2-3-3　ユーザブルセキュリティ
2-3-3　Usable Security: Overview and Case Studies

藤田 彬　長谷川 彩子　松田 美慧　鈴木 悠　笠間 貴弘
FUJITA Akira, HASEGAWA Ayako, MATSUDA Misato, SUZUKI Haruka, and KASAMA Takahiro

本稿では、人と社会のセキュリティに関わる学問分野のうち、特にユーザブルセキュリティ分野及び関連する分野における研究対象を解説し、サイバーセキュリティ研究室における当該分野での研究開発の成果を紹介する。

In this paper, we describe our research interests in human and social security, particularly usable security and related fields of study, and present the results of research and development in these fields at the Cybersecurity Laboratory.

1　まえがき

インターネットが普及し、生活に欠かせないインフラとなり、人々の様々な活動がデジタル化される中、セキュリティ技術は主にサイバー攻撃の発見や防御を行うシステムやセキュアな情報サービスの実現に焦点を当てて進化を遂げて来た。しかしながら近年、人（ユーザ）の認知を標的にする攻撃（フィッシングやMisinformation/Disinformation など）が増加しており、サービスやシステムへのセキュリティ対策のみでは低減できない脅威が顕在化してきている。例えば、フィッシング攻撃はメールやウェブサイトを通じて偽の入力フォームをもった画面にユーザを誘導し、正規性を信じて情報を入力したユーザから個人情報や銀行口座情報などを窃取する攻撃であるが、問題となる画面は基本的に通常のウェブページと同様の仕組みをもっているため、非正規性を自動的な手法で見抜くことには技術的な困難が伴う。ユーザが騙されないで済むか否かは、ユーザが気づけるか否か、ひいてはユーザの認知の状況に、その成否が強く依存する攻撃手法といえる。

ユーザブルセキュリティはこのような、ユーザが情報サービスを利用する際の認知や、情報サービス自体のプロセスやルールに焦点を当て、セキュリティとプライバシーの課題に取り組む研究開発領域である。当該領域では、社会科学や心理学の手法を取り入れてユーザの行動や認識を観察し、理解することで、より適切なセキュリティとプライバシーの選択を行いやすくする技術の実現を目指している。例えば、ユーザがセキュリティ技術を適切に利用できない理由や技術の誤解が生じる原因の追究、フィッシングなどの手法がなぜ成功するのか（ユーザが攻撃者の仕掛けた罠にかかってしまうか）を明らかにするなど、多くのユーザに有益な、ユーザの情報サービス及びICT に関する専門知識の有無に関わらず適用可能なセキュリティ技術の研究がなされている。また、ユーザブルセキュリティ領域が「ユーザ」として取り上げる対象には、ここまで述べたような情報サービスの純粋なユーザであるいわゆる「エンドユーザ」に限らず、情報サービスを構築し、運用または管理する人々やセキュリティの専門家、研究者などの「エキスパートユーザ」も含む。情報サービスの開発者が脆弱（ぜいじゃく）なシステムを構築する原因を理解し、それに対する開発者の支援技術を作り出したり、セキュリティ専門家が暗黙の知識を形式化し、システム管理者が組織内でセキュリティ運用の課題を解決するための策を模索するなど、様々な課題が研究されている。

ユーザブルセキュリティはこのように人と社会のセキュリティを取り扱う領域といえるが、目標に共通する部分のある領域として 1）Misinformation/Disinformation の対策技術と 2）ソフトウェアサプライチェーンセキュリティ技術が挙げられ、いずれも昨今の社会的な問題に関わる技術として注目されている。

インターネットでは、主にソーシャルメディアプラットフォームを中心に、虚偽情報を含むコンテンツが急速に増え、それらが拡散される現象が顕著になっている。Misinformation は、虚偽であると知らずに発信・共有された情報を指し、一方、Disinformation は、意図的に発信・共有された虚偽または操作された情報を指す。虚偽情報は非常に短時間の間に広まることが

