

CYBER GRID

サイバー・グリッド・ジャーナル

JOURNAL VOL. 9



ニッポンのミライを救う
サイバーセキュリティにおける
「未病改善」の考え

TABLE OF CONTENTS

3 巻頭言

小笠原 恒雄

4 特集

ニッポンのミライを救う

サイバーセキュリティにおける「未病改善」の考え

④ マルウェアのDNA鑑定で系統を自動判定する

小笠原 恒雄

⑥ リサーチャーの眼

研究・開発の最前線からお届けする技術情報

第6回 AIによる脅威予測 ～どこまで可能なのか～

庄司 勝哉

⑩ 座談会

研究開発のこれまでとこれから

～ラックのノウハウと研究の融合で「先回り防御」を実現したい～

一藁 俊裕、外谷 渉、高原 健、三川 草平、船引 裕司(司会)

14 ラックの顔 さまざまな場所で活躍する社員をご紹介

第9回 サイバー攻撃を未然に防ぐために続ける

社会の意識改革への挑戦

田原 祐介／関 宏介

18 巻末あとがき

オリンピックイヤーに突入。 サイバーセキュリティは 転換期を迎えています

小笠原 恒雄

サイバー・グリッド・ジャパン
次世代技術開発センター長



ラグビーワールドカップ2019日本大会を終え、東京オリンピック・パラリンピック開催年に入りました。2020年を区切りの年と考える人は多いと思いますが、IoTやAI技術が浸透した超高度デジタル社会に突入しようとする昨今において、サイバーセキュリティの分野も転換期を迎えています。

攻撃者の視点で見ると、IoTデバイスやクラウド利用の普及などで急激にターゲットが増加しています。さらに標的型攻撃等の高度サイバー攻撃は円熟期を迎え、さまざまな工夫をして攻撃を仕掛けている状況です。一方、対策防御においては、国内のセキュリティ意識は高まっており、実際にサイバーセキュリティの政策検討や協議、また情報連携・共有などの取り組みが盛んに行われていますが、民間企業が行った日本経営層に対する調査では、セキュリティ対策に遅れを感じているという調査結果があり、対策防御側は多くの悩みを抱えているように感じています。

こうした様相を踏まえて組織におけるセキュリティ対策を考えた場合、守るべき領域が拡大し、ITサプライチェーン・リスクへの対応や人材不足など、さらに多くの課題があり、組織への負担はますます大きくなることが予想されます。このような課題を解決するために、「未病改善」の考えを取り入れてセキュリティ対策を見直す必要があると考えています。

医療において「未病改善」とは、自分自身がより健康的な状態に近づけるような取り組みを常日頃から行うことです。健康を維持するためには、健康診断や人間ドックを年に一度受診し、異常が見つかったら治療に取り組むという単調なサイクルだけではなく、栄養バランスに配慮した食品の摂取や運動を生活に取り入れるなど、個人で取り組める日々の生活改善を行うことが必要となります。つまり、セキュリティ対策で考えるとレガシーな“受け身のセキュリティ対策”だけではなく、新しい技術や知恵を積極的に取り入れて効率化を図り、“サイバー攻撃に立ち向かう組織体制”を構築することが求められます。これまで定説として言われてきた「事故前提社会のセキュリティ対策」という考えだけで構成されたセキュリティモデルでは時代に合わなくなっていると考えています。

このような時代背景を見据えて、当センターではこれまでCYBER GRID JOURNAL Vol.4^①で紹介した予兆・予測につながる取り組みとして「脅威情報」というテーマで研究開発を進めてまいりました。そして次のステップとして、「アクティブ・サイバー・ディフェンス」というテーマで研究開発をスタートさせる計画です。これは対策防御をする立場の組織が、事故発生後だけでなく、事故が起こる前から脅威や脆弱性の情報収集とその活用を行って、変化への対応など積極的に対策を講じて事故を未然に防いでいく、あるいはこれまでは見つけれなかった事故を早期発見するという取り組みを指し、これを実施しているか否かが、今後組織のセキュリティ対策の明暗を分けると考えています。

① https://www.lac.co.jp/lacwatch/report/20170901_001374.html

ニッポンのミライを救う サイバーセキュリティにおける 「未病改善」の考え

マルウェアの DNA鑑定で システムを自動判定する

サイバー・グリッド・ジャパン 次世代技術開発センター長 小笠原 恒雄

現在の犯罪捜査においては、DNA鑑定が犯人の特定や犯罪事実の証明に欠かせないものとなっていますが、「マルウェアのDNA鑑定」によって種類やサイバー攻撃グループなどのマルウェア特性を判定する技術をご存じでしょうか。ここでは、この技術を知っていただくために当センターが研究開発で使用している「Intezer Analyze^①」について紹介したいと思います。

マルウェア解析職人の技術を自動化した 「Intezer Analyze」

「Intezer Analyze」は、クラウド上でマルウェアと思われるプログラムをスキャンすることで、そのプログラムがマルウェアなのか、マルウェアだった場合、その種類やどのサイバー攻撃グループが使用している可能性が高いのかなどの特性を判定するサービスです。このサービスのユニークな点は、マルウェアの判定方法にあります。「Genome Database」と呼ばれる“プログラムのゲノム”に相当するプログラムの特徴的なコードや文字列を蓄積したデータベースとの照合により、対象プログラムが悪性か良性かを判定します。この判定技術をDNA鑑定に見立てており、対象のマルウェア内の作りが過去に発見されたマルウェアとどのくらい類似性があるのかを数値化し、マルウェア特性の判定結果を導き出します。

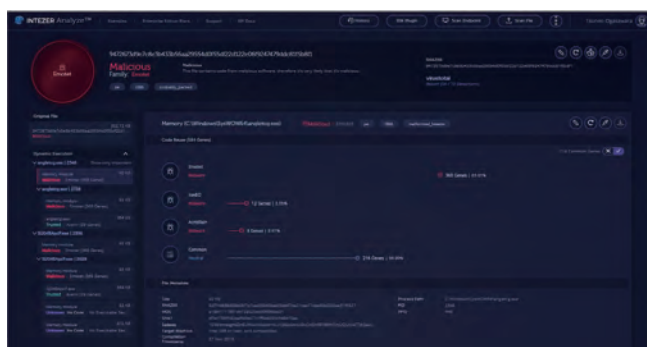


図1 マルウェア「EMOTET(エモテット)」として判定されたときの「Intezer Analyze」の画面。画面中央に別プログラムとのコード類似性を示す棒グラフがパーセンテージ表示されている

つまり、プログラムの「コードの再利用」に着目しているわけですが、これはマルウェア解析者と同じアプローチをとっています。マルウェア解析者は、さまざまなツールを駆使し、コードを読み解きます。そして図2に示すようなイメージで、過去に調べたプログラムの構造やコードと比較しながら

マルウェア特性の判定を行います。「Intezer Analyze」はこれに近い作業工程をシステム化して提供しているのです。バックグラウンドでは、日々数万のプログラムを自動収集・解析し、「Genome Database」を成長させていると聞きます。

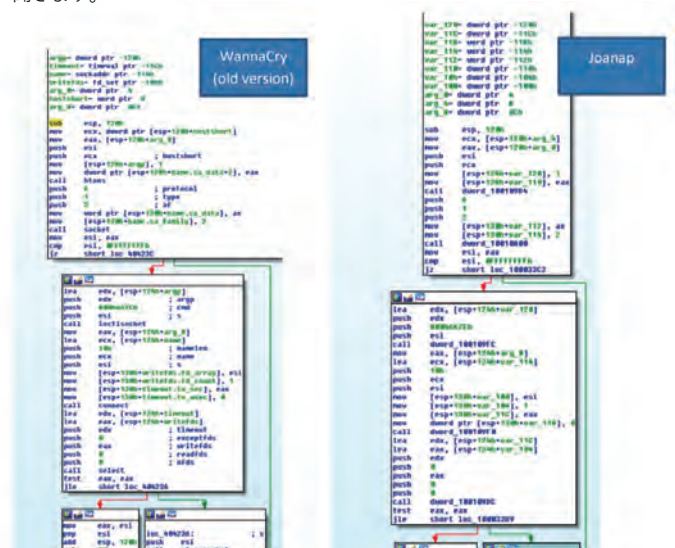


図2 Intezer社が公開したランサムウェア「WannaCry」に関する分析レポート^②からの抜粋。この図は「WannaCry」と北朝鮮が関与しているとされるマルウェア「Joanap」とのコードの類似性を示している

