



E コマンド

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

eou allow clientless

クライアントレス エンドポイント デバイスの Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) ポスチャ検証をイネーブ爾するには、**eou allow clientless** コマンドを使用します。クライアントレス エンドポイント デバイスのポスチャ検証をディセーブルにするには、コマンドの **no** 形式を使用します。

eou allow clientless

no eou allow clientless

シンタックスの説明 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)	このコマンドが導入されました。

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。
このコマンドにライセンスは必要ありません。

例 次に、クライアントレス エンドポイント デバイスの EAPoUDP ポスチャ検証を許可する例を示します。

```
switch# config t
switch(config)# eou allow clientless
```

次に、クライアントレス エンドポイント デバイスの EAPoUDP ポスチャ検証が行われないようにする例を示します。

```
switch# config t
switch(config)# no eou allow clientless
```

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。

eou default

EAPoUDP のグローバルまたはインターフェイスの設定値をデフォルトに戻すには、**eou default** コマンドを使用します。

eou default

シンタックスの説明 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
インターフェイス 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)	このコマンドが導入されました。

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。
このコマンドにライセンスは必要ありません。

例 次に、グローバル EAPoUDP 設定をデフォルトに変更する例を示します。

```
switch# config t
switch(config)# eou default
```

次に、インターフェイスの EAPoUDP 設定をデフォルトに変更する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou default
```

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。

eou initialize

EAPoUDP セッションを初期化するには、**eou initialize** コマンドを使用します。

```
eou initialize {all | authentication {clientless | eap | static} | interface ethernet slot/port | ip-address
  ipv4-address | mac-address mac-address | posturetoken name}
```

シンタックスの説明		
all		すべての EAPoUDP セッションを初期化します。
authentication		特定の認証タイプの EAPoUDP セッションを初期化します。
clientless		クライアントレス ポスチャ検証を使用して認証するセッションを指定します。
eap		EAPoUDP を使用して認証するセッションを指定します。
static		静的に設定された例外リストを使用して認証するセッションを指定します。
interface ethernet slot/port		特定のインターフェイスの EAPoUDP セッションを初期化します。
ip-address ipv4-address		特定の IPv4 アドレスの EAPoUDP セッションを初期化します。
mac-address mac-address		特定の MAC アドレスの EAPoUDP セッションを初期化します。
posturetoken name		特定のポスチャ トークンの EAPoUDP セッションを初期化します。

デフォルト なし

コマンド モード 任意のコマンド モード

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)	このコマンドが導入されました。

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。
このコマンドにライセンスは必要ありません。

例 次に、すべての EAPoUDP セッションを初期化する例を示します。

```
switch# eou initialize all
```

次に、静的に認証された EAPoUDP セッションを初期化する例を示します。

```
switch# eou initialize authentication static
```

次に、インターフェイスの EAPoUDP セッションを初期化する例を示します。

```
switch# eou initialize interface ethernet 1/1
```

次に、IP アドレスの EAPoUDP セッションを初期化する例を示します。

```
switch# eou initialize ip-address 10.10.1.1
```

次に、MAC アドレスのすべての EAPoUDP セッションを初期化する例を示します。

```
switch# eou initialize mac-address 0019.076c.dac4
```

次に、ポスチャ トークンのすべての EAPoUDP セッションを初期化する例を示します。

```
switch# eou initialize posturetoken healthy
```

関連コマンド

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

eou logging

EAPoUDP ロギングをイネーブルにするには、**eou logging** コマンドを使用します。EAPoUDP ロギング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。

eou logging

no eou logging

シンタックスの説明 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

グローバル コンフィギュレーション：ディセーブル

インターフェイス コンフィギュレーション：グローバル コンフィギュレーション設定

コマンド モード

グローバル コンフィギュレーション

インターフェイス 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)	このコマンドが導入されました。

使用上のガイドライン

インターフェイス上の EAPoUDP ロギングの設定はグローバル設定を上書きします。

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。

このコマンドにライセンスは必要ありません。

例

次に、グローバル EAPoUDP ロギングをイネーブルにする例を示します。

```
switch# config t
switch(config)# eou logging
```

次に、グローバル EAPoUDP ロギングをディセーブルにする例を示します。

```
switch# config t
switch(config)# no eou logging
```

次に、インターフェイスの EAPoUDP ロギングをイネーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou logging
```

