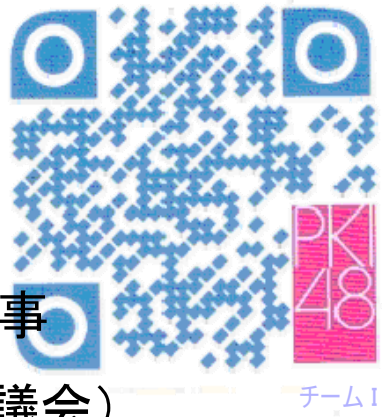
開発者のための
PKI/電子署名の利用法

2016年5月23日

政本　廣志
JNSA 電子署名WG
NTTアドバンステクノロジ

略歴紹介

政本 廣志 （現：NTTアドバンステクノロジ）



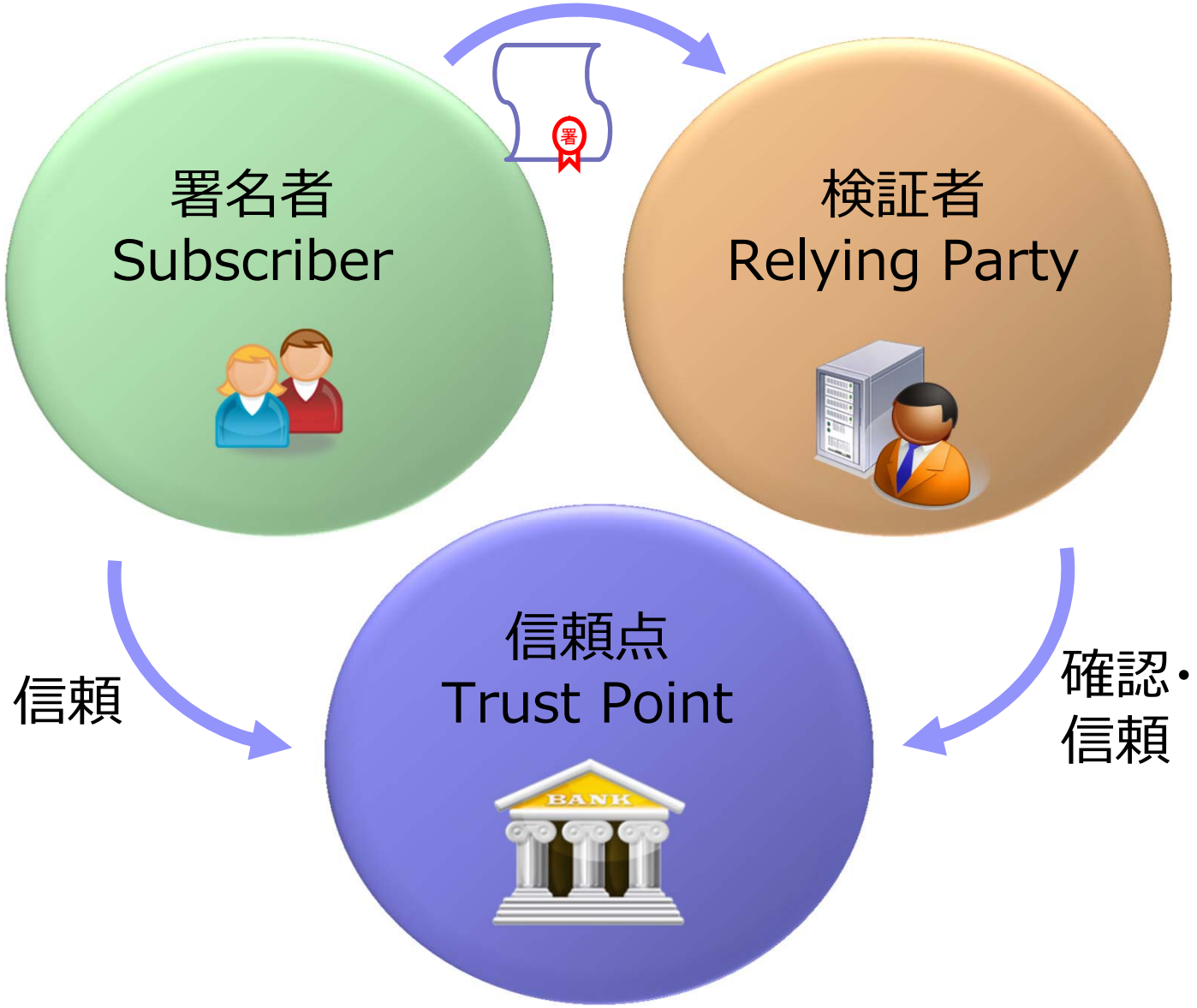
- 1990年代後半～
  - 電子認証・電子公証関連の研究開発に従事
    - 2004年～　ECOM（次世代電子商取引推進協議会）
      - 電子文書の長期保存
      - 電子署名普及に向けた調査検討
      - 長期署名フォーマット相互運用性実験
      - （2006　CAdES/XAdESプロファイルJIS化作業）
    - 2010.3　ECOM解散（eRAPに移行）
- 2010.4～　現所属
  - 2013年～　JNSA　電子署名WG参加
    - 長期署名プロファイル標準化等
    - （2014～　PAdES規格原案作業WG、
      - TBF電子証明基盤検討WG）

