標的型攻撃メールの予防対策

Protective Measure for Targeted Cyber Attack Mail

伊藤　史人†，高見澤　秀幸†，佐藤　郁哉†
Fumihito ITO†, Hideyuki TAKAMIZAWA†, Ikuya SATO†

ito@cio.hit-u.ac.jp, h.takamizawa@cio.hit-u.ac.jp, ikuya.sato@cio.hit-u.ac.jp

†一橋大学情報基盤センター

†Center of Information and Communication Technology, Hitotsubashi University

概要

標的型攻撃メールは，ある特定の組織や個人を狙った機密情報等を窃取する手段に利用されている．攻撃に利用するメールにはファイルが添付されており，受信者がそのファイルを開くことでシステムの脆弱性等を突き任意のコードを実行する．メールの文面は，受信者が不審に感じ難いものとしていることが多く，完全な防御は極めて難しい．その一方で，効果的な対策としては，教育的効果を狙って模擬標的型攻撃メールを対象者に送り，同種の攻撃に対する意識を高めることが挙げられる．本論文では，標的型攻撃メールを病原体と仮定し，模擬標的攻撃メールを「予防接種」として作用させ，「人」に免疫反応を引き起こすことで攻撃への耐性を高める試みについて報告する．具体例として，一橋大学の学生 196 名と事務職員 200 名に対する模擬標的型攻撃メールを予防接種した結果と，解析結果から得られた今後の対策案について述べる．

キーワード

標的型攻撃メール, Web ビーコン, 脆弱性, 情報漏えい, 個人情報

1. はじめに

標的型攻撃メールは，セキュリティにおいて最も弱点となりやすい「人」をターゲットとしている点に特徴がある．「人」に対する情報セキュリティ対策は，統一的に実施するのは困難である．攻撃手法においては，未知のウイルスや脆弱性を悪用してシステムへの侵入を試みるため，確実な対策は極めて難しい．

そのため，標的型攻撃メールは認知されてから 7 年ほど経っており，もはや新しい手法ではないにも関わらず，未だ完全な対策が打てないのが現状である．今日も公官庁や大手電機メーカーからの機密情報漏えいが止むことはなく，情報セキュリティ対策は依然として対症療法的な対応とならざるを得ない状況が続いている．

セキュリティ対策としては，標的型攻撃メールが「人」に対する攻撃であることから，システムのみによる対策は実効性に乏しく，やはり「人」への対策が必須である．

本論文では，標的型攻撃メールそのものを病原体（抗原）と仮定し，模擬標的攻撃メールを「予防接種」として利用し，「人」に免疫反応を引き起こすことで攻撃への耐性を高める試みについて述べる．

2. セキュリティ対策と標的型攻撃メール

標的型攻撃メールは 2011 年の衆議院議員会館や原子力発電設備関連の情報漏えいで大いに話題になったため，新しい攻撃手法と思われがちであるが，インターネットの歴史の時間軸からみればけっして新しいものではない．ここでは，過去のウイルスメールについて振り返り，標的型攻撃メールの対策について考察する．

2.1. インターネット経由の攻撃活動の変遷

インターネットが一般家庭に普及した 2000 年以降, 大きく分けて 4 段階の攻撃手法に分類することができる[1].

2000 年初頭は,「均一的かつ広範囲にわたる単発被害」と表現することができる. 被害としては Web サイトのページ書き換え等が相当する．当時はセキュリティ対策が甘いサーバも多く，攻撃者は手動でも比較的容易に攻撃を成功させることができた．ユーザのセキュリティ意識も低かったことから，ウイルスが含まれた添付ファイルによって感染が広まった．Happy99 は愉快犯的なウイルスであるが，世間に多く広まったことから，コンピュータウイルスへの意識を高める契機となった．

また，当時の代表的なウイルスは，Nimda や Code Red が挙げられ，これらは無防備なシステムに感染し，ユーザの共有フォルダデータを消去するなど大きな被害をもたらした．さらには，サイバー攻撃を組織的に行うことで情報を窃取し, それをビジネスとする流れも生まれた.

2005 年にかけては,「均一的かつ広範囲にわたる連鎖的被害」となる．攻撃者は攻撃を多様な手段で自動化してマルウェアを流布するとともに, ワームを Web サイトに仕込むことでユーザのシステムを攻撃し，以前よりも広範囲かつ連鎖的に感染させることに成功した[3].

2005 年以降は「類似した局所的な被害」として，SQL インジェクションによる Web サイト攻撃や Winny, Share による情報流出が挙げられる．また，フィッシングやスパイウェア，さらにはボットなどが活発になった時期であった.

