

MRAサービスのためのExpresswayトラフィックサーバ証明書検証のトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[信頼済みCAチェーン](#)

[SANまたはCNの確認](#)

[動作の変更](#)

[X14.2.0より前のバージョン](#)

[X14.2.0以降のバージョン](#)

[シナリオのトラブルシューティング](#)

[1. リモート証明書に署名したCAが信頼されていない](#)

[2. 証明書に接続アドレス \(FQDNまたはIP \) が含まれていない](#)

[簡単に検証する方法](#)

[解決方法](#)

[関連情報](#)

はじめに

このドキュメントでは、Cisco Bug ID [CSCwc69661](#)またはCisco Bug ID [CSCwa25108](#)に関連するExpresswayバージョンX14.2.0以降の動作の変更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。

- Expresswayの基本設定
- MRA基本設定

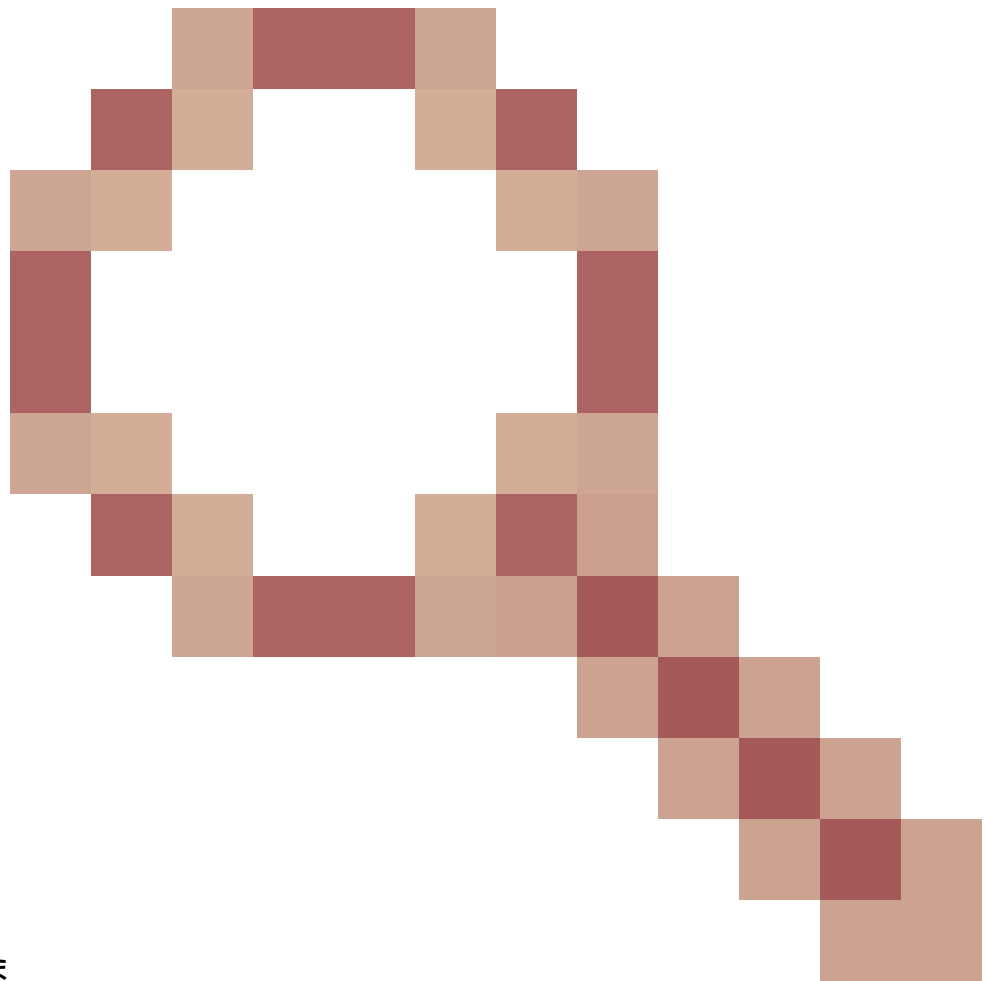
使用するコンポーネント

このドキュメントの情報は、Cisco ExpresswayバージョンX14.2以降に基づくものです。

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。

背景説明



Cisco Bug ID [CSCwc69661](#) まで

またはCisco Bug ID [CSCwa25108](#) で示されているこの動作変更により、Expresswayプラットフォーム(MRA)上のトラフィックサーバは、モバイルおよびリモートアクセス(MRA)サービス用にCisco Unified Communication Manager(CUCM)、Cisco Unified Instant Messaging & Presence(IM&P)、およびUnityサーバノードの証明書などの検証を実行します。この変更により、Expresswayプラットフォームでのアップグレード後にMRAログイン障害が発生する可能性があります。

Hypertext Transfer Protocol Secure(HTTPS)は、Transport Layer Security(TLS)を使用して通信を暗号化する安全な通信プロトコルです。このセキュアチャネルは、TLSハンドシェイクで交換されるTLS証明書を使用して作成されます。このサーバには、認証(リモート側の接続先を知る)とプライバシー(暗号化)の2つの目的があります。認証は中間者攻撃から保護し、プライバシーは攻撃者が通信を傍受して改ざんするのを防ぎます。

