20th Anniversary

情報セキュリティ大学院大学（IISEC）開学20周年
NPO情報セキュリティフォーラム（ISEF）設立20周年
記念リレー講座・シンポジウム講演録

情報セキュリティ文化の醸成を目指して

IISEC開学・ISEF設立20周年記念誌制作委員会 編

20th Anniversary

情報セキュリティ大学院大学（IISEC）開学20周年
NPO情報セキュリティフォーラム（ISEF）設立20周年
記念リレー講座・シンポジウム講演録

情報セキュリティ文化の醸成を目指して

IISEC開学・ISEF設立20周年記念誌制作委員会 編

Contents

はじめに……6

▶▶IISEC開学ISEF設立20周年記念リレー講座

第1回
DXの実現を担うプラス・セキュリティ人材とリスキリング……11

登壇者 デロイトトーマツコンサルティング 執行役員 **森 正弥 氏**
情報セキュリティ大学院大学 学長 **後藤 厚宏**
ファシリテーター：MM総研 代表取締役所長 **関口 和一 氏**

第2回
セキュリティ人材のキャリアパス……27

登壇者 国立研究開発法人 情報通信研究機構 執行役
サイバーセキュリティ研究所長 **盛合 志帆 氏**

第3回
汚れたインターネットと通信事業者の戦い
―対マルウェア攻防の20年、将来はどう守るのか？―……41

登壇者 NTTコミュニケーションズ株式会社 情報セキュリティ部長
株式会社エヌ・エフ・ラボラトリーズ 代表取締役社長 **小山 覚 氏**

第4回
英国Cybersecurity Fellowship 参加報告
―若者向けサイバーセキュリティ人材育成：英国と日本の比較―……57

登壇者 株式会社BLUE 代表取締役
千葉工業大学変革センター 研究員 **篠田佳奈 氏**

第5回
インフォデミック時代における フェイクメディア克服の最前線……67

登壇者 国立情報学研究所 情報社会相関研究系 研究主幹・教授
シンセティックメディア国際研究センター長 **越前 功 氏**

第6回
事業継続を脅かす サイバーリスクの実態と対策……85

登壇者 八雲法律事務所 弁護士/ カリフォルニア州弁護士
情報処理安全確保支援士 **山岡 裕明 氏**

第7回
世界に普及可能な日本発 サイバー技術の生産手段の確立……99

登壇者 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 サイバー技術研究室長
東日本電信電話株式会社（NTT東日本）特殊局 ビジネス開発本部 特殊局員
筑波大学 客員教授
ソフトイーサ株式会社 代表取締役 **登 大遊 氏**

▶▶ IISEC開学ISEF設立20周年記念シンポジウム

【基調講演】

人生はゲームだ!!
様々な挑戦を乗り越え得られた多くのもの……119

登壇者 株式会社SNK代表取締役社長 松原 健二 氏

【基調講演】

セキュリティコミュニティの
入り方・歩き方・活かし方……125

登壇者 Elastic社 Senior Security Research Engineer 中島 明日香 氏

NPO 情報セキュリティフォーラム
20年の軌跡と今後の展開……131

登壇者 特定非営利活動法人 NPO情報セキュリティフォーラム 理事・事務局長
学校法人　岩崎学園 理事・専務執行役
植田 威

IISEC 情報セキュリティ人材育成ビジョン2024
これまでの20年とこれから……137

登壇者 情報セキュリティ大学院大学 学長 後藤 厚宏

【OBOGによるパネルディスカッション】

VUCA時代のキャリア構築とIISEC
— IISEC Alumni reunion 2024 —……143

パネリスト Amazon Web Services Japan
プロフェッショナルサービス本部
Senior Data Analytics Consultant 吉濱 佐知子 氏

ガートナージャパン
アソシエイトディレクター 澤田 忍 氏

NTTセキュリティ・ジャパン株式会社
セキュリティプリンシパル 羽田 大樹 氏

モデレーター Japan Digital Design株式会社
Head of TDD 兼 VP of Security 唐沢 勇輔 氏

登壇者プロフィール……157
おわりに……162

※各回に記載されている登壇者の肩書は登壇時点のものです。

はじめに

2003年のNPO情報セキュリティフォーラム（ISEF）設立・2004年の情報セキュリティ大学院大学（IISEC）開学から20年、インフラとしての情報ネットワークへの地球規模での依存度が増す一方、様々な要因によるリスクの増大により、予測困難な事態への対応が求められる場面も少なくなく、情報／サイバーセキュリティの重要性がますます高まっています。一方、OECD（経済協力開発機構）が今世紀初頭に策定した情報セキュリティガイドラインにおいて、全世界の情報ネットワーク参加者が共有すべきものとして謳った「セキュリティ文化」は、この20年でどのような変化を遂げ、この先20年でどのように進化していくのでしょうか。

私たちはこうした課題意識から、ISEF設立・IISEC開学20周年記念事業の一環として、2023年の終わりから2024年にかけて「情報セキュリティ文化の醸成を目指して」を共通テーマとしたリレー講座を開講し、その締めくくりとして学校法人岩崎学園の創立記念日である11月1日には、情報セキュリティ大学院大学同窓会の協力を得て記念シンポジウムを開催いたしました。

本講演録は、さまざまな形でISEF/IISECを支えてくださっている皆様への感謝の気持ちを込め、また両機関の活動内容や情報セキュリティに関心をお寄せいただいている皆様に向け、このリレー講座とシンポジウムの内容を、日経BPコンサルティングの編集協力により臨場感あふれるダイジェストで再現し、20周年記念誌に代えてお届けするものです。

以下、簡単に各回の内容をご紹介させていただきます。

第1回リレー講座では、「DXの実現を担うプラス・セキュリティ人材とリスキリング」をテーマに、IISEC学長後藤厚宏がMM総研の関口和一氏、デロイトトーマツコンサルティング（※講演時）の森正弥氏をお迎えし、ミニレクチャーと鼎談形式で、コロナ禍を経て一気に進展しているDXの成否のカギを握るセキュリティ人材の現状と、時代やトレントの変化に翻弄されない強靭なスキルや素養をどのように身につけるべきかについて議論しています。デジタル依存が進む中でのサイバーリスクに対する複合的対応の必要性や、AIの進化による利便性の陰に潜むセキュリティリスク、情報共有不足が被害を拡大する懸念が示され、多様な視点からの包括的セキュリティ対策と、人材育成を通じた安全な社会構築の重要性が再認識されています。

第2回リレー講座では、「セキュリティ人材のキャリアパス」をテーマに、国立研究開発法人情報通信研究機構の盛合志帆氏にご講演いただきました。サイバーセキュリティ人材の需要とキャリアパスに焦点を当て、特にセキュリティをビジネスリスクとして再認識することの重要性が述べられています。経営陣の意識改革と異分野からの人材参入が求められており、セキュリティ分野の開放性を高める必要性などが指摘されています。

第3回リレー講座では、「汚れたインターネットと通信事業者の戦い―対マルウェア攻防の20年、将来はどう守るのか？―」をテーマに、NTTコミュニケーションズ株式会社の小山覚氏にご講演いただきました。サイバークリーンセンター（CCC）の活動を始めとする20年間のマルウェア対策の取り組みや、実際に受けたサイバー攻撃の経験からフォレンジック調査の重要性と基本的なセキュリティ対策の徹底が求められること、また、実践的なセキュリティ人材育成の推進とOffensive Securityによる対策強化などについてお話しいただいています。

第4回リレー講座では、「英国 Cybersecurity Fellowship 参加報告―若者向けサイバーセキュリティ人材育成：英国と日本の比較―」をテーマに、株式会社BLUEの篠田佳奈氏にご講演いただきました。英国と日本における若者向けサイバーセキュリティ人材育成の現状と課題を比較検討し、国家戦略に基づく一貫した取り組みがあり、早くからセキュリティ教育を開始している英国に対し、日本では各省の教育プログラム間の連携が不足しており、今後に向けてより洗練された人材育成の体制を整える必要性を強調されています。

第5回リレー講座では、「インフォデミック時代におけるフェイクメディア克服の最前線」をテーマに国立情報学研究所の越前功教授にご講演いただきました。生成AI技術の進化により生成が容易となった高精度なフェイクメディアに対抗するため、深層学習モデルを用いた検出手法や、サイバーワクチンのような技術を駆使し、高度な検出・無毒化技術の実現を目指していること、今後に向けては、AIを使ったコンテンツモデレーションや透明性の確保に加え、新たな偽情報手法への対抗技術の開発の必要性が強調されています。

第6回リレー講座では、「事業継続を脅かすサイバーリスクの実態と対策」をテーマに八雲法律事務所の山岡裕明弁護士にご講演いただきました。企業の事業継続を脅かす主要なサイバーリスクとしてランサムウェア攻撃を取り上げ、大企業のみならず中小企業もターゲットとなっている状況を指摘するとともに、攻撃が分業化し誰でもサイバー攻撃を実行できてしまう現状を踏まえ、VPNのぜい弱性管理や多要素認証の利用、BCPの策定を提案するとともに、経営層が積極的にサイバーセキュリティ体制構築に関与する必要性を強調されています。

第7回リレー講座では、「世界に普及可能なコンピュータやネットワーク技術の生産手段の確立」をテーマにソフトイーサ/NTT東日本/IPAの登大遊氏にご講演いただきました。ITが社会基盤としての重要性を持つ中で、新しい人材育成の方法が求められていること、特に自由な技術開発環境の創設や試行錯誤を通じて国際競争力を高めることが重要であり、また、OSSの活用やセキュリティを強化する体制整備も必要であること、IT人材の育成と技術力の向上が今後の日本の産業競争力の鍵となることなどを指摘されています。

これらのリレー講座シリーズの締めくくりとして、2024年11月1日に「情報セキュリティ文化の醸成を目指して―明日の信頼を創ろう―」をテーマに、情報セキュリティ大学院大学（IISEC）開学およびNPO情報セキュリティフォーラム（ISEF）設立20周年記念シンポジウムを開催いたしました。

株式会社SNKの松原健二氏による基調講演「人生はゲームだ!!」では、大学院を卒業後、日立製作所でスーパーコンピュータの開発に従事したのち、日本オラクルを経てゲーム業界に転身した経緯に触れ、同氏が多様なキャリアを通じて得られた経験が語られています。ゲーム制作の理性と感性の両面に魅力を感じ、業界の発展と自らの成長を実現してきたこと、グローバルなビジネス経験を積み、業界全体の技術向上と国際展開を目指す活動へ取り組んでいることなど、挑戦し続けることで得られる多くのことが示唆されました。

Elastic社の中島明日香氏による基調講演「セキュリティコミュニティの入り方・歩き方・活かし方」では、NTT研究所からElastic社へとキャリアを経た自身の経験をもとに、成功の鍵は、積極的なネットワーキングと情報発信であることとされています。実力をバランスよくアピールすることで様々なチャンスを得てコミュニティの価値を最大限に活かし、自身のキャリアや組織の発展に寄与することができると強調されています。

シンポジウムの最後のセッションでは、モデレーターに現IISEC同窓会長であるJDDの唐沢勇輔氏、パネリストとして3名のIISECの修了生―AWSジャパンの吉濱佐知子氏、ガートナージャパンの澤田忍氏、NTTセキュリティ・ジャパンの羽田大樹氏―に登壇いただき「VUCA時代のキャリア構築とIISEC―IISEC Alumni reunion 2024―」と題したパネルディスカッションが行われました。それぞれの立場からIISECでの経験がキャリア形成にどのように影響したかを振り返り、セキュリティの内製化が進む中で技術とビジネスの双方を理解する人材の重要性が強調されるとともに、AIの進展が業界に与える影響、特に生成AIが代替可能な仕事と人間の価値を高める仕事の区別についても議論いただいています。また、IISECのOBOGとして母校に望むのは、多様性と国際性を兼ね備えた人材育成の強化であり、教育プログラムのさらなる拡充についてもご要望をいただきました。

皆様には、情報セキュリティ関連の各分野を牽引する研究者、技術者、実務家の方々をお迎えして実現した本シリーズの講演内容について、ぜひご関心のあるテーマからお読みいただき、サイバー・フィジカル融合時代に私たちが目指すべき、あるいは共有すべきセキュリティ文化について考えるきっかけとしていただければ幸いです。

第 1 回

DXの実現を担うプラス・セキュリティ人材とリスキリング

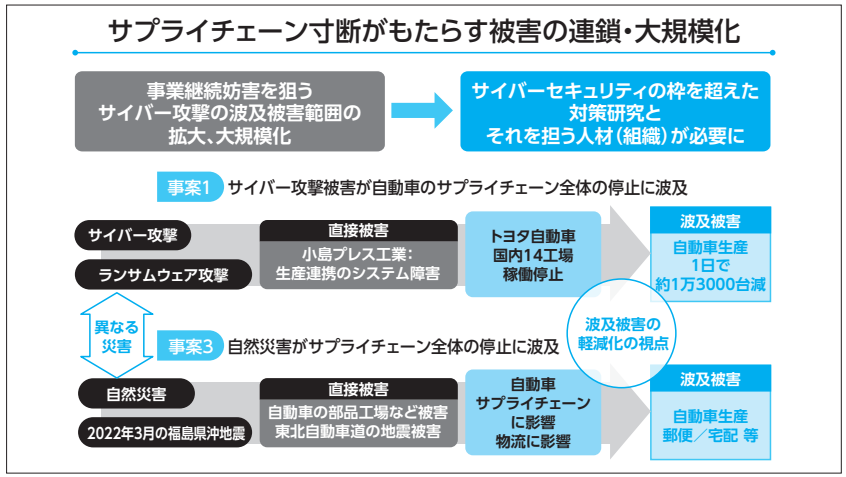
登壇者

デロイトトーマツコンサルティング 執行役員　**森 正弥** 氏
情報セキュリティ大学院大学 学長　**後藤 厚宏**
ファシリテーター：MM総研 代表取締役所長　**関口 和一** 氏

森 氏　後藤　関口 氏

DXの実現を担う人材に なぜ「プラス・セキュリティ」を求めるか

情報セキュリティ大学院大学 後藤厚宏：私たちは日常生活から仕事まで、どっぷりとデジタルに依存しています。国、社会、産業、生活において、デジタルへの依存が急速に高まっています。こういう状況で、どのようなリス



クを考えるべきなのかというと、3つの観点があります。

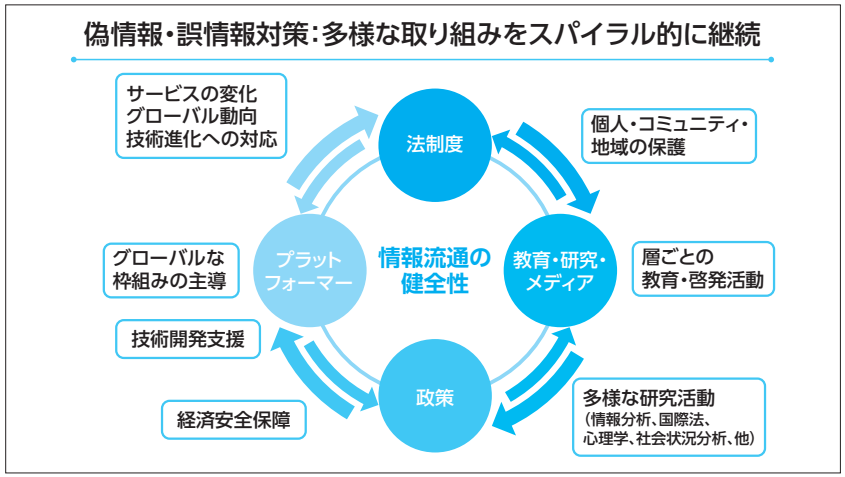
3つの観点のうち2つは、サプライチェーンのサイバーリスクと、その波及被害です。サイバー攻撃で何か事件が起こったときの波及被害が非常に広がってきています。特にサプライチェーンの寸断による事業継続問題への波及が深刻です。

前ページの図の上はサイバー攻撃が発端で、下は地震が発端ですが、起こっている波及被害には類似性があり、双方とも被害が広がっています。そうなると、これまで私たちはサイバー攻撃の問題を考えるときに防災や地震の専門家に相談してきませんでしたが、今後は相談する必要があるのではないか。やはり同じように問題が大きくなることを考えると、防災の専門家とわれわれサイバー領域の専門家が一緒になってしっかり議論したほうがいいのではないか、と考えます。

3つ目は、偽情報、誤情報です。英語ではミスインフォメーションまたはディスインフォメーションという言い方をしますが、それが社会をいろんな意味で不安にさせています。

巧妙な偽情報がいろいろと作られているため、どうしてもだまされるリスクが高まっています。偽情報かどうかの確認に手間もかかります。

これは、個人、コミュニティーの社会活動や、企業活動の全体としての質



の劣化、または効率の劣化を招きます。せっかくITで効率を良くしたはずが、偽情報が混じっているかもしれないということで効率が落ちてしまいます。

「偽情報を止める法律を作ればいいんじゃないの」というそんな簡単な話ではありません。法制度から教育、研究、メディア、政策、プラットフォーマー、全ての人たちがそれぞれの取り組みをしながら、お互いに連携し合って対策を進める必要があります。多角的な取り組みを連携させていかないと、この問題は解けないためです。

デロイトトーマツコンサルティング 執行役員 森正弥氏：特にコロナ禍によってグローバルのサプライチェーンの分断など、さまざまなダメージを受けましたが、むしろそれによってデジタルの実用化がすごく進んできた面もあります。サプライチェーンのデジタル化によって、サプライチェーンのリスクが広がっています。

私は、デロイトトーマツグループでAIのイニシアチブを統括しており、毎年グローバルで3000社ほどの企業にAIの活用度調査を行っています。去年（2022年）までは日本企業のAI活用度は、世界平均から見て非常に遅れていました。世界平均ではこれぐらいAIを活用していて、これぐらい成果を出しているみたいな値に、日本企業が全然及んでいませんでした。しかし、今年のサーベイで初めて逆転しました。日本が進み始めてきているのです。いくつかの領域で、AIの適用が少し進んできているところがありました。

その内の1つとしてあるのが、製造業のサプライチェーンでした。これは現場でのIoT化の進行の影響が結構あるのかなと思っています。IoTは特にセキュリティに気をつけなければいけません。従前の企業のシステムがあって、その周辺がIoT化していって、従前の企業システムとつながり始める。しかもいろいろヘテロジーニアスな環境の中で。だから攻撃しやすいような穴をいっぱい作ってしまうかもしれないようです。

特にサプライチェーンにおけるAI、デジタルの関係は、すごく活用の余地があります。例えば生成AIも需要予測や販売予測の高度化にすごく効くというのが、業界の共通認識になっています。例えば、このニュースがこの需要に影響する、このサプライチェーンに影響するみたいな需要予測や販売予測はすごく高度化できるという論文がものすごくいっぱい出てきています。

また、われわれはシンガポールの海運会社のコンサルティングを担当していますが、さまざまなサプライヤーから戻ってくる見積もりを、今までは専門家が分析していました。それを全部生成AIが判断するという仕組みをその海運会社が作りまして、期間も大幅に短縮したそうです。

本当にいろいろなところにデジタル化やAIの実用化が進んでいて、攻撃しようと思うとできてしまう話が増えています。活用によって便利になるのと同時に、守りということもやっていかないといけないと、後藤先生のプレゼンを聞いて思いました。

MM総研 代表取締役所長 関口和一氏：私は進行役であると同時にパネリストとして参加させてもらっているので、後藤先生の話を伺って思ったことを一言だけお話したいと思います。MM総研というのはITの調査会社なので、いろいろ調査はしているんですけど、先ほど森さんからお話があった生成AIの活用は、かなり日本は出遅れているという感じでした。しかしながらここに来て、だいぶ巻き返しているということですけれども、そういう新しい技術がきちんと使えているかというと、そうではないというのが今の日本の状況ではないかと思います。

従来のセキュリティの問題というのは、以前はコンピュータに対してネットワークで攻撃するといったことが主で、サイバー空間・電子空間の中で完結していたわけです。一方、ここに来て増えているのが、新しい情報通信技術を活用してリアルの世界を変えていくということ。すなわち自動運転やドローン、あるいは3Dプリンターですとか、こういったリアルな世界が実はICTの技術で変わっていっているというところから、セキュリティについても問題の裾野が広がっていっているのではないかと思います。

【ディスカッション1】

■ 世の中に絶対大丈夫だという手段はない

関口氏：さて、それではここからディスカッションに入りたいと思います。後藤先生にはまず、直近で起きている新しいこととは一体何なのか、ということをもう一度お聞きしてよろしいでしょうか。

後藤：IoTなど、いわゆる本体のコンピュータだけでなく周辺のものに広がっています。全てのものが何らかの意味でデータに関係している。100分の1でも関係していると、サイバー攻撃か人為ミスかにかかわらず、その1%の不具合であっても全てが止まってしまう。そういうことに関して、改めて意識を変えないと、今後のサイバーセキュリティリスクをとてもカバーし切れないのではないか、というのが1つです。

私たちは完璧な100%の解を求めてしまうわけですが、もう何が起こるか分からないです。絶対大丈夫だという手段は世の中にはありません。いわゆるシルバーバレット（困難を一発で解決できる方法）はない状態と思わないといけないのではないでしょうか。

関口氏：今までの日本の製造業の現場というのは、インターネットと隔離されたようなところでやってきたのが、この10年ぐらいで一気にインターネットとつながるようになってきました。そういう意味でマルウェアなどが入ってくる口がいろいろなところに出てきています。それに対して現場のシステムも追いついていないし、また人もそれに対する学習がきちんとできていなかったりと、いろいろな危険性があると思います。その辺りはいかがでしょうか。

後藤：そこもおっしゃる通りですね。以前海外で、ネットワークから完全に切り離されているコンピュータに、保守員の人がマルウェアを運んでしまった事件がありました。これもいろいろな説がありますが、USBメモリーで運び込んでしまったという話が有力です。先日も日本で似たような事件がありました。一瞬でも外につながれば、そこにリスクがあるということです。

関口氏：森さんはいかがですか。

森氏：波及効果の話ですが、2022年6月に3つのクラウドサービス事業者で合計4000億円以上の被害が立て続けに発生したという事件がありました。社労

士向けのクラウドサービスと、LPガス事業社向けのクラウドサービスと、一般のクラウドサービスでランサムウェアの攻撃があって、社労士向けのサービスでは2700社以上、LPガス向けでは1100社以上、一般向けサービスでは1000社以上というインパクトが出て被害を被った、というものです。これはサプライチェーンではないですけれども、その1つの起点として大きな被害を受けるみたいな話がすごく広がった事例だと思っています。

つまりこれは、誰かがクラウド化をするというのはもう当たり前になってきたので、こういう攻撃が出てきたということです。デジタル化は知らず知らずのうちに結構進んでいるので、至るところでやはりサイバーセキュリティの防御というところをきちんと取らなければいけないんだと思っています。

【ディスカッション2】

■ **クラウドといえどもお任せでは危険**

関口氏：日本は東日本大震災が起きるまではあまりクラウドは使っていませんでした。東日本大震災で病院や学校のコンピュータが流されてデータもなくなってしまい、患者さんの診療に当たれない、あるいは通信簿が付けられないという状況になり、やはりこれはクラウドを使ったほうがいいと思うように変わったわけです。

また、DX＝（イコール）クラウド化みたいなところがあって、この10年でクラウド化が急激に進みました。これはセキュリティの観点で言えば、もともと日本ではデータは自分のところに持っているのが一番安心で、人に渡すのはとんでもないという話だったわけです。それが、餅は餅屋に任せたほうが安心だという説に急激に変わったわけです。でも、それによってセキュリティの度合いは危なくなったのか、良くなったのか、どうなんでしょうか？

後藤：私自身は、普通の組織、企業のセキュリティ対策に比べれば、昨今のクラウドサービスのほうがセキュリティレベルは断然高いと認識しています。

ただし、クラウド大手は、世界中のシステムを扱っているわけですね。1社でこぢんまりとやっている場合と比較して、何か起こったときの社会的なインパクトは計り知れない。とんでもない破壊的な被害が起こるわけなのです。ではそのようなクラウドサービスを使っているユーザの方はそのときの覚悟ができていますか、というのは問いかけたくなります。

あと、クラウドサービス大手の会社のサービスも、実はたくさんの部品クラウドサービスで出来上がっています。つまり、SaaSの世界は、たくさんのクラウドサービスの集合体で成り立っているのです。そのどこかが問題を起こすと、やはりサービスが止まってしまうということになります。特に最近話題となっているのが、ID管理関係ですね。認証の部分に何かしら不具合が起こることで、関連するクラウド全体に被害が及ぶというのも実際に起こっています。

関口氏：森さんは、クラウドに関していかがですか。

森氏：後藤先生が最初におっしゃった通り、クラウドのほうが安全だという場面はありますね。特にさまざまな規制に対応できる企業は少ない。グローバルのクラウドに乗っかったほうが対応できるというのは間違いありません。ただ一つ言えるのは、手放しで自分たちは何もしないでOKではないということです。例えば、アプリケーションや、あるいはデータベースの組み方によって、いくらでも穴を作ってしまえます。

クラウドを利用するとインフラは安全だというところがありますが、手放

しでは駄目で、結局のところサイバーセキュリティへの対策をやらなければいけません。どのような環境であれ、現代のIT環境を構築する上ではセキュリティは必要不可欠であるということ。そこがもっと浸透していく必要があるのかなという気はします。

関口氏：クラウド化が進んだことによって、昨今よく使われているのが、APIの活用プロジェクトです。すでに作られた、しっかりしたものを上手に使えば、短期間で新しいソフトをすぐに作れるし、社内にIT本部みたいな大がかりな仕組みを持たなくても最新の情報通信技術が使えるという意味では非常に良いと思います。

一方で日本というのは、いまだに自前主義がはびこっていて、自分のところで開発しないと心配だ、人のものには頼れないということで、自前のものとそうでないものをつなぎ合わせたりしています。クラウドについても、ハイブリッドクラウドなどと言って、自前のシステムとクラウドをつないだりしていますが、そういうところにも危険性が潜んでいるのではないかと個人的には思います。後藤先生はいかがでしょうか。

後藤：今、ハイブリッドクラウドを構築する際の注意点について授業で扱っているところですが、本当に簡単ではありません。まずクラウドの良さを発揮するのは当然であって、そこで今おっしゃったように、提供しているAPIが理解できて、ユーザーはきちんとクラウドを使いこなせているのかが問われるわけですが、実はそこが違う場合が多いようです。私は数年前から、そういうAPIをお客様にきちんと説明するようにクラウドサービスは努力しなさいよ、お客様はそれの勉強をしなさいよ、というガイドラインを作っています。にもかかわらず、いまだに問題が増え続けています。さらに、別の観点の取り組みも必要なのではないかなという気がしています。

【ディスカッション3】

■ 人間もAIもミスをする

関口氏：森さんはいかがですか。

森氏：それで関係してくるのは、もしかしたらAIのトレンドかもしれません。というのは、基本的にはAIの研究者は、データを中心とした世界でやっているので、サイバーセキュリティに基本的に関心を持つ機会が少ないんです。それで作ってしまってリリースして出たものが、すごくセキュリティ上の穴があるというケースが少なくありません。

なので、今AIのアプリケーションがどんどん世の中に公開される一方で、セキュリティ上の穴があったりして、そういうのがAPIで出てくるみたいなところはあります。そういう意味で言うと、新しい技術のAPIというのは、確かにリスクがありますね。

話が変わりますが、大企業は基本的にリスク回避型なので、先行事例がない限りはやらないという姿勢だったのが、ChatGPTなどの生成AIに関しては先行事例に積極的に取り組んでいます。しかも企業システムと普通にリンクしています。これはすごく興味深い動きだなと思っています。他の国のプロフェッショナルと話すと、「日本は異様に進んでいる」みたいな話になり

ます。ゆえに、生成AIのトラブルに各企業の皆さんが今直面されている話につながってきています。特に一番多いのが、社内のデータと連携させて検索するシステムを生成AIで作るケースです。これの性能、精度が全然出ないというのが、各社さんのトラブルとしてあります。これはある意味学びをしているという意味で良いのですが、セキュリティ的な問題が発生するような話もあったりするので、アプローチを少し考えたほうがいいのかもしれません。

関口氏：プログラミングにも生成AIが使えるわけでして、人間が書くよりもきれいなコードができるという話を聞いています。でも、本当に正しいものができているのかどうか、多分どこにも保証がないのではないかと思います。また、問題が起きたときに、人間が作ったものではないですから、人間が対応できなかったりすることもあると思います。そういう問題はどうなんでしょうか。

森氏：いわゆる「ハルシネーション」ですね。生成AIに回答を作らせると、それっぽい本当のことのようなアウトプットを生成してしまうのが問題になっています。それを回避する手段の一つがRAG（Retrieval-Augmented Generation：検索拡張生成）です。それが日本の大企業で非常にはやっているのがポイントで、ハルシネーションを回避する手段は、各企業でもいろいろ模索しながらやっています。

併せて、出てきたアウトプットをそのまま使っては駄目だよというのは、日本の企業の方はみなさん思っています。だからそのままアウトプットを使っているというのは、日本の企業のリスク回避的な性格からそれはないという感じですね。

人間もミスをする。AIもミスをする。何にミスするかというのでミスのタイプが違いますという話と、もう1つはどれぐらいの割合でミスをするかという話があります。場合によっては生成AIもミスをしますが、人間のミスとは違うところでミスをします。そこを注意すれば大丈夫という話とともに、実はミスの発生率は人間より低いということがあります。特に画像認識での医療の診断みたいな話は、たぶんAIの画像認識の医療診断もミスをしますが、お医者さんのミスより圧倒的に少ないという話があります。ですから組み合わせの話うんぬんでもあります。あともう1つは生成AIの結果をそのままスルーさせずに人間のチェックは必ず必要だということです。

関口氏：情報セキュリティ大学院大学では、生成AIについて特に何か試みや取り組みをされているんですか。

後藤：私ども情報セキュリティ大学院大学の方針は、積極的に生成AIを使おうよです。森さんがおっしゃったように、AIの未熟なところも自分で使ってみないと分からないよね。どんどん使ってそれを確かめてみようよ、ということを呼びかけています。まずはAIを使ってみて、「このツールを使ったらこんなのができた」「使い方を誤ると危ないね」など、そういうことをオープンに議論し合うことを大事にしています。その後に授業の中で、次のステップのAIはどういうものが作れるのか、さらにそこはどういうセキュリティ的な問題があるのかという議論もしています。もちろん、セキュリティ対策にAIを使ってみることもたくさんやっています。それこそマルウェアの分析にAIを活用する研究もあります。今後、良い成果が出ればなと思います。

【ディスカッション4】

■ まずは波及被害の把握が大切

関口氏：インシデントが起きてしまった際の対応をどうするかというのも大きなテーマになっていると思うのですが、その辺はどういう取り組みをされていくのでしょうか。

それと、セキュリティ対策に無制限にコストをかけるわけにはいきません。どの程度のさじ加減でやったらいいのか、その辺りはいかがでしょうか。

後藤：大事なのは、波及被害の予測です。例えば直接の被害が1億円だと、波及被害は10億なのか、100億なのか、1兆円なのか、そういう見積もりはやはり必要だと思います。その感覚がないと対策に生かせません。

一方、例えば南海トラフ地震に関しては、ハザードマップが発表されています。現在は社会全体を守る必要があるという認識がわれわれの間に広まってきたので、地震や水害、台風のハザードマップに関して自分の住んでいる地域の危険度の値を私たちは受け入れられるようになりました。同様に、サイバーセキュリティの世界でも、例えばこの会社がサイバー攻撃を受けた場合にどのような被害が発生するか、自社との依存関係から波及被害規模などはどのぐらいになるのか、ということを事前に把握すべきだと思います。

まずはシミュレーションによって、定量的に被害の予測や対策を検討することから始めないといけないのではないかというのが今の問題意識です。

関口氏：森さんはいかがでしょうか。

森氏：定量的に、試算をして、それを社会に提供するのは、確かに重要なことだと今伺っていて思いました。確かに言われてみれば、サイバーセキュリティに対しての社会的なインパクトというのはもっと共有されてよいのではないでしょうか。そうしたときに私たちも変わっていくのではないでしょうか。

例えば、環境負荷や環境保護みたいな話は、欧州を中心にいろいろな政策が共有されることによって、行動変容がもたらされているということがあります。そういう意味で言えば、サイバーの被害も共有することで行動変容が起きるというのは必要かなと思います。

関口氏：私の友人で保険会社に勤めている人がいますが、保険会社の観点で言うと、技術的にセキュリティインシデントを食い止めるのは彼らの仕事ではありません。セキュリティインシデントが起きてしまったときにどうすればよいか。被害をいかに最小限にするかということを、企業に対し常日ごろから指導するという立場にあるそうです。彼らのコンセプトとして注目しているのが、PMLすなわち「Probable Maximum Loss（想定被害総額）」です。もしこういうインシデントが起きたらこれだけ被害を被るよ、というのを事前にシミュレーションしてみると、どれだけコストをかけてセキュリティを担保すべきかということが分かってくるそうです。

今まで日本の場合は、セキュリティ部門というのは会社組織の中ではコストセンターと見られ、かかるお金が少なければ少ないほど良いという視点だったと思います。ですが、そのPML的な発想で、どれだけ被害が及ぶか最初に分かっていれば、売上高の何%まではお金をかけていいよねという企業内でのコンセンサス作りがしやすくなるそうです。そういう企業の取り組みは今、変わってきているのでしょうか。

森氏：企業の中では、セキュリティは意識的にはやらなければいけないというのはだいぶ浸透したと思います。

生成AIの話になりますけれども、多くの人が生成AIの普及と同時に、リスクコントロールを自らの問題として考えるようになりました。そのリスクコントロールのコンサルタントは今すごく引き合いが多いです。「AIガバナンスおよびリスクコントロール」です。

サイバーセキュリティに関する今年のサーベイで企業の意識というのを調査したところ、「サイバーセキュリティは、あなたにとって何ですか」みたいな問いかけで、「技術の課題に対して自信が持てるようになった」という答えが一番多かったんです。つまりサイバーがあるからこそ自分でChatGPTが活用できるんだという意識をちゃんと持てるようになった。要するに、アク

セルを踏みながらブレーキを踏むみたいな印象がすごくある。だから、今まではセキュリティは別にやらなくていいんでしょうみたいな話はあったかもしれないですけど、そこら辺がだいぶ変わってきている気はしています。

関口氏：後藤先生、セキュリティ投資の度合いはどうでしょうか。

後藤：上向きには感じます。ただ、十分という感覚とはまだまだかけ離れています。企業のCxOの方々で話が通じる人が少ないのが現状でして、なかなか投資という意味で言うと、もう一押ししないと、という感じです。

