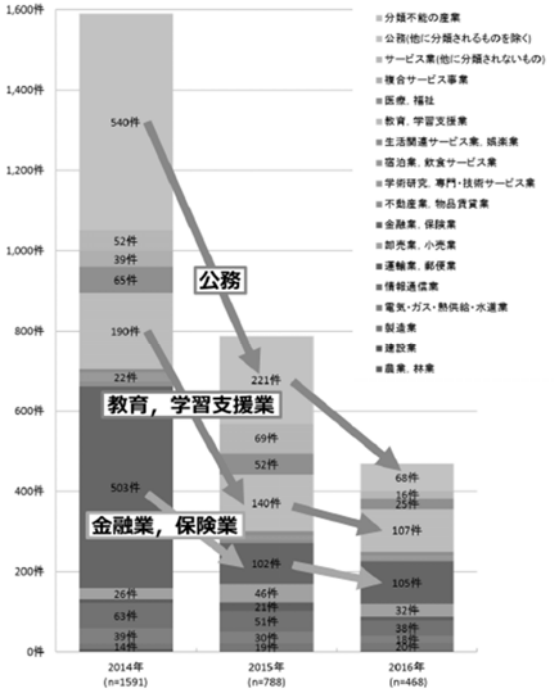
<情報セキュリティインシデント事例から研修・啓発の仕組みを考える>

S-2.「標的型攻撃メール対策の訓練事例」

早稲田大学　高橋 智広

背景

- 教育機関は、**個人情報を大量に所持する３大業種の１つ**と認識
- ワースト１位を獲得し、色んな意味で厳しい目が向けられている

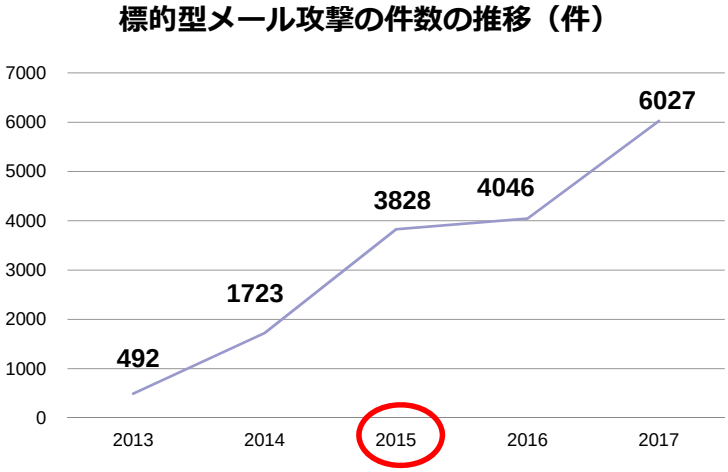


（出典）JNSA 2016年情報セキュリティインシデントに関する調査報告書

- ✓ 情報セキュリティインシデントの発生件数において、教育機関は３大発生源の一角になっている。
- ✓ 2016年度、教育機関は、金融業・保険業、公務に抜かれてワースト１位に！

背景

- 国内におけるサイバー攻撃は、**増加傾向**
- 標的型攻撃の手口は、**年々巧妙化**



（出典）警察庁「平成28年におけるサイバー空間をめぐる脅威の情勢について」広報資料

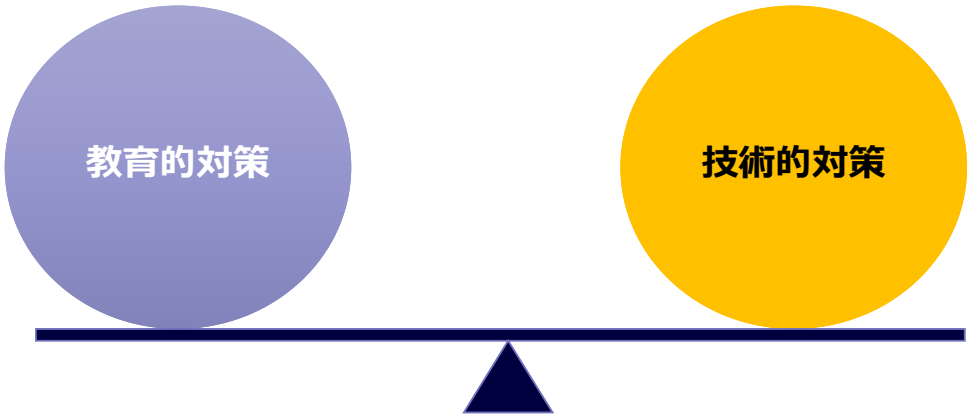
- ✓ 従来のような不自然な機械翻訳による日本語ではなく、組織内関係者を装った流暢な日本語によるメールも多くなってきている。
- ✓ 未知のウイルスにより、技術的対策が追いつかず組織内へのウイルスの侵入を防げないケースも考えられる。

