UPKI電子証明書発行サービスのご案内

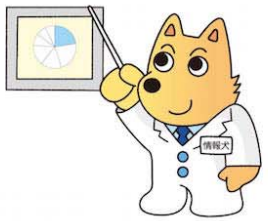
2015年2月3日

水元明法（国立情報学研究所）

新

電子証明書

はじめました。

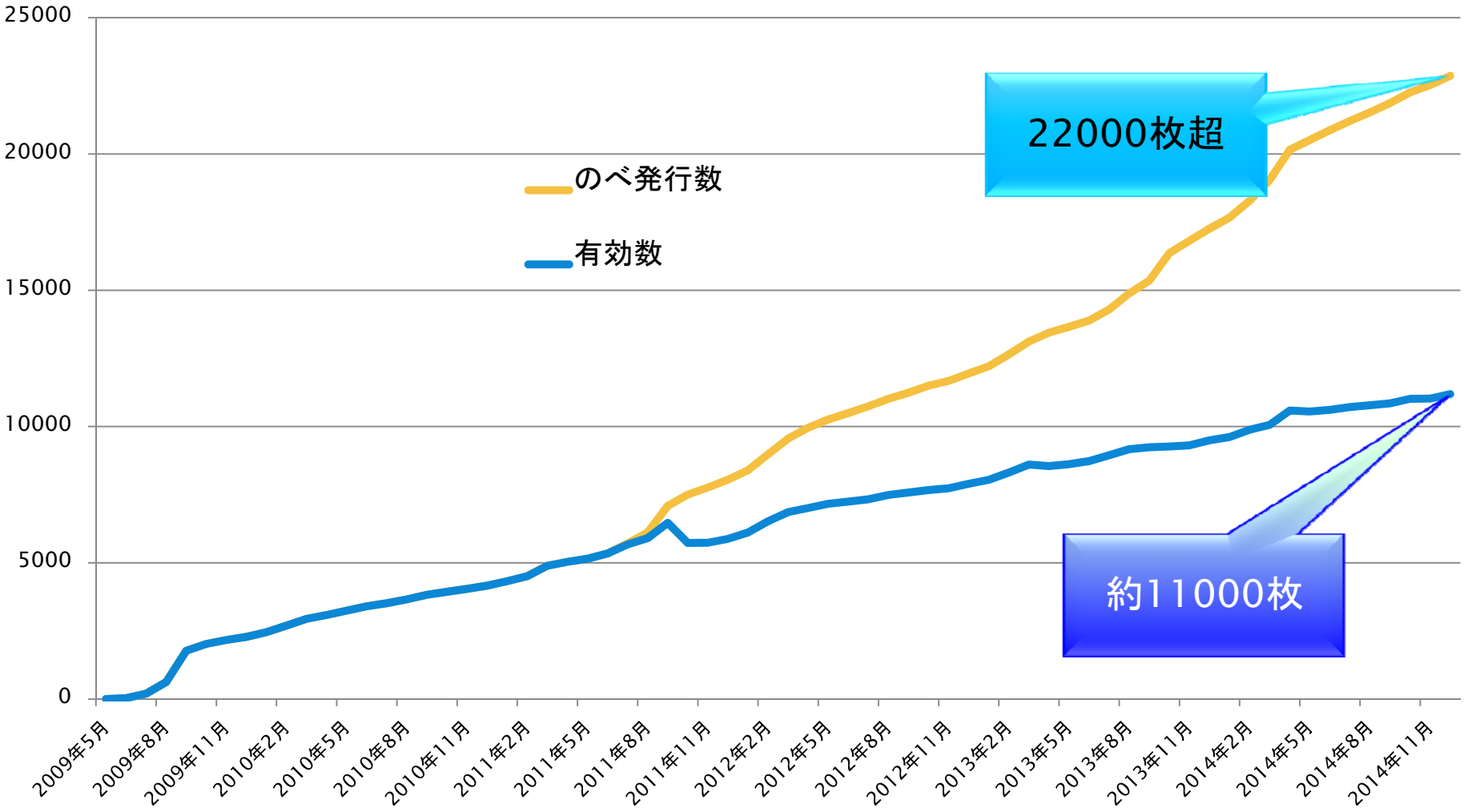


これまでのサーバ証明書発行プロジェクト

- サーバ証明書発行・導入のための啓発・評価研究プロジェクト（第一期プロジェクト）
  - 平成19年4月2日～平成21年6月30日
  - 参加機関数97機関　のべ発行枚数2,413枚
- UPKIオープンドメイン証明書自動発行検証プロジェクト（第二期プロジェクト）
  - 平成21年4月1日～平成24年3月31日
  - 参加機関数276機関　のべ発行枚数9,561枚
- UPKIオープンドメイン証明書自動発行検証プロジェクト 延長（第二期プロジェクト2）
  - 平成24年4月1日～平成27年6月30日
  - 参加機関数337機関　のべ発行枚数22,865枚（平成26年12月時点）

