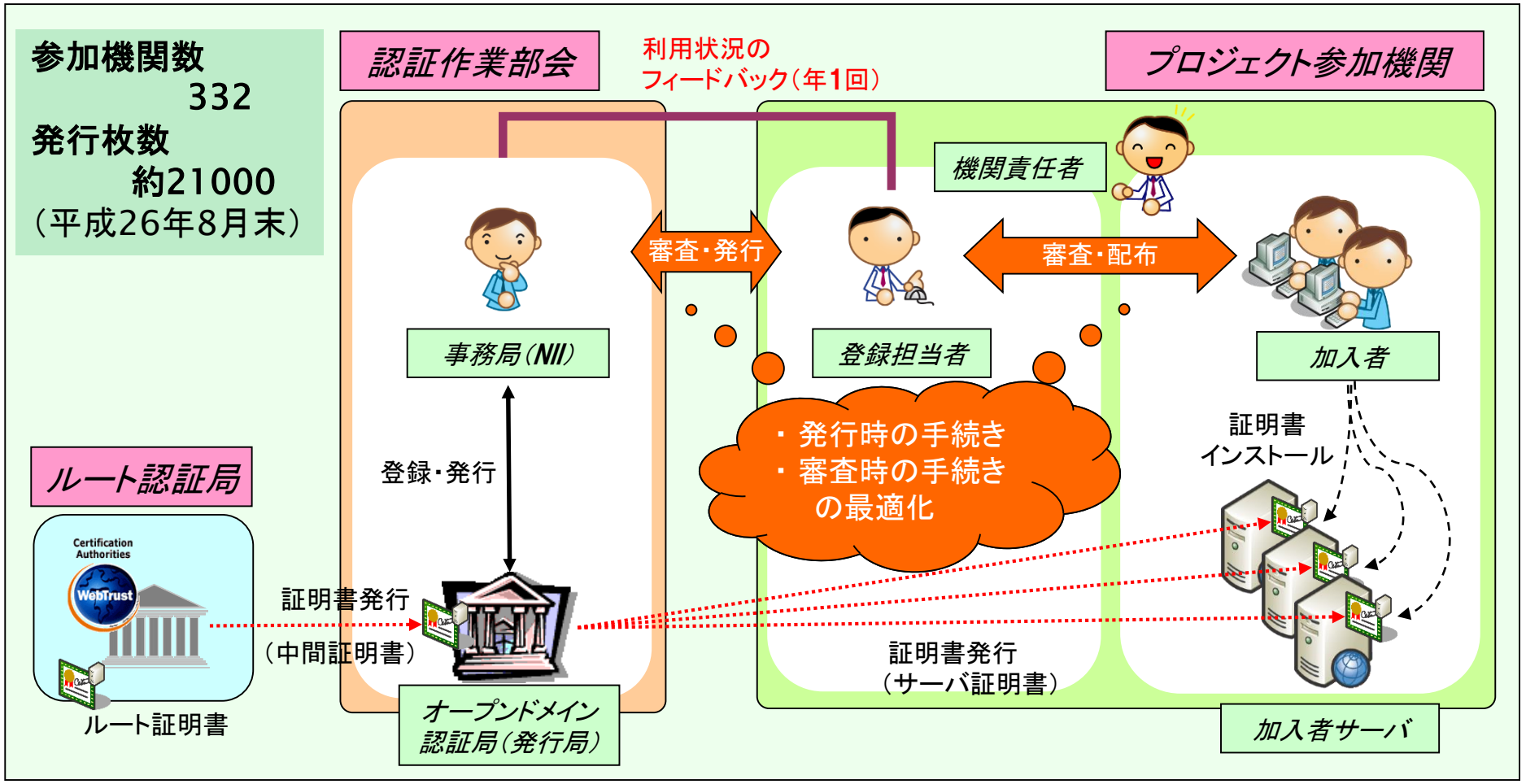
次期証明書発行サービスについて

2014年度 SINET及び学認・UPKI証明書説明会資料（2014.10.31@京都）

国立情報学研究所

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

