2.4 セキュリティー・トラスト

情報システムや情報サービスの安全性を確保するためのセキュリティーと、それら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二つの側面から研究開発動向を俯瞰する。情報システムや情報サービスは進歩・発展を続けており、我々の生活に欠かせない存在になっている。このため、悪意ある第三者の攻撃から情報システムや情報サービスを保護するためのセキュリティー、および人や社会がそれらを安心・信頼して受け入れることができるかというトラストが重要になってきている。

［セキュリティー・トラストの俯瞰図（時系列）］

本区分の時系列の俯瞰図を図2-4-1に示す。この図では、横軸が年代、縦軸が社会への広がりを大まかに表している。通信や制御システムなどインフラが発展し、さまざまなものがつながるようになってきたこと、また多種多様なプラットフォームが登場し人々が利用できるようになってきたこと、さらに社会の中で多岐にわたる情報サービスが展開されてきたことを示している。図中には、その時期に台頭した技術、および攻撃事案やその他のエポックをプロットしている。

通信の流れは、1970年代の専用線を利用したデータ通信から始まる。専用線は、企業や組織におけるコンピューターを直接つなぐ接続方式であり、利用者間でクローズドなデータのやりとりが行われていた。この状況を劇的に変えたのが、インターネットの登場である。ISDN（Integrated Services Digital Network）やケーブルテレビ（CATV）、ADSL（Asymmetric Digital Subscriber Line）などにより、より高速・大容量なインターネット接続が可能になると、オンライン上のコミュニケーションは限りなくオープンなものへと移行していった。2000年代中頃になると、モバイル化の流れが加速していく。3G（第3世代移動通信システ

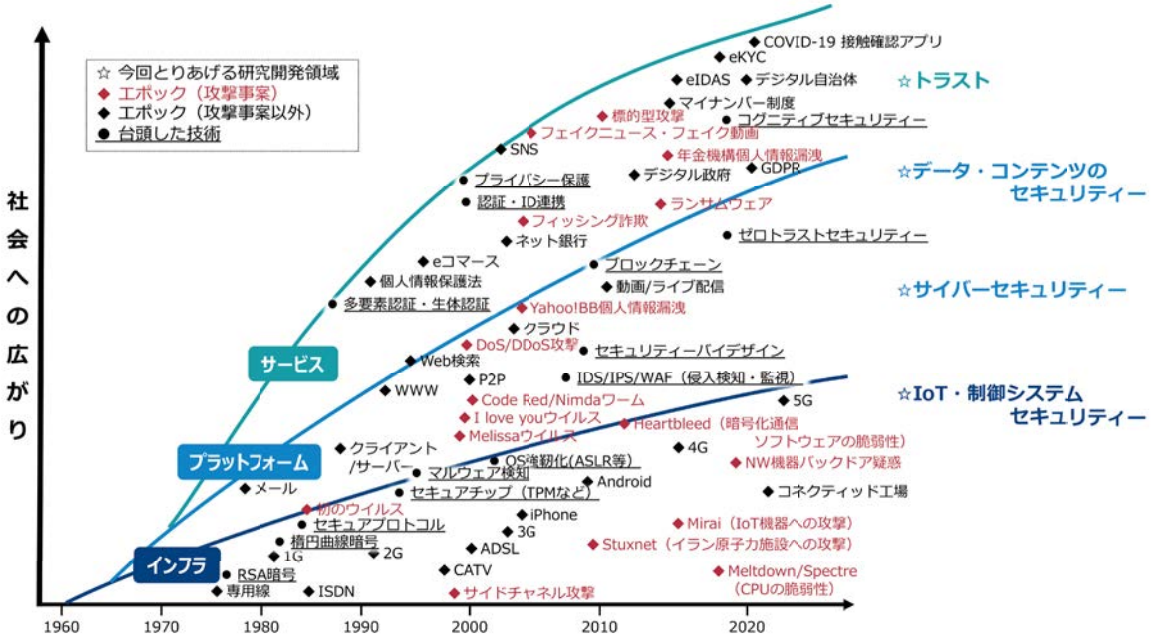

図2-4-1　　セキュリティー・トラストの俯瞰図（時系列）

ム）によって、モバイル端末がコンピューターと同様にインターネットに接続され、さまざまなサービスが利用可能になると、モバイル端末からインターネットにアクセスする利用者が増加した。 iPhoneやAndroidの登場によって、スマートフォンが急速に普及するとともに、モバイル向けの通信規格も4G、そして5Gへと進みつつあり、より高速・大容量な通信がモバイル端末でも実現できるようになった。モノがインターネットの多様なサービスに接続され、相互に情報が交換されるIoT（Internet of Things）も広がりつつある。従来は人やコンピューターがインターネットを介して接続され、情報やサービスを交換してきたが、自動車や家電などの個人の身の回りの物、あるいは電気やガス、交通設備などの社会インフラもネットワークに接続され、あらゆる情報が交換されるようになってきた。また、通信インフラの発展・普及に応じて、電子メールやウェブ検索、クラウド、動画やライブ配信などのプラットフォームや、eコマースやネット銀行、SNS（Social Networking Service）、電子政府などの多様なサービスが登場するようになった。これまでの文字ベースの情報から、画像や映像を含むさまざまな情報のやりとりが可能になり、これによって一方向の情報提供から、双方向のユーザー参加型のコミュニケーションへと、サービスが変遷してきた。インターネットを含むさまざまな情報システムやサービスの利用者は拡大し、同時にセキュリティーやトラストの問題が認識されるようになってきた。

サイバー攻撃は、その目的や手法を変えつつ、社会に大きな被害と影響を与えてきている。マルウェア（不正プログラム）によるウェブサイトやデータの改ざんなど、個人や企業へのいたずら行為として始まった攻撃は、インターネットの普及に伴い深刻化してきた。攻撃の目的は、企業・組織への妨害や、個人情報や金銭の搾取へと悪質化し、攻撃手法もDoS（Denial of Service）・DDoS（Distributed Denial of Service）攻撃や標的型攻撃、フィッシング詐欺など多様化した。近年では、スパイやテロ、国の重要インフラを狙った攻撃など、国家の関与が疑われる組織的な攻撃へと発展している。 IoTや制御システムに対する攻撃は、情報漏えいやプライバシー侵害などにとどまらず、物理的な被害に直結し、時には人命にも大きな被害を与える可能性がある。しかも、ネットワークに接続されるモノの寿命は、これまで接続されてきたコンピューターなどに比べると格段に長くなり、そのセキュリティーの確保は一層困難になりつつある。このような課題に対抗すべく、暗号技術やマルウェアの検知、認証技術をはじめとする、さまざまなセキュリティー技術による強化対策に加え、個人情報保護法などの制度面での対策が同時に進展してきている点も、セキュリティーにおける重要な流れである。

また近年、社会への影響度の点で無視できないのは、情報システムや情報サービスにおける安心・信頼である、トラストである。情報技術がますます高度化し、情報システムや情報サービスへの社会の依存度が高まる中、フェイクニュースによる情報サービスや情報そのものへの不信感や、COVID-19の接触確認アプリによる個人情報漏えいへの懸念や国の監視・管理への不信感など、人々のトラストを揺るがす事態が生じている。情報技術の活用は社会と密接な関係があり、技術的な信用の担保だけではなく、人間の心理的な要素や、制度による保証などもあわせて、多面的に考慮することが重要になってきている。

［セキュリティー・トラストの俯瞰図（構造）］

本区分の俯瞰図（構造）を図2-4-2に示す。この図では、本区分の全体像を、基盤層、情報・システム・デバイス層、人・社会層の3層に分けている。基盤となる領域としては、心理学・経済学・人文社会学、数学・暗号技術・コンピューターサイエンス、教育・人材開発、法制度があり、これらがセキュリティー・トラスト分野において重要なベースとなる役割を果たしている。この土台の上に、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

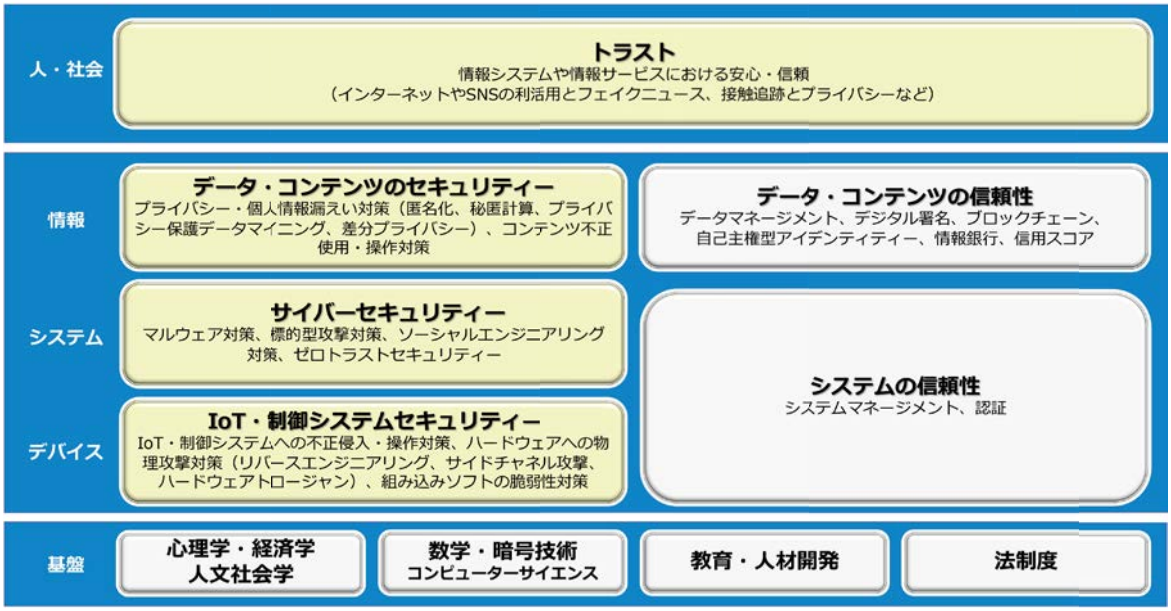

図 2-4-2　　セキュリティー・トラストの俯瞰図（構造）

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づけた。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。最上位の層としては、人・社会との関係に注目する層として、トラストを位置づけた。

本区分においては、以下の❶から❹までを研究開発領域として取り上げる。

❶ IoT・制御システムセキュリティー

パソコンやスマートフォンなどの従来の情報端末に加え、家電、医療、工場・インフラなどの産業用途、自動車・宇宙航空など、更なるIoT化の進展が見込まれている。一方、セキュリティーのリスクは増大しており、ソフトウェアやハードウェア、ネットワークなど、広範かつ縦断的なセキュリティー確保が必要となってきている。

❷ サイバーセキュリティー

インターネットの進歩・発展の影で、インターネットを経由したサイバー攻撃は日々高度化を続けている。一方、既にインターネットは生活や産業など多くの社会活動が依存する社会インフラとなっており、そのサイバー攻撃への対策は、安心・安全な社会を実現する上で必要不可欠である。

❸ データ・コンテンツのセキュリティー

パーソナルデータの活用は、「インターネットにおける新しい石油」とも評され、インターネット経済の発展の鍵となっているが、同時に、欧州を中心にプライバシー保護への要求も高まっている。また近年では、フェイクニュースと呼ばれる悪意を持った情報操作が社会問題化している。データ経済の発展には、セキュリティーやプライバシーの保護とデータ利活用を両立する技術が重要である。

❹ トラスト

近年、情報システムのセキュリティーに加え重要になってきているのが、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「トラスト」である。情報技術がますます高度化し、情報システムや情報サービスへの社会の依存度が高まる中、注目が集まるトラストを、人間の心理、制度、および技術の側面から捉える。

本区分ではとりあげていないが、情報システムや情報サービス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）に関する技術や仕組みも重要である。個別の内容については、ブロックチェーン、および自己主権型アイデンティティー（SSI：Self-Sovereign Identity）は「2.5.7 ブロックチェーン」を、情報銀行、および信用スコアは「2.1.9 社会におけるAI」、および「2.5.5 IoTアーキテクチャー」を参照されたい。

2.4.1 IoT・制御システムセキュリティー

（1）研究開発領域の定義

IoT（Internet of Things）の進展によって、個人利用による情報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である。

（2）キーワード

IoT（Internet of Things）、LPWA（Low Power Wide Area）、信頼の基点、ハードウェアセキュリティー、耐タンパー性、M2M（Machine to Machine）通信、計測セキュリティー、サプライチェーンリスク、ハードウェアトロージャン、サイドチャネル攻撃、意図的な電磁妨害、オフェンシブセキュリティー、サイバーフィジカルシステムセキュリティー、ハードウェアレジリエンス

（3）研究開発領域の概要

［本領域の意義］

ネットワークにつながる機器の台数は年々増加している。パソコンやスマートフォンなどの従来のインターネット接続端末に加え、家電などの電子機器、医療、工場・インフラなどの産業、自動車・宇宙航空など、今後IoT化の大きな進展が見込まれている[1)]。

このように普及するIoTにおいては、サイバー攻撃を受ける可能性がある領域（アタックサーフェース）が拡大している。 IoT機器は、利用目的や環境によって多種多様なソフトウェア・ハードウェアを搭載しているのに加え、接続される通信方式もさまざまである。また、外部との接続を想定していない時代に設計されたレガシーシステムなど、セキュリティー対策が行き届いていない機器も存在している。国立研究開発法人情報通信研究機構（NICT：National Institute of Information and Communications Technology）が発表したNICTER（Network Incident analysis Center for Tactical Emergency Response）観測レポート2019では、NICTERプロジェクトの大規模サイバー攻撃観測網で2019年に観測されたサイバー攻撃関連通信のうち、全体の約半数がIoTのサービスやシステムの脆弱性を狙った攻撃であることが明らかにされており[2)]、当該分野におけるセキュリティー対策の重要性が高まっている。

