信頼される安心を、社会へ。
SECOM

DXのためのデジタルトラスト実現に向けて

2021年10月15日

JNSA標準化部会 副部会長/ PKI相互運用技術WGリーダ
松本　泰　（セコム株式会社IS研究所）

JNSA 特定非営利活動法人
日本ネットワークセキュリティ協会
Japan Network Security Association

今回の開催趣旨
DXのためのデジタルトラスト実現に向けて

- デジタルトランスフォーメーション（DX）実現のためには、紙文書や押印などに依存した既存の仕組み（既存のトラストのメカニズム）もまた、デジタルを前提としたトラストの仕組み（デジタルトラスト）も変革していく必要があります。
- また、セキュリティにおいてもこれまでの境界線防御によるセキュリティからゼロトラストへの大きな変革の潮流がありますが、これはデジタル庁が掲げるデジタル改革にも重要な意味を持つと考えられます。
- 本セミナーでは、トラストサービスなどの法制度、ゼロトラストを実現するためのアイデンティティ管理、これらのベースとなるプラットフォームで実装されるトラストなどDXのためのデジタルトラストの実現に向けたあり方を議論します。

松本の講演概要　－ DXのためのデジタルトラスト実現に向けて4名の講演者の方の講演とパネルディスカションのためのイントロ

- 2011年のマイナバー制度の議論から10年、デジタル改革を掲げるデジタル庁が創設されましたが、ここではやはりマイナバー制度などを軸としたトラスト基盤のあり方が課題として浮上しています。
- 本講演では、デジタル庁が創設にあたり議論されてきた「包括的データ戦略」に盛り込まれたデジタルトラストの議論などを、JNSA標準化部会の各WGでの活動と重ね合わせ紹介します。
- また、デジタルトランスフォーメーション・デジタル改革をささえるデジタルトラストに関する本日の各講演と、パネルディスカションの意図するところを説明します。

DXのためのデジタルトラスト実現に向けて

- (1). デジタル庁とトラスト
  - データ戦略に組み込まれるデジタルトラスト
- (2). JNSA標準化部会におけるデジタルトラストに関連した活動
  - JNSA標準化部会の各WGの活動とデジタルトラストの関係
- (3). 本日のプログラムにおけるDXのためのデジタルトラスト
  - デジタルトラストトランスフォーメーション　DTX??

デジタル庁とトラスト

データ戦略に組み込まれるデジタルトラスト

出典：　デジタル庁の政策
https://www.digital.go.jp/policies

デジタル庁

ホーム › 政策

政策

政策分野

誰一人取り残さないデジタル社会の実現のため、各分野において取組を進めています。主な分野の取組状況は以下のとおりです。

1. デジタル社会に必要な共通機能の整備・普及

ID・認証

行政サービス等を効率的かつ安全・安心に提供するため、個人や法人を特定・識別し、その真正性・完全性等を保証するID・認証機能を整備します。

マイナンバー（個人番号）制度

行政手続等における特定の個人を識別するための制度です。行政機関の情報連携により、各種の行政手続における添付書類の省略などが可能となります。また、マイナンバーカードは、民間サービスでの本人確認等にも利用できます。

GビズID

行政手続等において手続を行う法人を認証するための仕組みです。1つのID・パスワードで本人確認書類なしで様々な政府・自治体の法人向けオンライン申請が可能になります。

その他認証関連制度

電子署名制度
電子委任状制度

デジタル庁の政策分野の一丁目一番地？？

１丁目??
　　デジタル社会に必要な共通機能の整備・普及
一番地??
　　ID・認証

松本の勝手な解釈

デジタル社会において必要不可欠な
デジタルトラストの確立が
デジタル庁の政策の一丁目一番地
（だと思う）

「包括的データ戦略」

包括的データ戦略

2021年6月18日に閣議決定された「デジタル社会の実現に向けた重点計画」の別紙として提出された「包括的データ戦略」　57ページの文書

主なキーワード	出現頻度
トラスト	66
セキュリティ	33
プライバシー	19
プラットフォーム	66
データ戦略	35
DFFT	13
ベース・レジストリ	50
ルール	76

トラストに関するキーワード	出現頻度
トラスト基盤	12
トラストサービス	24
トラストアンカー	11

令和３年（2021 年）６月 18 日

出典：
https://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20210618/siryou3.pdf

■昨年末にデータ戦略タスクフォースとりまとめで示された課題について実装に向けた検討項目を整理

ビジョン 現実空間とサイバー空間が高度に融合したシステム（デジタルツイン）により、新たな価値を創出する人間中心の社会

データ戦略のアーキテクチャ		第一次取りまとめ	包括的データ戦略　検討項目
人材・セキュリティ	戦略・政策	**データ戦略の理念と データ活用の原則の提唱**	・**データ活用原則** （①データがつながり、使える、②勝手に使われない、安心して使える、③みんなで協力する） ・**行政におけるデータ行動原則の構築** ①データに基づく行政(文化の醸成)、②データエコシステムの構築、③データの最大限の利
	組織（行政／民間）	**社会実装・業務改革** デジタルツインの視点で ビジネスプロセスの見直し	・**プラットフォームとしての行政が持つべき機能** ・**デジタル庁の策定する情報システムの整備方針にデータ戦略を反映**
	ルール（データガバナンス／連携ルール）	**トラストの枠組み整備** トラストの要素（意思表示の証明、発行元証明、存在証明）を整理	・**トラスト基盤の構築（認定スキームの創設）** **【デジタル庁を中心として関係省庁が協力して、2020年代早期の実装を目指す】** ・**トラスト基盤構築に向けた論点整理** （トラスト基盤の創設[各プレイヤーの役割の明確化]、認定基準、国際的な相互承認　等）
	連携基盤（ツール）	**プラットフォームの整備** 分野共通ルールの整理 分野毎のプラットフォームにおける 検討すべき項目の洗い出し (官民検討の場、ルール、ツール等)	・**データ連携に必要な共通ルールの具体化、ツール開発** ・**データ流通を促進・阻害要因を払拭するためのルールの整理** （意図しないデータ流通・利用防止のための仕組みの導入／ロックイン防止　等） 【デジタル庁と知財本部事務局は、2021年末までにガイドライン策定】 ・**重点的に取組むべき分野(健康・医療・介護、教育、防災等)のプラットフォーム構築** **【関係省庁はデジタル庁と協力して、2025年までに実装を目指す】** ・**データ取引市場のコンセプトの提示**
	データ	**ベース・レジストリの整備** **オープンデータ** **データマネジメント**	・**ベース・レジストリの指定**（法人３情報、地図情報、法律・政令・省令、支援制度　等） ・**ベース・レジストリの整備に向けた課題の抽出と解決の方向性の検討** **【デジタル庁と関係省庁は協力して、2025年までの実装を目指す】** ・**データマネジメントの強化／オープンデータの推進**
	利活用環境	**引き続き検討すべき事項** データ利活用の環境整備 民間保有データの 活用の在り方 人材／国際連携／インフラ	デジタルインフラ：・**通信インフラ（Beyond 5G）（2025年大阪・関西万博にて成果提示）、計算インフラ（富岳等コンピューティングリソースの民間利用）、半導体産業基盤の強化、データ取扱いのルール等の一体的整備** 人材・組織：・**データ戦略に必要な人材像、データ整備・AI活用を含むデータ戦略責任者の設置** セキュリティ：・**セキュリティバイデザインの推進、安全安心なサイバー空間の利用環境の構築**
	インフラ		国際展開：・**理念を共有する国との連携や様々なフォーラムにおけるDFFTの推進** （貿易、プライバシー、セキュリティ、トラスト基盤、データ利活用、次世代インフラ） ・**G７DFFTロードマップへのインプット【2023年G7日本会合を見据え成果を目指す】**

