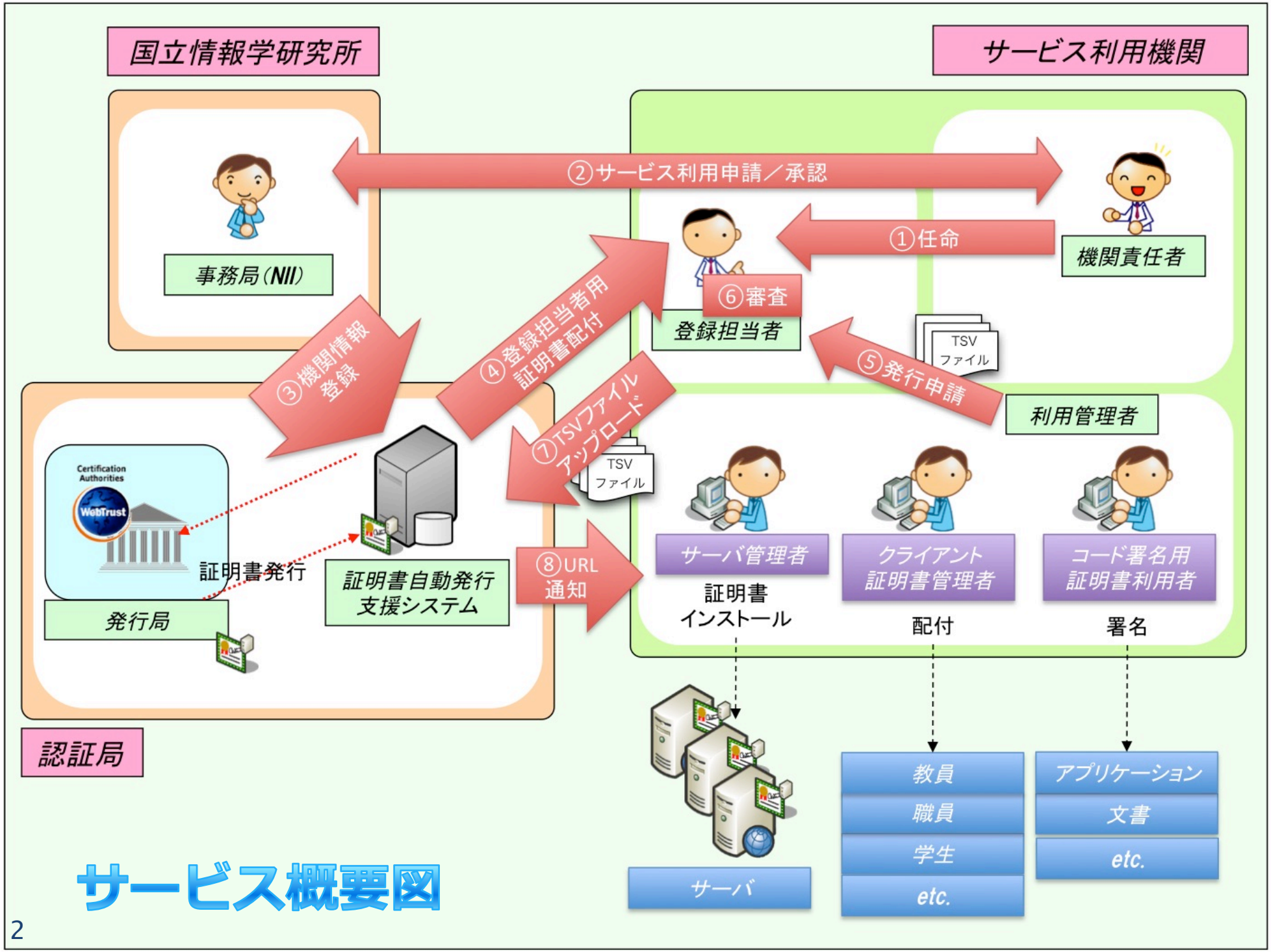
クライアント / コード署名用証明書のおさらい

2017年6月9日 学術情報基盤オープンフォーラム2017

国立情報学研究所　西村 健


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
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
証明書自動発行支援システム
⑧URL通知
発行局
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.

