セコムIS研究所
Intelligent Systems Laboratory

ちょっとさきのことをみんなで考える

2023年11月22日
セコム（株）IS研究所　顧問
松本　泰

みんなで考える

松本の自己紹介　　セコム（株） IS研究所 顧問

セコム IS研究所 Intelligent Systems Laboratory

- 1978年　計測器メーカにてハードウェアの設計などに従事.　->　学生時代からマイコンの洗礼
  - #マイコンを使った各種計測器などの設計。半導体工場の仕事も多かった（LSIテスターなど）
- 1984年　UNIX上のビデオテックス・パソコン通信システムなどのソフトウェア開発などに従事
  - #生活構造研究所入社　　UNIXがやりたく転職
    - 当時の生活構造研究所はUNIXのソースコードライセンスを持ちVAX11/750 4.1bsdが稼働
    - 当時の生活構造研究所は昨年12月に亡くなられた高橋徹さんが、在籍されていた。
- 1994年　各種インターネットサービスの設計、開発、運用に従事
  - 1994年東京インターネット設立（設立時は、高橋徹さんが社長）
  - 商用サービスであることから、
    ネットワークセキュリティに興味を持つようになった。
- 1999年　サイバーセキュリティ事業の立ち上げに従事
  - #2001年からNPO JNSA PKI相互運用技術WGリーダ・「Challenge PKIプロジェク」
- 2007年　経済産業省 商務情報政策局長表彰「情報セキュリティ促進部門」受賞
- 2011年-2012年
  - 社会保障・税に関わる番号制度　情報連携基盤技術WG　構成員
  - 社会保障・税に関わる番号制度　社会保障分野サブWG　構成員
- 2013年-2014年　内閣官房　パーソナルデータに関する検討委員会・技術検討WG　構成員
- 2008年-2018年　JDCC 日本データセンター協会　セキュリティWGリーダ
- 2023年2月　情報セキュリティ大学院大学・情報セキュリティ文化賞受賞

この後、インターネットにどっぷりの４年間だった。

広いドメインで利用されるデジタルアイデンティティの活動へ

マイナンバー制度の議論

改正個人情報保護法に至る議論

「Challenge PKIプロジェクト」は、NPO JNSA が、2001年に開始したプロジェクト

Challenge PKI Project
The Multidomain PKI Interoperability Framework

Japanese
English

Contents

- ニュース
- はじめに
- プロジェクト
- 発表資料
- 連絡先
- パートナ

ニュース

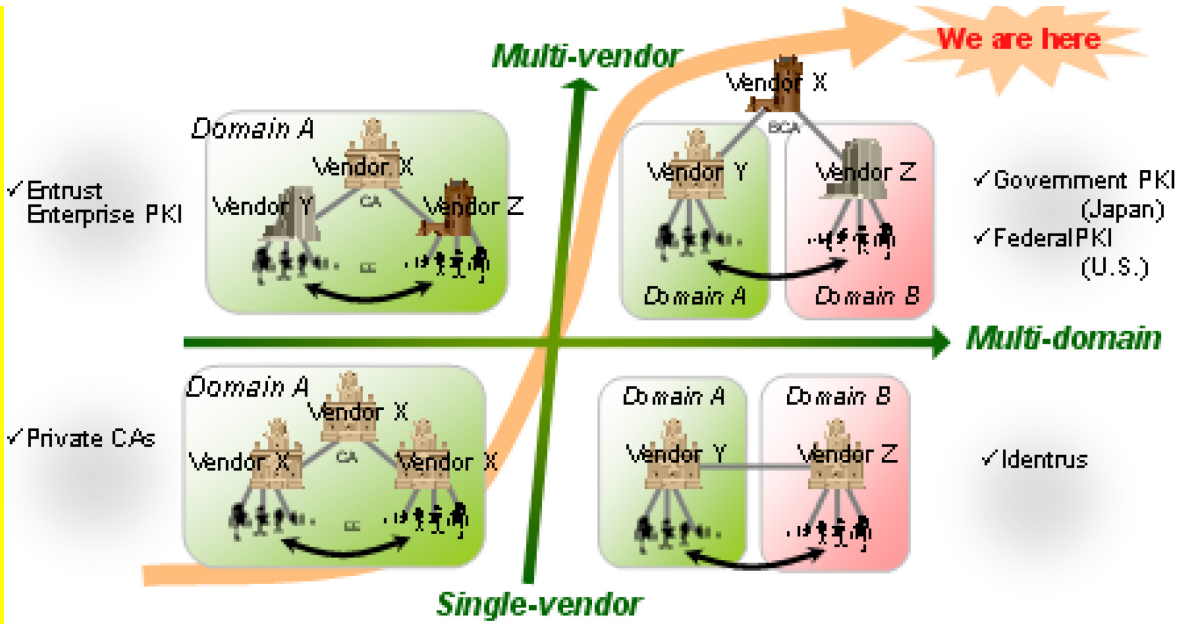
- インターネット・ドラフト 「マルチドメインPKIの相互運用性に関するメモ」がRFC 5217として公開されました。 (2008/07) NEW!
- Challenge PKI Test Suite 2.0で利用可能な、タイムスタンプ・プロトコル(TSP)用のテストケースが 公開されました。(2004/7)
- Challenge PKI Test Suite 2.0で利用可能な、GPKI、地方公共団体認証基盤(LGPKI)、公的個人認証(JPKI)に対応したテストケースが公開されまし

