UPKI電子証明書発行サービスについて

2023年10月17日　NIIサービス説明会

UPKI電子証明書発行サービス概要

UPKI電子証明書発行サービスとは

学術機関（大学，短大等）の実情にあった発行手順で，存在性・真正性の確認を行うことで，比較的安価で効率的に，電子証明書を発行するサービスです.

発行した証明書は，Web サーバやメール クライアント（Thunderbird や Outlook などのメーラー）などに組み入れ．暗号化・署名などに使用します.

UPKI電子証明書発行サービスの特徴

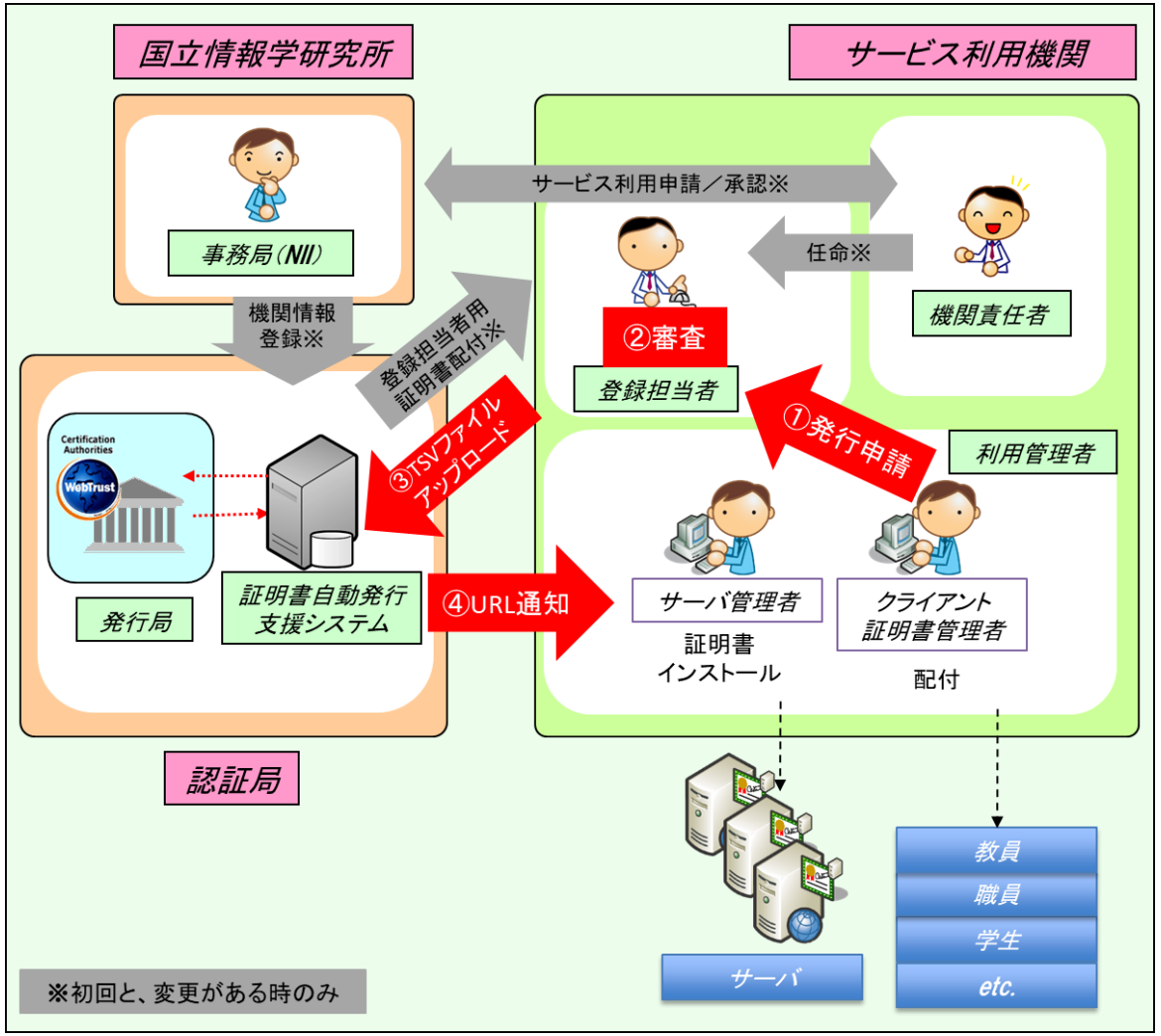
- 商用水準の電子証明書

  商用として実績のある電子証明書と同等のものを提供しています

- 証明書取得までのタイムラグを軽減

  電子証明書の発行申請は，1枚あたり最短10分以内で処理されます

UPKI電子証明書発行サービス
証明書発行の流れとメリット



- 本サービスでは，機関ごとに，年間定額料金で，枚数に制限なく，証明書を発行することができます．
- 都度の証明書の発行においては追加費用無く，機関で申請から発行まで完了することができます．利用者が個別で契約する必要がなく，機関の中で効率的に証明書を発行することが可能です．
- 各担当者を設定し，それぞれの業務を担当していただくことで，この運用を可能とすると同時に，比較的安価な料金設定を実現しています．
  - 年間定額料具体例：構成員数1-200人の場合，
    ￥30,000 (1ドメイン含む・枚数制限なし)

