NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

PKI day 2019
トラストサービスの在り方 篇
オーバービュー

2019年4月17日

JNSA 電子署名WG サブリーダー
JT2A（日本トラストテクノロジー協議会） 運営委員
佐藤 雅史

トラストサービスを主題にしたPKI dayの講演やパネル

PKI Day 2015 「サイバーセキュリティの要となるPKIを見直す」

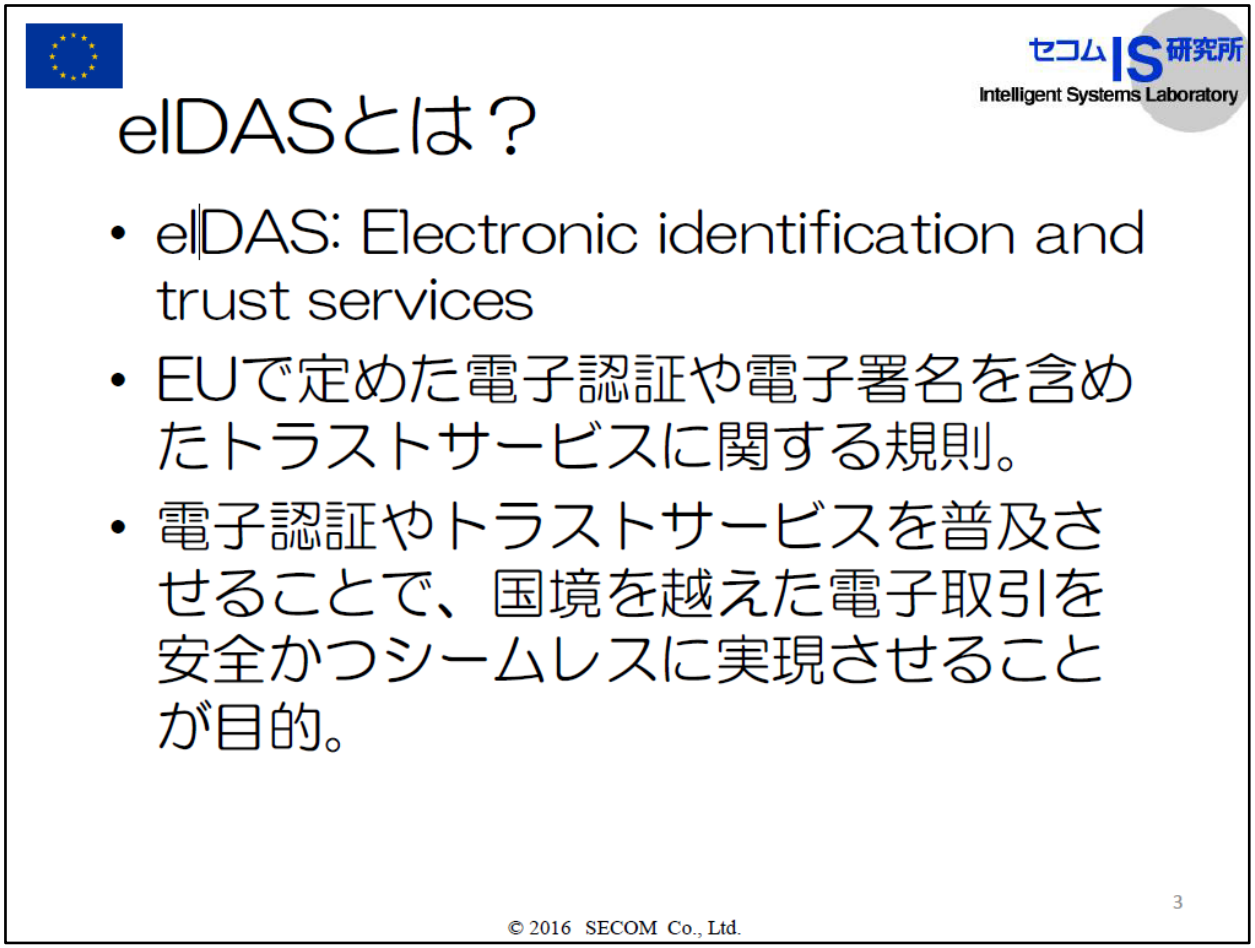
- 「欧州の動向-電子署名指令からeIDAS規則へ」／濱口 総志 氏
- 「トラストリストと信頼のグローバル化」／村尾 進一 氏

