

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

(eviDaemon for PAdES、タイムスタンプSDKご利用ユーザー様向け)

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。

- eviDaemon for PAdES
- タイムスタンプSDK

※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（※取り込み対象は、ルート証明書のみになります。）

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】

弊社サービスへの適用までに、次ページ以降に説明する対応が必要です。

2027年1月末までの対応をご計画ください。

3. 影響について

お客様環境で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
- ・ タイムスタンプ取得の失敗
- ・ 電子署名・検証処理におけるエラー

本資料の対象製品（eviDaemon for PAdES、タイムスタンプSDK）は、Java上で動作しており、弊社サービスとのHTTPS通信もJavaの機能を用いて行われます。

そのため、通信先のSSLサーバ証明書を検証する際には、OSではなくJavaの信頼済み証明書ストア（cacerts）が参照されます。

このため、新しいルート証明書は、Javaの証明書ストアに登録されている必要があります。

※OSの証明書ストアに登録されていても、Java側に登録されていない場合は通信できません

■ 必須対応

**eviDaemon/タイムスタンプSDKが動作しているJavaのバージョンを確認してください。
非対応バージョンの場合やカスタマイズされた「cacerts」をご使用の場合は、次ページ以降の対応を実施してください。**

Javaバージョン	対応済みバージョン
Java 25	初期から対応済み
Java 21	21.0.4以上
Java 17	17.0.12以上
Java 11	11.0.24以上
Java 8	8u421以上

4. 対応方法

新しいルート証明書非対応の場合は、標準で登録されているJavaバージョンにバージョンアップしていただくか、バージョンアップが難しい場合は、cacertsへの手動登録が必要となります。

■ 手動登録の手順

① GMOグローバルサイン社の新しいルート証明書を取得し、任意の場所に保存します：

リポジトリURL：https://jp.globalsign.com/support/rootcertificates/ssl.html#dv03

保存ファイル名：gCCR46R00T.cer

② 以下のコマンドを実行し、証明書を登録します：

Windows の場合：

```
keytool -importcert -alias globalsignr46 -file gCCR46R00T.cer -cacerts -noprompt
```

※証明書ストアへの書き込みに管理者権限が必要となる場合があります。うまく登録できない場合は、コマンドプロンプトを「管理者として実行」して再度お試しください。

Linux / Mac の場合：

```
sudo keytool -importcert -alias globalsignr46 -file gCCR46R00T.cer -cacerts -noprompt
```

※ルート証明書ファイルの指定には、保存場所によってパスの指定が必要になります。

※cacerts のデフォルトパスワード：changeit （パスワード入力が必要です）

■ 登録状況の確認方法

以下のコマンドで、GlobalSignの証明書が登録されているか確認できます。

Windows：

```
keytool -list -cacerts | findstr /i globalsign
```

Linux/Mac：

```
keytool -list -cacerts | grep -i globalsign
```

複数の証明書が表示される場合は、エイリアスを指定して詳細情報を確認してください。

```
keytool -list -v -cacerts -alias <エイリアス名>
```

※表示された証明書の「CN（例：GlobalSign Root R46）」および有効期間（2019年～2046年）が一致することを確認してください。

(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、eviDaemon/タイムスタンプSDKが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。そのため、GlobalSignの新しいルート証明書をJava側に登録しても、プロキシサーバ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。

この場合は、プロキシサーバまたはセキュリティ機器側での設定変更が必要となるため、お客様ネットワーク管理者へご確認ください。

(2) 同一コンピュータ上に複数のJavaが存在し、デフォルトのJava以外で動作している場合

同一コンピュータ上に複数のJavaが存在する場合、デフォルトのJavaに証明書を登録しても、eviDaemon/タイムスタンプSDKが使用しているJava環境に反映されず、通信エラーが解消されないことがあります。

必ず、eviDaemon/タイムスタンプSDKが動作しているJavaのインストールディレクトリ配下のbinフォルダにあるkeytoolを使用し、該当環境のcacertsに証明書を登録してください。

SEIKO

セイコーソリューションズ株式会社