HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.33

株式会社 日立システムズ

Human * IT

Hitachi Systems security Jounral VOL.33

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

日本の先駆者にセキュリティ業界の動向を訊く

鵜飼 裕司 インタビュー（後編）

前号に引き続き鵜飼氏のインタビューをお届けしよう。今回は政府の研究調査会の資料から見える日本のセキュリティ業界が抱える課題がテーマだ。自身の経験を踏まえつつ、エンジニアや経営者といった多様な視点から語ってもらった。

取材・文・撮影＝斉藤健一

二極化する組織のセキュリティ対策

インタビュー前編は前号に掲載※1

斉藤（以下 S ）：鵜飼さん自身、セキュリティ業界に長年いて、ユーザー企業のセキュリティ対策をご覧になってきたと思いますが、どのように変化してきたとお考えですか。

鵜飼（以下 U ）：2011 年あたりと比較すると、体制の整備や仕組みの整備をしてきた組織は増えたと感じています。一方で、対策を講じていない組織が多いことも確かで、二極化が進んでいる状況です。大企業と中小企業との差であれば致し方ないとも思えますが、同じ業界の同じ規模の企業であっても、セキュリティ対策を行なっているところとそうでないところに開きがあります。

S なるほど。

U 地方自治体なども同様です。村役場などは全く対策できていない所も多いようです。「何も分かりません。全部お任せしていますんで…」という組織もあります。もちろんきちんと対策をしている自治体もあります。本来であれば同じネットワークに繋がっているわけですから、同レベルの対策が必要ですし、最低限のリテラシーも持つべきなのですが、セキュリティ対策のレベルが低い組織がそのまま残っているのが現状です。

S ネットワークではセキュリティのレベルはもっとも低いところに合わされてしまいますよね。

U そうなってしまうケースが多々あります。同様のことは重要インフラと呼ばれているところでも往々にして起きています。政府もそういった格差を問題視しており、最低ラインのベースをどのように底上げするか、その策を思案しています。中小企業に特化した予算立て、例えば IT 導入補助金や、中小企業へのサイバー保険の導入といった議論も行なわれています。

S 格差の要因は、組織にいる人間の意識の差ということになるのでしょうか。

U そうなのかもしれませんが、実際のところ、村役場のような場所でサイバーセキュリティ対策といっても、現場の人の理解を得るのは難しいと思います。リテラシーを高めるには時間がかかります。ですから、インフラごとうまく囲い込む仕組みを考えたり、それを実行できる体制を整えたりすることも重要です。

S 自治体のネットワークというと、以前であれば

●鵜飼 裕司（うかい・ゆうじ）
1973 年徳島県生まれ。博士（工学）。Kodak 研究開発センターにてデジタルイメージングデバイスの研究開発に従事した後、2003 年に渡米。カリフォルニア州 eEye Digital Security 社に入社。 セキュリティぜい弱性分析やぜい弱性診断技術、組み込みシステムのセキュリティ脅威分析等に関する研究開発に従事。
2007 年 7 月、セキュリティコア技術に関する研究、コンサルティングサービス、セキュリティ関連プロダクトの開発・販売を主事業とする株式会社ＦＦＲＩを設立。
また、独立行政法人情報処理推進機構の研究員を兼務（非常勤）し、コンピュータセキュリティを とりまく脅威の分析・対策立案のための活動に取り組む。
内閣官房「内閣サイバーセキュリティセンター本部研究開発戦略専門調査会」、経済産業省「産業サイバーセキュリティ研究会 WG3」、総務省「サイバーセキュリティタスクフォース」、総務省「サイバーセキュリティタスクフォース 情報開示分科会」、一般財団法人日本情報経済社会推進協会（JIPDEC）「IoT セキュリティ WG」、JNSA「サイバーセキュリティ事業における適正な事業遂行の在り方に関する検討委員会」など、多数の政府関連プロジェクトの委員、オブザーバーを歴任。
第 13 回情報セキュリティ文化賞受賞。
米国 BlackHat Conference および CODE BLUE のレビューボードメンバー

※1 Hitachi Systems Security Journal Vol.32
https://www.hitachi-systems.com/report/specialist/hj/

