JNSA

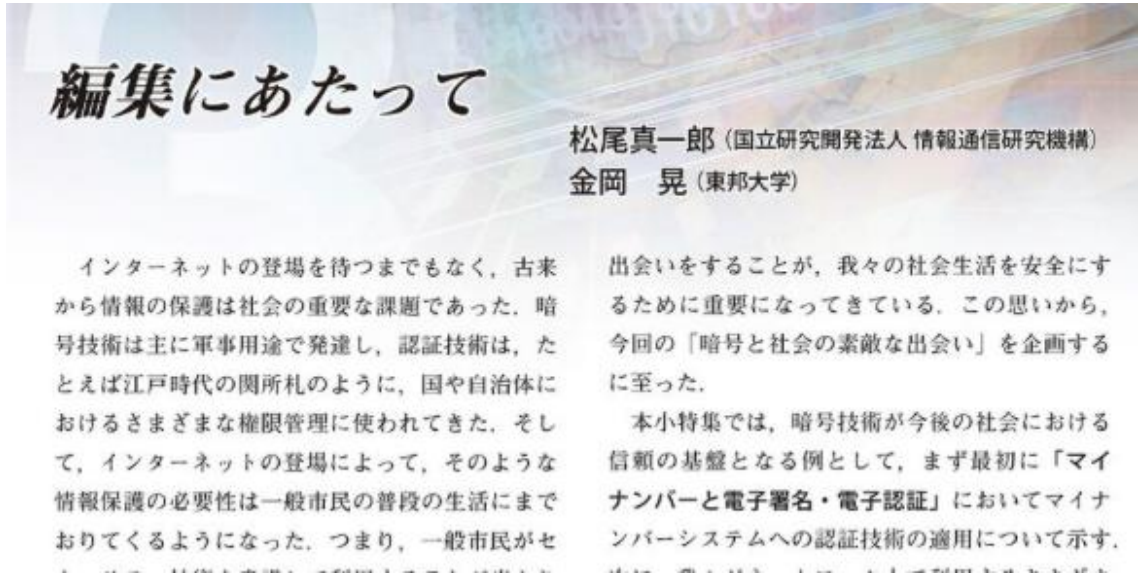
改めて考えるデジタル社会における公開鍵暗号の重要性

-- 続・続・暗号と社会の素敵な出会い --

2025年1月29日

NPO JNSA フェロー　松本　泰

https://www.fujisan.co.jp/product/1281696853/b/1357856/



編集にあたって

松尾真一郎（国立研究開発法人 情報通信研究機構）
金岡　晃（東邦大学）

インターネットの登場を待つまでもなく，古来から情報の保護は社会の重要な課題であった．暗号技術は主に軍事用途で発達し，認証技術は，たとえば江戸時代の関所札のように，国や自治体におけるさまざまな権限管理に使われてきた．そして，インターネットの登場によって，そのような情報保護の必要性は一般市民の普段の生活にまでおりてくるようになった．つまり，一般市民がセ

出会いをすることが，我々の社会生活を安全にするために重要になってきている．この思いから，今回の「暗号と社会の素敵な出会い」を企画するに至った．

本小特集では，暗号技術が今後の社会における信頼の基盤となる例として，まず最初に「**マイナンバーと電子署名・電子認証**」においてマイナンバーシステムへの認証技術の適用について示す．

招待講演#2 —Invited Talk—

- 講演タイトル

  続・暗号と社会の素敵な出会い

- 講演者

  松尾　真一郎
  バージニア工科大学　研究教授 (Research Professor, Virginia Polytechnic Institute and State University)
  ジョージタウン大学　研究教授 (Research Professor, Georgetown University)

https://www.iwsec.org/scis/2024/invited.html

- 日時

  2024年1月24日（水）[2日目] 16:50~17:50

Copyright 2025 NPO日本ネットワークセキュリティ協会

改めて考えるデジタル社会における公開鍵暗号の重要性
-- 続・続・暗号と社会の素敵な出会い --

- 2000年に成立した電子署名法は、公開鍵暗号が法制度に組み込まれたという意味において画期的な出会いでした。それから20数年経った現在、まだ公開鍵暗号と社会の素敵な関係を築いたとは言えないかもしれませんが、この素敵な関係こそがデジタル社会におけるトラストの確立に大きく貢献すると考えられます。
- 本講演では、Socity5.0実現などが目指されているデジタル社会において、なぜ公開鍵暗号などを駆使したデジタルトラストが重要なのか説明するとともに、併せて今後の暗号・セキュリティ分野の研究に対する期待を述べます。

果たして、我々は、「暗号と社会の素敵な出会い」から「暗号と社会の素敵な関係」を築いてこられたのか？？

Copyright 2025 NPO日本ネットワークセキュリティ協会

プロローグ
自己紹介とイントロ

Copyright 2025 NPO日本ネットワークセキュリティ協会

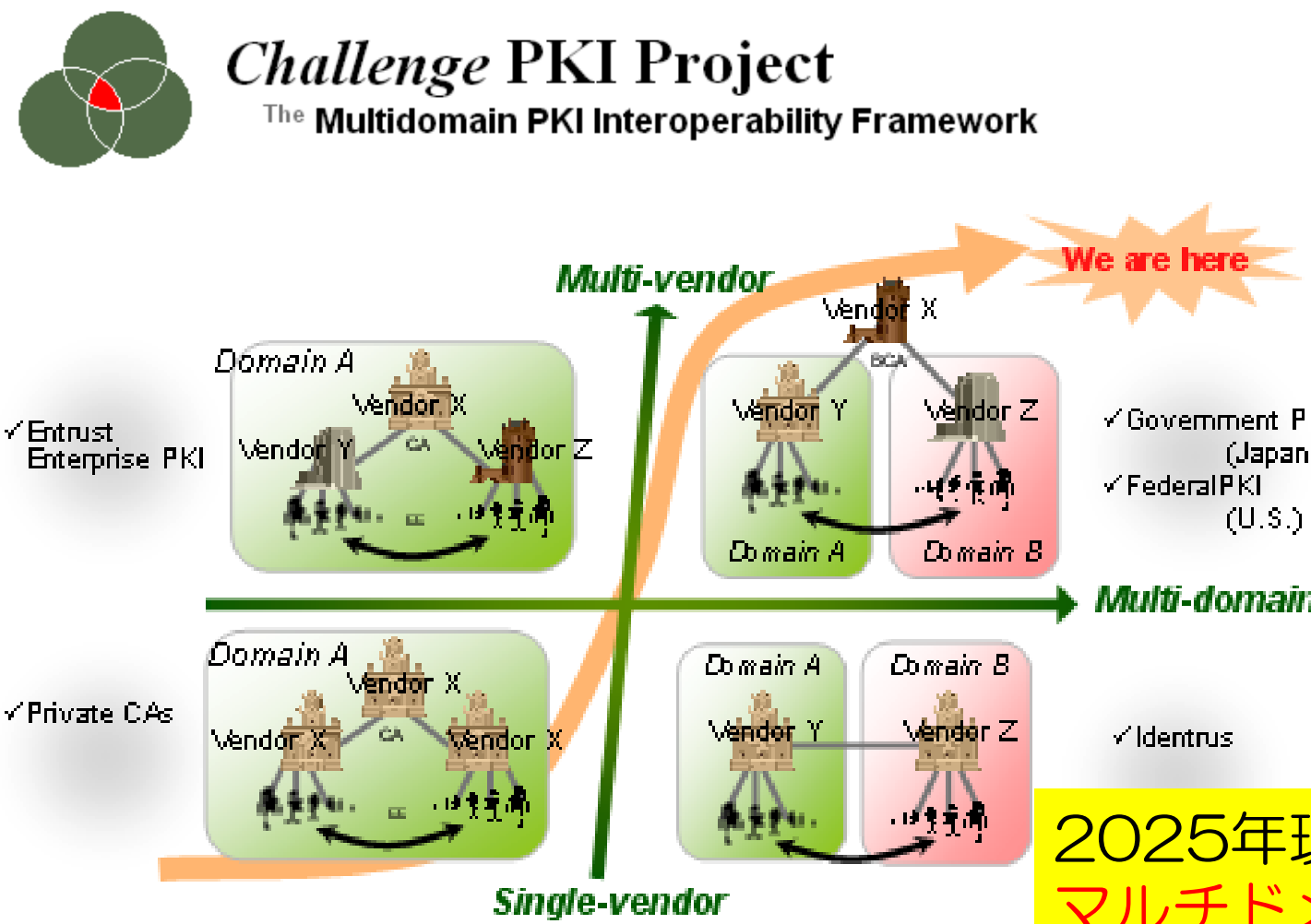
松本の自己紹介　　NPO 日本ネットワークセキュリティ　フェロー

1978年　計測器メーカにてハードウェアの設計開発に従事
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設計開発などに従事
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　→ ネットワークセキュリティとか
1998年　サイバーセキュリティ事業の立ち上げに従事　→　不正侵入検知サービス、電子認証サービスなど
2003年-2007年　工学院大学「セキュアシステム設計技術者の育成」プログラム客員教授
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
2007年-2012年　IPA 情報処理推進機構 情報セキュリティ分析ラボラトリー 非常勤研究員
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
2001年 - 2023年末　　NPO JNSA PKI相互運用技術WGリーダ
2025年1月現在
　NPO 日本ネットワークセキュリティ　フェロー
　デジタル庁　電子署名法認定基準のモダナイズ検討会　座長
　金融庁　預金取扱金融機関の耐量子計算機暗号への対応に関する検討会　委員　（2024年10月で終了）
　JST RISTEX　デジタルソーシャルトラスト　プログラムアドバイザー
　ウラノス・エコシステムの拡大及び相互運用性確保のためのトラスト研究会
　CRYPTEC 暗号技術検討会構成員（2006年より）、暗号技術評価委員会　委員
　（独）中小企業基盤整備機構　最高情報セキュリティアドバイザー
　総務省　サイバーセキュリティエキスパート
　一般財団法人 日本情報経済社会推進協会 客員研究員
　セコム科学技術進行財団　理事

この辺りの話

Copyright 2025　NPO日本ネットワークセキュリティ協会

2001年－2023年末 NPO JNSA PKI相互運用技術WGリーダ
→ 2001年にJNSAが開始したChallenge PKI プロジェクト



Transition of PKI models

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。

2025年現在において、国や産業分野などの、マルチドメイン（≒トラストドメインを超えた）データ連携は、非常に大きな Challenge

出典：Challenge PKI Project The Multidomain PKI Interoperability Framework https://www.jnsa.org/mpki/index_j.html

Copyright 2025 NPO日本ネットワークセキュリティ協会

2024年度 デジタル庁電子署名法認定基準のモダナイズ検討会　座長

「認定基準については法施行当初から大きな改正が行われていない」この認定基準の最新化についての検討会　https://www.digital.go.jp/councils/digitalsign-modernization

2000年過ぎ電子署名法制定時においてこの認定基準の策定には大きな労力が割かれた

図８　電子署名法の認定基準等に関する検討会」と　暗号技術に関する検討会」の体制

< 電子署名法の認定基準等に関する検討会 >

電子署名及び認証業務に関する法律における特定認証業務の認定基準等に関する検討会
辻井重男座長）
（事務局 総務省／法務省／経済産業省）

- 電子署名技術WG（松本勉グループ長）
  - ・特定認証業務で対象となる電子署名の基準を検討
- 認定基準等WG（手塚悟グループ長）
  - ・設備基準、利用者の真偽確認基準、業務管理・運用基準等、認定に係る基準を検討

・特定認証業務の認定要件について検討。
⇒ 政省令の作成・見直し作業に反映

< 暗号技術に関する検討会 >

暗号技術検討会
令井秀樹座長）
（事務局 総務省／経済産業省）

・評価依頼
・技術事項に関する助言依頼
・評価結果の報告
・技術事項に関する助言

暗号技術評価委員会
令井秀樹委員長）
（事務局 情報処理振興事業協会／通信・放送機構）

・技術評価を行う。
・電子政府暗号利用に資するガイドライン作成。
・技術事項に関する助言を行う。

- 共通鍵暗号評価小委員会（金子敏信委員長）
- 公開鍵暗号評価小委員会（松本勉委員長）

・両省に対して暗号利用に関する助言を行う。
・電子政府における暗号利用に関する政策的判断を行う。
・具体的な暗号の評価依頼を行う。

暗号技術要件調査WG
佐々木良一リーダ）

2002年3月15日電子署名法の認定基準等に関する検討会

暗号を核とする
情報セキュリティ評価の
在り方について

2002年4月16日
暗号技術検討会顧問
暗号技術評価委員会顧問
辻井重男（中央大学）

出典：暗号を核とする情報セキュリティ評価の 在り方について
https://www.cryptrec.go.jp/events/2001/slides/2_tsujii.pdf

- デジタル社会へと大きく変化している中、取り残され、また、関心も薄い「電子署名法認定基準」
- たぶん　SCIS2025の参加者でも、認定基準自体に関しては、関心が薄いのでは？？？？
- こうした基準は、デジタル社会にこそ重要なのでは？

Copyright 2025 NPO日本ネットワークセキュリティ協会

金融庁　預金取扱金融機関の耐量子計算機暗号への対応に関する検討会　委員（2024年10月で終了）

令和６年７月４日
金融庁

「預金取扱金融機関の耐量子計算機暗号への対応に関する検討会」の開催について

１．趣旨

量子コンピュータが実用化されると、現在広く利用されている公開鍵暗号の安全性が損なわれることが指摘されており、耐量子計算機暗号（Post-Quantum Cryptography、PQC）への移行に向けた検討が国内外で始まっています。金融庁では、金融分野における課題や留意事項について、幅広い関係者と議論を行ってきました。

今般、上記の検討の一環として、PQCへの移行を検討する際の推奨事項、課題及び留意事項について関係者と更に検討するため、本検討会を開催します。

- PQC移行はとっても大変。なぜならば公開鍵暗号は、既に社会に深く浸透しているから・・
- ＃と考えていたが・・世の中的には、そのようには認識されていないかも（何処で使われているのかも分からない）
- ＃逆に、公開鍵暗号は、社会を裏から支える仕組みであることを実感

「預金取扱金融機関の耐量子計算機暗号への対応に関する検討会」

メンバー等名簿

（敬称略、五十音順）

座長	寺井　理	株式会社みずほフィナンシャルグループ グループ執行役員・情報セキュリティ担当（グループ CISO） 金融 ISAC FinTech セキュリティワーキンググループ座長
メンバー	安藤　彰英	株式会社名古屋銀行　執行役員　業務部長
	岩崎　三郎	株式会社静岡銀行　リスク統括部長
	宇根　正志	日本銀行　金融研究所　参事役
	大城　徹	株式会社しんきん情報システムセンター　上席執行役員
	菅野　洋平	労働金庫連合会　情報システム部　副部長
	白井　大輔	株式会社三井住友フィナンシャルグループ グループ CISO　サイバーセキュリティ統括部長
	高瀬　徹	農林中央金庫　IT 統括部部長（システムリスク管理担当）
	松本　泰	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 フェロー
	峰　匡親	株式会社三菱 UFJ フィナンシャル・グループ グループ CISO　サイバーセキュリティ推進部　部長
	村山　朋彦	信組情報サービス株式会社　常勤取締役
オブザーバー	一般社団法人金融 ISAC、CRYPTREC 事務局、公益財団法人金融情報システムセンター、日本銀行　金融機構局、内閣サイバーセキュリティセンター	
事務局	金融庁	