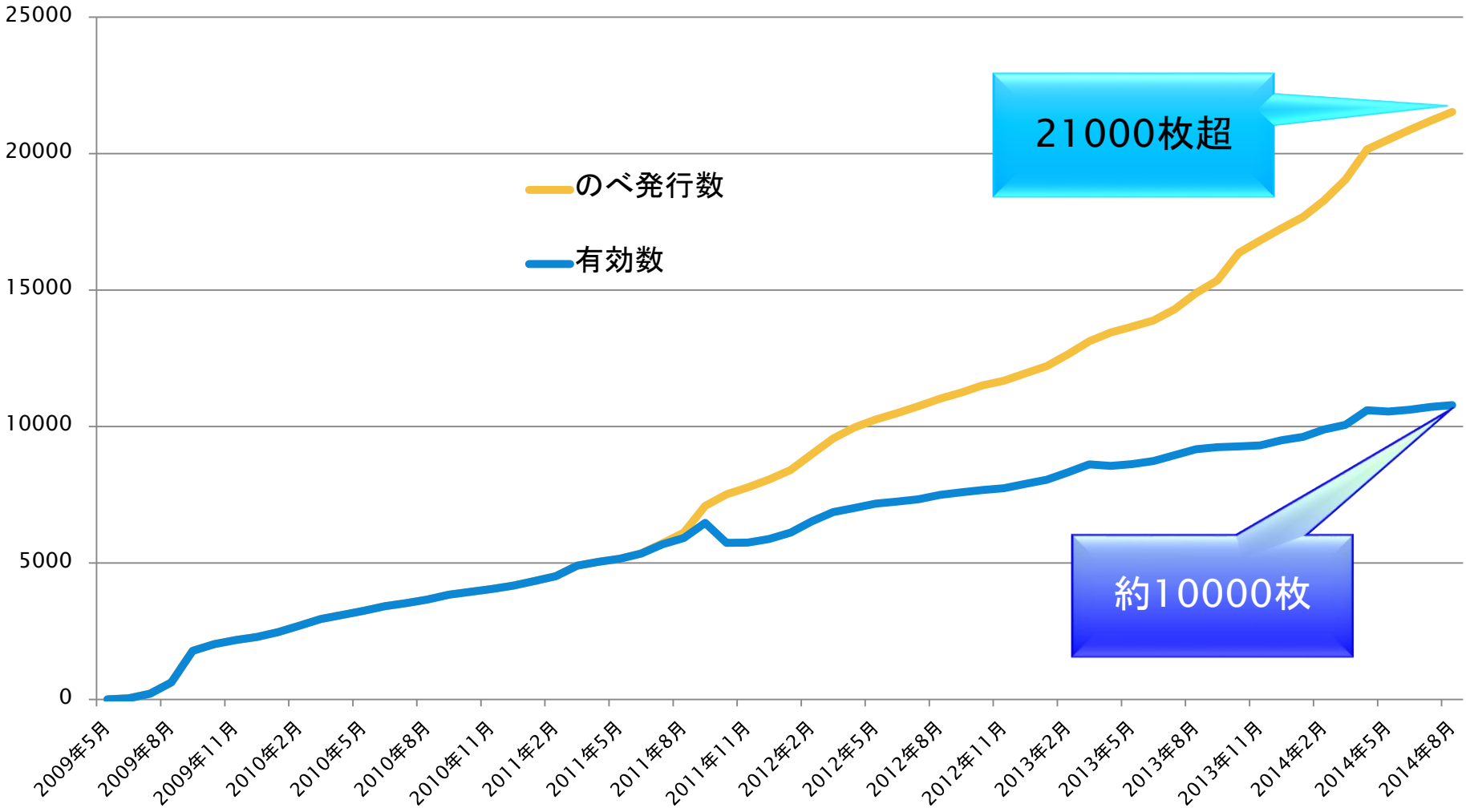
これまでの活動

- 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332機関　のべ発行枚数21,527枚（平成26年8月時点）

