PKIのこれまでとこれから

2024年3月7日

NPO 日本ネットワークセキュリティ協会　フェロー
松本　泰

JNSA

PKIのこれまでとこれから

1. PKIのこれまで　--　20分で語るPKIの25年間？？
2. PKIの今(FACT編??)
3. PKIのこれから(妄想編??)
4. 最後に

PKIのこれまで

20分で語るPKIの25年間？？

（１）　Challenge PKIプロジェクト（2001年から2008年頃まで）
（２）　2005年から（2021年まで）のPKI dayなど

2000年

日本インターネット協会(IAJ)セキュリティ部会主催
第2回 セキュリティ・フォーラム レポート. 2000年12月7日 開催

出典：https://www.iajapan.org/bukai/isec/forum/2000/20001207report.html

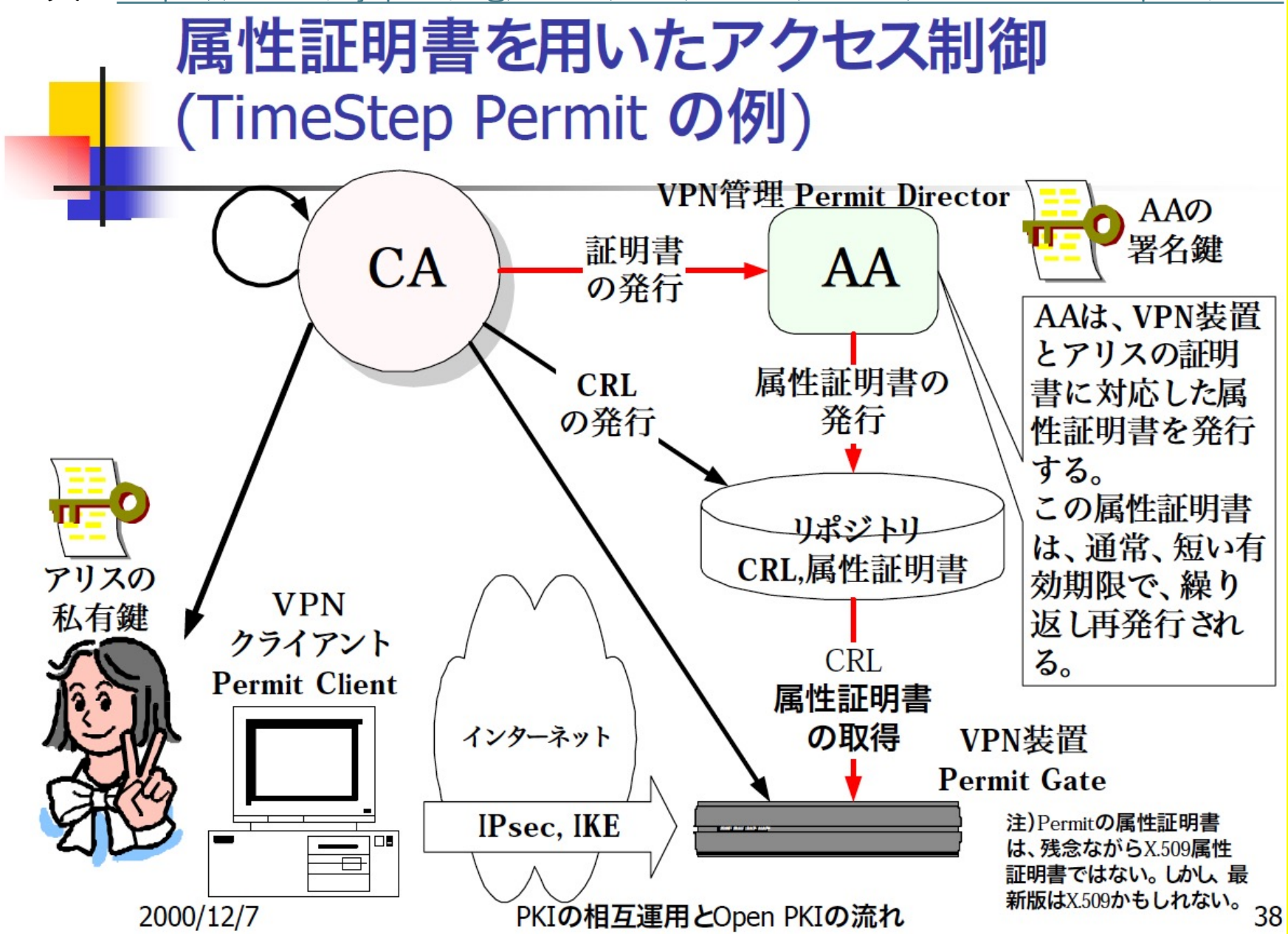
- (前略）今回は「PKIの相互運用とOpen PKIの流れ」と題して、セコム株式会社の松本泰さんにお話いただきました。 PKIはeビジネスの広がりや電子政府への取り組みの中で、ネットワーク上での本人確認と、 取引や情報の真実性等の確認と保証のための基本的枠組みを提供するもので、様々なソリューションが提供されだしていると共に、 共通性・互換性を持った社会基盤としての有効性・利便性等の実現に向けて様々な試みや開発が進められている分野です。

- 松本さんのお話はまず「ボブはいかにしてアリスを信用するか」という設問の下に、 夫々の信頼ポイントである自己のCA(電子認証局)同士の間での相互認証の仕組みという基本構造の解説からスタートし、 X.509を中心とする技術基準の動向と証明書のクラス(信頼性レベル)の問題、 信頼ドメインの概念とその相互認証・相互接続の仕組みや例、証明書失効リストの関係へと進みました。 そして相互認証証明書と証明書パスの構築による信頼の連鎖の仕組みが解説され、さらに、 複数PKI間の相互接続・相互運用のモデルと様々な技術課題の紹介にまで展開されて終りました。

- 普段なにげなく考えている電子署名やCAの問題がいかに複雑で奥が深く、 世界規模でのシームレスな運用のためにはまだまだ解決すべき問題が、単に技術だけでなく経済主体や社会基盤、 法整備や国際間のルールの確立も含めて多くあることが理解できました。（後略）

「PKIの相互運用とOpen PKIの流れ」 2000年12月7日

出典：https://www.iajapan.org/bukai/isec/forum/2000/20001207report.html



- 2024年現在の話題
- Verifiable Credentials(VC)
  - 属性証明が注目されている
  - 属性証明書は、VCの源流
  - 属性証明書にはないプライバシー保護技術を取り入れた選択的開示やゼロ知識証明などの標準化が進行中
  - → 属性証明を用いたアクセス制御は、とっても重要
- ゼロトラストアーキテクチャ
  - Pertmit Gateは、FIPS-140-2(レベル２：ハードウェア）認証取得　→ 耐タンパー性
  - Pertmit Gateに格納されるトラストアンカー(公開鍵）のみをトラストし、外部のデータ（ex. ユーザリスト）は、すべて検証（Verify）すなわち署名検証を行う。
  - → Never trust, always verify

「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

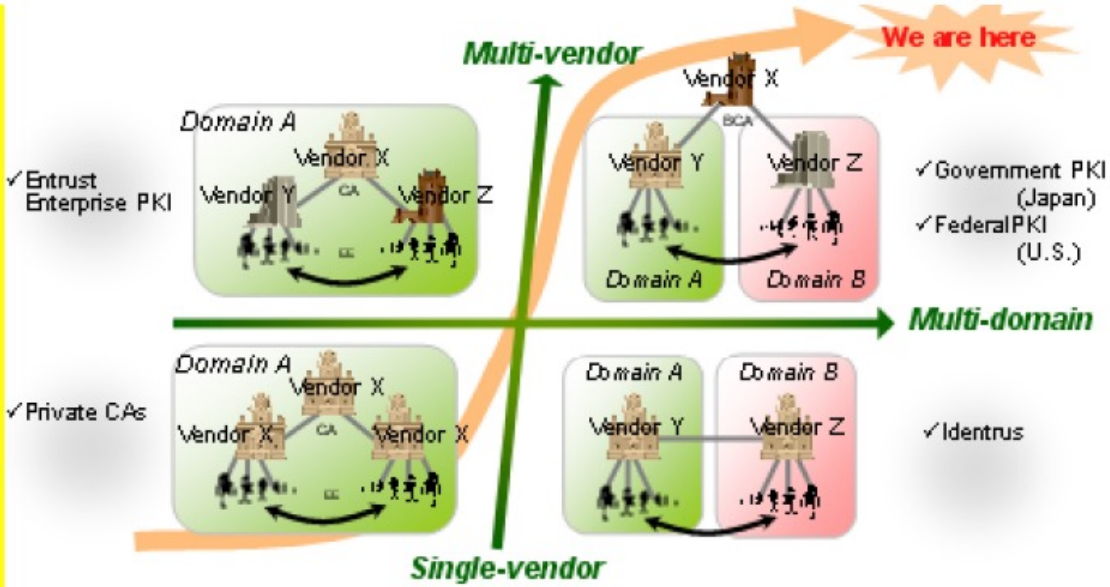
- インターネット・ドラフト 「マルチドメインPKIの相互運用性に関するメモ」がRFC 5217として公開されました。 (2008/07) NEW!
- Challenge PKI Test Suite 2.0で利用可能な、タイムスタンプ・プロトコル(TSP)用のテストケースが公開されました。(2004/7)
- Challenge PKI Test Suite 2.0で利用可能な、GPKI、地方公共団体認証基盤(LGPKI)、公的個人認証(JPKI)に対応したテストケースが公開されまし

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」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

出典：InternetWeek2023. 2023年11月22日　第二部：ちょっとさきのことをみんなで考える

2005年時点の「PKIのこれまでとこれから」

PKI day 2005
最初のPKI day

JNSAセキュリティセミナー（2005年） セミナー情報

RETURN ◀ PKI Day - PKI技術最新事情

プレゼンテーション資料を公開しました

- 日時： 2005年10月28日(金) 10：30～17：30（受付開始 10:00）
- 場所： セコムホール(セコム株式会社本社ビル2F) 東京都渋谷区神宮前1-5-1
  - ■原宿駅(竹下口より徒歩7 分)
  - ■明治神宮駅(出口5より徒歩5分)
- 主催： NPO 日本ネットワークセキュリティ協会 PKI相互運用技術WG
- 定員： 100名
- 料金： 参加無料
- 申込方法： **申し込み受付は終了しました。**
- 概要： PKIは、情報社会の様々なインフラとなるべき技術ですが、その技術の幅は非常に幅広く、また、奥深いものがあります。PKIが普及していないという指摘がある一方、電子パスポート、金融機関のICキャッシュカード、医療PKIなどPKI技術を利用した様々なインフラは、今後のIT社会における信頼を確立するため深く浸透して行くものと考えられます。
  NPO JNSAのPKI相互運用技術WGおよびChallenge PKIプロジェクトでは、PKIの相互運用技術をキーワードに様々な活動を行ってきました。今回のセミナーでは、これまでの活動の成果などを踏まえ、PKI技術の最新動向について説明します。

★プレゼンテーション資料 （※10/31更新）
恐れ入りますが、セミナーご参加の方は、事前に資料をダウンロード、プリントアウトの上、当日ご持参いただけますようお願い致します。

- **経営幹部にPKIを理解してもらうためには...**(290KB) 宮川 寧夫 氏
- **PKI標準化最新動向**(811KB) 稲田 龍 氏
- **マルチドメインPKIと相互運用性のBest Current Practice**(1.65MB) 島岡 政基 氏
- **グリッドコンピュータとPKI**(1.83MB) 奥野 琢人 氏

↑圧縮(zip)ファイルはこちらからどうぞ(1.5MB)

- **JPNIC認証局 ～IPアドレス認証局(認証)～**(1.56MB) 木村 泰司 氏
- **WS-FederationとPKI**(3.53MB) 鈴木 章太郎氏

↑圧縮(zip)ファイルはこちらからどうぞ(1.9MB)

- **Challenge PKIプロジェクトとPKI最新技術事情**(312KB) 松本 泰 氏

出典： PKI Day - PKI技術最新事情 (PKI day 2005)
https://www.jnsa.org/seminar/2005/seminar_20051028.html

Challenge PKIプロジェクトの活動

活動履歴

セコムIS研究所 Intelligent Systems Laboratory

2001	2002				2003				2004				2005
4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q

Challenge PKI 2001

Challenge PKI 2002 GPKI 相互運用フレームワーク

Challenge PKI 2003 タイムスタンプ・プロトコル セキュリティAPI

Challenge PKI 2004 PKI における UTF8String 問題

55th IETF アトランタミーティングの PKIX WG において発表 2002.11.20

57th IETF ウィーンミーティングの PKIX WG において発表2003.7.17

62th IETF ミネアポリスミーティングの PKIX WG において発表 2005.3.8

JNSA主催 NSF2002での発表 2002.6.12

2002.12.17 JNSA W2002セミナ

JNSA ChallengePKI IETF参加等活動報告会の開催 2004.4.27

セキュリティAPIセミナーを開催 2004.8.26

54th IETF 横浜ミーティングの PKIX WG において発表 2002.7.17

56th IETF サンフランシスコ・ミーティングの PKIX WG において発表 2003.3.20

JNSA主催 NSF2003での発表 2002.10.24

認証技術の動向」セミナーを開催 2004.12.9

PKI day 2005
最初のPKI day

出典： PKI Day - PKI技術最新事情 (PKI day 2005)
https://www.jnsa.org/seminar/2005/seminar_20051028.html
Challenge PKIプロジェクトとPKI最新技術事情
https://www.jnsa.org/result/pki/seminar/2005/2005-017.pdf

