

はじめに -サーバ証明書インストールマニュアルについて-

| 改版履歴 | | | |
|-------|-----------|----|-----|
| 版数 | 日付 | 内容 | 担当 |
| V.1.0 | 2018/2/26 | 初版 | NII |

目次

1. はじめに

- 1-1. CSRとは
- 1-2. OpenSSLの利用について
- 1-3. 他のサーバ証明書インストールマニュアルとの比較について
- 1-4. 本書の範囲

1. はじめに

証明書自動発行支援システムサーバ証明書インストールマニュアル（以下、「本マニュアル」）は、UPKI電子証明書発行サービス（以下、「本サービス」）から発行された証明書を使用するためのCSRの作成方法、発行したサーバ証明書をインストールする方法について記載します。

1-1. CSRとは

CSR（証明書発行要求：Certificate Signing Request）は証明書を作成するための元となる情報で、その内容には、利用管理者が管理するSSL/TLS サーバの組織名、Common Name（サーバのFQDN）、公開鍵などの情報が含まれています。NII では、利用管理者に作成いただいたCSR の内容を元に、証明書を作成します。

```
CSRの例
----BEGIN CERTIFICATE REQUEST----
MIIBSTCB9AIBADCBjjELMAkGA1UEBhMCSIAXEDAObgNVBAcTB0FjYWRIbWUxKjAo
BgNVBAoTUU5hdGlvbmFslEluc3RpdHV0ZSBvZiBJbmZvcmlhdGJlc3EiMCAGA1UE
.....
IGu3rQIDAQABoAAwDQYJKoZIhvcNAQEEBQADQQCqpoKhuE6W4GpUhpSAJX51z
/ze
BvHWjt2CBnDeyalVNGr3+zdGKUpvWYG70RkIss4ST6PDF+RQw+TRdkzl8TUF
----END CERTIFICATE REQUEST----
```

1-2. OpenSSLの利用について

証明書を申請する際に必要となる鍵の作成やCSRの生成にはOpenSSLを利用することができます。OpenSSL のインストール方法等はOpenSSL Project (<https://www.openssl.org>) 等のインターネット上のサイトやダウンロードしたファイルに付属しているインストールマニュアルを参照してください。

1-3. 他のサーバ証明書インストールマニュアルとの比較について

本マニュアルでは、各サーバで使用する鍵ペア、CSR生成ツールとして、【鍵ペア生成時の共通事項】に記述したツールを使用して説明します。また、各サーバへインストールする必要がある証明書を【サーバ証明書インストールに必要な証明書一覧】に記述します。

【鍵ペア生成時に利用するツール】

○・・・該当する -・・・該当しない

| | OpenSSL | JavaKeytool | iKeyman |
|------------------|---------|-------------|---------|
| IBM- HTTP Server | - | - | ○ |
| OpenLDAP | ○ | - | - |
| Tomcat | - | ○ | - |
| Apache(mod_ssl) | ○ | - | - |
| IIS7.5 | ○ | - | - |
| IIS8.0 | ○ | - | - |
| IIS8.5 | ○ | - | - |

| | | | |
|---------|---|---|---|
| IIS10.0 | ○ | - | - |
| Nginx | ○ | - | - |

【サーバ証明書インストールに必要な証明書一覧】

○・・・該当する -・・・該当しない △・・・既存の証明書がある場合は該当しない

| | ルートCA証明書 | 中間CA証明書 | サーバ証明書 |
|------------------|----------|---------|--------|
| IBM- HTTP Server | ○ | ○ | ○ |
| OpenLDAP | - | ○ | ○ |
| Tomcat | ○ | ○ | ○ |
| Apache(mod_ssl) | - | ○ | ○ |
| IIS7.5 | △ | ○ | ○ |
| IIS8.0 | △ | ○ | ○ |
| IIS8.5 | △ | ○ | ○ |
| IIS10.0 | △ | ○ | ○ |
| Nginx | - | ○ | ○ |

1-4. 本書の範囲

本マニュアルでは以下の作業について記述をします。

| マニュアル名 | 内容 |
|---------------------|--|
| 操作手順書（利用管理者用） | <ol style="list-style-type: none"> 1. 利用管理者が実施する本システムへのサーバ証明書発行申請・取得について（「支援システム操作手順書 / 利用管理者用」 2-1.サーバ証明書新規発行手続き概要 に記載） 2. 利用管理者が実施する本システムへのサーバ証明書更新申請・取得について（「支援システム操作手順書 / 利用管理者用」 2-2.サーバ証明書更新申請手続き概要 に記載） 3. 利用管理者が実施する本システムへのサーバ証明書失効申請について（「支援システム操作手順書 / 利用管理者用」 2-3.サーバ証明書失効申請手続き概要 に記載） 4. 本システムへの証明書アップロードフォーマットについて(「支援システム操作手順書 / 利用管理者用」 5.本システムで扱うファイル形式 に記載) |
| サーバ証明書インストールマニュアル※1 | <ol style="list-style-type: none"> 1. CSRと鍵ペアの作成方法について 2. サーバ証明書のインストール方法について |

※1 以下のマニュアルを総称して「サーバ証明書インストールマニュアル」と呼びます。

- ・証明書自動発行支援システムサーバ証明書インストールマニュアル IBM-HTTPServer編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル Tomcat編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル Apache (mod_ssl)編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル IIS7.5編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル IIS8.0・IIS8.5編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル IIS10.0編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル Nginx編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル OpenLDAP編