「我が国における PKI の不幸」

ネットワーク社会における信頼関係の基盤の上で…

2007年 6月25日 月曜日

独立行政法人 情報処理推進機構
セキュリティセンター
宮川 寧夫

2年前の講演の復習

- 「経営幹部に PKI を理解してもらうためには…」

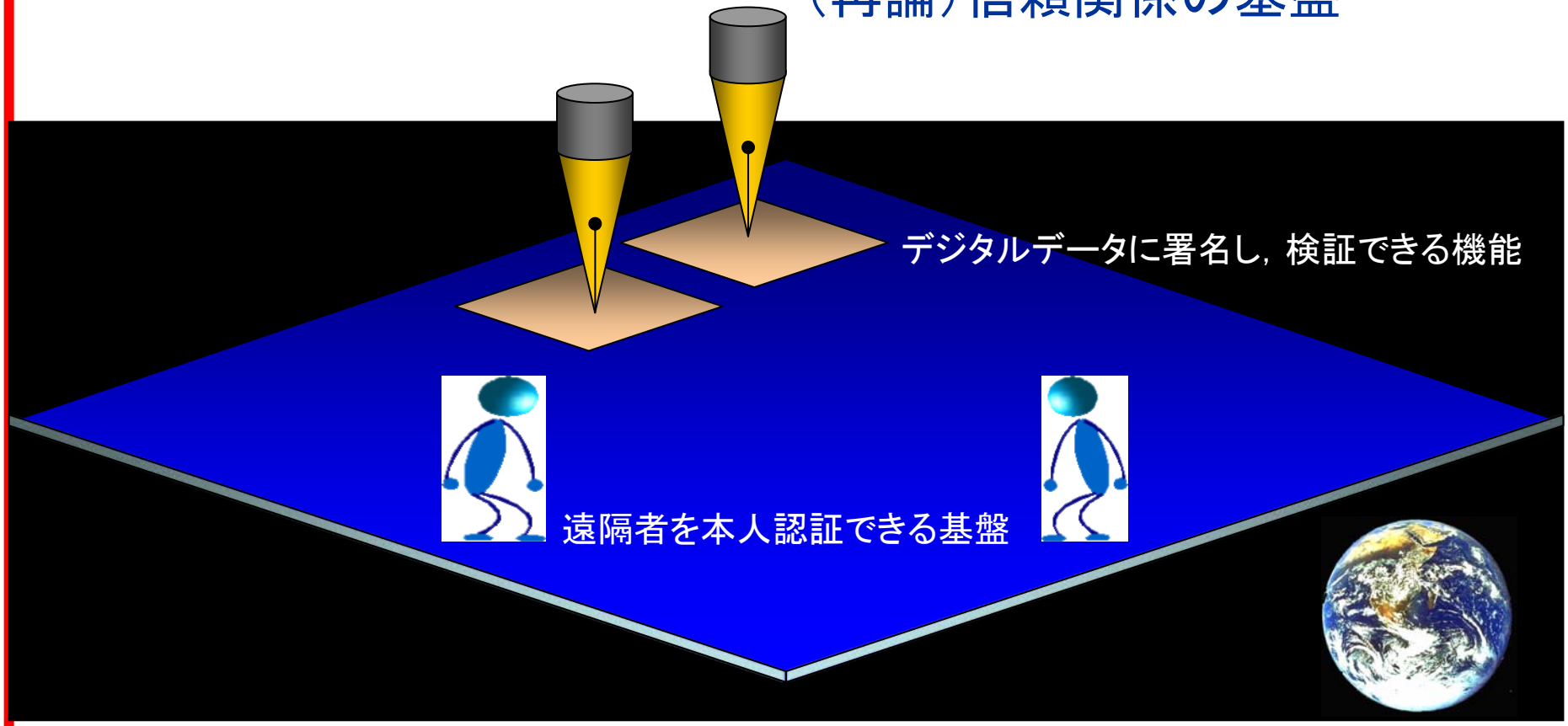
  公開鍵暗号技術を応用する
  ネットワーク社会における信頼関係の基盤
  - » http://www.jnsa.org/seminar/2005/seminar_20051028/0miyakawa.pdf