JNSA Challenge PKIプロジェクト
Challenge PKI 2001 – 参加団体
(と今日のセミナーの講演者)

セコムIS研究所 Intelligent Systems Laboratory

実験参加企業(団体)	製品	
セコムトラストネット/エントラストジャパン	Entrust PKI 6.0	島岡、松本
SSH	SSH Certifier 2.0	
NECソフト	NEC Carassuit電子政府版Ver1.1	
RSAセキュリティ	Keon Cerficate Authority 6.0	
富士ゼロックス/富士ゼロックス情報システム	未発表製品	稲田さん
マイクロソフト プロダクトディベロップメント リミテッド	Microsoft Windows Server	及川さん
日本ベリサイン	(非公開)	
名古屋工業大学	Easy Cert(開発 奥野　琢人氏)	奥野さん
WIDEプロジェクト	ICAP v2.51(ICAT)	木村さん

９個のCA製品orサービスを使ったCA相互接続実験

6

PKI day 2005
Challenge PKI 2001

2001年当時
IPA：「電子政府情報セキュリティ技術開発事業 /
IPsec 相互接続実証実験

このサブプロジェクト的に行ったのが、CA相互接続実験が、
Challenge PKI 2001

色々な方に参加を呼びかけ、出会い、その後の人的コミュニティに繋がった

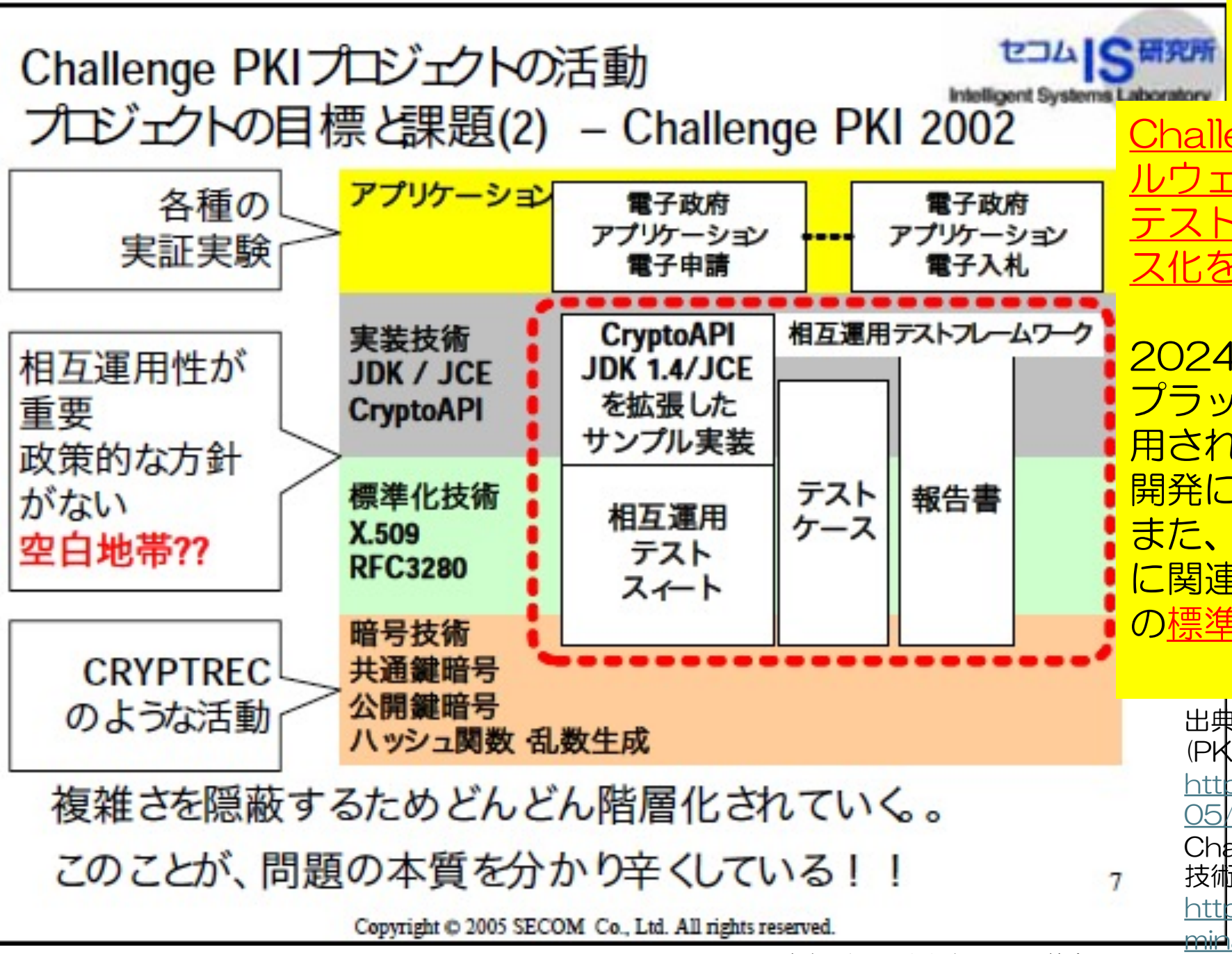
出典：PKI Day - PKI技術最新事情 (PKI day 2005)
https://www.jnsa.org/seminar/2005/seminar_20051028.html
Challenge PKIプロジェクトとPKI最新技術事情
https://www.jnsa.org/result/pki/seminar/2005/2005-017.pdf

JNSA

PKI day 2005
Challenge PKI 2002

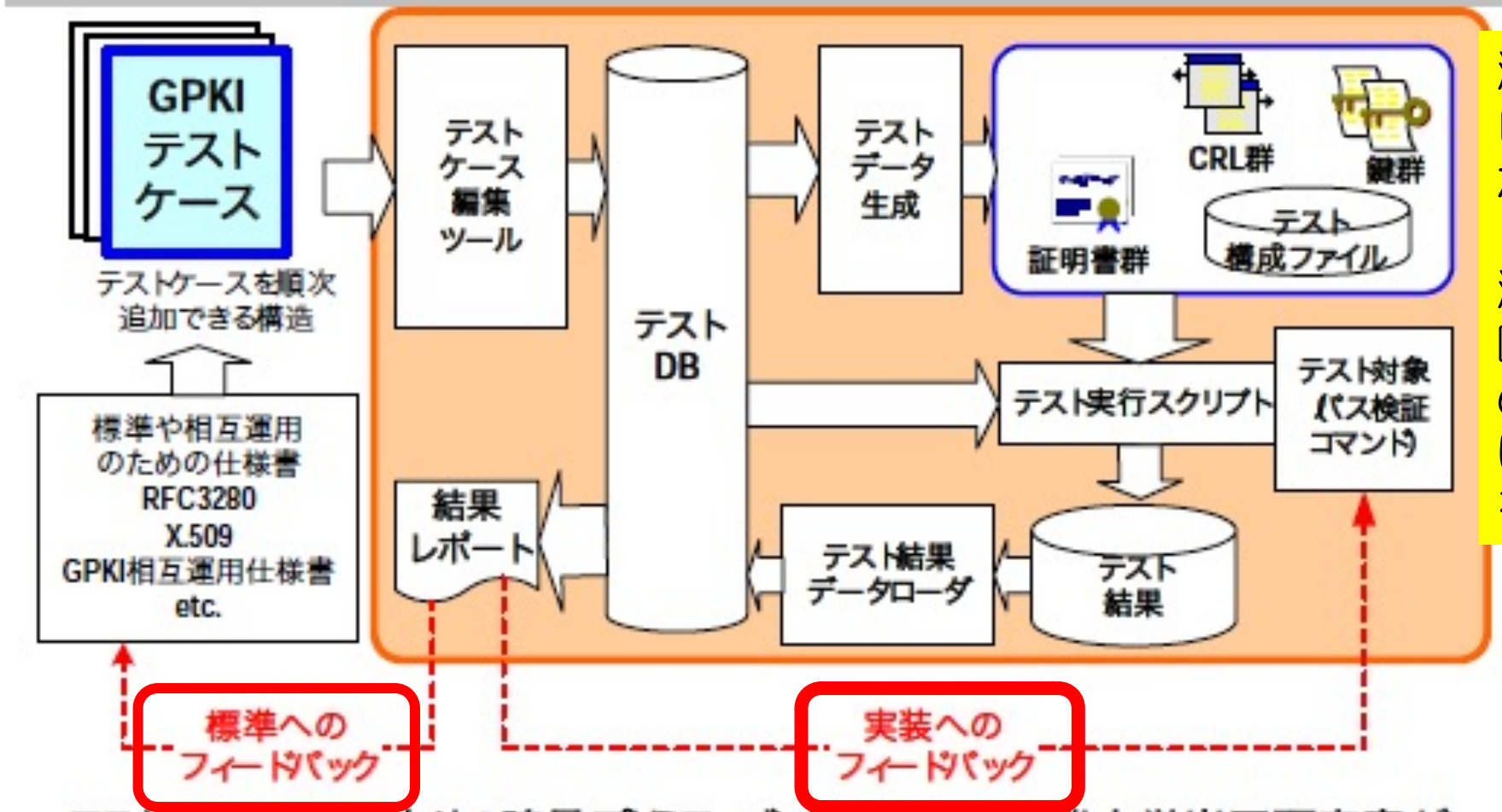
Challenge PKI 2002では、ミドルウェアーのレファレンスコード、テストースィートのオープンソース化を目指した。

2024年現在、欧州においては、プラットフォームとして共通に利用されるビルディングブロックの開発に多くの予算を配置している。また、そのビルディングブロックに関連する相互運用性確保のための標準化に力を入れている。



出典： PKI Day - PKI技術最新事情 (PKI day 2005)
https://www.jnsa.org/seminar/2005/seminar_20051028.html
Challenge PKIプロジェクトとPKI最新技術事情
https://www.jnsa.org/result/pki/seminar/2005/2005-017.pdf

Challenge PKI 2002-プロジェクトの成果物
相互運用テストスィート



テストデータ生成のための暗号プリミティブには、名古屋工業大学岩田研究室が開発したAICryptoを使用

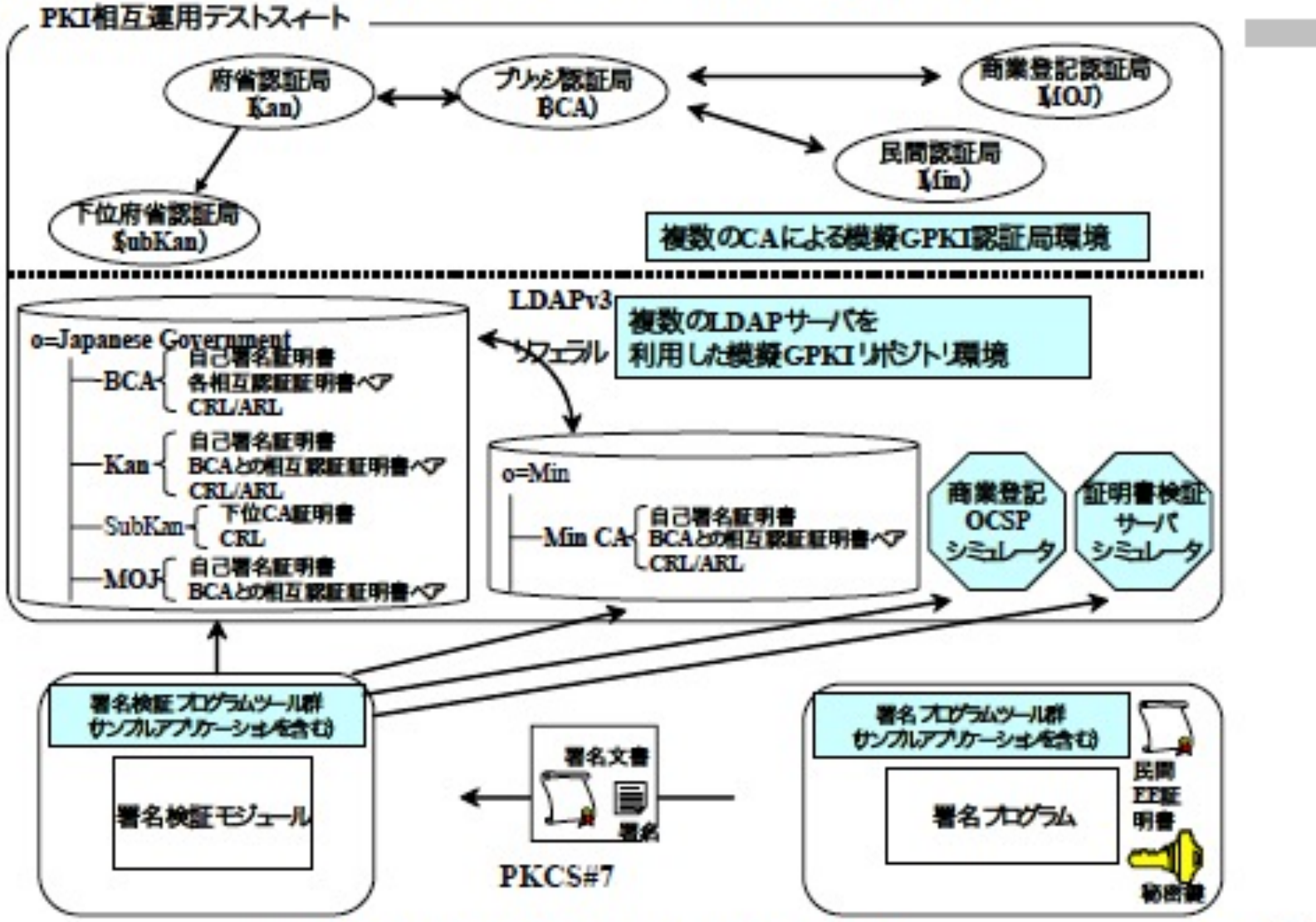
PKI day 2005
Challenge PKI 2002

漆嶌賢二さん（現GMOグローバルサイン）が、かなりの部分を設計、開発。

漆嶌さんは、この後、欧州の標準化団体であるETSIのリモートプラグテストにおいても、類似したテスト環境を構築した。

出典：　PKI Day - PKI技術最新事情 (PKI day 2005)
https://www.jnsa.org/seminar/2005/seminar_20051028.html
Challenge PKIプロジェクトとPKI最新技術事情
https://www.jnsa.org/result/pki/seminar/2005/2005-017.pdf

