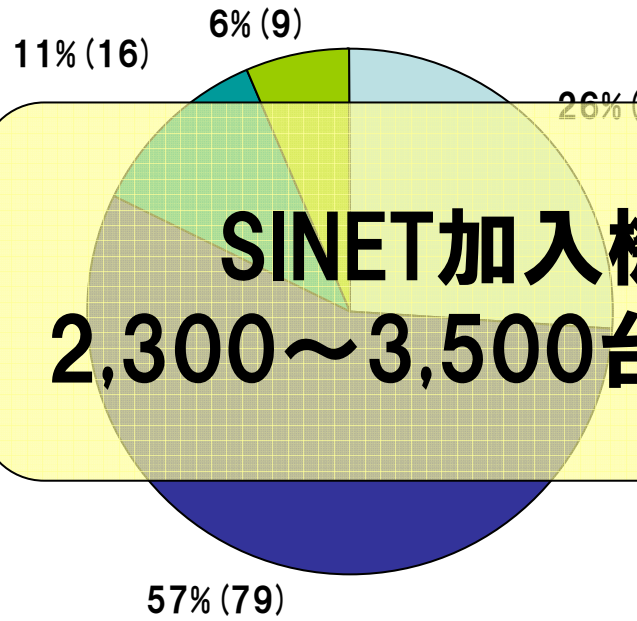
サーバ証明書発行プロジェクト
－ UPKIイニシアティブ －

名古屋大学情報連携基盤センター
国立情報学研究所学術情報ネットワーク運営・連携本部（客員）

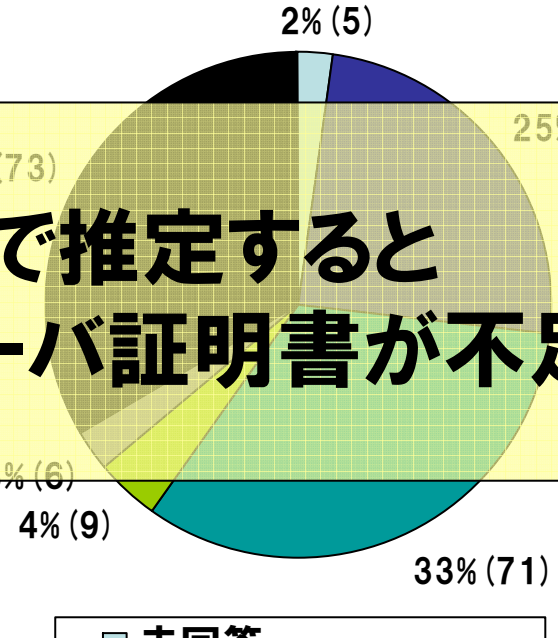
平野 靖

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

認証局を用いた評価研究

体験を通じて啓発

- 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

UPKIとは

- **大学間連携のための全国共同電子認証基盤**
  - 大学が有する教育研究用計算機，電子コンテンツ，ネットワークを**安全・安心**に有効活用するための**電子認証基盤の構築**
    - 最先端学術研究の加速支援
    - 学術人材の（物理的・仮想的）流動への対応
- U+PKI
  - University　／Universal　　／Ubiquitous
    大学の　　汎用の・全世界の　いつでもどこでも
  - PKI（公開鍵認証基盤）
    - ただしPKIに限定せず認証技術を幅広く扱う

UPKI:体制と効果

- 体制:
  - UPKIプロジェクト:7大学情報基盤センターとNII
  - UPKIイニシアティブ:全国の学術機関

- 効果
  - 大学間の相互認証
    → 研究資源、教育コンテンツの有効活用(e-learning, 単位互換)
  - 電子署名・暗号化
    → 情報漏洩、なりすましの防止によるセキュリティ強化
    研究成果の真正性の証明
    電子決済・電子回覧による効率化
  - ネットワークローミング → 無線LAN, 公衆Web端末
  - グリッドコンピューティング
    → 7大学スパコンリソースを統合
    京速コンピュータ時代へ向けての利用者管理基盤

