JPRS サーバー証明書発行サービス

CSR 生成手順

Tomcat （新規/更新）

Version 1.1

株式会社日本レジストリサービス（JPRS）

更新履歴

日付	Version	
2016/07/29	1.0	初版リリース
2017/10/18	1.1	「1.4 サーバー識別名 (DN) 情報の入力」を更新

次の手順に従い、鍵ペアと CSR を生成してください。
本手順書では、Unix 環境で Tomcat 4～8 で JRE 6～8 の JSSE を使用していることを前提に説明しています。 CSR 生成時は、TLS/SSL のサーバーをホストしているコンピュータに管理者として ログインしていることを確認してください。

【注意事項】

本手順ではパスワードを入力する手順がありますが、 パスワード入力の際、バージョンにより入力したパスワードがエコーバックされる場合があります。 パスワードの漏洩のないようにご注意ください。

また、古いバージョンの Tomcat 及び JRE には深刻な脆弱性も知られていますので、
Tomcat 及び JRE は、最新版に更新しておくことを推奨します。

«Tomcat 4 をご利用の場合»

Tomcat 4 では PureTLS を優先します。JSSE をご使用の場合は、以下に示すいずれかの方法でご対応ください。

- server.xml ファイルで Factory 要素の TLS/SSLImplementation 属性の値を「org.apache.tomcat.util.net.JSSEImplementation」 と明示する
- PureTLS をアンインストールする

«Windows 版をご利用の場合»

実際の表記や用語が異なりますので、 作業時に読み替えてください。

環境	Unix	DOS（Windows）
変数置換	${変数名}	%変数名%
パス名	/ディレクトリ名/ファイル名	ドライブ名:¥ディレクトリ名¥ファイル名
プロンプト	#や$	ドライブ名>
拡張子	sh	bat
コマンド・インタープリタ	シェル	コマンド プロンプト

1 鍵ペアの生成

1.1 ファイル生成マスクの値の記録および変更

1.1.1 ファイル生成マスクの値の記録

次のコマンドを実行し、 出力 (ファイル生成マスクの値) を記録します。

コマンド例： `$ umask`

※正常に終了すれば、「22」「007」など 0～7 までの数字が 1～4 桁 表示されます。

ここで出力された（記録した）数字は、手順　1-3.で使用します。

1.1.2 ファイル生成マスクの値の一時変更

1.1.3 出力された数字が 「77」「077」「0077」の 3 つ以外の場合

鍵情報の漏洩を防ぐため、 次のコマンドを実行してください (出力はありません)。

コマンド例： `$ umask 77`

1.2 鍵ストアと鍵ペアの生成

鍵ストアや鍵ペアの生成には、 keytool というコマンドを使用します。

※keytool のインストール箇所は、　${JAVA_HOME}/bin ディレクトリです。

（ `${JAVA_HOME}` : JRE を導入したディレクトリ）

鍵ペアを生成するためのコマンドを入力します。

現在ご利用中の鍵ペアがある場合は、上書きしないようご注意ください。

ⓘ **部署 (Organizational Unit) 名のある場合**

コマンド例： `$ keytool -genkey -alias tomcat -keyalg RSA -keysize 2048 -keystore /your/keystore/filename`

ⓘ **部署 (Organizational Unit) 名のない場合**

コマンド例：`$ keytool -genkey -alias tomcat -keyalg RSA -keysize 2048 -keystore /your/keystore/filename -dname "CN=www.jprs.co.jp, O=Japan Registry Services Co.¥, Ltd., L=Chiyoda-ku, ST=Tokyo, C=JP"`

※「-dname」 の後には、ウェブ・サーバー識別名 (DN)を指定します。
ここに指定する値が 「,」 文字を含む場合、「¥,」 のように入力してください。
シェルの種類によっては、
「"」 文字を 「'」 文字に変える
「¥¥」 のように重ねて指定する
場合があります。 シェルの仕様詳細はシステムに添付のマニュアルなどをご確認ください。
また、DN に指定する値については、手順 1-3.のプロンプトの説明を参照してください。

