

Acrobat (Reader) を使った 1-2-3 証明書による電子署名



初版: 2020 年 10 月 3 日
改訂第二版: 2021 年 9 月 30 日
改訂第三版: 2023 年 10 月 13 日
改訂第四版: 2023 年 12 月 4 日

インフラウェア株式会社

内容

1	1-2-3 証明書のインストール.....	3
2	Acrobat の設定.....	3
2.1	証明書の確認.....	3
2.2	署名方法の設定.....	4
2.3	タイムスタンプサーバの設定.....	5
2.4	署名プロファイルの作成.....	9
2.5	署名検証方法の設定.....	12
3	PDF ファイルに電子署名する.....	14
4	トラブルシューティング.....	18
4.1	証明書パス.....	18
4.2	信頼の状態.....	20
4.3	失効情報の確認.....	21

この文書は、Windows 10 または Windows 11 上の Acrobat を用い、1-2-3 証明書で PDF に電子署名する方法を説明したものです。Acrobat は Standard 版だけでなく、無償で利用できる Acrobat Reader も利用できます。

Windows、Acrobat は 2023 年 12 月現在の最新版を用いて説明しています。バージョンアップ等により GUI (画面) や操作が変更になる可能性もあることは、ご了承ください。

1 1-2-3 証明書のインストール

まず、入手した 1-2-3 証明書を Windows の「証明書ストア」に導入します。お手元の PC に 1-2-3 証明書ファイルを用意してください。当社で発行した 1-2-3 証明書は、お客様が Web 経由でダウンロードすることで入手できます。手順の詳細については、Web サイト

<https://www.infra-ware.net/jcan/get-123/>

<https://www.infra-ware.net/jcan/install-123/>

をご覧ください。

2 Acrobat の設定

2.1 証明書の確認

最初に、Acrobat で 1-2-3 証明書が利用可能になっていることを確認します。Acrobat を起動して、以下の手順に従ってください。

1. [メニュー] > [環境設定] をクリックします。

以下のようなダイアログが表示されますので、左側の [署名] をクリックします。

次に、右側の [ID と信頼済み証明書] の項の [詳細] ボタンをクリックします。

※ Acrobat がバージョンアップされ、操作メニューが変わっています。古いバージョンの Acrobat をお使いの場合は [編集] > [環境設定] と進みます。以下、この文書では読み替えてください。

Acrobat (Reader) を使った 1-2-3 証明書による電子署名



2. 以下のようなダイアログが表示されます。
左側の [デジタル ID] を選択し、右側に Windows 証明書ストアにインストールした 1-2-3 証明書が表示されていることを確認してください。



3. ここに自分の 1-2-3 証明書が表示されていれば、Acrobat による電子署名の基本的な準備は完了しています。

2.2 署名方法の設定

この項目は必須です。この設定は、長期検証を有効にし、証明書の有効期限を超えて文書を保存するために必要です。

1. Acrobat を起動します。
起動後、[メニュー]>[環境設定] をクリックします。
以下のようなダイアログが表示されますので、左側の [署名] をクリックします。
次に、右側の [作成と表示方法] の項の [詳細] ボタンをクリックします。

Acrobat (Reader) を使った 1-2-3 証明書による電子署名



2. 以下のようなダイアログが表示されます。
ここで [デフォルトの署名形式] を図のように、また [署名の失効ステータスを含める] にチェックを入れてください。



2.3 タイムスタンプサーバの設定

電子署名そのものにはタイムスタンプは必須ではありませんが、長期検証を有効にし、証

Acrobat (Reader) を使った 1-2-3 証明書による電子署名

明書の有効期限を超えて文書を保存するためには必要です。ご自身で契約したタイムスタンプサーバを利用できる場合は、ここで設定しておくことで、電子署名にタイムスタンプを付加することができます。タイムスタンプの指定がない場合は、埋め込みタイムスタンプとして、署名に用いた (Acrobat を動作させている) PC の内部時計が用いられます。

なお

<https://www.infra-ware.net/support/freetsa/>

に、無償で利用できるタイムスタンプサーバの情報を掲載してあります。特に上記 Web サイト上にある SSL.com のタイムスタンプサーバは、認証局の証明書が Adobe に認定されており (AATL 対応)、検証に特別な設定が不要です。SSL.com のタイムスタンプサーバをご利用ください。

電子帳簿保存法・スキャナ保存制度用途など、認定事業者のタイムスタンプサーバが必要な場合は、別途認定事業者と契約してください。事業者より発行された URL、ID、パスワードを設定することで、タイムスタンプが利用できます。

