Webを支える情報通信技術(12)
～ PKI ～

佐藤周行、中山雅哉、西村健

先週の復習

- サーバ証明書
  - 公開鍵とサーバ(名)を結びつけるもの
  - ↑の正しさを証明するもの

  - 演習:Webサーバへの組み込み(SSL対応+証明書)

今週の内容

- PKI (Public Key Infrastructure)

クライアントの観点から:
通信先は大丈夫？

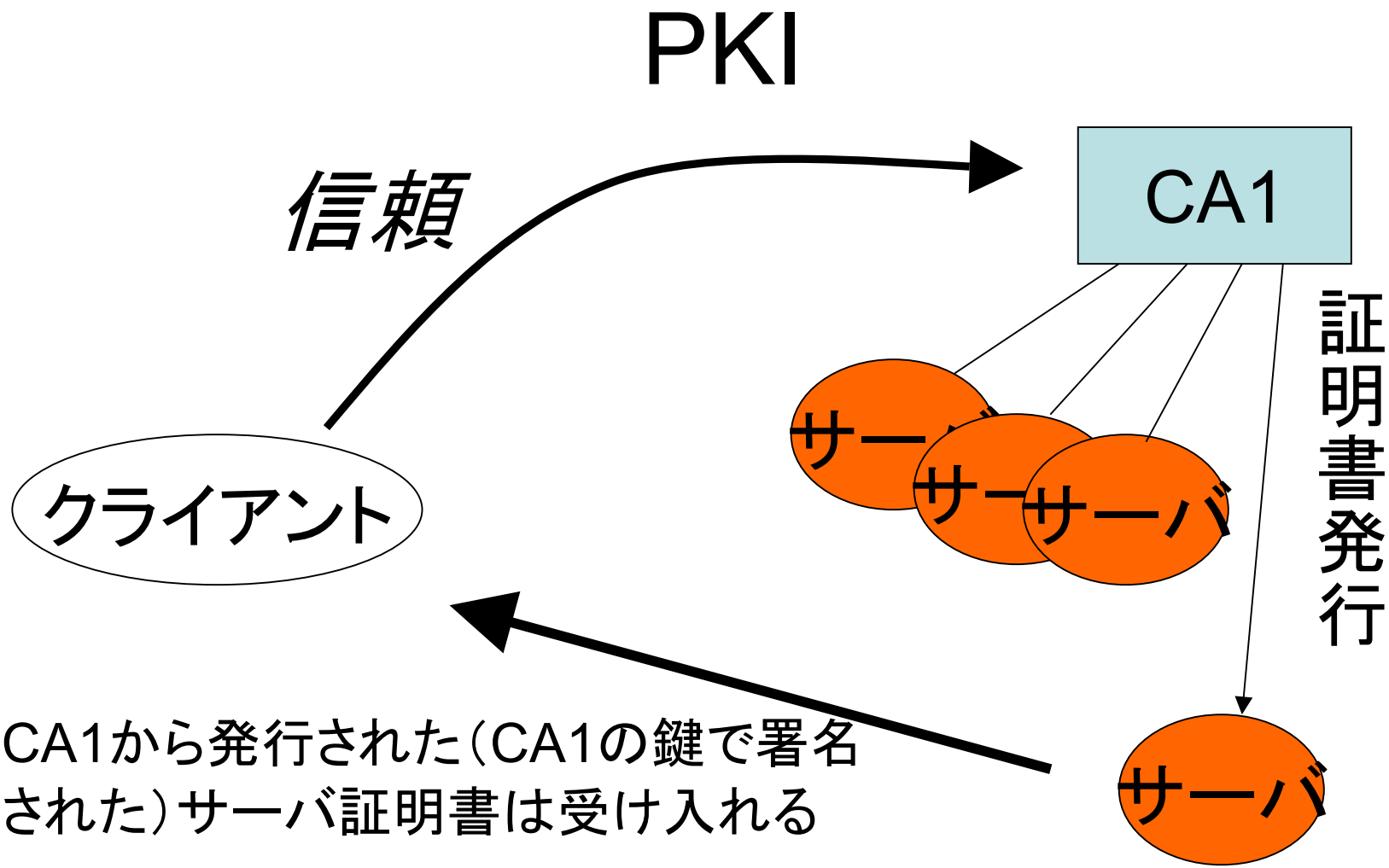
- Man in the Middle Attack
  - 第三者によって通信を介入された状態
- 参考:フィッシングサイト
  - メールのリンクをたどるなど
  - 本物と似たような体裁をとっている
  - そもそもアクセス先がニセモノ

暗号化の問題点の変遷

- そもそも共通鍵の共有方法どうするの？
  ↓　公開鍵暗号
- 使用アルゴリズムの合意方法は？公開鍵の配布方法は？
  ↓　SSLプロトコル
- 公開鍵と対象（Webサイト）の紐付け
  ↓　公開鍵証明書
- 電子署名自体が信用できない　←いまここ
  ↓　PKI
- 認証局が*信頼*できるものであればOK

PKI (Public Key Infrastructure)

- 公開鍵基盤（公開鍵暗号基盤、公開鍵認証基盤とも）
- 世の多くの人が信頼する認証局(Certification Authority, CA)を構築し、認証局が各サーバに証明書を発行する
  - つまり、認証局が独自の鍵ペアを持ち、サーバ証明書の署名は認証局の秘密鍵により生成される
- 商用認証局の有名どころはVeriSign, Thawte, GeoTrust, Comodoなど


PKI
信頼
CA1
証明書発行
サーバ
サーバ
サーバ
クライアント
サーバ
CA1から発行された（CA1の鍵で署名
された）サーバ証明書は受け入れる

信頼の仕方

- SSLを行なうアプリケーション（e.g. ブラウザ）が管理していることが多い
  - ブラウザに認証局の公開鍵（自己署名証明書、認証局証明書）が最初からインストールされている場合
  - 安全な手段により認証局証明書を取得し、それを自らインストールする場合

演習：世の中のSSLサーバの証明書を確認してみよう

- Safariにて、ウィンドウ右上の南京錠マーク（もしあれば）をクリックすると証明書階層が表示される

```
https://kiku.itc.u-tokyo.ac.jp/
```

演習：サーバ証明書を発行してもらう

- 自Webサーバのサーバ証明書を認証局から発行されたものと入れ替える
- ライセンスID:
  WS0001-XXXXXX-XXXXXX-XXXXXX

確認方法

- Firefoxを起動しhttps://test.pki.itc.u-tokyo.ac.jp/wsca_ra/airegistにアクセス
- 一番下の[CA証明書をダウンロード]から認証局証明書をダウンロード
- メニュー左上の[Firefox]→[環境設定]→[詳細]→[暗号化]→[証明書を表示]→[認証局証明書]→[インポート]でインストール
- Firefoxで自Webサーバにアクセスしてみる

- 実験終了後はCA証明書を削除（アンインストール）しておくこと

現状のサーバ証明書

- ブラウザが信頼している認証局は玉石混淆
- 最低レベルのものはドメインの存在（正しく使用されていることの）確認のみ
  - ドメインを確認できる状況でないと意味がない
    - サーバ証明書を持つフィッシングサイト(2006/02)
  - ちゃんとした会社が運営してる？

  →認証局の目視確認？
  EV (Extended Validation) SSL Certificate

PKIの他の利用例

- サーバでなく個人に対する身元確認
  - SSLクライアント認証
    - SSL/TLSの使用の一部
- メールの暗号化・電子署名
  - S/MIME
- 文書に対する電子署名
  - XML署名
  - 電子カルテ