

WSAの新しい信頼できるルート証明書バンドルの更新 – 2017年4月

内容

[概要](#)

[背景説明](#)

[更新の説明](#)

[WSA ユーザにとっての意味](#)

概要

このドキュメントでは、Cisco Trusted Root Bundles(SRB)の2017年4月のアップデートと、Cisco Webセキュリティアプライアンス(WSA)への影響について詳しく説明します。

背景説明

シスコ製品のセキュリティを最高レベルに維持するための努力Cisco Cryptographic Services チームは、シスコの信頼されたルート バンドル リリース サイクルの次回リリースを発表しました。この変更はWSAに影響します。サポートされているすべてのバージョンの Cisco AsyncOS for Web ではバンドルが自動的に更新されるため、WSA 管理者が行う必要がある作業はありません。

更新の説明

これらのバンドルは、2016年11月の時点でのアップストリーム信頼ルートストアからのバンドルに対する最新の更新を反映しています。

注目すべきシスコの信頼されたルート バンドルの最も重要な変更を次に示します。

- 主要な信頼ストア ([Google](#)、[Apple](#)、[Mozilla](#)) による WoSign/StartCom からのルートの削除の決定に基づき、新しいシスコの信頼されたルート バンドルにはこのルートが含まれなくなりました。これらのストアからアップストリーム ルート ストアに新しいルートが再送信される場合、シスコは信頼バンドルからそれらを削除するという決定を再検討します。
- 新しい ACT2 チップセットをサポートするため、新しい Cisco Root CA 2099 がすべてのバンドルに追加されました。
- Core バンドルに存在した古い VeriSign ルートが、VeriSign mPKI 証明書への正しいチェーンを含む新しいルートに置き換えられました。
- シスコは今後このチェーンからのルートを発行しないため、DST Root CA X1 は Core バンドルのみから削除されました。

WSA ユーザにとっての意味

- Cisco WSAは、シスコのアップデートプロセスを使用する新しいルート証明書バンドルをダ

ダウンロードします。WSA管理者からのアクションは必要ありません。

- WSA が復号を使用するように設定されている場合は、WoSign/StartCom により署名された SSL 証明書を使用するサイトに対する要求は、デフォルトで WSA によりドロップされます。これは、更新後には WSA はこのベンダーのルート CA 証明書を信頼しないためです。
- または、WSAは、[HTTPS Proxy] > [Invalid Certificate Handling] > **[Unrecognized Root Authority / Issuer]** で設定されたアクションを適用します。このアクションはデフォルトでは DROP です。デフォルトの Unrecognized Root Authority アクションは変更しないことをお勧めします。

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。