2.4.4 人・社会とセキュリティー

（1）研究開発領域の定義

情報サービスのユーザーの観点からセキュリティーの問題を解決し、社会に受容され人々に活用され、社会を守るセキュリティー技術の研究開発を行う領域である。セキュリティーの観点において、人の脆弱性を狙った攻撃の解決や、情報サービスが実現できることと情報サービスを利用する人が期待することのギャップ（Socio–technical gap）の解決、多数の人・組織の関わりにおいてセキュリティー技術の普及を阻害する要因の解決、法制度などの社会的要請に応えられるセキュリティー技術の設計、情報が社会に拡散することによる影響の分析・対策などが盛んに研究開発されている。

（2）キーワード

ユーザブルセキュリティー、ユーザー調査、EU一般データ保護規則（GDPR）、ダークパターン、Misinformation、Disinformation、ファクトチェック、サプライチェーンセキュリティー、ソフトウェアの透明性（Software Component Transparency）、ソフトウェア部品表（SBOM）、サイバーセキュリティー研究倫理

（3）研究開発領域の概要

［本領域の意義］

インターネットの発展に伴い、多種多様な活動がデジタル化され複雑な相互接続が急速に進む中で、セキュリティー技術の対象は個人・組織・産業などに拡大している。これまで、セキュリティー技術として、サイバー攻撃の検知・対策や脆弱性のないセキュアなシステム・サービスの技術的な実現などが研究されてきた。一方、近年では、ユーザーの認知を標的にする攻撃（フィッシング攻撃やMisinformation・Disinformation）による脅威が増してきた。例えば、フィッシング攻撃では、フィッシングメールやフィッシングサイトを使って人をだまして重要情報を搾取しようとしている。システムへの不正侵入でもフィッシングメールを使って人をだましてパスワードを搾取してシステムに侵入する事例も発生している。また、サプライチェーンは複雑化・グローバル化しており、1つのソフトウェアの脆弱性が世界中のシステムに影響を及ぼす事例もある。さらに、虚偽の情報（Disinformation）を含んだフェイクニュースにより世論が誘導される問題も起こっている。法規制の面では、EU一般データ保護規則（GDPR：General Data Protection Regulation）などのユーザーのプライバシーを保護するための法規制の整備が世界的に進み、情報サービスを取り巻く状況が大きく変わってきており、情報サービスを利用するユーザーに法制度との関係を提示する必要性や、法規制に適合したシステムの開発が求められている。情報サービスを利用するのは人であり、情報システムを開発・運用するのも人である。本研究領域では、セキュリティーに関する技術だけではなく、セキュリティー技術を活用するユーザー（人）、ユーザーが情報サービスを利用する際の社会的・組織的なプロセスやルールにも着目している。この研究開発領域は、これまでのセキュリティー分野の技術に加えて、心理学、経済学などの人文・社会科学を含めた学際的アプローチにより総合的に取り組む必要がある。情報を使った人への攻撃や、それによる組織、社会への影響、情報サービスが実現できることと情報サービスを利用する人が期待することのギャップ、情報サービスの開発・運用の複雑さは、日々、増しており、人・社会に関するセキュリティー技術を確立することは、人々にとって安心・安全に利用できる情報サービスや社会を実現する上で必須である。

［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

セキュリティーは、デバイスやOS、システム、ネットワーク、情報などの守る対象への攻撃を防御するこ

とを主眼としている。一方で、情報サービスを利用するのは人であり、また、情報機器や情報システムを開発・運用するのも人である。サイバー攻撃が多様化する中で、守る対象として人の重要性が高まっている。例えば、フィンシング詐欺の報告件数は、年々増加している。システムへの不正侵入でも、2021年には初期アクセスにフィッシングを悪用する攻撃の割合が41%と、2020年までのシステムの脆弱性を悪用する攻撃を抜いてトップに浮上している[1)]。守る対象として重要性が高まっているもう一つが社会である。近年、サプライチェーンが大規模化、グローバル化しており、ウィルスが混入したソフトウェアがサプライチェーンを介して供給され、多数の企業に影響を与える事例が発生している。例えば、2020 年12月には、米国のネットワーク監視ソフトウェアを提供する会社が攻撃を受け、ウィルスに感染したソフトウェアがサプライチェーンを介して世界中で利用されている同社のシステムに配信され、大きな影響を与えたという報告がある。また、さまざまな製品で利用されているオープンソースソフトウェア（OSS：Open Source Software）でも、脆弱性が発見されると、それを狙った攻撃により多数の製品に被害が及ぶ。2021年4月には、多くの製品やソフトウェアで使用されているOSSに脆弱性が見つかり、世界中の製品が攻撃のリスクに晒された。また、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するようになった。その結果、フェイクニュースと呼ばれる、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。サイバー攻撃や悪意を持った情報操作などは、社会に大きな影響を与えており、今後、情報攻撃からいかに社会を守るかについても考える必要がある。

このような人や社会に関係するセキュリティーとして取り組まれている代表的な技術として、以下では、ユーザブルセキュリティー技術、Misinformation・Disinformationの対策技術、ソフトウェアのサプライチェーンセキュリティー技術について紹介する。

・ユーザブルセキュリティー技術

ユーザブルセキュリティーは、情報サービスを利用する人（ユーザー）を中心にしてセキュリティーやプライバシーの問題解決に取り組む分野である。ユーザーが情報サービスを利用するさまざまなシーンにおいて認識（perception）・行動（behavior）を観測してユーザーを理解することで、ユーザーがより適切な認識や意思決定（decision–making）を行いやすいセキュリティー・プライバシー技術の確立を目指している。

