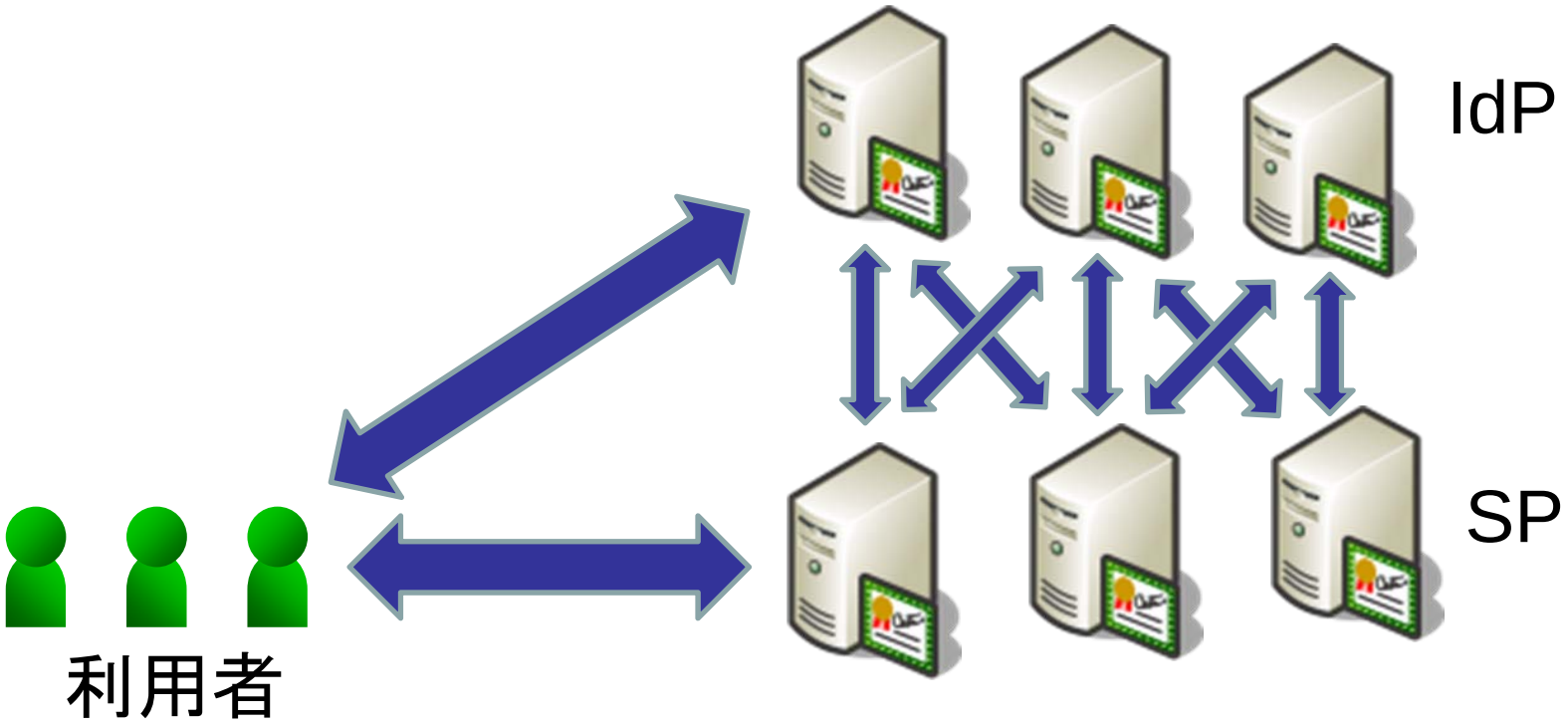
電子証明書自動発行の認証フェデレーションへの活用

国立情報学研究所
西村　健

学術認証フェデレーションと サーバ証明書

- IdP/SP等**サーバの認証**に証明書を用いる
  - 電子証明書（PKI）はWebセキュリティの根幹



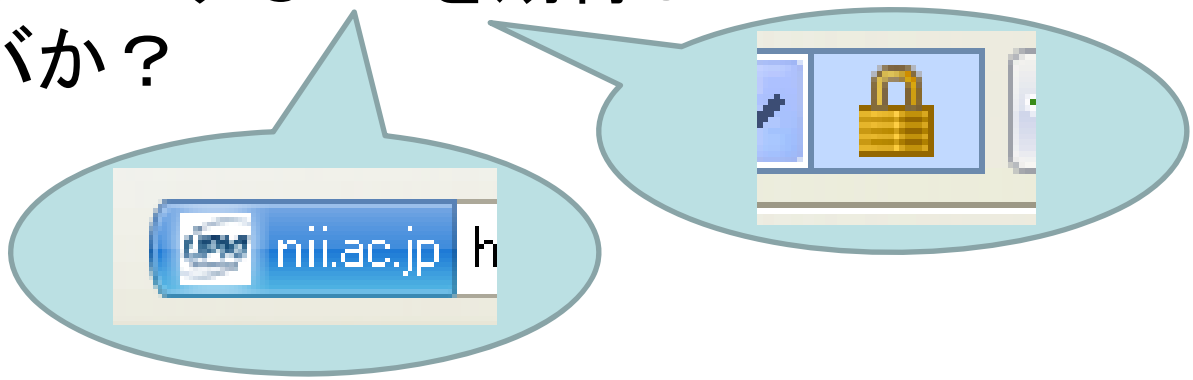
これだけある本プロジェクトのメリット

学術認証フェデレーションに関連して:

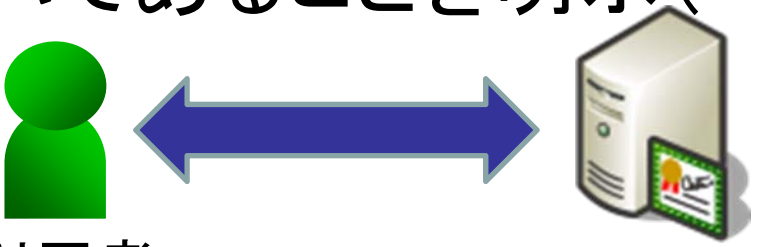
1. 学内構成員に安心してID/パスワードを入力してもらう(IdP)
   サービス利用者に安心して利用してもらう(SP)
2. IdP - SP間の安全性のために
