情報セキュリティ部門報告

後藤田 中[1] 米谷 雄介[1] 小野 滋己[2] 青木 有香[2] 福家 隆[2] 高橋 岳水[3] 川口 政秀[2] 土居 敬典[4]
山下 俊昭[2] 末廣 紀史[2]

N.Gotoda[1] Y.Kometani[1] T.Fuke[2] T.Takahashi[3] M.Kawaguchi[2] Y.Doi[4] S.Ono[2] T.Yamashita[2] N.Suehiro[2]
Y.Aoki[2]

(香川大学 総合情報センター/創造工学部[1], 香川大学 学術・地域連携推進室 情報グループ[2],
香川大学 医学部情報ネットワーク管理室[3], 香川大学 農学部会計係[4])

1. まえがき

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。

後者の組織・体制面の強化として，2016年4月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た香川大学情報セキュリティインシデント対策チーム “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月中旬および2017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，総合情報センターにおける CSIRT の構築という枠組みの中で，標的型攻撃メール訓練の設計と実施をその特徴的な取り組みとして報告する。

2. CSIRT の活動

CSIRT はインシデント対応だけでなく，情報セキュリティの啓蒙活動も行っているので，その一部を紹介する．

2.1. 情報漏洩・不審メールへの注意喚起

CSIRT 発足は2017年3月であり，発足前の注意喚起メール送信数は月1件ほど，発足後の注意喚起メール送信数は月1.7件ほどで，CSIRT 活動の効果が現れているといえる。

2.2. 不審メールの情報提供

CSIRT に情報提供のあった不審メール数について，2017年11月には，楽天や Apple などの実在企業を騙った不審メールが急増した。2017年12月以降はいったん沈静化し，2018年3月末頃から再び報告数が増える傾向にある。本学構成員の不審メールに対する情報セキュリティ意識が浸透してきていると判断できることから，今後も啓蒙活動を続けていく。

2.3. 情報セキュリティ教育

2017年度も教育活動として情報セキュリティ e ラーニングを実施した。大学における FD（Faculty Development）の一環として行っており，実施期間は，システムリプレイスによる LMS(香川大学 Moodle)の改修のため，年度跨りの2018年3月26日～5月11日であった。

e ラーニングは香川大学 Moodle を活用し，情報セキュリティ対策の自己点検シートと一般的な情報セキュリティの知識を問うクイズ形式とした。教材は，既存の教材[4-9]を基に大学教職員にとって有用と思われる内容を抽出し，大学組織の特徴に合わせ本学内部で修正したオリジナル教材である。Moodle の機能である多肢選択式問題と自動採点機能を利用し，回答に対して判断の正誤および詳細な解説が提示されるようにしたことにより，学習としても機能するようにし，正答率が80%を超えることを修了条件とした。なお，後述する標的型攻撃メール訓練の結果を受けて香川大学の正規 Web サイト URL と不審な URL リンクを見分ける設問を必須問題とした。受講率は，全学で60%ほどと昨年度の45%ほどから，受講者が増えた。

3. 標的型攻撃メール訓練

3.1. 本訓練の目的

標的型攻撃メールの大学への潜在的脅威の認識及び，大学教職員の情報セキュリティ意識の向上，情報セキュリティインシデントが発生した場合に，報告・連絡，被害拡大防止等，迅速かつ的確な初動対応を取れるように訓練を実施した。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 URL の開封を行わなくなる。

(2) 対象者が標的型攻撃メールを開封し，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⑵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。

訓練を繰り返すことにより上記の効果を期待し，これらを見据えた情報セキュリティ意識調査項目を設計し，実践後，教職員に対してアンケートを実施した。

3.2. 本訓練の体制

本学の教育組織は６学部（教育，経済，法，工，医，農）７研究科（教育，経済，法，工，医，農，地域マネジメント）体制で構成されており，これらに加えて法人本部および各種の機構，センター，室により支えられている。学内部局によっては，独自に情報環境（メールサーバ等）を立ち上げている。こうした背景から本学では，情報セキュリティポリシー（対策基準）は大学全体での共通基準とし，各部局の状況を反映した部局ごとの実施手順を整備する体制を取っている。各部局にはシステム管理責任者が存在し，通常のインシデント対応手順は各構成員から CSIRT に集約することとなっているが，今回の訓練結果の調査に関しては情報システム管理責任者に依頼し，部局ごとに集約した内容を CSIRT に連絡する方法を採用している。

上記の本学の現状を考慮し，手順を以下の７つのステップで構成した。

⑴ 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。

⑵ 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。

⑶ 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（5 日間）において実施することを周知した。

⑷ 標的型攻撃メールの訓練実施

対象者に対して，訓練メールの配信を行った．メールは，学内に訓練用のサーバを設置しそこから配信した。

⑸ 報告・連絡・被害拡大防止等実施の確認

⑵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。

⑹ 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⑷におけるメールの内容を公開した。

⑺ 訓練の解説及びアンケートの実施

訓練用メールの解説を学内専用サイトに掲載し，メールにて対象者に案内を行った．解説サイトのページ最下部にアンケートへのリンクを設け，対象者に回答してもらった。

3.3. 訓練メールの内容

2017 年度では，題材として，「人事部局による年末調整」を利用した。より具体的には，2017 年 11 月頃の実在企業等を騙ったメールの増加，および他大学のメールアドレス詐称事例を参考にした。「人事部局による年末調整のお知らせ」は実施時期（12 月）に応じた内容であり，普段から高い情報セキュリティを持っているかどうかを評価することをねらいとした。主要な内容は以下のとおりである：

