VBAマクロ形式編

改版履歴			
版数	日付	内容	担当
V.1.0	2018/2/26	初版	NII
V.1.1	2018/7/30	PKCS#12ファイル作成方法の追記	NII
V.1.2	2020/6/4	中間CA証明書のURLとリポジトリのURLの変更	NII
V.1.3	2020/12/22	中間CA証明書のURL変更	NII
V.1.4	2021/5/31	コード署名用証明書の中間CA証明書を修正	NII

目次

1. コード署名用証明書の利用

1-1. 動作環境について

本マニュアルでは以下の環境における操作手順のみ記載しています。

対応環境
Microsoft Excel 2016以上

1-2. 前提条件

Microsoft Excelでコード署名用証明書を使用する場合の前提条件について記載します。適宜、コード署名用証明書をインストールする利用管理者様の環境により、読み替えをお願いします。
（本マニュアルでは Microsoft Excel 2016での実行例を記載しております）
また、コマンドプロンプト上で実行するコマンドは「>」で示しています。

前提条件
1. コード署名用証明書がWebブラウザへインストールされていること （Webブラウザへのインストールマニュアル Microsoft Internet Explorer編に記載） 2. Microsoft Excel 2016以上がインストールされていること 3. Openssl がインストールされていること

1-3. PKCS#12ファイルの作成

本章ではPKCS#12ファイルの作成方法について記述します。

1-3-1. 事前準備

事前準備として、「ルートCA証明書」、「中間CA証明書」、「コード署名用証明書」を取得してください。

事前準備

1. 「証明書の申請から取得まで」で受領したコード署名用証明書を任意の名前で任意の場所に保存してください。
2. 「ルートCA証明書」と「中間CA証明書」を準備し、この2つを連結させます。

   「中間CA証明書」を下記リポジトリより取得してください。
   セコムパスポート for Member 2.0 PUB リポジトリ：
   https://repo1.secomtrust.net/spcpp/pfm20pub/index.html

   【2021年5月31日00:00以前の発行証明書が対象】
   リポジトリ内にある「証明書の種類」より中間CA証明書を取得してください。
   https://repo1.secomtrust.net/spcpp/pfm20pub/codecag2/CODECAG2.cer
   次に、「ルートCA証明書」を下記リポジトより取得してください。
   Security Communication RootCA2 リポジトリ：
   https://repository.secomtrust.net/SC-Root2/index.html
   Security Communication RootCA2 証明書：
   https://repository.secomtrust.net/SC-Root2/SCRoot2ca.cer

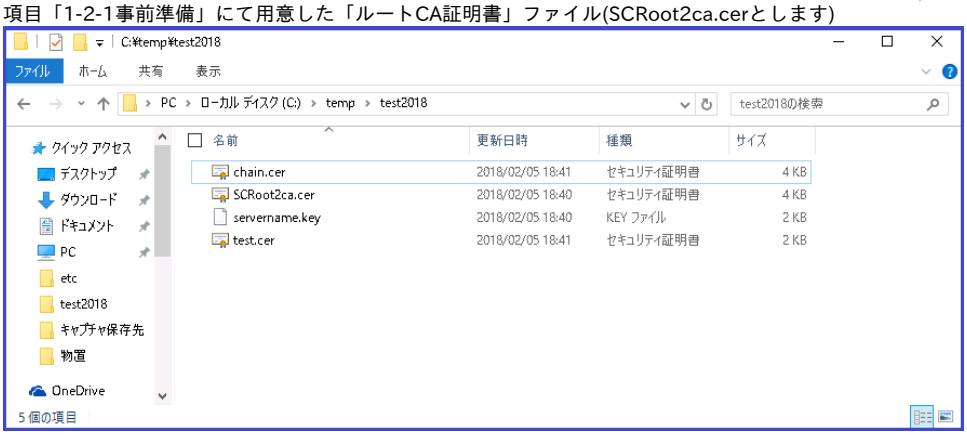
   【2021年5月31日00:00以後の発行証明書が対象】
   リポジトリ内にある「証明書の種類」より中間CA証明書を取得してください。
   https://repo1.secomtrust.net/spcpp/pfm20pub/codecag2/CODECAG2SCROOTCA3.cer
   次に、「ルートCA証明書」を下記リポジトより取得してください。
   Security Communication RootCA3 リポジトリ：
   https://repository.secomtrust.net/SC-Root3/index.html
   Security Communication RootCA3 証明書：
   https://repository.secomtrust.net/SC-Root3/SCRoot3ca.cer

