cybertrust

DigiCert EV コード署名証明書
Javaコード 署名手順書

2015/07/31

はじめに

【！】本手順書をご利用の前に必ずお読みください

1. 本ドキュメントは「Windows」の環境下で、DigiCertのEV コード署名証明書をご利用いただく際の署名手順について解説するドキュメントです。
2. 本ドキュメントの手順は「Microsoft Windows 7」「Java SE Development Kit 8 Update 40」の環境下で動作確認をしており、署名を付与するコードが完成していることを前提としております。
3. 実際の手順はお客様の環境により異なる場合があり、Javaの動作を保証するものではございません。あらかじめご了承ください。
4. このドキュメントは予告なく変更される場合があり、サイバートラスト株式会社はその内容に対して責任を負うものではありません。また、このドキュメント内に誤りがあった場合、サイバートラスト株式会社は一切の責任を負いません。
5. このドキュメントで説明するソフトウェアはライセンスに基づいて配布されるものであり、ライセンスの条項に従った使用のみ許可されます。このドキュメントは、本来の使用目的のために発行され、公に発行されるものではありません。
6. このドキュメントの一部または全部を複製することは禁じられており、提供または製造を目的として使用することはできません。ただし、サイバートラスト株式会社との契約または同意文書で定められている場合に限り、この注記の添付を条件として複製することができます。
7. サイバートラスト株式会社から事前に書面による合意を得ない限り、このドキュメントまたはその一部から直接的または間接的に知り得た内容または主題に関して、個々の企業やその従業員などの第三者に対し、口頭、文書、またはその他のいかなる手段によっても伝達することはできません。

目　次

1.デジタル署名前の準備 --- P 4

2.準備（１）java.securityの編集 --- P 5

3.準備（２）eToken.cfgファイルの作成 --- P 6

4.準備（３）USBトークンスロットと別名の確認 --- P 7

5.デジタル署名の付与 --- P10

6.エラー時の確認方法 --- P12

1. デジタル署名前の準備

- デジタル署名を行うためには、事前に「Java SE Development Kit（JDK）」のインストールが必要です。

  ※JDKがバージョン7以下の場合、 64bitOSの場合においても32bitOS用JDKのインストールが必要です。

  - 「Java SE Development Kit」はOracle社のサイトでダウンロードできます。
    http://www.oracle.com/technetwork/java/javase/downloads/index.html

2. 準備（１）java.securityの編集

1. テキストエディタ（メモ帳など）で、次の場所にある「java.security」ファイルを開きます。

   例：C:¥Program Files (x86)¥Java¥jdk1.8.0_40¥jre¥lib¥security

2. 次の文字列を検索します。

```
security.provider.10=sun.security.mscapi.SunMSCAPI
```

3. 上記文字列の次の行に、以下を記載して上書き保存します。

```
security.provider.11=sun.security.pkcs11.SunPKCS11 ./etoken.cfg
```

※お客様の環境、使用するテキストエディタによっては「アクセスが拒否されました」とのメッセージが表示される場合があります。この場合、テキストエディタを管理者権限で起動してください。

3.準備（2）eToken.cfgファイル作成

1. 新規ファイルを作成するためテキストエディタ（メモ帳など）を開き、以下の3行を記載します。

```
name=eToken
library=c:¥WINDOWS¥system32¥eTPKCS11.dll
slot=0
```