マルウェアの自動解析や分類に関連する研究は、さまざまなアプローチで行われており、私たちも取り組んでいました。そういう中で「Intezer Analyze」を知ったのは2年ほど前のことです。当時はIntezer社がサービスを本格化する時期でしたが、彼らのシステムやサービス概要、コンセプトを聞いて構想がかなり進んでいて洗練されていることを知りました。私もそのコンセプトや構想には賛同できたので、当社の研究開発やシステムとの連携を図りたいと考え、それから検証評価を開始しました。

① <https://analyze.intezer.com/>

② <http://www.intezer.com/wp-content/uploads/2017/07/Intezer-WannaCry.pdf>

APT攻撃で使用されたマルウェアを解析してみる

判定結果の精度を確認するため、日本をターゲットとするサイバー攻撃グループがAPT攻撃で使用したとされるマルウェアのサンプル106件③を対象とし、解析をかけました。その時の結果を紹介したいと思います。

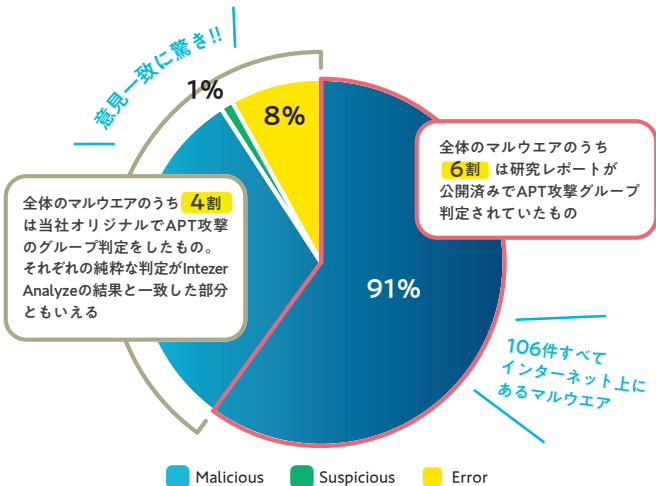


図 3

APT攻撃で使用されたマルウェアの「Intezer Analyze」での判定結果 (2017年11月当社調べ)

マルウェアが悪性か否かを解析したところ、図3に示すとおり、マルウェアのサンプル106件中、うち8つのマルウェアは「Intezer Analyze」の制限サイズ50MBを超えるファイルのため、解析エラーとなりましたが、97件は悪性(Malicious)と判定され、残りの1件は悪性の疑いがある(Suspicious)という結果になりました。解析エラーとなったサンプルを除く計98件のマルウェアについて、想定するAPT攻撃で使用したマルウェアと判定できるのか、同じサンプルで2017年と2019年の2度にわたって確認を行いました。その結果が図4となります。

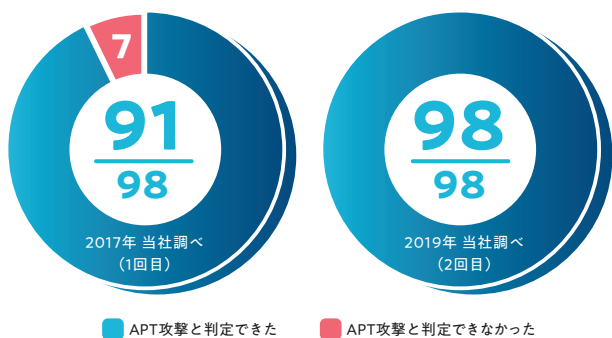


図 4

「Intezer Analyze」でサンプル全106件中 98件のマルウェア (Malicious/Suspicious判定されたもの)の1回目と2回目の判定結果の遷移

以前は、一部APT攻撃と判定できないマルウェアが存在しましたが、今回2回目の調査では、全てのマルウェアがAPT攻撃と判定できるようになりました。実は1回目の調査でAPT攻撃と判定できなかった7件は全てパッカーにより難読化が施されていたマルウェアでした。パッカーとは、プログラムの圧縮や難読化を実現することができるもので、多くのマルウェアで使われています。これによってプログラム本来の構造と内容が隠されてしまい、プログラムのDNA鑑定が上手くできなかったものと推測されます。それが2回目の調査時点では、大幅な強化(=アンパック機能とメモリ解析機能のリリース)

が行われており、プログラム本来に対するDNA鑑定ができるように進化していました。

研究開発で培ったノウハウをセキュリティ対策の現場で活かす

私たちの研究開発の中では、「サンドボックス」と呼ばれるプログラムの動作振る舞いが確認できるシステムと併用して「Intezer Analyze」を使用しています。これと似たシステムが図5に示す現在当社サイトにて公開中の「FalconNest④」で提供するMalware Analyzer(MA)です。

私たちは、日々の研究活動でさまざまな情報源から脅威情報を収集しています。その中には正体不明のプログラムが含まれていることもあるため、プログラムファイルが入手できた場合は全てマルウェアかどうかを判定し、もしマルウェアだった場合は通信先情報などを含む解析結果にタグを付けて自動分類を行い、脅威情報としてデータベースに蓄積しています。これにより、例えばAPT攻撃で使われた疑いがある緊急性の高いマルウェアにもすぐに対処することができ、迅速に次の分析ステップにつなげることができるようになりました。また、「Intezer Analyze」の最近の機能アップデートでは、ファイルの特定が難しい場合でもスキャンできるように感染端末上でのメモリ解析をサポートしたので、今後は最新のマルウェア感染手口を解明する研究などに活用したいと考えています。



図 5

当社サイトにて公開中の無料調査ツール「FalconNest - Malware Analyzer (MA)」の画面。オプション「コードインテリジェンス分析を使用する」を付けることで、「Intezer Analyze」の結果を取得することができる

読者の皆さまの組織のマルウェア対策はいかがでしょうか。マルウェアは何件検出されているか把握していますか？ もし、その中で緊急性の高いマルウェアが検出されていたらどうでしょう。仮に組織内で1つでも見つかり、深刻な事態になる恐れもあり、このような場合インシデント対応による的確な判断と行動が求められます。また、検出・駆除されたからといって、インシデント対応を完了していないでしょうか。念のために、当該端末をクリーンインストールしたとしても、見つかったマルウェアはすでに残骸で、攻撃者は他の端末で密かに活動しているかもしれません。

このように、的確な判断を行うには、これまでは高い知識と経験を備えるスタッフが必要とされていました。しかし、今回紹介した「Intezer Analyze」に限らず、今では高い技術力をサービスやツールで補うことができるので、システム化を図ることで、組織内の取り組みで知見(=インテリジェンス)を獲得し、積極的な対策を推進する体制を組むことが、ある程度はできるようになってきました。ただし、このような取り組みは、日本国内ではなかなか普及していないのが現状です。私たちは、研究開発で成果を挙げることに加え、その過程で培ったノウハウなども含めて事業部門や研究パートナーと連携し、お客さまが抱えるさまざまな問題を解決できる存在になりたいと考えています。

③ 本調査では、「APT10」「APT12」「Tick」と呼ばれるサイバー攻撃グループが使用したとされる公開情報から得たマルウェアを使用

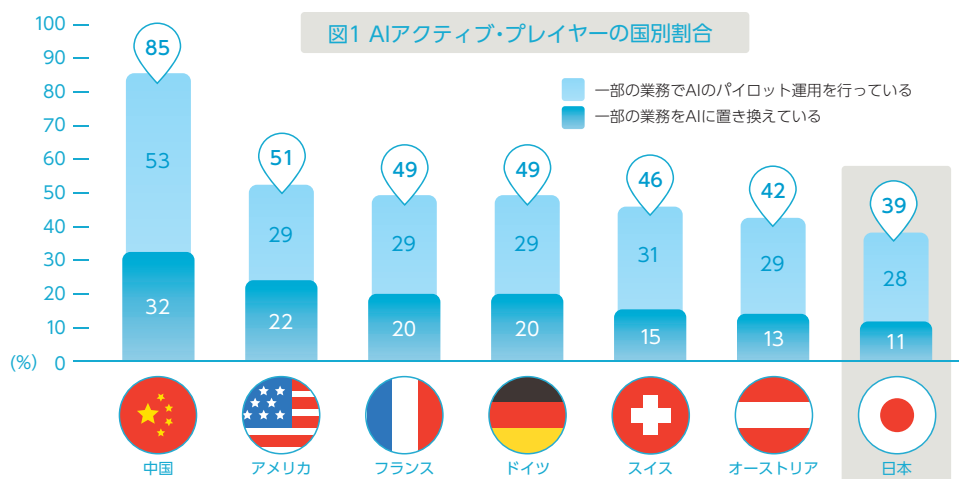
④ <https://tools.lac.co.jp/>



これまでなかった「脅威予測」をAIで

近 年、あらゆる場面で「AI」という言葉を聞くようになりました。自動運転、不良品検出、がんの早期発見、タクシーの需要予測、AIスピーカー、ロボット掃除機、将棋ソフトなど、AI技術の活用には今や数えきれない事例があります。2018年に行われたアンケート調査では、一部の業務をAIに置き換えている日本企業は11%、一部の業務でパイロット運用を行っている日本企業は28%という結果が出ており(図1)、AIの導入拡大が予想されます。

