HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.32

株式会社 日立システムズ

Human * IT

Hitachi Systems security Jounral VOL.32

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（前編）

AI、5G、IoT など新たな技術の登場によってわれわれの社会が大きく変わろうとしている。一方ではサイバー空間の覇権を巡り大国間の衝突も起こっている。今回、話を伺う鵜飼裕司氏は、エンジニア、経営者、政府のサイバーセキュリティ研究開発会議の委員などの顔を持つ。そこで今号と次号の 2 回にわたり、今後の動向について語ってもらうこととした。

取材・文・撮影＝斉藤健一

さまざまな要素が絡み合う
サイバーセキュリティ　脅威の予測は困難!?

斉藤（以下 S ）：鵜飼さんは現在、セキュリティ企業、ＦＦＲＩの経営者としてご活躍ですが、エンジニア出身で米国スタートアップ企業に在籍された経験もお持ちです。また、BlackHat や CODE BLUE といったカンファレンスのレビューボードであるとともに、政府や官公庁のセキュリティ関連委員会のメンバーも務められるなど、さまざまな顔をお持ちです。今回はサイバーセキュリティを取り巻く状況について、多様な視点からお話しを伺いたいと思います。よろしくお願いします。

鵜飼（以下 U ）：こちらこそ、よろしくお願いします。

S 2019 年も約半分が過ぎようとしていますが、今後のセキュリティ業界について考えてみたいと思います。まずは、発生が予想される新たな脅威についてです。セキュリティカンファレンスでの発表テーマの動向などとあわせてお聞かせいただけると幸いです。

U 7 ～ 8 年前であれば、マルウェアやぜい弱性、最新の攻撃手法など、カンファレンスで話された脅威がその後のセキュリティに直接的に影響を与える事例も多かったと思います。5 年ほど前でも、IoT の脅威が取り沙汰されていて、それほど深刻ではないにせよ、一定の議論が行なわれてきました。しかし、ここ 2 ～ 3 年は、その傾向が変化してきたように思います。

S それはどのような変化でしょうか。

U 1 つはサイバーセキュリティを取り巻く状況の変化です。現在、サイバー空間で起きている問題は貿易や外交といった要因とも密接に関係しています。また、サイバーセキュリティがカバーする範囲も以前とは比較にならないほど広がっています。ですから、技術的な視点からだけで今後の脅威を予測することは難しいのです。

S 近年では、国家の関与が指摘されるサイバー攻撃が報道されるなど、技術的な側面だけでは語れないケースも数多くありますね。

U もう 1 つは、カンファレンスなどで話題になるトピックの変化です。人目を引くキャッチーなタイトルが付いてはいるものの、それが本当に深刻な影響を与えるか否かについては疑問なものが増えてきているように思います。

S 確かに。理論上は攻撃可能だけれども実際の悪用は困難というぜい弱性が大々的に報じられることも多いと聞きます。

U とはいえ、注目すべきトピックもあります。まずは AI や機械学習の分野です。セキュリティ業界でも防御の仕組みとして AI や機械学習が使われています。

●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

S 具体的にはどのような形で使われているのでしょうか。

U 例えば、マルウェアを検知する目的で多数のサンプルをコンピューターに読み込ませて、マルウェアに特有な部分を導き出せるように学習させます。また、マルウェア以外にも応用して、攻撃パケットの特長を学習させたり、大量のパケットから攻撃に用いられるものを抽出したりといったことが考えられます。人間の長年の経験や勘を必要とする領域には向いていると思います。しかし、AI や機械学習に大きく依存した対策にはリスクがあります。

S AI や機械学習も万能ではないということですか。

U そのとおりです。以前、マルウェア対策としてサンドボックスがもてはやされた時代もありましたが、現在ではマルウェア側がサンドボックスを検知して動作を停止するものもあります。過信は禁物です。現在の AI では大量の学習データセットが必要となりますが、いちばんの落とし穴は、サンプルとなるデータセットはどこから得られるかというと、それは攻撃者からだということです。その気になれば攻撃者はデータセットをコントロールできるのです。

S それは構造上大きな問題ですね。

U 防御側が学習のデータセットとして集めているものに対して攻撃者が何か手を加えた汚染されたデータを流してしまうということが考えられます。いわゆるポイズニングや敵対的学習と呼ばれる手法です。

S 興味深い話題です。これらのテーマはどんな場所で議論されているのでしょうか。

U BlackHat などでは、機械学習による検出をどう回避するかといった研究がトレンドの 1 つになっています。“AI vs Virus” といったタイトルが付いていることもあります。われわれのようなセキュリティベンダーも、このあたりのジャンルには敏感になっています。