  – 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
     - 公開鍵暗号技術から説明すると…短時間に理解することは，不可能
     - 信頼関係モデルの話として説明する

       » *今回もCP（証明書ポリシー）の話をします.*

PKI の社会的性格：（再論）信頼関係の基盤



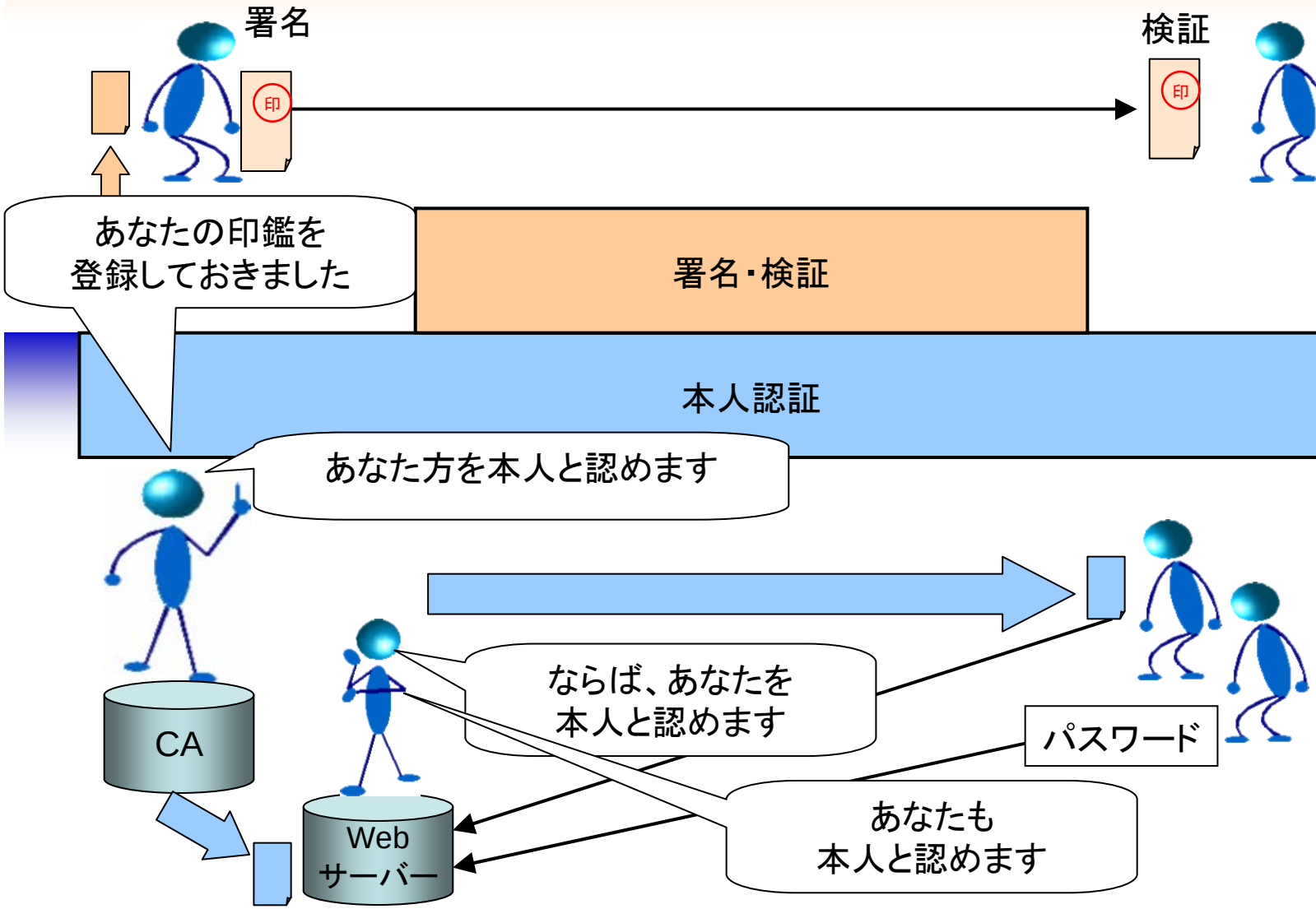
「信頼関係の基礎として，『（主張されているとおりの）本人であること』を知ることができるようにしたい」

