CHAPTER 2

ユーザ アカウントの管理

この章では、ユーザ アカウントを設定する方法を説明します。内容は次のとおりです。

ユーザ アカウントについて

Cisco Nexus 1000V にアクセスするには、ユーザ アカウントをセットアップする必要があります。このユーザ アカウントによって、各ユーザに許可される具体的なアクションが定義されます。ユーザ アカウントは最大 256 個作成できます。各ユーザ アカウントには、次の情報が含まれています。

ロール

ロールとは、同じグループのユーザによって共有可能なアクションを具体的に定義する規則の集合です。たとえば、次のような幅広い権限を持つロールをユーザ アカウントに割り当てることができます。これらのロールは Cisco Nexus 1000V 内であらかじめ定義されたものであり、変更はできません。

```
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
```

管理者は、ユーザのアクセス権を定義するロールをこの他に 64 個作成できます。

各ユーザ アカウントには少なくとも 1 つのロールを割り当てる必要があり、最大 64 個を割り当てることができます。

管理者が作成できるロールでは、アクセスを許可できるコマンドがデフォルトでは次のものに限られています。機能の設定をユーザに許可するには、規則を追加する必要があります。

- **show**
- **exit**
- **end**
- **configure terminal**

表 2-1 に、ロールを構成するコンポーネントの説明を示します。

表 2-1　ロールのコンポーネント

コンポーネント	説明

ルール	定義済みロール基準の 1 つ（たとえば、許可または拒否するコマンド）。各ロールには最大 256 個の規則を追加できます。
	事前定義されているロールの規則は次のとおりです。
	• **role: network-admin**
	`---------- Rule Perm Type Scope Entity ---------- 1 permit read-write`
	• **role: network-operator**
	`---------- Rule Perm Type Scope Entity ---------- 1 permit read-only`

機能	個々の機能（syslog や TACACS+ など）。この機能に対するアクセス権を規則の中で定義することができます。使用可能な機能の一覧を表示するには、**show role feature** コマンドを使用します。
機能グループ	機能をグループ化したもの。このグループに対するアクセス権を規則の中で定義することができます。このグループは、最大 64 個作成できます。使用可能な機能グループの一覧を表示するには、**show role feature-group** コマンドを使用します。
コマンド	単一のコマンド、または 1 つの正規表現で表現されるコマンドの集合。このコマンドに対するアクセス権を規則の中で定義することができます。 コマンドへのアクセスを許可するロールは、そのコマンドへのアクセスを拒否するロールよりも優先されます。たとえば、あるユーザに割り当てられているロールの 1 つでは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ているけれども、このユーザに割り当てられた別のロールでそのコマンドへのアクセスが許可されている場合は、アクセスは許可されます。

ユーザ名

ユーザ名とは、個々のユーザを特定するための一意の文字列です（たとえば「daveGreen」）。ユーザ名は、最大 28 文字で、英数字を使用でき、大文字と小文字が区別されます。数字だけで構成されたユーザ名は許可されません。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。

パスワード

パスワードは、大文字と小文字が区別される文字列です。パスワードによって特定のユーザによるアクセスが可能になり、不正なアクセスの防止に役立ちます。パスワードを指定せずにユーザを追加することもできますが、そのユーザはデバイスにアクセスできなくなる可能性があります。パスワードは、強力なものでなければなりません。容易に推測できるパスワードは、不正アクセスの原因となります。

次の文字は、クリア テキスト パスワードには使用できません。

- ドル記号（$）
- スペース

次の特殊文字は、パスワードの先頭には使用できません。

- 引用符（" および '）
- 縦線（|）
- 右山カッコ（>）

表 2-2 に、強力なパスワードの特性を示します。

表 2-2　強力なパスワードの特性

強力なパスワードに含まれるもの	強力なパスワードに含まれないもの
• 最低 8 文字 • 大文字の英字 • 小文字の英字 • 数字 • 特殊文字	• 連続する文字（例：abcd） • 文字の繰り返し（例：aaabbb） • 辞書に載っている単語 • 固有名詞

強固なパスワードの例を次に示します。

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

パスワード強度のチェック

デバイスによるパスワード強度のチェックは、デフォルトでは自動的に行われます。管理者がユーザ名とパスワードを追加するときに、パスワードの強度が評価されます。パスワードの強度が低い場合は、次に示すエラー メッセージが表示されます。

```
n1000v# config t
n1000v(config)# username daveGreen password davey
password is weak
```

```
Password should contain characters from at least three of the classes:
 lower case letters,upper case letters, digits, and special characters
```

