cybertrust

DigiCert SSL/TLS 証明書

Tomcat

CSR 作成/証明書インストール手順書

（新規・更新用）

Version 1.4

PUBLIC RELEASE

2018/10/25

改訂履歴

日付	バージョン	内容
2017/03/08	1.0	初版リリース
2017/04/28	1.1	「はじめに」の記述内容を修正
2018/08/09	1.2	「OU」に関する記述内容を修正
2018/10/01	1.3	「グローバル IP」「OU」に関する記述内容を修正
2018/10/25	1.4	ドメイン名変更に伴い記述内容を修正

目次

はじめに

【！】本手順書をご利用の前に必ずお読みください

本ドキュメントは、Microsoft 社「Windows OS」/「Tomcat」の環境下で DigiCert SSL/TLS 証明書の申し込み時にご利用いただく CSR 作成とサーバー証明書のインストールの作成手順について解説するドキュメントです。

本手順は、「Windows XP SP3」「Tomcat 6.0.26」「JRE 6.0」の環境下で動作確認をしております。

また、上記がすでに設定されており、Tomcat 単独での動作確認ができている事を前提としております。

実際の手順はお客様の環境により異なる場合があり、Tomcat 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。

なお、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。

サーバー証明書お申込みフロー

サーバー証明書のご購入については、以下のお申込みフローをご確認ください。

本手順では、赤枠で囲まれた部分のフローをご案内しています。

STEP1	CSR の作成　P6～
↓	
STEP2	WEB からのお申し込み(Cert Station)
↓	
STEP3	必要書類送付/申請の意思確認(電話) 証明書の発行
↓	
STEP4	証明書のダウンロード　P15～
↓	
STEP5	証明書のインストール　P16～
↓	
STEP6	SSL 通信の確認　P21～

cybertrust

CSR の作成

1. CSR 作成前のご確認事項

CSR 作成前に以下についてご確認ください。

1.1. 公開鍵長のご指定について

公開鍵長は「2048bit」をご指定ください。

1.2. CSR 作成時に指定する項目(DN)について

CSR 作成時に以下の項目を指定いただきますので、あらかじめ必要項目をご確認ください。

【!】以下の点についてご注意ください。

・●印がついている項目は必須設定項目です。
・各項目の最大文字数は半角 64 文字(半角スペースを含む)です。日本語は 20 文字です。
・CSR に使用出来る文字は半角英数字(a～z, A～Z, 0～9)と記号(「"」「#」「;」「+」を除く)です。
・組織名(O)、市町村名(L)、都道府県(S)については、CSR 作成時の値に関わらず、
申請法人で指定した値(日本語 or 英語)が証明書情報へ反映されます。

入力項目		内容	入力例
●	コモンネーム(CN)	実際に接続する URL の FQDN(※1)	https://www.cybertrust.ne.jp/index.html ⇒ www.cybertrust.ne.jp
	組織単位名(OU)	部署名(任意)(※2)	Technical Division
●	組織名(O)	申請組織の名称(英名)	Cybertrust Japan Co.,Ltd.
●	市町村名(L)	申請組織の事業所住所の「市町村名」(英名) ※東京は 23 区	Minato-ku
●	都道府県名 (S/ST)	申請組織の事業所住所の「都道府県名」(英名)	Tokyo
●	国名(C)	申請組織の国名(JP 固定)	JP

※1 DigiCert SSL/TLS 証明書は、グローバル IP アドレス、プライベート IP アドレスならびにベースドメイン名、ホスト名はコモンネームとしてご指定いただけませんのでご注意ください。

※2 OU の値は空欄で申請することをお勧めします。詳細はこちらをご覧ください。

1.3. 本手順の設定例について

本手順では以下の設定を例としてご案内しております。

種類	名称
キーストアのファイル名	server.keystore
サーバー証明書のエイリアス名	cybertrust
CSR のファイル名	server.csr

【！】注意事項

・お客様の環境によりファイルやパスが異なりますので、環境に合わせてお読み替えください。

・既存のファイルと同名で作成した場合、既存のファイルへ新しいファイルが上書きされますので、別名をご指定ください。

2. キーストアファイル・キーペアファイル・CSR の作成

「Windows OS」/「Tomcat」の環境下では、コマンドプロンプト上で keytool を用いてキーストアファイルを作成・エイリアスをご指定のうえ、キーペアファイル(公開鍵・秘密鍵のペア)と CSR を作成します。