3. バックエンドに対する認証

1) 利用者にサーバを安心して利用してもらう

- 利用者がアクセスしているものが本物か?
  - 利用者がアクセスすることを期待しているサーバか？



- xxx.nii.ac.jpという名前のサーバであるということだけでなく**NIIのサーバ**であることを明示（組織認証）

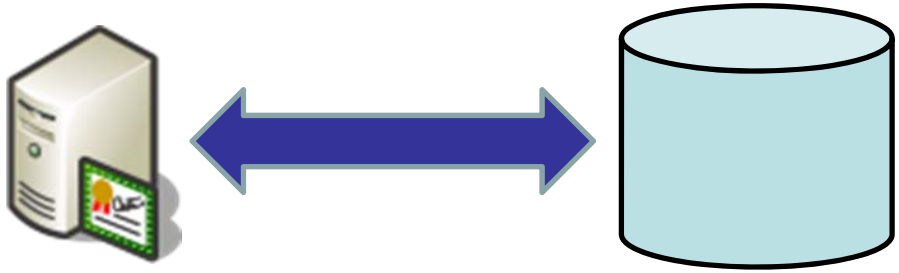


2) IdP – SP間の安全性

- IdP（大学）とSP（サービス）の間で**情報**をやり取りする
  - 「認証された」という情報
  - 「学生である/教員である」という情報（属性）
- **本物のIdPから本物のSP**に情報が渡されているのを保証するのがサーバ証明書
  - 組織認証が重要性を持つ