✓ 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）



※2009年5月から2014年8月まで

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

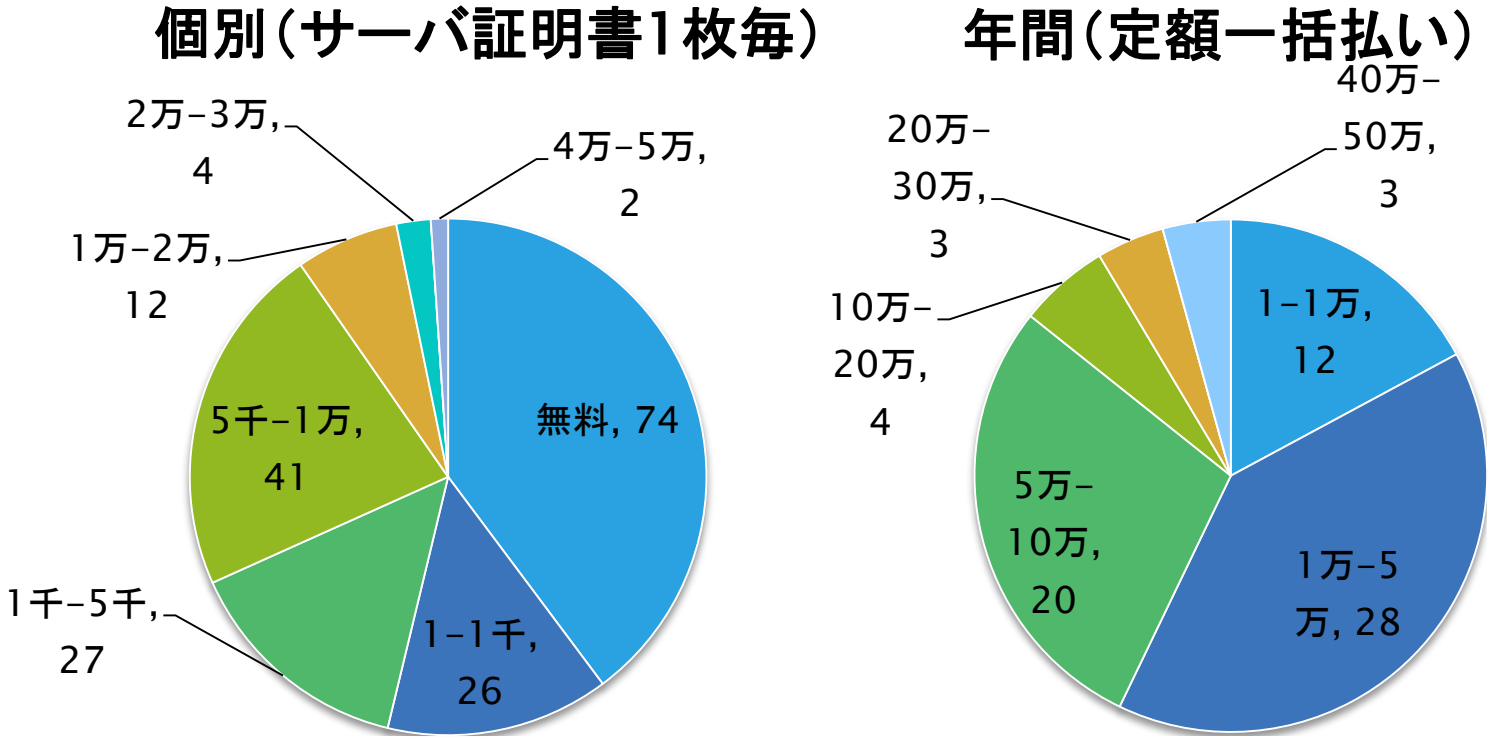
サービスの継続についての検討

- 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

GakuNin

- 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

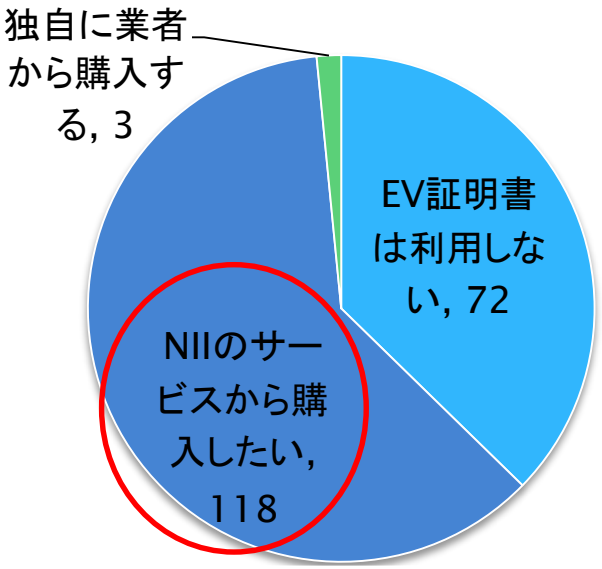
クラウドサービスの信頼度		信頼度Ⅰ	信頼度Ⅱ	信頼度Ⅲ	信頼度Ⅳ