2. ファイル名を「eToken.cfg」として、JDKのbinフォルダに保存します。

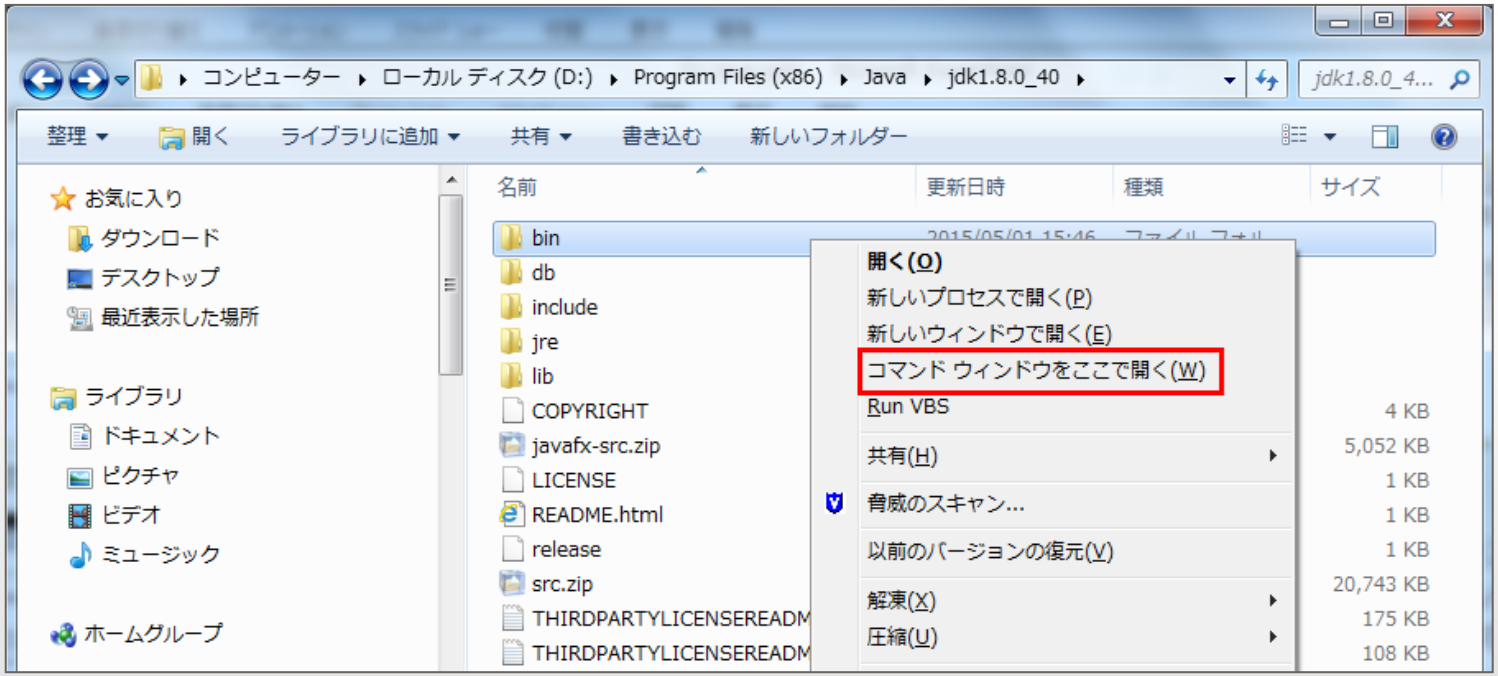
   例：C:¥Program Files (x86)¥Java¥jdk1.8.0_40¥bin

