Catalyst SD-WANセキュリティアドバイザリの修正 – 2026年5月

内容

はじめに

このドキュメントでは、2026年5月14日付けのPSIRTアドバイザリに基づいて、SD-WANの重要なセキュリティ脆弱性を特定して修正する手順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。

- Cisco Catalyst SD-WANアーキテクチャおよび制御コンポーネント(vManage、vSmart、vBond)
- Cisco Catalyst SD-WANのアップグレード手順
- Cisco TAC Case ManagementおよびAdmin-Tech収集手順

使用するコンポーネント

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たものです。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。

バックグラウンド情報

詳細な背景情報と最新のアップデートについては、PSIRTの公式アドバイザリページを参照してください。

これらのアドバイザリは、次のリンクから入手できます。

- Cisco Catalyst SD-WAN コントローラの認証バイパスの脆弱性
- Cisco Catalyst SD-WAN の脆弱性

これらの不具合は、次のPSIRTアドバイザリで対処されています。

- Cisco Bug ID CSCwt50498
- Cisco Bug ID CSCwt38739
- Cisco Bug ID CSCwt38767
- Cisco Bug ID CSCwt55544

是正ワークフローの概要

注：すべてのSD-WANコントローラおよびマネージャに脆弱性が存在するため、すべてのコントロールコンポーネントを即座にアップグレードする必要があります。ただし、すべてのコントローラがセキュリティ侵害の証拠を示すわけではありません。

必要な処置：管理手順を収集し、修正済みリリースにアップグレードしてから、Cisco TACケースをオープンします。これにより、TACは管理手順をスキャンして、セキュリティ侵害の痕跡を検出できます。

TACは次のユーザが利用できます。

- セキュリティ侵害の指標に関して提供した管理テクノロジーをスキャンする
- アップグレード中に問題が発生した場合は、アップグレードサポートを提供します
- セキュリティ侵害の指標が特定された場合は、追加の修復方法を案内します。

1. Admin-Techsの収集:診断データが失われないように、アップグレードの前にすべての制御コンポーネント(vSmart、vManage、vBond)でadmin-techを実行します。 Log and Tech optionsを選択します。 コアは必要ありません。

   

注意:vSmart admin-techsは同時に実行しないでください。一度に1つずつ実行してください。その他の情報は、任意の順序で収集できます

2. 修正済みリリースへのアップグレード：すべてのSD-WAN制御コンポーネント(vManage、vSmart、vBond)を、修正済みソフトウェアバージョンの表に記載されている修正済みソフトウェアバージョンにアップグレードします。

注:TACスキャン結果を待たずにアップグレードを実行してください。修正済みリリースへのアップグレードは最も優先度が高く、この脆弱性を解消します。 ステップ3のTACスキャンで、アップグレード後にさらなるアクションが必要かどうかが判断されます。

3. TACケースを開き、セキュリティ侵害の指標をスキャンするAdmin-Techをアップロードする:Cisco TACケースを開き、ステップ1で収集したすべてのAdmin-Techログバンドルをアップロードします。TACは管理テクノロジーをスキャンして、セキュリティ侵害の痕跡を検出します。
4. セキュリティ侵害が特定された場合はTACガイダンスに従う:TACがお客様の環境でセキュリティ侵害の指標を特定した場合は、TACが提供するすべての修復ガイダンスに従います。セキュリティ侵害の兆候が見つからない場合は、アップグレード以外のアクションは必要ありません。

ステップ1：すべての制御コンポーネントからAdmin-Techファイルを収集します

必須：診断データが失われないように、アップグレードの前にすべての制御コンポーネントからadmin-techファイルを収集します。これらのファイルは、TACがステップ3で環境をスキャンして侵害の痕跡を検出するために使用されます。

コレクション：

注:admin-tech生成の場合は、LogおよびTechオプションを選択します。 コアは必要ありません。

1. すべてのコントローラ(vSmarts)でadmin-techを実行します。これらを同時に実行しないでください。1つずつ収集します。
2. すべてのマネージャ(vManages)でadmin-techを実行します。
3. すべてのバリデータ(vBond)でadmin-techを実行します。

注:vSmart admin-techsは同時に実行しないでください。一度に1つずつ収集します。マネージャおよびバリデータのAdmin-techsは、任意の順序で収集できます。