対応 認証レベル（LoA）		Level1	Level2	Level3	Level4
機関が保有する情報の重要度	重要度Ⅰ	←	←	←	←
	重要度Ⅱ		←	←	←
	重要度Ⅲ			←	←
	重要度Ⅳ				←

クライアント証明書の利用

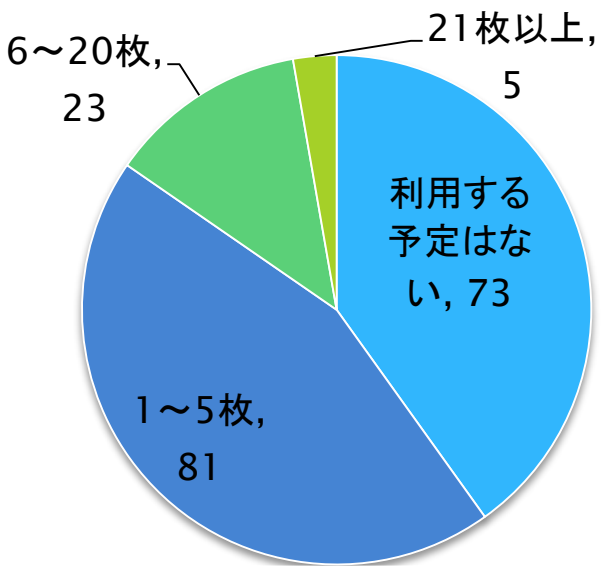
大学からのニーズ

- 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？

EV証明書のニーズ



利用予定枚数



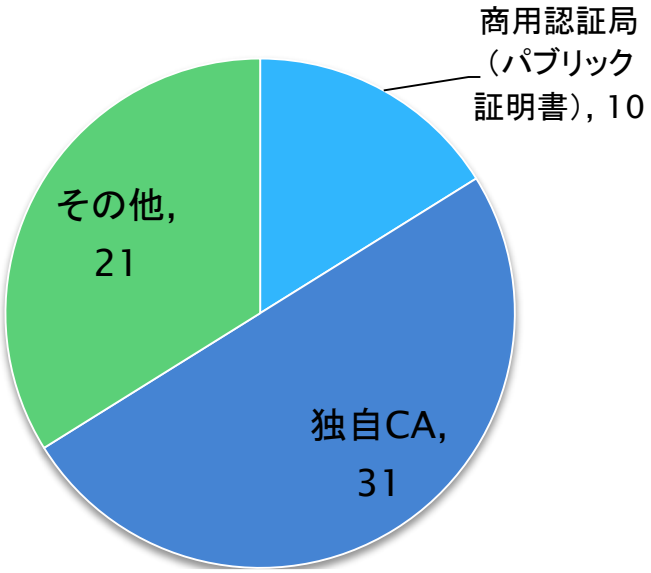
参考：シマンテック　セキュア・サーバID EV　170,100円／年
セコムパスポート for Web EV　141,750円／年

