電子定款や本人確認情報などのPDFファイルに日司連カードで行った電子署名を検証すると「無効」などと表示される

時々、電子定款や本人確認情報などのPDFファイルに日司連カードで行った電子署名を 検証すると「無効」あるいは「ルート証明書が得られません」などと表示されるがどうした らよいかという質問を受けます。

この現象は、電子証明書の発行者である司法書士認証局の自己署名証明書が、署名を検証 するパソコンにインストールされていないため、PDFファイルに電子署名した場合に、次 のように、証明書の信頼性が確認できない旨の警告が発せられるものです。

	SkyPDF Pro CA Edition の場合		Adobe Acrobat+		
	,			電子認証キット Pro	(リーガル社)の場合
電子署名アイコン	離別名 2005 日日日 2005年 理理 場所 名前、並木 一地			識別名:200 副年:200 理由 場所 1 金本	
	SkyPDF Pro CA E	idition V2 署名	青報 🕅	$\mathcal{I} \oplus \mathcal{R} \neq \epsilon$	×
	署名情報署名横	IF		署名検証状況: 有効(証明書未確認)	<u>a</u>
	検証結果: 無効 検証目時: 2008/02/15 18:40:06+09:00			著名者: 鈴木 一也 著名曰時: 2008/02/15 18:24:05 著名地: 理由: Filter: MOUSignDoc SubFilter: adbe.pkcs7.detached	+09'00'
	署名本人性	但 977月97日版 使言止	有効期間内です		王明書チェック
		(言頓性橋証	(言語)ないのにかればうてきません。		・ ルート証明書が得られません
	文書完全性	文書改ざん検証	なざんはありません		OK 2
奥				証明書の有効性を確認する場合には「証明 証明書の内容を確認する場合には「証明	[明書有効性確認」を押してください。 書詳細表示」を押してください。
名検	 閉じる(<u>©</u>)			証明書詳細表示	[証明書有効性確認] 閉じる
証				有効性確認結果	
和果の画面				ルート証明書が自己署名証明書でん	ごはないので有効性確認できませ 🚿
				証明書の有効性確認結果をファ 結果を保存」を押してください	イルに保存する場合は、「確認
				確認結果を保存	* 閉じる

※Adobe Acrobat+電子認証キット Pro の場合は、SkyPDF Pro CA Edition が1 画面で表示する内容を2 画面に分割しているものの、表現している内容は同じです。

「司法書士認証局の自己署名証明書」とは、書面で言えば司法書士認証局の印鑑証明書に 相当する電子証明書だと思えばよいでしょう。これと署名者の電子証明書(作成名義人は司 法書士認証局です)を照合することによって、当該電子署名に使用された電子証明書が真正 なものかどうかが確認できるのです。ということは、これがインストールされていないパソ コンで日司連カードによる電子証明書を使って電子署名しても、電子証明書の有効・失効以 前に、その電子証明書が真正な物かどうかが確認できないということになるので、これをも って有効な電子署名がなされたと判断することはできないのです(電子証明書の失効状態検 証とは、失効リストと照合するだけであって、失効リストに記載がないものはすべて「有効」 と判定されます)。仮に、これを確認しないまま済ませても、司法書士認証局の自己署名証明 書がインストールされているシステムでそのファイルを読み込んで署名検証を行えば、電子 証明書の真正性が確認できるので、支障ないといえない事もないのですが、作成の時点で真 正性が確認できない電子定款や本人確認情報を提供することはやはり問題でしょう。したが って、上記の警告が発せられる場合は、司法書士認証局の自己署名証明書をパソコンにイン ストールしたうえで、当該電子署名を検証しておかなければならないのです。司法書士認証 局の自己署名証明書は、インターネットの司法書士認証局の証明書情報のページからダウン ロードし、インストールすることができます。手順を以下に示します。

①司法書士認証局の証明書情報のページ(https://ca2.nisshiren.jp/repository/info.html) にアク セスし、下図赤囲みの「こちら」の文字をクリックします。

司法書士認証サービス Chiho-Shoshi Lawyer Inthentication Service						
HOME	┃ 証明書情報					
認証業務規程(CPS)	 認証局証明書のフィンガーブリント 					
利用規約・利用料金	フィンガーブリント値	8E5B 3FD8 B787 44D5 1173 BDAC 7742 2C81 8C5A 7400				
証明書情報	ハッシュ関数	SHA-1				
	有効期間	2007年08月07日~2017年08月06日				
申請書類	シリアル番号	01				
文字情報 ICカードR/W FAQ	 認証局証明書はこさ ※案名検証を行うにお 	らからダウンロードできます。 あたり、あらかにめ認証局証明書をインストールしておく必要				
問い合わせ先	る場合があります。言	認定は、ののののののののののののです。 認定局証明書のインストール方法については <u>こちら</u>				
過去のお知らせ	V.C.V.	Get Adobe Reade				