パスワード強度チェックはディセーブルにすることができます。

有効期限

デフォルトでは、ユーザ アカウントは無期限に有効です。ただし、管理者はアカウントがディセーブルになる有効期限を明示的に設定することができます。

注意事項および制約事項

ユーザ アクセスに関する注意事項と制約事項は次のとおりです。

- あらかじめ定義された 2 つのユーザ ロールに加えて、最大 64 個のロールを作成できます。
- 1 つのユーザ ロールに最大 256 個の規則を作成できます。
- 最大 64 個の機能グループを作成できます。
- 最大 256 人のユーザを追加できます。
- 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。
- ローカル ユーザ アカウントと同じ名前のリモート ユーザ アカウントが AAA サーバ上に存在する場合は、そのリモート ユーザには AAA サーバ上で設定されているユーザ ロールでなく、ローカル ユーザ アカウントのユーザ ロールが適用されます。

デフォルト設定

表 2-3 に、ユーザ アクセスのデフォルト設定を示します。

表 2-3　ユーザ アクセスのデフォルト

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 アカウントの有効期限	なし
ユーザ アカウント ロール	network-operator
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

ユーザ アクセスの設定

ここでは、次の内容について説明します。

- 「機能グループの作成」（P.2-11）
- 「インターフェイス アクセスの設定」（P.2-12）
- 「VLAN アクセスの設定」（P.2-14）

パスワード強度チェックのイネーブル化

ここでは、強度の低いパスワードの作成を防ぐための Cisco Nexus 1000V によるパスワード強度チェックをイネーブルにする手順を説明します。

はじめる前に

この手順を開始する前に、次のことを確認または実行しておく必要があります。

- EXEC モードで CLI にログインしていること。
- パスワード強度のチェックは、デフォルトではイネーブルになっています。ディセーブルにされていても、ここで説明する手順を実行すれば再度イネーブルにすることができます。

手順の概要

1. **config t**
2. **password strength-check**
3. **show password strength-check**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**password strength-check** 例： `n1000v(config)# password strength-check`	パスワードの強度確認をイネーブルにします。デフォルトはイネーブルです。 パスワード強度のチェックをディセーブルにするには、このコマンドの **no** 形式を使用します。

ステップ 3	**show password strength-check**
	
	例：
	`n1000v# show password strength-check`
	`Password strength check enabled`
	`n1000v(config)#`
		（任意）パスワード強度チェックの設定を表示します。

ステップ 4	**copy running-config startup-config** 例： `n1000v# copy running-config startup-config`	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

パスワード強度チェックのディセーブル化

ここでは、パスワード強度のチェックをディセーブルにする手順を説明します。

はじめる前に

この手順を開始する前に、次のことを確認または実行しておく必要があります。

- EXEC モードで CLI にログインしていること。
- パスワード強度のチェックは、デフォルトではイネーブルになっています。この手順を使用すると、ディセーブルにすることができます。

手順の概要

1. **config t**
2. **no password strength-check**
3. **show password strength-check**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**no password strength-check**
	
	例：
	`n1000v(config)# no password strength-check`
	`n1000v(config)#`
		パスワード強度のチェックをディセーブルにします。
		デフォルトはイネーブルです。

ステップ 3	**show password strength-check**
	
	例：
	`n1000v# show password strength-check`
	`Password strength check not enabled`
	`n1000v(config)#`
		（任意）パスワード強度チェックの設定を表示します。

ステップ 4	**copy running-config startup-config** 例： `n1000v# copy running-config startup-config`	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

ユーザ アカウントの作成

ここでは、ユーザ アカウントを作成して設定する手順を説明します。このアカウントによって、Cisco Nexus 1000V に対するアクセス権が定義されます。

はじめる前に

この手順を開始する前に、次のことを確認または実行しておく必要があります。

- EXEC モードで CLI にログインしていること。
- ユーザ アカウントは最大 256 個追加できます。
- ユーザ アカウントに対する変更が有効になるのは、そのユーザがログインして新しいセッションを作成したときです。
- 次に示す語をユーザ アカウントで使用しないでください。これらは、他の目的のために予約されています。

adm	gdm	mtsuser	rpcuser
bin	gopher	news	shutdown
daemon	haltlp	nobody	sync
ftp	mail	nscd	sys
ftpuser	mailnull	operator	uucp
games	man	rpc	xfs

