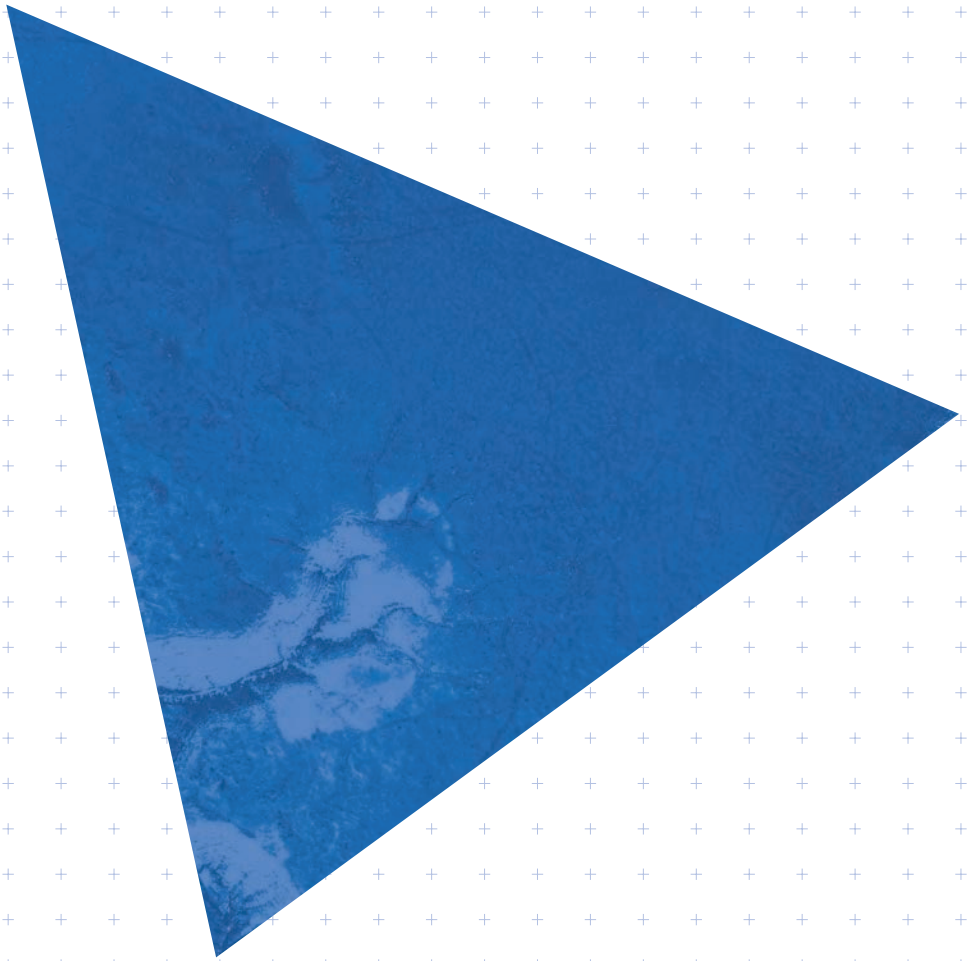
ワークショップ報告書
CRDS-FY2021-WR-02

俯瞰ワークショップ報告書

セキュリティー・トラスト分野の動向と今後の展望

2021年5月27日（木）開催



国立研究開発法人科学技術振興機構
研究開発戦略センター

エグゼクティブサマリー

本報告書は、国立研究開発法人科学技術振興機構（JST）研究開発戦略センター（CRDS）が、2021年5月27日に開催した俯瞰ワークショップ「セキュリティー・トラスト分野の動向と今後の展望」に関するものである。

「セキュリティー・トラスト」は、2021年3月、CRDSが発行した「研究開発の俯瞰報告書　システム・情報科学技術分野（2021年）」の中で動向を俯瞰する5区分のうちの1つである。図のように全体を俯瞰し、特に「IoT・制御システムセキュリティー」「サイバーセキュリティー」「データ・コンテンツのセキュリティー」「トラスト」という4つの研究開発領域に注目している。当該区分は、情報技術の潮流や社会・経済的な動きを背景に、今回の俯瞰報告書で新しく設立した区分であり、より深く分野の動向や問題意識を捉え、今後の俯瞰・提言活動へ活かすべく、今回のワークショップを実施した。

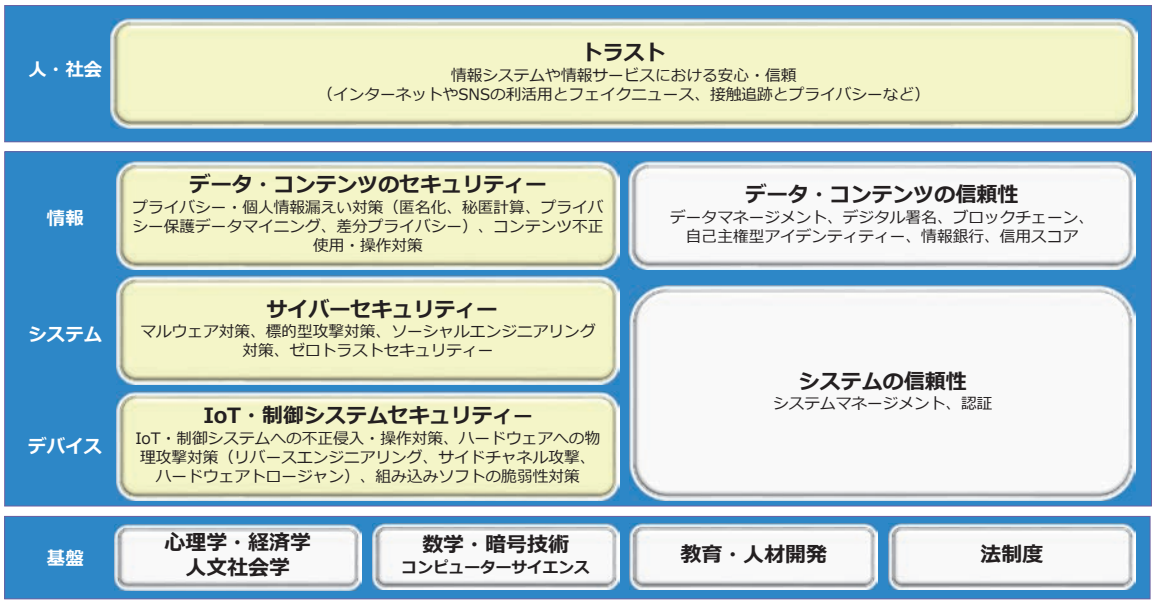


図　　セキュリティー・トラスト区分　俯瞰図

ワークショップには、当該俯瞰報告書の執筆協力者や、産学官の有識者、合計約40名が参加した。まず、当該区分にて取り上げた各研究開発領域の動向について、JSTより説明を行った。その上で、各有識者が抱いている問題意識や特に注目すべきトピック、俯瞰報告書のまとめ方などについて、参加者全員で議論を行った。

以下に、特に重要な示唆をまとめる。

①全体を通して

- セキュリティーを構成する要素からのボトムアップ的なまとめ方に加え、アプリケーション側から見たトップダウン的なまとめ方を検討することも有用である。
- セキュリティーが、社会に及ぼす影響や範囲が拡大している。人文社会科学系の研究者や行政を含む、幅広い層との連携が重要である。また、実データを持つ企業を巻き込んだ産学官共同研究の促進が望まれる。

②IoT・制御システムセキュリティー

・自律走行（オートビークル）など、具体的なアプリケーションについても触れられるとよい。
・特に注目すべきトピックとして、信頼の基点・ハードウェアセキュリティー、フォレンジック、強電磁界による意図的な電磁妨害攻撃への対策、長期に渡るIoTシステムの維持、スマートフォンのセキュリティーなどが挙げられる。

③サイバーセキュリティー

・サイバー攻撃の標的や目的が大きく変化してきている様子がより捉えられるとよい。
・特に注目すべきトピックとして、組織間の情報連携、ヒューマンファクター研究、連鎖するサイバー攻撃の観測に関する研究などが挙げられる。

④データ・コンテンツのセキュリティー

・特に注目すべきトピックとして、データの信頼の基点、セキュリティー・プライバシーを確保したデータの利活用などが挙げられる。

⑤トラスト

・今回は、社会的な受容性の観点でトラストをまとめている。他の観点として、あらゆるものに対するデジタル証明の付与や遠隔からの検証、デバイスに必要なRoot of Trustの確立、自律化・自動化に必要なFAccT（Fairness, Accountability and Transparency）などの要求やそのための検証などがある。
・特に注目すべきトピックとして、プラットフォーマーによるトラスト投資や、情報システム・サービス全体のトラストチェーンの構築などが挙げられる。

これらの議論を踏まえ、CRDSでは、更に当該区分の動向調査を充実させ、今後の研究開発の俯瞰報告書や、戦略プロポーザルなどの提言活動へ活かしていく予定である。

目次

1 ｜ 開催趣旨

JST研究開発戦略センター（CRDS）は、科学技術に求められる社会的・経済的なニーズを踏まえて、国として重点的に推進すべき研究開発領域や課題、その推進方策に関する提言を行っている。

この活動の一環として、2021年3月、CRDSシステム・情報科学技術ユニットは、「研究開発の俯瞰報告書　システム・情報科学技術分野（2021年）」を発行した。本俯瞰報告書では、Society 5.0の実現に向けてシステム・情報科学技術が目指すべきビジョンと、技術トレンドの両方の観点から、戦略的に重要度が高い研究開発領域を特定し、「人工知能・ビッグデータ」「ロボティクス」「社会システム科学」「セキュリティー・トラスト」「コンピューティングアーキテクチャー」という5つの区分に分けて、動向を俯瞰している。

本ワークショップにおいては、上記5区分のうち「セキュリティー・トラスト」区分に焦点を当て、同区分において取り上げた研究開発動向を共有する。また、各研究開発領域における問題意識や、今後特に取り組むべき課題などについて議論を行い、今後のCRDSにおける調査・提言活動へ活かすこととする（図1）。

研究開発の俯瞰報告書（2021年）
セキュリティー・トラスト区分

①俯瞰報告書で取り上げた研究開発動向等のご説明
②各研究開発領域の問題意識や、
今後特に取り組むべき課題等についての議論

ワークショップ報告書の発行

CRDSにおける調査・提言活動へ
（次期俯瞰報告書や、戦略プロポーザル等）

図1　　ワークショップ開催趣旨

2 ｜ 俯瞰報告書セキュリティー・トラスト分野

2.1 セキュリティー・トラスト総論

「研究開発の俯瞰報告書」は、国内外の社会や科学技術イノベーションの動向、および関連する政策動向を把握・俯瞰・分析し、今後のあるべき方向性を展望するものである。

図2-1-1に、情報科学技術の潮流と社会の要請・ビジョンを示す。情報科学技術のトレンドは、大きく3つに分けて捉えることができる。1つ目のトレンドは、「あらゆるもののデジタル化・コネクティッド化」である。これによって、サイバー世界とフィジカル世界の高度な融合が進んだ。その上で、2つ目のトレンドとして「あらゆるもののスマート化・自律化」が加わったことで、データ駆動型/知識集約型の価値創造へと発展してきている。近年特に注目されるのは、3つ目のトレンドである「社会的要請との整合、人間の主体性確保」である。社会課題解決と人間中心社会の実現というビジョンを目指して、この動きが活発化してきている。

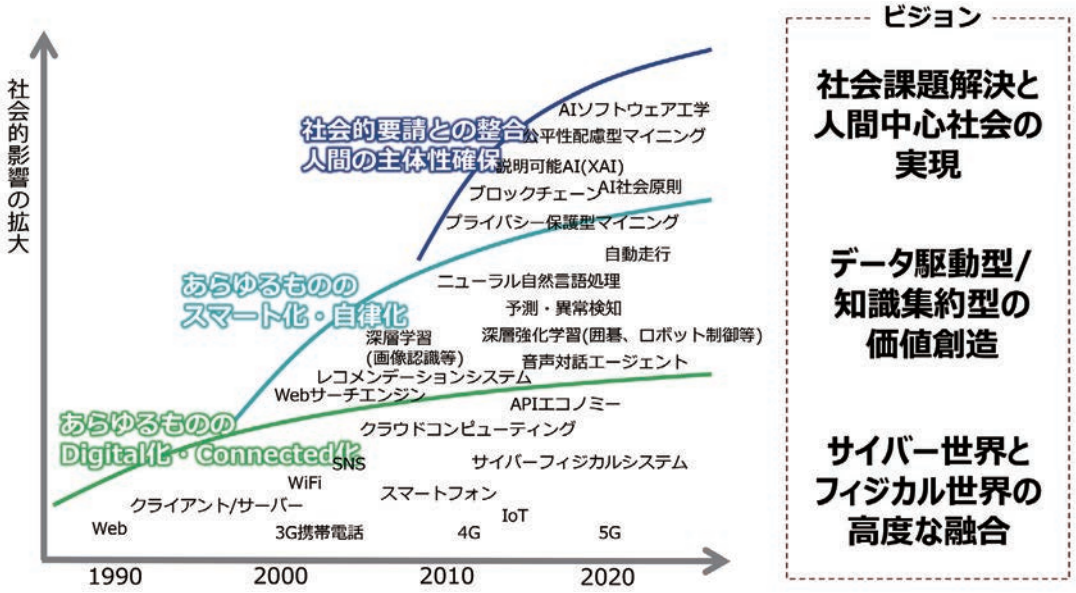


図2-1-1　　情報科学技術の潮流と社会の要請・ビジョン

これらの情報科学技術のトレンドを踏まえ、「エマージング性」「社会の要請・ビジョン」「インパクト」の3点を基準として、戦略的に重要度が高い研究開発領域を合計36領域特定した。この36領域を、前述の「あらゆるもののデジタル化・コネクティッド化」「あらゆるもののスマート化・自律化」「社会的要請との整合、人間の主体性確保」という3つのトレンド上にマップし、「人工知能・ビッグデータ」「ロボティクス」「社会システム科学」「セキュリティー・トラスト」「コンピューティングアーキテクチャー」の5つの区分でまとめたのが、図2-1-2である。

