

Umbrellaでの公開キーピングと証明書ピングについて

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[概要](#)

[Umbrella SWGとの互換性](#)

[その他の証明書ピングアプリケーション](#)

はじめに

このドキュメントでは、Cisco Umbrellaでの証明書ピングと公開キーピングについて説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco Umbrella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。

概要

証明書ピングは、誤って発行されたデジタル証明書やその他の不正なデジタル証明書を使用して、アプリケーションがHTTPSサーバに対するなりすましを阻止できるようにするインターネットセキュリティメカニズムです。これは、サーバを定義済みの公開キーのセットに関連付けることによって行われます。公開キーのセットは、そのサーバへの接続に対して信頼できる唯一の公開キーになる場合があります。証明書ピングには、次の2つのテクニックがあります。

- 公開キーピング(PKP RFC7469)は、Webブラウザで証明書ピングをトリガーするため

の廃止されたメカニズムです。固定された証明書は、HTTPヘッダーを使用してブラウザに送信されます。

- 静的証明書ピンングでは、特定の証明書または認証局を想定してアプリケーションをハードコードします。一部のデスクトップ/モバイルアプリケーションでは、追加のセキュリティのために静的な証明書ピンングメカニズムを使用します。

これらのWebアプリケーションがUmbrellaによってプロキシされる場合、Umbrellaによって提供される公開キーが一致しないため、アプリケーションはHTTPS接続を閉じます。証明書のピンングは、最近のWebブラウザではPKPのサポートが削除されているため、デスクトップ/モバイルアプリケーションにのみ適用されるのが最も一般的です。

Umbrella SWGとの互換性

Umbrellaは、特定の状況で証明書のピンングの問題を解決するために、SSL復号化から既知のURLをバイパスします。表1には、すべてのUmbrellaカスタマーに対してグローバルにバイパスされたアプリケーションが含まれています。表1には、その時点または書き込み時に証明書ピンングを使用することが判明している他のアプリケーションも含まれています。これらのアプリケーションのいずれかを使用している場合は、後で説明する方法を使用して、HTTPSインスペクションからのアプリケーションをバイパスすることもできます。表2に、表1で説明するアプリケーションサービスの詳細を示します。

その他の証明書ピンングアプリケーション

Umbrellaの[選択的復号化](#)機能を使用して証明書のピン接続の問題を解決するために、カスタマー単位（ポリシー単位）でアプリケーションをバイパスできます。これらの例外は、ドメイン、アプリケーション名、またはカテゴリに基づいて簡単に実装できます。Umbrella SWGには、アプリケーションデータベースにアプリケーションの大規模なライブラリが含まれています。

ほとんどの場合、アプリケーションをバイパスするかどうかは、IT管理者が決定します。復号化例外を追加すると、Webコンテンツのセキュリティやファイル検査が防止されるため、セキュリティ上のトレードオフになります。これは、アプリケーションのタイプやビジネスニーズに応じて個別に決定します。たとえば、証明書のピン接続の問題がモバイル/デスクトップアプリケーションにのみ影響する場合、管理者は例外を追加してモバイルアプリケーションを機能させるか、代わりにユーザにアプリケーションのWebバージョンを使用するように依頼することができます。

これは、Umbrellaカスタマーに対してグローバルにバイパスされ、アクションが不要であるか、または作成時に証明書ピンングを使用することが確認されており、デフォルトではUmbrellaによってバイパスされないアプリケーションのテーブルです。デフォルトでバイパスされないアプリケーションを使用している場合は、前述の方法を使用して、所定の理由により、HTTPSインスペクションからアプリケーションをバイパスすることを検討できます。

