R-2

ネット犯罪の加害者視点を用いた体験型学習教材の開発

橋浦研究室　1145128　内野雅敏　1145406　福田侑生

1. はじめに

近年ネット犯罪は増加の一途をたどっており，ネット犯罪に関する適切な知識の習得が求められている.警察庁[1]や IPA[2]が動画教材を公開しているが，視聴覚教育では，受動的態度となり，表面的理解に留まる危険性がある．また，手口を知っているにもかかわらず被害にあうこともあり，知識の定着率を高められるだけでなく，自己の脆弱性を適切に認知する必要がある.

2. 研究目的

本研究は，自己の脆弱性を認知させることによりネット犯罪を防げるようになる学習教材の開発を目的とする.

これは，被害者視点ではなく，加害者視点からネット犯罪を体験的に学習することにより，自己の脆弱性認知が向上すると考えたためである.

3. 加害者視点による学習

自己の脆弱性を認知するためには，根本的な帰属の誤りを減少させる必要があり，事前に原因を考えさせる方法[3]が提案されている．この他にも，サイバー犯罪の演習として攻守に分かれて行う演習[4]がある.これらのことから，別の視点での学習，つまり加害者視点での学習が有効であると考えられる.

4. 扱うネット犯罪

本研究では，増加傾向のネット犯罪としてアカウント乗っ取りと，不正アプリを扱う.

5. 学習教材

環境は Web 上に HTML で実装する.以下に手順を示す.

① 選択したネット犯罪の手口や対策方法,被害にあったときの対処方法などの説明を行う

② ネット犯罪を加害者の視点から体験的に学習させる

③ もう一度対処方法を説明する

アカウント乗っ取りの体験内容は，被験者に架空のプロフィール(図１)を見てもらい，パスワードを予想させる．不正アプリについては、非正規マーケットへ誘導するためのメール、非正規マーケットのデザイン、情報を取るためのパーミッションについて選択肢を示し，その中から騙されやすいものを予想させる.

図 1. 架空のプロフィール

6. 実験

開発した教材の有効性を確認するために，被験者を用いた実験を行った．日本工業大学学生 6 名に事前テスト，教材，事後テスト，アンケートの順に回答させる．アカウント乗っ取りの事前・事後テストは，SplashData が公開している WORST PASSWORDS of 2016[5]から 25 問，FUJITSU が公開している危険なパスワード[6]から 7 問を用いて，安全だと思うパスワードに○をつけさせた．表 1 に事前・事後テストの結果を示す.

表 1. アカウント乗っ取りについての得点

被験者	A	B	C	D	E	F
事前テスト	27	30	28	31	31	29
事後テスト	30	31	28	31	32	29

表 1 より，事前テストの得点が高くて，事後テストの得点が上がらなかった.

不正アプリのテストは，①アプリのインストールを促すメッセージ，②アプリマーケット，③パーミッションの中から危険もしくは安全なものを選択し，その理由を記述させた.テスト問題は全部で 13 問あり，16 点満点とする．対象者の得点を表 3 に示す.

表 3．不正アプリについての得点

被験者	A	B	C	D	E	F
事前テスト	4	6	11	12	12	10
事後テスト	7	9	12	12	11	14

表 3 より，事前テストの得点と事後テストの得点に，あまり変化がなかった．

7．考察

アカウント乗っ取りの有意性を示せなかった原因として 2 つのことが考えられる．

1 つ目の有意性を示せなかった原因として，事前テストの点数が高いことが考えられる．32 満点のテストで平均点が約 29.3 点と高得点を取っている．このことから日本工業大学の情報工学科以外の学生のパスワードに対する認識が高いことが窺える．

2 つ目の優位性を示せなかった原因として，安全と危険の両方の条件を満たしているパスワードを出していたことに原因があると考えられる．安全なパスワードとして英字・数字・記号を組み合わせることを挙げているが，危険なパスワードとして英字の O や L を数字の 0 や 1 に変えただけのものや，キーボード上の羅列を挙げているもの．安全なパスワードとして八文字以上のものを挙げているが,8 文字以上だが単純な羅列のため危険なパスワードのものがある．こうした問題の間違いは事後テストで 6 か所あり，その内の 4 か所は事前テストで正解している場所であった．6 か所のうち，5 か所は，数字と記号で構成されているパスワードであった．このことから，危険なパスワードでも，数字と記号で構成されているパスワードは，安全だと認識されやすいと考えられる．

不正アプリのテストで有意性を示すことができなかった要因は，まず①の問題で，対象者が問題内容を誤解して解いたことが挙げられる．安全だと判断した理由を記述する解答欄に，怪しいと判断した理由を記述した学生が 2 名いた．そのため，正確な値を測ることができなかった．

③の問題においては，学習前は，アプリの機能の実現するために必要なパーミッションを正確に判断できていた問題を，学習後にアプリの機能の実現に不必要なパーミッションであると判断した学生が 3 名いた． 教材の中では危険なパーミッションについての説明を行っていたため，学習により危険なパーミッションに過敏に反応したと考えられる．

しかし，②の問題については有意性を確認することができた．本教材による学習を通して，非正規のアプリマーケットが安全ではないことを理解することができたためだと考えられる． 学習後に，非正規のアプリマーケットでは不正アプリの危険性が高いと判断できるようになった学生は 3 名おり，その学生はアプリの評価やコメントの内容が良かった場合でも，不正アプリの危険性に気付くことができた.本教材により,安全と判断する時の条件が増えたことが窺える.

8．結論と今後の課題

本研究では加害者視点を用いた体験学習によるネット犯罪を防止する教材の作成を行った.

今後の課題として，数字と記号で構成されている危険なパスワードの学習に力を入れる必要があると考える．また，危険なパーミッションの説明では，危険性を強調するのではなく，そのパーミッションに含まれるアクションの内容を中心に説明をするようにする．

参考文献

[1] 警視庁サイバー犯罪対策プロジェクト，”情報セキュリティ対策ビデオ，” http://www.npa.go.jp/cyber/video/, 2017. 02. 14, (2017. 12. 26 閲覧).
[2] IPA,”映像で知る情報セキュリティ～映像コンテンツ一覧～，” https://www.ipa.go.jp/security/keihatsu/videos/,2017.04.03, (2017. 12. 26 閲覧).
[3] 外山 みどり，”社会的認知の普遍性と特殊性:態度帰属における対応バイアスを例として，”タイ人社会心理学研究，1 巻，pp. 17-24，2001.
[4] 江連 三香,”増加した社会インフラを標的としたサイバー攻撃:5. サイバー攻撃に備えた実践的演習．”情報処理，55 巻，7 号，pp. 666-672，2014. 6. 15.
[5] TeamsID,”Announcing our Worst Password of 2016,” https://www.teamsid.com/worst-passwords-2016/, 2017. 12. 01, (2017. 12. 26 閲覧).
[6] FUJITSU,”あなたは大丈夫！？危険なパスワードを改善して安全性を高めよう(1/2),” https://azby.fmworld.net/usage/closeup/20110427/, 2011. 04. 27, (2017. 12. 26 閲覧).