【ディスカッション5】

■ 素早い情報共有が安全につながる

関口氏：サプライチェーンを正しく維持して、かつそういった波及被害を少なくするためには、個人的には情報の共有が大切だと思っています。ただ、残念ながら日本には、恥の文化といいますか、被害に遭ったことを公に言いたがらないという風潮があります。そうすると報告が遅れてしまい、現場から情報を上に上げる際にもそこにタイムラグがあり、またその上に伝えるのも遅れるということになります。この連鎖が結果的には被害をどんどん大きくしていると思うんですね。

情報を速やかにつまびらかにして共有するという、対応策は進んでいるのかどうか。後藤先生、いかがでしょうか。

後藤：米国ではCISA（Cybersecurity and Infrastructure Security Agency：米国サイバーセキュリティ・社会基盤安全保障庁）がセキュリティの大元締めとして国の政策を担っています。特に重要インフラなどを担っている企業は、セキュリティ事故が発覚したら報告する義務があります。報告しないと罰せられるんです。

ただその報告をしたときにCISAから叱られるのではなくて、CISAの専門官チームがサイバーセキュリティ事故の救助にかけつけてくれるのです。つまり被害が広がったりしないようにまずは被害に遭った組織を助ける。それが大事だという姿勢を国が示しているんです。

日本でもサイバー攻撃の被害に遭ったら届けなさい、という指示は出ているんですけど、報告すると被害に遭ったことに加えお役所から叱られます。そうであれば企業は全部収まるまで、全部言い訳ができるまで公表しなくなってしまう。もともと日本には恥の文化がありますけど、まずは国などが率先して、「いや、そうじゃなくていいんだよ。早く報告してくれれば社会全体が守れるから、助けるよ」という姿勢を示すべきだと思います。

関口氏：やはり日本のメディアの取り上げ方も良くなくて、本当は攻撃をした方が悪いのに、攻撃を受けた方が悪いかのように報道をしてしまう。そうすると、悪く書かれるのが嫌なので、言いたくないという雰囲気があるのではないのかと思います。海外のメディアですと、「攻撃を受けた」ときちんと書くんですが、日本ではどうしても「情報が流出した」という書き方になりがちなんですね。

森氏：関口さんがおっしゃったように、メディアの協力も必要だと思います。

関口氏：そういう意味でも、正しいセキュリティ文化の醸成が必要です。情報セキュリティ大学院大学の情報セキュリティ文化賞という表彰事業も、正

しいセキュリティ文化をこの国に根付かせていこうという取り組みです。そして最終的に大事なのはセキュリティ人材の質やセキュリティ意識の向上だと思います。専門的なセキュリティ人材の育成も大事ですし、経営層のセキュリティ意識の自覚も大事です。また世の中の一般投資家が企業のセキュリティ投資をどう評価するかも大事でしょうし、セキュリティインシデントが起きた場合のメディアの正しい取り上げ方も重要だと言えるでしょう。

第 2 回

セキュリティ人材のキャリアパス

登壇者
国立研究開発法人 情報通信研究機構
執行役　サイバーセキュリティ研究所長　**盛合 志帆** 氏

セキュリティ人材需要を探る
海外動向調査と国内外事例インタビュー

情報通信研究機構（NICT）のサイバーセキュリティ研究所では、この分野ではどのような人材の需要があるのか、また海外の動向はどのようになっているかなどを定期的に調査しています。今日は、NICTサイバーセキュリティ人材育成レポートとして「サイバーセキュリティ・トランスフォーメーション『ビジネスリスクのニューノーマル』」と題して2022年に公開したものに沿ってお話ししていきます。

今日ご紹介するサイバーセキュリティ人材の需要調査は、NICTのナショナルサイバートレーニングセンターで実施しています。なおこのセンターでは、実践的サイバー防御演習「CYDER（サイダー）」や、25歳以下の若手の人材育成「SecHack365」のようなプログラムを行っています。

今回のレポートは、海外の各種調査レポートの分析や国内外でセキュリティ人材育成事業を推進している組織のトップの方へのインタビュー、セキュリティ人材を取り巻く諸課題を調査報告書として取りまとめています。

昨今のサイバーセキュリティ分野の人材の不足は、ビジネス環境に由来しているところがあると思います。特にコロナ禍以降、デジタル化が大きく進

展している中、サイバーリスクが非常に高まり続けているのにもかかわらず、特に国内では海外と比べると経営者自体のコミットメントが高くありません。サイバーセキュリティのエンジニアを見ても、国内では給与待遇が低いままという課題があります。

コロナ以降のビジネスのニューノーマルで見ると、サイバーセキュリティを事業の全体に統合していく、トランスフォーメーションが重要になってくると考えています。セキュリティプロフェッショナルに関しては、権限や給与体系、教育システムの見直しや他部門の優秀な人材をセキュリティ部門に再配置することも求められるでしょう。現在サイバーセキュリティにとって最も必要とされているのは、特に経営層の意識の変革と、異分野からセキュリティ分野に人材の参入を促すセカンドキャリアの支援だと考えています。サイバーセキュリティはもはや情シス部門や技術部門が対応するニッチな業務ではなく、ビジネス全体に関わる基盤インフラと考えて、今後のビジネスを見据えて、今すぐに経営者やセキュリティ業界がすべきことをこのレポートにまとめています。

サイバーセキュリティのリスクはビジネスリスクとして捉えるべき

第１章の「経営者のためのサイバーセキュリティの新常識」についてポイントをご紹介します。コロナ禍以降、業務環境の変革やランサムウェア攻撃なども非常に増えています。デジタル化を進める企業にとって、サイバーセキュリティのリスクは、IT部門が統括するテクノロジーリスクではなく、もはやビジネスリスクなのです。にもかかわらず、多くの企業ではなかなか十分な対応ができていません。サイバーセキュリティをめぐる企業の課題と処方箋について俯瞰（ふかん）していきたいと思います。

「サイバーセキュリティはビジネスリスク」ということで、これはガートナーの2021年の少し古いデータですけれども、海外での調査結果では、取締役会の88%がサイバーセキュリティをテクノロジーリスクではなくてビジネスリスクとして見なしています。その一方で、取締役会レベルのサイバーセキュリティの専門委員会を設置している企業はたった12%しかありません。最近はランサムウェアやサプライチェーンアタック等があり、その企業自体のオペレーションを狙ってくる、企業、組織、病院などにとってクリティカルなところをターゲットとしてくるということで、セキュリティはもはや事業に直結する問題になっています。IT部門だけではなく経営戦略として解決にあたるべき問題になっています。

これは最高情報責任者（Chief Information Officer, CIO）や最高情報セキュリティ責任者（Chief Information Security Officer, CISO）が経営陣と連携してサイバーセキュリティの投資をビジネスの文脈で捉え直して、しっかりとセキュリティ投資をビジネス全体に対しての説明責任として共有していく必要があるということです。

一方、情報セキュリティアナリストについてですが、米国では『100 Best Jobs』という人気職業ランキングがあり、ここでは毎年上位の職業です。このレポートを出した2022年の調査では1位ということで人気が高いのが分かります。給与面のスコア、将来性のスコアなどが高く、またストレスのスコアは、サイバーセキュリティの対応というのは大変ストレスがあるのでないかなと思いますが、例えば外科医などの医療系の従事者に比べると低めです。ワークライフバランスも比較的取りやすいということで2024年では7位になっています。米国での人気職業ランキングの2位以下の業種をみると、ファイナンシャルマネージャー、ソフトウェアデベロッパー、4位がITマ

サイバーセキュリティはビジネスリスク

- 取締役会（Board of Directors）の88%が、サイバーセキュリティをテクノロジーリスクではなく、ビジネスリスクと見なしているが、サイバーセキュリティ専門委員会を設置している企業はわずか12%（Gartner, 2021）。
- ランサムウェアやサプライチェーンアタックの多くは、オペレーションや企業にとってクリティカルな領域をターゲットとしている。セキュリティはもはや事業に直結する問題であり、IT部門だけで解決に当たるような閉じた問題ではない。
- CIOとCISOは経営陣と連携し、サイバーセキュリティ投資をビジネスの文脈で捉え直し、ビジネス全体における説明責任を共有する必要がある。

ネージャーです。6位がメディカルアンドヘルスサービスマネージャーということで、医療関係とIT関係が並んでいます。7位に情報セキュリティアナリストがあって、その下にデータサイエンティスト、その下に保険やリスクの監査をするアクチュアリーという職業が並んでいます。この辺りの職業は日本でこんなに人気が高いかな、と思いますが、本質的にセキュリティ分野は将来性を秘めている職業であることをわれわれも発信していく必要があると感じています。

また、日本企業が押さえるべき10の論点ということで、ガートナーが今年の1月に出した10個のポイントをここでまとめています。1つ目が新たなセキュリティガバナンスです。サイバーセキュリティやデジタルトレンドを踏まえて、新しい脅威の変化が出てきているため、ファクトベースで経営陣やビジネスリーダーに伝える、そして理解を促すことが重要です。セキュリティは組織全体として対応すべき問題であると共通理解を得ることが重要なのです。それから意思決定を迅速に行えるようにするためにも、分散型の意思決定を可能とするようなプロセスに移行していく必要があるという指摘もあります。

2つ目が新たな働き方とセキュリティです。テレワークもありますし、日常的に仕事の中にAIの活用が浸透していきます。ユーザーとして「検索窓や変換の入力に、組織の機密情報を含むいろんなデータを不用意に入れてしまったりしないようにね」など、新たに認識すべきリスクも増えるわけですので、従業員に対してのセキュリティ教育のあり方をこのタイミングで見直すべきということがこの調査では指摘されています。

3点目は、セキュリティオペレーションの進化に関することで、脅威への対策製品についてです。さまざまな対策を導入している企業が多いと思いますが、個々の製品がどのようにログを出力するのか、それを使ってどのように運用するのかなど運用の負荷について課題を抱えている組織も多いかと思います。またセキュリティ情報やイベントの管理のプラットフォーム、XDRと呼ばれるような製品なども導入する企業もあると思いますが、セキュリティのオペレーションをどう効率化していくかも重要になっていきます。

4点目は、インシデント対応の強化です。かなりサイバー攻撃の巧妙化も進んでおり、原因の究明にも時間がかかるようになってきています。IT領域だけではなくてOTやオペレーション、それからIoTの領域も攻撃対象になってきていますので、インシデントの対応範囲は、もう自分たちの製品や設備などいろいろなところまで拡大しているのが現状です。サイバー攻撃を受けてしまった場合に業務を停止する時間を短くするために、原因究明ももちろん大事ですが、システムをどう暫定的に復旧するかが優先されるように、対応プロセスを見直す必要があるという意見も出てきているところです。

他にも論点9では、データアナリティクスのリスクへの対応ということで、セキュリティチームと実際にデータを使う事業部門との間で、意思の疎通がうまくいっていないことがあって、事業部門側でデータのセキュリティやプライバシーに対する認識不足により、セキュリティに関する議論が十分に尽くされないまま、実際に解析をどんどん進めてしまうという可能性があります。個人情報を扱う場合に、セキュリティだけではなくプライバシーの配慮等の取り組みが、漏れなく実施される必要があります。

10番目がAIのリスクへの対応です。生成AIにまつわるセキュリティの話はいろいろなところで議論になっていますが、いくつか対応事例が挙がっています。①生成AIを職員が業務の中で利用するという場合、②自社の生成AIを自分たちのオペレーションに合わせる形で作っていくという場合、③生成AIをセキュリティオペレーションに利用する場合、そして、④生成AIを使ってさまざまなサイバー攻撃を高度化する動きが世の中で起こっている中での対応策についてです。こういうリスクマネジメントの必要性がプラスアルファで増えてきています。

日本のトップCISOによる新たなサイバーセキュリティの定義

次は、日本のトップCISOが語るサイバーセキュリティの新たな定義です。まず一つ目が、Preferred Networks執行役員の高橋正和さんへのインタビューになります。高橋さんには、サイバーセキュリティを経営にいざ統合

しようとすると決して簡単ではなく、セキュリティをめぐる組織内での考え方の齟齬、サイバーポリシーの重要性、経営とセキュリティの距離、それからこれから必要となる人材など、難しいところを乗り越えていくためにやるべきことについてお話を伺いました。

例えば事業統括のようなポジションになって経営に触れなくてはいけなくなった人たちにとってどのような準備が必要かなどをお聞きしています。高橋さんは特にインシデントシミュレーションを強調しています。必ずしもレッドチーミングというように、実際に商品やサービスに対して攻撃を仕掛けるようなものではなくて、机上の演習でもいいので、そのセキュリティの対策を通しでやってみることが重要だということです。セキュリティ対策の多くは、組織がサイバー攻撃を受けたり、インシデントが起きてしまったときに、チェックリストはあっても、デバッグやシステムテストみたいなことをやっていない組織が多いと思います。シミュレーションを一度事前に事業部門を巻き込みながらやっておくと、その事業部門の人が実際に攻撃が起きて復旧をするときに一体何を大切にしているか、ということもその中で分かってくるということです。

インシデントシミュレーションの助けになると思われる、私たちNICTで提供している実践的サイバー防御演習CYDERについてご紹介します。日々巧妙化するサイバー攻撃は、その脅威は個人のPCだけにとどまらず、国の機関や地方公共団体、重要インフラにまで及んでいます。攻撃の手法は多様化し、セキュリティ対策製品やサービスの導入だけでは完全に防ぎきれないのが実情であり、万が一攻撃による被害を受けてしまった際には、組織的に迅速かつ的確な対応が求められています。

CYDERは政府のサイバーセキュリティ戦略に基づき、総務省予算を受けて実施している公的なプログラムで、NICTが持つサイバーセキュリティの技術的知見と、北陸StarBED技術センターを核とする大規模計算環境を活用した体験型の演習プログラムです。

2013年からスタートしたCYDERは、これまで国の機関、地方公共団体など重要な機関の方々にご参加いただき、今や参加者累計1万人を超える規模の国内最大級の演習プログラムに成長しました。受講者の皆さんは、ある組織の情報システム担当者としてチームで演習に参加します。組織の仮想LAN環境下で実際さながらのサイバー攻撃を受け、被害発覚から収束までの一連の流れを体験、その具体的な対処を学んでいきます。CYDERは事前オンライン学習と、会場に集合して行うオリエンテーション、実習、グループワークのプログラムで構成されています。事前オンライン学習では、攻撃

実践的サイバー防御演習「CYDER」の概要

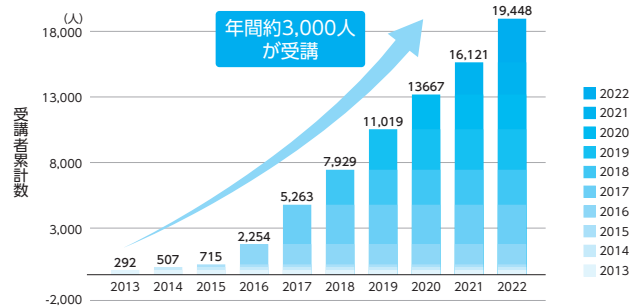
- 国の機関、地方公共団体及び重要インフラ事業者等の情報システム担当者等を対象に、仮想空間上に組織のネットワーク環境を再現し、一連のインシデント対応を模した実践的な防御演習を行う人材育成プログラム。
- 毎年、集合演習（全都道府県で100回程度）を中心に、約3,000人が受講（2017年度以降、延べ17,000名超が受講）。 ※令和5年度の受講者数は5700名超

概要（2023年度）

【受講対象】 国の機関、指定法人、独立行政法人、地方公共団体の職員（無料）
重要社会基盤事業者、民間企業等（77,000円　Cコース：121,000円）
【開催形式】 集合演習（グループワーク+実機演習）
オンライン演習（座学+実機演習）

コース名	演習方法	レベル	受講想定者（習得内容）	受講想定組織
A	集合演習	初級	システムに携わり始めたばかりの方（事案発生時の対応の流れ）	全組織共通
B-1		中級	システム管理者・運用者（主体的な事案対応・セキュリティ管理）	地方公共団体
B-2				地方公共団体以外
C		準上級	セキュリティ専門担当者（高度なセキュリティ技術）	全組織共通
入門	オンライン演習	入門	情報システム担当経験1年前後で知識のアップデートをお考えの方	全組織共通
プレCYDER		-	インシデント発生時の対応の学習をこれから始める、又は始めたばかりの方	国の機関等、地方公共団体

CYDER受講者数の推移（累積数）



の手法や対策など演習に必要な知識を丁寧に説明します。会場に集合して行う演習では、まず初めにオリエンテーションを行います。事前学習の内容を振り返り、不明点や疑問を解消し、より万全な状態で演習に参加できるようになります。本番の演習では、実際にサイバー攻撃を受けたことを想定したシナリオに基づいてデータを分析したり、対応をチーム内で議論したり、関係組織とコミュニケーションを取ったりしながら適切な行動を学んでいきます。グループワークでは参加者自身が所属する組織において、演習と同じインシデントが発生する想定でどう対応するかを検討します。この検討によって、単に演習を受けたということで終わらず、所属する組織に戻った後にすぐに行動に移すことができます。事前学習から受講後までしっかりとサポートするプログラムによって、単なる知識の習得にとどまらず、インシデント対応の一連の流れを体験的に学ぶことができます。そして、その体験の中での気付きを実務にしっかりと生かすことができるのです。

CISOのインタビューの第2弾ですが、こちらは楽天グループでCISO、CSIRTを担うお二人にお話を伺いました。まず、サイバーセキュリティと経営の統合について伊藤彰嗣さんは、「経済産業省が2015年にサイバーセキュリティ経営ガイドラインを出して、それを旗印にいろいろな企業がすでに取り組む中で、楽天もセキュリティというものをどう戦略として経営の中に取り込んでいくのかを考えるようになってきた」と語っています。伊藤さん自身はCISOを支える立場ということで、CISOの方が描いた戦略としてのセキュリティを肉付けしたり、その考え方を共有して手足として動けるような状態を作ったりしています。つまりセキュリティ戦略を戦術に落とすというところが役割ということでした。

経営とセキュリティを統合するという旗を振っただけでは、なかなか物事は進まないのが現状で、実際に実行していく役割の人が日本全体で不足していることを痛感されていました。実際、社内には必ずしもセキュリティを専門とした人材は多くなく、いわゆる文系の方でも職種を転換してセキュリティの仕事に従事することの可能性を聞いたところ、橘喜胤さんによると「セキュリティのエンジニアとなると、やはりITのスキルというのは最低限必要になってきますが、例えばCSIRTの活動はエンジニアだけが関わるものではなくて文系の方も少なからずいる」ということでした。特にセキュリティエンジニアというと、世間的にもどこかオタクっぽくてコミュニケーションは苦手といった印象もあるかもしれませんが、CSIRTの活動はむしろコミュニケーションが非常に重要なファクターになっているので、あちこちの部門の人たちやCISOが経営層と正しい言葉でコミュニケーションが取れる能力というのは必要で「文系理系が関係なく関われる領域というはたくさんある」ということです。

女性人材については、「今の時代は性別にフォーカスする必要もなくなってきており、国籍や人種についても特に楽天グループでは多種多様な人材がセキュリティに関わっている」ということです。お互いの価値観を共有し合う部分もセキュリティに加えて重要だとしてコミュニケーションの仕方については気を使っているそうです。

サイバーセキュリティ教育の第一人者である台湾科技大学の吳宗成先生は、「サイバーセキュリティプロフェッショナルの仕事において最も重要な資質はチームワークする能力だ」と指摘しています。そのことを伊藤さんに尋ねると、「CSIRTのTはコンピューター・セキュリティ・インシデント・レスポンス・チームのチームのTを取ったものであり「チームワークというのがサイバーセキュリティにおいての仕事の基盤であり源泉だ」と語ってくださいました。

セキュリティ分野のキャリアパスと環境整備に向けて

第３章では、「セキュリティプロフェッショナルにキャリアはあるか」というテーマで、ラック代表取締役社長の西本逸郎さんにお話を伺っています。特にサイバーセキュリティのキャリアパス不在という課題についてお話を聞きました。「日本はエンジニアへのリスペクトが低い」という指摘とともに「技術立国日本と言いながら技術者を切り捨ててきたところがあるのではないか」と語っています。米国では職種ごとに雇用を支える仕組みがあり、具体的にはセキュリティ業界というと、会社をまたいでいくつか仕事ができます。一つの会社で経験を積んで、それを元に別の会社でステップアップしていく仕事のやり方ができる業界になっています。一方、日本は一つの企業で経験を積むというのが現状で、一般企業だとなかなかサイバーセキュリティ技術者を継続的に雇用しないところがある。本来であれば組織内のキャリアパスとして、セキュリティエンジニアがステップアップできると良いのですが、そこが整備されているところが少ないようです。

ただ最近は、一部のCIOの方が、業界を超えて会社を移って活躍するという事例もあり、これからのセキュリティの技術者やCISOの方が、そういうキャリア設計ができるように、日本の習慣が変わっていくといいと述べられていました。キャリア形成に有意義なツールとして、SecBoK（Security Body of Knowledge）というものがあります。これはJNSA（日本ネットワークセキュリティ協会）で発行されているもので、情報セキュリティに関する業務に携わる人が身に付けるべき知識やスキルを体系的に整理したものになっています。そういう基準があることで、エンジニア自身もそのレーダーチャートを活用し、「ここは自分の強みだけど、ここは弱みだな」というところが把握できる。企業側も求人広告を出すときに、「ここの強みがある人を募集したい」というように、より良いマッチングができるので、こういうツールの有効性も指摘しています。

多様な人材のチームワークと学際性がセキュリティ教育のカギを握る

第４章では、台湾のサイバーセキュリティ教育に尽力してきた台湾科技大学の吳宗成先生にお話を伺いました。

2016年に蔡英文氏が台湾総統に就任して「サイバーセキュリティ＝ナショナルセキュリティ」（資安即国安）を打ち出し、それを受けて台湾教育部が大規模な予算を組みサイバーセキュリティ人材育成に関わる大型プロジェクトを立ち上げ、吳先生が担当してきました。「台湾は毎日のようにサイバー攻撃がある」という発言が印象的でした。台湾でも人材不足で、吳先生の人材育成のプログラムを修了した方は、複数の企業から内定をもらって選ぶほどだということでした。待遇も良いようです。またピボット教育ということで、一般企業等に在職しながらサイバーセキュリティの訓練を受けられるコースも官民で開設しています。特にサイバーセキュリティで重要な資質というのがチームワークですが、これはグローバル・サイバーセキュリティ・キャンプ（GCC）も重視されているキーワードです。韓国、日本、台湾等でこれまで開催されてきて、参加者も非常に国際的で、チームも多国籍チームが結構多いのですが、こういうところでもすごく重視されている。今後のサイバーセキュリティの国際対応ということで、チームワークはさらに重要になってくると考えておられます。またダイバーシティの観点では、ガールズ・イン・サイバー・セキュリティ（GICS）という構想もあるということで、女性向けの研修プロジェクトなども国を挙げて推奨されているということです。また今後は学際性も重要で、技術や管理の専門家だけではなくて、法律を含めた多種多様な分野の人材が必要ということも強調されています。

また、サイバーセキュリティは上層部のコミットが重要で、例えば、台湾の金融監督管理委員会で、サイバーセキュリティオフィサーはバイスプレジデント以上であることが法律で義務付けられているそうです。サイバーセキュリティの対策の実行には権限が必要だからということです。

海外と異なるサイバーセキュリティの捉え方
未経験者の育成や支援する仕組みの重要性

第5章は「誰でもセキュリティプロフェッショナルになれる」というタイトルで、GMOサイバーセキュリティ byイエラエの代表取締役社長の牧田誠さんにお話を伺いました。GMOサイバーセキュリティはいろいろな会社を巻き込んで事業を拡大しています。牧田さん自身はもともとイエラエセキュリティを運営しており、GMOサイバーセキュリティに2年前に参画したということですが、診断やペネトレーションテストなどの領域で、世界レベルのエンジニアを抱えています。待遇も良いということで具体的なお話も聞いています。

まず、現在の日本のサイバーセキュリティ業界には、諸外国に比べて攻撃がわかるセキュリティエンジニアの数が不足していることを指摘しています。イスラエルや韓国などの兵役がある国では、サイバーセキュリティが国防と関わっており、例えばイスラエルの「8200部隊」では、優秀な学生がリクルーティングされて軍のサイバー部隊のエリートとして育成されています。さらにそこを出た方は出口もきちんと用意されていて、「8200部隊出身」というブランドで、除隊した後にスタートアップなどを立ち上げるときも資金調達がしやすいそうです。国と個人とがWin-Winの関係になっているところも戦略になっていると指摘していました。日本はそういう環境にないということもあって、サイバー攻撃への意識に差が出てしまう側面があるようです。

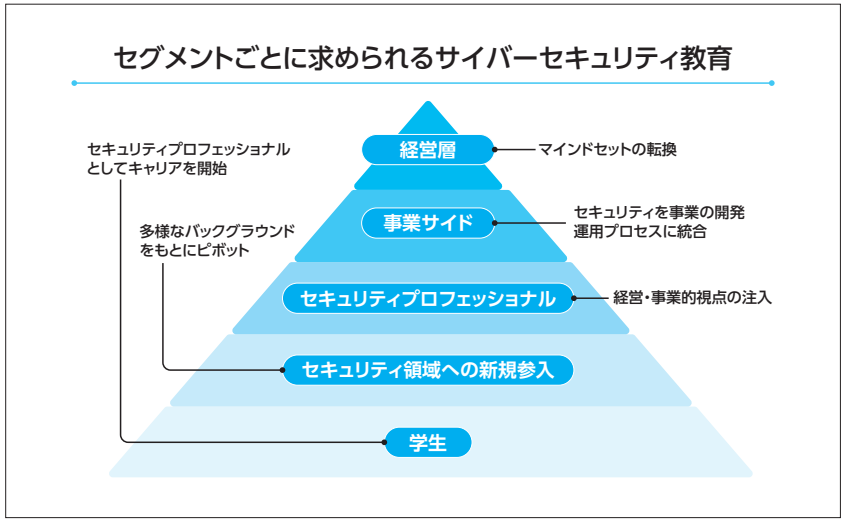
また牧田さん自身がこういう会社を立ち上げて考えていることとしては、「サイバーセキュリティエンジニアの良いロールモデルを作って、魅力的な職業にして、若手の人気の職業にしたい」という思いがあるとのことでした。そこでまずは給与を高くしているそうです。学歴は関係なく、大卒で年収1000万円や1200万円という人たちがいる一方、中には、高卒の方でも能力がある方には2000万円という人もいるということでした。つまり完全な能力主義にしているということですね。サイバーセキュリティの仕事は社会的意義が高いということは間違いないので、あとは給料がきちんと上がっていけば、自然と優秀な人たちが目指したい職業になっていくはずだと信じていると語っています。

セキュリティ技術は変化のスピードが速いのでスキルアップのサポートは手厚くしています。プログラムを提供するだけでなく、エンジニア自身が学びたいことを学べるよう自主性も重視しているそうです。もちろんそのためには学習時間も必要なのでスキルアップの時間的余裕を作るため、残業ゼロを目指しているそうです。一方で、評価制度については技術力をどう評価して給与に還元するのかは課題もあるということでした。また、「ゼロからの育成」として、セキュリティ業界未経験者を育成することも重視しており、例えば金融機関の営業からIT歴4カ月で入社してきた人材や、未経験で新卒で応募してきた人材を育成した事例もあるそうです。

サイバーセキュリティを事業のリスクと認識し
セキュリティ分野の開放性を高める

第6章では、「セキュリティ教育をめぐる施策とナラティブ」としてまとめ、冒頭で「DXから始めよ」と述べています。ここまでの調査で見えてきたことを整理すると、サイバーセキュリティは事業リスクとして考慮されなくてはいけない。そのためには、経営＝マネジメントの一環として、企業の経営に組み込まれなくてはいけないということです。ゆえに、役員会のコミットメントが不可欠です。さらに事業の運営サイドとの橋渡しや統合が必要だというところが見えてきました。

経営とサイバーセキュリティの統合ということでまとめてみますと、実際にデジタルテクノロジーが事業の基盤になっていくことは、後戻りしようのない現実です。それをマネジメント層がどれぐらい強く認識しているかということですね。それから、セグメントごとに求められるサイバーセキュリティ教育はやはり違います。経営層の方はマインドセットの転換が欠かせません。それから事業サイドの方は、セキュリティを事業の開発運用プロセスにしっかり統合することが大切です。セキュリティプロフェッショナルとして活躍中の方は、逆に経営や事業の視点から考えていく必要があります。そ



れぞれのレイヤーの人がセキュリティを意識していくことが重要です。

今後は、セキュリティ業界に新規参入していく多様なバックグラウンドを持つ人もどんどん増やすことが重要です。セキュリティの仕事をより魅力的にするために、給与や待遇の向上、それからやりがい、満足度の向上も考えていく必要があります。セキュリティプロフェッショナルが事業の上流工程から参加していくなど、満足度につながるような流れにしていこうという取組も必要です。

セイバーセキュリティという領域は、これまで閉鎖的で、専門的かつ同質性の強い面があったかもしれません。しかし、チームワークが重要な領域であり、開放性にシフトすることが重要なキーワードです。理系、またセキュリティ技術だけではなくて、文系、法律などの分野にまで広がる学際的な分野であることも忘れてはいけません。さらに、女性や外国籍の方も含めて、多様性といったキーワードもナラティブとして、シフトしていくことが重要だと考えています。

第 3 回

汚れたインターネットと通信事業者の戦い

―対マルウェア攻防の20年、将来はどう守るのか？―

登壇者
NTTコミュニケーションズ株式会社 情報セキュリティ部長
株式会社エヌ・エフ・ラボラトリーズ 代表取締役社長
小山 覚 氏

サイバークリーンセンターの活動で日本を世界一安全な国に

私の出身は三重県です。縁があって昭和63年（1988年）にNTTに入社しました。当時はまだ情報セキュリティという用語すら一般的ではない時代でした。私が配属されたのは、電柱やケーブル関連のエンジニア職で、ラインマンと呼ばれていました。私はそういう屋外設備の専門家として育てられました。

1995年に発生した阪神淡路大震災の復旧現場で働いていたある日、テレビをつけたら「電話の復旧より先に、インターネットが開通して東京とやりとりができるようになりました」とNHKのニュースで言っていました。このときはインターネットを全くというぐらい知らなかったので、「いつかインターネットに関わりたい」という思いが心の隅にずっと残りました。それから、大阪・日本橋の電気屋に行ってハブとルーターを買って、モデムを付けて……と、自分で手を動かしながら勉強を始めていき、97年に立ち上がったばかりのOCNのサービス開発部門に異動し、東京にやって来ました。

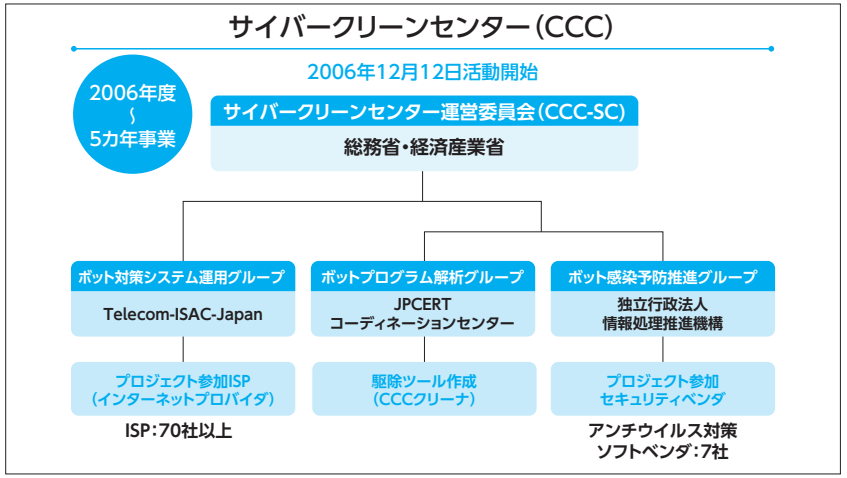
今日のお話の前半では、私がOCNのセキュリティ担当者として、2006年

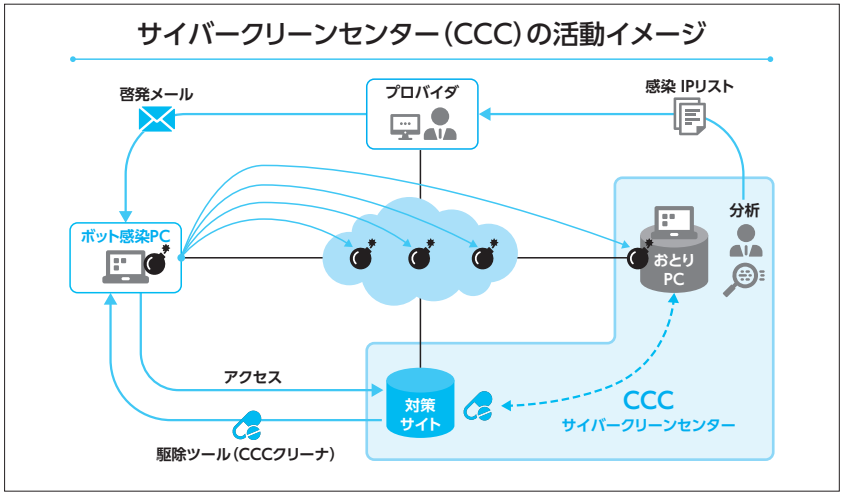
度に始まった「サイバークリーンセンター（CCC）」の活動に携わった経験談をお話しします。サイバークリーンセンターの名前を聞いたことがある人はいらっしゃいますか？ まずCCCがどんな活動をしていたかご説明します。当時Windowsに感染したボットがいろいろな悪さを始めていました。インターネットに接続したおとりパソコン、今で言うハニーポットを立てて待ち構えていると、無差別感染攻撃がいつかハニーポットに当たります。そこで分析を行い、攻撃者≒感染しているIPアドレスのリストをプロバイダーに渡して、「この人は感染しているから注意喚起してください」と警告するわけです。

プロバイダーがユーザーのIPアドレスとタイムスタンプから氏名を調べる行為は、通信の秘密を侵害しています。そこで国（総務省）に相談し「こういう仕事（正当業務）であれば大丈夫ですよ」と許可をいただきました。

このハニーポットでは、検体も取ります。その検体を駆除する駆除ツールも作りました。対策サイトに上げて、ユーザーには「あなたは感染しているので、このサイトにアクセスして駆除ツールをダウンロードして使ってください」と通知するわけです。

