身近なPKI:
サーバ証明書の重要性

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 <shimaoka@nii.ac.jp>

Webサイト利用時の主な脅威

- 盗聴
  - 機密情報の漏洩
    - 機密文書、ID・パスワード、カード番号など

通信経路の暗号化

- なりすまし
  - 機密情報の引き出し
    - ID・パスワード、カード番号など
    - 悪意あるサイトへの誘導

サーバの真正性

- (通信データの) 改竄
  - 改竄された情報の受信
    - 悪意あるサイトへの誘導
    - 誤った情報による二次的な損害

情報に対する電子署名

サーバ証明書はこれらの対策に有効

Webサイトに関する最近の傾向

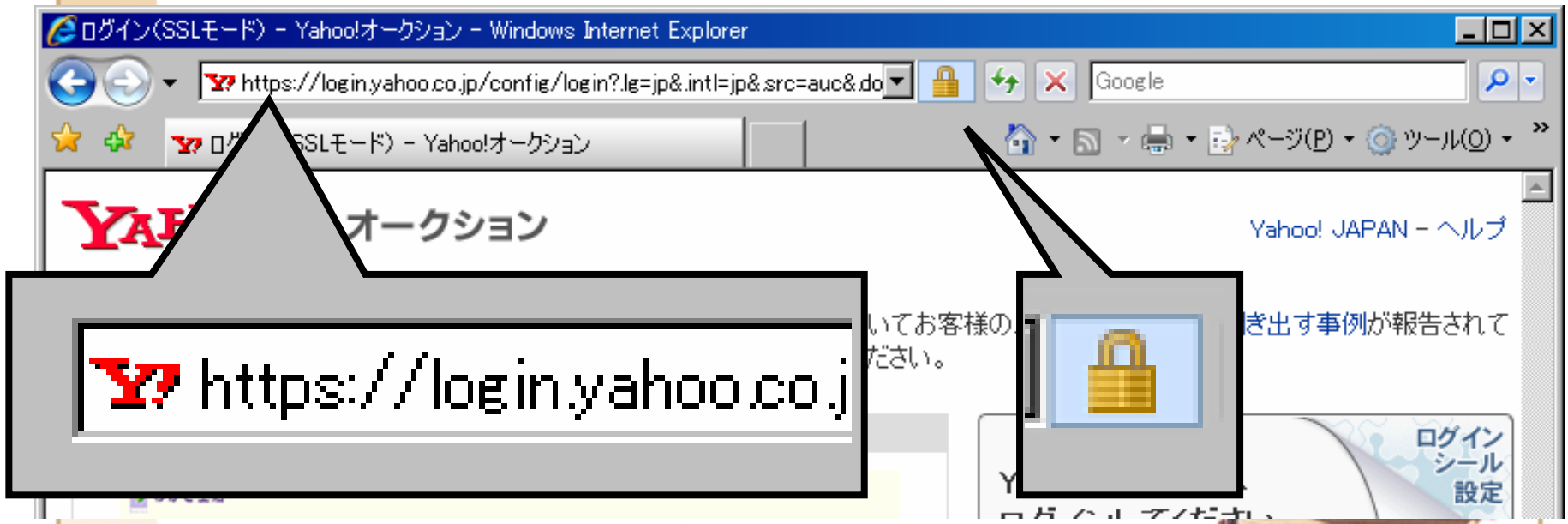
- 類似ドメインの氾濫
  - どれが本物でどれがニセモノ?
  - 「なりすまし」しやすい状況に。

- フィッシング詐欺
  - 偽サイトへの誘導
  - 偽サイト上での詐欺行為

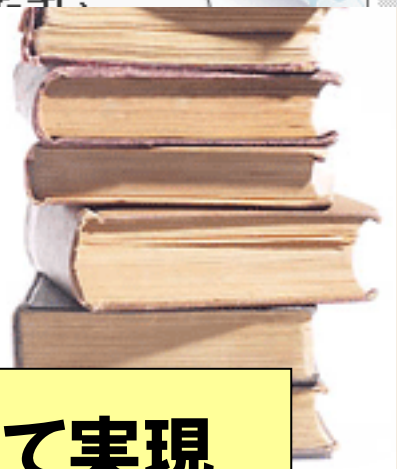
- 「サイト目利き」が増えた
  - クチコミサイト、Blog、SNS、etc.
  - ユーザのリテラシー向上

