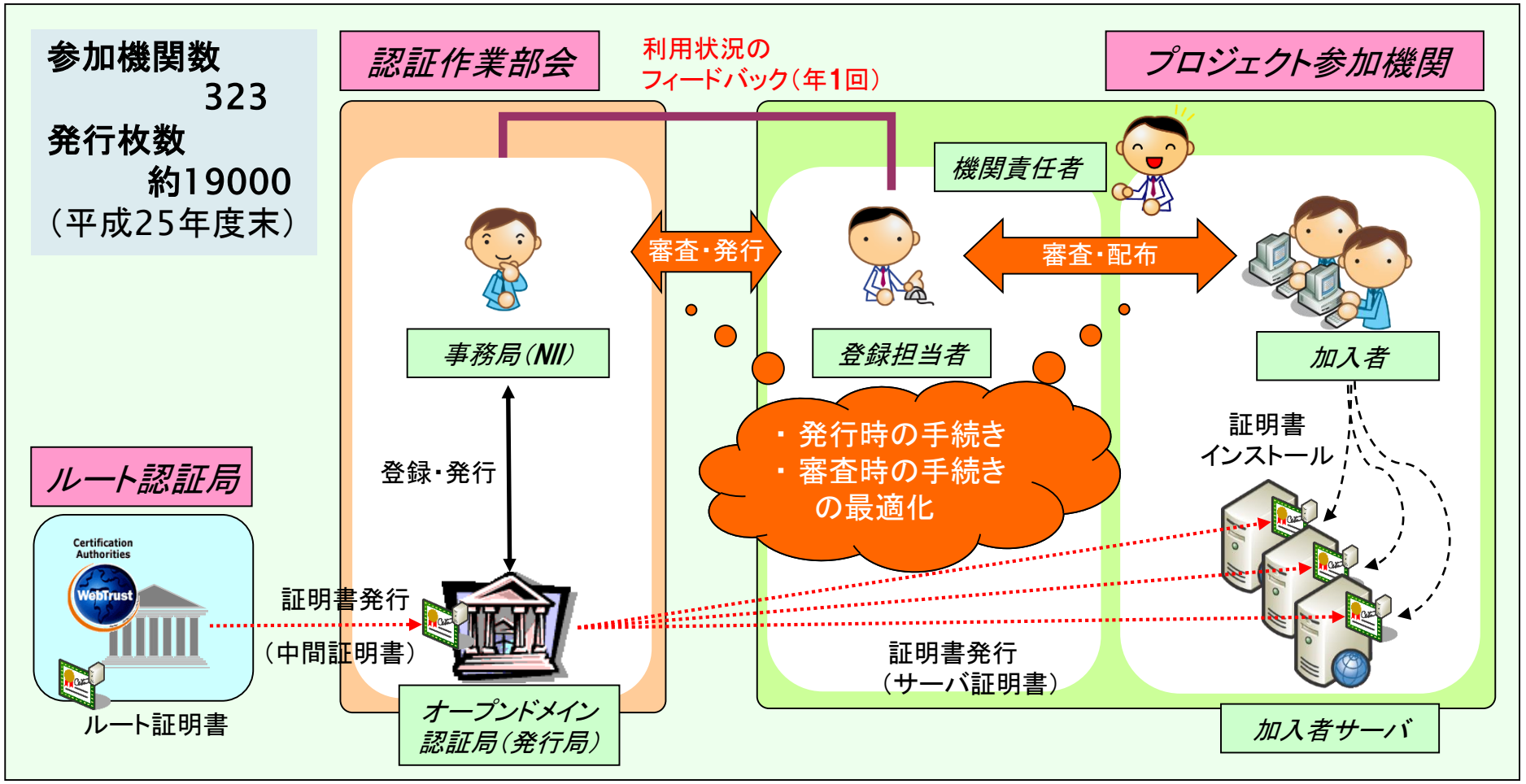
次期証明書発行サービスの詳細仕様と価格体系

2014-05-29

国立情報学研究所 学術基盤推進部 学術基盤課 認証担当

サーバ証明書の大学向け発行サービス

- 学術スキームに基づくUPKIオープンドメイン証明書



学術スキームとは

- 通常は商用認証局が行う証明書発行のための審査等を，NIIや大学で分担して行うことで、信頼性を高めつつ、業務の効率化やコスト削減を実現する方法

（NIIや大学は必要に応じて商用のルート認証局から監査を受ける）

			商用認証局				学術スキーム			
			DV		OV/EV		機関審査		発行審査	
			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
①	組織	本人性	×		○		○			
②		実在性	×		○		○			
③	ドメイン	本人性	○		○		● →	○		
④		実在性	○		○		● →	→	○	
⑤	機関責任者	本人性					○			
⑥		実在性					○			
⑦	登録担当者	本人性						○		
⑧		実在性						○		
⑨	加入者	本人性	×		○		● →	→	○	
⑩		実在性	×		○		● →	→	○	
⑪	加入者サーバ	本人性		○		○				○
⑫		実在性		○		○			○ ←	●

