京都大学における標的型攻撃メールへの対応状況

山口 倉平 [1)], 石井 良和 [1)], 宮部 誠人 [1)], 津田 侑 [2)]

1) 京都大学 情報部
2) 京都大学 情報環境機構

i-s-office@iimc.kyoto-u.ac.jp

Status of Response to Targeted Attack Emails at Kyoto University

Souhei Yamaguchi [1)], Yoshikazu Ishii [1)], Makoto Miyabe [1)], Yu Tsuda [2)]

1) Information Management Department, Kyoto University.
2) Institute for Information Management and Communication, Kyoto University.

概要

京都大学では標的型攻撃メールによるセキュリティリスク軽減のため、2015 年度から全教職員を対象に標的型攻撃メール訓練を実施している。また標的型攻撃メール等の不審なメール受信時に教職員や学生が通報できる窓口を設置して運用している。本稿では、訓練の取り組み状況と結果、通報窓口の状況と結果について紹介し、また判明した課題における改善策を紹介する。

1 はじめに

IPA（情報処理推進機構）が発表している「情報セキュリティ 10 大脅威 2025 [1]」において、機密情報等を狙った標的型攻撃やビジネスメール詐欺といったメールに関する脅威は、近年の脅威として毎年選出されている。また他の脅威についても、メールが攻撃手口や糸口として悪用され、マルウェア感染や個人情報の漏えいの原因となっており、様々なセキュリティインシデントのきっかけとなっている。

京都大学（以下、「本学」という。）では、2015 年度より本学教職員を対象に毎年度標的型攻撃メール対応訓練[1]を実施し、標的型攻撃メールへの対応能力向上に取り組んでいる。訓練メールの内容は毎年変更し、実際に本学に届いた標的型攻撃メールの内容や流行りを参考にして作成した訓練メールを一斉送信して行う。また標的型攻撃メールを受信した際の通報窓口を運用し、通報を受けた不審メールから学内への注意喚起や拒否リストへの適用による通信遮断といった対策を進めている。

本稿では、これまでの訓練や通報窓口の運用状況についてまとめ、得られた知見について報告する。

標的型攻撃メール訓練については、2015 年度から 2024 年度の 10 年間の取組みの概要とその結果を述べる。通報窓口については、2021 年度から 2024 年度の 4 年間の取組みの概要とその結果について述べる。さらに、結果を踏まえて標的型攻撃メール通報についての改善について述べる。最後に取組み全体についての考察を述べる。

2 標的型攻撃メール訓練

2.1 訓練の概要

全教職員を対象に疑似的な訓練メールを一斉送信し、標的型攻撃メールやその可能性がある不審なメールを受信した際に、リンクへのアクセスや添付ファイルの開封を行わない等の適切な対応が行えるかを訓練する。また各自が必要な報告を行い、本学におけるセキュリティリスクを軽減することを目的としている。なお、訓練前には標的型攻撃メールの見分け方や受信時に取るべき対応をまとめた資料を通知している。

通知資料の内容は以下のとおりである。

- 標的型攻撃メールの説明と事例
- 怪しいメールを見分けるポイント
- URL の読み方、見分け方
- メールを受信したときの通報方法
- セキュリティ対策、機密情報を取扱う対策
- 不審なメールの添付ファイル開封や URL をクリックしてしまった場合の対応

表 1　訓練結果（2015 年～2024 年）

年度(対象者)	開封率					通報状況			
	1 回目		2 回目		2 回とも開封	1 回目		2 回目	
	開封者	通報者	開封者	通報者		電話	メール	電話	メール
2015(6,470)	8.3%	3.6%	9.2%	3.6%	2.0%	52	178	56	177
2016(12,023)	3.0%	2.6%	11.7%	1.8%	0.7%	46	264	34	177
2017(12,137)	2.8%	3.6%	4.6%	3.1%	0.5%	13	427	9	368
2018(12,281)	21.7%	3.1%	12.1%	3.9%	4.3%	26	350	13	462
2019(12,379)	15.3%	2.0%	7.8%	1.2%	2.7%	2	250	3	148
2020(12,457)	14.9%	4.5%	23.3%	3.2%	5.4%	20	553	12	389
2021(12,455)	18.0%	2.0%	2.7%	2.8%	0.6%	3	247	4	350
2022(12,570)	1.5%	3.6%	-	-	-	59	391		
2023(12,678)	5.0%	0.6%	-	-	-	2	62		
2024(12,801)	12.1%	3.0%	-	-	-	7	379		

