Optimizing Your Security

最大の脆弱性「人」をどう改革する？
働き方の変化で問い直されるセキュリティ

セキュリティ製品で固めても、人からほころびが生まれてしまう

新型コロナウイルス対策で、企業のテレワークは爆発的に加速した。これは、何層ものセキュリティ技術で守られた上でルールに従って利用してきた社内ネットワークではなく、自宅のような防御が薄く自分勝手に運用できるネットワーク環境から会社にアクセスすることを意味している。こうした中、これまで以上に重要になるのは社員のセキュリティに対する「意識」と、それをどう「教育」していくかだ。

INTERVIEWEE

株式会社電通国際情報サービス
金融ソリューション事業部
営業企画部

赤澤 卓真

KnowBe4 Japan 合同会社
日本代表

根岸正人

アルテア・セキュリティ・コンサルティング
代表

二木真明

「セキュリティは大切」というかけ声だけでは守れない

しばしば「人は最大の脆弱性」と言われる。たとえ次世代ファイアウォールやUTM、サンドボックスといったさまざまなセキュリティソリューションを導入していても、取引先や顧客を装い、実際のやりとりをそのままなぞった電子メールの添付ファイルをうっかり開いたり、本文中のURLをクリックしたりすると、悪意あるソフトウェアに感染することは避けられない。こうした人の脆(もろ)さを突かれ、情報漏えいやランサムウェアによって業務停止に追い込まれるケースは枚挙にいとまがない。

セキュリティは技術だけでは確保できない。さまざまなサイバー攻撃から自社の業務や機密情報、顧客の個人情報を守るには、人や組織がセキュリティの大切さを意識することが重要だ。こうした問題意識に基づいて、昨今、多くの企業が従業員のセキュリティ教育を定期的に実施している。この結果、たとえば従業員に「セキュリティは大切ですか？」と尋ねたら、10人が10人とも「はい」と答えることだろう。

だがそれは果たして、具体的な行動に結びつくレベルに達しているだろうか。頭ではセキュリティの重要性を理解したつもりでも、クラウドサービスを始めとする新たな環境で未知の攻撃に遭遇したときに、身を守る最も適切な方法を選べるだろうか。

テレワークが「新常態」となりつつある今、既存のセキュリティ教育の限界を打破した、新たなアプローチが求められている。

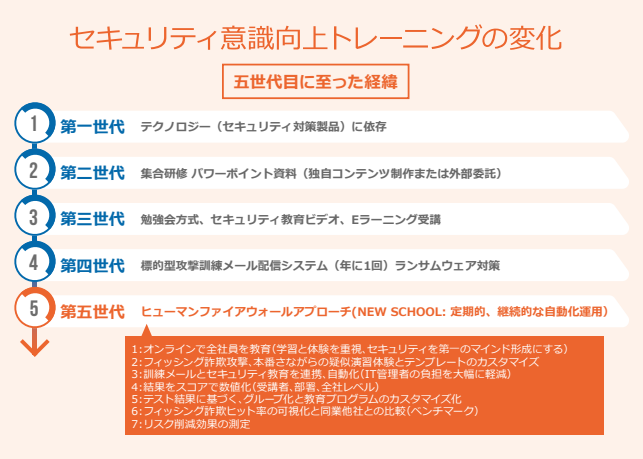
新たな環境で頼りになるのは 1人ひとりのセキュリティ意識

この数年、働き方改革の一環として、またデジタルトランスフォーメーション(DX)の一手段として、クラウドをはじめとする新たなテクノロジーの導入が進んだ。こうした変革には多くのメリットがあるが、一方で過去は明確だった企業の内と外とを分ける境界があやふやになる事態も招いている。

しかも、こうした取り組みにはスピード感が求められる。新型コロナウイルス感染対策の一環として一気に広がったテレワーク導入の場合が顕著だが、環境整備を急ぐあまりにセキュリティ面の検討には目をつむってしまうケースは少なくない。その結果、セキュリティのルール整備の穴や人の心理の隙を突いたサイバー攻撃がどんどん広がっている。

この問題は、テレワークを前提とする新しい働き方の中でさらに重要になるだろうと、アルテア・セキュリティ・コンサルティング代表で、電通国際情報サービス(ISID)金融ソリューション事業部のセキュリティビジネス技術戦略アドバイザーを務める二木 真明氏は言う。

「自宅で仕事をしていると、会社にいるときと違って、何かあったときにサポート部門へ尋ねたり、周りに相談したりすることは難しいのではないでしょうか。そのような中で、人の心理的弱点を突いたサイバー攻撃が激化しているのです」と二木氏は述べ、実際に新型コロナウイルスそのもののほか、企業のIT部門やクラウドサービスのサポート部門を装ったフィッシング攻撃が増えていると指摘した。