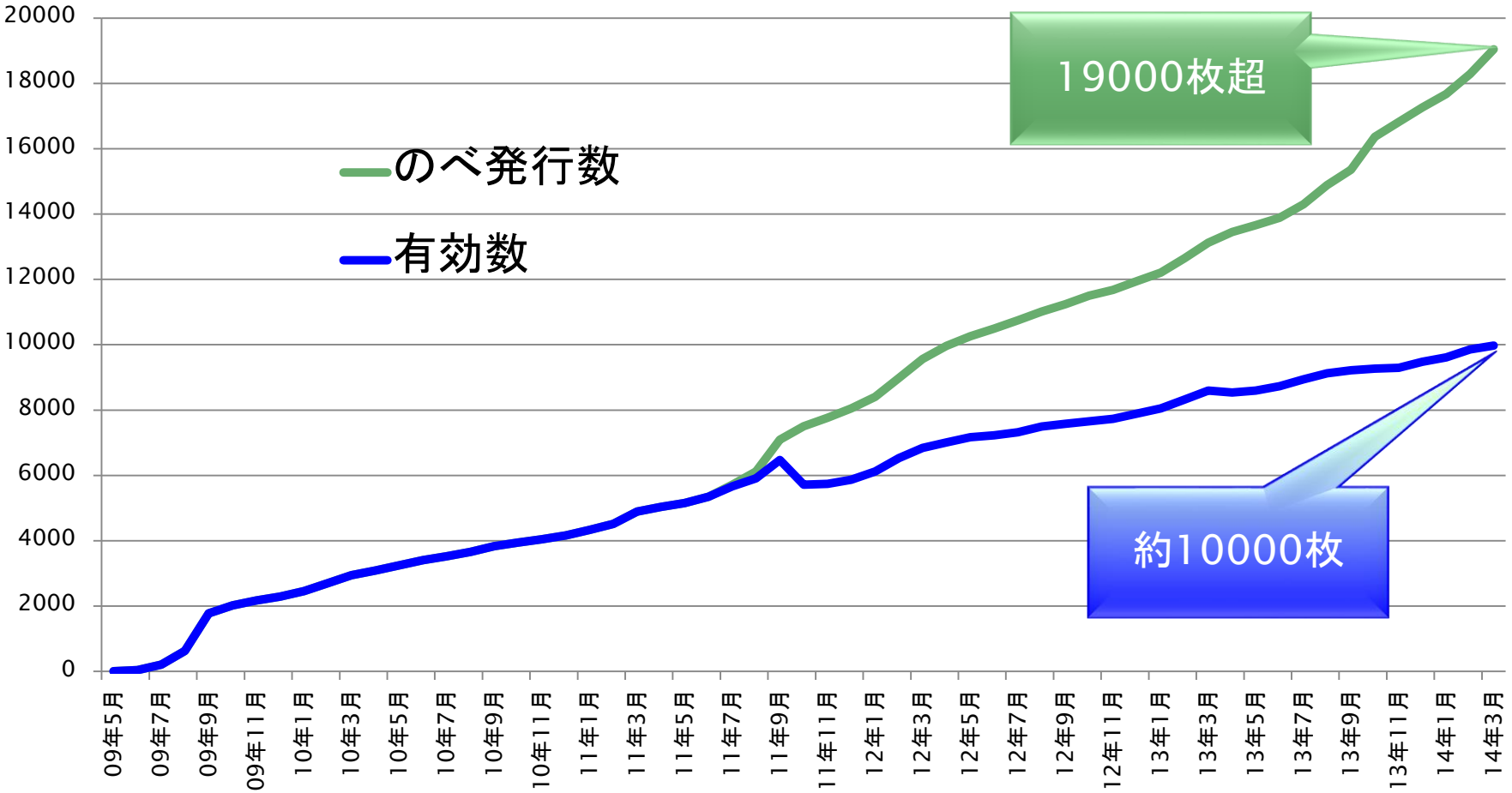
業務の委任（→）により効率化

これまでの活動

- サーバ証明書発行・導入のための啓発・評価研究プロジェクト（第一期プロジェクト）
  - 平成１９年４月２日～平成２１年６月３１日
  - 参加機関数97機関　のべ発行枚数2,413枚
- UPKIオープンドメイン証明書自動発行検証プロジェクト（第二期プロジェクト）
  - 平成２１年４月１日～平成２４年３月３１日
  - 参加機関数276機関　のべ発行枚数9,561枚
- UPKIオープンドメイン証明書自動発行検証プロジェクト延長（第二期プロジェクト2）
  - 平成２４年４月１日～平成２７年３月３１日
  - 参加機関数323機関　のべ発行枚数19,009枚（平成25年度末時点）

- ✓ 大学等のドメインに対するOV証明書を無償にて発行
- ✓ 証明書の有効期限:25ヶ月

のべ発行数と有効数（第二期プロジェクト）



経済効果

- 例：第二期プロジェクト(前半）：３年間の総額

有効期間2年の証明書を9,561枚購入した場合の経費：1,104,295,500円
＝本プロジェクトの委託経費　　：　36,225,000円
　＋バルク契約による削減経費　　：530,635,500円
　＋学術スキーム導入による削減経費　　：537,435,000円

セコムパスポートfor Web SR2.0の購入経費年額57,750円として計算
30枚以上購入時には30,000円となるため，差額27,750円からバルク契約の削減経費を計算

