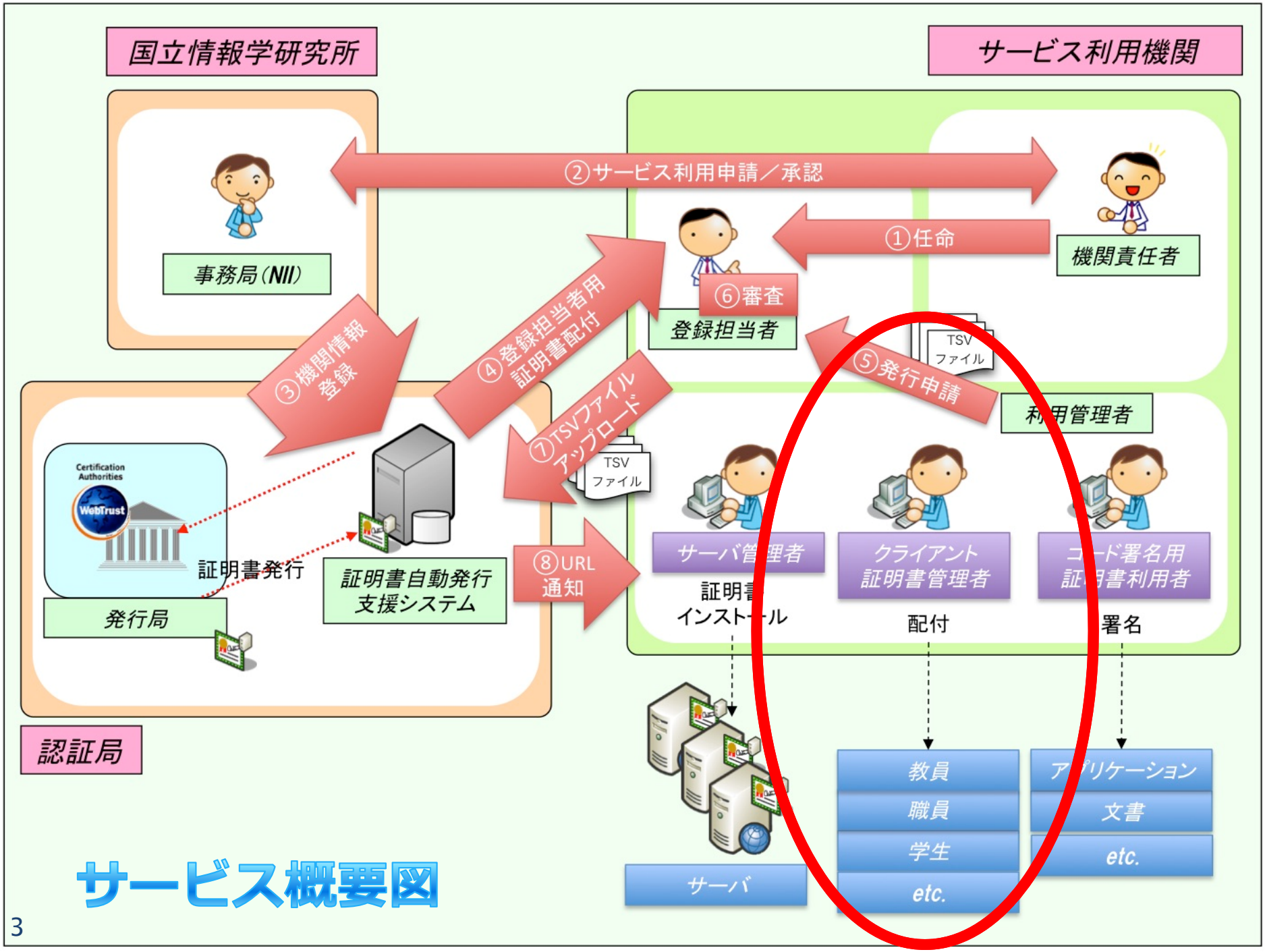
クライアント証明書発行までの道のり

UPKI

2015年6月12日

西村　健（国立情報学研究所）

クライアント証明書発行手順、そこに至るまでの手順をご紹介します

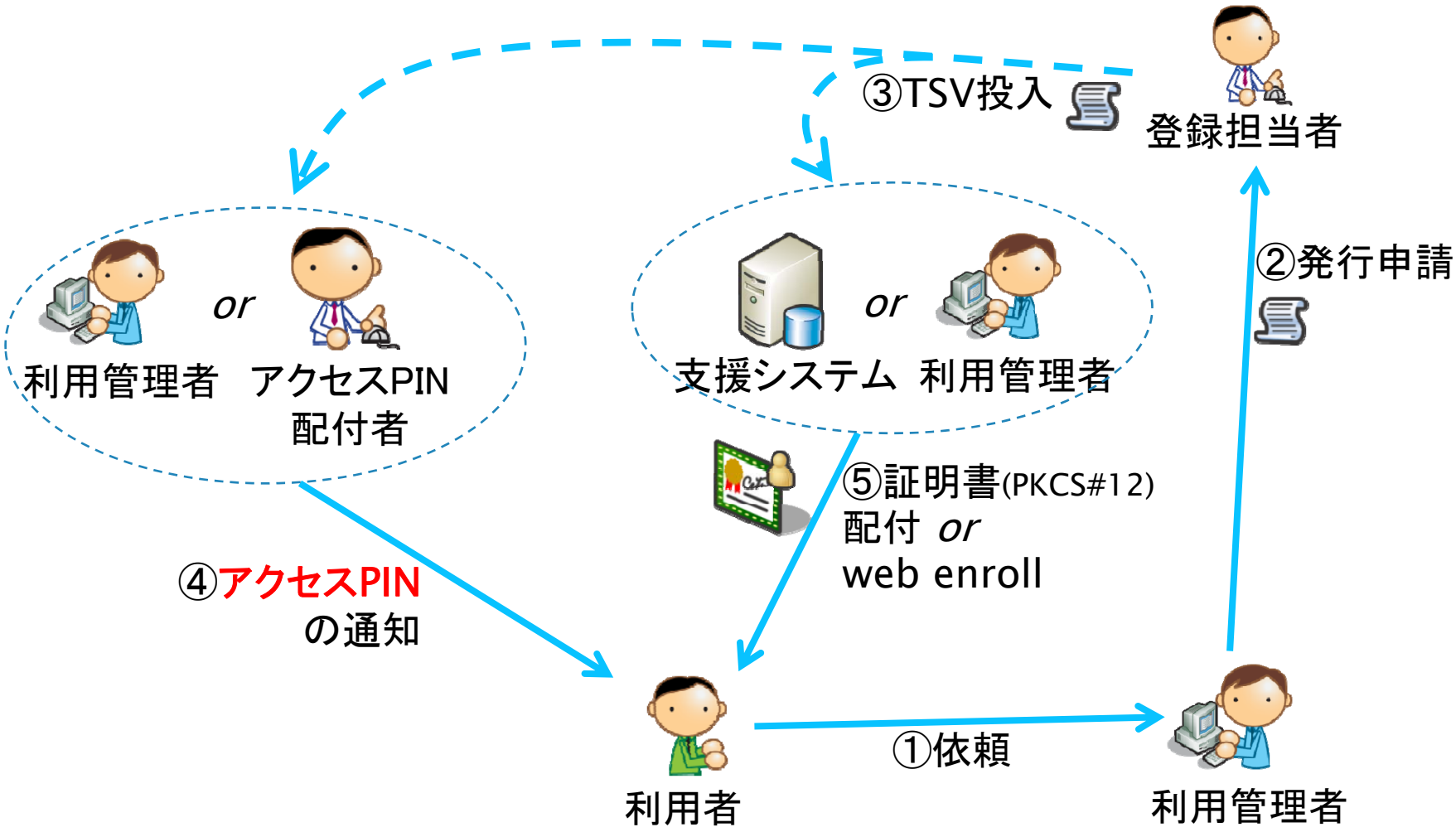

国立情報学研究所
サービス利用機関
事務局（NII）
②サービス利用申請／承認
①任命
機関責任者
⑥審査
登録担当者
③機関情報登録
④登録担当者用証明書配付
⑤発行申請
TSV ファイル
①TSVファイルアップロード
TSV ファイル
利用管理者
Certification Authorities
WebTrust
証明書発行
発行局
証明書自動発行支援システム
⑧URL通知
サーバ管理者
クライアント証明書管理者
コード署名用証明書利用者
証明書インストール
配付
署名
認証局
サーバ
教員
職員
学生
etc.
アプリケーション
文書
etc.

サービス概要図

