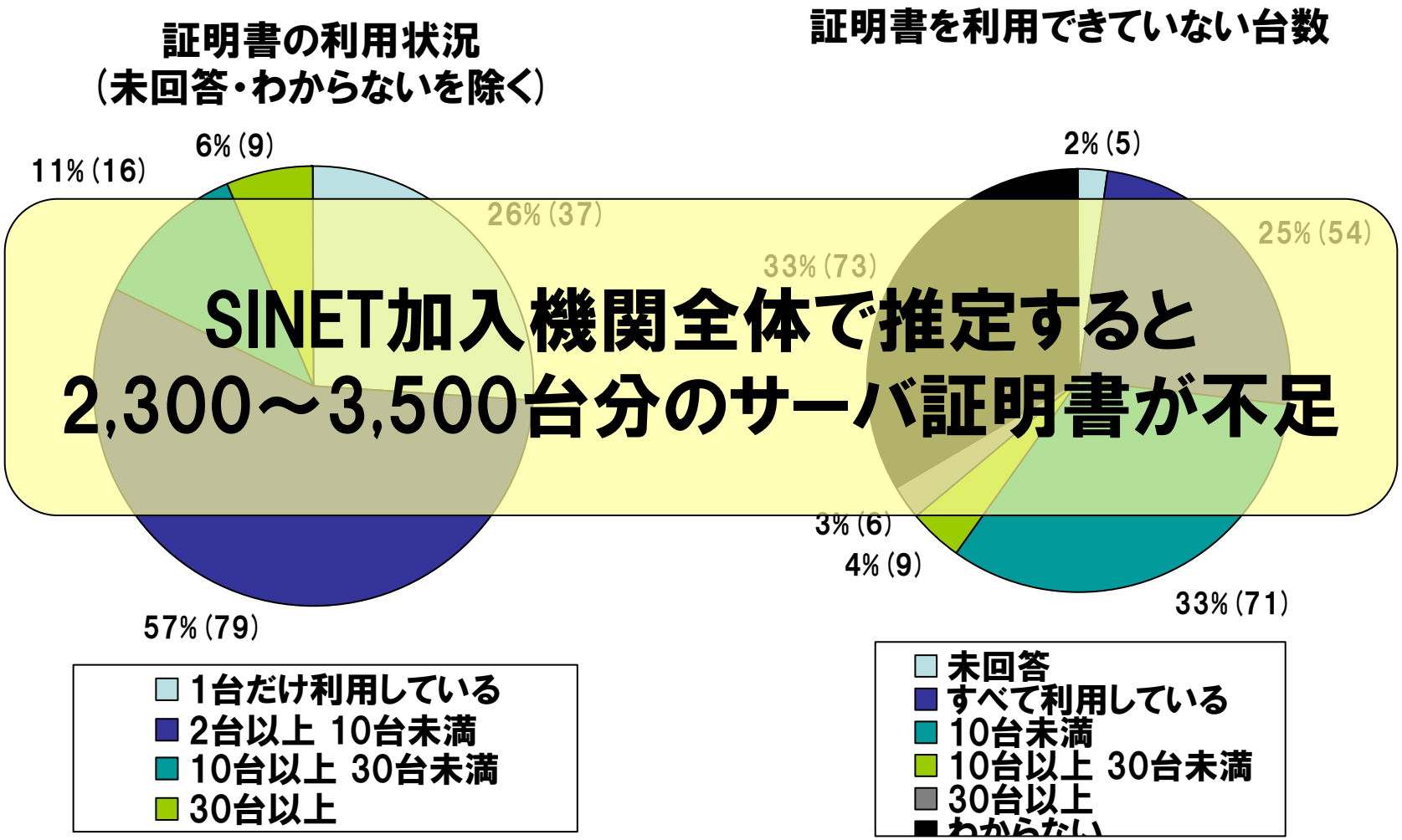
サーバ証明書発行・導入の啓発・評価研究プロジェクト

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

- 背景
  - 大学におけるサーバ証明書の現状
- SSL/TLSサーバ認証とは
  - SSL/TLSサーバ認証の機能と仕組み
  - オレオレ認証局とオープンドメイン認証局
- サーバ証明書プロジェクトのご紹介
  - プロジェクト概要
  - プロジェクト諸元

大学等におけるサーバ証明書の実態

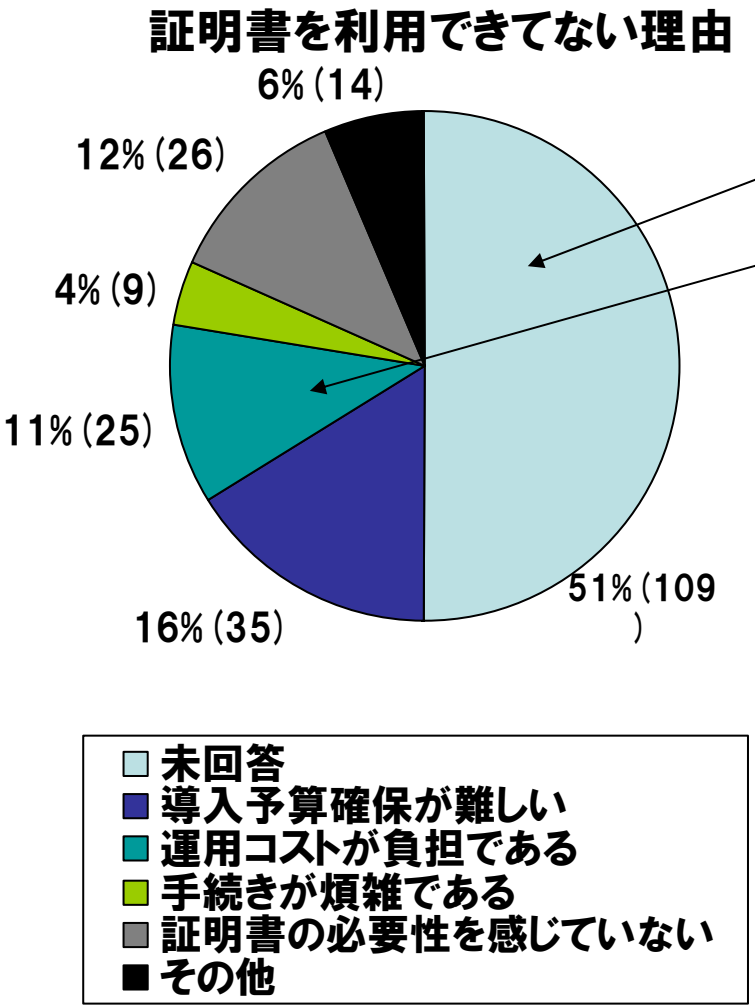


SINET加入機関全体で推定すると
2,300～3,500台分のサーバ証明書が不足

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?

大学におけるサーバ証明書の重要性

- 多くのネットワークサービスに不可欠なユーザ認証
  - SSL-VPN, WebMail, POP3S, IMAPS, 802.1X (EAP-TLS, PEAP, EAP-TTLS), etc.
  - 多くのサービスがSSL/TLSサーバ認証をサポート
- ネットワーク越しに認証する時の脅威
  - 通信経路上での盗聴　→**通信経路の暗号化**
  - なりすましサーバへの情報流出　→**サーバの真正性確認**