TLS(証明書)検証は認証の観点で実行され、正しいリモートの当事者に接続していることを確認できません。検証は、次の2つの個別の項目で構成されます。

1. 信頼された認証局(CA)チェーン
2. サブジェクトの別名(SAN)または共通名(CN)

信頼済みCAチェーン

Expressway-CがCUCM / IM&P / Unityが送信する証明書を信頼するには、信頼するトップレベル (ルート) 認証局(CA)へのその証明書からのリンクを確立する必要があります。このようなリンク、つまりエンティティ証明書をルートCA証明書にリンクする証明書の階層は、信頼のチェーンと呼ばれます。このような信頼のチェーンを確認できるように、各証明書には、Issuer (または「Issued by」) とSubject (または「Issued To」) の2つのフィールドが含まれています。

CUCMがExpressway-Cに送信するサーバ証明書などのサーバ証明書は、「件名」フィールドに、通常はCN内の完全修飾ドメイン名(FQDN)を持っています。

```
Issuer: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA
Subject: C=BE, ST=Flamish-Brabant, L=Diegem, O=Cisco, OU=TAC, CN=cucm.vngtp.lab
```

CUCM cucm.vngtp.labのサーバ証明書例SubjectフィールドのCN属性に、Country(C)、State(ST)、Location(L)、...などの他の属性とともにFQDNが含まれています。また、サーバ証明書がvngtp-ACTIVE-DIR-CAという名前のCAによって配布 (発行) されることもわかります。

トップレベルCA (ルートCA) は、自身を識別する証明書を発行することもできます。このようなルートCA証明書では、IssuerとSubjectの値が同じであることがわかります。

```
Issuer: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA
Subject: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA
```

これは、ルートCAが自身を識別するために配布する証明書です。

一般的な状況では、ルートCAはサーバ証明書を直接発行しません。代わりに、他のCAの証明書を発行します。このような他のCAは、中間CAと呼ばれます。中間CAは、サーバ証明書または他の中間CA用の証明書を直接発行できます。サーバ証明書が中間CA 1によって発行され、次に中間CA 2から証明書が取得されるという状況が考えられます。最終的に中間CAがルートCAから自身の証明書を直接取得するまで (証明書はルートCAから直接取得されます)、

Server certificate :

```
Issuer: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-1
Subject: C=BE, ST=Flamish-Brabant, L=Diegem, O=Cisco, OU=TAC, CN=cucm.vngtp.lab
```

Intermediate CA 1 certificate :

```
Issuer: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-2
Subject: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-1
```

Intermediate CA 2 certificate :

```
Issuer: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-3
Subject: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-2
```

...

Intermediate CA n certificate :


```
Issuer: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA
Subject: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-n
```

Root CA certificate :

Issuer: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA

Subject: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-C

ここで、Expressway-CがCUCMから送信されるサーバ証明書を信頼するためには、そのサーバ証明書からルートCA証明書までの信頼チェーンを構築する必要があります。そのためには、ルートCA証明書およびすべての中間CA証明書を (存在する場合は、ルートCAがCUCMのサーバ証明書を直接発行した場合を除いて) Expressway-Cの信頼ストアにアップロードする必要があります。

 注：IssuerフィールドとSubjectフィールドは、信頼のチェーンを人間が読める方法で簡単に構築できますが、CUCMでは、これらのフィールドを証明書で使用しません。代わりに、「X509v3 Authority Key Identifier」フィールドと「X509v3 Subject Key Identifier」フィールドを使用して、信頼のチェーンを構築します。これらのキーには、Subject/Issuerフィールドを使用するよりも正確な証明書のIDが含まれています。同じSubject/Issuerフィールドを持つ2つの証明書が存在する可能性があります。そのうちの1つは期限切れであり、1つはまだ有効です。両方とも異なるX509v3 Subject Key Identifier(SUBJECT KEY ID)を持つため、CUCMは正しい信頼チェーンを引き続き判別できます。

