

SEIKO TRUST タイムスタンプの SSL サーバ証明書 の移行に伴う検証用証明書ファイルの追加方法等

アンテナハウス株式会社

作成日: 2026 年 7 月 22 日

1 概要と背景

本稿は、「e-Success/ScanSave」で「Seiko Trust タイムスタンプサービス(以下、セイコータイムスタンプ)」をご利用になられているユーザーを対象としたご案内です。

この度、セイコーソリューションズ(株)より、セイコータイムスタンプで使用する SSL サーバ証明書の信頼チェーンが、インターネットの安全性向上のため旧ルート証明書から新しいルート証明書へ変更されると発表されました。

ルート証明書の変更に伴い、これに対応するためにユーザーの環境で新しい検証証明書ファイル(ルート CA と中間 CA)の 2 種類追加が必要となります。

2027 年 1 月末日までに、必ず本稿の対応を行っていただくことをよろしくお願い申し上げます。対応しない場合は、「e-Success/ScanSave」でのタイムスタンプ付与関係でタイムスタンプ検証不備など問題を起こします。

<目次&補足説明>

- 1 概要と背景<対応期限>
- 2 対象のユーザー
- 3 検証証明書ファイルをダウンロード<最初にすること>
- 4 追加方法(Windows マシンへのインストール) <対象のパソコン>
 - 4.1 新しいルート CA の追加
 - 4.2 新しい中間 CA の追加
- 5 追加方法(store フォルダへの追加)< e-Success.exe / ScanSave.exe)のインストール先にあ
る「store」>
 - 5.1 対応概要<利用中の e-Success.exe / ScanSave.exe)関連アプリが対象>
 - 5.2 各種 Windows アプリケーション について検証証明書を追加する手順
 - 5.3 各種 Web アプリケーション について検証証明書を追加する手順

2 対象のユーザー

以下の 1 点を満たしているユーザーが対象となります

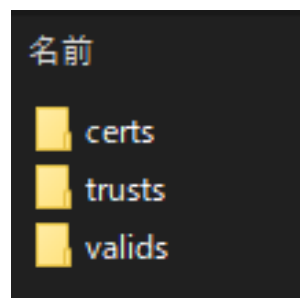
- ・「Seiko Trust タイムスタンプサービス」をご利用されている方

3 検証証明書ファイルをダウンロード

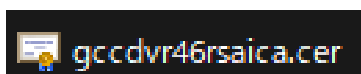
以下の URL より追加する検証証明書ファイルをダウンロードします。

https://www.antenna.co.jp/e-success/download/gmo_r46_cert.zip

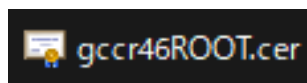
ダウンロードしたファイルを解凍すると「certs」「trusts」「valids」の 3 つのフォルダがあります。



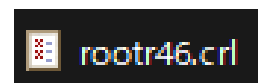
「certs」フォルダには中間 CA ファイル、「trusts」フォルダには、ルート CA ファイル、「valids」フォルダには CRL ファイルと、それぞれ 1 つずつ保存されています。



「certs」フォルダ



「trusts」フォルダ



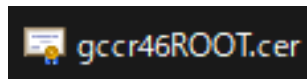
「valids」フォルダ

4 追加方法(Windows マシンへのインストール)

4.1 新しいルート CA の追加

① 「[3 検証証明書ファイルをダウンロード](#)」でダウンロードした「gmo_r46_cert.zip」の「trusts」フォルダを開きます。

② 「gccr46ROOT.cer」をダブルクリックします。



③ セキュリティ警告が表示されますが、「開く」をクリックします。

④ 「全般」タブの「証明書のインストール」をクリックします。



- ⑤ 「保存場所」を「ローカルコンピューター」で選択し、「次へ」をクリックします。

×

←  証明書のインポートウィザード

証明書のインポートウィザードの開始

このウィザードでは、証明書、証明書信頼リスト、および証明書失効リストをディスクから証明書ストアにコピーします。

証明機関によって発行された証明書は、ユーザー ID を確認し、データを保護したり、またはセキュリティで保護されたネットワーク接続を提供するための情報を含んでいます。証明書ストアは、証明書が保管されるシステム上の領域です。

