CHAPTER 22

ユーザ アカウントと RBAC の設定

この章では、Cisco Nexus 4001I/4005I Switch Module for IBM BladeCenter でユーザ アカウントと Role-Based Access Control（RBAC; ロールベース アクセス コントロール）を設定する方法を説明します。

この章で説明する内容は、次のとおりです。

- 「ユーザ アカウントと RBAC の概要」（P.22-1）
- 「注意事項と制限事項」（P.22-3）
- 「ユーザ アカウントの設定」（P.22-4）
- 「RBAC の設定」（P.22-5）
- 「ユーザ アカウントと RBAC の設定の確認」（P.22-9）
- 「ユーザ アカウントと RBAC 設定の例」（P.22-9）
- 「デフォルト設定」（P.22-10）

ユーザ アカウントと RBAC の概要

ユーザ アカウントを作成して管理し、スイッチ上で行える操作を制限するロールを割り当てることができます。RBAC は、ユーザが実行する必要のある管理操作の許可を制限するロールの割り当ての規則を定義することを可能にします。

ここでは、次の内容について説明します。

- 「ユーザ アカウントについて」（P.22-1）
- 「強固なパスワードの特性」（P.22-2）
- 「ユーザ ロールについて」（P.22-2）
- 「規則について」（P.22-3）
- 「ユーザ ロール ポリシーについて」（P.22-3）

ユーザ アカウントについて

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）　ユーザのパスワードは、設定ファイルでは表示されません。

注意　そのユーザ名が TACACS+ または RADIUS で作成されたのか、ローカルで作成されたのかに関係なく、スイッチでは、すべて数値のユーザ名はサポートされません。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 サーバ上にすべて数字のユーザ名が存在して、それがログインで入力された場合、そのユーザはログインできません。

強固なパスワードの特性

強固なパスワードは、次の特性を持ちます。

- 長さ 8 文字以上
- 連続的な文字（「abcd」など）を多く含まない
- 繰り返し文字（「aaabbb」など）を多く含まない
- 辞書ワードを含まない
- 正式な名前を含まない
- 小文字、大文字、数字、特殊文字のうちの少なくとも 3 種類の組み合わせになっている

強固なパスワードの例を次に示します。

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

ヒント　パスワードが脆弱な場合（短い、解読されやすいなど）、スイッチはそのパスワード設定を拒否します。サンプル設定にあるような強固なパスワードを設定してください。パスワードの大文字小文字は区別されます。
クリアテキストのパスワードに、ドル記号（$）やスペースを含めることは一切できません。また、パスワードの先頭に引用符（" または '）、縦棒（|）、大なり記号（>）などの特殊文字を含めることもできません。

ユーザ ロールについて

ユーザ ロールには、そのロールを割り当てられたユーザが実行できる操作を定義する規則が含まれています。各ユーザ ロールに複数の規則を含めることができ、各ユーザが複数のロールを持つことができます。たとえば、ロール 1 では設定操作の実行だけが許可されており、ロール 2 ではデバッグ操作の実行だけが許可されている場合、ロール 1 とロール 2 の両方に属するユーザは、設定操作とデバッグ操作を実行できます。特定の VLAN やインターフェイスだけにアクセスを制限することもできます。

スイッチには、次のデフォルト ユーザ ロールが用意されています。

- network-admin（スーパーユーザ）：スイッチ全体に対して完全な読み取りと書き込みのアクセス権を持ちます。
- network-operator：スイッチに対して完全な読み取りアクセス権を持ちます。

（注）　複数のロールに属するユーザは、そのロールで許可されるすべてのコマンドの組み合わせを実行できます。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、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が拒否されたロール A を持っていたとします。また、コンフィギュレーション コマンドへのアクセスが許可されたロール B も持っていたとします。この場合、ユーザはコンフィギュレーション コマンドを使用できます。

