サーバ証明書発行・導入における
啓発・評価研究プロジェクト

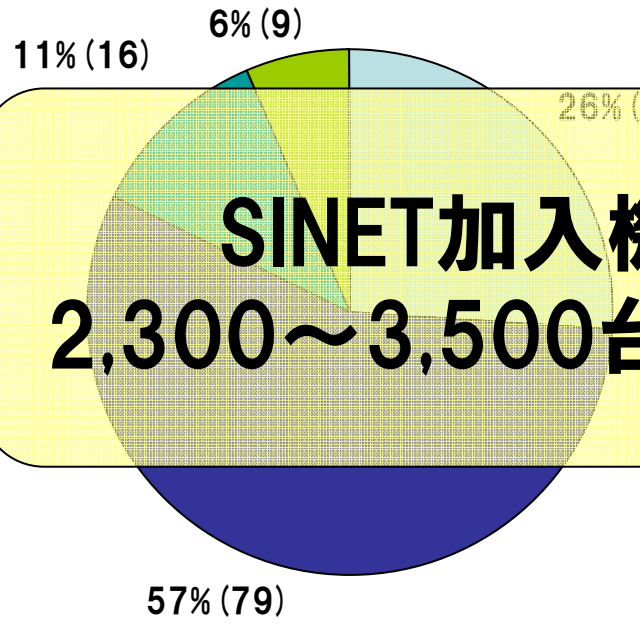
概要説明

平成19年5月28日

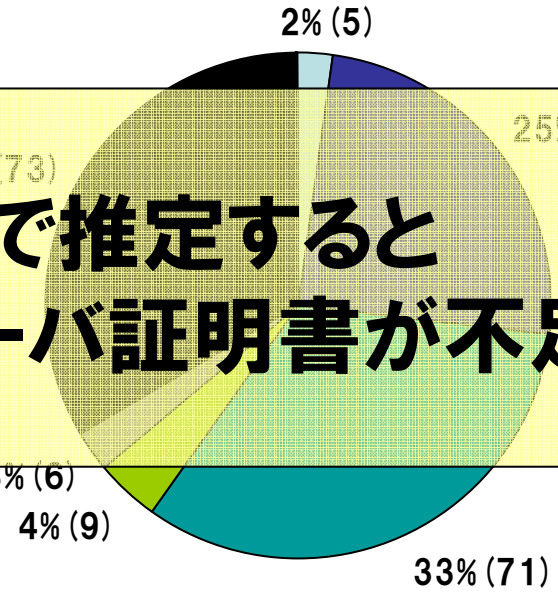
国立情報学研究所
学術情報ネットワーク運営・連携本部
認証作業部会

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

プロジェクトの概要

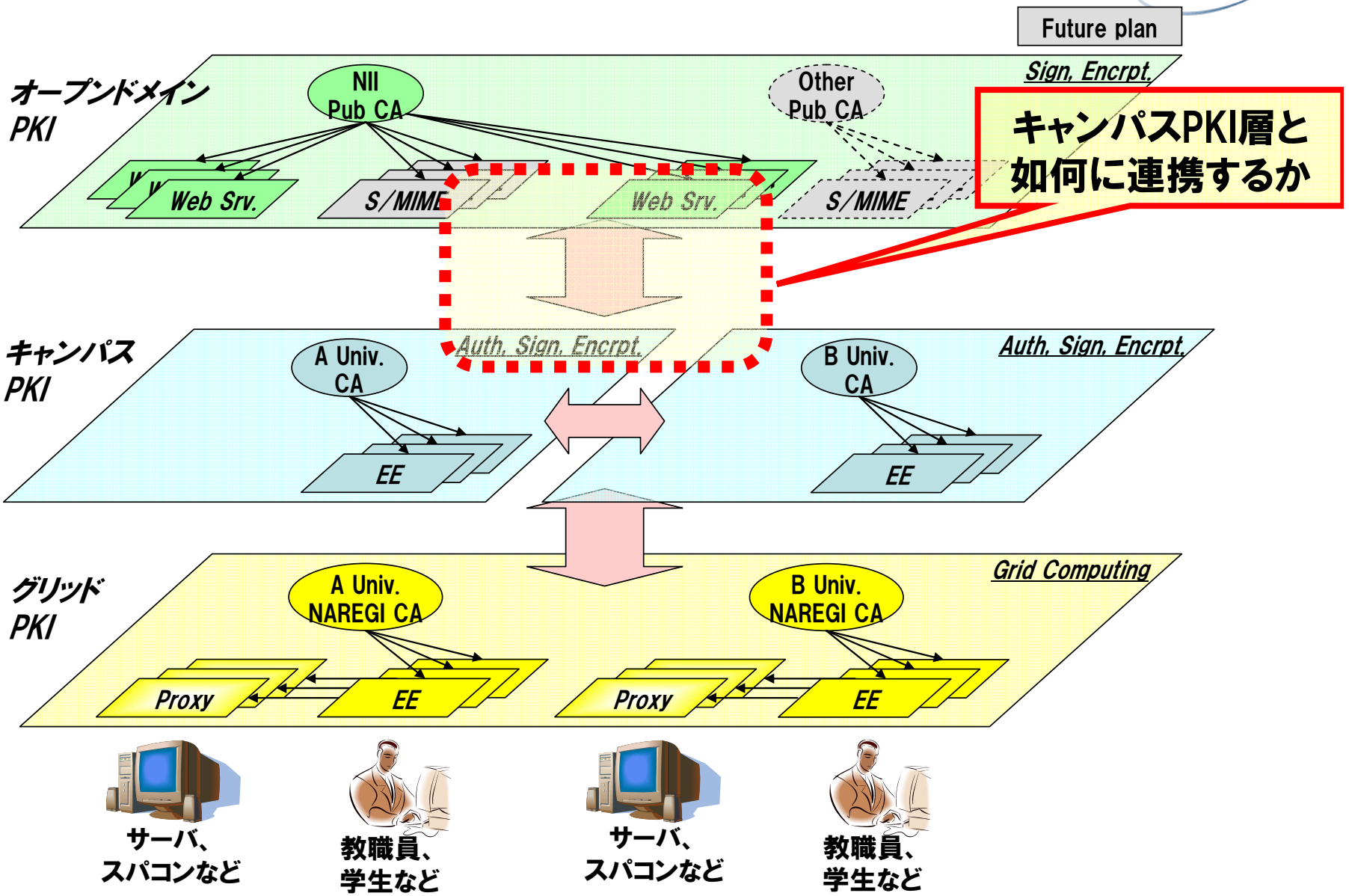
- 目的
  - 大学等のサーバ証明書の普及を推進
  - 認証局を用いた研究開発 ⇒ 登録発行業務の改善
  - 学術機関のWebサーバ信頼性向上
  - サーバ証明書の導入・運用ノウハウの共有
  - 参加者のサーバに対してのサーバ証明書無償配布
- 期間
  - 2007/04/01～2009/03/31
- ゴール
  - H19年度: サーバ証明書の普及が進まない理由・課題の整理
  - H20年度: サーバ証明書の普及促進の仮説・立証
  - 将来的に: キャンパスPKI層を活用した証明書発行業務の自動化
- 主な作業
  - プロジェクト参加機関の募集
  - 各登録担当者へのS/MIME証明書発行
  - 参加機関が管理するサーバに対するサーバ証明書の発行
  - 参加機関加入者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）