そして, 2006 年以降は「すべてが異なる局所的な被害」として標的型攻撃が認知されるようになった．攻撃者は不特定多数を対象にするのではなく，ある目的を持って特定の対象を決めてより確実な攻撃を仕掛けるようになったのである．このことは，以前よりもサーバの堅牢性が増したことと無関係ではなかったと考えられる．サーバのセキュリティ対策に比べ，クライアントについては脆弱性が放置されていることが多く，標的型攻撃はその穴を狙ったものであるといえる．そして，現在，標的型攻撃は完全防御できない攻撃手法として各所で大きな被害を出すに至っている.

2.2. 階層毎のセキュリティ対策

セキュリティ対策を実施するにあたって，一般的には階層毎に対策を行うこととなる.

表 1 にその例を示す.

ネットワーク階層においては，ファイアウォールやフィルタリングによる対策を実施することで，おおむねセキュリティは全体的に向上する．しかし，ネットワークの未知の脆弱性や，正常なプロコトル通信を悪用した被害からは免れることはできない．それらは，ゼロデイ脅威としてセキィリティ対策の大きなウィークポイントとなっている.

サーバおよびクライアントの階層ではウイルス対策ソフトやセキュリティアップデートにより，多くのセキュリティホールを塞ぐことが可能である．ただし，ネットワーク階層と同様に，ゼロデイ脅威となるソフトウェアの未知の脆弱性やウイルスによるセキュリティの低下は必至である．このことから，事前経験のない未知の脅威に対してはやはり完全に無防備であるといってよい.

パケットの振る舞いに着目して未知の亜種ウイルスに対応する手法も研究されているが，まったくの未知のウイルスに対してはやはり効果を発揮しない[2]．亜種ウイルスを予測するにはあらかじめベースとなる本体ウイルスを解析しておく必要があるためである.

最後に「人」の階層でのセキュリティ対策である.「人」は機械と異なり，推測する能力においては極めて高いとされる．その特性を活かすのと併せて，個人への教育や組織体制の見直しにより，ゼロデイ脅威に対して有効な作用を発揮する．機械が行う解析ベースのセキュリティ対策よりも柔軟に対応することが可能である．つまり，未知の脅威に対しても，教育等により完全に無防備になることなく，一定以上の効果を見込むことができるのである.

2.3.「マスメール型」と「標的型」

ウイスルメールには，コンピュータウイルスに感染したパソコンから更にウイルスメールを送ることで感染を拡大する「マスメール型」と，特定の組織や個人からの情報窃取を目的とした「標的型」に大別することができる[1].

「マスメール型」は愉快犯的なウイルスも含まれており，その脅威は件数のみで判断できない．一方で,「標的型」はその目的から明らかに悪意のある場合が多いと考えられ，今日も重大なセキュリティインシデントを発生させている．そのため，ウイルス届出件数が減少してい

る現在においてもウイルスの脅威は決して減少していない.

なお，ウイルス感染の届出件数は，2005 年の 54,174 件から右肩下がりで減少し, 2010 年には 13,912 件まで減少している[4]．しかしながら，重大な情報漏えい事件はむしろ増加しており[5]，ウイルスの危険性や脅威は件数からはまったく判断できないことが分かる．あらゆる組織が情報化した今，少数の攻撃が過去に例を見ないほどの重大なインシデントを発生させており，脅威の総量はむしろ増大しているといってよい.

2.4. 標的型攻撃メールの攻撃方法とその防衛としての予防接種

標的型攻撃メールの特徴は，前述のように「マスメール型」とは異なり特定の組織や個人を狙っているということである．メールを攻撃対象者に信用させ，添付ファイルを開かせることができれば前段階の攻撃は成功である．次に，添付ファイルがシステムの脆弱性を突いてワーム等を送り込むことができれば攻撃はほぼ成功したことになる．攻撃者としては，まずは前段階の攻撃を成功させなくてはならず，それには対象者を考慮した事前の準備が必須となる．なお，メールヘッダやコードパターンの解析によりある程度の防衛は可能であるが完全に防ぐことはできない[6][7]．ウイルス対策ソフトウェアの定義ファイルに含まれないコードパターンは事前検知が不可能であるが，悪質なコードとの類似性によりある程度の対策は可能である．ただし，必要なメールが誤検知されることもあるため，検知に用いるしきい値設定は一般ユーザには難しい作業となる[8][9].

攻撃者はあらかじめ対象者についての何らかの情報を収集していると考えられる[10]．例えば，対象者の業務内容や人的ネットワーク等である．それらの情報から，攻撃者は信用に足るメール文面を生成する．通知文等の定型文を流用した，やや「マスメール型」的な標的型攻撃メールも存在しているが，対象者像を想定してメールを送り付ける点では，信用に足るメール文面となることには違いはない[11]．その点はフィッシングメールと同じ手法となるが[12]，より文面が巧妙である傾向があるとされる.