1. Acrobat を起動します。

起動後、[メニュー]>[環境設定] をクリックします。

以下のようなダイアログが表示されますので、左側の [署名] をクリックします。

次に、右側の [文書のタイムスタンプ] の項の [詳細] ボタンをクリックします。



2. 以下のようなダイアログが表示されます。

上部の [新規] ボタンをクリックしてください。

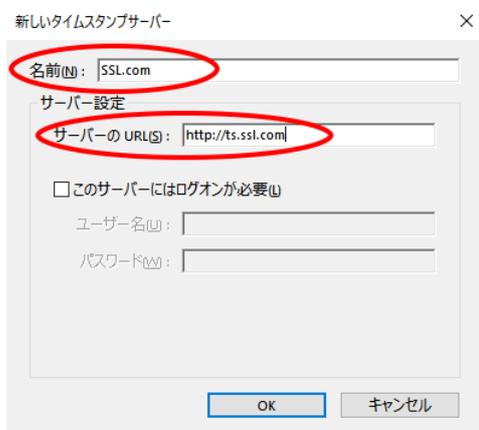


3. 以下のような、タイムスタンプサーバを設定するダイアログが表示されます。

[名前] には、サーバを表す適当な文字列を指定します。

[サーバ URL] には、タイムスタンプサーバの URL を指定します。タイムスタンプサーバに認証が必要な場合は [このサーバにはログオンが必要] をチェックし、指定された [ユーザ名] および [パスワード] を指定します。

入力完了後、[OK] ボタンをクリックしてダイアログを閉じます。

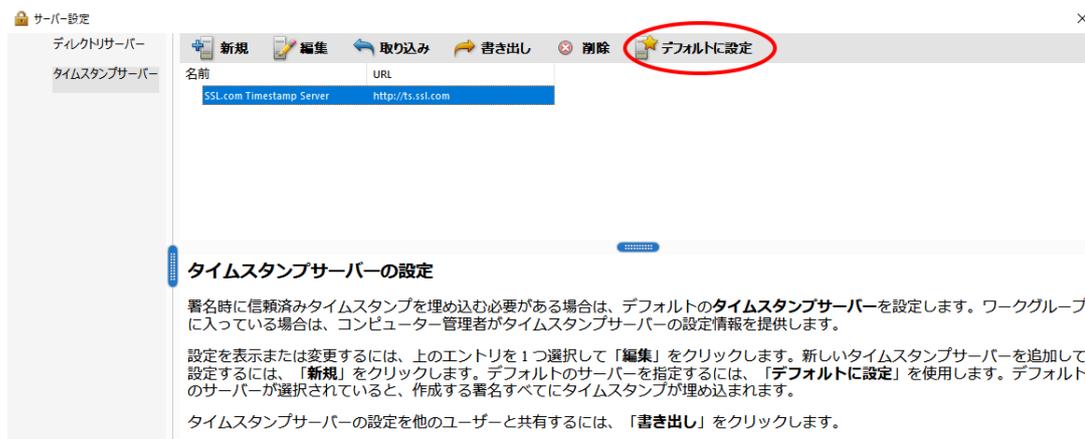


4. 下記のように、登録済みタイムスタンプサーバの一覧に、設定したサーバが追加されています。

追加したタイムスタンプサーバ名を選択した状態で、上部の [デフォルトに設定] ボタンをクリックします。

このダイアログは、右上の [X] で閉じてください。

Acrobat (Reader) を使った 1-2-3 証明書による電子署名



5. 以上でタイムスタンプサーバの設定は完了です。

2.4 署名プロファイルの作成

この項目は必須ではありません。署名のプロファイルを作成することで、あらかじめ登録した印影や自署画像などを、PDF 上に見える形で付けることができます（下図の例 2 点、これを可視署名と言います）。



電子署名者: TEST
DN: c=JP, st=Tokyo, l=Minato, ou=OU2-jipdec-00118(test), ou=OU1-1.2.392.200063.80.1.1(test purpose only), o=JIPDEC, cn=TEST
理由: この文書の正確さおよび完全性を証明する
場所: 横浜市
日付: 2020.06.29 17:03:16 +09'00'

藤原敏樹

電子署名者: BN-
Fujiwara.Toshiki(Infragistics)-RD001
理由: この文書の正確さおよび完全性を証明する
場所: 横浜市
日付: 2020.06.29 17:03:54 +09'00'