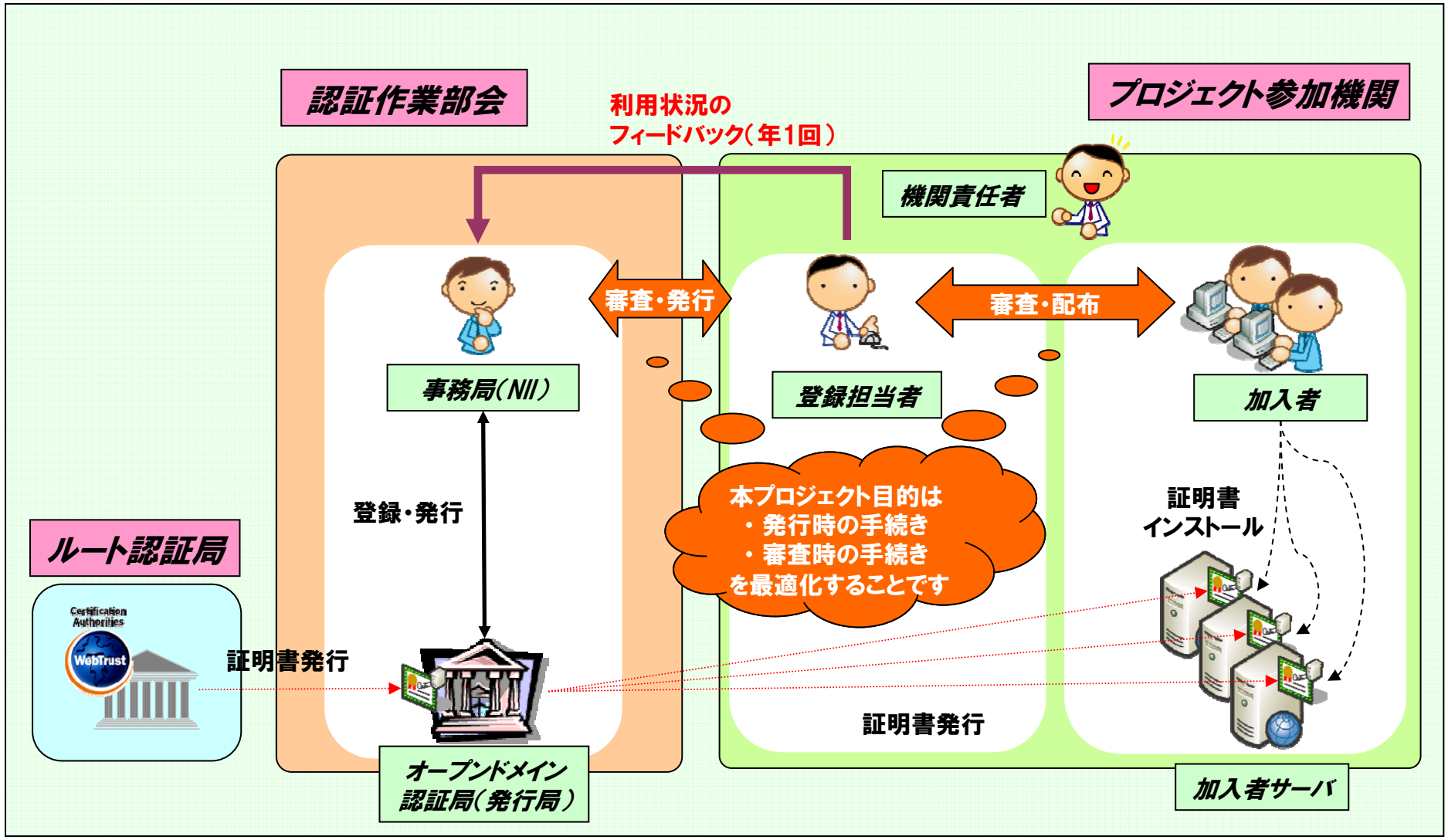
証明書発行の基本方針

- 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

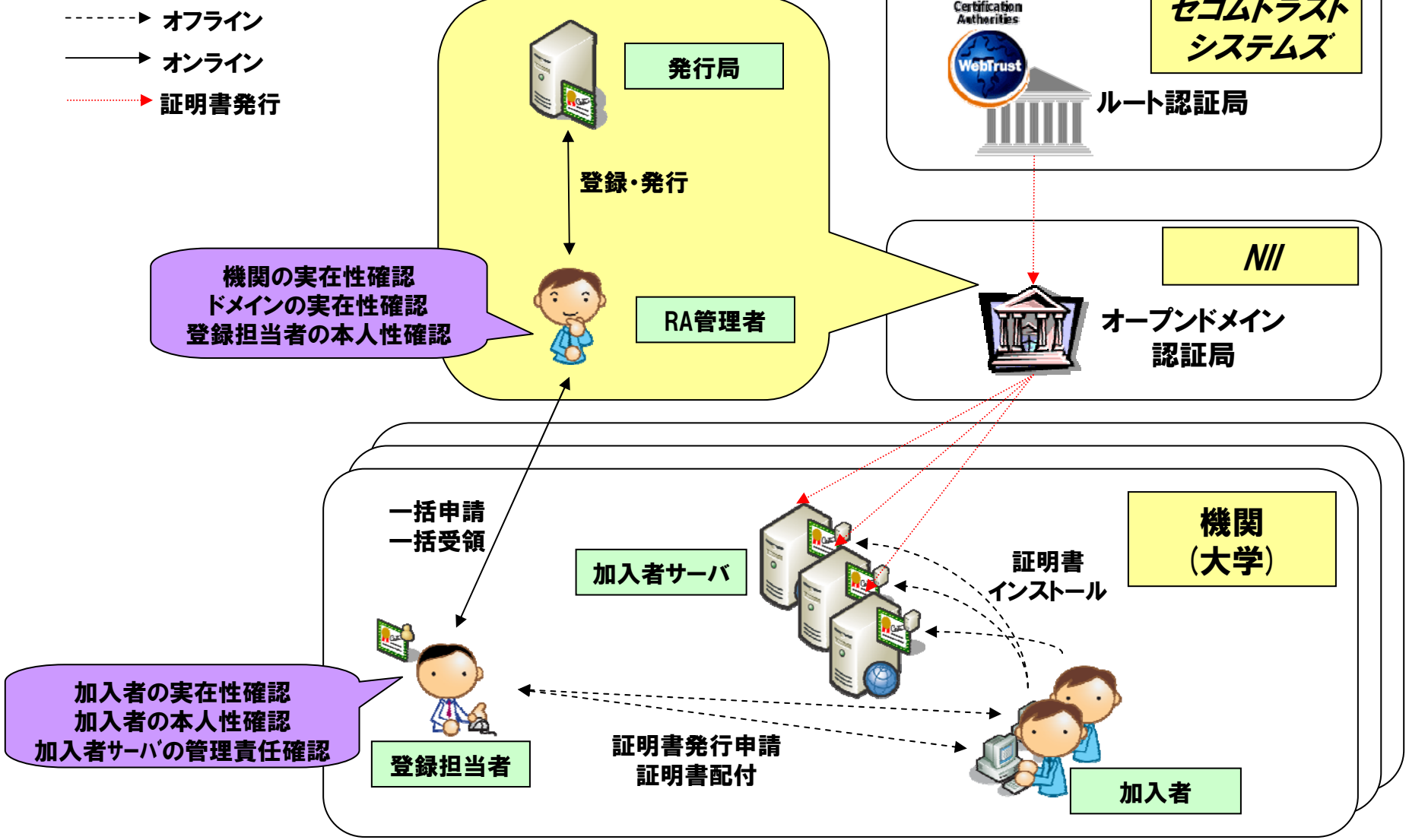
プロジェクトで利用する用語と役割

組　織	用語	説　明
NII	オープンドメイン認証局（発行局）	本プロジェクトで使用する，サーバ証明書を発行するための認証局。Web Trust for CAに準拠しており，世界的に信頼できる証明書の発行が可能です。また，この証明書は，主要なウェブブラウザ等のPKIアプリケーションに標準でルート認証局が搭載されているため、商用のサーバ証明書と同様に利用することができます。
	事務局	プロジェクト参加申請、証明書発行申請にあたり、審査業務を行なうNIIの事務窓口です。
各大学	機関責任者	本プロジェクト参加にあたり，各機関で選出いただく代表者の方。課長職相当または准教授以上の方にお願いいたします。
	登録担当者	本プロジェクトの参加機関側の事務的な窓口をお願いする方。大学の規模に応じて複数名選出していただくことが可能です。
	加入者	Webサーバを管理し，本プロジェクトのサーバ証明書を利用される方。プロジェクト参加機関内の教職員の方であれば，どなたでも加入者となれます。
	加入者サーバ	加入者の方が管理するWebサーバ。
不特定多数	利用者	PKI加入者サーバにアクセスする，不特定多数の方々のことを，この説明では利用者と呼びます。利用者は、ウェブブラウザ等の標準の機能を利用して加入者サーバの証明書を検証いたします。

プロジェクト全体概要


認証作業部会
利用状況の
フィードバック（年1回）
プロジェクト参加機関
機関責任者
審査・発行
審査・配布
事務局（NII）
登録担当者
加入者
登録・発行
本プロジェクト目的は
・発行時の手続き
・審査時の手続き
を最適化することです
証明書
インストール
ルート認証局
Certification Authorities
WebTrust
証明書発行
証明書発行
オープンドメイン
認証局（発行局）
加入者サーバ

