東北大学における標的型攻撃メール対応訓練

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

Training for Responding to Targeted Email Attacks 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 27 年度から標的型攻撃メール対応訓練（以下、メール訓練）を実施しているが、年度ごとに訓練結果を評価し、次回の訓練に反映することでブラッシュアップを図っている。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 27 年 6 月に発生した日本年金機構の事案を受けて、平成 27 年度から標的型攻撃に対応するためのメール訓練を実施している。初年度は、事務系職員約 1,600 人を対象に外注で実施したが、次年度となる平成 28 年度以降は、全教職員約 12,000 人を対象に内製で実施している。毎回単調な訓練内容では、メール訓練の有効性が薄まってしまう可能性があるため、年度ごとに結果を評価し、次回に反映することでブラッシュアップを図っている。内製によって、予算・コストによる制約を抑えながら臨機応変に対応できることにもつながっている。

本稿では、このメール訓練の取組みについて紹介する。

2 メール訓練の概要

2.1 メール訓練の目的

メール訓練の目的は、身近に起こりうる危機を認識し、典型的な攻撃パターンを体験し、見分ける知識を身に付けることとした。

2.1 メール訓練の流れ

メール訓練は、事前周知、訓練本番、事後アンケートという流れで行った。

事前周知では、訓練の目的、実施期間、訓練手順、メール受信者を騙す手口、それを見抜くための着眼点等を周知した。

訓練本番では、全教職員に付与されている東北大メールアドレス宛てに疑似的な標的型攻撃メール（以下、攻撃メール）を送信した。メール受信者が添付ファイル又は URL リンクをクリックした場合、誰がクリックしたのか集計できるようにした。また、クリックした際には、ウェブサイトが表示されるようにし、このメールが訓練であることを伝えて、メール受信者を騙す手口や、それを見抜くための着眼点等を再確認するように促した。なお、本学には、全教職員からの報告を一挙に受理できるほどの体制がまだ無いため、攻撃メール受信時の報告や、クリック時のネットワーク隔離及び報告作業は訓練に含めなかった。

全教職員分のメール送信が完了してから数日後に、訓練完了メールを一斉送信し、今回のメール受信者を騙す手口や、それを見抜くための着眼点等を周知しつつ、事後アンケートを依頼した。

2.2 各年度のメール訓練の概要

表 1 に各年度のメール訓練の概要を示す。

3 平成 27 年度のメール訓練

3.1 攻撃メール

平成 27 年度の訓練では、攻撃メールを送信した。情報システムの利用環境が把握できる事務系職員が対象であり、外注したこともあって、トラブルもなく訓練が完了した。

表１　各年度のメール訓練の概要

	平成 27 年度		平成 28 年度	平成 29 年度
対象者	事務系職員		全教職員	全教職員
対象人数	1,619		12,206	12,213
回数	1 回目	2 回目	—	—
訓練期間	2 日間	3 日間	12 日間	22 日間
メール文面	1 種類	1 種類	2 種類	13 種類
送信方法	一括	一括	1 日 2,000 通 （東北大 ID 順）	1 日 1,000 通 （ランダム）
メール形式	URL リンク	添付ファイル	添付ファイル	URL リンク
開封数	330	174	639	1,686
開封率	20.4%	10.7%	5.2%	13.8%
外注/内製	外注		内製	内製
費用	約 140 万円		0 円	約 1 万円

4 平成 28 年度のメール訓練

4.1 攻撃メール

平成 28 年度は、前年度実施のノウハウを生かして内製にて訓練を行うこととした。事務系職員とそれ以外に分類し、表２に示す 2 種類の攻撃メールを送信した。

差出人については、IPA [1]によると標的型攻撃メールの 71%がフリーメールから送信されていること、並びに日本年金機構 [2]によると、平成 27 年 6 月の個人情報流出事案においては標的型攻撃メールの送信元はフリーメールアドレスであったことから、フリーメールアドレスを選定した。

メール本文の「実名差し込み」については、日本年金機構[2]によると、平成 27 年 6 月の個人情報流出事案においては非公開のメールアドレスに対して実名を差し込んだメールが送信されたことから、実名差し込みを取り入れることにした。