金融庁の預金取扱金融機関の耐量子計算機暗号への対応に関する検討会
https://www.fsa.go.jp/news/r6/singi/20240704.html

Copyright　2025　NPO日本ネットワークセキュリティ協会

JST RISTEX　デジタルソーシャルトラスト　プログラムアドバイザー

明治大学の湯淺墾道先生が領域代表、デジタル社会におけるトラストに起因する多様な課題とその解決

https://www.jst.go.jp/ristex/digist/

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)

能力

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

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

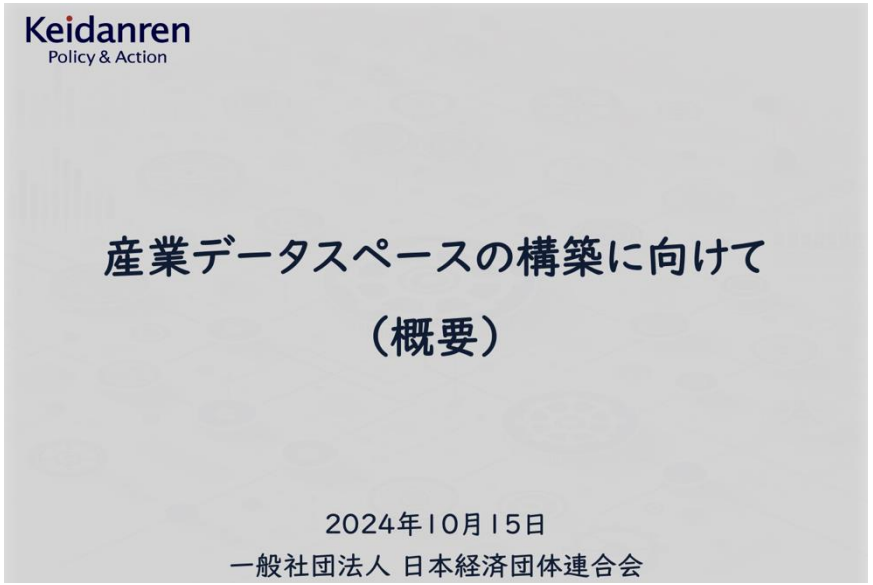
Trusteeの信頼性（trustworthiness）の検証が可能な（トラスト）メカニズムの研究

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

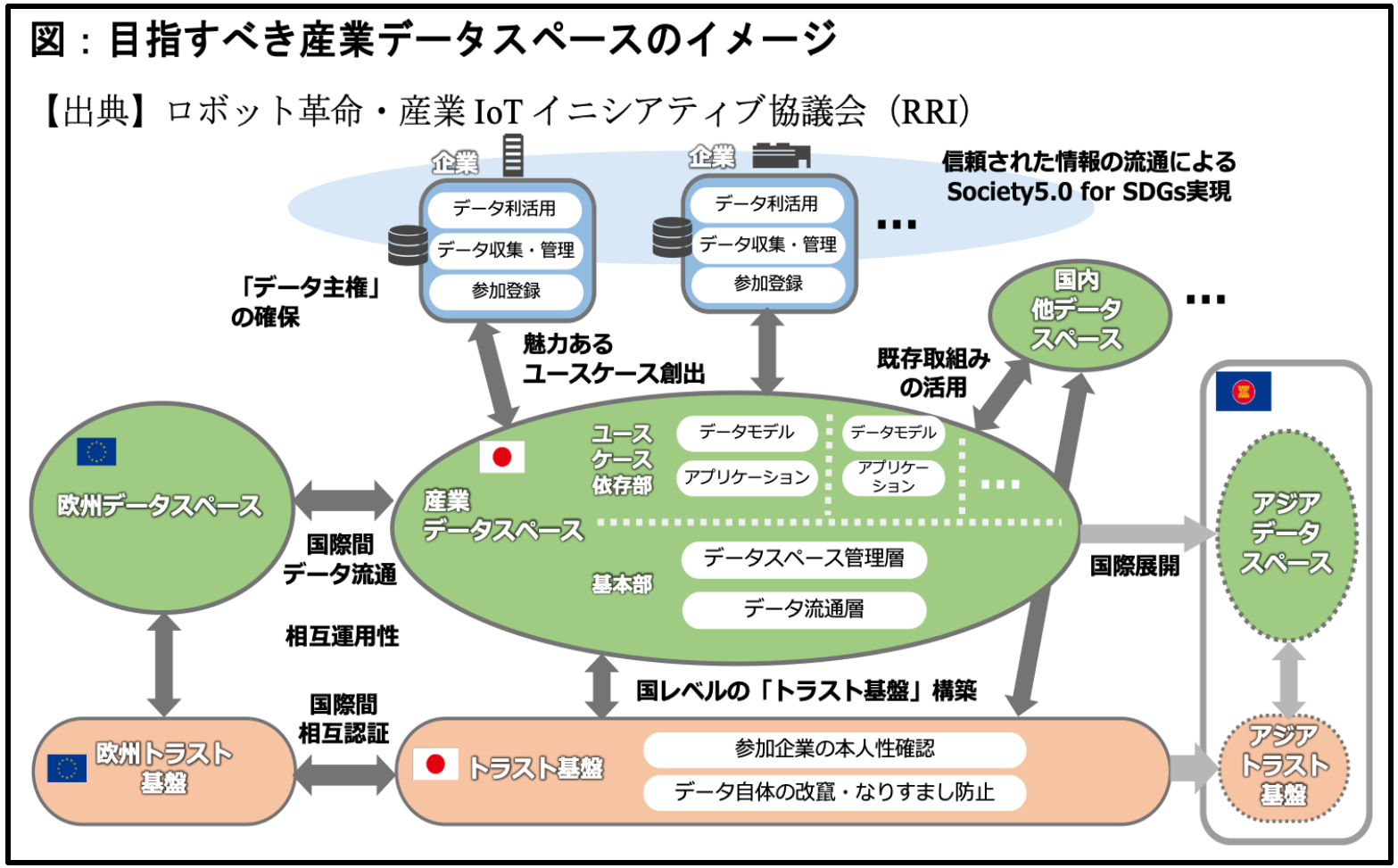
より客観的

Copyright 2025 NPO日本ネットワークセキュリティ協会

経済産業省
ウラノス・エコシステムの拡大及び相互運用性確保のためのトラスト研究会　委員
https://www.meti.go.jp/policy/mono_info_service/digital_architecture/ouranos_trust.html
DFFT（Data Free Flow with Trust）のTrust の研究会？？？



「EU等の海外の産業データスペースとの相互運性確保のため、トラスト基盤の国際相互運用承認や国際的なルール形成に関する議論を、日本がリードしていくことも必要となる」というこの提言書の主張



出典：産業データスペースの構築に向けて　https://www.keidanren.or.jp/policy/2024/073.html

なぜ今、トラストなのか？　また、トラスト自体や、トラスト基盤に関して、共通の理解があるのか？

Copyright 2025　NPO日本ネットワークセキュリティ協会

総じてデジタルトラスト・公開鍵暗号と社会の素敵な関係の説明は、とっても難しい
→　なので、ちゃんと説明出来るようになりたい！！！

- JST RISTEX　デジタルソーシャルトラスト　プログラムアドバイザー
  - デジタル社会におけるトラストと不信（distrust）に起因する様々な問題の顕著化
  - セキュリティ的には、コグニクティブセキュリティ、ユーザビリティセキュリティに隣接する課題を多く扱っている
  - ここでの「トラスト」と公開鍵暗号などの文脈で使われるデジタルトラストとの関係は？？？
- デジタル庁　電子署名法認定基準のモダナイズ検討会　（松本が座長）
  - 公開鍵暗号が法制度に組み込まれた画期的な出会いであった電子署名法。電子署名法の中の「認定基準」は、なぜ、顧みられることが少なかったのか？
- 金融庁 預金取扱金融機関のPQCへの対応に関する検討会 （すでに終了しているが、絶賛ハマり中）
  - PQC移行はとっても大変。なぜならば公開鍵暗号は既に社会に深く浸透しているから（のはずだが、世の中的には、認識されていないかも）
  - ＃公開鍵暗号も、社会を裏から支える仕組みであることを実感
- 経済産業省　ウラノス・エコシステムの拡大及び相互運用性確保のためのトラスト研究会　委員
  - 「トラスト研究会」だけど。。。トラストについての共通の理解は、簡単じゃない。
  - 共通の理解は、（プラットフォーム化に必要な）相互運用性確保のベース

Copyright 2025　NPO日本ネットワークセキュリティ協会

改めて考えるデジタル社会における公開鍵暗号の重要性 -- 続・続・暗号と社会の素敵な出会い --

- （１）　トラストについて
  - TRUSTとTrustworthinessの区別
- （２）　ゼロトラストからみたトラスト
  - ゼロトラストは、明示的なトラスト（ explicit trust ）
- （３）　データスペースにおけるトラスト
  - 信頼性（ Trustworthiness ）証明という方向性
- （４）　まとめ
  - 暗号と社会の素敵な出会いから素敵な関係に向けて
- 付録

Copyright 2025　NPO日本ネットワークセキュリティ協会

トラストについて
TrustとTrustworthinessの区別

- 議論の前提となる「トラスト」の理解
- 本日は、松本の独断と偏見？？に基づきトラストを説明します
→. そーじゃないと先に行かないから

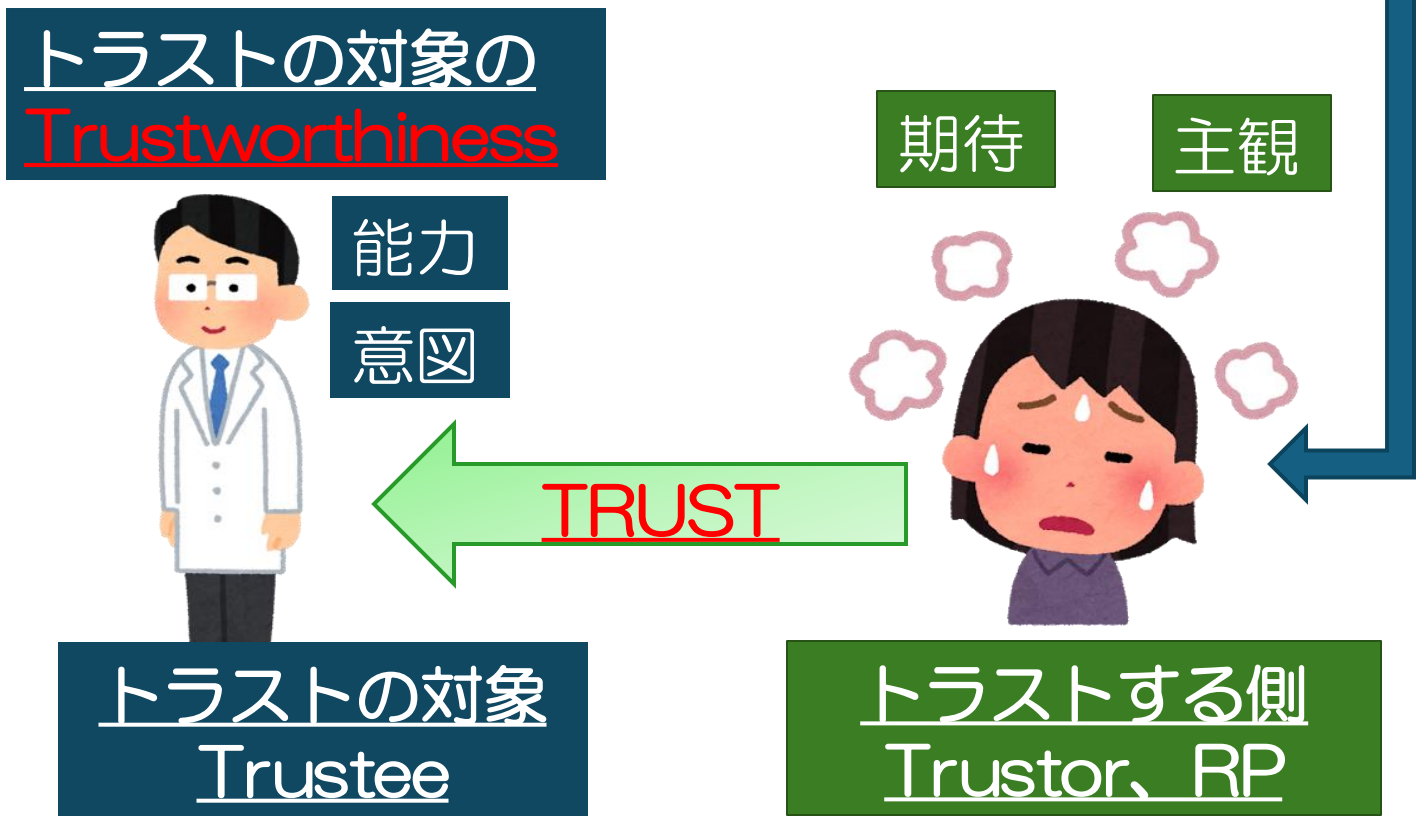
Copyright 2025 NPO日本ネットワークセキュリティ協会

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 品質・性質・能力など
  - シンプルには、Trustee の属性（Attribute）と捉える
- 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)でもある制度的フレームワーク



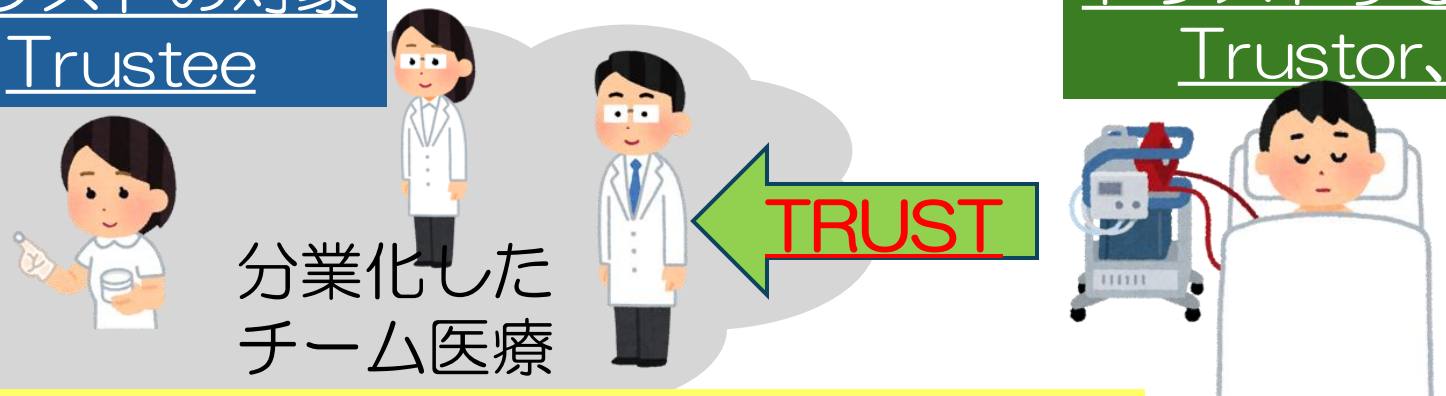
付録　トラストに関する議論の紹介、TrustとTrustworthinessの説明

Copyright 2025　NPO日本ネットワークセキュリティ協会

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
トラストの対象（Trustee）が、複雑なシステム（System Of Systems）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

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
プライバシ侵害
サイバー攻撃

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

ネット上の評判
医師、医療機関の評判システム

Trust in medical AI　Computational Trust??

