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

- フィッシング詐欺とSSL
  - SSL: Secure Socket Layer
- SSLの解説
- おまけ: PKIの基礎知識

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

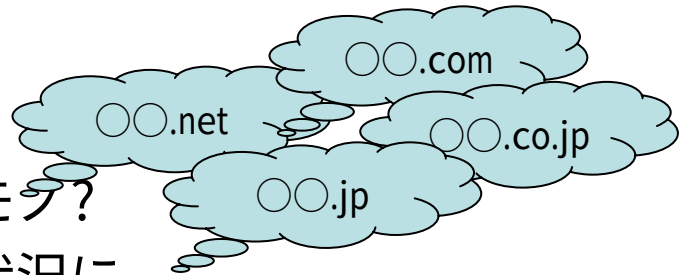
- (通信データの)改竄
  - 改竄された情報の受信
    - 悪意あるサイトへの誘導
    - 誤った情報による二次的な損害

通信経路の暗号化

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。



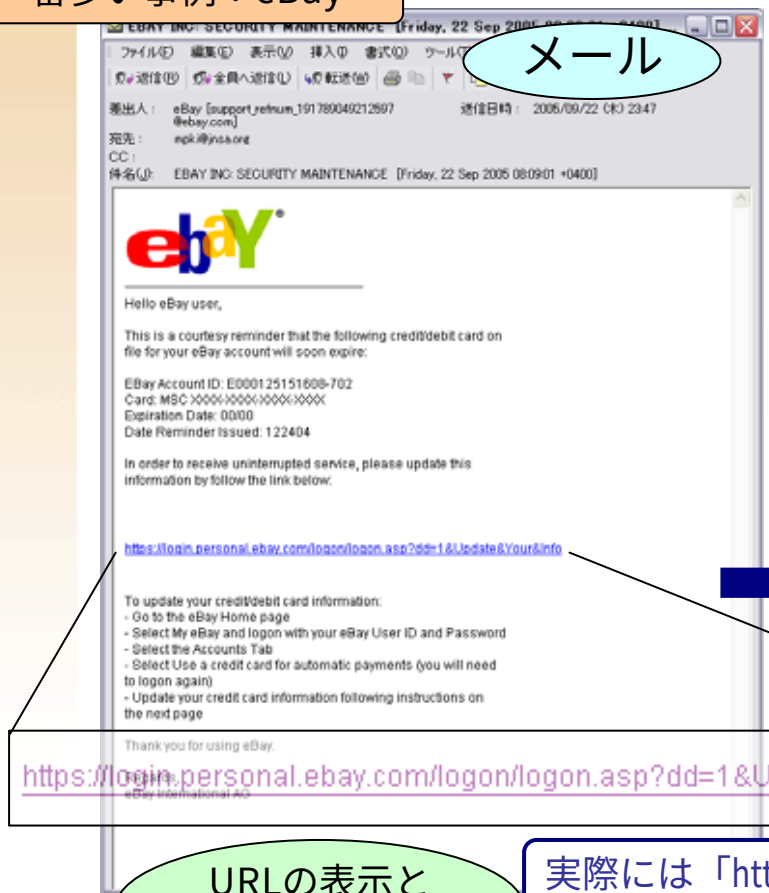
- フィッシング詐欺
  - 偽サイトへの誘導
  - 偽サイト上での詐欺行為

- 「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

サーバ管理者→なりすまされない安全なサイト作り
ユーザ→だまされないリテラシー

フィッシング事例：eBay

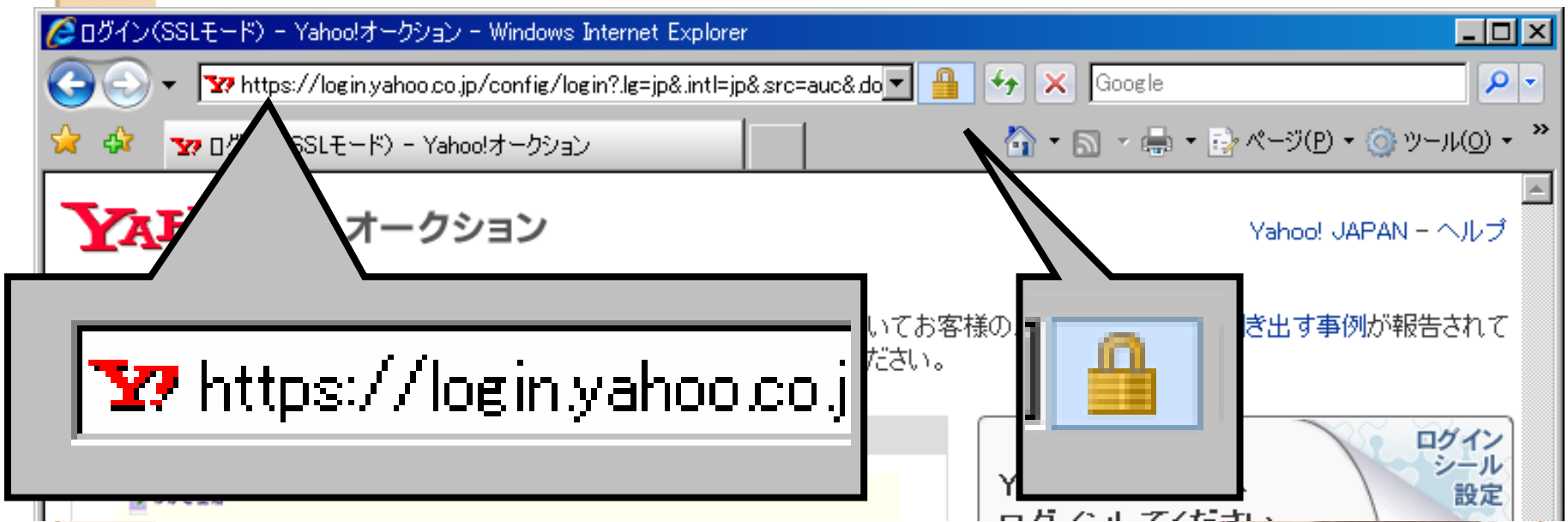
一番多い事例：eBay



URLの表示と
実際のリンク先

