

SSLサーバ証明書のルート移行 弊社テストサイトによる事前確認について

(eviDaemon for PAdES、タイムスタンプSDKご利用のお客様向け)

2026年9月3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

はじめに

本資料は、eviDaemon for PAdES または タイムスタンプSDK をご利用のお客様向けに、新しいSSLサーバ証明書への対応状況を確認する方法をご案内するものです。

弊社では、2027年2月にSSLサーバ証明書を新しい証明書チェーンへ移行する予定です。
お客様が、新しいSSLサーバ証明書への切り替え後も継続して弊社サービスをご利用いただける状態であることを事前にご確認いただけるよう、SSL/TLS接続確認用のテストサイトをご用意いたしました。また、本番環境の設定変更が難しいお客様向けに、本番環境へ影響を与えることなく接続確認を実施できるSSL/TLS接続確認用テストツールもご用意しました。

本資料では、以下の2つの確認方法についてご説明します。

1. SSL/TLS接続確認用テストサイトによる確認

eviDaemon for PAdESまたはタイムスタンプSDKの接続先URLを、一時的に弊社が提供するテストサイトへ変更し、新しいSSLサーバ証明書とのSSL/TLS接続可否を確認する方法です。

→詳細は2ページ「1. 弊社テストサイトへのSSL/TLS接続による確認」をご参照ください。

2. SSL/TLS通信確認用テストツールによる確認

本番環境の設定変更が難しい場合に、eviDaemon for PAdESまたはタイムスタンプSDKが利用しているJava実行環境上で専用テストツールを実行し、新しいSSLサーバ証明書とのSSL/TLS接続可否を確認する方法です。

→詳細は3ページ「2. SSL/TLS通信確認用のテストツールによる確認」をご参照ください。

本番サービスとは別に、「SSL/TLS接続確認用テストサイト」をご用意し、
本番サービスへの適用に先行して、新しい証明書チェーンのSSLサーバ証明書をテストサイトに適用します。
「SSL/TLS接続確認用テストサイト」では、**タイムスタンプ取得や署名の処理は行えませんが、
SSL/TLS通信が確立できること（＝SSL通信エラーにならないこと）をご確認いただくことが可能です。**
【SSL/TLS接続確認用テストサイト】 ※eviDaemon for PAdES ver6以降 の場合

※evjDaemon for PAdES ver5.1またはタイムスタンプSDK をご利用の場合のURLについては、次ページをご参照ください。

お客様

eviDaemon
モジュール

SSL確立エラー

Java cacerts 対応未済

Java cacerts 対応済

ログイン認証エラー

SSL接続確認用サイト (https://pades01-stg.seiko-cybertime.jp)

SSLサーバ証明書
(新ルート)

SSL通信確立

ログイン認証

タイムスタンプ/署名処理

©2026 Seiko Solutions Inc. All rights reserved.

SSLサーバ証明書のルート移行に伴う事前確認

eviDaemon for PAdES ver5.1 または タイムスタンプSDK をご利用の場合

■ eviDaemon for PAdES ver5.1 の場合

【SSL接続確認用テストサイトURL】

<https://pades01-stg.seiko-cybertime.jp/basic>

【確認ポイント】

表示されるメッセージ	判定
PKIX path building failed	未対応 Java環境および信頼済み証明書設定の確認が必要
HTTP response code: 401	対応完了