背景: クライアント証明書の発行対象は人

- 従来のフロー（サーバ証明書の発行フロー）
  - サーバはFQDNが識別子(ID)
    → DNSが各機関共通の信頼できる情報源(authoritative source)となりうる→フローがある程度共通になり説明が楽
    - IDを利用するシステムが単一(ブラウザ)、仕様が標準化されている(TLS)
- 対して「人」のIDおよび管理方法は各機関ばらばらであり、フローの共通化が困難
  - 人事データベースで管理している？中身はどんなもの？
  - IDは教職員番号？メールアドレス？ePPN？
    （IDとして何を選ぶべきかは証明書を利用するシステムに依存し、そのシステムも多様）
- なお、本説明ではサーバ証明書の発行方法については熟知しているものとしています（すみません）

クライアント証明書発行フロー概要



用語: 利用管理者と利用者の違い

- 利用管理者 
  - 常勤の教職員
  - 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
  - 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

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「大学法人」を区別して扱いますのでご注意ください

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

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

補足: CNとして何を記載すべきか

- CNにIDを入れておくことで、証明書を利用するシステムでIDを取得することが容易になります(*)
  - 再掲となりますが、IDとして何を選ぶべきかは証明書を利用するシステムに依存します
- CNの候補:
  教職員番号/学籍番号, ePPN, メールアドレス, 氏名ローマ字, …
  - 氏名のように重複がある場合はDN全体で一意となるように適宜修正してください

