香川大学での標的型攻撃メール訓練の実施と課題調査について

小野 滋己[1)], 後藤田 中[1)], 青木 有香[1)], 八重樫 理人[1)], 藤本 憲市[1)]
林 敏浩[1)], 今井 慈郎[1)], 最所 圭三[1)]

1) 香川大学

jyohosenm@jim.ao.kagawa-u.ac.jp

The Response Training and the Survey of Improvement against the E-mail of the APT in Kagawa University

Shigemi Ono [1)], Naka Gotoda [1)], Yuka Aoki [1)], Rihito Yaegashi [1)], Ken'ichi Fujimoto [1)]
Toshihiro Hayashi [1)], Yoshiro Imai [1)], Keizo Saisho [1)]

1) Kagawa University

概要

日本年金機構に対する標的型攻撃（2015 年 6 月）では多数の個人情報が流出し、香川大学（以下：本学）の医学部附属病院でも、同様の攻撃によって端末 1 台がウイルスに感染するインシデントが発生した。本学では、こうした事例に基づき、情報セキュリティ対策の強化の一環として、構成員（特に教職員）に対する標的型攻撃メール対応を重要と捉え、その訓練を 2016 年 12 月に実施した。それと共に、攻撃に対する本学の潜在的課題や訓練自体の課題を探るための調査も事後に実施した。本稿では、訓練やこの調査方法を紹介する。

1 はじめに

Emdivi による標的型攻撃[1]は 2015 年 6 月にかけて「医療費通知のお知らせ」を中心として、関係者・組織を装い、全国の官公庁・高等教育機関・企業を含め、組織内の端末が感染し、組織内外への攻撃への踏台利用や情報漏洩のインシデントが多数発生した。端末におけるマルウェアによるウイルス感染の脅威について、標的型は特定の個人を攻撃対象としていながら、組織への被害（脅威）が極めて高くなっている[2]。このことから、インシデントに対して、個々の構成員におけるセキュリティ意識向上を含めた資質強化と、被害拡大を抑制するために、迅速かつ的確な初動対応がとれる組織・体制面強化の両面から取り組むことが必要な状況である。

本学では、後者の組織・体制面の強化として、2016 年 4 月には、本学の総合情報センターに情報セキュリティ部門を設置、従来よりも専任に近い形で、教職員スタッフを配置した。また、2017 年 3 月には、部局ごとのセキュリティチームを再編し、横断的な組織対応を意識し、”KADAI CSIRT”を発足させ、情報セキュリティのガバナンスを強化している。

一方で、本学の医学部附属病院における端末のウイルス感染によるインシデント発生後より、前者の対応として、IPA の教材[3]等に基づき「標的型攻撃メールの見分け方」に特化した講習会を全学の教職員を対象に実施した。一方で、その講習を活かした対応訓練を実施することにより、当事者意識の強化や講習で習得した知識の実践が可能と考え、2016 年 12 月中旬に全学教職員を対象とした標的型攻撃メール訓練も実施した。

本稿では、この訓練に関する紹介とともに、個人の訓練だけでは解決できない、潜在的課題や訓練自体の課題を探るための調査も実施したため、その調査内容についても紹介する。

2 標的型攻撃メール訓練について

2.1 訓練の実施狙い

標的型攻撃メール訓練に関する主な目的は以下の通りとした。

(1) 標的型攻撃メール訓練対象者(以下：訓練対象者)が、標的型攻撃メールを受信した際には、不審な添付ファイル、また記載された URL の開封を行わなくなる。

(2) 対象者が万一標的型攻撃メールを開封する等

し、ウイルス感染の可能性が疑われる場合には、本学で定められた手順に従い、部局のシステム管理者・責任者等、情報セキュリティ対応関係者に速やかに連絡・相談を行うようになる。