Challenge PKI 2002- プロジェクトの成果物
相互運用テストスィート+テストケース = GPK 模擬環境



Copyright (c) 2003 NPO日本ネットワークセキュリティ協会 page 24

PKI day 2005
Challenge PKI 2002

出典： PKI Day - PKI技術最新事情 (PKI day 2005)
https://www.jnsa.org/seminar/2005/seminar_20051028.html
Challenge PKIプロジェクトとPKI最新技術事情
https://www.jnsa.org/result/pki/seminar/2005/2005-017.pdf

Challenge PKI 2002 - プロジェクトの背景
GPKIの要求とパス検証の実装

	Microsoft CryptoAPI Win-2000	Micosoft CryptoAPI Win-XP	JDK1.4 Cert. Path lib.	サンプル実装(*1)	GPKIの要求 (パス構築、パス検証)
基本制約拡張	○	○	○	○	必須
ポリシ制約拡張	×	○	○	○	必須
ポリシマッピング拡張	×	○	○	○	必須
名前拡張	×	○	○	○	必須
AIA拡張 / OCSP	×	×	×	○	必須(官側のみ)
動的パス構築	×	△	○	○	必須
CRL IDP *2	×	○	×	○	必須

***1 Challenge PKI 2002プロジェクトで開発したサンプル実装**

***2 CRL IDP (issuing distribution point)**

PKI day 2005
Challenge PKI 2002

PKI相互運用性の鍵となる
RFC 2459 1999年
-> RFC 3280 2002年
-> RFC 5280 2008年
Internet X.509 Public Key Infrastructure Certificate and CRL Profile
「トラストチェーン」の検証の重要性
→ ドメインが広がるほどに難しくなる。これは、2024年現在においても大きな課題

出典： PKI Day - PKI技術最新事情 (PKI day 2005)
https://www.jnsa.org/seminar/2005/seminar_20051028.html
Challenge PKIプロジェクトとPKI最新技術事情
https://www.jnsa.org/result/pki/seminar/2005/2005-017.pdf

PKI技術最新事情と今後の課題
今後取り上げたいテーマでもある。。。

セコム Intelligent Syster

PKI day 2005
2005年時点のPKIのこれから

- SHA-1問題
  - 「PKI における UTF8String 問題」と似た課題を抱える？
  - どうやって移行するのか??誰が全体を取りまとめるか??
- 電子署名法の改正の検討??
  - 技術の問題ではないかもしれない。。
  - しかし技術と政策の乖離が様々な問題を引き起こしているのではないか？
- 医療PKI
  - 医療のIT化等による、医療の効率化、質の向上、利便性向上等の要求
  - これらを実現するセキュリティ基盤としてのPKI
- その他注目すべき動向
  - e文書法に対応した動向
    - ECOMの「長期署名フォーマットのプロファイルの相互運用性テスト」など
  - PKI＆アイデンティティマネージメント
    - 大規模なPKIは、連携アイデンティティ・マネージメントへと進化していく
  - グリッドコンピュータとPKI
  - 学術系認証基盤の動向
  - 機器認証、プラットフォーム認証　TPM/TCG等

普及といった観点からは、ライトウェイトなPKIの重要性も認識されるべき

暗号アルゴリズムの2010年問題へ
2024年現在は、暗号アルゴリズムの
2030年問題、そしてPQC移行問題へ

次スライド

出典：　PKI Day - PKI技術最新事情 (PKI day　2005)
https://www.jnsa.org/seminar/2005/seminar_20051028.html
Challenge PKIプロジェクトとPKI最新技術事情
https://www.jnsa.org/result/pki/seminar/2005/2005-017.pdf

TCG25周年！！関連する技術、標準が、2024年現在、大きく変貌。
HW Root OF Trustとリモートアテステション

JNSA

PKI day 2005
2005年時点の今後

電子署名法改正の議論

セコムIS研究所 Intelligent Systems Laboratory

- 正式名称
  - 「電子署名及び認証業務に関する法律」
- 主な内容
  - 電磁的記録の真正な成立の推定
  - 認証業務に関する任意的認定制度の導入
    - 「特定認証業務」の認定 – 2005年10月時点で17件の認定
- 対象
  - 自然人の電子署名が対象
- 対象外
  - 法人、サーバ、エージェント。。。。の署名
  - 電子認証(Authentication)??、暗号
- 電子署名法の施行　2001年4月1日に施行　（来年で5年）
  - 政府は、この法律の施行後五年を経過した場合において、この**法律の施行の状況について検討を加え、その結果に基づいて必要な措置を講ずる**ものとする」(附 則　第三条)
    - 5年前、当初目指していた社会との齟齬はたくさんあるはず。

19

出典：　PKI Day – PKI技術最新事情 (PKI day 2005)
https://www.jnsa.org/seminar/2005/seminar_20051028.html
Challenge PKIプロジェクトとPKI最新技術事情
https://www.jnsa.org/result/pki/seminar/2005/2005-017.pdf

電子署名法改正の議論
電子署名法特定認証業務認定制度の問題

セコムIS研究所 Intelligent Systems Laboratory

- 非常に認定基準が厳しい
  - 結果、高コスト
  - 「認定基準が厳しい」ことは悪いことではない。問題は「認証事業者」以外がそのことを知らないこと。
- 非常に制約が厳しい　#技術の不理解が融通の利かない制度を作っている??
  - 結果、柔軟なPKIが構築できない
  - 自然人にしか証明書が発行できない
    - 「電子署名法」の範疇は、人と人の関係だけで、人と物、物と物の信頼関係を築けない。もしくは、人と物、物と物の信頼関係を分断しているかもしれない – いわゆる「オレオレ証明書」問題も関係あるかも。。。。

民間における電子署名法特定認証業務認定認証局の問題

- 「非常に認定基準が厳しい」+「非常に制約が厳しい」=民間におけるビジネスの創造を阻害している可能性がある。現実に純粋に民間向けの認証局は少ないし減少傾向にある。これは本来の制度の目的を満たしていない。また、普及しないのであれば「制度」自体の意味をなさない。

20

2024年現在の電子署名法は、既存の法律の「民事訴訟法228条2項」に対応する「電子化」の対応であり、法律の立て付けとして、2024年現在におけるデジタル社会におけるDX（デジタルトランスフォーメーション）を目指した発想に乏しい。

JNSA

IETF(pkix)における標準化活動

Challenge PKI 2002 活動報告
「IETFでのPKI関連技術動向」

NPO日本ネットワークセキュリティ協会
富士ゼロックス株式会社
稲田　龍 <Ryu.Inada@fujixerox.co.jp>

2003年　6月 4日

JNSA ChallengePKI2002

- JNSAが行ったChallenge PKI 2002の説明とデモンストレーションを行った。
- 報告書の英訳とソースコードの公開を約束

- 2003年当時　IETF PKIX WGチェア
- RFC 2459（1999年）の著者
- SP800-63　電子認証に関するガイドラインの初版（2004年）の著者

出典：
https://www.jnsa.org/nsf2003spring/pdf/b5.pdf

IETFにおける標準化活動

RFC 5217

Network Working Group
Request for Comments: 5217
Category: Informational

M. Shimaoka, Ed.
SECOM
N. Hastings
NIST
R. Nielsen
Booz Allen Hamilton
July 2008

Memorandum for Multi-Domain Public Key Infrastructure Interoperability

Status of This Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Abstract

The objective of this document is to establish a terminology framework and to suggest the operational requirements of Public Key Infrastructure (PKI) domain for interoperability of multi-domain Public Key Infrastructure, where each PKI domain is operated under a distinct policy. This document describes the relationships between Certification Authorities (CAs), provides the definition and requirements for PKI domains, and discusses typical models of multi-domain PKI.

出典： https://www.rfc-editor.org/rfc/rfc5217.html

IETF 61 ワシントンD.C. 2004年11月

第61回IETFミーティング報告

富士ゼロックス株式会社 稲田 龍
セコム株式会社IS研究所 島岡 政基
NPO日本ネットワークセキュリティ協会 安田 直義

写真2 Nelson E. Hasting氏との打ち合わせの風景
(左より富士ゼロックス 稲田、セコムIS研究所 島岡氏、
IPAセキュリティセンター 宮川氏、NIST Hasting氏)

出典：
https://www.jnsa.org/jnsapress/vol13/13_17-24.pdf

PKI day 2019 までの歩み

セコム IS研究所 Intelligent Systems Laboratory

1	2005	PKI技術最新事情	技術中心の議論
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	法制度も含めた議論
7	2011	番号制度時代のPKI	
8	2012	・我が国における信頼基盤の連携に向けて ・PKIへの攻撃とその対応	
9	2014	・公開鍵暗号に関連する周辺技術動向の共有 ・デジタル社会のための「電子署名を見直す」	
10	2015	サイバーセキュリティの要となるPKIを見直す	
11	2016	マイナンバー時代のPKI	社会の変化に伴う議論??
12	2017	IoT・ブロックチェーン時代のPKI	
13	2018	超スマート社会（Society 5.0）におけるトラストの在り方	
14	2019	午前の部　IoTのトラスト 午後の部　トラストサービスの在り方	

PKI & TRUST Days online 2021
「デジタル社会におけるトラスト」

第１日目：2021年4月15日（木）　テーマ：変貌するトラストアーキテクチャ
第２日目：2021年4月16日（金）　テーマ：デジタルトラストにおける法と技術のあり方

JNSA

2010年頃からの暗号鍵管理の議論

寄　稿

暗号技術による個人情報保護の制度と技術の動向

セコム株式会社 IS 研究所
松本　泰、伊藤　忠彦

1. はじめに

個人情報を適切に保護するための暗号技術については、個人情報保護法が施行された当時から現在に到るまで、様々な議論があったようです。個人情報に限らず、暗号技術により情報を保護するためには、「暗号アルゴリズム」、「暗号モジュールの実装」、「暗号化に利用する鍵の管理」、それらすべてが適切である必要があります。

7月3日に開催された「JNSA／第2回 鍵管理勉強会」ではこうした暗号技術・鍵管理技術のあるべき姿と、これらの技術が制度にどう組み込まれていくべきか等を念頭に、「暗号技術による個人情報保護の制度と技術の動向」を勉強会のテーマとして取り上げ、議論を行いました。