4.準備（3）USBトークンスロットと別名の確認

1. コマンドプロンプトで「keytool.exe」があるフォルダを開きます。

   例：C:¥Program Files (x86)¥Java¥jdk1.8.0_40¥bin

参考：エクスプローラでフォルダを選択した状態から、[Shift]+右クリックでコンテキストメニューに「コマンドウィンドウをここで開く」が追加されます。



4.準備（3）USBトークンスロットと別名の確認

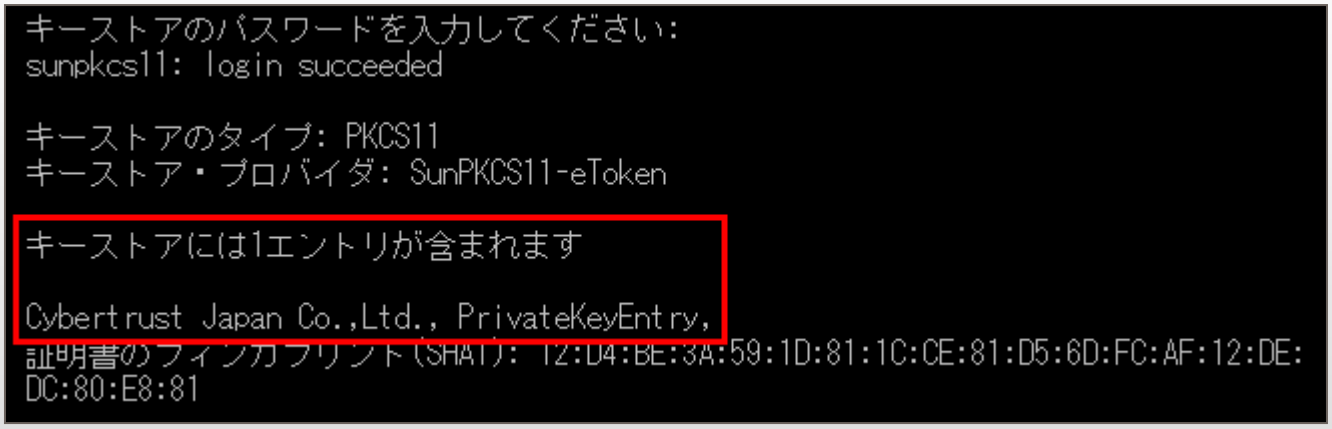
2. USBトークンをコンピュータに接続し、以下のコマンドを実行して、パスワードを入力します。

```
keytool -keystore NONE -storetype PKCS11 -list -J-Djava.security.debug=sunpkcs11
```