PKI Day 2016「マイナンバー時代のPKI」

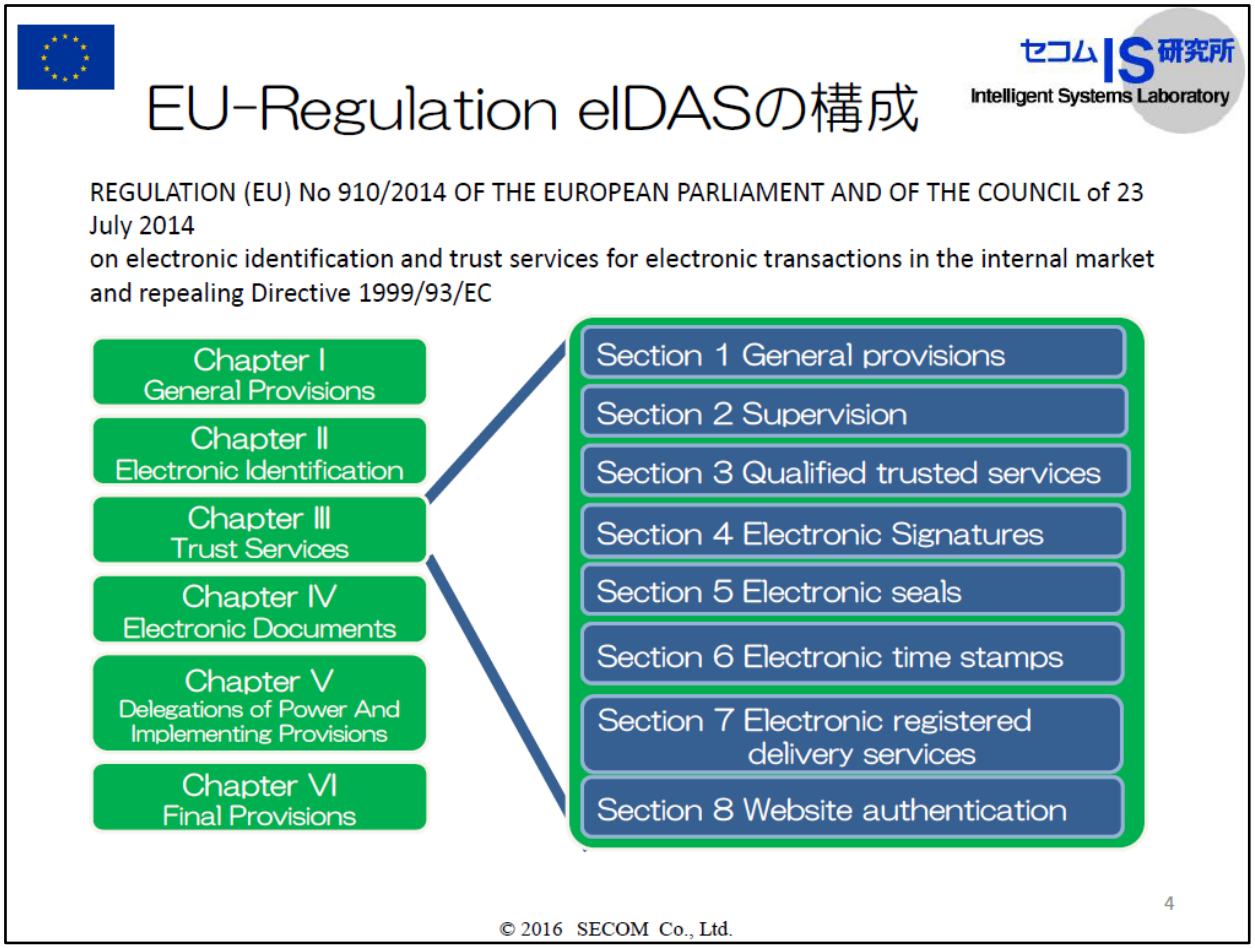
- 電子署名標準化動向から今後の方向性を探る／佐藤 雅史

PKI Day 2018「超スマート社会（Society 5.0）におけるトラストの在り方」

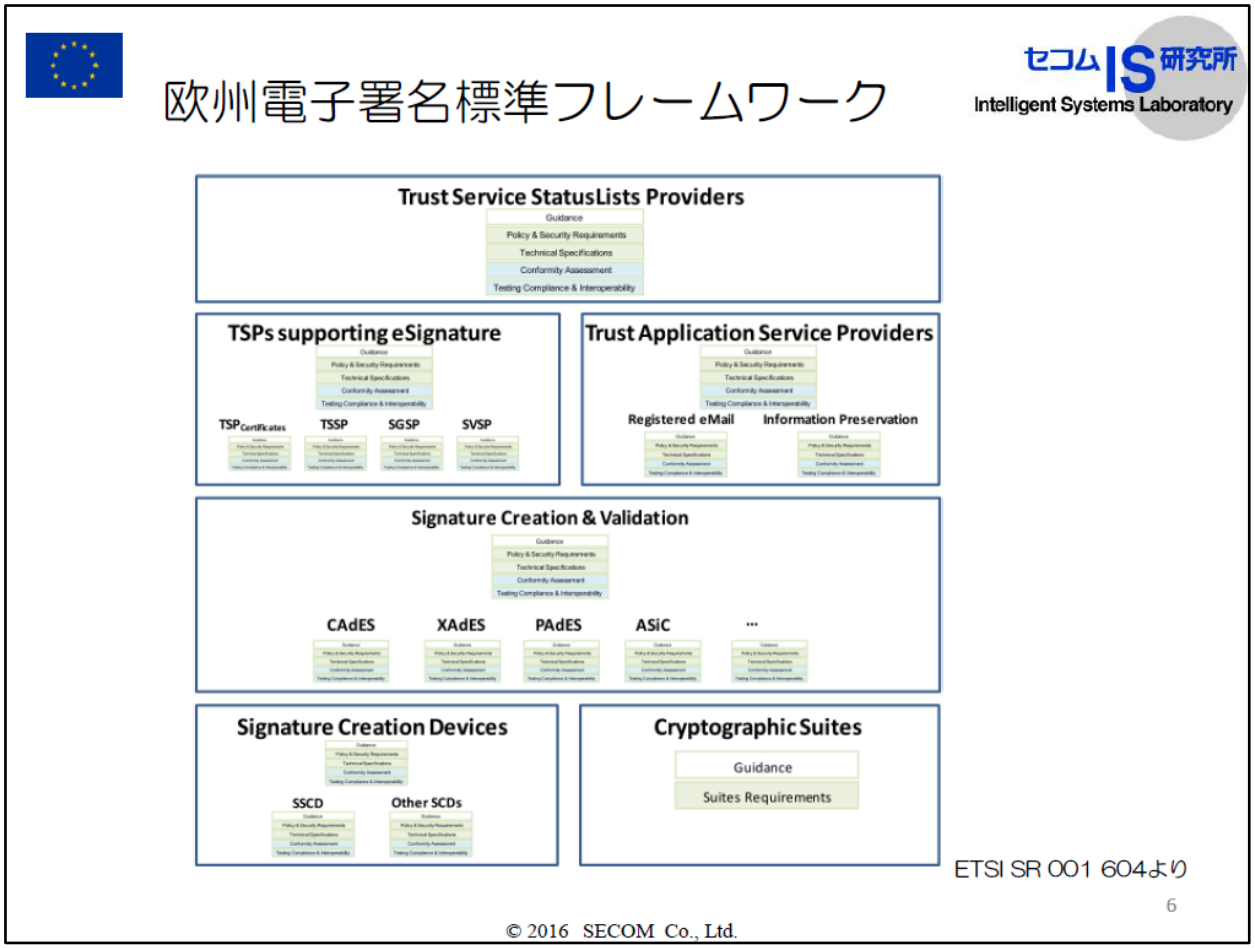
- 超スマート社会（Society 5.0）におけるトラストの在り方／山内 徹 氏、宮崎 一哉 氏、小川 博久 氏



PKI day 2016 電子署名標準化動向から今後の方向性を探る（佐藤）
https://www.jnsa.org/seminar/pki-day/2016/data/2-2_sato.pdf



PKI day 2016 電子署名標準化動向から今後の方向性を探る（佐藤）
https://www.jnsa.org/seminar/pki-day/2016/data/2-2_sato.pdf



PKI day 2016 電子署名標準化動向から今後の方向性を探る（佐藤）
https://www.jnsa.org/seminar/pki-day/2016/data/2-2_sato.pdf