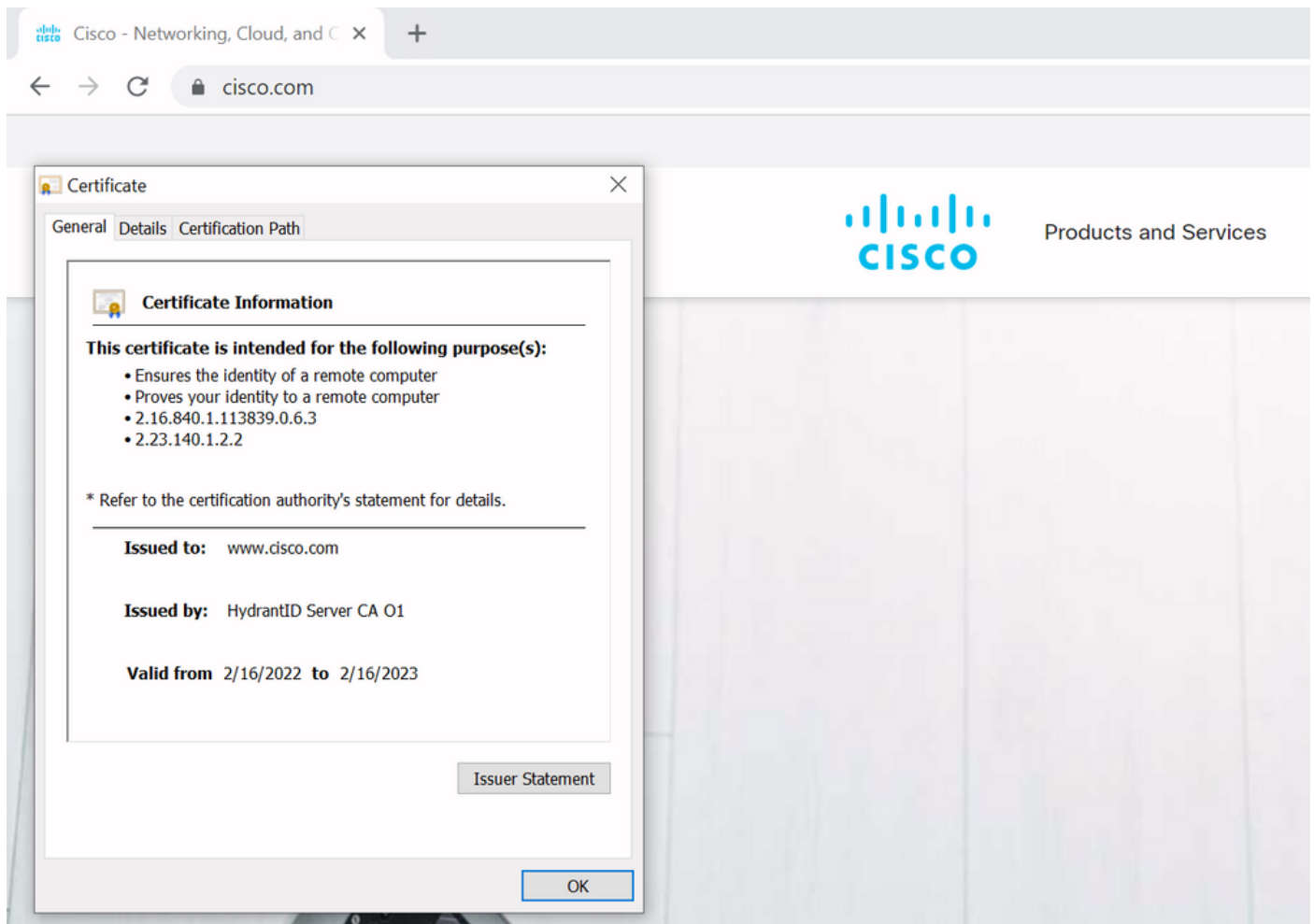
Cisco Bug ID [CSCwa12905](#)によると、これはExpresswayには該当せず、同じ共通名(CN)を持つ2つの異なる (自己署名されたなど) 証明書をExpresswayの信頼ストアにアップロードすることはできません。これを修正する方法は、CA署名付き証明書を使用するか、異なる共通名(CN)を使用するか、または常に同じ証明書を使用していることを確認する方法です (CUCM 14の再使用証明書機能を使用する可能性があります) 。

SANまたはCNの確認

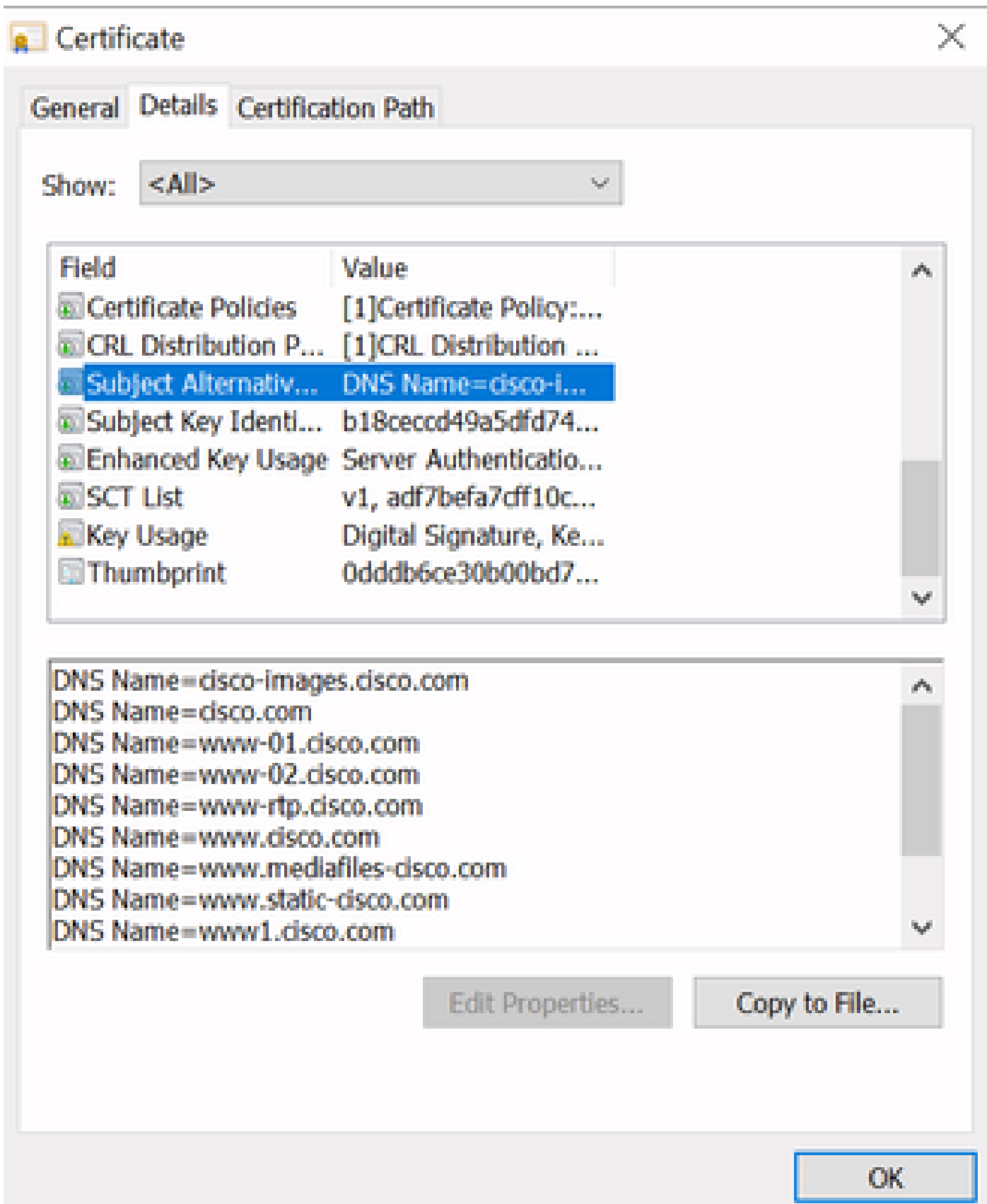
ステップ1は信頼ストアをチェックアウトしますが、信頼ストア内のCAによって署名された証明書を持つユーザは、その時点で有効になります。これは明らかに十分ではありません。したがって、特に接続するサーバが正しいものであるかどうかを検証する追加チェックがあります。これは、要求が行われたアドレスに基づいて行われます。

