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 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	「2.1.2 サーバー識別名（DN）情報の入力」の更新

1 鍵ペアの生成

※Windows 環境でご利用の場合は　鍵ペアの生成 (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

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： `$ openssl genrsa -aes256 2048 >servername.key`

1.3 ファイル生成マスクの値の復旧

1-1.で umask 77 コマンドを実行した場合のみ対応いただきます。

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

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)
  - "-"(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
- CSR は、 emailAddress を含めないよう生成ください。
  - emailAddress を含んだ CSR を送付いただいても、当社発行の証明書には emailAddress は含まれません

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**

  部署又はグループの名前になります。この項目は省略できます。

  なお、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

- **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。

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。

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)**

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。

ここで生成した CSR を、お申し込み画面に貼り付けて申請いただきます。

※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ますので、 ご注意ください。