F コマンド

この章では、F 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。

feature（ユーザ ロール機能グループ）

ユーザ ロール機能グループに機能を設定するには、**feature** コマンドを使用します。ユーザ ロール機能グループから機能を削除するには、このコマンドの **no** 形式を使用します。

feature *feature-name*

no feature *feature-name*

構文の説明

feature-name	**show role feature** コマンドの出力に表示される Cisco NX-OS 機能名。

デフォルト

なし

コマンド モード

ユーザ ロール機能グループ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(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

このコマンドで使用できる有効な機能名を表示するには、show role feature コマンドを使用します。

このコマンドには、ライセンスは不要です。

例

次に、ユーザ ロール機能グループに機能を追加する例を示します。

```
switch# configure terminal
switch(config)# role feature-group name SecGroup
switch(config-role-featuregrp)# feature aaa
switch(config-role-featuregrp)# feature radius
switch(config-role-featuregrp)# feature tacacs
```

次に、ユーザ ロール機能グループから機能を削除する例を示します。

```
switch# configure terminal
switch(config)# role feature-group name MyGroup
switch(config-role-featuregrp)# no feature callhome
```

関連コマンド

コマンド	説明
show role feature-group	ユーザ ロール機能グループを表示します。

feature cts

Cisco TrustSec 機能をイネーブルにするには、**feature cts** 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。

feature cts

no feature cts

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。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(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、**feature dot1x** 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。

（注） Cisco TrustSec 機能には、ライセンス猶予期間はありません。この機能を設定するには、アドバンスト サービス ライセンスをインストールする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、Cisco TrustSec 機能をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature cts
```

次に、Cisco TrustSec 機能をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no feature cts
```

関連コマンド

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。
show cts	Cisco TrustSec のステータス情報を表示します。

feature dhcp

デバイス上で DHCP スヌーピング機能をイネーブルにするには、**feature dhcp** コマンドを使用します。DHCP スヌーピング機能をディセーブルにし、DHCP リレー、Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）、IP ソース ガード設定を含む、DHCP スヌーピングに関連するすべての設定を削除するには、このコマンドの **no** 形式を使用します。

feature dhcp

no feature dhcp

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。

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

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(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

デフォルトの設定では、DHCP スヌーピング機能はディセーブルです。

DHCP スヌーピング機能をイネーブルにしないと、DHCP スヌーピングの関連コマンドを使用できません。

ダイナミック APR インスペクションおよび IP ソース ガードは、DHCP スヌーピング機能に依存します。

DHCP スヌーピング機能をディセーブルにすると、次の機能を含む、DHCP スヌーピング設定に関連するデバイス上のすべての設定が廃棄されます。

- DHCP スヌーピング
- DHCP リレー
- DAI
- IP ソース ガード

DHCP スヌーピング設定を保持したまま、DHCP スヌーピング機能をオフにしたい場合には、**no ip dhcp snooping** コマンドを使用して、DHCP スヌーピングをグローバルにディセーブルにします。

DHCP スヌーピング機能がイネーブルに設定されている場合、アクセス コントロール リスト（ACL）の統計情報はサポートされません。

このコマンドには、ライセンスは不要です。

例

次の例では、DHCP スヌーピングをイネーブルにする方法を示します。

```
switch# configure terminal
switch(config)# feature dhcp
switch(config)#'
```

関連コマンド

コマンド	説明
clear ip dhcp snooping binding	DHCP スヌーピング バインディング データベースを消去します。
ip dhcp snooping	デバイスの DHCP スヌーピングをグローバルにイネーブルにします。
service dhcp	DHCP リレー エージェントをイネーブルまたはディセーブルにします。
show ip dhcp snooping	DHCP スヌーピングに関する一般情報を表示します。
show running-config dhcp	IP ソース ガード設定を含めて、DHCP スヌーピング設定を表示します。

feature dot1x

802.1X 機能をイネーブルにするには、**feature dot1x** 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。

feature dot1x

no feature dot1x

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。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(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