住基ネット、現在ではマイナンバー制度を運用するネットワークがあると思います。導入当初はそれなりに話題となっていましたが、現在では話題になることも少なくなった印象です。この背景には何かあるのでしょうか。

U 自治体のネットワークには、オープン系、LGWAN、マイナンバー系などがあります。セキュリティに対する意識は自治体によってさまざまですが、危機感を持っている組織もあり、調査を行なったりしています。弊社では徳島県と連携して組織の PC に yarai を導入して実証実験を行ないました※2。自治体としては導入によって組織が抱える問題が明らかになりますし、弊社としてもソフトウェアの改善要望といったフィードバックを得ることができました。

S 徳島県は鵜飼さんの出身地ですが、連携されたのには他の理由もあるのでしょうか。

U 知事が IT に明るいというのが大きな理由です。例えば、徳島県内の限界集落の通信インフラを整備して、企業のサテライトオフィスを誘致するなどの IT を利用した施策に取り組んで注目を集めています。また知事自身が J-LIS（地方公共団体情報システム機構）の代表者会議の委員を務められており、自治体の IT 化においてリーダーシップを発揮されています。

S yarai といえば、セキュリティソフトで、シグニチャーベースでなく、プログラムの振る舞いを検知するものという認識です。それを県庁職員などユーザーの PC に導入したということで良いのですか？

U そのとおりです。総務相の「地方公共団体における情報セキュリティポリシーに関するガイドライン」においても不正プログラムの挙動を検知する方式について記述されています※3。

S 分かりました（編注）。これまでの話では、組織間に厳然として存在するセキュリティ意識の格差を是正するのはリテラシーの向上とおっしゃっていますが、他の方策は何かありますか。

U それが正しいかどうかという判断はさておき、欧州では GDPR（EU 一般データ保護規則）があり、米国でもカリフォルニア州において「消費者プライバシー法案」（California Consumer Privacy Act）が成立しており、連邦政府も同様の法案を検討していると言われています。こういった法律ができれば取り組みは加速すると思いますが、企業への負担も大きくなることから、その是非については慎重な議論が必要です。

国産サイバーセキュリティの現状と課題

S 鵜飼さんは NISC のサイバーセキュリティ本部の分科会である研究開発戦略専門調査会に委員として参加されています。本年 3 月に行なわれた第 10 回の会合において、鵜飼さんは「国産サイバーセキュリティの現状と課題」と題するプレゼンテーションをされました※4※5。これについて伺いたいと思います。最初に確認なのですが、プレゼンテーションのテーマは鵜飼さんからの発案なのですか、それとも調査会事務局からの要請なのでしょうか。

※ 2「徳島発！『サイバー攻撃対策強化』実証実験」を実施
https://ssl4.eir-parts.net/doc/3692/ir_material11/85394/00.pdf

※ 3 総務相「地方公共団体における情報セキュリティポリシーに関するガイドライン（平成 30 年 9 月版）」の、「6.4. 不正プログラム対策 」iii- 92 に下記の記載が追記された。
「（注 3）インターネットからの不正プログラム感染、侵入を防御するための方式として、パターンファイルで検知が難しい不正プログラムも存在することから、不正プログラムの挙動を検知する方式もある。」
http://www.soumu.go.jp/main_content/000575052.pdf

編注 2018 年 10 月 23 日に開催された「地方自治情報化推進フェア 2018」において FFRI の岡田一彦氏と徳島県経営戦略部の山住健治氏が行なった講演の内容がログミー Biz に掲載されている。
「自治体へのサイバー攻撃、いかに対策するか？情報セキュリティ専門家集団と徳島県の取り組み」
https://logmi.jp/brandtopics/320172

※ 4 NISC サイバーセキュリティ戦略本部 研究開発戦略専門委員会 会議資料
https://www.nisc.go.jp/council/cs/kenkyu/index.html

※ 5 国産サイバーセキュリティの現状と課題
https://www.nisc.go.jp/pdf/council/cs/kenkyu/dai10/10shiryou03.pdf

