

PKI Day 2015

# サイバーセキュリティの要となるPKIを見直す

2015年 4月 10日

松本 泰 セコム（株）IS研究所



# PKI Day 2015

## サイバーセキュリティの要となるPKIを見直す

- 今日、サイバー空間におけるセキュリティの確保や信頼関係の構築に、PKIは欠かせない技術になっています。
- また、サイバー空間の広がりとともに、IoT/M2M等の新しいPKIの応用領域も期待されています。
- その一方、社会基盤としてのPKIは、制度的な課題や、更には実装や展開等において様々な課題も浮上しています。
- PKI day 2015 では、以上のことを踏まえ、「サイバーセキュリティの要となるPKIを見直す」をテーマに、今後の社会におけるPKIの在り方を議論します

# 10回目のPKI day

回	年	PKI day テーマ
1	2005	PKI技術最新事情
2	2006	PKIの展開と最新技術動向
3	2007	PKIの過去・現在・未来
4	2008	PKIの標準から実装まで 最新動向
5	2009	さまざまな分野に展開されるPKIの最新動向
6	2010	社会基盤としてのPKI/PKIの10年
7	2011	番号制度時代のPKI
8	2012	<ul style="list-style-type: none"><li>・我が国における信頼基盤の連携に向けて</li><li>・PKIへの攻撃とその対応</li></ul>
9	2014	<ul style="list-style-type: none"><li>・公開鍵暗号に関連する周辺技術動向の共有</li><li>・デジタル社会のための「電子署名を見直す」</li></ul>
<u>10</u>	<u>2015</u>	<u>サイバーセキュリティの要となるPKIを見直す</u>

# PKI Day 2015

## サイバーセキュリティの要となるPKIを見直す

- 基調講演 東京工科大学 手塚 悟 先生
  - サイバーセキュリティの状況とPKIの取組み
- 第1部
  - 新しい時代の電子署名
- 第2部
  - SSL/TLS実装の今とこれから
- 第3部
  - 広がるサイバー空間に対応するPKIの新しい応用領域

# サイバーセキュリティの要となるPKIを見直す 背景について

- サイバー空間の広がり、本格的なデジタル社会の到来
  - CPS (Cyber Physical System)、制御システム等のオープン化
  - 紙台帳前提の社会制度からデジタルデータ前提の社会制度へ
- サイバーセキュリティの重要性
  - 情報システムのための情報セキュリティだけでなく、より広範囲な制御システム、CPS等も含めたサイバーセキュリティ
- サイバーセキュリティの要であるトラストサービスの重要性
  - サイバー空間上のトラスト（信頼関係）の確立なくして、サイバー空間におけるセキュリティ確保はあり得ない。
- PKIの重要性
  - サイバー空間においてトラストを構築するための暗号技術の重要性
  - 多様なステークホルダー間のトラストを構築する公開暗号技術の重要性
  - 標準化された公開暗号技術であるPKIの重要性
- 多くの課題
  - 現状のトラストサービス(SSL/TLS関連等)の様々なほころび
  - トラストを構成する要素の整合（ビジネス・制度・技術等の整合）
  - 今後の社会における大量、多様なエンティティ間のトラスト

# 1部 新しい時代の電子署名

- 欧州のeIDAS
  - 欧州においては、1999年のEU電子署名指令 (Directive) から、より広範囲なトラストサービスを扱い、より強制力のあるeIDAS規則 (Regulation) へ
  - 欧州においては、個人情報保護法においても、EUデータ保護指令 から、より強制力のあるEUデータ保護規則 へ
  - EU域内におけるパーソナルデータの利活用と保護のためのEUデータ保護規則。同時に、パーソナルデータの利活用と保護・情報連携等を支えるトラストサービスのためのeIDAS規則
- 欧州におけるサイバーセキュリティ・トラストサービスの標準化と展開
  - eIDASのような規則（ないし規制）とETSI等での技術標準化がセットで検討されてきた
  - 強制力のある規則により、制度、技術、ビジネスの統合が難しいトラストサービスの展開を行っているように見える。
  - ex. 欧州における自動車のサイバーセキュリティ等も同様に見える？
- 欧州の規制モデル型 vs. 米国の市場モデル型
  - では、日本の立ち位置は？

## 第2部 SSL/TLS実装の今とこれから

- 近年のインターネット上の重要なトラストを提供しているSSL/TLSの様々な問題
  - 2008年 MD5不正CA証明書
  - 2011年 DigiNotar不正証明書発行事件、BEAST
  - 2012年 CRIME
  - 2014年 HeartBleed、POOLDE、CCS Injection
  - 2015年 FREAK
  - Etc……
- 背景
  - SSL/TLSの社会基盤化 → 攻撃対象へ
  - 暗号技術・暗号技術の組み込んだ実装の難しさ
  - トラストを構成する様々なステークホルダー
    - 競争の中でのトラスト、エコシステムによるトラストの難しさ
- では。。