今回は、この「セキュリティー・トラスト」区分を対象に、ワークショップを実施する。本区分で特定された研究開発領域としては、「IoT・制御システムセキュリティー」「サイバーセキュリティー」「データ・コンテンツのセキュリティー」「トラスト」の4領域がある。

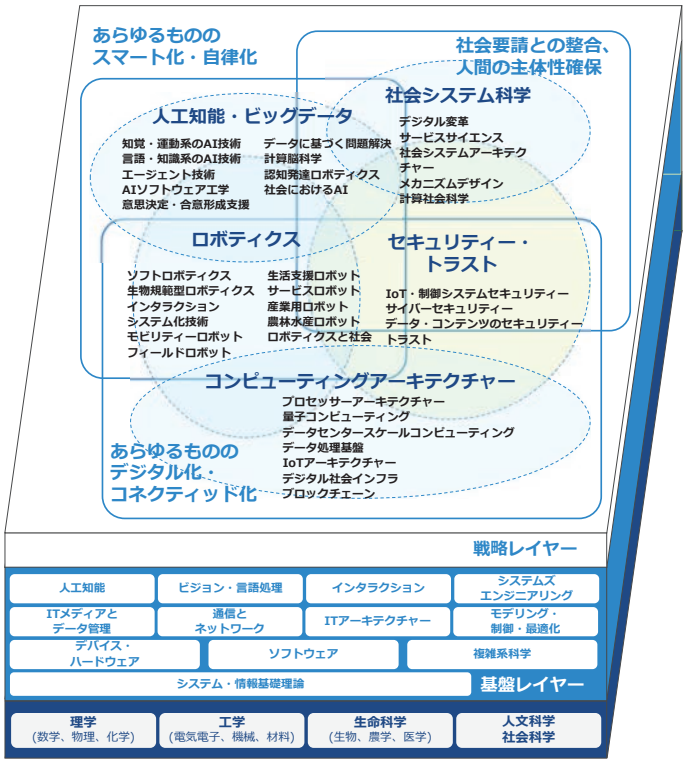


図 2-1-2　　戦略的研究開発領域の俯瞰

「セキュリティー・トラスト」区分は、情報システムや情報サービスが進歩・発展している中で重要度が増してきている「セキュリティー」、および社会やユーザーの視点から見たときに、情報システムや情報サービスを安心して利用できるよう信頼を確保するための「トラスト」という２つの側面から捉える区分である（図2-1-3）。

図 2-1-3　　セキュリティー・トラスト区分

セキュリティー・トラスト区分の全体像を図2-1-4に示す。この図では、本区分を大きく３つのレイヤーに分けている。一番下が基盤レイヤー、中央が情報システムのレイヤー、一番上が人・社会との関係を示すレ

イヤーである。中央の情報システムのレイヤーには、悪意ある第三者の攻撃からの保護である情報システムや情報サービスのセキュリティー、およびそれらの想定する機能が安定して維持されるという広義の信頼性（ディペンダビリティー）に関する技術群を位置付けている。ここでは横軸をセキュリティー技術と信頼性を確保するための技術に分け、縦軸を守る対象であるデバイス、システム、および情報に分けて示している。今回、図2-1-4に黄色で示す4つの研究開発領域を取り上げ、俯瞰報告書にまとめている。

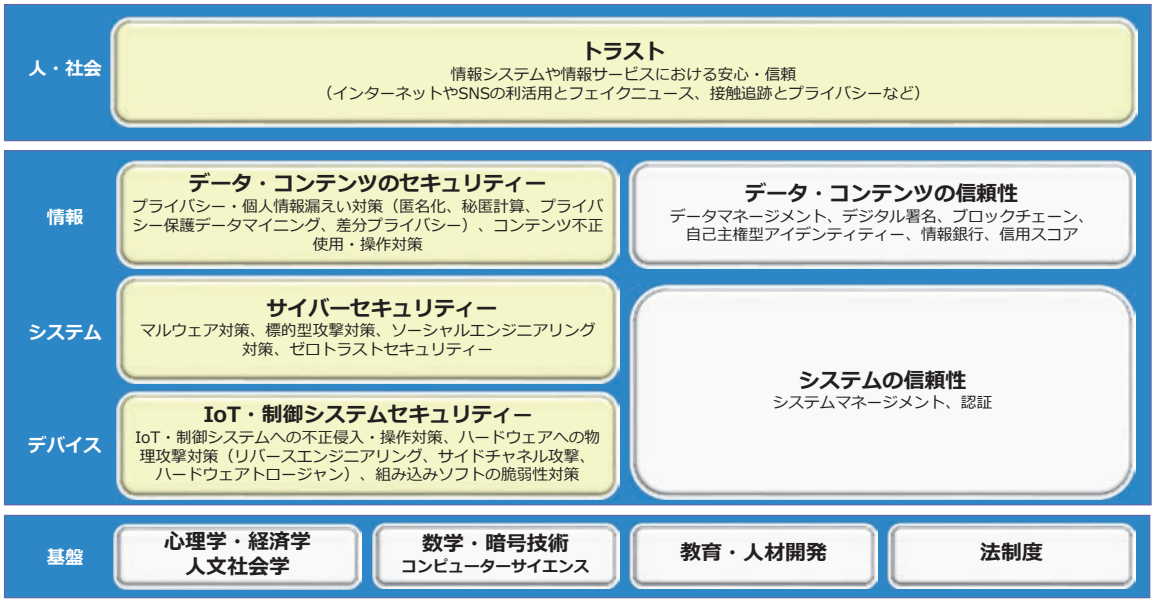


図2-1-4　　セキュリティー・トラスト区分　俯瞰図（再掲）

セキュリティー・トラスト区分の時系列の俯瞰図を図2-1-5に示す。同図が示すように、「インフラ」「プラットフォーム」「サービス」という3つの大きな流れが広がる中で、セキュリティーとトラストの重要性が高く認識されるようになってきた。

有線通信や無線通信、スマートフォンの発展といった通信インフラが発展し、さらにIoT（Internet of Things）が広がることによって、身の回りの物から電気やガスなどの社会インフラに至るまでもがネットワークにつながるようになってきた。このようなインフラの発展に伴い、電子メールやウェブ検索、クラウドなどのプラットフォームや、eコマースやSNS（Social Networking Service）、電子政府などの多様なサービスが続々と登場してきている。

このような状況の中、多種多様なマルウェア（不正プログラム）の増加や、DoS（Denial of Service）・DDoS（Distributed Denial of Service）攻撃や標的型攻撃など攻撃手法の多様化、個人情報漏えいによるプライバシー保護の問題など、セキュリティー上のリスクが高まっている（図2-1-5における赤色の事項）。同時に、さまざまなセキュリティー技術による強化対策（図2-1-5における下線部の事項）や、制度面での対策が発展してきている点も、重要な流れである。

また近年、社会との関係においては、フェイクニュースやCOVID-19の接触確認アプリにみられるように、情報システムや情報サービスにおける安心・信頼の概念であるトラストが重要視されるようになってきている。

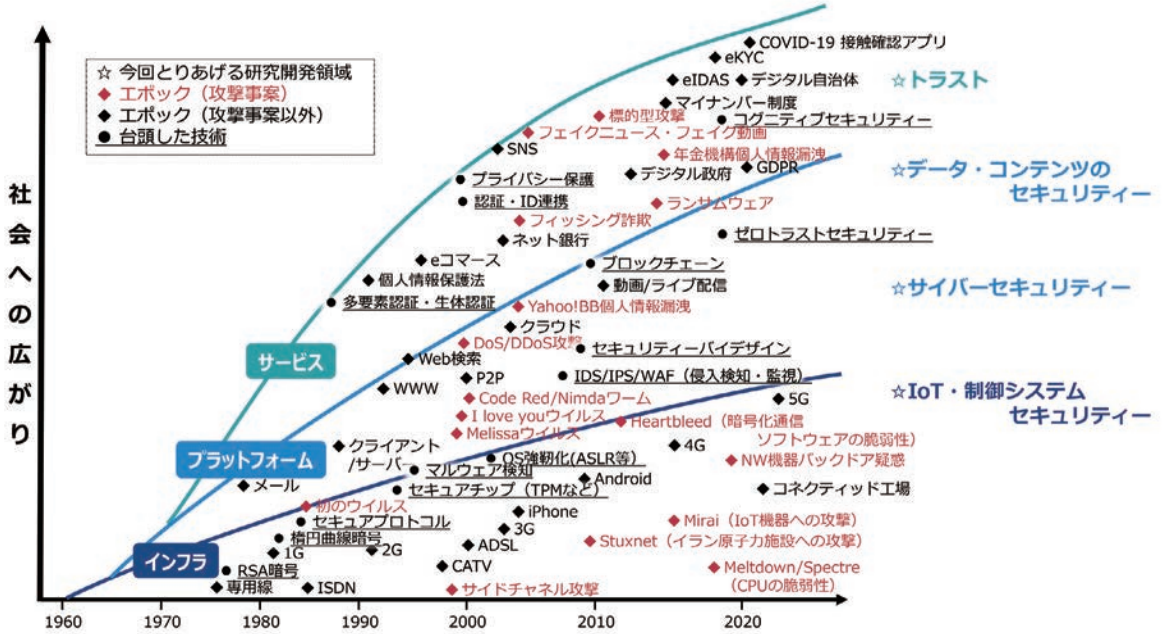


図 2-1-5　　セキュリティー・トラスト区分　時系列俯瞰図

【議論】

（俯瞰図（構造図））

C：今回の俯瞰報告書では、セキュリティーを構成する要素を先に考えマッピングしている。これは一つの切り口ではあるが、セキュリティーは総合的なものなので、全てのレイヤーはつながっている。アプリケーション・出口側から見て、そのセキュリティーをどう守っていくかを考える、トップダウン的なアプローチもあるのではないだろうか。これによって共通のビルディングブロックの洗い出しができ、別のマップが描けるかもしれない。

C：すべての技術はつながっているので、区切るのは難しい。例えば、IoTはクラウドを含んでサービスを実現しているし、個人情報も含んでいる。

C：セキュリティーとトラストという括りでよいのかなという疑問はある。セキュリティーとしてマッピングされている技術の中には、トラストにマッピングした方がよいと思われるものもある。

C：最近のキーワードであるデジタルトランスフォーメーション（DX）のセキュリティーをどこかに位置づけてもらえると、今後の指針としてありがたい。

（俯瞰図（時系列））

C：サイバーセキュリティーにおけるAIの活用の歴史について触れられるとよい。例えば、シグネチャーベースのマルウェア検知が破綻し始めたことに対し、防御側はAIで対抗するようになり、攻撃側はAI回避のためファイルレスマルウェアを活用しはじめ、そして防御側は振る舞い検知の努力をしていくという歴史がある。他にもAIの活用は進んでおり、1つのエポックと呼んでよいのではないだろうか。

C：インフラにStuxnetが入っていることに違和感がある。確かにインフラへの攻撃事案であるが、Meltdownのようなハードウェアの問題ではなく、中身はマルウェアなので、もう少し上のレイヤーの方がよいかもしれない。

2.2 IoT・制御システムセキュリティー

近年のIoTの進展によって、個人の利用端末はもちろんのこと、さまざまなセンサー搭載機器や、工場・インフラの制御機器などの「モノ」がネットワークに接続されつつある。これらの「モノ」がつながることによって発生するリスクが増大しており（図2-2-1、図2-2-2）、そのためのセキュリティー対策を実現するための研究開発領域を、「IoT・制御システムセキュリティー」とする。

IoTの進展

「モノ」がつながることで発生するリスク増大

IoT・制御システム・セキュリティー
「モノ」がつながることによって発生するリスクに対するセキュリティー対策を実現するための研究開発を行う領域

図2-2-1　　IoT・制御システムセキュリティー

IoT機器に関しては、2016年に「Mirai」と呼ばれるマルウェアの感染によって、大規模なDDoS攻撃が発生した。これによって重要なインターネットサービスを一時的に機能不全に陥れた。重要インフラも、近年外部ネットワークに接続されるようになったため、サイバー攻撃の対象になりつつある。原子力施設や石油会社などを狙った攻撃が多数報告されており、今後ネットワーク接続の拡大とともにさらなる脅威の増大が予想される。さらに、システムの基盤であるハードウェアに直接アタックする攻撃も顕在化してきている。

図2-2-2　　IoT・制御システムセキュリティーに関するリスクの顕在化

このような中、注目する動向として3つのトピックを紹介する（図2-2-3）。

1つ目が、「IoT向けのオペレーティングシステム（OS）の研究開発の加速とセキュリティー」である。IoT機器では、組み込み用のLinuX OSや、多様なRTOS（Real Time Operating System）が使われてきたが、近年のIoTの普及に伴って新しいIoT向けOSの研究が盛んになってきている。一方、IoTシステムのOSを狙った新しい攻撃の可能性が高まってきており、対策が急がれている。

2つ目が、「ハードウェアトロージャン」である。ハードウェアトロージャンとは、製造サプライチェーンにおいて設計者の意図に反して付加される回路のことであり、これによってIC（Integrated Circuit）の破壊やセキュリティー低下を引き起こす恐れがある。新たなセキュリティーの脅威として、その検知や抑制する技術の開発が求められている。