より高い信頼性を証明するEV証明書発行の期待

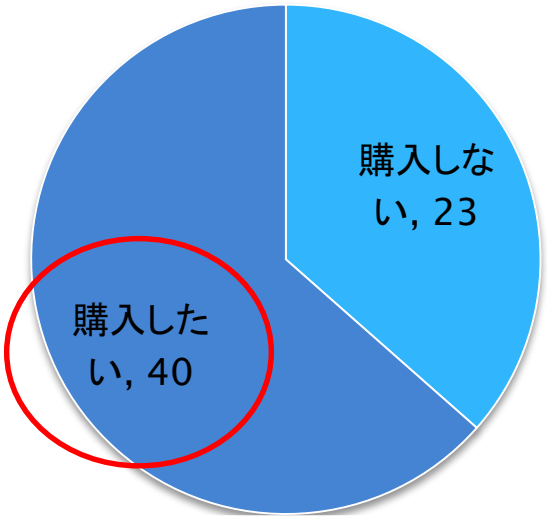
大学からのニーズ

- 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電子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，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
- 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

事業参加費

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
  - ✓ サーバ証明書に課金
- ✓ 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

補足：「ドメイン」に含まれる範囲

登録ドメイン

domainname.ac.jp

サブドメイン

- info.domainname.ac.jp
- secretariat.domainname.ac.jp
- sub.domainname.ac.jp
- sub.sub.domainname.ac.jp

など

構成員数に応じて設定される金額（¥30,000～¥120,000）に含まれます

追加ドメイン1

domainname.jp

サブドメイン

- library.domainname.jp
- faculty.drive.domainname.jp

など

追加ドメイン１件の金額（¥20,000）に含まれます

※ワイルドカード証明書（例：*.domainname.ac.jp）は発行できません

EV証明書

- EV証明書については、本サービスの範囲外となっております
- どのようなサービスが可能か、引き続き検討してまいります
  - EV (Extended Validation)
  - OV (Organization Validation)
  - DV (Domain Validated)

	審査レベル	組織実在審査	信頼度
EV	高	あり	高
OV	中	あり	中
DV	簡易	なし	低

次期サービスへの参加申請

- 受付開始時期
  - 12月からを予定
- 参加費について
  - 2014年度内（2015年1月～3月）
    - 無料といたします
  - 2015年度以降（現在の予定）
    - 申請受理の後、請求書を発行します（請求書のみの発行となります）
      - 当該年度内のお支払いにご協力ください
    - 2014年度中に参加申請をいただいた場合、2015年度分よりご請求致します
    - 原則として年度毎に1年分の参加費をお支払い頂きます
    - 年度途中で参加申請をいただいた場合、残りの期間に応じて金額を決定し、請求いたします
      - 詳細な手続きや所要期間は所内で調整中です
      - 「年度の残りの期間」は、四半期を単位として算出する予定です
        - 例：
          - 4月から6月末日までに登録完了した場合、年額の3/4
          - 7月から9月末日までに登録完了した場合、年額の2/4

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：初期約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）