2.2 訓練結果

本稿ではこの中で特徴的な結果をいくつか紹介する。2018 年度 1 回目は、メールボックスの保存容量が上限に達した通知メールを訓練に利用した。開封者の内訳としては、どの職位においても開封されており、メールが利用できなくなる緊急性も重なり、開封率が高くなった。

次に 2020 年度 2 回目は、本学の財務会計系のシステムから機械的に送付される振込通知のタイトルをそのまま利用して訓練を行った。開封者の内訳としては、振込通知が日頃から多数届くと思われる職位において、より開封率が高くなった。

個人にかかわる内容で自身に関係のある可能性の場合に開封率が高くなることが判明した。

また 2022 年度に、本学で Emotet の感染による情報漏えいが発生したため、感染事例を参考にマクロ型添付ファイルをパスワード付き Zip にて訓練を行った。開封率は 1.5%と低い値ではあるが、186 名が開封したことは、油断ができない結果となった。

2.3 訓練時の通報

訓練時の通報状況について、メールは、不審メールを受信した際の通報アドレス宛、情報部の問い合わせアドレス宛、Web サイトの問い合わせページに届いた件数である。ここでも、いくつかの特徴的な事象について紹介する。

電話での通報が多かった 2022 年度 1 回目については訓練メールのシグネチャに電話番号を記載したことが理由であると思われる。またメールでの通報が多かった 2018 年度 2 回目、2020 年度 1 回目については、いずれも会議の日程調整や開催通知を利用したものであった。開封率同様に自身に関連する可能性がある場合に、通報する傾向が高いと思われる。

2.4 訓練の課題

訓練の課題として、訓練メール開封者には、種明かしとして訓練であった旨の通知と標的型攻撃メールの注意喚起を行い、学習を目的としているが、未開封者にとっては学習効果が低いことが想定される。そのため 2022 年度からは標的型攻撃メール訓練の回数を減らし、代わりに Web ブラウザ上で実際の攻撃被害を疑似的に体験できるロールプレイング型コンテンツの提供を開始した。標的型攻撃メールやランサムウェア、Emotet、サポート電話詐欺等の攻撃シナリオが用意されている。

3　標的型攻撃メール通報

3.1 標的型攻撃メール通報の概要

本学では、標的型攻撃メールやその可能性がある不審なメールを受信した際、メールによる通報窓口の設置をしている。通報窓口では、見分けるのが困難なメールの相談も受け付けており、リンクや添付ファイルについて確認し回答を行っている。

通報メールは、隔離した VLAN の専用端末からのみ内容確認できるよう制限している。通報内容の確認方法としては、目視での確認、添付ファイルのウイルスチェック、サンドボックス環境による確認などを使い分けて判断している。判断結果を通報者に回答し、通報件数が多いもの、学内への影響が大きいもの、見分けるのが困難なもの等

図 1 通報窓口の運用

については、Web サイトや学内掲示板に掲載し注意喚起を行っている。また特定の部局や研究室を対象にした攻撃メールについては部局の担当者に連絡し注意喚起を促している。なお、フィッシングサイト等のリンクについては情報環境機構で運用している DNS フィルタリング[1]の拒否リストに登録を行い、学内ネットワークからの通信を制限することで、被害の軽減に繋げている。