SD-WAN環境でのAdmin-Techの収集とTACケースへのアップロード

注:TACはこれらのファイルを分析して、お客様の環境に侵入の痕跡がないか評価し、適切な修復パスを指示します。

代替：手動検証（Admin-Techを収集できない場合のみ）

admin-techファイルを共有できない場合は、手動の検証手順を使用できます。これらの手順は、文書化してTACと共有する必要がある暫定的な指標を提供します。

詳細な手順については、このドキュメントの最後にある「手動確認手順」のセクションを参照してください。調査結果をすべて文書化し、サポート案件でTACに提供します。

ステップ2：修正済みソフトウェアバージョンへのアップグレード

ステップ1でアドミニストレーションテクノロジーを収集した後、すべてのSD-WAN制御コンポーネント（vManage、vSmart、およびvBond）を修正済みのソフトウェアバージョンにアップグレードします。

重要:TACスキャン結果を待たずにアップグレードを実行してください。修正済みリリースへのアップグレードは最も優先度が高く、この脆弱性を解消します。ステップ3のTACスキャンで、アップグレード後にさらにアクションが必要かどうかが判断されます。

このドキュメントの「修正済みソフトウェアバージョン」の表から適切なバージョンを選択します。

警告：アップグレードは現在のメジャーリリースの範囲内で行う必要があります。TACのガイダンスがない場合は、上位のメジャーリリースにアップグレードしないでください。

vManage GUIまたはCLIを使用したSD-WANコントローラのアップグレード

注：アップグレード中に問題が発生した場合は、TACサービスリクエストをオープンしてアップグレードサポートを受けてください。

ステップ3:TACケースを開き、スキャン用のAdmin-Techファイルをアップロードする

ステップ2でアップグレードを行った後、Cisco TACサポートケースをオープンし、ステップ1で収集したadmin-techファイルをアップロードします。TACは管理テクノロジーをスキャンして、セキュリティ侵害の痕跡を検出します。

必要なアクション：

1. 「CVE-2026-20182」とタイトルに関連するPSIRT IDを含む重大度3 TACケースをオープンし、スキャニングプロセスを開始します。
2. ステップ1で収集したすべてのadmin-techログバンドル（コントローラ、マネージャ、およびバリデータ）をアップロードします。
3. TACがスキャンを完了し、結果を通知するのを待ちます

注:TACはadmin-techファイルを分析し、スキャンの結果を通知します。セキュリティ侵害の兆候が見つからない場合は、アップグレード以外のアクションは必要ありません。

ステップ4：セキュリティ侵害が特定された場合：TACのガイダンスに従う

お客様の環境におけるセキュリティ侵害の痕跡がTACによって特定されると、TACから具体的な修復ガイダンスが提供されます。TACが提供するすべての指示に従ってください。

侵害の兆候が見られない場合は、ステップ2で完了したアップグレードで十分であり、それ以上の修復は必要ありません。

修正済みソフトウェアバージョン

次のソフトウェアリリースには、特定された脆弱性に対する修正が含まれています。

現在のバージョンに適用	修正済みバージョン	利用可能なソフトウェア
20.3、20.6、20.9	20.9.9.1	20.9.9.1 vManage、vSmart、およびvBondのアップグレードイメージ
20.12の20.10、20.11、20.12.5以前	20.12.5.4	20.12.5.4 vManage、vSmart、およびvBondのアップグレードイメージ
20.12.6.x	20.12.6.2	20.12.6.2 vManage、vSmart、およびvBondのアップグレードイメージ

現在のバージョンに適用	修正済みバージョン	利用可能なソフトウェア
20.12.7	20.12.7.1	20.12.7.1 vManage、vSmart、およびvBondのアップグレードイメージ
20.15の20.13、20.14、20.15.4.3以前	20.15.4.4	20.15.4.4 vManage、vSmart、およびvBondのアップグレードイメージ
20.15.5.x	20.15.5.2	20.15.5.2 vManage、vSmart、およびvBondのアップグレードイメージ
20.16、20.17、20.18.x	20.18.2.2	20.18.2.2 vManage、vSmart、およびvBondのアップグレードイメージ