ブラウザでも同様の操作が行われますので、例を挙げて見てみましょう。

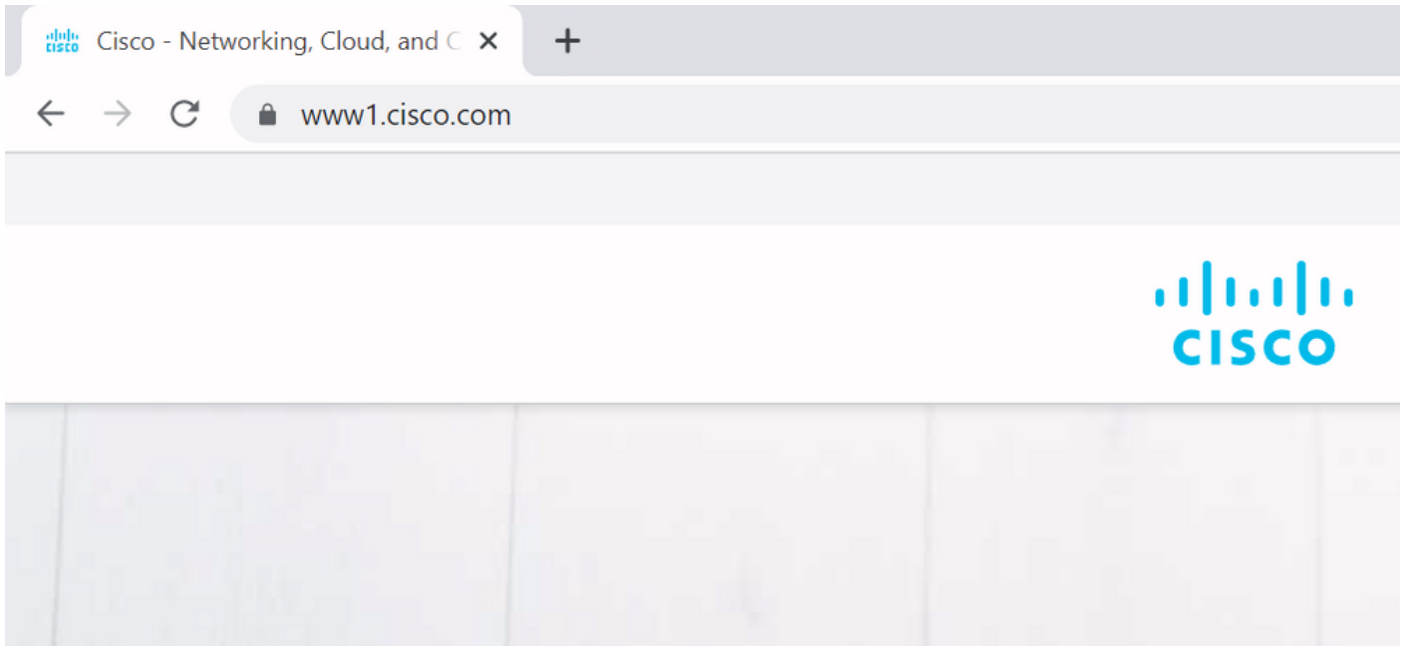
<https://www.cisco.com>を参照すると、入力したURLの横にロックアイコンが表示され、それが信頼できる接続であることを意味します。これは、CA信頼チェーン (最初のセクションから) と SANまたはCNチェックの両方に基づいています。証明書を (ブラウザのロックアイコンをクリックして) 開くと、共通名 (「Issued to:」フィールドに表示) がwww.cisco.comに設定されており、接続先のアドレスに正確に対応していることがわかります。この方法で、正しいサーバに確実に接続できます (証明書に署名し、証明書を配布する前に検証を実行するCAを信頼するため) 。



