2.4.1 IoTシステムのセキュリティー

（1）研究開発領域の定義

IoT（Internet of Things）の進展によって、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IoTシステムのハードウェア、ソフトウェア、センサー、ネットワーク、サプライチェーンなどの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）、信頼の基点、計測セキュリティー、ハードウェアセキュリティー、意図的な電磁妨害、サイドチャネル攻撃、テンペスト、ハードウェアの真正性、耐タンパー性、サプライチェーンセキュリティー、ハードウェアトロージャン、オフェンシブセキュリティー、レジリエンス、パブリッシュ・サブスクライブ型通信

（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。その中でも、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・ドローン・宇宙航空など、IoT化が大きく進展している[1)]。 IoT機器には、利用目的や環境によって、各種のオペレーティングシステム（OS：Operating System）やセンサー、LSI（Large Scale Integration）などの多種多様なソフトウェア・ハードウェアが搭載され、イーサネットやWiFi、4G/5G、LPWA（Low Power Wide Area）などさまざまな通信方式が利用されている。このため、IoT機器では、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。また、IoT機器は、その台数が非常に多く、従来のパスワードによる保護が不十分な機器や、外部との接続を想定していない時代に設計された自動車のCAN（Controller Area Network）などの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。さらに、ハードウェアやアナログ情報を扱うセンサーへの物理攻撃のリスクも存在する。

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 2021[2)] では、2021年にNICTERプロジェクトの大規模サイバー攻撃観測網で観測されたサイバー攻撃関連通信のうち、全体の約3割が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、引き続き当該分野におけるセキュリティー対策が重要であることを示している。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施設においては、システムの誤動作や停止などによって、組織、およびわれわれの生活を含む社会全体に大きな影響を与えうる。また、IoT機器に実装されるハードウェアやソフトウェアは、さまざまなサプライヤーから提供されている。ソフトウェアの脆弱性やハードウェアの製造時における不正な部品の混入が発生すると、世界中で稼働しているIoT機器に影響を与えることとなる。このため、IoT機器では、設計から製造、検査、流通、運用に至るサプライチェーンの観点からもセキュリティー対策が必要である。

以上のように、IoTシステムは、自動車や電気・水道・ガスなど、われわれが生活していく上で必須なものとなってきており、さらに、わが国が目指すサイバー空間とフィジカル空間を高度に融合したシステムによるSociety5.0の基盤となるものである。これらを悪意のある第三者からの攻撃から守り、安全・安心にIoTシステムを利用できるものとするために、IoTシステムのセキュリティーの研究開発は必要不可欠である。

［研究開発の動向］

❶ IoTシステムのセキュリティーリスクと研究開発のトレンド

IoT機器は、無人でかつ第三者が物理的にアクセス可能な場所に設置されることによる物理的な場所でのセキュリティー攻撃のリスクに加えて、ネットワークに接続されることによる遠隔からのセキュリティー攻撃のリスクへの対策が重要になってきている。 IoTシステムの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。このように、IoT機器に対してマルウェア感染などを通して行われる遠隔からのサイバー攻撃は、情報システムへのサイバー攻撃のような情報の搾取よりも、IoT機器の乗っ取りやサービスの停止などを目的としている場合が多い。「Mirai」の亜種や新種は、ルーターの脆弱性を狙う「Satori」やAndroid OSを搭載したIoT機器を狙う「Matryosh」など2021年も多数発生している。

・IoT機器の認証と信頼の基点

「Mirai」に感染した事例では、多くの IoT機器が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たことや、IoT機器の制御がスーパーバイザーモードやルート特権により保護されていなかったため、そこを狙われて大規模なDDoS攻撃を実現したものである。IoT機器に関するインシデントの原因はIoT機器のパスワード管理が不適切であることが多いが、多数のIoT機器を個別のパスワードで管理することは難しい。 IoT機器の認証には、証明書を利用する方法もあるが、証明書が保存されているデバイスから抜き取られて複製されるリスクも存在する。このため、デバイスの外部から覗かれたり改変されたりしない耐タンパー性に優れたハードウェアに認証鍵を保管する「信頼の基点」が必要である 。内閣府の戦略的イノベーション創造プログラム（SIP）第2期では、極小のIoT端末に搭載できるハードウェアによる「信頼の基点」の開発が進められている。今後は、信頼の基点の上に暗号、認証、認可などの機能を統合していくことが求められている。