1-3-2. PKCS#12ファイルの作成

本項目ではWindowsOS上で任意のフォルダにPKCS#12ファイルを作成する方法を記述します。
以下は、例としてWindows10上での作成方法を記載します。

PKCS#12ファイルの作成

1. 任意のフォルダ(ここではC:\temp\test2018とします)にて以下の4つのファイルを用意してください。
   a. 項目「鍵ペアの生成」にて作成した鍵ペアのファイル(servername.keyとします)
   b. 項目「証明書の申請から取得まで」にて取得したコード署名用証明書(test.cerとします)
   c. 項目「1-2-1事前準備」にて用意した「ルートCA証明書」と 「中間CA証明書」を連結させたファイル(chain.cerとします)
   d. 項目「1-2-1事前準備」にて用意した「ルートCA証明書」ファイル(SCRoot2ca.cerとします)



2. CAfile に指定する証明書をDER形式からPEM形式に変換します。

・Security Communication RootCA2の場合
openssl x509 -inform der -in SCRoot2ca.cer -outform pem -out SCRoot2ca.cer

・中間CA証明書（2021年5月31日00:00以前の発行証明書が対象）の場合
openssl x509 -inform der -in CODECAG2.cer -outform pem -out CODECAG2.cer

3. コマンドプロンプト上にて上記で取得した「ルートCA証明書」と「中間CA証明書」を以下のコマンドにより、連結させてください。中間CA証明書の下部にルートCA証明書が併記されるファイルとなります。

＞ type (中間CA証明書のパス) (ルートCA証明書のパス) > (出力するファイル名)

4. 連結したファイルがPEM形式になっていることを確認してください。
例）PEM形式の証明書

```
----BEGIN CERTIFICATE----
MIIEcTCCA1mgAwIBAgIIasWHLdnQB2owDQYJKoZIhvcNAQELBQAwbzELMAkGA1UE
BhMCSlAxFDASBgNVBAcMC0FjYWRlbWUtb3BzMSowKAYDVQQKDCFOYXRpb25hbCBJ
bnN0aXR1dGUgb2YgSW5mb3JtYXRpY3MxHjAcBgNVBAMMFU5JSSBPcGVyYXRpbmcg
Q0EgLSBHMjAeFw0xNTAzMTIwMTA4MDJaFw0xNzA0MTEwMTA4MDJaMHAxCzAJBgNV
（中略）
LmeW0e/xkkxwdmKv5y5txLlFcp53AZl/vjn3BHp42PFkkTISEmAUiCtQ2A25QDRR
RG33IaC8E8Tl/SnOA8h95XQtGWm47PrIjXyYtIe0rFousbpIoW8MZw4gDXVQ3485
XEftqwwIMcLNxttJ6i6f9XVyPMRhHy9rdDPseHiXayxcBxJMuw==
----END CERTIFICATE----
```

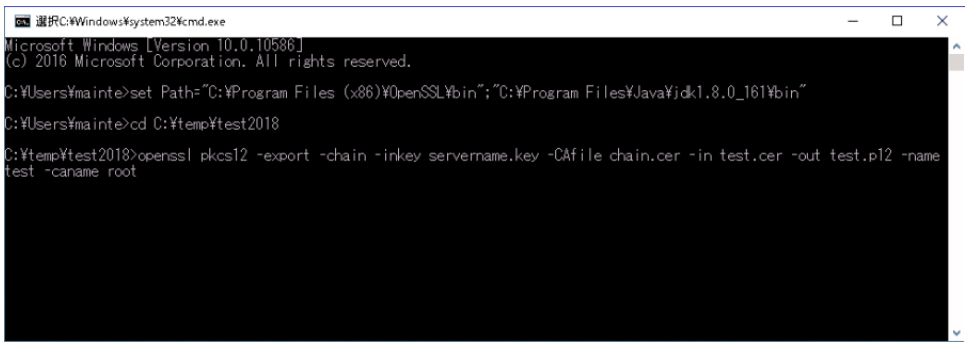
5. コマンドプロンプトを開き、ファイルのある任意のフォルダ(ここではC:\temp\test2018)へ移動します。

