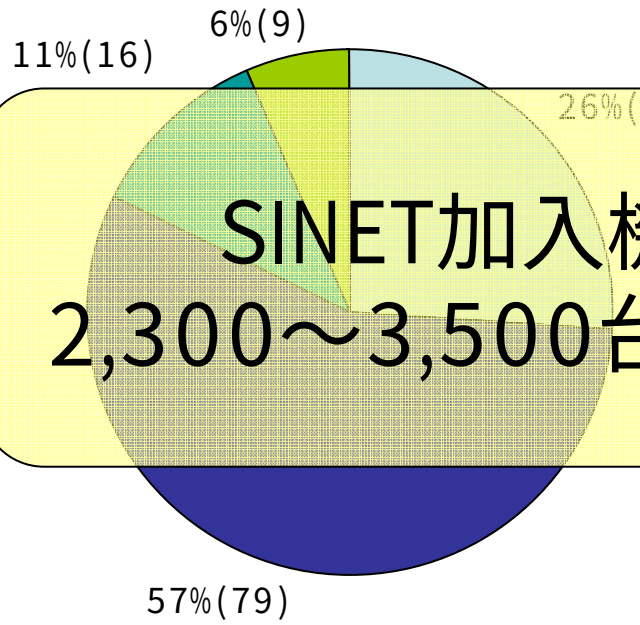
サーバ証明書発行・導入の啓発・評価研究プロジェクト

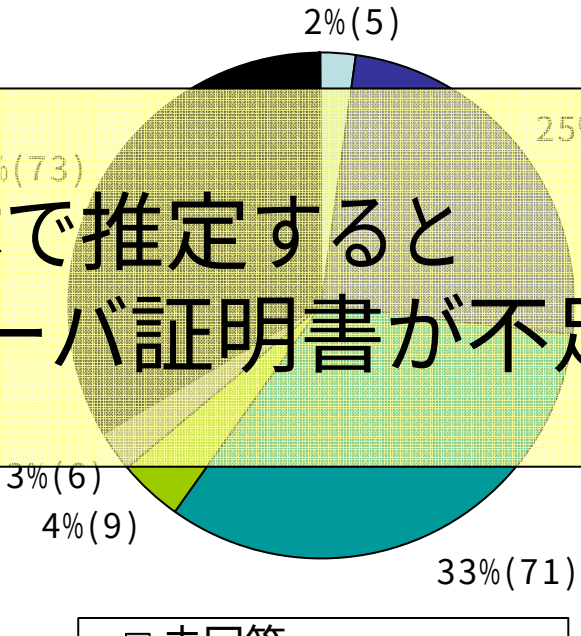
国立情報学研究所
学術ネットワーク研究開発センター
島岡 政基

大学等におけるサーバ証明書の実態

証明書の利用状況
(未回答・わからないを除く)