さて、サイバーセキュリティ分野においては、どのようにAI技術を活用することができるでしょうか。本特集では、次世代技術開発センターで研究を進めている「脅威予測」について説明します。



(出典) ポストンコンサルティンググループ(2018)「企業の人工知能(AI)の導入状況に関する各国調査」

※AIアクティブ・プレイヤーの定義は、「一部の業務をAIに置き換えている」または「一部の業務でAIのパイロット運用を行っている」のいずれかに該当し、かつ自社のAI導入を「概ね成功している」と評価した企業

当社におけるAI技術の活用事例

- 九州工業大学とAIを活用したサイバー防御における共同研究(ラック)
https://www.lac.co.jp/news/2019/08/29_press_01.html
- Instagram画像分析ツール「Image Projector」(ジャパン・カレント)
<https://www.japan-current.com/news/detail/20191015.html>
- 企業の保持する大量の画像や動画情報から、指定した画像に類似する画像を抽出するサービス「AI画像検索サービス」(ジャパン・カレント)
<https://www.japan-current.com/news/detail/20180910.html>
- 一般消費者の動向を把握するマーケティング提案向けInstagram解析ツール「Hugin(フギン)」(ジャパン・カレント)
<https://www.japan-current.com/news/detail/20171108.html>
- 商品やサービスの消費動向やSNS上のトレンドを「見える化」するSNS画像解析サービス(ジャパン・カレント)
<https://www.japan-current.com/news/detail/20170718.html>

国内他社におけるAI技術の活用事例(サイバーセキュリティ分野)

- セキュリティ監視サービスにAI技術を活用した脅威分析システムを導入 - NEC
https://jpn.nec.com/press/201705/20170508_02.html
- サイバー攻撃への対処要否を判断するAI技術を開発 - 富士通
<https://pr.fujitsu.com/jp/news/2019/01/22-2.html>
- セキュリティ監視業務効率化AIソリューション - 日立
https://www.hitachi.co.jp/products/it/security/solution/securitymanagement/ai_utilizing/index.html
- サイバー・セキュリティ対策向けのクラウドベースのコミュニティ・プラットフォーム「IBM Security Connect」 - IBM
<https://www-03.ibm.com/press/jp/ja/pressrelease/54427.wss>
- Webアプリケーションの脆弱性スキャンAI「SAIVS」 - 三井物産セキュアディレクション株式会社
https://www.mbsd.jp/blog/20160113_2.html
- 機械学習ツールによる異常検出の効率化「Machine Learning Toolkit (MLTK)」 - Splunk
https://www.splunk.com/ja_jp/software/splunk-enterprise/machine-learning.html

どこまで可能なのか～

庄司 勝哉

サイバー・グリッド・ジャパン
次世代技術開発センター
リサーチャー



「脅威予測」の実現

脅 威予測について簡単に説明すると、「サイバーセキュリティ上の脅威を予見すること」です。例えば、「このIPを使って攻撃してくる」「このような攻撃コードを使って攻撃してくる」「サイバー攻撃キャンペーンが行われる」「APT攻撃グループがこの企業をターゲットに攻撃してくる」といった予兆を検知します。脅威予測を実現するには、脅威情報の収集と分析が必要です。

脅威情報の収集

サ イバー攻撃が行われると、IoC (Indicators of Compromise) という、攻撃の痕跡情報が残ります。IoCには、次のようなものがあります。

- 攻撃元やマルウェア通信先などの不正なアドレス/ドメイン名
- 攻撃に使われたURLやメールアドレス
- 身代金の振込先ビットコインアドレス
- 攻撃に使われたマルウェアのハッシュ値や特性
- 悪用された脆弱性のCVE番号(脆弱性を一意に判別する番号)

次世代技術開発センターでは、上記のようなIoC情報をさまざまな情報源から収集しています。当社のセキュリティ監視・運用サービスであるJSOCの検知データや、サイバー救急センターのマルウェア分析データ、サイバー・グリッド・ジャパンが独自に収集した情報、外部組織から提供を受けた情報などです。収集されたIoC情報は脅威情報として蓄積します。サイバー・グリッド・ジャパンが独自に収集した情報の中には、世界各国のセキュリティリサーチャーやセキュリティベンダーのレポートといった、一般に公開されている情報をもとにしたOSINT (Open Source INTelligence) が含まれています。OSINTは、無料で手に入る情報ながら即時性のある情報を入手できる、重要な情報源です。

図2 脅威情報の収集



OSINTの情報源は、主にWebページ (HTML文書) です。脅威情報には、情報を分類するためのタグを付けていますが、膨大な数のWebページを人が一つずつ確認するのは現実的ではありません。そのため、AIを活用してWebページの文章からタグを選定する試みを行っています。

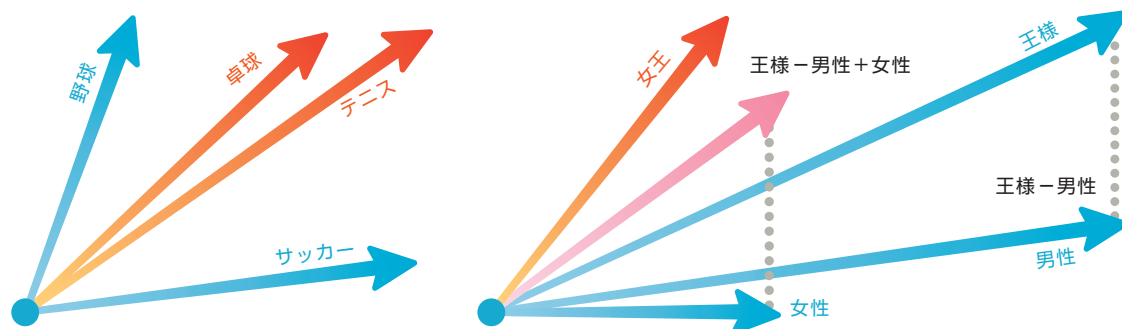


AIによる脅威予測 ～どこまで可能なのか～

文章からタグを生成するためには、単語の意味を知る必要があります。コンピューターが単語の意味を扱うにはどうすればいいでしょうか。近年では、AI技術を活用して単語をベクトル化することにより、単語の意味を扱う技術がよく用いられています。「単語をベクトル化する」と言われても、ほとんどの方がピンとこないと思います。以下に例を出して説明します。

「テニス」と「卓球」という単語をそれぞれベクトル化するとどうなるでしょうか。「テニス」と「卓球」はどちらもラケットでボールを打つスポーツです。中央にネットがある、試合の形式はシングルス・ダブルス・混合ダブルスがある、自分か相手のサーブからボールを打ち合う、など共通することは多々あります。すると、お互いのベクトル方向は近くなります。つまり、似ている単語は近いベクトル方向になる、ということです。また、単語のベクトルは足したり引いたりすることができます。例えば、「王様」－「男性」＋「女性」を計算すると、「女王」のベクトル方向に最も近くなります。

図3 単語のベクトル化



単語の意味をベクトルに表してしまえば、コンピューターで容易に計算できるようになります。例えば、文章から「情報セキュリティ」に関連するワードを抽出したい場合は、「情報」と「セキュリティ」を足し合わせたベクトルと文章内の各単語のベクトル方向が近いものが、「情報セキュリティ」に関連するワードであると判断できます。このように単語のベクトルを活用して、文章に合ったタグを選定します。

実は、AI技術を利用して文章を解析するサービスはいくつか存在します。Google社が提供しているNatural Language APIがその一例です。しかし、それらのサービスはサイバーセキュリティに特化したものではありません。OSINTのタグには、脆弱性の名称や、マルウェア名、サイバー攻撃グループ名を入れたいところですが、単純にキーワードを抜き出すだけでは、そのような言葉が入るとは限りません。そのため、サイバーセキュリティの関連文書から学習する、新しい脆弱性の名称やマルウェア名を検出する、といった独自の実装でOSINTのタグ付けを試みています。

