2020/3/31

一般社団法人データ流通推進協議会

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

欧米におけるトラストサービスに関わる調査業務　報告書

慶應義塾大学　環境情報学部

教授　手塚 悟

2020/3/31
一般社団法人データ流通推進協議会

目次

1 EUにおけるトラストサービスの動向調査

1.1 eIDAS 規則と欧州におけるトラストサービスの全体概要

欧州では、1999 年に定められた電子署名指令に代わり、「eIDAS 規則」（注）が 2014 年 7 月に採択された。EU 加盟国はそれぞれ電子署名指令に従った独自の電子署名法を定めていたが、これらの各加盟国の電子署名法は、すべて「eIDAS 規則」に上書されることになった。「eIDAS 規則」は、電子署名の法的効力を承認した電子署名指令を継承するもので、その適用範囲は電子署名を含むトラストサービスと eID に拡大されている。

トラストサービスには、電子署名やタイムスタンプ、e シール、e デリバリー、ウェブ認証等が定められ、これらは経済活動の電子化促進に必要不可欠なセキュアインフラである。

eID とは、電子認証（つまり，電子的な本人確認）を行うことが出来る機能のことであり、我が国のマイナンバーカードも電子認証の機能を有していることから、eID の概念に含まれると言える。「eIDAS 規則」は、この eID の認証結果を各国で受け入れ合うことを定めている。EU 全域で、トラストサービスと eID に関する統一的な法的効力を承認することで、確定申告や銀行口座の開設、入札への参加、大学への入学手続等をオンラインで申請できるようになり、また、他の加盟国への申請も行えるようになる。

つまり、「eIDAS 規則」とは、eID とトラストサービスの法的効力を承認し、電子申請、オンライン決済、電子契約等における信頼性が紙の世界と同等であることを担保することで、電子化と効率化の促進を狙いとした法律である。この電子化と効率化による競争力の向上及び経済成長を狙いとすると同時に、加盟国間の隔たりをなくすことで、欧州全体で 1 つの大きなデジタル市場を形成しようとしている。

1.1.1 トラストサービス

eIDAS 規則では主として以下のトラストサービスの要件と法的効力を定めている。

電子署名

特定の要件を満たした電子署名を適格電子署名といい、手書き署名と同等の法的効力であることを保証する。

e シール

技術的には電子署名と全く同じ仕組みであるが、署名行為は自然人でなければ行えないため、法人向けに新たに e シールというトラストサービスが定義された。電子データの起源と完全性を法的に保証する。

タイムスタンプ
電子データの時刻の正確性とデータの完全性を保証する。

e デリバリー
データの送受信者の特定及び送受信日時と送受信データの完全性を保証する。

ウェブ認証
ウェブサイトの運営者及び運営組織の身元を保証する。

1.1.2 トラストサービスプロバイダ

eIDAS 規則で法的効力が認められたトラストサービスを提供する事業者を適格トラストサービスプロバイダと言い、適格トラストサービスプロバイダになるためには厳格な第三者監査を受け、政府機関によって eIDAS 規則への適合性が認められる必要がある。

適格トラストサービスプロバイダが提供するトラストサービスは、EU 域内の全加盟国において同等の法的効力が認められることが eIDAS 規則によって保証されている。

現在欧州では 29 加盟国において 180 の適格トラストサービスプロバイダが登録されている。

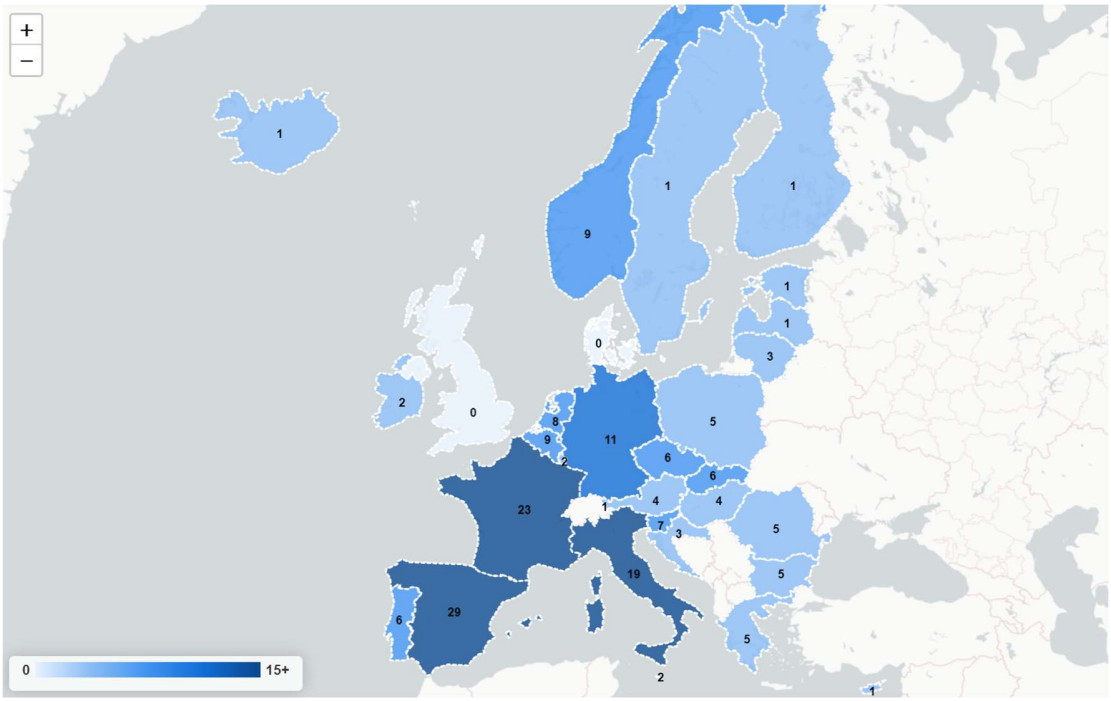


図 1　EU におけるトラストサービスプロバイダの統計データ

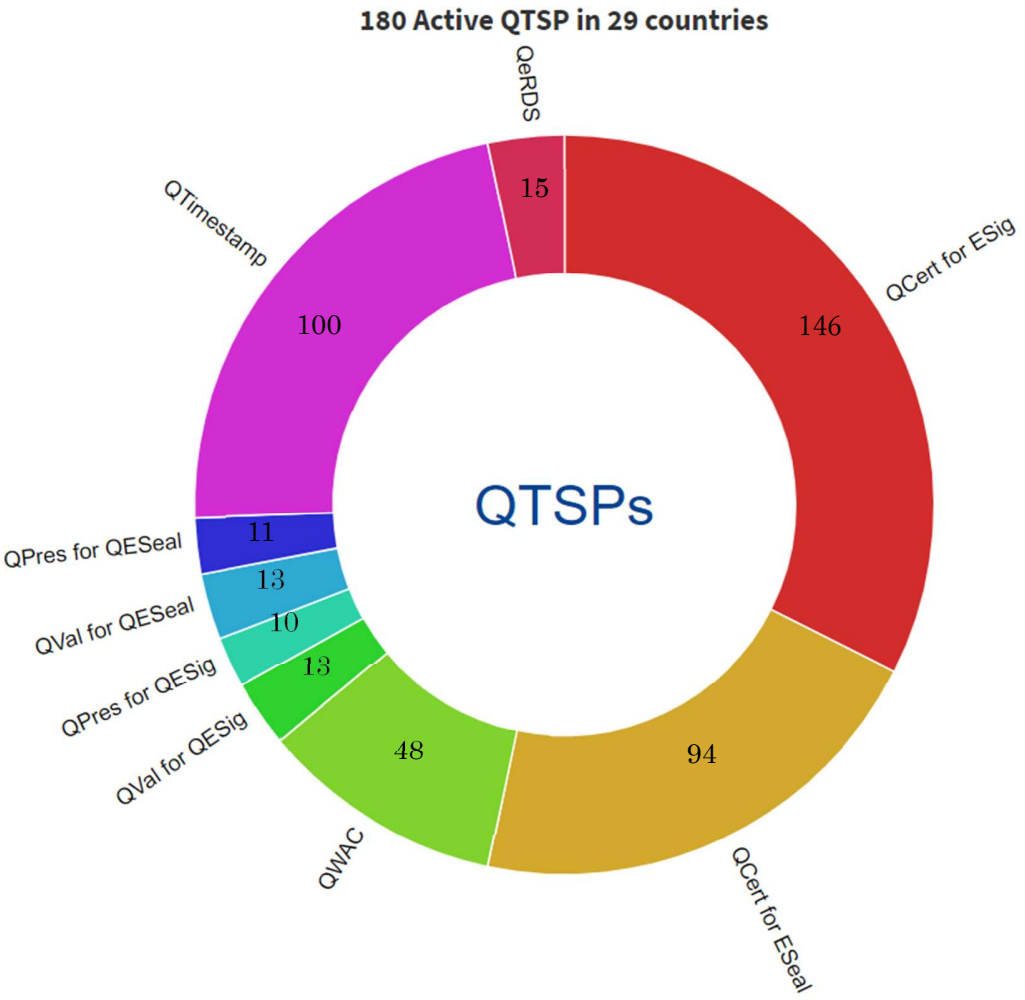


図 2　適格トラストサービスの登録数とその比率

1.1.3 トラステッドリスト

各 EU 加盟国は自国の適格トラストサービスプロバイダとそのトラストサービスに関する情報をトラステッドリストに掲載し公開する義務を負っている。このトラステッドリストは XML 形式で公開されており、加盟国の政府機関がトラステッドリストに電子署名を行うことで真正性及び完全性を保証している。また、加盟国のトラステッドリストとは別に、欧州委員会はリストオブトラステッドリスト（LoTL）と呼ばれるリストを公開しており、このリストには各加盟国のトラステッドリストへのリンクと、トラステッドリストの署名検証を行うための公開鍵に関する情報が記載されている。これにより、トラストサービスの依拠当事者は LoTL を通じてトラステッドリストの有効性検証を行い、当該トラストサービスがリストに載っているトラストサービスであるか否かを自動で検証できるようになっている。

1.2 FutureTrustの動向調査

1.2.1 FutureTrustプロジェクトの概要

FutureTrust は、欧州研究・イノベーション枠組み計画（Horizon 2020）より資金を提供され、2016年6月1日から2019年8月31日まで実施されたプロジェクトである。

このプロジェクトは、EU域内市場での電子識別(eID)及びトラストサービスに関するeIDAS規則の実用的な実装をサポートしており、世界中で法的効力に裏付けられた電子取引を実現するために、ヨーロッパ以外でも、信頼できる eID 及びトラストサービスの利用と普及することを主目的としている。

FutureTrust は、現在の eIDAS 規則のエコシステムを補完するオープンソースのコンポーネントとサービスを設計及び開発し、開発されたコンポーネントを使用して、eIDAS 準拠の実用的なアプリケーションを構築及び使用する方法を示している。

また、eIDAS 規則に於けるトラストサービスステータスリスト（TSL）基盤を「グローバルトラストサービスステータスリスト（GTSL)」に拡張し、電子署名とシール用の拡張性のある保存サービスと同時に、包括的なオープンソースの検証サービスも開発する。　さらに、国境を越えた適格証明書の eID ベースのアプリケーションのコンポーネント、モバイル環境における信頼できるリモート署名とシールの作成のためのコンポーネントを提供する。

FutureTrust のシステムアーキテクチャは、eIDAS 規則のエコシステムを拡張し、さまざまなFutureTrustサービスとFutureTrustパイロットアプリケーション、及び「グローバルトラストサービスステータスリスト」（gTSL）を統合する。図 3 は FutureTrust が開発したサービスとアプリケーション概要、表1はその詳細を表す。

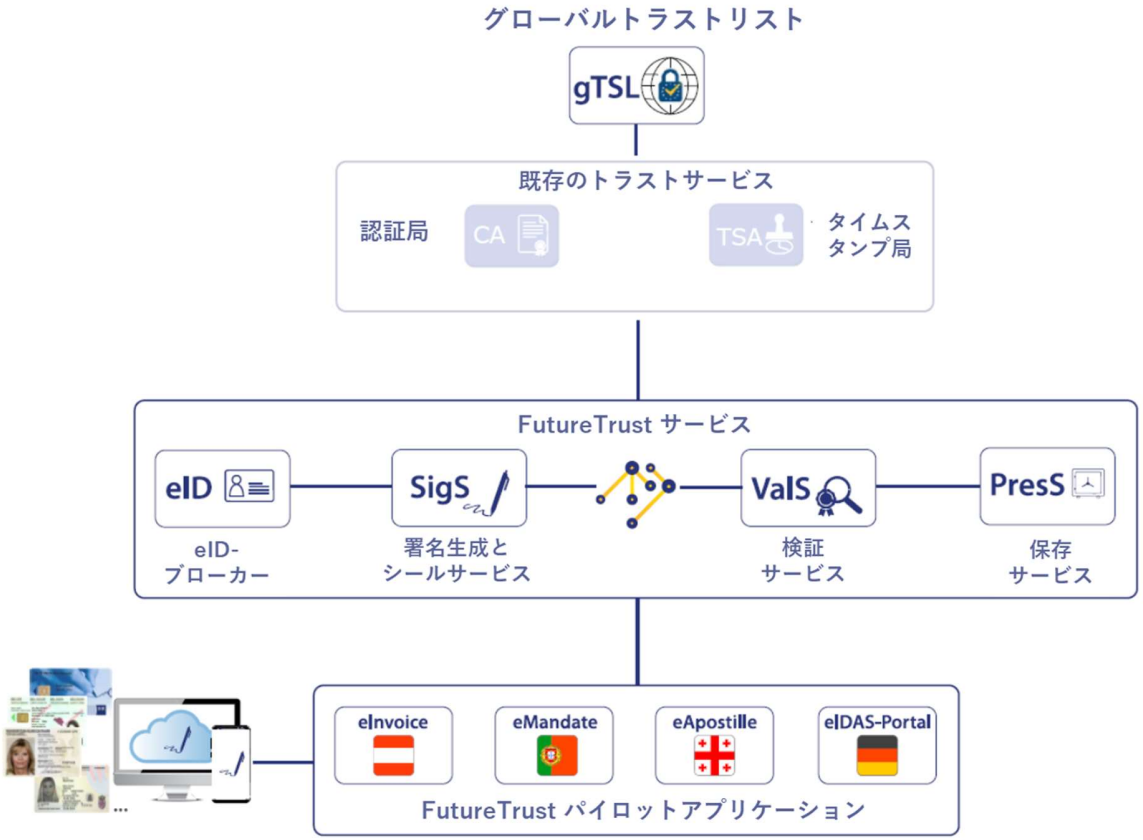


図 3　FutureTrust が開発したサービスとアプリケーション概要
＜出典：FutureTrust Pilots Portal, https://pilots.futuretrust.eu/overview より＞

表 1　FutureTrust サービス及びパイロットアプリケーション

基本的な FutureTrust サービス	・全ヨーロッパの eID ブローカー（eID ブローカー、eID）
	・署名生成サービス（SigS）
	・検証サービス（ValS）
	・保存サービス（PresS）
FutureTrust パイロットアプリケーション	・ポルトガルの電子 SEPA eMandates（eMandates1）サービス
	・オーストリアの電子請求書サービス（eInvoice）
	・ジョージアの電子アポスティーユ（eApostille2）サービ

[1] eMandates: 電子的プロセスを使用したmandate(委任)サービス。SEPA口座振替スキームを使用して、サプライヤーの銀行が特定の契約（商品やサービスの購入など）の支払いを購入者の銀行口座から徴収できるようにする口座振替の認証。
[2] eApostille: 国際アポスティーユ条約の規則に従って、公文書に外務省、公証人役場等が実施する付箋により証明され、合法化された文書の電子版の作成。

	ス
	・ドイツの eID ベースの本人確認後に証明書を登録できる eIDAS-Portal（eIDAS-Portal）

1.2.2 Trust Model

1.2.2.1 eIDAS エコシステム

「eIDAS エコシステム」は、「ユーザ」、「eIDAS ベースのトランザクションサービス」、様々な「eIDAS サービス」、そしてトラストに関連するアスペクトを持ち、eIDAS 規則第 22 条、2015/1505/EU、TS 119 162 (v2.1.1)に従いトラステッドリストのトラストアンカーを公開する「eIDAS トラストシステム」の集合である。(図 4 参照)

「eIDAS トラストシステム」は、「eIDAS エコシステム」の規制のフレームワークみなすことができ、「eIDAS サービス」はその信頼できるサービス指向型インフラストラクチャを提供する技術的バックボーンとみなされる。一方で、ユーザと「eIDAS ベースのトランザクションサービス」のプロバイダは、関係するステークホルダの利益のために異なるサービスを提供・組み合わせることにより価値を生み出す経済システムを構成する。

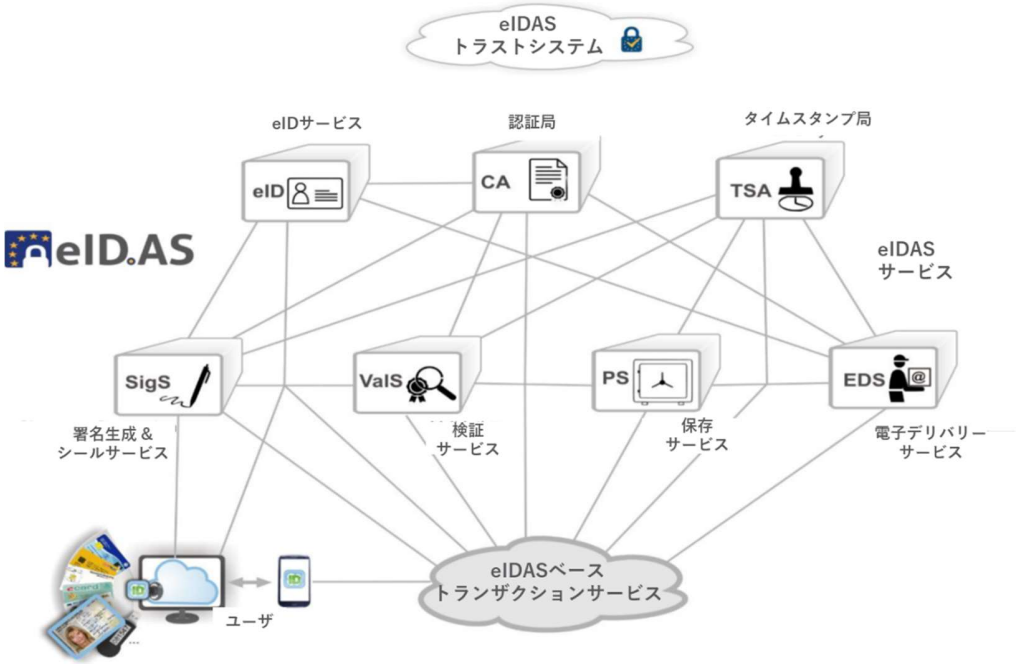


図 4　eIDAS エコシステム

＜出典：FutureTrust Architecture Plan, https://www.futuretrust.eu/deliverables より＞

1.2.2.2 eIDAS トラストシステム

「eIDAS トラストシステム」は、eIDAS エコシステムのトラストに関連するアスペクトを維持するために相互に作用するさまざまな組織、法律、規制機関で構成される。最終的に、既存の eIDAS サービスの信頼性と、証明書と暗号鍵の有用性と有効性に関する情報を提供する XML ベースのリストを提供する。

