

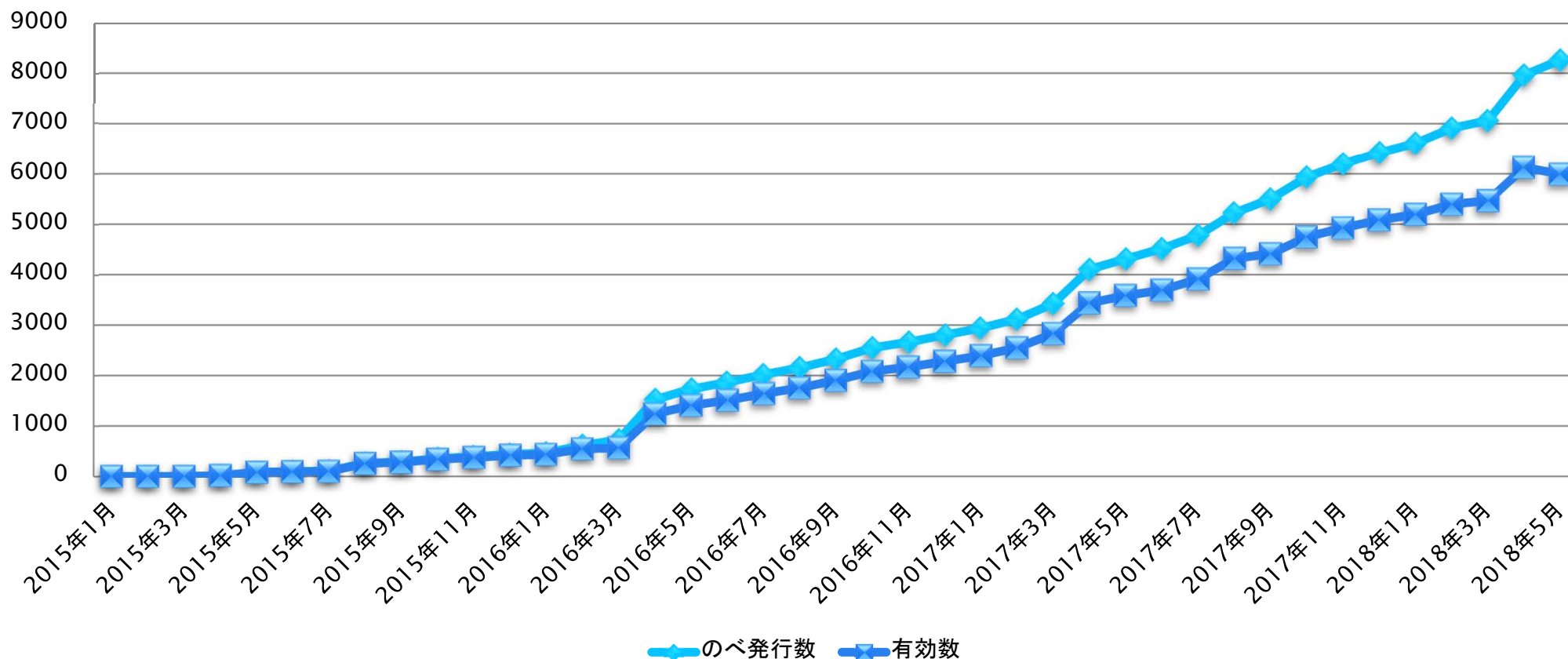
学認連携 クライアント証明書 発行システム



2018/6/21

中村素典 / 国立情報学研究所

クライアント証明書の発行数の推移



- ▶ クライアント証明書の普及を推進するには
 - ▶ クライアント証明書を活用するサービスの普及
 - ▶ クライアント証明書発行・配付の利便性向上



クライアント証明書を活用したいサービス

▶ 認証

▶ WiFi接続

▶ EAP-TLS

▶ VPN接続

▶ PPTP, SSTP, openVPN, ...

