Cisco Secure Firewall によって送信される RST パケットについて

内容

はじめに

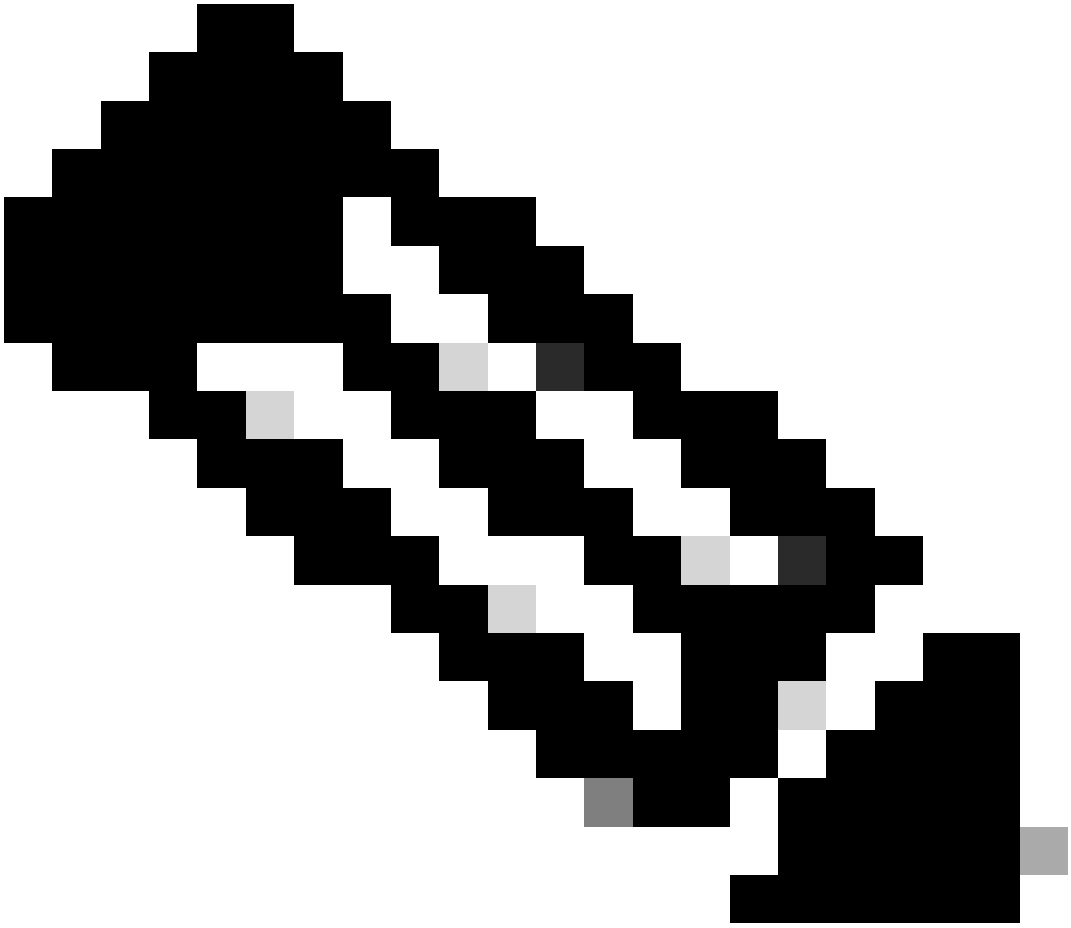
このドキュメントでは、ファイアウォールを通過しようとする TCP セッションに対して TCP リセットが送信された場合のシスコファイアウォールの動作について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ASA パケット フロー
- FTDパケットフロー
- ASA/FTDパケットキャプチャ



注：この動作は、ASAおよびセキュアファイアウォール脅威対策に適用されます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づくものです。

