UPKI電子証明書発行サービスについて

2021年11月17日 NIIサービス説明会

中間認証局の切り替えについて

- UPKIの証明書をセキュアに継続して利用いただくためには、「CA/Browser Forum Baseline Requirements」 および「Mozilla Root Store Policy」への準拠が必須です
- これらの改訂に伴い、下記の対応を実施しています
  - 1. UPKI電子証明書発行サービスの証明書を発行する中間認証局を、外部監査を受けたものに切り替えました
    - 2020年12月25日より稼働開始しました
  - 2. サービス利用機関は、現在有効なサーバ証明書とクライアント証明書を監査を受けた中間認証局から再発行し、置き換えを実施いただきました
    - サーバ証明書
      2020年12月25日(金) ～ 2021年4月26日(月)まで
      ※当初のご案内（5月24日まで）より**1ヶ月程度の期間短縮**となりました
      - 経緯のご説明については、NII学術情報基盤オープンフォーラム2021の資料をご参照ください
    - クライアント証明書
      2020年12月25日(金) ～ 2021年12月末まで
      - →次スライドより詳細にご説明します

Mozilla Root Store Policy 改訂（2021年5月1日）への対応 1

- Mozilla Root Store Policy が2021年5月1日に改訂され、従来以上に認証局の管理の厳正化がなされました
  - Mozillaによって、セコムトラストシステムズ含む複数社の中間CAに対し是正の指摘がありました
  - 本サービスの旧クライアント証明書中間CAも対象に含まれました

Mozilla Root Store Policy 改訂（2021年5月1日）への対応 2

- 本件では、末端のクライアント証明書移行の前倒しは実施しません
  - ただし、Mozillaの是正指摘への対応のため、旧中間CA証明書を同鍵ペアで、また一部パラメータを変更して更新発行しました
  - 認証などの用途でクライアント証明書をご利用中の場合、この更新発行した中間CA証明書をシステムにインストールする対応をいただきました
- 移行の期間（2021年12月まで）を延長するものではありません
  - 引き続き、新中間CAから発行したクライアント証明書への移行をお願い申し上げます

タイムスケジュール

- 対象：2020年12月24日までクライアント証明書を発行していた中間CA
  - NII Open Domain CA - G4
  - NII Open Domain S/MIME CA
- 2021年7月（15日頃予定）
  - 同鍵ペアで、EKU:Extended Key Usageを付与した中間CA証明書（更新版）を発行し、リポジトリで公開（UPKI作業）
- 2021年8月27日まで
  - 利用機関の認証サーバ等で使用する中間CA証明書を更新版に切り替え、テスト等を実施する（利用機関作業）
- 2021年8月31日まで
  - 更新元中間CA証明書失効（UPKI作業）

  -----ここまで完了-----
- 2021年12月まで
  - クライアント証明書の移行を完了（利用機関・利用者作業）
- 2022年1月
  - 中間CA証明書更新版を失効（UPKI作業）

主体者DNでのOU廃止について

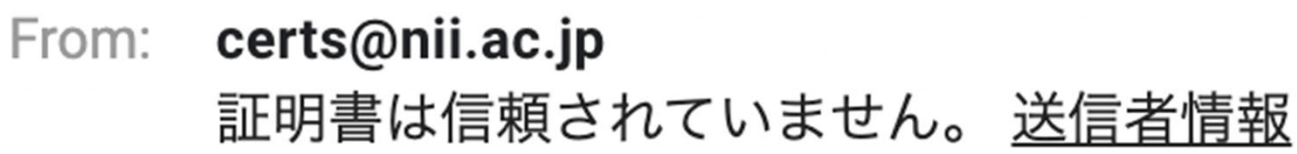
- CAB/Forumにて、証明書主体者DNの値のうち、 OUの廃止が可決されました
- BR1.7.9（2021/08/16リリース）に掲載
  - 2022年8月31日まで、OUを含む主体者DNを持つ証明書が発行可能
  - 2022年9月1日以降、OUを含む主体者DNを持つ証明書は発行できない
- UPKIの証明書でも、期限までにOUを廃する対応を行います
  - 今後の証明書申請時には、OU廃止前でも、OUが必須でない場合は主体者DNから取り除いての申請をご検討ください
- 2022年8月31日の期限までに発行されたOUを含む証明書は、証明書記載の有効期限まで問題なく利用できます

