※本稿は大学ICT推進協議会での口頭発表内容
（平成30年11月時点）

弘前大学における標的型攻撃メール対応訓練とフィッシング対策

葛西 真寿 [1),2)], 須藤 勝弘 [3)], 小倉 広実 [3)], 竹内 淑怜 [3)]

1) 弘前大学 大学院理工学研究科
2) 弘前大学 総合情報処理センター
3) 弘前大学 附属図書館 情報基盤グループ

cnc-director@hirosaki-u.ac.jp

The trainings against the targeted attack e-mails and anti-phishing measures in Hirosaki University

Masumi Kasai[1),2)], Katsuhiro Suto[3)], Hiromi Ogura[3)], Sumire Takeuchi[3)]

1) Graduate School of Science and Technology, Hirosaki Univ.
2) Computing and Networking Center, Hirosaki Univ.
3) Hirosaki University Library

概要

本稿では，本学が策定した情報セキュリティ対策基本計画に基づいて平成 28 年度と 29 年度に実施した標的型攻撃メール対応訓練について事例紹介する。また，平成 30 年 6 月に発生したフィッシングメールによる情報漏えいを受けて本学が実施した対策や，有効性が期待されるフィッシング対策についてもあわせて紹介する。

1 はじめに

昨今多発している情報セキュリティインシデントを受け，中長期的な視点を持って情報セキュリティ対策の強化を組織的かつ計画的に実施するため，本学は平成 28 年度を起点とした弘前大学情報セキュリティ対策基本計画を策定し，学長了承のもと全学情報総括責任者（企画担当理事）の指示により全学体制で実施している。本稿では，この基本計画に基づいて平成 28 年度と 29 年度に実施した標的型攻撃メール対応訓練について事例紹介する。

また，平成 30 年 6 月に発生したフィッシングメールによる情報漏えいを受けて本学が実施した対策や，有効性が期待されるフィッシング対策についてもあわせて紹介する。

2 平成 28 年度標的型攻撃メール対応訓練

平成 28 年度の標的型攻撃メール対応訓練は，本学役員並びに課長級以上の幹部職員から抽出した 105 名を対象として実施した。訓練メールの配信は，平成 29 年 2 月 27 日と 3 月 6 日の 2 回行った。第 1 回及び第 2 回の訓練メール本文は以下の通りである。

件名：	アンケートに関するご協力のお願い
送信アドレス：	理事（企画担当）Y澤 <pcsecurity@office-　.jp>

本文

職員の皆様

日々の業務お疲れ様です。
昨今、企業におけるウイルス感染等による情報漏えい事件が
度々報道されておりますが、本学においてもセキュリティ対策
の一環としてウイルス対策ソフトの運用、並びに個人PCの
セキュリティアップデートに関する状況についてアンケート
調査を行います。