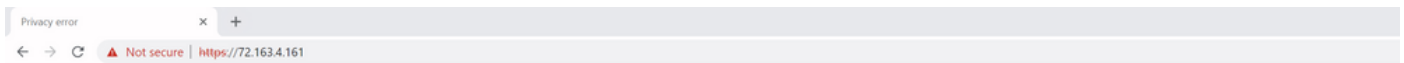
証明書の詳細、特にSANエントリを調べると、同じことが他のFQDNと同様に繰り返されていることがわかります。



つまり、たとえば<https://www1.cisco.com>への接続を要求する場合、SANエントリに含まれているため、セキュアな接続としても表示されます。



ただし、<https://www.cisco.com>をブラウズせず、IPアドレス(<https://72.163.4.161>)を直接参照する場合、署名したCAを信頼しますが、提示された証明書にはサーバへの接続に使用したアドレス(72.163.4.161)が含まれていないため、セキュアな接続は表示されません。



```
Command Prompt - nslookup
C:\Users\stejanss>
C:\Users\stejanss>nslookup
Default Server: dns-aer1.cisco.com
Address: 173.38.200.100

> cisco.com
Server: dns-aer1.cisco.com
Address: 173.38.200.100

Name: cisco.com
Addresses: 2001:420:1101:1::a
           72.163.4.161
>
```

A warning message from a browser. It features a red triangle icon with an exclamation mark. The text reads: "Your connection is not private". Below this, it says: "Attackers might be trying to steal your information from 72.163.4.161 (for example, passwords, messages, or credit cards). Learn more". The error code "NET:ERR_CERT_COMMON_NAME_INVALID" is displayed. There are two buttons: "Hide advanced" and "Back to safety". At the bottom, it says: "This server could not prove that it is 72.163.4.161; its security certificate is from www.cisco.com. This may be caused by a misconfiguration or an attacker intercepting your connection." and "Proceed to 72.163.4.161 (unsafe)".

ブラウザでは、これをバイパスできますが、これはバイパスが許可されていないTLS接続で有効にできる設定です。そのため、証明書には、リモートのユーザが接続に使用する予定の正しいCNまたはSAN名が含まれていることが重要です。

動作の変更

MRAサービスは、CUCM/IM&P/Unityサーバに対するExpressway経由の複数のHTTPS接続に大きく依存して、適切に認証し、ログインするクライアントに固有の適切な情報を収集します。この

通信は通常、ポート8443および6972経由で行われます。

X14.2.0より前のバージョン

X14.2.0より前のバージョンでは、これらのセキュアなHTTPS接続を処理するExpressway-Cのトラフィックサーバは、リモートエンドから提示された証明書を確認しませんでした。これにより、中間者攻撃が発生する可能性があります。MRA設定には、Configuration > Unified Communications > Unified CM servers / IM and Presence Service nodes / Unity Connection serversでCUCM / IM&P / Unityサーバを追加するときに、「TLS Verify Mode」を「On」に設定してTLS証明書を検証するオプションがあります。例として、設定オプションと関連情報ボックスを示します。この例では、SAN内のFQDNまたはIP、証明書の有効性、および証明書が信頼できるCAによって署名されているかどうかを確認します。



Cisco Expressway-C

Status > System > Configuration > Applications > Users > Maintenance >

Unified CM servers You are here: [Configuration](#)

Unified CM server lookup

Unified CM publisher address	cucmpub.vngtp.lab
Username	* administrator i
Password	* i
TLS verify mode	On i
Deployment	Default deployment i
AES GCM support	Off i
SIP UPDATE for session refresh	Off i
ICE Passthrough support	Off i

このTLS証明書検証チェックは、CUCM/IM&P/Unityサーバの検出時にのみ実行され、MRAログイン中にさまざまなサーバが照会されることはありません。この設定の最初の欠点は、追加したパブリッシャアドレスに対してのみ確認が行われることです。パブリッシャノードのデータベースからサブスクリバノード情報 (FQDNまたはIP) を取得するため、サブスクリバノード上の証明書が正しく設定されているかどうかは検証されません。この設定の2つ目の欠点は、接続情報がExpressway-C設定に配置されたパブリッシャアドレスと異なる場合があるため、MRAクライアントにアドバタイズされる情報が異なる点です。たとえばCUCMのSystem > Serverで、サーバをIPアドレス (たとえば10.48.36.215) でアドバタイズし、それを (プロキシされたExpressway接続を介して) MRAクライアントが使用します。ただし、FQDNをcucm.steven.labにしてExpressway-CのCUCMに追加できます。したがって、CUCMのtomcat証

明書にIPアドレスではなくSANエントリとしてcucm.steven.labが含まれている場合、「TLS検証モード」を「オン」に設定した検出は成功しますが、MRAクライアントからの実際の通信は異なるFQDNまたはIPを対象とすることができるため、TLS検証は失敗します。

