複合メディアと LMS を活用した教職員向け情報セキュリティ教育

田名部 元成 [1)], 中野 淳 [2)]

1) 横浜国立大学 情報基盤センター

2) 株式会社日経 BP

tanabu-motonari-dz@ynu.ac.jp

Information Security Awareness Training for Faculty and Staff by Utilizing Comprehensive Media and Learning Management System

Motonari Tanabu [1)], Atsushi Nakano [2)]

1) Information Technology Service Center, Yokohama National University

2) Nikkei Business Publications, Inc.

概要

技術的か人的かによらず、情報セキュリティ対策は、大学にとって極めて重要な経営課題となっている。しかしながら、人員や予算などの資源制約から、十分な対策が講じられていない現状にある。特に、セキュリティ教育は、多忙な業務に追われる教職員の置かれた状況を十分な配慮をせずに行うと、認知的身体的負荷の増加や学習意欲低下を招き、教育効果を低減させてしまうことから、現場の教職員が無理なく学び続けられるような解決策が求められている。本論では、大学教職員に、絶え間なく変化する情報セキュリティ動向に継続的に関心を持ってもらい、負担感なく情報セキュリティへの意識向上を促す方策として、複合メディアと学習管理システムを融合させた仕組みを用いた情報セキュリティ教育方法を提案し、その実証実験の計画について述べる。

1 はじめに

近年、教育機関において深刻な事態をもたらす情報セキュリティインシデントの発生が多発している[1]。一方、教育、研究、地域貢献という大学のミッションの達成において、事業継続を確実にすること，事業リスクを最小限にすること，並びに投資に対する見返り及び事業機会を最大限にすることを目的として[2], 大学にとって価値ある情報資産を適切に保護することが、社会から当然のものとして要請されるようになってきた。十分な対策を講じないことによる情報セキュリティインシデントの発生やインシデントに対する不適切な対応は、大学教職員、学生、学外関係者その他に損害や不利益を与えるのみならず、大学の社会的信頼が損なわれる可能性があり、大学は、他の重要な事業資産と同様に、組織にとって価値がある資産である情報を適切に保護する必要がある。

このように、情報セキュリティ対策は、大学にとって極めて重要な経営課題となっているにも関わらず、人員や予算などの資源制約から、十分な対策が講じられていない現状にある。特に、情報セキュリティ対策に効果が高いとされる人的対策としてのセキュリティ教育は、多忙な業務に追われる教職員にとっては、教職員の置かれる業務的環境や状況を十分に配慮して実施しなければ、認知的、身体的な負荷を増加させ、学習に対する意欲を低下させ、セキュリティ教育を形式的・表面的にし、教育効果を低減させてしまうことから、現場の教職員が無理なく学び続けられるような解決策が求められている。本論では、大学教職員に、絶え間なく変化する情報セキュリティ動向に継続的に関心を持ってもらい、負担感なく情報セキュリティに対する意識向上を促す方策として、複合メディアと学習管理システムを融合させた仕組みを用い

た情報セキュリティ教育の方法を提案し、その実証研修の計画について述べる。

2　情報セキュリティ教育の目的と方法

情報処理推進機構[3]によれば、組織では、情報セキュリティ教育の対象には、1）幹部教育：CISO の育成、2）セキュリティ管理者教育、3）セキュリティ技術者教育、4）一般ユーザ教育の４つある。これに習うと、国立大学における情報セキュリティ教育の対象は、1）CISO および CIO の育成、2）情報企画課などの情報系事務組織や情報系センターにおけるセキュリティ管理業務(CSIRT 等)担当の教職員、3）全学的に利用している情報システム（ネットワーク基盤、クラウドサービスを含む）の技術的管理を行う情報系センターや情報企画課等の教職員と、部局等の情報システムを管理運営する教職員、4）一般ユーザとしての教職員と学生、が考えられるが、セキュリティ管理者を明示的に配置していない場合もあり、この区分が厳密に適用されない大学も多いと考えられる。また、学生に対する利用者教育を、教職員と同じ方法ではなく、情報リテラシー教育として正規授業の中で行う場合もあり、民間企業にはない大学固有の対応も存在する。