U 事務局からの要請でした。プレゼンテーションの背景には海外、主に北米企業の製品やサービスに大きく依存している日本のサイバーセキュリティ産業の現状があります。産業としても国家安全保障の観点からも日本国内での研究開発をより活発化させる必要があります。北米企業はリスクを取って研究開発を行なっていますから、ビジネスでは当然いちばん良いところを持って行きます。日本企業は輸入して展開する販売店の位置付けですから利益は少なくなります。研究開発をしっかり行なっておかないと、産業界で今後何かイノベーションが起こったときに、サイバーセキュリティがボトルネックになって進まないという状況にも陥りかねません。結局のところ、コントロールできないという状況は安全保障の面から言っても問題なのです。

S プレゼンテーションの手応えはいかがでしたか。

U プレゼンテーションでは現状のメリット・デメリットを考察していますが、セキュリティベンダーにとって研究開発を行なわないのはデメリットしかないと多少の皮肉も込めて力説しました。

S 確かに。リスクもないけれど利益も少ないということですね。これでは他社との差別化も難しくなります。

U 価格による差別化は考えられますが、それは消耗戦ですよね。以前から日本の IT 業界は、3K や 5K などと揶揄される厳しい労働環境です。その裏側にはこうしたビジネスの仕組みも関係していると思いますし、会議の場でも同様の話をさせてもらいました。

S プレゼンテーションのスライドでは技術者が起業する環境についても触れられています。海外と日本ではベンチャー・キャピタル（VC）などが果たす役割に違いなどはありますか。

U 日本の VC はハンズオン（投資先の経営に深く関与する）まで積極的に行なうところはまだ少ないように思います。現在、経産省や NICT によるベンチャー支援も行なわれているようですが、起業家への周知もいまだ不十分だと聞いています。海外の場合、技術以外何も分からずに起業したエンジニアであっても、VC をはじめとして業界内にサポートする仕組みが整っています。これが日本とのいちばん大きな違いだと思っています。日本の技術力そのものが海外に比べて劣っているわけではないのです。

S 分かりました。起業に関連するのですが、サイバーセキュリティにおいて日本が得意な分野でビジネス展開が期待できるものは何かありますか。

U 難しい質問ですね。ビジネスでは先の展開を読むことが重要になります。われわれもさまざまな研究開発を行ないながら、次の一手を模索しています。その点からいうと、現在ある資産（日本の強み）をどのように活かすかという発想は、勝負の土俵を自ら限定することになるので、個人的には良いとは思いません。全く新しい分野であれば「強みも弱みもない」はずです。

S 確かにおっしゃるとおりです。

U カテゴライズされた従来の分野では多くの研究者がいて、基礎から応用までさまざまな研究がなされており、すでにビジネスにもなっています。ですから、現在のマーケットは小さいけれど今後の成長が見込めそうな分野を探していく方が現実的だと思います。例えば自動車のセキュリティなどは数年前まではマーケットが全くありませんでした。

S はい。

U IoT の分野もしかりです。IoT といっても領域は広範囲にわたります。IoT のシステム全体を守る場合は既存の ICT でカバーできるはずですから、イノベーティブなことは起こりにくいと思います。ただし、今後新たな IoT デバイスが普及した場合にどのような攻撃が起こりうるかを予想し、その対処策を実装していくことなどは新たな方向性の 1 つではないでしょうか。

S 話が具体的でイメージしやすいですね。

U アーキテクチャーについても同様です。現在、PC の世界ではインテル、スマートフォンでは ARM 系が圧倒的なシェアを誇っていますが、今後の IoT では新たなアーキテクチャーやプラットフォームが出てくる可能性もあります。こうしたプラットフォームの攻撃や防御を研究する中で何か展開があるかもしれません。

S ヒントがいろいろと見えてきました。ありがとうございます。引き続き国内セキュリティ企業の海外展開について伺いたいと思います。他の媒体のインタビューだったと思いますが、鵜飼さんは、

全世界のサイバーセキュリティのマーケットで日本が占める割合は 10% ほど。一方で日本企業の売り上げは非常に小さいと発言されていました。この現状をどのようにお考えになりますか。

U 売り上げの規模は非常に小さいですね。日本企業の海外展開が進まない理由の１つは国際的に通用する製品・サービスを持っている企業が少ない点にあります。日本の製品・サービスは国内のニーズに合わせていますから、ある意味でガラパゴス化しています。サイバーセキュリティ産業において、そのまま海外で展開できるのはわれわれの製品くらいではないかと思っています。