X14.2.0以降のバージョン

X14.2.0バージョン以降では、Expresswayサーバは、トラフィックサーバを介して行われる個々のHTTPS要求に対して、TLS証明書の検証を実行します。つまり、CUCM/IM&P/Unityノードの検出中に「TLS Verify Mode」が「Off」に設定されている場合にも、これが実行されます。検証が成功しない場合、TLSハンドシェイクが完了せず、要求が失敗します。その結果、冗長性やフェールオーバーの問題などの機能が失われたり、ログイン障害が完了したりする可能性があります。また、「TLS検証モード」を「オン」に設定しても、すべての接続が後の例で説明するように正常に機能するとは限りません。

ExpresswayがCUCM / IM&P / Unityノードに対してチェックする正確な証明書は、『[MRAガイド](#)』のセクションに示すとおりです。

TLS検証のデフォルトの他に、X14.2で導入された変更もあります。これにより、アップグレードパスに応じて、暗号リストの異なる優先順位がアダプタイズされる可能性があります。アップグレード前にCUCM（またはECDSAアルゴリズム用の個別の証明書を持つその他の製品）からCisco TomcatまたはCisco CallManager証明書を要求する一方で、アップグレード後にはECDSAバリエーション（実際にはRSAよりも安全な暗号バリエーション）を要求する必要があるため、ソフトウェアアップグレード後に予期しないTLS接続が発生する可能性があります。Cisco Tomcat-ECDSAまたはCisco CallManager-ECDSA証明書は、別のCAによって署名することも、自己署名証明書だけで署名することもできます（デフォルト）。

この暗号の優先順位の変更は、Expressway X14.2.1の[リリースノート](#)で示されているようにアップグレードパスによって異なるため、常に関連するわけではありません。要するに、「ECDHE-RSA-AES256-GCM-SHA384:」をプリペンドするかどうか、各暗号リストのMaintenance > Security > Ciphersで確認できます。そうでない場合は、RSA暗号よりも新しいECDSA暗号が優先されます。存在する場合は、以前のRSAの動作よりも優先度が高い動作になります。

Cipher Preferences - ECDSA Cipher Preference Over RSA

ECDSA certificates are preferred over RSA.



Important

The following points lists the various upgrade path(s) that are mandatory for upgrading ciphers.

1. When upgrading from version lower than 14.0 to 14.2, the ECDSA would be preferred. If you prefer RSA certificates over ECDSA, then prefix the cipher string with "ECDHE-RSA-AES256-GCM-SHA384:" using either Web User Interface (Maintenance > Security > Ciphers) or CLI command (xConfiguration Ciphers).
2. When upgrading from version equal or higher than 14.0 to 14.2 or higher version, you have appended "ECDHE-RSA-AES256-GCM-SHA384:" to the default Ciphers List to prefer RSA certificates over ECDSA. If you prefer ECDSA certificates over RSA, then remove "ECDHE-RSA-AES256-GCM-SHA384:" from the cipher string using Web User Interface (Maintenance > Security > Ciphers) or CLI command (xConfiguration Ciphers).
3. Any customer has a fresh install X14.2 image, ECDSA is being preferred. If you prefer RSA certificates over ECDSA, then prefix the cipher string with "ECDHE-RSA-AES256-GCM-SHA384:" using either Web User Interface (Maintenance > Security > Ciphers) or CLI command (xConfiguration Ciphers).

このシナリオでTLS検証が失敗する可能性のある方法は2つあります。これについては後で詳しく説明します。

1. リモート証明書に署名したCAが信頼されていない

a. 自己署名証明書

b. 不明なCAによって署名された証明書

2. 証明書に接続アドレス（FQDNまたはIP）が含まれていない

シナリオのトラブルシューティング

次のシナリオは、ExpresswayをX14.0.7からX14.2にアップグレードした後にMRAログインが失敗したラボ環境でも同様のシナリオを示しています。ログは類似していますが、解決方法が異なります。ログは、MRAログイン前に開始し、MRAログイン失敗後に停止した診断ログ (Maintenance > Diagnostics > Diagnostic loggingから)によって収集されます。追加のデバッグロギングは有効にされていません。

1. リモート証明書に署名したCAが信頼されていない

リモート証明書は、Expressway-Cの信頼ストアに含まれていないCAによって署名されているか、Expressway-Cサーバの信頼ストアに追加されていない自己署名証明書 (本質的にはCA) である可能性があります。

次の例では、CUCMに送信される要求(10.48.36.215 - cucm.steven.lab)がポート8443 (200 OK応答) で正しく処理されますが、TFTP接続に対してポート6972でエラー (502応答) がスローされることを確認できます。

```
<#root>
```

```
===Success connection on 8443===
```

```
2022-07-11T18:55:25.910+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:25,910" Module="net
```

```
2022-07-11T18:55:25.917+02:00 vcsc traffic_server[18242]: Event="Request Allowed" Detail="Access allow
```

```
2022-07-11T18:55:25.917+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:25,916" Module="net
```

```
2022-07-11T18:55:25.955+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:25,955" Module="net
```

```
2022-07-11T18:55:25.956+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:25,955" Module="net
```

```
200
```

```
"
```

```
===Failed connection on 6972===
```

```
2022-07-11T18:55:26.000+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:26,000" Module="net
```

```
2022-07-11T18:55:26.006+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:26,006" Module="net
```

```
2022-07-11T18:55:26.016+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:26,016" Module="net
```

```
2022-07-11T18:55:26.016+02:00 vcsc traffic_server[18242]: [ET_NET 0]
```

```
WARNING: Core server certificate verification failed for
```

```
(cucm.steven.lab).
```

```
Action=Terminate Error=self signed certificate server=cucm.steven.lab(10.48.36.215)
```

```
depth=0
```

```
2022-07-11T18:55:26.016+02:00 vcsc traffic_server[18242]: [ET_NET 0]
```

```
ERROR: SSL connection failed for
```

```
'cucm.steven.lab': error:1416F086:
```