あり、受け手の意識や判断に影響を与え、時には国を超えた規模で世論を動かすことさえある。このようにMisinformation 及び Disinformation の拡散は、人々の認知をゆがめ、誤った意思決定を促す効果をもつことがあり、人の認知に対するサイバー攻撃と見なされることもある。SNS のプラットフォーム及びその事業者においては、虚偽情報の拡散を防止するための手段が講じられている。例えば、一部の SNS などでは、コンテンツの信頼性が低いもしくは有害であると見なされる場合に注意を喚起するソフトモデレーションや、虚偽であることが明らかな情報や有害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。これらの対策は人手による判断、自動手法による判断の両方に基づいて行われていると考えられるが、いずれもテキスト及びコンテンツへの深い意味理解と、人の認知上の特性の理解が必要となるため、技術的にいっても高度なタスクといえる。

ソフトウェアサプライチェーンについても、虚偽情報の拡散と同様、社会全体への影響が大きい点で重要な研究対象といえる。昨今のソフトウェアプロダクトは、単位の組織によりフルスクラッチで制作されることは少なく、多くの場合、オープンソースソフトウェア（OSS）や他組織による開発物を用いて複数の組織の開発者が連携し、サプライチェーンを形成しながら、効率的に開発及び改良が進められる。この時、オープンソースソフトウェアや関連する組織での開発体制に脆弱性やセキュリティ上の問題が見つかった場合、その脆弱性や問題はサプライチェーン全体に広がり、多くのプロダクトに影響が及ぶ可能性がある。このようなリスクに対処することは、開発対象のプロダクトに使われるソフトウェアコンポーネントを把握しながら開発を進めるための手法、もしくは完成したプロダクトから使用されているコンポーネントを把握する手法、また、開発に携わる人のセキュリティに対する意識を維持するための施策など様々な技術的要素をもった研究上の課題を含む。

サイバーセキュリティ研究室でユーザブルセキュリティの研究開発に関わるメンバ（以下、USEC チーム）は、ユーザブルセキュリティ領域の研究を中心にしながら、厳密にユーザブルセキュリティとカテゴライズされる領域に留まらず、関係する Misinformation/Disinformation の対策技術やソフトウェアサプライチェーンセキュリティ技術も研究対象に含め、広い視野で、人と社会のセキュリティに関わる研究開発を行っている。

2　サイバーセキュリティ研究室 USEC チームの研究開発成果

当室 USEC チームのメンバがこれまでに行ってきた研究を紹介する。はじめに、エンドユーザがセキュリティを確保するために、自ら対策行為を実施する際にユーザが直面している課題を明らかにし、専門家やサービス提供者が実施すべき対策について検討した研究を 4 件紹介する。次に、エキスパートユーザがセキュリティ対策の実施を行う際や実態調査をする際の課題を実証して解決に向けた提言を行った研究を 1 件紹介する。最後に、ユーザブルセキュリティ分野の方法論に関する研究を 1 件紹介する。

2.1　エンドユーザに関する研究

エンドユーザ向け Q&A サイトに投稿されたセキュリティ及びプライバシーに関する質問の分析：長谷川らは、セキュリティの非専門家である一般ユーザが日

表 1　Q&A サイトに投稿された質問のテーマ（トピック）とその頻度及び各テーマにおける頻出名詞

Theme	Frequency	Top 10 Nouns
Cyberattack	40.7 %	website, virus, password, fraud, information, email, account, infection, phone number, smartphone
Authentication	16.2 %	login, authentication, password, account, phone number, Google, iPhone, code, screen, two-step
Security software	13.0 %	security, computer, website, Windows, Norton, Virus Buster, smartphone, software, screen, McAfee
Privacy abuse	7.9 %	smartphone, friend, account, LINE, information, privacy, password, history, Twitter, Instagram
Account and device management	7.0 %	account, iPhone, password, device, login, setting, factory reset, email address, data, iCloud
Secure connection	6.5 %	connection, VPN, security, setting, port, router, encryption, key, Wi-Fi, IP address
Privacy setting	5.6 %	setting, information, location, iPhone, privacy, accept, consent, website, restriction, company

常生活で直面するセキュリティ及びプライバシーに関する懸念点を特定するため、日本の最大規模の非専門家向け Q&A サイトに投稿されたセキュリティ及びプライバシーに関連する質問 445 件の内容を質的分析した [1][2]。

