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、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、フィッシング攻撃、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 for Security、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。インターネットはすで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。個人についても、フィッシングによる情報の盗取や盗取情報の悪用による不正アクセス、スマホ決済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。また、テレワークの普及に伴い社外から社内システムにアクセスするためのVPN製品の脆弱性を対象とした攻撃も増加している。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。このように、サイバーセキュリティーはわれわれの生活の安心・安全から国家の安全維持にまで関わり、安心・安全な社会を実現するためにはサイバー攻撃への対策を継続的に行うことが必要不可欠といえる。

［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

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。例えば、侵入検知では、シグネチャーと呼ぶ検出ルールに従って不正侵入を検出するIDS（Intrusion Detection System）や検出した際に遮断まで行うIPS（Intrusion Prevention System）が導入されている。最近では、AIを用いて、ネットワーク内の通信内容や端末の挙動などを観測して不正侵入を検知する方法も導入されている。マルウェアの検知でも、これまではシグネチャーベースのマルウェア検知手法が利用されてきたが、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効果が低下しており、検査対象のファイルを実際に動かして検知する方法や、検知したマルウェアをAIで学習して未知のマルウェアを検知する方法が研究されている。また、不正侵入の防御では、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、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導入が進展している。サイバーセキュリティーの研究は、従来、ソフトウェアやネットワーク技術、暗号理論などが中心であったが、現在ではその領域は拡大しつつあり、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。急増するサイバー攻撃の検知や防御にAIを活用する研究も進展している。また、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研究開発だけでなく、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。

セキュリティーの研究開発では、実際の攻撃に基づき対策を検証する必要があるため、観測データの蓄積が重要な役割を持っている。国立研究開発法人情報通信研究機構（NICT：National Institute of Information and Communications Technology）は、日本最大規模のサイバー攻撃観測・分析・対策システムNICTERを構築し、そこで収集したデータを活用して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。また、NICT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きている。今後、さらなるサイバー攻撃の観測データ基盤の拡充が求められている。

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が示され、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[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。バイデン政権においてもサイバーセキュリティーは最優先事項と位置づけられ、さまざまな施策が展開されている。大統領令[2)]（2021年5月）では、同月に起きた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、サプライチェーンの安全性向上を主な目的としてサイバーセキュリティーの強化が指示されている。また、2022年4月には、サイバースペースでの国家安全保障、デジタル近代化を担うサイバースペースおよびデジタル政策局（Bureau of Cyberspace and Digital Policy）が発足している。

わが国においては、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センター（NISC：National center of Incident readiness and Strategy for Cybersecurity）が、2015年に初めてのサイバーセキュリティー戦略を策定し、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。2021年には3回目となる同戦略が策定され、「Cybersecurity for All」がコンセプトとして掲げられている。また、2022年には、経済活動に関して行われる国家および国民の安全を害する行為を未然に防止することを目的として経済安全保障推進法が成立している。さらに、第6期科学技術・イノベーション基本計画でも、サイバーセキュリティーの研究開発の重要性が示されている。ファンディングでは、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）第2期」（テーマ：IoT社会に対応したサイバー・フィジカル・セキュリティ）や「官民研究開発投資拡大プログラム（PRISM）」（テーマ：サイバーセキュリティ対策の高度化AIを活用したサイバー攻撃対策技術の開発）、総務省が主導する「電波資源拡大のための研究開発」（テーマ：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）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、かつユニークな観測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サイバー攻撃の観測データに基づく研究開発になる傾向が強く、ビッグデータの蓄積と分析の重要性が高まっている。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。NICTが構築し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や、Web媒介型攻撃対策技術の実用化に向けた研究開発（WarpDrive）は、その一例である。

❷ 観測データのプライバシーを配慮した分析

サイバーセキュリティーの研究開発は上述のとおりビッグデータ分析が求められるケースが多いが、大規模なデータを用意するには、複数機関で連携してデータを収集する、もしくは複数機関が保有する異なるデータを共有して分析することが有効なケースも存在する。しかし、組織の壁を越えてデータを共有する際には、扱うデータによってはプライバシーや機密性の観点から配慮を要するケースが多い。そのような配慮を着実に実施してデータを収集するケースもあるが、データを暗号化したままで分析を行うプラバシー保護データマイニング技術[1]や、データ自体の共有を行わないで学習を実施する連合学習技術[2]、プライバシーに配慮した形でデータを共有し演算を実施する差分プライバシー技術[3]の活用も進められている。