実際には「http://www.******.net/.www.eBay.com/eBayISAPI.php」

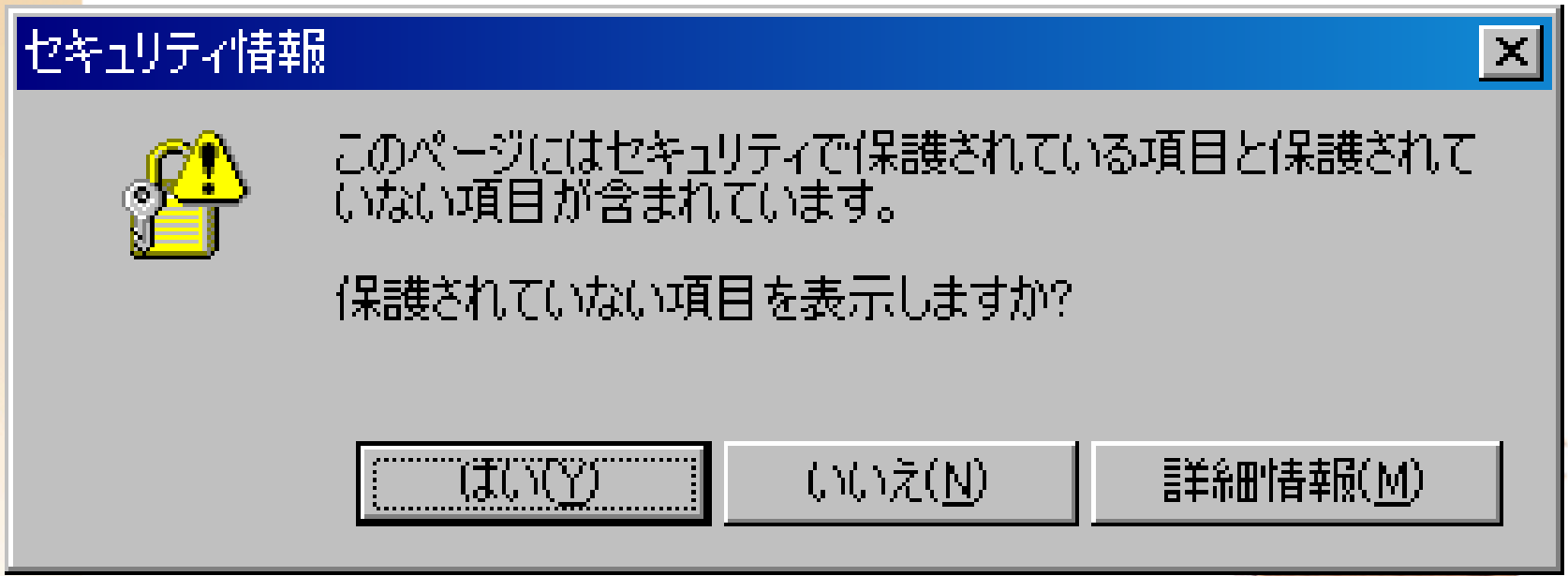
オンラインショッピングなどで使われるSSL



- 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

一見暗号化されているようでも…



- https://～で始まるURLでも、ページに含まれる画像等のURLがhttp://～で始まっている場合に表示されます。
- 送信する情報が暗号化されない可能性もあります！！

大学におけるサーバ証明書

サーバ証明書を導入したサーバのうち、
72%が認証用サーバ

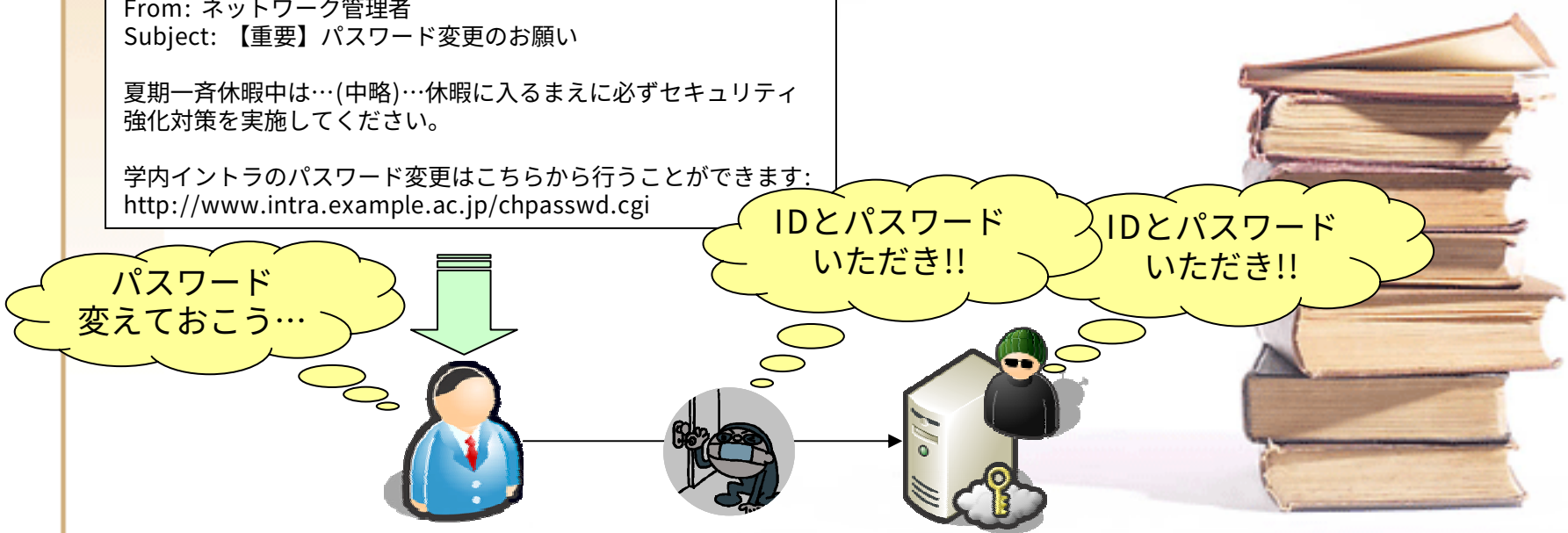
(NIIサーバ証明書プロジェクト H19年度末調査より)

- 認証サーバの真正性保証や通信経路の暗号化ができないと…

From: ネットワーク管理者
Subject: 【重要】パスワード変更のお願い

夏期一斉休暇中は…(中略)…休暇に入るまえに必ずセキュリティ強化対策を実施してください。

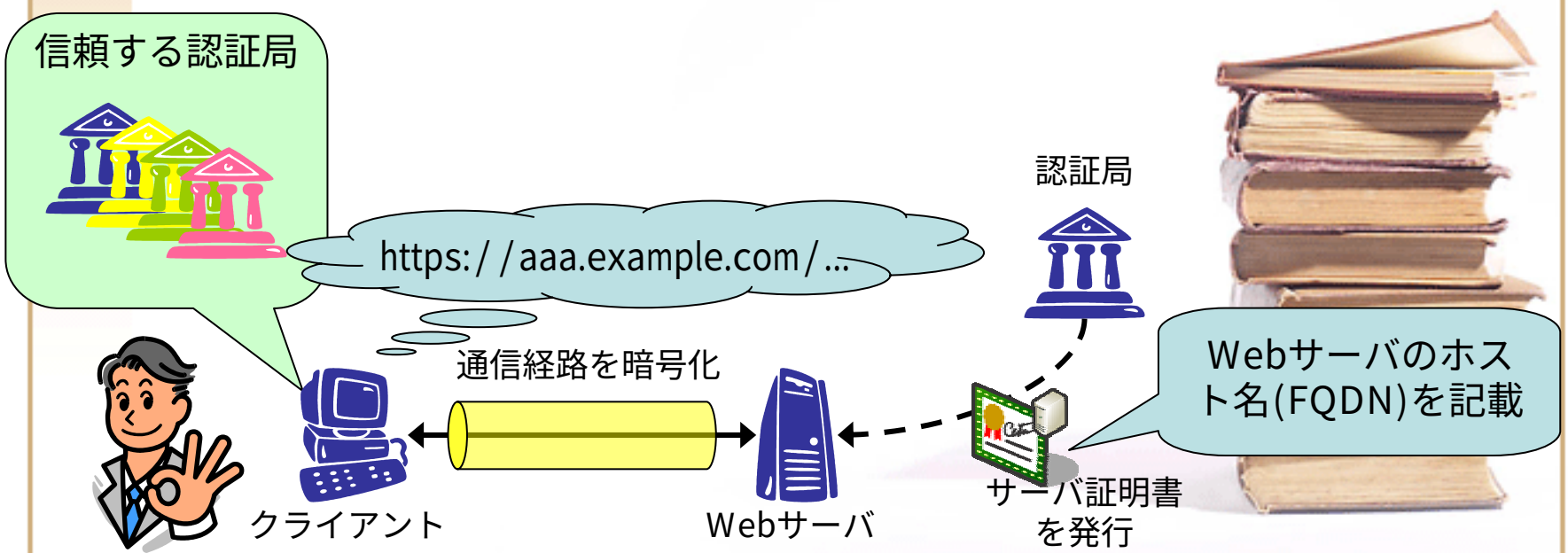
学内イントラのパスワード変更はこちらから行うことができます:
http://www.intra.example.ac.jp/chpasswd.cgi