はじめに

各国の電子政府プロジェクトや電子商取引が活発化するなかで、PKI(Public Key Infrastructure)は 安全で安心できる電子社会を実現するための、重要な要素技術となっています。 初期のPKIは、ごく少数のベンダによって提供され、また単一の管理主体（ドメイン）の下で使われていました。 しかし昨今では、PKIを提供・利用する沢山のプレイヤーが存在し、複数のドメインが相互に接続されています。 政府認証基盤（GPKI）や、米国のFederalPKIが代表例です。 我々は、この複雑なPKIのモデルを、「マルチドメイン・マルチベンダPKI」と呼んでいます。

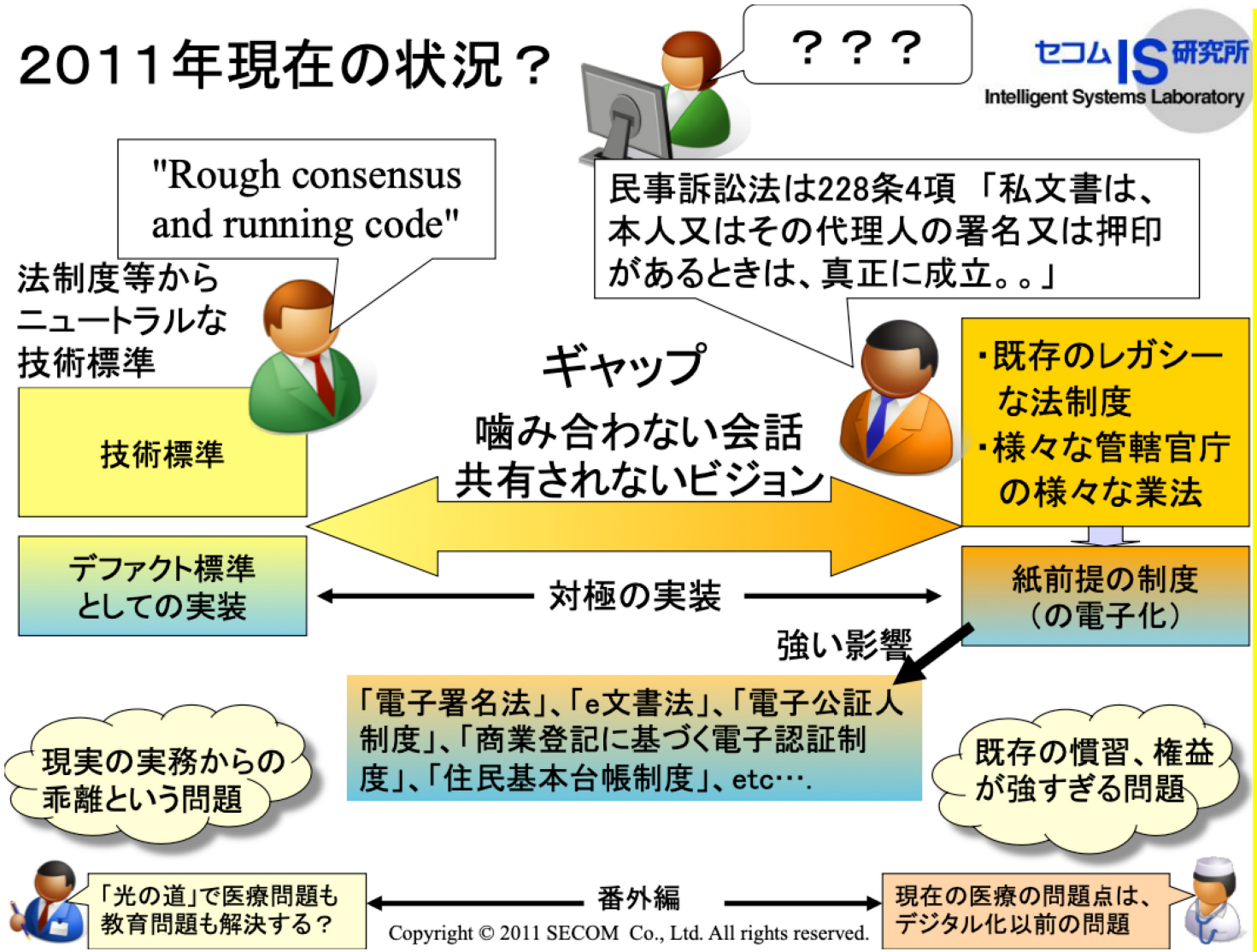
- マルチドメイン・マルチベンダーPKIのための標準化活動や、テス トスイートなどの開発を行なってきた。
- 「Challenge PKIプロジェクト」から20年以上経った2023年現在、
  - マルチドメイン（クロスドメイン、マルチステークホルダー）のトラストの確立、及び、相互運用性の確保は、PKI以外も含め、今日の インターネットにおけるデジタルアイデンティティの大きな課題と同様

出典: https://www.jnsa.org/mpki/index_j.html



Transition of PKI models

ちょっとさきのことをみんなで考える（は、とっても大変！）



- ちょっとさきのこと考える
  - AsIs,ToBeを理解した上でのCanBe
  - 理想(ToBe)と現実(AsIS)の双方の理解
  - 過去から現在そして将来
- みんなで考える
  - マルチステークホルダー
  - 色々な立場の方（異なる価値観、世界観）
  - 有意義な議論にためには、互いのリスペクトが必要

