HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.37

株式会社 日立システムズ

Human * IT

Hitachi Systems security Jounral VOL.37

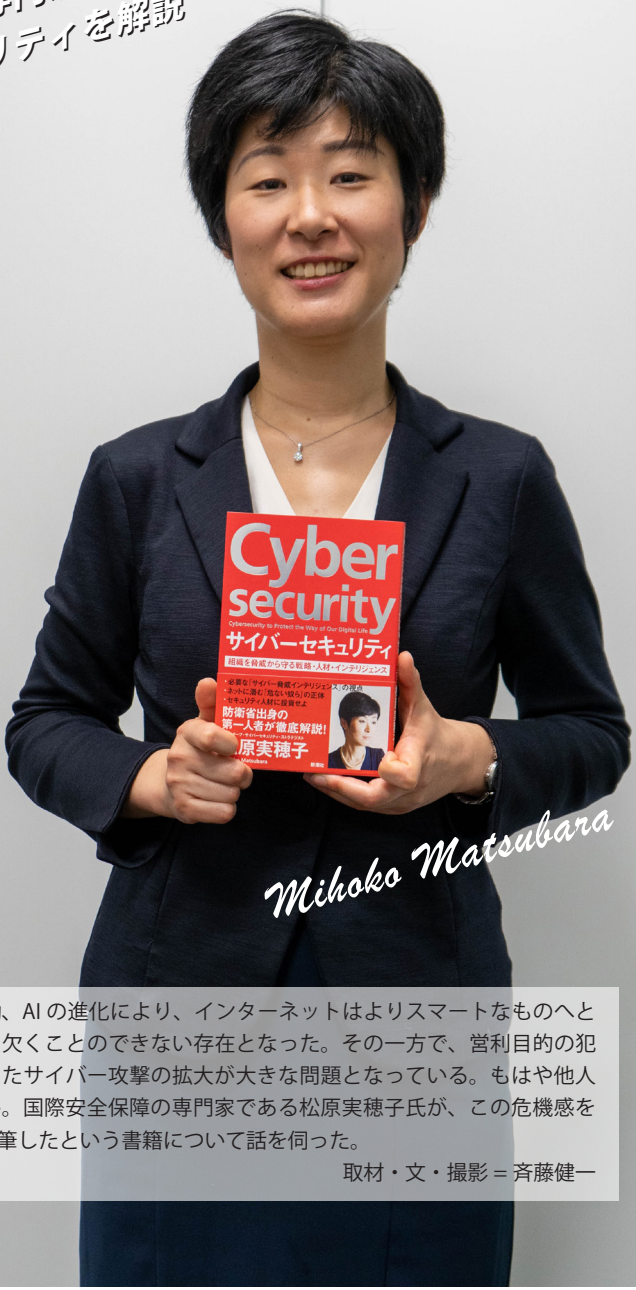
TABLE OF CONTENTS

●はじめに

本文書は、株式会社日立システムズ の公開資料です。バックナンバーは以下の Web サイトで確認できます。
https://www.hitachi-systems.com/report/specialist/index.html

国際安全保障の専門家が
サイバーセキュリティを解説

松原実穂子 インタビュー



IoT の普及、5G の本格稼働、AI の進化により、インターネットはよりスマートなものへと変わり、われわれの生活に欠くことのできない存在となった。その一方で、営利目的の犯罪や国家による諜報といったサイバー攻撃の拡大が大きな問題となっている。もはや他人事で済ますことはできない。国際安全保障の専門家である松原実穂子氏が、この危機感を一般の人へ伝えるために執筆したという書籍について話を伺った。

取材・文・撮影＝斉藤健一

さまざまな知見が詰まった サイバーセキュリティの解説書

斉藤（以下 S）：松原さんが先日ご上梓なさった『サイバーセキュリティ　組織を脅威から守る戦略・人材・インテリジェンス』（以下本書）を拝読しました。一般の方に向けて執筆されたとのことですが、サイバーセキュリティに詳しい業界の方でも読み応えがあると思いました。

松原（以下 M）：ありがとうございます。どういう点でそのように思われたのですか。

S 本書では世界各国で起きたサイバー攻撃の実例を紹介しています。Stuxnet を例にすると、技術系のニュースサイトなどでは、「Windows のぜい弱性を突いて…」「シーメンス社製の PLC の SCADA を標的に…」といった攻撃の手法に関する技術的な解説が中心です。一方、本書は一般向けであるため、技術的な説明を省いています。そのかわりに、「CIA とイスラエルはイランの技術者の中に協力者を得て…」や、「攻撃者は、施設のモニターには正常値を示し続けるようにするという手の込んだ仕掛けをした…」など、攻撃者がどうしてそのような行動を取ったのか、地政学的な背景を含めてドラマが描かれています。

M サイバーセキュリティや IT に詳しくない方でも、ストーリーが目の前に思い浮かぶよう、臨場感のある記述を心がけました。

S 執筆に際して、松原さんが攻撃者の人となりや生活ぶり、守る側の悩みや喜びについてつけ加えられているので、読み物としてのリアリティが増している印象です。事例を紹介する視点が異なるので、技術的な文書に接しがちなセキュリティ業界の方にとっても新鮮に感じられると思いました。