また，添付されるファイルは，PDF や Word など日常的に頻繁に利用するファイル形式であるため[13]，対象者が脅威に感じにくいのも対策の難しさのひとつとなっている[14]．メールクライアントのスパムフィルタは統計的な手法を用いる場合については，その効果も限定的なものとなる[15][16].

表 1　階層毎のセキュリティ対策

階層	対応策	効果／欠点
ネットワーク	● ネットワーク監視	○：既知の脆弱性や不審な通信の検知 ×：未知の脆弱性や正常な通信での悪用
	● ネットワーク構成の最適化	○：被害範囲の最小化
	● ファイアウォールの設定（IN/OUT 双方の通信制御） ● プロキシや URL/メールフィルタリング	○:正常でない通信先やプロトコルの悪用を阻止 ×：正常な通信先やプロトコルでの悪用は阻止できない
	● 各種ログのモニタリング	○：被害の早期発見
サーバ	● OS やサーバアプリケーションのセキュリティ修正プログラム適用	○：既知の脆弱性 ×：未知の脆弱性
	● 要塞化	○：未知の脆弱性の被害低減
クライアント PC	● OS のセキュリティ修正プログラム適用 ● クライアントソフトウェア（PDF，ZIP 等）のセキュリティアップデート ● セキュリティ設定による機能制限	○：既知の脆弱性 ×：未知の脆弱性
	● アンチウイルスソフトウェア	○：既知のウイルス ×：未知のウイルス
人	● セキュリティ教育	○：情報セキュリティリテラシーの向上 △：全員には行き届かない
	● インシデントレスポンス体制の確立	○：事故発生時の被害最小化 △：全員には行き届かない
	● セキュリティ事故を想定した訓練	○:体験型学習による免疫効果やエスカレーション体制が機能するか確認 △：全員には行き届かない

そこで，無防備に近い対象者を標的型攻撃メールから防衛するには，「予防接種」としてあらかじめ擬似的に攻撃を体験し，個人もしくは組織に「抗体」を生成するのが肝要である[17]．潜在的対象者が，添付ファイルをむやみに開かいないことや，OS やアプリケーションのアップデートを怠らないなどを習慣とすれば，脅威も自ずと減少すると考えられ，ユーザの意識向上が最も効果的であるとされる[18]．ただし，抗体の効果は長続きしないとも考えられ，定期的に予防接種を行い続ける必要がある．

3. 模擬攻撃の予備実験

本学職員への模擬標的型攻撃メールの送信を控え，著者の受け持つ学生への標的型攻撃メールの予備実験を行った例を報告する．単発のみの配信であるため，予防接種としての効果は算定できないが，一斉送信における解析方法および問題点を確認するために実施した．

3.1. 本学学生に対する標的型攻撃メールの予備実験の実施

一般教養科目および共通科目を履修している学生 196 名（文系学部・18～25 歳）に対して，標的型攻撃メールを模したメールを，大学が提供した学生メールアドレス宛てに一斉送信し，開封状況等を観察した．なお，講義中には，昨今のセキュリティ事情として標的型攻撃メールについて触れており，送信元ドメイン等の確認は怠らないよう注意をしてある．

メールの配信は，学外ドメインを持つホスティングサーバの SMTP とメール配信ソフトである Mail Distributer [19] を利用して一斉送信した．送信元のドメインは普段教員から送られるものとは異なるようにした．危険なメールを判別するためのヒントとするためである．

メールの文面は図 1 のように記載し，期末テストに関連する内容とした．文面冒頭には，メール配信ソフトの文字列差し込み機能を利用して，学生（攻撃対象者）の所属と氏名を入れた．テスト期間に近い時期だったため，学生にとっては極めて関心の高い内容である．添付ファイルを解凍すると，期末テストに関する情報が得られるとの指示を記載している．

添付ファイルは，Windows 実行ファイルをリネームして添付した．実行ファイルは，実行したことを記録するため既定のブラウザを起動して，プリセットされた URL の Web サーバにアクセスする．記録内容は，通常の Web アクセスログおよび実行時に利用している PC 名やログインユーザ名等とした．ここで，添付した実行ファイルをリネームした理由としては，本学学生が利用している Gmail が *.EXE を受け付けないための措置である．

実行ファイルを起動すると，図 2 のようにブラウザ画面が表示される．教育的効果を狙って，一見恐怖心を煽る画像を挿入している．文面としては，「送信元のドメインを確認せず，うかつに添付ファイルを開いてはいけません」という趣旨である．

