UPKI電子証明書発行サービスについて

平成27年度SINET及び学認・UPKI証明書説明会

国立情報学研究所

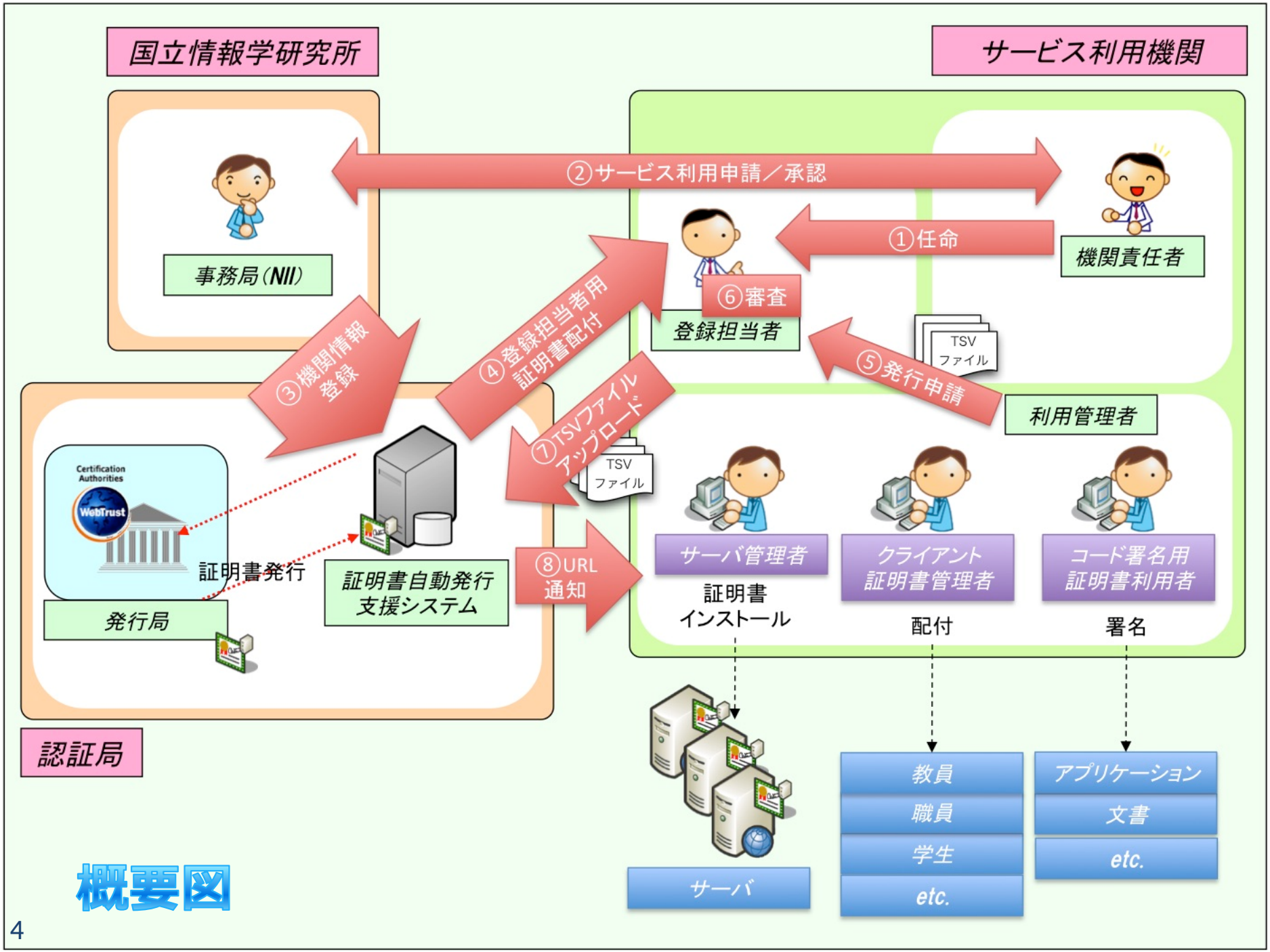
[2015-10-23版]

新

電子証明書はじめました。

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も4月より提供中
- 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）
    - 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
  - 一年分を一括で請求いたします


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
TSV
ファイル
⑤発行申請
③機関情報
登録
④登録担当者用
証明書配付
①TSV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
クライアント
証明書管理者
コード署名用
証明書利用者
証明書
インストール
配付
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.