ユーザブルセキュリティーの研究では、ユーザーのより深い理解を試みる社会科学・心理学のアプローチを取り入れた観測が行われる。例えば、ユーザーがセキュリティー技術を十分に活用できていない状況や技術の誤解（misconception）が発生する理由、また、フィッシングなどによって、攻撃者にだまされる原理などを解明することで、専門性が必ずしも高くないユーザーにも十分な恩恵が得られるセキュリティー技術が研究されている。さらには、開発者が脆弱なシステムを作ってしまう原因の理解と、それに基づく開発者のサポート技術の創出、セキュリティー技術者が解析作業を行う際の明文化されていないノウハウ（暗黙知）を形式知化する試み、システム管理者が抱える組織におけるセキュリティー運用の困難さと解決策の模索なども研究対象となっている。

・Misinformation・Disinformationの対策技術

インターネットでは、ソーシャルメディアプラットフォーム（ソーシャルネットワークサービス、コメントの投稿が可能なニュースサイトなど）を中心に虚偽の情報を伴ったコンテンツが投稿され、それら虚偽の情報が受け手により拡散される事象の発生が急増している。 Misinformationは、情報を最初に発信した者に虚偽であることの自認もしくは拡散の意図があるかないかを問わない情報を指し、一方、Disinformationは、最初の発信者に虚偽の自認および拡散の意図があると見なされる情報を指す。これらの事象においては、虚偽の情報が高速かつ幾何級数的な広まりをもって流布され、情報の受け手を扇動することで、時として極めて短時間のうちに国を跨ぐ規模で世論を動かす結果をもたらすことさえある[2), 3), 4)]。このような虚

偽の情報拡散は人々の認識をゆがめ誤った判断を誘発することから、人の認知に対するサイバー攻撃であるとも捉えられる。プラットフォームでは、虚偽の情報拡散を未然に防ぐための介入手段が講じられている。例えば、SNSなどのプラットフォームでは、情報の内容を確認して何らかの対処を行うコンテンツ・モデレーション（Content Moderation）が行われている。コンテンツ・モデレーションでは、信頼性の低いもしくは有害である可能性が高い情報に関して注意を表示するソフトモデレーションと、虚偽であることが明らかである情報や有害であることが明確な情報を削除するハードモデレーションが行われている。

・ソフトウェアのサプライチェーンセキュリティー技術

サプライチェーンは複雑化・グローバル化しており、今日ではプロダクト開発が単一の組織で完結することはまれである。このような背景において、サプライチェーンのセキュリティーリスクは、一つのプロダクトを開発するために、多様な人々や組織によって作り出される構成要素（ソフトウェア/ハードウェアのコンポーネント）の脆弱性に起因するものが多い。

効率的かつ迅速なプロダクト開発においてオープンソースソフトウェア（OSS：Open Source Software）が果たす役割は非常に大きい。一方で、ソフトウェアコンポーネントとして活用されるOSSに脆弱性が発見された場合、この脆弱性は、サプライチェーンにおいて容易にかつ広範囲に波及し、そのソフトウェアコンポーネントを利用するあらゆるプロダクトに影響を及ぼす可能性がある。 OSSに脆弱性が発見された場合、迅速に対応するためには、事前にプロダクトで利用されているソフトウェアコンポーネントを把握しておくことが必要となり、ソフトウェアコンポーネント（特にOSS）を特定・列挙するための技術としてソフトウェア・コンポジション解析（SCA：Software Composition Analysis）が実施されている。

❷ セキュリティー・プライバシーに関する法規制とシステムデザイン

法規制とセキュリティー・プライバシーには密接な関わりがある。特に、2018年に欧州で運用が開始されたGDPRは、個人情報保護を強化するという世界的な潮流を作り、日本の改正個人情報保護法や米国のカリフォルニア州消費者プライバシー法（CCPA：California Consumer Privacy Act of 2018）などにも影響を与えている。

プライバシーに関する法規制と実際のシステム・サービスの運用とのギャップについてはしばしば指摘されている。例えば、Cookieの使用同意では、サービス事業者が同意を得ることだけを目的とするあまり、Cookieの意味や関連する情報がどのように活用されるのかがユーザーに対して十分に説明されていないことや、さまざまな状況でユーザーが同意を求められることで「同意疲れ」が発生していることが指摘されている。また、個人情報を本人の同意なく第三者提供できるオプトアウト提供においても、一般のユーザーにとってオプトアウト提供を停止するための操作が難しい（例えば、Webサイトのトップページから簡単にアクセスできない）という指摘がされており、今後、改善の検討が必要である。

一方で、ユーザーが抱いているプライバシーに関する認識と法規制として定められている内容とのギャップも指摘されている。例えば、GDPRでは、「自動化された個人に対する意思決定とプロファイリング（Automated individual decision-making and profiling）」の中で、個人データを収集分析して判断を行うプロファイリングによる自動意志決定（例えば、常習的なスピード違反かにより罰金額を決める）に関するプライバシー保護を規定している。 GDPRでは、個人データを保護するために適法性・公正性・透明性を原則として挙げているが、ユーザーの視点からの調査では、自動意思決定からいかにして個人データが保護されるかが分かりにくく、上記の原則が十分に実現できていないという報告がある。今後、このような問題に対して、法規則の内容をユーザーに対してわかりやすく提示でき、かつユーザーが使いやすいシステムデザインを実現する取り組みが期待されている[5)]。

さらに、法規制とシステムを開発する開発者の認識との間にもギャップがあることが報告されている。例えば、個人のWebアクセス情報を利用する広告サービスと連携したモバイルアプリを開発する場合、モバ

イルアプリの開発者は広告サービスと連携するためのソフトウェアライブラリーやAPIを利用するだけで開発できる。このため、プライバシー法規制に関する実装内容がブラックボックスとなり、さらに、広告サービスの提供者から提示されるプライバシー法規制の構成や文言も複雑で開発者が十分に理解できないことから、システム開発においてプライバシーに関する法規制が順守されていない場合があることが報告されている。今後、開発者がソフトウェアライブラリーやAPIの内容やプライバシー法規制を理解した上で開発するために、ソフトウェアライブラリーやAPIの開発サポート技術やプライバシー法規制の直感的なドキュメンテーションなどが求められている[6)]。