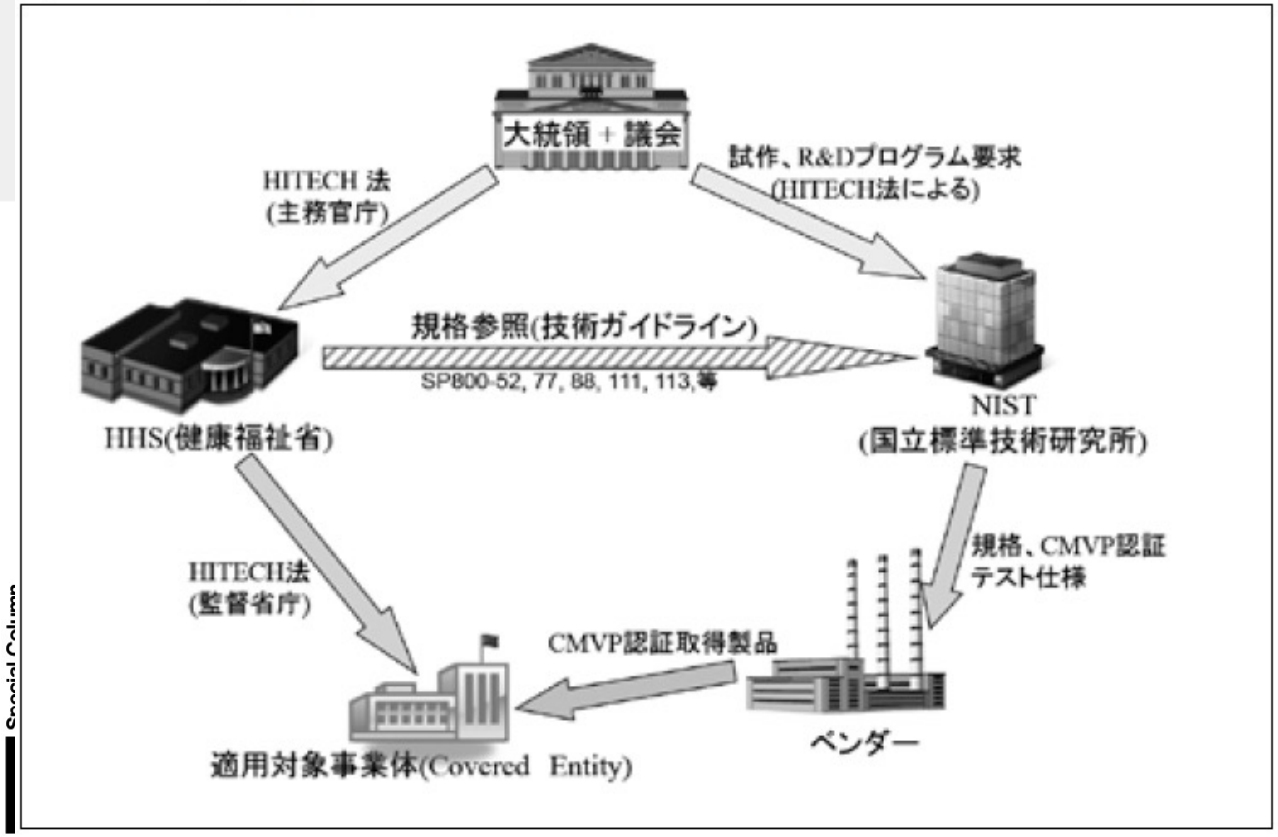
本稿では、鍵管理勉強会の議論も踏まえ、日本と米国の状況を説明し、今後の日本における課題を考察します。

それにより特定の個人を識別することができることとなるものを含む。）をいう。

法第20条
個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

同法に対しては、主務官庁が作成するガイドラインが40以上存在し、その中でそれぞれが第2条第1項と第20条の解釈を示しています。例えば、「個人情報保護に関する法律についての経済産業分野を対象とするガイドライン」（経済産業省 2009 年改訂）では、同法第2条第1項の「個人情報」について「暗号化等により秘匿化されているかどうかを問わない」としています。同時に、同ガイドラインは同法第20条の対策として「高度な暗号化等による秘匿化を講じる事

図1：HITECH 法のスキーム



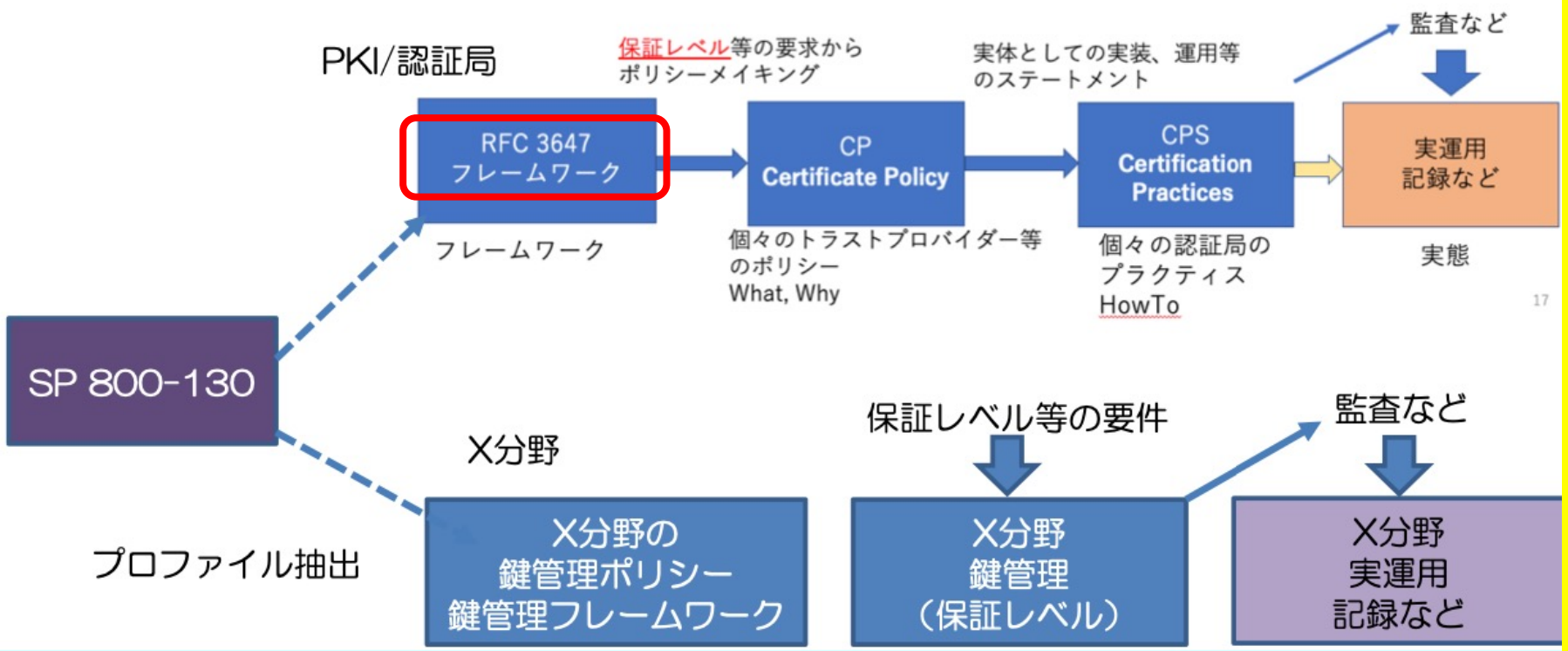
個人情報の「高度な暗号化等の秘匿化」
これは、結局のところ「暗号化に利用した暗号鍵管理」に大きく依存する。しかし「暗号鍵管理」の重要さの認識が。。。。

出典：JNSA Press 第34号　2012年9月発行
https://www.jnsa.org/jnsapress/vol34/3_kikou.pdf

第1回 鍵管理勉強会（2010年11月22日開催）
https://www.jnsa.org/seminar/seckey/101122/
第2回 鍵管理勉強会（2012年7月3日開催）
https://www.jnsa.org/seminar/seckey/120703/
第3回 鍵管理勉強会（2020年10月13日（火）開催）
https://www.jnsa.org/seminar/seckey/201013/index.html

SP 800-130　2013年

A Framework for Designing Cryptographic Key Management Systems



RFC 2527.　1999
->RFC 3647　2003
Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

PKIの保証レベルの基礎となるフレームワーク（鍵管理、Identity proofing　などのフレームワーク）

Identity proofingは、NIST SP800-63等へ

鍵管理は
NIST SP800-130等へ

出典：　第３回 鍵管理勉強会　「暗号鍵管理の重要性」
https://www.jnsa.org/seminar/seckey/201013/data/1_matsumoto.pdf

PKIの今(FACT編??)

ゼロトラストアーキテクチャ　　Never trust, Always Verify

Never trust　　何も（暗黙的に: Implicit ）信頼しない

→ だけど、PKI（と、デバイスのHW Root OF Trust)には、暗黙の信頼を置く。

Always Verify　PKIのトラストアンカーを起点に、 Always Verify を行う。

→　属性証明書で説明したPertmit Gateと同様

→　属性証明を利用したアクセス制御へ

（１）　Apple （Private）PKI

（２）　CSA Matter　PKI

信頼される安心を、社会へ

SECOM

Appleの製品・サービスのビジネスモデル＆トラストを支えるApple のPKI

- Apple Root CA
  - Apple Application Integration CA (AAI Sub-CA)
  - Worldwide Developer Relations CA (WWDR Sub-CA)
  - Software Update Sub-CA
  - Developer ID Sub CA
  - General Timestamp CA

５種類の認証局

出典：
https://www.apple.com/certificateauthority/

出典：　PKI & TRUST Days online 2021「デジタル社会におけるトラスト」
https://www.jnsa.org/result/pki/seminar/2021/2021-019.pdf

JNSA

Appleの製品・サービスのビジネスモデル＆トラストを支える Apple のPKIから発行される様々なデジタル証明書

信頼される安心を、社会へ SECOM

- WWDR iOS Software Development Certificates (“iOS Development Certificates”)
- WWDR iOS Software Submission Certificates (“iOS Submission Certificates”)
- WWDR Apple Push Notification service Development SSL Certificates (“Development SSL Certificates”)
- WWDR Apple Push Notification service Production SSL Certificates (“Production SSL Certificates”)
- WWDR Push Certificate Signing Request Signing Certificates (“Push CSR Signing Certificates”)
- WWDR Safari Extension Signing Certificates (“Safari Certificates”)
- WWDR Mac App Development Certificates (“Mac App Development Certificates”)
- WWDR Mac App Submission Certificates (“Mac App Submission Certificates”)
- WWDR Mac Installer Package Submission Certificates (“Mac Installer Package Submission Certificates”)
- Mac App Store Application Signing Certificates (“Mac App Store Application Certificates”)
- Mac App Store Installer Package Signing Certificates (“Mac App Store Installer Package Certificates”)
- Mac App Store Receipt Signing Certificates
- Mac Provisioning Profile Signing Certificates
- Pass Certificates
- Website Push Notification Certificates
- OS X Server Authentication Certificates
- VoIP Services Push Certificates
- Apple Pay Merchant Certificates
- Apple Pay Pass Certificates
- TestFlight Distribution Certificates
- WatchKit Services Certificates
- Apple Pay Provisioning Encryption Certificates
- Enhanced Pass Certificates
- tvOS Application Signing Certificates
- WWDR Apple Push Services Client Authentication G2 Certificates
- Apple Pay Merchant Client Authentication Certificates
- WWDR Apple Development Signing Certificates ("Apple Development Certificates")

５種類の認証局の一つ Worldwide Developer Relations　認証局 が発行する、デジタル証明書（公開鍵証明書）

2024年現在、28種類の公開鍵証明書を発行している。

出典：
https://images.apple.com/certificateauthority/pdf/Apple_WWDR_CPS_v1.22.pdf

出典：　PKI & TRUST Days online 2021「デジタル社会におけるトラスト」
https://www.jnsa.org/result/pki/seminar/2021/2021-019.pdf

JNSA

リモートアテステーションのためのPKI&CA（Certification Authority）認証局

セコムIS研究所 Intelligent Systems Laboratory

Apple Private PKI
https://www.apple.com/certificateauthority/private/

５種類の認証局とは、別に新たな４つのプライベート認証局

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)

Appleのリモートアテステーションは、比較的、新しいサービス

出典　SecurityDay2023.　Socity5.0実現にとっての(ゼロ)トラスト：
https://drive.google.com/file/d/1aQ5RYf9HrSgpJMmLu1DcOQMTvt1ejGqt/view