一方、情報セキュリティ教育の方法には、クラス形式の集合教育、e ラーニングや課題図書による自己学習、自己点検チェックシートへの記入のほか、標的型メール攻撃訓練などがある。これらの教育方法の選択は、教育対象者ごとの目的や実施に必要な人的予算的資源の制約、および制度的、技術的、時間的な制約によって、その決定は組織によって異なってくる。例えば、大人数を対象とした同一内容の情報セキュリティ教育を展開する場合、講師や時間と場所の確保の問題から e ラーニングという方法が選ばれるだろう。一方で、役員や部局長などの管理層を対象とした教育においては、ディスカッションやゲーミングを用いた集合教育が効果的であるかもしれない。大学における教職員向けの e ラーニング教材は、情報セキュリティに関わらず、不正会計、ハラスメント、著作権などに関わる内容の教育方法として広く用いられているが、管理する側が、当該の内容を一通り教育したという既成事実をつくるために利用される側面も否めない。また、教える主体が不在の自己学習であるため学習に対する動機付けが十分に与えられないと、長続きしなかったり、学習履歴を残すということが目的化したりし、知識の定着が行われず実質的な教育効果が期待ほど得られないという可能性も考えられる。さらに、情報セキュリティ教育においては、新しく登場する情報技術に加え、サイバー攻撃の新しい手口についても知識を更新する必要があるため、継続的な学習が求められる。

したがって、一般ユーザとしての大学教職員に対する情報セキュリティ教育においては、絶え間なく変化する情報セキュリティ動向に継続的に関心を持ってもらい、十分な動機付けが行われ、負担感なく情報セキュリティに対する意識向上が図れる仕組みが必要となる。本論では、この課題に対して、LMS(Learning Management System) を利用した e ラーニングによる教材提供と教職員の興味関心を集めやすい教育機関における情報セキュリティインシデントや効果的な取り組みなどの速報性の高い情報の提供を有機的に組み合わせる方法を提案する。

3　複合的なメディアの利用

近年の情報媒体は、新聞やテレビといったマスメディアに加えて、電子メールやブログなどのネットワークメディア、あるいは、双方向コミュニケーションによる社会的相互性を原理とするソーシャルメディアなど多種多様なものが存在する。とくに、インターネット上のメディアでは、文書や動画のようにコンテンツが蓄積（ストック）されて利用されるものと、SNS のように、速報性の高い情報が他者に伝達（フロ

ー）されて利用されるものとがある。e ラーニングの教材は、ストック型のメディアと見ることができる。

情報セキュリティ分野においては、その教育内容は絶えず変化するため、ストック型のメディアの利用のみでは、その変化スピードに追従することは難しい。情報セキュリティ対策動向の変化に即時に対応した教材を開発するには、追加的なコストと時間が必要となるからである。したがって、情報セキュリティ教育を展開するためには、速報性の高い情報を学習者へ提供するとともに、その情報に関連性が高い（ストック型の）教材の活用が効果的であると考えられる。新規教材の開発は、即時対応が難しいが、必要となる教育内容に関連の強い既存コンテンツを必要とする文脈の中に埋め込んで提供することは比較的容易であると考えられるからである。

本論では、変化の激しい情報セキュリティ分野の教育においては、関心を維持できるような速報性の高い情報を提示しながら、その情報に関連する既存の教材や記事を、特定の文脈に埋め込んで再構成した“教材”を使った教育が効果的であると仮定し、その実施方法として、ストック型のメディアとフロー型のメディアを組み合わせ、冊子体、スマートフォン、タブレット端末、PC などの多様なデバイスとチャネルを使って情報セキュリティに対する意識を顕在化させるための仕組みを提示する。