なりすまされない安全なサイト作りが社会的責任に

オンラインショッピングなどで使われるSSL



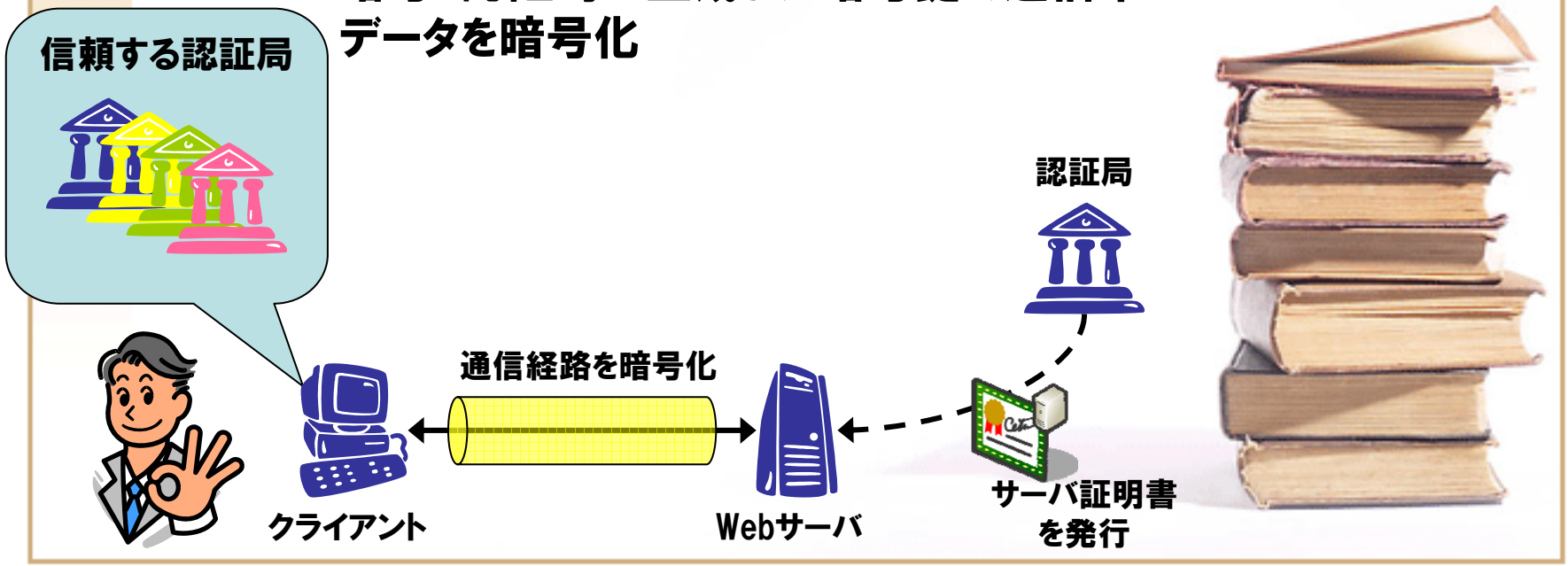
- https://～で始まるURL
- 通信が暗号化されていることを示す鍵マーク



