアを上書きします。
		古い DSA キーを削除し、新しく指定されたビットを使用してサーバ キーペアを設定します。

SSH ホストのクリア

clear ssh hosts コマンドは、信頼できる SSH ホストの既存のリストをクリアし、SCP/SFTP を特定のホストの **copy** コマンドとともに使用することを再許可します。

SCP/SFTP を **copy** コマンドとともに使用する場合は、信頼できる SSH ホストのリストが作成され、スイッチ内に保存されます（例 32-9 を参照）。

例 32-9　SCP/SFTP を使用したファイルのコピー

```
switch# copy scp://abcd@10.10.1.1/users/abcd/abc
bootflash:abc The authenticity of host '10.10.1.1 (10.10.1.1)'
can't be established.
RSA1 key fingerprint is 01:29:62:16:33:ff:f7:dc:cc:af:aa:20:f8:20:a2:db.
Are you sure you want to continue connecting (yes/no)?yes
Added the host to the list of known hosts
(/var/home/admin/.ssh/known_hosts).[SSH key information about the host is
stored on the switch]
abcd@10.10.1.1's password:
switch#
```

copy コマンドとともに SCP/SFTP を使用する前にホストの SSH キーが変更された場合は、エラーが表示されます（例 32-10 を参照）。

例 32-10　SCP/SFTP を使用したファイルのコピー（SSH キーの変更によるエラーの発生）

```
switch# copy scp://apn@10.10.1.1/isan-104
bootflash:isan-ram-1.0.4
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA1 host key has just been changed.
The fingerprint for the RSA1 key sent by the remote host is
36:96:ca:d7:29:99:79:74:aa:4d:97:49:81:fb:23:2f.
Please contact your system administrator.
Add correct host key in /mnt/pss/.ssh/known_hosts to get rid of this
message.
Offending key in /mnt/pss/.ssh/known_hosts:2
RSA1 host key for 10.10.1.1 has changed and you have requested strict
checking.
```

SSH または Telnet サービスのイネーブル化

デフォルトでは、SSH サービスはディセーブルです。

SSH サービスをイネーブルまたは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`	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)# ssh server enable` `updated`	SSH サービスの使用をイネーブルにします。
	`switch(config)# no ssh server enable` `updated`	SSH サービスの使用をディセーブル（デフォルト）にし、スイッチを工場出荷時のデフォルトにリセットします。

SSH プロトコル ステータスの表示

SSH プロトコルのステータス（イネーブルまたはディセーブル）、およびそのスイッチでイネーブルになっているバージョンを表示するには、**show ssh server** コマンドを使用します（例 32-11 を参照）。

例 32-11　SSH プロトコル ステータスの表示

```
switch# show ssh server
ssh is enabled
version 1 enabled
version 2 enabled
```

指定されたキーまたはすべてのキーのサーバ キーペアの詳細を表示するには、**show ssh key** コマンドを使用します（例 32-12 を参照）。

例 32-12　サーバ キーペアの詳細の表示

```
switch# show ssh key
rsa1 Keys generated:Sun Jan 13 07:16:26 1980
1024 35
fingerprint:
1024 67:76:02:bd:3e:8d:f5:ad:59:5a:1e:c4:5e:44:03:07
could not retrieve rsa key information
dsa Keys generated:Sun Jan 13 07:40:08 1980
ssh-dss
AAAAB3NzaC1kc3MAAABBAJTCRQOydNRel2v7uiO6Fix+OTn8eGdnnDVxw5eJs5OcOEXOyjaWcMMYsEgxc9ada1NElp
8Wy7GPMWGOQYj9CU0AAAAVAMCcWhNN18zFNOIPo7cU3t7d0iEbAAAAQBdQ8UAOi/Cti84qFb3kTqXlS9mEhdQUo0lH
cH5bw5PKfj2Y/dLR437zCBKXetPj4p7mhQ6Fq5os8RZtJEyOsNsAAABAA0oxZbPyWeR5NHATXiyXdPI7j9i8fgyn9F
NipMkOF2Mn75Mi/lqQ4NIq0gQNvQOx27uCeQlRts/QwI4q68/eaw=
fingerprint:
512 f7:cc:90:3d:f5:8a:a9:ca:48:76:9f:f8:6e:71:d4:ae
```

（注）　SSH を使用してスイッチにログインするときに、**aaa authentication login default none CLI** コマンドが発行済みの場合、ログインするには 1 つまたは複数のキー ストロークを入力する必要があります。キー ストロークをまったく入力しないで Enter キーを押すと、ログインが拒否されます。

デジタル証明書を使用した SSH 認証

Cisco MDS 9000 ファミリ スイッチ製品の SSH 認証はホスト認証に X.509 デジタル証明書のサポートを提供します。X.509 デジタル証明書は出処と完全性を保証する 1 つのデータ項目です。保護された通信を行うための暗号キーを含み、提出者の身元を証明するために、信頼できる認証局（CA）によって「署名」されています。X.509 デジタル証明書のサポートにより、認証に DSA と RSA のいずれかのアルゴリズムを使用します。

証明書インフラストラクチャは Secure Socket Layer（SSL）をサポートする最初の証明書を使用し、セキュリティ インフラストラクチャにより照会または通知の形で返信を受け取ります。証明書が信頼できる CA のいずれかから発行されたものであれば、証明書の検証は成功です。

スイッチは、X.509 証明書を使用する SSH 認証、または公開キー証明書を使用する SSH 認証のいずれかに設定できますが、両方に設定することはできません。いずれかに設定されている場合は、その認証が失敗すると、パスワードの入力を求められます。

