学生に向けた標的型攻撃メールに関する考察

A Discussion of Targeted Attack to Students

中島　一輝†　　坂﨑　尚生†
Kazuki NAKASHIMA†　　Hisao SAKAZAKI†
† 玉川大学工学部ソフトウェアサイエンス学科
† Faculty of Engineering, Tamagawa University

1. はじめに

近年、標的型攻撃が社会問題になっている[1]。また、コロナ禍においてリモートワークが増えたこともあり、セキュリティ対策が手薄な環境は標的型攻撃がされやすい状況になっている。特に玉川大学では学生に BYOD(Bring Your Own Device)を推進しているため、自宅から接続する際にプロキシ等によるアクセス制限を受けない場合がある。そのため、より危険な状態と考える。

本研究では、学生に向けた標的型攻撃メールについて考察し、実際に玉川大学の一部の学生に対して標的型攻撃メールの実験を行った。

2. 標的型攻撃メール実験システムの構成

自作した実験システムの全体構成を図 1 に示す。本システムは、G-mail より訓練メールを被験者宛に送信し、添付ファイル開封または URL をクリックした場合、Web サーバにアクセスログが記録される。

3. 攻撃者が取得可能な情報の整理

玉川大学をはじめ各大学では、様々な情報を公開している。本研究では、攻撃者がそれら公開情報を用いて攻撃メールを作成する可能性を考慮した。玉川大学の場合、大学 HP より以下のような情報が取得できる。

- 学科の教員名、研究室名[2]
- 授業のカリキュラム[2]
- コロナウイルスの大学の対応について、等

4. 実験メール作成

攻撃者は教員名と研究室名、コロナウイルス対応等の情報を取得できるものとし、以下の内容で添付ファイル版と URL 版の 2 種類の実験メールを作成した。

【添付ファイル版】Word ファイルに Web ビーコンと呼ばれる仕組みを埋め込み、Word ファイルを編集モードで開封した際、Web サーバにアクセスログが収集される。攻撃者は学科の教員名と研究室名を取得できるとし、実在する教員から添付ファイルより個人面談の日程調整に答えてもらう内容にした。(図 2 参照)。

【URL 版】URL 版は、メール本文に記載されている URL をクリックすると Web サーバに遷移しアクセスログが取られる。本文は、学生に新型コロナウイルスのアンケートに答えてもらう内容にした。

5. 実験結果

被験者として研究室の 9 名に依頼した。実験期間は 7/21-8/31 とし、8/19 に添付ファイル版を 8/23 に URL 版を送信した。結果、添付ファイル版では 6 名が偽ファイルを開封し、URL 版では 2 名が偽サイトにアクセスした。

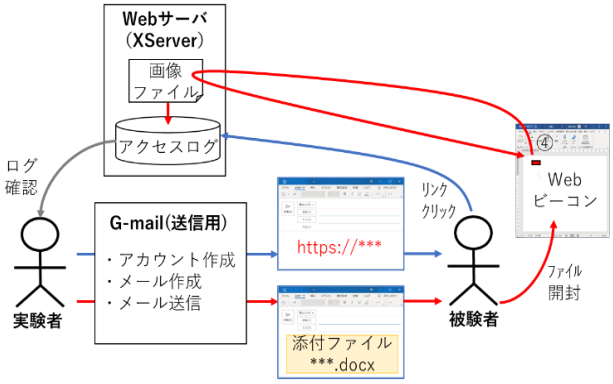

図 1　訓練システムの全体構成

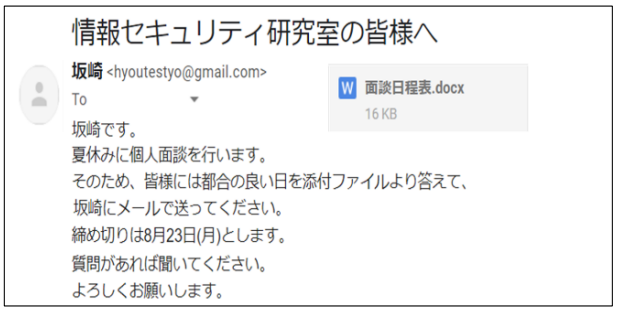

図 2　添付ファイル版の本文

添付ファイル版の開封率が高かった理由として「教員からのメールは疑いなく開いてしまう」との意見があった。見破った人のポイントとしては、「送信アドレスに不信感を抱いた」との意見が多々あった。

6. 考察

学生はレポート等で Word ファイルをよく使い、また、そのレポートは教員宛に提出される。即ち学生から教員、さらには大学全体へと影響が及ぶことが考えられる。対策として実験より、送信者のアドレス確認が有効と考える。しかし、教員が必ずしも大学ドメインからメールを送信するとは限らない。また学生も送信者のアドレスを確認するとは限らない。

本研究では、利便性を考慮し、教員に大学ドメインの使用を強要させるのではなく、教員が利用するメールアドレスをサーバに登録し、学生側のメーラがチェックする機能を検討及び設計もした。

参考文献

[1] 深澤,松原，三重大学における標的型攻撃メール訓練の実施について，技術職員による技術報告集，vol 26, pp.36-39, 2018.
[2] 玉川大学　ソフトウェアサイエンス学科，https://www.tamagawa.ac.jp/college_of_engineering/software/