- 追加するユーザ パスワードは、クリア テキストと暗号化テキストのどちらでも指定できます。
  - クリア テキストのパスワードは、実行コンフィギュレーションに保存される前に暗号化されます。
  - 暗号化されたパスワードは、それ以上の暗号化を行わずに実行コンフィギュレーションに保存されます。
- 1 つのユーザ アカウントが最大 64 個のロールを持つことができますが、少なくとも 1 つのロールを持つ必要があります。ロールの詳細については、「ロール」（P.2-1）を参照してください。
- 管理者がパスワードを指定しない場合は、そのユーザがログインできなくなる可能性があります。
- パスワードでなく SSH 公開キーを使用する手順については、「公開キーを持つユーザ アカウントの設定」（P.7-5）を参照してください。

手順の概要

1. **config t**
2. **show role**
3. **username** *user-name* **[password [0 | 5]***password***] [expire** *date***] [role** *role-name***]**
4. **show user-account** *user-name*
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **例：** n1000v# config t n1000v(config)#	CLI グローバル コンフィギュレーション モードを開始します。
ステップ 2	**show role** **例：** n1000v(config)# show role	（任意）ユーザに割り当てることのできるロールを表示します。 新しいユーザ ロールを作成する場合は、「ロールの作成」（P.2-9）の手順を使用してください。
ステップ 3	**username** *name* [**password** [**0** | **5**] *password*] [expire date] [role *role-name*] **例：** n1000v(config)# username NewUser password 4Ty18Rnt	ユーザ アカウントを作成します。 • **name**：最大 28 文字の英数字ストリングです。大文字と小文字が区別されます。 • **password**：デフォルト パスワードは未定義です。 – **0** =（デフォルト）入力するパスワードがクリア テキストであることを指定します。Cisco Nexus 1000V は、クリア テキストのパスワードを実行コンフィギュレーションに保存する前に暗号化します。 例では、実行コンフィギュレーションのパスワード **4Ty18Rnt** は password 5 形式で暗号化されています。 – **5** = 入力するパスワードがすでに暗号化形式であることを指定します。Cisco Nexus 1000V は、パスワードを実行コンフィギュレーションに保存する前に暗号化しません。 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。 • **expire date**：YYYY-MM-DD。デフォルトは無期限です。 • **role**：少なくとも 1 つのロールを割り当てる必要があります。最大 64 個のロールを割り当てることができます。デフォルトのロールは、**network-operator** です。

	コマンド	目的

ステップ 4	**show user-account** *username*
	
	例：
	`n1000v(config)# show user-account NewUser`
	`user:NewUser`
	`  this user account has no expiry date`
	`  roles:network-operator network-admin`
	`n1000v(config)#`
		新しいユーザ アカウントの設定を表示します。

ステップ 5	**copy running-config startup-config** 例： `n1000v# copy running-config startup-config`	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

ロールの作成

ここでは、許可または拒否する具体的なアクションのセットを定義するロールを作成します。このロールは、定義されているアクションに一致するアクセス権を必要とするユーザに割り当てます。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 最大 64 個のユーザ ロールを設定できます。
- 1 つのロールに最大 256 個の規則を設定できます。
- 1 つのロールを複数のユーザに割り当てることができます。
- 規則番号は、その規則が適用される順序を表します。規則は番号の降順で適用されます。たとえば、あるロールに 3 つの規則がある場合は、最初に規則 3 が適用され、次に規則 2、最後に規則 1 が適用されます。
- デフォルトでは、管理者が作成するユーザ ロールでアクセスを許可できるコマンドは、**show**、**exit**、**end**、および **configure terminal** コマンドだけです。機能の設定をユーザに許可するには、規則を追加する必要があります。

手順の概要

1. **config t**
2. **role name** *role-name*
3. （任意）**description** *string*
4. **rule** *number* {**deny** | **permit**} **command** *command-string*

   rule *number* {**deny** | **permit**} {**read** | **read-write**}

   rule *number* {**deny** | **permit**} {**read** | **read-write**} **feature** *feature-name*

   rule *number* {**deny** | **permit**} {**read** | **read-write**} **feature-group** *group-name*
5. 手順 4. を繰り返して、このロールに必要なルールをすべて作成します。
6. **show role**
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**role name** *role-name*
	
	例：
	`n1000v(config)# role name UserA`
	`n1000v(config-role)#`
		ユーザ ロールの名前を指定して、そのロールのロール コンフィギュレーション モードを開始します。
		