CA およびデジタル証明書の詳細については、第 36 章「認証局およびデジタル証明書の設定」を参照してください。

管理者パスワードの回復

次の 2 通りの方法のいずれかで管理者パスワードを回復できます。

- network-admin 権限を持つユーザ名による CLI の使用
- スイッチの電源再投入

この項では、次の項目について説明します。

- 「network admin 権限での CLI の使用」（P.32-19）
- 「スイッチの電源の再投入」（P.32-20）

network admin 権限での CLI の使用

network-admin 権限を持つユーザ名でスイッチにログインしているか、ログインできる場合に、管理者パスワードを回復するには、次の手順を実行します。

ステップ 1　ユーザ名に network-admin 権限があることを確認するには、**show user-accounts** コマンドを使用します。

```
switch# show user-account
user:admin
        this user account has no expiry date
        roles:network-admin

user:dbgusr
        this user account has no expiry date
        roles:network-admin network-operator
```

ステップ 2　ユーザ名に network-admin 権限がある場合は、**username** コマンドを発行して新しい管理者パスワードを割り当てます。

```
switch# config t
switch(config)# username admin password <new password>
switch(config)# exit
switch#
```

ステップ 3　ソフトウェア コンフィギュレーションを保存します。

```
switch# copy running-config startup-config
```

スイッチの電源の再投入

network-admin 特権を持つスイッチ上でセッションを開始できない場合は、スイッチの電源を再投入して管理者パスワードを回復する必要があります。

注意　この手順を実行すると、スイッチ上のすべてのトラフィックが中断されます。スイッチとの接続はすべて 2 ～ 3 分間切断されます。

（注）　管理者パスワードは、Telnet または Secure Shell（SSH; セキュア シェル）セッションからは回復できません。ローカル コンソール接続を使用できる必要があります。コンソール接続の設定の詳細については、「Cisco MDS 9000 ファミリのスイッチの始動」（P.5-2）を参照してください。

スイッチの電源を再投入して、管理者パスワードを回復するには、次の手順を実行します。

ステップ 1　2 つのスーパーバイザ モジュールを搭載した Cisco MDS 9500 シリーズ スイッチの場合は、シャーシのスロット 6 からスーパーバイザ モジュールを取り外します。

（注）　Cisco MDS 9500 シリーズでは、パスワード回復手順をアクティブなスーパーバイザ モジュールで実行する必要があります。スロット 6 のスーパーバイザ モジュールを取り外すことで、パスワード回復手順中にスイッチオーバーが発生しないようにします。

ステップ 2　スイッチの電源を再投入します。

ステップ 3　スイッチが Cisco SAN-OS ソフトウェアのブート シーケンスを開始したときに **Ctrl+]** キー シーケンスを押して、`switch(boot)#` プロンプト モードを開始します。

```
Ctrl+]
switch(boot)#
```

ステップ 4　コンフィギュレーション モードに切り替えます。

```
switch(boot)# config terminal
```

ステップ 5　**admin-password** コマンドを発行して、管理者パスワードをリセットします。

```
switch(boot-config)# admin-password <new password>
```

強力なパスワードの詳細については、「強力なパスワードの特性」（P.32-11）を参照してください。

ステップ 6　EXEC モードに切り替えます。

```
switch(boot-config)# exit
switch(boot)#
```

ステップ 7　**load** コマンドを発行して、Cisco SAN-OS ソフトウェアをロードします。

```
switch(boot)# load bootflash:m9500-sf1ek9-mz.2.1.1a.bin
```

注意　コンフィギュレーションを保存するために使用するイメージより古いシステム イメージをブートし、**install all** コマンドを使用せずにシステムをブートする場合、スイッチはバイナリ コンフィギュレーションを消去し、ASCII コンフィギュレーションを使用します。この場合は、**init system** コマンドを使用してパスワードを回復する必要があります。

ステップ 8　新しい管理者パスワードを使用してスイッチにログインします。

```
switch login: admin
Password: <new password>
```

ステップ 9　Fabric Manager の SNMP パスワードとしても使用できるようにするために、新しいパスワードをリセットします。

```
switch# config t
switch(config)# username admin password <new password>
switch(config)# exit
switch#
```

ステップ 10　ソフトウェア コンフィギュレーションを保存します。

```
switch# copy running-config startup-config
```

ステップ 11　以前に取り外したスーパーバイザ モジュールをシャーシのスロット 6 に挿入します。

デフォルト設定

表 32-2 に、スイッチのすべてのスイッチ セキュリティ機能のデフォルト設定を示します。

表 32-2　スイッチ セキュリティのデフォルト設定

パラメータ	デフォルト
Cisco MDS スイッチでのロール	ネットワーク管理者（network-operator）
AAA 設定サービス	Local
認証ポート	1812
アカウンティング ポート	1813
事前共有キーの送受信	クリア テキスト
RADIUS サーバ タイムアウト	1 秒
RADIUS サーバ再試行	1 回
TACACS+	ディセーブル
TACACS+ サーバ	未設定
TACACS+ サーバのタイムアウト	5 秒
AAA サーバへの配信	ディセーブル
ロールに対する VSAN ポリシー	許可
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
アカウンティング ログ サイズ	250 KB

表 32-2　スイッチ セキュリティのデフォルト設定 （続き）

パラメータ	デフォルト
SSH サービス	ディセーブル
Telnet サービス	イネーブル