ユーザ アカウントの管理

この章の内容は、次のとおりです。

- ユーザ アカウントについて，1 ページ
- ユーザ アカウント作成の注意事項と制限事項，4 ページ
- ユーザ アカウント作成の注意事項，4 ページ
- ユーザ アクセスのデフォルト設定，5 ページ
- ユーザ アクセスの設定，5 ページ
- ユーザ アクセス設定の確認，14 ページ
- 設定例，15 ページ
- MIB，15 ページ
- ユーザ アカウント機能の履歴，15 ページ

ユーザ アカウントについて

Cisco Nexus 1000V へのアクセスは、各ユーザに許可される特定のアクションを定義するユーザ アカウントを設定することで実現されます。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
- ユーザ名
- パスワード
- 有効期限

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 内で事前に定義されたものであり、変更できません。

```
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**

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。 すべてが数字のユーザ名が AAA サーバに存在し、ログインの際に入力されても、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（>）

次の表に、強力なパスワードの特性を示します。

表 *1*：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	連続する文字（例：abcd）
大文字の英字	文字の繰り返し（例：aaabbb）
小文字の英字	辞書に載っている単語
数字	固有名詞
特殊文字	

次に、強力なパスワードの例を示します。

- 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。 これが脆弱なパスワードの場合、次のエラー メッセージが表示されて、通知されます。

```
switch# config terminal
switch (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。

ユーザ アカウント作成の注意事項と制限事項

- 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。

ユーザ アカウント作成の注意事項

- 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	mtuser	rpcuser
bin	gopher	neews	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。
- パスワードを指定しない場合、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、OpenSSH キーの設定を参照してください。

ユーザ アクセスのデフォルト設定

パラメータ	デフォルト
ユーザ アカウント 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にアクセス可能
VLAN ポリシー	すべての VLAN にアクセス可能

ユーザ アクセスの設定

パスワード強度チェックのイネーブル化

Cisco Nexus 1000V でパスワード強度のチェックをイネーブルにして、ユーザ アカウントに対して弱いパスワードを設定できないようにするには、この手順を使用します。

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。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **password strength-check**	パスワードの強度確認をイネーブルにします。デフォルトではイネーブルになっています。 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	switch(config)# **show password strength-check**	（任意） パスワードの強度の確認の設定を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に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て、変更を継続的に保存します。

```
switch# configure terminal
switch(config)# password strength-check
switch(config)# show password strength-check
Password strength check enabled
switch(config)# copy running-config startup-config
```

パスワード強度チェックのディセーブル化

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **no password strength-check**	パスワード強度のチェックをディセーブルにします。 デフォルトではイネーブルになっています。
ステップ 3	switch(config)# **show password strength-check**	（任意） パスワードの強度の確認の設定を表示します。

	コマンドまたはアクション	目的
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に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て、変更を継続的に保存します。

```
switch# configure terminal
switch(config)# no password strength-check
switch(config)# show password strength-check
switch(config)# copy running-config startup-config
```

ユーザ アカウントの作成

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(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。
ステップ 3	switch(config)# **username** *name* [**password** [**0** | **5**] *password*] [**expire date**] [**role** *role-name*]	ユーザ アカウントを作成します。 引数およびキーワードは次のとおりです。 • 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：デフォルトのパスワードは定義されていません。 ◦ 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、実行コンフィギュレーションに保存する前にクリア テキストのパスワードを暗号化します。

	コマンドまたはアクション	目的
		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 = 入力した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、実行コンフィギュレーションに保存する前にパスワードを暗号化しません。 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。
ステップ 4	switch(config)# **show user-account** *username*	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	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に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て、変更を継続的に保存します。

```
switch# configure terminal
switch(config)# show role
switch(config)# username NewUser password 4Ty18Rnt
switch(config)# show user-account NewUser
user: NewUser
     this user account has no expiry date
     roles:network-operator network-admin
switch# copy running-config startup-config
```

ロールの作成

はじめる前に

- この手順を開始する前に、EXEC モードで CLI にログインする必要があります。
- 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

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **role name** *role-name*	ユーザ ロールに名前をつけて、そのロールのロール コンフィギュレーション モードに切り替えます。 *role-name*は大文字と小文字が区別される 16 文字以下の英数字文字列です。
ステップ 3	switch(config-role)# **description** *description-string*	（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	switch(config-role)# **rule** *number* {**deny**| **permit**} **command** *command-string* • switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**} すべての操作を許可または拒否する 1 個の規則を作成します。 • switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature** *feature-name* 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。 • switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature-group** *group-name* 機能グループ アクセスの規則を作成します。	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 ***は、すべてのイーサネット インターフェイスへのアクセスを許可または拒否します。