また、右側に表示される項目（名前、場所など）の取捨選択も可能です。

1. Acrobat を起動します。

起動後、[メニュー]>[環境設定] をクリックします。

以下のようなダイアログが表示されますので、左側の [署名] をクリックします。

次に、右側の [作成と表示方法] の項の [詳細] ボタンをクリックします。



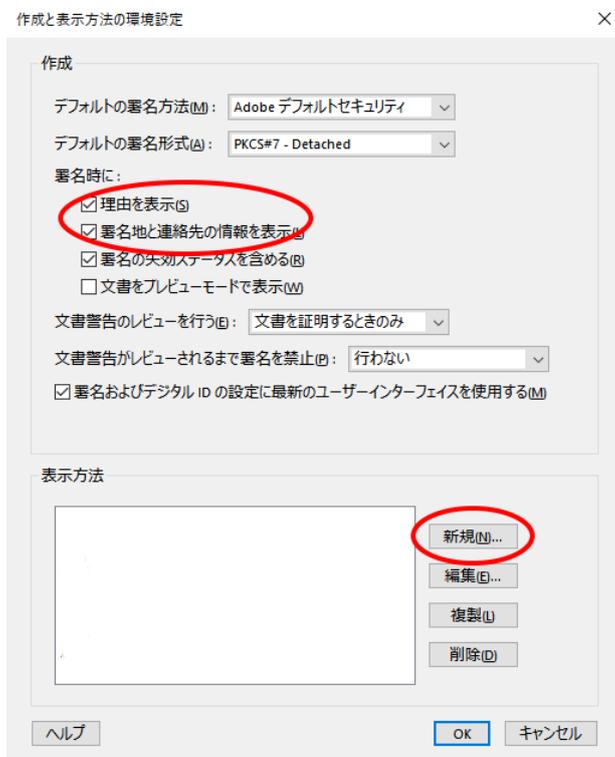
2. 以下のようなダイアログが表示されます。

ここで [理由を表示]、[署名地と連絡先の表示] にチェックを入れると、署名時にこれ

Acrobat (Reader) を使った 1-2-3 証明書による電子署名

らの情報を入力することができ、可視署名の右側に表示することができます。これらの項目は署名の有効性には影響せず、必須ではありません。

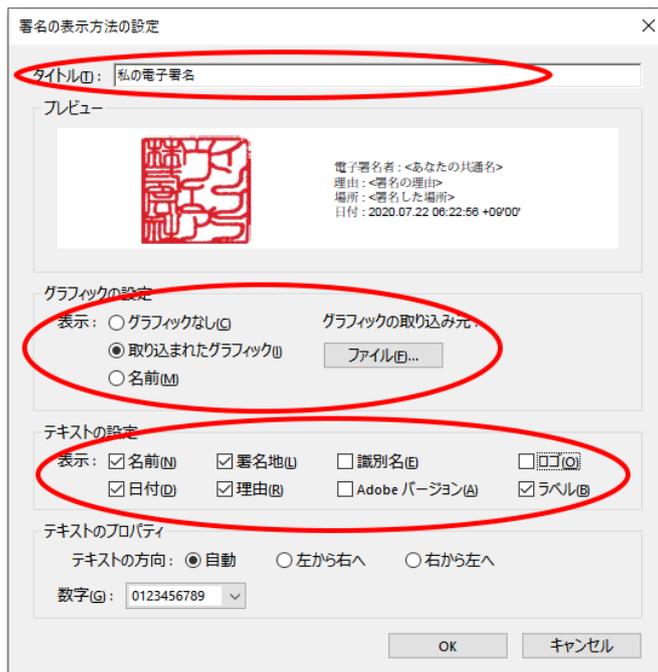
下段の表示方法の項にある [新規] ボタンをクリックします。



3. 以下のようなダイアログが表示されます。

[タイトル] には適切なプロファイル名を指定してください。

[グラフィックの設定] では、署名欄の左側に表示する内容を選択します。



ここで、[取り込まれたグラフィック] を指定すると、右側の [グラフィックの取り込み元] で PC 上のファイルを指定できます。あらかじめ用意しておいた自署イメージや印影ファイルを指定すると、その画像が表示可能です。ただし、画像は JPEG や PNG は指定できず、PDF である必要があります。あらかじめ PDF 化しておいてください。JPEG などから PDF に変換するには、

https://www.ilovepdf.com/ja/jpg_to_pdf

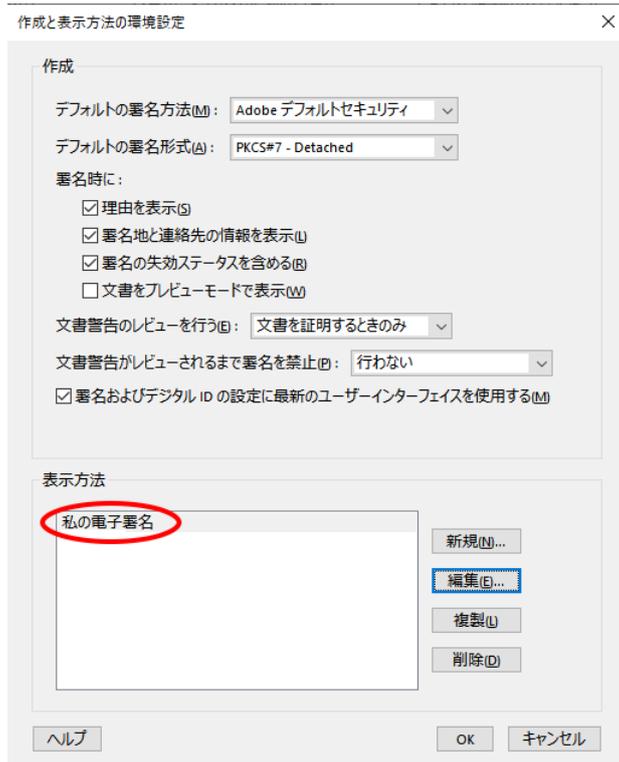
のようなサイトが利用可能です。

また、[テキストの設定] で [署名地] や [理由] にチェックを入れると、それらの情報が可視署名の右側に表示されるようになります。これらの表示項目も署名の有効性には影響しません。すべて任意です。

