R コマンド

この章では、R で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

radius-server deadtime

Cisco Nexus 5000 シリーズ スイッチにすべての RADIUS サーバのデッド タイム間隔を設定するには、**radius-server deadtime** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server deadtime *minutes*

no radius-server deadtime *minutes*

構文の説明

minutes	デッド タイム間隔の分数。有効な範囲は 1 ～ 1440 分です。

コマンド デフォルト

0 分

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

デッド タイム間隔は、応答のなかった RADIUS サーバをスイッチが確認するまでの分数です。

（注） アイドル タイム インターバルが 0 分の場合、RADIUS サーバの定期的なモニタリングは実行されません。

例

次に、すべての RADIUS サーバの定期的なモニタリングを実行するグローバル デッド タイム間隔を設定する例を示します。

```
switch(config)# radius-server deadtime 5
```

次に、すべての RADIUS サーバのグローバル デッド タイム間隔をデフォルトに戻して、サーバの定期的なモニタリングをディセーブルにする例を示します。

```
switch(config)# no radius-server deadtime 5
```

関連コマンド

コマンド	説明
show radius-server	RADIUS サーバ情報を表示します。

radius-server directed-request

ログイン時にユーザが認証要求を特定の RADIUS サーバに送信できるようにするには、**radius-server directed-request** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server directed-request

no radius-server directed-request

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

設定した RADIUS サーバ グループに認証要求を送信します。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

ログイン時、*username@vrfname:hostname* を指定できます。*vrfname* は使用する VRF、*hostname* は設定した RADIUS サーバ名です。ユーザ名が認証用に RADIUS サーバに送信されます。

例

次に、ログイン時にユーザが認証要求を特定の RADIUS サーバに送信できるようにする例を示します。

```
switch(config)# radius-server directed-request
```

次に、ログイン時にユーザが認証要求を特定の RADIUS サーバに送信できないようにする例を示します。

```
switch(config)# no radius-server directed-request
```

関連コマンド

コマンド	説明
show radius-server directed-request	指定要求 RADIUS サーバ設定を表示します。

radius-server host

RADIUS サーバ パラメータを設定するには、**radius-server host** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server host {*hostname* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret* [**pac**]] [**accounting**]
[**acct-port** *port-number*] [**auth-port** *port-number*] [**authentication**] [**retransmit** *count*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds* [**retransmit** *count*]]

no radius-server host {*hostname* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret* [**pac**]] [**accounting**]
[**acct-port** *port-number*] [**auth-port** *port-number*] [**authentication**] [**retransmit** *count*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds* [**retransmit** *count*]]

構文の説明

hostname	RADIUS サーバの Domain Name Server（DNS; ドメイン ネーム サーバ）名。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 256 です。
ipv4-address	*A*.*B*.*C*.*D* 形式の RADIUS サーバの IPv4 アドレス。
ipv6-address	*X*:*X*:*X*:*X* フォーマットの RADIUS サーバの IPv6 アドレス。
key	（任意）RADIUS サーバ事前共有秘密キーを設定します。
0	（任意）RADIUS クライアントとサーバ間の通信を認証する、クリア テキストで指定された事前共有キーを設定します。これはデフォルトです。
7	（任意）RADIUS クライアントとサーバ間の通信を認証する、暗号文で指定された事前共有キー（7 で表示）を設定します。
shared-secret	RADIUS クライアントとサーバ間の通信を認証する事前共有キー。事前共有キーには、出力可能な ASCII 文字の使用が可能です（空白文字は使用できません）。大文字と小文字が区別され、最大文字数は 63 です。
pac	（任意）Cisco TrustSec と連動させるために、RADIUS Cisco ACS サーバで Protected Access Credentials（PAC）の生成をイネーブルにします。
accounting	（任意）アカウンティングを設定します。
acct-port *port-number*	（任意）アカウンティング用の RADIUS サーバのポートを設定します。指定できる範囲は 0 ～ 65535 です。
auth-port *port-number*	（任意）認証用の RADIUS サーバのポートを設定します。指定できる範囲は 0 ～ 65535 です。
authentication	（任意）認証を設定します。
retransmit *count*	（任意）スイッチがローカル認証に戻る前に RADIUS サーバへの接続試行を行う回数を設定します。有効な範囲は 1 ～ 5 回で、デフォルトは 1 回です。
test	（任意）テスト パケットを RADIUS サーバに送信するようにパラメータを設定します。
idle-time *time*	サーバをモニタリングするための時間間隔を分で指定します。有効な範囲は 1 ～ 1440 分です。
password *password*	テスト パケット内のユーザ パスワードを指定します。パスワードは、英数字で指定します。大文字と小文字が区別され、最大文字数は 32 です。

