Solaris cachefsデーモンのヒープオーバーフロー

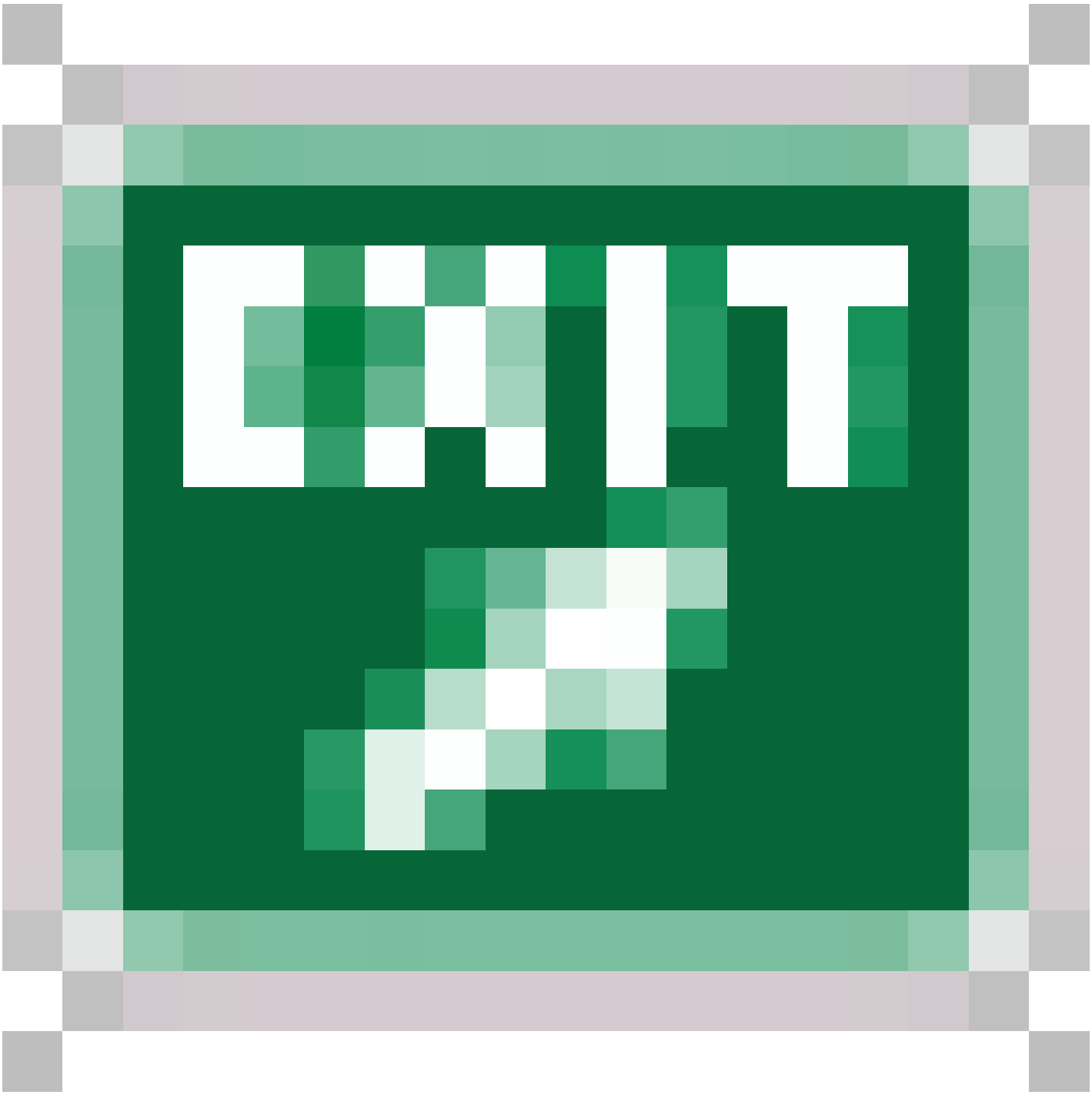
アドバイザリーID : cisco-sa-20020724-solaris-cachefs
初公開日 : 2002-07-24 16:00
バージョン 1.1 : Final
回避策 : No Workarounds available
Cisco バグ ID :

CVE-2003-1063
CVE-2002-0085
CVE-2002-0084
CVE-2002-0033

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

このアドバイザリでは、Solarisオペレーティングシステムにインストールされているシスコの製品およびアプリケーションに影響を与える脆弱性について説明します。このアドバイザリは、Solarisオペレーティングシステム内の共通サービスに基づくもので、シスコの製品またはアプリケーションの不具合に起因するものではありません。「cachefs」プログラムの脆弱性により、攻撃者がSolaris OSで任意のコードを実行できることが判明しました。この脆弱性は、CERT Advisory CA-2002-11で公開されました。Solaris OSにインストールされているすべてのシスコ製品およびアプリケーションは、回避策が適用されていない限り、基盤となるオペレーティングシステムの脆弱性に対して脆弱であると見なされます。この脆弱性の詳細については、http://sunsolve.sun.com/search/document.do?assetkey=1-26-44309-1のSun(sm) Alert Notificationを参照してくだ