・産業用システムやレガシーシステムのセキュリティー

産業用設備・機器の制御システムは、従来、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。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や、2021年の米国の石油パイプライン施設におけるマルウェア感染による米国東海岸のガソリン価格高騰、2021年の国内の医療機関におけるマルウェア感染による新規患者・救急搬送の受け入れ停止など、社会に影響を与えるインシデントが多数報告されている。近年、このような重要インフラのセキュリティー対策が重要視されており、各国政府から各種指針が公開されている。

また、従来はネットワークに接続されていなかったレガシーシステムもネットワークに接続されるようになってきている。例えば、自動車はネットワークに接続されコンピューターで制御されるコネクティッドカー（CAV：Connected Autonomous Vehicle）となる一方で、ネットワークを経由して自動車の制御システムに侵入できることが報告されている[5)]。内閣府の戦略的イノベーション創造プログラム（第2期）「自動運転（システムとサービスの拡張）」では、持続的に安全・安心な自動運転の実現に向けた新たなサイバーセキュリティーの研究が行われている。今後も、産業用システムやレガシーシステムのネットワーク接続の拡大にともない脅威の増大が予想されるため、早急に対策の強化が必要になってきている。

・計測セキュリティー

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、取得した情報をクラウドやローカルで処理し、その結果をアクチュエーターにより実空間にフィードバックしている。センサーによる計測を攻撃から守る計測セキュリティーの重要性も高まっている。例えば、センサーが計測する信号に対して超音波で機械的共振を起こさせたり、レーザーで偽情報を発生させたりする攻撃のリスクや、センサー自体が別物に置き換えられたりするリスクも存在する。近年は、攻撃の対象が自動運転で重要な役割を持つLiDAR（Light Detection And Ranging）など、さまざまなセンサーに広がっている。IoT機器の計測データへの攻撃は、実空間における事故に直結する可能性があるため、計測データへの攻撃に対する防御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ことが求められている。

・ハードウェアのセキュリティー

IoT機器のソフトウェアに対する攻撃に加えて、システムの基盤となるハードウェアへの物理的な攻撃のリスクも高まっている。例えば、機器内部に強制的に電磁界を誘導し、IC（Integrated Circuit）や素子を破壊する意図的な電磁妨害などの侵襲攻撃や、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、非暗号デバイスの内部情報を奪うテンペストなどの非侵襲攻撃がある。以下では、意図的な電磁妨害、サイドチャネル攻撃、テンペストについて紹介する。

a）意図的な電磁妨害

意図的な電磁妨害（IEMI：Intentional Electromagnetic Interference）は、電磁波によりハードウェアの信頼性、およびセキュリティーを低下させる脅威である。 IEMIは、高出力電磁パルスを用いて機器内部に強制的に電磁界を誘導し、ICや素子を誤動作させたり破壊したりするものであり、IoT機器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。交通網やデータセンターなどの社会インフラに関係するIoTシステムを対象として、IEMIの発生装置、および大電力電磁波を空間に放出させるアンテナなどが研究されている[6)]。

b）サイドチャネル攻撃

サイドチャネル攻撃は、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攻撃であり、これまで、主にスマートカードが攻撃の対象であったが、近年は暗号モジュールが搭載されたハードウェア全般に広がっている。従来は暗号モジュールのごく近傍からの攻撃がメインであったが、近年の研究では、機器から十分離れた遠方からでもサイドチャネル攻撃が可能であることが報告されている。また、IoT機器で使用されている汎用的なプロセッサーからもサイドチャネル攻撃により秘密鍵を取得できることが報告されており、攻撃の対象となるハードウェアや取得される情報が拡大している。さらに、機械学習モデルの取得を目的としたサイドチャネル攻撃も提案されている[7)]。今後は、サイドチャネル攻撃による物理現象に着目した対策技術などの確立が求められている（詳細は「（5）科学技術的課題❷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」に記載）。

c）テンペスト

テンペストは、ハードウェアから非意図的に生ずる電磁情報を計測し、機器内部の秘密情報を取得する攻撃の総称であり、人と機器の間でやりとりされる暗号化が困難な情報を対象としている。例えば、ディスプレイ、プリンタ、キーボード、マイクロフォン、スピーカなどの入出力ハードウェアが対象となる。この攻撃の成否は機器から漏えいする電磁情報の計測精度に依存するため、これまでは高度な知識と専用の高精度な計測器を用いなければ困難であったが、近年、ソフトウェア無線、およびその制御ソフトウェアを用い