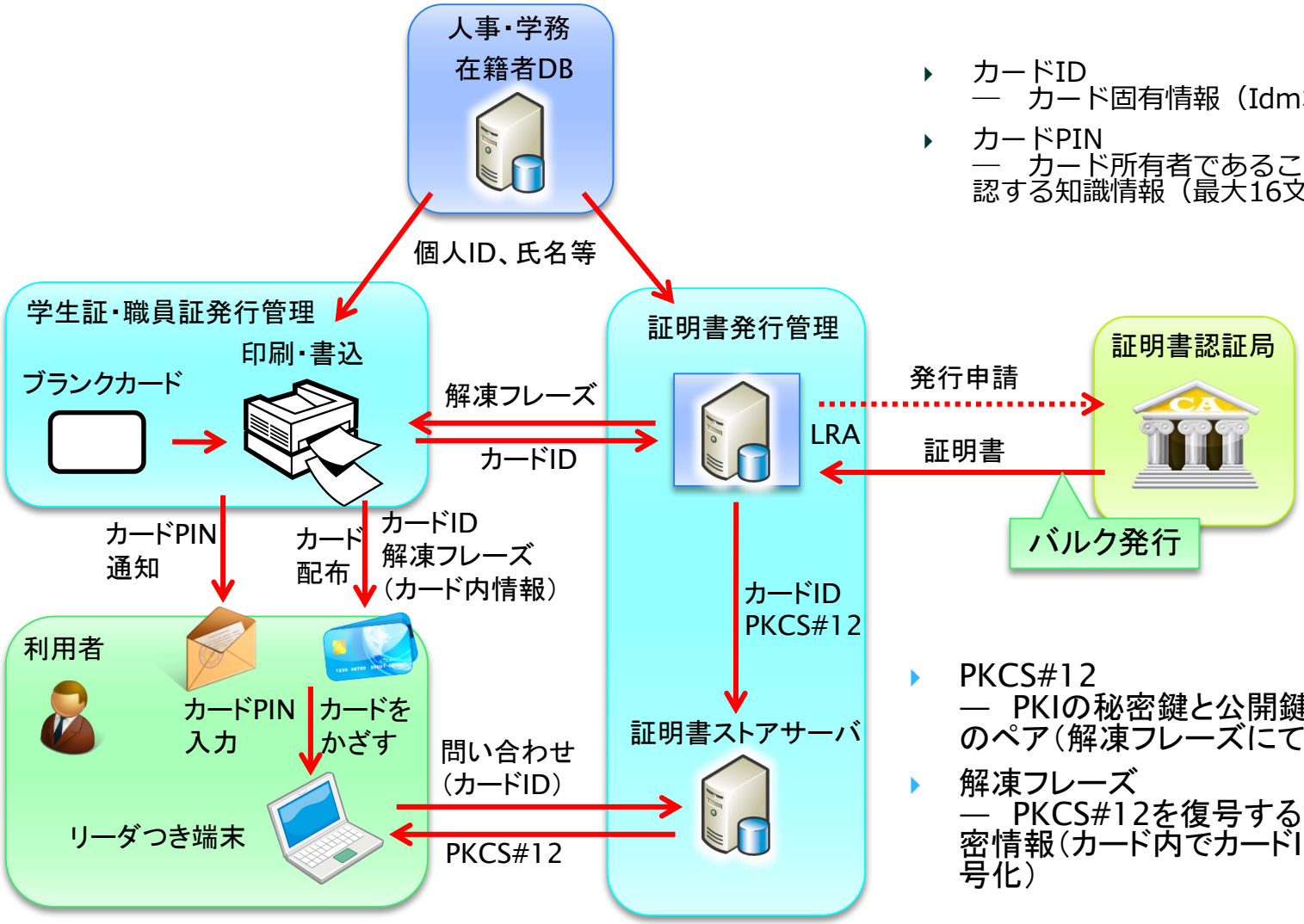
クライアント証明書の活用

- 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
  - 利用者1名あたり1枚
    - 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1台あたり1枚
    - 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