# 3部 広がるサイバー空間に対応する PKIの新しい応用領域

- より社会基盤化するインターネットにおけるトラストの向上
  - インターネットは、暗号技術普及以前に広く普及したが、普及し社会基盤化する程に、より高いトラストが要求されるようになってきた
  - RPKI、DNSSEC
- 制御システム等のオープンネットワーク化
  - 従来の制御システム等は、物理的なセキュリティにより守られたクロードネットによりトラストを実現してきた
  - 閉じた世界の制御システム等に、多様な「繋がり」を求められている  
→ 広く「繋がる」ためには、物理的なセキュリティだけでは実現できない (ex. 車の場合、ITS、自動運転等の要求で外部と接続)
  - 「繋がり」「オープンネットワーク化」では、PKI等の暗号技術によるトラストの構築が必要
- IoT時代の数百億のデバイス
  - 現在のSSL/TLSによるWebサイト認証やコード署名等以上に、大量で多様なエンティティ、そして多くのステークホルダー、そうした中での多様なトラストの構築



# PKI day 2015のオーバビュー

3部 広がるサイバー空間に対応するPKIの新しい応用領域

時代の要請

マイナンバー  
制度の時代

ビッグデータ  
時代

IoT時代

行政サービス

医療サービス

金融サービス

Webサービス

電子契約書

医療記録

プログラム  
(コード署名)