- メール題名：【重要】年末調整の確認について
- 送信者：香川大学の人事関連部局
- アドレス：人事関連部局を騙った存在しない学内アドレス（kagawa-u.ac.jp）
- 添付ファイル：なし
- 外部リンク：詳細を確認できるようにした．本リンク先で本メールが訓練メールであることの種明かしを行った．リンク先が学外の不審なアドレス，マウスオーバーで確認することができるようにした。

3.4. 採用した訓練メールシステム

学内で別途メールサーバを立て，そこから送るようにした。2017 年 11 月の実在する企業を騙ったメールの増加を鑑みて，攻撃メールの実態に沿った形で，メール本文に記述する形にした。メール本文表記と実 URL が異なる偽装した URL リンクを用意し，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 Web ビーコン型で情報を収集した。

3.5. 訓練の実施結果

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であった．対象者の総数は， 2017 年度は 2,388 名であった。

表 1 に標的型攻撃メール訓練の結果を示す．2016 年度の結果では，低い値となっていたのは，総合情報センター名で送信されることを含めて，添付された PDF に記載の URL クリックを開封としたことから，世間一般のものと比較して標的型攻撃メールと気づかれやすいものだったと部門として判断した。そこで 2017 年度は真に訓練に繋がることを狙いに，より判別が難しいテーマを選択した。その結果として，表 1 に示すとおり，メール開封率は上昇したが，標的型攻撃メール訓練としては教職員へ有効な課題を提供できたと考えている。

表 1　標的型攻撃メール訓練の結果

年度	受信者数	開封者数	受信報告数	開封報告数	開封率	受信報告率	開封報告率
2016	2179	241	452	65	11.1%	20.7%	27.0%
2017	2388	767	533	306	32.1%	22.3%	39.9%

表 1 の組織全体の開封報告率をみると，2016 年度は実際に開封を行った対象者のうち，報告があったのは，27.0% にとどまったが，2017 年度はこれが 39.9%まで大幅に改善した，開封者の母数が増えたこともあるが，啓蒙活動の成果ととらえたい。

4. 事後のアンケート調査について

4.1. 調査の趣旨および各年度の目的

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ために，訓練対象者から訓練実施後に 2016 年度に続きアンケート調査を実施した。

2017 年度は昨年度の結果を受けて訓練題材の改善を行った。

4.2. 調査方法

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，CSIRT の Web サイトで標的型攻撃メール訓練の解説を掲載し，その最後に Google Form を用いたアンケートへのリンクを掲載し，Web ブラウザから回答を行ってもらった。

4.3. 調査項目

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
- 標的型攻撃メールをどのように見抜いているか
- 部局内で情報共有したか
- 報告を行わなかった理由は何か

4.4. 調査結果

アンケートは，訓練対象となった教職員全員 2388 名に対して，回答数は 384 件で回答率は 16.1%であった。先に示したとおり，本学メールアドレスを実施時期に即した内容のメールを題材としたことから開封率が上昇したとみられるが，一部回答者は，メール本文の内容で訓練メールであると判断されていた。2016 年度の報告率と同程度の結果のため，報告していない理由を見ると，訓練であるためや，開封していないためなどを理由として報告をしていないケースが目立った。開封の有無に関わらず不審メールを受け取ったことを報告することが，訓練の目的の一つであることを周知してきたが，受信報告率が示すとおり，さらなる訓練の趣旨や報告体制の浸透が課題であると考えている。

情報共有をしなかった理由は，URL リンクをクリックしてページを開いたことに対して罪悪感をもち，周囲に話せなかったという意見が得られた。インシデントの予防としては，このような意識を払拭することが重要であり，根本的な組織文化をより開いたものへと変えていく施策が必要であると当部門としては考えている。そのための方策として CSIRT がより構成員にとって相談しやすい存在になることが重要であると考えている。

5. おわりに

標的型攻撃メール訓練は，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，2018 年度以降も実施予定である。訓練実施後のアンケート結果から，連絡体制がわかりにくいといった意見は 2 年連続で多く，窓口を一本化することに対するニーズがあることがわかった。これを実現するためには，各学内部局の実施手順を変更する改定が必要であり，学内ヒアリングによって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。

以上，CSIRT 活動報告及び 2016 年度，2017 年度と継続して実施した標的型攻撃メール訓練の概略報告をもって当部門の年次報告とした。

6. 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

[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

[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

[4] IPA，“ここからセキュリティ！：セキュリティチェック，”http://www.ipa.go.jp/security/kokokara/quiz/

[5] 内閣官房情報セキュリティセンター，“情報セキュリティ自己診断チェックリスト，”http://www.nisc.go.jp/security-site/files/checklist_20120417_02.pdf

[6] TREND MICRO，“is702：クイズで判定あなたのセキュリティレベルは？，”https://www.is702.jp/special/1314/partner/12_t/

[7] MOTEX，“セキュリティ 7 つの習慣・20 の事例，”http://www.motex.co.jp/vision/enlightenment_activity/education_book/

[8] 日本ネットワークセキュリティ協会，“知っておきたい情報セキュリティ理解度セルフチェック，”https://slb.jnsa.org/slbm/

[9] JPCERT コーディネーションセンター，“新入社員等研修向け情報セキュリティマニュアル，” https://www.jpcert.or.jp/magazine/security/newcomer.html