3) バックエンドに対する認証

- 多くの場合において、IdPサーバはバックエンドにあるデータベースに問合せを中継する
  - 専用線でつなぐ? IPアドレス制限?
- **SSLクライアント証明書認証！**
  - これまでの要件を全て一つの証明書で賄える
  - Windows Server上Active Directoryで実証



UPKIオープンドメイン証明書 自動発行検証プロジェクトの概要

- 目的

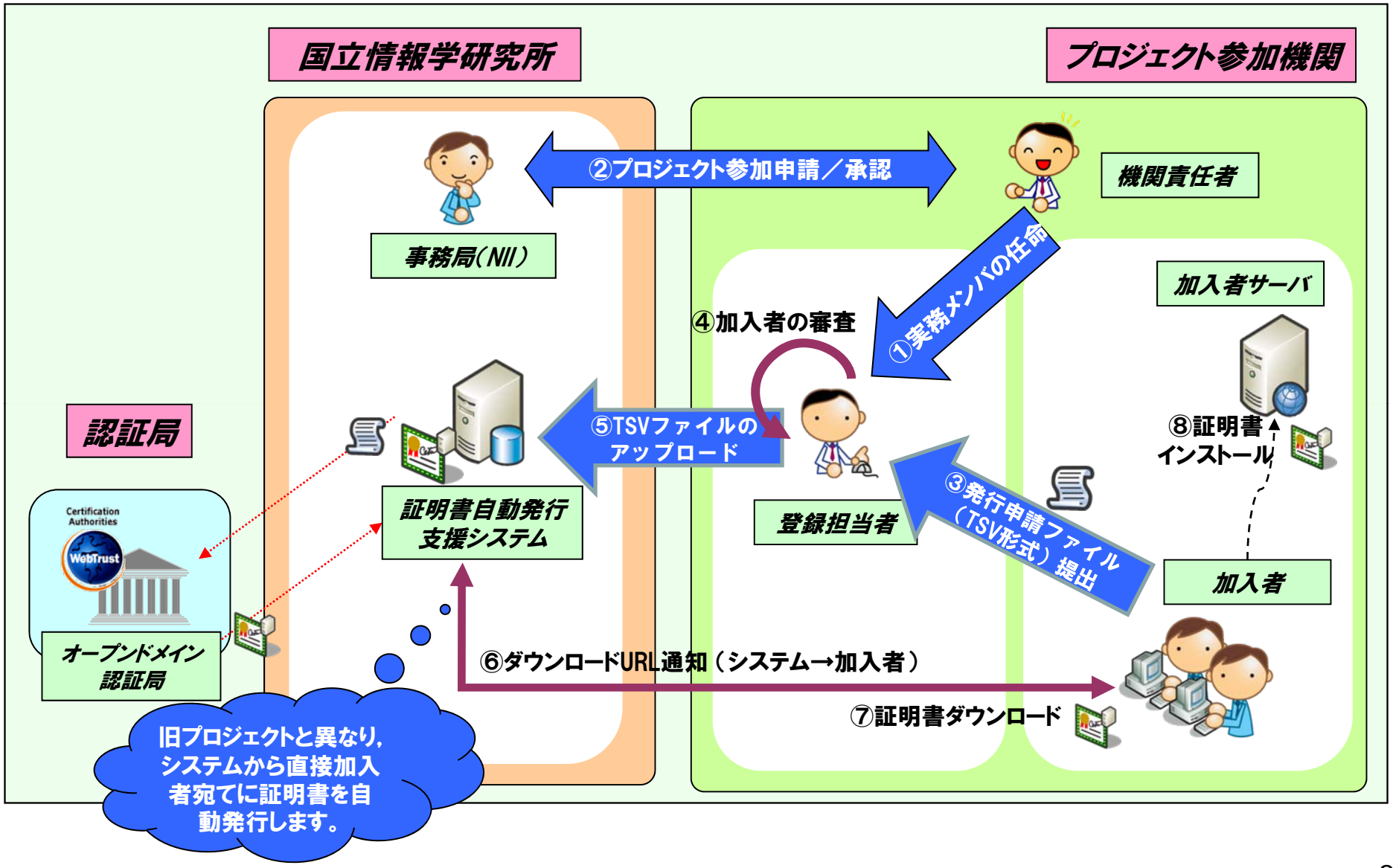
  サーバ証明書発行・導入における啓発・評価研究プロジェクト（旧プロジェクト）で得た知見をもとに，NIIが開発した電子証明書自動発行支援システムを用いて，学術機関へのサーバ証明書発行プロセスの最適化および自動化について検証を行う。