図 5 に示すように、「eIDAS トラストシステム」は、つぎの要素から構成されている。

- 欧州委員会（EC)、
- 欧州認定協力（EA)、
- EU 加盟国（MS)、
- 2008/765/EC に従い MS と EA によって指名される国家認定機関（NAB)、
- 2014/910/EU 第 17 条に従い MS によって指定される監督機関（SB)、
- 毎年 SB から違反通知の概要を受け取る 2014/910/EU 第 19 条（3）に従うネットワーク及び情報セキュリティのための欧州連合機関（ENISA)、
- 適合性評価を実施する 2008/765/EC に従う NAB によって認定される、2014/910/EU 第 3 条（18 ）に従う適合性評価機関（CAB)、
- 少なくとも 1 つ以上の eIDAS サービスを提供する 2014/910/EU 第 3 条 (19)—(20)に従う（適格）トラストサービスプロバイダ（(Q）TSP)。

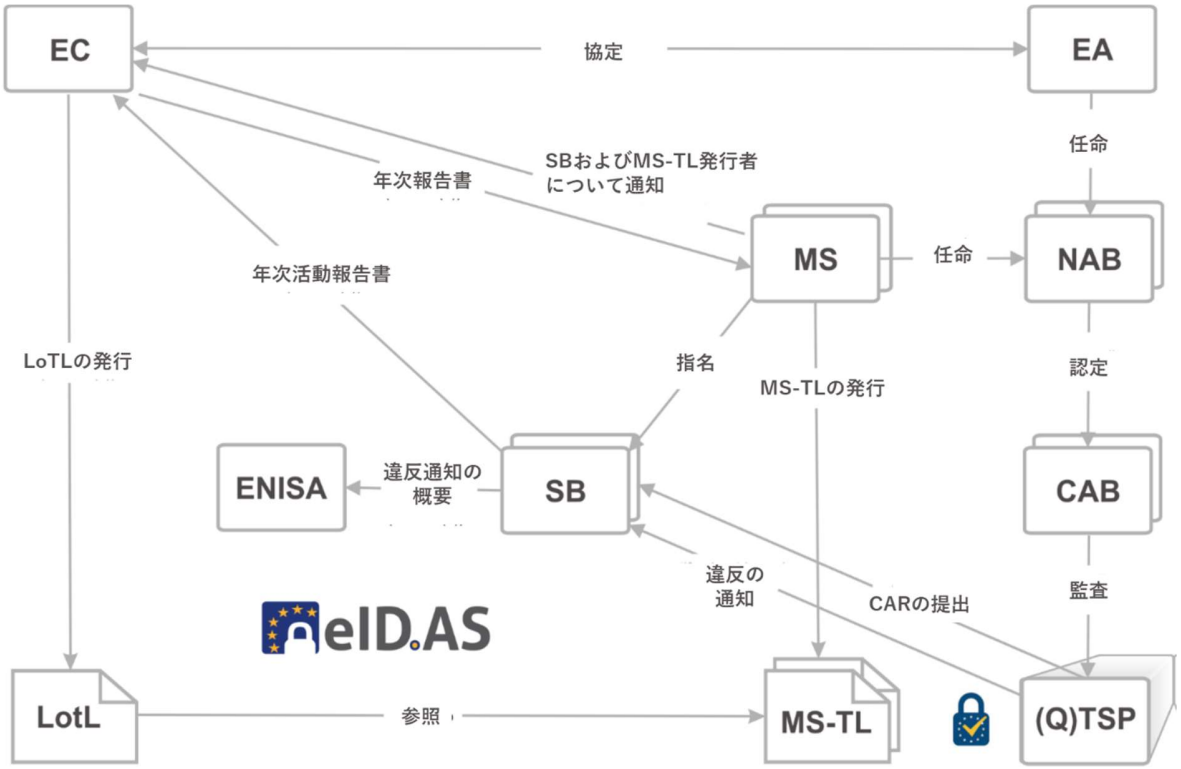


図 5　eIDAS トラストシステム

＜出典：FutureTrust Architecture Plan, https://www.futuretrust.eu/deliverables より＞

MS は EC に「各国のトラステッドリスト、及びリストの公開場所の詳細、署名、又はシールに使用される証明書の設定、維持、及び公開に責任を負う機関について」通知する。　EC はこの情報を使用して、「List of the Lists」（LotL）を発行する。したがって、LotL は、さまざまな加盟国のトラストリスト（MS-TL）を参照することができる。

TSP は、MS-TL にリストされるために、TSP の提供するトラストサービスの適合性を CAB から監査を受ける必要がある。　監査の結果は、適合性評価レポート（CAR）として監督の SB に提出される。SB は CAR を確認し、その TSP 及びトラストサービスに関連する情報を対応する MS-TL に含める。

1.2.2.3 eIDAS サービス

eIDAS のトラストサービスとして、以下のようなサービスがある。

- eID サービス
- 認証局（CA）

- タイムスタンプ局（TSA）
- 署名生成及びシールサービス（SigS）
- 検証サービス（ValS）
- 保存サービス（PresS）
- 電子デリバリーサービス（EDS）

1.2.2.4 eIDAS ベーストランザクションサービス

eIDAS エコシステムは、eIDAS トラストシステムと様々な eIDAS サービスに加えて、ユーザと eIDAS ベーストランザクションサービスを含む第 3 層を備えている。ユーザはさまざまな eIDAS サービスを直接使用できるが、これには、それぞれのインターフェースをローカル環境及びアプリケーションに統合する必要があり、複数のサービスを統合する必要がある場合に維持管理が難しいことが分かる。「eIDAS ベースのトランザクションサービス」を導入することにより、eIDAS 規則によって管理される 1 つ以上のサービスを使用する付加価値のあるトランザクションサービスを生み出すためにユーザに代わって異なる eIDAS サービスを組み合わせて、、ビジネスプロセス全体を実施することができる。

1.2.3 FutureTrust のアーキテクチャプランと成果

1.2.3.1 アーキテクチャプラン概要

「FutureTrust アーキテクチャプラン」（図 4 を参照）は、FutureTrust プロジェクトの成果示す。

図 6 のように、FutureTrust プロジェクトは、eIDAS のエコシステムのサブセットであり、eID サービス（eID)、署名生成及びシールサービス（SigS)、検証サービス（ValS)、保存サービス（PS)、これらに加えて、「グローバルトラステッドリスト」と FutureTrust が扱う他の eIDAS サービスを使用するさまざまな FutureTrust パイロットアプリケーションを用いた拡張されたトラストシステムを含んでいる。

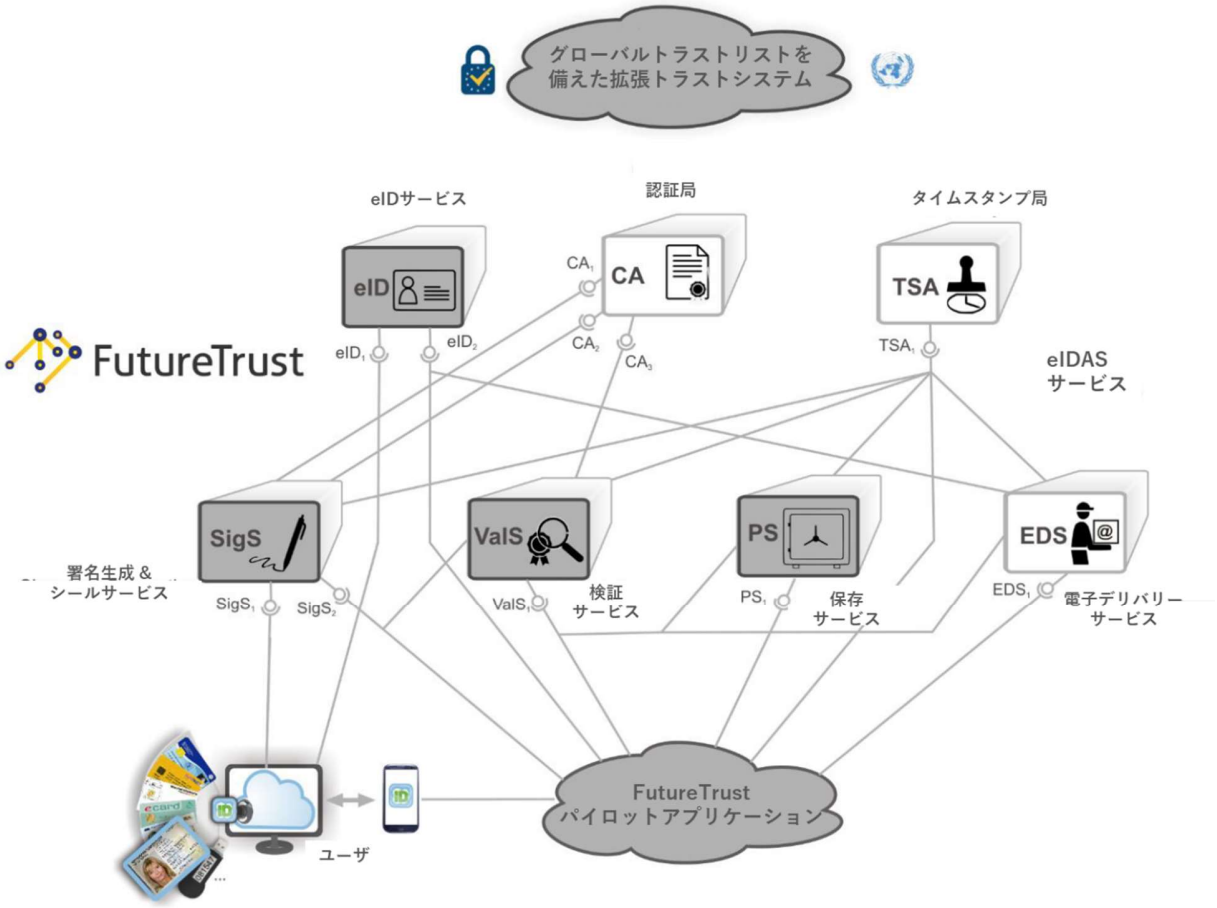


図 6　FutureTrust アーキテクチャプランと成果
＜出典：FutureTrust Architecture Plan, https://www.futuretrust.eu/deliverables より＞

1.2.4 gTSL

Global Trust Status List （gTSL）の主な目的は、現在の TSL モデルを拡張し、欧州の加盟国とそれ以外の国の適格トラストサービスプロバイダ（QTSP）に関連する情報を管理及び提供することである。さらに、レジリエンスの側面と管理性を改善するために、現在の配布スキームを分散化するを目的としている。

1.2.4.1 トラステッドリストの課題

現在、欧州委員会は署名済みの LoTL を公開している。各リストは、TSP の加盟国の TSL の配布ポイントであり、このような国別リストには、適格及びオプションの非適格 TSP に関する情報と、提供する適格及び非適格トラストサービスに関する情報が含まれている。

このスキームでは、1 か国のリストの内容の変更により、全ての国のリストを再公開する必要が生じるが、リストが配布される URL、又はリストの署名に使用される証明書で行われた変更は、国別リストと LoTL の両方の再公開を必要とする。

このように、TSL 配布スキームが集中化しているため、以下の様な問題が生じる。

- 加盟国の TSL は、LoTL に基づいてのみ取得可能であるため、現在のスキームは、単一障害点（Single Point Of Failure）となりうる。
- さまざまな場所から情報をダウンロードして検証する必要があるため、パフォーマンス/遅延の問題が発生する可能性がある。
- TSL は、ノードを配布するすべての加盟国がアクティブであることを要求する。
- アプリケーション固有の TL を作成・管理する手段がない。

さらに、現在の TSL スキームには履歴がないため、TL に対する修正が記録されていない。そのため、TL の新しいバージョンは以前のバージョンを完全に無効にするため、バージョン間で実施された変更を追跡することができない。

1.2.4.2 G-TSL の 3 層アーキテクチャ

前項のトラステッドリストの課題を解決するために、gTSL は 2 つの主要なオープンソースコンポーネント、 グローバルトラストサービスライフサイクルマネージャ（Global Trust Service Lifecycle Manager）とグローバルトラストサービスレスポンダ（Global Trust Service Responder）に依拠している。 さらに、日々の管理機能（たとえば、トラスト情報の更新、証明書の更新など）については、管理インターフェースに依存している。

これらのコンポーネントとシステムのユーザとの関係は、図 7 に示されている。

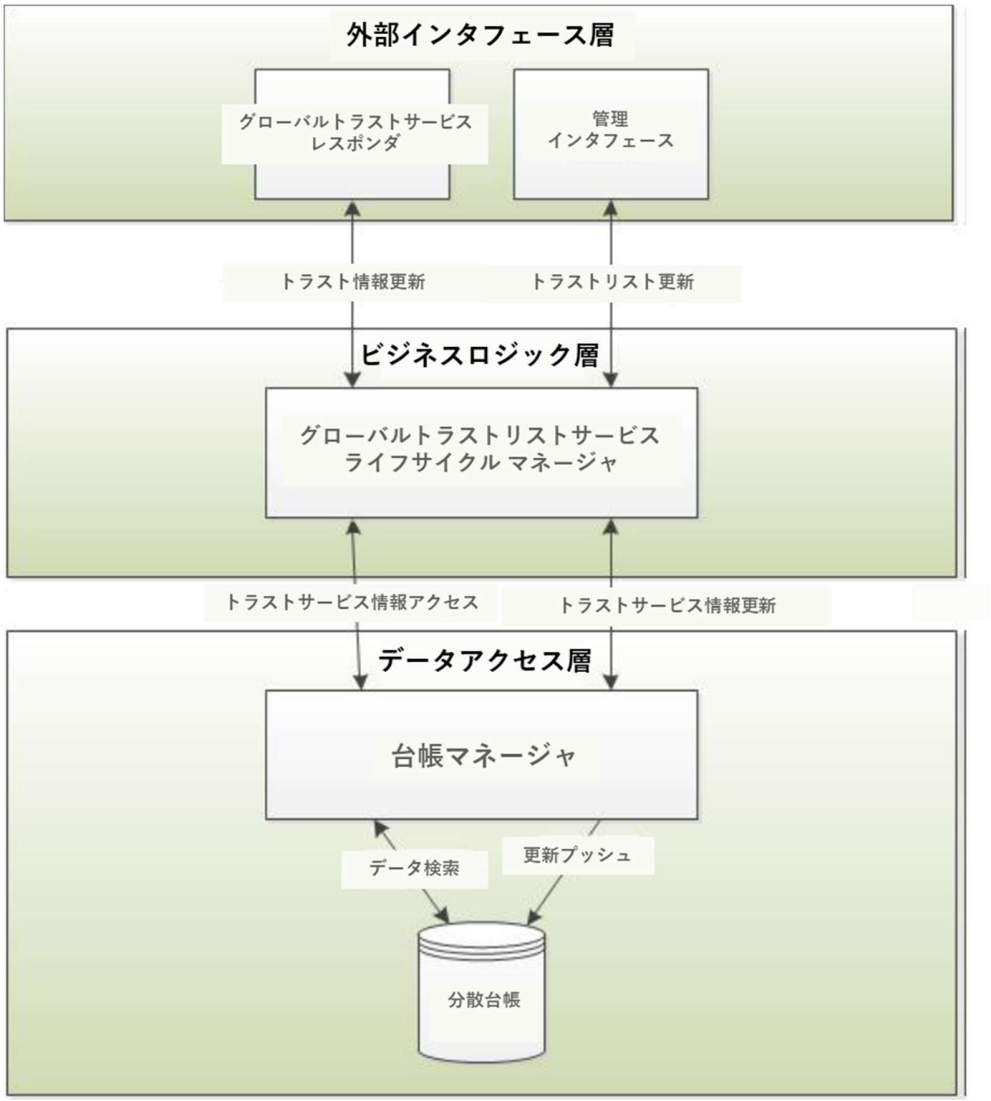


図 7　gTSL-3 層アーキテクチャ

＜出典：Global Trust Service Status List, https://www.futuretrust.eu/deliverables より＞

グローバルトラストサービスレスポンダの目的は、特定の時点でのステータスを確認するために、外部アプリケーションとユーザが TSP に関連する情報を gTSL に照会できるようにすることである。したがって、トラストステータス情報要求に応答するために必要な機能を提供する。

グローバルトラストサービスライフサイクルマネージャの目的は、トラストサービスの階層の処理を容易にし、時間の経過とともに各 TSP のステータスを更新できるようにすることである。そのため、トラストステータス情報の作成、更新、配布に必要な機能を提供する。

アーキテクチャの観点から、gTSL は 3 層アーキテクチャに依拠している。

- 外部サービス層は、システムの外部インターフェースを公開する、すなわち、グローバルトラストサービスレスポンダ及び管理インターフェースである。
- ビジネス層は、グローバルトラストリストサービスライフサイクルマネージャで構成される。
- データ層は、gTSL をデータストレージソリューションに接続できるインターフェースとコンポーネントに対応する。

gTSL の目的の 1 つは、現在の集中型配布スキームから離れて、分散型アプローチを採用することである。ブロックチェーンベースのデータストレージソリューションの出現は、この分散化を達成するための解決策である。

台帳を使用してすべての TSP 及びトラストサービス情報を保護すること、つまり、署名済みトランザクションのチェーンリスト、及びノードのネットワークにおいてすべての gTSL データを複製することにより、情報の完全性と可用性の両方が確保される。すべての情報が台帳のすべての先行情報とともに署名されるため、多数のノード間の分散により、DoS 攻撃に対する強力なレジリエンスが提供される。

参考資料

[1] FutureTrust Architecture Plan D.3.1
https://2e06f8c1-edcc-4de4-9e0f-222a5feadd60.filesusr.com/ugd/2844e6_8212d700085b4229af70f7709f845d5d.pdf

[2] Global Trust Service Status List D.3.2
https://2e06f8c1-edcc-4de4-9e0f-222a5feadd60.filesusr.com/ugd/2844e6_e6319b29397446cdb152b5936e58e1d2.pdf

1.3 UNCITRAL

1.3.1 UNCITRAL 概要

UNCITRAL（The United Nations Commission on International Trade Law, 国際連合商取引法委員会）は、1966 年に国連総会において国際商取引法の調和と統一の促進を目的に設置された委員会である。この委員会の中で欧州は eIDAS 規則のトラストサービス及びそのフレームワークをモデル法の中に組み込む活動をしている。モデル法とは、法整備が整っていない国に向けた国連の推奨法案である。MLTER（The Model Law on Electronic Transferable Records）は UNCITRAL で検討され 2017 年に国連総会で採択されたモデル法の一つであり、この中に電子署名や e シール、タイム

スタンプといった eIDAS 規則における用語や定義が組み込まれている。欧州委員会はこのモデル法を通じて eIDAS 規則のエコシステムの拡大を狙っていると思われる。

1.3.2 最新動向

MLTER は UNCITRAL の WG6 で検討されているが、2019 年 4 月に第 58 回 WG ミーティングにおいて、MLTER で定義されている IdM(Identity Management)とトラストサービスの信頼性について、信頼性の保証レベルや国境を越えた相互運用性と相互承認について議論された。特に「Draft Provisions on the Cross-border Recognition of IdM and Trust Services」では eIDAS 規則の用語、定義を引き継いだ内容で草案文書が議論された。この草案の主目的は、地域や適用法律の違いに関わらず受け入れられる IdM やトラストサービスに関する基準を定めることにある。