出典：「番号制度とPKI」
https://www.jnsa.org/seminar/pki-day/2011/data/06_matsumoto.pdf

自律（ Autonomous ）・分散（ Distributed ）・協調(Cooperative）の意味することの変化？？
その変化に対応したアーキテクチャ→　デジタルトラスト、デジタルアイデンティティの重要性

- インターネットの成長の原動力（古典的なインターネットにおける）「自律分散システムによる協調」
  - 自律　　Autonomous　　相手（Trustee)を、暗黙のトラスト(implicit trust)した上での自律系システム
  - 分散.　Distributed　　分散コンピューティング（ distributed computing）の延長上
    - →　テクニカルな相互運用性がもっとも重要
  - 協調　　比較的狭いコミュニティにおいて、薄い利害関係と、そのコミュニティ内での暗黙のトラスト(implicit trust)を前提とした自律分散システムによる協調
- 「自律分散システムによる協調」の意味にするところの変化？？　→　ここは議論が必要
  - 自律　　DAO（ Decentralized autonomous organization ）？？→ インターネットコミュニティがこれを目指していたかは微妙？？　自律の意味が、人の介在を最小にしたルールを記述したコードによる自動化へ
  - 分散　　Decentralized??　　異なる価値観、利害関係があるマルチステークホルダーによる分散システム
  - 協調　　厳しいビジネス的な競争、強い利害関係??、パワーバランスの中での協調（の要求）
  - →　自律・分散・協調に必要な、相互運用性の意味するところも変化している？？？　Slide 14,Slide 15
- 今後のインターネットにおける自律・分散・協調に求められるデジタルトラスト＆デジタルアイデンティティ
  - 強い利害関係に中で求められるトランスペアレンシー、アカウンタビリティ、トレーサビリティなど
  - これらを実現するのためのデジタルトラスト＆デジタルアイデンティティの重要性
  - 暗黙のトラストを前提とした自律分散システムから、明示的なトラスト(explicit trust ,Verifiable ）を前提としたの自律分散システムアーキテクチャへ　→　　RPKI ,　DNSsec. なども、その一環

名前（空間）とデジタルアイデンティティの関係
-- インターネットプロトコルにより駆逐されたOSIプロトコルの世界観 --

セコムIS研究所 Intelligent Systems Laboratory

- X.500　ディレクトリーサービス（の世界観） --　1988年のX.500シリーズ勧告
  - インターネット以前の「電話屋さんの電話帳？？の発想」が強い？？
    - #リアルスペースの分厚い紙の電話帳も駆逐された。これはプライバシーの課題の浮上も大きい
    - ある意味、 OSIプロトコルの世界観におけるOne World. One Net. One Vision. を実現するためのディレトリー＆リポジトリー　→　たぶん、2023年現在も「ディレトリー＆リポジトリー」はとっても重要、だけど議論が少ない
  - フロントエンドのインターネットプロトコルLDAP は、ある程度普及した
    - 企業内というトラストドメインにおいては、X.500の延長上にある Microsoft Active Directoryが広く利用されている（プライバシーという課題が少ない）
  - 名前（ X.500 識別名 (DN) ）　C=JP,OU=XXX,C=Alice.　名前と属性と公開鍵を結びつける
    - 名前と、その名前の属性のバイディング、名前と公開鍵＆プライベート鍵（X.509公開鍵証明書）のバインディング
    - PKI (X.509ベースのPKI)は、もともとX.500を前提に考えられていた。
  - -> X.500ベースの公開鍵システムは、普及しなかったが、ある意味「デジタルアイデンティティ」のシステムとしては、ある程度完成されていた？。→ Microsoft Active Directoryが組織内では広く利用されていることからも理解できるかも。
- 実際に普及したWebPKI
  - X.500ディレクトリーサービス, X.500 識別名 (DN) も使われていない（なので既存？のインターネットとの親和性があった）　→ しかし、何らかのディレクトリーサービスがないことがWebPKIの限界にもなっているかもしれない？？

1988年に勧告されたX.500ディレクトリーサービスが目指した世界観
名前と実体（自然人、法人、デバイス・サービスなど）と、名前と属性、名前と公開鍵のバイディングなどは、2023年現在のインターネットにおけるデジタルアイデンティティとっても大きな課題

百花繚乱 or カオス　デジタルトラスト・デジタルアイデンティティの議論

Trustの対象(TP)が
遠隔の何か？クラウド上の何か
複雑化、ブラックボックス化
→ Trustworthinessの議論

Trustworthy　mechanism
trustworthy AI
zero trust architecture

書面や押印などからデジタルへ
Trustworthy　mechanism の
技術と法制度の変革
→ トラストサービスの議論

スマート化のためRPもシステム
ex.. Zero trust トラストエンジン

Untrusted environment or
Zero trust environment

trustworthiness
ability
transparency
accountability

TP
Trustee

chain of trust

Trusted device
Root Of Trust

Untrusted network or
zero trust network

TRUST・
Verifiable, Always Verify

RP
Trustor

Verifiable Credentials
remote attestation(token)
Entity Attestation Token (EAT)

qualified　electronic attestation of attributes　by eIDAS2.0

Web3
Trusted Webの議論

AML（Anti-Money Laundering）の議論
FATF対応

新しい概念の用語が乱立？
全体としては、デジタルトラスト・デジタルアイデンティティの議論

変貌するトラストアーキテクチャ（コンピュータアーキテクチャ）

trustworthiness claim → Verifiable Claims

デジタル社会全体　→　トラスト・ガバナンス・フレームワークの議論？

みんなでみんなで考える　--　基本的な用語とその概念が定まっていない中、議論が錯綜する、また議論が噛み合わない。（上記の）これらは、深い関連性ががあるが、個別に議論されている??。それぞれをリスペクトして議論するのはとっても難しい。