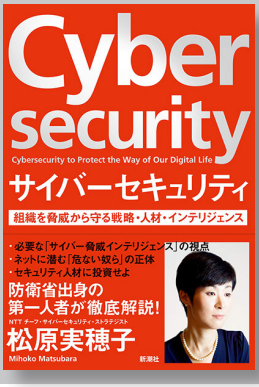
M そう言っていただけるととうれしいです。

S 他にも、エストニアが被害に遭ったサイバー攻撃事例では、松原さんの専門である国際安全保障や地政学の要素がふんだんに盛り込まれています。本書には 1980 年代中盤にネットワークを通じてアメリカの機密情報を盗んだソ連のスパイが登場しますが、これはクリフォード・ストールのベストセラー『カッコウはコンピュータにタマゴを産む』※1 でも扱われていました。私がこの本を読んだのは 20 年以上前の 1990 年代前半でしたので、非常に感慨深かったです。

M 1980 年代にもサイバー攻撃が行なわれており、攻撃側と防御側の熾烈な戦いが繰り広げられていた事実は、各国間のサイバー攻撃の現状と照らし合わせると、色々考えさせられます。

S 次に、本書を執筆された経緯を教えていただけますか。

M 2020 年のオリンピック・パラリンピック※2 の開催地が東京に決定された 2013 年以降、政府機関をはじめ、産業界においても、サイバーセキュリティに注力していこうという機運が高まってきました。サイバー攻撃やサイバーセキュリティに関する報道も増えてきています。その一方、そもそも「サイバー」とは何か、用語の意味を噛み砕いて説明する機会はあまりありません。カタカナ



サイバーセキュリティ
組織を脅威から守る戦略・人材・インテリジェンス

松原実穂子著　新潮社刊　1700 円（税別）
https://www.shinchosha.co.jp/book/353031/

サイバーセキュリティの概要をわかりやすく解説した 1 冊。世界各地で起きたサイバー攻撃の実例を挙げ、背後に潜む攻撃者たちの正体に迫る。サイバー攻撃の最前線で奮闘するセキュリティチームの仕事や、防御の指針となるサイバー脅威インテリジェンスにも触れている。一般向けのビジネス書であり、技術的な解説にはあえて踏み込んでいないが、著者の専門分野である国際安全保障や地政学などの知見が詰まっている。なお、版元の Web ページで、まえがきの一部を読むことができる。

※ 1 **『カッコウはコンピュータにタマゴを産む』（文庫上下巻）** http://www.soshisha.com/book_search/detail/1_2309.html
※ 2 **編注** 今回のインタビューが行われたのは 2020 年 2 月下旬で、この時点では東京オリンピック・パラリンピックの開催延期は決定されていなかった。

語やアルファベットの略字が多いため、とっつきにくく感じる人が多いでしょう。ITがこれだけ生活やビジネス活動に浸透している以上、サイバーセキュリティも身近になっていくべきなのに、実際は多くの人にとってわかりにくい存在になっています。しかし、一般の方々がITを使う以上、皆さんの理解と支援を得られなければ、サイバーセキュリティを生活やビジネスで確保できません。そこで、一般の人向けのわかりやすい本を書こうと決意しました。

S 松原さんの方から出版社に企画を持ち込まれたのですか。

M はい。最終的に、新潮社から出版していただけることとなりました。

S それは積極的ですね。

人間ドラマにフォーカス 攻撃側・防御側それぞれを顔の見える存在に

S 執筆ではどのような点で苦労されましたか。

M 一般読者に興味を持っていただくため、新潮社の編集者の方の助言を得つつ、工夫しました。

S 例えば、どのような工夫をされましたか。

M「サイバー攻撃の技術的な詳細についての記述を読むのはハードルが高い」とおっしゃる一般読者が多いでしょう。一方、お金の使い方や教育など生活に密着した要素であれば、誰にとっても身近に考えられます。攻撃者が稼いだお金をどう使っているのか、何を考えていたのか、一般向けの記事で説明しているものはほとんどありません。ですから、そうした人間ドラマを描けば、読者に興味を持ってもらえやすいと考えたのです。

S 確かに。本書では、高級車を何台も購入するなど豪勢な暮らしぶりを自慢げにSNSに投稿していた攻撃者が登場していましたね。

M 攻撃者を顔の見える存在にした方が、「戦わなくてはならない」という気持ちに読者はなりやすいでしょう。防御側も同様で、どのようなバックグラウンドを持った人たちがどういう態勢で日々サイバー攻撃と戦ってくれているのかを具体的に紹介しました。読者に「応援したい」という気持ちが芽生えて欲しいと願っています。

S 本書では、サイバー攻撃の最前線で戦う防御側の人たちを「ヒーロー」と呼んでいます。これも今おっしゃったことの現れですね。

M はい。攻撃者がどの国の政府機関に所属しているかを説明した本は、これまでも出ています。しかし、サイバーセキュリティ人材が日々どのような業務をしているのか、ご存知の一般人の方はほとんどいらっしゃらないでしょう。コンピューターに向かってひたすらキーボードを叩いているイメージがあったとしても、そこでどんなことが起きているかまではわかりません。IT化の進んだ私たちのビジネス活動を守り、下支えしてくれる縁の下の力持ちである彼らにスポットライトを当て、読者の方に応援していただきたいと考えたのです。

S なるほど。

M 本書でもサイバーセキュリティ人材のストレスについて触れましたが、これは海外で大きな問題になっています。機微な仕事内容のため社外に悩みを相談できる人が見つかりにくい、長時間労働である、会社や社員、顧客を守るための業務を遂行しても感謝されない、などの理由で燃え尽きてしまう人が増えているそうです。サイバー攻撃が

