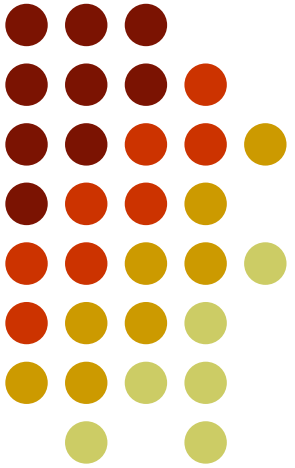
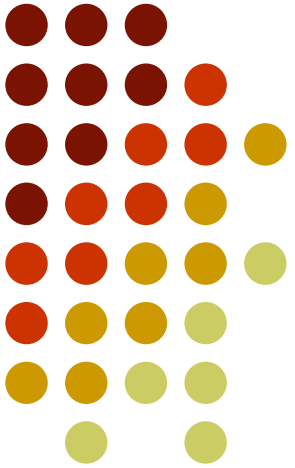
大学のサーバ証明書 自動発行を目指して

国立情報学研究所
島岡 政基



プロジェクトの紹介

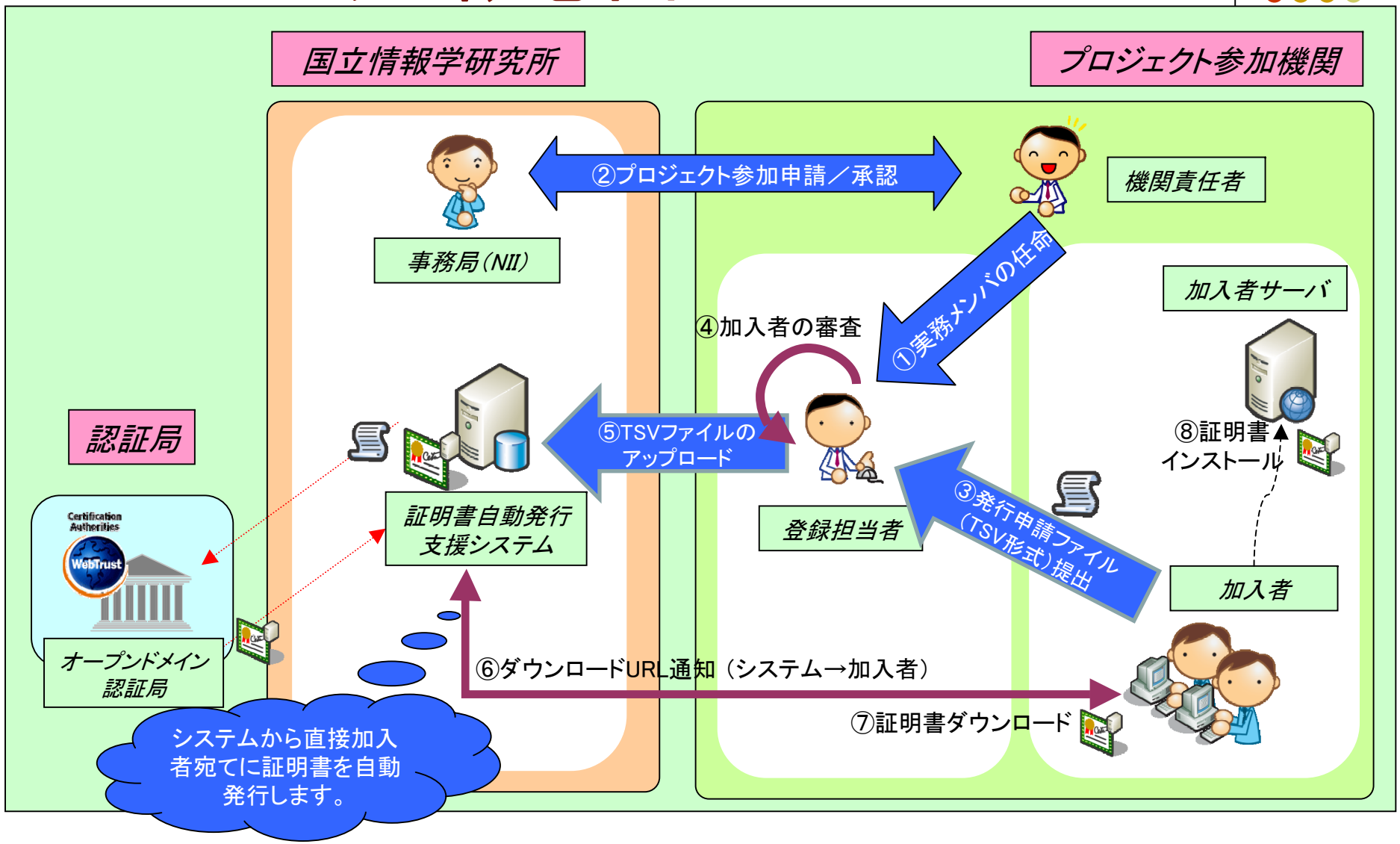
UPKIオープンドメイン証明書
自動発行検証プロジェクト



UPKIオープンドメイン証明書自動発行検証プロジェクト

- 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。
- 期間
  - 平成21年4月1日～平成24年3月末まで(3年間)
- 対象
  - SINETに加入している学術機関など