保存場所

☐ 現在のユーザー(C)

☒ ローカル コンピューター(L)

続行するには、[次へ] をクリックしてください。

 次へ(N)

キャンセル

- ⑥ 「証明書をすべて次のストアに配置する」を選択し、「参照」をクリックします。

←  証明書のインポートウィザード

証明書ストア

証明書ストアは、証明書が保管されるシステム上の領域です。

Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。

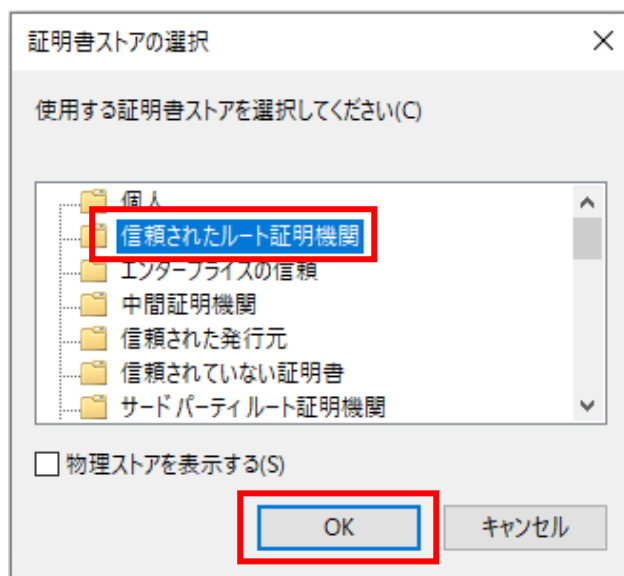
☐ 証明書の種類に基づいて、自動的に証明書ストアを選択する(U)

☒ 証明書をすべて次のストアに配置する(P)

証明書ストア:

参照(R)...

- ⑦ 「信頼されたルート証明書」を選択し、「OK」をクリックします。その後、「次へ」をクリックして、画面を進めてください。



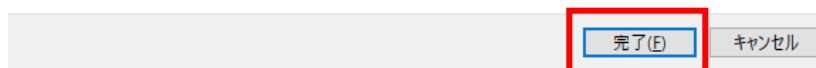
- ⑧ インポートする証明書のストアの確認ができたなら、「完了」をクリックします。

証明書のインポートウィザードの完了

[完了] をクリックすると、証明書がインポートされます。

次の設定が指定されました:

ユーザーが選択した証明書ストア	信頼されたルート証明機関
内容	証明書



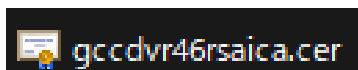
以上で、新ルート CA のインポートは完了となります。あとは、「OK」をクリックして、画面を閉じてください。

