

## 参考

<https://qiita.com/t-kuni/items/d3d72f429273cf0ee31e>

<https://github.com/t-kuni/self-sign-cert>

## Tomcat でオレオレ証明書を使って SSL を有効にする

手軽に有効にしたい場合は Java KeyStore ( JKS ) を使用する

### キーストア作成

1. `keytool -genkeypair -alias localhost -keyalg RSA -keysize 2048 -validity 36500 -ext SAN=DNS:localhost -keystore /usr/local/tomcat/conf/localhost-rsa.jks -storepass changeit -keypass changeit -dname "CN=localhost, OU=SSL_TEST, O=SSL_TEST, L=SSL_TEST, ST=SSL_TEST, C=SSL_TEST"`
  1. `sotrepass` のデフォルトパスワードは `changeit`
  2. `-validity 36500` で 100 年有効

### server.xml 修正

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
    maxThreads="150" SSLEnabled="true">
  <SSLHostConfig>
    <Certificate certificateKeystoreFile="conf/localhost-rsa.jks"
      certificateKeystorePassword="changeit"
      certificateKeystoreType="JKS" />
  </SSLHostConfig>
</Connector>
```

### ブラウザにインポートする証明書

```
keytool -exportcert -alias localhost -keystore /usr/local/tomcat/conf/localhost-rsa.jks -storepass changeit -file certificate.crt
```

出力されたファイルを「信頼されたルート証明機関」にインポートして、chrome を再起動する。