「tomcat」：
生成する鍵ペア名
Tomcat 6 または 7 の場合は、「tomcat」以外の鍵ペア名をつけることも可能です。

「/your/keystore/filename」：
生成する鍵ストアファイル名（ファイル名は任意）

1.3 鍵ストアのパスワード設定

プロンプトが表示されますので、鍵ストアに設定するパスワードを入力してください。

コマンド例： `Enter keystore password: changeit`

ⓘ **確認入力を促すプロンプトが表示された場合は**

同じパスワードを再入力してください。

コマンド例：`Re-enter new password: changeit`

1.4 サーバー識別名 (DN) 情報の入力

証明書内に組み込むサーバー識別名 (DN) 情報を入力します。

入力には以下の点にご注意ください。

- 半角の英数字 64 文字以内で入力してください。

- 識別名の入力には、以下の文字が使用できます。

  your first and last name（DN 情報の「CN」）

  - 半角英数字
  - "-"(ハイフン)
  - "."(ドット)
  - "*"(アスタリスク)

  その他の各項目

  - 半角英数字
  - 半角スペース
  - ","(カンマ)
  - "-"(ハイフン)
  - "."(ドット)
  - "/"(スラッシュ)
  - "("(かっこ)
  - ")"(閉じかっこ)
  - "'"(アポストロフィ)
  - ":"(コロン)
  - "="(イコール)
- 「&」が含まれる場合、半角英字の and 等に入力してください。
- スペースのみの入力はお控えください。 スペースのみの入力項目がある場合、 証明書が発行されません。
- 「,」が含まれる場合も、ここではそのまま入力できます。（「¥」を前置きするのは、コマンド行の引数として DN を指定する場合です）

各項目については以下を参照してください。

- **your first and last name（DN 情報の「CN」）**

  コモン・ネームになります。

  例）TLS/SSL 通信を行うサイトが<https://www.jprs.co.jp/>の場合

  「www.jprs.co.jp」

注意点

Web サーバー名に以下を使用することはできません。

- プロトコル特定子(http://)
- IP アドレスやポート番号
- パス名
- 「*」や「?」といったワイルドカード文字（※）

※：ワイルドカード証明書の場合「*.example.jp」のように、一番左側のラベルにワイルドカード文字を指定します。ワイルドカード証明書以外の証明書では、ワイルドカード文字は使用できません。

Webサーバー名は、TLS/SSL通信を行うサイトのURLのFQDN（Fully Qualified Domain Name）と同一でなければなりません。証明書に登録する Web サーバー名とサイトの URL のホスト名が一致しない場合、ブラウザがサイトへの安全な接続を拒否する場合があります。

例えば、コモン・ネームを「jprs.co.jp」として証明書を発行した場合、＜https://www.jprs.co.jp/＞でアクセスすると、Web サーバー名と(後方の一部は一致していますが)完全には一致していないため、ブラウザに警告が表示されます。なお、JPRS では「www」が含まれている名前と含まれている名前の双方について同一の証明書を利用可能にする「ダブルアドレスオプション」を提供しております。

※：ワイルドカード証明書の場合、サイトの URL の FQDN の一番左側のラベルとして、任意のホスト名を使用できます。ただし、*.example.jp に対し、test1.test2.example.jp など、複数の階層を持つ Web サーバー名を指定することはできません。

- **your organizational unit（DN 情報の「OU」）**

部署又はグループの名前になります。

※この項目を省略するには、手順 1.1 を参照ください。また、以下の情報は入力しないでください。

- ドメイン名および IP アドレス
- 記号のみ、およびスペースのみの値
- 「空欄」「該当なし」などの意味を示す文字列（「null」、「N/A」など）

- 申請組織以外の情報と誤解される恐れのある名称・社名・商号・商標
- 法人格を示す文字列（「CO.,Ltd」など）
- 特定の自然人を参照させる文字列
- 住所を示す文字列
- 電話番号

- **your organization（DN 情報の「O」）**

  申請組織名になります。

  例）日本レジストリサービスの場合 「Japan Registry Services Co.,LTD.」

- **your City or Locality（DN 情報の「L」）**

  通常、組織の本店（代表）が置かれている市区町村名になります。

  例）千代田区の場合 「Chiyoda-ku」

- **your State or Province（DN 情報の「ST」）**

  都道府県名になります。

  例）東京都の場合 「Tokyo」

- **the two-letter country code for this unit（DN 情報の「C」）**

  ISO による 2 文字の国名の符号になります。「JP」と入力してください。

  コマンド例：

```
What is your first and last name?
  [Unknown]: www.jprs.co.jp
What is the name of your organizational unit?
  [Unknown]: Sales Dept.
What is the name of your organization?
  [Unknown]: Japan Registry Services Co.,LTD.
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
```

1.5 DN 情報の確認

DN 情報が表示されますので、内容を確認してください。

コマンド例： Is CN=www.jprs.co.jp, OU=Sales Dept., O=Japan Registry Services CO.,LTD., L=Chiyoda-ku, ST=Tokyo, C=JP correct?