サービス概要図

発行できる証明書の種別

CPに書かれています。

- サーバ証明書
  - サーバ認証および通信経路でのデータ暗号化
  - 本稿ではばっさり省略
- クライアント証明書
  - クライアント認証・Webサイトのアクセス制御
  - データファイルへの電子署名
- S/MIME証明書
  - 上記用途＋電子メールへの電子署名および電子メールの暗号化
  - 以後、「クライアント証明書」に含めて扱います
- コード署名用証明書
  - プログラムファイルへの電子署名

クライアント証明書記載事項

- 例:
  C=JP
  L=Academe
  O=機関名
  OU=部局名
  CN=教職員番号/学籍番号（あくまでも例です）

- OUは複数可、省略可
- S/MIME証明書の場合はメールアドレスも記載される
  （参加申請時の対象ドメイン配下のもの）

コード署名用証明書記載事項

- 例:
  C=JP
  ST=…,L=…（後述）
  O=機関名
  OU=部局名
  CN=機関名

- OUは複数可、省略可

クライアント証明書発行対象

- 発行対象（利用者）
  - 学術機関に所属する者
  - 学術機関が認めた役職、組織（係、班や課などを単位とするもの）
  - 学術機関が認めた、業務上証明書が必要な者
- コモンネーム（CN）に記載できる内容
  - 利用者氏名
  - 利用者識別子（文字列や数字）
  - 利用者に含まれる組織名
  - 利用者に含まれる役職名
  - 組織内のさまざまな部門名

登録担当者

- 機関責任者から任命を受け、機関内ての証明書発行・失効・更新等にかかる申請の審査（※）とその業務を担当します
- 証明書の発行・更新・失効の操作は「国立情報学研究所電子証明書自動発行支援システム」を使って行います。自動処理されるので、申請から数分て証明書を取得することかてきます
- 登録担当者は、トメインことに複数名任命することかてきます

- ※審査について
  - サービス利用申請時に提出した、「確認実施手順調査票」の手順に基づいて、実在性・本人性を確認しなければなりません

利用管理者

- NII か定める各種規定に合意し、証明書に記載された公開鍵と対になる秘密鍵を管理する人、組織をいいます
- 登録担当者を介して証明書の発行申請を行います
  - サーバ証明書の場合、利用管理者はサーバ管理者であることが多いです
- 利用管理者の範囲
  - 教員、職員等の学術機関に所属する者てあり、本 CA 又は登録担当者か本人性及び実在性を確認てきる者
  - 学術機関と何らかの契約関係にある等、学術機関に所属する者か当該利用管理者の実在性、本人性を確認てきる者