▶ Webページ等のアクセス

▶ 署名・暗号化

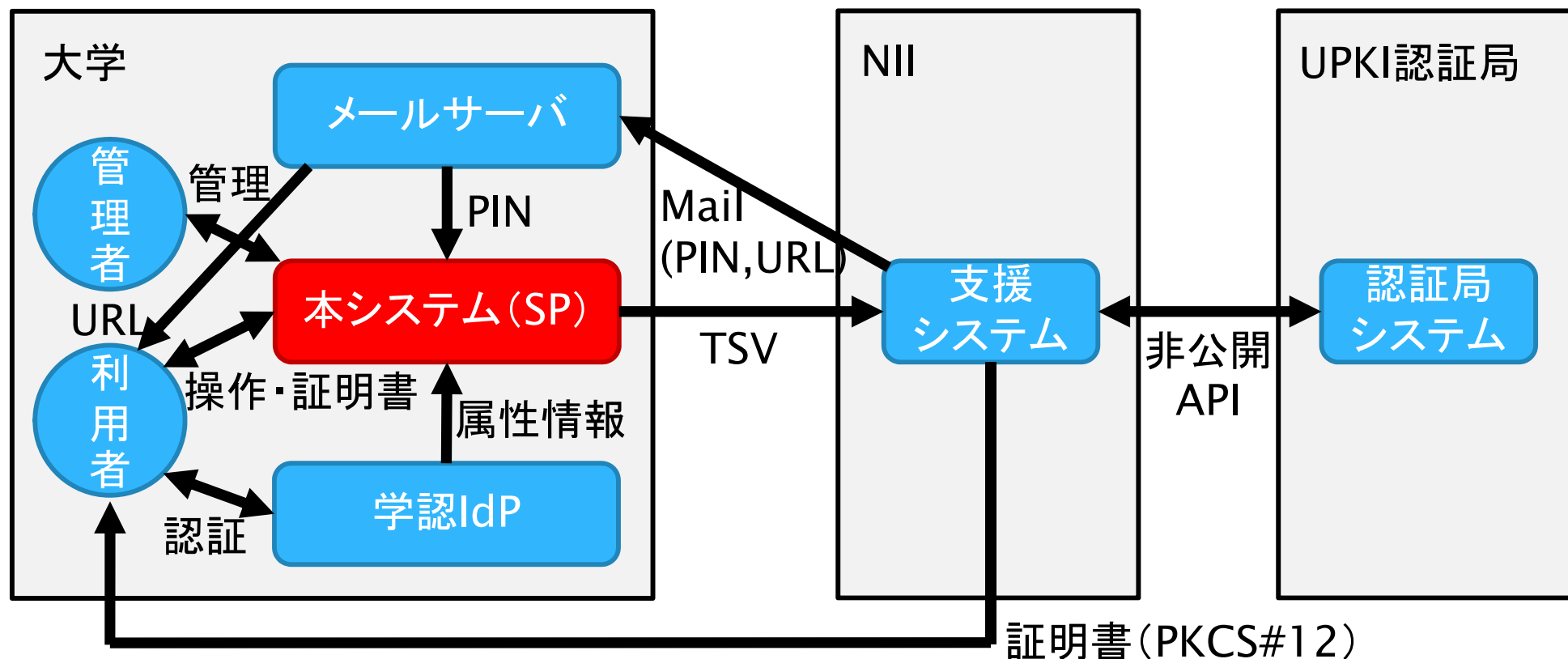
▶ S/MIME (電子メール)

▶ ドキュメントへの署名



クライアント証明書発行・配付の利便性向上に向けて

- ▶ 京都大学開発の「Shibcert: 学認連携に基づく個人証明書申請管理システム」 (プロトタイプ)
 - ▶ 利用者を認証し、クライアント証明書の発行申請を受け付けて、NIIに発行申請を自動中継する
 - ▶ 参考：オープンフォーラム2016発表資料
 - ▶ https://www.nii.ac.jp/csi/openforum2016/track/pdf/20160526PM_G_05_komura.pdf
- ▶ これをベースに汎用に拡張
 - ▶ 利用者情報
 - ▶ 属性情報eduPersonPrincipalName, email, displayNameから取得
 - ▶ 発行する証明書の選択
 - ▶ 認証用証明書、S/MIME証明書、認証+S/MIME両用証明書
 - ▶ 利用者自身による証明書一覧確認と失効申請
 - ▶ サイトの運用は機関毎を想定 (ソフトウェア提供)
 - ▶ 将来のUPKI Pass対応を考慮



