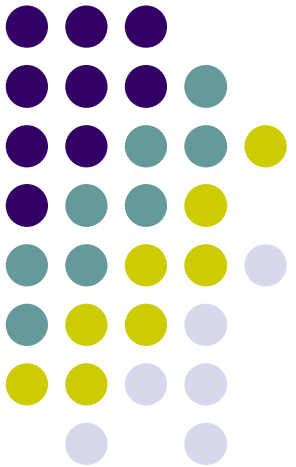
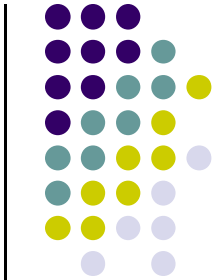
電子証明書の意義と サーバ証明書 新プロジェクトの計画

国立情報学研究所
学術ネットワーク研究開発センター
特任准教授　島岡 政基



本日の概要

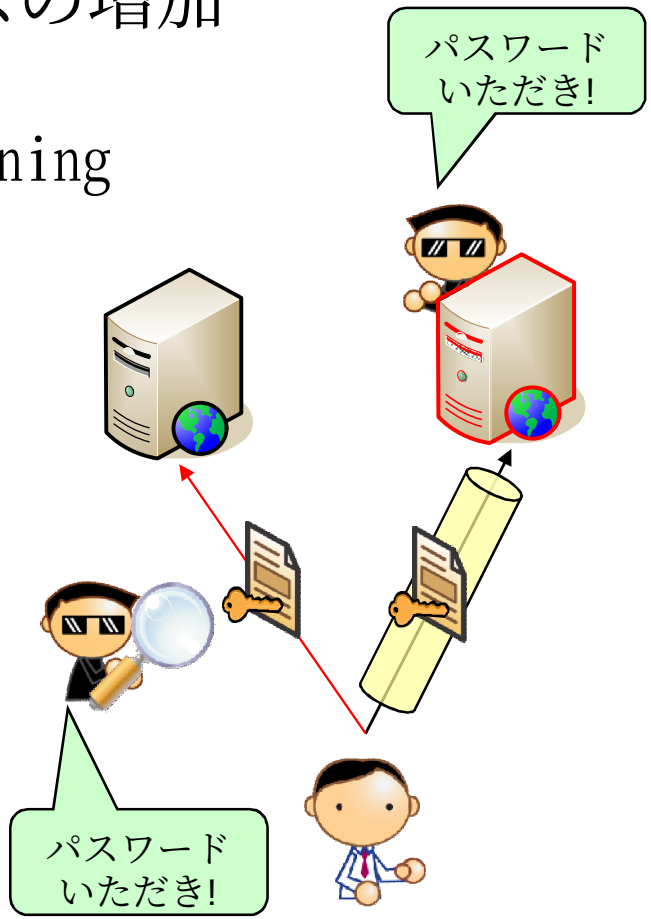


- 証明書の意義
  - なぜ大学にサーバ証明書が必要なのか?
  - SSL/TLSサーバ認証とは
  - サーバ証明書を発行する認証局
- 新プロジェクトの計画
  - 証明書自動発行支援システム
  - 対応環境
  - 移行スケジュール(案)

なぜ大学に
サーバ証明書が必要なのか?

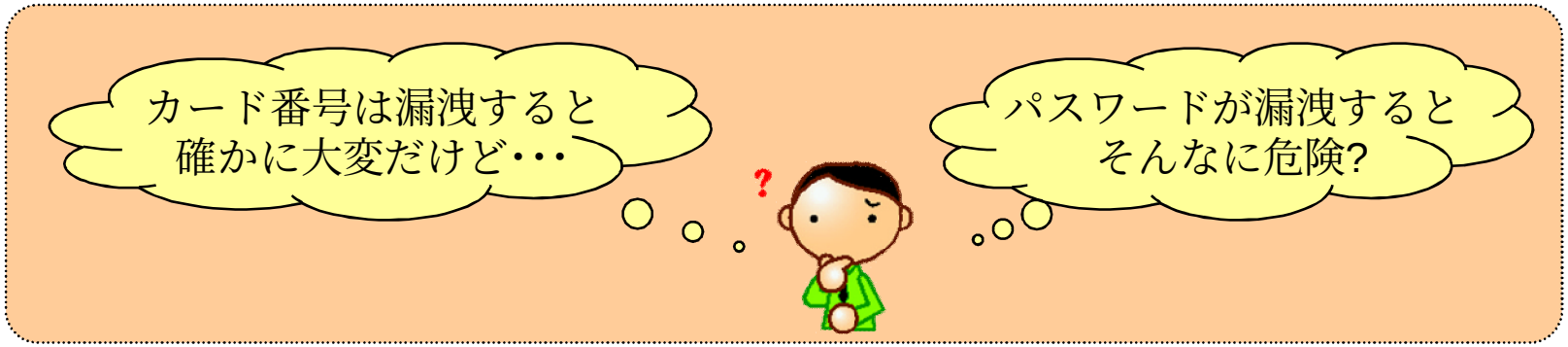
- ユーザ認証を前提とするサービスの増加
  - メール、LDAP、ファイルサーバ
  - グループウェア、SNS、CMS、e-Learning

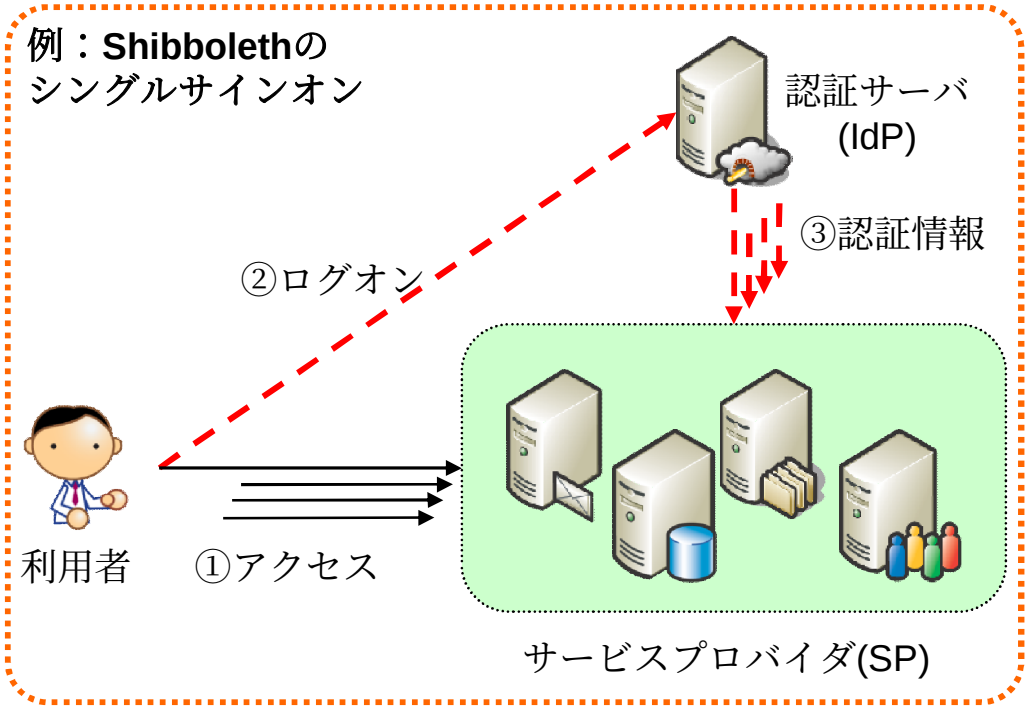
- 認証情報の漏洩対策
  - ✓ 通信経路の暗号化 ← 盗聴防止
  - ✓ サーバの真正性確認 ←なりすまし防止