当時の家庭用インターネット環境は、今みたいにWi-Fiが飛び交って、家に端末が何台あるのか分からないというものではありませんでした。お茶の





間にお父さんが管理するパソコンが1台あるような場合が多かったです。なので、パソコンが感染してますよって注意喚起すると「あっ感染していた」というのが分かるんです。

命令する人や悪さをする人は国外にいるので、逮捕できません。では、C&Cサーバーを封鎖すればいいのではないかというと、それもまたいたちごっこなんです。でも、感染パソコンにはアプローチできるので、先ほどの検体を収集して感染者を特定して注意喚起する作業を愚直に繰り返し行いました。

CCCの活動は約5年やりましたが、最終年度の2010年7月末時点で、検体は1667万件収集しました。その内、ユニークな検体が138万検体でした。注意喚起は累計51万5000回になりました。駆除ツールのダウンロード回数も130万回になりました。当時はアンチウイルスベンダーに協力をいただきました。

2006年にスタートしたときのブロードバンドインターネット利用者はまだ2000万人でした。このプロジェクトが終わる2010年度は3170万人、まだパソコンが家に1台の時代です。ハニーポットに検体を送り込んでくる人のIPアドレスや検体の種類から推定すると、ボットに感染している人は日本の2.5%

ぐらい。これはかなり正確な数字です。ここを1%未満にしようという目標を立てて注意喚起を何回もやったわけですが、結果として0.6%まで下げることができました。

これは自画自賛ですが、当時のマイクロソフトがセキュリティレポートを出していまして、世界地図で各国のマルウェア感染状況を表示し、危ない国は赤色に塗っていました。取り組みのスタート時点で、日本は9番手だったんですが、この対策が終わる頃には世界ナンバーワンの安全な、グリーンな国に変わっていました。

残念なことに、この対策は万能ではありませんでした。インターネットにモデム直結で直接接続しているような家庭がどんどんなくなっていくと、効果が出ないのです。例えば、NATの配下に5台も6台もパソコンやスマホなどがつながっていると、プロバイダーから「おたくのパソコンは感染していますよ」と言われても「どれですか？」という話になって、こういった駆除ツールを使った注意喚起の取り組みは、あまり有効ではなくなってしまったのです。

話は飛びますが、当時の状況を今に置き換えて課題を考えますと、頭が痛いのはIoT機器です。「パッチを当ててくださいよ」でIoT機器にパッチを当てられる人は少ないでしょう。コマンドを打たないとパッチ適用もできないという機器もありますので、IoTのセキュリティ対策は、20年前のサイバークリーンセンター以上に対策が難しいと思います。

ネット界を騒がした歴代のマルウェア

■ CodeRedワーム

サイバークリーンセンターが立ち上がる2007年2月までの5、6年は、私のセキュリティ人生を決定づけるようなマルウェアがたくさん出てきました。

まず、2001年に「CodeRedワーム」が登場しました。当時はマルウェアの数もそんなに多くなかったですし、「これ」というものには名前が付いていました。

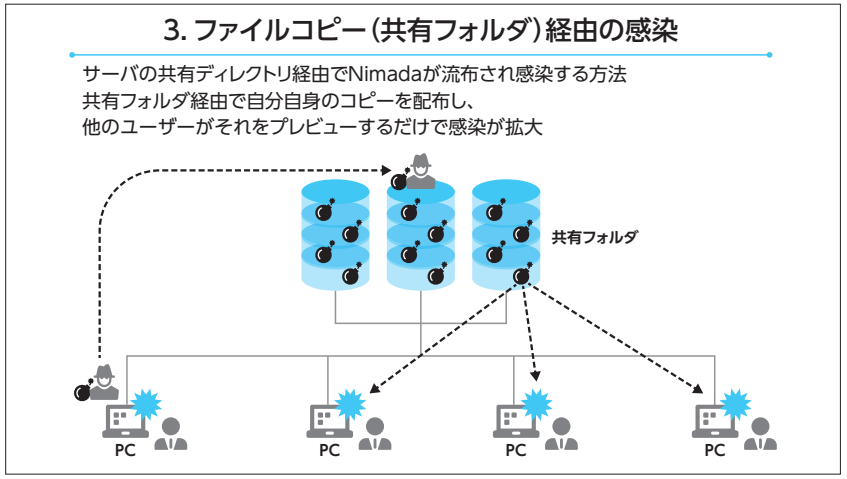
ワームは自己感染型の、直接インターネットに接続するホストのぜい弱性などを突いて、どんどん感染拡大するタイプのマルウェアです。Windowsサーバーが攻撃対象になっていました。海外の研究者が感染サーバーをマッピングしたところ、世界地図が真っ赤に染まってしまいました。

このCodeRedワームを収集して、いろいろ解析しました。すると、CodeRedワームは大変にふざけたマルウェアだということが分かってきました。まず、今だと常識なのですがバックドアを作る。そして、他のWindowsサーバーに感染するための大量の感染パケットを出します。力いっぱい通信をするんです。プロバイダーが悲鳴を上げるような通信でした。

CodeRedワームはホワイトハウスにもDDoS攻撃を仕掛けました。ホワイトハウスはこのCodeRedワームを解析して、対策としてホームページのIPアドレスを変えたんです。ホワイトハウスがそこまで解析するんだ、というのも驚きでした。

■ Nimda（ニムダ）

CodeRedワームの後、同じ年に登場したのが「Nimda（ニムダ）」。これは「admin」を逆からつづったものです。2001年は高度な機能を積んだマルウェアがいっぱい出てきて、その悪意を集大成するような形で登場したのが、このニムダです。私はチームで解析をしました。解析というのは、ハニーポットを立てて通信記録を取るんです。どことどういう通信をしているかを解析



していると、どんな悪さをしているか、大体推測がつきました。

例えば、感染するとニムダは自分の感染したIPアドレスの近場のIPアドレスをスキャンして、ぜい弱性があるとそこを突いて攻撃して……を繰り返していきます。データセンターといったサーバーが立っているところには同じようなバージョンのマシンがあるということも考えられますので、これは理にかなった攻撃方法だなと思いました。

さらに、ウェブ改ざんも行います。当時インターネットエクスプローラーというブラウザーがあったんですが、自動的にダウンロードが開始されてしまうというバグがありました。それが軒並み襲われていきました。このバグ、勝手にダウンロードは行われるものの、ポップアップウィンドウは出るんです。ポップアップウィンドウで「ああ、なんかおかしい」と気づかれないように、ニムダはウィンドウの開く場所をPC画面の外に指定していました。

こうやってパソコンに侵入すると、そこは企業のイントラネットの中であったりします。あの頃はまだぜい弱なプロトコルでファイル共有が行われていましたので、ニムダは共有フォルダーに自分のコピーをばらばらとばらまいて、同じようにアクセスした人が軒並み感染して……ということが行われました。ニムダの作者は、イントラネットでの感染拡大というものについて、実験していたのではないかなと思います。

さらにニムダは、感染したパソコンからIPアドレスを抽出してスパムメールを投げるということもします。今あるマルウェアのほぼ全ての機能を、2001年に見事に実装したのがニムダでした。

■ Antinny

「Winny」は映画にもなったのでご存じの方は多いと思います。2000年代前半に普及したファイル共有ソフトです。いまからお話しするのは2004年から05年、06年ぐらいまでにかけてのことです。当時、CD-ROMで映画のコンテンツや音楽が流通していましたが、それをパソコンにダウンロードして、ネットワーク上でリストアップして共有できるのがWinnyの特徴です。誰が持っているかは分からないけれども自分が欲しいなと思うコンテンツがあれば、それをクリックするとダウンロードできます。当時は、音楽や映画のふりをしたマルウェアを配った連中がいたのです。ダウンロードした人は気付かない。MP3だと思ってダウンロードしてクリックしたけど、違っていた。それで次のファイルをあさりにいくのですが、実はその時点でもう感染しています。多くの人は自宅のパソコンで会社の仕事を普通にしていた時代です。お役所の方などが土日に仕事を家に持ち帰って自宅のパソコンで作業をする。そこにWinnyが入っていて、そのWinnyに感染したAntinnyというものがパソコンの重要情報を全部Winny上に放り上げてしまう。機密情報が漏れた例もありますし、プライバシーに関わるような恥ずかしい情報が漏れてしまった人も出ました。

こういった被害を防止するために、Telecom-ISACが中心となりトレンドマイクロに駆除ツールを作ってもらい通信事業者経由で注意喚起をしたのですが、1000通のメールを出しても数十人ぐらいが反応するようなレベル感でした。Winnyのユーザーは自分が著作権法違反をしているのは分かってやっている方が多かったものですから、真面目に通信事業者の言うことを聞くなんていう状況ではなかったんです。知らないふりをしていたと思います。

次の作戦として、マイクロソフトに協力を仰ぎました。WinnyはWindows上のアプリケーションでした。実はWindowsアップデートは、OSのアップデートと同時に当時のマルウェアをごっそり取るような仕掛けが裏

で動いていたんです。そこにAntinnyの検体を登録してもらって、根こそぎ取ってもらうことをお願いしました。最初はマイクロソフトも相手にしてくれなかったのですが、粘り強い交渉の末、対応してくれることになりました。

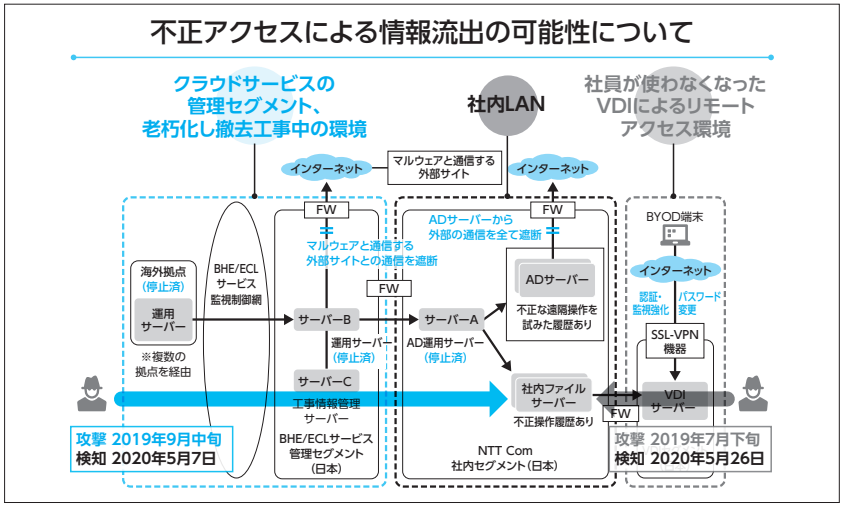
リムーバブルツールを動かすと、一気に4割の感染通信や攻撃通信が減るんです。すごいですね。ということは、逆に言うと、Winnyユーザーの4割ぐらいの人がWindowsアップデートをしていたということです。さらに言うと、6割の人には効果がないんです、Windowsアップデートをしていない。ずっと違法コンテンツの収集のみを行っているような人がいたんです。

これはなんとかせねばということで、内閣官房やNISC（内閣サイバーセキュリティセンター）、マイクロソフトなどいろいろなところにお願いして、NHKにも取材をしてもらって、一大キャンペーンをしました。私もNHKのニュースに出たりもしました。亡くなった安倍さんが官房長官のときに「大切なのはWinnyを使わないことです」と発表してもらったりもしました。

また、攻撃者からの通信を分析して、IPアドレスを特定して、使用者を調査し、その使用者ごとにトラッキングできる、個人情報にひも付かない形で個人を特定するIDを生成するシステムも作りました。このシステムを活用して「あなたには2回目の注意喚起です」というようにメールをしつこく送っていくと、どんどん対策が進んでいくということが分かりました。当事者に届くメッセージをしっかり出せば対策が進むんだな、ということが分かりました。

NTTコミュニケーションズも不正アクセス被害に

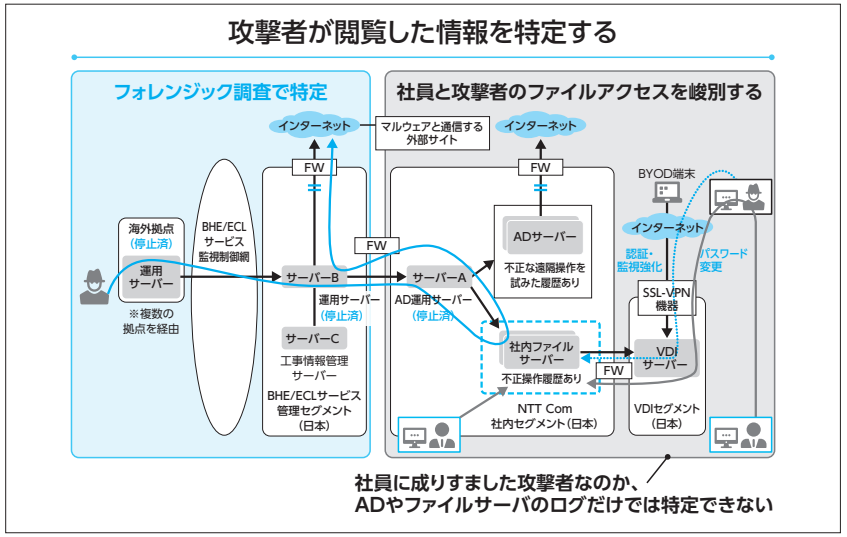
2020年にNTTコミュニケーションズは不正アクセスに遭いました。これは2回目にご報告した際の図なのですが、真ん中の枠の中が社内LANなんです。「ネットワークを分離しましょう」とおっしゃる方もいますが、ネットワークはどこかでつながっていまして、今回はクラウド環境を構築する、海外のデータセンターをつなぐ管理セグメント経由で、シンガポールの拠点からドンと不正アクセスを受けました。



もう一つは右側、社員が使わなくなった古いリモートアクセスの環境から侵入されました。調べてみると、気付いたのは2020年5月ですが、侵入されていたのはその前の年、侵入はしずしずとかなり時間をかけてやって来るということが分かりました。

5月8日の金曜日に私の電話が鳴りました。金曜日の電話連絡には良い思い出がないんですが、「もしかしたら侵入されたかもしれません」という連絡が来ました。夜中の12時過ぎにまた電話があって、「シンガポールから侵入されていました」と。その報告を受け私の頭の中は真っ白になるんですね。なぜかというと、セキュリティ屋はファイアウォールやプロキシなど自分が持っているログの分析はできるんですが、シンガポールから侵入された場合は、「それはグループ会社のネットワークですよね、誰に言うとログがもらえるんでしょうか」となります。自分が準備してきた対策ではインシデント対応ができないのです。社長に電話して「現在の情報セキュリティ部の能力を超えていますから、危機管理体制を立ち上げてください」とお願いしました。

社内の協力でログ分析を行うと、攻撃者は半年かけて日本の領域に入って



来ていました。ゆっくりゆっくり来るんです。そして真っ先にファイルサーバーのところに行って、特定のユーザーに成りすまして、情報を持ち出そうとするんです。

図の青い線で何が持ち出されたかを解明するためにフォレンジックが有効でした。攻撃者はサーバーにログインして、権限昇格してというセオリー通りの攻撃手法を採っていましたので、フォレンジックをすることで多くのことが分かりました。

ところが課題となったのは右側の青い線なんです。この線はVDIによる通信です。ということは、攻撃者は画面情報を持ち出しているのです。VDIの画面情報の録画は行っていませんでしたので、どのファイルにアクセスしたかを正確に見分けないと、例えば、攻撃者は社員のIDを悪用していますから、社員も見ているファイルサーバーの中で攻撃者を特定することをしないと、攻撃者が見ていないファイルも見たこととしてお客さんに説明することになってしまうんです。

NTTの持っている情報は、単なる回線の設置場所であったとしても、それは国家の重要な施設であったりすると機密情報に当たりかねません。「正確に攻撃者が閲覧した情報を特定しないとまずい」となりました。ここは本当に真剣にやりました。

どうやってやったかと言いますと、社員と攻撃者のファイルアクセスを峻別（しゅんべつ）するという作業です。

社員と同じIDを使った攻撃者に対しては、「これはなんでアメリカのIPアドレスなんだろう？　この人は東京からもアクセスしているよね」「あれ、社内からもアクセスしているよね」「入退館の記録を残しているよね」といろいろな情報を組み合わせて分析していきました。

社内のデータサイエンティストにお願いして、彼らにアクティブディレクトリの分厚い専門書を片手に、どのログがどのタイミングで出るかを解明してもらいながら、攻撃者の足取りを明らかにしていきました。

疑わしい通信は、AzureやGoogleのGCPなど正規のクラウドサイトとの通信でした。当社が正規のクラウドにアクセスしているなら分かるんですが、向こうから通信が来ているんです。つまり、攻撃者がお金をかけて攻撃基盤を作って、社員に成りすましているとしか思えない。

さまざまなものを組み合わせて、データサイエンティストが1.5カ月かけて「これで絶対間違いなく当たりです」というロジックを開発してくれました。それに基づいて閲覧されたファイルを特定して、お客さまにご説明して、場合によってはネットワークを作り替えるということもやらせていただきました。

■ 広報対策

不正アクセスを受け、2回報道発表をしました。皆さんにお伝えしたいのは「情報は漏れる」ことを前提に準備を進めるということです。2回とも木曜日の16時に報道発表しました。これは市場に変な影響を与えないなど、いろいろな考慮の結果です。

ツイッター（現X）を分析すると、われわれの不正アクセスに関するつぶやきが、われわれが報道発表を開始する前に出ていることが分かりました。それを知っているのはわれわれの社員とお客様しかいません。お客様に事前

に説明に行くと、取材能力にたけているメディアがすっぱ抜くぞ、ということを想定して、そういう想定問答集も作っておりました。案の定、後から分析すると自分たちの報道発表より早いぐらいのタイミングで報道がなされました。

1回目の報道発表は5月28日16時に掲載しました。その16分後にわれわれの報道発表よりかなり詳しい記事が出ました。2回目は、われわれが報道発表する16時のなんと5時間前にニュース記事が出ていました。われわれの公表より報道が早いことを想定して準備していましたので、その対応も落ち着いて行うことができました。

こういうことが不正アクセスの現場では起きてきますので、セキュリティ屋がセキュリティの仕事ができなくなってしまうんです。いろいろなところでいっぱい質問をされます。「これはどうなっている？」「どうなっているの？」と言われると、セキュリティ対応などできなくなってしまいます。

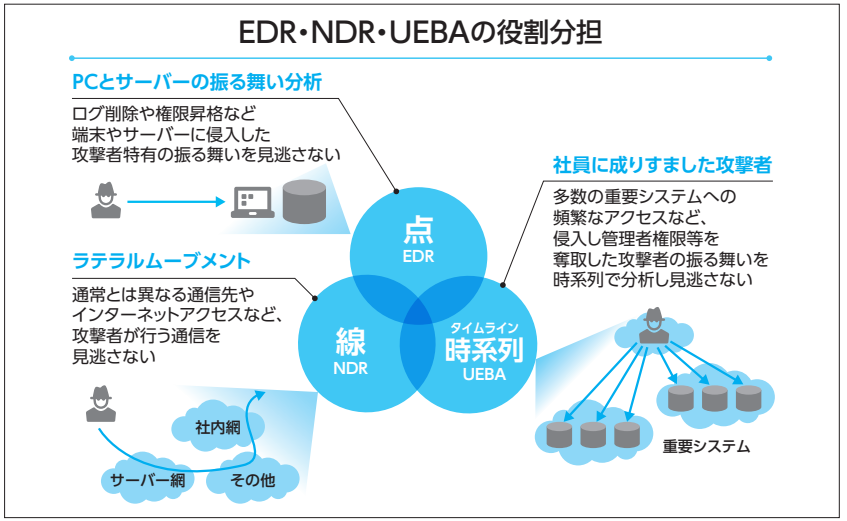
■ 再発防止策

再発防止策は、社内に侵入する糸口を与えない、これに尽きます。まず、アカウントをきちんと管理する。このときは使わなくなったVDIにアカウントが残っていました。さらに、多要素認証をきちんと使っていなかった。そこで、もともとの基本を徹底することをやりました。

ぜい弱性対策は全てやり切る。イントラネットの中であったとしてもぜい弱性対策をやる。ワンテンポ遅れてもぜい弱性対策をやらないと、攻撃者にとって安住の地を与えることになってしまう。スピード感を持って取り組もう、が第1番目。

2番目は、それでも入って来られる可能性があるので、社内であったとしても通信先を限定しようということです。これはなかなか難しいんです。LANの中でIPアドレス同士のフィルタリングをかけたりはできません。それでNDRといわれるような、通信経路を見て普段と違う通信が出るとスコア値を高くしてアラートを上げてくる、という仕組みを導入しようとしました。

大反省は、途中の踏み台サーバー。メンテナンスするためにログインするサーバーが何カ所も置いてあるんですが、そちらは古い環境ですとアカウント管理が徹底されていないだけではなくて、特権ID管理もおろそかになっていたり、それぞれの組織が勝手に立てて管理できていない、といったいろいろなことが分かってきた。そういう基本を徹底しようと。



そしてファイルサーバーを禁止しました。ファイルサーバーという便利なものを置くからこうなるんだということで、ファイルサーバーをやめてシェアポイントに切り替えて、重要情報に暗号をかけるようにしました。その代わりどこからでもファイルにアクセスできる環境を作ろう。つまり、ひっくり返すとインターネットにつながる環境をどんどん作っていったんです。その上でセキュリティをレベルアップしていこう、ということをやりました。

情報資産管理をしっかりやりつつ、セキュリティソリューションを導入していくんです。まずEDRは全て入るところを全部入れろと。NDRのようなフローを見る仕組みを導入して、UEBA、IDごとに「この人はIPアドレスはいつも日本の国内からなのに、なんでこれは海外なのか」ということでスコア値を上げるような、そういったIDの振る舞いをチェックしました。あるいは「システムアクセス権限のない人がシステムにアクセスしているよね、おかしいよね」ということもチェックしました。

点を守るEDRと、線を見ていくNDRと、時系列、タイムラグのUEBAを

組み合わせて導入しました。

その後、スタッフの負担を減らすために、サイバー攻撃への対処や復旧の自動化も進め、今ではマイクロソフト環境の自動化率は95%に達しました。

セキュリティの要は人財育成

セキュリティ対策に重要なのは、人材育成です。人材を獲得しようと思っても難しい。高い給料を提示しても、NTTでセキュリティをやりたいという人ばかりではないことは痛いほど分かりましたので、人材育成の会社を作りました。エヌ・エフ・ラボラトリーズという会社です。FFRIセキュリティの社長の鵜飼さんと私は友達だったので「相互に出資して会社を作ろうよ」と持ち掛け、NTTと共同出資で作らせてもらいました。どんな会社かと言いますと、NTTとFFRIのノウハウと、お客さまと一緒になってセキュリティ人材をお互いの知見で育成していこうという会社です。

会社の人材育成は、大学のような時間に制限がある育成方法ではなく、マルウェア解析など特定の分野を集中的に、1年間1000時間以上、1200時間ぐらい缶詰めにして徹底的に仕込みます。1人の講師当たり3人の育成対象者というぐらいの割合で、社員が社員育成をします。

会社を作って目指しているところをお話ししますと、今までのNTTの人材育成は、スキルは幅広く教えるので後は自分で頑張れ。もっと言うと、専門領域はベンダーに丸投げとは言いませんが、外部に委託してしまうというところがあったんです。そこで、エヌ・エフ・ラボラトリーズはそうではなくて、自分で特定分野の狭い領域でいいから一回深く掘って理解して、自分で手を動かして実現する人を育成してみようではないかと。本業と関係ない専門スキルを企業にいながら身に付けることは難しいと思いますので、それを実現する育成プログラムを作ってみよう、ということで、今だとソフトウェア開発やいろんな分野でこういったことができるようになっています。

勉強の仕方も座学中心ではなくてアクティブラーニング、最終的には人に教えるというところで自らのスキルを定着させていくところを目指しています。1000時間と言いましたが、新入社員を今年（2024年）実は30人ほど研修コースに送り込んでいまして、彼らは最初のBootUp研修では、入社してから3カ月間ぐらいのうちの1.5カ月ぐらいは手を動かす研修を行います。CSIRT業務や製品のぜい弱性など。C言語も教えます。もちろんPythonもやるんですが、侵入してパソコンのメモリをどうコントロールできるのかというところをプログラムで理解しようと思うと、やはりC言語が便利です。

卒業した人を、さらに高度な業務にアサインすることを繰り返しやって、5年たちました。

卒業生は、OSCEなどが取れるようになります。OSCE3という、2022年の時点で世界で60人しかいない資格を取る人が出てきました。本当に手を動かしながら考える環境を与えると人は成長するんだなということを、身をもって体験しております。

意外と離職率は高くないです。ただどういう人が離職していくかと言いますと、われわれの会社の中でその人のスキル、成長意欲を満足させるような高度な業務を与えられなくなったときに、彼らは自分のやりたい仕事を探して出て行くんですね。そこは仕方ないかなと思っています。

最後になります。マルウェアが使われなくなると、地道に侵入経路を探して攻撃を仕掛けてくる。どうやって守っていくのかというと、基本的なセキュリティ対策を徹底するしかないわけです。そういうことを行うためには、Quality of Security、ソフトウェアの品質の一つとしてのセキュリティをどう織り込んでいくか、というところは重要になってくると思います。これをやり遂げない限り、攻撃者のコストを上げることはできないと思います。

では、われわれはどうやってそれにアプローチしていくのかというと、Offensive Securityをやるしかないのかなと思います。要するに攻撃能力を高めるというよりも、攻撃者と同じぐらいのスキルを持って、今のセキュリティ対策で足りていないところを見つけられるようなOffensive Securityに人材育成の出口を求めていこうと考えています。

第4回

英国Cybersecurity Fellowship参加報告

―若者向けサイバーセキュリティ人材育成：英国と日本の比較―

登壇者
株式会社BLUE 代表取締役
千葉工業大学変革センター 研究員　**篠田 佳奈** 氏

国際連携による サイバーセキュリティ人材育成

今日は「英国Cybersecurity Fellowship参加報告」と題して、若者向けのサイバーセキュリティ人材育成について、英国と日本の違いを比較しながらお話したいと思います。

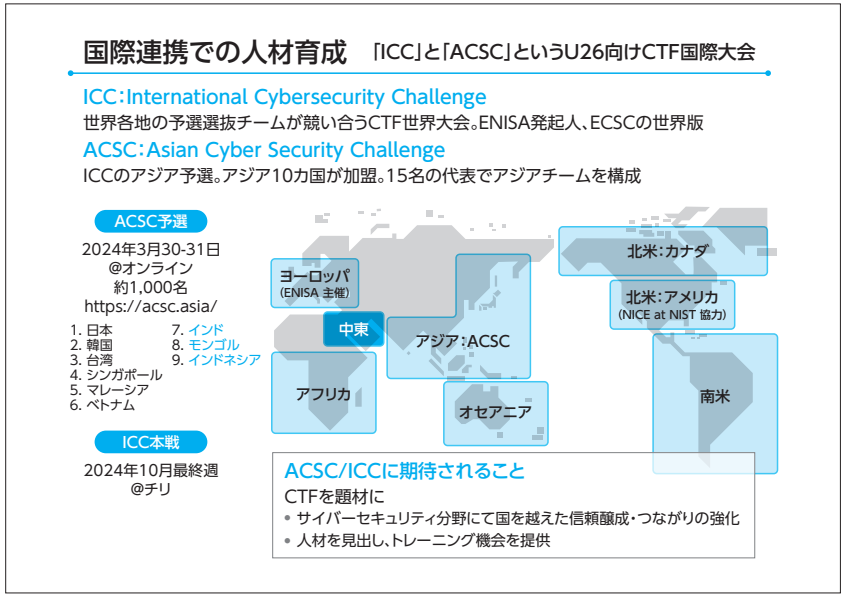
私は、日本発の情報セキュリティ国際会議「CODE BLUE」を運営しており、今年で12回目の開催を迎えます。「CODE BLUE」の特長は、もちろん最新の講演内容や各種コンテストなどもありますが、若い世代を積極的に巻き込んでいる点は海外から注目されるポイントのひとつになっています。また、多様性も大きな特長です。技術だけではなく、法制度やオープンソースツールなどさまざまな観点からの講演を提供し、議論を深めています。

さらに2年前から千葉工業大学の変革センターで研究員としても活動を始めました。オンライン詐欺の撲滅に取り組む国際機関「Anti-Phishing Working Group（APWG）」にも参加し、「一般社団法人セキュリティ・キャンプ協議会」では実行委員として国際連携ワーキンググループのリーダーを務めています。現在、2つのプロジェクトが進行中で、その1つはアジア9カ国が共同で若い世代に向けて1週間のトレーニングを合宿形式で提供する

「Global Cybersecurity Camp」。もう1つは、欧州ネットワーク・情報セキュリティ庁（ENISA）が発起人で世界の各地から集まったチームがCTFで競い合う国際大会「International Cybersecurity Challenge（ICC）」です。

先に挙げた「セキュリティ・キャンプ」が協力するGCCの内容は非常に多岐にわたり、受講生は大体50名程度で英語で進行します。日本人は英語でのコミュニケーションが苦手ですが、情報セキュリティ技術には傾向として自信があります。参加した多くの学生がコミュニティに継続的に関わり合いを持ちたいと思い、講師やチューター、スタッフとして戻ってきています。良い循環が生まれています。例えば、セキュリティ・キャンプのGCC活動は日本から参加した1期生2名が対応していますし、タイ、マレーシアの中心人物も現在はGCC卒業生です。ここで目指しているのは、CODE BLUEもそうですが、人の橋渡しです。彼らが企業や政府に入る前に交流を持ってほしいという思いがあります。

ICCは、25歳以下が対象の国際的なCTF大会で、地域ごとのチームが競い合います。この大会の目的は、国境を越えた信頼関係の構築ですが、さらに



狙いとしてケイパビリティの向上もあります。大会ではU26カテゴリのため25歳を超えると選手としては参加できませんが、その年齢を超えた参加者は、今度はコーチやチャレンジの作成担当として貢献します。アジア代表チームは、2022年度は第2位、2023年度は第3位という成績を収めましたが、いずれの年も攻防戦ではトップの成績を誇りました。

英国のCybersecurity Fellowshipに参加して

まず、Cybersecurity Fellowshipについて説明します。正式名称は「Chevening Indian and Japanese Fellows」で、もともとはインドやスリランカを対象にしたファンドが始まりました。サイエンスを学ぶ人々を対象にしたオックスフォード大学での10週間のプログラムがあり、サイバーセキュリティの分野が発展してきたのは、この10年ほどです。今年初めて日本人がこのプログラムに参加することになりました。

このプログラムは（今回はパイロット版として）英国政府が出資し、Cranfield大学が運営しています。Cranfield大学はDefence Academyと密接に連携し、軍関係者の教育もになっています。私たちもDefence Academyに通い、4月21日から5月23日の5週間にわたるコースに参加しました。元々は10週間のプログラムですが、日本からの参加者は後半の5週間に短縮され

ています。

プログラムの内容は、多岐にわたり、技術に寄っていません。例えば、初日の授業がデジタル・フォレンジックというので、私自身はハンズオン授業を期待していましたが、実際には全くマシンには触れませんでした。講師は技術に精通しているものの、私たちに対して「なぜそうしなければならないか」「なぜこういう作り・手法になっているか」といった根本的な部分にフォーカスし、民主主義のためには、捜査の公平性や透明性が重要であることを私たちに考えさせ、その答えを自ら引き出させるといったスタイルでした。これが英国らしいアプローチだと感じました。

また、GCHQの下でサイバーセキュリティを統括するNCSCの初代所長の講義がありました。彼は「技術が分からないままサイバーセキュリティの国家戦略を立てる怖さを理解しているか」と話し、さらに「サイバーセキュリティの盗難は盗まれるのではなくコピーされるのだ」と強調しました。つまり、物理的な盗難とは異なり、デジタルな世界では何も消失せず、ただ複製されるという指摘です。技術者にとっては当たり前ですが、非技術者の整理と法律・施策の上での整理、私にはない観点で、これもまた日本ではあまり聞かれない話でした。

次に、シュリヴェンハム防衛アカデミーでの体験です。担当の先生はウェールズ出身で、ウェールズ訛りが強く、英語の理解に苦労しましたが、授業を受けながら会社の業務も進行しており、朝6時から日本と会議、7時過ぎに通学、という日々でした。プログラムでは、多様な内容がありましたが、港湾沿いにある防衛施設の船の出航を妨害するシミュレーションゲームは面白かったです。与えられた環境の中、意思決定の機会が何度かあり、グループで相談し、伏せられたカードグループを選択し、与えられたアイテムの中から、次に取るべきアクションを決めるという内容です。

このシミュレーションはDefence Cyber Academyのプログラムの一部で、攻撃に焦点を当てたものです。攻撃者の立場で、港湾にある防衛施設に停泊している船を出航させないための方法を考えるという設定で、私はインドの軍人や警察関係者、サイバーセキュリティシステムを提供している業界の社長と一緒に議論しました。私たちのアクションプランでは三日間だけ時間がある前提で考え、公安の電力を遮断するというアイデアを採用しました。電力がなくても手動でロックは解除できますが、その間に時間を稼ぐという戦略です。

カリキュラムの内容は他にもたくさんあるのですが、担任の先生からは「皆さんはもうプロなので、カリキュラムの内容に力を入れる必要はあまりありません。それよりも人脈を築くことに注力してください」とアドバイスを受けました。その結果、外務省やオックスフォード大学、Cyber系のカンファレンスに訪問する機会を得ました。最後には、研究結果が冊子としてまとめられました。

幼少期から体系的に展開される サイバーセキュリティ教育プログラム

次に、英国のサイバーセキュリティ教育についてお話しします。英国では、いくつかの人材育成プログラムがありますが、その中でも特に注力しているのがCyber Firstです。このプログラムは、7歳から18歳＋まで一貫して提供されており、GCHQの下部組織であるNCSC（National Cyber Security Centre）が主導しています。

Cyber Firstでは、7歳から18歳＋までの一貫した学習パスが設けられてお

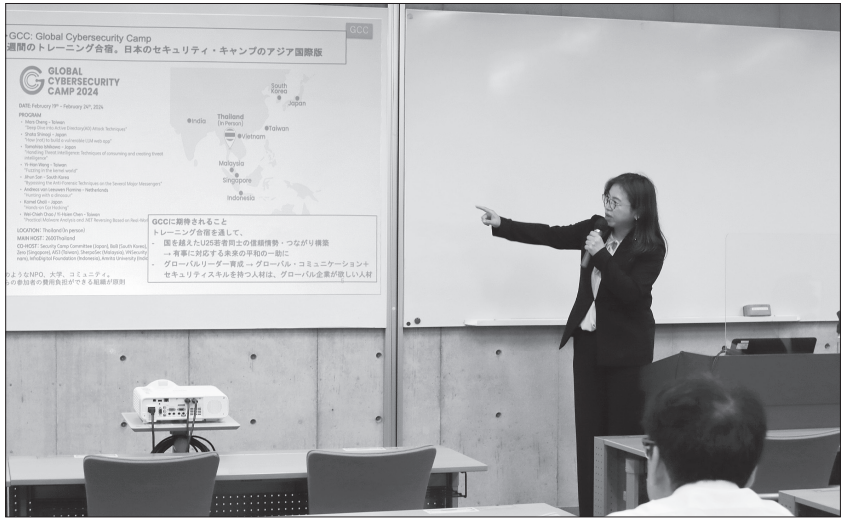
7歳～

- CyberFirst – Sprinters
- 7歳以上。
- オンラインでゲーム形式。言葉や文化に親しむ
- 学校の副教材
- 家庭向けのパズルやアクティビティも
- ゲーム>https://bit.ly/3RKlmSQ
- https://www.ncsc.gov.uk/training/ncsccyber-security-for-young-people-englishscorm-v2/index.html