次に、インターフェイスの EAPoUDP ロギングをディセーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# no eou logging
```

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。

eou max-retry

EAPoUDP の最大試行回数をグローバルに、またはインターフェイス単位で設定するには、**eou max-retry** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

eou max-retry count

no eou max-retry

シンタックスの説明

count 最大リトライ試行回数。有効範囲は 1 ～ 3 回です。

デフォルト

グローバル コンフィギュレーション : 3

インターフェイス コンフィギュレーション : グローバル コンフィギュレーション値

コマンド モード

グローバル コンフィギュレーション

インターフェイス 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) このコマンドが導入されました。

使用上のガイドライン

インターフェイスの最大リトライ回数は、グローバル設定値より優先されます。

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。

このコマンドにライセンスは必要ありません。

例

次に、EAPoUDP のグローバル最大リトライ試行回数を変更する例を示します。

```
switch# config t
switch(config)# eou max-retry 2
```

次に、EAPoUDP のグローバル最大リトライ試行回数の設定をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# no eou max-retry
```

次に、インターフェイスの EAPoUDP 最大リトライ試行回数を変更する例を示します。

```
switch# config t
switch(config) interface ethernet 1/1
switch(config-if)# eou max-retry 3
```

次に、インターフェイスの EAPoUDP 最大リトライ試行回数の設定をデフォルトに戻す例を示します。

```
switch# config t
switch(config) interface ethernet 1/1
switch(config-if)# no eou max-retry
```

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。

eou port

EAPoUDP の User Datagram Protocol (UDP; ユーザ データグラム プロトコル) ポート番号を設定するには、**eou port** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

```
eou port udp-port
```

```
no eou port
```

シンタックスの説明

udp-port UDP ポート番号。有効範囲は 1 ~ 65535 です。

デフォルト

21862 (0x5566)

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)	このコマンドが導入されました。

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。

このコマンドにライセンスは必要ありません。

例

次に、EAPoUDP の UDP ポート番号を変更する例を示します。

```
switch# config t
switch(config)# eou port 21856
```

次に、EAPoUDP の UDP ポート番号をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# no eou port
```

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。

eou ratelimit

EAPoUDP ポスチャ検証の同時セッション数を設定するには、**eou ratelimit** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

eou ratelimit sessions

no eou ratelimit

シンタックスの説明	<i>sessions</i> EAPoUDP ポスチャ検証の最大同時セッション数。有効範囲は 0 ~ 200 です。
------------------	---

デフォルト	グローバル コンフィギュレーション : 20 インターフェイス コンフィギュレーション : グローバル コンフィギュレーション設定
--------------	--

コマンド モード	グローバル コンフィギュレーション インターフェイス 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) このコマンドが導入されました。

使用上のガイドライン	EAPoUDP レート制限をゼロ (0) に設定すると、ポスチャ検証の同時セッションは許可されません。インターフェイスの EAPoUDP レート制限設定は、グローバル EAPoUDP レート制限設定を上書きします。 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。 このコマンドにライセンスは必要ありません。
-------------------	--

例	次に、EAPoUDP ポスチャ検証のグローバル最大同時セッション数を変更する例を示します。 <pre>switch# config t switch(config)# eou ratelimit 30</pre> 次に、EAPoUDP ポスチャ検証のグローバル最大同時セッション数をデフォルトに戻す例を示します。 <pre>switch# config t switch(config)# no eou ratelimit</pre> 次に、インターフェイスの EAPoUDP ポスチャ検証の最大同時セッション数を変更する例を示します。 <pre>switch# config t switch(config)# interface ethernet 1/1 switch(config-if)# eou ratelimit 30</pre>
----------	--

次に、インターフェイスの EAPoUDP ポスチャ検証の最大同時セッション数をデフォルトに戻す例を示します。

```
switch# config t  
switch(config)# interface ethernet 1/1  
switch(config-if)# no eou ratelimit
```

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。

eou revalidate (EXEC)

EAPoUDP セッションを再検証するには、**eou revalidate** コマンドを使用します。