メールの配信時間は平日午後 7 時とし，その後 24 時間を添付ファイル開封調査時間帯とした．

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 1　模擬標的型攻撃メールの文面

図 2　模擬標的型攻撃メールの起動時に表示される Web 画面

3.2. 予備実験の結果と考察

予備実験の結果，開封者は196名中93名であり，開封率47%となった．当初80%を超えるものと想定していたが大きく下回ることとなった．

しかし，後日の聞き取り調査の結果，未開封者の中には，そもそも大学が提供しているメールを利用していない者がいることが判明した．また，開封調査時間帯の24時間では，アルバイト等でメールを確認できなかったケースがあったことも分かった．学生の生活リズムは，各人で時間的に大きな振れ幅があるため，それらを考慮した集計が必要だったと思われる．

ただし，開封調査時間帯を多く取ると二重開封をカウントしてしまう可能性が高まる．そのため，職員に対する予防接種においては，二重カウントを技術的に防ぐ仕組みが必要であることが分かった．さらに，実行ファイルをリネームできなかった学生もおり，潜在的な開封者も確認できたため，より簡単に開封者をカウントできる仕組みも必要であった．

なお，被験者の学生の感想としては，おおむね次のようなものであった．多数の同様の意見があったもののみ列挙する．

- 授業では標的型攻撃メールのことは聞いていたが，まさか自分に来るとは思わなかった．
- 焦って開いてしまった．
- 送信元ドメインなど気に留めなかった．
- 実際に攻撃を受けてみて，防衛がたいへん難しいことが分かった．

特に，最後に記載した感想は，標的型攻撃メールの予防接種を実施する前提として極めて有用だと考えられる．

以上の予備実験による反省点を踏まえ，職員に対する予防接種を実施した．

4. 標的型攻撃メールの予防接種

本学職員に対する標的型攻撃メールの予防接種は，株式会社ラック [20] の協力を仰ぎ，予備実験で得られた反省点を改善した上で実施した．また，事前に学内上位組織による承認を得た．

4.1. 予防接種の実施概要

予防接種の実施概要を表 2 に示す．定時出勤前の8:00を目途に，事前に決定したメールアカウントへ予防接種となる添付ファイル付きメールを配信する．その後，同日夕方には開封者データの集計を打ち切る．同じフローで1週間の時間を置いて実施する．2回行う理由としては，初回からの予防接種効果を確認するためである．

なお，対象は200名であるが，一部は共用アドレス化しているため，同一メールを複数人が閲覧する可能性がある．後述するWebビーコンの仕様により開封者数を二重カウントすることはない．しかし，共用する誰かが開封するとカウントされてしまう．

予防接種後は，全職員向けにセキュリティ講習を実施し標的型攻撃メールについてはもちろんのこと，近年のセキュリティ事故などについての知識を新たにしてもらうこととした．

表 2　予防接種の概要

項目	内容
対象	本学事務系職員200名（常勤・契約職員・パート職員） ただし，メールアカウントは複数職員で共用している場合がある．
目的	擬似的な標的型メール攻撃を実施して組織としての開封率などの指標を調べる．また，これを体験することで各個人に耐性をつけ，その結果として組織の耐性を向上させる
方法	添付ファイルには，マルウェアの代わりにWord 文書に Web ビーコンを仕込んだ擬似攻撃メールを配信し，Web ビーコンのログから添付ファイルの開封状況を計測する．
分析	Web ビーコンから得られた基礎データから以下の解析結果を得る． 開封者数／開封日時／開封率／非開封率／時系列の開封状況／対象者の属性 等
実施日時	・第1回メール配信 2012年3月7日 8:00 模擬訓練であることを通知 同日 19:16 ・第2回メール配信 2012年3月15日 8:00 模擬訓練であることを通知 同日 16:18

4.2. 模擬攻撃メールの文面

メールの文面は，対象者に攻撃であることを感じさせないことが重要である．今回は，表 3 および 表 4 に示すように，社会情勢や情報セキュリティ事情に合わせた内容とした．

送信元のドメインは，本学職員にとっては初見であり，これまでの情報セキュリティ講習の経験のある者であれば当然注意するはずの情報である．メールクライアントは職員で統一したものを利用しており，送信元ドメインの確認は容易なインターフェースとなっている．

標的型攻撃メールを判別するには，以下について意識しておく必要がある．

- 差出人の名前やアドレスが，見慣れないものである．
- 組織内の話題なのに，外部のメールアドレスから届いている．
- 添付ファイルを開くよう不自然に誘導している．
- 急がせて，メールの内容を吟味させまいとしている．
- 差出人の署名や名乗りが無いか曖昧である．
- 架空の差出人の名前や組織名を名乗っている．