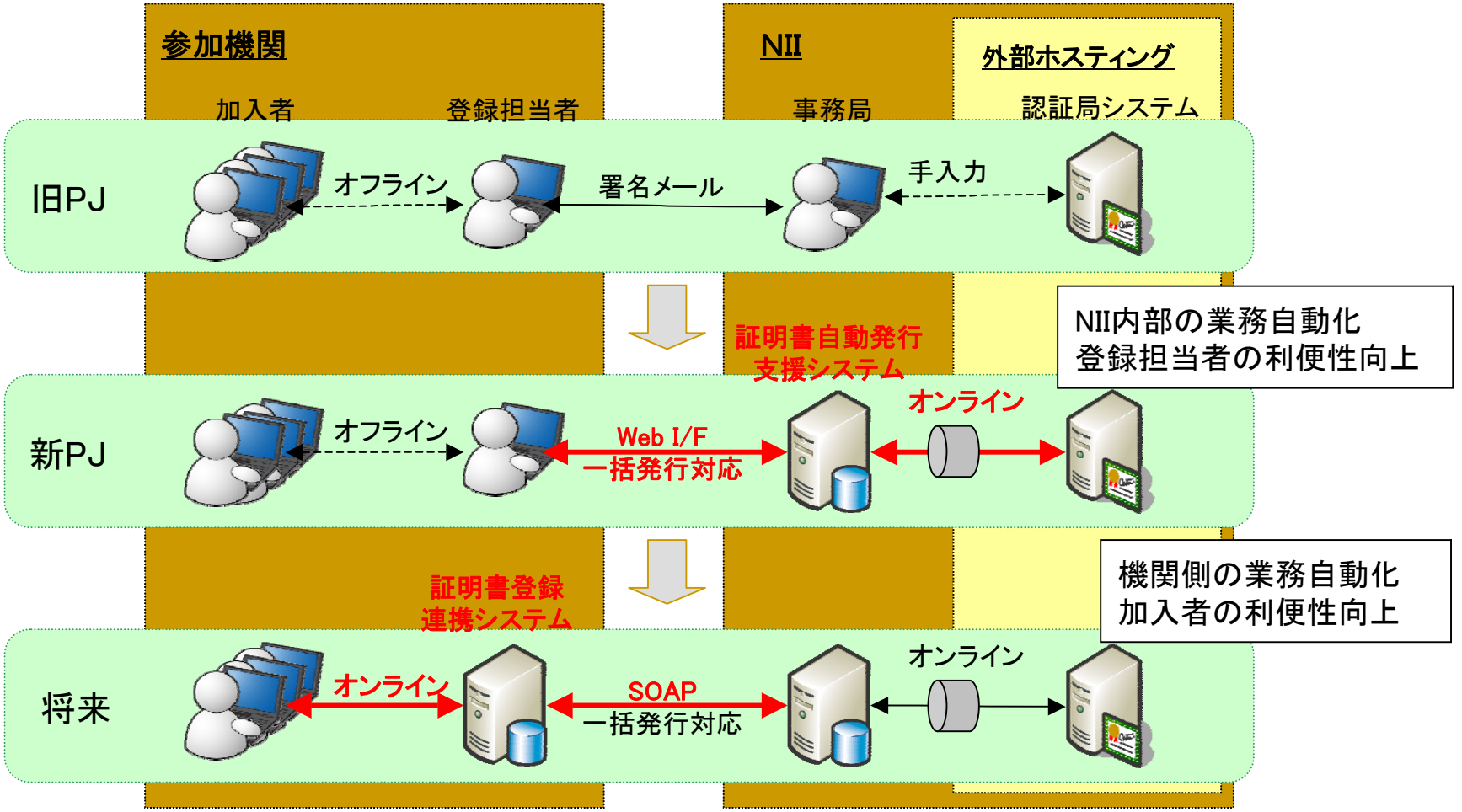
プロジェクト概念図


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
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
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。

登場人物・用語など

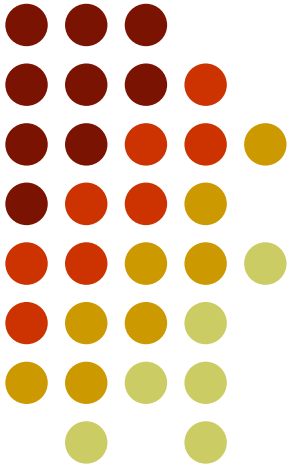
組　織	用　語	説　明
NII	オープンドメイン認証局	本プロジェクトで使用する，サーバ証明書を発行するための認証局。Web Trust for CAに準拠しており，世界的に信頼できる証明書の発行が可能です。また，この証明書は，主要なウェブブラウザ等で，商用のサーバ証明書と同様に利用することが可能です。
	証明書自動発行支援システム	Webブラウザで本システムにアクセスすることによって，登録担当者からの証明書発行申請や，加入者による証明書ダウンロードなどの機能をご利用いただけます。
	TSVファイル	本プロジェクトでは，証明書発行要求(CSR)や失効申請，その他各種申請についてTSVファイルというタブ区切りファイルを作成いただき，システムに投入していただくこととなります。
	事務局	プロジェクト参加申請や証明書発行申請にあたり審査業務等を実施するNIIの事務窓口です。
各大学	機関責任者	本プロジェクト参加にあたり，各機関で選出いただく代表者の方。課長職または准教授相当以上の常勤教職員の方にお願いいたします。
	登録担当者	本プロジェクトの参加機関側の事務的な窓口および加入者の審査業務の一部をお願いする方です。大学の規模等に応じて複数名選出していただくことも可能です。
	加入者	サーバを管理し，サーバ証明書を実際に利用される方。プロジェクト参加機関内の常勤の教職員の方であれば，どなたでも加入者となれます。
	加入者サーバ	加入者の方が管理するサーバ。