以下の「アンケート票」に必要事項をご記入の上、明日16時
までに各自回答ください。なお、本件に関する問合せは、
情報システム担当へ行わないようご注意下さい。

お忙しいところ大変恐縮ですが、ご協力をお願いいたします。

http://ww15.office-*.jp/urcvb/b.cgi?*********

図 1. 平成 28 年度第 1 回訓練メール本文

件名：	緊急アンケートのお願い
送信アドレス：	総合情報処理センター <syusakei@jou　.jp>

本文

イントラシステムの使い勝手についてアンケート調査を
行います。

イントラシステムにはWebインタフェースをはじめとして、
いくつかのサブシステムがありますが、どれも使いにくい
という声があります。

http://ww15.office-*.jp/urcvb/b.cgi?*********

そこで、業務効率改善その他の目的のために、広く意見
を収集し、改善を図ることになりました。つきましては、
アンケートに至急ご回答ください。

情報システム担当メンバーにつきましては、他部署より
早めの集計が必要なため、本日中に回答をお願いします。

総合情報処理センター　葛西

図 2. 平成 28 年度第 2 回訓練メール本文

訓練結果の概要を紹介する前に注意しておくが，平成 28 年度の訓練は，受注した業者がいうところの（難易度が高く，ひっかかりやすい）「レベル 3」模擬攻撃メールであった。ご本人の快諾を得て実在する理事の実名で送信したことや，一斉送信メールによる事前予告なく送信したこともあり，受信した役員・幹部職員が模擬攻撃メールと思わず，非常に高い関心を持って受け止められ，文中のリンク先についても極めて迅速なクリックが行われたため，「開封率」（本文中の不審リンクをクリックする率）が高くなった。

3　平成 28 年度訓練結果概要

第 1 回の訓練メールについては，実在する理事の実名で送信したこともあり，受信した役員・幹部職員の多くから非常に高い関心を持って受け止められたため，比較的多くの受信者が本文中のリンク先をクリックして開封してしまった。冷静に見れば，送信者のアドレスが弘大メールアドレス（***@hirosaki-u.ac.jp）ではないことから，不審メールであることは判断可能である。しかし，役員が使用しているスマートフォンのメールアプリでは，デフォルトでは送信者のメールアドレスまで確認できないため，実在の理事からのメールと信じたまま，本文中のリンクをクリックしたとの報告が事後にあったように，実在の理事の表示名に反応してクリックしてしまうことが開封率を上げた要因と考えられる。

第 2 回の訓練メールでは開封率は大きく下がったが，第 1 回の訓練メールの送信者である理事に比べれば役職的に下位である総合情報処理センター長の実名で送信したためなのか，2 回目であることによる訓練の効果なのか，判断が難しい。

訓練で重要視したのは開封率そのものよりも，不審メールを受信した際の対応状況である。不審メールを受信した旨を弘前大学 CSIRT に報告した件数は，第 1 回，第 2 回とも少なかった。一つの理由として，訓練メール受信者が役員・幹部職員だということがあげられる。通常業務では報告を受ける側であることも留意する必要があるかもしれない。

4　平成 29 年度標的型攻撃メール対応訓練

平成 29 年度の訓練は，本学職員からランダムに抽出した 1000 アカウントに対して，平成 30 年 1 月 30 日および 2 月 14 日の 2 回にわたって模擬攻撃メールを送信することで実施した。今回は 1000 アカウント対象の大規模な訓練であるため，一斉送信メール等で事前に十分な訓練予告の周知を行った上で実施した。訓練メール本文を以下に示す。

Subject: 震災時の行動マニュアルについて
Date: Tue, 30 Jan 2018 10:37:40 +0900
From: 危機管理担当 <info_＊＊＊＊@yah00co.jp>
Reply-To: kunren_＊＊＊＊@yah00co.jp
To: ＊＊＊＊@hirosaki-u.ac.jp

東日本大震災の経験を踏まえ、大規模地震が発生した場合の行動マニュアルを整備しました。

内容を確認いただき、適切に対応いただくようお願いします。

http://www1.***.co.jp/cgi-bin/check.cgi?code..

以上

図 3. 平成 29 年度第 1 回訓練メール本文

Subject: ホームページのリニューアルについて
Date: Wed, 14 Feb 2018 10:13:06 +0900
From: 営業担当 <support_＊＊＊＊@yah00co.jp>
Reply-To: kunren_＊＊＊＊@yah00co.jp
To: ＊＊＊＊@hirosaki-u.ac.jp

各位
お疲れ様です。
このたび営業活動の一環として、ホームページをリニューアルしました。
なかなかの出来栄えです。取引先やお客さまにご紹介するなど、営業活動に活用してください。

http://www1.***.co.jp/cgi-bin/check.cgi?code=..