り、例えば7歳から始まる『CYBER SPRINTERS』というプログラムでは、オンラインでゲーム形式を用いてサイバーセキュリティの用語や文化を楽しく学べるもので、学校の副教材としても活用されています。

11歳から14歳向けには、オンラインと対面型のプログラムが充実しています。オンラインでは「Navigators」と「Explorers」の2つのプログラムがあり、Navigatorsはビデオや音声、インタラクティブなコンテンツを通じて安全なインターネットの利用法について学ぶ内容です。Explorersでは、日常生活におけるサイバーセキュリティの役割や、関連するさまざまな職業についてゲームを通じて学びます。これらのゲームを修了すると証明書が発行され、学校の補助教材としても使用できます。

対面型のプログラムもあり、3つのコースからなる半日イベント「Trailblazers」、同じく半日イベントの「Adventurers」、1日イベントの「Investigators」などがあります。Trailblazersの中の「Go Create」コースでは、ウェブサイトのカスタマイズを通してウェブの基礎を学ぶことに重点を置いています。「Digital Detective」コースではOSINTを活用し、例えば病気の発生源を特定するシミュレーションを行います。「Creative Computing」コースは、メディアや広告業界におけるデザインやアート、テクノロジーの役割を探るプログラムです。



Cyber First Girls Competition

過去7年間毎年開催され、2023/2024年には英国全土から12,500人が参加し、750の学校と3,608チームが競技に参加した。

- 4名1チーム。
  1つの学校で何チームも参加可能
- クイズ形式。
  暗号、AI、ネットワークなど幅広い
- 優勝者にはノートPC。学校に賞金
- 予選>本戦なのか、
  オンラインで一斉開催>表彰式
  なのかは不明
- 遠い地域の女子学生同士の人脈を増やし、
  キャリアを支援するには非常に役に立っている様子

「Girls Competition」は、英国では非常に力を入れているプログラムで、これまでに7年間開催されています。国家サイバーセキュリティ戦略と共に始まり、それ以来受け継がれてきました。昨年と今年は1万2500人が参加し、4名1チームで構成され、1つの学校から複数のチームが参加可能な仕組みです。クイズ形式で暗号やAI、ネットワークなど幅広いテーマが扱われ、優勝者には新しいノートPCが授与されます。スコットランドでのヒアリングでは、スコットランドのコミュニティーが小規模であるため、英国全体の多くの女子中学生と交流でき、共に学び成長できる点が高く評価されていました。

次は、高校生向けのプログラムとして16 ～ 17歳を対象とした「Advanced on demand」があります。これは、コンピューターサイエンスを学んでいる学生を対象とし、デジタル・フォレンジック、暗号、OSINT、ペネトレーションテストなど、専門的なツールや技術の学習内容が提供されます。1週間か2週間程度の期間限定でラボを開放し、学生は自分のペースで学習を進められるようになっています。このプログラムを修了した学生はCapture the Flagコンテストに参加でき、全国の他の学生と競い合うことができます。また、コミュニティーに参加できるため、非常に人気があります。

「Bursary」は18歳以上を対象にしたプログラムで、奨学金を意味します。優秀な学生には、最大4年間のサポートと24,000ポンドまでの資金援助が提供され、有料のサイバーセキュリティ研修を受けることも可能となり、学生等のキャリアのスタートを支援します。

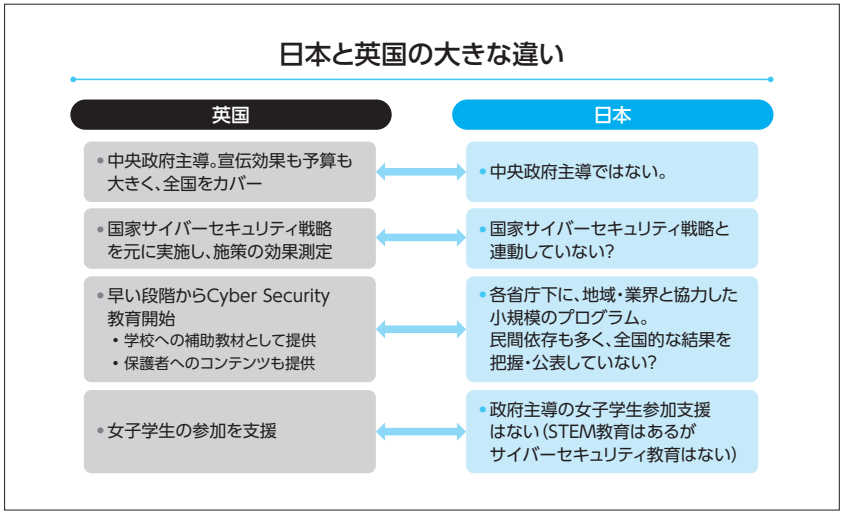
これらのプログラムの結果は、「Cyber First 年次報告書」として公開され、どのプログラムがどれだけの人ににリーチし、どのような結果をもたらしたかが定期的に報告されています。また、「Cyber Choice by CSA」という警察による教育コンテンツもあり、サイバーセキュリティスキルの合法的な使用と非合法的な使用の線引きをゲーム形式で学ぶこともできます。このプログラムでは、子どものデジタルスキルの需要の高さや、将来の高給の可能性、犯罪の誘惑に直面するリスクを保護者に強調することが狙いです。

これらのプログラムの特徴の一つは、他のCyber Firstプログラム同様に、必ず親向けのプログラムが用意されている点です。サイバーセキュリティ関連企業に就職することのメリットを保護者に伝える内容も含まれています。また、「NCSC-certified degree」という、大学や教育機関が提供するサイバーセキュリティ関連の学位の質を評価する制度もあり、学生や雇用主双方にとって有益な仕組みとなっています。

さらに、UK Cyber Councilは、サイバーセキュリティにおける役割や資格を定義し、他国のサイバーセキュリティ国家資格との互換性を考慮したキャリアフレームワークの開発も進めています。

英国との比較から見る 日本のサイバーセキュリティ教育の課題

一方で、日本の状況について見てみましょう。小中学生向けには、IPAが実施しているNPOによるインターネット安全教室や、経済産業省（METI）の提供する「セキュリーナ」の動画がまだ存在しています。しかし、中学生向けのプログラムは特に充実していません。現状では、「Security Camp junior」や「Mini Camp」、「Seck Hack 365」に少数の優秀な学生が参加しているのみです。



高校生向けには、高専で行われていた「K-SEC」がありましたが、これは2024年3月で政府支援は終了しています。大学生向けには「enPit」というプログラムが提供されていましたが、こちらも2023年3月で政府支援は終了しています。そのあとの展開は各組織が学んだ点を活かして頑張ってらっしゃるのだと思いますが、現在のところ不透明な状況です。

日本の学生にとって、サイバーセキュリティをどこで学べば良いのか迷う現状があるように感じます。このような状況の中、国家資格による人材育成が一つの手段として進められています。現在、日本には2つのサイバーセキュリティ国家資格があります。「情報セキュリティマネジメント資格」と「情報処理安全確保支援士」です。また、デジタルスキル標準に関連するDX人材育成プログラムもあり、その中でサイバーセキュリティに特化したのは「サイバーセキュリティマネジャー」と、「サイバーセキュリティエンジニア」の2つです。これにより、年末までに17万人の人材を育成する計画があります。しかし、17万人育成するという目標が他の施策と連動しているかは明確ではありません。これらの施策をできるだけ連携させて進めていくべきではないかと感じます。毎年合計45万人のデジタル人材を育成し、5年後には総数を230万人に達することを目標にしている施策もあり、より総合的な

アプローチが求められているでしょう。

日本の人材育成の仕組みは、文部科学省、経済産業省、総務省、そして各種NPOや業界団体がそれぞれ独立してバラバラに動いているように見えます。さらに、大学では政府が認定したコースもなく、若年層に向けた施策も少ないのが現状です。

日本と英国の大きな違いは、英国では中央政府が主導してサイバーセキュリティを進めている点です。英国では、宣伝効果も予算も十分に確保され、全国的にプログラムが展開されています。国家サイバーセキュリティ戦略に基づき、施策の効果測定が行われているため、戦略と施策がしっかり連動している印象です。また、英国では早い段階からサイバーセキュリティ教育が始まり、学校への補助教材として提供されているほか、保護者向けのコンテンツも充実しています。この点に関しては、日本も学ぶべき点が多いと思います。特に中学生向けの教育に重点を置くのは良いアプローチです。また、女子中学生のサポートが実を結んでいる点も注目に値します。

今後、英国に欠けているもの、日本に不足しているもの、それぞれをしっかりと考え、より良い未来を築いてゆく必要があると感じます。

第5回

インフォデミック時代における フェイクメディア克服の最前線

登壇者

国立情報学研究所
情報社会相関研究系 研究主幹・教授
シンセティックメディア国際研究センター長　**越前 功** 氏

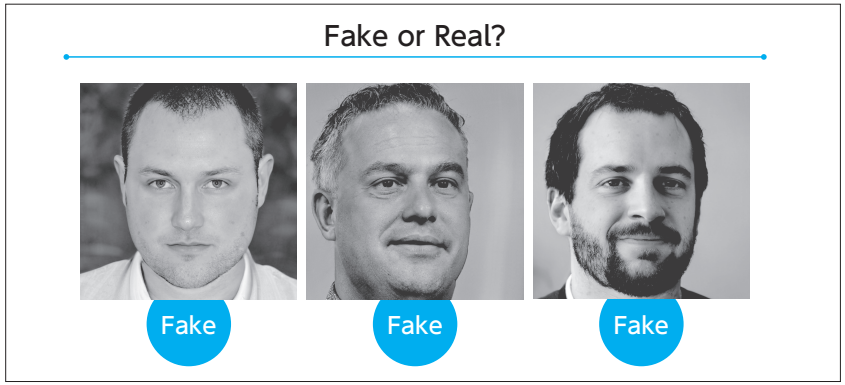
人間由来の情報を用いた フェイクメディアの生成

生成AI技術を使って人間には見分けが難しいフェイクメディア（偽の画像・映像・音声・文章など）が容易に作成できるようになり、大きな社会問題になっています。

まず、3人の顔画像をご覧いただきます（次ページ）。これらの顔画像はフェイクでしょうか、それともリアルでしょうか。間近で見ても分かりにくいのですが、実はいずれもフェイクです。顔に特化した最新の生成AI技術「StyleGAN3」を使い、瞳の虹彩、髪の生え際を見ても精緻に生成されています。もし、この画像がSNSに上がれば本当に実在する人物として惑わされてしまうかもしれない状況です。

こうした人間由来の情報を用いたフェイクメディアが生成されるようになった背景をお話しします。1つは、顔、音声、身体、自然言語などの人間由来の情報がサイバー空間に高度化されたデータセットとして出て来たことです。その結果、緻密で解像度の高い、高品質な人間由来の情報を容易に取得することができるようになりました。

もう1つは、生成AI技術の進歩です。高性能なGPUにより、AIの学習も低



コストに行えるようになり、生成AIを使って人間由来の情報を手軽に生成、加工、修正することができます。

海外でフェイクメディアの問題が言われ始めたのは2018年ごろです。顔の映像を別人に置き換えるディープフェイク（フェイク顔）をはじめ、フェイク音声で企業の幹部に成りすまして現金を窃取した事案や、SNS上で架空の人物に成りすまして株価操作を目論むといった事案も2019年に発生しています。

また、2022年には拡散モデルを使ったプロンプトと呼ばれる命令文で任意の画像を作り、偽情報が拡散した事案や、ChatGPTを用いたマルウェアやフィッシングメールの作成といった事案も報告されています。

プラットフォーマーが学術研究用途で公開した生成AIの学習モデルをチューニングしてネガティブな用途に使うといった、倫理的にも問題のある「野良AI」がたくさん出ているのが実情です。

プロンプトから著名人や政治家の顔画像を生成

次に、顔を対象としたフェイクメディアの生成についてお話しします。

以下の5つのタイプがあります。

(1) 顔全体の合成。ノイズ（潜在変数）から実世界に存在しない顔画像を生成する。先ほどご覧いただいたフェイク顔画像で使われている画像生成モデルのStyleGANや、プロンプトから画像を生成する拡散モデルのStable Diffusionなどがあります。

(2) 顔の属性操作。いわゆるスタイル変換と呼ばれ、ターゲットの顔画像の髪の色、肌の色、表情などを変更した顔画像を生成するものです。

上記の(1)の拡散モデルに関して、Stable Diffusionはプロンプトから写実的な画像を生成できますが、特定の人物やキャラクターを含む画像を生成することは困難でした。しかしながら、2023年初頭に、事前学習済みモデルを低コストでファインチューニング可能なLoRAという手法をStable Diffusionに適用することで、特定の人物やキャラクターに特化した画像生成が盛んに行われるようになりました。

例えば、ウクライナのゼレンスキー大統領の数十枚の顔画像を用いてLoRAでStable Diffusionをファインチューニングすることにより、ゼレンスキー大統領の顔画像を生成するモデルができてしまうのです。他にも、日本の著名人や政治家などの顔画像の生成も確認されるなど、大きな問題となっています。

今後、拡散モデルは、画像生成モデルだけではなく、映像や音声を生成するモデルとしても広がっていくのではないかと見ています。画像よりも写実性のある映像のほうがSNSでの注目度が高く、さらに音声が付くとなると極めてリスクが高くなると危惧しています。

従来のディープフェイクは素材となる画像を探して顔の部分を置き換えるといった作り込みが必要でした。ところが、拡散モデルは、プロンプトから画像や音声付きの映像が簡単に作れることから、誰もが「攻撃者」になる可能性があり、個人的に懸念しているところです。

(3) 顔映像・画像の表情操作。表情転写とも呼ばれます。攻撃者の表情とターゲットの顔映像を合成し、攻撃者の表情と同期したターゲットの顔映像を生成するFace2Faceと呼ばれる手法や、顔映像ではなく1枚の顔画像からターゲットの顔映像を生成するNeural Talking Heads Modelなどが知られています。

例えばインターネット銀行の口座を開設する際、オンラインで本人確認を

行うeKYC（electronic Know Your Customer）を利用する機会が増えています。これは、口座開設者がスマートフォンで撮影した本人の免許証などと共に、カメラで本人の顔映像・画像を提示して本人確認を行うものです。ただ、表情操作・表情転写技術を悪用して本人確認時に成りすますといった脅威が今後、深刻化するのではないかと危惧しています。

（4）顔映像の話し方操作。リップシンクとも呼ばれ、音声またはテキスト情報とターゲットの画像・映像を合成することで、当該の音声・テキストを発声するターゲットの顔映像を生成するものです。

（5）顔の入れ替え。Face swapとも呼ばれます。ソースとなる映像の顔の部分をターゲットの顔と入れ替えるなど、以前からある伝統的な手法と言えます。

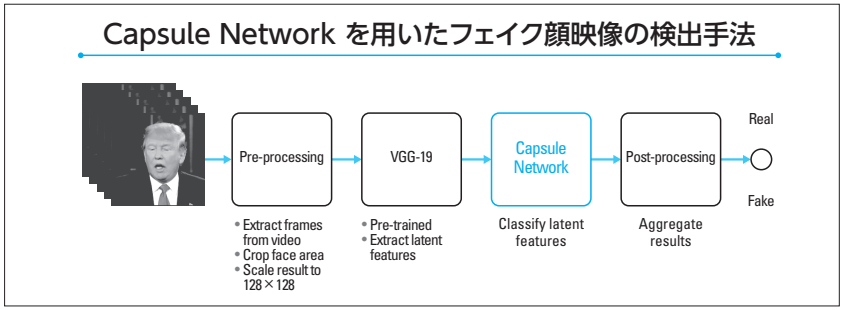
顔を対象としたフェイクメディアの生成について5つのタイプを紹介しましたが、中でもプロンプトから顔画像を生成する拡散モデルのチューニングが最も脅威であると感じています。顔画像の素材を用意する必要がなく、攻撃者にとって敷居が低いからです。ターゲットとなる著名人や政治家などの顔画像を学習させたモデルを使い、チューニングする。技術的には公序良俗に反するようなデジタルコンテンツを作れる可能性もあるのです。

フェイク顔映像を検出する深層学習モデルの研究開始

こうした問題に対応するための取り組みの1つとなるのが、顔を対象としたフェイクメディアの検出方法です。リアルとフェイクの顔画像を見分ける技術の研究についてお話しします。

2018年にディープフェイクによる脅威が知られるようになりましたが、私たちの研究グループは、2018年12月にMesoNetと呼ばれるフェイク顔映像を検出する深層学習モデルを世界で初めて考案し、マルチメディアフォレンジック分野の著名な国際会議WIFS2018に発表しました。この論文は、Deepfake detection分野の最初の論文と認識されており、被引用回数は1600回を超えています。当時はフェイク顔画像の学習データが少なく、動画サイトなどからフェイク顔画像を集めて学習させたことを覚えています。MesoNetは、4層のCNN（Convolutional Neural Network：畳み込みニューラルネットワーク）によるコンパクトな深層学習モデルですが、顔映像の目や口の周りを見て、生成AIで作られたフェイクなのか、あるいはリアルなものなのかを識別するモデルを世界で初めて作ったのです。

その後、CNNの深層学習モデルを改良し、Capsule Networkのアーキテクチャを用いたフェイク顔映像の検出手法を考案し、信号処理分野で著名な国際会議ICASSP2019で発表しました。Face2FaceやFace swapによる顔映像の真贋（がん）判定も可能で、国際会議ICASSPで発表された直近5年の研究論文の被引用数でも上位になるなど、大きなインパクトがありました。



さらに、リアルとフェイクの真贋判定だけでは実務的には不十分ではないかという議論が今後出てくると予想し、真贋判定に加えて、改ざんされた領域を推定することが重要ではないかと考えまして、2019年に世界で初めて発表したのが、マルチタスクラーニングによる「フェイク顔映像の判別と改ざん領域の推定を同時に行う手法」です。

当時、さまざまな手法が発表される中、フェイク顔映像の生成手法によって変更される領域が異なることに着目。修正された領域を見て、どの手法で生成されたのかを推測するというものです。例えば、「Face swapのスムージングマスクを使って顔映像が改ざんされている」といったように推測することが可能です。

インフォデミックの克服に向けた共同研究を推進

今、私たちが研究を進めているCREST FakeMediaやSYNTHETIQ VISION、社会実装についてお話しします。

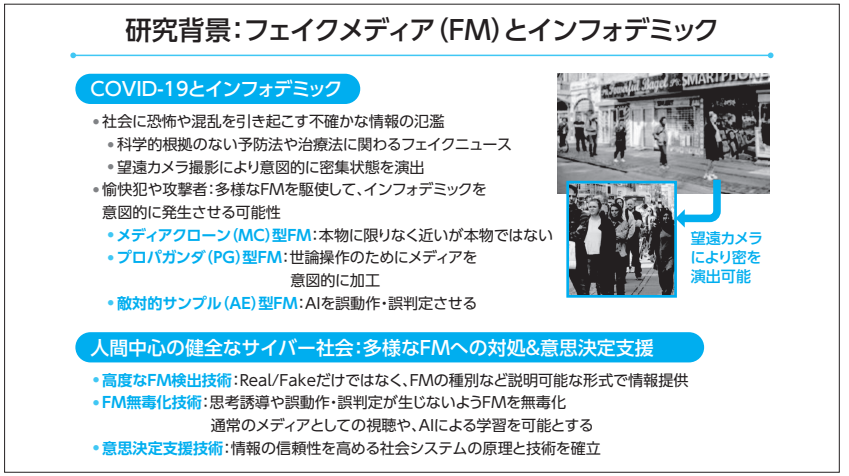
フェイクメディアの研究の重要性が認知されてきたのが2020年ごろです。国立研究開発法人 科学技術振興機構（JST）の戦略的創造研究推進事業CRESTにおいて、情報の改ざんなどフェイクの問題が取り上げられるようになりました。

そして、申請を経て、「インフォデミックを克服するソーシャル情報基盤技術」の研究が立ち上がりました。研究期間は2020年12月から2026年3月までです。

主たる共同研究者は、馬場口登氏（大阪大学データビリティフロンティア機構特任教授）、笹原和俊氏（東京工業大学環境・社会理工学院教授）です。

研究背景を記した申請当時の資料（フェイクメディアとインフォデミック）を紹介しましょう。

2020年当初は新型コロナウイルスCOVID-19が世界中で猛威を振るい始めた頃です。インフォデミックとは「社会に恐怖や混乱を引き起こす不確かな情報の氾濫」を指します。



当時を思い返すと、科学的に根拠のない予防法や治療法に関わるフェイクニュースが飛び交っていました。WHO（世界保健機関）がデマに惑わされないように注意を喚起しても、「高速モバイル通信の5GはCOVIDに悪い影響を与える」といったフェイクなど、さまざまな偽情報が拡散されていました。

他にも、望遠カメラの撮影により、意図的に密集を演出するものもありました。上図の画像は実際のものですが、本当はソーシャルディスタンスを守っています。それを特定の方向からズームで撮影すると密に見えるのです。意図的な演出が入ることで、人々の気持ちをファクトと異なる方向へ誘導するようなこともあるのではないか。それも広義の意味ではフェイクメディアに含まれると考えます。

メディアクローン型など3種類のフェイクメディア

2020年前半ごろは今のような生成AIのことはあまり聞かれませんでした。愉快犯や攻撃者は多様なフェイクメディアを駆使して、インフォデミックを意図的に発生させる可能性があると指摘しました。

想定されるフェイクメディアのパターンとして、以下の3種類に分類しま

した。

(1) 本物に限りなく近いが本物ではない「メディアクローン型フェイクメディア」(ディープフェイクや大規模言語モデルなどで生成されたメディア)
(2) 世論操作などを目的として素材となるメディアを意図的に編集、生成した「プロパガンダ型フェイクメディア」
(3) 人間には識別が困難だが、AIを誤動作・誤判定させることを目的に生成した「敵対的サンプル型フェイクメディア」

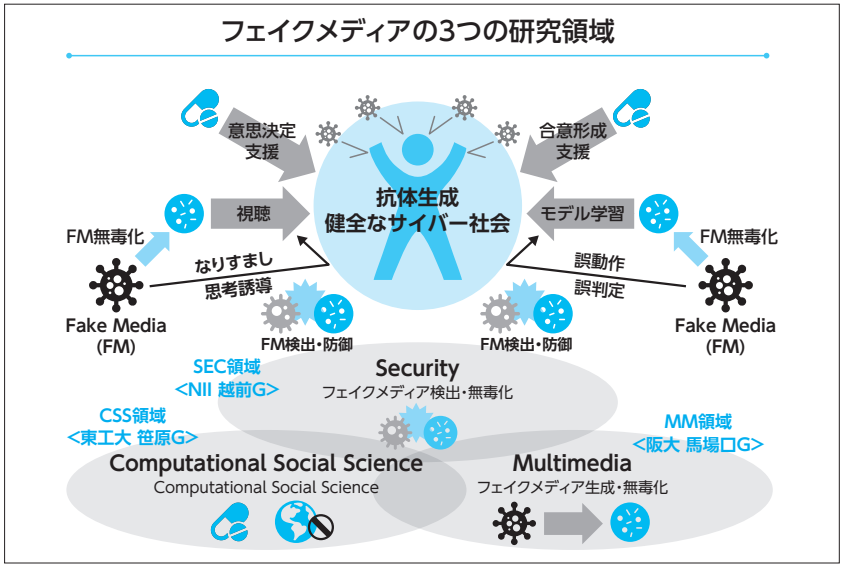
メディアクローンという言葉は、生成AIを使った本物のような偽物にどう対抗していくかを意味します。当時はディープフェイクという言葉が存在せず、私たちはメディアクローンと定義していました。

また、前述の望遠カメラで密を演出した画像のように、世論操作のためにメディアを意図的に加工するものも、リアル／フェイクを問わずフェイクメディアであるとしました。そして、今ではよく知られるようになった、AIをだます敵対的サンプルについても、フェイクメディアになると考えました。

私たち研究チームの目標は、人間中心の健全なサイバー社会を維持することです。そのために多様なフェイクメディアへの対処と意思決定を支援するものです。具体的には、リアルかフェイクかだけでなく、フェイクメディアの種別など説明可能な形式で情報を提供する「高度なフェイクメディア検出技術」、思考の誘導や誤動作・誤判定が生じないようにフェイクメディアを無毒化する「フェイクメディア無毒化技術」、情報の信頼性を高める社会システムの原理と技術を確立する「意思決定支援技術」を提案し、研究に取り組んでいます。

多様な意思決定を支援する情報技術基盤を確立

無毒化とは、フェイクメディアの「毒」を排除することです。例えば敵対的サンプル。AIがモデル学習する、識別する前に毒となる敵対的ノイズをそぎ落とすことも無毒化の1つです。また、顔が別人に置き換えられたフェイク画像・映像からオリジナルの顔を復元することも無毒化に含まれます。申請当時は、実際に無毒化を実現できるかどうか分からないところもありましたが、後でお話しするように、画期的な無毒化技術を提案することができました。



私たちの研究の目的は、フェイクメディアがもたらす潜在的な脅威に適切に対処すると同時に、多様なコミュニケーションと意思決定を支援するソーシャル情報基盤技術を確立することです。その研究を支えるのが、フェイクメディアを検出・無毒化する「Security」領域、フェイクメディアを生成・無毒化する「Multimedia」領域、思考誘導の排除、偽情報拡散を抑制する「Computational Social Science」の3つの領域です。

前述の3種類のフェイクメディアのパターンを想定し、4つの研究実施項目に取り組みました。

(1) 映像(顔、身体など)、音声、文書などの多様なモダリティに対するフェ

イクメディア生成技術を確立する「多様なモダリティによる高度なフェイクメディア生成技術」（主担当: Multimedia領域 馬場口氏）

(2) 前項目の1で生成した多様なフェイクメディアを対象とした高度な検出・防御技術を確立する「フェイクメディア検出・防御技術」（主担当: Security領域 越前）

(3) 思考誘導、誤動作・誤判定が生じないようにフェイクメディアを無毒化し、通常のメディアとして活用できる技術を確立する「フェイクメディア無毒化技術」（主担当: Multimedia領域、Security領域）

(4) 項目1 ～ 3の要素技術を最大限に生かし、情報の信頼性を高める社会システムの原理と技術を確立する「インフォデミックを緩和し、多様な意思決定を支援する情報技術」（主担当: Computational Social Science領域　笹原氏）

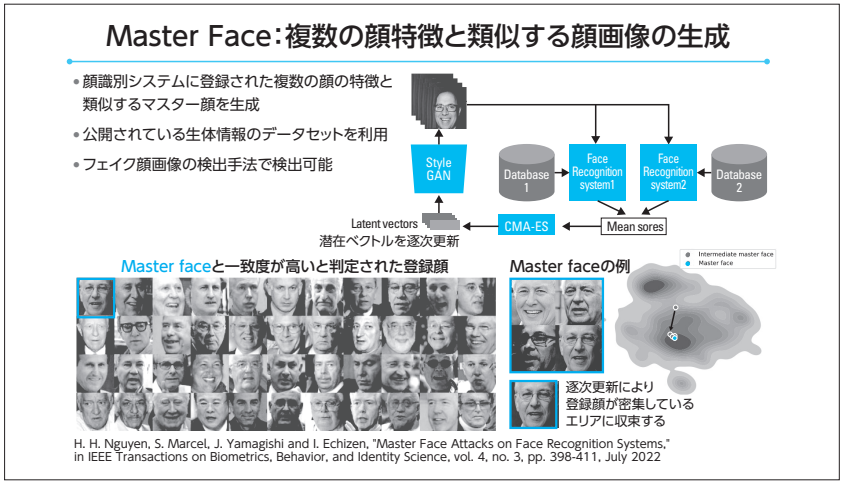
研究期間の中間点を越え、査読付きジャーナル論文やメディア掲載など、さまざまな形で私たちの研究が取り上げられています。研究のアピールだけでなく、社会に生成AIの問題を啓発する意味もあり、メディアの取材も積極的にお受けしたり、総務省の令和5年版情報通信白書に研究開発の取り組みが紹介されたりしています。

データベースの顔情報から マスター顔画像を生成

CREST FakeMediaの研究成果について紹介します。

Master Faceは、複数の顔の特徴と類似する顔画像を生成する攻撃手法の一つです。顔識別システムに登録された複数の顔の特徴と類似するマスター顔を生成します。マスター顔の生成は、公開されている生体情報のデータセットを利用します。一方で、私たちが過去に提案したフェイク顔映像の検出手法で検出することが可能です。

マスター顔の名称の由来は、ホテルのマスターキーを想像していただくと分かりやすいと思います。ホテルのマスターキーを使えば、どの部屋の鍵でも開けることができます。冒頭でStyleGANを使ったフェイク顔画像を紹介しましたが、潜在変数の与え方をちょっと変えるだけで複数の顔の特長と類似する顔画像を作ることができます。

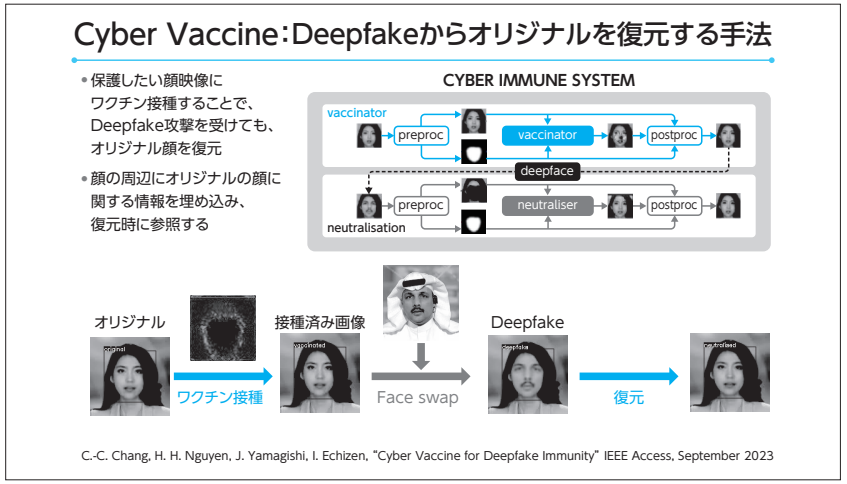


このStyleGANで作った顔画像に対して、顔識別システムで検証します。大規模な顔のデータベースです。上図で例示したように、Master Faceと一致度が高いと判定された登録顔がたくさんあることが分かります。

以前はターゲットの人の顔画像を入手し、偽造して成りすますといった手口が多かったのですが、今は違います。生体情報のデータベースから顔や静脈の情報を入手することができます。そして、入手した顔の情報から、顔特有の癖を見つけ、複数の顔と一致しやすい人工的な顔を作ることが可能です。つまり、ターゲットの顔画像を入手することなく、公開されたデータベースの顔情報からマスターキーを作ることができるのです。

フェイクからオリジナル顔映像を 復元可能なサイバーワクチン

フェイク顔映像に対抗する防御の話をします。ディープフェイクからオリジナルを復元する手法として「サイバーワクチン」があります。これは、保



護したい顔映像にワクチンを接種することで、ディープフェイク攻撃を受けてもオリジナル顔を復元することができるというものです。顔の周辺にオリジナルの顔に関する情報をあらかじめ埋め込み、復元時にその情報を参照してオリジナルの顔に戻す仕組みです。

サイバーワクチンを接種している場合と、接種していない場合の復元画像を比較したデータがあります。200枚の顔画像における類似度の平均値は、ワクチン接種が0.99に対して、非接種が0.57となっており、ワクチンを接種した方が高い精度でオリジナルを復元できることが分かりました。このフェイク動画の復元技術を2023年夏に発表した際、大きなインパクトがあり、マスコミでも取り上げられました。

前述のサイバーワクチンは接種後、オリジナルを復元することで効果を発揮します。次に紹介するサイバーワクチンは接種後、即効果を発揮するというものです。AIをだます敵対的サンプルに対して、プライバシー保護のためにこのサイバーワクチンを使います。

私たちがSNSなどサイバー空間で顔画像を公開する場合、顔画像がさまざまな学習モデルで使われることがあります。法的には問題がないものの、自分の顔画像が勝手に使われるのは嫌だという場合、このサイバーワクチンを打っておくのです。

具体的には、パーソンセグメンテーションと呼ばれる手法を対象として、人物の切り出しをできなくするノイズを人物画像の衣服などの部分に埋め込むことで、パーソンセグメンテーションによる人物の切り出しを防御できます。つまり、サイバー空間でAIから見えないようにするためのワクチンです。

人物の顔画像だけでなく、画像に映ったランドマークなどから自分の家などの位置情報を推測されたくないこともあります。その場合、ワクチンを打ってランドマークの画像解析を不能にするといった使い方も可能です。このワクチンは即効性に加え、圧縮画像に対しても効果があります。

フェイクメディア検出に資する大規模なデータセットを構築

私たちの研究チームで取り組んでいるのが、フェイクメディア検出の向上を目指した高品質な大規模データセットの構築です。従来のデータセットは実世界のフェイクモデルから乖離（かいり）しており、例えば被写体も1名というものが少なくありません。画像内の複数オブジェクトを同時に検出するモデルが近年、提案されており、フェイクメディア検出においても同時検出に対応するモデルが提案される可能性があります。そして、複数の人が映っている自然な画像のフェイクメディア検出のデータセットが求められていました。

また、従来のディープフェイク検出は1つひとつの顔画像を検出していましたが、一気にセグメンテーションして同時にフェイクメディアを検出することに加え、改ざん領域を推定するセグメンテーションにも対応するデータセットを構築しました。データセットは公開され、多数の人にダウンロードされています。

この他、eKYC（オンライン本人確認）におけるディープフェイク攻撃を想定したフェイク顔映像の大規模データセットにも取り組んでいます。成りすまし攻撃を受けても、高い精度で真贋判定が行えるというものです。