3つ目が、「意図的な電磁妨害」である。これはIoT機器内部に強制的に電磁界を誘導させるものであり、これによってICや素子の破壊・データ漏えいの恐れがあることが注目されてきている。リアルタイムにセンシングし、その動作を決定するようなIoT機器にとっては、致命的なダメージを与え得る脅威であり、対策を講じていく必要がある。

図2-2-3　　IoT・制御システムセキュリティー　注目トピック

国内外の注目プロジェクトを図2-2-4に示す。

1つ目が、内閣府の戦略的イノベーション創造プログラム（SIP）である。第1期SIPで「重要インフラ等におけるサイバーセキュリティの確保」、その後の第2期SIPで「IoT社会に対応したサイバー・フィジカル・セキュリティ」が実施されている。第2期SIPにおいては、信頼の基点をIoT端末で実現するためのキーデバイス「セキュア暗号ユニット」の開発が進められ、今後さまざまな応用展開が期待されている。

2つ目が、2018年に産業技術総合研究所内に設立された、サイバーフィジカルセキュリティ研究センターである。特に、ハードウェアセキュリティー技術に関する研究開発を重点的に実施している。

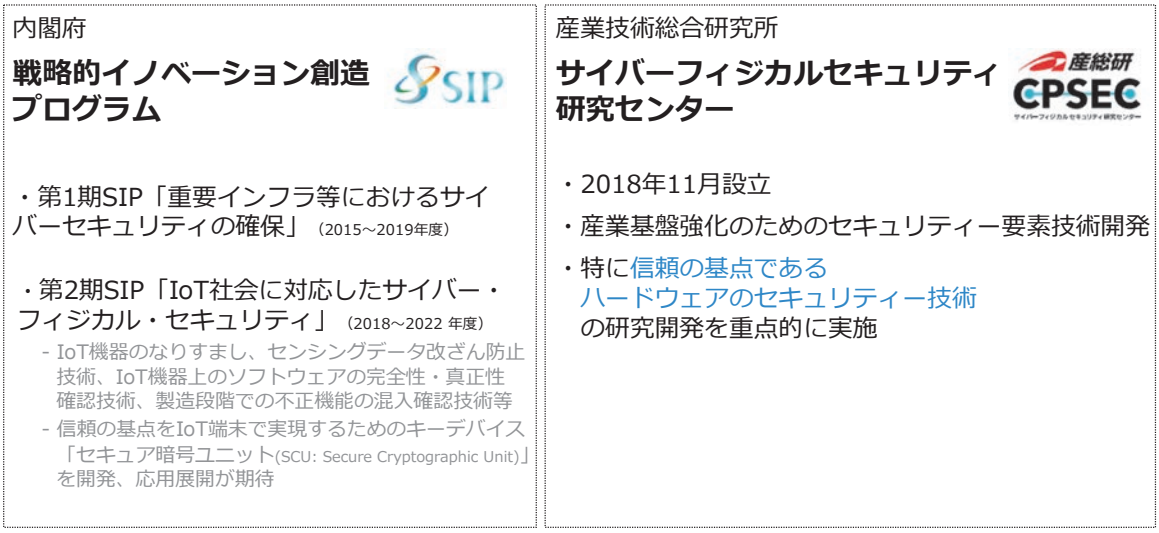


図2-2-4　　IoT・制御システムセキュリティー　国内外のプロジェクト

本研究開発領域における科学技術的課題として、3カテゴリー、合計6つの課題が挙げられる（図2-2-5）。

1）データ改ざん・なりすまし、ハードウェアへの攻撃への対策

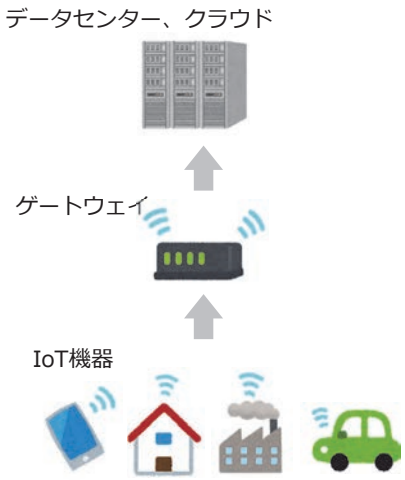
「信頼の基点、機器認証」「計測データの真正性保証」「ハードウェアセキュリティーを低下させる物理現象に着目した対策技術の確立」「オフェンシブセキュリティー・ハードウェアレジリエンス」の4つの課題がある。IoT機器は、無人でかつ第三者でも物理的にアクセス可能な場所に設置されることが多く、IoTシステムの「信頼の基点、機器認証」の構築、およびIoT機器による「計測データの真正性保証」の十分な考慮が必要である。また、さまざまなハードウェアに対する攻撃がある中で、これまでは個別の攻撃に対して対策がとられてきたが、ハードウェアレベルでのセキュリティー低下は、物理現象まで突き詰めると同一メカニズムで引き起こされている可能性があり、これに着目して統一的な対策技術が求められるようになってきている。さらに、機器の設計の段階から攻撃者の立場で脆弱性を洗い出す「オフェンシブセキュリティー」や、インシデントに備えた耐性を確保する「ハードウェアレジリエンス」の考え方・開発・実装が重要になってきている。

2）盗聴・なりすましへの対策

課題として、「高セキュリティーを実現するIoTネットワークの確立」が挙げられる。IoTシステムでは、多数のIoT機器が接続され、また頻繁に接続する機器が追加/削除されるという特徴がある。同時に、不適切な機器が接続される恐れもあり、それによって他のM2M（Machine to Machine）通信を盗聴したり、他の機器になりすましてデータを送出するなどの危険性がある。IoTのオープンな特性を維持しつつ、高いセキュリティーを実現するIoTネットワークの確立が求められている。

3）全体設計

IoTシステムにおいては、システム構築時にセキュリティーが十分に考慮されていないため、脆弱性が存在しているケースも見られる。設計時にセキュリティー対策の十分性を客観的に評価する「セキュリティーシステム検証方法の確立」が課題になっている。



全体設計（脆弱性の十分な考慮）

・セキュリティーシステム検証方法の確立
設計時の客観的な脅威分析

盗聴・なりすまし（不適切な機器が接続）

・高セキュリティーを実現するIoTネットワークの確立
IoTネットワーク構成、ネットワーク・プロトコルの脆弱性検査手法

データ改ざん・なりすまし、ハードウェアへの攻撃

・信頼の基点、機器認証
耐タンパ性に優れたハードウェアに暗号鍵を保管、物理特性の差やコンテクスト認証

・計測データの真正性保証
真正性保証のためのスキーム、攻撃によって改変されたデータが後段に与える影響

・ハードウェアセキュリティを低下させる物理現象に着目した対策技術の確立
物理現象まで突き詰めると、同一メカニズムで引き起こされている可能性

・オフェンシブセキュリティー・ハードウェアレジリエンス
攻撃者の立場で脆弱性を洗い出す　　インシデントに備えた耐性確保

図2-2-5　　IoT・制御システムセキュリティー　科学技術的課題

最後に、表2-2-1に国際比較を示す。

表2-2-1　　IoT・制御システムセキュリティー　国際比較

国	フェーズ	現状	トレンド	状況
日本	基礎研究	○	→	センサーのセキュリティーで、先導研究が実施。 ハードウェアセキュリティー分野に活気（研究会設立等）。
	応用研究・開発	○	↗	CCDSが、国内対象にIoTセキュリティー認証制度を開始。 SIPにて、組込み機器対応セキュア暗号ユニットの社会実装開始。
米国	基礎研究	◎	↗	セキュリティーのトップカンファレンスでの活動が著しい。 トップレベルの人材が米国に集まり、若手の育成も進んでいる。
	応用研究・開発	◎	↗	NISTがIoTセキュリティー基準に関して世界を先導。 設計段階からハードウェアセキュリティーを意識した実装に取り組む。
欧州	基礎研究	○	↗	航空機のIoTで、システム検証を取り入れた安全な設計技術研究を推進。 重要社会インフラに関して、意図的な電磁妨害に関する研究が活発。
	応用研究・開発	◎	↗	IoTにおけるプライバシー保護制度で先行。ハードウェアセキュリティー保証スキーム、意図的な電磁妨害関連の脅威について、標準化が推進。
中国	基礎研究	○	↗	米国機関の在籍者や、米国大学との共同執筆による国際会議論文は多い。 過去5年間で、ハードウェアセキュリティー論文数はアメリカに次いで2位。
	応用研究・開発	○	↗	SC41に多数の規格提案を出している。

【議論】

（具体的なアプリケーション）

C：IoT・制御システム・セキュリティーに関して、具体的なアプリケーションを説明の中に取り入れるとよい。

C：車載エレクトロニクスに関するセキュリティーは重要で、記載があった方がよい。今後は車車間通信や路車間通信など、今までと違うネットワークが使われるようになるし、車は数が多く安全性に直に関わってくるので重要である。

C：自動運転というと、車が前提という印象があるが、実際にはドローンや電車なども今後自動運転が進んでいくように思う。これらは共通の技術でセキュリティーを捉えることができるかと思うので、広めに

「自律走行[1]（最近の国際会議だとオートビークル）」として検討するのもよいだろう。

（信頼の基点・ハードウェアセキュリティー）

C：IoTデバイスや制御システムが人が関わっていないところに置かれる以上、第三者によってデータが収集されたり改ざんされたりする恐れがある。その中で、収集されたデータをもとに何かを判断するとなると、そのデータが本物（本当）なのかを保証してあげる必要がある。そのために、どこに信頼の基点を置くかが重要な問題になってきている。

C：情報がネットワークに流れていくときも、車が動くときも、外界へのアクションが生ずる時にはハードウェアが必要となる。そのため、ハードウェアが信頼の基点となることが多いが、そうした状況においてハードウェアの中でどの部分を基点とするのか、ハードウェア内部の構造を精査した上で検討する必要がある。また、サプライチェーン含めて、ハードウェア内部の信頼の基点となるコンポーネントを国内で作り上げていくことが今後の課題である。

その1つの解となるのが、内閣府SIPで開発しているセキュア暗号ユニットである。完全に国産で、製造工程含めて信頼できるよう、サプライチェーンから全部考え直して開発を行っている。国内でこういった事例を多く生み出すことが重要である。

C：日本では、ハードウェアを基点としたトラストチェーンの構築が弱い。リモートアテステーションなどのリモートからの検証技術もある。ハードウェアとセットで検討していくとよい。

（フォレンジック）

C：IoT・制御システムセキュリティーにおいて、フォレンジック（セキュリティーインシデントへの対応や、電磁的記録の調査・分析などを行う技術の総称）は重要である。

C：IoTデバイスは、基本的に人間が関わっていない場所に置かれる。したがって、事故が起きたときに、何が起きたかを後から解析する手段を残しておく必要がある。自動車でも、事故の原因は運転にあるのか、機器の故障なのか、外部からの攻撃なのかが問われる。客観的にシステムやデータによって解析できるようにしておく必要がある。

C：今後、IoTデバイスが膨大に増えることを考えると、デバイス同士が互いに見張るような相互監視ということも考えられるかもしれない。例えば、ドライブレコーダーは、自分の車の事故の証明を行うが、前方を走っている車のことも記録してくれている。そのように視野を広げることで、社会全体へのよい意味での見守りを与えられるだろう。

（その他）

C：近年注目するものとして、強電磁界による意図的な電磁妨害による攻撃があり、車や電車などが攻撃の対象になってきている。米国や欧州、中国などでは、こうした攻撃もスコープに入っており研究が進んでいるが、日本では本研究領域にあまり焦点が当てられていない。電子戦というと特殊な分野に属してしまい、セキュリティーのカテゴリーとして検討するのが難しいせいかもしれない。

Q：普通の自動車に対して電磁波を浴びせて事故を起こすという攻撃もあり得るか。

A：実例が報告されている。車はフェールセーフの機構がしっかりしているので、強電磁界をかけることで、ブレーキが作動するのだが、高速道路でそれが起きた場合は逆に事故になる。こうしたケースまで自動運転では考える必要がある。

1 自律走行に関する最近の研究事例では、以下のようなものが挙げられる。
https://www.ndss-symposium.org/ndss-program/autosec-2021/

C：IoT・制御システムの場合、時間軸が長くなることも考慮することが重要である。新旧のデータ処理や、さまざまなデバイスの混載、拡張性や更新など、長期にわたるシステムをどう維持していくのかという観点も見ていく必要がある。

C：40年以上前のCP/M（Control Program for Microcomputers）がまだ動いているという話も聞く。飛行機も40～50年飛ぶし、普通の車でも平均寿命は10数年ある。どう維持していくか、難しい問題である。

C：本研究開発領域では、既存の制御システムの話題と、今後の膨大な数のIoTデバイスの話題は分けて整理した方が分かりやすい。今後、膨大な数のIoTデバイスをリモートから管理するためには、信頼の基点が必須となる。トラストの面からのビックピクチャーを描くとわかりやすいかもしれない[2]。

2 【参考】松本泰, AI・IoTによるイノベーションを支える暗号技術によるトラスト, https://www.jnsa.org/jnsapress/vol47/2_kikou-2.pdf

