ISSN 2186-5647

P-73

SNS利用の危険性体験を目的としたシリアスゲームの試作

日大生産工　○小林 優太　　日大生産工　古市 昌一

１ はじめに

Twitterなどは匿名で利用できるSNSとして広く受け入れられている. しかし利用者の中には他人に見られているという意識が低いためか, 個人情報に注意する事無く利用している場合がある. たとえ注意して利用していたとしも, 利用者が複数の内容を同じSNSに投稿していた場合, その情報を組み合わせる事により個人情報が特定される事もあるため, その事実に気がつきにくい. その結果匿名でSNSを利用していたとしても多くの情報が流失している場合がある. 実際に匿名でSNSを利用していたアカウントが炎上してしまい, ユーザーの個人情報が特定や公開された事により, 甚大な被害が出るケースが多々発生しているという問題があった. 他にもSNSを利用しない理由をアンケートで調べた結果, 理由の多くは個人情報の懸念に関する項目が挙げられており[1]，現在SNSにおける個人情報に対する教材の必要性は高いと考える.

そこで本研究では擬似的なSNS環境下で失敗をして繰り返す事でSNSの利用方法を学ぶシリアスゲームの試作を行った.

２ 既存の対策

個人情報流失防止の方法として自分がどのような個人情報を流失しているか把握するために個人情報漏えい検出システムを作成した研究がある[2]．システムの精度としては名前や性別に対して約60%は完全に一致する事には成功した. しかし他の項目については５%未満という結果に終わってしまい現実的に使用するには厳しい, また精度が良くてもシステムが情報流失を見つけられなかった場合, このシステムに依存しているユーザーは流失を食い止められないと考えられるため, ユーザー自身が個人情報流失に対して学ぶ必要がある.

またSNSにおける個人情報取り扱いに対する一般的な対策としては, 総務省が提示しているようなガイドライン[3]や市の講習会が挙げられる. しかしこれらだと, SNSに無闇に情報を出すのは危険だと認識できるが具体的にどんな情報の組み合わせで個人情報を特定されてしまうのか分かりにくく学ぶ事は難しい.

他の対策としては「スマホに潜む 疑似体験アプリ」がある[4]．このアプリではネットを利用する上で想定される被害を被害者視点においてストーリー形式で見る事ができ, その中で一例としてSNSを取り扱ったものがある. しかし詳しく一例を知れたとしても少ない事例で対策するのは困難かつ, 復習する場が無いため身に付きにくい. また全ての対策に対して言える事だが, これらは興味が無いと講座やアプリなどの対策知識について知るきっかけが少ないため対策を講じる必要があると考えられる.

３　提案方式

３.１　設計コンセプト

既存対策の共通の問題点を解決するために教材はシリアスゲームにする事により個人情報に対して興味が無い人でもゲームに興味を持たせる事で学習する機会を与える事ができると考えた．本提案では既存の対策のように，教わってそのまま終わるのではなく，自らが擬似的なSNS上のゲームで勝つために個人情報について試行錯誤しながら考え失敗する（個人情報を特定される）事で個人情報流失対策について学び，それを活かし再度繰り返しプレイする事によって繰り返し学習をしていく．また疑似的な環境でゲームを行う事でSNSを使用した事がなく不安な人にも実害無く取り組み学習する事ができる.

プレイ環境については場所を問わず使用できる様にスマートフォンで利用出来る形式とした.

A prototype of a serious game to experience the risk of SNS

Yuta KOBAYASHI, Masakazu FURUICHI

３.２　ゲームの進行

３.２.１　基本ルール

このゲームのルールは各プレイヤーがSNSを使用する事によってポイントを稼ぎ，ランキング上位を目指す事である．プレイヤーはゲームを始めるとシステムが生成した架空のキャラクターと特定カードというものが与えられ，キャラクターにはそれぞれ名前，住所，職業，学生だった場合は学校の場所と学校名といったようにプロフィールが設定されている．プレイヤーにそれぞれ与えられたキャラクターはプロフィールを元にその日，どういう行動をするかシステムが生成されプレイヤーに通知される．プレイヤーは通知された行動に対してそれぞれそれを投稿するか選択する事ができ，投稿するとポイントを得る事ができる．また投稿をする際は行動に関する情報（例えば誰と行動したか，どこで行動したかなど）を隠して投稿する事ができる．実際のSNSでは，一度公開した情報を完全に消す事は困難という点を踏まえ，一度投稿したものに関しては消す事が出来ない仕様にした．

ゲーム内にはノーマルとクラッカーの２つに分かれており，それぞれポイントの獲得方法が異なる．各プレイヤーは自分のポイントを獲得するために疑似SNSを使用して一定期間が過ぎると最終的にスコアが確定し，そこでゲーム終了となる．

３.２.２　ノーマル

このゲームの大半のプレイヤーはこのノーマルに属する．投稿をすることにポイントを稼ぐことができるが，投稿する時に情報を隠せば隠すほど投稿した時のポイントは少なくなる．また後述するクラッカーによって最初に配られた特定カードに記載されている個人情報が一定数特定されるとゲームオーバーになってしまうので，ノーマルは個人情報を特定されない様に出来るだけ情報を出しながら投稿していきポイントを得る必要がある．

３.２.３　クラッカー

クラッカーはノーマルから明確に判別はできないようになっており，ノーマルと違い投稿ではポイントを得る事ができないが，ノーマルの投稿されたものから様々な個人情報を特定する事によってポイントを獲得できる．

５ 評価方法

本研究の評価には，主観評価とゲームのデータログでの相対関係とペーパーテストを使用する事で行う．

主観評価では，ゲームを行う前と行った後ではSNSの個人情報に対して意識の変化があったかについてアンケートを実施する．

ゲームのデータログではノーマルの場合特定カードに書いてある個人情報は特定されないようになってきているか，ランキングのスコアはどうなっているかなどを測る．

ペーパーテストでは個人情報に関しての問題を事前と事後に実施する事で学習効果の相関を評価する．

５ まとめ

今回はSNSにおける個人情報流失に対する教育としてシリアスゲームを試作したが，どのような情報の組み合わせに対して情報が特定されると気がつく事は難しい等の統計を採るのにも使用できると考える．

また今後評価を行い良い結果が得られる事が出来れば，本提案のシリアスゲームの拡張として身近な浮気や約束破りなど身近で個人的な問題も取り入れる事により更に学習範囲の拡大と共に，ゲームとしての面白さに繋げる事ができ，より良いシリアスゲームへの発展が出来ると考えられる．

「参考文献」

1) 平成23年版 情報通信白書，
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h23/html/nc232340.html
（アクセス日：2014年10月27日）

2) 孫 尚君，SNSからの意図しない個人情報漏えい検出システムの開発，
筑波大学大学院博士課程　システム情報工学研究科特定課題研究報告書，
2012年3月

3) 国民のための情報セキュリティサイト・ 総務省，
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/attention/02.html
（アクセス日：2014年10月27日）

4) スマホにひそむ危険 疑似体験アプリ，デジタルアーツ株式会社
http://www.daj.jp/cs/sp/app/
（アクセス日：平成26年10月27日）