データ戦略タスクフォースで議論されてきた内容

キーワード
- トラスト
- ルール
- プラットフォーム
- ベースレジストリー

出典：
包括的データ戦略（案）の概要
https://www.kantei.go.jp/jp/singi/it2/dgov/data_strategy_tf/dai7/siryou8-1.pdf

トラストの基盤の構築

4

トラスト基盤の構築

○ 電子署名法や公的個人認証法等、個別の制度構築がなされているが、**データ社会全体を支えるトラスト基盤が必要**

○ 意思表示の証明、発行元証明、存在証明等の**トラストサービスに共通する水平横断的な一般原則と共通要件を整理し、認定スキームを創設することが必要**

○ その際、**国際的な同等性等を配慮した国際相互承認を念頭**に置いて検討する。

トラスト基盤の構築における主要な論点

①認定スキームの創設
・意思表示の証明、発行元証明、存在証明等に関するトラストサービスについて、適合性評価機関が一定の基準に基づき評価し、クオリファイドサービスとして認定するスキームを創設
・適合性評価機関は、国又は民間主導の認定機関が認定

②トラスト基盤の創設
・国又は民間主導の認定機関、適合性評価機関等の役割の明確化及びトラストサービス事業者に対する認定・監督等の一般原則と共通要件を検討

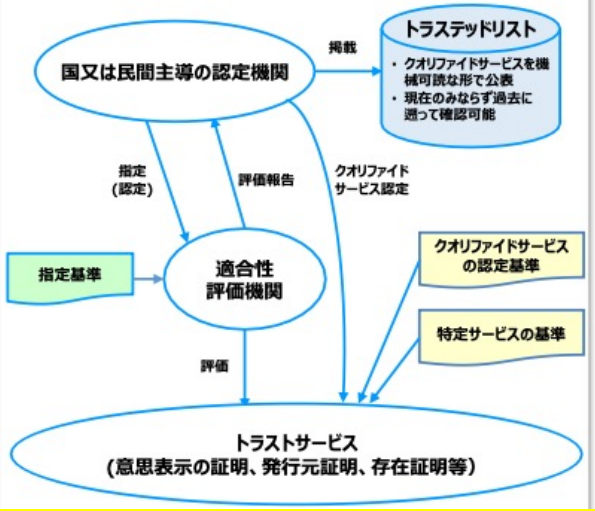
③認定の効果
・クオリファイドサービスの認定の効果、特定サービスの効果を、官民間の公的手続きにおける許容性や民民間の書類やデータの流通性等のニーズを把握した上で検討

④認定基準
・トラストサービスの共通要件、個別要件、特定サービスの基準、クオリファイドサービスの認定基準を体系化することが必要(設備基準、技術基準、運用基準等)
・適合性評価機関の指定基準について、国際的な動向を踏まえることが必要

⑤クオリファイドサービスをトラステッドリストとして公表
・認定を受けたクオリファイドサービスを機械可読な形で公表し、利用者が自動的に検証できるようにすることが必要

⑥国際的な相互承認
・国際的な相互承認を得るためには、技術基準の整合性や監督・適合性評価のレベル、国内制度の整合性等を確認することが必要

【認定スキームの想定イメージ】



データ戦略
タスクフォース・
トラストに関する
ワーキングチーム
で議論されてきた内容

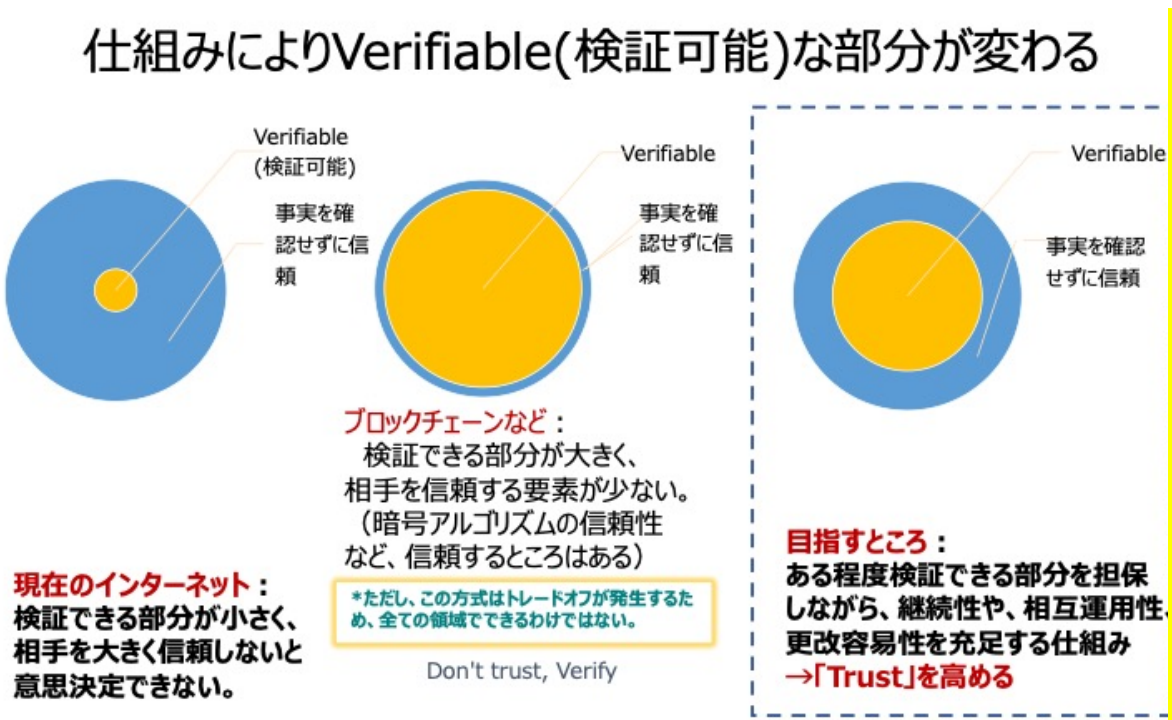
キーワード
・トラスト基盤
・トラストサービス
・トラステッドリスト

出典：
包括的データ戦略（案）の概要
https://www.kantei.go.jp/jp/singi/it2/dgov/data_strategy_tf/dai7/siryou8-1.pdf