		名前は最大 16 文字の英数字ストリングです。大文字と小文字が区別されます。

ステップ 3	**description** *description-string* **例：** `n1000v(config-role)# description Prohibits use of clear commands`	（任意）ロールの説明を設定します。説明にはスペースを含めることができます。
ステップ 4	**rule** *number* {**deny** | **permit**} **command** *command-string* **例：** `n1000v(config-role)# rule 1 deny command clear users`	特定のコマンドを許可または拒否する規則を作成します。 指定するコマンドには、スペースや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 インターフェイスへのアクセスが許可または拒否されます。 この例の規則では、**clear users** コマンドへのアクセスが拒否されます。
	rule *number* {**deny** | **permit**} {**read** | **read-write**} **例：** `n1000v(config-role)# rule 2 deny read-write`	あらゆる操作を許可または拒否するための包括的規則を作成します。 この例の規則では、どの操作に対しても読み取りアクセスだけが許可されます。
	rule *number* {**deny** | **permit**} {**read** | **read-write**} **feature** *feature-name* **例：** `n1000v(config-role)# rule 3 permit read feature eth-port-sec`	機能アクセスの規則を作成します。 **show role feature** コマンドを実行すると、使用可能な機能の一覧が表示されます。 この例の規則では、イーサネット ポート セキュリティ機能に対する読み取り専用アクセスがユーザに許可されます。
	rule *number* {**deny** | **permit**} {**read** | **read-write**} **feature-group** *group-name* **例：** `n1000v(config-role)# rule 4 deny read-write feature-group eth-port-sec`	機能グループ アクセスの規則を作成します。 **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。 この例の規則では、特定の機能グループへのアクセスが拒否されます。
ステップ 5	ステップ 4 を繰り返して、指定したロールに必要な規則をすべて作成します。	

	コマンド	目的
ステップ 6	**show role** 例： n1000v(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	**copy running-config startup-config** 例： n1000v(config)# copy running-config startup-config	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

機能グループの作成

ここでは、機能グループを作成して設定する手順を説明します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 最大 64 個のカスタム機能グループを作成できます。

手順の概要

1. **config t**
2. **role feature-group name** *group-name*
3. show role feature
4. **feature** *feature-name*
5. 機能グループに追加するすべての機能について、4. を繰り返します。
6. **show role feature-group**
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** 例： n1000v# config t n1000v(config)#	CLI グローバル コンフィギュレーション モードを開始します。
ステップ 2	**role feature-group name** *group-name* 例： n1000v(config)# role feature-group name GroupA n1000v(config-role-featuregrp)#	グループ名を指定して、そのグループの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**：最大 32 文字の英数字ストリングです。大文字と小文字が区別されます。

	コマンド	目的
ステップ 3	**show role feature** 例： n1000v(config-role-featuregrp)# **show role feature** feature: aaa feature: access-list feature: cdp feature: install . . . n1000v(config-role-featuregrp)#	機能グループを定義するときに使用できる機能の一覧を表示します。
ステップ 4	**feature** *feature-name* 例： n1000v(config-role-featuregrp)# feature syslog n1000v(config-role-featuregrp)#	機能を機能グループに追加します。
ステップ 5	機能グループに追加するすべての機能について、ステップ 6 を繰り返します。	
ステップ 6	**show role feature-group** 例： n1000v(config-role-featuregrp)# show role feature-group feature group: GroupA feature: syslog feature: snmp feature: ping n1000v(config-role-featuregrp)#	（任意）機能グループの設定を表示します。
ステップ 7	**copy running-config startup-config** 例： n1000v(config-role-featuregrp)# copy running-config startup-config	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

インターフェイス アクセスの設定

ここでは、特定のロールのインターフェイス アクセスを設定する手順を説明します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 「ロールの作成」（P.2-9）の手順 を使用してユーザ ロールが 1 つ以上作成済みであるものとします。この手順では、作成済みのロールに変更を加えます。
- デフォルトでは、ロールによってすべてのインターフェイスへのアクセスが許可されます。この手順では、すべてのインターフェイスへのアクセスを拒否してから、特定のインターフェイスへのアクセスを許可します。

手順の概要

1. **config t**
2. **role name** *role-name*

3. **interface policy deny**
4. **permit interface** *interface-list*
5. **show role**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**role name** *role-name*
	
	例：
	`n1000v(config)# role name network-observer`
	`n1000v(config-role)#`
		ユーザ ロールを指定して、そのロールのロール 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	**interface policy deny**
	