特に医療、自動車分野などでは、セキュリティー対策の不十分性や欠落が人命を左右する問題に直結し、また電力やガス、水道などの重要インフラシステムにおいては、システムの誤動作や停止などによって、組織、および我々の生活を含む社会全体に強い影響を与えうる。今後のさらなるIoTの進展に向けて、セキュリティー技術の確立が急務といえる。

［研究開発の動向］

❶ IoT・制御システムにおけるセキュリティーリスクの顕在化

IoTセキュリティーの重要性が顕在化したのは、2016年9月に発生した「Mirai」と呼ばれるマルウェアの感染事例である[3), 4)]。感染したIoT機器が一斉に大規模なDDoS（Distributed Denial of Service）攻撃を行ったことにより、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。感染した多くのIoT機器は、デフォルトパスワードや容易に推測可能なパスワードを利用して運用されていることや、デバ

イスの制御がスーパーバイザーモードやルート特権による保護もされていないなどの実情があり、そこを突いて大規模なボットネットによる攻撃を実現したものである。

産業用設備・機器や制御システムにおいては、従来は固有のプラットフォーム、専用ソフトウェア、独自プロトコルで構築され、外部ネットワークと接続しない環境での運用が想定されてきた。しかしながら、近年汎用のプラットフォームや標準プロトコルの採用が進み、さらにメンテナンスや管理などの目的で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。2010年のイラン原子力施設におけるマルウェアStuxnetの感染、2012年のサウジアラビアの石油会社におけるマルウェアShamoonの感染、2015年と2016年のウクライナの電力システムを狙ったサイバー攻撃による大規模停電など、インシデントが多数報告されている。今後ネットワーク接続の拡大とともに脅威の増大が予想され、早急に対策の強化が必要になってきている。

さらに、システムの基盤となるハードウェアへの物理的なアクセスによる攻撃のリスクも高まっている。例えば、LSI（Large Scale Integration）パッケージを開封・加工し、その内部構造や回路動作を解析するリバースエンジニアリングなどの侵襲攻撃、またハードウェア動作中に副次的に生じる物理量を観測して、暗号処理に用いる秘密鍵を盗むサイドチャネル攻撃や、非暗号デバイスに対し内部情報を奪うテンペストなどの非侵襲攻撃がある。近年はこのような攻撃の対象がハードウェア全般に広がっている。

このように、さまざまな機器やシステムがつながることによってセキュリティーのリスクが増大しており、接続するネットワークのセキュリティーや、そこにつながる機器のソフトウェア・ハードウェアのセキュリティーなど、広範かつ縦断的なセキュリティー確保が必要となってきている。加えて、ハードウェアへの物理的な攻撃は、端末のオフライン化では対処できず、脅威を事前に想定した対策が必要となってきている。

❷ 海外・国内政策動向

米国では、オバマ大統領による2013年の大統領令13636号（重要インフラのサイバーセキュリティーの向上）が、当該分野のセキュリティー施策における重要なマイルストーンとなった。当該大統領令を受け、2014年に米国国立標準技術研究所（NIST：National Institute of Standards and Technology）から「重要インフラのサイバーセキュリティーを改善するためのフレームワーク（CSF：Cyber Security Framework）」が発行された。CSFは、業種や企業規模などに依存しない、汎用的・体系的なガイドラインとなっており、現在では重要インフラ分野を超えて、また国を超えて、多くの組織で採用されている[5)]。2018年4月には、CSF Version 1.1へと改訂されている。

我が国においては、重要インフラ分野のセキュリティーについては、内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）から「重要インフラの情報セキュリティ対策に係る第4次行動計画」（2020年1月改訂）や、「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）」（2019年5月改訂）が策定されている。IoTセキュリティーについては、同じくNISCより「安全なIoTセキュリティシステムのためのセキュリティに関する一般的枠組み」が2016年8月に策定、さらに経済産業省や総務省からも政策が積極的に出されている。経済産業省・総務省によるIoT推進コンソーシアムのワーキンググループから2016年7月に発表された「IoTセキュリティガイドラインVer1.0」をはじめ、経済産業省から「サイバー・フィジカル・セキュリティ対策フレームワーク」が2019 年4 月に、「IoTセキュリティ・セーフティ・フレームワーク」が2020年11月に策定された。総務省からは「IoTセキュリティ総合対策」が2017年10月に、その改訂版として「IoT・5Gセキュリティ総合対策2020」が2020年7月に策定された。

その他、国内外ともに、さまざまな民間団体からも当該分野に関するガイドライン資料が発表されている。

❸ 国際標準・規格

国際標準は、国際標準化機構（ISO：International Organization for Standardization）や国際電気標準会議（IEC：International Electrotechnical Commission）、国際電気通信連合電気通信標準化部門（ITU-T：International Telecommunication Union Telecommunication Standardization Sector）などが定めている。情報分野の標準化については、ISOとIECが独立して活動していたが、1987年にISO/IEC JTC1（Joint Technical Committee 1）が設立され、合同で審議されるようになった。ISO/IEC JTC1は、分野毎に42個のSubcommittee（SC）に分かれており、現在は約20のSCが活動している。この中でIoTセキュリティーについて注目すべきは、SC27のセキュリティー関連技術とSC41のIoT関連技術である[6)]。 IoTでつながる設備や機器などの「モノ」までを対象としたセキュリティーの規格が急ピッチで進められている。

セキュリティー認証制度としては、ISO/IEC15408に基づくCC（Common Criteria）認証、制御システムの認証として、IEC62443に基づくCSMS（Cyber Security Management System）認証、およびEDSA（Embedded Device Security Assurance）認証がある。IoTデバイスのセキュリティー認証にはまだ国際的な制度がないが、国内では一般社団法人重要生活機器連携セキュリティ協議会（CCDS：Connected Consumer Device Security Council）が、2019年11月にIoT機器のセキュリティー認証事業を開始している[7)]。

（4）注目動向

［新展開・技術トピックス］

❶ IoT 向け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

パソコンやスマートフォンのOSであるWindows、iOS、Android、Linux に対して、IoT機器では、組み込み用のLinuxや、多様なRTOS（Real Time Operating System）が使われている。 RTOSの開発には長い歴史があるが、IoTの普及に伴って、自動車や産業用の制御システム、医療機器、カメラなどのマルチメディア機器、家電などで利用が拡大しており、IoT向けの新しいOSの研究開発が盛んになっている。一方、IoTシステムに対するサイバー攻撃として、新たにRTOSのリアルタイム制御やRTOSの省電力制御を侵害する攻撃の可能性が高まってきており、対策が急がれている。

❷ ハードウェアトロージャン検出・抑制

IoT機器などのハードウェアメーカーの中には、自社で設計したIC（Integrated Circuit）チップを、サードパーティーのファウンドリーを利用して製造することがある。こうした状況下では、ICチップ製造のサプライチェーンにおいて、チップ設計者が意図しない機能が付加され、ICの破壊やセキュリティーの低下を引き起こす可能性がある。こうした設計者の意図に反して付加される回路は、ハードウェアトロージャン（HT：Hardware Trojan）と呼ばれ、新たなセキュリティーの脅威として早急な対処が必要になっている。近年では、ICや他の素子部品をプリント基板（PCB：Printed Circuit Board）に実装する工程や、PCBを複数接続し機器を組み上げる工程においても、ハードウェアトロージャンが混入する可能性があることが指摘されている[8)]。機器のアセンブリーまで含めた広範な対象に対し、製造過程だけでなく製品出荷後も継続的にハードウェアトロージャンの実装を検知、抑制する技術の開発が求められている。

❸ 意図的な電磁妨害

電磁波による信頼性、およびセキュリティーの低下に関する脅威として、意図的な電磁妨害（IEMI：Intentional Electromagnetic Interference）がある。 IEMIは、機器内部に強制的に電磁界を誘導し、ICや素子を破壊するものであり、IoTシステムの中で、ハードウェア周囲の情報を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デバイスにとっては致命的なダメージを与え得る脅威である。

また、機器を破壊することなく、本来は無線受信機能を有しない電源線や有線通信経路を経由してハードウェアに電磁波を誘導させることで、一時的な故障を引き起こし機器内部の機密性の高い情報を漏えいさせたり、ハードウェア内に任意のコマンドを実行させたりする可能性も示されている。こうした新たな脅威と従来検討されてきたサイドチャネル攻撃やテンペストと組み合わせることで、外界からアクセスできない環境にある機器に対しても、ハードウェアレベルでの攻撃が成立する可能性がある。さらに、ソフトウェア無線、およびその制御ソフトウェアの普及により、従来は高価な計測器を用いなければ困難であった出力電磁波の時間・周波数領域での高精度な制御が容易になったことから、攻撃の敷居が下がっている。

今後、より多くのハードウェアが攻撃対象となる可能性もあり、こうした新たなハードウェアセキュリティーの脅威についても十分な対策を講じていく必要がある。

［注目すべき国内外のプロジェクト］

❶ 戦略的イノベーション創造プログラム（内閣府）

内閣府の戦略的イノベーション創造プログラム（SIP）では、社会実装を強く意識した取り組みが推進されている。当該分野に関しては、第1期SIPにおいて「重要インフラ等におけるサイバーセキュリティの確保（2015～2019年度）」が実施された。

続く第2期SIPにおいては、第1期SIPの技術成果を引き継ぎ、「IoT社会に対応したサイバー・フィジカル・セキュリティ（2018～2022年度）」が実施されている。IoTシステム・サービス、および中小企業を含む大規模サプライチェーン全体を守るサイバーフィジカルセキュリティー対策基盤を開発し、サイバー脅威に対するIoT社会の強靭化が目指されている。第2期SIPでは「信頼の創出・証明」技術として、IoT 機器のなりすまし、およびセンシングデータの改ざんを防止する技術や、IoT 機器上のソフトウェアの完全性・真正性を確認する技術、製造段階での不正機能の混入を確認する技術などの開発が進められている。また、それらの技術を実現する上で鍵となる「信頼の基点」をIoTの末端端末で実現するためのキーデバイスとして、セキュア暗号ユニット（SCU：Secure Cryptographic Unit）の開発も進められ、今後さまざまな産業分野への応用が期待されている。

❷ サイバーフィジカルセキュリティ研究センター（産業技術総合研究所）

2018年11月に国立研究開発法人産業技術総合研究所内に「サイバーフィジカルセキュリティ研究センター」が設立され、サイバー空間とフィジカル空間にまたがり価値を創造する産業基盤のセキュリティーを強化するためのセキュリティー要素技術の開発が進められている。

特に重点的に取り組まれている研究課題として、信頼の基点となるハードウェアのセキュリティー技術の研究開発がある。研究成果を産業分野に広く普及させる取り組みはもちろんのこと、これまで十分な議論がなされていなかったハードウェアセキュリティーを定量的に評価するためのセキュリティー基準の検討が、将来の標準化も見据えながら進められている。本センターを起点とした産学官連携のハードウェアセキュリティー領域の連携の加速と、開発された技術の迅速な社会実装が期待される。

（5）科学技術的課題

❶ 信頼の基点と機器認証

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あり、データの改ざんや機器のなりすましが発生するリスクが高い。従って、IoTシステム全体のセキュリティー確保のためには、耐タンパー性に優れたハードウェアに暗号鍵を保管するなど、IoTシステムの「信頼の基点」の構築が必要である。SIP第2期で開発が進められているセキュア暗号ユニット（SCU）は極小のIoT端末に「信頼の基点」を実現できる技術として期待が高い。

また、IoT機器がネットワークに接続する際に、機器自身に接続権限があることをサーバー側に証明し、またサーバーが真正なサーバーであることをデバイス側で確認できなければならない。そのためには、信頼の基点の上に、機器認証の仕組みを築く必要がある。機器の物理的特性の差を用いた認証方法の他、コンテクスト認証と呼ぶ、機器が置かれた環境の情報で機器を識別する方法も提案されている。

❷ 高いセキュリティーを実現する IoT ネットワークの確立

IoTでは、低消費電力、かつ広範囲の無線通信を可能とするLPWA（Low Power Wide Area）方式が複数提案されている。通信プロトコルとしては、MQTT（Message Queue Telemetry Transport）やCoAP（Constrained Application Protocol）などの、パブリッシャー・サブスクライブ型プロトコルが有力である。この方式では、センサーなどのIoT機器側を「パブリッシャー」、処理を行うサーバー側の機器などを「サブスクライバー」として定義し、その間に「ブローカー」と呼ばれる中継サーバーをおいて通信環境を構築する。これらは、ブローカーを介し、非同期で1対多の通信を確立できるため、多数の機器が接続され、また頻繁に追加／削除されるIoTシステムには適しているものの、不適切な機器が接続されるリスクがあり、他の機器になりすましてデータを送出したり、他のM2M通信を盗聴したり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ネットワーク構成、およびIoTネットワークやプロトコルの脆弱性検査手法の確立が必要である。

❸ セキュリティーのシステム検証方法の確立

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、設計時に脅威分析に基づく対策を講じておく必要がある。システム仕様を論理式で記述し、セキュリティー対策の十分性を客観的に評価する検証方法の確立が望まれている。

❹ 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

これまでのハードウェアセキュリティーの検討は、ハードウェア内部で取り扱われる情報ごとに脅威の分析や対策技術の提案が行われている。一方で、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のメカニズムによって引き起こされている可能性があり、統一的な対策技術が求められる。

例えば、サイドチャネル攻撃やテンペストは「機器の内部から外側への電磁界伝搬により引き起こされる脅威」であり、電磁波を用いた攻撃や意図的な電磁妨害は「機器の外側から内側への電磁界伝搬により引き起こされるセキュリティー低下の脅威」と考えられる。こうしたセキュリティー低下を引き起こす物理現象に着目し、メカニズムを解明することで、多種多様なハードウェアに統一的に適用可能な対策技術となる可

