5ZC-03

サイバーセキュリティ対処能力向上を目的とした シリアスゲームへの攻撃者視点の導入

菅原 大暉† 小島 健資† 小林 優太‡ 古市 昌一‡

日本大学 生産工学部 数理情報工学科† 日本大学大学院 生産工学研究科 数理情報工学専攻‡

1. はじめに

我が国における標的型攻撃メールの被害件数は年々増加し，攻撃者の手口は多様化・巧妙化しているため，標的型攻撃メール対策は継続的かつ適時に実施する必要がある．現代社会においてメールは重要な連絡手段であり，企業や組織はメールを介したサイバー攻撃に対して対策することが重要である．対策にはシステム側で対処する方法と，人的な対処能力を高める方法とがある．我々は後者に着目し，この解決手段として我々はシリアスゲームの利用が有効であると考え，“成り上がれ”を開発したが[1]，更なるゲーム性の向上が求められていた．そこでこの問題を解決するため，“成り上がれ”では防御の視点だけを考慮していたものに，新しく攻撃者の視点を導入することによって臨場感を高めゲーム性を向上させた．本稿では，試作したシステム“成り上がれ 3”の概要を示す．

2. 既存研究

学習を促進させる手段のひとつとして，e-learning がある．場所や時間を問わずに受講できるのが長所である一方，学習意欲を自己コントロールにより持続するのは容易ではないという，学習における根本的な問題点がある．これは作業の単調性に飽きる場合や，時間をかけても覚えられない等，学習が上手くいかなくなると学習意欲が減衰してしまうのが主な原因であると考えられる．また，e-learning は知識伝達型教育であるため，サイバー攻撃の全体像をイメージするのが容易ではないという問題点がある．

これらを解決するため，我々は先にシリアスゲーム“成り上がれ”を開発した．本ゲームは送られてきた標的型攻撃メールに潜んでいる脅威を発見し報告することで対処方法を学ぶことを目的としたシリアスゲームであり，実技的な項目を学習できる．また，メール処理をどれだけ正確に行えるかによって，より多くの経験値を獲得し，ランクアップを目指すことができ，対処手法の学習に対する意欲が高まる．

一方，既存の“成り上がれ”は対処者の視点を中心としたもので，攻撃者の視点がないことから，防御者と攻撃者を含めたサイバー攻撃全体のイメージを体験することが不十分であった．また，さらなるゲーム性の向上が求められていた．

3. 提案方式

前述した問題点を解決するため，本研究では既存研究の“成り上がれ”に，新たに攻撃者側視点の体験を導入することにした．ゲームのシナリオは，我が国の企業を対象として最新の技術情報等を盗むべく海外の企業がサイバー攻撃を仕掛けるというものである．

対象ユーザは主にセキュリティ対処能力向上が求められる社会人であるため，会社内で行うことを想定し PC での利用を想定した．

従来方式では，防御者が予め用意しておいたメールを処理するのみであり，攻撃者の視点がないことによりサイバー攻撃の全体像をイメージすることが容易ではないという問題点があった．この問題点に対しては，新たに攻撃者がメールを防御者に送信する仕組みを導入することで解決した．

さらに，本システムではユーザが防御者と攻撃者に分かれ対戦を行い，各ユーザのランキングを設けることでユーザ同士の対抗意識が高める機能を導入した．また，防御者は標的型攻撃メールの脅威を正確に報告できる程多くの経験値を獲得でき，攻撃者は作成したメールを防御者が脅威を正確に報告できない程多くの経験値を獲得できる．

以上のことから，対処能力を高めたいという向上心が生まれることで意欲を持ってセキュリティの知識と対処能力を身に付けることが期待される．

４．試作システム概要

前章で示した提案方式の有効性を確認するため，シリアスゲーム“成り上がれ”の拡張版“成り上がれ 3”を試作した．図 1 に“成り上がれ 3”

Introduction of Attacker's Scenario to a Serious Game to Improve Capability of Cyber Security, Masaki Sugawara,Takeshi Kojima,Yuta Kobayashi,Masakazu Furuichi. Nihon University College of Industrial Technology,Graduate School of Industrial Technology