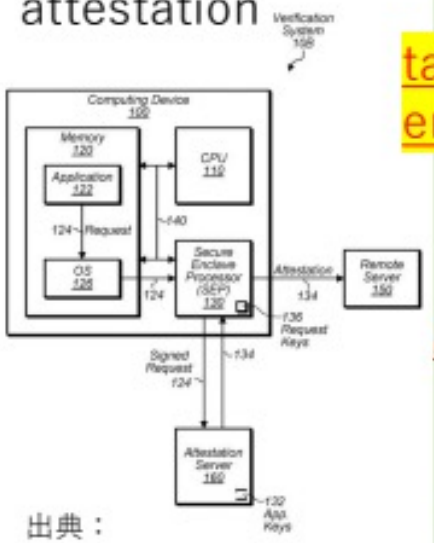
JNSA

Apple のApp. Attestation

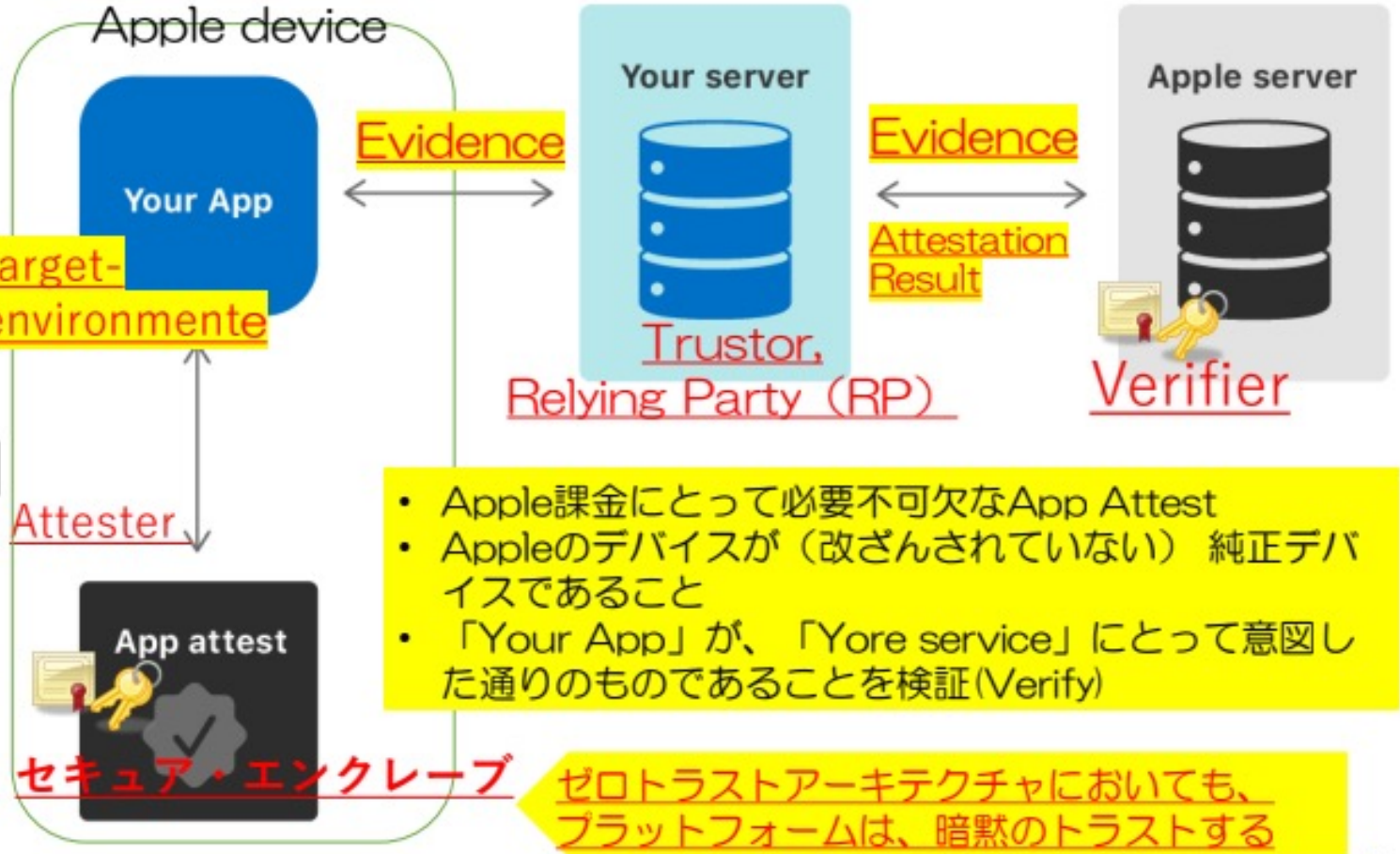
出典： https://developer.apple.com/documentation/devicecheck/validating_apps_that_connect_to_your_server

セコムIS研究所 Intelligent Systems Laboratory

Apple社の特許
Application integrity attestation



出典：
Application integrity attestation
https://patents.google.com/patent/US20200159966A1/



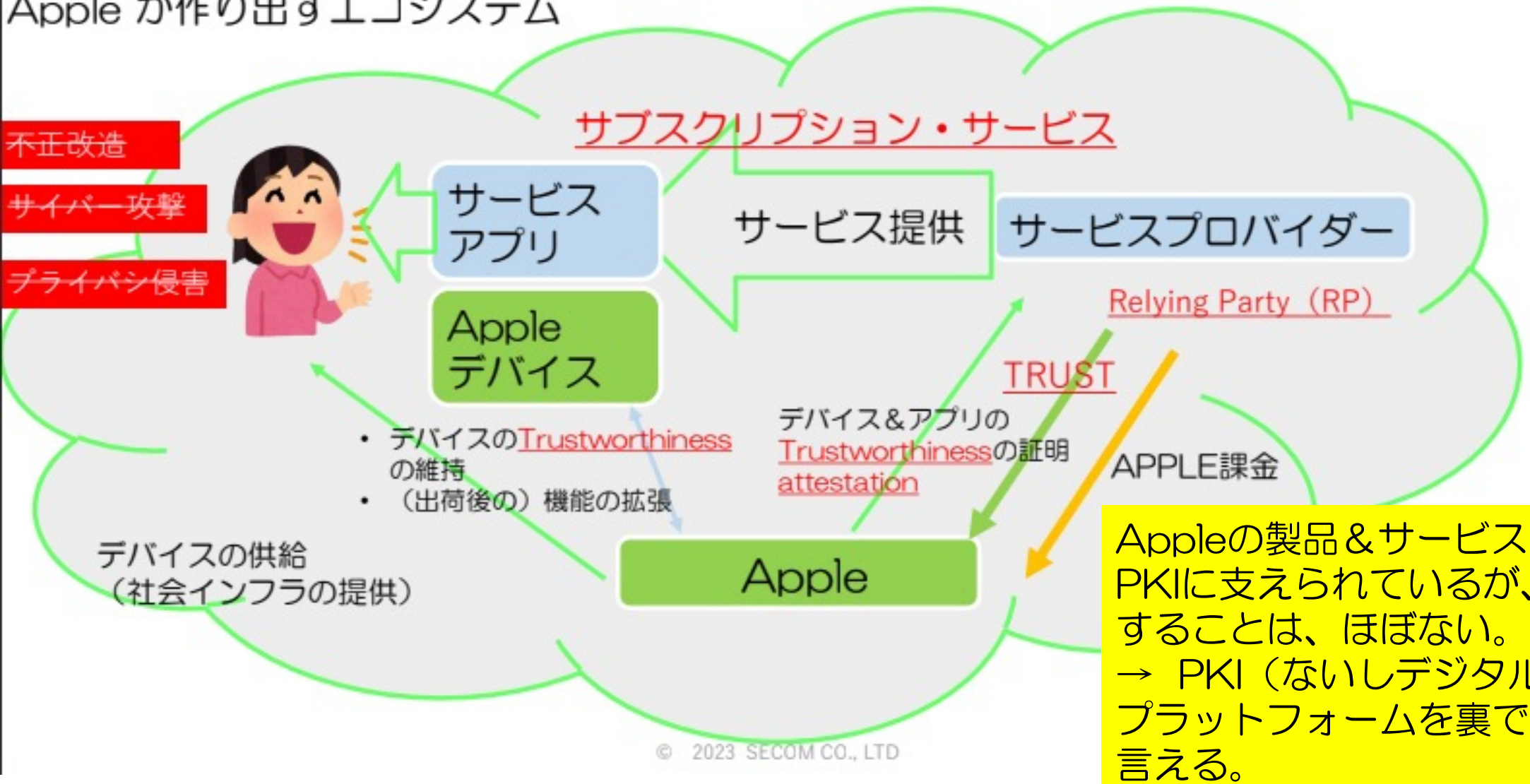
- Apple課金にとって必要不可欠なApp Attest
- Appleのデバイスが（改ざんされていない） 純正デバイスであること
- 「Your App」が、「Yore service」にとって意図した通りのものであることを検証(Verify)

ゼロトラストアーキテクチャにおいても、プラットフォームは、暗黙のトラストする

出典
SecurityDay2023.
Socity5.0実現にとっての(ゼロ)トラスト：
https://drive.google.com/file/d/1aQ5RYf9HrSgpJMmLu1DcOQMTvt1ejGqt/view

・比較的よく理解されている署名の使い方
　→ 文書（のハッシュ値）に署名を行い、リモートのRP/Verifierは、ドキュメントの改ざん検出を行う。
・リモートアテステーションの署名の使い方　→　2024年現在、こうした署名の使い方が急激に増えている？？
　→ デバイスの構成・アプリケーションなど（ハッシュ値）に、デバイスに組み込まれたアテスターが署名を行い、リモートの RP/Verifierは、デバイスの構成・アプリケーショ等が意図通りなのか、改ざん検出を行う。

Apple課金（税）と言うビジネスモデルを支える
システムのデジタルトラスト（Apple のゼロトラストアーキテクチャ）
Apple が作り出すエコシステム



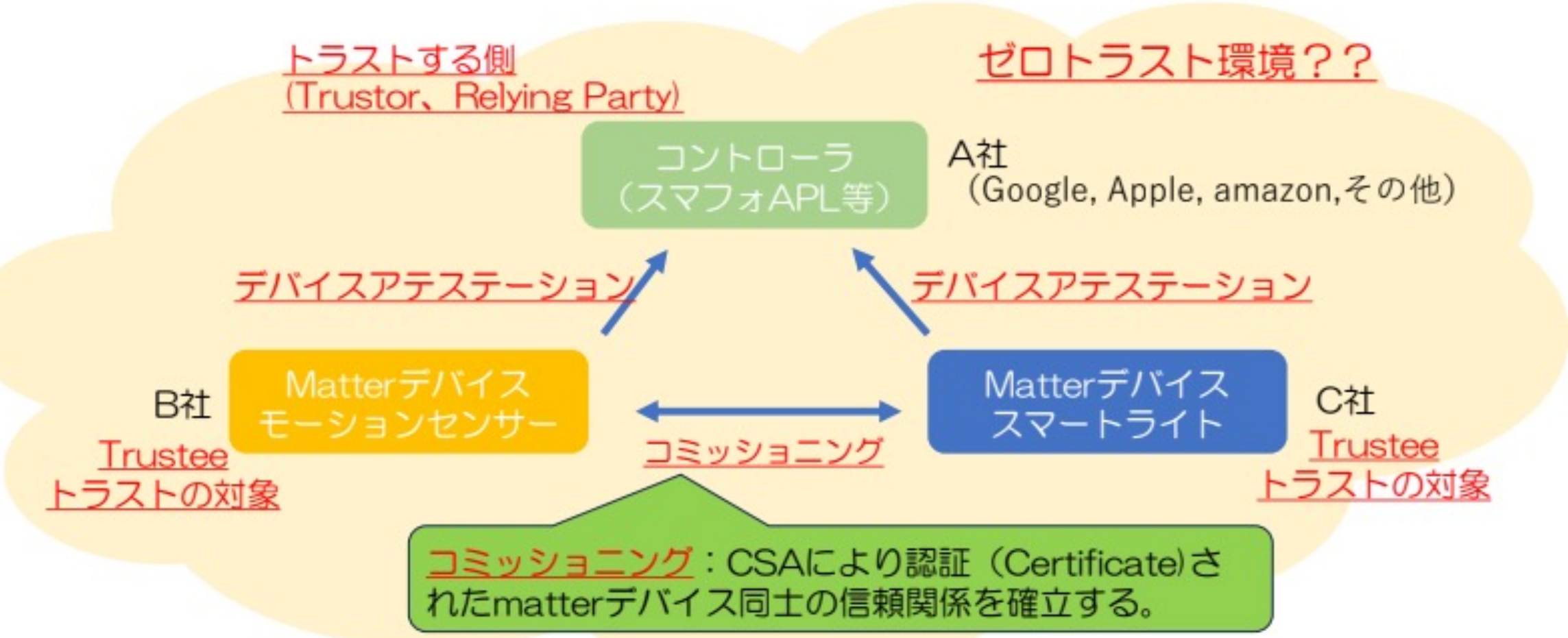
Appleの製品＆サービスは、AppleのPKIに支えられているが、利用者が意識することは、ほぼない。
→ PKI（ないしデジタルトラスト）は、プラットフォームを裏で支える仕組みと言える。
→ プラットフォーマに全面的に依存するのであれば、PKIは要らないかも？？

出典　SecurityDay2023.　Socity5.0実現にとっての(ゼロ)トラスト：
https://drive.google.com/file/d/1aQ5RYf9HrSgpJMmLu1DcOQMTvt1eiGat/view

CSA Matter　PKI

セコムIS研究所 Intelligent Systems Laboratory

CSA matterのデバイスアテステーション



出典　SecurityDay2023. 2023年12月14　開催　　Socity5.0実現にとっての(ゼロ)トラスト：
https://drive.google.com/file/d/1aQ5RYf9HrSgpJMmLu1DcOQMTvt1eiGqt/view