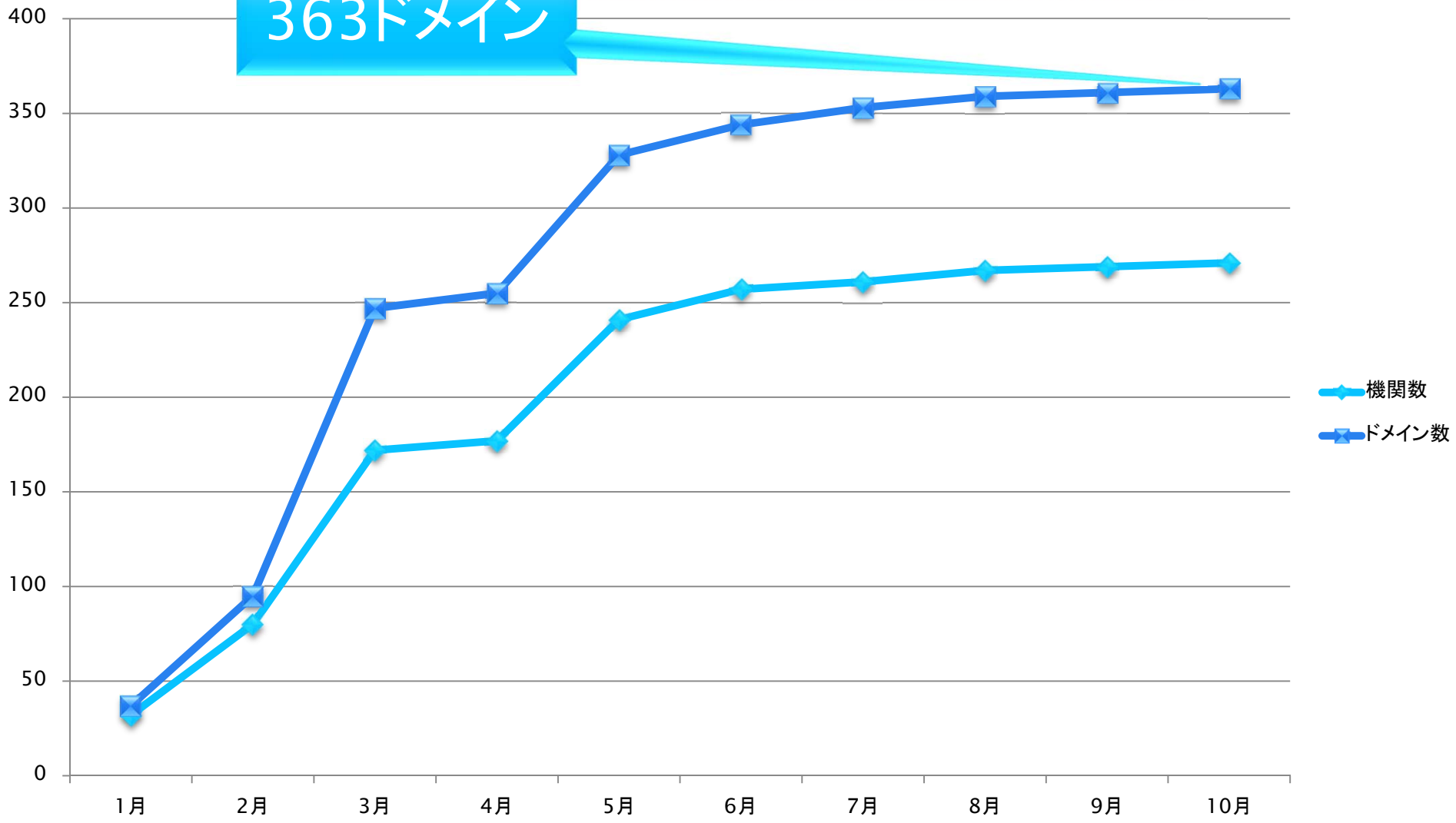
概要図

新サービスへの移行

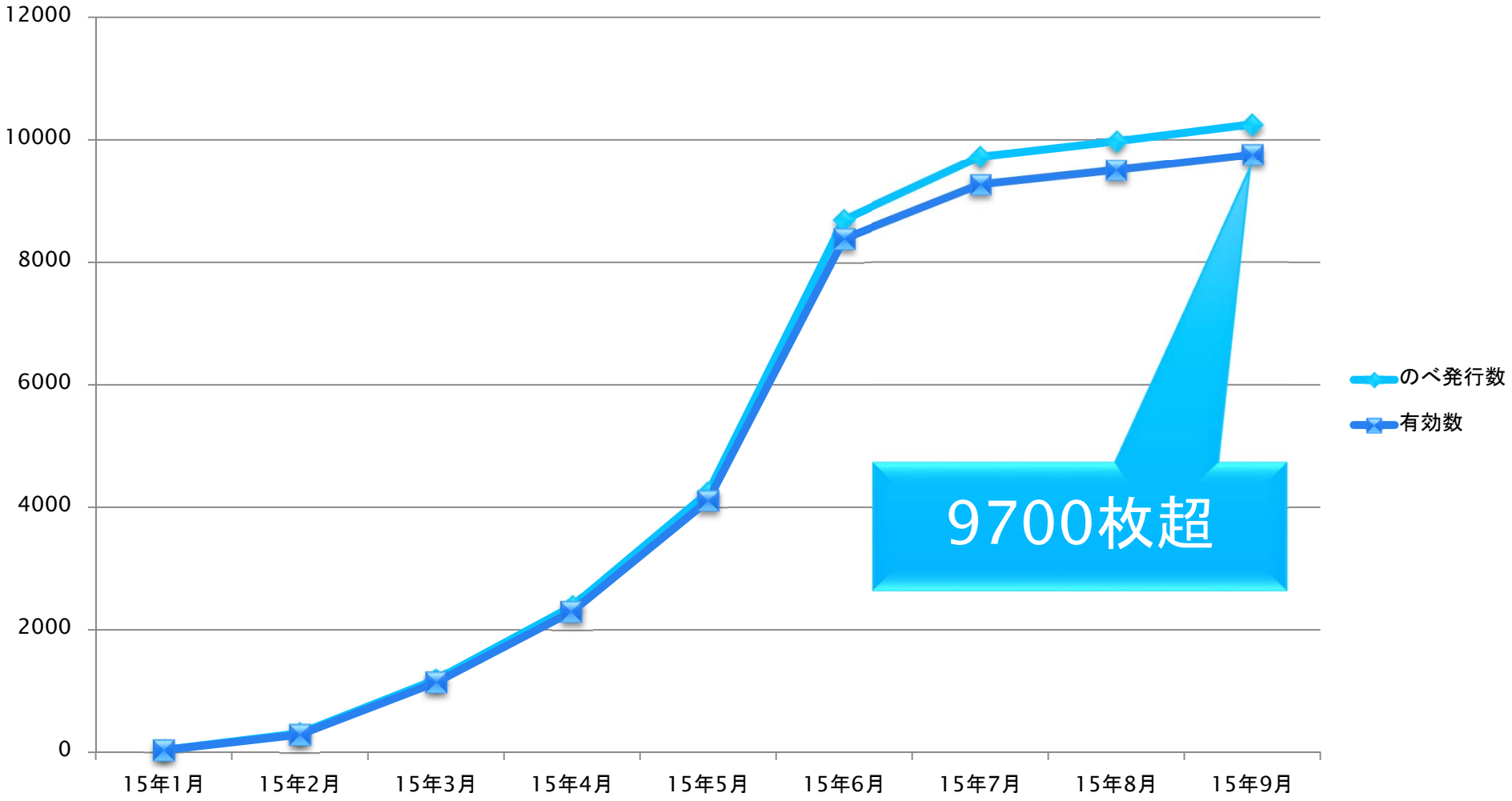
- 新サービスへの利用申請は随時受付中
- 請求書発行状況
  - 1月ー10月に利用開始した機関に，請求書を送付済み
- サービス利用の更新
  - 年度ごと更新（各年度末に利用継続を確認）

