

TDB 電子証明書の SYMANTEC 名義の現行ルート CA の運用が終了になる関係で、必要となる新ルート CA と中間 CA の追加方法

アンテナハウス 酒井

作成日: 2021 年 2 月 10 日

更新日: 2023 年 10 月 26 日

1 概要と背景

本稿は、ScanSave/e-Success のタイムスタンプ「XAdES」「PAdES 長期署名」で使用する新しいルート CA と中間 CA の追加方法について記載した文書になります。

中間証明書の追加が必要となりました背景は、2021 年 2 月 Microsoft と Apple 社などの各ブラウザベンダーによるルート証明書の信頼設定の変更と S/MIME 用証明書のプロファイル制限の意向を示したことから、弊社の取引先である帝国データバンクと開発会社のデジサート・ジャパンより、「TDB DigiCert 電子認証サービス Class2」が、2021 年 12 月 6 日(月)より新しい仕様となったからにあります。

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。

なお、TDB 電子証明書の Class2 証明書で利用中の Symantec 名義の現行ルート CA は 2023/3/31 に運用が終了となりますので、電子証明書を更新する際は、必ず本稿の対応を行ってください。

2 対象のユーザー

タイムスタンプの種類を「XAdES」もしくは「PAdES 長期署名」（署名&タイムスタンプ）を使用されている方

※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 追加方法

3.1 新しいルート CA の追加

この項目では、新しいルート CA の追加方法について、説明します。

①下記の URL にアクセスします。


- ・ DigiCert Trusted Root Authority Certificates

<https://www.digicert.com/kb/digicert-root-certificates.htm>

②ページにアクセスすると各種ルート CA のダウンロード URL が一覧で表示されます。
その中の「DigiCert Global Root G2」の「Download DER/CRT」をクリックして、新
ルート CA をダウンロードしてください。

Download PEM Download DER/CRT	SHA1 Fingerprint: A0:30:3D:3A:03:E3:E3:04:1 SHA256 Fingerprint: 43:48:A0:E9:44:4C:78:C Demo Sites for Root: Active Certificate
DigiCert Global Root G2 Download PEM Download DER/CRT	Valid until: 15/Jan/2038 Serial #: 03:3A:F1:E6:A7:11:A9:A0:BB:28:64:B1: SHA1 Fingerprint: DF:3C:24:F9:BF:D6:66:76: SHA256 Fingerprint: 0B:3C:0B:B7:60:31:E5: Demo Sites for Root: Active Certificate
DigiCert Global Root G3	Valid until: 15/Jan/2038 Serial #: 05:55:56:BC:F2:5E:A4:35:35:C3:A4:0F:1 SHA1 Fingerprint: ...