- ASA
- セキュアファイアウォール脅威対策FTD

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

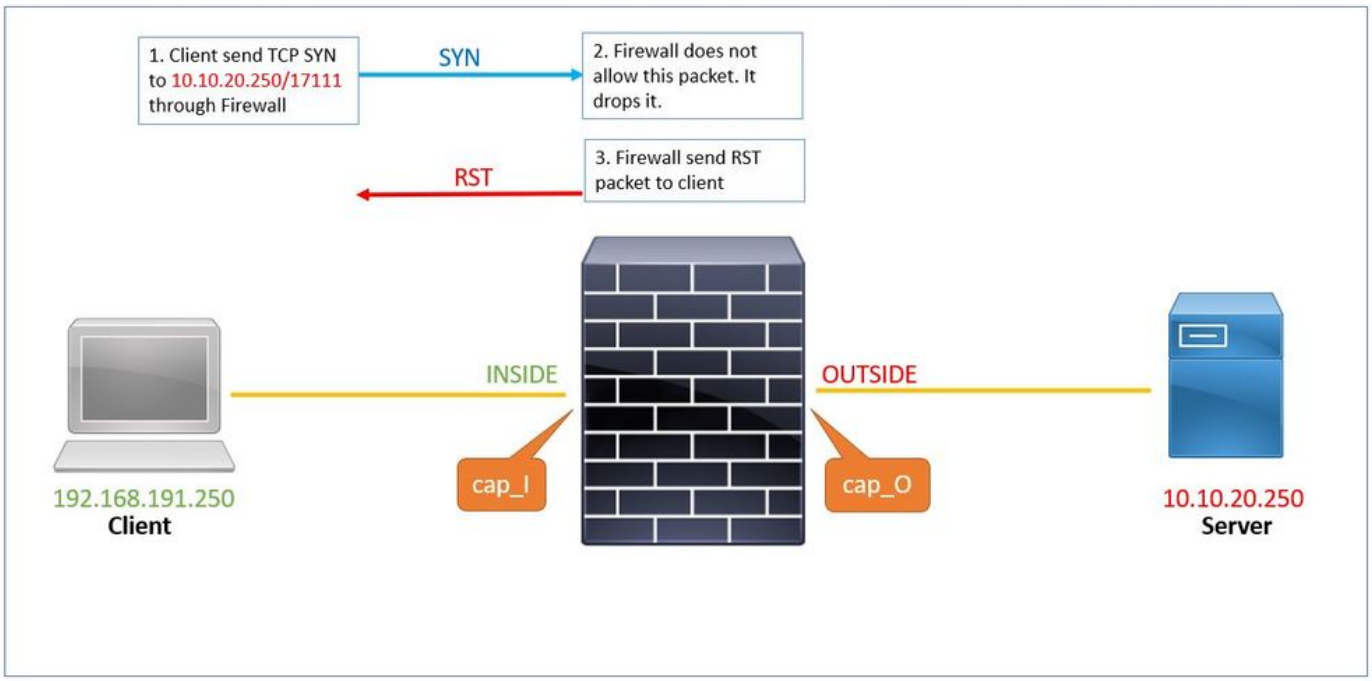
トラブルシュート

ファイアウォールは、ファイアウォールの通過を試みるTCPセッションに対してTCP Resetを送

信し、アクセスリストに基づいてファイアウォールによって拒否されます。また、アクセスリストで許可されていても、ファイアウォール内に存在する接続に属していないためにステートフル機能によって拒否されているパケットに対しても、ファイアウォールはリセットを送信します。

ケーススタディ1：サービス resetoutbound が有効で、クライアントからサーバへのトラフィックが拒否される。

デフォルトでは、service **resetoutbound**はすべてのインターフェイスに対して有効になっています。このケーススタディでは、クライアントからサーバへのトラフィックを許可するルールはありません。



ファイアウォールに設定されているキャプチャは次のとおりです。

```
# show capture
capture cap_I type raw-data trace trace-count 50 interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.191.250 host 10.10.20.250
capture cap_O type raw-data trace trace-count 50 interface OUTSIDE [Capturing - 0 bytes]
match tcp host 192.168.191.250 host 10.10.20.250
capture asp type asp-drop all [Capturing - 0 bytes]
match tcp host 192.168.191.250 host 10.10.20.250
```

Service resetoutboundはデフォルトで有効になっています。したがって、show run service コマンドの出力に何も表示されない場合、それが有効であることを意味します。

```
# show run service ...
```