- 新サービス利用機関数 271（うち新規24機関）
- 証明書発行対象ドメイン数 363
  - およそ90%の機関が旧プロジェクトから新サービスへ移行済み

機関数・ドメイン数の推移

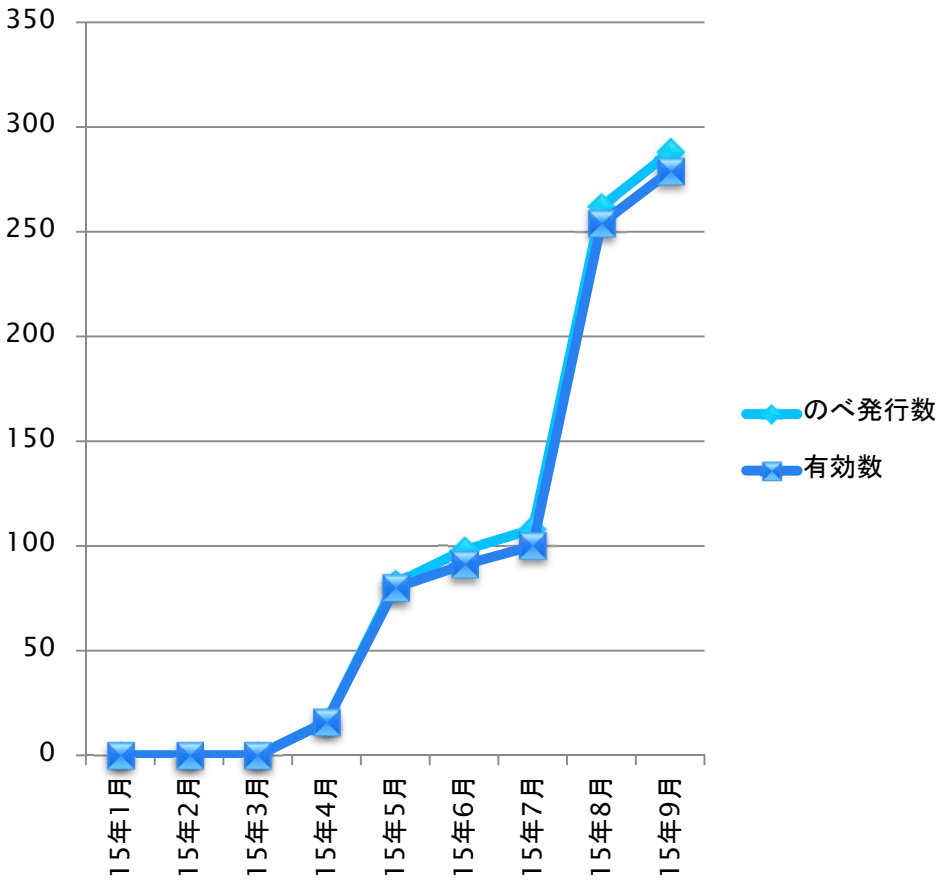


証明書発行状況ーサーバ証明書

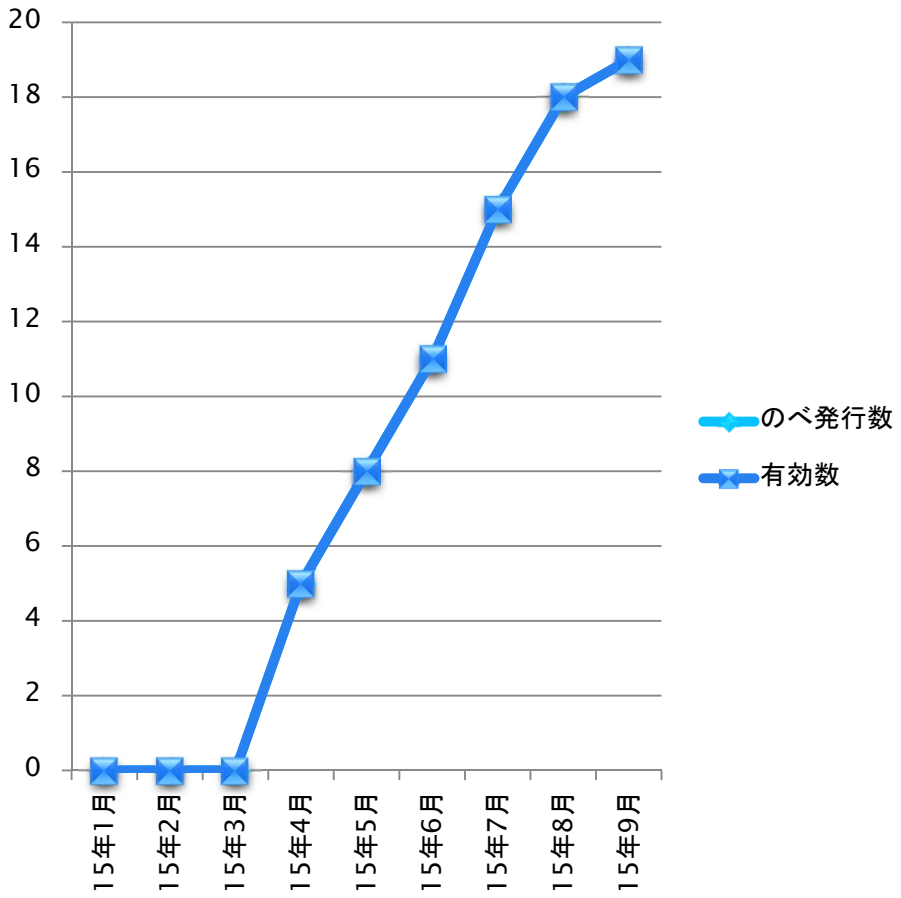


証明書発行状況ークライアント証明書
コード署名用証明書

クライアント証明書



コード署名用証明書



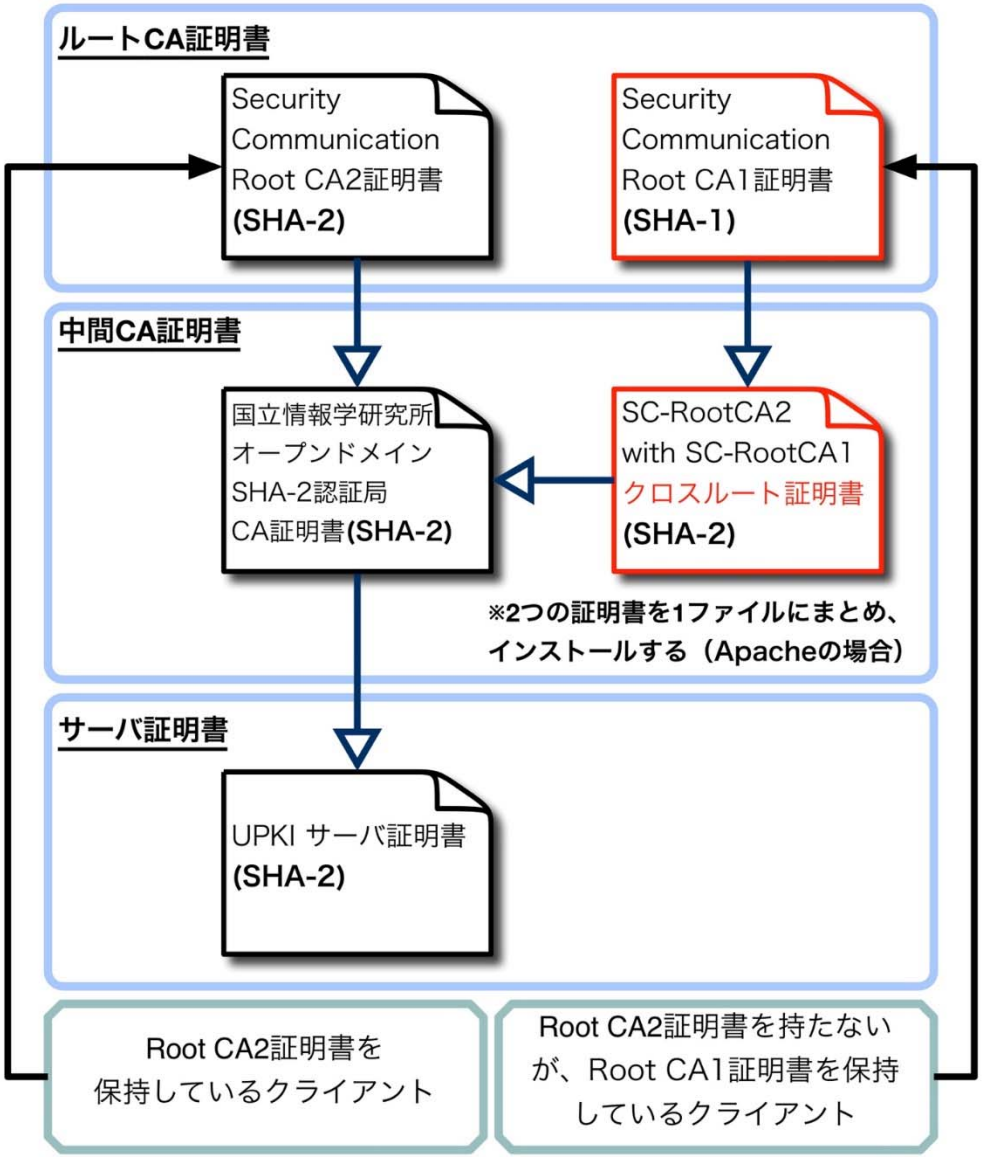
Windows10 対応状況（検証中）

- Windows10搭載のInternet Explorer 11 及び Microsoft Edge を用いて検証を進めております
  - 可能な操作
    - サーバ証明書の検証
    - 各証明書のダウンロード
    - 発行済みの証明書を用いたクライアント認証
  - 不可能な操作
    - クライアント証明書 ブラウザ発行

- 不可能な操作については、セコムトラストシステムズにおいて、システムの改修計画を検討中との連絡を受けております
- 登録担当者と、クライアント証明書利用予定の機関には、Windows10へのアップグレードをお待ちいただくことをお勧めします
  - ただしFirefoxを使う場合、現時点で問題は見つかっておりません
- Windows10の対応状況については、随時UPKIのウェブサイトでお知らせしていきます

