挑戦する研究者たち
CHALLENGERS

秋山満昭

NTT社会情報研究所
上席特別研究員

あらゆる技術者がセキュリティの素養を持つことが当たり前の世界になったらいい

世界最先端の暗号技術やサイバーセキュリティ対策技術等の情報科学分野の研究開発を長きにわたり積み重ねてきたNTT研究所．社会価値，人々の幸せ，法制度，社会受容性等の社会科学分野の研究開発を融合し，社会の変革と発展をめざす秋山満昭上席特別研究員に研究の進捗と研究者としてのあり方を伺いました．

「技術」「人間」「社会」の関係・相互作用に立脚した社会技術システム（Socio-technical system）の観点からのアプローチ

2019年にご登場いただいてから3年が経ちましたが，その後の研究活動はいかがでしょうか．

前回から継続して，サイバー攻撃に対応して，ユーザの安心・安全を守るためのサイバーセキュリティについて，①サイバー攻撃の特徴を分析，情報を蓄積し（サイバー攻撃対策用インテリジェンス），それを活用して将来発生し得る類似の攻撃を防ぐことをテーマとした研究，②攻撃者の視点に立ってシステムやサービスのバグ等の潜在的なセキュリティ・プライバシ脅威欠陥を発見し，対処することで攻撃を未然に食い止めるオフェンシブセキュリティの研究，③セキュリティ・プライバシ脅威発見のための実験方法や発見した脅威の公開方法など，先進的研究成果を正しく社会に還元するためのサイバーセキュリティ研究倫理に関する活動，④システム・サービス等に対するユーザのセキュリティ・プライバシ意識や行動の把握に基づいたセキュリティ脅威の定量化を行うことで，セキュリティ脅威への対処の優先度付けやユーザの認識を助け，より安全な行動の判断ができるシステム設計等をめざす，ユーザブルセキュ

リティの研究を行っています．

2021年７月に研究所の組織再編が行われ，NTT社会情報研究所（社会研）が設立されました．社会研は，さまざまな領域の研究開発を複合的に進める必要があると考え，人々の幸福の実現をめざしたWell-being研究，ICTと人文社会科学を融合させた社会システムの変容を促す技術，サイバー攻撃等の脅威を排除する新たな技術の確立，社会情報の分析・予測によるセキュアな社会システムの実現のための先進的変容のコンセプトを具現化する技術の確立，高付加価値な社会システムの実現に向けて安全性と利便性を両立した情報流通・利活用を促進する技術の確立，暗号理論に加え物理的な性質を活用した新しいデータ保護技術の確立，世界を牽引する次世代暗号の基礎理論の創出などに取り組んでいます．

これまで「セキュリティはコスト」としてとらえられることが多かったのですが，社会研ではこうした観念から脱却し「セキュリティ・プライバシが保たれているからこそ人や社会を動かし，発展させられる“原動機”となる技術」として研究開発に臨んでいます．そこで私は，社会研において研究活動を進めるというチャンスを活かして，以前と比べて人間の行動や社会的な側面等の学際的部分のウエイトを高くしてきています．現在，新しい技術に関するセキュリティやプライバシについて十分に明らかでないまま，それを利用せざるを得ない状況であり，セキュリティ・プライバシに関する新しい脅威が顕在化しています．こうした状況にあって，私は改めてサイバーセキュリティの科学的基礎の確立，および学際的な観点から問題を解決するアプローチが必要であると考えています．

まず，産業界ではサイバーセキュリティ技術は日々発生するサイバー攻撃に対して対症療法的で，経験則的なセキュリティ対策および運用が主流でした．このような事後対策のセキュリティでは，膨大な対処がモグラたたき状態で必要になるため，人的コスト増，対応の迅速性の欠如，セキュリティ疲れが発生し，高度化するサイバー攻撃に対して信頼できるICTシステムを維持することが困難です．問題の本質をとらえた根本的な解決のためには，理論的に正しい数理科学的手法，包括的な理論，原理的なシステム設計手法，複雑かつ動的なシステムに対するさまざまなレイヤ・スケールにおけるモデル化，セキュリティ技術の効果を評価するための指標づくり等を通して，透明性・再現性・検証可能性のあるサイバーセキュリティ技術をつくり出すことが重要であると考えています．

また，学際的アプローチの観点から，「技術」「人間」「社会」の関係・相互作用に立脚した社会技術システム（Socio-technical system）を追究しています．技術がセキュアであっても，人間が誤った利用方法をすればセキュアではなくなることもあり，また，社会に普及しなければその恩恵を十分に受けられません．