- 実施期間

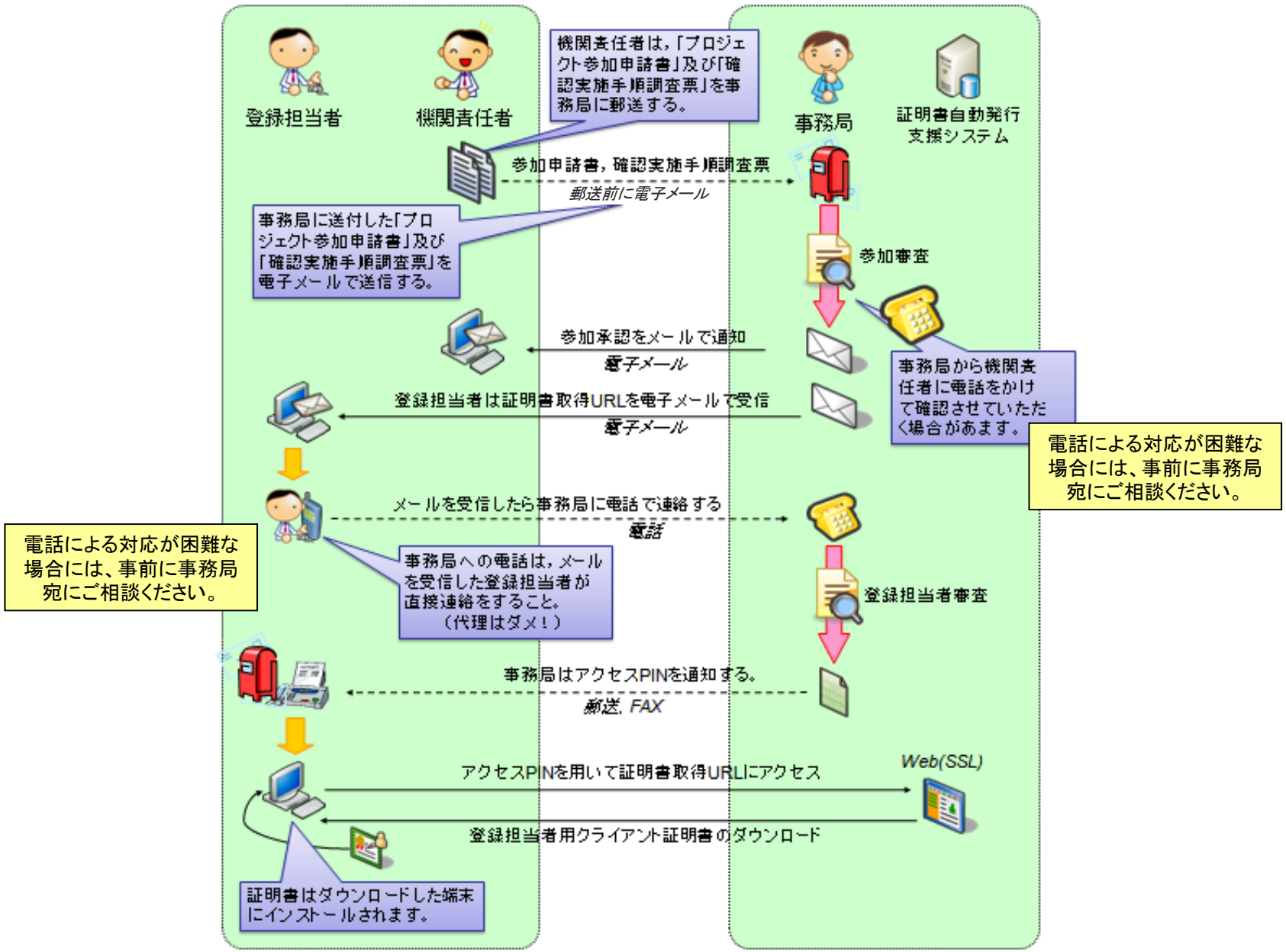
  平成21年4月1日 ～ 平成24年3月31日

- 実施内容
  - プロジェクトに協力いただく機関(参加機関)を募集します。
  - 参加機関に対してサーバ証明書を発行し，協同して検証評価を実施します。（年度末に評価項目について調査を実施）

