

オンライン情報セキュリティ教材の開発

原田晶子, 上田祐史¹, 隅谷孝洋, 中村純

広島大学

739-8521, 広島県東広島市鏡山 1-7-1

TEL: 082-424-6544

e-mail: harada@minerva.ias.hiroshima-u.ac.jp

概要

広島大学で開発している全構成員を対象としたオンライン情報セキュリティ教材「セキュリティ・エッセンシャル」について、そのねらい、構成、概要、今後の方針を報告する。「難しい内容を笑いながら学ぶ」ことを目指して、傍若無人ではちやめちな鬼ヶ島大学・桃唐太郎教授と、それを支える犬神助手、学生の狼田、雉子が活躍するというストーリーを教材に組み込んだ。情報教育センター協議会とメディア教育開発センターで作られた「情報倫理ビデオ」のクリップを一部に利用する。

1. はじめに

広島大学ではマイクロソフト株式会社と2004年10月に、1) 情報セキュリティ分野における人材育成、トレーニングの実施、2) 情報アクセシビリティ分野における情報バリアフリーに向けた協力の、2点を中心とした協定を結んだ。この第一点に関する協力の第一歩として、マイクロソフトが保有する「MCAセキュリティ」のトレーニングカリキュラムを活用して、広島大学の全学生および全教職員を対象に、情報セキュリティに関するトレーニングを2005年4月より実施することが同意されている。まずマイクロソフトにより、広島大学でMCAセキュリティのトレーニングが行われ、本稿の4著者を含む22人が試験に合格した。

次のステップでは2万人を超す広島大学の構成員(学生、教職員)に対するセキュリティ教育が課題となった。ネットワーク管理者等への講習会を別として、大多数の構成員への短期間での効率のよい教育はオンライン教育を中心とするのが現実的であるとの結論になり、中村、隅谷にその作成の依頼があった。MCAセキュリティトレーニングを受講し、試験に合格していた原田と上田に中村から協力要請があり、原

稿執筆を開始した。

2. 克服すべき問題点

教材の検討を始めてすぐ明らかになったことは以下の点である。

1. MCAセキュリティ・コースで要求されている内容は、暗号化、認証などの技術的な問題を多く含む [1]。
2. 本教材の内容は、全構成員に学習することが求められており、セキュリティについての知識も様々なレベルの人がいると考えられる。
3. しかし、インセンティブは特に用意されているわけではないので、十分に興味を持つ内容にしなければならない。
4. MCAセキュリティは、マイクロソフトの製品を想定しており、また資格試験という観点から多数の項目の正確な知識が求められている。しかし、大学の教材としては、利用されている他のOSも考慮し、何故脆弱性が発生し、それに対してシステムはどのように構成されていくべきか体系的に理解できるようなものが相応しい。

Development of on-line learning material for information security

A. Harada, Y. Ueta, T. Sumiya, A. Nakamura
Hiroshima University

¹ 現在：洲本市役所

難しい内容をいろいろな角度から繰り返し学習してもらうためには、説明の間に仮想人物を登場させ、学習者に抑えてもらいたい点を質問

させて答えるという手法がある。しかし、通常使われる「博士と太郎君、花子さん」型は、今回のように学習者が大学の学生、教員、職員である場合は、学習者が教材そのものを馬鹿にする危険がある。

そこで、登場人物たちの構成を少し捻り、責任者であるべき教授がおかしなことを言い、その尻拭いを助手や学生がするという形式を採用ことにした。これは、大学構成員にとっては、大学のパロディとして捉えることもできるので、内容を十分に練れば学習者の共感を得ることができるはずである。登場人物は鬼ヶ島大学・メディアセンターの桃唐太郎教授、犬神助手、学生の狼田君、雉子さんである。たとえば、VPNの節では桃唐教授は隣の部屋の学生たちと話をするために研究室の壁を壊してトンネルを作ってしまう。このように、技術的な説明だけでなく学習者がイメージしやすいたとえを用いる工夫を行った。

また、文字・画像情報のみが続いて単調になることを防ぎ、学習者の理解を深めるために、中村が参画しているプロジェクトである情報倫理ビデオ(国立大学情報教育センター協議会・メディア教育開発センター)からいくつかのクリップを取り込み教材として使用した。

3. 内容

検討の結果、章の構成は以下のようなものとなった。

第1章 セキュリティの基礎

暗号鍵, 共通鍵暗号方式, 対称鍵暗号方式, ハッシュ, デジタル署名, 認証局, DoS 攻撃 他

第2章 ソフトウェアの更新

セキュリティ修正プログラム, Windows Update, パッチ 他

第3章 ウイルス対策

ワーム, トロイの木馬, スパイウェア, バックドア, ウイルス定義ファイル, 検索エンジン 他

第4章 コンピュータセキュリティ

OSのインストール, サービス(デーモン), アクセス権, Administrator 他

第5章 認証のセキュリティ

認証の脆弱性, 辞書攻撃, ブルートフォース攻撃, スニフィング, リプレイ攻撃, ソーシャルエンジニアリング, バイオメトリック認証, Kerberos 認証 他

第6章 ネットワークセキュリティ

気密性, 完全性, SSL, VPN, パケットフィルター, ゲートウェイ, プロキシ, ファイアウォール, 無線 LAN, IEEE801.11x, ESS-ID, WEP, ウォードライビング, RADIUS サーバー 他

第7章 アプリケーションのセキュリティ

ウェブビーコン, クロスサイトスクリプティング, フィッシング, ゾーン, HTML メール, Office update, モバイルコード, Cookie 他

第8章 セキュリティに対する日常の取り組み

これは、マイクロソフトのMCAセキュリティのカリキュラムの内容を考慮し、またエンドユーザーの直面する問題を重視して構成したものである。サーバー管理者の知っておくべき項目は今回は取り扱わない。¹

4. おわりに

現在、原稿のオンライン化を行い1年生の前期の授業で「セキュリティ・エッセンシャル」コースとして利用し、評価を行っている。教材の公開から約1ヶ月間で約1000人の学生が受講、終了した。

「セキュリティ・エッセンシャル」を終了した学生に難易度についてのアンケートを行ったところ約400人の回答が得られ、ちょうど良いと答えた学生が40%、やや難しいと答えた学生が48%であった。また、デジタル署名やウイルス定義ファイルなどの用語について理解できたかどうかとの問いには、約半数の学生がこの教材によって理解したと回答した。これらの評価を元に、効果の高い教材の完成を目指して行く。

参考文献

- [1] Microsoft Corporation: 「MCA Security」(2004).

¹第2部で取り扱う予定である