ることで計測環境の構築が容易になり、インターネットに公開されている攻撃パラメーター情報を利用することで攻撃が可能となり、そ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、ネットワークから切り離しても完全には防げないため、脅威を事前に分析して対策しておくことが求められている。

・IoT機器のサプライチェーンセキュリティー

最近の重要なリスクの一つに、IoT機器のサプライチェーンリスクがある。 IoT機器は、さまざまなサプライヤーから提供されるハードウェア、ソフトウェアにより構成され世界中で利用されている。2020年6 月には、過去20年以上、多くのIoT機器で利用されているTCP/IPライブラリーで「Ripple20」と呼ばれる脆弱性が発見され世界中の多くのIoT機器に影響を及ぼした。2020年12月にはオープンソースとして公開されているTCP/IPスタックに「AMNESIA：33」と呼ばれる脆弱性が発見され世界中の多くのIoT機器に影響を及ぼした。また、ハードウェアにおいても、最先端プロセスの半導体チップの需要増や新型コロナウイルス感染症のパンデミックなどによる部品の供給不足により、IoT機器の製造時に不正な部品が混入するリスクが発生している。半導体メーカーの正規品の製造能力の増強や、不正な半導体流通の抑止、半導体チップ真正性の検証技術の開発が必要である。近年、各国政府においてサプライチェーンのセキュリティーが重要視されており各種指針が公開されている（詳細は「（3）研究開発領域の概要［研究開発の動向］❷海外・国内政策動向」に記載）。

❷ 海外・国内政策動向

米国では、オバマ前大統領による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（2018年4月にCSF Version 1.1へ改訂され、CSF Version 2.0への改訂が計画されている）。 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越えて、多くの国・組織で採用されている[8)]。バイデン政権においても大統領令14028号により、2021年5月に起きた米国の石油パイプライン施設へのサイバー攻撃などに対応すべく、サイバーセキュリティー強化のためにIoT機器を含むサプライチェーンの安全性向上が指示されている。当該大統領令を受け、2022年にNISTからサプライチェーンのセキュリティー強化のための各種文書が発行されている[9)]。わが国においては、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）、「重要インフラのサイバーセキュリティに係る行動計画」（2022年6月）が公表されている。

IoTについては、NISCより「安全なIoTシステムのためのセキュリティに関する一般的枠組み」（2016年8月）や、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は「IoTセキュリティガイドラインVer1.0」（2016年7月）を公表しており、これに基づきISO/IEC27400の規格化が進められている。経済産業省からは、「サイバー・フィジカル・セキュリティ対策フレームワークVer1.0」（2019 年4 月）や、「IoTセキュリティ・セーフティ・フレームワーク」（2020年11月）が公表されている。総務省からは「IoTセキュリティ総合対策」（2017年10月）や、その改訂版として「IoT・5Gセキュリティ総合対策2020」（2020年7月）、「ICTサイバーセキュリティ総合対策2022」（2022年8月）が公表されている 。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[10)]。

サプライチェーンセキュリティーについては、半導体メーカーによる正規品の製造能力を増強するために、米国では、商務省（DoC）と国立標準技術研究所（NIST）による半導体推進プログラム（CHIPS）[11)]が推進されている。また、欧州では、2022年2月にEuropean Chips Act[12)]により430億ユーロ規模を想定した半導体の研究開発・製造能力の増強プログラムが提案され、2030年に現在の市場シェアを2倍の20%にするという目標が掲げられている。

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、分野ごとのSubcommittee（SC）に分かれて活動している。この中でIoTセキュリティーについて注目すべきは、SC27（Information security, cybersecurity and privacy protection）のセキュリティー関連技術とSC41（Internet of things and digital twin）のIoT関連技術である[13)]。また、ISO/TC184（Automation systems and integration）、IEC/TC65（Industrial–process measurement, control and automation）もIoTシステムのセキュリティーと関係がある。 SC41では、日本の提案2件が採択されている[14), 15)]。