- 学術スキーム導入による経費削減効果は，約1.8億円/年

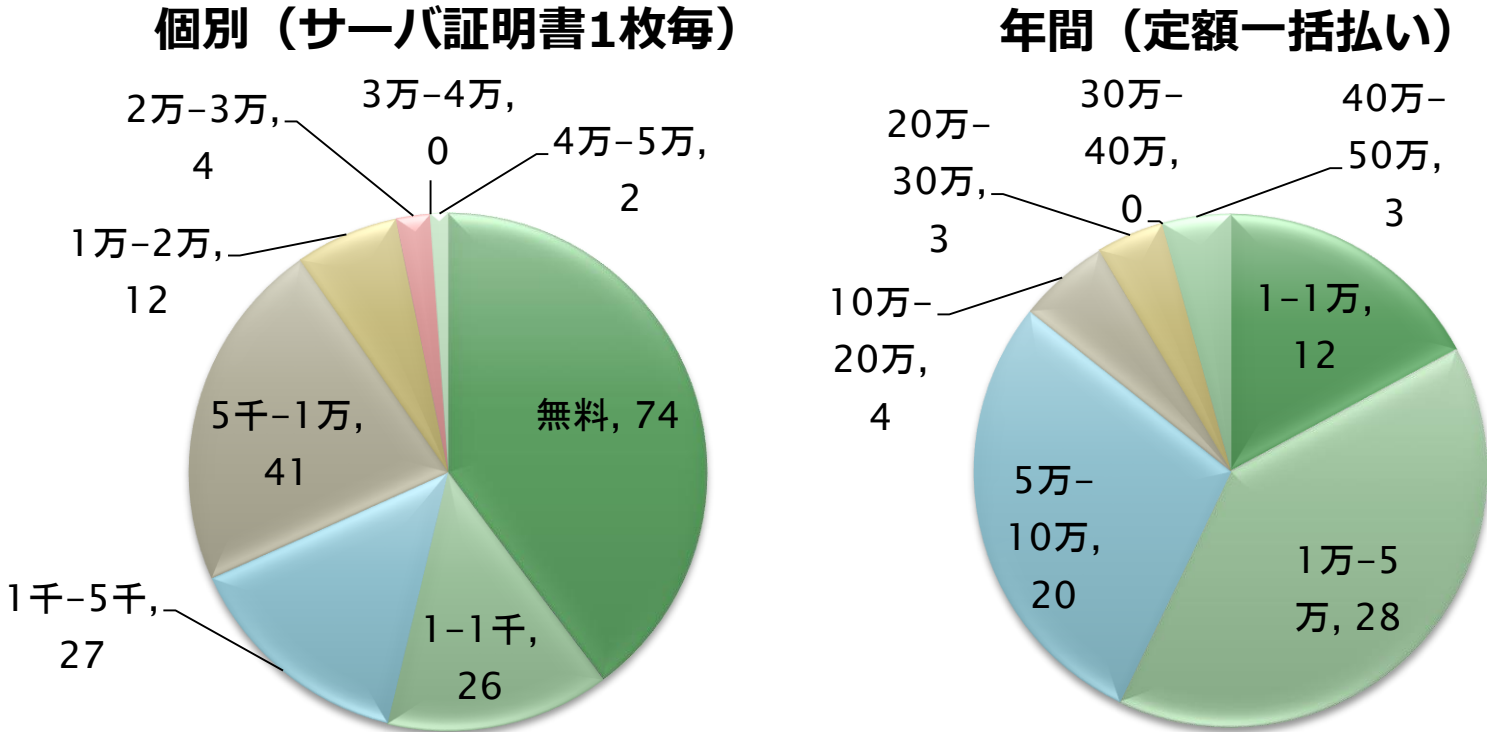
サービスの継続についての検討

- 大学視点
  - 大学のインフラの一部として定着
    - 大学サービスのセキュリティ・信頼性を担保
  - サービス継続への強い希望
    - 有料化となったとしてもサービスの継続を希望
  - 学内CAを構築するのと同等の利便性

- NII視点
  - 大学サービスのトラストアンカーとしてNIIが機能
    - ドメインと機関の関係を保証し，大学サービスの信頼性の礎となる証明書発行サービスをNIIが提供することの意義
  - 学術スキームにおけるNIIの役割
    - NIIが主体となり継続する必要性（商用サービスでは実現不可）
    - 学術全体としての安全性・信頼性とブランド力の向上

大学からのニーズ

- 本サービスが有料化される場合、いくらまでならば支払うことができますか？



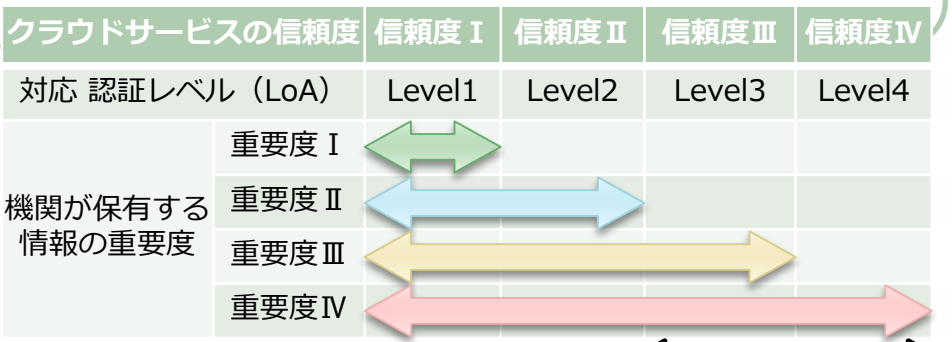
有料化となってもサービスの継続利用を希望

サービス拡張に対する期待

- サーバ証明書

  - 従来のOV（Organization Validation）証明書だけでなく，より信頼性のレベルの高いEV（Extended Validation）発行への期待
- クライアント証明書
  - 現在各大学で個別に購入 or 独自に発行しているクライアント証明書発行への期待

