# 医学系の教職員・学生向け情報セキュリティ教育

葭葉 純子, 中村 直毅, 長瀬 祥子 , 伊藤 和哉 ,

高畑 知香, 鈴木 麻里恵, 冨永 悌二

東北大学大学院 医学系研究科・医学部 情報基盤室

yoshiba@med.tohoku.ac.jp

# Information Security Education for Faculty and Students of School of Medicine

Junko Yoshiba, Naoki Nakamura, Sachiko Nagase, Kazuya Ito,

Chika Takahata, Marie Suzuki, Teiji Tominaga

Information Infrastructure Office, School of Medicine, Tohoku University

**概要**

医学系の学生は、患者情報に接する機会が多数あるため、教職員と同様に、個人情報保護や情報漏えいに関して充分な啓発を行う必要がある。そこで、情報基盤室では、平成 20 年度から、学部生、大学院生、教職員向けに個人情報保護や情報セキュリティに関する教育を実施してきた。

情報セキュリティ教育の実施内容は、個人情報保護、情報漏えい事例、情報漏えいを起こさないための情報セキュリティ対策等の項目からなる。さらに、学生には、教育実施後に簡単な選択式テストを実施するとともに、教育内容を理解した上で誓約書に署名することを義務付けている。これまで教育内容を充実させるために、アンケートを実施し、その結果を反映して教育コンテンツを改善してきた。また、理解度を向上させるために、できるだけ身近な事例で解説したり、ウィルス解説動画の活用等も行っている。

平成 28 年度まで教育を継続して実施した結果、平成 20 年の教育開始時と比較すると、個人パソコンでもウィルス対策ソフトが導入され OS がアップデートされている、USB メモリの紛失トラブル報告も聞かなくなるなどの効果が得られている。今後は、東北大学の公式 e-learning システムの活用、警察や企業に講演を依頼して外部講師による最新の情報セキュリティセミナーの開催等を行い、さらに情報セキュリティ啓発活動を進めていきたい。

## 1 はじめに

近年では、多くの人が自分の携帯電話やパソコンを所有しており、簡単にインターネットに接続してウェブサイトの情報を閲覧したり、SNS で情報発信したりできる環境が整っている。また、大学で学習や研究をする上でもインターネットはなくてはならないものとなっている。一方、大規模な個人情報漏えいなどの情報セキュリティに関するニュースは後を絶たず、安易にインターネットを利用することで、誰でも意図せずに情報漏えいの被害者、加害者になりうることが懸念される。

医学系研究科・医学部の学生は、臨床実習等で直接患者様に接する機会や、病院情報システムで患者情報を参照する機会が多数あるため、教職員と同様に個人情報保護や情報漏えいに関して充分な啓発が必要である。そこで、情報基盤室では、平成 20 年から毎年少しずつ内容を改良しながら、学部生・大学院生・教職員向けに個人情報保護、情報セキュリティの教育を実施している。本稿では、情報セキュリティ教育の実施内容、スケジュール、教育内容を充実させるために行った改良点、結果と現在の問題点、今後の進め方について述べる。