S ＦＦＲＩの海外展開の状況はいかがでしょうか。

U 残念ながら市場でのプレゼンス（存在感）はまだまだ低く、大きな課題となっています。ただ、ビジネスがやりにくいかと言われればそうではない側面もあります。

S それはどういうことでしょうか。

U 理由はいろいろと考えられると思いますが、日本企業はどの国にも嫌われていないという特徴があるようです。その中には日本企業に対して強い信頼感を持っている人たちもいますから、チャンスはあると思います。

S 最後の質問になりますが、今後２～３年を見据えたＦＦＲＩの目標をお聞かせください。

U 先ほどもお話しましたが、日本のサイバーセキュリティ業界のプレゼンスをグローバルで高めていきたいと考えています。日本はサイバーセキュリティ立国の推進に努めていますが、グローバルはそのような見方はしていません。少なくとも日本のＦＦＲＩという企業の存在をグローバルに浸透させていきたいですね。弊社では yarai の販売を行なっていますが、サイバーセキュリティで解決すべき技術的課題は他にも数多くあります。これらを解決する技術を確立し普及させていきたいと考えていますし、その過程でグローバルカンパニーとして成長していきたいとも考えています。

S 本日はご協力いただきありがとうございました。

ハクティビズムとインテリジェンスをテーマにした
セキュリティカンファレンス

REVULN '19 レポート

取材・文・撮影 =tessy

香港で開催されたクローズドな カンファレンス

本年 5 月、香港にて REVULN というカンファレンスが開催された。テーマをハクティビズムと OSINT（Open source intelligence）に絞り込み、参加者も招待客オンリーというクローズドなイベントだった。今回は講演の模様などを紹介するとともに、主催者のルイージ・オーリエマ（Luigi Auriemma）氏にインタビューを行ない、イベント開始の経緯や今後の展望などについて語ってもらうこととした。

主催者オーリエマ氏は、2011 ～ 2012 年にかけて多数のぜい弱性を発見し、独自のアドバイザリや PoC（Proof of Concept：検証コード）、ゼロデイの公開などで知られており、その後は制御システム関連の研究などで活躍する人物だ。

そのような彼に筆者が初めて会ったのは 2012 年の秋、韓国で開催されたカンファレンス POC（Power of Community）でのことだった。余談だが当時のオーリエマ氏の講演スライドは REVULN のサイトで公開されている。※ 1

そして本年 1 月、彼からメールが届いた。その内容は「香港でハクティビズムと OSINT をテーマとしたカンファレンスを企画しており、そのテーマで講演者を捜している。特に日本に関係するテーマ、講演できる人を捜して欲しい、また宣伝にも協力してほしい」というものだった。こちらからは「可能な範囲で協力する」と返答。これが話の始まりだった。

カンファレンスの模様

カンファレンスの開催は 5 月 15 日・16 日の 2 日間。会場は香港島北部に位置するハーバープラザ・ノースポイント。講演者は、Web サイトのアジェンダにもあるように地元香港をはじめとして、中国・台湾・日本・韓国・フィリピン・シンガポール・タイ・ロシアなどから、研究者・大学教授・CSIRT 関係者・警察・軍関係といった面々が揃った。※ 2

一方、参加者数は約 40 ～ 50 名ほど。招待者オンリーということもあったが、当初こちらが聞かされていた予定よりも少ない印象だ。講演者の同僚、同業者が多かったが、金融機関や他の SOC で働く人など、こちらも多彩な顔ぶれであった。

講演について、個人的に興味を惹かれたものは非公開になってしまっているものが少なくないが、NTT セキュアプラットフォーム研究所の 小寺博和氏、二関学氏による講演 “Catch Phish If You Can” はフィッシングサイトの調査にフィッ シングキットの解析を用いるというアプローチによるもの。 攻撃者が設置に失敗したフィッシングサイトからフィッシングキットをダウンロー ドし、それらの解析を行なった。 OSINT 手法なども組み合わせて、インドネシアの攻撃者を追跡した 事例などを紹介。多数の丹念な調 査に基づくもので非常に興味深いものであった。