- ▶ 大学毎に本システムを運用 (IdPとローカル連携)
- ▶ 管理者は事前に、支援システムアクセス用のクライアント証明書を本システムにインストール
 - ▶ 本システムは、「管理者」の代理として支援システムをアクセス



提供される機能

1. クライアント証明書発行（PKCS#12形式）
2. S/MIME証明書発行（PKCS#12形式）
3. UPKIパス用証明書発行（開発中）
4. ネットワーク認証用証明書発行（PKCS#12形式）
 - ▶ 3と4は無効化可能
 - ▶ 3と4は一方のみ有効化可能

管理者画面

ファイル(E) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(I) ヘルプ(H)

国立情報学研究所 電子証明書E x +

← → 国立情報学研究所 電子証明書E x (JP) ... ☆ ↺ ↓

情報・システム研究機構
国立情報学研究所
National Institute of Informatics

国立情報学研究所 電子証明書自動発行支援システム

ログアウト

●クライアント証明書 発行・更新・失効 証明書情報一括ダウンロード ●利用管理者情報 更新 全証明書情報一括ダウンロード 発行証明書統計照会  クリックして 証明書の内容を ご確認ください。	●クライアント証明書 発行・更新・失効画面 クライアント証明書申請ファイルをアップロードして下さい。 処理内容を選択してください ▼ 処理中にエラーが発生した場合 ☒ 全件処理を中断する ☐ 入力値不備のないデータのみ登録する 参照... ファイルが選択されていません。 アップロード
---	--



利用者画面（ログイン直後）

学認連携: クライアント証明...

ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(I) ヘルプ(H)

学認連携: クライアント証明書発行申請システム [English|Japanese] ユーザー test001_displayname アカウントメニュー▼

クライアント証明書発行申請ダッシュボード

このページではクライアント証明書の発行申請・管理が行えます。本システムは国立情報学研究所(NII)のUPKI電子証明書発行サービスを利用しています。また利用には学認のアカウントが必要です。

クライアント証明書とは、PC・タブレット・スマートフォンなどのコンピュータにインストールして電子的な本人確認ができるようにするデジタル証明書です。

証明書の種類を選択して申請

- 認証用 クライアント証明書
クライアント証明書を申請
- メール暗号化/署名用 S/MIME証明書
S/MIME証明書を申請

証明書の発行状況（申請番号をクリックで詳細表示）

申請番号	証明書の種類	申請日	申請状況	メモ
画面更新				



利用者画面（発行申請）

The screenshot shows a web browser window with the URL https://g-cert-dev.gakunin.nii.ac.jp/ja/certs/request_result/1. The browser's address bar and tabs are visible. The page header includes the text "学認連携: クライアント証明書発行申請システム" (Academic Cooperation: Client Certificate Issuance Application System), a language selector "[English|Japanese]", a user identifier "ユーザー test001_displayname", and an "アカウントメニュー" (Account Menu) dropdown.

申請完了

UPKIクライアント証明書の発行申請を行いました。

5分程度で、証明書の利用に必要な **PIN (Personal Identification Number)** を本システムで確認できるようになります。
また、CAサポートセンター <ca-support@ml.secom-sts.co.jp> から、あなたのメールアドレス <test001_email@nii.ac.jp> 宛てに、
証明書ダウンロード用URLが記載されたメールが届きます。
本システムで **PIN** を確認のうえ、メールに記載されたURLにアクセスして、証明書をダウンロードして下さい。
ダウンロードした証明書をシステムに登録する際にパスフレーズの入力を求められるので、同じ **PIN** を入力して下さい。

PINは発行完了後の一定期間、本ポータル of 証明書情報確認画面で確認できます。

また、下記URLから、中間CA証明書もダウンロードしてシステムにインストールして下さい。
<https://nii-odca3sha2.cer>

[証明書情報確認](#)