S/MIME証明書プロファイルについて

- S/MIME証明書は、現在下記3プロファイルで提供しています
  - 7:S/MIME証明書（sha256WithRSAEncryption）(証明書有効期間:**52ヶ月**)
  - 15:S/MIME証明書（sha256WithRSAEncryption）(証明書有効期間:**13ヶ月**)
  - 16:S/MIME証明書（sha256WithRSAEncryption）(証明書有効期間:**25ヶ月**)
- S/MIME証明書を取り巻く環境に変化があり、プロファイル選定時、とくに**有効期間**に注意が必要です
- 今後は特段の理由がない限り、プロファイル15と16をお勧めいたします

S/MIME証明書プロファイルについて—Gmail

- Gmail では有効期間27ヶ月を超えるS/MIME証明書の署名検証でエラーが表示されます
  - Google Workspaceでの証明書ルールによるものです
    https://support.google.com/a/answer/7300887
  - 「証明書は信頼されていません。」と表示



  - これを回避するには、プロファイル15または16を指定してください

S/MIME証明書プロファイルについて —Apple Root Certificate Program

- Apple Root Certificate Programにて、下記の条件が指定されました（抜粋）
- Effective April 1, 2022, S/MIME certificates must:
  - not have a validity period greater than 825 days

    https://www.apple.com/certificateauthority/ca_program.html
- 2022年4月1日以降、52ヶ月有効なプロファイルのS/MIME証明書によって署名されたメールは、Appleのプラットフォーム上で検証エラーが発生するものと思われます
  - Apple製品での実装・具体的な条件などについては開示されていません
  - 未然に検証エラーを回避するには、プロファイル15または16を指定してください

S/MIME証明書プロファイルについて —補足

- 加えて、現在CA/B Forumで議論されている S/MIME用 Baseline Requirements のドラフトが開示されています
  - こちらでも有効期間825日未満と定められています
  - ドラフト段階ですが、このBRが正式版となったら、各プラットフォームでも準拠するための変更が加えられるものと思われます
- 本件では詳細が未定の部分も多く、継続してUPKIより情報提供予定です
- S/MIME証明書を運用中の機関、また検討中の機関では、引き続き注視いただきたくお願い申し上げます
- なお、S/MIME機能を持たない個人認証用証明書は、現在この対象外です

お知らせ

ご要望への対応 1

- 証明書更新自動化について
  - 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
    - 認証局と話し合い、実現に向けて調整進めております
    - 2022年度後半以降となる見込みです。
- TSVツールについて
  - 機能拡充のご要望をいただいております
    - 証明書自動発行支援システムへのTSVファイル投入前に、CSR等の仕様に反した部分を判別して表示する
    - TSVファイル作成時のエラーへの対処方法の充実
    - TSVファイルのエラーチェックツールとしての動作 など
  - 登録担当者の負荷軽減になるよう、年度内を目途に改修予定です

ご要望への対応 2

- 文書への署名に関するマニュアルの充実
- 下記のマニュアルを近日提供予定です
  - Adobe Acrobat を用いたPDFへの署名付与方法
    - 署名のみ
    - 署名とタイムスタンプを付与する場合
    - 複数名の署名とタイムスタンプを付与する場合
    - 検証手順
  - Officeファイルへの署名付与方法
    - 署名
      - Windows版のみ
      - Mac版は電子署名書での署名に非対応
    - 検証手順
      - Windows/Mac双方で可

機関所在地とドメイン所有権の確認

- 利用機関の**所在地**確認と**機関責任者在籍**確認を特定記録郵便にて実施（書類の到達と返送）

- 対象ドメインの**所有権**確認を、WhoisDB記載の連絡先メールアドレスを対象に実施（メール到達と返信）
  - WhoisDBのメンテナンスをお願い申し上げます

- これらには13ヶ月の有効期間があります
  - 2021年8月より再度の確認を実施中です
  - 機関によって実施日は異なります

請求書の発送について

- 10月27日、利用期間更新申請をいただいた機関を対象に請求書を発送いたしました
  - 2021年9月1日までに利用期間更新申請をいただいた機関が対象です。これ以降に提出いただいた機関については、次回発送いたします
- 利用期間更新申請の提出状況を確認したい場合
  - 提出状況が不明な場合、UPKI申請システムにログインしてダッシュボードをご参照ください
  - 「基本情報」にある「利用期間」の終了が2022年3月31日となっている場合は、利用期間更新申請のご提出と、UPKI担当での確認処理が完了しております。

基本情報

機関名	国立情報学研究所 / National Institute of Informatics
所在地	〒 101 - 8430 東京都千代田区一ツ橋2-1-2
利用期間	2015年 05月 01日 ～ 2022年 03月 31日

おわりに

- 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