

GMO グローバルサイン電子証明書のルート CA の変更に伴う、検証証明書ファイルの追加方法

アンテナハウス 酒井

作成日: 2025 年 2 月 19 日

1 概要と背景

本稿は、ScanSave/e-Success の「GMO グローバルサイン」製の電子証明書を使用したタイムスタンプ「XAdES」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、2024 年 12 月の「GMO グローバルサイン」製の電子証明書の検証証明書ファイルの変更に伴い、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)の追加が必要となります。

そのため、旧仕様と新仕様の両方の電子証明書でタイムスタンプ付与・署名検証を可能とする環境を構築するために本稿の作成にいたしました。

2024 年 12 月以降に「GMO グローバルサイン」製の電子証明書を新しく発行もしくは更新されるユーザーの皆様には、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。

2 対象のユーザー

以下の 2 点を満たしているユーザーが対象となります

- ・タイムスタンプ方式「XAdES」をご利用されている方
- ・「GMO グローバルサイン」製の電子証明書をご利用されている方

※なお、「PAdES」(ドキュメントタイムスタンプ:タイムスタンプのみの付与方式)ユーザー、および e-SuccessV5.1.7 以降 をご利用されているユーザーの皆様につきましては、対象外となります。

3 検証証明書の追加に関する検証結果の違い

3.1 検証証明書を追加しない場合

検証証明書を追加しない場合、システムは信頼できる証明書が存在しないため、署名検証に失敗します。その結果、検証画面でエラーメッセージが表示され、以下の画像のように結果が「×」（失敗）として表示されます。

全ON	全OFF	全 20 件	
処理	書類番号	検証結果	ファイル
<input checked="" type="checkbox"/>	0000020	×	e-Success 9.pdf
<input checked="" type="checkbox"/>	0000019	×	e-Success 8.pdf
<input checked="" type="checkbox"/>	0000018	×	e-Success 7.pdf

「書類検索・検証」画面での検証結果

```
xades.setRootStore : 12
xades.loadXml : 1
xades.getType : 4197
xades.getTypeStr : XAdES-A
xades.getVersion : 2.04.R2
xades.verify : -100
=> 警告：署名証明書のルートが信頼できるか別途確認が必要です。
バージョン： v3
シリアル番号：
署名アルゴリズム： SHA-384 with RSA
発行者： GlobalSign Client Authentication Root R45, GlobalSign nv-sa, BE
有効期間開始： 2020-03-18T09:00:00
有効期間終了： 2045-03-18T09:00:00
所有者： GlobalSign Client Authentication Root R45, GlobalSign nv-sa, BE
公開鍵アルゴリズム： RSA-4096bit
公開鍵値：
公開鍵識別子：
基本制限： SubjectType=CA/criticality=YES
鍵用途： 86(digitalSignature,keyCertSign,cRLSign)/criticality=YES
私有鍵識別子：
指紋(SHA-1)：
検証完了 【問題あり】
```

検証結果の詳細

3.2 検証証明書を追加した場合

検証証明書を追加した場合、システムは信頼できる証明書を使用して署名検証を行います。その結果、検証が正常に行われ、下の画像のように結果が○（成功）として表示されます。

全ON 全OFF 全 20件

処理	書類番号 ▼	検証結果	ファイル
<input checked="" type="checkbox"/>	0000020	○	e-Success 9.pdf
<input checked="" type="checkbox"/>	0000019	○	e-Success 8.pdf
<input checked="" type="checkbox"/>	0000018	○	e-Success 7.pdf

「書類検索・検証」画面での検証結果

```
対象 : 0000002.xml
xades.setRootStore : 12
xades.loadXml : 1
xades.getType : 4197
xades.getTypeStr : XAdES-A|
xades.getVersion : 2.04.R2
マニフェストあり 1個
xades.verify : 1
Result : ◎文書正常
Signer : ts-test01
STS-Time : 2025-02-20T18:54:47.895727
ATS-time : 2025-02-20T18:54:49.067934
Valid : 2036-01-18T15:57:06
ma.verifyReferences(9) : 1
検証完了 問題なし
```