設定後 [OK] ボタンをクリックしてダイアログを閉じてください。

4. 以下のように [表示方法] 一覧に、作成したプロファイルが追加されているのを確認できます。

[OK] ボタンをクリックし、ダイアログを閉じてください。

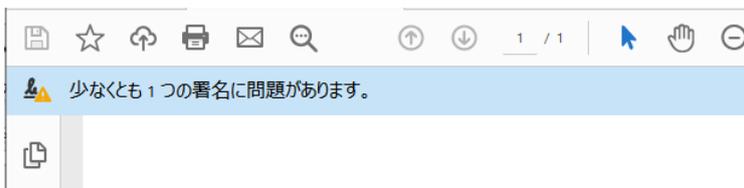


5. 以上で署名プロファイルの設定は完了です。

2.5 署名検証方法の設定

この項目は必須です。ここでは、作成された署名を検証するための設定をおこないます。

未設定の状態ですら署名済みの PDF を開くと、Acrobat の画面左上に、下図のように「少なくとも、1つの署名に問題があります」と表示されます。



これは、1-2-3 証明書の認証局を Acrobat が認識していないためで、以下の設定で認識させ、正常に検証させることができます。

1. Acrobat を起動します。

起動後、[メニュー]>[環境設定] をクリックします。

以下のようなダイアログが表示されますので、左側の [署名] をクリックします。

次に、右側の [検証] の項の [詳細] ボタンをクリックします。

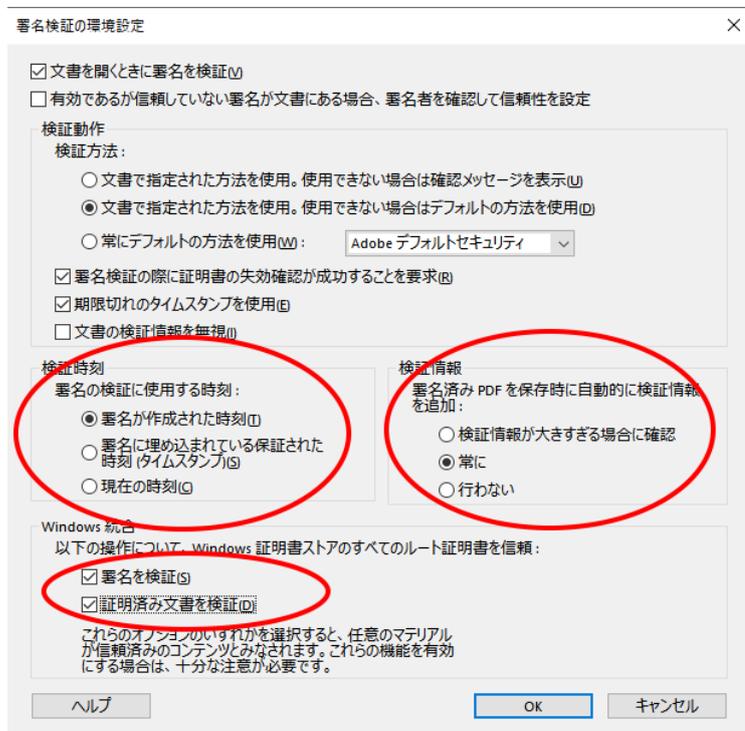


2. 以下のようなダイアログが表示されます。すべて図の赤丸のようにチェックを入れてください。

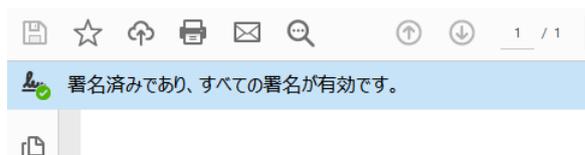
Windows には、1-2-3 認証局の上位認証局である GlobalSign の証明書がプリインストールされています。すなわち、Windows 上では GlobalSign 配下の証明書はすべて有効と認識されます。

Acrobat (Reader) を使った 1-2-3 証明書による電子署名

Windows 統合の項の [署名を検証]、[証明済み文書を検証] にチェックを入れることで、Acrobat は Windows が認識している認証局をすべて認識するようになり、従って 1-2-3 証明書も正式なものとして認識されるようになります。



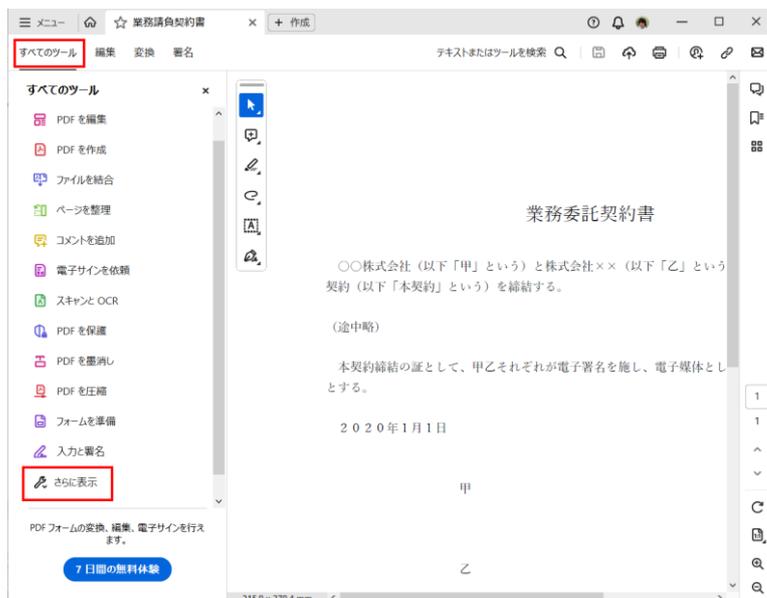
上記設定をした上で改めて署名済み PDF を開くと、下図のように「署名済みであり、すべての署名が有効です」となります。



