2020.06.22

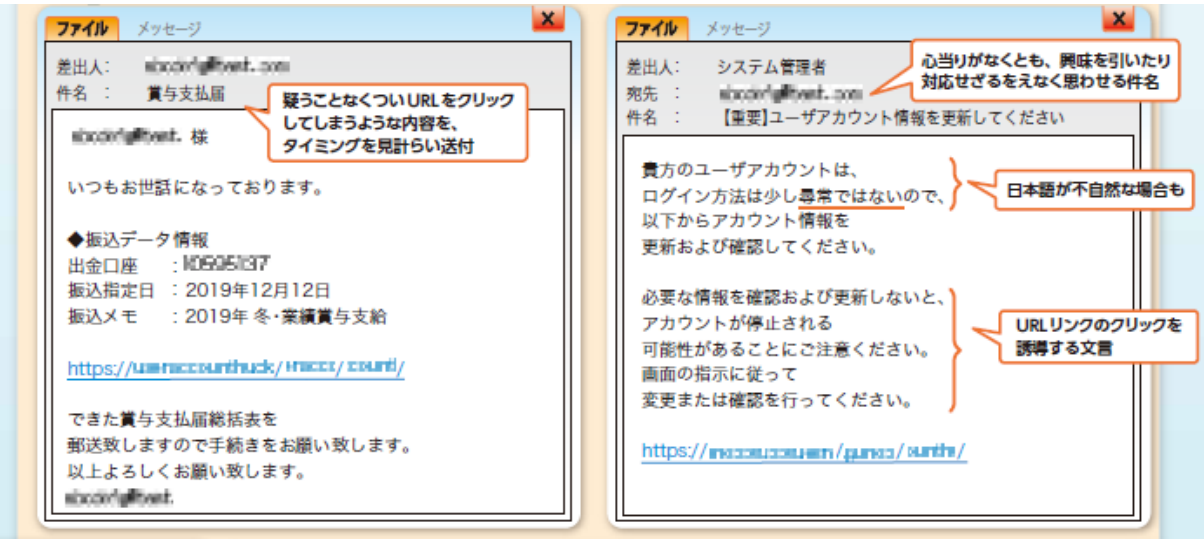
サイバーセキュリティニュース ＜2020 No.002＞

ナッジ理論でサイバーリスク対応力を養成する

【要旨】
■ 新型コロナウイルスの世界的な感染拡大の影響を受けて、多くの企業でテレワークが推進されている一方で、これに便乗したサイバー攻撃が急増しており、標的型攻撃を受けた企業では、甚大な被害が発生している。
■ 標的型攻撃への対策は、システム的な防御を強化するだけでは根本的な問題解決にはならない。従業員一人ひとりへの教育を通じたサイバーセキュリティに対する意識向上に加えて、インシデント発生時における事後行動を正しく且つ素早く実施することが最も重要な要素になる。
■ 本稿では、弊社が BEworks Inc. [1)] （以下、BEworks 社）と共同で行った、行動経済学の手法を応用した企業におけるサイバーセキュリティ向上に関する研究と、「ナッジ理論」でサイバーリスク対応力を養成するポイントを紹介する。

1．標的型攻撃の脅威と対策における課題

新型コロナウイルスの世界的な感染拡大の影響を受けて、多くの企業でテレワークが推進されている一方で、これに便乗したサイバー攻撃が急増している。とりわけ、特定の企業・組織を狙う標的型攻撃の手口はますます巧妙になっており、思わずメールの添付ファイルや URL リンクを開いてしまうように作りこまれている。標的型攻撃を受けた企業においては、機密情報の漏えいやランサムウェア感染による身代金請求、事業中断による機会損失・利益の逸失など甚大な被害が発生している。



【図１】標的型メール攻撃の文例

[1)] BEworks 社：2010 年にカナダのトロントで設立された、科学的思考と行動経済学を用いてビジネスの課題解決を支援するコンサルティング会社。同社は、行動科学、認知心理学、社会心理学、神経科学の専門家によって構成されており、科学的根拠に基づく生活者心理を明らかにし、マーケティングや新商品開発、価格設定等、幅広い経営上の課題解決を提案・実証している。