次に、「[4.2 新しい中間 CA の追加](#)」を行ってください。

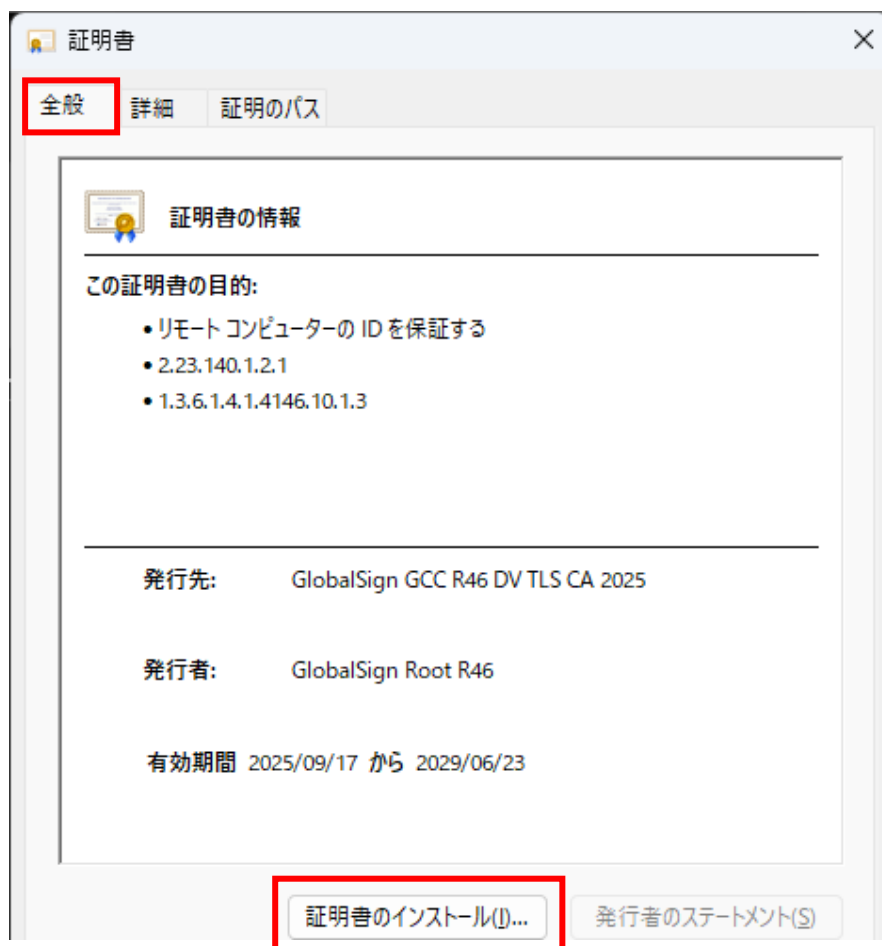
4.2 新しい中間 CA の追加

この項目では、新しい中間 CA の追加方法について、説明します。

- ① 「[3 検証証明書ファイルをダウンロード](#)」でダウンロードした「gmo_r46_cert.zip」の「certs」フォルダを開きます。
- ② 「gccdvr46rsaica」をダブルクリックします。



- ③ セキュリティ警告が表示されますが、「開く」をクリックします。
- ④ 「全般」タブの「証明書のインストール」をクリックします。



- ⑤ 「保存場所」を「ローカルコンピューター」で選択し、「次へ」をクリックします。

証明書のインポートウィザードの開始

このウィザードでは、証明書、証明書信頼リスト、および証明書失効リストをディスクから証明書ストアにコピーします。

証明機関によって発行された証明書は、ユーザー ID を確認し、データを保護したり、またはセキュリティで保護されたネットワーク接続を提供するための情報を含んでいます。証明書ストアは、証明書が保管されるシステム上の領域です。

保存場所

☐ 現在のユーザー(C)

☒ ローカル コンピューター(L)

続行するには、[次へ] をクリックしてください。

次へ(N)

キャンセル

- ⑥ 「証明書をすべて次のストアに配置する」を選択し、「参照」をクリックします。

← 証明書のインポートウィザード

証明書ストア

証明書ストアは、証明書が保管されるシステム上の領域です。

Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。

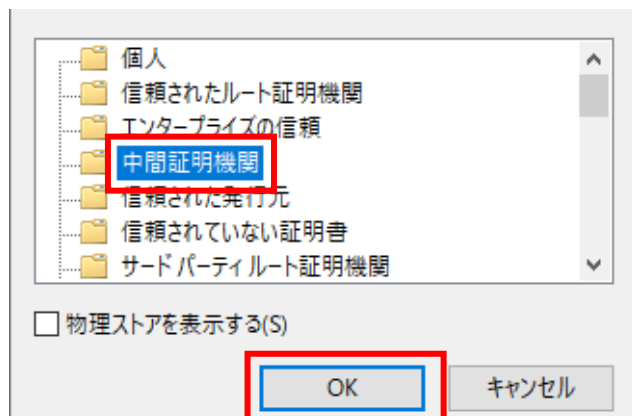
☐ 証明書の種類に基づいて、自動的に証明書ストアを選択する(U)

☒ 証明書をすべて次のストアに配置する(P)

証明書ストア:

参照(R)...