1. クライアントはファイアウォールを介してサーバ10.10.20.250/17111にTCP SYNを送信します。このキャプチャのパケット番号1:

```
# show capture cap_I
1: 19:48:55.512500 192.168.191.250.46118 > 10.10.20.250.17111: S 3490277958:3490277958(0) win 29200 <ms
```

2. このトラフィックを許可するACLがないため、セキュアファイアウォールはacl-dropの理由でこのパケットをドロップします。このパケットは、asp-dropキャプチャでキャプチャされます。

```
# show capture cap_I packet-number 1 trace det

1: 19:48:55.512500 a2c7.1e00.0004 0050.56b3.05b1 0x0800 Length: 74
192.168.191.250.46118 > 10.10.20.250.17111: S [tcp sum ok] 3490277958:3490277958(0) win 29200 <mss 1380
    (DF) (ttl 49, id 60335)

<output removed>

Subtype: log
Result: DROP
Config:
access-group allow_all global
access-list allow_all extended deny ip any any
Additional Information:

<output removed>

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
```

```
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame 0x0000561961c8333f flow
```

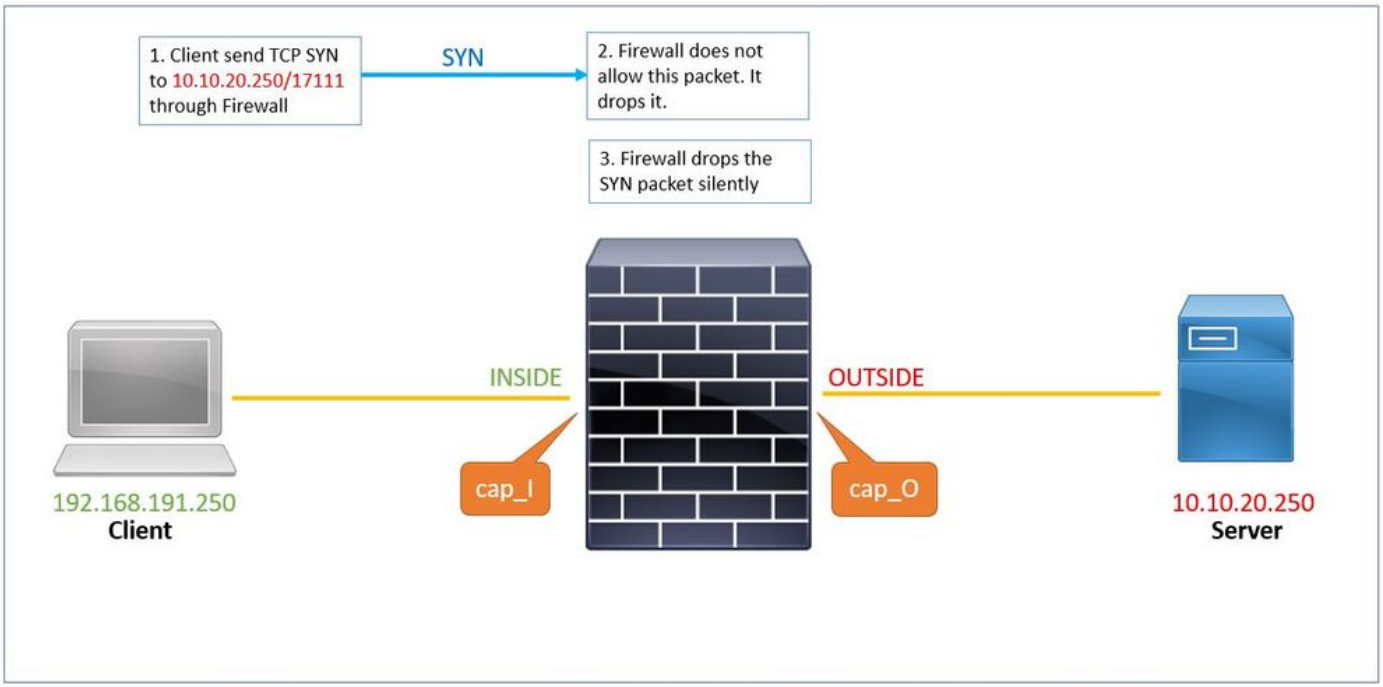
3. ファイアウォールは、送信元IPアドレスとしてサーバIPアドレスを使用してRSTパケットを送信します。このキャプチャのパケット番号2:

```
# show capture cap_I
1: 19:48:55.512500 192.168.191.250.46118 > 10.10.20.250.17111: S 3490277958:3490277958(0) win 29200 <ms
        timestamp 2096884214 0,nop,wscale 7>
2: 19:48:55.512806 10.10.20.250.17111 > 192.168.191.250.46118: R 0:0(0) ack 3490277959 win 29200
```

