MOTEX × CYLANCE™

Unbelievable Tour in Japan #2

未知の脅威は防げない。
その概念を覆す瞬間をあなたは“再び”目撃する!!

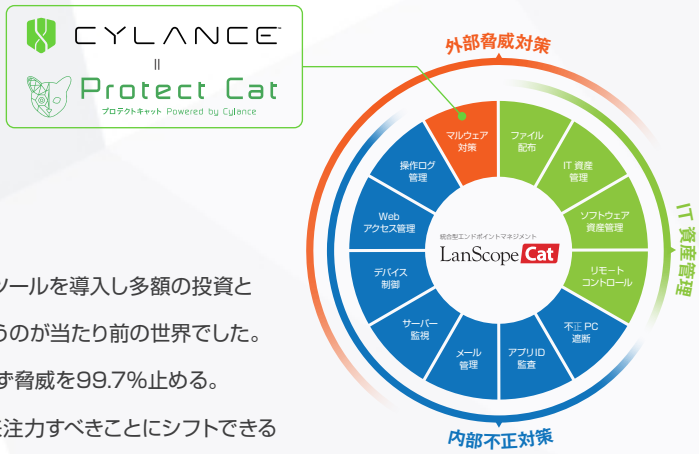
Event Report

Welcome Message

私は27年間IT業界で働いていますが、その間、様々な技術革新が繰り返されてきました。
その中で本日来日いただいているCylance Stuart氏の作ったAIエンジンは“破壊的技術革新”と呼べるものだと確信しています。その“破壊的技術革新”とは、表面的なものではなく、技術だけが優れているものでもなく、本質的かつ普遍的なものであり、その技術革新による価値が伴うものであると考えています。

「99.7%の検知率は何をもたらすのか」

MOTEXは2年前にCylanceとOEM契約を結び、CylanceのAIエンジンを弊社製品のLanScope Catに統合し提供しています。LanScope Catは従来、IT資産管理・内部不正対策をエンドポイントで行うソリューションでしたが、CylancePROTECTを統合することで、従来の機能と連動させ「統合型のエンドポイント製品」という新たな市場を創っていこうとしています。



これまでのサイバーセキュリティ市場は、様々なツールを導入し多額の投資とリソースをかけても、それでも止められないというのが当たり前の世界でした。
しかし、Cylanceと弊社が目指しているのは「まず脅威を99.7%止める。
それによりコスト・リソースを大幅に削減し、本来注力すべきことにシフトできる環境を提供する」ということです。

本日は、混沌としたサイバーセキュリティの世界にAIの技術で革命をもたらしたCylance Stuart氏をはじめ、日本のセキュリティ界を牽引する方々にお集まりいただき、私も参加して製品の枠を超えたディスカッションをさせていただく予定です。
ぜひ、みなさんの目で「本質的な技術とは何か」「今後サイバーセキュリティに対して企業はどう取り組めば良いのか」を確かめていただければと思います。

エムオーテックス株式会社
代表取締役社長　河之口 達也

INDEX

Keynote

CYLANCE

「セキュリティ× AI」でゲームチェンジを仕掛けた理由

Stuart McClure 氏　Cylance Inc.　会長 兼 CEO 兼 創業者

マカフィー / インテル セキュリティの EVP（エグゼクティブ バイスプレジデント）兼グローバル CTO（チーフテクノロジーオフィサー）兼セキュリティ管理事業部門ジェネラルマネージャーを務めたのち、Cylance を創設。サイバーセキュリティの世界に AI を導入し、シグネチャ型の検知アプローチから脱却した 革新的な技術を開発して、業界を牽引する企業を設立しました。現在は CEO として、脅威の検出と保護、そして対処を行う戦略的な製品開発、業務執行、財務投資を統括しています。また、25 年におよぶ情報セキュリティ業界での経験を生かし、業界の第一人者として啓蒙活動を通じて市場全体の発展にも貢献しています。

なぜ我々が Cylance を始めたのか

その真の答えは、「AIの準備」ができたからです。当時主流だった定義ファイルベースのアプローチをサイバーセキュリティから無くしていくことができないか、その上で、過去に見たことの無いサイバーアタックからの保護及び予防ができないか、というアイディアのもと2012年に会社を設立しました。これまで、Fortune500の企業のうち100社以上がCylanceを採用いただいています。現在では社員850名、グローバル顧客数6,000社以上、1000万台を超えるエンドポイントで稼働しており、販売開始3年半にも関わらず、大きく成功を成し遂げることができました。その理由は明確です。サイバーセキュリティにおいてAIが有効だからです。

数学によって未来を予測する方法とは何なのか？

Cylanceのミッション、製品を本当に理解するためには、本質的に数学を理解する必要があります。しかし数学はときに、とっつきにくい。そのため、非常に簡易なたとえでお話をしてみようと思います。

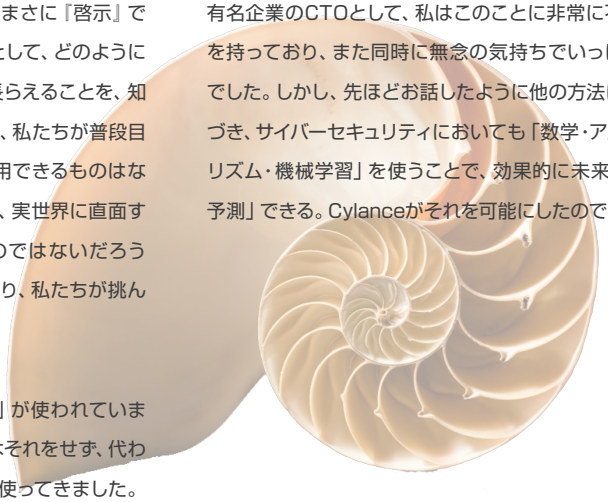
自然の生み出すリズムやハーモニーに目を向けてみるとき、そこには何かパターンがあることに気づきます。そのパターンは、アルゴリズムであり、アルゴリズムは数学です。みなさんが起きたとき、周りを見渡す。自然を見る。あらゆるパターンは、数学的に変化しています。私は『啓示』に気づき「あらゆる自然は数学であり、アルゴリズムが見つかれば数式が見つかる。数式によって未来を予測できる」と腑に落ちたのです。

例えばこの「アイディア：ひらめき」は、オウムガイにも見られます。これは海の生物であり、5億年前から、生存のために進化を続け、他の生物を圧倒する程の長い間存在し続けてきました。それはなぜか？また、どのようにそうしてきたのでしょうか。その理由は、数学で説明できます。

オウムガイの殻の中心から始まる各部屋は、その隣り合う部屋の1.33倍（黄金比）で大きくなっています。私がこれを知ったとき、それはまさに『啓示』でした。自然は、その根本的な要素として、どのように数学を使うか、それによって生き長らえることを、知っていたのです。これをきっかけに、私たちが普段目にするその他のことで、数学を活用できるものはないだろうか。そして数学を活用して、実世界に直面する問題を解決することができるのではないだろうか。これが、Cylanceの始まりであり、私たちが挑んだ課題なのです。

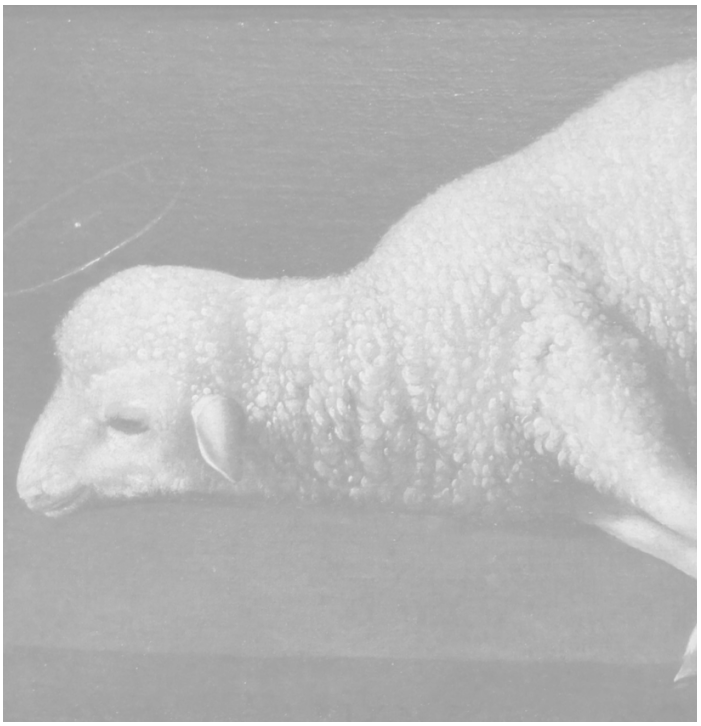
自然界では様々なところに「数学」が使われていますが、唯一、サイバーセキュリティはそれをせず、代わりにシグネチャ（定義ファイル）を使ってきました。

シグネチャは過去に経験したパターンですが、ここにおける問題はそれらは既に過去であるということです。新しい攻撃が行われたとき、そのシグネチャは無効です。それは新しい攻撃に対する新しいシグネチャは存在しない。誰も見たことがないからです。ある有名企業のCTOとして、私はこのことに非常に不満を持っており、また同時に無念の気持ちでいっぱいでした。しかし、先ほどお話したように他の方法に気づき、サイバーセキュリティにおいても「数学・アルゴリズム・機械学習」を使うことで、効果的に未来を「予測」できる。Cylanceがそれを可能にしたのです。



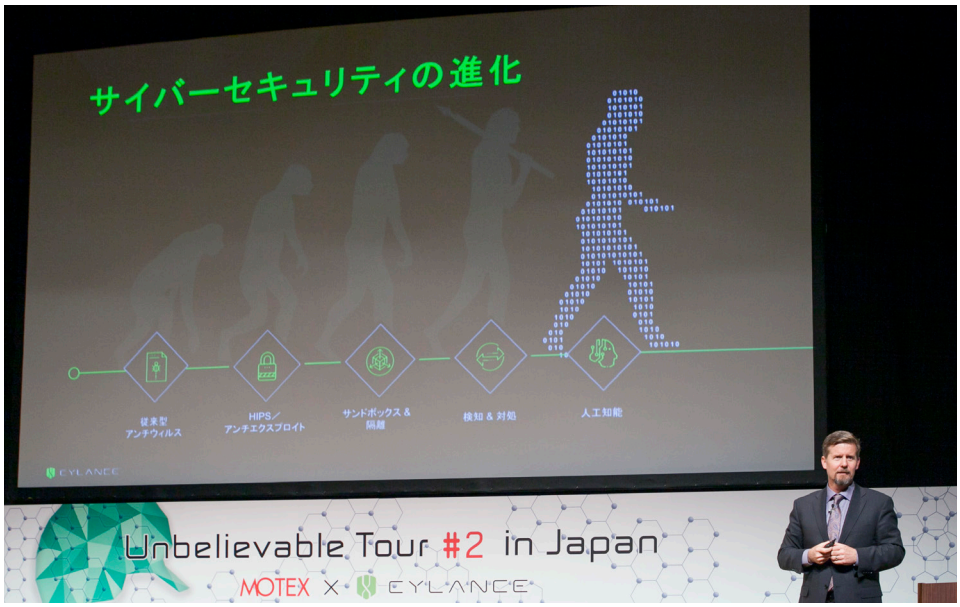
生贄の子羊はもういらない

さて、ここで従来のシグネチャによる手法を見て見ましょう。
私が前職である大規模な組織の長であったとき、毎日2,000人がシグネチャを作成していました。これは、あまり知られていないことですが・・・約7,000人の社員のうち2,000人が、可能な限り早くシグネチャ作る努力をしていました。しかしそのやり方は悪い事象が起こることをキャッチすることだったのです。
シグネチャによる手法をもう少し詳しく説明すると、まず、既知の攻撃に関するセット、そして過去の攻撃に関連のない新しい攻撃に関してのセット。そして、ここに新しい被害者（生贄の羊）がある。サンプルを取得し、サンプルによく似たサンプルをできるだけ多く取得し、人間による分析をします。つまり、それらサンプルを見て、リバースエンジニアリングを実施し、分解して新しいシグネチャとして作成するのです。それはクラウドにあげられ、管理者はそれをパターンファイルとして更新します。願わくは、彼らがそれと全く同じ攻撃を受けてしまう前に。しかしこの間に、攻撃ファイルが1バイトでも変わってしまえば、このシグネチャではそれを止めることはできません。この手法は長らく、サイバーセキュリティにおける主流な手法として使われており、今日においても世の中に存在するほぼすべてのサイバーセキュリティは、その根幹がこのモデルです。これは、自動車を運転するときに、バックミラーだけを見て運転すること、つまり過去を見て運転することと同じです。これでは衝突が絶えないのも仕方ありません。



