学術情報処理研究
No.18 2014 pp.3–15

フィッシング攻撃に対する組織的対策と効果の考察

A Study on the Effect on Phishing Attack with Systemic Measure

伊藤　史人†，高見澤　秀幸‡
Fumihito, ITO†, Hideyuki Takamizawa‡

fumi@ecs.shimane-u.ac.jp, h.takamizawa@cio.hit-u.ac.jp

†島根大学総合理工学研究科
‡一橋大学情報基盤センター

† Shimane University Interdisciplinary Faculty of Science and Engineering
‡ Center of Information and Communication Technology, Hitotsubashi University

概要

組織に対するフィッシング攻撃は年々脅威を増している．大学組織においても例外ではなく，その対策は必須であると考えられる．すべての攻撃を防ぐことは不可能であるが，予防接種的訓練によりそのリスクを低減させることは可能である．本研究は，組織の構成員に対して擬似フィッシング攻撃を行いその予防的効果をあげることを目的としており，合わせて構成員のセキュリティ意識向上も狙って行ったものである．擬似フィッシング攻撃訓練は，一橋大学の教職員約 600 名に対してそれぞれ 2 回実施した．その結果，過去に訓練を行ったグループとそうでないグループではフィッシング攻撃に対する有意な防衛力の差が確認できた．本論文では，実施の方法と結果を示し，偽装サイトのログイン情報やアンケート調査等から訓練の効果を考察した．

キーワード

フィッシング攻撃，標的型攻撃，セキュリティ対策，予防接種的訓練

1. はじめに

情報通信技術の急速な進歩や普及により，インターネットを利用したサイバー攻撃の脅威は年々増している．インターネット上に実現されたサービスの利便性が向上する一方で，悪意のある攻撃者の手口も多様化・巧妙化している．特に，大量の個人情報を収容しているシステムで，情報窃取を目的としたサイバー攻撃が成功するとその被害は甚大なものとなる．

近年，とりわけ政府機関や特定の企業を狙い撃ちする標的型攻撃や偽 Web サイトへ誘導することで情報や金銭を窃取するフィッシング攻撃と呼ばれる手法が横行している．大学組織においてもこれらの攻撃を想定した対策が必要となっているのは明らかである[1][2] ．

一般に，フィッシング攻撃は，金融機関（銀行やクレジットカード会社）等を装った電子メールを送り，住所・氏名・銀行口座番号・クレジットカード番号等の個人情報を詐取する行為のことをいう[3]．代表的な手口として

は，攻撃対象者に金融機関等のログインサイトを偽装したサイトの URL をメールで送りつけ，偽装ログインサイトに誘導し，ログイン情報を入力させることでパスワードを含むアカウント情報を窃取するものである．個々のパスワードは各システムやサービスで共用している場合が多いと思われ，パスワードがひとつ窃取されることで他システム等への不正ログインの危険性が一層高まる．一般的なインターネット利用者においては，9 割以上が複数のサイトで ID やパスワードを併用しているとの報告があり[4]，不正ログイン発生時の被害拡大が懸念される．大学においても他組織と同様に，メールシステムはもちろんのこと，会計システムや人事給与システム等の基幹システムはネットワーク上で運用されている．パスワードの共通利用（使い回し）は，フィッシング攻撃が行われた際に被害を拡大させる大きな要因になる．

フィッシング攻撃対策の困難な点は，システム的な対策が極めて難しい点に尽きる．マルウェアについては専用アプライアンスや対策ソフトウェアにより効果が期待できるが，フィッシング攻撃や標的型攻撃等についてはシステム的なセキュリティ対策のみでは十分な効果が得られない．これらが「人」への攻撃である以上，「人」への対策が不十分である場合のリスクは極めて大きいものとなる．これは標的型攻撃メールを含むソーシャルエンジニアリング全般に当てはまる．

そこで，一橋大学（以下，本学）では，これらのサイバー攻撃への対策として，擬似サイバー攻撃により予防接種的効果をねらった擬似フィッシング攻撃訓練を実施した．過去の実際の攻撃事例を参考にして，より本物に近い擬似攻撃とした．教職員を対象に実務業務の中で実際にフィッシング攻撃を体験させた．その体験を組織および個人に予防接種のように作用させ，フィッシング攻撃に対する「抗体」をもたらすことを期待したものである. なお, 対象は本学における常勤教職員の全員となる，教員 400 名および事務職員 200 名である．

予防接種的訓練は被験者となった教職員に情報セキュリティに対する意識の変化をもたらし，フィッシング攻撃について現実的な脅威として捉えられるようになった．本論文では，フィッシング攻撃訓練の実施経緯を含め訓練の方法と結果を示し，偽装サイトのログイン情報や被験者のアンケート結果等から予防接種的訓練の効果を考察した．

2. 背景と目的

フィッシング攻撃により学生の成績情報や個人情報等が窃取された場合，個人の損害は当然ながら，大学の信用は大きく低下する．その結果，大学運営に致命的な影響を与えかねない．

フィッシング攻撃への防衛力を高めるためには，組織として「人」への対策が必須である[5]．そこで，標的型メール攻撃の対策として有効であった予防接種的訓練をフィッシング攻撃に応用し，大学組織の情報セキュリティの底上げを目的として実施する．

2.1. 大学におけるサイバー攻撃対策の難しさ

大学におけるサイバー攻撃への防衛力は，一部の私立大学や新設大学を除いて，大手企業や中央省庁に比べると脆弱であると言わざるを得ない．未だに各部局で利用するシステムが一元管理されていない例が多いことからもわかる．縦割りのシステム導入が行われ続けているのは大学だけではないが，同規模組織と比べてその傾向が強い．サイバー攻撃対策を実施する上でシステム統合が不十分な場合，システム毎に対策を練らなければならず組織にとって大きな負担になる．本学の場合，学務系システムであれば複数のシステムで学生の個人情報（住所等）を保存している．つまり，システム統合すれば情報漏洩の危険箇所を減らせるのと同時に，集中的にセキュリティ対策を施すことも可能である．なお，地方自治体においてもシステム統合が不十分であり，一元管理によるセキュリティの確保が命題のひとつとなっている[6].

