# D コマンド

この章では、D で始まる Cisco NX-OS TrustSec コマンドについて説明します。

# deny

セキュリティ グループ アクセス コントロール リスト（SGACL）で拒否アクションを設定するには、**deny** 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。

**deny** {**all** | **icmp** | **igmp** | **ip** | {{**tcp** | **udp**} [{**dest** | **dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number*} | **range** *port-number1 port-number2*}]} [**log**]

**no deny** {**all** | **icmp** | **igmp** | **ip** | {{**tcp** | **udp**} [{**dest** | **dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number*} | **range** *port-number1 port-number2*}]} [**log**]

## 構文の説明

| | |
|---|---|
| **all** | すべてのトラフィックを指定します。 |
| **icmp** | インターネット制御メッセージ プロトコル（ICMP）トラフィックを指定します。 |
| **igmp** | インターネット グループ管理プロトコル（IGMP）トラフィックを指定します。 |
| **ip** | IP トラフィックを指定します。 |
| **tcp** | TCP トラフィックを指定します。 |
| **udp** | ユーザ データグラム プロトコル（UDP）トラフィックを指定します。 |
| **dest** | 宛先ポート番号を指定します。 |
| **dst** | 宛先ポート番号を指定します。 |
| **src** | 送信元ポート番号を指定します。 |
| **eq** | ポート番号と同等の番号を指定します。 |
| **gt** | ポート番号より大きい番号を指定します。 |
| **lt** | ポート番号より小さい番号を指定します。 |
| **neq** | ポート番号と同等ではない番号を指定します。 |
| *port-number* | TCP または UDP のポート番号。指定できる範囲は 0 ～ 65535 です。 |
| **range** | TCP または UDP のポート範囲を指定します。 |
| *port-number1* | 範囲の開始ポート。指定できる範囲は 0 ～ 65535 です。 |
| *port-number2* | 範囲の終了ポート。指定できる範囲は 0 ～ 65535 です。 |
| **log** | （任意）この設定に一致するパケットをログに記録することを指定します。 |

## コマンド デフォルト

なし

## コマンド モード

ロールベース アクセス コントロール リスト（RBACL）

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 5.1(3)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

このコマンドを使用するには、まず **feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにしてから、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

RBACL ロギングをイネーブルにするには、VLAN での RBACL ポリシーの強制をイネーブルにする必要があります。また **cts role-based counters enable** コマンドを使用して Cisco TrustSec カウンタをイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

## 例

次に、SGACL に拒否アクションを追加し、RBACL ログをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# deny icmp log
switch(config-rbacl)#
```

次に、SGACL から拒否アクションを削除する例を示します。

```
switch# configure terminal
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# no deny icmp log
switch(config-rbacl)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **cts role-based access-list** | Cisco TrustSec SGACL を設定します。 |
| **cts role-based counters** | RBACL カウンタをイネーブルにします。 |
| **feature cts** | Cisco TrustSec 機能をイネーブルにします。 |
| **feature dot1x** | スイッチ上で 802.1X 機能をイネーブルにします。 |
| **permit** | SGACL に許可ルールを設定します。 |
| **show cts role-based access-list** | Cisco TrustSec SGACL の設定を表示します。 |