サーバ証明書を使った
SSL/TLSサーバ認証で解決

SSOに不可欠なサーバ証明書



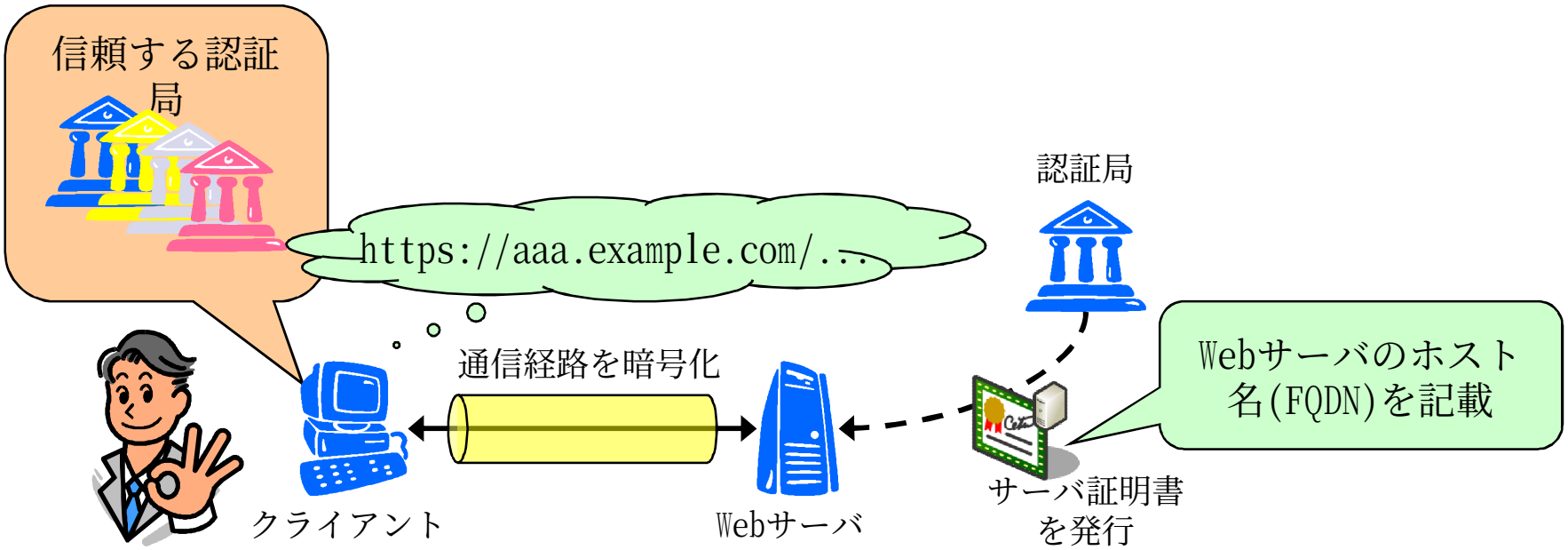


- シングルサインオンは認証情報が安全にやり取りされることが大前提
- 認証情報が漏洩するような基盤では実現できない

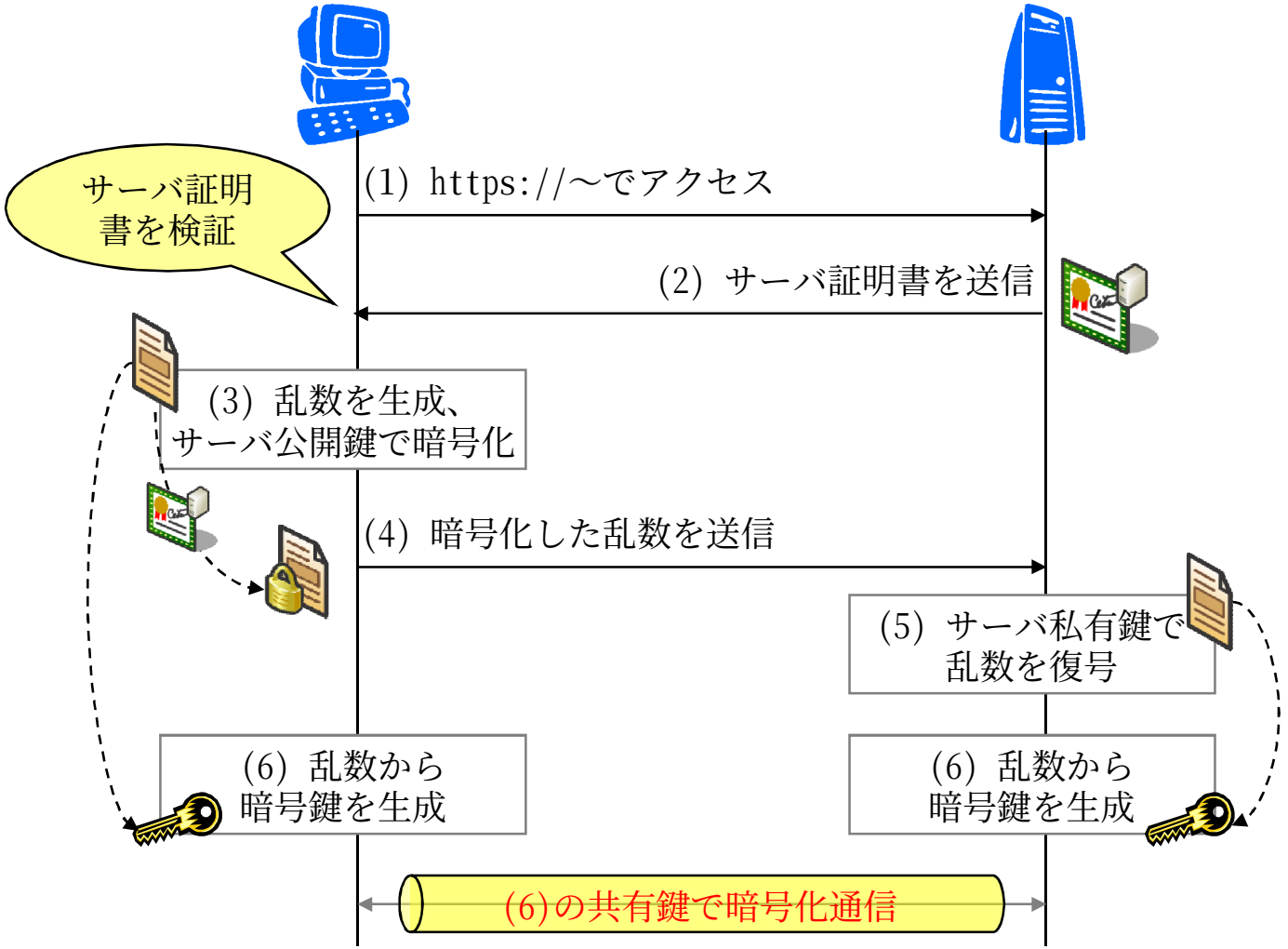
サーバ証明書はフェデレーション(UPKI-Fed)にも不可欠

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
  - 認証時に生成した暗号鍵で通信中のデータを暗号化