ケーススタディ2：サービス**resetoutbound**が無効で、クライアントからサーバへのトラフィックが拒否される。

ケーススタディ2では、クライアントからサーバへのトラフィックを許可するルールはなく、サービス**resetoutbound**は無効になっています。

show run service



コマンドにより、service **resetoutbound**が無効になっていることが表示されます。

```
# show run service
no service resetoutbound
```

1. クライアントはファイアウォールを介してサーバ10.10.20.250/17111にTCP TCPを送信します。このキャプチャのパケット番号1:

```
# show capture cap_I

1: 19:48:55.512500 192.168.191.250.46118 > 10.10.20.250.17111: S 3490277958:3490277958(0) win 29200
<mss 1380,sackOK,timestamp 2096884214 0,nop,wscale 7>
```

2. このトラフィックを許可するACLがないため、セキュアファイアウォールはacl-dropの理由でこのパケットをドロップします。このパケットは、 **asp-drop capture**.

```
# show capture cap_I packet-number 1 trace det

1: 19:48:55.512500 a2c7.1e00.0004 0050.56b3.05b1 0x0800 Length: 74 192.168.191.250.46118 > 10.10.20.250
```

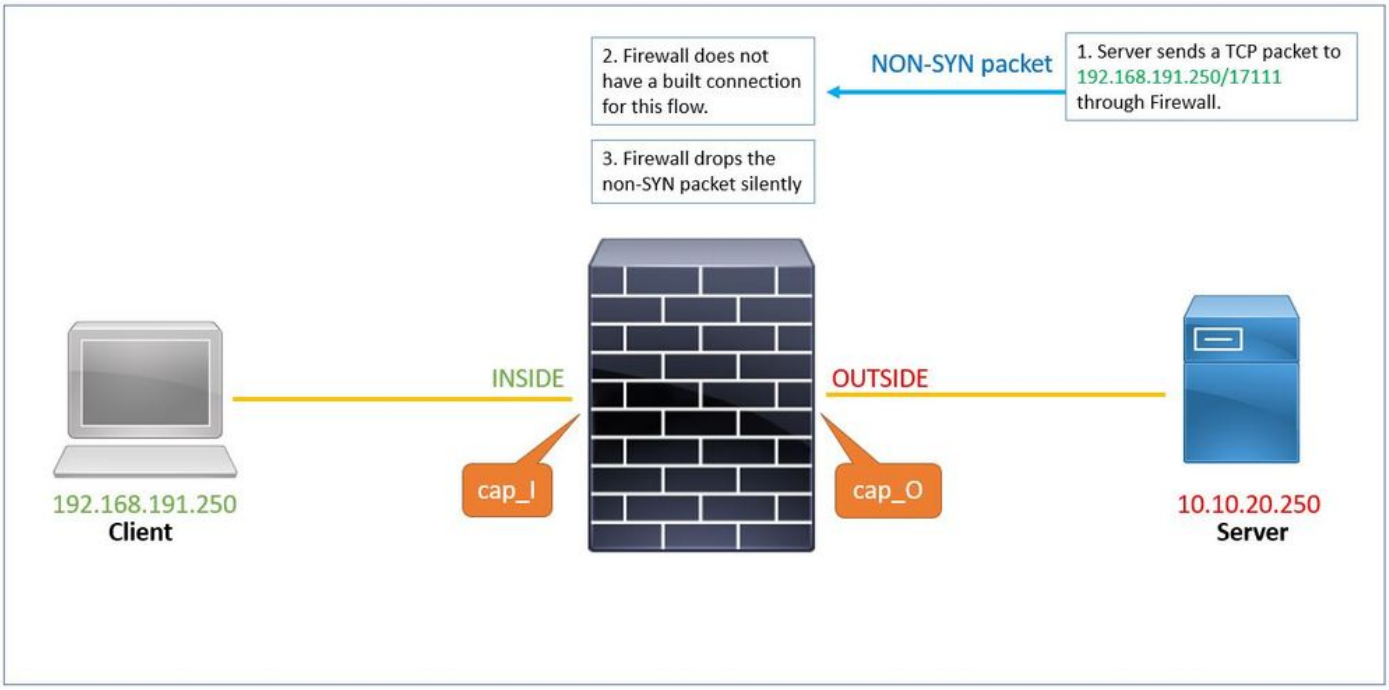
3. **asp-drop capture** はSYNパケットを示していますが、内部インターフェイス経由でcap_I captureに返信されたRSTパケットはありません。

```
# show cap cap_I
1: 23:58:32.850755 192.168.191.250.46118 > 10.10.20.250.17111: S 3490277958:3490277958(0) win 29200 <ms

# show cap asp
1: 23:58:32.850999 192.168.191.250.46118 > 10.10.20.250.17111: S 3490277958:3490277958(0) win 29200 <ms
```