❸ 説明可能なAIに関する研究

機械学習や深層学習などのAI技術の発展により、さまざまな分野において自動化技術が発展してきているが、AI技術が下した判断の根拠を理解することは難しく、AI技術の社会実装の一つの問題点となっている。サイバーセキュリティー分野においても同様の問題があり、AI技術が下した判断をもとに人が検証した上で対策を実行するケースが多い。AI技術が判断の根拠を示すことができれば、人手による検証作業の効率化が期待できる。AI分野では説明可能なAI技術が研究されており、サイバーセキュリティー分野へ適用するための研究が望まれている。

❹ 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、クラウドサービスやリモートアクセスの利用が進み、クラウド内に保存されている企業の機密情報や個人情報などにどこからでもアクセスすることが可能となってきている。近年、これらの情報を狙うサイバー攻撃では、フィッシングなどのユーザーの隙を突いたソーシャルエンジニアリング攻撃が利用されるケースが増加している。システム的側面だけでなく、ICT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[4]。

1 詳細は「2.4.3（3）研究開発領域の概要［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　プライバシー保護データマイニング」を参照いただきたい。

2 詳細は「2.4.3（4）注目動向［新展開・技術トピックス］❷連合学習」を参照いただきたい。

3 詳細は「2.4.3（5）科学技術的課題❷局所差分プライバシーによるデータ活用」を参照いただきたい。

4 詳細は「2.4.4 人・社会とセキュリティー」を参照いただきたい。

❺ スマートコントラクトに関する研究

ブロックチェーンは、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への利用が開始されており、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。一方で、これらのシステムにもさまざまな脆弱性が発見され、実際に攻撃による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に関する研究が世界的に活発に行われている。

❻ 研究倫理への配慮

国際学会では、相当数の学会で研究倫理に配慮することが投稿の条件となっており、特に難関国際学会ではその傾向が高い。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、適切な対応を実施するといった責任ある情報開示（Responsible Disclosure）の重要性が、学術界を中心に認識されるようになっている。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が求められている。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ため、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研究者自身が確認しながら研究を実施することが求められている。

［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）

上述のとおり、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。NICTでは、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）が進められた。本プロジェクトは2021年3月31日をもって終了したが、2021年4月1日より、NICTのCYNEX事業の一つとして継続して実施されている。本プロジェクトでは、複数の研究開発機関が結束し、ユーザーがブラウザーからWebページにアクセスした履歴を日本中の実験参加者から収集し、それをもとに研究開発、そして社会展開することを目指している。特に、単なるWebページのアクセス記録だけでなく、そのユーザーがどのようなWebページへ遷移するアクションをとったのかなどのきめ細かな情報が取得され、今後の研究開発に活用できる貴重な情報が蓄積されている。この取り組みは、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）第2期（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）第2期では、社会展開までを意識した研究開発が実施されている。研究開発テーマ「IoT社会に対応したサイバー・フィジカル・セキュリティ」では、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・セキュリティ対策基盤のための「信頼の創出・証明」「信頼チェーンの構築・流通」「信頼チェーンの検証・維持」技術の研究開発が進められている。

❸ 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官民研究開発投資拡大プログラム（PRISM）でも、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「サイバー攻撃ハイブリッド高速分析プラットフォームの研究開発」の中でAIを活用したサイバー攻撃対策技術の開発が行われ、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いる。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の実用化を国が研究開発プロジェクトとして進めている。

❹ 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」では、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。

❺ 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（NOTICE）（総務省および NICT）

総務省およびNICTはインターネットプロバイダーと連携して、脆弱なID・パスワードの利用など、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の取り組み（NOTICE：National Operation Towards IoT Clean Environment）を実施している。 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。施行から数年が経過した現在、調査対象ポート・プロトコルの拡大が検討されている。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。