また、eIDAS 規則と同様に、IdM やトラストサービスのホワイトリスト（eIDAS 規則におけるトラステッドリスト）を用いて有効性検証することが提案されている。これは同時にリストに記載されている際の第三者監査の必要性を示唆しており、欧州はトラステッドリスト型の検証基盤を拡大しようとしていると思われる。

一方で技術基準については、他の法律に漏れず UNCITRAL も技術的中立性を保持する観点で定められており、IdM やトラストサービスの最小システム要件を定めたガイダンスの必要性を示唆するにとどまっている。

参考資料

[1] UNCITRAL Model Law on Electronic Commerce
http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html

[2] UNCITRAL Model law on electronic signatures
http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html

[3] UNCITRAL Working Group IV (Electronic Commerce) - A/CN.9/WG.IV/WP.158 - Explanatory Remarks on the Draft Provisions on the Cross-border Recognition of Identity Management and Trust Services
https://undocs.org/en/A/CN.9/WG.IV/WP.158

[4] UN Convention on the Use of Electronic Communications in International Contracts
https://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf

[5] UNCITRAL Model Law on Electronic Transferable Records
https://www.uncitral.org/pdf/english/texts/electcom/MLETR_ebook.pdf

2 米国動向調査

2.1 ジョージア工科大学におけるトラストマーク

2.1.1 概要

トラストマーク及びトラストマークフレームワークは、米国の NSTIC(National Strategy for Trusted Identity in Cyberspace)、サイバー空間における信頼できるアイデンティティに関する国家戦略)のパイロットプロジェクトの一つとして、ジョージア工科大学において 2013 年から 2016 年にかけて検討／開発された。トラストマーク及びトラストマークフレームワークでは、単一のトラストフレームでは複数のコミュニティにおけるニーズを満たすことができないという課題に対して、各トラストフレームワークをモジュール化し、再利用可能なコンポーネントとして扱うことを解決策としている。再利用可能なコンポーネントはトラストマークと呼ばれる。

2.1.2 トラストマーク及びフレームワーク

トラストマークは、トラストマークプロバイダによって発行される機械可読な暗号署名されたデジタルアーティファクトであり、トラストマークの依拠当事者、つまりデータの受領者の、受領データを信頼するための要件（トラストマーク定義）に対して第三者であるトラストマークプロバイダがその要件への適合性を証明することを示す目的で使用される。トラストマークがどの要件のセットに対して、その適合性に関する信頼性を示しているかは、トラストマーク定義によって定められる。トラストマークプロバイダは、組織間（あるいは個人間）のデータ交換時の信頼を確立するためのメカニズムとして、トラストマークを取得および使用したい組織（トラストマーク受領者）に署名して発行する。

図 8 は、トラストマークのフレームワークの基本要素を示す概念図である。 トラストマークとは何か、どのように定義されているか、どのように使用されているかについての大まかな概要を示している。

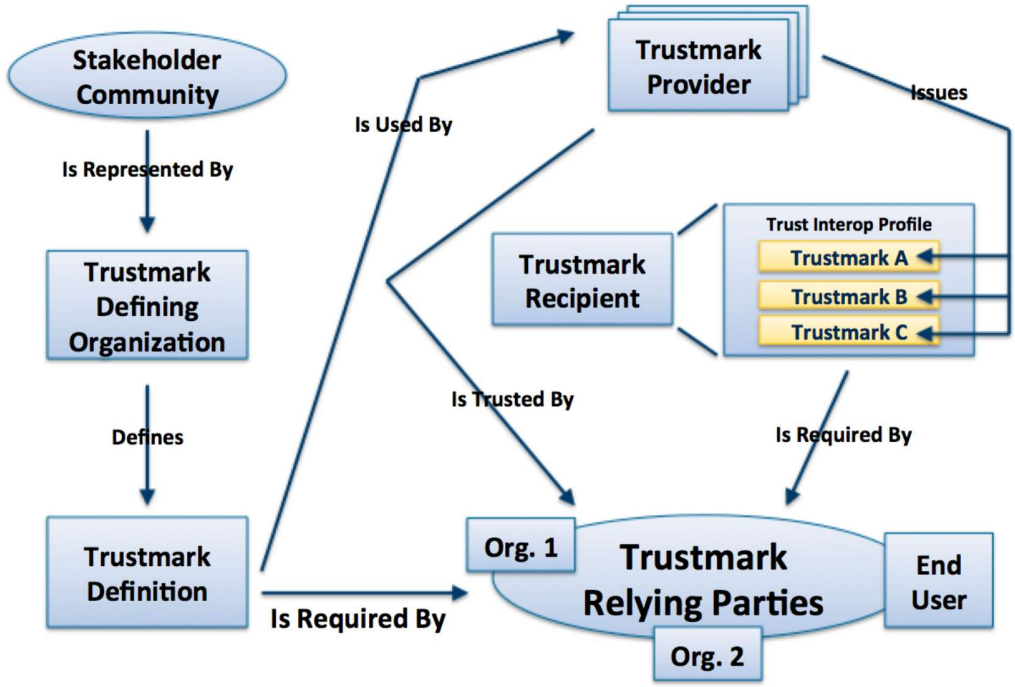


図 8　トラストマークフレームワークの概念図
（出典： TRUSTMARK FRAMEWORK TECHNICAL SPECIFICATION より）

署名されたアーティファクトであるトラストマークは eXtensible Markup Language（XML）形式のオブジェクトであり、その発行者であるトラストマークプロバイダはトラストマークの完全性を保証するためにデジタル署名を行う。

トラストマークの受領者は、トラストマークの依拠当事者が要求する一連の要件に対して、トラストマークプロバイダから発行及び署名されたトラストマークを示すことによって適合性を主張することができる。

トラストマーク定義は、トラストマーク受領者が満たすべき適合基準及びトラストマークプロバイダによるその適合性評価プロセスを定める。トラストマークにはさまざまな種類があり、各トラストマークには独自のトラストマーク定義がある。 トラストマーク定義もトラストマークと同様に XML オブジェクトとして存在している。

トラストマーク定義は、トラストマーク定義組織によって開発／維持される。

トラストマーク依拠当事者は、信頼および相互運用性の要件を満たすために、トラストマーク受領者が備えるべきトラストマークのセットに関して信頼および相互運用性ポリシーを表すトラスト相互運用性プロファイル（XML オブジェクト）を定義する。

発行されたトラストマークのステータスに関する情報は、トラストマークステータスレポート（XML オブジェクト）によって提供される。これは公開鍵証明書における CRL（Certification Revocation List）と類似しており、例えばトラストマークのステータスが「アクティブ」から「失効」または「期限切れ」に変更があった場合にレポートが更新される。トラストマーク依拠当事者は、トラストマークがまだ有効であるか確認するために、必要に応じてトラストマークステータスレポートを要求することができる。

2.1.3 トラストフレームワークの法的側面

図 9 は、トラストマークの法的フレームワークを示している。 これは、図 7 に示されている基本的なトラストマークフレームワーク概念図に基づいており、トラストマークの発行、使用、および信頼が法的観点からどのように機能するかについての詳細を追加している。

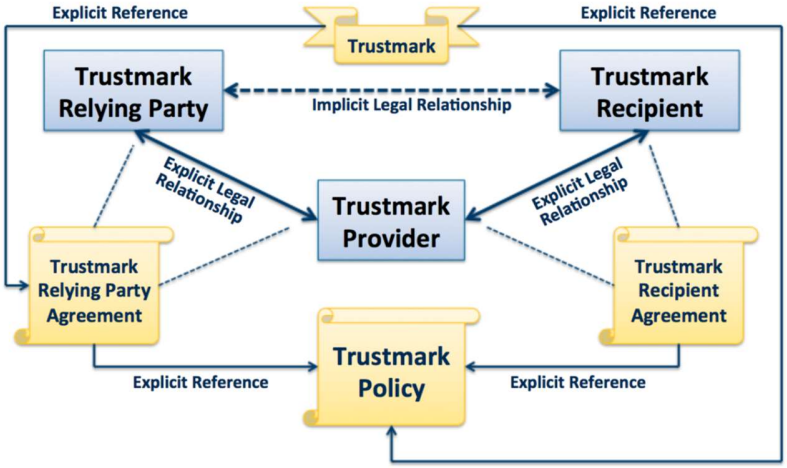


図 9　トラストマーク法的フレームワーク
（出典： TRUSTMARK FRAMEWORK TECHNICAL SPECIFICATION より）

トラストマーク法的フレームワークの中では、トラストマークはトラストマーク受領者契約の下で、トラストマークプロバイダからトラストマーク受領者へ発行される。 トラストマーク受領者アグリーメントは、トラストマークプロバイダとトラストマーク受領者との間の明示的な法的合意を確立する標準的な 2 者間の契約であり、トラストマークポリシが参照として組み込まれている。 トラストマークプロバイダとトラストマーク受領者は、共にトラストマーク受領者アグリーメントに署名してそれを実施する必要がある。

トラストマーク依拠当事者がトラストマークを信頼することを選択した場合、トラストマーク依

拠当事者はトラストマークプロバイダとトラストマーク依拠当事者アグリーメントを締結する必要がある。トラストマーク依拠当事者アグリーメントは、2 者間契約でもあるが、両者が署名しなければならないのは、標準的な 2 者間アグリーメントではない。代わりに、トラストマークプロバイダによって発行されたトラストマークを使用または信頼するトラストマーク依拠当事者によって有効になる「クリックラップ」または「クリックスルー」アグリーメントである。トラストマーク依拠当事者アグリーメントには、トラストマークポリシも参照として組み込まれている。

トラストマークの発行には、適切なトラストマークポリシ、トラストマーク受領者契約、およびトラストマーク依拠当事者アグリーメントの設定が必須である。

2.1.4 NIEF におけるトラストマークの適用例

NIEF（National Identity Exchange Federation）は米国政府における法執行に関する機微なデータ共有を目的とした米国政府機関の集合体であり、CISA（Criminal Information Sharing Alliance)、RISS (Regional Information Sharing Systems)、 DHS（US Department of Homeland Security ）や FBI (Federal Bureau of Investigation) 等が参加しており、情報共有時の信頼保証にトラストマーク及びトラストマークフレームワークを採用している。

以下の図 10 は NIEF(National Identity Exchange Federation)におけるトラストマークの例を示す。

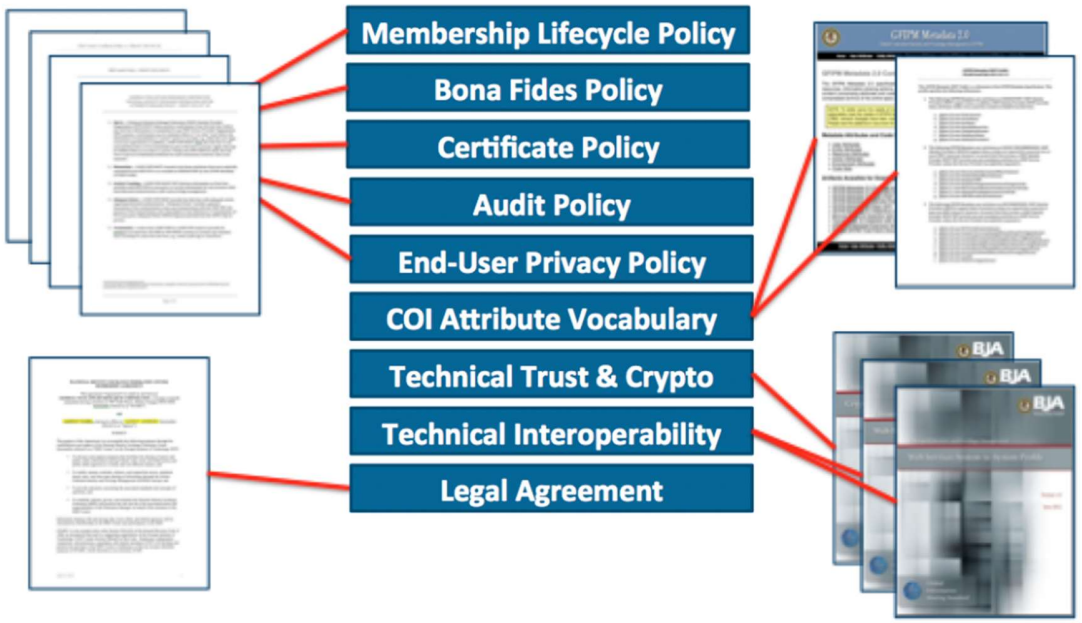


図 10　NIEF におけるコンポーネント化とトラストマーク

- Membership Lifecycle Policy
  政府機関の NIEF への参加条件及び脱退に関する規定
- Bona Fides Policy
  政府機関がその正当性を確認するための文書及びアーティファクトに関する規定
- Certificate Policy
  SAML アサーション等の他の政府機関が依拠する機微なデータへ署名を行う場合の秘密鍵の管理に関する規定
- Audit Policy
  メンバー及びメンバー候補に対し、NIEF のポリシーへの適合性監査を実施する際の規定
- End-User Privacy Policy
  メンバーが従うべきプライバシー保護に関する規定
- COI-Specific Attribute Vocabulary
  IdP が保証するユーザの属性情報に関する構文とその意味 (Syntax and Semantics)に関する規定
- Technical Trust & Crypto
  信頼性検証に関する規定
- Technical Interoperability
  メンバー間の標準通信プロトコル（SAML や SOAP 等の）に関する規定
- Legal Agreement
  メンバーの法的な役割及び責任関する規定

参照情報

[1] Trustmark Framework Technical Specification
https://trustmarkinitiative.org/specifications/trustmark-framework/1.2/tfts-1.2.pdf

2.2 NIST Cyber-Physical System

2.2.1 NIST Cyber-Physical System 概要

NIST は Cyber-Physical System（CPS）のフレームワークとして NIST SP 1500-201 を 2017 年に公開している。このフレームワークでは、CPS 分析の方法論と用語を定義することを主目的としている。以下の図 11 はこのフレームワークの概要図である。

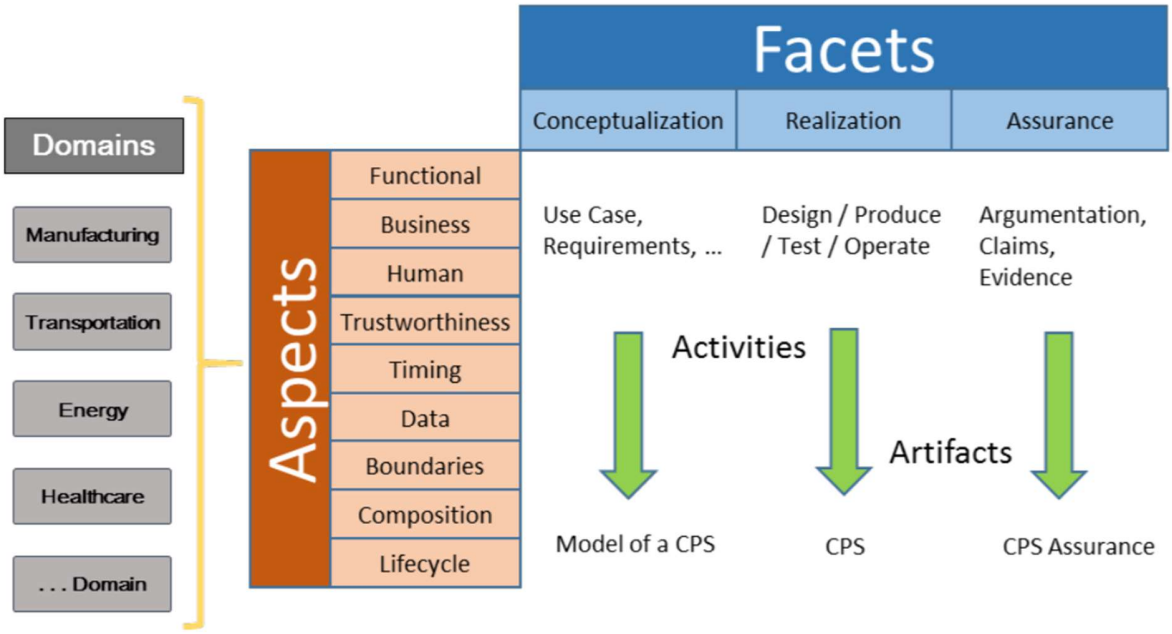


図 11　CPS フレームワーク

- Domains（ドメイン）
  アプリケーションに応じた CPS のドメイン。製造業、輸送業、エネルギー産業、ヘルスケア産業等の異なるアプリケーションによって CPS に求められる要件は変化する。
- Aspects（観点）
  ドメイン間の社会的／ビジネス的／技術的な横断的懸念事項を特定し、共通項をグルーピングした結果、9 つの観点を定義している。
- Facets（ファセット、側面）
  各観点に対してそれぞれ、概念化(Conceptualization)、現実化(Realization)、保証(Assurance)の 3 つの側面を定義している。

概念化の側面では、CPS の目標やユースケース、機能要件等を定義し CPS のモデル化を行い、現

実化の側面では設計、製造、シミュレーション、試験及び運用等を通じて実際の CPS の構築を行い、保証の側面では、概念化によってモデル化された CPS の要件を現実化によって構築された実際の CPS が満たしているかを検証する。

2.2.2 観点と懸念事項

NIST CPS で特定されている CPS の観点は全部で 9 つであり、それぞれに対して複数の懸念事項が特定されている。

1. Functional(機能)
   懸念事項：Actuation, Communication, Controllability, Functionality, Manageability, Measurability, Monitorability, Performance, Physical, Physical context, Sensing, States, Uncertainty
2. Business(ビジネス)
   懸念事項；Enterprise, Cost, Environment, Policy, Quality, Regulatory, Time to market, Utility
3. Human(人間)
   懸念事項：Human factors, Usability
4. Trustworthiness（信頼）
   懸念事項：Privacy, Reliability, Resilience, Safety, Security
5. Timing(タイミング)
   懸念事項：Logical time, Synchronization, Time awareness, Time-interval and latency
6. Data（データ）
   懸念事項；Data semantics, Identity, Operation on Data, Relationship between Data, Data velocity, Data volume
7. Boundaries(境界)
   懸念事項：Behavioral, Networkability, Responsibility
8. Composition(構成)
   懸念事項：Adaptability, Complexity, Constructivity, Discoverability,
9. Lifecycle（ライフサイクル）
   懸念事項：Deployability, Disposability, Engineerability, Maintainability, Operability, Procureability, Producibility

2.2.3 各側面（ファセット）におけるアクティビティ

前項の 9 つのドメイン及び懸念事項に対して、CPS が定義する概念化、現実化及び保証の各側面に対するアクティビティとアクティビティの成果物であるアーティファクト（表中、➡表記で示す）

は以下の表2の通りである。

表2　側面（ファセット）とアクティビティ及びアーティファクトの対応表

側面（ファセット）	アクティビティ
概念化	ミッションとビジネスケースの開発 ➡ビジネスユースケース
	機能分解 ➡詳細なユースケース、アクター、情報交換
	要件分析 ➡機能／非機能要件要件定義
	要件配分 ➡HW/SW 構成アイテム
	インターフェース要件分析 ➡インターフェース要件
現実化	ビジネスケース分析 ➡トレードスタディ（トレードオフスタディ)、ライフサイクルコスト分析、インセンティブや規制の特定
	ライフサイクルマネジメント ➡ライフサイクルマネジメントプラン、持続可能性プラン
	設計 ➡設計文書、トレードオフ分析、要件検証、ヴァーチャルプロトタイプ
	製造／実装 ➡製品、統合製品、テスト計画、テスト結果
	運用 ➡性能、品質、製品発展追跡
	廃棄 ➡再利用、持続性とエネルギー回収評価、廃棄マニフェスト
	サイバーフィジカルアブストラクション層の形成 ➡ドメイン固有の存在論、モデリング言語、セマンティック仕様
	物理層の現実化 ➡CPS の物理的要素
保証	アイデンティティ保証目標 ➡保証目標／分析レポート
	保証戦略の定義

