パブリックCA証明書でのクライアント認証EKUのサンセットに対するCisco ISEの準備

内容

はじめに

このドキュメントでは、クライアント認証EKUを使用してパブリック認証局(CA)によって発行されるTLS証明書に対する今後の変更によるISEサービスへの影響について説明します。

バックグラウンド情報

デジタル証明書は、信頼できる認証局(CA)によって発行される電子証明書で、認証、データの整合性、機密性を確保することによってサーバとクライアント間の通信を保護します。これらの証明書には、その目的を定義する拡張キー使用法(EKU)フィールドが含まれています。

- サーバ認証EKU(id-kp-serverAuth)：サーバが身元を証明するために証明書を提示するときに使用されます。
- クライアント認証EKU(id-kp-clientAuth)：双方が互いを認証する相互TLS(mTLS)接続で使用されます。

従来、1つの証明書にサーバ認証とクライアント認証の両方のEKUを含めることができるため、二重目的で使用できます。これは、異なる接続シナリオでサーバとクライアントの両方として機能するCisco ISEなどの製品にとって特に重要です。

問題の定義

Chromeルートプログラムポリシーの変更

2026年5月以降、多くの公開証明機関(CA)は、クライアント認証の拡張キー使用法(EKU)を含むTransport Layer Security(TLS)証明書の発行を中止します。 新しく発行された証明書には、通常、サーバ認証EKUのみが含まれます。

主要なポリシー要件

- パブリックルートCAは、サーバー認証(id-kp-serverAuth)に対してのみ拡張キー使用法(EKU)をアサートする必要があります
- 証明書には、サーバ認証EKUのみが含まれている必要があります。
- これらの証明書にクライアント認証EKUを含めることは禁止されています
- クライアント認証EKUを使用して証明書を発行し続けるルートCAは、最終的にChromeルートストアから削除されます
- パブリックサーバのTLS証明書に使用するルートCAが混在することがなくなりました。
- 実施期間:2027年3月

パブリックCA応答のタイムライン

- 2025年10月：多くのパブリックCA(DigiCert、Sectigo、SSL)が、デフォルトでサーバ専用証明書の発行を開始しました。
- 2026年5月：多くの公開CAサーバがClient Authentication EKU証明書の発行を停止
- 2027年3月：Chromeルートプログラムポリシーが完全に発効

注：このポリシーは、パブリックCAによって発行された証明書にのみ適用されます。プライベートPKIおよび自己署名証明書は、このポリシーの影響を受けません。

Cisco ISEへの影響

該当製品

すべてのCisco ISEリリースが影響を受けます。

- ISE 3.1
- ISE 3.2
- ISE 3.3
- ISE 3.4
- ISE 3.5

注:Cisco ISE 2.xバージョンも影響を受けます。ただし、これらのリリースはサポート終了(EOL)に達しているため、修正の予定はありません。

Cisco ISEのデュアルロール

ISEは、さまざまな接続シナリオでサーバとクライアントの両方として機能し、サーバ認証とクライアント認証の両方のEKUを持つ証明書を必要とします。

サーバとしてのCisco ISE（サーバ認証EKUが必要）:

- pxGrid
- ISEメッセージングサービス

クライアントとしてのCisco ISE（クライアント認証EKUが必要）:

- TC-NAC
- セキュアSyslog
- LDAPS
- Radius DTLS(RADIUS DTLS)

影響を受ける具体的な使用例

次の表は、クライアント認証EKUの変更によって影響を受ける可能性があるCisco ISEサービスと、各サービスに対して予想される影響をまとめたものです。

サービス	影響

pxGrid	pxGrid証明書は、ISEノードと外部pxGrid統合との間の通信に使用されます。外部pxGrid統合ではサーバ認証EKUのみが必要ですが、Cisco ISEでは現在、UIの制限により、インポートされたpxGrid証明書にサーバ認証EKUとクライアント認証EKUの両方を含める必要があります。その結果、パブリックCAによって発行されたpxGrid証明書は、通常、両方のEKUとともに導入されます。
ISEメッセージングサービス(IMS)	IMSは、内部ISEサービス間のバックエンド通信に使用されます。Cisco ISEでは現在、IMS証明書にサーバ認証EKUとクライアント認証EKUの両方を含める必要があります。サーバ認証EKUのみを使用してパブリックCAによって更新された証明書は、IMSには使用できません。そのため、内部ISE通信で障害が発生する可能性があります。
TC-NAC	管理証明書にサーバ認証EKUのみが含まれている場合、FIPSモードが有効になっているか、TenableがmTLSを使用して設定されている（ISEバージョン3.4P3および3.5で導入された）ときにTC-NACの証明書ベースの認証が影響を受ける可能性があります。
セキュアSyslog	
LDAPS	
RADIUSのDTLS	