＞ set Path=**(OpenSSLインストールディレクトリ)**\bin
※OpenSSLインストールディレクトリをプログラムを探すディレクトリに指定します

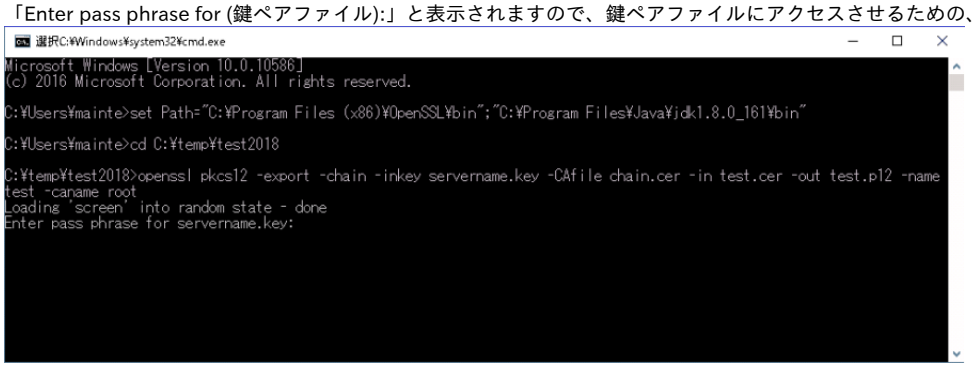
＞ cd **(作業ディレクトリ) ←作業ディレクトリ**

6. 移動後、以下のコマンドを実行しPKCS#12ファイルを作成してください。

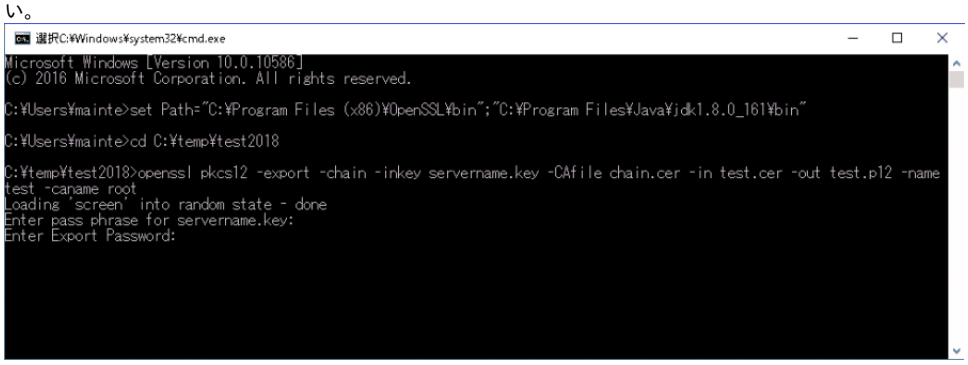
＞ openssl pkcs12 -export -chain -inkey (鍵ペアのファイル名) -CAfile (ルートCA証明書と中間CA証明書を連結させたファイル) -in (コード署名用の証明書ファイル名) -out (PKCS#12形式で出力するファイル名) –name (コード署名用証明書のエイリアス名) –caname (ルートCA証明書と中間CA証明書のエイリアス名)



7. 「Enter pass phrase for (鍵ペアファイル):」と表示されますので、鍵ペアファイルにアクセスさせるための、アクセスPINを入力してください。

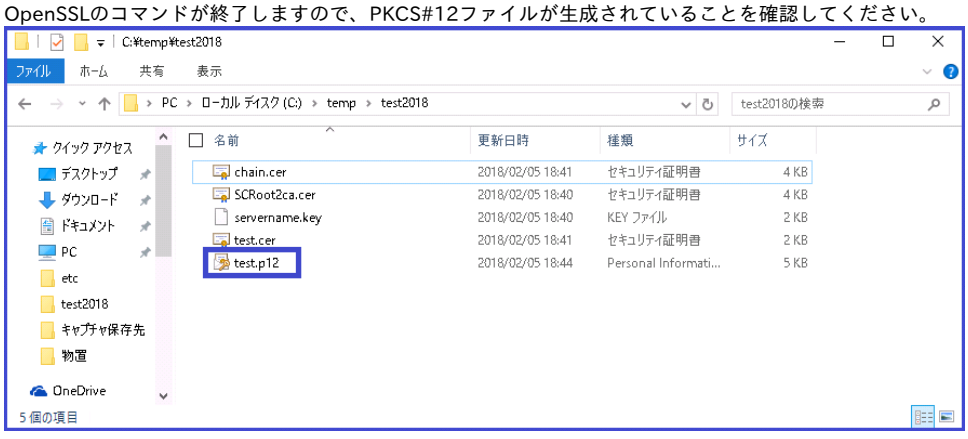


8. 「Enter Export Password:」と表示されますので、PKCS#12形式のファイルを保護するためのアクセスPINとして任意の文字列を入力してください。