背景

PKI/電子署名は普及しているか

- 2000年頃から、PKI/電子署名の必要性、重要性が言われて久しい
  - 欧州では1999年に電子署名指令制定
  - e-Japan構想(2000)、電子署名法(2001)、e-文書法(2005)、等
- 「普及は周回遅れ」と言われたこともあった
  - しかし最近、医療、建築関係など、活用の兆し
  - マイナンバーカードの普及にも期待
- 本格的な普及につながるか(正念場?)
  - そのためには、何が必要か、、、

PKIのトライアングル（仕組み）



普及のトライアングル

良いサービスなら使う

利用者

サービス提供者

インフラが整っていればサービス創出

インフラ

利用者が多ければインフラを整備

普及を阻む要因

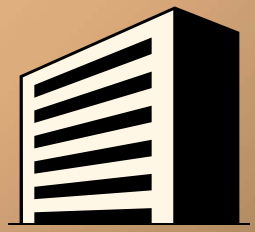
開発・導入のコストが大きい

技術・開発

難しい！

経営視点

儲かるの？
やらなきゃいけないの？



制度・法律

難しくて理解されにくい

法的根拠・強制力がない

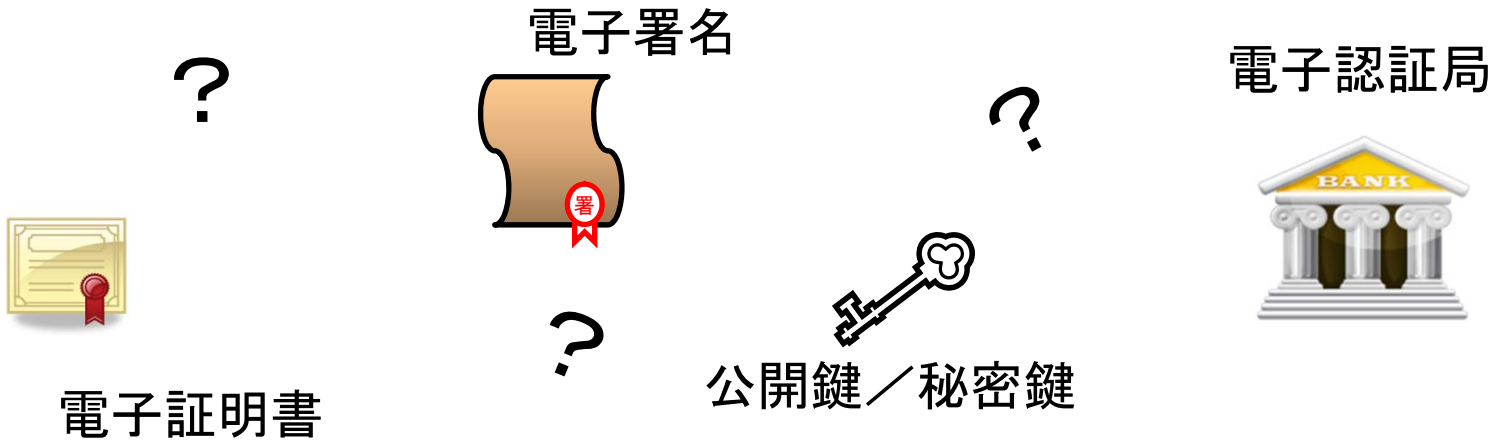
必要なの？

サービス開発者・システム設計者にとって

以下、厳密な解説ではありませんので、ご容赦を。

PKIとか電子署名って、、、

- 何に使えるの？　　・・・適用領域
- どう使ったらいいの？　・・・設計上の留意点



Ⅰ　適用領域

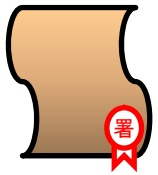
おさらい

- 電子化/ネット社会の“4つの脅威”

脅威	対策技術
盗聴	暗号化
なりすまし	相手認証
改竄	電子署名
否認	電子署名と証明書

PKI/電子署名の効用

- 効用1

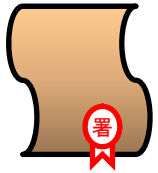


電子署名

改竄防止できる ×

改竄があれば検知できる
（つまり抑止になる）

- 効用2



＋

電子証明書

証明書で身許確認できる △

(証明書は公開情報)
検証すれば(署名者を)確認できる