❸ サイバーセキュリティー研究倫理

サイバーセキュリティーの研究は、その研究行為や研究成果が社会システムやそれを利用する人々に対して、直接的な影響（場合によっては悪い影響も含まれる）を与えうる。十分に前例のない研究対象や研究手法を取り扱う際には倫理的な問題にも直面しやすいため、特に配慮が必要になる。研究者の行動規範として研究者の間で認識され順守されるものが研究倫理であり、これにより研究に対して社会から信頼を獲得するとともに、社会的要請（社会に対する貢献）に応えることができる。特にサイバーセキュリティーに関する研究倫理として、社会との関わりの中での研究行為・成果の説明責任や法令・関連規則などの順守が重要視されている。このような考え方は、2012年に米国・国土安全保障省によりMenlo Reportと呼ばれるセキュリティーを含むICT研究全般の研究倫理原則が発行されて以降、欧米の学術国際会議を中心に認識が広まった[7)]。

サイバーセキュリティーの研究倫理としては、ヒューマンファクターの問題、および脆弱性発見時の責任ある情報開示（responsible disclosure）が頻繁に議論の対象になっている。前者は、研究行為においてユーザーのプライバシーや心身が適切に保護されることが推奨され、後者は脆弱性を発見した際に適切に関係各所に情報が開示され論文発表までに適切な対策が取られることが推奨される。サイバーセキュリティーの国際会議では、このような倫理的配慮はCall for Paperにも記載されるなど必須事項となっており、倫理的配慮がなされていない論文は不採択になる可能性がある。

（4）注目動向

［新展開・技術トピックス］

❶ 多様なユーザーの調査とサポート技術

ユーザブルセキュリティー研究ではユーザー調査によって課題発見や創出したサポート技術の有効性評価が実施される。この際、情報サービスのユーザーとして研究対象になるのは、「エキスパートユーザー」と「エンドユーザー」とに大別される。エキスパートユーザーは、情報サービスを作り出したりその技術を運用や管理したりする人々を指し、開発者、オペレーター（システム管理者、ネットワーク管理者など）、セキュリティー専門家、セキュリティー研究者などが当てはまる。エンドユーザーは、上記のエキスパートユーザーとは異なり、情報サービスの純粋なユーザーを指す。

従来のユーザブルセキュリティー研究の多くはエンドユーザーを対象としていたが、近年ではエキスパートユーザーを対象とした研究が増加傾向にある。エキスパートユーザーを対象とした研究として、例えば、開発者が誤って脆弱なプログラムを作成してしまう要因の分析やセキュア開発のための開発サポート技術、セキュリティー専門家、例えばSOC（Security Operation Center）やCSIRT（Computer Security Incident Response Team）などが直面するセキュリティー運用の現場における課題の明確化と効率的なセキュリティー運用をサポートする技術などが研究されている[8)]。

エンドユーザーには多様な属性が存在しており、近年では特に「at–riskユーザー」と呼ばれる人々に対する研究が盛んに実施されている。「at–riskユーザー」とは、セキュリティー・プライバシー（さらにはセーフティー）に関する被害に遭いやすい人々を指し、例えば、情報リテラシーが低いユーザーや、被害による

リスクが大きいユーザーなどに対する調査と技術的な解決策の検討が進んでいる[9]。このようなより被害に遭いやすい人々への調査の関心が高まっている傾向は、心理学やヒューマンコンピューターインタラクションの分野と同様に、従来のユーザブルセキュリティーが暗黙的に欧米在住者・健常者・十分な教育を受けている人々ばかりを対象として調査されてきたことの裏返しであることを意味している。

❷ Misinformation・Disinformationのファクトチェック技術

Misinformation・Disinformationの広まりを未然に防ぐため、情報拡散の原理の分析、コンテンツの分析、およびその対策方法は、ヒューマンコンピューターインタラクションやソーシャルメディアに関する学術会議において議論されてきたが、近年ではセキュリティー関連の学術会議でも議論の対象になってきている。

Misinformation・Disinformationの疑いがある情報への対策として、コンテンツに対して補助的な情報を付与して注意を促すなどの対策方法（ソフトモデレーションの一種）やその効果が研究され始めており、ソーシャルメディアにおいても実験的な取り組みが始まっている。例えば、COVID–19関係のコンテンツに対して公的機関の情報源のリンクを付与することや、第三者による誤解しやすいコンテンツに対する第三者による事実確認と情報付加機能などがある[10), 11)]。

ファクトチェック（Fact Checking）とは、情報の真偽を検証する行為であり、プラットフォーム事業者やメディア関連団体、ファクトチェック推進団体、行政機関などによって実施されている。特に近年においては、新型コロナウイルス感染症に関する情報発信に関連したファクトチェックの重要性が注目されており、令和3年情報通信白書においても取り上げられている[12)]。

アメリカ国立科学財団（NSF：National Science Foundation）はMisinformation・Disinformation対策に関係する研究開発プロジェクトにファンディングを実施している。例えば、虚偽の情報を迅速に捉えて分析するフレームワークを開発し、実世界で生じる虚偽情報に複数のステークホルダーが協働しながら即時に対処する試み[13)]や、特定の目的をもった意図的な情報操作とその結果もたらされる影響について心理的、社会的、経済的などの側面から分析する試み[14)]などが挙げられる。