9. 「Verifying - Enter Export Password:」と表示されますので、確認のため、同じアクセスPINを再度入力してください。

10. OpenSSLのコマンドが終了しますので、PKCS#12ファイルが生成されていることを確認してください。



1-4. インストール手順

証明書のインストール手順
コード署名用証明書がWebブラウザへインストールされている場合、インストールは不要です。

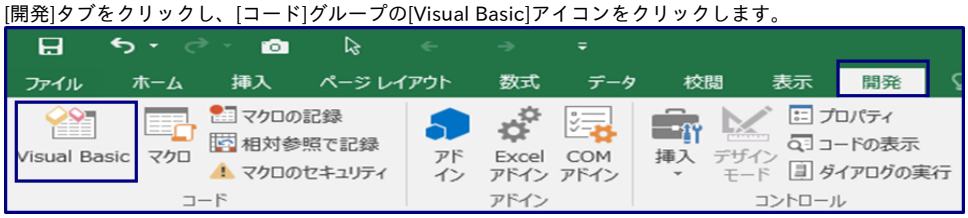
1-5. 署名

本章ではVBAマクロ形式のファイルにWindowsOS上にてデジタル署名をする方法について記述します。以下は、例としてWindows10上での作成方法を記載します。

1-5-1. 署名追加

署名追加作業

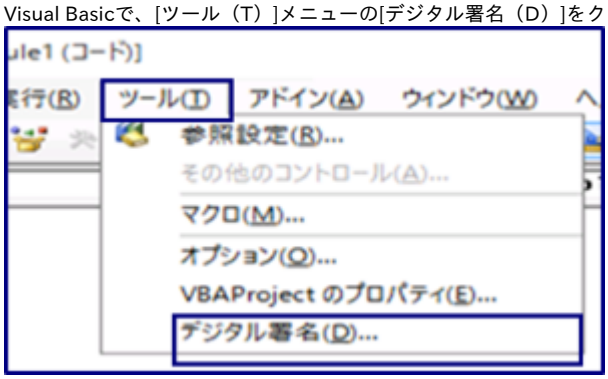
1. 署名するVBAマクロ形式のファイルを開きます。
2. [開発]タブをクリックし、[コード]グループの[Visual Basic]アイコンをクリックします。



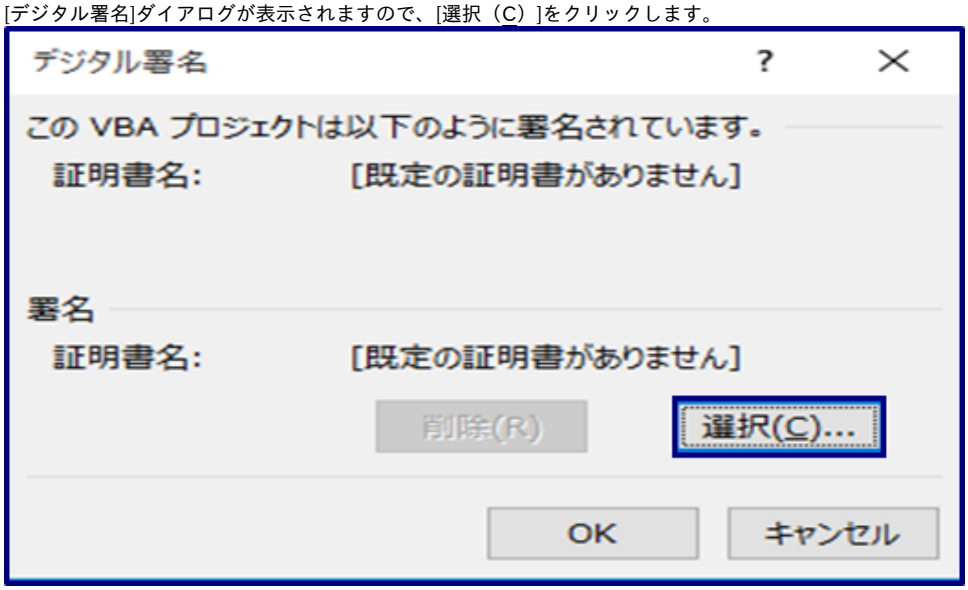
注意：[開発]タブが表示されていない場合は、[ファイル]タブをクリックします。
[オプション]タブをクリックします。[リボンのユーザー設定]をクリックし、[リボンのユーザー設定（B）]一覧の

