JSiSE Research Report
vol.32,no.5(2018-1)

大学事務職員向けのサイバーセキュリティ教材開発

林一雅[*1], 三好史恵[*2], 庄司紘一郎[*2], 辻澤隆彦[*1]
*1 東京農工大学総合情報メディアセンター, *2 東京農工大学学術情報課

Development of Cyber Security Awareness and Education for a University Administrative Staff

Kazumasa Hayashi[*1], Fumie Miyoshi[*2], Koichiro Shoji[*2], Takahiko Tsujisawa[*1]
*1 Information Media Center, Tokyo University of Agriculture and Technology,
*2 Academic information and ICT, Tokyo University of Agriculture and Technology

2014 年に施行されたサイバーセキュリティ基本法により, 教育研究機関はサイバーセキュリティの確保や教育を実施することとなった．本稿では，情報セキュリティ意識調査の実施結果と先行研究を踏まえてサイバーセキュリティ教材の開発過程について報告する．サイバーセキュリティ教材の内容は，マルウェア対策，パスワード管理，標的型攻撃メールの対応，USB メモリ等の外部記憶装置の 4 点で，いずれも基本的な注意事項をスライド形式にまとめてウェブ配信した. 最後に教材の満足度調査を実施した.

キーワード: サイバーセキュリティ教育，大学事務職員，e-learning

1. はじめに

2014 年にサイバーセキュリティへの対応に向けた基本ポリシーとなるサイバーセキュリティ基本法が施行された．その第 8 条には，教育研究機関の責務として,「基本理念にのっとり，自主的かつ積極的にサイバーセキュリティの確保，サイバーセキュリティに係る人材の育成並びにサイバーセキュリティに関する研究及びその成果の普及に努める」とあり各機関には対応が求められている．それらのサイバーセキュリティに対応するため，大学事務系職員向けにサイバーセキュリティ意識向上を目的とした意識調査を実施した(1). この調査は，非技術的な対策を実施するための第一歩として，個人の行動に関するリスクを明確化することを目的に大学事務職員 299 人を対象として実施した情報セキュリティに関する意識調査である.

本稿では，2017 年 2 月に実施した情報セキュリティ意識調査の結果(1)に基づいて，大学事務職員を対象としたサイバーセキュリティ教材開発過程について報告する.

主な調査内容は，日常的な行動と対策強化の要請が高い「標的型メールへの対応」,「USB メモリなどの外部記憶装置の利用」, 及び「マルウェア対策」等である.

調査結果として次に記述する点と検討すべき点がわかった. 標的型メール攻撃に関しては, 例示された「標的型メール攻撃」に対しての行動と，一般的な設問として示された「不明なメールアドレスからのメール」に対する行動には差があり，回答者は標的型攻撃メールと不明なメールアドレスからのメールは脅威が異なるものと判断していると推察された．サイバーセキュリティ教育においては，認識に差があることを前提に教材開発する必要性が考察された.

「USB メモリなどの外部記憶装置の利用」に関しては，情報の暗号化は実際に利用するには負荷が高いと感じており，暗号化の必要性は認識しつつも，約 14-20%が「安易に利用してしまう」と回答している．サイバーセキュリティ対策として，簡便な代替手段の提供やシステム的な対応を進める必要性が考察された.

マルウェア対策ソフトアウェアや OS を最新の状態にすることについては，情報セキュリティ対策として有効であるという認識は高いが，19.4%の回答者は，その迅速な対策の実施には至っていないことがわかった．理由としては，作業負荷や技術的・知識的困難が

理由と分析しており，システム的な対応による負荷軽減が重要となる．これらの結果を踏まえて，サイバーセキュリティの教材を開発する．

2. サイバーセキュリティ教材の開発

サイバーセキュリティ教材作成の先行研究については，大学生向け情報セキュリティ意識向上の先行研究によると，サイバーセキュリティの重要性やニーズは理解しているが，様々なところから断片的なセキュリティ概念を学んでおり，継続的なトレーニングが必要であるとしている(2)．また，NIST SP 800-50 の「IT セキュリティの意識向上およびトレーニングプログラムの構築(3)」によると，セキュリティ意識向上キャンペーンとトレーニングが必要であるとしている．しかし，サイバーセキュリティ意識向上プログラムについて，セキュリティ意識が何であるかを理解していないと失敗につながる要因を分析している(4)．これらに対応するために，リスクのあるユーザを特定できないこととサイバーセキュリティがどのようにユーザに学ばれているかについて理解されていない点があるとして，データ分析を行うことで，よりよい教材設計ができるとしている(5)．

