



JPRS サーバー証明書発行サービス

サーバー証明書 インストール手順 (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 |
| 2026/04/28 | 1.1 | クロスルート証明書の手順を追記 古いバージョンに関する記載を削除 |

注意事項

作業の前に Java の系列を確認してください。インポート時と実行時とで Java の系列が異なると、鍵ストア・ファイルがうまく読めないことがあります。

《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行ってください。

| 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> |
| ファイルをつなぐコマンド | cat | type |
| 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 |

中間 CA 証明書、サーバー証明書をダウンロードし、次の手順に従い証明書を設定してください。

1 事前準備

1.1 中間 CA 証明書とクロスルート証明書のダウンロード

以下より中間 CA 証明書とクロスルート証明書をダウンロードし、保存してください。

- 中間 CA 証明書について

<https://jprs.jp/pubcert/info/intermediate/>

1.2 サーバー証明書のダウンロード

1.2.1 JPRS から送付される場合

JPRS から送付されるメール「サーバー証明書ダウンロード手続きのご案内[FQDN]」に記載されている URL より証明書をダウンロードしてください。

1.2.2 指定事業者から提供される場合

それぞれの事業者の指定する方法にてダウンロードしてください。

※詳細はサーバー証明書を購入した指定事業者にお問合せください。

2 証明書インストール方法

2.1 サーバー証明書と中間 CA 証明書、クロスルート証明書をつなぐ

次のコマンドを入力し、ダウンロードしたサーバー証明書（例：example.crt）と上記の中間 CA 証明書（例：JPRS.cer）とクロスルート証明書（例：tlsrsarootca2024cross-pem.cer）をつなぎます。

```
コマンド例： $ cat example.crt JPRS.cer tlsrsarootca2024cross-pem.cer  
>combined.crt
```

「combined.crt」：任意のファイル名

2.2 証明書のインストール

次のコマンドを入力し、つないだ証明書をインストールしてください。

```
コマンド例 : $ keytool -import -alias tomcat -file combined.crt -keystore  
/your/keystore/filename
```

「tomcat」 : 申し込み時に作成した鍵ペアの名前。

Tomcat 6 以降をご利用の場合は、設定ファイル
(conf/server.xml) の Connector 要素の keyAlias 属性に指
定した値と同一です。

「combined.crt」 : 上記手順 1-1.で作成したファイルの名前

「/your/keystore/filename」 : 申し込み時に作成した鍵ストアのフルパス名

2.3 パスワードの入力

プロンプトが表示されたら、パスワードを入力してください。

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

「changeit」 : 申し込み時に作成した鍵ストアのパスワード

※JRE のバージョンにより、次のようなプロンプトが表示されることがあります。表示
された場合は、「yes」と入力してください。

コマンド例 :

```
Top-level certificate in reply:  
Owner: CN=www.jprs.co.jp, O="Japan Registry Services Co., Ltd.", L=Chiyoda-ku, ST=Tokyo, C=JP  
Serial number: af0956e23f804902  
Valid from: Fri Jul 15 15:32:59 JST 2016 until: Sun Aug 14 15:32:59 JST 2016  
Certificate fingerprints:  
MD5: B9:F8:68:FD:01:71:73:83:77:DB:1A:81:68:E4:97:72  
SHA1: 1B:66:D1:1E:2D:3A:3E:25:9B:69:92:E1:1C:18:A4:3D:FC:49:A0:E6  
SHA256: D6:31:38:E3:0B:51:AC:3E:A3:FB:9C:7E:CA:4F:52:11:50:B0:E5:80:A6:1B:66:9A:7F:5A:E7:E2:FE:E8:D4:9F  
Version: 1  
... is not trusted. Install reply anyway? [no]: yes
```

プロンプトが日本語表示の場合

環境によっては、次のように日本語で表示される場合があります。

コマンド例 :

```
所有者: CN=www.jp.rs.co.jp, O="Japan Registry Services Co., Ltd.", L=Chiyoda-ku, ST=Tokyo, C=JP
発行者: CN=www.jp.rs.co.jp, O="Japan Registry Services Co., Ltd.", L=Chiyoda-ku, ST=Tokyo, C=JP
シリアル番号: af0956e23f804902
有効期間の開始日: Fri Jul 15 15:32:59 JST 2016 終了日: Sun Aug 14 15:32:59 JST 2016
証明書のフィンガプリント:
MD5: B9:F8:68:FD:01:71:73:83:77:DB:1A:81:68:E4:97:72
SHA1: 1B:66:D1:1E:2D:3A:3E:25:9B:69:92:E1:1C:18:A4:3D:FC:49:A0:E6
SHA256: D6:31:38:E3:0B:51:AC:3E:A3:FB:9C:7E:CA:4F:52:11:50:B0:E5:80:A6:1B:66:9A:7F:5A:E7:E2:FE:E8:D4:9F
署名アルゴリズム名: SHA256withRSA
バージョン: 1
この証明書を信頼しますか。 [no]:
```

