# 京都教育大学

# UPKI 証明書申請マニュアル

V1.4 2024 年 10 月 31 日

情報処理センター

## 1 概要

UPKI 電子証明書発行サービス（以下、UPKI）は、国立情報学研究所が運用している、サーバー証明書、クライアント証明書、S/MIME 証明書の発行サービスです。暗号化（TLS）を用いた通信の普及のため、情報処理センターでは UPKI の契約を締結し、任意に発行することができるようにしています。学外へ公開するサービスだけではなく、全ての利用者向けサービスについてサーバー証明書を取得し、暗号化を行うことを推奨します。

このマニュアルでは、情報処理センターに UPKI 証明書の発行を申請する手順を説明します。各手順を実施するに当たり、UPKI の公式サイトにある規程・マニュアルを参考にしてください。

UPKI 公式サイト https://certs.nii.ac.jp/

サービスによって技術的な事柄に関する手順は異なります。CSR の作成や登録については、サービスの保守業者にお問い合わせください。

証明書発行に関する最新の情報、または、このマニュアルの最新版は情報処理センターホームページの「UPKI 証明書発行サービス」を参照してください。

UPKI 証明書発行サービス
https://www.kyokyo-u.ac.jp/c_ipc/services/upki-certificate.html

## 2 サーバー証明書発行手順

サーバー証明書はサーバーにインストールすることで、通信の暗号化とサーバーが本物であることの証明を行います。おもに Web サービスに使用されますが、Web サービス

以外にも使用できます。

安全な暗号化には必要最低限セキュリティを保つために比較的新しい技術が求められます。そのため、発行される証明書は、Internet Explorer 等の古いブラウザーやガラケーなどの古い機器では使用できない場合があります。

## 2.1 発行条件

下記の条件を満たす場合のみ UPKI のサーバー証明書を発行します。

1　国立大学法人京都教育大学（附属学校園を含む、以下、大学という）が所有または借用している学内（場所を借用したデータセンターを含む）に設置された機器（プライベートクラウド上の仮想マシンを含む）、または、情報処理センターが契約・運用・管理しているパブリッククラウド上で提供されるサービス向けであること。
2　“kyokyo-u.ac.jp”ドメイン、または、そのサブドメインのホスト名（FQDN）が付与されていること。
3　申請者が大学の教職員であること。
4　サーバーを運用・管理する部署（学科、附属学校園等を含む）が実在すること。

## 2.2 CSR または TSV 作成

規定・マニュアルについては UPKI サイトを参考にしてください。マニュアルの内容は度々変更されるため、必ず毎回確認してください。

UPKI マニュアル https://certs.nii.ac.jp/manual/manuals

マニュアルおよび後述の DN 情報に従い、CSR または TSV を作成し、情報処理センターへ提出してください。情報処理センターで処理を実施後、発行された証明書のダウンロード URL が申請者のメールアドレスに送られます。有効期限内にダウンロードしてください。

CSR または TSV の作成時には、以下の点にご注意ください。

- 証明書の秘密鍵は、他の証明書と共通で使用せず、証明書毎に異なる鍵を作成してください。
- 証明書更新時は、既存の鍵を再利用せず、必ず新規に鍵を作成してください。

- 証明書の秘密鍵は厳重に取り扱ってください。漏洩した場合、証明書の再発行が必要になります。
- 一つのホスト名(CN)に付き一つの証明書を発行します。複数のサーバーで使用する場合は秘密鍵と証明書をコピーして使用してください。同一ホスト名(CN)に対して複数の証明書は発行できません[1]。

### 2.2.1 DN 情報

CSR 作成時の DN は下記のようにしてください。

| 項目 | 値 | 説明 |
|---|---|---|
| Country (C) | JP | 固定値 |
| State or Province Name (ST) | Kyoto | 固定値 |
| Locality Name (L) | Kyoto-shi | 固定値 |
| Organization Name (O) | Kyoto University of Education | 固定値 |
| Organizational Unit Name (OU) | (無し) | 利用禁止 |
| Common Name (CN) | URL のホスト名(FQDN) | |
| Email | (無し) | 利用禁止 |

CN の値であるホスト名(FQDN)は全て小文字にしてください。CN に大文字が含まれる場合、申請を受け付けません。OU および Email の値は設定しないでください。OU または Email が設定されている場合、申請を受け付けません。

CN 以外の名前が必要な場合でも、CSR に SAN(subjectAltName フィールド)は付けないでください。CSR で設定されていた SAN の値は証明書発行時に無視します。

---

[1] 証明書の SAN に記入する dNSName は名前が重複して発行可能です。複数の証明書が必要な場合は、証明書には異なる CN をつけて、TSV 発行時に同じ dNSName を指定してください。

### 2.2.2 新規・更新

TSV の作成は必須ではありません。TSV 作成方法がわからない場合は CSR をお送りください。(CSR の送付者が TSV での担当者になります。)

新規発行する場合は新規用 TSV を、既存の証明書から更新の場合は更新用 TSV を作成してください。更新用 TSV には失効対象証明書のシリアル番号が必要です。シリアル番号は現在の証明書から確認してください。

### 2.2.3 失効

サービス廃止等の理由で証明書が不要になった場合や、証明書の秘密鍵が漏洩した場合は、ただちに証明書失効処理を行う必要があります。失効用 TSV を提出、または、ホスト名と廃止理由を明記した上で情報処理センターにご連絡ください。