規則について

規則は、ロールの基本要素です。規則は、そのロールがユーザにどの操作の実行を許可するかを定義します。規則は次のパラメータで適用できます。

- Command：コマンドまたは正規表現で定義された一連のコマンド。
- Feature：スイッチにより提供される機能に適用されるコマンド。
  - **show role feature** コマンドを入力すれば、このパラメータに指定できる機能名が表示されます。
- Feature group：デフォルトまたはユーザ定義の機能グループ。
  - **show role feature-group** コマンドを入力すれば、このパラメータに指定できるデフォルトの機能グループが表示されます。

これらのパラメータは、階層状の関係を作成します。最も基本的な制御パラメータは command です。次の制御パラメータは feature です。これは、その機能にアソシエートされているすべてのコマンドを表します。最後の制御パラメータが、feature group です。feature group は、関連のある機能を結合して、既存の管理が簡単に行えるようにします。

各ロールに、最大 256 個の規則を設定できます。規則が適用される順序は、ユーザ指定の規則番号で決まります。規則は、降順で適用されます。たとえば、1 つのロールが 3 つの規則を持っている場合、規則 3 が規則 2 よりも前に適用され、規則 2 は規則 1 よりも前に適用されます。

ユーザ ロール ポリシーについて

ユーザ ロール ポリシーを定義することにより、ユーザがアクセスできるスイッチ リソースを制限できます。ユーザ ロール ポリシーを定義して、インターフェイス、および VLAN へのアクセスを制限できます。

ユーザ ロール ポリシーは、ロールに定義されている規則で制約されます。たとえば、特定のインターフェイスへのアクセスを許可するインターフェイス ポリシーを定義した場合、インターフェイス コマンドを許可するコマンド規則をロールに設定しないと、ユーザはインターフェイスにアクセスできません。「ユーザ ロール インターフェイス ポリシーの変更」（P.22-8）に、設定例があります。

コマンド規則が特定のリソース（インターフェイス、または VLAN）へのアクセスを許可する場合、たとえそれがそのユーザにアソシエートされているユーザ ロール ポリシーにリストされていなくても、ユーザにはこれらのリソースへのアクセスが許可されます。

注意事項と制限事項

ユーザ アカウントと RBAC には、次の設定ガイドラインと制限事項があります。

- ユーザ ロールには最大 256 個の規則を追加できます。

- 1 つのユーザ アカウントに最大 64 個のユーザ ロールを割り当てられます。

（注）　ユーザ アカウントは、少なくとも 1 つのユーザ ロールを持たなければなりません。

ユーザ アカウントの設定

1 つのスイッチ上に最大 256 個のユーザ アカウントを作成できます。ユーザ アカウントは、次の属性を持ちます。

- ユーザ名
- パスワード
- 失効日
- ユーザ ロール

ユーザ アカウントは、最大 64 個のユーザ ロールを持つことができます。ユーザ ロールの詳細については、「RBAC の設定」（P.22-5）を参照してください。

（注）　ユーザ アカウントの属性に加えられた変更は、そのユーザがログインして新しいセッションを作成するまで有効になりません。

ユーザ アカウントを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# show role`	（任意）使用可能なユーザ ロールを表示します。必要に応じて、ユーザ ロールを設定できます（「ユーザ ロールと規則の作成」（P.22-5）を参照してください）。
ステップ 2	`switch# configure 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 3	`switch(config)# username` *user-id* `[password` *password*`] [expire` *date*`] [role` *role-name*`]`	ユーザ アカウントを設定します。*user-id* 引数は、最大 28 文字の長さの英数字のストリングで、大文字小文字が区別されます。 デフォルト パスワードは定義されていません。 （注）　パスワードを指定しなかった場合、ユーザはスイッチにログインできません。 **expire** *date* オプションの形式は、YYYY-MM-DD です。デフォルトでは、失効日はありません。
ステップ 4	`switch(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 5	`switch# show user-account`	（任意）ロールの設定を表示します。
ステップ 6	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、ユーザ アカウントを設定する例を示します。

```
switch# configure terminal
switch(config)# username NewUser password 4Ty18Rnt
switch(config)# exit
switch# show user-account
switch# copy running-config startup-config
```