能性がある。また、こうした対策の検討により、強固な新しいセキュリティーが実現できる可能性を秘めている。

❺ 計測データの真正性保証

IoT機器の多くは、搭載されたセンサーを用いて実世界の情報をセンシングし、取得した情報をサイバー空間やローカルで処理し、その結果を実空間にフィードバックすることで挙動を制御している。センサーの収集対象となる情報の多くはアナログデータであり、収集過程においてセンサー内部でデジタルデータに変換され、蓄積・処理される。一方、センサーが計測するアナログデータには従来の認証アルゴリズムの適用は困難なため、計測データの真正性は現状十分保証されていない。また、センサー自体が別物に置き換えられ、収集されるデータが改ざんされる可能性についても十分な考慮がなされていない。IoT機器への攻撃により生ずるセキュリティー低下は、物理空間における事故に直結する可能性があり、計測データの真正性を保証するためのスキームが求められている。また攻撃によって改変された計測データが、後段のソフトウェア処理や学習モデルに与える影響についても検討を進める必要がある。

❻ オフェンシブセキュリティーとハードウェアレジリエンス

現状では、ハードウェアに生ずる脆弱性は、製品出荷後に対策を施すことが難しい。そのため、発見された新たな脅威はリコールの対象となり、企業が受ける経済的な損失は非常に大きい。こうした状況を打破するには、機器の設計時から脅威を想定したセキュリティー対策が求められ、そのためには、攻撃者の立場でシステムや機器の脆弱性を洗い出すオフェンシブセキュリティーが必要である。また同時に、インシデントが発生した後にもその脅威に対して耐性が獲得できるようにするという概念も重要であり、それを実現するためのハードウェアレジリエンス機能の開発・実装が求められる。

（6）その他の課題

❶ サプライチェーンリスク

IoT機器や制御システムの製造、利用は一国に止まらない。現在の電子機器は非常に複雑な構成となっており、ハード系は制御、電子部品、ソフト系はファームウェア、OS、ミドルウェア、アプリケーションプログラムなどに分かれる。これら全てを 一社でまかなうことは不可能であり、多数の会社が連携して一つの部品を構成しているため、その中にセキュリティーリスクが紛れ込む可能性がある。またそれらの機器やシステムは、さまざまな事業者や拠点がつながって運用されており、その中の一社／一拠点を狙った攻撃が、サプライチェーン全体に大規模な損失や閉鎖などの影響を引き起こす危険性がある。国際標準[1]に則って認証された部品やベンダーを使うことや、第2期SIP「IoT社会に対応したサイバー・フィジカル・セキュリティ」の取り組みのように、サプライチェーンにおける脆弱性を検出・検証する方法を確立すること、サプライチェーン全体のセキュリティー対策の一層の向上などが求められる。

1 サプライチェーンの国際標準化動向については、「サプライチェーン全体のサイバーセキュリティ強化に求められる取組の国際標準化動向調査報告書」（2019年3月）に詳しい。
https://www.meti.go.jp/meti_lib/report/H30FY/000453.pdf

❷ 分野連携

当該分野の研究開発を進めるにあたっては、情報系、電気系、物理系など幅広い知識が必要である。情報系に限っても、ソフトウェア、通信方式、ネットワークなどの知識が要求されるし、電気系・物理系では、センサー、アクチュエーター、電子回路、半導体、熱管理、電波干渉などの知識が必要である。これらを全て熟知している人材は少ない。専門家集団の分野横断的な活発な議論や連携が必要である。

（7）国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	○	→	・センサーのセキュリティーで、先導的な研究が進められている。 ・2017年に電子情報通信学会にハードウェアセキュリティ研究会が設立され研究分野に活気がある。
	応用研究・開発	○	↗	・ルネサスエレクトロニクス社のTrusted Secure IP（TSIP）は、堅牢なセキュリティーを実現する信頼の基点として世界的成果である。 ・CCDSが、国内対象であるが、IoTのセキュリティー認証制度を世界に先駆けて開始した。 ・内閣府SIPによって開発された組込み機器対応セキュア暗号ユニットの社会実装が始まっている。 ・産業技術総合研究所にサイバーフィジカルセキュリティ研究センターが設立され、産学官連携体制が構築されつつある。
米国	基礎研究	◎	↗	・DEFCONやBlackhatなどのハッカー向き国際会議での活動が著しい。 ・セキュリティーのトップカンファレンスであるIEEE S&P、USENIX Security、ACM CCSは米国を中心に進んでおり、トップレベルの人材が米国に集まっている。また、こうした研究者によって当該分野の若手の育成も進んでいる。
	応用研究・開発	◎	↗	・IoTのセキュリティー基準に関して、NISTが世界の先導的役割を果たしている。 ・特に自動車分野のセキュリティー技術開発で躍進している。 ・米国内の半導体メーカーでは、設計段階からサイドチャネル攻撃などを含むハードウェアセキュリティーを意識した実装が進められている。
欧州	基礎研究	○	↗	・航空機のIoTでは、エアバスが中心となってシステム検証を取り入れた安全な設計技術研究を進めている。 ・重要社会インフラのハードウェアセキュリティーに関して、意図的な電磁妨害に関する研究が活発に行われてきている。
	応用研究・開発	◎	↗	・ICカードのセキュリティーで先行。 ・IoTにおけるプライバシー保護について、GDPRなどの制度で先行する。 ・CC認証において、ドイツの提案が目立つ。 ・ハードウェアセキュリティー保証スキーム、および意図的な電磁妨害関連の脅威について、標準化が進められている。
中国	基礎研究	○	↗	・米国の研究機関に在籍する中国人や、米国の大学と中国の大学との共同執筆による国際会議論文は多い。 ・過去5年間に出版されたハードウェアセキュリティーの論文数は1位のアメリカに次いで2位であり、基礎研究は加速している印象。
	応用研究・開発	○	↗	・SC41に多数の規格提案を出している。
韓国	基礎研究	△	→	・小数の研究者で研究を遂行している印象であり、分野形成には至っていない。
	応用研究・開発	△	→	・CC認証への提案がある。

（註1）フェーズ

基礎研究：大学・国研などでの基礎研究の範囲

応用研究・開発：技術開発（プロトタイプの開発含む）の範囲

（註2）現状　※日本の現状を基準にした評価ではなく、CRDS の調査・見解による評価

◎：特に顕著な活動・成果が見えている　　○：顕著な活動・成果が見えている

△：顕著な活動・成果が見えていない　　×：特筆すべき活動・成果が見えていない

（註3）トレンド　※ここ1～2年の研究開発水準の変化

↗：上昇傾向、→：現状維持、↘：下降傾向

関連する他の研究開発領域

・MEMS　・センシングデバイス（ナノテク・材料分野　2.3.4）

参考文献

1）総務省『令和2年版情報通信白書』, https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/pdf/02honpen.pdf

2）国立研究開発法人情報通信研究機構サイバーセキュリティ研究所サイバーセキュリティ研究室「NICTER観測レポート 2019」『Technical report』（2020）：1-13, https://www.nict.go.jp/cyber/report/NICTER_report_2019.pdf

3）B. Herzberg, I. Zeifman and D. Bekerman, “Breaking down mirai：An IoT DDoS botnet analysis”, imperv, https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/

4）H. Sinanović and S. Mrdovic, "Analysis of Mirai malicious software", 2017 25th International Conference on Software, Telecommunications and Computer Networks（SoftCOM）, Split（2017）：1-5. doi：10.23919/SOFTCOM.2017.8115504

5）木下翔太郎『「つながる世界」のサイバーリスク・マネジメント「Society 5.0」時代のサプライチェーン戦略』佐々木良一（監修）(東京：東洋経済新報社, 2020）.

6）松井俊浩『IoTセキュリティ技術入門』(東京：日刊工業新聞社, 2020）.

7）一般社団法人重要生活機器連携セキュリティ協議会「CCDSサーティフィケーションプログラムの概要」, https://www.ccds.or.jp/certification/index.html

8）林優一, 川村信一「ハードウェアセキュリティの最新動向：3. ハードウェアトロージャンの脅威と検出」『情報処理』61巻6号（2020）：568-571.

2.4.2 サイバーセキュリティー

（1）研究開発領域の定義

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である。特に、セキュリティーオペレーションを自動化する技術に関する研究開発に主眼があり、各組織へのサイバー攻撃の迅速な検知、インターネット上での脅威状況の把握、マルウェアの分析など、システム管理者やセキュリティーアナリストが実施している業務を強力にバックアップする、もしくは自動化する技術を構築する。近年は、攻撃者の振る舞いや背景の理解、脅威情報の把握、攻撃を受けた際の対応、組織構成員の教育など、より広範囲の対策に資する研究開発が行われるようになってきている。

（2）キーワード

侵入検知、標的型攻撃、ドライブ・バイ・ダウンロード攻撃、DDoS（Distributed Denial of Service）攻撃、マルウェア分析・対策、脅威インテリジェンス、サイバーセキュリティー演習、サイバー攻撃、インシデントレスポンス、脆弱性検知、ゼロトラストセキュリティー、AIとセキュリティー、機械学習、ビッグデータ分析

（3）研究開発領域の概要

［本領域の意義］

インターネットの進歩・発展の陰で、インターネットを経由したサイバー攻撃も日々高度化を続けており、個人、組織、国家に直接的、間接的に影響を及ぼす重大な社会問題となっている。インターネットは既に社会基盤となっており、多くのビジネスが本基盤に依存しているだけでなく、私生活面においてもその依存度は高い。 IoT（Internet of Things）や5Gなどに代表される通信技術の発達を背景に、自動運転や遠隔医療など、さまざまな応用分野の発展が今後見込まれており、これらの発展の基盤にサイバーセキュリティー技術が必須であることは言うまでもない。また個人ユーザーについても、フィッシングによる重要情報の盗取や盗取情報の悪用による不正アクセス、SNS（Social Networking Service）でのアカウント乗っ取り、オンラインバンキングでの不正送金などが問題となっている。サイバー攻撃への対策を継続的に行うことは、安心・安全な社会を実現する上で、必要不可欠といえる。

サイバーセキュリティーは、金銭的な対価を得るための攻撃から、国家を背景とした攻撃まで、その対象範囲は幅広い。産学官の連携、国際連携により対策を進める必要がある。一方、中核となる技術や情報が国際的に共有されることは必ずしも期待できないため、自国内で高い技術水準、情報の蓄積を継続的に行うことが特に重要となっている。

［研究開発の動向］

❶ これまでの研究開発の流れと近年のトレンド

従来、侵入検知やマルウェア（不正プログラム）の解析、検知、駆除などの対策について、さまざまな研究開発が行われてきた。一方、常に新たな攻撃が出現する中、その直接的な対策技術を開発するような対処療法的な対応だけでなく、組織、組織の構成員、システム、システムを構成する機器群、それらの運用、保守体制を含め、多様かつ総合的な対策を行う研究開発へと裾野が広がってきている。

また、サイバーセキュリティーの研究は、ソフトウェアやネットワーク技術、暗号理論などが従来の技術の中心であったが、現在ではその領域は拡大しつつあり、もともとは交わることの薄かった機械学習、自然

言語処理、ハードウェアなどの周辺分野との交わりが積極的になされている。さらに、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、サイバーインシデントが実社会に実害を与えるようなケースも取り扱う必要があり、サイバー社会にさまざまなものが移行してくるにつれ、サイバーセキュリティーが扱う技術領域は今後も拡大傾向にあると考えられる。

❷ 海外・国内政策動向

諸外国の中では、特に米国がサイバーセキュリティー分野の研究開発をリードしている。トランプ前政権では、防衛やサイバーセキュリティーの研究開発に重点が置かれてきた。2017 年には大統領令により、連邦政府としてサイバーセキュリティー・リスクを管理するという基本姿勢を示し、それに続く形でさまざまなサイバーセキュリティー戦略が策定されており[1)]、豊富な研究資金に基づき大小幅広いプロジェクトが継続的に実施されてきた。バイデン新政権のサイバーセキュリティー分野への姿勢にも注目が集まっている。

我が国においては、2014年にサイバーセキュリティー基本法が制定され、サイバーセキュリティー分野における研究開発の重要性が唱えられた。本基本法を受けて、内閣サイバーセキュリティーセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）は、2015年にはじめてのサイバーセキュリティー戦略を策定。日本のサイバーセキュリティーの施策目標や実施方針が示された。2018年に第2回目となる同戦略が策定、2021年に第3回目の戦略が策定される予定である。また、第5期科学技術基本計画でも、サイバーセキュリティー研究開発の重要性が示されている。主なファンディングとして、内閣府が主導する「戦略的イノベーション創造プログラム（SIP）」、「官民研究開発投資拡大プログラム（PRISM）」や、総務省が主導する「電波資源拡大のための研究開発」の中で、実践的な応用研究が進められている。

（4）注目動向

［新展開・技術トピックス］

❶ 大規模、かつユニークなデータ収集を強みとしたビッグデータ分析

サイバーセキュリティーの研究開発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。より大規模かつユニークなデータを収集することにより、他者の追従が困難な研究開発が実施できる。データは、研究開発機関が自ら収集するケースもあるが、大規模な商品・サービス展開を実施している企業から提供されるケースも存在する。

❷ 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

デジタルトランスフォーメーションの進展やCOVID-19の感染対策を契機としたテレワークの急速な普及を背景に、コミュニケーションツールやコラボレーションツールの利用が進み、世界的にビジネスにおけるICT利用形態が大きく変遷してきている。これに伴い、価値のある情報がこれまで以上にネットワーク上を流通し、クラウド内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、これらの新しい技術に対する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これまで以上に活発化する恐れがある。これらに対して、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、およびシステム的側面だけでなく、それを扱う人間の振る舞いの理解、すなわちヒューマンファクターを考慮したセキュリティー研究の重要性が高まっている。

❸ スマートコントラクトに関する研究

ブロックチェーンの応用が進み、さまざまなサービスが開始されるに従い、これに対するサイバー攻撃が行われ、多大な経済的損失をもたらすインシデントも多数発生している。仮想通貨だけでなく、スマートコントラクトなどを利用した多様なサービスが検討されており、その基盤となるシステムやソフトウェアの開発も進んでいるが、これらのシステムにもさまざまな脆弱性が発見され、実際に攻撃により経済的損失が発生している。この対策として、スマートコントラクトのプラットフォームや、その上で動作するプログラムであるスマートコントラクト自体の脆弱性を調査する研究が世界的に活発に行われている。