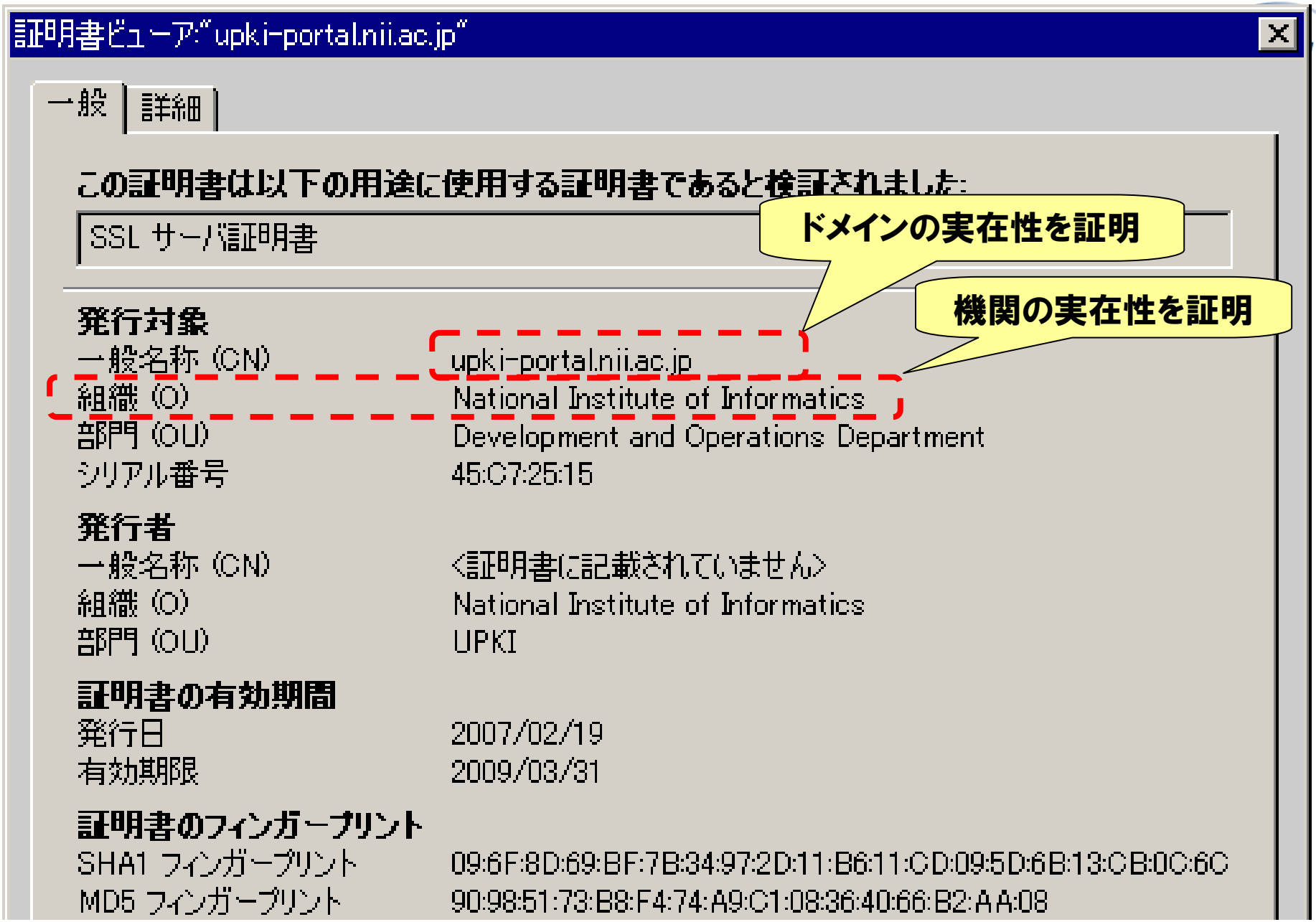
証明書発行の流れ


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
登録担当者の本人性確認
Certification Authorities
WebTrust
セコムトラスト
システムズ
ルート認証局
NII
オープンドメイン
認証局
一括申請
一括受領
加入者サーバ
証明書
インストール
機関
(大学)
加入者の実在性確認
加入者の本人性確認
加入者サーバの管理責任確認
登録担当者
証明書発行申請
証明書配付
加入者

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	機関責任者	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	○		○		○			
機関責任者	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					× →	○		
加入者	本人性確認	×		○		× →		○	
	実在性確認	×		○		× →		○	
加入者サーバ	本人性確認		○		○				○
	管理責任確認		○		○			○ ←	×

「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:"upki-portal.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
ドメインの実在性を証明
機関の実在性を証明
発行対象
一般名称 (CN) upki-portal.nii.ac.jp
組織 (O) National Institute of Informatics
部門 (OU) Development and Operations Department