図4は、開発している文章解析処理の結果の一例です。ラックが公開した、「PoshC2」に関する記事①について、情報セキュリティに関連したキーワードをランキングしたものです。この結果を見ると、サイバー攻撃グループであるAPT33やC2フレームワークのPoshC2が比較的上位になっており、情報セキュリティとの関連が結果に表れていると考えます。しかし、TOP5を見ると、一見セキュリティとは関連がないワードが並んでおり、どれも文章の区切り方がおかしくなっています。これらの問題を解決するため、「情報セキュリティ」以外のワードとの関連を評価に加える、文章の係り受けから文章の区切りを決める、といったアプローチを行い、さらに精度を改善していきたいと思っています。

図4 文章解析結果の一例

(原文)

ラックの石川です。

私の所属する脅威分析チームでは、日本を標的とする様々な攻撃を日々調査しています。その過程で、オープンソースで公開されているPoshC2*1を悪用した攻撃を、今年(2019年)1月頃から確認しています。また、2018年12月末のFireEyeのブログ*2によると、イラン政府の関与が疑われる攻撃者グループAPT33*3が、PoshC2をエンジニアリング業界に対する一連の攻撃の中で悪用したとも報告されており、PoshC2がサイバー攻撃で使用する事例を最近多く目にする機会があります。(以下省略)

① https://www.lac.co.jp/lacwatch/people/20190213_001770.html



[情報セキュリティに関するキーワードのランキング]

1. 正初期リクエスト例2.AWS上
2. 規クラウドサービス(GCP=GoogleCloudPlatform
3. CoreDropper(上:デコード後
4. 実行画面(v3
5. コード(一部抜粋)攻撃手口2
- ...
20. 攻撃者グループAPT33
- ...
72. PoshC2
- ...
230. 月頃

脅威情報の分析

収 集した脅威情報を分析し、攻撃の予兆を検知します。研究・開発中の脆弱性関連情報分析とAPT情報分析をご紹介します。

脆弱性関連情報分析では、脆弱性が発見されてから修正パッチ提供が行われるまでの時系列や、攻撃発生の有無、攻撃方法などを分析します。この機能を活用すると、「ゼロデイ攻撃」と呼ばれる攻撃の予兆を検知することができます。

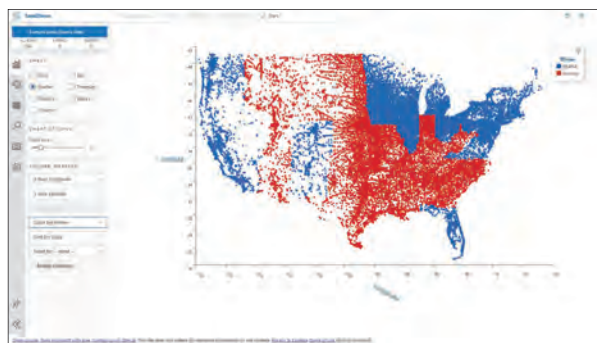
ゼロデイ攻撃とは、脆弱性が発見されて修正パッチが提供されるより前に、その脆弱性を悪用する攻撃のことです。この攻撃は、サーバーやPC、ネットワーク機器のOSプログラムやソフトウェアの修正パッチが提供されてすぐに適用する運用になっていたとしても、防ぐことができません。もし修正パッチ未提供の脆弱性を悪用した攻撃が発生していれば、対象機器やソフトウェアを使用しているユーザーにいち早く注意喚起をすることができます。また、攻撃方法が分かれば、その攻撃をファイアウォールやウイルス対策ソフトで防ぐということも可能になるでしょう。

APT情報分析では、各APTの活動を分析します。APT (Advanced Persistent Threat) とは、サイバー攻撃グループのことを指し、「APT」に番号を付けて判別しています。日本では、中国を拠点とするサイバー攻撃グループとされるAPT10が特に有名です。

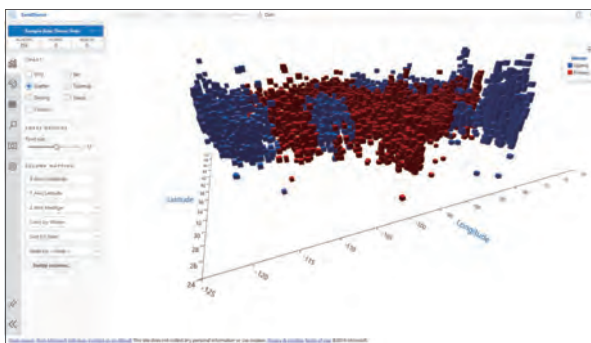
APTによる攻撃では、標的型メール攻撃と呼ばれる攻撃がよく用いられます。標的型メール攻撃とは、実在する組織や実在する業務の担当者へのなりすましなどにより、メールの添付ファイルや悪意のあるURLを開かせ、マルウェアに感染させる攻撃です。攻撃者は、標的型メール攻撃で感染させたマルウェアを通して、機密情報や個人情報の窃取や、破壊活動などを行います。もし、あるAPTが活発に活動していれば、標的型メール攻撃に気を付けるよう、注意を促すことができます。

脅威情報の分析結果については図5や図6のようなアプリケーションで可視化をし、さまざまな角度から分析ができる環境づくりに取り組もうと考えています。図5は、Microsoft社が公開している、「SandDance」というデータ可視化Webアプリケーションです。SandDanceでは、表示するデータや表現の種類、フィルターなどを容易に設定し、データ表示できるインターフェースを提供します。図6は、Intezer社が公開している、「APT-ecosystem」というAPTが使用するマルウェアの関連性を可視化するWebアプリケーションです。

図5 データ可視化アプリケーション[SandDance]



米大統領選挙の勝敗をプロットしたもの(2D)



左図に加えて平均年齢を高さに設定したもの(3D)

図6 APTの可視化アプリケーション[APT-ecosystem]



ロシアのAPT情報を可視化したもの

まとめ

こ れまでのサイバーセキュリティは、ネットワーク監視、マルウェア分析、脆弱性診断といった分野をそれぞれ深堀りすることで知見を深めてきました。対して、本稿で述べた「脅威予測」は、それぞれの知見を集めてさまざまな角度から分析することで新しい知見を得る、これまでにない先進的な取り組みです。AI技術は、多くの種類のデータから特徴を見つけ、予測・分類することを得意としており、「脅威予測」と相性の良い技術だと考えます。その活用についてはまだまだ道半ばですが、現在、着実に研究を進めているところです。近年大きな発展を遂げているAI技術とともに「脅威予測」を大きく発展させ、サイバーセキュリティにとって、なくてはならない存在にしていきたいと思います。

座 談 会



研究開発の これまでとこれから

～ラックのノウハウと研究の融合で「先回り防御」を実現したい～

サイバー空間における攻撃の手法は、日々進化を続けている。姿の見えない脅威に立ち向かうためには、攻撃されてからの対応ではなく「先回りの対処」が不可欠だ。社内外の組織と連携し、サイバー攻撃の予兆・予測を実現するための技術開発を行う、ラックの次世代技術開発センター。「サイバー脅威インテリジェンス」の最前線で脅威と戦う4人のスタッフが、研究に注ぐ思いや意見を語り合った。

一 藁 俊 裕

Toshihiro Ichiwara

サイバー・グリッド・ジャパン
次世代技術開発センター

2006年入社。システムインテグレーション部門で6年間開発とマネジメント業務に従事した後、研究職へ転向。現在は、視覚障がいや有するメンバーでは難しいサイバー管理やネットワーク運用、開発・テストに関するアドバイスなど主にサポート的側面で参画している。

外 谷 渉

Sho Sotoya

サイバー・グリッド・ジャパン
次世代技術開発センター

2009年入社。システムインテグレーション部門で3年間、開発業務に従事した後、自社の監視サービス用ログ分析システムの開発を3年間担当。2015年より研究開発に従事。全盲の雇用促進・人材育成のため、自身の経験やスキルを社内外に発信するメディア対応や意見交換会等の活動も積極的にしている。最近、ラック囲碁サークルの代表に就任。

高 原 健

Ken Takahara

サイバー・グリッド・ジャパン
次世代技術開発センター

2006年4月、大手電機メーカーの情報システムのグループ会社に入社。NGN(Next Generation Network)やバイオメトリクス技術の研究開発、ISP向けポータルサイトや電力管理システムなどさまざまなプロジェクトで実績を上げる。2019年4月ラックに入社。強度の弱視で、拡大表示とスクリーンリーダーを併用して、JavaやPython、JavaScriptなどのさまざまな開発言語を駆使して、フルスタックのエンジニアとして研究開発を担当している。