■ タイムスタンプSDKの場合

【SSL接続確認用テストサイトURL】

<https://pades01-stg.seiko-cybertime.jp/basic/Timestamp?type=AccreditedA3>

【確認ポイント】

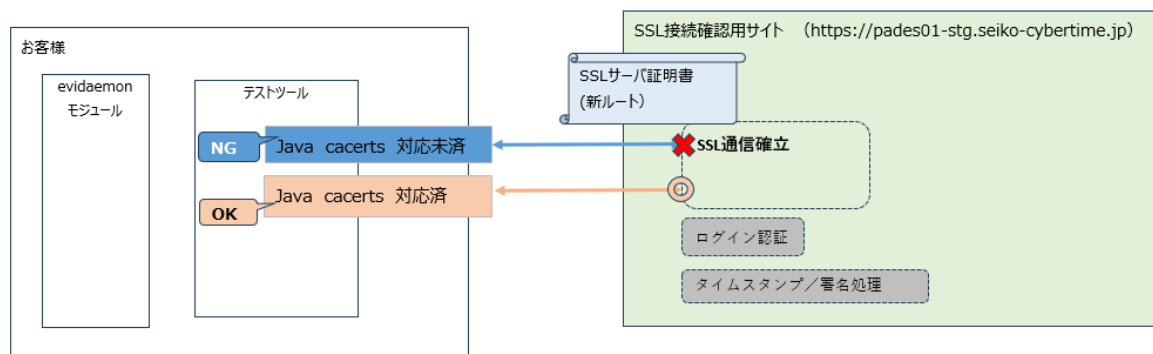
表示されるメッセージ	判定
PKIX path building failed	未対応 Java環境および信頼済み証明書設定の確認が必要
HTTP response code: 401	対応完了

SSLサーバ証明書のルート移行に伴う事前確認

2. SSL/TLS通信確認用のテストツールによる確認

本番ご利用中のeviDaemon for PAdESまたはタイムスタンプSDKを使用したご確認が難しい場合を想定し、ご要望のお客様にSSL/TLS通信確認用のテストツールをご提供いたします。

eviDaemon for PAdESまたはタイムスタンプSDKが実際に使用しているJava実行環境で、本ツールを実行し、SSL/TLS接続確認用テストサイトとのSSL/TLS通信が確立できることをご確認ください。



実行結果例)

・SSL/TLS接続成功の場合

```
***** ↓
Java version : 21.0.2 ↓
Java vendor : Oracle Corporation ↓
Java home : C:\Program Files\Java\jdk-21.0.2 ↓
JVM version : 21.0.2+13-LTS-58 ↓
JVM name : Java HotSpot(TM) 64-Bit Server VM ↓
OS name : Windows 11 ↓
***** ↓
connection test to https://pades01-stg.seiko-cybertime.jp/status ↓
HTTP Status: 200 (OK) ↓
connection successful. ↓
```

・SSL/TLS接続失敗の場合

```
***** ↓
Java version : 21.0.2 ↓
Java vendor : Oracle Corporation ↓
Java home : C:\Program Files\Java\jdk-21.0.2 ↓
JVM version : 21.0.2+13-LTS-58 ↓
JVM name : Java HotSpot(TM) 64-Bit Server VM ↓
OS name : Windows 11 ↓
***** ↓
connection test to https://pades01-stg.seiko-cybertime.jp/status ↓
javax.net.ssl.SSLHandshakeException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException:
at java.base/sun.security.ssl.Alert.createSSLException(Alert.java:130) ↓
at java.base/sun.security.ssl.TransportContext.fatal(TransportContext.java:378) ↓
at java.base/sun.security.ssl.TransportContext.fatal(TransportContext.java:321) ↓
at java.base/sun.security.ssl.TransportContext.fatal(TransportContext.java:316) ↓
at java.base/sun.security.ssl.CertificateMessage$T12CertificateConsumer.checkServerCerts(CertificateMessage.java:647) ↓
at java.base/sun.security.ssl.CertificateMessage$T12CertificateConsumer.onCertificate(CertificateMessage.java:467) ↓
at java.base/sun.security.ssl.CertificateMessage$T12CertificateConsumer.consume(CertificateMessage.java:363) ↓
```

SSL/TLS接続失敗の場合には、エラーメッセージが出力されます。
javax.net.ssl.SSLHandshakeException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable
to find valid certification path to requested target

SEIKO

セイコーソリューションズ株式会社