デジタルトラストの概念と動向

2025年10月23日

JNSA フェロー　松本　泰

デジタルトラストの最新動向と展望

- 社会のデジタル化が急速に進展するなか「デジタルトラスト」の重要性が一層高まっています。
- JNSA標準化部会では、従来からデジタルトラストを支える電子署名、デジタルアイデンティティ、PKI（公開鍵基盤）の分野で活動を行ってきました。
- これらの分野では近年、属性証明（Electronic Attestation of Attributes）、リモートアテステーション、Verifiable Credentials（VC） といった新たな技術要素が急速に注目されており、これらの国際標準化は「信頼の対象（Trustee）の信頼性（trustworthiness）の証明」を重視する方向に進んでいます。
- これらは、デジタルアイデンティティウォレットやデータスペースにおける相互運用性、ならびに耐量子計算機暗号（PQC）への移行といった要素と連携しながら、次世代のデジタルトラスト基盤およびトラストフレームワークの構築を促進しています。
- 今回のセミナーでは、標準化部会の関連のワーキンググループ（WG）が、それぞれの専門分野から最新の技術動向と標準化の課題を紹介します。また、日本政府（デジタル庁）によるデジタルトラスト政策・制度設計の現状についても解説いただきます。
- 最後に、講演者を交えたパネルディスカッションを通じて、今後のデジタルトラストの方向性や国際標準化への対応、日本における展開と役割の展望について議論します。

本日のセミナーで説明したい ＆議論したいキーワード

- 「デジタルトラストの概念と動向」（デジタルトラストの概念と目指すデジタル社会）→　【講演１】で説明
  - （旧来からの）トラスト
    - 暗黙のトラスト(Implicit Trust)
      - 一般的な（人主にの関係の）関係におけるトラストの理解　→　だが、本日のデジタルトラストの範囲外
    - 明示的なトラスト（explicit trust）：　明示的に根拠が提示されるトラスト
      - 過去には、物理的・社会的証明が中心。旧来から存在する制度的トラスト（Institutional Trust）などにより実現（旧来は比較的静的なトラスト）
  - デジタルトラスト　＃ここでは、デジタル社会における明示的なトラスト（explicit trust）として捉える
    - 技術的トラスト（Technical Trust）と制度的トラスト（Institutional Trust）などにより実現
    - 現在のトレンドとして、リアルタイムに（動的に）、属性の検証が可能へ　→　動的なトラスト
      - ベイファアブルトラスト（Verifiable Trust）　→　ゼロトラストのalways verify
      - 様々な属性証明が鍵　->　この辺りが本日のテーマ
    - ToBeとしてデジタル社会を変革するリアルタイムな信頼性証明（属性証明）という方向性
- どのように実現するのか？そのための最新の標準化、主に技術的トラスト（Technical Trust）のキーワード
  - 属性証明（Electronic Attestation of Attributes）など　→　【講演2】で説明
  - Verifiable Credentials（VC）など　→　【講演3】で説明
  - リモートアテステーションなど　→　【講演4】で説明

デジタルトラストの概念と動向

- （1）　トラスト＆デジタルトラストと関連するキーワード
- （2）　目指すデジタル社会
  - デジタルトラストで実現される世界観・デジタルトラストのToBe
- （3）　JNSA標準化部会の活動との関係
- （4）　まとめ　デジタルトラストの方向性
- 参考資料

トラスト＆デジタルトラストと関連するキーワード

- トラストの対象　Trustee
- トラストする側　Trustor、Relying Party（RP)
- Trust and　Trustworthiness　（TrustとTrustworthinessの区別）
- 暗黙的なトラスト(Implicit Trust)
- 明示的なトラスト（Explicit Trust）
- 制度的トラスト（Institutional Trust）
- 技術的トラスト（Technical Trust）

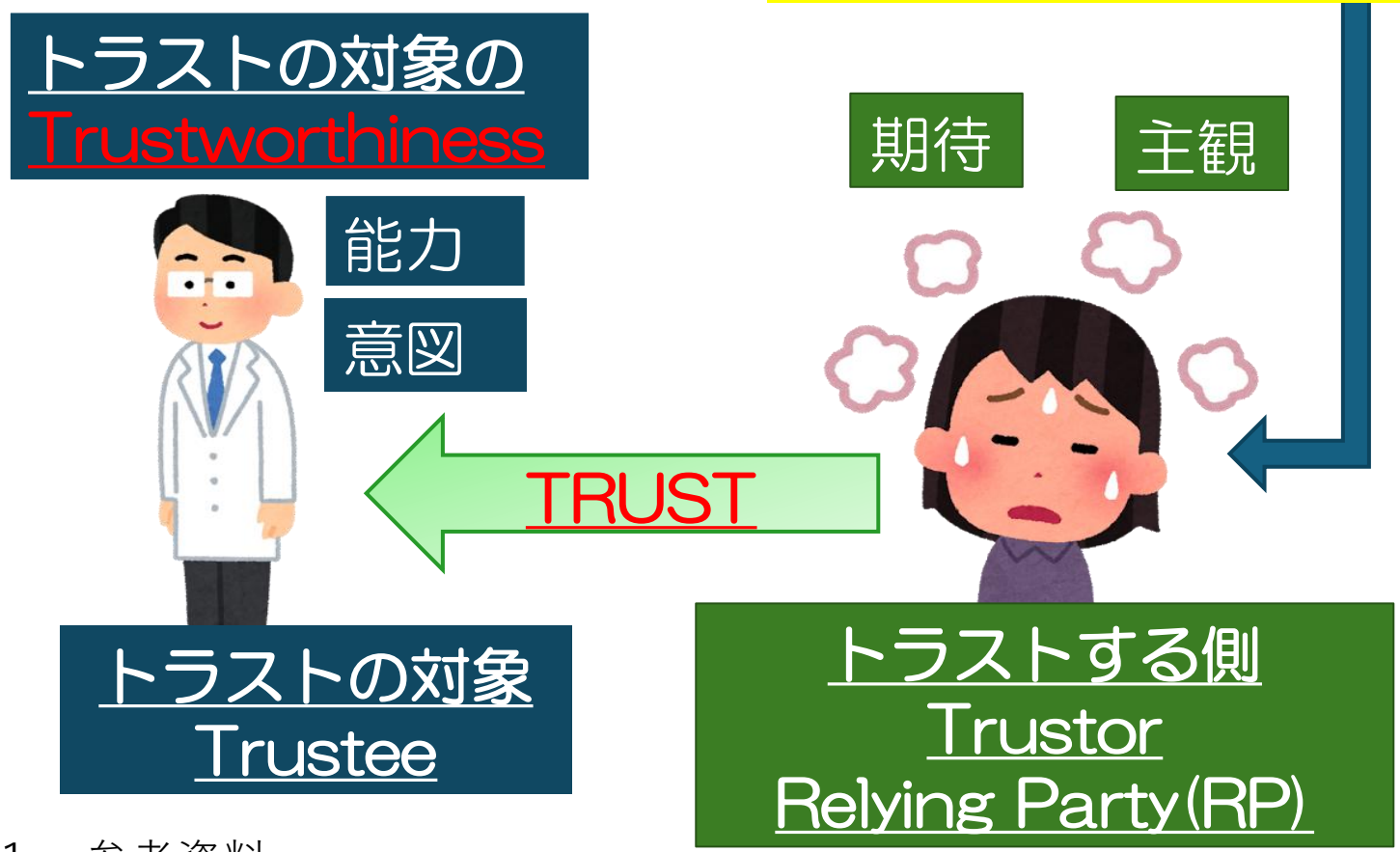
基本的な用語の理解　TrustとTrustworthiness　の区別

- トラストの対象
  - Trustee
- トラストする側
  - Trustor、Relying Party（RP）
- Trustworthiness（信頼性）
  - Trustee の品質・性質・能力など
  - シンプルに Trustee の属性（Attribute）と捉える
    - ＃属性証明との関係の説明ため
- トラスト（Trust）
  - トラストは、 Trusteeの何かが、Trustorへ伝わるメカニズムと捉える（その上でのTrustorの判断）
- 心理学などにおけるトラスト
  - Trusteeの意図（Intentional）により注目している。Trustorの期待、主観（認知バイアスとも言う？）

医療の信頼(Trust)と信頼性（trustworthiness） を支える制度等

・医師資格という国家資格
・医師免許証という医師資格の証明
・医療機関の認可制度（開設許可）

社会的な複雑性の縮減メカニズム(*1)でもある制度的トラストのフレームワーク



＊1　参考資料

JST RISTEX　デジタルソーシャルトラスト　https://www.jst.go.jp/ristex/digist/
「デジタル社会におけるトラストのほころび」に対する課題特定、課題解決

Trusteeの分野、種類などによる分類

Trusteeの信頼性（trustworthiness）の評価、向上などの研究

Trustorの認知バイアスが働きやすい、暗黙のトラストこの認知バイアスの研究

Trustorの分野、種類などによる分類

Trustorのリテラシーの向上、教育などの研究

より主観的

より暗黙的

信頼性（trustworthiness）

暗黙のトラスト(Implicit Trust)