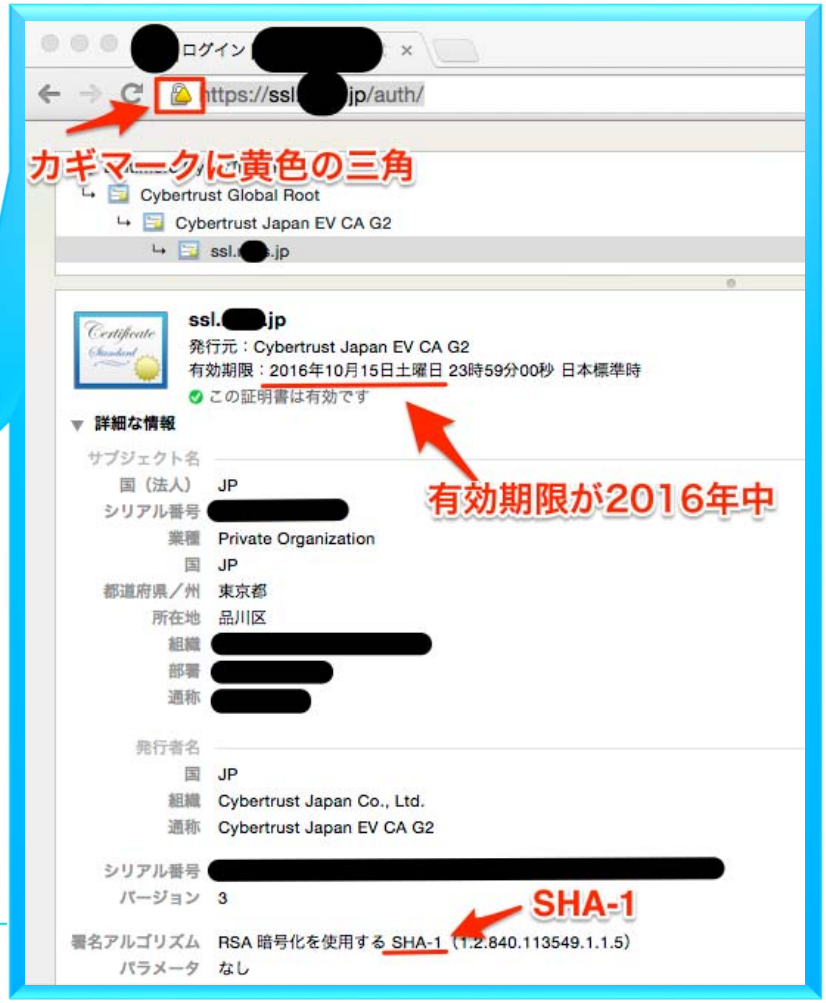
クロスルート証明書

- SHA-1 のルート証明書で署名した SHA-2 認証局証明書(SC-RootCA2 with SC-RootCA1クロスルート証明書)を提供開始しました
  - SHA-2証明書を使いたいがカバー範囲が心配，という場合に，少しでもカバー範囲を広くすることができます
  - SHA-1の認証局情報のみを保持している端末を、SHA-2証明書を使用する環境に対応させたい場合に利用できます
- 対応環境
  - スマートフォン
    - Windows phone ver7以上
    - Android ver1.5以上
    - iOS ver2.0以上
    - BlackBerry ver.5.0以上
  - フィーチャーフォン
    - 一覧を下記URLに掲載しております
      - https://certs.nii.ac.jp/cross-root/



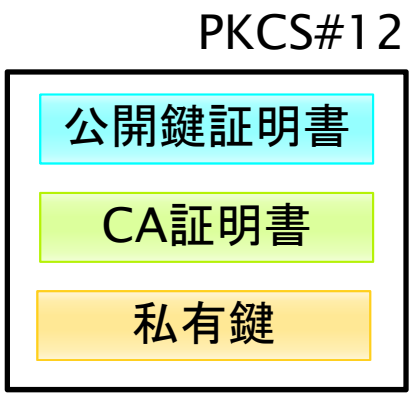
SHA-1を使用したサーバ証明書の発行期限と利用期限

- CAブラウザフォーラムにて、SHA-1を利用したサーバ証明書の発行期限および利用期限が策定されました
  - 発行期限　：2015年12月31日まで
  - 利用期限　：2016年12月31日まで
- 本サービスでは、SHA-1/2双方の証明書が発行可能（3プロファイル）
  - sha1・有効期間 2016 年 12 月まで
  - sha1・有効期間 2015 年 12 月まで
    - Chrome対応のため：
      →2015年12月末日より後に有効期限が来る証明書を使用したサイトにアクセスすると、警告を表示する
  - sha256・有効期間25ヶ月
- UPKIのSHA-1証明書の発行は、2015年末までとなります
  - クライアント証明書の利用で不都合が生じるなどの場合、情報提供をお願いします



クライアント証明書の発行

- 配布形態
  - ユーザごとに1枚（複数端末で共用）
    - 端末紛失等で、当該ユーザの全端末に証明書の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
- 発行単位
  - ユーザごと（大学担当者が申請し、利用者が受領）
  - バルク（大学担当者がまとめて申請、受領）
    - 大学のID管理システムとの連携の考慮
- 発行方法
  - PKCS#12 （私有鍵をCAが生成）：個別・一括
  - Web enroll （ブラウザ内で私有鍵を生成）：個別のみ



クライアント証明書の発行 ― まずは発行対象を決めてください

- クライアント証明書を発行する対象を明確にしてください
  - 例えば、
    「人事・学務データベースに登録されている人」とか
    「職員証が発行されている人」とか
- 利用申請で登録いただいた機関（利用機関）に所属する人のみに制限してください
  - 所属しない人を利用者としてクライアント証明書を発行することはできません
  - 利用機関は「大学」と「法人」（国立大学法人や学校法人）を区別して扱いますのでご注意ください