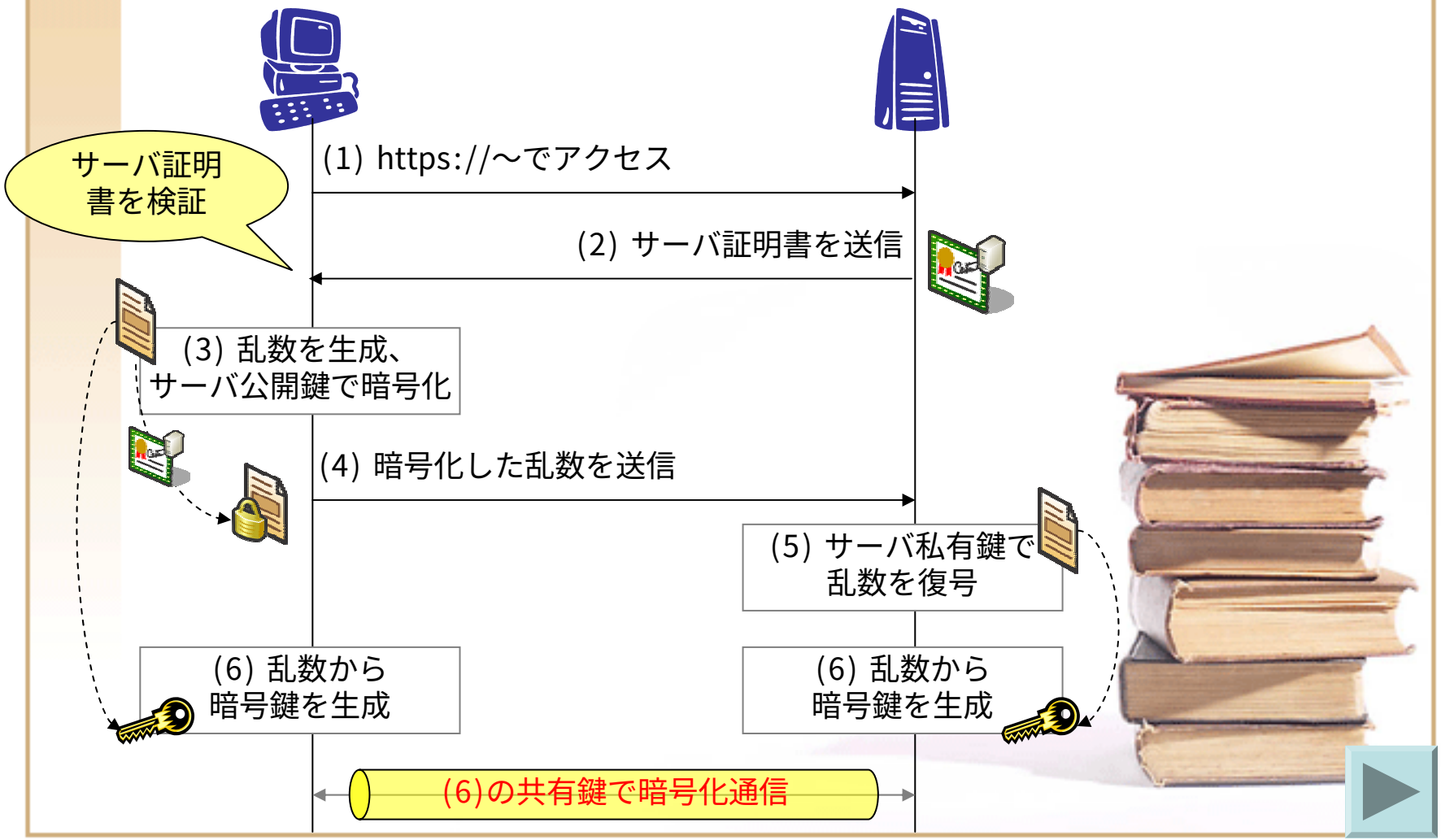
- フィッシング詐欺とSSL
- SSLの解説
- おまけ: PKIの基礎知識

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
    - 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”
  - 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



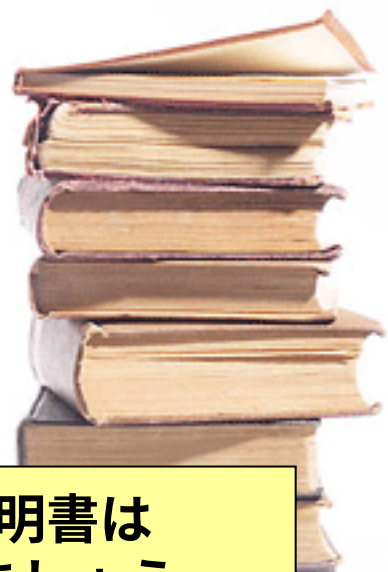
サーバ認証から暗号鍵の共有まで



サーバ証明書を発行する認証局

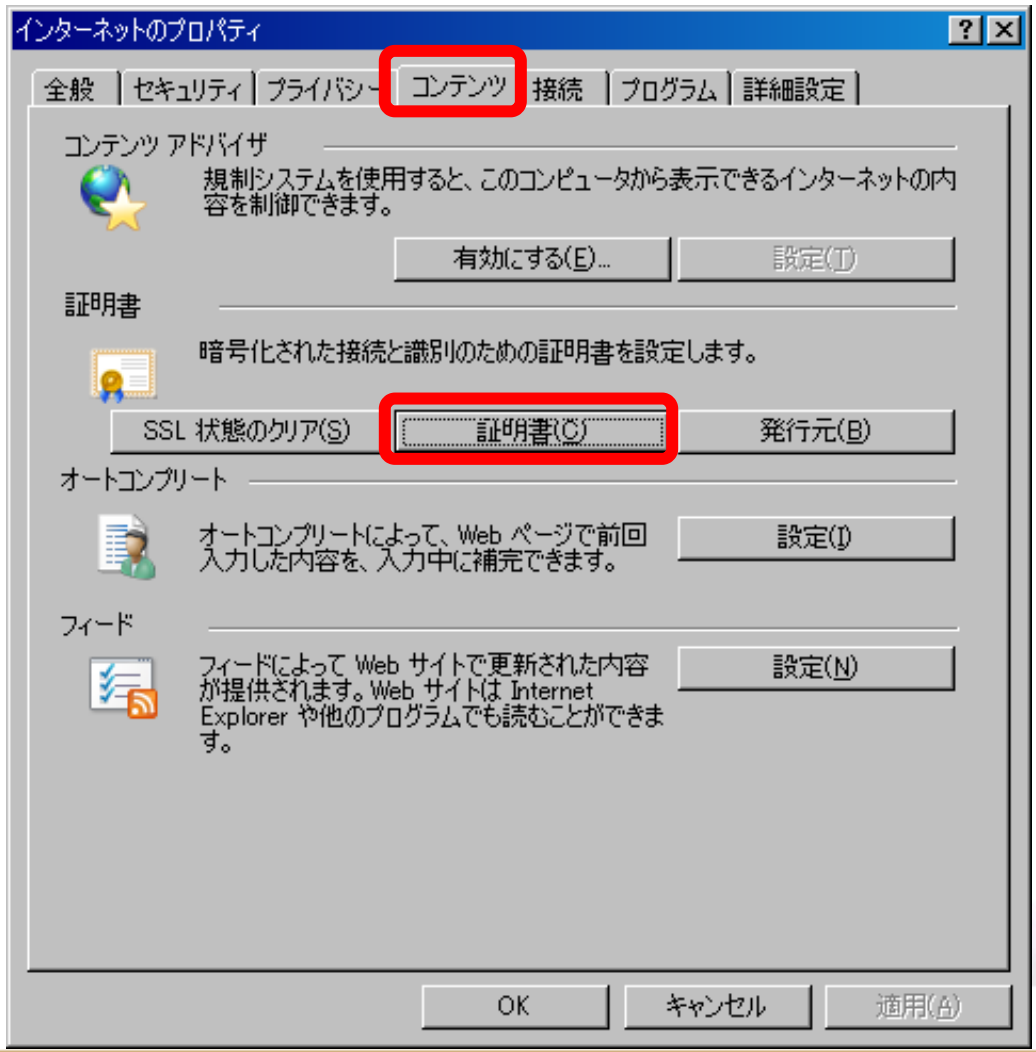
- 予めクライアント側のPKIアプリケーションが信頼している認証局でなければならない。
- 主要なPKIアプリケーションにはいくつかの認証局が予め登録されている。
  - IE: 「信頼されたルート証明機関」
  - Firefox: 「証明書マネージャ」
- ユーザが後付けで認証局を登録することも可能ですが…
  - 安全を保証できない認証局を登録することは非常に危険!!
  - 安全を保証できる認証局だと判断できますか?