❸ ダークパターンと法規制

ユーザーが無意識のうちに自身に不利な行動を取るように誘導するデザインのことをダークパターンと呼ぶ。このダークパターンを利用してユーザーから金銭、プライバシーデータ、注意・依存性を引き出す事象が多発している。例えば、有料プログラムを無料プログラムよりも目立たせることで、ユーザーを有料プログラムに誘導するものや、値引きオファーとカウントダウンタイマー（実際はカウントダウンタイマーが切れた後も値引きが有効）とを合わせて表示することでユーザーに購入を促すものなどがある。このようなダークパターンは30年も前から観測されており、小売業界などで日常的に行われている欺瞞的慣行であった。ダークパターンではナッジ（Nudge：行動科学に基づいてユーザーをある行動に導くために後押しをするアプローチ）が悪用されている場合もある[15)]。

ダークパターンにより生じる消費者の不利益を防ぐため、法によってダークパターンを規制する動きも存在する。例えば、米国カリフォルニア州では2021年、既存のカリフォルニア州消費者プライバシー法（CCPA：California Consumer Privacy Act）にダークパターンの使用を禁止する項目を追加した。カリフォルニア州ではダークパターンの使用が特定された場合、当該サービス主体の組織に状況の是正が求められ、その後一定期間を経過しても改善が認められない場合は罰金が科される。

❹ ソフトウェア部品表（SBOM：Software Bill Of Materials）

サプライチェーンセキュリティーにおいて、プロダクトに利用されているソフトウェアの透明性（software component transparency）の担保が重要視されている。ソフトウェアの透明性を担保するための方法と

して、ソフトウェアコンポーネント（プロダクトが内包するコンポーネント、ライブラリー、モジュールなど）を部品表としてまとめたSBOM（Software Bill of Materials）が提案されている。2021年5月に米国大統領により「サイバーセキュリティー強化のための大統領令」[16]が発されたことにより、ソフトウェアサプライチェーンに関するセキュリティーの向上に資するガイドラインの策定やSBOMの発行の必須化などが米国連邦政府の公式な取り組みとして定められた。これに伴い2021年7月、米国商務省・国家電気通信情報局（NTIA：National Telecommunication and Information Administration）がSBOMに記載すべき最小要素を規定する文書[17]を公開した。また2022年2月、米国・国立標準技術研究所（NIST：National Institute of Standards and Technology）は、ソフトウェアの購入者にSBOMを提供することの必要性を含んだ文書[18]を公開している。このような動きを受け、日本でもSBOMに関する検討が進められており、経済産業省では「サイバー・フィジカル・セキュリティー確保に向けたソフトウェア管理手法等検討タスクフォース」にてSBOMの作成・共有・活用などに関する議論およびそれらの実証に向けた検討が進められている[19]。

SBOMを生成・管理することは、ソフトウェア開発者にとってのソフトウェア脆弱性管理のメリット[20]、およびソフトウェア使用者によるセキュリティー対策に有効な情報となるメリットがある。 SBOMの導入・活用にはサプライチェーンのリスクを根本から低減する効果が想定されており、活用が期待されている。

❺ 倫理的なサイバーセキュリティー研究のサポート

日本国内においては2016年頃から、各研究コミュニティーにおいて、サイバーセキュリティーの研究倫理に関する認識状況の確認や課題の整理、アクションプランの考案などを行う動きが広まった。2018年には、日本学術振興会サイバーセキュリティ第192委員会にワーキンググループが設置され、以後研究分野全体を横断する形で啓発活動が推進されている。これらの動向に伴い、研究倫理上配慮すべき具体的項目の整理や、個別の研究事例について妥当性を相談する場の開設が行われるようになった。例えば、サイバーセキュリティー分野における国内最大級の学術シンポジウムである「コンピュータセキュリティシンポジウム（CSS：Computer Security Symposium）」においては、2018年に研究倫理相談窓口が開設され、2019年には「サイバーセキュリティ研究における倫理的配慮のためのチェックリスト」[21]が整備され、研究論文の投稿者は同リストの活用により倫理的配慮のセルフチェックが可能になっている。

［注目すべき国内外のプロジェクト］

❶ Security Behavior Observatory（カーネギーメロン大学）

カーネギーメロン大学（CMU：Carnegie Melon University）は、プライバシーとセキュリティーについての意思決定に関連するユーザーの行動を調査するプロジェクト「Security Behavior Observatory（SBO）」を実施している[22]。SBOでは、同プロジェクトに参画したユーザーの端末にデータ収集ソフトウェアをインストールし、Webブラウザーやネットワークトラフィック、ファイルシステムなどのさまざまな要素のモニタリングを常時行い、モニタリング結果を同プロジェクトのサーバーに集約している。 SBOはこれらのデータを用いて、ユーザーがコンピューターを短期的および長期的に使用する際に日常的に直面する問題を理解することを目的としている。

❷ Web媒介型攻撃対策技術の実用化に向けた研究開発（WarpDriveプロジェクト）（NICT）

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、Webを媒介する攻撃への対策として、ユーザーに配布するエージェント型アプリケーションを介して悪性サイトの閲覧履歴の収集および閲覧時の警告を行うプロジェクト「WarpDrive（Web媒介型攻撃対策技術の実用化に向けた研究開発）」を実施した[23, 24]。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の研究開発の一つとして継続して実施されている。悪性サイト

閲覧時の警告の他にも、ユーザーのネットワーク環境において攻撃に遭いやすいポートの開放・サービスの稼働があった場合に注意喚起の通知を実施する試みや、悪性サイト閲覧直前のアクセスログから、その後悪性サイトに至る危険性の高い検索行為、およびその際に用いられる検索単語を割り出し、その単語を用いて新たに検索を行うユーザーにその危険性を通知する試みなど、新たな視点での警告や注意喚起のあり方が検討されている。このような取り組みを通して今後の研究の基礎となる有用なデータが蓄積されてきている。