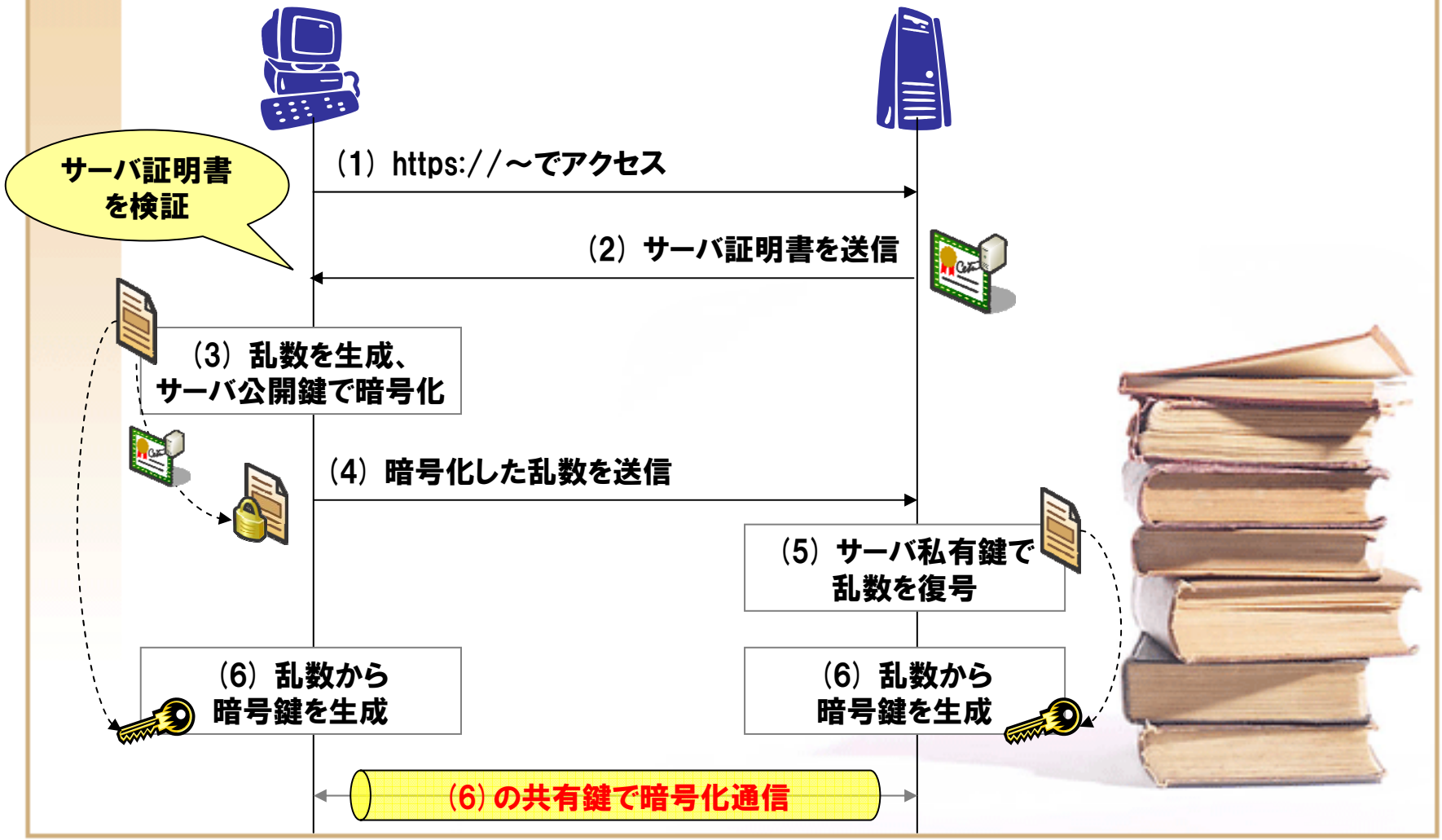
サーバ証明書を使ったSSL認証によって実現

SSL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
  - 認証: 信頼する認証局から発行された証明書を使って確認
  - 暗号: 認証時に生成した暗号鍵で通信中のデータを暗号化



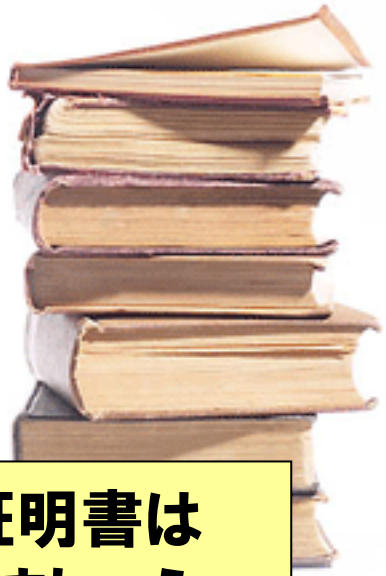
サーバ認証から暗号鍵の共有まで



サーバ証明書を発行する認証局

- 予めクライアントアプリケーションが信頼している認証局である必要あり。
- クライアント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?