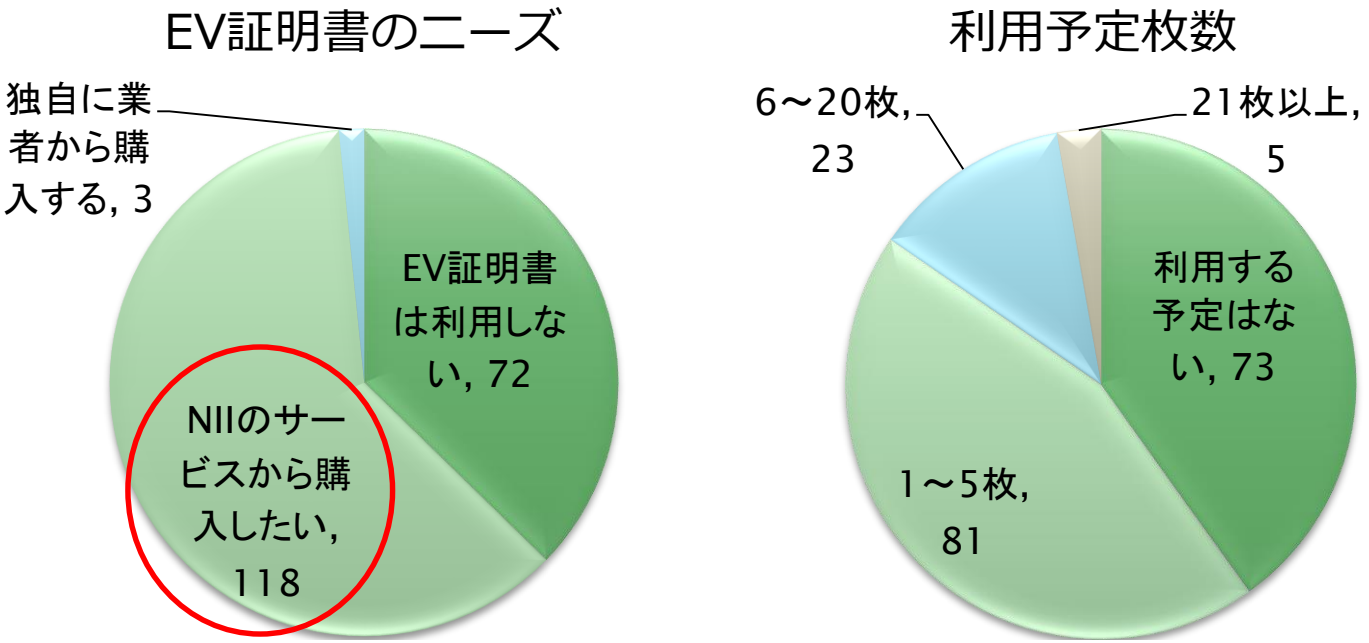
学認の普及も後押し



- 学内統合認証基盤の普及
  - 機微な情報を含む学内の多くのサービスに接続
- ID/Password認証の限界
  - クライアント証明書等を使ったセキュアな認証方法の必要性

大学からのニーズ

- 現行のOV証明書だけでなく，EV証明書の利用ニーズはありますか？



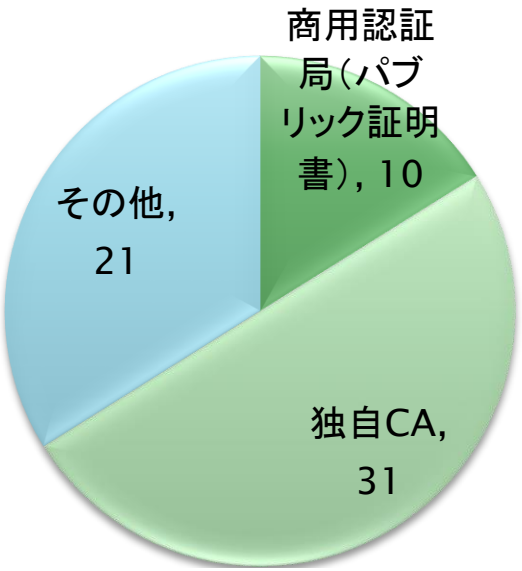
参考：シマンテック　セキュア・サーバID EV　170,100円／年
セコムパスポート for Web EV　141,750円／年

より高い信頼性を証明するEV証明書発行の期待

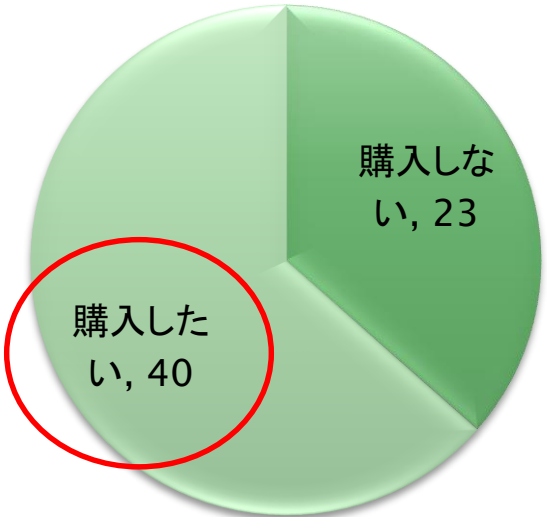
大学からのニーズ

- クライアント証明書の利用ニーズはありますか？

現在利用している証明書の発行元



NIIからの購入希望



参考：京都大学　独自CAの運用コスト，初期導入約6000万，運用900万円／年
JIPDEC　JCAN証明書　80,000円＋(1,050円)*人／年

クライアント証明書の発行サービスに対する期待

サービス拡張に対する期待

- コードサイニング証明書
  - 大学ICT環境の高セキュリティ化要請への対応
  - プログラム等に署名することで、利用者が警告を無視することなく利用可能
    - 大学が提供するサービス、研究成果等の公開・配布

- コードサイニング証明書とは
  - Webサーバ等で提供されるプログラムやドキュメントに署名
    - Java、Flash、ActiveX、MS Office BVA、実行ファイル(.exe)、Androidアプリ、PDFなど
  - 各機関のプログラム開発者やドキュメント管理者に対して証明書を発行
  - 署名ツールを利用してプログラムに署名
    - 署名の正当性を、OS、ブラウザ、ウイルス対策ソフト等が検証してから実行
    - 署名を行ったコードサイニング証明書の有効期限内であれば、付与された署名が有効
    - 事業者が発行するタイムスタンプ（無料）を含めれば、コードサイニング証明書の有効期限に関係なく５～２０年程度有効（各タイムスタンプサーバの署名の有効期限内）

海外の動向

- 米国：InCommon Certificate Service
  - 学術スキームと同等の委任手続きを採用
  - OV, EV，クライアント，コードサイニング証明書を発行
  - 267機関が参加（ 2013年11月18日現在）
  - 有償サービス
    - 研究大学：$20K/year, 小規模大：$3K/year
    - 個別購入の1/4～1/5程度の価格で提供
- 欧州：TERENA Certificate Service
  - 学術スキームと同等の委任手続きを採用
  - OV, EV，クライアント，e-Science，コードサイニング証明書を発行
  - 欧州の29国のNRENが参加（ 2013年11月18日現在）
    - 合計発行枚数：80,870枚
  - 有償サービス
    - NREN毎の定額制（さらに各国NRENで独自の料金徴収モデルをもつ）
    - EV証明書は＄150/year/枚