期待

主観

品質、

仲介者

現代社会における、トラストに起因する様々な問題の多くは、Trusteeの信頼性（trustworthiness）が、Trustorからのトラストに繋がらない。さらに、この不一致からくる不信（distrust）から生じていることが多い。
→　明示的なトラスト（explicit trust）は、これら解決の方向性の一つ

トラストメカニズムの研究？

Trustee
トラストの対象

Trustor
Relying Party(RP)

より明示的

明示的なトラスト（explicit trust）

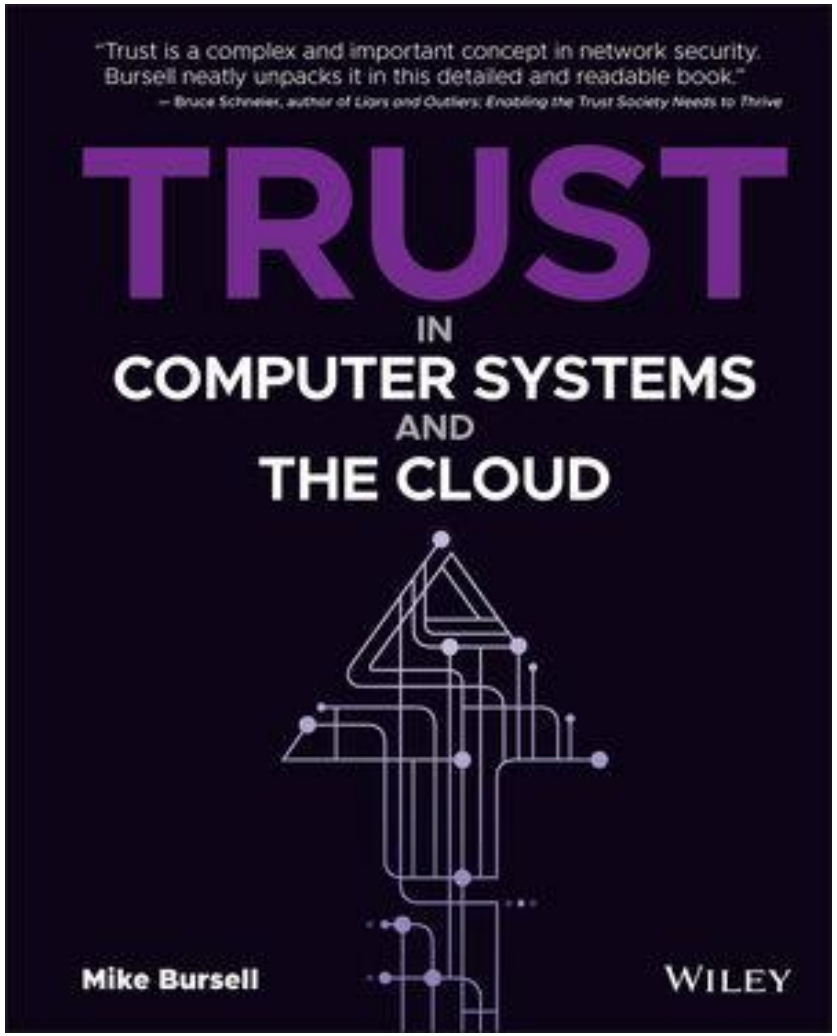
様々なステークホルダーを俯瞰した上での制度設計に関する研究

Trusteeの信頼性（trustworthiness）の検証が可能な（トラスト）メカニズムの研究

デジタルソーシャルキャピタルを支えるデジタルトラストの研究

より客観的

デジタルトラストの一つの考え方・トラストの対象（Trustee）が複雑なシステム
コンピュータシステムとクラウドにおけるトラスト →　過去にはないトラストの形態



- 著者のマイク・バーセル氏は、
  - コンフィデンシャルコンピューティングなどのアーキテクト
  - コンフィデンシャルコンピューティングは、機密性（confidentiality）などをリモートから検証可能
    - これが明示的なトラスト（explicit trust）であり、技術的トラスト（Technical Trust）により実現。
- マイク・バーセル氏は、「ゼロトラスト（ Never trust, always verify ）」は、「“explicit trust”明示的なトラスト」と呼ばれる方が良いと主張している（*1）。
  - →　ゼロトラストは、Zero　implicit trust
- 結論？？
  - ゼロトラストは、技術的トラスト（Technical Trust）による明示的なトラスト（explicit trust）でありデジタルトラスト

従来からのトラスト研究では、（人が大前提で）手間がかかる確認（検証）を行わないで判断することを 「トラスト」としていた側面がある。なので、用語の混乱がある？？？

•Trust in Computer Systems and the Cloud、2021　https://www.wiley.com/en-us/Trust+in+Computer+Systems+and+the+Cloud-p-9781119692324

*1　Zero trust and Confidential Computing https://aliceevebob.com/page/2/

Consolidated report on the socio-economic basis for trust and trustworthiness.
トラスト(Trust)と信頼性（ trustworthiness）のための社会経済的基盤に関する統合報告書
2015年　　欧州のFP7のプロジェクトの成果物

- OPTET（Operational Trustworthiness Enabling Technologies）の目的
  - 「社会的・経済的にトラストできるICTシステムを実現するため、トラスト（Trust）と信頼性（trustworthiness）を定量的かつ操作可能にする技術を開発する」
- 本報告書は、OPTET (Project FP7-ICT-2011-8) における「信頼（Trust）」と「信頼性（Trustworthiness）」の社会経済的基盤を整理した最終成果であり、両概念を統合的にモデル化し、設計・運用の全ライフサイクルでトラストを扱う方法を示している。

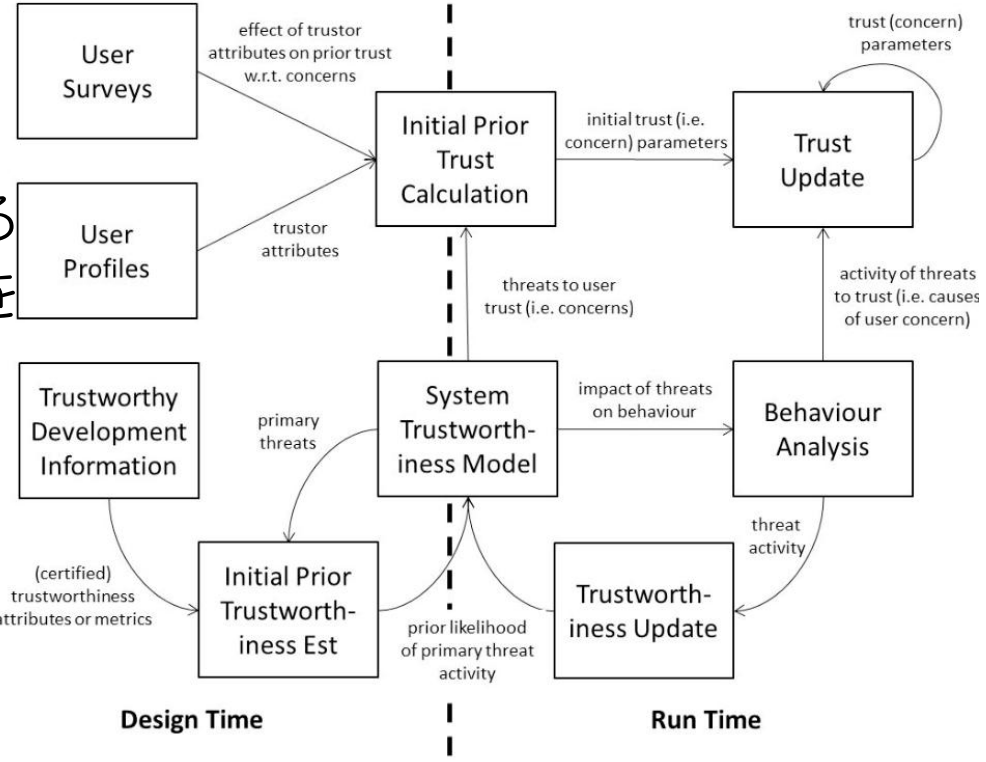


Figure 1. OPTET WP2 Modelling Approach

「デジタル社会におけるトラストのほころび」の対策というアプローチではない。デジタル社会における明示的なトラスト（explicit trust）の実現に関する報告書と考えられるが、日本において、類似する議論は皆無なのでは？