```
eou revalidate {all | authentication {clientless | eap | static} | interface ethernet slot/port | ip-address
  ipv4-address | mac-address mac-address | posturetoken name}
```

シンタックスの説明		
all		すべての EAPoUDP セッションを再検証します。
authentication		特定の認証タイプの EAPoUDP セッションを再検証します。
clientless		クライアントレス ポスチャ検証を使用して認証するセッションを指定します。
eap		EAPoUDP を使用して認証するセッションを指定します。
static		静的に設定された例外リストを使用して認証するセッションを指定します。
interface ethernet slot/port		特定のインターフェイスの EAPoUDP セッションを再検証します。
ip-address ipv4-address		特定の IPv4 アドレスの EAPoUDP セッションを再検証します。
mac-address mac-address		特定の MAC アドレスの EAPoUDP セッションを再検証します。
posturetoken name		特定のポスチャ トークンの EAPoUDP セッションを再検証します。

デフォルト なし

コマンド モード 任意のコマンド モード



(注)

NX-OS ソフトウェアは、グローバル コンフィギュレーション モードの **eou revalidate** コマンドをサポートします。グローバル コンフィギュレーション モードで EXEC レベルの **eou revalidate** コマンドを使用するには、必須キーワードを指定します。

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)	このコマンドが導入されました。

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。
このコマンドにライセンスは必要ありません。

例 次に、すべての EAPoUDP セッションを再検証する例を示します。

```
switch# eou revalidate all
```

次に、すべての EAPoUDP セッションを再検証する例を示します。

```
switch# eou revalidate authentication static
```

■ eou revalidate (EXEC)

次に、すべての EAPoUDP セッションを再検証する例を示します。

```
switch# eou revalidate interface ethernet 1/1
```

次に、すべての EAPoUDP セッションを再検証する例を示します。

```
switch# eou revalidate ip-address 10.10.1.1
```

次に、すべての EAPoUDP セッションを再検証する例を示します。

```
switch# eou revalidate mac-address 0019.076c.dac4
```

次に、すべての EAPoUDP セッションを再検証する例を示します。

```
switch# eou revalidate posturetoken healthy
```

関連コマンド

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

eou revalidate (グローバル コンフィギュレーション、インターフェイス コンフィギュレーション)

EAPoUDP セッションの定期的な自動再検証をグローバルに、または特定のインターフェイスでイネーブルにするには、**eou revalidate** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

eou revalidate

no eou revalidate

シンタックスの説明 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 グローバル コンフィギュレーション：イネーブル

インターフェイス コンフィギュレーション：グローバル コンフィギュレーション値

コマンド モード グローバル コンフィギュレーション
インターフェイス 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)	このコマンドが導入されました。

使用上のガイドライン インターフェイスの自動再検証の設定は、グローバル自動再検証の設定を上書きします。



(注) NX-OS ソフトウェアは、EXEC コンフィギュレーション モードの **eou revalidate** コマンドをサポートします。グローバル コンフィギュレーション モードで EXEC レベルの **eou revalidate** コマンドを使用するには、必須キーワードを指定します。

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。

このコマンドにライセンスは必要ありません。

例 次に、EAPoUDP セッションのグローバル自動再検証をディセーブルにする例を示します。

```
switch# config t
switch(config)# no eou revalidate
```

次に、EAPoUDP セッションのグローバル自動再検証をイネーブルにする例を示します。

```
switch# config t
switch(config)# eou revalidate
```

■ eou revalidate (グローバルコンフィギュレーション、インターフェイスコンフィギュレーション)

次に、インターフェイスの EAPoUDP セッションの自動再検証をディセーブルにする例を示します。

```
switch# config t
switch(config)# no eou revalidate
```

次に、インターフェイスの EAPoUDP セッションの自動再検証をイネーブルにする例を示します。

```
switch# config t
switch(config)# eou revalidate
```

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。
eou timeout	EAPoUDP の定期的な自動再検証のタイムアウト間隔を設定します。
show eou	EAPoUDP 情報を表示します。


eou timeout

EAPoUDP グローバル タイマーまたはインターフェイスの EAPoUDP タイマーのタイムアウト間隔を設定するには、**eou timeout** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

```
eou timeout {aaa seconds | hold-period seconds | retransmit seconds | revalidation seconds |
status-query seconds}
```

```
no eou timeout {aaa | hold-period | retransmit | revalidation | status-query}
```

シンタックスの説明

aaa seconds	AAA タイムアウト間隔を指定します。有効範囲は 0 ～ 60 秒です。
	 (注) AAA タイムアウト間隔をゼロ (0) に設定すると、AAA タイマーがディセーブルになります。
hold-period seconds	ホールド タイムアウト間隔を指定します。有効範囲は 60 ～ 86400 秒です。
retransmit seconds	再送信タイムアウト間隔を指定します。有効範囲は 1 ～ 60 秒です。
revalidation seconds	定期的な自動再検証タイムアウト間隔を指定します。有効範囲は 5 ～ 86400 秒です。
status-query seconds	ステータス クエリー タイムアウト間隔を指定します。有効範囲は 10 ～ 1800 秒です。

デフォルト

グローバル AAA タイムアウト間隔：60 秒 (1 分)
 グローバル ホールド時間タイムアウト：180 秒 (3 分)
 グローバル再送信タイムアウト間隔：3 秒
 グローバル再検証タイムアウト間隔：36000 秒 (10 時間)
 グローバル ステータス クエリー タイムアウト間隔：300 秒 (5 分)
 インターフェイス タイムアウト間隔：グローバル コンフィギュレーション値

コマンド モード

グローバル コンフィギュレーション
 インターフェイス 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)	このコマンドが導入されました。

使用上のガイドライン

インターフェイス タイマーのタイムアウト間隔値は、グローバル タイムアウト値を上書きします。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。このコマンドにライセンスは必要ありません。

例

次に、グローバル AAA タイムアウト間隔を変更する例を示します。