❹ IoT セキュリティー

近年、脆弱なネットワークカメラやルーターなどのIoT機器を乗っ取り、サービス妨害攻撃に悪用する事例や、大量の通信を送信することにより高負荷をかけてサービスを妨害する事例など、攻撃が大規模化している。IoT機器のセキュリティー対策は、既に広く流通している既存の機器群への対応と、今後開発され、流通することになる将来の機器群のセキュリティー強化という両面があり、どちらも重要な研究要素をもっている。諸外国においてもIoT機器の大量マルウェア感染を契機に、コンシューマーデバイスのセキュリティーの重要性を認識し、各種のガイドラインやセキュリティー要件の策定が進められている[2),3),4)]。

（詳細は、「2.4.1 IoT・制御システムセキュリティー」を参照）

❺ 研究倫理への配慮

研究倫理に配慮することが投稿の条件となっている国際学会が相当数登場している。一般にレベルが高いと思われる学会では特にその傾向が高い。例えば、特定のソフトウェアの脆弱性が発見された際には、その情報をベンダーに報告し、適切な対応を実施したことを明記してから論文投稿することが求められている。同様に、プライバシーにかかわる情報を扱う場合には、研究倫理委員会にて問題がないことを確認するなど、ユーザーのプライバシーに十分配慮した対応がなされていることが分かるような記載を求められる。セキュリティーの研究は、報告することで攻撃者に資する状況を生じてしまう可能性があるが、研究倫理への配慮を徹底することで、そのリスクを最小化する、もしくはリスクよりもメリットの方が格段に大きいことを確認していく潮流ができてきている。これにより、従来はグレー領域と言われて大手を振って発表できなかった研究も適切な形にて発表する土壌が出来つつある。

［注目すべき国内外のプロジェクト］

❶ Web 媒介型攻撃対策技術の実用化に向けた研究開発（NICT）

上述の通り、サイバーセキュリティー領域では、より大規模かつユニークなデータを収集することが競争力の源泉になりうる。 Web媒介型攻撃対策技術の実用化に向けた研究開発（WarpDrive：Web-based Attack Response with Practical and Deployable Research Initiative）は、国立研究開発法人情報通信研究機構（NICT：National Institute of Information and Communications Technology）による委託研究で、複数の研究開発機関が結束し、Webアクセスユーザーのアクセス履歴を日本中の実験参加者から収集し、それを基に研究開発、そして社会展開を実施していくプロジェクトである。本プロジェクトではそのデータを各ユーザーのブラウザー上にて収集するため、単なるアクセス記録だけでなく、そのユーザーがどのようなページ遷移のアクションをとったのかなど、きめ細かな情報が取得できる点がユニークである。サイバーセキュリティーに関する情報を収集し巨大なデータハブを作ろうとする構想であり、本

業界におけるデータ収集の重要性が強く認識されている状況が伺える。

❷ 戦略的イノベーション創造プログラム SIP と官民研究開発投資拡大プログラム PRISM（内閣府）

内閣府が実施している戦略的イノベーション創造プログラム（SIP）と官民研究開発投資拡大プログラム（PRISM）では、社会展開を意識した研究開発が実施されている。令和元年度のPRISMでは、AIを活用したサイバー攻撃対策技術の開発が行われ、SIPの「重要インフラ等におけるサイバーセキュリティの確保」研究と連携し、ICチップの設計回路などに仕込まれた不正回路や不正動作を検知する技術の開発や、大規模なサイバー攻撃につながるマルウェアの初期挙動を検知する技術の開発が行われてきた。このような機械学習を用いたサイバーセキュリティー技術について、実用化を国の研究開発プロジェクトが推し進めている点に注目されたい。

❸ 電波資源拡大のための研究開発（総務省）

総務省が実施している電波資源拡大のための研究開発では、さまざまな研究開発が実施されているが、その中で「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」においては、IoT マルウェア、および関連情報の詳細分析技術の開発を行うとともに、遠隔からの IoT マルウェアの無害化および無機能化を実現するための研究開発が実施されている。本研究の中では機械学習がツールとして用いられることが記されているが、本研究の目的は機械学習技術自体の発展ではなく、最終的にIoT機器のセキュリティー対策を実現することにある。

❹ IoT 機器を悪用したサイバー攻撃防止に向けた注意喚起の取り組み（総務省および NICT）

脆弱なID・パスワード設定などのためサイバー攻撃に悪用されるおそれのあるIoT機器の調査、および当該機器の利用者への注意喚起（NOTICE：National Operation Towards IoT Clean Environment）が、総務省およびNICTによりインターネットプロバイダーと連携して実施されている。NICTの業務に、サイバー攻撃に悪用されるおそれのある機器の調査などを追加（5年間の時限措置）する「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」が2018年11月1日に施行され、法的に問題がない形で上記調査を2019年2月20日より実施している。このような取り組みを実施しなければならないほど脆弱なIoT機器の現状は危機的な状態であり、対策が急がれている。

❺ 米国・NSF によるサイバーセキュリティー研究開発支援

米国のNSFが支援を行うサイバーセキュリティー研究開発プロジェクトの1つに、SPLICE（Security and Privacy in the Lifecycle of IoT for Consumer Environments）プロジェクトがある。このプロジェクトには、ダートマス大学、ジョンズホプキンス大学、モーガン州立大学、タフツ大学、イリノイ大学、メリーランド大学、ミシガン大学が参画し、一般消費者向けのIoT機器のライフサイクルにおけるセキュリティーとプライバシーをテーマとし、主にスマートホームにおける適切なセキュリティー、プライバシーの管理のためのシステムの設計、開発を行うとされている。また、同様にNSFが支援するSecure Constrained Machine Learning for Critical Infrastructure CPSプロジェクトでは、テネシー大学により重要インフラにおけるサイバーフィジカルシステムでの機械学習の利用において想定される、敵対的学習による攻撃への対策を検討するとされている。

❻ 欧州・Horizon2020によるサイバーセキュリティー研究開発支援

欧州ではHorizon2020による研究開発支援が行われている。 Work Programme 2018-2020では、「Secure societies - Protecting freedom and security of Europe and its citizens[5)]」において、さまざまなサイバーセキュリティー研究プロジェクトが支援を受けている。この中では、例えば「Cybersecurity preparedness - cyber range、simulation and economics」において、5Gの仮想サイバーレンジ、航空、海事、およびスマートグリッド環境のシミュレーションに関するプロジェクトが採択され、研究を進めている。「Prevention、detection、response and mitigation of combined physical and cyber threats to critical infrastructure in Europe」では、地下鉄や鉄道、航空宇宙、ガスといった重要インフラにおけるセキュリティー研究プロジェクトが多数支援されており、テストベッドによるセキュリティー検証、サイバー攻撃への耐性や回復力を高める技術などが検討されている。また「Artificial Intelligence and security：providing a balanced assessment of opportunities and challenges for Law Enforcement in Europe」では、人工知能によるテロや、サイバー攻撃への防御や対応に関するプロジェクトが進められている。

（5）科学技術的課題

❶ インターネットレベルでのセキュリティー対策技術

・大規模感染型マルウェア対策技術

大規模感染型マルウェアは、インターネット上で依然猛威を振るっている。近年では、Windows端末だけではなく、Linux組み込み機器であるブロードバンドルーターやWebカメラなどのIoT機器がマルウェアに感染する事例も多くみられる。大規模感染型マルウェア対策技術として、大規模ネットワーク観測・分析の高度化と、その観測結果を活用した対策技術の開発が重要となっている。また、組み込み機器やモバイル機器に感染するマルウェアを想定した新しいハニーポット技術の確立も課題となっている。

・DDoS攻撃対策技術

特定のサーバーに通信を集中させ、外部からのアクセスを不能にするDDoS（Distributed Denial of Service）攻撃への対処は、サービス提供者や通信事業者にとって依然として重要な課題となっている。2013年初頭からDDoSツールやボットネットを利用した従来型のDDoS攻撃に加え、DNS（Domain Name System）やNTP（Network Time Protocol）などによる通信の増幅を悪用した、反射型分散サービス妨害（DRDoS：Distributed Reflection Denial of Service）攻撃が台頭しており、対策を一層困難にしている。 DDoS攻撃対策技術として、攻撃観測用ハニーポット技術、大規模ネットワーク観測技術、さらにそれらと被害サーバー側のDDoS攻撃観測情報を用いたDDoS攻撃の予測・早期検知・早期対策技術の確立が重要となっている。

・マルウェア分析技術

膨大な亜種マルウェアや解析回避機能を有するマルウェアの出現によって、シグネチャーベースのマルウェア検知手法の効果が低下している。マルウェア対策技術として、サンドボックス解析技術の高度化や、カーネルモードで動作するマルウェアの解析技術、マルウェアの長期動的解析技術、マルウェアの解析回避機能への対策技術の確立が求められている。また、組み込み機器やモバイル機器に感染するマルウェアの収集・解析技術の確立も重要となっている。

❷ Web セキュリティー技術

・ドライブ・バイ・ダウンロード攻撃対策技術

Webを介した攻撃であるドライブ・バイ・ダウンロード（DBD: Drive-by Download）攻撃は、ハニーポットなどの受動的観測では捉えられない攻撃である。 DBD攻撃に加担する悪性サイトをWebクローリングで検知する取り組みもあるが、クローリングのシード選択の問題や、数時間で生滅する悪性サイトを捉えられないなど、問題が多い。 DBD攻撃対策技術として、ユーザーのWebブラウザーや組織のWebプロキシーなどを観測点として取り込んだ大規模観測・分析技術の確立が必要となっている。

・ソーシャルエンジニアリング対策技術

ソーシャルエンジニアリング攻撃は、機密情報の公開やソフトウェアのダウンロードなど、閲覧者をだまして危険な行為に誘導する。ソーシャルエンジニアリングコンテンツが含まれるページを検知する技術として、URL名を分析する技術、コンテンツ自体を分析する技術など、さまざまなものが検討されてきている。

・マイニングウイルスの対策技術

感染することで自分のコンピューターが攻撃者のために仮想通貨のマイニングを実施してしまうマイニングウイルスは、多くの場合、不正なウェブサイトに仕組まれており、サイトを訪問すると感染する。また感染しなくとも、特定のページを閲覧している間だけ、ユーザーのリソースを利用したマイニングが実施されるものもある。このようなプログラムには、コインマイナーやCoinHiveなど、さまざまなものが存在するが、これらが仕組まれたサイトに対する対策技術の確立が重要となる。

❸ 組織の枠を超えた情報連携技術

・サイバー攻撃情報共有技術

サイバー攻撃は容易に国境を跨いで行われる。従って、サイバー攻撃対策には国際的なサイバー攻撃情報の共有が有効であり、脅威の源泉となっている攻撃者や攻撃グループの背景の把握、これらの脅威情報の収集、蓄積が重要である。しかし、多くの場合、人手による情報共有が主流となっており、また機微な情報の共有は困難となっている。サイバー攻撃情報共有技術として、サイバー攻撃に関連した情報のグローバルなリポジトリーの構築（そのためのサイバー脅威の記述方法や共有手順の統一、国際標準化）、機微情報のサニタイズ技術、高速な検索技術、異なる攻撃キャンペーン間の相関分析技術などの確立が重要となっている。

・脅威インテリジェンスの生成・活用技術

効率的なセキュリティー対策を実施するために、脅威インテリジェンスの重要性がこの数年間主張されてきている。脅威インテリジェンスとは、攻撃者の意図や目的、攻撃パターンなど、さまざまな情報を収集・分析して得た知見であり、これをもとにサイバー攻撃への効果的な対策を打つことが期待できる。しかしながら、そのインテリジェンスが有効に活用できていない現状が指摘され始めてきており、これらのインテリジェンスを活用したセキュリティー対策の自動化の研究の発展が求められている。また、インテリジェンス自体を自動生成する技術も検討されてきており、特に、ソーシャルメディアなどのWeb上の情報ソースを用いて自動的にインテリジェンスを抽出する技術などもその確立が望まれている。

❹ 各組織の中のセキュリティー対策能力を向上する技術

・標的型攻撃対策技術

標的型攻撃とは、特定組織をターゲットとした長期にわたる執拗な攻撃である。典型的な標的型攻撃では、周到に準備された電子メールに添付されたマルウェアが、組織内に侵入する。標的型攻撃では従来型の境界防御技術（入口対策、出口対策）が有効に働かないケースも多い。従って、標的型攻撃対策技術として、組織内部の観測・分析・検知技術（内部対策）の確立が重要となっている。さらに、組織内のログマネージメント技術や、インシデント発生後のフォレンジック技術の高度化も必要となっている。

・アラート対応疲れへの対応

SIEM（Security Information and Event Management）機器を導入することで、異常を検知しやすくなるが、これらの機器が生成するアラートを人間のオペレーターは検証する必要がある。その検証作業に非常に多くの時間を要するため、オペレーターが疲弊するという「アラート対応疲れ」という問題が近年指摘されてきている。これらの問題に対応すべく、喫緊にアクションが必要なアラートのみを抽出する技術が求められている。

❺ サイバー攻撃可視化技術

サイバー攻撃は元来不可視であるが故に検知や防御が難しく、また対策の重要性を組織のトップマネージメントが正しく理解することを阻んでいる。サイバー攻撃可視化技術はセキュリティーオペレーションの迅速化・効率化や、トップマネージメント層を含めたセキュリティーアウェアネスの向上を図る上で重要となっている。

（6）その他の課題

❶ 有用なデータ基盤の構築

サイバーセキュリティーは「データオリエンテッド」な研究分野であり、研究の成否は、いかに大規模な“実データ”を定常的に収集できるかにかかっていると言っても過言ではない。実データを定常的に収集するためには、収集技術の開発のみならず、システムの安定稼働や長期運用体制の構築、関係組織（例えば大学の場合は学内情報センター）との折衝など、人的コストの非常に高い作業を継続的に行う必要があり、有用なデータの収集が始まるまでに数年単位の時間を費やす事も珍しくない。研究の材料となるデータ内にユーザープライバシーや機密情報が含まれる可能性もあり、さらに入手を困難にしている[6)]。