内容を確認後、yes と入力してください。

コマンド例：[no]:yes

プロンプトが表示されますので、何も入力せずリターン・キーを押してください。

コマンド例：Enter key password for <tomcat>
(RETURN if same as keystore password):

1.6 鍵ストアの確認

1.6.1 生成した鍵ストアを確認する場合は、次のコマンドを入力してください。

コマンド例： $ keytool -list -v -keystore /your/keystore/filename

※「/your/keystore/filename」：手順 1.1 で指定した鍵ストア名

1.6.2 プロンプトが表示されますので、鍵ストアに設定したパスワードを入力してください。

コマンド例： Enter keystore password: changeit

鍵ストアのファイルが表示されます。

コマンド例：

Keystore type: jks
Keystore provider: SUN
Your keystore contains 1 entry
Alias name: tomcat
Creation date: July 19 , 2016
Entry type: keyEntry

```
Certificate chain length: 1
Certificate[1]:
Owner: CN= www.jprs.co.jp, OU=Sales Dept., O=Japan Registry Services
CO.,LTD., L=Chiyoda-ku, ST=Tokyo, C=JP
Issuer: CN= www.jprs.co.jp, OU=Sales Dept., O= Japan Registry Services
CO.,LTD., L=Chiyoda-ku, ST=Tokyo, C=JP
Serial number: 60caadcd
Valid from: Wed July 19 00:00:00 JST 2016 until: Wed July 19 00:00:00 JST
2017
Certificate fingerprints:
MD5: 2A:27:97:FE:28:FA:E7:12:F6:11:D2:04:DF:66:97:9D
SHA1: CA:C0:2F:84:FF:B6:0F:3F:7A:D8:20:B0:70:AB:06:E4:49:DA:66:5A
*******************************************
```

2 CSR の生成

鍵ペアが作成されたことを確認後、CSR を生成します。

2.1 CSR の生成

次のコマンドを入力し、 CSR を生成してください。

コマンド例： $ keytool -certreq -sigalg SHA256withRSA -alias tomcat -file server.csr -keystore /your/keystore/filename

※「tomcat」： 手順 1.1 で指定した鍵ペア名

※「/your/keystore/filename」： 手順 1.1 で指定した鍵ストア名

※「server.csr」：CSR が保存されるファイル名

2.2 パスワードの入力

プロンプトが表示されたら、鍵ストアに設定したパスワードを入力してください。

コマンド例： Enter keystore password: changeit

2.3 生成されたファイルの確認

CSR (例:server.csr)が生成、保存されます。

【CSR のサンプル】

```
-----BEGIN CERTIFICATE REQUEST-----
MIISDOIUIkmlsRRIkSIIskjauASKJIaIOSISLKjwBgNVBAgTDFdlc3RlcmAgQ2FwZTES
MBAGA1UEBxMJQ2FwZSBUb3duMRQwEgYDVQQKEwtPcHBvcnR1bmlOaTEYMBYGA1UECxMP
T25saW5lIFNlcnZpY2VzMRowGAYDVQQDExF3d3cuZm9yd2FyZC5jby56YTBaMA0GCSqG
SIb3DQEBAQUAAAkImLKSuIjSOIjsfBWu5WLHD/G4B8ZOwiJUUsIIkfq/IuuIz6oCq6h
tdH7/tvKhh
-----END CERTIFICATE REQUEST-----
```

ここで生成した CSR を、申し込み画面に貼り付けて申請いただきます。

※openSSL コマンドのインストールをされている場合、CSR の内容（DN 情報）は以下のコマンドで確認いただけます。

コマンド例： `$ openssl req -noout -text -in server.csr`

※「server.csr」 ： CSR を保存したファイル名

CSR および鍵ペアの生成は、以上で完了です。

※重要

- 作成した鍵ペアのファイルは、 必ずバックアップをとって 安全な場所に保管してください。また、鍵ストアに指定したパスワード、鍵ストアのパスワードを指定する server.xml ファイルやそのファイルのある conf ディレクトリのアクセス管理を、確実に行ってください。
- 鍵ペアのファイルの紛失、 パスワード忘れ等が発生した場合、 証明書のインストールができなくなります。 この場合、 新たに証明書をご購入いただくことになりますので、 ご注意ください。必要な場合は、システムのフルバックアップをおとりください。フルバックアップ方法につきましては、製品のマニュアル等をご確認ください。