## 2 情報セキュリティ教育

### 2.1 実施計画

表 1　平成 28 年度の情報セキュリティ教育実施計画

| 対象者 | | 実施日時 | | | 実施内容 | | | | | 配布書類 | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 実施日 | 実施時間 | 所要時間 | ①個人情報保護・守秘義務 | ②病院情報システム | ③情報セキュリティ<br>④SNS利用上の注意<br>⑤情報システム利用方法<br>⑥電子ジャーナルの適正利用 | ⑦テスト回収不要 | ⑧誓約書記入回収 | 利用手引 | 安全倫理ガイドライン | SNS利用ガイドライン | 誓約書 | テスト |
| 新任教職員 | － | 4/7(木) | 14:00-14:30 | 30分 | ○ | － | ○ | － | － | ○ | － | ○ | － | － |
| 大学院生 | 1年 | 4/8(金) | 13:00－14:00 | 60分 | ○ | － | ○ | － | △<br>(後で回収) | ○ | ○ | ○ | ○ | － |
| | 1年 | 10/3(金) | 10:00－11:00 | 60分 | ○ | － | ○ | － | △<br>(後で回収) | ○ | ○ | ○ | ○ | － |
| 学部生<br>医学科 | 1年 | 5/9(月) | 8:50－10:50 | 130分 | ○ | － | ○ | ○ | ○ | － | － | ○ | ○ | ○ |
| | 2年 | 4/6(水) | 9:10－10:25 | 75分 | ○ | － | ○ | ○ | ○ | － | － | ○ | ○ | ○ |
| | 3年 | 4/5(火) | 10:10－11:10 | 60分 | ○ | － | ○ | ○ | ○ | － | － | ○ | ○ | ○ |
| | 4年 | 4/22(金) | 13:10－14:10 | 60分 | ○ | － | ○ | ○ | ○ | － | － | ○ | ○ | ○ |
| | 5年 | 4/4(月) | 10:55－12:05 | 70分 | ○ | ○ | ○ | ○ | ○ | － | － | ○ | ○ | ○ |
| | 6年 | 4/4(月) | 13:10－14:10 | 60分 | ○ | － | ○ | ○ | ○ | － | － | ○ | ○ | ○ |
| 学部生<br>保健学科 | 1年 | 4/7(木) | 14:00-15:00 | 60分 | ○ | － | ○ | ○ | ○ | － | － | ○ | ○ | ○ |
| | 2年 | 4/8(金) | 9:05－10:05 | 60分 | ○ | － | ○ | ○ | ○ | － | － | ○ | ○ | ○ |
| | 3年 | 4/8(金) | 13:00－13:40 | 40分 | ○ | － | ○ | ○ | ○ | － | － | ○ | ○ | ○ |
| | 4年 | 4/8(金) | 14:30－15:10 | 40分 | ○ | － | ○ | ○ | ○ | － | － | ○ | ○ | ○ |

表 1 は、平成 28 年度の情報セキュリティ教育の実施計画である。教育の対象者は、新任教職員、大学院新入生、学部生全学年としている。実施日時は、基本的に 4 月のオリエンテーション時とし、具体的な日程は、学生向けを教務課、教職員向けを総務課が調整しており、事務部と協力して情報セキュリティ教育を行っている。実施内容は、教職員学生とも基本部分は同じものを使用し、学生に対しては、誓約書の配布と説明、テストの実施を行うなど、対象者によって調整している。また、配布書類として、教職員と大学院生に情報基盤室作成の「情報システム利用手引き」を、大学院生にはさらに、東北大学情報シナジー機構作成の「コンピュータネットワーク安全倫理に関するガイドライン」[1]を、全対象者に医学系研究科広報室作成の「SNS 利用ガイドライン」を配布している。