電子領収書

オープン化する制御システム

医療機器

ITS

車の車載器

IPルーティング

信頼が必要な  
情報連携サービス

信頼が必要な  
デジタルコンテンツ

数百億個のデバイスの  
多様な信頼関係

トラスト  
レイヤー

eIDAS

電子署名

タイムスタンプ

電子シール

電子配布

Webサイト認証

Web trust for CA

Webサイト認証

DNSSEC

RPKI

(広義の) トラストサービス

トラストを  
構成する  
要素

デジタル社会  
のための  
法制度

法制度と  
整合性のある  
標準化

信頼のおける  
運用

セキュアな  
実装技術

暗号技術等の  
コア技術

1部 新しい時代の電子署名

2部 SSL/TLS実装の今とこれから

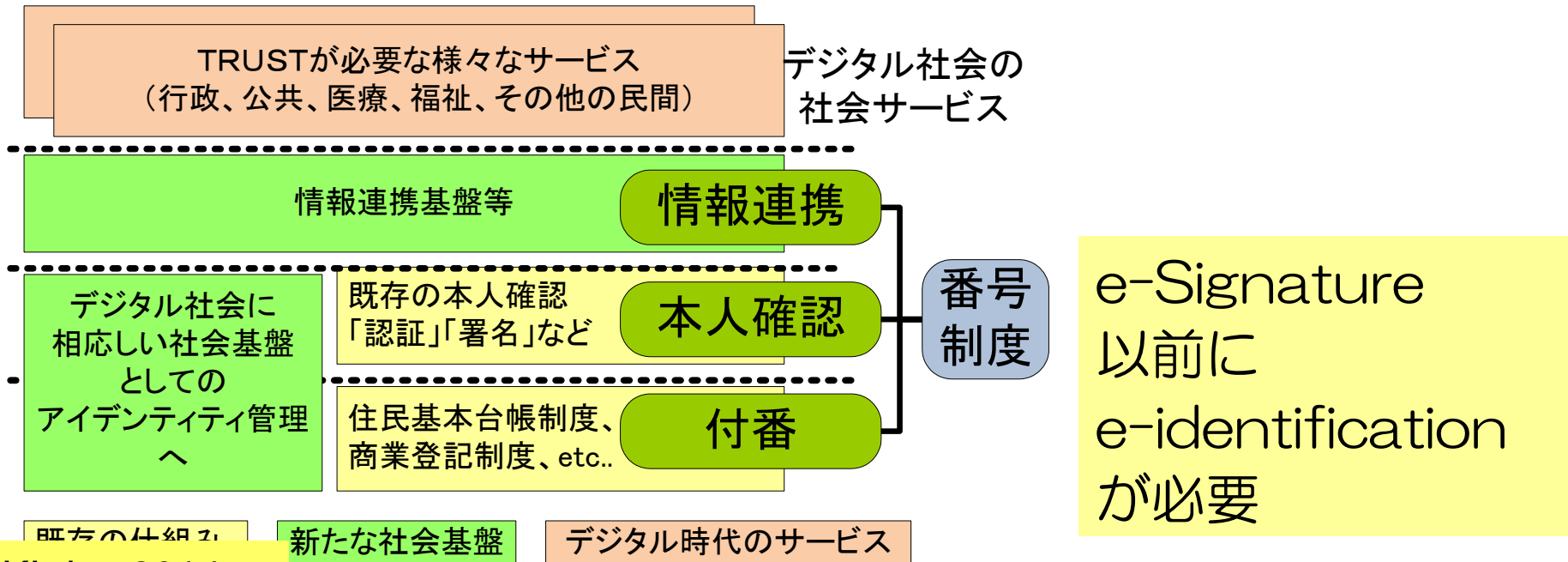
# 広義のトラストサービスへの期待と課題

- ニーズからのビュー（期待）
  - マイナンバー時代、ビッグデータ時代、IoT時代において、様々なトラスト（信頼関係）を必要としているサービスがある
- シーズからのビュー（課題）
  - 技術、制度、ビジネスの整合
    - トラストを構成する多くの要素の整合

# 過去のPKI dayの関連スライド

# 2013年に成立した番号法

- 番号制度を構成する3つの仕組み
  - 「付番」「本人確認」「情報連携」
  - 申請主義の行政サービスからプッシュ型の行政サービスへ
    - 紙台帳の仕組みを引きずった制度からの脱却
      - 紙台帳の電子化の発想からの脱却
    - そのための識別の見直しを行った制度？



デジタル時代の  
日本の社会？



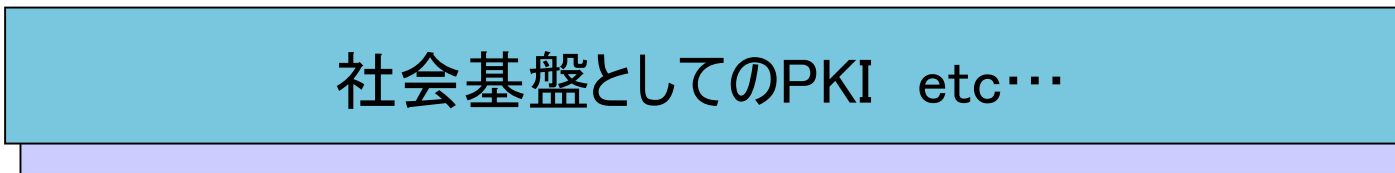
効率的で、透明性があり  
競争力のある社会？



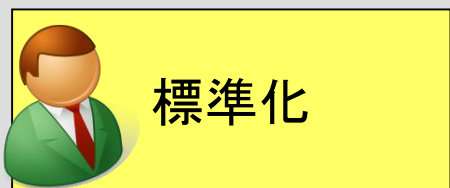
デジタル時代の  
社会サービス



デジタル時代の  
社会基盤



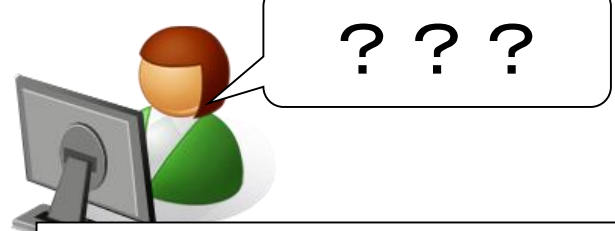
デジタル時代の  
(信頼のための)  
フレームワーク



デジタル時代の  
要素技術



# 標準化と法制度の関係



"Rough consensus and running code"

法制度等から  
ニュートラルな  
技術標準

IETF等の  
標準化

デファクト標準  
としての実装

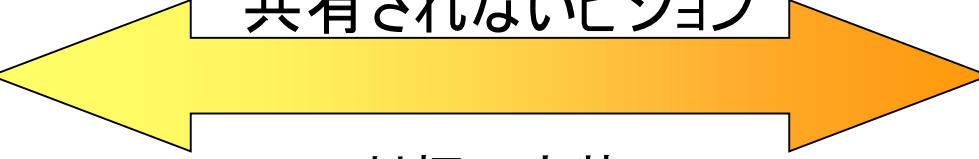
民事訴訟法は228条4項「私文書は、本人又はその代理人の署名又は押印があるときは、真正に成立。。」

ギャップ

噛み合わない会話  
共有されないビジョン

- ・既存のレガシーな法制度
- ・様々な管轄官庁の様々な業法

紙前提の制度  
(の電子化)



対極の実装

強い影響

「電子署名法」、「e文書法」、「電子公証人制度」、「商業登記に基づく電子認証制度」、「住民基本台帳制度」、「タイムビジネス信頼・安心認定制度」、etc...