●松原実穂子（まつばら・みほこ）

早稲田大学卒業後、防衛省で9年間勤務。フルブライト奨学金を得て米ジョンズ・ホプキンス大学高等国際問題研究大学院（SAIS）に留学し、国際経済・国際関係の修士号取得。その後、アメリカのシンクタンク研究員などを経て、現在はNTTのチーフ・サイバーセキュリティ・ストラテジストとしてサイバーセキュリティに関する情報発信と提言に努める。著書に『サイバーセキュリティ　組織を脅威から守る戦略・人材・インテリジェンス』（新潮社）。現在、東洋経済オンラインにて連載中（https://toyokeizai.net/）。

増加する中、彼らの負荷が増大しています。

S 本書では疲弊するサイバーセキュリティの現場の例として、2019 年の RSA カンファレンスでの講演が取り上げられていました。また、最近では、最高情報セキュリティオフィサーである CISO (Chief Information Security Officer) の在職期間や燃え尽き症候群に関するニュースも報じられていました※ 3。

M CISO はまだ 25 年しか歴史がありません。CISO が最初に誕生したアメリカですら、CISO が組織でどのような役割を担うべきか議論の最中です。アメリカでは CISO は社外から雇われることが多く、新規で入った分、組織の中で事業への貢献と IT 化の推進、サイバーセキュリティの確保をバランスを取りながら短期間で達成するのは困難です。巧妙なサイバー攻撃が増えているため、会社を守るプレッシャーも大きく、平均在職期間が 2 年程度と短くなるのだと思います。

S 2 年ほど前、BlackHat USA のスピーチの概要を調べていた時に、講演でメンタルヘルスをテーマにしたものが増えたように感じました。こういったことも関連しているのかもしれませんね。

M 今年の RSA カンファレンスでも、メンタルヘルスについての講演が行なわれます。アメリカではそれだけ注目されているのだと思います。ビジネスがグローバル化する中、日本でも知っておくべきだと思います。

1 本の論文がきっかけで サイバーセキュリティの世界へ

S 本書を読んで松原さんのバックグラウンドに興味を持ちました。略歴を拝見すると、大学卒業後、防衛省に勤務されています。志望の理由を教えていただけますか。

M 大学生時代、横田めぐみさんをはじめ北朝鮮による日本人拉致被害者の問題や、北朝鮮の不審船が日本海で発見されるなどのニュースが報じられました。そこで、日本の安全保障に貢献できる仕事に就きたいと考えたのが主な理由です。当時は省ではなく防衛庁でした。最初、防衛施設庁で沖縄の米軍基地の返還・縮小に関する業務を担当しました。

S その後、奨学金を得て、米ジョンズ・ホプキンス大学高等国際問題研究大学院に留学されました。どのような勉強をされたのでしょうか。

M 国際安全保障に今後より貢献するには、国際的な環境で専門的に勉強する必要があると思い、仕事を辞めて留学しました。この時が大学院で学ぶ最後の機会になるかもしれないと考え、安全保障を学ぶのに最善の環境を選ぼうと決めたのです。留学に際して 2 つの目標を立てました。

S どのような目標だったのですか。

M 1 つは、勉強の成果を形に残すため、2 年の在学中に署名記事を出そうと決意しました。政治の中心地であるワシントン DC には、政府機関、大使館、国際機関、シンクタンクが集まっています。わざわざ留学する以上、 2 つ目の目標としてさまざまな国の人たちと友好を深め、周りから得られるものはすべて吸収しようと考えました。

S 署名記事は出せたのですか。

M はい。私が留学したのは 2009 年～ 2011 年でした。2010 年 1 月、ヒラリー・クリントン国務長官が中国からのサイバー攻撃に対して、名指しで非難し、アメリカの一般紙でもサイバー攻撃やサイバーセキュリティについて報じられるようになったのです。

S Google の中国撤退が取り沙汰されたのもこの頃でしたね。

M ある時、同級生のアメリカ人女性があわてた様子で私の所にやってきました。彼女は国際政治や安全保障に特化したジャーナルの編集者で、アジアのサイバーセキュリティについて記事を書いてくれる人を探していると言うのです。千載一遇のチャンスと思い、手を挙げました。但し、学業で手一杯、睡眠と食事の時間を削っての生活だったため、それに加えての執筆は死ぬ思いでしたが。

S それは大変でしたね。

M 同級生の彼女は優秀かつ親切で、執筆を手伝ってくれただけでなく、署名入りで記事を出させてくれたのです。ワシントン DC でサイバーセキュリティへの関心が高まる中、この執筆が後の就職

※ 3 **CISO むしばむストレスや燃え尽き症候群 -- 平均在職期間はわずか 26 カ月** https://japan.zdnet.com/article/35149411/

活動に役立ちました。大学院卒業後、アメリカのシンクタンクで日米間のサイバーセキュリティ協力について研究を続け、サイバーセキュリティについてさらに執筆を続けられたのです。帰国後、日立システムズでサイバー脅威インテリジェンスの仕事に携わりました。日本国内外の専門家と一緒に仕事をし、民間企業の視点も初めて実地で学べ、本当に貴重な経験を頂いたと感謝しています。

S 人生の転機はどこにあるかわかりませんね。もう 1 つの目標である交友関係はいかがでしたか。

M 多くの同級生や同窓生とつながりを持てました。留学から 9 年経ちましたが、今でも、友人宅に泊めてもらうことがあります。国際関係を専門とする大学院だったため、友人たちは世界中に散らばっています。本書の執筆で助けてくれた友人たちもいます。