医療におけるITの役割　→　これらに対するサイバー攻撃

Copyright　2025　NPO日本ネットワークセキュリティ協会

JST RISTEX　デジタルソーシャルトラスト　プログラムアドバイザー
デジタル社会におけるトラストに起因する様々な課題の解決

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

より主観的

より暗黙的

Trustorのリテラシーの向上、教育などの研究

信頼性（trustworthiness）

暗黙のトラスト(Implicit Trust)

能力

仲介者

期待

主観

現代社会における、トラストに起因する様々な問題は、
Trusteeの信頼性（trustworthiness）がTrustorから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

Copyright 2025　NPO日本ネットワークセキュリティ協会

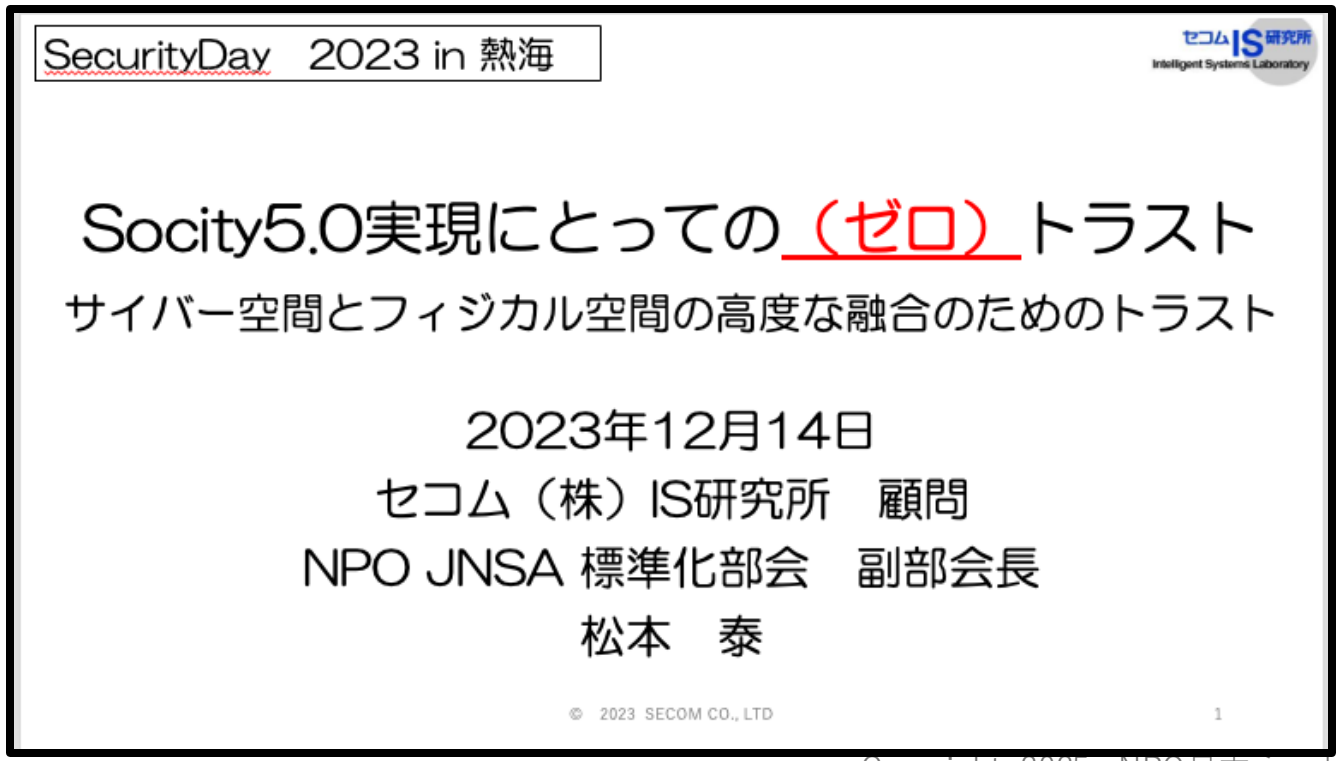
トラストについてのまとめ

- TrustとTrustworthinessの用語の使い分け
  - Trustworthiness
    - なるべくシンプルにトラストの対象（Trustee ）の性質（属性）と考える
  - Trust
    - トラストの対象（Trustee）の性質（属性）が、Trustor（RP）に伝わるメカニズムとTrustorの判断と捉える
- 暗黙的なトラスト(Implicit Trust)と明示的なトラスト（explicit trust）
  - より暗黙的なトラスト(Implicit Trust)　　より主観的
    - 心理学などにおけるトラストでは、Trusteeの意図（Intentional）により注目している。
      - Trustorの期待、主観（バイアスとも言う？）
    - ここに人間の脆弱性？　→　コグニティブセキュリティ、ユーザブルセキュリティの研究分野
  - より明示的なトラスト（explicit trust）　　より客観的
    - 検証（verification）により得られるトラスト
    - 一般論としては、検証にはコストがかかる　→　ここを全体最適化しコストを低減する
      - #→ コストを低減するために（公開鍵）暗号と社会の素敵な出会い・関係が求められるのでは？？
- 複雑性が増すデジタル社会におけるトラストの課題
  - トラストの対象（Trustee ）が、複雑化、ブラックボックス、System Of Systems
  - →　旧来からのトラストメカニズムとも言える「より暗黙的なトラスト（Implicit Trust）の限界」

Copyright 2025　NPO日本ネットワークセキュリティ協会

ゼロトラストからみたトラスト

ゼロトラストは、明示的なトラスト（ explicit trust ）


SecurityDay　2023 in 熱海

セコムIS研究所
Intelligent Systems Laboratory

Socity5.0実現にとっての（ゼロ）トラスト

サイバー空間とフィジカル空間の高度な融合のためのトラスト

2023年12月14日

セコム（株）IS研究所　顧問

NPO JNSA 標準化部会　副部会長

松本　泰

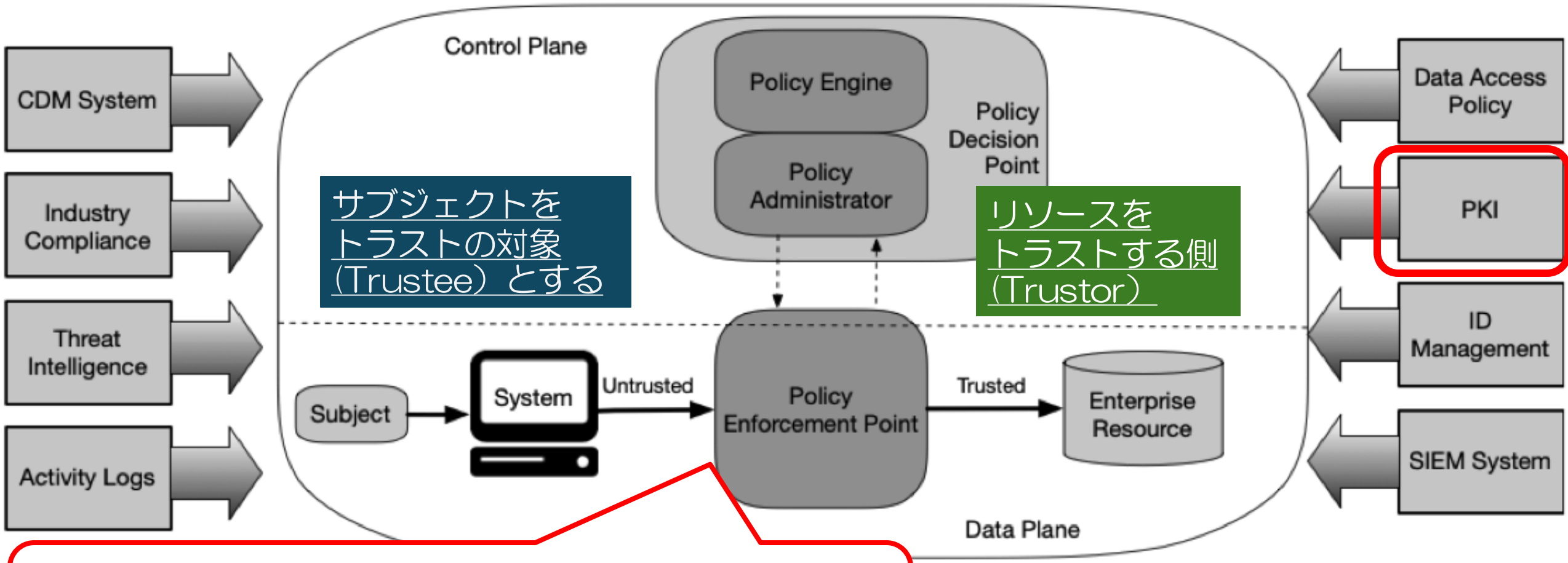
© 2023 SECOM CO., LTD　1

出典：
SecurityDay 2023
https://www.securityday.jp/past-events/securityday2023

https://drive.google.com/file/d/1aQ5RYf9HrSgpJMmLu1DcOQMTvt1ejGqt/view

Copyright 2025　NPO日本ネットワークセキュリティ協会

ゼロトラストアーキテクチャ　Never trust,　always verify
NIST SP800-207 (Zero Trust Architecture)



トラストの対象（Trustee）trustworthinessと、
アクセスするリソースの分類・性質などによる
ダイナミックなアクセス制御　→　トラスト管理

al Components

出典：
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Copyright 2025　NPO日本ネットワークセキュリティ協会

「Trusteeのtrustworthiness」は、変化する！なのでalways verify が必要

ソフトウェア更新
新機能追加

不正改造

サイバー攻撃

プライバシ侵害

ゼロデイ
攻撃

トラストの対象（Trustee）

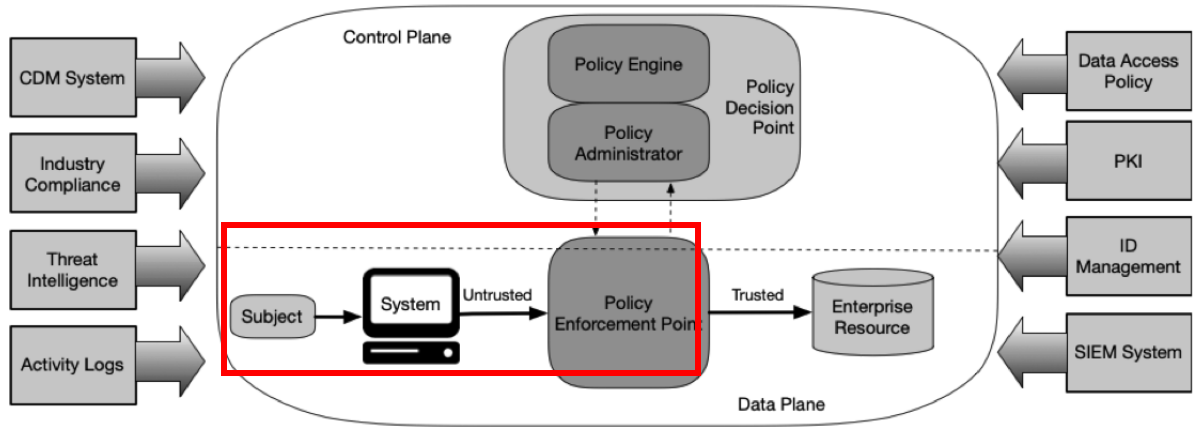
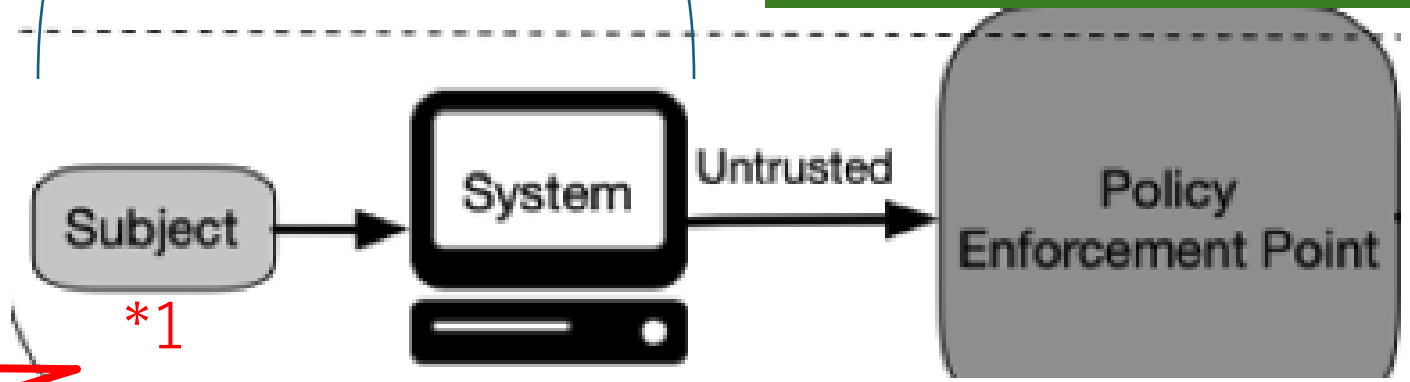


