（参考資料としての利用に限る）

Tomcat　CSR ファイル作成方法および証明書設定方法（新規・更新）

【必ず参照してください！】Tomcat 上でのサーバ証明書の取り扱いには Keytool が必須です。以下サイトで Keytool の概要をまずは、把握してください。

https://docs.oracle.com/javase/jp/1.5.0/tooldocs/windows/keytool.html

1.　証明書の生成・設定に関わる処理は、キーストアファイルとトラストストアファイルが格納されたディレクトリ内（keytool は実行元のディレクトリにキーストアファイルを作成します）で行います。

2.　外部サーバで生成した秘密鍵およびお客様サーバ証明書をインポートされる場合には、直接 4. にお進みください。

3.　CSR の作成方法

(ア) 事前準備

①　Tomcat 上で CSR を生成するためには、Java Keytool が必要です。
Keytool は JDK(Java SE Development Kit)の中に含まれておりますので、以下 Oracle 社のホームページより **Java2 SDK1.2 以上**を入手してください。
なおデフォルトでのパスワード設定は **changeit** になっています。
http://www.oracle.com/technetwork/java/javase/downloads/index.html

②　本ガイドでは以下環境を前提としていますので、お客様の環境に合わせてご活用ください。
コモンネーム　　www.jcert.biz
キーストアのファイル名　　sfssl.keystore　（一つのキーストアファイルに複数の鍵ペアを生成することや、1 台のサーバに複数のキーストアファイルを作成することも可能です。）
証明書エリアス名※　jcert　（エリアスとは、証明書あるいは秘密鍵を管理する単位で、お客様が認識できれば任意に名付け頂いて結構です。　証明書エリアスにより 1 つの秘密鍵を特定することができます。）
CSR のファイル名　　newcsr.csr

③　CSR 生成情報入力に使用できる文字には、以下の制限があります。これを守らないと、CSR が生成できません。 入力は、全て半角で行います。**なお、コモンネームには以下の「英字」「数字」および「 - （ハイフン）」のみが利用できます。**

字種	使用できる範囲
英字、数字	大文字 A～Z　小文字 a～z　0～9
記号 スペース	'(アポストロフィ)　-（ハイフン）　.(ピリオド)

④　更新の際の注意点

更新の際は、キーストアを新規に作成することをお勧めします。

誤ってキーストアファイルを上書きしないよう、ファイル名に日付を付加するなどご注意ください。　（他方、前回と同じ秘密鍵をご利用になる場合、前回生成した CSR をご用意いただくか、　以下手順（エ）のみ実行してください。）

(イ) キーストア内に秘密鍵を作成

①　次のコマンドを実行し、お客様情報（弊社情報を適宜変更してください）を入力します。

```
#keytool -keysize 2048 -genkey -alias jcert -keyalg RSA -keystore sfssl.keystore
Enter keystore password:  changeit
What is your first and last name?…コモンネームを指定してください！
  [Unknown]:  www.jcert.biz
What is the name of your organizational unit?
  [Unknown]: System 1
What is the name of your organization?
  [Unknown]:  J Cert Inc.
What is the name of your City or Locality?
  [Unknown]:  Chiyoda-ku
What is the name of your State or Province?
  [Unknown]:  Tokyo
What is the two-letter country code for this unit?
  [Unknown]:  JP
Is <CN=www.jcert.jp, OU="SSL Servces", O="J Cert Inc.", L=Chiyoda-ku, ST=Tokyo, C=JP>
correct?
  [no]:  yes（入力情報に誤りがなければ、yes と入力してください）
Enter key password for <tomcat>
        (RETURN if same as keystore password):  （デフォルト設定から変更しない場合はそのままリターンキーを押してください）
```

※KeyStore のパスワードと秘密鍵のパスワードを同じものにして下さい。別々のパスワードを設定すると Tomcat が起動出来ません。

②　これでキーストア **sfssl.keystore** に秘密鍵ができます。

(ウ) 秘密鍵のバックアップについて

① サーバ証明書が発行されるまでに、サーバトラブルなどで、秘密鍵が失われてしまう可能性があります。

② 秘密鍵とサーバ証明書はペアですので、秘密鍵が失われるとサーバ証明書も使用できなくなってしまいます。

③ これを防止するためにも、秘密鍵ファイルを別の媒体にバックアップしておきます。

(エ) CSR の作成

① 次のコマンドを実行しデフォルトのパスワード changeit を入力すると、newcsr.csr というファイル名で CSR が生成されます。

```
# keytool -certreq -keyalg RSA -alias jcert -file newcsr.csr -keystore sfssl.keystore
```