❸ am I infected?（横浜国立大学）

横浜国立大学 情報・物理セキュリティー研究拠点では、総務省の電波資源拡大のための研究開発における委託研究「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、上記WarpDriveプロジェクトとも連携して、令和4年2月より家庭向けルーターやウェブカメラなどのIoT機器がマルウェアに感染しているかもしくは脆弱性を有するかを診断するサービス「am I infected?」を運営している[25)]。当該サービスを訪れたユーザーは、Webサイトに自身のメールアドレスと現在のネットワーク環境（自宅・勤務先など）を入力するだけで、即時に感染・診断を受けて診断結果を確認することができ、診断対象のネットワークに問題が発見された場合は、当該サービスの運営側から利用ユーザーに対して推奨される対策が提供される仕組みとなっている。この取り組みを通して、感染と対策を通知したユーザーの行動（対策するか、放置するか）やユーザーが対策する際に持つ疑問点、ユーザーへの通知方法によるユーザーの行動の違いなどの有益なデータが蓄積されていきている。

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（NOTICE）（総務省およびNICT）

総務省はNICTおよびインターネットプロバイダーと連携して平成31年2月より、サイバー攻撃に悪用されるおそれのある機器の調査および当該機器のユーザーへの注意喚起を行う取り組み「NOTICE（National Operation Towards IoT Clean Environment）」を実施している。安易なパスワード設定により容易に管理権限を奪取されるおそれのあるIoT機器を特定し、インターネットプロバイダーを介して該当機器のユーザーに電子メールや郵送などによる注意喚起を行う。注意喚起の内容照会や機器の設定変更のサポートをユーザーが希望した場合に応じるサポートセンターも設置されている。問題のある機器を適切な設定に修正するまでの操作は、通常、複数の手順を含んでおり、特に技術的な知識が豊富でないユーザーにとっては複雑かつ不可解である。 NOTICEでは、インターネットプロバイダーや関係機関が連携して知見を蓄え、ユーザーが円滑に対策行動を起こせるよう平易かつ正確に説明を行う通知手法が検討され、有益なデータが蓄積されてきている。

❺ サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）

サプライチェーンの脆弱性は、ある一企業の製品で発見された問題が、同時に、その製品を利用している多数の企業の製品に共通した問題として発展し、大規模な被害をもたらす危険性がある。そのため、組織間で脆弱性の具体事例や、その脆弱性に対して起きうるサイバー攻撃の手法などを共有・整理し、継続的に予防策と対応策を講じることが肝要となる。この課題に対処する取り組みとして、令和2年11月に経済産業省が中心となり、「サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）」が設立されている[26)]。 SC3では、中小企業を含めた産業サプライチェーンに関わる組織が多数参加し、サイバー攻撃事案に関する情報共有、機微な技術情報などを含む場合の関係者への報告、攻撃による被害が不特定多数に及ぶ可能性がある場合の事案公表に関する取り組みを推進している。また、サイバーセキュリティー人材の育成や、学術研究機関におけるサイバーセキュリティー対策の強化などを行うWGを設立し、産学官の連携も推進している。

❻ 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））

コグニティブセキュリティー（Cognitive Security）は、認知を意味するコグニティブ（Cognitive）とセキュリティーを合わせたものであり、フィッシング攻撃など人の心理的な隙やミスにつけ込むソーシャルエンジニアリングや、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に対処するための技術の一つである。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、近年注目されている。DARPA（Defense Advanced Research Projects Agency）では、画像・動画の改ざんやフェイクの検知[27]、ソーシャルエンジニアリングの検知・防御[28]、情報拡散による社会への影響の認知と対策[29] に関する研究開発プロジェクトが推進されている。

（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 ユーザー調査のためのユーザー募集方法

ユーザブルセキュリティー研究では、実際のユーザーに対して認識や行動を調査することで、問題の発見や対策技術の有効性が評価される。その際にまず参加者の募集が行われるが、調査対象のユーザーをピンポイントで募集することの難しさがある。多くのユーザー調査では、クラウドソーシングサービスを利用して大規模に募集されるが、このようなサービスに登録しているユーザー層と調査対象のユーザー層に乖離が発生しやすい。このような問題は参加者募集が難しいユーザーになるほど顕著になりやすく、特に近年の傾向であるエキスパートユーザーを対象にした研究や、エンドユーザーの中でもアットリスク・ユーザー（at-risk user）を対象にした研究においては、適切な実験参加者を集めること自体が容易ではない。そのため、一般的に、研究者の身近にいる人々を実験参加者として募集する便宜的標本抽出法（Convenience Sampling）が実施されることが多く、そのような場合においては母集団の代表性があるとは必ずしも言えない。ユーザー募集を円滑に進めるために、調査対象となるユーザーがいる組織との連携体制の構築やユーザーが安心して調査に参加できるよう調査データのセキュリティーが確保されプライバシーが保護されるデータ管理基盤を作ることが必要と考えられる。

❷ 適切なユーザー調査手法

ユーザー調査手法として、ラボ実験、サーベイ（アンケート）、インタビューなどが一般的に用いられるが、セキュリティーやプライバシーに関する調査を実施する際、参加者に対してさまざまなバイアスがかかりやすい状況があることが知られている。例えば、ラボ実験において、実験参加者に実験の趣旨を説明しすぎることで実験参加者が研究者の期待に応えようと行動してしまうホーソン効果（Hawthorne Effect）が発生したり、普段とは異なる人工的な環境で作業をすることで本来の自然な行動を観測できない生態学的妥当性（Ecological Validity）が低い事象が発生したりする。これらは、実験が日常生活で行っている行動と照らし合わせて意味のあるものになっているかという観点において、問題視されている。例えば、フィッシングメールに対する反応を調査する場合、実験前に実験参加者にフィッシングメール判別であることを説明しすぎると普段以上に警戒した行動を取りやすくなり、普段の環境でのフィッシングメールに対する自然な反応を観測することが難しくなる。他にも、サーベイやインタビューなどでは、本来とは異なる社会的に望ましいとされる回答をする「社会的望ましさバイアス（Social Desirability Bias）」や、言い回し（Wording）による回答のバイアスが発生しやすい。このようなバイアスが含まれにくい調査方法の設計や、生態学的妥当性を向上するための調査方法の確立が求められる。