証明書サーバと連携するICカードの利用形態

- Felicaカードを用いるが、証明書を書き込まず、証明書サーバから秘密鍵と公開鍵証明書を取得して利用する方式
- 特徴
  - 証明書をカードに保存しないため、証明書の更新処理にカード側の処理を不要にできる
    - 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
  - 他の用途（アプリケーション）との共存に有利
    - カード上に大きな領域の確保が不要
- JIPDECの「JCANパス方式」をベースに詳細検討中
  - 新名称：UPKIパス？

ベースとするJCANパス方式の運用イメージ



- カードID
  - カード固有情報（Idmなど）
- 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の秘密鍵と公開鍵（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（カード内でカードIDにて暗号化）

JIPDECとの連携ーROBINS(1)

- JIPDEC：一般社団法人日本情報経済社会推進協会
  - http://www.jipdec.or.jp
- 提供サービス
  - JCAN証明書
    - いくつかの機関で導入
    - NIIでも事務局全体と、希望した教員で試験中
  - ROBINS
    - 電子的な法人台帳
    - 機関の正式名称、URL、所在地等、様々な情報を掲載

JIPDECとの連携ーROBINS(2)

- アカデミックROBINS（検討中）
  - ROBINSに、NIIがサービス参加機関情報を登録
    - ROBINSキー(RB-XXXXXXXXXX)が割り振られる
      - 証明書プロファイルに記入して利用可能
    - 機関の情報は、ROBINSも独自に調査・確認
    - 機関の実在性確認にも利用可

- 提供サービス
  - シール
    - Webページに表示し、クリックして機関情報を確認
  - DKIM対応
    - 現在はヤフー、ニフティのみ
  - S/MIME利用時、Thunderbirdアドオンで機関情報表示

クライアント証明書プロファイル（予定）

証明書フィールド		文字数	記述内容（例）	クライアント認証用	S/MIME
Subject	CountryName	2	JP	固定値	
	StateName	128	Kyoto	固定値	
	LocalityName	128	Kyoto	固定値	
	OrganizationName	64	KYOTO UNIVERSITY	固定値	
	OrganizationUnitName	64	RB-XXXXXXXXXXXXXX （ROBINSキー）	ROBINSキー利用時 固定値	
	OrganizationUnitName	64	学部名等	任意	
	OrganizationUnitName	64	プロジェクト名等	任意	
	OrganizationUnitName	64	その他	任意	
	CommonName	64	名前、学生番号等	必須	
	Postal Code	40	606-8501	必須	
	Street Address1	128	Sakyo-ku Yoshida Hommachi	必須	
	Street Address2	128	Street Address1に 入らない場合利用	任意	
	Street Address3	128	Street Address2に 入らない場合利用	任意	
extension	SubjectAltName Rfc822Name	—	abc@kyoto-u.ac.jp	任意	必須