よく使われる喩え

※分かり易いが、違いにも注意。

紙の発想に縛られないように注意

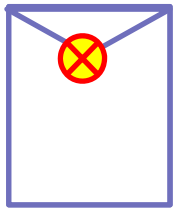
現実の世界

- 署名

手書きサイン

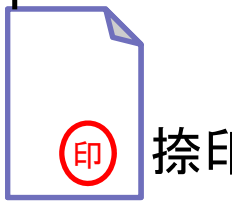
・誰のものかは暗黙知

- 封緘

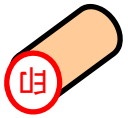


封蝋(Seal)

- 実印



捺印



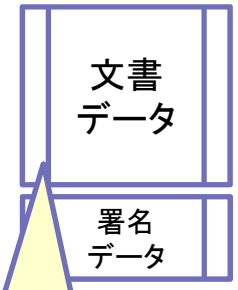
実印

役所

印鑑登録証
(印影)

・日本特有の制度

電子の世界

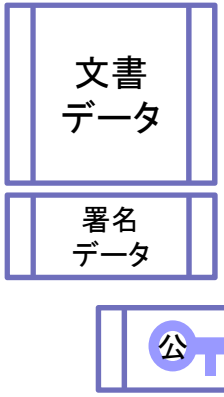


電子署名

・切り離せる
・コピーできる

・中身は見える

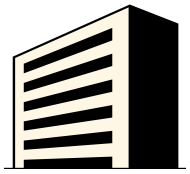
・誰のものかは証明書で確認



電子署名

公開鍵証明書

秘密鍵



認証局

もう少し自由に考えてみよう

- 改竄検知＋身許確認

  - ”それ”は本物(非改竄) だ
    - ⇒　実在性、証拠に使える
    - ・完全性（Integrity）
    - ・存在証明（PoE）
  - “その人”が生成した(承認した)
    - ⇒　否認防止、文責、意思表明に使える
    - ・説明責任（Accountability）
    - ・透明性（transparency）

『何か』(デジタルデータ)を証明したい

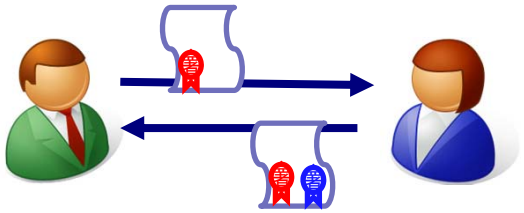
例

- 文書　⇒　文書署名
  - 電子署名法、e-文書法、等に基づくもの
- プログラム　⇒　コード署名
  - ウィルス／マルウェア対策
- メール　⇒　S/MIME
  - 暗号メール(親展)にも
- カルテ　⇒　電子カルテ
- 認定書、合格証　⇒　資格証明
- 免許、パスポート　⇒　許可証
- 成績書、卒業証書　⇒　学歴証明
- 発明、特許　⇒　権利保護(先発明主義)