username *name*	テスト パケット内のユーザ名を指定します。ユーザ名は、英数字で指定します。大文字と小文字の区別がなく、最大文字数は 32 です。
timeout *seconds*	RADIUS サーバへの再送信タイムアウト（秒単位）を指定します。デフォルトは 1 秒です。有効な範囲は 1 ～ 60 秒です。

コマンド デフォルト

アカウンティング ポート：1813
認証ポート：1812
アカウンティング：イネーブル
認証：イネーブル
再送信数：1
アイドル時間：0
サーバ モニタリング：ディセーブル
タイムアウト：5 秒
テスト ユーザ名：test
テスト パスワード：test

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

アイドル タイム インターバルが 0 分の場合、RADIUS サーバの定期的なモニタリングは実行されません。

例

次に、RADIUS サーバの認証とアカウンティングのパラメータを設定する例を示します。

```
switch(config)# radius-server host 192.168.2.3 key HostKey
switch(config)# radius-server host 192.168.2.3 auth-port 2003
switch(config)# radius-server host 192.168.2.3 acct-port 2004
switch(config)# radius-server host 192.168.2.3 accounting
switch(config)# radius-server host radius2 key 0 abcd
switch(config)# radius-server host radius3 key 7 1234
switch(config)# radius-server host 192.168.2.3 test idle-time 10
switch(config)# radius-server host 192.168.2.3 test username tester
switch(config)# radius-server host 192.168.2.3 test password 2B9ka5
```

関連コマンド

コマンド	説明
show radius-server	RADIUS サーバ情報を表示します。

radius-server key

RADIUS 共有秘密キーを設定するには、**radius-server key** コマンドを使用します。設定した共有秘密キーを削除するには、このコマンドの **no** 形式を使用します。

radius-server key [**0** | **7**] *shared-secret*

no radius-server key [**0** | **7**] *shared-secret*

構文の説明

0	（任意）RADIUS クライアントとサーバ間の通信を認証する、クリア テキストで指定された事前共有キーを設定します。
7	（任意）RADIUS クライアントとサーバ間の通信を認証する、暗号文で指定された事前共有キーを設定します。
shared-secret	RADIUS クライアントとサーバ間の通信を認証するために使用される事前共有キー。事前共有キーには、出力可能な ASCII 文字の使用が可能です（空白文字は使用できません）。大文字と小文字が区別され、最大文字数は 63 です。

コマンド デフォルト

クリア テキスト認証

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

RADIUS 事前共有キーを設定して、RADIUS サーバに対してスイッチを認証する必要があります。キーの長さは 65 文字で、出力可能な任意の ASCII 文字を含めることができます（スペースは使用できません）。グローバル キーは、スイッチにあるすべての RADIUS サーバ コンフィギュレーションで使用するよう設定できます。**radius-server host** コマンドで **key** キーワードを使用することでこのグローバル キーの割り当てを上書きできます。

例

次に、RADIUS 認証を設定する各種のシナリオを提供する例を示します。

```
switch(config)# radius-server key AnyWord
switch(config)# radius-server key 0 AnyWord
switch(config)# radius-server key 7 public pac
```

