京都大学における標的型攻撃メールへの対応訓練

片桐 統 [1)]，斎藤 紀恵 [1)]，石橋 由子 [1)]
1） 京都大学　企画・情報部　情報基盤課
i-s-office@iimc.kyoto-u.ac.jp

The response training against the E-mails of the APT in Kyoto University

Osamu KATAGIRI [1)], Norie SAITO [1)], Yoshiko ISHIBASHI [1)]
1） IT Service Division, Planning and Information Management Department, Kyoto University

概要

2015 年 6 月に日本年金機構に対する標的型攻撃[1]により、多数の個人情報が漏洩する事案が報道され、その後高等教育機関においても標的型攻撃への対策は重要な情報セキュリティの課題となっている。京都大学では、標的型攻撃への対策の一環として、教職員が標的型攻撃メールを受け取った際に適切に対応できるよう、2015 年度は職員を対象に対応訓練を実施した。本稿では、この訓練ついて紹介する。

1　はじめに

2015 年 6 月に日本年金機構に対する標的型攻撃[1]により、多数の個人情報が漏えいする事案が報道された。その後、官公庁・高等教育機関を含め、標的型攻撃による情報漏えい等の多数のセキュリティインシデントが報道されており、高等教育機関においても標的型攻撃への対策は重要な情報セキュリティの課題となっている。

京都大学（以下、本学という。）においては、本稿執筆時点までにおいて、幸い標的型攻撃により個人情報等が漏えいする事案は確認されていないが、同様の事案を未然に防ぐために、教職員が標的型攻撃メールを受け取った際に適切に対応できるよう、訓練を実施することが緊急の課題である。

本学の職員は約 6500 名であり、事務職員、技術職員、教務職員、医療系職員（看護師等）などの職種で構成される。またそれぞれ職種に、常勤職員、非常勤職員、派遣職員など多彩な雇用の形態がある。

本稿では、本学における標的型攻撃への対策の一環として、これら本学の職員を対象に標的型攻撃メールに模したメールを送付し、標的型攻撃メールを受け取った際に適切な対応ができるように意識づけを行うとともに、ウイルス感染が疑われる際の連絡対応の訓練として実施した、標的型攻撃メールへの対応訓練について紹介する。

2　標的型攻撃メールへの対応訓練を実施する目的

本学において、標的型攻撃メールへの対応訓練を実施するにあたり、以下の点を目的として設定した。

(1) 訓練対象者が、標的型攻撃と疑われるメールを受信した際、添付ファイルや URL を開封せず削除し、訓練対象者が適切に連絡を

行えるようにする。

(2) 添付ファイルやURLを開封してしまいウイルスに感染した可能性が高い場合、本学に決められた連絡要領に従い、訓練対象者及び情報セキュリティ対応関係者が適切にインシデント対応を行えるようにする。

3　標的型攻撃メールへの対応訓練の実施全体像

標的型攻撃メールへの対応訓練のフローをFig. 1 標的型攻撃メール訓練フローに示す。

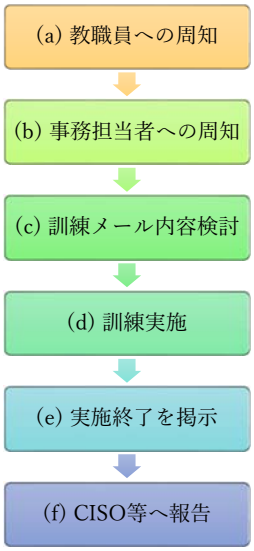

Fig. 1 標的型攻撃メール訓練フロー

(a) 事前に教職員に対し、不審なメールを受信した際の対応方法を周知し、訓練を実施する旨を通知する。

(b) 各部局の情報セキュリティの連絡担当者に、不審なメールを受信した又はウイルスに感染した旨の報告があった場合の対応を周知する。

(c) 訓練メールの内容を検討する。

(d) 訓練メールの送信を実施する。今回の訓練では訓練対象者に3回異なる内容で送信した。

(e) 最後に送信した訓練メールの集計期間終了後、全学掲示板において、訓練メールの内容とともに、実施終了を掲示する。集計期間とは、訓練メールを送信後に、訓練対象者が確認することを待つ期間で、今回の訓練では1週間の設定とした。

(f) CISO 及び部局長会議へ訓練結果を報告する。

4　事前周知の内容

4．1　教職員への周知

まず、教職員には標的型攻撃メールを受け取った際にどのような点に注意し、行動すべきかを周知する必要がある。このことから、訓練実施に先駆けて、標的型攻撃メールの概要と対応について、次の内容を教職員に周知した。

(1) 標的型攻撃メールとは

標的型攻撃メールの説明と、攻撃のパターンを図示。

(2) 標的型攻撃メールの例

具体的な標的型攻撃メールの例を示す。

(3) 怪しいメールを見分けるポイント

IPA が作成している「標的型攻撃メールの例と見分け方」[2]を参考に、見分けるポイントを表で示す。

(4) ウイルスが添付されている可能性のある疑わしいメールを受信したときは

疑わしいメールは、添付ファイルの開封、URL のクリックを決して行わず、セキュリティ対策掛まで連絡するように記載。

(5) OS やウイルス対策ソフト等の更新は万全ですか？

ウイルス感染を未然に防ぐため、一般的なセキュリティ対策や、機密・個人情報を取り扱う際の対策を記載。

(6) ウイルス感染の可能性がある場合の対応

ウイルス感染の可能性がある場合の対応などを記載。(以下は、内容の抜粋)

