UPKIパスについて

2016/5/26

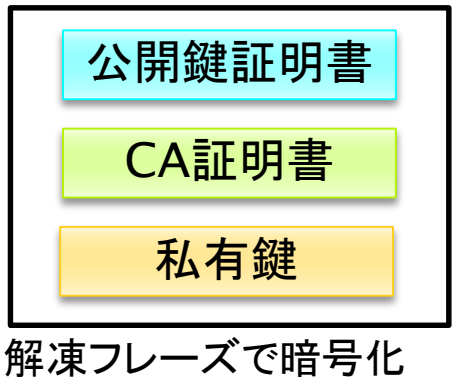
中村素典 / 国立情報学研究所

クライアント証明書の活用

- 用途
  - 認証、署名、暗号化
    - 証明書にメールアドレスの記載なし
  - 電子メール（S/MIME）
    - 証明書にメールアドレスを記載
- 形態
  - 端末にインストール
  - ICカード（Type B等）、USBトークン、SIMカード等に格納
    - 耐タンパ性のあるものを用いることによる安全性
      - ユーザに直接扱わせる必要がない
  - FCF（FeliCa）等と連携
    - **JCANパス方式（前項のICカードに近い使い勝手）に基づくUPKIパス方式**

JCANパス方式とは

- JCAN (Japan CA Network)
  - 一般財団法人日本情報経済社会推進協会（JIPDEC）による統一仕様パブリッククライアント証明書普及プロジェクト（2009～）
- JCAN証明書
  - 共通仕様（CNやOU2）に基づくパブリックなクライアント証明書
  - JIPDECがCA、LRAを認定
- JCANパス（カード）
  - JCAN証明書（PKCS#12フォーマット）を利用するために、PKCS#12の解凍フレーズを暗号化して書き込んだFCF Version 3規格のICカード（フェリカ）
  - FCF V2のC4領域と、V3のD1領域を利用
- JCANパス方式
  - JCANパスを利用して、利用する時だけ、PKCS#12に格納された私有鍵＋公開鍵証明書を一時的に証明書ストアにインストールして利用可能な状態にする方式
  - スタンドアロン（ローカルファイル）型とサーバ型がある



FCF Version 3

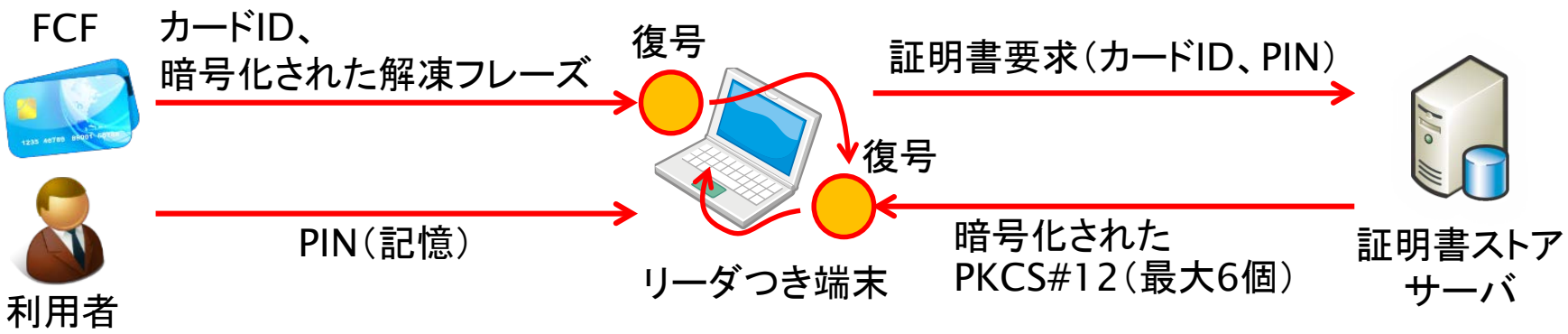
- 2013/11公開
- V2からV3へのバージョンアップには再発行が必要

	エリア	用途	読出鍵	書込鍵	ブロック数
	システム	製造ID (IDm)			4
	A	基本ID情報	なし	あり	8
New!	N	FCF-UN	なし・あり	あり	6
	B	追加サービス履歴	あり	あり	10
	C1	追加サービス	あり	あり	7
	C2	追加サービス	あり	あり	7
	C3	追加サービス	あり	あり	13
	C4	追加サービス	なし・あり	あり	7
New!	D1	追加サービス	なし・あり	なし	16