利用者画面（発行申請直後）

ブラウザのアドレスバー: <https://g-cert-dev.gakunin.nii.ac.jp/ja/certs/1>

学認連携: クライアント証明書発行申請システム [English|Japanese] ユーザー Naoto Miyachi アカウントメニュー▼

証明書の詳細

申請番号	1
証明書タイプ	クライアント証明書
申請状況	新規申請中
証明書の状態	申請中
PIN番号	まだPIN番号は発行されていません。申請完了メール送信までお待ちください。
メール送信	m[redacted]@nii.ac.jp (受付通知メール送信待ち)
申請日時	2018/03/26 21:08:56
シリアル番号	未発行
DN(識別名)	CN=1 [redacted], OU=No 1, OU=dev05, OU=UPKI Client Cert Enrollment System Develop, O=National Institute of Informatics, L=Academe, C=JP
用途メモ	(例)ノートPCの接続用 メモを保存
失効操作	失効

[ダッシュボードページに戻る](#) / [画面更新](#)



利用者画面（証明書未取得）

ブラウザのアドレスバー: <https://g-cert-dev.gakunin.nii.ac.jp/ja/certs/1>

学認連携: クライアント証明書発行申請システム [English|Japanese] ユーザー Naoto Miyachi アカウントメニュー▼

