516 Upstream Certificate CN Mismatchエラーの解決

内容

はじめに

このドキュメントでは、516 Upstream Certificate CN Mismatchエラーを解決する方法について説明します。

問題

Umbrella Secure Web Gateway(SWG)プロキシがHTTPSインスペクションを実行するように設定されている場合、HTTPS URLを使用してWebサイトをブラウズすると、「516 Upstream Certificate CN Mismatch」エラーページを受け取る場合があります。

このエラーは、Webサイト証明書のサブジェクトフィールドの共通名(CN)属性に問題があることを示しているわけではありません。むしろ、証明書のサブジェクト代替名(SAN)拡張のDNS名属性に関する問題です。

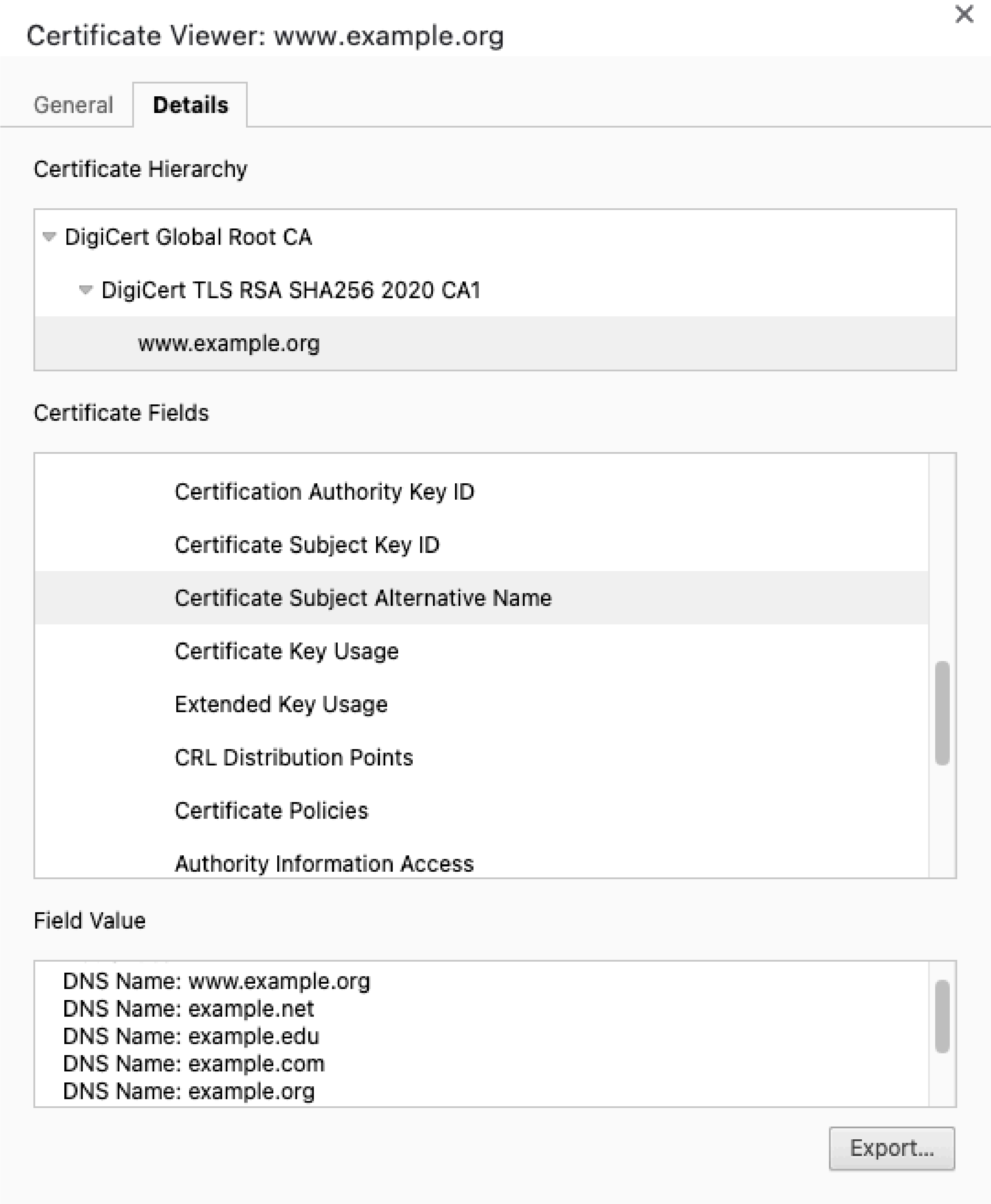
この記事を参照した後、516エラーページの理由を特定できない場合は、Umbrellaのテクニカルサポートに連絡して、このドキュメントの「証明書IDエラー」セクションで指定されている情報を提供してください。