シリアル番号 45:C7:25:15
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 09:6F:8D:69:BF:7B:34:97:2D:11:B6:11:CD:09:5D:6B:13:CB:0C:6C
MD5 フィンガープリント 90:98:51:73:B8:F4:74:A9:C1:08:36:40:66:B2:AA:08

動作確認済みWebサーバ

- Apache(mod_ssl) ※注1）
- Apache-SSL ※注1）
- Microsoft Internet Information Server 5.0
- Microsoft Internet Information Server 6.0
- IBM HTTP Server 6.0.2 以上
- Jakarta Tomcat ※注2）

※注1)Apacheバージョンについて
Apache(mod_ssl-2.8.25-1.3.34)、apache_1.3.33+ssl_1.55より動作確認を行っています。
古いバージョンにつきましては、深刻な脆弱性が報告されていますので、最新版をご使用いただくことをお勧めいたします。
※注2)Jakarta Tomcatについて
Jakarta Tomcat 4.1.31 と Jakarta Tomcat 5.0.30につきましての動作確認を行っています。

推奨ブラウザ

- Netscape Communicator 4.78 以上
- Netscape Communicator 7 以上
- Microsoft Internet Explorer 5.5 以上
- Microsoft Internet Explorer 5.2 (MacOS) 以上
- Opera 7.6 以上
- FireFox 1.0 以上
- Safari 1.2.2 以上