- トラストやトラストサービスをテーマとした日本の業界団体
  - JNSA （PKI相互運用技術WG、電子署名WG）
  - JT2A: 日本トラストテクノロジー協議会
  - OpenID Foundation Japan
  - JIPDEC（インターネットトラストセンター）
  - TSF： トラストサービス推進フォーラム

  など

- 最近のトラストサービス/トラストに関連する議論
  - プラットフォームサービスに関する研究会（総務省）
    - トラストサービス検討会ワーキンググループ
  - 第二期SIP（内閣府）

戦略的イノベーション創造プログラム（SIP：エスアイピー）

SIP 戦略的イノベーション創造プログラム
Cross-ministerial Strategic Innovation Promotion Program

総合科学技術・イノベーション会議が自らの司令塔機能を発揮して、府省の枠や旧来の分野のたすことを通じて、科学技術イノベーションを実現するために新たに創設するプログラムです。

戦略的イノベーション創造プログラム（ＳＩＰ）シンポジウム２０１８

戦略的イノベーション創造プログラム（ＳＩＰ）YouTubeチャンネル（移動

戦略的イノベーション創造プログラム（ＳＩＰ）の概要

- 戦略的イノベーション創造プログラム（SIP）概要（20180719改正）（PDF：316KB）
- 研究開発計画　第１期　11課題（PDF形式：665KB）
- 研究開発計画　第２期　12課題PDF形式：709KB）
- 戦略的イノベーション創造プログラム（ＳＩＰ）平成30年度実施方針（PDF：136KB）

https://www8.cao.go.jp/cstp/gaiyo/sip/

03. IoT社会に対応したサイバー・フィジカル・セキュリティ

後藤 厚宏（ごとう あつひろ）
情報セキュリティ大学院大学 学長

目指す姿

概要

セキュアな Society 5.0 の実現に向け、様々なIoT機器を守り社会全体の安全・安心を確立するため、IoTシステム・サービス及び中小企業を含む大規模サプライチェーン*1全体を守ることに活用できる『サイバー・フィジカル・セキュリティ対策基盤』の開発と実証を行う。多様な社会インフラやサービス、幅広いサプライチェーンを有する製造・流通・ビル等の各産業分野への社会実装を推進する*2 。

*1: 自動車産業の延べサプライヤー数は100万社超（2012年）　*2:「未来投資戦略 2017」閣議決定（2017年6月）

目標

スマート家電等の一般消費者向けの機器から産業用システムまで、多様なIoT機器・システム・サービスのセキュリティを確保できる『サイバー・フィジカル・セキュリティ対策基盤』を確立する。実証を通じて有効性を確認し、実稼働するサプライチェーンに組み込み実用化する。本基盤の社会実装を他国に先駆けて推進することで、サイバー脅威に対するIoT社会の強靭化を図り、我が国のセキュアなSociety5.0実現に寄与する。

出口戦略

当初から課題認識のある製造・流通・ビル等のユーザ企業と連携した研究開発と実証実験を進め、参画企業が主体的に製品化・事業化。欧米の基準とすり合わせながら府省による制度整備と連携してIoTシステム・サービスやサプライチェーンへの導入を促進し、2030年までにサプライチェーン対策が求められる中小企業の50％に成果の導入を目指す。

社会経済インパクト

IoT社会の強靭化（サイバー犯罪による経済損失回避）により、Society5.0の実現がもたらす約90兆円の価値創出を支える。さらにグローバルなサプライチェーンに参画する要件*3となるセキュリティ確保を適切なコストで実現することにより、日本の製品・サービスの国際競争力を強化（輸出主体の製造業の参入機会の確保）する。

*3: 米国のNIST SP800-171や、欧州のサイバーセキュリティ認証フレームワーク等の動き

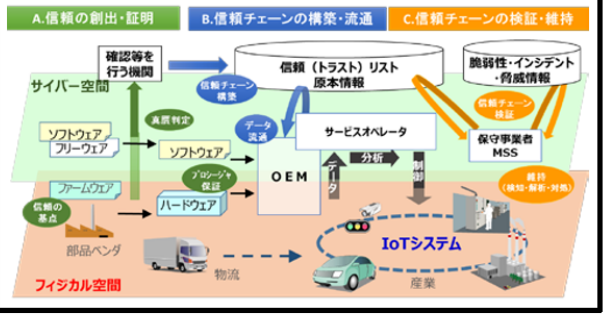
達成に向けて

研究開発内容

IoT機器やサプライチェーンの各構成要素についてセキュリティの確保（信頼の創出）とその確認（信頼の証明）を繰り返し行い、信頼のチェーンを構築・維持することで、IoTシステム・サービス及びサプライチェーン全体のセキュリティを確保するため、