証明書IDメカニズム

HTTPS URLを要求する場合、ブラウザまたはその他のWebクライアントは、URL内のドメイン名を、TLSネゴシエーションのClient Helloメッセージ内のServer Name Indication(SNI)拡張を介してWebサーバに送信します。サーバは多くの場合、複数のWebサイトをホストし、一部またはすべてのサイトに対して異なる証明書を持つことができるため、サーバはこのSNI値を使用して、クライアントに戻るサーバ証明書を選択します。

サーバ証明書をWebクライアントが受信すると、クライアントは要求されたドメイン名を、証明書のSubject Alternative Names拡張のDNS Name属性のドメイン名と比較することで、証明書が要求に対して正しいものであることを確認します。次の図は、サーバ証明書内のこれらのSANを

示しています。



16796247745556

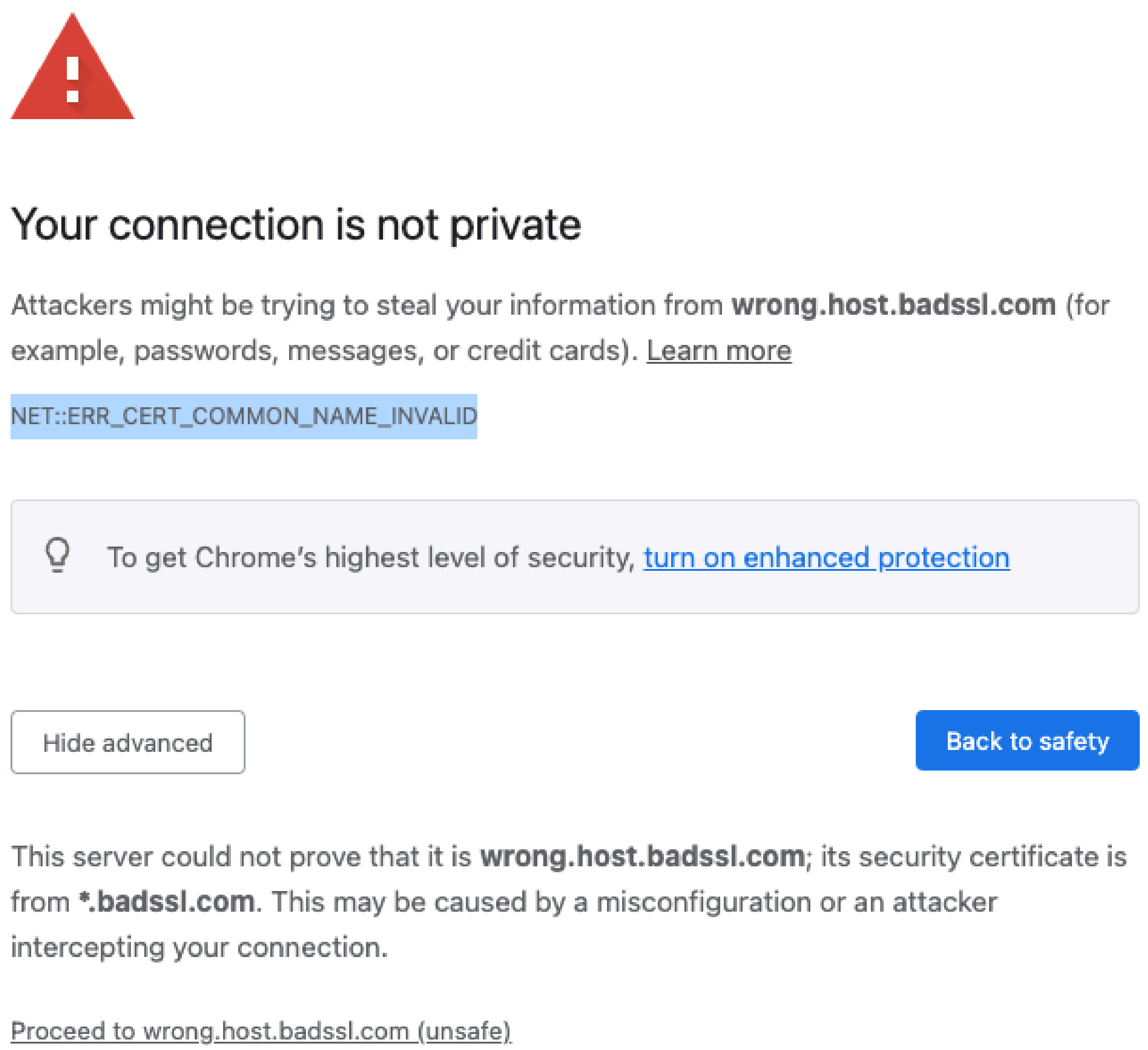
このWebサーバーは、これらのSNI値を含む要求と、[フィールド値]パネルに表示されない他の値に応答してこの証明書を返します。

