# 次期証明書発行サービスの概要


2017年6月9日 学術情報基盤オープンフォーラム

国立情報学研究所 水元 明法

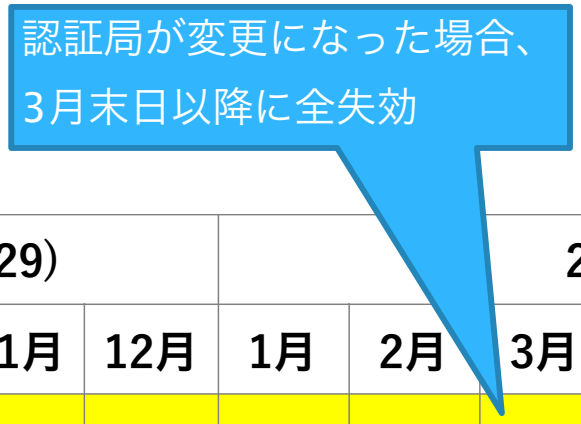
# 本資料の取り扱いについて

- 本資料は、学術情報基盤オープンフォーラムにおいて、次期証明書発行サービスに含めたい機能・サービスを議論するためのたたき台として作成するものです
- 2018年1月から提供する予定のUPKI電子証明書発行サービスにおいて、本資料記載内容の実現をお約束するものではありません

# 次期調達について

- 次期認証局調達に向けた準備をすすめています
  - 現在の認証局での証明書発行契約（セコムトラストシステムズ）は、2017年12月末日までとなっています
  - 次期認証局による証明書発行は2018年1月開始予定です
  - 次期サービスへのご意見・ご要望がありましたらサービス窓口までお寄せください
    - certs@nii.ac.jp
  - 認証局が変更になった場合、発行済みの証明書は、2018年3月末日もしくはそれ以降に失効予定です。
    - 2017年2月末日発行分より、各証明書の有効期限を2019年3月末日までとしてご案内しておりましたが
    - →個々の証明書の有効期間は、短縮しないこととしました
    - 2018年1月から証明書全失効までの期間を、新認証局発行の証明書への移行期間といたします

# スケジュール




| | | 2017(H29) | | | | 2018(H30) | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 3月 | — | 11月 | 12月 | 1月 | 2月 | 3月 | 4月 | 5月 | 6月 | 7月 |
| 現行 | 契約期間 | | | | | | | | | | | |
| | 発行申請可能 | | | | | | | | | | | |
| | 失効申請可能 | | | | | | | | | | | |
| 次期 | 契約期間 | | | | | | | | | | | |
| | 発行申請可能 | | | | | | | | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 備考 | 認証局移行期間 | | | | | | | | | | | |

# 発行可能な証明書ー変更なし

- サーバ証明書
- クライアント証明書
  - S/MIME証明書
    - クライアント証明書のうち、S/MIME署名の機能を有するものを特にS/MIME証明書と呼びます
- コード署名用証明書

# 証明書の署名アルゴリズム

- sha256WithRSAEncryption
- 廃止：sha1WithRSAEncryption
- New! サーバ証明書については、加えて下記いずれかが使用できること（楕円曲線暗号）
  - ecdsa-with-SHA256
  - ecdsa-with-SHA384
  - ecdsa-with-SHA512

# 有効期間

- 最低限の有効期間を設定
  - サーバ証明書
    - 発行日から25ヶ月
  - クライアント証明書
    - Update! 発行日から48ヶ月
  - コード署名用証明書
    - 発行日から25ヶ月

# サーバ証明書 ー対応ブラウザ Update!

- Microsoft Internet Explorer 11
- Microsoft Edge 38以上
- Firefox 52.0以上
- Opera 40以上
- Apple Safari 10.0以上
- Google Chrome 56以上
- iOS9.3.5以降に対応したSafari
- Android 4.4以降に対応したGoogle Chrome

# サーバ証明書 ー対応Webサーバ・ミドルウェア

**Update!**

- Apache 2.2
- Apache 2.4
- Microsoft Internet Information Server 7.5
- Microsoft Internet Information Server 8.0
- Microsoft Internet Information Server 8.5
- Microsoft Internet Information Server 10.0
- IBM HTTP Server 7.0
- Nginx 1.2.0 New!
- Apache Tomcat 7
- OpenLDAP 2.4 New!