### 2.2.4 証明書アルゴリズム

アクセス元が最新 OS に限定される場合は ECDSA 証明書を推奨しますが、古い OS でもアクセス可能にしたい場合は RSA 証明書を発行してください。鍵の Bit 数、署名アルゴリズム、中間証明書は変更されることがあります。マニュアル及び発行時のメールを確認してください。

- ECDSA 証明書(ecdsa-with-SHA384)【推奨】(対象注意)
  - 暗号アルゴリズム: EC
  - 曲線名: secp384r1
  - 鍵の Bit 数: 384
  - 署名アルゴリズム: SHA384
  - 中間証明書: NII Open Domain CA - G7 ECC (nii-odca4g7ecc.cer)
  - 対応ブラウザー: 主要な最新ブラウザー(Apple 製品は最新 OS に限る)[2]
- RSA 証明(sha256WithRSAEncryption)
  - 暗合アルゴリズム: RSA
  - 鍵の Bit 数: 2048
  - 署名アルゴリズム: SHA256

---

[2] Apple 製品の ECDSA 証明書対応は、macOS 15、iOS 18、iPadOS 18、tvOS 18、watchOS 11 以降です。これらより古い OS では証明書の警告が表示される場合があります。

- 中間証明書: NII Open Domain CA - G7 RSA (nii-odca4g7rsa.cer)
- 対応ブラウザー: ほとんど全てのブラウザー

Apple の古い OS は ECDSA 証明書に対応していません。最新の OS にアップデートできない古い Apple 製品(2018 年以前に発売された Mac、iPhone、iPad 等)からアクセスされる可能性がある場合は、使用しないでください。

秘密鍵は安全に管理されていれば暗号化しておく必要はありませんが、暗号化する場合は AES256 以上のアルゴリズムを使用することを推奨します。

### 2.2.5 URL とホスト名(FQDN)

DN の CN に記載する名前は URL のホスト名です。CN とホスト名が一致しない場合、ブラウザーで警告が表示され、正常に閲覧できません。URL が「https://example.kyokyo-u.ac.jp/」であった場合、"example.kyokyo-u.ac.jp"がホスト名になります。DN の CN にこの名前を入れてください。

同一サーバー(同一 IP アドレス)に複数のホスト名が必要な場合、dNSName による SAN(代替名)を利用することができます。dNSName に CN 以外の名前を追加することで、別名でも証明書を使用することができます。dNSName を追加する場合は次のようにしてください。

1. DN の CN には代表するホスト名をつけて、CSR を作成します。
2. TSV 作成時に「dNSName」に CN 以外の使用するホスト名を追加します。複数追加することも可能です。CN に記載されているホスト名は入れないでください。

CN に記載するホスト名も dNSName に記載するホスト名も小文字である必要があります。大文字が含まれる場合は、申請を受け付けません。

TSV 作成方法がわからない場合は、追加したいホスト名とあわせて CSR のみ提出してください。dNSName を使う場合は下記にご注意ください。この方法には以下の欠点があります。

- 複数追加可能ですが、追加可能な個数(全体の文字数)には制限があります
- 新たに追加が必要な場合は証明書を発行し直す必要があります。

dNSName を使う方法以外に SNI(Sever Name Indication)という機能を使うことで、ホスト名毎に異なる証明書を紐付けることが可能です。ホスト名毎に証明書を発行し、Web サーバーに複数の証明書を見に行くように設定します。追加数の制限はなく、また、新規追加時も既存の証明書の再発行は不要になります。ただし、下記の欠点は残り

ます。

- HTTPS 等の SNI に対応したプロトコルでのみ可能であるため、Web サービス以外の用途では使用できない場合があります。

## 2.3 申請・提出

CSR または TSV の提出をもって、発行依頼の申請とします。現在のところ、特に書類等の提出は必要ありません。下記問い合わせ先(情報処理センター)にメールで提出してください。

### 2.3.1 提出時の注意事項

- UPKI の規約上、業者からの申請は受け付けることができません。必ず、教職員から申請するようにしてください。
- CSR のみ送付する場合は、次の情報もお送りください。なお、TSV に記載する利用管理者は申請者の名前を登録します。
  - 証明書を使用する Web サーバーソフトウェア等
  - CN 以外で dNSName に設定する必要があるホスト名(ある場合)
- 申請者と TSV に記載の管理者が異なる場合は問い合わせさせて頂く場合があります。

# 3 クライアント証明書・S/MIME 証明書

UPKI はクライアント証明書と S/MIME 証明書の発行が可能です。現在のところ、本学では利用者への一般提供をしていません。教育・研究または業務で必要になる場合は個別で対応・発行しますので、情報処理センターまでご相談ください。

# 4 問い合わせ先

証明書発行サービスに関するお問い合わせは情報処理センターまでお願いします。

- 情報処理センター
  - メールアドレス: ipc@kyokyo-u.ac.jp
  - 電話番号: 075-644-8340

# 5 変更履歴

- v1.4 2024 年 10 月 31 日
  - ECDSA 証明書の Apple 製品対応状況に応じて推奨アルゴリズムを変更。
- v1.3 2024 年 7 月 25 日
  - CN 及び dNSName を小文字に限定。
  - ガラケーなどの古いブラウザーに関する記述を最初に記載。
  - コード署名用証明書の記載を削除し、S/MIME 証明書の記載を追加。
- v1.2 2022 年 1 月 1 日
  - 2022 年 1 月 1 日以降の OU 利用禁止。
  - 全体の調整。
- v1.1 2020 年 12 月 25 日
  - 2020 年 12 月 25 日の UPKI 中間認証局変更に対応。
- v1.0 2018 年 7 月 11 日
  - 初版発行。

以上