Optimizing Your Security

やっぱり理想論？ セキュリティ教育で「全社員に対策を徹底させる」ことはできるのか

テクノロジーでは防げない “人”という脆弱性をどうすれば良いのか

組織には、どれだけ堅牢なセキュリティ製品を導入しても、カバーしきれない脆弱性が存在する。それは、“人”である。フィッシングメールを社員の誰か1人でもクリックしてしまったら、あるいはテレワークをしている外出先にパスワードを書いたメモを置いてきてしまったら……。たちどころにセキュリティは崩壊する。だが、従来のセキュリティ教育ではそうした過失を防ぐことはなかなか難しい。今求められるのは、セキュリティの“知識”ではなく“意識”の変革なのである。

みゅーらぼ代表
セキュリティアウェアネスエバンジェリスト
情報通信研究機構（NICT）招へい専門員
平田 真由美 氏

電通国際情報サービス
金融ソリューション事業部
DXビジネスユニット
デジタルイノベーション部
シニアコンサルタント
小幡 廣和 氏

過去最多を記録したフィッシング報告件数、“人”が狙われている

ランサムウェア、サプライチェーン攻撃、テレワークを狙った攻撃……。新型コロナウイルス感染症のパンデミック以降、サイバー攻撃は激化している。

そして、こうした攻撃をよく見ると、ある共通点があることに気づく。それは、攻撃の入り口として“人”が狙われていることだ。マルウェアを潜ませたファイルをメールに添付して送りつける、あるいはマルウェアを組み込んだWebサイトに誘い込むなど、“人”を起点として攻撃が始まっているのである。

この傾向はデータでも裏付けられている。フィッシング詐欺に関する情報を収集・発信しているフィッシング対策協議会の調査によれば、2021年8月のフィッシングメールの報告件数およびフィッシングサイトのURL件数は、2008年の調査開始以来、ともに最多を記録したという。

企業・組織において、“人”は明らかな脆弱性である。これまでITシステムへのセキュリティ対策は継続的に行われてきたが、“人”に対する対策は十分ではなかったのではないか、という疑問が出てくる。

こう書くと「我が社では半年に1回、フィッシングメールの訓練を実施している」「社員全員にセキュリティ研修を受けさせた」といった反論があるだろう。しかしそれでセキュリティ意識が全社員に定着したと言い切れるだろうか。……実際には難しいだろう。社員側からしても「やらされ感」があり、また頻度も少ないため、“なんとなく知っているレベル”にとどまるのではないだろうか。

こうした現実を踏まえて、米国では「セキュリティアウェアネス（Security Awareness）」というキーワードが注目されている。本記事の続きではセキュリティアウェアネスの専門家の意見を聞きながら、これからのセキュリティ教育を考えていこう。社員のセキュリティ意識を、たとえば私たちが外から帰ってきたら手洗いをするように、“やって当たり前のレベル”にまで高めるには何が必要なのだろうか。

エバンジェリストが教える「セキュリティアウェアネス」

「セキュリティアウェアネスエバンジェリスト」として、セキュリティアウェアネスの普及活動を行っているのが、みゅーらぼ代表 平田 真由美 氏である。

同氏は、日本ネットワークセキュリティ協会（JNSA）などの非営利団体や独立行政法人で情報セキュリティ啓発や人材育成、コミュニティ作りなどに携わった経歴を持つ。現在はセキュリティアウェアネスに関する活動のほか、国立研究開発法人情報通信研究機構（NICT）の招へい専門員、IPA10大脅威選考メンバーなども務める。

「JNSA時代、経済産業省が所轄するインターネット安全教室という事業に携わり、その後もセキュリティ対策推進協議会（SPREAD）で、セキュリティについて各地域でサポートする『情報セキュリティサポーター』を育成する取り組みにも参画しました。こうした活動を通じて感じたのが、興味を持っていない方にセキュリティの考え方を伝える難しさでした」（平田氏）