松本の現状の違和感

- フェデレーション、クロスチェーン（、マルチドメインPKI）などに必要なポリシーメイキング　→　分散に必要なポリシーの合意
  - 実際に動くコードや、デファクトスタンダードによる市場獲得を急速に求めるあまりに、（非技術的な要素も多く、非常に面倒な）ポリシーメイキング、ポリシーの合意が議論されない、曖昧なまま突き進んでるように思える。
  - これは、結果的に「分散」ではなく「分断」を生むのでは？？
  - ＃この説明がとっても難しい。 Challenge PKIプロジェクトの経験から感じること
- 暗号鍵管理（技術）への関心が薄い
  - 現代のデジタルトラスト、デジタルアイデンティティを支える（非常に面倒な）暗号鍵管理の重要性が、ほぼ理解されていないように見える？？
    - ＃事業者、サービスプロバイダーとしては致命的だと思うけど現実に見える？
  - エンドユーザは、（知らない間に）スマフォが持つ鍵管理に依存を深めていく？？(Passkeysも同じ)。 Slide 16
  - その結果として、新たな独占、寡占化の方向に向かうのでは？

結局のところ非常に面倒なところは、誰もやりたがらない。
結果、（社会の裏の仕組みで市場を席巻する）プラットフォーマーに頼る？？

Backup Slide

INTERNET Watch　ウォッチャー金丸のNEWS Watch　1997年5月26日版

https://internet.watch.impress.co.jp/www/news/backno1/970526.htm#tokyoi

インターネットにどっぷりの４年間の中で「東京サーバファーム」の立ち上げ

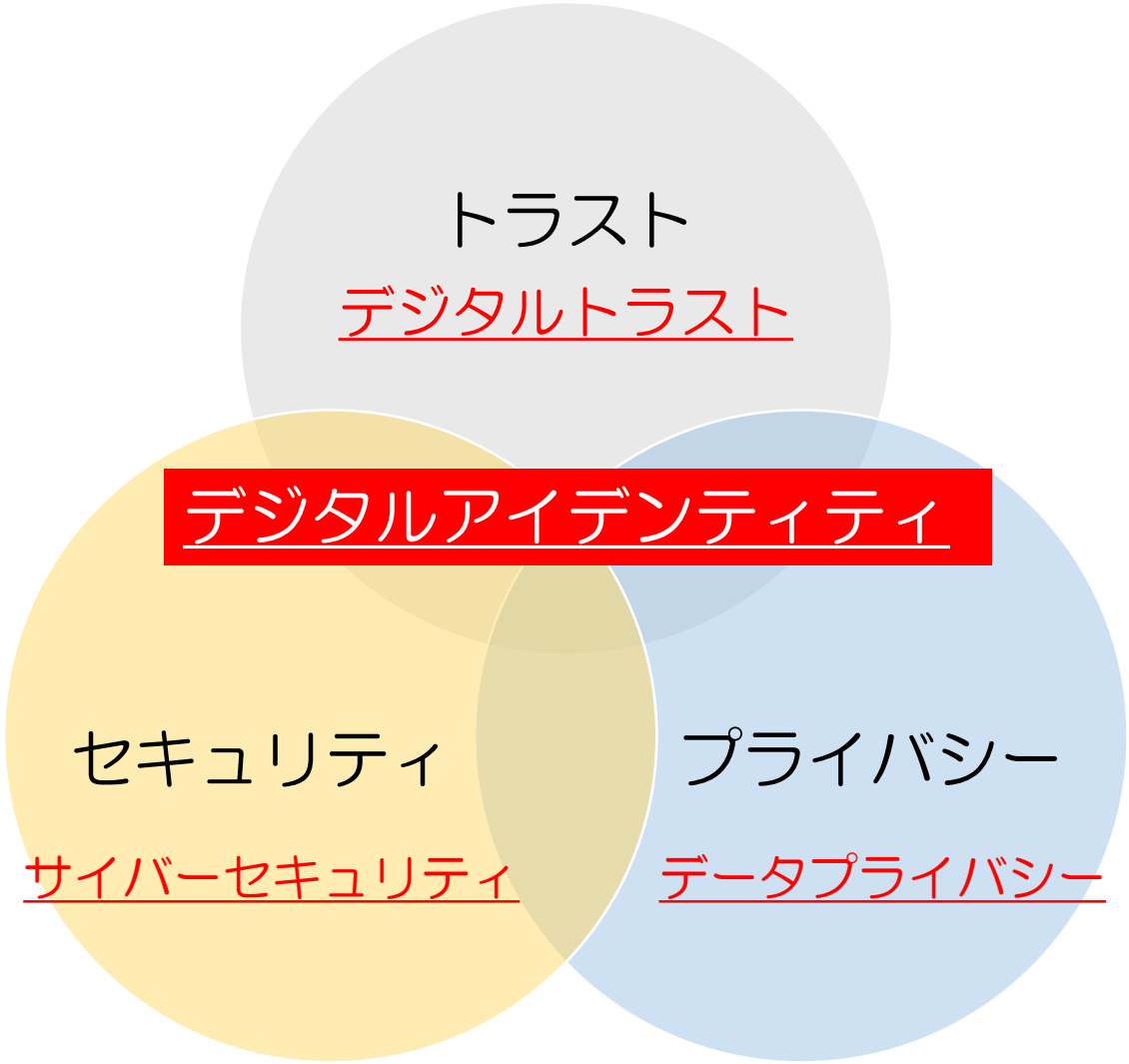
- [プロバイダー][サービス]（レベルA’）
●東京インターネットの新サーバー運用管理サービス「東京サーバーファーム」開始
- 同じく日経産業新聞2面には、東京インターネットが6月中旬から、多機能で大規模なサーバー運用を管理する新サービス「東京サーバーファーム」を開始する記事が掲載された。その第1号として、Yahoo!JAPANからサーバーの管理業務を受託したようだ。
- 同サービスはユーザーが保有するサーバーやアプリケーションなどを24時間・365日体制で人を張り付けて運用監視する他に、各種ウィルス対策などのセキュリティ機能を持たせているということらしいので、高速接続性を保ったサービスを運用したいが、運用/管理者の確保が難しい企業（特にインターネット関連のベンチャーなど）にとっては、セキュリティ管理も含めて使いたくなるサービスではないだろうか。（もちろん、コストとの兼ね合いはあるのだが）
- このところの大手企業などのインターネット・コンテンツ・サービスなどでは、自前でサーバー立ち上げ/運用管理する場合に、ソフト等の開発費はもとより、特に管理者等の人件費（ランニング・コスト）も高度な知識を持つものを雇うだけに大きく、かつ事業拡大と供に人手も必要となることから、続いて行かないケースもまま見られるようになってきた。それだけに、インターネット・エキスパートに丸々管理してもらった方が、収益などを考慮した場合に得であるという方針も出てくるのだろう。
- このサービスは、前記事のIIJ（AIH）の通信インフラを強化することによる、インターネット・プロバイダーとしての事業拡大を押し進める方式とは別に、これまで培った大型サーバー管理などのノウ・ハウを活かしたコンテンツの取込みによるもう一つの事業拡大の仕方と言えるだろう。
- インターネット回線増強にこだわるIIJと、コテンツ・サービスの拡大を模索する東京インターネット。かつて学術ネットの時代から日本のバックボーンを支えてきた両老舗の取組みが、今後の日本のインターネットを含めた通信サービスの枠組みにどのような影響を与えるか、注目される。