全体として欧州のeIDAS規則を意識した議論がなされているように見受けられる
トラステッドリスト・クオリファイドサービスなどはeIDAS規則における枠組み

Trusted Web ホワイトペーパー Ver1.0

出典：https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/pdf/documents_210331-2.pdf



- Verifiable(検証可能)が、デジタルトラストに関わるキーワードとして捉えている
- ゼロトラストにおける「Never Trust, Always Verify」のAlways Verifyでは、サブジェクトがVerifiable(検証可能)である必要がある。
- Trusted Web では、DID: Decentralized Identity（分散型識別子), SSI: Self-Sovereign Identity(自己主権型アイデンティティ）に関する議論がなされている（W3Cの標準化と連動）
- 2021年6月に公表された欧州のeIDAS2.0(案)では、DID,SSIの利用が示唆されている。

内閣府 -> デジタル市場競争本部 ->. Trusted Web推進協議会
https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/index.html

JNSA標準化部会における デジタルトラストに関連した活動

- デジタルアイデンティティWG
- 日本ISMSユーザグループ
- 電子署名WG
- PKI 相互運用技術WG

JNSA 特定非営利活動法人 日本ネットワークセキュリティ協会 Japan Network Security Association

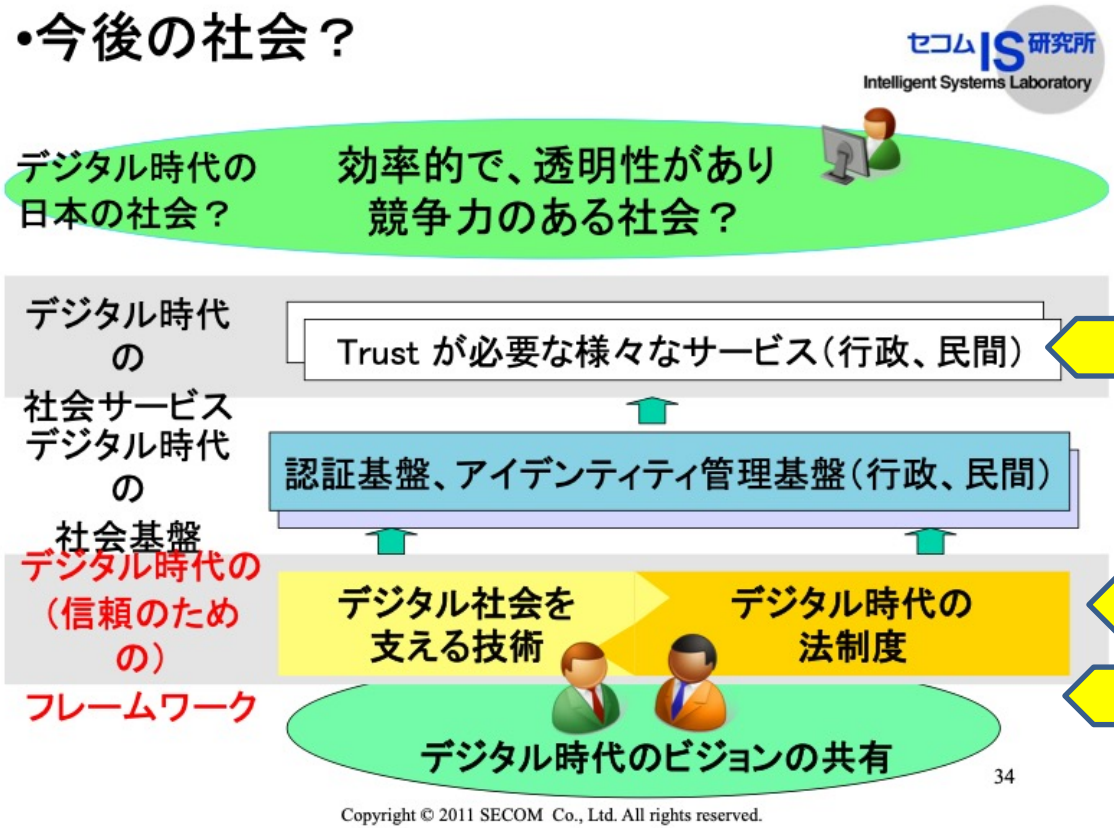
JNSA標準化部会における
デジタルトラストに関連した各WGの活動

- デジタルアイデンティティWG
  - 2021年度の予定成果物・ゼロトラスト環境におけるアイデンティティ管理（仮称）
  - -> 本日の講演者　貞弘 崇行　氏
- 日本ISMSユーザグループ
  - ゼロトラスト環境におけるISMSの構築や運用の検討を開始している
- 電子署名WG
  - データ戦略タスクフォース等で議論されているトラストサービスで利用される電子署名の標準化など
  - PKI & TRUST Days online 2021「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」に関連した議論　　日本版eIDAS規則？？？
- PKI 相互運用技術WG
  - PKI & TRUST Days online 2021「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　→　ゼロトラストのアーキテクチャ？？

特定非営利活動法人
日本ネットワークセキュリティ協会
Japan Network Security Association

2011年9月26日 に開催されたPKI Day 2011-＜番号制度時代のPKI＞ → 2021年現在のデジタル庁に関連したデジタルトラストの議論と類似する議論

出典：PKI Day 2011＜番号制度時代のPKI＞https://www.jnsa.org/seminar/pki-day/2011/data/06_matsumoto.pdf



目指すデジタル社会

サービスプラットフォーム

トラスト基盤

ルール

トラストアーキテクチャ

2011年9月26日 に開催されたPKI Day 2011-＜番号制度時代のPKI＞
→ 2021年現在のデジタル庁に関連したデジタルトラストの議論と類似する議論

出典：PKI Day 2011＜番号制度時代のPKI＞　https://www.jnsa.org/seminar/pki-day/2011/index.html

14：45
|
16：40

【パネルディスカッション】「番号制度とPKI」

MOVIE

＜モデレータ＞
セコム株式会社 IS研究所／PKI相互運用技術WGリーダー　松本 泰 氏
＜パネリスト＞
宮内　宏　氏　　宮内宏法律事務所　弁護士
手塚　悟　氏　　東京工科大学　教授
満塩尚史 氏　　経済産業省CIO補佐官
佐藤直之 氏　　日本ベリサイン株式会社　主席研究員

【講演内容】
番号制度は、国の根幹を成す制度と理解されつつあります。番号制度には、法人番号も含まれていますが、自然人、法人も含め、本格的なデジタル社会に相応しい「社会基盤としてのアイデンティティ管理」の整備への動きと捉えられるのではないでしょうか。そしてPKIの証明書は、本来「社会基盤としてのアイデンティティ管理」に基づき発行されるべきものと言えます。
パネルディスカッション「番号制度とPKI」では、「番号制度」にPKIや電子署名法等の制度が、どのように対応していくべきか等を議論します。

