【特別対談】

これからのIT セキュリティは自動化に向かうのか？

今、そしてこれから取り組むべきIT セキュリティ対策とは

（写真左より）新免泰幸氏、満永拓邦氏

2017年、社会全体を巻き込んだランサムウェア Wannacry。数々の被害を生み出す一方で、サイバー攻撃がもはやすぐそばにある脅威であり、日常レベルでもその対策が急務であることに気づかされる大きなきっかけとなった。

2020年の東京五輪開催を控え、サイバー攻撃の急増が見込まれる中で、企業はどのような心がけをするべきか。

本記事では、東京大学 大学院情報学環 セキュア情報化社会研究グループ 特任准教授であり、セキュリティに関する数々の著書を持つ満永 拓邦氏と、CSIRTの支援やアクティビティを自動化する「Network Insight」を提供する Core Security ジャパン カントリーマネージャー 新免泰幸氏の対談から、今後必要となるセキュリティ対策を探ってみる。

セキュリティ対策は、ツールの導入よりもオペレーションの整理が先

満永氏　セキュリティ対策と聞くと、多くの方が「ツールや機器の導入」を思い浮かべると思います。ですが、サイバー攻撃というものは、何かを買って入れておけば防げるという類のものではありません。どんな高価で高性能の機器でも、それを効果的に運用できなければ意味をなさないのです。

新免氏　数年前と比較して、大企業はもちろん、中小企業でも ITセキュリティに対する意識は急速に高まっているように感じます。多くの企業は何らかのセキュリティ対策は行っていますし、機器・ソリューションの導入にも前向きです。ただ、セキュリティの運用管理については、あまり目が行き届いていないように私も感じています。

満永氏　私自身、セキュリティをテーマに据えた様々なセミナーにお招き頂き講演することもあるのですが、その際には「事前の備え 5項目」というものをお伝えしています。ツールや機器を導入するのなら、まずはこの 5項目が実行できる体制を整えて、その上でちゃんとオペレーションできるものを導入しなければなりません。

事前の備え5項目

1. **エスカレーション体制 (社内連絡体制)**
   インシデント発生時に連絡する窓口や、対応の責任者を事前に定めておく。
2. **情報資産の管理**
   組織が保有する情報資産 (データ)を洗い出し、リスク評価を通じて事業継続に影響を与えるものについて把握し、アクセス権を設定するなど適切な管理を行う。
3. **IT資産の管理**
   組織が保有しているパソコンやサーバなどのIT資産について、管理担当や設置場所について把握し、アップデートなどの更新管理を含めて適切に管理を行う。
4. **ネットワーク構成管理**
   パソコンやサーバなどの IT資産が接続する車内ネットワーク並びに、インターネット接続の構成、各種ネットワーク機器の設定を管理する。
5. **ログ取得と活用**
   インシデント発生に備えて、サーバやネットワーク機器にてログを取得し、保存する。原因追求と影響範囲の特定には、ログが不可欠である。

セキュリティの現場を、若い人が憧れるような場所にしたい ― でなければ日本の IT に先はない

新免氏　CSIRTや SOCの重要性は、数年前と比べかなり浸透したように感じています。ただ、体制を作るためには人材が必要となります。実はここが一番のネックなのではないでしょうか。

満永氏　そうですね。やはり優秀な人材の確保は難しく、そのためセキュリティ対策が進まないという企業からの声をよく聞きます。しかし、セキュリティ対策や運用の全てをセキュリティに詳しい担当者が手動で行う必要はありません。セキュリティ分野であっても定常的に発生する業務フローについては手順を明確化して、自動化を進めるのが良いと考えています。COBITと呼ばれるフレームワークでは、IT管理プロセスが適切に定義され、運営されているかを測定する手段として、6段階の成熟度モデルが提唱されています。例えば、担当者が場当たり的な対応をしている (レベル１)や、手順が標準化および文書化されており、後任に訓練を通じて伝達されている (レベル３)など、成熟度の指標が示されています。こうしたプロセスの成熟度という観点からセキュリティの業務を見直して、できるだけ属人化を避け、自動化を進めて効率化を図るというアプローチも重要だと考えています。もともと ITは業務効率をあげるための手段であるはずなのに、最近はITやセキュリティに振り回されているようなケースが見受けられます。