### 2.2 説明内容

説明資料は、パワーポイントで作成しており、以下の①から⑤の内容からなる。内容の作成にあたっては、IPA の「対策のしおり」[2]を参考にした。

①個人情報保護

・患者情報、個人情報とは

・医師等医療関係者の守秘義務

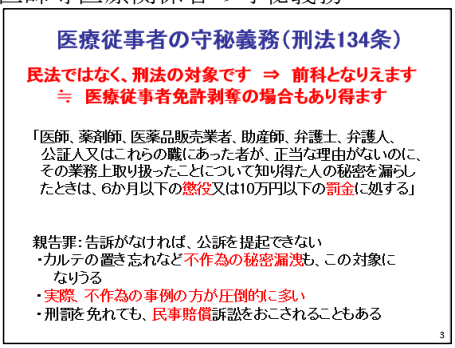


図 1 ①個人情報保護の資料例

②情報漏えい事例

・過去半年以内に起きた病院での個人情報漏えい事例の提示と解説

・情報漏えい後どうなるか（新聞発表･･･）

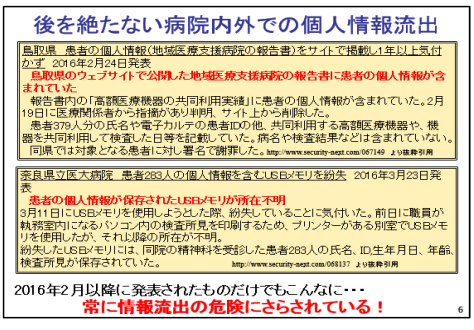


図 2 ②情報漏えい事例の資料例

③情報セキュリティ対策

「情報漏えいを起こさないため」という観点から、情報セキュリティ対策をまとめている。

・見る必要のない情報を見ない、書かない
・廊下、エレベーターで実習内容を話さない
・USB メモリは持ち歩かず、医学部提供のネットワークストレージの使用を推奨
・ウィルス感染対策
・最新のセキュリティ脅威事例の情報提供
・セキュリティ被害事例

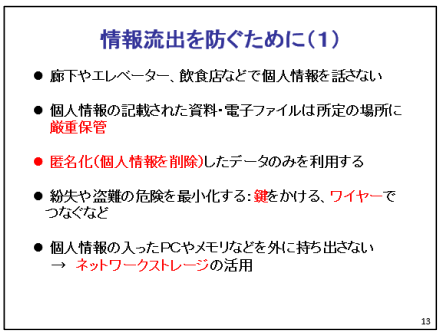


図 3 ③情報セキュリティ対策の資料例

特に、セキュリティ被害事例は、自部局での被害事例や先輩達の失敗事例が記憶に残りやすいため、なるべく身近な事例を提示して説明するようにした。図 4 は、医学部のメールアドレス宛に多数届いた東北大学の管理者を装ったフィッシングメールの事例である。

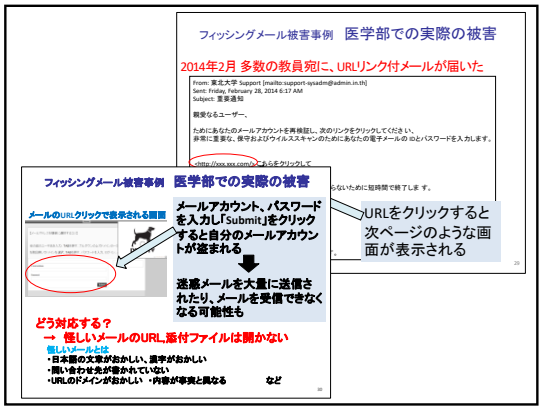


図 4 セキュリティ被害事例

また、パワーポイントの文字と図の説明だけでは、ウィルス感染の仕組みはわかりづらく、説明も聞き飽きてしまうため、その年に流行った攻撃に関する解説動画を活用して、理解しやすい内容にしている。

平成 28 年度は、図 5 の警察庁のランサムウェア説明動画を使用した。過去には、セキュリティメーカー作成の USB メモリで感染するウィルスの解説動画や、スマートフォンを乗っ取るウィルスの解説動画等を活用している。