クライアント証明書の発行 ― 機関内フローの明確化

- クライアント証明書発行・更新・失効の機関内フロー（申請手順・審査手順）を定めてください
- すでにあるサーバ証明書のフローに準じる形にするのも一案です
  - 従来フローの「サーバ」を「利用者」と読み替えて、フローとして問題ないか確認してください
- 誰を利用管理者と認めるか、についても各機関の判断に委ねられます（後述）
  - サーバ証明書でいう利用管理者の範囲と一致しなくてもかまいません

クライアント証明書の発行 ー プロファイルの決定

- 各機関の事情・用途に合わせて証明書記載事項（DN等）を決定してください
- 例:
  C=JP
  L=Academe
  O=機関名
  OU=部局名
  CN=教職員番号/学籍番号

- S/MIMEを使用する or しない
  - S/MIMEを使用する場合、用途(eKU)の追加と別名(subjectAltName)にメールアドレスが設定されます
- SHA-2 or SHA-1

- 全ての記載事項が信頼できる情報源から取得できる／で確認できることを確認してください

クライアント証明書発行対象の拡充

- 現状、クライアント証明書は人に対して発行するものとしております

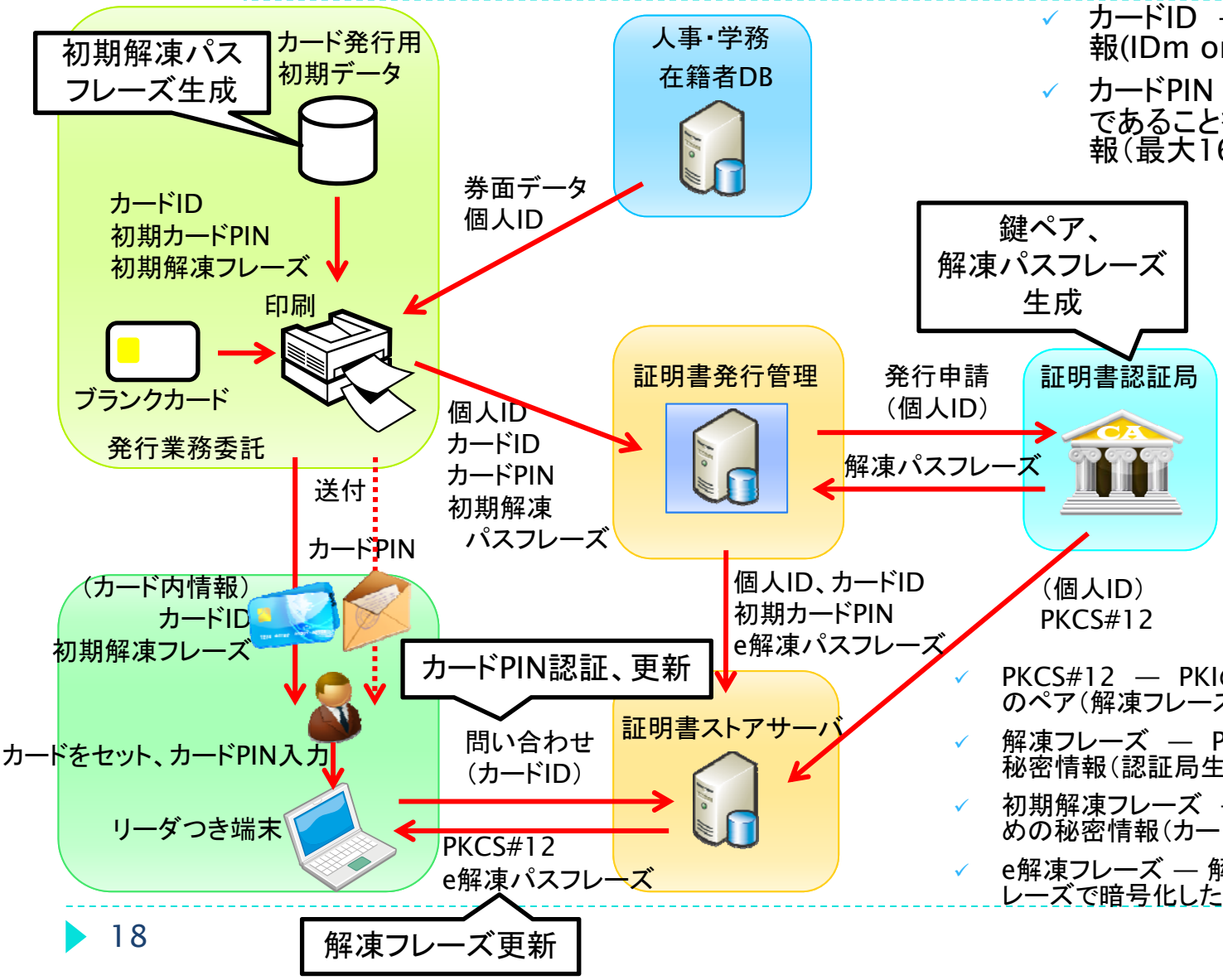
- サービス開始以降、下記のような要望をいただいております
  - 役職、組織（係、班や課などを単位とするもの）を対象として発行できないか、またこれを引き継いで使えるようにできないか
  - 業務委託の職員などにも業務上必要となるので使わせたい
- これは現在のCP（Certificate Policy：証明書ポリシ）では不可となっておりますが、クライアント証明書を利用しやすくするために、改訂を検討しております
  - サービス利用機関においては、上記のような対象に発行したい場合、このための審査基準を作成していただく必要があります
    - 発行対象は、たしかにその機関に実在するか？
    - 証明書の発行を申請した者は、たしかにその発行対象で間違いないか？