Figure 2: Core Zero Trust Logical Components

トラストする側（Trustor）



出典：
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

トラストの観点からは、ここでのSubject とsystemも併せて、トラストのSubject(対象者）と理解するのがよい？

Copyright 2025 NPO日本ネットワークセキュリティ協会

ゼロトラストアーキテクチャの一般化

トラストの対象(Trustee）が、トラストできない環境（ゼロトラスト環境）におかれたサブジェクト　→　　この際の公開鍵暗号・デジタル署名の役割を考えてみる

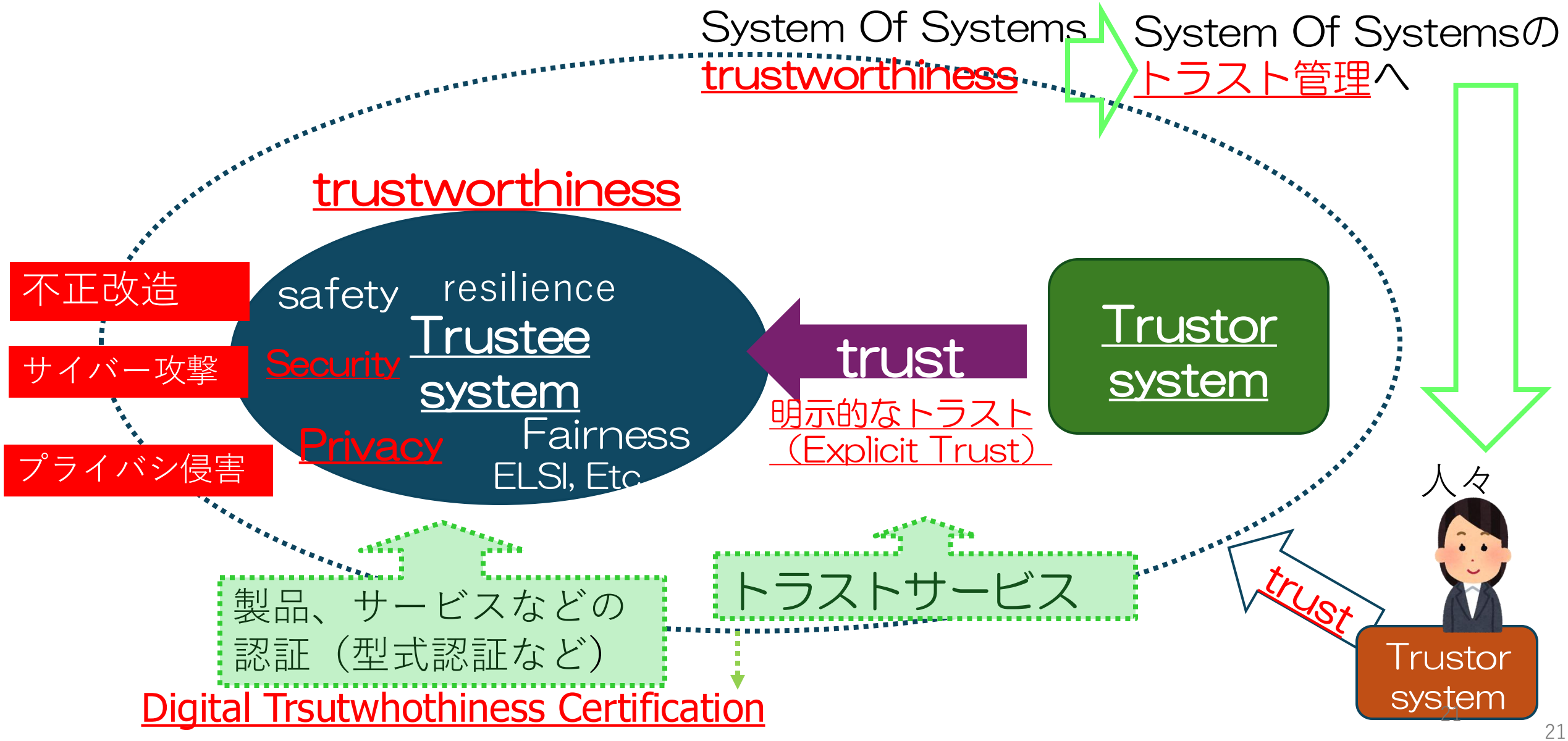
- ゼロトラストアーキテクチャにおけるNever trust, always verifyの意味するところ
  - Never trust　　->　Never　implicit trust　　暗黙のトラスト(implicit trust)をしない
  - always verify　　->　動的に検証することにより得られる明示的なトラスト(explicit trust)
- このalways verifyは、Trustee が意図した状態を保っているのか？（trustworthinessの検証）
  - プリミティブ的には、ほぼ、（公開鍵暗号による）デジタル署名とその検証
  - プロトコル的には、「リモートアテステーション」が利用される傾向にある
- リモートアテステーションにおけるデジタル署名の使い方
  - デジタルドキュメントにおけるデジタル署名の使い方
    - ドキュメント（のハッシュ値）に（署名者：人などが）署名を行い、RP/Verifier（検証者：人などの）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におけるデジタル署名の使い方
    - 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（システム）である Trustor,RP/Verifierが、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。
    - →　2025年現在、こうしたデジタル署名の使い方が急激に増えている？？

Copyright 2025 NPO日本ネットワークセキュリティ協会

System２System（ないし　Machine２ Machine ）のトラスト
さらに、System Of Systemsのtrustworthiness、トラスト管理へ

System Of Systems trustworthiness

System Of Systemsの トラスト管理へ



Copyright 2025　NPO日本ネットワークセキュリティ協会

ゼロトラストアーキテクチャにおける信頼の起点
→ always verify　検証するにしても信頼の起点が必要

- ゼロトラストにおける信頼の起点（および暗黙のトラスト）
  - ゼロトラストにおいても、信頼の起点は、（検証できず）暗黙的なトラストが置かれる
- 暗黙的なトラストが置かれるに相応しいセキュリティの要求
  - まずは、「公開鍵暗号アルゴリズム」に暗黙のトラストを置く
    - →　なのでPQC移行は大変
  - デバイスに組み込まれたHW Root Of Trust
    - ハードウェアセキュリティが非常に重要になっている一番の背景
  - トラストアンカーとなるPKIのRoot CAの公開鍵（＆プライベート鍵）
    - ゼロトラストでは、この公開鍵から全てがトラストチェーンで結ばれ、検証できることが理想的　→　この公開鍵は、トラストドメインにおいてトラストアンカーとなる裏付けが必要
- デジタル社会におけるゼロトラストアーキテクチーの適用
  - 企業内のゼロトラストではなく、マルチステークホルダー・エコシステム、さらには、社会全体においてゼトトラストアーキテクチャを適用を考えた場合
  - →　20年間、あまり顧みられなかった「電子署名法認定基準」は、とっても重要なのでは？？、
  - →　現状の電子署名法の適用範囲は、あまりのも狭い

Copyright 2025　NPO日本ネットワークセキュリティ協会

（欧州の）データスペースにおけるトラスト
信頼性（Trustworthiness）のデジタル証明という方向性

- DFFT（Data Free Flow with Trust）
- 欧州の　trust in data spaces
- 課題は、エコシステム・マルチステークホルダー間のトラスト

Copyright 2025　NPO日本ネットワークセキュリティ協会

Keidanren
Policy & Action

産業データスペースの構築に向けて
（概要）

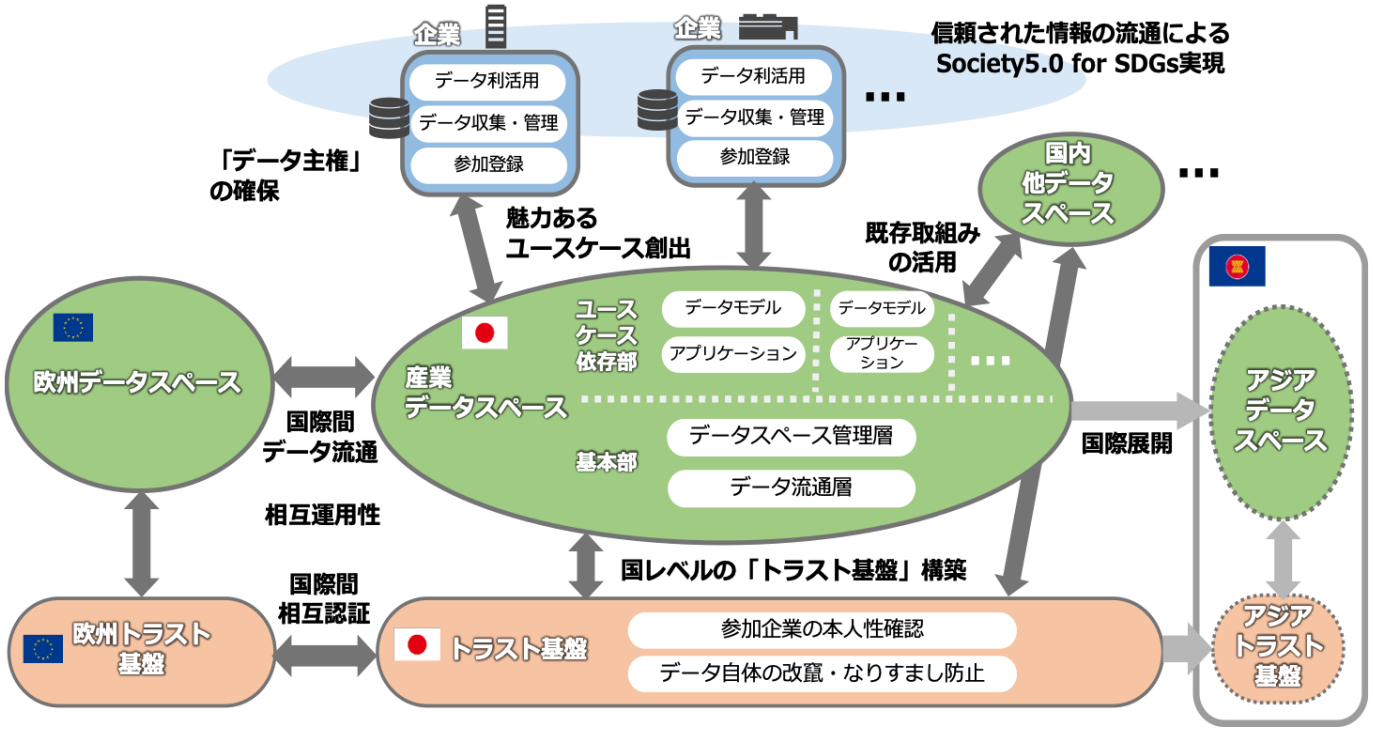
2024年10月15日
一般社団法人 日本経済団体連合会

https://www.keidanren.or.jp/policy/2024/073.html

DFFT（Data Free Flow with Trust）

図：目指すべき産業データスペースのイメージ

【出典】ロボット革命・産業IoTイニシアティブ協議会（RRI）



「EU等の海外の産業データスペースとの相互運性確保のため、トラスト基盤の国際相互運用承認や国際的なルール形成に関する議論を、日本がリードしていくことも必要となる」

松本の考えるトラスト基盤は、明示的トラストに必要な（証明と）検証のコストを、技術と法制度の相互運用性を確立するにより、最小化するための基盤

Copyright 2025 NPO日本ネットワークセキュリティ協会

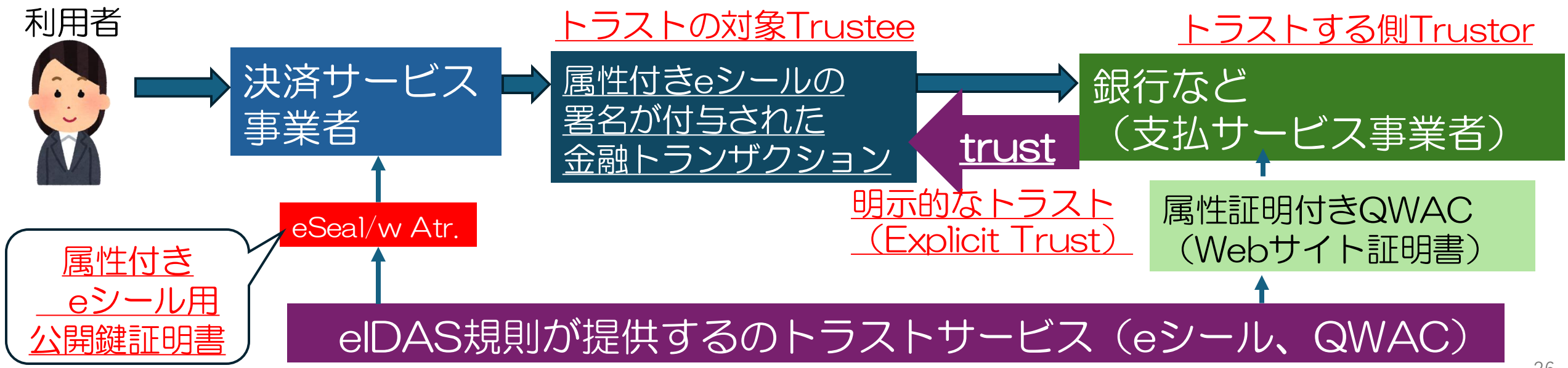
前提知識：電子署名、eシール、eIDAS2.0の属性アテステーションなどの道具

- 電子署名法における電子署名　　自然人による（否認防止のための）署名
  - 過去から存在する「民事訴訟法 228 条 4 項　→　私文書は、本人〔略〕の〔略〕押印があるときは、真正に成立したものと推定する」のデジタル文書への適用
  - 基本的に「人（自然人）が書いた（ヒューマンリーダブルな）文書を、人が目視で文書の内容（検証して）を読む」と言うことに関しては、デジタル社会以前と同様の目的
- eシール　　法人による署名　　eSeal/w Atr.
  - 欧州において2014年6月に成立したeIDASで法制化（日本おいては、総務省が検討中）
  - 適用範囲としては、現行の電子署名法の範囲よりも広い（今日の一般的なデジタル署名の使い方）
    - →　例えば「コード署名」　署名対象がプログラムコード、出自の証明、検証者が多数で自動的に検証してコードを実行　→　マシンリーダブルな署名対象が多い
  - 一般論としては、「機械が署名を行い、機械が署名検証を行う」といった方向に向かっている
    - DFFTのようなデータ連携、人の介在を最小にした自動化、スマート化、効率化などの際の、トレーサビリティ、トランスペアレンシー、アカウンタビリティなどの確保などに利用
- 属性アテステーション（Electronic Attestation of Attributes）、VC：Verifiable Credentials
  - 欧州において2024年6月に成立したeIDAS2.0では、この属性アテステーション（ないしVC）自体に信頼性を与えるための制度的フレームワーク　　attestation
  - 信頼の対象（Trustee,：企業、データなど）の属性証明（アテステーション）

Copyright 2025 NPO日本ネットワークセキュリティ協会

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



Copyright 2025 NPO日本ネットワークセキュリティ協会

欧州の「データスペース」におけるトラスト　by　Data Spaces Help Center　https://dssc.eu

trust in data spaces　のためのTrust Framework https://dssc.eu/space/BVE/357075461/Trust+Framework