A. 信頼の創出・証明　（IoT機器向け真贋判定技術 等）
B. 信頼チェーンの構築・流通　（トラストリストを用いた信頼チェーン構築技術 等）
C. 信頼チェーンの検証・維持　（インシデントの検知・解析・対処など信頼チェーンの維持技術　等）

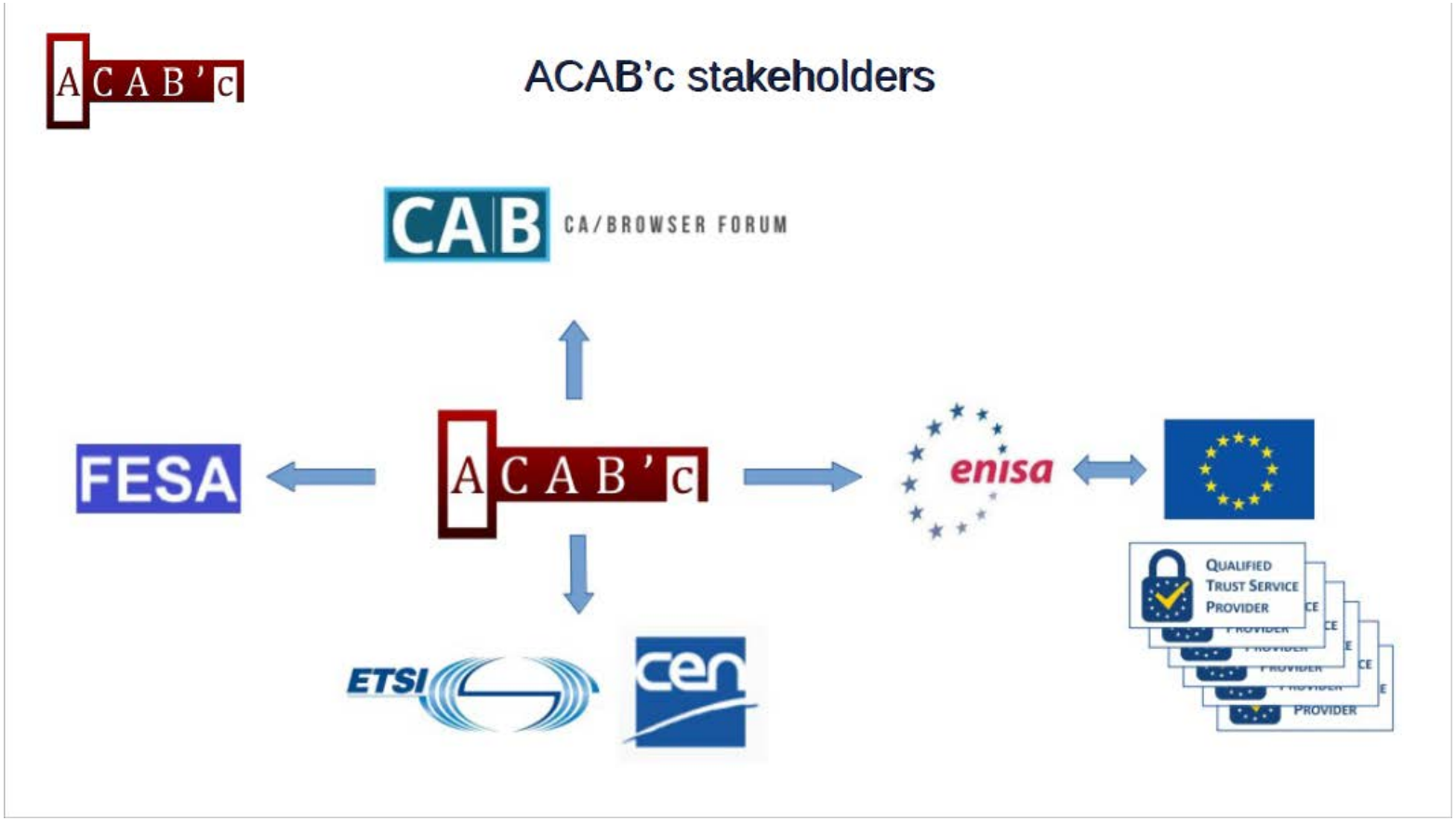
及び、その他、必要な研究開発・動向調査を行い、実サービスや各産業分野において実証を行う。



