

対称NATとの相互運用性のためのTLOC拡張用スタティックNATの設定

内容

[はじめに](#)

[推奨事項](#)

[使用するコンポーネント](#)

[問題](#)

[トポロジ](#)

[条件](#)

[問題の特定](#)

[ステップ 1 : BFDセッションの確認](#)

[ステップ 2 : NATタイプの確認](#)

[ステップ 3 : NAT設定をチェックします](#)

[ステップ 4 : パブリックIPとポートを確認します。](#)

[ステップ 5 : NAT変換をチェックします](#)

[手順 6 : FIAトレースのチェック](#)

[手順 7 : BFDカウンタの確認](#)

[解決方法](#)

[検証](#)

[参考資料](#)

はじめに

このドキュメントでは、対称NATの背後にあるピアと連携するために、NATオーバーロードを使用して、TLOC拡張ルータでスタティックNATを設定する方法について説明します。

推奨事項

次の項目に関する知識があることが推奨されます。

- Cisco Catalystソフトウェア定義型ワイドエリアネットワーク(SD-WAN)
- ネットワーク アドレス変換 (NAT)
- TLOC拡張

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- C8000Vバージョン17.15.1a

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。

問題

『[Cisco Catalyst SD-WAN設計ガイド](#)』では、特定のタイプのネットワークアドレス変換(NAT)がコントロール接続とBFDトンネルの形成に影響を与える可能性があることが強調されています。

連携して動作しない2種類のNATは、ポート/アドレス制限付きNATと対称NATです。これらのNATタイプでは、各ポートでトラフィックを許可するために内部ネットワークからセッションを開始する必要があります。つまり、外部トラフィックは、内部からの事前の要求がない限り、内部ネットワークへの接続を開始できません。

対称NATの背後にあるサイトでは、ピアサイトとのBFDセッションの確立に問題が生じることがよくあります。これは、NATオーバーロード（別名、ポート/アドレス制限付きNAT）の背後でTLOC拡張を使用するサイトとピアリングする場合に、特に困難です。