SSL routines:tls_process_server_certificate:certificate verify failed

2022-07-11T18:55:26.024+02:00 vcsd traffic_server[18242]: UTCTime="2022-07-11 16:55:26,024" Module="net

502 connect failed

"

「certificate verify failed」というエラーは、Expressway-CがTLSハンドシェイクを検証できなかったことを示しています。その理由は、自己署名証明書を示すため、警告行に表示されます。深さが0と表示されている場合は、自己署名証明書です。深さが0よりも大きい場合は、証明書チェーンがあることを意味し、不明なCAによって署名されています (Expressway-Cから見た場合)。

テキストログに示されているタイムスタンプで収集されたpcapファイルを見ると、CUCMがCNがcucm-ms.steven.lab (およびSANがcucm.steven.lab) で、steven-DC-CAによって署名された証明書を、ポート8443でExpressway-Cに提示していることがわかります。

The screenshot shows a Wireshark capture of a TLS handshake. The 'Details' pane for the failed certificate verification shows the following structure:

- Certificate (2423 bytes)
 - Certificate Length: 1507
 - Signature: 308205f206204c7a0030201020134500001220956058d3... (id-at-commonName=cucm-ms.steven.lab, id-at-organizationalUnitName=TAC, id-at-organizationName=Cisco, id-at-localityName=Oiegen, id-at-stateOrProvinceName=Belgium, id-at-countryName=BE)
 - Version: v3 (2)
 - serialNumber: 0x45000001220956058d34860844200200000122
 - signature (sha1withRSAEncryption)
 - issuer: rdnsSequence (0)
 - validity
 - subject: rdnsSequence (0)
 - subjectPublicKeyInfo
 - extensions: 9 items
 - Extension (id-ce-keyusage)
 - Extension (id-ce-keyusage)
 - Extension (id-ce-subjectAltName)
 - Extension Id: 2.5.29.17 (id-ce-subjectAltName)
 - critical: True
 - GeneralNames: 3 items
 - GeneralName: dNSName (2)
 - dNSName: cups.steven.lab
 - dNSName: steven.lab
 - dNSName: cucm.steven.lab
 - Extension (id-ce-subjectKeyIdentifier)
 - Extension (id-ce-authorityKeyIdentifier)
 - Extension (id-ce-cRLDistributionPoints)
 - Extension (id-pe-authorityInfoAccessSyntax)
 - Extension (id-ms-certificate-template)
 - Extension (id-ms-application-certificate-policies)
 - algorithmIdentifier (sha1withRSAEncryption)
 - padding: 0
 - encrypted: 9fb07874637a2a92071ef608f22709cecc7ec44470c82b...

しかし、ポート6972で提示された証明書を調べると、これがcucm-EC.steven.labとして設定されたCNを持つ自己署名証明書 (発行者自身) であることがわかります。-EC拡張子は、これがCUCMで設定されているECDSA証明書であることを示します。

スも確認します。たとえば、CUCMでIPアドレス(10.48.36.215)を使用してSystem > Serverを設定すると、Expressway-Cはそのようにクライアントにアドバタイズし、クライアントからの後続の要求 (Expressway-C経由でプロキシされる) はこのアドレスに向けて送信されます。

その特定の接続アドレスがサーバ証明書に含まれていない場合、TLS検証も失敗し、502エラーがスローされます。このエラーは、たとえばMRAログインが失敗する原因となります。

<#root>

```
2022-07-11T19:49:01.472+02:00 vcsc traffic_server[3916]: UTCTime="2022-07-11 17:49:01,472" Module="network" HTTPMSG:
```

```
|GET http://vcs_control.steven.lab:8443/c3RldmVuLmxhYi9odHRwcy8xMC40OC4zNi4yMTUvODQ0Mw/cucm-uds/user/emusk/...
...
```

```
2022-07-11T19:49:01.478+02:00 vcsc traffic_server[3916]: UTCTime="2022-07-11 17:49:01,478" Module="network" HTTPMSG:
```

```
2022-07-11T19:49:01.478+02:00 vcsc traffic_server[3916]: UTCTime="2022-07-11 17:49:01,478" Module="network" HTTPMSG:
```

```
|GET /cucm-uds/user/emusk/devices?max=100 HTTP/1.1
...
```

```
2022-07-11T19:49:01.491+02:00 vcsc traffic_server[3916]: [ET_NET 2]
```

```
WARNING: SNI (
```

```
10.48.36.215
```

```
) not in certificate
```

```
. Action=Terminate server=10.48.36.215(10.48.36.215)
```

```
2022-07-11T19:49:01.491+02:00 vcsc traffic_server[3916]: [ET_NET 2]
```

```
ERROR: SSL connection failed for
```

```
'10.48.36.215': error:1416F086:
```

```
SSL routines:tls_process_server_certificate:certificate verify failed
```

c3RldmVuLmxhYi9odHRwcy8xMC40OC4zNi4yMTUvODQ0Mwは(base64)を steven.lab/https/10.48.36.215/8443に変換します。これは、接続アドレスとして cucm.steven.labではなく10.48.36.215に接続する必要があることを示しています。パケットキャプチャに示すように、CUCM tomcat証明書にはSANのIPアドレスが含まれていないため、エラーがスローされます。