ゴール：
学内認証基盤との連携による自動発行

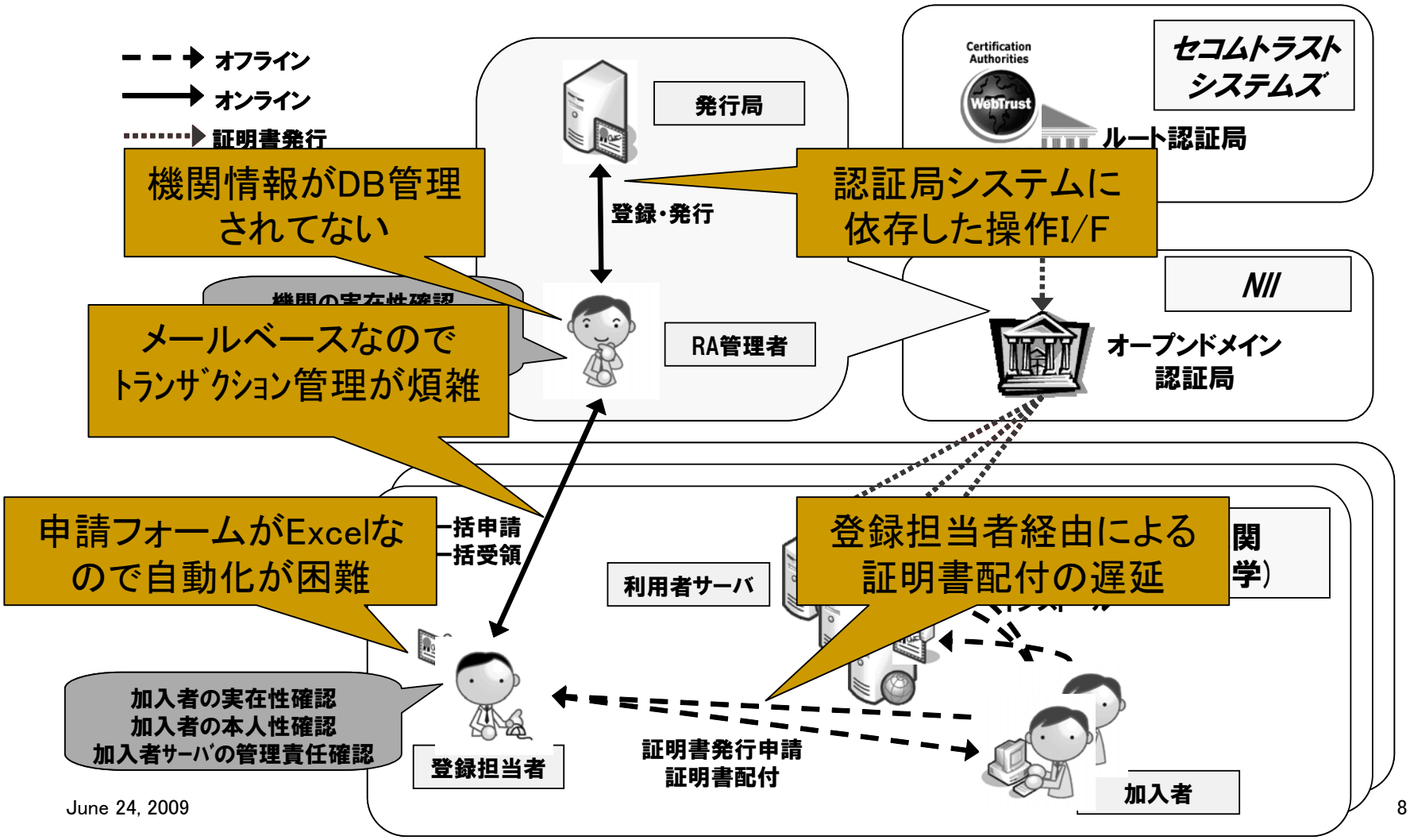


システムの紹介と自動発行の仕組み

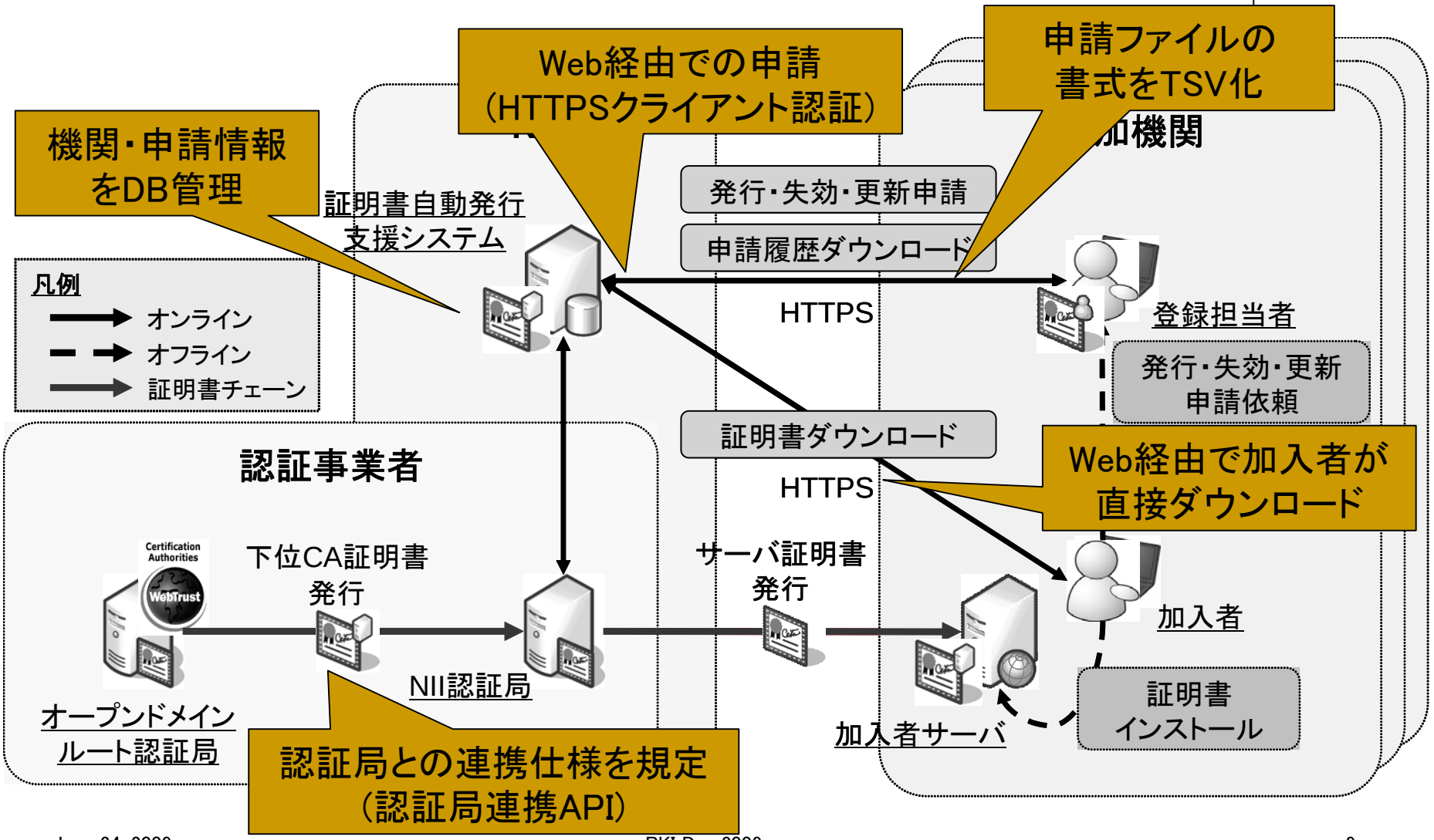
証明書自動発行支援システム



～自動発行へ向けて～