UPKI証明書発行サービス

- NIIサービスとして事業化
  （普及啓蒙、学術スキームの構築から，さらに次のステップへ）
- 従来のOV証明書に加えて，EV証明書，
  クライアント証明書，コードサイン証明も発行
- 発行ドメインの制約緩和
- 各機関の負担コストを抑えつつ継続運用するための
  独立採算を目指した有償化
- クライアント証明書，コードサイン証明書は
  普及啓蒙フェーズとしてサービス開始

有料化の基本方針

- 機関の規模に応じた定額制
  - OV，クライアント，コードサイン証明書の発行枚数無制限
- OV証明書
  - 購入しやすい価格 → 学校の規模ごとに段階的に設定
  - ドメイン単位に課金（発行ドメインの制約緩和）
    - 追加ドメインの料金は小規模大学のオリジナルドメイン程度
    - 発行対象機関は従来どおり高等教育・研究機関等
- EV証明書は1枚ごとに別途課金
  - サービス開始時期については検討中
- クライアント証明書，コードサイン証明書は当面無料
  - 普及啓蒙フェーズ

サーバ証明書の差異—EV, OV, DV

- EV (Extended Validation)
- OV (Organization Validation)
- DV (Domain Validated)

	UPKI	組織実在審査	費用	審査レベル	信頼度
EV	○	あり	別※	高	高
OV	○	あり	参加費に含む	中	中
DV	×	なし	—	簡易	低

※1枚ごとに別途支払いが必要

事業参加費（仮称）

GakuNin

構成員数	年額（税別）
1–200	¥30,000
201–400	¥40,000
401–600	¥50,000
601–800	¥60,000
801–1000	¥70,000
1001–1200	¥80,000
1201–1400	¥90,000
1401–1600	¥100,000
1601–1800	¥110,000
1801以上	¥120,000
追加ドメイン	¥20,000

- ✓ 構成員数 ＝ 常勤の教員・研究者数（CiNiiと同基準）
- ✓ 年額には、1ドメインのOV証明書・クライアント証明書・コード署名用証明書を含む
  - ✓ サービス開始当初は、クライアント証明書とコード署名用証明書は無償
- ✓ ドメイン追加時には、追加ドメインの額をプラス
- ✓ 各証明書の発行枚数に上限なし
- ✓ 数年後に改訂の可能性あり

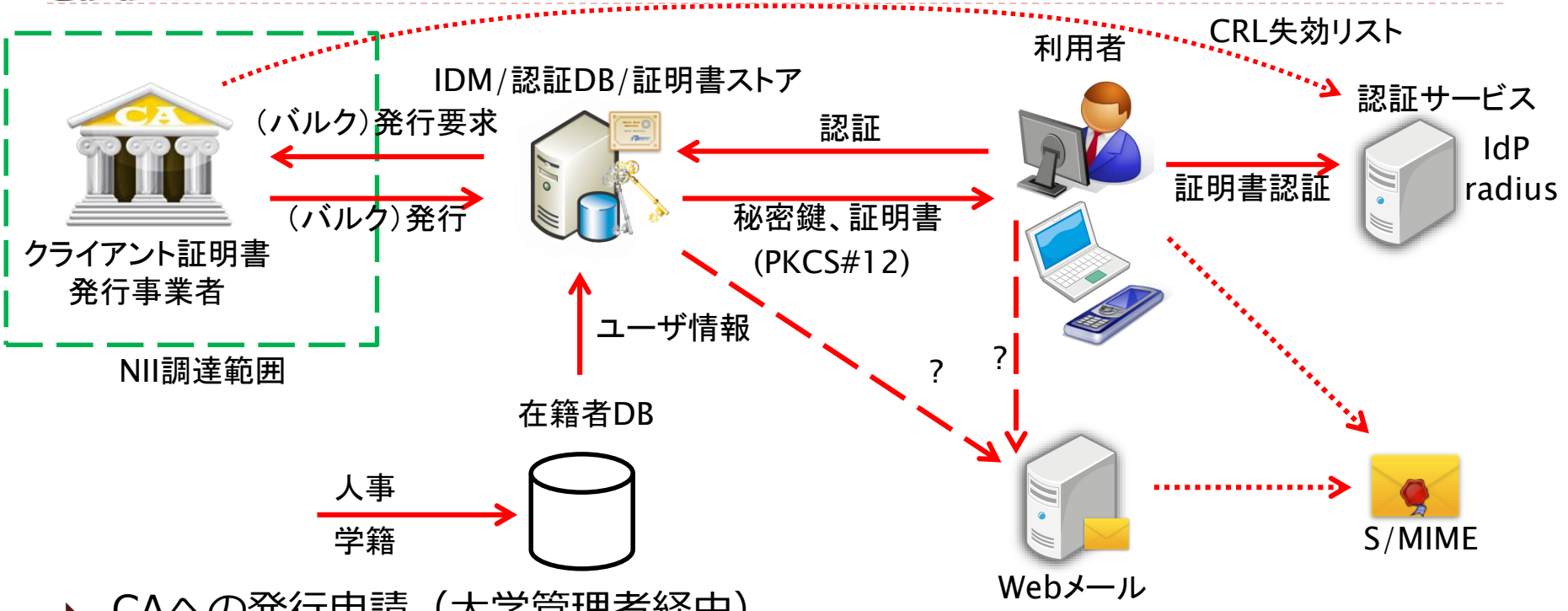
クライアント証明書発行に関する経済効果

- 2012年度末アンケート調査
  - クライアント証明書使用中：41機関
    - 商用認証局から購入：10機関
    - 独自CA構築・運用：31機関
- クライアント証明書運用にかかる費用
  - JIPDEC JCAN証明書：初期8万円＋1,000円/人・年
    - 商用認証局から購入するともっと高価
  - 独自CAを構築すると導入に約6千万＋運用に約9百万/年
    （大規模大学での運用コスト例）
- 1万人規模の大学で導入すると1,000万円/年
  - 単純に40倍すると、**4億円/年** の経費が必要
    - この費用を大幅に圧縮
    - 大学での本格活用をきっかけに民間での活用が進むことを期待
      （特にS/MIME）