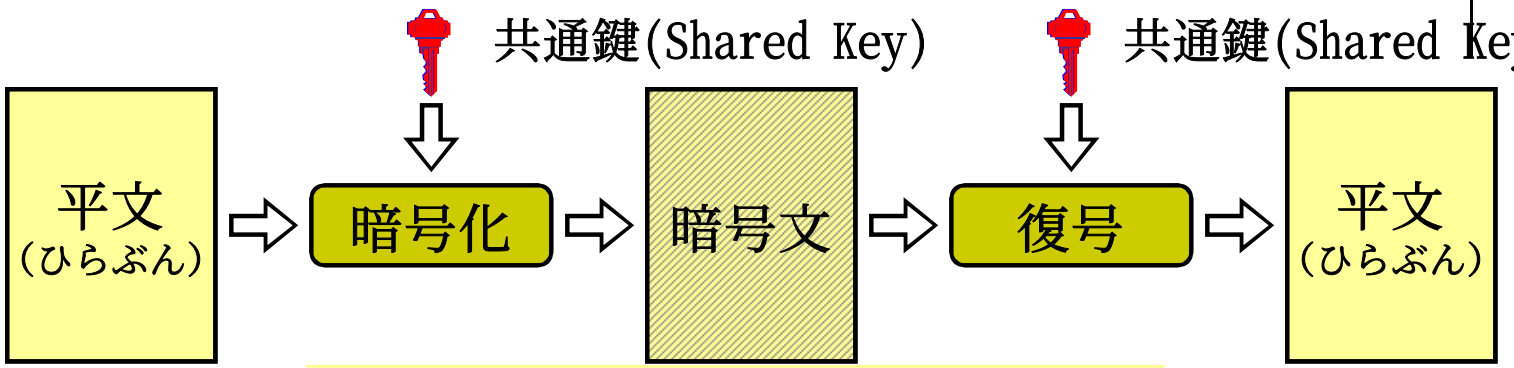


サーバ認証から暗号鍵の共有まで



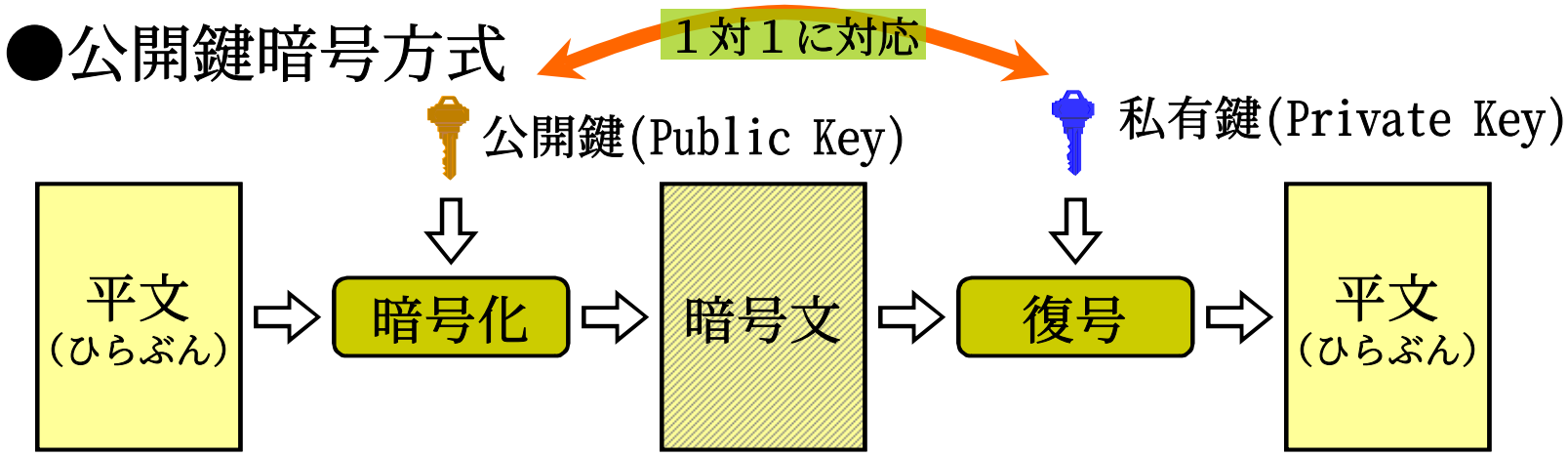
共通鍵暗号方式と公開鍵暗号方式

●共通鍵暗号方式



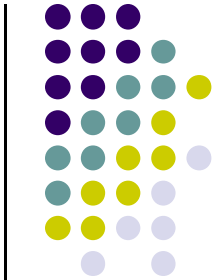
→暗号化と復号の鍵が同一

●公開鍵暗号方式



→暗号化と復号の鍵が異なる

サーバ証明書を発行する認証局



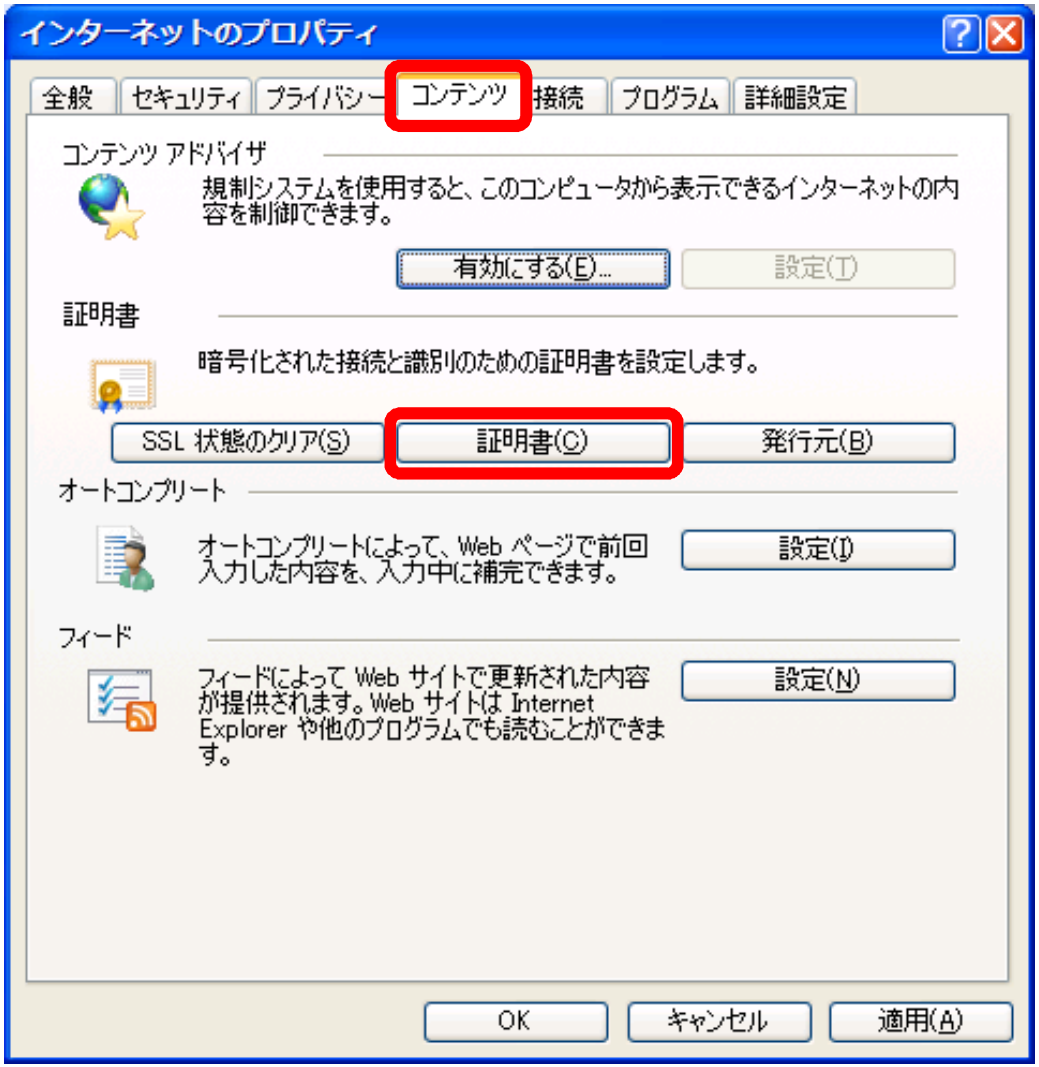
- 予めクライアント側のPKIアプリケーションが信頼している認証局でなければならない。
- 主要なPKIアプリケーションにはいくつかの認証局が予め登録されている。
  - IE: 「信頼されたルート証明機関」
  - Firefox: 「証明書マネージャ」

