秋山満昭　NTTセキュアプラットフォーム研究所　上席特別研究員

「誰もが正しく物事を理解し，選択して，活用できるセキュリティ技術」を創造する

サイバー空間は人間の活動空間を拡大させ，ビジネスのみならず一般的な人々の生活の一部となっています．こうした環境下で恩恵とともに脅威にさらされる機会も増え，安心・安全なICT環境が求められています．このような状況において，我が国では2018年に「サイバーセキュリティエコシステム」構築をめざし，新戦略を掲げています．サイバー空間の安心・安全を保つにはどのような研究開発が必要なのか，秋山満昭NTTセキュアプラットフォーム研究所　上席特別研究員に研究の動向を伺いました．

多種多様なサイバー攻撃の未然防止で数々の成果を上げている

●現在手掛けている研究を教えていただけますでしょうか．

近年，サイバー攻撃という言葉がさまざまなメディアに出てきています．サイバー攻撃は，自己顕示，社会的・政治的主張，諜報活動などの多様な目的がありますが，一般のユーザの多くが直接的に巻き込まれ得るのは経済的利益を目的としたサイバー攻撃です．経済的利益を目的とする以上，攻撃者は「いかに効率的に攻撃を実施し，コストに見合った利益を獲得するか」を考えます．

こうした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研究しています．サイバーセキュリティ研究といっても，分野は多岐にわたっています．その中で，①サイバー攻撃の特徴を分析，情報蓄積し（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潜在的なセキュリティ・プライバシ脅威を発見し，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て，より安全な行動の判断ができるシステム設計をめざす，ユーザブルセキュリティの研究を行っています（**図1**）．

●具体的な評価，成果は得られましたか．

私がNTTに入社した2007年ごろはマルウェア感染端末を踏み台としたサイバー攻撃が猛威を振るっていたこともあり，組織を越えて技術者・研究者が集まってICT-ISAC（Information Sharing And Analysis Center）Japan等で現場の情報共有や対策のアイデアを議論していました．総務省が主導するサイバー攻撃対策の実証実験では，ICT-ISACや日本の主要ISP（Internet Service Provider）各社やセキュリティベンダが参画し，私たちが開発したハニーポット* が活用され，大規模なマルウェア感染の実態調査と悪性通信のフィルタリング対策の効果が検証されました．これらの結果は，一般社団法人電気通信事業者協会等の電気通信事業者関連団体が共同で検討し，発行する「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン」策定の後押しとなりました．

＊ ハニーポット：システム等を脆弱なシステムやサービス等を装う「おとり」として動作させておくことで，攻撃者を誘い込んでさまざまな攻撃の手口を明らかにする技術．

一方，人々の生活をより豊かにするために進化し続けるICT社会，それを支える部品として新しいソフトウェア・ハードウェア・プロトコル等が日々開発され続けています．しかしこれら部品そのものが膨大になっていること，また部品の組み合わせ方が複雑になっていることから，設計ミスやバグに起因するセキュリティ上の欠陥がシステムやサービスに混入してしまう問題があり，これを根本的に解決することが難しい状況にあります．このような状況では，攻める側が圧倒的に有利な状況であり，守る側は次から次に明るみになる問題をパッチワークで対処することで精一杯になってしまいます．このような防戦一方な状況を転換するために，攻撃者の視点に立ってシステムやサービスの潜在的な欠陥を発見する，オフェンシブセキュリティの取り組みによって，攻撃者に先んじて潜在的な欠陥を発見し，悪用される前に対策を講じることができます．多様なWebサービス上のセキュリティ・プライバシ脅威の発見を目的に数年前から取り組んでいますが，世の中の多くのシステム・サービスに影響するような深刻な脅威をすでにいくつか発見しました．攻撃に悪用される前に脅威の影響を受ける大手ソーシャルWebサービスに通知して対策を実施したことで数億人規模のユーザをセキュリティ・プライバシ脅威から守れたこと等の成果を上げています．