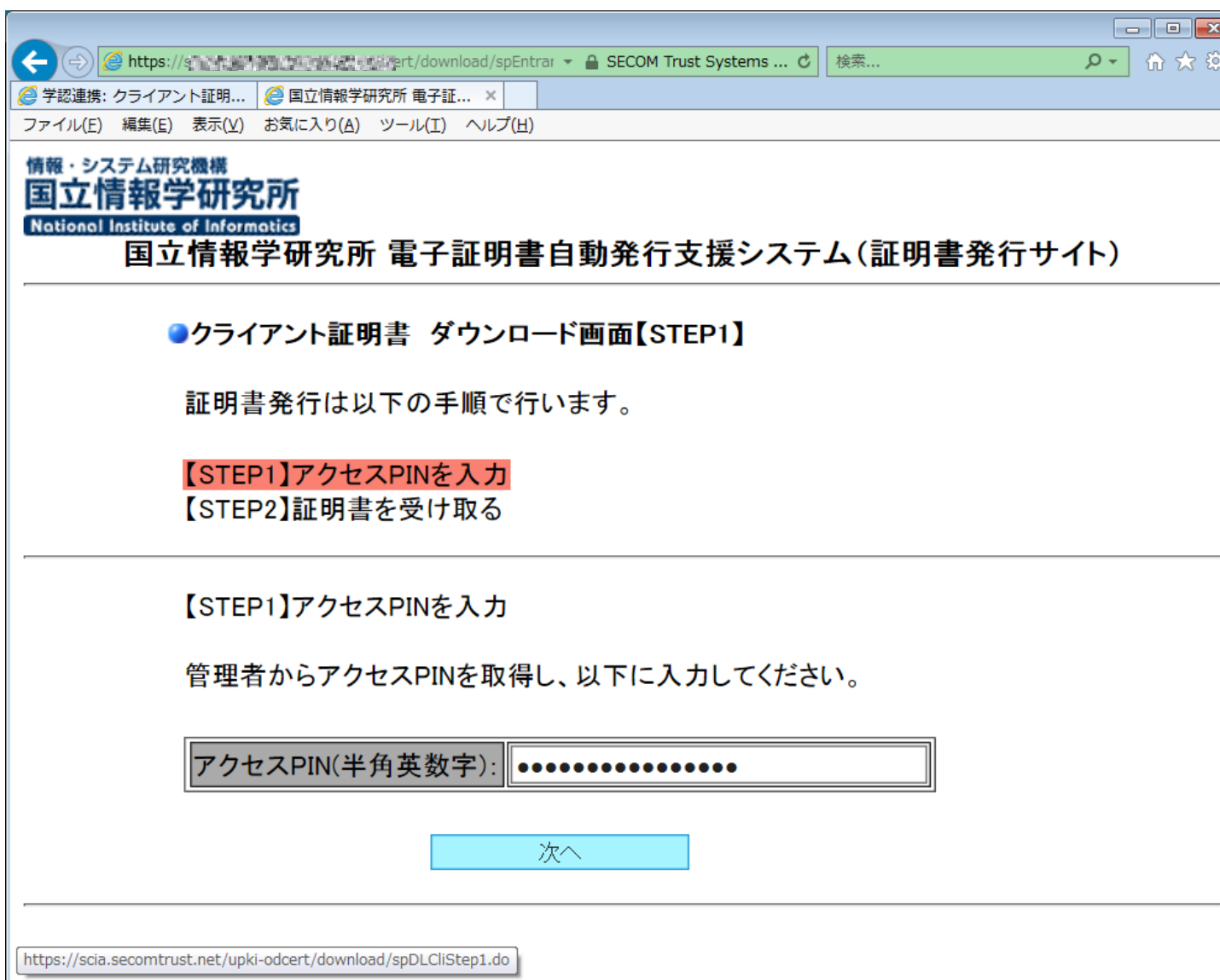
証明書の詳細

申請番号	1
証明書タイプ	クライアント証明書
申請状況	新規申請PIN取得済
証明書の状態	有効
PIN番号	XXGYjZkumwNMpvQ4
メール送信	m[redacted]@nii.ac.jp (受付通知メール送信済み)
申請日時	2018/03/26 21:08:56
シリアル番号	未発行
DN(識別名)	CN=1[redacted],OU=No 1,OU=dev05,OU=UPKI Client Cert Enrollment System Develop,O=National Institute of Informatics,L=Academe,C=JP
用途メモ	(例)ノートPCの接続用 メモを保存
失効操作	失効

[ダッシュボードページに戻る](#) / [画面更新](#)



証明書取得画面



情報・システム研究機構
国立情報学研究所
National Institute of Informatics

国立情報学研究所 電子証明書自動発行支援システム(証明書発行サイト)

●クライアント証明書 ダウンロード画面【STEP1】

証明書発行は以下の手順で行います。

【STEP1】アクセスPINを入力
【STEP2】証明書を受け取る

【STEP1】アクセスPINを入力

管理者からアクセスPINを取得し、以下に入力してください。

アクセスPIN(半角英数字):