```
switch# config t
switch(config)# eou timeout aaa 50
```

次に、インターフェイスの AAA タイムアウト間隔を変更する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou timeout aaa 60
```

次に、グローバル ホールド時間タイムアウト間隔を変更する例を示します。

```
switch# config t
switch(config)# eou timeout hold-period 480
```

次に、インターフェイスのホールド時間タイムアウト間隔を変更する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou timeout hold-period 540
```

次に、グローバル再送信タイムアウト間隔を変更する例を示します。

```
switch# config t
switch(config)# eou timeout retransmit 5
```

次に、インターフェイスの再送信タイムアウト間隔を変更する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou timeout retransmit 4
```

次に、グローバル再検証タイムアウト間隔を変更する例を示します。

```
switch# config t
switch(config)# eou timeout revalidation 34000
```

次に、インターフェイスの再検証タイムアウト間隔を変更する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou timeout revalidation 30000
```

次に、グローバル ステータス クエリー タイムアウト間隔を変更する例を示します。

```
switch# config t
switch(config)# eou timeout status-query 240
```

次に、インターフェイスのステータス クエリー タイムアウト間隔を変更する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou timeout status-query 270
```

関連コマンド

コマンド	説明
<code>feature eou</code>	EAPoUDP をイネーブルにします。
<code>eou revalidate</code> (グローバル コンフィギュレーション)	エンドポイント デバイスの定期的な自動再検証をイネーブルにします。
<code>show eou</code>	EAPoUDP 情報を表示します。

eq

単一ポートを IP ポート オブジェクト グループのグループ メンバーとして指定するには、**eq** コマンドを使用します。ポート オブジェクト グループから単一のポート グループ メンバーを削除するには、このコマンドの **no** 形式を使用します。

```
[sequence-number] eq port-number
no {sequence-number | eq port-number}
```

シンタックスの説明

<i>sequence-number</i>	(任意) このグループ メンバーのシーケンス番号。オブジェクト グループ内のグループ メンバーの順序は、シーケンス番号によって維持されます。有効なシーケンス番号は 1 ~ 4294967295 です。シーケンス番号を指定しない場合は、デバイスによって現在のオブジェクト グループで最も大きいシーケンス番号よりも 10 大きい番号が割り当てられます。
<i>port-number</i>	このグループ メンバーが一致するポート番号。有効なポート番号は、0 ~ 65535 です。

デフォルト

なし

コマンド モード

IP ポート オブジェクト 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)	このコマンドが導入されました。

使用上のガイドライン

IP ポート オブジェクト グループには方向がありません。**eq** コマンドが送信元ポートまたは宛先ポートのいずれに一致するか、またインバウンドとアウトバウンドのいずれのトラフィックに適用されるかは、ACL でオブジェクト グループをどのように使用するかによって決まります。

このコマンドにライセンスは必要ありません。

例

次に、ポート 443 から送受信されるトラフィックに一致するグループ メンバーを持つ port-group-05 という名前の IP ポート オブジェクト グループを設定する例を示します。

```
switch# config t
switch(config)# object-group ip port port-group-05
switch(config-port-ogroup)# eq 443
```

関連コマンド

コマンド	説明
gt	IP ポート オブジェクト グループの指定値より大きい値のグループ メンバーを指定します。
lt	IP ポート オブジェクト グループの指定値より小さい値のグループ メンバーを指定します。
neq	IP ポート オブジェクト グループの指定値に一致しないグループ メンバーを指定します。
object-group ip port	IP ポート オブジェクト グループを設定します。
range	IP ポート オブジェクト グループのポート範囲内のグループ メンバーを指定します。
show object-group	オブジェクト グループを表示します。