CASE STUDY

IT 目利きが選んだ人への投資：トップディストリビューターが採用したヒューマンリスクマネジメントプラットフォーム

●脅威の高まりを背景に、より体系だったセキュリティ教育と訓練を検討

株式会社ネットワールドは、IT インフラストラクチャーのソリューション ディストリビューターとして、クラウド時代の企業 IT 基盤を変革する技術製品と関連サービスを提供している。サーバー、ストレージやネットワーク、セキュリティ、そしてアプリケーションやデスクトップの仮想化に早期から取り組み、AI 活用を前提とする新世代の IT インフラストラクチャーのあるべき姿をリードしている。

そして、サイバー脅威が顕在化してきた 2022 年ごろからは、セキュリティ領域にも力を注ぎ始めている。顧客にセキュリティソリューションを提案するのはもちろん、社内でも、エンドポイントセキュリティからUTMによるネットワークセキュリティ、そして社内教育による人のセキュリティに至るまで、包括的な取り組みを進めてきた。

ただ、組織のセキュリティレベルを上げていくためには、まだ改善の余地があると考えていた。それまでセキュリティ教育は年に一回、e ラーニング形式で個人情報の適切な扱いを主としたセキュリティ教育を実施するほか、情報システム部からの定期的なセキュリティに関する注意喚起メールの送付などが中心で、不審なメールかどうかの判断は、個人の勘や能力に依存する部分もあり、より行動変容につながるような体系立った仕組みや教育が必要ではないかと考え始めていた。

●「ヒューマン・リスクマネジメント」に感銘し、販売店と同時にユーザーとしても導入

そんな折、ディストリビューターの立場で KnowBe4 とミーティングを行う機会があった。

常に IT 業界の最新動向をウォッチする立場から、以前から KnowBe4 の名前は把握していたという。「SaaS 市場、セキュリティ市場が成長している中、日本では聞いたことのない KnowBe4 という会社が米国では急成長していることは知っており、なぜこれほど伸びているのかに興味を抱いていました」（同社管理本部 情報システム部 部長 盛永昌二郎 氏）

実際に日本法人の担当者と対話し、KnowBe4 の掲げる「ヒューマン・リスクマネジメント」の考え方、仕組みに感銘を受けたことが、自社のセキュリティ意識向上へ向けた採用の決め手になった。

「調べれば調べるほど日本は社員教育で立ち後れていることを認識し、従業員一人一人がファイアウォールになって守るべきだという考え方に感銘を受けました」（盛永氏）

ネットワールド株式会社

業界
IT・通信

本社
東京都千代田区

キーフレーズ
「危険に囲まれたインターネット社会においてさまざまなリスクから社員自身を守るため、ぜひ KnowBe4 を通して社員のセキュリティスキルを上げてもらいたいと思っています」

株式会社ネットワールド
管理本部　情報システム部
部長　盛永昌二郎 氏

ポイント
- 豊富なコンテンツを生かして個人のレベルに沿った教育と年 15 回のフィッシングメール訓練を実施
- クリック率の低下と Phish Alert Button（PAB）による報告数の増加を実現

検証のためコンテンツを確認してみて、その思いはさらに深まったという。「フィッシングメールの見分け方一つ取っても、体系立ててどこをチェックすべきかを、動画を織り交ぜながらきちんと教えてくれるなど、e ラーニングの質の高さも評価しました」（盛永氏）

国内ベンダーが提供する教育ソリューションも調査したが、セキュリティ教育コンテンツの質に加え、フィッシングメール対策訓練も一つのプラットフォームに組み込まれ、全体のリスク評価やベンチマーク比較までできることも決め手となり、採用することとした。同社 管理本部 リスク管理部の新納辰見氏は「訓練についても非常に簡単に設定でき、何度でも実施できると判断し、パートナーとして扱うだけでなく自社でも活用していくことを決めました」と振り返る。