3.2 通報件数

メールによる通報件数について、表 2 に示す。

表 2 通報件数（メール）

年度	教職員	学生	計
2021	556	19	575
2022	628	34	662
2023	455	35	490

- 教職員からの通報が 95%を占めている。
- 学生からの通報のうち、35%が関係する教授や研究室メンバを騙ったメールが最も通報があった。

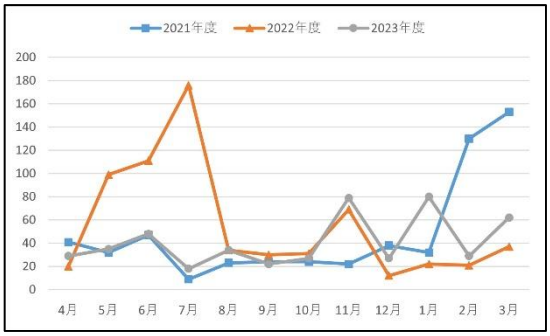

図 2 通報件数（月別）

- 2021 年 2 月から通報件数が増加しているのは世界的に Emotet の感染が大幅に拡大した影響によるものである。
- 2022 年 7 月にかけての通報件数が増加しているのは本学での Emotet 感染が発生した影響によるものである。
- 例年 11 月ごろに通報件数が増加しているのは標的型攻撃メール訓練により、通報窓口へ報告する意識向上によるものである。

3.3 通報内訳

通報があったメールについて、窓口にて確認し標的型攻撃メールに該当するか判断した結果を図 3 に示す。

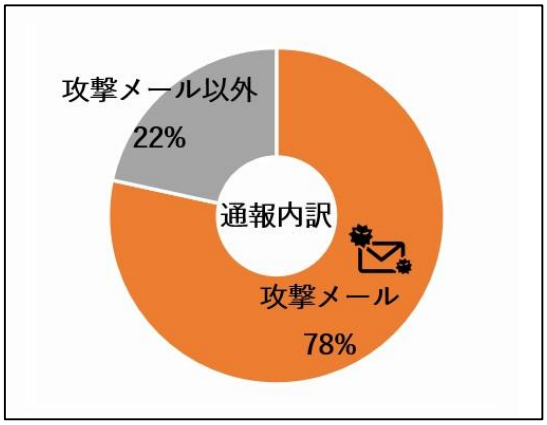

図 3 通報内訳（2021 年～2023 年）

標的型攻撃メールとしては、メール利用（パスワード、容量制限、システムアップデート）に関するものや、仮想通貨を要求する詐欺メールについ

て多く寄せられている。また標的型攻撃メール以外としては、外部のクラウドサービスを利用した本学システムからの正規の通知メールが通報されることがある。理由としては、送信元メールアドレスやリンクが、本学ドメイン（kyoto-u.ac.jp）以外になっているため不審に感じて通報されている。今後もクラウドサービスを利用したシステムは増加していく傾向にあることから、通知メールについて、運用ルールを整理していく必要がある。

3.4 メールによる通報の課題

メールによる通報は、メールサービスのセキュリティ機能により転送メールが届かない事例、レピュテーション低下の懸念、メールヘッダ情報の確認が出来ず安全性の十分な確認が難しいといった課題があった。

また通報内容について、通報者からの報告のみであるか、それとも判定が出来ずに確認を依頼しているのかが判らないために、メール確認後全ての通報に回答を行っていた。

これらの課題解決、業務の効率化のために通報フォームによる運用を開始した。

4　標的型攻撃メール通報の改善

4.1 通報フォームの概要

通報用の Web フォームは、Google フォームにて作成した（図 4）。

図 4 通報フォーム

本学は、Google Workspace for Education と契約しており、教職員は Google アカウントを所持している。通報フォームの利用は、本学の Google アカウントを持つ教職員を対象とし、ログインを必須にして制限している。フォームの入力項目はヘッダ情報を含む eml ファイルのアップロード、窓口からの返信有無を必須とし、ヘッダ情報を含むメールの保存方法については、情報環境機構の Web サイトに手順をまとめて案内するようにした。

なお、Google フォームが Google ドライブの共有ドライブ上に保存されている場合、Google の仕様によりファイルのアップロード機能が利用できない。そのため Google フォームをマイドライブ上に保存し、フォームより投稿された eml ファイルが保存されるアップロードフォルダを窓口担当者にて共有している。またその際、通知に対して迅速に対応できるように、Slack と連携して通知を行うようにした（図 5）。