- www.example.org
- example.net
- example.edu
- example.com
- example.org

SANの「example.com」はSNIの「www.example.com」と一致しません。 ただし、「*.example.com」のワイルドカードSANは、「www.example.com」のSNI、またはexample.comの前に単一のラベル（「。」文字のない文字列）を含むその他のドメイン名と一致しますが、複数のラベルとは一致しません。たとえば、「www.hr.example.com」と「*.example.com」は一致しません。「www.hr」は「www」と「hr」の2つのラベルで構成されるためです。 1つのワイルドカードは、1つのラベルにのみ一致します。

証明書IDエラー

Webクライアントがサーバ証明書を受信したときに、要求されたURLのドメイン名のSNIと一致するSANのDNS名が1つもない場合、Webクライアントは通常ユーザにエラーを表示します。次の図は、Chromeで「NET::ERR_CERT_COMMON_NAME_INVALID」の中間ページが表示されていることを示しています。



16794294817428

図では、要求されたサイトは「https://wrong.host.badssl.com」で、どのSANとも一致しません。証明書には、ワイルドカードSAN DNS名「*.badssl.com」が含まれています。このワイルドカードは、「host」などの1つのラベルにのみ一致します。 また、証明書には、正確な値が「wrong.host.badssl.com」のSAN DNS名または「*.host.badssl.com」のワイルドカードSANがないため、ユーザにこのエラーが表示されます。

証明書IDの不一致の理由を特定するには、ブラウザの証明書の表示機能を使用して証明書のSAN DNS名を調べ、要求されたURLのドメイン名と比較します。また、証明書のIDの問題を診断するために、Qualys SSL Server Testなどのツールを使用することもできます。