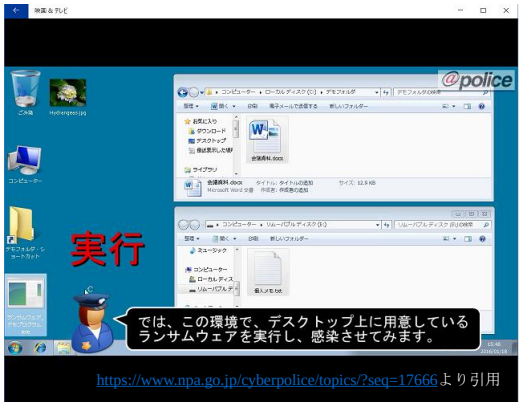


図 5 警察庁のランサムウェア説明動画

④SNS 利用上の注意

・アップロードしてはいけない情報
・ダウンロードしてはいけない情報、著作権
・安易に写真等をアップロードしたことによるトラブル事例


図 6 ④SNS 利用上の注意の資料例

⑤情報システム利用方法

・情報共有用のグループウェアの利用方法
・ネットワークストレージ、無線 LAN、VPN 接続、メール取得方法 など

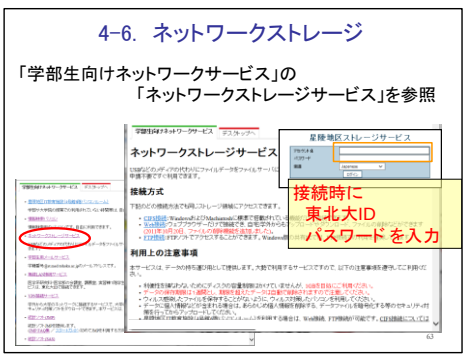


図 7 ⑤情報システム利用方法の資料例

### 2.3 確認テスト（学部生対象）

全学部生に対し、毎年、教育を実施しているため、上級生ほど私語が多く説明を聞かない傾向にある。そこで、学部生には最後にテストを実施することをあらかじめ伝え、なるべく聞かせるようにするとともに、テストの答え合わせの際に解説をすることで、説明内容の理解が深まるようにしている。

図 8 は、平成 28 年度のテストと解説資料の抜粋である。テストは、簡単な選択式問題 6 問程度からなり、毎年、少しずつその年度の説明内容に合わせて変更している。

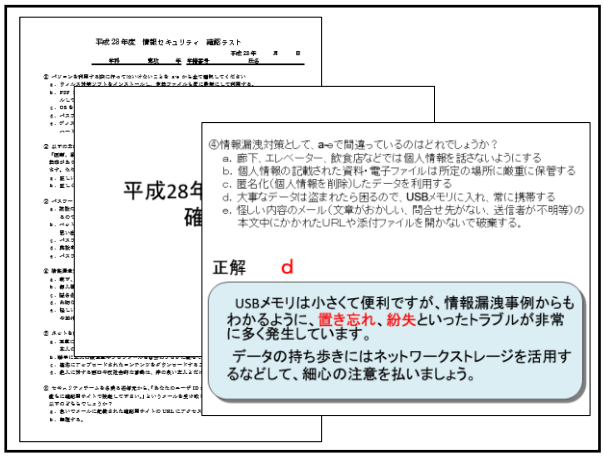


図 8　テストと解説資料

### 2.4 誓約書

大学院生、学部生には、教育実施後に誓約書を配布し、内容を理解した上で署名・捺印してもらい教務課で保管している。誓約書の細かな内容については、大学院、学部（医学科、保健学科）の各教務委員会で検討し決定している。図 9 に誓約書のイメージを示す。

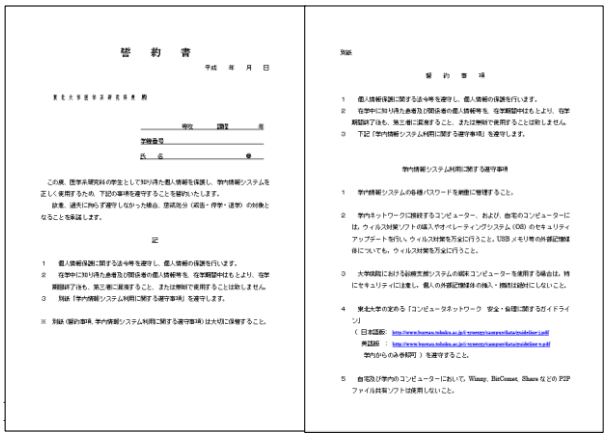


図 9　大学院生の誓約書イメージ

## 3 教育内容の充実

情報セキュリティ教育の内容をより効果的に理解してもらうために、アンケートを実施しアンケート記入内容に関し結果の反映を行った。

具体的には、平成 22 年度の教育の際に学部生を対象として、図 10 の簡単なレポートの記入を依頼した。対象者は、医学科 2 年から 6 年生、保健学科 1 年から 4 年生の約 1,200 名である。