オープンドメイン認証局と呼びます

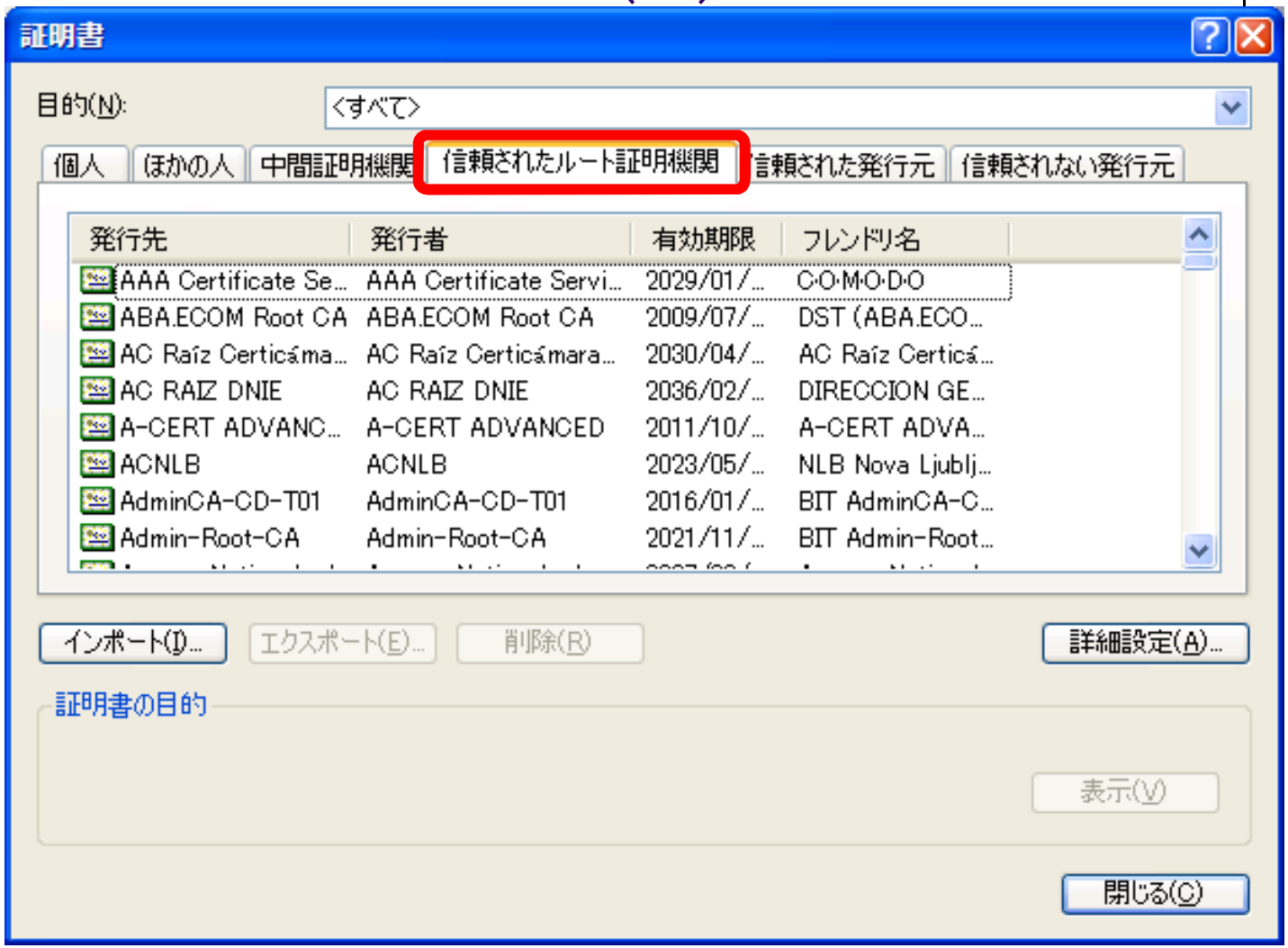
- ユーザが後付けで認証局を登録することも可能ですが…
  - 安全を保証できない認証局を登録することは非常に危険!!
  - 安全を保証できる認証局だと判断できますか?

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

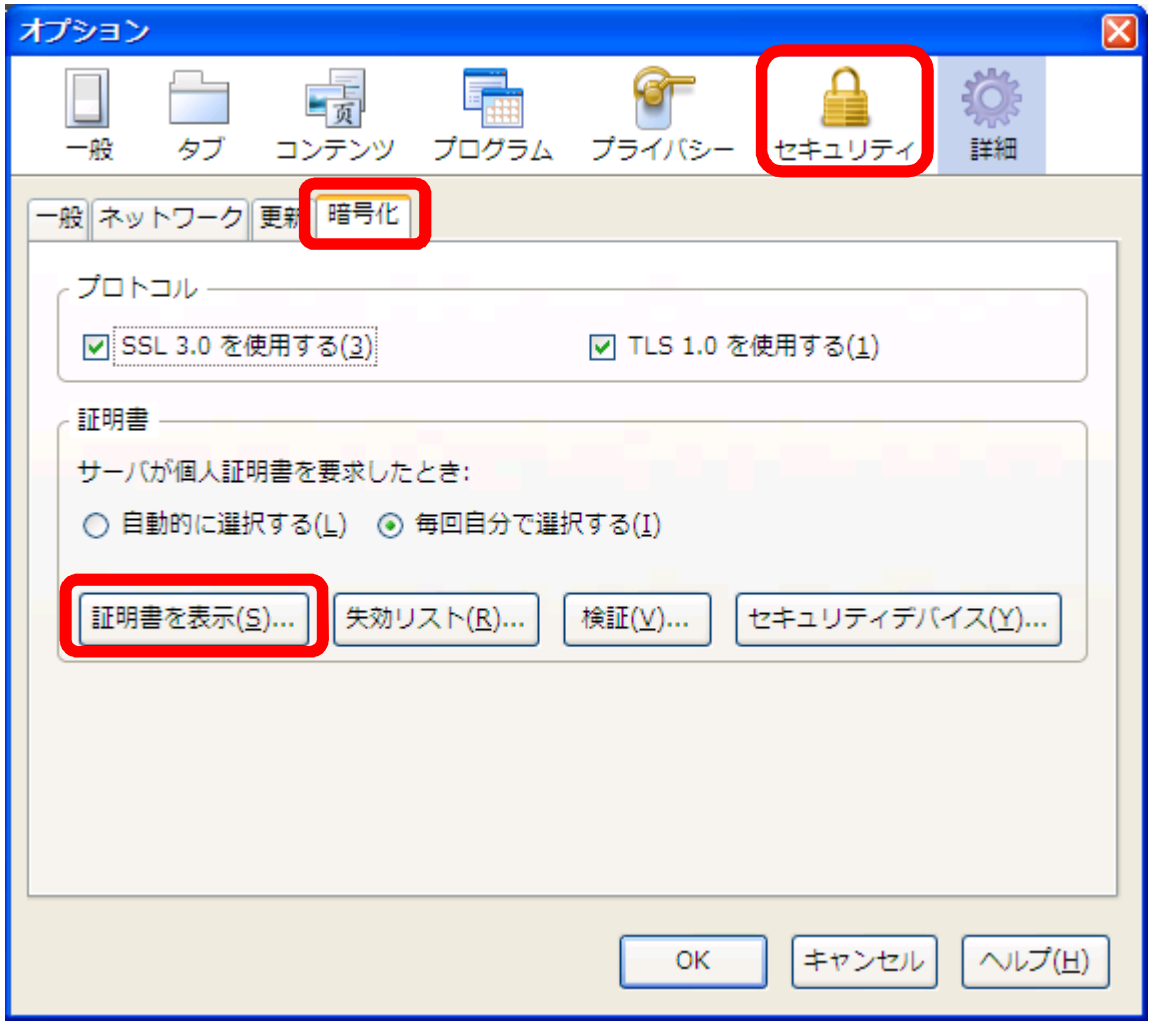
IEの証明書リスト(1)


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)