各種の多層防御で守られていた企業システムとは異なり、守りが手薄なテレワーク環境で頼りになるのは、個々人のセキュリティ意識だ。

「これまで会社のオフィスやファイアウォールなどの壁に守られ『このルールを守ってやりなさい』と言われてきた人たちが、いきなりルールがないところで仕事をしなければならない状況です。そんなとき、何が最良の方法なのか自分の頭で考えられないと、適切に守ることは困難です」(二木氏)

楽しく学べるコンテンツと 実戦さながらの訓練、分析によって意識変革を実現

壁に守られた内側で「このルールさえ守っていればいい」という一種の思考停止に陥っていたセキュリティの世界。それを根本的に変え、新しいICT技術や環境変化にも対応できる「セキュリティ意識改革」を実現しようとしているのが、KnowBe4だ。

KnowBe4 Japan合同会社の日本代表マネージングディレクター 根岸 正人氏は、長年サイバーセキュリティ業界に携わってきた経験も踏まえて**「情報セキュリティ教育ではなく、社員1人ひとりのセキュリティ意識改革、セキュリティアウェアネスが求められています。マインドセットに変革を起こし、日々求められるさまざまなセキュリティ上**

iSID

KnowBe4
Human error. Conquered.

の判断において、社員が的確な意思決定を下せるようにしていく。それが『Human Firewall』の形成につながります」と述べ、ひいては企業の中にセキュリティカルチャーを根付かせていくことが重要だとする。

Human Firewallという目的を実現するためにKnowBe4が提供しているのが、セキュリティ意識向上に向けたさまざまな教育と、フィッシングをはじめとする多様なサイバー攻撃のシミュレーションによる訓練と、その分析・レポートを統合し、継続的に繰り返し実施できるSaaSプラットフォーム「KnowBe4」だ。

おそらく多くの人が思い浮かべる「情報セキュリティ教育」は、無味乾燥な集合研修やeラーニングに参加し、分かりきった事柄や、逆になんだか難しすぎてよく分からない内容を受け身で学ぶというイメージだろう。

これに対しKnowBe4では「早く続きを見たい」と思わせる1100種類以上のドラマ仕立ての動画を通じて、セキュリティを自分ごととして捉え「自分たちの周囲にどんな危険性があるのか」「不用意な行動がどんな被害を招く恐れがあるのか」など、さまざまな学びが得られるようになっている。

また、本物のサイバー攻撃さながらのメールを用いた訓練・演習も大事な構成要素だ。KnowBe4では5100種類以上のテンプレートの中から、フィッシングメールや標的型攻撃メール、あるいはビジネスメール詐欺（BEC）など、さまざまな種類の訓練メールを従業員に送付し、不審なメールに気付く力を身に付ける手助けをしていく。

特徴の1つは、添付ファイルの開封率だけでなく、開かれたOfficeドキュメントでマクロが有効にされたかどうかや、URLをクリックしてランディングページに誘導され、さらにユーザーIDとパスワード情報を入力してしまったかどうかなど、細かなアクティビティまで把握できることだ。こうした情報を基に、セキュリティ担当者が「我が社はどの手口に弱いか」「どの部署にどんな傾向があるか」というリスクを把握し、どのように対処するかを考えるのに役立てる。

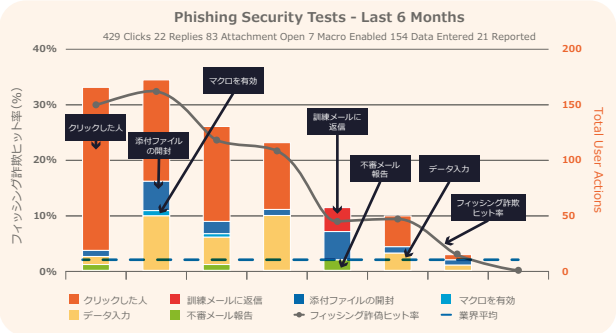
すでに少なくない企業が、サイバー攻撃の巧妙化を受け、標的型攻撃メール訓練を年に1、2回の頻度で実施しているだろう。だがその多くは監督官庁や関係会社に言われたからとりあえずやるという感じで、成果に結びついていない恐れがあると根岸氏は指摘する。

「訓練メールを用意する手間やコストも課題ですが、何より、前回の訓練と比較して会社のリスクがどのくらい変化し、どのくらい改善したかという観点がないため、訓練の効果が測定できていません」（根岸氏）