❻ 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・NSF（National Science Foundation）は、2022年8月にNSFにおける最大規模の研究プログラムThe Secure and Trustworthy Cyberspaceプログラム[3), 4)]として、サイバーセキュリティーとプライバシーに関する最先端研究に2540万ドルの資金を投入することを発表している。このプログラムによってサポートされるプロジェクトの一つに、ノースカロライナ州立大学が主導する「安全で信頼できるソフトウェアサプライチェーンの実現」[5)]がある。このプロジェクトでは、一般消費者、政府、産業界、学界が使用するソフトウェアのリスクを軽減することを目指して、ソフトウェアのセキュリティーを確保するための原則やツール、プロセスを策定し、サプライチェーンセキュリティーの指標を示すことを目標としている。ワシントン大学が主導する「不利な立場にある人々のコンピューティングの未来の確保」[6)]では、セキュリティーやプライバシーに関する機能を十分に活用できずリスクに晒されている弱い立場の人々をサポートするソリューションを開発することを目標としている。インディアナ大学が主導する「分散秘匿コンピューティングセンター」[7)]では、信頼できる実行環境を実現するハードウェア機能を利用し、クラウドコンピューティング環境などの分散コンピューティングシステム全体で悪意のあるソフトウェアによる侵害を防ぎ計算を実行する方法に取り組むことを目標としている。

❼ 欧州・Horizon Europeによるサイバーセキュリティー研究開発支援

欧州ではHorizon 2020の終了に伴い、Horizon Europe（2021–2027）による研究開発支援が行われている。 Horizon Europeの長期計画として、「The first Horizon Europe strategic plan（2021–2024）」が発行されており、それによるとHorizon Europeには3つの柱が存在し、そのうちの一つの「Global Challenges & European Industrial Competitiveness」では6つのクラスタが定義されている。サイバーセキュリティーはこの6つのクラスタのうちの「Civil Security for Society」において大きく取り上げられているほか、クラスタをまたがる事項として、その重要性が認識されている。欧州ではHorizon

Europeとは別に、European Defence Fund（EDF）による研究開発支援も存在する。 EDFは防衛に関する研究開発に対して支援を実施するもので、2016年に提案され2017年に設立されたものである。 EDFではサイバーセキュリティーに関する研究開発も取り上げられている。

（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 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おり、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に加えて、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。マルウェアのコード分析（静的解析）においても、パッカーなどを通じた亜種の大量生成に左右されない分析技術や、CPUアーキテクチャーの差異を超えた分析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 説明可能なAI技術

AIの判定結果の根拠を説明するための技術は、さまざまな分野において、その重要性が認識され始めているが、現時点では、AI分野での研究開発が主流であり、サイバーセキュリティー分野での判定結果の説明性を提供できる技術は確立されていない。AIのアルゴリズムの入力・出力・モデルだけに着目した分析・説明性の提供がAI技術の分野にて研究されている段階であり、その技術をそのままサイバーセキュリティー分野に適用しても、AI技術に精通していないセキュリティーオペレーターが理解できる説明性を担保できる状況にはなっていない。現在、AIはすでにシステムの中の部品として用いられており、サイバーセキュリティー分野のオペレーターにも理解できるレベルの説明性を提供できる技術の開発が求められている。

❸ 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ための大規模観測・分析技術

フィッシング攻撃や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。インターネット上に存在するWebサイトを巡回して情報を収集（Webクローリング）して、その中から攻撃に加担する悪性サイトを検知する取り組みもあるが、Web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。特にフィッシングサイトに関しては引き続き増加傾向にある。これらの攻撃は人間がだまされるという側面があり、対策にはヒューマンファクターの理解が重要となる。どのようにしてユーザーがだまされ、被害者になっていくのかというユーザー視点での分析のためには、ユーザーのWebブラウザーや組織のWebプロキシーなどの観測データを取り込み、分析を行うための大規模観測・分析技術の確立が必要となっている。