などなど

UPKIパス

- UPKIのクライアント証明書とFeliCaカードの連携
- JCANパス方式を教育/研究機関向けに改良
  - JCANパス（カード）
    - JCAN証明書のPKCS#12を利用するために、その解凍フレーズを暗号化して書き込んだFCF Version 3規格のICカード（FeliCa)
    - V2のC4領域と、V3のD1領域を利用
  - JCANパス方式
    - JCANパスを利用する時だけ、PKCS#12に格納された私有鍵＋公開鍵証明書を一時的に証明書ストアにインストールして利用可能な状態にする方式
- 公開に向けて、仕様の検証とドキュメント精査中

UPKIパス（JCANパス方式の改良）



- ✓ カードID — カード固有情報(IDm or FCF-UN)
- ✓ カードPIN — カード所有者であることを確認する知識情報（最大16文字）

- ✓ PKCS#12 — PKIの私有鍵と公開鍵（証明書）のペア（解凍フレーズにて暗号化）
- ✓ 解凍フレーズ — PKCS#12を復号するための秘密情報（認証局生成）
- ✓ 初期解凍フレーズ — PKCS#12を復号するための秘密情報（カード初期データ）
- ✓ e解凍フレーズ — 解凍フレーズを、初期解凍フレーズで暗号化したもの

コード署名用証明書

- コード署名用証明書の主体者DN表記ルールでは、CN=Oとなっています
  - 例：
    CN=National Institute of Informatics,
    OU=Cyber Science Infrastructure Development Department,
    O=National Institute of Informatics,
    L=Academe,
    C=JP
- 個々のコード署名用証明書の区別は、OUで行うことを想定しています
  - 個人ではなく、研究室、プロジェクト、部局単位での利用が多いと考えているからです
  - 署名されるソフトウェアごとに証明書を用意する必要はありません

【重要】旧プロジェクトの終了と全証明書の失効

- 旧プロジェクトは，2015年6月30日をもって終了いたしました
- 旧プロジェクトで発行したサーバ証明書は，2015年7月1日で全て失効しました
- 7月1日以降，旧プロジェクトで発行したサーバ証明書を使用しているサーバにアクセスした場合，ブラウザに警告が表示されます

各種申請について

- サービス利用申請
  - サービス利用申請書
  - マスタ登録依頼書
- ドメイン申請
  - ドメイン申請書
  - 確認実施手順調査票
- 変更申請
  - 変更申請書
- 登録担当者情報変更届
  - 登録担当者情報変更届

https://certs.nii.ac.jp/archive/regulations/formats/

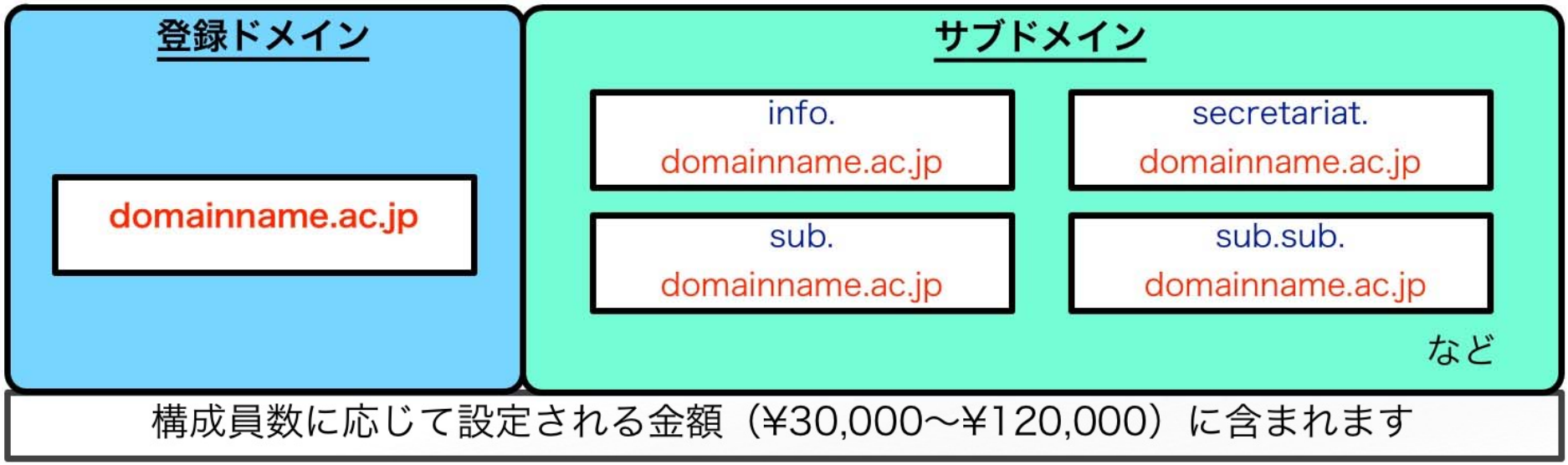
サービス利用申請

1. 「確認実施手順調査票」を作成する
2. 登録担当者を任命する
3. 「サービス利用申請書」を作成する
4. 「ドメイン申請書」を作成する
5. 1,3,4で作成したExcelファイルをメールでサービス窓口に送る
6. 内容確認完了の通知を受領後，郵送する
7. NIIにて審査を実施
8. 承認通知（利用開始日記載）を受領

ドメイン申請

- 追加
- 削除
- ドメイン申請（追加）の注意
  - 初回申請時，ドメインを1つ（以上）あわせて申請する
  - 追加するドメインの組織名(O=)は，サービス利用申請書に記入したものと同じ
    - 組織名を変えたい場合は，それぞれ別の機関としてサービス利用申請を行ってください
  - 機関名はWebサイト(https://certs.nii.ac.jp)でも確認できます