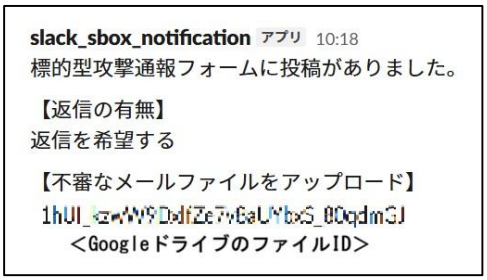

図 5　Slack 通知

4.2 通報件数

Web フォームによる通報件数について、表 3 に示す。

表 3　通報件数（Web フォーム）

	通報件数	返信希望
2024 年度	436	234 (53.6%)
(訓練時のみ)	278	158 (56.8%)

- 通報のうち、約半数が返信を希望している。
- 標的型攻撃メール訓練時も、約半数が返信を希望しており、訓練であることを見抜けたかは不明である。
- 訓練時のメール通報に関して、自動応答を設定することで、これまで手動で行っていたメール返信作業の効率化に繋がった。
- 2024 年度の通報メールによる通報は 237 件であり、訓練を除いた通報フォームによる通報は 158 件であり、通報メールによる通報の方が多い。

通報フォームにて、返信（調査）を希望する通報者が明確になったことで、窓口として必要な問い合わせに対して、より重点的に調査回答を行うことが可能となった。

4.3 通報フォームの課題

通報フォームの運用を開始して、返信を希望する通報者がどういった調査回答を希望しているのかが分かりにくい状況となっていた。任意項目としてコメント欄を追加し、調査確認してほしい点や不審と感じた点について確認するようフォームを修正した。なお、返信を希望しない通報者からもコメントがあり、通報者とのコミュニケーションがとれるように改善されたと思われる。

また通報フォームでは、調査のために eml ファイルのアップロードを求めているが、それ以外のファイル形式(テキストファイルや PDF ファイル、画像ファイル等）でアップロードされる場合が散見された。eml ファイルを求める理由にはメールヘッダを含めた調査の必要性があるが、通報者の中には『不審なメールをファイルとしてダウンロードする』こと自体に抵抗感がある可能性がある。eml ファイルが調査に必要であることの意義を周知し、抵抗感なく eml ファイルをやり取りする手段も継続的に検討していく必要がある。

4.1 に記載した通り、通報フォームは本学の Google アカウントでのログインが必須となっているため、学生からの通報は通報メールのみで受け付けている。学生からの通報についても、今後検討していく必要がある。

最後に通報フォームにアップロードされた不審なメールや添付ファイルが、Google ドライブに保存する際に検査され確認できない可能性が考えられる。ただ、現在のところ教職員に届いたメールについては Gmail のスパムフィルタにて正当なメールと判定されたものであるためか、問題は発生していない。

5 考察

本学の標的型攻撃メール訓練については、定期的かつ継続的に実施した結果、教職員のセキュリティ向上に効果があった。ただ、現在の訓練方法では攻撃メール開封者は学習できるが、未開封者が十分に学習できていない。不審なメールを受信した際には、開封せずに通報等の適切な対応を取ることが重要だと考えており、訓練方法の見直しを検討していく必要がある。そのために適切な通報手順や体制の整備、通報に対するフィードバックの整理が必要である。

また部局の構成員に不審なメールが届いた際の部局内での報告手順の整備状況について確認したところ、半数の部局では報告手順等の整備がされていない状況であった。全学の通報窓口との連携を強化しつつ大学全体のセキュリティ向上に繋げていく必要がある。

通報フォームについては、学生からの通報が受けられない点や、不審メールをアップロードすることに課題があるが、窓口側の業務効率化が実現できた。今回更なる改善のため入力項目を追加したが、フォームの入力項目や選択肢が多いと通報者側の手間がかかり通報を躊躇う可能性も考えられる。通報者側の意見も参考にして、通報方法の提供や周知を行い、標的型攻撃メールに対するセキュリティを行っていく必要がある。

6 関連研究

定期的なメール訓練は数多くの大学において実施され、一定の効果が見られると報告されている[4][5][6]。また、生成 AI を活用してメール文面の作成・送信する手法[7]や、メール文面以外にも攻撃サイトも併せて自動生成する手法[8]も提案されており、メール訓練を改善する取り組みが進められている。 文献[9]では、メール攻撃への意識向上を狙って生成 AI が組み込まれたシリアスゲームが提案され、攻撃に対する認知が向上することや検知する自信が高まることが示されている。

