4F-01

行動科学を援用したサイバーセキュリティ対応 ～セキュリティ心理学の確立を目指して ～

内田 勝也‡
情報セキュリティ大学院大学

1 はじめに

2017 年 リチャード・セイラーは，人間の行動分析の 1 つ「**ナッジ理論**」で，ノーベル経済学賞を受賞した．「ナッジ(nudge)」は，ヒジで軽く突く意味で，オランダ・スキポール国際空港の小便器にハエの絵を描き，清掃費を 8 割削減させた．ナッジをサイバーセキュリティに利用する試みは，国内外で報告されているが，まだ，十分な効果を得られていない [1][2].

本稿は「フィッシング攻撃訓練」を考えているが，国内 6%程度．米国は，毎月実施し，内容の工夫を行い 4%にクリック率を下げたが，スキポール空港の 20%削減では，サイバーセキュリティ援用は大幅な改善が必要になる[3].

2 机上訓練実験概要

本稿は，机上訓練を想定した実験で電子メールを各参加者に送れないため，いくつかの工夫をした.

2-1 前提条件及び実験環境

(1) 対象者：(公社)日本心理学会情報セキュリティ心理学研究会の月例会の参加者を対象にした実験で，コンピュータ知識やセキュリティ経験を持った被験者が多い.
回答者 24 名，女性 4 名，男性 20 名，平均年齢 48 歳，40～60 歳が 22 名．コンピュータ知識(0～5)：平均 4，セキュリティ経験： 5 年以下 7 名，フィッシング経験：情報入力者 1 名，クリックのみ 4 名，フィッシングメール：全員受信経験あり.

(2) 実験環境： セキュリティ心理学研究会を開催している場所(大学・教室)で，フィッシング画面や質問はプロジェクタ（カラー）表示し，同一内容を 2 スライド／A4 用紙で白黒印刷し，回答は別途 A4 用紙で配布.

2-2 実験内容

机上実験は以下の通り実施した.

(1) 机上実験(1)：実験前に基本的なセキュリティ心理学理解のための項目を説明．詳細及びビデオ等は省略．項目概要は以下の通り.
① ナッジの考え方とサイバーセキュリティは100%近い安全が求められる
② 過去の標的型メール攻撃訓練結果等
③ セキュリティ心理学を活用した訓練結果
④ 人間の特性：同調効果（正常化バイアス／傍観者効果）等と報告の重要性
⑤ 五感の脆弱性／ヒューマンエラー
⑥ ハインリッヒの法則

(2) 机上実験(2)：実験前メッセージの選択
① 2 つのメッセージを表示し，(a)メッセージの選択，参加の意気込みレベル等の回答

(3) 机上実験(3)：**フィッシング画面(1)**，(1-2)
① 払戻し告知画面で，クリックの有無とフィッシングメールの判断レベル回答
② ①のクリック者：画面(１-2)の操作の回答
③ 未クリック者への送付メッセージ：未クリック後に送るメッセージの選択の回答
④ クリック者への送付メッセージ：クリック後の送付メッセージの選択，相談者の有無
⑤ フィッシングの解説

(4) 机上実験(4)：**フィッシング画面(2)**の説明
① クリック有無とフィッシングの可能性
② フィッシングの説明(URL にカーソルを近づけると，異なる URL が表示)．文章が途中で切れているなど

(5) 机上実験(5)：**フィッシング画面(3)**
① Pin コード入力部分でのクリックの有無
② メール画面の解説：URL 偽装など

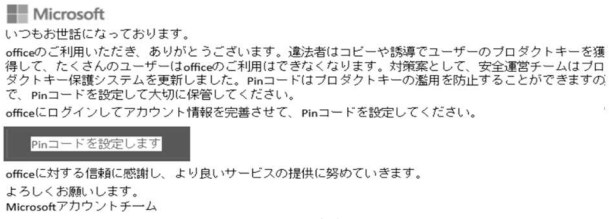
(6) 結果情報メッセージ：メッセージ内容の選択．メッセージ送付タイミング(1～4)