2.4 インストールの確認

次のように表示されることをご確認ください。

コマンド例 : `Certificate reply was installed in keystore`

以上で証明書のインストールは完了です。

証明書のファイルの削除

作業完了後、作成した証明書のファイルは不要になりますので、次のコマンドの入力により削除していただいて問題ありません。

コマンド例 : `$ rm -f combined.crt`

3 TLS/SSL の有効化 および 再起動

TLS/SSL を有効にし、再起動を行います。TLS/SSL を設定済みであれば、次のように設定されているかどうかをご確認いただき、再起動を行ってください。

3.1 TLS/SSLの有効化

次のような Connector 要素を、server.xml ファイルに指定してください。

- 「443」 : Tomcat が待ち受けるポートの番号
※ Tomcat 付属の設定ファイルでは 8443 番ポートですが、https では既定で 443 番ポートを使用します。
- 「changeit」 : 申し込み時に作成した鍵ストアのパスワード
- 「/your/keystore/filename」 : 申し込み時に作成した鍵ストアのフルパス名
- 「tomcat」 : 申し込み時に作成した鍵ペア名

注意:

鍵ストアのパスワードは、server.xml ファイルに**平文で指定**します。パスワードや秘密鍵が他人に漏洩しないよう、このファイルや conf ディレクトリの**許可モード**などにご注意ください。

Apache Tomcat 8.0.9 以降、Apache Tomcat 8.5.3 以降、Apache Tomcat 9.0.4～9.0.73 の場合

```
<!-- Define an SSL HTTP/1.1 Connector on port 8443
This connector uses the NIO implementation that requires the JSSE
style configuration. When using the APR/native implementation, the
OpenSSL style configuration is required as described in the APR/native
documentation -->
<!--
-->
<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol"
maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
keystoreFile="/your/keystore/filename" keystorePass="changeit"
keyAlias="tomcat"
clientAuth="false" sslProtocol="TLS" />
<!--
-->
```

Apache Tomcat 9.0.74 以降の場合

```
<!-- Define an SSL/TLS HTTP/1.1 Connector on port 8443
This connector uses the NIO implementation. The default
SSLImplementation will depend on the presence of the APR/native
library and the useOpenSSL attribute of the AprLifecycleListener.
Either JSSE or OpenSSL style configuration may be used regardless of
the SSLImplementation selected. JSSE style configuration is used below.
-->
<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol"
    maxThreads="150" SSLEnabled="true"
    maxParameterCount="1000"
    keystoreFile="/your/keystore/filename"
    keystorePass="changeit" keyAlias="tomcat">
```

Apache Tomcat 8.5.3 以降、Apache Tomcat 9.0.4 以降で SNI プロトコル拡張を使用する場合

Connector 要素の内側に次のような SSLHostConfig 要素を追加してください。

Connector 要素が「/>」で終わる自己区切りのときは、「/」文字の削除と同様、閉じタグ（「</Connector>」）も忘れず追加してください。

「JKS」でうまく機能しない場合、「pkcs12」も試してみてください。

```
<SSLHostConfig hostName="www.example.jp">
  <Certificate certificateKeystoreFile="/your/keystore/filename"
    certificateKeystorePassword="changeit"
    certificateKeyAlias="tomcat"
    certificateKeystoreProvider="SUN"
    certificateKeystoreType="JKS"
    type="RSA" />
</SSLHostConfig>
```

サーバー証明書 インストール手順 (Tomcat)

Apache Tomcat 10.0.2 以降、Apache Tomcat 10.1.0 以降、Apache Tomcat 11.0.0 以降 の場合

ひとつの Connector 要素の中に複数の SSLHostConfig 要素をお使いの場合、SSLHostConfig 要素の hostName 属性の値に FQDN を指定してください。

UpgradeProtocol 要素のあった場合でも、UpgradeProtocol 要素の変更は不要です。

```
<!-- Define an SSL HTTP/1.1 Connector on port 8443
This connector uses the NIO implementation. The default
SSLImplementation will depend on the presence of the APR/native
library and the useOpenSSL attribute of the
AprLifecycleListener.
Either JSSE or OpenSSL style configuration may be used regardless of
the SSLImplementation selected. JSSE style configuration is used below.
-->
<!--
-->
<Connector port="443" protocol="org.apache.coyote.http11.Http11NioProtocol"
    maxThreads="150" SSLEnabled="true">
  <SSLHostConfig>
    <Certificate certificateKeystoreFile="/your/keystore/filename"
      certificateKeyAlias="tomcat"
      certificateKeystorePassword="changeit"
      type="RSA" />
  </SSLHostConfig>
</Connector>
<!--
-->
```

注意:

鍵ストアのパスワードは、server.xml ファイルに**平文で指定**します。パスワードや秘密鍵が他人に漏洩しないよう、このファイルや conf ディレクトリーの**許可モード**などにご注意ください。

3.2 Tomcat の停止・再起動

設定を反映させるため、Tomcat を停止・再起動してください。

停止コマンド `$ ${CATALINA_HOME}/bin/catalina.sh stop` または

`$ ${CATALINA_HOME}/bin/shutdown.sh`

「`${CATALINA_HOME}`」 : Tomcat を導入したディレクトリ

再起動コマンド `# ${CATALINA_HOME}/bin/catalina.sh run` または

`# ${CATALINA_HOME}/bin/startup.sh`

参考: 待ち受けるポート番号によっては、スーパーユーザー特権が不要な場合もあります。

証明書のインストールは、以上で完了です。