	➡戦略文書／計画
	制御保証のエビデンス ➡制御文書
	エビデンス分析 ➡分析レポート
	保証引数の提供 ➡保証引数レポート
	確信度の推定の提供 ➡確信度の推定
	構成監視 ➡製品構成評価
	要件検証 ➡要件／テスト結果評価
	製品認証、規制適合性試験 ➡認証書

2.3 CPS の適用例：IES-City フレームワーク

NIST CPS のフレームワークに基づいてドメイン固有の CPS フレームワークが定義されている一例として IES-City(Internet of things Enabled Smart City)フレームワークがある。スマートシティのさまざまなアーキテクチャ設計の原則、分類法、および標準は複数の場、組織において開発および提案されているが、IoT の可能性をスマートシティで実現するための標準化の取り組みはまだ収束していない。NIST は、米国内および国外パートナーと共に、「IoT 対応スマートシティフレームワークに関する国際テクニカルワーキンググループ」を設立し、既存アーキテクチャ全体の相互運用性（PPI）の要点を特定し、共通のアーキテクチャ機能のコンセンサスフレームワークドキュメントを作成した。このフレームワークドキュメントは、都市がコミュニティのニーズを満たす相互運用可能でスケーラブルなスマートシティソリューションを採用する際にサポートとなる文書である。

IES-City フレームワークでは、NIST SP 1500-201 の CPS フレームワークに基づいたスマートシティにおける CPS フレームワークの策定だけでなく、スマートシティの設計／開発、管理者、アプリケーションベンダー向けのツールを作成している。このツールは、アプリケーションのカテゴリーとサブカテゴリー、ICT レベル、ジオドメインを選択することで、当該アプリケーションにおける懸念事項とスマートシティ分野の CPS における要件が自動でリスト化されるものである。

2.3.1 IES-City アプリケーションのカテゴリ、サブカテゴリ、ICT レベル及びジオドメイン

以下の表 3 は IES-City フレームワークで特定された、スマートシティ CPS におけるカテゴリ、サブカテゴリ、およびジオドメインの一部抜粋である。カテゴリとしては表 3 のほかに輸送、教育、ヘルス、社会経済開発、公共安全がある。

表 3　カテゴリ、サブカテゴリ、ジオドメインの抜粋

カテゴリ	サブカテゴリ	ジオドメイン
環境構築	スマートホーム	住宅
	スマートビルディング	住宅
		ビルディング
		集合体（ショッピングモール、大学キャンパス等)
		全て
	土地利用／管理	街
		国
		全て
水道及び排水	取水／管理	区域
		街
		国
		全て
	給水	集合体（ショッピングモール、大学キャンパス等)
		街
		国
		全て
	消費	住宅
		ビルディング
		集合体（ショッピングモール、大学キャンパス等)
		区域
		街
		全て
	排水管理	集合体（ショッピングモール、大学キャンパス

		等)
		区域
		街
		全て
エネルギー	電力供給	集合体（ショッピングモール、大学キャンパス等)
		区域
		街
		国
		全て
	送配電	国
		全て
	電力需要	集合体（ショッピングモール、大学キャンパス等)
		区域
		街
		全て

この分類に加え、アプリケーションがどの ICT レベル（センサー、データ、アプリケーション、ユーザインタフェースあるいはすべて）であるのかをツール上で選択することで、スマートシティアプリケーションの CPS における懸念事項、レディネス及び利益が自動でリスト化される。

以下の表 4 は、スマートビルアプリケーションにおけるツールで自動生成されたアウトプットの例である。

表 4　スマートビルアプリケーションにおける懸念事項リスト

Aspect	Concern	Abstract requirements	Specific implementation requirements
Functional	Actuation	- to control building energy systems - Device control and configuration (Support of remote monitoring, control and configuration of devices)	- actuation capabilities - smart devices

	Communication	- capacity to exchange information internal to the system - Heterogeneous communication support (various kinds of wired or wireless technologies (ZigBee, Bluetooth, …) and support for heterogeneous device related communication technologies) - sensors communication protocols (standard-based) - sensor network communication protocols (based on standard) - user centric design applications - accessibility	- Home management systems - Sensor network
	Functionality	- energy management - alarm management - fault detection and diagnosis	- Automation and real-time analytics - integration with utilities and city infrastructure

	Controllability	- Device control and configuration (Support of remote monitoring, control and configuration of devices)	- Internet connection - remote control software
	Performance	- to provide feedback in time to act	- fast and reliable network - real-time systems
	Physical context	- to detect presence of people	- sensors (motion, presence, ...)
	Sensing	- to detect presence of people - persistent communications - to elaborate data received from home energy systems - capacity to analyze and elaborate received data and make decisions	- sensors - persistent communications technologies - decision support systems
	Monitorability	- dashboard - authentication mechanisms	

Human	**Usability**	- to provide human readable, unambiguous and aggregated data - Programmable interfaces	
Business	**Utility**	- to provide effective information to reduce costs - to improve quality of life of residents	- fast and reliable network - real-time systems
Trustworthiness	**Safety**	- persistent monitoring - to provide data in time to act	- fast and reliable network - real-time systems
	Privacy	- to define privacy policy	- privacy protection mechanisms

	Security	- to preserve authorized restrictions on access and disclosure - to prevent modification or destruction of system - to ensure non-repudiation and authenticity - to ensure timely and reliable access to and use of a system - sensor network security protocols - digital signature - cryptography - Communication security (Secure, trusted and privacy protected communication) - Data management security (Secure, trusted and privacy protected data management capability) - entity authentication mechanisms - intrusion detection systems - intrusion prevention systems	- firewall - antispyware - antivirus

		- service provision security (Secure, trusted and privacy protected service provision capability) - Integration of security policies and techniques (ability to integrate different security policies and techniques: consistent security control over the variety of devices and user networks) - reliability - mutual authentication and authorization	
Timing	**Logical time**	- to take into account the sequence of the events	
	Time awareness		
	Managing timing and latency	- to send data in a timely manner - managing time and latency systems	
	Synchronization	- to send data with a common time scale - sensor synchronization algorithm	- Time synchronization

Data	Data semantics	- to correctly understand the meaning of the data - standard data models - semantic annotation and access to data of things - semantic storage, transfer and aggregation of data of thing	
	Operations on data	- to harmonize data from different sources - electronic data format (based on standard) - public interfaces	
	Relationship between data	- to connect data from different sources - public, shared and standard data models - public interfaces	
Boundaries	Behavioral	- capacity to interact with system from other domains	- Software interfaces

参照資料

[1] NIST Special Publication 1500-201, Framework for Cyber-Physical Systems: Volume 1, Overview, Version 1.0
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf

[2] A Consensus Framework for Smart City Architectures, IES-City Framework, V.1.0
https://s3.amazonaws.com/nist-sgcps/smartcityframework/files/ies-city_framework/IES-CityFramework_Version_1_0_20180930.pdf

3 慶應義塾大学主催サイバーセキュリティ国際シンポジウム

3.1 第 8 回シンポジウム

3.1.1 開催概要

サイバーセキュリティは様々な形で議論されている一方、その相対となる「トラストサービス」が今日まさに始まろうとしている。同時に、経済活動はすでにデジタル化され、国際化されている状況にある。我々の日常生活において、トラストサービスは人の信頼を基本にサイバー空間に取り入れられている。今後の課題は、この「トラスト」を技術、運用、政策のレベルで、どのように解決していくかにある。

第 8 回シンポジウムでは、デジタル・エコノミーの越境問題を解決するために、AI、ビッグデータ、IoT などを活用したソサエティー5.0、グローバル・サプライチェーンを前回のシンポジウムに引き続き議論し、安心安全なサイバー空間を提供するトラストサービスの本質に焦点を当てた。米国、英国、イスラエル、EU、オーストラリア、日本の有識者ならびに関係者などが一堂に介し検討した。

2 日間にわたるプログラムでは、全体会議での基調講演とパネルセッション、テーマごとにより深いパラレルセッションを設け、世界最高峰の専門家がサイバーセキュリティとトラストの世界情勢について、産官学の関係者を交えて、意見交換をした。

3.1.2 スケジュール

Date:
July 11 - 12, 2019
DAY 1 (Thursday, July 11, 2019) 9:00 - 18:10 Plenary Keynote Speeches & Panels
18:30 - 20:00 Reception
DAY 2 (Friday, July 12, 2019) 9:00 - 17:45 Keynote Speeches & Panels
Venue:
Keio University, Mita Campus, 1F West School Building (#5 on the campus map)
https://www.keio.ac.jp/en/maps/mita.html
Reception Venue:
West School Building B1F Student Cafeteria
Host and Organizer:
Keio University Cyber Security Research Center & Sasakawa USA
Registration Fee:
Free (Reception included)

プログラム
1日目 - 2019年7月11日(木) –

9:00 - 15:45 全体会議: 西校舎 1F ホール (同時通訳付き)

9:00 - 9:05	オープニング - 手塚 悟 （慶應義塾大学大学院 政策・メディア研究科特任教授） - デニス・ブレア （笹川平和財団米国会長） ※ビデオメッセージ
9:05 - 9:15	慶應義塾からの挨拶 - 村井 純 （慶應義塾大学大学院 政策・メディア研究科委員長 兼 教授） - 國領 二郎 （慶應義塾常任理事、総合政策学部教授） - デイビッド・ファーバー（慶應義塾大学サイバー文明研究センター教授）
9:15 - 9:25	INCS-CoE からアナウンスメント チャーター合意調印式と新ボードメンバー紹介
9:25 - 10:05	各国からの挨拶 - 藤末 健三 （参議院議員） - キース・カーカム（在日米国大使館商務担当公使） - スー・木下 （駐日英国大使館 公使参事官） - アリエ・ロゼン （駐日イスラエル大使館 文化・科学担当官） - フランチェスコ・フィニ （駐日欧州連合代表部 公使） - リチャード・コート （駐日オーストラリア大使）
10:05 - 10:15	MOU 調印式
10:15 – 10:25	休憩 (コーヒーブレイク)
10:25 - 10:45	基調講演 – 遠藤 信博 （日本電気株式会社 代表取締役会長）
10:45 - 12:15	日本国政府講演 - 其田 真理 （個人情報保護委員会事務局長） - 大鷹 正人 （外務省 総合外交政策局 審議官 サイバー政策担当大使） - 山内 智生 （内閣官房 内閣サイバーセキュリティセンター副センター長 内閣審議官） - 竹内 芳明 （総務省サイバーセキュリティ統括官） - 三角 育生 （内閣官房 内閣サイバーセキュリティセンター 内閣審議官経済産業省サイバーセキュリティ・情報化審議官） - 菱山 豊 （文部科学省大臣官房サイバーセキュリティ・政策立案総括審議官）
12:15 - 13:00	休憩
13:00 - 14:00	基調パネル テーマ：サイバーセキュリティにおけるトラストサービス モデレータ： アラン・フリードマン （米国商務省NTIAサイバーセキュリティ戦略ディレクター） パネリスト： - 村井 純 （慶應義塾大学大学院 政策・メディア研究科委員長 兼 教授） - アンドリュー・マーチン （オックスフォード大学） - ステファン・クレーマー （駐日欧州連合代表部） - ジョン・マンファデリ （ノースイースタン大学）
14:00 - 15:00	各国講演 米国： アラン・フリードマン （米国商務省NTIAサイバーセキュリティ戦略ディレクター） 英国：クリス・ハンキン（インペリアル・カレッジ・ロンドン セキュリティ科学技術インスティテュート副ディレクター） EU： コスタ・カプソロポウロス （欧州委員会 DG COONECT 政策官） ※ビデオメッセージ
15:00 - 15:45	INCS-CoE メンバー講演 - ハワード・シュローブ （Principal Research Scientist, CSAIL, MIT） テーマ： C2C CTF - アンドリュー・マーチン（Prof of Systems Security, Director, Centre for Doctoral Training in Cyber Security, Department of Computer Science, University of Oxford） タイトル：信頼できるインターネットへ向けて：頑強なトラスト・オンライン・サービスを構築するステップとは？
15:45 – 16:00	休憩

=DAY 1= 16:00 – 18:10: パラレルセッション （以下 4 会場）

16:00 – 17:00 (S1)

D1-T1-S1: 北館 1 F ホール - 同時通訳付き

在日米国大使館

モデレータ：アラン・フリードマン （米国商務省NTIAサイバーセキュリティ戦略ディレクター）

パネリスト：

- バーバラ・グルーイ （MITRE Corporation）
- ジョン・マンファデリ （ノースイースタン大学）
- 出雲 秀一 （シスコシステムズ グローバル政策・政府渉外本部長）
- 片山 建 (日本マイクロソフト株式会社 政策渉外・法務本部デジタル政策部長)
- オム プラカシュ (ノースロップ グラマン ジャパン)

D1-T2-S1: 東館 6F G-Sec Lab.

「制御システム分野」でのセキュリティ人材育成への取組み

モデレータ：

砂原 秀樹（慶應義塾大学大学院メディアデザイン研究科 教授/ 慶應義塾大学先導研究センターサイバーセキュリティ研究センター センター長）

パネリスト：

- 千葉 寛之 （株式会社日立製作所 セキュリティ事業統括本部サイバーセキュリティ技術本部 セキュリティ人財統括センタ センタ長）
- 荒川 大 （一般社団法人サイバーリスク情報センター 事務局長）

D1-T3-S1: 北館 3F 大会議室

日本企業が本当に必要とする人材とは？ ～今必要なのは「プラス・セキュリティ人材」だ～

モデレータ：上杉 謙二 （日本サイバーセキュリティ・イノベーション委員会 主任研究員)

パネリスト：

- 中村 和訓 （東日本旅客鉄道株式会社 技術イノベーション推進本部システムマネジメント部門部長）
- 丸山 満彦
（デロイトトーマツサイバー合同会社執行役員（Chief Business Development Officer）兼デロイトトーマツサイバーセキュリティ先端研究所所長）
- 平山 敏弘 （日本サイバーセキュリティ・イノベーション委員会 主任研究員）

D1-T4-S1: 研究室棟 A会議室/ B会議室

Country 2 Country CTF

モデレータ：ハワード・シュローブ （Principal Research Scientist, CSAIL, MIT）

パネリスト：

- フランク・スタヤノ （ケンブリッジ大学）
- キース・メイス （ロイヤル・ホロウェイ）
- アダム・ヘンリー （ニューサウスウェールズ大学 キャンベラ 非常勤講師）

17:00 - 17:10 Break

17:10 - 18:10 (S2)

D1-T1-S2: 北館 1 F ホール - 同時通訳付き

テーマ： トラストと協調的ディフェンス（英国モデル）

サブ・テーマ： 協調的ディフェンスとしての脅威情報

モデレータ：小原 浩之 (デジタル規範研究所Director)

パネリスト：

- カータン・マクローリン （日本サイバーディフェンス株式会社CEO）
- トニー･バイロン （日本サイバーディフェンス株式会社UK 上席脅威情報コンサルタント）

D1-T2-S2: 東館 6F G-Sec Lab

強化する日米二カ国間情報共有：なぜ今重要なのか？

モデレータ： リントン・ウェルズ （ジョージ・メイソン大学）

パネリスト：

- ポール・ゴールドシュタイン （Pacific Tech Bridge）
- 藤末 健三 （参議院議員）
- 苫米地 英人 (カーネギーメロン大学CyLabフェロー)

D1-T3-S2: 北館 3F 大会議室

トラストサービスのある社会、無い社会

- 楠 俊樹（株式会社三井住友銀行事務統括部 上席推進役）
- 小川 博久（NPO日本ネットワークセキュリティ協会（JNSA） 電子署名WG サブリーダー/ 日本トラストテクノロジー協議会（JT2A） 運営委員長）
- 大泰司 章 （JIPDEC インターネットトラストセンター 企画室長）
- 坂本 恒之 （株式会社スマイルワークス代表取締役社長）

- 柴田 孝一 （トラストサービス推進フォーラム（TSF） 企画運営部会長）
- 上原 小百合 （日本文書情報マネジメント協会(JIIMA) R&Dデータ保存研究会 座長）

D1-T4-S2: 研究室棟 A会議室/ B会議室
Enhancing Trust through Security Policy
モデレータ： 土屋 大洋 （慶應義塾大学大学院政策・メディア研究科 教授）
パネリスト：
- 伊奈 康二（経済産業省 商務情報政策局 サイバーセキュリティ課 課長補佐）
- 横浜信一（CISO, NTT）
- 後藤 淳（CISSP, Executive Specialist, National Security Solution Division, NEC)
- ラスティ・トス（ノースロップ・グラマン）

18:30 - 20:00 レセプション（慶應義塾大学三田キャンパス 西校舎B1F食堂）

2日目 - 2019年7月12日(金) –

9:00 - 13:30 全体会議及びスピーチとパネル: 西校舎 1F ホール (同時通訳付き)

9:00 - 9:05 オープニング
- 手塚 悟 （慶應義塾大学大学院 政策・メディア研究科特任教授）
- バッド・ロス （笹川平和財団米国） ※ビデオメッセージ

9:05 - 9:25 Society 5.0
佐藤 文一 （内閣府大臣官房審議官（科学技術・イノベーション担当））

9:25 - 10:55 全体パネル
テーマ：Society 5.0を支えるトラスト基盤
モデレータ： 市川 芳明 （多摩大学 客員教授）
パネリスト：
- 新井 亨 （株式会社JERA 東日本O&M営業部 部長）
- 森 伊織 （東日本旅客鉄道株式会社 技術イノベーション推進本部 主席）
- 須賀 千鶴 （世界経済フォーラム第四次産業革命日本センター長）
- 迫田 章平 （経済産業省産業創造課）

10:55 - 11:10 - 休憩 (コーヒーブレイク)

11:10 - 12:10 講演
- バーバラ・グルーイ (MITRE Corporation)
タイトル:「サイバーのサプライチェーン：不完全な世界におけるリスク管理」
- リントン・ウェルズ （Executive Advisor for the C4I & Cyber Center, George Mason）
タイトル：「5GとSociety 5.0 について」
- ポール・ゴールドシュタイン （President/CEO, Pacific Tech Bridge）
タイトル：「世界政治の状況変化：日米関係のチャレンジとは？」

12:10 - 13:30 休憩

=DAY 2= 13:30 – 17:45 パラレルセッション （以下 4 会場）

15:45 - 16:45 (S3)

D2-T1-S3: 北館 1 F ホール - 同時通訳付き
オーストラリアにおけるサイバーセキュリティ対策について
モデレータ：スコット・モリス （オーストラリア大使館 参事官（商務））
パネリスト：
- クリストファー・リッキー （メルボルン大学 情報理工学系研究科 教授）
- クレイグ・ヴァリ （エディスコーワン大学 理工学部サイバーセキュリティ研究科 教授）
- アダム・ヘンリー （ニューサウスウェールズ大学 キャンベラ 非常勤講師）

