京都教育大学

UPKI 証明書申請マニュアル

V1.2 2022 年 1 月 1 日

情報処理センター

（2020 年 12 月 25 日 中間認証局変更対応版）
（2022 年 1 月 1 日 OU 廃止対応版）

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、コード署名用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

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。(2022 年 1 月 1 日以降)

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

2022 年 1 月 1 日以降は、OU を利用できません。[2]OU の値を設定されている場合、申請を受け付けません。

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 のみお送りください。(CSR の送付者が TSV での担当者になります。)

---

[1] 名前のエイリアスを記入する dNSName は重複して発行可能です。複数の証明書が必要な場合は、異なる CN をつけて、同じ dNSName で発行してください。

[2] UPKI のマニュアルでは OU の設定は任意となっていますが、2022 年 9 月 1 日から OU の利用が禁止されます。本学では先行して 2022 年 1 月 1 日から廃止します。

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。シリアル番号がわからない場合は、情報処理センターで更新用 TSV を作成しますので、CSR のみお送りください。

OU の利用禁止に伴い、2021 年 12 月 31 日以前に発行した証明書は、既存の証明書からの更新であってもすべて新規発行として処理する必要があります。以前の証明書で OU が設定されていた場合でも、CSR 作成の際は OU をつけないでください。TSV を作成する場合は新規発行として作成してください。

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

通常は 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。

- RSA 証明(sha256WithRSAEncryption)【推奨】
  - 暗合アルゴリズム: RSA
  - 鍵の Bit 数: 2048
  - 署名アルゴリズム: SHA256
  - 中間証明書: NII Open Domain CA - G7 RSA (nii-odca4g7rsa.cer)
  - 対応ブラウザ: ほとんど全てのブラウザ(サポートが終了した旧バージョンやガラケー等を除く)
- ECDSA 証明書(ecdsa-with-SHA384)
  - 暗号アルゴリズム: ECDSA
  - 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: Windows 上の Microsoft Edge と Google Chrome 等のみ(Windows 上の Mozilla Firefox や Mac OS、iOS、Android 上のブラウザは未対応)

UPKI では ECDSA(楕円曲線 DSA)サーバー証明書の発行に対応していますが、

Windows の証明書ストアを利用する一部のブラウザのみ対応になっています。OS およびブラウザが限定されている場合を除き、使用しないでください。

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 によるエイリアス(別名)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。

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。
- 一部のガラケーや古いスマートフォン、古いブラウザは対応していません。(最新ブラウザ、最新のスマーフォトンであれば問題はありません)

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。

- 一部のガラケーや古いスマートフォン、古いブラウザは対応していません。(最新ブラウザ、最新のスマーフォトンであれば問題はありません)

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・コード署名用証明書

UPKI はクライアント証明書とコード署名用証明書の発行が可能です。現在のところ、本学では一般に提供するスキームやシステムはありません。サービスの提供にあたり必要であれば個別で対応・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

- v1.2 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

以上