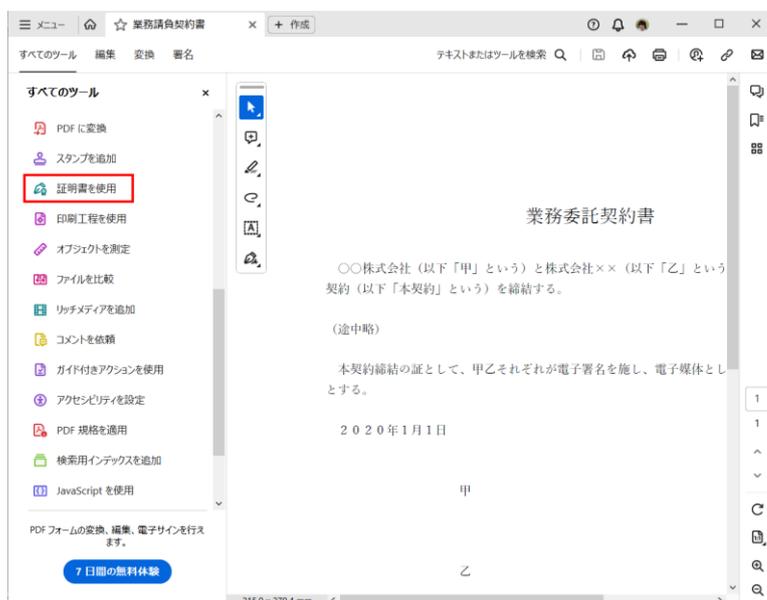
3 PDF ファイルに電子署名する

ここでは、実際に PDF に電子署名する方法を説明します。

1. まず、署名する PDF ファイルを Acrobat で開いてください。
文書左側のメニューの [すべてのツール] から [さらに表示] をクリックします。



2. 以下のように [証明書を使用] メニューが表示されますので、選択してください。



3. 以下のように、画面左側に [デジタル署名]、[タイムスタンプ] メニューが現れます。
[デジタル署名] をクリックしてください。

Acrobat (Reader) を使った 1-2-3 証明書による電子署名



4. 下図のように、マウスの左ボタンを押しながら、可視署名を入れたい場所（矩形）をドラッグします。



5. 証明書が複数インストールされている場合は、下図のように署名に用いる証明書を選択できるようになっています。適切なものを選択してください。その後、[続行] をクリックします。

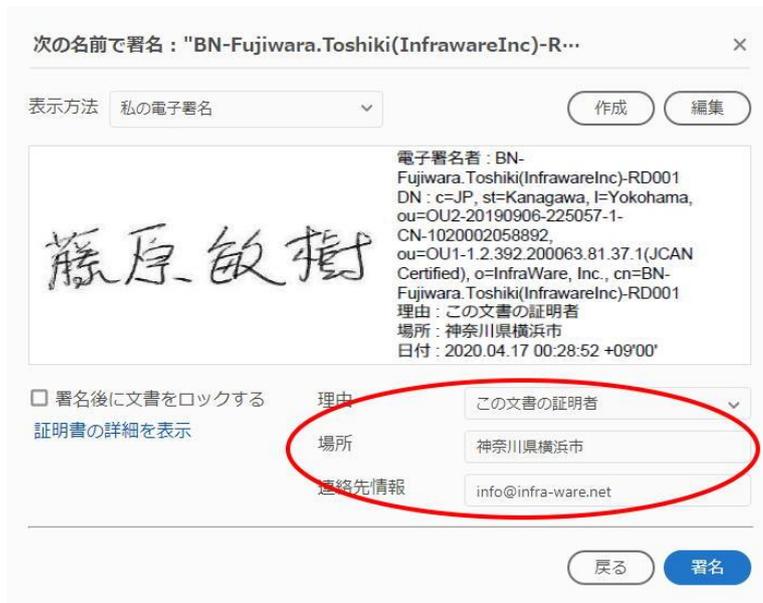


6. 前述の署名プロファイルの設定を行っている場合、[表示方法] で設定したプロファイルを選択します。プロファイルに従って、最終的に付加される可視署名のイメージが中段に表示されます。
下図の例は、[取り込まれたグラフィック] で自署イメージを表示するように設定したプロファイルを用いています。右側には、同じくプロファイルで選択した [署名地]、

