# 標的型攻撃メール対応トレーニングの紹介

Training for spear-phishing email attack

明石 敬*

Kei Akashi

大手重工業を標的とした攻撃の報道以降、数多くの組織で標的型攻撃メールの脅威が注目され対策が検討されている。当社では、机上の標的型攻撃メールの教育だけではなく、受信者に攻撃を模擬したメールを送信し、標的型攻撃メールの体験を通して対応法を身に着ける、標的型攻撃メール対応トレーニングを提供している。本稿では、標的型攻撃メールの特徴を述べるとともに標的型攻撃メール対応トレーニングの内容および効果について説明する。

Since cyber attacks targeted to major heavy industry company, many companies are considering solutions for the threat of spear-phishing email attacks. We provide spear-phishing awareness training service that is sending spoofing emails to trainees to experience the attack. This paper explains spear-phishing email attacks features, our spear-phishing email awareness training services and effectiveness of our service.

## 1. まえがき

標的型攻撃メールは、特定の企業や組織に対して、興味を引くタイトルや関係者を装った「なりすましメール」を利用して受信者を欺き、添付ファイルやURLリンクをクリックさせることでマルウェアに感染させる。この攻撃によって、一旦マルウェアの侵入を許すと、社内の重要情報を盗み出されるなどの甚大な損失を被る可能性がある。

こうした、標的型攻撃メールへの対策は、「標的型攻撃メールであることに気がつき、不要な操作をしない」ことを社員一人一人が徹底することが重要である。

## 2. 標的型攻撃メール

### 2.1 従来攻撃メールと標的型攻撃メールの違い

標的型攻撃メールは、表１の通り、従来攻撃とは異なる特徴を持っている。最も大きな差異は、攻撃者の目的である。従来型の攻撃メールでは、社会騒乱や多数のPCをターゲットとしていたが、標的型攻撃メールでは、特定組織の情報搾取、特定のシステムの妨害が主な目的である。そのため、標的となる組織・人物向けに攻撃を仕掛ければ十分であるので、感染数が少なく、検体収集が困難となる。また、特定の組織・人物に高い確率で感染してほしいため、標的の環境にあわせた言語・本文・送信者を詐称して送信する。

### 2.2 従来対策の限界

従来は、主に、ファイアーウォールやアンチウィルスソフト、スパムメールフィルタの機器といった入口対策によってある程度の攻撃を防いできた。これらの機器は、過去に実施された攻撃の検体を収集し、同じ特徴を持った通信やファイル・メールを検知し、遮断する仕組みで成り立っている。従来型の攻撃メールは、多量に世の中に出回るため検体を容易に収集することができるが、2.1で述べたとおり、標的型攻撃メールの検体はな

表１　従来攻撃メールと標的型攻撃メール

| | 従来型攻撃メール | 標的型攻撃メール |
|---|---|---|
| 攻撃者の目的 | 社会騒乱<br>多数のPCを操りたい | 特定組織の情報搾取<br>システムの妨害 |
| 感染数 | 多数 | 少ない |
| 検体収集 | 容易 | 困難、ゼロデイ |
| 言語 | 主に英語 | 日本語 |
| 本文 | 一般的な用件 | 自分に関係ありそうな用件 |
| 送信者 | 不明な組織 | 官公庁<br>実在する組織 |
| 感染後のPC | PC動作が重たくなる<br>異常停止 | 特に変わらず |

参考文献(1) から一部引用

＊鎌倉事業部　ICTソリューション開発部

かなか手に入らない。したがって、従来の対策では、標的型攻撃メールを防ぐことが難しく、受信者の端末まで攻撃メールが到達してしまう。

## 3. 標的型攻撃メール対応トレーニング

### 3.1 標的型攻撃メール対応トレーニング

当社では、机上の標的型攻撃メールの教育だけではなく、受信者に攻撃を模擬したメールを送信し、標的型攻撃メールの体験を通して対応法を身に着けていただく、標的型攻撃メール対応トレーニング（以下、本トレーニング）を提供している。

