# JPRS サーバー証明書発行サービス

## CSR 生成手順

OpenSSL（新規/更新）

Version 2.0

株式会社日本レジストリサービス（JPRS）

Copyright© 2025 Japan Registry Services Co., Ltd.

# 更新履歴

| 日付 | Version | |
|---|---|---|
| **2016/07/29** | 1.0 | 初版リリース |
| **2017/10/18** | 1.1 | 「2.1.2 サーバー識別名（DN）情報の入力」の更新 |
| **2024/03/21** | 1.2 | 「1.2 鍵ペアの生成」の更新、誤植の修正 |
| **2025/06/06** | 2.0 | 手順全体の更新 |

Copyright© 2025 Japan Registry Services Co., Ltd.

# 1 鍵ペアの生成

**OpenSSL 1.1 以降、または Windows 環境でご利用の場合は、鍵ペアの生成 (手順の 1-2.) のみを実行してください。**

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。

## 1.1 ファイル生成マスクの値の記録および変更（一部の環境のみ）

### 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

**出力された数字が 「77」「077」「0077」の 3 つ以外の場合にのみ**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 鍵ペアの生成

### 1.2.1 鍵ペアの生成コマンドの入力

以下の例では、 2048 ビットの RSA 鍵ペアを生成し、「servername.key」 (ファイル名は任意) というファイル名で保存することを示しています。
コマンド例：

秘密鍵にパスフレーズを設定せずに生成する場合

```
$ openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -out servername.key
```

Copyright© 2025 Japan Registry Services Co., Ltd.

※OpenSSL 1.0 以前の環境では以下のコマンドを入力してください。

```
$ openssl genrsa  -out servername.key 2048
```

秘密鍵にパスフレーズを設定して生成する場合

```
$ openssl genpkey -algorithm RSA -aes256 -pkeyopt rsa_keygen_bits:2048 -
out servername.key
```

※Windows 環境や古い nginx など、パスフレーズによる保護をサポートしていない
プラットホームやサーバーの場合、パスフレーズは設定しないでください。

## 1.3 ファイル生成マスクの値の復旧（一部の環境のみ）

1-1 で umask 77 コマンドを実行した場合のみ対応してください。

umask 77 コマンドを実行した場合は、ファイル生成マスクの値を復旧するため、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 《ファイル生成マスク値》`

「《ファイル生成マスク値》」：1-1.で記録した数字

Copyright© 2025 Japan Registry Services Co., Ltd.

# 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

### 2.1.1 CSR の生成コマンドの入力

以下の例では、アルゴリズム SHA-256 で CSR を作成し、「server.csr」 (ファイル名は任意) というファイル名で保存することを示しています。

コマンド例： `$ openssl req -new -key servername.key -out server.csr -sha256`

「servername.key」 : “1.鍵ペアの作成“で作成した、鍵ペアのファイル名

「-sha256」: アルゴリズムを示すオプション。

※0.9.8 以降の OpenSSL が、このアルゴリズムをサポートしています。

### 2.1.2 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。

  Common Name : サーバー名 :
  - 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)

Copyright© 2025 Japan Registry Services Co., Ltd.

- "-"(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 等に置き換えてください。
- 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

各項目については以下を参照してください。

- **Country Name : 国名**
  ISO による 2 文字の国名の符号になります。「JP」と入力ください。
- **State or Province Name : 都道府県名**
  都道府県名になります。
  例） 東京都の場合 「**Tokyo**」
- **Locality Name : 市区町村名**
  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**」
- **Organization Name : 組織名**
  お申込み者の組織名になります。
  例） 日本レジストリサービスの場合 「**Japan Registry Services Co., Ltd.**」
  ※申請組織とドメイン名登録者が異なる場合
  ドメイン名登録者の組織名ではなく、証明書発行先となる申請組織名の登録となりますので、ご注意ください。
- **Organizational Unit Name : 部署名**
  この項目は発行に先立ち削除されます。

Copyright© 2025 Japan Registry Services Co., Ltd. 

- **Common Name : サーバー名**

  コモン・ネームになります。

  例） TLS/SSL 通信を行うサイトが <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。

以下の項目は指定しないでください。

- **Email Address (emailAddress)**
- **A challenge password (challengePassword)**
- **An optional company name (unstructuredName)**

Copyright© 2025 Japan Registry Services Co., Ltd.

## 2.2 **生成されたファイルの確認**

要求された情報の入力が完了すると CSR が生成され、指定した名前のファイル (例：server.csr) に保存されます。

以下のコマンドで CSR の内容（DN 情報）を確認し、内容に間違いがないことをご確認ください。

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 CSR および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。鍵ペアのファイルの紛失が発生した場合、 証明書のインストールができなくなり、証明書の再発行が必要になりますのでご注意ください。

Copyright© 2025 Japan Registry Services Co., Ltd.