- Summary
- このビルディング・ブロックの最初の重要な要素はトラストの概念である。この概念について一般的に受け入れられている定義*によると、トラストとは、ある約束が果たされる当事者のreliability 、 truth 、 abilityに対する確固たる信念（ firm belief ）と定義されている。
- データスペースの文脈では、この定義は以下のことを意味する：
- トラストまたは不信（ distrust ）は、意思決定当事者が設定する閾値の結果であり、提供された証拠からトラストレベルを決定するリスク評価**に基づく。
- この証拠とは、卒業証明書や運転免許証など、特定の文言を証明するものである。
- データ・スペースにおけるトラストの 概念は、トラストレベルを決定するために意思決定当事者がリスク・アセスメントを行うことを支援するための一連のルールへの準拠に変換することができる。これは、透明性、セキュリティ、制御性(controllability)、相互運用性に関する情報を提供する技術的枠組みを通じて検証することができる。
- その出発点は、データスペースの要件、基準、規制の必要性を概説したデータスペース・ガバナンスのフレームワークである。
- これらの要求事項や基準を厳格に遵守することで、参加者間の信頼と信頼性の最低基準レベルが保証される。
- 認定トラスト・アンカー（Accredited Trust Anchors）は、様々な検証メカニズムを用いて、参加者の自己宣言（self-declarations）や追加属性などの主張の正確性（accuracy）と正当性（legitimacy）を検証することができる。
- 第二に、法的、意味的、組織的、技術的な相互運用性レイヤーを提供する欧州相互運用性フレームワーク（EIF）によって明確に認識されているように、相互運用性はこのビルディングブロックの重要な構成要素である。
- ここで説明するトラストフレームワークは、ガイドラインと最も一般的に使用されるメカニズムの基礎を提供することで、組織的および意味的相互運用性レイヤーを特に扱っている、
- 例えば、ポリシー、権利、義務などを表現する共通言語としてODRL（Open Digital Rights Language）を使用する。

データスペース
データ交換

データの信頼性・トラスト
トラストフレームワーク

eIDAS2.0トラストサービス
eシール
属性アテステーションなど

「透明性、セキュリティ、制御性(controllability)、相互運用性に関する情報を提供する技術的枠組みを通じて検証することができる」
→　eIDAS. eシール・デジタル署名、属性アテステーションの検証に落とし込む。
データの出自の証明だけでなく参加する企業や提供するデータの信頼性（ trustworthiness ）の証明へ

Copyright　2025　NPO日本ネットワークセキュリティ協会

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

authorized source

公証人
eSeal/w Atr.

業界特有の
適合性評価
eSeal/w Atr.

ある分野の
管轄官庁
eSeal/w Atr

eSeal/w Atr. 署名に使用されるQeSeal 公開鍵証明書

attestation 属性証明（署名者が存在する）

ある分野データスペースXのトラストドメイン

紙のある
証拠を変換
attestation

適合性評価の
証明など
attestation

許認可など
attestation

トラストの対象Trustee

データを販売する企業
eSeal/w Atr.

eSeal　署名されたデータ
タイムスタンプの付与

トラストする側Trustor

データを購入する企業

trust

明示的なトラスト
（Explicit Trust）

attestation
自己宣言書
（自分で署名）

attestation
データスペース会員証

eSeal/w Atr.
データスペース・ガバナンス・オーソリティ

eシール、証明書、属性証明など
の検証のためのトラストアンカー

eSeal/w Atr.
eシール QSTP

eSeal/w Atr.
QEAA（Qualified Electronic Attestation of Attributes）

eSeal/w Atr.
デジタルタイムスタンプ

トラストリスト

クオリファイ・トラストサービス

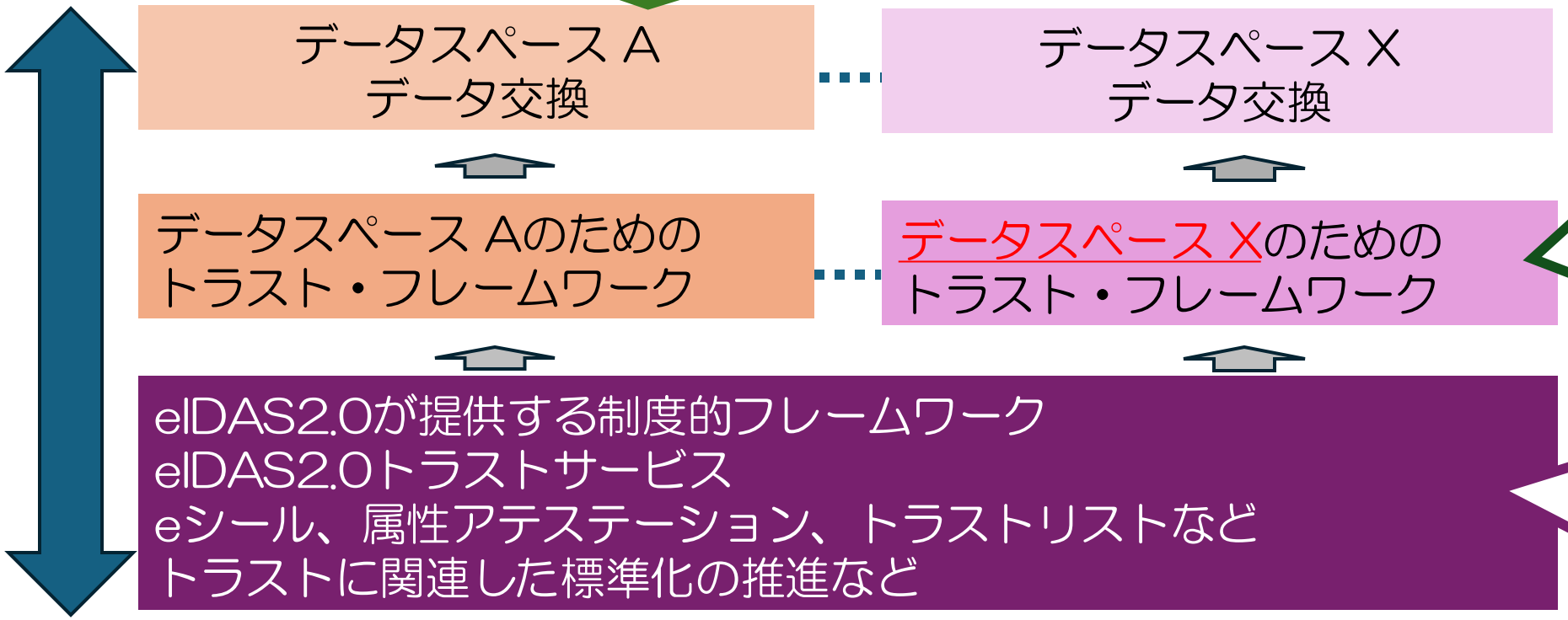
Copyright 2025 NPO日本ネットワークセキュリティ協会

トラスト基盤？？　２階層？？

Trustworthinessは、個々のデータスペースの依存性が強い
トラストメカニズムは、なるべく共通に（そのための標準化もeIDAS2.0の役割）

データスペースにおけるステークホルーダーは、個々のデータスペース毎に大きく異なる。同様にデータのTrustworthinessも個々のデータスペース毎に大きく異なる。

業界APLより



社会基盤より

データスペースにおけるトラストフレームワークは、属性証明≒信頼性（Trustworthiness）証明のフレームワークに向かっている。

eIDAS, eIDAS2.0の大きな役割の一つは、（産業）分野などによるフラメンテーション（細分化）を防ぐことにある。

Copyright 2025　NPO日本ネットワークセキュリティ協会

公開鍵暗号・デジタル署名によるトラストの考え方の変遷

- 2001年の電子署名法的な考え方　　署名対象は、ヒューマンリーダブル
  - 署名者による否認防止のための署名　　→　署名者は、署名した文書の内容を否認できない
  - ＃署名者や、署名対象である文書自体の信頼性（Trustworthiness)は、電子署名法の対象外
- 2019年　PSD2（ eIDAS1.0　eシール　＋　QWAC ）　→　署名対象は、マシンリーダブル
  - 出自に関しては、属性付きeシールによる欧州の金融監督官庁が認めた決裁指示サービス事業者による要求（署名）であることが証明される。
  - 金融監督官庁の監督のもと、署名者（決裁指示サービス事業者）自体の一定の信頼性（Trustworthiness)が保たれる。
    - ＃なんらかの重大なインシデントが生じたい場合は、監督官庁が認可などを取り消す??
  - 署名されるトランザクションは、決裁指示サービス事業者の責任として作成する。
- 2025年　欧州のデータスペースの方向性
  - 標準化された信頼性がある属性証明（attestation）の利用
    - 署名者や、署名対象のデータ自体の信頼性（Trustworthiness)の証明へ
    - 属性証明の集合が、信頼性（ Trustworthiness ）証明へ
  - 法人やデータの信頼性（Trustworthiness)の実行時のリアルタイムな検証
    - Trustor・リライングパーティの判断も自動化
    - →　これは、「ゼロトラストアーキテクチャ」ともいえる

Copyright 2025　NPO日本ネットワークセキュリティ協会

まとめ

改めて考えるデジタル社会における公開鍵暗号の重要性

「暗号と社会の素敵な出会い」から
「暗号と社会の素敵な関係」に向けて

Copyright 2025 NPO日本ネットワークセキュリティ協会

改めて考えるデジタル社会における公開鍵暗号の重要性
-- 続・続・暗号と社会の素敵な出会い --

- 現代社会における様々な社会的問題は、トラストに起因していることが多いと言えます。Trusteeの信頼性（trustworthiness）が、Trustorからトラストに伝わらないこと、また、信頼に値しないTrusteeを、Trustorがトラストしてしまうといったことが、様々な不信（distrust）や分断を生んでいるとも言えます。
- このように、デジタル社会に向かって、トラストに関わる様々な課題が浮上していますが、デジタル技術により社会が変わると考えるのならば、当然、こうした問題を内在している現在のトラストのメカニズムも変わるべきとも言えます。
- # 多分、改竄が容易な「羊皮紙」から「紙」に移行した際にもトラストのメカニズムは変わったと考えられますが、これよりもはるかに大きな変化がデジタルへの移行
- こうした中、新たなトラストメカニズムの一つとして、現状の「暗黙的なトラスト」が強い状況から、公開鍵暗号などを利用した「明示的なトラスト」などの実装による、より「明示的なトラスト」が可能な状況へのシフトが考えらます。
  - #ここは、そんなに安易に書ける話ではないことは重々承知の上で、また、そうした議論が浮上することも期待して。。。
- 信頼に値するTrusteeの信頼性（trustworthiness）がTrustorが検証は、デジタル社会におけるゼロトラストアーキテクチャの適用だとも捉えられることも出来きます。
- 2000年に成立した電子署名法は、公開鍵暗号が法制度に組み込まれたという意味において、暗号と社会の画期的な出会いでしたが、これを発展させて「（公開鍵）暗号と社会の素敵な関係」築くことこそがデジタル社会におけるトラストの確立に大きく貢献すると考えらます。

Copyright 2025 NPO日本ネットワークセキュリティ協会

今後の暗号・セキュリティ分野の研究に対する期待
デジタルトラストから見た２つの側面の研究のアプローチ

- 暗号・セキュリティ分野において、信頼の基点（暗黙のトラスト）には、信頼に値すること(信頼性：trustworthiness)のセキュリティが必要
  - ＃これらは、デジタル社会を裏で支える仕組み（それがトラスト）であり、それが故に、理解が得にくいかもしれない
  - 暗号アルゴリズム　　PQCの評価と、PQC移行は、暗号アルゴリズムに暗黙的なトラストを置く上で、非常に重要
  - トラストアンカーとなる暗号鍵管理　（電子署名認定基準など）
  - RoTなどのセキュアな暗号鍵を扱うハードウェアセキュリティ、プラットフォームセキュリティ
  - こうしたデジタル社会を裏で支える仕組みであるが故に、理解が得にくい研究分野
- デジタル社会における検証可能な仕組み（ゼロトラストアーキテクチャ）
  - 「明示的なトラスト」が可能な仕組みを、広くデジタル社会に実装することが一つの解決策として考えられる（マルチドメイン環境におけるゼロトラストアーキテクチャ）
    - SystemOfSystemsのトラスト管理（ リモートアテステーション、etc.. ）
    - Trusteeのtrustworthiness を明示的に伝える「明示的なトラスト」は、 Trusteeのtrustworthinessを高めるインセンティブにつながる！！
    - →. このインセンティブこそが、社会全体のセキュリティを高めることにつながる

Copyright 2025　NPO日本ネットワークセキュリティ協会

付録

- トラストに関する議論の紹介
- TrustとTrustworthinessの説明
- トラストアンカーをめぐる対立
- その他

Copyright 2025 NPO日本ネットワークセキュリティ協会

トラストに関する議論の紹介

Copyright 2025　NPO日本ネットワークセキュリティ協会

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

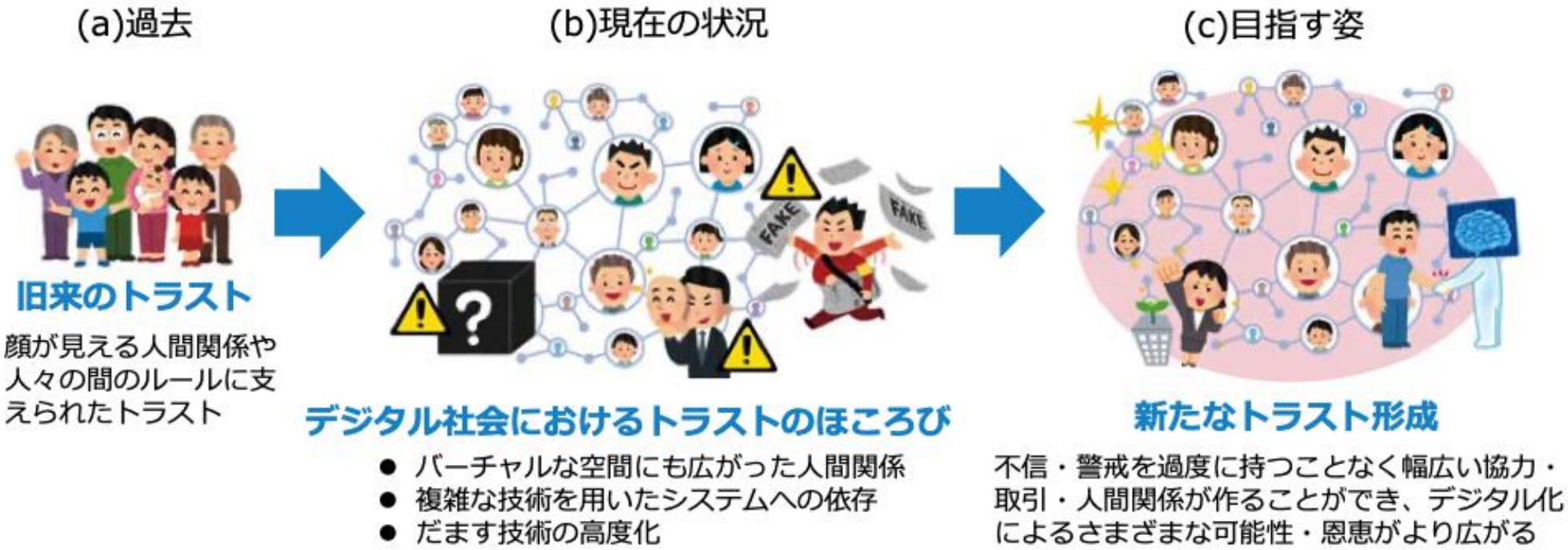


図1-1　デジタル社会におけるトラストの問題認識と目指す姿

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

松本の考えとしては、デジタル技術が社会の仕組みを変えると考えるのならば、当然、トラスト（ないしトラストメカニズム）も仕組みも変わっていく

CRDS 研究開発戦略センター

Copyright 2025　NPO日本ネットワークセキュリティ協会

トラストって何よー??