※プロファイルについて、ご要望がありましたら是非お知らせ下さい

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

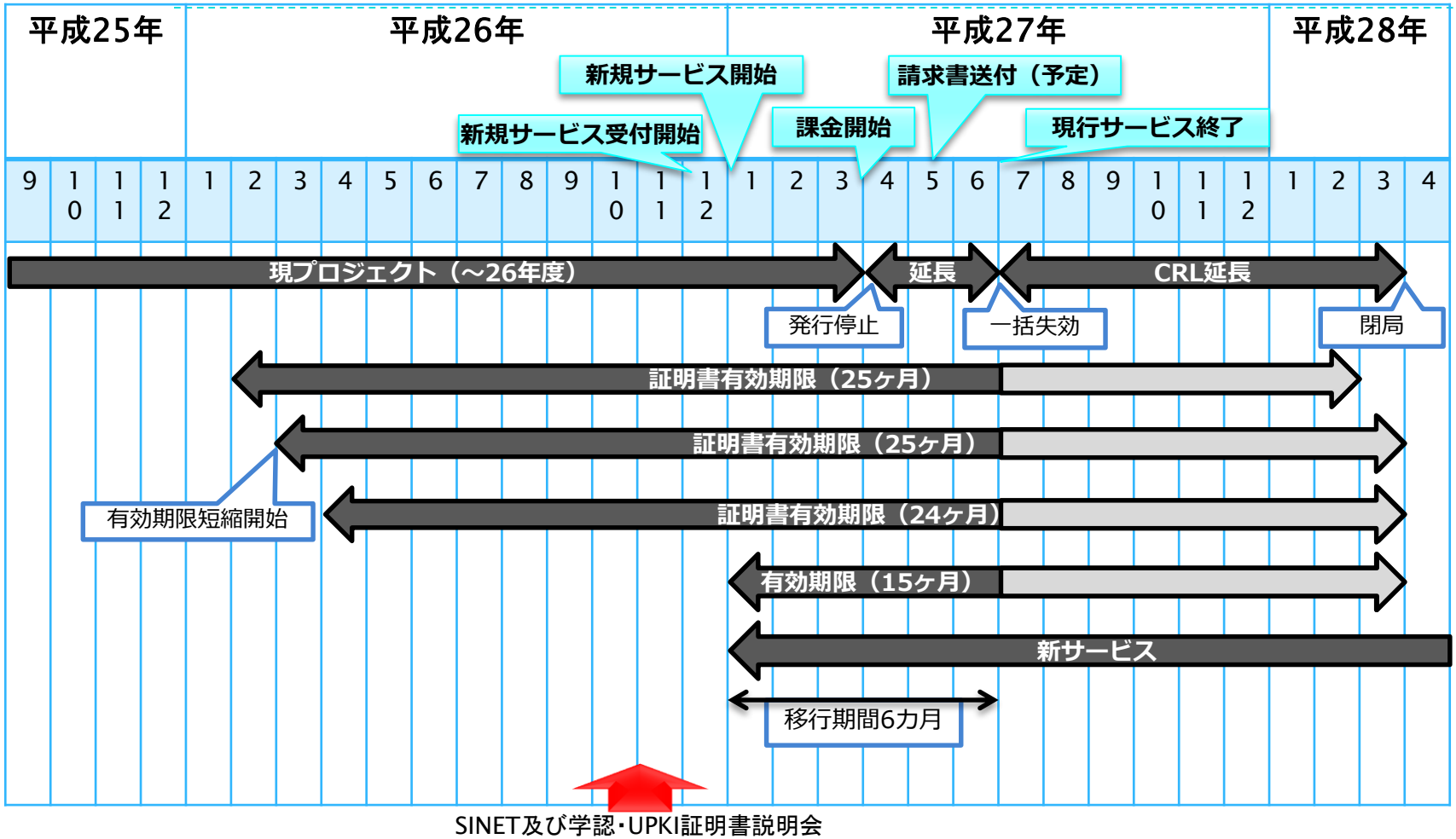
- マイクロソフト セキュリティ アドバイザリ 2880823（2013年11月13日公開）
  - マイクロソフト ルート証明書プログラムでの SHA-1 ハッシュ アルゴリズムの廃止
  - 「マイクロソフトは、マイクロソフト ルート証明書プログラムのポリシーを変更したことをお知らせします。新しいポリシーでは、2016 年 1 月 1 日以降、ルート証明機関は SSL とコード サイニングの目的で、SHA-1 ハッシュ アルゴリズムを使って X.509 証明書を発行できなくなります。」
  - 「マイクロソフトは、証明機関が SHA-1 ハッシュ アルゴリズムを使って新しく生成された証明書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

移行スケジュール



- 詳細な情報を、下記URLに順次掲載してまいります
  https://upki-portal.nii.ac.jp/docs/news/odcert/20140424

ご連絡・お問い合わせ先

- 国立情報学研究所　学術基盤課
  総括・連携基盤チーム（認証担当）
  - Mail：cerpj2@nii.ac.jp
  - 電話：03-4212-2218
  - 担当：水元