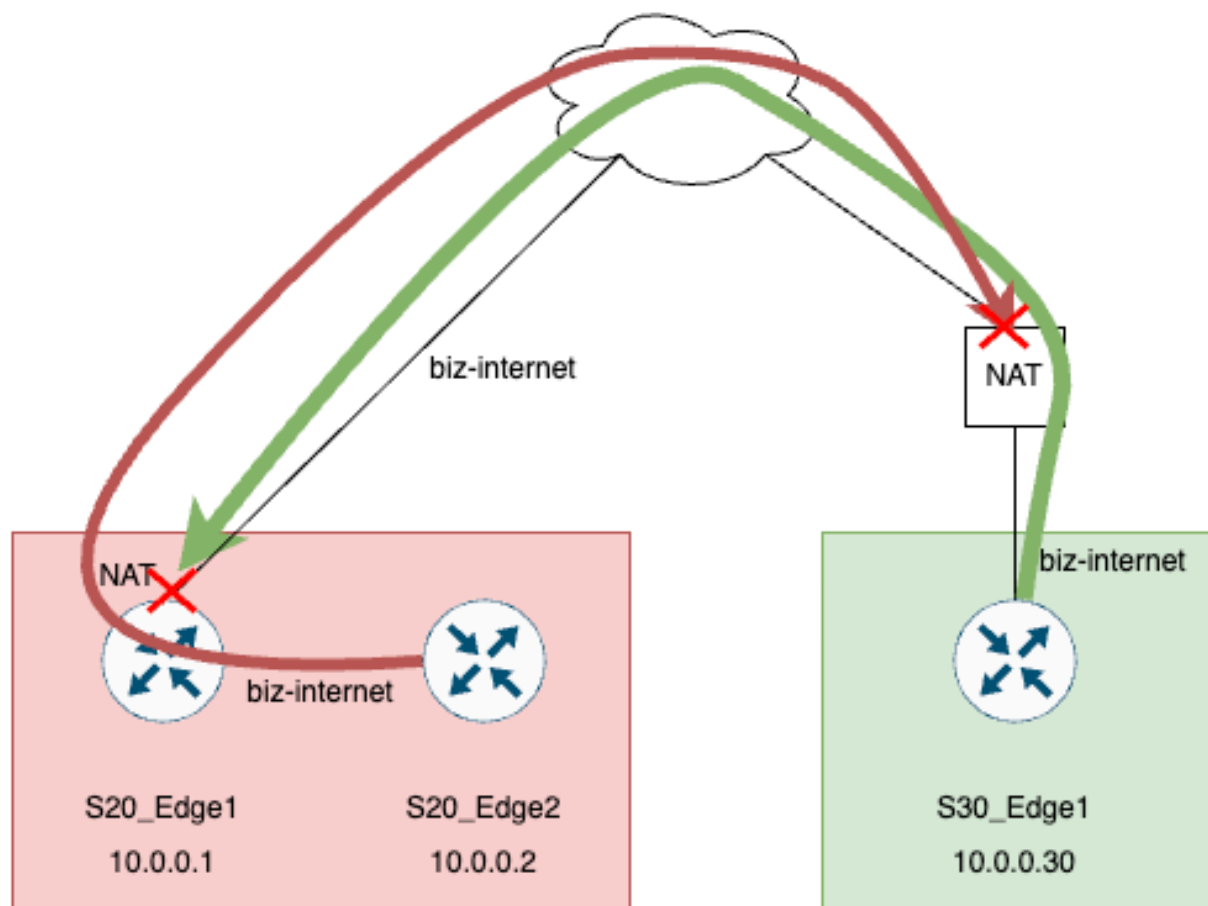
トポロジ

条件

1. S30_Edge1が対称NATの背後にある
2. S20_Edge2は、S20_Edge1がNATオーバーロード(PAT)を使用してEdge2からのフローをNATするTLOC拡張の背後にあります。

この結果、ピアからの不明なポートに対するセッションが存在しないため、対称NATデバイスとS20_Edge1でBFD helloがドロップされます。

S20_Edge1デバイスでは、これらのhelloパケットがNATテーブルのどのセッションとも一致しないため、これらのhelloパケットに対する暗黙的なACLドロップが示されます。



問題の特定

ステップ 1 : BFDセッションの確認

S30_Edge1のshow sdwan bfd sessions出力から、S20_Edge2、10.0.0.2へのBFDセッションがダウンしていることがわかります。

```
S30_Edge1#show sdwan bfd sessions
```

SYSTEM IP	SITE ID	STATE	SOURCE TLOC COLOR	REMOTE TLOC COLOR	SOURCE IP
10.0.0.2	20	down	biz-internet	biz-internet	192.168.30.2
10.0.0.1	20	up	biz-internet	biz-internet	192.168.30.2

ステップ 2 : NATタイプの確認

出力の下部では、NATタイプAがS30_Edge1に表示されています。これは対称NATを示しています。また、パブリックIP 172.16.1.34とポート31048にも注目してください。

```
S30_Edge1# show sdwan control local-properties
```

```
site-id          30
domain-id        1
protocol         dtls
tls-port         0
system-ip        10.0.0.30
```

```
NAT TYPE: E -- indicates End-point independent mapping
          A -- indicates Address-port dependent mapping
          N -- indicates Not learned
          Note: Requires minimum two vbonds to learn the NAT type
```

INTERFACE	PUBLIC IPv4	PUBLIC PORT	PRIVATE IPv4	PRIVATE IPv6
GigabitEthernet1	172.16.1.34	31048	192.168.30.2	::

ステップ 3 : NAT設定をチェックします

トポロジから、S20_Edge2がTLOC拡張の背後にあることがわかります。この時点で、S20_Edge1のPAT設定を確認できます。

S20_Edge1にはNATオーバーロードの設定がすでに存在します

```
S20_Edge1#sh run int gi1
interface GigabitEthernet1
 description biz-internet
 ip dhcp client default-router distance 1
 ip address 192.168.20.2 255.255.255.0
 no ip redirects
 ip nat outside
 load-interval 30
 negotiation auto
 arp timeout 1200
end
```

```
S20_Edge1#sh run | i nat
```

```
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet1 overload
```