❸ Misinformation・Disinformationの介入技術

Misinformation・Disinformationが発生しやすい状況として、ユーザーの行動分析に基づくパーソナ

ライズされた推薦アルゴリズムによって提示された偏った情報に囲まれてしまうフィルターバブル（Filter Bubble）や、価値観の似た考えを持つユーザーで形成される狭いコミュニティーにおいて自分の意見が増幅・強化されるエコーチェンバー（Echo Chamber）などが知られている。このような状況を改善するために、ユーザーに対して自身とは異なる意見の情報を提示するなど、多様な情報・意見を提示することで客観性を持たせるための効果的な介入手段を実現することが課題となっている。 Misinformation・Disinformationが発生しやすい話題の一つとして政治があるが、誤った情報を拡散するユーザーに対して公の場で訂正行為（Debunking）を行う場合、そのユーザーの党派性や言葉の有害性が高まり、コンテンツの正確性から注意が逸れてしまうという逆効果（Backfire Effect）が発生することが知られている。今後、介入手段が効果を発揮する適切な状況や方法についてのさらなる調査が期待される[30)]。

❹ ダークパターンの定義と検知

企業が収益を重視するあまり、意図せず自社のサービスにダークパターンを含めて設計してしまう場合がある。米国やフランスでは、ダークパターンに対して法的な規制が始まっているが、実際の対策は十分とは言えない状況である。一方で、一部のダークパターンについて実態調査と問題指摘がされている。例えば、ウェブサイトにおけるオプトアウト提供やサブスクリプション解除の設定の難しさの定量的な調査や、ユーザーが設定しやすい推奨されるウェブサイトの設計が提案されている。しかしながら、調査対象となるダークパターンやユーザーは限定的であり、将来的にはダークパターンの先鋭化も想定されるため、ユーザーへの影響の幅広い調査・評価、ダークパターンの定義や識別方法を明確化する取り組みが必要である。

❺ ユーザーへの効果的なセキュリティー注意喚起

セキュリティーの問題をユーザーに効果的に通知する方法の研究が盛んに取り組まれている。 Webブラウザーにおいて問題があるWebサイトにアクセスする場合に表示されるセキュリティー警告画面（例えばTLSに不備があるWebサイト）はユーザーによって無視されることが多いことが知られている。専門性が高くないユーザーであっても脅威の内容が理解しやすいテキスト・アイコン・レイアウトなどに改良することが課題になっている。

一方で、直接的にセキュリティーの注意喚起を通知することが難しい事例もある。インターネット上をスキャンするツール（Zmap、Masscanなど）やWebサービス（Shodan、Censysなど）によってインターネットにつながる脆弱なデバイスを早期に発見できるようになったものの、デバイス所有者との直接的なコミュニケーション方法が存在しないため、発見した問題の対策を依頼できないという問題がある。デバイス所有者と間接的にコミュニケーションする方法としては、デバイスのIPアドレスを管理している組織（インターネットサービスプロバイダー（ISP）やホスティングサービスプロバイダー）や当該IPアドレスが属する国のナショナルCSIRTを介してコミュニケーションする方法がある。しかし、デバイス所有者が判明しない事例も多く、判明したとしても多少の差異はあるものの、どのコミュニケーション方法であってもデバイス所有者からの反応は高くないことが知られている。コミュニケーション方法の確立やデバイス所有者への適切な通知方法について検討が必要である。

❻ OSSプロジェクトに対する攻撃の対策

近年のプロダクト開発においてOSSは基本的な機能を実現する上で欠かせない存在であるが、OSSプロジェクトに対する攻撃も確認されており、OSSに脆弱性や攻撃コードが混入しやすいことが明らかになっている。例えば、コードリポジトリのフォークやクローンに悪性なコードを挿入する事例が多く発見されている[31), 32)]。例えば、2020年から2021年にかけて、Linux Kernel開発コミュニティーに対して大学研究者が「善意の開発者」を装って脆弱なコードをコミットする実験を実施したことが大きな問題になった[33)]。この研究者はOSSにおけるコードレビュープロセスの問題点を発見することを目的にしていたものの、調査方

法自体は開発コミュニティーには受け入れられず、開発コミュニティーは研究者によってコミットされた全てのコードを再検証するために膨大な人的コストを負うことになった。この研究ではくしくも、OSSプロジェクトにおいて悪意のある開発者・コードが入り込む余地があることを広く知らしめることになった。このように、OSSの開発においてもセキュアな開発を行うために、開発段階におけるコードを悪意のある開発者から保護することが課題になっている。

（6）その他の課題

❶ 法規制

近年、無料サービスを提供するプラットフォーム事業者が増加しており、こういったプラットフォーム事業者は、取得・集積したユーザー情報を利用して、ユーザーに対して商品・サービスなどの推薦を幅広く行っており、ユーザーにとっては利便性向上の一助にもなっている。一方で、ユーザーはその趣旨と方法を正しく理解しないまま情報を取得・利用され、また無自覚・無意識のうちに推薦の結果に影響される可能性がある。

総務省が主催する「プラットフォームサービスに関する研究会」（2018年10月～）では、検討対象の一つとして電気通信事業者と国内外のプラットフォーム事業者における、ユーザー情報（通信の秘密やプライバシー情報など）の取扱状況、およびそれらに対するルールなどの差異について検討を行っている[34)]。これまで当該問題については、電気通信事業法の観点から、主に通信の秘密に関して電気通信事業者やその設備に着目して法規制の議論がなされてきたが、今後は電気通信サービスのユーザーのプライバシー保護も電気通信事業法の目的の範疇とし、ユーザー情報を取り扱う者全てが保護すべき義務を負う形での法整備が必要である旨の課題提言が行われ、検討が進められている。また、ユーザーによる理解促進も課題の一つとして捉えられており、ユーザーのリテラシー向上にむけた周知啓発の推進や、事業者のプライバシーポリシーの外部レビュー実施（分かりやすい通知もしくは公表であるか、同意取得の方法は適切か、など）も検討が進められている。