4　情報セキュリティ教育のためのシステム

大学に対する ICT の利用動向に関する 2015 年の調査[4]によれば、国立大学の 89.9%(n=69)、公立大学の 50.0%(n=56)、および私立大学の 63.2%(n=391)が LMS を導入していると回答しており、その利用動向は 2015 年までに年々増加していたことから、現時点においては、それ以上の割合で LMS が利用されていると考えられる。この状況から、大学において教職員向けに LMS を利用することは難しくない。実際、横浜国立大学では、学生向けに利用していた LMS を利用して、教職員向けの e ラーニング教育を行なっている(2018 年度)。LMS を活用することで、学習者ひとりひとりの学習進捗を管理することが容易となり、オンラインのテストによりコンテンツ理解度の自己確認も行なうことができるようになる。

筆者らは、大学における現時点での情報システムや情報端末の利用状況を考慮し、LMS 上での e ラーニング教材、e ラーニング教材と合わせて読める冊子体教材、e ラーニング教材の取り扱う内容に関連するコンテンツ群、e ラーニングや各種記事へのアクセスのトリガーとなるニュース速報を複合的に組み合わせる情報セキュリティ教育の仕組みを図 1 のように具現化した。以下、主要な構成要素について述べる。

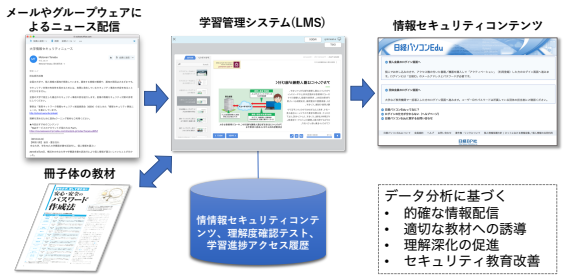

図 1　複合メディアと LMS による教育システム

4.1 学習管理システム LMS

本論で提案する教育システムの中核は、e ラーニング教材の特定に内容に直接リンク可能な SCORM 対応の LMS である。現時点で、この要件を満たす LMS は複数存在する。実証実験のために富士通社製の CoursePower V2 を利用した。LMS では、後述する情報セキュリティコンテンツを再構成して作られた e ラーニングコンテンツを提供するか、既成のコンテンツを提供する。図 2 は、筆者が、コンテンツ提供サービスを活用して独自に作成した SCORM 形式の e

ラーニング教材を LMS 上で表示したところを示している。PowerPoint 形式のファイルを e ラーニング形式のコンテンツに変換するソフトウエアを利用すれば、教員が保有する教材を効率的に e ラーニング化することが可能となる。

図 2　既存記事の再構成による e ラーニング教材

4.2 情報セキュリティコンテンツ提供サービス

2 つ目の要素は、クラウド型の教育・研修用コンテンツ提供サービスである。実証実験にむけて、日経 BP 社が提供する日経パソコン Edu [5]を利用した。このサービスは、情報セキュリティや情報倫理のみならず、PC 操作、ソフトウェアやクラウドサービスの利用法、資格取得などに関する PDF コンテンツをパソコンやタブレット、スマートフォンなどから閲覧することが可能である(図 3)。

図 3 クラウド型コンテンツ提供サービス

認証は、ID・パスワードのほか、学術認証フェデレーション（学認）が利用可能である。また、事前に各コンテンツの権利処理が行われているため、コンテンツの一部を流用して独自教材や e ラーニングのコースを作成することができるのが大きな特徴である。また、各コンテンツには、独自の URL が割り当てられているため、メールや Web ページ、LMS などに当該 URL を配置することで、研修対象の教職員に対して、必読のコンテンツを容易に告知できる。

4.3 プッシュ型のニュース情報

本実証研修では、教育機関の情報セキュリティインシデントの事例を日経 BP 社が提供する。上述した通り、教育現場での具体的なインシデントの内容や原因を紹介することで、研修参加者の情報セキュリティに対する関心を高め、学習に対する動機付けが与えられると考えているからである。図 4 は、情報セキュリティニュースの配信例を示している。