機関責任者：機関責任者は，所属する機関の長より委嘱を受け，本サービスの利用に関する責任を負います．

登録担当者：機関責任者から任命を受け，機関内で証明書発行・失効・更新等にかかる申請の審査とその業務を担当します．

利用管理者：NIIが定める各種規定に合意し，証明書に記載された公開鍵と対になる秘密鍵を管理します．登録担当者を介して証明書の発行を行います．

UPKI電子証明書発行サービス
提供する証明書の種類

- **サーバ証明書(OV)**
  - Webサイトを提供する機関の身元を証明できます
  - TLSで，サーバと利用者間の通信を暗号化し，盗聴を防ぐことができます
- **クライアント証明書・S/MIME証明書**
  - 文書と電子メールへの署名
    送信元を保証し，なりすましと改ざんを防止することができます
  - 電子メールの暗号化
    盗聴を防ぎ，情報漏洩などを防ぐことができます
  - 個人認証
    パスワードに変わる，安全で強固な認証

UPKI電子証明書発行サービス
参加対象機関

1.大学，短期大学，高等専門学校，大学共同利用機関

2.国立大学法人，大学共同利用機関法人および公立大学法人，ならびに，学校法人であって学校教育法（昭和二十二年法律第二十六号）第八十三条に定める大学もしくは同法第百十五条に定める高等専門学校を設置する機関

3.国公立試験研究機関，ならびに，高等教育機関の教育研究活動支援を目的とする法人

4.1.から3.に該当する大学・研究機関等が設置する機関

5.その他，本サービスの利用が必要であると研究所が認めた機関

二つ以上のドメインを申請できるのは，1.～3.の機関のみです．

UPKI電子証明書発行サービス
規定・マニュアル

各種規定，マニュアルは，以下のUPKI電子証明書発行サービスのホームページに掲載しています.

https://certs.nii.ac.jp/manual

S/MIME証明書　BR対応
S/MIME BRの制定

- 電子証明書を使った通信の安全性と利便性を向上させるためのガイドラインを策定している会員制の任意団体である 認証局/ブラウザ（CA/B）フォーラム が定める，基本要件（Baseline Requirements，以下BR）は，すべての公開認証局が遵守する必要があります．このBRは，認証局/ブラウザ（CA/B）フォーラムにて，常に改訂が検討されており，改訂された場合は，本サービスも対応しています．
- 2023年1月1日に，CAブラウザフォーラムにて可決された 「S/MIME Baseline Requirement（Ver.1.0.0）」は，2023年9月1日から，施行されました．
- 本サービスは，この決定に対応するためシステム改修を行いました．2023年８月29日から，証明書の新規・更新発行を変更しました．

■対象となる機関・証明書

全機関のS/MIME証明書（2023年8月28日以降に発行する証明書）

7: S/MIME 証明書(sha256WithRSAEncryption 有効期間:27ヶ月)
15: S/MIME 証明書(sha256WithRSAEncryption 有効期間:13ヶ月)
16: S/MIME 証明書(sha256WithRSAEncryption 有効期間:25ヶ月)

※切り替え日より前に発行済みの証明書は，切り替え日以降も有効期限までご利用可能です．発行し直す必要はありません．

S/MIME証明書　BR対応
本サービスの主な変更点

S/MIME BR（Ver.1.0.0）では，3つのポリシーと4つの証明書プロファイルが規定され，その内，セコムトラストシステムでは，社内方針として，ポリシーはStrict，証明書プロファイルはメールボックス認証を採用しました．本サービスの変更点は次の通りです．

主体者DN

- UPKI S/MIME証明書の主体者DNは，CN（CommonName）以外含まれません．
- CNはメールアドレスのみ設定可能となります．

  ［発行・失効方法］
  - 新規・更新発行，失効時は，これまで通り，主体者DNにCN以外の値（OU,O,L,ST,C）も含めて申請してください．
  - CNは，メールアドレスのみを入力してください．CNに入力するメールアドレスは，利用者メールアドレスと一致させてください．
  - 申請後，証明書自動発行支援システム上では主体者DNの情報を保持しますが，証明書にはCNのみを記載して発行されます．

拡張鍵の使用法（EKU）

- UPKI S/MIME証明書で個人認証用証明書として利用できません．

  ［証明書の利用方法］
  - クライアント認証の用途で証明書を発行する場合，個人認証用証明書を発行し，ご利用ください．

個人認証用証明書を発行するCAの切り替えとプライベート化

セコムトラストシステムズから，次の理由のため，個人認証用証明書を発行するCAを現状のパブリックからプライベートに切り替えについて提案がありました.

