セキュリティを「面」で考えてみよう

アルテア・セキュリティ・コンサルティング代表
二木　真明

変化の見え方は視点によって変わる

昨今、サイバー攻撃の中身が変化してきていると言われています。以前は、興味本位とか自己顕示的な「実験」であったサイバー攻撃が「営利」など明白な目的を持った実用的なものに変化しているという意味で、ここ数年のトレンドとして語られることが多い話です。たしかに、IT という視点から見れば、その傾向は間違いがないように思います。でも、それは正しい表現なのでしょうか。

また、攻撃が、いわゆる IT 技術だけではなく、ソーシャルエンジニアリングなど、人間系を標的にしたものと組み合わされ、「ハイブリッド化」しているとも言われています。これも、実際に起きている事件を見れば明らかです。こうした傾向は、最近のこととして話題に上りがちですが、はたして本当に新しいものなのでしょうか。

ちょっと視点を変えてみましょう。まだ IT がそれほどクローズアップされる以前、インターネットもなかった時代に、たとえば企業から情報を盗んでいた産業スパイの手口を考えて見てください。同じように、パソコンもネットも使わないお年寄りからお金をだまし取る「振り込め詐欺」の手口を考えてみてください。こうしたスパイや詐欺の手口も、昔々から大きく変わっていません。昨今「ソーシャルエンジニアリング」と言われているものの多くが、こうした手口と同じものです。つまり、これらは IT 以前に「犯罪」の手口として、ずっと存在していたものなのです。こうした「犯罪」の歴史という視点から見ると、「変化」は違った形で見えます。つまり、古くからあった犯罪、つまり、ある動機があって、目的があり、それを達成する手段があるという流れの中の「手段」にあたる部分に IT が使われ出したという見方になります。

つまり、我々の視点ではサイバー攻撃の「動機」、「目的」の大きな変化に見えたものが、実は犯罪という視点から見れば、単に手段の変化に過ぎなかったということになります。どちらが、より広い見方であるかは自明でしょう。犯罪の手段には様々あり、その一つの要素である IT が最近では大きな比重を占めるようになってきた、ということなのです。

単純に、犯罪のレベルとそれに使われる IT のレベルを軸とした面を考えてみれば、図1のようになります。

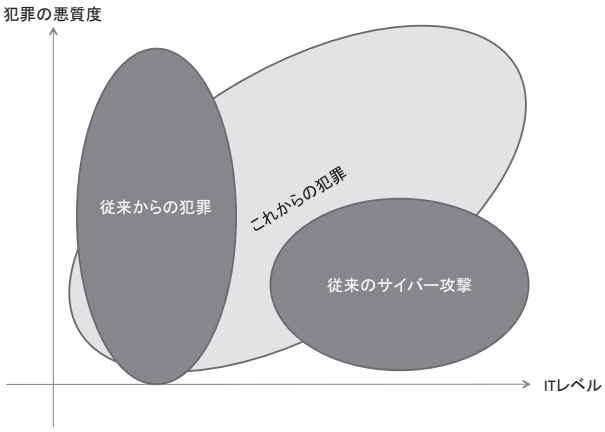

図 1

もちろん、これは犯罪だけではありません。戦争、テロ、過激な主張・抗議のための活動、いわゆるアクティビスムなどすべてにおいて同じことが言えるでしょう。最も身近な例は日常生活やビジネスなどです。これらも、IT を手段のひとつとして、どんどん変化しています。我々はついついセキュリティを中心に物事を見ようとしてしまいます。しかし、それが自分たちの視野をかなり狭めてしまっていることに気づいていなかったのかもしれません。IT ＋セキュリティとそれが手段になっている何かという、ふたつの軸を持つ面として全体をとらえてみると、これまで見えていなかった本質が見えてくることも少なくないのです。

ビジネス V.S IT V.S セキュリティ

ビジネスと IT、ビジネスとセキュリティ、IT とセキュリティの相関関係を同じように書いてみると面白い傾向が見えます。たとえば、IT 化はビジネスの効率を向上させますが、ビジネス効率に寄与する度合いの高い新技術ほど、安定性や安全性に問題がある傾向があります。これを図にしてみると図2のような形になるでしょう。