さい。

脆弱性が存在する他のシスコ製品はありません。

Sunはパッチを開発中です。パッチがリリースされるまで、該当するすべてのユーザは「回避策」セクションで説明されている回避策を適用することを推奨いたします。

このアドバイザリは、
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20020724-solaris-cachefsで確認できます。

該当製品

このセクションには、該当製品に関する詳細が掲載されています。

脆弱性のある製品

次のSolarisリリースに基づくすべての製品が影響を受けます。

- Solaris 2.5.1
- Solaris 2.6
- Solaris 7
- Solaris 8

次の製品が影響を受けます。

- Media Gateway Controller (MGC) および関連製品
  - Solaris 2.5.1で稼働している製品には、CSCOh013.pkgリリース1.0(9)以降がインストールされていない限り、脆弱性が存在します。このバージョンのSolarisに基づく製品は、シグナリングコントローラ2200 (SC2200)です。
  - Solaris 2.6で稼働している製品には、CSCOh013.pkgリリース1.0(9)以降がインストールされていない限り、脆弱性が存在します。Solaris 8で稼働している製品には、CSCOh013.pkgリリース2.0(2)以降がインストールされていない限り、脆弱性が存在します。これらのバージョンのSolarisに基づく製品は次のとおりです。
    - SC2200
    - Cisco仮想スイッチコントローラ(VSC3000)
    - Cisco PGW2200公衆電話交換網(PSTN)ゲートウェイ
    - Cisco Billing and Management Server(BAMS)
    - Cisco Voice Services Provisioning Tool(VSPT)
- Cisco Element Management Framework(CEMF)および関連製品
  CEMFのすべてのリリースに脆弱性が存在します。関連製品は次のとおりです。
  - Cisco 12000マネージャ
  - Cisco DSLマネージャ
  - Cisco 7200および7400シリーズルータ用Element Managerソフトウェア
  - Catalyst 6500シリーズおよびCisco 7600シリーズルータ用Element Managerソフトウェア
  - ユニバーサルゲートウェイマネージャ
  - Cisco Cable Manager
  - Ciscoメディアゲートウェイマネージャ
  - Cisco MGC（メディアゲートウェイコントローラ）ノードマネージャ
- Cisco IPマネージャ
  All releases.
- Cisco Secure ACS for UNIX（登録ユーザ専用）

All releases.

