シリアスゲームを用いた
セキュリティインシデントについての理解促進

１４３２０８３　瀬古優香
指導教員：山崎治　准教授

1. はじめに

セキュリティインシデントとは、コンピュータの利用や情報管理、情報システム運用に関してセキュリティ上の脅威となる事象を指す。セキュリティインシデントに対する意識は、企業など組織中での経験を通じて向上していくものと考えられる。そのため、企業での実務経験のない学生では、セキュリティインシデントに対する理解度向上が困難であり、関連知識の獲得に負の影響がでることも考えられる。そこで、学生のうちに情報系セキュリティ資格試験に出題されるレベルのセキュリティインシデントの問題に対して理解度を高めるために、知識獲得のための学習と並行して「疑似的な実務経験」を積むことを提案する。本研究では、このような「疑似的な実務経験」を与える材料として、セキュリティに関するシリアスゲームを用いる。

2.目的

セキュリティインシデントに関するシリアスゲームにより、疑似的な実務経験を積むことで、セキュリティ関連の知識獲得に影響が出るかを検証する。

3. 実験

3.1 方法

実験参加者：本学情報科学部情報ネットワーク学科生 18 名

実験計画：プレテスト及びポストテストを用意し、テストの間に行う作業において「統制条件」「ゲーム無し条件」「ゲーム有り条件」の 3 条件を設け、1 要因 3 水準参加者間計画で実験を実施した。

材料:プレテスト及びポストテストは Google フォームを利用した。テスト内容は資格取得用の過去問題集（例えば（五十嵐 2017）など）より 15 問引用した。「ゲーム無し条件」「ゲーム有り条件」で使用するテキストは、資格教本からプレテスト・ポストテストに関連があるページを抜粋し、作成を行った。「ゲーム有り条件」では、トレンドマイクロ株式会社で配布されているインシデント対応ボードゲームを使用した。

手続き：実験は「プレテスト」「学習フェーズ」「ポストテスト」の 3 つから構成されている。プレテストと学習フェーズは同日に実施し、ポストテストはその後の指定期間内で実施するよう求めた。

統制条件の参加者は、学習フェーズでは何も行わず、退室してもらった。ゲーム無し条件の参加者は、実験者が提供するテキストを使用して、20 分間、自身のやりやすい方法およびペースで学習をしてもらった。また、ポストテストの実施までの間に再度勉強しても良いことを伝えた。ゲーム有り条件の参加者は、テキストを用いた 20 分間の学習後、参加者ペアでインシデント対応ボードゲームを行ってもらった。また、ゲームの解説資料を渡し、ポストテストの実施までの間に再度勉強しても良いことを伝えた。

「ポストテスト」のフェーズでは、「学習フェーズ」から 24 時間をあけて PC もしくはスマホから Google フォームにアクセスしてもらい、ポストテストを行ってもらった。

3.2 結果

図 1 に各条件のポストテストの平均点を記す。

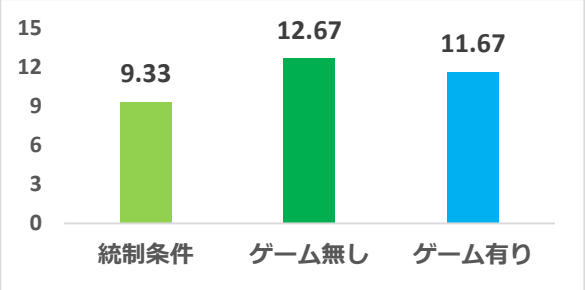

図 1：ポストテスト平均点

1 要因分散分析により分析を行った結果、有意差が確認された(F(2,15)=3.87,p=.04,偏η^2=.34)。多重比較を行った結果、統制条件とゲーム無し条件の間で有意な差が認められた(t(15)=2.71,p<.05,r=.57)。

また、図 2 にポストテストからプレテストの点数を引いた差を平均した点数を記す。

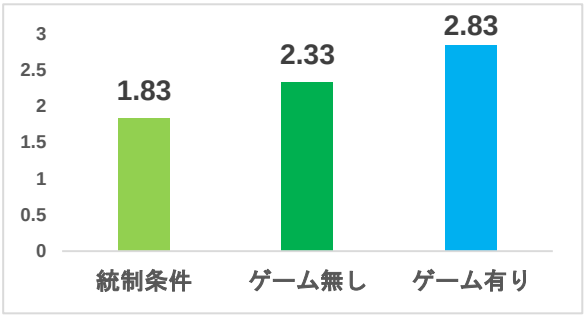

図 2:ポストとプレの差の平均点

1 要因の分散分析を行った結果、有意差は認められなかった(F(2,15)=0.46, n.s.,偏η^2=.06)。

4. まとめ

本実験では、シリアスゲームがセキュリティインシデントの理解度に影響することが明確に示せなかった。

ポストテストの平均点では有意な差が出たにも関わらず、ポストテストからプレテストの点数を引いた点数の差では有意な差が見られなかったことから問題数の増量や実験参加者数の増加などの改善点があげられる。また、シリアスゲームの内容を実験用に変更したため、実際のゲーム内容により近くすることでゲーム有り条件の結果に影響を与えると考えられる。

参考文献

五十嵐聡　(2017).　平成 29 年【下半期】IT パスポートパーフェクトラーニング過去問題集　技術評論社