セキュリティー認証制度では、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の国際的な制度はまだないが、国内では2019年11月に、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IoT機器のセキュリティー認証事業を開始している[16)]。米国では、サイバーセキュリティーに関する米国大統領令 14028号を受けて、米国・NISTが2022年2月に、消費者向けのIoT機器とソフトウェアのためのセキュリティーラベリング基準を策定している[17)]。これは、サイバーセキュリティーの専門的な知識を必要とせずに、消費者がIoT製品やソフトウェアを購入できるよう支援するものである。 IoT機器のラベリングでは10個の評価項目（6 つのTechnical Product Criteriaと4つのNon–Technical Criteria）が、ソフトウェアのラベリングでは15個の評価項目（7個のDescriptive Claimsと8個のSecure Software Development Claims）が示されている。また、EUでは、ハードウェア、およびソフトウェア製品の安全性を確保することを目的としたCyber Resilience Actが提案されている[18)]。

（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OSの研究開発が盛んになっている。例えば、Google は、従来のLinuxをベースとしたOSではなく、Fuchsiaと呼ぶ新しいリアルタイムカーネルを用いた IoTデバイス向けのRTOSを公開している。一方で、OSやネットワークなどの周辺機能を安価に利用するために、組み込みLinuxなどの従来のOSも多くのIoT機器で使われている。従来のOSをサイバー攻

撃から守るために、マルウェアによるOSカーネルへの不正アクセスを監視する研究も行われている。また、新たにRTOSのリアルタイム制御や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、これらの攻撃や防御の研究も行われている。暗号機能やアプリケーションについても、ハードウェアセキュリティモジュール（HSM：Hardware Security Module）と呼ばれるデバイスの外部から覗かれたり改変されたりしない耐タンパー性に優れたハードウェアや信頼できる実行環境（TEE：Trusted Execution Environment）を用いて暗号鍵の管理や暗号化処理機能をマルウェアから守る研究や、アプリケーションを独立した仮想マシン上で実行することでセキュリティーリスクを低減する研究が行われている。

❷ IoTシステムのソフトウェア更新

IoT機器はその台数が膨大であるため、新しく発見された脆弱性に迅速に対処するためには無線回線経由でソフトウェアの更新を行うOTA（Over The Air）機能が重要な役割を持つ。一方で、この機能を攻撃者が悪用するとIoT機器が乗っ取られるリスクがあるため高いセキュリティーが求められている。例えば、インターネット技術の通信仕様を策定しているIETFではIoT機器のためのソフトウェア更新のRFC（Request For Comment）としてSUIT（Software Update for Internet of Things）、自動車向けでは既存のITシステムのソフトウェア更新フレームワークであるTUF（The Update Framework）をベースにしたUPTANEの仕様化が進められており研究が活発化している。ソフトウェア更新の信頼性を保証するためには、信頼できる認証局が発行した証明書を用いる方法やチップ内の信頼の基点を用いる方法、ブロックチェーンにより分散管理されている情報を用いる方法なども研究されている。

❸ IoT機器のコンテクスト認証

IoT機器をサーバーに接続する際、IoT機器のなりすましを防ぐために、サーバーはIoT機器の接続権限を認証する。IoT機器はその台数が膨大であるため、従来のパスワードによる認証はパスワード管理などの点で現実的でない。また、信頼の基点に認証情報を格納して認証する方法が研究されているが、認証情報が改ざんされるリスクも存在する。そのため、機器の位置情報や、複製が困難な機器・チップ固有の物理複製困難関数（PUF： Physically Unclonable Function）などの機器に関するコンテクストを用いるコンテクスト認証が研究されている。

❹ パブリッシュ・サブスクライブ型 IoT ネットワークのセキュリティー確立

IoT機器の通信では、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）と呼ばれる方式が検討されており、通信プロトコルとしては、MQTT（Message Queue Telemetry Transport）やCoAP（Constrained Application Protocol）、DDS（Data Distribution Service）などの、パブリッシュ・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（またはフォグ）」と呼ばれる中継サーバーを用いるか、あるいは「パブリッシャー」からのブロードキャストを用いて通信環境を構築する。これらの通信方式は、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が、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が送信されたり、他の機器の通信が盗聴されたりする危険性がある。また、IoT機器は処理能力に制限があるため、IoT機器の認証や暗号化、IoT機器間の通信のチェックなどのセキュリティー機能をフォグで集中的に処理する方法も研究されている。今後は、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持つIoTネットワークの確立、およびIoTネットワークのプロトコルに係わる脆弱性検査手法の確立も必要である。