D2-T2-S3: 東館 8F ホール
Smart Cityの推進におけるセキュリティ課題について
モデレータ：今井 俊宏 （シスコシステムズ合同会社 イノベーションセンター センター長）
パネリスト：
- 木村 公彦 （総務省 サイバーセキュリティ統括官付参事官（総括担当））
- 相川 航 （総務省 サイバーセキュリティ統括官室 参事官補佐）
- 藤田 範人（日本電気株式会社 セキュリティ研究所 研究部長（兼）PSネットワーク事業推進本部 シニアエ

キスパート）

D2-T3- S3: 北館 3F 大会議室
今考える、超スマート社会を支えるこれからのサプライチェーンに必要なこと
モデレータ：石原 修 （株式会社日立製作所 セキュリティ事業統括本部 セキュリティインキュベーション推進本部 本部長）
パネリスト：
- 鴨田 浩明 （経済産業省商務情報政策局サイバーセキュリティ課 企画官）
- 神納 祐一郎 （三菱重工業株式会社 マーケティング＆イノベーション本部 フェローアドバイザー）
- 中島 洋 （株式会社 日立ハイテクノロジーズ）
- 渥美 俊之 （株式会社日立製作所 サービスプラットフォーム事業本部 セキュリティ事業統括本部 セキュリティインキュベーション推進本部
セキュリティインキュベーション推進部 担当部長）

D2-T4- S3: 研究室棟 A会議室/ B会議室
暗号資産交換所システム運用のセキュリティ
モデレータ：鈴木 茂哉 （慶應義塾大学大学院 政策・メディア研究科 特任教授）
パネリスト：
- 林 達也 （ココン株式会社 技術領域投資室 パートナー）
- 中島 博敬 （株式会社メルカリ R4D シニアリサーチャー）

16:45 - 17:45 (S4)

D2-T1-S4: 北館 1 F ホール - 同時通訳付き
ISACs 2.0
モデレータ：バーバラ・グルーイ （MITRE Corporation）
パネリスト：
- 青木 一彦 （電力ＩＳＡＣ 事務局次長/ 電気事業連合会 情報通信部 副部長）
- チャーリー・ハート （Auto-ISAC lead, Hitachi America, R&D）
- 益岡 竜介 （富士通システム統合研究所 シニアプロフェッショナル）

D2-T2-S4: 東館 8F ホール
クラウド署名の最新グローバル動向ークラウド署名コンソーシアムの活動報告
モデレータ：
小川 博久（NPO日本ネットワークセキュリティ協会（JNSA） 電子署名WG サブリーダー/ 日本トラストテクノロジー協議会（JT2A） 運営委員長）
パネリスト：
- アンドレア ヴァッレ （アドビ ドキュメントクラウド シニアプロダクトマネージャー クラウド署名コンソーシアム 会長）
- 宮地 直人 （有限会社ラング・エッジ 取締役、プログラマ）

D2-T3-S4: 北館 3F 大会議室
経営課題としてのサイバーセキュリティ
モデレータ：
梶浦敏範 （株式会社日立製作所 上席研究員/ 日本経済団体連合会 デジタルエコノミー推進委員会企画部会 部会長代行,
サイバーセキュリティ委員会サイバーセキュリティ強化WG 主査/ 日本サイバーセキュリティ・イノベーション委員会（JCIC）代表理事）
パネリスト：
- 中谷 昇 （ヤフー株式会社 執行役員 政策企画統括本部長）
- 青木 優美 （日本サイバーセキュリティイノベーション委員会 主任研究員）

D2-T4-S4: 研究室棟 A会議室/ B会議室
サイバーセキュリティと監査
モデレータ：大木 栄二郎 （工学院大学 名誉教授）
パネリスト：
- 相羽 律子 （株式会社日立製作所 セキュリティ事業統括本部 サイバーセキュリティ技術本部 セキュリティ人財統括センタ 統括主任技師）
- 洞田 慎一 （一般社団法人 JPCERTコーディネーションセンター 経営企画室 兼 早期警戒グループ 担当部

門長）
- 永宮 直史 （特定非営利活動法人日本セキュリティ監査協会 事務局長）

3.1.3 サプライチェーンとトラストに関わるセッション

3.1.3.1 【基調パネル】 サイバーセキュリティにおけるトラストサービス

モデレータ：Allan Friedman（米国商務省 NTIA サイバーセキュリティ戦略ディレクター）
パネリスト：
村井　純（慶應義塾大学院　政策・メディア研究科委員長　兼　教授）
Andrew Martin（オックスフォード大学）
Stefan Kramer（駐日欧州連合代表部）
John Manferdelli（ノースイースタン大学）
[概要]
○　Trusted service は何か。
①　最も簡単なものとして、CA が提供する身元があるが、このサービスにおいても大きな問題が発生してきた。
②　ソフトウェア（更新を含む）については、過去 15 年間で劇的に改善されたが、いまだに不均一で評価が困難である。
③　ハードウェアについては、以前は評価が簡単であったが、現在では非常に困難であり、大きな問題となっている。
④　世評に基づくその他のサービス（および監査されたプロセス）については、Google、銀行（ただし、米国では失敗に対する法的責任を負う）、CNN、Gmail、など...
○　技術：サービス ID は大きな課題である。（多くの ID 保証作業がユーザ ID に費やされているのにも関わらず、サービス ID の障害は日常的に悪用されている。）
○　技術とビジネス：特にセキュリティ/トラスト面で、多くの QoS 差別化要因があり、必ず前面に現れる。これまでも負荷時の稼働時間とパフォーマンス/拡張性は恐らく最大であったが、データとアルゴリズムの適切な取り扱いを示す手段は、より明白なものになる。これは、プロバイダが経済的問題や合併・吸収に直面した場合に特に問題となる。
同様に、サービスサプライチェーンの可視性を高めることは、今後の堅牢なビジネスと規制の遵守に不可欠である。、データの出所は多くの研究的関心を集めている一方、「偽のデータ」に依存するリスクは、現状、あまり注目されていない。しかし、これは、今後の課題であることに間違いない。

3.1.3.2 【各国講演】 ソフトウェア部品表　ソフトウェアコンポーネントの透明性に関する NTIA の取り組みの概要

Allan Friedman（米国商務省 NTIA サイバ―セキュリティ戦略ディレクター）
[概要]
○　透明性は市場の繁栄に役立つ
・　食品成分と食品ラベル

・　化学産業における安全性データシート
・　業界のハードウェア部品表
・　コンポーネントに名前を付けて追跡することで、イノベーションを促進できる。
（例：CVE）

○　ソフトウェアサプライチェーンの役割と SBOM のメリット
○　どうして今日これをしないのか？
・　ライセンスに関する懸念－GPL コードを出荷するのは誰か？
・　困難：利益を得るには、より広範な採用とマシンの可読性が必要。
・　誰もソフトウェアデータを要求しないので、提供されない。 同様に、誰もそれを提供しないので、誰もそれを求めない。
○　NTIA モデル：「マルチステークホルダープロセス」

多様なステークホルダをまとめるオープンで透明性の高いコンセンサスベースのプロセスは、エコシステム全体の実質的な進展を促進する。

図 The NTIA model: “multi stakeholder processes”
＜出典：講演資料　Software Bill of Materials　An overview of NTIA’s initiative on Software Component Transparency より＞

○　NTIA が実施していないこと
・　規制
・　ソースコードの開示
・　標準の開発
○　解決すべき問題
・　最新のソフトウェアシステムには、複雑で機能的なサプライチェーンが含まれる。
・　これらのシステムの構成と機能に対するシステムの透明性の欠如は、開発、調達、および保守のコストだけでなく、サイバーセキュリティリスクにも大きく影響している。
・　相互接続がますます進む世界では、リスクとコストは個人や組織だけでなく、公共の安全や国

家安全保障などの集合財にも直接影響する。

○　透明性ソリューションがどのように役立つか

・　脆弱なシステムとインシデントの根本原因の特定の強化
・　疑わしいまたは偽造のソフトウェアコンポーネントの特定
・　計画外および非生産的な作業の削減
・　十分な情報に基づいた市場の差別化とコンポーネントの選択をサポート
・　複数のセクターにわたってフォーマットを標準化することにより、作業の重複を削減

3.1.3.3【INCS-CoE メンバー講演】 信頼できるインターネットへ向けて：頑強なトラスト・オンライン・サービスを構築するステップとは？

Andrew Martin（Prof of Systems Security, Director, Centre for Doctoral Training in Cyber Security, Department of Computer Science, University of Oxford）

[概要]

○　信頼できるコンピューティングプラットフォーム（PC、モバイル）

信頼できる実行環境をサポートできるコンピューティングエンドポイント（PC、モバイルなど）を構築するために、過去 10～20 年で多くの努力がなされてきた。

すべての PC を軍事グレードの仕様に合わせて構築する余裕はないため、コモディティコンポーネントが必要である。

○　トラステッドプラットフォームモジュール（TPM チップ）

セキュリティ機能を保証するために、TPM チップが使用される。このチップにより、特定のブートソフトウェア/オペレーティングシステムカーネルが実行されていることを保証される。　問題は、プラットフォームにはさらに多くのソフトウェアがあり、この方法ですべてを評価するのは困難である。

○　　TPM チップは、Windows 10 および Google の Chrome OS のセキュリティ設計についてよく知られている。ただし、オペレーティングシステムカーネル自体のセキュリティを確保することに限定されている。

○　TrustZone

モバイルプラットフォーム向けの他の技術（TrustZone）には、ソフトウェア無線を正常に動作させるために特定の要件がある。

○　SGX

SGX と呼ばれる Intel の CPU 機能が最近注目されている。これは、個々のソフトウェアサブシステムを相互に、またオペレーティングシステムから保護することを目的としており、信頼できるソフトウェアをサービスとして提供するための有望な技術である。

○　クラウドでソフトウェアサービスを使用する際の課題

ラップトップを使用して、ここ以外のサービスにアクセス場合、そのサービスが何であるかについ

ての保証はない。デジタル証明書に基づいて、サービスプロバイダに対して何らかの保証された ID を持っている場合があるが、それ以外の場合は、プラットフォームや提供されるサービスの性質、ソフトウェアの正確な機能など、非公式に確立される。これでは、何が起こっているのか簡単には判断できない。
しかも、信頼されるべきコンポーネントが多くあるが、それらをコントロールすることができない。クラウドサービスはあなた自身の IT よりも信頼できるとよく言われるが、そう言うのは必ずしも簡単ではない。

○　難問

- クラウドの「ユーザ」は、サービスを信頼できるようにしたい
- サービスプロバイダは、信頼できるシステムを提供したい
- クラウドプロバイダは、必要以上に内部クラウドアーキテクチャを公開したくない

2 種類の証明が必要

① サービスプロバイダ内：
サービスが正しく運用されていることを保証する

② 顧客に対して：
サービス運用に関する保証
顧客提供のコードに関する保証

○　ビジョンと目標　まとめ

クラウドで信頼できるサービスを構築する手段を開発しようとしており、。このための技術は既に利用できる。ただし、すべての問題が解決されているわけではなく、軍用レベルのセキュリティを確立しているわけでもない。これらはコモディティコンポーネントであり、コモディティサービスに適している。

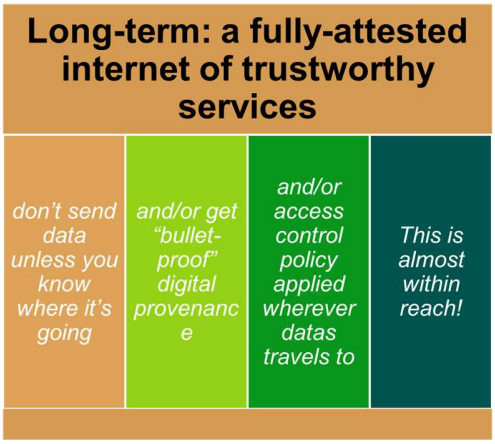


図　Long-term: a fully-attested internet of trustworthy services
<出典：講演資料　Towards a Trustworthy Internet:　steps to strongly trusted online services より>

- 「完璧な」セキュリティは常に手の届かないところにある。
- 証明サービスは、その正確性を証明することとは同じではないが、これも必要である。
- 証明はハードウェアに依拠している。ハードウェアが改ざんされていないことを保証するための個別の対策が必要である。
- 「非常に強い」ではなく、「強い」敵に抵抗する。
- 多くの複雑さが残っている。

3.1.3.4【講演】サイバーのサプライチェーン：不完全な世界におけるリスク管理

Barbara Grewe（MTRE Corporation）

[概要]

○ サプライチェーンリスクとは何か？

攻撃者が意図的に脆弱性を悪用したり、意図せずに使用して妨害や悪意のある機能を導入したり、アイテムやシステムの設計、整合性、製造、生産、流通、設置、運用、保守を損なう可能性があること。

その結果、知的財産の損失からコストの増加、パフォーマンスの低下、国家安全保障の侵害、生命の損失などが引き起こされる。

○　サプライチェーンリスクマネジメント（SCRM）は新しいものではない。

サプライチェーンリスクマネジメントには 100 年以上の進化がある。

しかし、サイバーサプライチェーンは複雑で曖昧である。

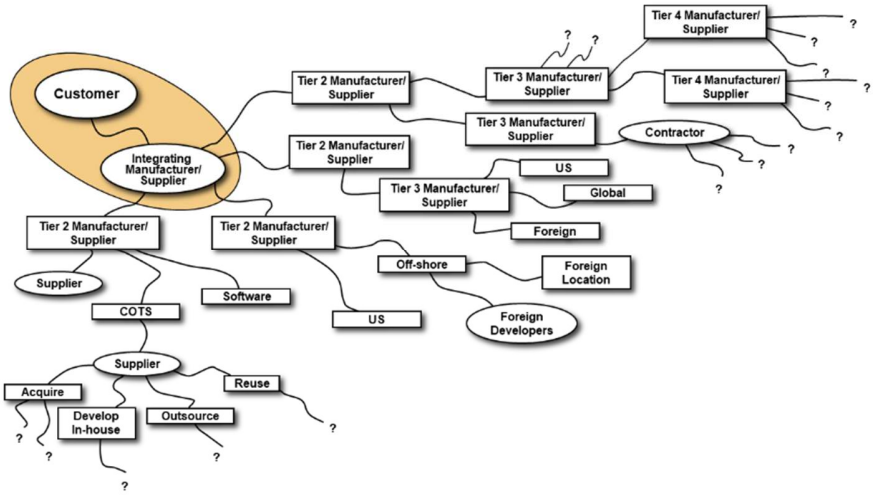


図　The Cyber supply chain

<出典：講演資料　Cyber Supply Chain – Managing Risk in an Imperfect World より>

○　多くの重要機能の多くにリモート攻撃の対象となる機能がある

重要機能はコネクテッドソフトウェアとハードウェアで構成されており、攻撃対象となっている。

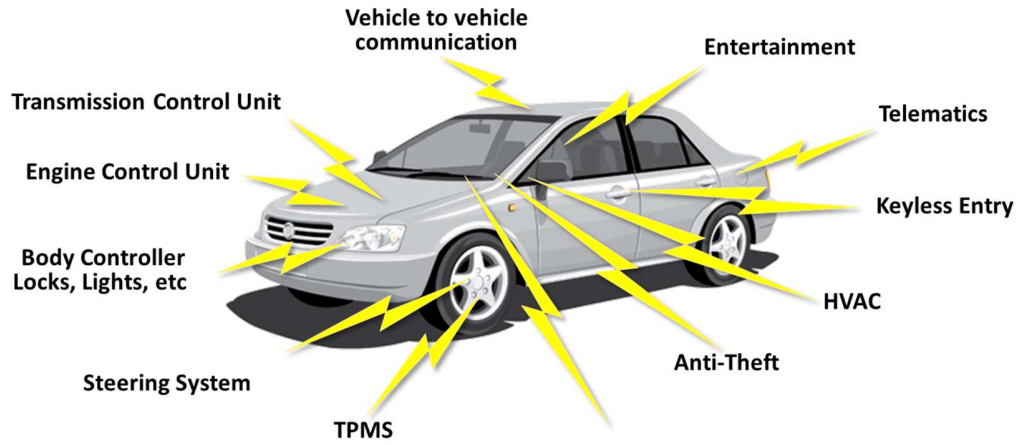


図　The Cyber supply chain
<出典：講演資料　Cyber Supply Chain – Managing Risk in an Imperfect World より>

○　国家安全保障問題でもある

・　たとえば、ボーイング 747 には、多数のサプライヤーのソフトウェアに含まれる 1400 万行以上のコードがある。
・　F35 戦闘機には 2350 万行のコードがある。
・　米軍のドローンの制御ソフトウェアには 350 万行のコードがある。
・　多くのタイプの戦闘システムは、センサー、アクチュエーター、およびソフトウェア起動制御装置にますます依存している。

コネクテッドソフトウェア対応技術への依存度はかつてないほど高くなっている。ハードウェア/ソフトウェアが脆弱であるため、これらのシステムは、意図的な行為と意図しない行為の両方に対して脆弱である。

○　サイバーサプライチェーンのライフサイクル全体が攻撃対象となりうる。

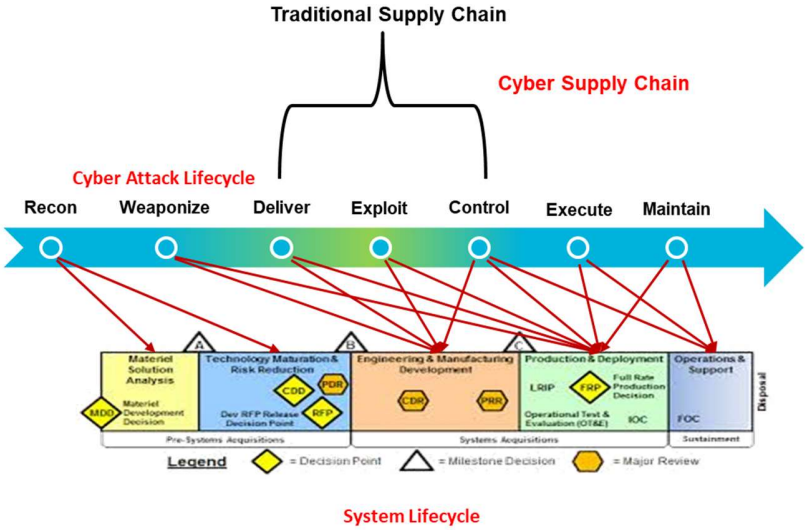


図　The Cyber supply chain lifecycle
<出典：講演資料　Cyber Supply Chain – Managing Risk in an Imperfect World より>

○　NIST サプライチェーンリスクアセスメントプロセス

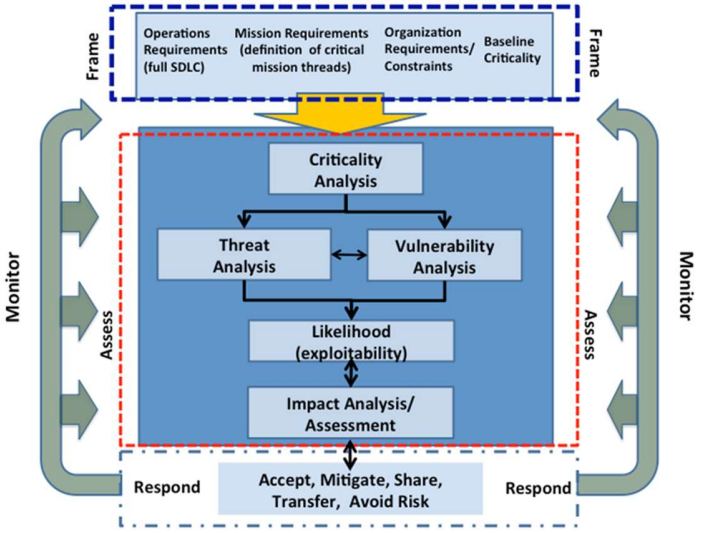


図　Derived from Supply Chain Risk Management Model (NIST SP 800-161)
<出典：講演資料　Cyber Supply Chain – Managing Risk in an Imperfect World より>