[開発]にチェックを入れ、[OK]をクリックします。

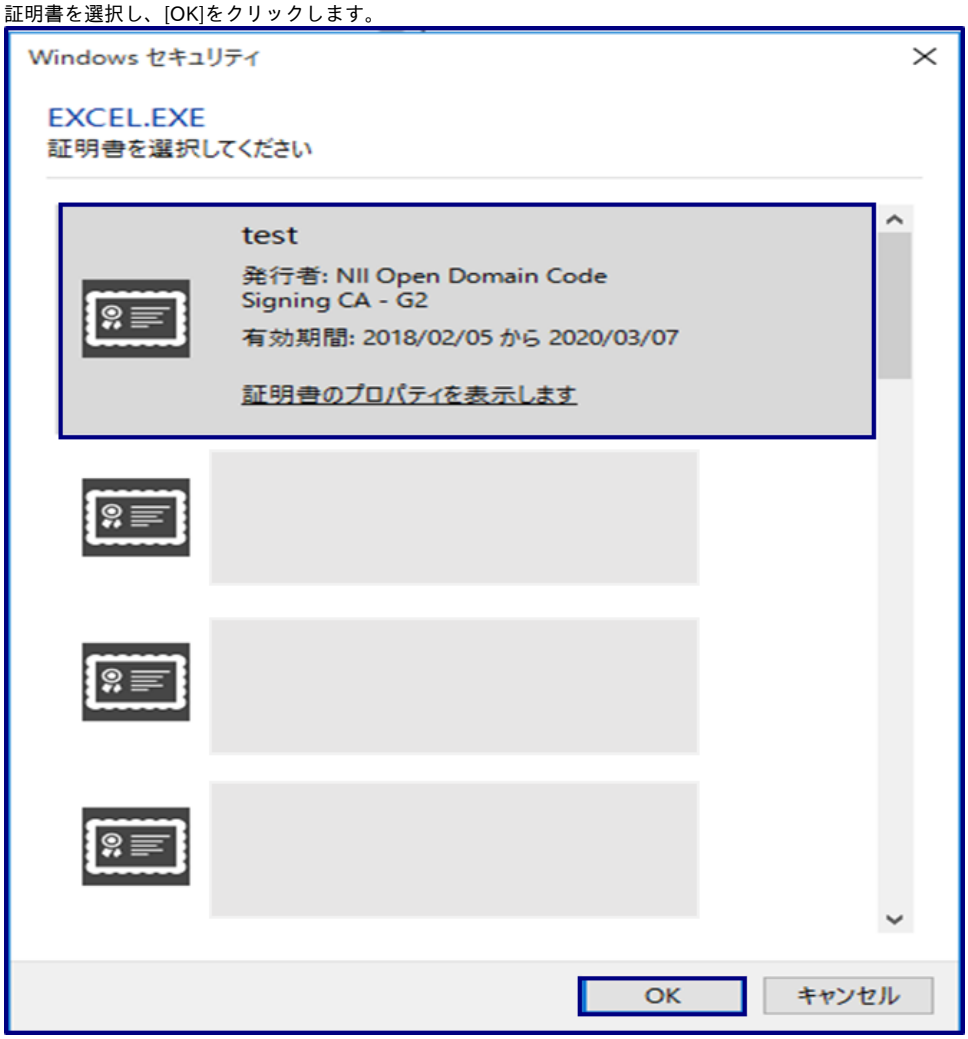
3. Visual Basicで、[ツール（T）]メニューの[デジタル署名（D）]をクリックします。