クライアント証明書の活用

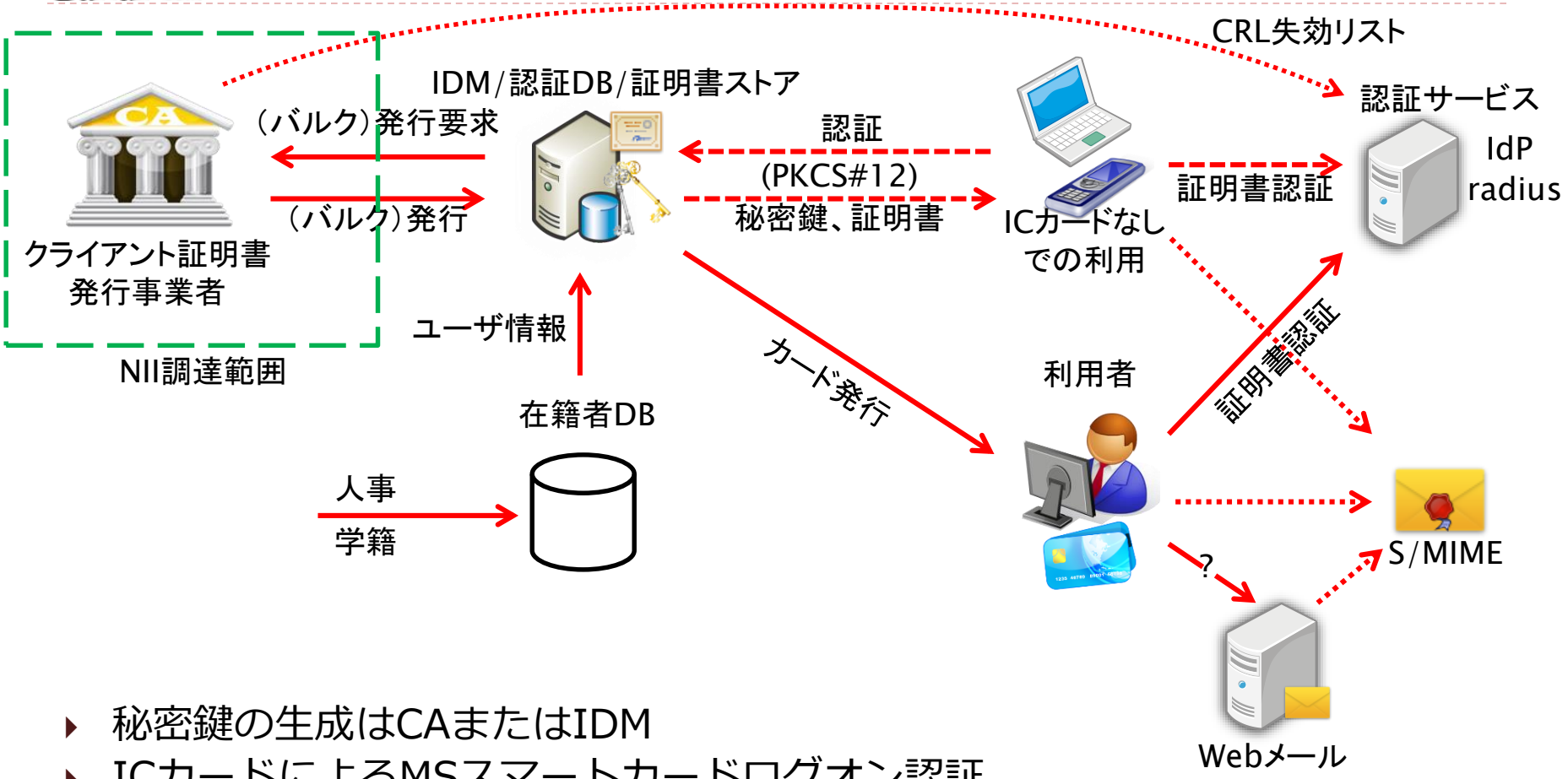
- 用途
  - 認証
  - 署名（電子メール、文書、…）
  - 暗号化（電子メール、…）
    - 電子メールで使用する場合は、証明書にメールアドレスの記載が必要
- 配布方法
  - ユーザ単位　－　端末紛失等で、当該ユーザの全端末証明書の再インストールが必要
  - 端末単位　－　電子メールの暗号化利用に難あり
- 発行方法
  - バルク（大学担当者がまとめて申請、受領）
  - ユーザごと（大学担当者を経由して申請し、利用者が受領）
- 有効期限
  - 2～3年程度で検討中
- 活用形態
  1. アプリケーション（モバイルデバイス等）にストア
  2. ICカード（Type B等）にストア
  3. FCF等（FeliCa）と連携