脆弱性を含んでいないことが確認された製品

次の製品は影響を受けません。

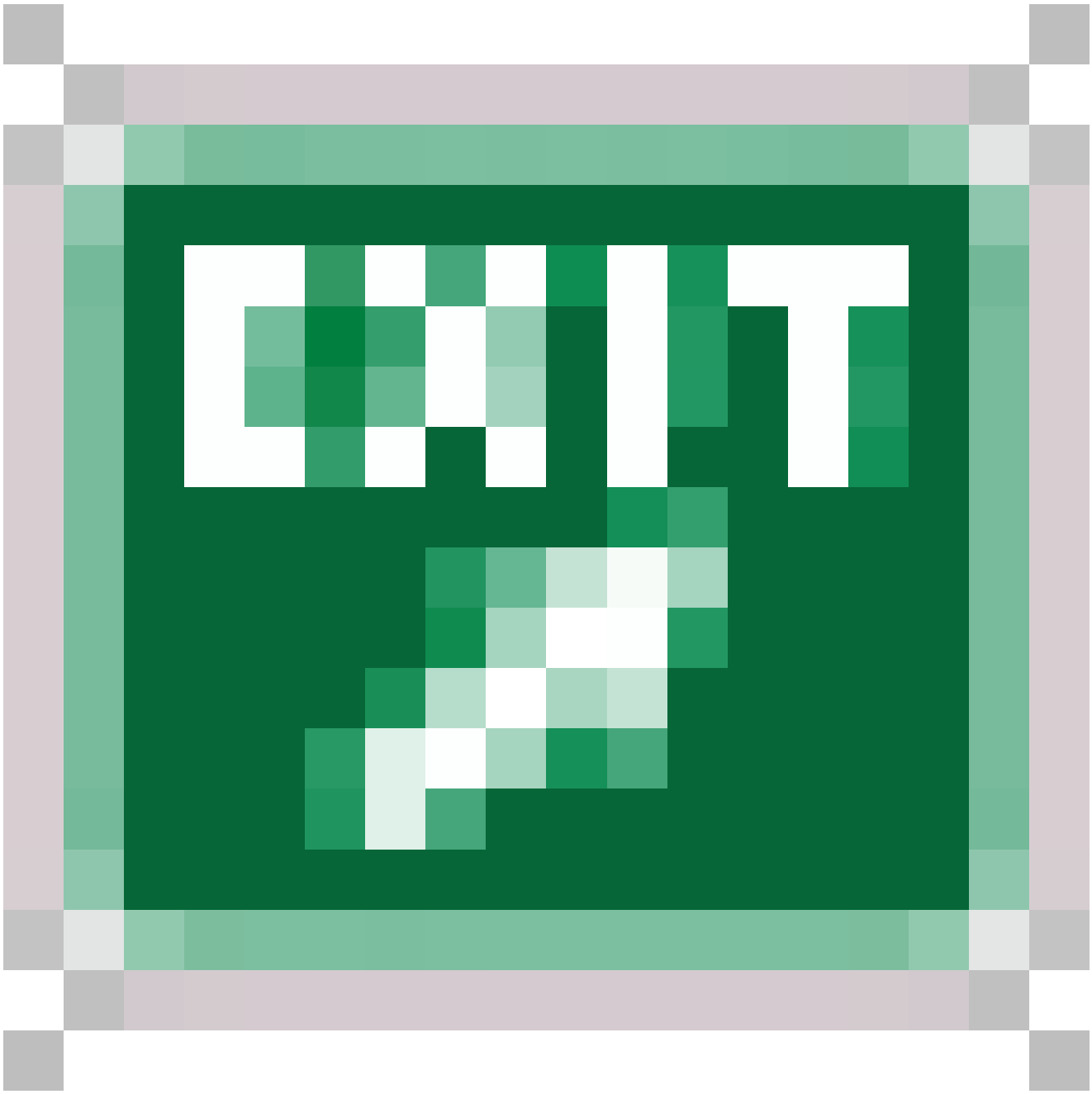
- 0.BTS10200
- Cisco IDS

他のシスコ製品においてこのアドバイザリの影響を受けるものは、現在確認されていません。

詳細

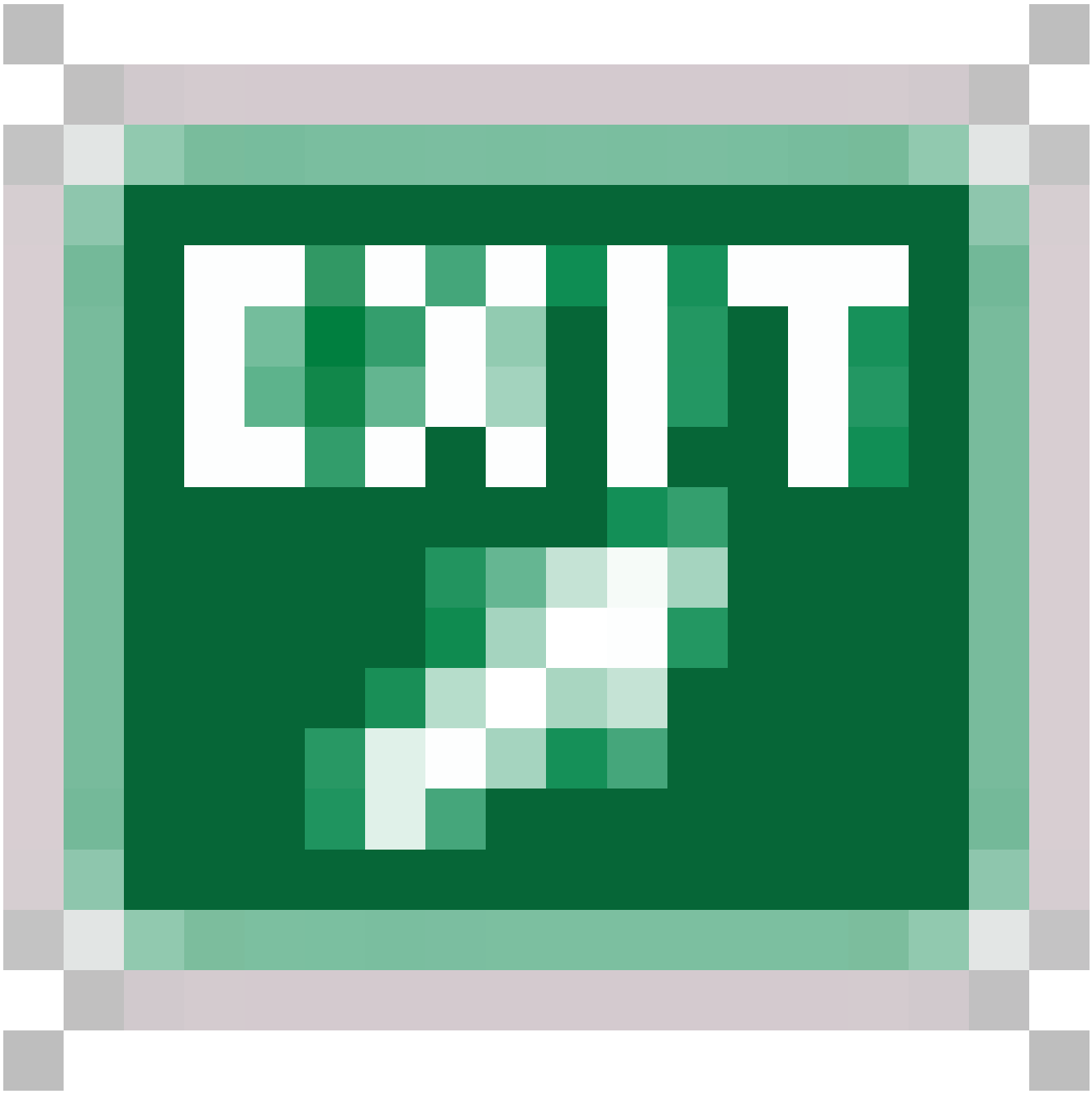
この脆弱性は、次のアドバイザリ/通知で説明されています。

- Sun Alert Notification(http://sunsolve.sun.com/search/document.do?assetkey=1-26-44309-1)を参照してください。
- CERT Advisory CA-2002-11(http://www.cert.org/advisories/CA-2002-11.html



)

- この問題はCAN-2002-0033(http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0033を参照)としても言及されてい



ます。

リモートから不正利用できるヒープオーバーフローがcachefsdプログラムに存在します。デフォルトでは、Sun Solaris OSにインストールされます。Cachefsdは、NFSプロトコルを使用してマウントされたリモートファイルシステムに対する操作の要求をキャッシュします。攻撃者は、巧妙に細工されたRPC要求をcachefsdプログラムに送信して、脆弱性を不正利用する可能性があります。

Sun Microsystemsによると、この脆弱性を不正利用する試みが失敗すると、ルートディレクトリにコアダンプファイルが残る可能性があります。コアファイルは他のプロセスによって作成される可能性があり、その存在は侵害の特定の兆候ではないことに注意してください。また、ファイル/etc/cachefstabが存在する場合、既知のキャッシュディレクトリ以外のエントリ（例：/cachefs/cache0）が含まれている可能性があります。

回避策

この回避策は、このアドバイザリに記載されているすべてのシスコ製品に適用できます。MGCおよび関連製品では、CSCO013.pkgからスクリプトを適用している場合は保護されており、この回避策を適用する必要はありません。