表 3　第 1 回メール配信の文面

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

表 4　第 2 回メール配信の文面

Subject	至急： PDF に関する注意喚起
From	情報化推進本部 <security@joshisu. jp>
Message	各位 最近，PDF ファイルを送りつけることで，ソフトの未発見のセキュリティホールを突いて侵入を試みる事例が激増しています． 多くの場合は適切な設定をしておくことで危険を回避できるものですので，添付の確認手順にしたがってお手元の PC の設定を至急点検し，より安全な設定にしていただきますようにお願いします． 情報化推進本部
Attach	点検手順. doc

4.3. Web ビーコンによるロガー

予備実験では，実行ファイルにより開封者データをロガーしたが，予防接種においては Web ビーコン [21] を Word ファイルに埋め込んだ．さらに，各添付ファイルには特定の ID を仕込むことで個人の特定を確実にした．Web ビーコンを仕込むことで Word ファイルの挙動が変わることはなく，職員（対象者）にとっては通常の文書を読むのと何ら変わることはない．

ところで，職員が利用する PC にはセキュリティ対策ソフトが導入されており，通信の常時監視により不正なトラフィックはブロックする仕様である．Web ビーコンの通信もブロック対象になる可能性もあったが，本学の使っているセキュリティ対策ソフトでは反応しなかった．

参考として図 3 に Web ビーコンを仕込んだ Word ファイルを DUMP したキャプチャを示す. 四角で囲った部分から分かるように，ファイルを開くと特定の URL にアクセスするようになっている．

図 3　Web ビーコンを含んだ Word ファイル

4.4. 訓練であることの周知

予防接種は業務中に実施するため，それによって業務を混乱させてはならない．すみやかに模擬訓練であることを知らせるために，添付ファイルには 図 4 のように「標的型偽装メールの実施ついて」として，模擬訓練であることを学内承認済みであることと共に明記した．この通知を行わないと，情報担当部署に大量の問い合わせが寄せられたり，苦情や思わぬトラブルが発生する可能性がある．

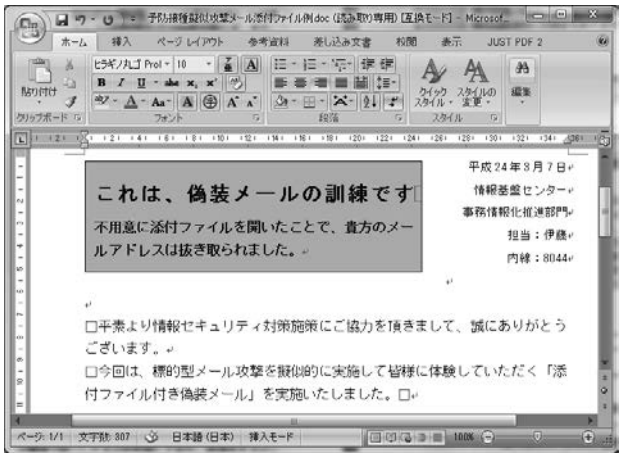

図 4　訓練であったことを明示

5. 結果と考察

予防接種当日，大きな混乱は無かったものの，職員の中には不審メールに気づき，開封の可否を情報担当部署

に問い合わせるケースが 5 件ほどあった．また，部署によっては先に開封してしまった者が他者に開封を留まらせるなどのケースもあった．

5.1. 時系列の開封率

図 5 に時系列の開封状況を示す. 本学の開封状況を比較するため，他組織平均のデータを[22]より引用した．他組織については，表 5 における他組織 A ～ E であり，いずれも同様の標的型攻撃メール予防接種を実施した日本国内の一般企業である．

図中において，本学の開封率は ◆ で示し，他組織平均は ○ で示している．開封者数比（縦軸）は，擬似攻撃メール配信時刻から 10 分刻みでその 10 分間の内に開封した被験者が全開封者に占める比率を示している．経過時間（横軸）は，擬似攻撃メール配信時刻から 1 時間刻みでの経過時間を示している．

他組織平均では全開封者のうちの半数が開封するまでに，擬似攻撃メール配信後およそ 30 分間しかかかっていないことがわかる. 今回の配信は 8:00 に行っており，平均累積開封者数比の傾向より緩やかな経過をたどるものの，1 時間経過した時点で今回の開封者のうちの 6 割程度がすでに開封している．一般的にも，メールを受信した直後に多くの開封者が開封しているという傾向があり，標的型メール攻撃への対策として人間が介在して情報集約するような仕組みでは間に合わない可能性が高いと考えられる．

やはり，スパム対策などの入口対策・ OS やソフトウェアのアップデートなどのデスクトップでの対策・DLP（Data Leak Prevention：情報漏えい防止策） などの出口対策を組み合わせて実施する必要があるといえる．