一方、わが国においては公的な競争的資金は数年程度の年限で設定されており、大規模なデータ収集基盤の構築に多くの時間を割くことが難しく、そのためオリジナルな“実データ”を用いた研究環境を構築できている国内大学は数えるほどしか存在しない。また、公的な競争的資金では研究の新規性やデマケーション（他の研究との差別化）が重視されるため、既に構築したデータ収集基盤の長期運用という重要な項目に予算計上することが難しい。

❷ 産学連携

サイバーセキュリティーは実践的な研究分野であり、常に実用化を目指した研究開発が重要である。米国の例をみると、ミシガン大学の研究グループが設立したArbor Networks社（DDoS対策製品でトップシェアー）や、カリフォルニア大学サンタバーバラ校などの研究グループが設立したLastline社（標的型攻撃

対策製品に強み。2020年VMware社が買収）など、大学の学術研究が実用化に直結している。さらに、それら企業の製品が集めた実データを学術研究にフィードバックすることで、新たな研究を生み出しており、実データを中心とした研究のライフサイクルが確立している。日本では、サイバーセキュリティー分野において国内大学の研究成果が実際の製品やサービスに結びついた例はほぼ皆無であり、産業界と学術界の間で大きなギャップが存在している。今後、日本国内でも実現可能な産学連携の方策を模索するべきである。

また、サイバーセキュリティー分野は、既に顕在化している、または、その兆候が表れている問題を対象にする傾向が強いため、研究トピックの変遷、研究開発された技術の陳腐化が早く、普遍的な科学技術、学問分野としての蓄積が難しい。今後の社会的、技術的な動向の予測に従い、サイバーセキュリティーの観点で高いニーズが予想される領域を特定し、産学連携で研究者が参入できる環境・体制を確立することで、国際競争力をつけることが重要といえる。

さらに、サイバーセキュリティーにおいては、分野横断の学際的研究が重要である。既に取り組みが始まっている「サイバーセキュリティー × 経済学・経営学」、「サイバーセキュリティー×心理学」、「サイバーセキュリティー×金融工学」など、広い視点からの産学連携・学際連携が期待される。

❸ ファンディング

日本の公的な研究資金ではデマケーションが重要視されるため、類似の研究課題に関して複数の研究グループが研究資金を獲得して同時並行的に研究開発を進めることは、ほぼ起こり得ない（そして、研究資金獲得後は競争が発生しない）。米国では、前述の通り複数の省庁がサイバーセキュリティーに関する研究予算を計上しており、その全体調整はNITRD（The Networking and Information Technology Research and Development）が受け持っているが、省庁間のデマケーションを行うのではなく、ある程度の重複は許容しつつ、年度ごとの評価を厳正に行い、高い研究成果を上げている研究グループが生き残る仕組み（つまり資金獲得後の競争の仕組み）を構築している。そのために、研究資金提供側の組織も各分野の専門家を擁しており、技術的な評価を行える体制を敷いている。

❹ 人材育成

サイバーセキュリティーの研究開発の現場では、慢性的な人材不足に悩まされている。我が国では「（文科省）成長分野を支える情報技術人材の育成拠点の形成（enPiT）」のセキュリティー分野の取り組みなどの人材育成プログラムが実施されているが、さらなる拡大・拡充が必要である。セキュリティーは、機械学習やネットワーク技術、自然言語処理などさまざまな分野と隣接・重複しており、必然的に人材の獲得競争率が上昇する。また、セキュリティーはその性質上、誰にでも仕事を任せられるものではなく、例えば海外の人材を無条件で採用するのは難しい。さらには、国内におけるサイバーセキュリティー関係の職種の給与水準は欧米と比べて未だに見劣りするのが現状である。国や自治体が、自らセキュリティー人材の処遇改善をリードする施策も重要である。

海外では、産業界での経験を活かして学術界で活躍するケースや、逆に学術界の研究成果を基に産業界に進出するケースが見られる。実用性が高く実務経験が重要となるサイバーセキュリティー分野においては、このような人材の流動性があることが望ましい。また、米国標準技術研究所（NIST：National Institute of Standards and Technology）が国家サイバーセキュリティー教育イニシアチブ（NICE：National Initiative for Cybersecurity Education）の下で資金提供をするとともに、2020年2月にはサイバーセキュリティー人材育成のためのベストプラクティスを共有するなどの取り組みを行っている[7)]。我が国において

も、人材流動や人材育成を促進するためのキャリアパス支援、セキュリティー産業育成が必要である。

（7）国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	○	↗	・国内シンポジウムなどでの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大学、企業とも増加傾向にある。一方、著名な国際会議での発表件数は多くはないものの、ここ数年、着実に伸びてきている。従来は海外の研究機関の共著という形で採録されているものが時々存在していた程度であったが、直近ではNDSS 2020、USENIX 2020、RAID 2020にて、それぞれ早稲田大学、電気通信大学、情報通信研究機構にて、日本人が主著の研究論文がそれぞれ採録されるなど、国際的な成果も伸びつつある。
	応用研究・開発	○	→	・内閣府が主導する「官民研究開発投資拡大プログラム（PRISM）」、総務省が主導する「電波資源拡大のための研究開発」の中で、実践的な応用研究が進められている。 ・日本最大規模のサイバー攻撃観測・分析・対策システムNICTERを中心とした研究開発を推進しており、特にそのリアルタイム分析・可視化技術は世界をリードしている。 ・国産のセキュリティー製品は非常に少なく、大部分を海外ベンダーに依存している。大手企業の多くも、海外製品のSI業に徹しており、自社製品が普及している例は少ないものの、FFRI社のアンチウイルス製品（Yarai）など、国産製品の普及が徐々に進んでいる事例が出て来ている。 ・情報通信研究機構が開発した対サイバー攻撃アラートシステムDAEDALUSは、クルウィット社により商用サービス化（SiteVisor）されるなど、公的機関の研究開発が産業化される事例も出て来ている。
米国	基礎研究	◎	→	・米国の大学・公的研究機関による基礎研究レベルは非常に高く、著名な国際会議でのプレゼンスも高い。 ・NSF、DoD、DHSなどからの豊富な研究資金に基づく大小のプロジェクトが継続的に実施されている。 ・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を目指した応用研究であるものが多く、ミシガン大学発祥のArbor Networksや、カリフォルニア大学サンタバーバラ校発祥のLastline社など、起業につながっている例も多い。 ・Palo Alto Networks（ファイアウォール）、Sourcefire（IDS）、FireEye（サンドボックス）などのセキュリティー企業による製品や、CiscoやJUNIPER NETWORKSなどのネットワーク機器ベンダーによる製品など、セキュリティー市場における支配的立場にある。 ・巨大IT企業から大手セキュリティー企業、通信機器メーカー、スタートアップ[8)]までさまざまな規模で製品やサービスを展開している。
欧州	基礎研究	○	→	・ウィーン工科大学（オーストリア）やEurecom Institute（フランス）など、マルウェア解析技術やサイバー攻撃観測技術などで高い研究成果を上げている。 ・一方で、優秀な研究者が米国などの研究機関に移籍する事例も多く、研究人材の確保は容易ではないように伺える。

	応用研究・開発	○	↗	・全欧州規模で実施される、研究及び革新的開発を促進するための欧州研究Horizon 2020が2014-2020にて実施されている。セキュリティーは7つの社会的課題の1つにあげられている。その後続であるHorizon Europeでは、Horizon 2020を上回る予算規模となる見通しであり、応用研究はさらに進むものと思われる。 ・Kaspersky（ロシア）、F-Secure（フィンランド）、Sophos（イギリス）、Panda Security（スペイン）、Avast（チェコ）、ESET（スロバキア）など、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、アンチウイルスやセキュリティー製品で国際的に高いシェアを有している。
中国	基礎研究	◎	↗	・中国国内のトップクラスの大学の学生が米国などに留学し、研究成果を上げており、近年では中国国内の研究機関における研究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	△	↗	・これまで国際的に注目される大規模研究プロジェクトは公表されているレベルでは見られない。 ・アンチウイルスなどの国内ベンダーのうち、国際的な普及を果たしている著名なものは存在しない。 ・Huaweiなど通信産業で世界をリードする技術を示し、Qihoo 360など国内向けのセキュリティー産業も成長してきている。
韓国	基礎研究	○	→	・KAISTやPOSTECHなどのトップクラスの大学の研究成果が、ACM CCSやNDSSなどの著名な国際会議に採録されるなど、基礎研究の国際的な評価は上がりつつある。
	応用研究・開発	○	→	・国家的なセキュリティーインシデントを多数経験しており、政府主導のセキュリティー対策を実践している。 ・KISA、ETRI、KISTIといった公的機関が、サイバーセキュリティー技術の研究開発や、モニタリング、インシデント対応を行っており、特に政府機関に導入されているセキュリティー機器は100%国産と言われている。

（註1）フェーズ

基礎研究：大学・国研などでの基礎研究の範囲

応用研究・開発：技術開発（プロトタイプの開発含む）の範囲

（註2）現状　※日本の現状を基準にした評価ではなく、CRDS の調査・見解による評価

◎：特に顕著な活動・成果が見えている　　○：顕著な活動・成果が見えている

△：顕著な活動・成果が見えていない　　×：特筆すべき活動・成果が見えていない

（註3）トレンド　※ここ1～2年の研究開発水準の変化

↗：上昇傾向、→：現状維持、↘：下降傾向

参考文献

1）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『研究開発の俯瞰報告書　主要国の研究開発戦略（2020年）』（CRDS-FY2019-FR-02）（2020）.

2）Federal Office for Information Security, “BSI TR-03148：Secure Broadband Routers Version 1.1：Requirements for secure Broadband Routers”, Federal Office for Information Security, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03148/TR03148.pdf?__blob=publicationFile&v=2

3）European Telecommunications Standards Institute（ETSI）, “CYBER; Cyber Security for Consumer Internet of Things”, ETSI European Standard（EN）303 645, https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf

4）Michael Fagan et al., “Foundational Cybersecurity Activities for IoT Device Manufacturers”, NIST Interagency/Internal Report（NISTIR）8259（2020）：1-36, https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf
5）European Commission, “Horizon2020, Work Programme 2018-2020, 14. Secure societies - Protecting freedom and security of Europe and its citizens”, European Commission Decision C 1862, https://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-security_en.pdf
6）Muwei Zheng et al., “Cybersecurity Research Datasets：Taxonomy and Empirical Analysis”, Proceedings of the 11th USENIX Conference on Cyber Security Experimentation and Test（2018）：1-8, https://tylermoore.utulsa.edu/cset18.pdf
7）Dwight Weingarten, ”NIST Releases Roadmap on How to Build Cybersecurity Workforce”, MeriTalk, https://www.meritalk.com/articles/nist-releases-roadmap-on-how-to-build-cybersecurity-workforce/
8）Louis Columbus, “The 20 Best Cybersecurity Startups To Watch In 2020”, Forbes, https://www.forbes.com/sites/louiscolumbus/2020/06/08/the-20-best-cybersecurity-startups-to-watch-in-2020/#3b202dec7130

2.4.3 データ・コンテンツのセキュリティー

（1）研究開発領域の定義

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である。第三者の攻撃からの保護であるセキュリティーに対し、プライバシーは他人に知られたくない私事でありそれをコントロールする基本的人権である。情報自体の保護に加え、その適正な取り扱いも重要である。セキュリティー・プライバシー保護対策の代表的な技術には、①個人を識別不能にする匿名化技術、②プライベートなデータを暗号化したままで任意の計算を実行する秘匿計算技術、③プライバシーを保護した上でデータマイニングを実施する技術、④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差分プライバシー技術がある。

（2）キーワード

匿名化、秘匿計算、秘密計算、プライバシー保護データマイニング、差分プライバシー、準同型暗号、秘密分散、秘匿回路計算、コグニティブセキュリティー

（3）研究開発領域の概要

［本領域の意義］

「パーソナルデータは、インターネットにおける新しい石油である」と評されるように、パーソナルデータの活用はインターネット経済の発展における中心的役割を果たす。その一方で、データ活用におけるプライバシー保護への要求は、欧州連合における一般データ保護規則（GDPR：General Data Protection Regulation）の適用開始を契機に高まる一方である。データ活用とプライバシー保護は、相反する方向に作用するデータ経済の両輪であり、データ活用を妨げないセキュリティー、およびプライバシー保護技術の確立は、データ経済の発展に不可欠な技術的課題である。

［研究開発の動向］

❶ これまでの研究開発の流れとトレンド

多くの企業が顧客の情報や購買履歴などを管理して、ビジネスに活用する動きが加速している。いわゆるビッグデータと呼ばれる、大規模で機械的に収集される多量のデータが、あらゆる分野で注目を集めている。その一方で、データの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た。例えば、アクセス制限の不備によって約450万人分ものYahoo! BB登録者の個人情報が漏えいした2004年の事件や、日本年金機構に対し外部からの標的型攻撃メールが送られ、年金管理システムに保管されていた125万人分の個人情報が漏えいしたという2015年の事件が記憶に新しい。2019年には、2億6,700万人以上のFacebookユーザーのユーザーID、電話番号、名前が、パスワードやその他の認証なしにオンライン上で閲覧可能な状態に置かれていたとの報告[1)]があった。さらに近年では、技術の発展によって膨大な情報が非常に速いスピードで拡散されるようになった結果、フェイクニュースやフェイク動画と呼ばれる、悪意・扇動意識を持った思考誘導の情報操作が起きるようになり、社会的な問題になってきている。

このようなデータ・コンテンツへのセキュリティー・プライバシー保護対策のため、取り組まれている代表的な技術として、匿名化技術、秘匿計算（秘密計算と呼ばれることもある）技術、プライバシー保護データマイニング技術、および差分プライバシー技術について紹介する。なお、フェイクニュースやフェイク動画