個人認証用証明書を発行する中間CA証明書の有効期限

- 個人認証用証明書を発行する共有CA「SECOM Passport for Member PUB CA8」が，中間CA証明書の有効期限が2028年1月9日までとなる.
- UPKIの個人認証用証明書は3種のプロファイルの内，最長の有効期限であるプロファイルID5の証明書の有効期限は48か月（4年）で，（ 2028年1月9日の4年前の）2023年12月初めにCAの切り替えが必要となる.

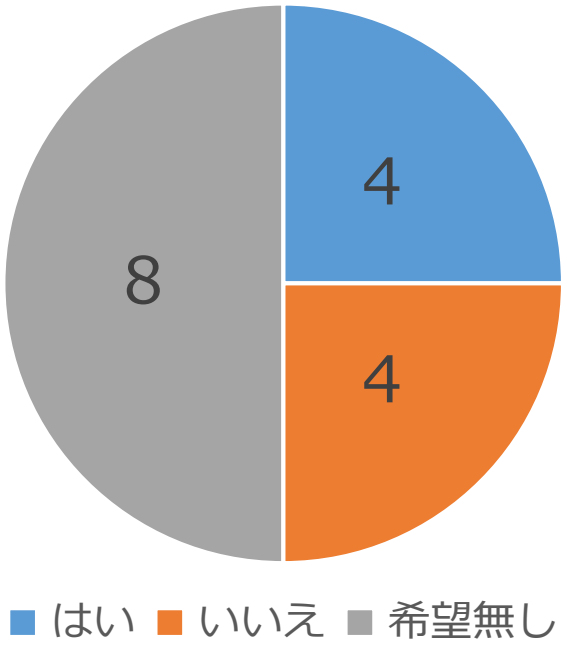
GoogleのChrome Root Program Policyの改訂

- GoogleのChrome Root Program Policyの改訂により，2022年9月以降，Chrome（Chromeブラウザ）に搭載されるRoot CA証明書が，TLSサーバー証明書用途のみ
- ChromeのRoot Storeには今後，個人認証用証明書を発行する新Root CAが搭載されることはない.
- 今後，Microsoftのみに搭載可能な個人認証用証明書はパブリックとして発行可能だが，従来に比べて搭載OSが減少することや，個人認証用証明書そのものがパブリックである必要性が低いことから，パブリックで新CAを構築して発行を行わない方針

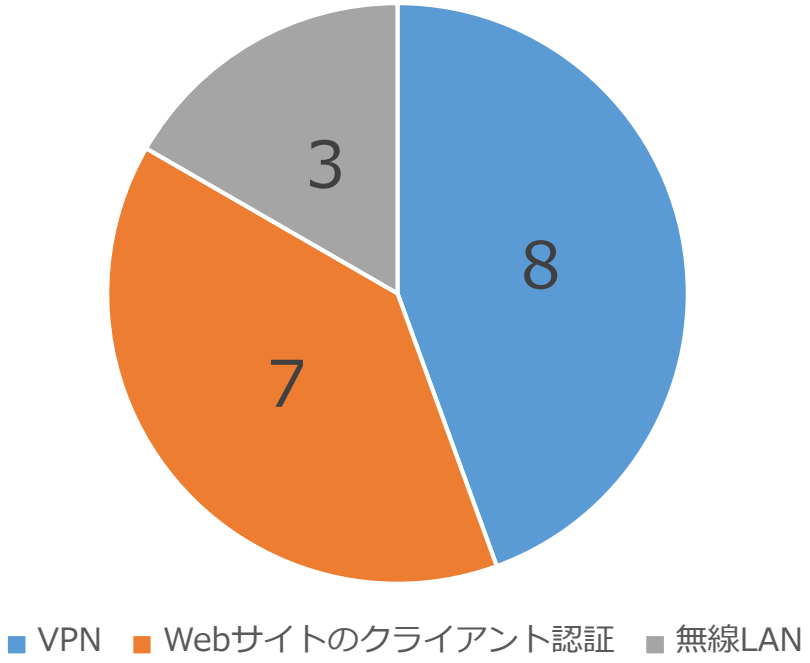
個人認証用証明書を発行するCAの切り替えとプライベート化利用機関の意見まとめ

有効な個人認証用証明書発行数上位20機関（全体の個人認証用証明書の発行数の90%以上）を対象にアンケートを実施しました.
ご協力ありがとうございました.

