UPKI電子証明書発行サービスについて

2022年12月６日　NIIサービス説明会

© 2022 National Institute of Informatics

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

- ecdsa-with-SHA384 対応

  UPKI電子証明書発行サービスの証明書は，Windowsプラットフォームでのみ検証可能ですが，楕円曲線DSAが使用可能です

- 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
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

- **コード署名用証明書**
  - プログラムやアプリケーション，スクリプトへの署名
    作成元を保証することができます

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

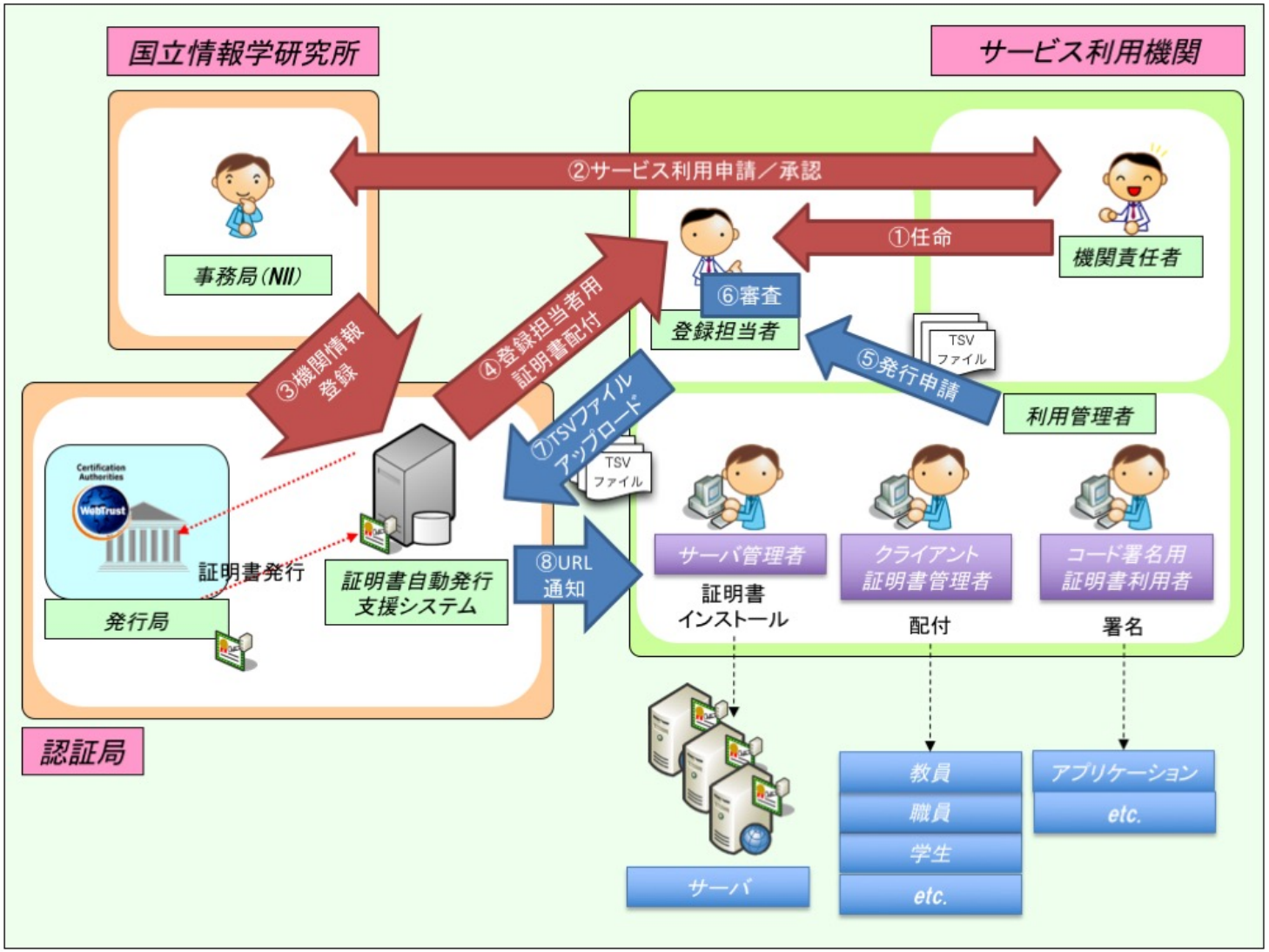
二つ以上のドメインを申請できるのは，1.～3.の機関のみです.