利用管理者と利用者の比較

クライアント証明書についてのみ「利用者」という役割が存在します

- 利用管理者
  - 常勤の教職員もしくは委託先正社員等
  - 登録担当者に対して発行申請する人

- 利用者
  - 学生等、利用管理者になれない人も含む
  - 役職や組織を利用者とするのもアリ
  - 証明書の発行を受ける人（証明書の主体者）

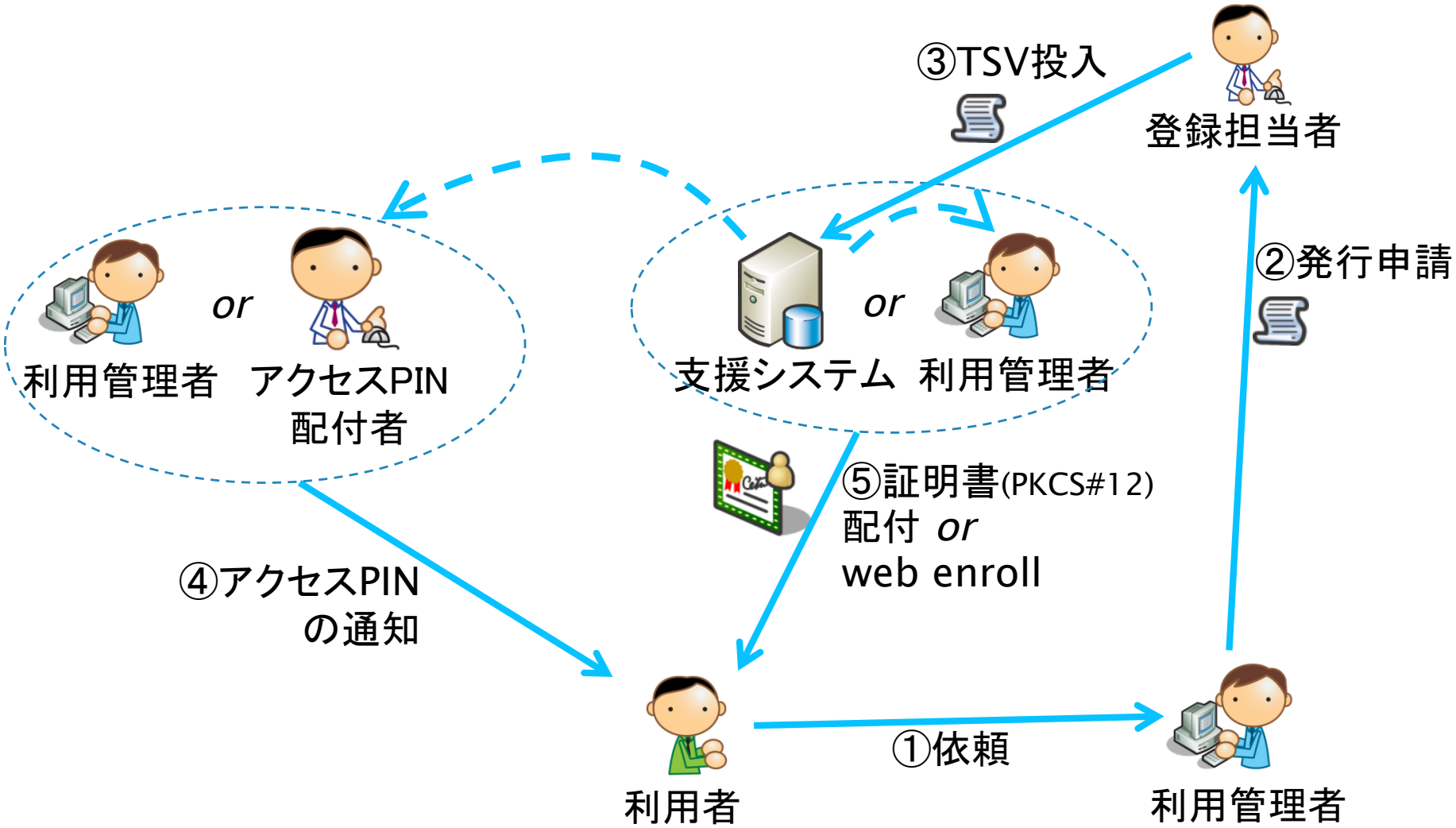
利用管理者が、利用者の代わりに（利用者の確認を行ったうえで）発行申請をするイメージ