大学組織の特性として，教員組織に対しては研究環境の不可侵を理由に厳しいネットワーク制限が実施できないことも理由に挙げられるだろう．さらには，教員個人では個人用 PC を多用している傾向があるため，ウィルス対策ソフトや OS のセキュリティパッチの管理が不十分である．そのような環境で学生の成績情報や個人情報を管理していることもあり，サイバー攻撃時の潜在的なリスクを大きく高めている．さらに，情報リテラシーの低い教員も少なくないと思われ，情報セキュリティの観点からは危機的な状況であると考えられる．企業等であれば，業務における個人用 PC の利用が制限している例も多いが大学教員に対しての徹底は難しいだろう．

事務職員については教員に比べれば業務で利用するソフトウェアやシステムを限定しやすいことや，業務システムにおいては導入時に一定のセキュリティ対策がなされている場合が多く，全体として一定程度の情報セキュリティ対策がなされていると考えられる．本学の場合，ウィルス対策ソフトの定義ファイル一括更新やドメイン等による PC 管理がさており，教員組織に比べるとシステム的なリスクは少ない．

ただし，情報セキュリティの意識は教員同様に高いとは言えない状況にある．これらの現状は大学組織全体のセキュリティレベルの低下をもたらし，サイバー攻撃へ

のリスクを高める．FD や掲示等の啓蒙活動ではサイバー攻撃への備えは不完全にならざるを得ない．

2.2. 本学におけるサイバー攻撃への予防的対策

本学では，ファイアウォールをはじめ，検疫システムや事務用 PC のドメイン管理，ウィルス対策ソフトの定義ファイルの一元管理等によりセキュリティ対策を実施している．

しかし，近年のサイバー攻撃は，これらシステム的なセキュリティ対策を中心とした仕組みでは対処しきれない[6]．フィッシング攻撃や標的型攻撃を代表とするソーシャルエンジニアリングはまさにその例である．これらは，「人」への攻撃であり，構成員の情報セキュリティのスキルがそのまま組織の防衛力に反映される[8]．

そこで，本学では，平成 23 年度と 24 年度に事務職員 200 名を対象とした「標的型攻撃メール予防接種訓練」を実施した[1] [8]．これは，不審なメールを識別する能力を養うために，本学情報基盤センターで作成した擬似ウィルスの添付ファイルが付いた擬似標的型攻撃メールを事務職員に送付するものであった．添付ファイルを開封するかどうかの訓練であり，被験者が情報セキュリティについての知識が十分であり，メールの内容等に不信感を感じることができれば添付メールを開かない．メールが不審なものであることを判別するヒントとしては，差出人メールドメインやメール本文等であった．

表 1 職員への擬似攻撃メール例（平成 23 年度）

Subject	事業継続計画の定期見直し
From	危機管理・災害対策本部 <drc@jigyokeizoku. jp>
Message	一斉メール：危機管理・災害対策本部です. 2011 年 3 月 11 日に発生した東北地方太平洋沖地震では，計画停電や公共交通機関の大幅な乱れにより出勤が困難な状況となりました. つきましては，災害発生時の緊急対応方法について事業継続計画の見直しを行うこととしましたので，添付ファイルの指示に従って現状の調査にご協力をお願いします. 現状調査の項目には，各自の通勤経路(災害時の帰宅経路含む) の項目もありますので，全員の回答が必要です．よろしくお願いします. 一斉メール：危機管理・災害対策本部
Attach	事業継続計画現状確認シート 3. doc

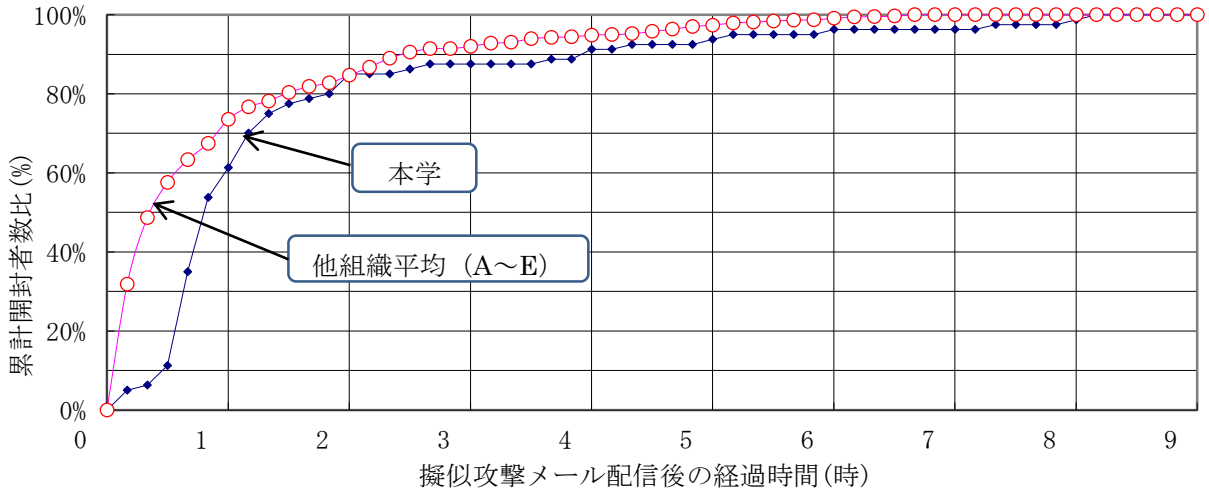


図 1　時系列開封状況（平成 23 年度）

表 2　各開封パターンによる開封率（平成 23 年度）

	被験者数	第 1 回 開封者	第 2 回 開封者	両回 開封者	第 1 回のみ 開封者	第 2 回のみ 開封者	非開封者	開封 減少率
本　学	200	80 40.0%	57 28.5%	34 17.0%	46 23.0%	23 11.5%	97 48.5%)	28.8%
他組織 A	2,927	623 21.3%	253 8.6%	80 2.7%	543 18.6%	173 5.9%	2,131 72.8%)	59.4%
他組織 B	500	102 20.4%	21 4.2%	8 1.6%	94 18.8%	13 2.6%	385 77.0%	79.4%
他組織 C	438	125 28.5%	19 4.3%	10 2.3%	115 26.3%	9 2.1%	304 69.4%	84.8%
他組織 D	200	66 33.0%	55 27.5%	22 11.0%	44 22.0%	33 16.5%	101 50.5%	16.7%
他組織 E	110	52 47.3%	25 22.7%	9 8.2%	43 39.1%	16 14.5%	42 38.2%	51.9%