人間の心理の隙を突いてくる標的型攻撃への対策は、企業のリスクマネジメントにとって極めて重要な取組課題となっており、近年、標的型メール訓練を実施する企業が増えている。弊社でも 2016 年からサービスを開始し、のべ 700 社、訓練参加者は 20 万人を超えたが、訓練メールの開封率はサービス開始当初から大きく改善することなく、17～20%を推移している。

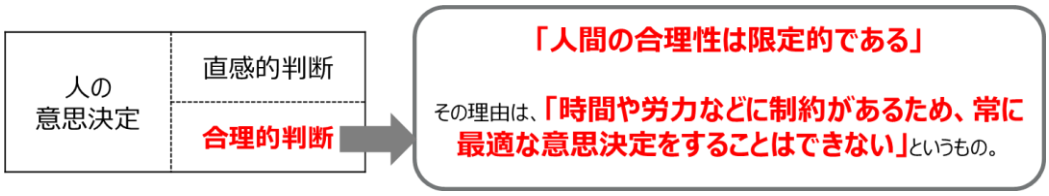
教育・訓練を通じて、従業員による不審メールの開封率を低下させるとともに、受信時の適切な対応の習得が求められるが、メールの開封率ばかりに注目し、不審メール開封の有無にかかわらず、「取るべき行動」ができなかった者に対して十分なフォローアップが行われていないケースが散見される。

標的型攻撃への対策は、システム的な防御を強化するだけでは根本的な問題解決にはならず、それを使う「ヒト」を変えなければならない。すなわち、従業員一人ひとりが危機意識を持ち、不審なメールを開かない、不審な URL はクリックしないといった、「個人への教育を通じたサイバーセキュリティに対する意識向上」と「インシデント発生時における事後行動を正しく且つ素早く実施すること」が最も重要な要素になる。

本稿では、弊社が BEworks 社と共同で行った、行動経済学の手法を応用した企業におけるサイバーセキュリティ向上に関する研究と、「ナッジ理論」でサイバーリスク対応力を養成するポイントを紹介する。

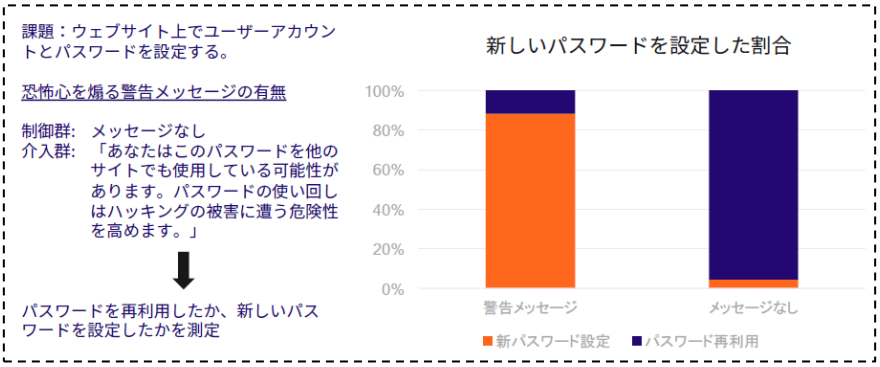
２． 行動経済学とは

行動経済学とは、人がさまざま経済活動において、どのように選択・行動し、その結果どうなるかを究明するため、実際の行動を実験を通じて観測することを重視した経済学の一分野で、「必ずしも人は合理的に判断して行動するわけではない」という前提に立って、人の行動や意思決定の在り方を研究している学問である。



【図２】行動経済学の理論

中でも、人の心理的な行動原理を利用して、強制や規制、金銭的なインセンティブのみに頼ることなく、人がより良い選択をすることを狙った「ナッジ（nudge：肘で軽くつつくという意味）」と呼ばれる手法に関心が高まっている。



【図３】「ナッジ」の事例[2)]（BEworks 社との共同研究資料より）

2) 出典：BEworks 社「Jenkins, J. L., Grimes, M., Proudfoot, J. G., & Lowry, P. B. (2014). Improving password cybersecurity through inexpensive and minimally invasive means: Detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time fear appeals. Information Technology for Development, 20(2), 196-213.」