- ただし、S/MIMEに利用する場合は氏名を入れることをお勧めします
  - メールソフトが署名証明書のこの部分を表示するため

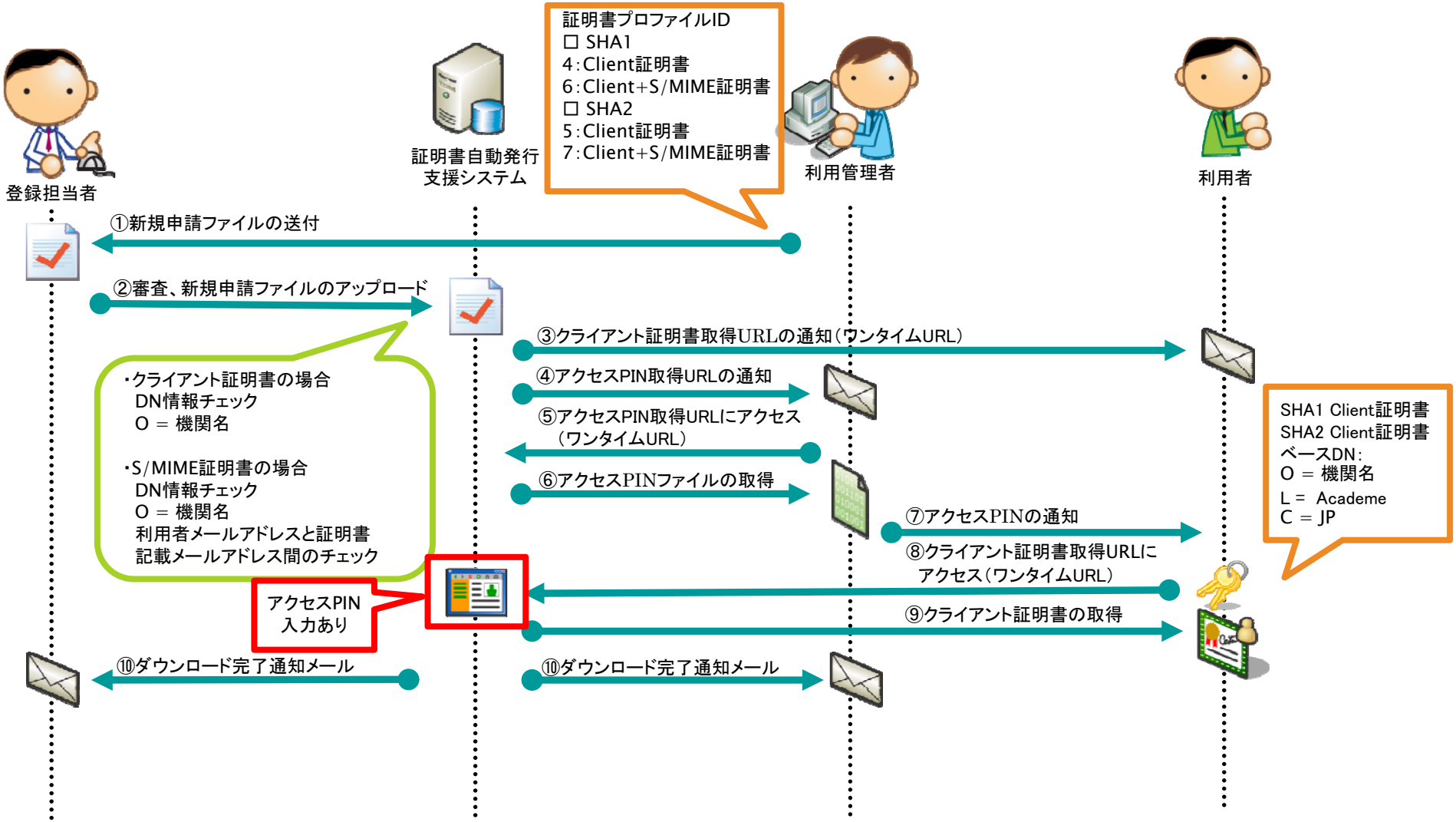
(*) - もちろんCNに格納する以外にも、OUに入れる、S/MIME使用の場合subjectAltNameからメールアドレスを取得する、IDと証明書の紐付けをDBで管理する、などの方法が考えられます