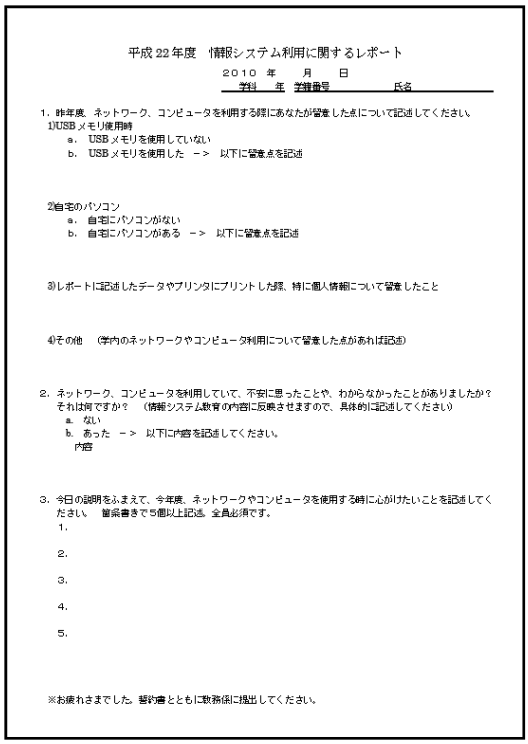


図 10 情報システム利用に関するレポート

このレポートの「②ネットワーク、コンピュータを利用していて不安に思ったこと、わからなかったこと」に関し、「あった」と記入したのは、1,200 人中約 200 人であった。この「不安に思ったこと、わからなかったこと」に記入された内容を集計しまとめた結果の一部を表 2 に示す。