RBAC の設定

ここでは、次の内容について説明します。

- 「ユーザ ロールと規則の作成」（P.22-5）
- 「ユーザ ロール インターフェイス ポリシーの変更」（P.22-8）

ユーザ ロールと規則の作成

各ユーザ ロールが、最大 256 個の規則を持つことができます。1 つのユーザ ロールを複数のユーザ アカウントに割り当てることができます。

指定した規則番号が、規則の適用される順序を決定します。規則は、降順で適用されます。たとえば、1 つのロールが 3 つの規則を持っている場合、規則 3 が規則 2 よりも前に適用され、規則 2 は規則 1 よりも前に適用されます。

ユーザ ロールを作成して規則を指定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure 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)# role name` *role-name*	ユーザ ロールを指定し、ロール コンフィギュレーション モードを開始します。*role-name* 引数は、最大 16 文字の長さの英数字のストリングで、大文字小文字が区別されます。

	コマンド	目的
ステップ 3	switch(config-role)# **rule** *number* {**deny** | **permit**} **command** *command-string*	コマンド規則を設定します。 *command-string* には、スペースおよび正規表現を含めることができます。たとえば、「interface ethernet *」と指定すると、すべてのイーサネット インターフェイスが含まれます。 必要な規則の数だけこのコマンドを繰り返します。
	switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**}	すべての操作に対して、読み取り専用規則か読み取りと書き込みの規則かを設定します。
	switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature** *feature-name*	機能に対して、読み取り専用規則か読み取りと書き込みの規則かを設定します。 **show role feature** コマンドを使用すれば、規則のリストが表示されます。 必要な規則の数だけこのコマンドを繰り返します。
	switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature-group** *group-name*	機能グループに対して、読み取り専用規則か読み取りと書き込みの規則かを設定します。 **show role feature-group** コマンドを使用すれば、機能グループのリストが表示されます。 必要な規則の数だけこのコマンドを繰り返します。
ステップ 4	switch(config-role)# **description** *text*	（任意）ロールの説明を設定します。説明にはスペースも含めることができます。
ステップ 5	switch(config-role)# **exit**	ロール コンフィギュレーション モードを終了します。
ステップ 6	switch(config)# **show role**	（任意）ユーザ ロールの設定を表示します。
ステップ 7	switch(config)# **copy running-config startup-config**	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、ユーザ ロールを作成して規則を指定する例を示します。

```
switch# config terminal
switch(config-role)# rule 1 deny command clear users
switch(config-role)# rule 2 deny read-write
switch(config-role)# rule 3 permit command config t
switch(config-role)# description This role does not allow users to use clear commands
switch(config-role)# exit
switch(config)# show role

Role: network-admin
  Description: Predefined network admin role has access to all commands
  on the switch
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read-write

Role: network-operator
  Description: Predefined network operator role has access to all read
  commands on the switch
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read

Role: user1
  Description: This role does not allow users to use clear commands
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  3       permit  command                         config t
  2       deny    read-write
  1       deny    command                         clar suers
switch(config)# copy running-config startup-config
[########################################] 100%
switch(config)#
```

機能グループの作成

機能グループを作成する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure 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)# role feature-group name` *group-name*	ユーザ ロール機能グループを指定して、ロール機能グループ コンフィギュレーション モードを開始します。 *group-name* 引数は、最大 32 文字の長さの英数字のストリングで、大文字小文字が区別されます。
ステップ 3	`switch(config-role-featuregrp)# exit`	ロール機能グループ コンフィギュレーション モードを終了します。

	コマンド	目的
ステップ 4	`switch(config)# show role feature-group`	（任意）ロール機能グループの設定を表示します。
ステップ 5	`switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

