東北大学における教職員を対象とした情報セキュリティ教育

小野﨑 伸久 [1)], 曽根 秀昭 [2)], 水木 敬明 [2)]

1) 東北大学 情報部情報基盤課
2) 東北大学 サイバーサイエンスセンター

i-security@grp.tohoku.ac.jp

Information Security Training for Staff in Tohoku University

Nobuhisa Onozaki [1)], Hideaki Sone [2)], Takaaki Mizuki [2)]

1) Information Infrastructure Division of Information Department, Tohoku Univ.
2) Cyberscience Center, Tohoku Univ.

概要

東北大学では、平成 29 年度から全教職員を対象にした情報セキュリティ教育を e ラーニング形式で実施しているが、本学の情報セキュリティポリシー及び情報システム利用環境の実態に合わせた教育コンテンツを提供するため、これを内製で作成している。本稿では、この取組みについて紹介する。

1 はじめに

本学では、平成 29 年 3 月に策定した情報セキュリティ対策基本計画をもとに、平成 29 年度から全教職員約 12,000 人を対象にした情報セキュリティ教育を e ラーニング形式で年 1 回実施している。このような情報セキュリティ教育の実施にあたっては、自組織の情報セキュリティポリシー及び情報システム利用環境の実態に合わせて、非現実的な理想論に終始せず、きちんと実践できる内容の教育コンテンツを作成することが重要であると考え、内製で取り組んでいる。

本稿では、この情報セキュリティ教育の取組みについて紹介する。

2 情報セキュリティ教育の概要

2.1 教育コンテンツの構成

教育コンテンツは、動画教材及び理解度確認テストの２つである。各コンテンツは日本語版と英語版を作成している。

受講者は動画教材を視聴し、理解度確認テストに合格することで受講完了となる。なお、理解度確認テストは 10 問中 8 問以上の正答で合格となることとした。

2.2 動画教材の作成方法

動画教材は、Microsoft 社の PowerPoint を使用してスライドを作成し、アニメーションや画面切り替えをクリック操作ではなく自動的に行われるように設定したうえで、エクスポート機能を用いてビデオ形式(mp4)に変換した。また、動画に流す音声は、音声合成ソフトで作成したデータをスライドに挿入し、アニメーションと同じように自動的に再生されるようにした。

2.3 e ラーニング基盤

情報セキュリティ教育のコンテンツ配信と理解度確認テストの実施には、本学の教員向けに提供されている e ラーニング基盤である東北大学インターネットスクール（ISTU）を使用した。

3 教育コンテンツの内製

3.1 平成 29 年度の教育コンテンツ

平成 29 年度では、本学として初の試みであるため、情報セキュリティ関連機関の公開情報及び本学の事前アンケートをもとに教育コンテンツを検討した。

IPA の情報セキュリティ 10 大脅威 2016 [1]によると、この 10 年、様々な脅威が現れ、攻撃者の手口は年々巧妙になってきているが、攻撃の糸口はあまり変わっておらず、表 1 に示す「情報セキュリティ対策の基本」による効果は多いに期待できるとのことであるため、これを動画教材に取り入れることにした。また、事前アンケートによると、ＯＳ・ソフトウェアのアップデート状況、セキュリティ対策ソフトのインストール状況及び定時ス

キャンの実施状況、パスワードの設定状況が不十分であることがわかったため、原点に立ち返って、これらの対策の必要性や設定方法などを動画教材に取り入れることにした。その他、当時の情報セキュリティの動向・情勢を踏まえて、表２に示す内容に絞り込んだ。

理解度確認テストについては、どの程度の難易度が適切であるか判断できず、手探りの状態であったため、ひとまずは情報セキュリティの初級者に照準を合わせることにし、表３の通りに作成した。

このようにして作成した動画教材及び理解度確認テストについては、本学の情報セキュリティポリシー等を検討する「情報セキュリティWG（ワーキンググループ）」において審議を行った。

表１　情報セキュリティ対策の基本

攻撃の糸口	情報セキュリティ対策の基本
ソフトウェアの脆弱性	ソフトウェアの更新
ウイルス感染	ウイルス対策ソフトの導入
パスワード窃取	パスワード管理・認証の強化
設定不備	設定の見直し
誘導（罠にはめる）	脅威・手口を知る