証明書を利用できていない台数

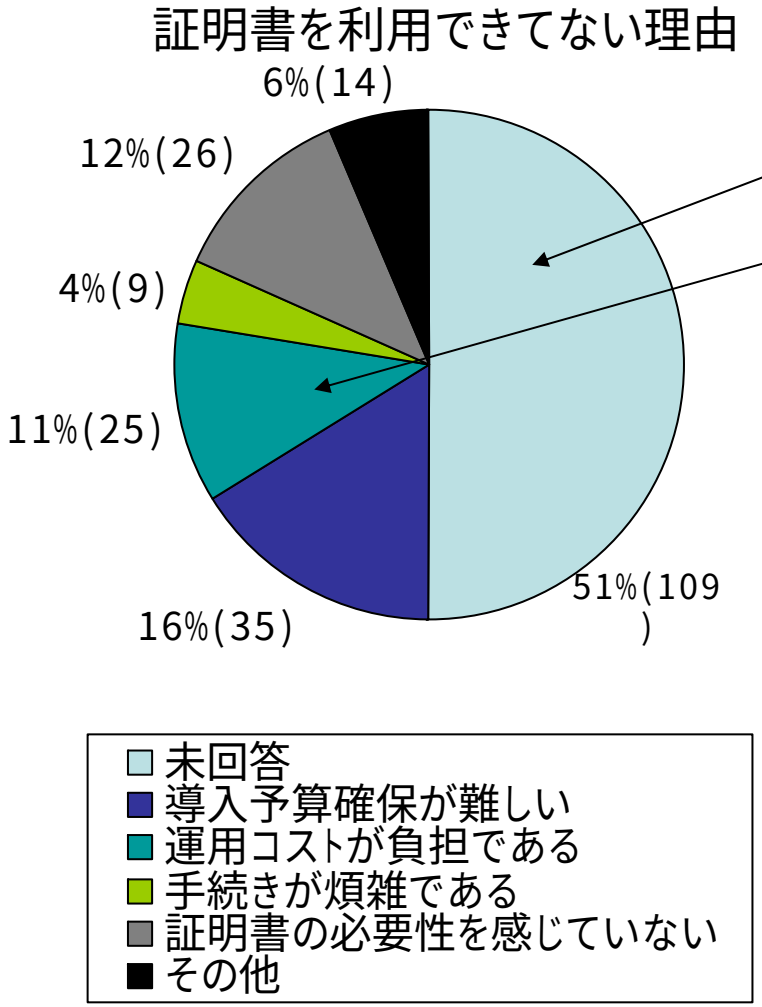


SINET加入機関全体で推定すると
2,300～3,500台分のサーバ証明書が不足

H18年度「**大学等における電子証明書の利用状況に関する実態調査**」より

対象: SINET**加入機関**818**件、うち有効回答**218**件**

普及が進まない理由



- 理由がわからない!!
- 運用コストの負担
  - 実際に生じる負担は?

実際に使ってもらって
確認してはどうか?

プロジェクトの概要

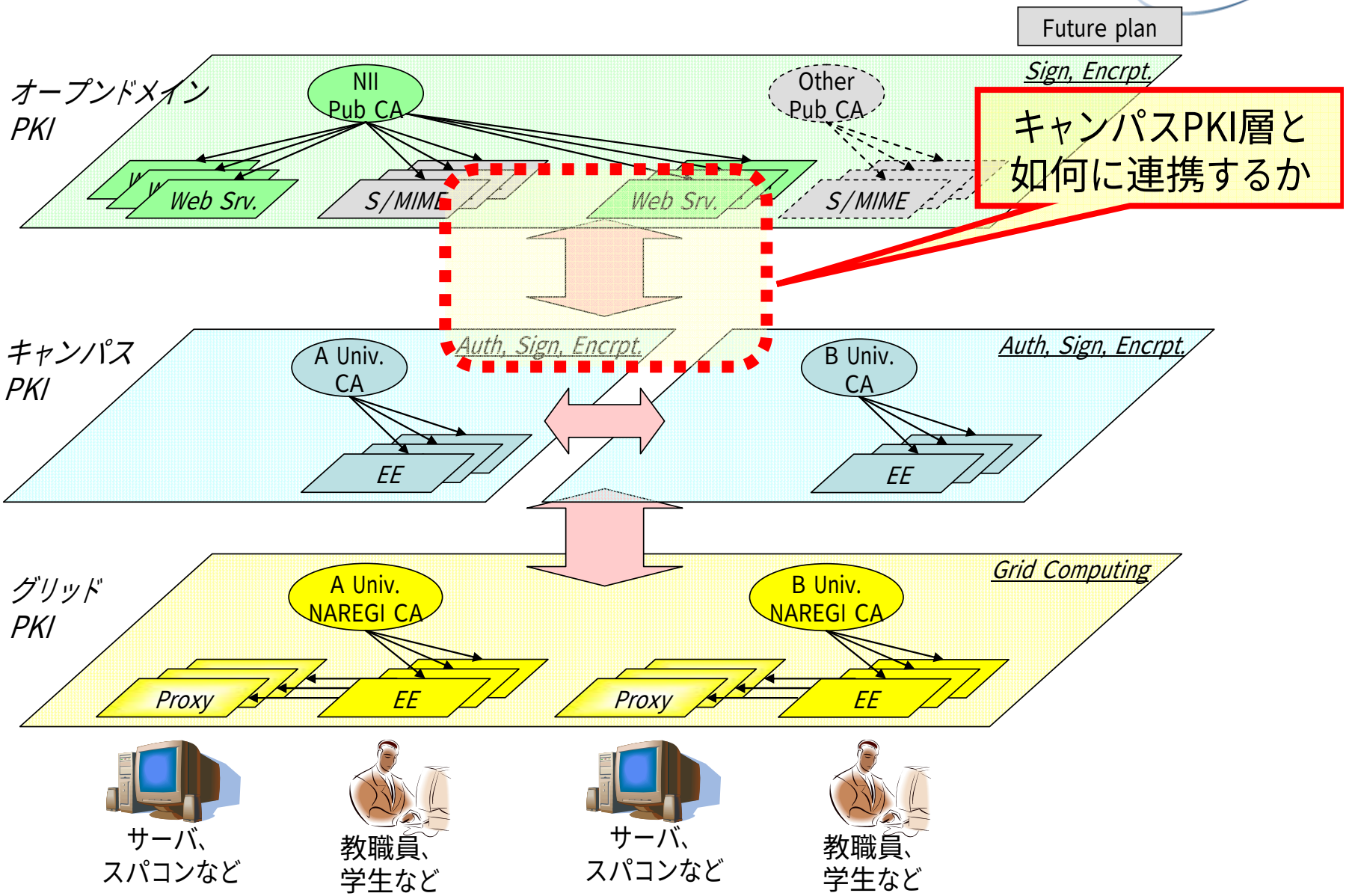
- 目的
  - 大学等のサーバ証明書の普及を推進
  - 認証局を用いた研究開発 ⇒ 登録発行業務の改善
  - 学術機関のWebサーバ信頼性向上
  - サーバ証明書の導入･運用ノウハウの共有
  - 参加者のサーバに対してのサーバ証明書無償配布
- 期間
  - 2007/04/01～2009/03/31
- ゴール
  - H19年度: サーバ証明書の普及が進まない理由･課題の整理
  - H20年度: サーバ証明書の普及促進の仮説･立証
  - 将来的に: キャンパスPKI層を活用した証明書発行業務の自動化
- 主な作業
  - プロジェクト参加者(ユニット)の募集
  - ユニット登録担当者へのS/MIME証明書発行
  - ユニットメンバが管理するサーバに対するサーバ証明書の発行
  - ユニットメンバによるサーバ証明書の導入･運用
  - 発行手続、導入手順などに対する改善案･Tipsのフィードバック
  - 改善案･Tipsなどの整理･公開など