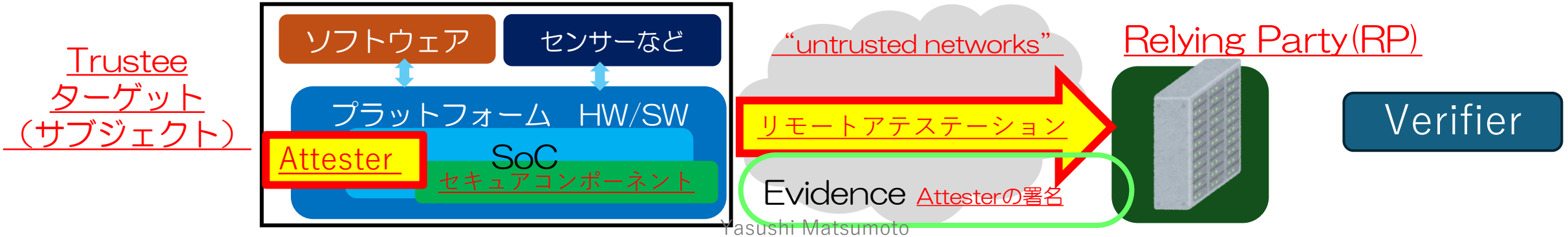
Design timeのTrustworthinessの保証
→ 従来からの適合性証明、型式証明など
Run Time のTrustworthinessの保証
→ リアルタイムな信頼性証明へ

****. Executive Summaryの冒頭の文書**
出典：https://eprints.soton.ac.uk/410774/1/OPTET_WP2_D2_5_v1_0.pdf

リモートアテステーションにおける　Trust　と　Trustworthiness

出典：　RFC 9334.　Remote ATtestation procedureS (RATS) Architecture https://datatracker.ietf.org/doc/html/rfc9334

- リモートアテステーションは、 トラスの対象(Trustee)となるリモートのデバイスなどの「実行時」のリアルタイムな信頼性（trustworthiness）の（リモート）検証というトラストメカニズム
- リモートアテステーション（RFC 9334）で説明されているTrust　と　Trustworthiness
  - このドキュメントはトラストと trustworthiness について書かれています。
  - トラストとは、（RPから見た）他のシステムに対して行う選択です。
  - Trustworthiness とは、他のシステムをトラストするかどうかの判断に利用できる、（RPから見た）他のシステムに関する品質(quality)です。
- リモートアテステーションの実現の技術の中核はデジタル署名
  - 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　→ 2025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



目指すデジタル社会

デジタルトラストで実現される世界観
ToBeとしてのデジタルトラスト

- 近年の欧州のR&Dプロジェクトに見られるゼロトラスト
- 企業内(単一ドメイン)におけるゼロトラスト話ではなく、マルチドメイン（マルチステークホルダーによるエコシステム）におけるゼロトラスト

デジタルトラスト・ゼロトラストにより実現する世界観??

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
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，自動運転を融合
（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？？）

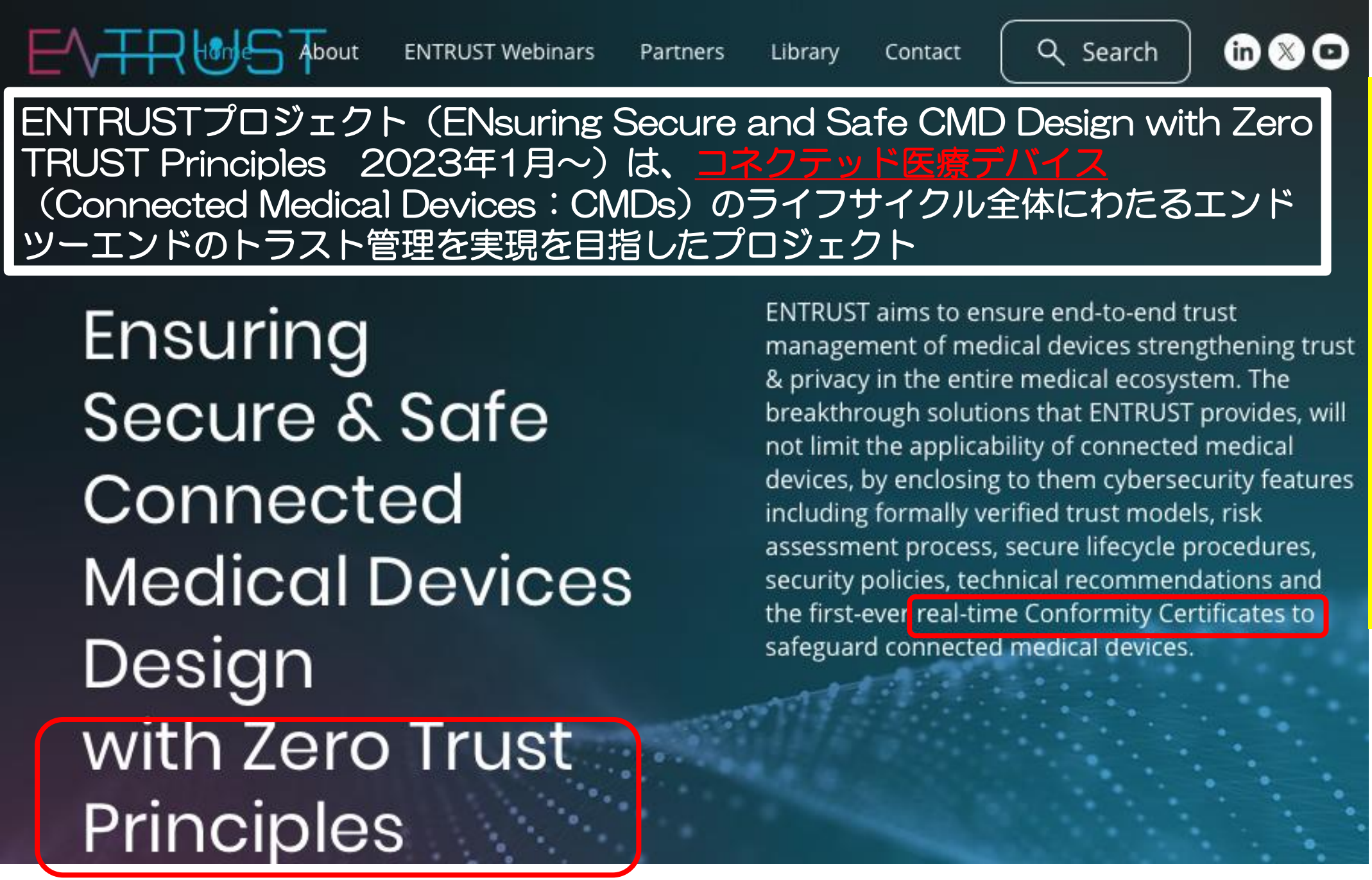
CONNECTは
→　このCCMAのための協調的なトラスト管理
（Cooperative Trust Management）
を目指したプロジェクト
（協調は、人の関係性だけではなく、マシン間の関係性）

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

CONNECTプロジェクトにおけるトラスト（ゼロトラスト）
→ デジタルトラストは、デジタル社会におけるイノベーションのために重要

- 欧州におけるCCMAでは、自動運転車や高度ITSの連携により、交通安全の向上、交通制御の最適化、輸送時間と燃料費の削減を目指している。
- ここでは、車両、インフラ、サービスの連携による衝突回避など、セーフティ・クリティカルな機能の意思決定を含むトラスト管理が必要となる。
- CONNECTでは、車両、エッジ（MEC: Multi-access Edge Computing）、クラウドを含むノードごとにリアルタイムに検証を行う継続的なトラスト評価フレームワークを適用している。
- その実現はゼロトラストアーキテクチャーの原則に基づいているが、アクセスやデータ利用のすべてにおいて検証と制御を行う。
- 例えば、車両というノードには、Hardware Root Of Trust（HW RoT）とHW RoTから検証されるTEE(Trusted Execution Environment: 信頼された実行環境)が組み込まれる。
- そして、TEEに実装された暗号鍵やアテステーション処理などを安全に行うプログラムが車両全体の信頼性（Trustworthiness）を検証し、その検証結果がリモートアテステーションにより他のノードから検証される。
- このようなリモートアテステーションによりエコシステム（System Of Systems）全体の信頼性（Trustworthiness）評価を可能としている。
- CONNECTでは、データも信頼の対象（Trustee）となり、信頼性（Trustworthiness）が検証されたノードがデータを生成し、また、そのノードによるデジタル署名が付され、結果、データの信頼性（Trustworthiness）も検証できることとなる。