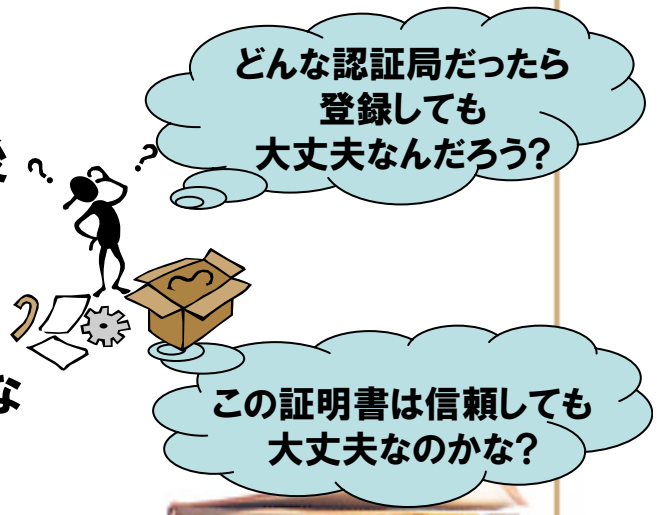
オープンドメイン認証局



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

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。

(サーバ証明書に関しては) 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

証明書用途に
適した確認内容

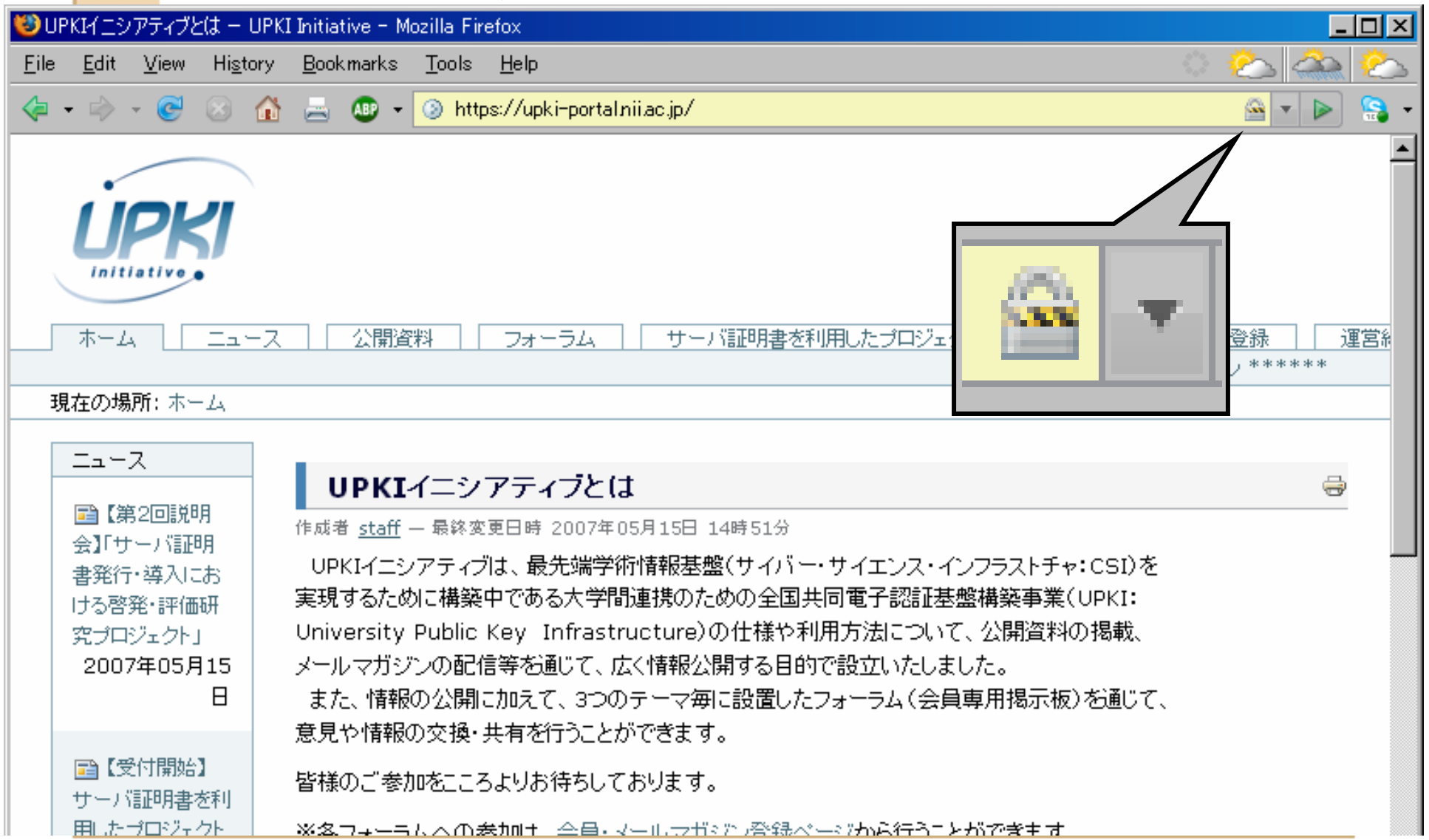
認定された認証局だから安心だね！
何も操作しなくても信頼できるから簡単だね！

余談：オープンドメイン認証局になるのは大変!!