発行形態の選択

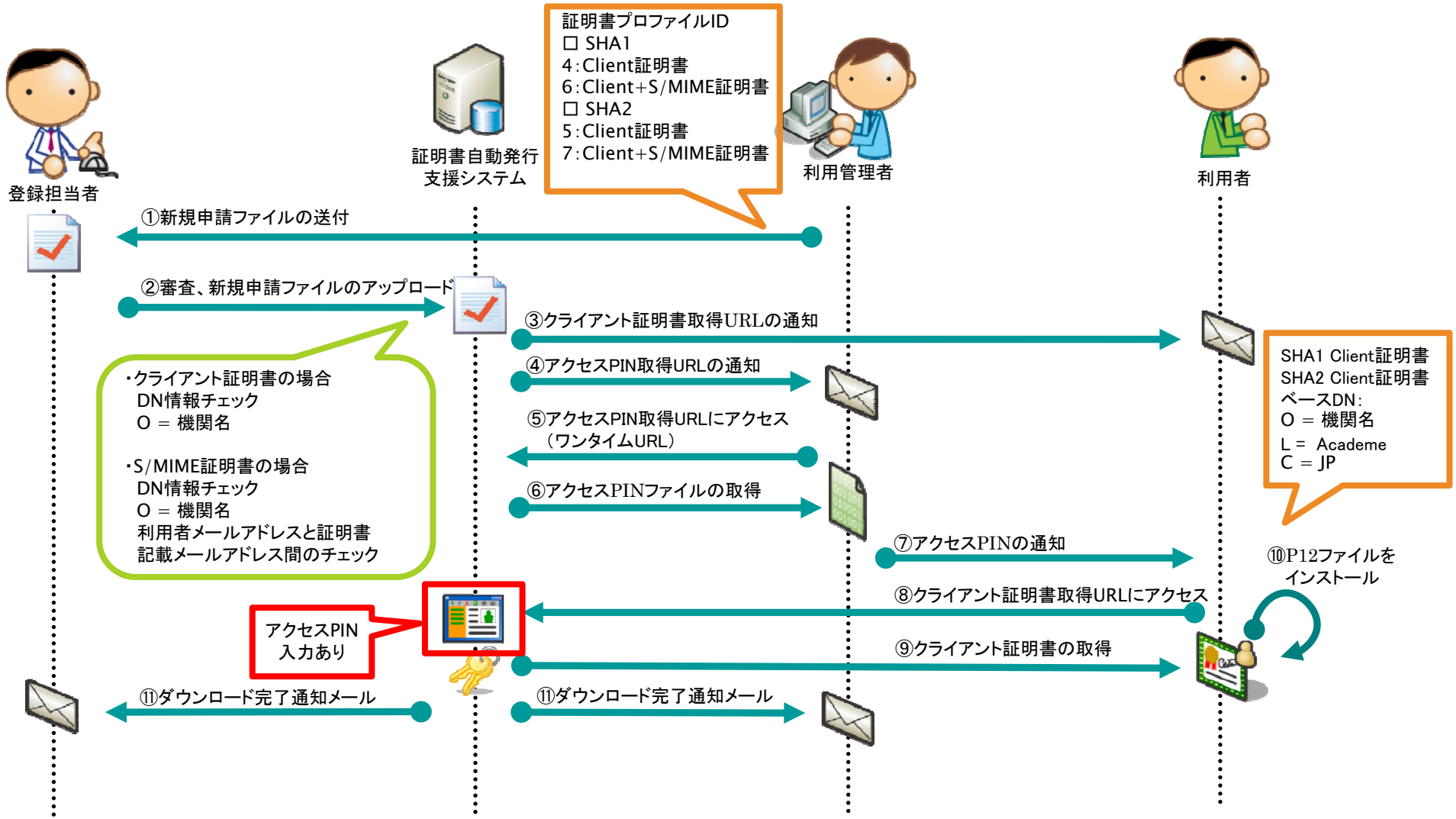
証明書用途や機関の事情、利用者のスキル等によって
3つの形態から選択してください

1. 「ブラウザ発行」
   - 証明書インストール(web enroll)を利用者に任せる
   - ブラウザ内で秘密鍵が生成されるため機密性が高い
   - 利用者にスキルがあってIE/Firefoxを強制できる場合
2. 「P12個別」
   - 証明書(PKCS#12)インストールを利用者に任せる
   - IE/Firefox以外も対象とする場合
3. 「P12一括」
   - 発行フローが発行側で完結しており、利用者には見えない
   - 証明書配付まで機関がコントロールしたい場合
     - 職員証/学生証に格納して配付　など