2.3 サイバーセキュリティー

「サイバーセキュリティー」は、インターネットが進歩し発展している中で、日々高度化するサイバー攻撃へのセキュリティー対策を扱う研究開発領域である（図2-3-1）。

インターネットの進歩・発展

日々高度化する
サイバー攻撃
へのセキュリティー対策

サイバーセキュリティー
サイバー攻撃の検知や遮断、侵入後の調査や復旧、分析・防御技術の確立などのための研究開発を行う領域

図2-3-1　　サイバーセキュリティー

従来、サイバーセキュリティー研究は、侵入検知やマルウェア（不正プログラム）の解析、検知、駆除など、それぞれの攻撃に対する直接的な対策がとられてきた。一方、近年は常に新しい攻撃が出現する状況の中、そのような対処療法的な対応だけでなく、システム構成やその運用・保守体制、組織構成なども踏まえた、多様かつ総合的な対策へと研究開発の流れが広がってきている。また、サイバーフィジカルセキュリティーという言葉が象徴するように、サイバー攻撃が実社会に多様な影響を与えるようになっており、サイバーセキュリティーが扱う技術領域が拡大してきているという傾向にある（図2-3-2）。

従来
攻撃への直接的な対策

・侵入検知
・マルウェアの解析・駆除
・・など

近年　常に新たな攻撃
多様・総合的な対策

実社会に多様な影響
サイバーセキュリティーが扱う技術領域が拡大

図2-3-2　　サイバーセキュリティー研究の流れ

本研究開発領域における注目トピックを、3つ紹介する（図2-3-3）。

1つ目は、「大規模・ユニークなデータ収集を強みとしたビッグデータ分析」である。サイバーセキュリティーは、データドリブンな研究開発になる傾向が強く、ビッグデータ分析の様相を呈している。いかに大規模でユニークなデータを収集できるかが、研究開発の強みになってきている。

2つ目は、「ゼロトラストセキュリティー、およびヒューマンファクターを考慮したセキュリティー研究」である。デジタルトランスフォーメーション（DX）の進展や、COVID-19を契機とした働き方の変革により、人々のICT利用形態が大きく変遷してきている。価値ある情報がこれまで以上にネットワーク上を流通し、またクラウド上に蓄積されることで、これを狙うサイバー攻撃も増加することが予想される。また、新しいICT環境の中で、ユーザーの不十分な理解や認識のずれを突いたソーシャルエンジニアリング攻撃が活発化する恐れがある。そこで、境界防御でなく、組織内外に関わらずセキュリティー脅威が存在するという前提に基づいたゼロトラストセキュリティーの概念や、システム的側面だけでなく、それを扱う人間の振る舞いに着目する、ヒューマンファクター研究の重要性が高まっている。

3つ目は、「研究倫理への配慮」である。相当数の国際学会で、研究倫理に関する配慮が投稿条件になってきている。これによって、学会に投稿することによる、攻撃者に資するリスクを最小化すること、同時にメリットを格段に大きくすることを確認する潮流ができてきている。

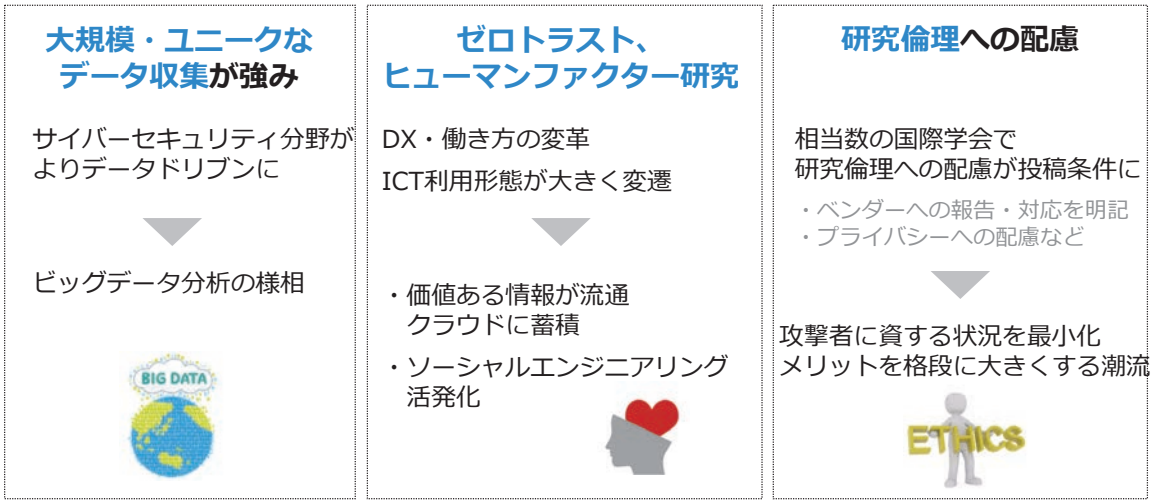


図2-3-3　　サイバーセキュリティー　注目トピック

国内外の注目プロジェクトを図2-3-4に紹介する。

国内では、主要なものとして、NICT（National Institute of Information and Communications Technology）と総務省による取り組みを示す。1つ目が、NICTによる「Web媒介型攻撃対策技術の実用化に向けた研究開発（WarpDrive）」で、ウェブアクセスの履歴を収集して、攻撃の対策技術について研究開発・社会実装を進めているものである。2つ目が、同じくNICTによる「NOTICE（National Operation Towards IoT Clean Environment）」で、サイバー攻撃に悪用される恐れがあるようなIoT機器を調査して、注意喚起を行うものである。3つ目が総務省による「電波の有効利用のためのIoTマルウェア無害化/無機能化技術等に関する研究開発」で、IoTマルウェアなどの詳細分析や無害化、無機能化に関する研究が進んでいる。

海外では、米国のNSFと欧州のHorizon2020を中心に、さまざまな研究開発が広く行われている。

図 2-3-4　　サイバーセキュリティー　国内外のプロジェクト

本研究開発領域における科学技術的課題の一覧を、表 2-3-1 に示す。大きく 5 つの項目でまとめている。1 つ目が「インターネットレベルでのセキュリティー対策」、2 つ目が「Web セキュリティー」、3 つ目が「組織の枠を超えた情報連携」、4 つ目が「各組織の中のセキュリティー対策能力の向上」、5 つ目が「サイバー攻撃可視化」である。

表 2-3-1　　サイバーセキュリティー　科学技術的課題

項目	脅威・脆弱性	具体的な課題
インターネットレベルでのセキュリティー対策	大規模感染型マルウェア DDoS攻撃	大規模ネットワーク観測、攻撃予測・早期検知・早期対策など
	マルウェア （膨大な亜種・解析回避機能）	サンドボックス解析技術高度化、マルウェア解析回避機能対策など
Webセキュリティー	ドライブ・バイ・ダウンロード （DBD）攻撃	Webブラウザを観測点とした大規模観測・分析など
	ソーシャルエンジニアリング	URL名やコンテンツ自体の分析など検知技術
組織の枠を超えた情報連携	サイバー攻撃情報共有の難しさ	グローバルなレポジトリの構築、異なる攻撃の相関分析など
	脅威インテリジェンスの生成・有効活用の難しさ	インテリジェンスを活用した対策の自動化、インテリジェンス自体の自動生成など
各組織の中のセキュリティー対策能力の向上	標的型攻撃	組織内の観測・分析・検知、組織内のログマネジメント、フォレンジックなど
	アラート対応疲れ	喫緊に対応が必要なアラートの抽出など
サイバー攻撃可視化		オペレーションの迅速・効率化、セキュリティーアウェアネスの向上など

最後に、表 2-3-2 に国際比較を示す。

表 2-3-2　　サイバーセキュリティー　国際比較

国	フェーズ	現状	トレンド	状況
日本	基礎研究	○	↗	サイバーセキュリティーやマルウェア解析に関する発表件数は増加傾向。著名な国際会議での発表件数も、ここ数年着実に伸びてきている。
	応用研究・開発	○	→	内閣府PRISMで、実践的研究が推進。サイバー攻撃のリアルタイム分析・可視化技術(NICTER)は世界をリード。国産セキュリティー製品は少ない。
米国	基礎研究	◎	→	基礎研究力が高く、著名な国際会議でのプレゼンスも高い。豊富なファンディングで大小のプロジェクトが継続実施。 産業界からの人材流入も多い。
	応用研究・開発	◎	→	大学での研究が実用化を目指したものが多く、起業につながる例も多い。巨大企業からスタートアップまで様々な規模で製品やサービスを展開。
欧州	基礎研究	○	→	マルウェア解析技術やサイバー攻撃観測技術等で高い研究成果。一方、優秀な研究者の米国等への移籍例も多く、研究人材確保は容易ではなさそう。
	応用研究・開発	○	↗	国際的に活躍するセキュリティーベンダーが複数存在し、セキュリティー関連製品で高いシェアを保有。
中国	基礎研究	◎	↗	トップクラスの大学の学生が米国等に留学し、研究レベルを上げている。中国国内の研究機関における成果が著名な国際会議に採録されてきている。
	応用研究・開発	△	↗	国際的に注目される大規模研究プロジェクトは見られない。Huawei等が通信産業で世界をリード、国内向けセキュリティー産業が成長中。

【議論】

（全体）

C：IoT・制御システムセキュリティー領域では、ミクロな視点で、個々のデバイスのセキュリティーレベルをいかに上げるかに注目していたのに対し、サイバーセキュリティー領域はマクロな視点で、サイバー空間全体のセキュリティーを見ている印象がある。冒頭の俯瞰図の示し方も、このような観点が何らかの形で反映されるとよい。

（サイバーセキュリティー動向の変化）

C：サイバー攻撃の標的や目的が変化してきている。いたずらや嫌がらせだった行為が、いまやビジネス化されてきているというトレンドがある。実際、ランサムウェアでかなりの資金が犯罪者に流れているという話があったり、攻撃が分業化されたりしてきている。また攻撃の背後に国家の存在が伺えるケースもある。

Q：確かに、攻撃がどんどん大掛かりになってきている印象がある。それに対して、どのような課題を解決していけばよいか。

A：攻撃の影に国家の存在がみえるなど大きな問題になると、技術だけで解決するのは難しい。研究者としてできることと政治的に行うべきことを分けて、連携して考えていく必要があるだろう。

（情報連携をスムーズに行わせる仕組み）

C：組織間の情報連携は非常に重要である。現在、IoTデバイスから得られた情報は、ほとんどの場合クラウドに集約される。したがって、それぞれの企業がそれぞれのデータを集めているという状況である。しかし、例えば将来のコネクティッドカーサービスを考えると、どこの企業の車であってもそのサービスを使いたいという、業種横断的な情報連携も出てくると思う。また、スマートシティでも、都市OSが仲介して、スマートメーターや電気の使用量、健康情報など、さまざまな情報を合わせることで、更によいサービスを作ることが想定できる。そのためにも、情報連携が重要であり、それがDXを実現するの一つの鍵になるだろう。

Q：「データ・コンテンツのセキュリティー」領域で取り上げられる匿名化などの技術を使って、組織間の情報共有をするのはどうか、ということか。

A：そのとおりである。情報を別の機器に渡す際に、渡す側でセキュリティー・ポリシーを定められるよう

にすべきである。例えば、名前と年収のデータをペアで使ってはいけないが、個別に使うのはよいなど。

C：確かに、サービスやハードウェアはどんどん仮想化されて、いろいろな組み合わせが出てくるだろうから、情報を横通しで見ていくのは重要だろう。また技術的に対応できる部分でもある。

Q：情報の共有は、単一の組織だけでは促進されないので、何らかの仕組みや支援が必要ではないだろうか。

A：例えば、法執行機関は、押収したサーバーから多くのダークマーケットの情報を得ている。将来的にそのような情報にアカデミアがアクセスできるようにすることや、アクセス可能なトラストな研究環境を構築するということが考えらる。

A：情報共有の枠組みがあるとよいが、実際にはアナリスト同士が個人的なつながりで情報連携をしている方がうまく回っているという感覚もある。情報連携を強制させる動きよりも、そのようなコミュニティ活動を支援するということがよい作戦かもしれない。

C：2019年のダボス会議で安倍晋三首相（当時）が提言したData Free Flow with Trust（DFFT, 信頼ある自由なデータ流通）における「with Trust」が、情報共有を実現する鍵でもある。

C：トラスト・ガバナンスとDFFTに関して、日本から世界経済フォーラムを通じて白書[3]を出しているので、参考にされたい。

（ヒューマンファクター研究）

C：ヒューマンファクター研究は今、1つの大きなトピックになっている。ソーシャルエンジニアリングや騙しが根幹にあるのだろうと感じている。そういう騙しがあったときに人間はどのように認知してしまうのかとか、攻撃者はどのように考えているのかなど、ヒューマンファクターはより広く捉えることができる。技術的には、セキュリティーインジケーターを示すこと、教育の観点では、人のリテラシーをあげることなどが挙げられる。科学技術的課題として取り上げる中でも、もう少し膨らませてもよいだろう。

C：特に、DXやテレワークの推進により、データ共有、コラボレーション・コミュニケーションツールが増えることが予想され、その脆弱性やセキュリティー不備を突いた攻撃も増えるだろう。ちょうど、プロジェクト管理、共有ツール経由でのインシデントがニュースになっている。

C：ヒューマンファクター研究は、（フィッシングに引っ掛かるような）エンドユーザーだけでなく、システムを管理・対策する管理者やアナリスト、システムを作成する開発者に対しての研究（いかに脆弱性を作り込まないかなど）も進んでいる。このあたりのヒューマンファクター研究は日本はまだまだ進んでいない。

C：暗号資産を狙う攻撃においても、個人の認知のすきをついて騙すような事例が多数起きている。金融庁も注意喚起を行っている。

（連鎖するサイバー攻撃の観測に関する研究動向）

Q：IDとパスワードが盗まれ、そこから別の情報が抜き取られ、攻撃者も連鎖し、最終的に暗号資産の消失やパイプラインのストップなど、大きなターゲットへの攻撃につながるという、サイバー攻撃の連鎖が起きている。これに対する日本の研究の状況はどうなっているか。