●高頻度な訓練とわかりやすい教育によって着実に向上したリテラシー

社内の情報セキュリティ体制強化を進め、ISMS 取得を目指す中、ネットワールドでは 2024 年 1 月から本格的に KnowBe4 を用いた社内セキュリティ意識評価の分析、セキュリティ教育、攻撃メール訓練を開始した。

個人情報保護に限らず幅広いサイバーリスクに備えた教育を四半期に一回実施するほか、攻撃メール訓練は基本的に月一回実施している。さらに、毎年 4 月は「セキュリティ強化月間」と位置付けて毎週訓練を実施しており、通年で 15 回の訓練を実施している形だ。

非常に高い頻度で訓練を実施しているが、「これは KnowBe4 だから実施できたようなものです。カテゴリを選び、豊富なテンプレートの中からどれを使うかを選んで指示するだけで訓練メールが送信できるため、少ない手間で高頻度の訓練を実施できています」と新納氏は述べる。

訓練の結果は、クリック率などとともに経営層に報告するほか、ダッシュボードに表示される業界平均と比べて顕著に高い場合は、各本部ごとに対策をしている。部署ごとの傾向を踏まえ、どのように手当てし、不注意を減らしていくべきかの検討も進めているという。

教育についても同様だ。ダッシュボードを参考に、用意されたコンテンツの中から事業部毎に受講させる最適な内容を選び、いつまでに受講するかを決めて告知するだけで済むため、手間が大幅に省かれた。そのうえコンテンツは動画主体で、しかも日本語による字幕が付いているため、従業員にとってわかりやすいと評価している。

「e ラーニングというと、一般的には先生が画面上で講義をし、それを生徒が聞くという流れでしたが、KnowBe4 の教育はドラマ仕立てで見やすくする工夫が随所にあるため、社員も非常にわかりやすかったのではないかと思います」（盛永氏）。フィッシングの手口など典型的な攻撃手法に加え、生成 AI 利用時の注意点など、随時追加されていく最新の動向を踏まえたトレーニングコンテンツも活用している。

こうして一年以上にわたって KnowBe4 による教育と訓練を重ねたことで、従業員のセキュリティ意識やリテラシーは確実に向上してきた。
「現場からは、メールが届いた時に送り主が正しいかどうか、きちんと確認するようになったという声をよく聞きました」と盛永氏は述べる。また生え抜きの社員はもちろん、中途採用で新たに加わった社員に対しても教育・訓練を繰り返し実施することで、開封率が低下してきているという。

訓練だけでなく、実際に不審なメールが手元に届いた際に報告も増加した。「月に 80 件から 100 件近くの報告が届くようになっています。VirusTotal との連携機能を用い、本当に不審なものかどうかの判断が簡単に行える点でも助かっています」（新納氏）

●社員自身を守るため、KnowBe4 を生かしてさらなるスキル向上を

KnowBe4 の包括的なソリューションに対し、盛永氏は「フィッシングメール訓練はリスクを最小化するものであって、ゼロにはできません。そこを補うのが教育です。その意味でも、この二つがセットになっている KnowBe4 は素晴らしいと感じています」と評価する。
今後は、外部の脅威アクターが仕掛けてくる攻撃だけでなく、不注意や故意による情報漏洩をはじめ、内部不正対策にも KnowBe4 を活用し、社員一人一人のセキュリティ意識を強化していきたいと考えている。

「セキュリティというと会社の情報や会社を守るためのものと見られがちですが、最終的には社員自身を守るためにあると考えています。危険に囲まれたインターネット社会においてさまざまなリスクから社員自身を守るため、ぜひ KnowBe4 を通して社員のセキュリティスキルを上げてもらいたいと思っています」（盛永氏）

さらに、こうして自社で教育・訓練を継続してきたノウハウを生かし、パートナーとして KnowBe4 を提供し、顧客やその従業員を守る支援も行っていく。自らユーザーとして活用した経験や生の声を踏まえ、顧客に寄り添った提案やサポートを展開していく計画だ。

© 2025 KnowBe4, Inc. All rights reserved.Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.