5.2. 各開封パターンによる開封率

開封率は各開封パターンで集計した. 各パターンとは，第 1 回および第 2 回の開封者，両方の回の開封者，第 1 回もしくは第 2 回のみの開封者，非開封者である．表 5 では全被験者を対象にこれら各パターンの開封率を他組織平均の情報と併せて示している．

表 6 は, 予防接種実施後に行ったアンケート（表 7 および 表 8 参照）の回答者のみを対象に集計した結果である．なお, アンケート回答者数は 200 名中 29 名であった．

今回の予防接種では 1 回目は 40.0%，2 回目は 28.5% の開封率であり，他組織平均と比較して高い傾向にあった．特に，1 回目 2 回目とも開封した被験者の割合が全体の 2 割近くであり，他組織平均と比較して高い値であるといえる．

今回の予防接種は初めてだったため，標的型攻撃メールへの耐性が低い被験者が多い可能性があり，継続した注意喚起や教育訓練の実施など対人間向けの教育を充実させることで組織の意識レベルのさらなる向上を図る必要がある．

また，攻撃が実際に行われた場合，それが届いたことを規程に従って報告させ，それを集約して警告を出すような対応策では時間的に間に合わない．

さらに，対象者からのアンケートでも業務関係のメールは違和感を覚えても開封する傾向が判明しており，被害を最小限にとどめるためには人的対策と組み合わせてスパム対策などの入口対策といった多層防御の考え方による防御態勢を整えることが求められる．

5.3. 被験者属性と開封率

表 7 に本学の被験者アンケート結果について, その選択肢毎に各回配信の開封者数・非開封者数を集計した結果を示す．どのグループの開封率が高いといった，有意な差や傾向は認められなかった．

他組織では，メール習熟度・平日 1 日当たりのメール数・1 時間当たりの処理メール通数・予防接種経験の有無・業務関連度 等で強い相関関係を示した例もある．しかしながら，本学ではこれらの属性については強い相関は認められなかった．

年齢層についてはやや有意な結果が出ており，全年齢層の中で 30 代の開封率が低いことが分かる. この年代は IT と業務に熟練した人材が多く，セキュリティに関する知識も十分であった可能性がある．20 代については，勤続期間の短いパートタイム職員が含まれるため，IT や業務に関して未熟である場合が考えられる．高齢の職員については，情報セキュリティについて知識はもとより，IT 全般に関するリテラシーの意識に乏しい可能性が極めて高い[23].

5.4. 被験者の感想

表 9 にアンケートの回答から得られた被験者の感想の一部を挙げる．職員に対しては，標的型攻撃メールの危険性について，日常的にポスターや講習等で周知していた．そのため，その存在自体は知っていたものの，実際の攻撃には無力であったとの感想が散見された．