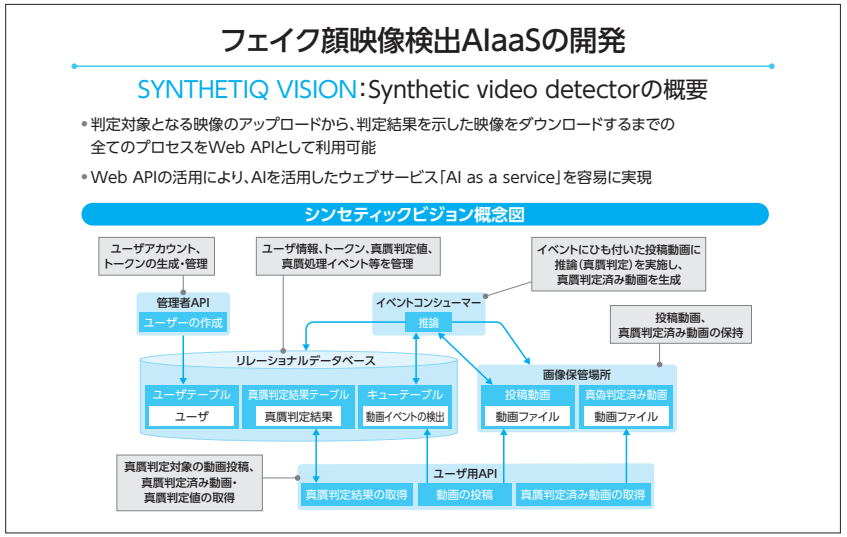
フェイク顔映像を自動判定する「SYNTHETIQ VISION」を開発

次にインフォデミック克服に向けた社会実装について概観します。

2021年ごろから日本でも生成AIの脅威が深刻化してきました。詐欺・詐称、思考誘導、世論操作、特定個人に対する名誉毀損（きそん）やいじめといった事案がマスコミでも報道されています。

こうした状況の中で、社会実装として推進したのが、「フェイク顔映像検出AIaaS」の開発です。具体的には、AIで生成されたフェイク顔映像を自動判定するプログラム「SYNTHETIQ VISION」を開発。このプログラムは、判定対象となる映像をサーバーにアップロードし、その判定結果を示した映像をダウンロードするまでの全てのプロセスをWeb APIとして利用可能なことが大きな特徴です。このWeb APIの活用により、AIを活用したWebサービス「AI as a Service」を容易に実現します。

これまで一般企業がフェイク顔映像の判定を行うには、高度なディープラーニング技術を利用する必要があるなど、高いハードルがありました。しかし、私たちがWeb APIを整備することにより、判定対象となる映像をアップロードし、判定結果を示した映像をダウンロードするだけの手軽なものになりました。



海外でもAPIを介して類似するサービスを提供するベンチャー企業がありますが、大きな違いは、私たちはソースコードを渡して組織内に閉じたシステムを構築する仕組みにしていることです。

その理由は、私たちの所属機関である国立情報学研究所がAPIを介して民間企業のようなサービスを提供することができないからです。また、センシティブな画像や、犯罪に使われるかもしれない画像を組織外や特に海外のサーバーに上げるのはどうかという問題もあります。

そこで、SYNTHETIQ VISIONに関心のある企業に対して、クラウド環境などを整備いただいた上で、ソースコードをお渡しして、企業内にシステムを構築するといった仕組みにしています。

SYNTHETIQ VISIONはさまざまな企業の関心を集めています。例えば、サイバーエージェントでは、タレントやアーティストなどの著名人の分身となるデジタルツインをキャスティングするサービスを展開しています。その「デジタルツインレーベル」に登録した著名人のディープフェイク映像を検知するために、有償のソフトウェアライセンスを導入しています。

想定されるユースケースとして、エンターテインメント業界が真贋判定によるフェイクメディアの削除や、報道機関が報道前の真贋判定による誤報道の防止、金融機関がリモートでの本人確認時に真贋判定による成りすましの検知に役立てるなど、システムを自社内で構築できることから、さまざまな分野でSYNTHETIQ VISIONの利用が広がると期待されています。

自動ファクトチェックや透明性の確保が今後の課題

今後の課題の1つが、AIを活用したコンテンツモデレーション、すなわちAIを用いた自動検知や自動ファクトチェックの必要性です。例えば、ファクトチェックを人間の手作業で行っている組織もありますが、自動化のニー

ズは高く、効果、効率性の観点からも必須の技術となり得ると考えています。

また、透明性やアカウンタビリティの確保が重要ですが、課題もあります。前述のSYNTHETIQ VISIONにしても、AIの学習データやベンチマークを全て公開すると、それを逆手に取って自動検知を迂回するような偽・誤情報の生成手法が出現する可能性もあるのです。

極めて難しい問題ですが、細かなアルゴリズムを公開するのではなく、どれだけ真贋判定の検知を行ったのかといった実績を積み重ね、透明性を図っていくことに落としどころがあるのではないかと考えています。

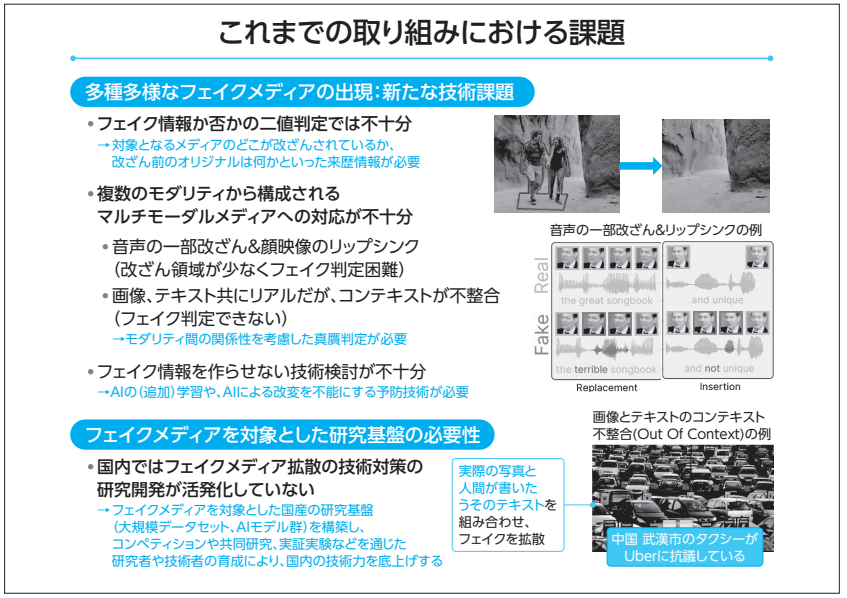
もう1つの課題は、多種多様な偽情報の生成手法が出現してきたときに、対応していかなければならないことです。そのためには、定期的なデータセットの更新や自動検知モデルの追加学習が必要になります。既知の手法で生成された偽情報の検知精度を確保しながらの追加学習はコストが大きくなります。また、多種多様な生成手法を安定的に自動検知できるかどうかといった問題もあります。

例えば、SYNTHETIQ VISIONの追加学習をいかに効率的に行うかも課題です。公表はできませんが、ある程度の方策は見つかっており、今後のバージョンアップなどで対応できると考えています。

AIで作られたことを示す情報をコンテンツに埋め込む電子透かしの活用が期待されます。ただし、電子透かし技術は顔を置き換えるといったAI操作に対しての耐性が問題となり、同時に電子透かし埋め込みによるコンテンツの品質劣化防止をいかに高めていくかが課題となります。

また、自動検知モデル、データセット、ベンチマークにおける課題もあります。研究レベルではデータを使ってさまざまなものが提案されていますが、現実の社会環境を反映していないものも見受けられます。産学でデータを共有しながら開発・実証を進めるなど、産学連携が重要です。プラットフォーム事業者やAI関連事業者から研究者へのデータ提供も期待されます。

自動ファクトチェックの課題もあります。信頼できる情報と照らし合わせ、正しいか否かを自動判定するものですが、難しいのは、信頼できる情報源をいかに維持するかです。信頼できる情報源は何なのか、それをどのように収集し、メンテナンスしていくのかが課題となります。



多種多様なフェイクメディアの出現により、新たな技術課題があります。フェイク情報か否かの二値判定では不十分ということです。そこで、対象となるメディアのどこが改ざんされているか、改ざん前のオリジナルは何かといった来歴情報が重要になります。

画像や映像、音声といった複数のモダリティから構成されるマルチモーダルメディアへの対応も不十分と言わざるを得ません。音声の一部の改ざんや顔映像のリップシンクの場合、改ざん領域が少なく、フェイクの判定が困難です。また、画像、テキスト共にリアルでも、コンテキストが不整合といった場合にもフェイクの判定が難しく、モダリティ間の関係性を考慮した真贋判定が必要です。

そして、フェイクメディアを対象とした国産の研究基盤（大規模データセット、AIモデル群など）を構築し、コンペティションや共同研究、実証実験などを通じた研究者や技術者を育成することにより、国内の技術力を底上げすることも喫緊の課題と言えます。

第6回

事業継続を脅かす サイバーリスクの実態と対策

登壇者

八雲法律事務所
弁護士/カリフォルニア州弁護士
情報処理安全確保支援士

山岡 裕明 氏

サイバーリスクの過小評価が会社に大きな被害を及ぼす

私は、インシデントレスポンスというサイバー攻撃を受けた企業の支援を専門としています。本日はサイバーリスクの最前線、事業継続を脅かすサイバーリスクの実態と対策についてお話しします。

ここ数年、サイバーリスクのゲームチェンジが起きています。何がゲームチェンジを引き起こしたのか。それは身代金要求型ウイルス「ランサムウェア」です。

経営者の方々とお会いして「御社のサイバーリスクは何だと思いますか」と尋ねると、皆さん「個人情報漏えいですかね」と口をそろえます。では、「個人情報漏えいで御社は倒産しますか」と聞くと、「いえ、倒産はしないですね」と答えます。

ところが、ランサムウェアは個人情報漏えいにとどまらず、事業継続を脅かすほどのリスクになっている。経営者はその認識を改めないと、サイバーリスクを過小評価して適切なセキュリティ対策を講じることなく、大きな被害を会社に及ぼす結果になりかねないのです。

それでは、どう認識を改めてもらうか。サイバー攻撃による最前線、つまり現場の被害の実状をお伝えすることにより、認識を変えていただくようにしています。

ちなみに、「どうして弁護士がサイバーセキュリティなんですか」とよく聞かれます。サイバー攻撃を受けた企業の現場に入ると「弁護士なのにセキュリティが分かるのですか」と懐疑的な質問を受けることもあります。私は米国UC Berkeleyの情報大学院、コンピュータサイエンスの大学院でハードウェア、ソフトウェア、ネットワーク、ハッキングを学び、サイバーセキュリティの修士号を取得しています。

こうした経験から、内閣サイバーセキュリティセンターのタスクフォースメンバーや、最近は内閣官房の「サイバー安全保障分野での対応能力の向上に向けた有識者会議」の委員も拝命しています。

サイバーリスクのゲームチェンジとなる「身代金」

ランサムウェアは、企業・組織が保有する電子ファイルを窃取して暗号化し、身代金を要求するサイバー攻撃です。WordやExcel、PDFなどのファイルが暗号化されるとコンピュータが識別できず、ファイルを開けなくなります。

ハッカーの目的は金銭です。ランサムウェアに感染した端末の画面にランサムノート、いわゆる犯行声明が表示されます。「あなたのパソコンは暗号化されました。ここに掲載されているデータは二度と復号できません。復号してほしければ暗号資産のビットコインで○○までに支払ってください」と書いてある。

画面には支払期限までのタイマーが表示され、制限時間内に身代金を支払わなければ交渉は打ち切りとなり、データは戻らないというわけです。感染被害に遭った企業・組織を焦らせ、判断を誤らせて身代金を支払わせる。これがランサムウェア攻撃の手口です。

ランサムウェアの被害実態と近時の傾向

■従来のランサムウェア
感染端末の暗号化
→復旧(復号)と引き換えに身代金(ランサム)を要求。

引用元:IPA「事業継続を脅かす新たなランサムウェア攻撃について」

この金銭を支払わせることが「ゲームチェンジ」の理由です。かつてのサイバー攻撃はデータを盗むだけでした。政府機関や重要インフラを扱う企業などのデータを盗み取るものの、それだけでした。ところが、ランサムウェアはデータを盗み、暗号化して終わりではなく、金銭を要求する点で新しい手口と言えるのです。

最近は暗号化被害だけではなく、ダークウェブ上のリークサイトに企業名を掲載し、期限までにお金を支払わないと盗んだデータをリークサイトに掲載してダウンロードできる状態にすると脅す。

金銭目的の攻撃になり企業規模に関係なく狙われる

近年は「二重の脅迫型」と呼ばれるランサムウェア攻撃が増えています。企業のネットワークに侵入してファイルサーバーなどからデータを盗み取ってリークサイトにアップロードし、脅迫する。同時にネットワーク内の電子ファイルを暗号化する。2つの側面から脅迫する、いわゆる二重の脅迫型が

主流になっているのです。

企業は二つの側面から脅迫を受けるため、お金を支払ってでも解決したいと考えるようになります。ハッカーは犯罪収益を高く得られる方向へと攻撃手法を変えています。

ランサムウェアによる被害は、独立行政法人情報処理推進機構（IPA）が毎年公表している「情報セキュリティ 10大脅威」（組織編）のレポートを見ても分かります。2016年から連続9年ランクインしており、2021年～24年まで4年連続1位となっています。

また、NPO法人　日本ネットワークセキュリティ協会（JNSA）の「インシデント損害額調査レポート　被害組織調査」には興味深いデータが出ています。リークサイトに載ったランサムウェア被害組織を日本地図にマッピングしたものです。

企業数の多い関東や関西、中部地区の被害件数が多いのは当然ですが、地図を見ると北海道から九州まで印がついています。ここから分かることは、ハッカー集団にとって、被害企業の場所、規模、産業別は関係がないということです。

地方の中小企業の皆さんにサイバーリスクの話をすると、「うちは中小企業だから狙われない」とおっしゃいますが、違います。ハッカーの目的はお金です。お金さえ払ってもらえれば、どこでも、誰でもいい。侵入できるところを狙って、データを盗んで暗号化して脅かすのです。かつては大企業や政府機関などが主なターゲットだったかもしれませんが、今は金銭目的になったことで、いつ、どの企業・組織が狙われても不思議ではありません。経営者はこの変化を認識し、セキュリティ対策を行う必要があります。

ランサムウェア攻撃による被害事例

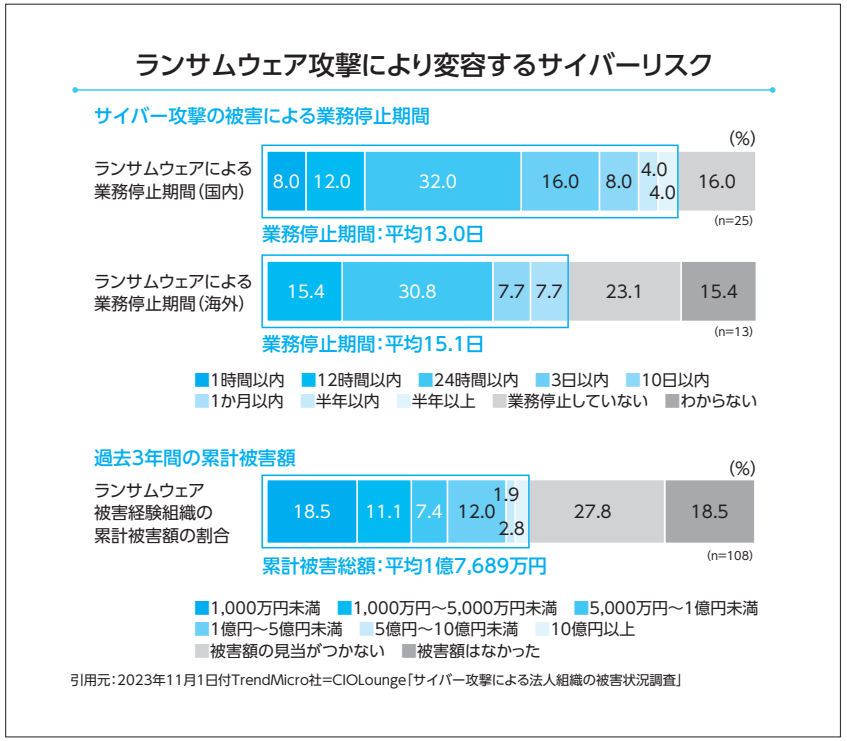
システム停止で業務が滞り
多額の被害が発生

ランサムウェア攻撃による企業・組織の被害調査もあります。業務停止期間は国内で平均13日、海外で15日となっています。累計被害額は平均1億7689万円に上ります。

海外の事例では、中国の大手金融機関の米国子会社がランサムウェア攻撃の被害に遭っています。一般に金融機関はセキュリティに厳しく、対策に多額の投資を行っています。この事案は、米国子会社へのサイバー攻撃により取引未決済となり、他金融機関に対して90億ドルの債務を負ったものです。つまり、金融機関もランサムウェア攻撃に無縁ではないのです。

もう一つ、米国のランサムウェア攻撃の事案を紹介します。石油パイプラインの企業がランサムウェア攻撃を受けてパイプラインの稼働が停止。再稼働までの1週間、政府が燃料の輸送に関する緊急措置を宣言するなど社会的な混乱を引き起こしました。影響が1週間程度で済んだのは、同社がハッカーに約5億円の身代金を支払い、システムを復旧させたからと言われています。

ランサムウェア攻撃でサイバーリスクが変容しています。企業・組織のリ



引用元:2023年11月1日付TrendMicro社=CIOLounge「サイバー攻撃による法人組織の被害状況調査」

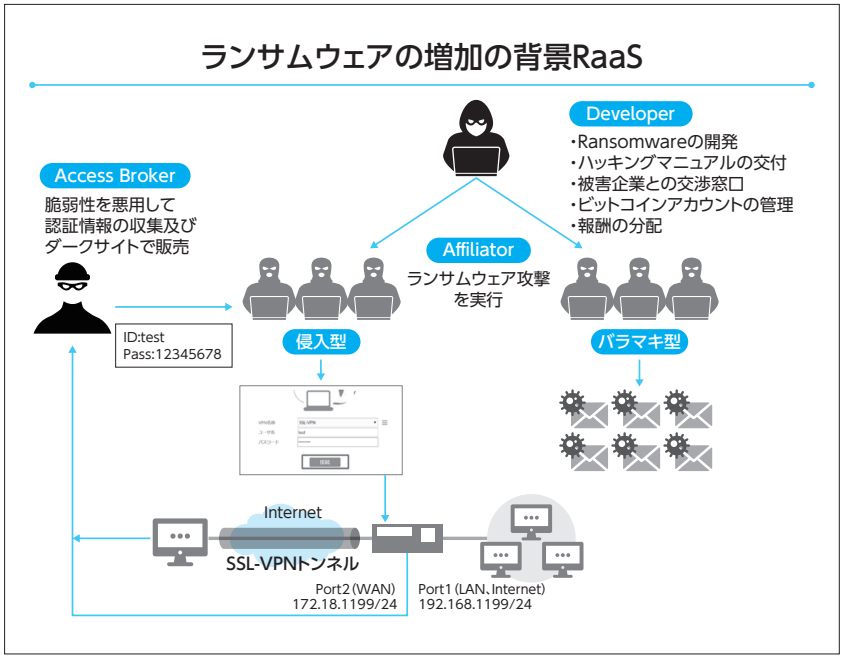
スクを算出する際、「深刻度×発生頻度」で考えます。深刻度でいえば、ランサムウェア攻撃により事業継続が脅かされるという点で、自然災害に匹敵すると考えます。例えば、地震によってデータセンターがストップする。台風や水害で送電・通信システムが停止する、輸送システムが止まるのと同様です。

発生頻度はどうでしょうか。インフラに大規模な被害を及ぼすような震災は数十年に一度、台風は数年に一度くらいでしょう。ところが、ランサムウェア攻撃は人為的に発生します。しかも攻撃者が捕まりにくい。そのため発生頻度は自然災害よりも高いと言えます。つまり、企業・組織にとって「深刻度×発生頻度」で考えると、ランサムウェア攻撃は最大級のリスクと言っても過言ではないのです。

ランサムウェアの開発や実行が分業体制になり攻撃が容易に

ランサムウェアが何故、増加しているのか、背景をお話しします。その理由の一つがRaaS（Ransomware as a Service）の普及、換言すればランサムウェア攻撃のコモディティ化です。よく知られているSaaSは、複数のソフトウェア、アプリケーションを集めてパッケージ化し、誰でも使いやすくする。ランサムウェア攻撃も同様にハッキングのスキームがパッケージ化され、技術が未熟なハッカーでも攻撃ができるという状況です。

そして、ランサムウェアの開発やハッキングマニュアルの交付などを行う「デベロッパー」、ランサムウェア攻撃を実行する「アフィリエイター」、ぜい弱性を悪用して認証情報を収集、ダークサイトで販売する「アクセスブローカー」の完全分業体制が出来上がっていることも、ランサムウェア攻撃が増加する一因になっているのです。



デベロッパーの役割は電子ファイルを高速で暗号化するランサムウェアの開発と配布です。また、ハッキングマニュアルを作成し、アフィリエイターに配布します。さらには、ランサムウェア攻撃の被害企業の交渉窓口となり、身代金として暗号資産を支払わせ、報酬の分配まで担当しています。

アフィリエイターの役割は、ランサムウェア攻撃を実行することです。ランサムウェア攻撃が流行した初期に多かったのは、バラマキ型でメールの添付ファイルを開くと端末に感染して暗号化するといった手口でした。PC1台が被害を受けるだけですので、被害範囲は限定的であり、その結果、身代金の要求額も数万円程度でした。

今は、侵入型に移行しています。典型的な手口としては、侵入に使用するためのID、パスワードといった認証情報をアクセスブローカーから購入するのです。アフィリエイターは攻撃の際に購入した正規のID、パスワード、つまり「合鍵」を使って企業のネットワークに侵入します。

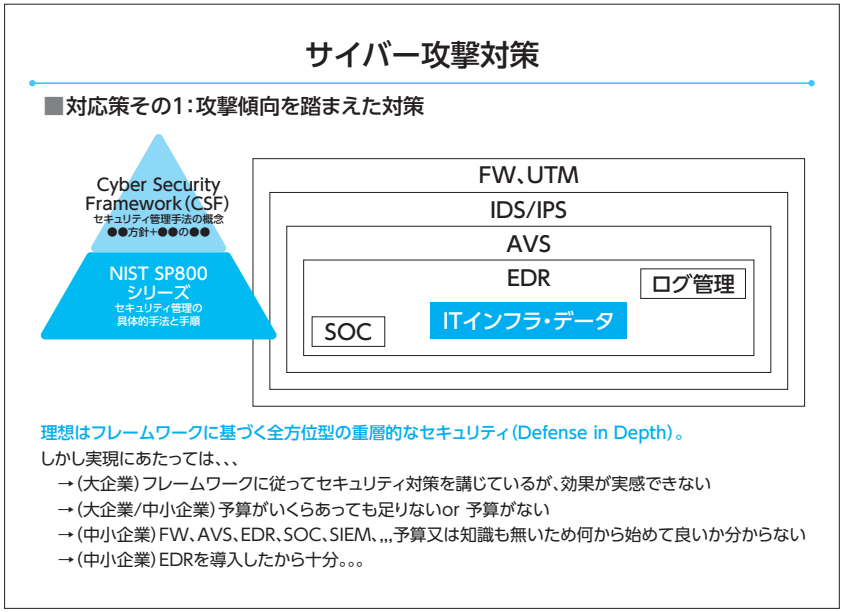
侵入型はデータがすべて窃取され、システムも破壊されることから企業のダメージが大きく、身代金の要求額も跳ね上がる傾向にあります。仮に企業が身代金として1億円支払った場合、デベロッパーやアクセスブローカーに代金を支払っても十分に元が取れるのです。

デベロッパーとしては、攻撃を実行するアフィリエイターをいかに増やすか。実行犯が増えれば、デベロッパーの収益が増えるため、ハッカー集団はリークサイトでアフィリエイターをリクルートしているのが実情です。

攻撃傾向を踏まえた現実解となるVPNのぜい弱性対策

増加する一方のランサムウェア攻撃に対して、どう防御すればいいのか。対応策について説明します。その第一が「攻撃傾向を踏まえた対策」です。理想はフレームワークに基づく、全方位型の重層的なセキュリティ対策、Defense in Depthです。

しかし、サイバーセキュリティの現場にいる私から見ても、重層的なセキュリティを実現するとなると、難しいのが実情です。大企業からは、フレームワークに従ってセキュリティ体制を講じているが、効果が実感できない。中小企業からは、予算がいくらあっても足りない、そもそもセキュリティツールの知識がないので、何から始めればいいのかわからないといった声も聞かれます。



そこで、攻撃傾向を踏まえて当該傾向に対する対策を優先的に講じることが現実解だと思うに至りました。例えば、ランサムウェア攻撃の傾向として「VPN」経由があります。警察庁の「令和5年におけるサイバー空間をめぐる脅威の情勢等について」の中で、サイバー攻撃の侵入経路を調査、公表しています。最も多いのが「VPN機器からの侵入」（63%）で、以下、「リモートデスクトップからの侵入」（18%）、「不審メールやその添付ファイル」（5%）となっています。

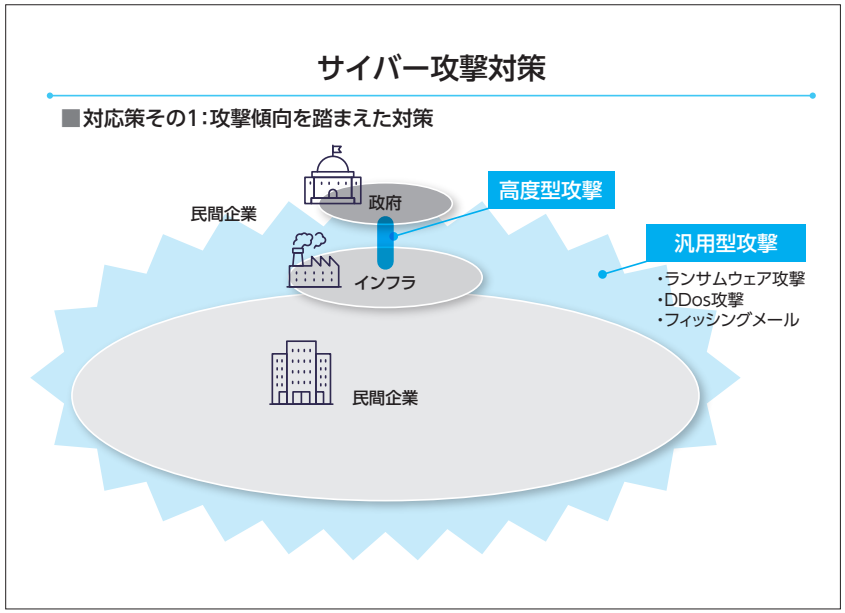
VPNやリモートデスクトップはコロナ禍のテレワークで盛んに使われるようになったリモートアクセス用のツールです。この調査から分かることは、リモートアクセスをきちんと管理すれば、サイバー攻撃、ランサムウェ

アのリスクを81%減らせるということです。

VPNのぜい弱性管理と多要素認証で攻撃を防ぐ

これらの事案から、侵入される原因を考えると二つのパターンがあります。一つはVPN機器のぜい弱性に対してベンダーが提供する修正用ソフトウェアが適用されないまま放置されたぜい弱性を突いて裏口から侵入されるパターン。もう一つは、ID、パスワードが盗まれ、「合鍵」を使って侵入されるパターンです。

この二つに集約すれば対策はシンプルです。一つは、ぜい弱性管理を徹底すること。ベンダーからアップデート通知が届いたら、速やかに適用することです。もう一つは、多要素認証を利用すること。ID、パスワードの「合鍵」を盗まれても、複数の認証方法を組み合わせ、「チェーンロック」をかけておけば侵入は防げます。



多要素認証は設定画面上でONにすればよく、コストをかけずに対策が可能です。ぜい弱性対策と多要素認証の二つを実行すれば、ランサム攻撃の8割のリスクを減らせることになります。

サイバー攻撃のパターンを見ると、政府機関や重要インフラを狙う高度型攻撃と、民間企業を狙うランサムウェア攻撃などの汎用型攻撃があります。

ここで重要なのは、高度型攻撃がすべてだと考え、重層的サイバーセキュリティ対策を行おうとすると非現実的なアプローチになりかねないという点です。民間企業を対象とするほとんどのサイバー攻撃は汎用型攻撃です。企業・組織が限られたリソースの中でやるべきことは、攻撃傾向を踏まえた汎用型攻撃への対策です。余力があれば高度型攻撃に備える。このアプローチを間違えないようにしてほしいと思います。

自然災害への備えと同様にサイバーリスクBCPを策定

サイバー攻撃の対応策として、サイバーリスクBCPがあります。多くの企業・組織では自然災害などに備えてBCPを策定しています。そのサイバーリスク版です。サイバー攻撃で万一、事業が中断されても、ダウンタイムを小さくして事業復旧を速やかに行うものです。

私は企業・組織にサイバーリスクBCPの策定をお勧めしています。サイバーリスクBCPを検討する際、ランサムウェア攻撃の身代金を要求されたらどう対応するかについても考えておきます。日本の場合、ランサムウェア攻撃を受けてもほとんどの企業・組織が身代金を支払わないという判断をしていますが、最近は支払うケースが増えているという報道もあります。サイバーリスクBCPで、有事に備えるシナリオを考えておいてほしいと思います。

もう一点、サイバー攻撃の対策として必要なのが、バックアップの確保で

す。盗まれた情報は戻りませんが、ランサムウェア攻撃で電子ファイルが暗号化されてもバックアップがあれば業務の早期復旧は可能です。

ただ、注意が必要なのは、バックアップを業務システムなど他のシステムと同じネットワーク上に置かないことです。他のシステムと同様にバックアップも暗号化されるリスクが高くなるからです。

実際に、BCP対策としてバックアップをとっていたものの、業務システムと同じネットワーク上に置いていたため暗号化されたという事案もあります。バックアップの取り方、取得のタイミングには工夫が必要です。

賠償損害や費用損害、利益損害をカバーするサイバー保険

サイバー攻撃対策として検討したいのが、サイバー保険の活用です。国内の損害保険会社の保険内容を比較したところ、概ね個人及び取引先といった第三者からの「賠償損害」、調査費用や弁護士費用、再発防止策に要する費用といった「費用損害」、事故がなかったら計上できた営業利益をカバーする「利益損害」の3つで構成されています。

また、金銭的な補償だけではなく、サイバー保険に加入していると、副次的な効果として、サイバー攻撃に遭った場合、フォレンジック調査会社や弁護士などの専門機関を紹介してくれます。昨今は企業・組織と取引する際、サイバー保険の加入の有無を確認されるケースも増えてきました。つまり、加入していないと受注にも影響するというわけです。

サイバー保険は単なる「費用」ではなく、信用を獲得するための「投資」の側面があります。いずれは、自動車の自賠責保険のようにサイバー保険も加入することが当然となる保険になるのではないかと期待しています。

経営者の義務になるサイバーセキュリティ体制の構築

サイバーリスクに対して、法務が抑えるべきポイントの一部を紹介します。私が一番言いたいことは、サイバーセキュリティ体制の構築は経営層の義務であるということです。現場のタスクではなく、トップダウンで取り組むべき義務なのです。

政府のサイバーセキュリティ戦略本部の文書にも「会社におけるサイバーセキュリティに関する体制は、その会社の内部統制システムの一部と言える。取締役会の内部統制システム構築義務には、サイバーセキュリティを講じる義務が含まれる」と明記されています。

また、意思決定機関が決定したサイバーセキュリティ体制が適切でなかった場合、組織に対して損害賠償請求が問われる可能性があることです。経営者が適切なセキュリティ対策を講じずに会社に損害を与えた場合、株主から訴えられる時代を迎えているのです。

サイバーリスクは「if」もしもではなく、「when」いつあってもおかしくない状況です。もしかすると、皆さんの会社のID、パスワードが盗まれているかもしれません。サイバーリスクは企業・組織にとって最大級のリスクであることを認識していただきたいと思います。

第 7 回

世界に普及可能な日本発 サイバー技術の生産手段の確立

登壇者

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
サイバー技術研究室長

登 大遊 氏

東日本電信電話株式会社（NTT東日本）
特殊局 ビジネス開発本部
特殊局員
筑波大学　客員教授
ソフトイーサ株式会社
代表取締役

自由に技術開発できる環境で IT人材不足の課題を解決

今やITは社会基盤となり、企業や行政、個人の活動を支え、非常に重要な地位を占めるようになっています。ところが、このITはぜい弱でなかなか安定しない。基盤は堅牢でなくてはなりません。それは国の統治や企業活動の安定性にも関わり、基盤がきちんとしていなければ、上位のシステムも危ないということです。

そのため、私たちは基盤をしっかりしたものにしなければなりません。ただ、その活動は1度で終わるものではなく、次の世代、その先の世代も活動を継続することになります。

例えば、法律は社会基盤となり、各組織には、法律の基本的・基礎的な事柄を理解する人がたくさんいるので安定して社会が動いています。法律と同様にITも重要な社会基盤であるにもかかわらず、各組織に基本的・基礎的な部分を理解している人が少ないのではないでしょうか。このアンバランス

な状況を解決するのが私たちの世代の役割になると思います。

その解決方法は、人材育成にあります。これまでのITの人材育成は、私を含め、各個人の幸運と偶然に頼ってきた面があります。そうではなく、再現可能な形で人材育成を体系化する。それを皆さんと作り上げることができれば、50年、100年後も残るものができる可能性があります。ここにITに関わる人材育成を行わなければならない理由があるのです。

今日はいくつもの職場で「けしからんじゃないか!!」と言われながら、ネットワークやセキュリティなどの開発・提供に取り組んできた私自身の体験に基づくお話をします。

IT人材不足は日本の国難ともいえ、その解決が急務となっています。第一の問題は、各組織の目前のIT人材不足、リテラシー不足をどう解決できるか。そして第二の問題は、OS、クラウド、通信、セキュリティ、ゼロトラストなどのシステム、ソフトウェア技術や産業（プラットフォーマー）を自ら生み出せるIT人材を、どうすれば日本でも育成できるかです。

その答えの第一は、素質のある人が自律的なコンピュータ／ソフトウェアの実験環境を自力で勝手に構築することを黙認し、その環境の上で彼らが自由に技術開発できるようにする。これにより、自然に人材が育ち、魅力的な職場となり、優秀な人材が志願し、世界一のIT技術が生まれます。これは歴史の法則です。