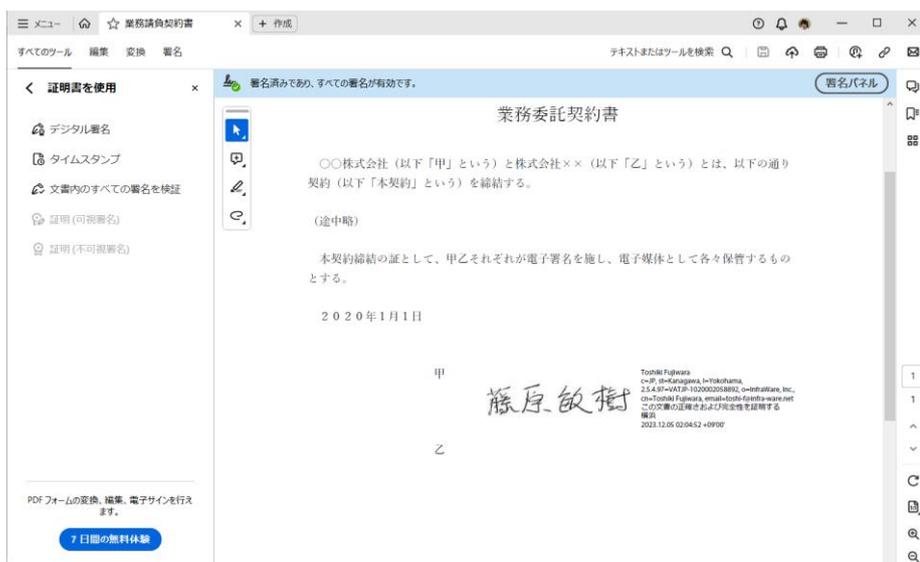
Acrobat (Reader) を使った 1-2-3 証明書による電子署名

[理由] などが表示されるとともに、下段に [理由]、[場所 (署名地)] などを入力する欄が表示されます。

それぞれ適切に入力し、[署名] ボタンをクリックします。



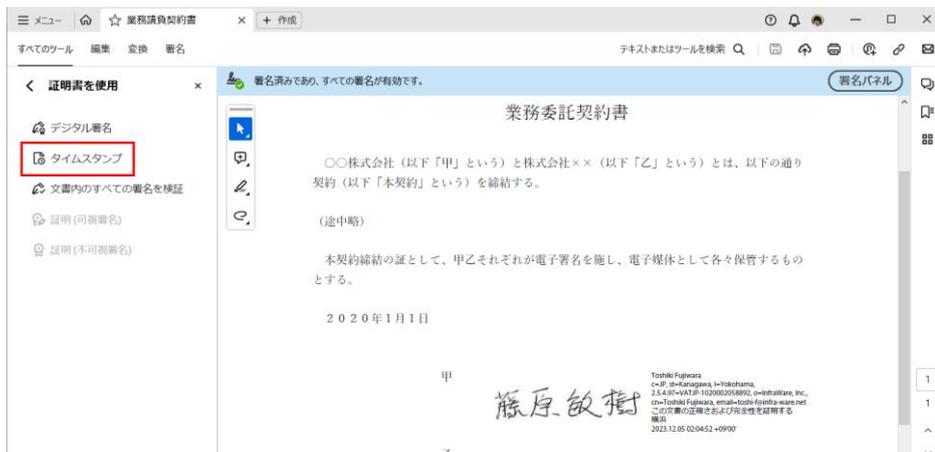
7. 以上で電子署名がなされ、最後にファイルを保存する場所、ファイル名を設定するダイアログが表示されますので、適当な場所・名前を入力します。元のファイルを上書きすることも可能ですが、署名がない状態の元のファイルは失われますので、注意してください。
8. このように、可視署名とともに、電子署名が付加されました。



9. 可視署名の内容については、署名プロファイルの設定を変更しながらお試しの上、好みの表示方法を決定してください。
10. 最後に、電子署名にかぶせてタイムスタンプを付与します。複数の署名者がいる場合、

Acrobat (Reader) を使った 1-2-3 証明書による電子署名

全員の署名が終わってから、一度だけ以下の処理をしてください。
電子署名の時と同じ手順で [証明書を使用] > [タイムスタンプ] が表示されますので、
[タイムスタンプ] をクリックします。



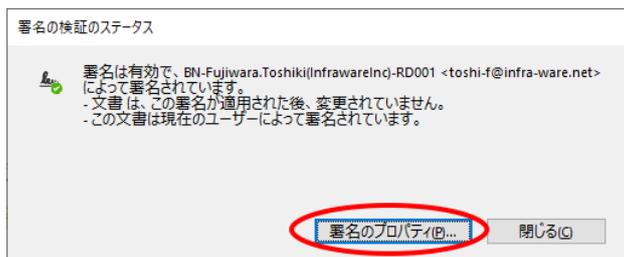
11. 最終的に、署名パネルで確認し、下図のように署名の最後にタイムスタンプが付与されていることを確認してください。下図の例では、2名の署名の後に、タイムスタンプを付与しています。