3. 実行結果が以下であることを確認します。
   - キーストアには1エントリが含まれます
   - お客様の会社名, PrivateKeyEntry,

     ※ここで表示された会社名が「別名」と呼ばれるもので、署名付与時に入力します。

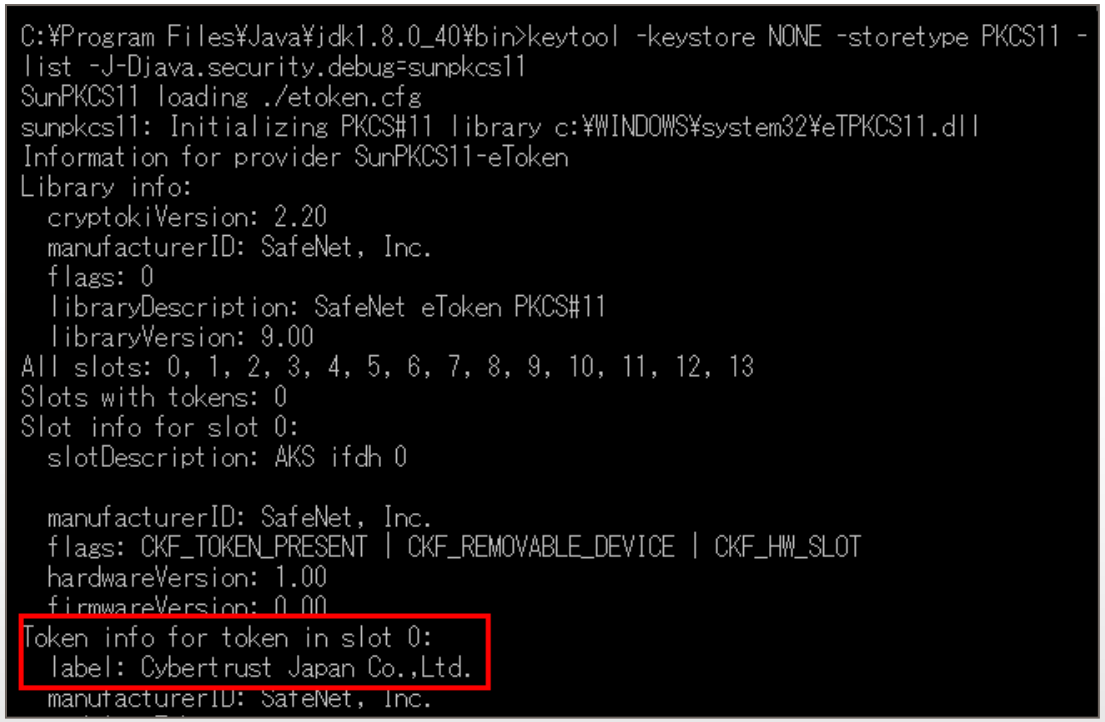
コマンドプロンプトの表示例：実行結果の下部分



4.準備（3）USBトークンスロットと別名の確認

- 「slot」が0であること
- 「label」に会社名が入っていること

コマンドプロンプトの表示例：実行結果の上部分



※複数のUSBトークンを使用している場合やエラーが表示された場合は
P13「6.エラー時の確認方法」をご覧ください。

5.デジタル署名の付与

1. コマンドプロンプトで「jarsigner.exe」があるフォルダを開きます。

   例：C:¥Program Files (x86)¥Java¥jdk1.8.0_40¥bin

2. 以下のコマンドを実行し、パスワードを入力します。

   jarsigner -tsa http://timestamp.digicert.com -verbose -keystore NONE -storetype PKCS11 -providerClass sun.security.pkcs11.SunPKCS11 -providerArg ./eToken.cfg "D:¥sample.jar" "**Cybertrust** Japan Co.,Ltd."

   ※赤文字部分は署名を付与するファイルのパス、確認した別名をそれぞれ入力します。
   ※パスワードを入力しても反応が無い場合は、USBトークンを一度取り外します。
   エラーが表示された後にUSBトークンをもう一度接続し、再度コマンドを実行します。

   コマンドプロンプトの表示例

```
D:¥Program Files (x86)¥Java¥jdk1.8.0_40¥bin>jarsigner -tsa http://timestamp.digicert.com -verbose -
keystore NONE -storetype PKCS11 -providerClass sun.security.pkcs11.SunPKCS11 -providerArg ./eToken.
cfg "D:¥sample.jar" "Cybertrust Japan Co.,Ltd."
キーストアのパスワードを入力してください:
  更新中: META-INF/CYBERTRU.SF
シグネチャ・タイムスタンプのリクエスト
TSAの場所: http://timestamp.digicert.com
  更新中: META-INF/CYBERTRU.RSA
    署名中: ElementTreePanel$1.class
    署名中: resources/open.gif
    署名中: resources/paste.gif
    署名中: resources/save.gif
jarは署名されました。
```

以上でデジタル署名の付与は完了です。

5.デジタル署名の付与

参考：以下のコマンドで、署名した内容を確認できます。
jarsigner -verify -certs -verbose "D:¥sample.jar"