表 2　レポート集計結果抜粋

| 分類 | 記入内容 | 記入者数 | 記入内容に対する回答 |
|---|---|---|---|
| セキュリティ対策について | どこまでウィルス対策したら良いのか？ウィルス対策ソフトでどこまで防げるのか？ | 13 | 残念ながらこれを行えば絶対大丈夫というものはありませんが、<br>以下の対策を行ってください。<br>1. ウィルス対策<br>①OSは最新の状態に<br>②ウィルス対策ソフトをインストールする<br>③ウィルス対策ソフトの定義ファイルは最新にする<br>④最低、週1回は全ファイルスキャンする<br>->ウィルス対策ソフトを入れていても最新のウィルス（定義ファイルが対応していないウィルス）には感染してしまうことがあるため、週1回全ファイルスキャンしてください。<br>2. それでもウィルス感染した場合への対処<br>①データのバックアップをとる<br>->ウィルスを駆除できない場合は、クリーンインストールした後、バックアップデータから復旧することになります。 |
| | ウィルスに感染してしまったらどうしたら良いのか？ | 3 | ウィルス対策ソフトで駆除できない場合は、HP等でウィルス対策方法を調べてそれに従ってウィルスを削除してください。それが無理な場合は、パソコンを初期状態に（クリーンインストール）し、バックアップデータから復旧してください。 |
| | ウィルス対策がしっかりできるか不安 | 7 | 以下の対策を行ってください。<br>1. ウィルス対策<br>①OSは最新の状態に<br>②ウィルス対策ソフトをインストールする<br>③ウィルス対策ソフトの定義ファイルは最新にする<br>④最低、週1回は全ファイルスキャンする<br>->ウィルス対策ソフトを入れていても最新のウィルス（定義ファイルが対応していないウィルス）には感染してしまうことがあるため、週1回全ファイルスキャンしてください。<br><br>2. それでもウィルス感染した場合への対処 |
| | その他 | 32 | ー |
| | 小計 | 55 | ー |
| ウィルス対策ソフトについて | ウィルス対策ソフトインストール方法、更新方法がわからない | 6 | 大学で提供しているウィルス対策ソフトをインストール場合は、EASTの学生ネットワークサービスメニューからF-secureなどのリンク先よりダウンロードできます。その際は自分のパソコンを大学に持ってきて無線LANに接続してダウンロードするか、または、自宅からVPN接続してダウンロードしてください。ダウンロード後の操作は、マニュアルに従ってください。<br>ウィルス対策ソフトをインストールすると標準で、定義ファイルを自動更新、リアルタイム検索等の設定が有効になっています。さらに、最低、週1回は全ファイルスキャンをするように設定してください。 |
| | どんなウィルス対策ソフトを使えば良いのか？ | 5 | どのソフトが一番良いというのはありません。既にウィルス対策ソフトを利用している場合は、そのソフトを利用してください。検討中の場合は、大学で提供しているソフトを使ってみてはいかがでしょうか。 |
| | ウィルスバスターなどのウィルス対策ソフトを入れていれば大丈夫なのか？ | 1 | ウィルス対策ソフトを入れていても、最新のウィルス（定義ファイルが対応していないもの）には、感染していまいます。最低、週に1回は、全ファイルスキャンを行って、ウィルスの駆除等を行ってください。ウィルス対策ソフトで駆除できないウィルスの場合は、該当するホームページのウィルス対応方法に従って作業をしてください。 |
| | その他 | 10 | ー |
| | 小計 | 22 | ー |
| OSの更新について | OSの更新方法がわからない | 3 | Windowsの場合は、Windows Updateの設定で「更新プログラムを自動的にアップデートする」にしておけば、自動的に最新にできます。手動でWindows Updateを実行する場合は、IEのメニューより「Windows Update」を選択してください。 |
| | その他 | 2 | ー |
| | 小計 | 5 | ー |
| 個人情報保護について | 個人情報を保護するために何を心がけるべきかメンタルな注意も教えてほしい | 1 | 知る必要の無い情報は知ろうとしないこと。個人情報に関係あることは話さない・書かないことを心がけて下さい。 |
| | レポートを書く際にどこまで情報を伏せるべきか | 1 | 個人が特定されないように注意する必要があります。不安な場合には、担当の先生に相談してください。 |
| | 小計 | 2 | ー |

表 2 のレポート集計結果では、

・ウィルス対策ソフトでどこまで防げるのかわからない
・どのウィルス対策ソフトを使えばいいのか
・ウィルス対策ソフトのインストール方法、更新方法がわからない
・コンピュータ用語がわからない

等の意見が多くみられた。また、教育の内容に関しては、

・色々複雑すぎてわからない
・情報が多いのでどれが正しいかわかりづらい
・なんとなくわかったが具体的に何をして良いかわかりづらい

という意見も見られた。

そこで、表 2 の一番右側に「記入内容に関する回答」を記入し、グループウェア上に掲載して学生に周知することとした。

また、教育への「情報が多い」「具体的に何をすれば良いかわかりづらい」という意見に対しては、翌年からの教育の資料を「情報セキュリティ対策として最低限行うことを各自がすぐに対応できる具体的な作業内容で提示」するように改良した。

例えば、ウィルス対策ソフトの導入では、大学で提供するウィルス対策ソフトを、グループウェア上のどのページのどの項目からリンクしていけばインストールできるか、OS のアップデートは、画面上のどこで何を設定すれば良いかをそれぞれ画面で説明する。また、ウィルス対策を行っても感染する可能性はあるため、「重要なデータは必ずバックアップ」することが大切であることも伝えている。

## 4 結果と現在の問題点

具体的な数値では出せていないが、平成 20 年に情報セキュリティ教育を開始した頃と比較すると、以下の改善が見られるようになった。

・以前は、OS がアップデートされておらずウィルス対策ソフトも入っていない個人パソコンをしばしば見かけたが、最近は、OS のアップデートが徹底され、ウィルス対策ソフトもインストールされて定義ファイルも更新されている。