前述のとおり、サイバー攻撃による被害を最小化するには、従業員のサイバーセキュリティに対する意識向上やエンゲージメントを高めることが重要である。

BEworks 社との共同研究では、行動経済学の知見を活用し、やる気を促す学びの機会を提供することで、従業員がサイバーセキュリティに対して、①真剣に向き合い、②向上心を持って自ら学ぶようになることを目的とした。

３．共同研究を通じて得た気づき

BEworks 社との共同研究では、標的型メール訓練において、以下の二点に注目しながら、行動経済学的アプローチを応用した実証実験を行った。

- 不審メール内にある URL リンクや添付ファイルをクリックして開いてしまうといった「不適切な行動の抑制」
- クリックしてしまった後に「実施すべき事後行動」を正しく且つ素早く実施する

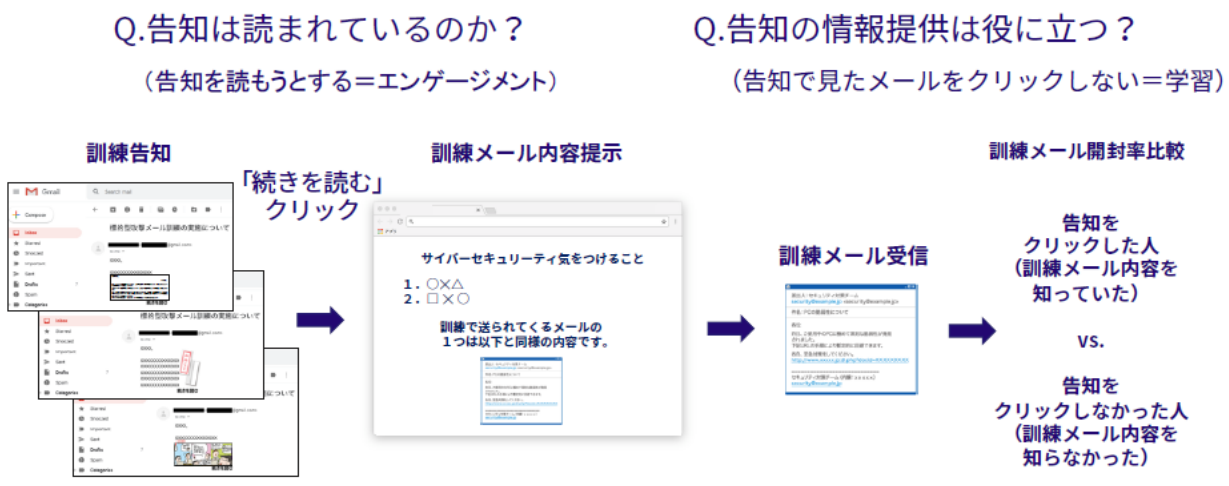
実証実験は、現状における課題である「サイバーセキュリティに対する興味・意識・学習意欲が欠如している」状態、すなわち従業員の心理的障壁を把握した上で、その心理的障壁を取り除く仮説を構築し、実験を通じて仮説の検証を行った。