質問のテーマ(トピック)は表 1 に示す 7 つのテーマに分類された。サイバー攻撃に関する質問が最も多く、次いで認証とセキュリティソフトウェアに関する質問が多かった。具体的には、受信したメールがサイバー攻撃であるかどうかや、認証エラーの解決方法、及びアンチウイルスソフトの使い方に関する質問が多く投稿されていた。また、プライバシー侵害やアカウント／デバイス管理に関する質問の中には、回答を強く求める文言が含まれていることが多かった。

ロールプレイング型調査に基づくマルウェア感染通知の実効性分析：藤田らは、所有機器のマルウェアへの感染を知らせる通知を受けたユーザが対策行動を行うまでには心理的あるいは認知的な障害があるとし、通知を受容する際の心理状態と行動の関係を分析し、最適な通知文を検討した [3]。実験では、マルウェアに感染した恐れのある IoT 機器の所有者がインターネットサービスプロバイダから対策を促す数件のメールを受け取るというシナリオで模擬調査を実施し、757 名からの回答を得た。結果として、通知文に含まれる重要性の訴求の程度、与える不審な印象の度合、理解の進みやすさといった特徴は、対策行動の促進する要因にはなりにくいと推察された。参加者は、通知文に記述された内容を読み進めることには抵抗が少ないが、自らの状況について情報提供をするように要望を受けた場合や通知内容を不審に感じた場合はメールの読解を中断し、適切な対策行動を実施しないことが示された。

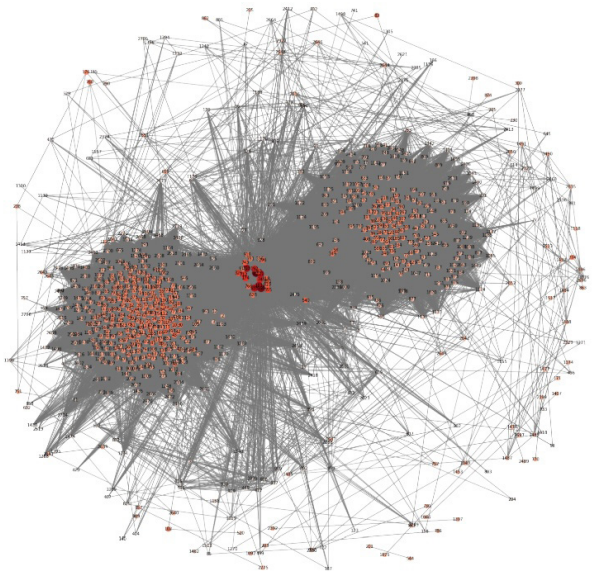

図 1　犯罪と関連する可能性が高い投稿を拡散（再投稿）するアカウント間の関係図

プライバシーポリシーにおける収集データと利用目的の対応関係の実態調査：原及び長谷川らは、プライバシーポリシーにおいて収集することが示されているデータとその利用目的の対応関係がユーザへ明確に示されているかを明らかにするため、ユーザがよく利用する 102 個のサービスのプライバシーポリシーの内容を分析した [4]。このうち 86 % のプライバシーポリシーにおいて収集データと利用目的の対応関係が明確に示されていないことが明らかになった。具体的には、収集データと利用目的が異なるセクションに羅列されて示されていることによりその対応関係が不明瞭であるケースなどが見られた。また、収集データもしくは利用目的の説明が欠如しているプライバシーポリシーも数件確認され、これらは GDPR(EU 一般データ保護規則)における通知の義務を満たしていないと言える。対応関係が明示されたプライバシーポリシーは、ユーザがサービスに対して抱く信頼度を高めるなどの効果がある一方で、対応関係を丁寧に説明することで説明文が長くなり、ユーザの負担が高いと考えられることから、ユーザにとって最適な説明文の構造を特定する必要性が示された。