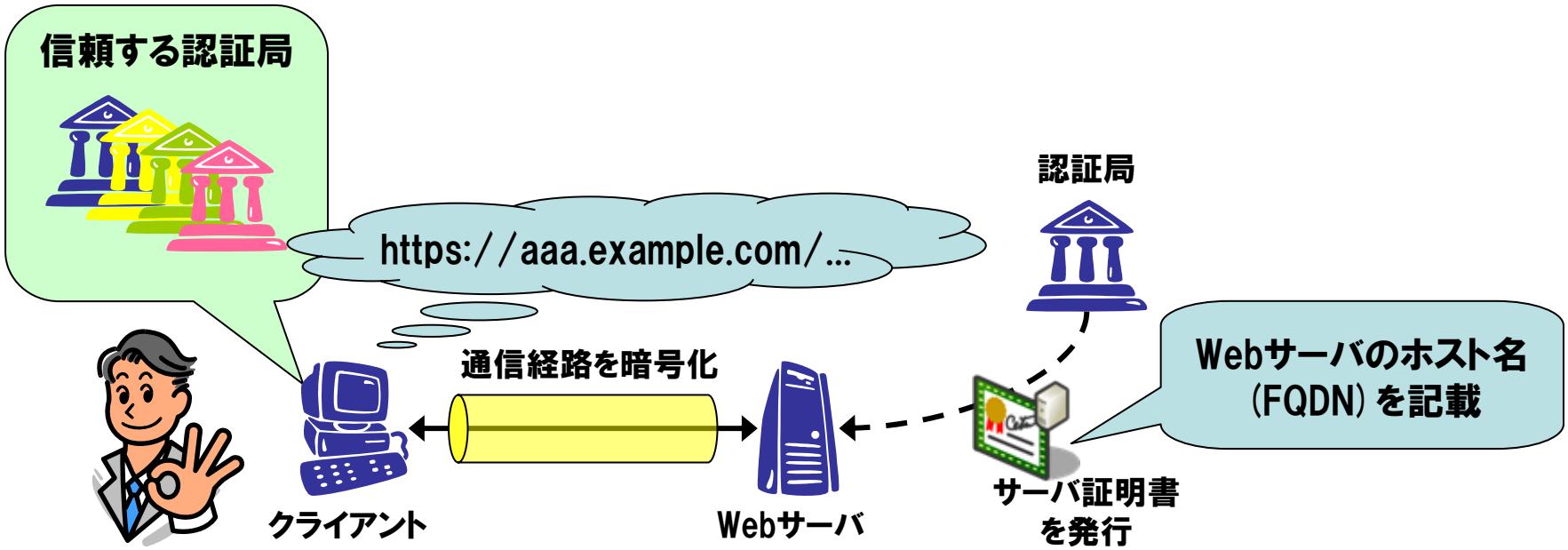
企業に限らず大学でもサーバ証明書が必須！

…でも身内だけならオレオレ証明書でいいんじゃないの？

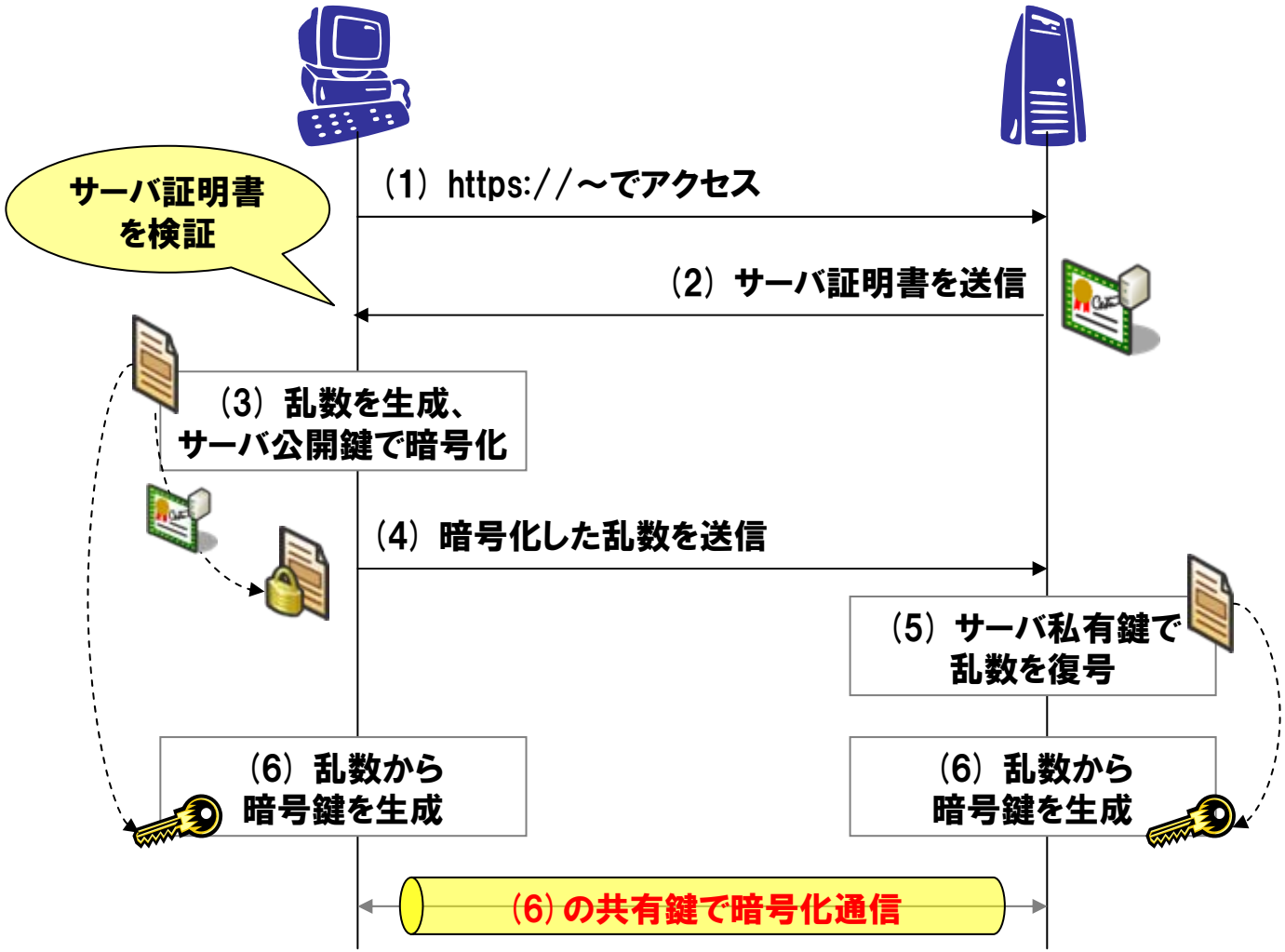
- 背景
  - 大学におけるサーバ証明書の現状
- SSL/TLSサーバ認証とは
  - SSL/TLSサーバ認証の機能と仕組み
  - オレオレ認証局とオープンドメイン認証局
- サーバ証明書プロジェクトのご紹介
  - プロジェクト概要
  - プロジェクト諸元

SSL/TLSサーバ認証とは

- サーバの真正性を確認し、通信経路を暗号化する技術
  - 信頼する認証局から発行された証明書を使って確認
    - 証明書にWebサーバのホスト名(FQDN)を記載
    - 下例で言えば “aaa.example.com”
  - 認証時に生成した暗号鍵で通信中のデータを暗号化