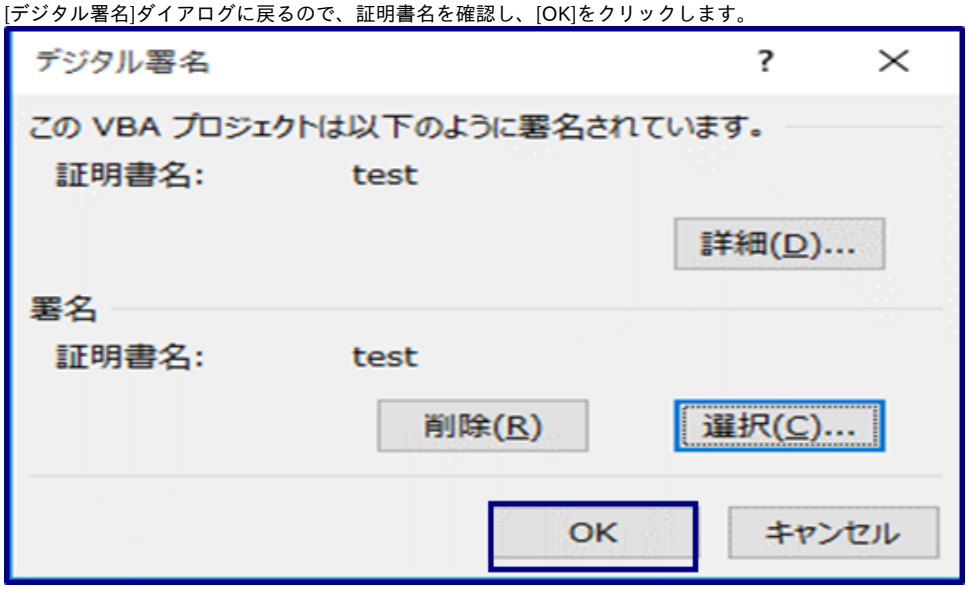
4. [デジタル署名]ダイアログが表示されますので、[選択（C）]をクリックします。



5. 証明書を選択し、[OK]をクリックします。



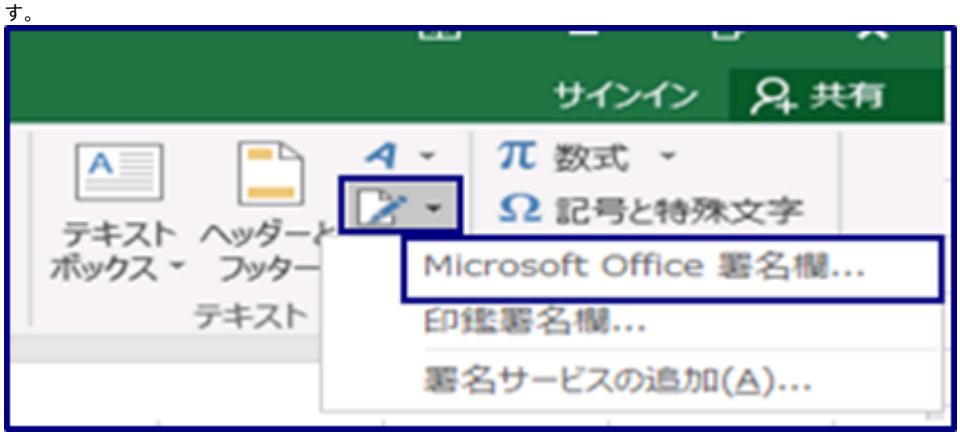
6. [デジタル署名]ダイアログに戻るので、証明書名を確認し、[OK]をクリックします。



