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.