添付ファイルについては、警察庁 [3]によると標的型攻撃メールの添付ファイルは圧縮形式のファイルであることがほとんどであり、その中には「exe」の実行形式ファイルが最も多く用いられていることから、これを取り入れることにした。

4.2 内製作業

添付ファイルについては、アクセスした人を特定するウェブサイトを PHP で用意し、そのサイトにアクセスする exe ファイルをフリーソフトの「Hot Soup Processor」で作成した。一人一人異なるパラメータを設定しないとクリックした人を特定できないため、人数分のファイルを作成することとなったが、フリーソフトの「UWSC」を用いて短時間で作成した。

メール送信については、Microsoft 社の Excel マクロ及び Outlook を使用して、順次送信した。

4.3 評価

フリーメールについては、添付ファイル（zip in exe）が送信できるものが少ないこと、そして Outlook による SMTP 送信ができるものが少ないことにより、訓練に利用できるものを見つけ出すのに苦労した。また、送信数の制限がかけられているが、その閾値が非公開のために、試行錯誤で検証することになってしまった。結果的には、フリーメールは訓練には不適切であった。

添付ファイル（zip in exe）についても、Windows 以外の機器では、実行しても何も反応せず、訓練であることを明示した画面も表示されないため、混乱を引き起こすことになってしまった。また、東北大メールアドレスから普段使用しているメールアドレスに転送している場合、転送時に添付ファイルがエラーに引っかかり、到達しないこともあった。結果的には、様々な情報機器を使用している全教職員に対しては、添付ファイル方式は不適切であった。

訓練開始日に、メール受信者から各部局の情報システム担当者への問い合わせが一挙に発生し、日常の業務に影響してしまった。各部局の情報システム担当者に対しては、事前に攻撃メールの具体的な内容を周知しておくべきであると認識した。

図３に示す通り、訓練後半にかけて、開封率が

右肩下がりになっていることが分かる。これは、同じ文面のメールを数日間に渡って送信しているため、時間が経つにつれて、まだ受信していない人に対しても、メール内容が知れ渡ってしまったことが原因とみている。事後アンケートによると、メール訓練に引っかかった人は満足度が高く、そうではない人は低い傾向があったため、これは大きな問題点であった。数日間に分けて送信するならば、メール文面は日々変更するべきであると認識した。

表 2　平成 28 年度の攻撃メール

	1 回目	2 回目
件名	人事異動内示について	科研費について
差出人	東北大学<ukagiadukohot@フリーメール 5 種類>	
本文	●●様（実名差し込み） 参考までに、人事異動案内示を転送します。 ご確認のほどよろしくお願いいたします。	●●様（実名差し込み） 先日の教授会で議題になった件について、ご意見を伺いたく、資料を送付させて頂きます。 ご確認のほどよろしくお願いいたします。
添付	人事異動内示.zip（人事異動内示.exe）	資料.zip（資料.exe）