- 遠隔者を本人認証できること（＋人以外も）

「他の目的も，これに基づいているといえます．」というのは…

- デジタル署名・検証のこと

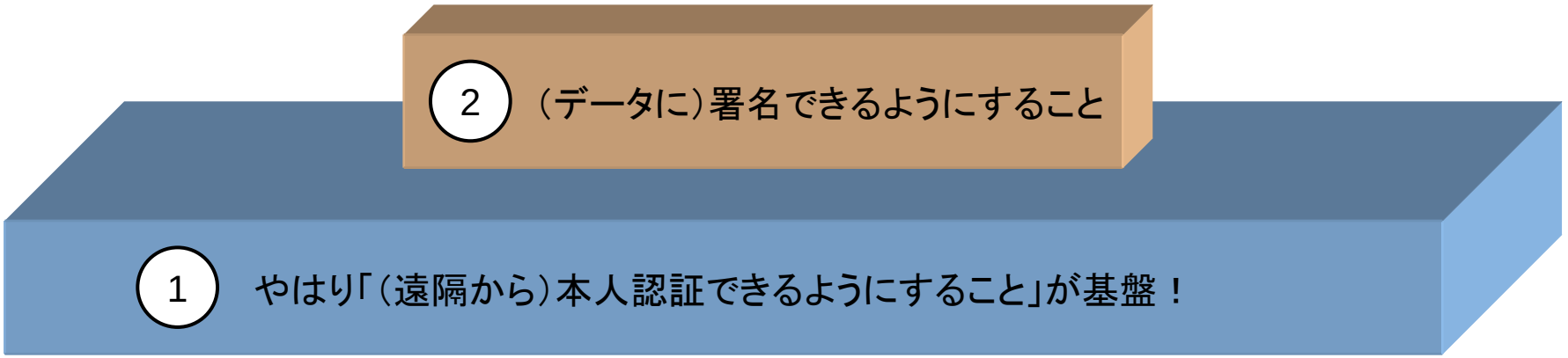
PKIの社会的性格：目的



PKIの社会的性格：目的（つづき）

- 社会的な視点からは，縦の議論となる：

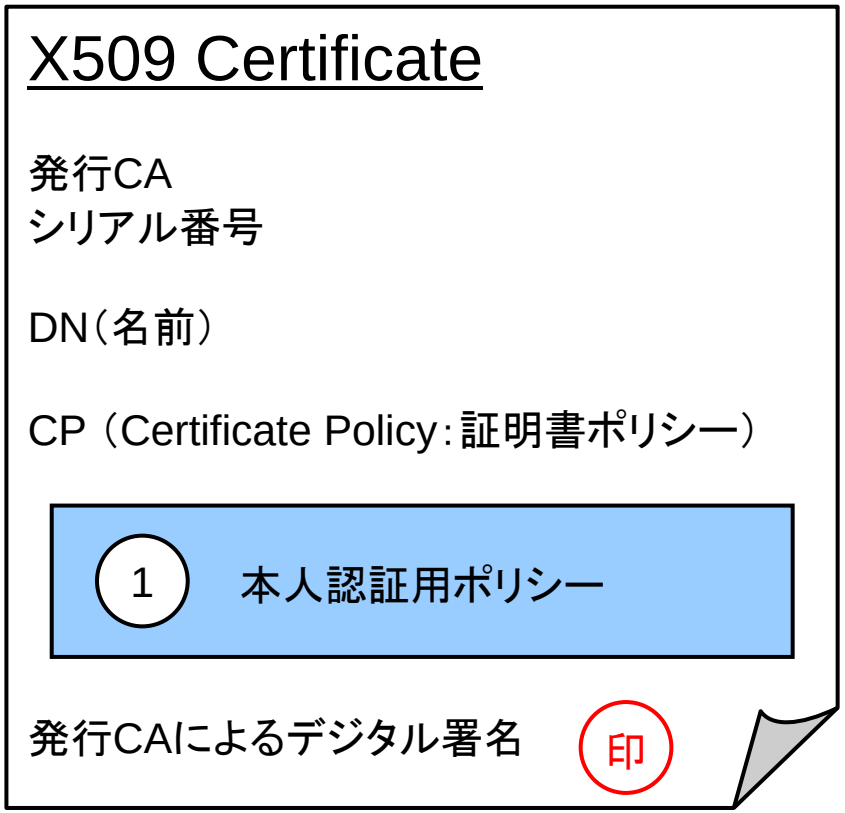
プライオリティ：①→②

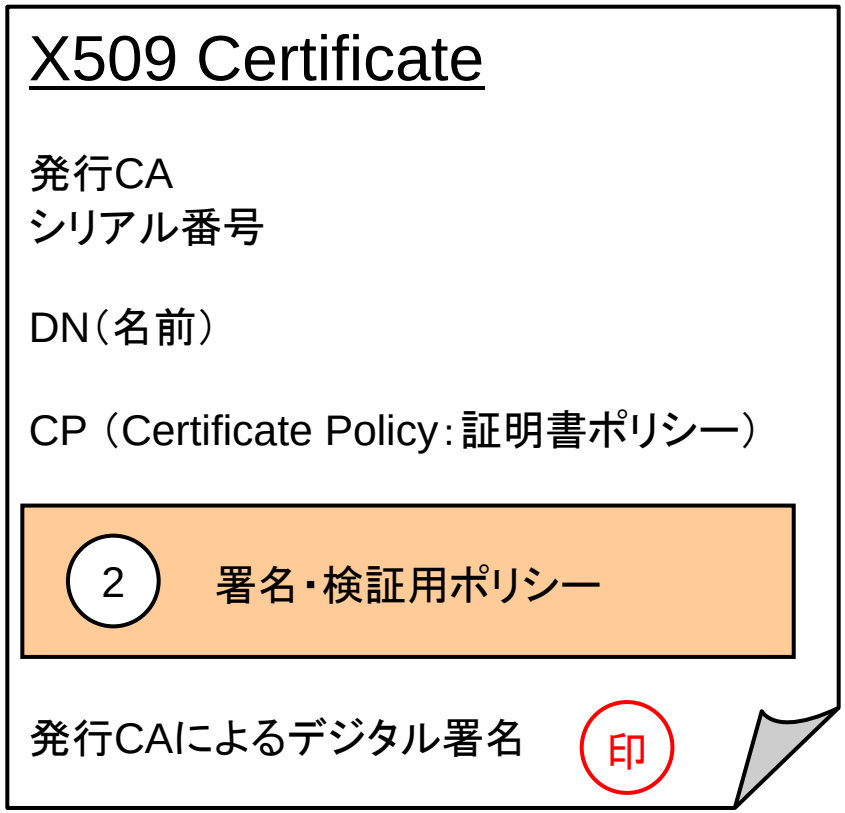


1. 「広く（遍く）人々が，遠隔から『本人であること』を証明できるようにすること」が先決事項．
2. （データに）署名する人は特別な人？！
   「データに署名する意義は？」→「電子署名法」
   技術的にはリンクしないが…，やはり，「本人であること」を踏まえたいところ…

PKI証明書の技術的可能性

- 技術的な視点からは，並存の議論となる：





CP（証明書ポリシー）

RFC 3647には2種類の分類の元に例が掲げられているが…

- カナダの例は難しいもの
- 一方のアプリケーション・クラスに注目
  - 本人認証用
  - デジタル署名・検証用
    - さらに，レベルを設定することがある