講演資料は公開可能なものに限られるが Web サイトのスピーカーページに掲載されている。※ 3

REVULN はオーリエマ氏にとって初主催のカンファレンスだった。スモールスタートで当初は司

※ 1 https://revuln.com/files/Ferrante_Auriemma_0wning_Multiplayer_Online_Games.pdf
※ 2 https://revuln.com/revuln19.htm#event_agenda
※ 3 https://revuln.com/revuln19.htm#event_speakers

会進行役すらいないような大胆（?）なものだったが、振り返れば講演者と参加者との距離が近く、日頃接点のない人たちと交流できる貴重な機会となった。数年の間、連絡が途絶えていたにも関わらず、招待してくれたオーリエマ氏に感謝の意を表したい。

なお、REVULN の Medium にて、カンファレンスの振り返りと今後の展望が述べられている。それによれば、2019 年中に次回を開催したいとのこと。今回はハクティビズムと OSINT がメインテーマだったが、次回のテーマは柔軟に考えているという。現在 3 つの案を検討しており、夏までに 1 つに絞り込むそうだ※ 4。（次頁に主催者インタビューを掲載）

Catch Phish If You Can: A Case Study of Phishing Website and Actor の講演を行なった小寺博和氏（写真左）と二関学氏（写真右）

※ 4 **Next steps – REVULN – Medium** https://medium.com/@REVULN/next-steps-ca3fc4fa520f

REVULN 主催者　インタビュー

– なぜアジアでイベントを開催することにしたのか？

ここ数年アジアで多くの時間を過ごしてきた。その中で、それぞれの地域の人間が自国や自身の経験について話し合う場を作りたいと思うようになってきた。

サイバーセキュリティのイベントでは多くの場合、ジャーナリストを意識して、特定のトピックや、ニッチもしくは議論を呼ぶテーマ、ハードコアなハッキングを減らし、アイデアや議論の場を増やすことに注力している。

スポンサーなしですべての準備を自分で行なうというのは大きなチャレンジだった。自身の名前やREVULN というブランドも知られていないアジアという地域では実現不可能と思われたこともあった。

香港は多くの人にとって渡航の際に特別な VISA などを必要としない国であり、場所としては完璧だと思う。ただ東京と同様にアジアの中では物価が高いのが難点だ。

– なぜテーマを OSINT とハクティビズムにしたのか？

これらのトピックは情報セキュリティのカンファレンスであまりカバーされていないトピックであること、さらにアジアではこれらのテーマがほとんど見ることがなかったからというのが理由。

こういった、他がやっていないことに特化することは多く開催されているカンファレンスと差別化をするための唯一の方法である。

付け加えると「ハクティビズム」のトピックは 2 つの解釈をしており、思想に基づくサイバー攻撃自身と、これらの違法行為を阻止するために当局が採用した優れた対策としている。また実際に招待者の中には法執行機関の顔ぶれもあった。

私が望んでいた 2 つのプレゼンテーション（暗号通貨の社会的側面と日本におけるハクティビズム）が実現できなかったのは残念だったが、これはまた次回としたい。

– なぜ招待オンリーのクローズドなイベントとしたのか？

当初のアイデアは、チケットから全てのコストをカバーする、つまり初期予算によって（通常のプラチナスポンサーシップと同じ）で継続的にできる形態で考えていた。

ルイージ・オーリエマ（Luigi Auriemma）氏

イベントに取り組んでいる間に、出席者をよりよくコントロールすることに決めた。それは予算が問題ではなかったので、招待のみという解決策を選び、招待された人々が誰でも、堅苦しくなく、リラックスして会合に参加できるようにと自分自身で選択、承認をした。

– 今後の予定は？

このプロジェクトは 2018 年 3 月に始まり、多くの分野での学びや多くの人々とのコンタクトを得ることができた。そのため「見返りがない」というポイントははるか昔に過ぎてしまった。

このテーマをベースとして、スポンサーなし、招待者オンリーのスタイルのイベントを国際的なスピーカー達と続け、他の都市にも持っていきたいと考えている。東京は間違いなく行きたい都市の 1 つである。

少ない予算で準プライベートの会議を運営するプロジェクトにおいては、会議は何が機能するかを理解する機会になり、改善の必要性や他のイベント運営者と話をするということを念頭に置いている。

それは TV 番組のパイロットエピソード（海外ドラマなどで先行して製作される試写版）のようなものだと考えている。

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.33

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