オンライン詐欺や犯罪へ誘導する SNS 投稿文の類型化と特徴の分析：松田らは、ソーシャルメディアで犯罪や詐欺へユーザを誘引する脅威への対策を講じるため、ソーシャルメディアより“高額バイト”と称して人材を募集する投稿文を収集し、犯罪の実行役を募集している可能性の高い投稿とオンライン詐欺への誘引が確認された投稿について、これらの投稿を共有したアカウントの関係や投稿文の特徴を分析した [5]。アカウントの分析では、ほぼ同一の投稿文を拡散するアカウント群が特定され、犯罪に関連する可能性の高い投稿の拡散において中心的な役割を果たすアカウントがあることが明らかになった。図 1 に示すように、中心付近に赤色でプロットされたアカウントグループがその左右にプロットされたアカウントグループのそれぞれと投稿を頻繁に再投稿することで、互いのグループのメッセージが効率的に拡散するよう活動している状況がみてとれる。また、投稿内容の分析では、犯罪に関連する多くの投稿は地名を多く含み、同一の投稿文を使いまわす傾向があり、オンライン詐欺への誘引が確認された投稿では個別アカウントにメンションをしてターゲットを限定するような語句が多用する傾向が見られた。

2.2　エキスパートユーザに関する研究

産業界におけるセキュア開発ガイドラインの利用実態の調査：金井及び長谷川らは、日本及び米国のソフトウェア開発者を対象に、セキュア開発ガイドラインの利用に関するアンケートを実施した[6][7]。図2に示すように、特に日本では、Web上で参照可能なパブリックなガイドラインとの併用を含めても、自社製のガイドラインが広く利用されている実態が明らかになった。また、表2に示すように、日米で共通して自社製のガイドラインのみを利用している場合にガイドラインへの準拠が義務付けられている割合が最も高く、パブリックなガイドラインのみを利用している場合においては準拠が義務付けられている割合が低い傾向にあることがわかった。加えて、既存研究で推奨されているガイドラインの運用方法は、小規模なプロジェクトに所属するソフトウェア開発者など、特定の属性を持つ人々にとって実践が困難であることを明らかにした。

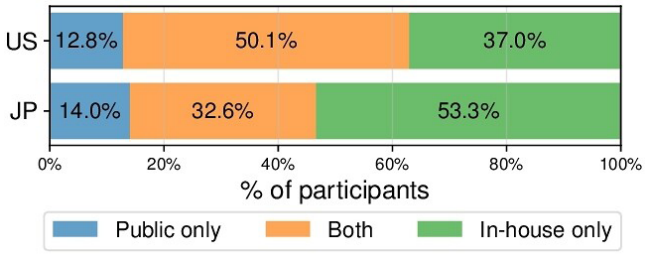

図2　参加者が利用しているガイドラインの種別の割合
(US: N = 359, JP: N = 285)

表2　ガイドラインへの準拠が義務付けられている参加者の割合

Country	Public only	In-house only	Both
US	67.4 % (31/46)	85.4 % (111/130)	81.8 % (144/176)
JP	67.6 % (25/37)	83.1 % (113/136)	82.4 % (70/85)

2.3　ユーザブルセキュリティ分野の方法論に関する研究

ユーザブルセキュリティ分野の調査におけるユーザ調査参加者の地理的偏りに関する分析：長谷川らは、ユーザブルセキュリティ分野の既存研究におけるユーザ調査参加者がWEIRD（Western, Educated, Industrialized, Rich, and Democratic）に該当する国々の住民に偏っており、文化的に多様なユーザを理解することへの障害となっている可能性があるとして、この偏りの程度や影響を調査した[8]。具体的には、2017年から2021年までの5年間に発表された当