注：SD-WAN Cloud（旧称Cloud Delivered Cisco Catalyst SD-WAN [CDC]）をご使用のお客様も、20.15.506は修正済みのリリースです。これは特にシスコがホストするクラスタの導入に適用され、標準のアップグレードパスとは別に処理されます。そのようなお客様はすべて、すでに修正済みリリース20.15.506にアップグレードされています。

重要な参考資料

- アップグレードマトリックス
- コントローラ互換性マトリクス

付録：手動による検証手順（Admin-Tech収集ができない場合のみ）

注:Admin-tech収集が推奨される方法です。admin-techファイルの収集と共有が絶対に不可能な場合は、手動検証のみを使用してください。admin-techファイルを収集できない場合は、次の手動の手順を使用してTACの暫定的なインジケータを収集します。

注：

- これらの手順では、暫定データのみが提供されます
- 正確な評価には、admin-techの収集を強く推奨
- 結果を文書化し、サポートケースでTACと共有します。
- TACが正式な評価を決定

要件：これらの手順は、すべての制御コンポーネントで実行する必要があります。

検証1：認証ログでの不正なSSHログインのチェック

ステップ1：有効なvManageシステムIPの特定

各vSmartコントローラにアクセスし、次を実行します。

```
west-vsmart# show control connections | inc "vmanage|PEER|IP"
```

出力例：

```
                                                PEER
      PEER  PEER  PEER            SITE       DOMAIN  PRIV    PEER                                    PUB
INDEX TYPE  PROT  SYSTEM IP       ID         ID      PRIVATE IP                        PORT    PUBLIC I
-----------------------------------------------------------------------------------------------------------
0     vmanage dtls 10.1.0.18     101018     0       10.1.10.18                        12346   10.1.10.1
```

ステップ2：正規表現文字列の構築（vBondおよびvSmartのみ）

ステップ1のすべてのシステムIPをOR正規表現パターンに結合します。

```
system-ip1|system-ip2|...|system-ipn
```

ステップ2b:vManageシステムの追加ステップ

vManage自体でこれらのコマンドを実行する場合は、localhost IP(127.0.0.1)、ローカルシステムIP、すべてのクラスタIP、およびVPN 0トランスポートインターフェイスIPを正規表現に追加します。

```
system-ip1|system-ip2|...|system-ipn|127.0.0.1|
```

ローカルvManageシステムIPを検索するには、次のコマンドを使用します。

```
show control local-properties
```

VPN 0トランスポートインターフェイスIPとクラスタIPを見つけるには、次のコマンドを使用します。

```
show interface | tab
```

ステップ3：検証コマンドの実行

次のコマンドを実行して、REGEXをステップ2で得た正規表現の文字列に置き換えます。

```
west-vsmart# vs
west-vsmart:~$ zgrep "Accepted publickey for vmanage-admin from " /var/log/auth.log* | grep -vE "\s(REG
```

注：このコマンドは、予期しないソースからのvmanage-adminログインだけを表示するように認証ログをフィルタリングします。正規のログインは、vManage関連のIPからのみ発信される必要があります。

ステップ4：結果の解釈とTACのドキュメント

出力が表示されない場合は、次の手順を実行します。

- このデバイスでは侵入の痕跡は検出されない
- この結果をTACケースに文書化します。
- 残りのコントローラの評価を続行

ログ行が出力される場合：

- 示されている各IPアドレスを注意深く調べる
- IPがvManageインフラストラクチャ（クラスタIP、古いシステムIPなど）に関連していないことを確認します。
- 送信元IPが正当なものであると特定できない場合、侵害の潜在的なインジケータを示している可能性があります
- ログエントリには、タイムスタンプと送信元IPアドレスが表示されます
- すべての調査結果を文書化し、TACサービスリクエストを直ちにオープンする
- ケースにログエントリ、タイムスタンプ、および送信元IPを含めます
- TACが公式評価の決定を行う

検証2：コントローラのsyslogで不正なピア接続をチェックする

このコマンドは、コントローラのsyslogファイルからすべてのピアタイプとピアシステムのipのペアを抽出し、確認できるようにリストとして出力します。疑わしいエントリに自動的にフラグが設定されることはありません。出力を調べて、各ピアシステムIPがSD-WANインフラストラクチャの既知の正当な部分かどうかを判断する必要があります。すべてのコントロールコンポーネント（コントローラ、マネージャ、およびバリデータ）でこれを実行します。