FCFサービスコード
“UPKIパス”

解凍フレーズ×6

UPKIパスの動作概要



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（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
  - *New!* 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）

JCANパスのデメリット

- サーバにアクセスできる環境が必要
  - ログイン認証、ネットワークアクセス認証には使いづらい
- サーバの厳格な運用管理が求められる（鍵の漏洩対策）
  - 脆弱性診断は必須
- 端末にリーダとソフトウェアのインストールが必要

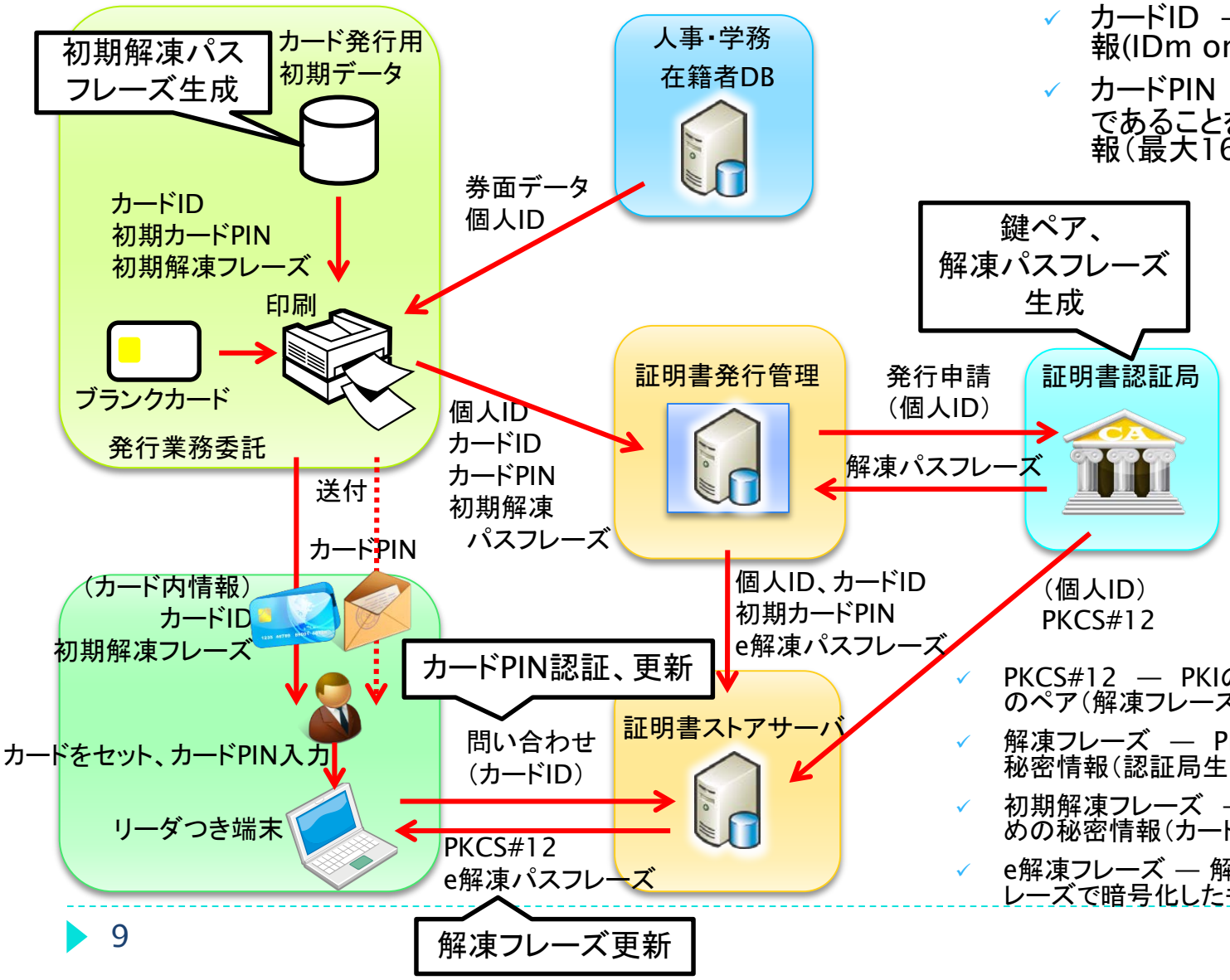