ENTRUSTプロジェクト（ENsuring Secure and Safe CMD Design with Zero TRUST Principles　2023年1月～）は、コネクテッド医療デバイス（Connected Medical Devices：CMDs）のライフサイクル全体にわたるエンドツーエンドのトラスト管理を実現を目指したプロジェクト



real-time Conformity Certificates
リアルタイム適合性証明書

→ 従来からの医療デバイスの適合性証明は、製品の設計（のみ）に対して行われている。

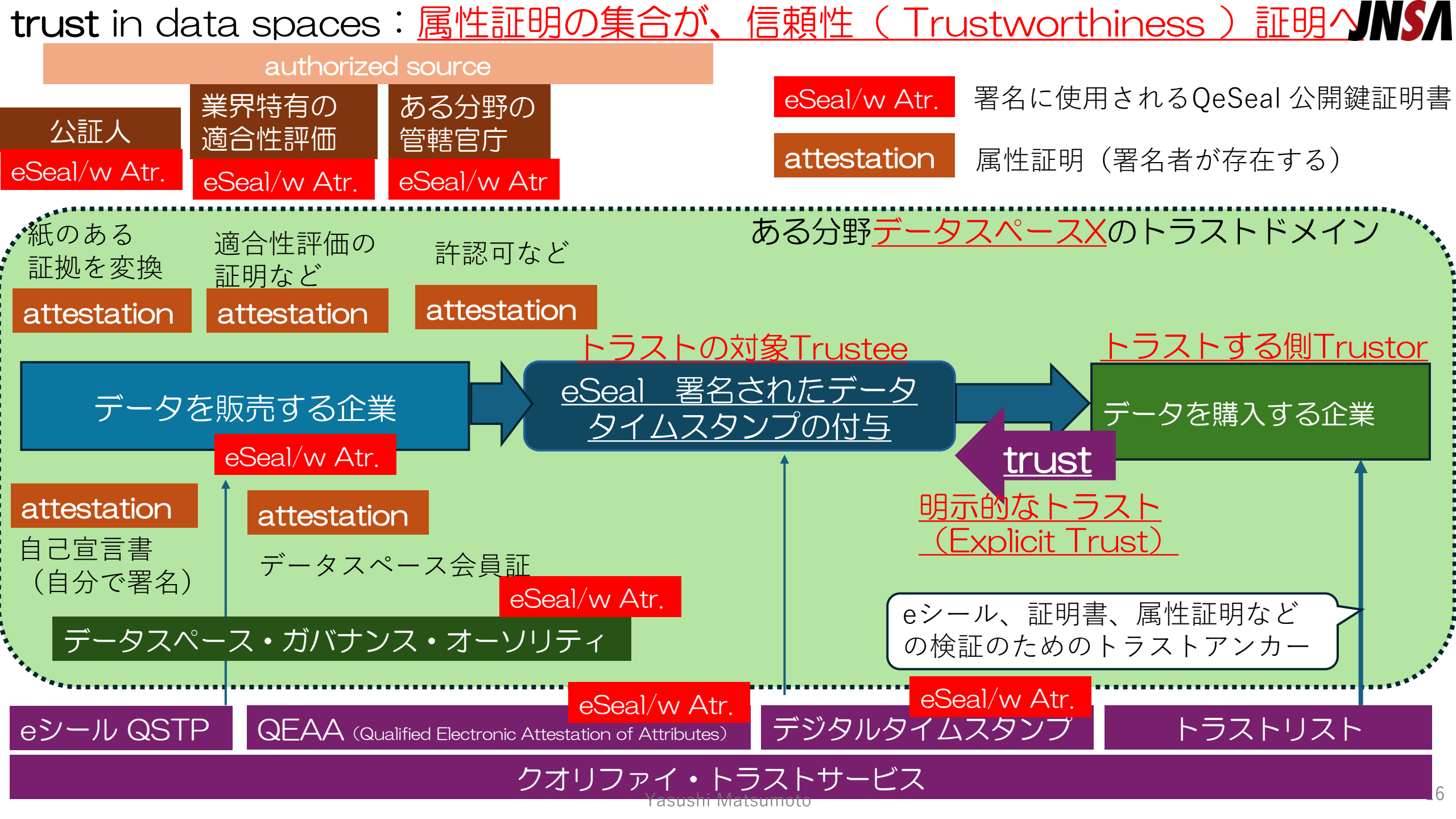
出典：https://www.entrust-he.eu

欧州のR&Dプロジェクトに見られるゼロトラスト
→　OPTET(制度的トラストと技術的トラストの融合）＋ NIST SP800-207

- コネクテッド医療デバイス分野のENTRUSTプロジェクトは、ライフサイクル全体にわたるエンドツーエンドのトラスト管理を実現するために、設計時の形式的に検証された信頼モデル、リスク評価プロセス、安全なライフサイクル手順、リアルタイムな適合証明書などを導入し、医療デバイスエコシステム全体の信頼性（Trustworthiness）の確保とプライバシーの強化を行っている。
- CONNECTの自動車、ENTRUSTの医療機器などでは、自動車のSDV (Software Defined Vehicle)や医療デバイスのSaMD （Software as a Medical Device ）いずれもソフト化が進んでいるという共通点がある。
- これらの従来から規制のある分野ででは、設計段階や出荷段階では、型式認証、出荷検査などによって信頼性が確保されてきた。　　→　出荷時の信頼性（ trustworthiness ）
- しかし、出荷後もソフトウェア更新が想定されるこうした分野では、サービス時や運用時に対応する規制と規制に対応する仕組みが重要になっている　-> 出荷後・サービス時の信頼（ trustworthiness)
- こうした規制分野では、運用時のトラスト管理に必要なリアルタイムな適合性証明などのような仕組みが必要となる。また、リアルタイムな適合証明は、他のシステム・ノードから検証できることによりエコシステム全体のトラスト管理が可能となる。　→　個々のシステム・ノードの信頼性の検証可能な仕組み

CONNECTプロジェクト、ENTRUSTプロジェクトなどに共通する基盤
→　信頼性証明のベースとなる属性証明、そのためのトラスト基盤・トラストフレームワーク
技術的トラストと（デジタル社会に適合した）制度的トラストの融合による明示的トラストの実現

trust in data spaces：属性証明の集合が、信頼性（ Trustworthiness ）証明へ



JNSA標準化部会の活動との関係

- 電子署名WG 【講演２】
  - 属性証明（Electronic Attestation of Attributes）など
- デジタルアイデンティティWG【講演３】
  - Verifiable Credentials（VC）など
- PKI相互運用技術WG 【講演４】
  - リモートアテステーションなど
- （日本ISMSユーザグループ）

標準化においてもデジタルトラストに関連する用語は氾濫＆混乱している？？
（様々な標準化においてデジタルトラストが注目されているからこそ起きている）
→訳語も定まらず日本語での議論も難しくしている（ex Trustworthiness, Attestation ）

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、AI
→ 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

Untrusted network or
zero trust network

Trustworthiness
ability/capability
property

transparency
accountability

TP
Trustee

chain of trust

TRUST・
Verifiable, Always Verify

RP
Trustor

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。

Verifiable Credentials （VC）
Remote attestation(token)
Entity Attestation Token (EAT)

Trusted device
Root Of Trust

qualified electronic attestation of attributes by eIDAS2.0

新しい概念の用語が乱立？
トラストアーキテクチャの議論

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）

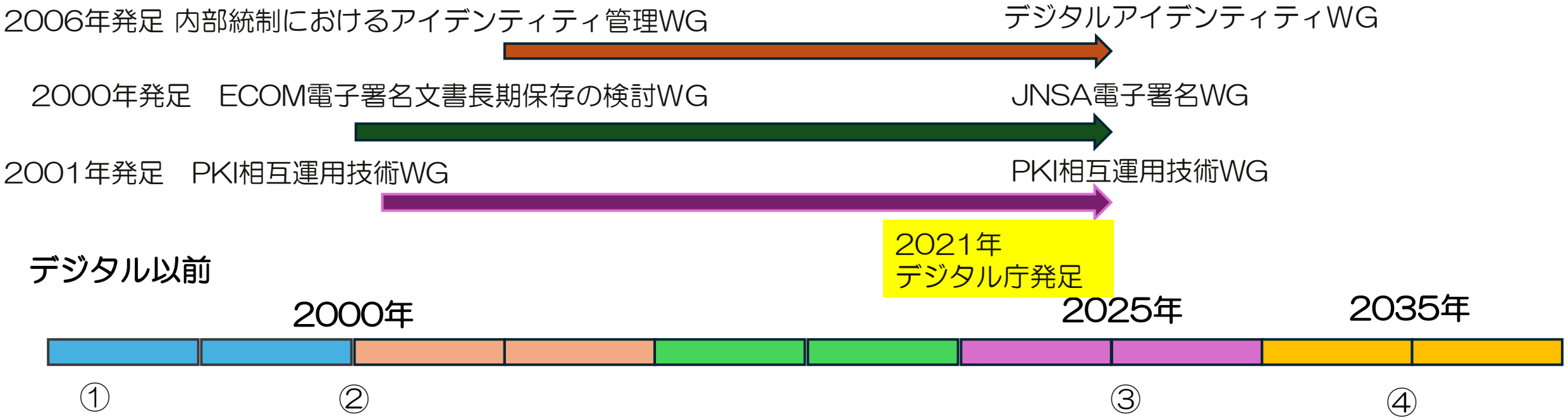
trustworthiness claim → Verifiable Claims