◆ JPNIC News & Views vol.666【定期号】2009.8.17 ◆
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2009/vol666.html

セコム IS研究所 Intelligent Systems Laboratory

- 【２】News & Views Column 「後方互換性が生む、インターネット技術の移行の困難さ」 セコム株式会社 IS研究所 松本泰
- インターネットが社会基盤となったと言われるようになって久しいのですが、社会基盤化したインターネットは、IPv6移行問題等をはじめとしてさまざまな移行問題を抱えています。
- こうした社会基盤の移行は、複雑に絡み合ったさまざまな関与者の調整が必要になり、これに技術の複雑化も加わると、移行はこれまでに誰も経験したことのない難しさがあるように思います。
- インターネットのセキュリティも、また多くの移行問題が存在します。多くのインターネットプロトコルは、〝Rough consensus and running code〟といったコンセプトで開発され、これらのプロトコルが、後方互換性を保ち発展してきました。そして、このことがインターネットの爆発的な普及の要因の一つになっていると思います。
- しかし、現在のインターネット上のさまざまな問題、特にセキュリティに関連した問題の多くは、よりセキュアなプロトコルに移行できないことにあります。そして移行できない理由の多くは、既存の環境を動作させるための後方互換性の要求に起因しています。普及したDNSに対するDNSSECへの移行等は典型例かと思います。
- 昨年のInternet Week 2008では、「次世代暗号アルゴリズムへの移行～暗号の2010年問題にどう対応すべきか～」というセッションを担当させていただきました。ここでは、暗号アルゴリズムの脆弱化に伴う、暗号アルゴリズムの移行問題を議論しました。インターネットに関わる暗号と言えば、SSL証明書の暗号アルゴリズムの移行問題があります。
- これは、末端のSSL証明書というよりは、さまざまなブラウザや携帯等の機器に埋め込まれたルート証明書の移行がより重要な問題になります。また、プロトコル的には、古いSSLのプロトコルや脆弱な暗号アルゴリズムを切っていく、すなわち後方互換性を切っていく必要があります。これは、これまでのインターネットの常識とは異なるものです。
- 社会基盤化したインターネット上の移行問題は、IPv6に限らず本質的な問題です。今後、こうした問題の幅広い議論が期待されます。

なぜ今、デジタルトラスト・デジタルアイデンティティが重要なのか？
初期のインターネットでは、あまり考慮されていなかった
セキュリティ・プライバシー・トラスト



- セキュリティ
  - フィジカルセキュリティと
  - サイバーセキュリティの違い
  - ＃守る対象などの違いからくる技術などの違い
- プライバシー
  - 古典的なプライバシー権→「一人でほっておいてもらう権利」
  - データプライバシー
    - ビッグデータの活用、個人情報保護法、etc…
- トラスト
  - 従来からのトラスト？？
  - デジタルトラスト？？
    - -> なかなか議論が噛み合わない？