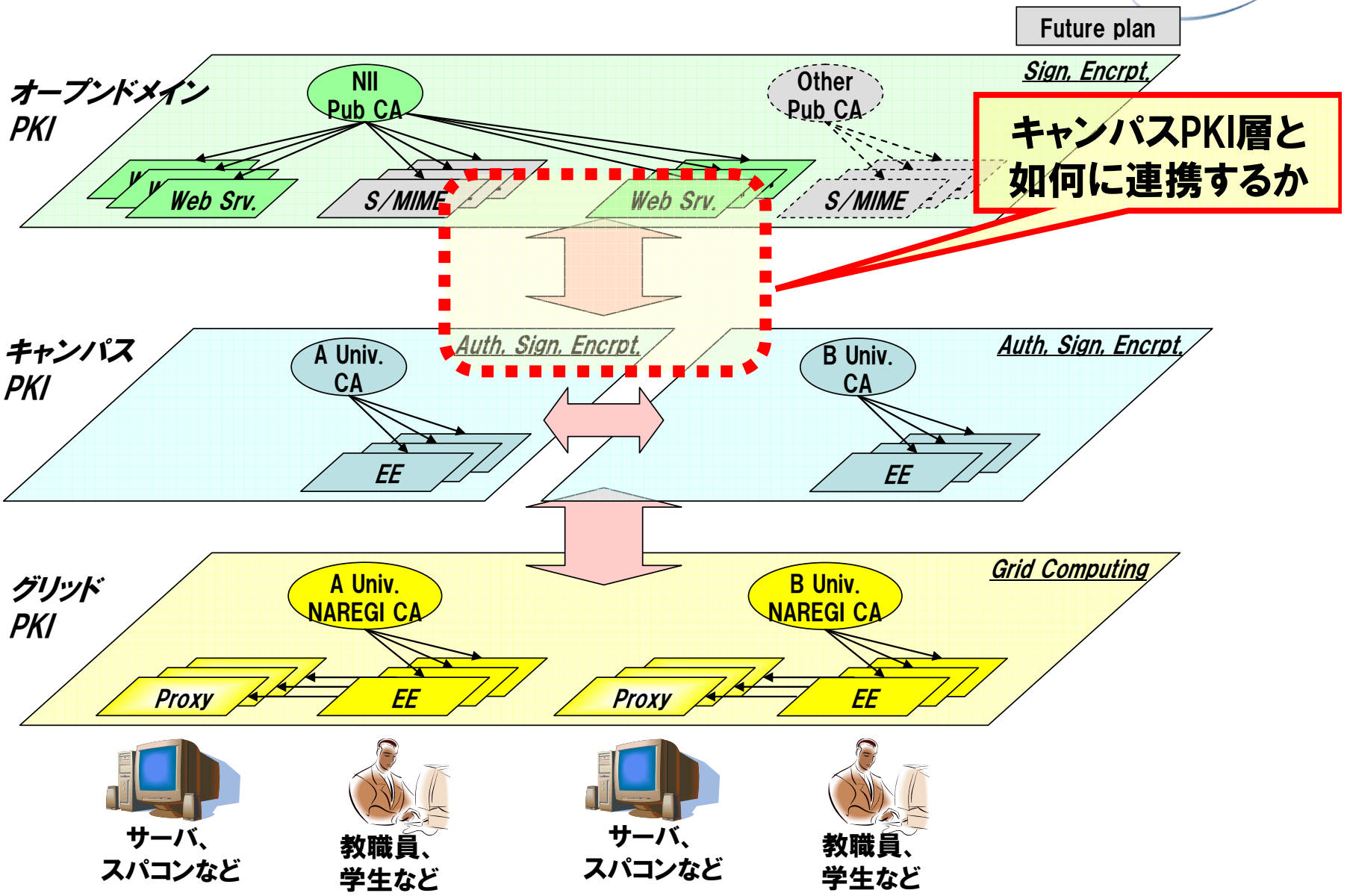
PKIで何ができるのか？

プライバシーの侵害や情報漏洩の防止が可能

- **盗聴**：機密情報が悪意の第三者に知られ，盗まれること
- **なりすまし**：悪意の第三者が他人になりすまし，情報入手などを図ること
- **改ざん**：悪意の第三者が機密情報を故意に変更すること
- **事後否認**：当事者間がそのやり取りそのものを否認すること．送信者が送信行為を否認 or 受信者が受信行為を否認