これに対しKnowBe4では、教育・トレーニングを経た後に訓練を実施し、社員が本当にその内容を理解しているかを確認し、その結果に基づいて適切なコンテンツを用いて再トレーニングをし、さらにその効果を計測していく……というサイクルを、年間サブスクリプション契約の中で繰り返していくことができる。

可視化と分析を可能にする次世代型プラットフォーム

フィッシング詐欺ヒット率を数値化



KnowBe4を活用することで、たとえば当初は30%前後だった添付ファイルの開封率が、1年後には2%にまで低下できるといった効果も現れているが、そこは本質ではない。最終的な目的は社員のセキュリティ意識を改革し、不審なメールに気付く力を身に付け、何かおかしいなと思ったら「PhishAlert」ボタンを通じて即座に報告する習慣を身に付け、セキュリティを意識した運用を実現することだ。

二木氏も**「こうした訓練を通じて、何百人、何千人という社員の中から1人でも怪しいメールを報告してくれれば、それを元にSOCが調査し、本当にまずい攻撃であれば全社員に注意喚起を出すことができます。100人のうち1人が気付いて報告すれば、残り99人が守られることになるのです」**と述べた。

こうした特徴を備えたKnowBe4プラットフォームを、同社は「第五世代」の学び方と定義している。これにより楽しく簡単に、現状を分析して弱いところを把握し、新たに動画中心のコンテンツで教育を実施することで継続的にセキュリティ意識を醸成していくというわけだ。

統合プラットフォームだからこそ実現できる効率的で計画的な学習

ただ、いくら従業員のセキュリティ意識の変革が容易にできるとしても、IT管理者、セキュリティ担当者に過度の負担をかけてしまうようでは健全とは言いがたい。その点KnowBe4は、教育と訓練、分析を1つのプラットフォームに統合し、少ない手間で運用していける。部署、あるいは訓練結果に基づく「グループ」ごとに、どういう教育プログラムを実施するかを簡単に設定して実施し、その結果を一元管理できる。

KnowBe4のパートナーとして販売を行うISIDの赤澤 卓真氏は「SCORMに準拠した自社所有の教育コンテンツや動画ファイルも取り込めるため、セキュリティだけでなく社員教育全般のプラットフォームとしても活用できる。また、従業員をグループ化し『訓練後、開封してしまった人をグループ化し、それを補う教育を受けさせる』といったジョブをWebインターフェース上で簡単に作成できることも特長だ」と説明し、バラバラの製品やサービスを組み合わせるのではない統合プラットフォームならではのメリットを強調した。

さらに二木氏は**「たとえば、あらかじめ定めた年間計画やスケジュールをKnowBe4のプラットフォームに登録すれば、後はそれを自動で実施していける。省力化した分、セキュリティ担当者は、その時々の流行の手口や注意喚起が必要な内容にフォーカスした個別のトレーニングに力を振り向けることができる」**と述べた。

ISIDでは、多言語対応、グローバルプラットフォームという点も踏まえ、同社が強みを持つ製造業や金融サービス業などを中心にKnowBe4を提供し、従業員のセキュリティ意識改革を支援していく。中には、従業員のセキュリティ意識を数値化できる点を評価して日本の本社よりも先に海外拠点側がKnowBe4を採用し、後にグローバル展開として全世界の従業員を対象に展開されるケースもあるという。

日本の製造業が世界で評価された原動力の1つは、ただマニュアル通りに作業を進めるのではなく、従業員1人ひとりが問題意識を持って自分たちの頭でよりよい方法を考え、仕事の仕方を変えながらもの作りに取り組んだからだ。

サイバーセキュリティも同じように、1人ひとりがセキュリティ意識を持つことで、想定外の事態に直面しても「こういうときにはこういう理由でこうしてきたから、この場合はこうすべきだ」とスムーズに判断を下し、リスクを回避していくことができるだろう。KnowBe4はそれを手助けする大きな力になってくれるはずだ。

KnowBe4
Human error. Conquered.

実際の攻撃を基にした4,800種類以上のテンプレートから社員向けに模擬攻撃を行い、その結果を基に個人や部署毎のセキュリティレベルをスコア化。社員のレベルに合わせた教育メニューを、約1,100種類以上の教育コンテンツから選択し、受講させることができます。社員のセキュリティ意識を向上させる事でビジネスメール詐欺等の「人」を狙うセキュリティ脅威から個人、組織、企業を防御することを支援します。

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　営業企画部

〒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://www.isid-security.com/knowbe4/

本ソリューションの詳細情報はこちら