本トレーニングでは、図１に示す通り、従業員が攻撃者に狙われていると想定し、標的型攻撃メールに似せた訓練メールを当社のメールサーバから送信する。訓練メールには、添付ファイルもしくはURLリンクを記載する。実際の攻撃では、添付ファイルの開封や、URLリンクをクリックしてページの閲覧をすることによって、マルウェアに感染する。トレーニングでは、実際のマルウェアは使用せずに、安全な方法で、添付ファイルの開封、URLリンクのクリックを計測し、受信者のうち、どれだけファイルの開封/リンクをクリックしてしまうのかを測定する。

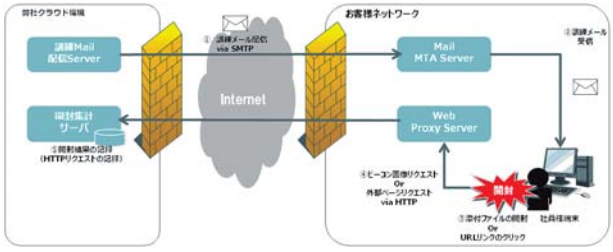


図１　トレーニング概要

### 3.2 効果

訓練メールを同一の受信者に対して２回送信し、１回目と２回目の開封率を比較することによって、本トレーニングの効果を測定することができる。

本トレーニングを昨年度実施した結果の平均値を表２に示す。第一回目の開封率は、29.0%であり、約３人に１人が訓練メールを開封している。本トレーニングを受けたすべての組織で、事前に机上による教育を行っていた。机上の教育を行っていても、約３人に１人が標的型攻撃メールを開封するということである。一方、第二回目の配信では、11.9%まで低下しており、標的型攻撃メールを開封するのが、約10人に１人の割合となっている。受信者に、第一回目の配信を行った結果、標的型攻撃メールに対する耐性が付き、第二回目では、開封率が低下している、と考えられる。

表２　2013年度トレーニング結果

| 項目 | 数値 |
|---|---|
| 第一回目開封率(平均) | 29.0 % |
| 第二回目開封率(平均) | 11.9 % |

## 4. トレーニングの流れ

本トレーニングは、以下の流れで実施する。要望によっては、メールの配信回数や本文の内容などをカスタマイズしている。

（１）実施前打ち合わせ

事前に対象者のメールアドレスの提供方法、トレーニングの進め方などの打ち合わせを実施する。状況に応じて、訓練のメール内容や添付ファイルの内容、方式について調整する。

（２）疑似攻撃演習

本番の訓練メールを送る前に、関係者内で送信予定の訓練メールを送信し、問題なく訓練が実施できることを確認する。

（３）教育資料展開

当社より、教育資料を提供し、事前に標的型攻撃メールについて教育していただく。

（４）疑似標的型攻撃メール配信

事前打ち合わせなどで調整した内容の標的型攻撃メールを模擬した訓練メールを計２回配信する。

（５）結果報告

添付ファイルの開封率やURLリンクのクリック率をレポートにまとめて報告する。

## 5. むすび

本稿では、標的型攻撃メールの特徴と標的型攻撃メール対応トレーニングの概要とその効果について説明した。

標的型サイバー攻撃は、従来型のアンチウィルスソフトやスパムフィルタといったセキュリティ製品では防ぎきれない。最終的には、受信者一人一人の危機意識に委ねられてしまう。机上の教育を実施しても本稿で述べたとおり、標的型攻撃メールを受信した場合、約３人に１人はマルウェアに感染してしまうため、本トレーニングのような体験型の教育が非常に重要である。

本サービスの詳細については、下記窓口に問い合わせ頂きたい。

営業本部　ソリューション営業部　第一課
〒105-6132　東京都港区浜松町二丁目4番1号
世界貿易センタービル32階
TEL：03-3435-4737　FAX：03-3435-4745

## 参考文献

（1）IPAテクニカルウォッチ標的型攻撃メール分析に関するレポート,情報処理推進機構（2011/3/30）

## 執筆者紹介

明石　敬
2007年入社。主に、製品事業、官公庁・民間企業の受託開発事業に携わる。2011年より情報セキュリティ製品・サービス関連業務に従事、現在に至る。