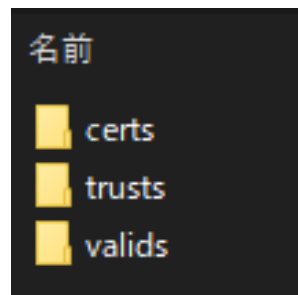
検証結果の詳細

4 検証証明書ファイルをダウンロード

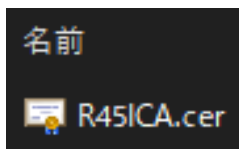
以下の URL より追加する検証証明書ファイルをダウンロードします。

https://www.antenna.co.jp/e-success/download/gmo_r45_cert.zip

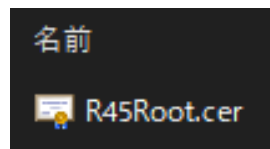
ダウンロードしたファイルを解凍すると「certs」「trusts」「valids」の3つのフォルダがあります。



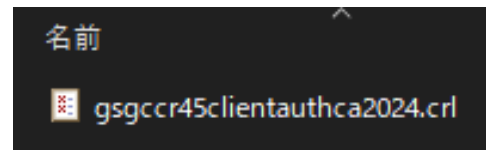
「certs」フォルダには中間 CA ファイル、「trusts」フォルダには、ルート CA ファイル、「valids」フォルダには CRL ファイルと、それぞれ1つずつ保存されています。



「certs」フォルダ



「trusts」フォルダ

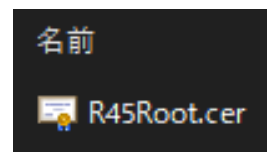


「valids」フォルダ

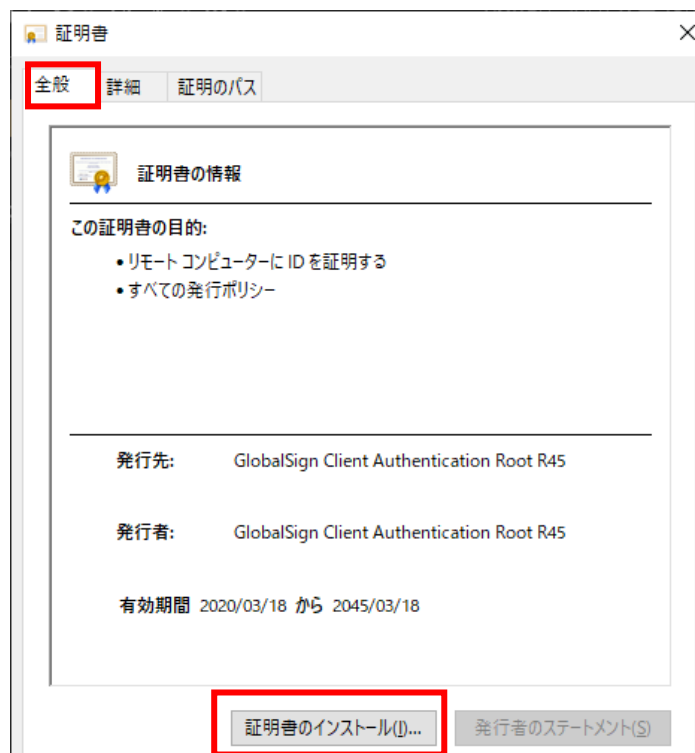
5 追加方法 (Windows マシンへのインストール)

5.1 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_r45_cert.zip」の「trusts」フォルダを開きます。
- ② 「R45Root.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

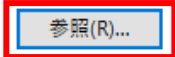
証明書ストアは、証明書が保管されるシステム上の領域です。

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。

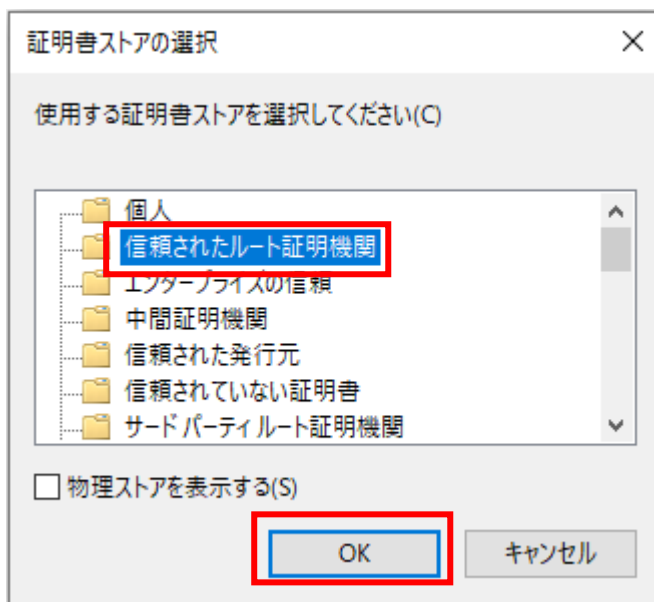
証明書の種類に基づいて、自動的に証明書ストアを選択する(U)