サーバ認証から暗号鍵の共有まで



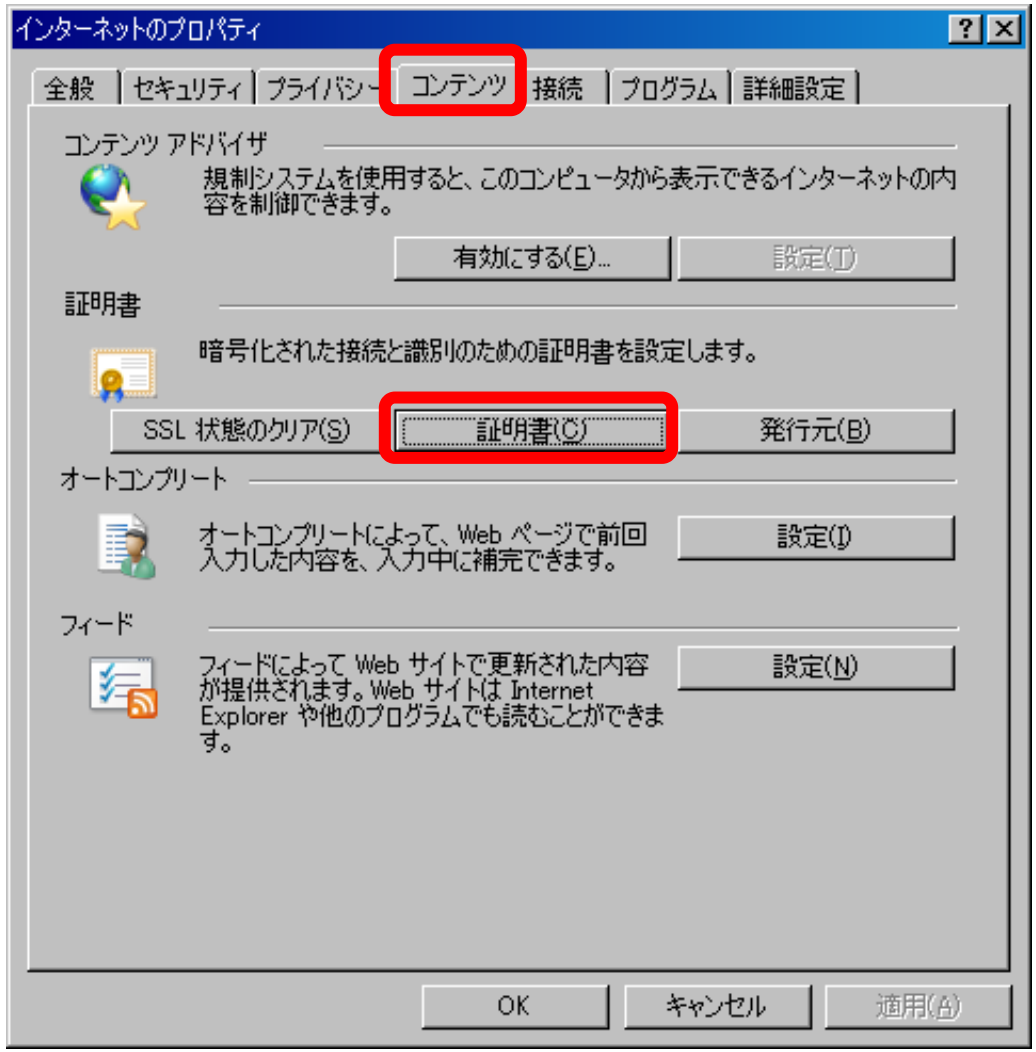
サーバ証明書を発行する認証局

- 予めクライアント側のPKIアプリケーション
  が信頼している認証局でなければならない。
- 主要なPKIアプリケーションにはいくつかの
  認証局が予め登録されている。
  - IE:「信頼されたルート証明機関」
  - Firefox:「証明書マネージャ」
- ユーザが後付けで認証局を登録することも
  可能ですが…
  - 安全を保証できない認証局を登録することは
    非常に危険!!
  - 安全を保証できる認証局だと判断できますか?