- ネットワークから切り離し、部局窓口とセキュリティ対策掛へ連絡すること
- ウイルス対策ソフトで完全スキャンをすること
- OS をクリーンインストール

・ 報告書の提出

(7) インシデント対応連絡手順

学内の連絡手順を図示したもの。

４．２　各部局の連絡担当者への対応の周知

本学におけるインシデント対応は、第一義的には各部局において行うことになっている。標的型攻撃メールに関する教職員からの連絡も、部局の情報セキュリティに関する連絡担当者に入ることになる。この際に連絡担当者がどのように対応を行うのかについて、対応訓練実施に先駆けて周知した。

周知の際に特に注意を払ったのは、対応訓練のメールによる連絡であるのか、本当の標的型攻撃メールであるのかが、連絡担当者では見分けがつかない点である。これについては、訓練実施の目的(2)を念頭に、実際のウイルス感染時の対応を取る手順を示した。

５　訓練メールの準備と送信

５．１　訓練メール内容検討時に注意した点

訓練メールは、訓練対象者に 3 回送信した。内容を検討するにあたり、以下の点に注意を払った。

(1) 通常業務へ影響を与えない

実際の事務連絡等の文書を改変することや、実際にある部署名等を使用すると、意図せず学内の信頼関係を傷つけてしまい、訓練後に円滑な本学の業務遂行にマイナスの影響を与えかねない。訓練によってこのようなマイナスの影響を本学に与えることは、避けなければならない。

(2) 嘘は書かない

訓練対象者の中には、訓練メールを訓練とは気づかない者も少なからずいることが想定される。そのような者へ誤った情報を与えてはならない。情報提供を装った訓練メールを作成する場合の内容については、科学的に信頼できる情報を引用して作成した。

(3) 多くの人が興味を惹く内容を

訓練対象の職員 6500 名といっても、事務、技術、医療などさまざまな職種があり、例えば事務という職種の中でも、総務系、財務系、学務系などさまざまな業務分野がある。これら職種や分野が違えば、当然興味を持つ内容も異なることが想定される。また、職階によっても、興味を持つ内容が異なることは想像に難くない。

このことも踏まえ、できる限り多くの人が興味を惹く内容を検討した。

５．２　メールサーバの負荷軽減

訓練対象の 6500 名に対して一斉にメールを送信すると、メールサーバの負荷が上昇して遅延を発生させる。

このため、メールサーバの負荷軽減として、1 秒間に 1 通ずつメールを送信し、約 2 時間かけてすべてを送信した。

これにより、本学のメールサーバには、まったく影響を与えずに訓練を実施することができた。

５．３　送信順序

メールは、訓練対象者のメールアドレス宛に送信する。前項に示した通り、最初のメール送信者から最後のメール送信者まで 2 時間の差があり、同じ順序で送信すると、同じ部署内において受け取る順序が固定化される。これを防ぐため、3 回とも異なる順序で送信した。

６　訓練メールの内容

訓練メールの内容は、以下の通りである。

第 1 回

送付日時：

2016 年 1 月下旬

メール件名：

献血のお願い

送信者：

社会部 syakaibu@学外のドメイン

第 2 回

送信日時：

2016 年 2 月上旬

メール件名：

【機密性 2 情報】運営会議資料送付

送信者：

全学メールアドレス

<sato@学外のドメイン>

第 3 回

送信日時：

2016 年 2 月中旬

メール件名：

インフルエンザの流行について

送信者：

京都保険機構

7　訓練実施結果

訓練の結果、3 回目の開封率は、1 回目の 1/10 程度まで減少した。

8　訓練総括

本学における、訓練の総括を以下に述べる。

- 開封率が、第 3 回で低下しており、訓練による成果が表れている。他組織の平均開封率と比較して、一定のレベルには達していると考えられる。
- 事前連絡に従って報告が行われ、各部局における連絡報告体制の訓練としての成果もあった。
- 訓練終了後、不審なメールを受け取った旨の報告が増加したことで、訓練による意識向上の成果が見られる。

9　訓練実施後のセキュリティ対策掛の対応

8 章訓練総括でも述べた通り、訓練実施後は不審なメールを受け取った旨の報告・相談が増加した。構成員の意識が向上したと喜ばしい反面、セキュリティ対策掛としては、日々送られてくるウイルスの可能性があるメールへの対処業務が増加した。

セキュリティ対策掛では、報告・相談として転送されてくる不審なメールについて、ウイルスであるか否かを簡易判定して回答するが、判定する際に、セキュリティ対策掛の業務環境にウイルス感染を引き起こす懸念が少なからず存在する。

これに対処するため、インシデント報告用のメールアドレスとは別に、不審なメールの通報用のメールアドレス(sbox)を作成し、不審なメールの報告・相談は、sbox アドレスへ送るように依頼している。sbox アドレスにメールが届くと、セキュリティ対策掛員のアドレス宛に you_have_mail_at_sbox という件名のメールが届き、専用端末でメールを確認するという作業を行っている。

10　おわりに

本稿では、2015 年度に本学において実施した、標的型攻撃メールの対応訓練について報告した。

標的型攻撃メールの被害に遭わないためには、標的型攻撃メールの対応訓練は、繰り返し実施することが重要と言われている。

2016 年度以降も引き続き、本学では標的型攻撃メールの訓練を実施していく予定としている。

参考文献

[1] 情報セキュリティ戦略本部、日本年金機構における個人情報流出事案に関する原因究明調査結果、
http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf

[2] 独立行政法人情報処理推進機構（IPA)、標的型攻撃メールの例と見分け方、
https://www.ipa.go.jp/security/technicalwatch/20150109.html