❺ 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は、自社で設計したIC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。この時、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回路が付加され、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。これに対して、例えば、機器から漏えいするサイドチャネル情報を用いてハードウェアトロージャンを検出する方法が研究されている[19)]。近年は、ICや他の電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指摘されている[20)]。機器の組み立てに必要なPCBや電子部品のサプライチェーンは世界中に広く拡大しており、信頼できるサプライチェーンの構築とともに、機器の組み立てまで含めた広範な対象に対して、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を検知、抑制する技術の開発が求められている。ハードウェアトロージャンやデバイスの真正性を主たるスコープとする国際会議であるIEEE International Conference on PHYSICAL ASSURANCE and INSPECTION of ELECTRONICS（PAINE）においてもPCBのハードウェアトロージャンに関する発表が増加している。

❻ 低出力の電磁波を用いた意図的な電磁妨害

意図的な電磁妨害では、高出力電磁パルスなどを用いて、機器内部の素子やICなどのデバイスを破壊し、IoT機器の信頼性や可用性を低下させる攻撃がこれまで行われてきた。近年、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低出力の電磁波を誘導させることで、機器そのものを破壊することなく、セキュリティの低下が引き起こされる可能性も示されている。このように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。また、スマートフォンやスマートスピーカーへのコマンド注入攻撃やデバイスの制御信号を改ざんして動作を妨害、または制御を乗っ取るといった新たな脅威も示されている。従来は高価な計測器を用いなければ困難であったが、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、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。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（SIP）第2期「IoT社会に対応したサイバーフィジカルセキュリティ」（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、SIP第1期において「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、重要インフラなどのIoT機器の監視・防御技術の研究開発やセキュリティー人材育成などサイバー脅威に対するIoT社会の強靭化が目指された。続くSIP第2期においては、SIP第1期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。SIP第2期では、「信頼の創出・証明」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機器のソフトウェアの完全性・真正性を確認する技術、PCBのハードウェアトロージャンの検知やLSI設計で利用するIPコアのハードウェアトロージャンの混入を設計・製造段階で検証する技術などの研究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機器でも利用できるように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）の研究開発も進められ、今後さまざまな産業分野への応用が期待されている。

❷ CREST「基礎理論とシステム基盤技術の融合によるSociety 5.0のための基盤ソフトウェアの創出」（JST）

JSTのCREST「基礎理論とシステム基盤技術の融合によるSociety 5.0のための基盤ソフトウェアの創出（2021～2029年度）」では、安心・安全で信頼できるデータ駆動型社会の実現に向けて、原理的に安心・安全で信頼できる他国に依存しないオープンな基盤ソフトウェアの創出が目指されている。当該分野に関しては、近年増加しているハードウェアやOSの新たな脆弱性への対処を踏まえ「信頼できないハードウェアやOSを含む計算環境で安全なシステムを構築可能とするセキュリティ技術の創出」が進められている。その中で、ゼロトラストの概念を路襲しIoTのトラストチェーンの正当性の数学的証明と実行隔離・自動検知・自動対処を行うゼロトラストIoTシステムの研究が進められている。ゼロトラストアーキテクチャーはIoTにとっても有用であるが、IoT機器ではソフトウェアや証明書が改変され乗っ取られているリスクがあるため何を信頼の基点としてIoT機器を検証するか、IoT機器の処理能力に制限がある中で情報の漏えいや改ざん（機密性）を完全に防ぐのではなく攻撃を受けた後のIoT機器の運用の維持（可用性・完全性）・回復のためのレジリエンスをどう実現するか、についての研究開発も求められている。

（5）科学技術的課題

ここでは、「（3）研究開発領域の概要、（4）注目動向」に関する科学技術的課題を紹介する。

❶ 水平連携型IoTシステムのセキュリティーの確立

従来のIoT機器は、あらかじめ登録されているクラウドと接続することを前提としていたが、移動するIoT機器では、IoT機器同士が直接つながって通信する水平連携型IoTシステムが検討されている[21)]。例えば、自動車では、自動運転のために路側機器と通信したり、行き交う自動車同士で通信したりするケースが想定される。このためには、不特定のIoT機器同士が相互認証できるセキュリティー技術が必要となる。IoT機器では、ソフトウェアや証明書が改変され乗っ取られているリスクもあるため、何を信頼の基点として相互認証するかが課題となっている。

❷ 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

従来、ハードウェアセキュリティーでは、ハードウェア内部で取り扱われる情報ごとの脅威の分析や対策技術が研究されてきている。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期待されている。例えば、サイドチャネル攻撃やテンペストは「機器の内部から外部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「機器の外部から内部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て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を実現できる可能性がある。例えば、サイドチャネル攻撃やテンペストでは、攻撃者が機器の電磁界を外部から計測することによるその周辺の電磁波の乱れに着目し、その乱れを検出することで攻撃を検知する方法が研究されている。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。