のシステム構成図を示す．

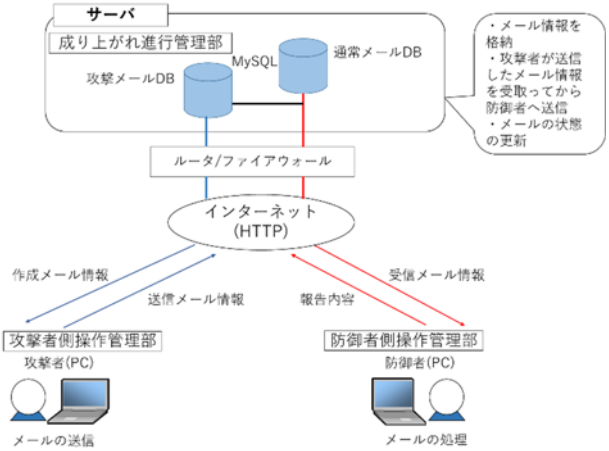

図 1　システム構成図

攻撃者が作成したメール情報は攻撃メール DB に保存される．また，攻撃者は攻撃メール DB から，作成されたメール情報を取得することができる．予め用意しておいたメール情報は通常メール DB に保存されており，防御者はこの攻撃メール DB と通常メール DB からメールを受け取れるようにする．防御者はこの送られてきたメール情報に潜んでいる脅威を報告した報告内容を送信する．

図 2 に「防御者側のメール本文画面」例を示す．

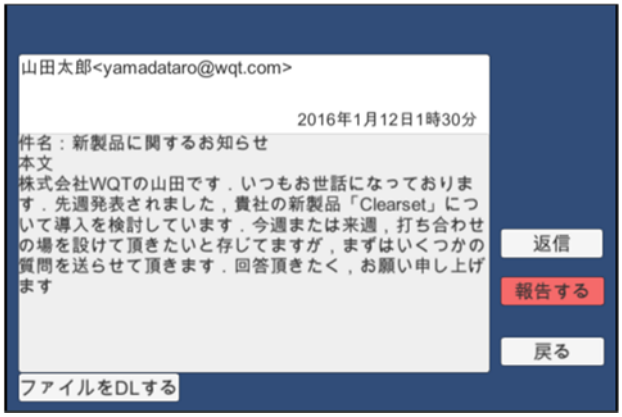

図 2　防御者側のメール本文画面

本画面では差出人名，受信した時間，件名，本文を表示する．図中の「報告する」をクリックすると，メール本文にある脅威を報告する報告画面へと遷移する．「返信」をクリックすると脅威がないものとして報告する．「ファイルをDLする」をクリックするとこのメールに添付されている添付ファイルの脅威をチェックすることができる．図 3 に「攻撃者側のメール本文画面」例を示す．

図 3　攻撃者側のメール本文画面

ここでは攻撃者のメールの作成画面として，差出人名，宛先，送信した時間，件名，本文を表示する．図中の「送信」ボタンをクリックすると，この画面で作成したメールを防御者が対処を行えるようになる．「保存」をクリックすると送信はせず下書きとして保存する．「ファイルを添付する」をクリックするとファイルを添付することができる．

5.　評価方法

本システムの有効性確認にあたり実施する評価実験の概要を示す．実験に際し，プレイ前後でテストを行い，点数の変化を確認する．テストでは，実験対象者が名前，所属等の業務内容を踏まえた上で，メールに潜んでいる脅威を解答する．想定人数は学内で 20 人，一般で 100 人を予定し，実験環境を準備中である．

6.　おわりに

本稿では，攻撃者視点を導入した“成り上がれ 3”の概要と，効果を確認するための試作システムの評価方法を述べた．

今後，評価結果を基にさらに意欲的にセキュリティ知識と対処能力を身に着けられるようにすることが課題である．

謝辞

本研究において攻撃者側視点を導入するにあたっては，“成り上がれ”の開発，評価及び改良に協力していただいた多数の皆様との情報交換を参考に致しました．この場を借りて感謝の意を表します．

参考文献

[1]　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”，日本デジタルゲーム学会年次大会　予稿集(2015年3月8日)

[2]　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施方法への応用”，　日本デジタルゲーム学会(2016)

[3]　IPA テクニカルウォッチ　フリーメールからの送信が増加傾向に：最近の標的型攻撃メールの傾向と事例分析：IPA 独立行政法人 情報処理推進機構, http://www.ipa.go.jp/about/technicalwatch/20121030.html(アクセス日：2016 年 12 月 26 日)