実際に，これまで多くのセキュリティ技術が考案されているにもかかわらず，十分に活用されなかったものは数多くあります．エンドユーザがフィッシング詐欺に騙されること，開発プロジェクトにおいてセキュリティ・バイ・デザインを実践する難しさ等の理由が解き明かされていないために，技術が正しく活用されなかった事例も多々あります．

こうしたことから，私は根本的な原因を人間や社会の観点から明らかにして，ICTシステムの設計から見直そうと考え，コンピュータサイエンスに加え，社会科学や社会心理学等を含めた学際的なアプローチも取り入れています．特に，ユーザブルセキュリティにおいては，システムに着目するだけでは解決できない人間の認識・判断に依存するセキュリティ・プライバシ問題を解決することをめざしています．具体的には，セキュリティ・プライバシの観点から人間の行動・メンタルモデル・意思決定プロセスを観測・分析し，得られた知見をシステムの設計・実装・運用にフィードバックすることで，人々がセキュリティ・プライバシに関して正しい認識に基づいた適切な判断を可能にすることです．

これを実現するには人間の行動や認識をいかに適切に観測・分析するかが重要になると考え，新たに誤情報拡散対策に臨んでいます．誤情報拡散とは，意図せず誤った情報が拡散されるmisinformation，害を与える意図を持って誤った情報が拡散されるdisinformationの総称です．例えば，ソーシャルメディアにおける誤情報拡散は人間の正しい認知や判断を脅かす次世代のサイバー攻撃ですし，誤

情報拡散はフィッシングの被害に遭う・デマに騙されるなどの個人の問題にとどまらず，2016年の米国大統領選のように民主主義に大きな影響を及ぼすこともあります．

数々の世界トップ会議で採択．社会的課題を浮き彫りに

これらの研究活動において，大きな学術的成果を上げられたそうですね．

オフェンシブセキュリティについては，サイバーセキュリティのトップ会議の１つであるNDSS2020に採択され，Distinguished paper awardを受賞しました(1)．Webコンテンツを別のWebサイトに再ホストして利用するサービスをWebリホスティングサービスと命名し，これらWebリホスティングサービスに対して複数の脅威モデルを考え，検証によって実際にそれらが顕在化する条件を明らかにしたことが評価されました（**図１**）．具体的には，Webリホスティングサービスにおいて，元々は異なるオリジン（URLのプロトコル・ホスト・ポートの組によって定義される属性）のWebコンテンツが同一のオリジンに統合される際に，Webセキュリティの根幹となる仕組みが作用しなくなるという，重大な現象を初めて発見しました．これはWebリホスティングサービスにおいてさまざまな攻撃が可能であること，そしてそれら攻撃を回避するためのWebサービスにおける設計指針を示すものです．

この研究により，脅威が顕在化する前に私たちが発見し，設計段階で対策ができたことで，事業者のサービスそのものの設計見直しの回避につながりました．先ほどもお話ししましたが「単に脆弱性を発見する」のではなく，このようなセキュリティ・プライバシ上の脅威を発見するためのより汎用的な検証方法や理論的基礎の確立をめざし，現在はさまざまな通信が集約されているWebの分野を対象として，多くの脅威とその検証方法を確立してきました．Webにおいては５年程度でこれまでの知見をまとめ，汎用性のある検証方法や理論的基礎の確立につなげたいと考えています．

ユーザブルセキュリティにおいては，開発者や開発プロジェクトに着目したセキュアなソフトウェア開発を実現するための研究が，サイバーセキュリティの難関会議ACSAC2021で採択されました(2)．これは，日米のプロのソフトウェア開発者に対して大規模オンラインアンケートを実施して，組織的な要因を明らかにしたもので，意思決定権限の有無や意思決定の困難さなどの問題等を明らかにしました（**図２**）．

さらに，人間が騙される原理を解明し適切なサポート技術をつくる研究は，サイバーセキュリティの難関会議SOUPS2021にて採択されました(3)．これまでは暗黙的に母国語のフィッシングメールに直面したときのユーザの認識や行動の調査・対策が研究されていましたが，私たちは世界の過半数を占める英語ノンネイティブに着目して，言