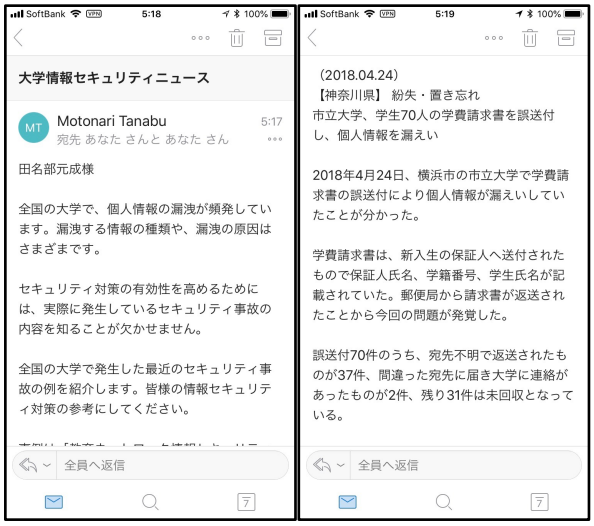

図 4　プッシュ型情報の配信例

4. 4 冊子体の教材

今回の実証実験では、LMS を用いた e ラーニング教材、コンテンツ提供サービス、プッシュ型情報の配信に加えて、冊子体による教材も利用する。この教材は今回の実証研修のために新たに制作した。最近では、全学的に利用してい

る大手商用クラウドサービスのアカウントが乗っ取られて、受信したメールが第三者に転送されるように設定が書き換えられ、結果として大規模の機密情報が漏洩するといった深刻なインシデントが多発していることを受けて、パスワードとアカウントの適切な管理方法についての解説、個人情報が漏洩した大学や教育委員会でのインシデントの事例などの記事を掲載した。

図 5 冊子体の教材

この教材は、上述した LMS 上の e ラーニング教材と連動するもので(図 6)、空き時間を利用して手軽に読むことができるように配慮した。

図 6 冊子体教材(左)と e ラーニング教材(右)

5 おわりに

本論では、大学教職員に、絶え間なく変化する情報セキュリティ動向に継続的に関心を持ってもらい、負担感なく情報セキュリティへの意識向上を促す方策として、複合メディアと学習管理システムを融合させた仕組みを用いた情報セキュリティ教育方法を提案し、その実証実験の計画について述べた。教育方法は、学習管理システム(LMS)とその上で動作する e ラーニング教材、コンテンツ提供サービスとその上で提供される情報セキュリティコンテンツ、プッシュ型のニュース情報、冊子体の教材からなる。e ラーニグ教材や冊子体の教材は、コンテンツ提供サービスを通じて取得した、予め権利処理されたコンテンツの再構成によって作成することを想定した。プッシュ型の情報は、メール等で研修対象者に送られる。この情報には、コンテンツ提供サービスや LMS 上の e ラーニング教材への直接リンク(URL)を配置することが可能なため、研修対象者を無理なく関連教材や記事に誘うことが可能となる。同様に、LMS からコンテンツ提供サービスに接続させることも可能となる。LMS を利用する利点は、コンテンツ提供サービスが提供していない、コンテンツ閲覧者の学習行動に関する詳しい情報を、研修実施者側で取得できるようになることにある。これらの情報は、教育研修をより実質化することや、研修プログラム自体の改善に用いることが可能であり、いわゆる情報セキュリティ教育の PDCA サイクルの実現に寄与すると考えらえる。

今後は、上述した計画に基づいて実証実験を行い、提案のする仕組みが、情報セキュリティ動向に継続的に関心を持ってもらい負担感なく情報セキュリティへの意識向上を促すものであるかを評価する予定である。

5 参考文献

[1] 教育ネットワーク情報セキュリティ推進委員会(ISEN), 情報セキュリティ事故ニュース, http://school-security.jp/

[2] JIS Q 27002:2006 (情報セキュリティ・マネジメントの実践のための規範), 2006.

[3] 情報処理推進機構 (IPA), 情報セキュリティ教育の対象, https://www.ipa.go.jp/security/manager/edu/training/index.html

[4] 大学 ICT 推進協議会(AXIES) ICT 利活用調査部会, 高等教育機関における ICT の利活用に関する調査研究結果報告書(第 3 版), 2016.

[5] 日経パソコン Edu, https://trendy.nikkeibp.co.jp/pcls/edu/