関連コマンド

コマンド	説明
show radius-server	RADIUS サーバ情報を表示します。

radius-server retransmit

スイッチが RADIUS サーバで要求を試行する回数を指定するには、**radius-server retransmit** コマンドを使用する必要があります。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server retransmit *count*

no radius-server retransmit *count*

構文の説明

count	スイッチがローカル認証に戻る前に RADIUS サーバへの接続試行を行う回数。有効な範囲は 1 ～ 5 回です。

コマンド デフォルト

再送信 1 回

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、RADIUS サーバに再送信回数を設定する例を示します。

```
switch(config)# radius-server retransmit 3
```

次に、RADIUS サーバに再送信のデフォルト数を設定する例を示します。

```
switch(config)# no radius-server retransmit 3
```

関連コマンド

コマンド	説明
show radius-server	RADIUS サーバ情報を表示します。

radius-server timeout

RADIUS サーバへの再送信間隔を指定するには、**radius-server timeout** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server timeout *seconds*

no radius-server timeout *seconds*

構文の説明

seconds	RADIUS サーバへの再送信間隔の秒数。有効な範囲は 1 ～ 60 秒です。

コマンド デフォルト

1 秒

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、タイムアウト間隔を設定する例を示します。

```
switch(config)# radius-server timeout 30
```

次に、デフォルトの間隔に戻す例を示します。

```
switch(config)# no radius-server timeout 30
```

関連コマンド

コマンド	説明
show radius-server	RADIUS サーバ情報を表示します。

remark

IPv4 または MAC アクセス コントロール リスト（ACL）にコメントを入力するには、**remark** コマンドを使用します。**remark** コマンドを削除するには、このコマンドの no 形式を使用します。

[*sequence-number*] **remark** *remark*

no {*sequence-number* | **remark** *remark*}

構文の説明

sequence-number	（任意）**remark** コマンドのシーケンス番号。これにより、スイッチはアクセス リストの番号が指定された位置にコマンドを挿入します。シーケンス番号は、ACL 内でルールの順序を保ちます。 シーケンス番号には、1 ～ 4294967295 の間の整数を指定できます。 デフォルトでは、ACL の最初のルールには、10 のシーケンス番号が与えられます。 シーケンス番号を指定しない場合、スイッチは ACL の最後にルールを追加し、前のルールのシーケンス番号より 10 大きいシーケンス番号を割り当てます。 **resequence** コマンドを使用して、シーケンス番号をリマークとルールに再度割り当てます。
remark	リマークのテキスト。引数に使用できる文字数は最大 100 文字です。

コマンド デフォルト

デフォルトでは、ACL にリマークが含まれません。

コマンド モード

IPv4 ACL コンフィギュレーション モード
MAC ACL コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

remark 引数には、最大 100 文字を指定できます。*remark* 引数に 100 を超える文字を入力すると、スイッチは最初の 100 文字を受け入れ、後の文字を廃棄します。

例

次に、IPv4 ACL にリマークを作成して、結果を表示する例を示します。

```
switch(config)# ip access-list acl-ipv4-01
switch(config-acl)# 100 remark this ACL denies the marketing department access to the lab
switch(config-acl)# show access-list acl-ipv4-01
```

関連コマンド

コマンド	説明
ip access-list	IPv4 ACL を設定します。
mac access-list	MAC ACL を設定します。
show access-list	すべての ACL または 1 つの ACL を表示します。

resequence

アクセス コントロール リスト（ACL）のすべてのルールまたは時間の範囲にシーケンス番号を再度割り当てるには、**resequence** コマンドを使用します。

resequence *access-list-type* access-list *access-list-name starting-number increment*