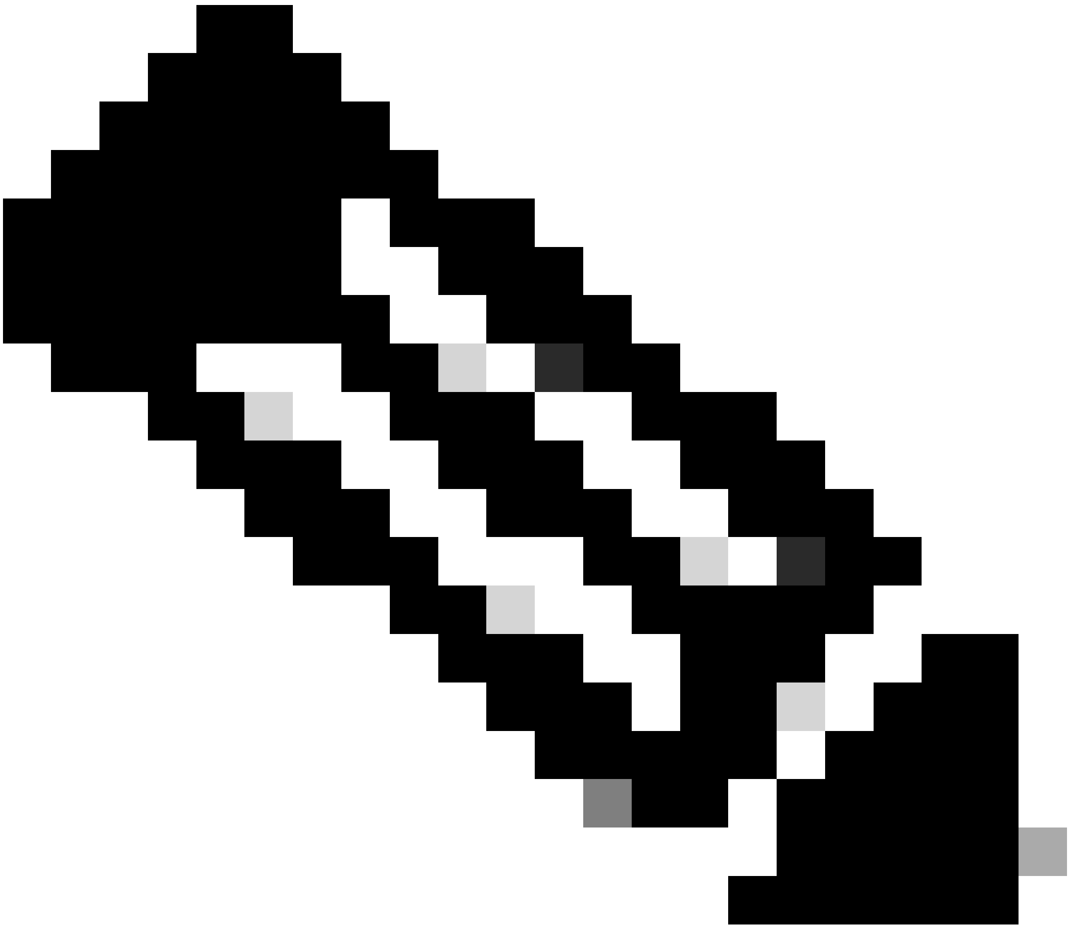
このセクションの情報を利用した後で516エラーの原因を特定できない場合、または次のセクションの解決策と回避策を使用できない場合は、Umbrellaテクニカルサポートでケースをオープンし、次の情報を提供してください。

1. キャプチャしたスクリーンショット
   - 要求されたURLを示すブラウザのアドレスバー
   - 516エラーページ全体（次のセクションの図を参照）
2. アドレスバーからコピーされたURLのテキスト

解決方法

この問題を解決するには、証明書内のSAN DNS名のいずれかに一致するドメイン名でサーバにアクセスします。この場合、Webサイトの管理者は、一致するドメイン名をゾーンのDNSに追加する必要があります。または、管理者は証明書を再発行して、SAN DNS名のいずれかにURLのドメイン名を含めることができます。

回避策として、URLのドメイン名を、セキュアWebゲートウェイプロキシの選択的復号化リスト、またはインテリジェントプロキシの宛先リストに追加できます。リストを適切なWebポリシーのルールセット設定（セキュアWebゲートウェイ）またはDNSポリシーの許可リスト（インテリジェントプロキシ）に適用します。 これにより、Webサイトへの要求がプロキシによって復号化されるのを防ぎ、プロキシが516エラーページを表示するのを防ぎます。