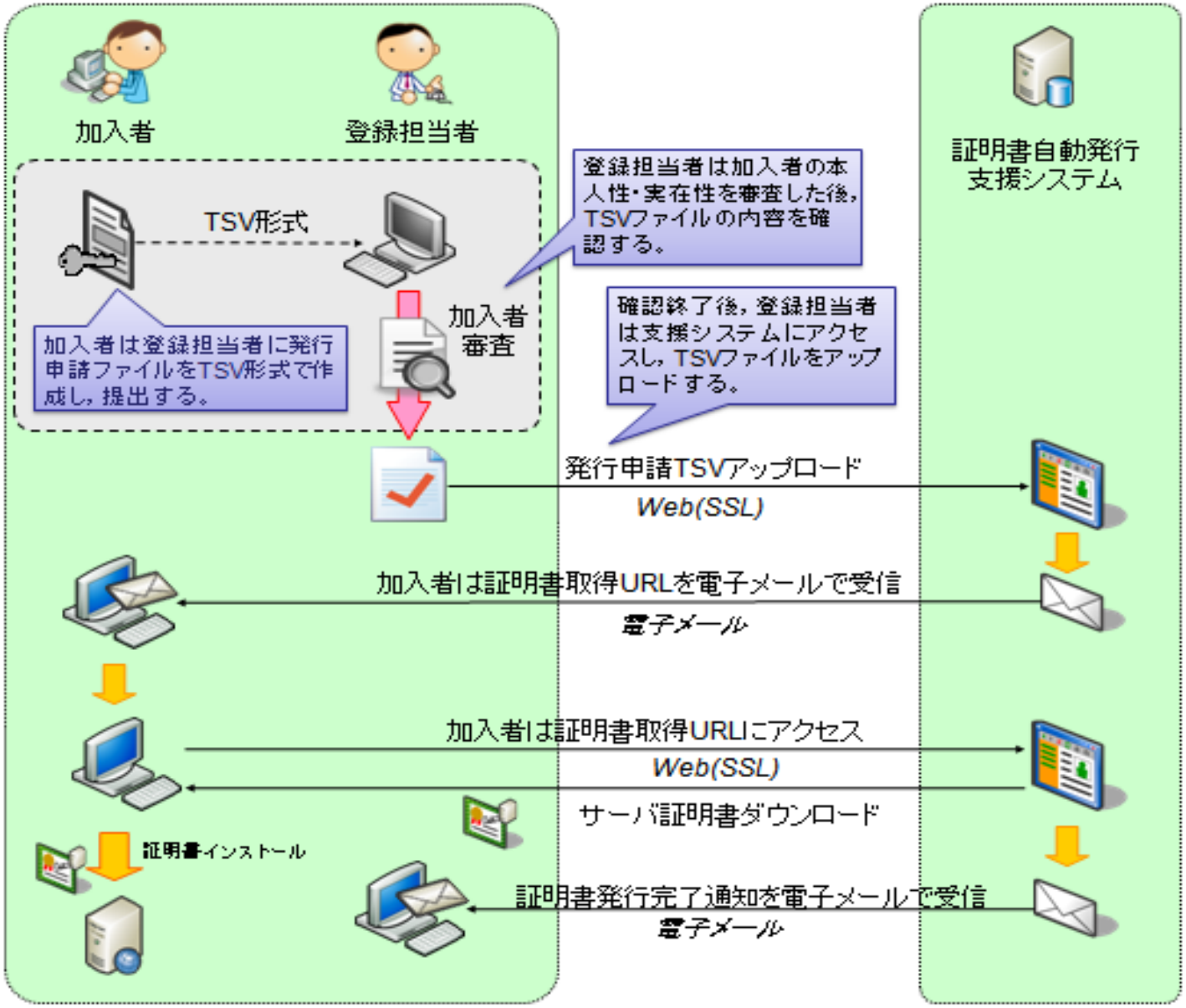
プロジェクト概念図


国立情報学研究所
プロジェクト参加機関
②プロジェクト参加申請／承認
機関責任者
事務局(NII)
①実務メンバの任命
加入者サーバ
④加入者の審査
⑤TSVファイルの
アップロード
⑧証明書
インストール
認証局
証明書自動発行
支援システム
登録担当者
③発行申請ファイル
（TSV形式）提出
加入者
Certification
Authorities
WebTrust
オープンドメイン
認証局
⑥ダウンロードURL通知（システム→加入者）
⑦証明書ダウンロード
旧プロジェクトと異なり，
システムから直接加入
者宛てに証明書を自
動発行します。

参加申請手順


登録担当者
機関責任者
事務局
証明書自動発行
支援システム
機関責任者は，「プロジェクト参加申請書」及び「確認実施手順調査票」を事務局に郵送する。
参加申請書，確認実施手順調査票
郵送前に電子メール
事務局に送付した「プロジェクト参加申請書」及び「確認実施手順調査票」を電子メールで送信する。
参加審査
参加承認をメールで通知
電子メール
事務局から機関責任者に電話をかけて確認させていただく場合があります。
登録担当者は証明書取得URLを電子メールで受信
電子メール
電話による対応が困難な場合には、事前に事務局宛にご相談ください。
メールを受信したら事務局に電話で連絡する
電話
事務局への電話は，メールを受信した登録担当者が直接連絡をすること。
（代理はダメ！）
電話による対応が困難な場合には、事前に事務局宛にご相談ください。
登録担当者審査
事務局はアクセスPINを通知する。
郵送，FAX
Web(SSL)
アクセスPINを用いて証明書取得URLにアクセス
登録担当者用クライアント証明書のダウンロード
証明書はダウンロードした端末にインストールされます。

証明書取得手順


加入者
登録担当者
証明書自動発行
支援システム
TSV形式
加入者
審査
加入者は登録担当者に発行申請ファイルをTSV形式で作成し，提出する。
登録担当者は加入者の本人性・実在性を審査した後，TSVファイルの内容を確認する。
確認終了後，登録担当者は支援システムにアクセスし，TSVファイルをアップロードする。
発行申請TSVアップロード
Web(SSL)
加入者は証明書取得URLを電子メールで受信
電子メール
加入者は証明書取得URLにアクセス
Web(SSL)
サーバ証明書ダウンロード
証明書インストール
証明書発行完了通知を電子メールで受信
電子メール