※証明書の更新や他社からのお乗換えの際も同様の手順となります。

2.1. キーストアファイルとキーペアファイルの作成方法

キーストアファイルとキーペアファイルを作成します。

A) コマンドプロンプトで以下のコマンドを入力し、キーストアファイルとキーペアファイルを作成します。

■ コマンド入力

keytool -genkey -alias「サーバー証明書のエイリアス名(任意)」-keyalg RSA -keysize 2048 -keystore「キーストアファイル名(任意)」

例) keytool -genkey -alias cybertrust -keyalg RSA -keysize 2048 -keystore server.keystore

※証明書の更新や他社からのお乗換えの際、キーストアファイル名は既存のキーストアファイル名と別名をご指定ください。

B) 以下が表示されますので、キーストアファイルのパスフレーズとして任意の文字列(6 文字以上)を入力します。

```
キーストアのパスワードを入力してください:
```

C) パスフレーズを再入力します。

```
新規パスワードを再入力してください:
```

D) DN 情報の入力

■ 姓名を入力してください。

入力必須項目です。

申請するサーバー証明書の FQDN 名(サーバー名＋ドメイン名)を入力してください。

例)www.cybertrust.ne.jp

```
姓名を入力してください。
  [Unknown]:  www.cybertrust.ne.jp
```

■ 組織単位名を入力してください。

任意入力項目です。

必要に応じて申請する組織の部署名を入力してください。

※OU の値は空欄で申請することをお勧めします。詳細はこちらをご覧ください。

例)Technical Division

```
組織単位名を入力してください。
  [Unknown]:  Technical Division
```

■ 組織名を入力してください。

入力必須項目です。

申請する英訳組織名を入力してください。

例)Cybertrust Japan Co.,Ltd.

```
組織名を入力してください。
  [Unknown]:  Cybertrust Japan Co.,Ltd.
```

■ 都市名または地域名を入力してください。

入力必須項目です。

申請する組織の市町村名を入力してください。(東京の 23 区を含む)

例)Minato-ku

```
都市名または地域名を入力してください。
  [Unknown]:  Minato-ku
```

■ **州名または地方名を入力してください。**

入力必須項目です。

申請する組織の都道府県名を入力してください。

例）Tokyo

```
州名または地方名を入力してください。
  [Unknown]:  Tokyo
```

■ **この単位に該当する 2 文字の国番号を入力してください。**

JPと入力します。

```
この単位に該当する 2 文字の国番号を入力してください。
  [Unknown]:  JP
```

E） 入力内容を確認し、誤りがなければ「yes」と入力して、Enter ボタンを押します。

```
CN=www.cybertrust.ne.jp, OU=Technical Division, O="Cybertrust Japan Co.,Ltd.", L=Minato-ku,
 ST=Tokyo, C=JP でよろしいですか?
  [no]:  yes
```

F） 何も入力せずに Enter ボタンを押します。

```
<cybertrust> の鍵パスワードを入力してください。
        (キーストアのパスワードと同じ場合は RETURN を押してください):
```

以上でキーストアファイルとキーペアファイルの作成が完了します。

2.2. CSR の作成方法

A) コマンドプロンプトで以下のコマンドを入力し、指定した秘密鍵ファイルから CSR を作成します。

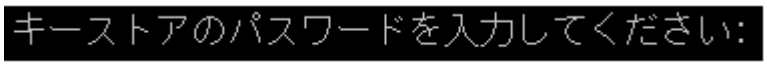
※CSR は既存の CSR と同ファイル名を指定した場合、ファイルが上書きされますので、ご注意ください。

■ **コマンド入力**

keytool -certreq -alias「サーバー証明書のエイリアス名」-file「CSR 名(任意)」-keystore「キーストアファイル名」

例)keytool -certreq -alias cybertrust -file server.csr -keystore server.keystore

B) キーストアファイルに設定したパスワードを入力します。



以上で CSR の作成は完了です。

3. キーストアファイルのバックアップ

秘密鍵ファイルを含むキーストアファイル(server.keystore など)は、証明書のインストール時に必要となります。

万が一に備えて、必ず別のメディア(CDや USB 等)にコピーして安全な場所に保管してください。

なお、弊社がお客様のキーストアファイルの情報を受け取ることはございません。あらかじめご了承ください。

4. 証明書のお申し込み

作成した CSR をテキストエディタで開いて内容をコピーし、WEB の申請サイト(Cert Station)の申請フォームへ貼り付けて、弊社へお申し込みください。