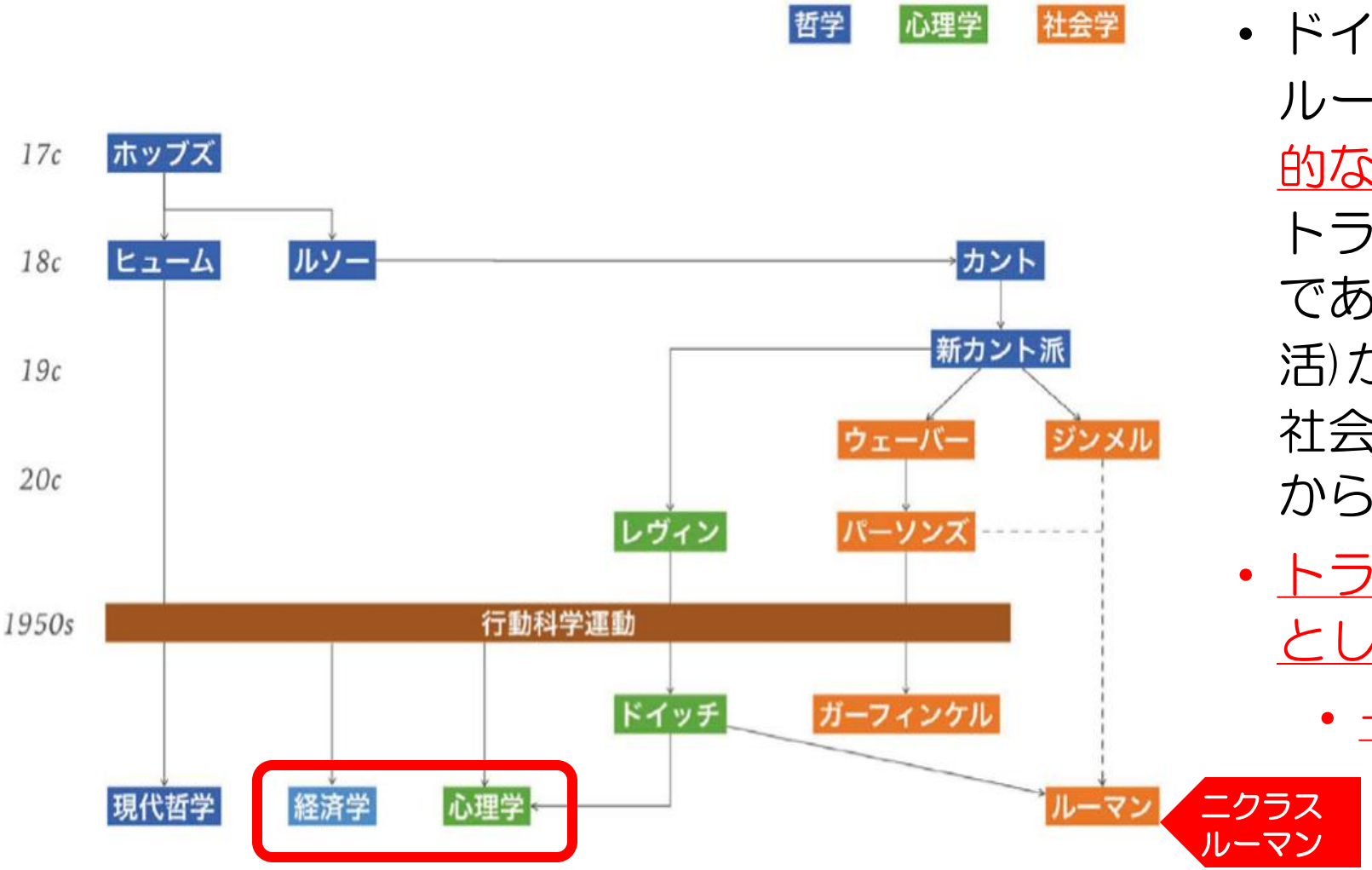


図 2-1-3　　信頼研究の系譜[3]

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

Copyright　2025　NPO日本ネットワークセキュリティ協会

JST（科学技術振興機構）CRDS（研究開発センター）の俯瞰報告書

- JST CRDS 俯瞰報告書
  - 2年毎に発行
  - 最新版（2023年版）は、2023年5月公開
  - ４つの分野（147の開発領域）
  - 4つの分野の一つが「システム・情報科学技術」
- 「システム・情報科学技術分野」
  - 706ページ
  - 2.4 セキュリティー・トラスト
    - 2.4.5 システムのデジタルトラスト

セキュリティ＆トラストの俯瞰を目指した？

松本が執筆協力

出典：https://www.jst.go.jp/crds/report/CRDS-FY2022-FR-04.html

Copyright 2025 NPO日本ネットワークセキュリティ協会

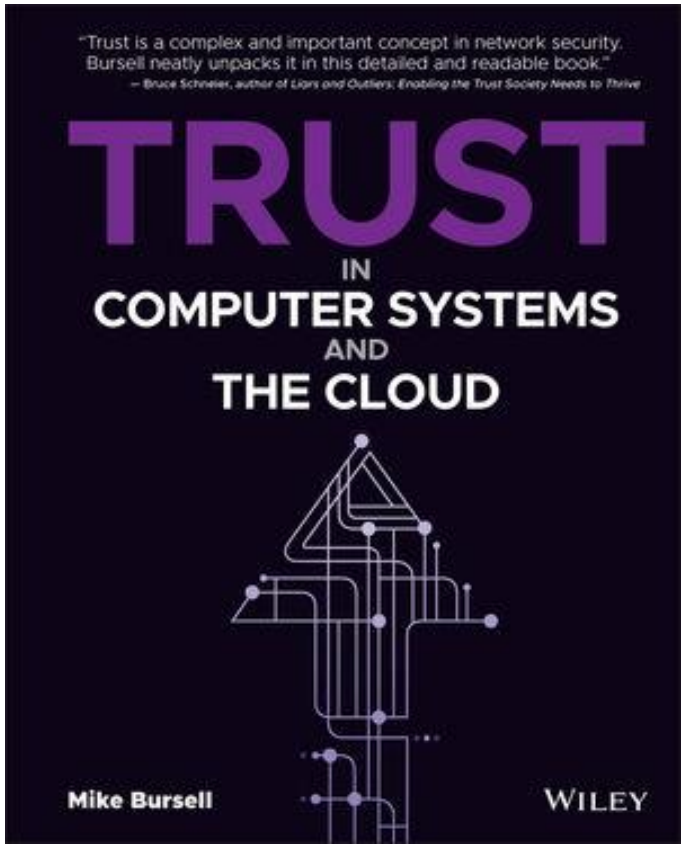
2.4.5 システムのデジタルトラスト

出典：
https://www.jst.go.jp/crds/report/CRDS-FY2022-FR-04.html
https://www.jst.go.jp/crds/pdf/2022/FR/CRDS-FY2022-FR-04/CRDS-FY2022-FR-04_20405.pdf

- (1) 研究開発領域の定義
  - サイバー空間とフィジカル空間を高度に融合したシステムによる Society5.0 では、そこに参加するステーク ホルダーが増加し、システムの数も膨大となる。暗号技術が組み込まれたコンピューティング技術を用いて、人を介さずに自動的に複数のステークホルダーの複数のシステム間における信頼関係を検証・確立し、信頼できるシステムによる情報サービスの提供を実現するシステムのデジタルトラストに関する研究開発を行う領域である。
- (3) 研究開発領域の概要［本領域の意義］
  - サイバー空間とフィジカル空間を高度に融合した Society5.0 においては、あらゆるもののデジタル化・コネ クティッド化、スマート化・自律化が進み、さまざまなステークホルダーのシステムが参加することにより社会に価値を提供すると考えられる。この際、各ステークホルダーのシステム間における信頼関係の確立が必要となる。一方で「あらゆるもののデジタル化・コネクティッド化」という観点からは、膨大な数の信頼関係の 確立とその維持が必要となり、「スマート化・自律化」という観点からは、人を介さないダイナミックな信頼 関係の確立が要求される。（。。。続く）

Copyright 2025 NPO日本ネットワークセキュリティ協会

トラストに関する参考図書



著者のマイク・バーセル氏は、「ゼロトラスト」は、「“explicit trust”」と呼ばれる方が良いと主張している。

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

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

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、「信頼の値すること（信頼性）の重要性」
→　信頼性（trustworthiness)のある trusteeがトラストされることの重要性

Copyright 2025　NPO日本ネットワークセキュリティ協会

TrustとTrustworthinessの説明

Copyright 2025 NPO日本ネットワークセキュリティ協会

D2.5 – Consolidated report on the socio-economic basis for trust and trustworthiness.　2015年　欧州のFP7のプロジェクトの成果物

OPTET Operational Trustworthiness Enabling Technologies

- Trust in a system is defined as a property of a stakeholder (known as the trustor) reflecting the strength of their belief that engaging in the system for some purpose will produce an acceptable outcome.
- システムに対するトラスト(Trust in a system)は、ある目的のためにシステムに関与することで、許容できる結果が得られると信じる強さを反映したステークホルダー（ trustorと呼ばれる）の特性として定義される。
- Trsutwhorthiness on the other side is a property of the system. A system is more trustworthy if it is able to produce an outcome acceptable to all trustors.
- 一方、 Trustworthinessはシステムの特性(property)である。すべてのtrustorに受け入れられる結果を出すことができれば、システムはよりトラストできる。

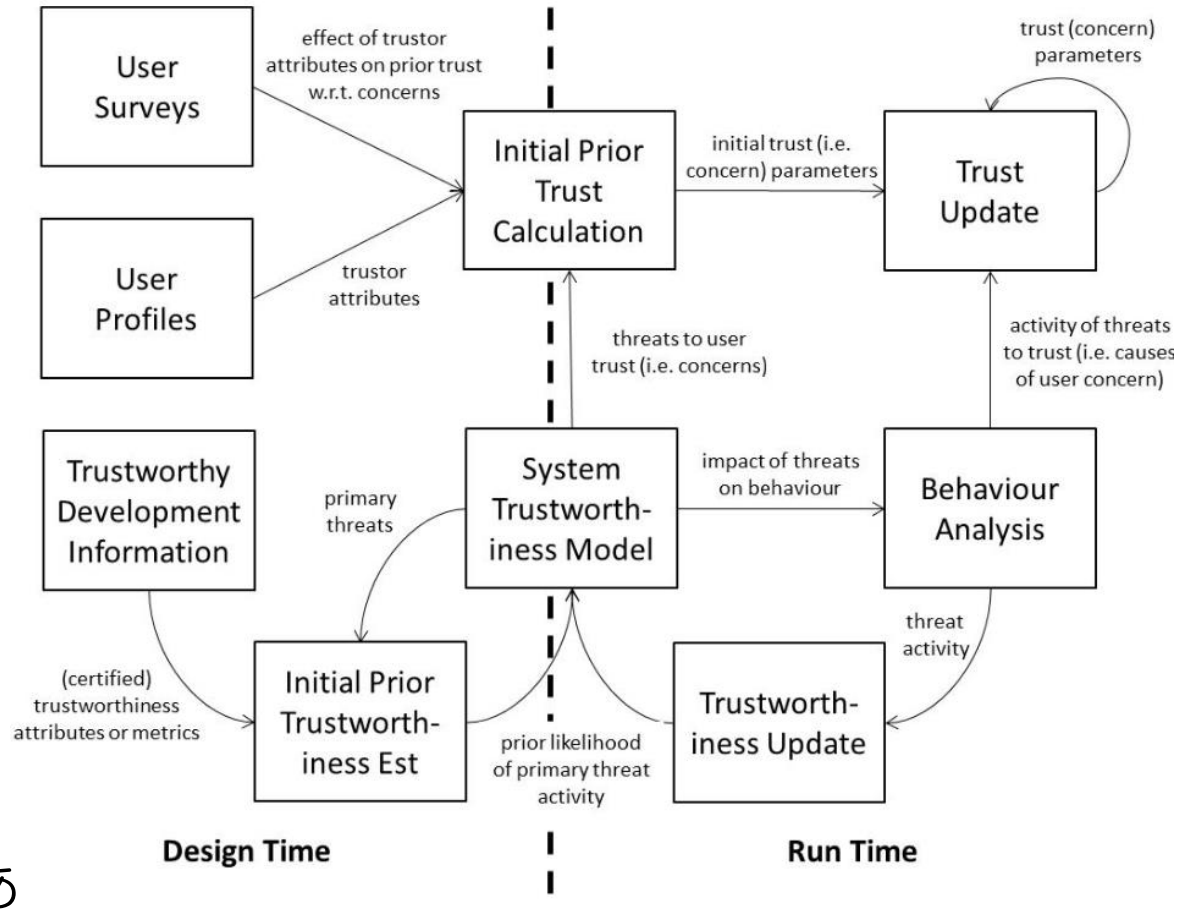


Figure 1. OPTET WP2 Modelling Approach

設計時とサービス時の二つのTrsutwhothinessモデルを示している

**. Executive Summaryの冒頭の文書

出典：https://eprints.soton.ac.uk/410774/1/OPTET_WP2_D2_5_v1_0.pdf

Copyright 2025　NPO日本ネットワークセキュリティ協会

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

- 原文
  - Amongst other things, this document is about trust and　trustworthiness.
  - Trust is a choice one makes about another system.
  - Trustworthiness is a quality about the other system that can be used in making one's decision to trust it or not.
  - This is subtle difference and being familiar with the difference is crucial for　using this document.
  - Additionally, the concepts of freshness and　trust relationships with respect to RATS are elaborated on to enable implementers to choose appropriate solutions to compose their Remote　Attestation Procedures.