2021年現在　手塚　悟　氏　　トラストに関するワーキングチーム主査、データ戦略タスクフォース構成員
宮内　宏　氏　　トラストに関するワーキングチーム構成員
満塩　尚史　氏　　トラストに関するワーキングチーム構成員

出典：https://www.jnsa.org/seminar/pki-day/2021/index.html - day2

デジタル安全保障からデジタル社会保障まで
支える
トラストサービス

2021年4月16日

慶應義塾大学
手塚　悟

トラストに関するワーキングチーム
主査：手塚　悟　慶応大学教授
構成員：有識者14名、行政機関職員

パネルディスカッション　15：35-17：50（途中休憩あり）

「デジタルトラストにおける法と技術のあり方」

モデレータ：
- **松本　泰 氏**（JNSA PKI相互運用技術WGリーダ／セコム株式会社IS研究所）

パネラー：
- **手塚 悟 氏**（慶應義塾大学 環境情報学部 教授）
- **宮内 宏 氏**（宮内・水町IT法律事務所 弁護士）
- **濱口 総志 氏**（コスモス・コーポレイション取締役 ITセキュリティ部責任者）
- **宮崎 一哉 氏**（JNSA電子署名WGリーダー／三菱電機株式会社）
- **宮地 直人 氏**（電子署名WGサブリーダー／有限会社ラング・エッジ）
- **山内 徹 氏**（一般財団法人日本情報経済社会推進協会（JIPDEC）常務理事）

手塚悟氏、宮内宏氏、濱口総志氏、山内徹氏は、「データ戦略タスクフォース・トラストに関するワーキングチーム」構成員
濱口 総志氏は、本日の講演者、JNSA電子署名WGメンバー

PKI & TRUST Days online 2021　第２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

出典：https://www.jnsa.org/seminar/pki-day/2021/index.html - day1

デジタルトラストアーキテクチャの要素技術をベースにトラストが構築されつつある
ゼロトラストネットワークとConfidential Computing

講演２
デジタルトラストとゼロトラストネットワーク
鈴木 研吾 氏（株式会社 LayerX シニアセキュリティアーキテクト）

講演３
Confidential Computing の技術動向
奥田 哲矢 氏（NTTセキュアプラットフォーム研究所 研究主任）

講演１　トラストを確立する技術の概要
HW Root OF Trust
セキュアーブート
セキュアエンクレーブ・TEE
リモートアテステーション
宮澤 慎一 氏（セコム株式会社 IS研究所 主務研究員）

講演４
プラットフォームで実装されるトラスト

プラットフォームに組み込まれて行くデジタルトラストアーキテクチャ

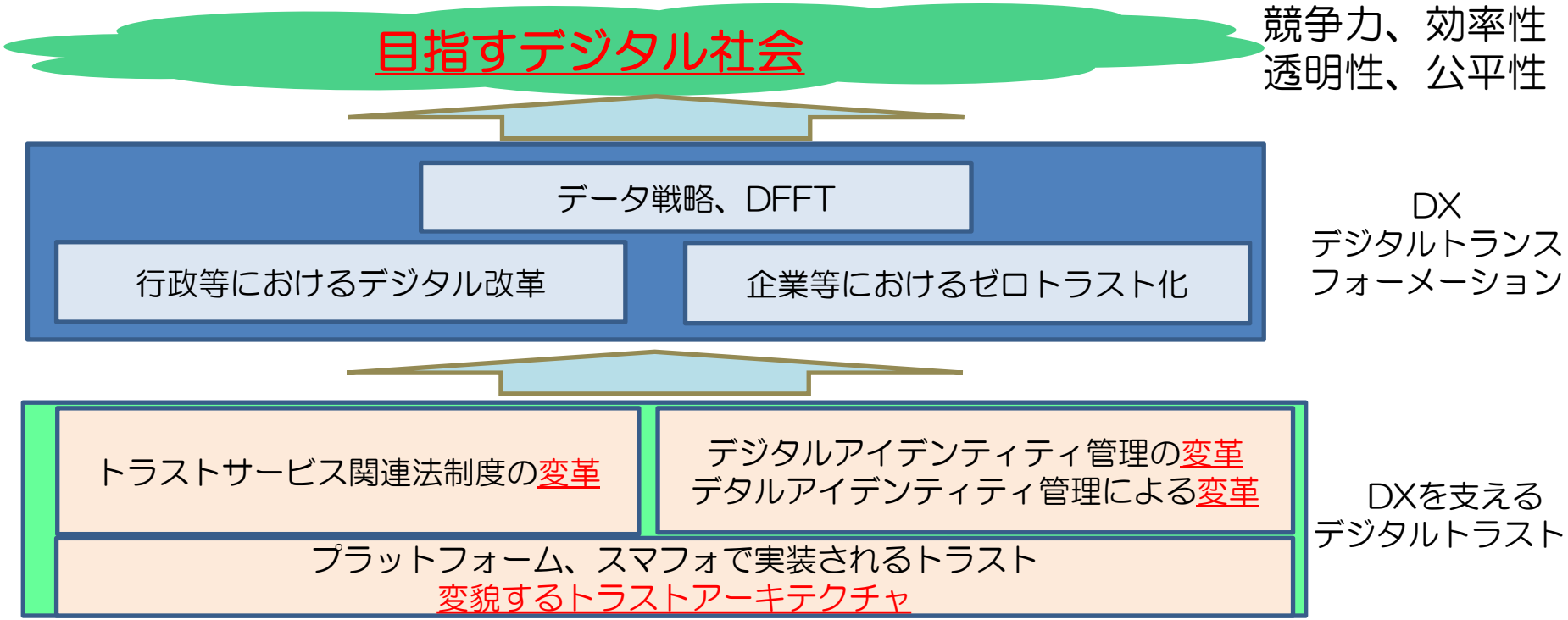
垣内 由梨香 氏
（Microsoft Corporation セキュリティ レスポンスチーム セキュリティ プログラム マネージャー）

「デジタルトラストに対応するコンピュータアーキテクチャの変化」
コンピュータアーキテクチャ自体に暗号技術（主に公開鍵暗号技術）が取り込まれて行く
→　デジタル・トラストアーキテクチャ

講演４の垣内 由梨香 氏は、本日の講演者

DXのためのデジタルトラスト

デジタルトラストトランスフォーメーション　DTX？



デジタルトラストトランスフォーメーション　DTX？

DXを成功させるためには、トラストの仕組み自体に、
トランスフォメーション（改革）が必要

- トラスト　－　社会的な複雑性の縮減メカニズム　（　by ニクラス・ルーマン　）
  - これまでの社会における既存のトラストのメカニズムの存在
  - -> 水や空気と同じく、普通に存在する。なので普段意識することは少ない
- トラストのパラダイムシフト
  - DX(デジタルトランスフォーメーション）は、（良くも悪くも）既存のトラストの仕組み（多くは、既存の法制度、慣習が作り出しているトラスト）を破壊する
  - ゼロトラスト、トラストレス　--　トラストのパラダイムシフト
    - 「何もトラストしない」「トラストがない」ではない。
    - ゼロ、レス　　→　既存のトラストのメカニズムではない
    - →　新たなトラストのメカニズム（デジタルトラスト）という側面