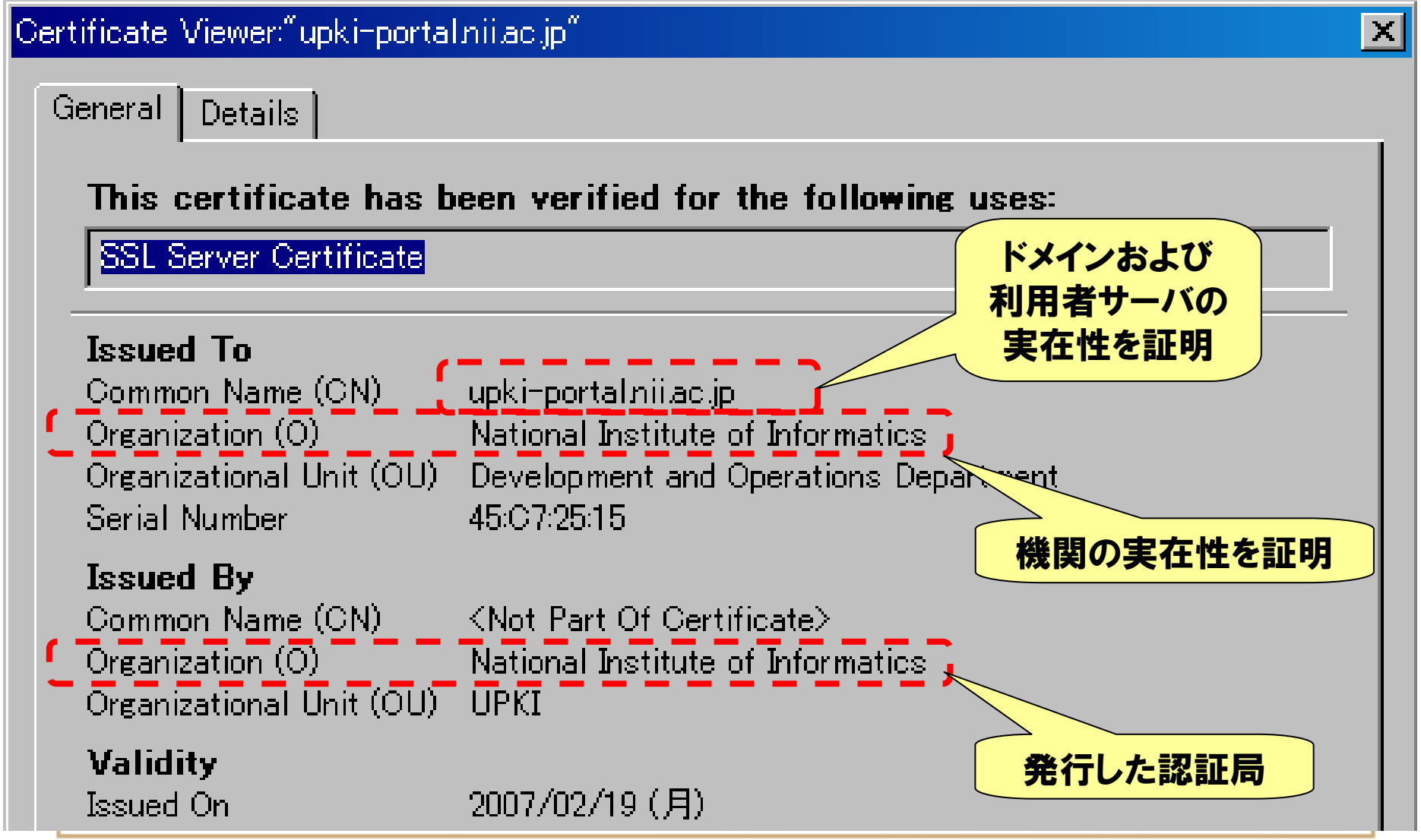
- WebTrust for CA規準
  - 認定取得コスト
  - 規準にもとづく運用
- 様々なPKIアプリケーションへの登録
  - 海外との交渉がほとんど
- 日本の特殊事情: 携帯
  - 機種毎に異なるブラウザ
  - キャリアとの交渉
  - 機種の世代交代