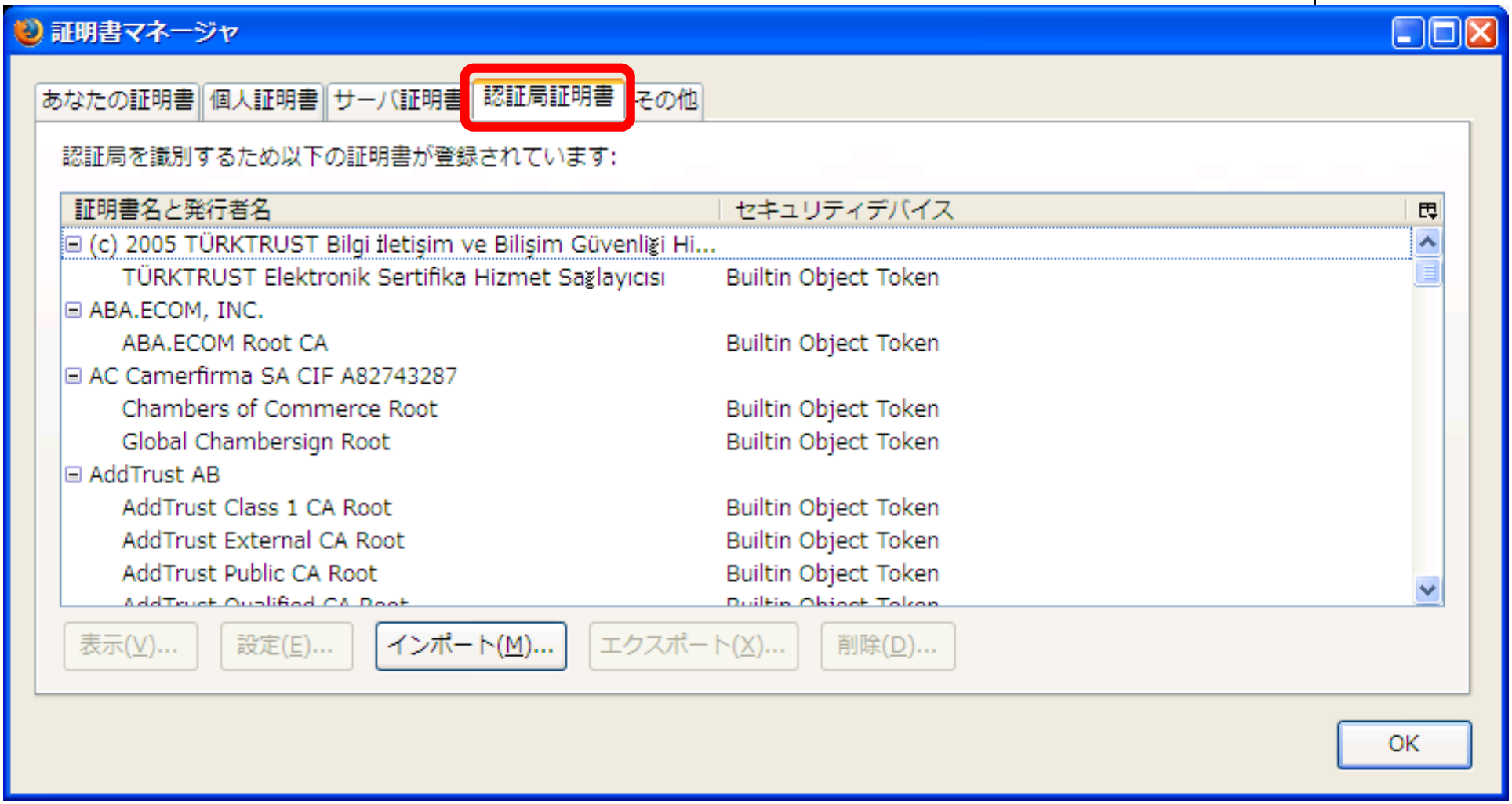
IEの証明書リスト(2)


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
AAA Certificate Se...
AAA Certificate Servi...
2029/01/...
C·O·M·O·D·O
ABA.ECOM Root CA
ABA.ECOM Root CA
2009/07/...
DST (ABA.ECO...
AC Raíz Certicáma...
AC Raíz Certicámara...
2030/04/...
AC Raíz Certicá...
AC RAIZ DNIE
AC RAIZ DNIE
2036/02/...
DIRECCION GE...
A-CERT ADVANC...
A-CERT ADVANCED
2011/10/...
A-CERT ADVA...
ACNLB
ACNLB
2023/05/...
NLB Nova Ljublj...
AdminCA-CD-T01
AdminCA-CD-T01
2016/01/...
BIT AdminCA-C...
Admin-Root-CA
Admin-Root-CA
2021/11/...
BIT Admin-Root...
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)



プライベート認証局と プライベート証明書

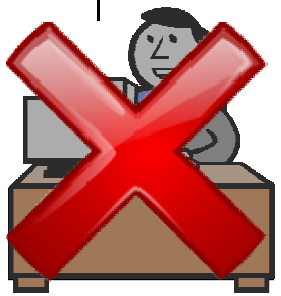
- プライベート認証局
  - ユーザがクライアントアプリケーションに後から登録する必要がある
- プライベート証明書
  - 認証局からの信頼を何らかの追加手順なしには確認することができない

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。

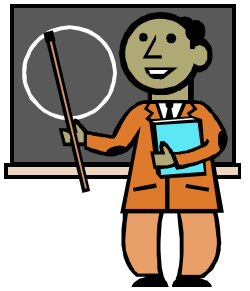
ここの確認手順を省略してしまうのがいわゆる「**オレオレ証明書**」

プライベート証明書は関係者限定の用途以外の利用は困難

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



十分な教育なしにプライベート証明書を使うことは
最高学府として学生にさせるべきではない

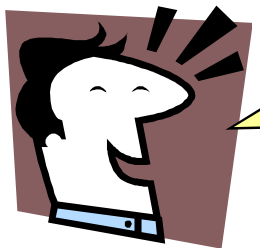
オープンドメイン認証局とは?