紙の歴史　－紙という技術が起こしたイノベーションとトラストの関係？

- 中国
  - 竹簡
  - 紙　　紙の発明は、紀元前2世紀頃。西暦105年頃に実用的な製紙法
- 西洋、イスラム圏
  - パピルス→羊皮紙→紙
  - 羊皮紙から紙へ
    - タラス河畔の戦い（751年）
- 羊皮紙
  - 1000年程度の保存が可能、高価
  - インクが染み込みにくいので、書き損じは削って直せるという利点があり、そのため公文書などが改竄されることもしばしばあった。
  - 参考　https://ja.wikipedia.org/wiki/羊皮紙

- 紙、押印、手書き署名、封印(Seal)などがトラストにどのような役割を果たしてきたのか？
- ハンコ不要と言われている昨今、ハンコの果たしてきた役割は？？？
- Soceity5.0，第4次産業革命におけるトラストの形は、どうあるべきなのか？？？

2011年のPKI Day 2011-<番号制度時代のPKI>
10年前からの変化　→　本日の重要な論点

- DXへの風、デジタル庁への期待
  - マイナンバー制度も含めた法制度も含めた見直しの機運
  - PKI & TRUST Days online 2021　2021年4月16日（金）「デジタルトラストにおける法と技術のあり方」
- ゼロトラストへのパラダイムシフト　→　トラストのパラダイムシフト
  - Never Trust, Always Verify
    - Verifiable(検証可能)なサブジェクト（主体者：人やモノやサービス）
      - 場所、属性、資格、権限、信頼性、etc….
  - →　デジタルトラストトランスフォーメーション
- プラットフォーム、スマートデバイス・エッジデバイスなどの進化
  - PKI & TRUST Days online 2021　第2日目：2021年4月15日（木）「変貌するトラストアーキテクチャ」

DXのためのデジタルトラストの実現に向けて

信頼される安心を、社会へ。
SECOM

- プラットフォームで実装されるトラスト
  - 垣内 由梨香 氏 （Microsoft Corporation セキュリティ レスポンスチームセキュリティ プログラム マネージャー）
- トラスト・プラットフォーム視点からのスマートフォン
  - 磯部 光平 氏（セコム株式会社 IS研究所）
- ゼロトラストにおけるID管理の役割　ートラストアンカーの一つとしてー
  - 貞弘 崇行 氏（株式会社アイピーキューブ）
- eIDAS規則の改正案“eIDAS 2.0”におけるEU Digital Identity Wallet
  - 濱口 総志 氏（コスモス・コーポレイション取締役 ITセキュリティ部責任者）

パネルディスカション
デジタルトラスト実現に向けての課題は何か？

- 企業におけるデジタルトラスト化
- Soceity5.0社会におけるトラスト

パネルディスカション
デジタルトラスト実現に向けての課題は何か？

- パネルディスカション「デジタルトラスト実現に向けての課題は何か？」では、「企業におけるデジタルトラスト化」「Soceity5.0社会におけるトラスト」のふたつのテーマを取り上げます。
- 前者では、企業のゼロトラスト化においてALWAYS VERIFYは、どのように実装されていくのか。ALWAYS VERIFYのためのアイデンティティ管理や、VERIFY可能なエッジデバイスのセキュリティはどのように進化していくのか。また、その課題は何かなどを議論します。
- 後者では、様々な社会課題を解決するためのアイデンティティ管理、クレデンシャル管理におけるスマートフォンなどのエッジデバイスの利用などにおいて、どういった技術的課題、法制度的課題があるのかを議論します。

企業におけるデジタルトラスト化　Always Verify
→ 企業におけるデジタルトラストへのパラダイムシフト

信頼される安心を、社会へ。
SECOM

Trusted Party
被信頼者

アイデンティティ管理＋デバイス管理

ZeroTrust Environment??

ゼロトラスト環境における
アイデンティティ管理

アイデンティティ管理
＋デバイス管理？？

サブジェクト

ユーザ

認証

ユーザ（ローカル）認証
認証レベル(LoA)、認証の

Attester

TEE（Trusted Execution Environment）

デバイス

検証

デバイスアテステーション
デバイスの確からしさ、デバイ

Attester

アプリケーション

監視

アプリケーション監視
アプリケーションの振る舞い、

Attester

Always Verify

リモートアテステーション

トラストエンジン
PDP：
Policy Decision Point

Relying Party(RP)
信頼者・検証者

リソース

OS

Chain Of Trust

トラステッドOS

(ユーザ所有の)
デバイス

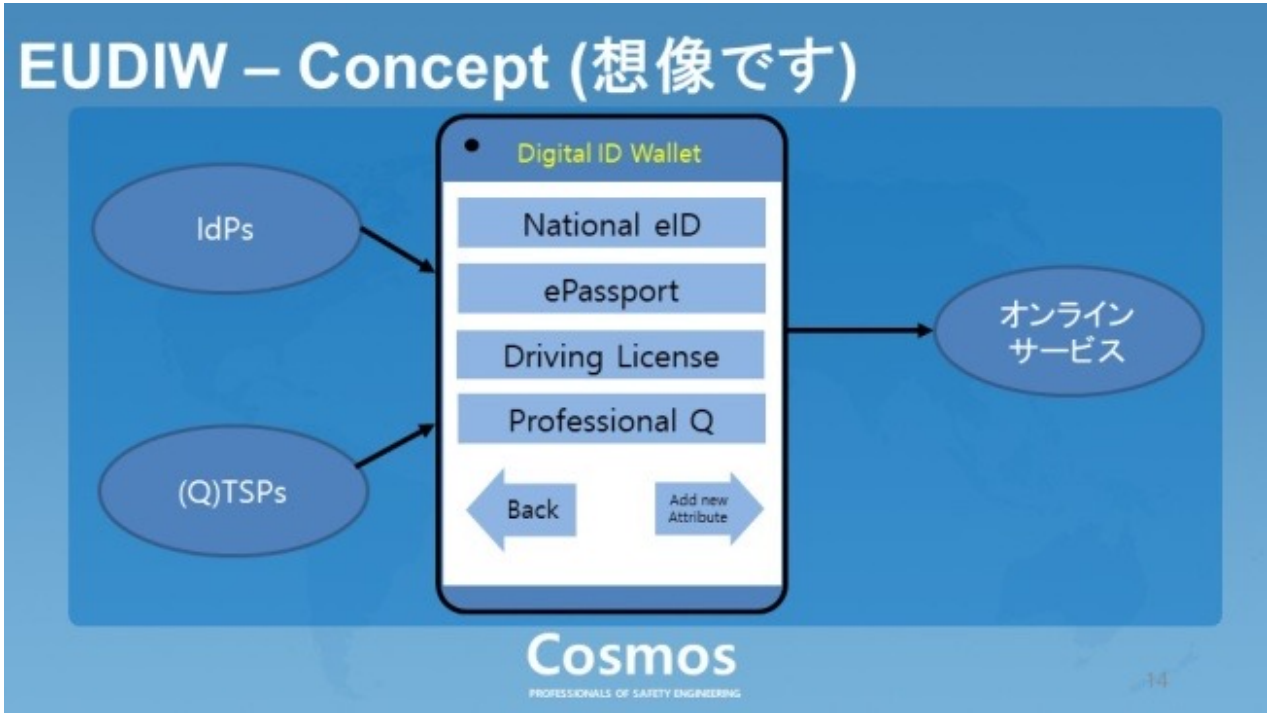
HWRoT・セキュア・エンクレーブ
耐タンパー、Cryptographic Boundary