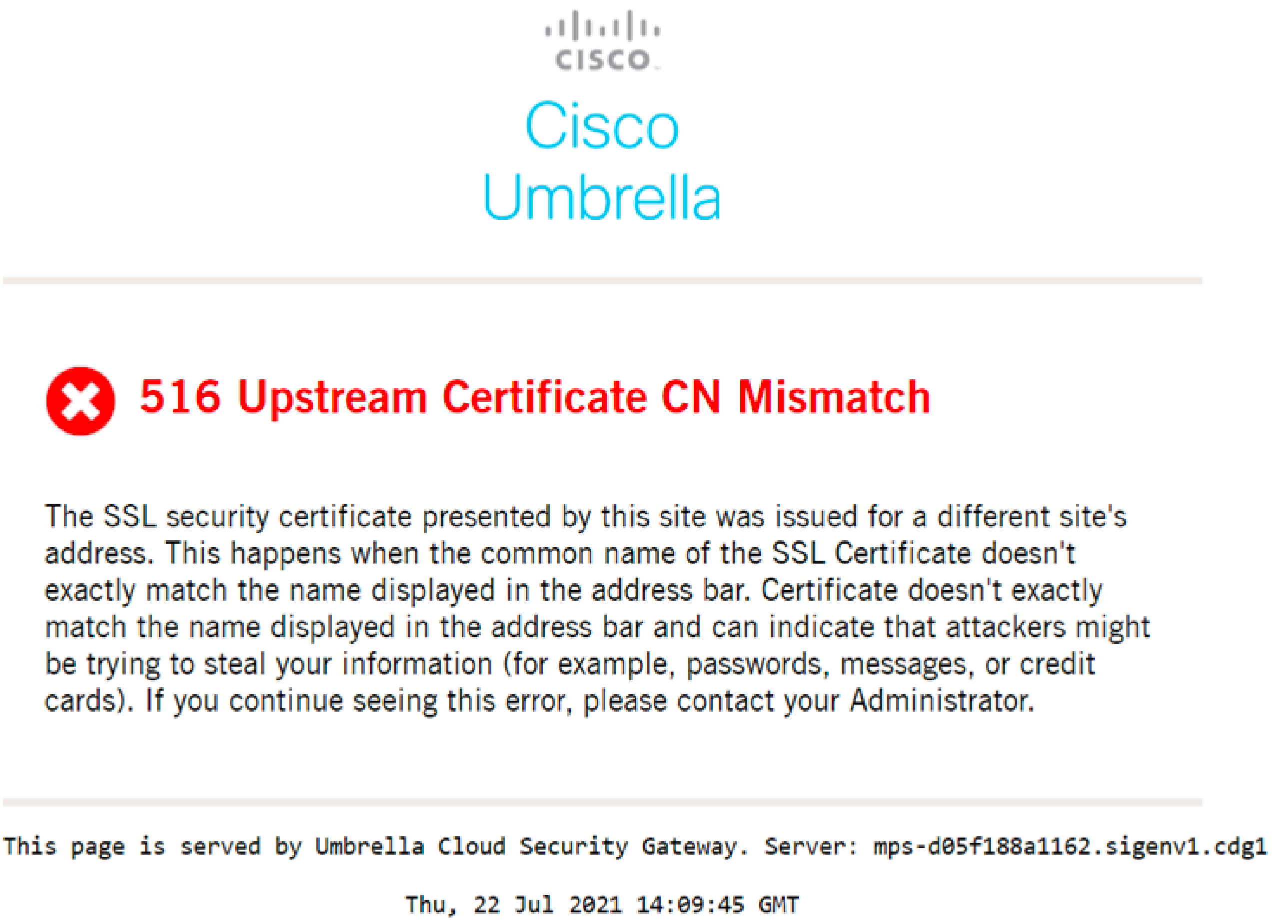


注:Secure Web Gateway(CWA)プロキシとインテリジェントプロキシの両方の使用はサポートされていません。組織ごとに採用できるプロキシテクノロジーは1つだけです。Secure Web Gatewayのサブスクリプションを所有している組織では、インテリジェントプロキシを使用せずにSWGを使用することを推奨します。

共通名の廃止

Webクライアントは、要求されたURLのドメイン名(CN)を、証明書のSubjectフィールドのCommon Name(CN)属性にもともと一致させました。このメカニズムは、最近のWebクライアントでは廃止されており、ドメインはSubject Alternative Name拡張のDNS Namesに照合されるようになりました。ただし、エラーメッセージのテキストは、Chromeの「NET::ERR_CERT_COMMON_NAME_INVALID」など、非推奨のメカニズムを引き続き参照することがよくあります。

同様に、SWGプロキシがWebサーバからURLを要求し、SAN DNS名の不一致が発生した場合、Umbrella SWGは次のテキストを含む516エラーページを表示します。



16794325789332

Cisco Umbrellaでは、今後このテキストを更新して、現在の動作をより正確に反映する予定です。

追加情報

証明書のサブジェクトについての情報は『RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile』のセクション4.1.2.6を、サブジェクト代替名についての情報はセクション4.2.1.6を参照してください。

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。