サイバーセキュリティの進化

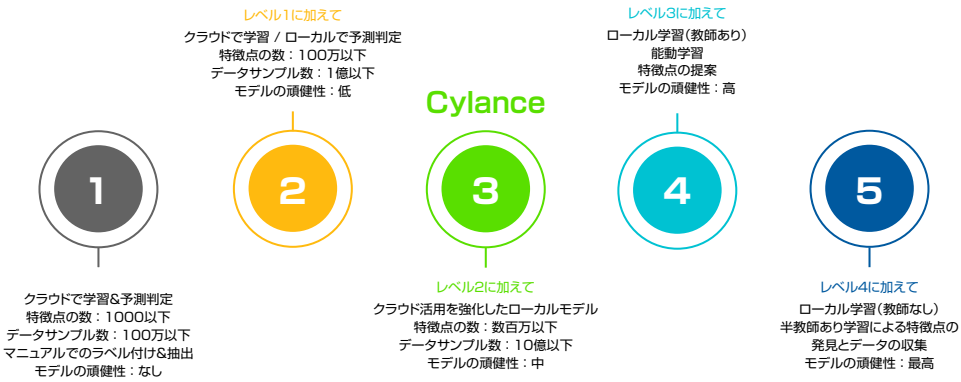
これらを解決するためには、過去を知ることです。過去を知ることは第1ステップであり、未来を作ることでもあります。
始まりはシグネチャ型のアンチウイルスです。その後、ヒューリスティック型（HIPS）と呼ばれる、より一般的にパターンを見るものが登場しましたが、これもまたシグネチャ型です。そして、サンドボックス（隔離）型が出現します。これは2008年代に現れ、ハードウェア・ソフトウェア両方のサンドボックスが存在します。しかし、これも攻撃を止めることはできません。そして、EDR（検知＆対策）が出てきました。これはつまり、防御は諦めるということに他なりません。もちろんそれを個人的に問い詰めるつもりはありませんが・・。
不思議なのは、これまでの技術では防ぎきれていない現状がありながら、サイバーセキュリティ企業の企業価値は上がっていることです。攻撃が発生し感染被害が増えると、それら企業価値が上がっているのです。これは何かの間違いではないか?と思いたい。



もう少し議論してみましょう。
EDR技術においては、何か攻撃を予防するということはほぼ不可能だという考え方です。なぜなら攻撃を検知し、それに対して対策（レスポンス）するということのみだからです。これが使える企業は、十分な人数の優秀な人材を雇えて、彼らが的確な時間に動き、攻撃が行われているそのときを捉え、そして可能な限り早く対策につなげ、攻撃による影響を最小限にすることが可能である必要があります。しかしこのモデルは現実的ではありません。私達は、幾度となくこれにトライしてきましたが、シグネチャ型のモデルに依存し続けている限り、私達は常に攻撃を防ぐことに失敗するのです。

私は大学で、心理学・哲学・コンピューターサイエンスを履修していましたが、実は数学は得意ではありませんでした。常にBやC（注：5段階評価の2－3程度）です。しかし統計学は好きでした。そしてコーディングも好きだでした。コンピューターをデータでトレーニングして、統計的に意味を見出すというアイディア、これがCylanceの基になっています。
2012年にCylanceを始めるにあたり、大きく2つのことが私達の後押しとなりました。

サイバーセキュリティにおける AI 活用のレベルと進化



1つ目は、データにアクセスできたことです。AIというのは、正しいデータが無ければ何の意味もありません。2つ目は、コンピューティング性能が向上し、大量のデータを処理し、高次のデータ領域を処理することができたことです。クラウド技術の進歩（例えばAmazonにみられる）がなければ、Cylanceを作ることは叶わなかった。幸運にも、それが可能だったのです。今や、多くの人が「AI」や「機械学習」という言葉を耳にしていると思います。またサイバーセキュリティ業界ほぼ全てのプレイヤーが、AIや機械学習を使っていると公表しています。しかし、これらのほとんどはマーケティングの意味合いが強いものばかりです。会社を始め、数理モデルやAIを喧伝しはじめたとき、周りにそれらを語る者はいませんでした。それが今は、みんなが語っています。彼らと私たちは何が違うのか。

まず第1には、誰よりも長くこの技術に携わっていることです。またグローバルで最大とは言いませんが、データサイエンティストの大きな組織を有しています。先日、データサイエンスチームの採用活動について、私達はハイテク企業Top10に入るGoogleやFacebookと肩を並べるほどであるという結果が発表されました。では、私達の技術は他とどう違うのか。

ほとんど（95%）の企業は機械学習を実装しているというが、実際はシグネチャ型やパターン認識を機械学習を使ってやっているだけです。一方全体の5%にも満たないが、第1世代の機械学習をやっているところもあります。がしかし、非常に限られたサンプル、特徴点を使い、クラウドでのみ検知判断を行っています。また学習に長い時間が掛かり、結果誤検知や検知ミス（False Negative）の多いものとなっています。

第2世代になると、より大きなデータセットと特徴点を持ち、そして検知判断をエンドポイント上で実施します。この方法であれば、攻撃の検知は非常に容易であり、検知のためにクラウドに接続する必要もありません。しかし今日において、他の誰もこの方法を取っていません。

最後に第3世代のAI。私たちはこの領域に達しています。ここでは第2世代よりも巨大な数理モデルがあり、それらモデルにて強靭な防御が可能になっています。しかし、私達はここでは終わりません。私たちはその先の第4世代、第5世代に至る道を見ています。大きなブレークスルーはちょうどここであると考えています。つまり、「何故それが起こったか」を表現できるようになる、ということです。AIにおいて「なぜ」を導き出すのは最も難しいことです。実際、このことは、なぜ人々がAIに不安を覚えるかということを考えると容易です。つまり彼らは「なぜ」が説明できないからなのです。なぜこの攻撃を捉えたのか。なぜこれを「悪意あるもの」と決定するのか。

最大の課題は、「これは良い・悪い」は判断できるが、「なぜ」は語れないのです。この市場にいる誰も、現時点でその領域には至っておらず、これはサイバーセキュリティ市場だけでなく、AIを使ういかなるプレイヤーを含めてもです。しかし、私達は第4世代に到達する道を捉えていると自負しているのです。これまで発生したすべての攻撃を見ていくと、主に3つのパターンに分けられます。1つ目は実行ファイルベースの攻撃。つまりウィルスやトロイの木馬、ランサムウェアやワームなどです。2つ目はアイデンティティベースの攻撃。これらは、あなたのIDを利用するもので、例えば安易なパスワードや、紙に残して見えるようにしていたり、傍受されるなどして盗まれることで、そのIDを使って攻撃するというものです。3つ目は、DoS攻撃。これらは、正常な通信を膨大な量送りつけることで攻撃し、コンピューターやサービスをダウンさせてしまいます。

これら3つは、サイバーセキュリティ業界において非常によく知られている用語に紐付けすることができます。それは、「機密性」「完全性」「可用性」です。攻撃者の周りにこれらの関連があることはよく知られています。

皆さまもこれらに該当する多くの事例を知っていると思います。例えば、WannaCry、Petya：などのランサムウェア、Equifax：ウェブ攻撃、Deloitte、OneLogin、Yahoo：IDベースの攻撃を受けたなど。また、内部脅威：内部の人間として文書を盗み、他に渡す。NSAがハッキングされ（シャドーブローカーによって）、CIAもハッキングされた（Vault7によって）。これらはIDベースの攻撃です。私達は、アイデンティティベースの領域に踏み込んでいきます。それは、数理モデルの「あなた」というアイデンティティを作れると考えているからに他なりません。そしてコンピューターにこのモデルを配信するのです。また同時に、攻撃への防御はどこであっても必要であるということを知っています。

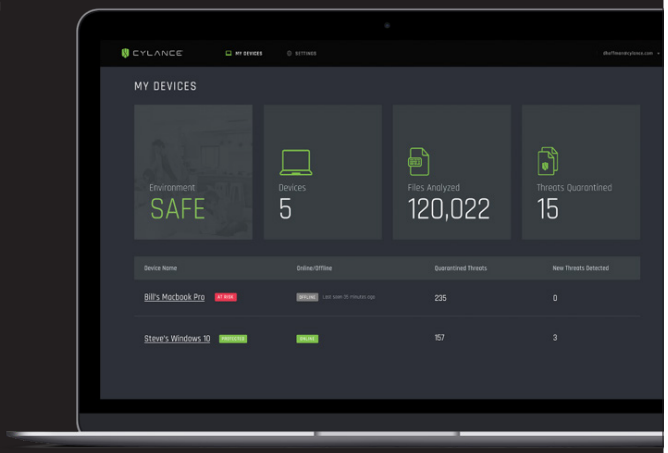
CylancePROTECT® Home Edition

私達は今年、コンシューマ向けのHome　Editionをリリースしました。Home　Editionでは、スマートかつシンプルなセキュリティを実現します。
こちらが、その概要です。現在の企業版モデルを非常に簡易に落とし込みをし、ユーザーにはほとんど影響を与えることはありません（ほとんど見えません）。実際には企業版でもユーザーにはほとんど見えないのですが。これにより、自宅で使うときも非常に簡単に使え、かつ簡単に管理できるようにしています。日本は2018年にリリースを予定していますので、ぜひご期待ください。

CylancePROTECT® Home Edition の概要

AIを駆使し、将来現れる未知のマルウェアの亜種を予測してブロックすることで、既存のどの消費者向けアンチウイルスソリューションよりも優れた保護を提供する、初の消費者向け次世代セキュリティ製品です。

- 家庭内で技術的な作業を担当するメンバーが、家庭環境にあるあらゆるデバイスのセキュリティの状態を確認し、把握できるように支援
- 従業員の家族全体をセキュリティで保護。また、遠隔地にいる家族（高齢の両親、大学生の子どもなど）のデバイスの安全性とセキュリティを確保し、保護
- 従来の消費者向けセキュリティ製品に関連する肥大化、システムの低速化、ノイズ、数多くのポップアップによるシステムの停止を回避
- 容易なインストール、容易な管理と構成、自動更新、消費者向けデバイスの自動的な保護によって、「一度設定するだけで管理不要」のセキュリティエクスペリエンスを提供



今後の展望

このように未来を見ていくなかで、私はこのメッセージを日本の皆さんにお送りしたいと思います。

「AIやそれによる機械学習やディープラーニング、数学を、恐れないでください。それらを受け入れ、理解し、人が介在する判断について問いかけ、知識化し、組織に存在するパターンを適応させてください。パターンを発見したとき、脳がそれを認識することで、これにより機械学習がより良くなるのです。
組織がAIを活用するようになれば、さらに容易に、未来への道が切り開けると確信しています。そうすれば困難な状況にはならないでしょう。私達は、サイバーセキュリティの歴史の中で、悪意ある攻撃者の先を行った最初の例です。今日、私達は99.9%の確率でいかなる攻撃も捉えることができます。私達を信じる必要はありませんが、自分自身でテストし、トライしてみてください。
AIによって、仕事を取られてしまうという懸念が流布しているが、私は、それが真実になることは全く無いと思います。それは何故か。それは現在の領域の半分がAIによって補われたとしても、依然取り組まなければならない領域はたくさんあり、むしろそれらは今までは取り組めてなかったということです。この領域に人を集中させることができるようになることは素晴らしいことなのです。
最後に、（暗に）誰も信用しないでください。自分自身を信用し、テストし、どのような分野であってもAIを活用していって欲しいと思います。」

ありがとうございました。

CYLANCE

1年前のエンジンで WannaCry は防げるのか？

乙部 幸一朗 氏　Cylance Japan 株式会社　最高技術責任者

名古屋大学卒業後、国内大手電気メーカーでのネットワークエンジニアを経験後、イスラエルおよび米国のセキュリティ企業を中心にサイバーセキュリティに関連した技術職を歴任。ジュニパーネットワークスではアジア太平洋地区担当プロダクトマネージャー、８年間在籍した前職のパロアルトネットワークスでは日本国内の技術責任者を務め、エヴァンジェリストとして業界や各種団体の講演やセミナーなどでも活躍。

私のセッションでは、「タイムマシン」と名前付けた弊社の製品のデモンストレーションを実施します。
その前に、まずはこの製品がどのようにして新しいマルウェアを検知するのかというロジックを改めてご説明します。

AI を使って作り出した数理モデル

「AIアンチウイルス」は人工知能を使ったアンチウイルスですが、人工知能という言葉は非常に定義が広いです。皆さんが今手に持っている携帯電話の中にも人工知能が入っていますし、グーグルの検索エンジンにも入っています。メーラーがスパムメールをフィルタしてくれていますが、あれも人工知能の技術・機械学習の技術を使っています。

またこの「人工知能」というキーワードはマーケティング的に使われることが多いですが、我々は違います。もう少し具体的に言うと、我々のユニークな部分は、機械学習という技術ではなくて、機械学習を使って数理モデルを作って予測判定をするというアプローチをとっていることです。
これは何がすごいのかというと、セキュリティの世界、特にこのサイバーセキュリティの世界では、歴史が始まって以来、攻撃者が常に有利な状況です。よく「いたちごっこ」と言いますが、守る側が先にいくことはありませんでした。攻撃者が必ず先に手をうって、それに対して守る側が技術を追いかけていく、こういった構図だったのですが、この推論判定の技術のすごいところは、おそらく歴史上初めてセキュリティ側が攻撃者の前をいく技術を手に入れたというところです。
機械学習という技術を使って、いわゆる人工知能のシステムに大量のファイルを学習させます。現状ですと、大体一回の学習あたり10億個ほどのファイルを使っています。これは「教師あり学習」というアプローチをとっており、あらかじめ勉強するファイルデータには答えが付いています。つまりそのファイルが良いファイルなのか、それとも悪いファイルなのか分かった状態で、人工知能・機械学習のシステムに学習させます。これは大量のコンピューティングリソースを必要とするため、全てAmazonのAWS上に構築をしています。