Q1.現状のままパブリックの中間CAから発行される証明書を希望しますか



Q2.個人認証用証明書の主な用途（複数回答可）



個人認証用証明書を発行するCAの切り替えとプライベート化 今後の方針

2023年12月初めごろに，個人認証用証明書を発行するのCAは，現状のパブリックからプライベートへ切り替えを行います．アンケートの際にもいただきました，変更による懸念点（利用者の負担，セキュリティ面）について，次の対策を行います．

- ルート証明書は，証明書と共に配布し，手続きが煩雑にならないように対応します．
- 利用者にルート証明書のインストール時に，警告メッセージが表示される際に，フィンガープリントを事前に確認するように通知やマニュアルを整備します．
- プライベートCAとなっても，これまでパブリックで運用していたCP/CPSに準拠しセコムトラストシステムズが運用します．

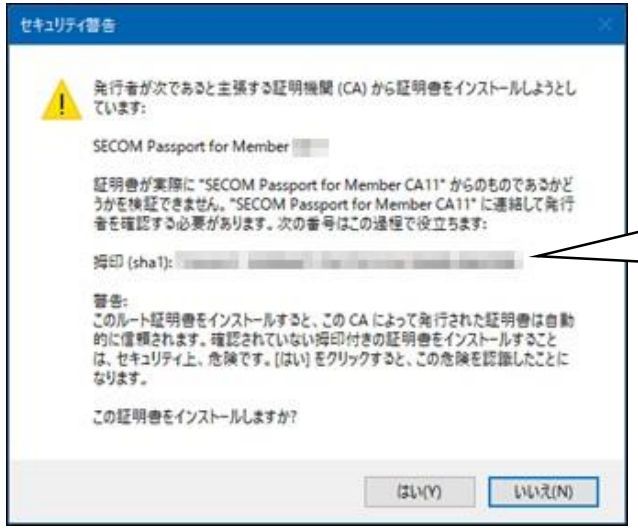
※CA切り替えを行っても，切り替え前に発効した証明書は，CA切り替え後も有効期限まで，ご利用可能です．証明書を発行し直す必要はありません．

個人認証用証明書を発行するCAの切り替えとプライベート化 変更点について

変更点１　ルート証明書

［現証明書］
　端末やブラウザにあらかじめルート証明書がインストール済み

［新証明書］
端末やブラウザにあらかじめルート証明書がインストールされていないため，インストールする
ルート証明書は，提供するP.12形式にルートを含めて配布します．



ルート証明書取得時にセキュリティ警告メッセージが表示されます．
フィンガープリントを確認の上，インストールしてください．

個人認証用証明書を発行するCAの切り替えとプライベート化 変更点について

変更点２　証明書の階層

［現証明書（3階層）］
Security Communication RootCA2（ルートCA）
↓
SECOM Passport for Member PUB CA8（中間CA）
↓
EE証明書

［新証明書（2階層）］
SECOM Passport for Member RSA CA16（ルートCA）
↓
EE証明書

独自のシステムの認証で個人認証用証明書を利用している場合は，サーバ側の中間CA証明書について，新ルート証明書のインストールを行ってください.

その他のお知らせ

請求書について

2023年度のサービス利用料については，７月までに利用機関更新申請をいただいた機関宛てに，８月に発送いたしました.
請求書記載の宛名は，申請システムで変更することが可能です．変更が必要な場合は，UPKI申請システムをご利用ください.
　UPKI申請システム＞取引先マスタ変更申請＞「取引先名」を変更

次期認証局の調達について

証明書発行事業者との契約について，現在の調達が2024年3月で終了となり，次期契約は2024年4月1日～となります.

これまでいただいた要望を次期契約で反映できるように，検討しています.
本サービスに関して，ご要望ございましたら，ご連絡ください.

ご連絡・お問い合わせ先

国立情報学研究所
学術基盤課 認証基盤・クラウド推進チーム（認証担当）

お問い合わせフォーム： https://certs.nii.ac.jp/contact/form

お問合せは，お問い合わせフォーム（Jira Service Management）で管理しております．お問い合わせフォームの利用についてご協力いただけますと幸いです．メールアドレス宛にいただいたお問合せは， Jira Service Managementに転送させていただく場合がありますので，ご了承ください.

原則，サービス利用機関または利用予定機関の機関責任者・登録担当者・経理担当者からお願いします.