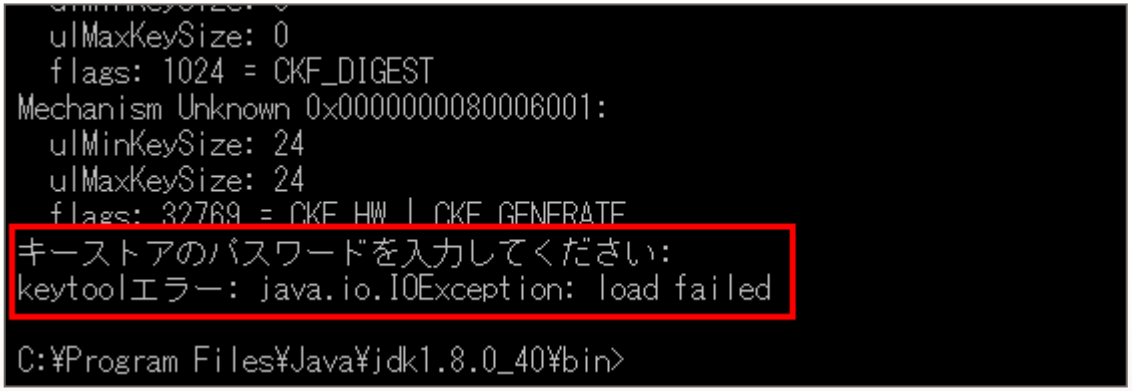
コマンドプロンプトの表示例

```
D:¥Program Files (x86)¥Java¥jdk1.8.0_40¥bin>jarsigner -verify -certs -verbose "D:¥sample.jar"

s       3699 Thu Apr 30 16:34:28 JST 2015 META-INF/MANIFEST.MF

      [エントリは15/05/01 16:34に署名されました]
      X.509, CN= Cybertrust Japan Co.,Ltd. , U= Cybertrust Japan Co.,Ltd.", L=Minato-ku, ST=Tokyo,
C=JP, OID.2.5.4.17=107-6030, STREET=Akasaka 1-12-32, STREET="Ark Mori, 30th Floor", SERIALNUMBER=01
0401065010, OID.1.3.6.1.4.1.311.60.2.1.3=JP, OID.2.5.4.15=Private Organization
      [証明書は15/03/23 9:00から16/03/30 21:00まで有効です]
      X.509, CN=DigiCert EV Code Signing CA (SHA2), OU=www.digicert.com, O=DigiCert Inc, C=US
      [証明書は12/04/18 21:00から27/04/18 21:00まで有効です]
      X.509, CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
      [証明書は06/11/10 9:00から31/11/10 9:00まで有効です]
```

6.エラー時の確認方法

1. 以下のエラーが表示される場合は、結果上部の「label」部分を確認します。

コマンドプロンプトの表示例：実行結果の下部分



6.エラー時の確認方法

コマンドプロンプトの表示例：実行結果の上部分

```
C:¥Program Files¥Java¥jdk1.8.0_40¥bin>keytool -keystore NONE -storetype PKCS11 -
list -J-Djava.security.debug=sunpkcs11
SunPKCS11 loading ./etoken.cfg
sunpkcs11: Initializing PKCS#11 library c:¥WINDOWS¥system32¥eTPKCS11.dll
Information for provider SunPKCS11-eToken
Library info:
  cryptokiVersion: 2.20
  manufacturerID: SafeNet, Inc.
  flags: 0
  libraryDescription: SafeNet eToken PKCS#11
  libraryVersion: 8.03
All slots: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13
Slots with tokens: 0
Slot info for slot 0:
  slotDescription: AKS ifdh 0

  manufacturerID: SafeNet, Inc.
  flags: CKF_TOKEN_PRESENT | CKF_REMOVABLE_DEVICE | CKF_HW_SLOT
  hardwareVersion: 1.00
  firmwareVersion: 0.00
Token info for token in slot 0:
  label: 31544747
  manufacturerID: SafeNet, Inc.
```

6.エラー時の確認方法

- 「label」に会社名が表示されている場合
  - 入力したパスワードが誤っている。
    - USBトークンを一度取り外してから数秒後に再度接続し、もう一度コマンドを実行します。
    - 正しいパスワードが不明の場合は、コード署名証明書の再発行が必要です。

- 「label」に会社名が表示されていない場合
  - 正しいUSBトークンが接続されていない。
    - USBトークンが正しいことを確認します。
  - 複数のUSBトークンを使用していて、コード署名証明書にアクセスできていない。
    - 次ページ以降をご参照ください。

6.エラー時の確認方法

2. 準備（２）で作成したeToken.cfgファイルをテキストエディタを開きます。

   例：C:¥Program Files (x86)¥Java¥jdk1.8.0_40¥bin

3. 正しいスロットを確認するため、「slot=0」を「slot=1」に変更し、上書き保存します。

```
name=eToken
library=c:¥WINDOWS¥system32¥eTPKCS11.dll
slot=1
```