A：アカデミアでは、マルウェアなどの機能を解析する研究が進んでいる。検体さえ捕まえることができれば解析は可能である。ただ、そこにつながる攻撃者が個人なのか組織なのかや、背景に経済的なことや政治的なことが絡んでいるかというところまで、時系列で追いかけることは難しい。ハニーポットを

3 World Economic Forum, Rebuilding Trust and Governance: Towards Data Free Flow with Trust (DFFT), http://www3.weforum.org/docs/WEF_rebuilding_trust_and_Governance_2021_JPN.pdf

仕掛けて、入り口部分を観測・解析することはもちろんのこと、入った後何をするのかというところも見るようにしていきたい。少しずつ情報は溜まってきているが、世の中で実際に起きている攻撃をリアルタイムで観測するところまではいっていない。

Q：そのような研究を加速させる環境や取り組みの事例はあるか。

A：国立研究開発法人情報通信研究機構（NICT：National Institute of Information and Communications Technology）のサイバー攻撃誘引基盤STARDUSTでは、そのような観測を行おうとしている。難しいのは、観測のために作った環境で検体を動かしても、リアルな環境とは違うので、長期的に深い観測することは難しいこと。リアルなプロダクションシステムの中で監視するのが一番よいが、機微な情報が入るので、研究材料として使うことが難しいというジレンマがある。

プロダクションシステムの中に、そのような観測的な要素を入れてデータを分析する環境として、大学のリアルなシステムを活用するという方法も考えられる。ただ現場で起きていることと研究での想定にはある程度のギャップがあるので、実際のインシデントに対し、研究した技術を入れていけるかは課題である。

（国際比較）

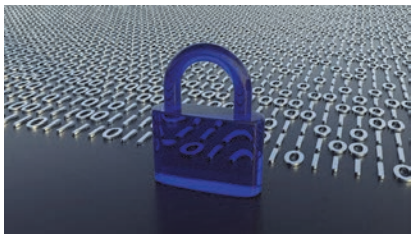
欧州のトレンドはもう少し上向きかもしれない。ただ、欧州は優れた研究もあるが、幅があると思うので、これも一つの結果ではある。

2.4 データ・コンテンツのセキュリティー

近年、多様かつ膨大なデータが得られるようになり、その社会・経済的な活用が進んでいる。一方で、データ活用から生じるセキュリティーやプライバシーの課題が浮き上がってきている。データ活用と、セキュリティー・プライバシー保護の両立が求められており、これに関する技術全般を扱う研究開発領域を「データ・コンテンツのセキュリティー」とする（図2-4-1）。

データ活用が
インターネット経済発展の中心
プライバシー保護への要求高まる

データ活用と
セキュリティー・プライバシー保護の
両立が重要



データ・コンテンツのセキュリティー
個人情報や機密情報の収集、流通、管理、解析などの過程において、セキュリティーやプライバシーを保護する技術全般を扱う研究開発領域

図2-4-1　　データ・コンテンツのセキュリティー

セキュリティー・プライバシーに関するインシデントの例を図2-4-2に示す。国内外で個人情報漏えいに関するインシデントが起きている。また近年では、フェイクニュースやフェイク動画などが社会問題化している状況にある。このようなセキュリティー・プライバシーに関する問題への代表的な対策技術として、匿名化や秘匿計算（秘密計算）、差分プライバシーが挙げられる。

2004年
Yahoo! BB　個人情報漏えい
アクセス制限不備による約450万人分の個人情報漏えい

2015年
日本年金機構　個人情報漏えい
標的型攻撃メールによる約125万人分の個人情報漏えい

2019 年
Facebook　個人情報オンライン閲覧可能状態
2億6,700万人以上の個人情報が閲覧可能な状態に

近年では
フェイクニュースやフェイク動画が社会問題に
悪意・扇動意識を持った思考誘導の情報操作

代表的な対策技術

①匿名化
データの削除・置換等によって、個人を識別不能にする技術

②秘匿計算
データを秘匿（暗号化）したまま、任意の計算や解析を行う技術

③差分プライバシー技術
抽出された知識からプライベート情報が漏えいしないように精度を落としたりノイズを加えたりする技術

cf: 局所差分プライバシー
個人がデータ収集者へデータ提供する際にプライバシー保護処理を行い、個人データを推定されないようにする技術
データ収集者が完全に信頼できるとは言えない状況があり、提案されるようになった。GAFAが取り入れ始めている

図2-4-2　　セキュリティー・プライバシー問題と対策

本研究開発領域における注目トピックを、2つ紹介する（図2-4-3）。

1つ目が、「AIシステムによる差別」である。 AIによる出力や決定が、人種や性別、健康、宗教などと相関する場合、差別の問題になる恐れがある。これに対して、差別配慮型のAIの学習や、AIによる決定を演繹的・説明可能にする研究が活発化している。

2つ目が、「敵対的生成ネットワーク（GAN：Generative Adversarial Networks）」の発展である。これによって、本物と見紛う画像や音声、映像を生成可能になってきていて、真正性の保証が揺らぐ状況にある。その対策として、フェイク検知やファクトチェック支援、メディアリテラシーの向上などが重要になってきている（詳細は、研究開発の俯瞰報告書　システム・情報科学技術分野（2021年）「2.1.5 意思決定・合意形成支援」参照）。

図2-4-3　　データ・コンテンツのセキュリティー　注目トピック

国内外の注目プロジェクトを図2-4-4に示す。

国内では、JSTの戦略的創造研究推進事業CREST「イノベーション創発に資する人工知能基盤技術の創出と統合化」領域において、「プライバシー保護データ解析技術の社会実装」という研究課題が推進されている。また、文部科学省における戦略目標「信頼されるAI」をもとに、2020年度からCREST、さきがけ、ACT-Xにおいて研究が開始されている。さらに、本俯瞰報告書執筆時点では確定していなかったが、戦略目標「Society 5.0時代の安心・安全・信頼を支える基盤ソフトウェア技術」が立ち上がり、2021年度からCREST、さきがけの研究公募が開始された。

海外では、米国のDARPA（Defense Advanced Research Projects Agency）において、コグニティブセキュリティー関連プロジェクトが活発化している。これは、フェイクに見られるような人々の思考や行動に対して悪影響を与える攻撃から守るための研究で、画像・動画の改ざんやフェイクの検知、ソーシャルエンジニアリングの検知・防御など、幅広い研究開発が進んでいる。

図2-4-4　　データ・コンテンツのセキュリティー　国内外のプロジェクト

本研究開発領域における科学技術的課題を2つ紹介する（図2-4-5）。

1つ目が、「AIセキュリティー・プライバシー」に関する課題である。個人情報やコンテンツ情報の偽装が近年容易化してきていることで、差別やプライバシー侵害、情報の偽造・悪用の恐れが高まっている。これに対し、取得・収集する入力データだけでなく、それを用いて学習した出力データに関する管理も課題になってきている。また、AIの学習には大量のデータが必要であるがコストが高いということや、法令上、収集する個人情報は最小限度とする要求があり、データ収集量を減らす、個人に情報をとどめる、といった対策をしつつ、高度なAIの学習を実現するような技術に注目が集まってきている。

2つ目が、「局所差分プライバシー」に関する課題である。局所差分プライバシーは、個人がデータ収集者にデータ提供する際にプライバシー保護処理を行い、個人データ推定を防ぐ技術であり、近年、GAFA（Google、Amazon、Facebook、Apple）が採用しているということで話題になってきている。この局所差分プライバシーについては、ユーザー側の送信データ生成に要する時間や、データ提供時の通信量が議論になっており、利用するデバイスやインフラに合わせたデータ収集スキームと理論解析が課題になっている。

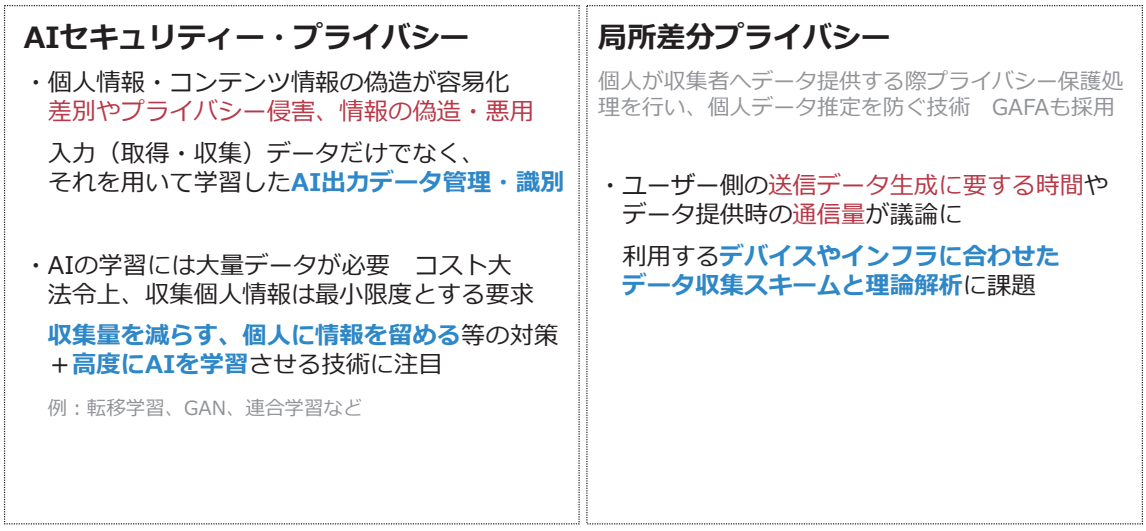


図2-4-5　　データ・コンテンツのセキュリティー　科学技術的課題

最後に、表2-4-1に国際比較を示す。

表2-4-1　　データ・コンテンツのセキュリティー　国際比較

国	フェーズ	現状	トレンド	状況
日本	基礎研究	○	→	暗号理論の基礎研究に従事する研究者は多いが、統計的プライバシー、AIセキュリティー・プライバシーは、研究者の数も少なく存在感が薄い。
	応用研究・開発	○	→	企業による秘密計算実装の提供などが行われているが、応用分野における先進的なプロジェクトは少ない。
米国	基礎研究	◎	↗	多くの学術論文が発表されている。いずれの研究領域においても、コアとなる理論的アイデアはほぼ米国の大学・企業の研究者から提案されている。
	応用研究・開発	◎	↗	局所差分プライバシーなど理論成果の実サービスへの導入が進んでいる。産学の人材交流も活発である。
欧州	基礎研究	○	→	GDPR施行もあって、データ利活用とプライバシーを見据えた基礎的な研究が活発である。
	応用研究・開発	◎	↗	エストニアにおける秘密計算の実用化など、実用を見据えた動きは活発である。
中国	基礎研究	○	↗	中国国内の大学・企業でも、分野問わずトップ国際会議における論文数は年々増加している。
	応用研究・開発	○	↗	民間企業において、秘密計算などの実用例が出始めている。

【議論】

（全体）

C：データ・コンテンツのセキュリティー領域の課題に関しては、他の領域に比べて、ふんわりした趣がある。何かが起きたときに、セキュリティー上の問題があるかどうかの問題提起からして難しいためである。その理由の1つとして、AIが僅かな情報からいろいろなことを当ててしまうという現状がある。そのため、何らかの情報が漏れたことによって、どのようなことが起こるかを予測することが難しくなっている。

C：従来からの秘密計算や差分プライバシーといったセキュリティー分野の研究は着実に発展している。秘密計算自体は、応用分野がブレークしているというところまではいっていない印象であるが[4]、研究自体は進んでいる。差分プライバシーは、技術が登場して15年程度である。これまで理論研究が主流であったが、ここ5年ほどでGAFAが技術を取り入れ始めている。匿名化自体は、技術上あまり難しさはなく、研究というよりはシステム開発上の仕様に近い。どの程度取り入れられているかは、国や法令によって依存するので、俯瞰的に見るのは難しいが、日本でも最近、個人情報保護法に、匿名加工情報に加えて仮名加工情報が導入されたことで、匿名化技術を使っていきたいという考え方は依然としてあると見ている。

（データの信頼の基点）

Q：IoTでハードウェアのセキュアチップのような、いわゆる信頼の基点の議論があった。データに関しても同様に、実社会では信頼の基点があるはず。例えば、自治体が発行する住民票や印鑑証明書、免許証などが、実生活の基のデータになっている。そのような信頼の基点をもとに、信頼できる手法で導き出したデータも信頼ができる、というような形のデータの信頼のチェーンも重要であるように思う。研究面ではどのように見ているか。

4　秘密計算の実用化に向けた企業の動きとして、NECとIT（情報技術）企業のデジタルガレージ、セキュリティー関連のレピダム（現インフォーズ、東京・渋谷）の3社が、秘密計算の普及を目指した「秘密計算研究会」を組織したとの報道が出ている。クラウドサービスなどでの同技術利用を想定し、安全性評価の基準作りなどに取り組む計画であるとのこと。https://style.nikkei.com/article/DGXMZO71492330Q1A430C2000000/?channel=DF010320171966

A：研究分野としては、データの身元を保証しながら活用していくという、トレーサビリティーやプロベナンス関係の技術がある。一時期研究が出ていたが、最近はあまり見かけない。ブロックチェーンもその技術の1つであると思うが、やること自体は現状の技術でなんとかできてしまう。難しいのは、使う人全員がそのプラットフォームに乗らないと意味がないということである。制度や普及、標準化といったことが問題なのかなという印象がある。個人データの分野では、実現して動いているシステムはあまり見かけない。産業上の機密性が高いようなデータなどでは、事例はあるかもしれない。