マイナンバー制度の議論（デジタルIDの議論）　２０１１年頃の議論
日本というドメイン（名前空間でもある）の中の議論

セコムIS研究所 Intelligent Systems Laboratory

社会保障･税番号大綱で示された番号制度を構成する
３つの仕組み　→　参考スライド27,28,29

そもそも「番号」や「ID」の意味するところは何か？

国民一人ひとりに唯一無二の番号を、最新の住所情報と関連付けて付番する仕組み

「番号」を利用する際に、利用者が「番号」の持ち主が本人であることを証明する本人確認の仕組み

IDentifier
個人番号（マイナンバー）

付番

番号制度

情報連携

本人確認

trusted IDentity exchange
・情報提供ネットワークシステム
・「特定個人情報」の定義と制度的フレームワーク

複数の機関において、それぞれの機関ごとに「番号」やそれ以外の番号を付して管理している同一人の情報を紐付けし、紐つけられた情報を活用する仕組み

クレデンシャル
IDentity credential
Identity Document
・個人番号カード（の券面、裏面）
・JPKI利用者証明用証明書と署名用証明書**

**「個人番号」は証明していない

出典：社会保障・税に関わる番号制度についての基本方針(2011年1月28日)
http://www.cas.go.jp/jp/seisaku/jouhouwg/renkei/dai1/siryou1_1.pdf より作図

11

３つの仕組みから
IDの多義的な意味を
理解する？

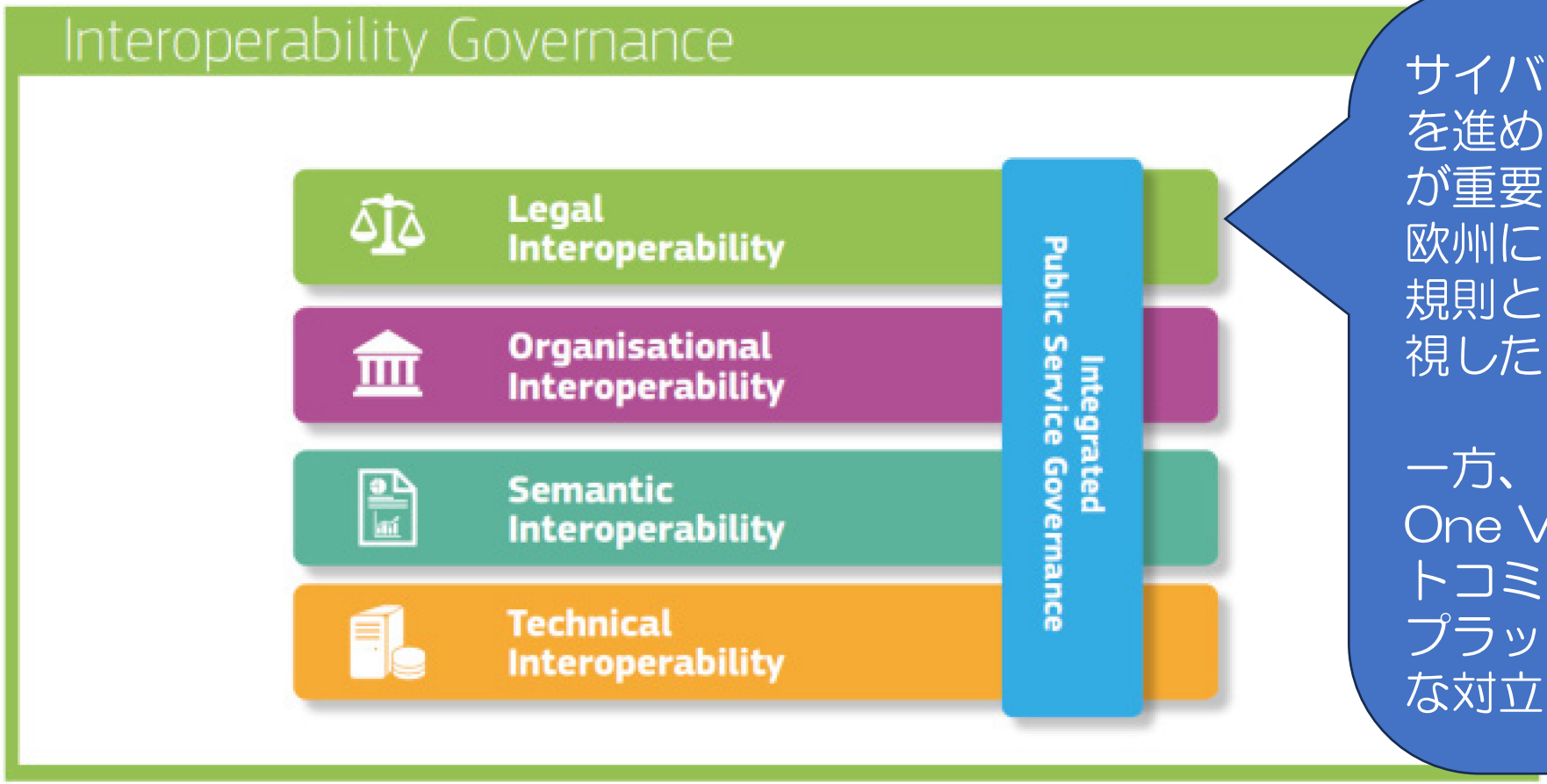
IDentifier
IDentity
Identity Document

本人確認・身元確認
IDentity Proofing
IDentity Verification

出典：
https://www.i-ise.com/jp/symposium/sym_160322_data/sym_20160322_matsumoto1.pdf