ステップ 4 : パブリックIPとポートを確認します。

S20_Edge2でshow sdwan control local propertiesの出力を確認し、パブリックIPとポート172.16.1.18およびポート5063を確認します

```
S20_Edge2#show sdwan control local-properties
```

```
site-id          20
domain-id        1
protocol         dtls
tls-port         0
system-ip        10.0.0.2
```

```
NAT TYPE: E -- indicates End-point independent mapping
          A -- indicates Address-port dependent mapping
          N -- indicates Not learned
          Note: Requires minimum two vbonds to learn the NAT type
```

INTERFACE	PUBLIC IPv4	PUBLIC PORT	PRIVATE IPv4	PRIVATE IPv6
GigabitEthernet2.100	172.16.1.18	5063	192.168.100.2	::

ステップ 5 : NAT変換をチェックします

次に、S20_Edge1デバイスのNAT変換を確認します。S30_Edge1、IP 172.16.1.34、およびポート31048に対して、アドバタイズされたIPとポートへのNATセッションだけが存在します。対称NATについて知っていることを考慮すると、これは当てはまりません。異なるIPとポートの組み合わせでない場合は、31048とは少なくとも1つの異なるポートが必要です(12346のような標準の

SD-WANポートではありません)。

```
S20_Edge1#sh ip nat translations
Pro  Inside global      Inside local      Outside local     Outside global
udp  192.168.20.2:5063  192.168.100.2:12346  172.16.1.69:12346  172.16.1.69:12346
udp  192.168.20.2:5063  192.168.100.2:12346  172.16.0.102:12446  172.16.0.102:12446
udp  192.168.20.2:5063  192.168.100.2:12346  172.16.1.50:12346   172.16.1.50:12346
udp  192.168.20.2:5063  192.168.100.2:12346  172.16.0.202:12346  172.16.0.202:12346
udp  192.168.20.2:5063  192.168.100.2:12346  172.16.1.82:12346   172.16.1.82:12346
udp  192.168.20.2:5063  192.168.100.2:12346  172.16.1.34:31048   172.16.1.34:31048
udp  192.168.20.2:5063  192.168.100.2:12346  172.16.0.201:12346  172.16.0.201:12346
udp  192.168.20.2:5063  192.168.100.2:12346  172.16.0.101:12446  172.16.0.101:12446
udp  192.168.20.2:5063  192.168.100.2:12346  172.16.1.98:12346   172.16.1.98:12346
```

手順 6 : FIAトレースのチェック

FIAトレースを実行して、S20_Edge1でパケットがドロップされていることを確認します。IPはアドバタイズされたIPと同じではない場合がありますが、この場合は単純化するため、同じであることを注意してください。

```
S20_Edge1#debug platform condition ipv4 172.16.1.34/32 both
S20_Edge1#debug platform condition start
S20_Edge1#debug platform packet packet 1024 fia
S20_Edge1#debug platform packet packet 1024 fia-trace
S20_Edge1#show platform packet summary
Pkt   Input          Output          State  Reason
0     Gi2.100         Gi1             FWD
1     internal0/0/recycle:0  Gi1             FWD
2     Gi2.100         Gi1             FWD
3     internal0/0/recycle:0  Gi1             FWD
4     Gi2.100         Gi1             FWD
5     internal0/0/recycle:0  Gi1             FWD
6     Gi2.100         Gi1             FWD
7     internal0/0/recycle:0  Gi1             FWD
8     Gi1             Gi1             DROP   479 (SdwanImplicitAc1Drop)
```

パケット8をチェックして、これが疑わしいパケットかどうかを確認します。

```
S20_Edge1#show platform packet packet 8
Packet: 8          CBUG ID: 482
Summary
  Input       : GigabitEthernet1
  Output      : GigabitEthernet1
  State       : DROP 479 (SdwanImplicitAc1Drop)
Timestamp
  Start      : 6120860350139 ns (04/18/2025 02:35:03.873687 UTC)
  Stop       : 6120860374021 ns (04/18/2025 02:35:03.873710 UTC)
Path Trace
  Feature: IPV4(Input)
```

```
Input      : GigabitEthernet1
Output     :
```

```
Source      : 172.16.1.34
Destination : 192.168.20.2
Protocol    : 17 (UDP)
  SrcPort   : 3618
  DstPort   : 12346
```