この機械学習のシステム（インフィニティ）では、まずファイルのどこに注目をして覚えるかという特徴点を抽出します。その特徴点に応じて学習をしていきます。特徴点というのは色々ありますが、例えばファイルのサイズ、ファイルのヘッダー…実行ファイル形式ですとセクションと呼ばれるデータなどがあります。このセクションのヘッダー、データ、中に入っている文字列、その文字が出てくる頻度であったり、データのばらつき具合であったり、様々なものが特徴点として挙げられます。今だと1回の学習で、1つのファイルあたり見ている特徴点の数は600万から700万あります。この特徴点を元に、インフィニティは学習をしていきます。つまり、ファイルサイズという一つの特徴点については、その中に良いもの悪いもののデータを与えていくと、そのサイズに対して何かしらのルールがあるのではないか、もしくはある特定の文字列が出てくる回数において、良いものと悪いものには何か見分けるヒントは無いかというのを学習の中で見つけていきます。この学習した結果を、数理モデルという…言ってしまえば数式の集合体のようなモデルを作って、この中に凝縮して出力をしていきます。

我々の「AIアンチウイルス」というのはまさにこの数理モデルを使い、新しい未知のマルウェアが来た場合でも、そのモデルに近いかどうかというので判定をします。言ってしまうとファイルのデータを入力して、スコアを計算する、計算ソフトのように働いて、

エンドポイント上でのファイルの悪い良いというのを判断していく、こういったアプローチになっています。
インフィニティは、今この瞬間も頑張って学習をしているのですが、学習というのはすごく時間がかかります。しかしながら、一旦学習をして出てきたモデルは、先ほど言ったとおり計算式ですので、推論判定と呼ばれるいわゆる良否判定を一瞬で終えることが出来ます。
これは皆さんの頭の中でやっていることと同じです。イメージしていただくと分かりやすいのですが、例えば動物の中で、「猫」という動物を小さいころから覚えてきたと思います。皆さんの頭の中にはこの数理モデルに似た、概念のようなモデルというものを持っています。この概念モデルに猫というラベルを貼っているのですが、学習するのには実はすごく時間がかかっています。
0歳から始まって、最初は何匹かの猫を見て、お父さんお母さんが「あれはニャンニャンだよ」と教えて覚えていくのですが、おそらくしばらくは犬を見ても「ニャンニャン」と言っていたと思います。しかし、何年も、何十、何百、何千、もしかすると何万もの猫を見て、猫という概念を覚えていっています。
皆さんは頭の中で猫の特徴を言えると思いますが、思いつく以上に猫の概念の特徴を捉えています。それは、見た目の特徴だけではなくて、例えば触った毛の感じ、におい、鳴き声、そういったものも含めて頭の中に猫のものすごく細かい特徴を持った概念を持っているのです。
今では猫の写真を見せられて、猫か犬かの判定に5分10分かかる方はいないと思います。判定は一瞬です。人間の頭の中でニューラルネットワークという神経回路網がやっている処理を、インフィニティは同じようにコンピュータシステム上で行って、モデルとして吐き出しています。これが数理モデルによる推論判定というアプローチになります。これが、我々がやっているアプローチの最もユニークな部分なのです。

検知デモ（最新のパターンファイルで検証）

では早速、実際に製品のデモンストレーションをご覧いただきたいと思います。今日使うのは、WannaCryという今年の5月に世界で数十万台感染被害をもたらした、ランサムウェアと呼ばれる身代金を要求するタイプのマルウェアです。今からWannaCryのサンプル50個を使って実際に検知できるかどうかをお見せします。
実際にWannaCryが出たのは日本時間で2017年の5月12日の金曜日の夕方から、ヨーロッパを皮切りにアメリカ、そしてアジアとどんどん世界中に感染が広まっていきました。この金土日の3日間で、インターネット上で数百のWannaCryのサンプルが報告されています。今日はそのうちの50個の検体を用意してきました。

今からデスクトップの空っぽのフォルダーにWannaCryの検体50個を投げ込んでいきます。コピーが終わったら、このフォルダーに対してアンチウイルスのスキャンをかけていきます。今、バックエンドでアンチウイルス製品がスキャンを始めました。見ていただくと分かるのですが、CPU使用率が大きく上下しています。これは何をやっているかというと、アンチウイルス製品は世の中にあるウイルスファイルを見つけてきて、それを止めるためのパターンを作っています。このパターンファイルというのは毎日、最近では一日数回更新していますが、このファイルの中には数十万という過去見られたマルウェアのパターンが入っています。このパターンをスキャンするときにはメモリー上に展開をして、また対象のファイルの中に同じパターンが無いかというのをつきあわせ・マッチングをしています。これはCPUにとってはすごく重い、大変な処理で、そのためこのようにCPU使用率が増加します。さらにスキャンが始まると多くのメモリーやディスクへのアクセスも発生しますので、皆さん経験があるように、アンチウイルスがスキャンを始めると、急に端末が遅くなります。これはこの製品に限らず、従来のアンチウイルス製品は全て同じ共通した技術をベースに動いています。
結果をみてみましょう。いくつか検知したとアラートが上がり、先ほど50個あったはずのファイルは消えて、2個だけファイルが残っています。これはつまり、48個を検出したということを意味しています。100%の検知率に直すと96%、ほとんどのWannaCryの検体をうまく検知し、きれいに取り除いてくれたということが分かります。

ではもう1つ別のアンチウイルス製品も同じようにスキャンをしてみたいと思います。全く同じことをします。デスクトップのフォルダーにWannaCryの検体を50個

Environment - 環境 -

2017 年 11 月 29 日時点の最新バージョンにアップデートした既存アンチウイルス２製品

Target - 対象 -

WannaCry のサンプル 50 個

Result - 結果 -

	製品バージョン	検知率
A 社	2017 年 11 月 29 時点での最新バージョン	46/50(96%)
B 社	2017 年 11 月 29 時点での最新バージョン	49/50(98%)

コピースキャンをかけます。先ほどの製品よりも、すごくCPUを消費しています。ほぼ100%張り付いているのが分かります。これは製品の考え方の違いで、ファイルがやってくる時点でコピーをすることで、ファイル自体が届かないようにする、そこに全力を注ぐ、そのためにはCPUを使い切ってもしょうがないという設計で製品を作られているのだと思います。

スキャンがほぼ終わりました。ここに検出したファイルを見ると1つだけファイルが残っています。つまり検知率に直すと98%、先ほどの別の製品と比べると1つ多く検知していますので、若干検知率が良いといえるかもしれないです。
この2製品、いずれも90%以上のWannaCryを検出することができました。ただしこれは、皆さん想像していただいているとおり、当たり前のことで、今年の5月に発生した有名なランサムウェアであるWannaCryを検知できるというのは、この2製品以外のどの製品でもおそらく同じです。

タイムマシンデモ（2017 年5月12日時点のパターンファイルで検証）

今日のメインはここからです。これからタイムマシンに乗って2017年の5月12日、WannaCryがパンデミックを起こしたまさにその日に戻ります。

皆さんが知りたいのは、実際にWannaCryが来たまさに当日、当時のアンチウイルス製品がどのくらい止められたのかということだと思います。今ここに先ほどと全く同じアンチウイルス製品が入った端末があります。シグネチャの作成日時を見てみると2017年5月11日になっていて、つまり実際にパンデミックが起こった5月12日時点での最新のシグネチャが入っています。この2台に対して先ほどと全く同じことをやっていきます。共有サーバーからWannaCryのサンプル50個をコピーし、明示的にスキャンをかけていきます。1つ目の製品は、先ほどはコピーをするところで49個のファイルを止めましたが、今回は全てのファイルがコピーできています。これはつまり、1つもファイルを検知できなかったということを意味しています。もう1つの製品も、1つアラートが上がっていますが、当然この時はWannaCryではないため、別の名前の検知が挙がっています。そして、ファイルの数を見ていくと、49個。つまり一つしか検知できず検知率は2%ということになります。

念のため動いてから止めるという製品もありますので、実際にこれらのすり抜けたものを動かして見ると・・・ランサムウェアに感染しましたというメッセージが出ました。それと同時に、デスクトップの画像も変えられているのが分かります。そしてここにあったExcel、Wordのファイルが消えて、新しいファイル…そのファイル名に「.wncry」という文字列がついた新しい暗号化されたファイルが出来上がっています。

今ここでアンチウイルス製品は何か検知しました。OSのSMB上で何かやられているというのに気付きましたが、この時点で見ていただいたら分かるとおり、暗号化されてしまっているという状況です。

このように、実際WannaCryが来た当日、2017年5月12日は、世界中のコンピューターでこの事象が起こっています。今日お見せした2製品が特段悪かったわけではなく、世の中にあるほぼ全てのアンチウイルス製品が同じ状況になっていました。つまり、見たことあるものに対してパターンファイルを作って止めていくということが間に合わない場合、このようにすり抜け、そして感染が起こってしまうのです。

Environment - 環境 -

2017 年 5 月 12 日時点の最新バージョンにアップデートした既存アンチウイルス 2 製品と 2016 年 6 月モデルの CylancePROTECT®

Target - 対象 -

WannaCry のサンプル 50 個

Result - 結果 -

	製品バージョン	検知率
Cylance	1380 （2016 年 6 月のモデル）	50/50(100%)
A 社	2017 年 5 月 12 時点での最新バージョン	0/50(0%)
B 社	2017 年 5 月 12 時点での最新バージョン	1/50(2%)

では、今から全く同じことをCylancePROTECT(プロテクトキャット)で試してみたいと思います。今日使うデータモデルは、1380（2016年の6月、WannaCryが出てくる1年以上前に作られたもの）を使います。イメージしていただくと、アンチウイルスで1年前のパターンファイルで動いているものと同じイメージになります。

それでは、デスクトップのフォルダにWannaCryの検体を50個コピーしていきます。この製品の特徴は実行前防御といって、マルウェアが動き出す直前で判定を行います。試しに1つ実行してみると、Windowsのエラーが出ましてファイルにアクセスできなかったと表示されファイルが1つ消えました。これで残り49個になっています。

OSの中にはカーネルという重要なコンポーネントがあります。これはWindowsであれMacであれLinuxであれ同じです。プログラムが起動するときは、カーネルが実行ファイルの上からプログラムコードを抜き出してメモリーを割り当てて、そのメモリー上でプログラムのコードを起動します。このプログラムを起動するという動作を見ると、CylancePROTECTは起動する前に、動かそうとするファイル自体・コード自体を判定します。つまり先ほど私がクリックしたあの瞬間にスコアを出してこのプログラムを動かして良いかの判定をしています。時間としては本当に数十ミリセック、人間が瞬きをする間もなく判定を終えているので、先ほどのようにファイルがないというエラーが返ってくるのです。

残りのマルウェアはまだ動いていませんが、何もしていないわけではありません。話している間にファイルの数が微妙に減り、40個になっています。CPUの使用率はほとんど何もしていないように見えますが、これはCylancePROTECTのもう一つの

スキャン機能「バックグラウンドスキャン」が走っています。動くという動作が無かったとしても、新しくやってくるファイルに対しては人工知能のモデルを使って能動的にスコアを出して判定していきます。これは今までのアンチウイルスのファイルスキャンと似ています。しかしCylancePROTECTはモデルを使っているため日々の定期スキャンは必要ありません。インストールすると端末上のファイルを一旦バックグラウンドスキャンでスキャンします。つまり端末上にあるプログラムファイルを一旦全てスキャンします。その後はその端末にあるファイルを再度スキャンする意味はありませんので、その毎日フルスキャンを行うことなく新しく来たファイルだけを静かに動作し続けます。

このままバックグランドスキャンが終わるのを待ってもいいですが、残ったファイルを全てスタートコマンドで動かしてみたいと思います。すると、コマンドの下に「access is denied」というのが出ています。つまり実行前防御によりマルウェアが検知され、OS上でアクセスがはじかれたということでエラーが返っていて、そのファイル自体が消えていったのが分かります。フォルダーの方には全て何も残っていない状況です。全て検知ができました。