表 3　被験者の感想（平成 23 年度）

No.	感　想[*1]
1	添付ファイル以外にも偽装リンク先等を掲載し，部署ごとに違うリンク先が掲載されたメールを送り何回，アクセスがあったか集計するとより，客観的なデータが取れて良いのではないか．　個人情報等を流失しないためにも定期的に IT セキュリティ予防接種があると職員の意識も高まり良いのではと感じました．
2	ドッキリみたいで面白かったです．二回目は予防接種だと気づきましたが，ついつい添付ファイルの内容を見てしまいました．
3	擬似攻撃メール配信から数時間後に，システム管理者から訓練を実施した旨がメールで報告されたが，当該メール・添付ファイルにも不審な要素があり，電話による確認作業を要するなど，混乱が続いた．
4	メールアドレスまで慎重に見るようになったので良かったと思う．
5	特にまだ入ったばかりで，上記の部分について把握しておりませんので今後，見解を深めていければと存じます．
6	今回の訓練の経験を踏まえ，少しは送信相手を確認するようになった．
7	送付されてきたメールアドレスをもう少し注意していれば，ひょっとしたら回避できていたかもしれません．2 回目は，その教訓が生きていたと思います．自分は，絶対大丈夫だと思っていましたから，少しショックでした．もう少し，メールそのものを疑って，注意深く確認するべきであると思い知らされました．どうもありがとうございました．
8	送信者を学外者の知られていない人物の名前にして試してみてはいかが？
9	1 回目の擬似攻撃メールの添付を開いて，失敗した！と思ったのですが，2 回目も同様にひっかかってしまいました．今後はメールを開くときに，注意深くしなければいけないと思いました．
10	メールに対する意識が変わりました．時々，訓練し意識しながらメールを使うようになる良い機会と思います．
11	不正メールへの対応について，各人の意識向上がはかれるので，重要なイベントだと思います．ですが，騙すことが目的ではないので，メールの内容が本務に限りなく近いと，狼少年のたとえのような状況となる場合もあるので，注意が必要とは思います．
12	擬似攻撃メールの訓練とのことだったので送信者名を確認してから添付も開いたが，通常は開かないと思われる．しかし，送信者名を騙られた場合はアウトだったと思うので反省すると当時に，その場合の見分け方等，予防策を教えてほしいと感じた．

被験者には標的型メール攻撃を実際に体験することで理解を深めてもらい，本物の攻撃に対しての防衛力を向上させることを目的とした．擬似攻撃メールは合計 2 回送信し，最初の擬似攻撃メールから 1 週間程度をあけて 2 回目を送信してその効果を測った．メールの文例を表 1 に示す．メールの宛先は実際の攻撃を模して私信としており，内容は対象者に関係のあるような内容としている．2 回目のメールも同様に業務に関連のある内容とした．

図 1，表 2 および表 3 は平成 23 年度実施分の結果である．は，添付ファイルが開封された数のうち，時系列での開封率を示している．添付ファイルには Web ビーコンが組み込まれており，添付ファイルの開封情報が集計サーバーに送られて開封状況が記録される仕組みとした．本訓練では，開封された添付ファイルのうち約 3 時間で約 9 割が開封された．メールは業務開始前の 8 時に送信しているので，午前中に多くが開封されていたことが分かる．他組織と比較すると最初の 1 時間の開封率は低いが，2 時間以降はおおむね同様の経過をたどっていた．

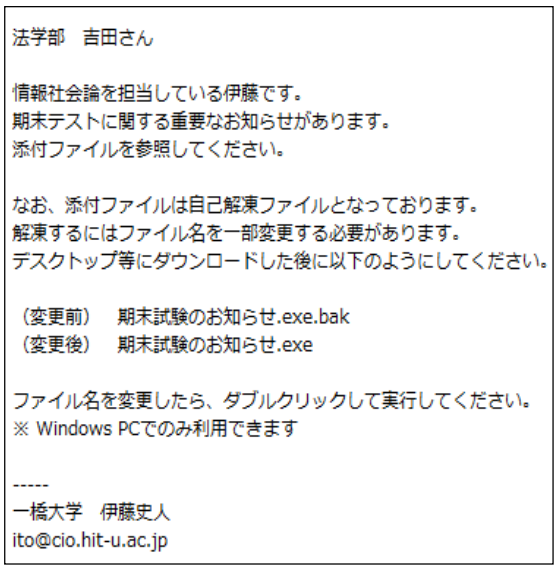
表 2 は本学と他組織における第 1 回と第 2 回における擬似攻撃メールの開封率を示したものである．本学の場合，被験者数 200 名で第 1 回の開封率は 40.0%に達しており他組織 E を除いて開封率が多い結果となった．第 2 回の開封率は減少して 28.5%となり開封減少率は 28.8%である．他の 5 組織と比べると他組織 D の次に開封減少率が低いことから，本学においては第 1 回の効果がやや少なかったと判断できる．一方で，開封減少率の中央値は 55.7%であり，本訓練の手法は効果があると判断できる．

平成 24 年度の結果は，第 1 回の開封率が 35.3%，第 2 回は 3.8%となり開封減少率は 88.9% であった．メール本文の内容によっても開封率は変化するが，約 90%の開封減少率は訓練の効果を示唆するものである．被験者は前年度の訓練を思い出し，第 2 回のメールに不信感を持つことが可能になったと推測される．

なお，訓練後のアンケート（表 3）では，多くの職員が情報セキュリティに対する意識向上に効果があったとの声を寄せており，一定の意義を認めることができた．訓練後は職員同士で怪しいメールへの対応を積極的に行うようになり，組織全体のセキュリティ意識が向上しているのが見て取れた．新聞やテレビニュースで報じられるセキュリティ事故についても理解できるようになり，自らを省みることにつながっているようである．

以上のことから，本論文で論じる擬似フィッシング攻撃訓練についても，標的型攻撃メール予防接種訓練と同様の手続きで実施するものであり，予防的効果を狙った訓練としては有効と考えられる．

ところで，学生に対しても同様の訓練を実施しており，学生にとっては関心の高い内容とした（図 2）．第 1 回約 40%，第 2 回で約 30%が開封しており，事務職員とほぼ同様の結果が得られた．


法学部　吉田さん

情報社会論を担当している伊藤です。
期末テストに関する重要なお知らせがあります。
添付ファイルを参照してください。

なお、添付ファイルは自己解凍ファイルとなっております。
解凍するにはファイル名を一部変更する必要があります。
デスクトップ等にダウンロードした後に以下のようにしてください。

（変更前）　期末試験のお知らせ.exe.bak
（変更後）　期末試験のお知らせ.exe

ファイル名を変更したら、ダブルクリックして実行してください。
※ Windows PCでのみ利用できます

一橋大学　伊藤史人
ito@cio.hit-u.ac.jp

図 2　学生への模擬標的型攻撃メールの文面

2.3. 予防接種対策によるフィッシング攻撃の教育的訓練の必要性

フィッシング攻撃について，その脅威とは裏腹に，正しく理解している教職員は多くはない．対策としては，まずはフィッシング攻撃がどのようなものかを理解することが重要である．標的型攻撃メールと同様に，フィッシング攻撃への根本的な対策は「人」への対策である．同様にフィッシング攻撃についても，擬似攻撃による予防接種的訓練が有効であると仮定できる．

一方で，フィッシング攻撃へのシステム的な対策は，関連サービスやブラウザの機能強化ソフトウェアにより徐々に整いつつあるが，すべての Web サイトへの対応は現実的ではない[9]．特に，上記のサービスやソフトウェアでも，大学で個別に運用しているような独自の Web システムへの対応は今後も実施されることはない．