三 川 草 平

Sohei Mitsukawa

サイバー・グリッド・ジャパン
次世代技術開発センター

2016年、広告メーカーの特例子会社に新卒として採用。IT事務の部署に2年間在籍し、Excelのマクロ開発などを担当。2017年末頃、社外の視覚障がい者向け意見交換会に参加し、主催メンバーの外谷と知り合う。そのつながりもあり2018年6月、ラックに入社、現在の部署に配属。5歳の頃から全盲の視覚障がいを持ち、点字ディスプレイとスクリーンリーダーを利用して研究開発に当たる。



司 会 船 引 裕 司

Yuji Funabiki

取締役 常務執行役員
サイバー・グリッド・ジャパン GM

1988年、国際電信電話株式会社(現KDDI株式会社)入社。主に、事業用電気通信設備の開発、運用に従事し、グローバルネットワークオペレーションセンター長、グローバルICT技術部長などを歴任。2019年4月、ラック常務執行役員に就任。2019年6月より現職。



蓄積したデータの 研究によって生み出された アプリケーション

LAC Journey

船引:今日は、サイバー・グリッド・ジャパン次世代技術開発センターに所属する4人のメンバーに、研究活動の内容や研究開発に対する思い、ご自身の働き方などについて語ってほしいと思います、お集まりいただきました。ではまず、自己紹介からお願いします。

外谷:外谷渉です。こちらの研究には、研究が始まった2017年から携わっていて、主にシステム開発を中心に開発全般を担当しています。

三川:三川草平と申します。2018年6月に入社しました。前職ではITの経験がほとんどなかったのですが、日々勉強しながら勤務しています。今はPython(パイソン)^①のプログラムの作成やデータベースの集計など、全体的な管理をしています。

一葉:一葉です。この中では、一番社歴が長いと思います。もともとはSIの開発チームにいて、2017年にこちらに異動してきました。このチームは視覚障がいをお持ちの方が多いので、皆さんが担当できない物理的な環境のメンテナンスや構築をメインに担当しています。

高原:高原健と申します。ラックには2019年の4月に入社いたしました。前職でも研究の仕事をしていました。多くのアナリストに使ってもらえることを目指して、脅威情報の収集や検索プログラム、ツールの開発を行っています。プログラム歴は結構長く、いろいろな言語を使ってシステムを作っています。

船引:ありがとうございます。皆さんの研究の大きなテーマは「サイバー攻撃の予兆・予測」ですが、一体どのような研究をしているのでしょうか？

外谷:今のセキュリティというのは、「攻撃を受けたから防御する」といった後追いの対策がメインになっていますが、我々の研究は、「今後こういう攻撃が来るであろう」とデータ分析に基づく予測をして、対策や防御をする人に提示をすることを目指しています。研究活動の道のりはだいぶ遠いと思っていますが、これを実現する要素技術の1つとして「サイバー脅威インテリジェンス^②」がとても重要と考えています。そのため、これまでの研究ではこの活動につながるデータの収集と分析をメインテーマとして取り組んでいます。独自のシステムにより収集したマルウェア等に関する研究データと、OSINT^③といわれるオープンソース、主にはインターネット上で収集できる情報ですが、大きくはこの2つのテーマでデータを蓄積して、分析しています。

船引:データの蓄積はどのように行っているのでしょうか。

三川:OSINTの収集に関しては、インターネット上に公開され利用可能なサイバー攻撃に関わる情報を集めるプログラムを作って対応し、IoC^④と呼ばれる、不正なIPアドレスやドメイン、マルウェアのハッシュ値といったものをひたすら溜めています。これに独自の研究で収集したデータやラックの事業部門から提供された分析済みのデータなどを合わせると、件数にして2億5000万件ほどのデータがMISP^⑤というデータベースに蓄積されています。

外谷:研究がスタートしてから3年近くたち、

さまざまな情報源からのデータがだいぶ蓄積されてきました。今までは、情報の検索や利用には特殊なシステムを使わなければならなかったのですが、実際にビジネスや事業に使えるような使い勝手のよい環境にするために検証を重ね、高原が中心となってLAC JourneyというWebアプリケーションを作成し、2019年10月に社内で公開しました。

高原:2億5000万件という大量のデータから有用な情報を抽出するためには、検索の高速性や検索の容易性などを確保しなければなりません。LAC Journeyは現在4つのMISPで構築されていますが、4つを並列する処理で検索を行い、検索が終了したものから順次画面に表示されるような仕組みにしました。検索がすべて終了してから画面に表示されるのではなく、検索が終わったところから順次表示されるので、アナリストが分析にかかる時間を大幅に短縮することが可能になっています。容易性という点では、必要な情報を入力して検索ボタンを押すだけ、という画面の作りにも配慮しました。オープンな情報だけでなく、公開制限があって関係者に限定した情報も取り扱っていますので、情報の種類と検索者の権限に応じた適切な表示がなされるよう考慮しつつシステムを構築しています。

一葉:LAC Journeyの裏側では、データベースや検索エンジンが動いています。これらを動かすためには、サーバーやネットワークの構築・拡張や管理が必要になりますが、こういった業務は物理的な側面が強いので、視覚に障がいのあるメンバーに代わって私がサポートしています。そもそも各サーバーに接続できればLAC Journeyは稼働しませんから、日々、サーバールームにこもって線をつなぐといったような作業は、私がメインで担当しています。

① プログラミング言語の一種 ② Cyber Threat intelligence／サイバー攻撃という脅威に関する情報を集約・蓄積・分析し、セキュリティ対策に活かす取り組み

③ open source intelligence／公開情報

④ Indicators of Compromise(侵害指標)／サイバー攻撃の痕跡情報

⑤ Malware Information Sharing Platform／セキュリティ上で脅威のある情報を蓄積・検索できるシステム(<https://www.misp-project.org/>)

ラック独自に得られた 「確かな情報」との コラボレーションが 先回りの対処を実現する

船引:いわゆるインテリジェンスの研究というものは、今や多くの企業で行われています。次世代技術開発センターの研究には、どんな独自性や特徴があるのでしょうか。

外谷:当社のJSOCやサイバー救急センターなどの事業部門では、サービス提供を通じて独自のノウハウを多く持っています。そういった確かな情報と、我々が蓄積している研究データやOSINTを紐づけることで、他社にはできない分析や、新たなインテリジェンスの創出が可能ではないかと考えています。また、当社の各アナリストが持っているさまざまな属人的ノウハウをシステムに取り込むことができれば、分析の自動化にもつながり、大きな強みになると思っています。

三川:インターネット上では世界中のリサーチャーによって日々脅威情報が発信されています。そういうものを迅速に取得して独自のデータと照合することで、確かな情報をスピード感を持って知らせることができ、攻撃による被害を最小限に抑えることができるのではないのでしょうか。

高原:ゼロデイ攻撃が発見されて修正パッチが提供されるまでに、エクスプロイト(脆弱性を悪用し攻撃を成立するためのスクリプトやプログラム)が公開されてしまうことがあります。

この情報が一番被害を拡大させる原因になるわけですが、対策する側は、こういった状況になるべく早い段階で手間をかけることなく、影響があるかどうかを把握し、影響がある場合は対策防御に迅速につなげるという活動が非常に大事になってくると思います。

船引:そのような環境を実現するための我々の課題として、どのようなものがありますか。

外谷:集めた情報はノイズを含んでいるため、活用の幅が狭いのが現状です。まずはノイズを除去してデータ品質を高めるのが第一だと思います。また、単純にIoCを収集し蓄積するだけでは、どんな攻撃属性やマルウェアの種類と関連があるのか、うまく情報を識別できないことがあるので、今後はAIを使った情報分析も必要だと思っています。

船引:AIをどのように使っていくのでしょうか。

外谷:まずは脅威情報の分類に使いたいと考えています。例えば、どこかのブログから情報を取ってきたときに今わかることは、「あくまでこれは英語のマルウェアのニュース情報です」ということに過ぎません。感染を拡大させているEMOTET(エモテット)というマルウェアがありますが、「この情報はそういった特定のマルウェアに関連している」だとか、「最近活動を活発化させているサイバー攻撃グループAPT10のキャンペーンに関するものだ」とか、具体的な内容とIoCとをうまく紐づけするのに活用できるのではないかと考えています。

三川:EMOTETに関する情報を集めようと思っても、この情報が本当にEMOTETに関するものなのかの判断がつかなければ宝の持ち

腐れですから。

一藁:今は、オンプレミスとクラウドのハイブリッド構成でシステム運用をしている状況なのですが、クラウド移行のおかげで可用性と拡張性にも優れた環境になってきました。各メンバーはコーディングに費やす時間が多いので、システムやネットワークの構築や変更にかかる業務負荷が課題でしたが、だいぶ改善されました。メンバーからのリクエストで一時的にシステムをスケールアウトするといったことも容易になり、健常者が不在でもある程度設定が可能になるなど運用面でもメリットが出ています。今後さらに扱うデータが増えていくので、分析基盤をもっとスマートにして、今のチームの特性が活かせる環境づくりを工夫し、研究のスピードアップができればと思っています。