自律・分散・協調に必要な、相互運用性の意味するところも変化？？
European Interoperability Framework

Figure 3 Interoperability model



サイバー空間とリアル空間の融合を進めすほどに、法的相互運用性が重要性が浮上している。
欧州においては、GDPR、eIDAS規則といった法的相互運用性を重視した法制度の動きが顕著

一方、 One World. One Net. One Visionといったインターネットコミュニティの考え方や、巨大プラットフォーマーとの間で新たな対立の構造も生んでいるかも。

出典：https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf

トラストキューブ　保証レベルの相互運用性という難題（デジタルアイデンティティの大きな課題）

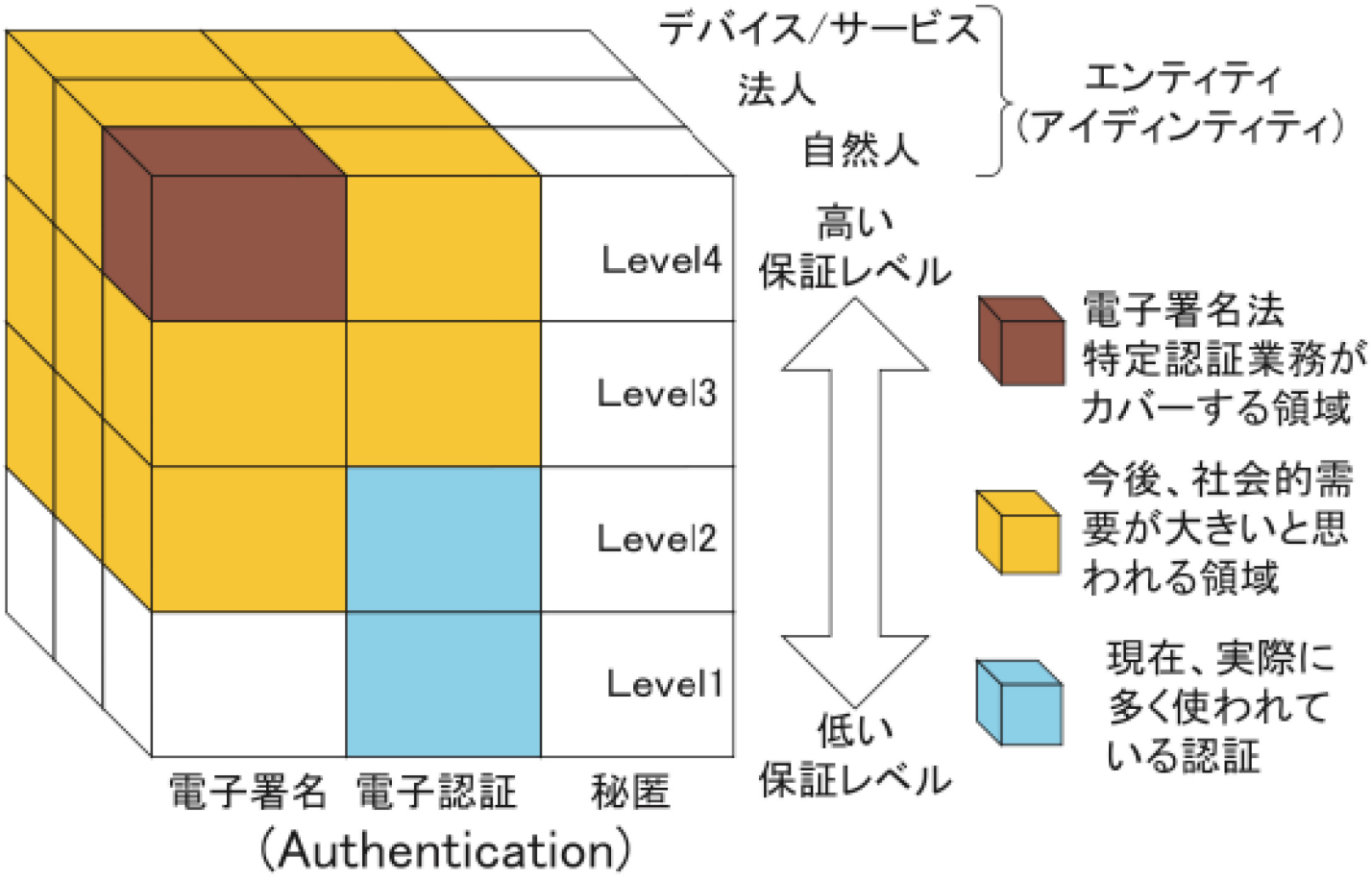


図３　トラストキューブ

社会基盤としての電子認証と電子署名　by 松本泰　2006
https://www.jstage.jst.go.jp/article/nig/43/5/43_5_324/_pdf

スマフォ依存の世界（スマフォが持つ鍵管理に依存）
Apple課金（税）と言うビジネスモデルを支える
Appleのプラットフォームセキュリティ、プライベートPKI、暗号鍵管理