選択(1)：既存事業者から商用証明書を購入
選択(2)：既存ルート認証局の下位認証局を構築

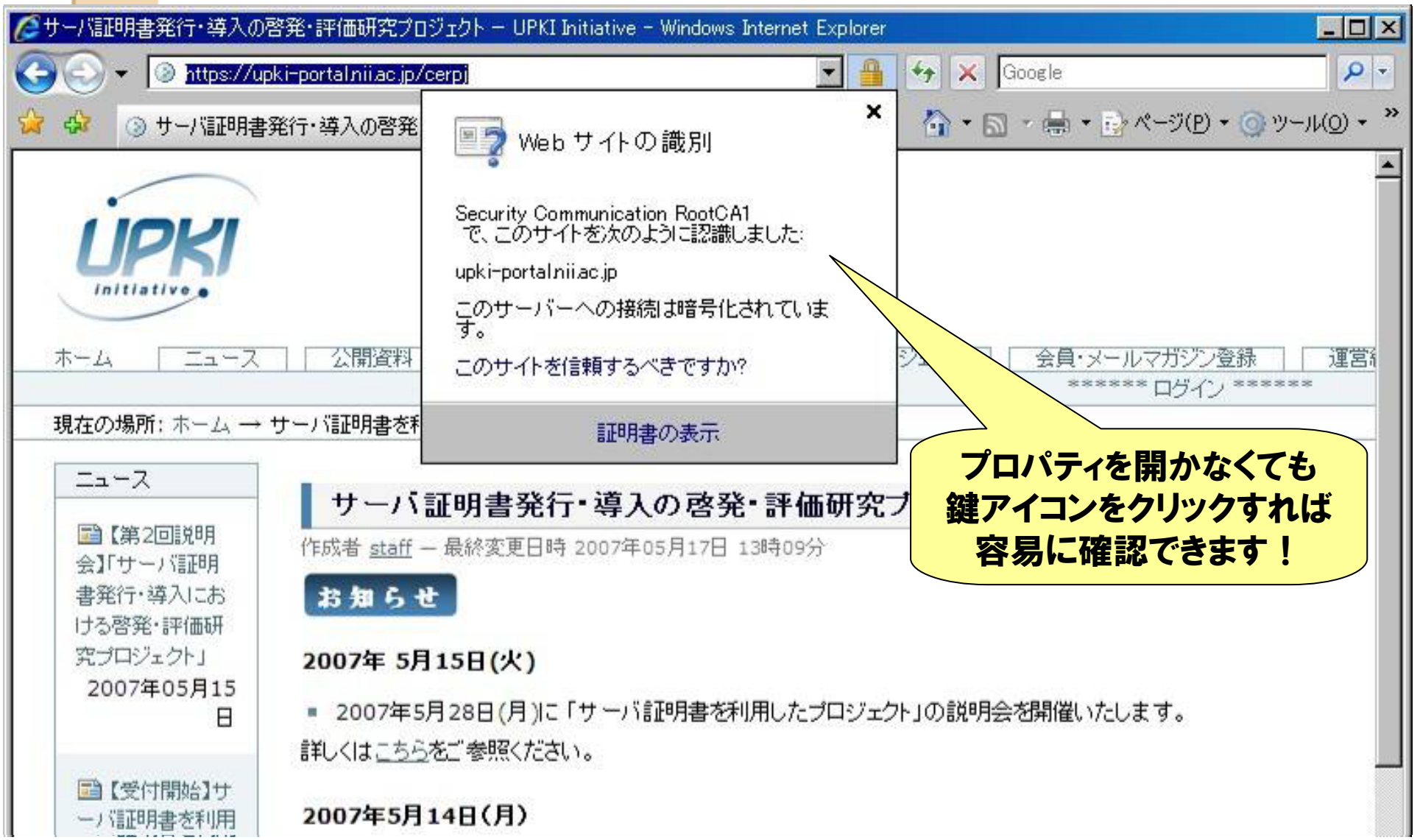
Firefoxで見るサーバ認証



Firefoxで見るサーバ認証



IE 7.0で見るサーバ認証



まとめ

- サーバ証明書の重要性
  - 盗聴、なりすまし、改竄に有効
  - 身許の明らかなサイト作りが社会的責任に
- 証明書を発行する認証局
  - オープンドメイン認証局の活用
  - 機関とドメインの実在性を証明
- ブラウザでの確認の仕方
  - 発行した認証局、サイトを運営する機関やドメインを確認できます

不特定多数の利用者に
オレオレ認証局や
オレオレ証明書はダメ！

ありがとうございました

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 <shimaoka@nii.ac.jp>