答えの第二は、その自然発生には、業務と合理的関連性があると説明できる、試行錯誤に適したコンピュータやネットワーク（所与のものでなく、自ら組み立てて実現するもの）の黙認、擁護が決定的に重要です。

そして答えの第三は、失敗の許容領域において、試行錯誤に基づくシステムの自作を推進すれば、単にコストダウンが実現できるだけでなく、IT好事家の技術力、内製力、セキュリティ能力、経営能力が向上します。その結果、魅力的な職場となり、人材難の問題も解決し、ITに限らず全領域における組織能力の飛躍的な発展が見込めると思います。

ブラックボックス化に対抗する透明性の高いシステム開発

日本の国家的課題として、ITの国際競争力の低下が挙げられます。差し迫った「国難」として、人材育成の問題だけでなく、国際競争力の低下や深刻な収益不足、サイバーセキュリティ、IT自給率の低下、安全保障などの問題があります。ITの国際競争力では、世界中で使われているIT技術（システムソフトウェア、アプリケーション、AI、クラウドサービスなど）を生み出す技術力が必要です。

例えば、米国のGoogleやAmazon、Microsoftのような巨大なプラットフォーマーが日本にはほとんど存在しませんが、これらをどのようにして生み出せばいいのかといった議論もあります。また、セキュリティ分野では、ビジネスをやろうとしてもなかなかうまくいかないという声も聞かれます。

近年のセキュリティソリューションはクラウドサービスとして提供されるタイプが増えています。しかし、クラウドの中はブラックボックス化され、どうなっているのかよく分からない。これには、セキュリティ上の本質的な問題があるのではないかと考えています。

これにはビジネス上の先行者の独占的利益追求の目的があるのです。ブラックボックス化されたクラウドサービスやセキュリティサービス、さらにAIサービス、仮想ネットワークサービスなど多種多様なサービスがありますが、これらのサービスを作っている人たちはその中身を公開しない場合も

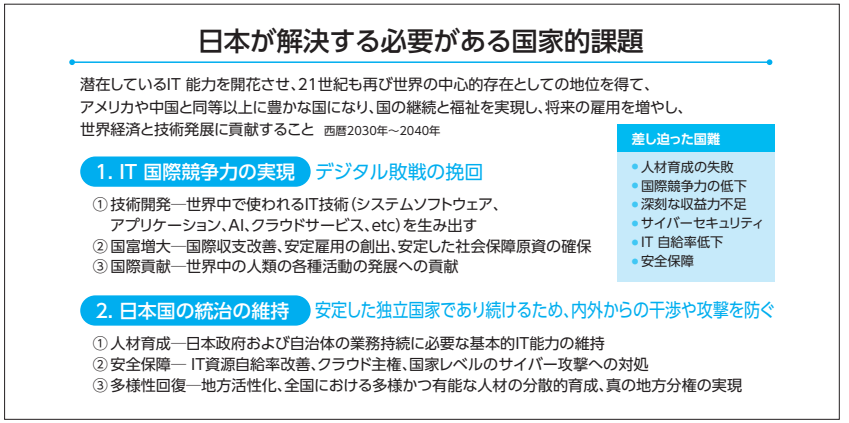
あるし、あえて中身を秘密にすることで自分たちのビジネスの優位性を保つといった動きも見受けられます。

これは本来、伝統的なコンピュータ技術者や科学者たちが信じてきたことと少し異なるのではないかと思います。昔の日本人は西洋の技術を学び、西洋の産業を参考にしながら、日本ならではのモノづくりで世界一になってきました。

今の西洋的なやり方をまねてブラックボックス化された独占的なものを作れば短期的には利益が上がるかもしれません。しかし、日本は別のより良いやり方があるのではないかと思います。世界の人々から信頼される日本で作るコンピュータシステムやセキュリティシステム、ソリューションは、信頼に耐え得るものができるチャンスであり、ITの国際競争力を高め、世界に貢献するチャンスでもあるのです。この方法なら、世界中の信頼を得、長期的な利益と繁栄を享受できます。

日本にプラットフォーマーが存在しないという問題は、国の統治の維持にも関係しています。安定した独立国家であり続けるためには、内外からの干渉や攻撃を防ぐ必要があります。行政システムや国民の重要なプライバシー情報を管理する場合、海外のブラックボックス化されていて安全性が検証不能な外国企業が管理するクラウドサービスには、セキュリティ上の限界があります。

セキュリティの考え方として、完全性・機密性・可用性があります。例えば、国や地方自治体などの公権力が運営するコンピュータシステムについては、機密性を最大限確保し、各個人の内面に関わる可能性がある住民情報を決して第三者に開示されないことが保障されなければなりません。自ら管理支配するコンピュータシステムであれば、これらは保障されます。しかし、外国のパブリッククラウド事業のクラウドでは、そうではありません。よく、契約上の義務があるから外部に漏らすことはないと言われます。しかし、契約は相手が守らなければ意味がありません。外国企業にこれを守ってもらうためには、契約が破られた場合に発生する膨大な国民的損害を補償できるだけの何らかの担保をあらかじめ差し出してもらうことが必要ですが、担保がないこともよくあります。



例えばクラウドサービスの場合、モノとしての実体を物権的に支配できず、システムの運営主体は、どのようにデータが取り扱われ、保全されているのか確認すらできないこともよくあります。また、データが棄損するような場合、クラウドサービス会社に修復を要求しますが、その際に、相手方の過失あるいは故意であることを裁判所に認定してもらうためには、証拠を集めるプロセスが必要です。しかし、証拠は、被告となる彼らのブラックボックスの中にあり、外から見るのは困難で、大きな情報格差が生じている。これでは、外国企業のパブリッククラウド事業者側が過失や故意で情報喪失・変質を発生させた場合でも、そのことを証明できず、原状回復あるいは賠償を請求できません。私たち日本の行政主体や日本企業が、外国企業のパブリッククラウド事業者のクラウドを利用する際に直面しているセキュリティの問題の一因はここにあるのです。

この問題を解決するため、欧米では、少なくとも自国の企業、エンジニアが作ったクラウドサービスやセキュリティシステムを利用する動きが広がっています。米国はもちろん、中国も同様です。日本もいずれは自国で開発した新しいクラウドサービスやセキュリティシステムが、国民や企業の情報を保護することができるようになることが期待されています。

国の統治の維持で重要になるセキュリティの知識

これまでに述べたような自国のITの自己統治を実現するためのシステムソフトウェアを、自国で、あるいは信頼できる者たちで開発する体制を作るには何が必要か。単なるプログラミングの知識やネットワークの知識だけではできません。セキュリティの知識が必要です。ただ、セキュリティの知識は一般的なプログラマーは持っておらず、ぜい弱なプログラムができる結果になる。そこで、私たちはもっとセキュリティを勉強する必要があります。セキュリティの知識とコンピュータ、OS、ネットワークなどの知識をうまく組み合わせることで、強固なクラウドサービスを作ることが可能です。

米国のプラットフォーマーの成功の要因は、次の通りです。彼らには、単一の組織の中にコンピュータ、ネットワーク、セキュリティの知識をいずれも持つ人たちがいます。一方、日本はどうかというと、コンピュータ会社、ネットワーク会社、セキュリティ会社というように組織が分かれています。

国際競争力を実現できるITプラットフォーマーを作ることと、日本の統治の安定性、自己統治権を維持することがセキュリティの観点からも重要になるのです。今はまだ、日本企業はさまざまなセキュリティ製品・サービスを購入し、組み合わせて使っていますので、自己統治の面ではまったく不十分です。そこで、日本の企業や行政機関などが自らシステムソフトウェア技術、製品・サービスを作ることができる創造力を総体的に身に付けることが、日本の国家的な課題であると思います。

IT人材育成では、実は、日本だけでなく米国のIT企業も課題を抱えています。米国においてすら、伝統的なOSやネットワーク、セキュリティ分野の基本的・基礎的な領域に関心を持つ若者がだんだん減っているというのです。コンピュータ分野の仕事は人気が高いのに、若者が増えないのは、彼らがより魅力的な職業に就くからです。例えば、ソリューションの開発や生成AIの分野などは即金的なので魅力があります。他方で、サイバーセキュリティやOSは重要な基盤であるにもかかわらず、それなりの努力をしなければ、基本的・基礎的なリテラシーを身に付けることが困難であり、米国IT企業ですら、いつの間にか優秀な人材が少なくなるという状況です。

人材育成においては、日本ならではのやり方があります。長期的な業務フローを作り、組織的に運用する。一人の天才に頼るのではなく、たくさんの秀才を束ね、もし一人が欠けても組織が回るようにするのが日本のやり方です。

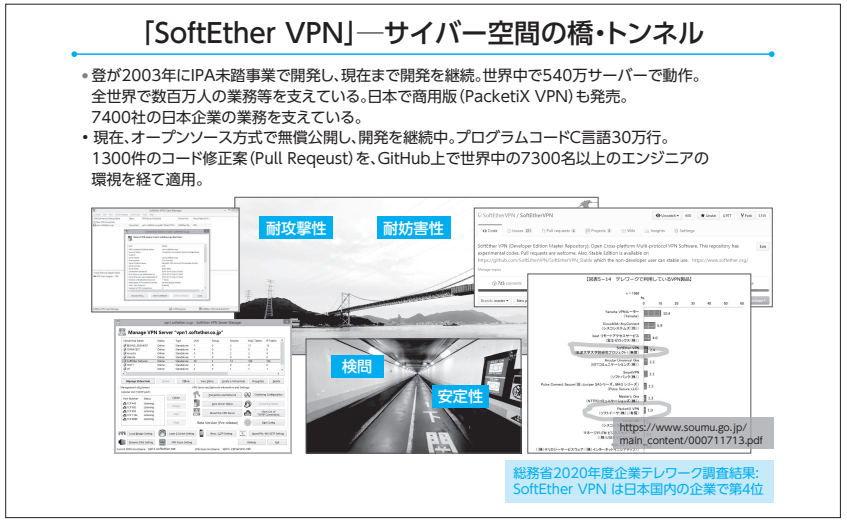
この組織的方法をコンピュータシステムやセキュリティ、クラウドの開発に応用することにより、米国ではおそらく実現できずに比較的低品質・短命な水準にとどまるような、クラウド等のシステムソフトウェア領域において、50年、100年持続可能な日本発の製品・サービスが豊富に生まれると思います。歴史を見ても、20世紀に、米国の電機メーカーや自動車メーカーは素晴らしい製品を作りましたが、日本の大手電機メーカーや自動車メーカーはさらにいいものを作り、世界に提供して、多くの面で世界一になりました。米国技術企業を倒産あるいは弱体化に追い込むくらいの実力がありました。こんな国は日本だけではないでしょうか。21世紀後半には、日本がITで再びキープレーヤーになると主権者は信じていると思います。

コロナ禍で短期間・低コストにテレワークシステムを開発・提供

次に私が手がけてきた「インチキ・システム」「けしからん!!」についてお話しします。「インチキ」の意味は、既存の確立されたプロ向けの手法ではなく、創意工夫を凝らして、新しいやり方でやってみること（＝イノベーション）です。

まず、「SoftEther VPN」は、私が筑波大学情報学類の学生だった2003年にIPAの未踏事業で開発したものです。現在、オープンソース方式で無償公開し、開発を継続中です。世界中の540万サーバーで動作し、数百万人の業務を支えています。日本では商用版（PacketiX VPN）も発売され、約7400社に利用されています。

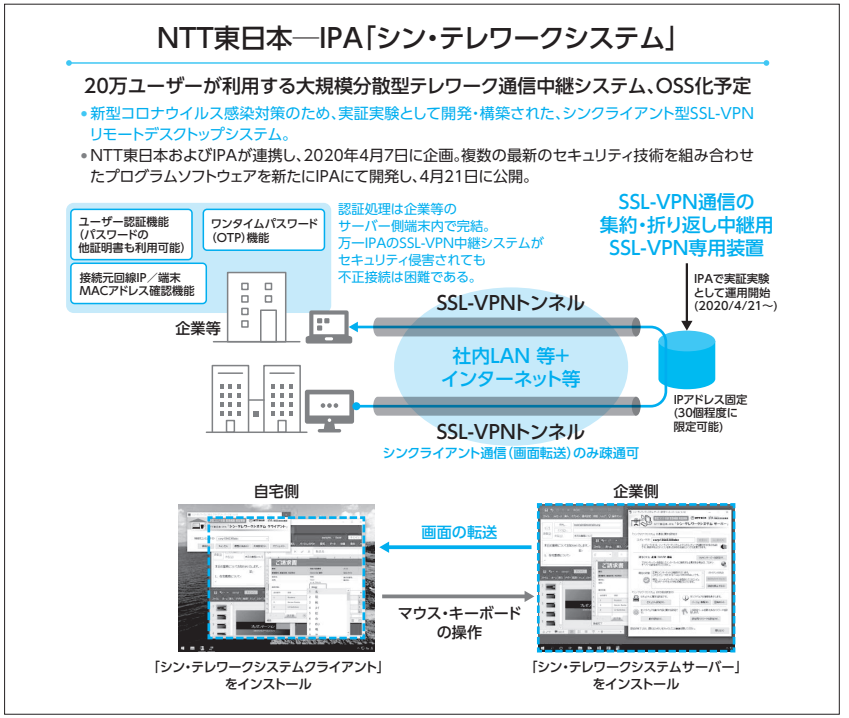
このSoftEther VPNはリリース当初、「VPN性能が強力過ぎる」「簡単過ぎて危ない」といった苦情があり、政府が配布の一時停止を要請する事態となりました。まさに「けしからん!!」というわけです。



そして、SoftEther VPNを基に開発したのが「VPN Gate」です。外国政府の検閲用ファイアウォールを無効化し、自由なインターネットアクセスを実現するための分散型中継VPNシステムです。インターネット検閲が行われている中国やロシア、イランなどの国・地域の市民、約4700万人のユニークユーザーに、自由な知識（Google、Wikipedia、YouTubeなど）へのアクセスを可能にしています。

言論統制に対抗するソリューションを作ることが許されている国は、世界の中でそれほど多くはありませんが、日本はそれが許されていますので、これを作る作業に積極的に取り組む必要があります。なぜやる必要があるかというと、インターネット検閲がある国・地域の若者たちがGoogleやWikipediaを閲覧して勉強しようとしても遮断される場合があるからです。そういう環境の若者たちが勉強できないのは残念なことです。彼らの人生は一度きりなのです。

政府が何らかの目的で情報を遮断するのは、各国の事情があります。しかし、それによって勉強したいと思っている人たちの学問上の記事へのアクセスまで、例えばGoogleやWikipediaのドメインごと遮断するのは、過度な制約ではないかと考えています。制約を上回る技術を使い、全世界に提供する



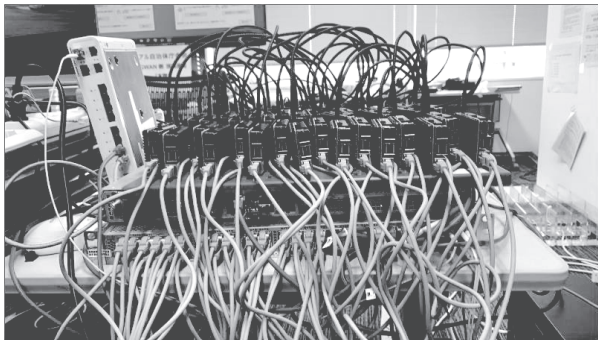
ことで情報を得たいと考えている人たちに対して、アクセスの自由を保障できるのではないかと思います。

大規模分散型テレワーク通信中継システム「シン・テレワークシステム」は、NTT東日本とIPAが連携し、2020年4月に新型コロナウイルス感染症対策のため、実証実験として開発、構築したシンクライアント型SSL-VPNリモートデスクトップシステムです。複数のセキュリティ技術を組み合わせたソフトウェアを新たにIPAで開発し、短期間で作ることができました。公開1年6カ月で日本企業の約20万ユーザーが利用しています。

そして、このシン・テレワークシステムの中継ゲートウェイのアイデアを生かしながら改良して作ったのが、IPAとJ-LIS（地方公共団体情報システム機構）による「自治体テレワークシステム for LGWAN」です。行政ネットワークはセキュリティ確保のためにインターネットと切り離されており、コ

IPAによるLGWAN インターネット間テレワーク用画面転送中継ゲートウェイ

本システムは、自治体庁内のLGWAN接続系端末から、全国規模のLGWAN閉域網を介し、IPAの中継ゲートウェイ（LGWAN-ASP）を経由して通信を行なう仕組みとなっている。従って、自治体庁内の既存のLGWAN接続系環境をそのまま利用でき、新たに自治体庁内からテレワーク用にインターネットとの接続環境を用意する必要も、ファイアウォールの設定を変更したりする必要もなく、回線費用等もかからない。



「自治体テレワークシステム for LGWAN」は、「シン・テレワークシステム」とは物理的に完全に分離された新たなシステムとして構築。しかしながら、「シン・テレワークシステム」で確立されたRaspberry Pi4を用いた安全で低コストな中継ゲートウェイシステムのアイデアはそのまま使用している。

ロナ禍でのテレワークが難しい状況でした。そこで、自治体職員がテレワークをできるようにIPAで開発を手がけることになったのです。

私が所属するIPAサイバー技術研究室のサーバー・ネットワーク実験部屋のラックいっぱいに小型のシングルボードコンピュータ「Raspberry Pi」を並べています。地方自治体の約半数、7万人以上の職員に「自治体テレワークシステム for LGWAN」が利用されています。

このシステムは、自治体庁内のLGWAN接続系端末から、全国規模のLGWAN閉域網を介してIPAの中継ゲートウェイ（LGWAN-ASP）を経由し通信を行う仕組みです。そのため、自治体庁内の既存のLGWAN接続環境をそのまま利用できます。新たに自治体庁内からテレワーク用にインターネットとの接続環境を用意したり、ファイアウォールの設定を変更したりする必要もありません。

OSSを活用してテレワークのセキュアな通信を実現

テレワークシステムなどの設計・構築を自前で行っていると、ファイアウォールやIDS（不正侵入検知）などのセキュリティについても自作したくなります。自作する上で強力な武器となるのがLinuxなどのOSS（オープン・ソース・ソフトウェア）です。

OSSを活用する場合、既存のプログラムをうまくつなぎ合わせる接着剤的な部分が最も重要になります。その部分さえ作ってしまえば、市販のファイアウォールなどのセキュリティソリューションよりも、よりシンプルで低価格、安全性の高いものが作れます。市販製品と異なり、生産終了によるサポート切れの心配もなく、内容もブラックボックス化されない形で実現できます。

IPAでは、2017年から市販のファイアウォールなどは使わずに、グローバルIPアドレスをBGP（Border Gateway Protocol）でインターネットに直結し、自分たちで管理・監視システムなども自作して運用しています。この環境により、極めて高いセキュリティを実現しています。そして、テレワークシステムを利用する企業ユーザー、行政職員のテレワークのセキュアな通信を支えているのです。

こうした自作による方式は、行政機関の1つであるIPAにとって、当初受け入れ難いものであると言われました。内閣官房のサイバーセキュリティの政府統一基準となるセキュリティポリシーに当てはめれば、違反しているのではないかと。ファイアウォールの設定、インストールするソフトウェアの種類など全て許可を得て、CISO（最高情報セキュリティ責任者）に申請しなければならないというのです。

以前のIPAには日本型企業によく見られるように、事務系ICTシステムのルールやセキュリティポリシー、物事の決定の仕組みしかなく、ブラックボックス信仰みたいなものもありました。しかし、それではいけないと思い、IPA内で従来とは異なるイノベーションを許容する独自ルールを作りま

した。これにより、自治体テレワークシステムなどを短期間かつ低コストで構築・提供できるようになったのです。そして、自分たちで作ったほうが安全なものができるということを実証し、その方針をIPAから全国の行政主体に普及する活動を続けています。

LAN/WAN構築・運用を自ら行いネットワーク技術を身に付ける

米国のプラットフォーマーのように、コンピュータ、ネットワーク、セキュリティの3分野に熟知した人材がそろえられれば理想的ですが、そうではない環境でどう人材を育てるか。ICT技術のうち、最も重要なコンピュータ・ネットワークに関する高度な技術は、LAN/WANの構築・運用を自ら行うことで身に付けることができます。

そのためには、単にソフトウェアやコンピュータだけの手元にある情報処理分野だけでなく、ダークファイバーや通信局舎などの物理ファシリティなどの情報通信分野を含め、日本国内に豊富に存在するリソースや設備を駆使して、若手IT人材が独立した自律ネットワークの設計、構築、実験、運用を自由に楽しむことを推奨するか、少なくとも黙認する必要があります。

また、日本の大企業をはじめ、政府の中央省庁、独立行政法人、大学、研究所などではグローバルIPv4アドレスを数多く保有しています。しかしながら、これらは活用されていないか、または単なる日常的な業務用インフラ（ICTユーザー用の社内LAN、学内LAN）として利用されているケースがほとんどです。

希少な資源であるグローバルIPv4アドレスが、若手ICT人材によって自由に利用され、新たな独自性のあるソフトウェア、システム、実証実験、クラウドサービスなどを構築するために生かされていないことが大きな問題です。これらを少しでも使えるようにするだけで、日本の企業・組織は強力なICT能力を手に入れることができます。加えて、自組織内のICT人材の活動によって自然に生み出されるICT技術は飛躍的に高まるはずです。つまり、プラットフォーマーと同じようなインターネットサービスやソフトウェアが作れるようになる可能性があります。

IPAの活動に関心のある地方の高専生や大学生、小規模な研究チームなどが「本物のネットワーク実験環境がIPAにあるらしい」「自由に機材を置かせてくれるらしい」といった噂を聞きつけ、IPAサイバー技術研究室などに私物の実験機材を持ち込むようになりました。

1980年代～2000年代に各地に密かに存在した「インチキ・サーバー置き場」は、実は超正統派の人材育成環境であったと思います。若手ICT人材の試行錯誤が許容され、育成された高度ICT人材と技術が現在の日本のICTとセキュリティを支えているのです。

超正統派コンピューティング人材育成環境の復活に向けて

コンピュータ、ネットワーク、セキュリティの人材育成は、手元に自由に扱えるマシンがあり、自分でOSをインストールし、ファイアウォールを設定することから始まります。万一、自作のコンピュータがハッカーに攻撃され、不正侵入される状況になっても、それがまた勉強になります。

ところが、2010年代以降、世代交代が進み、大学・研究機関・民間企業から、ICT人材と技術を育成する環境維持の責任を引き受ける管理者が見受けられなくなり、日本から超正統派コンピュータ・ネットワークの試行錯誤スペースがほとんど消滅してしまったのです。

その理由として、インターネットやシステムソフトウェア、クラウド等がサービス化されたことにより、これらのインフラ上で動作する単なるアプリケーションを作ったほうが、研究やビジネスの対象として手っ取り早く利益が得られるようになってきたことがあります。そして、優秀な人材が上位のレイヤーに集中した結果、より重要な、OSやセキュリティ、通信システムなど下位レイヤーのインフラ技術開発の重要性と面白さが分かる人材が、日本の組織の中ではまれになってしまったのです。そこで、再び2000年代の超正統派コンピュータ&ネットワーク環境の復活に向けて活動を進めています。

ICT技術を船に例えると、アプリケーションは船室やレストラン、倉庫などの設備に該当します。つまり、取り換え可能で、変化が激しく、長続きしない技術領域です。アプリケーション領域は魅力的で、短期的には収益が上がりますが、新規参入の難易度が低い分、長期的な競争力の確保は難しいと言えます。

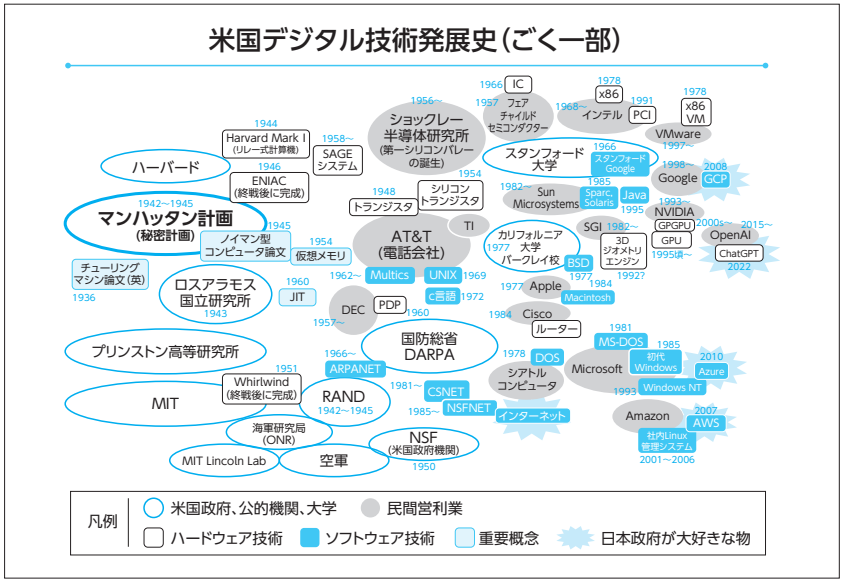
船の基盤となるのが、船体やエンジン、操舵などで、システムソフトウェア、インフラに該当します。造船所で一度作られると長期間、普遍的に使われる技術領域です。プラットフォーマーもいわば造船所の役割を担っています。

OSやセキュリティシステム、クラウドシステム、通信システムなどシステムソフトウェアを作るのは大変ですが、一度作ってしまえばなかなかまねをされることなく長期的な経済的利益の獲得も可能です。そこで、国際競争力の根源となるシステムソフトウェアに関わる人材を育成したいと考えています。

自由な創意工夫と試行錯誤で日本のICT産業を育てる

システムソフトウェアを作るといっても、必ずしもOSレベルから作る必要はなく、前述したようにOSSのLinuxなどを活用すればよいのです。AmazonやGoogle、Microsoftなどプラットフォーマーが提供するサービスの最深部を見ると、結構Linuxが使われており、そのLinuxの部分は独自に堅牢なものをつくることで、他社に依存していないのです。他社に依存するとOSなどの更新時にぜい弱性が忍び込んだりするリスクもありますが、自社でぜい弱性のメンテナンスも行なうなどコントロールしているのです。

かつてメインフレームやエンタープライズサーバーなどの開発・構築で培った日本のIT企業のソフトウェア技術力は高く、他社に依存しないシステムソフトウェアの開発も可能だと思います。例えば、以前の日本の基幹産業であった造船をはじめ、鉄鋼、自動車、半導体、家電などの分野で世界トップクラスでした。諸外国の産業技術を吸収し、それを超えて進化させ、世界トップクラスの技術と製品を実現しました。



ここで重要なのが、自由な創意工夫と試行錯誤です。日本のICT産業の試行錯誤はこれからです。日本が米国のプラットフォーマーのようにクラウドやAIサービスを作れるようになるには、クラウド型コンピュータシステムの基本構造を知り、戦略を立案する必要があります。

その1つがOSSの活用です。OSSの部品を組み合わせていいものを作る。プラットフォーマーは皆、これを実行しています。Amazonの仮想サーバーサービスAmazon EC2もそうです。当初はバーチャルマシンに他社製のハイパーバイザーを使っていましたが、その後OSSを使って自社で開発しています。

日本のクラウドサービスはどうでしょうか。創意工夫や試行錯誤といった「遊びの環境」がなく、他社製のハイパーバイザーなどを購入し、クラウドもどきを作っているのです。これでは他社との競争力も生まれません。セキュリティ機能を実装するにもOSSと違って、メーカー独自のソフトウェアでは勝手に触ることはできず、ぜい弱性対策もメーカー任せ、他社任せになってしまいます。

日本が世界に対して生み出せるデジタル技術の例(世界が求める実用技術)

今、全世界の政治家・役所・大企業・SE・若手人材が皆困っているのは、以下のようなごく当たり前のデジタル技術がどこにも存在しないことにある。

長寿命OS技術 40年間以上使えるOS、システムソフト、基本Appまたはその延命技術
- WindowsやLinuxを40年以上挙動変更なしに利用できる仕組み
- カーネル、定番のメールサーバー、Webサーバー、言語、DB等のセキュリティパッチをメンテナンス

クラウド技術 40年間以上確実・簡単にクラウドを構築・運営できるクラウド技術
- 誰でもAmazon EC2, S3同等のクラウドサービスを簡単・確実に構築し完全に所有できるソフトウェア(誰でもAWSのようなパブリッククラウドサービスを開業したり、同様に、自組織で安心して簡単に使えるプライベートクラウドが構築できる)

ネットワーク技術 40年間以上使えるネットワーク技術
- 誰でもCiscoのようなルーターや、ファイアウォールや、仮想ネットワーク(VPN、SDN)を簡単・確実に実現できる、ハードウェアに依存せずにいつまでも利用可能なネットワークOS(ファームウェア)

汎用コンピュータ回路 40年間以上生産し続けることが可能な挙動が安定したRaspberry Piのようなもの
- 自国のみで無限に安価に生産でき、2個以上のネットワーク端子が付いた、LinuxやネットワークOS(3.の技術等)が動作可能な、信頼性の高い、Raspberry Piのような組み込みハードウェア生産法(ARM等のライセンスが一切不要)

文書検索・AI技術 既存の巨大組織向けのセキュアなドキュメント学習AI 技術
- 複雑・膨大な蓄積ドキュメントやメールによる組織内知見に対してChatGPTのように問い合わせできる完全スタンドアロンの高機密性対応AIシステム

人材育成手段 上記の各システム群のアーキテクチャを理解し、これらに類するものを一から発想できるに足る知識を整理・体系化する教科書群と人材育成環境
- 日本人に加えて、日本よりも後進の国の方々もデジタル技術を生み出すことができるようにする

私が作成した日本デジタル技術発展史で見ると、わが国は2020年代～2030年代にかけていいポジションにいると見ています。デジタル技術、ICT技術に知見のある人たちが官民学のさまざまな組織におり、彼らが集まっていろいろな「遊び」にチャレンジすることが重要です。

例えば、世界で今後40年間以上使われるような日本発のデジタル技術の開発に取り組む方法もあります。その一つが、40年間以上使えるOS、システムソフトウェアなどの「長寿命OS技術」です。WindowsやLinuxを40年間以上、挙動変更することなく利用できる仕組みや、カーネル、メールサーバー、Webサーバーなどのセキュリティパッチのメンテナンスの延命技術です。

また、40年間以上、誰でも簡単・確実にクラウドを構築・運営できる「クラウド技術」、40年間以上、誰でもルーターやファイアウォール、仮想ネットワークを簡単・確実に使える「ネットワーク技術」、40年間以上、生産し続けることが可能で挙動が安定した「汎用コンピュータ回路」、膨大な蓄積ドキュメントなど組織内知見に対して問い合わせが可能で機密性の高い「文書検索・AI技術」です。

そして、これらの技術、アーキテクチャを理解し、知識を整理・体系化する教科書群と人材育成環境を実現する「人材育成手段」が求められています。実は、世界の人たちが困っているのは、こうした当たり前のデジタル技術がどこにも存在しないことなのです。だからこそ、日本発のデジタル技術で国際競争力を高めていくことも可能です。

超正統派ICT技術開発の手法となる「けしからんいたずら」

最後に、「けしからんいたずら」の重要性についてお話しします。これは何かというと、あまり仕事とは関係ないように見える個人的な作業を会社・組織の設備を使ってやってしまおうということです。つまり、「けしからんいたずら」は「おもしろインチキ」の超正統派ICT技術開発手法と言えます。

米国の会社ではこうした手法がうまく作用しているので、いい人材が集まる。日本の会社も自由なシステムを作るときには「けしからんいたずら」が必要です。

例えば、UNIXも「けしからんいたずら」から生まれました。米国の電話会社AT&Tに勤めていたケン・トンプソン氏らの「インチキ社員たち」が社内のコンピュータで宇宙飛行ゲームを自作して遊んでいたところ、「けしからん」と考えた会社によってそのコンピュータが撤去されそうになりました。

彼らは会社でゲームができなくなるのは嫌なので、ゲームを他の小型コンピュータに移植しようとしたのです。当時はそんな開発ツールもOSもありません。そこで、自分たち専用の移植性のあるOSとプログラミング言語を一から「インチキ開発」したのです。これがUNIXとC言語の起源となりました。この経緯には諸説ありますが、最近、時間をかけて昔の文献を多数分析した結果、正しいとの確信があります。

今、私たちが取り組んでいるのは、超正統派コンピュータ&ネットワーク環境を日本中に普及させることです。そのためには日本の各伝統的組織（大企業、自治体、大学など）に特殊空間を作り、自由な試行錯誤を許容する。例えばIPAでは、持ち込み機材をインターネットに直結できるネットワークと自由実験の許容スペースを用意しています。

こうした試行錯誤環境を日本中の各所で実現することにより、日本型の伝統的組織を維持したまま、それらの組織の資源を活用して1万人の超正統派ICT人材の育成が可能になると見ています。多種多様な新技術を生み出すことで、かつての日本の産業界のようにICT分野においても世界トップクラスの技術と製品が作られるICT技術国が実現します。

そして、皆さんが自ら参加し、セキュリティ分野でも新しい技術・製品が生み出されることを期待しています。

人生はゲームだ!!
様々な挑戦を乗り越え得られた多くのもの

登壇者
株式会社SNK
代表取締役社長
松原 健二 氏

メインフレームやスーパーコンピュータの開発に携わる

「人生はゲームだ!!」をテーマに、人生で豊かな経験をする上で、私の体験が少しでもお役に立てればと思います。最初に私の略歴を紹介します。東京大学大学院情報工学を修了後、日立製作所に入社。米国マサチューセッツ工科大学経営大学院で学び、日本オラクルに入社しました。

その後、コーエー（現コーエーテクモゲームス）に入社し、2007年６月から代表取締役社長に就任。以降、シンガジャパン代表取締役社長、セガゲームス（現セガ）代表取締役社長を歴任し、2021年8月からSNK代表取締役社長を務めています。大学を出たときにはこのような人生を歩むとは思っていませんでしたが、さまざまなご縁や皆さんに助けていただきながら、気が付けばゲーム業界で4社の社長を務めていることになります。

まず、社会人としてスタートした日立製作所時代のお話しをします。日立ではミッションクリティカルなメインフレームやスーパーコンピュータの開発に携わり、スーパーコンピュータは1996年当時、世界最速を達成しています。

海外経験もしており、ヒューレット・パッカード（HP）社とのマイクロプ

ロセッサの共同開発や、スタンフォード大学で開催されていたマイクロプロセッサの学会にも参加しました。学会に参加して気が付いたのは、企業の人たちが交流していることです。集まってお互いに情報交換している姿は、私にとって画期的なことでした。