旧プロジェクトの課題



証明書自動発行支援システム



審査用語の定義

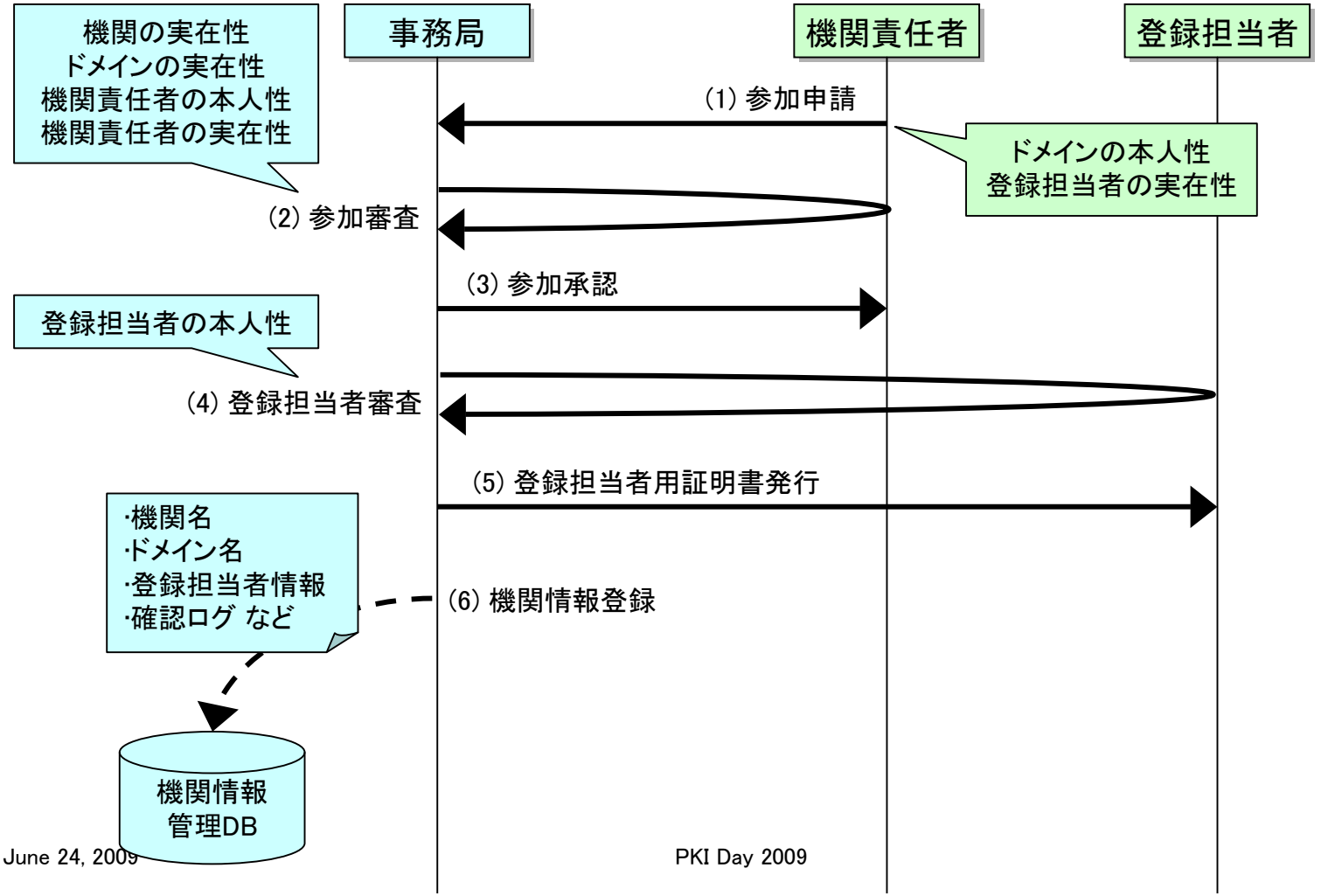
- 本人性確認
  - なりすましや否認を防止するために本人意思を確認する作業
- 実在性確認
  - 証明書に記載する組織に実在することを確認する作業