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。



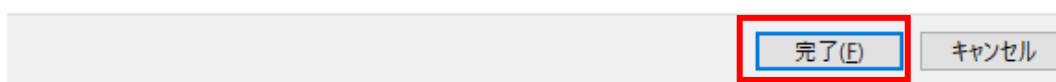
- ⑧ インポートする証明書のストアの確認ができたなら、「完了」をクリックします。

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



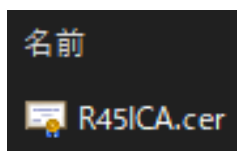
以上で、新ルート CA のインポートは完了となります。あとは、「OK」をクリックして、画面を閉じてください。

次に、「[4.2 新しい中間 CA の追加](#)」を行ってください。

5.2 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_r45_cert.zip」の「certs」フォルダを開きます。
- ② 「R45ICA.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。

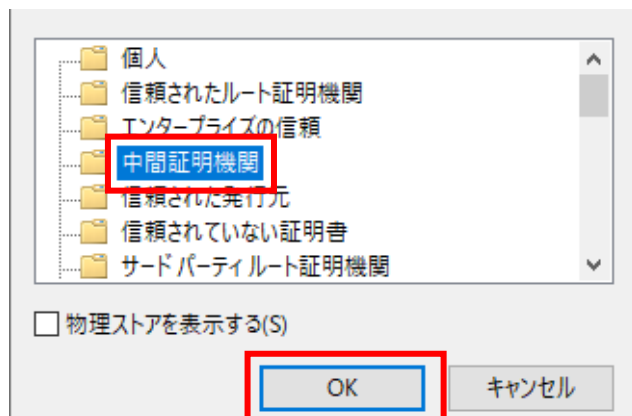
証明書の種類に基づいて、自動的に証明書ストアを選択する(U)

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。



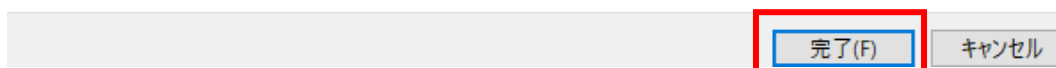
- ⑧ インポートする証明書のストアの確認ができたなら、「完了」をクリックします。

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	中間証明機関
内容	証明書



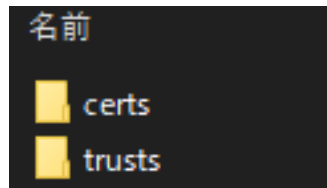
以上で、新中間 CA のインポートは完了となります。あとは、「OK」をクリックして、画面を閉じてください。

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

6 追加方法 (store フォルダへの追加)

6.1 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_r45_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_r45_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。

6.2 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 / ScanSaveBulkImport.exe)

※自動一括取込アプリのインストール先に「store」フォルダが無い場合は、自動タイムスタンプ付与アプリのインストール先にある「store」フォルダを、フォルダごとそのままコピーしてください。

○ 対応手順

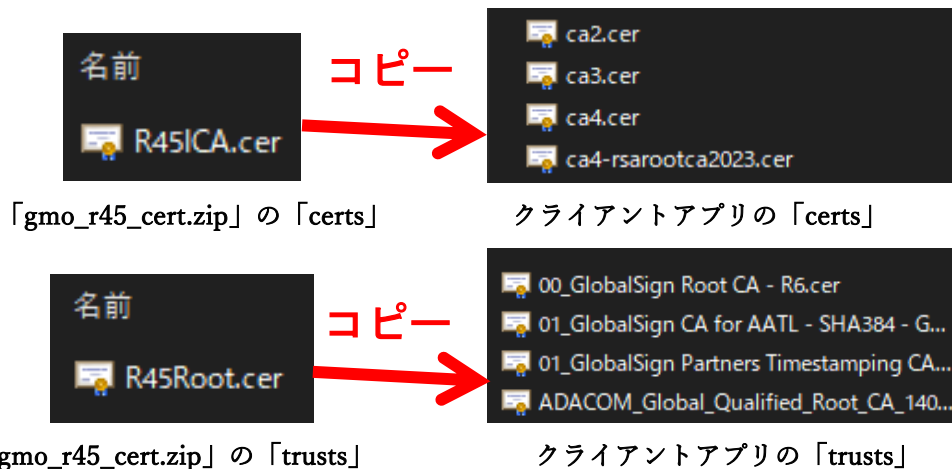
- ① クライアントアプリのインストール先を開きます。
- ② 「store」フォルダを開きます。



