京都教育大学

UPKI 証明書申請マニュアル

V1.7 2026 年 6 月 10 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 作成や証明書インストール等の方法については、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「証明書発行サービス」を参照してください。

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

2 サーバー証明書発行手順（手動）

【警告】UPKI で発行されるサーバー証明書の有効期限は段階的に短くなり、2029 年3

月までに 47 日になります。UPKI がサポートする限り手動での更新方法は維持しますが、2029 年 3 月以降は毎月更新が必要になるため、現実的な方法ではありません。2029 年 3 月までに自動で証明書更新が可能になる ACME へ切り替えを行ってください。ACME の利用についての詳細は次章の「サーバー証明書発行手順（ACME）」をご確認ください。

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 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 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 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(Subject 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

[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、同じ「別名」を申請してください。

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されます。

2.2.2 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)【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
  - ルート CA: Security Communication ECC RootCA1
  - 対応ブラウザー: 主要な最新ブラウザー(Apple 製品は最新 OS[2]に限る)
- 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
  - 中間証明書: NII Open Domain CA - G8 RSA
  - ルート CA: SECOM TLS RSA Root CA 2024
  - 対応ブラウザー: ほとんど全てのブラウザー(クロスルート証明書[3]使用)

ECDSA 証明書は Apple の古い OS に対応していません。最新 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

[2] macOS 15、iOS 18、iPadOS 18、tvOS 18、watchOS 11 以降。

[3] Security Communication RootCA2 発行のクロスルート証明書。

セスされる可能性がある場合は、使用しないでください。

RSA 証明書を使用する場合は、中間証明書だけではなく、ルート CA のクロスルート証明書も証明書チェーンに追加してください。現在、SECOM TLS RSA Root CA 2024 を直接信頼するブラウザーは一部に限られますが、Security Communication RootCA2 から発行されたクロスルート証明書を使うことで、間接的に信頼されます。クロスルート証明書がないと、ブラウザーによっては信頼されない場合があります。

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してください。

2.2.3 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、SAN を利用することができます。SAN に CN 以外の dNSName 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。別名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. 申請時に、CN 以外の使用するホスト名を「別名」として指定してください。複数記載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 SAN の 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。また、いずれも “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）でなければなりません。別名は複数追加でき、規格上の数に制限はありませんが、UPKI では数と長さに制限があります[4]。別名は後から追加できないため、変更が必要な場合は証明書を発行し直す必要があります。

SAN 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振り分けて見に行くように設定します。追加数の制限は

[4] CN も含めてホスト名が 8 個以下、”dNSName=”をつけた全体の長さが 250 文字以内でなければなりません。

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、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

問い合わせ先（情報処理センター）へ、メールで CSR の提出することで、発行依頼の申請とします。書類の提出は必要ありません。メールには CSR を添付するともに、下記内容を記載してください。

- 担当部署
- 担当者
- メールアドレス（申請メール送信者）
- ホスト名（CN）
- Web サーバーソフトウェア名等
- 別名（複数可、必要な場合のみ）

新規発行と更新では申請に違いはなく、既存の発行済証明書があれば自動的に更新とみなします。更新の場合は、原則、有効期限の 30 日前からになりますが、理由があれば 31 日以上前から更新も可能です。有効期限の 31 日以上前に更新したい場合は、利用を明記してください。

2.3.1 申請時の注意事項

- 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。
- 「メールアドレス」は申請メールの送信者と同じでなければなりません。このメールアドレスに発行した証明書や有効期限切れ警告等が送られます。担当者が変更しても受け取れるように、部署等で使用するサーバーでは組織メールアドレスを使用してください。
- 「ホスト名」は CSR 記載の CN と同じでなければなりません。
- 「Web サーバーソフトウェア名等」は必須です。証明書をインストールするソフトウェア名またはサービス名を記述してください。
- 「別名」は複数記載することができますが、数と長さに制限があります。

- 発行に数営業日かかる場合があります。スケジュールに余裕をもって申請してください。即日発行が必要な場合は、事前にお問い合わせ先(情報処理センター)までご連絡ください。
- 更新対象証明書の情報は不要です。
- TSV での申請は受け付けません。[5]