＜CSR サンプル＞ ※ こちらは申請にご利用いただけません。

```
-----BEGIN NEW CERTIFICATE REQUEST-----
・・・・・
MIIEhDCCA2wCAQAwgYkxCzAJBgNVBAYTAkpQMQ4wDAYDVQQIDAVUb2t5bzESMBAG
A1UEBwwJTWluYXRvLWt1MSIwIAYDVQQKDBlDeWJlcnRydXNOIEphcGFuIENvLixM
dGQuMRIwEAYDVQQLDAlUZXNOIFVuaXQxHjAcBgNVBAMMFXRlc3QuY3liZXJOcnVz
2t/rD9fTPgo7u4aYzw4BpnAqLmGgy3XpsvCo6f4ROcFsgrk05FgeUCaeDFyllEST
・・・・・
-----END NEW CERTIFICATE REQUEST-----
```

「-----BEGIN NEW CERTIFICATE REQUEST----- 」から、「-----END NEW CERTIFICATE REQUEST----- 」までをハイフンを含め、すべてコピーし申請画面に貼り付けてください。1 文字でも欠けるとフォーマットエラーとなりますのでご注意ください。

【！】CSR 作成後の注意事項

発行されたサーバー証明書は CSR を作成したエイリアスと同一のエイリアスへインストールします。インストールを行う前にキーストアファイルやエイリアスの削除を行わないよう、ご留意ください。

証明書のインストール

【！】本手順はサーバー証明書の発行後に行います。

5. 証明書のダウンロード

インストールが必要となる中間 CA 証明書・SSL サーバー証明書を事前にダウンロードします。

5.1. ルート・中間 CA 証明書のダウンロード

サーバー証明書をご利用の際、お使いの機器へルート証明書と中間 CA 証明書のインストールが必要となります。

ご選択いただいた商品により必要な証明書が異なりますので、証明書の種類をご確認のうえ、以下弊社ホームページからダウンロードしてください。

≫ EV SSL Plus 中間 CA 証明書ダウンロード

≫ SSL Plus 中間 CA 証明書ダウンロード

5.2. SSL サーバー証明書のダウンロード

SSL サーバー証明書が発行されましたら、証明書発行のお知らせのメール内リンクより事前にダウンロードし、【.cer】や【.txt】などの拡張子で保存してください。

6. 証明書のインストール

ルート証明書、中間 CA 証明書、SSL サーバー証明書の順番でインストールします。

※本手順では以下の設定を例としてご案内しています。

項目	ファイル名	エイリアス名
ルート証明書	DCRoot.cer	root
中間 CA 証明書	DC_CA.cer	CA
SSL サーバー証明書	DigiCert.cer	cybertrust
作成したキーストア	server.keystore	

6.1. ルート証明書のインストール

ルート証明書のインストールを行います。

A) コマンドプロンプトで以下のコマンドを入力し、ルート証明書をインストールします。

※「ルート証明書エイリアス名」は、他のエイリアス名と重複しないように異なるエイリアス名を指定してください。

■ コマンド入力

keytool -import -alias 「ルート証明書エイリアス名(任意)」 -keystore 「キーストアファイル名」 -file 「ルート証明書ファイル名」

例)keytool -import -alias root -keystore server.keystore -file DCRoot.cer

B) キーストアファイルに設定したパスワードを入力します。

```
キーストアのパスワードを入力してください:
```

C) 「yes」と入力して Enter ボタンを押します。

```
この証明書を信頼しますか? [no]:  yes
```

D) 以上でルート証明書のインストールが完了します。

```
証明書がキーストアに追加されました。
```

6.2. 中間 CA 証明書のインストール

中間 CA 証明書のインストールを行います。

A) コマンドプロンプトで以下のコマンドを入力し、中間 CA 証明書をインストールします。

※「中間 CA 証明書エイリアス名」は、他のエイリアス名と重複しないように異なるエイリアス名を指定してください。

■ **コマンド入力**

keytool -import -alias「中間 CA 証明書エイリアス名(任意)」-keystore「キーストアファイル名」-file「中間 CA 証明書ファイル名」

例)keytool -import -alias CA -keystore server.keystore -file DC_DC.cer

B) キーストアファイルに設定したパスワードを入力します。

```
キーストアのパスワードを入力してください:
```

C) 以上で中間 CA 証明書のインストールが完了します。

```
証明書がキーストアに追加されました。
```

6.3. SSL サーバー証明書のインストール

SSL サーバー証明書のインストールを行います。

A) コマンドプロンプトで以下のコマンドを入力し、SSL サーバー証明書をインストールします。

※「SSL サーバー証明書エイリアス名」は、キーペアファイル作成時に指定したエイリアス名を指定してください。

■ **コマンド入力**

keytool -import -alias 「SSL サーバー証明書エイリアス名」 -keystore 「キーストアファイル名」 -file 「SSL サーバー証明書ファイル名」