※SafariはMacのOS X以上に標準搭載されているブラウザ。OS X以前は、IE などの利用になります。

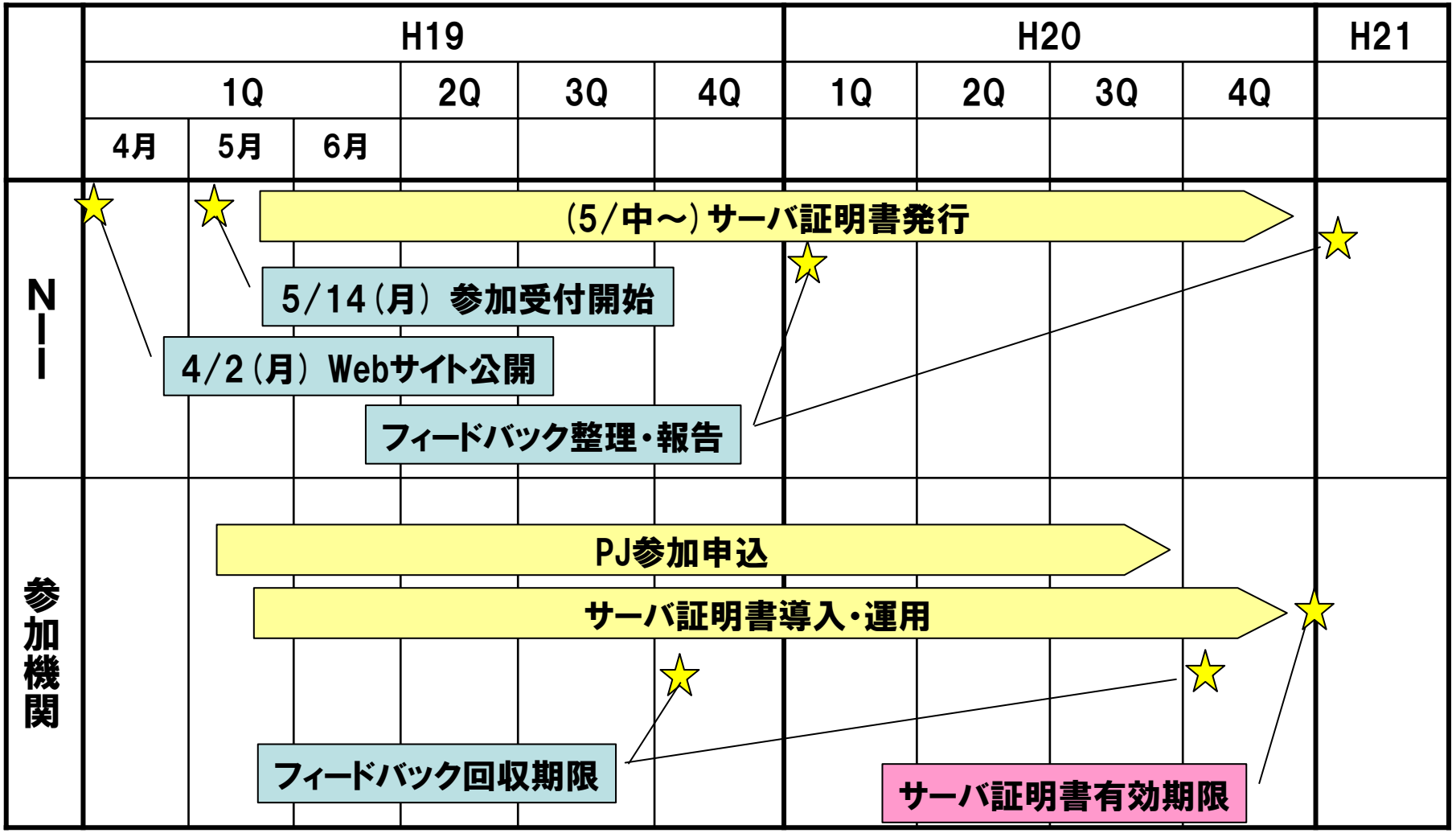
プロジェクトへの参加条件

- 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
    - その他の独立行政法人等
- 参加単位
  - 機関毎に参加申し込みを行う。
    - 異なるドメインを用いる場合には、別途相談。
  - H19年度当初は、審査処理等の都合により、受付機関数に制限あり
- 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。
    - 加入者の本人性確認、実在性確認、加入者サーバの管理責任確認
    - 申請書類の保管
  - 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
    - 原則としてac.jpドメイン
    - プロジェクト参加申込時に指定
- 注意
  - 次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



ありがとうございました