S では、攻撃者による AI の利用についてはどうでしょう。DEFCON 24（2016 年）で DARPA（米国防高等研究計画局）が開催した CGC（Cyber Grand Challenge）では AI がプログラムのぜい弱性を探っていきました※ 1。こういった動向に変化はありますか。

U 現実的にはどうでしょう。現時点ではサンプルも少ないですし、AI でハッキングの攻撃技術がどこまでできるのか、正直まだ分かりません。さまざまなことが実験的に行なわれていますので、それらの研究成果を待たないと具体的な言及はできないと思います。

S I oT の分野はどうでしょう？

U すでにさまざまな機器がネットワークにつながっていますが、これらの中にはセキュリティ対策を意識していない製品も含まれており、攻撃者による悪用の危険性も指摘されています。今のうちに根本的な対策を講じておくことが重要です。さもないと、2000 年代初頭の Windows のように「攻撃され放題」の状況になってしまうと思います。

S 総務省や NICT（国立研究開発法人情報通信研究機構）が IoT 機器を調査し利用者への注意喚起を行なう NOTICE（National Operation Towards IoT Clean Environment）が、まさしくこの根本的な取り組みの 1 つと言えますね※ 2※ 3。

U そのとおりです。

S 他の分野でいえば、サプライチェーンのセキュリティ問題があります。製品やサービスの製造・流通の過程において不正なプログラムやファームウェアの改ざんなどが行なわれるリスクですが、こちらはいかがですか。

U 一部中国メーカー製品へのスパイウェア混入疑惑に端を発した問題もここに含まれます。いまでは米中の貿易・外交問題へと発展し、当該メーカーに対する制裁措置も実施されています※ 4。この問題は混沌としており、全体を俯瞰できる人は技術者の中にはいないと思います。米国の主張どおり製品に情報漏えいのリスクがあるとすれば大きな問題ですが、現時点において米国政府はエビデン

※ 1 **DARPA Cyber Grand Challenge** https://www.darpa.mil/research/programs/cyber-grand-challenge

※ 2 **NOTICE** https://notice.go.jp/

※ 3 **マルウェアに感染している IoT 機器の利用者に対する注意喚起の実施（総務省）**
http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00025.html

※ 4 **編注：**本年 6 月 29 日、米国トランプ大統領は G20 大阪サミット閉幕後の記者会見において、米国メーカーが当該中国メーカーとの取引を容認する発言を行なっている。

スを明らかにしていません。

S おそらく今後もエビデンスが公表される可能性は低いでしょうね。さて、2018 年には Spectre や Meltdown といった CPU のぜい弱性が立て続けに発見・公表されました。サプライチェーンのセキュリティ問題を考えれば、より精査されなくてはならない重要な分野であるはずです。ところが、こうしたぜい弱性を探すことができる研究者は非常に限られると思います。この点はどのようにお考えですか。

U この分野はもはや個人でできる研究の範疇を超えており、国家としてぜい弱性探しに取り組んでいるところもあります。日本でも産官学が一体となりサプライチェーンリスクに対応するための技術検証体制の整備をはじめようとしています。これは NISC（内閣サイバーセキュリティセンター）のサイバー戦略本部が掲げる「サイバーセキュリティ 2019」の中でも取り組み強化の方針が打ち出されています※5。

S 昨年 12 月、外務省や NISC が中国を拠点とするサイバー攻撃者グループ「APT10」に対して警戒を表明しました※6※7。特定グループを名指ししたのは異例のことと言えます。コメントするのも難しいとは思いますが、何かご意見はありますか。

U 先ほど申し上げたとおり、サイバーセキュリティには国家間の外交・貿易・安全保障など多くの要素が含まれるようになりました。各国がサイバーセキュリティに関して具体的な対処を始めたと言えます。これは同時に、サイバーの分野が重要であるとの各国の意思表明でもあると思います。

リテラシー向上こそが最上のセキュリティ対策

S 話題を転じます。サイバー攻撃には経済犯による犯行も含まれています。防御側としてはどういった手立てを講じればよいと思いますか。

U サイバー攻撃の規模としては経済犯が圧倒的な多数だと思います。もちろん防御側もさまざまな対策を講じてきたと思いますが、攻撃者も次々と新たな手法を繰り出しています。ランサムウェアの被害は落ち着いてきたように感じますが、昨年は暗号通貨の取引所を狙った事件も発生しており、被害額としては大幅に増えていると思います。

S そのとおりですね。

U 被害を防ぐためには結局のところ、資産を持つ側のリテラシー向上をめざした啓発活動しかありません。逆を考えれば、啓発活動を怠ったところが被害に遭ったという見方ができるかもしれません。さらに、この啓発活動は一度で済むというわけに行きません。常に注意を払っておく必要があると考えています。また、この啓発は民間に限らず、政府もきちんと行なう必要があるだろうとも考えています。