❹ 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ている。脅威インテリジェンスの中でもサイバー攻撃の通信先IPアドレスやURIなどの痕跡を表すIoC（Indicator of Compromise）情報は比較的普及しており利用が進んでいるものの、IoC以外の情報については十分に活用されていないといわれており、効果的に記載・共有できるインテリジェンスを用意するなどしてオペレーターがより効果的な現状把握・対策を講じることを可能にすることが求められている。また、IoC情報についても、セキュリティー対策のより高度な自動化の実現など、さらなる活用が望まれている。一方で、インテリジェンス自体を自動生成する技術も研究されている。インテリジェンスには、一般に公開されている情報から得られるインテリジェンスであるオシント（OSINT：Open Source Intelligence）や、人が人に接触して収集するヒューミント（HUMINT：Human Intelligence）、通信などを傍受して収集するコミント（COMINT：Communication Intelligence）などがある。 OSINTの一つであるソーシャルメディアなどのWeb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の確立が望まれている。

・観測データのプライバシーを配慮した分析技術

複数の機関が収集した観測データのプライバシーを配慮して分析するためには、データ自体を共有することなく分析する技術や、データを共有しても共有先に解読されない技術を活用することが有用である。学習したモデルだけを共有する連合学習や、データを暗号化したまま演算を実施する準同型暗号技術、データを分割し処理空間を分けることでデータの秘匿性を担保する秘密分散技術などが存在している。今後、これらの技術がサイバーセキュリティー領域でも適用可能性および有用性を検証した上で活用されることが望

まれる。

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、セキュリティーオペレーターが攻撃の状況を迅速に理解することを難しくしている。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・効率化のための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。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に役立てることにも活用できる。

❻ 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。標的型攻撃対策では、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ため、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、人間のオペレーターがこれらの機器が生成するアラートを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だけを抽出する技術が求められている。

（6）その他の課題

❶ 有用なデータ基盤の運営拠点の構築

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る。そのため、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。さらに、研究の材料となるデータの中にはプライバシー保護が必要な情報や機密情報が含まれる可能性もあり、入手を困難にしている[8)]。また、わが国の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、すで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。データ基盤の構築・運用のためには、サイバーセキュリティーの研究のための実データを扱うシステムの構築から関係組織との調整・ノウハウ蓄積などを一元的に行い、期限が限定されていない資金で運営が行える拠点の構築が望まれる。

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対策製品に強み。NETSCOUT社が買収）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き大規模に産業展開し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、すでに顕在化している、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や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・体制を確立して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必要である。すで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）。今後、研究成果を高めるためには、重要なテーマについては複数の研究グループに研究資金を提供し、高い研究成果を上げた研究グループを評価する仕組みなどにより研究グループ間の競争を促すことが必要である。そのためには、研究資金提供側の組織も各分野の専門家を擁して、技術的な評価を行える体制が必要である。例えば、米国では、前述のとお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（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。

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。 NICTで2022年4月に新たに組織されたサイバーセキュリティネクサスでは、国内のセキュリティー人材の育成を促進するため、NICTが開発した演習教材と実機の演習環境から成るサイバーセキュリティー演習基盤のオープン化トライアルを開始している。これは、これまで主に国の機関や地方公共団体向けに行ってきた実践的なサイバーセキュリティー演習を、国内の民間事業者や教育機関向けにも提供するトライアルであり、2023年度に本格運用が開始される予定である。情報処理推進機構（IPA）サイバーセキュリティセンターでは、模擬プラントを用いた演習や攻撃防御の実践経験、最新のサイバー攻撃情報の調査・分析などを通してセキュリティー人材を育成するプログラムを実施している。また、文部科学省「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、セキュリ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[5]。これらの取り組みを含め、今後、さらなる人材育成の拡大・拡充が必要である。

5 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）」を実施している。

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いま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、産業界での経験を生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を見ることができる。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取り組みなどを行っている[9)]。わが国においても、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。