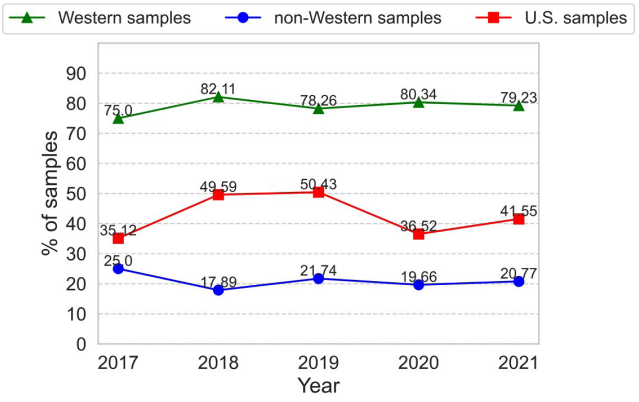

図3　2017年から2021年までの5年間における西洋諸国、非西洋諸国、米国の参加者サンプルの割合の経年変化

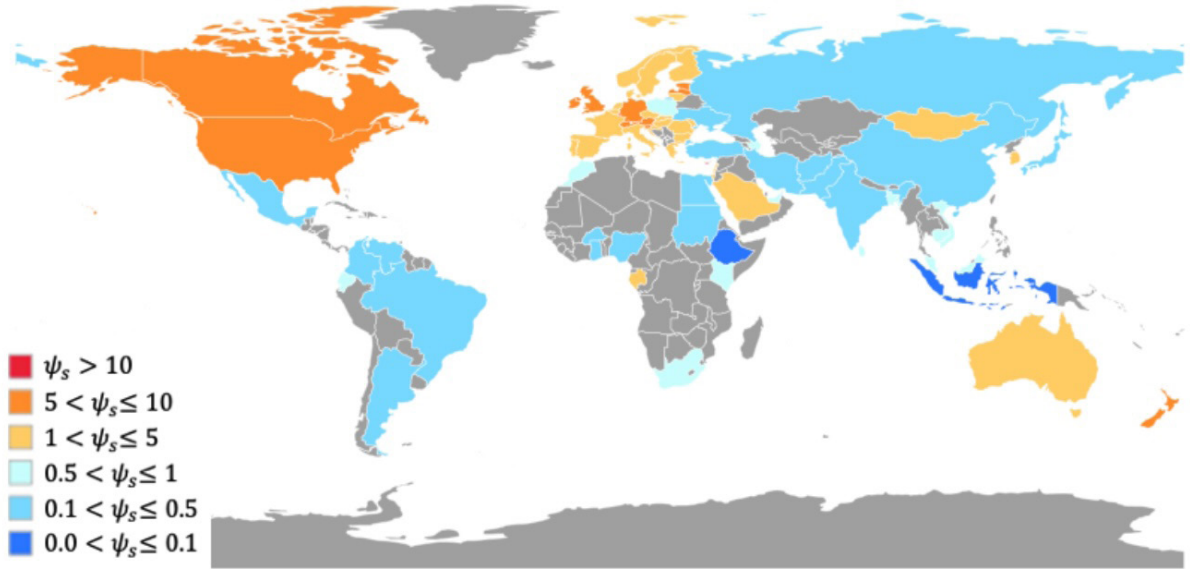

図4　各国の参加者サンプル数（世界人口に占める各国の人口比率で正規化したもの）の分布

該研究分野の論文715件を対象に、ユーザ調査の研究手法や参加者に関する情報、著者の所属及び研究のトピックなどを分析した。その結果、図3に示すように、当該分野の約8割の参加者サンプルが西洋諸国の住民であることが明らかになった。図4に示すように、調査対象期間5年間に調査された国は79か国のみであり、アフリカ、南米、中東、アジアの多くの国が全く調査されていない、または世界人口に占める人口比率に比べて調査された回数が極端に少なかった。このようなユーザ調査参加者の地理的偏りは、当該分野の研究者の所属の地理的偏り及びユーザ調査実施の際の地理的・言語的障壁に起因していることも明らかになった。このような参加者の地理的偏りを是正し、文化的に多様なユーザを理解するための試みとして、研究の再現性の向上と複製研究の推奨、研究手法における地理的及び言語的な問題への対処、WEIRD諸国とそうでない国との公正な研究協力の推奨などについて議論を行った。

3　おわりに

本稿ではユーザブルセキュリティ領域及び関連する研究開発テーマの趣旨及び目標について概要を説明し、サイバーセキュリティ研究室USECチームでの当該領域・テーマに関する研究開発成果を一部紹介した。