オープンドメイン認証局

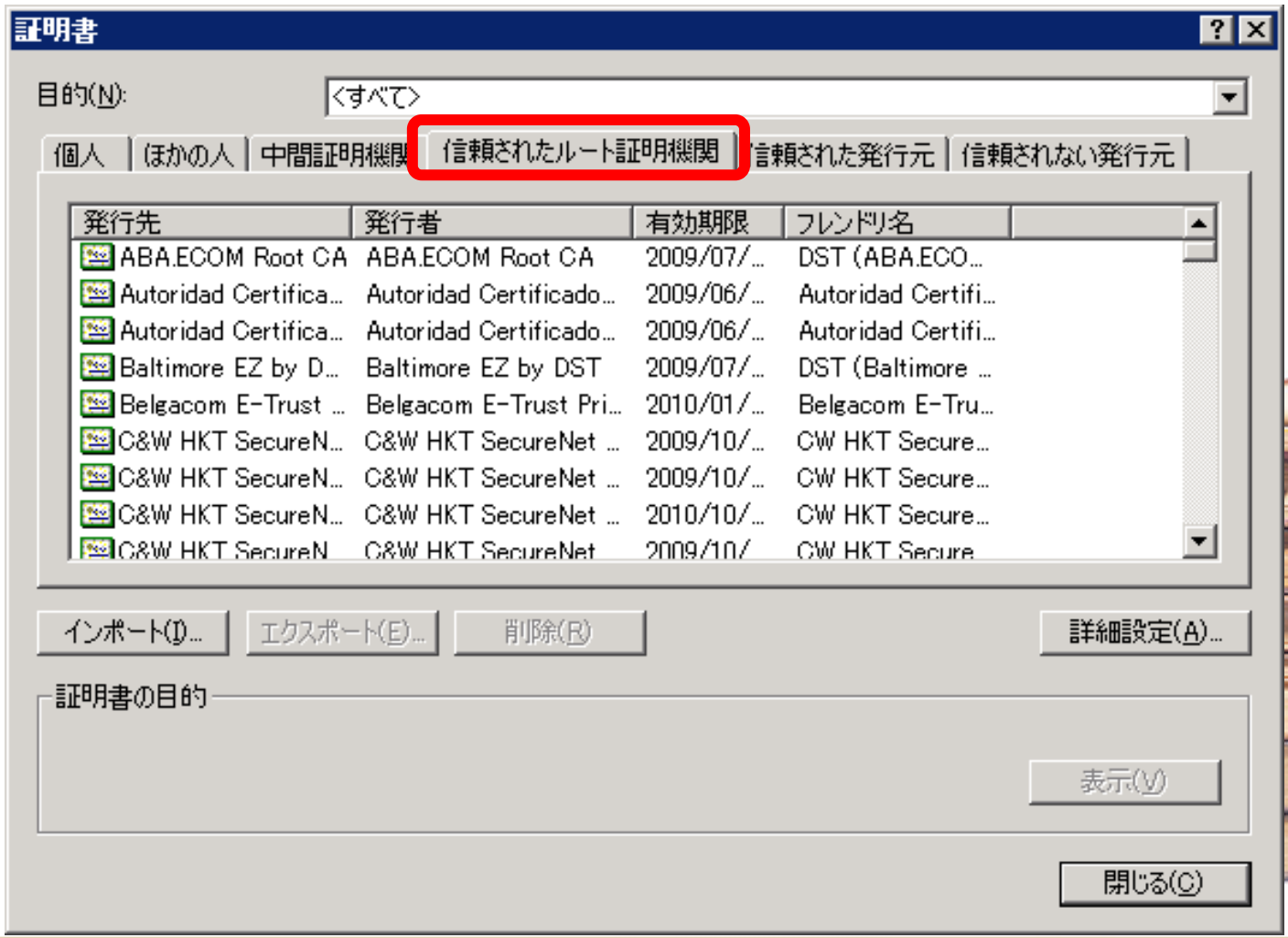


不特定多数がアクセスするサイトのサーバ証明書は
オープンドメイン認証局から発行してもらいましょう

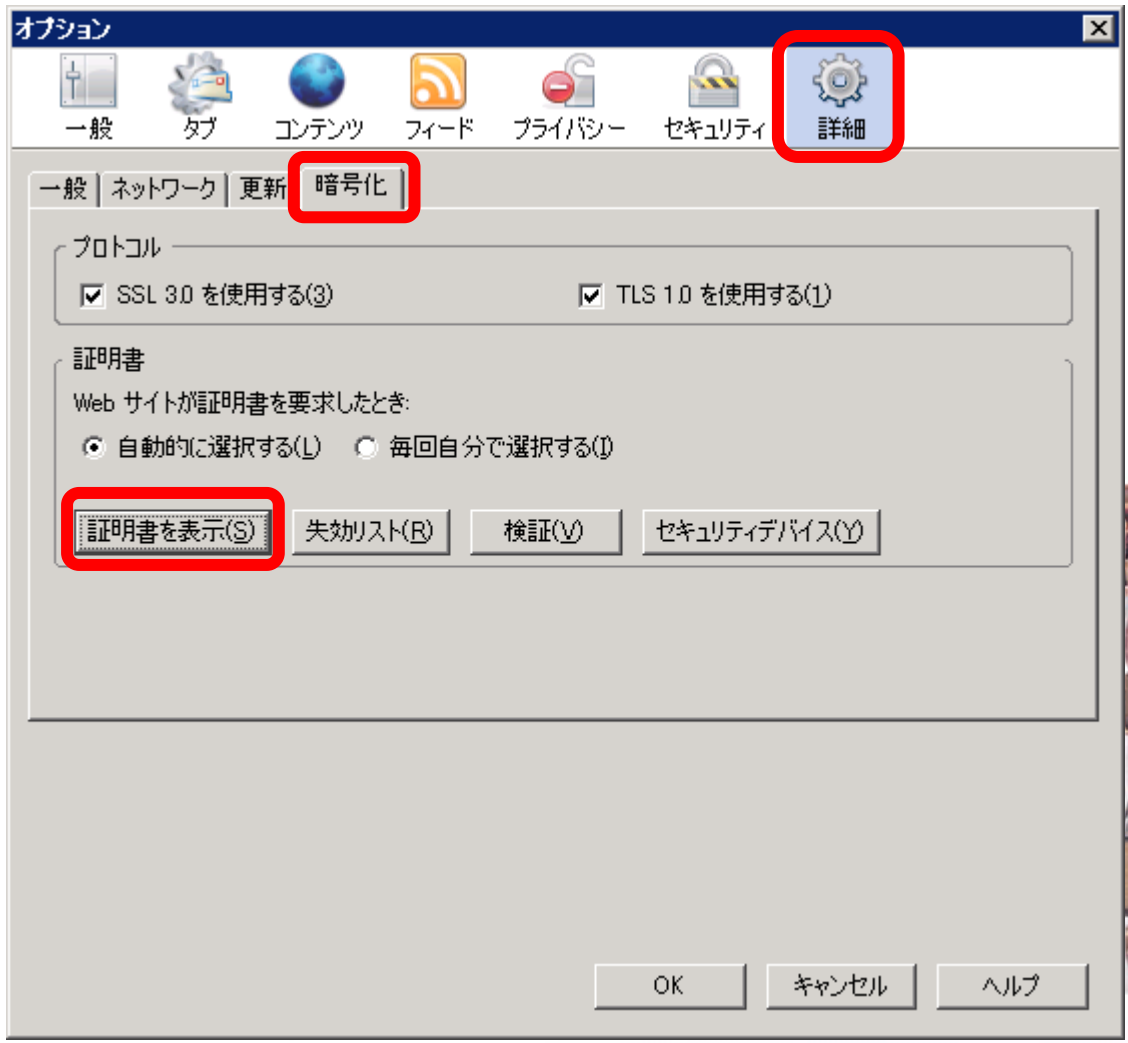
IEの証明書リスト(1)


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)