に関する動向や対策については、「2.1.5 意思決定・合意形成支援」も参照されたい。

・匿名化技術

匿名化技術は、データとデータ主体（あるいは所有者）との間の相関を取り除く技術である。パーソナルデータの収集において、姓名などの識別子を削除しただけでは、上記の相関は完全には取り除けず、他の属性情報・履歴情報を束ねて見ることで個人が特定され得るリスクがある。このようなリスクを定式化し、低減するための考え方として k-匿名性[2)] がよく知られている。具体的には、表形式データについて、パーソナルデータの属性値の組み合わせが同じであるデータが、パーソナルデータ集合中に k 個以上存在している状態が、k-匿名性が成立した状態である。データの正確性は犠牲になるが、パーソナルデータを改変することで、k-匿名性を成立させ、個人特定を困難にする。その後、k-匿名性を基礎概念として、匿名化対象を表形式データからグラフや時系列データに拡張する研究や、k-匿名性モデルにおいて十分にプライバシーを保護できない状況下におけるより強力な匿名性定義の研究などが進められてきた（l-多様性、t-近似性など）。個人情報保護法による匿名加工情報の実装において実務上重要な技術である。

・秘匿計算技術

秘匿計算（マルチパーティー・コンピュテーション， MPC：Multi-Party Computation）技術は、互いに開示できない情報を持つ複数のグループが、それらの情報を利用した計算について、計算結果以外の情報を一切開示することなく、計算可能にする技術である。安全な秘匿計算のためのプロトコルは、1980年代から研究が開始された。近年では、理論的には成熟しつつあり、実用的な時間で動作する秘匿計算を実行するための汎用コンパイラーが開発され、専門家でなくても秘匿計算を利用したシステム開発を行うことが可能になりつつある。代表的なシステムソフトウェアには、EMP-toolkit、Obliv-C、ObliVM、SCALE-MAMBA（SPDZ）、Sharemind、ABYなどが知られる[3)]。また、秘匿計算の応用事例も徐々に登場している。例えば閾値暗号は、秘密鍵を複数の情報に分割し、暗号上の操作（復号や署名など）の分散実行を可能にする暗号であるが、この鍵情報の保管に秘匿計算を利用することで鍵の盗難や流出に対するリスクを低減する技術の実用化への取り組みが盛んである。暗号通貨の署名鍵の保護にも同様の手法の利用が期待され、具体的にはUnbound Tech.[4)]、Sepior[5)]、Curv[6)] などのセキュリティー企業の取り組みがある。

・プライバシー保護データマイニング技術

プライバシー保護データマイニング（PPDM：Privacy Preserving Data Mining）技術は、利用者のプライバシーを保護しながらビッグデータの活用を実現する技術である。

PPDM研究の原点は、2000年に発表された二つの同名の論文「Privacy Preserving Data Mining」である。一つは、公開鍵と秘密鍵のペアからなる公開鍵暗号方式を用いる暗号学的アプローチによるもの[7)]で、もう一方はランダムなデータを入力に加えてマイニング処理を行うランダム化アプローチによるもの[8)]であった。両論文のアプローチは異なるが、対象は両者ともプライバシー保護を考慮した決定木学習（与えられたデータから決定木と呼ばれる木構造のグラフを生成する手法）を実行するものであったことは、興味深い事実として知られる。この二つの論文を出発点として、PPDMに関して盛んに研究が行われるようになった。

PPDMの主な要素技術としては、暗号化したまま加算や乗算の演算が可能な準同型暗号があり、加算

が可能なPaillier暗号[9]や乗算が可能なRSA暗号[10]が知られる。これらの要素技術の研究開発や安全性評価は2000年代にはほぼ完成していて実現可能性は確認されているが、暗号化にかかる計算コストが大きく、広い実用化のレベルには至っていない。この技術的な困難さを改良するために、加法、乗法の両方の演算が可能な完全準同型暗号などの暗号要素技術の改良が重ねられている。

・差分プライバシー技術

差分プライバシー技術は、データ収集者が信頼できる場合に、データ収集者が公開した統計情報から個人に関する情報が推測されることを防ぐ技術である[11]。ただし、（3）❶に記載したFacebookの事例が示すように、多額のセキュリティー投資をしているプラットフォーマーでさえも、完全に信頼できるとはいえない。この問題を解決するために、個人がデータを提供する際にプライバシー保護処理を行い、その個人に関する情報が推測されることを防ぐことを保証する、局所差分プライバシー（LDP：Local Differential Privacy）が提案されるようになった[12]。

基本的な統計処理の流れを考える。データは個人が保持しており、そのデータを個人から収集者へ提供する。収集者は収集した個人データに対して統計処理を行い、それを解析者へ公開する。この流れの中で、差分プライバシーにおいては、収集者が解析結果を解析者に公開するときに個人データが漏えいしないようにプライバシー保護処理を行う。ただ、収集者は生の個人データを閲覧することができるため、個人が収集者を信頼できる必要がある。一方、局所差分プライバシーでは、個人がデータを提供する際、つまり収集者が個人データを収集する際にプライバシー保護処理を行い、個人のデータが漏えいしないようにする。従って、信頼できない収集者に対する個人データの漏えいも防ぐことができる。

このように、局所差分プライバシーでは、個人から収集者への提供データにノイズを加えて、元のデータが推測できないようにするとともに、収集者はノイズが入った提供データを用いて所望の統計処理を行う。従って、データセット全体で見たときには、差分プライバシーと比べて多くのノイズが加えられるため、実用性が低下しやすく、適用範囲が広いとはいえない。しかし、仕組みの単純さとプライバシー保証の強力さのために、多くのユーザーから情報を収集するGAFA（Google、Amazon、Facebook、Apple）を含むプラットフォーマーは、局所差分プライバシーを利用したデータ収集を取り入れ始めている。

❷ 海外・国内政策動向

個人データの取り扱いに関する研究は、欧州においては2018年から施行されたGDPRに大きく影響されたといえる。 GDPRの一つの大きな特徴は、IPアドレスやCookieなどのインターネットで利用される識別子を含む情報も、個人情報として取り扱うこととなったことにある。このことは、Web経由で個人のデータを暗黙的に収集してきた事業者に多くの影響を与えた。またGDPRは、個人情報を取り扱うサービスやシステムについて、設計段階でデータ保護が組み込まれ、利用者が明示的に設定しなくても、十分なプライバシー保護が初期状態で設定されていることを要求する（設計段階、および初期状態におけるプライバシー）。この設計思想は、プライバシー・バイ・デザインの影響を受けたものである。

さらにGDPRは、プロファイリングを含む個人に対しての自動化された意思決定について、分析する側に透明性の確保（プロファイリングしている事実を知らせること、およびプロファイリングの方法やその影響について説明すること）などを求めるとともに、利用者はこのような自動化された意思決定を受けない権利を有するものとした。「プロファイリング」とは、「個人の特定の側面を評価するために、個人データを自動的に処理すること」であり、特に個人の業務実績、経済状況、健康、個人的嗜好、興味、信頼、行動、

所在、または移動など、個人について重要な判断を伴う分析・予測やそれを提供するシステムとそのロジックについて、透明性の確保と説明責任を求めるとともに、そのような決定を受け入れない権利があることを定めている。

我が国においても、個人情報保護法が2020年6月に改正され、事業者が保有する個人データの利用停止・消去の権利や漏えい報告の義務化、仮名化の導入、罰金の強化・課徴金の導入などについて盛り込まれた。 GDPRの規定も意識した改正であると考えられる。また2018年5月、医療分野の研究開発に資するための匿名加工医療情報に関する法律（次世代医療基盤法）の施行や、同年6月に総務省および経済産業省がとりまとめを行なった「情報信託機能の認定に係る指針ver1.014」によって、認定された事業者によるデータ収集や利活用ができるようになってきた。今後の安心・安全なデータ利活用のため、データ・コンテンツに関するセキュリティー、およびプライバシー保護技術がますます重要になってきている[13)]。

（4）注目動向

［新展開・技術トピックス］

プライバシーや個人情報保護に関する注目トピックとして、AIシステムによる人種、性別、健康、宗教などによる差別の問題が挙げられる。 AIの入力データにこれらの情報が含まれる場合には、プライバシー・個人情報保護の問題となるが、AIによる出力や決定がこれらの情報と相関する場合には、差別の問題となる。差別配慮型のAIの学習は、人工知能分野においてはホットトピックである。またGDPRでは、AIがどのように自分の情報を使用するかの決定権を個人が持つことを保証するよう求めており、AIによる決定のロジックに透明性があることが必要とされている。深層学習を始めとしてAIによる決定は帰納的であり、決定のロジックが説明不可能であることが多い。AIによる決定を、演繹的・説明可能にするための研究もここ数年盛んになってきている。

またコンテンツの不正使用や操作に関して、敵対的生成ネットワーク（GAN：Generative Adversarial Networks）が注目されている。GANの発展により、写実的、かつ実在しない顔や物体の画像・音声・映像のバリエーションを無限に生成可能となったことから、GANを利用した実在の人物を模した偽の演説動画（例えば、DeepFake）などを生成できるようになった。写実性のある動画像や音声が、真正性の保証には利用できなくなるなどの弊害が予想されている。

［注目すべき国内外のプロジェクト］

❶ 戦略的創造研究推進事業におけるプロジェクト（JST）

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」研究領域においては、「プライバシー保護データ解析技術の社会実装」研究課題が実施されている。個人情報や企業の機密情報などのあらゆる機微情報を、安全性を保ったまま任意のデータ処理に適用可能とするプライバシー保護データ解析技術を創出することを目的としている。2016年度にスモールフェーズの研究を開始し、2019年度からは加速フェーズへと移行し社会実装に向けた研究が進められている。

さらに、2020年度には文部科学省において「信頼されるAI」という戦略目標が決定された。達成目標の一つとしてデータの信頼性確保及び意思決定・合意形成支援技術の創出があり、フェイクニュースやフェイク動画、データ改ざんなどを検知し対処する技術などが想定される研究として挙げられている。当該戦略目標の下、CREST「信頼されるAIシステム」や、さきがけ「信頼されるAI」、ACT-X「AI活用で挑む学問の革新と創成」研究領域が設立された。

❷ コグニティブセキュリティー関連プロジェクト（米国国防高等研究計画局（DARPA））

フェイクニュースに見られるように、悪意を持ったオンラインやオフラインでの誘導・干渉によって人々の思考や行動に影響を与える問題は、コグニティブセキュリティー（Cognitive Security）と呼ばれる分野の中心課題の一つである。「2.4.2 サイバーセキュリティー」で紹介した、ソーシャルエンジニアリング攻撃もこれに含まれる。これらの問題は、個人から国家まで幅広い影響を与えており、近年注目を集めるようになった。 DARPAでは、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・防御などに関するさまざまな研究開発プロジェクトを推進している（詳細は、「2.1.5 意思決定・合意形成支援」参照）。

（5）科学技術的課題

❶ AI セキュリティー・プライバシー

データ解析に関わる個人情報の問題は、これまでは取得・収集データ（入力データ）の扱いにフォーカスされてきたが、AI技術の発展により、取得・収集された個人データを用いて学習したAIの出力データの扱いにも、配慮が必要となりつつある。例えば、AIの出力データが引き起こす差別やプライバシー侵害、個人を識別する情報（顔認証や指紋認証データ、顔画像・動画、音声など）の偽造、マルチメディア情報の偽造などである。従来の情報処理技術でも同様のことは可能であったが、これまでは生成にはコストと人手を要した。AIの利用によって、このような情報が極めて低コストで、無尽蔵に生成できるようになった。さらには、人間が執筆したテキストと遜色ないテキストを自動生成できる文章生成言語モデルGPT-3（Generative Pre-trained Transformer 3）[14] が登場した。このような技術の悪用による、犯罪や名誉毀損、扇動などが危惧される。現実の情報とAIによる生成情報の管理・識別は、今後の課題である。

また、人工知能の学習には大量の情報が必要であり、特に個人情報や個人の行動履歴を入力とする場合には、大量の個人情報の適切な収集と管理にコストがかかる。さらにGDPRをはじめとする法令上の規制から、個人情報の収集は必要最小限度に留めることが求められている。これによって、個人情報の収集が可能であったとしてもなるべく収集量を少なくする、情報の提供者である個人の手元に情報を留める、などの対策をとりつつ、高度なAIを学習させる技術が注目されつつある。具体的には、既存のAIを少量の情報のみを用いて別の目的のAIに転換する転移学習、少量の情報を基に、その情報の特徴を踏まえ類似情報を大量に生成するGAN、個人の手元に情報を留め、情報そのものではなく学習の手がかりになる情報（学習モデルの勾配）のみを収集してAIを学習させる連合学習（Federated Learning）などである。これらの技術は本来個人情報保護とは無関係に機械学習技術として発展してきた技術であるが、GDPRの発足とともに、個人情報保護を目的とした利用技術に発展していく可能性がある。さらに、これらの技術と局所差分プライバシーや秘密計算の併用も、発展の余地がある。

❷ 局所差分プライバシーと対話モデル

局所差分プライバシーには、個人データを提供するユーザーやデータ収集者の間のやり取りの制限を定めた対話可能性という概念が理論解析において必要となる。ユーザーが一斉にデータをランダム化し、収集者がそれらの処理済みデータを一旦収集してから統計処理を行うモデルを非対話的モデル、ユーザーがデータをランダム化する際にユーザーと収集者全員に共有された乱数を活用できるモデルを公開コインモデルと呼ぶ。公開コインモデルはユーザー負担の増加が少ないが、非対話モデルに比べて大きな精度の向上が見られる場合があり、前に紹介したGoogleやAppleの事例で利用されている。ユーザー一人ずつ逐次

的にデータの収集を行う逐次的対話モデルや、同じユーザーに対して何回もデータ収集を行うことが可能な完全対話モデルは、プライバシーに配慮した機械学習を行うための対話モデルとして盛んに研究が行われている。加えて局所差分プライバシーにおいては、極めて多くのユーザーからのデータ収集がプロセスに含まれること、ユーザーはスマートフォンなど限られた計算能力と限られた通信帯域しか持たないデバイスを通じてデータ提供を行うこと、などの事情から、サンプル複雑度に加えて、ユーザーサイドにおける送信データ生成に要する時間やデータ提供時の通信量なども合わせて議論の対象となる。スマートフォンやIoTなど実際にデータ収集に利用され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は、未解決課題である。

