ISSN 2186-5647

7-4

標的型攻撃メールの対処能力向上を目的としたシリアスゲーム“成り上がれ2”の開発

日大生産工（院）　○小林 優太　　日大生産工　古市 昌一

1 はじめに

近年，JTBにおける情報漏えい事件に代表される，特定の企業や政府機関の機密情報を狙った標的型サイバー攻撃が急増している．中でも電子メールによって個人のPCやシステムをウイルスに感染させ，それにより組織内に侵入を行う標的型攻撃メールは近年猛威を振るっている[1]．標的型攻撃メールは，不特定多数を狙った攻撃とは違い，攻撃者は予めターゲットの情報収集を行う．それにより普段メールでやり取りしている人に件名や本文で巧妙になりすまし，添付ファイルやリンクを偽造することによってメールの受信者が不信感を抱かずに，安全なものだと思わせる事が容易であり，その結果受信者はウイルスに感染してしまう．

標的型攻撃メールの対策としては，メールフィルターやアンチウイルスソフトの導入をすることで一部を防ぐ事は可能とされている．しかしメールは受信者ごとに1つ1つ用意され，そのメールに仕込まれるウイルスは公表されていない新種のウイルスもあるため防ぐことが困難である．そのためシステム面だけでなく一人一人が標的型攻撃メールに対応する力を養う必要がある．

2 既存対策と関連研究

2-1 標的型攻撃メール対策

従業員に対する標的型攻撃メール対策としては講義やe-learning，業務中に告知なしで標的型攻撃メールを実際に送るといった方法[2]がある．しかし，講義は講師や受講者が同じ時間に同じ場所にいる必要があるため，自らのペースに合わせて学習を行う事ができず，e-learnigはいつでも自分のペースで学習できる反面，座学のため後述する実際のメールによる実技的な学習よりも学習効果が低くなってしまう．

業務中に告知なしで標的型攻撃メールを実際に送る方法は，実際に体験（受信）することで自らのレベルを測る事ができ，もしその場で対処できなかった場合でも，失敗したことが学習に繋がる．そのため，1通目を対処できなかった人の内，半数は2通目の標的型攻撃メールを対処することができているため，高い効果が得られることが知られている．しかし，実際に標的型攻撃メールを作成する必要があり，様々なシチュエーションにおける学習がしにくい．例えば，就職活動中に成りすました標的型攻撃メールを作成しても，受信者の状況によって学習効果が変化してしまう恐れがある．また人によっては作業中断を促してしまう場合もあり，業務に影響を与える問題がある．

2-2 学習に関する既存研究

教材設計者が教材の設計過程において，学習者の動機づけの問題に取り組むためのモデルとしてKellerのARCS動機づけモデルがある[3]．ARCS動機づけモデルは学習意欲を注意(A)，関連性(R)，自信(C)，満足感(S)の４つの要因に分類している．また，それぞれの要因を高めることによって教材に対する学習者のモチベーションを高められる事が知られている．近年このモデルを使用することでゲームを用いて学習を行うシリアスゲームを効果的に構築する研究が行われている[3]．

3 提案手法

前章で述べた問題点を解決するためにシリアスゲーム“成り上がれ２”を開発した．本ゲームは実際に会社に入って業務を行っていく新人をプレイヤーとしたシュミレーションゲームである．ゲームのためe-learningと同じように自分のタイミングで取り組むことができる．また現実と近い環境で学習するため高い学習効果を期待でき，実際に業務を行う際にも違和感なく学習した経験を元に対処できると考える．図1にゲーム中のメール画面を示す．

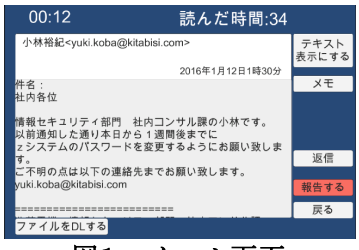

図1　メール画面

A Development of Serious Game to Improve the Skills to Prevent Targeted E-Mail Attack

Yuta KOBAYASHI, Masakazu FURUICHI

本提案手法は実際に機能する標的型攻撃メールやウイルスを作成する必要はない．そのため，出題者も学習者も安全であり新種のウイルスを学習したい場合は見た目や挙動などを登録すれば，そのウイルスがあった場合をゲームで体験し練習することができる．更にゲームの場合，様々な時期を模したメール訓練をゲームデザインにより短時間で経験でき，現実では起こりうるアクシデントなど考慮せず，焦点を当てたい要素だけピックアップして効率的に学習することができる．