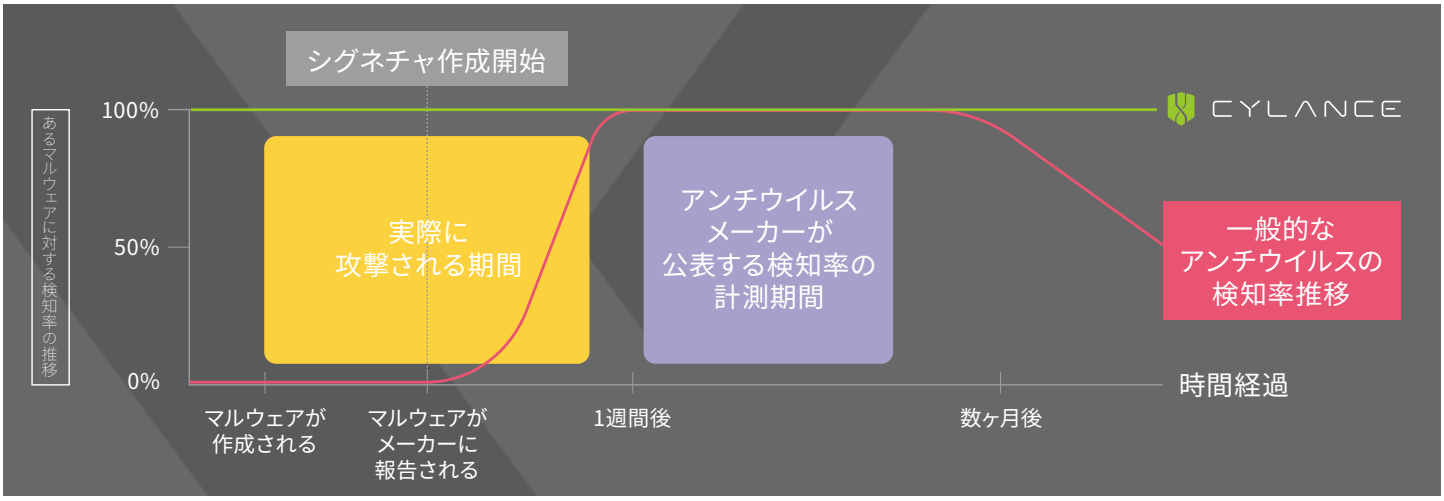
このように、WannaCryの検体50個を検知・ブロック・隔離できたのですが、この製品のすごいところは、推論判定をしているところです。先ほど申しましたとおり、このモデルは2016年の6月のモデルですので、今から1年半以上前、WannaCryが出てくる1年前のモデルでここまで検知をしています。つまり、ここにあるモデルから見たら、5月のWannaCryであろうが、明日出てくるWannaCryの亜種であろうが関係なく推論判定をしていきます。どちらも見たことがないマルウェアですので、同じように未知のものに対して高い判定を出せるというのが、この製品の大きな特徴です。

検知率比較の真実

この検知率について分かりやすく説明したいと思います。今回のWannaCryの例で言うと、使われたSMBの脆弱性が公開されたのが4月ですので、4月の末から5月にかけて、誰かがWannaCryを作ったと考えられます。そして5月12日、使われたWannaCryの検体が初めて世界で見つかり、そこからアンチウイルスメーカーはシグネチャーを作り始めます。しかしほとんどのアンチウイルスメーカーは、すごく優先度が高い　を作るために早くても24時間から48時間、ケースによっては1週間かかります。WannaCryの場合は優先度が高いので、5月13日から14日ぐらいには各メーカーからシグネチャが提供され、ほとんど100%に近い検知ができる状態になりました。しかし、パターンファイルにはサイズの上限がありますので、アンチウイルスメーカーは、一般的にあまり世の中で見られなくなった、話題にならなくなったパターンというのはどんどん消していきます。WannaCryのパターンというのはまだ残っていますが、既に発見から半年以上経っていますし、おそらくまた1年2年経つと、世の中がWannaCryをほとんど忘れたときに、アンチウイルスメーカーはWannaCryのシグネチャを消していって製品上では検知ができなくなっていくという状況になります。一般的に皆さんがマルウェアの検知試験をやる時は、大体世の中で発見されてから1週間以上たった、どのメーカーも既にファイルを入手した状態で試験をしますので、あまり検知率の比較では差が出ません。しかし、今日私がやったとおり、実際に攻撃が起こったタイミング、つまりまだ世の中のアンチウイルスメーカーが見たことが無いタイミングで比較をすると、大きな検知率の差が出てきます。

WannaCryに関して言うと、実は今日デモでやったモデルのもう一世代前のデータモデル、具体的には2015年の11月、つまりWannaCryが出てくる1年半前のタイミングで人工知能はWannaCryの形を予測していました。つまりCylancePROTECTを入れていたお客様は、その時点から1年半後に出てくるWannaCryに対する防御ができていたということです。これが予測判定というアプローチの強力な部分になります。

おそらく今日ここまでデモをやったとしても、たまたまWannaCryだけ検知できたのではないかと思われる方もいらっしゃるかと思います。我々は皆さんの前で見ていただくというデモをやっていますが、当然、同じことを皆さんの環境でもしていただくことが出来ます。日々やってくる、おそらくまだ誰も持っていないようなマルウェアのサンプルを使って、CylancePROTECTを使って検知ができるかというのを実際にその目で見ていただいて、この製品の予測検知・推論判定の能力を確かめていただきたいと思います。



株式会社アスタリスク・リサーチ
OWASPJapan　代表
岡田 良太郎 氏

デロイト トーマツリスクサービス株式会社
代表取締役社長
丸山 満彦 氏

奈良先端科学技術大学院大学
情報科学研究科　教授
門林 雄基 氏

Cylance Japan 株式会社
最高技術責任者
乙部 幸一朗 氏

Cylance Inc.
会長 兼 CEO 兼 創業者
Stuart McClure 氏

TalkSession 1　テクニカルセッション“AI × セキュリティ”

「"AI" の進歩はセキュリティに何をもたらすのか」

ネット環境の変化による事業環境の変化 IT 技術の進歩、特に "AI" と呼ばれるものが貢献する可能性

トークセッション1では、AIを活用した脅威防御でサイバーセキュリティ業界に「破壊的革新」をもたらしたCylance Stuart氏を囲み、“AI×セキュリティ”をテーマにテクニカルな観点でディスカッション。
ゲストスピーカーには、奈良先端科学技術大学院大学　門林教授（インターネット工学、サイバーセキュリティの研究開発、2008 年より ITU-T においてサイバーセキュリティの国際標準化に従事）、デロイト トーマツリスクサービス　代表取締役社長　丸山氏（経済産業省の情報セキュリティ監査研究会、情報セキュリティ総合戦略策定委員会、個人情報保護法ガイドライン策定委員会、厚生労働省の情報セキュリティ関連の委員会等の委員を歴任）、Cylance Japan 最高技術責任者　乙部氏を迎え、ここでしか聞けないスペシャルトークセッションが実現。モデレーターは、アスタリスク・リサーチ代表　岡田氏（システム開発のコンサルティング事業を展開、システム堅牢化競技 WASForum Hardening Project のオーガナイザー、アプリケーションセキュリティ団体 OWASP Japan チャプターの代表）に務めて頂いた。

岡田 イベント前半では、スチュワートさんに Cylance のヒストリーも含めたお話をいただいて、乙部さんから AI はもちろん、製品として他とどう違うのかをデモで見せていただきました。非常にわかりやすかったですね。さて、このトークセッション前半のテクニカルセッションでは、もうちょっと根掘り葉掘り聞いてみようと思います。去年はこのアンビリーバブルツアーで、おそらく極秘事項なんじゃないかと思うような内容をディスクローズしていただけるというようなセッションになったので、今回社長さんも来られていることもあって、大変期待しています。スチュワートさんはこれまで何度か日本に来られているとのことですが、改めまして、今回の来日を歓迎します。（会場拍手）

Stuart お招きいただき感激しています。何回も来ていますが、今回初めて、日本でサンクスギビングのお祝いをしました。ターキーを探すのがちょっと大変でした。

" 外部 " 環境の変化

岡田 まずは、ご来場の皆さんと共有していきたい点すなわち「外部環境の変化」についてです。この点は、乙部さんから先ほどのセッションでお話いただいたのですが、エンドポイントに限らず、企業の外部環境も含め、最近変わったなと思っているところはありますか？

乙部 脅威の兆候ということでいうと、相変わらずメールで来るものが多いですね。。最近流行りのオリックスさんとか楽天さんとか、三井住友さんとか、中身が開きやすいものに変わっており、メールの中身が高度になっています。中には、リンクが入っているフィッシング系のメールで、メールが来たときにはアクティベートされていなくて、届いたタイミング、おそらくユーザーさんがメールを開くであろうタイミングでリンクがつながる状態になるというものもあります。

岡田 え！それはどういうことですか？

乙部 まず、元の悪意のあるメールが日本時間の夜中くらいに飛びます。その時にはそのメールにあるリンクはつながらない状態なんです。最近のサンドボックスのソリューションではメールサーバー上にあるうちにそのリンクのチェックをするわけなのですが、そのタイミングではリンクは生きていない。なので、チェックしても何も起こりません。そしてユーザーさんに届いて、おそらく朝くらいにメールソフトで見る頃に、リンクはつながる。すごくシン

プルですが効果的、というわけです。

Stuart そう、これってサンドボックスを迂回する攻撃としてよく知られているんですね。他に、AegisCrypter（訳注：Exe の暗号化、マルウェア化ツール）でファイルの実行を遅らせるということができます。75 分、という時間枠が一般的に知られていますが、つまりサンドボックスはそのくらいの時間で検証してみて、何もなければ実行を許してしまうので、こういう実行を遅らせる手段というのがよく知られています。

岡田 確かに先週今週と私のところに届いた、ある銀行を装ったメールは、Google のフィルターもやすやすと潜り抜けて、普通に inbox に入っていたりしましたね。他の視点はありますか？丸山さん。

丸山 外部環境でいうと、最近の銀行や EC サイトのメールは私個人のアカウントにも来ていますし、会社にも来ていたので、対策しないといけないなという話をしていたところです。最近の傾向としては、日本語もちゃんとしていて見分けも難しくなってきたということもあり、組織的にやっているなという感じがとてもします。適当にやるのではなく、研究して本気でやってきているなという感じですよね。

岡田 そういうのはグローバルでも同じなんでしょうか？門林さん、いかがでしょうか。

門林 そのようです。私もいろいろな人たちと情報交換をしていますが、先週もカナダの方も同じだと言っていました。

岡田 その国のカルチャーとかブランドも上手に合わせてローカライズしてくるということですね。

門林 そうですね。幸い日本の場合は、日本語がちょっと変だったり、エンコーディングがちょっと違ったりと気付くことも多いらしいのですが、クラウドによるチェックや検知の仕組みが存在することを前提にして攻撃してきているのが最近のホットトピックです。いよいよ迂回が始まったねと。これはイベージョンアタックとも言われます。

岡田 マルウェアでも、他のものとのコンビネーションで決まるという。いくつかの条件が重なったら初めて攻撃だと分かるというものが増えたと思います。スチュワートさんの観測ではいかがですか？色々なお客様の話をお聞きすると思うのですが。

Stuart ランサムウェアの攻撃なども、急速に洗練されていますし、様々な方法で拡散されています。WannaCry のように、Microsoft の SMB 脆弱性を利用したゼロデイとして拡散しましたし、またランサムウェアでも、コンピューターのブートの非常に早い段階や、ファームウェアで動作するものも観測していますね。これに加えて、ICS（産業機械）の IoT デバイスへの標的型攻撃が増加していると見ています。この 3 年の間に、2 つの調査文書を公開しています。一つは、日本を含めた、全世界の社会インフラを対象にした複数年に渡る攻撃作戦を記録した Operation Dust Storm（「砂嵐大作戦」）、それから Operation Cleaver というものです。日本語版 (※) もありますので、ぜひご覧ください。

※ダウンロードはこちらから可能です。https://www.cylance.com/content/dam/cylance/pdfs/reports/Op-Dust-Storm_JAPANESE_FINAL_1.pdf

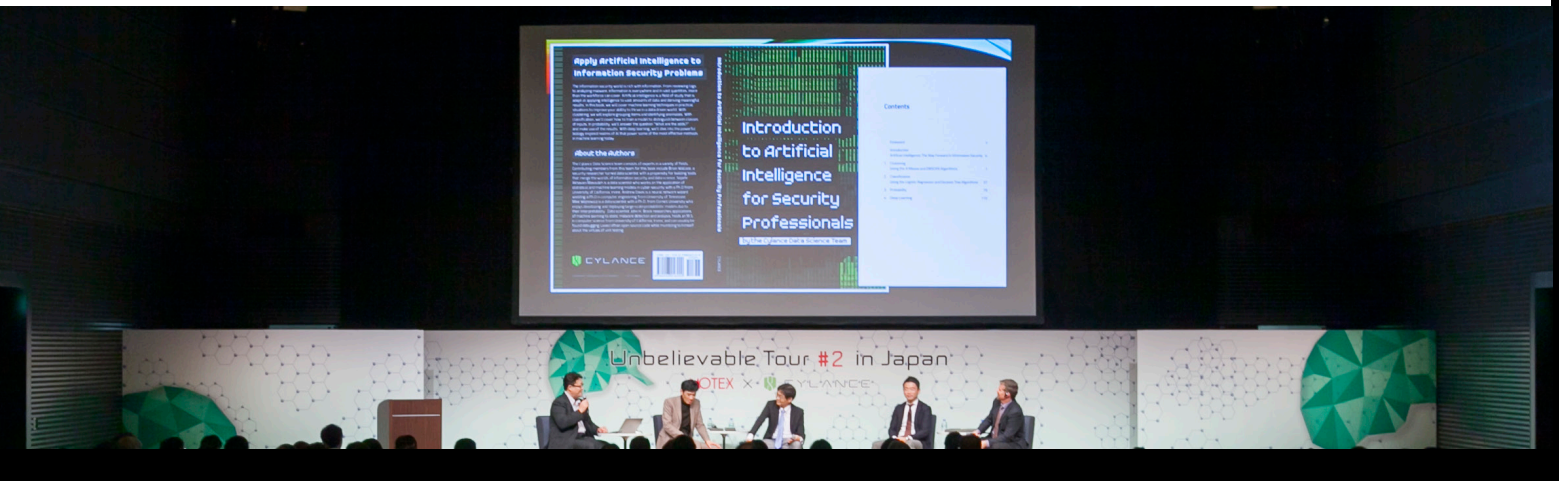
攻撃を迂回するアタックの急増

岡田 従来の、メールサーバーに釣りメールを沢山送りつけてというシンプルなものから変化し、どんどん企業のクラウド化に乗じたものが多くなっているという感じですね。対策ベンダーさんの提供価値というのも変わって来なければならないのではないでしょうか。アンチウィルスだけパソコンに入れておいたら大丈夫なんて時代から、UTM、サンドボックス、またレイヤーごとに細部化されたようなソリューション、それらの組み合わせなど。ユーザ企業から見れば、この変化をどう考えたら良いのでしょう。