視覚障がいの有無に

かかわらず、同じように

世界中の安全に

貢献できるという仕事

船引:皆さんは、非常に先端的で難しい研究を行っていると思うのですが、どういった思いや希望を持って仕事に向かっているのでしょうか。

三川:セキュリティ研究という業務は、目に見えないような気がしています。私は視覚に障がいがあって全盲なのですが、セキュリティやデータ収集といったことに関しては割合、力を発揮しやすいので、自分の力を社会貢献に生かせることは非常にモチベーションになっています。

高原:私は学生時代の頃から、ソフトウェアやシステム開発するのがとにかく楽しかったんです。開発には大変な労力や知識を使うので、新しいことを吸収するという苦勞を伴うのですが、システムが完成して動いたときのうれしさ、そしてそれを使ってくれた人が「ありがとう」と感謝してくれる。それを目指してものづくりをしていくことに幸せを感じています。研究そのものというよりも、研究の中でソフトの開発を楽しみながら、一緒に社会に貢献していくことが働く原動力になっているのかなと思います。



脅威情報ポータルサイト「LAC Journey」のMISP横断検索が行えるWebUI画面。社内ではOffice365を導入しているため、SharePointでサイトを作成しており、WebUIはPythonの開発フレームワークであるDjangoとJavaScriptのフレームワークReactを使用して開発。WebUIだけではなくAPIによるデータ連携機能も提供する。

一葉:先ほどお話があった研究の独自性ということにも関わってくる話なのかもしれないですけど、事業部門との連携には今の形の逆もあると思っています。具体的にいうと、今は事業部門から分析されたデータの提供を受けていますが、それを我々の研究で分析して、アラートを発信できるようにして、それを事業部門に還元するというような連携です。数千社にもものぼるラックのお客さまに先回り情報をリアルタイムで発信できるようにすれば、それがラックの大きな強みになるのではないかと思います。

外谷:そうですね。あとは標的型攻撃のような、ターゲットとなる組織内でしかわからない攻撃がどんどん進化してきているので、我々が生み出す強みをたくさんの人に使っていただき、潜在的な脅威や最新の攻撃に対抗する手段を系統的にすぐ提供できるような分析基盤を実現したいです。攻撃が起きてからの対処ではなく、被害を未然に防ぐための対処につなげて積極的思考でセキュリティ対策や防御を実現する「アクティブ・サイバー・ディフェンス」の概念を提言していければと考えています。今後はこのテーマで研究を進めていく予定です。

一葉:今までの仕事は、お客さまと一対一で向き合うことが多かったのですが、今の研究は日本中、ひいては世界中の人の安全を守るということに関わるので、規模が大きくなってきたなというのは実感しています。今はまだまだ構築中ですが、その根幹を一步一步大きくしていこうという研究だということにやりがいを感じますね。

船引:総合すると大きく2つのことが語られているように思います。1つは、会社ですから事業

に貢献し、お客さまの役に立ち、日本のインフラをサイバー攻撃から守るという使命感。もう1つは、このチームは視覚障がい者が多いので、同じようなハンディを持った方に対してこのメッセージを発したい、ということです。健常者であろうが、障がい者であろうが、作ったものが動くということは非常に面白いし、こういったことができるんだということは積極的に発信していきたいですね。

外谷:ラックは、オンラインでの情報共有や会議など、リモートワークのできる環境が非常に整っていると思います。今日は座談会のために皆が顔を合わせていますが、普段は誰かしらがテレワークをしている、という自由度を持って仕事できています。効率的に、生産性の高い仕事ができるこの環境は、とても働きやすいです。三川:自分と同じ視覚障がい者の方が活躍している環境にも、非常に心強さを感じています。ビデオ会議などで社員全員に対して情報発信をする機会があるというのも楽しいですね。

一葉:目の前のお客さまが欲しいものを作るということではなく、「これがあれば世界中が助かるだろう」とか、「5年後、10年後にこれがあったらきっと役に立つ」というような研究はある意味壮大です。メンバーと一緒に、夢みたいな話をゲラゲラ笑いながら語り合えるというのも、モチベーションの1つかなと思います。研究自体は徐々に、段階的に進むわけですが、LAC Journeyをリリースできて、反響をもらえたというような一步一步、前に進んでいる感覚が後押しをしてくれているような気がします。

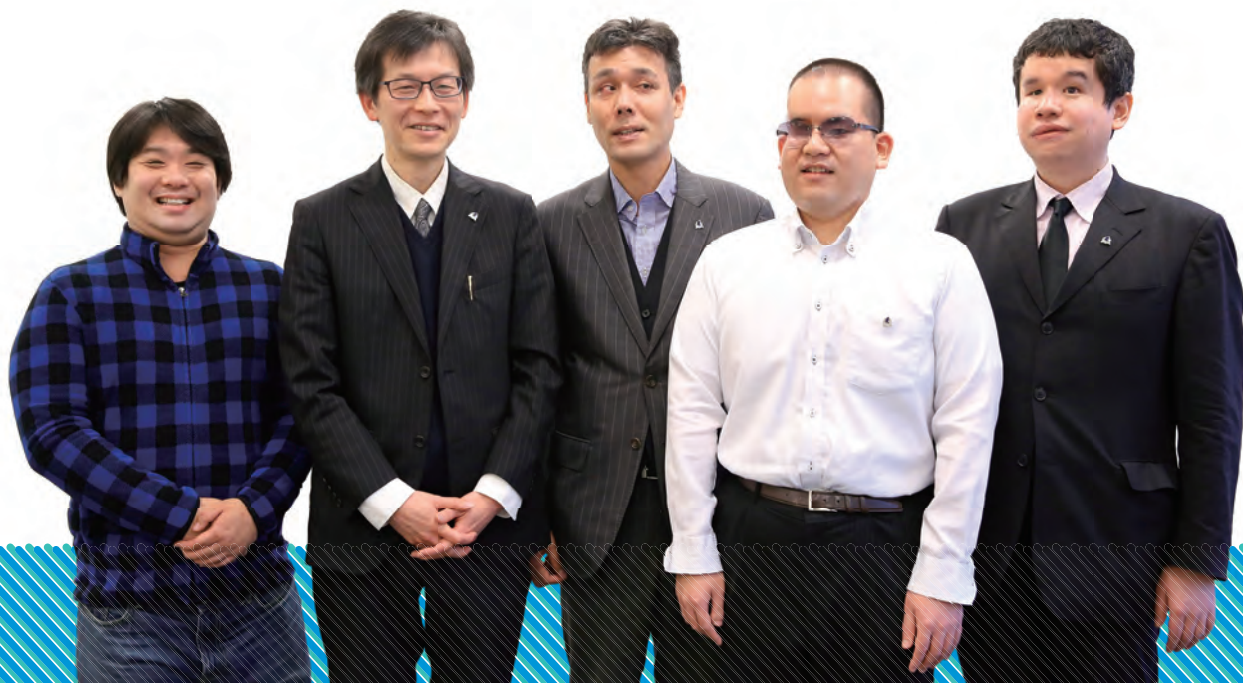
高原:同感です。夢を膨らませて、時間をかけて

しっかり正しい成果を出していくというのは研究の魅力だと思っています。今回、LAC Journeyをリリースしたことでもいろいろなアナリストから意見をいただき、アナリストがどういった分析をしているのかという意見や要望を広く収集することができました。このおかげで、画面からの検索だけではなく、APIによるシステム間連携や、アナリストへのプッシュ型の脅威情報の通知機能の必要性に気づくことができ、次にどのような研究をしていけばいいのかという課題が見えてきて、本当に飽きずに研究が続けられる。常に課題があることがむしろ幸せなのかなと、非常にポジティブに考えています。

船引: LAC Journeyができたことは非常に社内にインパクトがありました。このアプリケーションが、安全、安心な社会を築くことにつながっていけばいいと思います。

三川:我々のデータを使ってみたい、データ連携をしたいという方や「アクティブ・サイバー・ディフェンス」の実現に興味があるという方がいらっしゃいましたら、ぜひご連絡をいただければと思います。社内だけでなく外部の方ともデータの連携や交換をして、お互いの分析や実環境での利活用の促進を図ることで、Win-Winの関係を作ることができるといいなと思います。