❸ ハードウェアの経年劣化と真正性を検証可能な技術の確立

近年、最先端プロセスの半導体チップの需要増やIoT機器の保守に不可欠なレガシー半導体チップの供給不足により、IoT機器の製造では、半導体メーカーが保証する正規の半導体チップに加えて、リユース品やリファービッシュ品（保証付き再生品）を使うケースも発生している。リユース品やリファービッシュ品では、偽造・模造品、あるいは異常な経年劣化特性を有する「フェイクチップ」が混入するリスクが高まっている。これに対して、IoT機器に搭載される半導体チップの真正性の検証や流通から製造に至るまでの

半導体チップのトレーサビリティーを検証する仕組みが提案されている。例えば、半導体チップに埋め込んだ暗号モジュールを用いて半導体チップを認証する方法[22]や半導体チップが持つ複製が困難な機器・チップ固有の物理複製困難関数（PUF：Physically Unclonable Function）を用いる方法が提案されている。また、半導体チップの経年劣化特性を用いて真正性を判定する方法が米国を中心に研究されている[23]。しかしながら、これらの方法は、半導体チップ内部に専用回路を搭載したり、専用の半導体試験装置を開発したりするなど、半導体メーカーに依存している。近年、情報機器全般に対してフェイクチップが混入するリスクが高まっており、半導体メーカーに依存することなく、機器の製造者が半導体チップの経年劣化と真正性を検証できる技術の確立が求められている。

❹ オフェンシブセキュリティーと脅威分析の拡充、レジリエンス

IoT機器では、セキュリティー対策が十分に考慮されずに設計され、ハードウェアやソフトウェアに脆弱性が存在したままの状態で長期間運用されると、その間に脆弱性が攻撃されるリスクが高くなる。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、事前に脅威を想定して対策を施しておくオフェンシブセキュリティーの考え方を取り入れ、設計時に、発生しうる攻撃を想定し、脅威分析に基づく対策を講じておくことが重要である。脅威分析では、攻撃パターンのデータベースが重要となるが、サイバーセキュリティーと比較するとまだ規模が小さく、今後拡充していく必要がある。また、IoTシステムのセキュリティーの専門人材が不足しており、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かつ自動的に評価する検証方法の確立も望まれている。 IoT 機器は、重要な社会インフラの一部として機能していることも多く、攻撃による被害の影響は広範囲に及ぶ可能性が高いため、インシデントが発生した後も、機能を回復・維持し、その脅威に対して耐性が獲得できるようにするレジリエンスの研究も求められる。

（6）その他の課題

❶ 分野連携

IoTシステムのセキュリティーの研究開発では、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、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く、今後、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。米国では、集積回路関連の学会（International Solid–State Circuits Conference（ISSCC）[24]やSymposia on VLSI Technology and Circuits[25]、環境電磁工学関連の学会[26]で分野横断的な議論が始められている。国内では、電子情報通信学会のハードウェアセキュリティ研究会が分野横断的な議論ができる場となっており、今後、議論が活発化することが望まれる。また、IoTシステムのセキュリティーは、システム開発、運用とも密接に関係しており、アカデミアと産業界が連携して取り組む必要がある。戦略的イノベーション創造プログラム（SIP）（内閣府）では産官学により社会実装を目指した取り組みが、電子情報技術産業協会（JEITA）でも産学による電子部品、電子機器の規格化が行われており、今後、さらにIoTのセキュリティー分野の産官学による連携が拡大していくことが望まれている。

❷ 人材育成

IoTシステムのセキュリティーでは、上述のとおり分野横断的な幅広い知識が必要となるが、そのような人材が不足している。これまで、文部科学省における補助事業「成長分野を支える情報技術人材の育成拠点の形成（enPiT）」（第2期）では、セキュティー分野の人材育成プログラムが2016年から2021年3月

まで実施された[1]。セキュリティー分野における課題は年々増加しており、例えば、サプライチェーンセキュリティーではサプライチェーンにおける脅威を俯瞰し解決策を講じられる人材の育成など、従来以上に分野を縦横断した学際的な人材を育成するための育成事業と教育プログラムが重要となっている。これまでの取り組みを含め、今後さらなる人材育成の拡大・拡充が必要である。