ゼロトラスト環境における
ISMSの構築や運用

「ゼロトラスト環境におけるトラステッド・エッジ」

Soceity5.0社会におけるトラスト
マルチステークホルダー間のトラスト

- マルチステークホルダーで社会課題を解決するためのアイデンティティ管理
- スマートフォンなどのエッジデバイスにおけるクレデンシャル管理のあり方



出典：
eIDAS2.0 – eIDAS規則の改正案の解説
https://www.jipdec.or.jp/library/report/20210713-3.html

参考スライド

- 変貌するトラストアーキテクチャ
- Soceity5.0社会におけるデジタルトラスト

変貌するトラストアーキテクチャ

- 様々なエンティティの信頼性（Trustworthiness）が、 リモートからVerifiableになるアーキテクチャ
    - 様々なエンティティに組み込まれる Verifiable Credentials
- always verify　→ 実行時のverify　→ リモートアテステーション

デジタル社会におけるトラスト　そのための技術

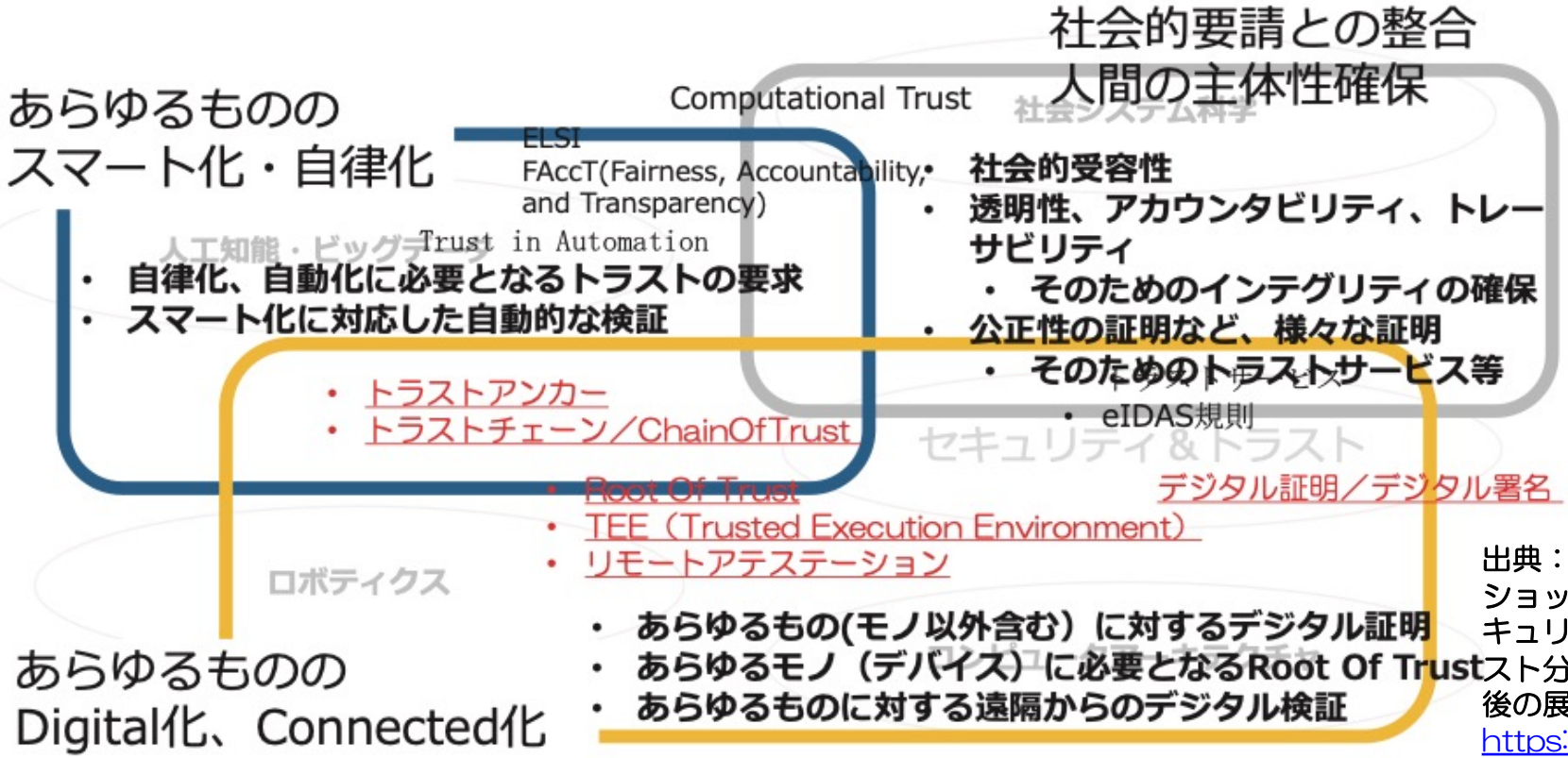
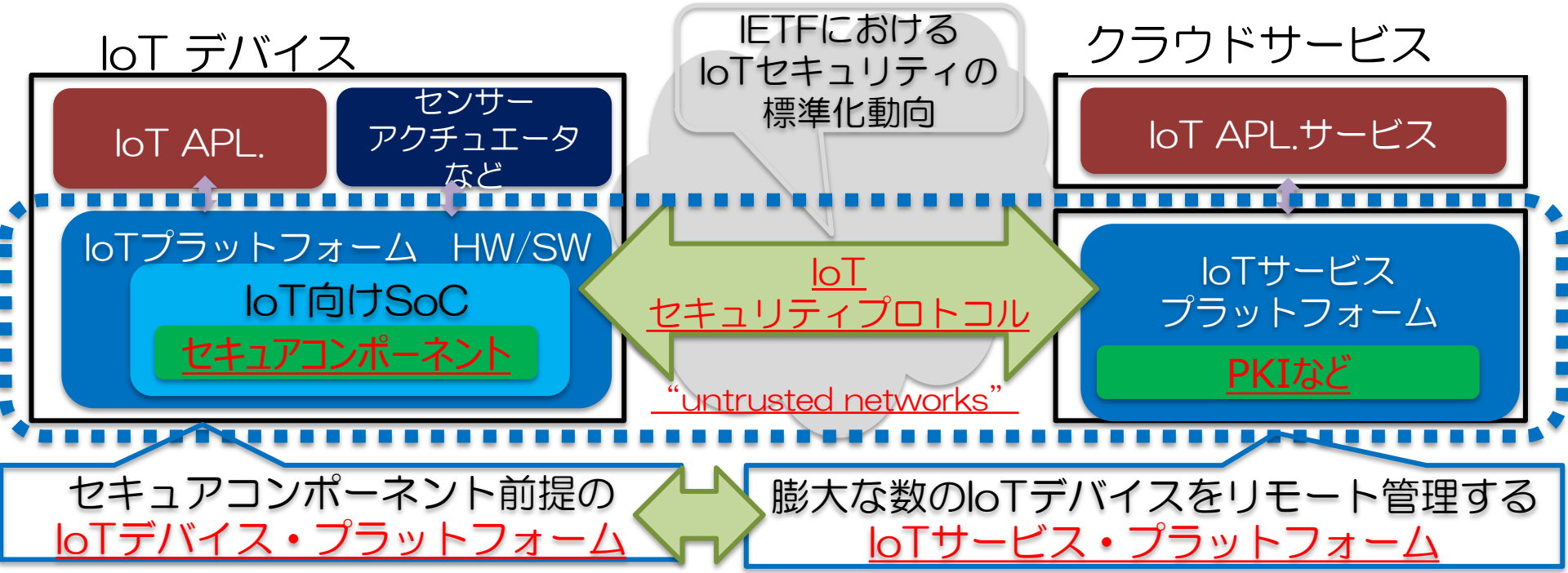