新免氏　特にセキュリティ運用の観点で付け加えますと、その ITが生み出す膨大なセキュリティ関連の情報に振り回されているのが実状だと思います。

満永氏　セキュリティは、組織の IT基盤を支える重要な要素だと思います。しかし現実として､セキュリティ担当者は非常に厳しい立場に置かれていて、何も起きなければ｢彼らはいったい何をやっているんだ？」と陰口を叩かれ、何か起きれば｢彼らはいったい何をやっていたんだ！」と叱責を受けるような場合もあります。安定したシステム稼働を支えるという業務の重要性が理解されず、セキュリティ担当者が適切に評価されないのであれば、優秀な若い人材の確保も難しくなります。

東京大学 大学院情報学環 特任准教授
満永 拓邦 氏

京都大学情報学研究科修了後、神戸デジタル・ラボのセキュリティソリューション事業部に所属し、ペネトレーションテストやセキュリティインシデント対応などの業務を行う。
2011 年、JPCERT/CC 早期警戒グループに着任し、標的型攻撃などサイバー攻撃に関する分析等に従事する。
2015 年、東京大学情報学環セキュア情報化社会研究寄付講座特任准教授として着任し、サイバー攻撃防御手法の研究やセキュリティ人材育成、Fintech・ブロックチェーンなどの研究を行う。
「サイバー攻撃からビジネスを守る」や「CSIRT」(ともにNTT 出版) 等の書籍の共著・監修も行っている。

新免氏　それは面白い話ですが、残念でもありますね。若く優秀な人材にとって働きがいのある現場にするためにも、多様なセキュリティ脅威の手法が生まれていることに対してセキュリティ担当者が新しいアイデアを創造したり議論したりする時間を確保することは、業界全体における課題なのかも知れませんね。そのためには業務効率化は欠かせない。

今、セキュリティの自動化に取り組んでおけば、5 年後は負担が軽減されます

満永氏　昨今のセキュリティ現場は、人手不足と同時に属人化の問題も顕著になってきています。例えば、経営陣からのセキュリティ専門チームである CSIRTを構築せよ、という“号令”が出た時には、上層部から信頼が厚く、社内の各部門に顔が利き、調整能力が高いスタープレイヤーが配属されることが多くみられます。ただし、組織が安定期に入れば当然異動が行われるわけで、彼らがその対象になることも例外ではありません。その際、彼らが引っ張っていたセキュリティ専門チームは、その人がいないとスムーズなオペレーティングができないという事態を招く可能性があります。これを私は「2代目問題」と呼んでいます。属人化され過ぎた組織では、業務の再現性が低くなり、業務の質の安定化が図れなくなってしまうのです。

新免氏　おっしゃる通りですね。業務の再現性で言いますと、例えば、セキュリティの脅威検知においても疑わしいものに対してアラートが発せられた場合、それが誤検知なのか真の脅威なのか、脅威だとしてもそれがどの程度深刻なものなのか、緊急を要するのか、様子見でも大丈夫なのか、それらの判断はそれらの判断は満永さんのおっしゃる「スタープレイヤー」であるセキュリティアナリストの手に委ねられています。お言葉を借りれば２代目問題はここにもあってスタープレイヤー頼みの状態ではダメなのです。

満永氏　少し話が外れますが、私が担当する講座では、独立行政法人 情報処理推進機構から委託を受けてセキュリティ担当を育成するプログラムを実施しています。現在は 1年間に 75人を育成する体制となっていますが、将来的にはより多くの人材を育成する体制の構築を期待されています。これに対応するには、背中を見て学ぶという徒弟制度や家内制手工業のような人材育成では難しく、トレーニング環境の自動構築と映像授業を組み合わせたような、教育の自動化を進めていかないとできません。しかし、逆に言えば、そうした環境が整えば人材育成が加速できます。企業のセキュリティ運用や人材育成においても、同じことが言えるはずなのではないでしょうか。