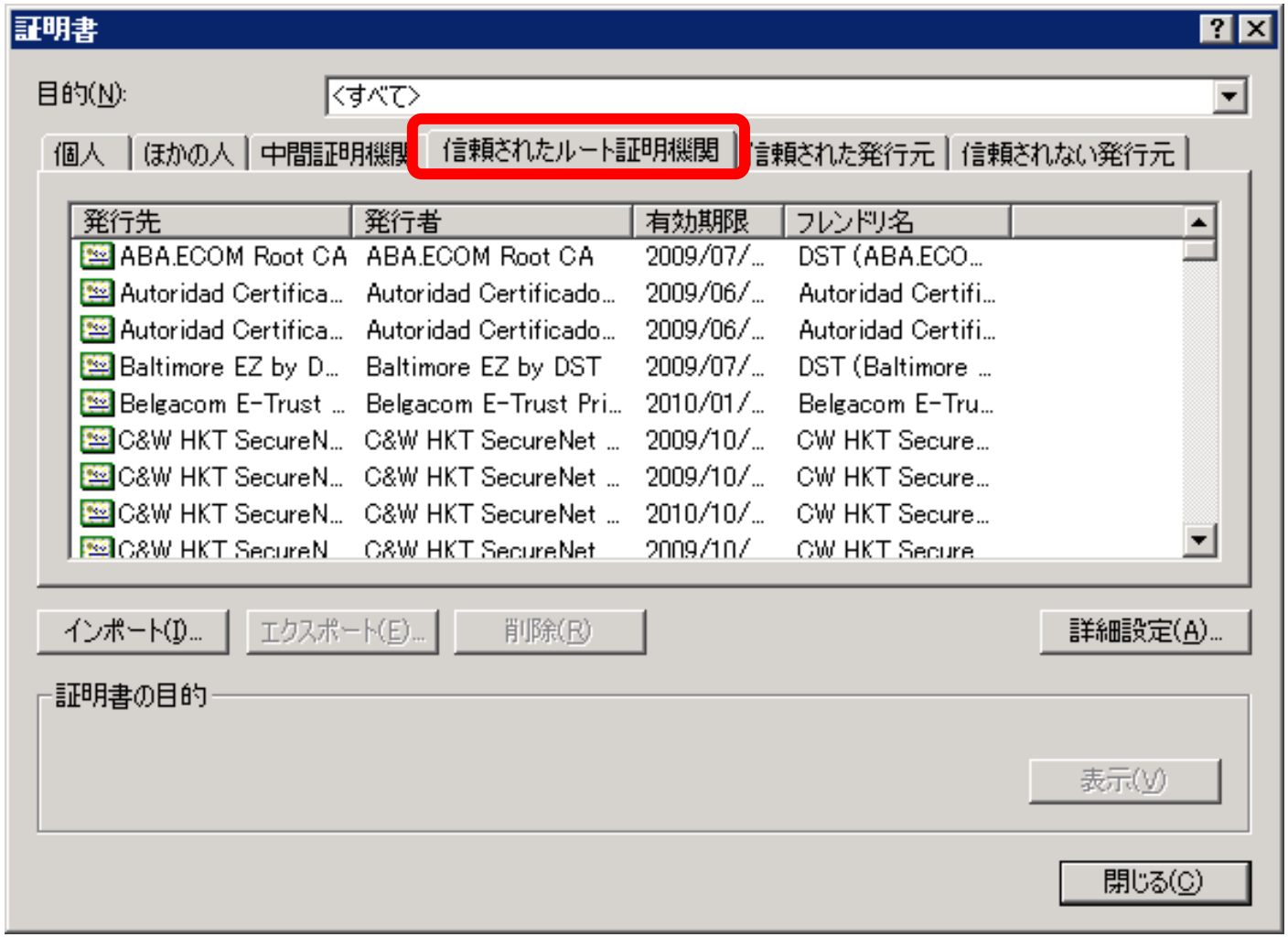
オープンドメイン
認証局

**不特定多数がアクセスするサイトのサーバ証明書は
オープンドメイン認証局から発行してもらいましょう**

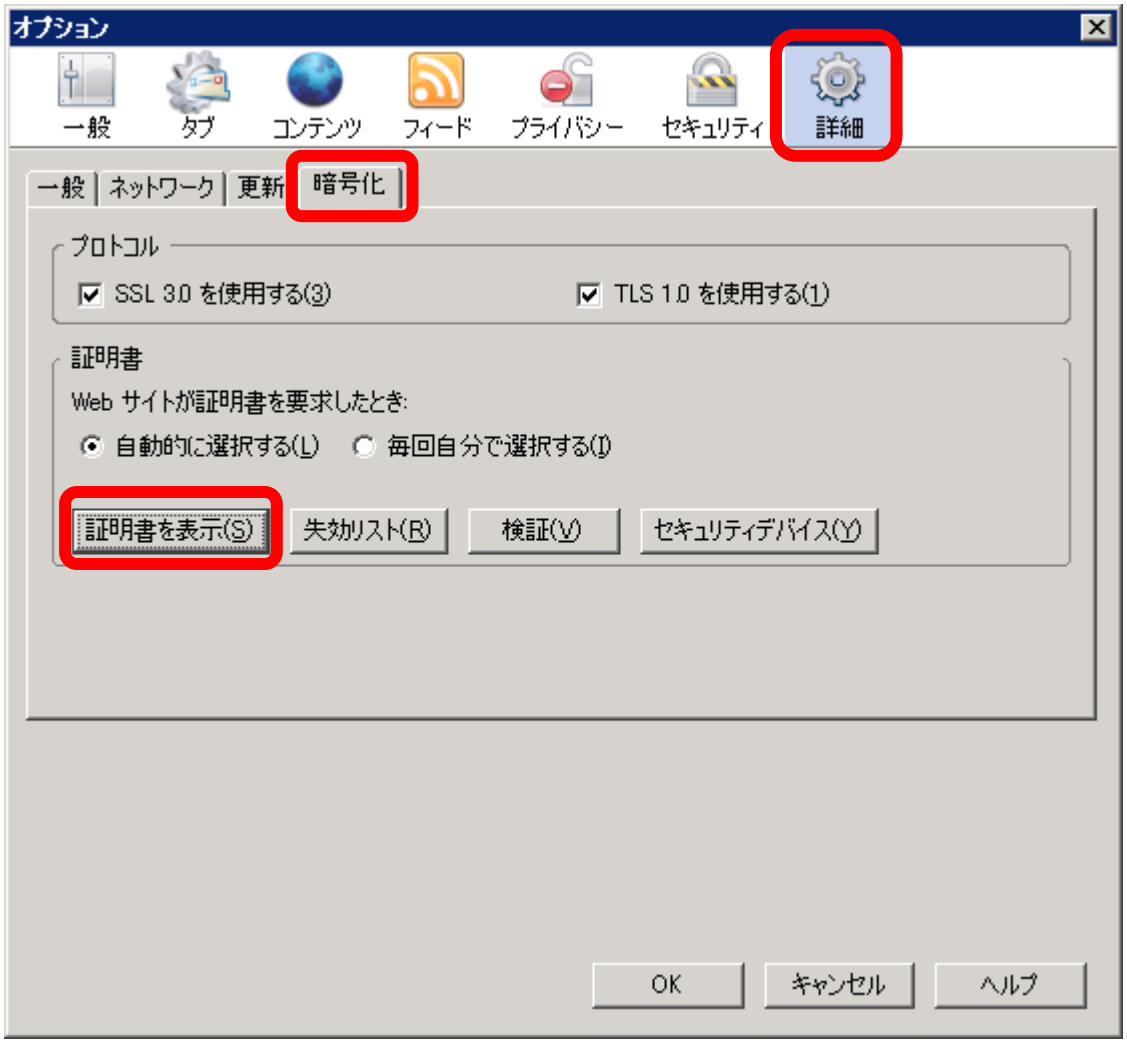
IEの証明書リスト（1）


インターネットのプロパティ
全般
セキュリティ
プライバシー
コンテンツ
接続
プログラム
詳細設定
コンテンツ アドバイザ
規制システムを使用すると、このコンピュータから表示できるインターネットの内容を制御できます。
有効にする(E)...
設定(T)
証明書
暗号化された接続と識別のための証明書を設定します。
SSL 状態のクリア(S)
証明書(C)
発行元(B)
オートコンプリート
オートコンプリートによって、Web ページで前回入力した内容を、入力中に補完できます。
設定(I)
フィード
フィードによって Web サイトで更新された内容が提供されます。Web サイトは Internet Explorer や他のプログラムでも読むことができます。
設定(N)
OK
キャンセル
適用(A)

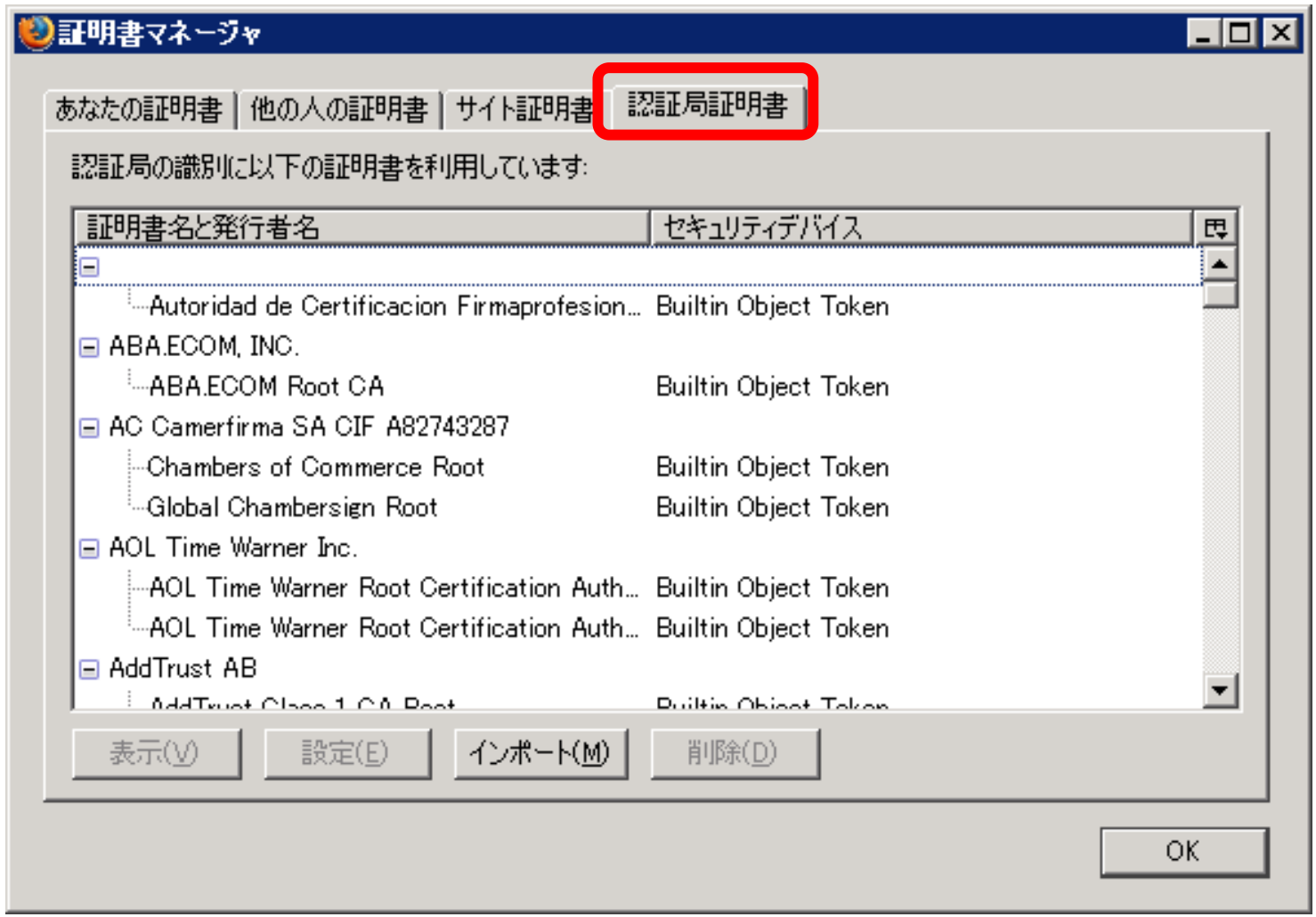
IEの証明書リスト(2)


証明書
目的(N):
<すべて>
個人
ほかの人
中間証明機関
信頼されたルート証明機関
信頼された発行元
信頼されない発行元
発行先
発行者
有効期限
フレンドリ名
ABA.ECOM Root CA
ABA.ECOM Root CA
2009/07/...
DST (ABA.ECO...
Autoridad Certifica...
Autoridad Certificado...
2009/06/...
Autoridad Certifi...
Autoridad Certifica...
Autoridad Certificado...
2009/06/...
Autoridad Certifi...
Baltimore EZ by D...
Baltimore EZ by DST
2009/07/...
DST (Baltimore ...
Belgacom E-Trust ...
Belgacom E-Trust Pri...
2010/01/...
Belgacom E-Tru...
C&W HKT SecureN...
C&W HKT SecureNet ...
2009/10/...
CW HKT Secure...
C&W HKT SecureN...
C&W HKT SecureNet ...
2009/10/...
CW HKT Secure...
C&W HKT SecureN...
C&W HKT SecureNet ...
2010/10/...
CW HKT Secure...
C&W HKT SecureN
C&W HKT SecureNet
2009/10/
CW HKT Secure
インポート(I)...
エクスポート(E)...
削除(R)
詳細設定(A)...
証明書の目的
表示(V)
閉じる(C)

Firefoxの証明書リスト(1)



Firefoxの証明書リスト(2)



オレオレ認証局とオレオレ証明書

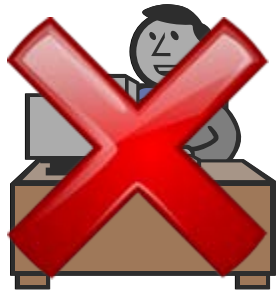
- オレオレ認証局
  - ユーザがクライアントアプリケーションに後から登録する必要がある認証局
- オレオレ証明書
  - 認証局からの信頼を何らかの追加手順なしには確認することができない証明書