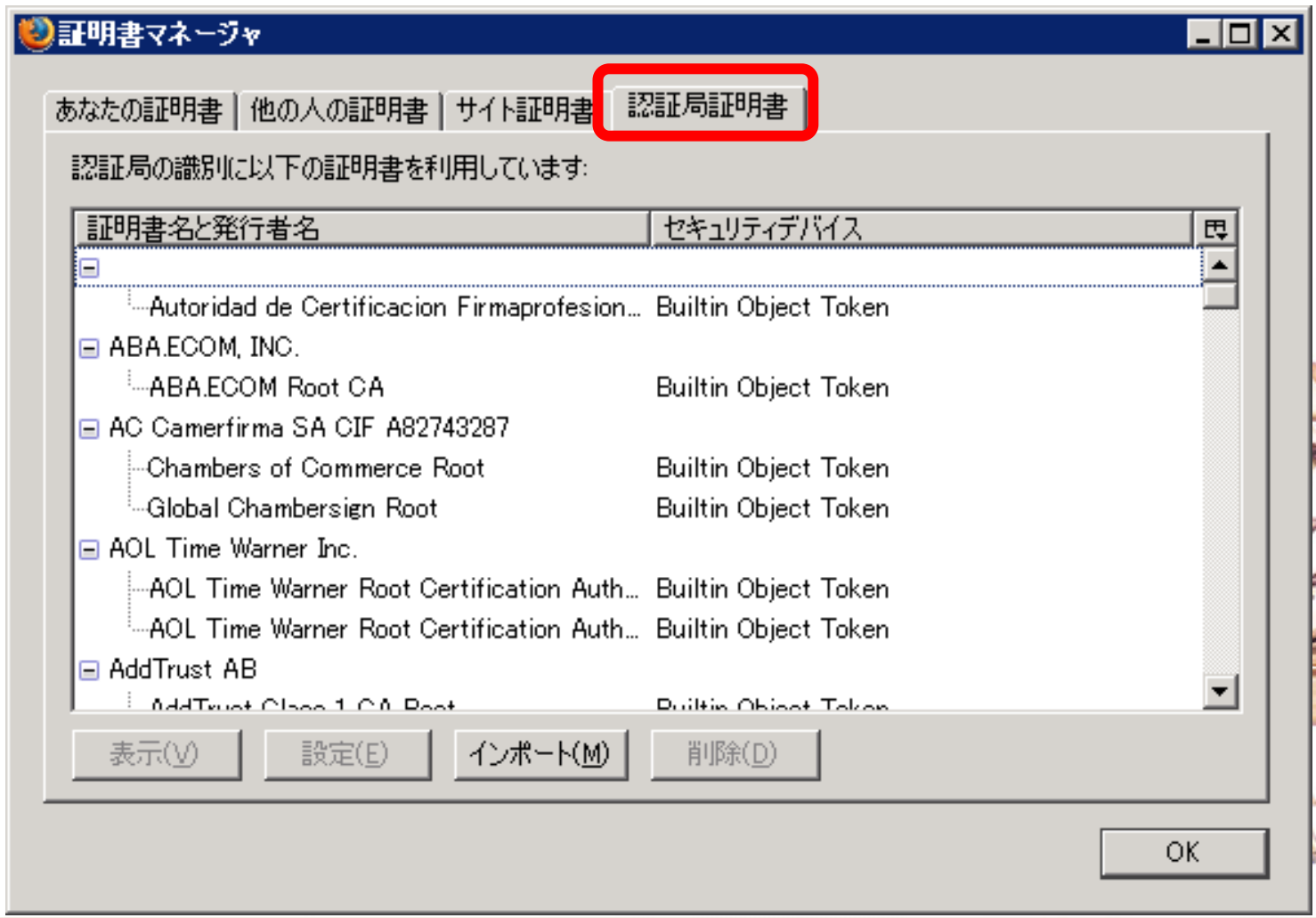
IEの証明書リスト(2)


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

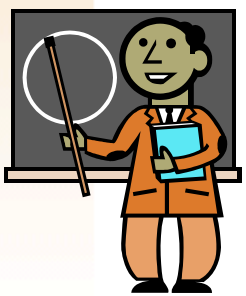
- オレオレ認証局
  - ユーザがクライアントアプリケーションに後から登録する必要がある認証局
- オレオレ証明書
  - 認証局からの信頼を何らかの追加手順なしには確認することができない証明書