# クライアント証明書 ー対応環境 Update!

- Microsoft Internet Explorer 11
- Microsoft Edge 38以上
- Firefox 52.0以上
- Opera 40以上
- Apple Safari 10.0以上
- Google Chrome 56以上
- iOS9.3.5 以上
- Android 4. 4以上

# クライアント証明書 ー用途

- SSL/TLSクライアント認証用証明書
- S/MIME証明書
  - Microsoft Office Outlook 2013以上
  - Apple Mail 10 以上
  - Mozilla Thunderbird 52.0 (Windows, macOS) 以上

# コード署名用証明書 ―対応環境

- Windows用 .exe形式
- Windows用 .cab形式
- Windows用 .dll形式
- Windows用 デバイスドライバ形式
- Windows PowerShell用スクリプト形式
- JAVA .jar形式
- Android用アプリケーション .apk形式
- Microsoft Silverlight ベースアプリケーション形式
- Adobe AIR 形式
- 廃止：OSX用

# OCSPレスポンダ

- OCSP( Online Certificate Status Protocol )による証明書ステータス確認機能の提供
  - サーバ証明書
  - コード署名用証明書 New!

# タイムスタンプサービス New!

- UPKIの証明書を用いた長期署名( RFC5126 )に利用できる、タイムスタンプサーバを提供
  - 目安となる利用回数を設定したいと思います

# サーバ証明書 ―Certificate Transparency対応

**New!**

- Certificate Transparency（RFC6962 ）
  - 2018年4月より、Google Chromeにて対応が義務化される予定
  - UPKIのサーバ証明書でも対応を必須とします

# 証明書発行支援システム

- 基本的にこれまでの機能はそのまま備える
  - 発行・失効・更新の受付
  - 一覧の取得
  - クライアント証明書による認証必須

# 証明書発行支援システム ―発行統計 New!

- 証明書発行状況の統計情報を表示できるように
- たとえばこんな項目
  - 発行状況
    - 各証明書 のべ発行数・失効数、有効数
  - 取得状況
    - ダウンロード・取得操作完了数
    - 同未了数
  - 有効期限間近な証明書の数

# 証明書発行支援システム ーメール通知 Update!

- これまで通り各種通知を登録担当者や利用管理者にメールでお届けします
- あらかじめ設定された期日に送信が決まっているメールについては、極力1通にまとめて送信します
  - たとえば
    - 証明書の有効期限の通知
    - リマインド などなど・・・

# マニュアル

- オンラインマニュアルの提供 Update!
  - これまでPDF、Wordで提供していましたが、Webページに記述する形式にします
    - システムからPDF出力も可能です
  - 各ソフトウェアに対応したマニュアルはもちろん、証明書利用者を対象とするものについては英語版も提供 New!
    - クライアント証明書のインストール
    - S/MIME証明書のメーラへのインストール

# まとめ

- 認証局
  - SHA1廃止
  - SHA2継続
  - ECDSA新設
- 対応Webサーバ・ミドルウェア追加
- 署名に用いるタイムスタンプの提供
- サーバ証明書のCT対応必須化
- クライアント証明書の有効期間を48ヶ月以上に設定
- 通知メールのダイジェスト版
- 発行統計の表示
- マニュアルのWebページ化
  - meatwikiに掲載

# 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）
    - Mail：　certs@nii.ac.jp
    - 電話：　03-4212-2261
    - Web：　https://certs.nii.ac.jp
  - 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・登録担当者からお願いします