ステップ1：各制御コンポーネントでコマンドを実行します。

まず、vshellにアクセスし、ログディレクトリに移動します。

```
vs
cd /var/log
```

次に、次のコマンドを実行してvsyslog*ファイルglobを検索します。

```
awk '{
  match($0, /peer-type:([a-zA-Z0-9]+)[^ ]* peer-system-ip:([0-9.:]+)/, arr);
  if(arr[1] && arr[2]) print "(" arr[1] ", " arr[2] ")";
}' vsyslog* | sort | uniq
```

messages*ファイルglobとvdebug*ファイルglobに対してこれを繰り返します。

ステップ2：結果の解釈とTACへのドキュメントの提出

出力に既知のvManage/vSmart/vBondシステムIPのみが表示される場合：

- このチェックではセキュリティ侵害の兆候は検出されませんでした
- この結果をTACケースに文書化します。
- 残りの制御コンポーネントの評価を続行する

出力に認識されないピアシステムIPが含まれている場合：

- 示されている各IPアドレスとピアタイプを注意深く調べます
- IPが既知のSD-WANコントロールプレーンインフラストラクチャに関連していないことを確認します。
- 送信元IPが正当なものであると特定できない場合、侵害の潜在的なインジケータを示している可能性があります
- すべての調査結果を文書化し、TACサービスリクエストを直ちにオープンする
- この場合は、ピアタイプとピアシステムIPペアを指定してフルコマンド出力を含めてください
- TACが公式評価の決定を行う

検証3：アクティブなコントロール接続に存在しないchallenge-ackがないかどうかを確認する

このチェックは、control connections detailの出力を検査して、アクティブとして報告された（または最近解除された）ピアセッションで、予期されるchallenge-ack交換が欠落しているかどうかを調べます。両方向でhelloパケットを交換し、TxまたはRx統計情報でchallenge-ack 0が示されるセッションは、ピアが予期されるチャレンジハンドシェイクを完了しなかったことを示します。これは、調査を必要とする異常です。すべてのコントロールコンポーネント（コントローラ、マネージャ、およびバリデータ）でこれを実行します。

ステップ1：制御接続の詳細出力を収集します

デバイスのCLIで、次のコマンドを実行します。

```
show control connections detail
show control connections-history detail
```

検査用のファイル(vdaemon.txtなど)に出力を保存します。

ステップ2：確認する内容

(REMOTE-COLOR-/SYSTEM-IP-ヘッダーで区切られた)ピアレコードごとに、次の条件すべてに当てはまる場合は、そのレコードにフラグを付けます。

- セッションの状態がUPまたはTEAR_DOWN
- Tx Statistics helloカウンタとRx Statistics helloカウンタは両方ともゼロ以外です（helloは両方向に流れています）
- challenge-ackがTx Statistics（tx統計）ブロックまたはRx Statisticsブロック（あるいはその両方）で0になっている。

一致するレコードの例(欠落しているchallenge-ackを強調表示する<<<<の矢印に注意)

```
-----------------------------------------------------------------------------------------------
 REMOTE-COLOR- default SYSTEM-IP- 10.2.2.2   PEER-PERSONALITY- vmanage
-----------------------------------------------------------------------------------------------
site-id             432567
domain-id           0
protocol            dtls
private-ip          10.0.0.1
private-port        12346
public-ip           192.168.1.1
public-port         50825
state               up [Local Err: NO_ERROR] [Remote Err: NO_ERROR]
uptime              0:00:16:58
hello interval      1000
hello tolerance     12000

  Tx Statistics-
  --------------
    hello                   3423293
    challenge               1
    challenge-response      0
    challenge-ack           0           <<<< MISSING challenge-ack (Tx)
```

```
   ...

  Rx Statistics-
  --------------
    hello                   3423291
    challenge               0
    challenge-response      1
    challenge-ack           0           <<<< MISSING challenge-ack (Rx)
    ...
```