S 先の APT10 の警告は、国による啓発活動の一環だとも言えそうですね。

U そうかもしれませんね。ともかくリテラシーの向上には時間も費用もかかりますから、日本全体で考えていかなくてはならない問題だと思います。

政府のセキュリティへの取り組み

S 日本の目下の課題は、2020 年に行なわれる東京五輪大会の成功だと思います。こちらについてはいかがですか。

U 課題としてはそのとおりだと思います。ただ残念ながら私自身は東京 2020 には携わっていませんのでお話しできることがありません。この話題は競技大会組織委員会などに聞かれるのがよいと思います。

S 分かりました。別の機会に関係者の方に話を伺ってみたいと思います。現在、政府のサイバーセキュリティは NISC が各省庁を横断的に取りまとめて行なうようになりました。とはいえ、国民が持つ行政のイメージは縦割りですから、ここにたどり着くまでには長い道のりがあったのだろうと推測しています。鵜飼さんは長年、各省庁のセ

※5 **サイバーセキュリティ 2019** https://www.nisc.go.jp/pdf/policy/kihon-s/cs2019.pdf

※6 **中国を拠点とする APT10 といわれるグループによるサイバー攻撃について（外務報道官談話）** https://www.mofa.go.jp/mofaj/press/danwa/page4_004594.html

※7 **APT10 といわれるグループによるサイバー攻撃について（注意喚起）** https://www.nisc.go.jp/active/kokusai/pdf/press-1221.pdf

キュリティ関連の研究会・タスクフォース・ワーキンググループなどのメンバーとして活躍されてきました。そこで現在と過去を比較して話を伺いたいと思います。鵜飼さんが委員として参加されたのはいつ頃からですか。

U はっきりと覚えてるわけではありませんが、ＦＦＲＩ設立後のことですから 2007 年以降だと思います。

S その頃のサイバーセキュリティのトピックにはどのようなものがありましたか。

U こちらも記憶があいまいですが…　Winny などファイル共有ソフトが話題になっていたかもしれません。

S 各省庁のセキュリティへの取り組みはいかがでしたか。

U おっしゃるとおり、各省庁がバラバラにセキュリティ対策を進めようとしていた縦割りの時代もありました。現在では NISC がとりまとめの軸となっています。さまざまな会議に出席すると、関係省庁の方々が垣根を越えてオブザーバーなどの形で出席するようになってきていますし、情報共有もされていると思います。

S 会議の雰囲気などはどうでしょう。

U 当時も当時なりの切迫感はあったと思います。ただ、現在から振り返って考えると、当時の感覚は薄かったといえるかもしれません。というのも現在の方が真剣に議論しなくてはならないトピックが増えているからです。

S 変化のタイミングはどこにあったのでしょうか。

U 日本で標的型攻撃が話題になってきた 2011 年あたりだと思います。

S 日本の防衛産業を担う大手機械メーカーへの標的型攻撃が報道された時期ですね。

U はい。このあたりからじわりじわりと、国としてサイバーセキュリティの施策を打たなくてはならないという空気が醸成されるようになってきました。

S そこから 2014 年のサイバーセキュリティ基本法の施行、そして東京 2020 大会の取り組みへとつながっていくのですね。（次回へ続く）

Mizuho Cyber Challenge Cup（MC3）レポート

取材・文＝斉藤健一／写真提供＝みずほ FG

みずほ FG のセキュリティ・コンテスト

2019 年 3 月 18 日、東京都千代田区内のみずほフィナンシャルグループ（FG）本社にて、MIZUHO Cyber Challenge Cup（MC3）が開催された。MC3 とは、みずほ FG のセキュリティ・コンテストでレッドチーム演習などと呼ばれる形式で行なわれる。グループ各社がブルーチーム（防御）として参加し、主催者側のレッドチーム（攻撃）によるサイバー攻撃に対処する。セキュリティの実践的なスキルを競うというものだ。

MC3 の開催は今年で 2 回目。開催日は内閣サイバーセキュリティセンター（NISC）が定めるサイバーセキュリティ強化月間の最終日で、数字の語呂合わせで「サイバーの日」となっている。

MC3 の新たなる挑戦

イベントの開始は午前 9 時。開会式が行なわれたセミナー会場には競技参加者をはじめ、IT ベンダーや他の金融機関の社員といった外部の見学者など大勢が集まっている。開会式ではコンテストの目的や新たな取り組みなどについて触れられた。MC3 の目的はサイバーセキュリティの人財発掘および育成で、座学だけでなく手を動かすことで、より実践的なスキルを身につけることができるという。