図2-5-7　　システム・情報科学技術分野におけるトラストの整理例

出典：　俯瞰ワークショップ報告書：セキュリティー・トラスト分野の動向と今後の展望
https://www.jst.go.jp/crds/pdf/2021/WR/CRDS-FY2021-WR-02.pdf

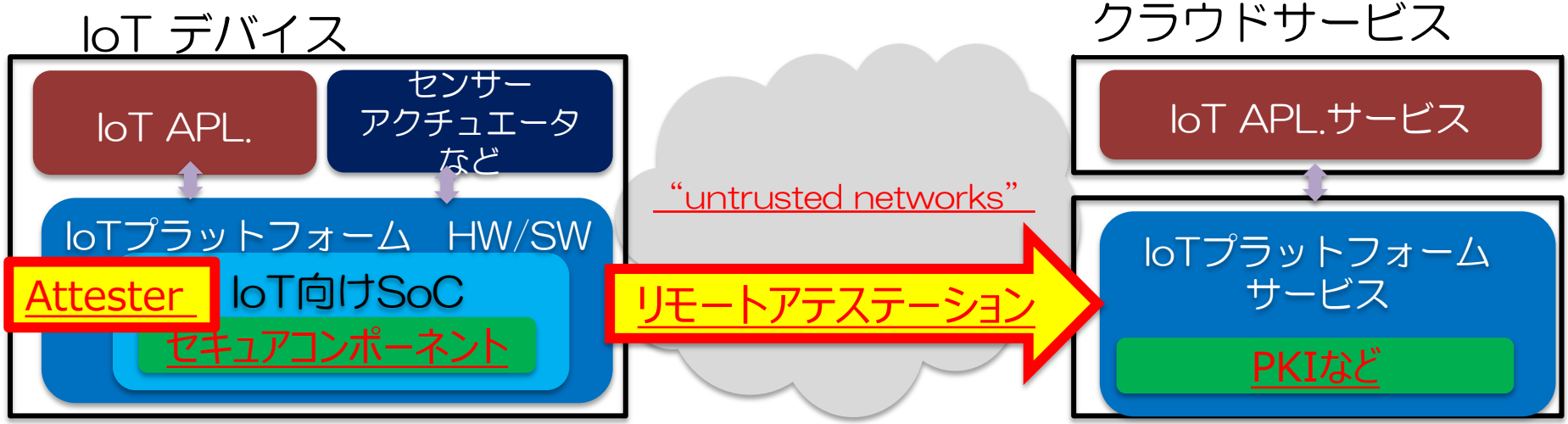
IETFにおけるIoTセキュリティの標準化動向に見る デジタルトラストへのパラダイムシフトと変貌するトラストアーキテクチャ



リモートアテステーション
IETF Remote ATtestation ProcedureS (rats)WG

https://datatracker.ietf.org/wg/rats/about/

- 変貌するトラストアーキテクチャが
  - 高信頼実行環境TEE(Trusted Execution Environment）などのIoTデバイス・環境への搭載
  - 従来からの「デバイスの識別・認証」
  - IoTデバイスの利用時における様々な信頼性（trustworthiness）の証明



リモート認証(Authentication)ではなくリモートアテステーションの要求
リモートのターゲットが「意図通り」動いているのか？

- On the Internet, Nobody Knows You're a Dog
- 「インターネットでは、実はキミが犬だって事を誰も知らないのさ」
- 1993年7月5日　米国の雑誌『The New Yorker』

２０２１年現在の課題
あんた（TP:Trusted Party）が犬でないことは分かったし、あんたが、私（RP: Relying Party）が信頼しているAさんであることも分かった。
けど、あんたのスマフォ（TP）は、大丈夫なの。乗っ取られているよみたいよ。

出典　https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog

企業におけるデジタルトラスト化　Always Verify
→ 企業におけるデジタルトラストへのパラダイムシフト

信頼される安心を、社会へ。
SECOM

Trusted Party
被信頼者

アイデンティティ管理＋デバイス管理

ZeroTrust Environment??