❷ 人材育成

独立行政法人情報処理推進機構（IPA：Information-technology Promotion Agency）では、平成29年4月に「産業サイバーセキュリティセンター（Industrial Cyber Security Center of Excellence）」を設立し、情報系・制御系システムを想定した模擬プラントを用いた演習や、攻撃防御の実践経験、攻撃情報の調査・分析などを通じて、重要インフラや産業基盤を狙ったサイバー攻撃への対策の中核となる人材を育成している[35)]。産業サイバーセキュリティーの実務担当者やCEO、CIO・CISO、部門長などの責任者クラスなど、多岐にわたる対象者に向けた育成プログラムが提供されており、毎年、さまざまな業界からの参加者が修了している。修了後も修了者間で最新の知見に基づいた情報交換が可能なコミュニティーが設けられており、業界を横断した制御システムセキュリティーの連携体制が構築されている。この人材育成の取り組みにおいては、インシデント発生時、インシデントへの対処のみでなく原因調査、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を実行できる人材や、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をどのように育成していくかが課題として捉えられている。また、今後は必ずしもIT・セキュリティーの専門知識や業務経験を有していない人材であってもセキュリティー専門人材との協働が必要となる場面があり得るため、そのような際に追加して習得しておくべき知識「プラス・セキュリティー知識」をいかにして従前に補充するか、ひいてはそのための人材育成プログラムをどのように整理するかが課題として捉えられている。

（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	○	↗	・国内ではユーザブルセキュリティーの研究コミュニティーが2017年に立ち上がり、大学や企業の研究発表数も増加傾向にある。 ・国際会議での存在感も徐々に増してきており、直近では、EuroUSEC 2021でBest Paper Awardを早大/NTTが受賞している。 SOUPSでは日本から2015年に1件（早大/NTT）、2021年に1件（NTT/早大）、2022年に3件（東大、KDDI/CMU、NTT/早大）採択されている。 ・サイバーセキュリティー研究倫理について、国内学会でチェックリストの整備や相談窓口の設置などサポート体制の充実が確認できる。
	応用研究・開発	△	↗	・ユーザーの行動観測やユーザーに対する注意喚起などを実施するいくつかのプロジェクトが始動しており、今後の研究成果や社会実装が期待できる。
米国	基礎研究	◎	→	・米国はユーザブルセキュリティーの黎明期から研究分野をけん引・発展させてきた。中心的な研究グループが属するCMU Cylabや、そのOB/OGの多くが米国の各大学（メリーランド大、シカゴ大など）で研究チームを作り、本分野をけん引している。
	応用研究・開発	◎	→	・ユーザブルセキュリティーの研究成果はNISTなどのガイドライン（NIST SP800-63Bなど）に取り入れられて、米国だけでなく、欧米や日本などでも広く参照されている。 ・SBOMの仕様策定や普及推進活動が活発に行われている。
欧州	基礎研究	◎	↗	・GDPRを後押しに、ここ数年で多数の研究成果をあげている。またユーザブルセキュリティーに関して有力な研究グループが増加しており、UKに加えて、ドイツの複数の研究グループの成果が顕著である。
	応用研究・開発	◎	↗	・GDPRによるプライバシーの規制は、プライバシーポリシーやCookieなどインターネット上でのビジネス活動に大きな影響を与えている。またEUに限らず、米国や日本などに対してもビジネス/法規制の面で大きな影響を与えている。
中国	基礎研究	×	→	・顕著な成果はみられない。
	応用研究・開発	×	→	・顕著な成果はみられない。
韓国	基礎研究	△	→	・ユーザブルセキュリティーに関する国際会議発表がいくつか確認できる。
	応用研究・開発	×	→	・顕著な成果はみられない。

（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) IBM, “IBM Security X-Force Threat Intelligence Index 2023,” https://www.ibm.com/reports/threat-intelligence/jp-ja/,（2023年2月24日アクセス）.

2) Claire Wardle, “Information disorder: Toward an interdisciplinary framework for research and policy making（2017）,” Council of Europe, https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-

making.html,（2023年2月24日アクセス）.
3) Directorate-General for Communications Networks, Content and Technology, “A multi-dimensional approach to disinformation,” European Commission, https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1,（2023年2月24日アクセス）.
4) House of Commons, Digital, Culture, Media and Sport Committee, “Disinformation and ‘fake news’: Final Report, Eighth Report of Session 2017-19,” UK Parliament, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf
5) Smirity Kaushik, et al., ““How I Know For Sure”: People's Perspectives on Solely Automated Decision-Making（SADM）,” in the Proceedings of the Seventeenth Symposium on Usable Privacy and Security（USENIX Association, 2021）, 159-180.
6) Mohammad Tahaei, et al., “Charting App Developers’ Journey Through Privacy Regulation Features in Ad Networks,” in Proceedings on Privacy Enhancing Technologies Symposium（De Gruyter Open Ltd., 2022）, 33-56.
7) U.S. Department of Homeland Security, “The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research, August 2012,” https://www.dhs.gov/sites/default/files/publications/CSD-MenloPrinciplesCORE-20120803_1.pdf,（2023年2月24日アクセス）.
8) Mannat Kaur, et al., “Human Factors in Security Research: Lessons Learned from 2008-2018,” arXiv, https://doi.org/10.48550/arXiv.2103.13287,（2023年2月24日アクセス）.
9) Noel Warford, et al., “SoK: A Framework for Unifying At-Risk User Research,” in 2022 IEEE Symposium on Security and Privacy（SP）（IEEE, 2022）, 2344-2360., https://doi.org/10.1109/SP46214.2022.9833643.
10) Twitter, Inc.「TwitterのBirdwatchについて」https://help.twitter.com/ja/using-twitter/birdwatch,（2023年2月24日アクセス）.
11) Twitter Japan「ファクトチェック機能「Birdwatch」をさらに充実」https://blog.twitter.com/ja_jp/topics/product/2022/building-a-better-birdwatch_2022,（2023年2月24日アクセス）.
12) 総務省「情報通信白書令和3年版」https://www.soumu.go.jp/johotsusintokei/whitepaper/r03.html,（2023年2月24日アクセス）.
13) U.S. National Science Foundation（NSF）, “Collaborative Research: SaTC: CORE: Large: Rapid-Response Frameworks for Mitigating Online Disinformation,” https://www.nsf.gov/awardsearch/showAward?AWD_ID=2120496&HistoricalAwards=false,（2023年2月24日アクセス）.
14) Sylvia Butterfield, Kellina M. Craig-Henderson and Margaret Martonosi, “Inviting Proposals Related to Information Integrity to the Secure and Trustworthy Cyberspace Program,” U.S. National Science Foundation（NSF）, https://beta.nsf.gov/funding/opportunities/inviting-proposals-related-information-integrity-secure-and-trustworthy,（2023年2月24日アクセス）.
15) Arvind Narayanan, et al., “Dark Patterns: Past, Present, and Future: The evolution of tricky user interfaces,” Queue 18, no. 2（2020）: 67-92., https://doi.org/10.1145/3400899.3400901.
16) 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）.
17) The United States Department of Commerce, “The Minimum Elements For a Software