前例のない領域の問題を扱うと同時に，倫理的課題に直面する

●世の中へのインパクトが大きい成果を次々と挙げられているのですね．

サイバーセキュリティの研究は，十分に前例のない領域の問題を取り扱う場合があると同時に，社会に対して直接的な影響を与え得るため「倫理的」な問題にも直面します．例えば，サイバー空間に蔓延する脆弱なデバイスを発見するためのネットワークスキャンの許容範囲，セキュリティ上の欠陥を発見するために実在するシステムに対して行う実験，欠陥や脆弱性を発見した場合に発見者がとるべき行動等で，研究活動やその結果の世の中への伝え方を誤ったが故に，世間から批判される事例や法廷闘争に発展する事

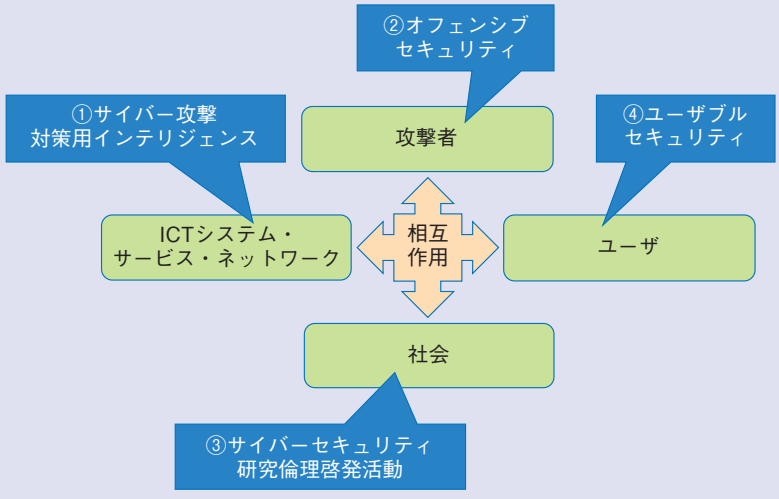

図1　ユーザの安心・安全を守るためのサイバーセキュリティ研究の対象

例が多々あります．研究者が萎縮することで科学技術の発展が妨げられるのは避けなければなりませんし，研究者自身が無責任に実験を実施し，攻撃手法や脆弱性を公開するのではなく，責任ある研究者としてどのように倫理的に取り組めば良いかを考える必要があります．

生命医科学分野では，臨床研究に関して倫理的課題の議論と取り組みが半世紀以上にわたって行われてきました．ニュルンベルク綱領やベルモント・レポートに基づいて研究に関する倫理的なリスクアセスメントを実施しています．一方でベルモント・レポートの倫理原則をICT・セキュリティ研究の文脈で拡張したメンロ・レポートは2012年に発表されたばかりで，この倫理原則に従ってどのように研究で実践するかについて今まさに欧米の研究コミュニティを中心に議論が進んでいるところであり，学術国際会議の論文執筆要綱では研究倫理に関する記述を著者に求めることが一般的になっています．このような動向の中，日本ではこれまでICT・セキュリティ研究の知見が十分に蓄積されている研究倫理審査委員会を保有する研究組織が少ないことや，サイバーセキュリティの研究倫理に対する認識が十分に広まっていませんでした．

●生命医科学の分野では倫理の話が出るのですが，サイバーセキュリティの分野でも倫理に関する議論があるのですね．日本では緒に就いたばかりのサイバーセキュリティ研究倫理ですが，どのように啓発，展開されるのでしょうか．

私は日本から革新的で競争力のあるセキュリティ技術を世界に向けて発信するためには，研究成果が社会に受け入れられるための倫理的配慮も必須であると考え，2016年からサイバーセキュリティ研究における倫理的な研究プロセスに関する啓発活動を学術組織横断的に推進しています．前述のオフェンシブセキュリティ研究では，研究成果を適切に世の中に還元するためにステークホルダなどの関係各所と連携・協力しました．このような経験自体も「ベストプラクティス」として本活動を通じて研究者に向けて公開しています（**図2**）．