Freshness(鮮度）は、 always (verify)と同意

- 仮訳
  - 中でも、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、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、他のシステムに関する品質です。
  - これは微妙な違いであり、この違いをよく理解しておくことはこのドキュメントを使う上で非常に重要です。
  - さらに、RATSに関する鮮度とトラスト関係の概念について詳しく説明し、実装者がリモートアテステーション手続きを構成するために適切なソリューションを選択できるようにする。

TrustとTrustworthiness の使い分けが、非常に重要
（日本語に訳した場合、ここが曖昧になることが多い？？）

Copyright 2025　NPO日本ネットワークセキュリティ協会

トラストアンカーをめぐる対立

eIDAS2.0 45条QWACをめぐるブラウザベンダーと欧州の対立

QWAC : Qualified certificates for website authentication

Copyright 2025 NPO日本ネットワークセキュリティ協会

eIDAS2.0 45条QWAC

- 第45条
- ウェブサイト認証用適格証明書の要件
- 1.　ウェブサイト認証用適格証明書は、Annex IV に定める要件を満たすものとする。これらの要件への準拠の評価は、本条第 2 項で言及される基準、仕様、手順に基づき実施される ものとする。
- 1a.　本条第 1 項に従って発行されたウェブサイト認証用適格証明書(QWAC: Qualified certificates for website authentication)は、ウェブ・ブラウザのプロバイダによって承認されるものとする。ウェブ・ブラウザのプロバイダは、証明書に証明される身元データおよび追加的に証明される属性が、ユーザにとって使いやすい方法で表示されることを保証するものとする。（中略）
- 2.　欧州委員会は、2025 年 5 月 21 日までに、実施法（ Implementing Act ）によって、参照基準のリストを確立し、必要に応じて、本条第 1 項に言及するQWACの仕様および手順を確立するものとする。これらの実施法は、第48条2項に規定される審査手続きに従って採択されるものとする；
- 第45a条
- サイバーセキュリティの予防措置
- 1.　ウェブ・ブラウザのプロバイダは、第 45 条に定める義務、特にQAWCを認識する義務、および提供された アイデンティティデータをユーザーフレンドリな方法で表示する義務に反するいかなる措置も講じてはならない。
- 2.　第 1 項の適用除外として、特定された証明書または一連の証明書のセキュリティ侵害または完全性の喪失に関して実証された懸念がある場合に限り、ウェブ・ブラウザのプロバイダは、当該 証明書または一連の証明書に関して予防措置を講じることができる。
- （後略）

民間のサービス・製品であるブラウザのトラストリストに欧州の法制度が介入を強制する。属性の表示も非常に重要。

ブラウザベンダーが猛烈に反発？？

ブラウザベンダーによるTSP「取り潰し」の余地を残す

欧州の視点からは、欧州の重要インフラ事業者であるQTSPの生存権をブラウザベンダー・米国プラットフォーマに委ねることにもなる。

Copyright 2025　NPO日本ネットワークセキュリティ協会

MozillaによるQWAC(eIDAS45条）反対キャンペーン

https://securityriskahead.eu

When using the internet, your browser protects valuable information you send to websites. The first draft of eIDAS forced browsers to accept QWACs – lower-security standard website certificates and providers that issue them. This would lower the bar for protection and open up users to possible malicious attacks and online crime.

Update 29/02/2024: After two years of review by EU legislators, critical changes in the law were approved in a vote in the European Parliament. This means EU citizens can continue to safely browse the web, provided the law is implemented correctly.

QWAC（適格ウェブサイト認証証明書）に対するEUの現在のアプローチは、オープン・ウェブのセキュリティを弱体化させるだろう
ウドバフ・ティワリとベン・ウィルソン　2020年10月8日
https://blog.mozilla.org/netpolicy/2020/10/08/the-eus-current-approach-to-qwacs-qualified-website-authentication-certificates-will-undermine-security-on-the-open-web/

1998年の設立以来、Mozillaは人権に準拠したイノベーション、そしてインターネット上の人々のための選択、コントロール、プライバシーを支持してきました。私たちは、インターネットを推進するウェブ標準の作成を積極的にリードし、参加することによって、ウェブ上の何十億ものユーザーのためにこの信念を実現するために努力してきました。私たちは最近、eIDAS規制に関する欧州委員会の調査および公開協議に意見を提出し、ユーザーのセキュリティにとってより良いeIDASの解釈を提唱し、グローバルインターネットの革新と相互運用性を維持することを主張しました。
ウェブサイト・セキュリティのためのトランスポート・レイヤー・セキュリティ（TLS）標準を策定した背景を考慮すると、適格ウェブサイト認証証明書（QWAC）をTLS証明書とバインドすることを義務付けるeIDASの解釈は、深く懸念されるものであると考える。ユーザーのセキュリティを弱めるだけでなく、欧州の単一デジタル市場とグローバル・インターネットにおけるその地位にも深刻な弊害をもたらすだろう。
欧州委員会の調査に対する我々の最近の複数の提出書類で明らかにされた、このような立場をとるいくつかのハイレベルな理由は以下の通りである：
QWAC（適格ウェブサイト認証証明書）に対するEUの現在のアプローチは、オープン・ウェブのセキュリティを弱体化させるだろう。

Copyright 2025 NPO日本ネットワークセキュリティ協会

https://last-chance-for-eidas.org

- eIDASを修正する最後のチャンス：インターネットのセキュリティを脅かすEUの秘密法
  - 2023年11月2日
  - 長年の立法プロセスを経て、eIDAS規則のほぼ最終的な文章がEUの主要機関を代表する政治的三者（ trialogue ）協議の合意され、年内に国民と議会に提出され、承認される予定である。
  - 最近の非公開会議で導入され、まだ公開されていない新しい法律条文は、欧州で配布されるすべてのウェブ・ブラウザが、EU政府によって選択された認証局と暗号鍵をトラストすることを要求されることを想定している。
  - これらの変更により、政府の管理下にある暗号鍵がEU全域で暗号化されたウェブトラフィックを傍受できるようになり、EU政府が市民を監視する能力が根本的に拡大する。
  - どのEU加盟国も、ウェブブラウザで配布する暗号鍵を指定する能力を持ち、ブラウザは政府の許可なしにこれらの鍵の信頼を失効することを禁じられている。
  - これにより、どのEU加盟国の政府も、傍受と監視のためにウェブサイト証明書を発行することができる。加盟国が許可する鍵やその使用に関して下す決定に対して、独立したチェックやバランスは存在しない。
  - 法の支配の遵守がすべての加盟国で一様でなく、政治的目的のために秘密警察によって強制された事例が記録されていることを考えると、これは特に問題である。
  - （中略）
  - 学界、市民社会、産業界にまたがる抗議
    - 世界中の500人以上のサイバーセキュリティ専門家や研究者が、EUにこれらの計画を放棄し、ウェブを保護するよう求める公開書簡に署名しました。
    - （中略）
    - サイバーセキュリティの専門家、研究者、またはNGOの代表である場合は、https://eidas-open-letter.orgで公開書簡に署名することを検討してください。

Copyright 2025 NPO日本ネットワークセキュリティ協会

欧州の事業者団体（QTSP)による反論

https://www.european-signature-dialog.eu/ESD_answer_to_Mozilla_misinformation_campaign.pdf

- なぜMozillaはこのような誤情報を流すのか
- Mozillaは一般的にGoogleのサテライトとして認識されており、Googleが自らの商業的利益を押し通すための道を開いている。
- Mozillaは2000- 2009年には、30%マーケットシュアを持ち独立したブラウザとして高く評価されていました 。
- 今日、 Mozillaマーケットシュアは、わずか３%であり、は財政的に苦しんでいる。
- 対照的に、Googleは現在65%の 世界市場シェアを持っており、ヨーロッパでは支配的なブラウザであり、事実上すべての人のためのルールを設定する。
- Mozillaは今や一般的に、Googleのすべてのポリシーに従うGoogleのサテライトに過ぎないと見られている（証明書発行者の信頼を担当するMozilla委員会にGoogleのスタッフが含まれているほどだ）。
- MozillaがGoogleから受け取る資金なしで運営を続けられるかどうかは不明だ。
- 2020年の記事によると、MozillaがFirefoxで行われるすべての検索にGoogleの検索エンジンを裏で使用しているという理由だけで、GoogleがMozillaに年間4億ドルから4億5000万ドルを支払うという ものである。
- ある記事によると、これはMozillaの通常の収入源のおよそ92%に相当する。MozillaはGoogleに大きく依存しており、業界の多くはMozillaの方針決定はもはやGoogleから独立していないと考えている。
- （中略）

Copyright 2025 NPO日本ネットワークセキュリティ協会

欧州の事業者団体（QTSP)による反論　　続き

https://www.european-signature-dialog.eu/ESD_answer_to_Mozilla_misinformation_campaign.pdf

- MozillaとGoogleは、すべてのQTSPと競合するウェブサーバ証明書発行会社に出資している
- Mozilla（とGoogle）は、「Let's Encrypt」と呼ばれる、すべてのQTSPと競合するウェブサーバ証明書発行会社の事実上の出資者（プラチナレベルのスポンサー）である
- Let's Encryptは、所有者の身元情報を持たない匿名証明書のみを発行しており、何千ものこれらの証明書が、Mozillaブラウザでフィッシングやマルウェアのウェブサイトを「安全」と表示するために使用されている。
- 近年、Mozillaを含むブラウザは匿名証明書を好んでいるように見え、その結果、彼らは2019年に以前のQTSPアイデンティティUI（ユーザーインターフェース）を削除し、EUのユーザーはもはや違いを見分けることも、ウェブサイトが確認されたアイデンティティ情報によってサポートされていることを知ることもできなくなった。
- これらの潜在的な理由はどれも、MozillaがeIDASのウェブサイトに掲載した深刻な誤報を 正当化するには十分ではない。
- ドイツの独占禁止法当局でさえ、過去のブラウザの行動やeIDAS第45条見直しへの反対が、EUとドイツの独占禁止法に違反する可能性があると深刻な懸念を表明している(*1)。
- EU議会と理事会のメンバーは、偽ブラウザのロビー活動を無視し、欧州市民のオンライン・セキュリティを向上させるeIDAS第45条を支持すべきである。

*1. Proceedings in Transport Layer Security Certificates against Google terminated
https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2022/B7-250-19.pdf?__blob=publicationFile&v=4

Copyright 2025　NPO日本ネットワークセキュリティ協会

ドイツ最大のデジタル関連団体であるBitkomの見解
Position Paper　2023/12　　Bitkom on eIDAS 2.0 and QWACs

- 概要
- 11月8日に行われた政治的三者協議の結果、eIDAS規則の最終的な妥協が成立した。ITRE-委員会での投票を前に、この規則の最終版について、第45条をめぐって多くの論争が起きている。
- この規制の最終版に関するITRE-Committeeでの投票を前に、第45条とQWAC（Qualified Website Authentication Certificates）をめぐる多くの論争があった。
- ドイツ最大のデジタル関連団体であるBitkomは、現行版のeIDAS規則全体と、特に第45条の改訂を、明確かつ強固に支持している。
- 特に欧州加盟国によって導入される可能性のあるスパイウェアに関する予言された疑惑は、規制上も技術上も間違っている。
- それどころか、BitkomはQWACと改正されたArticle. 45は、欧州のデジタル主権を強化するための中心的なツールである。
- Bitkomは、QWACと改正された第45条を、欧州デジタル主権、欧州市場、欧州消費者保護を強化するための中心的な手段であると考えている。
- QTSPは、セキュリティとプライバシーに明確に焦点を当てた、独立監査人による定期的かつ精力的な監査プロセスと適合性評価を受ける。
- このように、EUは多くのチェック・アンド・バランスを構築し、不正行為に対する高い基準と障壁を設けている。
- 我々は、ITRE委員会の全メンバーに対し、事実と、交渉の失敗が、欧州におけるデジタル化の将来と、すべての欧州加盟国とその国民のデジタル主権に及ぼす影響について検討するよう強く求める。

出典：　https://www.bitkom.org/sites/main/files/2023-11/291123-Bitkom-on-QWACs-in-eIDAS.pdf

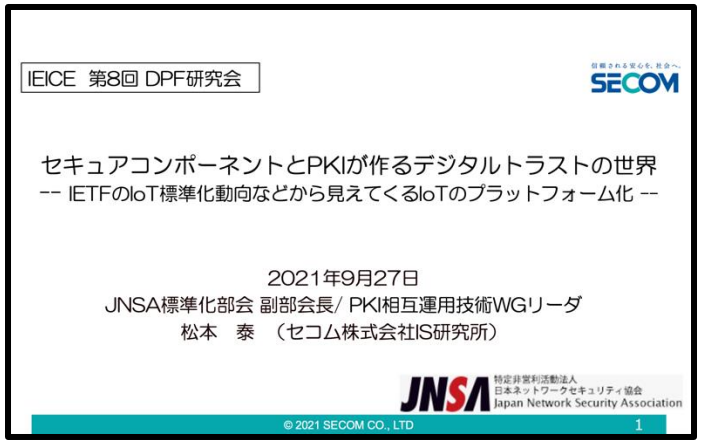
Copyright 2025　NPO日本ネットワークセキュリティ協会

その他

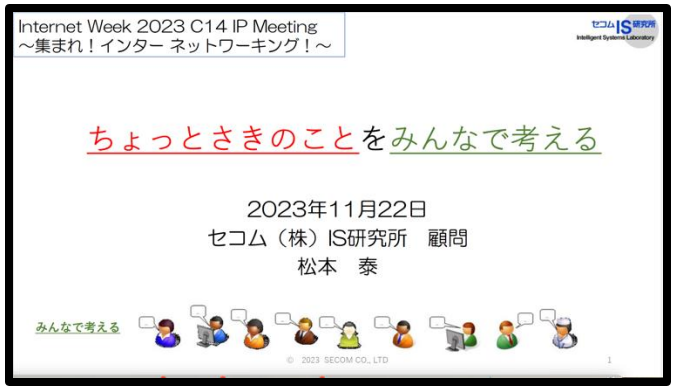
Copyright 2025 NPO日本ネットワークセキュリティ協会

本日の講演に関連した比較的最近の講演など（公開されている講演資料など）

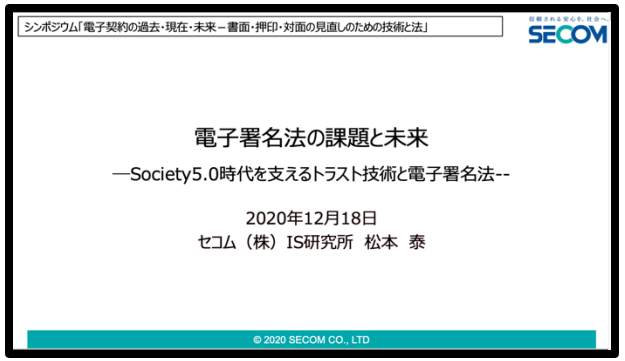
2024年
PKIコミュニティー向け
https://www.nic.ad.jp/ja/materials/workshop/20240307/20240307-mathumoto.pdf