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？

各WGの活動とデジタルトラストとの関係->近年、属性証明に関連する活動が盛ん

- JNSA標準化部会のデジタルトラスト関連WGの活動
  - 電子署名WG → 2000年発足 ECOM電子署名文書長期保存の検討WG
    - 旧来からの電子署名の大きな役割のひとつは「否認防止」
      - Trustorから見てTrustee の否認を防止する → 否認防止は、トラストのための一つの重要な要素
    - 属性証明がトレンドになりつつある
      - 日本においても制度化される eシール → 組織などの属性証明の基礎となる
      - 欧州のeIDAS2.0 における属性証明（Electronic Attestation of Attributes）
  - デジタルアイデンティティWG → 2006年発足「内部統制におけるアイデンティティ管理WG」
    - 企業内におけるデジタルアイデンティティ管理だけでなく、インターネット上のデジタルアイデンティティ管理も
    - アイデンティティ・Identity ≒ Identifierと実体のバインディング ＋ 属性
      - トラストフレームワークの中でVC(verifiable credentials)が使われつつある
  - PKI相互運用技術WG → 2001年発足 PKI相互運用技術WG
    - 長年 IETFのセキュリティエリアでの活動を行っている
      - IETFにおいてPKI に関連した標準化は現在においても活発に行われている。現在の大きな注目点、課題は、PQC移行
    - IETFで標準化されているリモートアテステーションと、最近のアテステーションの議論
- JNSA標準化部会のデジタルトラスト関連WGのスコープ外？？
  - 個別分野のトラストの対象（ Trustee）の信頼性（Trustworthiness）は、活動の中心ではない。
    - トラストメカニズム・技術的トラストが主なスコープ
    - 共通の（トラスト）基盤、共通のトラストフレームワークが活動の中心

３つのWGは、それぞれ異なる視点からデジタルトラストの変遷を長年見てきた！



制度的トラストの進化（アナログ → デジタル初期 → デジタル社会）」 を示したタイムライン図

- ①デジタル以前：紙の証明書・印鑑・公証人・役所に依存、国内中心 -> 静的な制度的トラスト
- ②2000年前後：電子署名法・認定CAなどによる国内的な効力付与
  - 紙文書から電子文書に置き換えのための電子署名、本人特定（なりすまし防止）、改竄防止など
- ③2025年：EUDI/EUBW、VC、リモートアテステーションなどにより（自動的な）検証
  - デジタルトラストフォーメーションのため・自動化のための属性証明とその検証のフレームワーク
- ④2035年：PQC移行完了？、様々な分野においてリアルタイム適合性証明などの実現？→松本妄想?
  - 技術的トラストと制度的トラストの融合によるAIシステムなどを含む複雑なエコシステムの明示的なトラスト（explicit trust）の実現

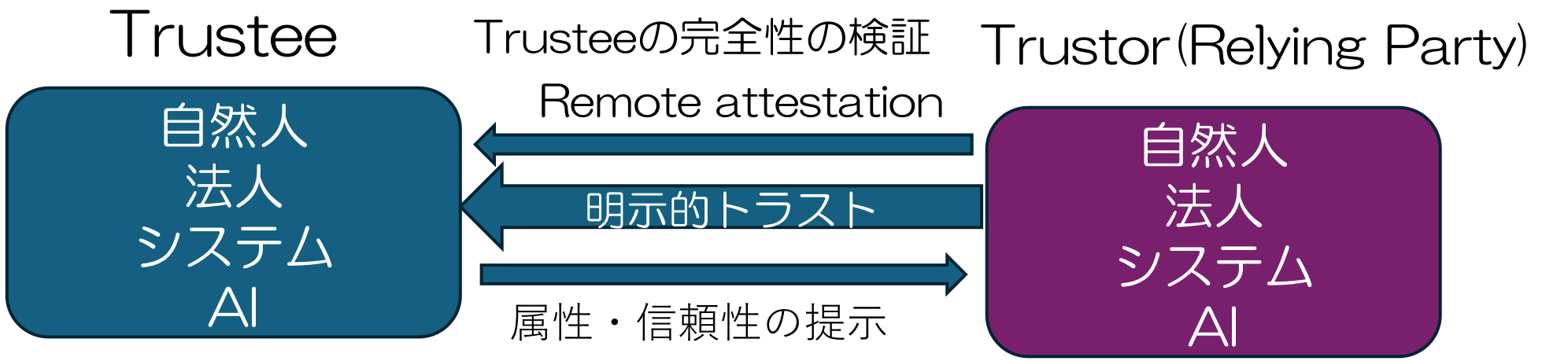
各WG活動との関係から見たデジタルトラストの（共通の）課題

- デジタルトラスト自体の概念の理解　→　現状、ここに共通の認識があるとは言えないかもしれない
  - 非常に曖昧なトラストの概念を、システム（ System of Systems ）に落とし込む必要があるが、そのためには、デジタルトラスト自体の概念と用語が整理される必要がある。
    - → デジタルトラストは注目されているが故に用語が乱立している問題など
- 適切な（属性証明の）LoA（Level of Assurance）
  - 属性証明（のLoA）ということに関しては、コスト（経済性）、証明を行うオーソリティとの関係（属性を含めたトラストモデル）など、まだまだ、課題が大きい。　→　制度的な課題でもある
- 個別分野毎のトラストの対象（ Trustee）の信頼性（Trustworthiness）は、スコープ外？？
  - JNSA標準化部会の活動のスコープとは言えないが、「個別分野の信頼の対象（ Trustee）の信頼性（Trustworthiness） 」を必要としているステークホルダーとは協調していく必要がある。
- 技術的トラストと制度的トラストの融合
  - JNSA標準化部会の活動は、技術的トラストに関する活動が中心だと考えられるが、そこに（デジタル社会に適合した）制度的トラストが噛み合う必要がある。
  - 例えは、. real-time Conformity Certificatesリアルタイム適合性証明書・型式証明のようなものは、技術的トラストだけでは実現できず、何らかの制度的トラストの関わりが必要になる

今後の展望（Future Outlook）→　ここは、松本私見（妄想？？）

- PQC時代に適応するトラスト基盤・トラストフレームワーク
  - 2030年（2035年）を見据え、耐量子計算機暗号（PQC）を組み込んだリアルタイム信頼性証明などの普及
- 技術的トラストの制度的トラストの（世界的な）融合・相互運用
  - eIDAS2.0の属性証明（EAA/QWAC）と日本の電子署名・マイナンバー制度の相互運用のような世界的なデジタルとラストの構築
- 利用者・市民にも見える「（明示的）トラストのUX」　（暗黙的なトラストにならない）
  - デジタルアイデンティティウォレット（DIW）における「属性証明の可視化」により、直感的にトラストできる世界へ
- AIと新たなトラスト課題
  - 現状のAIのトラストの議論は、ほぼAIのTrustworthinessの議論（トラストメカニズムではない）
  - しかし、これから生成されるデータのほとんどは、AIにより生成されたデータという世界の到来
  - AI＆デジタル社会においては、生成AI・自律システムとこれらが生成するデータに対する「信頼性証明」「リモートアテステーション」の実現は、非常に重要
- 日本とJNSA標準化部会が（期待される？）役割
  - 国際標準化（ETSI/IETF/ISO）などでの積極的な発信
  - データスペース・自動車・医療・製造業など様々な分野でのユースケースに基づいたトラストに関する協調
  - 技術的トラスト（Technical Trust）と制度的トラスト（Institutional Trust）などをつなぐ「共通基盤」と「共通理解」を整理するハブとしてのJNSA

「デジタルトラストの最新動向と展望」まとめ



トラスト基盤、トラストフレームワーク

まとめ　　デジタルトラストの最新動向と展望

- デジタルトラストは社会基盤へ
  - トラストの対象は「人」から「（人も含む）システム・データ・AI」へ拡大
- なぜデジタルトラストが重要なのか？
  - 複雑化するデジタル社会において、これまで社会が暗黙的に成り立たせてきたトラストの前提を、可視化・検証可能化し、制度的・技術的に自動化・スマート化していくため。
- 実際のアクションと方向性としては
  - リアルタイムな信頼性証明などが中核に　　→　その一歩としての属性証明
    - 明示的・検証可能なトラストによる透明で説明可能なデジタル社会
  - 世界的な技術的トラストと制度的トラストの融合
    - eIDAS2.0 / EUDI Wallet、PQC移行などと日本の制度・基盤などとの相互運用へ
- JNSA標準化部会の役割
  - 「国際動向と国内制度・技術の橋渡し点として整理・共有」
  - 分野横断的な「共通理解」と「共通基盤」の形成をリード
- 2030（2035）年を見据えて
  - PQC移行・AIトラスト・データスペースが融合する新時代に備える