- 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

客観的で
公平な規準

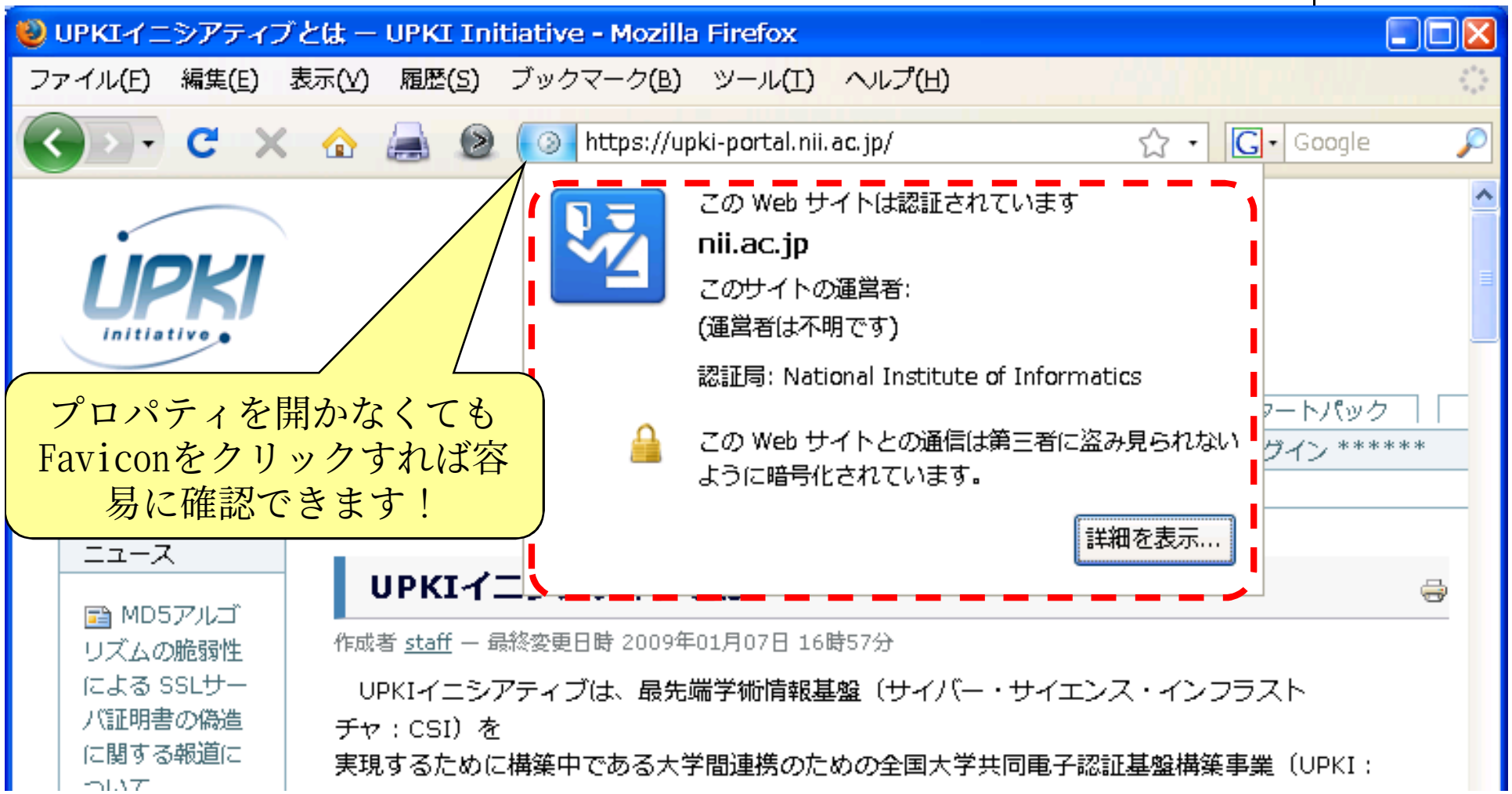
証明書用途に
適した確認内容

- 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。

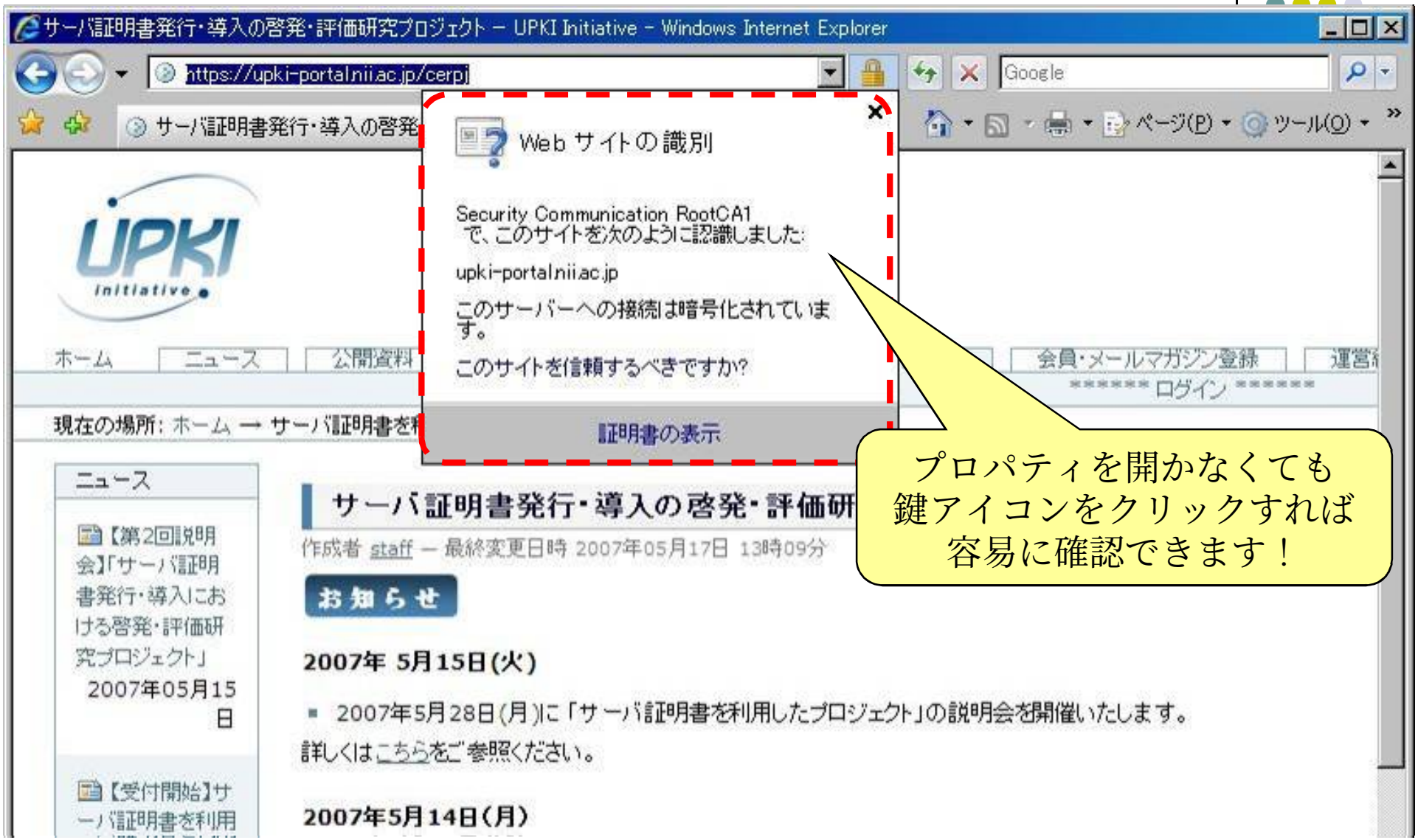


認定された認証局だから安心だね！
何も操作しなくても信頼できるから簡単だね！

Firefox 3.0で見るサーバ認証

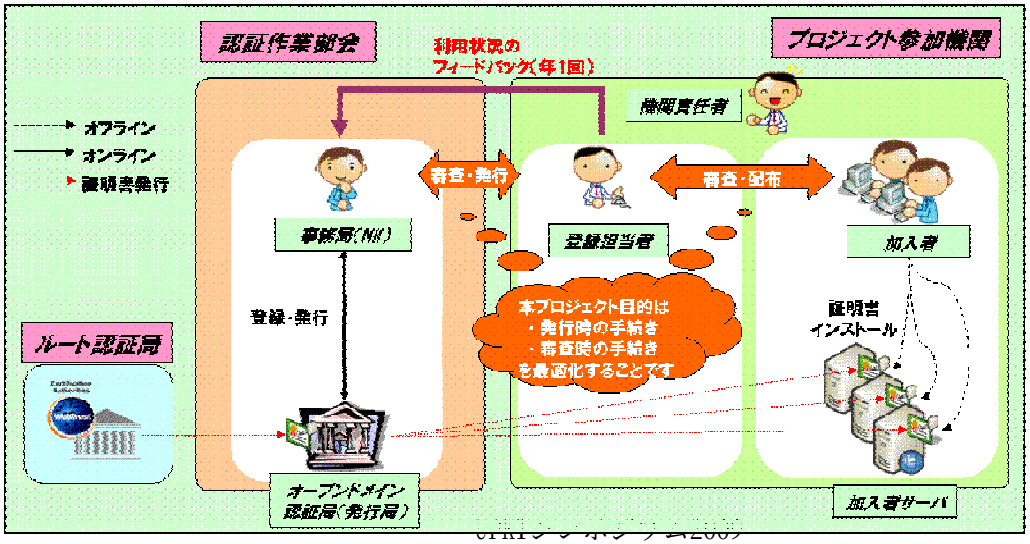


IE 7.0で見るサーバ認証



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(現行)