船引:我々が手がけたLAC Journeyをよりよいものにするために、さまざまな形で連携し合っていけたらいいですね。本日は、貴重なお話をありがとうございました。



ラックの 顔

第9回

サイバー攻撃を 未然に防ぐために続ける 社会の意識改革への挑戦

セキュリティ業界で近年トレンドワードとなっている「脅威予測」。攻撃の傾向を研究・分析することで攻撃の予兆を察知し、事前に手を施すという新しい概念だ。ラックは昨年、監視や診断といったさまざまなセキュリティ事業によって蓄積されたノウハウを集約し、新たなサービスを生み出すためのセクションを設立した。メンバーとして抜擢され、セキュリティの最前線に立ってソリューション開発に邁進する2人の社員に、「見えない脅威」との戦い方を聞いた。

学生時代に培われたコンピューターの知識が キャリアの基礎となった

田原は、コンピューター専門の大学として日本で初めて開設された会津大学の2期生という学歴を持つ。入学は、一般家庭へのパソコンの普及を一気に加速させたOS“Windows95”発売の前年に当たるといから、田原は日本における黎明期からのインターネットユーザーだといえるだろう。

「高校生の頃に親が買ったパソコンを勝手に使い始めたのが、コンピューターに興味を持ったきっかけでした。簡単なプログラムを自作するなど、結構やり込んでいて、親に叱られることもありましたが(田原)」

設備やカリキュラムを見て入学を決意し、その後6年間、コンピューターについて学んだという田原。大学院を卒業する頃には、すでにセキュリティに関心を抱いていたというから、就職先の企業にラックを選んだことも、ごく自然な流れであったと振り返る。

「当時、日本でセキュリティをビジネスにしている企業はわずかでしたが、その中

でもラックは、コミュニティの運用や海外エンジニアの招聘など、面白いことをやっていた。入社試験も尖ったものだろうと身構えていましたが、思いのほか普通でした(笑)。当時のラックは、セキュリティ事業を立ち上げたばかりの状態だったわけですから、当然といえば当然ですね(田原)」

一方、「医師を目指して大学受験に臨んだ」という関は、ラックのビジネスとは異なる分野の職業に目を向けていた。

「職業に対しては、特殊なスキルで人の役に立つことができ、なおかつ感謝をされるようなものがないと漠然と考えていました。理系で上を目指していたら必然的に医師に行きついたという感じです(関)」

受験では力を発揮できず、医学部では

田原 祐介

yusuke tahara



なく生命理工学部で遺伝子組み換えや再生医療などについて学んでいたという関が、コンピューターに興味を持ったのは、学生時代のアルバイトだ。

「ドラッグストアのアルバイトで、店舗の基幹システムやWi-Fiのネットワークを

構築したことが転機になったと思います。Linuxを初めて触ったときには、あまりの面白さに徹夜でいろいろ調べるなど、趣味としてかなりのめり込んでいましたね(関)」

プログラムを使って生物の動きをシミュレーションするなど、大学でも比較的深く

コンピューターを使っていたという関。しかし関は、「現在の自分のベースになっているインフラエンジニアとしての知識は、アルバイトで蓄えられた」と自認しているという。

拡大を続ける事業領域に身を置き、自らの知識と経験を磨き上げる

今でこそ、セキュリティはラックのビジネスにおける大きな柱となっているが、田原が入社した2000年当時は、ラックにとってセキュリティを事業化したばかりの時期で

あった。これから拡大していこうと会社が注力している事業に新卒で携わったことが、現在の自分にとって大きな影響を与えた和田原は話す。

「例えば、ファイアウォールを構築する仕事であれば、新人でも、お客さまへの説明、設計、構築、納品までを全部任される。セキュリティ監視サービス(JSOC)の立ち上げにも、ゼロベースの状態から参画しました。100ページくらいのマニュアルを通勤の往復で読み込み、翌日から業務に挑むというような生活でしたが、当時のさまざまな経験は確実に糧になりました(田原)」

JSOCの立ち上げから一貫してJSOCに関わる業務を続けてきた田原とは異なり、関は、入社後3年ほどでキャリアチェンジを図っている。コンピューターウイルス被害の頻度が急拡大したことを受け、ラックが2009年に設立したサイバー救急

センターへの異動だ。

「後のサイバー救急センターの前身として緊急対応業務を行う人員の社内公募が2008年にあり、応募しました。実際に経験してみると、緊急対応は相当ハードな仕事ではあったのですが、情報漏えいの原因を特定し、報告したときのお客さまのほっとした表情が、何よりモチベーションになりました。同時に、『やっぱり漏れていたのか』という落胆の表情も印象的ではあったのですが(関)」

緊急対応の業務は、自分がもともと目指していた医師の仕事に近い、と関は続ける。

「当時の上司は、『緊急対応はICUや救命医療のようなものだ』とっていました。穴が開いているものを治す、という視点で見れば、救うものが人命か情報か、という違いだけで、セキュリティの仕事と医師には類似性があると感じています(関)」

日本企業のセキュリティ対策が 海外に後れをとる理由は経営者の意識の差

田原と関が現在所属している、「セキュリティソリューション企画開発室」。各部門が独自に取り組んでいた新規サービスの企画を専門に行う部署として、2019年4月に新設されたセクションだ。ラック社内で異なるキャリアを築い

てきた2人ではあるが、セキュリティのたたき上げとしてさまざまな経験を積み、サービスや製品について精通しているという点は、同室の事業で大いに役立つだろうと期待されている。

「各部門で新規サービスを企画する場合、その部門がターゲットとしている製品や

関 宏 介

kosuke seki

領域から外れることがないため、新しい発想が出にくい側面があります。しかし、サービスの開発を横串で行おうとする場合、監視、緊急対応、脆弱性診断といったさまざまな分野の知識や経験が複合的に必要になってくる。多様な経験値を持つメンバーを集めることで、セキュリティ企画開発の一元化を実現する部署だといえるでしょう(田原)」

新たなサービスを通じ、日本企業におけるセキュリティ対策の推進をリードしていく立場に立つ2人が懸念するのが、海外企業に後れを取る、日本企業のセキュリティ対策だ。

「日本企業は従業員がやっていることを縛るという形でセキュリティの強化を

図ることが多く、結果的に環境がどんどん使い勝手のよくないものになってしまうことが少なくありません。一方、海外では環境をよりよく、利便性の高いものにするためにセキュリティ対策を行うという考え方がベースとなっている。考え方の違いが、対策に大きな差を生んでいることは否めません(田原)」

関は、セキュリティ対策への費用を、投資ではなくコストと考える経営者の意識を指摘する。

「当社社長の西本は、セキュリティを車のブレーキに例えて話します。『ブレーキがなければ、車はスピードを出すことはできない。速く走る、すなわち自社のサービスや事業を拡大するためにはセキュリ

ティが必要だ』と折に触れていいますが、そういった考えを日本でも醸成していく必要があると思います。お客さまの要望を聞いていると、セキュリティ対策を“仕方なくやっている”という企業も少なからずある。安全にしたい、というよりは、とりあえずやっている、という印象はありますね(関)」

関の実感に対して、田原も同感だと話す。「お客さまからは同業他社の状況を質問されることが多いのですが、本来、セキュリティは個々の企業によって必要な対策やレベルが異なるもの。なぜ対策をしなければいけないのかという自発的な必要性よりも周囲の状況で判断している企業が多いように思います(田原)」

過去の体験と日々の情報収集が脅威の予測を実現する

新規サービスの提案に当たっては、顧客の希望や状況のヒアリングが欠かせない。セキュリティの専門家としてどのようなスタンスで顧客の話を聞いているのか、2人に聞いた。

「当社にお問い合わせをされるお客さまは、基本的に何らかの課題を感じているわけですが、話を聞いてみるとその課題が何なのかというところまで気づいていない方も多くいます。厳しいいい方ですが、私は、『お客さまがいう課題を信じない』ようにしています。我々には、攻撃の手法や手段を知っているからこそ気づけることがある。逆にいえば、悪質な手口を知らないお客さまから一部の発想しか出てこないのは当然だと思うのです(田原)」

「私は長年の緊急対応経験を通じて、さまざまな攻撃事例を目の当たりにしてきました。今は安全が保たれているが、今後どうなるかはわかりません。自分が知っている攻撃パターンに当てはめて、インシデントにならないよう未然に防ぐということに心がけています(関)」

セキュリティ対策においては、「攻撃を受け、それに気づいてから対処を行う」という考え方はもはや過去のものとなりつつある。田原や関がいうような、「事前に気づく」「未然に防ぐ」といった意識——つまり、攻撃を予測して防御する、「プロアクティブセキュリティ」という視点が、今後のセキュリティには不可欠だ。2人が有する多様な経験がまさに活かされる領域だといえるが、田原は、