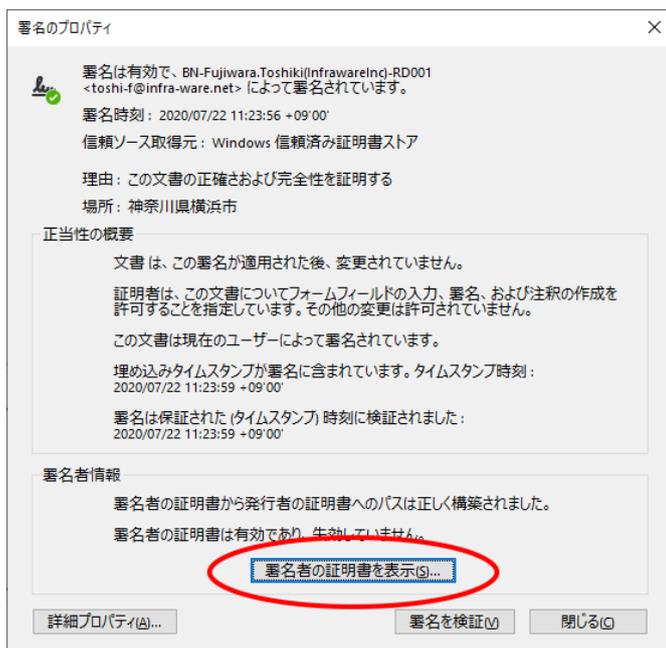
4 トラブルシューティング

ここでは、検証が失敗するなどのトラブルシューティング時の情報収集、あるいは署名が正しくなされているかどうかの確認方法などを説明します。

1. 署名済みの PDF ファイルを Acrobat で開きます。
署名部分をマウスでクリックしてください。以下のようなダイアログが表示されますので、[署名のプロパティ] をクリックします。



2. さらに以下のようなダイアログが表示されます。[署名者の証明書を表示] をクリックしてください。



4.1 証明書パス

以下のようなダイアログが表示されます。

ウインドウ左上赤丸部分には、署名に用いた 1-2-3 証明書と、それを発行した認証局の情報が階層で表示されます (認証局の階層は一段階とは限りません)。1-2-3 証明書の場合、最上位の認証局 (これをルート CA と呼びます) は GlobalSign となります。この階層を、証

Acrobat (Reader) を使った 1-2-3 証明書による電子署名

明書パス・信頼パスと言います。意味としてはルート CA の GlobalSign が GlobalSign GCC R6... という下位認証局を承認。GlobalSign GCC R6... がユーザの証明書を発行して認証する、という仕組みを表しています。この仕組みがあるため、ルート CA である GlobalSign を信頼することで、すべてのユーザの 1-2-3 証明書も信頼できることとなります。

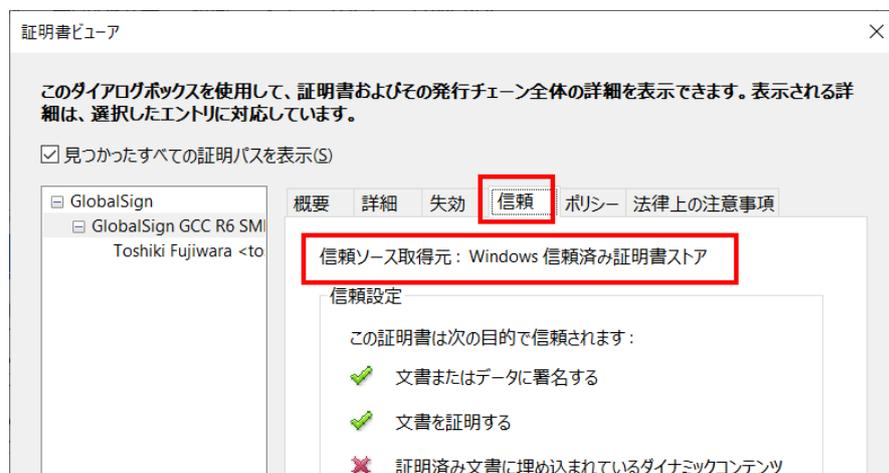
なお、Microsoft は GlobalSign を信頼できるルート CA として認識しているため、Windows には GlobalSign のルート CA 証明書がプリインストールされています。Windows を使う限りでは、ユーザの 1-2-3 証明書はすべて信頼済み、とも言えます。