商用証明書との審査項目の比較

		商用サービス				本プロジェクト			
		ドメイン認証(DV)		組織認証(OV)					
		登録局	加入者	登録局	加入者	登録局	機関責任者	登録担当者	加入者
機関	本人性確認	×		○					
	実在性確認	×		○		○			
ドメイン	本人性確認	○		○		× →	△		
	実在性確認	○		○		○			
機関責任者	本人性確認					○ →			
	実在性確認					○ →			
登録担当者	本人性確認					○			
	実在性確認					× →	△	←	
加入者	本人性確認	×		○		×		△	
	実在性確認	×		○		×		△	
加入者サーバ	本人性確認		○		○				○
	実在性確認		○		○			△	×

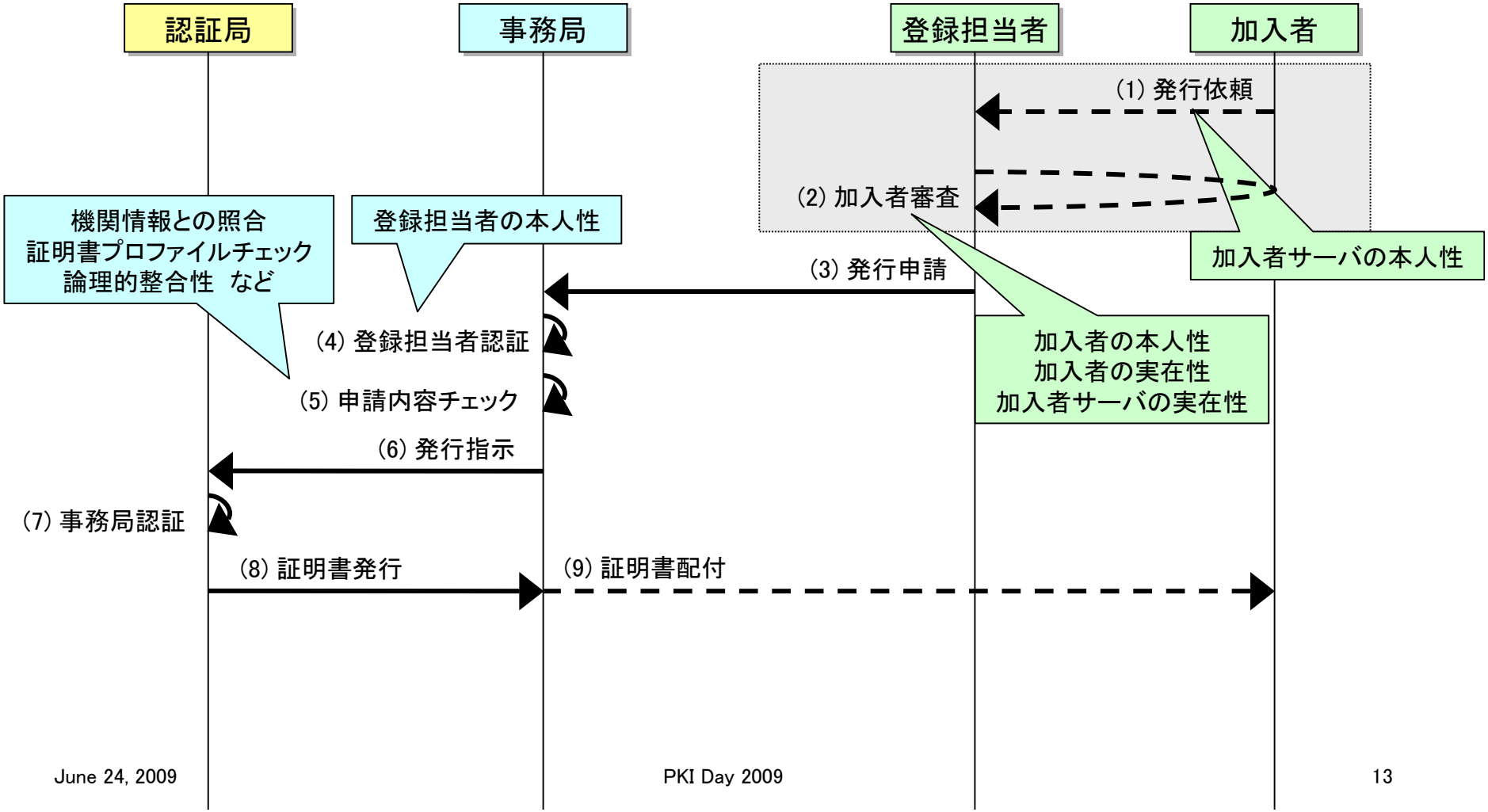
参加申請における審査

〇機関の実在性
△ドメインの本人性
〇機関責任者の本人性
〇機関責任者の実在性
〇登録担当者の本人性
△登録担当者の実在性
－加入者の本人性
－加入者の実在性
－加入者サーバの本人性
－加入者サーバの実在性



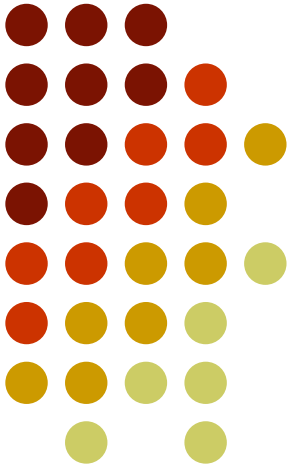
発行申請における審査

－機関の実在性
－ドメインの本人性
－機関責任者の本人性
－機関責任者の実在性
〇登録担当者の本人性
－登録担当者の実在性
△加入者の本人性
△加入者の実在性
〇加入者サーバの本人性
△加入者サーバの実在性