S 現在は NTT でチーフ・サイバーセキュリティ・ストラテジストとして活躍されています。NTT ではどのようなお仕事をされているのでしょうか。

M サイバーセキュリティの分野で日本や NTT がどのようなことを行なっているのか、対外的に発信する仕事をしています。社会一般に対してサイバーセキュリティの知見を共有するための専属チームを営利活動とは切り離した形で設けているのは、日本でおそらく NTT だけです。2014 年に発足し、国内外で活動しています。

S 日本国内と国外では、それぞれどのような活動をされているのですか。

M 日本国内では経営層や一般の方々に向けて、講演・セミナーや書籍・記事の執筆を通じて、サイバー攻撃の現状とサイバーセキュリティの基本についてお伝えしています。一方、海外で力を入れているのは、政府やシンクタンク、企業、業界団体の方々に向けて日本の産業界や NTT の取り組みなどについて説明し、信頼の輪を少しずつ広げる活動です。

今こそ必要とされる サイバー脅威インテリジェンスの視点

S 本書の中で強く印象に残っているのは、第 4 章「今こそ役立つサイバー脅威インテリジェンス」でした。日本のインテリジェンス体制の不十分さや、それがもたらす外交や国際安全保障上の弊害、サイバー脅威インテリジェンス人材育成の必要性が説かれています。特にハッとさせられた箇所を引用します。松原さん自身、外国の軍人から「『憲法 9 条があるから仕方ない』と思うのは日本人だけだ。海外では日本よりずっと小国でもインテリジェンスに投資しているのに、世界第三位の経済大国である日本がなぜインテリジェンスに予算を割かないのか理解できない」と言われたそうですね。これは日本人にはなかなか気づけないことだと思いました。本書を通じて日本の状況を一般の読者へと伝えようとする松原さんの強い意志を感じました。

M インテリジェンスとは、断片情報を収集し、分析を加え、意思決定に役立てるものです。本書でも触れていますが、国によってはサイバー攻撃を情報機関が行なっています。逆に、防御を担う人材の育成も情報機関が担う国もあります。世界のサイバー攻撃の実態を理解するには、情報機関の役割を含め、インテリジェンスの理解が不可欠です。そのため、本書でインテリジェンスについて大きく扱いました。

S ベンダーによって、サイバー脅威インテリジェンスの定義が異なるように思います。例えば、国家の支援を受けた攻撃者グループの動向を調査したレポートも、アンチウイルスをはじめとしたエンドポイント・セキュリティ製品のシグネチャーもサイバー脅威インテリジェンスと呼ばれます。ユーザー側はどう捉えればよいでしょうか。

M さまざまなサイバー脅威インテリジェンスサービスがあり、ユーザー企業は、自組織が解決すべき問題をまず理解しなければなりません。例えば、海外での事業展開を考えている企業があるとします。この企業は技術情報も必要でしょうが、社長が交渉のため海外出張に行なった時のサイバーセキュリティ対策はどうするか、展開先の国のサイバーセキュリティや IT に関する規制はどうなっているか、など経営判断の助けになる情報も必要なはずです。

S そのとおりですね。

M 組織は、サイバー攻撃だけでなく、新型コロナウイルスの感染拡大、貿易摩擦、為替レートの変動、台風や地震といった自然災害など数多くのリスクに晒されています。限りある予算をどう分配してビジネスリスクを管理するか判断する上で必要なのが、インテリジェンスなのです。

S 確かに。

M 今の社会には IT が不可欠ですから、サイバー攻撃は必ずあるリスクです。リスクを見える化しなければ、対処のしようもありません。だからこそ、サイバー脅威インテリジェンスでリスクを見える化し、判断材料を得る必要があります。

S まずは、自組織のサイバーセキュリティ対策について理解しておく必要があるということですね。

M サイバー脅威インテリジェンスは、意思決定とその後の行動に役立ててこそ意味があります。そのためには、自組織内にサイバーセキュリティチームが必要です。

S 最後の質問です。今後の活動で、目標や抱負などはありますか。

M 現在、NTT のチーフ・サイバーセキュリティ・ストラテジストとして、より多くの方にサイバーセキュリティについて知って頂くための活動をしています。執筆を含め、日本語での一般向けの発信にもっと力を注いでいくつもりです。また、日本は今、アメリカでもない中国でもない、それ以外の国の声として非常に注目されています。ですから、英語でも日本の優れた取り組みを発信し、日本の知名度を上げ、国際協力が拡大するよう微力ながら貢献していきたいです。

S 本日はどうもありがとうございました。

次世代リーダーたちの国境を越えたコミュニティ作り

GCC Tokyo
Global Cybersecurity Camp レポート

取材・文・撮影＝斉藤健一

2020 年 2 月 10 日～ 14 日、千葉県船橋市のセミナーハウス クロス・ウェーブ船橋にて、GCC Tokyo - Global Cybersecurity Camp（ 以 下 GCC）が開催された※ 1。2019 年、韓国・ソウルでの開催に続く 2 回目となる。主催は一般社団法人セキュリティ・キャンプ協議会。「国籍・人種を超えた専門知識のあるグローバル人材の育成」と「国境を超えた友情とゆるやかなコミュニティの形成」を目的としたトレーニングキャンプで、日本を含む 7 ヵ国・地域（後述）から学生を中心に 29 名の若者が集まった。