- 目的
  - オープンドメイン層の認証基盤の構築
  - サーバ証明書の審査・証明書配付方式の大学最適化
  - サーバ証明書の重要性の啓蒙活動
- 概要
  - サーバ証明書発行業務（審査）の一部を大学で実施
  - 参加機関に対して“本物”のサーバ証明書を発行
  - １月末現在，９０機関が参加し，２０００枚の証明書を発行

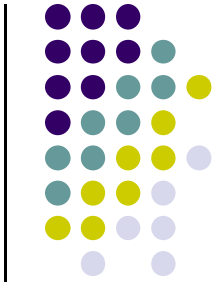


現行プロジェクトの評価(1)

H19年度 プロジェクト参加機関への調査から抜粋(回答：44機関、448サーバ)

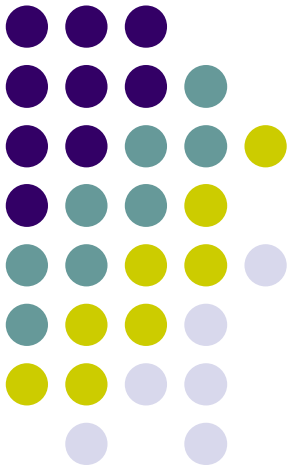
- 各機関のモチベーション
  - 証明書導入コスト←88.6%
  - オレオレ証明書のリプレース←65.91%
- 得られた知見
  - 公開サーバよりも学内サーバ（38% vs．49%)
  - ユーザ認証を必要とするサーバがほとんど←86%
- 課題
  - 携帯電話を含む対応機器の拡充
  - 導入事例・ケーススタディなどのナレッジベース構築
  - 登録担当者の利便性向上(オンライン化)

現行プロジェクトの評価(2)

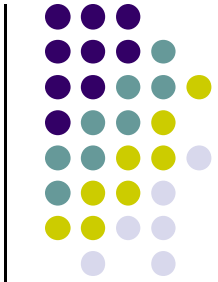


- オレオレ証明書を使う・使ってもらう後ろめたさがなくなった
- 費用対効果が説明しにくい学内サーバや認証サーバへの導入が進んだ
- 大学の実情に応じた確認手段・発行体制を確立できた
- (学内の)審査を効率化・オンライン化するために学内認証基盤の必要性を実感した
- サーバの管理体制、ドメインの管理体制を見つめ直し、学内の内部統制の足掛かりになると期待している
- 大学のサービスに関する信頼性・信用性を自分たちの手で支える仕組みなので今後も利用したい
- 加入者にもクライアント証明書を配布して欲しい

新プロジェクトの計画



証明書自動発行
検証プロジェクト(仮称)

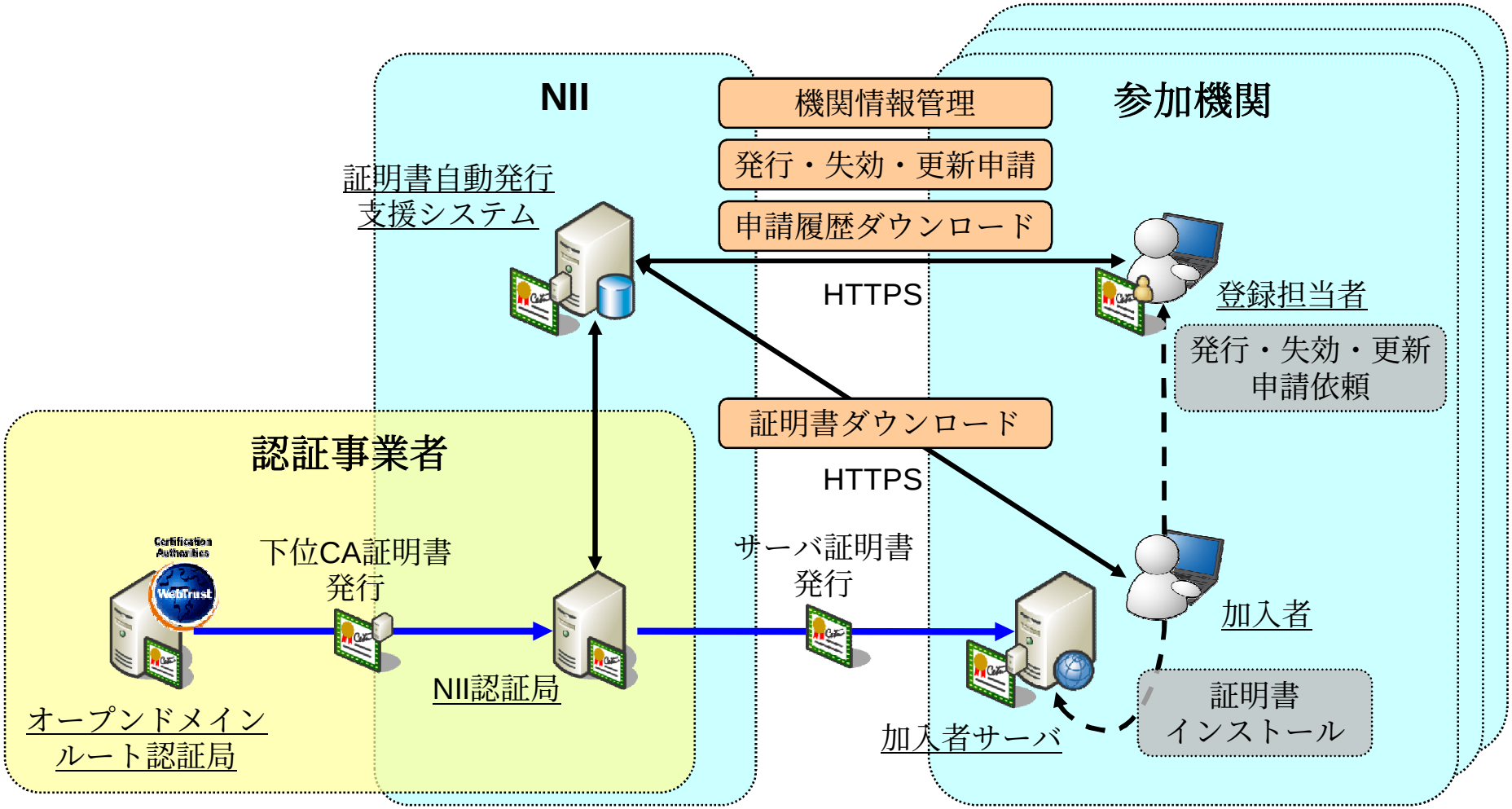


- 目的
  - 登録担当者の利便性向上
  - 学内認証基盤との連携・自動化を目指す
- 実施期間
  - 平成21年4月～平成24年3月末 (3年間)

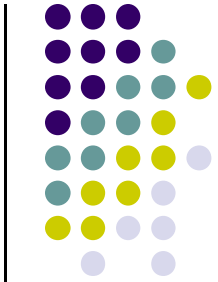
- 現行プロジェクトをベースに、発行処理の自動化を目指す
  - Webベースの申請に対応
  - 申請フォームをExcelからTSVに変更

- 現行プロジェクトからのスムーズな移行がカギ

証明書自動発行支援システム



対応Webサーバ



- Apache(mod ssl) (1.3.34+2.8.25)
- Apache-SSL(1.3.33+1.55)
- Microsoft Internet Information Server 5.0
- Microsoft Internet Information Server 6.0
- IBM HTTP Server6.0.2
- Jakarta Tomcat 4.1.31

対応Webブラウザ

- Microsoft Internet explorer 5.5以上
- Firefox1.0.8以上
- Opera8.0以上
- Apple Safari3.0.4以上
- Google Chrome0.2.149以上

