UPKI電子証明書発行サービスについて

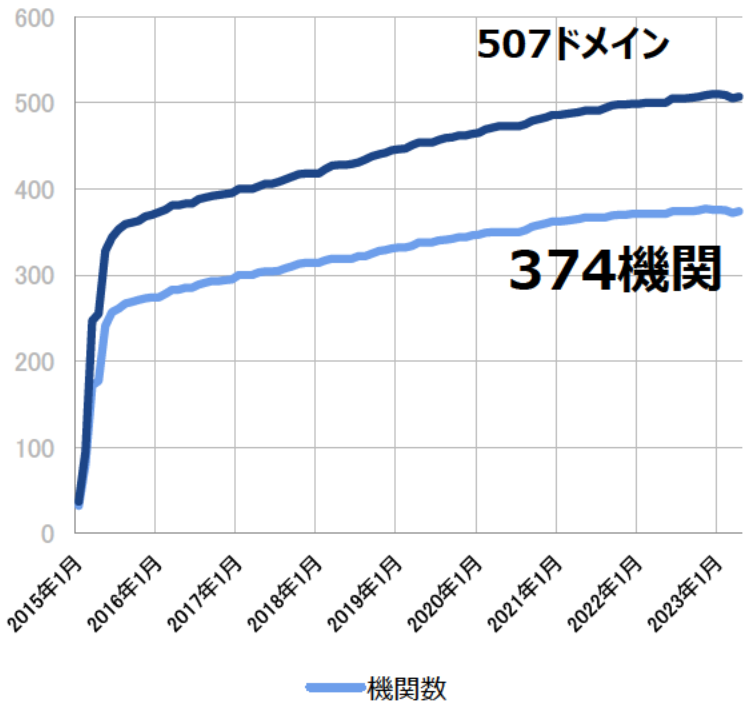
NII 学術情報基盤 オープンフォーラム 2023
2023年5月30日 認証トラック2

UPKI電子証明書利用状況（2023年4月末日現在）

374機関 507ドメイン で利用中

- サーバ証明書発行有効枚数 23,992枚（のべ発行数113,733枚）
- クライアント証明書有効枚数 32,936枚（のべ発行数61,547枚）
- コード署名用証明書有効枚数 35枚（のべ発行数219枚）

機関数とドメイン数



機関の内訳

機関	機関数
私立大学/私立短期大学	143
国立大学/国立大学法人	87
公立大学/公立大学法人	48
学校法人	47
大学共同利用機関/大学共同利用機関法人	18
独立行政法人/地方独立行政法人	16
財団法人	5
試験研究機関	4
公立高等専門学校	3
その他	3

コード署名用証明書　BR対応
コード署名用証明書提供終了について

- 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、2023年6月1日から、施行されます。
- 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。

  ◆対象の証明書　UPKIで発行したすべてのコード署名用証明書

※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
コード署名用証明書提供終了について

- 本サービスは、2023年4月24日で、コード署名用証明書の新規・更新発行の受付を終了し、失効のみ受け付けることとしました。
  （終了の理由）利用実績が少ない、費用の発生が避けられない 等
- 2023年4月23日までに発行済みの証明書は、2024年3月までは確実にご利用可能です。
- 現認証局のセコムトラストシステムズにおいても、有償となりますが、個別に契約することで、コード署名用証明書を発行することが可能です。

S/MIME証明書　BR対応
S/MIME BRの制定

- 2023年1月1日に「S/MIME Baseline Requirement（Ver.1.0.0）」が CAブラウザフォーラムにて可決されました。2023年9月1日から、施行される見込みです。

- 本サービスも、S/MIME Baseline Requirementの要件に沿って、改修を進めます。

S/MIME証明書　BR対応
S/MIME BRの主な内容

- 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ます。
  - ポリシー

Legacy	将来的には非推奨となる予定。
Multipurpose	拡張鍵使用法等があり、証明書の複数用途での利用を想定。
Strict	「extKeyUsage」を「id-kp-emailProtection」に限定。 「Subject DN属性」およびその他の拡張機能をより厳格に使用。

  - 証明書プロファイル

メールボックス認証	サブジェクトはemailAddress および/またはserialNumber 属性に限定される。
組織認証	サブジェクトに組織 (法人) 属性のみが含める。
スポンサー認証	個人 (自然人) 属性と (関連付けられた法人) 属性を結合する。
個人認証	サブジェクトに個人(自然人)属性のみが含まれる。

S/MIME証明書　BR対応
本サービスの対応

- S/MIME BR対応が始まるまでに発行した証明書は、引き続きそのままご利用いただくことが可能です。
  利用者のS/MIME証明書の入れ替え作業の必要はありません。

- 本サービスでは、2023年9月1日から、S/MIME証明書の新規・更新発行方法が変更となる予定です。

- 詳細が決まり次第ご案内いたします。

Security Communication ECC RootCA1 ブラウザ搭載状況

- 「NII Open Domain CA - G7 ECC」のRoot CAである「Security Communication ECC RootCA1」のブラウザ搭載状況について報告します。対象：証明書プロファイル11 サーバ証明書(ecdsa-with-SHA384)

  - Microsoft Windowsは搭載済み。
  - 2022年8月30日 Chrome105（Windows版）で、「chrome_root_store」にRoot CA証明書が搭載
  - 2022年10月19日 通常版のFirefox 106に搭載。
  - Appleは搭載審査中。
  - 他のOSについては、セコムトラストシステムズが、信頼済みルート認証局に加えてもらえるよう対応中。

機能改善

UPKI申請システム

- 申請システムにマスタ登録用のタブを追加

  改善点：これまで、登録済みのマスタ登録情報から変更が発生しても、申請システムで修正不可であったところ、この改修により、登録担当者が申請システムで登録情報を変更することが可能となった。

電子証明書自動発行支援システム

- サーバ証明書の入力チェック処理にdnsName設定数チェックを追加

  改善点：
  これまで：上限数を超えて設定して申請した場合、エラーが表示されず申請受理されたように見えたが、発行処理が止まっており、登録担当者でエラーに気づき難かった。

  →この改修により、申請の時点でエラーを表示するので対処できるようになった。

TSVツール

- 電子証明書自動発行支援システムに入力できる文字コードに合わせてチェック機能を追加

  改善点：
  現在の仕様：入力不可の文字は、登録担当者が電子証明書自動発行支援システムに申請する際にエラーになる。

  →この改修により、利用管理者がTSVツールにてTSVファイル作成の際に入力不可の文字の使用を確認できるので、登録担当者の手元にTSVファイルが来る前に、利用管理者にてエラー発生を防ぐことができる。

マニュアルの整備

本サービスのマニュアルは、ホームページに掲載し、更新しております。ご活用ください。

- UPKI電子証明書発行サービス マニュアル
  https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=26182293

次期認証局の調達

- 証明書発行事業者との契約状況

  現行契約　2022年4月1日～2024年3月31日
  次期契約　2024年4月1日～

現在の調達が2024年3月で終了となります。
次期調達について検討を進めております。

ご連絡・お問い合わせ先

国立情報学研究所
学術基盤課 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

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。