UPKI電子証明書発行サービス 利用料金

構成員数	基本料 （1ドメイン分含む）
1-200	¥30,000
201-400	¥40,000
401-600	¥50,000
601-800	¥60,000
801-1000	¥70,000
1001-1200	¥80,000
1201-1400	¥90,000
1401-1600	¥100,000
1601-1800	¥110,000
1801 以上	¥120,000

- UPKI電子証明書発行サービス利用料として設定（年間定額）
- 組織の規模ごとに段階的に設定
- 年額には，OV証明書，クライアント証明書，コード署名用証明書を含む
- 発行枚数に制限なし
- 追加ドメイン¥20,000
  ドメイン追加時には，1ドメインごとに追加ドメインの額をプラス

UPKI電子証明書発行サービス
証明書発行までの流れ



UPKI電子証明書発行サービス 担当者について

- 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 利用申請方法

利用申請の流れは以下のとおりです.

1. 登録担当者を任命する
2. UPKI申請システムにサインアップする
3. UPKI申請システムで以下を作成する
   a)サービス利用申請
   b)ドメイン申請
   c)確認実施手順調査票
   d)体制図（ExcelテンプレートをDLして作成後アップロード）
4. 事務局での申請内容確認後，申請システムよりa,b,cのPDFをダウンロード
5. a,b,c,のPDFとdのExcelファイルを印刷・記名押印の後，事務局に郵送
6. 事務局にて機関の参加審査を実施
7. 参加承認の受領

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

コード署名用証明書 BR対応
鍵ペアの作成と管理

2022年4月6日にCAブラウザフォーラムにて「Ballot CSC-13 - Update to Subscriber Private Key Protection Requirements（投票 CSC-13 - 加入者秘密鍵保護要求事項の更新）」が成立しました.

これにより，コード署名用証明書においては，秘密鍵を保存するセキュリティデバイスの管理が厳密になります.

◆対象機関

コード署名用証明書を利用中の機関

※2022年6月2日開催の学術情報基盤オープンフォーラム2022での説明と内容は変わりません.

コード署名用証明書 BR対応 変更点

- **変更点**
  コード署名用証明書を新規または更新発行する場合，鍵ペアの作成と管理方法が以下のとおり変更となります．

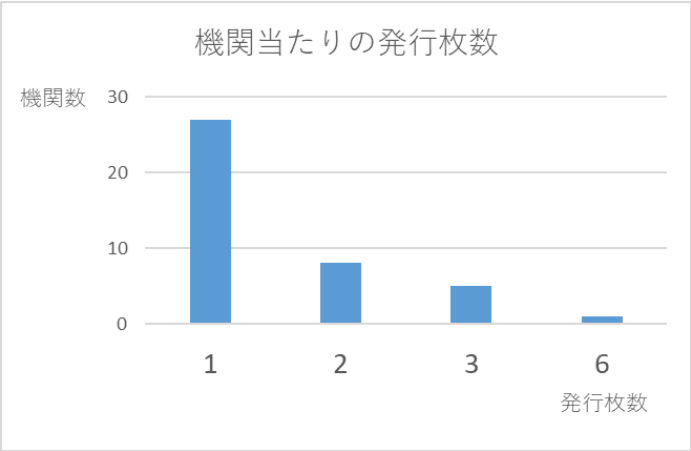
変更前	変更後
秘密鍵を保存するセキュリティデバイスとして制限はなし 秘密鍵はUSBデバイスで管理し，使用時のみPCに接続	秘密鍵を保存するセキュリティデバイスとして適切なハードウェア暗号モジュールの利用が必須．

- **変更期日について**
  上記の対応は，2022年11月15日より適用となる予定でしたが，2023年6月1日からの適用に変更されることが，CAブラウザフォーラムの投票により，9月26日に可決されました．
  2022年11月15日　⇒　2023年6月1日