❺ CSIRTの拡充

CSIRT（Computer Security Incident Response Team）は、セキュリティーインシデントが発生した際に対応するチームであり、セキュリティーインシデントへの対応や脆弱性情報の収集・共有、セキュリティーインシデント対応の窓口機能などを持つ。 CSIRTには、企業などの組織に関わるセキュリティーインシデントを扱うInternal CSIRTや、国や地域全体に関わるセキュリティーインシデントを扱うNational CSIRT（例：JPCERT/CC）、グローバル連携を目的としたFIRST（Forum of Incident Response and Security Teams）などがある。 CSIRTには、さまざまなセキュリティーインシデントに対応するために、情報セキュリティーマネージメントのスキルに加えて、ITインフラやサイバー攻撃、セキュリティー対策などの幅広い知識と高度なスキルを持つ人材が必要となる。さらに、今後は、高度化する攻撃へ対応するために、情報の蓄積・分析、改善策の考案などのインテリジェンスサイクルの実行や、異なる国・文化圏で働くベンダーやサプライヤースタッフとの連絡調整が正確にできる人材が求められる。このためには、「本節（6）❹人材育成」や「2.4.4（6）❷人材育成」でも述べているように、セキュリティーに関する高度なスキルを持つ人材の育成が求められている。

（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と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、横浜国立大学、早稲田大学、電気通信大学、情報通信研究機構などから、日本人が主著の研究論文が採録されるなど、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きている。

				・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きている。
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[10]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	◎	↗	・CISPA Helmholtz Center for Information Security（ドイツ）では国の強力な経済的支援を基に国内外から優秀な研究者が集まり、トップカンファレンスで多数の発表を行うなど、急速に成果をあげている。 ・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および革新的開発を促進するための欧州研究Horizon Europe（2021–2027）がHorizon 2020（2014–2020）に続いて実施されており、セキュリティーは重要な課題として取り上げられている。 ・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）』(2020), https://www.jst.go.jp/crds/pdf/2019/FR/CRDS-FY2019-FR-02.pdf.

2) Joseph R. Biden Jr., “Executive Order on Improving the Nation’s Cybersecurity,” The White House, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/,（2023年2月24日アクセス）.

3）U.S. National Science Foundation, “Secure and Trustworthy Cyberspace（SaTC),” https://beta.nsf.gov/funding/opportunities/secure-trustworthy-cyberspace-satc,（2023年2月24日アクセス）.

4）The Japan Society for the Promotion of Science（JSPS）Washington Office「NSF、高セキュリティ・高信頼性サイバースペースプログラムの下で総額2,540万ドルを助成（8月1日）」https://jspsusa.org/wp/academic_trends/nsf、高セキュリティ・高信頼性サイバースペース/,（2023年2月24日アクセス）.

5）U.S. National Science Foundation, “Collaborative Proposal: SaTC: Frontiers: Enabling a Secure and Trustworthy Software Supply Chain,” https://www.nsf.gov/awardsearch/showAward?AWD_ID=2207008,（2023年2月24日アクセス）.

6）U.S. National Science Foundation, “Collaborative Proposal: SaTC: Frontiers: Securing the Future of Computing for Marginalized and Vulnerable Populations,” https://www.nsf.gov/awardsearch/showAward?AWD_ID=2205171&HistoricalAwards=false,（2023年2月24日アクセス）.

7）U.S. National Science Foundation, “Collaborative Proposal: SaTC: Frontiers: Center for Distributed Confidential Computing（CDCC),” https://www.nsf.gov/awardsearch/showAward?AWD_ID=2207231&HistoricalAwards=false,（2023年2月24日アクセス）.

8）Muwei Zheng, et al., “Cybersecurity Research Datasets: Taxonomy and Empirical Analysis,” in Proceedings of the 11th USENIX Conference on Cyber Security Experimentation and Test（USENIX Association, 2018), 2.

9）Dwight Weingarten, “NIST Releases Roadmap on How to Build Cybersecurity Workforce,” MeriTalk, https://www.meritalk.com/articles/nist-releases-roadmap-on-how-to-buildcybersecurity-workforce/,（2023年2月24日アクセス）.

10）Louis Columbus, “The Top 20 Cybersecurity Startups To Watch In 2021 Based On Crunchbase,” Forbes, November 29, 2020, https://www.forbes.com/sites/louiscolumbus/2020/11/29/the-top-20-cybersecurity-startups-to-watch-in-2021-based-on-crunchbase/?sh=293066926f21.