IPA
Information-technology Promotion Agency, Japan

基調講演
「経営幹部に PKI を理解してもらうためには…」

公開鍵暗号技術を応用する
ネットワーク社会における信頼関係の基盤

2005年10月28日 金曜日

独立行政法人 情報処理推進機構
セキュリティセンター
情報セキュリティ技術ラボラトリー
宮川 寧夫

IPA
Information-technology Promotion Agency, Japan

PKI についての関心が高まっている一方で…

- PKI 技術は，（やはり）難しい．
  - 情報セキュリティ技術分野の中でも，とりわけ難しい．
    - 「難しさ」の意味合い：
      - 複合技術ゆえ→複雑
      - 複数の（社会的）目的を許容・実現する
        - » 本人認証，経路の守秘，デジタル署名・検証等
      - 人間を対象とする場合以外に，デジタル文書，デバイス等を対象とする場合もある

      技術者であれば，時間をかければ必ず理解できるようになる！
    - 今日のネットワークセキュリティ技術：
      - 社会的な目的に関する技術ゆえ
        - » 技術者以外も巻き込まれる
          （例：電子商取引，phishing 対策等）

      非技術者に対して，上手に（かつ，正しく）説明する必要がある

IPA
Information-technology Promotion Agency, Japan

説明における戦略

1. PKI の社会的性格から説明する
   - 経営幹部は，社会的存在
     - 社会的な目的から導く説明に慣れている
       - *注意：PKI の目的は，単一ではない！*

2. 本質的な難しさ（複雑性）も説明してしまう
   - 経営幹部は，簡潔な説明を求めるが…
     - 短時間に完全に理解することは，不可能
     - 「複雑であること」については，説明可能

3. 技術者の良心にかけて
   - 適切な用語と比喩をつかう

3

IPA
Information-technology Promotion Agency, Japan

PKI の社会的性格から説明する

PKI の説明方法 1

- よく行われているであろう説明方法
  - （名詞どおり）公開鍵暗号技術の応用として説明
    - ‘Public Key (Cryptography)’ Infrastructure
    - ボトムアップ的な説明方法

    公開鍵暗号技術から説明すると…

    全体像にたどり着くことができない！

4

Information-technology Promotion Agency, Japan

PKI の社会的性格から説明する（つづき）

公開鍵暗号技術から説明すると…

- 歴史・変遷
  - 公開鍵暗号技術の発明から？
    - Whitfield Diffie, Martin E. Hellman, “New Directions in Cryptography”, 1976.
    - (James Ellis, Cliff Cocks, CESG, 1973)

現在の PKI 技術にたどり着くことができない…

Dr. Whitfield Diffie, *Sun Fellow and Chief Security Officer of Sun Microsystems, Inc.*

"Building public key infrastructure that realizes the promise of public key cryptography has proved more difficult than anyone imagined when Marty Hellman and I came up with the idea of public key systems in the 1970s,"

Support for OASIS PKI Action Plan, 2004

5

Information-technology Promotion Agency, Japan

PKI の社会的性格から説明する（つづき）

- 複合技術ゆえ…
  - 暗号技術の範囲内においても，公開鍵暗号技術だけが使われるわけではない
    - 暗号化・復号：組み合わせの中で，共通鍵暗号技術の役割
    - 署名：組み合わせの中でセキュア・ハッシュ関数の結果について
  - X.509証明書の導入
    - PEM , S/MIME v2, S/MIME v3
    - 説明者に広範な関連知識が要求される
    - X.509証明書項目, ASN.1表記, UTF8String…難関がいっぱい

肝心な PKI らしい論点（例：複数の社会的目的があること，信頼関係の連鎖等）まで説明が至らなくなってしまう…

6

Information-technology Promotion Agency, Japan

PKIの社会的性格から説明する（つづき）

- PKI の説明方法 2
  - お勧めする説明方法
    - 信頼関係モデル（trust model）から説明する
      - 信頼関係モデルは，社会的モデル
    - 「認証局」なる存在を「階層型」信頼関係モデルに位置づける
      - 注：認証局がひとつの場合を説明することが基本となるが，この場合だけでは「階層型」の意味も「信頼関係の連鎖」も理解できない．
        - » *「信頼関係の連鎖」が理解できないと，PKIの肝心なことを理解できない！*
    - 「デジタル証明書（certificate）」について
      - X.509等，技術仕様の用語よりも…
      - 証明書ポリシー（CP：Certificate Policy）を説明する．
        - » *注：“Certification Policy”という用語は無い！*

Information-technology Promotion Agency, Japan

信頼関係モデル（trust model）

- 「信頼関係モデル」
  - ネットワーク越しに存在する者同士の間の「信頼関係（trust）」の類型化
    - ここにいう’trust’とは？
      「認定結果を信頼する」の意

「階層型」信頼関係モデルを説明する前に…

- Web of trust：錯綜した信頼関係

  仮面を被った国において…
  - AさんとBさんがお互いに本人であると知っており，そのBさんが「Cさんと Dさんがお互いに本人と知りあっていること」を知るとき，Dさんが Eさんが本人と知った場合，Aさんは，Eさんが本人であると信頼できるか？

  自分が知っていることを信頼することが基本となる世界
  - 確かめられそうだが面倒…
  - Bさんが記憶喪失になったら？

Information-technology Promotion Agency, Japan

信頼関係モデル (trust model) つづき

「階層型」信頼関係モデルを説明する前に…

– Trust file が在る世界：(例：web ブラウザの中)