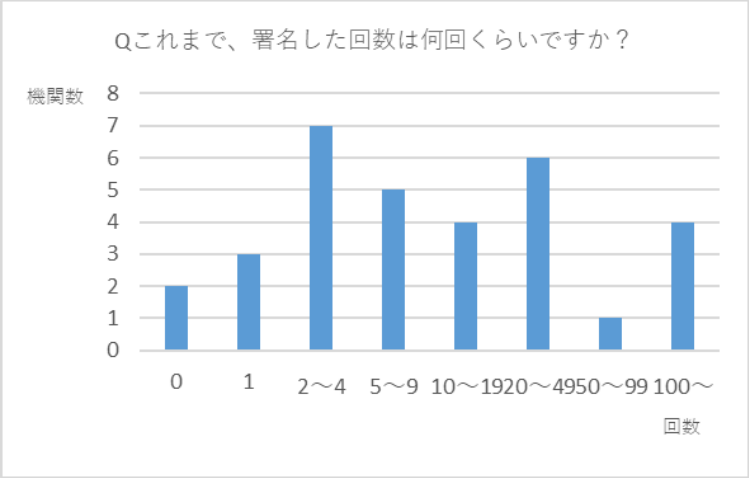
※2022年6月2日開催の学術情報基盤オープンフォーラム2022での説明から変更期日のみ変更されました．

UPKIコード署名用証証明書利用状況

利用機関：４１機関（全３７５機関中１１％）　有効枚数：６４枚　（2022年10月末日）



2022年8月10日に，コード署名用証明書の利用状況調査のため，アンケートを実施しました．
ご協力いただきありがとうございました．



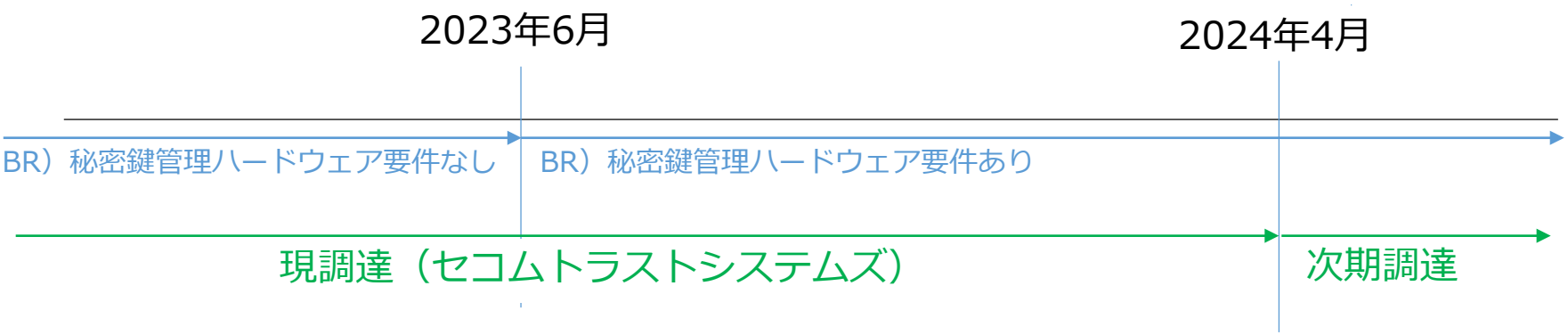
コード署名用証明書 BR対応
今後の運用

今後の運用方法については，現在検討中ですが，現状の発行方法は，2023年5月からは行えなくなります.

ただし，それまでに発行した証明書は，2024年3月までは確実にご利用可能です.

このため，2024年3月まで期限を迎える証明書については，早めに更新してください.

詳細が決まり次第，弊所ホームページでご案内いたします.



ご要望の対応状況について
証明書更新自動化

2020年9月1日に変更となった，証明書有効期間短縮（396日間）の影響から，証明書更新の自動化について，ご要望を多くいただいております．

ご要望に対しては，これまで，認証局と相談し，ACME対応のサービスを提供できるように検討を進めておりましたが，OVに対応するための調整に時間がかかっております．
また，今年度につきましては，他のBR対応に時間を割いておりますため，対応目途は未定となっております．2023年度から検討を開始いたします．
本件について，お待たせしており，申し訳ありません．

進捗があり次第，弊所ホームページでご報告いたします．

ご連絡・お問い合わせ先

国立情報学研究所
学術基盤課総括・連携基盤チーム（認証 担当）

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

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.