どうすればセキュリティへの関心の低い相手にも、セキュリティの重要性を伝えられるのか。なかなか答えを見いだせない中、海外のワークショップで出会った言葉が「セキュリティアウェアネス」だったと平田氏は語る。

「セキュリティアウェアネス」とは何か。平田氏は“健康”を例に次のように説明する。

「皆さん、健康になるために必要な知識は持っていると思います。バランスの良い食事、適度な運動、睡眠をしっかりとる、などですね。では、それを実践できているでしょうか。知識やリテラシーがあるのと、実際にやるかどうかは同じではないのです。しかも運動しろ、野菜を食べろ、と押し付けられると嫌になるのが私たち人間なのです。けれど、健康を意識して生活している人は自分からそういった情報を収集し、自ら実践していますよね。健康を意識している人は健康に対するアウェアネスが高いということになります。これが知識・リテラシーとアウェアネスの違いです」（平田氏）

健康に関する知識があったとしても、それを日常から実践するのは難しい。実践を可能にするには、アウェアネス（意識）なのである。セキュリティに関しても同様だ。そのアウェアネスが高まれば、教育で得た知識、トレーニングで獲得したスキルを日常生活の中で自ら活用・実践しようとする。さらに、自ら知識・スキルを獲得しようとする。

このように、継続的にリスクを認知し、回避しようとする習慣化された行動・判断を生み出すセキュリティに対する意識こそが、「セキュリティアウェアネス」なのである。

ISIDが作成した「セキュリティアウェアネス」解説動画
https://youtu.be/53mZGdegHfQ

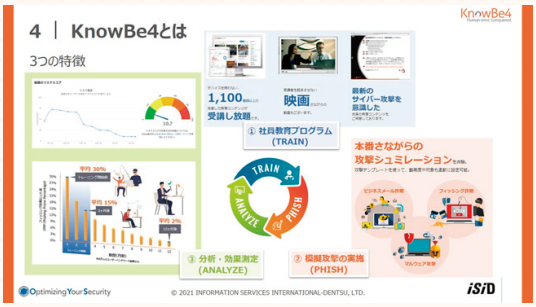
iSiD　KnowBe4 Human error. Conquered.

多種多様なコンテンツを通してセキュリティアウェアネスを醸成する

では、セキュリティアウェアネスを高めるために必要な取り組みは何か。1つは、1人ひとりのセキュリティの知識・スキルに応じた適切かつ継続的な教育・トレーニング。もう1つがその可視化だ。

そして、この2つを備え、グローバルで4万社以上に活用されている「セキュリティアウェアネス・プラットフォーム」が「KnowBe4」である。KnowBe4の国内代理店の電通国際情報サービス（ISID）シニアコンサルタント 小幡 廣和 氏は、次のように説明する。

「KnowBe4は、全従業員に対するセキュリティ意識向上トレーニング、多様なテンプレートを使った疑似フィッシングメール訓練、訓練結果の分析という3つの要素から構成されます。そして、この3つのサイクルを回していくことで、組織全体のセキュリティアウェアネスを高めます」（小幡氏）



▶ KnowBe4の特徴

KnowBe4の特長の1つが、多彩で魅力的なコンテンツだ。従来のセキュリティ教育のコンテンツというと、プレゼンテーション資料を中心にした「真面目」「堅い」……といったイメージがあるかもしれない。もちろんKnowBe4にも比較的硬いコンテンツはあるが、一方でハイクオリティの映像コンテンツにゲームやクイズといった、セキュリティに関心のないユーザーでも積極的に楽しもうと思えるコンテンツが豊富にそろっている。

KnowBe4の人気コンテンツの1つ、『The Inside Man』のダイジェスト版
https://youtu.be/5rHEal82BME

「セキュリティ教育で弊社にお問い合わせいただくお客さまの多くが、『個人の知識・スキルに合った訓練をしたい』とおっしゃいます。その点でもKnowBe4は最適です。さまざまなコンテンツがそろっているので、あらゆるレベルのユーザーに最適なコンテンツを提供することが可能です」（小幡氏）