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

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。

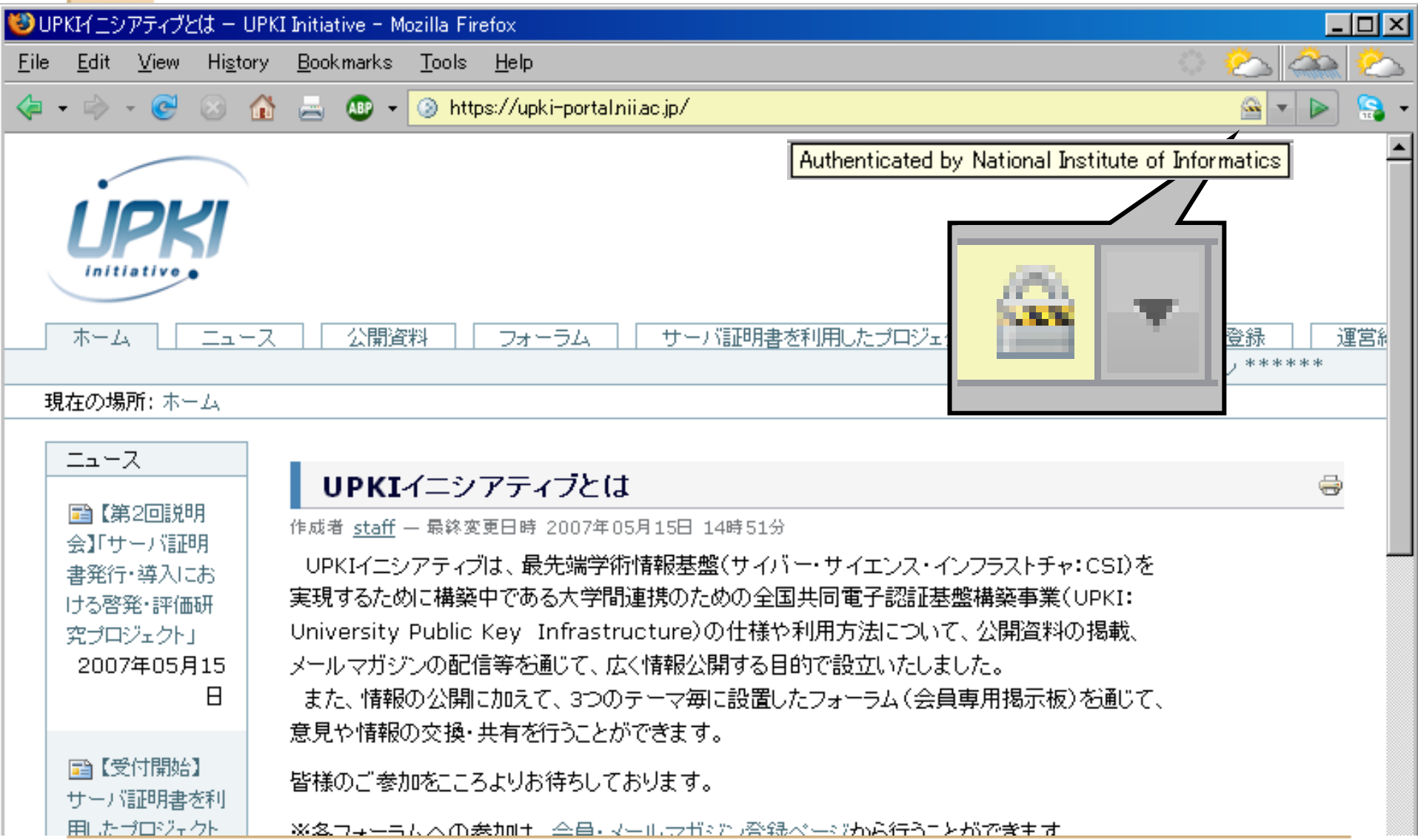
証明書用途に適
した確認内容

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！

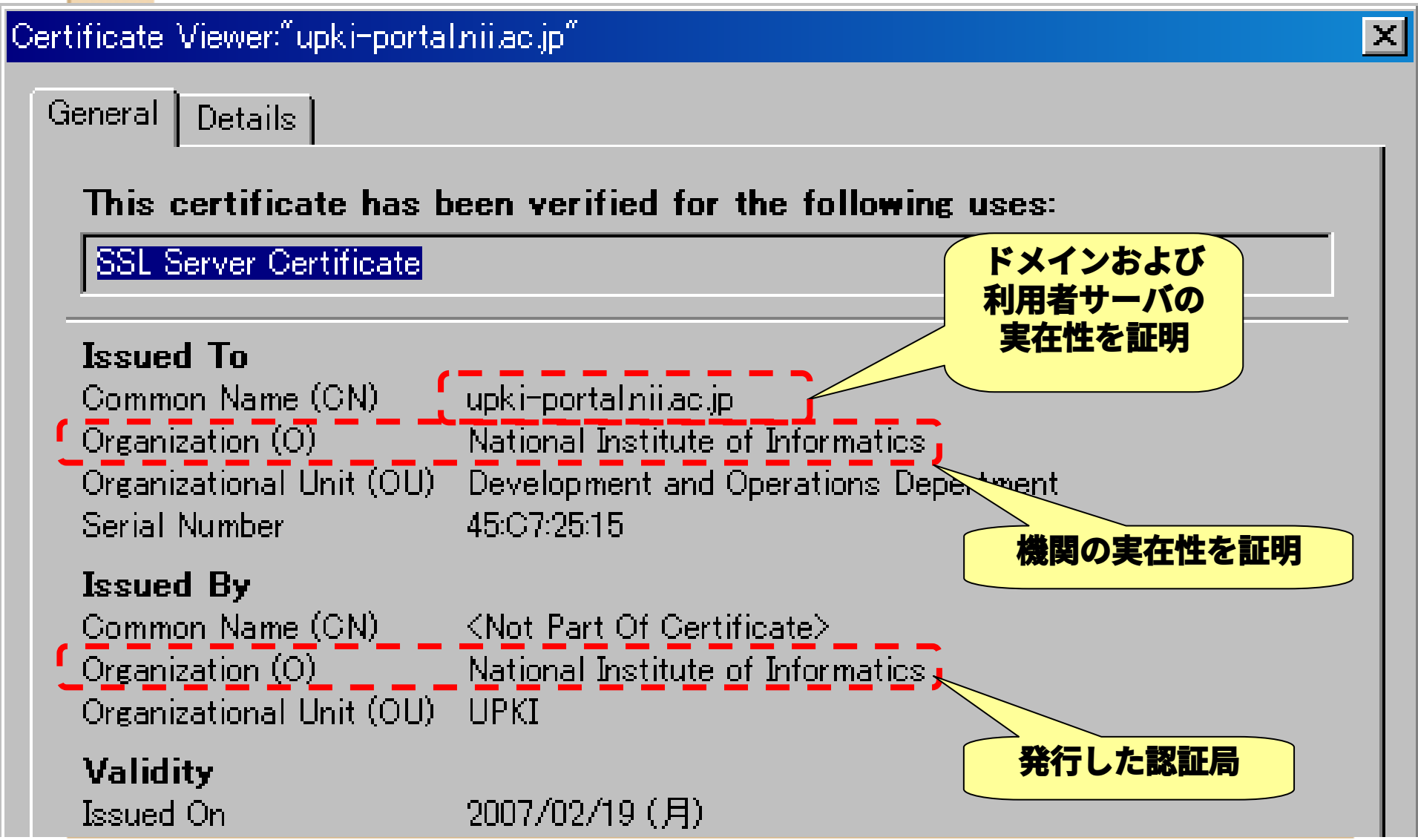
認証局を守る物理セキュリティ(例1)

認証局を守る物理セキュリティ(例2)