② 生成された CSR をテキストエディタで展開し、ハイフン（-----BEGIN）からハイフン（END NEW CERTIFICATE REQUEST----）までを漏らさず、弊社申請画面に Paste してください。

4. 証明書設定（インストール）

(ア) 事前準備

本ガイドでは Starfield ルートを利用して以下環境を前提としていますので、**Go Daddy ルートを利用される場合は sf -> gd に置換えてご活用ください。**

コモンネーム　www.jcert.biz
キーストアのファイル名　　sfssl.keystore
ルート証明書エリアス名　※　　sfroot　（エリアスとは、証明書と秘密鍵のペアを管理する単位で、お客様が認識できれば任意に名付け頂いて結構です。）
中間 CA 証明書エリアス名　※　sfinter
ルート証明書のファイル名　　sfroot-g2.crt
中間 CA 証明書のファイル名　　sfig2.crt

(イ) ルート証明書のインストール

ルート証明書（sfroot-g2.crt）は、「証明書を設定する前に（準備作業)」をご一読頂き、**中間証明書一覧から取得**してください。　https://www.jcert.co.jp/support/certificate.html
サーバに保存後、次のインストールコマンドを実行します。

```
# keytool -import -alias sfroot -keystore sfssl.keystore -trustcacerts -file sfroot-g2.crt
Enter keystore password:  changeit
----（ルート証明書情報）----
Trust this certificate? [no]:  yes
Certificate was added to keystore（ルート証明書インストール完了！）
```

一つのキーストアファイルには、一対のルート証明書および中間証明書が設定されていれば、複数の【証明書エリアス】（秘密鍵）で共有できます。

(ウ) 中間証明書のインストール

中間証明書（sfig2.crt）は、「証明書を設定する前に（準備作業）」をご一読頂き、**中間証明書一覧から取得**してください。　https://www.jcert.co.jp/support/certificate/

```
# keytool -import -alias sfinter -keystore sfssl.keystore -trustcacerts -file sfig2.crt
    Enter keystore password:  changeit
    ----（中間証明書情報）----
    Trust this certificate? [no]:  yes
    Certificate was added to keystore（中間証明書インストール完了！）
```

(エ) サーバ証明書のインストール

① **サーバ証明書は、キーストアファイル内の【証明書エリアス】ごとに設定します。（ここでは jcert として設定）**

② 弊社からの「証明書発行」通知メールに添付された ZIP ファイルから、サーバ証明書のデータをテキストエディタで展開し、（-----BEGIN CERTIFICATE----- から -----END CERTIFICATE----- まで）をコピーしてサーバに保存（**ファイル名：jcert.crt**）します。

③ 次のインストールコマンドを実行します。（キーストア作成時のエリアスを指定します。）

```
# keytool -import -alias jcert -keystore sfssl.keystore -trustcacerts -file jcert.crt
    Enter keystore password:  changeit
    Certificate reply was installed in keystore（サーバ証明書インストール完了！）
```

(オ) 次のコマンドを実行することで、上記で設定されたキーストアの内容を確認できます。

```
# keytool -list -v –alias jcert -keystore sfssl.keystore
```

(カ) SSL 通信有効化設定

① "server.xml"をテキストエディタに展開し、**下記③に該当する<Connector>タグ（のみ）を編集することで SSL 通信が有効**になります。

② 通常、デフォルトで当該記述がコメントアウトされておりますので、"<!--" と "-->" の符号を削除したうえで編集してください。

③　ポート番号がデフォルトでは **8443** になっているのを **443** に修正し、キーストアファイルのパスおよびパスワードを設定。

```
<Connector port="443"  address="IP アドレス"
protocol="HTTP/1.1"   SSLEnabled="true"   scheme="https"   secure="true"
clientAuth="false"   sslProtocol="TLS"   （その他のパラメータは任意設定可能です）
keyAlias="jcert"
keystoreFile="sfssl.keystore までのパス"     keystorePass="changeit" />
```

（注）**keyAlias** において、（証明書エリアス **jcert**）を特定することで、ひとつのキーストア内の複数の証明書・秘密鍵のペアを**<Connector>**タグ により区分設定できます。ただし、それぞれ個別の **IP** アドレスに関するパラメータ（上記青色帯）の追加記述が必要です。

④　tomcat を再起動。
お使いの環境に合わせた再起動プログラムを実行して下さい。
以下は Unix 環境での再起動例になります。
/etc/init.d/tomcat restart

5. 外部生成した「秘密鍵+証明書」のインポート
別途、当社お客様限定の詳細なる資料を用意しております。
https://jstore-v2.jcert.co.jp/user/contact
からお問い合わせ下さい。