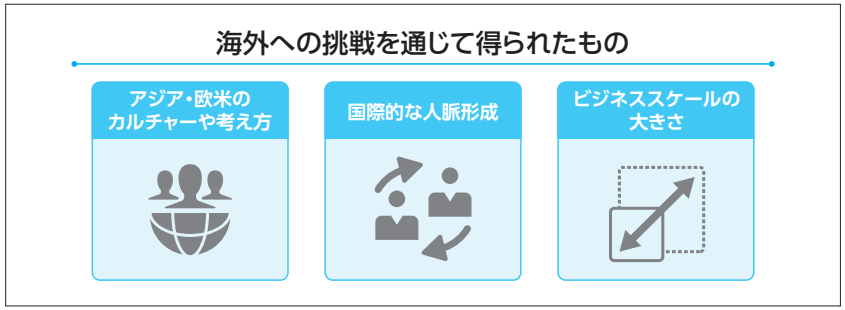
アメリカで生活しているうちにエンジニア業務では学ぶことが難しいマクロ・ミクロ経済学や会計学、マーケティング・統計学、人事・組織論といった「経営の基礎」を習得したいと思うようになり、1995年から97年までマサチューセッツ工科大学経営大学院で学びました。

海外への挑戦で得られたアジア・欧米のカルチャーや考え方の違い

そして、海外でチャレンジしたいと考え、お世話になった日立製作所には申し訳なかったのですが、外資系企業に転職することになりました。入社したのが日本オラクルです。選択のポイントは外資系企業での経験とリーディングカンパニーとしてのビジネスの作り方を学びたいと考えていたからです。

これまでのモノづくりのプロジェクト管理やマネージャーの経験を生かすことができます。また、オラクルはデータベースの分野でナンバーワンのシェアがある。顧客や市場を分析し、一歩先の未来で必要になる技術を自分たちの手で創造することをやってみたかったのです。

海外への挑戦を通じて得られたことは、アジアと欧米のカルチャー、文化



の違いです。HPにしても、オラクルにしても、日本企業と異なり、結論、進むべき方向性が先にあるのでコミュニケーションの取り方が効率的です。そして、国際的な人脈形成です。米国のビジネススクールには世界中の人たちが学びに来るので、さまざまな地域の人たちとつながりを持てたことがいい経験になりました。

米国オラクル本社での勤務を志望していたものの、私の力不足もあり、希望はかないませんでした。そこで、インターネットが注目され始めていたこともあり、関連する製品・サービスの仕事をしたいと考えていたときに知り合いの紹介で、「ゲーム業界」いう新しい分野へのチャレンジを決心したのです。

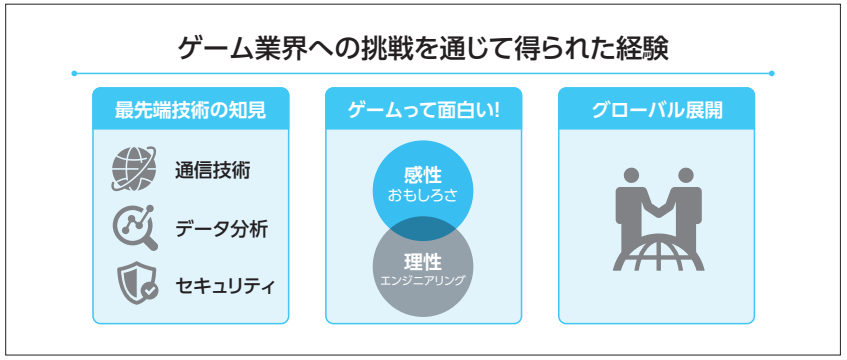
モノづくりの本質はハードもソフトも同じ

そして、2001年にオンラインゲームの事業責任者としてコーエーに入社しました。最初に戸惑ったのが、部下たちが使っている用語です。何を言っているのか分からない。ゲームの中身も分からない。そこで最初の数カ月はゲームを覚えるため、プレイに専念していました。

私がプロデュースしたタイトルの一つに「信長の野望 Online」があります。2003年のリリース以来、20年以上経った今もサービスを続けています。モノづくりの本質はハードでもソフトで同じであり、私が長くゲーム業界で仕事をしているのも、日本人に非常に向いていると感じたからです。

例えば、開発したゲームのバグを取り、きちんと動作するかどうか検証する。まさにゲーム開発は理性的なエンジニアリングそのものなのです。一方、売れるかどうかは感性的なおもしろさにかかっています。おもしろさを工学的に分析して開発、販売する。ゲームはもちろんプレイすることが楽しいわけですが、つくることも非常に楽しいと実感しています。

オンラインゲームの経験を生かし、独立してデータの収集・解析サービスを始めたいと考えるようになりました。コーエーを辞める決心をしていましたが、創業者から説得され、辞めるのを止めて「社長業」へのチャレンジを



決心することになったのです。ステークホルダーの皆さんと会社を代表してお話しする機会が増え、私自身の成長となりました。

また、会社のあるべき姿を明確化して従業員が一体となって目標に進む。そんなときに役立ったのが、顧客や市場を分析して未来の技術を創造するというオラクル時代の経験です。このほか、M&Aやタイトルの海外展開、ゲームの展示イベントなど、それまでの経験を生かしながらグローバルな規模でのビジネスが行えたことも大きなポイントです。

ゲーム業界への挑戦を通じて得られた経験はさまざまあります。例えば、通信技術やデータ分析、セキュリティなど最先端技術の知見です。ビデオゲームのビジュアルのリアルタイム処理には最先端のGPUが使われています。GPUというとAIで利用されていますが、高性能なGPUを搭載したマシンでゲームを楽しむ人は少なくありません。

日本のゲーム業界全体の開発技術を高め、世界に展開

人と人、会社と会社がつながる場についてお話しします。コーエーの社長就任後、CESA（一般社団法人コンピュータエンターテインメント協会）の理事になり、どのように日本のゲーム業界全体の開発技術を高め、世界に展開していくかを考えるようになりました。

開発者が出会い、研鑽する環境づくりに向け、コンピュータエンターテイメント開発者を対象としたカンファレンス「CEDEC（Computer Entertainment Developers Conference）」の改革に乗り出しました。横浜で開催されているCEDECの参加者はかつて1000名程度でしたが、現在は1万人弱、オンラインを含めると約15000人の開発者がカンファレンスに参加しています。ゲーム業界の中で会社の垣根を越えて開発者が出会い、交流し、研鑽し合う場を通じて業界の活性化、発展に貢献しています。

最後に、UNIXのコンピュータRPG「ローグ」についてお話しします。プレイするたびにマップやダンジョンが変化するローグライクをご存知の方もいると思います。私が大学の研究室にいたとき、先輩が使っているコンピュータの処理が終わるまでローグをやっていました。

この経験が私にとってゲームの原点になっています。今のようなグラフィック技術がない時代でも、遊び方のおもしろさ、ワクワク感は十分に実感できたのです。ゲームに登場するモンスターは、まさに私の人生の中で直面した苦労そのものであり、そのモンスターを倒すために挑戦し、乗り越えてきたことで今があると思います。

セキュリティコミュニティの入り方・歩き方・活かし方

登壇者
Elastic社
Senior Security Research Engineer
中島 明日香 氏

産業系国際会議のデビューを意気込んだものの失敗の連続

「セキュリティコミュニティの入り方・歩き方・活かし方」と題して、私自身の経験をお話しします。まず、自己紹介すると、大学卒業後、約10年間、NTT研究所で脆弱性発見・対策の研究を行い、2022年からElastic社でエンドポイントセキュリティの研究開発に従事しています。

また、セキュリティコミュニティ活動に力を入れ、女性セキュリティ技術者コミュニティ「CTF for GIRLS」の発起人として2023年度までの約10年間代表を務めたり、セキュリティ啓発活動として「サイバー攻撃」や「入門セキュリティコンテスト」の著書を発表したりしています。

セキュリティコミュニティ、特に海外のコミュニティをテーマにお話しする理由は、私が海外コミュニティに深く入り込んだ経験があるからです。例えば産業系の国際会議であるBlackHat USA/Europe/Asiaや学術会議だとAsia　CCSなどにも登壇しています。そうした活動が認められBlackHat USAやCODEBLUEなどの国際会議の委員を務めています。国際会議での活動が評価され、Bsides Singapore 2023やBlackHat Asia 2024などの基調講演を任せられるようになりました。

そもそも、セキュリティコミュニティについて関心を持つようになったのは、2015年、駆け出しの研究者だった頃、研究がある程度形になってきたため、産業系国際会議にデビューするぞと意気込んで投稿論文（CFP）に応募していたのです。ところが、不採択が続き、採択コメントが返ってこないので落ちる理由も分かりません。社内で産業系国際会議のノウハウを持つ人もいない状況でした。

海外との接点をつくるため著名エンジニアとの交流会に参加

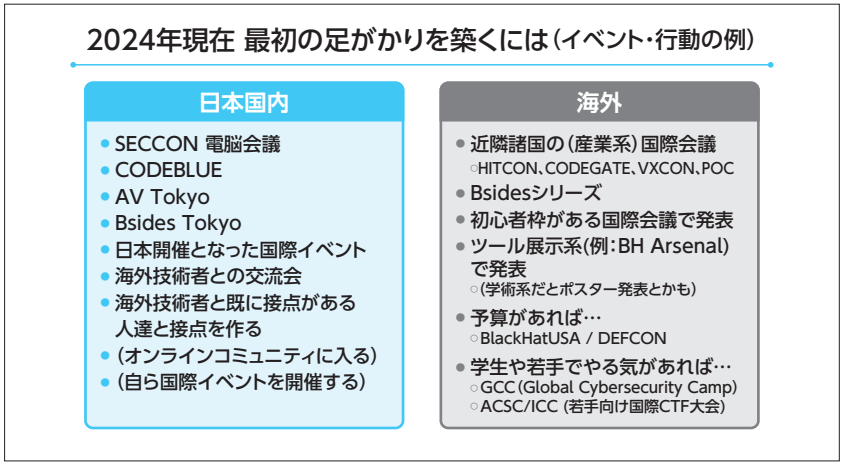
こうした状況を打開するため、それまでの行動パターンを変えることにしました。最初に行ったのは、産業系国際会議の情報を入手するため海外との接点を作ることでした。ちょうど、日本でSECCON CTF　2015決勝大会が開催され、米国や韓国、台湾など海外のCTFチームが来日しており、接点を作るため交流会に参加したり、観光ガイド役を引き受けたりしました。

そして、各国のCTFチームの方々と雑談する中で、私の研究の話になり、Positive Hack Daysという産業系国際会議への投稿を勧められたのです。その結果、投稿が採択され、国際会議にデビューすることができました。

また、海外の著名なエンジニアとの交流会にも積極的に参加するようにしました。例えば、米国のCTFチームだけでなくバイナリ差分解析ツールBinDiffの開発者であるHalvar Flake氏との交流会に参加。いつも持ち歩いているパソコンをカバンから取り出して私の研究をその場でプレゼンするなど、積極的に交流しました。

こうした接点づくりの結果、Halvar Flake氏から合宿形式の国際セミナーDagstuhl Seminarに招待され、そこで発表の機会を得ることができました。その国際セミナーに参加して分かったのですが、世界中から約40名の著名な技術者、研究者が招待されており、そうした方々との交流を通じて海外のセキュリティコミュニティに入り込むことができました。

最初の一歩を振り返ってみて、コミュニティの入り方のコツがわかってきました。まず、海外技術者との交流の機会がありそうなイベントに顔を出すことです。そして、発表後に質問に行くなど自分から積極的に声をかけてみるのが大事です。



また、若いうちは年長者にお願いしてネットワーキングを助けてもらう方法もあります。私の場合は、CODEBLUE創設者の篠田佳奈さんとご縁があり、サポートしていただきました。このほか、自分の研究、取り組みを英語で説明できるようにしておくことや、情報発信する側に回ると相手から声をかけてもらえる可能性があります。

2024年現在、国内ではSECCON電脳会議やCODEBLUEなど、アジアでは台湾のHITCONや韓国のCODEGATEなどのイベントがあり最初の一歩としてはお勧めです。イベントは男性が多く、女性は参加しにくいと思われる方もいるかもしれません。女性のセキュリティコミュニティとして、国内ではCTF for GIRLS、海外では台湾のHITCON GIRLS、米国のWomen in Security and Privacyなどがあります。

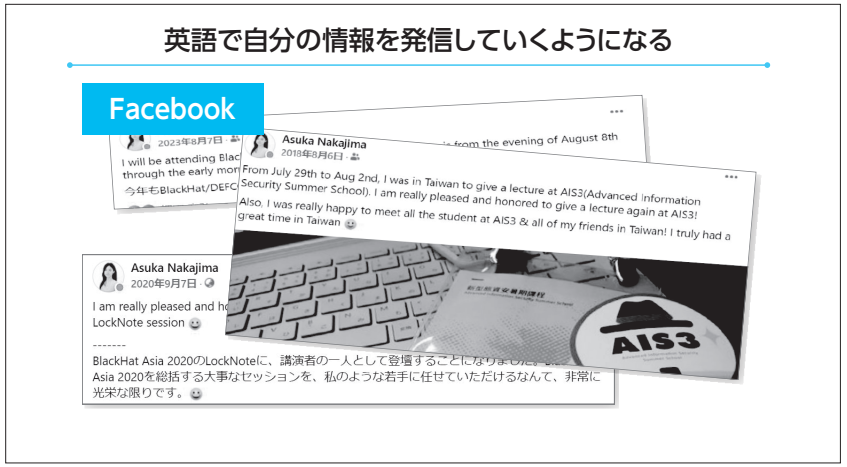
SNSやWebサイトなど英語で自分の情報を発信

海外との接点をつくり、コミュニティに入り込んだことで私自身の認知度が上がり、さまざまなチャンスが舞い込むようになってきました。例えば、台湾の高度人材育成プログラムAIS3にて招聘講師として招待されたり、会社でも米国のカーネギーメロン大学との共同研究の主導を任されたりしました。

海外イベントに呼ばれるようになり、ネットワーキング（歩き方）のコツを覚えていきました。私のことを覚えてもらうために、例えばお土産を持っていく、名刺を配る、自分の活動を宣伝する著書などを持っていく、研究のスライドをパソコンに入れ、機会があれば紹介する、一緒に食事をして仲良くなるといった努力をしたこともその一例です。

また、ネットワーキングするにあたり、FacebookやX（旧ツイッター）などのSNSやプロフィールのサイト、英文の履歴書を用意するなど、英語で自分の情報を発信するように心がけました。こうした活動の結果、海外のコミュニティにおいて私の実績や人となりが伝わり、BlackHat AsiaのReview Boardに推薦され、着任することになりました。2018年のことです。

ただ、注意が必要なのは、単にアピールすればいいというわけではありません。実力があってもアピールしなければ欲しい機会は得づらい、逆に自分の宣伝ばかりしていても実力は身に付きません。実力と宣伝力の両輪で回すことが重要です。



コミュニティに入り込むことでチャンスが増え、選択肢が広がる

私がコミュニティに入り込む際に大事にしているのは、自分が周囲に提供できる価値を常に意識することです。「提供できる価値があるスキルは自分には無い」とここで悩む方もいるかもしれないのですが、心配する必要はありません。例えば私は自分が日本人であることを活かしています。例えばBlackHat Asiaはアジアの会議なので、アジア人である私の意見は尊重されます。また、日本のホットなトピックを共有すると喜ばれたり、日本人の投稿を確認することもあります。カーネギーメロン大学との共同研究では、一般消費者向けにIoT機器を販売している日米の事業者を対象に、セキュリティパッチの公開日などを調査し、私は特に日本語のリリースノート分析に貢献しています。

日本で活動しているので、何も困っていない、私は無関係という方もいるかもしれません。しかし、海外のコミュニティに入り込むことで得られるものはさまざまあります。個人としては、いい機会をもらえるチャンスが増え、キャリアの選択肢を広げられます。日本で生活しながら海外企業で働くことも可能です。そして、世界の中で自分自身の相対的価値を知ることができます。

組織としては、注目され始めている技術や研究テーマなどのトレンドや、ルールをいち早く把握できます。その結果、共同研究やイベントの依頼が舞い込むなど、組織としてのチャンスも増えます。そして、トレンド/ルールを作る側になることで日本の国益にもなります。これらがセキュリティコミュニティの活かし方と言えます。

NPO情報セキュリティフォーラム 20年の軌跡と今後の展開

登壇者

特定非営利活動法人
NPO情報セキュリティフォーラム
理事・事務局長

植田 威

学校法人　岩崎学園
理事・専務執行役

啓発普及事業として情報セキュリティトピックセミナーなどを開催

情報セキュリティ大学院大学（IISEC）とNPO情報セキュリティフォーラム（ISEF）はいずれも岩崎学園が中心となって創設され、20周年を迎えました。情報セキュリティ大学院大学は人材育成と研究活動、NPO情報セキュリティフォーラムは啓発普及活動を担い、二つの組織が車の両輪のように活動してまいりました。

NPO情報セキュリティフォーラムの会員企業は13社・団体、ほかに個人会員が21名いらっしゃいます（2024年7月1日現在）。皆さん方の会費で運営され、講座数は年間200講座を超える状況です。職員は神奈川県内の小中学校などで出前講座を行い、好評です。啓発普及事業として、「情報セキュリティトピックセミナー」や「e-ネット安心講座」「ケータイ・ネット安全教室」「インターネット被害未然防止講座」を実施しています。

まず、「情報セキュリティトピックセミナー」は、情報セキュリティ大学院大学と連携したオンラインセミナーで、神奈川県、横浜市、神奈川県警察と共催し、サイバーセキュリティに関する普及啓発活動を集中的に実施するサイバーセキュリティ月間の時に対面講座を行っています。参加者はご年配

情報セキュリティトピックセミナー

の方も多く、どんな対策を講じたらいいのか分からないという声に対して、具体的な対策を交えながら講座を進めています。実績は5講座、受講者総数523名を数えています（2023年度）。

ネットやSNS、ケータイを安全・安心に利用する講座

啓発普及事業の「e-ネット安心講座」。保護者や教職員の皆さんから子どもたちをどう指導すれば分からないという悩みをよく耳にします。そこで、小学校や中学校、高校、専門学校、一部の大学に出向き、保護者、教職員などを対象とした子どものネットの安全・安心に関する出張講座です。

講座の内容は、ネット依存やサイバー犯罪から身を守る力、ネットトラブルとSNS、スマートフォンの情報セキュリティ対策、無料通話アプリの検証、家庭内のルールなどはその一例です。現実の世界で子どもとのコミュニ

ケータイ・ネット安全教室

ケーションを大切にし、自己肯定感の持てる家庭や地域、学校づくりを支援しています。毎年、同じ学校に出向いたり、入学式などに呼ばれたりすることもあり、実績は8講座、受講者総数は1,545名に上ります（2023年度）。

「ケータイ・ネット安全教室」は小学校、中学校、高校の児童・生徒を対象としたネットの安全・安心な利用に関する出張講座です。講座の内容は、サイバー犯罪の現状や、SNSでの不適切な発言による炎上、無料通話アプリの検証、スマートフォンの情報セキュリティ対策などです。

講座では、情報の受信時は情報の信頼性を考えることを伝えています。例えば、見た目だけで判断せず、複数の情報から判断する。確信が持てない時は信用しないといったことです。また、情報発信は慎重に行う。自分の情報のみならず、他人の情報も安易にネットに出さない、特定の人しか見ていないという安心感はダメといったことを伝えています。

実績は、99講座、受講者総数は13,769名に上ります（2023年度）。講座数は年間200講座を超えるとお話ししましたが、約半数がこの「ケータイ・ネッ

ト安全教室」になります。

会場にパソコンを持ち込み 被害の疑似体験のデモを実施

「インターネット被害未然防止講座」は神奈川県からの委託講座として実施しています。一般消費者向けに、ワンクリック請求の被害やネットショッピングのトラブルなどに遭わないための消費生活講座です。神奈川県内の学校や企業・団体に出向いて講座を実施するほか、県内の交通機関の駅前などに会場を借り、NPO情報セキュリティフォーラムの職員がパソコンを持ち込んで、被害の疑似体験のデモを行っています。疑似体験なので、年配者にもわかりやすく好評です。

講座の内容は、占いサイトなどを通じての個人情報の漏えいと迷惑メールに関するものや、パソコンのデスクトップから消えないワンクリック請求画面への対応、有料のメッセージ交換サービスへの誘導、ネットショッピングによる消費トラブル、無料を謳うオンラインゲームでもすべてが無料ではないこと、スマートフォンの情報セキュリティ対策、SNSで炎上トラブルに巻き込まれないためにどうすればいいかといった講座内容を用意しています。依頼元、講座時間に応じて内容を検討することも可能です。

実績は、学校出前講座が110講座、受講者13,140名、団体出前講座が28講座、受講者559名、参加者募集講座が16講座、受講者232名と多くの受講者に参加していただいております（2023年度）。

小学校のプログラミング教育の 事例をアンケート調査

NPO情報セキュリティフォーラムでは、調査・研究開発事業を行っています。小学校でプログラミング教育が行われていますが、学習指導要領に例示された内容を実施している学校は少なくありません。例えば小学校5年生の算数の場合、プログラミングを通して、正多角形の意味を基に正多角形を書くといったことです。

教員は他校でどのように授業でプログラミングを行っているのか分からないこともあります。そこで、「小学校における情報教育の現状調査」として、プログラミング教育の事例についてアンケート調査を実施しています。理科でどう使うの、国語でどう使えばいいのといった具体的な事例を集め、公表する事業を進めています。

また、教育事業では中小企業向けの「中小企業情報セキュリティ講座」を行っています。2023年度の実績は2講座、総受講者数は150名です。講師は情報セキュリティ大学院大学の卒業生にお願いしています。

このほか、教育事業として「児童福祉施設での小学生プログラミング教室」を行っています。児童福祉施設には子どもが使えるパソコンがないところもあります。しかし、学校ではプログラミングなどでパソコンを使うため、練習が必要です。

児童福祉施設にパソコンを持ち込んでプログラミングの練習をします。例えば、自分の好きなことわざをビジュアルプログラミングで動画を作ってみたり、夏休みの思い出を動画にする、水族館の魚を動画にしてみたりといった活動を続けています。

教育事業として神奈川県開催の「高校生ICT Conference 2024」の運営をお手伝いしています。今回のテーマは「今、高校生が考える生成AIとの付き合い方～誤情報・偽情報を超えた活用法を考える～」で、参加した高校生は熟議を重ねていました。

このほか、プログラムコンテンツのアーカイブ更新や、セミナーなどへ講師を派遣する相談支援事業、事業や活動報告をWebサイトに掲載する出版事業を行っています。NPO情報セキュリティフォーラムでは、保護者、教員対象のセミナー講師や、児童、生徒、学生対象のセミナー講師、中小企業の社員対象のセミナー講師を募集しています。ぜひ、活動への参画をお願いします。

IISEC情報セキュリティ人材育成ビジョン2024 これまでの20年とこれから

登壇者
情報セキュリティ大学院大学
学長
後藤 厚宏

情報セキュリティの人材育成の「輪」を広げる

情報セキュリティ大学院大学（IISEC）は2004年の開学以来、情報セキュリティの人材育成を行ってまいりました。「研究と実務融合による高度情報セキュリティ人材育成プログラム（ISSスクエア）」、「分野・地域を越えた実践的情報教育協働ネットワーク（enPiT）」、オンライン講座（JMOOC）、社会人向けのProSec、政策提言などを行うセキュアシステム研究所（SSL）などの活動を通じ、情報セキュリティ人材育成の「輪」を広げてきました。

IISECのカリキュラムの特徴は「360度」、つまり情報セキュリティにかかわる技術はもちろん、法制度や倫理まで全方位の教育を含み、倫理観を持って現実の課題解決を担う高度な専門技術者、実務家および将来の方向をリードする創造性に富んだ研究者を育成してきたことです。そして、2024年９月までに修士557名、博士53名の修了生を輩出し、産業界や官公庁での情報セキュリティを支える人材として活躍していることが、本学の一番の財産となっています。

産官学の各分野の関係者と協同で、セキュリティ人材育成の輪をつくる取り組みが、ISSスクエア、enPiT/SecCapです。本学において、ISSスクエア

では1年制の准参加を合わせると約300名、enPiTでは約250名が修了しています。また、ISSスクエア修了者に対して、オープンバッジ発行の取り組みを進めています。

企業の研修にも利用される初級講座やProSecコース

普及啓発、産学連携、政策への貢献の取り組みについてお話しします。情報セキュリティに関心持ってもらうための普及啓発活動として、オンライン講座JMOOCがあります。2015年度には新たに一般人、大学生、専門学校生向けの情報セキュリティ「超入門」講座、超入門をステップアップした情報セキュリティ「初級」講座を開講しました。

2016年からは有償の講座を始め、当初は内閣サイバーセキュリティセンター（NISC）の施策もあり主要官庁の情報セキュリティ担当者に受講していただきました。今は、企業の研修として受講し、企業内の資格審査として両講座を利用するケースもあります。

また、ProSecにはメインコースのほか、２～６日間程度のクイックコースを設けています。具体的には、セキュアシステム技術演習（基礎）クイックコース、CSIRT構築クイックコース、IoTセキュリティコース、グローバルリスク分析コース、デジタル製品セキュリティコースといったコースがあり、受講者数は年々増加しています。本学のコースは社内研修の代替としても利用されており、企業ニーズに対応できていると感じています。

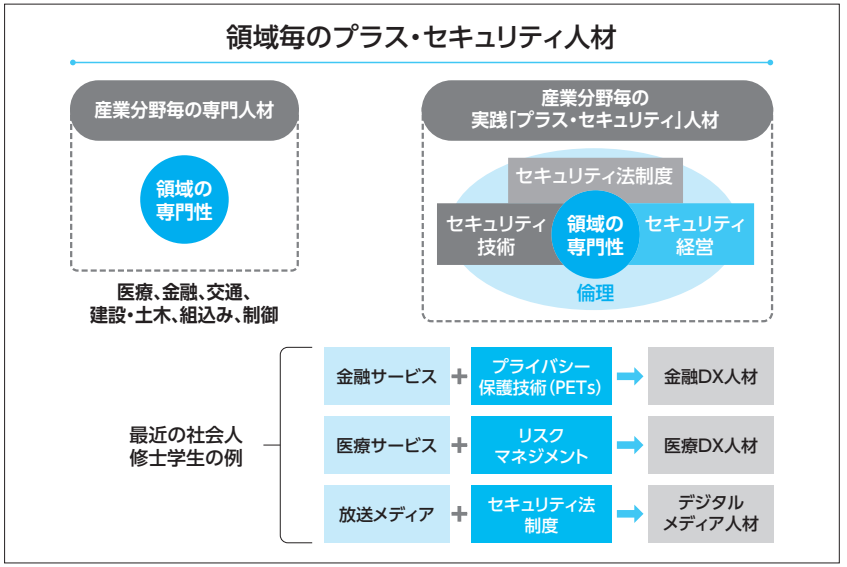
サイバーセキュリティ政策などに向けた活動では、セキュアシステム研究所によるインターネットと通信の秘密プロジェクトや、JNSA、ISEPAなどと連携したセキュリティ人材キャリア開発プロジェクトなどがあり、サイバーセキュリティ政策にも貢献しています。

こうした活動を支えていくためには、情報セキュリティ文化の醸成が大切です。我が国において情報セキュリティの進展に大きく貢献した個人を表彰する情報セキュリティ文化賞は2004年度の創設以来、既に20回、受賞者総数は108名、特別賞は６名を数え、情報セキュリティ文化の「輪」を広げることができました。

高度人材に加え、領域ごとのプラス・セキュリティ人材を育成

IISECにおける人材育成の取り組みを紹介します。開学以来、セキュリティ実践力のある実務者やセキュリティエキスパートを育成してきました。活躍中のIISECのOBOGの半数以上はこうしたエキスパートとしての道を歩んでいます。高度人材育成では、先端領域と産業分野の広がりに対応。情報セキュリティ（コア）をはじめ、IoT・AI・クラウド・ビッグデータ、製造・金融・社会インフラまで高度人材育成のテーマを広げているところです。

一方、近年、セキュリティ人材のニーズが多様化し、流通、製造、ICT、インフラ、金融、医療といった各分野において「プラス・セキュリティ」人材の育成が求められています。こうしたニーズに対応していることも本学の新たな特徴となっています。例えば、金融機関の人にプライバシー保護技術などを学んでもらい金融DX人材として育成する、医療機関の人にリスクマ



ネジメントなどを学んでもらい医療DX人材として育成する、放送メディアの人にセキュリティ法制度などを学んでもらいデジタルメディア人材として育成するなどがその一例です。

こうした先端領域・産業分野の拡大に対応し、プラス・セキュリティ人材へ対応するため、カリキュラムを日々アップデートしています。サイバーセキュリティとガバナンスコース、セキュリティ/リスクマネジメントコース、システムデザインコース、数理科学とAIコースの4コース体制を整え、情報セキュリティ心理学、実践的IoTセキュリティ、AIと機械学習、クリティカルシンキングとイノベーションなどを順次開講する一方、演習コースの拡充を通して、ISSスクエア、enPiTシリーズにおける実践力の向上を図るなど、新しい時代に適応できるIISECとして発展しています。

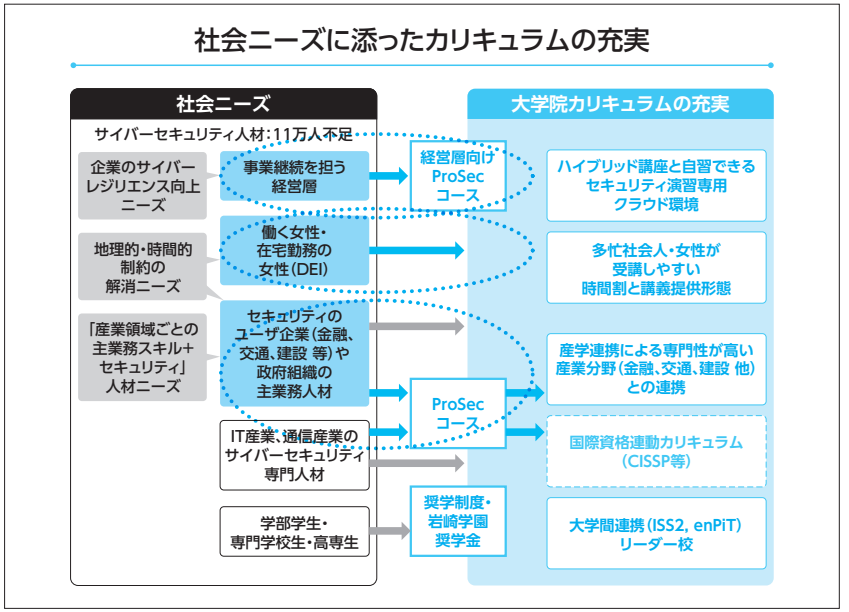
経営者向けや働く女性向けのカリキュラムを充実

今後の展開についてお話しすると、IISECを取り巻く状況、環境は多岐に渡っています。例えば、産業界では経営リスク（事業継続性）としてのサイバーセキュリティ対策や新産業分野（AI関連、半導体など）におけるセキュリティ人材不足、中小企業におけるセキュリティ人材不足、柔軟な雇用に対応したセキュリティ・リスキリングなどが挙げられます。

また政策面では、政府・自治体・防衛・警察におけるセキュリティ人材不足が顕著であり、政策ニーズとしては経済安全保障と研究開発、重要インフラのレジリエンス、グローバルな動向ではサプライチェーンのセキュリティ確保などがあります。

このような社会ニーズ、つまり、事業継続を担う経営層にどのようにしてセキュリティの重要性を伝えていくのか、働く女性や在宅勤務の女性が増える中でセキュリティを学ぶチャンスをどう提供していくか、さらに金融や交通、建設などの産業領域や政府組織のセキュリティ人材をどう育てるかといった要望に対し、カリキュラムの充実で応えていきます。

例えば、経営層向けサイバー訓練コースでは、経済産業省のサイバーセキュリティ経営ガイドラインや全米取締役協会のサイバーリスク・ハンドブックなどをベースに、リスクマネジメントや平時及び有事における経営者の役割、重大インシデント発生時における経営者の役割などを学んでいただきます。また、働く女性や在宅勤務の女性をはじめ多忙な社会人が学びやすいよう、毎週木曜日のカリキュラムをオンラインで行ったり、ProSec短期コースを充実させて社会人の大学院への導入パイプにするといった取り組みを進めています。



これらの取り組みに共通するのが産官学の連携・協業の拡大です。研究活動、セキュアシステム研究所、社会人向け短期コース、大学院カリキュラムの各分野で取り組みを進めていきます。そして、政策・法制度・技術が一体となったセキュリティ研究とリーダー育成に向けて貢献してまいります。

VUCA時代のキャリア構築とIISEC ―IISEC Alumni reunion 2024―

パネリスト

Amazon Web Services Japan
プロフェッショナルサービス本部
Senior Data Analytics Consultant　**吉濱 佐知子 氏**

ガートナージャパン
アソシエイトディレクター　**澤田 忍 氏**

NTTセキュリティ・ジャパン株式会社
セキュリティプリンシパル　**羽田 大樹 氏**

モデレーター

Japan Digital Design株式会社
Head of TDD 兼 VP of Security　**唐沢 勇輔 氏**

それぞれの思いを胸にIISECで学ぶ

唐沢：これからパネルディスカッションを始めたいと思います。まず、自己紹介をします。私はセキュリティ製品ベンダーで製品開発を担当した後、

唐沢 勇輔 氏

2019年 にJapan Digital Design株式会社に入社してセキュリティ部門を立ち上げ、2021年からエンジニア部門全体の責任者を務めています。

IISECに は2012年4月 か ら2014年3月までの2年間、私費で通い、当時の学長だった田中先生の研究室で大変お世話になりました。現在の学長である後藤先生の研究室が隣にあり、合宿へ一緒に参加させていただくなど、いい思い出です。そんなご縁もあり、昨年から同窓会長を務めています。

吉濱：私は大学卒業後、日本企業でSEとして仕事をしていました。そのとき、通信の標準化に関係する国際会議に参加して海外の企業に興味を持ち、米国IBMでユビキタスコンピューティングの研究を担当。その後、日本IBMに入り、情報セキュリティ関連の仕事をすることになりました。

それまでセキュリティ分野とは縁がなく、よく分かりませんでした。ただ、面白そうだと思い、本格的に勉強しようと開学したばかりのIISECに入学したのです。2期生でした。

日本IBMでセキュリティの研究を10年ほど行い、その後、産業系の研究開発を経て、現在はAmazon Web Services Japanにてコンサルタントとして仕事をしています。また、業務とは別に情報処理学会の理事やJTS CRDS特任フェローなどの活動を続けています。