また，コンピュータセキュリティシンポジウム（CSS）では，サイバーセキュリティ研究や法制度の専門家からなる研究倫理相談窓口を設置して，研究者からの研究倫理に関する懸念点に対して適切にアドバイスを実施しています．これまでの活動の知見から得られたCommon pitfall（共通的な落とし穴）をまとめたチェックリストを公開し，研究者自身が実験実施時もしくは論文執筆時にセルフアセスメントできるようにしました．これら取り組みが，世界的に競争力のあるセキュリティ技術を創出するための研究コミュニティの醸成に寄与することを願っています．

それから，私は「誰もが正しく物事を理解し，選択して，活用できるセキュリティ技術」を創造することが，多種多様な人々を受容する真の意味でのICT社会を実現できると考えています．私たちは，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の研究を実施しています．ユーザの普段のセキュリティ・プライバシ認識や行動を把握することでセキュリティ上の脅威にユーザがどの程度影響を受けるかを定量化し，優先度をつけて真に重要な脅威から対処することや，ユーザの認識を助け，より安全な行動の判断ができる設計等をめざしています．

協働すれば大きな課題に挑むことができる

●研究成果のみならず，研究者の取り組み方にまで活動を広げられているのですね．今後はどのようなことに取り組まれますか．

世の中の役に立つ研究という観点から，現在はユーザブルセキュリティに注力しています．ICTやそれに伴う社会システムがどんどん高度化するに従って，ユーザに求められるセキュリティ上の判断・行動が複雑化しています．本来は誰しもが平等にICTの恩恵を享受できるべきはずが，求められる判断・行動が複雑化した状況では，対応できないユーザが取り残されてしまう懸念があります．例えば，ブラウザ上でセキュリティ警告が表示された場合にそれが「どのようなリスクで，どのように行動すれば良いのか」をユーザが適切に判断することが難しくなっています．ま

た，偽の警告画面を表示することでユーザに誤った行動を誘発させるようなソーシャルエンジニアリングによる攻撃も発生しており，これはユーザの認知的な脆弱性をついた巧みな攻撃であるともいえます．私は「誰もが正しく物事を理解し，選択して，活用できるセキュリティ技術」を創造することが，多種多様な人々を受容する真の意味でのICT社会を実現できると考えています．ユーザブルセキュリティは，まさにこれを実現していくうえで大きなテーマであり，ユーザの普段のセキュリティ・プライバシ認識や行動を把握し，セキュリティ脅威を定量化していくことで，

① セキュリティ上の脅威にユーザがどの程度影響を受けるかを定量化し，優先度をつけて真に重要な脅威から対処する

② 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を設計する等をめざしています．

また，研究倫理に関する活動も推進していくつもりですが，さらにチームとして学際領域の課題に挑戦します．ある意味研究倫理についても学際領域でもありますが，これとは別に，サイバーセキュリティ研究はソフトウェア工学，計算機科学，ネットワーク等のコンピュータ科学分野のさまざまな基礎技術を総合的に組み合わせた問題を解く分野ですが，これに加えて社会科学，心理学，ヒューマンコンピュータインタラクションなど多岐にわたる学際的な技術・知見を取り入れなければ解けない課題に挑戦しています．1人ですべての分野を極めることは到底困難なので，各分野の専門家と協働でチームとして取り組むことで1人では解けなかった大きい課題を解きたいと思っています．

●研究者になられたきっかけは．

サイバーセキュリティを題材にした『The Net』という映画をきっかけに，子ども心にかっこいい，こんな研究者になりたいと思い，大学，大学院とセキュリティ研究の道に進みました．特に大学院では，セキュリティ研究の大家である故山口英教授に師事することができ，山口先生の技