丸山 コンサルをする中でお客様にもお伝えしていることですが、最新のテクノロジーを使わないといけないと思っています。というのも、先ほどの門林さんのお話にもあったように、攻撃者側が迂回をしてくる。攻撃者のパターンが変わってきて、今までの守り方では守れないようなことを攻撃者がやってきているので、最新のテクノロジーを使うほうが効率的だと思います。
ただ、何かのソリューションを入れれば解決するというわけではなくて、総合的に対策をしないといけない。Cylance はすばらしい製品ですが、Cylance を入れたら全てが解決するわけでもないし、別のものを入れたら Cylance にとってかわるというわけでもない。なので、色々なソリューションを組み合わせていく必要があります。もはや一つ入れたら終わりという簡単な世界ではないので、そこを理解してどれをやっていくか、これを選んだらこれができて、まだ何が実現されていない、次はそこを考えないといけないといったような、全体を考えたセキュリティをやっていかなきゃいけないですね。

岡田 そこで提案者のポジションから、乙部さんいかがでしょう。また、お客様の悩みの変化、特に一生懸命頑張ってらっしゃるところほど課題を持ってらっしゃるという観察はありますか？

乙部 一般的によく言われますが、サイバーセキュリティは当然プロダクトだけでは対処できません。

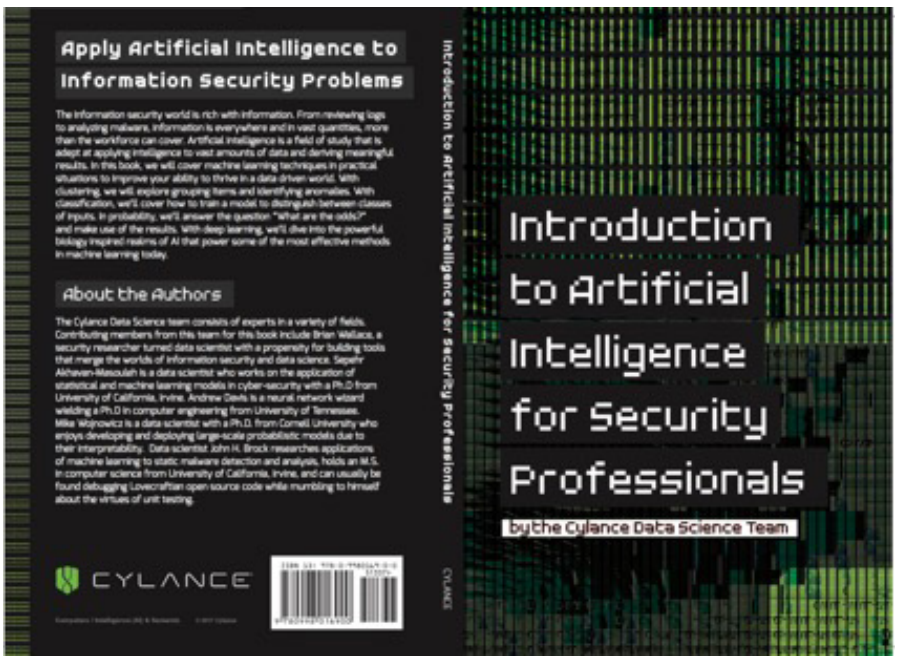


よく 3 つの P「プロダクト」「ピープル」「プロセス」でやるというのはずっと変わっていないと思います。最近特にプロセス部分を含めた経営ガイドラインなど、ようやく世の中の意識が強まってきたかなと感じます。
特にプロダクトの関連でいくと、セッションの冒頭でも話しましたが、皆さんいたちごっこのようなイメージを持たれていると思います。例えばサンドボックスがなんとなく流行ってくると、皆さんがサンドボックスを入れるようになりますし、SIEM が出てくると SIEM を入れます。振る舞い型のエンドポイントが流行ると振る舞い型を入れます。
ただやはり迂回するものが出てきたり、WannaCry が出てきて検知できなかったとなると、皆さんやはり「ちょっとこれじゃだめだ」と思って、また新しいものと…皆さん疲弊されていますよね。
ピープル、プロセスの部分は、メール訓練をしたり、プロセスや CSIRT を作るということが大分進んできていると思うのですが、プロダクトの部分は一向に昔と変わらない。いろいろなものを入れて試してダメ、入れて試してダメということを繰り返しているわけで、あまり進歩が無い。逆にそういったところについて、我々、特に Cylance の日本法人に注目していただきたいと思っています。

リスクコントロールに”AI”は鍵となるのか。

岡田 もう少し詳しくお聞きしていいですか？
やってくるメールが怪しいか怪しくないかを分けるというのは量も膨大ですし、類型も様々ですから、「ピープル」や「プロセス」では追いつかず、やはり「プロダクト」なりで調達したプログラムで対応せざるをえない。しかし一方で、最近メールだけがエンドポイントを攻撃する手段ではなく、様々なパスがありますよね。なんからのパスで感染させた RAT(リモートアクセスツール) からまた新たに別の何かを仕掛けてくるなど、攻撃シナリオも様々です。そこで、「エンドポイントプロテクション」というビジョンのもと、Cylance さんはどういうカバレッジでエンドポイントを守っていくのですか？

Stuart これまでを振り返っても、この市場は攻撃への防御や予防について遅れを取っています。従来型のアンチウイルスがうまく機能しないので、防御する層をいくつも重ねる方法で、攻撃が入ってくる場所へのフィルタをしていました。つまりメールフィルタ、ウェブフィルタ、USB フィルタなど。でもこれらフィルターは、既知の攻撃に対するものであったので、すぐに迂回されてしまいます。加えて、このように複雑にしてしまうので、システム、ユーザー双方に負担がかかってしまいます。
私達は、攻撃対象に対して常に新しい攻撃手法があると考えています。WannaCry のようにネットワーク越しのもの、Stuxnet のように USB 経由のもの、イランで発生したクリティカルインフラの攻撃など、そのほかメール、ウェブ、Bluetooth なども考えられるでしょう。もちろん、人による対応やセキュリティ製品、網羅的なセキュリティ対策が必要ですが、考えてみてください。最初から「予防」のアプローチを取っており、それが 99%くらいの精度で機能していたとしたら、検知の数も、それに対応する数も減らすことができるはずである。私にとっては、これがセキュリティ運用として一番良い形と考えています。つまり「初めから予防することに注力する」ということです。



岡田「予防」のアプローチですか。なるほど。そういうことで最近御社でこんなドキュメント（図 : Introduction to Artificial Intelligence for Security Professionals）を出されているんですね。乙部さん、解説していただいても良いですか？

乙部 もともとの背景から話しますと、我々は人工知能のアンチウイルスというのをマーケティングとしてうたっていますが、その中でも機械学習を使ったアプローチというのは、ここにきて各社が言い始めて、うちも機械学習、うちも機械学習と…

岡田 そうなんですよ！全部「Powered by AI」

乙部 開発の途中で検索エンジンを使ったら、機械学習使ってるって言えるんじゃないかなと私思っているのです

が。スパムフィルターを使っている会社が開発したら、機械学習を使った開発していますみたいな…。（一同 笑）

岡田 その手があったか（笑）

乙部 ですが真面目な話、人工知能は歴史的にずっと変わらないのですが、新しいカテゴリの技術の中で人工知能や機械学習の技術が使われると、最初は「機械学習」とか「AI」とかって呼ばれるのですが、しばらくしてそのカテゴリができると、その製品のカテゴリの名前で呼ばれるようになり、だれも「機械学習」「AI」と呼ばなくなります。先ほど言った検索エンジンだったり、スパムフィルターもそうです。知名度を得る前までは、人工知能や AI として認知されているけれども、実のところ中身、本質は変わらないというところがあると思っています。
そういう意味では我々も今過渡期にいて、この数理モデルを使ったアプローチでセキュリティの製品を出していますが、そもそもこの機械学習、特にサイバーセキュリティの中での機械学習を使うというのはどういうことなのか、どういうステージやレベルがあるのかということを、うちのデータサイエンティストが書いたものがこの本なんです。正直けっこう分厚く、いまは英語しかありません。ただかなり技術者寄りなので、あまり読んでもらえないというか（笑）読む人はパワー入れて読まないといけないくらいの技術者向けの本です。ただすごく面白い本になっていまして、このドキュメントは日本語化します！

岡田 こっちからトスを投げる前に言っちゃいましたね（笑）門林さん、こういうドキュメントどう思われますか？プロの目から見て。

門林 この本の中身、コンテンツを見たら、「k-nearest neighbor」「deep learning」とあともう一つくらい書いてありましたけれど、要するに機械学習という理論がありますが、非常に簡単に言うとパターン認識なんですよね。
音声認識や顔画像認識とかあるじゃないですか。あれを今や「AI」とは言わないですよね。でもあれも同じ技術なんですよね。音声認識や顔画像認識でやっている技術で、こういう k-nearest neighbor、deep learning、とか support vector machine とかいろいろあるのですが、そういったものがずっと作られていて、本当にここ最近 10 年くらいサイバーセキュリティに応用されるようになってきたというところです。

私は 10 年間やっているので、10 年前のことが思い出されるのですが、10 年前はこういったことをセキュリティに応用しようと思う人はあまりいませんでした。我々が機械学習の会議に行って、サイバーセキュリティのワークショップをやって、データセットをこちらから提供しないと解析してくれなかったのですが、今や産業化されるところまで来たと。感慨深いですけれども、それくらい技術的には全うな系譜、蓄積があるものです。

岡田 すごくベーシックな質問かもしれませんが、そういったものをサイバーセキュリティに適用しようと、業界全体が動いて きた背景は何ですか？

門林 一つはやはり、敵が自動化しているということだと思います。要するにビットコインで 2000 円くらい払うとマルウェアを作れるという話があります。結局アドバーサリー（adversary）ですね、敵が波状攻撃でやってくる。日本時間の朝の 8 時とか 9 時に新種のマルウェアがばんばん来るという状態で、従来ですとアンチウイルス会社の方が朝の 8 時や 9 時に慌ててシグネチャ書いてアップデートして配信するということをやっていたのですが、そのアプローチだともう間に合わない。なのでパターン認識の技術、従来は顔画像認識や音声認識に使われていた技術をマルウェア認識に使おうじゃないかという、至極まっとうな発想だと思います。

岡田 スチュワートさんいかがでしょうか。もともとエンドポイントの違ったキャリアを歩んでこられたとお聞きしていますが、「よし、これはエンドポイントを AI で守る会社を作ろう！」と思われたバックストーリーを教えてくださいますか。

どんな「コンセプト」「技術」があるのか。

Stuart 私はもともと、ネットワーク寄りの専門家でした。ホワイトハッカーとして成功していたし、どんなコンピューターでも簡単にハッキングできたと思うくらい、ネットワークを熟知していました。しかし同時に気づいていたのが、すべての攻撃は、エンドポイントに向けられているということです。エンドポイントにあるデータやユーザー情報、CPU リソースなどです。そのため、エンドポイントこそが最終ゴールであり、ここを守る必要があると思ったのです。しかし巷にある技術ではそれが実現できていない。将来に渡って価値が認められ、予測可能なものを作らないといけないと思いました。同時に、皆さんが今指摘された通り、今日の AI の機械学習というのは、非常に複雑なパターンマッチングに過ぎません。もちろんいろんな人がより良くしようとしているが、基本的にはそうであるに過ぎません。しかしながら、機械学習は、過去よりもより良くなっていることも事実です。コンピューターは「忘れない」し、学習することでより良くなっていきます。人間にはこの点は難しい。過去の攻撃からの学習を通して、将来の攻撃を予測するということはアプリケーションには非常に向いているのです。

それらはどんな問題を解決に導くのか？

岡田 有効に活用できそうだなというところもあると思うのですが、課題もあると思います。どうしても 100% を目指しているけれど達成できないというのは分かっているものの、それをどうするのか？というところについて、門林さんコメントいただけますか？