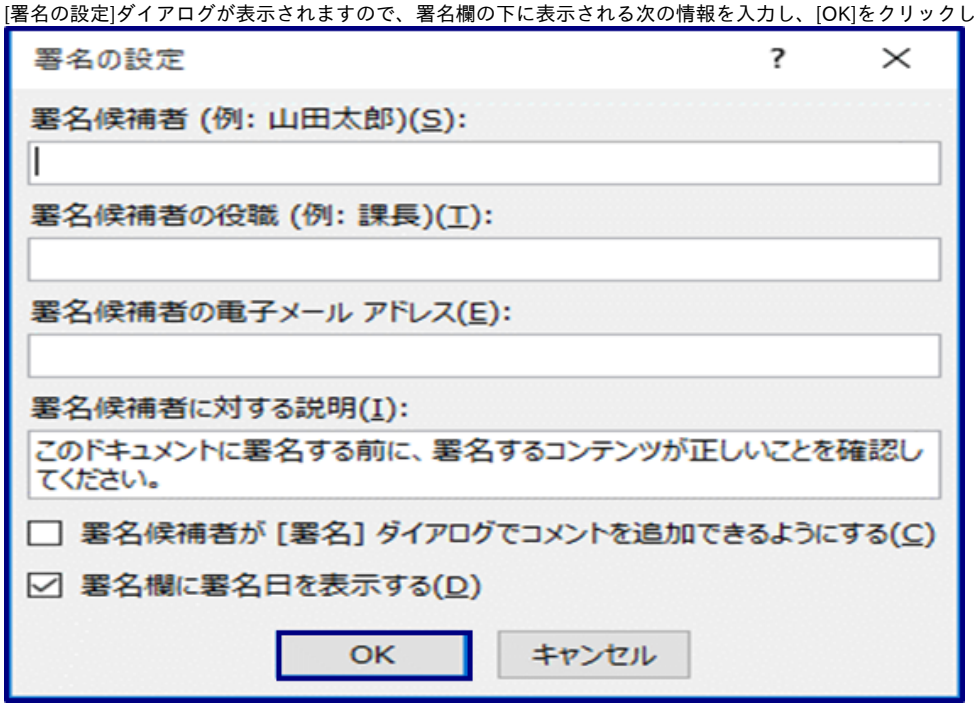
1-5-2. 署名作成

署名作成作業

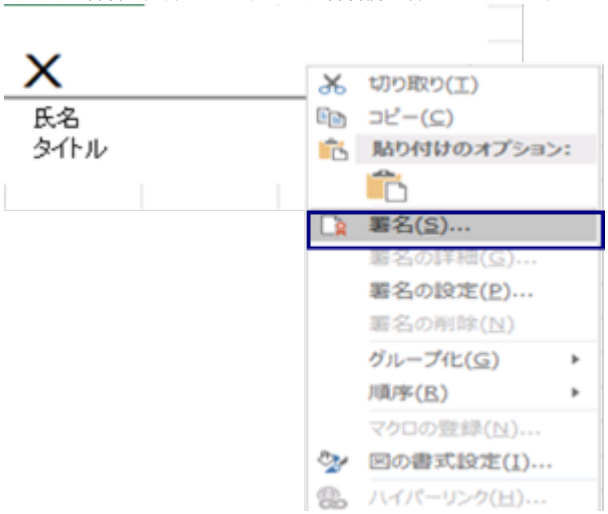
1. 署名欄を作成する場所をポイントします。
2. [挿入]タブをクリックし、[テキスト]グループの[署名欄]ボックスをクリックし、[Microsoft Office 署名欄]をクリックします。



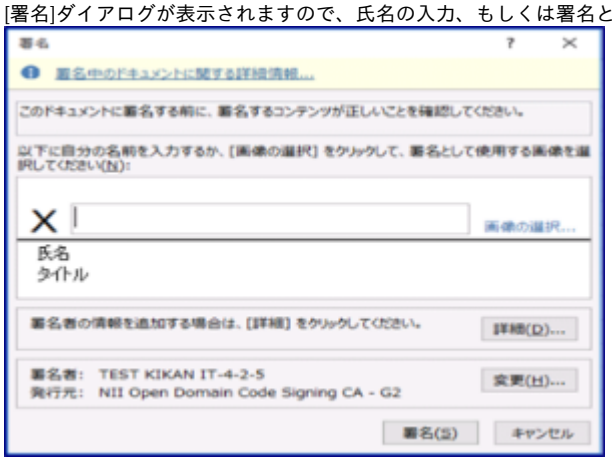
3. [署名の設定]ダイアログが表示されますので、署名欄の下に表示される次の情報を入力し、[OK]をクリックします。



