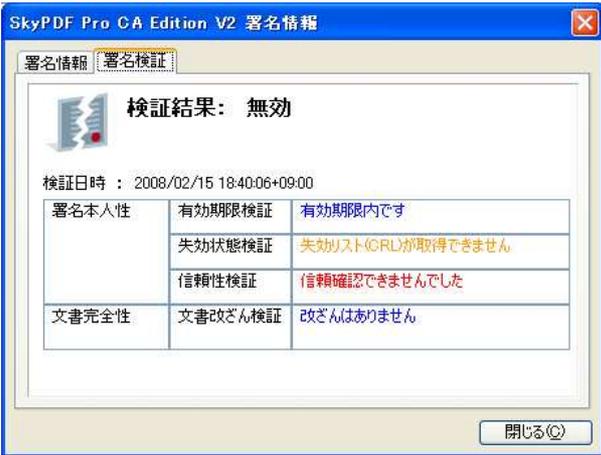
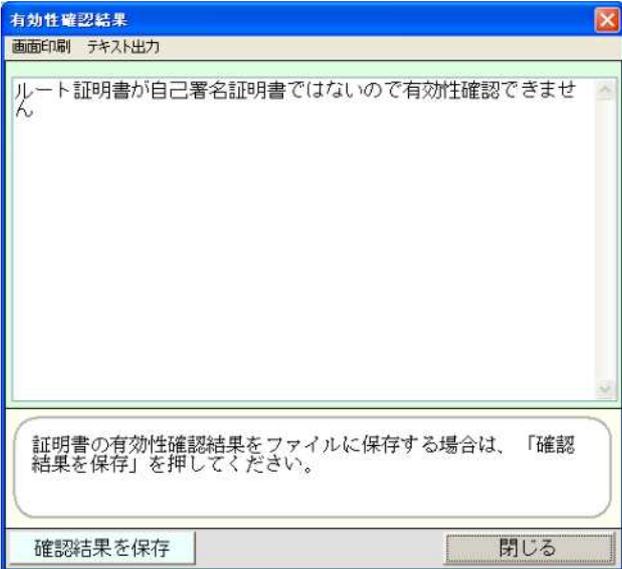


電子定款や本人確認情報などのPDFファイルに日司連カードで行った電子署名を検証すると「無効」などと表示される

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。

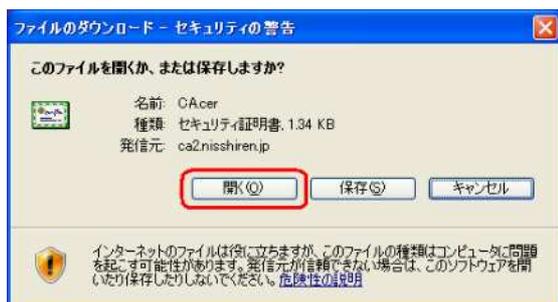
この現象は、電子証明書の発行者である司法書士認証局の自己署名証明書が、署名を検証するパソコンにインストールされていないため、PDFファイルに電子署名した場合には、次のように、証明書の信頼性が確認できない旨の警告が発せられるものです。

	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		
署名検証結果の画面		 

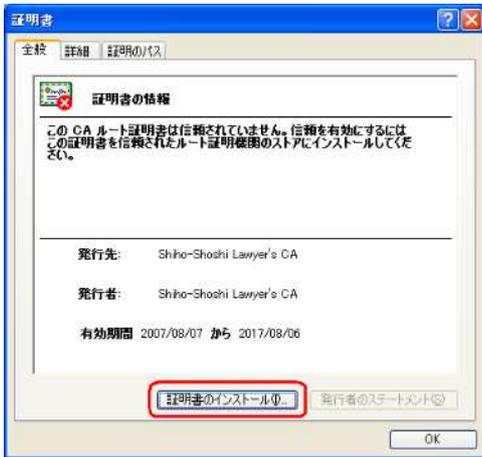
※Adobe Acrobat+ 電子認証キット Pro の場合は、SkyPDF Pro CA Edition が 1 画面で表示する内容を 2 画面に分割しているものの、表現している内容は同じです。

「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を確認できるのです。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を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。