Q：データの信頼のチェーンに関しては、技術的な研究と、社会科学的な研究のギャップが生じている、つまり実社会での貢献はできていないということか。

A：そのような認識である。費用対効果ということもある。サプライチェーン全体で実現するためには、相当のコストがかかるので、そこに一斉で乗り換えるということには、なかなかならないだろう。

C：データのトラストチェーンといったときに、データの身元保証と、中身の信憑性の担保という2つの意味がある。身元がしっかりしていても、その人が言っていることがフェイクだったり、必ずしもきちんとした情報に基づいていないという可能性があることが、データのトラストチェーンの難しさである。

C：技術的には、ゼロ知識証明など、実現するためのビルディングブロックはあるが、やはり計算コストが高いという問題がある。そこまでコストをかけて得られるものが少ないという状態だと、なかなか広まっていかないのかなと思う。

C：データを保有する企業の視点では、データの流通のされ方にリスクを感じる。流通される側が流通させる意思決定を下しやすい仕組みの確立も必要である。

（セキュリティー・プライバシーを確保したデータの利活用）

C：現実の世界では、膨大な量の正規化されていないスモールデータが散在しているという状況がある。これらのセキュリティー・プライバシーを確保したデータの利活用を、技術的に解決することは難しい。デジタル庁がベースレジストリ[5]の整備に動こうとしているが、これによってデータの相互運用性がとれるようになると、これらの技術・研究領域も脚光を浴びるようになるのではないだろうか。

C：過去のCREST研究[6]で、データが散在していて集まっていないだけという仮定をおき、そのバラバラなデータを秘密計算などの技術によってプライバシーの問題を解決し活用するという研究を実施した。ただ、データを集めてきたから急に役に立つということはなかった。医学研究におけるデータだと、コントロールされたデータを収集し、きちんとした統計的解析を行って結論に導くということが至上命題であるが、野良データを集めてもその結論を信頼できるかという問題が生じるためである。疫学研究の範囲では、後ろ向きにデータを集めても、得られるものは知れているというネガティブな印象もあった。ただ、少しラフな議論でよいようであれば、後ろ向きデータでも十分役立てることはできる。共通のフレームワークが整備されると、より活用できるようになるだろう。

C：法制度との関係も非常に難しい。日本の個人情報保護法は、データの性質で個人情報か否かを判別し制約を課している。このこともあって、処理として、このようなセキュリティー・プライバシー関係の技

5 ベースレジストリとは、公的機関などで登録・公開され、さまざまな場面で参照される、人、法人、土地、建物、資格などの社会の基本データであり、正確性や最新性が確保された社会の基幹となるデータベースとされている。
ベース・レジストリの概要（データ戦略タスクフォース）：
https://www.kantei.go.jp/jp/singi/it2/dgov/data_strategy_tf/dai1/siryou2.pdf
防災とベース・レジストリ（内閣官房IT総合戦略室）：http://www.bousai.go.jp/kaigirep/pdf/210421_01.pdf

6 JST戦略的創造研究推進事業CREST研究領域「ビッグデータ統合利活用のための次世代基盤技術の創出・体系化」研究課題「自己情報コントロール機構を持つプライバシ保護データ収集・解析基盤の構築と個別化医療・ゲノム疫学への展開」（研究期間：2013年10月～2019年3月）

術を活用することがグレーであり、また、処理の是非に関して判断するオーソリティーも必ずしも存在しない。このような課題を解決していかないといけない。

（その他）

C：本領域において、量子暗号や耐量子コンピューター暗号などについても触れてもよいと思う。

C：本領域で紹介されているフェイクニュース・フェイク動画については、ファクトチェックの自動化やディープフェイク検知技術以外に、ヒューマンファクターの観点から偽情報にどうだまされるかやどう対処すればよいかを検討することも重要である。

C：プライバシー保護に関するトピックとして、データのトラッキングの問題がある。Googleが進めるポストCookie/FLoC[7]や、AppleによるiOSのトラッキング防止[8]など、データを流通させたくない、データの囲い込みのようなものがあるかもしれない。

Q：認証/ID/データ主権にかかわる技術トレンドは「信頼性」の方に分類する整理か。セキュリティーと信頼性の区分が難しい。

A：ご指摘のとおり、俯瞰図において「信頼性」に分類している。ただ機器認証など、一部はセキュリティーの領域内でも取り上げており、互いに重なる部分なので整理の難しさを感じている。本日の議論をもとに、取り上げる技術やその整理の仕方について、引き続き検討していく。

7 FLoC（Federated Learning of Cohorts）は、Googleが導入を進めているCoockieの代替技術。
https://developers-jp.googleblog.com/2021/04/floc.html

8 Appleでは、iOS14.5以降、アプリがユーザーをトラッキングしたり、ユーザーのデバイスの広告識別子にアクセスする際には、ユーザーの許可を得る必要があるとした（対応するiPadOSやmacOSなども同様）。
https://developer.apple.com/jp/app-store/user-privacy-and-data-use/

2.5 トラスト

トラストは、古くから社会学や心理学を始めとするさまざまな分野で研究がなされてきた。一方で、情報化が進み、複雑性・ブラックボックス性が増す情報社会において、トラストの概念や仕組みが大きく変化してきている。トラストの定義は分野ごとにさまざまであるが、今回の俯瞰報告書では、情報システムや情報サービスにおける安心や信頼の概念の総称であると定義している。これには技術だけではなく、心理学や人文社会科学の概念を含むものと捉えている（図2-5-1）。

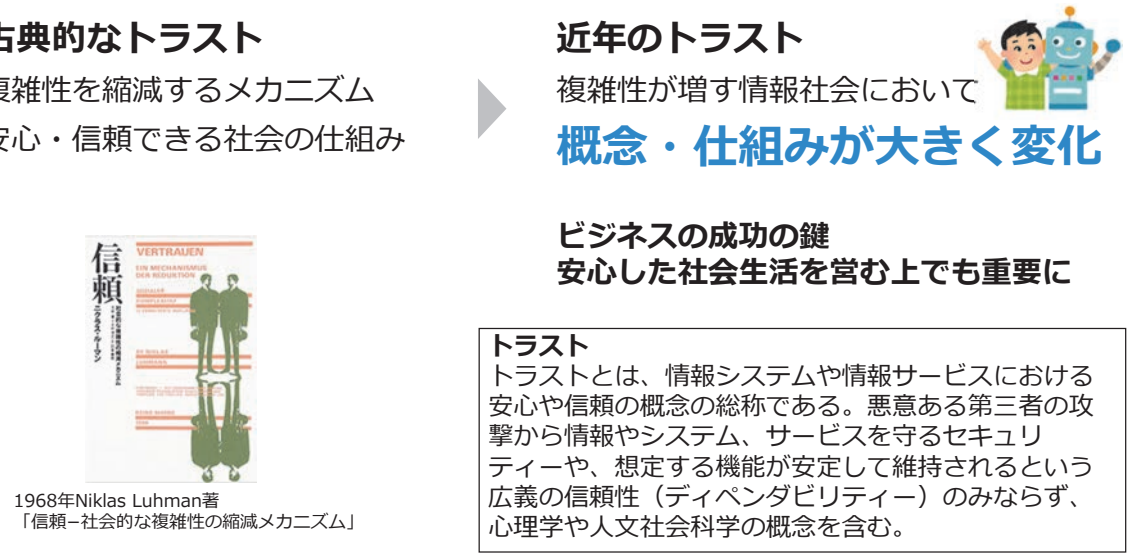


図2-5-1　　トラスト

近年、情報システム・情報サービスが発展し、我々の生活に欠かせない存在になっている。一方で、人々のトラストを揺るがしかねない事態も発生している（図2-5-2）。例えば、インターネットやSNSは、個人から企業まで幅広く活用され普及している。一方、フェイクニュースが社会問題化してきており、情報サービスや、情報自体のトラストを揺るがす状況にある。また、COVID-19感染拡大防止のため導入された接触確認アプリCOCOA（COVID-19 Contact Confirming Application）では、プライバシーが確保されたデザインになっているものの、普及率は低い状態で留まっており、社会からトラストを得られているとは言い難い。

情報システム・サービスへの社会の依存度が高まる中

人々のトラストをゆるがす事態が発生

インターネット、SNS
個人から企業まで幅広く活用、普及
一方、フェイクニュースの社会問題化

接触確認アプリCOCOA
プライバシーが確保された設計
一方、普及率は留まる

図 2-5-2　　デジタル社会におけるトラストの問題

情報システムや情報サービスに対して、人々や社会からトラストを得るためにはどうしたらよいだろうか。今回注目したのが、図 2-5-3 に示す 3 つの要素である。

1 つ目が、人間の心理面への考慮である。情報システムや情報サービスをトラストするかどうかは非常に主観的なものであって、個人が育ってきた時代や環境、社会的な背景などによって多様かつ複雑である。そこで、心理学や経済学、人文社会科学などを含む学際的な検討が必要であろう。

2 つ目が、法律や制度による保証である。基盤となる法律や制度はもちろんのこと、第三者機関や保険制度などを活用することもトラストを得る方法であると考えられる。

3 つ目が、技術的なアプローチである。前節で説明したセキュリティー技術や、公平性・解釈性を担保する技術などによって、技術面でのトラストの確保が可能であろう。

人間の心理面への考慮

心理学や経済学、人文社会科学などを含む学際的な検討が必要
情報システム・サービスをトラストするかは主観的なもの
時代や環境、社会的な背景などによって多様かつ複雑

法律や制度による保証

基盤となる法律や制度、第三者機関、保険制度などによる保証
例）欧州のeIDAS規則：トラストサービスについて欧州全域にわたる枠組み
大規模災害やサイバー攻撃などのリスクに備える制度やサービスを提供する保険　など

技術的な担保

悪意ある第三者の攻撃から守るためのセキュリティー技術
情報システムや情報そのものの信頼性を保証する技術
その他、情報システムの公平性・解釈性を担保する技術や、技術の統合化など

図 2-5-3　　トラストを確保するために　注目する要素

トラスト自体の研究も変遷してきている。図2-5-4に示すように、従来は哲学、心理学、社会学、経済学などが中心だったが、1990年代頃から情報分野におけるトラスト研究が盛んになってきている。近年ではAIに対するトラスト研究が特に活発化してきている。

従来　哲学、心理学、社会学、経済学などが中心

1990年代～
コンピューテーショナルトラスト（Computational Trust）
トラストを計算科学からアプローチする研究
①被信頼者の信頼性情報を定量的・客観的に観測のための研究、②観測されたトラストバリューの評価計算手法・形式化研究、③それに基づく意思決定のためのトラストポリシー研究

1990年代中頃～
トラストインオートメーション（Trust in Automation）
認知システム工学的アプローチからの研究
機械の自動化・自律化が進む中、人間が機械の振る舞いをどう認知・信頼し、その利用にどう影響を与えるかを扱う。近年は自動運転研究でも盛ん。

近年
人工知能（AI）に対するトラスト
AI実装時の社会・人間への影響やELSI
どうすれば人間がAIをトラストできる？

図2-5-4　　トラスト研究の動向

トラストに関する注目トピックとして「トラストサービス」が挙げられる（図2-5-5）。トラストサービスとは、インターネット上における人、組織、データなどの正当性を確認し、改ざんや送信元のなりすましなどを防止する仕組みである。このトラストサービスについて先行しているのが欧州である。欧州全体にわたる枠組みとして、eIDAS規則（Electronic Identification, Authentication and Trust Services）が定められており、これによってデータの主体性の証明やデジタル証明を行う第三者機関を規定していたり、国境を超えて保証レベルを相互運用できるような仕組みにしたりしている。また、トラストサービスの標準化を欧州がリードしているという状況にある。

トラストサービス
インターネット上における人、組織、データなどの正当性を確認し、
改ざんや送信元のなりすましなどを防止する仕組み
例）電子署名、タイムスタンプ、ウェブサイト認証など

eIDAS規則（Electronic Identification, Authentication and Trust Services）
トラストサービスに関する、欧州全域にわたる枠組み
・データの主体者の証明やデジタル証明を行う第三者機関を規定
・保証レベルの相互運用性確保
・トラストサービスの標準化をリード

図2-5-5　　トラスト　注目トピック

国内外の注目プロジェクトを図2-5-6に示す。

国内では、日本学術振興会における科学研究費助成事業の基盤研究（B・C）として、「情報社会におけるトラスト」研究が進められている。トラストの客観的な評価尺度や評価方法、トラストの設計と実現手法、社会的な取組の強化など、人文社会科学を含めた多面的な研究が推進されているようである。

海外の事例としては、GAIA-Xプロジェクトを挙げている。これはEU規模でのデータ共有や利活用を支援するような枠組みであり、データ流通の観点から企業間のトラストの在り方に影響を与えるものとして注目されているものである。

図2-5-6　　トラスト　国内外のプロジェクト

【議論】

（全体）

C：いまトラストが注目を集めるようになってきた。理由の1つとして、DXを進める際に、これまでの社会のトラストの仕組みが足かせになっているということがある。一番身近な事例として、ハンコが挙げられる。ハンコを押す行為には、一定の心理的圧力が加わるため意味があるし、制度的にも強制されてきた。ただこれを続けていると紙から脱却できない。トラストの仕組み自体も変革しないといけない。これがデジタルトラストである。そこには、技術で対応できることと、制度で対応すべきことが混在している。