③ダウンロードした「DigiCertGlobalRootG2.crt」をダブルクリックします。

名前	更新
 DigiCertGlobalRootG2.crt	202

④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。

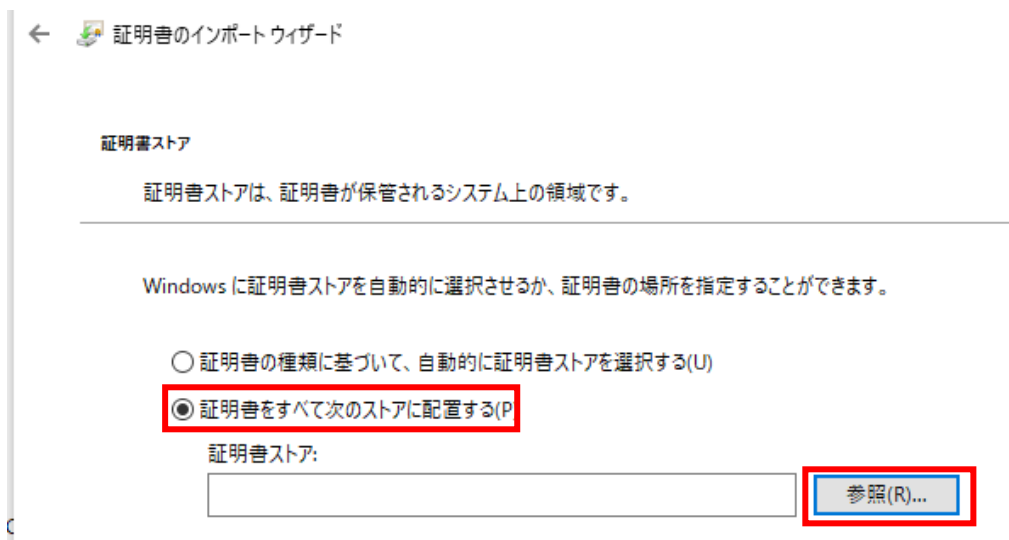
⑤ 「全般」タブの「証明書のインストール」をクリックします。



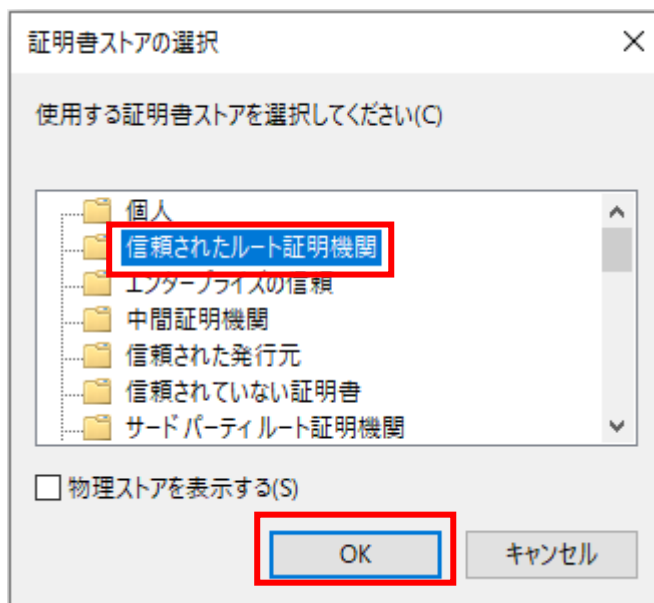
⑥ 「保存場所」を「ローカルコンピューター」で選択し、「次へ」をクリックします。




- ⑦ 「証明書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。



- ⑧ 「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。



⑨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。

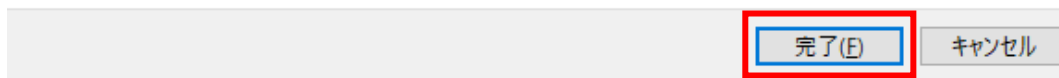
 証明書のインポートウィザード

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、「[3.2 新しい中間 CA の追加](#)」を行ってください。

3.2 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下記の URL にアクセスします。

- ・ DigiCert PKI Class2 中間 CA 証明書

https://www.digicert.co.jp/repository/intermediate/dc_pki_2_ca.html

②ページにアクセスすると中間 CA のダウンロード URL が表示されます。

「最新の DigiCert PKI Class2 Service オンライン CA 証明書のダウンロード」をクリックして、新中間 CA をダウンロードしてください。

デジサート・ジャパン トップ > リポジトリ > 中間CA証明書 > DigiCert PKI Class2中間CA証明書

DigiCert PKI Class2中間CA証明書

 ツイートする  いいね! 0

DigiCert PKI Class2 Service オンライン CA証明書

C = JP

O = DigiCert Japan G.K.

CN = Individual Certificate Issuance Service CA

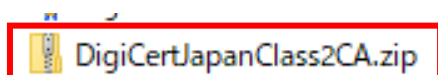
Serial Number: 0af7:60:fc:68:07:34:5f:5e:12:3d:55:90:79:93:9e

Operational Period: 03/11/2021 to 03/10/2036

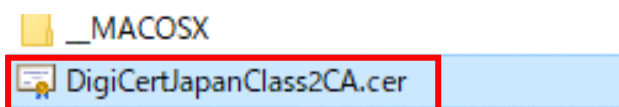
Certificate SHA1 Fingerprint: af:be:db:e2:1a:e2:4d:c2:7a:0c:81:6e:5c:c4:51:a9:fd:4d:a0:ff

- ・ [最新の DigiCert PKI Class2 Service オンライン CA 証明書のダウンロード](#)