これらは信頼してもらうには、利用者に何らかの設定や操作をしてもらう必要があります。

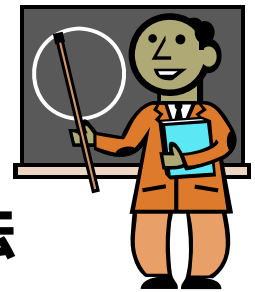
(オレオレ証明書に関しては) 関係者などに限定した用途以外には使わないでください。

オレオレ証明書と大学教育

- 誤った理解
  - 警告が出ても無視していい
    - 何かしらの理由がなければ警告は出ません
  - 警告を回避するには証明書を登録すればいい
    - どんな証明書でも登録していいわけではありません



- 必要な教育
  - 警告の理由と無視してもよい状況の説明
  - 登録してよい証明書といけない証明書の識別方法



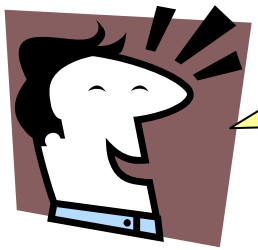
十分な教育なしにオレオレ証明書を使うことは最高学府として学生に勧めるべきではない

オープンドメイン認証局とは？

客観的で
公平な規準

- 国際規準WebTrust for CAに準拠
  - 認証局の運用の厳格さを審査する規準
    - 定期的に外部監査を受けているか？
    - 認証局の鍵ペアは安全に管理されているか？　など
- Webサーバに関する実在性を確認
  - Webサーバのドメイン
  - Webサーバを所管する機関
- 主要なPKIアプリケーションの証明書リストに予め登録済。