そこで，本学では，平成 25 年度に，教員および事務職員に対して，偽装グループウェアサイトへ誘導するための擬似攻撃メールを送付する「フィッシング攻撃予防訓練」を実施した．本訓練では，グループウェアの偽装ログインサイトに訓練対象者（教職員）を誘導し，実際にログイン情報の入力させることでフィッシングを体験してもらうこととした．ログイン情報等は集計データとして記録し，標的型攻撃メール訓練と同様に効果を測るための情報とする．

なお，本学の利用するグループウェアは教員と事務職員が共通で利用しており，情報共有にための重要なインフラとなっている．特に事務職員については，業務中は常にアクセスしていることもあり，本学において利用率の最も高いシステムである．フィッシングサイトとしてグループウェアを対象とすることにより，教職員への訓練効果がより高いと考えた．

3. 方法

擬似フィッシング攻撃の方法は，擬似標的型メール攻撃訓練とおおむね同様である．大きな違いは，擬似マルウェア添付メール（標的型メール攻撃）を開封するか，偽装サイト（フィッシング攻撃）にログインするかである．

3.1. 組織内の周知とセキュリティの担保

擬似攻撃による予防接種的訓練は，実務への影響を完全に無くすことは難しい．なぜなら，業務で実際に使われているメールアカウントに対して擬似攻撃メールを送信するからである．偽装サイトにログインしても実害は一切生じないが，被験者にとっては不安・不快に感じてしまう恐れはある．そこで，本訓練においては組織のトップから承認を得て実施し，被験者からの苦情等に対しては万全の準備を行った．

各研究科の教授会および大学組織内における事務部局の連絡会議において本訓練の概要を説明し，実施の承認を得た．ただし，実施日時については未定とし，おおよその時期のみを通知した．これは，訓練の効果をより高めるためである．

また，本訓練で利用する偽装サイトの作成および管理にあたっては，訓練実施者以外の者に監査を依頼した．これは，予防接種の実施フローの中で被験者がパスワードを入力するため，入力したパスワードをサーバーに保管しないこと担保するための措置である．具体的には，偽装サイトのソースコードを監査者が常に監視できる環境を準備した．

偽装サイトへの通信は SSL 通信としてログイン情報の通信を暗号化する．これは，偽装サイトへログインする被験者は，正しいログイン情報を入力することが想定されるためである．さらに，ログインの記録データは暗号化する．

3.2. 被験者（訓練対象者）

本訓練の対象としたのは，常勤の教員 400 名と事務職員 200 名である．実務への影響を考慮して，教員と事務職員はそれぞれ別の日程で実施した．

3.3. 実施のフロー

訓練実施においては，事前準備・訓練当日・訓練後の

3 つのフェーズに分けてマニュアルを作成した．ここでは，実施者と被験者のフローを以下に記す．

実施者は情報基盤センター事務情報化部門である．

実施者のフロー

事前準備

① 教授会・事務連の承認
② 偽装サイトの準備および監査者の選定
③ 被験者の選定
常勤の教員および事務職員全員を対象とする
④ 擬似攻撃メールの準備および動作試験

訓練当日　＊2 回目も同様に実施する

① 8:00 ころ，対象職員への擬似攻撃メールの送信
本学ドメイン以外から同報メール送信ソフトウェアにより配信
② アクセス記録の確認
偽装サイトへのログイン時に取得する
時刻・ID・OS・IP アドレス 等
ただし，パスワードは記録しない
③ 16:00 ころ，グループウェアトップページへの訓練実施報告（種明かし）の掲載
④ 2 回目終了後はアンケート採取
⑤ 被験者からの電話対応等

訓練後

① 監査人から不正の有無の確認
② 開封状況の解析とデータの破棄
③ 結果レポートの公表

被験者のフロー

事前準備

特になし．実施日時は知らされていない．

訓練当日

① 個人メールアカウント宛の擬似攻撃メールを受信
※ フィッシングに気づいた者はここで終了
② メールから偽装サイトへアクセス
メール内の URL リンクをクリックすることでアクセス
③ ログイン情報入力とサブミット（ログイン）
偽装グループウェアにて『これはフィッシング訓練です』等の表示をして訓練であることを明記

訓練後

本訓練の集計結果の報告を受ける

3.4. 偽装サイトと擬似攻撃メール

偽装サイト（図 3）においては外部ドメインの URL を持ったサイトとする．擬似攻撃メールの本文に URL が記載されており，URL リンクもしくは URL のコピー&ペーストで偽装サイトにアクセスさせる．一般的なフィッシングサイトと同様に，偽装サイトは偽装対象のウェブサイトとまったく同じ外観を持っているため，きちんと URL を確かめなければ偽装サイトであることは判別できない．本学の事務職員が利用するブラウザは一元管理している PC を利用しているため URL が表示されるようになっている．ただし，教員の使うブラウザについては，それぞれの設定による．

偽装サイトにはユーザー名とパスワードを入れる欄はあるものの，実際には認証は行わずに何らかの文字列が入力されていればサブミット（ログイン）を可能としている．これは本訓練には実際のユーザー認証を行う必要がないためである．実際のグループウェアの仕様では，ユーザーID およびパスワードの両方の入力がないとサブミットできない．

図 3　偽装サイト（グループウェアログイン画面）

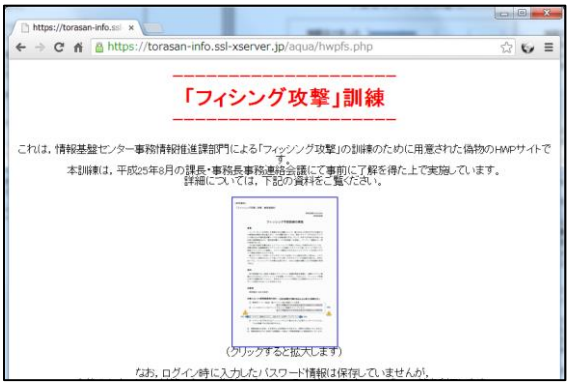


図 4　偽装サイトのトップページ

サブミット時には，アクセス解析のためのパラメータ（時刻・ユーザーID・パスワード等）を取得して集計データとする．サブミット後のページでは，フィッシング訓練であること明記した画面を表示して訓練であることを知らせる（図 4）．入力したパスワードは保存されていないことや，教授会等で承認された訓練であること等を

記している．

なお，本学では各システム間でシングルサインオンを構成しているため，パスワードが漏洩するとその影響は他システムへの不正ログイン等，広い範囲に及ぶと考えられる．前述のようにパスワードは集計データとして記録しないよう監査人を付け，可能な限りのセキュリティ環境を担保する．