「経験だけでは予測は実現しない」と襟を正す。

「日々、情報収集をしていると、次の手として何をすべきかがおのずと見えてきます。“経験”は重要ではありますが、それは“過去の体験”という意味ではなく、まさに今、世の中で起きていることを知識として蓄えることで経験に変えていく、それを続けることが一番、効果的だと思います。ただ、過去の体験があるからこそ次の手を考えられるわけですから、どちらが欠けても予測は難しいと思います(田原)」

「少し前までは、一般的に“海外で起きたインシデントは数年後に日本にやってくる”といわれていました。日本語という言葉の特殊性や、ガラパゴスなどといわれるさま



田原 祐介
yusuke tahara

SSS事業統括部 セキュリティ事業戦略部
セキュリティソリューション企画開発室 室長

2000年、ラック入社。当時事業化して間もなかったセキュリティビジネスに携わる。その後、セキュリティ監視サービスおよびJSOC(Japan Security Operation Center)の立ち上げメンバーとして従事し、JSOCに関わる業務で経験を積む。2019年4月より現職。趣味はスキーとスケート、ヘヴィメタルのライブで、趣味も仕事もアグレッシブにというのがモットーだが、体はいうことを聞かない。

さまざまな独自規格が背景にあり、日本は攻撃の標的になりにくい国であったというのがその理由ですが、日本語の研究が進み、さまざまなデバイスの基盤が世界共通になりつつある今、そのタイムラグはどんどん短くなっています。リアルタイムでの情報収集が予測のカギになることは間違いないでしょう(関)」



ゼロトラストの普及でよりよい社会、よりよい日本の未来を築く

脅威を「未然に防ぐ」というセキュリティの新たな時代を迎え、今後どのような新規ソリューションが必要とされるのか。会社の期待がかかる部署におけるチャレンジについて、田原はこう話す。

「基本的に日本企業のセキュリティ対策は、社員を全面的に信じるという性善説で成り立っています。しかし実際には、外部の攻撃者が社員のパソコンを乗っ取って社内から攻撃を仕掛けるというパターンが大半です。結果、重大な情報漏えいが起こっているわけですが、そういった状況にもかかわらず、性善説ベースの状況は変わりません。攻撃者が悪いのは当然ですが、それを許してしまう土壌を変えていかなければならない。ゼロトラストの実現は並大抵のことではないと思っていますが、その概念を取り入れたシステムインテグレーション(SI)のビジネスで、ゼロトラスト

を浸透させたいと思っています(田原)」

ゼロトラストの実現については、関もチャレンジの視野に入れているという。

「お客さまを説得してゼロトラストを進めるといっても、セキュリティ企業のトップランナーとして、ラックがまずゼロトラストに取り組むこと、それができればセキュリティ業界にインパクトはとても大きいと思います。当社が持つ知見を活かし、“この脅威はこれからきっと問題になる、そしてこのソリューションで防げる”という、お客さまにとって真に役に立つサービスを提供していきたいと思っています(関)」

インターネットが欠くことのできないインフラとなった今、セキュリティ事業が拡大の一途をたどることは間違いないだろう。仕事を共にする未来のパートナーに向けたメッセージを最後に聞いた。

「ラックはもともとSIの会社。セキュリ

ティのエンジニアは、SIのことを知っているべきだし、反対にSIのエンジニアはセキュリティを知っているべきだと思っています。セキュリティとSIを両輪で回していける、そんな人材に期待したいです(田原)」

「規模の割にベンチャー気質が残っているのがラックの魅力。社員がやりたいことを可能な限り後押ししてくれる文化があります。私も社内公募にチャレンジし、自分の希望を実現させてきました。積極的に自分から飛び出す意欲を持つ人は、成長できる会社だと思います(関)」

いまだ顕在化されていない脅威を予測するというのは至難の業だが、その実現が社会に大きく貢献することは確かだ。2人の言葉には「仕事を通じて人の役に立ちたい」という強い意志があふれていた。



関 宏介
kosuke seki

SSS事業統括部 セキュリティ事業戦略部
セキュリティソリューション企画開発室 担当部長
兼 同統括部 サイバーセキュリティサービス部
サイバー救急センター

2005年、ラック入社。検査グループでOSやサーバーアプリ等、プラットフォームの脆弱性診断などを経験する。2008年より現在のサーバー救急センターにてセキュリティインシデント対応やフォレンジックに従事。侵害を受けたシステムの調査、原因究明と対策の立案などに携わる。2019年4月より現職。趣味はゲームと食べ歩き。最近、猫を飼い始め、2人の娘と一緒に遊ぶのが癒し。



活動の ご紹介

政

府は、人類がこれまで歩んできた「狩猟社会」「農耕社会」「工業社会」「情報社会」に次ぐ第5の新たな社会を、デジタル革新、イノベーションを最大限活用する社会として「Society 5.0」と名付けています。そして、サイバー空間とフィジカル空間を高度に融合させることにより、多様なニーズにきめ細かに対応したモノやサービスが提供されることで、経済的発展と社会的課題の解決を両立する社会の実現を提唱しています。

Society 5.0の実現に向けたICTイノベーションの過程には、最新技術のシステムへの実装や利用開発、運用技術、情報リテラシー等、各々の連携において、さまざまな隙間やほつれが変化しながら広がっていきます。この連続的な隙間やほつれを、我々は総じて「ギャップ」と呼んでいます。

サイバー空間と フィジカル空間の ギャップ

サイドチャネル攻撃が例としてあげられるような、サイバー空間以外のフィジカル空間との狭間の領域を指します。ここで見られる事象を分析・利用した先端テクノロジーは新たな攻撃手法にも現れてきており、攻撃検出の新たな技術としても利用できる可能性があります。

脅威変化と 対応能力のギャップ

情報システムを脅かす脅威の変化スピードと、情報システム利用者側が対策を施す対応能力スピードの差を指します。例えば、ソフトウェアの脆弱性情報が発見されると、公的機関から対象範囲と対処法などの情報が公表されますが、その更新頻度が高い場合、利用者側である企業の脆弱性管理担当者における自社のシステムやプロダクトへの影響調査や対応といった負荷が顕著に高まります。最近では、この差を利用する攻撃も数多く確認されています。

情報サービスと 情報リテラシーの ギャップ

一般的なICT利用者の情報リテラシー、モラル、セキュリティ意識、インターネット上における消費生活知識の向上には、高度技術者に対するものとは全く異なった啓発・支援活動や法整備が重要で、人文科学や社会科学の視点も必要となります。ICTイノベーションによるインターネットサービスの変化に追従できない人や組織で発生するインシデントの多くは、このギャップが原因であると考えています。

これらのギャップには、新たなビジネスチャンス（課題解決をニーズと捉えた、ソリューションやサービスの創出）を生む一方で、国家や宗教、思想を理由にギャップが利用された社会生活での脅威（Attack SurfaceやExposure Gap等）が生まれる可能性があると考えており、「国を護る」をスローガンとする当社としては看過できない状況となってきました。

サイバー・グリッド・ジャパンでは、これらのギャップをさまざまな視点から研究することで、当社の将来的な新規事業のアイデアを発見し、またセキュリティ技術の向上を促進することができると考えています。

CYBER GRID JOURNAL^{VOL.}9

サイバー・グリッド・ジャパンは株式会社ラックの研究開発部門です。

サイバー攻撃や各国のセキュリティ事情、セキュリティ防御技術などに関する最先端の研究のほか、複数のセキュリティ企業との連携や新たな製品・サービスの開発、各種啓発活動などにより日本のセキュリティレベルと情報モラルの向上に貢献しています。

サイバー・グリッド・ジャーナル(以下本文書)は情報提供を目的としており、

記述を利用した結果生じるいかなる損失についても株式会社ラックは責任を負いかねます。

本文書に記載された情報は初回掲載時のものであり、閲覧・提供される時点では変更されている可能性があることをご了承ください。

LAC、ラック、サイバー・グリッド・ジャパン、JSOC(ジェイソック)は、株式会社ラックの商標または登録商標です。

この他、本文書に記載した会社名・製品名は各社の商標または登録商標です。

本文書の一部または全部を著作権法が定める範囲を超えて複製・転載することを禁じます。

©2020 LAC Co., Ltd.

株式会社ラック サイバー・グリッド・ジャパン

〒102-0093 東京都千代田区平河町 2-16-1 平河町森タワー

E-MAIL : sales@lac.co.jp <https://www.lac.co.jp/>

株式会社ラック
サイバー・グリッド・ジャパン