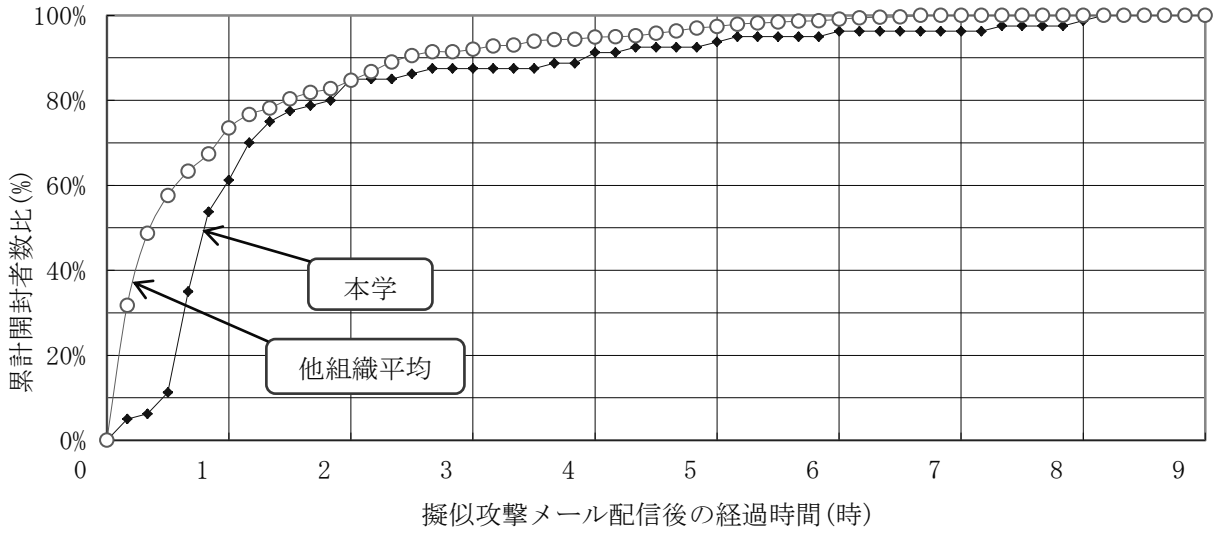

図 5　時系列開封状況

表 5　各開封パターンによる開封率（全被験者）

	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 6　各開封パターンによる開封率（アンケート回答者）

	アンケート 回答者数	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	29	14 48.3%	11 37.9%	6 20.7%	8 27.6%	5 17.2%	10 34.5%	21.4%
他組織 A	1006	240 23.9%	86 8.5%	45 4.5%	195 19.4%	41 4.1%	725 72.1%	64.2%
他組織 B	182	40 22.0%	4 2.2%	2 1.1%	38 20.9%	2 1.1%	140 76.9%	90.0%
他組織 C	47	15 31.9%	4 8.5%	2 4.3%	13 27.7%	2 4.3%	30 63.8%	73.3%
他組織 D	32	11 34.4%	8 25.0%	6 18.8%	5 15.6%	2 6.3%	19 59.4%	27.3%
他組織 E	37	20 54.1%	5 13.5%	1 2.7%	19 51.4%	4 10.8%	13 35.1%	75.0%

表 7　被験者（職員）属性と開封率

設問[*1]	選択肢	第 1 回配信			第 2 回配信		
		開封	非開封	開封率	開封	非開封	開封率
性別 #1	男性	8	10	44%	8	10	44%
	女性	6	4	60%	3	7	30%
年齢層 #2	20 歳未満	0	0	0%	0	0	0%
	20 歳代	4	2	67%	4	2	67%
	30 歳代	2	6	25%	1	7	13%
	40 歳代	4	4	50%	4	4	50%
	50 歳代	3	2	60%	2	3	40%
	60 歳以上	1	0	100%	0	1	0%
職務 #3	役員	0	0	0%	0	0	0%
	管理職	2	1	67%	1	2	33%
	サービス・ CS	0	0	0%	0	0	0%
	事務職	11	12	48%	9	14	39%
	その他技術者	1	1	50%	1	1	50%
メール処理の習熟度 #4	非常に熟練	0	0	0%	0	0	0%
	熟練している方	1	1	50%	0	2	0%
	平均的	11	12	48%	9	14	39%
	あまり熟練していない	2	1	67%	2	1	67%
	ほとんどできない	0	0	0%	0	0	0%
メール数 #5	25 通/ 日未満	10	9	53%	8	11	42%
	25 以上 100 未満	4	4	50%	3	5	38%
	100 以上 250 未満	0	1	0%	0	1	0%
	250 以上	0	0	0%	0	0	0%
メールの処理時間 #6-1	2 時間/ 日未満	9	4	69%	7	6	54%
	2 以上 4 未満	3	9	25%	3	9	25%
	4 以上	2	1	67%	1	2	33%
1 時間当たりのメール処理数 #6-2	25 通/時未満	12	12	50%	9	15	38%
	25 以上 100 未満	2	2	50%	2	2	50%
	100 以上 250 未満	0	0	0%	0	0	0%
	250 以上	0	0	0%	0	0	0%
予防接種経験 #7	経験済	0	2	0%	0	2	0%
	未経験	14	12	54%	11	15	42%
業務関連度 #9	非常に強い関連	2	2	50%	3	2	60%
	どちらかと言えば関連	7	8	47%	5	8	38%
	わずかに関連	5	3	63%	3	6	33%
	無関係	0	1	0%	0	1	0%

*1 各設問の #(数字) は 表 8 の設問 No. に相当する

表 8　被験者アンケートの設問例

No.	感　想
1	あなたの性別を選択してください.
2	あなたの年齢層を教えてください.
3	あなたの職務は以下のどれに最も近いですか？
4	業務上の連絡を電子メールで送受する場合を想定すると，あなたは電子メールの取り扱いにどの程度熟練していますか？
5	あなたは業務上のメールを送受信合わせて何通程度取り扱いますか？
6	あなたは業務上のメールをどの程度の時間をかけて処理していますか？
7	あなたは過去に IT セキュリティ予防接種を経験しましたか？
8	あなたは今年度の第 1 回配信の擬似攻撃メールにどのように対応しましたか？
9	第 1 回配信の擬似攻撃メールの本文や表題は，あなたの担当業務とどの程度関連していましたか？
10	あなたは今年度の第２回配信の擬似攻撃メールにどのように対応しましたか？
11	第２回配信の擬似攻撃メールの本文や表題は，あなたの担当業務とどの程度関連していましたか？
12	予防接種について，ご感想・ご意見などを自由にご記述ください.