(7) 机上訓練の有効性
① 一定の効果がある／効果を感じない
② 机上訓練と実訓練の比較（1～3）

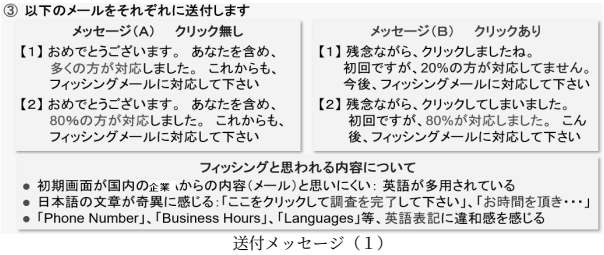
フィッシング画面(1)

Approach of endpoint security using behavioral science such as Nudge - Establishing security psychology
‡「Katsuya UCHIDA・Institute of Information Security」

フィッシング画面(2)



フィッシング画面(3)



送付メッセージ（1）

3 実験結果

(1) 実験前メッセージの選択：選択の相違は低く，内容に問題がある可能性が高い．
参加の意義：平均 3.6（0〜5）

(2) フィッシング画面(1)：3 名/24 名がクリック．入力時点で気づくが，画面はフィッシングと思っている【平均 4.2（0〜5)】
クリック後に送付するメッセージでは，「80%の方が対応」(17 名)が多い．具体的に数値で示すことが望ましいとしている
クリックした 1 名は，相談をしたと回答
フィッシング解説は，ほぼ全員（22 名）が欲しいと回答

(4) フィッシング画面(2)：3 名がクリックし，その内 1 名は(3)でもクリックした．
画面がフィッシングと思った者【平均 4.0（0〜5)】は，画面(1)より悪い

(5) フィッシング画面(3)：2 名がクリック，1 名は前 2 回もクリック
画面をフィッシングと思った者【平均 4.5】が増えている
クリック後送付メッセージは，「多くの社員」(10 名)が，「かなりの社員」(8 名)より多いが，大きな相違はない
メッセージ受信時点で，1 回目の後(9 名)，数回目の後(5 名)，80%を越える時点(3 名)，具体的な割合を達成した時点(6 名)となった

(6) 机上訓練：効果あり(22 名)，効果なし(1 名)で，机上訓練も効果あり
机上訓練の効果：クリック率 10%を越える効果あり(10 名)，従来程度(10 名)，あまり効果ない(2 名)

4 今後の課題

① フィッシング攻撃訓練では，机上訓練でも一定の効果があることがわかった
② 今回の被験者はコンピュータ知識やセキュリティ経験が通常より高く，実際の組織での検証は必要
③ 机上訓練を，自治体や企業等だけでなく，学校等や個人を対象に実施できる
④ グループを複数作り，受信メールがフィッシングか否かやその理由の回答等で，シミュレーションゲームを行い，効果を高める
⑤ フィッシング画面を多数集め，組織や個人を対象とした訓練に対応できるようにしたい
⑥ 画面をみて，「フィッシング画面」だとの判断ができる仕組みを考える事が大切との指摘があったが，今後の検討課題に
⑦ 今回の実験は，事前調査・準備も少なく，時間的な制約（Q&A を含め，2 時間弱）もあり，多くの批判はある．本格的訓練では標的型攻撃訓練ツールを使い，個々の操作ログ検証を行いながら，適切なメッセージやより発見が困難なフィッシング画面を提供し，効果的な実験も可能

5 謝辞

(公社)日本心理学会情報セキュリティ心理学研究会[4]の月例会の参加者の協力で机上実験ができた．
また，フィッシング画面については，フィッシング対策協議会[5]で公開されているものを利用した．
ありがとうございました．

参考資料

[1] 寺田剛陽,他(2019)，ユーザのセキュリティパッチ適用行動を促す心理アプローチの検討，情報処理学会 CSEC
[2] A. Sebgurbateva, M. Sedova, Why Data-driven Personalized Journeys Are The Future Of Security Training, RSA Conference 2019
[3] 内田勝也，標的型メール攻撃に対するセキュリティ心理学・セキュリティマネジメントからの考察，経営情報学会 全国研究発表大会要旨集 2015 年秋季全国研究発表大会
[4] 日本心理学会情報セキュリティ心理学研究会，http://www.uchidak.com/InfoSecPsycho/
[5] フィッシング対策協議会，https://www.antiphishing.jp/