Bill of Materials（SBOM）：Pursuant to Executive Order 14028 on Improving the Nation's Cybersecurity, July 12, 2021," National Telecommunications and Information Administration（NTIA）, https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf,（2023年2月24日アクセス）.
18) National Institute of Standards and Technology（NIST）, "Software Supply Chain Security Guidance Under Executive Order（EO）14028, Section 4e, February 4, 2022," https://www.nist.gov/document/software-supply-chain-security-guidance-under-executive-order-eo-14028-section-4e,（2023年2月24日アクセス）.
19) 経済産業省「サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース」https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/index.html,（2023年2月24日アクセス）.
20) Stephen Hendrick「SBOM（ソフトウェア部品表）とサイバーセキュリティへの対応状況（2022年1月）」The Linux Foundation, https://www.linuxfoundation.jp/wp-content/uploads/2022/05/LFResearch_SBOM_Report-ja.pdf,（2023年2月24日アクセス）.
21) CSS2019研究倫理委員会「コンピュータセキュリティシンポジウム2019：サイバーセキュリティ研究における倫理的配慮のためのチェックリスト」International Workshop on Security（IWSEC）, http://www.iwsec.org/css/2019/files/ethics_list.pdf,（2023年2月24日アクセス）.
22) Societal Computing, "Security Behavior Observatory," Carnegie Mellon University, https://sc.cs.cmu.edu/research-detail/146-sbo,（2023年2月24日アクセス）.
23) WarpDrive, https://warpdrive-project.jp,（2023年2月24日アクセス）.
24) 国立研究開発法人情報通信研究機構（NICT）「高度通信・放送研究開発委託研究：Web媒介型攻撃対策技術の実用化に向けた研究開発」https://www.nict.go.jp/collabo/commission/k_190.html,（2023年2月24日アクセス）.
25) 横浜国立大学「am I infected?」https://amii.ynu.codes,（2023年2月24日アクセス）.
26) サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）, https://www.ipa.go.jp/security/sc3/,（2023年2月24日アクセス）.
27) William Corvey, "Semantic Forensics（SemaFor）," Defense Advanced Research Projects Agency（DARPA）, https://www.darpa.mil/program/semantic-forensics,（2023年2月24日アクセス）.
28) Bernard McShea, "Active Social Engineering Defense（ASED）," Defense Advanced Research Projects Agency（DARPA）, https://www.darpa.mil/program/active-social-engineering-defense,（2023年2月24日アクセス）.
29) Brian Kettler, "Influence Campaign Awareness and Sensemaking（INCAS）," Defense Advanced Research Projects Agency（DARPA）, https://www.darpa.mil/program/influence-campaign-awareness-and-sensemaking,（2023年2月24日アクセス）.
30) Mohsen Mosleh, et al., "Perverse Downstream Consequences of Debunking: Being Corrected by Another User for Posting False Political News Increases Subsequent Sharing of Low Quality, Partisan, and Toxic Content in a Twitter Field Experiment," in Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems（New York: Association for Computing Machinery, 2021）, 182., https://doi.org/10.1145/3411764.3445642.
31) Alan Cao and Brendan Dolan-Gavitt, "What the Fork? Finding and Analyzing Malware in GitHub Forks," Network and Distributed System Security Symposium 2022, https://www.ndss-symposium.org/ndss-paper/auto-draft-275/,（2023年2月24日アクセス）.

32) Check Point Software Technologies Ltd., “Github “Supply Chain” Attack,” https://blog.checkpoint.com/2022/08/03/github-users-targeted-in-supply-chain-attack/,（2023年2月24日アクセス）.
33) Thorsten Holz and Alina Oprea, “IEEE S&P’21 Program Committee Statement Regarding The “Hypocrite Commits” Paper,” IEEE Computer Society Technical Community on Security and Privacy, https://www.ieee-security.org/TC/SP2021/downloads/2021_PC_Statement.pdf,（2023年2月24日アクセス）.
34) 総務省「プラットフォームサービスに関する研究会」https://www.soumu.go.jp/main_sosiki/kenkyu/platform_service/index.html,（2023年2月24日アクセス）.
35) 独立行政法人情報処理推進機構（IPA）「産業サイバーセキュリティセンター」https://www.ipa.go.jp/icscoe/,（2023年2月24日アクセス）.