802.1X を設定する前に、**feature dot1x** コマンドを使用する必要があります。

（注） 802.1X 機能をディセーブルにすると、すべての 802.1X 設定が失われます。802.1X 認証をディセーブルにする場合は、**no dot1x system-auth-control** コマンドを使用します。

このコマンドには、ライセンスは不要です。

例

次に、802.1X をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature dot1x
```

次に、802.1X をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no feature dot1x
```

関連コマンド

コマンド	説明
show dot1x	802.1X のステータス情報を表示します。

feature eou

Extensible Authentication Protocol over User Datagram Protocol（EAPoUDP）をイネーブルにするには、**feature eou** コマンドを使用します。EAPoUDP 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。

feature eou

no feature eou

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。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(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

EAPoUDP を設定する前に、**feature eou** コマンドを使用する必要があります。

（注） EAPoUDP をディセーブルにすると、Cisco NX-OS ソフトウェアにより EXPoUDP 設定が削除されます。

このコマンドには、ライセンスは不要です。

例

次に、EAPoUDP をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature eou
```

次に、EAPoUDP をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no feature eou
```

関連コマンド

コマンド	説明
feature eou	EAPoUDP をイネーブルにします。
show eou	EAPoUDP 情報を表示します。

feature ldap

Lightweight Directory Access Protocol（LDAP）をイネーブルにするには、**feature ldap** コマンドを使用します。LDAP 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。

feature ldap

no feature ldap

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。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

LDAP を設定する前に、**feature ldap** コマンドを使用する必要があります。

（注） LDAP をディセーブルにすると、Cisco NX-OS ソフトウェアにより LDAP 設定が削除されます。

このコマンドには、ライセンスは不要です。

例

次に、LDAP をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature ldap
```

次に、LDAP をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no feature ldap
```

関連コマンド

コマンド	説明
show running-config ldap	実行コンフィギュレーションの LDAP 設定を表示します。
show startup-config ldap	スタートアップ コンフィギュレーションの LDAP 設定を表示します。

feature port-security

ポート セキュリティ機能をグローバルでイネーブルにするには、**feature port-security** コマンドを使用します。ポート セキュリティ機能をグローバルで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。

feature port-security

no feature port-security

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。

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

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(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

デフォルトの設定では、ポート セキュリティはグローバルでディセーブルです。

ポート セキュリティは、各 Virtual Device Context（VDC; 仮想デバイス コンテキスト）に対してローカルです。必要な場合、このコマンドを使用する前に正しい VDC に切り替えます。

このコマンドには、ライセンスは不要です。

ポート セキュリティのイネーブル化

ポート セキュリティをグローバルでイネーブルにすると、ポート セキュリティに関連する他のすべてのコマンドが使用可能になります。

ポート セキュリティを再イネーブル化する場合、ポート セキュリティが最後にイネーブルだった時点のポート セキュリティ設定は復元されません。

ポート セキュリティのディセーブル化

ポート セキュリティをグローバルでディセーブルにすると、すべてのポート セキュリティ設定が削除されます。デバイスがアドレスをどのように学習したかに関係なく、ポート セキュリティのすべてのインターフェイス設定、およびすべてのセキュア MAC アドレスが削除されます。

例

次に、ポート セキュリティをグローバルでイネーブルにする例を示します。

```
switch# configure terminal
```

```
switch(config)# feature port-security
switch(config)#
```