resequence time-range *time-range-name starting-number increment*

構文の説明

access-list-type	ACL のタイプ。この引数の有効値は、次のキーワードです。 • **arp** • **ip** • **mac**
access-list *access-list-name*	ACL の名前を指定します。
time-range *time-range-name*	時間範囲の名前を指定します。
starting-number	ACL の最初のルールまたは時間の範囲のシーケンス番号。
increment	スイッチが後続の各シーケンス番号に追加する数。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

resequence コマンドを使用すると、ACL のルールまたは時間の範囲にシーケンス番号を再度割り当てることができます。最初のルールの新しいシーケンス番号は、*starting-number* 引数によって決まります。その他の各ルールは、*increment* 引数によって決まる新しいシーケンス番号を受け取ります。最大シーケンス番号がシーケンス番号の許容最大値を超えると、シーケンスが実行されず、次のメッセージが表示されます。

```
ERROR: Exceeded maximum sequence number.
```

最大シーケンス番号は、4294967295 です。

例

次に、**show ip access-lists** コマンドを使用して、100 のシーケンス番号で開始し、10 ずつ増える ip-acl-01 という名前の IPv4 ACL のシーケンスを再度実行し、**resequence** コマンドの使用の前後のシーケンス番号を確認する例を示します。

```
switch(config)# show ip access-lists ip-acl-01
```

```
IP access list ip-acl-01
        7 permit tcp 128.0.0.0/16 any eq www
        10 permit udp 128.0.0.0/16 any
        13 permit icmp 128.0.0.0/16 any eq echo
        17 deny igmp any any
switch(config)# resequence ip access-list ip-acl-01 100 10
switch(config)# show ip access-lists ip-acl-01

IP access list ip-acl-01
        100 permit tcp 128.0.0.0/16 any eq www
        110 permit udp 128.0.0.0/16 any
        120 permit icmp 128.0.0.0/16 any eq echo
        130 deny igmp any any
switch(config)#
```

関連コマンド

コマンド	説明
ip access-list	IPv4 ACL を設定します。
mac access-list	MAC ACL を設定します。
show access-lists	すべての ACL または特定の ACL を表示します。

role feature-group name

ユーザ ロール機能グループを作成または指定し、ユーザ ロール機能グループ コンフィギュレーション モードを開始するには、**role feature-group name** コマンドを使用します。ユーザ ロール機能グループを削除するには、このコマンドの **no** 形式を使用します。

role feature-group name *group-name*

no role feature-group name *group-name*

構文の説明

group-name	ユーザ ロール機能グループ名。*group-name* の最大文字数は 32 で、大文字と小文字が区別され、英数字文字列で指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、ユーザ ロール機能グループを作成して、ユーザ ロール機能グループ コンフィギュレーション モードを開始する例を示します。

```
switch(config)# role feature-group name MyGroup
switch(config-role-featuregrp)#
```

次に、ユーザ ロール機能グループを削除する例を示します。

```
switch(config)# no role feature-group name MyGroup
switch(config)#
```

関連コマンド

コマンド	説明
feature-group name	ユーザ ロール機能グループを指定または作成して、ユーザ 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。
show role feature-group	ユーザ ロール機能グループを表示します。

role name

ユーザ ロールを作成または指定し、ユーザ ロール コンフィギュレーション モードを開始するには、**role name** コマンドを使用します。ユーザ ロールを削除するには、このコマンドの **no** 形式を使用します。

role name {*role-name* | **default-role** | *privilege-role*}

no role name {*role-name* | **default-role** | *privilege-role*}

構文の説明

role-name	ユーザ ロール名。*role-name* の最大文字数は 16 で、大文字と小文字が区別され、英数字文字列で指定します。
default-role	デフォルトのユーザ ロール名を指定します。
privilege-role	特権のあるユーザ ロール。次のいずれかの値になります。 • priv-0 • priv-1 • priv-2 • priv-3 • priv-4 • priv-5 • priv-6 • priv-7 • priv-8 • priv-9 • priv-10 • priv-11 • priv-12 • priv-13

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。
5.0(2)N1(1)	権限ロール作成のサポートが追加されました。