表２　平成 29 年度動画教材

No.	内容
1	最近の動向
2	今回の範囲
3	情報セキュリティ対策 ・ソフトウェアを最新に保つ ・セキュリティ対策ソフト ・パスワードの取扱い ・騙されないために手口を知る ・持ち出し時の対策 ・インシデント発生時の初動対応

表３　平成 29 年度理解度確認テスト（抜粋）

No.	設問・選択肢
2	情報セキュリティ対策は、ウイルス感染のような特殊な技術を駆使したサイバー攻撃だけでなく、人的ミス（メール誤送信、設定ミス、盗難、紛失）についても対策が必要である。 ● 正しい ○ 正しくない
4	Windows Update は時間がかかるうえに、パソコンの動作が遅くなるので、業務の繁忙期が終わるまでは行わない。 ○ 正しい ● 正しくない
5	セキュリティ対策ソフトをインストールすれば安全なので、定期的なフルスキャンは不要である。 ○ 正しい ● 正しくない
8	普段使用しているパソコンを持ち出すことになった際の対処として、推奨されないものはどれか。 ○ 事前に、個人情報や機密情報を含むデータを持っていないことを確認した。 ○ パソコンのログオンパスワードをかけた。 ○ パソコンのハードディスクを暗号化した。 ● 出先で困らないように、パスワードのメモをパソコンに貼りつけた。

3.2 平成 30 年度の教育コンテンツ

平成 30 年度では、前回の事後アンケートをもとに教育コンテンツを検討した。

動画教材は以下の通りに内容を検討し、表４の通りに作成した。

① 本学や他大学のインシデント事例を踏まえて対策例を紹介してほしいという要望を取り入れた。

② 前回の内容を復習するため、ダイジェスト版としてブラッシュアップして再度取り扱うことにした。

③ クラウドサービス利用時の対策及びソーシャルメディアによる情報発信時の対策に関する要望を取り入れた。

④ NII-SOCS の要確認情報の調査時によく見かけられる事例を踏まえて、研究室における私物の持ち込み PC、ルータの設定、及びバックアップについて、取り扱うことにした。

⑤ 別途要望があり、情報セキュリティの範囲外ではあるが、情報資産の適切な利用として利用目的の遵守並びに著作権の尊重について、取り扱うことにした。

⑥ 前回の動画教材は約 23 分であったが、長すぎて受講の負担が大きいとの意見が寄せられたため、約 13 分に短縮した。この短縮によって、説明が不十分になってしまった部分は、ウェブサイトに詳細を掲載し、必要に応じて参照できるようにして補った。

⑦ 教職員向けのｅラーニングが他にも複数あり、受講者の負担が大きいとの意見を考慮して、各教育の実施時期を合わせ、個人情報保護に関する教育とは合同で実施することにした。

確認テストについては、動画教材を視聴しなくても正答できるほど問題が易しすぎるという意見が多かったため、動画教材を視聴していないと容易に正答できないようにレベルを見直し、表５の通りに作成した。

このようにして作成した教育コンテンツについて、今回も情報セキュリティＷＧで審議した。

表４　平成 30 年度動画教材

No.	内容
1	はじめに ・CISO のメッセージ ・詳細はウェブサイトで
2	情報セキュリティインシデントの事例 ・富山大学 ・大阪大学 ・東北大学
3	基本的な情報セキュリティ対策 ・ソフトウェアを最新に保つ ・セキュリティ対策ソフト ・パスワードの取扱い ・騙されないために手口を知る ・持ち出し時の対策 ・インシデント発生時の初動対応
4	クラウドサービス利用時の対策 ・クラウドサービスとは ・主な対策 ・心構え ・アカウント管理 ・公開範囲
5	ソーシャルメディアによる情報発信時の対策 ・ソーシャルメディアの特性を理解する ・慎重に取り扱う
6	情報資産の適切な利用
	・利用目的を遵守する ・著作権侵害行為を行わない
7	研究室での対策 ・私物の持ち込みＰＣ ・ルータ ・バックアップ