上記の例では、TxとRxの両方のhelloカウンタはゼロ以外（アクティブ接続）ですが、両方向でchallenge-ackが0になっています。

ステップ3：手動検索コマンド

保存されたvdaemon.txt(またはshow control connections detailの出力が含まれている任意のファイル)から候補レコードをすばやく表示するには、次のコマンドを実行します。

```
grep -A20 'SYSTEM-IP' vdaemon.txt | grep -B5 'challenge-ack  0'
```

返される各ブロックは、challenge-ackが0として報告されるピアセッションを表します。各ブロックを完全に調べて、stateがupまたはtear_downであること、およびTxとRxの両方のhelloカウンタがゼロ以外であることを確認してから、ヒットとして扱います。

ステップ4：結果の解釈とTACのドキュメント

3つの条件をすべて満たすレコードがない場合：

- このチェックではセキュリティ侵害の兆候は検出されませんでした
- この結果をTACケースに文書化します。
- 残りの制御コンポーネントの評価を続行する

1つ以上のレコードが3つの条件をすべて満たしている場合：

- フラグが設定された各レコードのSYSTEM-IP-、private-ip、およびpublic-ipの値を注意深く調べます
- ピアがSD-WANコントロールプレーンの既知の正当な部分（クラスタメンバー、DRサイト、以前にコンポーネントに割り当てられたIPアドレス）ではないことを確認します。
- ピアを正当なものとして識別できない場合、侵害の潜在的な兆候を示している可能性があります
- すべての調査結果を文書化し、TACサービスリクエストを直ちにオープンする
- 完全に一致するピアレコードとsourceコマンドの出力をケースに含めます
- TACが公式評価の決定を行う

FAQ

Q：このセキュリティアドバイザリに対処するための最初のステップは何ですか。

A：すべてのコントロールコンポーネントからadmin-techファイルを収集し、すべてのコントロールコンポーネントを修正済みのソフトウェアバージョンにアップグレードします。アップグレードが完了したら、TACケースを開き、管理手順をアップロードします。これにより、TACが環境をスキャンして侵害の痕跡を検出できます。

Q.どのバージョンにアップグレードする必要がありますか。

A.できるだけ早い段階で、最も近い修正済みバージョンにアップグレードしてください。

Q：すべての制御コンポーネントからadmin-techsを収集する必要がありますか。

A：はい。TACが環境を適切に評価するには、すべてのコントローラ（vSmart、1つずつ収集）、すべてのマネージャ(vManage)、およびすべてのバリデータ(vBond)のadmin-techファイルが必要です。

Q:TACはシステムが侵害されたかどうかを判断する方法を教えてください。

A:TACは、専用ツールを使用してアドミンテクノロジーファイルを分析し、侵害の痕跡がないか環境を評価します。

Q:TACツールを使用して独自の自動スキャンを実行する方法はありますか。

A：コントロールコンポーネントからadmin-techsを再スキャンするために、お客様はセルフサービスの「Check Bug Applicability」ツール(Cisco Bug ID CSCwt50498のBug Search Toolページに組み込まれている)を使用することもできます。

Q：セキュリティ侵害の兆候が見つかった場合、どうなりますか。

A:TACから連絡があり、お客様の環境に固有の次のステップとガイダンスについて話し合います。シスコがユーザに代わって修復を実行することはありません。TACは、ユーザが作業を進めるために必要なガイダンスを提供します。

Q：使用する修正済みソフトウェアのバージョンを知るにはどうすればよいのですか。

A：このドキュメントの「修正済みソフトウェアバージョン」の表を参照してください。ご使用の環境に適したバージョンのTACの確認

Q:TACが管理技術者を分析する前に、アップグレードを開始できますか。

A：はい。管理手順を収集し、修正済みリリースにアップグレードしてからTACケースをオープンします。これにより、TACは管理手順をスキャンして侵害の痕跡を検出できます。

Q：修復中にダウンタイムが発生する可能性はありますか。

A：影響は、導入アーキテクチャと修復パスによって異なります。TACは、プロセス中のサービスへの影響を最小限に抑えるためのガイダンスを提供します。

Q：セキュリティ侵害の兆候が見つからない場合、すべてのコントローラをアップグレードする必要がありますか。

A：はい。すべてのSD-WAN制御コンポーネント（vManage、vSmart、およびvBond）を修正済みのソフトウェアバージョンにアップグレードする必要があります。コントローラのサブセットのみをアップグレードするだけでは不十分です。