認証局を用いた評価研究

体験を通じて啓発

H19年度作業

UPKIにおける位置づけ(ゴール)



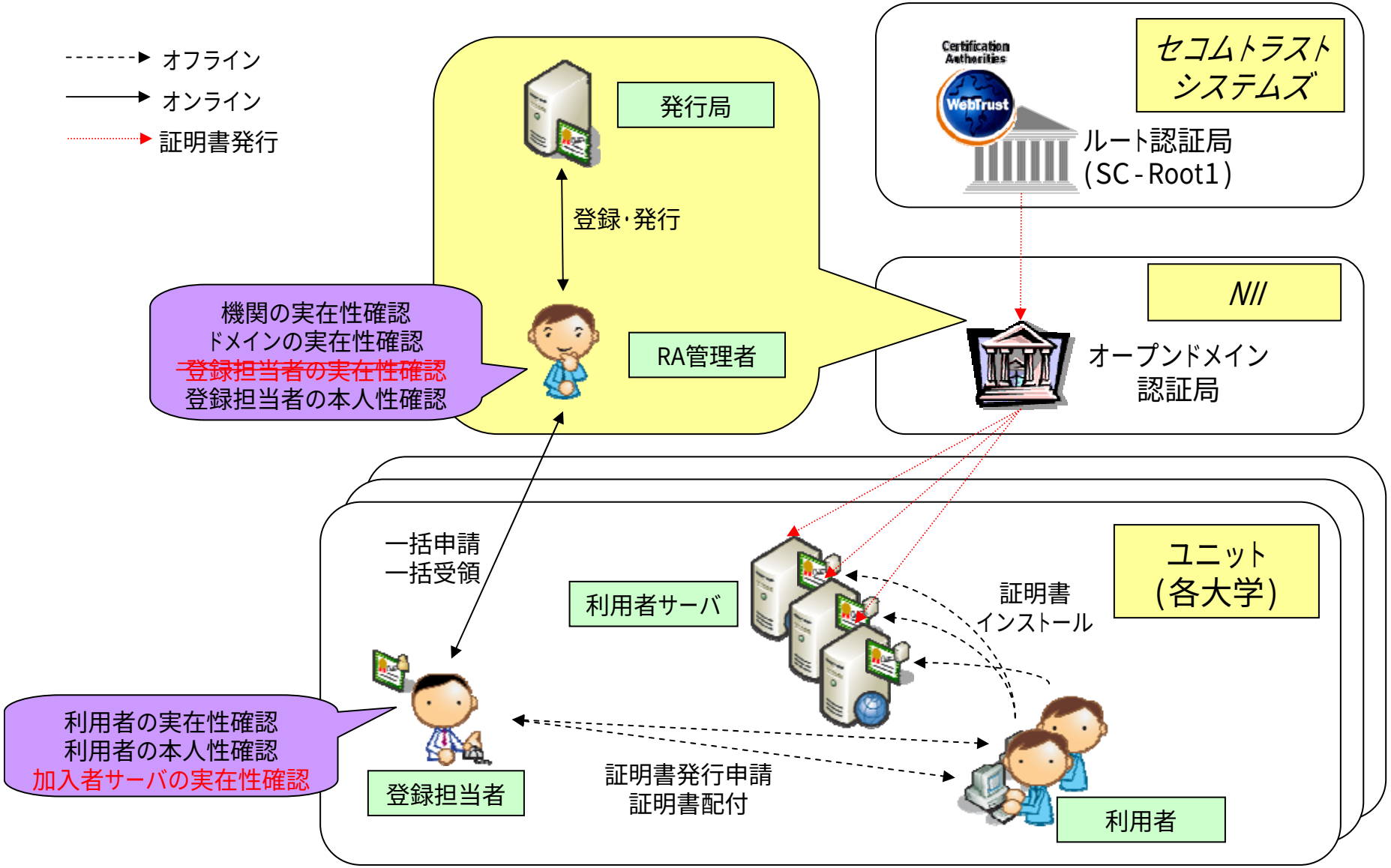
証明書発行の基本方針

- 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
- 審査項目の分担による発行業務の最適化
  - その審査を一番手早く実現できるのは誰か?
  - 認証局が最低限責任を負うべき項目は?
- 商用サービスと同等の保証レベル
  - 機関の実在性認証まで含めた審査項目→分担して実現

プロジェクト参加者の役割

組織	役割	説明
NII	発行局	認証局の鍵管理、サーバ証明書発行など セコムトラストシステムズへ運用委託
	登録局	参加申し込みにあたり、各種の審査(後述)を行う。
各大学	ユニット	PJへの参加単位。1大学1ユニットが原則。
	ユニット代表者	PJに対する窓口。 参加申込やフィードバックのとりまとめを行う。
	登録担当者 (ユニット内に1名)	ユニット内の利用者からの申請を適時とりまとめ、代理申請を行う。代理申請にあたり、利用者の審査を行う。
	利用者	サーバ管理者であり、証明書の管理に責任を負う。
不特定多数	検証者	サーバへアクセスし、その証明書を検証する。