関係府省：総務省、経済産業省、NISC、IT室、警察庁、防衛省、厚生労働省

https://www8.cao.go.jp/cstp/gaiyo/sip/kenkyugaiyo2.pdf

一方で、Webのトラストは？

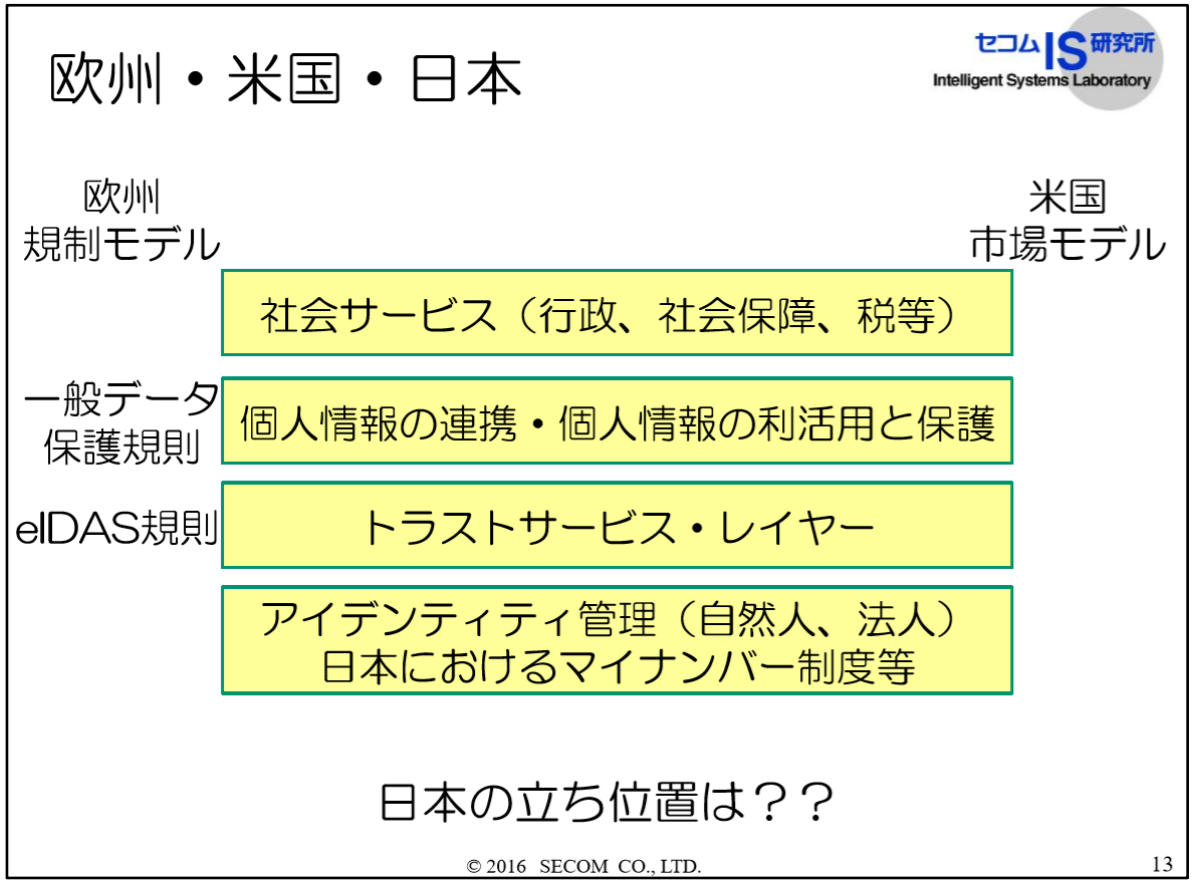


https://www.enisa.europa.eu/events/tsforum-caday-2018/presentations/02_04_Gonnot.pdf

