Moodle を利用した全学セキュリティ教育について

富山大学　CSIRT　沖野　浩二

平成 28 年に本学において、大きな情報インシデントが発生した。これを受けて、本学では、大学をあげてのセキュリティ体制の整備を行うこととなった。その一環として、構成員のセキュリティレベルの向上を目的とし、LMS である Moodle を利用したセキュリティ教育を行うこととした。本論文では、この実施における検討事項および現状、今後の課題について述べる。

１．はじめに

近年、大学の高度な教育・研究において情報機器の利用および情報ネットワークの活用はなくてはならないものとなっている。大学構成員における大学 ID の申請は、ほぼ 100%であり、大学においては利用しないユーザはいないと言える。

情報機器およびネットワークの利活用の推進に伴って、情報セキュリティ意識の構築や著作権等の情報コンプライアンスの理解など、一般に情報モラルと呼ばれる情報化社会における情報セキュリティ教育の必要性が叫ばれている。

これらの知識不足により引き起こされる情報インシデントは後を絶たない。インシデントの防止には、これらの知識を適切に習得することが重要である。

本稿では、大学における情報セキュリティ教育における諸課題および内容の整理、本学における実施方法、その現状、最後に今後の課題を述べる。

２．セキュリティ教育における問題点

セキュリティ教育には、大きく分けて一般的なものと、職種等に伴う専門に対するものに分けられる。一般的なものは、初等中等教育に行われる情報モラル教育である。専門に対するものとしては、研究者に対する知的財産保護に関する情報管理や、医療従事者に対するプライバシー情報に対する取り扱いなどが挙げられる。

大学におけるセキュリティ教育は、初歩的な情報モラル教育から知的財産の保護・活用を前提とした専門性を有した情報管理教育との間にあるものであり、また、携帯電話のフィルタリング機能に代表される保護された環境から、自ら積極的に守る環境への移行時に行われる教育であると言える。

さらに、大学構成員を対象とした場合には、学生だけでなく教職員も対象となり、教職員に対する教育は、学生とはまた異なる問題点が存在する。具体的な例としては、情報セキュリティ教育は、ここ数年で構築されてきたものであり、教員の年齢や背景によりその理解内容が大きく異なっているという面である。

これ以外の問題も含めて、大学におけるセキュリティ教育の問題点を整理すると、大きく、次の３つに分けられる。

i)内容

情報セキュリティ教育における内容については、技術および情勢の速い変化によりスタンダ

ードと呼ばれるものがないのが現状である。例えば、昨今のパスワード教育においては、頻繁に変更することの問題も指摘されている。そのような中で、教育項目として、参考となりえるものとしては、IPAのセキュリティ関連資料や、国立情報学研究所が中心となり策定された「高等教育機関の情報セキュリティ対策のためのサンプル規定集」(2015 年版)の“A3301 教育テキスト作成ガイドライン（一般利用者向け）“が挙げられる。

加えて、情報セキュリティ教育では、情報倫理教育と共通部分も多く、大学の一般教養にて開設されている「情報処理」科目との切り分けも考える必要がある。

ii)多様性

大学の全構成を対象にした場合には、学生・教育職員や事務職員などの職種の違いだけでなく、留学生など教育背景や社会的背景が異なる多くの構成員がいる。この中には、必ずしも日本語が得意ではない人や知的財産権に関する理解が正しくない人も含まれる。

iii)持続性

セキュリティ教育を行う上では、定期的なコンテンツの改変が避けては通れない。これは、i)内容のところでも触れたが、習得すべきスタンダードが決まっていないことに加えて、内容が刻々と変化しているからである。また、受講者に対して、自分に被害が及ぶ身近な問題として感じてもらうためには、具体例を見せることが重要である。このためには、誰かが常に情報を収集するだけでなく、新聞などのコンテンツを利用する必要があり、これらの権利処理も必要となる。

さらに、本学の構成員は、1万人程度であり、これら全員に対して、定期的に教育を行うことは莫大なコストが掛かる。これらのコストは、教育システムの開始時だけでなく、構成員が毎年入れ替わる大学においては、毎年発生することとなる。

3．セキュリティ教育内容

構成員全員が学ぶべきセキュリティ教育内容として、先に述べたIPA資料やサンプル規定集を参考にし、これに本学におけるインシデント発生状況を鑑みて、検討した結果、次の項目を含むことが必要だと考えた。

<u>法的部分</u>

・基本的人権
・知的財産権（特に著作権）
・個人情報・機密情報の保護
・その他、情報を取り扱う上で知っておくべき法的知識

<u>マナー部分</u>

・メール利用時のマナー
・SNSなど利用時のマナー
・情報公開時のマナー

<u>技能部分</u>

・アカウントの管理
・コンピュータウイルス
・暗号化などの情報を守る技術
・PC管理上の注意

4．全学教育方法

3章で検討した内容に関して、大学構成員すべてを対象にした場合には、次の問題があるこ

とが指摘される。

・カリキュラムの整備

学生と教職員では理解すべき内容が異なるだけでなく、技能職種により求めるべき内容が異なるのではという問題がある。例えば、医療職と教育職では前提となる法令が異なる問題や、ユーザとして利用している学生とサーバを管理している教員などは、求められるレベルが異なるということである。本来ならば、基礎から専門に繋がるセキュリティ教育カリキュラムを整備する必要がある。しかし、今回は、検討および準備期間の関係から、内容を構成員の共通理解を求める範囲に絞ることとし、学生向け内容と教職員向け内容の２本立てとした。