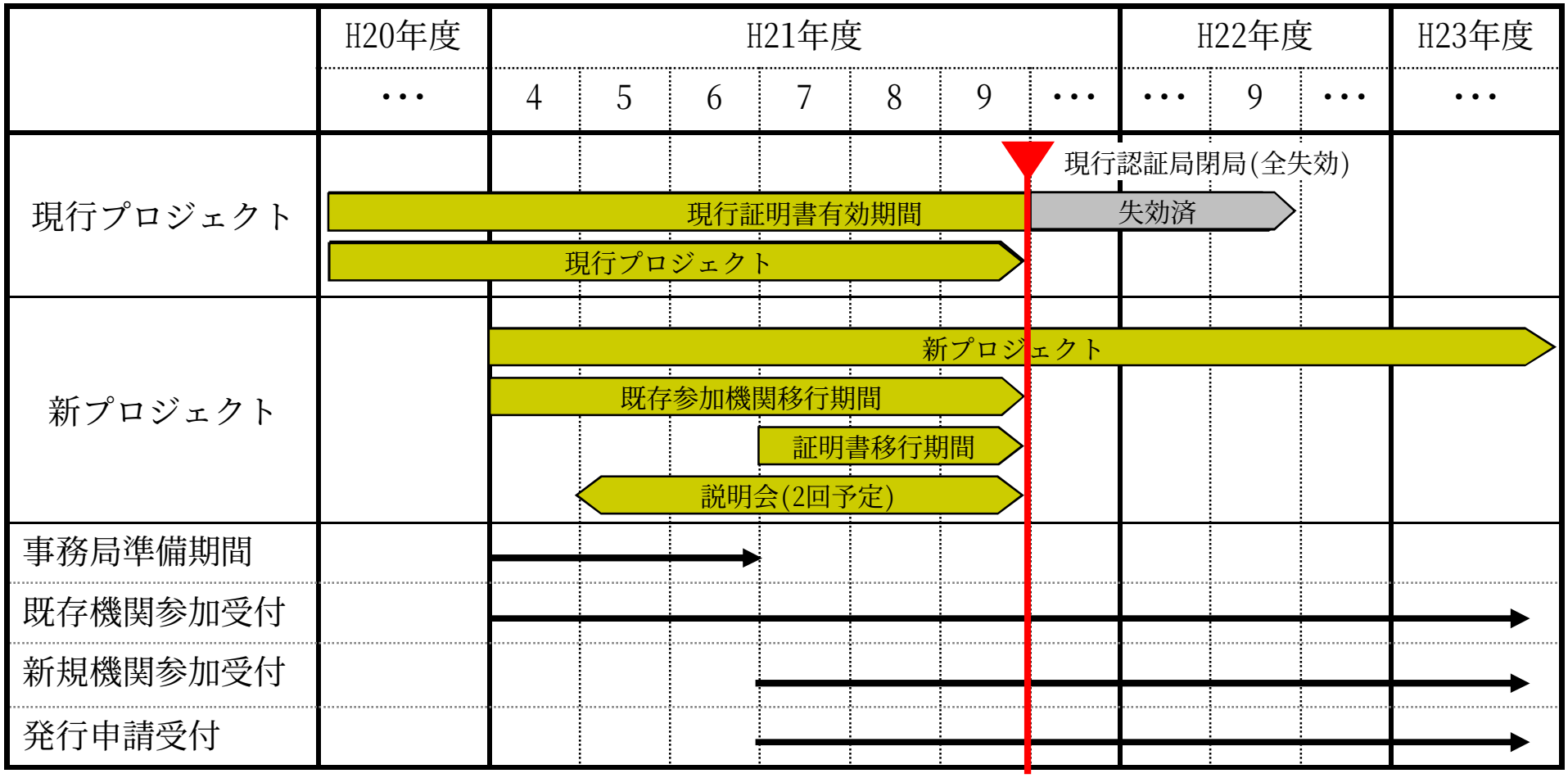




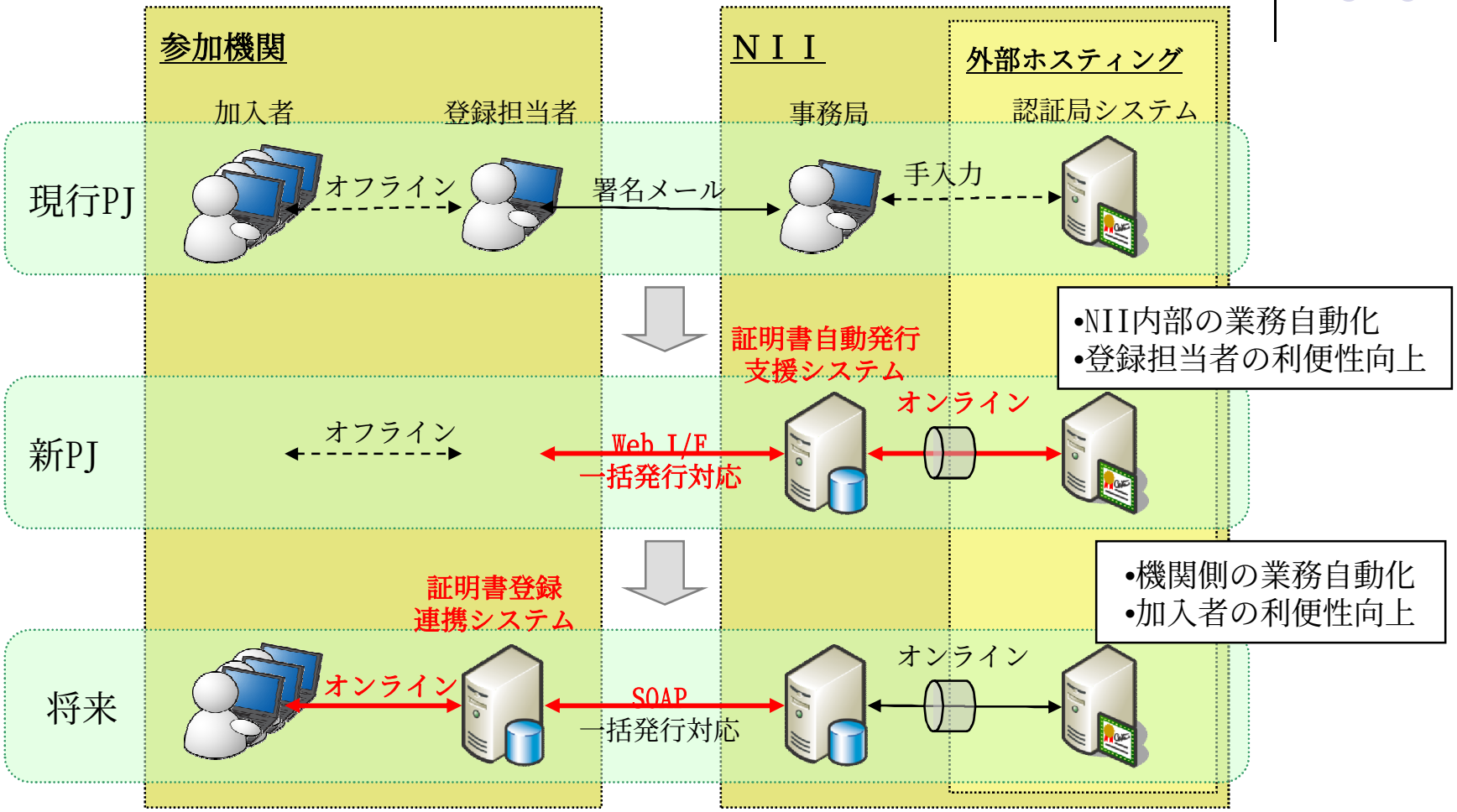
対応携帯電話

- 2006年6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、
- かつ、ルート認証局証明書の鍵長RSA2048bitに対応したブラウザ

新プロジェクトへの移行スケジュール(案)



最終ゴールは
学内認証基盤を活用した完全自動化



学内認証基盤を構築することで、機関側も省力化が可能になります

新プロジェクトも引き続き
ご協力よろしくお願いします

当面は新プロジェクトも同じURLで
情報発信していきます

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