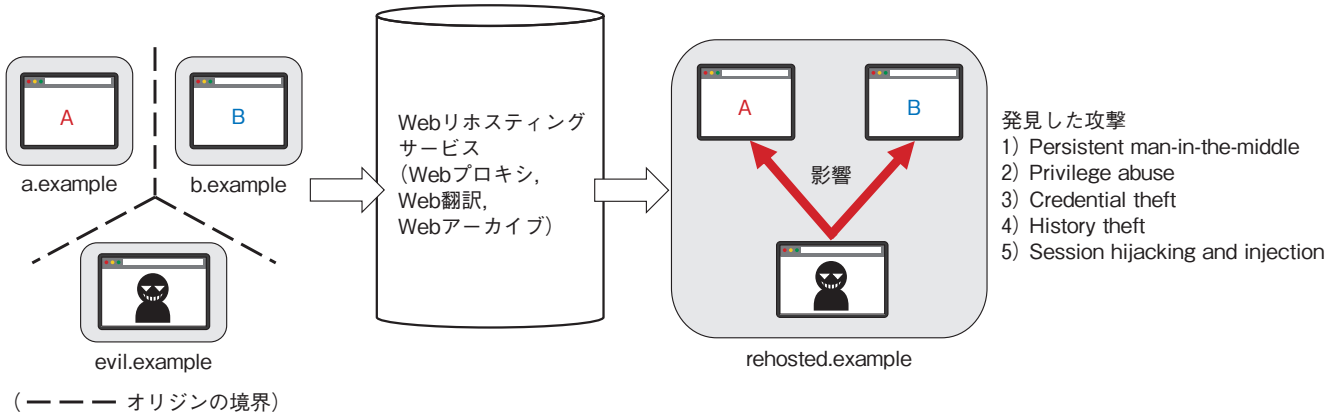

図１　Webリホスティングサービスの潜在的な脅威

語とフィッシングメールへの対処の関係を大規模調査で初めて明らかにし，英語ノンネイティブ特有のサポート技術を提案しました．

そして，サイバーセキュリティの難関会議EuroUSEC2021では，ユーザスタディの正しい方法論の研究で，フィッシングに関して人間がなぜ騙されるのかに関するユーザ調査手法の問題点を明らかにした研究が採択され，Best paper awardを受賞しました[4]．具体的には，ユーザスタディにおいて利用されている実験参加者のスクリーニング手法では，もっともデータが必要となるはずの“フィッシングに騙されやすい不注意な実験参加者”を除外してしまうという，大きな矛盾があることを初めて明らかにしたものです．

ほかにも，ソーシャルメディアにおける誤情報拡散対策に関する研究は，国際会議NetSci-X2022にて採択される等の成果が出ており[5]，その中のいくつかはNTT R&Dフォーラムにおいても出展・報告しました．

好きこそものの上手なれ

課題やテーマを探すときに心掛け，意識して実行していることを教えてください．

まず，新しい技術やサービスに興味を持ち，常に自分の知識をアップデートすることです．技術単体で考えるのではなく，技術がどのように活用されるのかを，それにかかわる人々や組織，社会，法律や倫理などの観点から総合的に考えています．

加えて，異なる分野の専門家と議論することです．何かを実現しようとすると，自分の専門分野を越えることはよくあることですから，学際的アプローチのために他分野の研究者との連携は必須といえます．その意味では，NTT研究所は改めて人材の宝庫だと感じています．

私は「好きこそものの上手なれ」という言葉は研究者としての大切な姿勢であると感じています．私自身は人より優れた特別な研究の才能を持っているとは思っていませんが，サイバーセキュリティの諸問題について「面白いと思う気持ち」は人一倍持っていると思います．

これまで，技術的な能力がとても高いにもかかわらず研究をやめてしまった人，「研究をやっていく自信がない」といって研究職に就かなかった人を多く見てきました．しかし，研究はすぐに成果が出ないもので，１つの成果を出すのに数年，場合によっては10年，20年かかるものもあります．そのような状況において，「自分には才能がない」と思ってやめてしまうこともあるかもしれませんが，もし，自分が好きなことであれば，たとえ成果が出ようが出まいが誰に命令されるわけでもなく，高いモチベーション・興味を持って継続することができるのではないでしょうか．継続して取り組むことができれば，結果的に成果が出る可能性は確実に上がります．