(3) 標的型攻撃メールは、特定の個人を対象とする事例も多いが、複数人への攻撃（特に対象アカウントがメーリングリストであった場合の複数人受信）の可能性もあり、標的型攻撃と疑われるメールを受信した場合には、部局内の関係者に情報共有を行い、また、必要に応じて（2）の手順と同様に対応関係者へ連絡・相談を行うようになる。

2.2 訓練対象者について

訓練対象者は、本学の教職員とし、教務職員、事務職員、技術職員、看護師等の附属病院等における医療系職員も含め対象者数は、約 2,000 名であった。

2.3 全体的な実施手順

実施手順を図 1 に示す。標的型攻撃メールの配信時期は、具体的な訓練用標的型攻撃メール（以下：訓練メール）の配信から報告等の訓練期間は、2016 年 12 月中旬に実施した。

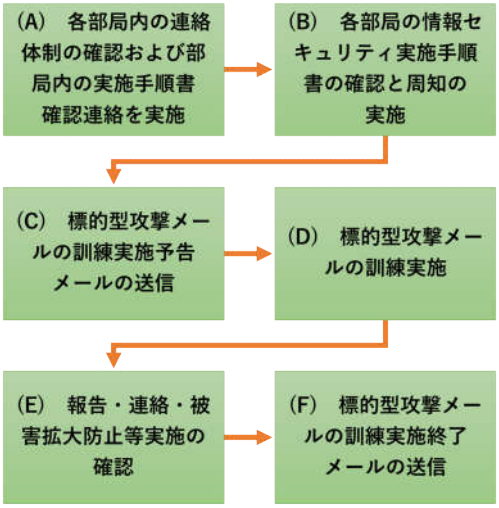

図 1 本学における訓練フロー

(A) 各部局内の連絡体制の確認と部局内の実施手順書確認連絡を実施

セキュリティ対応関係者へ、部局内で整備されている連絡体制の確認と訓練を含むインシデント発生時に、迅速な対応が可能なようセキュリティ対応関係者間の連絡手順について確認するよう連絡を行った。

(B) 各部局の情報セキュリティ実施手順書の確認と周知の実施

訓練に先立ち、対象者へ、セキュリティ対応関係者への連絡先やインシデント発生時の対応手順の確認を行うよう通知した。

(C) 標的型攻撃メールの訓練実施予告メールの送信

対象者へ、訓練を予告に定める期間内において実施することを周知した。

(D) 標的型攻撃メールの訓練実施

後述する学外サービスを用いて学外より、対象者に対して、訓練メールの配信を行った。

(E) 報告・連絡・被害拡大防止等実施の確認

（B）の手段により、対象者からの開封に関する連絡・相談、また情報共有について、報告を受け付けた。なお、その状況を訓練後に取りまとめられるよう、事前にセキュリティ関係者へ記録の依頼を行った。

(F) 標的型攻撃メールの訓練実施終了メールの送信

訓練の終了を通達すると同時に（D）におけるメールの内容を公開した。

2.4 採用した訓練メールサービスについて

2016 年度の訓練については、同様に訓練を実施している他の組織と本学の比較を行う等の理由から、ALSOK と株式会社ラックが業務提携した訓練サービスとして「IT セキュリティ予防接種」を利用した。

本学で採用した訓練メールには、PDF ファイルが添付され、ファイル内において、表記 URL と実 URL が異なる偽装した URL リンクを用意されている。この実 URL は送信先に対してユニークに紐づいており、この URL をクリックすると、開封者が特定される形で情報が収集される。この Web ビーコン型のアクセスログ解析によって、開封者情報を収集した。

2.5 訓練メールの内容について

標的型攻撃メール訓練の内容検討に関する留意すべき点が存在する[4][5]が、偽装された組織を実質的な訓練実施部局である本学の総合情報センターとすることで、実在する組織ではあるが、業務への影響を避けた。具体的なメール内容は以下のとおりである。また、同部局が取り扱う情報インフラを題材とすることで、興味を惹く内容とした。