C：今回の俯瞰報告書では、高度な技術に対する受容性を確保するためにどうすればよいかという視点でのトラストを扱っている。情報技術が複雑になりブラックボックス化が進む中で、それに対する受容性をどうすればよいかという観点である。これについては、特にAIでの議論が多い。他に、トラストのリアルタイムな検証（ゼロトラストでいう検証を行うための技術）や、人が直接介さないIoTデバイスにおける信頼の基点の確立なども、トラストにおける重要なキーワードである。

C：今回のトラストでは、トラストに係る課題の解決や科学技術の進歩が、人類の役に立つという前提で書かれているが、もう一つの側面としてトラストによる囲い込みがあり、トラストは競争領域でもである。トラストに係る技術に非常に熱心に投資しているのは、GAFAのようなプラットフォーマーである。きれい事だけではトラストを獲得できないのではと思うところがある。

（トラストの要素について）

C：俯瞰報告書の中で描かれていた、システム・情報科学技術分野の3つの潮流：①あらゆるものの

Ditigal化、Connected化、②あらゆるもののスマート化・自律化、③社会的要請との整合、人間の主体性確保に分けて、トラストの構成要素を図示すると、例えば図2-5-7のようになる。

Q：①におけるトラストについて。GAFAが投資しているという話があったが、それはプラットフォーマーとして、このようなトラストを提供しているよという意味か。

C：そうである。世の中のトラストやセキュリティーに関する共通の要求は、どんどんプラットフォームに実装されつつあり、これによってプラットフォーマーは次のビジネスを狙っていることが伺える。そのため基本となるコンピューティングアーキテクチャー自身も変わっていっている。

Q：②におけるトラストについて。スマート化というと、機械同士のトラストという意味か。

A：例えば自動運転など、自律的に動くものをどうトラストするかということ。俯瞰報告書にも記載しているトラスト・イン・オートメーションの話にも近い。自律的に動くものには、アカウンタビリティーやトレーサビリティー、トランスペアレンシーが必要で、そのための技術が重要になってきている。

C：③におけるトラストは、主に今回の俯瞰報告書で書かれた視点である。とても重要であり、制度的な解決なしにはこのトラストは形成されない。新たなトラストのメカニズムづくりに、行政に求められるものは大きい。

C：社会学的な信頼の基準は、社会状況や時代とともに移り変わるだろう。一律に決められない難しさを感じる。

Q：標準化などによる保証も大きいように思うが、いかがか。

A：そう思う。トラストサービスの重要な点は、トラスト自体ではない。トラストサービスには、トラストを伝えるという役割や、デジタルな証明の役割がある。スマート化の観点からは、リモートアテステーションのようなリアルタイムに検証できる仕組みが重要であるが、ここは、標準化も進んでいる。

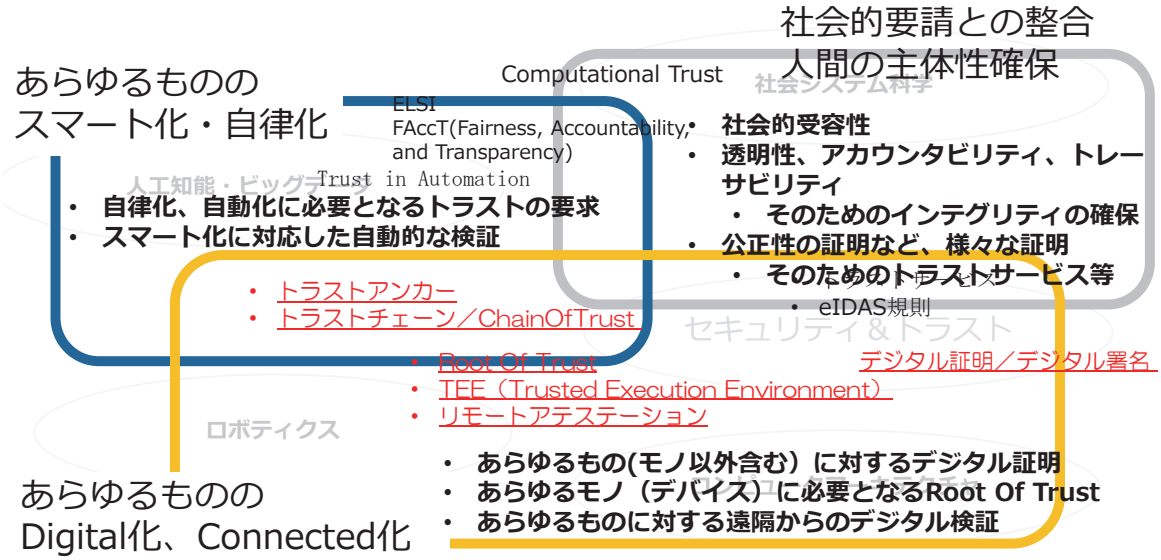


図2-5-7　　システム・情報科学技術分野におけるトラストの整理例

（“見えない”、“測りにくい”トラスト）

Q：人と機器・サービスとの間のトラストを考えると、ヒューマンファクターの要素があるはずである。研究として取り組むべきポイントはあるか。例えば、人によっては、何をもってトラストするかということも変わるはず。一律に、あなたはこれとこれをトラストしなさい、ということは、ヒューマンファクターの視点からは言えないと思う。どういう観点でトラストを確立できるのか、研究として何ができるか。

A：従来から、行動経済学や、社会心理学などでの研究が多い。今は、デジタル化が進み、見えないモノや非常に抽象化されたものがトラストする対象になってきているが、やはり分野としては、行動経済学や社会心理学などの延長線上になるだろう。それに対して、何らかの証明や保証をするというのは、むしろ法制度の仕組みの話になる。それらがうまく噛み合えばよいのだが。

Q：見えないものをどう見えるようにして伝えるかということもあると思うが、いかがか。

A：すでにトラストできるかどうかわからないものの上に、さまざまなサービスが乗っかっている構造になっている。そこはまさにサプライチェーンセキュリティーの問題に近い。そこが整備されて初めて安心してサービス提供できる。やはり制度的な枠組みが重要である。

C：日本は海外と比較して遅れている気がする。例えば、欧州はGDPR（General Data Protection Regulation; EU一般データ保護規則）が強い。またアメリカのCCPA（California Consumer Privacy Act; カリフォルニア州消費者プライバシー法）は、GDPRの強力版。CCPAは特にダークパターンの規制が強い。ダークパターンとは、企業に利するような情報を吸い取りやすいデザインにして、ユーザーに気づかせないようにいろいろな情報をとるような、そういうUIにするというものを言う。世の中でそのようなものが横行していて、それを禁止する法律もできているが、日本はそういう観点でもまだ進んでいない感触がある。技術ではなく、法制度かもしれないが。

C：WebPKI（Public Key Infrastructure; 公開鍵基盤）などは、ゼロかイチかをはっきりさせている点で、トラストを扱いやすくしている印象がある。

C：トラストは大きく分けると、2値のトラストと、連続値のトラストがあるように思う。トラストチェーンやWeb of Trustは、信頼するかどうかの2値だが、あの人やあのサービスが信頼できるは、連続値のような気がする。後者の信頼は、ゲーム理論などで説明できる気がする。

C：Trusted Web推進協議会[9]でも議論されている。

（サイバーフィジカルシステムにおけるトラスト、トラストチェーン）

C：IoTにおけるリモートアテステーションはとても重要であるが、知らない情報を取っているのではないかなど、プライバシー、セキュリティー的に疑われやすい。リモートアテステーションにいかにトランスペアレンシーを与えられるかが重要な技術的・制度的課題となる。サイバーフィジカルシステムのトラストは、そういったところが大きな課題。法的に何らかの形で、第三者が証明したものがリモートアテステーションに反映されるようになっていくのではないだろうか。

C：リモートアテステーションは、完全性を検証するものと認識している。認められるシステムにするには、ハードウェアや、その検証プロセスやプロトコルも含めて信頼できないといけない。したがって、システムに加えて運用する人までをつなぐトラストの話が重要である。

C：そのとおり。トラストチェーンをいかに切れ目なくできるか、ミッシングピースをいかに埋めるかが大きな課題である。

C：また時間軸で考えた際に、ソフトウェアのアップデートや、起動後のプログラムが関連性が担保されて実行できるかということも大事になってきている。

（国内外のプロジェクト、特にプラットフォーマーによるトラストへの投資）

Q：産業界の動きとして、GAIA-Xを挙げている。これは研究として進めているのではなく、もう産業界として、企業間の契約をデジタル化するために必要だからやっているというふうに捉えている。日本にお

9 Trusted Web推進協議会, https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/index.html

けるそのような実務的なトラストの動きはあるか。また、国内では科研費の取り組みが挙げられている。海外の基礎研究としてのこのようなトラストの研究はどうなっているか。

A：今一番ホットなのは、コンフィデンシャルコンピューティング。そこに対する基礎研究というのは、数年前から進んでいる。

C：アプリケーションレイヤーになると、企業間、マルチステークホルダーで物事を解決する方向に向かっている。 GAIA-Xは、欧州のプロジェクトということがあるかもしれない。例えばアメリカはプラットフォーマーがやればいいと思っているだろう。欧州は違って、弱者連合であっても何とかしなくちゃいけないとなっている。日本も同じかもしれない。

C：プラットフォーマーからすると、クライアント側の仕組みからCPUまで、トラストの機能を持ち込むことによって、トラストのベースラインを上げようとしている。それによって自分たちはより社会受容性が高いサービスが提供できるね、という戦略なのかなと見ていた。

C：そうかもしれない。例えば、マイクロソフトはハードウェアはやっていなかったが、PCに組み込むRoot of Trustとなるチップを自社で設計している。そこを押さえた上で、IoTで重要なキーワードである「オンボーディング」、つまり展開できる仕組みを作ろうとしているように見える。

C：そうなったときに、それでは我々は何を研究したり、何を産業界で取り組まないといけないか。そこをきちんと議論しないといけない。

C：プラットフォーマーにトラストを完全に押さえられてしまうと、彼らの言いなりにならざるを得ないので、代替手段を持つ戦略も必要である。

（その他）

C：トラストやデータ戦略は、科学技術だけでは解決できないのはその通りであると思う。今、自民党の提言、内閣官房 情報通信技術（IT）総合戦略室の検討、総務省の検討がとても早く進んでいるので、社会的な俯瞰は、そちらを注視し必要に応じ関与する方がよい[10]。

C：ブロックチェーン自体ではなく、ブロックチェーンを使ったトラストというのはどうなるか、議論になってもよいだろう。

C：アリペイや芝麻信用など、社会的には話題になっているので、報告書内で触れられるとよい。

10 自民党 政策, https://www.jimin.jp/news/?category=policy&more=1
デジタル・ガバメント閣僚会議, https://www.kantei.go.jp/jp/singi/it2/egov/
Trusted Web 推進協議会, https://www.kantei.go.jp/jp/singi/digitalmarket/trusted_web/index.html
総務省 研究会, https://www.soumu.go.jp/menu_sosiki/kenkyu/kenkyu.html など

2.6 各研究開発領域共通の課題

各研究開発領域共通の課題として、図2-6-1に示す「サプライチェーンリスク」「データ基盤」「産学官連携/分野連携」「人材育成」「法制度との関係」という5つの課題が挙げられる。左には具体的な課題を、右にはそれに対する対策や考え方を紹介している。

これら5つを個別の課題と捉えることもできるが、1つの関連する課題と捉えることもできるだろう。例えば、「サプライチェーンリスク」を取ってみると、デバイスのサプライチェーンだけでなく、「データ・コンテンツのセキュリティー」領域で議論があったように、データにもサプライチェーンが存在している（データ基盤）。システムやサービスまで含めるとかなり多様な問題になってきている。それに対し、「産学官連携/分野連携」「人材育成」「法制度」との関係が共通の課題として関係してくるだろう。

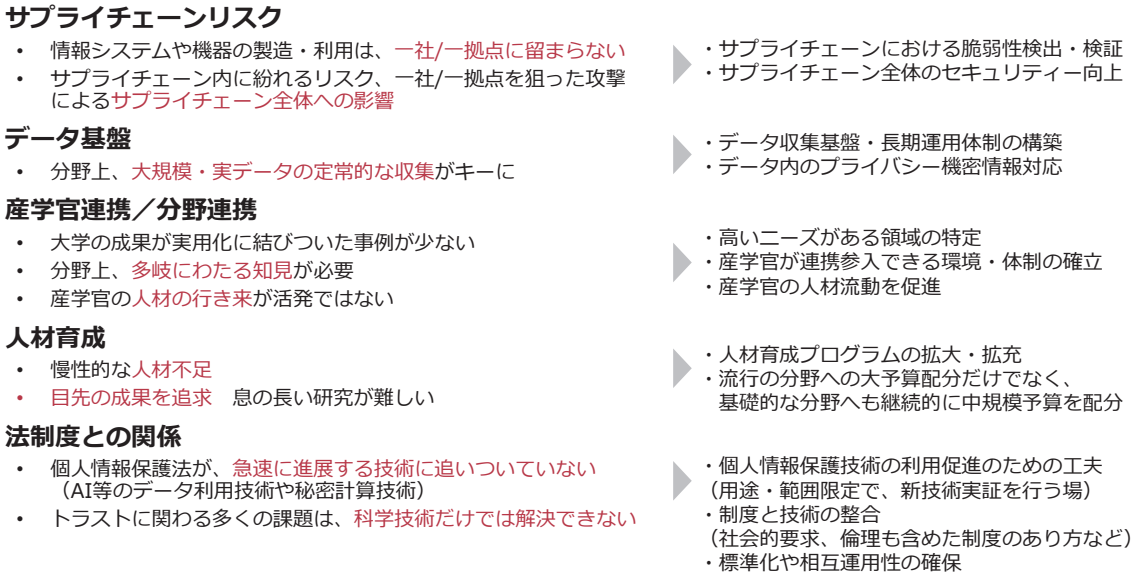


図2-6-1　　各研究開発領域共通の課題

【議論】

（サプライチェーンリスク）

C：サプライチェーンには、オープンソースも入るだろう。

C：オープンソース自体が、本当にオープンソースとしてちゃんと管理されているかどうかという話もある。米国では、ソフトウェア部品表（SBoM：Software Bill of Material）をサプライチェーンで交換しようという議論もある。このあたりは、5G端末や医療機器などで動こうとしている。