CPのデータ・フォーマットはシンプル

- オブジェクトID！（登録する：データ処理（パス検証時）：人間が読んでも…）
- URL（リンク先：人間が読める）

「以上！」と言いたいところ…拡張もある

拡張がCP をサポートするために使われる

- 証明書ポリシー拡張（クリティカル・フラグ）
- ポリシーマッピング拡張およびポリシー制約拡張（マルチ・ドメイン用）

PKI証明書の技術的可能性（つづき）

	① 本人認証用証明書	② 署名・検証用証明書
Certification パス	本人認証用の証明書同士が階層的に連鎖	署名・検証用の証明書同士が連鎖するように組織間関係を表現
採用するデジタル署名アルゴリズム	オンラインに利用できる程度の応答性（→安全性の観点から許容できる範囲で軽いもの）	オフラインで検証できればよい 安全性が高い方が良い

混ざらないようにする

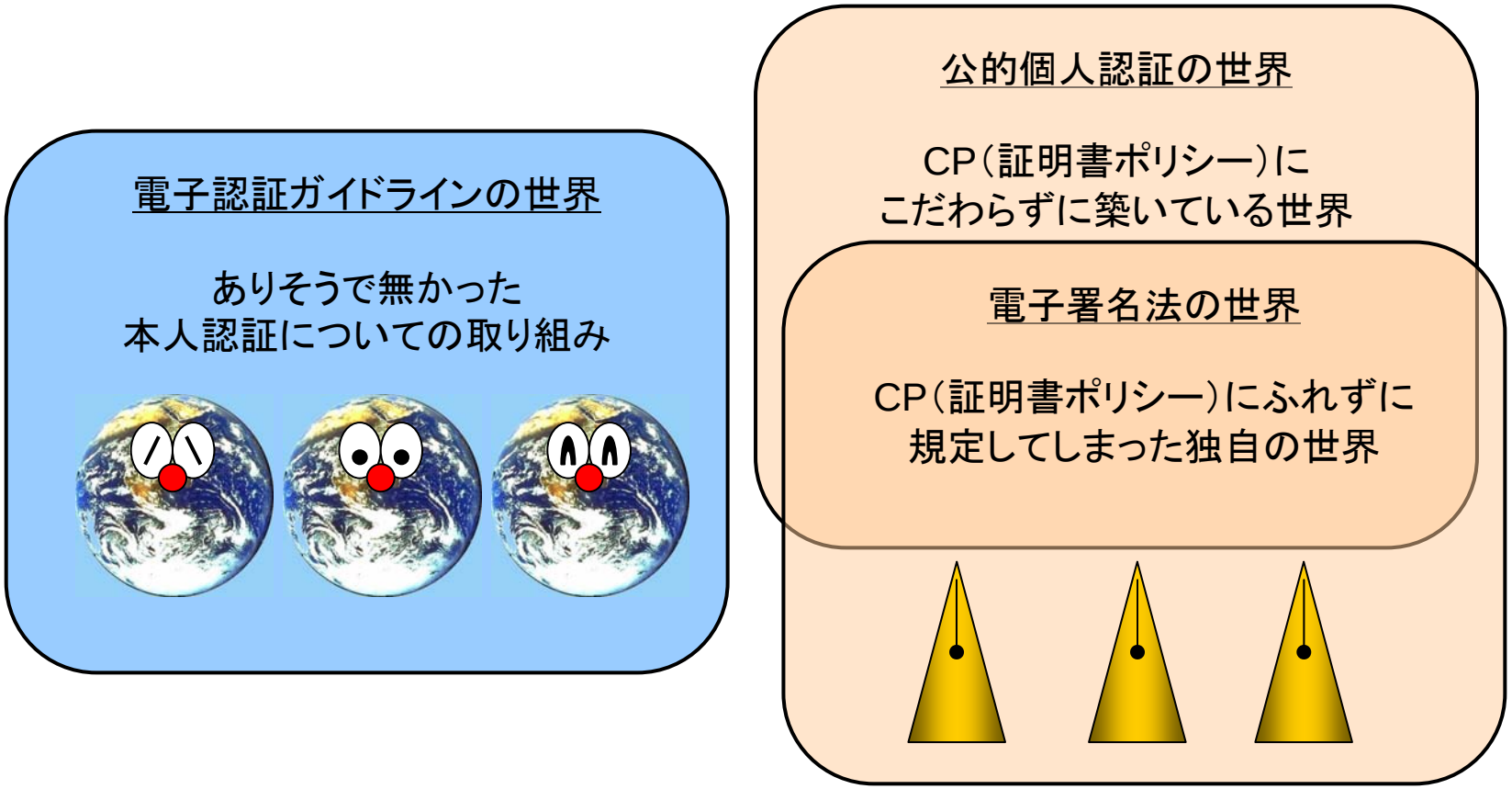
それぞれ別の論理的PKIを構築する構図