	コマンドまたはアクション	目的
	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。 **例**： この例では、**clear users** コマンドへのアクセスを拒否する規則を設定します。	
ステップ 5	指定したロールに必要なすべての規則を作成するには、ステップ 4 を繰り返します。	
ステップ 6	switch(config-role)# **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-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。

```
switch# configure terminal
switch(config)# role name UserA
switch(config-role)# description Prohibits use of clear commands
switch(config-role)# rule 1 deny command clear users
switch(config-role)# rule 2 deny read-write
switch(config-role)# rule 3 permit read feature eth-port-sec
switch(config-role)# rule 4 deny read-write feature-group eth-port-sec

switch# configure terminal
switch(config)# role name UserA
switch(config-role)# rule 3 permit read feature snmp
switch(config-role)# rule 2 permit read feature dot1x
switch(config-role)# rule 1 deny command clear *
```

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。 最大64個のカスタム機能グループを作成できます。

はじめる前に

- この手順を開始する前に、EXEC モードで CLI にログインする必要があります。
- 最大 64 個のカスタム機能グループを作成できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **role feature-group name** *group-name*	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。
ステップ 3	switch(config-role-featuregrp)# **show role feature**	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	switch(config-role-featuregrp)# **feature** *feature-name*	機能を機能グループに追加します。 機能グループに追加するすべての機能に対してこの手順を繰り返します。
ステップ 5	switch(config-role-featuregrp)# **show role feature-group**	（任意） 機能グループの設定を表示します。
ステップ 6	switch(config-role-featuregrp)# **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。

```
switch# configure terminal
switch(config)# role feature-group name GroupA
switch(config-role-featuregrp)# show role feature
feature: aaa
feature: access-list
feature: cdp
feature: install
. . .
switch(config-role-featuregrp)# feature syslog
switch(config-role-featuregrp)# show role feature-group
feature group: GroupA
feature: syslog
feature: snmp
feature: ping
switch(config-role-featuregrp)# copy running-config startup-config
```

```
switch# configure terminal
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 dot1x
 switch(config-role-featuregrp)# feature aaa
 switch(config-role-featuregrp)# feature snmp
 switch(config-role-featuregrp)# feature acl
 switch(config-role-featuregrp)# feature access-list
```

インターフェイス アクセスの設定

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。 すべてのインターフェイスへのアクセスを拒否し、選択したインターフェイスへのアクセスを許可して、すでに作成されているロールを変更します。

はじめる前に

この手順を開始する前に、次のことを確認してください。

- CLI に EXEC モードでログインしていること。
- 1 つまたは複数のユーザ ロールを作成していること。 この手順では、作成済みのロールに変更を加えます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config) # **role name** *role-name*	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	switch(config-role)# **interface policy deny**	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	switch(config-role-interface)# **permit interface***interface-list*	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	switch(config-role-interface)# **show role** *role-name*	（任意） ロール設定を表示します。
ステップ 6	switch(config-role-featuregrp)# **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。

```
switch# configure terminal
switch(config)# role name network-observer
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 2/1-4
switch(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
switch(config-role-featuregrp)# copy running-config startup-config
```

VLAN アクセスの設定

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、選択した VLAN へのアクセスを許可して、作成済みのロールを変更します。

はじめる前に

この手順を開始する前に、次のことを実行する必要があります。

- EXEC モードで CLI にログインしてください。
- 1 つまたは複数のユーザ ロールを作成しておいてください。 この手順では、作成済みのロールに変更を加えます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	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)# **vlan policy deny**	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	switch(config-role-vlan)# **permit vlan** *vlan-range*	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。 ダッシュを使用して VLAN の範囲を指定します （1-9 または 20-30 など）。

	コマンドまたはアクション	目的
		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。
ステップ 5	switch(config-role)# **show role** *role-name*	（任意） ロール設定を表示します。 role-name は、作成したロールに割り当てた名前です。
ステップ 6	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。

```
switch# configure terminal
switch(config)# role name network-observer
switch(config-role)# vlan policy deny
switch(config-role-vlan)# permit interface ethernet 2/1-4
switch(config-role)# show role name network-observer
role: network-observer
  description: temp
  Vlan policy: permit (default)
  Interface policy: deny
  Permitted interfaces: Ethernet2/1-4
switch(config-role)# copy running-config startup-config
```

ユーザ アクセス設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

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。

コマンド	目的
show user-account	ユーザ アカウント情報を表示します。

設定例

機能グループ作成の設定例

```
switch# config terminal
switch(config-role)# role feature-group name security-features
switch(config-role)# feature radius
switch(config-role)# feature tacacs
switch(config-role)# feature dot1x
switch(config-role)# feature aaa
switch(config-role)# feature snmp
switch(config-role)# feature acl
switch(config-role)# feature access-list
```

ロール作成の設定例

```
switch# config terminal
switch(config)# role name UserA
switch(config-role)# rule 3 permit read feature snmp
switch(config-role)# rule 2 permit read feature dot1x
switch(config-role)# rule 1 deny command clear *
```

MIB

MIB	MIB 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

この表には、機能への追加または変更が行われたリリースの更新のみが含まれています。

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。