・USB の代わりにネットワークストレージの使用が浸透したため、USB メモリを紛失したことによるトラブル報告を聞かなくなった。
・安易な考えで SNS を使って不適切な情報　発信をしてしまったという報告を聞かなくなった。

現在は、学生のウィルス感染や SNS での不適切な情報発信等の報告はほぼなくなっているが、教職員宛のフィッシングメールが多数届く、教職員がメールアカウントをハッキングされスパム発信されてしまうといった被害が増えてきている。

図 11 に、2014 年から 2016 年 10 月までの医学系研究科のメールサーバでのこれまでのスパム発信対応件数を示す。管理対象のメールアカウントは約 3,000 アカウントである。2014 年の 11 月、12 月にフィッシングメールが多数届き、被害数が多くなってしまった。その際の対応として、メールパスワードの変更依頼、パスワードチェックの強化、グループウェアを利用したフィッシングメールへの注意喚起通知などを行うことで被害がやや収束した。しかし、2016 年に入り、またスパムメール発信の被害が増えてきている。

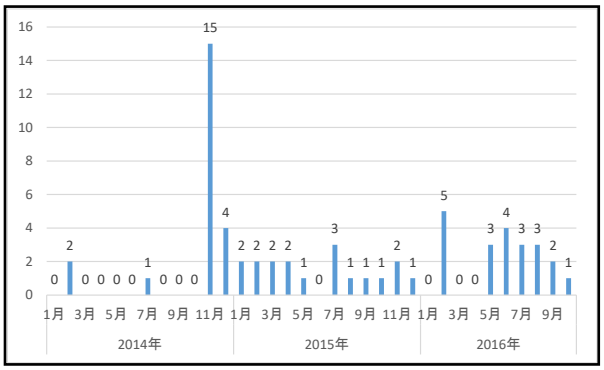


図 11　スパム発信対応状況

## 5 今後の進め方

学部生は毎年全学年を、大学院生は新入生全員を対象としているため、学生の在籍者には、ほぼ全員に教育を実施できている。しかし、教職員は、新任者のみを対象として毎年 4 月に 1 回だけ実施しているため、5 月以降の採用者や、以前からの在籍者には、教育を実施できていない。そこで、東北大学公式 e-learning システム（以下、ISTU と記載）を使用して教育用コンテンツを作成し、教職員の在籍者には必ず 1 回受講してもらうなどの対策を検討中である。病院側では既に ISTU 用の個人情報保護の教育コンテンツを準備しているため、病院と共同して情報セキュリティ対策コンテンツを追加作成し、不審なメールの URL に入力しない、添付ファイルを開かない等も含めたメールアカウントのハッキング対策も行っていきたい。なお、教育と平行してメールサーバ側でもスパムメールを発信させないための認証方法の変更を検討中である。

さらに、警察や企業に講演を依頼してセキュリティセミナーを開催し、内部講師だけでなく、外部の講師による最新の情報セキュリティ啓発活動も進めていきたい。

## 6 おわりに

平成 20 年より、毎年、学生や教職員対象に個人情報保護、情報漏えい対策を中心とした情報セキュリティ教育を行ってきた。情報を漏えいさせないための対策方法を継続して伝えてきたことで、成果が得られてきている。しかし、情報セキュリティの脅威は日々変化し、次々に新しい攻撃が行われるため、その都度、グループウェアからの緊急通知や ISTU での教育コンテンツを活用した啓発を実施し、情報セキュリティ対策を行っていきたい。

## 参考文献

[1] 東北大学情報シナジー機構、情報セキュリティポリシー・情報システム関連規程、コンピュータネットワーク安全倫理に関するガイドライン、2016.（東北大学学内限定）

[2] 情報処理推進機構 IPA、情報セキュリティ対策のしおり、https://www.ipa.go.jp/security/antivirus/shiori.html 、2014 年.