関連コマンド

コマンド	説明
clear port-security	ダイナミックに学習されたセキュア MAC アドレスをクリアします。
debug port-security	ポート セキュリティのデバッグ情報を提供します。
show port-security	ポート セキュリティに関する情報を表示します。
switchport port-security	レイヤ 2 インターフェイス上のポート セキュリティをイネーブルにします。

feature privilege

TACACS+ サーバでコマンド認可にロールの累積権限をイネーブルにするには、**feature privilege** コマンドを使用します。ロールの累積権限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。

feature privilege

no feature privilege

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。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、ライセンスは不要です。

feature privilege コマンドをイネーブルにすると、権限ロールは低いレベルの権限ロールの権限を継承します。

例

次に、ロールの累積権限をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature privilege
```

次に、ロールの累積権限をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no feature privilege
2010 Feb 12 12:52:06 switch %FEATURE-MGR-2-FM_AUTOCKPT_IN_PROGRESS: AutoCheckpoint
system-fm-privilege's creation in progress...
switch(config)# 2010 Feb 12 12:52:06 switch %FEATURE-MGR-2-FM_AUTOCKPT_SUCCEEDED
AutoCheckpoint created successfully
```

関連コマンド

コマンド	説明
enable *level*	ユーザが高い権限レベルに移行できるようにします。
enable secret priv-lvl	特定の権限レベルのシークレット パスワードをイネーブルにします。
show privilege	現在の権限レベル、ユーザ名、および累積権限のサポートのステータスを表示します。
username *username* **priv-lvl**	ユーザが認可に権限レベルを使用できるようにします。

feature ssh

仮想デバイス コンテキスト（VDC）の Secure Shell（SSH; セキュア シェル）サーバをイネーブルにするには、**feature ssh** コマンドを使用します。SSH サーバ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。

feature ssh

no feature ssh

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。

デフォルト

イネーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.1(2)	このコマンドは、**ssh server enable** コマンドを置き換える目的で導入されました。

使用上のガイドライン

Cisco NX-OS ソフトウェアは、SSH バージョン 2 をサポートしています。

このコマンドには、ライセンスは不要です。

例

次に、SSH サーバをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature ssh
```

次に、SSH サーバをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
```

関連コマンド

コマンド	説明
show feature	機能のイネーブル ステータスを表示します。
show ssh server	SSH サーバ鍵の情報を表示します。

feature tacacs+

TACACS+ をイネーブルにするには、**feature tacacs+** コマンドを使用します。TACACS+ 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。

feature tacacs+

no feature tacacs+

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。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(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

TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

（注） TACACS+ をディセーブルにすると、Cisco NX-OS ソフトウェアにより TACACS+ 設定が削除されます。

このコマンドには、ライセンスは不要です。

例

次に、TACACS+ をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature tacacs+
```

次に、TACACS+ をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no feature tacacs+
```

関連コマンド

コマンド	説明
show tacacs+	TACACS+ 情報を表示します。

feature telnet

仮想デバイス コンテキスト（VDC）の Telnet サーバをイネーブルにするには、**feature telnet** コマンドを使用します。Telnet サーバ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。

feature telnet

no feature telnet

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。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.1(2)	このコマンドは、**telnet server enable** コマンドを置き換える目的で導入されました。

使用上のガイドライン

このコマンドには、ライセンスは不要です。

例

次に、Telnet サーバをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature telnet
```

次に、Telnet サーバをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no feature telnet
XML interface to system may become unavailable since ssh is disabled
```

関連コマンド

コマンド	説明
show feature	機能のイネーブル ステータスを表示します。
show telnet server	SSH サーバ鍵の情報を表示します。

filter

フィルタ マップ内に 1 つ以上の証明書マッピング フィルタを設定するには、**filter** コマンドを使用します。

filter [**subject-name** *subject-name* | **altname-email** *e-mail-ID* | **altname-upn** *user-principal-name*]

構文の説明

subject-name	証明書のサブジェクト名を指定します。
subject-name	LDAP 識別名（DN）ストリング フォーマットでの必要なサブジェクト名。次に例を示します。 cn=%username%,ou=PKI,o=Acme,c=US
altname-email	代替名としてメール ID を指定します。
e-mail-ID	サブジェクト代替名として証明書に存在する必要があるメール アドレス。次に例を示します。 %username%@*
altname-upn	代替名としてユーザ プリンシパル名を指定します。
user-principal-name	サブジェクト代替名として証明書に存在する必要があるプリンシパル名。次に例を示します。 %username-without-domain%@%hostname%