「これらの方々は，本人です．」と認定するリストがある世界

- 「そのリストを作った方は，何様ですか？」
- 「私も，そのリスト (ファイル) に載せてください．」

「階層型」信頼関係モデルの世界

– 世の中の信頼関係の整理論：

あたかもデータをディレクトリに整理するかのように…

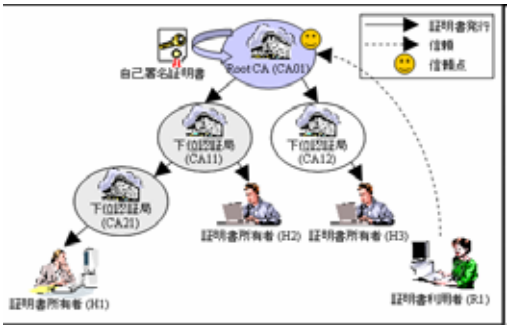
・「認証局 (CA：Certification Authority)」登場

– 同時に「インフラストラクチャ」出現

「認定局」と言いたいところ…

Information-technology Promotion Agency, Japan

「階層型」信頼関係モデル



- 「認証局 (CA：Certification Authority)」は，大勢について，本人であることを知っており，個別に本人であることを「認定 (certification)」する証明書 (certificate) を有効期間を設けて発行してくれる．
  – 注：「本人認証／デバイス認証 (authentication)」
- 「認証局」は，他の「認証局」を本人であると認定して，証明書を発行することがあり，信頼関係が連鎖する．

今日の (X.509証明書を用いる) PKIは，階層型信頼関係モデルに馴染む．

IPA
Information-technology Promotion Agency, Japan

「信頼の連鎖」の十分性検証

用語（英単語と翻訳）に注意！

- **認定パス** (certification path)
  - **本人であることを認定する連鎖（基本形：上位→下位）**
  - **信頼関係の連鎖（但し，方向性あり）**
    - **認定パスについての十分性検証方法** (path validation)
      - **「証明書」が連鎖し、そのすべての証明書が有効であること**
      - **「最後の証明書の検証」を含む**

      複数ドメインの PKI の認定パス（信頼関係）は？

- **本人認証** (authentication)
  - PKI **において：「最後の証明書の検証** (certificate validation)」
    - **該当する証明書上のデジタル署名についての公開鍵暗号技術的な検証**
    - DN **という名前の一致の確認**

11

IPA
Information-technology Promotion Agency, Japan

本質的な難しさ（複雑性）も説明してしまうか？

1. **複合技術ゆえの複雑性**
   - **公開鍵暗号技術の応用であることは確かであるが，単純な応用ではない．**

     これについては，説明しよう！
   - **各要素技術ごとに（セキュリティに関する）論点が存在する．**

     これについて説明する必要があるか？（／説明できるか？）

2. **想定される利用目的が単一ではないゆえ**…
   - **例** 1：Webアプリケーション (HTTP over SSL/TLS)
     - **本人認証かつ経路守秘**
   - **例** 2：**デジタル署名・検証（ローカル）**
     - **真正性の検証（改ざん防止）**
   - **例** 3：**電子メール** (S/MIME)
     - **暗号化**
     - **デジタル署名**
     - **暗号化かつデジタル署名**

これらについては，該当の目的以外も説明しよう！

CPと関連づけて説明できるはず…

12

Information-technology Promotion Agency, Japan

本質的な難しさ（複雑性）も説明してしまうか？（つづき）

3. **人間のみが対象となるとは限らないゆえ…**
   - **人間**
   - Web**サーバー**
   - **デバイス**
     - **例**：IPsec **ルーター**（pki4ipcec）
   - **デジタル文書**

   これについては，説明しよう！

参考：複雑性と闘う局面

- **相互運用可能性を確保するためには，複雑な場合分けごとの検証，複数の組み合わせによる検証が必要となる！**
- **複数ドメイン**PKI **においては，さらに複雑な場合分け…**

  テストケースとソフトウェアから成るテスト・スィートを開発する意義

Information-technology Promotion Agency, Japan

技術者の良心にかけて

- **無理がある比喩表現を避ける**
- **専門用語を正しく使うように務める**

  例：
  - **「公開鍵」と「プライベート鍵」**

    「秘密鍵？」，「私有鍵？」
  - ‘Certification’ **と** ‘Authentication’

    「認証」をめぐる日本語の混乱
  - CP **と** CPS

    標準文書が混同していたが整理された

    （RFC 2537 → RFC 3647）

Information-technology Promotion Agency, Japan

専門用語を正しく使うように務める

- CP と CPS

  RFC 3647 Certificate Policy and Certification Practices Framework

  - **認証実施規定**：CPS (Certification Practice Statement)
    - 「CA および他の関係者が，(一定のドメインにおいて) CP において言明されている要件に適合させるために，どのように手順やコントロールを実装するか？」について，単独の CA が言明するもの
    - 「どのように関係者が各々の役割を果たし，コントロールを実施するか？」を開示するもの

    説明する必要があるときに説明する

  - **証明書ポリシー**：CP (Certificate Policy)
    - 「関係者が何をしなければならないか？」が証明書に示される．

    証明書には，用途がある！

    (暗号アルゴリズムを使い分けることができる)

15

Information-technology Promotion Agency, Japan

信頼関係の基盤

ネットワーク社会に生きるすべての人々に

- 「信頼関係の基礎として，『(主張されているとおりの) 本人であること』を知ることができるようにしたい」という関心事を理解してもらえるように務めましょう．

  他の目的も，これに基づいているといえます．

技術者自身は

- 複合技術である今日の PKI について，(焦らず) 段階的に理解を深めましょう．

  必ず理解できるようになります．

16