一方で、メール訓練の効果についても議論されている。文献[10]では、訓練でメール中の URL を開封した参加者には高いストレスレベルと自己効力感の低下がみられ、これらが訓練や報告行動に影響を与える可能性を指摘している。文献[11]では、訓練が URL の開封率の低減や報告行動の改善に繋がるとは言えないと述べている。

本学では、標的型攻撃メール訓練の実施によってセキュリティの向上に効果が見られてきた。一方で、標的型攻撃メール訓練では未開封者には十分な学習機会を提供できないこともあり、ロールプレイング型の攻撃疑似体験コンテンツの提供を始めた。また、不審なメールの報告手順や体制の整備、報告への素早いフィードバックを実現する

ための通報窓口の整備や、それに伴う窓口側の業務効率化を実施してきた。

7 おわりに

本稿では、本学における標的型攻撃メールへの対策の取り組みと結果、考察について述べた。

標的型攻撃メール訓練を実施することで、訓練の成果によりセキュリティの向上に効果があった一方課題もあることが判明した。また通報方法を改善したことで、必要な調査を行い返信することが可能となった。課題としては、メール通報が大量に寄せられた場合、通報に対する対応が滞ってしまうことが問題となっている。同様の攻撃メールに関する通報に関して、自動応答の活用や通報があった情報を学内に適切に注意喚起することで効率化を図るようにしていく。構成員には、攻撃メールを見分けるための教育や通報窓口の周知を継続し、本学の情報セキュリティ対策向上となるよう実施していく。

参考文献

[1] IPA 情報処理推進機構、情報セキュリティ 10 大脅威 2025、2025 年

[2] 片桐 統, 斎藤 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、2016 年

[3] 石井 良和, 山口 倉平, 片桐 統, 戸田 庸介、京都大学情報環境機構における DNS フィルタリングの導入と運用について、大学 ICT 推進協議会 2024 年度年次大会、2024 年

[4] 米谷 雄介, 後藤田 中, 小野 滋己, 青木 有香, 宮﨑 凌大, 八重樫 理人, 藤本 憲市, 林 敏浩, 今井 慈郎, 最所 圭三, 香川大学での標的型攻撃メール訓練の導入と改善点の検討, 学術情報処理研究, 22 巻, 1 号, p. 54-63, 2018 年.

[5] 青木 謙二, 川畑圭一郎, 黒木 亘, 園田 誠, 廿日出 勇, 宮崎大学の全構成員に対する標的型攻撃メール訓練, 学術情報処理研究, 22 巻, 1 号, p. 64-70, 2018 年.

[6] 温井 章文, 2024 年度 標的型攻撃メール訓練実施報告, 関西大学 IT センター年報, 第 15 号, p.29-33, 2024 年.

[7] 徳野 響, 五味 悠一郎, 自動生成した標的型メールを用いた訓練用標的型メール配信システムの開発と評価, コンピュータソフトウェア, 2025, 42 巻, 2 号, p. 2_52-2_57, 2025 年.

[8] 東野 正幸, 生成 AI を用いた不審メール対応訓練システムの試作, コンピュータセキュリティシンポジウム 2024, 2024.

[9] Argianto Rahartomo, Ahmed Tareq Ali Ghaleb, Mohammad Ghafari, Phishing Awareness via Game-Based Learning, IEEE Conference on Software Engineering Education and Training (CSEE&T 2025), 2025.

[10] Markus Schöps, Marco Gutfleisch, Eric Wolter, and M. Angela Sasse, Ruhr University Bochum, Simulated Stress: A Case Study of the Effects of a Simulated Phishing Campaign on Employees' Perception, Stress and Self-Efficacy, USENIX Security '24, 2024.

[11] Andrew T. Rozema and James C. Davis, Anti-Phishing Training (Still) Does Not Work: A Large-Scale Reproduction of Phishing Training Inefficacy Grounded in the NIST Phish Scale, https://arxiv.org/abs/2506.19899, 2025.