澤田：私は大学院修了後、NTTデータに入り、システム開発を担当していました。専門的な知識、技術を身に付けたほうが働きやすいと考え、2006年社内公募でセキュリティ部門に手を挙げたのです。その翌年、上司の勧めもあり、企業派遣の形でIISECに入学しました。企業の方々と学生同士として話せたのはいい経験でした。

NTTデータで10年以上、セキュリティコンサルティングに従事した後、DXやAIなどの技術情報発信やマネジメントを担い、2023年6月からガートナージャパンでコンサルティングを行っています。例えば、グローバルなベンダーと一緒に脅威分析や疑似攻撃テストなどを進めています。

吉濱 佐知子 氏

今振り返ると、セキュリティをやっていて本当によかったと思います。ガイドラインや法規制などを専門家と一緒に考えていくことは自分の性格にも合っています。当時、情報セキュリティマネジメントシステムや、NISTのサイバーセキュリティフレームワークなどが策定される過程を知ることができたのは、今も貴重な経験となっています。

若い人たちにお伝えしたいのは、知りたいことがあれば年上の分かりそうな人に聞いた方が早いということです。IISECなどを活用して効率的に学ぶといいと思います。

羽田：私は今、NTTセキュリティ・ジャパンでセキュリティプリンシパルをつとめています。IISECには2011年、後藤先生が移ってこられた年に入学しました。当時、私を含め後藤研究室の学生は2名で、土曜日の午後、2名だけで後藤先生のゼミを受けるというぜいたくな環境で勉強したことを覚えています。

IISECに入学した2011年は、CTFがブームになり始めたころで、SECCONがスタートしたのもこの年です。当時、CTFチームで有名な「sutegoma2」にならってIISECで「mochigoma」を立ち上げたのも2011年でした。

その後、2015年に日本年金機構の重大インシデントが発生するなど、セキュリティが経営課題として認識されるようになってきたこともあり、博士課程にチャレンジしました。今は会社勤務のほか、IISECの客員講師や研究指導の助手をしています。

IISECでの経験やキャリアのエポックメイキングを語る

唐沢：ありがとうございます。経歴を紹介していただきましたが、IISECで経験したことを含め、皆さんにとってキャリアのエポックメイキング、人生の転機になった出来事があれば、聞かせていただけますか。

澤田：NTTデータでは、2006年からセキュリティ部門の担当になりましたが、入社以来、セキュリティ部門だった人たちに比べると、生え抜きのセキュリティ人材ではないような劣等感がありました。ただ、セキュリティを始めたのは遅かったものの、情報セキュリティ大学院大学にも通い、2016年になってシナジーが現れたといいますか、それまでの経験がすべて統合され、次のステップに進むことができました。寄り道であると感じることがあっても、いつか役に立つ可能性があり、私の場合は、入社後公共分野に配属されシステム開発やお客様対応を経験したことが、後々マネジメント的な視点で物事を判断できるとも評価され、2016年に課長に登用されました。

人からアドバイスを受けたり、これやってみたらと言われたりしたことを拒絶するのではなく、ちょっとやってみる。私自身、それで自信が付き、周囲の目も変わったと思います。これが私にとって最初の転機です。

羽田：技術者なので、技術力が大切なのは当然ですが、私の場合、仕事と趣味が一致しているといいますか、休日も我を忘れて解析に取り組むなど、技術に対して無我夢中になれることが周囲から評価されたのだと思います。

たまに転職エージェントの方とお話しする機会がありますが、お客様のところに出向いてプレゼンしたり、説明したりすることが得意だと伝えると、技術力がありながらそうした顧客対応の経験やマネージャーとしての経験を持つ人はあまりいないと言われました。そういった業務に取り組む機会や環境があり、積極的にチャレンジしたことが私にとってエポックメイキングとなりました。

澤田 忍 氏

唐沢：ありがとうございます。私も会社で採用の担当をしていて、そういう人材がなかなかいないと実感しています。次に吉濱さんのお話しを聞かせてください。

吉濱：私は数回、転職を経験していますが、羽田さんのように技術力で評価されるというより、ヤル気と勢い（笑）で評価されていると思います。AWSの採用プロセスは独特で、Amazon社員の行動原則、リーダーシッププリンシプルに沿った行動ができるかどうかで評価されます。

例えば主体性や責任感を持って仕事ができるか、新しいことを積極的に学べるかといったさまざまなポイントがあり、ソフトスキル的なところが評価される気がします。そして、私自身は論理的な思考力もあるし、技術力もそれなりにあると自負しています。ビジネス面とのバランスを取りながら考えられるところが評価されているのだと思います。

VUCA時代に活躍が期待されるセキュリティ人材

唐沢：パネルディスカッションのテーマは「VUCA時代のキャリア構築とIISEC」です。まさに将来の予測が困難な時代ですが、今後、活躍が期待されるセキュリティ人材のイメージが以前と変わっているのか、過去と比較してこれからどんな人材が求められるかなど、皆さんのお考えを聞かせていただけますか。

羽田：10年、20年前はセキュリティ技術者の立場はそれほど高くなかったと思います。ところが、2015年の日本年金機構のインシデントを契機に技術者がセキュリティをきちんと理解し、運用しなくてはいけないという考え方が浸透してきたように感じています。

さらに、近年は内製化の動きも加速しています。セキュリティは企業の生命線となり、社外の事業者に任せ切りにするのはリスクがあると考えるようになってきました。そこで、自前でSOC（セキュリティオペレーションセン

ター）を運営する、セキュリティ技術者を抱えるといった動きが出てくるようになりました。

羽田 大樹氏

私はSOCサービスを提供する事業者側なので、運用方法などを説明すると「自社でやるのは難しい」となり、外注するケースも少なくありません。とはいえ、企業がセキュリティを経営課題として捉えられるようになったことが大きな変化であり、セキュリティ人材がどんどん必要になる時代になると見ています。

唐沢：ありがとうございます。そうしますと、ユーザー企業に在籍するセキュリティエンジニアが増えそうということでしょうか？

羽田：はい。会社の業務を理解しながらセキュリティを担う人材が必要になってくると思います。

唐沢：確かに業務を理解した上でセキュリティの必要性を説くことが大事になると思います。この席にお二人のコンサルタントがいらっしゃる前で申し訳ありませんが、よくある話としてコンサルティング会社がユーザー企業に入ってセキュリティ規程を作ったりセキュリティシステムを導入したりしますが、その後の運用がユーザー企業任せになって必ずしもセキュリティが向上しないということがあると思います。セキュリティの内製化が進めば、こういった問題も解決するかもしれませんね。

生成AIにとって代わられる仕事と人間の価値を出せる仕事

吉濱：唐沢さんのご指摘のように、日本の事業会社の中にはITベンダーがシステムを開発し、自前のIT技術者の人材が不足しているという企業も少なくありません。これは日本独特の事情で、海外ではシステム開発にしても内製化が進んでいます。その結果、業務のデジタル化、DXなどが促進されるという面もあります。

ところが、日本企業の多くはベンダー任せでシステム構築を行い、ベンダーが去った後は状況がよく分からないというのは、大きな損をしているように思います。自社でIT技術者を抱え、社内に技術を任せられる人材を増やしていくことが、日本企業の課題になると思います。

また、近年の生成AIにより、大きな変化が生まれています。コンサルタントの仕事も5年後には生成AIにとって代わられる可能性がある。そういう時代に生き残る人材に何が求められるのか、よく考える必要があります。

唐沢：生成AI時代に必要な人材ですか。

吉濱：はい。これまで技術者が行っていたコードを書く、ドキュメントをつくるといった仕事もいずれ生成AIがとって代わる可能性があります。そうした中で、人間の価値を出せるところは、さまざまな社会課題に対して課題を深堀し、理解し、AIが回答を導き出せるところまでブレイクダウンするといった仕事が考えられます。

課題を抽象化して本質を明らかにしたり、こういう課題にはこういう技術、手法が使えたりするのではないかといった判断は人間の得意分野です。そういう人材を増やしていくことが生成AI時代で重要になると思います。

唐沢：吉濱さんのお話は大変、興味深いです。人間の仕事が生成AIにとって代わられる可能性について、お二人はどのようにお考えですか。

羽田：私の仕事は生成AIに代わってほしいと思いますが（笑）、AIが人間のようにかゆいところまで手が届くのはもう少し先になると見ています。ただ、生成AIがまだ難しいのは、人脈や経験に関係するところです。経験を生かしてどう判断を下すのか、どう責任を取るのかといったところまで生成ITにシフトするのには時間がかかると思います。

唐沢：確かにAIに責任は取れというのは難しいですね。澤田さんはいかがお考えですか。

澤田：セキュリティ分野も生成AIの影響を受けるようになるでしょう。私が所属するガートナーでは、AIの信頼性、リスク、セキュリティマネジメントを考えるAI TRiSMという概念を打ち出しています。いずれ、生成AIに

とって代わられるものはいろいろあると思いますが、まず人間が先手を打つことで、次の打ち手も考えられると見ています。

唐沢：ありがとうございます。生成AIの話で盛り上がりましたが、改めて将来の活躍が期待される人材像について、聞かせていただけますか。

澤田：私も以前は生涯、同じ会社で勤め上げるのは素晴らしいことだと思っていました。親世代もそうですし、今もそう考える人はいると思います。一方、仕事先を変えながらさまざまな経験をしている人は会社でコアな情報を得ていく。

そういう人が多くの情報量を持ちながら仕事をしていくのに対し、ずっと同じところで仕事をすることがリスクになる可能性もある。何がホットで、どうすれば自分の価値が上がるかを考え続けながら仕事をしたほうがいいと感じています。

唐沢：澤田さんがおっしゃるように、確かに動かないことがリスクになるというのは、その通りだと思います。

OBOGの立場からIISECに期待すること

唐沢：さて、IISEC開学20周年記念シンポジウムということで、OBOGの立場で今後のIISECはこうなってほしいというご意見があれば聞かせていただけますか。

吉濱：IISECで既に取り組まれているかもしれませんが、これから人材のリスキリングが重要になってきます。さまざまなタイプの方々に幅広く、あるいは深く掘り下げてセキュリティ教育に力を入れていただければと思います。

唐沢：さまざまなタイプの方々とおっしゃいましたが、とくにセキュリティ教育が重要になりそうな年代はありますか。

吉濱：とくにどの年代というより、すべての人にセキュリティはかかわってきます。高齢者の皆さんもセキュリティ教育は必要です。

澤田：後藤学長の講演でもお話しされていましたが、短期コースがもっと充実すればいいと思います。企業のセキュリティ部門にいる人は別としても、

自分でセキュリティの勉強をしたいと考える人にとって、いきなり2年制の大学院に入るのはハードルが高いこともあります。短期間学んでみる、自費でも賄えるコースが充実すれば、もっと勉強しやすくなると思います。

また、アジアやグローバルで日本が大好きという外国人も少なくありません。私もかつてオーストラリアに興味があり、何か研修先はないか調べたことがあります。同様に、日本の情報セキュリティに関心を持つ外国人向けに短期のコースを設けるなど、範囲を広げていく方法もあると考えています。

唐沢：ありがとうございます。羽田さんはいかがですか。

羽田：私にとって、IISECで学んだ経験と人脈がその後の人生の大きな財産になっています。何かにぶつかったとき、一緒に学んだ仲間たちも同じ課題、悩みを抱えている。自分だけが分からないのではなく、仲間も同じ課題を抱えていることが分かるだけでもありがたいですね。澤田さんが指摘されたグローバル化もそうですが、仲間、人脈をどんどん広げていけるよう多様性のあるIISECが望ましいと思います。

また、IISECでの貴重な経験として、後藤先生から様々な学会に投稿するよう言われたことを覚えています。締め切りに向けて必死に研究を進めたこ

とで、学会でいろいろなディスカッションを行い、フィードバックを受けられたことは、その後の貴重な財産となりました。

在学生、修了生のつながりも IISECの大きな魅力

唐沢：このパネルディスカッションにはIISECの在学生や、今後、進学を検討されている方もいらっしゃると思います。そうした社会人や学生の皆さんに対して、進学先としてのIISECの魅力を聞かせていただけますか。

澤田：修了して分かったのが、本当にIISECのような大学院大学は他にはなく、貴重なんだなということです。演習がたくさんあるとか、実際に社会人が来て学んでいるところってなかなかないですよね。私にとって想像以上に貴重な場でした。IISECで一緒に学んだ方々が業界の重鎮になられていく姿をみることができ、それが長く続く大学はそうはありません。進学先としてIISECを選択する価値は十分にあります。

また、若い方も年配の方も世代に関係なく、どんどん気軽に質問してつながっていくといいと思います。いろいろ質問することで教えていただけるし、チャンスが広がっていきます。今振り返ると、私ももっと質問すればよかったと考えています。

基調講演でコミュニティとしてのCODEBLUEなどのお話しをされていましたが、人のネットワークは信頼関係につながり、研究や仕事、実績も広がっていきます。そうした場の一つとしてIISECを利活用していけばいいのではないでしょうか。転職を経験した今だからこそ、本当にそう感じています。

羽田：IISECに入学希望の人にアドバイスすると、卒業後は必ずセキュリティ人材の色が付くということです。他のどの大学を卒業するよりも、周囲からはセキュリティ人材としてみなされます。IISECにいる2年間で勉強できることはセキュリティの膨大な分野の中でごく一部ですが、卒業後はセキュリティのことは何でも知っていると周囲から見られ、何でも聞かれることになります。

私自身も、セキュリティに詳しいですよねと言われますが、別にすべてを知っている必要はなく、知らないことでも自分が手探りで解決してきたという経験が自信になります。そのやり方を学べるのがIISECだと思います。ぜひ、何か問題を見つけ自分で解決したという経験を在学中に身に付けていただければと思います。

唐沢：ありがとうございます。羽田さんのおっしゃる通りですね。そうなりたいためにIISECに入学する方もいるかもしれません。ちなみに、セキュリティのことなら何でも聞かれるとお話しされましたが、私もIISECのシステムデザインコースで学んだだけにも関わらず、個人情報保護法に関係することをよく聞かれました。

サイバーセキュリティと個人情報保護法は外から見れば同じように思えるかもしれませんが、皆さんご存知のように専門領域としてそれぞれ異なることも多いです。質問者に対し、個人情報保護法上、どう答えたらいいのかよく分からない場合、改めて勉強し、自分なりの回答を導き出すようにしていました。

セキュリティの専門性を磨きながら 幅広い知識や見識を身につける

吉濱：T型人材という言葉があります。Tの文字の横軸が示す幅広い知識と、縦軸が示す特定の領域の専門性の両方を備えた人材の意味で使われますが、私はIISECには小さなTと大きなTがあると思っています。小さなTはセキュリティそのもので、IISECでそれぞれの研究領域で専門性を磨きながら、幅広くいろんな観点からセキュリティを学び、小さなTの横軸をしっかり育てる。

一方、大きなTの縦軸がセキュリティ全般だとすると、そこはIISECを修了した人の強みになります。それに加えて、例えばサプライチェーンのセキュリティなど、幅広い技術領域やビジネスをカバーする観点でセキュリティを考え、大きなTの横軸を強化していく。この大小のTの両方でセキュリティを考えていただくと良いのかなと思います。

唐沢：セキュリティのためのセキュリティ屋になるなということですね。今は減りましたが、かつてはセキュリティ原理主義を標榜する人もいましたね。

吉濱：そういう人がいてもいいとは思いますが、社会や企業で求められるセキュリティ人材で言えば、バランス感覚があったほうがいいのではないでしょうか。

技術面だけに偏らない インシデント報告のあり方

唐沢：さて、会場でパネルディスカッションをお聴きの皆さんに、ぜひパネラーの方に聞いてみたいことがあれば挙手をお願いできますか。

質問者：セキュリティ分野で感じるのは、インシデント発生時の分析が技術的な側面からの分析しか行われていないことです。日本年金機構のインシデントの話がありましたが、私の考えでは技術的な問題ではなく、セキュリティポリシー、あるいはガバナンスの問題だったように思います。パネラーの皆さんのお考えを聞かせてください。

唐沢：このシンポジウムでは、IISECとしてお答えする立場にないので、個人的な意見であることをご承知おきください。今のご質問で、インシデントの報告が技術面に偏っているのではないかというご意見でしたが、私もそう感じることはあります。

セキュリティインシデントの発生が増えるとともに、インシデントに対応するセキュリティベンターの数も多くなっています。ユーザー企業などがセキュリティインシデントを起した場合、その調査を外部の専門家に依頼することが一般的です。

説明責任を果たすためにも専門家に調査を依頼すべきだと思いますし、ユーザー企業が自らフォレンジック調査を実施するのは難しいという問題もあります。調査を依頼した外部のベンダーが提出する報告書は専門的、技術的になる傾向があるのは確かです。

ただ、ご指摘のようにユーザー企業側が報告書の内容をきちんと理解できる人がいて、ガバナンスの問題としてここがまずかったというような分析がなされるべきであることは間違いないと思います。

質問者：パネラーの皆さんは企業の現場におられるので、今おっしゃっていただいたようなことを考えながら検証していただきたいと思います。セキュリティ文化のお話しもありましたが、技術面だけに偏らないようなインシデント報告の仕組みづくりが今後、必要になると考えています。

VUCA時代のキャリア形成に 必要な人間力と技術力のバランス

唐沢：ありがとうございます。他に質問のある方はいらっしゃいますか。

質問者：シンポジウムのテーマはVUCA時代のキャリア構築ですが、私自身、技術力のベースラインをどのあたりにおけばいいのか考えているところです。私は仕事で業務委託先のリスク評価やクラウドサービスのリスク評価など、どちらかというと、人間力が求められる運用を行っています。一方、車の両輪ではありませんが、技術力も必要であると感じており、どのあたりを目指していけばいいのか、ご意見をお聞かせください。

唐沢：ご質問ありがとうございます。羽田さん回答をお願いできますか。

羽田：はい。組織として考えた場合、個人で何でもできる必要はないと思っています。技術を含め内容をしっかり理解できる人、その内容を基にビジネスの判断ができる人のそれぞれが能力を発揮すればいいのです。

ただ、内容をできるだけ理解する方がいいという考え方もあります。例えば、ベンダーから報告書が上がってきたときに、どこまで内容を理解できるか。書かれていることを理解するだけでなく、その裏にどんな手法があり、この報告書が出されたのかといったところまでイメージできるスキルがあればすばらしいと思います。

唐沢：ドラクエではありませんが、チームとしてうまく進めていくことと、T型人材の縦軸の深い専門性、そして今のお話しのようにベンダーの報告書を鵜呑みにするのではなく、技術的なバックグラウンドを理解した上でコミュニケーションを進めることの大切さを実感しました。他に質問される方はいらっしゃいますか。

質問者：IISECのOBです。今は事業会社に勤めていますが、ドラクエの攻撃側と回復側にたとえると、事業側と管理側があり、何か問題があった時に事業部門は攻め、管理部門は回復する立場です。管理側の地位をもっと高めるためのアイデアがあればお聞かせください。

澤田：難しい問題ですね。ただ、日本でもIT系の事業会社の管理部門の地位はそれほど低くはないと思いますが、コスト重視の業界ではオーバーヘッドと見られがちになる傾向があるかもしれません。

管理側の重要性を理解してもらうには、自社のセキュリティやDXなどを連動させながら、社内・社外に向けてメリットになるようなサービスを打ち出すなど、事業側にアピールするような方策が必要でしょう。

また、情報セキュリティ部門というと、問題発生時の「回復」が仕事と考える人も社内にいるかもしれません。SOCの運営など高度な技術力を持った人たちにしかできないことがあれば、社内から一目置かれる存在になると思います。

吉濱：インシデントが起きてから回復に着手するのでは多分、手遅れです。システムの企画・設計段階からセキュリティ対策を組み込むセキュリティ・バイ・デザインがセキュリティのあるべき姿です。そうなると企業のガバナンスの問題となるので、回復側ではなく、ガバナンス側になるのがいいのではないかと思います。

唐沢：質問された方々もご理解いただけたでしょうか。パネラーの皆さんもありがとうございます。これでIISECのOBOGによるパネルディスカッションを締めくくらせていただきます。

登壇者 プロフィール

2025年3月現在

後藤 厚宏（ごとう あつひろ）
情報セキュリティ大学院大学 学長・教授

1984年工博。NTT研究所にて並列・分散処理アーキテクチャ、インターネットセキュリティ技術、高信頼クラウドコンピューティグ技術等に従事。2007年よりNTT情報流通プラットフォーム研究所長等の後、2011年7月より本学教授。IEEE Computer Society理事、情報処理学会理事を歴任。2019年2月よりサイバーセキュリティ戦略本部員。2017年4月より本学学長。

関口 和一（せきぐち わいち）氏
株式会社MM総研 代表取締役所長

1982年一橋大学法学部卒、日本経済新聞社入社。88年フルブライト研究員として米ハーバード大学留学。英文日経キャップ、ワシントン支局特派員などを経て96年より2019年まで編集委員。2000年から15年間、論説委員として情報通信分野の社説を執筆。19年MM総研代表取締役所長就任。08年より国際大学GLOCOM客員教授を兼務。NHK国際放送コメンテーター、東京大学客員教授などを務めた。著書に『NTT 2030年世界戦略』『パソコン革命の旗手たち』など。

森 正弥（もり まさや）氏
博報堂DYホールディングス 執行役員、Chief AI Officer

外資系コンサルティング会社、インターネット企業、グローバルプロフェッショナルファームを経て現職。東北大学特任教授。東京大学 協創プラットフォーム開発顧問。日本ディープラーニング協会顧問。情報処理学会アドバイザリーボード、経済産業省技術開発プロジェクト評価委員、CIO育成委員会委員等を歴任。著書に『信頼できるAIへのアプローチ』（監訳）など。

盛合 志帆（もりあい しほ）氏
国立研究開発法人 情報通信研究機構 執行役 経営企画部長

1993年京都大学工学部卒業。NTT、ソニーなどの勤務を経て、2012年国立研究開発法人 情報通信研究機構入所。サイバーセキュリティ研究所長等を経て、2024年4月より現職。経済産業省平成23年度工業標準化事業表彰（国際標準化奨励者表彰）、平成26年度科学技術分野の文部科学大臣表彰（科学技術賞）、2021年第17回情報セキュリティ文化賞、令和5年度「情報通信月間推進協議会会長表彰（情報通信功績賞）など受賞。博士（工学）。

小山 覚（こやま さとる）氏
NTTコミュニケーションズ株式会社 情報セキュリティ部長
株式会社エヌ・エフ・ラボラトリーズ 代表取締役社長

1988年日本電信電話株式会社入社。1997年からOCNの立ち上げに参加し、セキュリティサービスの開発に従事する。1999年のグループ再編でNTTコミュニケーションズに所属。2015年10月より同社情報セキュリティ部長。2019年1月、株式会社エヌ・エフ・ラボラトリーズを設立し代表取締役社長に就任。NTTグループで10人しか認定されていない「NTTセキュリティマスター」。
警視庁 サイバー犯罪対策協議会副会長、ICT-ISAC 運営委員長などを歴任。2024年第20回情報セキュリティ文化賞受賞。警視庁 サイバー犯罪対策協議会副会長、ICT-ISAC 運営委員長などを歴任。2024年第20回情報セキュリティ文化賞受賞。

篠田 佳奈（しのだ かな）氏
株式会社BLUE 代表取締役
千葉工業大学変革センター 研究員

セキュリティエンジニアを経て（株）ネオテニーに参画、暗号・セキュリティの調査研究、新規事業開発支援に従事。その後情報セキュリティ国際会議Black Hat Japanの企画・運営を経験。米国サイバー犯罪対策APWGのアジア・リエゾンとして活動。内閣官房サイバー安全保障分野での対応能力向上に向けた有識者会議他、各省庁委員会に参加。世界トップクラスのサイバーセキュリティ国際会議 CODE BLUE発起人。2017年第13回情報セキュリティ文化賞受賞。

越前 功（えちぜん いさお）氏
国立情報学研究所 情報社会相関研究系 研究主幹・教授
国立情報学研究所 シンセティックメディア国際研究センター長

1997年東京工業大学大学院理工学研究科修士課程修了。日立製作所システム開発研究所を経て、現在、国立情報学研究所情報社会相関研究系研究主幹・教授、東京大学大学院情報理工学系研究科教授（併任）。情報セキュリティ、マルチメディア、プライバシー保護の研究に従事。IFIP日本代表，IFIP TC11日本代表。2014年・2005年情報処理学会論文賞、2016年第12回情報セキュリティ文化賞、2014年ドコモ・モバイル・サイエンス賞など受賞。博士（工学）（東京工業大学）。

山岡 裕明（やまおか ひろあき）氏
八雲法律事務所　弁護士（日本・カリフォルニア州）
情報処理安全確保支援士

University of California, Berkeley, School of Information修了（Master of Information and Cybersecurity（修士））。内閣サイバーセキュリティセンター（NISC）タスクフォース構成員（2019 ～ 20、21 ～ 22）。「サイバー安全保障分野での対応能力の向上に向けた有識者会議」構成員（2024）。2024年第20回情報セキュリティ文化賞受賞。

登 大遊（のぼり だいゆう）氏
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 サイバー技術研究室長
東日本電信電話株式会社（NTT東日本）特殊局 ビジネス開発本部　特殊局員
筑波大学 客員教授
ソフトイーサ株式会社 代表取締役

企業や自治体等で広く使われているテレワークシステムや、SoftEther VPN（暗号通信）技術等を開発しているソフトウェア技術者。世界中に数百万人のユーザーを有する。2004 年大学在学中にソフトイーサ株式会社を起業。2017年博士（工学）。2017年から筑波大学産学連携准教授、2022年から同大客員教授。2018年からIPA サイバー技術研究室長。2020年から NTT東日本本社特殊局員（いずれも現役）。2022年第18回情報セキュリティ文化賞受賞。

松原 健二（まつばら けんじ）氏
（株式会社SNK 代表取締役社長）

1986年東京大学大学院情報工学修士修了。日立製作所でメインフレームやスーパーコンピュータのCPU開発に従事。2001年にコーエー（現コーエーテクモ）入社、オンラインゲーム開発を担当。2007年に同社社長に就任。その後、Zynga Japan、セガゲームス（現セガ）の代表取締役社長を歴任。2021年、株式会社SNKの代表取締役社長に就任。ゲーム開発者の育成に長年取り組んでいる。

中島 明日香（なかじま あすか）氏
（Elastic Senior Security Research Engineer）

2013年に日本電信電話株式会社に入社し、約10年ソフトウェアセキュリティの研究開発に従事。2022年にElasticに入社。現在はエンドポイントセキュリティの研究開発を担当。女性セキュリティ技術者コミュニティ「CTF for GIRLS」の発起人。加えて、国際会議BlackHat USAおよびAsiaのReview Boardを務める。著書に『サイバー攻撃』（講談社）と『入門セキュリティコンテスト』（技術評論社）がある。

植田 威（うえだ たけし）
学校法人岩崎学園 理事・専務進行役
（兼）NPO情報セキュリティフォーラム 理事・事務局長

1982年岩崎学園奉職。行政と地域企業による情報化支援組織（かながわマルチメディア産業推進協議会、かながわIT産業推進協議会）の運営に参画。情報セキュリティ大学院大学の設立と同時期に、NPO情報セキュリティフォーラムの設立に参画。2021年11月神奈川県私立学校教育功労者表彰受賞、2024年6月神奈川県民功労者表彰受賞。

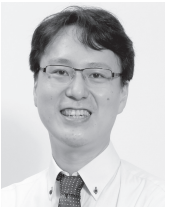
吉濱 佐知子（よしはま さちこ）氏
（Amazon Web Services Japan プロフェッショナルサービス本部 Senior Data Analytics Consultant）

2003年より日本IBM東京基礎研究所で情報セキュリティ関連、AIやブロックチェーン技術を活用した金融業界向けの研究開発等を担当。現在はAmazon Web Services Japanにて、データ基盤、生成AI活用、サステナビリティ、などの支援に従事。2021年より情報処理学会理事. ACMおよびIEEE会員．博士（情報学）。

澤田 忍（さわだ しのぶ）氏
（ガートナージャパン株式会社 アソシエイトディレクター）

2000年神戸大学大学院卒。同年に株式会社NTTデータに入社。システム開発を経験した後に、10年以上にわたりセキュリティコンサルティングに従事、さらには技術広報としてDX情報発信やブランディングの経験を有している。2023年6月より現職ガートナージャパンに転職し、セキュリティのみならずIT戦略全体に関わるコンサルティングを提供している。

羽田 大樹（はだ ひろき）氏
（NTTセキュリティ・ジャパン株式会社 セキュリティプリンシパル）



博士（情報学）。情報セキュリティ大学院大学客員講師。セキュリティ・キャンプ全国大会講師（2024等）、マルウェア対策研究人材育成ワークショップ 実行委員、Black Hat Arsenal（2017、2018、2023）。現在の業務はセキュリティ脅威分析業務、レッドチーム等。

唐沢 勇輔（からさわ ゆうすけ）氏
（Japan Digital Design株式会社 Head of TDD 兼 VP of Security）

セキュリティ製品ベンダーにて製品開発を担当したのち、2019 年 Japan Digital Design 株式会社に入社し、セキュリティチームを立ち上げ、2021年より現職。そのほか、日本ネットワークセキュリティ協会 社会活動部会副部会長、フィッシング対策協議会 副運営委員長。OpenID ファウンデーション・ジャパン理事、金融ISAC フィンテックセキュリティ WG副主査を務める。

おわりに

最後までお読みいただきありがとうございます。

本シリーズでご登壇いただいた皆様のお話しを振り返り、改めて、この20年で急速に「情報セキュリティ」という概念がカバーする領域の拡大と深化が進んできたこと、いわゆる専門人材のみならず広義のセキュリティ人材の活躍の場が広がりかつ生成されていることを実感いただけたのではないかと思います。

一方、2004年の本学（IISEC）開学・ISEF設立記念シンポジウムにおいて掲げたテーマ「セキュアな情報がもたらす価値創造と産業活性化」が示す、情報セキュリティが担う根源的な役割への期待はいっそう高まっているのではないでしょうか。

インターネットに代表される情報科学技術の発展によって、「情報」は21世紀の重要なキーワードの1つとなり、種々の情報が世界を行き交い、それらを使った多岐にわたるビジネスや活動が行われている一方、特定の企業・組織を狙った標的型攻撃や、フィッシング、情報の漏洩、国境を越えたサイバー攻撃など、様々な情報セキュリティ問題が社会を揺るがしており、国家的課題にもなっているこれらの解決なしに情報社会の発展は困難です。

実際に、個人情報保護法が成立し、ISEF（NPO情報セキュリティフォーラム）が設立された2003年、本学が開学した2004年以降を見ても、毎年のように情報／サイバーセキュリティに関する大きな事件・事故が発生し、攻撃の主体や方法についても、多様化、複雑化、高度化の一途をたどっています。設立・開学から10年後の2014年にはサイバーセキュリティ基本法が成立、翌2015年にはマイナンバー制度の導入、とリテラシーのあるなしに関わらず、着々と情報／サイバーセキュリティを意識せざるを得ない社会の仕組みが進行してきました。さらに、2020年初頭からの世界規模での新型コロナパンデミックを契機とした新しい生活様式・行動様式への転換、ロシアによるウクライナ侵攻を始めとした地政学的な要因による経済・文化・学術活動等へのリスクの増大など、予測不可能な事態への対応が求められる場面は少なくないことが予想され、わが国における情報／サイバーセキュリティの重要性がますます高まっていくことは確実といえます。

こうした状況を踏まえ、IISECとISEFはこれからも車の両輪として、大学院正規課程における教育・研究活動のさらなる充実による高度専門人材の輩出と企業・官公庁・教育機関等への短期的な教育・研修プログラムの提供、広く一般へのセキュリティ啓発に資するような情報発信など、全方位的な貢献への取り組みを継続し、情報セキュリティ文化の醸成に貢献していきたいと考えています。

最後になりますが、ISEFと本学が無事に20周年を迎えられたことにつきまして、たゆまぬ情熱をもって草創期をリードしてくださった、ISEF初代理事長の岡崎洋様、本学初代学長の辻井重男先生、初代副学長（第2代学長）の林紘一郎先生、初代情報セキュリティ研究科長（第3代学長）の田中英彦先生へ、改めて敬意と感謝を申し上げます。

また、この20年間、両組織に関わってくださった多くの方々―ISEF会員の皆様、各種教育・研修プログラムやセミナーをご利用いただいている皆様、本学のOB・OG・在学生の皆様とご家族の皆様、派遣元企業・官公庁、採用企業等各社の皆様、教育・研究活動でご協力いただいている連携企業・連携大学の皆様、アドバイザリーボードの皆様はじめ多くの皆様―にも、心からお礼を申し上げます。

さらに、お忙しい中、いつも母校の発展と後輩諸君のキャリアを気にかけてくださり、さまざまなアイディアで本学を盛り上げるために尽力いただいている同窓会幹事の皆様、皆様のご協力なしでは今回の一連の20周年事業は実現できませんでした。本当にありがとうございます。

そして、これからIISECへ入学される皆様、ISEFの活動に興味を持ってくださっている皆様へ。

ようこそ、お待ちしておりました。一緒に「明日の信頼」を創ってまいりましょう！

2025年3月吉日

情報セキュリティ大学院大学（IISEC）開学・
NPO情報セキュリティフォーラム（ISEF）設立20周年記念誌制作委員会

情報セキュリティ大学院大学

日本初の情報セキュリティに特化した独立大学院として、学校法人岩崎学園が2004年に開学。学部新卒者に加え、さまざまな職域から多くの意欲的な社会人学生が集う。情報セキュリティおよび関連分野において産業界・官公庁等で活躍中のコア人材を多数輩出。
https://www.iisec.ac.jp/

特定非営利活動法人 NPO情報セキュリティフォーラム

情報セキュリティに関する啓発普及・教育活動などを行う団体として2003年に設立。団体会員・個人会員のご協力により運営している。情報セキュリティに関する研修・講座を教育機関・行政機関・経済産業団体・企業等から多くの依頼をうけ実施。
https://www.isef.or.jp/

情報セキュリティ大学院大学（IISEC）開学20周年
NPO情報セキュリティフォーラム（ISEF）設立20周年
記念リレー講座・シンポジウム講演録

情報セキュリティ文化の醸成を目指して

2025年3月発行

発行　IISEC開学・ISEF設立20周年記念誌制作委員会
住所　神奈川県横浜市神奈川区鶴屋町2-17（法人本部）
TEL　045-311-7784（大学院代表）

企　画　IISEC開学・ISEF設立20周年記念誌制作委員会
編集協力　日経BPコンサルティング

本書の無断複写・複製（コピー等）は、著作権法上の例外を除き、禁じられています。

明日の信頼を創ろう。

情報セキュリティ大学院大学

INSTITUTE of INFORMATION SECURITY

NPO ISEF

Not-for-Profit Organization of Information Security Forum