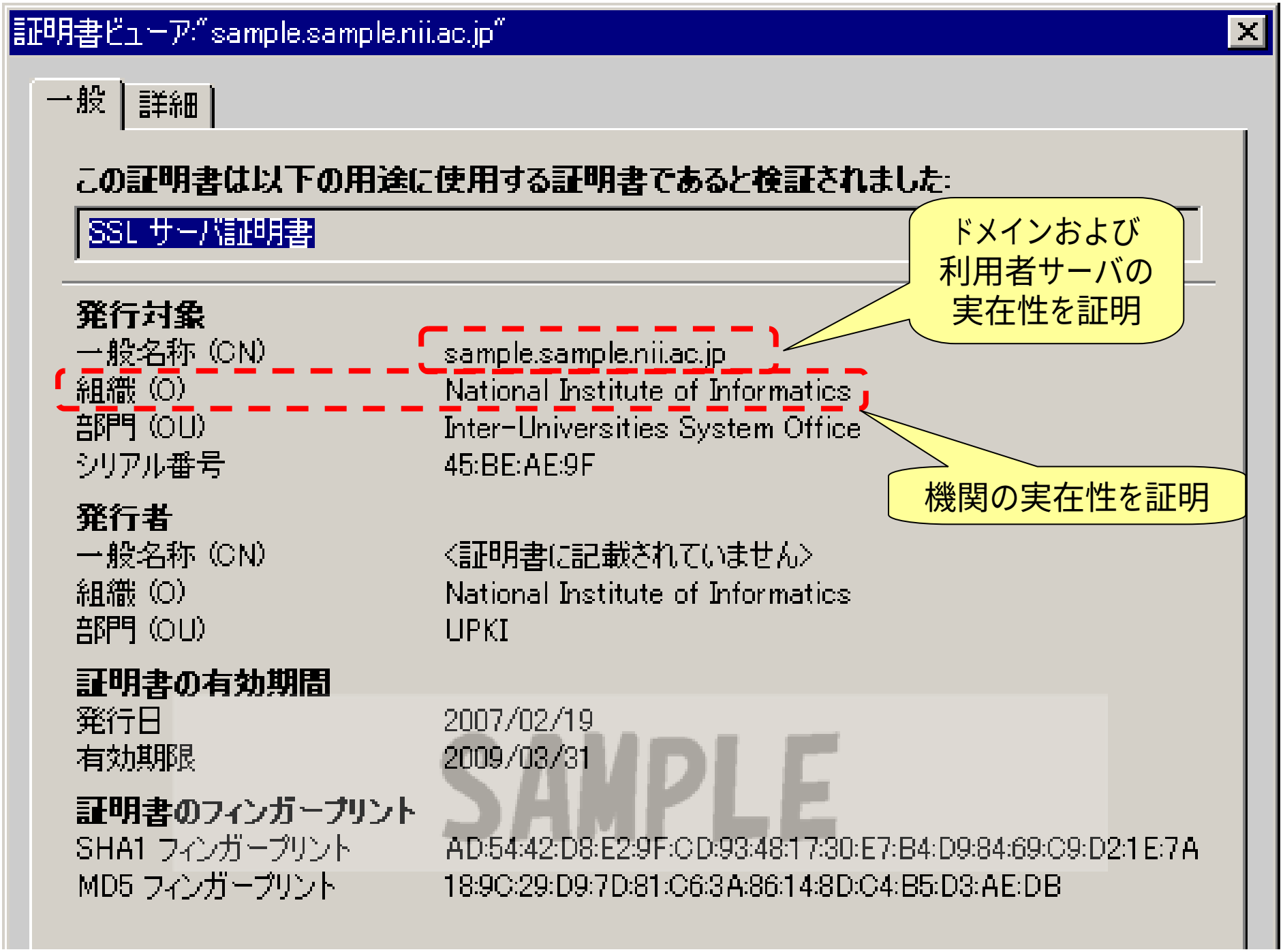
証明書発行の流れ


オフライン
オンライン
証明書発行
発行局
登録･発行
RA管理者
機関の実在性確認
ドメインの実在性確認
~~登録担当者の実在性確認~~
登録担当者の本人性確認
セコムトラスト
システムズ
ルート認証局
(SC-Root1)
NII
オープンドメイン
認証局
一括申請
一括受領
利用者サーバ
証明書
インストール
ユニット
(各大学)
利用者の実在性確認
利用者の本人性確認
加入者サーバの実在性確認
登録担当者
証明書発行申請
証明書配付
利用者

商用証明書との比較
～審査項目の違い～

審査項目	審査者	商用サービス				本プロジェクト			
		オンライン認証		機関認証					
		登録局	利用者	登録局	利用者	登録局	ユニット代表者	登録担当者	利用者
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	○		○		○			
ユニット代表者	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					× →	○		
利用者	本人性確認	×		○		× →		○	
	実在性確認	×		○		× →		○	
利用者サーバ	本人性確認		○		○				○
	実在性確認		○		○			○ ←	×