- ⑦ 「中間証明機関」を選択し、「OK」をクリックします。その後、「次へ」をクリックして、画面を進めてください。



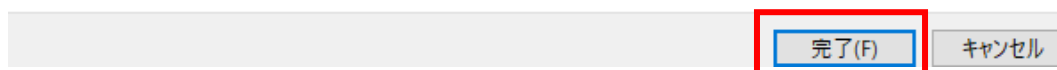
- ⑧ インポートする証明書のストアの確認ができたなら、「完了」をクリックします。

証明書のインポートウィザードの完了

[完了] をクリックすると、証明書がインポートされます。

次の設定が指定されました:

ユーザーが選択した証明書ストア	
内容	証明書
	中間証明機関



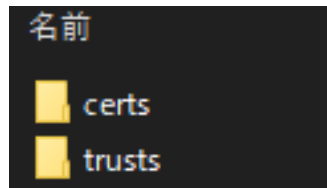
以上で、新中間 CA のインポートは完了となります。あとは、「OK」をクリックして、画面を閉じてください。

次に、「[5 追加方法\(store フォルダへの追加\)](#)」を行ってください。

5 追加方法(store フォルダへの追加)

5.1 対応概要

クライアントアプリ(e-Success.exe / ScanSave.exe)のインストール先を開くと「store」というフォルダがあります。



その中を開くと、「[3 検証証明書ファイルをダウンロード](#)」でダウンロードした「gmo_r46_cert.zip」と同様「certs」「trusts」のフォルダがあります。



このフォルダの構成に合わせ「gmo_r46_cert.zip」に入っている証明書を、「store」フォルダの「certs」「trusts」フォルダのそれぞれに入れていきます。

なお本対応ですが、「Windows アプリケーション」と「Web アプリケーション」で一部作業が異なります。

対象となる各種アプリケーション、詳細な対応手順については、次のページで説明します。

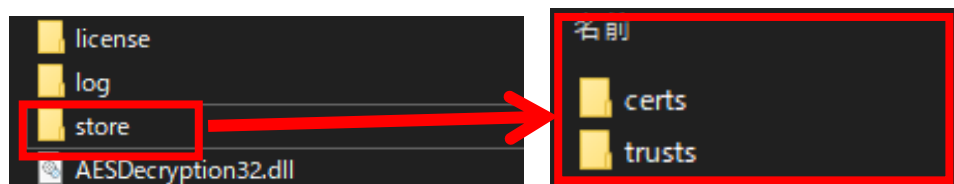
5.2 各種 Windows アプリケーション について検証証明書を追加する手順

○ 対象となるアプリケーション

- クライアントアプリ (e-Success.exe / ScanSave.exe)
- 自動タイムスタンプ付与アプリ (e-SuccessTimeStamp.exe / ScanSaveTimeStamp.exe)
- 自動一括取込アプリ (e-SuccessBulkImport.exe) 【e-Success-V5 系以前は対象外】

○ 対応手順

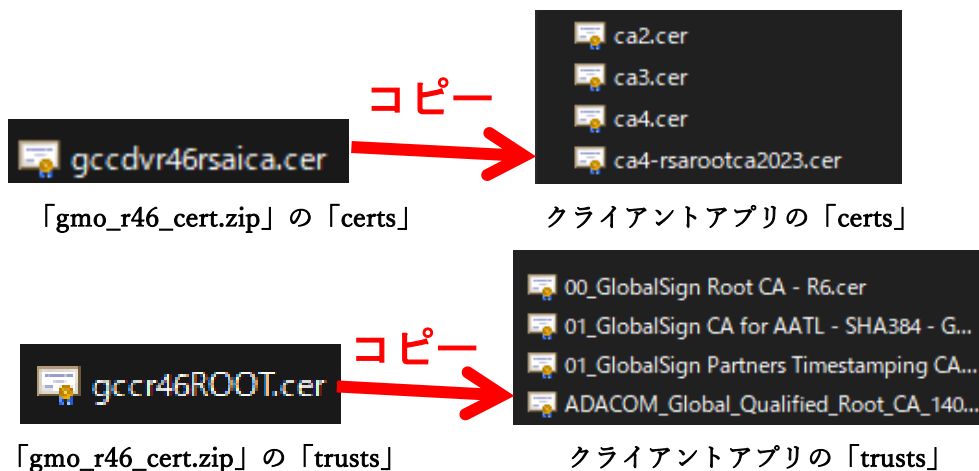
- ① クライアントアプリのインストール先を開きます。
- ② 「store」フォルダを開きます。