○　その他の推奨されるアクション

- 「全ソース」のサプライチェーン脅威インテリジェンスと戦略的警告を共有するために、国家反テロセンターをモデルにした政府国家サプライチェーンインテリジェンスセンター（NSIC）全体を形成する。
- リスク評価と SCRM プログラムの効果的な実施方法（リスク評価の実施を含む）について SCRM 実践者を教育するためのトレーニングを提供する
- 契約条件を使用してサプライヤーにインセンティブを与え、セキュリティを強化し、サプライチェーンリスクを効果的に管理する
- 各サプライヤーを評価するスコアリングシステムを確立するための独立したプログラムを確立する（FICO スコアリングと同様）

3.2 第 9 回シンポジウム

3.2.1 開催概要

サイバー攻撃が年々増加しており、その中には、国家の関与が疑われるものもある。2020 年のオ

リンピック/パラリンピックでも、サイバー攻撃が予想されており、深刻な被害が懸念されている。それらへ如何に対応していくか。また、5G/IoT の時代と呼ばれ、Society5.0 の社会への変遷が進行する中、トラストサービスの重要性が高まってきている。　どのようにして、デジタルエコノミーを国際間で相互協調して信頼を築いていくか。第 9 回サイバーセキュリティ国際シンポジウムでは、現状と相互協調実現のための様々な取組みの説明、議論が行われた。

3.2.2 スケジュール

Day 1

3.2.2.1【基調講演】信頼できるデジタル社会へ　~No Trust, No Digital~

高綱　直良（富士通株式会社　執行役員副会長）
[概要]
○　　サイバーセキュリティの被害が毎年増大している。Society5.0 への社会の変遷に伴い、サイバー空間とフィジカル空間の融合が進みつつあるが、Society5.0 の社会を実現させるためには、DFFT が不可欠である。
○　　富士通は、次の 2 つの取り組みを行っている：
・ルール形成－実世界で生まれ、動的に変化するデータのためのルール（安全保障、プライバシー、トラストデータ流通）が必要。
・テクノロジー開発－Trust3.0--自律分散したトラストテクノロジーで構築されるトラスト
○　　トラストな社会形成に向けた取り組み
3 つの重要なテクノロジー領域における研究開発を進めている。
①　　サイバー空間の認証基盤
②　　分散データの真正性確保
③　　サイバー攻撃対策（Proactive AI など）

3.2.2.2 日本政府講演

日本政府の各省庁より、以下の講演があった。

3.2.2.2.1　内閣サイバーセキュリティセンター　NISC

山内　智生（内閣官房　内閣サイバーセキュリティセンター副センター長　内閣審議官）
[概要]
○ 日本全体の動きとして、2018 年 7 月に、サイバーセキュリティ基本法に基づく 2 回目のサイバーセキュリティ戦略が決定し、2020 年のオリンピック／パラリンピックに備えて、今後 3 年間の諸施策の目標及び実施方針が示された。
○ 重要インフラの保護のためには、リスクアセスメントを行い、対策を行った後の残存リスクのリスクマネジメントが大切である。　常に変化するサイバーの世界に対応して、重要インフラのセ

キュリティレベルを上げる必要がある。

○ 政府として、安全・安心にクラウドサービスを採用し、継続的に利用していくために、クラウドサービスの安全性評価の仕組み--政府として安全と認めたものを登録する枠組み--を検討中である。

3.2.2.2.2　総務省

竹内　芳明（総務省サイバーセキュリティ統括官）

[概要]

○ 総務省が管轄する重要インフラは、地方公共団体及び情報通信である。

○ 国立研究開発法人 情報通信研究機構（NICT）では、未使用の IP アドレス約 30 万個（ダークネット）を活用し、サイバー攻撃の状況を観測している。　観測されたサイバー攻撃は、2018 年には 2015 年の 3.9 倍に増加し、2,000 億件を超えている。　このうち、約半数が IoT 機器を狙った攻撃となっている。

○ IoT 機器へのサイバー攻撃例として、2016 年に米国で大規模な DDoS 攻撃がある。サイバー攻撃元は、「Mirai」というマルウェアに感染した大量の IoT 機器であった。

○ 日本では、IoT 機器を狙ったサイバー攻撃への対策として、IoT 機器の脆弱性調査及び利用者への注意喚起プロジェクト「NOTICE」が、2019 年 2 月より実施されている。

　また、積極的な取り組みとして、今後製造される IoT 機器に対し、次の対策が実施されている。

- IoT 機器の要件の規定（技術基準の改正　2020 年 4 月より発効）
- CCDS3サーティフィケーションプログラム(2019 年 10 月開始)

○ 総務省主催で、電子署名、タイムスタンプ等の我が国におけるトラストサービスの在り方についての検討4が行われ、2019 年 12 月までに報告書が取りまとめられ、その後、実装に必要な措置が講じられる予定である。

3.2.2.2.3　経済産業省　業界向けのサイバーセキュリティポリシーの最近の動向

三角　育生（内閣官房　内閣サイバーセキュリティセンター内閣審議官経済産業省サイバーセキュリティ・情報化審議官）

[概要]

○　クラウドサービスの利活用

日本政府は、2018 年 6 月に、政府の情報システムに対し、クラウドバイデフォルトの原則を打ち出した。　日本では、CSP（クラウドサービスプロバイダ）がどんなセキュリティを満たしているか

[3] CCDS(Connected Consumer Device Security Council：一般社団法人 重要生活機器連携セキュリティ協議会)

[4] トラストサービス検討ワーキンググループ

を確認する仕組みがないため、安全性を評価する仕組みを決める必要がある。　まず、政府が基準を作り、セキュリティを確認できる仕組みを公表するために、経済産業省と総務省が協力して検討を行っており、間もなくパブリックコメントを募集する予定である。セキュリティ要件については、できるだけ国際標準を参考として、プロセスをしっかり確認する仕組みを作っていく。ボリュームゾーンからスタートし 2020 年秋に制度の立ち上げを予定している。なお、この制度運用のための法律が改正され、政府調達におけるクラウドサービスの安全性評価制度の実施業務を IPA が行えるようになった。

○　サイバー／フィジカルセキュリティフレームワーク（CPSF）

Society5.0 のサプライチェーンの価値創造過程のための CPSF の具体的適用に向け、3 つの TF を設置し検討を行っている。

・　3rd レイヤ TF－データ区分に応じたセキュリティ対策要件の作成
・　2nd レイヤ TF－実空間とサイバー空間を接続するデバイスに隠れたリスク
・　ソフトウェア TF－ソフトウェアマネジメントの要件

個別の標準については、セクタ毎にワーキングを作っていく。

○　サイバーセキュリティサポータ for SMEs

中小企業向けサイバーセキュリティ事後対応支援実証事業（サイバーセキュリティお助け隊)。来年度も中小企業に対して支援を行っていく。

3.2.2.2.4　外務省　日本のサイバーセキュリティ外交

山口　勇（外務省総合外交政策局　新安全保障課題政策室長）

[概要]

○　以下の 3 つを柱として、日本は、アジア太平洋地域と国際社会(UNGGE[5]、UNOEWG[6]、G7、ARF[7]、etc.)の平和と安定にさらに貢献することを目指している。

①　サイバー空間における法の支配の促進

サイバー空間への国際法の適用と平時における拘束力のない規範の展開に関する議論を促進する。

②　信頼醸成措置の開発

サイバー空間の透明性と安定性を強化することにより、サイバー紛争やエスカレーションを防ぐために、平時における信頼醸成措置を展開する。

・2 国間のディスカッションを実施　（中国、ロシア、Asia-Pacific）

③　能力開発に関する協力

他国のセキュリティホールが日本を含む世界全体のリスク要因であることを考慮して、能力開発と人材開発の支援を行う。

・セミナーの支援など(バンコクでのトレーニング提携等)

[5] UNGGE:国連サイバー政府専門家会合
[6] UNOEWG:サイバーセキュリティに関する国連オープン・エンド作業部会
[7] ARF: ASEAN地域フォーラム

3.2.2.2.5　文部科学省　大学向けのサイバーセキュリティ対策の強化

田口　康（文部科学省サイバーセキュリティ・政策立案総括審議官）

[概要]

○　大学のサイバーセキュリティについては、多くの多様な情報がある、管理が大変、及び研究者は管理されるのを嫌う等の課題がある。

○　2019 年 5 月　文部省より各大学（国立、公立／私立、先端技術）へサイバーセキュリティ対策強化を通知した。この通知の基本コンセプトは以下である。

1. 必要なシステムの準備、リソースの確保、関連スタッフの意識の向上
2. バランスのとれた優先順位付けされた対策の実施
3. 高度な技術情報を含む機密情報の保護

○　大学自身のサイバーセキュリティに対する意識を高める施策

・　大学のシステマチックなセキュリティトレーニングの実施

・　M-CYMAT[8]

・　ペネトレーションテストの実施

・　相互監査による監査―コスト節約、スキル向上、及び意見交換を実施

（山口大学と鹿児島大学）

・　Academic CSIRT ネットワークの構築

3.2.2.2.6　防衛省　自衛隊のサイバーセキュリティの施策の紹介

深澤　雅貴（防衛省サイバーセキュリティ・情報化審議官）

[概要]

○　サイバーセキュリティの状況

公開情報からだけでも、世界各地で数々のサイバー攻撃によるインシデントが発生している。その中には、非国家からの攻撃、及び国家が関与していると思われる攻撃もある。

○　自衛隊のサイバー攻撃への 6 つの対策

① 情報および通信システムのセキュリティの確保

② 専門部隊によるサイバー攻撃対処

サイバー防衛隊（24h/365 日、150 名増員し 500 名体制にする予定）など、サイバー攻撃から防護する部隊による対応

③ サイバー攻撃対処態勢の整備

情報システムのセキュリティ対策基準の制定など

④ 最先端技術の研究

サイバー演習環境構築技術、AI 活用の研究、及びサイバーレジリアンス技術

⑤ 人材育成

サイバーセキュリティの人材を育成し組織に配置、維持確保

[8] M-CYMAT (MEXT Cyber incident Mobile Assistant Team)：文部科学省サイバーセキュリティ緊 急対応支援チーム。

2020 年から防衛省主催でのコンテスト開催予定

⑥ 他機関との連携

- 日米サイバー防衛協力
- サイバーポリシーに関する日本－米国のフレームワークの確立など。
- 英、独、オーストラリア、エストニア及び NATO 等の関係国・国際機関との様々なレベルでの協議を通じた情報共有等の協力

3.2.2.2.7 警察庁　サイバーセキュリティ　日本の警察の視点

河原　淳平（警察庁サイバーセキュリティ・情報化審議官）

[概要]

○ サイバー犯罪

- サイバーテロ － 重要インフラのコアシステムへのサイバー攻撃、又はサイバー攻撃により引き起こされたと考えられるコアシステムの重大な障害。
- サイバースパイ活動

○ 日本を取り巻く環境

- 高度技術と価値ある知的財産技術を持った多くの企業が存在する。
- Society5.0 のサイバー空間と実空間の統合が進展している。
- 国家の関与が疑われるサイバー攻撃が続発している。
- 2020 年のオリンピックとパラリンピックが来年に控えている。

多くの人々はサイバーセキュリティに関して切迫感を感じていない。しかし、実際には、サイバー犯罪は増大している。

○ 最近の傾向として、オンライン銀行詐欺の件数は減少していたが、2019 年 9 月に SMS フィッシングによる不正送金被害が急増した。また、標的型攻撃による情報窃取のケースなど。IoT 機器の増大と Society5.0 への移行により、生活の利便性が増すが、同時に、サイバー空間の脅威が実空間に大きな影響を与えるようになった。また、医療機器として IoT 機器が普及してきたことにより、サイバー攻撃は人命を脅かすようになった。

○ 警察の強み

- 調査当局である。
- 全国に実働部隊がある。
- 独自の技術力を持っている。

○ 2018 年 9 月に日本の警察のサイバーセキュリティ戦略を改定した。警察の強みを生かして、当面の課題である 2020 年のオリンピック／パラリンピックに対して、サイバー攻撃の発生を前提とした対策を行う。

3.2.2.2.8 個人情報保護委員会　個人情報保護法　制度改正大綱（骨子）

其田　真理（個人情報保護委員会事務局長）

[概要]

○ 個人情報保護法は、3 年毎に見直す規定があり、2019 年が見直しに該当する。 今回、見直しの 4 つの柱を公表した。今後年内に大綱を公表し、パブリックコメントを経て、令和 2 年早期の改正法案提出を目指す。

① 個人の権利の在り方－利用停止・消去の請求に係る要件を緩和し個人の権利の範囲を広げる。

② 事業者の守るべき責務の在り方－漏洩等報告及び本人通知を義務化する、など。

③ データ利活用に関する施策の在り方―個人情報と匿名加工情報の中間的な規律としての「仮名化情報」を創設する、など。

④ 法の域外適用・越境移転の在り方－日本でビジネスをする外国人に対しても日本企業と同様に報告徴収・命令の対象とする、など。

また、これからの研究課題として、以下について議論を開始した。

- 行政機関の持っている個人情報－民間とルールが違う
- 地方自治体の個人情報－条例に依るため、地方によって異なる

3.2.2.3【基調パネル】トラストサービスの国際相互認証

モデレータ：Riccardo Genghini（ETSI TC ESI 会長）

パネリスト：

Arno Fiedler（Expert for ETSI, Nimbus Technologieberatung GmbH）

David Temoshok（NIST）

稲葉厚志（GMO グローバルサイン株式会社）

[概要]

◎EU の状況

2001 年　ヨーロッパでは TSP[9]は 2-3 社、欧州とアメリカは同調していなかった。

2019 年　市場は拡大し、180 の TSP が存在し、ISO、ヨーロッパにおける標準が出てきた。

○ EU トラストサービスの背景

- ETSI TC ESI　トラストサービスのための規格を開発してきた。
- ETSI 規格は、一般フレームワークを基礎としトラストサービスの要件を記述している。

○ 信頼できる国家レベルでトラストを構築する。

○ EU では広汎に Google、Facebook、Amazon…などもトラストサービスをやっている。彼らにも受け入れてもらわないといけない。

○ 世界中の PKI ベースのトラストサービススキームとそのトラストモデルの調査

- アンケートを行う。
- 地域ワークショップを開催（ドバイ、東京、メキシコ及びニューヨーク）

○ EU eIDAS トラストサービスと他の非 EU スキームとの相互認識の促進が目的

[9] TSP(Trust Service Provider):トラストサービスプロバイダ

○　相互承認のための技術的基盤の識別が必要
・モデル、障壁、解決策含む
○　4 つの柱の方法論
・法的背景、監督と監査、ベストプラクティス、トラスト表現
強調したいのは、“4 つの柱がトラステッドインフラには必要である“ということ。

◎ID 管理の米国標準 NIST SP 800-63-3 Digital Identity Guidelines
○　U.S. Federal Information Security Management Act：FISMA（米国連邦情報セキュリティマネジメント法）
　・　2002 年に制定され、2014 年に更新された米国連邦法
○　FISMA の実装における NIST の役割
　・　FISMA の実装のための情報システムセキュリティとリスクマネジメントのガイドラインと標準を SP 800-XXX シリーズとして発行
○　NIST SP 800-XXX Series の範囲は非常に広い
　・　サイバーセキュリティの脅威の評価と管理策
　・　セキュリティ脆弱性の特定
　・　情報システム、資産及びビジネスを保護するためのセキュリティ管理策
　・　データと情報セキュリティとプライバシー
○　NIST セキュリティと管理策　保証（トラスト）レベル
　・　NIST サイバーセキュリティ標準 800-63-3-3 は、リスクマネジメントに基づく管理策と保証レベルを提供
○　SP 800-63-3 保証(トラスト)レベル
　・　適正なレベルのリスク＋適正なレベルの保証
　・　3 種類の保証タイプに対し 3 つの保証レベルがある。
　- Identity Assurance（IAL）　　レベル 1, 2, 3
　- Authentication Assurance（AAL）　レベル 1, 2, 3
　- Federation Assurance（FAL）　　レベル 1, 2, 3
　・　相互認証の重要性
○　国際的なサイバーセキュリティの標準化
・　国際的なセキュリティ基準は国境を越えた信頼にとって重要。
・　NIST は、SP 800-XXX 規格を国際規格に合わせるよう取り組んでいる。

◎日本の PKI 状況
1.　法律の下で発行されたデジタル証明書
　　(1) 法人の代表者　（商業登記）
　　(2) 自然人

(3) 個人　[JPKI]

2. デジタル証明書の普及状況
   (1) パブリックトラステッドデジタル証明書
   (2) プライベート CA
3. 注目のトピック
   (1) トラストサービスへの政府の関心
   - ウィーンでの日欧 ICT 戦略ワークショップ　2018 年 12 月
   - 政府がトラストサービスに関する研究グループを設立
   (2) 国際相互承認に向けた試み

国際相互承認のための技術ワーキンググループ（IMRT-WG）が慶應義塾大学によって設立された

3.2.2.4 米国 NIST

David Temoshok（Senior Policy Advisor, Applied Cybersecurity, Information Technology Laboratory National Institute of Standards and Technology, U.S. Department of Commerce）

[概要]

○ NIST は、米国だけではなく世界的に採用できる標準を通じて、サイバーセキュリティと情報プライバシーに取組んでいる。
○ NIST サイバーセキュリティフレームワークと FISMA 標準は、効果的なサイバーセキュリティと情報システムセキュリティに対処するためのフレームワークと要件を提供している。
○ サイバーセキュリティフレームワークは 3 つのコンポーネント（コア、層、プロフィール）から成っている。
○ NIST と日本の取組みの 1 つとして、Japanese Cross-Sector Industry Forum がある。

この Forumの利点として、フォーラムの会員会社は日本内外で活動し 2020 年の東京オリンピック／パラリンピックの後援を行っており、会員は政府や業界のグローバルサイバーセキュリティの専門家とグローバルに共有された言語で通信し、ドメイン全体でサイバーセキュリティを推進することができる。

3.2.2.5 英国 National Cyber Security Centre（NCSC）

Chris Hankin（Imperial College London (UK)）（個人の見解である旨アナウンスあり）

[概要]

○ NCSC は 2016 年に活動を開始し、2019 年 10 月 第 3 回年次報告書を発行した。最初の 2 年間は、政府＆重要インフラの企業のサイバーセキュリティ向上に貢献してきた。 2019 年は市民のサイバーセキュリティを向上する年にする。NCSC は、運用開始以降、約 1,800 件のインシデントを取扱ってきた。
○ 活動の成果

1 構造化および自動化されたエコシステムを作成

2 英国、パートナー、同盟国の防御を強化
3 脅威の認識を構築および強化することにより、検出と防御の強化
4 企業の被害者に対する悪意のある攻撃を迅速に警告

○　サイバーファースト（CyberFirst）
- 若い才能を見つけて育てることを目的とし、テクノロジーへの情熱を探求し、それを実践するために必要なスキルと知識を提供