現実の実務からの乖離という問題

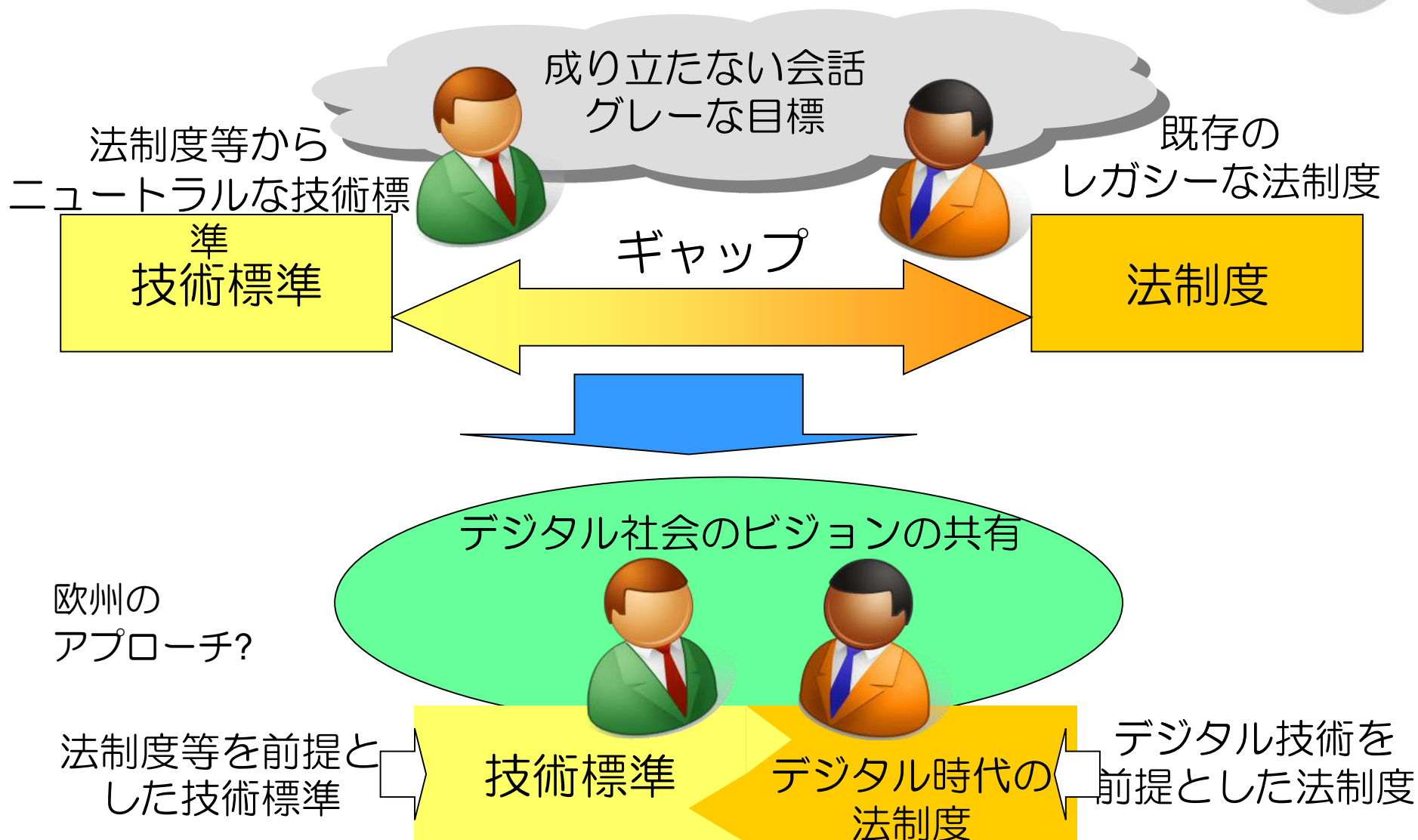
既存の慣習、権益が強すぎる問題

PKI day 2010 「光の道」で医療問題も決まる？

番外編

現在の医療の問題点は、デジタル化以前の問題

# 技術と制度をかみ合わせるためには



# SSL証明書の暗号アルゴリズムの移行問題 ステークホルダーの声??

モバイル  
キャリア



メモリの関係から、よく使われるルート証明書だけを格納したい。

認証局



「全ての端末をサポート」して欲しいというお客様がいる限り古いルート証明書を使うしかない。

ブラウザベンダ



基準を満たしている限り、証明書リストに入れていくけど、暗号のことはどうしましょーね。後、古いOSは、勘弁してね？

信頼できる証明書なんて分らないからブラウザを信頼するしかない

とにかくPCも携帯も全ての端末をサポートして欲しい



サーバ運営者



利用者



SSL