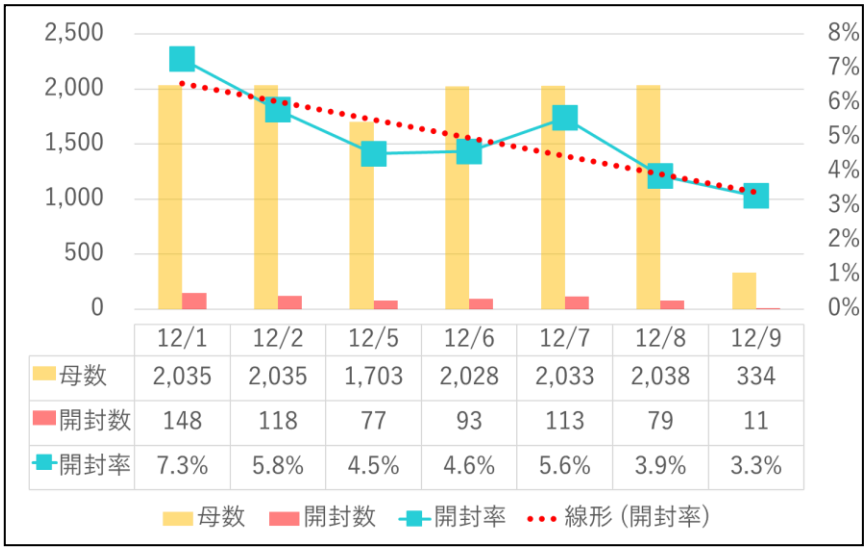


図 3　平成 28 年度の開封率の推移

5 平成 29 年度のメール訓練

5.1 攻撃メール

平成 29 年度の訓練では、前年度の反省を活かし、表 4 に示す 13 種類の攻撃メールを送信した。

ウェブサーバ及びメールサーバ、並びに本学公式の「tohoku.ac.jp」を模倣した「tohoku-ac-jo.info」というドメインをレンタルし、差出人のメールアドレス及び URL リンクとして使用した。

差出人の苗字は、知人からのメールだと錯覚させるため、本学の教職員に多い苗字を集計し、上位から順番に使用した。

HTML 形式のメールにして、本学のロゴマークを挿入した。これは、本学に実際に到達したことのあるフィッシングメールで用いられていた手口であったため、取り入れることにした。

5.2 事前周知

事前周知において、各部局の情報システム担当者に対して、訓練本番で送信する攻撃メールの内容も周知することにした。

5.3 内製作業

前年度の添付ファイルと同様に、アクセスした

人を特定するウェブサイトを PHP で用意し、そのサイトにアクセスするための URL リンクを設定した。メール送信についても前年度と同様に、Microsoft 社の Excel マクロ及び Outlook を使用して、順次送信した。

5.4 評価

レンタルのメールサーバから送信したため、前年度のように送信制限などのトラブルにかかることもなく、スムーズに実施できた。

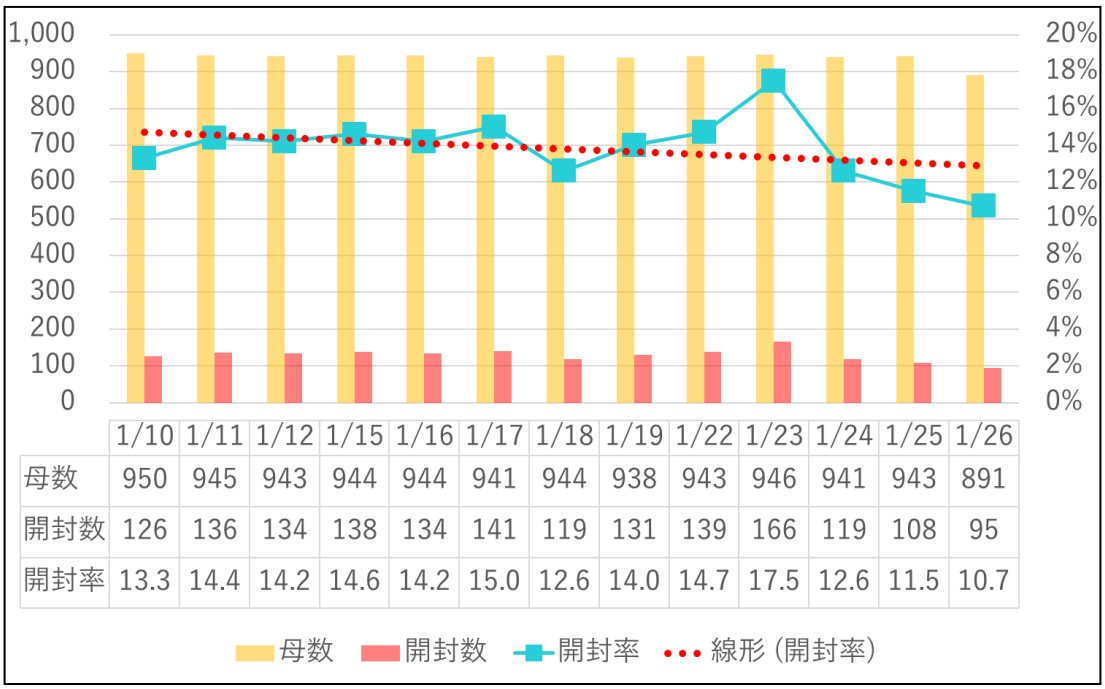
また、差出人の苗字については、上司だと錯覚して不用意にクリックした人も出ており、名前ではなくメールアドレスを確認することの意識付けにつなげることができたと考えられる。