新型コロナウイルス感染拡大という逆風の中での開催

GCC 開催の 2 月初旬を振り返ると、新型コロナウイルス感染拡大のニュースはすでに世間を賑わせていた。だが、全国小中高の一斉休校や大型イベントの自粛要請などはまだ行なわれておらず、この原稿を執筆している 3 月下旬と比較すれば、状況はさほど深刻ではなかったといえる。仮にスケジュールが数週間ほど後だったとしたら、開催は困難だったに違いない。

GCC 初日に行なわれたトレーニングの様子。実践的にインシデントレスポンスを学ぶ

参加は各国の判断に委ねられており、第 1 回のホスト国である韓国は参加を見送った。GCC 開催にあたっては、参加学生の体温測定および問診の実施、教室内の机や備品のアルコール除菌を徹底するなど、主催者による細心の注意が払われた。

国際連携の輪は 4 から 8 ヵ国・地域へと拡大

そもそも、サイバー攻撃はボーダーレスであることから、防御側も国境を越えて協力・連携する必要がある。若手技術者が国境や個別の利害を超えて交流し、さまざまな課題に取り組むためのきっかけとしたい。これが GCC 設立に携わった主催者の共通の想いだという。連携の輪は日本・韓国・台湾・シンガポールの 4 ヵ国・地域から始まり、2 回目となる今回は、オーストラリア・マレーシア・タイ・ベトナムの 4 ヵ国が加わることとなった。前述のとおり、今回のキャンプには韓国の参加はかなわなかったが、主催者によれば開催期間中にビデオ会議を通じて韓国参加者とも交流できる時間を設ける予定だという。

参加人数および運営組織は次頁にある表 1 のとおり。参加者には複数のティーンエイジャーが含まれている。ちなみに最年少は 17 歳とのこと。また、各運営組織は、ボランティア主導のコミュニティや教育機関、さらには政府機関が主導する

※ 1 **GCC Tokyo - Global Cybersecurity Camp** https://www.security-camp.or.jp/event/gcc_tokyo.html

表 1 各国の運営組織と参加人数

国・地域	組織名 URL	概要	学生の参加人数
日本	**一般社団法人セキュリティ・キャンプ協議会** https://www.security-camp.or.jp/	次代を担う情報セキュリティ人材を発掘・育成する「セキュリティ・キャンプ」を実施してきた。2018 年より一般社団法人として活動している。	6
オーストラリア	**UQ Cyber Security** https://www.itee.uq.edu.au/research/cyber-security/	クイーンズランド大学内に併設された情報技術・電気工学に特化した教育機関。グローバルなサイバーセキュリティの課題に対処。次世代リーダーの育成している。	4
マレーシア	**NanoSec** https://nanosec.asia/	アジア太平洋地域、とりわけマレーシアに焦点を当てた情報セキュリティ技術の国際会議。国内のセキュリティ専門家とコミュニティのボランディアメンバーによって運営されている。	2
シンガポール	**Division Zero(Div0)** https://www.div0.sg/	ボランティア主導によるオープンなサイバーセキュリティコミュニティ。イベントなどを企画するなどして、コミュニティに貢献できるプラットフォームを提供している。	3
タイ	**タイ国立電子コンピューター技術研究センター（NECTEC）** https://www.nectec.or.th/en/	タイ科学技術省管轄の政府機関。エレクトロニクスとコンピュータ技術の研究開発支援と促進を行なうとともに、研究者コミュニティと産業界との連携にも注力している。	5
台湾	**高度情報セキュリティサマースクール（AIS3）** https://ais3.org/	台湾教育部が主催する情報セキュリティ人材育成プログラム。2015 年より開始された。業界での実務経験を持つ専門家や教育機関の研究者などが講師を務める。	5
ベトナム	**VNSecurity** https://www.vnsecurity.net/	1998 年に設立されたセキュリティコミュニティ。さまざまなスキルを持つメンバーによって構成される。先駆的であり、ベトナム国内において最も影響力を持つチームである。	4

人材育成プログラムなどさまざまだが、どの組織も各国のセキュリティ業界において大きな存在感を放っている。

学生の選抜方法も国・地域ごとに異なる。日本の場合は参加応募者にインシデントレスポンス・リバースエンジニアリング・ファジングなどの分野で課題を課し、その解答によって選抜が行なわれた。また、タイではサイバーセキュリティに関する競技会を行ない、成績上位の学生が選ばれた。一方、書類や面接によって選考を行なった場合も複数あり、それらの国・地域では学生本人のスキルはもちろん、セキュリティコミュニティへ貢献しようとする意欲なども加味されたという。

世界最高水準のトレーニング提供を目指して

GCC 開催にあたり、主催者は世界最高水準のトレーニングを提供すべく “Call for Trainings” を実施。その結果、応募 13 件の中から 7 件を採択することとした。その内訳は次頁にある表 2 のとおり。どのトレーニングも著名な技術者が講師を務めている。

キャンプ 2 日目と 3 日目は 2 つのトラックが用意されており、参加者はいずれかのトレーニングを選ぶこととなる。なお、最終日の 2 月 14 日は異文化を理解するための交流（観光）に充てられた。

筆者が取材で GCC 会場を訪れたのは開催初日の 2 月 10 日のこと。この日に行なわれたのは CTF 形式の「インシデントレスポンスで攻撃者を追いかけろ」であった。