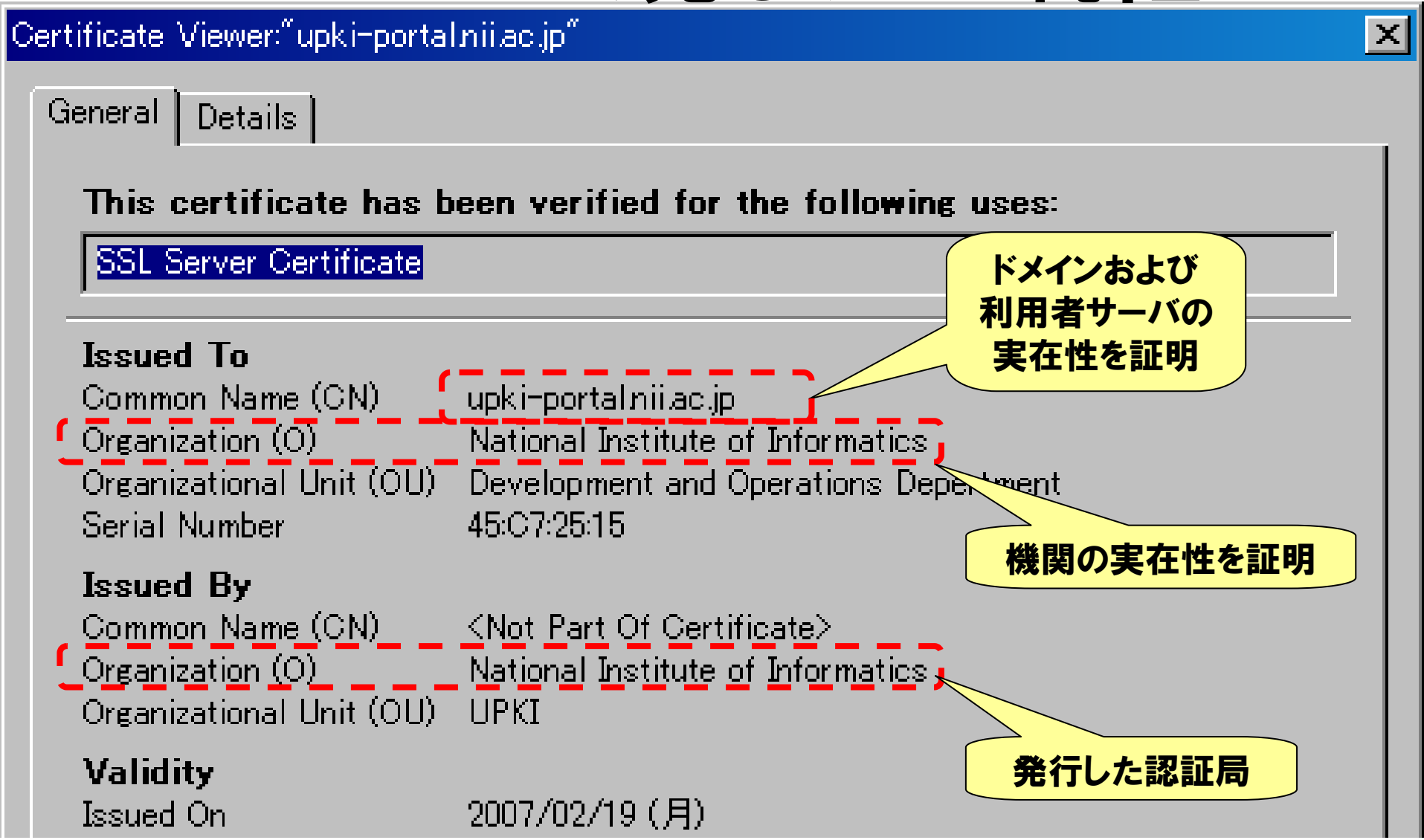
証明書用途に
適した確認内容



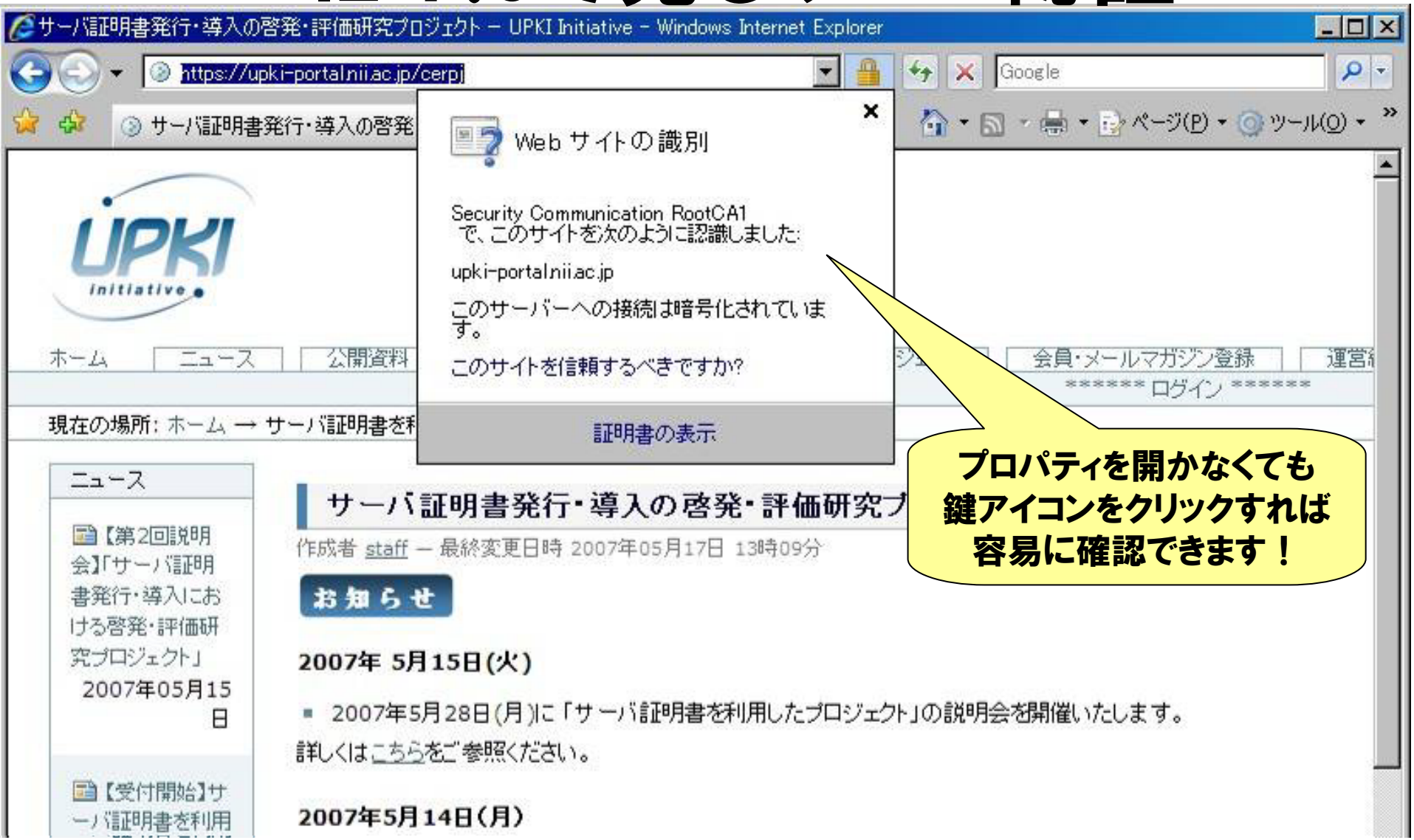
認定された認証局だから安心だね！
何も操作しなくても信頼できるから簡単だね！

Firefoxで見るサーバ認証

Firefoxで見るサーバ認証



IE 7.0で見るサーバ認証



- 背景
  - 大学におけるサーバ証明書の現状
- SSL/TLSサーバ認証とは
  - SSL/TLSサーバ認証の機能と仕組み
  - オレオレ認証局とオープンドメイン認証局
- **サーバ証明書プロジェクトのご紹介**
  - **プロジェクト概要**
  - **プロジェクト諸元**

プロジェクトの概要

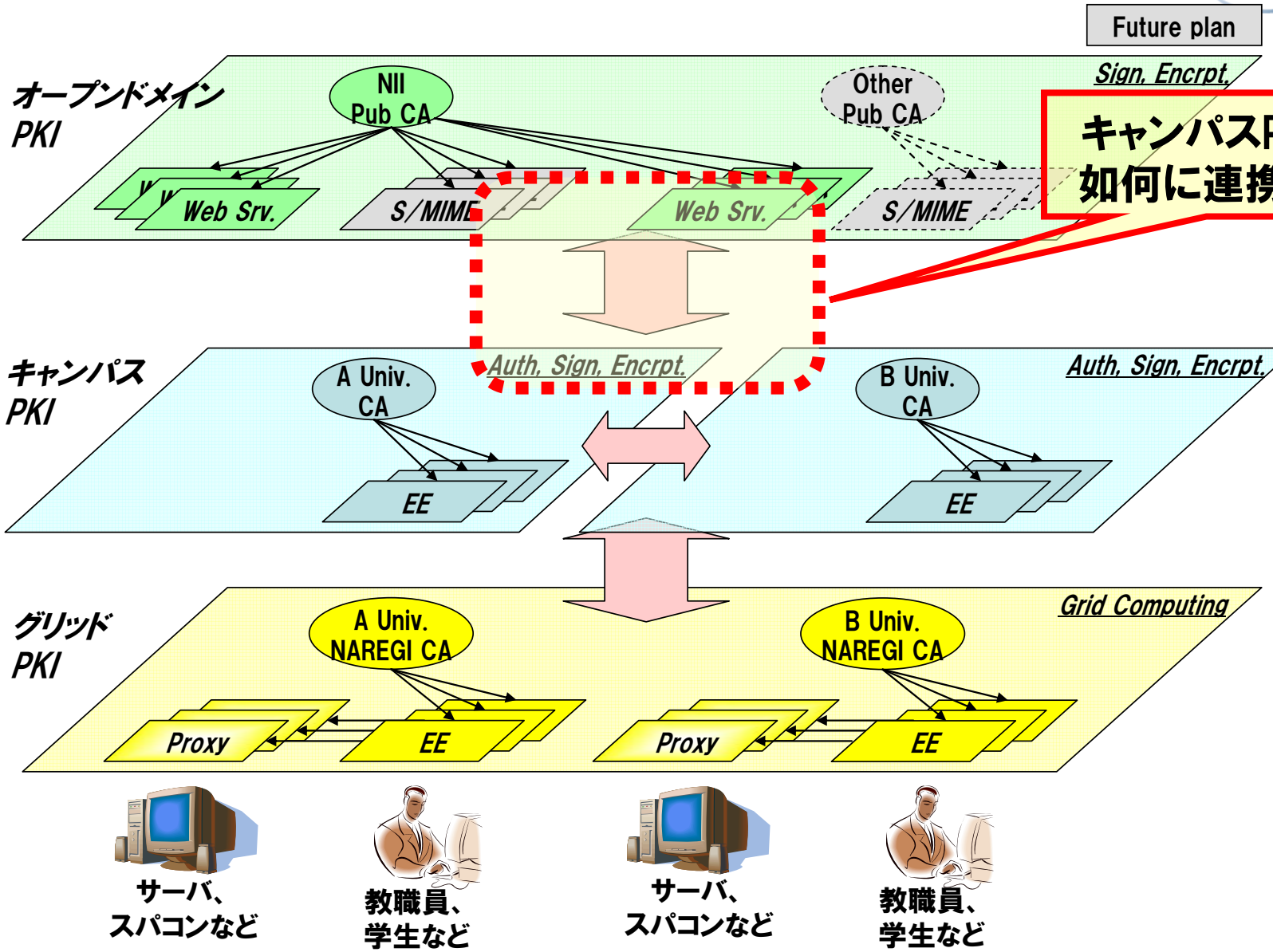
- 目的
  - 大学等のサーバ証明書の普及を推進
  - 認証局を用いた研究開発 ⇒ 登録発行業務の改善
  - 学術機関のWebサーバ信頼性向上
  - サーバ証明書の導入・運用ノウハウの共有
  - 参加者のサーバに対してのサーバ証明書無償配布
- 期間
  - 2007/04/01～2009/03/31
- ゴール
  - H19年度: サーバ証明書の普及が進まない理由・課題の整理
  - H20年度: サーバ証明書の普及促進の仮説・立証
  - 将来的に: キャンパスPKI層を活用した証明書発行業務の自動化
- 主な作業
  - プロジェクト参加機関の募集
  - 各登録担当者へのS/MIME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