これはS30_Edge1からのパケットのようです。

ステップ6でNATテーブルを再度チェックすると、このパケットにはセッションがないことがわかります。それがドロップの理由です。

手順 7 : BFDカウンタの確認

S20_Edge2からのBFDパケットはNATデバイス上のデバイスの外部にドロップされるため、S30_Edge1では認識されません。BFD Tx/Rxカウンタは、show sdwan tunnel statisticsコマンドで確認できます。

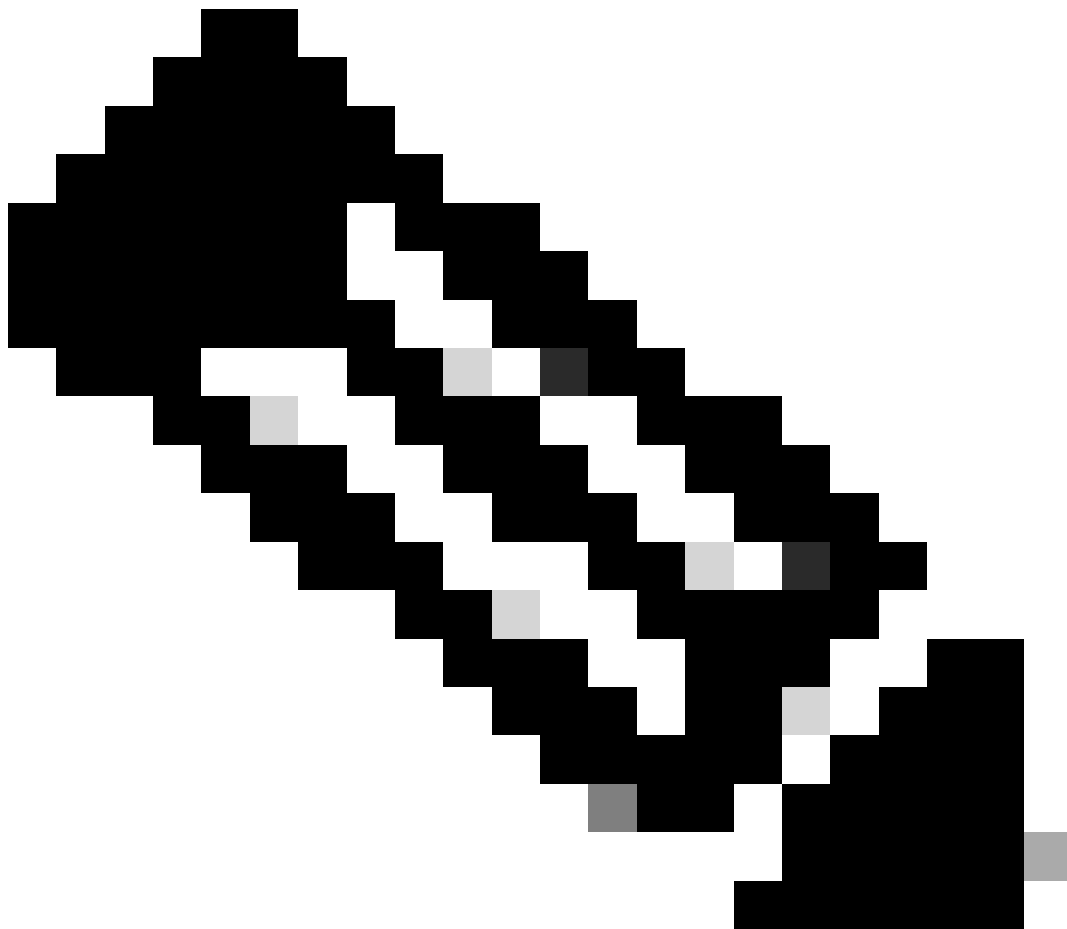
```
S30_Edge1#show sdwan tunnel statistics
tunnel stats ipsec 192.168.30.2 172.16.1.18 12346 12347
system-ip                10.0.0.2
local-color               biz-internet
remote-color              biz-internet
tunnel-mtu                 1438
tx_pkts                   10
tx_octets                  1060
rx_pkts                    0    <<<<<<<<<<<<
rx_octets                  0
tcp-mss-adjust            1358
ipv6_tx_pkts              0
ipv6_tx_octets             0
ipv6_rx_pkts              0
ipv6_rx_octets             0
tx_ipv4_mcast_pkts        0
tx_ipv4_mcast_octets      0
rx_ipv4_mcast_pkts        0
rx_ipv4_mcast_octets      0
tx_ipv6_mcast_pkts        0
tx_ipv6_mcast_octets      0
rx_ipv6_mcast_pkts        0
rx_ipv6_mcast_octets      0
```