我が国におけるPKI

- 不幸な歴史
  - 電子署名法 & GPKI（2000年）
    - GPKI（電子政府認証基盤）はデジタル署名・検証用
  - 公的個人認証基盤（2002年）
    - これもデジタル署名・検証用
      - *ICカードが配布されたが…*
  - 電子政府認証ガイドライン（2006年）
    - ようやく本人認証用についての議論

②署名・検証用が先
①本人認証用が後！

我が国におけるPKI（つづき）



- CA（認証局）は，両方の証明書を発行する能力を備える．
- CP（証明書ポリシー）を意識できるようにしておくことは，社会的にも重要！
  - 人々は，CPを意識していないかもしれない…

懸念事項

シナリオ1:

デジタル署名・検証用の証明書が本人認証用の証明書に転用されるようになると…

意味不明…

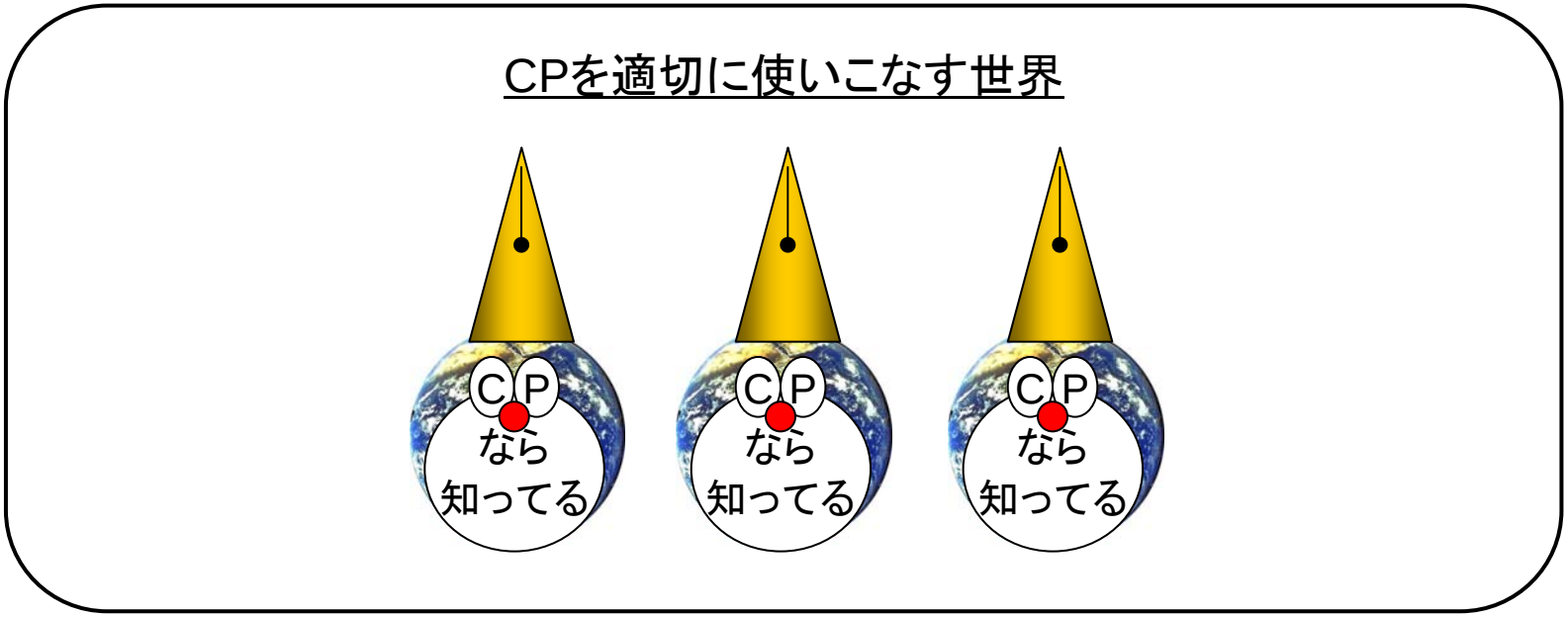
シナリオ2:

本人認証用の証明書のみがこれから発行されるようになると…

署名・検証用のものより強いハッシュアルゴリズムが選ばれてしまう可能性がある矛盾

我が国のPKIが進むべき道

- こんな感じ？：未着手分野を埋めるためのみならず…



「誰でも本人であることを遠隔から主張できると共に，
データについて署名が必要な場合には
そのデータに署名できるし検証もできる環境」
を低コストで実現する．

CP（証明書ポリシー）が設定されうる領域

サブジェクト	本人・本物認証用	電子署名・検証用
個人（自然人）	○	○ 法的効果 QCを規定？
ハンコ（法人・役職）	×	○ 法的効果
Webサーバー	○	×
タイムスタンプ・サーバー	△	○
ネットワーク機器	○	

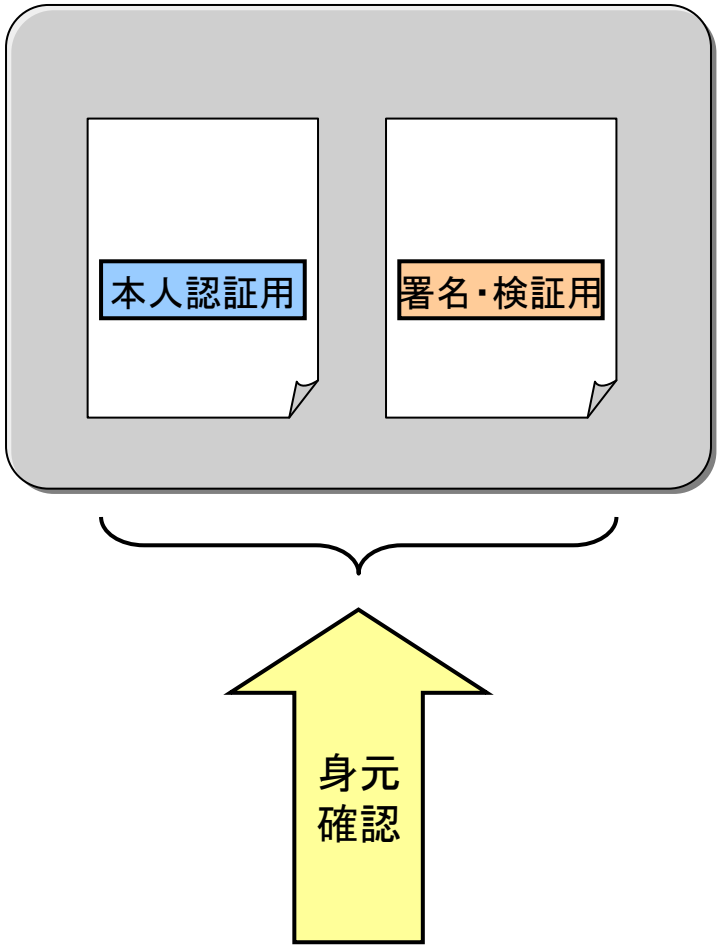
PA（Policy Authority）

- 米国の例
  - FPKIのPA
    - http://www.cio.gov/fpkipa/

  - CP論点を調整する機関の必要性
    - マルチドメインPKIの相互運用と関連
    - 各PKIドメイン代表と有識者から成る会議体？
    - 暗号アルゴリズム等の選択や移行への対応