参考スライド

- トラストについての補足
  - トラストに関する議論・書籍の紹介
- 属性証明の事例
  - ウェブサイトにおける属性証明トラスト

トラストについての補足
トラストに関する議論・書籍の紹介

JST(科学技術振興機構)CRDS(研究開発センター)のトラスト研究戦略

提言・提案
CRDS-FY2022-SP-03

戦略プロポーザル

デジタル社会における
新たなトラスト形成

STRATEGIC PROPOSAL
New Trust Formation
in the Digital Society

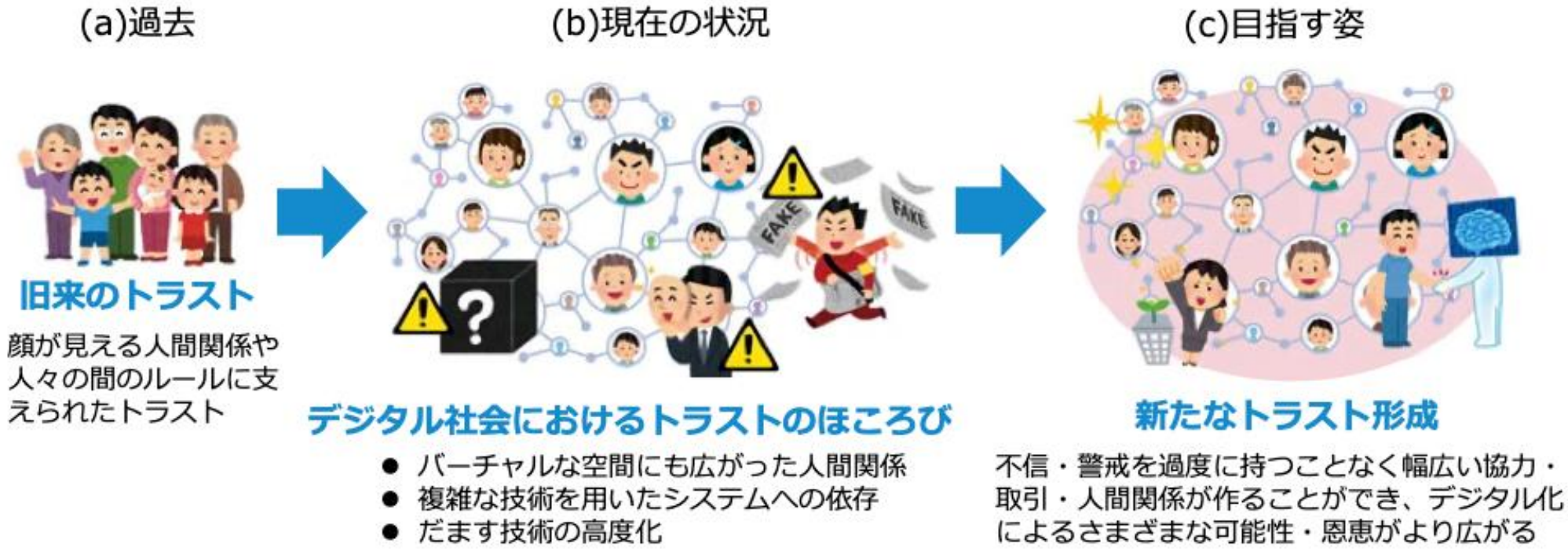


図1-1　デジタル社会におけるトラストの問題認識と目指す姿

出典：2022年9月 CRDS-FY2022-SP-03　デジタル社会における新たなトラスト形成
https://www.jst.go.jp/crds/report/CRDS-FY2022-SP-03.html

JST RISTEX　デジタルソーシャルトラスト　https://www.jst.go.jp/ristex/digist/
「デジタル社会におけるトラストのほころび」に対する課題特定、課題解決

JNSA

Trusteeの分野、種類などによる分類

Trusteeの信頼性（trustworthiness）の評価、向上などの研究

Trustorの認知バイアスが働きやすい、暗黙のトラストこの認知バイアスの研究

Trustorの分野、種類などによる分類

Trustorのリテラシーの向上、教育などの研究

より主観的

より暗黙的

信頼性（trustworthiness）

暗黙のトラスト(Implicit Trust)

品質、能力、性質

意図

他者や社会??

仲介者 intermediaries

仲介者に関連する研究
トラストの伝わり方など
Ex. エコーチェンバーなど
仲介者による情報の増幅など
トラストメカニズムの研究？

期待

主観

我々??
国民、市民など??

Trustee
トラストの対象

Trustor
Relying Party(RP)

より明示的

より客観的

明示的なトラスト（explicit trust）

様々なステークホルダーを俯瞰した上での制度設計に関する研究

Trusteeの信頼性（trustworthiness）の検証が可能な（トラスト）メカニズムの研究

デジタルソーシャルキャピタルを支えるデジタルトラストの研究

トラストって何よー??

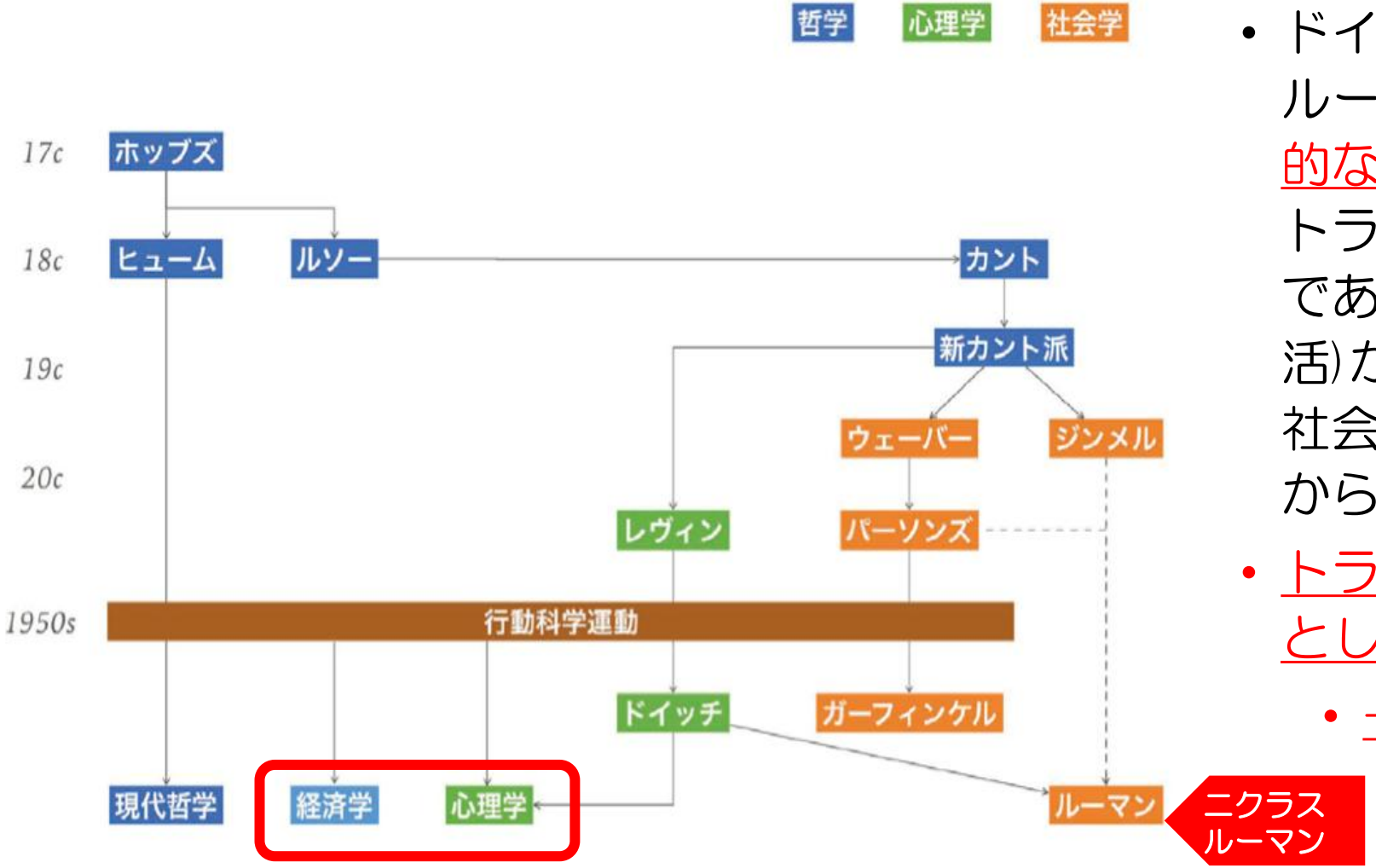


図 2-1-3　信頼研究の系譜[3]

出典：　JST/CRDS.　俯瞰セミナー&ワークショップ報告書
トラスト研究の潮流　~人文・社会科学から人工知能、医療まで~ 2021 年 7 月~ 10 月開催
信頼研究の系譜　by　小山　虎　先生
https://www.jst.go.jp/crds/pdf/2021/WR/CRDS-FY2021-WR-05.pdf

- トラストについて、
  - ドイツの理論社会学者であるニクラス ルーマン1968年の著作「信頼―社会的な複雑性の縮減メカニズム」の中で、トラストは「社会生活の基本的な事実である。(中略)こういうこと(社会生活)が可能であるのは、我々が他者や社会に対して一定の信頼をおいているからにほかならない」
  - トラスト（メカニズム）の一つの考えとして方
    - → 複雑性を縮減するメカニズム

信頼―社会的な複雑性の縮減メカニズム」
https://www.amazon.co.jp/信頼―社会的な複雑性の縮減メカニズム-ニクラス・ルーマン/dp/4326651202