「認証方法の違いによる役割と活用場面（企業の実在性認証とオンライン認証）」より
http://www.verisign.co.jp/server/first/difference.html


証明書ビューア:"sample.sample.nii.ac.jp"
一般
詳細
この証明書は以下の用途に使用する証明書であると検証されました:
SSL サーバ証明書
発行対象
一般名称 (CN) sample.sample.nii.ac.jp
組織 (O) National Institute of Informatics
部門 (OU) Inter-Universities System Office
シリアル番号 45:BE:AE:9F
発行者
一般名称 (CN) <証明書に記載されていません>
組織 (O) National Institute of Informatics
部門 (OU) UPKI
証明書の有効期間
発行日 2007/02/19
有効期限 2009/03/31
証明書のフィンガープリント
SHA1 フィンガープリント AD:54:42:D8:E2:9F:CD:93:48:17:30:E7:B4:D9:84:69:C9:D2:1E:7A
MD5 フィンガープリント 18:9C:29:D9:7D:81:C6:3A:86:14:8D:C4:B5:D3:AE:DB
SAMPLE
ドメインおよび
利用者サーバの
実在性を証明
機関の実在性を証明

対応Webサーバ

サーバ種別	バージョン等
Apache（mod_ssl）	Apache（mod_ssl-2.8.25-1.3.34）、apache_1.3.33+ssl_1.55 にて動作確認済。ただし脆弱性対策等の点から最新版での使用を推奨。
Apache-SSL	
Microsoft Internet Information Server	※動作確認中。
Netscape Enterprise Server	3.5.1 および 3.6にて動作確認済。
IBM HTTP Server	6.0.2以上。
Jakarta Tomcat	4.1.31および5.0.30について動作確認済。

推奨ブラウザ

分類	製品	詳細
PCブラウザ	Microsoft Internet Explorer	Windows2000、XP
	Opera	Ver.8
	Mozilla Firefox	Ver1.4
	Safari	ルート証明書搭載について交渉中 ※ルート証明書を手動登録することで対応可
携帯ブラウザ	NTTドコモ	P702iD、SH902iS、F902iS、P902iS、 N902iS、D902iS、SH702iS、N702iS SH902iSL、N902iX、D702iF、F882iES、 SH903i、P903i、D903i、F903i、 N903i、L601i(SIMPURE L1)
	au	W43H、W43CA、W45T、W42SA、W43SA
	Softbank	904SH、705T、905SH、705SH、705P、 810SH、811SH、910T、 705SC、706SC
組込ブラウザ	NetFrontSDK	Ver.3.2
電子メールソフト	オレンジソフト S/Goma	Ver.2.14PL8
PDA	順次搭載予定	ー

プロジェクトへの参加条件

- 対象
  - SINET加入機関のうち、
    - 大学, 短期大学, 高等専門学校, 大学共同利用機関
    - その他文部科学省の独立行政法人等
- 参加単位
  - ユニット毎に参加申し込みを行う。
    - 1大学(機関)1ユニットが原則。
    - 異なるドメインを用いる場合には、別途ユニットを組んで参加する。
  - H19年度当初は、審査処理等の都合により、受付ユニット数に制限あり
- 条件
  - PJ趣旨に賛同し、証明書利用結果についてのフィードバックを行うこと。
  - 証明書申請について責任を全うできること。
    - 利用者の本人性確認、実在性確認
  - 登録担当者が以下の環境を利用できること。
    - S/MIMEメーラ(申請ファイル送信時のデジタル署名)
    - Office XP以降のExcel(申請ファイルへのデジタル署名)

サーバ証明書の発行条件

- 対象サーバ
  - 属する機関が所有または管理するサーバ
  - サーバ認証を必要とするサーバ
- ドメイン
  - 属する機関の主たるドメイン
    - プロジェクト参加申込時に指定
- 注意
  - 下記のようなケースは対象外
    - 特定少数の検証者のみを対象としたサーバ
    - 検証者へのルートCA証明書の配布が容易に実現できる場合

プロジェクトスケジュール(予定)