使用上のガイドライン

Cisco Nexus 5000 シリーズ スイッチには、次のデフォルトのユーザ ロールがあります。

- ネットワーク管理者：スイッチ全体の読み取りおよび書き込みアクセスを完了します。
- スイッチ全体の読み取りアクセスを完了します。

デフォルトのユーザ ロールは変更または削除できません。

特権レベルのロールを表示するには、**feature privilege** コマンドを使用して TACACS+ サーバでのコマンド認可にロールの累積権限をイネーブルにする必要があります。権限ロールは、レベルが低い方の権限ロールの権限を継承します。

例

次に、ユーザ ロールを作成して、ユーザ ロール コンフィギュレーション モードを開始する例を示します。

```
switch(config)# role name MyRole
switch(config-role)#
```

次に、特権レベル 1 のユーザ ロールを作成して、ユーザ ロール コンフィギュレーション モードを開始する例を示します。

```
switch(config)# role name priv-1
switch(config-role)#
```

次に、ユーザ ロールを削除する例を示します。

```
switch(config)# no role name MyRole
```

関連コマンド

コマンド	説明
feature privilege	TACACS+ サーバでのコマンド認可に対するロールの累積権限をイネーブルにします。
rule	ユーザ ロールのルールを設定します。
show role	ユーザ ロールを表示します。

rollback running-config

実行コンフィギュレーションをロールバックするには、**rollback running-config** コマンドを使用します。

rollback running-config {**checkpoint** *checkpoint-name* | **file** {**bootflash:** | **volatile:**}[*//server*][*directory/*][*filename*] [**atomic**] [**verbose**]}

構文の説明

checkpoint	実行コンフィギュレーションがチェックポイントにロールバックされるよう指定します。
checkpoint-name	チェックポイント名。名前は、最大 32 文字まで指定できます。
file	実行コンフィギュレーションがコンフィギュレーション ファイルにロールバックされるよう指定します。
bootflash:	書き込み可能なブートフラッシュ ローカル ストレージ ファイル システムを指定します。
volatile:	揮発性の書き込み可能なローカル ストレージ ファイル システムを指定します。
//server	サーバの名前。有効な値は、**///**、**//module-1/**、**//sup-1/**、**//sup-active/** または **//sup-local/** です。2 個のスラッシュ（//）を含む必要があります。
directory/	ディレクトリの名前。ディレクトリ名では、大文字と小文字が区別されます。
filename	チェックポイント コンフィギュレーション ファイルの名前。ファイル名では、大文字と小文字が区別されます。
atomic	（任意）パッチの適用中に初めて失敗すると、ロールバック実行を中止するように指定します。これは、デフォルトのモードです。
verbose	（任意）ロールバック実行手順がロールバック操作中に表示されるように指定します。

（注） *filesystem*://*server*/*directory*/*filename* ストリングにはスペースを含めることはできません。この文字列の各要素は、コロン（:）とスラッシュ（/）で区切ります。

コマンド デフォルト

アトミック ロールバック

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

使用上のガイドライン

チェックポイント名またはファイルにロールバックできます。ロールバックする前に、**show diff rollback-patch** コマンドを使用して、現在のコンフィギュレーションまたは保存されているコンフィギュレーションを参照している送信元と宛先のチェックポイント間の差異を表示できます。

指定されたチェックポイントへのロールバックがチェックポイント コンフィギュレーションにシステムのアクティブ コンフィギュレーションを復元します。

ブートフラッシュ時のファイルへのロールバックは、**checkpoint** *checkpoint_name* コマンドを使用して作成されたファイルでのみサポートされます。他の ASCII タイプのファイルではサポートされません。

（注） atomic ロールバック中に設定を変更すると、ロールバックは失敗します。手動でエラーを修正し、**rollback** コマンドを実行する必要があります。