午後の部（トラストサービスの在り方 篇）のテーマの一つ

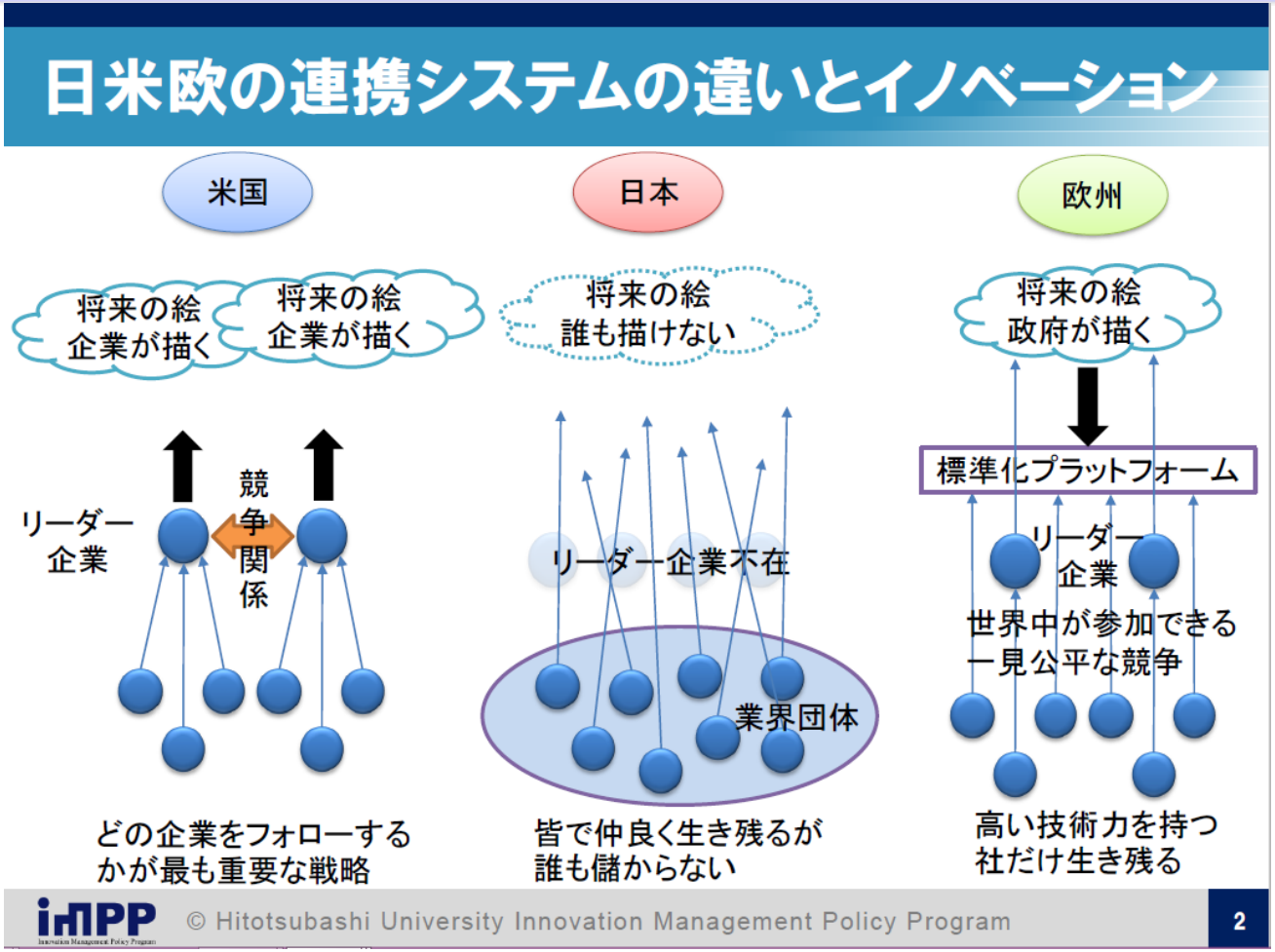
トラストサービスが1つのキーワードになっているが、実際にどういう世界なのか？

あるもう一つの観点



PKI day 2016 マイナンバー時代のPKI（松本 泰氏）
https://www.jnsa.org/seminar/pki-day/2016/data/2-4_panel_matsumoto.pdf