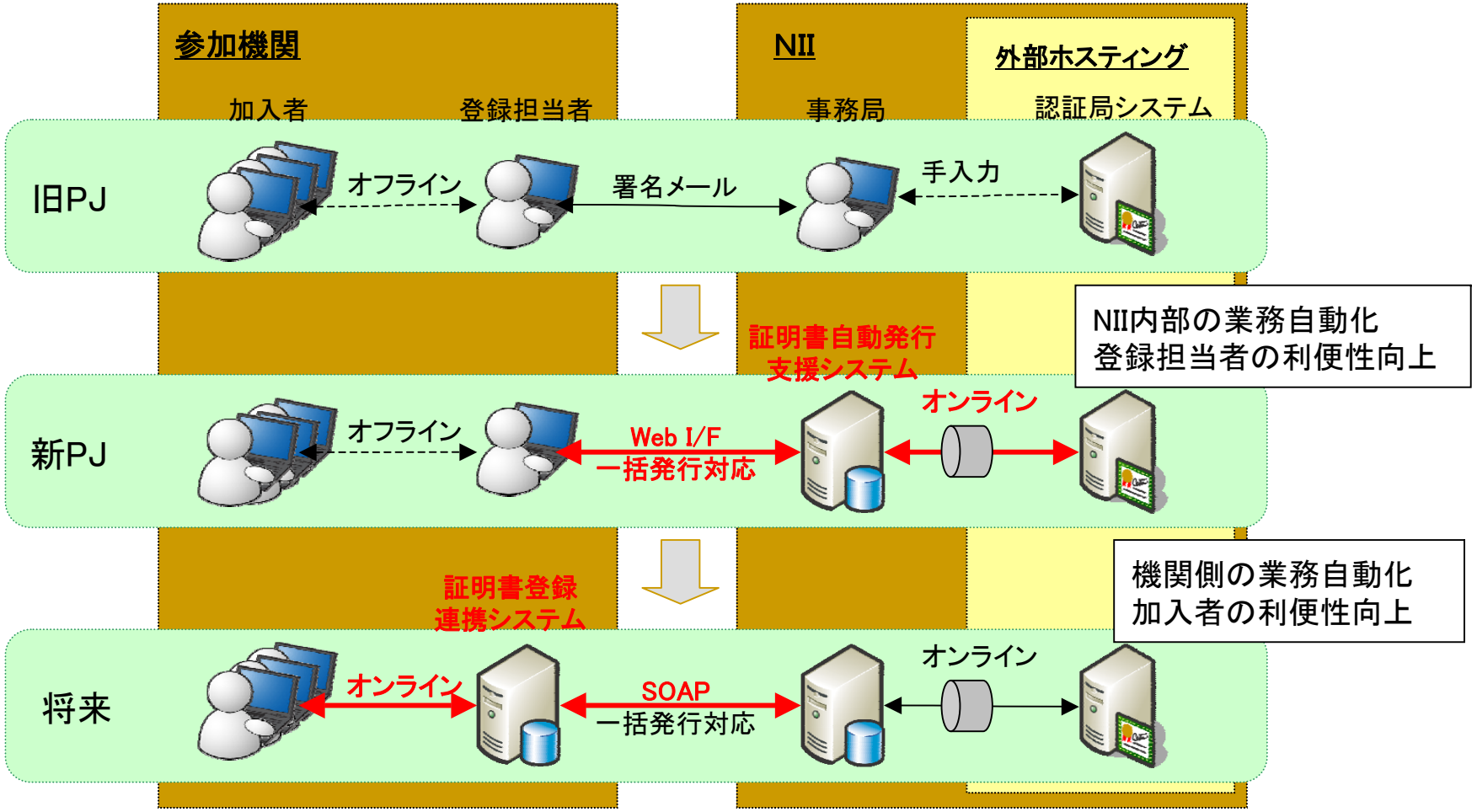


今後の目標
機関側処理の自動化

証明書登録連携システムの提案



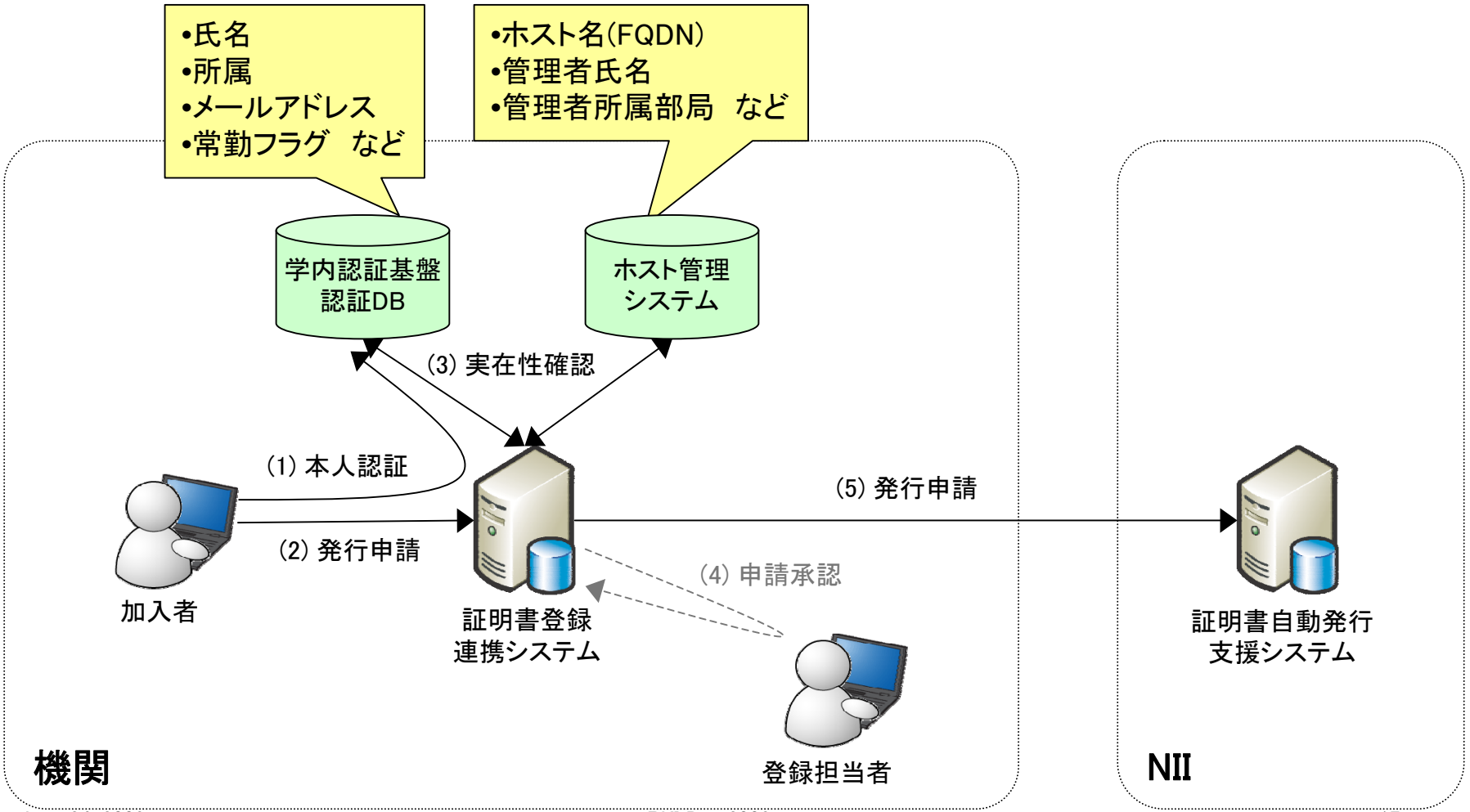
証明書登録連携システムによる機関側処理の自動化



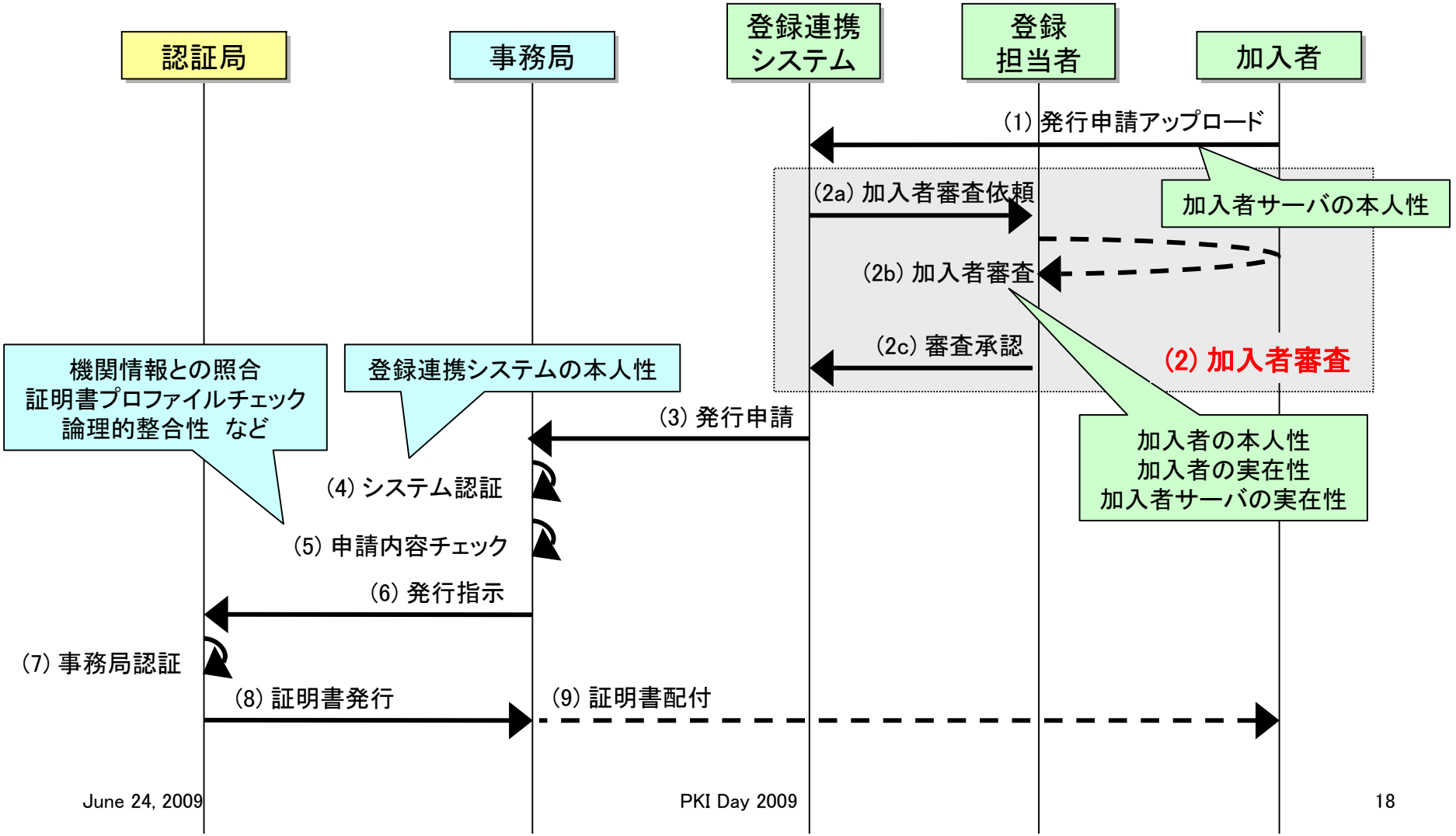
機関側の前提条件(案)

- 機関側に学内認証基盤が整備されていること
  - 加入者の本人性確認←本人認証
  - 加入者の実在性確認←属性管理
- サーバ管理データベースが整備されていること