クライアント証明書の発行形態

- クライアント証明書を機関の構成員に配付するとき、用途にあわせた発行形態をとることができます

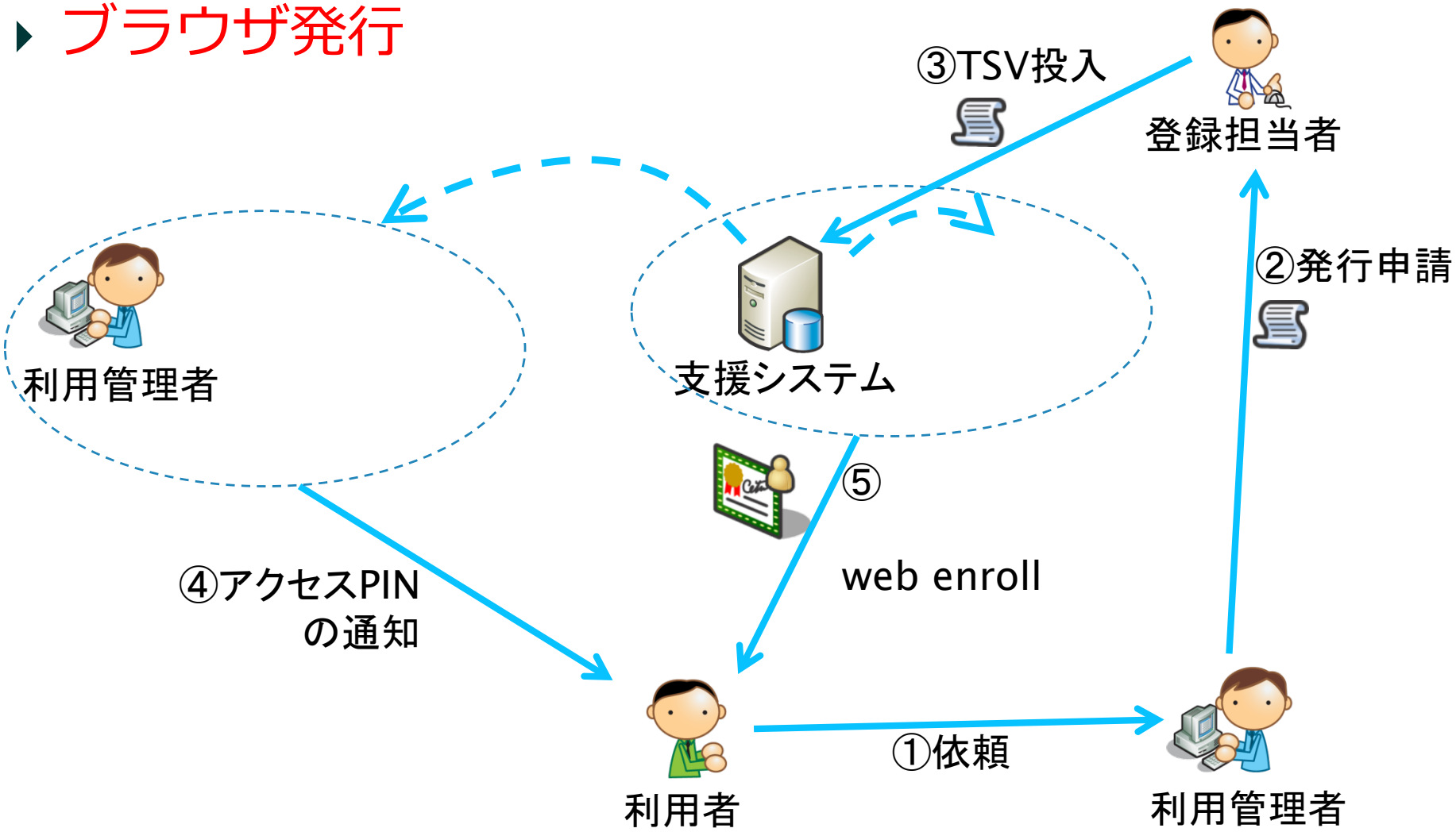
- バルクでまとめて発行
  - P12一括
    - ZIPでまとめて利用管理者が取得する方法です
    - 職員証/学生証に証明書を格納して配付する場合など
- 一枚ずつ個別に発行
  - P12個別
    - メールで個々人宛に、取得用URLが通知され、ダウンロードする方法です
    - ファイルで取得できますが、インストールのお手間があります
  - ブラウザ発行
    - ブラウザ（IE、Firefox）に、Webアプリケーションから直接インストールする方法です
    - 秘密鍵が外に出ないので安全性が高い
    - P12個別のようなインストールの手間はありませんが、バックアップ方法などを別に、利用者に案内する必要があります