次へ

<https://scia.secomtrust.net/upki-odcert/download/spDLCLiStep1.do>



利用者画面（証明書取得後）

学認連携: クライアント証明書発行申請システム

証明書の詳細

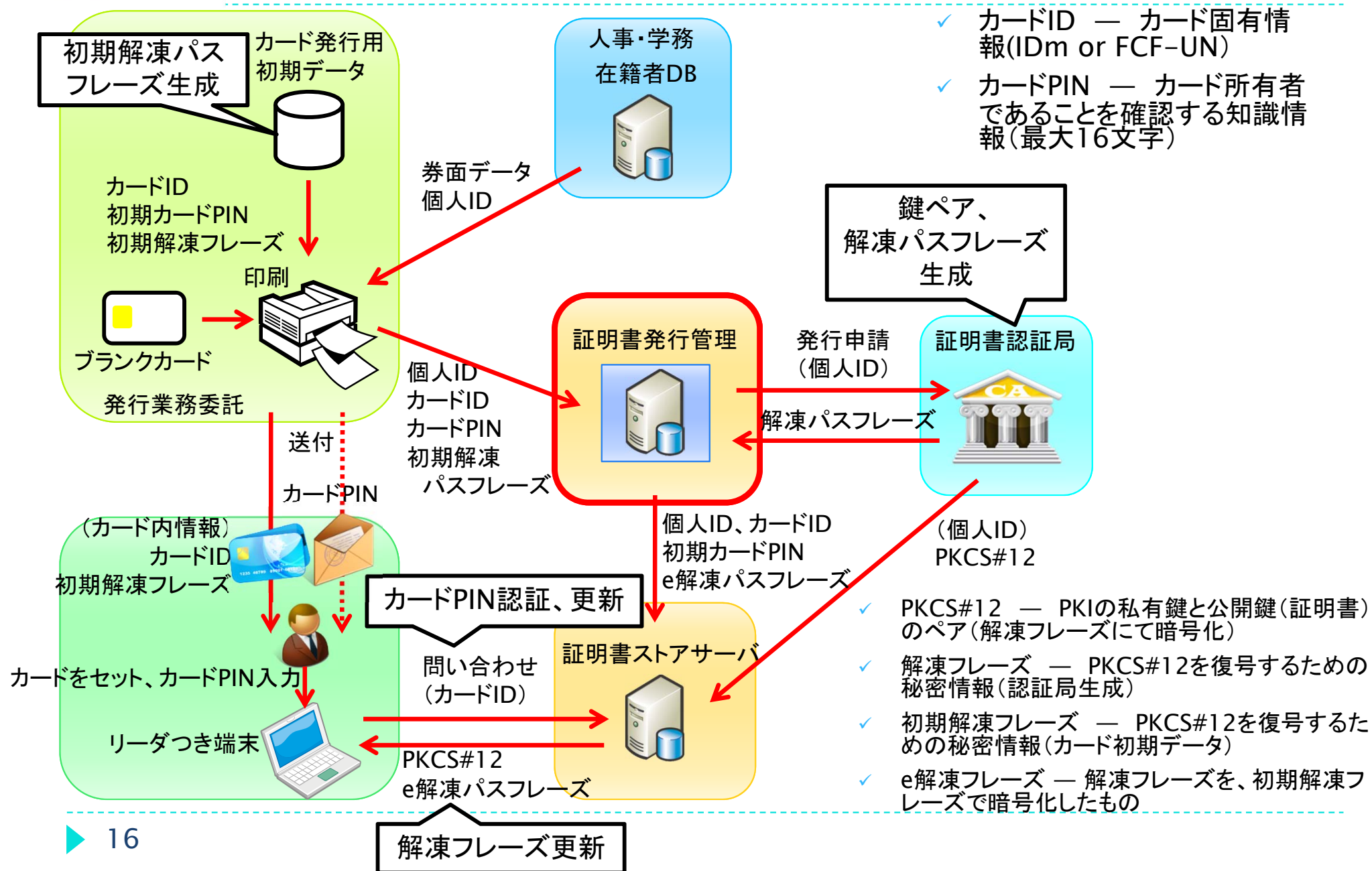
申請番号	1
証明書タイプ	クライアント証明書
申請状況	有効
証明書の状態	有効
PIN番号	XXGYjZkumwNMpvQ4
メール送信	.jp (受付通知メール送信済み)
申請日時	2018/03/26 21:08:56
シリアル番号	7082414538221694988
DN(識別名)	CN=, OU=No 1, OU=dev05, OU=UPKI Client Cert Enrollment System Develop, O=National Institute of Informatics, L=Academe, C=JP
用途メモ	(例)ノートPCの接続用 メモを保存
失効操作	失効

[ダッシュボードページに戻る](#) / [画面更新](#)



UPKIパスへの対応

- ▶ UPKIパスについては、オープンフォーラム2016の資料を参照
- ▶ https://www.nii.ac.jp/csi/openforum2016/track/pdf/20160526PM_G_08_matsuhira.pdf



UPKIパスのメリット

- ▶ 学生証や職員証として広く利用されているFCFが使える
 - ▶ 100万枚発行済。但し、FCF V3が必要
 - ▶ 身分証を利用することで、紛失や貸し借りの問題が減る
- ▶ フェリカの他のアプリと共存しやすい
 - ▶ 証明書を格納するための大きな領域が不要
 - ▶ 複数の証明書（6枚）と紐付けた運用が可能
- ▶ 証明書配布のために、PKCS#12や解凍フレーズを開示して各自でインストールさせる必要がない
 - ▶ 一般的なリーダー（パソリ等）が利用可能
 - ▶ 共有PCでもクライアント証明書が利用可能
 - ▶ PKCS#11 APIにも対応
- ▶ 証明書の更新がサーバ側のみで可能（有効期限が短くても可）
 - ▶ CAでのCRLによる失効とは別に、証明書ストアサーバ上での迅速な無効化が可能（CRL更新を待つ必要がない）



今後の課題

- ▶ 続・UPKIパスへの対応
 - ▶ FCFカード情報とのひもづけ
 - ▶ 証明書ストアサーバとの連携
- ▶ 汎用性の向上
 - ▶ UPKIのサービス変更・拡張への対応
 - ▶ 共通APIの策定？