情報セキュリティ意識調査の分析と先行研究を踏まえて，次の内容のサイバーセキュリティ教材を開発した．内容は，マルウェア対策，パスワード管理，標的型攻撃メールの対応，USB メモリ等の外部記憶装置の 4 点でいずれも基本的な注意事項をまとめており，スライド形式のウェブ配信にて閲覧できる教材である．教材の受講の流れは，想定受講時間を 15 分程度としてスライド教材を学習して，その内容に対して確認テストに回答する．

3. おわりに

図 1 に示すのは，本教材の満足度調査を実施し，212 名から得た結果である．Q1 の質問には，42.9%が役に立つと回答し，Q2 の質問には，60.8%が分量は適当であると回答し，Q3 の質問には，60.4%が何度は適当であると回答している．Q1 は 10.4%，Q2 は 21.7%，Q3 は 20.8%が「わからない」と回答され，詳細な分析を行う必要がある．

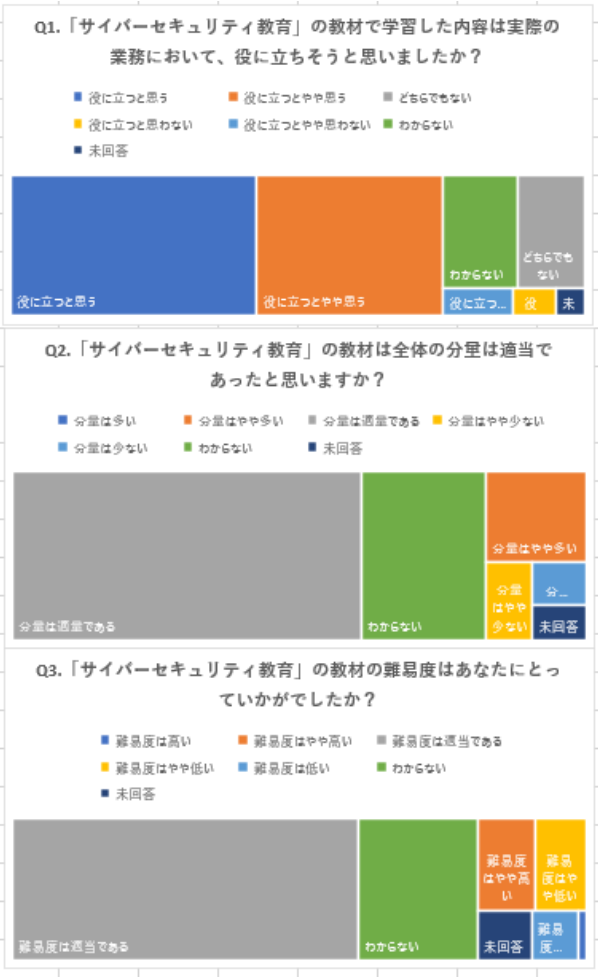

図 1 教材の満足度調査結果

参 考 文 献

(1) 辻澤隆彦，林一雅，川村喜和:”大学事務職員の情報セキュリティ意識調査（リスクの認識と行動について）.” 学術情報処理研究, No.21, pp.63-70, (2017)

(2) Eyong B. Kim.: "Recommendations for information security awareness training for college students", Information Management & Computer Security, Vol.22, Issue 1, pp.115-126, (2014)

(3) Mark Wilson, Joan Hash.: "Building an information technology security awareness and training program" NIST Special publication 800.50, pp.1-39 , (2003)

(4) Maria Bada, Angela Sasse, Jason R. C. Nurse.: "Cyber Security Awareness Campaigns: Why do they fail to change behaviour?", International Conference on Cyber Security for Sustainable Society, pp.118–131, (2015)

(5) Karina Korpela.: "Improving cyber security awareness and training programs with data analytics", Information Security Journal: A Global Perspective, 24.1-3, pp.72-77, (2015)