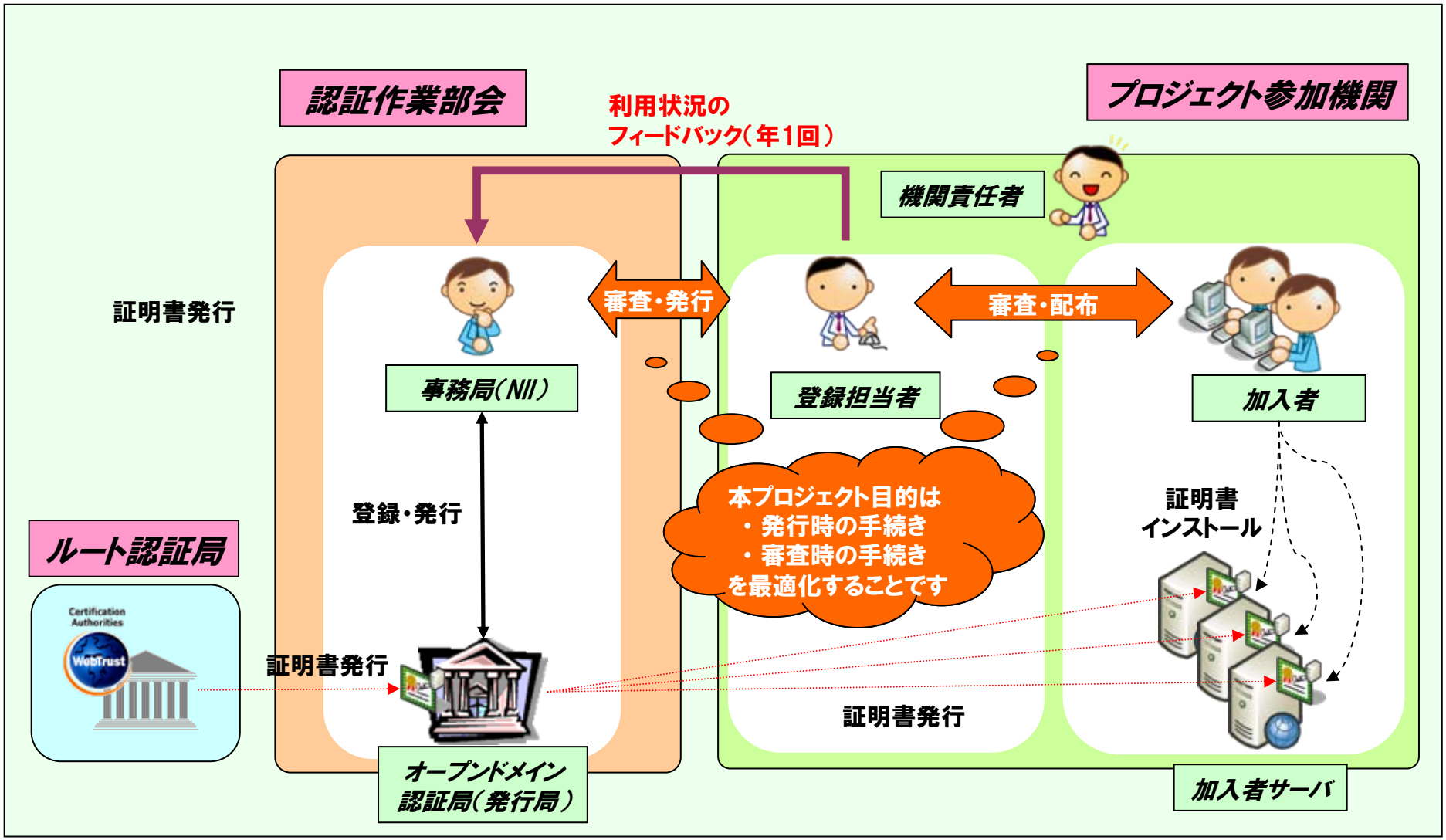
証明書発行の基本方針

- 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

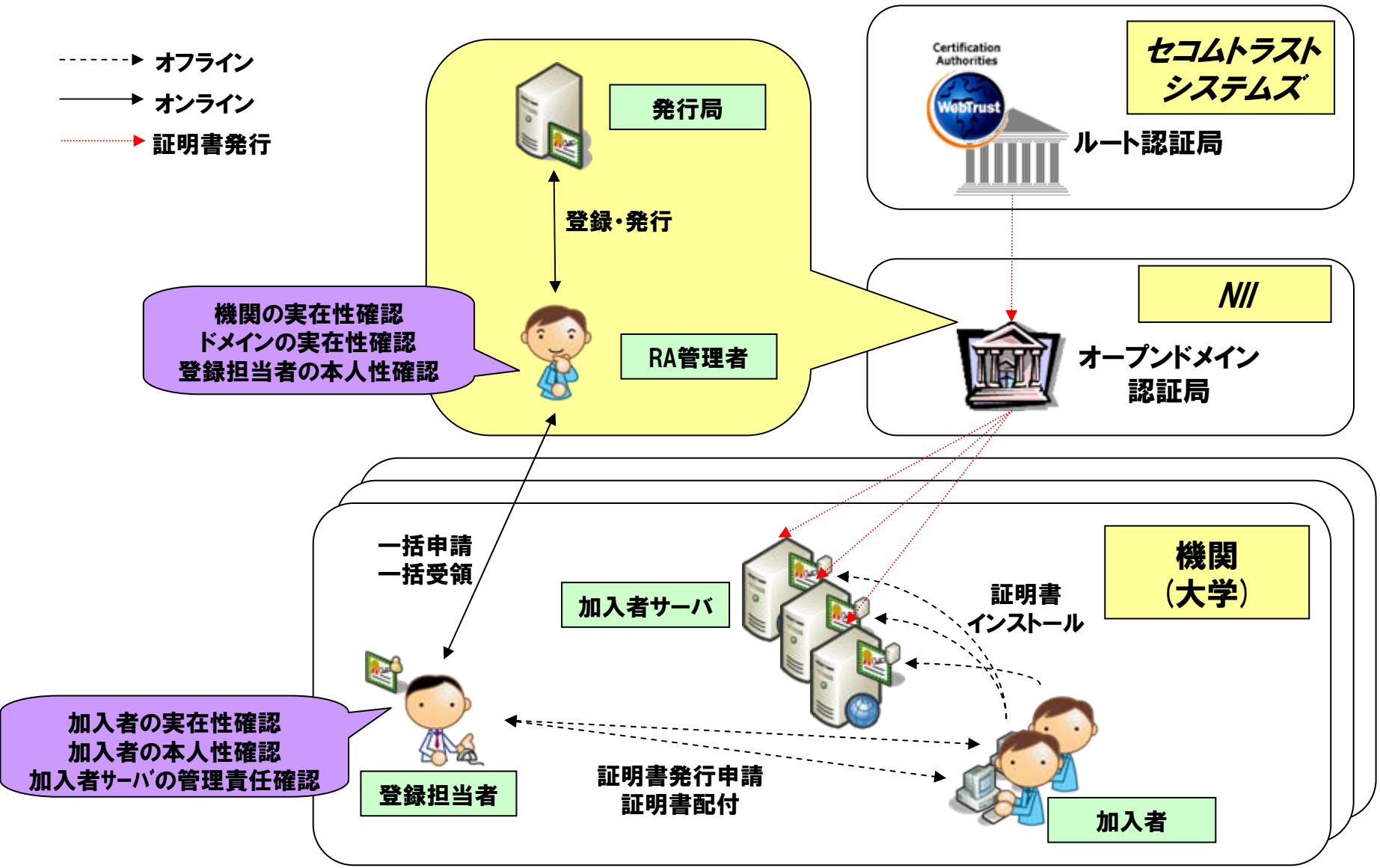
プロジェクト参加者の役割

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
	事務局	プロジェクト参加申請、証明書発行申請にあたり、審査業務を行う
機関 (大学)	機関責任者 (1機関1名)	本プロジェクト参加にあたり、各機関で選出した代表者。 課長職相当または准教授以上
	登録担当者 (複数名可)	本プロジェクトの参加機関側の事務的な窓口。 大学の規模等に応じて複数名選出可。
	加入者	Webサーバ(加入者サーバ)を管理し、本プロジェクトのサーバ証明書を利用する。 機関に所属する教職員。
不特定多数	利用者	加入者サーバへアクセスし、その証明書を検証する。

プロジェクト概念図


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
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
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