ゼロトラスト環境における
アイデンティティ管理

アイデンティティ管理
＋デバイス管理？？

サブジェクト

ユーザ

認証

ユーザ（ローカル）認証
認証レベル(LoA)、認証の

Attester

TEE（Trusted Execution Environment）

デバイス

検証

デバイスアテステーション
デバイスの確からしさ、デバイ

Attester

アプリケーション

監視

アプリケーション監視
アプリケーションの振る舞い、

Attester

Always Verify

リモートアテステーション

トラストエンジン
PDP：
Policy Decision Point

Relying Party(RP)
信頼者・検証者

リソース

OS

Chain Of Trust

トラステッドOS

(ユーザ所有の)
デバイス

HWRoT・セキュア・エンクレーブ
耐タンパー、Cryptographic Boundary

ゼロトラスト環境における
ISMSの構築や運用

「ゼロトラスト環境におけるトラステッド・エッジ」

デジタルトラストのための法と技術の整合

欧州と日本の電子署名法と個人情報保護法の動向

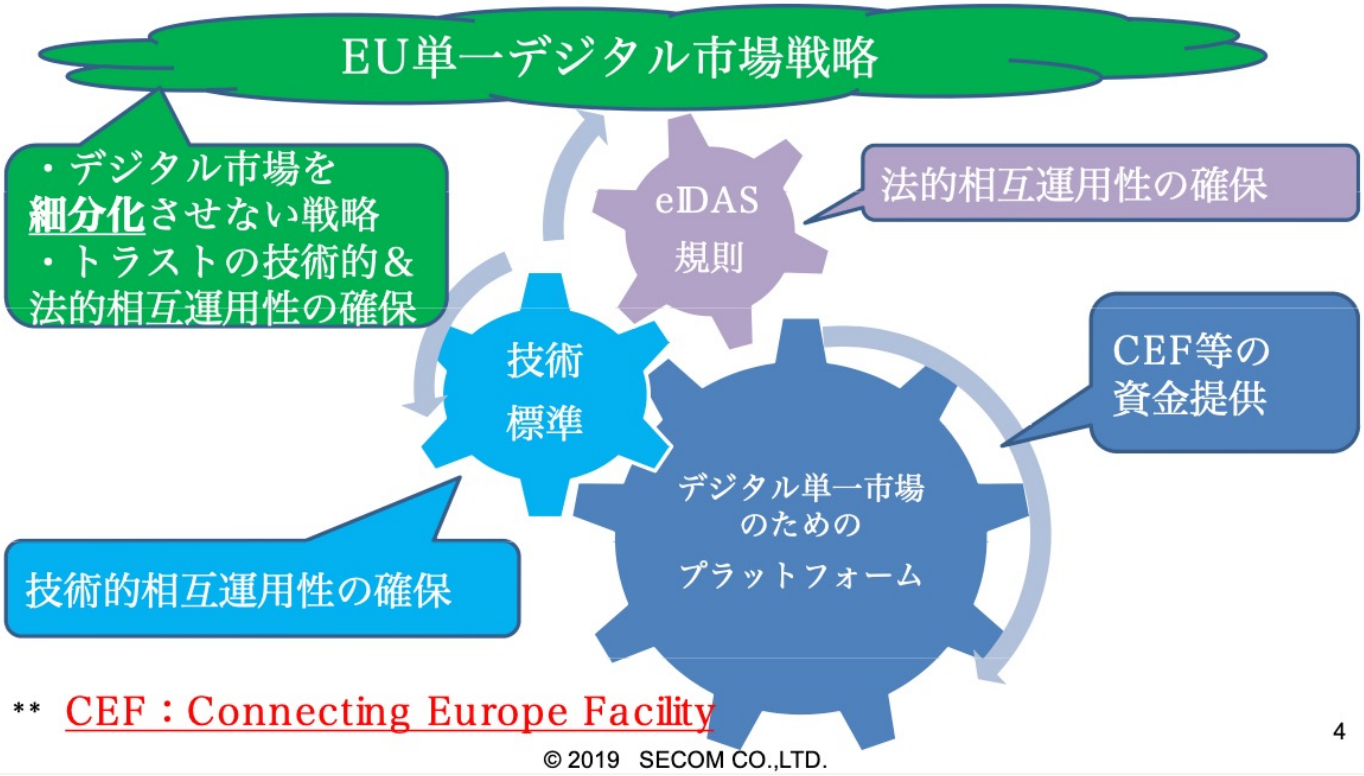
既存の仕組みの電子化のための電子署名法からDXのための電子署名法へ

→　より法と技術の整合が求められる。

- 1995年　EUのデータ保護指令
- 1999年　EUの電子署名指令
- 2001年　電子署名法施行
  - →　日本の電子署名法は、 EUの電子署名指令に大きな影響を受けた
- 2005年　個人情報保護法全面施行
- 2016年　EU eIDAS規則施行
  - 指令から規則へ。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
  - 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施行（GDPR）
  - 指令から規則へ。eIDAS規則と同じく、欧州の単一市場戦略の影響が大きい。
- 2021年　デジタル庁設立、20年ぶりの電子署名法の議論？？
- 202x年　電子署名法の未来？、欧州のeIDAS2.0

欧州のeIDAS規則

ＥＵの技術標準とデジタルプラットフォームの関係



** CEF：Connecting Europe Facility

4

出典：
2019年　トラストサービスの調査ワークショップ
EUの技術標準（松本）
https://itresearchart.securesite.jp/19ws207/docs/s03.pdf

欧州のeIDAS規則によるトラストサービス

出典：　https://www.eema.org/wp-content/uploads/entschew-fiedler.pdf

9

出典：
2019年　トラストサービスの調査ワークショップ
EUの技術標準（松本）
https://itresearchart.securesite.jp/19ws207/docs/s03.pdf

技術的観点、標準化、相互運用性の観点からは、「自然人による署名」が単独で存在しているわけではなく、他と深く連携している。

出典：
デジタル改革関連法案ワーキンググループ作業部会 とりまとめ
令和2年11月20日 デジタル改革関連法案ワーキンググループ作業部会
https://www.kantei.go.jp/jp/singi/it2/dgov/houan_wg/dai4/siryou2.pdf

8．個人・法人に係るＩＤ・認証・電子署名等のスキーム

個人・法人に係るID・認証・電子署名等のスキーム

- 個人・法人を一意に特定するものであって、行政機関等が保有する社会の基本情報が容易に参照され、活用されるための機能
- 情報の発信者の真正性や、情報そのものの真正性、完全性等を保証するための機能

	ID	認証	電子署名等			
個人	○ マイナンバー法 （マイナンバー）	○ 公的個人認証法 （電子利用者証明）	○ 電子署名法 （電子署名） 公的個人認証法 （電子署名）	ー	○ 電子委任状法	ー （タイムスタンプ） ※文書作成時刻の署名
所管府省	総務省 ※ＪＬＩＳ	総務省 ※ＪＬＩＳ	総務省、法務省、経産省 総務省 ※ＪＬＩＳ	－	総務省、経産省	－
法人	○ マイナンバー法 （法人番号）	○ （GビズＩＤ） ※法人以外に、個人事業主も含む	○ 商業登記法 （法人代表者の電子証明書）	ー （eシール） ※法人の電子証明書	○ 電子委任状法	ー （タイムスタンプ） ※文書作成時刻の署名
所管府省	国税庁	経産省	法務省	－	総務省、経産省	－

48

- 制度的なパズルのピースは、それなりに揃っているように見えるかもしれない。
- しかし、技術の観点からは、技術としての整合性、相互運用性が決定的に欠ける。
- その原因は、ボトムアップに作られてきた制度にある。
- 欧州においては、これらはeIDASに統合されている。