門林 いわゆるディープラーニングで何が騒がれているかというと、精度が一桁上がったんですよね。これまでの support vector machine とか KNN（k-nearest neighbor）は 95% くらいだったんですよ。95% は検知できますとなると、残りの 5%は人間がやらないといけない。誤検知も相当ある。5% の誤検知ならたいしたことないと思われるかもしれないですが、ものすごいデータ量のうちの 5% は、やはり相当なものです。先ほどのプレゼンテーションでもありましたけれども、例えばディープラーニングで 99.7%になると、誤検知率も 0.3%です。これまでの 10 倍以上精度が上がっています。誤検知の対応コストが人間のところも含めて飛躍的に少なくなっている。ある意味実用に耐えうるレベルになったのではないか。それで、皆さんディープラーニングと言っているのではないでしょうか。ただやはり、運用の現場では、その 0.3% の誤検知どうするの？という問題はありますので、そこをどうやっているのか、逆にビジネスの皆様に伺いたいです。

丸山 0.3% と言っても、例えばそれが 1 万件だと 300 件ですので、それなりにかかります。1 万ならいいけど、それが 10 万、100万となることもあります。でも人間でやっていた時、何%見ていましたか？という話になると、もっととても低くなるか、もしくは見ていないので見逃してました、という方が多いはずなので、そう考えるとマッチベターですよね。
確かに 300 件くらいは見なきゃいけない中でも、レーティングができれば例えば重要なもののうち 30 件でも見れば昔よりも大分良かった、という考え方でやるべきだと思います。コストは限界があるので。そこはやはり重要性でやるしかなくて、全部つぶすというのは諦めないといけないと思います。

岡田 そこで興味があるのは、Cylance エンジンの再学習と言いますか、漏れたものに対してどう対応するかの仕組みです。どういう仕組みになっているのですか？

乙部 大体半年から 10 ヶ月に一度くらい新しいデータモデルを出しています。インフィニティという機械学習システムは、その期間中に来た新しいデータを基に学習します。その中には世の中で見つかった新しいマルウェア、特に抜けたものだったり、逆に新しいビジネスで使う見たこと無かった良いファイルなんかもデータセットにはあって、そういったデータを使いながら学習しています。
インフィニティが使っているのはニューラルネットワークというシステムなのですが、4 層以上のディープニューラルネットワークを使っています。いわゆるディープラーニングをベースにしています。
結局システム自体の複雑さが増していて、コンピューティングパワーが必要になっていますが、データ量が増えれば増えるほど、基本的には精度が上がっていきます。前提としてそのデータのクオリティが高ければですが、クオリティが高ければ高いほど、量が多ければ多いほど、より良い学習ができますので、理論上、インフィニティは学習すればするほど検知精度を上げて、誤検知を減らすという動きになっていきます。

Stuart 完璧な説明です。一つ追加するとすれば、データ量が増えれば精度もあがり、私達は 6 − 8 ヶ月に一度の頻度で、新しい数理モデルをリリースしています。しかしこの間に、何か検知が出来なかったモノがあったとしたら、次のリリースを待つには長すぎる。そこでもう一つ、K 平均法（K-means）によるクラスタリングという統計的な手法を取っており、これによって、検知できなかったその攻撃に対して「例外」を認識させ、「曖昧さを持った統計的なモデル」として、それを配信、適用させることができます。よりモデル修正の適用時間を軽減することが可能なのです。

門林 非常によく考えられていると思います。機械学習のアルゴリズム一つで万能ということは無いので、今お話があったみたいに、一段目に K 平均法を使って、二段目にディープラーニングみたいなのは非常にクレバーだと思います。

岡田 エンドユーザーの目線でいくと、例えば Cylance は、実行形式のものには強くてもマクロウイルスはちょっと検知しにくいんじゃないかな、スクリプト言語で動くわけだし…というのが、おそらく過去のどこかの時点ではあったんじゃないかなと思うんです。
Windows の実行バイナリなら何でも来いだけど、マクロウイルスだとちょっときつい、みたいな…そういう新たなバリエーションや攻撃手法というものをどんどん学習させている、あるいはそれに適した学習方法を採用していくということでしょうか。

乙部 そうですね、まず前提として、スチュワートのセッションでもありましたとおり、現在サイバーセキュリティの中でも一番メインのコード実行型の攻撃・脅威の中で、入ってくる入り口は色々あります。メールだったり、メールでも添付ファイルが Excel だったり Word だったり、マクロだったり js ファイルだったり、そのまま EXE がきたりというケースがあります。コード実行タイプの攻撃のうち、ほとんどがいわゆるマルウェアを使っています。マルウェアを使った攻撃というのは、入口のファイルがマクロだろうが js ファイルだろうが、本体（ペイロード）を持っているというのが 99% 以上です。つまり、入り口が何であれ、実行ファイル形式のものが必ず落ちてくるというのがほとんどです。我々は確かに、モデルを作っていて、「PE ファイル」という本体を止めるモデルを作っていて、言い換えると 99% の実行型マルウェア攻撃を止めることができる。ただし手前の入り口に来ている、ドロッパーというものをそのモデルで見れるかというと、現在のモデルはあくまで PE ファイルに対してしか動きませんので、こういったものに対してさらにモデルを作っていくことで、手前の部分でも止めることができるようになります。これは多層防御の考え方と同じで、そもそもメールが届く前に止めれば防御できる可能性が高まるという話で、たとえメールが届いても悪性のマクロであれば止めるということができれば、そもそもマクロから本体が落ちてくることを止めることができます。

門林 プログラミング言語に関係なく、数学的には特徴ベクトルに変換できれば良いので、それが JavaScript であれパワーシェルであれ、何でも良いんですよね。Cylance のエンジニアさんであったらきっと 30 分くらいで処理するフィルター書いて、処理されると思います。

岡田 なるほど。面白いですね。一度見学に行かないといけないですね。

Stuart ぜひお越しください！

岡田 本当ですか！
それこそ本当の Unbelievable Tour(UBT) ですね！テクノロジーの進歩が実用に耐えうるところまで来た。それで、それを使う側がどうするのか？という課題があるというところで、第二セッションの方に移っていきます。最後に･･･先ほどご紹介したドキュメンテーションについて改めてお聞きしますが、日本語版をいつごろ出していただけますか？ 177 ページもありますが…

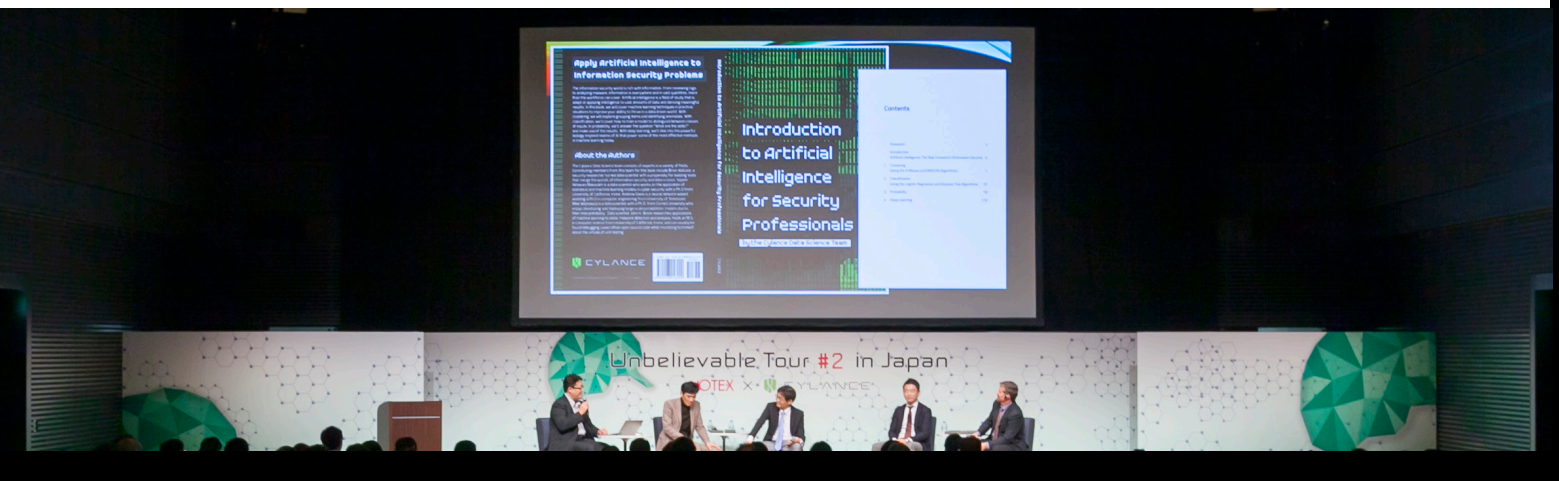
乙部 はい、まさに今翻訳しています。

岡田 そうですか！本当に楽しみにしています。
最後に、今日お集まりいただいた皆様に、技術の進歩でどうやってビジネスを守っていくのかということについて、ヒントや応援メッセージをスチュワートさん、乙部さんからいただけますでしょうか？

Stuart 私達の状況を良くしてくれるであろう技術について、常に注目しておくべきです。機械学習やデータサイエンスは、私達の技術を押し上げてくれるものであることに疑いはありません。旧来の技術は廃れていき、有効でなくなってくる。データサイエンスを適用した多くの技術を見ていくことで、よりセキュリティを高める道が開けるはずです。そしてみなさん自身の負荷を軽減してくれるはずです。そのためにはそれを恐れないこと。よく学び、より良い道に活かすことが大切です。

乙部 我々の機械学習を使ったセキュリティのアプローチというのは、出てきたばかりの技術ではあります。先ほどスチュワートが言ったとおり、本当に色々な技術を見て、怖がらずに試していただいたら良いかなと思います。当然、100% というのは世の中にありませんので、その中でその強みを生かしたセキュリティの設計や運用をしていただくことで、少しでも皆様の暮らしが良くなるというところがゴールだと思います。運用されている方が少し楽になったり、コストが少し下がったり、攻撃を受ける回数が減ったりというところを目指していく中で、我々がお手伝いできれば嬉しいです。

岡田 ということで前半のテクニカルセッションは Cylance からお二人をお招きし、根掘り葉掘り聞かせていただきました。ありがとうございました。



株式会社アスタリスク・リサーチ
OWASPJapan　代表
岡田 良太郎 氏

デロイト トーマツリスクサービス株式会社
代表取締役社長
丸山 満彦 氏

奈良先端科学技術大学院大学
情報化学研究科　教授
門林 雄基 氏

エムオーテックス株式会社
代表取締役社長
河之口 達也

TalkSession 2　ガバナンスセッション　“経営 × セキュリティ”

正しい“選択”は、企業成長の阻害要因ではなく促進要因になるか？

トークセッション2では、「“経営×セキュリティ”成長する事業経営の視点からセキュリティを考える」をテーマにディスカッション。ゲストスピーカーはトークセッション1に続き、奈良先端科学技術大学院大学　門林教授、デロイト トーマツリスクサービス　代表取締役社長 丸山氏に加え、エムオーテックスの河之口も参加。モデレーターは引き続きアスタリスク・リサーチ 代表　岡田氏に務めて頂き、関西弁による熱いトークが繰り広げられました。

岡田　さて、後半のガバナンスセッションは「経営×セキュリティ」と題して、「セキュリティは成長の阻害要因ではなく促進要因になるか」なんてことを書かせてもらいましたけど、要するに「社長に直接聞いてみたい！」ことをざっくばらんに公開討論会という形でやらせていただきたいと思っています。まずはMOTEX代表取締役社長の河之口さん、今日は本当にすばらしい会をおめでとうございます。(会場拍手)

河之口　ありがとうございます。

岡田　去年から実際にエンドポイントプロテクションと、監視の採用事例も伸びてきているとのことですが、実際に使ってらっしゃる方々の声はどのような感じでしょうか？

河之口　正直に言いますと、昨年MOTEXが新しい尖ったAIのアンチウイルス製品を担いで打ち始めたとき、世間は「は？」って思っていたのかなと思います。ところが今は非常に数多くのお客様が我々の元々のプロダクトとの連携（LanScope Catのログ連携）部分まで、我々が思っていた以上に評価いただいております。やはり使ってみたら全然違うと。いろいろなベンダーやメーカーの製品があって、みんな良い良い…と言うわけですけど、やっぱり使ってみたら全然違うというのが、この一年、お客様に使っていただいたリアクションだと感じています。

新たな問題の対応にもたもたする企業、さっさと対応を進める企業

岡田　このように新たな問題の対応にモタモタする企業、さっさと対応を進める企業のそれぞれの思惑や気持ちがあると思います。それを考えながら、どうやってセキュリティを見つつも、でも事業も邪魔したくないという社長さんや取締役会の一番の悩みについて、この第二セッションでは触れていきたいなと思っています。
セキュリティ技術がガンガン上がっていく中で、企業側の方のセキュリティ対応、あるいは事業の保護という視点でも、ここ一年二年で変化はありますか？