擬似攻撃メールの送信は合計 2 回行う．2 回目の送信は初回から 1 週間空けて送信して，効果を測るための情報とする．実際の攻撃を想定して，本学とは無関係の外部ドメイン（torasan.info）から個人用メールアドレス宛に送信する．メール文面は教職員が関心を持ちそうな内容か業務に関連があるものとし，文中に偽装サイトへ誘導する URL リンクを記載する（図 5および図 6）．その際，URL リンクは URL のフルアドレスが表示されるようにし，本物のグループウェアの URL かどうか識別できるように配慮している．

教員への擬似攻撃メールの件名は「【確認】使用 PC のセキュリティチェックのお願い」と「Windows XP パソコン更新における購入補助について」として，時節に合わせた内容としている．事務職員への擬似攻撃メールの件名は「【確認】使用 PC のセキュリティチェックのお願い」と「[Alert]メールボックスが制限容量に近づいています！」である．

From:情報システム担当 inf-js-g@torasan.info
Subject: Windows XP パソコン更新における購入補助について

<%Name%>　先生

情報推進課情報システム担当です。
お世話になっております。

<%Name%>先生のネットワーク利用履歴から Windows XP が使われていることが判明しました。

周知のとおり、Windows XP は来年の 4 月にサポートが期限を迎えます。それに合わせて、Windows Update も停止されるため、期限後に発見された脆弱性は改善されない見込みです。
そのため、Windows XP を利用し続けることはセキュリティリスクを高めることとなり、結果として本学全体のセキュリティレベルを大きく低下させる要因となります。

PC の更新については、期間限定で購入補助が受けられます。
下記の URL からログインして至急手続きをしていただくようお願いします。

購入補助手続き
https://torasan-info.ssl-xserver.jp/aqua/

****
国立大学法人　一橋大学
情報システム課　情報システム担当
inf-js-g@torasan.info
****

図 5　擬似攻撃メールの例（教員向け・2 回目）

From:情報システム担当 inf-js-g@torasan.info
Subject: [Alert]メールボックスが制限容量に近づいています！

<%Name%>　様

情報推進課情報システム担当です。
お世話になっております。

<%Name%>様のメールボックスが制限容量に近づいております。

容量確保のため、不要なメールは至急削除していただく必要があります。もしくは、メールボックスの容量を増量する対応が必要です。

メールボックス増量の依頼方法は，グループウェアで申請していただけます。

下記の URL からログインしてください。

連絡事項画面のログイン
https://torasan-info.ssl-xserver.jp/aqua/

****
国立大学法人　一橋大学
情報推進課　情報システム担当
inf-js-g@hit-u.ac.jp
****

図 6　擬似攻撃メールの例（事務職員向け・2 回目）

第 1 回目と第 2 回目のログイン数を適切に検証するため，件名および本文内容は同程度の関心が持たれるよう留意する必要がある．

なお，教員と事務職員は異なるメールシステムを利用しているがいずれも Web メールとなっている．どちらのメールクライアントも差出人のメールドメインが表示される．

4. 結果

教員・事務職員にそれぞれに擬似フィッシング攻撃訓練を行った結果を，偽装サイトへのログイン結果およびアンケート集計として示す．

4.1. ログイン結果

表 4 および表 5 に教員と事務職員の偽装サイトへのログイン結果を示す．教員については学外からメールを利用する者も多いのが特徴である．アクセスログを参照すると，教員は出張先や自宅等でメールを確認している場合が多いことがわかった．アクセスに利用したブラウザはスマートフォンやタブレット用のものが目立った．また，偽装サイトへのログイン情報としてダミーの文字列（aaaaaa, 123456 等）を入力してログインを試みている者が多数あった．グループウェアの偽装サイトに不信感を抱いたために取った行動と思われるが，これは事務職

員にはみられない行動である.

ところで，教員向けの2回目の擬似攻撃メールが，メールシステム（Gmail）のアンチスパム機能により400通中200通程度がブロックされてしまい被験者に配送されなかった．そのため，2 回目のログイン数に大きく影響し，本来よりも少ないログイン数になったものと考えることができる.

表 4　ログイン数（教員：400名）

	1回目	2回目
ログイン数	64 (16%)	33 (8%)
学外からのログイン数	24 (6%)	20 (5%)
ダミーが入力された数	9 (2%)	4 (1%)
ログイン減少率	50%	

表 5　ログイン数（事務職員：200名）

	1回目	2回目
ログイン数	25(13%)	8(4%)
学外からのログイン数	1 (1%)	2 (1%)
ダミーが入力された数	0 (0%)	0(0%)
ログイン減少率	68%	

4.2. アンケート集計結果

アンケートはグループウェアの機能を利用して採取した．アンケートの回収率は教員と事務職員でそれぞれ6.0% と37.0％ で大きな開きがあった．事務職員に比べて教員のグループウェアの利用率は低く，さらには，本訓練のような大学が実施する事業に協力的ではないことも関係していると考えられる.

図 7および図 8にアンケート集計結果を，表 6および表 7にアンケート自由欄の回答例を示す．表 8 は被験者が擬似攻撃メールに返信した例である．被験者が擬似攻撃メールを本物と疑わない者の中，内容に関する返信を送ってきた者が教員と事務職員でそれぞれ9名と3名あった.

5. 考察

5.1. ログイン

教員のログイン率は1回目 16%で2回目 8%であり，ログイン減少率は 50%であった（表 4）．事務職員のログイン率は，1回目 13%で2回目 4%であり，ログイン減少率は 68%であった（表 5）．事務職員のログイン減少率は教員に比べて18% 高く，1回目の効果が教員よりも高かった．これは，事務職員の過去の訓練結果がもたらした効果の可能性がある.

アンケート集計結果によると，本訓練と同種を訓練の経験したことがあるかを問う「過去に訓練を経験したか」に対して，教員は「経験した」が2.5%，事務職員は30.0%と10倍近い差があった（図 7および図 8）．これは，事務職員は平成23年と24年に標的型攻撃メールの訓練を実施しているための結果である．事務職員は教員と比べてログイン率とログイン減少率とも低いのは，前回までは標的型攻撃メールの訓練ではあったものの，訓練以降は，不審なメールが送られてくることに警戒感を持ち差出人のメールドメインを確認する習慣等が身についている者が多かったからと考えられる.

ところで，本学教員の勤務スタイルにおいて，グループウェア利用率は事務職員に比べて大幅に低い．事務職員はほぼ 100%が利用しているが，教員は 30%程度である．事務職員は，所属課内等でスケジュールの共有が必須であったり，事務業務システムの一部がグループウェアに統合されているため必然的に利用率が高い．これらの状況を考慮すると，教員の実際のログイン率はより大きい可能性が高いだろう．特に，2 回目についてはメーラーのアンチスパムの影響で半数のメールしか配送されなかったため，ログイン率は自ずと低下している.