他にもあるメリット

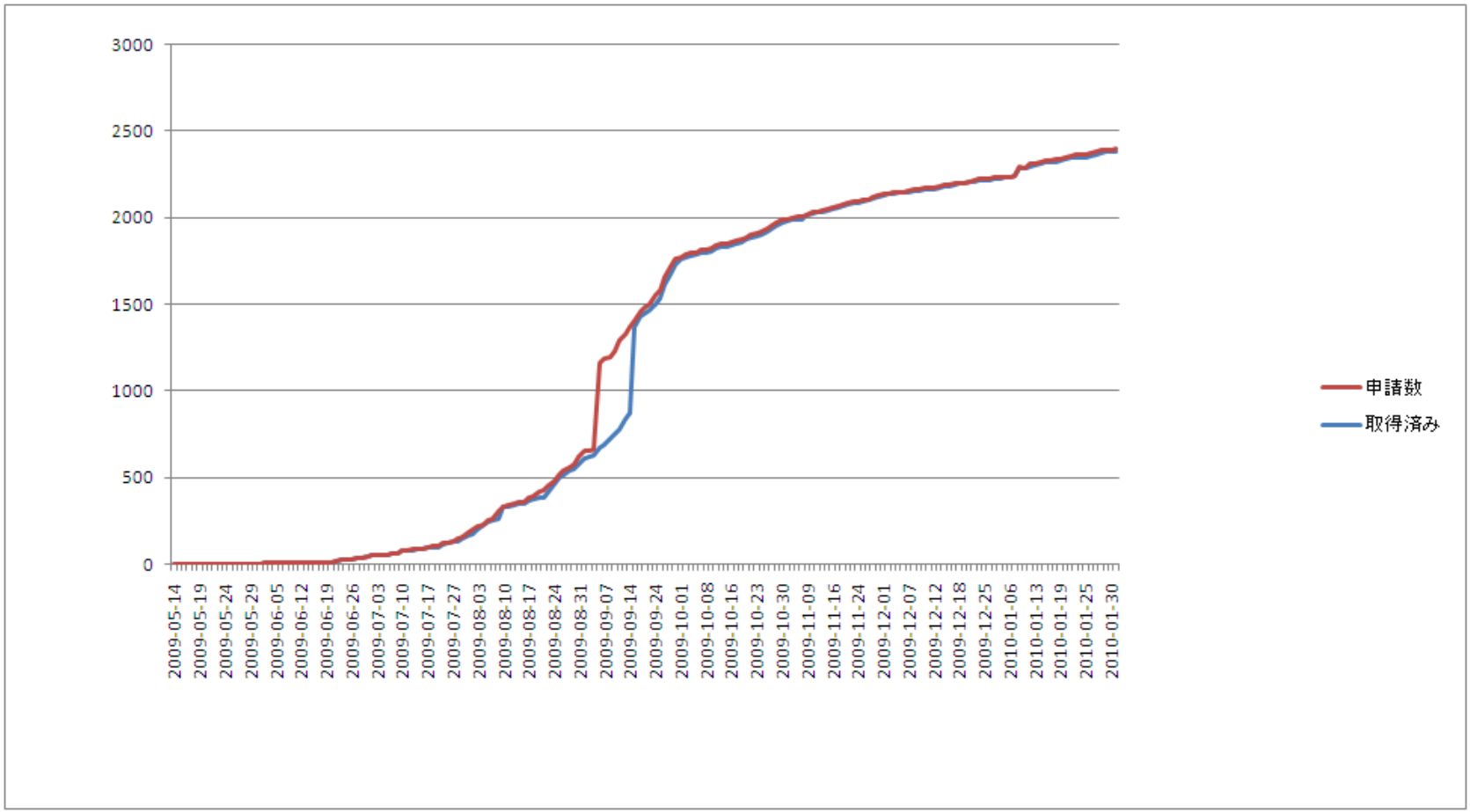
- 無償
- 申請がシンプル
  オンラインでの申請（登録担当者）
- 携帯電話からのアクセスのサポート
- 複数年証明書
- 1機関複数ドメインへの対応