補足：「ドメイン」に含まれる範囲



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

ドメイン追加の申請

- 利用できるドメインの制限緩和
  - 旧プロジェクトにあった、機関の主たるドメインという制限がなくなりました
  - 機関が保持または管理するドメインであれば申請可
  - ドメインごとに登録担当者を設定できます
    - ドメインAとBでまったく異なる登録担当者でもOK
    - ただし、機関での統制が煩雑になる可能性もあるので、機関の内情にあわせて考慮してください

確認実施手順調査票

- 証明書発行時に，機関において実施される確認手順についてご回答ください
  - ドメインを組織が保有または管理していること
  - 登録担当者の本人性・実在性
  - 証明書発行申請受領時の利用管理者本人性・実在性確認
  - 同電子証明書の管理責任
  - ドメインの実在性
  - 機関責任者と登録担当者の担当区分を記す体制図

変更申請

- 提出済みのサービス利用申請書の記載内容を変更する際に使用
- 以下の場合にご提出ください
  - 機関情報の変更
  - 機関責任者の交代
  - 機関の区分の変更
  - 構成員数の変更
  - 経理担当者の変更
- 機関名（英語表記）変更の場合，ケースによっては発行済みの全ての証明書を失効する必要があります

登録担当者情報変更届

- ドメイン申請書の登録担当者の記載内容を変更する際に使用
  - 登録担当者の追加・削除
  - 登録担当者の登録情報の変更
  - 登録担当者が申請できる証明書の種類の変更

電子証明書申請時の頻出エラー1

- 【エラーコード】【エラーメッセージ】
  の形で、TSVファイル投入後に表示されます

- 212 指定したDNはすでに存在しています。
  - 一度でも使用した主体者DNを用いて「新規発行申請」した場合に出ます
  - 更新申請を行ってください

- 242 主体者DNのLの値が規定のものではありません。
  - 主体者DNのうち，Lの値が誤っています
  - 新サービスでは L=Academe と指定してください
    - 旧プロジェクトでは L=Academe2 としていました

- 201 ○○は入力必須項目です。
  - 入力必須項目が空欄になっています
  - CSR，またはTSVファイルの各項目を確認してください

電子証明書申請時の頻出エラー2

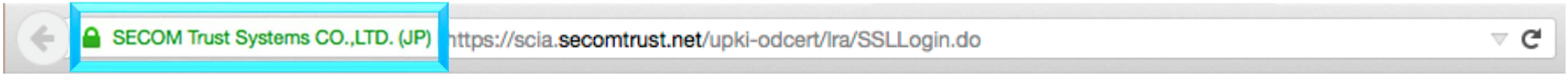
- 216 項目数が不正です。
  - TSVファイルの項目数（列数）が誤っています
  - TSVファイルを確認してください
- 241 主体者DNの機関名が申請者の所属機関名ではありません。
  - 機関名が登録されたものと一致していません
  - Webサイトで確認してください
- 233 有効な証明書データがないため，更新できません。
  - 更新もと証明書の指定が誤っています
  - 主体者DN，シリアル番号，証明書の状態フラグを確認してください
  - 発行済み証明書一覧（serverAll.tsvなど）をExcelで表示した場合，末尾4桁が0000と表示される場合がありますのでご注意ください

利用期間更新の確認

- 本サービスでも、年度末調査を実施いたします
- このとき、利用期間更新の確認（＝来年度も、4月から1年利用していただけますか？）もあわせて実施します
  - サービスは、年度ごとのご利用となります
- 期間の更新は、年度末調査に回答いただくことを必須とする予定です
- 「更新しない」と選択された場合、当該機関の全ての発行済み証明書は失効となります

EV証明書について

- 本サービス利用機関(※)に対し，証明書発行もとであるセコムトラストシステムズより，EV証明書が有償で提供されます



※サービスに登録したドメインである必要はありません

- ご希望の機関には，セコムトラストシステムズより提供された「申請ガイド」を送付いたします
  - certs@nii.ac.jp までご依頼ください！
  - 「申請ガイド」受領以降のEV証明書についてのお問い合わせ，発行手続き，お支払い等は，セコムトラストシステムズと直接行ってください

EV SSL証明書(セコムパスポートforWeb EV) の特徴

信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

◆ 機能　　アドレスバーが緑色に変化し、安全性をアピール

EV SSL証明書対応ブラウザでアクセスすると、アドレスバーが緑色に変化

OV(組織認証)証明書(セコムパスポートforWeb SR)では、https://でアクセスしてもアドレスバーの色は白色のままです。

危険なサイトはアドレスバーが赤色に変化

https://でアクセスしたとき、「失効されている」「有効期限が切れている」「WebサイトのURLと一致していない」疑わしいサイトの場合には、危険なサイトとして、アドレスバーが赤色に変化します。

◆ 効果　　識別情報の表示で運営組織を確認、 フィッシング対策に有効

従来、ブラウザの鍵マークをクリックしなければ確認できなかった「**サーバー証明書に記載されている組織名**」がアドレスバーの横に表示されます。

EV SSL証明書は、実在証明としてより一層安全性をアピールすることができます。

※アドレスバーが緑色に変化する仕組みに対応したブラウザ

・Microsoft Internet Explorer 7 以上
・Google Chrome 1.0.154.46 以上
・Opera 9.5 以上
（Windows/Mac OS X/Linux/FreeBSD/Solaris/BeOS）
・Mac Safari（Mac OS 10.5.7　以上）
・Firefox 3.5.4 以上

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：　03-4212-2218
    - 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