- 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_r45_cert」を開きます。



- ③ 「gmo_r45_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つに対しての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。

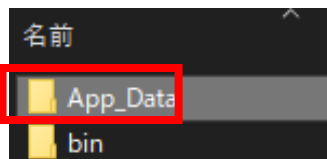
6.3 各種 Web アプリケーション について検証証明書を追加する手順

○ 対象となるアプリケーション

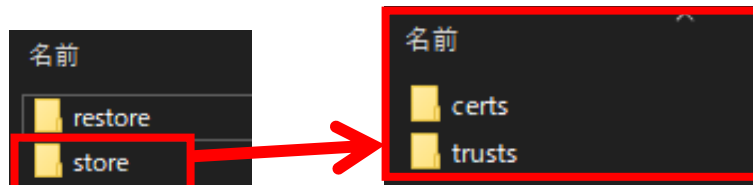
- Web 検索機能 (esuccess / scansave)
- リンクビュー (esuccesslinkview / scansavelinkview)

○ 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。



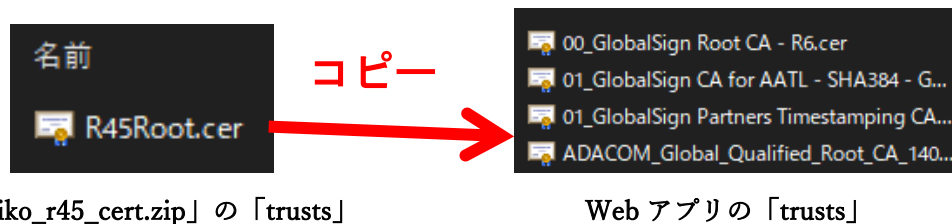
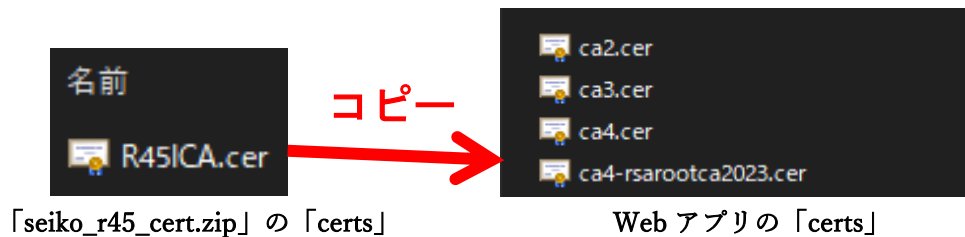
- ③ 「store」フォルダを開きます。



- 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_r45_cert」を開きます。



- ⑤ 「gmo_r45_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。



- ⑥ リンクビューについても①～⑤と同様の作業を行います。

7 CRL（証明書の失効情報）証明のインストール

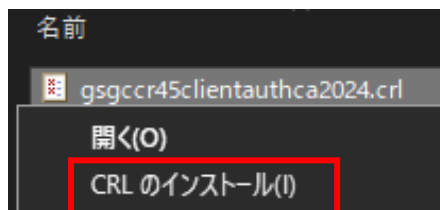
この項目では、2024年12月に変更したGMOグローバルサイン製を新しいルートCAと中間CAの失効情報をWindowsにインストールします。

以下の手順に従ってインストールしてください。

- 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_r45_cert」を開き、「valids」フォルダを開きます。



- ① ダウンロードした「gsgccr45clientauthca2024.crl」を右クリックし、「CELのインストール」を選択します。



- ② 証明書のインポートウィザードが開始されるので、「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。

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

- ③ 「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」を選択し、「次へ」をクリックします。

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

- ④ インポート内容に「証明書失効リスト」が確認できたら、「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:

選択された証明書ストア	ウィザードで自動的に決定されます
内容	証明書失効リスト

以上で、証明書失効リス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。

8 テスト(オプション)

2024年12月以降に発行した「GMO グローバルサイン」製の電子証明書へ更新して、その後、「[3 検証証明書ファイルをダウンロード](#)」「[4 追加方法\(Windows マシンへのインストール\)](#)」「[5 追加方法\(store フォルダへの追加\)](#)」「[6 CRL \(証明書の失効情報\) 証明のインストール](#)」の各対応完了後、電子証明書を動作確認する為に、下記の対応を実施していただく事をお勧めします。

- ① テスト用の書類を一度登録して、新しいURLでタイムスタンプ付与できるか確認
- ② ①が完了後、クライアントアプリ/Web 検索機能/リンクビューで書類検証を実行し、結果が「○」になるか確認

9 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。