（6）その他の課題

❶ 法規制

我が国の個人情報保護法は、入力データとしての個人情報を保護するために必要な措置や、その措置を緩和するための手続き（匿名加工情報・仮名加工情報）を定めているが、急速に進展する人工知能などのデータ利用技術や秘密計算技術にキャッチアップできているとは言い難い。データ活用とデータ保護技術に関して、法制度は「だれもが理解できる範囲」の技術しか想定していない。世界的なAI開発競争の波に乗り遅れないためにも、発展的な個人情報保護技術の利用を促進するための工夫が必要である。例えば、用途や範囲を限定した上で、既存の規制にとらわれることなく新たな技術の実証を行える場を導入することなどを検討できる可能性がある。日本政府からは、データ活用の在り方、AI技術活用の在り方について、それぞれ「データ戦略タスクフォース　第一次とりまとめ」[15)]が2020年12月に、「AI戦略 2019　～人・産業・地域・政府全てにAI～」[16)]が2019年6月に公表されたところであり、議論の活性化が期待される。

❷ 産学連携

産学連携は一昔前に比べれば活発になり、特に企業が所持するデータを利用した研究は盛んになった。一方で産学官の人材の行き来は欧米・中国に比べ活発ではなく、産は産、学は学、あるいは産から学への一方通行に限られる。クロスアポイントメント制度や時限付きで、アカデミアの人材が積極的にインダストリーの中で活躍できるような事例が増加してゆけば良い効果が生まれる可能性がある。

❸ 人材育成

日本における本分野のトップ国際会議での存在感は非常に小さい。トップ国際会議での発表には粘り強く精密な実験と精緻な議論を行う必要があるが、そもそも博士課程を目指す学生が減少する中、アカデミアでは目先の成果を追い求め、チームで息の長い研究を行う体力が失われている。また産業界では、研究成果を広くオープンにするなど人材を引き寄せ発展を促す戦略をとっていない場合も多い。研究者を目指す学生を手厚く支援し、キャリアプランを充実化させ、研究開発に取り組みたいと思う若い研究者を地道に増やすこと、また流行の分野に大型予算を配分するだけでなく、基礎的な成果にも分け隔てなく継続的に中規模の予算を多方面に配分することが必要である。

（7）国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
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く、論文も多く出ているが、統計的プライバシー、AIセキュリティー・プライバシーについては、取り組む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とんど米国の大学・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	○	↗	・中国本土の大学・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。
韓国	基礎研究	○	→	・各種の暗号アルゴリズムの基礎的な研究を行い、国際標準に提案活動を行っている。
	応用研究・開発	△	→	・特に目立った活動は見られない。

（註1）フェーズ

基礎研究：大学・国研などでの基礎研究の範囲

応用研究・開発：技術開発（プロトタイプの開発含む）の範囲

（註2）現状　※日本の現状を基準にした評価ではなく、CRDSの調査・見解による評価

◎：特に顕著な活動・成果が見えている　　○：顕著な活動・成果が見えている

△：顕著な活動・成果が見えていない　　×：特筆すべき活動・成果が見えていない

（註3）トレンド　※ここ1～2年の研究開発水準の変化

↗：上昇傾向、→：現状維持、↘：下降傾向

参考文献

1）独立行政法人情報処理推進機構（IPA）『情報セキュリティ白書2020』, https://www.ipa.go.jp/files/000087025.pdf

2）Latanya Sweeney, “k-Anonymity：A Model for Protecting Privacy”, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 10, no. 5（2002）：557-570. doi：10.1142/S0218488502001648

3）M. Hastings et al., “Sok：General purpose compilers for secure multi-party computation”, 2019 IEEE Symposium on Security and Privacy（SP）（2019）：1220-1237. doi：10.1109/SP.2019.00028

4）Unbound, “Secure Cryptographic Keys Across Any Environmrnt”, UNBOUND, https://www.unboundtech.com/
5）SEPIOR, “The New Standard for Key Management & Protection：Preventing Key Theft and Misuse for Data Privacy and Digital Asset Security, SEPIOR, https://sepior.com/
6）CURV, “The Institutional Standard for Digital Asset Security”, CURV, https://www.curv.co/
7）Yehuda Lindell and Benny Pinkas, "Privacy Preserving Data Mining", CRYPTO 2000, Lecture Notes in Computer Science 1880（2000）：36–54. doi：10.1007/3-540-44598-6_3
8）Rakesh Agrawal and Ramakrishnan Srikant, "Privacy-preserving data mining", Proc. of the ACM SIGMOD 2000 29, no. 2（2000）：439–450. doi：10.1145/342009.335438
9）Pascal Paillier, "Public-key cryptosystems based on composite degree residuosity classes", EUROCRYPT’99, Lecture Notes in Computer Science 1592（1999）：223–238. doi：10.1007/3-540-48910-X1_6
10）Ronald L. Rivest, Adi Shamir and Len Adleman, "A method for obtaining digital signatures and public-key cryptosystems”, CACM 21, no. 2（1978）：120-126. doi：10.1145/359340.359342
11）Cynthia Dwork et al., “Calibrating noise to sensitivity in private data analysis”, Journal of Privacy and Confidentiality 7, no. 3（2006）：17-51. doi：10.29012/jpc.v7i3.405
12）S. P. Kasiviswanathan et al., “What can we learn privately?”, SIAM Journal on Computing 40, no. 3（2011）：793-826.
13）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　システム・情報科学技術ユニット『科学技術未来戦略ワークショップ報告書 Society 5.0 システムソフトウエア』（CRDS-FY2020-WR-04）（2020年6月）.
14）T. B. BROWN et al., “Language models are few-shot learners”, 34th Conference on Neural Information Processing Systems（2020）：1-25.
15）デジタル・ガバメント閣僚会議　データ戦略タスクフォース『データ戦略タスクフォース　第一次とりまとめ（案）』（2020年11月）, https://www.kantei.go.jp/jp/singi/it2/dgov/data_strategy_tf/dai3/siryou2-1.pdf
16）統合イノベーション戦略推進会議『AI戦略 2019　～人・産業・地域・政府全てにAI～』, https://www.kantei.go.jp/jp/singi/tougou-innovation/pdf/aisenryaku2019.pdf

2.4.4 トラスト

（1）研究開発領域の定義

トラストとは、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。悪意ある第三者の攻撃から情報やシステム、サービスを守るセキュリティーや、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）のみならず、心理学や人文社会学の概念を含む。トラストに関しては、さまざまな分野で幅広い研究が行われているが、本研究開発領域では、情報システムや情報サービスへの社会の依存度が高まる中、社会との接点で生ずるトラストの問題や、トラストを確保するための取り組みについて、人間の心理、制度、および技術の側面から述べる。

（2）キーワード

人間の心理、法制度、公平性、解釈性、透明性、デジタル署名、リモート署名、トラストサービス、eIDAS（Electronic Identification, Authentication and Trust Services）規則、コンピューテーショナルトラスト（Computational Trust）、自動化システムにおけるトラスト（Trust in Automation）、倫理的・法的・社会的課題（ELSI：Ethical, Legal and Social Issues）

（3）研究開発領域の概要

［本領域の意義］

1968年、ドイツの理論社会学者であるNiklas Luhmannが著作「信頼―社会的な複雑性の縮減メカニズム[1)]」の中で、古典的トラストは「社会生活の基本的な事実である。（中略）こういうこと（社会生活）が可能であるのは、我々が他者や社会に対して一定の信頼をおいているからにほかならない」と述べているとおり、トラストは古くから安心・信頼できる社会を形づける重要な仕組みとして存在してきた。 Luhmannは、トラストのメカニズムを「複雑性を縮減するメカニズム」と述べているが、複雑性が増し、一般市民的な視点からはブラックボックス化が進む情報社会では、トラストの概念／仕組みも大きく変化してきている。この変貌するトラストの概念、およびその獲得は、例えばプラットフォーマーがビジネスを成功させる鍵と認識されるようになってきており[2)]、また人々が安心して社会生活を営む上でも重要になってきている。

［研究開発の動向］

❶ 情報システムや情報サービスの社会への浸透とトラスト

近年、さまざまな情報システムや情報サービスが日常的に利用され、我々の生活に欠かせない存在になっている。その一方で、利用者のトラストを揺るがしかねない問題も発生している。例えば、インターネットやソーシャル・ネットワーキング・サービス（SNS：Social Networking Service）は、幅広い企業や組織、個人で活用され、普及するようになった。企業や組織は、さまざまな情報を不特定多数の人々へ届け利用者の拡大を図るだけでなく、インターネットやSNS上の口コミや行動データをサービスへ生かす動きがある。利用者にとっても、コミュニケーションツールとしてだけでなく、商品やサービスを比較する際の有益な情報源としての活用も広がっている。一方で、インターネットやSNS上に溢れる情報は、必ずしも客観的に正しいと判断されるものばかりではない。COVID-19の感染が広がる中、2020年2月、「トイレットペーパーが不足する」という根拠のない情報が拡散された結果、日本中の店舗でトイレットペーパーが品薄となった事態は記憶に新しい。インターネットやSNSなどの情報ネットワークが浸透している現代では、このよう

なフェイクニュースまたは誤情報の拡散が社会問題にまで発展しており、情報サービスや情報そのものに対する不信感を招いている。また近年、行政サービスにおいてもデジタル化の動きが広がりつつある。 SNSや各種アプリを活用し、公共サービスや情報の提供を行うなど、各自治体での取り組みが進んでいる。2016年1月からはマイナンバーカードの交付が開始された。マイナンバーカードは公的な本人確認書類として利用できる他、さまざまな行政サービスを利用する際に活用することができる。一方、国が網羅的に個人情報を把握し管理するのではという不信感や、個人情報漏えいへの懸念が根強く、国民から広くトラストを得られているとは言い難い。普及率も人口の約23%にとどまっている（2020年12月1日時点）[3)]。

このようにさまざまな情報システムやサービスが社会に浸透すると同時に、それらに対するトラストの重要性が認識されるようになった。トラストの実現を目指し、後述のトラスト研究の動向でも紹介するように、さまざまな分野での研究が行われ議論されているところであるが、本領域においては、トラストを確保するための要素として、人間の心理、制度、および技術による側面に注目する。

まず、情報システムや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り、人間の心理に大きく影響される。例えば、インターネット上のショッピングサービスにおいて、クレジットカード番号を安心して入力するかどうかは、サービスのセキュリティーやユーザービリティーだけでなく、利用者自身の好みや直感などの内的な要素が関係することが示されている[4)]。セキュリティーやプライバシーが技術的に確保されていても、それを心理的に受け入れることができず、不安を感じること[5)]や、第三者の口コミや評判が肯定的にも否定的にも人間の心理に影響を与えることがある。このような人間の心理の様相は、育ってきた時代や環境、社会的背景などによって多様かつ複雑であり、心理学や経済学、人文社会学などを含む学際的な検討が行われている。

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によって、トラストを確保することもできる。例えば「トラストサービス」という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がある。欧州では2016年にeIDAS（Electronic Identification, Authentication and Trust Services）規則[6)]が施行されており、デジタル署名などのトラストサービスについて、EU全域にわたる枠組みが示されている。また民間の保険の中には、大規模災害やサイバー攻撃などのリスクに備えられるような制度・サービスを提供するものもあり、これを活用することもトラストを得る一つの方法である。

加えて、技術的な側面からのアプローチも有用である。「2.4.1 IoT・制御システムセキュリティー」、「2.4.2 サイバーセキュリティー」、および「2.4.3 データ・コンテンツのセキュリティー」で紹介した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や、デジタル署名、ブロックチェーン（詳細は、「2.5.7 ブロックチェーン」参照）、スマートコントラクトをはじめとする、情報システムや情報そのものの信頼性を保証する技術、そのほか情報システムの公平性・解釈性の確保などによって、情報システムのトラストを技術的に担保することが可能であろう。

❷ トラスト研究の動向

トラスト自体の研究は、従来、哲学、心理学、社会学、経済学といったさまざまな分野で進められてきた。例えば、心理学の観点からは、「なぜ人は他者を信頼するのか」という人間の心理や意図に関する研究が、社会学の観点からは、「なぜ人は他者から信頼されるように行動するのか」といった人間の行動に基点を置いた研究などが進められてきた[7)]。

1990年代に入ると、システム・情報科学技術分野でもトラスト研究が盛んに行われるようになってきた。

そのきっかけとして、マルチエージェントシステムや分散エージェント基盤の研究に従事していたStephen Marshが提唱したコンピューテーショナルトラスト（Computational Trust）がある[8)]。これは、人間社会の概念であったトラストを計算科学（Computational Science）からアプローチする研究であり、まさにデジタル社会に向けて変貌するトラストのための研究と言える。1）被信頼者の信頼性（Trustworthiness）に関する情報を定量的・客観的に観測するための研究、2）観測されたトラストバリューを評価計算する手法や形式化の研究、3）当該結果に基づく意思決定のためのトラストポリシーに関する研究に大別される。

1990年代中頃からは、機械の自動化や自律化が進む中で、人間が機械の振る舞いをどのように認知するか、つまり人間が機械をどのように信頼するかという問題を含む、Trust in Automation[9)]の研究が進められた。これは、人間の自動化システムに対する信頼が、（特に自律性の高い）システムの利用にどのような影響を与えるかを扱う、認知システム工学的アプローチである。もともとは工場などのプロセス制御系に端を発しているが、近年は自動運転などの研究においても盛んである。自律性がますます高まる機械や情報システムと、人間との協調を考えていく上で、両者の信頼関係をどのように構築・維持するかは重要な課題となっている。

近年では、より自律化した機械として、人工知能（AI）へのトラストに注目が集まっている。 AIが社会に実装されていったときに起こり得る、社会・人間への影響や倫理的・法的・社会的課題（ELSI：Ethical, Legal and Social Issues）の議論が活発化しており、どうすれば社会において人間がAIをトラストできるかの研究が盛んである（「2.1.9 社会におけるAI」参照）。