学習内容はIPAが提示している標的型攻撃メールの見分け方[1]を参考にし，見分けるポイントとして“件名や本文の文章”，“使用されているURL”，“添付ファイル”から判断する方法の3パターンを学習することとする．ゲーム中にメールを行う相手も社外・社内とそれぞれ様々なシチュエーションが想定されている．

また普段社会人がメールをやり取りする際には，まず自分が処理すべきメールなのかという基準も必要になってくる．そのためゲームという仮想世界ではあるが，現実と同じように主人公にはゲーム開始時に詳細な会社の設定が説明され，ゲーム進行と同時にそれらも変化していく．

シリアスゲーム“成り上がれ”[4]を評価した際は，期間を1週間とし1日平均20分以上のプレイを被験者にお願いしていたが，指定された時間をプレイした被験者が半数以下だった．そのため，“成り上がれ２”では2章で紹介したARCS動機づけモデルを適用することで，学習者のモチベーションを向上させ一定以上の学習を促す事で，学習効果向上を生むと考えた．ARCS動機づけモデルに適応するためのそれぞれ要素を表１に示す．

表１. ARCS動機づけモデル適応表

Attention (注意)	ゲームシナリオの追加やメールの学習内容（難易度）を徐々に変化させる
Relevance (関連性)	名前を設定，実際に起きている事例を紹介，クリアに必須ではない項目の追加（クリアタイムや正答率の表示）
Confidence (自信)	学習内容を分割，一時停止機能
Satisfaction (満足感)	フィードバックの充実，クリア条件を明確に提示

4 ゲーム構成

本章では開発した“成り上がれ２”の構成を説明する．本ゲームはキャラクターとの会話で行う勉強パートとメールを処理する実践パートの２つに分かれており，2つで1セットとなっている．学習内容は3つのフェーズに分けられているため，1セットを3回行う事でクリアとなる．各フェーズの実戦パートでメールを適切に処理し正しい対応が出来るようになった場合，次のフェーズに進むための確認テストを行う．確認テストはそれぞれのフェーズで学んだ内容を包括的に実戦形式で出題され，一定数正解するとそのフェーズがクリアとなる．クリアまでの目安は約1時間となっており，クリア後も繰り返し最初からプレイすることが可能となっている．

5 評価方法

本提案方式の評価はペーパーテストで行う．ペーパーテストの内容はIPAから提供されている資料[1]の「見分けるポイント」を総合的に出題する問題をベースに，セキュリティの専門家の意見を取り入れ作成した．問題はゲームと同様に数通のメールや添付ファイルを見て，怪しい箇所やその理由を問う問題である．

実験手順を以下に示す．

1. 事前テスト
2. シリアスゲームをプレイ
3. 事後テスト，アンケート

また，手順2はシリアスゲームを利用する群と利用しない群で分け，事前事後テストの結果の他にシリアスゲームのプレイ後に双方に変化があったか確かめることで評価を行う．

6 おわりに

本稿では，効率よく安全に標的型攻撃メールの対処能力向上を目的にとしたシリアスゲームの構築について示し，評価方法を述べた．

今後，上記の評価方法に基づき実験を実施することで，本提案の有効性を示すことが課題である．また本稿では継続性のためARCS動機づけモデルを用いたが，どのような要素を入れることで継続性に寄与しているかを評価することによって，今後シリアスゲームを構築する際に有効となるデータを残すことが出来ると考える．

「参考文献」

1) 独立行政法人情報処理推進機構，IPAテクニカルウォッチ「標的型攻撃メールの例と見分け方」，(2015)
2) 山口健太郎，小宮山功一郎，内田勝也，ユーザへの予防接種というアプローチによる標的型攻撃対策-2，情報処理学会第71回全国大会，(2009)
3) 粟飯原萌，古市昌一，ARCS改良モデルのシリアスゲームジャム実地方法への応用，日本デジタルゲーム学会，(2016)
4) 前川歩　他，標的型攻撃メール対処能力向上を目的とした現場でのカスタマイズ可能なシリアスゲーム構築法　～概要～，日本デジタルゲーム学会，(2014)