このトレーニングは各国・地域の参加者が交じるよう編成されたチームで行なわれる。各自にはマルウェアに感染したコンピューターのディスクイメージが配布されるので、これを解析する。参加者は主催者が用意した設問、例えば感染したマルウェアの名称や感染の日時、通信を行なっているホストの IP アドレスなどを解答することで得点を獲得する。問題は全部で 40 問ほど。それぞれの得点は難易度に応じて異なるという。

さまざまな国・地域の人たちとチームを組むということで、トレーニング開始直後は緊張の面持ちだった参加者の表情も時間がたつにつれて和らぎ、中盤以降は多くのチームが積極的にコミュニケーションを図るようになっていた。なお、この CTF 競技の結果は 2 月 13 日の夕方に発表される。それまでの間、参加者たちはトレーニング終了後の時間などを使い挑戦を続けた。

表 2 トレーニングの概要

日程	プログラム	講師	概要
2 月 10 日 午後～ 2 月 13 日 午後	**インシデントレスポンスで 攻撃者を追いかけろ**	鈴木博志、梨和久雄 日本	標的型攻撃事案のインシデントレスポンス。被害を受けた PC のディスクイメージを調査する。CTF 形式で問題に解答することで得点を得る。デジタルフォレンジクスやマルウェア解析などの技術を学ぶことができる。
2 月 11 日 午前・午後	**機械学習システムの構築とその突破手法**	Clarence Chio 米国・シンガポール	情報セキュリティの専門家の視点から見た機械学習に関するトレーニング。機械学習のアルゴリズムとシステムを学ぶと同時にセキュリティの検証も行なう。セキュリティエンジア・ペンテスター・アプリケーション開発者に有用。
2 月 11 日 午前・午後	**脆弱性解析及びバイナリエクスプロイト 生成の自動化**	木村廉 日本	ファジングツール（攻撃コードなどのデータを自動かつ大量に生成し、入力することでぜい弱性を見つけ出す）を構築し、オープンソースソフトウェアに対して実行する。万一、ぜい弱性が発見された場合は開発者と協調の上で情報公開を行なう。
2 月 12 日 午前・午後	**実践・難読化バイナリ解析**	黒米祐馬 日本	マルウェアでは解析の作業を妨げるためコードの難読化が行なわれている。このトレーニングでは実際の標的型攻撃で使用されたマルウェアを例に、難読化されたコードの解析手法を学ぶ。
2 月 12 日 午前・午後	**Qiling Framework を用いた IoT ファームウェアの リバースエンジニアリング**	kj (xwings) LAU マレーシア	ビデオ会議を通じて行なわれるトレーニング。ルーター、ネットワークカメラ、AI スピーカーなどの IoT 機器のファームウェアのぜい弱性を調査する。これらの機器では MIPS、ARM などが使用されるため、まず、CPU のエミュレーターを構築。次にフレームワークを使い調査を行なう。
2 月 13 日 午前	**攻撃ベクター解析による攻撃時の 挙動の解析**	Moonbeom Park 韓国	" 攻撃ベクター（攻撃に使われる技術手法）を列挙。それぞれの攻撃がどのような痕跡を残すのか、ログを解析することで攻撃者の操作（行動）を解き明かしていく実践的なトレーニング。
2 月 13 日 午後	**ソーシャルメディアセキュリティ： オンラインでの情報操作の特定**	王銘宏 （Ming-Hung Wang） 台湾	ソーシャルメディアで流れる情報の収集・分析や OSINT（オープン・ソース・インテリジェンス）などを組み合わせて、「情報の真偽」「意図的な拡散なのか否か」「発信者の特定」などの調査を行なう。

参加者インタビュー

●塚崎椋也（つかさき・りょうや）さん 20 歳

東京電機大学でコンピューターサイエンスを学ぶ 2 年生。2016 年のセキュリティ・キャンプ全国大会にも参加。セキュリティ企業で Web アプリのぜい弱性診断にも携わっているという。初日のトレーニングは実践形式ということもあり、やや難しく感じたとのこと。チームメンバーとのコミュニケーションではアジア独特の英語の発音に戸惑ったそうだ。将来の目標は、高レイヤーから低レイヤーまでマルチに活躍できるエンジニアになること。

●安松達彦（やすまつ・たつひこ）さん 24 歳

早稲田大学大学院 基幹理工学研究科 情報理工・情報通信専攻の 2 年生。GCC 参加のきっかけは応募課題が解けるか否か挑戦したことだった。学内の CTF チーム m1z0r3（ミゾレ）に所属。トレーニング中、チームメンバーとのコミュニケーションは良好だったという。直近の目標は友人たちと CTF チームを結成し SECCON CTF の決勝戦に出場することなのだそうだ。

GCC 開会式後に撮影した学生と運営スタッフを交えた集合写真

今後の発展に期待

開催初日には記者会見も行なわれた。セキュリティ・キャンプ協議会のステアリングコミッティの一員であり、GCC 設立に尽力した篠田佳奈氏は壇上でその経緯を説明した。GCC の枠組みは台湾電信技術センター（Telecom Technology Center：TTC）呉宗成博士の提唱によるもので、篠田氏が各国・地域のコミュニティと連携し、立ちあげるまでに 2 年の歳月を要した。

余談になるが、内閣サイバーセキュリティセンター（NISC）では、毎年サイバーセキュリティ月間に業界著名人のコラムを公開しており、本年 3 月 16 日の回では、篠田氏が「国際イベントを立ち上げた理由〜世界基準で考える人・コミュニティづくり〜」と題するコラムを寄稿している※ 2。GCC 設立に込めた願いを自らの言葉で語っているので、興味のある方は一読されることをお勧めしたい。