次に示すように、/etc/inetd.confのcachefsdをコメントアウトします。

- Solaris 2.6、7、および8の場合：

```
#100235/1 tli rpc/tcp wait root /usr/lib/fs/cachefs/cachefsd  cachefsd
```

- Solaris 2.5.1:

```
#100235/1 stream rpc/tcp wait root /usr/lib/fs/cachefs/cachefsd  cachefsd
```

行がコメントアウトされると、次のようになります。

- リブート、または
- HUPシグナルをinetd(1M)に送信し、既存のcachefsdプロセスを強制終了します。たとえば、Solaris 2.5.1および2.6では次の操作を行います。

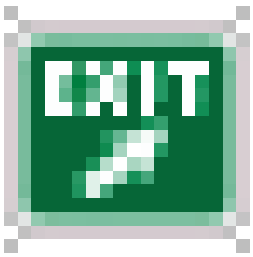
```
$ kill -HUP <PID of inetd>
       $ kill <PIDs of any cachefsd processes>
```

Solaris 7および8では、次の処理が行われます。

```
$ pkill -HUP inetd
       $ pkill cachefsd
```

修正済みソフトウェア

Sun Microsystemはパッチを実行しています。この脆弱性に関する最新のステータスは、



http://sunsolve.sun.com/search/document.do?assetkey=1-26-44309-1で確認でき

ます。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

CERT/CCによると、この脆弱性のエクスプロイトプログラムは一般に公開されており、この脆弱性が活発に不正利用されているという信頼できるレポートがあります。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20020724-solaris-cachefs

改訂履歴

リビジョン 1.1	2002年7月25日	詳細セクションに更新
リビジョン 1.0	2002年7月24日	初版リリース

利用規約

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。