（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	○	↗	・戦略的イノベーション創造プログラム（SIP）第2期「IoT社会に対応したサイバー・フィジカル・セキュリティ」（内閣府）や官民研究開発投資拡大プログラム（PRISM）（内閣府）でIoTシステムのセキュリティーの研究開発が進められている。 ・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。
	応用研究・開発	○	↗	・戦略的イノベーション創造プログラム（SIP）第2期「IoT社会に対応したサイバー・フィジカル・セキュリティ」（内閣府）において開発された技術が民間企業を通じて社会実装されつつある。 ・自動車を中心とした大規模なコネクティッド・シティーの実証実験が開始されている。 ・一般社団法人重要生活機器連携セキュリティ協議会（CCDS）が、国内企業を対象としてIoTのセキュリティー認証制度を2020年に開始した[16)]。 ・産業技術総合研究所のサイバーフィジカルセキュリティ研究センターを通して、産学官連携体制の構築が進められている。
米国	基礎研究	◎	↗	・DEFCONやBlackhat などのハッカー向き国際会議でのIoTセキュリティーの活動が著しい。 ・IC チップ真正性を保証する技術として、Supply Chain Hardware Integrity for Electronics Defense（SHIELD）で電子機器のライフサイクルにわたる追跡性を確保する仕組みを完成している。さらに、セキュリティー機能IC チップについて自動設計技術の創出を狙う研究開発プログラム（Automatic Implementation of Secure Silicon, AISS）が進行している。
	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。 ・自動車のセキュリティー技術開発で躍進している。 ・PCやサーバー向けのプロセッサ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。 ・IoTシステムを担う半導体の製造フローにおいても不正な半導体チップが正規品として混入するリスクを避けるために、商務省（DoC）と国立標準技術研究所（NIST）が半導体推進プログラム（CHIPS）を立ち上げ、米国内の製造能力の増強が計画されている。

1 現在は各分野・大学での自主運営に移行しており、情報セキュリティ大学院大学、東北大学、大阪大学、和歌山大学、九州大学、長崎県立大学、慶應義塾大学の7大学院が連携して「情報セキュリティプロ人材育成短期集中プログラム（enPiT Pro Security）」が実施されている。

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の研究を進めている。 ・Horizon Europeの「6. Civil Security for Society」[27] において、Hardware, Software and supply chain securityとして在庫管理、安全でないコンポーネントの検出、および廃棄のための効果的なメカニズムの構築が進められている。
	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（Common Criteria）認証においてドイツの提案が多い。 ・欧州提案のLPWAの複数の方式が実用フェーズに入った。 ・欧州発の自動車規格であるAutosarで自動運転も含めたセキュリティを検討している。 ・European Chips Act[12] として、430億ユーロ規模を想定した半導体の研究開発・製造能力の増強プログラムを提案し、2030年に現在の市場シェアを2倍の20%にするという目標を掲げており、米国同様に、半導体製造能力の増強を行うことで、不正な半導体の流入を防ぐための取り組みが行われている。
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10年間において、サプライチェーンにおいて悪意あるハードウェアが混入するシナリオを考慮した論文を出口とした学術研究は米国についで2位となっており、基礎研究に力を入れている。
	応用研究・開発	○	↗	・ISO/IEC JTC1 SC41 に多数の規格提案をしている。 ・自動車のセキュリティーについて中国独自の規格を定めている。 ・ハードウェアセキュリティーは軍事研究として行われている模様で、成果が見えない。
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。ブロックチェーン技術をIoTへ適用する研究がある。 ・他国と比べ、国内に十分な半導体製造能力を有していることから、ICチップ真正性保証技術などのハードウェアセキュリティーの基礎研究は十分ではない。
	応用研究・開発	△	→	・CC（Common Criteria）認証への提案がある。 ・ハードウェアセキュリティーは軍事研究として行われている模様で、成果が見えない。

（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）総務省「令和4年版情報通信白書（本編）」https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/pdf/01honpen.pdf,（2023年2月24日アクセス）.

2）国立研究開発法人情報通信研究機構（NICT）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2021」NICT, https://www.nict.go.jp/report/NICTER_report_2021.pdf,（2023年2月24日アクセス）.