クライアント証明書発行フロー概要



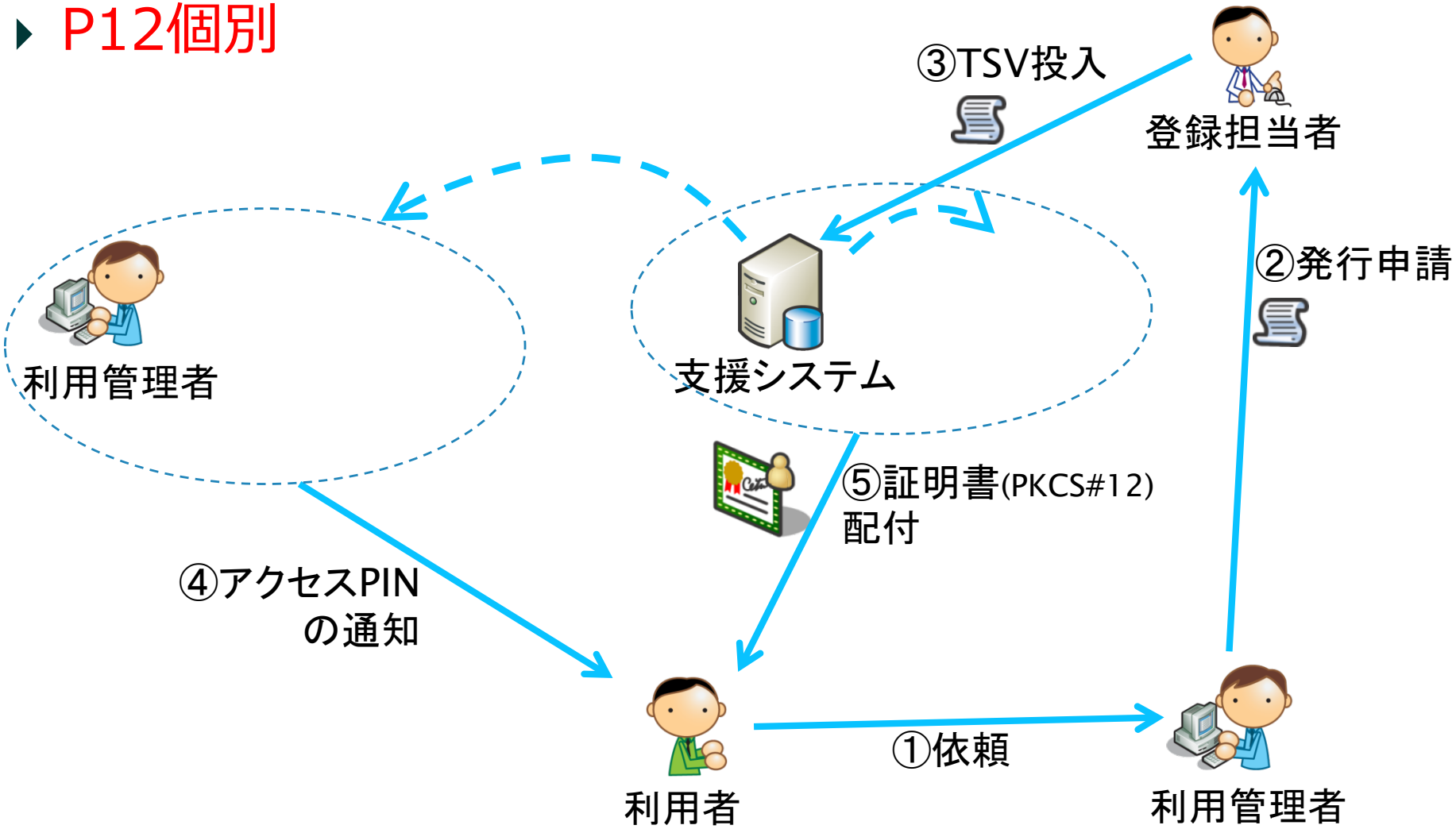
クライアント証明書発行フロー概要

- ブラウザ発行



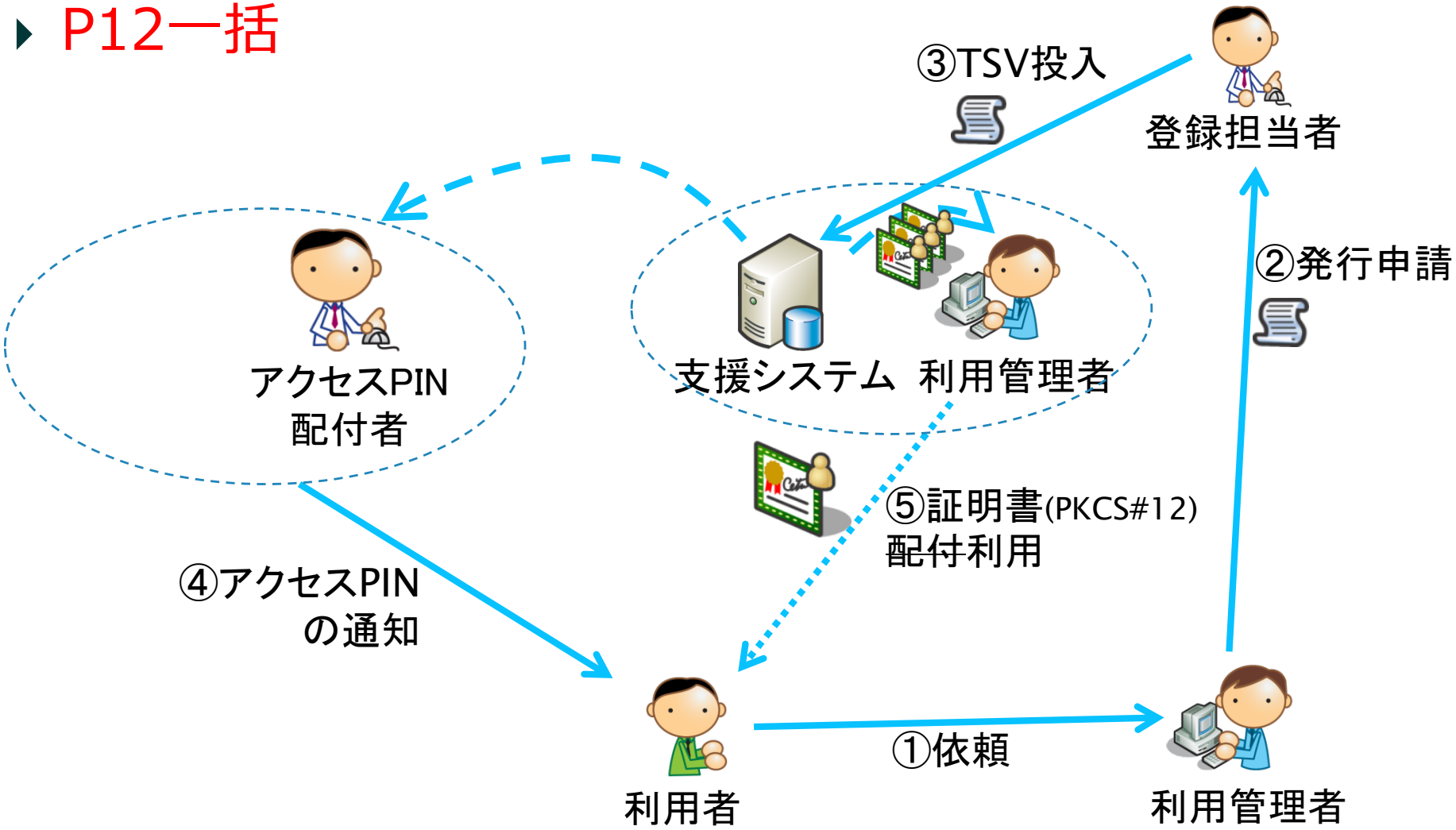
クライアント証明書発行フロー概要

- P12個別



クライアント証明書発行フロー概要

- P12一括



よりアドバンストな仕組み

- 機関独自の発行支援基盤を構築しているところもあります
  - 京都大学
  - 北陸先端科学技術大学院大学
- UPKIパス

以上については去年のオープンフォーラムの資料をご参照ください。
https://www.nii.ac.jp/csi/openforum2016/

コード署名用証明書発行フロー

- 発行形態：CSR個別 のみ（後述）
- サーバ証明書発行フローに類似
- 「利用者」は存在せず、利用管理者が当該証明書を利用する想定
- 「ブラウザ発行」のように秘密鍵は利用者側で生成し、ネットワーク上を流れることはなく、安全性が高い

これまでの変遷

- 2015年4月クライアント証明書・コード署名用証明書発行開始
  - Windows 10対応
  - SHA-1証明書終了
  - クライアント証明書発行対象拡充
- 現在発行している証明書は2018年3月？まで有効
  - 次期認証局へ

おわりに

UPKI電子証明書発行サービスが発行する証明書のおさらいをしました。

- 証明書の種別・内容
- 発行対象
- 登場人物・役割
- 発行方法