デフォルト

なし

コマンド モード

証明書マッピング フィルタ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
5.0(2)	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、新しいフィルタ マップを作成する必要があります。

証明書がマップに設定されているすべてのフィルタに合格した場合に、検証が合格します。

このコマンドには、ライセンスは不要です。

例

次に、フィルタ マップ内に証明書マッピング フィルタを設定する例を示します。

```
switch# configure terminal
switch(config)# crypto certificatemap mapname filtermap1
switch(config-certmap-filter)# filter altname-email jsmith@acme.com
```

関連コマンド

コマンド	説明
crypto certificatemap mapname	フィルタ マップを作成します。
show crypto certificatemap	証明書マッピング フィルタを表示します。

fragments

ACL で明示的な **permit** コマンドまたは **deny** コマンドに一致しない非初期フラグメントを、IPv4 ACL または IPv6 ACL で許可するか拒否するかについて最適化するには、**fragments** コマンドを使用します。フラグメントの最適化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。

fragments {**deny-all** | **permit-all**}

no fragments {**deny-all** | **permit-all**}

構文の説明

deny-all	ACL で一致するフローの非初期フラグメントが、常に破棄されるように指定します。
permit-all	フローの初期フラグメントが ACL で許可されたときに、フローの非初期フラグメントが許可されるように指定します。

デフォルト

なし

コマンド モード

IPv4 ACL コンフィギュレーション
IPv6 ACL コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.2(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

ACL で明示的な **permit** コマンドまたは **deny** コマンドに一致しない非初期フラグメントを許可または拒否する場合、**fragments** コマンドを使用すると、IP ACL の設定を簡素化できます。**fragments** キーワードを指定した、数多くの **permit** コマンドまたは **deny** コマンドを使用して非初期フラグメントの処理を制御する代わりに、**fragments** コマンドを使用できます。

デバイスで、**fragments** コマンドが含まれる ACL がトラフィックに適用される場合、このコマンドは、ACL での明示的な **permit** コマンドまたは **deny** コマンドに一致しない非初期フラグメントだけに一致します。

このコマンドには、ライセンスは不要です。

例

次に、lab-acl という名前の IPv4 ACL で、フラグメントの最適化をイネーブルにする例を示します。**permit-all** キーワードは、**fragments** キーワードが含まれる **deny** コマンドに一致しないすべての非初期フラグメントを ACL で許可することを意味します。

```
switch# configure terminal
switch(config)# ip access-list lab-acl
switch(config-acl)# fragments permit-all
```

次の例では、**fragments** コマンドが含まれる lab-acl IPv4 ACL を表示する方法を示します。便宜上、**fragments** コマンドは ACL の最初に表示されます。ただし、非初期フラグメントがデバイスで許可されるのは、ACL で非初期フラグメントが他のすべての明示的なルールに一致しなくなったあとだけです。

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

IP access list lab-acl
        fragments permit-all
        10 permit tcp 10.0.0.0/8 172.28.254.254/24 eq tacacs
        20 permit tcp 10.0.0.0/8 172.28.254.154/24 eq tacacs
        30 permit tcp 10.0.0.0/8 172.28.254.54/24 eq tacacs
```

関連コマンド

コマンド	説明
deny（IPv4）	IPv4 ACL に拒否（deny）ルールを設定します。
deny（IPv6）	IPv6 ACL に拒否（deny）ルールを設定します。
permit（IPv4）	IPv4 ACL に許可（permit）ルールを設定します。
permit（IPv6）	IPv6 ACL に許可（permit）ルールを設定します。
show ip access-list	すべての IPv4 ACL または特定の IPv4 ACL を表示します。
show ipv6 access-list	すべての IPv6 ACL または特定の IPv6 ACL を表示します。