JCANパスの改善 ― 「UPKIパス」

1. カードPINはカードに保存せず、証明書ストアサーバのアクセス認証に利用
   - 外出時に（インターネットから）利用できない

2. UPKI証明書の証明書発行方式に対応
   - PKCS#12の発行時に解凍フレーズが事前指定できない
   - 同時に利用可能な証明書の数の最大は6

3. 端末の証明書ストアに一時的に書き込まず、暗号トークンインタフェース（PKCS#11）等を利用
   - 鍵を容易にエクスポートできないように

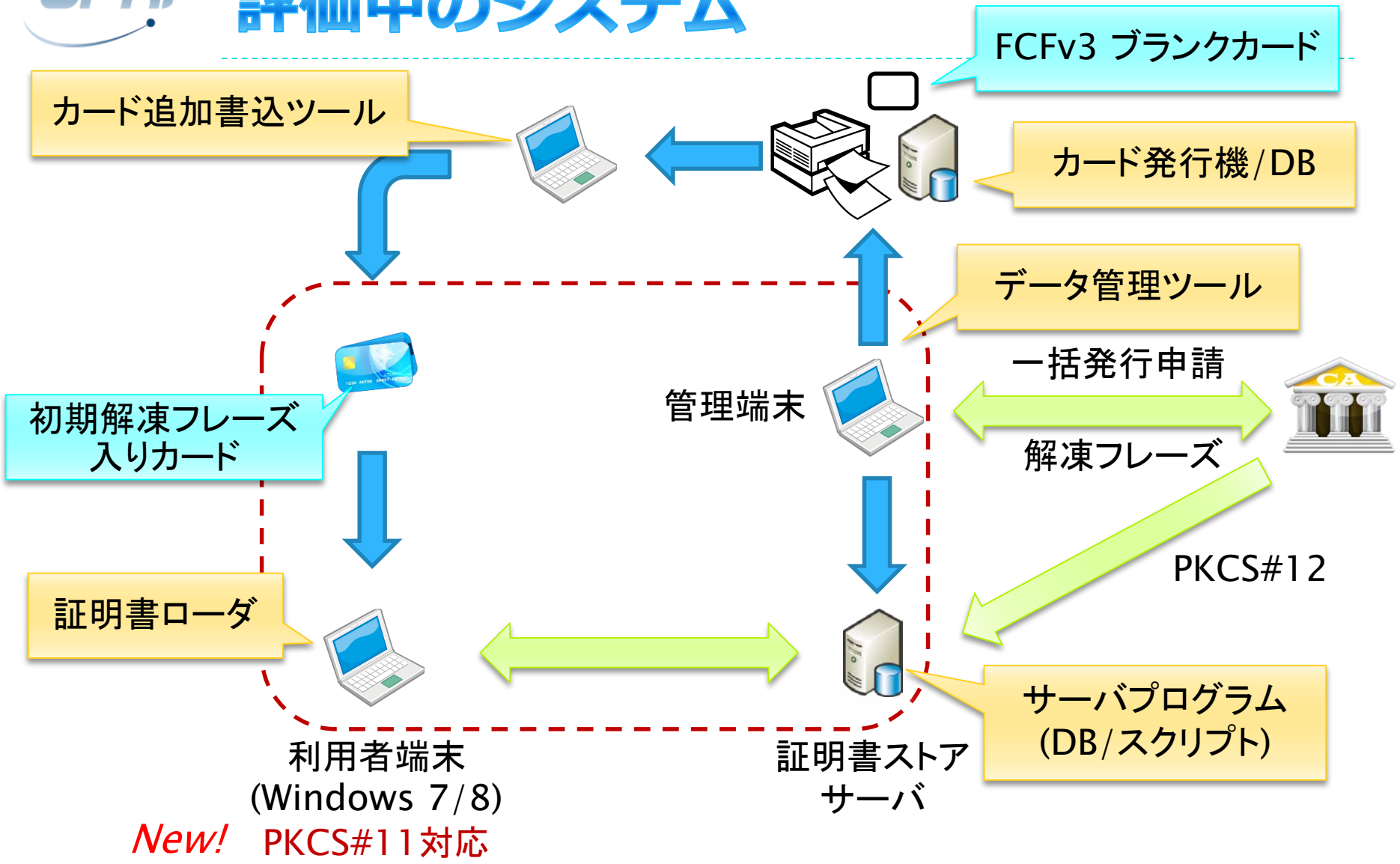
UPKIパス方式



- ✓ カードID — カード固有情報(IDm or FCF-UN)
- ✓ カードPIN — カード所有者であることを確認する知識情報(最大16文字)