丸山　実は私、日本のデロイトのグループのサイバーセキュリティのアドバイザリーもやっており、日本のデロイトの全メンバーで12,000人くらいいるのですが、ぶっちゃけトークでいうと、うちでも事故は起こります。起こるとやはり上から下までけっこう慌てます。お客さんにも色々と説明しないといけないですし。事故をするとセキュリティちゃんとしないといけないなということがよく分かりますよね。そうなると予防で防げるなら防いでおいた方が楽だなとなるわけです。一回は許してくれたとしても、二回三回続くとかなり辛い。ですので、きちんと「予防」する。でも当然ながらお金は無限にあるわけじゃないので、そこをどうするかということよく考えて賢くやろうという方向にうちの会社ではなっています。

岡田　そうですか。クライアントはどうですか？

丸山　クライアントは、気付いているところはそうなってるけど、気付いてないとこは、センサーが無い（事故したことに気付かない）から、血をだらだら流しながら歩いてるみたいな感じのところもありま

すよね。センサー無いと分からないですよね、自分はどうなっているのか。

岡田 あー（笑）。企業のリジリエンスに関わってくる部分だと思いますが、門林さんの観察ではどうですか？

門林 そうですね、私はビジネスにも関わっているのでよく分かるのですが、情報収集に来られる方の中でやってるところほど、そのことを言わないですね。「これは競合を追い落とすためのツールなので、セキュリティはもう弊社のコアコンピタンスです」ってことすら言わない会社さんも多いと思います。そのことに気付かずに情報収集だけしていても、トップがどれだけ真剣にやっているかは分からないと思いますね。

岡田 河之口さん、セキュリティや情報管理を真剣にやっている人たちの特徴はありますか？

河之口 まず日本特有のITベンダーとユーザーの関係があります。大中小関係なくベンダーとの関係が深い…別の角度からするとロックイン状態。長い付き合いで色々やってきてくれたので、ベンダーからプロダクトを導入するという世界があると思いますが、それとツールと良し悪しって違いますよね。

岡田 そうですね。ベンダーロックがかかっているところは、けっこう辛いところがありますよね。弊社も色々とセキュリティ関連のマネジメントサービスをやっていますが、開口一番、「うちはどこどこさんのお世話になってるから」と言われることがあります。とりあえずニーズが満たされていればそれでいいんです。けど、詳しく聞いたら色々問題があって、それでも「今のベンダーが必要だとか、うちではできない、とか言ってくれないと別のベンダーに相談できないんですよ」という。ポリティカルなことが施策の阻害要因になっています。

門林 そこは、僕ら傍から見ていると不甲斐ないですね。RFPの主導権を完全にユーザー企業で握っているところと、そうじゃないところで、かなりセキュリティの成熟度が違うと思います。我々は基本的にはSIerさんには仕様書を書いて、「これ持ってきてと依頼し、あとはインテグレーションはうちらでやるから」といったスタンスです。日本の会社でそれやってるところ、あんまりないと思います。「何つくったらいい？ああ、そうやって作るの？いくらかかるの？ああ、そんなにかかるのね」みたいなね。先ほどベンダーって話がありましたけど、日本の長らくユーザー企業とSIerの関係性っていうのが、かなり日本特有のランドスケープを生んでいるかなと思いますね。

岡田 なるほど、なるほど。そういう意味ではITに限らず、自社でそのサービスを責任持ってやっているところと、とにかく物作ってるんだけど全部他社さんのオーダーですというところで、ITや情報をどうやって守るのかというメンタルは違う気がします。SIerさんって、システムを作ることには真剣です。だけどそのシステムのセキュリティどころか、作ってる人たちの端末の監視ですら無頓着だったりする。

作ったものを自分のところで動かして商売をやらないから。かたや、ユーザ企業には、SIerさんに作ってもらうんだけど、自分のところでイニシアチブ持ってるとか、開発体制も自社にあるというか、MOTEXさんももちろんそういう会社だと思うんですけど、そういうところは作って動かしてるものに何かあったら大変なことになるので、それをどうにかすることに対してすごく真剣なのではないか…とまあ、こういう観察を持っています。
それが会社の事業を守るという視点で見たときに、LanScope CatとかCylanceなど、セキュリティ投資が必要な、ともすれば余分なものと思われがちなものに対して投資するときのメンタルに表れていると思うんです。そんな観察は無いですか、河之口さん。

河之口 根本的に、私ももともとこの業界で長い間営業をしてきて、お客様に提案をしたり導入させていただいたりと、いろんな会社とお付き合いさせていただきましたが、正直、社長、役員、特にITの担当役員を除いて、ベンダーの言うことを超えてさらにその自社のリスクとか、経営についてITを本気で考えようという方は、私はあまりお会いしたことが無いです。これはあんまり言うと怒られちゃうので…まあ大阪で、ってことにしときましょうか（笑）

岡田 そういうところでは、誰が頑張ってちゃんとやっているんでしょうかね？

河之口 こういう風にできないのか、こういう風にやってくれ。IT担当者がんばれよっていうのはもちろんあります。だけどそれ以上に踏み込むという方は、やっぱり分からないので・・・なかなかそれ以上はあまりないかなと思います。

外部環境の変化に対応する経営課題の変化

岡田 そうすると、経営層に対してのインプットをどうするかというところは一つ大事なポイントだっていうところですかね？

丸山 私は学生の頃、家庭教師をやっていたのですが、二つのパターンの依頼のされ方がありました。一つは、勉強はすごくやる気があるけどやり方が分かんないから教えてやってくれ、とお願いのされる方と、うちの子全然勉強しないんですよ、何とかしてくださいというパターンです。要はやる気があるけどやり方がわからないからそこをサポートしてほしいのと、やる気が無い人をなんとかしてくれということで、後者の依頼の場合は断っていました。
やる気が無い人を一生懸命教えることは難しいですよね。だから真剣に考えていない経営者見たら、深入りしないですかね。私は。経営者が無能だったらみんな不幸になります。僕も社長なので人のこと言えないですが。やり方がわからずに困っている方はたくさんいますからね。まずそこを助けます。

岡田 なるほど、そのスタンスだったとしてですね。じゃあやりたいんだけどやり方分からないと言ってくれるようになった会社は増えていっている傾向なのか、減っている傾向なのか？について河之口さんと丸山さんの観察はいかがですか？

丸山・河之口 増えてますね。

岡田 なぜ増えてるのでしょう？やはり事故ですかね？

丸山 事故ですね。自社で事故無くても、他社で起きてたら「おい、うち大丈夫か」ということももちろんあるし、調べたら実は…とあがってきた会社もあります。やはりWannaCryなどは、うち絶対大丈夫ってところも意外と被害にあってることもあり、ぼろぼろと騒がれるようになってますよね。10年前はNHKでセキュリティの話無かったと思うんですけど。NHKでセキュリティの話題するようになったら、さすがに今まで気にしなかった社長も、「セキュリティか」ってなりますよね。だからやっぱりちょっと意識上がってると思います。

岡田 なるほどね。その追い風要因というのは事故以外に無いものなんですかね？

河之口 日本に商用コンピューターが入ったのって50年くらい前だと思うんですよね。野村證券さんですかね。月給2万円の時代に、32キロバイトのメモリのコンピューターが月200万と昔読んだ気がします。そのころ、コンピューターって事業経営者からすると全くわからない専門的な世界だったと思います。でも今はポケットにアップル製品がある。先ほどのNHKも含めて、コンピューターの世界は、わけが分からないものから身近なものになってるのは間違いないと思います。

門林 特に若い経営者の方は教えなくても分かってるんじゃないかなと思っています。年齢と相関があると思ってまして、50から上の経営者の方が聞いてこられるのは「セキュリティ…どうやったらいいんですか?」と、おそらくあまりわかってない方が多いと思います。事業についてはすごくよく分かってるけど。で、40から下の経営者は「うち、これとこれ入れてるんですけど、EDRどうなんですか？機械学習どうなんですか?」という具体的な質問が多い気がします。主観ですけど。

岡田 確かにそうかもしれないですね。既に色々やってみてるんだけどどうだろう？って思ってる方が増えてきてるのはあるかも知れないですね。ノーガードじゃなくなっている。そういう観点で行くと、テクノロジーの選び方はどうしましょうか。先ほどのAIだとか色々ありますけれど、何かに付けて機械学習だAIだって言うじゃないですか？それをどうやって選んでいけば良いんでしょう。

丸山 どうでしょうか・・・AIとか機械学習については、理屈は昔からの話で、それを今まで音声認識とか画像認識って使っていたものを、同じパターン認識だったらセキュリティ、マルウェアの分析にこれ使えそうだって、目鼻が立つ人がいるのは重要ですよね。そうでないものもたくさんありますが、そこを見抜ける素養のある人が社内にいると思うので、そういう専門知識を持った人の話を聞いて、判断する人は判断するという役割分担でしょうか。

岡田 一方で、例えば未だにデータセンター保守要員何十人みたいなIT投資を見かけます。お金かけてやってると思うんですが、これだけクラウドの時代に、以前から体制が変えられてない。要するにリソース配分を変えていかないといけないんだけど、それは経営者じゃないと無理ですよね。

門林 そうですね。だから、その技術の潮目が四年ごとくらいに変わるというセンスをもって、経営者側が変えていかないといけない。一旦それ入っちゃったら、「俺はSUNのワークステーションっていう神殿を守るのが仕事だ」みたいな、神殿化するITって話あるじゃないですか。「触るな！！動いている…！！」みたいなね（笑）孤高のERPとかね。色々あると思いますが、それがクラウドですよ、IoTですよって。イノベーションの動きは非常に早いので、この業界は非常に早く変わるんだと。したがって二・三年に新しい血を入れていかないといけないっていう判断を経営者ができるかどうかってことだと思うんですよ。

今、考えるべき「成長」に影響する「リスクコントロール」

岡田 サイバーセキュリティリスクの変化だけではなくて、事業を推進するITの変化ってところが対策の変化を呼ぶということですね。　最近ネットとネットやデータのインフラと、それを使う人との関係性が変わっています。事業の成長のためにIT使う出来事は、あっという間にすごい安価に、市場の破壊的イノベーションというんですかね、突然やってくるじゃないですか。人間型とか犬型のロボット作ってたら、いきなりAIスピーカーに全部持ってかれるみたいな…変化にしたがってセキュリティの配分が変わっていけたら良いなと思うんですけどね。

門林 ただね、そこはすごく日本人って農耕民族的だと思うんですよね。「ここはオレの田んぼ」みたいな、収穫スケジュール決めたらそれを守ることは天才的なんですよ。日本人て。やっぱりアメリカ人、先ほどのスチュワートさんもそうですけど、狩猟民族なんで、今のやり方と次のやり方違うっていうのに全然抵抗が無い。

岡田　それはやっぱり怖いものなんですか？普通の社長さんは…社長さんおられるのでズバっと聞きますけれども。

河之口　そうですね。怖いですよね。例えば過去ERPが出てきたり、グループウェアが出てきたり、色んな流行物がありましたけど、よく言われる統合分散を繰り返すみたいな、なんとなく今はそういう時期なのかなという気はしますね。特にセキュリティの分野は。結局きっかけを作る何かが乗り込んできたときに起こると思うんですけど、今そういう時期に来てるのかなって思います。

丸山　「統合分散」はキーワードとしての振れ幅と実際の振れ幅が違うかなと思ってます。キーワードとしては大きく振れてるけど実際は小さい。僕が社内で下の人から怒られるのは、「全然言ってること一貫性無いけど」「忘れてんのちゃうの」って言われるくらい変化してる。
だから、変化が怖いかというと、逆に、現在についていってない自分が怖い。将来こうなるだろうってなんとなく見えますよね。そこに向かってない、全然違うところに行ってるというのが怖いんですよ。このまま行くと前に崖があって落ちるの分かってるのに、何で自転車こぎ続けてるんだろっていうのが嫌なんですよね。
こっち行ったら落ちるって分かったなら違う方向だなと。最初はこう言ってたけど実は間違っていたから訂正。やっぱり目の前で起こってる将来のことが見えてる中で、そこに向かってないのが怖いので、私はすぐ変えたい派なんですね。それを朝令暮改と言われているのだと思ってます。

門林　多分、日本の経営者のマインドから言うと、中期計画っていうのがあって、五年のグロースマイルストーンみたいなのがあると思うんですけど、たぶんサイバーセキュリティの世界で一番の鍵は投資なんですよ。インベストメント。アメリカはこういう状況ですとか、欧州中央銀行ドラギ総裁がこんなこと言いました、みたいな。金利政策変わると、日本円にレバレッジしようとか、証券じゃなく債券にいこうかとか、BRICsじゃなくてやっぱりヨーロッパだよとか、アメリカで…日本で…みたいなことやってるんですけど、この変化は割とそれに近いんですよね。例えば標的型攻撃で、「これはすごく悪い標的型攻撃だ！」と思って対策してたら、ある日それが、それはNSAですみたいな話になってバタバタバタバターって転ぶ。（一同爆笑）
そういうドラマ性というか、日々ドラマ性があると思ってまして、Bluetooth！ワイヤレス！クール！っていうのがあると思っていたら、BlueBorneとかKRACKとかやってきて、もうワイヤレスは終わった・・・みたいな。それが下の人から見ると、社長言ってること違うとなるわけですが、それが自然です。本来こうあるべきです。