証明書パスが正しく表示されていることを確認しましょう。



4.2 信頼の状態

次に、この状態で【信頼】タブをクリックします。

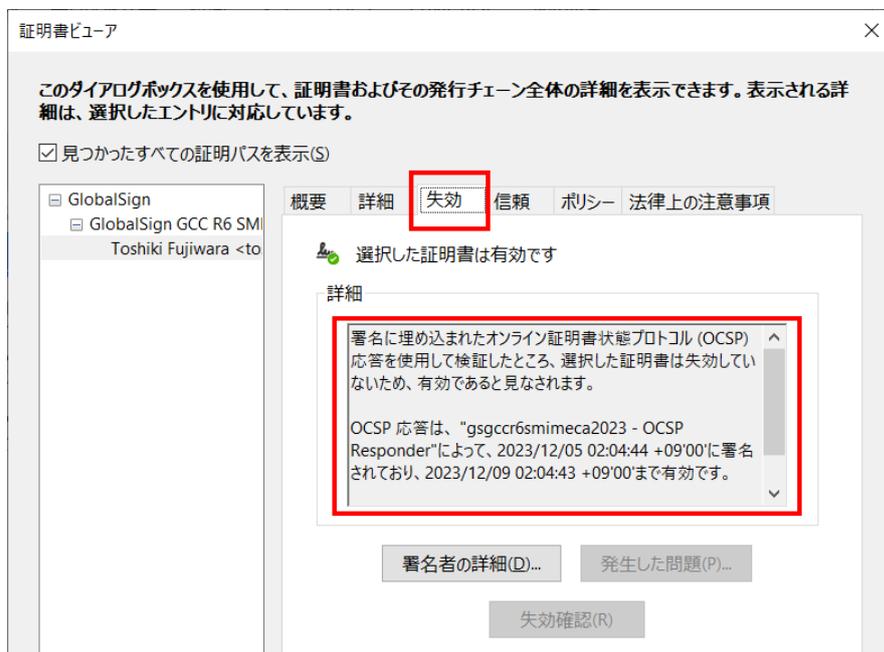


左側の証明書チェーンで選択した認証局や証明書（図では最下位のユーザの 1-2-3 証明書）の信頼状態が右に表示されます。図では「信頼ソース取得元: Windows 信頼済み証明書ストア」とありますが、これは前述のようにルート CA である GlobalSign が Windows によって信頼されているからです。

証明書チェーン各段階の信頼状態を、確認しておきましょう。

4.3 失効情報の確認

次に、[失効] タブをクリックしてください、下図のような表示になります。

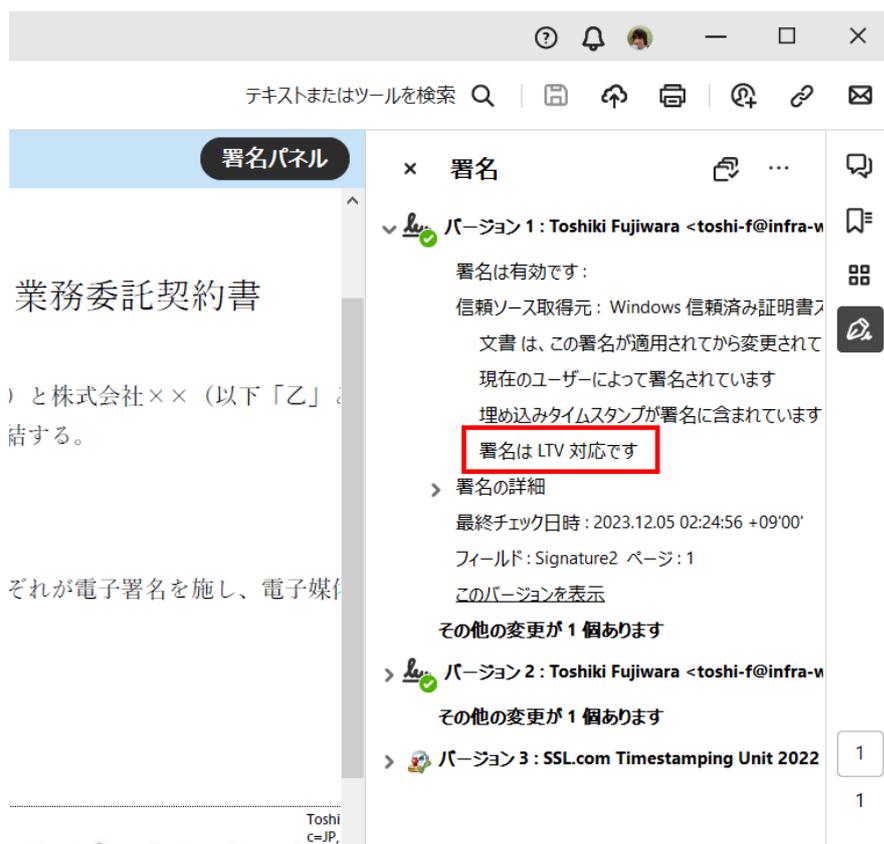


署名者の所属が変わった、死亡した、あるいは本人確認時の虚偽申告などの不正が発覚した場合など、証明書を「失効」することがあります。各認証局は失効した証明書のリストを保存しており、検証時の問合せに応える仕組みがあります。署名を行った時点で、その証明書のユーザが「失効リストにない」ことを確認して、はじめて署名が有効であるとみなされます。

[失効] タブを選択すると、署名時点で証明書が失効されていないかどうかの状態が確認できます。

ところが、この仕組みでは認証局は任意の時点の失効リストを将来にわたってすべて保存しなければなりません。これは非現実的です。Acrobat は、署名時点の失効リストを認証局から取り寄せ、PDF に埋め込みます。これにより、未来にわたって PDF 単体で（認証局に問い合わせることなく）署名の検証（署名時点で証明書が有効であること）を検証できることとなります。これを「長期検証」、LTV (Long Term Validation) と呼びます。

失効情報が正しく埋め込まれている場合、Acrobat の [署名パネル] で署名の内容を確認すると、下図のように「署名は LTV 対応です」と表示されます。



LTV 対応になっていない場合、証明書の有効期限が切れると検証ができなくなります。長期にわたって検証が必要になる書類は、かならず LTV 対応になっていることを確認してください。

「署名方法の設定」で説明した【署名の失効ステータスを含める】がチェックされており、「タイムスタンプサーバの設定」がなされていれば、LTV 対応になります。

以上