- ✓ 大学等のドメインに対するOV（組織認証）サーバ証明書を無償にて発行
- ✓ 証明書の有効期限:25ヶ月

のべ発行数と有効数（第二期プロジェクト）



※2009年5月から2014年12月まで

サービス拡張に対する期待（１）

- サーバ証明書

  - 従来のOV（Organization Validation）証明書だけでなく，より信頼性のレベルの高いEV（Extended Validation）発行への期待
- クライアント証明書
  - 現在各大学で個別に購入 or 独自に発行しているクライアント証明書発行への期待

学認の普及も後押し

GakuNin

- 学内統合認証基盤の普及
  - 機微な情報を含む学内の多くのサービスに接続
- ID/Password認証の限界
  - クライアント証明書等を使ったセキュアな認証方法の必要性

クラウドサービスの信頼度		信頼度Ⅰ	信頼度Ⅱ	信頼度Ⅲ	信頼度Ⅳ
対応 認証レベル（LoA）		Level1	Level2	Level3	Level4
機関が保有する情報の重要度	重要度Ⅰ	←	←	←	←
	重要度Ⅱ		←	←	←
	重要度Ⅲ			←	←
	重要度Ⅳ				←

クライアント証明書の利用

サービス拡張に対する期待（２）

- コード署名用証明書
  - 大学ICT環境の高セキュリティ化要請への対応
  - プログラム等に署名することで，利用者が警告を無視することなく利用可能
    - 大学が提供するサービス，研究成果等の公開・配布
      - 内容に誤りがないことを保証するものではないことに注意

コード署名用証明書とは

- Webサーバ等で提供されるプログラムやドキュメントに署名
  - Java，Flash，ActiveX，MS Office BVA，実行ファイル(.exe)，Androidアプリ，PDFなど
- 各機関のプログラム開発者やドキュメント管理者に対して証明書を発行
- 署名ツールを利用してプログラムに署名
  - 署名の正当性を，OS，ブラウザ，ウイルス対策ソフト等が検証してから実行
  - 署名を行ったコード署名用証明書の有効期限内であれば，付与された署名が有効
  - 別途，タイムスタンプを利用することで，コード署名用証明書の有効期限を越えた５～２０年程度有効（各タイムスタンプサーバの署名の有効期限内）