サイバーセキュリティの世界において、防御の効率を上げるためには情報共有が欠かせない。そのためには人的なネットワークが必要となる。GCC はこういったことを実感・実践してきた人たちによって設立された。

「人材の育成」と「コミュニティの形成」、どちらの課題も成果が目に見えるまでには時間がかかる。しかしながら、GCC はすでに世界各国から注目を集めているという。これは各国がセキュリティ人材のグローバルなネットワークを求めていることの証左といえるだろう。GCC に加入したいという要望する国をはじめ、欧州では GCC と同様の取り組みを独自に進める動きもあるそうだ。こうした流れが加速すれば、より大きなコミュニティへとつながるはずだ。第 3 回の開催地は台湾を予定している。今後の発展に期待したい。

※ 2 **国際イベントを立ち上げた理由〜世界基準で考える人・コミュニティづくり〜**
https://www.nisc.go.jp/security-site/month/column/200316.html

日本のサイバーセキュリティ技術を世界に発信 !!

RSA Conference 2020 ジャパンパビリオン出展レポート

文 = 秋島佳代子

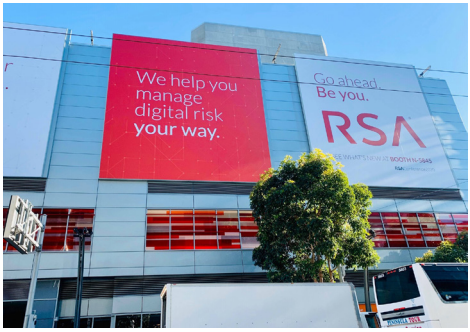
現在、日本は高いサイバーセキュリティ技術を有しているにも関わらず、世界のビジネスシーンにおける認知度は高いとは言えません。これは、日本政府の「サイバーセキュリティ戦略」からも伺えます（参考 1）。

このような状況から、特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）は、「サイバーセキュリティ戦略」を基にした総務省の施策を有効活用し、日本のサイバーセキュリティ技術を世界に発信すべく、「RSA Conference 2020」に「ジャパンパビリオン」を出展しました。弊社（日立システムズ）としてもその一翼を担うべく、この取り組みに参画することとしました。

RSA Conference とは

「RSA Conference 2020」は、毎年アメリカ（サンフランシスコ）で開催されている世界最大規模の情報セキュリティのカンファレンスで、今年は 2 月 24 日～ 2 月 28 日に開催されました。

例年 700 社以上の出展、4 万人以上の来場が見込まれています。今年は、新型コロナウイルス（COVIT-19）感染症の影響があったため、出展社数は、合計 658 社、来場者数も 3 万 6000 と若干落ち込んだ結果となりましたが、世界最大規模のイベントであることに変わりありません。



RSA Conference 2020 の会場となったサンフランシスコ・モスコーニ・センター

展示会では、各展示ブースで企業ごとにセキュリティ製品の展示や、セキュリティに関する多数のプレゼンテーションを実施します。展示会には、アメリカ企業のみならず、技術先進国であるイスラエル、ドイツ、中国、韓国なども、毎年国際パビリオンとして出展し、各国が保有する技術を競って世界に発信しています。日本もこれらの国々に後れをとることなく、日本の高いサイバーセキュリティ技術を世界に発信することが重要と考え、出展したものとなります。

ジャパンパビリオン出展状況

ジャパンパビリオンとしての出展 2 年目となる今年は、昨年度の 2 倍のスペースを確保し、スタートアップ企業 3 社を含む合計 16 社で出展しました（参考 2）。

ジャパンパビリオンでは大勢の方に立ち寄ってもらうための呼び込みアイテムとして、「すし消しゴム」をノベルティとして配布しました。「すし消しゴム」は好評を博し、日本の文化や日本に興味を持った方がブースに寄ってくださいました。このことにより、各企業のサービスや製品の説明のきっかけを作ることができ、日本のサイバーセキュリティ技術を世界に発信することができたと考えます。

ジャパンパビリオンの中で、特に大盛況だったブースは国立研究開発法人情報通信研究機構（NICT）でした。攻撃通信の可視化製品を展示し

来場者に好評だった寿司消しゴム

ており、攻撃されているトラフィックをリアルタイムに見ることができるため、多くの来場者が興味を持ったようで、足を止めてモニターを見つめ質問をしていました。また、他にも具体的なデモや、グラフィカルなダッシュボードがある出展企業のブースには、多くの来場者が集まってきていることが印象的でした。

加えて、ジャパンパビリオンの一角にはプレゼンテーションエリアを設け、各企業 10 分～ 20 分のプレゼンテーションを実施しました。このプレゼンテーションでも、具体的なデモや、リアルタイムの映像は注目を集めていました。

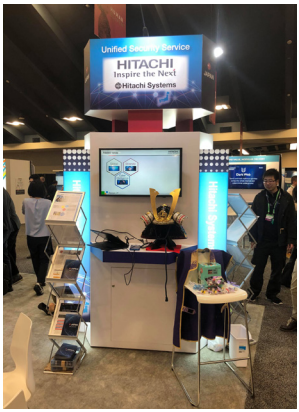
弊社は、IT システムや制御システム、IoT など多様な環境におけるセキュリティインシデントの解決を世界規模で支援するサービス「SHIELD 統合 SOC」を展示しました。