以下にて、実証実験の概要とその結果、実験で得た気づきを示す。

（１）不適切な行動の抑制

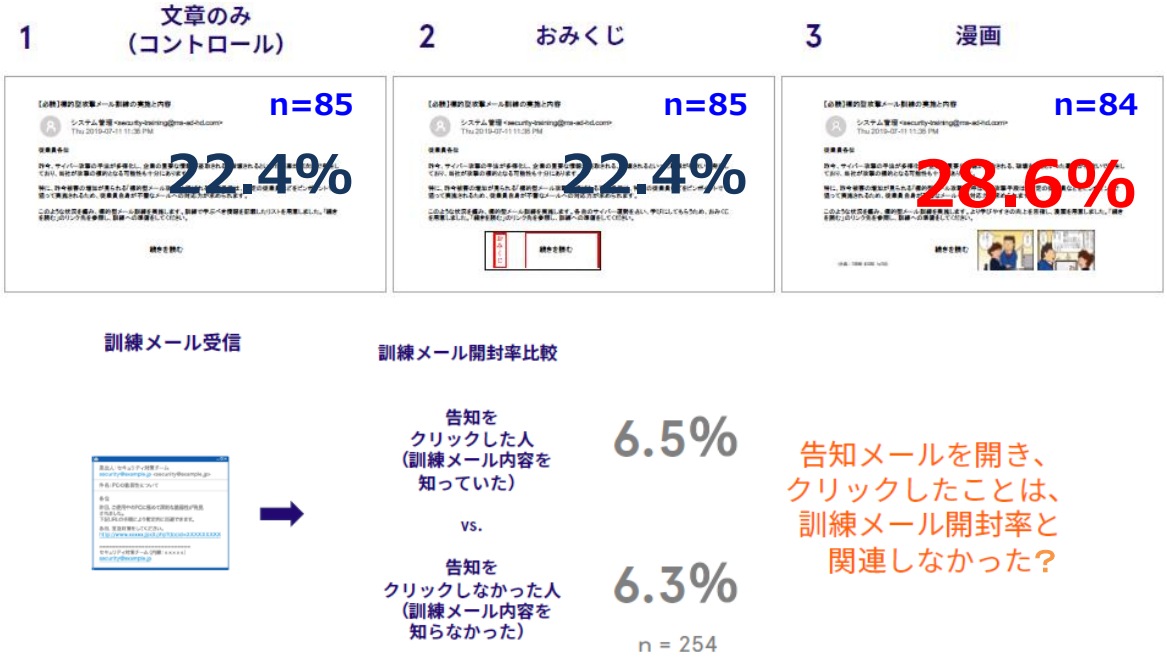
一つ目の実証実験では、従来の文字のみの告知に比べ、つい読んでしまうような媒体を用いた情報提供を伴った告知を行うと、学びに対してポジティブな行動を促すことができ、学習効果が高まると仮説を立て、検証した。

告知の媒体は、①文章のみ　②おみくじ　③マンガ　の 3 種類をランダムに従業員に送信し、告知のリンク先（この実証実験では、後に行うメール訓練の種明かし）を読んだかを計測した。また、告知のリンク先を読んだ従業員はメール訓練の種明かしを「学んだ」ので、訓練メールの URL リンクはクリックしないと仮説を立て、標的型メール訓練も実施、告知のリンク先をクリックしなかった従業員との開封率を比較した。



【図４】実証実験１「不適切な行動の抑制」の概要

実験の結果、文章のみやおみくじを使った告知と比べて、マンガを使った告知の方が多く読まれたが、告知をクリックした人としなかった人との間における訓練メール開封率に大きな差異は出なかった。



【図５】実証実験１「不適切な行動の抑制」の結果（BEworks 社との共同研究資料より）

我々は、「告知のリンクをクリックしたからといって、告知の文面を読んでいるとは限らない」と仮説を立て、告知のリンク先のアクセス時間も調査した。すると、告知のリンクをクリックしたほとんどの従業員が 1 分以下でリンク先の画面を閉じていたことが分かった。また、告知のリンク先のアクセス時間が長かった従業員の方が訓練メールに引っ掛かりにくく、マンガを使った告知を受け取った従業員はアクセス時間が長かったことがわかった。