簡単に検証する方法

次の手順で、この動作が簡単に変更されるかどうかを検証できます。

1. Maintenance > Diagnostics > Diagnostic Loggingの順に選択し、Expressway-EおよびCサーバ (理想的にはTCPDumpsが有効な状態) の診断ログを開始します (クラスタの場合は、プライマリノードから開始するだけで十分です)。

2. アップグレード後に、MRAログインを試行するか、破損した機能をテストします

3. 障害が発生するまで待ってから、Expressway-EおよびCサーバの診断ログを停止します（クラスタの場合は、クラスタの各ノードから個別にログを収集してください）

4. [コラボレーションソリューションアナライザツール](#)でログをアップロードして分析する

5. 問題が発生すると、影響を受ける各サーバについて、この変更に関連する最新の警告とエラーの行がピックアップされます

The screenshot shows the 'Diagnostic overview' page in the Collaboration Solutions Analyzer. The left sidebar contains navigation options: Home, Tools, Log Analyzer, Upload files, Diagnostics, and Analysis. The main content area is titled 'Diagnostic overview' and includes a search bar and tabs for 'Issues found', 'No issue', 'Not applicable', 'Missing information', and 'Potential problem'. Under 'Issues found', there is a list of issues. One issue is selected, showing details for 'diagnostic_log_vcsc_2022-07-11_17_33_18-DifferentCA-8443.tar.gz'. The issue is categorized as a 'defect' and is titled 'Traffic Server Enforces Certificate Validation of UCM/IMP/Unity nodes for MRA services [CSCw69661]'. The description states: 'The tomcat[-ECDSA] certificate of the following CUCM / IMP / Unity nodes is not trusted by the Expressway-C: cucm.steven.lab, 10.48.36.215. This leads to MRA login issues.' The condition is 'Expressway-C X14.2 and higher versions running MRA services are affected.' The further information section explains that starting with version X14.2, the Expressway-C traffic server will do a TLS certificate check on the CUCM / IMP / Unity tomcat[-ECDSA] certificates. The action section provides steps to update the Expressway-C trust store and a CLI command: 'xConfiguration EdgeConfigServer VerifyOriginServer: Off'. A snippet of log data is shown at the bottom.

CA診断シグニチャ


This screenshot is identical to the one above, showing the 'Diagnostic overview' page. The selected issue is 'diagnostic_log_vcsc_2022-07-11_17_49_11-ConnectCAwithIPonCUCM.tar.gz'. The description is: 'The tomcat[-ECDSA] certificate of the following CUCM / IMP / Unity nodes is not trusted by the Expressway-C: 10.48.36.215. This leads to MRA login issues.' The condition is 'Expressway-C X14.2 and higher versions running MRA services are affected.' The further information section states: 'Starting with version X14.2 and higher (due to CSCw69661), the Expressway-C traffic server will do a TLS certificate check on the CUCM / IMP / Unity tomcat[-ECDSA] certificates irrespective of the configuration of TLS Verify Mode set when discovering each of those servers.' The action section provides steps to update the Expressway-C trust store and a CLI command: 'xConfiguration EdgeConfigServer VerifyOriginServer: Off'. A snippet of log data is shown at the bottom.

SNI診断シグニチャ

解決方法

長期的な解決策は、TLS検証が正常に機能していることを確認することです。実行するアクションは、表示される警告メッセージによって異なります。

WARNING: Core server certificate verification failed for (<server-FQDN-or-IP>)が表示された場合 Action=Terminate Error=self signed certificate server=cucm.steven.lab(10.48.36.215) depth=x」というメッセージが表示された場合は、それに応じてExpressway-Cサーバの信頼ストアを更新する必要があります。この証明書に署名したCAチェーン(depth > 0)を使用するか、Maintenance > Security > Trusted CA Certificateで自己署名証明書(depth = 0)を使用します。この操作は、クラスタ内のすべてのサーバで必ず実行してください。別のオプションとして、Expressway-C信頼ストア上の既知のCAによってリモート証明書に署名する方法があります。

 注：Expresswayでは、Cisco Bug ID [CSCwa12905](#)のように、同じ共通名(CN)を持つ2つの異なる（たとえば自己署名された）証明書をExpresswayの信頼ストアにアップロードすることはできません。これを修正するには、CA署名付き証明書に移動するか、CUCMをバージョン14にアップグレードします。これで、TomcatとCallManagerで同じ（自己署名）証明書を再利用できます。

WARNING: SNI (<server-FQDN-or-IP>) not in certificateメッセージが表示された場合は、提示された証明書にこのサーバのFQDNまたはIPが含まれていないことを示しています。この情報を含むように証明書を適合させることも、設定を変更して（CUCMのシステム>サーバのように）、Expressway-Cサーバの設定を更新してアカウントに反映させることもできます。

関連情報

短期的な解決策は、文書化されている回避策を適用して、X14.2.0より前の動作にフォールバックすることです。新しく導入されたコマンドを使用して、Expressway-Cサーバノード上のCLIを介してこれを実行できます。

```
xConfiguration EdgeConfigServer VerifyOriginServer: Off
```

これは、

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。