ユーザ ロール インターフェイス ポリシーの変更

ユーザ ロール インターフェイス ポリシーを変更することで、ユーザがアクセスできるインターフェイスを制限できます。ユーザ ロール インターフェイス ポリシーを変更する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure 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)# role name role-name`	ユーザ ロールを指定し、ロール コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-role)# rule number permit command configure terminal ; interface *`	コマンド規則を設定して、すべてのインターフェイスへのアクセスを許可します。
ステップ 4	`switch(config-role)# interface policy deny`	ロール インターフェイス ポリシー コンフィギュレーション モードを開始します。
ステップ 5	`switch(config-role-interface)# permit interface interface-list`	ロールがアクセスできるインターフェイスのリストを指定します。 必要なインターフェイスの数だけこのコマンドを繰り返します。 このコマンドでは、イーサネット インターフェイスを指定できます。
ステップ 6	`switch(config-role-interface)# exit`	ロール インターフェイス ポリシー コンフィギュレーション モードを終了します。
ステップ 7	`switch(config-role)# show role`	（任意）ロールの設定を表示します。
ステップ 8	`switch(config-role)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

ロールがアクセスできるインターフェイスのリストを指定できます。これを必要なインターフェイスの数だけ指定できます。

```
switch(config-role-interface)# permit interface ethernet 1/1
```

ユーザ ロール VLAN ポリシーの変更

ユーザ ロール VLAN ポリシーを変更することで、ユーザがアクセスできる VLAN を制限できます。ユーザ ロール VLAN ポリシーを変更する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure 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)# role name` *role-name*	ユーザ ロールを指定し、ロール コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-role)# rule` *number* `permit command configure terminal ; vlan *`	コマンド規則を設定して、すべての VLAN へのアクセスを許可します。
ステップ 4	`switch(config-role)# vlan policy deny`	ロール VLAN ポリシー コンフィギュレーション モードを開始します。
ステップ 5	`switch(config-role-vlan)# permit vlan` *vlan-list*	ロールがアクセスできる VLAN の範囲を指定します。 必要な VLAN の数だけこのコマンドを繰り返します。
ステップ 6	`switch(config-role-vlan)# exit`	ロール VLAN ポリシー コンフィギュレーション モードを終了します。
ステップ 7	`switch(config-role)# show role`	（任意）ロールの設定を表示します。
ステップ 8	`switch(config-role)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

ユーザ アカウントと RBAC の設定の確認

ユーザ アカウントと RBAC の設定の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 role	ユーザ ロールの設定を表示します。
switch# show role feature	機能リストを表示します。
switch# show role feature-group	機能グループの設定を表示します。
switch# show startup-config security	スタートアップ コンフィギュレーションのユーザ アカウント設定を表示します。
switch# show running-config security [**all**]	実行コンフィギュレーションのユーザ アカウント設定を表示します。**all** キーワードを指定すると、ユーザ アカウントのデフォルト値が表示されます。
switch# show user-account	ユーザ アカウント情報を表示します。

ユーザ アカウントと RBAC 設定の例

次に、ユーザ ロールを設定する例を示します。

```
switch(config)# role name UserA
switch(config-role)# rule 3 permit command configure terminal ; vlan *
```

```
switch(config-role)# rule 2 permit read feature tacacs
switch(config-role)# rule 1 deny command clear *
switch(config-role)# exit
```

次に、ユーザ ロール機能グループを設定する例を示します。

```
switch(config)# role feature-group name Security-features
switch(config-role-featuregrp)# feature radius
switch(config-role-featuregrp)# feature tacacs
switch(config-role-featuregrp)# feature aaa
```

デフォルト設定

表 22-1 に、ユーザ アカウントと RBAC パラメータのデフォルト設定を示します。

表 22-1　デフォルトのユーザ アカウントと RBAC パラメータ

パラメータ	デフォルト
ユーザ アカウント パスワード	未定義
ユーザ アカウント失効日	なし
インターフェイス ポリシー	すべてのインターフェイスがアクセス可能
VLAN ポリシー	すべての VLAN がアクセス可能