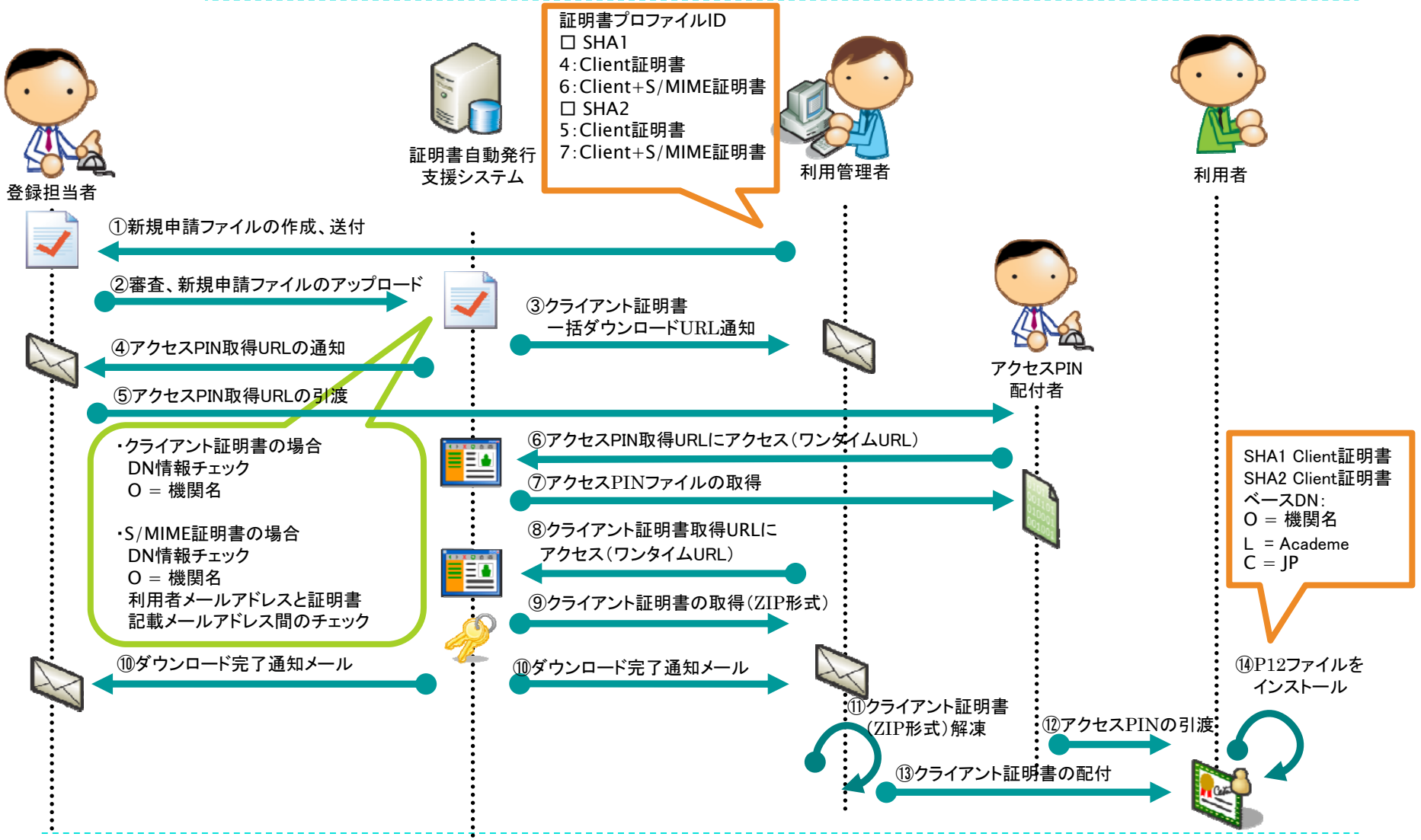
発行フロー（ブラウザ発行）



発行フロー（P12個別）


証明書プロファイルID
□ SHA1
4：Client証明書
6：Client+S/MIME証明書
□ SHA2
5：Client証明書
7：Client+S/MIME証明書
登録担当者
証明書自動発行
支援システム
利用管理者
利用者
①新規申請ファイルの送付
②審査、新規申請ファイルのアップロード
③クライアント証明書取得URLの通知
④アクセスPIN取得URLの通知
⑤アクセスPIN取得URLにアクセス
（ワンタイムURL）
⑥アクセスPINファイルの取得
⑦アクセスPINの通知
⑧クライアント証明書取得URLにアクセス
⑨クライアント証明書の取得
⑩P12ファイルを
インストール
⑪ダウンロード完了通知メール
⑪ダウンロード完了通知メール
・クライアント証明書の場合
DN情報チェック
O ＝ 機関名
・S/MIME証明書の場合
DN情報チェック
O ＝ 機関名
利用者メールアドレスと証明書
記載メールアドレス間のチェック
アクセスPIN
入力あり
SHA1 Client証明書
SHA2 Client証明書
ベースDN：
O ＝ 機関名
L ＝ Academe
C ＝ JP