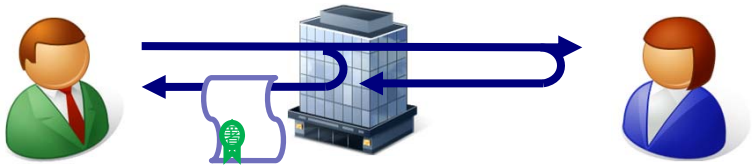
“やりとり”の中で『何か』を証明したい

例

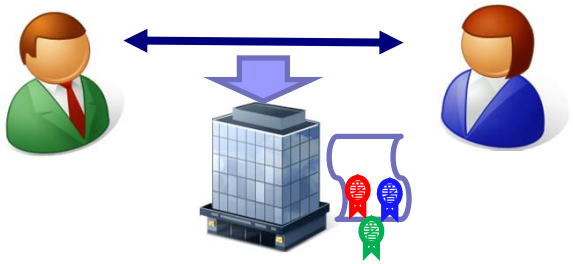
- 電子契約
  - 両者で署名、合意



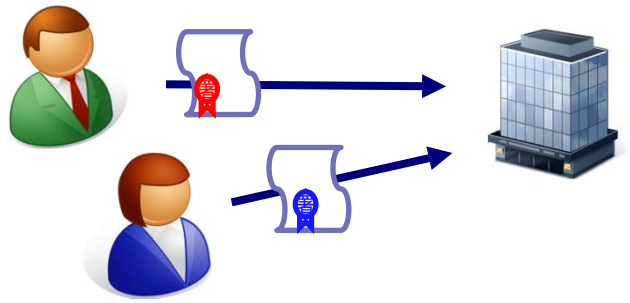
- 送達確認
  - 仲介者が保証



- 電子公証、内容証明
  - 第三者が証明



- 電子入札
  - 互いに事後否認防止



『誰』を証明するか

例

- 公的資格者　⇒　士業証明書、医師等資格証明書
- 国、自治体の職位者　⇒　GPKI、LGPKI
- 個人（住民）　⇒　JPKI（公的個人認証）
  - 属性は証明されていないことに注意
- 企業内従業員　⇒　社員証
- 学生　⇒　学生証
- その他、政治家、有名人（スポーツ選手、アイドル等）など