こうしたことから，私は，まず自分の取り組もうと思った研究について，自分自身が本当に好きかどうかを考えま

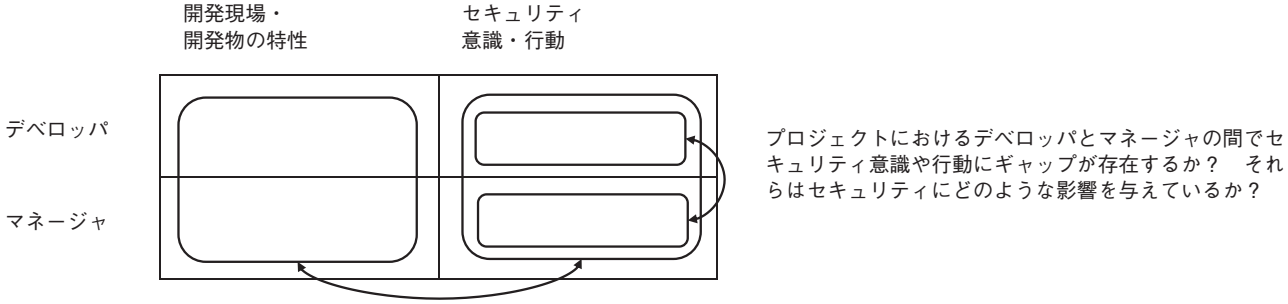

図２　セキュアなソフトウェア開発を阻害する要因の分析

写真　国内シンポジウムでのパネルディスカッションの様子

す．本当に好きならば，研究の成功・失敗はあくまでも結果として受け止めるだけなのでそれに左右されることなく，私にとって好きだという思いが揺らぐことはありません．

今後はどのように研究活動を展開されるのですか．

これまでセキュリティに関する研究開発が，個別の脅威に対して単体かつ後追いで考えられてきたことが多く，根本的な課題の解決に結びつきにくかったという現状があります．私はこれにかんがみ，セキュリティの専門家だけがセキュリティを考えるのではなく，あらゆる技術者がセキュリティの素養を持って，セキュリティを考慮したものづくりをすることが当たり前の世界になったらいいと思っています．つまり，技術者全員がセキュリティ技術者の側面も持ってくれることを望んでいるのです．誰でも利用できるセキュリティ技術をつくり出す手伝いをすることが私の仕事だと思っています．そうなると，セキュリティ技術者という言葉も意味が変わってきます．

それから，私は研究倫理にも取り組んでいます．国内のセキュリティ研究コミュニティにおいては，2016年ごろから継続してサイバーセキュリティ研究倫理の啓発をしていますが，その考え方が一定のレベルまで広まっています．実は，米国の学会であるIEEE S&Pでこういった対策がなされるよりも前の2018年から，日本では国内最大級のセキュリティシンポジウムCSSにおいて，相談窓口が設置されています．また，研究倫理チェックリストも各種研究会で活用できるかたちでCSEC（コンピュータセキュリティ）研究会から公開されるまでになりました．

2021年は，OSS（オープンソースソフトウェア）コミュニティにおけるコードレビュープロセスを評価するため，Linuxカーネルに脆弱性入りパッチをコミットする実験を行った論文が世の中で問題になったことを踏まえて，日本のサイバーセキュリティコミュニティにおいてもパネルディスカッションを実施，セキュリティ研究者と開発コミュニティとの関係について議論しました（**写真**）．このディスカッションにおいて私は，人間やその集まりであるコミュニティ・組織を対象にした実験は，それらに与える影響を十分に考慮したうえで設計・実施されなければならないし，開発コミュニティと研究者コミュニティとの分断があってはならない，研究者も開発者コミュニティの一員として一緒に取り組むことが重要，と主張しました．

今後も，このようにセキュリティ研究者がソフトウェア開発者をリスペクトし，より良い技術開発について協力していくことが重要であり，その普及啓発活動にも注力していきたいと考えています．

■参考文献

(1) T. Watanabe, E. Shioji, M. Akiyama, and T. Mori : “Melting Pot of Origins: Compromising the Intermediary Web Services that Rehost Websites,” NDSS 2020, San Diego, U.S.A., Feb. 2020.
(2) F. Kanei, A. A. Hasegawa, E. Shioji, and M. Akiyama : “A Cross-role and Bi-national Analysis on Security Efforts and Constraints of Software Development Projects,” ACSAC 2021, Austin, U.S.A., Dec. 2021.
(3) A. A. Hasegawa, N. Yamashita, M. Akiyama, and T. Mori : “Why They Ignore English Emails: The Challenges of Non-Native Speakers in Identifying Phishing Emails,” SOUPS 2021, Online, Aug. 2021.
(4) T. Matsuura, A. A. Hasegawa, M. Akiyama, and T. Mori : “Careless Participants Are Essential for Our Phishing Study: Understanding the Impact of Screening Methods,” EuroUSEC 2021, Online, Oct. 2021.
(5) S. Furutani, T. Shibahara, M. Akiyama, and M. Aida : “Competitive Information Spreading on Modular Networks,” NetSci-X 2022, Porto, Portugal, Feb. 2022.