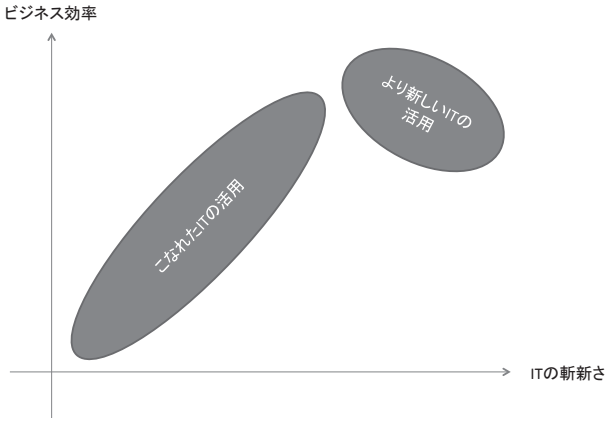

図 2

こうなる理由は、IT の斬新さとその安全性（安定性も含む）が、図3のような分布になってしまうからです。

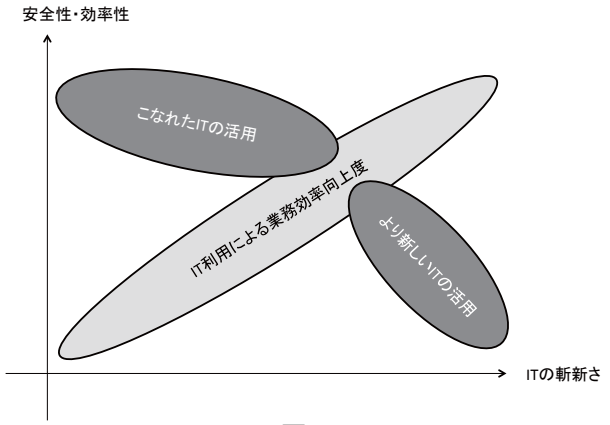

図 3

ビジネスの目的からすれば、可能な限り効率を上げるために IT を活用していきたいのですが、新しい技術にはリスクが伴います。つまり、図2のできるだけ右上に位置をとりたいのですが、図 3 の傾向があるため、より上に行こうとすると、逆にトラブルによって効率が下がってしまうリスクが大きくなってしまうわけです。

ここまで書けばもうおわかりでしょう。我々セキュリティに携わる関係者が何をすべきか、それは、図3の右下がりの傾きをできる限り小さくすることなのです。しかし、ともすれば我々は図3の右側のリスクの高い部分を使わないようにしようと考えてしまいがちです。極端な例を述べればノート PC の持ち出し禁止などがこれにあたります。これは、セキュリティからの偏った視点にほかなりません。ビジネスがセキュリティに求めていることとは本質的に違うのです。少なくともセキュリティのマネジメントに携わる人たちは、このことを決して忘れてはいけません。単に使うなと言うだけならば、こんな簡単なことはありません。いかに安全に使ってもらうか、そのために何をすべきかを一生懸命考えて実行するために給料をもらっている、セキュリティ部門のマネージャーはそう考えるべきなのです。また経営者はそれにみあった人材を正しい待遇をもって、そうした仕事に配置すべきなのです。決して、企業内のセキュリティ管理やリスク管理は「閑職」ではありません。もしそう考えている経営者がいるとしたら、会社の先行きは危ういと思うべきです。

情報技術（IT）V.S セキュリティ技術／IT 人材 V.S セキュリティ人材

昨今、情報セキュリティ人材の不足が叫ばれ、育成推進のかけ声高く、全国で CTF などが開催されています。では、「セキュリティ人材」とは、いったいどのような人材なのでしょうか。IT 人材全体のマッピングは ITSS などで細かく行われていますが、おおざっぱ

に見るならば、以下のようなものが上げられるでしょう。

・IT 企画やマネジメントにたずさわる人材
・IT 基盤技術者（ネットワーク）（設計、構築、運用・保守）
・IT 基盤技術者（サーバ・アプリ基盤）（設計、構築、運用・保守）
・アプリケーション技術者（設計、開発、構築、運用・保守）
・セキュリティ技術者（？？？？）

どうしてセキュリティ技術者の部分に？を入れたかというと、セキュリティのどの部分の仕事をするにしても、先に挙げたいずれかの知識や経験が必要になるからです。しかも、技術的に見れば、かなり高度な部類の知識や経験が必要になります。なぜなら、最先端のサイバー攻撃を考え出す連中は、こうした分野のトップクラスの技術者だと考えられるからです。必然的に、セキュリティ技術者も、レベルが上がるほど、それぞれの分野に分化していかざるを得ません。一方で、攻撃はあらゆる切り口から飛んできます。従って、どこから攻撃が行われているかを素早く判断して、適切な人材をディスパッチする役割も必要になるでしょう。こうした役割をになう人材は、幅広い技術全般にわたる一定レベルの知識とマネジメントスキルが必要になります。つまり、どれをとっても、「セキュリティ」という単独科目はないのです。むしろ、基本的なセキュリティの多くの部分は、IT の各分野に組み込まれています。つまり、本来ならば、その部分は「セキュリティ技術者」ではなく、その分野の「IT 技術者」がカバーすべき部分だと言えるのです。ここでも、セキュリティという単独の軸ではなく、IT という「面」でセキュリティをとらえると、問題の本質が見えてくるでしょう。強いて、セキュリティ技術者という名前をつけるならば、それは、IT 全般についてセキュリティがどうあるべきかを押さえられるジェネラリストか、もしくは特定の分野の技術の上に、そのセキュリティを極めたトップエンジニアに与えられる称号であるのかもしれません。これは極論かもしれませんが、それほどはずれた話ではないだろうと私は思っています。ゆえに、基本的なセキュリティ技術は、各分野の IT 技術に含まれる基礎科目として教えられていくべきものであって、それらと切り離されるべきものではないと考えます。