また，事務職員と同程度の利用率のウェブシステムで擬似フィッシング訓練を実施した場合，事務職員のログイン率をさらに上回るだろう．つまり，本訓練の場合，ほとんど予防接種的訓練を受けていないグループ(教員)のログイン率が，訓練を受けているグループ(事務職員)と大差のない結果だとしても，フィッシング攻撃や標的型メール攻撃への防衛力に大差がないとは言えない．実際は，過去に予防接種的訓練を受けていたグループの防衛力が高いと評価できる可能性が極めて高い.

勤務形態がログイン率に影響を与えることも想像できる．事務職員は同室内で複数人が業務にあたっていることが多い一方で，教員の多くは個室である．不審なメールがあった際に，事務職員であればお互いにその情報を共有しやすい．過去の訓練を経験した者がいることで，他の未経験の人がいてもグループで防衛力が維持される．本訓練でもそのような事例があり，ログインを免れた者が数名確認されている．教員については個人の防衛力がそのまま反映される.

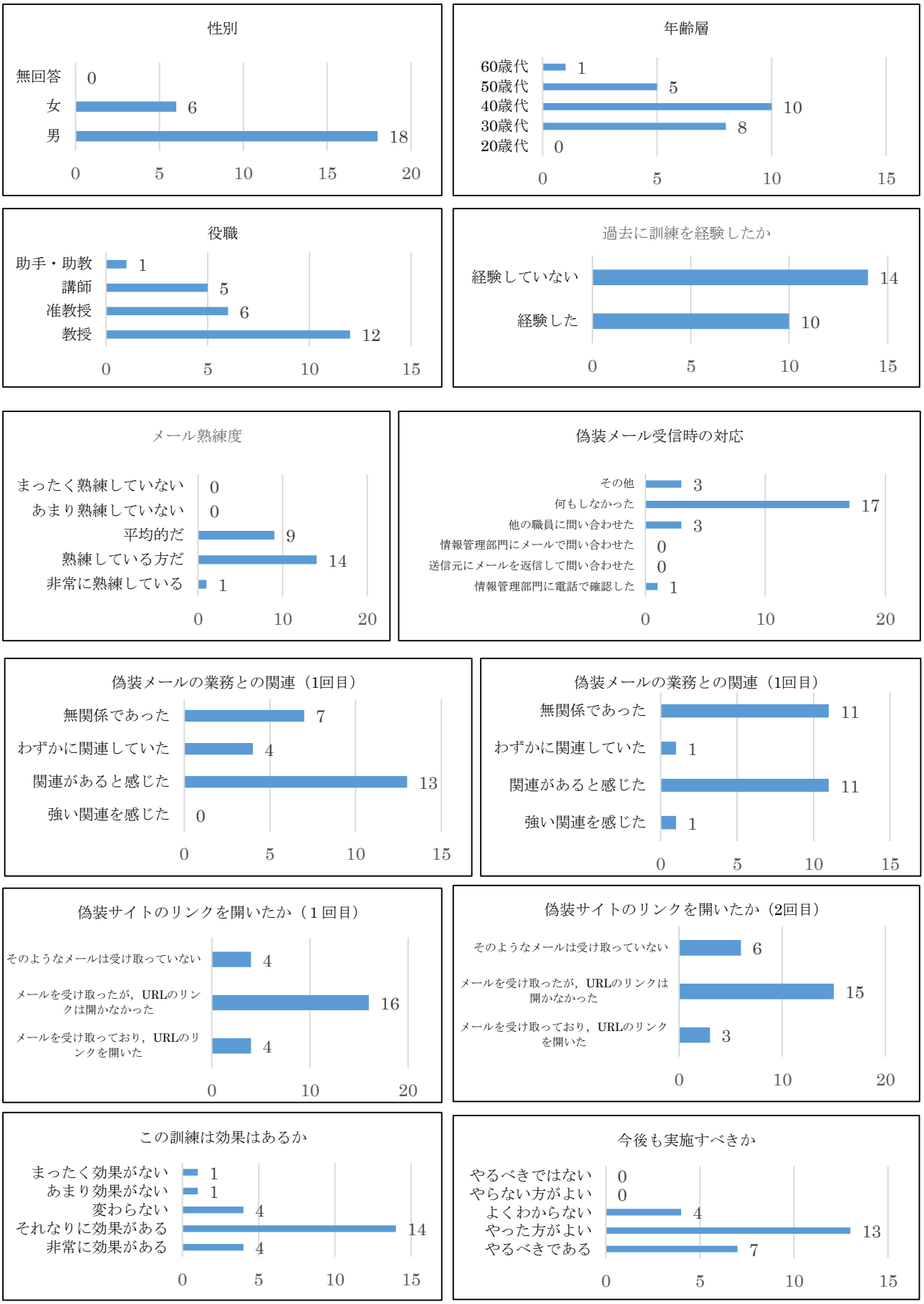


図 7　アンケート結果（教員 n=24）

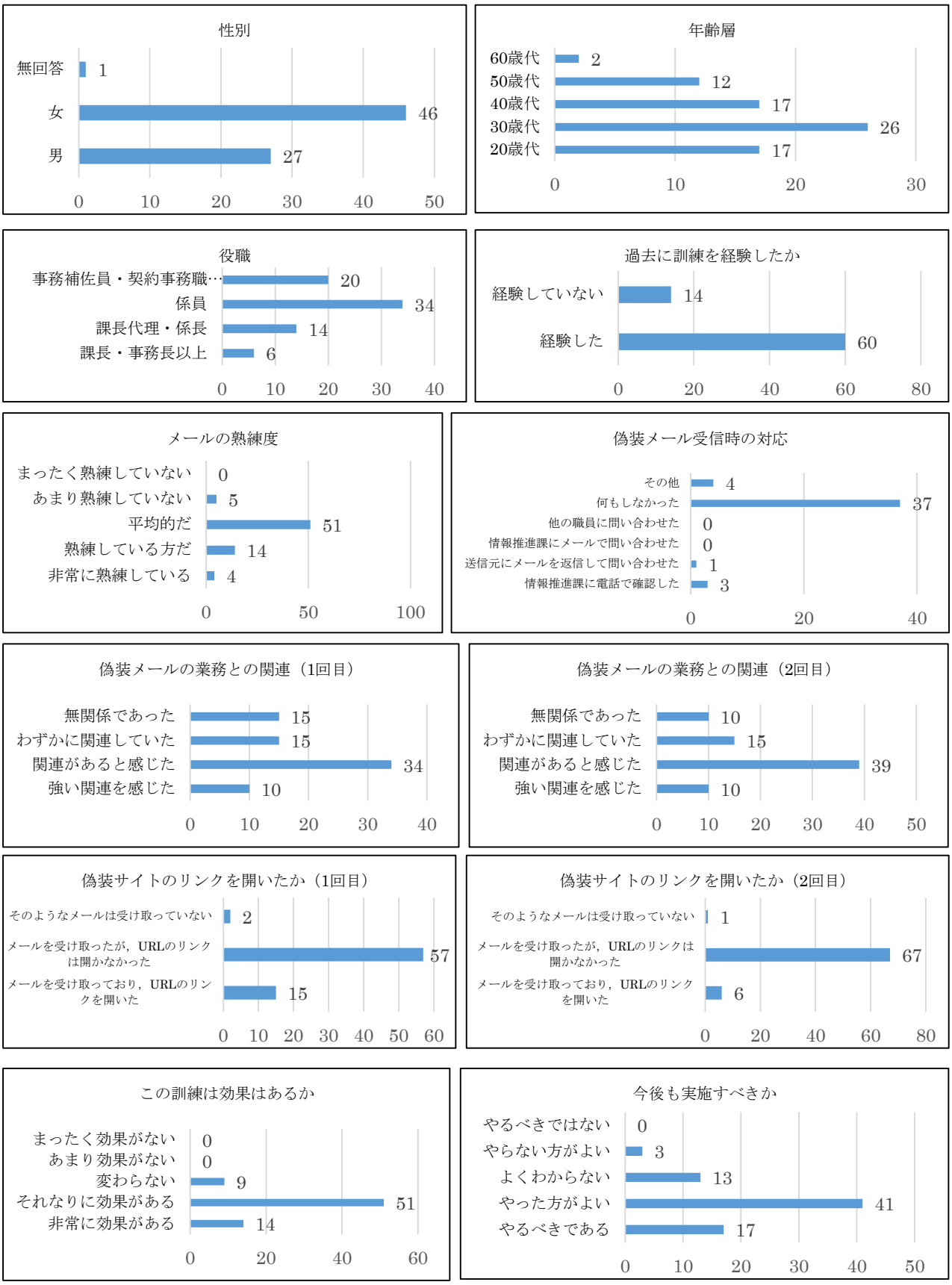


図 8　アンケート結果（事務職員 n=74）

表 6　被験者の感想（教員）

No.	感　想
1	以下の理由で擬似攻撃メールにひっかかったと自分の中で分析しております．①擬似攻撃メールを受け取ったときは，いろいろな業務が立て込んでおり，早く業務を処理したいという思いが強かった．さらにその前日までの仕事による疲労が回復していなかったため，判断力が低下していた．②日頃，グループウェアが非常に使いにくいと感じていた．毎回必要なドキュメントのページになかなかたどりつくことができず苦労している．上述のように早く業務を処理したかったため，メールにリンクがはってあったページにいってしまった．③その前日に，ウェブを使った操作(e-Rad)について事務室と頻繁にメールでやりとりしており，警戒心が薄れていた．
2	私自身は受け取った当初から「怪しい」と思って警戒したが，そのように思わずにクリックしてしまう教職員も存在すると考える．また，私自身も，将来，新手の方法でのフィッシングに引っかかってしまう可能性がないとは言えない（10年以上前に，同僚からのウィルスメールを開いてしまった経験がある）．したがって，定期的にこのような訓練を行い，注意喚起を行うことの効果はあると思われる．
3	これからは，擬似攻撃メールにより一層警戒し，だまされないようにしていきたいと思っております．しかし，業務がたまりせっぱつまった状況などで，完全にだまされないようにするのは不可能ではないかとも思っています．最後に，擬似攻撃メールを受け取ったときに，どこに連絡すればよいか教えていただけるでしょうか？私は，これまでこの点について，説明を受けたことはありません．