- ✓ PKCS#12 — PKIの私有鍵と公開鍵(証明書)のペア(解凍フレーズにて暗号化)
- ✓ 解凍フレーズ — PKCS#12を復号するための秘密情報(認証局生成)
- ✓ 初期解凍フレーズ — PKCS#12を復号するための秘密情報(カード初期データ)
- ✓ e解凍フレーズ — 解凍フレーズを、初期解凍フレーズで暗号化したもの

評価中のシステム



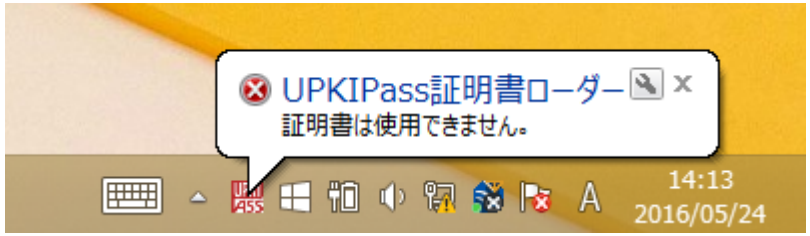
New! PKCS#11対応

評価環境


Panasonic CF-AX2
Let's note
Ultrabook
Shiodome University
学生証
坂上　登志男
SONY

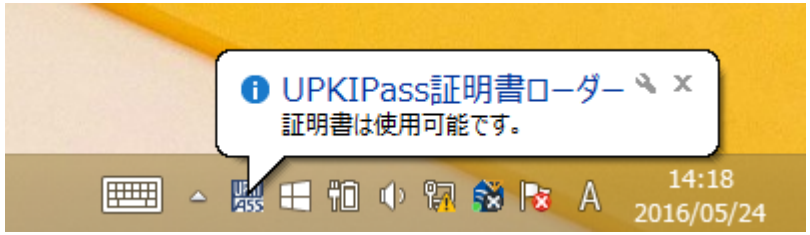
画面表示

- カードなし

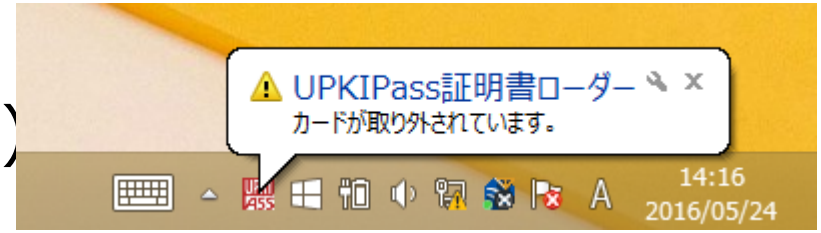


- カードをかざしただけ

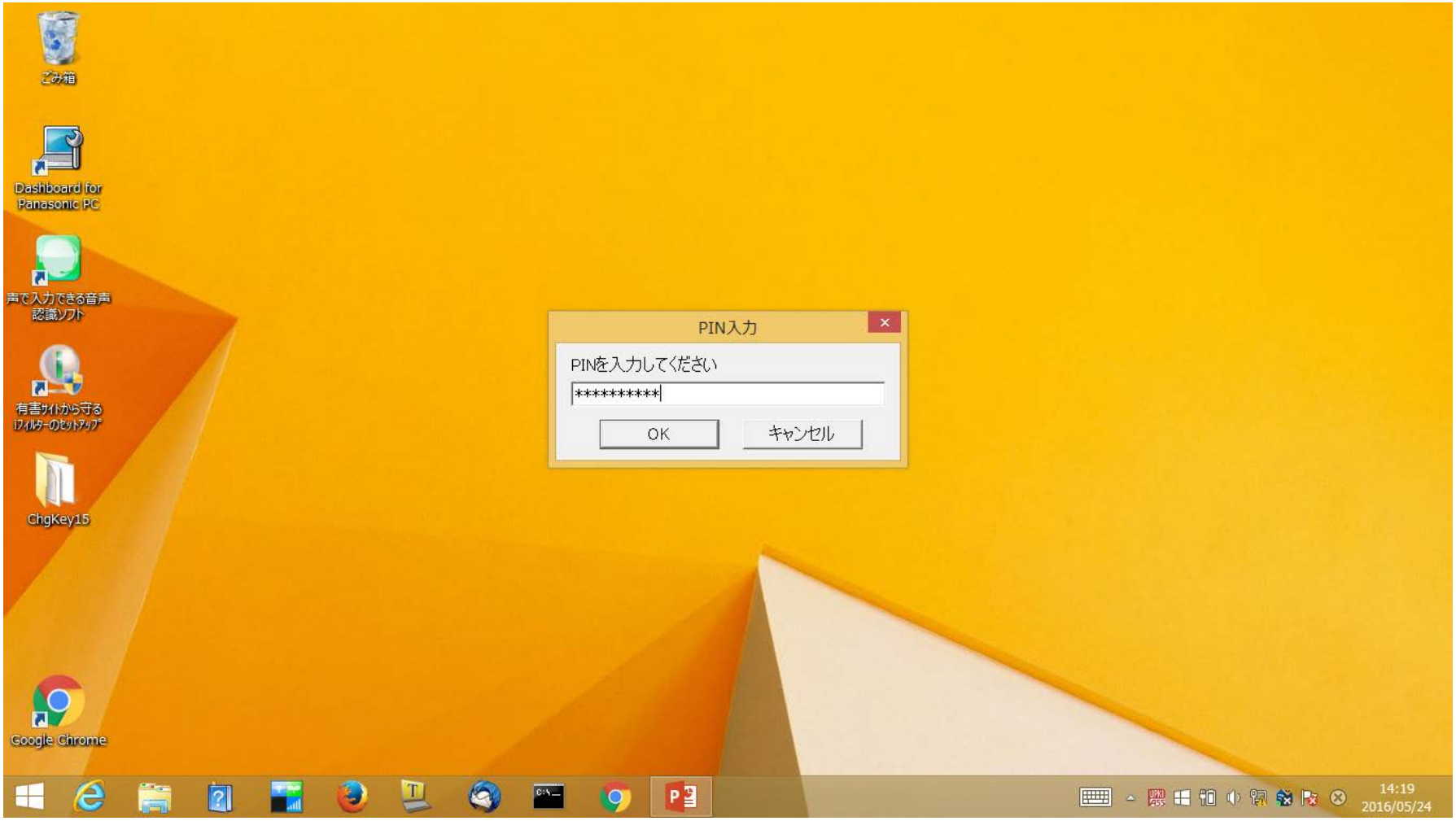
- PIN入力完了



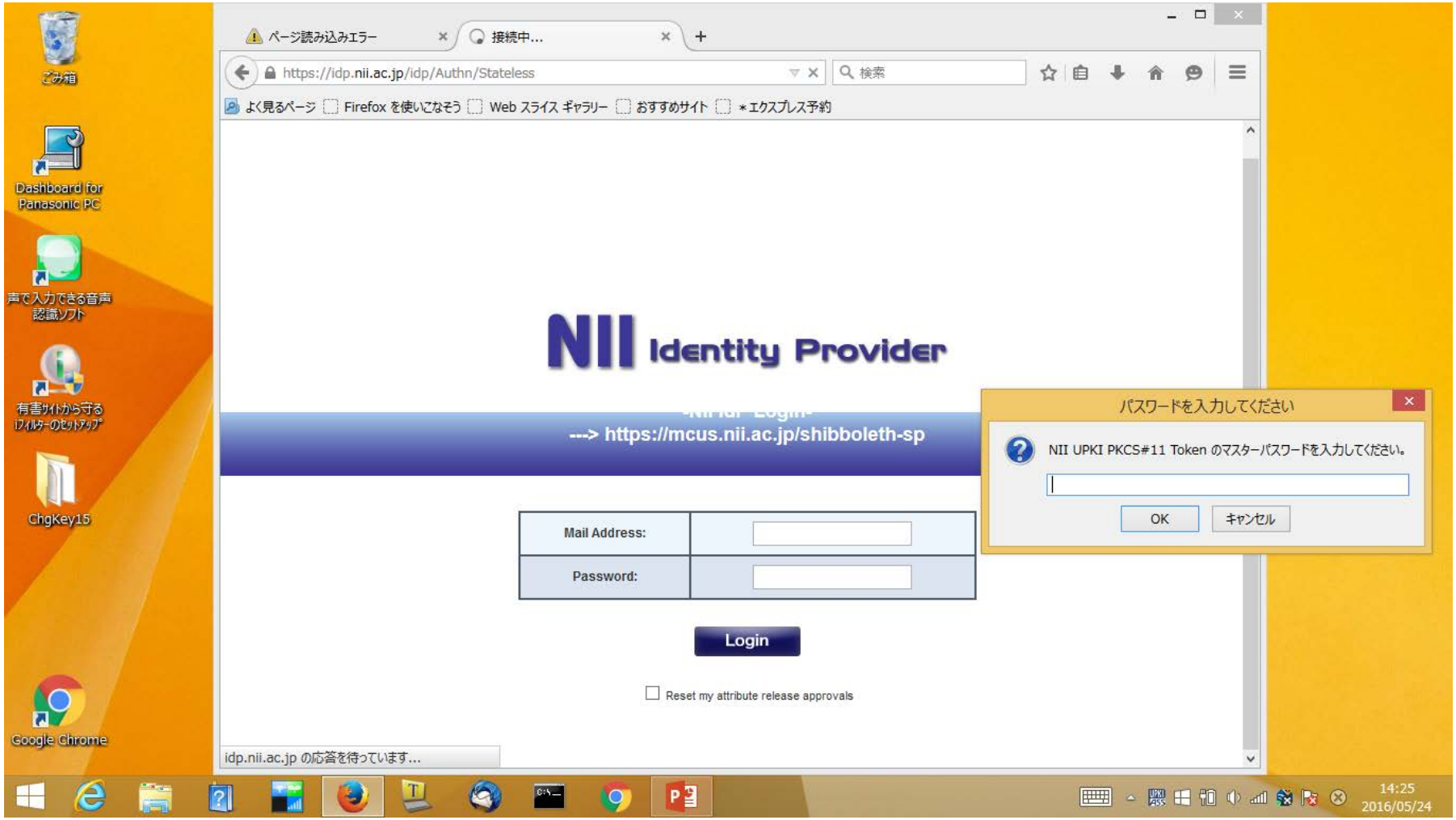
- カードをとる
  （すぐに戻せば継続利用可）



PIN入力画面


ごみ箱
