

T D B 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

2021/12/14 アンテナハウス（株）

1 概要と背景

この文書は、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 証明書と中間 CA 証明書の追加方法について記載したものです。

2021 年 2 月、Microsoft と Apple 社など、各ブラウザベンダーが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ため、これへの対応として、「TDB DigiCert 電子認証サービス Class2」が、2021 年 12 月 6 日(月)より新しい仕様に変更されることによります。

この変更に対応するため、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手順を以下に示します。

なお、T D B 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。電子証明書を更新される際は、必ずこの文書で示す作業を行って対応してください。

2 対象となるユーザー

タイムスタンプの種類として「XAdES」もしくは「PAdES 長期署名」を使用されているユーザー

なお、通常の「PAdES」を使用されているユーザー、及び e-Success V5.1.7 をご利用されているユーザーは、対象外です。

3 追加方法

3.1 新しいルート CA 証明書の追加

この項目では、新しいルート CA 証明書の追加方法について説明します。

適当な Web ブラウザを用いて以下に示す URL にアクセスします。

- ・ DigiCert Trusted Root Authority Certificates

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

アクセスすると各種ルート CA 証明書のダウンロード URL が一覧表示されます。

その中の「DigiCert Global Root G2」の「Download DER/CRT」をクリックして、新しいルート CA 証明書をダウンロードします。

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