図 4. 平成 29 年度第 2 回訓練メール本文

平成 28 年度訓練と比較すれば，平成 29 年度の模擬攻撃メールは「レベル 1」相当であり，実名を使用せず，明らかに怪しそうな文面とした。またメール形式をテキストメールとし，リンク URL が明らかに不審とわかるようにした。そのために，デフォルトでは弘大メールが迷惑メールと判断してしまい，訓練にならないため，ホワイトリストに入れて迷惑メールフォルダに落ちないようにする必要があった。

5　平成 29 年度訓練結果概要

模擬攻撃メール本文中のリンクをクリックして開封した受信者の割合は，第 1 回が 14.5%，第 2 回が 4.0% であり，2 回目の不審 URL のクリック率が減少したことがわかり，模擬攻撃メールを 2 回受信したことによる一定の抑止効果が見られる。また，不審メール報告者の割合は，第 1 回が 17.9%，第 2 回が 15.3% と，どちらも一定の不審メール報告があり，しかも 2 回目もそれほど低下していない。理由の一つとしては，訓練開始と終了を一斉送信で十分に周知したこと，不

審メール報告者全員に対して報告に対する謝辞と不審メールを受信した際の対応策を含む回答メールを送信したことで，訓練に対する参加意識が低下しなかったことが考えられる。

6 不正転送による情報漏えいと対策

平成 30 年，本学職員に対してフィッシングメールの送信があり，本学が利用している電子メールサービスのログイン画面に似せた偽サイトへの誘導により，パスワードが詐取され，12 名の職員のアカウントに対して，本人になりすまして不正な転送設定が行われるという事態が発生した。これらのメールアドレスに届いたメールが不正に外部へ転送され，メールアドレス情報を含む情報漏えいが発生した [1]。

本学 CSIRT および総合情報処理センターでは，事態把握後ただちに当該フィッシングメール受信者全員に対して，不正転送設定の有無を確認後，不正に設定された転送先については削除し，当該メール受信者全員のパスワード変更をおこなった。

さらに，本学の全ての構成員に対して，学外へのメール転送設定を禁止し，全ての学外へのメール転送設定を削除した。（ただし，スマートフォンではない携帯電話のみを利用している学生の事情を考慮し，学生に対しては，携帯電話 3 社へのキャリアメールへの転送に限り転送を許可する例外措置を設けている。）禁止措置後も学外へのメール転送設定を行った場合には管理者へアラートがあがり，その都度利用者への事前通告なしに管理者が転送設定を削除している。

7 フィッシング対策

以上の措置で，不正転送設定による情報漏えいを防止しているが，フィッシングメールによってパスワードが詐取されれば，本人になりすましてログインされて（不正転送設定以外の方法で）メール等の不正な閲覧が可能になってしまう。

訓練や教育啓蒙によってフィッシングメールによるパスワード詐取被害は減少させることはできてもゼロにすることは現実的には不可能である以上，パスワードが詐取されることを前提とし，たとえパスワードを詐取されても不正なアクセスを阻止できるようなフィッシング対策が必要である。

本講演では，有効性が期待できるフィッシング対策のうちの以下の項目について，概要を紹介する。

- 多要素認証
- 高度なフィッシング脅威防御オプション
- 不正アクセス保護機能を含む包括契約

8 おわりに

セキュリティ強化，利用者の利便性確保，経費節減，これら 3 点はどれも重要な要素であるが，実際にはこれらの 3 点を「全て同時に」満たすフィッシング対策を立案することは極めて困難な作業である。たとえば，セキュリティ強化は当然すべきこととして，利用者の利便性も確保するとなると，経費節減は困難であり一定の支出は避けられない。また，経費節減をはかりながらセキュリティ強化を推進するとなれば利用者の利便性の確保が困難になる。

情報セキュリティ強化対策の立案については経営判断が必須であり，実施にあたっては全学的な合意形成が肝要と考える。

参考文献

[1]【お詫び】フィッシングメールによる個人情報の漏えいについて｜弘前大学
https://www.hirosaki-u.ac.jp/35460.html
に掲載の報道発表資料。