発行フロー（P12一括）


登録担当者
証明書自動発行
支援システム
証明書プロファイルID
□ SHA1
4：Client証明書
6：Client+S/MIME証明書
□ SHA2
5：Client証明書
7：Client+S/MIME証明書
利用管理者
利用者
①新規申請ファイルの作成、送付
②審査、新規申請ファイルのアップロード
③クライアント証明書
一括ダウンロードURL通知
④アクセスPIN取得URLの通知
⑤アクセスPIN取得URLの引渡
アクセスPIN
配付者
・クライアント証明書の場合
DN情報チェック
O ＝ 機関名
・S/MIME証明書の場合
DN情報チェック
O ＝ 機関名
利用者メールアドレスと証明書
記載メールアドレス間のチェック
⑥アクセスPIN取得URLにアクセス（ワンタイムURL）
⑦アクセスPINファイルの取得
⑧クライアント証明書取得URLに
アクセス（ワンタイムURL）
⑨クライアント証明書の取得（ZIP形式）
⑩ダウンロード完了通知メール
⑩ダウンロード完了通知メール
SHA1 Client証明書
SHA2 Client証明書
ベースDN：
O ＝ 機関名
L ＝ Academe
C ＝ JP
⑭P12ファイルを
インストール
⑪クライアント証明書
（ZIP形式）解凍
⑫アクセスPINの引渡
⑬クライアント証明書の配付

アクセスPIN ZIPファイルフォーマット

- clientPin.zipもしくはclientAllPin.zipというファイル名でダウンロードされる
- 中にclientPin.txtもしくはclientAllPin.txtというファイルがある
  - TSV形式
  - 申請TSVの一部項目が併記され、突合できる
  - 内容の例:

利用者氏名	利用者mail	アクセスPIN	主体者DN
西村　健	takeshi@...	cVkKsC...	CN=...,...

P12 ZIPファイルフォーマット（P12一括の場合のみ）

- clientAll.zipというファイル名でダウンロードされる
- 中にclient.txtというインデックスファイルがある
  - TSV形式
  - 申請TSVの一部項目が併記され、突合できる
  - 内容の例:

シリアル番号	利用者氏名	利用者mail	主体者DN
6902…	西村　健	takeshi@…	CN=…,…

※シリアル番号は10進数表記

- 他に“<シリアル番号>.p12”というファイル名でPKCS#12ファイルが入っている

想定する利用管理者パターン

1. 登録担当者が引き受けるパターン
   - 利用管理者＝登録担当者
   - 小規模向け
2. 利用管理者=利用者とするパターン
   - 利用管理者の資格を持つ任意の人からの申請を受け付ける
   - 登録担当者は比較的楽
3. 部局に委譲するパターン
   - TSV形式各部局に利用管理者を1人ずつ割り当てる
   - 情報管理が分散している場合かつ大規模向け
4. 利用管理者は固定の1人とするパターン
   - ICカード発行者等の特定の者のみを利用管理者とする
   - P12一括発行と組み合わせて利用

最後に：利用者向けマニュアルの整備

- 利用者が迷わないように、機関ごとにフローに特化した証明書取得マニュアルを整備することをお勧めします
  - 本サービスが公開しているものは一般的・網羅的すぎる
- 公開しているマニュアルのWord版（依頼があれば提供）を適宜修正してもよいです

- その際、利用者に秘密鍵を厳重に管理するよう周知してください。また秘密鍵が危殆化した場合は速やかに報告するよう周知してください。

おまけ: スモールスタートの勧め

- 人事データベースから情報を取る形でなければクライアント証明書を発行してはいけないということではありません
- まずは身の回りの人に発行して、自分たちで使ってみるということも大事です
- その際、「何を情報源にしたか」「どんな確認を行ったか」記録を残すようにしてください

（予告）確認実施手順調査票の拡張

- 現状の調査票はクライアント証明書の発行体制を記述するには不十分
  - 主にサーバ証明書を念頭に置いたもの
- クライアント証明書発行に関する調査事項をとりまとめ、各機関に提出を依頼する予定です
- ご協力をよろしくお願いします