社会的責任のある人、ニセモノが懸念される人　⇒　政見、公約、メール・ブログ、サイン等

証明する（証明書を持つ）モチベーション

- ✓ 改竄や否認されて困る人が、『相手』に持たせる
- ✓ 改竄や否認していないことを主張したい『本人』が持つ

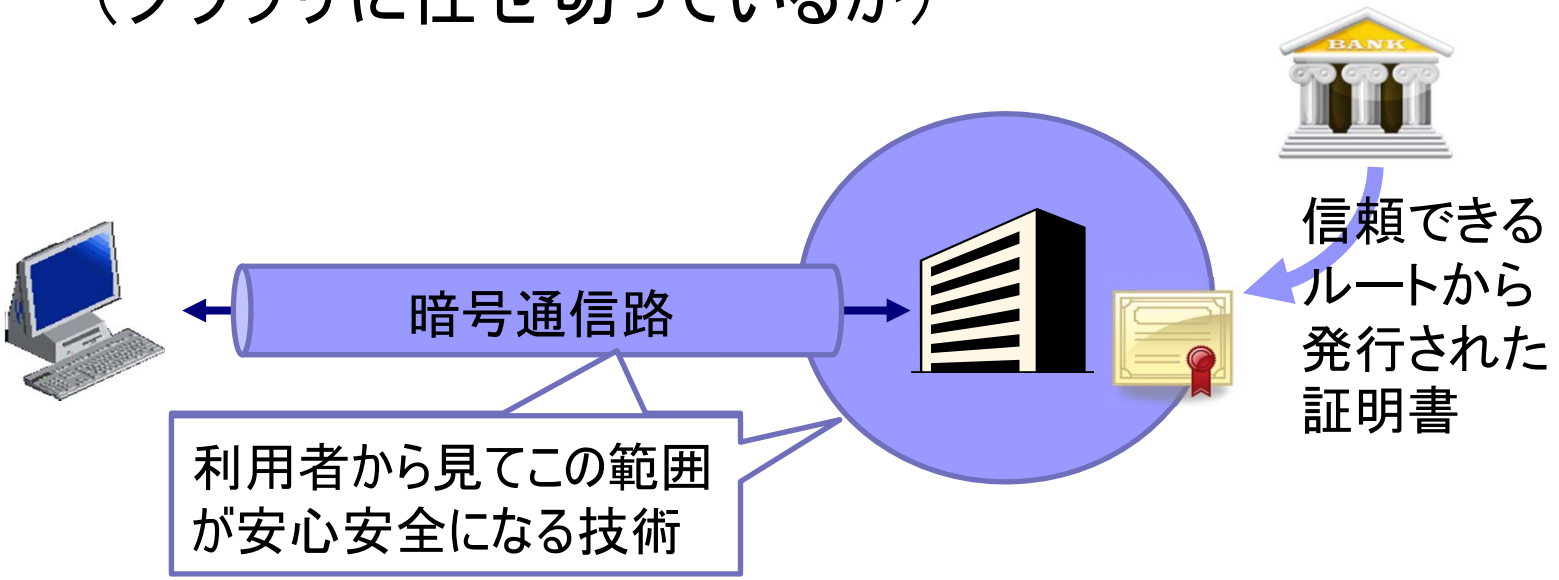
⇒　発想を広げて、いろんなことに使おう！

証明する内容は、5W1H

- 誰が（誰に）
- 何を（モノ、行為、意思）
- いつ　　・・・　タイムスタンプ技術
- どこで　・・・　これは意外と難しい

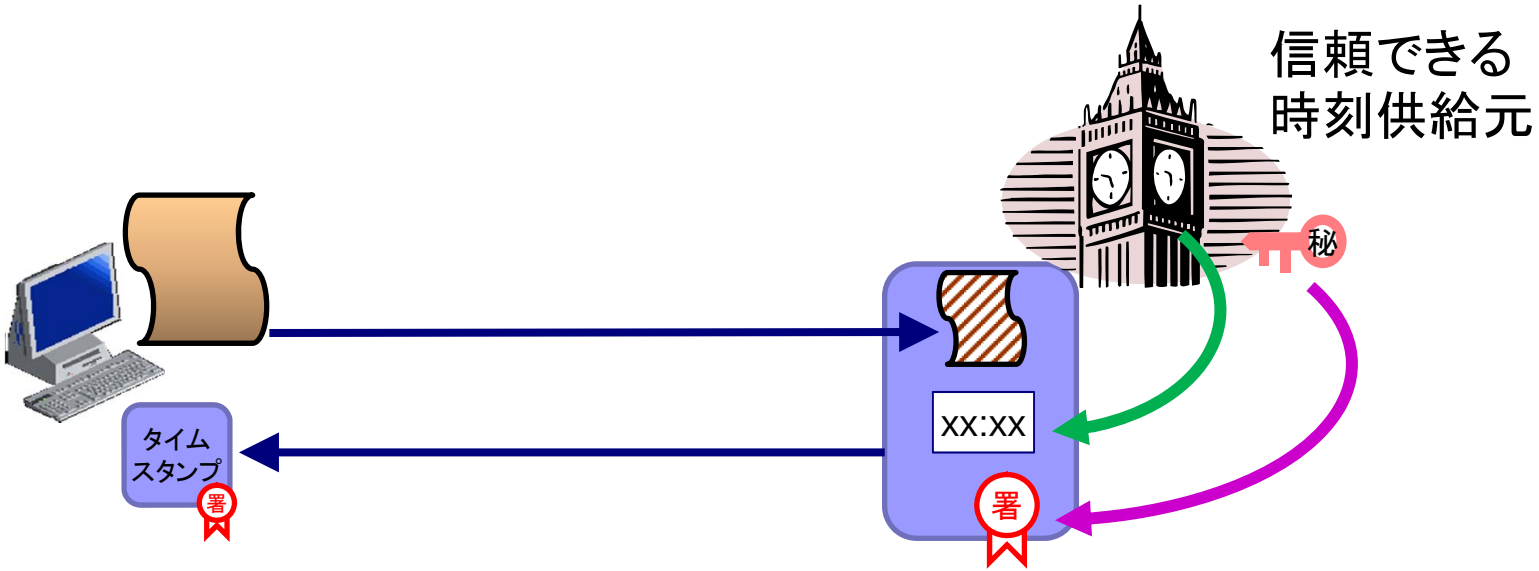
（よくできた例１）

- SSL/TLSサーバ認証の仕組み
  - 通信を暗号化して安全にする
    （SSL＝暗号化と思っている人も多いが）
  - サーバの証明書で正当性などを確認できる
    （ブラウザに任せ切っているが）



（よくできた例２）

- タイムスタンプ(時刻認証) RFC-3161方式の場合
  - 普遍情報である時刻情報と併せて、署名する
    （正しい時刻を扱える機関に限る）



Ⅱ　設計上の留意点

設計には、いろいろ留意点がある。。

1つ1つは重い内容になるので、ここでは紹介に留めます。

[技術面]

① 有効期限と失効

- 鍵/暗号の賞味期限、危殆化

  ⇒ 鍵更新、アルゴリズム移行、長期署名

② 鍵管理（利用者が安全に保持していることが大前提）

- 耐タンパ性、鍵配布・鍵運用

  ⇒ HSM、サーバ(リモート)署名

③ 検証（有効性と非改竄性）と相互運用性

- 検証手段はいろいろ。他と情報流通するなら相互運用性

  ⇒ プロファイルの標準化など

（つづき）

1つ1つは重い内容になるので、ここでは紹介に留めます。

[運用面]