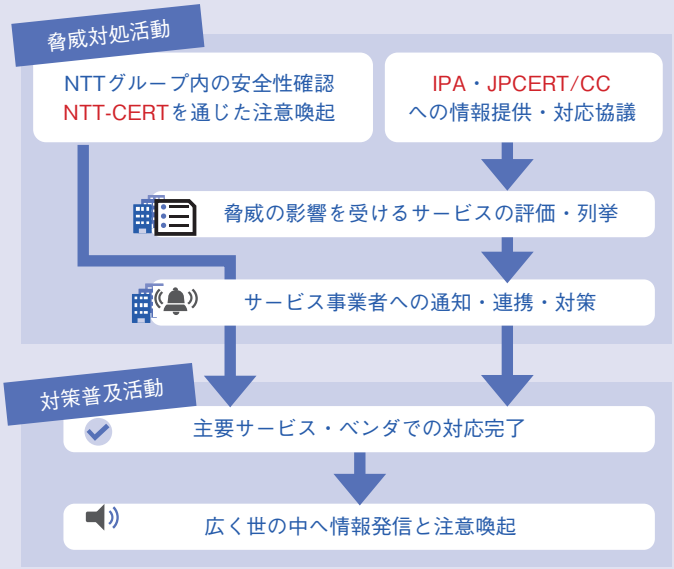

図2　サイバーセキュリティ研究における倫理的な研究プロセスに基づいた脅威対処活動と対策普及活動

術と社会のかかわりを意識し，安心・安全（セキュリティ）の恩恵を世の中に享受してもらおうとする姿勢に大きく影響を受けました．こうして研究者になった今も，世の中を良くしていく，変えていくという思いは変わらず持っております．

一方で，研究者である以上，新しい何かを発見し，その成果が先々に継承されて残っていくような研究をしたいです．先々といっても，昨今では技術革新が非常に速いので，100年後を予測するのは難しいのですが，10年後，20年後に残る研究をしていきたいです．それでは，どのような研究が残るかというと，本質を追究した研究は残ると思います．例えば，人間とコンピュータの関係も人間が中心にあって，生活を豊かにするためにあるものだという部分は変わらないでしょう．ですから，人間とコンピュータの間に生じる問題はこれからも存在すると思うのです．特にユーザブルセキュリティでいえば，技術の進展や複雑化に人間の認識が追いつかずギャップが生じ，そこをねらった攻撃が発生する．その問題に挑む研究というのは普遍だと考えます．

そして，このような研究は，自分が面白いと思っていなければ続けられないです．人から重要だからやりなさいと言われる研究は続かないし，飽きてしまいます．研究はすぐに成果の出るものではないので粘り強くないとできません．しかし，そのような試行錯誤の研究活動の中で，何かを発見すると「今これを知っているのは自分だけではないか！」というワクワクした気持ちが生まれ，ますますやる気がわいてきます．私たちがオフェンシブセキュリティの研究で世間に大きく影響する脅威を発見したときのことですが，当該者に通知したらシステムを再設計するなどして対応してくれました．そのときは，良いことができたという実感がわきました．

好きなら始めよう！自信は経験とともに後からついてくる

●研究者の皆さんへ一言お願いいたします．

学生の話を聞いていると研究に興味があるけれど自信がないという人が多いようです．自信は経験とともに後からついてくるものなので，自分が探求したいと思えるテーマがあるのなら研究を始めたほうが良いと思います．一番重要なのは研究の才能のあるなしよりも研究することが面白い，続けられるという感覚ではないかと私は思っています．私の場合，先輩に面白いねといわれたことが，自信のつくファーストステージだった気がします．次のステージは論文が採択されて世間に認められたときでした．そして，次の研究してみようかという良い循環ができました．論文採択までの過程において，査読を通すことに苦労することがあると思いますが，それに抱く感情も年齢とともに前向きに変わるものです．そして経験を積むことで，執筆の際のちょっとした工夫で査読が通るようになることもよくあり，こうした苦労や経験も自信につながるものだと思います．

もう1点は，人との出会い，つながりが大切だと思います．私の今があるのは良い仲間，そして良い恩師に恵まれたことだと思います．サイバーセキュリティ研究は研究領域が幅広くさまざまな分野の専門家が束になって挑戦するような問題が存在します．これに挑むためには各分野の研究者を尊重しなければなりませんし，素晴らしい研究者と出会うためにも国際学会等は非常に良い機会なので，積極的に参加しています．

このような中でも特に恩師との出会いは私にとって大きなインパクトがありました．きっかけは，前述のとおりセキュリティ研究の大家への師事ですが，こうして研究者となった今でも，先生が残された道や道標に驚かされることがしばしばあります．私も先生のレベルに達せないまでも，後輩が助走できるような道をつくれたら良いなと思います．