ダウンロードした「DigiCertGlobalRootG2.crt」をダブルクリックして、これを開きます。

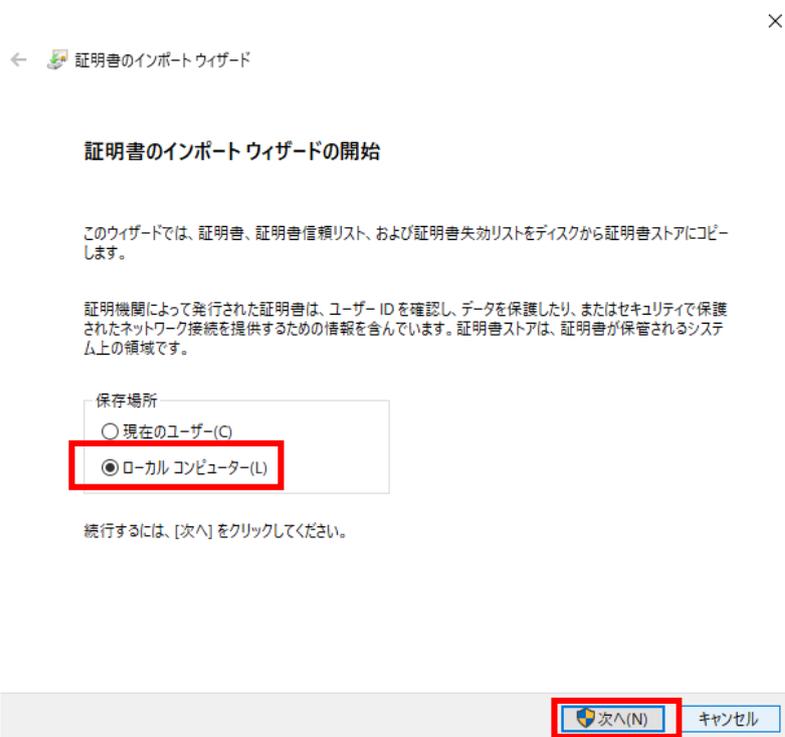
名前	更新
 DigiCertGlobalRootG2.crt	202

この時、セキュリティ警告が表示されますが、そのまま「開く」をクリックして、先に進めます。

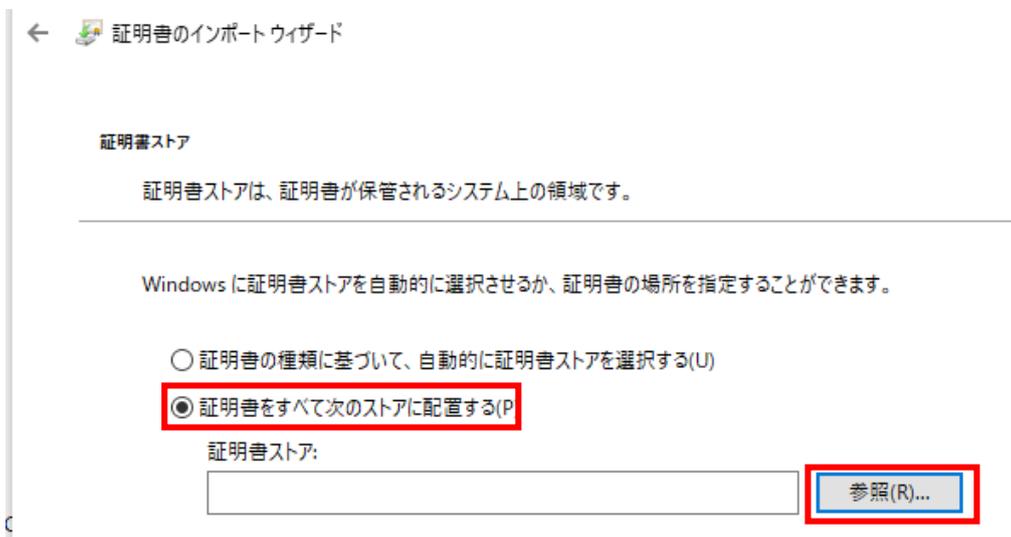
「全般」タブの「証明書のインストール」をクリックします。



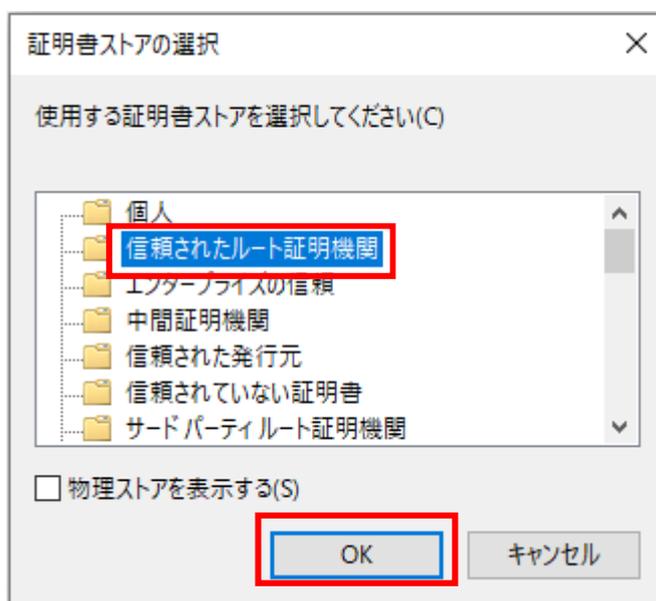
「保存場所」として「ローカルコンピューター」を選択し、「次へ」をクリックします。



「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。



「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。



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

完了(F)

キャンセル

以上で、新ルート CA 証明書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 証明書の追加](#)」を行います。

3.2 新しい中間 CA 証明書の追加

この項では、新しい中間 CA 証明書の追加方法について説明します。

適当な Web ブラウザを用いて以下の 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

アクセスすると中間 CA 証明書のダウンロード 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 をダウンロードします。

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

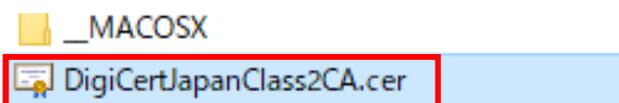
Certificate SHA1 Fingerprint: af:be:db:e2:1a:e2:4d:c2:7a:0c:81:6e:5c:c4:51:a9:fd:4d:a0:ff