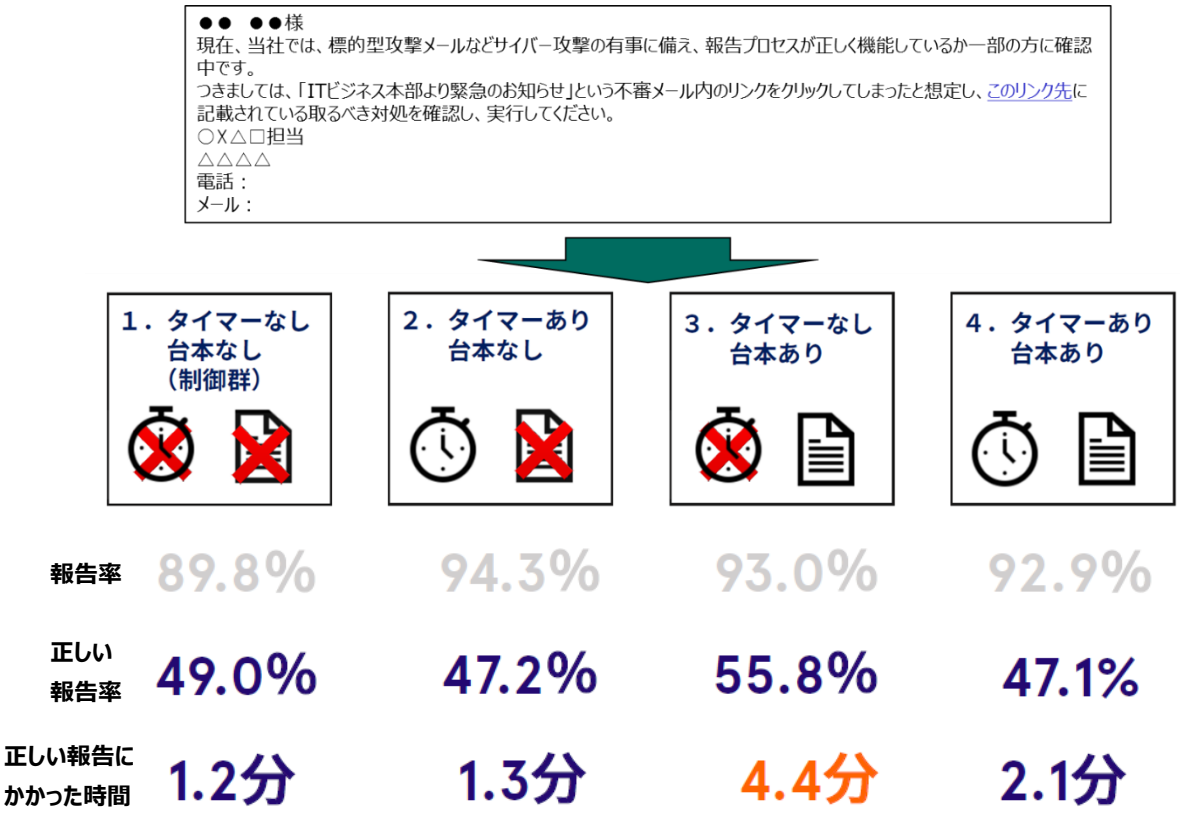
この実証実験から、文章のみやおみくじを使った場合と比べ、マンガを告知の媒体として使うとエンゲージメントが高まり、提供された情報により時間を費やし、その情報が学習につながるという傾向が伺えた。実験対象者数が比較的少ないため、統計的に再現性が高いとは言えないが、文章ベースの長い情報提供よりも、マンガによるコンパクトな情報提供のほうが正しい理解と訓練へのエンゲージメントにつながると考えられる。

（２）「実施すべき事後行動の促進」

二つ目の実証実験では、インシデントが発生したという想定で、報告を円滑にするツールを提供することによって報告率が上がるかを検証した。カウントダウンタイマーを表示し、緊迫感を与えることで迅速な報告につながり、報告時の台本を与えることで、報告に対する心理的負担を和らげ報告しやすくなるとの仮説を立てた。また、双方のツールを使うことで報告率への相乗効果が見られるか検証をした。

実験の結果、総じて高い報告率が見られたが、ツールを提供した条件においては、ツールが提供されなかった場合よりも高い報告率が見られた。ただし、タイマーありの条件で行った報告は、過半数が手順や報告先を誤った報告であった。一方で、タイマーなし・台本ありの条件は、他の条件と比較して、より長い時間を使った慎重かつ正しい報告につながるという傾向が見られた。

インシデント発生時における「取るべき行動」を台本で示すことで、従業員の心理的障壁を取り除くことができるが、過度に緊迫感を与えると焦りからエラーを起こしてしまい、適切なインシデント対応を習得する際の障害となってしまう可能性が考えられる。



【図６】実証実験２「実施すべき事後行動の促進」の概要と結果（BEworks 社との共同研究資料より）

４．「ナッジ理論」でサイバーリスク対応力を養成するポイント

繰り返し標的型メール訓練を実施している企業・組織は、特定の役職や部門で突出して高い開封率となっていないか、前回に実施した訓練の結果と比較して改善がみられるかなどを検証すると思われるが、開封状況の検証に留まらず、訓練実施により顕在化した課題の改善を着実に実行すべく、従業員へのフォローアップにも取り組んでいただきたい。