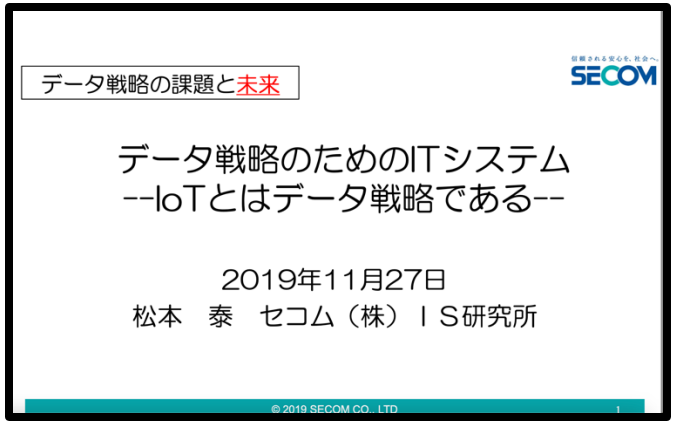
2019年
デジタルサービスプラットフォーム研究会
https://www.ieice.org/~dpf/wp-content/uploads/2021/08/松本DPF研究会.pdf



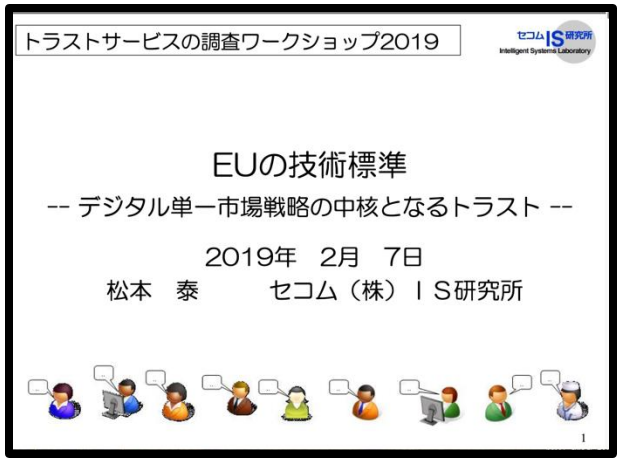
2023年
インターネットコミュニティ向けトラスト話
https://www.nic.ad.jp/ja/materials/iw/2023/proceedings/c14/c14-matsumoto.pdf



2020年
弁護士などの法律家向け
https://www.jlf.or.jp/wp-content/uploads/2021/01/itsympo2020siryou5.pdf



2019年
弁護士などの法律家向け
https://www.jlf.or.jp/assets/work/pdf/kenshu_190910_04.pdf



2019年
トラストサービス関係者向け
https://itresearchart.biz/19ws207/docs/s03.pdf

Copyright 2025 NPO日本ネットワークセキュリティ協会

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

JNSA

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

Untrusted network or
zero trust network

TRUST・
Verifiable, Always Verify

RP
Trustor

Web3
Trusted Webの議論

AML（Anti-Money Laundering）の議論
FATF対応

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

qualified　electronic attestation of attributes　by eIDAS2.0

Trusted device
Root Of Trust

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）

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

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。

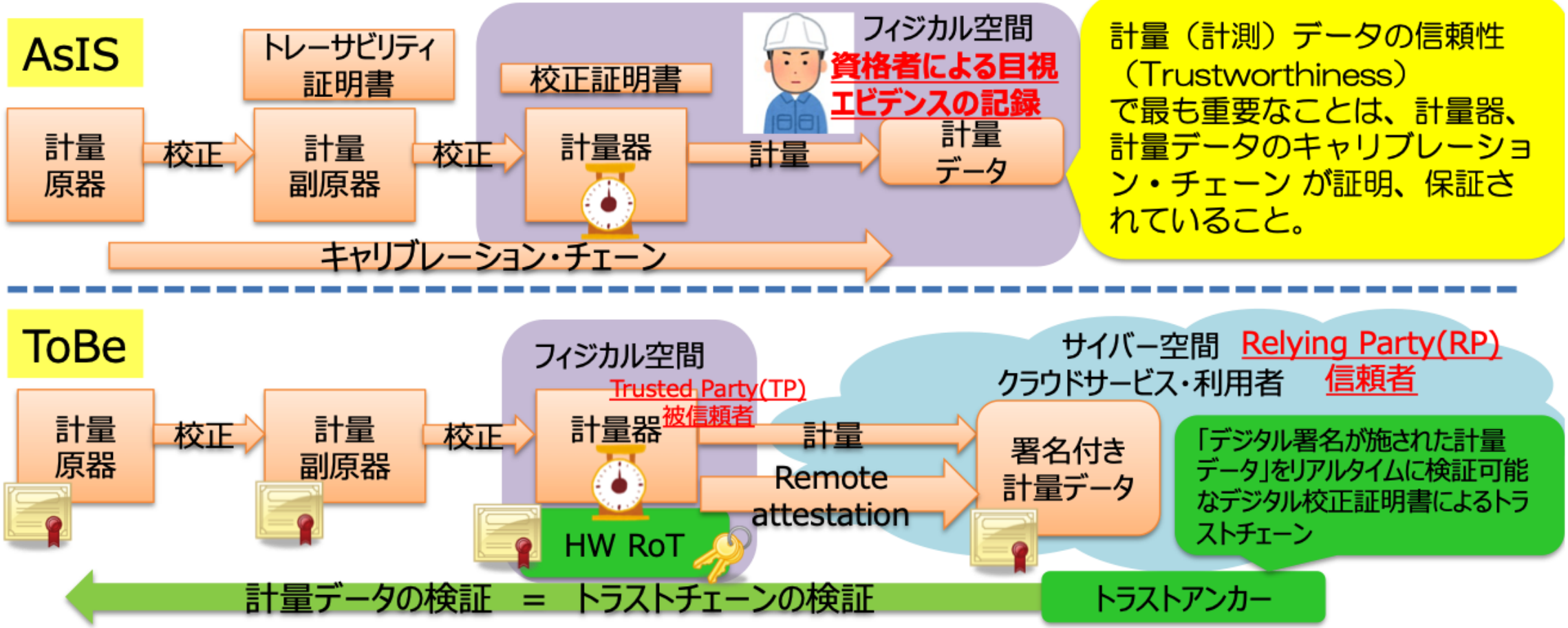
7

© 2023 SECOM CO., LTD

https://www.nic.ad.jp/ja/materials/iw/2023/proceedings/c14/c14-matsumoto.pdf

Copyright 2025　NPO日本ネットワークセキュリティ協会

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



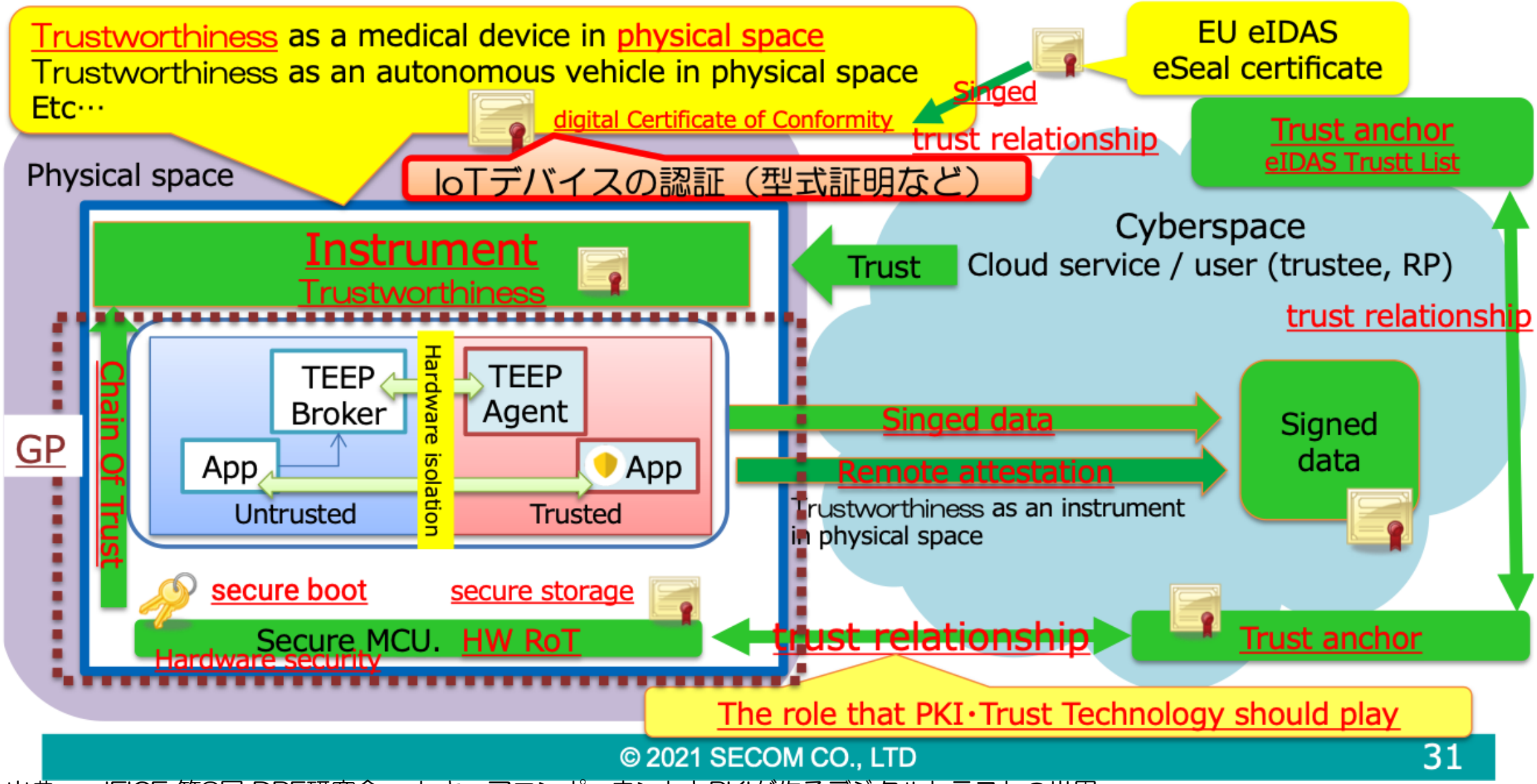
PKI・トラスト技術の役割　→　デバイス・データの信頼性（Trustworthiness）をRPに伝える
→ 人の目視に頼らず、デバイス・データの信頼性（Trustworthiness）が検証できること

© 2021 SECOM CO., LTD

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

Copyright 2025　NPO日本ネットワークセキュリティ協会

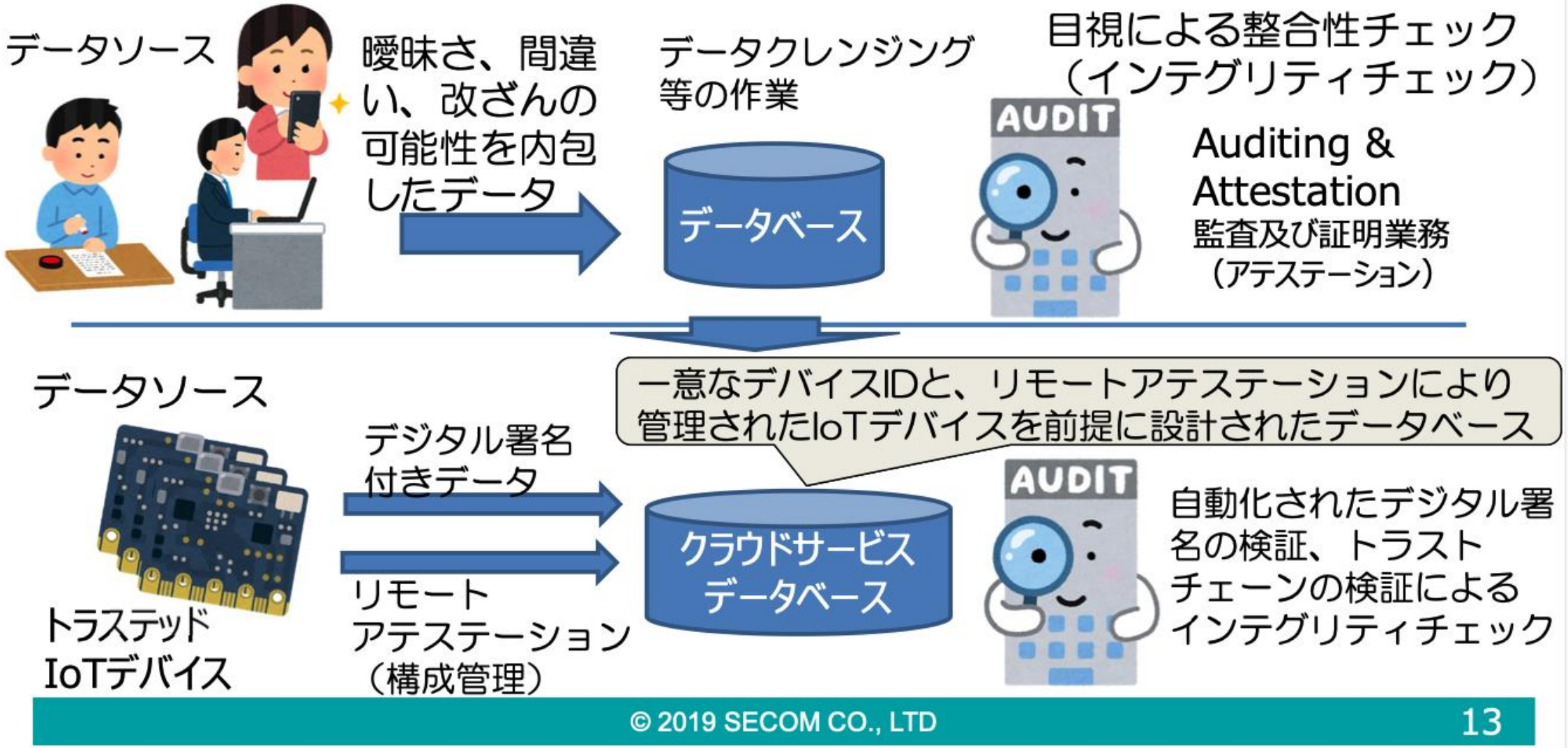
Role of PKI / Trust Technology--Trust in Cyber-Physical Systems



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

Copyright 2025　NPO日本ネットワークセキュリティ協会

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



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

Copyright 2025 NPO日本ネットワークセキュリティ協会