⚠ 注意:外部pxGridクライアントで使用されている証明書タイプを確認する必要があります。更新時に、パブリックCA署名付き証明書にクライアント認証EKUが含まれなくなる場合があります。ISEと通信する場合、外部pxGridクライアント統合にクライアント認証EKUを含める必要があります。含めないと、接続が拒否されます。

問題の症状

Cisco ISEでサーバ認証EKU only証明書を導入すると、選択したサービスの現在の拡張キー使用法(EKU)要件を満たしていないpxGridまたはISE Messaging Service(IMS)証明書をアップロードしようとすると、Cisco ISE GUIで証明書インポートの失敗が発生します。

GUIに表示されるエラーメッセージの例を次に示します。

推奨事項

現在の証明書の監査（必須の最初の手順）

- すべてのパブリックTLS証明書のインベントリを準備し、クライアント認証EKUを含む証明書を特定します
- 証明書の使用法のドキュメント化：上の表に従って、パブリックCAで署名された証明書を特定します。
- CAおよびルート情報の確認：各証明書を発行したCAおよびルートを文書化します。
- 有効期限の確認：ポリシー適用前に計画的に更新を計画

クライアントEKUを必要とするサービスに関する提案

次の表に、クライアント認証EKUを含む証明書に依存するCisco ISEサービスおよび統合の推奨処置を示します。

サービス	推奨処置
TC-NAC	• Tenableを使用する場合、接続を維持するために、Tenable側の厳密なEKU検証を無効にすることができます。
セキュアSyslog	
LDAPS	
RADIUSのDTLS	
PxGridクライアント（CatC、FMCなど）	
EAP-TLS	

短期的な回避策（2026年6月より前）

管理者は、次のいずれかの回避策を選択できます。

オプション1：結合されたEKU証明書を提供するパブリックルートCAに切り替える

一部のパブリックルートCA(DigiCertやIdentrustなど)は、代替ルートからの結合EKUを含む証明書を発行します。これは、Chromeブラウザの信頼ストアに含めることはできません。

パブリックルートCAおよびEKUタイプの例：

CAベンダー	EKUタイプ	ルートCA	発行側/下位CA
Identrust	clientAuth +サーバ認証	Identrustパブリックセクタルートca 1	Identrust Public Sector Server CA 1
デジタル証明書	clientAuth +サーバ認証	DigiCert Assured ID Root G2	DigiCert Assured ID CA G2

このアプローチの前提条件：

- CAプロバイダーと連携して、そのような証明書が使用可能かどうかを確認します。
- 証明書を展開する前に、証明書を提示するサーバと、証明書を使用するすべてのクライアントの両方が、対応するルートCAを信頼していることを確認してください。
- 通信ピアとルート証明書情報を交換する。
- このアプローチにより、ソフトウェアを即座にアップグレードする必要がなくなります。

証明書管理参照：

- Cisco Identity Services Engine 管理ガイド リリース 3.3
- ISEでの証明書更新の設定

オプション2：現在の証明書を更新して有効期間を延長する

2026年5月より前に公開ルートCAによって発行され、サーバ認証とクライアント認証の両方のEKUを持つ証明書は、その期間が満了するまで保持されます。

更新戦略

一般的な推奨事項は次のとおりです。

- ポリシーのサンセットが発生する前に結合されたEKU証明書を更新する
- 証明書の有効性を最大にするために、2026年3月15日より前に証明書を更新する予定です。
- この日付を過ぎると、パブリックCA発行の証明書は200日間だけ有効になります。
- このオプションを使用する場合は、証明書をこの日付より前に更新することを強くお勧めします。
- パブリックCAポリシーと実装の日付は異なる場合があります。
- 一部のパブリックCAは結合EKU証明書の発行を停止しており、デフォルトでは提供できません。
- EKUを組み合わせた証明書を生成するには、CA認証局と連携し、パブリックCAによって提供される特別なプロファイルを使用します。

オプション3：代替CAプロバイダーの評価と移行

プライベートPKIアプローチ

- プライベートPKIへの移行の実現可能性を評価する
- EKUを組み合わせた単一の証明書（必要なEKUを持つサーバ証明書とクライアント証明書）を発行するようにプライベートCAを設定する
- プライベートCA署名付き証明書を発行する場合、ルート証明書情報をピアと共有する必要があります。
- 証明書を発行または展開する前に、証明書を提示するサーバと、証明書を使用するすべてのクライアントの両方が、対応するルートCAを信頼していることを確認してください。
- プライベートCAは、Chromeルートプログラムポリシーの対象ではありません
- 証明書ポリシーの長期的な制御を提供する

長期的なソリューション（ソフトウェアのアップグレードが必要）

Cisco ISEを、新しいCAポリシーに基づいて発行された証明書をサポートするように更新された証明書処理を導入するパッチリリースにアップグレードする必要があります。

次のパッチリリースは、2026年4月に計画されているこの問題に対処するものです。

Cisco ISEのバージョン	パッチバージョン
ISE 3.1	パッチ11
ISE 3.2	パッチ10
ISE 3.3	パッチ11
ISE 3.4	パッチ6
ISE 3.5	パッチ3