SOC サービス自体はアメリカでは新しいサービスではなく、多くの企業が SOC を独自運用していたり、アウトソースしていたりするケースがほとんどです。しかし、その大半が IT システム向けのみのサービス提供であり、制御系システム、IoT 分野向けにサービスを提供できるベンダーはまだまだ世界中でも多くありません。そのため、来場者からは、制御系システムや IoT 分野のセキュリティ強化は今後ますます需要が増すことから、弊社の知見が大いに役立つと考えられるといったコメントをいただくなど、日本のサイバーセキュリティ技術を世界にアピールできたと考えます。

一方、来場者の方から逆に製品を売り込まれるというケースも多く見受けられ、まだまだ、日本のセキュリティ技術の認知度は低く、世界から見れば後進国と見えてしまっていると感じました。来年度以降も本カンファレンスに出展を続けるなど、日本のセキュリティ技術を積極的に広報し、認知度の向上に繋がる活動は不可欠と考えます。

レセプション「Sushi Night」

RSA Conference 開催 2 日目の夜に、ジャパンパビリオンの招待制レセプション「Sushi Night」を、現地日本食レストラン Ginto で開催しました。招待者は、ブース来場者の中で特に各社製品に興味を持っていただいた方、協業の可能性や今後の



ジャパンパビリオンブース（左から全体像、プレゼンテーションエリア、弊社ブース）

パートナーになり得そうな企業の方々です。

参加者は、日本の勤続経験がある方、日本へ留学経験がある方、日本支社がある企業の方、現地の大学教授などさまざまでしたが、現地での市場がどうなっているかなども含めざっくばらんに意見交換をできたのは大変有意義でした。

また、法律関係の大学教授より興味深い話を伺うことができました。データアナリティクスが当たり前となる中、さまざまなデータを集めて分析してできたデータの所有権が誰に属すのか、また、その所有権がいつまで有効になるか、といった問題が発生していると言うのです。具体的には、単体としてのそれぞれのデータの所有権については議論する余地もありませんが、分析してできたデータについては新しいもののため、これをどうやって取り扱っていくかは今後もっと大きな問題になるとのことでした。IT 資産などは法律や国の規制に大きく影響を受けることが多いので今後も注意を払っていく必要があると感じました。

このようなネットワーキングの場を提供することは、日本のセキュリティ技術を世界に発信する一助となります。加えて、参加企業と招待者の協業により、新たな可能性を見出したり、新たな発想を生み出す刺激になると考えます。今後も積極的に同様のグローバルカンファレンスに出展、参加することで世界へのネットワークを広げていきたいと強く感じました。

おわりに

弊社のジャパンパビリオンへの出展は、昨年度に続き 2 回目でしたが、集客数には課題が残る結果となりました。その理由としては、事前の通知や直前の呼び込みが不十分だったことや、新型コロナウイルス感染症の影響などが挙げられます。

しかしながら、現地や世界のトレンドを生で聞けたこと、われわれが提供している製品やサービスについても来場者の方との意見交換ができたこと、そしてマーケット拡大に向けたニーズ調査ができたことなど、ジャパンパビリオンの一員として出展できたことは大変有意義に思います。

このような現地のフィードバックをもとに、われわれのサービス、製品の質を向上させた上で、来年度も積極的に参加を検討していきたいと考えています。また、このような活動を通して、日本のサイバーセキュリティ技術の認知度向上に寄与していきたいと考えます。

参考 1

サイバーセキュリティ戦略、内閣サイバーセキュリティセンター

https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018-kakugikettei.pdf

(3) 先端技術を利活用したイノベーションを支えるサイバーセキュリティビジネスの強化
我が国の高いサイバーセキュリティが確保されたモノやサービス等についての国際展開を促すため、トップセールスや展示会等を活用したアピールを行うほか、サイバーセキュリティを理由とした自由貿易の障害となる措置を正当化する動きに対しては、国際的な連携の下、厳格に対処するなど、国際展開をしやすいビジネス環境の整備に取り組む。

参考 2

RSA Conference 2020 における日本パビリオン出展について
2019 年の 2 倍のスペースで出展企業も倍増、
特定非営利活動法人 日本ネットワークセキュリティ協会（JNSA）

https://www.jnsa.org/press/2019/200203.pdf

JNSA はスタートアップ企業 3 社を含む 16 社の日本企業による日本パビリオンを出展し、各社自社のセキュリティ製品・サービスの展示やプレゼンテーションを行う機会を設け、北米で世界各国から来場される？々に対して日本企業のプレゼンスを示し国産のサイバー技術をアピールします。本展示会では、イスラエル、ドイツ、中国、韓国などが毎年国際パビリオンを出展、日本は 2019 年 3 月に開催された RSA Conference 2019 に続いて 2 年目のパビリオン出展となり前回の 2 倍のスペースで出展します。カンファレンス期間中は、日本パビリオンへ延べ 2000 名以上の来場者が見込まれます。「東京 2020 オリンピック・パラリンピック競技大会」を視野に入れた日々増大するサイバー攻撃への対策となる、日本産の質の高いセキュリティ製品・サービスの海外展開を後押しする総務省の施策の一環として出展いたします。

Human * IT

人と IT のチカラで、驚きと感動のサービスを。

Hitachi Systems Security Journal VOL.37

株式会社 日立システムズ
本社 〒141-8672 東京都品川区大崎 1-2-1