○　Cyber Security Body of Knowledge[10]というサイト
- サイバーセキュリティの知識を体系化することを目的としている。
- サイバーセキュリティはチームスポーツ。産学官の協力で成り立っている。

3.2.2.6 イスラエル　ベン・グリオン大学

Yuval Elovici,（Director of the Telekom Innovation Laboratories, Ben-Gurion University of the Negev (BGU)）
[概要]

○　ビジネスの触媒としての政府
軍、企業、アカデミー、起業家の間で触媒となって効果を促進する。

○　サイバー都市　Beer-Sheva

○　手術支援ロボットであるダヴィンチでは、誰が手術しているかを認証する。

○　マルウェアにとるサイバー攻撃により CT スキャン画像を改変し、誤診を誘導することが可能。

○　AI とサイバーセキュリティ
AI を使用した防御、AI を使用した攻撃、敵対的 AI による攻撃。

3.2.2.7 ETSI TC

Riccardo Genghini（ETSI TC ESI 会長）
TC ESI, ETSI (EU)
　法的、技術的及び相互運用性を確保する。

○　eIDAS:　信頼を高め、ビジネスをサポートする。

○　eIDAS 規則
- 2 章　デジタル ID　　各国の主権が優先
- 3 章　トラストサービス　ステークホルダーが標準化のプロセスを通じて決定

○　eIDAS トラストサービス
　原則を元にレゴブロックのような形になっている。

○　基本的課題
- 規制の比較可能性

[10] https://www.ncsc.gov.uk/section/education-skills/cybok

- 英 BSI　7799
- ヨーロッパの TSP　29 カ国　178QTSP　数十億の市場

○　eIDAS の review　2020 年 7 月
○　国際アウトリーチ　UNCITRAL
○　EU と日本　2 国間協力

3.2.2.8 オーストラリア

Adam Henry（Director Education, Fifth Domain (Australia)）

○　オーストラリアのサイバーセキュリティ産業はコラボレーションに注力している。
政府、軍、学会及び Technical And further Education（TAFE s ）によるプロジェクト。
○　公的機関と民間のコラボレーションが真の結果をもたらすということが重要である。

3.2.2.9 全体パネル　＃1 日米 2 国間関係

モデレータ：Linton Wells（ジョージ・メイソン大学）
パネリスト：
Bud Roth (笹川平和財団米国)
東　秀敏（合同会社日本 PTB　日本代表）
大澤　淳（中曽根平和研究所）
Barbara Grewe (MITRE)
[概要]
○　サイバーセキュリティに関して
①　日本の国防
- サイバーディフェンスについて話が進んできた。日本で大きなサイバーインシデントが起こったときに日米安保条約の対象となるという話がでた。日本の憲法の下で、防衛と攻撃の態勢をどうするか。

・　サイバー演習を日本と協力することが大切である。
・　日本が攻撃されたとき、それが海外で行われた時、それを追跡してもいいか。
・　この意味でも演習して政策を練習しておかないと。

②　警察部門
- 海外の司法機関、ハーグ条約の下で捜査を行う。その結果を共有する。この際、他国の情報もないと捜査をしても解決できない。

③　個人情報保護
- より強力な法がないと、プライバシーの問題があるため、警察が必要とするときに、データの提出に躊躇するのではないか？インターネットにおける捜査をするためには、きちんと法的に規定されていることが必要。

○　民間の３つの問題はアメリカの問題でもある。

①　日本にはアメリカの基地がある。これは日本のキャリアによって支えられている。日本は脆弱性が高い。重要インフラに対しロシアが攻撃しようとしている。日米軍のサイバーセキュリティを強化していかないといけない。

②　日本の情報セキュリティは政治的問題

・　法律は前進しているが不十分。
・　政府に一元化された機関がない。
・　NISC は設置法がない。
・　不十分なリソース(人、資金)

○　日米の情報セキュリティの共同フレームワーク

③　政府の基盤が不十分なので：

・　ターゲットになりうる。　ロシア、中国がサイバー攻撃に出ている。
・　民間レベルも軍と同じレベルに上げないといけない。
・　サイバーセキュリティは防御からレジリアンスへ移行。
・　攻撃されても生き残る。
・　セキュリティ in トラスト（軍レベルのセキュリティ）をすべての民間レベルで考えるべき。

サイバーセキュリティのアーキテクチャを作るべき政府／民間。

○　どの種のサイバー攻撃にフォーカスすべきか（Must）

・　国としての対応は受け身だった。Passive Defence では不十分
・　State-Sponsored Cyber Attack　(国家によるサイバー攻撃)が起こっている。

ロシア－攻撃
中国　－知財の窃取が脅威

・　国益を狙ってくる攻撃に対しての対応

1 防止
2 抑止

・　攻撃者に対して継続的なモニタが必要

ビッグデータを使って 2 国間協力を提案

①　IP をネットから収集を止める
②　サイバー脅威　検知―警告　共有
③　自動サイバーインディケータ

○　日米 2 国間で共通の目的とゴールを持つ必要がある。

・　サイバー対話を通じて理解
・　2+2=5 になるという共通認識がある。
・　対話の結果を実行に結び付けるには互いに信頼できる状況にならないといけない。
・　行動のほうが言葉より重要。

- “Referred Trust”が情報交換では重要。

○　オリンピックの話

- 各々の国の Operation center が互いに協力して成功させたい。
- リアルタイムで数百万の人がそれを見れる。サイバー攻撃は 2020 年にも起こるだろう。すべての攻撃に対して対応はできない。
- アセスメントプロセス
- 残存リスクはあるのでレジリアンスが必要。IOC が各ベンダーとサービスレベルアプリケーションを交わしている。

○　2016 年の大統領選にロシアが介入したと言われている。日本で大きなサイバーインシデントが発生したとき、誰がやっているのかを分析するため、アトリビューションメカニズムが必要である。

- 日本にも CIA のような情報機関が必要
- その前に NISC の empower が必要
- 官民の協力

○　日本はアトリビューションの能力が必要。誰が攻撃の裏側にいるかを見極める必要

重要な情報を共有するには誰がメンバーなのかを知る必要がある。

3.2.2.10　　全体パネル　＃2 Cybersecurity’s Silent Spring

モデレータ：David Farber（慶應義塾大学サイバー文明研究センター教授）

パネリスト：

Eric Burger（ジョージタウン大学）

竹内　芳明（総務省サイバーセキュリティ統括官）

Gregory Rattray（コロンビア大学）

村井　純（慶應義塾大学環境情報学部教授）

[概要]

サイバー空間の持続的な発展に向けて―サイバーセキュリティの沈黙の春--

○　1990 年代破壊的イノベーション　インターネット→設計は性善説を前提としていた

○　インターネットのコンセプト

○　マルチステークホルダーアプローチによる自主的、分散、協力

[イノベーションのエコシステム]

↓

インターネットのサイバー衛生（cyber hygiene）

又は

新しいコンセプトのネットワークの紹介　[clean slate]

- 最近の動き

①　データフリーフロー　v.s. データローカライゼーション

② Society5.0 & 第四次産業革命
③ IoT/5G の急激な広がり　→　遡及的対策及び事前対策

○ 遡及的 IoT セキュリティ対策
・ 背景：IoT 機器は広く使用されている。しかし、大部分の使用ではそれらの ID/パスワード設定を配慮していない。
・ 対策：デフォルトの ID /パスワード設定で脆弱な IoT 機器を特定し、これらの機器のユーザに設定を変更するよう警告する。
  ➢ 問題：ユーザの許可なしにインターネット上の IoT 機器にアクセスすることは禁止されている。

↓

  ➢ 政府のアクション：上記の措置を合法的に実施するために 2018 年 5 月に法律を改正し、2019 年 2 月に「NOTICE」プロジェクトを開始した。

○ 政府による IoT セキュリティ事前対策
・ 改正された技術条件：　IoT 機器は、以下が必要
  ① リモートコントロール機能によるアクセス制御
  ② ユーザにデフォルトの ID /パスワードの変更を促す機能
  ③ セキュリティ修正のためのファームウェアアップデート機能
・ スケジュール：2020 年 4 月 1 日より発効。これ以降は、技術条件に適合する端末機器にのみ承認が与えられる。
○ IoT 機器の任意の認証プログラム
○ CSIRT 機能要件　　共有の迅速化
○ 国際協調
・ ボットネットは世界的に形成され、サイバー攻撃は国境を越えて行われる。
→ セキュリティ対策はすべての国々で必要である。
・ 安全でセキュアなサイバー空間を実現するために、各国は互いにベストプラクティスを共有し、IoT セキュリティ対策を実装する。
・ トラストサービスフレームワークの相互運用性と ISAC 協力が重要である。
○ Silent Spring 問題への対応
○ デジタル水平線の最初の亀裂
・ サイバーエスカレーションの新たなパターン
・ エスカレートのパターン 1 ：デジタルドメイン　－　データの変更または破壊
・ エスカレートのパターン 2 ：物理ドメイン－　サイバー手段を使用して物理的損傷を引き起こす

Day 2

3.2.2.11　　パラレルセッション

3.2.2.11.1 D2-T3-S1　信頼できるクラウドへのアプローチ

モデレータ：永宮　直史（特定非営利活動法人日本セキュリティ監査協会エグゼクティブフェロー）
パネリスト：渥美　俊英（一般社団法人　日本クラウドセキュリティアライアンス（CSAJ）副会長／JASA-クラウドセキュリティ推進協議会（JCISPA）アドバイザ）
小町　紘之（日本マイクロソフト株式会社　クラウド＆ソリューション事業本部　モダンワークプレイス統括本部　第 2 技術営業本部　セキュリティソリューション　プロフェッショナル）
堺　由美子（富士通株式会社　データセンターサービス事業本部　マネージャ）

○　JASA 監査 WG
- クラウドをどうやって監査するか
- クラウド上の環境をどうやって監査するか

◎プレゼンテーション「クラウドコンプライアンスの現在」
松本　照吾（アマゾンウェブサービスジャパン株式会社セキュリティアシュランス本部　本部長）
[概要]
○　クラウドファーストやクラウドネイティブの流れへ
- Government-published cloud policy も増えて来ている。
- 日本もクラウド業者を 2020 年から登録し、政府で利用していく。
- ニュージーランド

オーストラリア　DTA[11]
日本政府
→「クラウドを使ってより良いセキュリティを実現していこう」
○　セキュリティサービスの進化・民主化
セキュリティサービスは、ログの

PC flow logs	Guard duty	Building block
集約 ・ログモニタリング	分析 15 年前 ・ログ分析のための機材準備を踏まえた脅威検知	対応 ・セキュリティ自動化の実装 Lambda[12]によるイベント駆動型のリスク低減アクションの組み込み

○　分析された結果を見て対応を行えるようになった。必要に応じて多くのサービスがすでに提供

[11] DTA(Digital Transformation Agency):オーストラリアのデジタルガバメント推進組織

[12] Amazonが提供するサーバーをプロビジョニングしたり管理する必要なくコードを実行できるコンピューティングサービス。

されている。

○　変化に適合するものが生き残る

従来は設計したら使い続ける　→　今は、update によって機能が更新・強化されていく

○　CIA はクラウドを国としての意思決定のために利用している。

○　日本のクラウドは、10 年議論されてきて、普及面では初期段階。

多くのユーザが、クラウド Iaas の評価や試験運用の初期段階。従来のアウトソーシングと混同している。

ウサギは休まない。カメ（日本）はどーすべきか？！

○　課題

セキュリティ担当者、監査はクラウドにどう取り組むべきか？

どうやって育成するか？

◎クラウドとは仮想サーバサービス？

○　オンプレの代替インフラ　安い／早い／便利

○　クラウドのすべてのサービスはコンソールから、165 以上のクラウドサービスメニュー（AWS）

○　クラウドサービスの大半　≠　Iaas

最新のクラウドは　≠　Iaas

Paas + Saas +　マネージドサービス

○　銀行　クラウド利用が進んでいる

○　安全対策基準の改定（8 版から 9 版へ）

金融情報システムセンター（FISC）から「金融機関等コンピュータシステムの安全対策基準・解説書」が改定—30 年ぶりの大改訂

○　SOC[13]2　セキュリティのホワイトペーパー

◎信頼できるクラウドへのアプローチ

○　Shared responsibility model

クラウドのセキュリティとオンプレミスのそれはそれ程違わない。しかし、クラウドの特性を考えないといけない。「特性を理解して活用」

Saas　Paas　Iaas　オンプレ

○　クラウドサービスは責任分担が違う、オンプレミスは、自由度は高いが対応しきれない。例えば、ログ。クラウドではシンプルに簡単にできる。

◎SOC2

○　SOC2 レポートとは、サービスのセキュリティや可用性の対策についてプロバイダが監査法人に監査してもらってユーザに提供するレポート。「認定」「合格」ではない。要求事項を満足し

[13] SOC: Service Organization Controls

ているかが具体的に記述されている。
○　「確かめたい」に「応える手段」が SOC2 レポート
これをコミュニケーションツールに。
○　クラウドはわからない　→　わからないものは使わない
というのはダメではないか。

○　SOC2 レポートの使い方
・　対象サービスやその提供体制・組織について、その全体像を含めて体系的かつ詳細に把握できる。→　立入検査の代わりになる
・　（立入検査を行う場合も「現地でしか確認できないこと」にフォーカスできる）
・　セキュリティや安全性の観点から立入検査不可とされる箇所についても SOC2 監査法人による監査手続きと評価結果がわかる。
・　なぜ立入検査の代わりに使用できるのか？
「SOC2 は、監査法人が外部委任業務のセキュリティ面の内部統制を対象に保証業務を行う組織の基準として米国公認会計士協会が定めたもの。」であるから。
・　SOC2 セキュリティのホワイトペーパーを読みこなせる人材が必要

○　安全対策基準　第 9 版
【続 24】クラウド固有のリスク管理策
・　クラウド拠点（DC 自体ではない）の把握　国、州など
・　監査権などの契約への明記
・　監査の実施は技術の先進性を考慮して

3.2.2.11.2 D2-T2-S2　駐日英国大使館
モデレータ：クリス・ハンキン（インペリアル・カレッジ・ロンドン）
パネリスト：ダニエル・スガンジューラ（ロイヤル・ハロウェイ）
Glenn Lambert, BT Japan
［概要］
○　セキュリティの脅威が高まっており、セキュリティ側のスキル及びパワーが不足している現状で、正しいスキルにチャレンジしている。
○　BT（British Telecom）は、障壁を破るためのトレーニングやスキルを提供する。
○　若い人に知識を持ってもらうために、国のサイバーセキュリティプログラムを用意している。11 歳の子供にコンピュータの仕事をするためのプログラムを受けてもらう。
○　人材は重要であり、カギは、大学の支援。まずはトレーナーを支援することも必要。ディスカッションなど、楽しみながら力をつけてもらう。
○　女子生徒も半分くらいいるが、男子と比べると興味を持ってない傾向あり。大学としても、ジェンダーや多様性は課題である。

○　優れた学生は、企業に行ってしまいアカデミーに残ってくれない。アカデミーに魅力を感じてもらう努力も必要である。

3.2.2.11.3 D2-T3-S2　トラストサービス検討 WG での議論と今後

モデレータ：柴田　孝一（トラストサービス推進フォーラム（TSF）企画運営部会長）
パネリスト：
宮崎　一哉（トラストサービス推進フォーラム（TSF）副会長）
西山　晃（セコムトラストシステムズ株式会社　プロフェッショナルサポート 1 部　担当部長／トラストサービス推進フォーラム（TSF）幹事）
小川　博久（NPO 日本ネットワークセキュリティ協会（JNSA）電子署名 WG サブリーダ／日本トラストテクノロジー協議会（JTSA）運営委員長）
新井　聡（株式会社エヌ・ティ・ティネオメイト IT ビジネス本部主査）
[概要]
2019 年 1 月 31 日から 11 月 28 日まで、WG を 15 回開催した。経団連のアンケートも行った。最終報告案として、近々パブコメを行う。
○　Society5.0 の実現に向けて
デジタルの陥穽－デジタルは改ざん、捏造が容易であり、事後否認の可能性がある。この状態のもと、そうされないような取り組みが必要である。
電子署名は、署名法もある。一方、タイムスタンプは、指針はあるが効力の規定がない。きちんとしたトラストサービスを作る必要がある。
○　トラストサービスとは　　Society5.0 を目指す社会
トラストサービスは、誰もが信頼できる基準を満足しているサービス
・　TSP[14]が信頼できるか（技術的必然性、契約、法令、評価・監査）
・　ユーザは TSP が発行するトークンを検証するのみ
トラストサービスの信頼性を保証するフレームワークが必要
○　在り方を検討する上での 4 つの柱
①　第三者による評価：
②　評価の主体：　公平、専門性、基準
③　評価の基準：
→ 共通的な評価手順
→ 個別的な技術・運用基準
④　利用者への公開：　　自動的ではない
○　上記の仕組みを規定する公的な枠組みの整備が必要
公的枠組み：制度の枠組み
・　TSP に対する評価・検証体制の確保

[14] TSP:トラストサービスプロバイダ

・　技術的な基準とその評価体制の整備
・　トラストアンカーの開示
・　公的な枠組みの整備
○　リモート署名
　・　JT2A「リモート署名ガイドライン」策定中。
　・　リモート署名には、適合性を評価する仕組み（評価機関）がない。
○　e-seal
　・　法人証明書と紐づくデジタルシグネチャ
　・　社印、角印に相当する。日本にはない。
　・　法的根拠がないので、制度が必要。
○　海外動向
・　eIDAS 規則がスタートして、今は発展段階にあり、TSP の数も 180 に増加
・　UNCITRAL（国際連合国際商取引法委員会）にて Identity Management Trust Services を検討
○　まとめ
トラストサービスの課題
・　デジタルは改ざんが容易
・　相手否認
・　正確な情報入手
○　解決策
・　正確な相手認証
・　誰もが納得する情報の完全性

3.2.2.11.4 D2-T3-S3　経営層から見えるサイバーセキュリティ

モデレータ：梶浦　敏範（経団連　サイバーセキュリティ強化 WG　主査）
パネリスト：
宮下　清（一般社団法人　日本情報システム・ユーザー協会　参与）
持田　啓司（情報セキュリティ教育事業者連絡会　代表）
[概要]
○　サイバーセキュリティは、IT 部門や技術者の責任と思われている。しかし、企業の存続に関わる大問題である。
○　Society5.0 時代のサイバーセキュリティ
○　あらゆるものがかってなかった価値が生まれる。この一方でサイバー攻撃の対象が増加し、リスクも高まる。
○　どう対処するか？　次の 2 つの視点で。
　・　価値の創造－サイバーセキュリティ空間で価値を創出する。
→サイバーセキュリティが競争力になる
→グローバル市場でのビジネス環境確保