4	そもそも r.hit-u.ac.jp 宛のメールは通常ほとんど見ていないので，両メールとも 12/27 に確認しました．ただし，12/25 のメールは自動的に迷惑メールに振り分けられていました．いちおう教授会で予告されていたので，メールをみたときあのことだろうと思い，リンク先 URL でそれを確信しました．本当のグループウェアには，何かアナウンスがあるかもと思い，このアンケートを見つけていま回答しています．

表 7　被験者の感想（事務職員）

No.	感　想
1	メールの真偽を確かめる手段として送信元のドメインを確認しました．
2	訓練は不快で業務に支障がでましたが，啓発の意味もあるのでしょうから，実施していく必要があると思います．
3	非常に良い訓練でした．2 回目のメールボックスの容量の連絡には，見事に騙されてしまい，リンク先を開いてしまいました．しかし，グループウェアのログイン画面にジャンプしたところで，不審に思い，正規ルートからグループウェアへログインし，メールボックスの要領に関する内容を探しましたが，見つからなかったため，そこで訓練のメールだと気づきました．今後はリンク先を開く前に，メールアドレスやリンク先の URL を確認し，不審なものでないか判断したいと思います．
4	１回目は，アドレスが違うことを確認しましたが，２回目は，アクセスこそしませんでしたが，古いメールを削除して安心してアドレスを確認しませんでした．手をかえて試していただけるのは，良いと思います．いろいろな意見があってご苦労だと思いますが，私は必要なことだと思います．
5	ドメインにヒントがあるので，気付き易かったです．標的型攻撃メールやフィッシング等で，より悪質で巧妙なものがあれば，訓練として経験したいと思いました．
6	事務補佐員なので個人的に処理するメールが少ないので，「個人」に届き，メール操作の知識があまりない個人にとって，表題がびっくりする件名であったことで動揺した．訓練を定期的に実施していただけることは，個人的によいことだと思った．
7	毎回引っかかってしまいます．擬似攻撃メールを考えておられる方の頭の良さに敬服します．設問 12.のベストアンサーは，送信元である「情報推進課に電話して確認」することだと思いますが，実際はなかなか，そこまでの対応は遠慮してしまいます．した方がいいのだと思いますが．送信者が「一橋大学情報推進課課長」だと，信用してしまいますね．ただ，メアドが torasan.info だと，「トラさんだ！」と気がつくようになりました．
8	今回はログインを促す URL が一見して不自然とわかるものであり，また課長名でわざわざ個々の職員の個人アドレス宛にメールを送って注意を促すことなど想定しにくい（注意を促すならもっと手っ取り早い方法がいくらでもある）ことから，容易に擬似攻撃訓練と判断できるものだったと思います．もっと巧妙な内容にしても良いかと思います．
9	昨年，初めての訓練の時に失敗しましたので，それ以降は，注意しております．個人宛に，メールが来ると怪しいと感じるようになりました．しかし，第 2 回配信の時は，メールを本当に削除しなければないのかと思い，職員の方に削除のやり方を尋ねて，訓練だとわかりました．