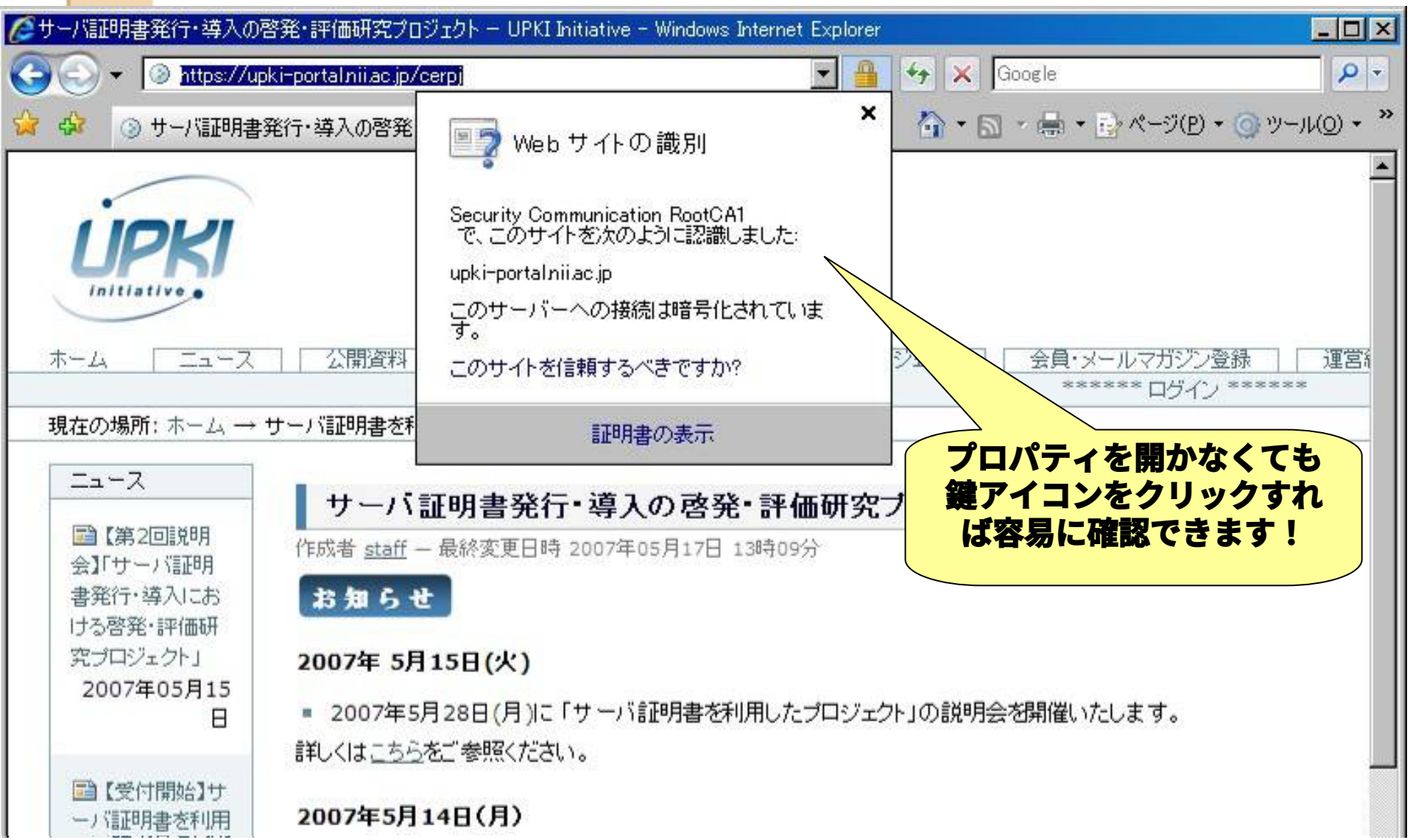
Firefoxで見るサーバ認証



Firefoxで見るサーバ認証



IE 7.0で見るサーバ認証



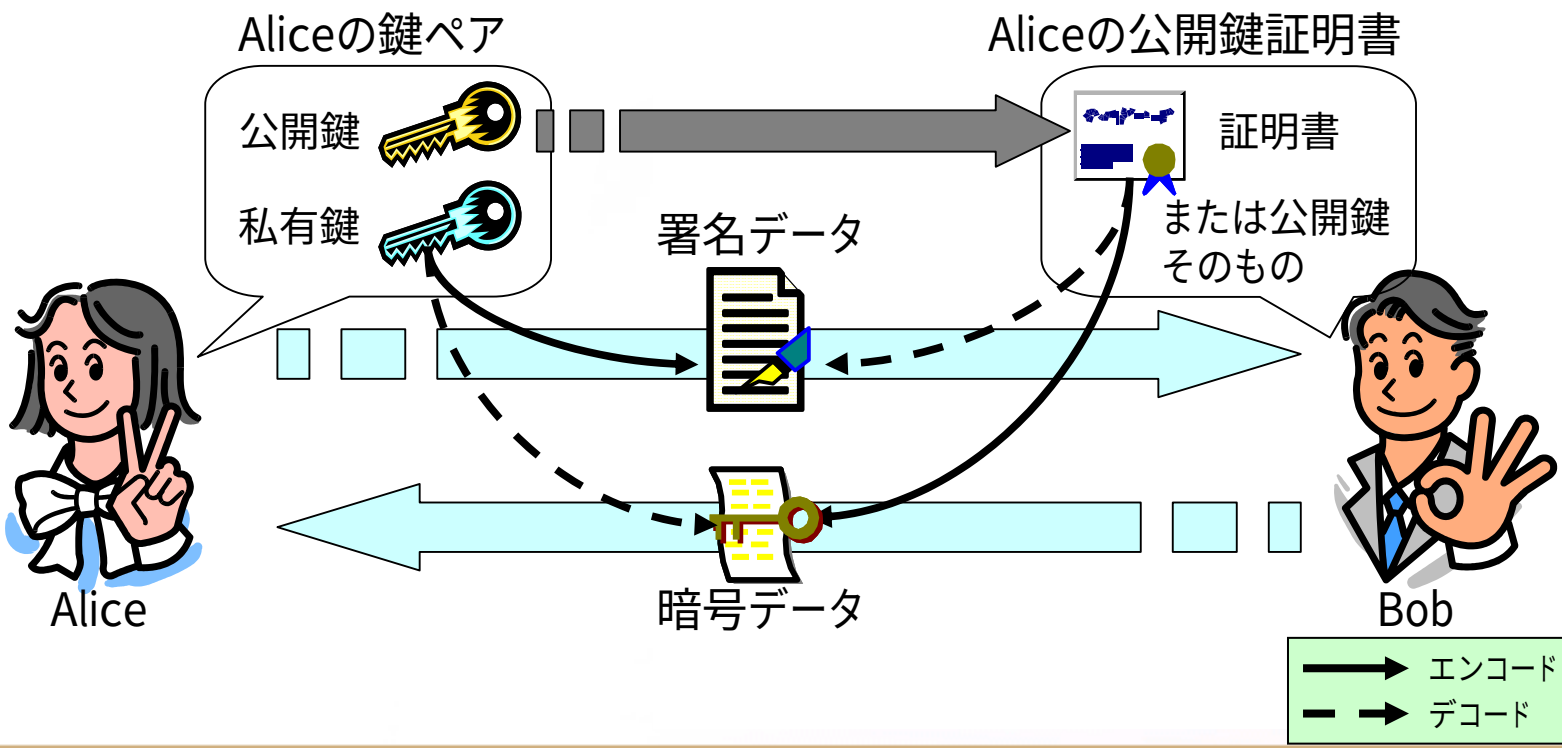
- フィッシング詐欺とSSL
- SSLの解説
- おまけ: PKIの基礎知識

PKI (Public Key Infrastructure)

- 広義には公開鍵認証基盤
  - 場合によってはPGPなども含めてPKIと言うこともある。
    - PGP: Pretty Good Privacy
- 狭義にはX.509(公開鍵)証明書を用いた、電子署名や暗号のフレームワーク
  - **秘匿性**(暗号)
    - 証明書の公開鍵で暗号
    - あるいは共通(暗号)鍵を安全に交換
  - **完全性**(署名)
    - 証明書を用いた署名検証によって改竄検知
  - **真正性**(認証)
    - 信頼のパスをたどることによって確認

署名/暗号の仕組み

- 以下の仕組みを利用して署名/暗号を実現
  - 公開鍵でエンコード(暗号)→私有鍵でデコード(復号)
  - 私有鍵でエンコード(署名)→公開鍵でデコード(検証)