情報を悪用した攻撃やそれに伴う組織や社会への影響、情報サービスの期待と実際のギャップ、情報サービスの複雑性が増していく中、人々が安心して利用できる情報サービスや安全な社会を実現するために、人や社会に焦点を当てたセキュリティ技術の確立は不可欠である。ユーザブルセキュリティの研究開発分野は、これらの課題に対し、従来のセキュリティ技術に加えて、心理学、経済学などの人文・社会科学や認知工学、認知科学、計算言語学などを含んだ学際的アプローチで、多角的な視点から課題を解決する手段を講じる分野である。サイバーセキュリティ研究室USECチームは学問的にも技術的にも多様なバックグラウンドをもつ研究者・技術者が集まっており、今後もこの特徴を最大限に活(い)かしながら社会課題の解決に向けた調査・研究を行っていく。

【参考文献】

1　A.A. Hasegawa, N. Yamashita, T. Mori, D. Inoue, and M. Akiyama, “Understanding Non-Experts’ Security- and Privacy-Related Questions on a Q&A Site,” Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022), pp.39–56, 2022.

2　A.A. Hasegawa, M. Akiyama, N. Yamashita, D. Inoue, and T. Mori, “Analysis of Non-Experts’ Security- and Privacy-Related Questions on a Q&A Site,” IEICE Transactions on Information and Systems, vol.106-D, no.9, pp.1380–1396, 2023.

3　藤田 彬，松田 美慧，笠間 貴弘，井上 大介，“ロールプレイング型調査に基づくマルウェア感染通知の実効性分析，” Technical Committee on Information and Communication System Security（ICSS），pp.97–102，2023.

4　原 亨，長谷川 彩子，J. Jamieson，秋山 満昭，“プライバシーポリシーにおける収集データと目的の対応関係の実態調査，” IPSJ-SIG Security Psychology and Trust（SPT），pp.1–8，2024.

5　松田 美慧，川口 大翔，藤田 彬，吉岡 克成，“オンライン詐欺と犯罪へ誘導するsns 投稿文の類型化と特徴の分析，” Computer Security Symposium 2023，pp.996–1003，2023.

6　F. Kanei, A.A. Hasegawa, E. Shioji, and M. Akiyama, “Analyzing the Use of Public and In-house Secure Development Guidelines in U.S. and Japanese Industries,” Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, pp.1–17, 2023.

7　金井 文宏，長谷川 彩子，塩治 榮太朗，秋山 満昭，“日米の産業界におけるパブリックおよび自社製のセキュア開発ガイドラインの利用実態調査，” IPSJ-SIG Computer Security Group（CSEC），pp.1–8，2023.

8　A.A. Hasegawa, D. Inoue, and M. Akiyama, “How WEIRD is Usable Privacy and Security Research? (extended version),” Proceedings of the 33rd USENIX Security Symposium (USENIX Security ’24 Summer), pp.1–18, 2023.

藤田 彬　（ふじた あきら）

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
主任研究員
博士（情報学）
ユーザブルセキュリティ、Webセキュリティ、IoTセキュリティ

【受賞歴】
2021年　電子情報通信学会 第16回通信ソサイエティ論文賞（優秀論文賞）
2012年　博報堂教育財団 第六回児童教育実践についての研究助成事業 優秀賞

長谷川 彩子　（はせがわ あやこ）

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
主任研究員
博士（工学）
ユーザブルセキュリティ

【受賞歴】
2021年　EuroUSEC2021 Best Paper Award
2020年　情報処理学会 CSS2020 最優秀論文賞
2018年　電子情報通信学会 ICSS 2018年度研究賞

松田 美慧　（まつだ みさと）

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
研究員
ユーザブルセキュリティ

【受賞歴】
2023年　情報処理学会 CSS2023 CSS2023奨励賞
2023年　ISSスクエアシンポジウム ISSスクエア賞・ベストポスター賞

鈴木 悠　（すずき はるか）

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
専門研究技術員
ユーザブルセキュリティ

【受賞歴】
2022 年　情報セキュリティ大学院大学 優秀論文賞
2022 年　ISS スクエアシンポジウム ISS スクエア賞・ベストポスター賞

笠間 貴弘　（かさま たかひろ）

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
室長
博士（工学）
サイバーセキュリティ

【受賞歴】
2022 年　電子情報通信学会 ICSS 2022 年度研究賞
2019 年　NDSS2019 Distinguished Paper Award
2011 年　情報処理学会 2011 年度山下記念研究賞