米国では2010年代の国民ID戦略の中でトラストフレームワークが生まれた。トラストフレームワークとは、オンラインサービスを利用・提供する際に、ユーザー認証の信頼性を保証し合い、ユーザー情報を、事業者間で安全に流通させるための、ガバナンス／プライバシー／テクノロジーを包括する枠組みである。米国政府の国民ID戦略の中で採用されただけでなく、米国以外の政府や、ISO（International Organization for Standardization）やITU-T（International Telecommunication Union Telecommunication Standardization Sector）などの国際標準化団体、世界経済フォーラム（ダボス会議）などでもプロジェクト化され、普及に向けた国際協調や制度的／技術的相互運用性について議論されている。国内では全国の大学などと大学共同利用機関法人情報・システム研究機構国立情報学研究所（NII：National Institute of Informatics）が連携して、「学術認証フェデレーション（通称：GakuNin）」として運用が開始されている。

このようにトラストに関する研究はさまざまな分野において多岐にわたって行われている。分野統一的なトラストの定義は存在しておらず、トラストを得るための要素にも多様な考え方がある。本領域においては、トラストは、デジタル化が進む現代社会で重要となる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とし、悪意ある第三者の攻撃から情報やシステム、サービスを守るセキュリティーや、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）のみならず、心理学や人文社会学の概念を含むものと捉える。

（4）注目動向

［新展開・技術トピックス］

❶ トラストサービスと eIDAS（Electronic Identification, Authentication and Trust Services）規則

トラストサービスに関わる制度として、我が国においては電子署名法[10)]が2001年に施行された。これは、

民事訴訟法上の否認防止の役割を果たす紙文書をデジタル文書へ置き換えるために必要な制度であった。一方、人（自然人）や法人、不動産などに加え、自動車や医療機器のようなIoTデバイスや暗号資産などがデジタルに識別・検証可能になれば、さまざまな処理を機械的に行ったり、連携させたりすることが可能になる。紙文書からデジタル文書への単なる置き換えではなく、このような本質的なデジタル社会に対応するために必要なトラストサービス全般に関して、現在総務省を中心に制度設計の議論が行われている。

欧州では、2016年からeIDAS規則が施行され、トラストサービスについて包括的に規定している。eIDAS規則では、自然人や法人などを識別可能として、これらが作りだしたデータの主体者の証明や、時刻のデジタルな証明（デジタルタイムスタンプ）を行う第三者機関の枠組みを提供している。また、国や分野の境界を超えるための保証レベル基準の相互運用性確保が図られていることは、欧州をまたぐ包括的な制度として重要である。さらにeIDAS規則は、欧州の標準化団体による標準化を実質的に義務付けており、多くの欧州標準が開発されてきている。トラストサービスでは、このeIDAS規則によって欧州が先行的にルール化を進め世界をリードしており、今後もその動向に注目が集まっている。

❷ 脱ハンコとリモート署名の活用

COVID-19が契機となりテレワークの導入が進む一方で、文書への押印のために出社せざるを得ないという「ハンコ（押印）出社」が話題となった。従来の紙文書と押印は、長くにわたり社会に浸透し慣習化してきたこともあり、本質的に否認防止を必要としないものまで過度にハンコを必要とする社会を生んでいた。行政手続きのデジタル化を進める政府は、手続きの多くで押印を廃止することを表明しており、脱ハンコへの動きが加速している。

不要な押印廃止の取り組みのため、本人認証や文書の真正性担保のための有効な手段として、デジタル署名の利用拡大に向けた取り組みが進められている。ただし、デジタル署名に使う暗号鍵／署名鍵を利用者が管理するのは安全性に課題がある。そこで、暗号鍵／署名鍵を事業者（トラストサービスプロバイダー）が管理するリモート署名という枠組みがある。欧州のeIDAS規則では、リモート署名を実施するトラストサービスプロバイダーの信頼性を保証するために、要求事項を明確化し、プロバイダー認証を行っている。我が国では、リモート署名を安全に利用するための技術的な要件が明確化されていないことに加え、現在の電子署名法の特定認証業務は、eIDAS規則のようにトラストサービスプロバイダーを位置付けられておらず、技術と制度の双方に渡った課題がある。

2020年4月に日本トラストテクノロジー協議会（JT2A：Japan Trust Technology Association）からリモート署名ガイドラインが公開されるなど、課題解決に向けた活動が進められている[11)]。

［注目すべき国内外のプロジェクト］

❶ 科学研究費助成事業「情報社会におけるトラスト」（日本学術振興会）

日本学術振興会（JSPS：Japan Society for the Promotion of Science）では、科学研究費助成事業・基盤研究（B・C）における特設分野研究として、「情報社会におけるトラスト」分野が設定され、研究が進められている（2019年度～）。当該特設分野研究では情報社会におけるトラストに関して、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、社会的な取り組みの強化など、多面的な研究が行われている[12)]。

❷ 欧州・SmartCom プロジェクト

IoT（Internet of Things）やCPS（Cyber Physical System）と呼ばれる、サイバーとフィジカルを高度に連携したシステムにおいては、フィールド（フィジカル空間）に配置されるセンサーの信頼性（Trustworthiness）が必要になり、またこのセンサーが法定計量としての計測が求められる場合、計量法に即した計測機器の校正トレーサビリティーの証明が求められる。さらに、利用者からトラストが得られる仕組みの構築も重要である。

これらの要求に対し、欧州のSmartCom（Communication and validation of smart data in IoT-networks[13]）プロジェクトでは、デジタル校正証明書によりトレーサビリティーを検証可能とすることが目指されており、そこでは信頼の基点の確立やハードウェアセキュリティー（「2.4.1 IoT・制御システムセキュリティー」参照）、eIDASの証明書の利用など、さまざまな要素を組み入れながら、システム全体として人や社会からのトラストの獲得を実現することが検討されている[14]。

❸ 欧州・GAIA-X プロジェクト

ドイツ政府とフランス政府が、2019年10月29日に発表したEU規模でのデータの共有や利活用を支援するため、クラウドサービスのインフラを構築する構想（GAIA-X プロジェクト）を打ち出している。GAIA-Xは、認証や契約手続に基づいてデータへのアクセスを制御し、データ主権を保護しつつさまざまなクラウドサービスとの相互運用性を確保する技術的な仕組みであり、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る。

（5）科学技術的課題

トラストに関する科学技術への要求は、改ざん防止／完全性（Integrity）、否認防止（Non-Repudiation）、真正性（Authenticity）などだけでなく、透明性（Transparency）や説明責任（Accountability）、トレーサビリティー（Traceability）などの社会的要求も結びついている。これらは、単一の技術のみで情報システム・サービス全体を担保することは難しく、複数の技術を組み合わせることが必要である。

例えばIoTシステムの場合、信頼の基点の構築や機器認証（「2.4.1 IoT・制御システムセキュリティー」参照）をベースとして、「2.4.2 サイバーセキュリティー」から「2.4.3 データ・コンテンツのセキュリティー」まで、ライフサイクル全体にわたるトラストを担保することによって、上記要求に応えたサービスとして価値を生むと考えられる。この中にミッシングピースとなる技術があるとトラストを揺るがすことになりかねず、システム全体を縦断した対策が不可欠である。またAIなどの自律的なシステムにおいては、特に社会との関係の中で公平性や解釈性、透明性の確保などが注目されており、そのための技術的な対策が検討されている（「2.1.4 AIソフトウェア工学」参照）。

（6）その他の課題

❶ 技術と制度の関係

トラストに関わる多くの課題は、科学技術だけでは解決できず、特に制度と技術の整合が重要である。既存の制度／法規制が科学技術の発展の壁となり、イノベーションを阻害する一面がある一方、デジタル社会に相応しい法規制が、技術開発を促進していく可能性もあり、国際的な競争力につながっていくことが期待できるためである。「排気ガス規制法」が排気ガス除去の技術を推進したように、デジタル社会におけ

るトラストを念頭においた制度／法規制は、トラストに関する技術的な課題を打ち破ると言っても過言ではない。そのためには、社会的要求、倫理も含めたデジタル社会の制度／法規制のあり方など、学際的な活動や、法規制、産学連携、分野連携、人材育成など多面的な取り組みが重要である。

また、トラストに関する制度で重要なのは標準化である。デジタル社会は、局所最適化ではなく、全体最適化を目指す方向に向かっている。その際、制度が果たす役割として、さまざまなシステムやデータなどの連携や相互のやりとりができる相互運用性の確保（特に法的相互運用性）と、そのための標準化の推進が必要になる。リスクに応じた保証レベルを、地域、分野を超えて適用するためには、適度な制度による強制力が必要であり、特に保証レベルの法的相互運用性の確保が出来ないと、デジタル技術によるスケールアウトしたサービスの構築が出来ない恐れがある。

❷ 接触追跡とプライバシー（個人データ活用とそのリスク）

COVID-19感染拡大防止のため、世界各国で市民の接触追跡（コンタクトトレーシング）の仕組みが導入されている。データを国の中央サーバーで管理する集中型と、スマートフォンなどの端末内に保管する分散型、接触把握手法をGPSの位置情報を用いるか、近距離無線通信Bluetoothによる接触情報を用いるかの違いなど、さまざまな形態が各国でとられている。コンタクトトレーシングは、市民の行動履歴や接触者履歴などのデータ収集・分析によって感染拡大防止の効果を期待できるが、その効果を最大限活かすためには、大多数の人々の間でこの仕組みが普及され活用される必要がある。行きすぎれば国による市民監視にもなりかねない中、どのように人々や社会からのトラストを得て、広く社会へ導入できるかが鍵となっている。

中国では、GPSの位置情報を基に移動経路や感染者との接触の有無などのデータを国が一元的に管理し、感染リスク度に応じた「ヘルスコード」が提示される仕組みを導入している。これによって、市民は公共交通機関やスーパーマーケットをはじめとするありとあらゆる場所の立ち入りや移動がコントロールされている。このような仕組みは、プライバシーの侵害だとの批判も見られるが、COVID-19の感染拡大を最小化できるという便益が重んじられた文化的な背景や、監視カメラを始めとするさまざまな監視や管理が政府主導で進められてきた経緯などから、社会に受け入れられたものと考えられる。

一方、欧州の多くの国や我が国は、プライバシー保護をより徹底したApple-GoogleによるAPI（Application Programming Interface）（以下、Apple-Google方式）を活用したアプリを導入している。Apple-Google方式は分散型のシステムであり、Bluetoothによる接触情報のみがユーザー端末に一定期間保管され、感染者との接触の有無については端末内でデータ照合がなされる。プライバシー保護を徹底することで社会からのトラストを得て、広い普及が目指された仕組みであるが、普及率はあまり高くない。我が国における接触確認アプリCOCOA（COVID-19 Contact Confirming Application）は、2020年6月に導入されたが、同アプリのダウンロード件数は、2020年12月28日時点で約2,245万件[15)]であり、徐々に利用数は増えつつも、依然として日本の人口の20%未満にとどまっている。プライバシー保護が確保されたデザインになってはいるものの、人々の心理的な障壁は依然として存在しており、トラストが得られていない状態と言える。接触確認アプリやその仕組みが広く人々からのトラストを得られるためには、プライバシー確保のための技術的要件だけでなく、意義・目的との適合性や差別の排除などの社会的要件も含めて仕組みを考慮することや、人々の視点に立った議論を十分に尽くし、理解が得られるような説明を継続的に実施していくことが重要と考えられる。

参考文献

1）ニクラス・ルーマン『信頼―社会的な複雑性の縮減メカニズム』大庭健, 正村俊之 訳（東京：勁草書房, 1990）.
2）レイチェル・ボッツマン『TRUST 世界最先端の企業はいかに〈信頼〉を攻略したか』関美和 訳（東京：日経 BP, 2018）.
3）総務省「マイナンバーカード交付状況」,https://www.soumu.go.jp/kojinbango_card/#kouhu
4）村山優子, 藤原康宏, “トラストの感情としての安心およびその要因について”, Reliability Engineering Association of Japan, Vol.31, No.1（2009）.
5）国立大学法人東京大学, 学校法人東洋大学, 日本電信電話株式会社「「インターネット利用における不安に関する国際比較調査」により”安心”と”安全”の乖離を実証～安全でも、不安を感じる日本人の特徴が明らかに～」（2010年9月2日）.
6）THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, “REGULATION（EU）No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC”, Official Journal of the European Union L257（2014）：73-114.
7）川崎千晶, “組織間における信頼のメカニズムと移行プロセス”, 早稲田大学大学院商学研究科紀要（72）（2011）, 40-49.
8）Stephen Paul Marsh, “Formalising trust as a computational concept”, Ph.D. dissertation. University of Stirling（1994）：1-184.
9）Bonnie M. Muir, "Trust in automation：Part I. Theoretical issues in the study of trust and human intervention in automated systems", Ergonomics 37, no. 11（1994）：1905-1922. https://doi.org/10.1080/00140139408964957
10）e-GOV 法令検索「平成十二年法律第百二号：電子署名及び認証業務に関する法律」, https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=412AC0000000102
11）日本トラストテクノロジー協議会リモート署名タスクフォース「リモート署名ガイドライン」, https://www.jnsa.org/result/jt2a/2020/index.html
12）日本学術振興会　科学研究費助成事業「別表3　特設分野研究」,https://www.jsps.go.jp/j-grantsinaid/03_keikaku/data/h30/h30_beppyo3.pdf
13）SmartCom, “Communication and validation of smart data in IoT-networks”, EURAMET, https://www.euramet.org/research-innovation/search-research-projects/details/project/communication-and-validation-of-smart-data-in-iot-networks/
14）Tuukka Mustapää et al., “Metrological Challenges in Collaborative Sensing：Applicability of Digital Calibration Certificates”, Sensors 20, no. 17（2020）：4730. doi：10.3390/s20174730
15）厚生労働省「新型コロナウイルス接触確認アプリ（COCOA）COVID-19 Contact―Confirming Application」, https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/cocoa_00138.html