

SSLサーバ証明書のルート証明書移行 に伴うご対応のお願い

(Seiko TRUSTタイムスタンプご利用ユーザ様向け)

2026年7月10日

DXソリューション本部

トラストサービス統括部

セイコーソリューションズ株式会社

1. 概要

平素より弊社サービスをご利用いただきありがとうございます。

このたび、GMOグローバルサイン社より、SSLサーバ証明書に使用されるルート証明書および中間CA証明書の移行が発表されました。

<https://info-globalsign.com/news/20260414>

インターネットの安全性向上のため、Firefox等を提供するMozilla社において、SSLサーバ証明書のルート証明書に関する要件が見直されています。これにより、一定期間経過した証明書や旧仕様の証明書は順次利用が制限されるため、認証局各社では新しいルート証明書への移行が進められています。これに伴い、弊社サービスにおいても、次回のSSLサーバ証明書更新時に新しい証明書チェーンへ移行予定です。

本資料では、以下の製品・サービスをご利用のお客様を対象として、対応についてご説明します。

- Seiko TRUSTタイムスタンプ

※上記サービスにおいて、弊社センターとHTTPS通信を行う環境が対象です

2. 変更内容

弊社サービスで使用するSSLサーバ証明書の信頼チェーンが、旧ルート証明書から新しいルート証明書へ変更されます。

変更対象：ルート証明書／中間CA証明書
提供元：GMOグローバルサイン株式会社

項目	移行前	移行後
ルート証明書	CN = GlobalSign O = GlobalSign OU = GlobalSign Root CA - R3 シリアル番号：04000000000121585308a2 有効期間：2009年3月18日 - 2029年3月18日	CN = GlobalSign Root R46 O = GlobalSign nv-sa C = BE シリアル番号：11d2bbb9d723189e405f0a9d2dd0df2567d1 有効期間：2019年3月20日 - 2046年3月20日

<https://info-globalsign.com/news/20260414> より転載

弊社サービス適用時期：2027年2月初旬予定

【重要】

**2027年2月予定のSSLサーバ証明書更新以降、
未対応の場合は通信エラーが発生する可能性があるため、
2027年1月末日までに必ずご対応ください。**

3. 影響について

お客様環境において、新しいルート証明書が信頼されていない場合、以下の影響が発生する可能性があります。

- ・ 弊社サービスとのHTTPS通信が確立できない
- ・ タイムスタンプの取得に失敗する
- ・ 電子署名および検証処理におけるエラー

なお、これらの影響は、タイムスタンプサービスに接続する際に証明書の検証が正しく行えないために発生します。

本サービスのご利用にあたり、ルート証明書の登録先は、ご利用のツールや実行環境によって異なります。具体的には、以下のいずれかの環境に証明書を登録する必要があります。

- ・ OSの証明書ストア（Windows証明書ストア等）
- ・ アプリケーションが利用するJavaの信頼済み証明書ストア（cacerts）

※一般的に、Javaで動作するツールの場合はJavaの証明書ストアが使用されます。

どちらの証明書ストアが使用されるかは、ご利用のツールの仕様や動作環境に依存します。そのため、対応方法（証明書の登録先や手順）については、ご利用のツールの提供元またはシステム管理者にご確認のうえ、適切な証明書ストアへ登録を実施してください。

※証明書の登録が不要な環境（最新OS・ミドルウェア）では対応不要となる場合があります。

4. 補足

(1) 代理証明書をご利用の場合

お客様ネットワークにおいてSSL代理証明書（プロキシによるHTTPS中継）が利用されている場合、お客様のツールが動作する端末では、検証する証明書はプロキシサーバが発行する証明書となります。

この場合、プロキシサーバまたはセキュリティ機器側が新しい証明書チェーンに対応していない場合は、通信エラーが発生します。そのため、JavaやOSに証明書を登録しても解決しない場合は、プロキシサーバ側の設定をご確認ください。

SEIKO

セイコーソリューションズ株式会社