Core Security ジャパン カントリーマネージャー
新免 泰幸 氏

日本電気 (NEC) でインターネット黎明期における企業向けのネットワーキングソリューション事業に従事。
Lucent Technologies 等テクノロジーベンダーで企業ならびに通信事業者向けプロダクトマーケティング、Nokia にて国内企業向け事業統括、Fortinet にてジャパンカントリーマネージャを経て、2015 年から Damballa(Core Security の前身) でサイバーセキュリティ運用ソリューションの事業開拓に従事。

新免氏　そうなんですね。実は私たちが扱っている「Network Insight」でセキュリティ自動化の典型的な事例があります。総務省から都道府県庁に“配下の市町村を網羅するセキュリティ運用体制を作るように”というお達しがありました。とは言うものの多くの市町村を抱える庁では、人力で運用し続けていくのは現実的ではないとのことで、某庁より自動化のご相談を頂きました。「Network

Insight」では、マルウェア感染の判定に必要なセキュリティアナリストのスキルと判定後対応の運用者の手間を自動化できるため、少ない人員の中でも運用を確立すること目論んでご導入いただいています。もちろん、すぐに全ての作業を自動化するのは難しいのですが、まずはできるところからやっていく。でなければ、セキュリティの現場は､今後どんどん身動きが取れなくなってしまう。

満永氏　自動化に関して時折受ける誤解は、“自動化すると絶対に楽になる”ということですね。むしろ自動化すると、これまで“気がつかなかったこと”や“知らなかったこと”が見えてきて、いろいろな新たな課題が生じてくることもあります。だから、自動化した当初はむしろ作業が増えることもあります。でも、本来それはやらなければいけないことなのです。最初は大変だけど、やっておくと 3 年後あるいは 5年後には負担が軽減されます。

新免氏　次々増えていく“やらなければならないこと”は必ずしも定型的な業務ばかりではありません。そこで AIや機械学習がグローバルレベルで蓄積したインテリジェンスを使って非定型な業務も自動で捌き、人は“気づかなかったこと”や“知らなかったこと”にフォーカスしていくべきだと思います。

満永氏　おっしゃるとおりですね。今後、セキュリティ担当者が高度な判断を求められる場面はより増えていきます。迅速、かつ正確な判断を下すには、セキュリティ担当者は、常に最新の情報をインプットして、いざという時に備えなければならない。となれば、知見を広げるためにセミナーや勉強会に参加する必要もあるでしょうし、情報交換をする機会を得なければならないでしょう。その時間を捻出する手段として、自動化は最適な方法でしょう。

Network Insightの特徴

Network Insightは、10年以上の科学調査とビッグデータインテリジェンスに基づく高度な感染端末検知システムです。実際のトラフィック内に存在する隠れた感染挙動を、自動的かつ正確に捉えることができます。端末が標的型の脅威やマルウェアに感染している疑いがあると、継続的に複数の脅威プロファイラーで証拠を積み上げ、インテリジェンスと照合して感染事実を判定し、同時に脅威リスクから対応の優先順位付けを行います。 犯罪が起きると複数の証拠を集めて犯行を特定するプロセスに似ています。

Network Insightは、端末の感染ソース、侵入経路、端末の OSに関わりなく、既知および未知の脅威に関する実践的な情報を提供します。また、CSIRT担当者が明確な証拠を入手できるため、直ちにリスクの高いデバイスへの対処を行うと共に、それ以外のデバイスへの感染も阻止することができます。

https://www.coresecurity.com/ja
150-0001
東京都渋谷区神宮前6-28-9
東武ビル6階

E-mail : japan@coresecurity.com