参考　小松文子：PKIハンドブック，ソフト・リサーチ・センター，2004，東京

UPKIにおける位置づけ（ゴール）



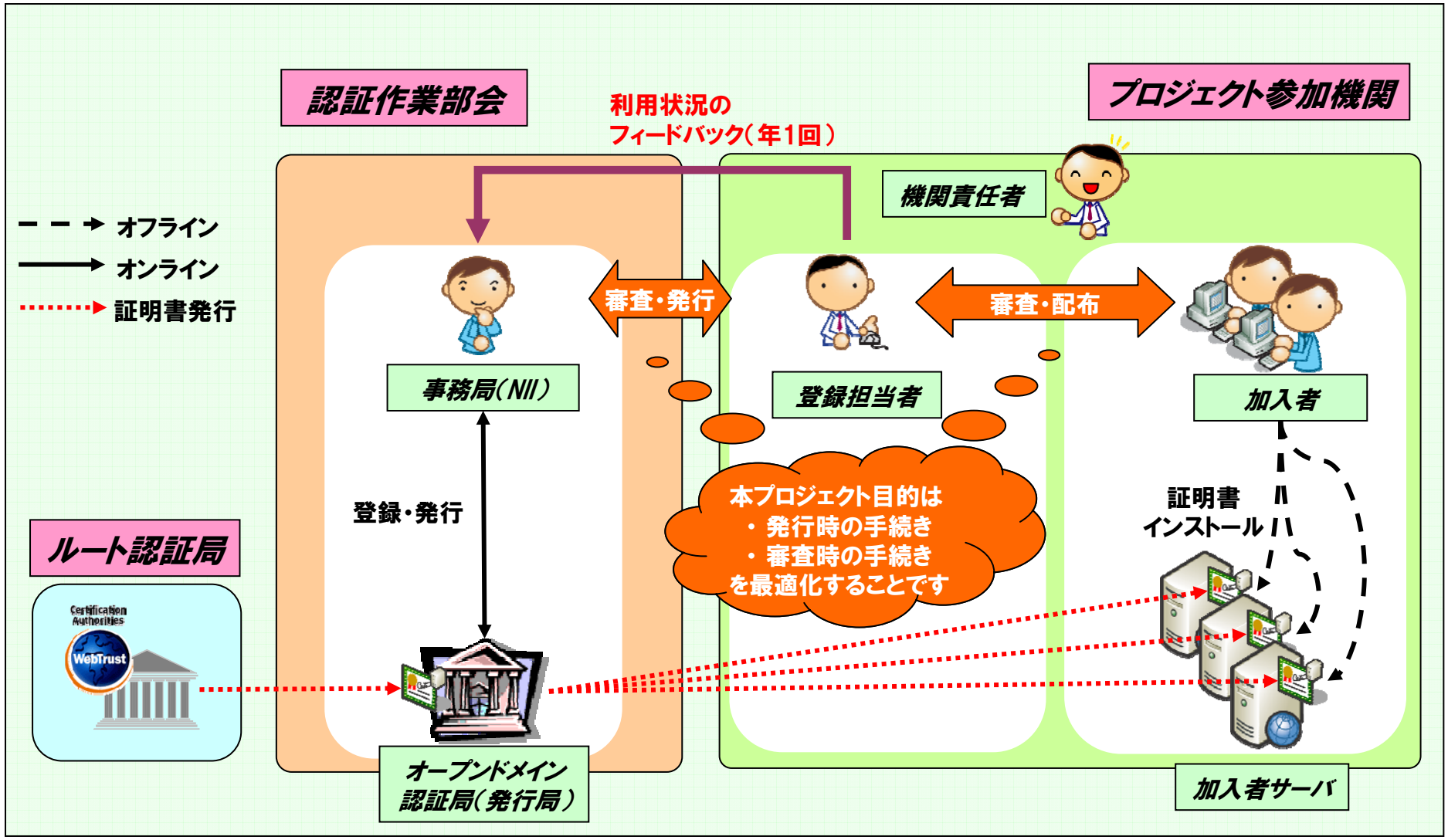
証明書発行の基本方針

- 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

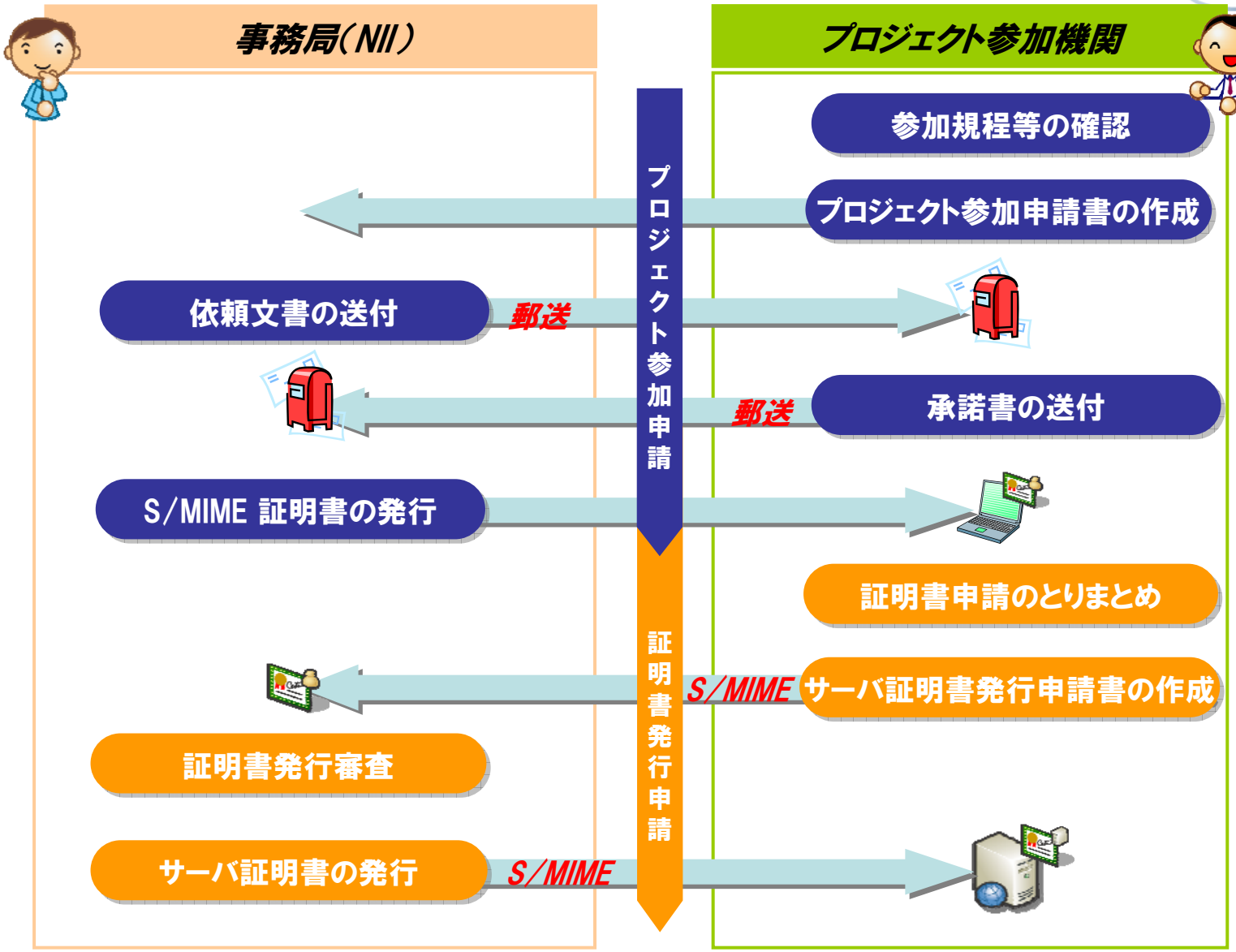
プロジェクトで利用する用語と役割

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。

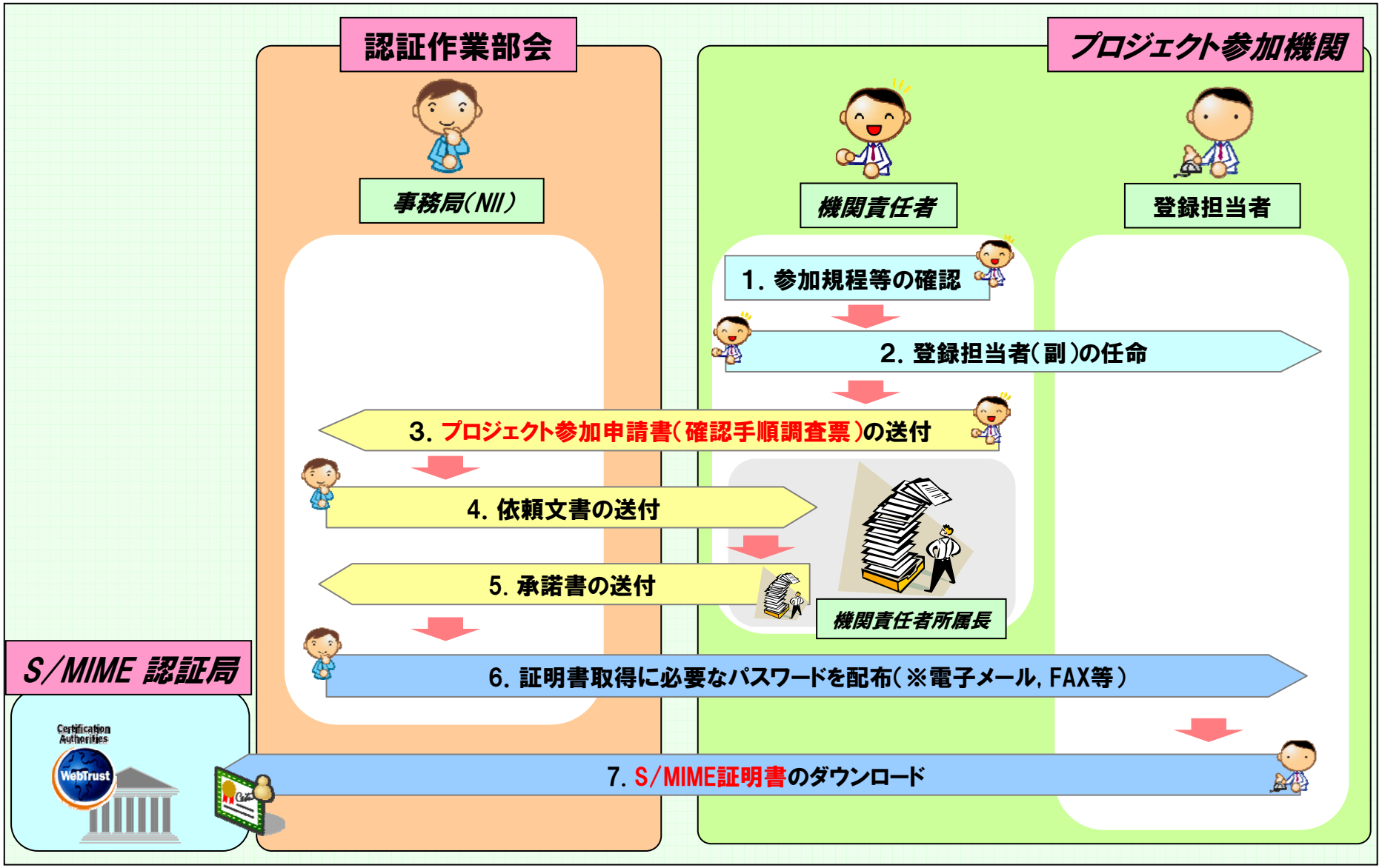
プロジェクト全体概要