今回は 2 回目の開催ということで「ビヨンド・ボーダーズ」というスローガンを掲げ、新たな技術要素・ビジネスシナリオの導入や競技参加枠の拡大などに取り組んだという。　競技の前提となるビジネスシナリオでは、フィンテックをはじめとする動きの早い金融業界の動向が反映されたものとなっている。

また、今回は競技参加枠を拡大し、みずほフィナンシャルグループ、銀行、信託銀行、証券、情報総研に加え、グループ会社および海外拠点からも参加者を募り、総勢 7 チーム（約 50 名）がしのぎを削ることとなった。

フィンテック関連のスタートアップ企業が競技の舞台

競技内容は全チーム同じ条件の下、いくつかの課題（サイバー攻撃の状況）が与えられる。技術的な調査結果の正確性・即時性、また経営層に対する報告の適切性を多面的に評価され、もっとも優れたチームが表彰される。

ビジネスシナリオによれば、舞台は大手金融企業が立ちあげたスタートアップの M 社。意思決定は早いが、事務・管理といったバックオフィスの業務が追いついておらず、承認のプロセスも定まっていない。こういった状態がしばらく続き、ガバナンスの目が行き届かなくなっているという設定だ。そして、競技で参加者が対峙することとなる今日的なリスクが「シャドー IT」だ。これは組織の管理が行き届かない IT 環境を指す。言葉としては昔からあるそうだが、現在ではシャドー IT がネットの向こう側（クラウド）にも存在するやっかいな状況となっている。

競技会場はチームごとにパーティションで区切られており、競技用 PC が置かれたテーブルやホワイトボードなどが用意されている。見学者は講演の合間などに会場を移動して競技の模様を見ることができる。

競技中の様子はチームによってさまざまだ。ホワイトボードを使いメンバー間でディスカッションするチームがある一方で、それぞれのメンバーが PC に向かい黙々と作業を続けているチームも

競技の様子

セミナー会場の様子

ある。また、会場にはスコアボードも設置されており、各チームの順位を把握することもできる。

一方、競技会場に隣接するセミナー会場では、競技中継をはじめ、見学者に向けた競技の解説や社内外の識者によるサイバーセキュリティをテーマにした講演なども行なわれた。

勝敗の行方

競技は 15 時 30 分に終了し、みずほ FG チームが優勝を飾った。16 時から行なわれた表彰式では参加した各チームから感想が述べられた。具体的には、サイバー・インシデントを実践的に学ぶことができた、攻撃のシナリオを予想して競技に臨んだがシャドー IT は全くの予想外だった、攻撃者の視点で考えてみることも大事といった声が挙がっていた。

一方、主催者は参加者に対して、競技を通じてサイバー攻撃が起きたときに要求される思考やプロセス、そしてあるべき行動の姿を意識してほしいと考えていたようだ。特に重要となるのは、攻撃の全体像を把握することであり、これはレスポンスのトリアージ（対処の優先性）を判断する上でも、インシデントの根本原因や再発防止策を考える上でも必須となると強調していた。

また、各チームの感想を聞くと、多くが競技開催の半年ほど前からチームを結成し、自主的に勉強会を開くなどして研さんを重ねてきたということが分かった。実は、競技前に行なわれたチームの紹介では、それぞれが意気込みを熱く語っていたのだが、これが準備期間の長さや熱意に比例しているのだと、この時はじめて納得した。

表彰式では、レッドチームによる競技参加者向けの技術的解説も行なわれた。レッドチームも準備期間に約 1 年を費やしたという。ただ、今回のシナリオは攻撃情報の詳細を含んでいることや、今後のワークショップなどで同じシナリオを使う可能性があることから、技術的な情報を誌面に掲載することは残念ながらできない。読者の皆さまにはあしからずご了承いただきたい。

MC3 を通じてコミュニティの輪を広げる

MC3 を主催するメンバーの 1 人に話を伺った。昨年に第 1 回目を主催して社内・グループ内でセキュリティに対する認知が広まったことと、それによって社内でセキュリティコミュニティを作り、定期的に活動するようになったことが大きな成果だという。

また、MC3 の今後については検討中としながらも、他の金融機関や IT ベンダーなどと連携しつつ、コミュニティの輪を広げていきたいと語ってくれた。

MC3 を取材した筆者の感想は、良くオーガナイズされたイベントだったということ。それは、競技の全体像を見学者に分かりやすく説明していたり、技術に詳しくない人にも分かるよう講演内容に配慮があったり、レッドチーム・ブルーチームの双方が準備に長い時間を掛けていたりすることから感じることができる。そして何よりも参加している人たちが楽しんでいることが伝わってくるのが印象的だった。MC3 の今後の展開に期待したい。

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.32

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