JNSA

CSA Matterについて https://csa-iot.org https://webui.dcl.csa-iot.org

セコムIS研究所 Intelligent Systems Laboratory

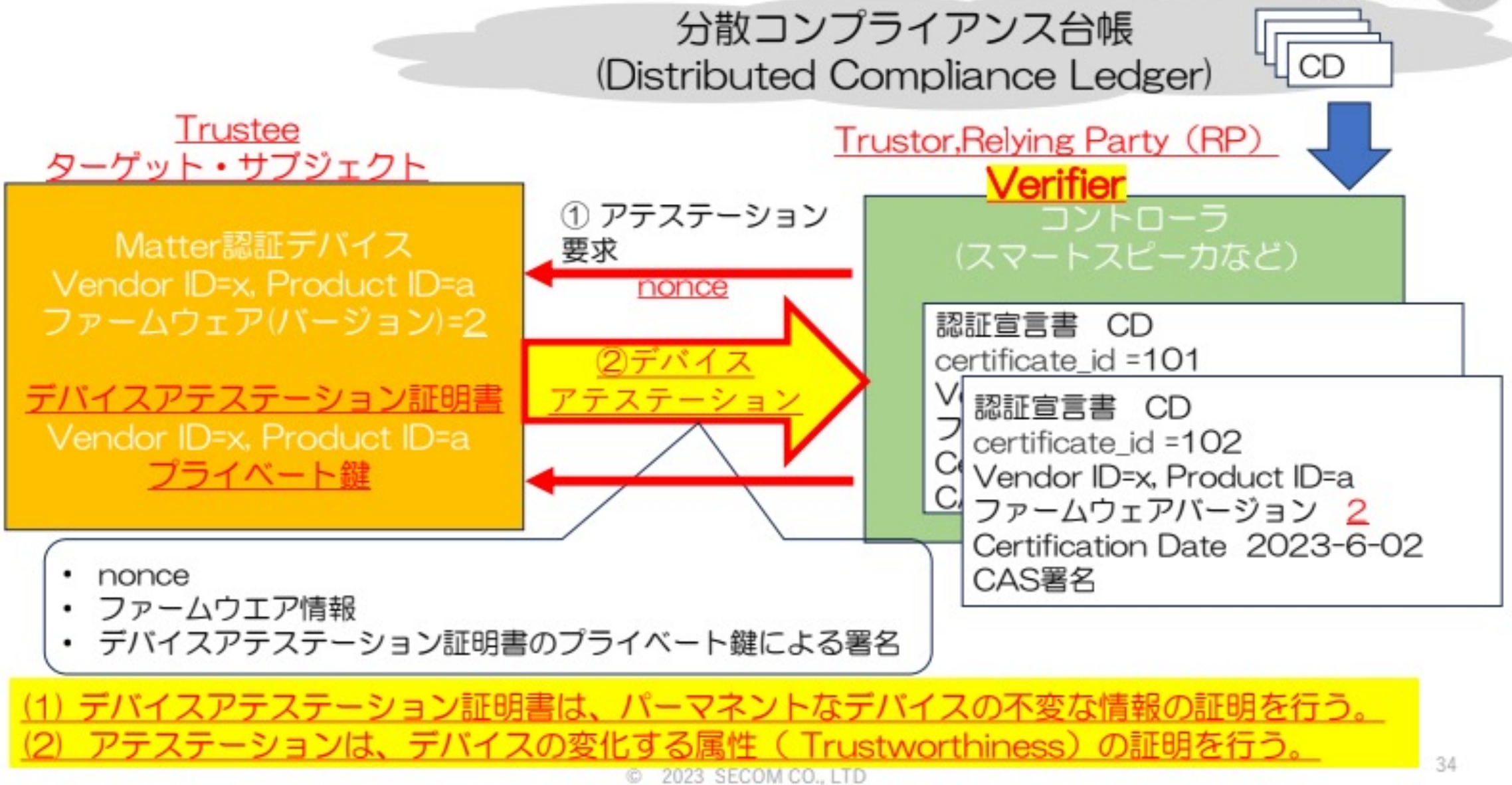
- CSA(Connectivity Standards Alliance) Matter
  - Matterは、CSAが策定しているスマートホームの標準規格。
- 参加ベンダー
  - 153社以上　(Apple, Google, Amazon, Samsung, Xiaomi, Signify(Philips), etc..)
- Matterデバイス認証(Certificate)
  - 2022年11月から認証開始　　認証製品　　846 製品以上
- 認証宣言書　CD (Certification Declaration)
  - デバイスがMatter認証（Certificate）を受けていることを表す書類・データ
  - **Vendor ID, Product ID**,ファームウェアバージョン、認証日など
- デバイスアテステーション証明書 (Device Attestation Certificate)　　MAX　600byte の制約
  - Matterデバイスに組み込まれるX.509公開鍵証明書（デバイスにはプライベート鍵も組み込まれる）
    - デバイスのMatter認証（Certification）、デバイスの**Vendor ID**、**Product ID** の証明とプライベート鍵のバインドを証明
- デバイスアテステーション　　→　　アテステーションは、属性証明
  - Relying Party(RP)であるコントローラに対して、 Matterデバイスの状態（ファームウェアバージョン等）を証明（アテステーション）。X.509公開鍵証明書のプライベート鍵による署名が施される。
- 分散コンプライアンス台帳 (Distributed Compliance Ledger)　　→　　CSAのリポジトリ
  - デバイスアテステーション証明書のトラストアンカー（ルート証明書など）、認証宣言書などが格納される。

出典　SecurityDay2023.　Socity5.0実現にとっての(ゼロ)トラスト：
https://drive.google.com/file/d/1aQ5RYf9HrSgpJMmLu1DcOQMTvt1ejGqt/view

JNSA

CSA Matterのデバイスアテステーション

セコムIS研究所 Intelligent Systems Laboratory



出典　SecurityDay2023.　Socity5.0実現にとっての(ゼロ)トラスト：
https://drive.google.com/file/d/1aQ5RYf9HrSgpJMmLu1DcOQMTvt1ejGqt/view

JNSA

CSA matterのデバイスアテステーション

セコムIS研究所 Intelligent Systems Laboratory

- CSA matter以前から、「モノ」の認証(Certificate)は、さまざまな分野で存在している（自動車、医療機器、etc.)
  - しかし、一般的に 「モノ」の認証(Certificate)が、リモートから動的に検証(Verify)できる手段は、提供されていなかった。　→　always verify は、できない
  - また、出荷後の個別の「モノ」のtrustworthinessの変化（ソフトウェア更新など）に対応する仕組みも無かったと考えられる。　→　出荷後は、更新、未更新のデバイスが混在する。
- CSA matterでは、現時点では、IETF RATSのリモートアテステーションほどの機能はないが、出荷後のデバイスのtrustworthinessを検証するために仕組みが、今後、整備されていくだろうと考えられる。
  - IETF RATSのリモートアテステーションのVerifier にかわり、コミッショナーデバイス（コントローラ）が、分散コンプライアンス台帳に登録された情報から、デバイスのtrustworthinessを検証する手段が、拡充されていく可能性がある？？。
- IoTデバイス自体のtrustworthinessを高めるための認証(Certificate)は、ともて重要だが、それだけでは、なかなか、 継続的にtrustworthinessを高めるインセンティブが、ベンダーに働かない。
  - CSA matterのデバイスアテステーションのような仕組みは、RPからの自動的な検証と接続ができることとなり、これは、IoTデバイスの継続的なtrustworthinessを高めるインセンティブが働く。

出典　SecurityDay2023.　Socity5.0実現にとっての(ゼロ)トラスト：
https://drive.google.com/file/d/1aQ5RYf9HrSgpJMmLu1DcOQMTvt1ejGqt/view

JNSA

PKIのこれから　（妄想編？？）

本日のゴール？？　（さて、ゴールまで辿り着けるか？？）
ゼロトラスト　Never Trust 、Always Verifyにより実現する世界観??

セコムIS研究所
Intelligent Systems Laboratory

出典：　https://horizon-connect.eu/wp-content/uploads/2022/11/CONNECT_Leaflet_web.pdf

- CONNECT: Continuous and Efficient Cooperative Trust Management for Resilient CCAM
  - 欧州のHorizon Europeのプロジェクト
  - 開始　2022年9月　（終了　2025年10月）
    https://horizon-connect.eu
- CCAM(Cooperative Connected Automated Mobility)
  - EUが推進するコネクテッド協調型自動運転
  - コネクテッドカー、協調型 ITS（高度道路交通システム）、自動運転を融合を目指したプロジェクト
  - マルチベンダー、マルチステークホルダー、マルチドメインで構成されるエコシステムで構成される System Of Systems
  - ->. 単体の自動運転車の話ではない
- CONNECTは、 CCAMのトラスト管理を目指したプロジェクト
- そのアーキテクチャのコンセプトは
  - Never Trust 、Always Verify
  - ゼロトラストアーキテクチャでトラスト管理を実現

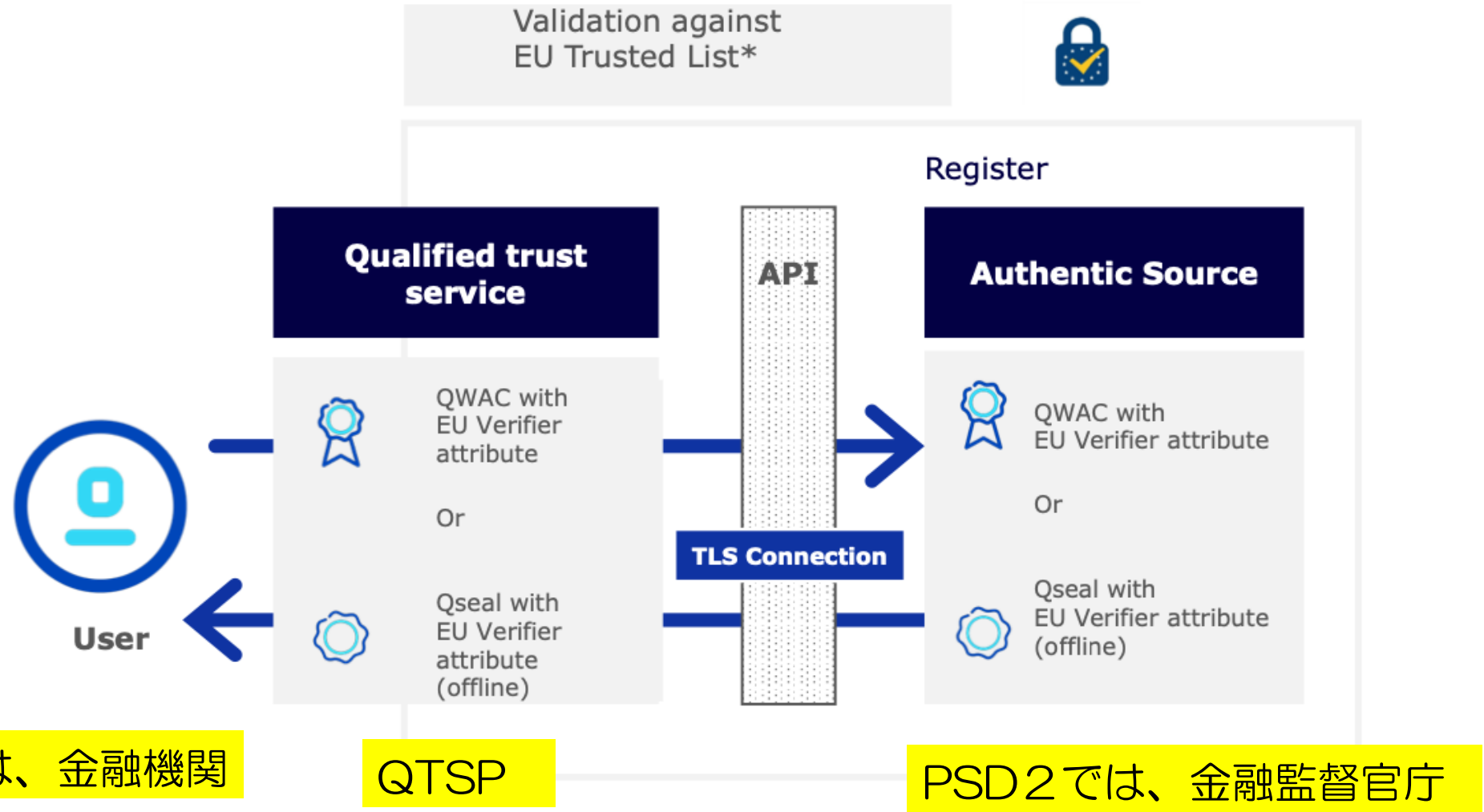
出典
SecurityDay2023.
Socity5.0実現にとっての(ゼロ)トラスト：
https://drive.google.com/file/d/1aQ5RYf9HrSgpJMmLu1DcOQMTvt1ejGqt/view

一応、2024年現在、松本が注目しているところ

- 属性証明　　eIDAS2.0における属性証明
  - EU Digital Identity Wallet
    - 属性アテステーション（electronic attestation of attributes）
      - →　たぶん、属性アテステーションへの署名には、 eSeal が利用される。
  - QWAC(Qualified website authentication certificate)とeSeal の属性付き公開鍵証明書
    - →　属性の保証をどのように実現するのか？？→ PSD2(Payment Services Directive 2)で実績あり
    - QWACとeSeal の属性付き公開鍵証明書は、同一法人にセットで発行される。たぶん。。
    - QWACでは、例えば、Webサイトでの個人情報の入力時に、そのサイトが欧州の金融監督庁が認めた金融機関であることが確認できる（ eIDAS2.0では、ブラウザベンダーにこうしたことを義務つけようとしている）。　　＃このQWACに関してEFF（ Electronic Frontier Foundation）などは猛烈に反発
  - → 2001年施行の日本の電子署名法は、1999年の欧州の電子署名指令の影響を強く受けた。しかし、2024年3月現在成立直前のeIDAS2.0は、日本の電子署名法とは全く別物
  - → eIDASは、日本ではその意義の認識が低い電子署名法の第四条以降（特定認証業務の認定等）が発展拡大
- サイバーフィジカルシステム（System Of Systems）のトラスト、トラスト管理
  - コンシューマIoTデバイスの認証　→　ETSI　EN　303 645などの単体デバイスの認証（Certificate）
    - →　この認証が、RPから検証可能（ verifiable、remote attestation ）へ→ CSA matterのような仕組み
    - →　結果、ゼロトラスト環境に置かれたSystem Of Systemsのトラスト管理可能な方向へ
  - クラウドとIoTデバイスが一体化したトラストアーキテクチャへ

