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

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、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。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 ルート CA 証明書をダウンロードします。

Download PEM   Download DER/CRT	SHA15 Higerprint: 40:90:50:54.05:25:25:24:4 SHA256 Fingerprint: 43:48:A0:E9:44:40:78:0 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: CB:3C:CB: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。

	明書の情報	
この証明書	の目的:	
• 9Ŧ	-トコンピューターに ID を証明する	
• ソフ	トウェアがソフトウェア発行者の送信であるか確認する	
•公	見後のソフトワエアの変更を禁止する スメールを促进する	
	先: DigiCert Global Root G2	
発行	者: DigiCert Global Root G2	

「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 〇 現在のユーザー(C) ④ 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

「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。
	<ul> <li>○ 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)</li> <li>● 証明書をすべて次のストアに配置する(P</li> </ul>
:	証明書ストア: 参照(R)

「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。

証明書ストアの選択	×
使用する証明書ストアを選択してください(C)	
	^
信頼されたルート証明機関	
- エノジェノフィスの信視	
「「「「「「「「「「「」」」」「「「」」」「「」」」「「」」」「「」」」「	
「「「「「「「「「」」」」	
	~
└── 物理ストアを表示する(S)	
ОК	キャンセル

インポートする証明書のストアの確認ができたら、「完了」をクリックします。

髪 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。

火り設定が損化されました
--------------

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( <u>F</u> )	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: 0a:f7:60: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

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

DigiCertJapanClass2CA.zip

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

\_\_MACOSX

🔄 DigiCertJapanClass2CA.cer

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。

💼 証明	書		×
全般	詳細 証明	ຄຸກ/ເລ	
-	<ul> <li>説明書の目的:</li> <li>リモートコン</li> <li>2.16.840.1</li> </ul>	情報 ビューターに ID を証明する .114412.3.25	-
-	発行先:	Individual Certificate Issuance Service CA	
	発行者:	DigiCert Global Root G2	
	有効期間 2	021/03/11 <b>/ሶら</b> 2036/03/11	
		証明書のインストール(I) 発行者のステートメント(S)	

「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。

Х

÷	☞ 証明書のインボート ウイザード
	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 〇 現在のユーザー(C) ④ 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

「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)

「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。

証明書ストアの選択	×
使用する証明書ストアを選択してください(C)	
	^
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	
サードパーティルート証明機関	¥
□ 物理ストアを表示する(S)	
OK キャンセノ	L

インポートする証明書のストアの確認ができたら、「完了」をクリックします。

← ಶ 証明書のインポート ウィザード

証明書のインオ	ペート 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
Let a set		

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<u>具体的に</u>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