IC-IDカードと身元確認

- 個人（自然人）がもつICカード内には、両目的の証明書を入れられるようにすべき
  - どちらかと言えば…
    署名・検証用の方がオプション
  - 単純に複数の証明書が入りさえすればよいのか？
    参考：OpenSC

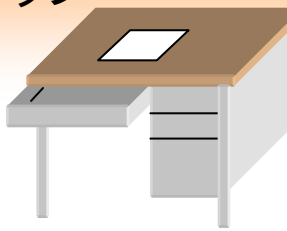


- 身元確認（identification）
  - 手続きは共通
  - 同時発行も可能なはず
    - 社会的コストの低減についても考慮する
    - CPSは各CPに対応するが…
      - *本人認証用のCPSが署名・検証用のCPSよりも難しいわけではない.*

タイムスタンプが
狂ってしまうが…

タイムマシンにお願い

技術的／社会的に素直なロードマップ



クォリファイド証明書の導入

電子署名法制
e文書法制

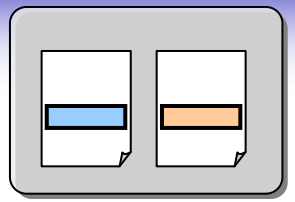
タイムスタンプ局のデジタル署名用証明書を発行

タイムスタンプサービス
開始

個人のデジタル署名・検証用証明書の普及
（オプション）

本人認証用証明書の普及

複数証明書を格納する
IC-IDカードの普及



Webサーバー認証用
証明書の普及

マルチドメインPKIの展開

横断認証用証明書の活用

我が国のPKIが 振り返るべき道： ビジョン

Authentication 街道と、相互運用可能な景色

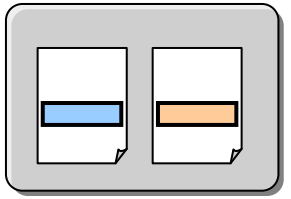
基礎固め

社会的なコストを検討

本人認証用証明書の普及

Webサーバー認証用
証明書の再普及

複数証明書を格納する
IC-IDカードの普及
相互運用可能性確保



マルチドメインPKIの
相互運用可能性確保

本人認証用についての各論

- Webサーバー認証用証明書の再普及
  - Webサービス全盛時代における基礎固め
    - Phishing対策の文脈から説く重要性
      - *本物のWebサーバーであるという主張*
- 本人認証用証明書の適度な普及
  - Webサービス全盛時代におけるWebサービスとの親和性
    - ログインすることによって提供されるサービス
      - *署名・検証用の証明書よりも使える局面が多いはず*
  - 社会的なコストを検討
    - 保証レベル（Level of Assurance）の考え方を導入
      - *パスワードでもよいサービスも多いはず*
- IC-IDカード仕様についての再レビュー

デジタル署名・検証用についての各論

- 詳しくは，また別の機会に…

- ちょっとだけ
  - S/MIME署名メールの普及
    - Phishing対策の文脈から説く重要性
      - *検証可能な人からのメールであるという主張*

「電子メールのセキュリティ」

» *http://www.ipa.go.jp/security/fy18/reports/contents/email/email.pdf*

以上

おまけ

コテコテ・デラックスな論点にも対応

電子署名法への
クォリファイド証明書の導入

作成基準の電子契約に対応する
ためのタイムスタンプ・システムは？

法人によるデジタル署名
の効果は？

応答性を確保するために複数の
タイムスタンプ・サーバーを立てると…？

PAの
設置

証明書の
移行手順

ハッシュ・アルゴリズム
の交換可能性確保

DNにUTF8Stringを使うのは…
やはり止めた方がよいのでは？

OCSP仕様の
要修正箇所は？

IC-IDカードの
あるべき仕様は？

SCVPの実装は？

PKI for IPsec
は難しい！

保証レベルに対応した
本人認証ガイドライン策定

携帯電話への
証明書の格納

サーバーサイドで
パス構築するには？

TLS 1.2がもたらす
相互運用可能性問題

ポリシーマッピングし易くするために
CPを抽象化する必要があるのでは？

マルチドメインPKI横断
のためのガイドライン