2.3.2 メールテンプレート

下記は申請時のメールのテンプレートです。項目に漏れがなければ、フォーマットが異なっていても受け付けます。

- 題名: UPKI サーバー証明書発行申請
- 宛先: ipc@kyokyo-u.ac.jp
- 添付ファイル: CSR ファイル
- 本文:

> --- UPKI サーバー証明書発行 ---
> 担当部署: {学科、学校名、部署名等}
> 担当者: {担当者の氏名}
> メールアドレス: {メール送信者と同じ}
> ホスト名: {CN と同じ}
> Web サーバーソフトウェア名等: {必須}
> 別名: {CN 名以外の別名(FQDN)、不要の場合は省略}
> --- ---

2.3.3 提出後の作業

証明書が発行され次第、ダウンロード URL が記載されたメールが送られますので、証明書をダウンロードしてください。中間証明書に関する情報はメールに記載されていますので、あわせて確認してください。

アプリケーションの設定で中間証明書がサーバー証明書に含まれるようにしてください。RSA 証明書の場合、ルート CA のクロスルート証明書も中間証明書として含めるようにしてください。中間証明書やクロスルート証明書が正しく設定されていない場合、信頼

[5] 記入間違い等による差し戻しが多いため、TSV の受付は廃止しました。

性チェーンに失敗し、ブラウザー側で証明書のエラーが発生する場合があります。

3 サーバー証明書発行手順（ACME）

ACME はサーバー証明書を自動的に発行する仕組みです。UPKI では ACME に対応しており、certbot 等を用いた証明書の自動更新が可能です。手順の大まかな流れは、次のようになります。

1. 利用者は情報処理センターに ACME 利用を申請します。
2. 情報処理センターは利用者に ACME アカウント作成に必要な EAB 情報を返します。
3. 利用者は EAB 情報を ACME クライアント（certbot 等）に登録します。
4. ACME クライアントは ACME アカウントを作成し、サーバー証明書を取得します。
5. ACME クライアントは証明書の有効期限が短くなると、自動的にサーバー証明書を更新します。

ACME で発行される証明書は手動での発行と同じ[6]です。DN やアルゴリズム等の詳細は前章の「サーバー証明書発行手順（手動）を確認してください。その他、ACME に関する情報や利用方法等のマニュアルは UPKI のサイトを参照してください。

3.1 制限事項

- チャレンジ方式は HTTP-01 のみ動作を確認しています。他のチャレンジ方式での動作は確認していません。
- 原則として、学外に公開された Web サーバーでのみ使用できます。学内限定サーバーや Web 以外のサーバーでは使用できません。
- ECDSA 証明書にも対応していますが、UPKI のマニュアルでは RSA の事例のみ記載されています。
- 発行される EAB 情報は一つのサーバーでのみ使用できます。複数サーバーで冗長化されているシステムの場合、そのまま使用することはできません。複数サーバーで運用については構成の確認を行いますので、事前にお問い合わせ先（情報処理センター）までご連絡ください。

[6] 自動更新を前提とするため、有効期限のみ手動の場合よりも短く設定されます。

- 複数の別名をつけることができます。別名の制限は手動の場合と同じです。詳しくは「2.2.3 URL とホスト名(FQDN)」を参照してください。

3.2 発行条件

サーバー証明書発行手順記載の発行条件と同じです。

3.3 申請

問い合わせ先(情報処理センター)へメールで発行依頼の申請をします。書類の提出は必要ありません。メールには下記内容を記載してください。

- 担当部署
- 担当者
- メールアドレス(申請メール送信者)
- ホスト名(CN)
- Web サーバーソフトウェア名等
- 別名(複数可、必要な場合のみ)
- アルゴリズム(RSA または ECDSA、省略時は RSA)

申請したホスト名で既に発行済みの場合は、発行が必要な理由について確認を行う場合があります。

3.3.1 申請時の注意事項

- 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。
- 「メールアドレス」は申請メールの送信者と同じでなければなりません。このメールアドレスに発行した EAB 情報が証明書に関する情報が送られます。担当者が変更しても受け取れるように、部署等で使用するサーバーでは組織メールアドレスを使用してください。
- 「Web サーバーソフトウェア名等」は必須です。証明書をインストールするソフトウェア名またはサービス名を記述してください。
- 「別名」は複数記載することができますが、数と長さに制限があります。
- 自動発行される証明書アルゴリズムは手動の場合と同じです。通常は RSA を選択してください。ECDSA を希望する場合は「アルゴリズム」に記述してください。