PKIのエンティティ

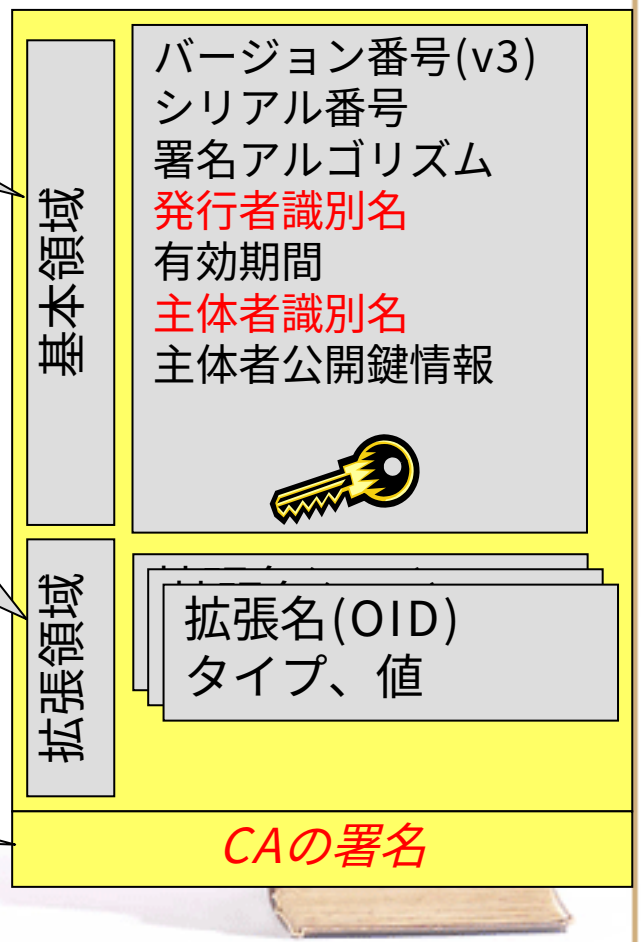
- サブスクライバ(Sc:Subscriber)
  - 認証局から証明書を発行されたエンティティ
  - 証明書に記載された公開鍵に紐づけられた私有鍵を持つ。
- リライングパーティ(Rp:Relying-party)
  - サブスクライバの証明書を検証するエンティティ
- 認証局(CA:Certification Authority)
  - 証明書を発行する機関
  - Scと利害関係を持たず、第三者信頼機関(TTP:Trusted Third-Party)であること。
- トラストアンカ
  - リライングパーティが信頼する認証局

X.509証明書フォーマット

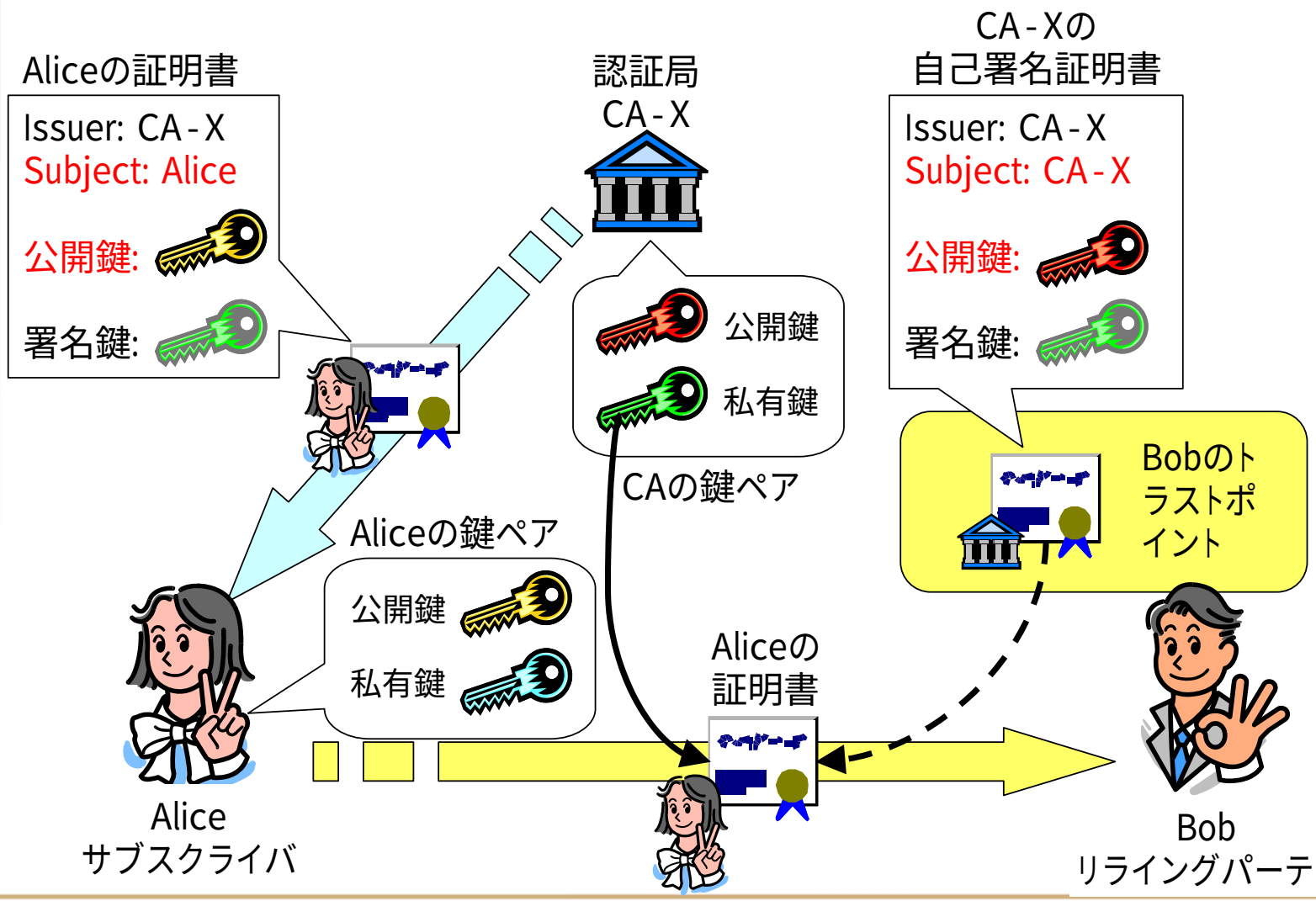
X.509証明書v1は基本領域のみ。
主体者公開鍵が含まれている。

X.509証明書v3で追加された領域。
鍵用途やCRL配布点、証明書ポリシなど16の標準拡張がある。
RFC3280では、この他に2つのインターネット拡張を定義している。
この拡張部分の処理が非常に難解。

基本領域、拡張領域を含めた全体に対してCAが署名することで、証明書内容の改竄を防止する。



信頼のリレー：「認証パス」


Aliceの証明書
Issuer: CA-X
Subject: Alice
公開鍵:
署名鍵:
認証局
CA-X
CA-Xの
自己署名証明書
Issuer: CA-X
Subject: CA-X
公開鍵:
署名鍵:
公開鍵
私有鍵
CAの鍵ペア
Bobのト
ラストポ
イント
Aliceの鍵ペア
公開鍵
私有鍵
Aliceの
証明書
Alice
サブスクライバ
Bob
リライングパーティ

まとめ

- サーバ証明書の重要性
  - フィッシング詐欺対策に限らず重要
  - 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
  - その通信は暗号化されていますか?

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>