平成21年度の参加状況

（平成22年2月末現在）

- 機関数　　…　130機関超
- 発行枚数　　…　2500枚超

平成21年度（新プロジェクト）の発行状況推移

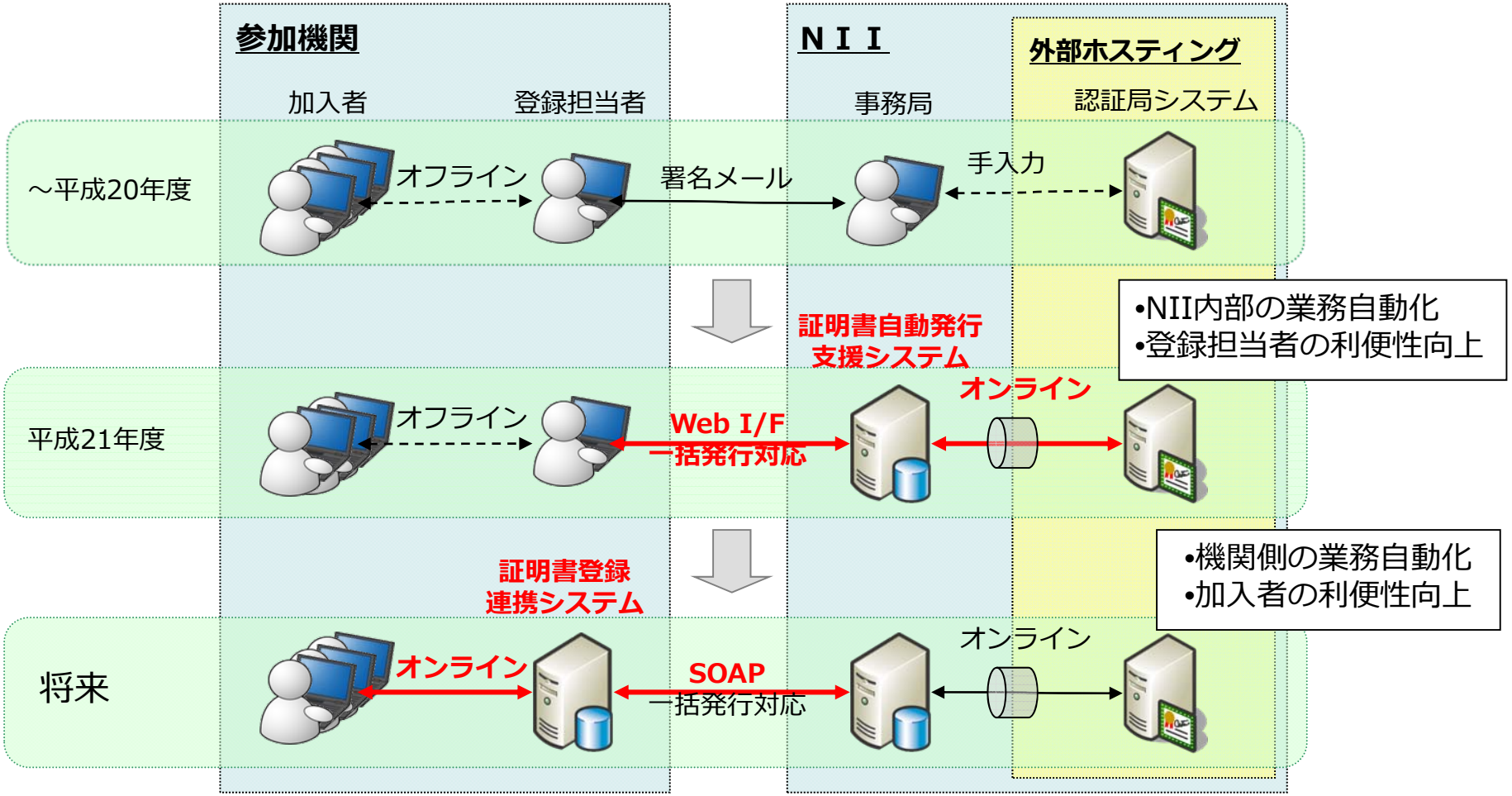


次年度以降に向けて

- 学術認証フェデレーションとの連携を検討
  - 1SPとしてサーバ証明書サービスを提供する

- 学内認証基盤との連携

ゴール: 学内認証基盤との連携



本プロジェクトに関するお問い合わせ等

UPKIオープンドメイン証明書自動発行検証プロジェクト

国立情報学研究所 学術基盤推進部基盤企画課
総括・連携システムチーム

メールアドレス：cerpj2@nii.ac.jp

プロジェクトホームページ
https://upki-portal.nii.ac.jp/docs/odcert