- 発行される証明書の DN は手動手順に記載のルールに従います。
- 発行に数営業日かかる場合があります。スケジュールに余裕をもって申請してください。即日発行が必要な場合は、事前にお問い合わせ先(情報処理センター)までご連絡ください。ただし、発行される EAB 情報の有効期限は 14 日間ですので、約 1 週間前に申請することを推奨します。
- TSV での申請は受け付けません。

3.3.2 メールテンプレート

下記は申請時のメールのテンプレートです。項目に漏れがなければ、フォーマットが異なっていても受け付けます。

- 題名: UPKI ACME 発行申請
- 宛先: ipc@kyokyo-u.ac.jp
- 添付ファイル: (無し)
- 本文:

  --- UPKI ACME 発行 ---
  担当部署: {学科、学校名、部署名等}
  担当者: {担当者の氏名}
  メールアドレス: {メール送信者と同じ}
  ホスト名: {CN と同じ}
  Web サーバーソフトウェア名等: {必須}
  別名: {CN 名以外の別名(FQDN)、不要の場合は省略}
  アルゴリズム: {RSA または ECDSA、省略時は RSA}
  --- ---

3.3.3 申請後の作業

EAB 情報が発行され次第、情報処理センターから EAB 情報が記載されたメールをお送りします。EAB 情報は certbot へ登録するコマンドラインとして記述されています。certbot 以外の ACME クライアントを使用する場合は、certbot のマニュアルを参考に必要な情報を読み替えて登録してください。

EAB 情報について、下記にご注意ください。

- EAB 情報が漏洩した場合、第三者による証明書の取得などの重大インシデントが発生します。メールで送付されるコマンドラインは厳重に管理してください。

- EAB 情報の有効期限は 14 日間です。メールを受信してから 14 日以内に ACME アカウントの作成（certbot 等の ACME クライアントへの登録）を行い、証明書を発行してください。14 日以内に証明書が発行されなかった場合は、ACME アカウントが無効になります。期限切れとなった場合は、後述の再発行を依頼してください。
- EAB 情報を用いて ACME アカウントを作成（certbot 等の ACME クライアントへの登録）を行えるのは 1 度だけです。複数サーバーや複数回の登録はできません。作成済み ACME アカウントを削除してしまった等の理由で再登録が必要になった場合は、後述の再発行を依頼してください。
- EAB 情報を用いて作成した ACME アカウント（秘密鍵）は作成したサーバー内で厳重に管理してください。原則、他サーバーや作業用 PC 等へコピーしてはいけません。

3.4 再発行

期限切れや登録後の ACME アカウント削除等で、EAB 情報が使用できなくなった場合は再発行が必要です。再申請はせず、ホスト名と再発行理由を明記した上で問い合わせ先（情報処理センター）にご連絡ください。なお、再発行した EAB 情報で ACME アカウントが作成されると、以前に作られた ACME アカウントは使用できなくなります。再発行により複数のサーバーに登録することはできません。

3.5 サーバーの変更

ホスト名の割り当てを別のサーバーを変更する場合、ACME アカウントを新しいサーバーに移行することはできません。その場合は、再発行ではなく、新規で申請してください。ホスト名が同じでも ACME アカウントは新規に作成でき、新旧両方を同時に使用できます。

移行完了後は、必ずご連絡ください。不要になり次第、古い ACME アカウントを失効します。

4 クライアント証明書・S/MIME 証明書発行手順

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、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、お問い合わせ先(情報処理センター)までご連絡ください。

5 失効について

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。ホスト名と廃止理由を明記した上でお問い合わせ先(情報処理センター)にご連絡ください。ただし、有効期限切れの証明書については自動的に失効処理を行いますので、連絡は不要です。

6 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

7 変更履歴

- v1.7 2026 年 6 月 10 日
  - ACME が SAN(別名)に対応。
- v1.6 2026 年 3 月 19 日
  - ACME によるサーバー証明書発行手順を追加。
  - TSV での受付を廃止。
- v1.5 2025 年 12 月 17 日
  - RSA 証明書の中間証明書変更とクロスルート証明書に関する記述の追加。
  - 「提出後の作業」を追加。
- 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