表５　平成 30 年度理解度確認テスト（抜粋）

No.	設問・選択肢
3	クラウドサービスとは、ネットワーク経由で、他人のコンピュータにデータを渡して各種サービスを受けることです。ストレージ、翻訳、PDF 編集、日程調整など、様々なサービスがあります。 そこで、クラウドサービス利用時の対策として、適切なものを全て選択してください。 ■ 無名だけれども便利そうな翻訳サービスを見つけたが、2015 年 2 月に翻訳サービスに入力した文章がネット上にそのまま公開されていた事例があり、万が一の可能性があるので、利用しないことにした。 ■ 無料で PDF 編集が行えるサービスを見つけたが、万が一の可能性があるので、個人情報や機密情報を含むファイルを編集しないようにした。 ■ 日程調整サービスは便利だが、万が一の可能性があるので、氏名や会議内容は書き込まないようにした。 □ アカウントのセキュリティオプション（ログイン通知、二段階認証など）が提供されていたが、面倒なので使用しなかった。
4	ソーシャルメディアによる情報発信では、その特性を理解し、慎重に取り扱うことが重要です。それは組織の公式アカウントのみならず、個人アカウントであっても同様です。 それでは、ソーシャルメディアによる情報発信時の対策として、適切なものを全て選択してください。 ■ 発信した情報は、誰にもコントロールできず、完全に削除できないので、常に慎重に吟味し、責任のもてる内容を発信する。 ■ 匿名のつもりでも、個人を特定されてしまうことがあるので、常に慎重に吟味し、

	責任のもてる内容を発信する。 ■ 「東北大学ではなく個人としての発言」と明記していても、社会的問題になれば東北大学の信用を損ねることがあるので、法令を遵守し、他者の人格を尊重する。 □ 職務上知り得た個人情報を発信する。
5	東北大学のネットワークに接続する場合は、例え私物の機器であっても、利用目的を遵守しなければなりません。 それでは、不適切な行為を全て選択してください。 ■ 私的なインターネットゲーム □ 学会出張のための旅行サイトの閲覧 □ 研究室の備品購入のためのショッピングサイトの閲覧 ■ ビットコイン等の仮想通貨の採掘（マイニング）
6	知の創造体として社会に貢献してきた東北大学が著作権を尊重しないことは、大学の存在を否定することと同じです。著作権侵害行為を行った場合は、本人に加えて、法人も責任を負うことになります。 それでは、著作権侵害行為にあたるものを全て選択してください。 ■ 研究・教育などの業務に必要なソフトウェアが高価だったため、海賊版ソフトウェアを入手し、パソコンにインストールして使用した。(海賊版とは、著作権者の許諾を受けずに複製された著作物のこと）" ■ ソフトウェアの購入を申請したところ、予算の都合で数を減らされたが､｢それでも業務上必要だから｣｢どうせチェックしないだろう」と考え、ソフトウェアを必要台数分インストールした。 ■ 漫画の切り抜きをスキャナーで取り込みPDF ファイルにしてインターネットで公開した。 □ 国内の大手家電量販店などの正規販売店で購入したビジネスソフトウェアをインストールして使用した。
7	研究室での情報セキュリティ対策として、適切なものを全て選択してください。 ■ 研究室に持ち込まれた私物パソコンは、ＯＳ・ソフトウェアが最新版にアップデートしていること、本学が提供するセキュリティ対策ソフトでフルスキャンしていること、海賊版ソフト等の不正ソフトがインストールされていないことを確認する。また、初回だけでなく定期的に確認する。 ■ ルータは接続機器のログを保存するように設定する。 ■ 研究データは定期的にバックアップをとる。 □ ＵＳＢ型の外付けハードディスクをパソコンデータのバックアップとして使用する場合は、パソコンに常時接続したままにする。

4 おわりに

本稿では、情報セキュリティ教育の実施にあたって、自組織の情報セキュリティポリシー及び情報システム利用環境の実態に合わせて、非現実的な理想論に終始せず、きちんと実践できる内容の教育コンテンツを内製で作成するための取組みについて紹介した。

他機関において、教育コンテンツのブラッシュアップに寄与できれば幸いである。

参考文献

[1] 独立行政法人情報処理推進機構（IPA)、情報セキュリティ 10 大脅威 2016、P12、独立行政法人情報処理推進機構、2016.

謝辞

情報セキュリティ教育コンテンツの作成にあたり、ご助言をいただいた情報セキュリティWGの皆さまに謹んで感謝の意を表します.