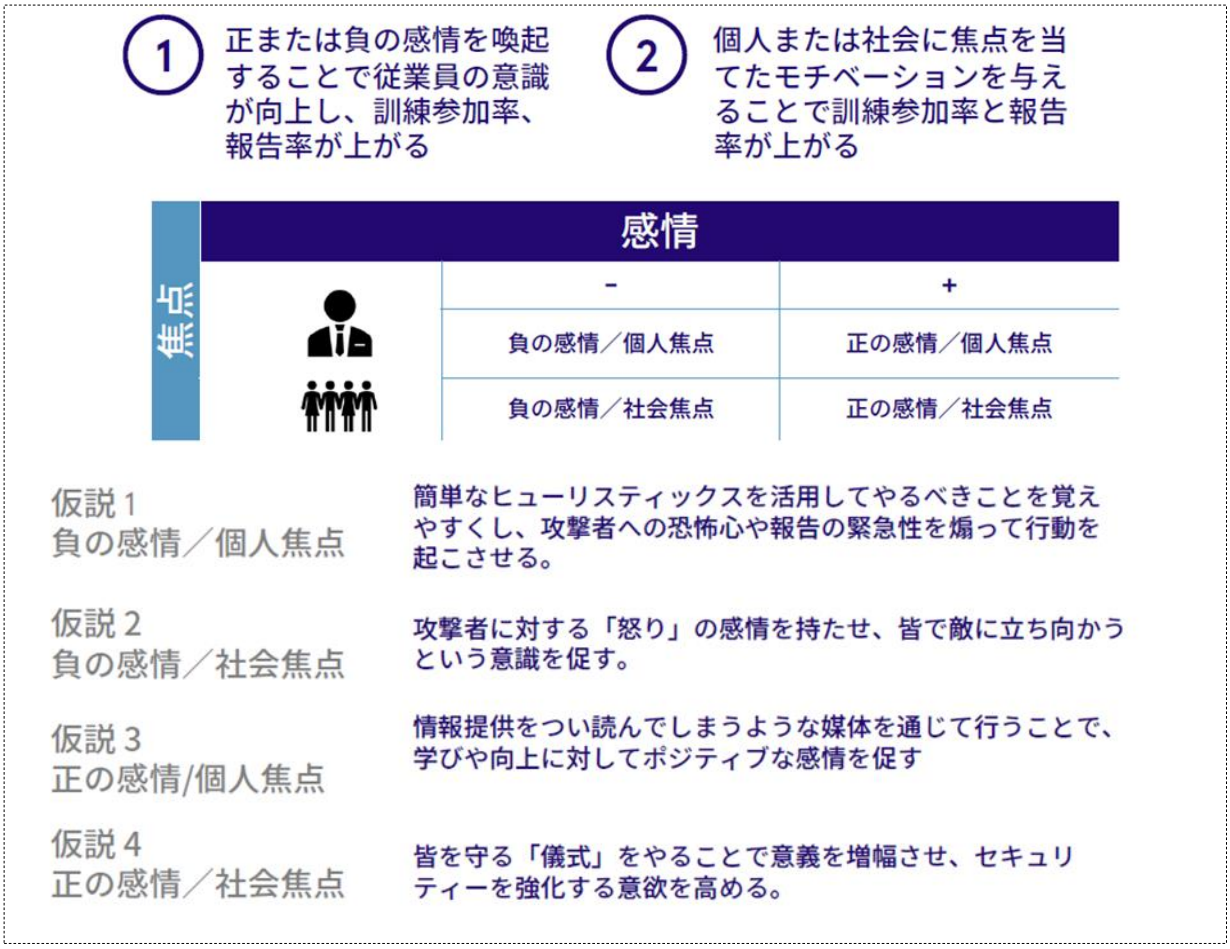
強制や規制、金銭的なインセンティブのみに頼ることなく、人がより良い選択をするように促すには、以下のポイントを押さえた教育・指導をすることが肝要である。

（１）正または負の感情を、状況に応じて使い分けて喚起する
感情は注意や行動を喚起し、意思決定や学びに影響する重要な要因であることが過去の研究より判明している。

（２）「取るべき行動」に応じて、モチベーションの焦点を変える
モチベーションの焦点をどこに当てるかにより、行動の実行や維持への影響が変わることが過去の研究より判明している。