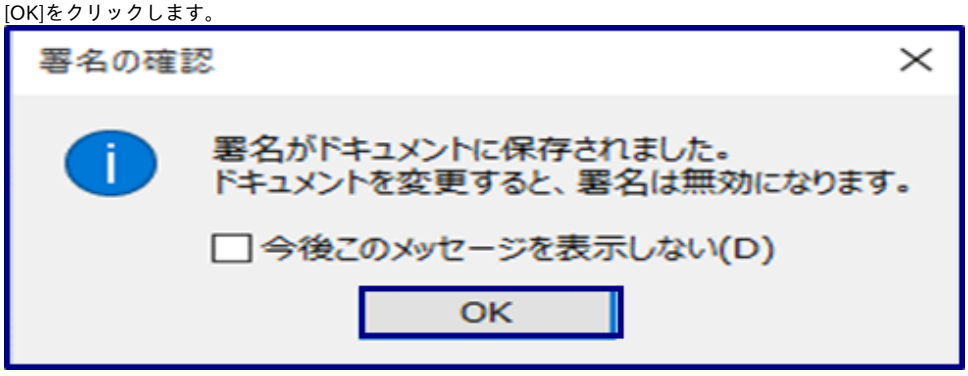
4. デジタル署名が追加されますので、署名欄を右クリックし、表示メニューの[署名（S）]をクリックします。



5. [署名]ダイアログが表示されますので、氏名の入力、もしくは署名として使用する画像を選択し[署名]をクリックします。



6. [OK]をクリックします。



7. [署名]ボタンが、ワークシートの最下部に表示されます。

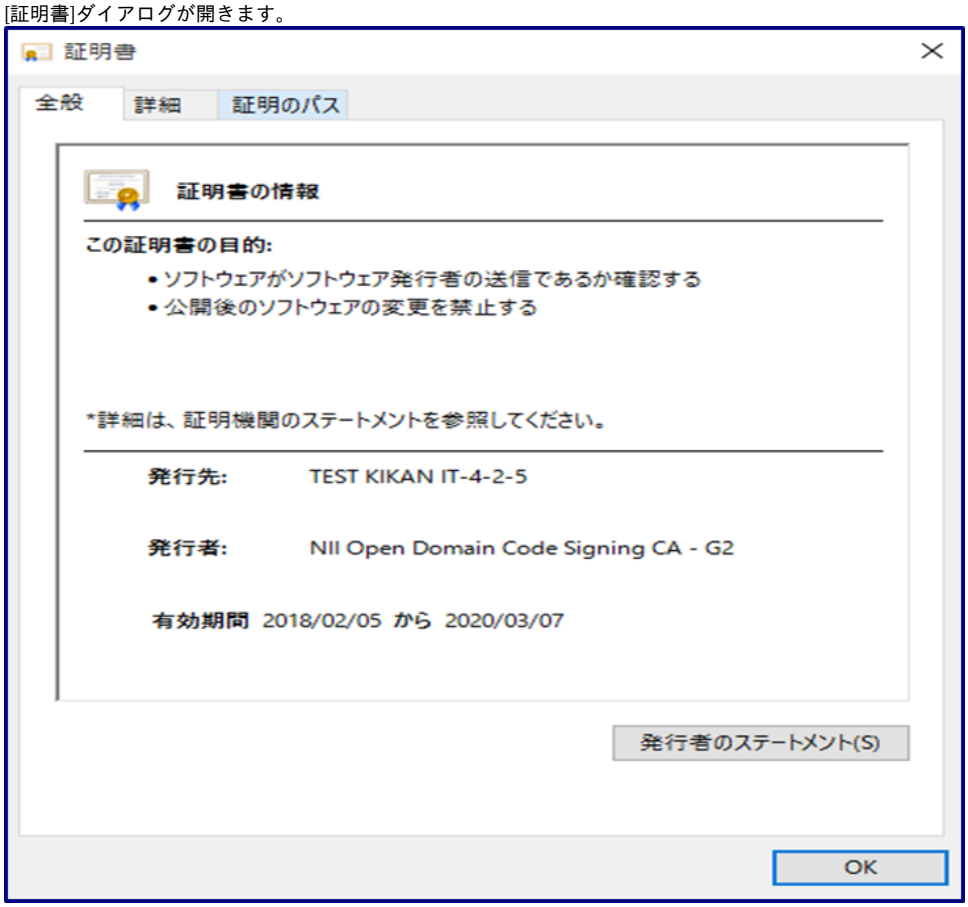
1-6. コード署名確認作業

本章ではデジタル署名したVBAマクロ形式のファイルについて署名確認作業について記述します。

署名確認作業

1. デジタル署名したファイルを開き、署名欄をダブルクリックします。
2. [署名の詳細]ダイアログが表示されますので、[表示（V）]をクリックします。

3. [証明書]ダイアログが開きます。



4. [証明のパス]タブをクリックし、証明書に問題がないことを確認してください。