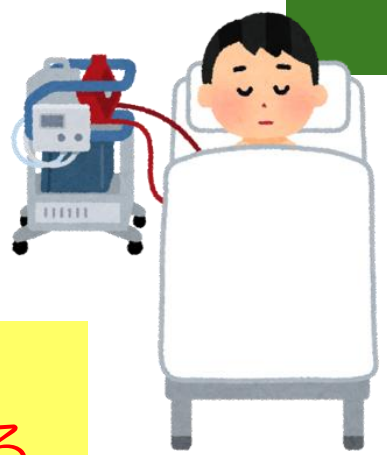
トラストが「複雑性を縮減するメカニズム（トラストメカニズム）」だとすると
より複雑性が増すデジタル社会におけるトラスト（≒広義のデジタルトラスト）とは？
トラストの対象（Trustee）が、複雑なシステムとかブラックボックスとか。。
例えば、AI医療時代（≒デジタル社会）の医療のトラストは？？

トラストの対象
Trustee

分業化した
チーム医療

TRUST

トラストする側
Trustor、RP



複雑な医療システムのtrustworthiness（信頼性）
→trustworthiness（信頼性）の意味が多義的になる

不正改造

オンライン診療

高度なIT技術が取り
入れられた医療機器

AI診療

Trust in medical AI

ネット上の評判
医師、医療機関の評判システム

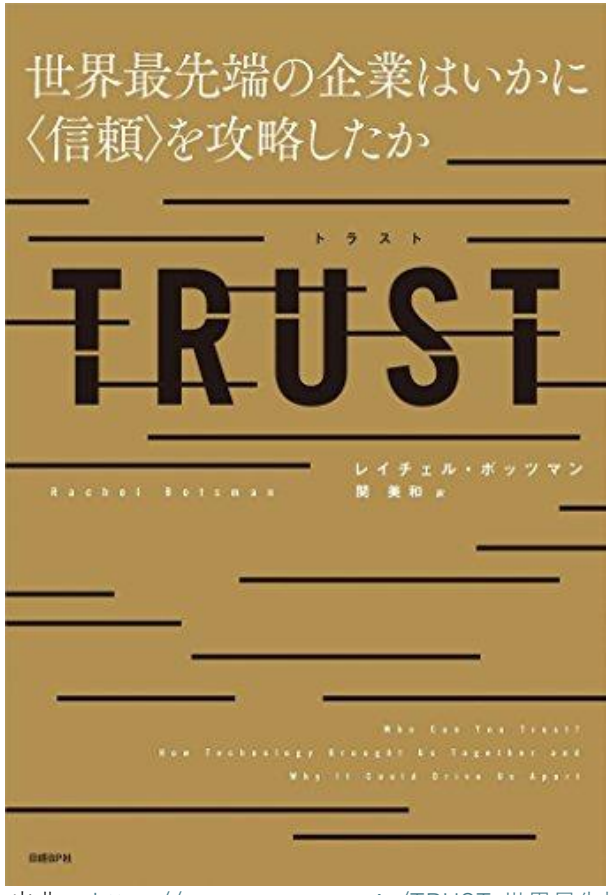
Computational Trust??

プライバシ侵害

サイバー攻撃

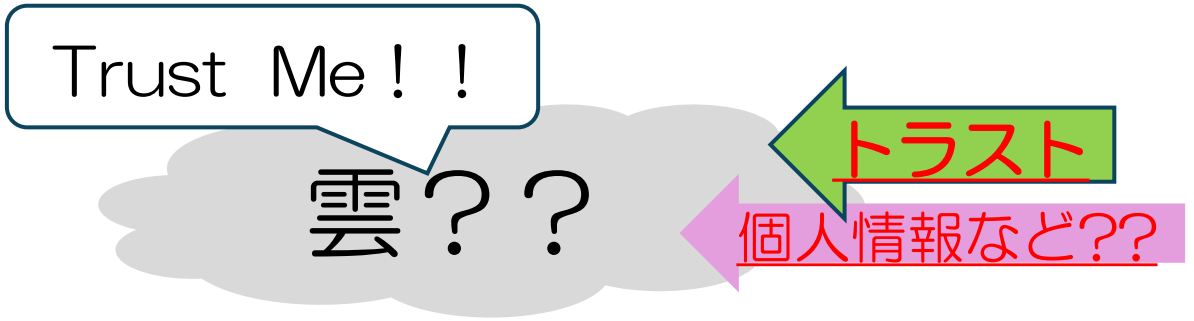
医療におけるITの役割　→　これらに対するサイバー攻撃

トラストの参考図書①世界最先端企業にとってのビジネストラスト？



出典： https://www.amazon.co.jp/TRUST-世界最先端の企業は いかに%E3%80%88信頼〉を攻略したか-レイチェル・ボッツマン-ebook/dp/B07F3MTV4M/ref=sr_1_1?__mk_ja_JP=カタカナ&crid=L2116702BIQK&keywords=B07F3MTV4M&qid=1651631306&sprefix=b07f3mtv4m%2Caps%2C393&sr=8-1

原題：WHO CAN YOU TRUST?
How Technology Brought Us Together and Why It Might Drive Us Apart



トラストの対象　Trustee

トラストする側
Trustor、RP

「社会生活の基本的な事実である。(中略)こういうこと(社会生活)が可能であるのは、我々がクラウドやスマフォに対して一定の信頼をおいているからにほかならない」？？？？？

- 古典的なビジネストラスト？？
  - Face2Faceベースのビジネストラスト->個別説得営業など
    - -> 短時間にスケールできない
- 世界最先端企業にとってのビジネストラスト
  - スケールアウトするトラストメカニズムがある？？
  - → 行動経済学などを駆使する？？？
  - → 信用スコア、評判管理（レピュテーション管理）
  - → 「デジタルトラスト」を駆使する→ 後半のテーマ

- ＜信頼＞を攻略したか → 日本のデジタル赤字の大きな原因の一つかもしれない？
- 一方で、行き過ぎたビジネス（トラスト）の要求が様々な綻びを生んでいる？

トラストの参考図書③　信頼と不信の哲学入門

JNSA

信頼と不信の哲学入門

信頼される人、組織になるにはどうすればよいのか。進化論、経済学の知見を借りながら、哲学者が迫った知的発見あふれる一冊。

著者	キャサリン・ホーリー 著 , 稲岡　大志 監訳 , 杉本　俊介 監訳
通し番号	新赤版 2044
ジャンル	書籍 > 岩波新書 > 哲学・思想 日本十進分類 > 哲学・心理学・宗教 > 哲学
刊行日	2024/12/20
ISBN	9784004320449
Cコード	0210
体裁	新書 ・ 254頁
在庫	在庫あり

出典：https://www.iwanami.co.jp/book/b654989.html

著者のキャサリン・ホリー氏（ 1971年 -2021年）の本書の結論は、

「信頼に値すること（信頼性）の重要性」

-> 信頼性（trustworthiness)のある trustee が、trustorからトラストされることの重要性

信頼に値しないものを信頼することは、裏切り、失望、搾取、すなわち不信の元となる。

-> Trustor が、信頼性（trustworthiness)のない trustee を信頼（trust）することが、裏切り、失望、搾取の元となり、負の連鎖を生む。

松本の理解としては、「デジタル社会におけるトラストのほころび」の多くは、信頼性（trustworthiness）が不確かなTrustee を、Trustorが暗黙的にトラスト(Implicit Trust)してしまう問題に起因している

既存のトラスト研究とデジタルトラストの関係

- 既存のトラスト研究（主に人文・社会学分野が多い）におけるトラスト
  - 哲学・社会学　社会がなりたつための仕組みの探求？　→ 「デジタル社会というパラダイムシフト」
  - 心理学、行動経済学など
    - 能力と意図　→　人であるTrusteeの能力や意図を人であるTrustorの主観でどのように認知するのかといった研究が多い？
    - 暗黙のトラスト（Implicit Trust）に対する認知バイアス？→ 人間自体の研究（心理学、脳科学）
      - → デジタル社会における認知バイアス（人の脆弱性）への攻撃に対応するセキュリティ研究（コグニクティブセキュリティ）の重要性も認識されつつある。
- デジタルトラスト??　--　広義には、デジタル技術に依存する社会におけるトラスト
  - デジタルトラストは、デジタル社会のビジネストラストともいえ、ビジネスの要求でもある。
  - デジタルトラストは、デジタルトランスフォーメーション、スマート化のためのトラストでもある。
    - 暗黙のトラスト（ Implicit Trust ）ではなく、明示的なトラスト（Explicit Trust）という要求
  - 一般論としては、技術的トラストと制度的トラストの融合による明示的なトラスト（Explicit Trust）の実現

属性証明の事例：ウェブサイトにおける属性証明
「ウェブサイトが真正なウェブサイトであることの証明」は可能なのか？
欧州のアプローチの紹介

eIDAS2.0　45条　　2024年5月成立

ウェブブラウザプロバイダーは、証明書（QWAC：Qualified Website Authentication Certificates）で証明されたアイデンティティデータと追加の証明された属性がユーザーフレンドリーな方法で表示されることを保証する必要がある。