事例1：アプリケーションにストア



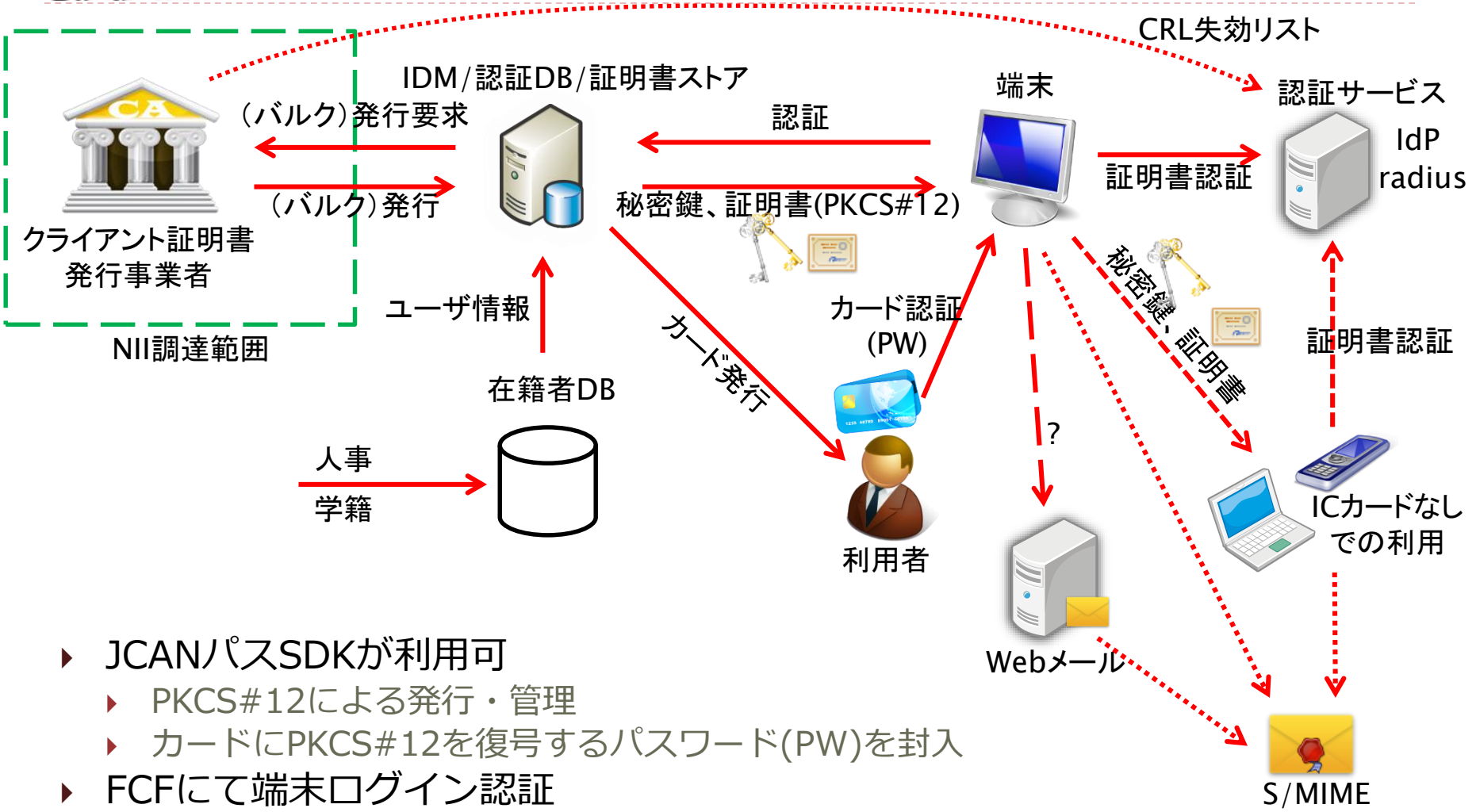
- CAへの発行申請（大学管理者経由）
  - バルク発行？個別発行？
- ユーザへの配布方法
  - CAから直接ダウンロード？大学の証明書ストア（リポジトリ）経由？
- ユーザごとの発行状況管理
  - 失効・再発行申請、複数証明書発行時のデバイスごとの紐付け
- Webメールとの連携？

事例2：ICカード(Type B等)にストア



- 秘密鍵の生成はCAまたはIDM
- ICカードによるMSスマートカードログオン認証
  - サードパーティCAへの対応
- Webメールとの連携？

事例3：FCF等と連携



- JCANパスSDKが利用可
  - PKCS#12による発行・管理
  - カードにPKCS#12を復号するパスワード(PW)を封入
- FCFにて端末ログイン認証
- Webメールとの連携？

サーバ証明書対応ブラウザ

- Microsoft Internet Explorer 8以上
- Firefox 24.0以上
- Opera 12.15以上
- Apple Safari 6.0以上
- Google Chrome 34.0.1847.116以上
- iOS用Safari 4.0以上
- Android 4.0以降に対応したGoogle Chrome
- 2009年1月以降に日本で発売された携帯電話に搭載されたWebブラウザで、ルート認証局証明書の鍵長RSA2048bitに対応したブラウザ

サーバ証明書対応Webサーバ

- Apache(mod ssl)　1.3
- Apache(mod ssl)　2.0
- Apache-SSL(1.3.33+1.55)
- Microsoft IIS 6.0～8.5
- IBM HTTP Server6.0.2
- Tomcat 5～7

クライアント証明書の対応環境

- Microsoft Internet Explorer 8 (Windows) 以上
- Firefox 24.0 （Windows, OSX） 以上
- Opera 12.15 (Windows, OSX) 以上
- Apple Safari 6.0 (OSX) 以上
- Google Chrome 34.0.1847.116 (Windows, OSX) 以上
- Android 4.0以上
- iOS 3.1.3以上

コード署名用証明書の用途

- Windows用 .exe
- Windows用 .cab
- Windows用 .dll
- Windows用 デバイスドライバ
- Windows PowerShell用スクリプト
- JAVA .jar
- Android用アプリケーション .apk
- Mac OSX .app bundles
- Microsoft Silverlight ベースアプリケーション
- Adobe AIR

SHA-2対応

- マイクロソフト セキュリティ アドバイザリ 2880823（2013年11月13日公開）
  - マイクロソフト ルート証明書プログラムでの SHA-1 ハッシュ アルゴリズムの廃止
  - 「マイクロソフトは、マイクロソフト ルート証明書プログラムのポリシーを変更したことをお知らせします。新しいポリシーでは、2016 年 1 月 1 日以降、ルート証明機関は SSL とコード サイニングの目的で、SHA-1 ハッシュ アルゴリズムを使って X.509 証明書を発行できなくなります。」
  - 「マイクロソフトは、証明機関が SHA-1 ハッシュ アルゴリズムを使って新しく生成された証明書に署名せずに、SHA-2 に移行することを推奨します。また、お客様ができるだけ早い機会に SHA-1 証明書を SHA-2 証明書に置き換えることを推奨します。」

    引用もと：https://technet.microsoft.com/ja-jp/library/security/2880823
- 当初はSHA-1/2双方扱えることとし、時期を定めてSHA-2への移行を進める予定です