セコム IS研究所
Intelligent Systems Laboratory

~~不正改造~~

~~サイバー攻撃~~

~~プライバシ侵害~~

サブスクリプション・サービス

サービス
アプリ

サービス提供

サービスプロバイダー

Relying Party（RP）

Apple
デバイス

TRUST

デバイス＆アプリの
健全性の証明
attestation

APPLE課金

- デバイスの健全性の維持
- （出荷後の）機能の拡張

デバイスの供給
（社会インフラの提供）

Apple

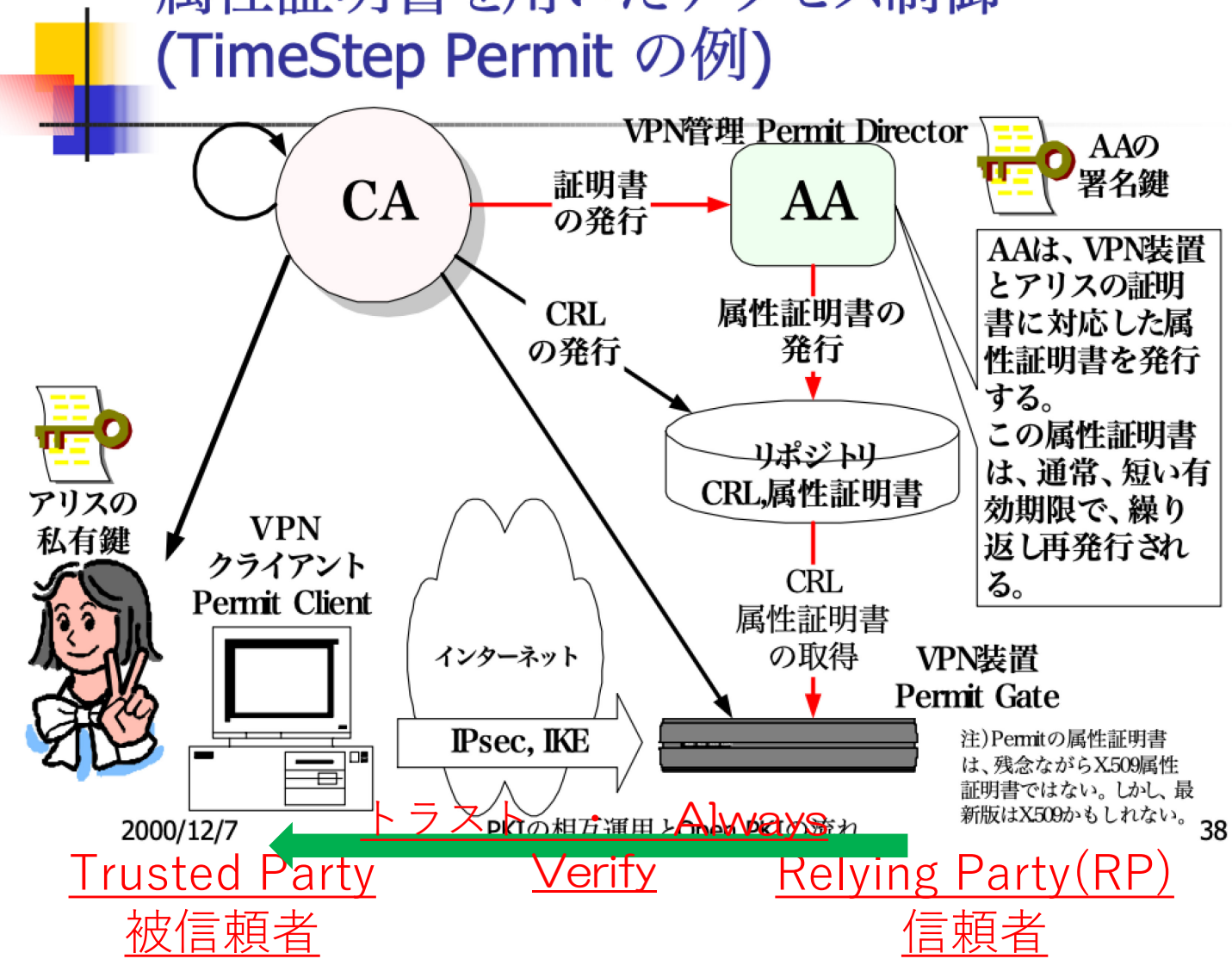
リモートアテステーションのためのPKI&CA（Certification Authority）認証局
Apple Private PKI
https://www.apple.com/certificateauthority/private/

Apple Private Root Certificate

- Apple App Attestation Root CA ▸ 2020年3月19日開始
- Apple WebAuthn Root CA ▸ 2020年3月19日開始
- Apple Secure Element Services Root CA ▸ 2019年4月18日 開始
- Apple Enterprise Attestation Root CA ▸ 2022年2月17日 開始

Apple Enterprise Attestation Root CA
iOS 16 からサポートされた企業におけるゼロトラスト実現のために管理対象デバイスのアテステーション (Managed Device Attestation)

VC(verifiable credentials)の議論の源流　X.509属性証明書



出典：日本インターネット協会(IAJ)セキュリティ部会主催の
第2回セキュリティフォーラム　2000年12月7日
https://www.iajapan.org/bukai/isec/forum/2000/20001207report.html

- 2023年現在のゼロトラスアーキテクチャと同様
  - VPN装置(Permit)は、FIPS140-2レベル２認証取得（ハードウェアセキュリティを具備している）
  - VPN装置内に格納されたRoot CAの公開鍵（検証鍵）がトラストアンカー
  - Relying Party としてのVPN装置は、トラストアンカー（公開鍵）から検証できる署名データ（公開証明書、属性証明書）以外は信頼しない（ゼロトラスト）。
- 2023年現在のVCの議論
  - アリスの名前を明かさず、属性のみを証明できる