③ダウンロードした「DigiCertJapanClass2CA.zip」を解凍します。



④解凍したファイルから「DigiCertJapanClass2CA.cer」をダブルクリックします。



⑤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。

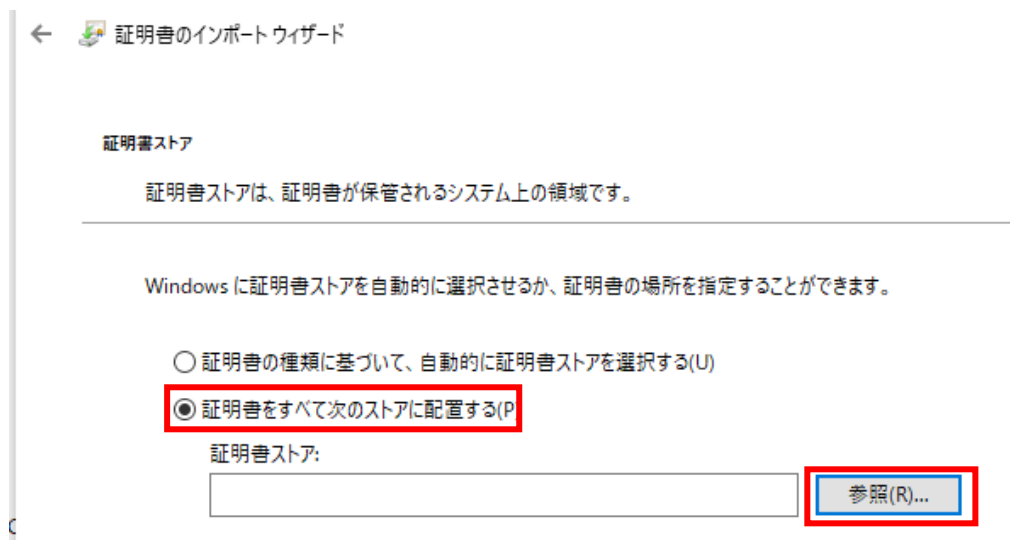
⑥ 「全般」タブの「証明書のインストール」をクリックします。



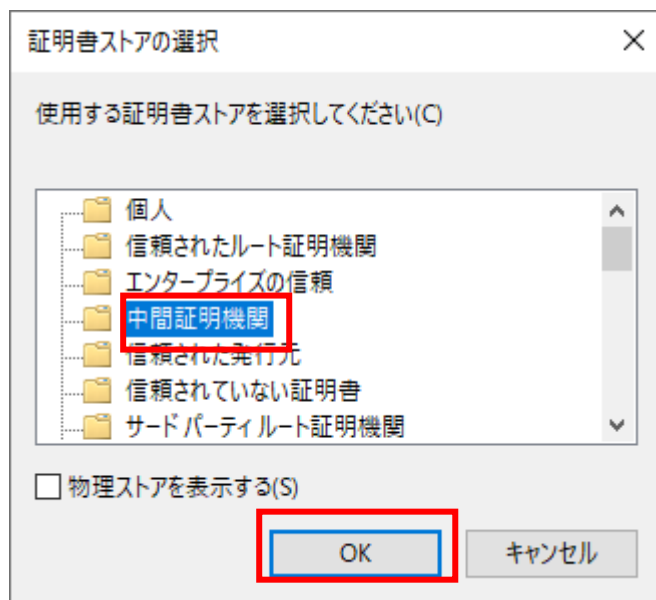
⑦ 「保存場所」を「ローカルコンピューター」で選択し、「次へ」をクリックします。




- ⑧ 「証明書すべてを次のストアに配置する」を選択し、「参照」をクリックします。



- ⑨ 「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。



⑩インポートする証明書のストアの確認ができれば、「完了」をクリックします。

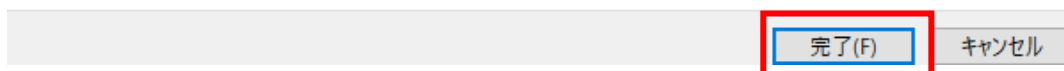
←  証明書のインポートウィザード

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。

4 CRL（証明書失効情報）証明のインストール

この項目では、2024年1月3日に失効する SYMANTEC 製の中間 CA 証明書とルート証明書の失効情報を Windows にインストールします。

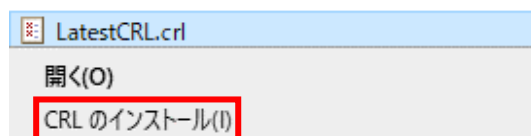
失効情報をインストールすることで、SYMANTEC 製の中間 CA 証明書とルート証明書の有効期限が切れた後、それらの証明書を排除し、新仕様で採用している Digicert 製の中間 CA 証明書とルート証明書を優先的に使用して、帝国データバンクの電子証明書によるタイムスタンプ付与処理あるいは検証処理を実行します。

以下の手順に従ってインストールしてください。

- ① 下記の URL にアクセスし、CRL ファイルをダウンロードします。

http://pki-crl.symauth.com/ca_0ae7dba2f378c9db5b4e41a029c73d38/LatestCRL.crl

- ② ダウンロードした「LatestCRL.crl」を右クリックし、「CEL のインストール」を選択します。



- ③ 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。



- ④ 「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

- ⑤ 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。

5 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