JNSA

PSD2 Model for the Authentic Source API



PSD２では、金融機関

QTSP

PSD２では、金融監督官庁

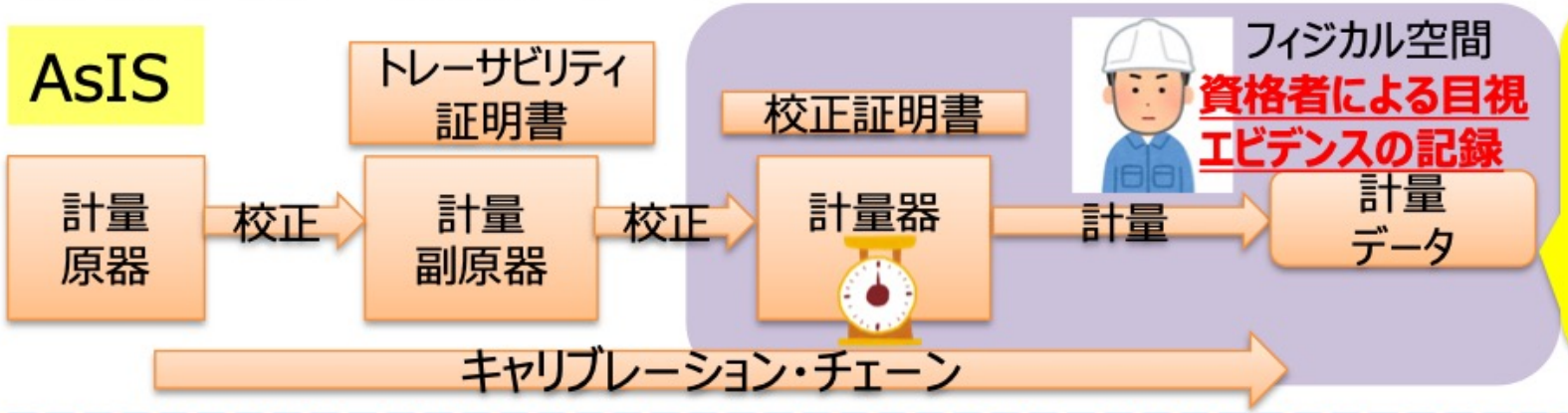
*European Trust Service List according to Implementing Decision (EU) 2015/1505 (https://webgate.ec.europa.eu/tl-browser)

https://www.teletrust.de/fileadmin/user_upload/01_Informationstag_Elektronische-Signatur-und-Vertrauensdienste_D-Trust_Nguyen.pdf

セキュアコンポーネントとPKIの役割　-- CPS上のトラスト
例えば、計量（計測）データの信頼性（Trustworthiness）では

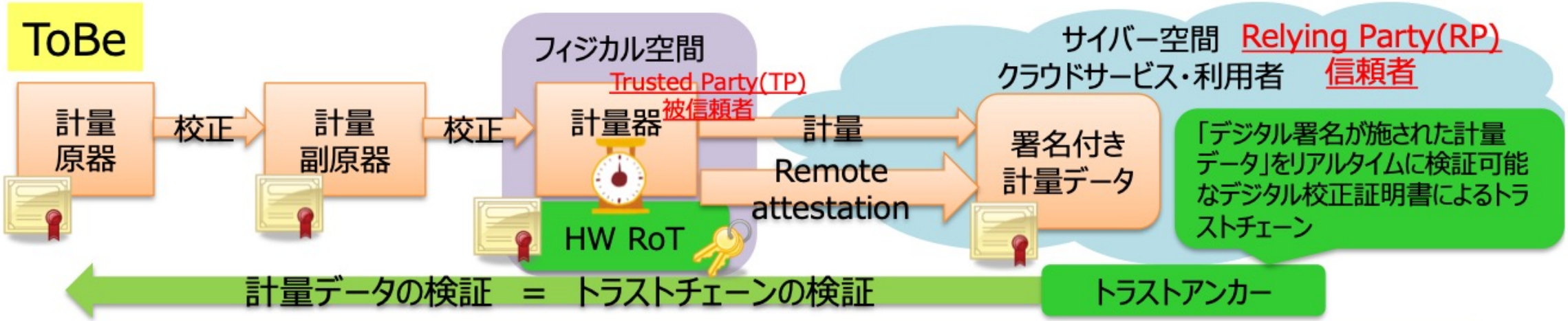
信頼される安心を、社会へ。 SECOM

AsIS



計量（計測）データの信頼性（Trustworthiness）で最も重要なことは、計量器、計量データのキャリブレーション・チェーン が証明、保証されていること。

ToBe



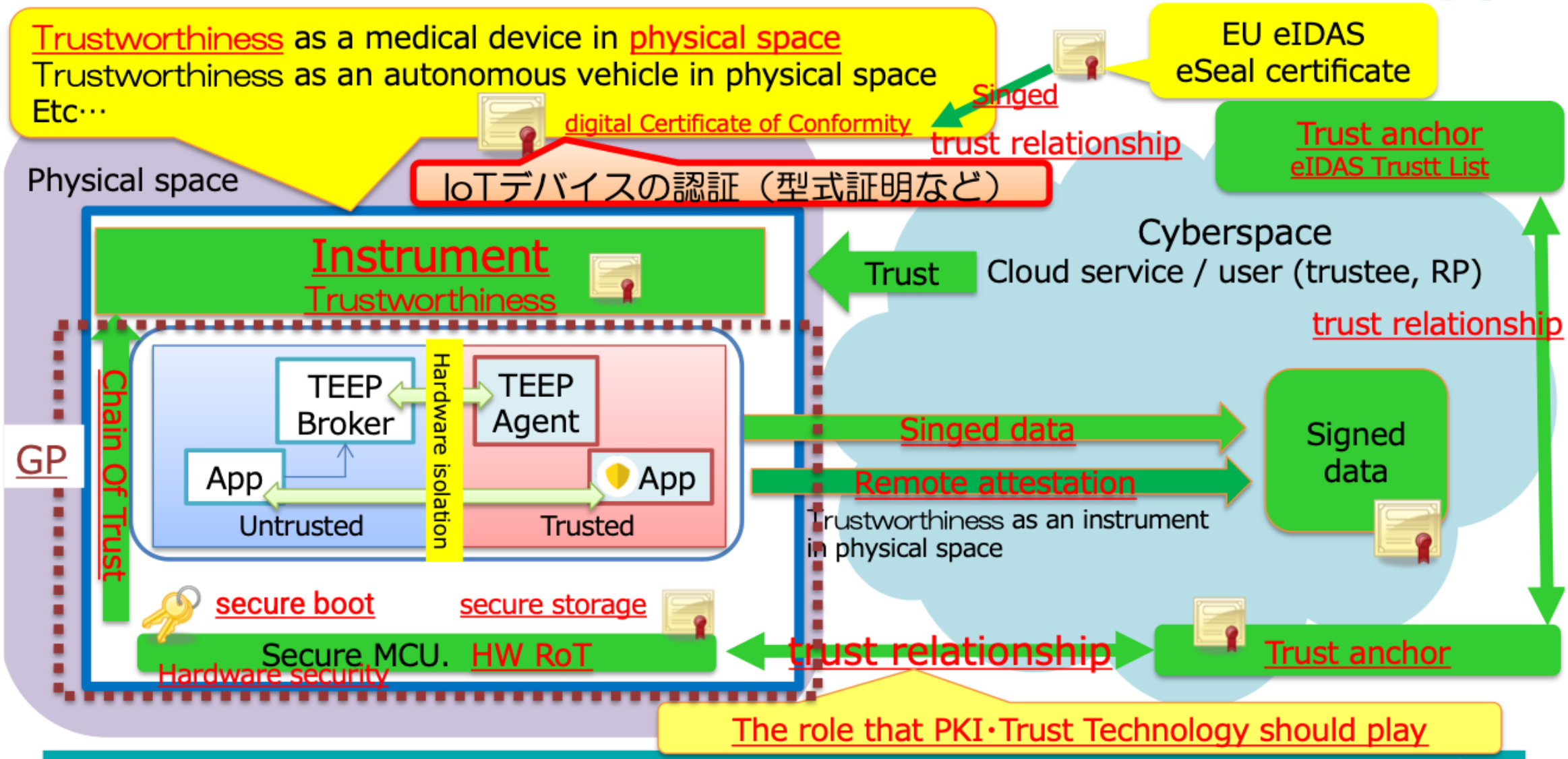
PKI・トラスト技術の役割　→　デバイス・データの信頼性（Trustworthiness）をRPに伝える
→ 人の目視に頼らず、デバイス・データの信頼性（Trustworthiness）が検証できること

出典：　IEICE 第8回 DPF研究会　セキュアコンポーネントとPKIが作るデジタルトラストの世界
https://www.ieice.org/~dpf/wp-content/uploads/2021/08/松本DPF研究会.pdf

JNSA

Role of PKI / Trust Technology--Trust in Cyber-Physical Systems

信頼される安心を、社会へ。 SECOM



出典： IEICE 第8回 DPF研究会　セキュアコンポーネントとPKIが作るデジタルトラストの世界
https://www.ieice.org/~dpf/wp-content/uploads/2021/08/松本DPF研究会.pdf

JNSA

インテグリティ実装のパラダイムシフト
→ Auditing & Attestation パラダイムシフト

信頼される安心を、社会へ。
SECOM

データソース

曖昧さ、間違い、改ざんの可能性を内包したデータ

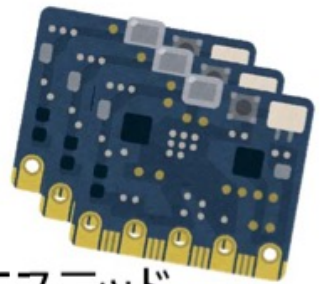
データクレンジング等の作業

データベース

目視による整合性チェック（インテグリティチェック）

Auditing & Attestation
監査及び証明業務（アテステーション）

データソース



トラステッド IoTデバイス

デジタル署名付きデータ

リモートアテステーション（構成管理）

一意なデバイスIDと、リモートアテステーションにより管理されたIoTデバイスを前提に設計されたデータベース

クラウドサービスデータベース

自動化されたデジタル署名の検証、トラストチェーンの検証によるインテグリティチェック

出典：　データ戦略の課題と未来　　2019年11月27日
https://www.jlf.or.jp/assets/work/pdf/kenshu_190910_04.pdf

JNSA

最後に？

井戸を掘った人々

鈴木優一さん
2005年7月6日永眠
享年66歳

「鈴木優一さんを偲ぶＩＴの会」ご案内

早くも秋になりましたが、皆様お元気のことと存じます。
急なことでご存じない方も少なくないと思われますが、われらが畏友・鈴木優一さんが去る７月６日にお亡くなりになりました。癌でした。病状が急速に悪化したためごく身近な友人だけしか知らず、告別式も身内の方だけで行われました。
この度、昌子夫人にもご賛同をいただき、鈴木優一さんのＩＴの世界での業績を偲び、ご関係の深かった方によるシンポジウムとパーティーを別記のように開催し、鈴木優一さんの遺り残したことを継承していきたいと思います。皆様のご参集をお願い出来れば幸いです。
なお、当日ご参加の方に、鈴木優一さんの２０数年にわたるＩＴ関連ドキュメントを収録しましたCDをお渡しすべく準備中です。
１０月３０日までに、出欠のご返事をメールにて、このお知らせを送信いたしました幹事までいただければ幸いです。

２００５年１０月１０日

代表世話人　田尾陽一（友人）　、
幹事世話人　松本　泰（セコムＩＳ研究所）、安田直義（JNSA）、木村吉博(JIMA)
世話人　杉井清昌（セコム株式会社執行役員、ＩＳ研究所所長）
牧野二朗（弁護士、牧野総合法律事務所）、
木村道弘（日本電気株式会社ＩＴ基盤システム開発事業部アーキテクチャ戦略主幹上席システムズアーキテクト）、
高橋　徹（インターネット戦略研究所　代表取締役会長）
下村正洋（NPO日本ネットワークセキュリティ協会事務局長、株式会社ディアイティ代表取締役社長）
中澤宣也（工学院大学常務理事・教授）

～稲田龍氏のコミュニティネットワークを引き継ぐ会～

情報セキュリティは、さまざまな組織、分野の連携があってこそ、展開することのできるものです。
本シンポジウムは、先日急逝された稲田龍氏がこの分野で尽力されていた、「コミュニティ作り」と「交流による連携」を引き継いで行くために企画しました。

稲田氏は、WIDE Projectや国内外のPKI コミュニティ、セキュリティコミュニティに広く関わり、意欲的にネットワーク作りに取り組んでいらっしゃいました。
同氏が専門としていた分野を理解し、同氏の遺したコミュニティネットワークを我々で引き継ぎ広げていくためにご参集頂ければ幸いです。