従業員に送信する疑似フィッシングメールも多様なテンプレートから選べる。その内容も、オリンピックや新型コロナウイルスなど、最新の社会情勢を反映したものに常に更新されつづける。

さらに「可視化」という点でも、疑似フィッシングメールの開封率を可視化し、時系列で確認したり、業界の平均値と比較したりすることも可能だ。

「専用のダッシュボードには組織全体のリスクスコアが数値で可視化されるのに加え、訓練メールのクリック率が時系列で表示され、時間とともに徐々に低下していく様子がグラフで確認できます。KnowBe4を導入している同じ業界の平均値も表示されるので、現在、自社がどの位置にいるかもわかります。また、訓練メールをクリックした従業員だけを絞り込んで、適切なトレーニングを実施するといったことも可能です」（小幡氏）

▶ KnowBe4のダッシュボードイメージ

強制されても身に付かない、「自ら選んで学ぶ」ことが大切

長年、セキュリティアウェアネスの啓発に取り組んできた平田氏も、KnowBe4を非常に有効なソリューションだと評価する。

「セキュリティアウェアネスを高めるには、自分に合ったコンテンツを自分で選択して自ら学習できることが非常に重要です。結局、学習を強制されてもこなすだけになってしまいがちです。KnowBe4には、動画やアニメーション、クイズなど、観たくなる、やってみたくなるさまざまなコンテンツがそろっていることがとても魅力的だと思います」（平田氏）

日本ではまだ認知が低い「セキュリティアウェアネス」だが、米国ではすでに市場が存在し、さまざまなソリューションが提供されている。その中でも、KnowBe4は最も注目されているソリューションの1つであると小幡氏は語る。

「特に最近は、製造業を中心に海外も含めたグループ全体のセキュリティアウェアネスを高めたいという声が増えています。従来は各国で個別に教育していたのが、それでは間に合わなくなり、KnowBe4のようなプラットフォームを求める声が大きくなっているのです」（小幡氏）

なお、KnowBe4を管理するのにITの知識・スキルは必要ない。IT部門はもちろんだが、総務部門や人事部門などでも問題なく活用できる。ただし、中長期で継続的に利用するものだけに、ある程度の計画は必要になる。そこについては、ISIDが支援を行う。

「KnowBe4の導入支援はもちろんですが、会社としてどういう取り組みが必要なのか、教育・訓練の計画をどう立てるか、あるいは訓練メールをクリックした従業員への教育をどうするかといったことまで細かく支援しますので、安心してご活用ください」（小幡氏）

トップ自らが先頭に立つことの重要さ。セキュリティを当たり前のものに

アフターコロナの時代、サイバー攻撃者はますます"人"を標的としてさまざまな攻撃を仕掛けてくるだろう。だからこそ経営トップの役割が重要だと、平田氏は次のように述べる。

「新型コロナウイルスで明らかになったのは、各国の文化の違いです。いくらマスクが有効だという科学的エビデンスがあっても、マスクを推奨しなかった国もあります。セキュリティも同じです。まずは企業トップがセキュリティの重要性を認識し、自ら行動することが、社内の文化を作り、組織のセキュリティアウェアネスを高めるために不可欠なのです。社会全体が、『セキュリティ対策？そんなの当たり前でしょ』となるといいですね」（平田氏）

KnowBe4であれば、経営トップから現場まで全員がそれぞれに最適なコンテンツを楽しみながら学び、個人そして組織全体のセキュリティアウェアネスを高めることができる。"人"に対するセキュリティ対策の必要性を感じているなら、ぜひ検討していただきたい。

株式会社電通国際情報サービス（略称 ISID）
金融ソリューション事業部　戦略アライアンス部

〒108-0075 東京都港区港南 2-17-1
E-mail：g-security@group.isid.co.jp
Tel：03-6713-7030
ソリューション紹介 URL：https://security.isid.co.jp/knowbe4/

本ソリューションの詳細情報はこちら