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
オフライン
オンライン
証明書発行
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
オープンドメイン
認証局（発行局）
加入者サーバ

事務フローの概要


事務局(NII)
プロジェクト参加機関
参加規程等の確認
プロジェクト参加申請書の作成
プロジェクト参加申請
依頼文書の送付
郵送
郵送
承諾書の送付
S/MIME 証明書の発行
証明書申請のとりまとめ
証明書発行申請
S/MIME
サーバ証明書発行申請書の作成
証明書発行審査
サーバ証明書の発行
S/MIME

プロジェクト参加申請フロー
（プロジェクト参加時のみ）



プロジェクト参加申請の説明

（プロジェクト参加時のみ）

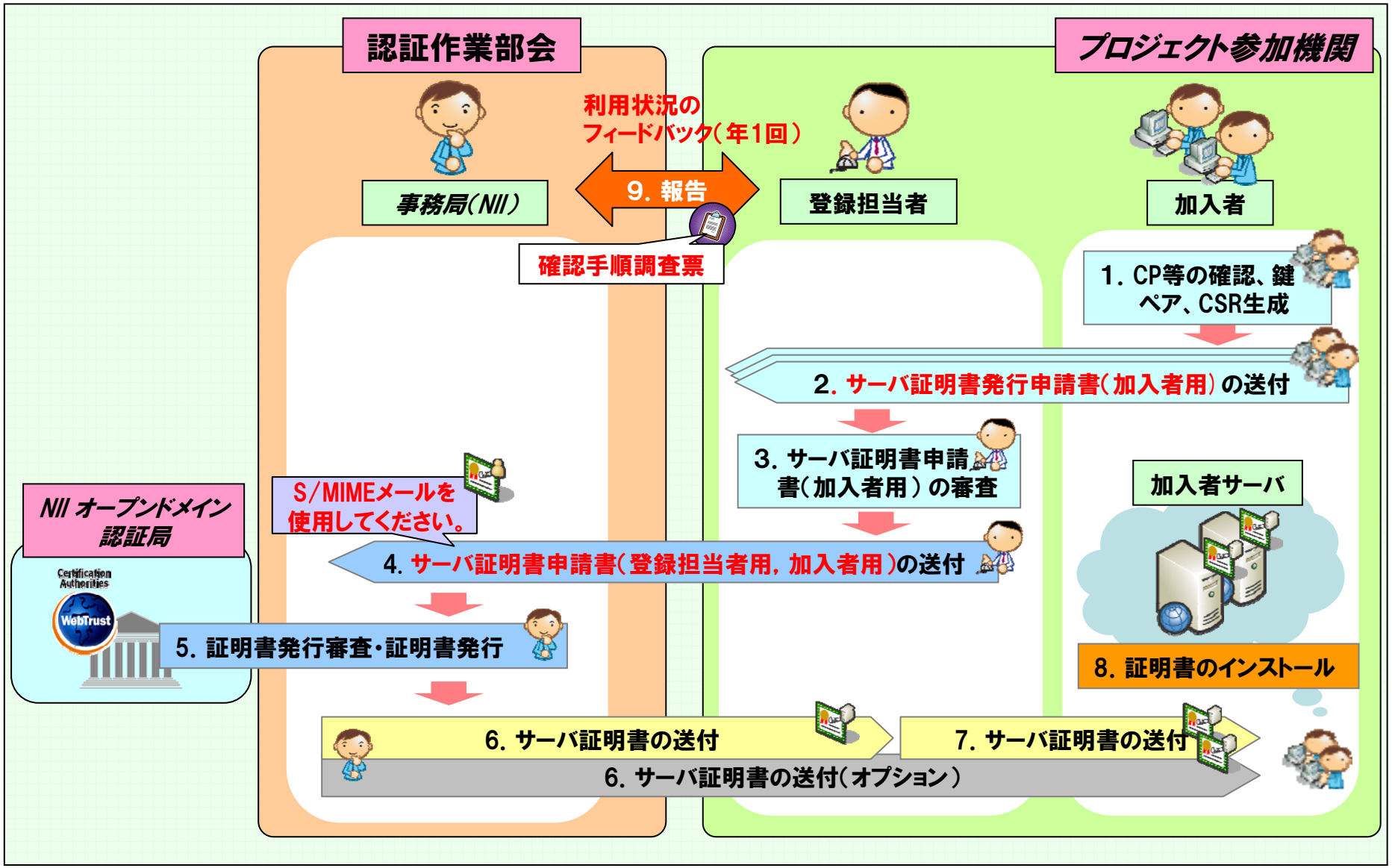
No.	項　目	担　当	説　明
1	参加規程等の確認	機関責任者	次の書類を十分に理解し，承諾してください。 ・本プロジェクト参加規程 ※1 ・本プロジェクトサーバ証明書利用規定※1 ・本認証局証明書ポリシー (Certificate Policy) ※2 ・本電子認証基盤認証運用規程 (Certification Practice Statement) ※2
2	登録担当者の任命	機関責任者	登録担当者(正、副)の任命を行なってください。
3	プロジェクト参加申請書の送付	機関責任者	プロジェクト参加申請書および確認手順調査票をご記入の上、事務局(NII)宛てに同申請書を郵送してください。なお、プロジェクト申請書には機関責任者の捺印が必要です。
4	委嘱状の送付	事務局(NII)	機関責任者の所属長宛に依頼文書を郵送いたします。
5	同意書の送付	機関責任者 (の所属長)	委嘱内容を確認し、事務局(NII)宛てに承諾書を郵送してください。
6	証明書に必要なパスワードを配布	事務局(NII)	同意書の確認後、プロジェクト参加申込書に記載されている登録担当者に対し、パスワードを電子メールおよびFAX等で配布いたします。 ※このパスワードは、S/MIME※3証明書の取得時に必要です。
7	S/MIME証明書のダウンロード	登録担当者	事務局(NII)から、送付されたパスワードをもとに、S/MIME証明書を取得してください。また、ご利用のメーラにS/MIME証明書を設定してください。