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

ダウンロードした「DigiCertJapanClass2CA.zip」を適当なフォルダに解凍します。



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

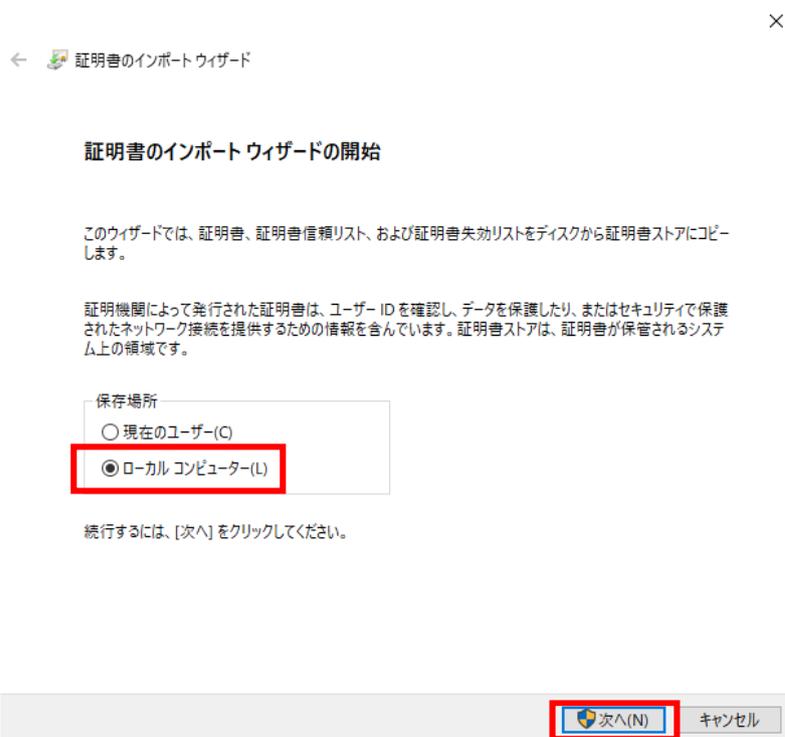


セキュリティ警告が表示されますが、そのまま「開く」をクリックしてこれを開きます。

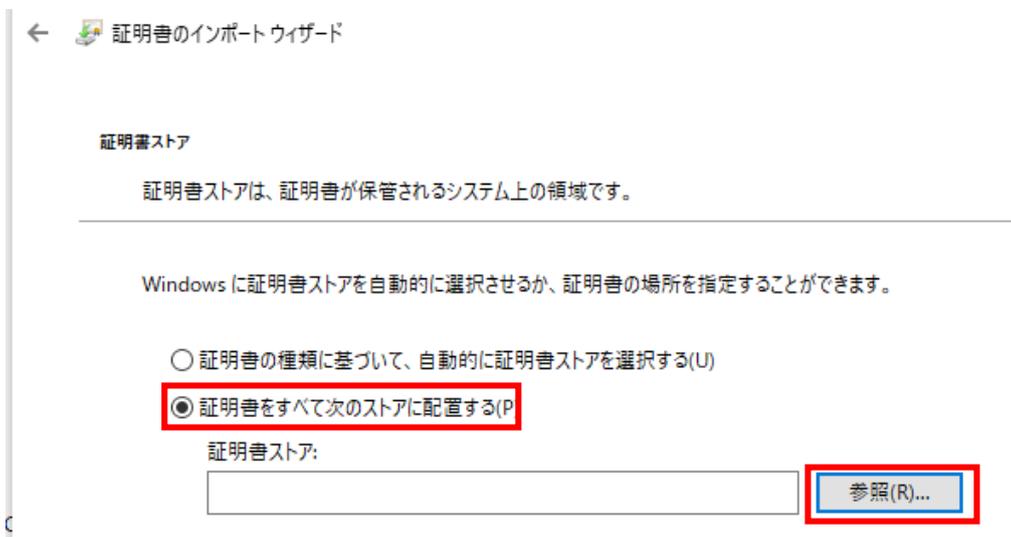
「全般」タブの「証明書のインストール」をクリックします。



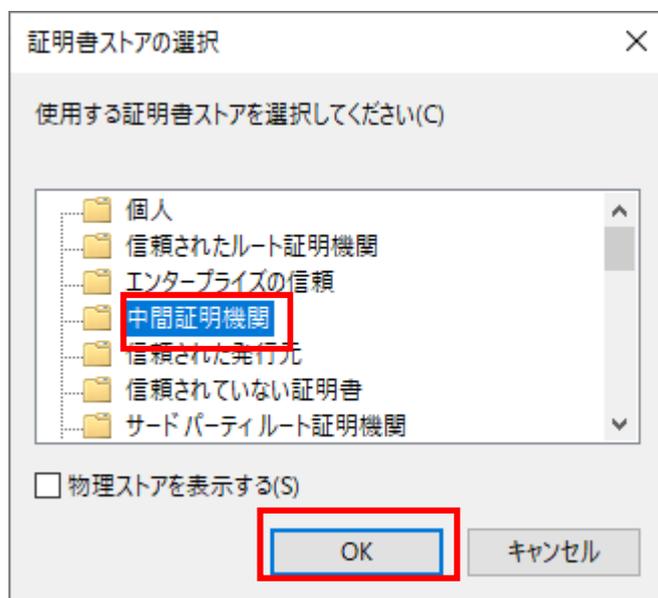
「保存場所」を「ローカルコンピューター」で選択し、「次へ」をクリックします。



「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。



「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。



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	中間証明機関
内容	証明書

完了(F)

キャンセル

以上で、新中間 CA 証明書のインポートは完了です。「OK」をクリックして、画面を閉じてください。

4 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、下記に示す弊社サポートセンターまで、電子メールにてお問い合わせください。

お問い合わせいただく際には、質問内容をできるだけ具体的に記述していただきますようお願いいたします。

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