ケーススタディ3：サービス**resetoutbound**が（デフォルトで）無効になっているサービス**resetinbound**が（デフォルトで）無効になっている

デフォルトでは、service **resetoutbound** はすべてのインターフェイスに対して有効であり、service **resetinbound** は無効です。



1. サーバがファイアウォールを介してクライアントにTCPパケット(SYN/ACK)を送信する。ファイアウォールには、このフローに対する接続が構築されていません。

```
# show capture cap_O

1: 00:22:35.111993 10.10.20.250.17111 > 192.168.191.250.46118: S 3475024584:3475024584(0) ack 349027795
```

2. リセットはファイアウォールからサーバに送信されません。このSYN/ACKパケットは、tcp-not-synの理由により、通知されることなく廃棄されます。これは、 asp-drop captureでもキャプチャされます。

```
# show capture cap_O packet-number 1 trace detail
1: 00:22:35.111993 a2c7.1e00.003e 0050.56b3.1ef5 0x0800 Length: 70
10.10.20.250.17111 > 192.168.191.250.46118: S [tcp sum ok] 3475024584:3475024584(0) ack 3490277959 win
   (DF) (ttl 255, id 62104)

<output removed>

Result:
input-interface: OUTSIDE
input-status: up
input-line-status: up
output-interface: INSIDE
output-status: up
output-line-status: up
Action: drop
Drop-reason: (tcp-not-syn) First TCP packet not SYN, Drop-location: frame 0x0000561961c89aaa flow (NA)/
</pre
```