  - 加入者サーバの実在性確認←FQDNと管理者をひもづけ
- 証明書登録連携システムの開発
  - 学内認証基盤による加入者の認証・認可
  - サーバ管理データベースによる照合

証明書登録連携システム(例)



学内認証基盤による
加入者審査の(半)自動化

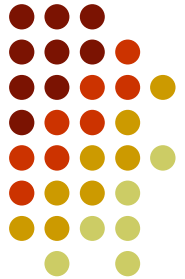


機関側の自動化対応へ向けた課題

- 学内認証基盤に対する要件の精査
  - なりすまし・否認防止
  - 申請権限(加入者要件)の認可
- 登録連携システムの自動化に対する考察
  - 機関によっては機械的審査が可能
  - 機械的承認の是非 – 機関によって様々
  - 学内認証基盤に大きく依存
- その他
  - 登録連携システムと登録担当者の識別の必要性
  - 支援システムのWeb I/Fの機能検証
  - 機関・事務局の運用負荷に対する評価

証明書自動発行支援システムを使ったフィージビリティスタディ

まとめ



- 証明書発行スキームの自動化
  - 大学に最適化した審査権限の分散
  - 証明書発行毎の事務局審査を完全自動化
- Webインタフェースによる申請手続きの改善
  - 各機関の登録担当者作業を効率化
  - 学内認証基盤との連携性向上
- 今後の目標
  - 学内認証基盤との接続連携・運用評価