4. コマンドプロンプトで再度以下のコマンドを実行し、「label」に会社名が表示されることを確認します。

   keytool -keystore NONE -storetype PKCS11 -list -J-Djava.security.debug=sunpkcs11

6.エラー時の確認方法

コマンドプロンプトの表示例：実行結果の上部分
※以下は「slot=1」を指定した場合です。

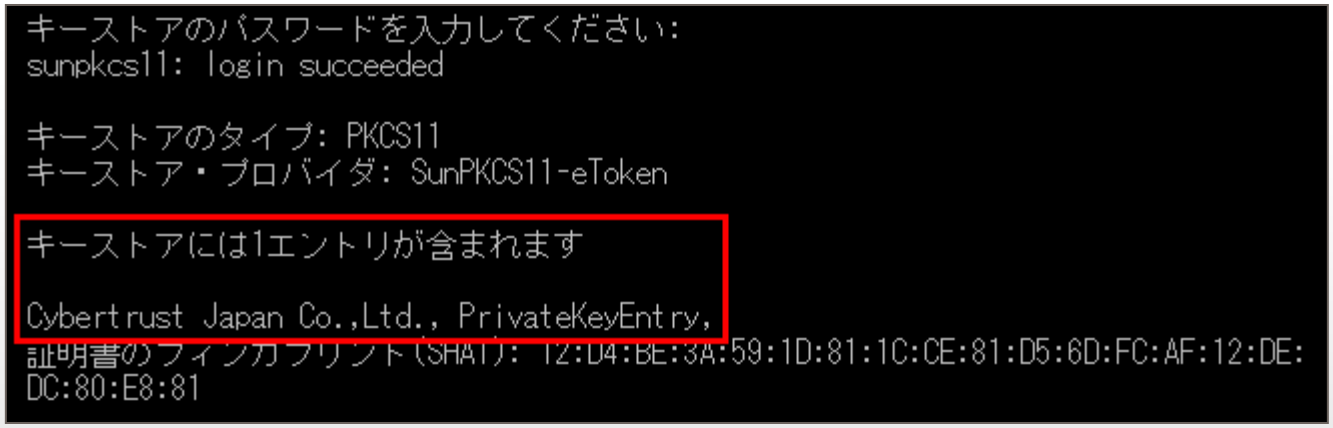
```
D:¥Program Files (x86)¥Java¥jdk1.8.0_40¥bin>keytool -keystore NONE -storetype PKCS11 -list -J-Djava
.security.debug=sunpkcs11
SunPKCS11 loading ./etoken.cfg
sunpkcs11: Initializing PKCS#11 library c:¥WINDOWS¥system32¥eTPKCS11.dll
Information for provider SunPKCS11-eToken
Library info:
  cryptokiVersion: 2.20
  manufacturerID: SafeNet, Inc.
  flags: 0
  libraryDescription: SafeNet eToken PKCS#11
  libraryVersion: 8.03
All slots: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13
Slots with tokens: 0, 1
Slot info for slot 1:
  slotDescription: AKS ifdh 1
  manufacturerID: SafeNet, Inc.
  flags: CKF_TOKEN_PRESENT | CKF_REMOVABLE_DEVICE | CKF_HW_SLOT
  hardwareVersion: 1.00
  firmwareVersion: 0.00
Token info for token in slot 1:
  label: Cybertrust Japan Co.,Ltd.
  manufacturerID: SafeNet, Inc.
  model: eToken
  serialNumber: 00c49fdb
```

6.エラー時の確認方法

5. パスワード入力後に「login succeeded」の表示が確認できるまで、手順2～5を繰り返します。
   ※手順5「slot=○」の数字を1つずつ増やして、確認します。

```
name=eToken
library=c:¥WINDOWS¥system32¥eTPKCS11.dll
slot=2
```

コマンドプロンプトの表示例：成功した場合



6. P7「4.準備（3）USBトークンスロットと別名の確認」の手順を進めます。

お問い合わせ先

サイバートラスト株式会社　DigiCertサポート係

e-mail : **digicert_support@cybertrust.ne.jp**

または、サイバートラスト総合受付

電話番号：0120-957-975

受付時間：平日 9:00～18:00