（３）「取るべき行動」は具体的に示す
曖昧な表現や抽象的な表現を避け、誰が行動しても同じ行動・結果となるように、「自分事」にしやすい表現で示す。

（４）従業員個々人に、適切なフィードバックをする
やりっぱなしの指導はＮＧ、各人のリスク感度や理解度に応じたフォローアップを実施する。



【図７】促す感情とモチベーションの焦点の掛け合わせの例（BEworks 社との共同研究資料より）

「ナッジ理論」は、本稿で紹介したサイバーリスク対応だけでなく、他分野のリスク対策や人材教育などに幅広く活用することができる。また、すでに医療・福祉、環境分野をはじめとした公共政策においても「ナッジ理論」は広く活用・応用されている。

京都府宇治市の「イエローテープ作戦」

- 庁舎入り口に設置した消毒用アルコールに気づいてもらえるように、床に矢印のテープを貼付してわかりやすくした
- 設置前と比較して、利用者が約 10%増加
- その後、宇治市に倣って他の自治体でも同様の取組が展開された

【図８】新型コロナウイルス対策におけるナッジの活用事例（出典：環境省「新型コロナウイルス感染症対策における市民の自発的な行動変容を促す取組（ナッジ等）の募集について」2020 年 5 月 1 日）

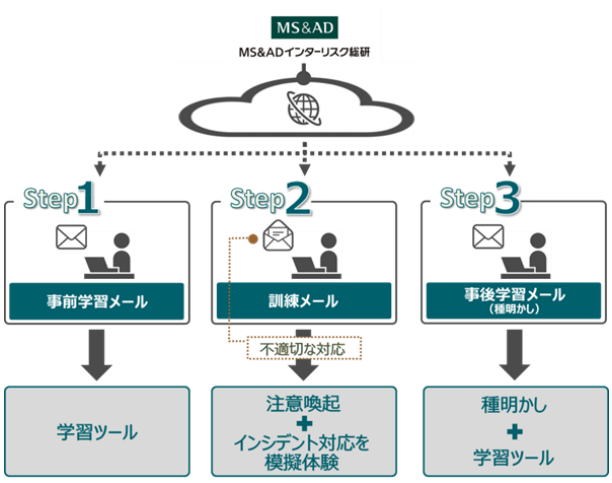
人間は、すべての意思決定において最良の判断を下すには時間とエネルギーが足りない故、判断をヒューリスティクス（心理的近道）やバイアスに委ねてしまい、不合理な行動を取ってしまう。しかし、本稿で紹介した研究からも見て取れる通り、その意思決定の環境をデザインすることで、よりよい選択を促がすことが可能である。

多くの企業が、従業員のポジティブ感情を引き出すことで、個々人に行動変容を促し、「やらされ感ばかりが目に付く訓練」をより良い学びの機会に進化させていただければ幸いである。

ＭＳ＆ＡＤインターリスク総研株式会社
新領域開発部 サイバーリスク室
マネジャー・上席コンサルタント　岡田　智之

ＭＳ＆ＡＤインターリスク総研株式会社では、標的型攻撃を巧妙に模した「訓練メール」を訓練参加者に送信し、その対応を個々人に評価する「標的型メール訓練サービス」を提供しています。

本サービスは、行動経済学の代表的な考え方である「ナッジ」を活用することで、「学び」のモチベーションを上げることを志向するとともに、訓練結果報告書に基づいて従業員個々人の不審なメールに対するリスク感度や学習の深度に応じたフォローアップを行うことができます。



【学習コンテンツのイメージ】

ＭＳ＆ＡＤインターリスク総研株式会社は、ＭＳ＆ＡＤインシュアランス グループのリスク関連サービス事業会社として、リスクマネジメントに関するコンサルティングおよび広範な分野での調査研究を行っています。
サイバーリスク・情報セキュリティに関するコンサルティング・セミナー等を実施しております。
コンサルティングに関するお問い合わせ・お申込み等は、下記の弊社お問合せ先、またはあいおいニッセイ同和損保、三井住友海上の各社営業担当までお気軽にお寄せ下さい。

お問い合せ先
ＭＳ＆ＡＤインターリスク総研株式会社
新領域開発部　サイバーリスク室
千代田区神田淡路町2-105 TEL:03-5296-8961／FAX:03-5296-8941
https://www.irric.co.jp/