※1 https://upki-portal.nii.ac.jp

※2 https://repo1.secomtrust.net/sppca/NII/ODCA/index.html

※3 電子メールの暗号化、署名方式の一つ。
本プロジェクトでは、証明書発行申請を行なう際に、電子メールに署名してください。

サーバ証明書発行申請フロー
（証明書の申請都度）



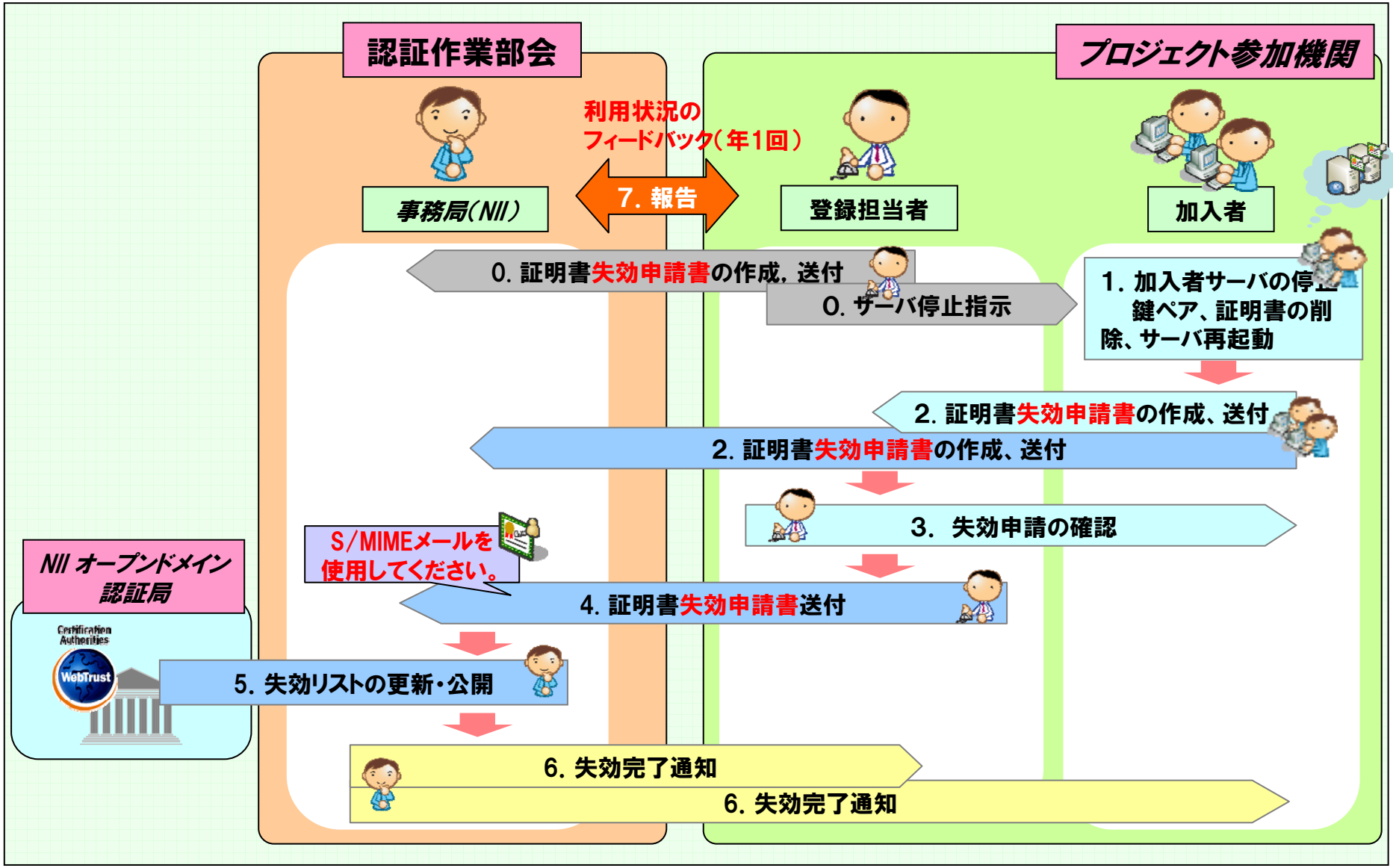
サーバ証明書発行申請の説明

（証明書の申請都度）

No.	項　目	担　当	説　明
1	CP等の確認、 鍵ペア、CSRの生成	加入者	サーバ証明書の発行に必要な情報を生成してください。 ・鍵ペア（秘密鍵は厳重に管理してください。） ・CSR（Certificate Sign Request）
2	サーバ証明書発行申請書 （加入者用）の送付	加入者	サーバ証明書発行申請書（加入者用）をご記入の上、登録担当者に同申請書をご送付ください。
3	サーバ証明書申請書 （加入者用）の審査	登録担当者	サーバ証明書発行申請書（加入者用）の記載内容をプロジェクト参加申請時に記載した審査内容に基づき審査し、サーバ証明書発行申請書（登録担当者用）をご作成ください。
4	サーバ証明書申請書 （加入者用、登録担当者用）の送付	登録担当者	サーバ証明書発行申請書（加入者用，登録担当者用）を取りまとめて事務局（NII）にご送付ください。 ※S/MIMEメール（署名）を使用してください。
5	証明書発行審査・証明書発行	事務局（NII）	サーバ証明書発行申請書を審査します。 ※申請内容に問題がある場合は、登録担当者にご連絡いたします。
6	サーバ証明書の送付	事務局（NII）	証明書を登録担当者にお送りいたします。オプションを選択することで、同時に加入者に対し、証明書を配布することも可能です。
7	サーバ証明書の送付	登録担当者	6のオプションを選択しない場合、登録担当者から加入者に証明書を配布いたします。
8	証明書のインストール	加入者 サーバ	証明書のインストールを行います。
9	報告（年1回）	登録担当者	証明書の利用状況について、事務局（NII）に報告します。 確認手順調査票を記入し提出します