Q：クラウドホスト型のSD-WANオーバーレイを所有しています。アップグレードにはどのようなオプションがありますか。

A：クラウドホステッドオーバーレイでは、次の2つのオプションがあります。

1. SSP > Overlay Details > Change Windowsの順に選択して、環境の自動アップグレードがスケジュールされているかどうかを確認します。
2. スケジュールされたアップグレードを待機しない場合は、次の2つのオプションがあります。
    - このドキュメントで入手できるアップグレードガイドを使用して、自分でアップグレードしてください。
    - 希望するメンテナンスウィンドウでスタンバイTACケースをオープンします。アップグレードで問題が発生した場合は、TACを利用できます。

Q：エッジルータもアップグレードする必要がありますか。

A：いいえ。Cisco IOS XEデバイスは、このアドバイザリの影響を受けません。

Q：シスコのホステッドオーバーレイです。ACLを修正するか、SSPでアクションを実行する必要がありますか。

A：シスコがホストするすべてのカスタマーは、SSPで確認できる独自のAllowed Inbound Rulesを確認し、こちら側の必要なプレフィックスのみが許可されていることを確認することをお勧めします。これらのルールは管理アクセス専用であり、エッジルータには適用されません。SSP > Overlay Details > Allow Inbound rulesで確認してください。シスコが外部からクラウドホステッドコントローラにプロビジョニングするDay 0では、ポート22および830がデフォルトで常にブロックされていることに注意してください。

Q：現在、SD-WANクラウド（旧称Cloud Delivered Cisco Catalyst SD-WAN [CDC]）を使用しています。 どのバージョンにアップグレードしますか？

A：現在のバージョンに基づいて、SD-WANクラウドクラスタは現在アップグレードの予定が入っているか、すでに修正済みバージョンにアップグレードされています。SD-WANクラウド（旧称CDCS）の修正済みリリースを次に示します。

1. Early Adopter Clusters = 20.18.2.2（これは実際には標準リリースと同じです）

2. 推奨リリースクラスタ= 20.15.506（PSIRT修正を含むCDCS固有バージョン）

SD-WANクラウドのお客様は、このPSIRTに対処するために効果的な措置を取る必要はありません。

Q:共有テナントがあります。どのバージョンにアップグレードしますか？

A：現在のバージョンに基づいて、共有テナントは現在アップグレードの予定が入っているか、

すでに修正済みバージョンにアップグレードされています。共有テナントの修正済みリリースを次に示します。

1. 推奨リリースクラスタ= 20.15.5.2

Q:Cisco TACでは、これらの脆弱性に対するフォレンジック分析や調査サービスを提供していますか。

A:Cisco TACでは、これらの脆弱性に関連するIndicators of Compromise(IoC)をスキャンすることで、お客様を支援できます。ただし、TACは詳細なフォレンジック分析やインシデント調査を実行しません。包括的なフォレンジック調査や詳細なセキュリティ調査を行うには、お客様が希望するサードパーティのインシデント対応(IR)会社に協力を依頼することをお勧めします。

Q: SD-WANオーバーレイの脆弱性を軽減するための一般的なベストプラクティスまたは方法を教えてください。

A: SD-WANオーバーレイの脆弱性を軽減するためのベストプラクティスと推奨事項については、『Cisco Catalyst SD-WAN強化ガイド』を参照してください。

Q：システム上の「root」ユーザのログが表示されます。 何か問題でも？

A：その時点でシステムで他に何が起こっているかを確認します。 これらのログは完全に予想できます。 たとえば、admin-techsが生成されると、「root」ユーザからのsystem-login-change口グが表示されます。 リブート中に「root」ユーザから口グを確認することもできます。

```
Feb 28 23:03:44 Manager01 SYSMGR[863]: %Viptela-Manager01-sysmgrd-6-INFO-1400002: Notification: system-

       user-name:"root" user-id:245  generated-at:2-28-2026T23:3:44

Feb 28 23:03:47 Manager01 SYSMGR[863]: %Viptela-Manager01-sysmgrd-6-INFO-1400002: Notification: system-

        user-name:"root" user-id:248  generated-at:2-28-2026T23:3:47
```

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。