例)keytool -import -alias cybertrust -keystore server.keystore -file DigiCert.cer

B) キーストアファイルに設定したパスワードを入力します。

```
キーストアのパスワードを入力してください:
```

C) 以上で SSL サーバー証明書のインストールが完了します。

```
証明書応答がキーストアにインストールされました。
```

以上でルート証明書、中間 CA 証明書、SSL サーバー証明書のインストールは完了です。

7. SSL 通信の有効化設定

SSL 通信を有効にするため、Tomcat の設定を行います。

※本手順では以下の設定を例としてご案内しています。

ファイル名	保存ディレクトリ
server.xml	C:¥Program Files¥Apache Software Foundation¥Tomcat 6.0¥conf¥server.xml
キーストアファイル	C:¥Program Files¥Apache Software Foundation¥server.keystore

7.1. SSL 通信の有効化手順

A) 「server.xml」をテキストエディタで開き、<Connector>タグを編集して、SSL 通信を有効にします。

以下の記述がコメントアウトされている場合は「<!--」と「-->」を削除し、「keystoreFile」と「keystorePass」の設定項目を追加してください。

■ **設定内容**

```
<!--
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="キーストアファイルのディレクトリ"
keystorePass="キーストアファイルのパスワード"
/>
-->
```

例）

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="150" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="C:¥Program Files¥Apache Software Foundation¥server.keystore"
keystorePass="Password"
/>
```

■ 更新や他社からの乗り換えの場合

以下のいずれかの設定を行ってください。

・「keystoreFile="キーストアファイルのディレクトリ"」の指定先を、新たに作成したキーストアファイルの保存先ディレクトリへ変更する。

・「keystoreFile="キーストアファイルのディレクトリ"」の指定先を変更せず、既存のキーストアファイル名と同一にリネームし、キーストアファイルを置き換える。

B) 必要に応じて使用するポートを変更してください。

例)8443 ポート(デフォルト)を 443 ポートへ変更する場合

＜変更前＞

Connector port="8443"

＜変更後＞

Connector port="443"

以上で、SSL 通信の有効化設定は完了です。設定を反映させるため、再起動を行ってください。

8. キーストアファイルのバックアップ

秘密鍵ファイルを含むキーストアファイル(server.keystore など)は、証明書のインストール時に必要となります。

万が一に備えて、必ず別のメディア(CDや USB 等)にコピーして安全な場所に保管してください。

なお、弊社がお客様のキーストアファイルの情報を受け取ることはございません。あらかじめご了承ください。

SSL 通信の確認

9. SSL 通信の確認

サーバー証明書が正しくインストールされ、エラーやセキュリティ警告が表示されず、正常に SSL 通信が可能であることを確認します。

SSL 通信の確認は設定を行っているサーバー以外の Web ブラウザや携帯電話、スマートフォンなどの携帯端末などから行うことを推奨します。

■ 設定確認例

- Internet Explorer 11

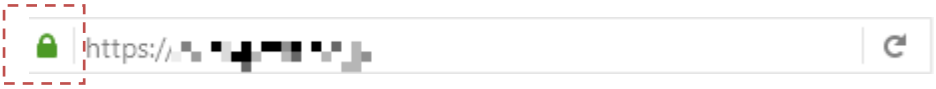
＜EV SSL Plus＞

＜SSL Plus＞

- Firefox 51

＜EV SSL Plus＞

＜SSL PLus＞



10. ご参考までに

ご参考までに、エイリアスの内容確認や削除方法をご案内します。

10.1. エイリアスの確認方法

以下のコマンドにてキーストアファイルに登録されているエイリアスの内容を確認できます。

■ コマンド

keytool -list -v -alias「エイリアス名」-keystore「キーストアファイル名」

例)keytool -list -v -alias cybertrust -keystore server.keystore

項目	内容
別名	エイリアス名
作成日	エイリアスを作成した日時
エントリタイプ	PrivateKeyEntry ⇒ 秘密鍵の含まれているエイリアス
	trustedCertEntry ⇒ 秘密鍵の含まれていないエイリアス
証明連鎖の長さ	エイリアスの中に登録されている証明連鎖の長さ 例)DigiCert EV SSL Plus および DigiCert SSL Plus の場合 ⇒「3」と表示されます。
証明書[n]	証明連鎖の番号

10.2. エイリアスの削除方法

以下のコマンドにてキーストアファイルに登録されている不要なエイリアスを削除できます。

■ コマンド

keytool -delete -alias「削除したいエイリアス名」-keystore 「キーストアファイル名」

例）keytool -delete -alias「cybertrust」-keystore 「server.keystore」

キーストアファイルに設定したパスワードを入力後、指定したエイリアスが削除されます。

```
キーストアのパスワードを入力してください:
```