- ① 「[3 検証証明書ファイルをダウンロード](#)」でダウンロードした「gmo_r46_cert」を開きます。



- ③ 「gmo_r46_cert」の「certs」「trusts」フォルダに入っている証明書を個々のクライアントアプリの「certs」「trusts」フォルダにそれぞれコピーします。アプリケーション1つに対する追加作業はこれで完了です。



- ④ 同様に自動タイムスタンプ付与アプリ、自動一括取込アプリについても①～④の作業を行います。

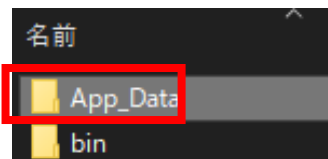
5.3 各種 Web アプリケーション について検証証明書を追加する手順

○ 対象となるアプリケーション

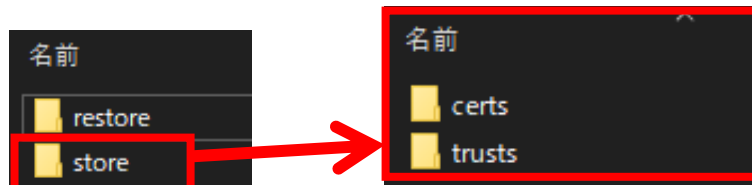
- Web 検索機能 (esuccess / scansave)
- リンクビュー (esuccesslinkview / scansavelinkview)

○ 対応手順

- ① Web 検索機能のインストール先を開きます。
- ② 「App_Data」フォルダを開きます。



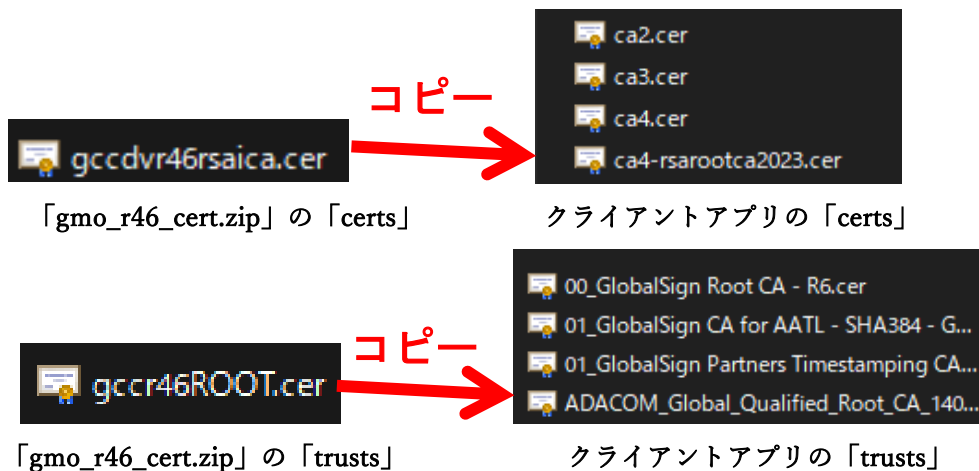
- ③ 「store」フォルダを開きます。



- ④ 「[3 検証証明書ファイルをダウンロード](#)」でダウンロードした「gmo_r46_cert」を開きます。



- ⑤ 「gmo_r46_cert」の「certs」「trusts」フォルダに入っている証明書を Web アプリの「certs」「trusts」フォルダのそれぞれにコピーします。



- ⑤ リンクビューについても①～⑤と同様の作業を行います。

6 お問い合わせ

もし、本マニュアルについて疑問点などがございましたら、下記の弊社のサポートセンターまで内容をご記入の上、お問い合わせください。

アンテナハウス株式会社 e-文書・証憑/スキャナ保存製品サポートセンター

メールアドレス: edocument@antenna.co.jp

※お問い合わせの際は、ScnaSave/e-Success の「お問い合わせ」ボタンをクリックして、
[クリップボードにコピー] ボタンをクリックすると、「お問い合わせ内容」欄に入力した内容がクリップボードにコピーされるので、メールを作成して、メール本文に貼り付けてご利用ください。