① 認証パスとトラストアンカー

- 最後は何を信頼するか

  ⇒ 欧州ではTSL（Trust Service status List)運用開始

② 登録とID基盤

- 証明対象を確実に登録・管理する基盤が必要

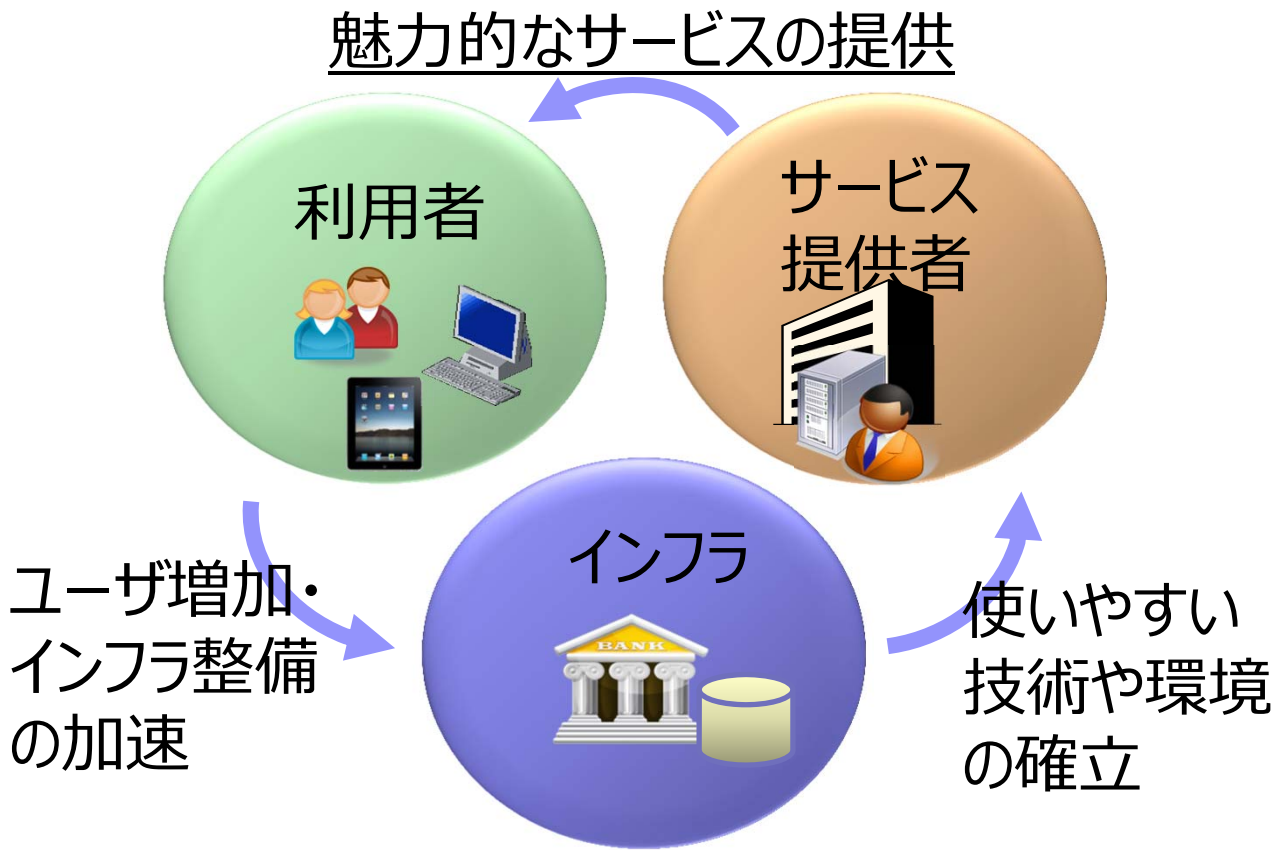
  ⇒ 対象に応じて適切に

③ 法・制度の整備、認定などによる保証と準拠

- 裁判等での法的根拠、信頼できる第三者機関の運営

  ⇒ 欧州のeIDASの動きなど注目

⇒　留意事項に注意して、いろんなことに使おう！



ご清聴ありがとうございました。

参考

署名利用のガイドラインや解説

PKIや電子署名の解説例の（ほんの）一部

- 『PKIハンドブック』H12.11　S.R.C.発行　小松他著
- 『電子署名利用者システムの構築・利用ガイドライン』 H13.3　ECOM
- 『社会システムとしての電子認証と電子署名』

  JNSA Press Special Column（松本）　2005　第15号
- 『電子政府ガイドライン作成検討会 セキュリティ分科会報告書』 H22.2
  - *www.kantei.go.jp/jp/singi/it2/guide/security_guide_line/siryou2.pdf*
- 『オンライン手続における リスク評価及び電子署名・認証ガイドライン』　2010.8
  - *www.kantei.go.jp/jp/singi/it2/guide/guide_line/guideline100831.pdf*
- 『もっと使える電子署名・認証』 2012　JIPDEC
- 『電子署名活用ガイド』第2版　2013　電子認証局会議

ECOMにおける署名普及の調査と経緯

- 「電子署名普及に向けた調査検討報告書」（H17年度）
  - 電子署名の利用が必ずしも進んでいない状況に鑑みて，電子署名の普及における問題点，普及へ向けた課題をまとめた。
- 「電子署名普及に向けた調査報告書（2）−海外及び国内金融分野での利用動向」（H18年度）
  - 普及の要件を調べるため，電子署名の利用状況を中心に海外におけるPKIの利用状況を広く調査した。
- 「電子署名の普及に関する活動報告」（H19年度）
  - 電子署名利用環境の再構築に向けて，欧州の先進事例を調査し，わが国の今後の展望を探った。
- 「電子署名普及に関する活動報告2008 」（H20年度）
  - 電子署名利用に関して，欧州のeIDとの関係や標準化状況を調査した。
- 「電子署名普及に関する活動報告2009 」（H21年度）
  - 社会基盤としての電子署名や証明書の利用について，官民連携や国民IDをテーマに検討した。