第一部: 情報セキュリティコミュニティシンポジウム

日時: 2019/11/07 17:00-18:00
場所: 慶應義塾大学日吉キャンパス協生館3F C3S02教室 **(地図 建物24番)**
参加費: 無料
講演者: 松本泰、木村泰二、砂原秀樹他

第二部: 稲田龍氏の遺したコミュニティネットワークを広げる会

日時: 2019/11/07 18:30-20:30
場所: 慶應義塾大学日吉キャンパス来往舎1F ファカルティラウンジ **(地図 建物9番)**

1984年、松本が（株）生活構造研究所に転職した際に、鈴木優一さん、高橋徹さんに出会った。1999年頃、高橋徹さんに依頼される形で、IAJセキュリティ部会に参加し、その後の業界活動につながった。
稲田さんは、1990年代に高橋徹さんと出会い、一緒にITU-Tの標準化調査を行う中で、PKIに出会ったらしい。

Backup slide

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

出典：InternetWeek2023　　2023年11月22日　　第二部：ちょっとさきのことをみんなで考える

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

出典：InternetWeek2023　2023年11月22日　第二部：ちょっとさきのことをみんなで考える

松本の現状の違和感

セコムIS研究所 Intelligent Systems Laboratory

- 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？

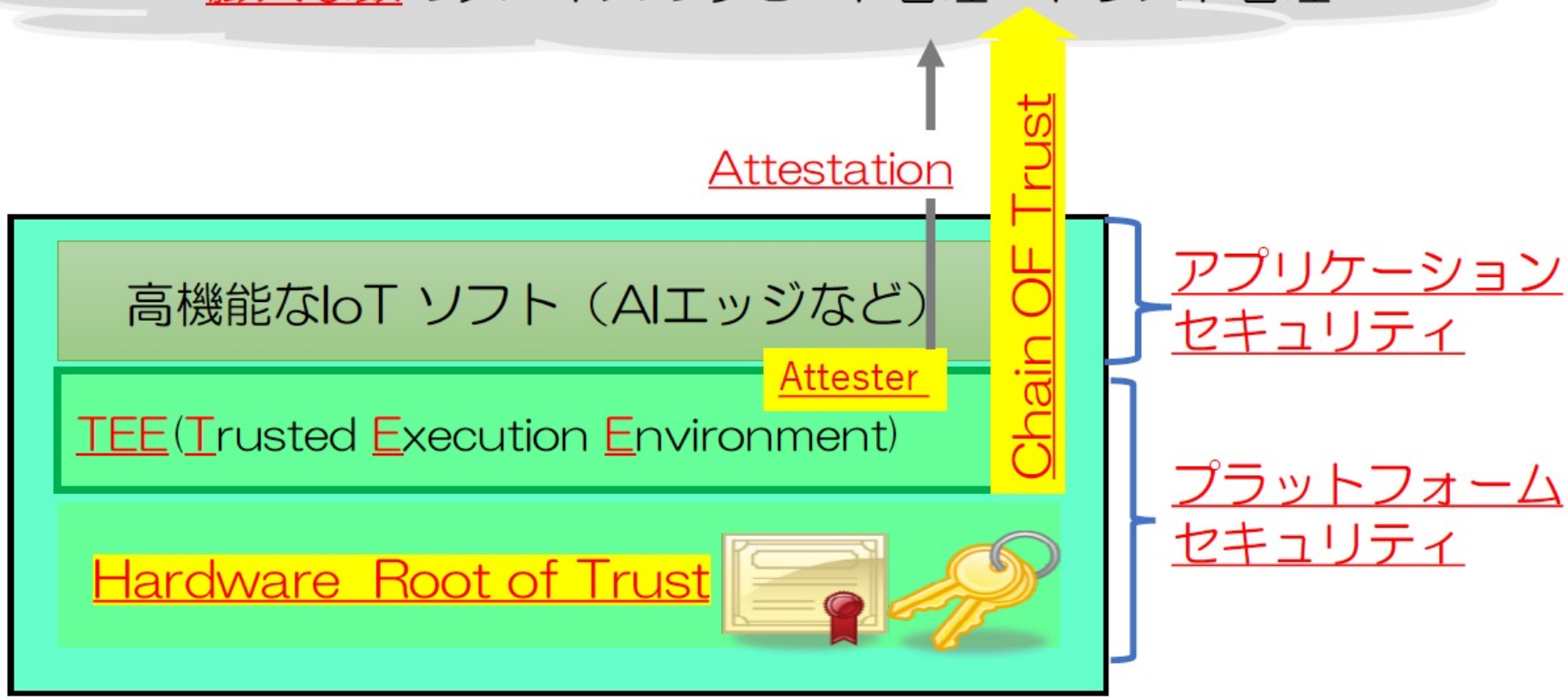
結局のところ非常に面倒なところは、誰もやりたがらない。
結果、（社会の裏の仕組みで市場を席巻する）プラットフォーマーに頼る？？

出典：InternetWeek2023　2023年11月22日　第二部：ちょっとさきのことをみんなで考える

プラットフォームセキュリティ
アプリーションセキュリティの関係
Root Of Trust, Chain Of Trust
→　　暗号技術をベースにしたトラストリレーションシップ

traceability
accountability
transparency

膨大な数のデバイスのリモート管理・トラスト管理



出典　SecurityDay2023.　Socity5.0実現にとっての(ゼロ)トラスト：
https://drive.google.com/file/d/1aQ5RYf9HrSgpJMmLu1DcOQMTvt1ejGqt/view

Always Verifyの実装となるリモートアテステーション

セコムIS研究所 Intelligent Systems Laboratory

- ゼロトラストアーキテクチャにおいては、
  - サブジェクトのtrustworthinessを、トラストエンジン・リソースがalways verifyすることにより明示的なトラストを得る（ explicit trust ）
  - → このalways verifyは、プロトコル的には、リモートアテステーション、プリミティブ的には、ほぼ、デジタル署名とその検証
- ゼロトラストアーキテクチャにおける暗黙のトラスト　→ Never trust といってるが実は、、
  - このalways verifyでは、 verifyのために信頼の起点に「暗黙のトラスト」を置くことが必要になる
  - （1）　プラットフォームに実装されるHW Root Of Trust、Chain Of Trustなど
  - （2）　ID基盤などにおけるトラストチェーンのトラストアンカーとなる公開鍵（公開鍵証明書）
- ゼロトラストアーキテクチャは、
  - 暗黙のトラストを置くに値するプラットフォームセキュリティ技術の進化が可能にした
    - → 技術的には、ゼロトラスト環境が前提のコンシューマ向けのスマフォが、技術（＋ビジネス）を確立させた
    - → もうひとつは、ゲーム機（攻撃者は、利用者）
  - → 現在、劇的な進化の途中？？。さまざまなtrustworthinessの検証が可能になりつつある？？

出典　SecurityDay2023.　Socity5.0実現にとっての(ゼロ)トラスト：
https://drive.google.com/file/d/1aQ5RYf9HrSgpJMmLu1DcOQMTvt1ejGqt/view

JNSA

欧州と日本の電子署名法と個人情報保護法の動向

- 1995年　EU データ保護指令.　Data Protection Directive 95
- 1999年　EU 電子署名指令　eSignature Directive 1999/93/EC
- 2001年　電子署名法施行
  - → 日本の電子署名法は、EU電子署名指令に大きな影響を受けた（が、そのEUの電子署名指令は、既に大きく変貌している）
- 2005年　個人情報保護法全面施行
- 2016年　EU eIDAS規則施行　→　eIDAS 規則は 49 条において 4 年毎の見直し
  - 指令（Directive）から規則（Regulation）へ。枠組み自体が大幅に変更された。
- 2017年　改正個人情報保護法施行　->　EUのGDPRとの整合が考慮された
  - 主務官庁制度から個人情報委員会へ、　4年毎の見直し
- 2018年　EU一般データ保護規則（ EU General Data Protection Regulation ）施行
  - 指令（Directive）から規則（Regulation）へ。
  - eIDAS規則と同じく、欧州の単一市場戦略(EU. Digital Single Market)の影響が大きい。
  - 相互運用性確保とその標準化の推進のためには、規則（Regulation）である必要があった？。
- 2021年　eIDAS2.0の立法提案（　eIDAS規則の改正　4 年毎の見直しによる改正）

出典：　https://www.jnsa.org/result/e-signature/seminar/2023/2023-001.pdf

標準化と法制度の関係
欧州のアプローチ?

Relationship between standardization and the legal system
European Approach??

セコムIS研究所
Intelligent Systems Laboratory

出典：社会基盤としてのPKI / PKIの10年
2010年6月29日
https://www.jnsa.org/seminar/pki-day/2010/data/5_a_matsumoto.pdf

2010年頃は、欧州においては、EUの電子署名指令の改正に向けての（eIDAS規則案に向けての）議論があった。

法制度等を前提とした技術標準へ
Toward technical standards based on the legal system

ETSI等の標準化
ETSI and other standardization

デジタル時代の法制度
Legal System in the Digital Age

デジタル技術を前提とした法制度へ
Toward a legal system based on digital technology

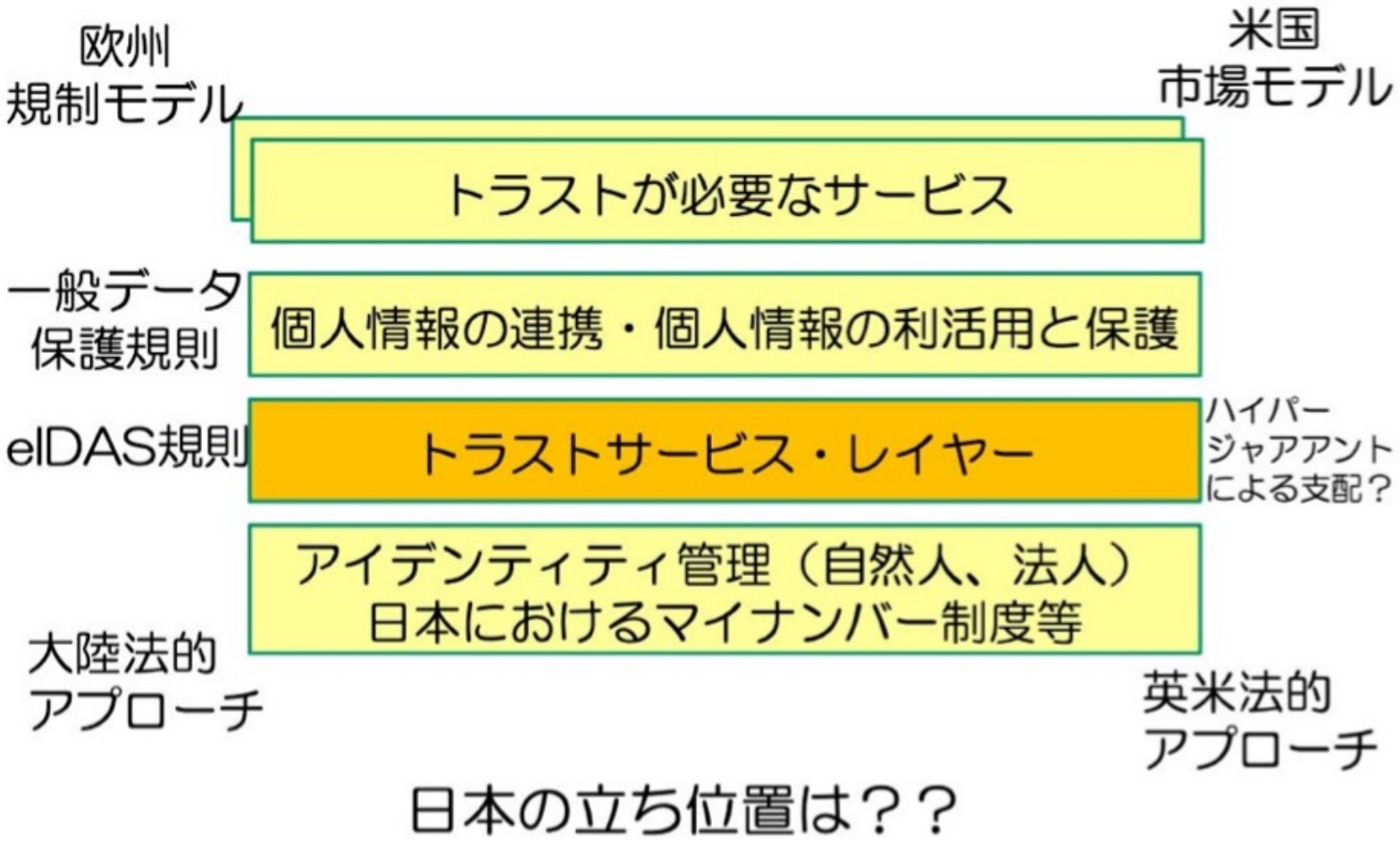
16

出典： https://www.jnsa.org/result/e-signature/seminar/2023/2023-001.pdf

欧州・米国・日本

セコムIS研究所 Intelligent Systems Laboratory

信頼される安心を、社会へ。 SECOM



11

出典：
暗号技術によるトラストの確立に向けて
2015 年　松本
http://c-faculty.chuo-u.ac.jp/~tsujii/pdf/160606matsumoto.pdf

出典：　https://www.jnsa.org/result/e-signature/seminar/2023/2023-001.pdf