表 9　被験者の感想

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 回目の偽装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.

*1 各感想は 表 8 の設問 No. 8, 10, 12 から採取した

6. おわりに

今後，大学においても標的型攻撃メールを懸念する事態になりかねない．大量の学生に関する個人情報を擁しているため情報漏えいのリスクは計り知れない．また，悪意のある者が自己の成績証明を書き換えることさえも考えられる．いずれのセキュリティインシデントも大学が長い時間を掛けて築き上げてきたブランドを貶める極めて深刻な事態である．われわれは，そのような事態を防がなければならい．

しかしながら，標的型攻撃メールは統一的に防衛することは不可能である．また，唯一の対策である予防接種の効果は，時間が経るにつれ限定的な効果しか発揮しない．大学組織は職員の出入りも少なくないため，年に複数回の実施は不可避であろう．

標的型攻撃メールは，情報部門と現場の職員との協働無くして防ぐことはできない．今後，すべて教職員に対して，情報セキュリティ全般の意識向上対策を行いつつ，絶対に漏えいしてはならない情報は LAN 経由でアクセスできないなどの対策を取る必要もある．さらには，学生に対する情報セキュリティ教育も必要であると考える．

参考文献

[1] 寺田真敏, “標的型メールがやってきた”, 情報処理, 51(3), pp.270-274, 2010

[2] 三森春佳, 阿部公輝, “ふるまいに着目した未知の亜種ウイルスの識別”, 電子情報通信学会技術研究報告（情報セキュリティ）,108(162), pp.1-7, 2008

[3] 高木浩光, “ソフトウェアのセキュリティ欠陥は誰が直すのか”, http://www.ipa.go.jp/security/fy14/events/ipa-winter2003-takagi-dist.pdf, 独立行政法人産業技術総合研究所, 2003

[4] IPA セキュリティセンター, “コンピュータウイルスの届出状況”, http://www.ipa.go.jp/security/txt/list.html, 独立行政法人情報処理推進機構, 2012

[5] 大谷尚道, “個人情報漏えいインシデントを減らすためには”, NTT データ, NTT セキュリティ被害調査 WG, Vol27, 2008

[6] 関根冬輝, 村井純, “メールヘッダ解析によるなりすましメールの検知手法の提案”, 慶応大学環境情報学部卒業論文, 2012

[7] 碓井利宣, 村井純, “コードの特徴に基づく悪性プログラムの分類”, 慶応大学環境情報学部卒業論文, 2012

[8] Georgios Sakkis, et at al., “Stacking classifiers for anti-spam filtering of e-mail”, Proceedings of the 6thConference on Empirical Methods in Natural Language Processing(EMNLP 2001), pp.40-50, 2001.

[9] Jose M.Gomez Hidalgo, “Combining Text and Heuristics for Cost-Sensitive Spam Filtering”, Proceedings of CoNLL-2000, pp.99-102, 2000

[10] 相馬基邦, “標的型攻撃への対処法 バックドア通信を遮断しウイルスの活動抑え込む”, 日経 systems (224), 40-45, 2011

[11] 山口健太郎, 小宮山功一朗, 内田勝也, “ユーザへの予防接種というアプローチによる標的型攻撃対策-2”, 情報処理学会第 71 回論文集, pp.349-350, 2009

[12] 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

[13] 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

[14] 八津川直伸, 石野貴子, “重大な脅威に対するセキュリティ設計手法の考察”, UNISYS TECHNOLOGY REVIEW 第 98 号, 2008

[15] 車古正樹, 松平拓也, 井町智彦, 中野三智子, 西川直樹, “Spam フイルタに関する統計”, 学術情報処理研究, No9, 2005

[16] 松平拓也, 車古正樹, 井町智彦, 西川直樹, “Spam メール及びウイルスメール対策システムの構築と運用”, 学術情報処理研究, No9, 2005

[17] 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

[18] 田村佑輔, 甲斐俊文, 佐々木良一, “ユーザ標的型 Web サイト改ざんに対する検索エンジンを用いた検知手法の提案”, 情報処理学会論文誌, 51(1), 191-198, 2010

[19] Mail Distributor ver.6.4, http://www.woodensoldier.info/soft/md.htm

[20] 株式会社ラック, http://www.lac.co.jp/

[21] Web ビーコン, http://d.hatena.ne.jp/Kango/20111024/1319462526

[22] 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

[23] 宮本貴朗, “大学におけるセキュリティ対策”, 総合情報センター年報情報. 2002, 8, pp.4-11