例

次に、verbose モードで chkpnt-1 という名前のチェックポイントに実行コンフィギュレーションをロールバックする例を示します。

```
switch# checkpoint chkpnt-1
<-- modify configuration in running configuration--->
switch# checkpoint chkpnt-2
<-- modify configuration in running configuration--->
switch# rollback running-config chkpnt-1 verbose
Note: Applying config parallelly may fail Rollback verification
Collecting Running-Config
Generating Rollback patch for switch profile
Rollback Patch is Empty
Collecting Running-Config
#Generating Rollback Patch
Rollback Patch is Empty

Rollback completed successfully.

switch#
```

次に、ブートフラッシュ ストレージ システムの chkpnt_configSep9-1.txt というチェックポイント コンフィギュレーション ファイルに実行コンフィギュレーションをロールバックする例を示します。

```
switch# checkpoint chkpnt-1
<-- modify configuration in running configuration--->
switch# checkpoint file bootflash:///chkpnt_configSep9-1.txt
<-- modify configuration in running configuration--->
switch# checkpoint file bootflash:///chkpnt_configSep9-2.txt
<-- modify configuration in running configuration--->
switch# checkpoint chkpnt-2
switch# rollback running-config file bootflash:///chkpnt_configSep9-1.txt
switch#
```

関連コマンド

コマンド	説明
rollback	保存されたすべてのチェックポイントにスイッチをロールバックします。
show checkpoint	チェックポイント情報を表示します。
show diff rollback-patch checkpoint	現在のチェックポイントと保存済みコンフィギュレーションの差異を表示します。

コマンド	説明
show diff rollback-patch file	現在のチェックポイント ファイルと保存済みコンフィギュレーションの差異を表示します。
show diff rollback-patch running-config	現在の実行コンフィギュレーションと保存済みチェックポイント コンフィギュレーションの差異を表示します。

rule

ユーザ ロールのルールを設定するには、**rule** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

rule *number* {**deny** | **permit**} {**command** *command-string* | {**read** | **read-write**} [**feature** *feature-name* | **feature-group** *group-name*]}

no rule *number*

構文の説明

number	ルールのシーケンス番号。スイッチは、最初に最大値を使用してルールを適用し、以降は降順で適用されます。
deny	コマンドまたは機能へのアクセスを拒否します。
permit	コマンドまたは機能へのアクセスを許可します。
command *command-string*	コマンド ストリングを指定します。コマンド文字列は最大 128 文字で、スペースを含めることができます。
read	読み取りアクセスを指定します。
read-write	読み取りおよび書き込みアクセスを指定します。
feature *feature-name*	（任意）機能名を指定します。スイッチの機能名を表示するには、**show role feature** コマンドを使用します。
feature-group *group-name*	（任意）機能グループを指定します。

コマンド デフォルト

なし

コマンド モード

ユーザ ロール コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。
5.0(2)N1(1)	拒否ルールを特権 0（priv-0）ロールに追加できます。

使用上のガイドライン

ロールごとに最大 256 のルールを設定できます。

指定するルール番号は、適用したルールの順序を決めます。ルールは降順で適用されます。たとえば、ロールに 3 つのルールがある場合、ルール 3、ルール 2、ルール 1 の順に適用されます。

拒否（deny）ルールは、どの権限ロールにも追加できません（特権レベル 0（priv-0）のロールを除きます）。

例

次に、ユーザ ロールにルールを追加する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# rule 1 deny command clear users
switch(config-role)# rule 1 permit read-write feature-group L3
```

次に、特権レベル 0 のユーザ ロールにルールを追加する例を示します。

```
switch(config)# role name priv-0
switch(config-role)# rule 1 deny command clear users
switch(config-role)#
```

次に、ユーザ ロールからルールを削除する例を示します。

```
switch(config)# role MyRole
switch(config-role)# no rule 10
```

関連コマンド

コマンド	説明
role name	ユーザ ロール名を作成または指定して、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロールを表示します。