一つの観点として



産業構造審議会 産業技術環境分科会 研究開発・イノベーション小委員会 [2019年2月14日]
一橋大学 イノベー ション研究センター　江藤学先生資料より
https://www.meti.go.jp/shingikai/sankoshin/sangyo_gijutsu/kenkyu_innovation/pdf/009_04_00.pdf

午後の部（トラストサービスの在り方 篇）のテーマのもう一つ

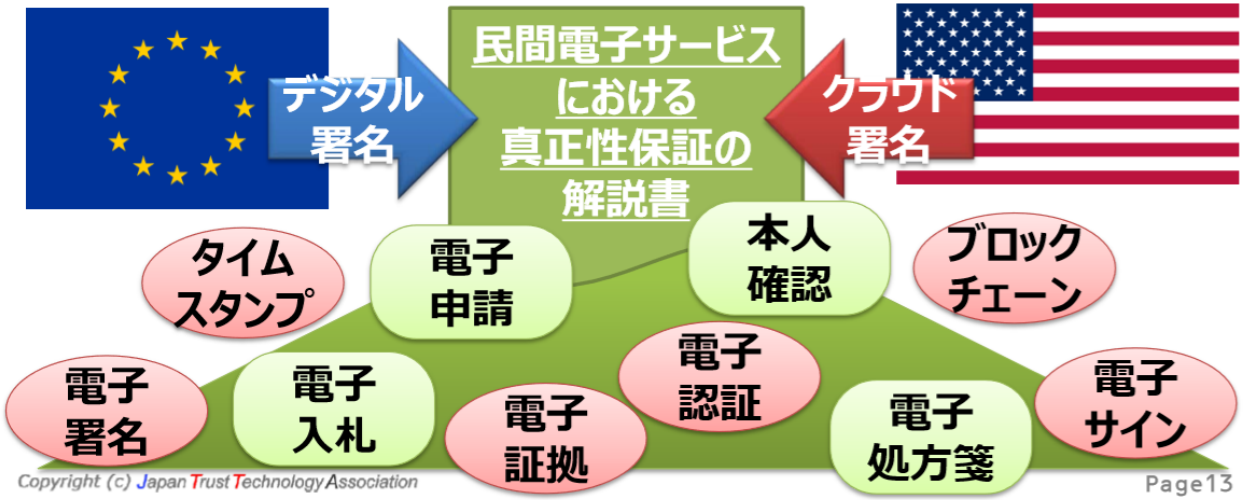
トラストサービスの背景にある狙いとは？

日本は何を考えるべきか？

日本におけるトラストサービス（？）とは？
社会インフラをさせるためには何が必要か？
さまざまな観点での議論が大切。

民間電子サービスにおける真正性保証の解説書 JT2A

- JT2A真正性保証TFでは、民間電子サービスを対象とした、開発者／ユーザ向けの真正性保証の解説書を作成。真正性に関連するユースケースや技術を解説。
- 解説書には欧米で主に利用されている技術も含む。
  - 欧州型：**デジタル署名**ベース
  - 米国型：**クラウド署名（電子認証＋電子証拠）**ベース



Network Security Forum 2019「署名検証・知ってるつもり」
山中 忠和 氏（三菱電機株式会社/ JT2A真正性保証TFリーダー）
https://www.jnsa.org/seminar/nsf/2019/data/NSF2019_A1_3.pdf

さまざまな観点、角度からトラストサービスの在り方を考えてみる。

- 講演「米国航空産業で利用されるPKI」
  株式会社コスモス・コーポレイション　濱口 総志 氏
- 講演「「英国オープン・バンキング」におけるトラストの確立」
  株式会社野村総合研究所　ＩＴ基盤技術戦略室 上席研究員　崎村 夏彦 氏
- 講演「Society5.0を支えるトラストサービスとトラスト基盤」
  慶應義塾大学　大学院政策・メディア研究科　特任教授　手塚　悟 氏

- パネルディスカッション「トラストサービスの在り方」
  モデレータ：佐藤 雅史
  パネリスト：
  宮内・水町IT法律事務所　弁護士　宮内　宏 氏
  有限会社ラング・エッジ　宮地 直人 氏
  慶應義塾大学　大学院政策・メディア研究科　特任教授　手塚　悟 氏
  株式会社コスモス・コーポレイション　濱口 総志 氏
  株式会社野村総合研究所　デジタル基盤開発部　上席研究員　崎村 夏彦 氏