解決方法

この問題を解決するには、S20_Edge1のNATオーバーロード(PAT)の上にスタティックNATを設定し、すべての制御パケットとBFDパケットを単一のIP/ポートの組み合わせにNAT変換します。

1. 最初に、この色でポートホッピングを無効にするか、S20_Edge2でシステム全体を無効にする必要があります。

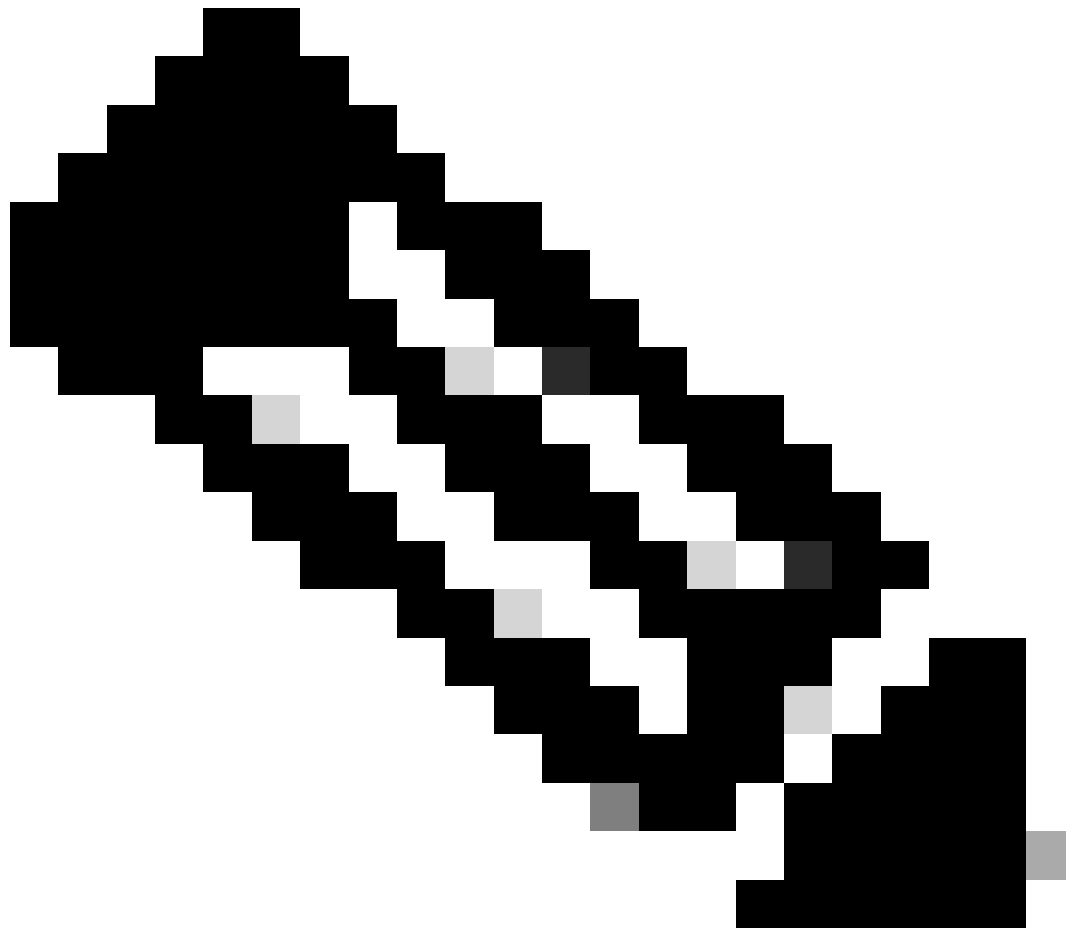
S20_Edge2のベストプラクティスとしてポートオフセットも追加されるため、S20_Edge1とS10_Edge2は制御接続またはBFDトンネルに同じ送信元ポートを使用しません。