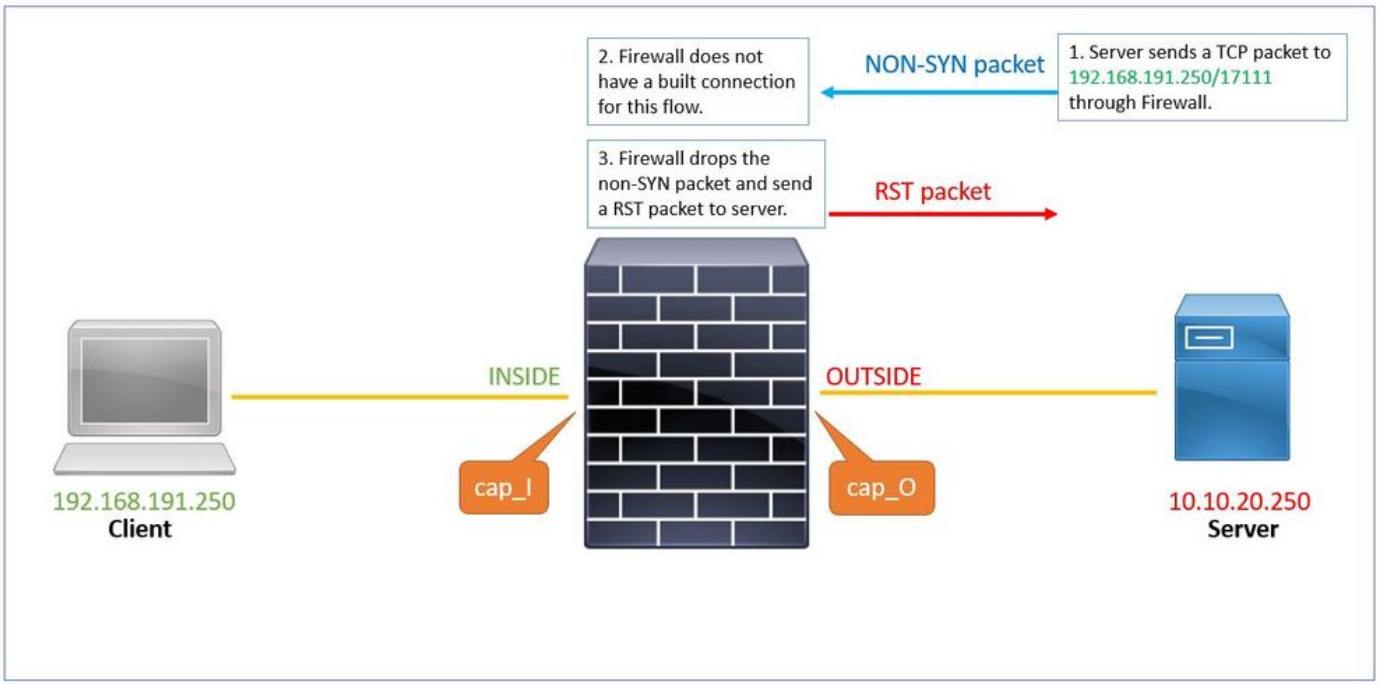
```
# show capture asp

1: 00:22:35.112176 10.10.20.250.17111 > 192.168.191.250.46118: S 3475024584:3475024584(0) ack 349027795
```

ケーススタディ４：サービスresetoutboundが（デフォルトで）無効になっているサービスresetinboundが無効になっている。

デフォルトでは、service **resetoutbound**はすべてのインターフェイスに対して無効であり、service **resetinbound**もコンフィギュレーションコマンドを使用して無効になっています。

show run service



コマンドの出力には、service **resetoutbound**が（デフォルトで）ディセーブルであり、コンフィギュレーションコマンドでservice **resetinbound**がディセーブルであることが表示されます。

```
# show run service
service resetinbound
```

1. サーバがファイアウォールを介してクライアントにTCPパケット(SYN/ACK)を送信する。

```
# show cap cap_O

1: 00:32:26.434395 10.10.20.250.17111 > 192.168.191.250.46118: S 3475024584:3475024584(0) ack 349027795
```

2. このフローに対する接続がファイアウォールに確立されておらず、ファイアウォールによってドロップされている。asp-drop capturesはパケットを表示します。

```
# show capture cap_O packet-number 1 trace detail
1: 00:32:26.434395 a2c7.1e00.003e 0050.56b3.1ef5 0x0800 Length: 70
10.10.20.250.17111 > 192.168.191.250.46118: S [tcp sum ok] 3475024584:3475024584(0) ack 3490277959 win
   (DF) (ttl 255, id 62104)

<output removed>

Result:
input-interface: OUTSIDE
input-status: up
input-line-status: up
output-interface: INSIDE
output-status: up
output-line-status: up
Action: drop
Drop-reason: (tcp-not-syn) First TCP packet not SYN, Drop-location: frame 0x0000561961c89aaa flow (NA)/
```

3. サービスが**resetinbound**状態になったため、ファイアウォールはクライアントの送信元IPアドレスを使用してRSTパケットをサーバに送信します。

```
# show capture cap_O
1: 00:32:26.434395 10.10.20.250.17111 > 192.168.191.250.46118: S 3475024584:3475024584(0) ack 349027795
2: 00:32:26.434608 192.168.191.250.46118 > 10.10.20.250.17111: R 3490277959:3490277959(0) ack 347502458
```

関連情報

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。