3）Ben Herzberg, Igal Zeifman and Dima Bekerman, “Breaking Down Mirai: An IoT DDoS

Botnet Analysis," Imperva, https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/,（2023年2月24日アクセス）.
4）Hamdija Sinanović and Sasa Mrdovic, "Analysis of Mirai malicious software," in 2017 25th International Conference on Software, Telecommunications and Computer Networks（SoftCOM）（IEEE, 2017）: 1-5., https://doi.org/10.23919/SOFTCOM.2017.8115504.
5）Charlie Miller and Chris Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle," IOActive, https://ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf,（2023年2月24日アクセス）.
6）William A. Radasky, "Electromagnetic Warfare is Here," IEEE Spectrum, https://spectrum.ieee.org/electromagnetic-warfare-is-here,（2023年2月24日アクセス）.
7）Lejla Batina, et al., "CSI NN: Reverse Engineering of Neural Network Architectures Through Electromagnetic Side Channel," in Proceedings of the 28th USENIX Security Symposium（USENIX Association, 2019）, 515-532.
8）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（東京: 東洋経済新報社, 2020）.
9）National Institute of Standards and Technology（NIST）, "NIST Issues Guidance on Software, IoT Security and Labeling," https://www.nist.gov/news-events/news/2022/02/nist-issues-guidance-software-iot-security-and-labeling,（2023年2月24日アクセス）.
10）独立行政法人情報処理推進機構「情報セキュリティ白書2022」184-185, https://www.ipa.go.jp/files/000100472.pdf,（2023年2月24日アクセス）.
11）CHIPS.GOV, "About CHIPS for America," National Institute of Standards and Technology（NIST）, https://www.nist.gov/chips,（2023年2月24日アクセス）.
12）European Commission, "Digital sovereignty: Commission proposes Chips Act to confront semiconductor shortages and strengthen Europe's technological leadership," https://ec.europa.eu/commission/presscorner/detail/en/ip_22_729,（2023年2月24日アクセス）.
13）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）.
14）独立行政法人情報処理推進機構（IPA）社会基盤センター「IoT製品・サービスにセーフティ・セキュリティ等を実装するプロセスが国際標準として出版：日本提案の規格が国際標準化団体ISO/IECにて出版」IPA, https://www.ipa.go.jp/ikc/info/20210621.html,（2023年2月24日アクセス）.
15）金沢工業大学「電気電子工学科の横谷哲也教授が主導してきたIoTプラットフォームが国際標準として出版。 IoTの普及促進に向けIoTプラットフォームを規定。大学院生も調査分析及び原理検証に貢献」https://www.kanazawa-it.ac.jp/kitnews/2021/0115_yokotani.html,（2023年2月24日アクセス）.
16）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,（2023年2月24日アクセス）.
17）Information Technology Laboratory, "Cybersecurity Labeling for Consumers: Internet of Things（IoT）Devices and Software," National Institute of Standards and Technology（NIST）, https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/cybersecurity-labeling-consumers-0,（2023年2月24日アクセス）.
18）European Commission, "Cyber Resilience Act," https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act,（2023年2月24日アクセス）.
19）Duy-Phuc Pham, et al., "Obfuscation Revealed: Leveraging Electromagnetic Signals for Obfuscated Malware Classification," in ACSAC '21: Annual Computer Security Applications Conference（New York: Association for Computing Machinery, 2021）, 706-719., https://doi.

org/10.1145/3485832.3485894.
20）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.
21）山崎育生, 他『oneM2Mハンドブック：水平連携型IoTシステムの標準規格と実装』山﨑徳和 編著（東京：森北出版, 2021）.
22）Serge Leef, “Supply Chain Hardware Integrity for Electronics Defense (SHIELD), (Archived),” Defense Advanced Research Projects Agency（DARPA）, https://www.darpa.mil/program/supply-chain-hardware-integrity-for-electronics-defense,（2023年2月24日アクセス）.
23）Lok Yan, “Automatic Implementation of Secure Silicon (AISS),” Defense Advanced Research Projects Agency（DARPA）, https://www.darpa.mil/program/automatic-implementation-of-secure-silicon,（2023年2月24日アクセス）.
24）International Solid-State Circuits Conference（ISSCC）, https://www.isscc.org,（2023年2月24日アクセス）.
25）2023 Symposia on VLSI Technology and Circuits, https://www.vlsisymposium.org,（2023年2月24日アクセス）.
26）EMC Society, “EM Leakage,” https://www.emcs.org/emleakage.html,（2023年2月24日アクセス）.
27）European Commission, “Horizon Europe Work Programme 2021-2022: 6. Civil Security for Society,” https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2021-2022/wp-6-civil-security-for-society_horizon-2021-2022_en.pdf,（2023年2月24日アクセス）.