各証明書の提供開始時期

- サーバ証明書
  - 2015年1月より
- クライアント証明書
  - 2015年4月以降予定
- コード署名用証明書
  - 2015年4月以降予定

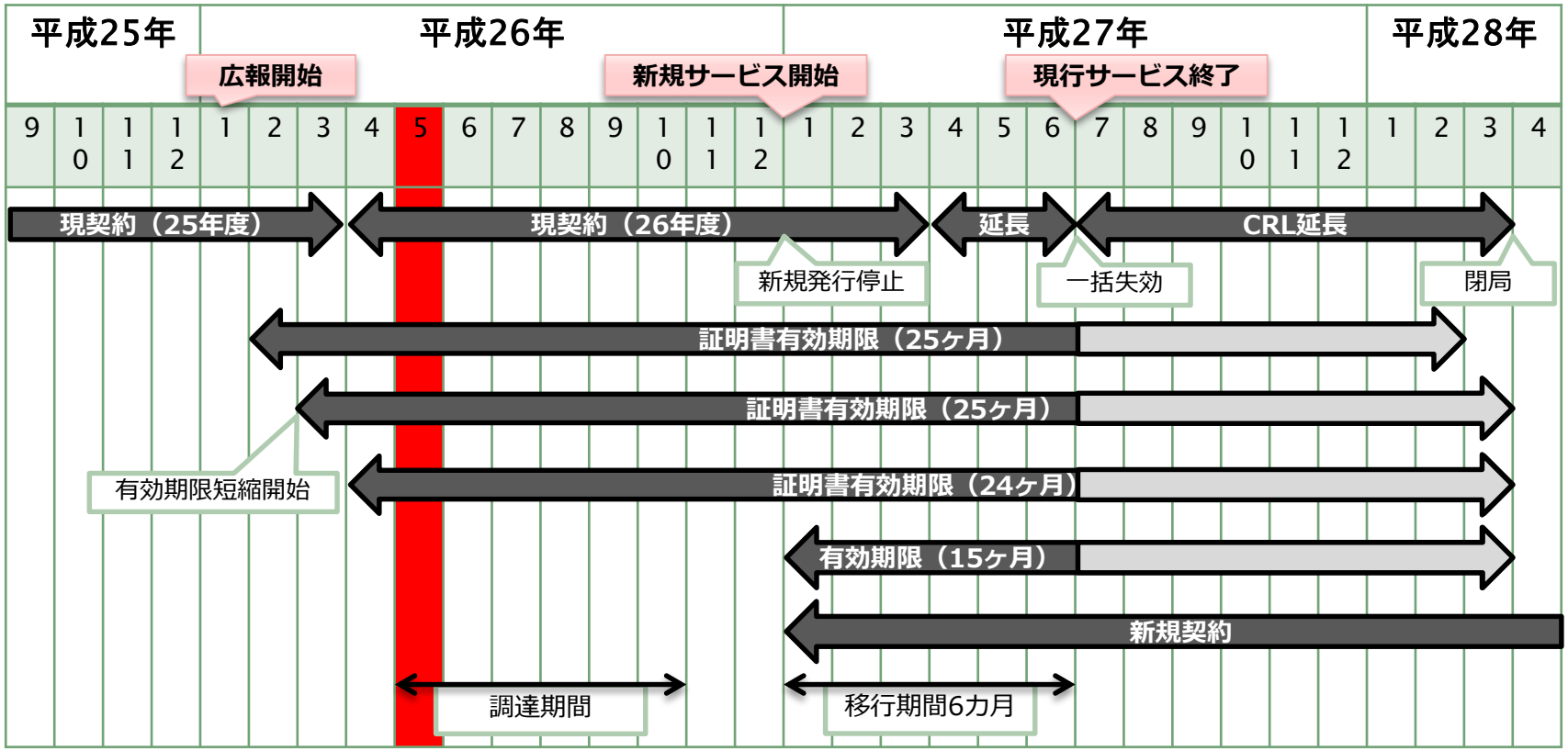
次期サービスへの参加申請

- 受付開始時期
  - 10月頃を予定
- 参加費について
  - 2014年度内（2015年1月～3月）
    - 無料とする予定
    - 移行期間という意味合い
  - 2015年度以降
    - 支払い方法・支払先
    - 調整中

今後の説明会

- 秋頃までに、各地域で説明会を実施予定です
- 形態、日程については、決まり次第 機関責任者・登録担当者用メーリングリスト、ホームページ(https://upki-portal.nii.ac.jp/)などでお知らせいたします

移行スケジュール


平成25年
平成26年
平成27年
平成28年
広報開始
新規サービス開始
現行サービス終了
9 10 11 12 1 2 3 4 5 6 7 8 9 10 11 12 1 2 3 4 5 6 7 8 9 10 11 12 1 2 3 4
現契約（25年度）
現契約（26年度）
延長
CRL延長
新規発行停止
一括失効
閉局
証明書有効期限（25ヶ月）
証明書有効期限（25ヶ月）
有効期限短縮開始
証明書有効期限（24ヶ月）
有効期限（15ヶ月）
新規契約
調達期間
移行期間6カ月

学認春CAMP2014(明日：5月30日)

Session 1　NIIとの共同研究報告会

一橋講堂

■10:00 - 10:40
「学認のサービス連携推進のための機能開発」
京都産業大学 秋山豊和

■10:40 - 11:20
「Shibboleth用多要素認証導入のための技術ガイド」
金沢大学 松平拓也

■11:20 - 12:00
「eduroamの最新動向と耐災害性・耐障害性向上」
東北大学 後藤英昭

Session 2　クライアント証明書BoF

小会議室

■14:30-15:50
「次期証明書発行サービスで提供されるクライアント証明書を徹底活用するためのディスカッション」

■デモ1
「続々登場中！クライアント証明書対応アプリ！」
～JCANパス(FCFキャンパスカード対応), ROBINS連携(Thunderbirdアドオン), スマホSIM活用等～

■デモ2
「クライアント証明書を中心とするエコシステムの創生」