UPKI電子証明書発行サービスの概要

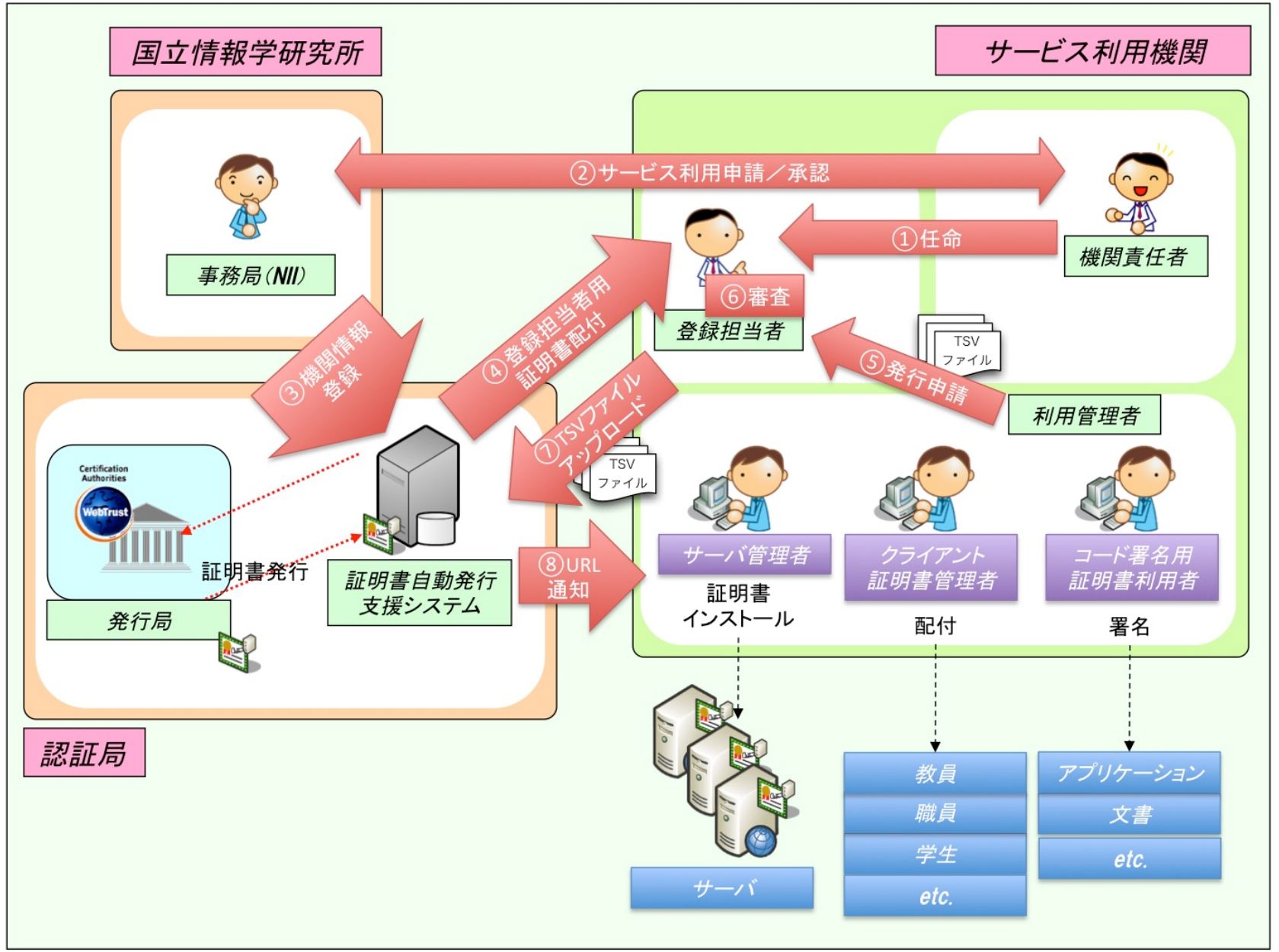
- 調査，検討の結果を踏まえNIIの事業として提供(有償)
- 提供する証明書の種類
  - サーバ証明書(OV)，クライアント証明書，コード署名用証明書
    - 追加ドメインの制約を大幅に緩和
    - クライアント証明書・コード署名用証明書は4月提供開始予定
- 費用
  - OV証明書
    - 発行枚数に制限なし
    - 組織の規模ごとに段階的に設定（定額，CiNiiの区分を踏襲）
    - 追加ドメインはドメイン単位に課金
  - クライアント証明書，コード署名用証明書は当面無料
    - 普及啓蒙フェーズ
- EV証明書
  - 1枚単位での料金
    （有効期間1年，発行業者に直接支払い，詳細調整中）

旧プロジェクトとの差異

	新サービス	旧プロジェクト
申請	機関の長から*	機関責任者から
費用	有償（定額）	無償
発行できる証明書	サーバ証明書 クライアント証明書 コード署名用証明書	サーバ証明書
ドメイン数	複数申請可能**	原則1つ
SINETへの加入	必須ではない	必須
署名アルゴリズム	SHA-1 SHA-256	SHA-1

*：大学であれば、学長にあたる方となります
**：機関が保持または管理するドメインであること

概要図


国立情報学研究所
サービス利用機関
事務局（NII）
②サービス利用申請／承認
①任命
機関責任者
⑥審査
登録担当者
③機関情報登録
④登録担当者用証明書配付
⑤発行申請
TSV ファイル
⑦TSVファイルアップロード
TSV ファイル
利用管理者
Certification Authorities
WebTrust
証明書発行
発行局
証明書自動発行支援システム
⑧URL通知
サーバ管理者
証明書インストール
クライアント証明書管理者
配付
コード署名用証明書利用者
署名
認証局
サーバ
教員
職員
学生
etc.
アプリケーション
文書
etc.