岡田　そうですね。IT使って仕事するのは、ホントのところはずいぶん大変になってきました。さて、すごく発散しましたけど、事業を何をもって成り立たせるのかっていうのがまずありきのセキュリティと考えると、事業側の変化に合わせて対応の側を変えていくというそのトリガーが一番分かりやすいかなと思うんですよね。
何が変化のきっかけになるかというと、事故はもちろんですが、でも事故ってセキュリティを意識するっていうより、「この事業止まったらこんなに大変だったんだ」っていうことを意識するから、止まらせられないようにするにはどうしたらいいんだろうって話かなと思います。
最近もある会社さんで、怪しいものが動いた、急に想定外のソフトが立ち上がった、と。なんでそんなことになったんだろうって思ったら、それをどういう経緯で誰が立ち上げたのか分からない。それを調べたいし、社員のせいじゃないっていうのをスクリーニングしたいんだけどそれができないって言うから、それなら端末監視ですよね、と。
あれ？なんだかLanScope Catを担いでしまうような形になってしまいましたが（笑）。

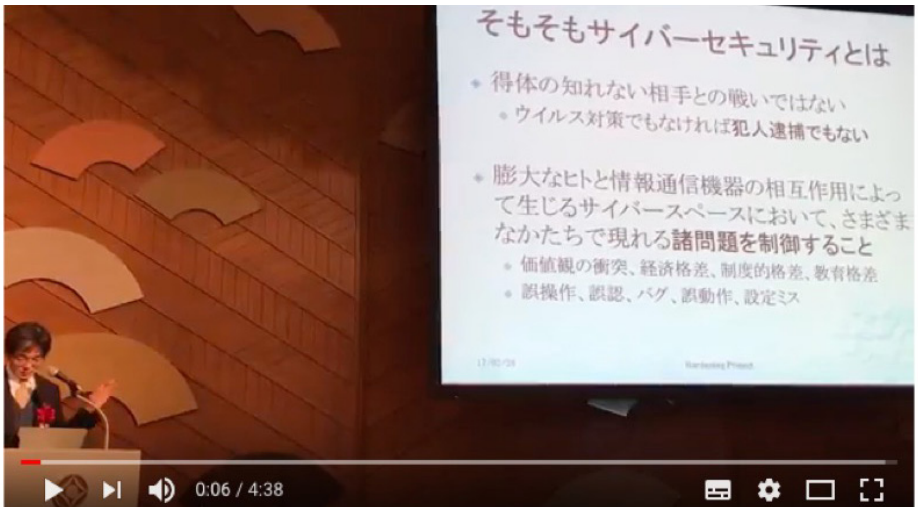
事業の流れとその時に起きるヒヤリハットみたいなものが、必要なソリューションへのトリガーになっている。セキュリティは防衛投資だと思っていて、自分のオフィスの領域を平和に保つためにどういう軍備を配置すべきなんだっけ、ずいぶん近いところから飛んでくるなと思ったらそれに対して何かしなきゃいけないというか…ちょっと政治的なことに誤解されたくはないんですが、ぶっちゃけそういう感じになるじゃないですか。なので、「セキュリティやっても儲からない」って言っている時点でもうダメだなと。ランニングコストだと思ってるからなんじゃないかなと思って。事業と社員を守るために最低限必要なものは毎年変わりますから。

丸山 事故はちょっとマシになってきたという話はしましたが、結局はブランドなんですよね。「デロイト」っていうブランドを守る。僕はセキュリティのコンサルをしているから、僕らからするとうちで事故されたら最悪なわけで。ブランドは品質を含めてちゃんと守らないといけないっていうのはビジネスの成功への基礎みたいな。
ブランドが無いところにビジネス作りにくいですよね。それが毀損されるっていうのが怖い。個人情報が漏えいして、事故起きました、結局ブランドが落ちるのが問題なわけで、そこで一人1000円だか500円だか配るっていうのは実はたいしたことないんですよね。本当はブランドのところがやっぱり一番将来にわたって売り上げを減らしてしまう可能性があるということが心配なんです。
信頼とかブランドとか気にしてセキュリティやる。ビジネスを成功させるための最もプリミティブなとこだと、経営者も含めて最近思ってくれています。

成長に貢献するセキュリティ経営を目指して

岡田 この写真に写っているのはネットでもう公開されている門林さんのある講演なのですが、「そもそもサイバーセキュリティとは」とあります。これちょっと解説してもらえますか。

門林 要するにサイバーセキュリティといったら、「そんなの警察に任せたらいい」って人がやっぱりいるんですよ。そうじゃないということを書いています。犯人逮捕でもない。ウイルス対策は一部です。結局、よくあるのが「うちの会社にはそんな悪い人いないから」「うちの会社の従業員めちゃめちゃ優秀だから」って言う人いるんですよね。やっぱり操作ミスしますよねって話で、操作ミスするし、警察がいたらなんとかなるのかっていうとそうではなくて、イスラム教の人もいるし、鯨食べるのが嫌な人もいるし、色々いるんですよね。そういう人たちがサイバースペースで価値観の衝突を起こしているんですよね。



だから「セキュリティどうにかしてくれたまえよ」という人もいるんですけど、人類が恒久平和を保てたらこの問題もなくなるんじゃないでしょうかって私は思います。貧富の差もありますし、人間だけじゃなくてバグとか誤動作とかというのもありますし。DNSで見てますと、ビット反転みたいなのも見えるんですけど、通信エラーも含めて諸問題があるんですよね。その中で、機械の問題、人間の問題、自然現象・ノイズみたいなものもありますし。誰かのせいにする、うちの問題じゃない、うちの従業員は優秀、政府や警察に任せとけばいいっていう問題じゃないって話ですよね。
例えば、自動車の事故はどこの会社さんでもあるじゃないですか。それはやっぱり自動車保険かけたりして、トレーニングして、対峙してるんですよね。同じだと思うんですよね。

岡田 この辺は、サイバーセキュリティを研究するとか、サイバーセキュリティで問題の無いビジネス環境を作るって言うときに重要なコンセプトだと思うんですけど、今年立ち上げられたサイバーリジリエンス構成学研究室っていうのは、まさにこういうことに取り組むって感じですか?

門林 そうですね。一言でいうと、安全運転を支援しようってことです。「アイサイト」に相当するものがネットに無いんですよ。そのリンクをクリックしても大丈夫な技術…例えばLanScopeとかMOTEXさんの技術や色々な技術を使う、というのが無いんですね。最終的には自動車も総合技術なんですよね。ブレーキっていう技術があります。シリンダーって技術があります。エンジンっていう技術があります。で、それなんか全部見て、分けわかんないなーっていう人いないですよね。だって自動車ですから。(一同爆笑) セキュリティの話になるとEDRとかWAFとかIPSとかよくわかんないんですよねって言われても「いや、それ部品ですから社長」って話なんですよね。そこのメタファーも含めて、業界として理解を醸成したいかなと。最終的には、サイバースペースで事故しても被害者が死なないようにする、

従業員を保護できるようにする技術を作っていきたいなと思っています。

岡田　MOTEXさんのところで作っている監視とかログとかの技術も、何か起こったときに、どうやってトレースするんだろうっていうところに皆さん喜ばれてるんですよね？

河之口　そうですね。ただ、我々が難しくするのではなく、簡単にシンプルにしていくことにチャレンジしたいと思っています。分散と言いましたが、要は複雑化してると思うんですよね。とにかく難しい世界にどんどん行きつつあるけど、できるだけシンプルにお伝えできればなということを思っています。

難しい複雑なことをお客様にご納得いただけるような翻訳作業が無いと、結局はベンダー側の思惑が色々あってサイバーセキュリティの世界はよく分からないとなってしまう。まずはシンプルに分かっていただきやすいように進んで行きたいなと我々は思っています。

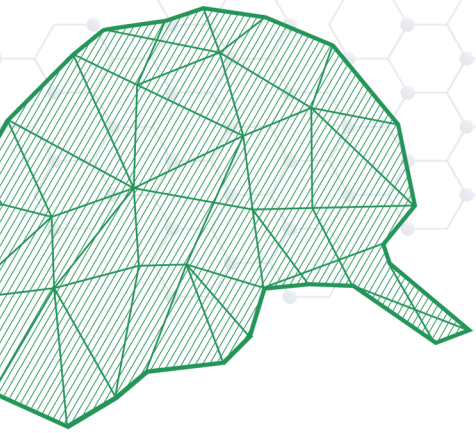
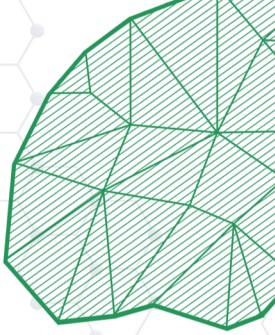
岡田　さて、今日はまず、技術に関することを、根掘り葉掘りざっくばらんに、作ってらっしゃる方・考えてこられた方にお聞きしながら、その裏づけも含めディスカッションしました。
そして後半は、社長さんもお呼びして観察などもお聞きしながら、セキュリティをうまくマネジメントし、成長の阻害要因は意外と事業の組み立て側にもあるよね、という形で話も拡がったところではあります。サイバーセキュリティを諦めていただきたくないなというところで、最後に、応援メッセージを一人一人に頂けますか。

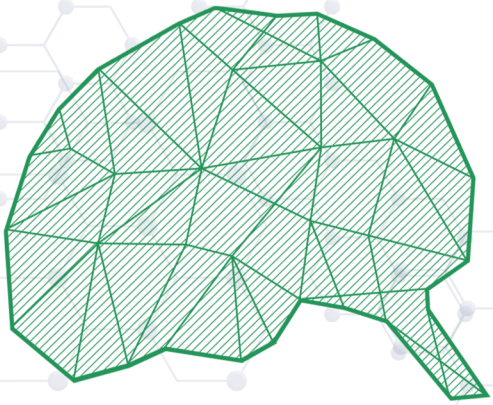
丸山 私は今、会社のグループ全体のアドバイザリーをやっている中で、会社が成長するため、ブランドを毀損しないためにセキュリティをちゃんとしないといけない、セキュリティだけじゃなくて、品質やブランドに関係するところはちゃんとやりましょうっていうのが、今後のビジネスの成長のプリミティブな底辺を支えるものだ、とトップが最近セキュリティの重要性に気付いている、深く理解し始めてきていると思っています。セキュリティは特別なものとしてやるのではなく、当たり前のようにやりましょうっていう感じになってきたので、成長してよかったなと思っています。

門林 セキュリティ、レジリエンスかもしれないですが、安全運転技術みたいなものが必要です。スマホとかパソコンとか相当な性能なんですよね。車で言ったら、皆さんがフェラーリを100円で乗り回せるみたいな感じですよ。みんなフェラーリ持ってるんですよ。アクセルをピュンって踏んだら時速300キロ出るんです。危なくてしょうがないですよね。そういうものをみんな使いこなして、ものすごく生産性高い仕事をしているわけです。当然それにまつわる安全運転支援技術が必要なはずなので、この分野の技術がもっと発達したら良いなと思います。

河之口　私はITベンダー側の自戒も含めてですが、技術的に良いからというのではなく、取引の長さとか勧めてもらえるからとか、技術の比較が無い世界…さっきロックインといいましたが、そのしがらみを越えるような世界を作るためには、やはり分かりやすく伝えていくということが重要だと思っています。先ほど翻訳と言った部分ですね。そういう世界になっていけば良いなと思います。我々が全てではないのですが、そういうスタンスで、本音でお伝えできるような会社にしていきたいと思っています。

岡田　今日はお聞きしていて、サイバーセキュリティを諦める必要は無いなということと、そして河之口さんのおっしゃった、できる限りシンプルに扱えるようにしていきたいということが、今日のパネリスト全員の思いなのかなとすごく感じました。シンプルに判断して、それをどうやって実行するかというところは、一生懸命汗かきましょうと、それが事業ってもんじゃないでしょうか、というところが共感してもらえたら、サイバーセキュリティに屈することなく成長を遂げていけるのではないかなと、勇気を得た感じです。ご来場の皆さん、ご登壇の皆さん、本日はありがとうございました。



MOTEX
Secure Productivity

エムオーテックス株式会社

本 社　〒532-0011　大阪市淀川区西中島 5-12-12 エムオーテックス新大阪ビル　TEL：06-6308-8980
東京本部　〒108-0075　東京都港区港南 1-2-70 品川シーズンテラス5F　TEL：03-5460-1371
名古屋支店　〒460-0003　名古屋市中区錦 1-11-11　名古屋インターシティ3F　TEL：052-253-7364
九州営業所　〒812-0011　福岡市博多区博多駅前 1-15-20　NMF 博多駅前ビル2F　TEL：092-419-2390

TEL：0120-968995 受付時間 9：30 - 12：00、13：00 - 17：30（月～金曜日）
※携帯電話・PHS からは 06-6308-8981 をご利用ください。
E-mail：sales@motex.co.jp　　ＵＲＬ：www.motex.co.jp

2018 年 2 月発行

●お問い合わせは当社へ