米国のソーラーウィンズという事案では、米国政府機関や大手企業がサイバー攻撃を受けた。いまだにニュースで報道されている。ICTシステムの監視システムのソフトウェア・アップデートが汚染されていた。国際関係の問題もあるが、その時の技術的な仕組みだけを見ても課題はありそう。一般の人にとっては、ウィンドウズアップデートが始めから汚染されていたらどうなるか、ということを話すと通じやすい。

IoTで端末の数が莫大に増える中、世界に何十億という端末が汚染される可能性がある。そこまで考えると、とんでもない話になる。ハードウェアセキュリティー、ソフトウェアの仕組み、社会的な仕組み、信用など、全部つながると思う。

（産学官連携/分野連携）

Q：本日全体の議論を聞いていて、技術的にできる部分と、社会の面で考えなければいけない部分があると感じた。最近の研究として、社会科学的な観点に研究開発を向けていく必要があるか。または別のコミュニティーの知見を利用するのがよいか。

A：例えばデジタルトラストについては、従来のトラストの研究者が、これからのデジタル社会自身をイメージすることが難しいのではと思うところがある。最先端の情報技術に関する研究者が、デジタル社会のトラストも見ていく必要がある。制度設計も同様で、どうしても制度が後追いになるのは、情報技術がつくる「ToBe」の姿が分からないことが原因にある。社会的受容性がどうあるべきかも、情報技術を理解した人間がやらないと、イメージもできない。

A：同感である。ただ、両方勉強するのは難しい。研究において、プラスセキュリティーが必要と感じている。制度屋さんや心理学の人、経済学の人にもセキュリティーに興味を持ってもらって、セキュリティー技術者と話ができ、一緒に研究できるような人を増やしていくことが重要。そうしないと全部は見きれない。また境界はない。

C：社会学や心理学などのコミュニティーともうまく接点を結ぶような、そういった営みも今後必要だと理解した。

C：データを持つ企業はデータを出せないケースが少なくない。研究者が、企業の中のデータにアクセスできる人とコラボできるとうまく進む可能性がある。そのためにはデータを使って研究者ができることを提示する方向性も必要である。そうした、産学官共同研究の促進に資するファンドがあると望ましい。

（その他）

JSTには、研究者が研究したいと思える課題の抽出に期待したい。

3 ｜ 議論のまとめ

2章で示した議論をもとに明らかになったポイントや重要な示唆を、以下にまとめる。
（議論の詳細は、2章の各節を参照のこと）

3.1 セキュリティー・トラスト総論、分野全体を通して

【全体のまとめ方】

①アプリケーション側から見たトップダウン的なまとめ方

セキュリティーを構成する要素からのボトムアップ的なまとめ方に加え、アプリケーション側から見たトップダウン的なまとめ方を検討することも有用である。

②新たに追加を検討すべきキーワード・エポック

・デジタルトランスフォーメーション（DX）のセキュリティー
・サイバーセキュリティーにおけるAI活用の歴史

【全研究開発領域にまたがる共通の注目トピック】

①サプライチェーンリスク

共通する課題として、サプライチェーンリスクが挙げられる。社会的な信用にもつながるものであり、世界中でIoT端末が莫大に増える中、注目すべき課題である。

②産学官連携/分野連携

セキュリティーが、政治や経済、社会に及ぼす影響や範囲が拡大している。人文社会科学系の研究者や行政などを含む、幅広い層との連携が重要である。また、実データを持つ企業を巻き込んだ産学官共同研究の促進が望まれる。

3.2 IoT・制御システムセキュリティー

【本研究開発領域のまとめ方】

①具体的なアプリケーション

具体的なアプリケーションについて触れられるとよい。例えば、自動運転車や電車、ドローンなどの「自律走行（オートビークル）」が挙げられる。

②既存のシステムと今後の整理

既存のレガシーな制御システムと、今後の膨大な数のIoTデバイスは、分けて整理した方が分かりやすい。

【特に注目すべきトピック】

③信頼の基点、ハードウェアセキュリティー

サプライチェーン含めて、ハードウェア内部の信頼の基点となるコンポーネントを国内で作り上げることが重要である。また日本は、ハードウェアを基点としたトラストチェーンの構築が弱い。リモートアテステー

ションなどのリモートからの検証技術なども、ハードウェアとセットで検討していくとよい。

②フォレンジック

IoTデバイスの特性上、人間が関わっていない場所に置かれるため、事故などに備えて、何が起きたかを客観的に解析できるようにしておく必要がある。

③強電磁界による意図的な電磁妨害の対策

近年脅威が高まっている攻撃として、強電磁界による意図的な電磁妨害がある。諸外国に比べ、日本では本領域に関する研究があまり進んでおらず、対策が必要である。

④長期に渡るIoTシステムの維持

IoT・制御システムは、稼働する時間軸が長い傾向がある。新旧のデータ処理や、さまざまなデバイスの混載、拡張性や更新など、長期にわたるシステム維持という観点でのセキュリティーも重要である。

⑤スマートフォンのセキュリティー

スマートフォンは金融決済に使われたり、個人情報を多く含むなど、高いセキュリティーが求められる。IoTとスマートフォンではセキュリティー機能が異なるので、分けて考えて取り組んだ方がよい。

3.3 サイバーセキュリティー

【本研究開発領域のまとめ方】

①サイバー攻撃の標的や目的の変化

サイバー攻撃の標的や目的が大きく変化している様子が捉えられるとよい。いたずらや嫌がらせなどの行為が、いまやビジネス化されてきている。攻撃の背後に国家の存在が伺えるケースもある。

②国際比較

欧州のトレンドはもう少し上向きに変更した方がよい。

【特に注目すべきトピック】

①組織間の情報連携

組織間の情報連携は非常に重要で、DXやDFFTを実現する鍵である。この実現のためには、例えば、情報提供側によるセキュリティー・ポリシーの策定・提示や、任意のデータ群にアクセス可能なトラストな研究環境の構築、研究者同士の情報連携（研究コミュニティ活動など）支援などが重要である。

②ヒューマンファクター研究

ソーシャルエンジニアリングや騙しなどを背景として、ヒューマンファクター研究が重要になってきている。エンドユーザーの他、システムの作成・管理・対策を行う者に対しての研究（いかに脆弱性を作り込まないかなど）も重要であるが、日本ではあまり進んでいない。

③サイバー攻撃の連鎖、攻撃の観測に関する研究

ID・パスワードの窃盗などを皮切りに、大きなターゲットへの攻撃につながるという、サイバー攻撃の連鎖が問題になっている。実際のインシデントにどれだけ対応した研究を行えるか（リアルタイムな観測や、プロダクション環境での長期的な観測など）が課題である。

3.4 データ・コンテンツのセキュリティー

【本研究開発領域のまとめ方】

①新たに追加を検討すべきキーワード・エポック

・量子暗号や耐量子コンピューター暗号

【特に注目すべきトピック】

①データの信頼の基点

IoTと同様に、データに関する信頼の基点や、信頼のチェーンが重要である。これを築くためには、制度や仕組みのあり方、標準化、コストなどが課題である。

②セキュリティー・プライバシーを確保したデータの利活用

現実の世界では、膨大な量の正規化されていないスモールデータが散在している状況がある。秘密計算などの技術によってセキュリティー・プライバシーを確保することで、データの利活用を広げることが期待できる。一方、個人情報保護法では、データの性質で個人情報か否かを判別しており、これらのセキュリティー・プライバシー関係技術の活用がグレーであるという課題がある。

3.5 トラスト

【本研究開発領域のまとめ方】

①トラストの要素・位置付け

今回は、社会的な受容性の観点でトラストをまとめている。他の観点として、あらゆるものに対するデジタル証明の付与や遠隔からの検証、デバイスに必要なRoot of Trustの確立、自律化・自動化に必要なFAccT（Fairness, Accountability and Transparency）などの要求やそのための検証などがある。

②新たに追加を検討すべきキーワード・エポック

・ブロックチェーンを使ったトラスト

・アリペイや芝麻信用

【特に注目すべきトピック】

①プラットフォーマーによるトラスト投資の流れ

いまやトラストは競争領域になっている。例えば、GAFAのようなプラットフォーマーが、自分たちのビジネスに即したトラストのモデルを形成しようとしている。そのような中で、何をアカデミアとして研究し、産業界で取り組むべきかは、議論が必要である。

②情報システムやサービス全体のトラストチェーンの構築

情報システムやサービスの信頼を得るためには、それらを運用する人や組織までをつなぐ信頼のチェーンが必要である。法律や制度的な枠組みにより保証を与えることも重要である。

付録

付録1 プログラム

（敬称略）

日時：2021年5月27日（木）9：30～12：00
場所：オンライン開催（Zoom）
主催：国立研究開発法人科学技術振興機構　研究開発戦略センター（CRDS）

9：30～ 9：50	趣旨説明		高島 洋典（JST-CRDS）
	開会挨拶		木村 康則（JST-CRDS）
			後藤 厚宏（情セ大）
9：50～11：45	俯瞰報告書セキュリティー・トラスト分野		
	各説明　5分		井上 眞梨（JST-CRDS）
	各議論　15分		全参加者
	1）　セキュリティー・トラスト総論		
	2-1）IoT・制御システムセキュリティー		
	2-2）サイバーセキュリティー		
	2-3）データ・コンテンツのセキュリティー		
	2-4）トラスト		
	※途中休憩あり		
11：45～12：00	総合討論	ファシリテーター	高島 洋典（JST-CRDS）
	閉会挨拶		木村 康則（JST-CRDS）

付録2 参加者一覧

（敬称略、所属・役職はワークショップ開催日時点のもの）

【招聘有識者】

後藤　厚宏　情報セキュリティ大学院大学 学長・教授
松井　俊浩　情報セキュリティ大学院大学 教授
林　優一　奈良先端科学技術大学院大学先端科学技術研究科 教授
吉岡　克成　横浜国立大学大学院環境情報研究院 准教授
佐久間　淳　筑波大学システム情報系 教授
松本　泰　セコム（株）IS研究所 マネージャー

森　達哉　早稲田大学理工学術院 教授
秋山　満昭　NTTセキュアプラットフォーム研究所 上席特別研究員
荒木　粧子　（株）ソリトンシステムズ ITセキュリティ事業部/Soliton-CSIRTエバンジェリスト
須賀　祐治　（株）インターネットイニシアティブ シニアエンジニア
高橋　健太　（株）日立製作所 主管研究員
永山　翔太　（株）メルカリ R4D（研究開発部門）シニアリサーチャー
本間　尚文　東北大学電気通信研究所 教授
山内　利宏　岡山大学学術研究院自然科学学域 教授
山田　明　（株）KDDI総合研究所 研究マネージャー

【関係府省庁】

上田　光幸　内閣官房 内閣サイバーセキュリティセンター（NISC）内閣参事官
織井　達憲　内閣官房 内閣サイバーセキュリティセンター（NISC）参事官補佐
浦川　隆志　内閣官房 内閣サイバーセキュリティセンター（NISC）参事官補佐
太田　陽基　内閣官房 内閣サイバーセキュリティセンター（NISC）参事官補佐
出口　夏子　文部科学省研究振興局 参事官（情報担当）付 参事官補佐
上村　理　文部科学省研究振興局 参事官（情報担当）付 専門官
齊藤　修啓　文部科学省研究振興局 参事官（情報担当）付 情報科学技術推進官
犬塚　恵美　文部科学省研究振興局 参事官（情報担当）付 係員
柴田　絵美　文部科学省研究振興局 参事官（情報担当）付 係員
塙　敏博　文部科学省研究振興局 計算科学技術推進室 技術参与

その他、JST内部関係者。

ワークショップ企画・報告書編纂メンバー

木村 康則	上席フェロー	（システム・情報科学技術ユニット）
井上 眞梨	フェロー	（システム・情報科学技術ユニット）
高島 洋典	フェロー	（システム・情報科学技術ユニット）

俯瞰ワークショップ報告書 **CRDS-FY2021-WR-02**

セキュリティー・トラスト分野の動向と今後の展望

令和 3 年 9 月　September 2021
ISBN 978-4-88890-758-3

国立研究開発法人科学技術振興機構　研究開発戦略センター
Center for Research and Development Strategy, Japan Science and Technology Agency

〒102-0076 東京都千代田区五番町 7 K's 五番町
電話　03-5214-7481
E-mail crds@jst.go.jp
https://www.jst.go.jp/crds/

本書は著作権法等によって著作権が保護された著作物です。
著作権法で認められた場合を除き、本書の全部又は一部を許可無く複写・複製することを禁じます。
引用を行う際は、必ず出典を記述願います。
This publication is protected by copyright law and international treaties.
No part of this publication may be copied or reproduced in any form or by any means without permission of JST, except to the extent permitted by applicable law.
Any quotations must be appropriately acknowledged.
If you wish to copy, reproduce, display or otherwise use this publication, please contact crds@jst.go.jp.

ISBN 978-4-88890-758-3

FOR THE FUTURE OF
SCIENCE AND
SOCIETY

https://www.jst.go.jp/crds/