Dashboard for Panasonic PC
声で入力できる音声認識ソフト
有害サイトから守るフィルターのセットアップ
ChgKey15
Google Chrome
PIN入力
PINを入力してください
****
OK
キャンセル
14:19
2016/05/24

PKCS#11経由のアクセス



導入に向けての検討

- カードの発行処理
  - カード事業者にどこまで委託するか
    - ブランクカード作成まで（券面印刷は全て大学）
    - 券面印刷まで（再発行時の券面印刷は大学？）
    - 郵送まで（入学手続き等との連携）
- カードと証明書の紐付け
  - TSVに記載する「利用者氏名」欄を利用
    - フォーマット：「識別子　氏名」（半角スペース区切り）
    - 証明書には含まれない情報
    - 一括発行フォーマットから自動抽出
- 「証明書発行管理システム」の構築
  - 大学のID管理システム（大学ごとに異なる）との連携
    - 証明書自動発行の仕組みの構築・連携も課題
  - 今のところ、簡易管理システムを提供

UPKIパス仕様の詳細について

- FCF V3上のデータフォーマット詳細
  - FCF推進フォーラム会員に対して、別途NDAの元で開示
- クライアント
  - Windows版（PKCS#11対応）
  - Mac版（PKCS#11非対応）
    - 高見沢サイバネティックス/高見沢ソリューションズ（以下、高見沢）が開発・提供
    - FCF推進フォーラム会員であれば開発可能
- サーバ
  - クライアント・サーバ間プロトコルは開示可
    - Windows版スタンドアロンサーバ（簡易管理システム）を高見沢が開発・提供
    - キャンパスID管理システムと連携したシステムの構築が望ましい

UPKIパス：まとめ

- 証明書ストアサーバとFeliCa連携による、クライアント証明書の活用
  - 毎回、証明書ストアサーバから私有鍵と公開鍵証明書を取得し、 Felicaカード上のキーで復号して利用する方式
- 特徴
  - FeliCaカード（FCF Version 3）を利用
  - 証明書をサーバに保持しカードに保存しないため、証明書の更新処理、利用停止処理が容易
    - 証明書の有効期限がカードの有効期限より短くても良い
  - 証明書をユーザに直接扱わせる必要がない等、セキュリティが向上
    - TypeB/Javaカード等の安全性には劣るが、クライアント証明書普及の一助になると期待
  - PKCS#11にも対応
- 今後の課題
  - NFC対応スマートフォン等でも利用できるようにしたい
  - CAPIへの対応