・言語能力の差

大学においては、日本語を母国語とする者だけでなく、それ以外の言語を母国語とするものが多数存在する。特に留学生においては、文化的背景からセキュリティに対する理解が浅いものも存在する。

そのため、コンテンツには、多言語化が必要と判断された。本学の外国籍構成員比率より、日本語以外に英語および中国語のコンテンツを準備することとした。

・教育コストの負担

現在、情報セキュリティ教育として 60 分のガイダンスを理工学系の４年生以上の学生、大学院生を対象に年６回行っている。これらの負担は教員の講義の実施の負担だけでなく、資料の印刷や出席の確認など事務も含め多大な負担が係っている。

実際に全構成員に対して、対面授業方式にて教育を行うことは、実施回数の増加だけでなく、英語だけでなく中国語の語学能力を有する教員の問題、資料の準備コストの負担、スケジュール調整などが必要となる。

本学の実施方法

これらの問題を考え、本学では、総合情報基盤センター　ICT 教育推進研究開発部門　の協力を得て、LMS である Moodle を利用し、全学教育を行うこととした。総合情報基盤センターの Moodle を利用することで、

・ほぼ全員が取得している総合情報基盤センターID が利用できる

・学習履歴の管理およびテストを実施できる

・対面授業と比較して、対応する教員および事務スタッフの負担を低減することができる

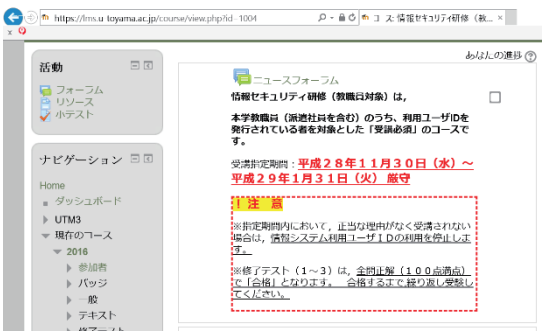
ことから、全構成員を対象にしたセキュリティ教育を試験的に実施することとした。

現実に実施するには、コンテンツの作成が必要であるが、多言語化の必要性および準備期間の関係から、日本語と英語および中国語版を有したデータパシフィック社製のコンテンツ

教員向け：教職員のための情報倫理
とセキュリティ

学生向け：INFOSS　情報倫理

を導入し、実施した。また、これらのコンテンツには、修了テストも付随しており、このテストを利用することにより、学習内容の確認を行うこととした。



５．結果（現状）

総合情報基盤センターの Moodle を活用し、市販のコンテンツを利用することにより、大学全構成員に対するセキュリティ教育を開始した。今回の実施に対して、2 章で述べた i)内容および ii)多様性、iii)継続性の問題点に対して考察する。

・i)内容に関しては、市販コンテンツを利用することにより、設定した内容を含む標準的なものとなった。

・ii)多様性に関しては、日本語以外にも英語および中国語のコンテンツを提供できた。

・iii)持続性に関しては、市販のコンテンツを更新することにより可能となる。また、市販のコンテンツを購入することにより著作権等の処理をコンテンツ作成側で行うため、実際の記事および具体的な商標を利用することが可能となった。

受講状況に関しては、教職員向け実施のスケジュール(平成 29 年 1 月 31 日まで受講予定)が終了し、コース修了率は、速報値（2/7 付)として、

部局系教職員 96.6%(1,415 名/1,465 名)

事務局系職員 100%（536 名/536 名）

となっている。この修了率は今年度中には 100%となる予定である。また、現在、学生向けも実施されている。(平成 29 年 4 月 28 日受講完了予定)

６．今後の課題

今回は、CSIRT メンバー（Computer Security Incident Response Team）が緊急対応ということで、企画および実施した。しかし、今後も同様な教育が推進できるかは大きな疑問がある。

1 点目として、モチベーションという点である。今回は、インシデント発生という要因が背景にあり、組織として、その必要性が求められた。しかし、今後は、受講者側の受講意欲の低減に加えて、大学側も受講させようとする意欲の低減が考えられる。

２点目として、セキュリティ教育カリキュラムという観点である。今回の内容は、全員が理解すべき基本的な内容であり、これを繰り返すだけでは知識が深まるとは言えない。今後、サーバ管理者向け講習や、具体的なインシデント発生時の対応など、既存のコンテンツを利用できない内容の教育をどのように行うか、加えて、個別の教育を体系的に構築し、理解を深めることが必要である。

１点目の対応としては、大学執行部におけるこの教育の必要性へのコミットメントの継続である。これは、執行部による強い意識の継続が、受講への強制力を生むという側面があるからである。

２点目の対応としては、構成員に対する教育を行うための組織整備（人・物・金・権限）が必要だと考えられる。組織整備により、教育の実施責任者が明確化され、その者の命令により、受講体制の整備、定期的な受講の呼びかけや受講状況の確認、カリキュラムの見直し、コンテンツの追加改変を行うことができる。さらに、e-Learning だけでなく、対面形式での講義や実機を使った実習などにより実践的な研修へと繋げることが可能となる。

今後、本学がセキュリティ教育を維持・向上させるためには、この２点の環境整備を行うことが重要だと考える。