表 8　擬似攻撃メールへの返信例（教員）

No.	感　想
1	表記の件，わざわざご連絡いただき，ありがとうございました．私はコンピューターに疎いものですので，現在使っているのは，Windows`7 Professional だと思っていたのですが，それは誤解でしょうか？
2	３月に定年退職するので，機器を買い換えるのは控えます．
3	ご連絡をありがとうございました．windows XP はここ数年，全く使用していません．また使用する予定もありません．そのまま廃棄になるかと思います．その場合はそのままでもよろしいでしょうか．
4	ご連絡有難うございます．了解いたしました．

前述のように，ログインした者の内，ダミーの文字列を入力しているのは教員の特徴である．ログイン履歴を詳細に確認すると，最初からダミーを入力したのではなく，最初は偽装サイトだと気付かずにサブミットし，その後ダミーを入力している例が 5 例あった．事務職員はダミーの入力は 0%である．教員のほとんどはこの種の訓練を受けたことがないため，偽装サイトだと分かった時に混乱または動揺したと想像できる．そのため，偽装サイトを再度確認するためにダミーを入力したと考えられる．事務職員については，過去に経験した同種の訓練と気付きそのまま事実を受け止められたのだろう．

5.2. アンケートと被験者の反応

フィッシング攻撃や標的型メール攻撃は，攻撃メールの内容次第で成否が分かれる．被攻撃者にとって関連があるか信用に値する内容であれば被害に合ってしまう可能性が高まる．アンケート結果によると，「偽装メールの業務との関連」において，教員の感じた偽装メール本文と被験者の業務との関連性については 1 回目と 2 回目でやや違いが生じている（図 7）．本来であれば両回とも同じ傾向である必要があった．業務との関連性が両回で異なれば，ログイン率に影響してしまい，訓練の効果が測りにくくなるためである．事務職員については，同じ傾向が出たので正しく測定できた（図 8）．

「この訓練は効果があるか」および「今後も実施すべきか」については，いずれも前向きな結果が得られた．アンケートの自由記述（表 6 および表 7）からも明らかなように，定期的な訓練がより効果的であろう．

ところで，擬似攻撃メールに対して，偽装メールであることを疑わずに返信した者が多数にのぼった（表 8）．特に教員に関しては，ログイン数に比べて事務職員よりも返信率が顕著に高い．偽装サイトにログインすれば訓練であることは分かったはずであるが，ログインせずに返信を送っている．グループウェアへのログイン方法が分からなかったか，ログインする前に返信したものと思われる．仮にログイン方法がわかっていれば偽装サイトにログインしまったと考えられる．メールの返信だけ行ってログインしていない例が 5 例あることから，ログイン方法の分かるウェブサイトであったらログインしていただろう．返信内容も，偽装メールに一切不信感を抱いていないのがわかる．

なお，教員のアンケートの回収率が低かった根本的な理由は不明であるが，前述のようにグループウェアの利用率が低いことと無関係ではないと考えられる．

6. おわりに

フィッシング攻撃や標的型メール攻撃等のシステム的な対策が困難なサイバー攻撃については「人」への対策重要である．本訓練において教員と事務職員のログイン率およびログイン減少率に違いが明らかであったように，予防接種的訓練はサイバー攻撃に効果のある方法である．しかしながら，完全に防ぐのは難しい．数百人に対する攻撃が発生したら，その内の数名は欺かれてしまうのは不可避である．ただし，攻撃の成功率を減少させることができれば，情報漏洩を起こすまでの事故は防げる可能性が高まる．情報漏洩に至るまでは，さらにいくつかの攻撃ステップが必要だからである．つまり，組織としては，サイバー攻撃による情報漏洩等を無くすには，少しでも最初の段階での攻撃成功率を減らすべきである．予防接種的訓練は，サイバー攻撃へのリスクをゼロにすることはできないが，現状に比べて大きく減少させることができる方法である．

一方で，今回の訓練で改めて浮き彫りになったのは，セキュリティ上怪しい事象が起きた際の学内での連絡先が周知されていないということであった．特に教員の場合が顕著であり，本学においては危険な徴候を見逃してしまう可能性が非常に高い状況にあると考えられる．本訓練は被験者の訓練であるのと同時に管理側の訓練にもつながった．

大学組織は人の入れ替わりが頻繁に発生していることから，本訓練のような予防接種的効果を持続させるには定期的に実施することが必要である．実施にあたっては，組織内のオーサライズが困難であるが，一度成功させることができれば次回以降は実施しやすい．

アンケート結果からも被験者の反応は好意的なものが多数を占める．情報セキュリティ事故は「人」が起こすものがもっとも被害を大きくする．昨今の個人情報の持ち出し事件も，システム的な対策では防げないものであった．予防接種的訓練は比較的簡便に実施できるものであるにも関わらず，その反面で効果は極めて大きい．今後，新しいサイバー攻撃が現れるはずであるが，「人」への対策が最後の砦であり続けるのは間違いないだろう．

参考文献

[1] 伊藤史人, “標的型攻撃メールの予防対策”, 学術情報処理研究, Vol.16, pp.100-110, 2012.

[2] 金野千里, “増大する脅威とそれに向けた取り組み”, 独立行政法人情報処理推進機構, IPA フォーラム 2011, 2011.

[3] 猪俣敦夫, ラーマン・ミザヌール, 岡本健, 岡本栄司,

“フィッシングメール防御のためのメールフィルタリング手法の提案”, SCIS2005, 2005.
[4] 岡田好史, “不正アクセス行為の発生状況の現状と課題 (3)”, 専修法学論集, Vol.116, pp.1-36, 2012.
[5] 独立行政法人情報処理推進機構, “IPA テクニカルウォッチ　標的型攻撃メールの分析に関するレポート～だましのテクニック事例 4 件の紹介と標的型攻撃メールの分析・対策～”, 2011.
[6] 森山勉, 駒木敬, “電子自治体の構築に向けた新たなソリューション・ビジネス「システム統合基板」”, UNISYS TECHNOLOGY REVIEW, Vol88, pp.90-103, 2006.
[7] 独立行政法人情報処理推進機構, “コンピュータウイルス・不正アクセス届出状況および相談受付状況 [2014 年第 1 四半期 (1 月～3 月)]”, http://www.ipa.go.jp/security/txt/2014/q1outline.html, 独立行政法人情報処理推進機構, 2014.
[8] 株式会社ラック, “IT セキュリティ予防接種結果報告書（一橋大学）”, 株式会社ラック, 2012.
[9] 加藤慧, “コンテンツベースフィッシング検知手法の大規模実例評価と改良”, 情報処理学会研究報告, Vol.48, pp.1-7, 2010.