・メール題名：
　【重要】メールシステムのトラブルについて
・送信者：
　香川大学 総合情報センター

・アドレス：
　support@学外のドメイン
　（サービス提供業者が用意）

・添付ファイル名：
　「【重要】メールシステムのトラブル状況（速報）」.pdf

これらの内容については、情報セキュリティ対応関係者には、事前に通知を行い、対象者の問い合わせ対応に対して、訓練と実際の標的型攻撃の違いが認識できる形で対処できるよう配慮した。

2.6 訓練の実施結果について

同サービスを実施している他組織の開封率の参考情報と比較を行ったところ、平均的な開封率よりも低くなっていた。また、官公庁・公共団体といった中でも、低い値となっていた。なお、実際に開封を行った対象者のうち、報告があったのは、1/7 程度にとどまった。

3　事後の課題調査について

3.1 調査の趣旨について

開封率や報告率については、訓練結果の集計によって定量的に観測可能である。一方で、明らかになった数値的指標の改善に向けた方略を検討するために、個人の意識、または、それに寄らない組織的な課題、訓練自体の課題等を調査する必要がある。これらを明らかにするために、対象から訓練実施後に声を拾い集めることとした。

3.2 調査方法について

訓練が終了した後、アンケートを対象者全員に対して、通知を行い実施した。アンケートは、Google Form を用いて、Web ブラウザから回答を行ってもらった。

3.3 調査項目について

課題を探るために、調査項目を事前に検討した。代表的な項目としては、以下があげられる。

- 標的型攻撃メールが届いたことを認識していたか
- 対象者が、標的型攻撃メールをどのように見抜いているか
- Web ビーコンログで取得した開封率はあくまで URL 開封であるが、実際には添付ファイルはどの程度の割合が開封していたか
- 報告を行わなかった理由は何か

以上の項目について、報告したかどうか等、対象者の行動判断と紐づけて要因の分析を行った。

3.4 調査結果について

アンケートは、訓練対象となった教職員全員に対して 1/6 程度の回答があった。先の調査項目からの課題がいくつか明らかになった。また、自由記述による意見としては、

- 訓練の事前通知方法に関する意見
- 今後の訓練の実施方法（回数や対象、訓練の中身等）に関する意見
- 訓練に関連した日常的なセキュリティ情報の提供に関する意見

等が寄せられた。全般的に訓練に対し、好意的な意見が多かった。

4 おわりに

本稿では 2016 年度に本学で実施した標的型攻撃メール訓練について報告した。同訓練は、本学の情報セキュリティ対策基本計画の実施項目にも掲げており、本年度も実施予定である。本年度は C-SIRT 発足後の訓練であり、それを窓口とした報告・相談等の手段も追加されており、訓練実施後、前年度比較を行い、さらなる課題や改善に向けた対応の検討を行う予定である。

謝辞

本発表にあたっては、香川大学総合情報センターおよび学術・地域連携推進室情報グループの多大なる協力を得た。ここに謝意を示す。

参考文献

[1] マクニカネットワークス株式会社、標的型攻撃の実態と対策アプローチ、https://www.macnica.net/file/security_report_20160613.pdf (参照日：2017 年 10 月 01 日)

[2] 独立行政法人情報処理推進機構（IPA）、情報セキュリティ 10 大脅威 2016 ～個人と組織で異なる脅威、立場ごとに適切な対応を ～、https://www.ipa.go.jp/files/000051691.pdf (参照日：2017 年 10 月 01 日)

[3] 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/files/000043331.pdf (参照日：2017 年 10 月 01 日)

[4] 片桐統、佐藤紀恵、石橋由子、京都大学における標的型攻撃メールへの対応訓練、大学 ICT 推進協議会 2016 年度年次大会、WE34、2016.

[5] 独立行政法人情報処理推進機構（IPA）、安心相談窓口だより:「組織における標的型攻撃メール訓練は実施目的を明確に」、https://www.ipa.go.jp/security/anshin/mgdayori20170731.html (参照日：2017 年 10 月 01 日)