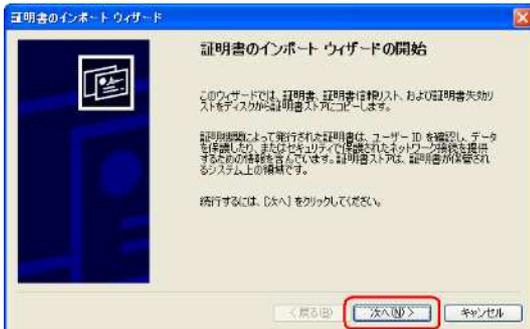
- ①司法書士認証局の証明書情報のページ (<https://ca2.nisshiren.jp/repository/info.html>) にアクセスし、下図赤囲みの「こちら」の文字をクリックします。



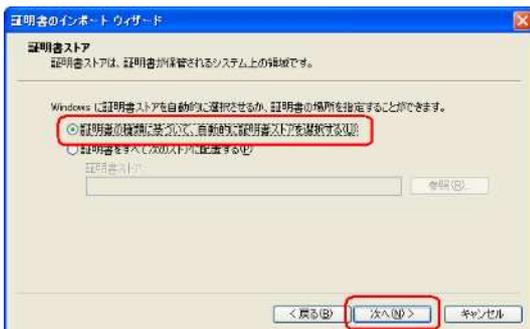
②「ファイルのダウンロード」のダイアログが表示されますので、**開く(O)** ボタンをクリックしてください（ここで **保存(S)** ボタンをクリックすれば司法書士認証局の自己署名証明書を保存しておくことができます）。



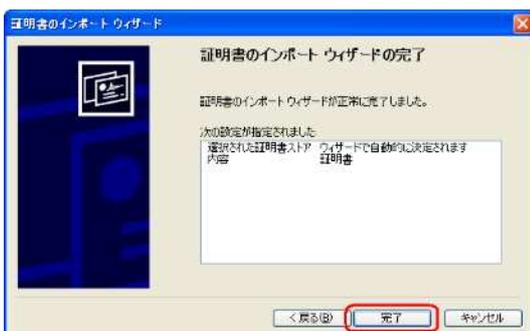
③司法書士認証局自己署名証明書の情報が表示されます（「詳細」のタブをクリックすれば詳しい情報が表示されます）。画面下部の「証明書のインストール(I)」ボタンをクリックします。



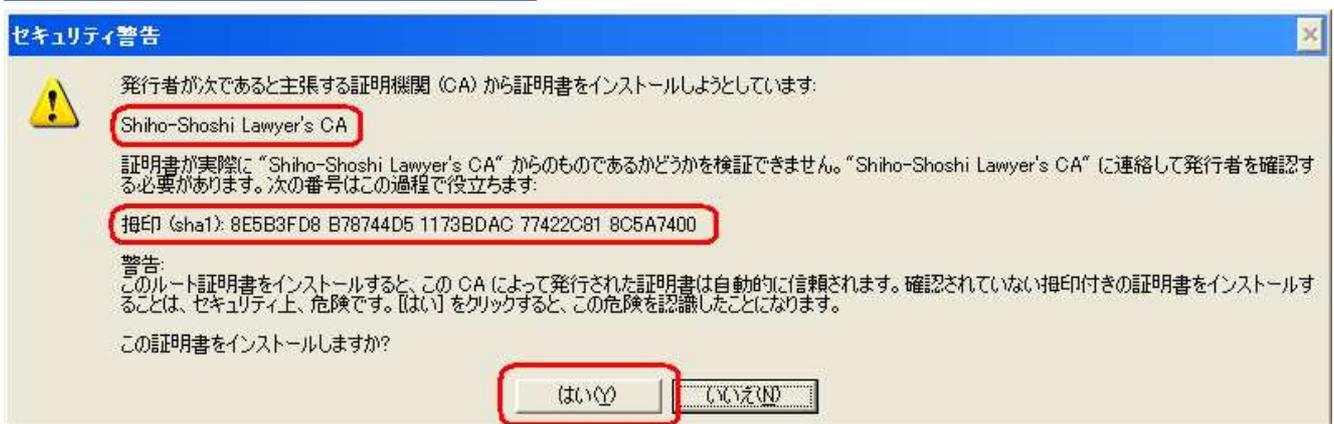
④「証明書のインポート ウィザード」が開始します（要するに証明書をインストールするための設定を行なうのです）。画面下部の「次へ(N) >」ボタンをクリックします。



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。



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。



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。念のため説明しておくと、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、前ページ一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。なお、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 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。