証明書失効申請フロー

※秘密鍵の漏洩，証明書記載情報の変更，運用停止等※



証明書失効申請の説明

（秘密鍵の漏洩，証明書記載情報の変更，運用停止等）

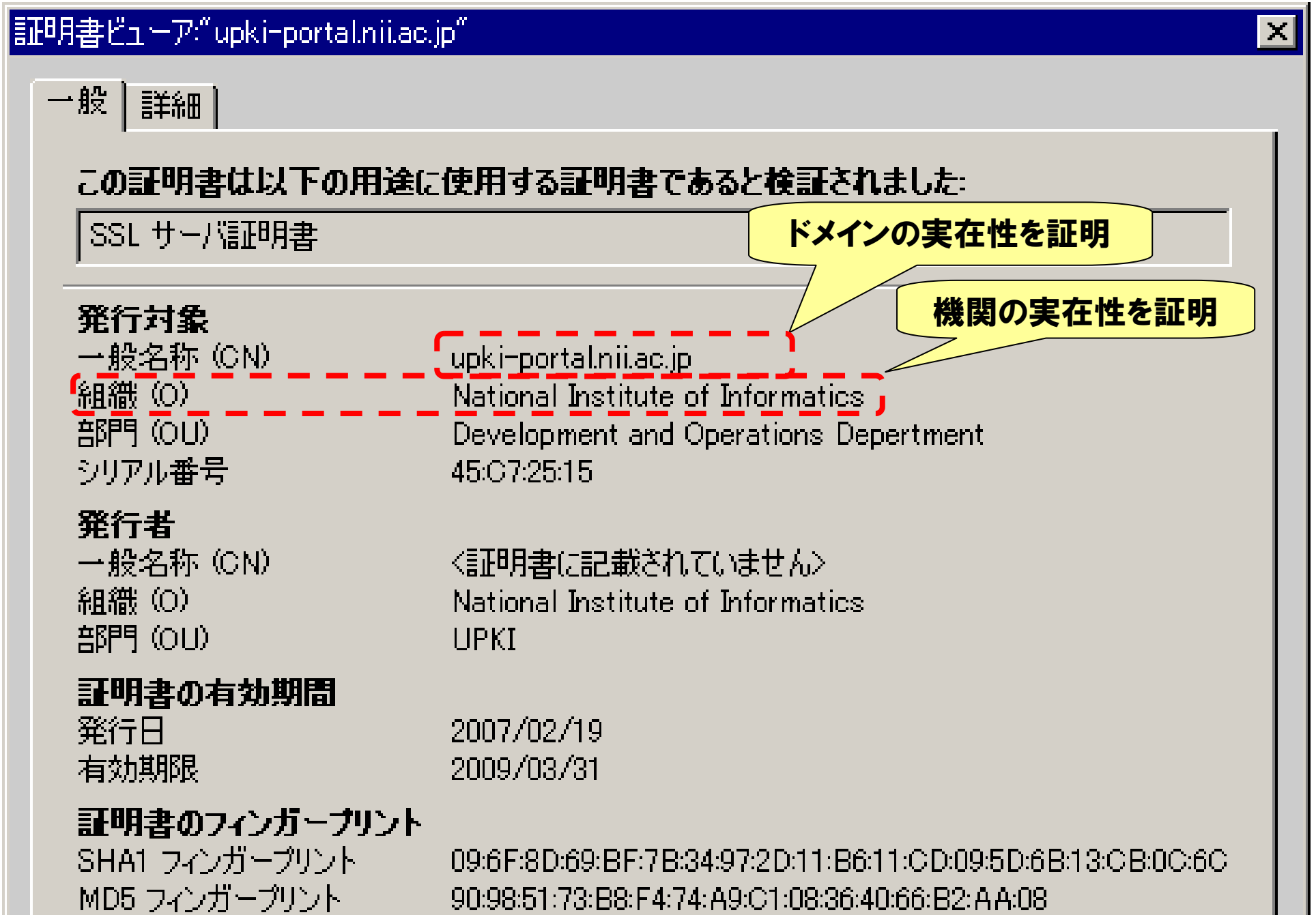
No.	項　目	担当	説　明
0※	証明書失効申請所の作成，送付	登録担当者	サーバ証明書失効申請書をご記入の上、登録担当者およびNII事務局に同申請書をご送付ください。
	サーバ停止支持	登録担当者	加入者に対し、サーバ証明書の失効を通知し、サーバ証明書に関する削除するように指示してください。
1	加入者サーバの停止、 鍵ペア、証明書の削除、 サーバ再起動	加入者 サーバ	鍵ペアやサーバ証明書等、サーバ証明書に関する情報を削除し、サーバを再起動してください。
2	証明書失効申請書の作成、送付	加入者	サーバ証明書失効申請書をご記入の上、登録担当者およびNII事務局に同申請書をご送付ください。
3	失効申請の確認	登録担当者	サーバ証明書失効申請書を受領後、加入者に速やかに失効申請に関して規定の確認を行い同申請書にその内容を記載する。事務局（NII）に同申請書を送付する。
4	サーバ証明書の失効申請書送付	登録担当者	サーバ証明書失効申請書を事務局（NII）にご送付ください。 ※S/MIMEメール（署名）を使用してください。
5	失効リストの更新・公開	事務局（NII）	失効申請書に従い証明書を失効します。
6	失効完了通知	事務局（NII）	失効完了したことを登録担当者と加入者に送付いたします。

※ 網掛けは、登録担当者が強制的に加入者サーバの証明書の利用を失効させる際に行なう処理です。
この場合、No.2 ～ No.4の手順は必要ありません。

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 Depertment
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

対応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
  - 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