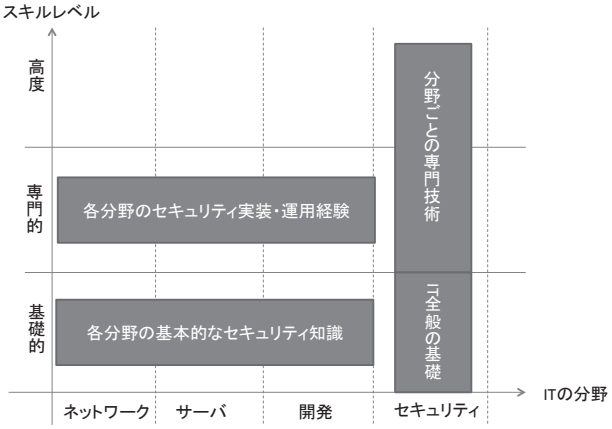

図 4

図 4 にそのイメージを示してみました。各分野の技術者には、基礎知識としての必要なセキュリティ技術と、その実装、運用の経験が求められます。たとえばネットワーク技術者ならば、ファイアウォールのポリシー実装や運用程度はできなくてはいけません。一方、セキュリティ技術者は、最低限、IT の全般的な基礎知識が求められます。その上に、セキュリティだけではなく、専門分野の知識が不可欠です。少なくとも、ネットワークセキュリティ技術者はネットワーク専門技術者と技術的な会話が出来る程度の知識がないと仕事になりません。こうした形でかみ合ってこそ、IT 分野にセキュリティが根付き、また、高度な相手に対して対抗できるセキュリティ専門家が活躍できる土俵ができるのです。

経験上申し上げれば、独学のみで育った中途半端なセキュリティ技術者ほど危ういものはないのです。きちんとした動機付けや倫理観の醸成が、セキュリティに携わるものにとってはきわめて重要です。CISSP のような国際的な資格取得時には、必ず職業倫理に関する宣誓書の提出が求められますし、ハッキ

ング技術などのセミナーを海外で受ける際にも同様の書面にサインを求められることが多々あります。そういう意味で、「とにかくCTF」というような昨今の風潮には大きな危惧を抱いています。

全国津々浦々から参加者を募って競技会を行い、トップレベルのチームを表彰することで、若者たちに与えられるモティベーションは、セキュリティを守ることではなく、単に勝って有名になることなのかもしれません。それでは、昨年、フィッシングサイトを作って補導された中学生の「目立ちたかった」という動機となにも変わらないのです。CTFの主催者は、こうした状況に陥らないように配慮する責任を負うのだということを忘れないでください。また、大量に技術者を育てたあげく、働く場所がないというような事態が生じれば、職にあぶれた技術者がダークサイドから誘惑を受ける可能性もあります。本当に今、それだけの技術者を育成して、働く場を提供できるのかどうかも、もう一度考える必要があります。

長年、JNSAも関わってきた育成イベントに「セキュリティキャンプ」があります。全国から応募してきた若者を書類で選考し、一堂に集めて集中的に高度なセキュリティ教育を行うのですが、そこでは技術のみならず、倫理観についての教育も必ず行われます。グループ活動を通じた一体感の醸成や、その中でセキュリティに関する正しい方向付けを行ってきました。また、キャンプ卒業生のコミュニティ育成にも力を入れ、彼らが孤立することがないように配慮し、さらに地方キャラバンなどを通じて、キャンプに直接参加できなかった若者たちへのフォローも行っています。残念ながら、予算、講師のキャパシティーなどの問題から限られた活動にとどまっていますが、卒業生にはセキュリティ分野で活躍している人も多く、着実に成果を上げてきたイベントと言えるでしょう。今回、このセキュリティキャンプの講師陣を中心に、新たなCTFイベント（SECCON）が進められています。JNSAでこのイベントを運営する意義は、単に優秀な若者を発掘するということではなく、地方大会に参加して敗れたチームをも含めて、その地域、地域にコミュニティ作りを進め、こうしたセキュリティに興味を持つ若者たちをダークサイドの誘惑から守っていくことにあるのだという点を強調しておきたいと思います。これも、CTFの優勝という「頂点」ではなく、裾野も含めて面として見ていくという考え方だろうと思います。

我々は、とかく物事をセキュリティ側から見ようとします。それを全否定するつもりはありませんが、時々は、セキュリティとそれが向かい合う別の何かをあわせて面で考えてみてください。きっと、新しいものが見えてくるだろうと思います。