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