図 5 に示す通り、訓練後半にかけても開封率が右肩下がりにならなかった。従って、全期間を通して有効な訓練を実施することができた。

表 4　平成 29 年度の攻撃メール

件名	【A】
差出人	【B】
本文	 【C】です。お疲れ様です。 先日お話しした【A】に関する資料が手に入りましたので PDF 化しました。 至急、こちらからダウンロードください。 http://www.tohoku-ac-jp.info/drive/?xxxxxxxxx.pdf 取り急ぎ。
補足	送信日毎に【A】,【B】,【C】を次表の通りに置換

送信日	【A】	【B】	【C】
10 日（水）	指定国立大学	東北大学 佐藤 <sato@tohoku-ac-jp.info>	佐藤
11 日（木）	日英表記	東北大学 鈴木 <suzuki@tohoku-ac-jp.info>	鈴木
12 日（金）	共同研究講座	東北大学 佐々木 <sasaki@tohoku-ac-jp.info>	佐々木
15 日（月）	中期目標・中期計画	東北大学 伊藤 <ito@tohoku-ac-jp.info>	伊藤
16 日（火）	運営企画会議	東北大学 髙橋 <takahashi@tohoku-ac-jp.info>	髙橋
17 日（水）	自動車入構ルール	東北大学 阿部 <abe@tohoku-ac-jp.info>	阿部
18 日（木）	グローバルイニシアティブ構想	東北大学 高橋 <takahashi@tohoku-ac-jp.info>	高橋
19 日（金）	時間外労働縮減	東北大学 齋藤 <saito@tohoku-ac-jp.info>	齋藤
22 日（月）	寄付講座	東北大学 加藤 <kato@tohoku-ac-jp.info>	加藤
23 日（火）	部局評価	東北大学 千葉 <chiba@tohoku-ac-jp.info>	千葉
24 日（水）	競争的資金等公募情報	東北大学 遠藤 <endo@tohoku-ac-jp.info>	遠藤
25 日（木）	オープンキャンパス	東北大学 小林 <kobayashi@tohoku-ac-jp.info>	小林
26 日（金）	大学発ベンチャー	東北大学 菅原 <sugawara@tohoku-ac-jp.info>	菅原



	1/10	1/11	1/12	1/15	1/16	1/17	1/18	1/19	1/22	1/23	1/24	1/25	1/26
母数	950	945	943	944	944	941	944	938	943	946	941	943	891
開封数	126	136	134	138	134	141	119	131	139	166	119	108	95
開封率	13.3	14.4	14.2	14.6	14.2	15.0	12.6	14.0	14.7	17.5	12.6	11.5	10.7

図 5　平成 29 年度の開封率の推移

6 おわりに

本稿では、平成 27 年度から実施しているメール訓練の取組みについて紹介した。

メール訓練の内製化により、前年度の実施結果を反映した手直しが、予算・コストによる制約を受けることなく対応できている。また、毎回単調な訓練内容では、メール訓練の有効性が薄まってしまう可能性があるため、年度ごとに結果を評価し、次回に反映することでブラッシュアップを図っている。

このような本学の取組みが、他機関において参考になれば幸いである。

参考文献

[1] IPA（独立行政法人情報処理推進機構）技術本部 セキュリティセンター、サイバー情報共有イニシアティブ（J-CSIP） 2014 年度 活動レポート、P16、独立行政法人情報処理推進機構、2015

[2] 日本年金機構 不正アクセスによる情報流出事案に関する調査委員会、不正アクセスによる情報流出事案に関する調査結果報告、日本年金機構、別添資料 3-3、2015

[3] 警察庁広報資料、平成 28 年上半期におけるサイバー空間をめぐる脅威の情勢等について、警察庁、P3-4、2016