	例：
	`n1000v(config-role)# interface policy deny`
	`n1000v(config-role-interface)#`
		インターフェイス コンフィギュレーション モードを開始し、このロールによるすべてのインターフェイス アクセスを拒否します。
		これで、**permit interface** コマンドを使用して明示的に定義しない限り、このロールはインターフェイスに一切アクセスできなくなりました。

ステップ 4	**permit interface** *interface-list* 例： `n1000v(config-role-interface)# permit interface ethernet 2/1-4`	このロールに割り当てられたユーザにアクセスを許可するインターフェイスを指定します。 このロールに割り当てられたユーザにアクセスを許可するインターフェイスがすべて指定されるまで、このコマンドを繰り返します。

ステップ 5	**show role** *role-name*
	
	例：
	`n1000v(config-role-interface)# show role name network-observer`
	
	`role: network-observer`
	`  description: temp`
	`  Vlan policy: permit (default)`
	`  Interface policy: deny`
	`  Permitted interfaces: Ethernet2/1-4`
		（任意）ロールの設定を表示します。

ステップ 6	**copy running-config startup-config** 例： `n1000v(config-role-featuregrp)# copy running-config startup-config`	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

VLAN アクセスの設定

ここでは、特定のロールの VLAN アクセスを定義する手順を説明します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 「ロールの作成」（P.2-9）の手順 を使用してユーザ ロールが 1 つ以上作成済みであるものとします。この手順では、作成済みのロールに変更を加えます。
- デフォルトでは、すべての VLAN へのアクセスが許可されます。この手順では、すべての VLAN へのアクセスを拒否してから、特定の VLAN へのアクセスを許可します。

手順の概要

1. **config t**
2. **role name** *role-name*
3. **vlan policy deny**
4. **permit vlan** *vlan-range*
5. **exit**
6. **show role**
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**role name** *role-name*
	
	例：
	`n1000v(config)# role name network-observer`
	`n1000v(config-role)#`
		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	**vlan policy deny**
	
	例：
	`n1000v(config-role)# vlan policy deny`
	`n1000v(config-role-vlan)#`
		VLAN コンフィギュレーション モードを開始し、このロールによるすべての VLAN アクセスを拒否します。
		
		これで、**permit vlan** コマンドを使用して明示的に定義しない限り、このロールは VLAN に一切アクセスできなくなりました。

ステップ 4	**permit vlan** *vlan-list* **例：** `n1000v(config-role-vlan)# permit vlan 1-4`	このロールに割り当てられたユーザにアクセスを許可する VLAN を指定します。 このロールに割り当てられたユーザにアクセスを許可する VLAN がすべて指定されるまで、このコマンドを繰り返します。

	コマンド	目的

ステップ 5	**show role** *role-name*
	
	例：
	`n1000v(config-role)# show role network-observer`
	
	`role: network-observer`
	`  description: temp`
	`  Vlan policy: deny`
	`  Permitted vlans: vlan 1-4`
	`  Interface policy: deny`
	`  Permitted interfaces: Ethernet2/1-4`
		（任意）ロールの設定を表示します。

ステップ 6	**copy running-config startup-config** 例： `n1000v(config-role)# copy running-config startup-config`	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

ユーザ アクセス設定の確認

ユーザ アカウントおよび RBAC 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
show role	使用可能なユーザ ロールとその規則を表示します。
show role feature	使用可能な機能のリストを表示します。
show role feature-group	使用可能な機能グループのリストを表示します。
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。
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。
show user-account	ユーザ アカウント情報を表示します。

構成例

次に、ロールを設定する例を示します。

```
role name UserA
  rule 3 permit read feature snmp
  rule 2 permit read feature dot1x
  rule 1 deny command clear *
```

次に、機能グループを設定する例を示します。

```
role feature-group name Security-features
  feature radius
  feature tacacs
  feature dot1x
  feature aaa
  feature snmp
  feature acl
  feature access-list
```

その他の関連資料

RBAC の実装に関連する詳細情報については、次を参照してください。

- 「関連資料」（P.2-16）
- 「標準」（P.2-16）
- 「管理情報ベース（MIB）」（P.2-16）

関連資料

関連項目	参照先
ユーザ アクセスのコマンド	『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*』
スイッチ上のユーザの管理	『*Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

管理情報ベース（MIB）

MIB	MIB のリンク
• CISCO-COMMON-MGMT-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

ユーザ アカウント機能の履歴

ここでは、ユーザ アカウントのリリース履歴を示します。

機能名	リリース	機能情報
ユーザ アカウント	4.0(4)SV1(1)	この機能が導入されました。