パッチインストール後の動作

PxGrid証明書

パッチリリースのインストール後：

- pxGrid証明書に対してサーバ認証EKUとクライアント認証EKUの両方を適用する現在のUI要件が削除されます。

- Cisco ISEでは、サーバ認証EKUのみ、サーバ認証EKUとクライアント認証EKUの両方、またはEKU拡張子なしを含むpxGrid証明書をインポートできます。
- クライアント認証EKUのみを含む証明書は受け入れられません。

ISEメッセージングサービス(IMS)証明書

ISE 3.1、3.2、および3.3の場合

パッチをインストールしても、動作に変更はありません。ISEメッセージングサービスでは、クライアントとサーバの両方のEKUを持つ証明書が引き続き必要です。現在の証明書の有効期限が切れた後に、ISE内部CA証明書を使用するように計画する必要があります。

ISE 3.4および3.5の場合

IMSは、サーバ認証EKUのみを含むパブリックCA証明書をサポートするようになりました。ただし、IMSは内部Cisco ISE通信にのみ使用されるため、証明書の更新時にISE内部CA 証明書を使用することをお勧めします。

デシジョンツリー

開始：Cisco ISEでパブリックCA証明書を使用しますか。

|

├─いいえ：プライベートPKIまたは自己署名

| └─対処の必要なし – ポリシーの影響を受けない

|

└─はい：パブリックCA証明書が使用されています

  |

  ├─「該当する具体的なユースケース」セクションに記載されているサービスに対して使用されますか。

  | |

  | ISEがTLSクライアントとして機能する場合の├─サービス

  | | └─「クライアントEKUを必要とするサービスの提案」セクションを確認してください。

  | |

  | ISEがTLSサーバ（PxGridまたはIMS）として機能する場合の└─サービス

  | |

  | └─アプローチの選択：

| |

| ├─オプションA：代替ルートCAへの切り替え

| | ├─代替ルートからの結合EKUについてCAプロバイダーに問い合わせてください

| | ├─すべてのピアが新しいルートを信頼することを確認します

| | └─ソフトウェアの即時アップグレードは不要です

| |

| ├─オプションB：期限前の証明書の更新

| | ├─ Cisco ISEへのパッチ適用を緊急にリリースできます

| | |

| | | ├─有効期間の延長： 2026年3月15日までに更新

| | └─証明書が期限切れになるまで時間を購入します

| |

| ├─オプションC：プライベートPKIへの移行

| | ├─プライベートCAインフラストラクチャのセットアップ

| | ├─組み合わせたEKU証明書を発行します

| | ├─ ISE信頼ストアに新しいCAをインストールします

| └─長期管理

| |

| └─オプションD：ソフトウェアアップグレードの計画

| ├─必要なISEパッチリリースを適用します（2026年4月から利用可能）。

よく寄せられる質問（FAQ）

一般的な質問

Q：プライベートPKIを使用する場合、この点について懸念する必要がありますか。

A：いいえ。このポリシーは、パブリックルートCAによって発行された証明書にのみ影響します

。プライベートPKIおよび自己署名証明書には影響しません。

Q：既存の証明書を引き続き使用できますか。

A：はい。結合EKUを含む既存の証明書は、有効期限が切れるまで有効です。この問題は、更新が必要になったときに発生します。有効期限が切れるまで、TLS接続とmTLS接続の両方に対して機能します。

Q:mTLSまたは標準TLSのどちらを使用しているかを確認するには、どうすればよいのですか。

A:「影響を受ける特定のユースケース」セクションを確認します。

アップグレードの質問

証明書の管理

スケジュールに関する質問

Q:2026年6月15日はどうなりますか。

A: Chromeは、サーバとクライアントの両方の認証EKUを含むパブリックTLS証明書の信頼を停止します。このような証明書を使用するサービスは失敗する可能性があります。

Q：なぜ2026年3月15日より前に更新する必要があるのですか。

A:2026年3月15日以降、証明書の有効期間は398日から200日に短縮されます。この日付より前に更新すると、証明書の有効期間が最大になります。

Q：アクションの期限はいつですか？

A：複数の期限があります。

- 2026年3月15日：証明書の有効期間を200日に短縮
- 2026年5月：ほとんどのパブリックCAが複合EKUの発行を完全に停止
- 2027年3月：Chromeポリシーを完全適用

関連情報

- Cisco Bug ID:CSCws83036:ISEでのClientAuth EKU適用の影響評価

外部参照

- Chromeルートプログラムポリシー

認証局のリソース

- Identrustポータル

結論

パブリックCA証明書でのクライアント認証EKUのサンセット設定は、mTLS接続を使用したCisco ISEの導入に影響を与える重要なセキュリティポリシーシフトを表します。これは業界全体に及ぶ変更ですが、影響評価は重要で、サービスの中断を防ぐために迅速な対応が必要です。

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。