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014R0910-20241018

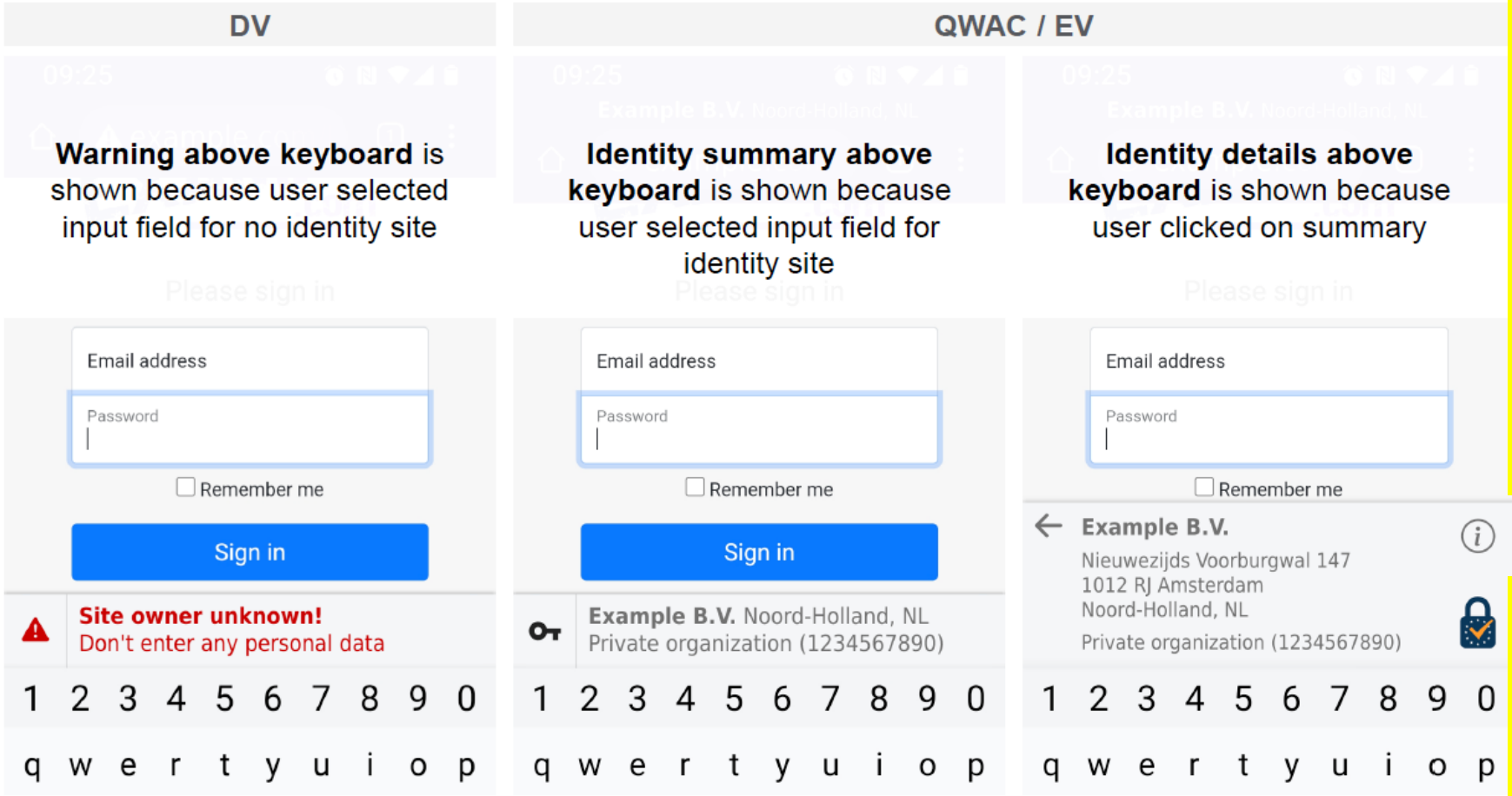
「真正なウェブサイト」の意味をもう少し深掘りする必要がある。
証明された属性　→　欧州の金融監督機関が、「認可した金融機関」であることを証明
この証明された属性（金融機関であることを）ユーザーフレンドリーな方法で表示されることを保証

https://www.slideshare.net/slideshow/etsi-esi-activities-fesa-ecats-2025-05-14-pdf/279151528

eIDAS2.0　45条　　2024年5月成立
ウェブブラウザのプロバイダーは、証明書（QWAC：Qualified Website Authentication Certificates）で証明されたアイデンティティデータと追加の証明された属性がユーザーフレンドリーな方法で表示されることを保証する必要があります。

情報入力時に警告するUIをブラウザに実装

Summary of EU compliant data entry interfaces



このスライドは、2021年、eIDAS2.0案が提出された後のChris Bailey, Entrustの提案

2024年に、ETSIにおいて、Web Authentication Task Forceが活動を開始しており、2025年現在もUIに関する検討は行われていると考えられる。

2024年6月 Google は、デジタル証明書のセキュリティを維持するため、Entrust の証明書をディストラストすることを発表している。
https://security.googleblog.com/2024/06/sustaining-digital-certificate-security.html

出典：　Designing the new eIDAS 2 browser UI
https://www.enisa.europa.eu/events/trust-servicies-forum-ca-day-2021/ca-day-presentation/05_chris-bailey_20210900-ca-day-designing-the-new-eidas-2-browser-ui.pdf

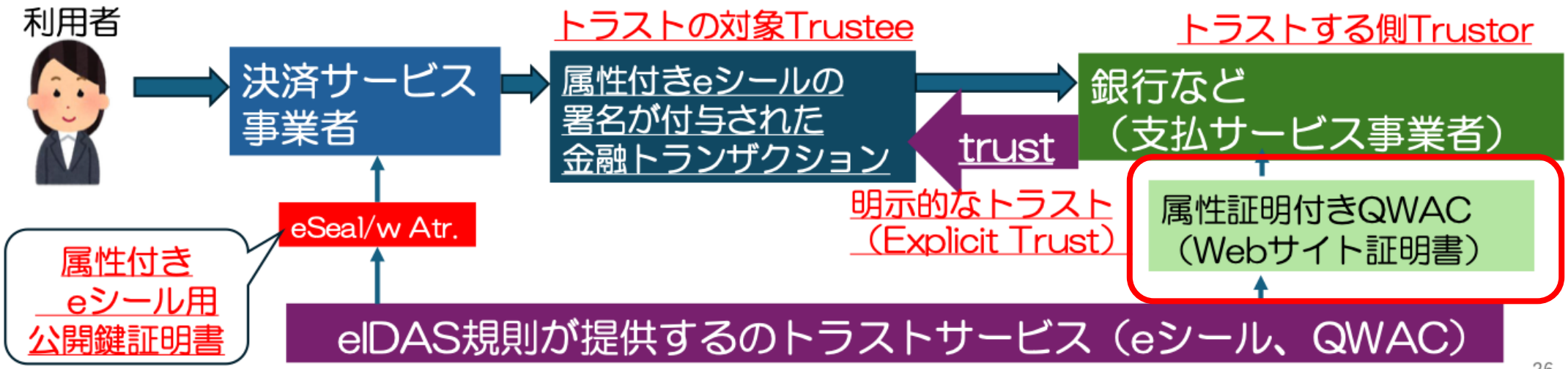
フィッシングのターゲットなるWebサイトの識別
EUのデジタルアイデンティウォレットで検討されているQWACによる属性証明
→ EUのデジタルアイデンティウォレットでは「証明された属性」によるアクセス制御が検討されている

- 従来からのEV証明書への批判
  - 正規の法人であれば、金さえ払えば証明書を発行しているので、信頼できる法人とは限らない（実際、そのようなサイトが作られたし、そもそもの法人登記が甘い国がある）
  - → 正規の法人によるWebサイトが、本当に、真正なWebサイトなのか？
- EUのデジタルアイデンティウォレットで検討されているQWACによる属性証明
  - 個人のDIWのアクセス先の明示（アクセス制御・制限も行う）　-> Draft 段階
  - relying party role　が　public administration、trust service providers、qualified trust service providers、public sector attestation issuer、banks and credit institutions
  - other regulated institutions on EU ..　その他。。。

欧州のPSD2における（トラスト）な金融トランザクションの考え方

＃ここでは、「金融トランザクション」をトラストの対象（Trustee）と捉える

- PSD2（Payment Services Directive 2）とは、欧州連合（EU）が2018年に施行した決済サービスに関する指令であり、決済サービスの透明性と競争の促進
  - 多対多の関係にある「決済サービス事業者」と「銀行など（支払サービス事業者）」間のトランザクションデータ（このトラストを如何に実現するのか）
- 属性付きeシール証明書は、欧州の金融監督庁が与えた属性（許可番号）の証明も行われている
  - → Trustworthinessは、許認可を行なっている欧州の金融監督機関の役割が大きい
  - → Trust メカニズムは、トラストサービスが発行するeIDAS 規則の(属性付き）eシールなどの役割
- 利用者は、欧州の決済エコシステムにおけるPSD2のような制度・トラスト管理に暗黙のトラストを置く



出典：https://www.iwsec.org/scis/2025/_img/page/YasushiMatsumoto_SCIS2025_InvitedTalk.pdf

欧州の金融管轄官庁により証明された属性（許認可された決済サービス事業者、支払いサービス事業者）によるアクセス制御（QWACを利用）は、欧州のPSD２で既に利用されている。