表1:証明書ピンングを使用できるアプリケーション

アプリケーション名	Cisco Umbrellaカバレッジ
Adobeサービス	包括ユーザ向けにグローバルにバイパス
Airbnb	アプリケーション制御によるサポート
アマゾンアレクサ	アプリケーション制御によるサポート
Amazonドライブ	アプリケーション制御によるサポート
アマゾンキンドル	アプリケーション制御によるサポート
Amazonワークスペース	アプリケーション制御によるサポート
振幅	包括ユーザ向けにグローバルにバイパス
アプリのダイナミクス	包括ユーザ向けにグローバルにバイパス
Apple iMessage (ベータ版)	アプリケーション制御によるサポート
Appleメール	アプリケーション制御によるサポート
Appleサービス(詳細は表2を参照)	包括ユーザ向けにグローバルにバイパス
シスコサービス(詳細については表2を参照)	包括ユーザ向けにグローバルにバイパス
Citrixワークスペース	アプリケーション制御によるサポート
破砕薬	包括ユーザ向けにグローバルにバイパス
CrowdStrikeファルコン	アプリケーション制御によるサポート
Diligent.com	アプリケーション制御によるサポート
Discordチャット	包括ユーザ向けにグローバルにバイパス

DocuSign契約クラウド	アプリケーション制御によるサポート
ドロッポックス	アプリケーション制御によるサポート
Druvaクラウドバックアップ	アプリケーション制御によるサポート
Egnyte接続	アプリケーション制御によるサポート
Evernote	アプリケーション制御によるサポート
Facebookメッセンジャー	アプリケーション制御によるサポート
Facebook	アプリケーション制御によるサポート
ファイル	アプリケーション制御によるサポート
4乗	アプリケーション制御によるサポート
ジフィー	包括ユーザ向けにグローバルにバイパス
GitHub	アプリケーション制御によるサポート
Googleドライブ	アプリケーション制御によるサポート
Google Playストア	アプリケーション制御によるサポート
Googleサービス(詳細については表2を参照)	包括ユーザ向けにグローバルにバイパス
Googleワークスペース	アプリケーション制御によるサポート
会議に移動	アプリケーション制御によるサポート
ハイプマシン	アプリケーション制御によるサポート
インスタグラム	アプリケーション制御によるサポート

LogMein Pro	アプリケーション制御によるサポート
エンドポイント用Microsoft Defender	アプリケーション制御によるサポート
Microsoft Intune	アプリケーション制御によるサポート
Microsoftサービス(詳細については表2を参照)	包括ユーザ向けにグローバルにバイパス
Microsoft Xbox Live	アプリケーション制御によるサポート
Netflix	アプリケーション制御によるサポート
OpenDrive	アプリケーション制御によるサポート
PayPal (有料)	アプリケーション制御によるサポート
PingOneのID	アプリケーション制御によるサポート
ラックスペース/クラウドドライブサービス	包括ユーザ向けにグローバルにバイパス
Salesforce CRM	アプリケーション制御によるサポート
セグメント	包括ユーザ向けにグローバルにバイパス
信号プラットフォーム	アプリケーション制御によるサポート
Skype for Businessを利用する	アプリケーション制御によるサポート
Snapchat	アプリケーション制御によるサポート
サウンドクラウド	アプリケーション制御によるサポート
スパイダオーク	アプリケーション制御によるサポート
Spotify	アプリケーション制御によるサポート

チームビューアー	アプリケーション制御によるサポート
ティクトク	アプリケーション制御によるサポート
トドイスト	アプリケーション制御によるサポート
Twitter	アプリケーション制御によるサポート
ビメオ	アプリケーション制御によるサポート
就業日HCM	アプリケーション制御によるサポート
会議のズーム	包括ユーザ向けにグローバルにバイパス

表2-の詳細表1に示すように、グローバルにバイパスされるサービス

Appleサービス	• Appleキャプティブポータルチェック • Apple iTunesおよびApp Store • 追加のAppleプラットフォームサービス
Cisco のサービス	• Cisco UmbrellaおよびOpenDNSサービス • Cisco WebexおよびWebex Teams • CiscoクラウドEメールセキュリティWebUI • AMPエンドポイントサービス • Duoセキュリティ2FA
Googleサービス	• Googleハングアウト • Web上のGoogleメッセージ • 追加のGoogleプラットフォームサービス
Microsoftサービス	• Microsoftネットワーク接続ステータスインジケータ • Windows Update • Windows翻訳サービス • 追加のMicrosoft/Windowsプラットフォームサービス

詳細については、「ブラウザ以外のアプリケーションのトラブルシューティング」を参照するか、[Umbrellaサポート](#)にお問い合わせください。アプリケーションは、エンジニアリングチームによるレビューの後、グローバルバイパスリストへの追加を検討できます。

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。