参加費

構成員数	年額（税別）
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
追加/ドメイン	¥20,000

- ✓ 構成員数：常勤の教員・研究者数（CiNiiと同基準）
- ✓ 年額には，OV証明書（1ドメイン分），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
  - ✓ クライアント証明書とコード署名用証明書は当面無償
- ✓ 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
- ✓ 数年後に改訂予定

補足：「ドメイン」に含まれる範囲

登録ドメイン

domainname.ac.jp

サブドメイン

- info.domainname.ac.jp
- secretariat.domainname.ac.jp
- sub.domainname.ac.jp
- sub.sub.domainname.ac.jp

など

構成員数に応じて設定される金額（¥30,000～¥120,000）に含まれます

追加ドメイン1

domainname.jp

サブドメイン

- library.domainname.jp
- faculty.drive.domainname.jp

など

追加ドメイン１件の金額（¥20,000）に含まれます

※ワイルドカード証明書（例：*.domainname.ac.jp）は発行できません

新サービスへの移行

- 現行サーバ証明書発行プロジェクト
  - 3月末まで発行，6月末まで有効
- 新サービスへの参加申請受付中
  - OVサーバ証明書の発行開始：2015年1月
  - クライアント，コード署名用証明書：2015年4月（予定）
- サービス利用の更新
  - 年度ごとに年度末に利用継続を確認
- 課金方法
  - 2014年度内（2015年1月～3月）：無料
  - 2015年度以降
    - 年度当初（申請受理後）に，当該年度分の請求書を発行
    - 年度途中の参加の場合は，残りの期間に応じて算定（１ヶ月単位）

SHA-2にも対応

- マイクロソフト セキュリティ アドバイザリ 2880823（2013年11月13日公開）
  - マイクロソフト ルート証明書プログラムでの SHA-1 ハッシュ アルゴリズムの廃止
    - 「マイクロソフトは，マイクロソフト ルート証明書プログラムのポリシーを変更したことをお知らせします。新しいポリシーでは，2016 年 1 月 1 日以降，ルート証明機関は SSL とコード サイニングの目的で，SHA-1 ハッシュ アルゴリズムを使って X.509 証明書を発行できなくなります。」
    - 「マイクロソフトは，証明機関が SHA-1 ハッシュ アルゴリズムを使って新しく生成された証明書に署名せずに，SHA-2 に移行することを推奨します。また，お客様ができるだけ早い機会に SHA-1 証明書を SHA-2 証明書に置き換えることを推奨します。」

    引用もと:https://technet.microsoft.com/ja-jp/library/security/2880823

- 当初はSHA-1/2双方の証明書が発行可能（3プロファイルを準備）
  - sha1・有効期間 2016 年 12 月まで
  - sha1・有効期間 2015 年 12 月まで
  - sha256・有効期間25ヶ月
- 時期を定めてSHA-2への移行を進める予定

クライアント証明書の活用

- 用途
  - 認証
  - 署名
  - 暗号化
    - 電子メールで使用する場合は，証明書にメールアドレスを記載
- 配付形態
  - ユーザごとに1枚（複数端末で共用）
    - 端末紛失等で，当該ユーザの証明書の再発行・全端末に再インストールが必要
  - 端末ごとに1枚
    - 同一メールアドレスだと，電子メールの暗号化利用に難あり
- 利用形態
  - 端末にストア
  - ICカード（Type B等），USBトークン，SIMカード等にストア
    - 耐タンパ性
  - FCF（FeliCa）等と連携

クライアント証明書発行概略

- 発行単位
  - ユーザごと（大学担当者を経由して申請し，利用者が受領）
  - 一括（大学担当者がまとめて申請，受領，利用者に配布・ICカードへの登録等）
    - 大学のID管理システムとの連携の考慮
- 発行方法
  - PKCS#12 （秘密鍵をCAが生成）
  - Web enroll （ブラウザ内で秘密鍵を生成，対応検討中）

まとめ

- 新UPKI電子証明書発行サービス
  - 2015年スタート
  - クライアント証明書，コード署名用証明書
  - 有償サービス
  - 対応環境などはWebサイトをご参照ください

- 電子証明書の活用はこのあとに！

- 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 野田・水元）
    - Mail：　certs@nii.ac.jp
    - 電話：　03-4212-2218
    - Web：　https://certs.nii.ac.jp