 ファイルのダウンロード」のダイアログが表示 されますので、開く(0) ボタンをクリックしてく ださい(ここで 保存(S) ボタンをクリックすれば 司法書士認証局の自己署名証明書を保存しておくこ とができます)。



証明書のインボートウィザード

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。

dows 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。

○説明書の確認に基づいて、自動的に説明書ストアを選択するUN ○説明書をすべて次のストリに記載するUP ③司法書士認証局自己署名証明書の情報が表示されます (「詳細」のタブをクリックすれば詳しい情報が表示され ます)。画面下部の 証明書のインストール() ボタンを クリックします。

④「証明書のインポート ウィザード」が開始します(要 するに証明書をインストールするための設定を行なう のです)。画面下部の 次へ(N)> ボタンをクリック します。

⑤証明書ストア(証明書のインストール先)を指定し ますが、最初にチェックされていた「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」のまま 画面下部の 次へ(N)> ボタンをクリックします。



112 (S).

<度る图 (次へゆ) キャンセル

⑥「証明書のインポート ウィザードの完了」画面が表示されます。画面下部の 完了 ボタンをクリックすると「セキュリティ警告」画面が表示されます。

セキュリテ	·警告 ×					
<u>.</u>	発行者が次であると主張する証明機関 (CA) から証明書をインストールしようとしています: Shiho-Shoshi Lawyer's CA					
	証明書が美国に、Shino-Shoshi Lawyer's CA からのものであるがとうがを復証できません。 Shino-Shoshi Lawyer's CA に連絡して発行者を確認す る必要があります。次の番号はこの過程で役立ちます:					
	(地印 (sha1): 8E5B3FD8 B78744D5 1173BDAC 77422C81 8C5A7400					
	警告: このルート証明書をインストールすると、この CA によって発行された証明書は自動的に信頼されます。確認されていない担印付きの証明書をインストールす ることは、セキュリティ上、危険です。[はい] をクリックすると、この危険を認識したことになります。 この証明書をインストールしますか?					

⑦この画面では、自己署名証明書の名義人と「拇印」を表示しています。

ここでは、「名義人は Shiho-Shoshi Lawyer's CA である『と主張している』」旨の表示をして います。わざわざこのようなもったいつけた言い回しをすることの意味は、「ここではまだ『自 称』であって、この証明書に記載された拇印が真正なものと一致していることを確認するま では『名義人は Shiho-Shoshi Lawyer's CA である』と認めることはできない」ということを 表しているのです。万一、自己署名証明書が改ざんされていると、これとの照合によって「真 正」と判断される電子証明書の信頼性はすべて無意味になってしまうので、拇印の照合は必 ず行なってください。念のため説明してあくと、拇印と言っても日司連会長や認証局の局長 の親指の指紋が登録されているわけではありません。司法書士認証局の自己署名証明書に、

ある演算を行った結果の値を「拇印」もしくは「フィンガープリント」と呼んでいるのです (前ページの「セキュリティ警告」画面では「拇印」と表示し、後述の証明書情報ページで は「フィンガープリント」と表示していますが、同じことです)。この演算で使われる関数を ハッシュ関数と呼び、得られた値をハッシュ値と呼びます。「拇印」もしくは「フィンガープ リント」とは、この「ハッシュ値」のことです。この値が前ページの警告メッセージに表示 された値と一致していれば、この「司法書士認証局の自己署名証明書は真正なものである」 と確認できるわけです。真正な司法書士認証局の拇印(=フィンガープリント)の値は、先 ほどの司法書士認証局の証明情報のページに記載されています。

フィンガープリント値	8E5B 3FD8 B787 44D5 1173 BDAC 7742 2C81 8C5A 7400
ハッシュ関数	SHA-1
有効期間	2007年08月07日~2017年08月06日
シリアル番号	01

左図の赤囲みの値が真正な司法書士認証局の拇 印の値です。これと、前ページー番下の図の中 ほどに表示されている値が完全に一致していれ ばインストールしようとしている自己署名証明 書の真正性は確認されますので、必ず確認して ください。なあ、ここでは4桁区切り、「セキュ

リティ警告」画面では8桁区切りになっていますが、これは問題ではありません。



これで<u>はい(Y)</u>ボタンをクリックすると、証明書のインストールが行われ、完了すると左のメッセージが表示されます。これで司法書士認証局の自己署名証明書のダウンロード及びインストールは完了しました。 これで、前に「無効」あるいは「ルート証明書が得られません」などと

表示された電子署名を再度検証すれば正常に検証できるはずです。