・　危機管理－サイバー攻撃対策を怠れば、事業継続が困難となり、関係者・市民に大きな影響を与える可能性がある。

→避けられないものとして認識

→事業継続の観点が重要

○　サイバーセキュリティ対策の全体像

・　意識改革とリソースの確保－一番大きいのは経営者の意識改革

・　意識改革＋人材育成・情報共有・投資促進・技術対策

○　経団連サイバーセキュリティ宣言

・　東京オリンピックまでを重点取組み期間とし、サイバーセキュリティ経営を宣言。

・　経済界が一丸となって全員参加で対策を推進することを明記。

・　「Society5.0」での価値創造に向けた前向きな投資としてサイバーセキュリティ対策に取り組む重要性を指摘。

・　サプライチェーンの対策や積極的な情報共有、国際連携などを通じて、社会全体のサイバーセキュリティ強化に貢献する点を強調。

○　サイバーセキュリティ成熟度の可視化

○　人材の可視化

セキュリティ人材の不足

↓

人材定義を使用したサイバーセキュリティ人材の可視化

CRIC-CSF　「IT 人材/OT 人材の定義」、ISEPA「JTAG」等

↓

企業は適材適所へ人材配置・採用が可能になる。

個人はキャリアパス開発に利用できる。

人材の質×量から企業のセキュリティ体力を推量することができるようになる。

○　セキュリティ成熟度の評価方法

サイバーセキュリティ経営ガイドライン V2.0 の指示 10 項目に対する達成度で評価する。

・　サイバーセキュリティ経営ガイドラインの達成状況　40～60%

「金融」「建築・土木」「社会インフラ」は成熟度が高い傾向がある。一方、

「素材製造」「機械器具製造」「商社・流通」は成熟度中～低の傾向である。

3.2.2.11.5 D2-T4-S3　トラストサービスの創るデジタルトランスフォーメンション

モデレータ：津田　宏（株式会社富士通研究所　セキュリティ研究所長）

パネリスト：

満塩　尚史（経済産業省　CIO 補佐官）

畠山　暖央（農林水産省　大臣官房　政策課　デジタル政策推進チーム）

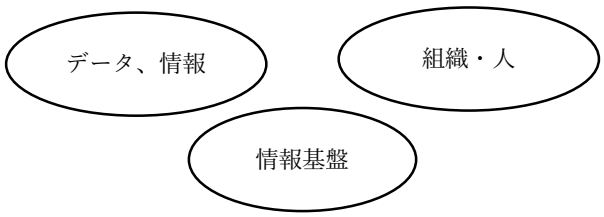
久野　保之（株式会社エヴァアビエーション）

［概要］
○セッションのねらい
・デジタルトランスフォーメーション（DX）・・・IDC Japan、METI 報告書
・トラストサービス・・・総務省トラストサービス検証 WG
○富士通の考えるトラスト
・　トラスト 1.0：人と人の間のローカルな信頼
・　トラスト 2.0：国や組織、制度などが保証する信頼
・　トラスト 3.0：テクノロジーがつくる信頼
○信頼できる企業にはデータを提供したい
○トラストを実現する仕組みの変遷
　SB327 信頼のデジタライゼーション　→　ブロックチェーン
［満塩 氏］
○METI DX、gBizID（法人共通認証基盤）
○METI DX・・・行政サービスと民間サービスの圧倒的な質の差が見過ごせないレベルに
○DX で行うこと
国民、事業者にとって便利な行政サービス提供
職員の効率的、効果的なツール
○より簡単に、より早く、面倒な手続きから解放
ワンスオンリー
民間とも共有
○情報をデジタル化し、効率的なマーケティングを実現
手の届く世界の現場主義　　データを活用した現場主義
○組織の変革に向けた取り組みを実施
官民交流の専門家集団
○法人デジタルプラットフォーム
gBizID 整備　ログインシステム
○gBizID・・・METI　→　政府全体へ
○保証レベル・・・SP800-63-3 ？
○本人確認ガイドラインと gBizID との対応・・・gBizID はガイドと整合を取りつつ整理
○gBizID の機能概要
ユーザ発行・管理
認証
通知
○所有物認証について・・・スマホアプリ認証、ワンタイムパスワード認証
○想定スケジュール・・・2021 年より本格版構築
［畠山 氏］

○農業の DX について
○我が国の DX： 産業のあり方の変革や、社会課題の解決を目指す
○世界の DX の動き： 主要国は、IoT やビッグデータ、ＡＩといったデジタル技術の社会実装を国家レベルの戦略として推進
○現行の食料・農業・農村基本計画策定時からの情勢変化：
デジタル技術の積極的な活用を前提とした施策の方向性を示す必要。
○農業の DX の必要性： 農業従事者の高齢化や労働力不足等の課題に対応しながら、農業の成長／産業化を進める・・・新たな農業への変革（DX）
○農業現場と農業政策の DX に向けた取り組み：
農林水産省として、デジタルトランスフォーメーションに向けた取組を統一的かつ強力に推進するため、省内外から広く人材を集め、新たな体制を構築
○プロジェクト①「農業新技術の現場実装推進プログラム」に盛り込まれた施策の確実な実施
○プロジェクト②農林水産省共通申請サービス
○プロジェクト③「デジタル地図」を活用した農地情報の管理に関する検討会
［久野 氏］
○エヴァアビエーションの紹介
　NIST SP800 – 171 対応
○Aero Space & Defense Industry
○民間機製造のグローバル化・・・B787
○国際共同開発の軍用機・・・F35
○サプライチェーンでの要件順守
○航空機産業の構造

エンジン	完成機
メーカー	メーカー
ロールスロイス	ボーイング、エアバス

○Exostar 社による A & D 業界のセキュアハブ
Exostar Identity Hub
○トラスト基盤の要素



○Exostar 社設立の経緯
大手防衛 5 社による設立
○組織・人・・・Hub による Identity 連携

○保護の対象となる情報・・・CUI（Controlled Unclassified Information）
○規制： 米政府の要求　国防装備（DoD）
調達特約条項 DFARS（252.204-7012）
○富士通プレスリリース 2019/9/26
NIST SP800-171（重要情報保護）基準に対応した Exostar 社クラウドサービスの利用をトータルにサポートする「Fort# Forum」を提供開始
○参）今後の A & D 日米トラストイメージ
○セキュア情報コミュニティイメージ

3.2.2.11.6 D2-T1-S1　3 極委員会：IoT と 5G

モデレータ：津田　宏（株式会社富士通研究所　セキュリティ研究所長）
パネリスト：
Dennis Blair（米国笹川平和財団）
Michael Chertoff（チャートフグループ）
伊東　寛（工学博士　最高技術責任者　ファイア・アイ株式会社）

National Security strategy for 5G
Findings & Recommendations on meeting the 5G challenge Trilateral Cyber Security Commission
[概要]
○　5G は協力が必要な分野。大きな市場になっていく。
○　Huawei の 2 つの脅威
・　脅威＃ 1　脆弱な装置の調達によって、デジタルの重要なインフラストラクチャが危険にさらされるリスクが高くなる。
・　脅威＃ 2　中国が主要な市場部門の「国家的チャンピオン」の市場努力を支援するた めに、経済スパイを含む国家資源を使用しているという証拠がある。
[推奨事項]
○　米国、日本、および同盟国の政府は、機器が次のことを確実にするために 5G 機器のレビューを必要としている。
・　セキュリティで保護されており、既知の脆弱性や週ごとのパスワードなどのずさんなセキュリティ機能が含まれていない。
・　機器が設置されている国に有害である敵対的な国家に代わって行動を起こした実績を持つ会社によって販売されていない。
○　「高脅威」企業を国家安全保障の脅威として指定し、これを反映するために個人の原告の裁定メカニズムを適合させるためのメカニズムを作成する。
○　強い国内 5G 産業の開発をサポート
○　このレポートで作成された推奨事項を調整するために、民間部門からの情報を提供して政府間国際グループを形成する。

米中対立・ファーウェイ・5G　～サイバーセキュリティの視点から～

○　5G によって、以下が実現可能になる

・　データをクラウドに瞬時に送り、複雑なタスクを処理した結果を遅延なく受信することができる。

・　端末側の負担が減り、デバイスはますますシンプルな構造になっていくし、おそらく省電力化も進むのではないか。

・　ウェアラブル端末が一般的になる

➢　例えば、今よりさらに高機能な翻訳デバイスなど

・　誰もスマホを持たなくて良い社会になるかもしれない。至る所に 5G 端末があるなら、そもそも自分で何かを持たなくても良い。

・　5G は製造業にも影響を与える　リアルタイムに操作　　スマートファクトリー

○　世界各国の動向

・　デロイトの調査によると、既に世界各国で 72 の通信事業者が 5G サービス実現に向けた評価を開始しており、そのうち 25 事業者が 2019 年内に 5G サービスをリリースすると言われています。2020 年までにはその数は倍になるとも書かれている。

・　中国の雄安新区、今年にも 5G を先行展開開始した。

・　3 大キャリアが北京に 5G 基地局を開設した。

○　日本では 5G の展開が遅いように見える。　理由は市場原理だろうか？

・　5G になると通信料金と端末価格が現在の 2～3 倍になると言われている。

・　例えば、韓国サムソンが先日リリースした折り畳み液晶画面の 5G 対応スマホは値段が 30 万円程度になる。4G のままでも一般の人々の暮らしには十分かもしれない。

○　5G の課題－コストダウンのため、汎用的な機材を利用しソフトウェアで機能を実現するようになる。ソフトの利用率が増えるが、それに伴って、

・　巨大化したソフトの検証は困難になる。

・　機材自体の数が増えることと相まって、アップデートやパッチあても難しくなる。

・　膨大な数の機材に関するサプライチェーンリスク問題も深刻化するだろう。

・　サイバーセキュリティ上の問題は増加する。

○　5G 関連特許

・　中国が 1/3、韓国が 1/4、米国 14%、日本 4%

・　米国は中国の特許技術を使うことを良しとしない。

・　中国が米国技術の利用に同意するはずもない。

・　5G の技術標準化は遅れるだろう―米国の反対で(2019 年中に確定する予定ではある)。

特許があっても、それが標準化されており、利用されなければ無意味である。

○　技術標準

中国工業・情報化部が 14 日に明らかにしたところによると、中国は国際電気通信連合（ITU）の 49

件の標準を主導し完成させ、新たに 73 件を立ち上げ、中国の標準が国際標準になるよう力強く推進している。

○　5G 問題(米国は何を恐れているか？)

・　5G 関連のネットワーク機器・端末等に色々な機能を（あらかじめ）付け加えることができる.。

-　これらの機材はユーザ側の情報をアップできる。

プライバシー、セキュリティ、インテリジェンスの問題

-　コントロールすることも可能。

サイバー攻撃に利用可能。

・　中国は、安売りにより彼らの機材のデファクトスタンダード化を狙っているだろう。

・　インターネットの支配を米国から奪うことが隠された目的かもしれない。

○　米中対立

・　ファーウェイ叩き(サイバーセキュリティ)

・　知的財産の保護

・　技術上の主導権争い

・　貿易摩擦

・　安全保障上の問題

・　米中覇権争い

対立の本質は、サイバーセキュリティではなく米国へのアイデンティティへの挑戦かもしれない。

○　日本はどうする。

避けるべき危険な状況

技術標準に関し、同盟国である米国寄りの立場を取るとして、気が付いたら

・　世界が「高くて性能が低く使用者の少ない日米技術連合」対「安くて性能が高い多数の中国技術利用国家群」になっていること。

・　さらに、そこに日本の優位な技術が全くなければ悪夢である。

○　インフラ整備の時間内に起死回生の手段を考える？

-　既存技術を利用

-　6G をやる

→　日本は非常につらい立場

○　Global の視点から

・　複数国でのアプローチが必要

・　5G はグローバルなインフラ

・　違った国は違った考えを持つ。

・　考え方を同じくする国々（日米欧、オーストラリアなど）で対応していく。

・　相互運用性

・　規模の拡大　多国間で投資

・　日米同盟　日米は理解しあうことが必要　共同開発

3.2.2.11.7 D2-T3-S4　企業セキュリティの情報公開の指針を

モデレータ：上杉　謙二（日本サイバーセキュリティ・イノベーション委員会主任研究員）
パネリスト：
相川　航（総務省　サイバーセキュリティ統括官室参事官補佐）
澤田　雅広（日本ユニシス株式会社　業務部リスク・セキュリティ管理室長）
白須賀　啓介（三菱 UFJ 国際投信株式会社　ESG 統括グループ　グループマネジャー）
花村　実（マイクロソフトコーポレイション　Chief Security Advisor）
[概要]
○　企業セキュリティの情報公開に関する課題
・　書き方がばらついている(客観性がない)
・　各々ビジネス戦略が異なる－セキュリティの厳しさの開示競争になってはいけない。
・　セキュリティとビジネスの連動性がみえないとコストと捉えられる。
上記が解決されないと、企業の DX 化が鈍化し成長戦略の障壁となる恐れがある。
○　平時のサイバーセキュリティ
・　「サイバーセキュリティ対策情報開示の手引き」
・　組織面、ルール面、及び技術面の 3 つの点から
・　PDCA に則して持続的なセキュリティレベル向上への取り組み
・　オムニチャネル戦略を書いてあり、その中で認証、CSIRT について具体的に
○　有事のサイバーセキュリティ
　・　インシデント発生時の情報公開
　・　平時の対策が優れていても被害を受けるとメディアは記事にする。
　・　メディアの記者が頼りにする専門家まで取り込めれば、炎上を抑えられる。

3.2.2.11.8 D2-T4-S4　サイバーセキュリティ人材育成エコシステムは実現可能か

衛藤 将史（国立研究開発法人情報通信研究機構 ナショナルサイバートレーニングセンター サイバートレーニング研究室 室長）
小早川 倫広（首都大学東京 東京都立産業技術高等専門学校 教授）
小野寺 好広（シスコシステムズ合同会社 シニア ソリューション アーキテクト）
［概要］
○人材育成の現状
2019 年で 19 万人の人材不足
○NICT の取り組み
サイバートレーニングセンターで、オペレータ、イノベーターの育成
○文科省、高専の取り組み
企業からの人材要求は、”倫理観”が必須

○Cisco Network Academy
排出人材は、経営層、ジェネラリスト、スペシャリスト

3.2.2.11.9 D2-T3-S5　サプライチェーン・サイバーセキュリティの社会実装に向けた課題-官民の施策・課題-

モデレータ：石原　修（株式会社日立製作所　セキュリティ事業統括本部　セキュリティインキュベーション推進本部　本部長）
パネリスト：
尾崎　洸（経済産業省商務情報政策局サイバーセキュリティ課　課長補佐）
斯波　万恵（株式会社東芝　技術企画部　サイバーセキュリティセンター参事）
渥美　俊之（株式会社日立製作所　セキュリティ事業統括本部　セキュリティインキュベーション推進本部　セキュリティインキュベーション推進部　担当部長）
[概要]
セッションの目的：Society5.0 実現におけるサプライチェーンのサイバーセキュリティ対策の課題について議論する
○　国の動き
「産業分野におけるサイバーセキュリティ対策」
情報セキュリティ 10 大脅威 2019（IPA）にもサプライチェーンが 4 位に登場
サイバー攻撃によるダメージが広がっている。
平成 29 年 5 月 wannacry
サイバー攻撃レベルの増大　　ウクライナの停電、ノルウェーでも。
○　サイバーフィジカルセキュリティ対策フレームワークの策定
Society5.0 の実現には新しいリスクへの対応が必要。どうやってサプライチェーンを守るか。
○　サイバーとフィジカル一体型社会のセキュリティ
CPSF　三層構造と 6 つの構成要素を持つ
第 3 層　サイバー空間における繋がり
第 2 層　フィジカル空間とサイバー空間の繋がり
第 1 層　企業間の繋がり
構成要素：　組織、人、モノ、データ、プロシージャ、システム
CPSF を具体化　実装推進　業界ごとに WG を作り対応する。
○　経営層向け
サイバーセキュリティ経営ガイドライン
中小企業の情報セキュリティ対策ガイドライン
○　サプライチェーンを守るためには中小企業も対策が必要
経産省は、中小企業向けのセキュリティにも注力している。
○　社会実装について

業種が違えばレベルが異なる。何でもかんでもガチガチにやるのは違う。命にかかわるのは厳しくとか・・・必要性に応じて対応すべきである。
○　ビル SWG　CPSF 実装ガイドラインを出した。ステークホルダー全体でセキュリティを守る。
　　他の業界でも。
○　企業間取引をする前に、新しい要件
GDPR、スマートコントラクト(ドイツ)など
○　SIP は整合性をどう確保するか。
サプライチェーン全体で要件を満たさなければいけない。となったとき中小企業は対応できるのか？　又、どうやったら普及するのか？
　① 運用
　② システムが出来たとして、広めていくときに一斉にやらないと効果がない。
考えを一にする仲間の音頭を取ってほしい　→　経産省
いままで Criteria（要件）が多すぎる。海外もチェーンの 1 つである

3.2.2.11.10　D2-T2-S5　Cyber Warfare and Critical Infrastructure Defense

Hidetoshi Azuma, President & CEO, Resilience Japan
Joe McReynolds, Fellow, Jamestown Foundation
［概要］
○Chinese Network Warfare
Network Warfare
Electromagnetic Warfare
Psychological Warfare
Information Warfare
Intelligence Warfare
○　以下、プーチンの戦略、米、英、独の動向など
　　↓
アメリカの良心（国民の選択)、レジリエンス
世界の再構築が必要
　↓
日本の力を西側世界のために！

3.2.2.11.11　D2-T3-S6　Society5.0 時代を見据えたデータ活用の現在

モデレータ：竹島　昌弘（株式会社日立製作所　社会イノベーション事業推進部　部長）
パネリスト：
奥井　規晶（一般社団法人　官民データ活用共通プラットフォーム協議会　代表理事）
廉　宗淳（e-Corporation JP 代表取締役社長）
[概要]

2020/3/31

一般社団法人データ流通推進協議会

◎韓国スマートシティ政策推進状況

○　1960→1990→2010 へと、一部の都市に人口が集中してきている。韓国の人口の 2/3 が都市に集まってきている。

1960～70　　経済成長のための拠点、　1980～90　生活の質の向上

○　急激な都市化により、U-city ブランドローンチング。韓国全体がモデルハウス。

○　スマートシティ要素技術単体、及びスマートシティパッケージにして他国への販売

○　政府のスマートシティ推進　　モデル都市として推進中

- Sejong（世宗特別自治市）-- 政府省庁をソウルから移管し、スマートシティを推進
- Busan（**釜山**）-- 港湾のスマートシティ

韓国では、まず各々やってみて後からつなぐときに標準化する。　既存のものをつぶして作り直す。法制度を整備しスマートパッケージを売り込んでいる。　韓国ではゼロベースでできる。しかし、日本では、このやり方はできない。

◎DPC の紹介　（官民データ活用共通プラットフォーム協議会）

「データ」をめぐる国際競争が激化する中、DPC を立ち上げた。ヨーロッパ GAFA 対応で EU 政府 400 億 FIWARE を構築。NGSI を採用したオープンソースのプラットフォーム（FIWARE）を構築、日本も「官民データ活用」で追走中。

○　NGSI の接続テスト　国際標準 NGSI による 4 社接続実証に成功　2019 年 4 月 19 日

富士通株式会社・日本電気株式会社・日鉄ソリューションズ株式会社・TIS 株式会社の 4 社のプラットフォーム接続実証

○　スマートシティは今まで日本もやってきた。しかしバラバラだった。日本ではサービスの実装を先にやりたがる。しかしアーキテクチャから考えるべき。都市 OS の API により各都市間を相互接続する。

○　つなぐの課題　　まずアーキテクチャを考えるのが先。

・　個人情報を保護すると言っておいて HDD が流出している（建前　日本）

・　日本では各省間でつなげるなんてありえなかった（縦割り）。特に警察と防衛はつながらない。

以上