注：この設定は、ルータのCLIまたはvManage CLIアドオンテンプレートを使用して実行できます。

```
S20_Edge2#config-t
S20_Edge2(config)# system
S20_Edge2(config-system)# no port-hop
```

```
S20_Edge2(config-system)# port-offset 1
S20_Edge2(config-system)# commit
```



注:show sdwan control local-propertiesをチェックして、この設定後にS20_Edge2がベースポート12347を使用していることを確認してください。ベースポートを使用していない場合は、clear sdwan control port-indexコマンドを使用してポートをベースポートにリセットします。これにより、ポートが上位のポートで実行されている場合にポートが変更されず、後でリブートします。clearコマンドは、制御接続とbfdトンネルをリセットします。

2. S20_Edge1にスタティックNATを設定する。

```
S20_Edge1#config-t
S20_Edge1(config)# ip nat inside source static udp 192.168.100.2 12347 192.168.20.2 12347 egress-interface
S20_Edge1(config)# commit
```

3. S20_Edge1のNAT変換をクリアします。

```
S20_Edge1#clear ip nat translation *
```

検証

1. ピアの1つでBFDセッションを確認します。

```
S30_Edge1#show sdwan bfd sessions
```

SYSTEM IP	SITE ID	STATE	SOURCE TLOC COLOR	REMOTE TLOC COLOR	SOURCE IP
10.0.0.2	20	up	biz-internet	biz-internet	192.168.30.2

2. S20_Edge1のNATセッションを確認します。

```
S20_Edge1#sh ip nat translations
```

Pro	Inside global	Inside local	Outside local	Outside global
udp	192.168.20.2:12347	192.168.100.2:12347	---	---
udp	192.168.20.2:12347	192.168.100.2:12347	172.16.0.202:12346	172.16.0.202:12346
udp	192.168.20.2:12347	192.168.100.2:12347	172.16.1.50:12346	172.16.1.50:12346
udp	192.168.20.2:12347	192.168.100.2:12347	172.16.0.102:12446	172.16.0.102:12446
udp	192.168.20.2:12347	192.168.100.2:12347	172.16.1.34:50890	172.16.1.34:50890
udp	192.168.20.2:12347	192.168.100.2:12347	172.16.1.69:12346	172.16.1.69:12346
udp	192.168.20.2:12347	192.168.100.2:12347	172.16.1.98:12346	172.16.1.98:12346
udp	192.168.20.2:12347	192.168.100.2:12347	172.16.0.101:12446	172.16.0.101:12446
udp	192.168.20.2:12347	192.168.100.2:12347	172.16.0.201:12346	172.16.0.201:12346
udp	192.168.20.2:12347	192.168.100.2:12347	172.16.1.82:12346	172.16.1.82:12346
udp	192.168.20.2:12347	192.168.100.2:12347	172.16.0.1:13046	172.16.0.1:13046
Total number of translations: 11				

すべての制御接続とBFDトンネルが、設定されたIPとポート192.168.20.2:12347に対してNATされていることが確認できます。また、172.16.1.34への接続は、S30_Edge1によってvSmartにアドバタイズされたポートとはまったく異なるポートに対する接続です。ポート50890を参照。

3. S30_Edge1からのshow sdwan control local propertiesの出力で、アドバタイズされたIPとポートが172.16.1.34とポート60506であることに注意してください。

```
S30_Edge1#show sdwan control local-properties
```

```
site-id          30
domain-id        1
protocol         dtls
tls-port         0
system-ip        10.0.0.30
```

NAT TYPE: E -- indicates End-point independent mapping
A -- indicates Address-port dependent mapping
N -- indicates Not learned
Note: Requires minimum two vbonds to learn the NAT type

INTERFACE	PUBLIC IPv4	PUBLIC PORT	PRIVATE IPv4	PRIVATE IPv6

GigabitEthernet1	172.16.1.34	60506	192.168.30.2	::

参考資料

[Cisco Catalyst SD-WAN設計ガイド](#)

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。