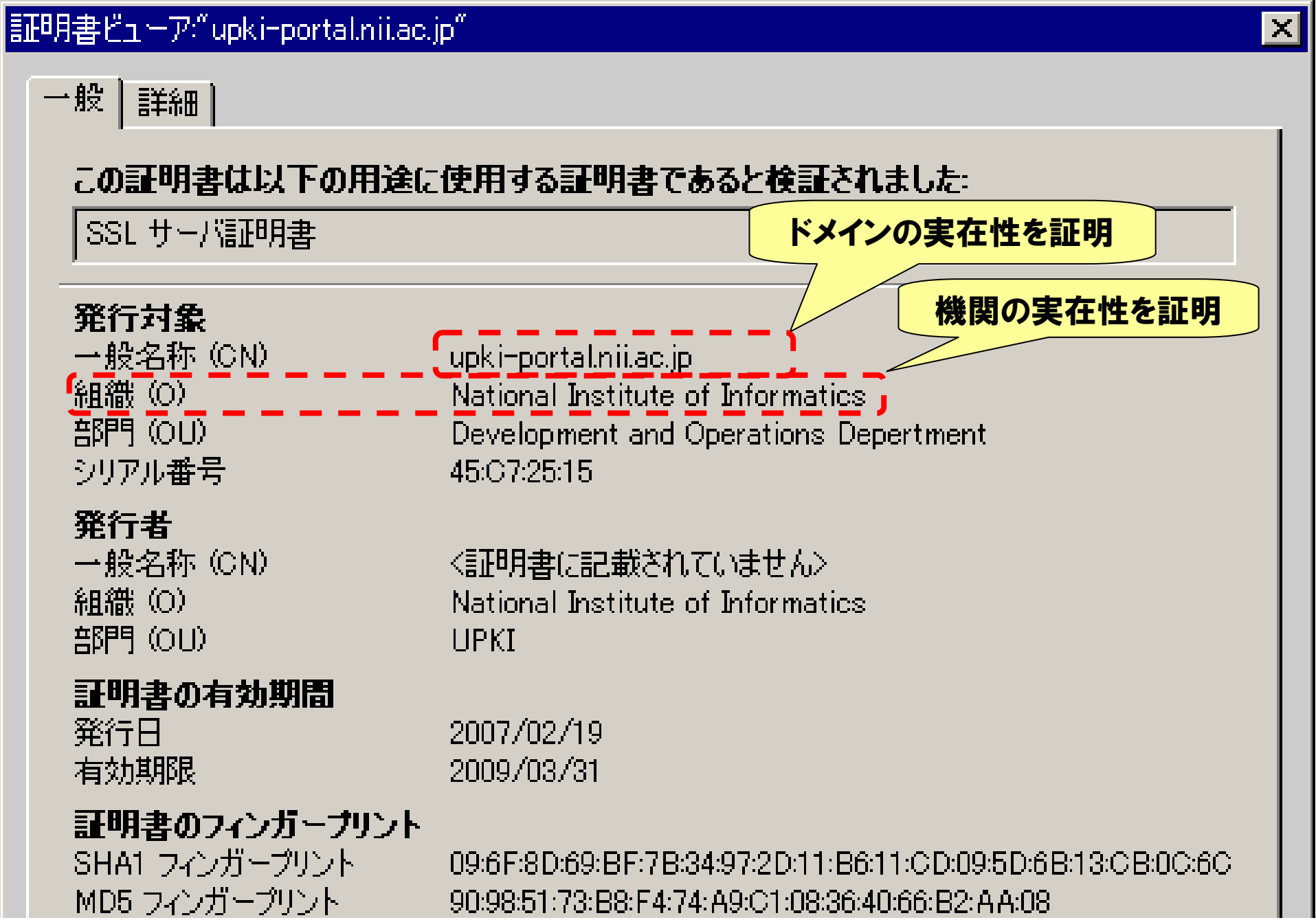

オフライン
オンライン
証明書発行
発行局
登録・発行
RA管理者
機関の実在性確認
ドメインの実在性確認
登録担当者の本人性確認
Certification Authorities
WebTrust
セコムトラスト
システムズ
ルート認証局
NII
オープンドメイン
認証局
一括申請
一括受領
加入者サーバ
証明書
インストール
機関
（大学）
加入者の実在性確認
加入者の本人性確認
加入者サーバの管理責任確認
登録担当者
証明書発行申請
証明書配付
加入者

商用証明書との比較
～審査項目の違い～

機関側の審査項目は確認手順調査表でチェック

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で動作確認
※注2)Jakarta Tomcatについて
Jakarta Tomcat 4.1.31、Jakarta Tomcat 5.0.30で動作確認

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

Javaアプレットを利用してサーバを構築している場合、クライアントが
JSE 1.6.0以降のバージョンのみ利用可能です。
（※JSE1.5では利用できないことを確認しています）

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，公益法人，文部科学省の独立行政法人等
  - 日本学術会議協力学術研究団体のうち、
    - 本プロジェクトが対象とするドメイン名を保有し部会が認めた団体
- 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。
- 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）
    - S/MIMEが利用できない場合は、Office XP以降のExcel
      →申請ファイルへのデジタル署名

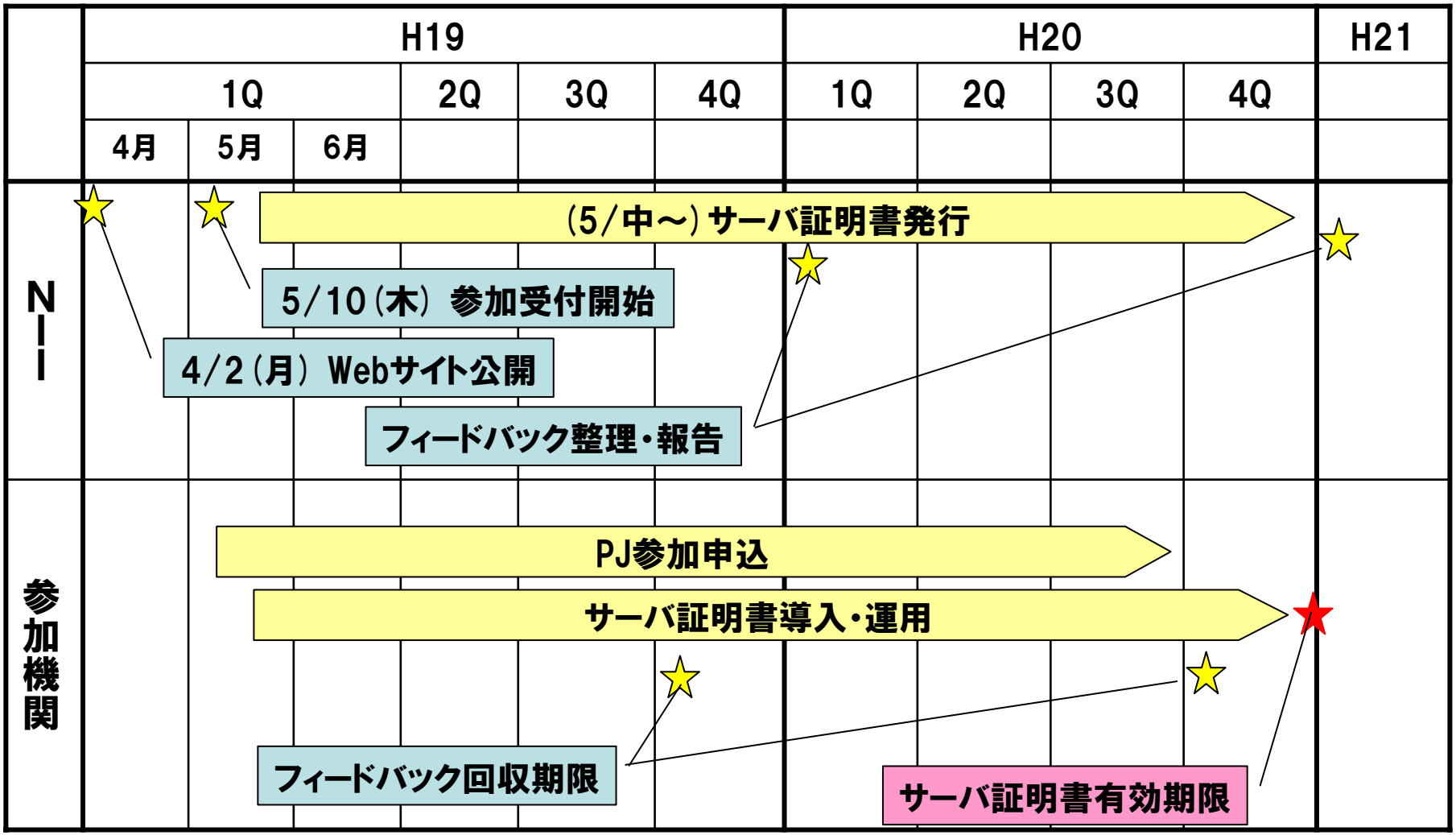
対象機関が
拡張されました!

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
  - 原則として鍵長は1024bit以上
    - 1024bit未満の場合には申請時にご相談ください
  - 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

鍵長の要件を
明記しました!

プロジェクトスケジュール（予定）



まとめ

- サーバ証明書の基本
  - サーバ証明書は認証に不可欠
    - 企業に限らず大学にも必要。
  - オープンドメイン認証局から発行されたサーバ証明書を使いましょう
    - オレオレ認証局・証明書は極めて限定的に。
- サーバ証明書プロジェクト
  - 商用認証局と同等（オープンドメイン認証局）のサーバ証明書を発行します
  - 機関の登録担当者に発行申請してください

皆様のご協力を
よろしくお願いいたします。

2月7日時点の実績：

参加機関数	42機関
証明書発行枚数	501枚

https://upki-portal.nii.ac.jp/cerpj

cerpj@nii.ac.jp