背景

- 標的型攻撃メールにおける典型的な攻撃方法は、マルウェアを仕込んだ添付ファイルやマルウェアを感染させるためのURL付のメールを送り付け、受信者が誤ってこれらにアクセスすることでマルウェアに感染させることから始まる
- マルウェアの中には、ウイルスチェックソフトで検知されない、マルウェア感染してもPCの異常な動作といった症状が現れない場合もあるため、メール受信者自身が感染自体に気付かないまま、不正侵入、感染拡大を許し、その結果、重要情報が盗み取られる事態へと繋がる危険性がある
- 標的型攻撃メールに対する技術的対策として、マルウェア感染やその後の不正侵入、情報流出を困難にする仕組みを複数講じることで、**攻撃を非常に困難にすることは可能だが、完全に防御することはできない**のが現状
- このような背景から、技術的対策のみならず、メール利用者が**標的型攻撃メールの脅威を認識し、不審メールを開いてしまった時に適切な対応**をとることが、有効な防御となる

早稲田大学での訓練の目的

- 訓練は、標的型攻撃メールの理解と疑似的な不審メールの取り扱いの実地訓練を通して、**メール利用者の標的型攻撃メールへの耐性を高める**ことを目的として行う
- 訓練の継続的実施により、日常的にメール利用者の**不審メールに対する警戒感等の意識づけ**効果を期待する



訓練実施のきっかけ

- 2015年6月に発覚した本学業務用PCのマルウェア感染による情報流出インシデント
- 二次被害を防ぐため、業務で利用する特定の通信を除き、全ての業務用PCから外部への通信を遮断
- 訓練に一定の理解が得られ、2015年12月に比較的スムーズに実施

訓練の着眼点

- 巧妙化が進む標的型攻撃に対応した訓練メール
- サイバー攻撃への耐性強化を目的に「感染**予防**対応」、「感染**拡大防止**対応」の視点で目標を設定
  - ✓ サイバー攻撃の脅威に対する「意識(気づき)」を持つこと
  - ✓ 標的型攻撃メールの見分け方の「知識」定着を図ること
  - ✓ 不審メール受信時に適切な行動をとること
  - ✓ 不審メールのURLアクセスや添付ファイル開封時に適切な行動をとること
- 訓練結果の受講者へのフィードバック

訓練の流れ

- 業務用PCを利用する職員、派遣等を対象に実施

(0) オンデマンド事前学習
- ✓ 原則、着任時に視聴を依頼

↓

(1) 訓練告知
- ✓ 訓練実施2週間前程度に告知
- ✓ いずれは告知なしで実施予定

↓

(2) 訓練メール送信
- ✓ 複数の種類の訓練メールを用意し、種類別に時間間隔を開けて送信

(3) アンケート
- ✓ 訓練メール受信後の行動調査
- ✓ 回答率は6割程度

↓

(4) フィードバック研修
- ✓ 実際の感染事例紹介
- ✓ 訓練結果の報告

(0) オンデマンド事前学習

- IPA 発行の以下を参考に教材を作成
  - ✓ 標的型攻撃メール<危険回避>対策のしおり
  - ✓ テクニカルウォッチ 標的型攻撃メールの分析に関するレポート
  - ✓ テクニカルウォッチ 標的型攻撃メールの例と見分け方

- 事前学習の柱
  - ① ウイルスメールとは？
  - ② 標的型攻撃の手口イメージ
  - ③ 標的型攻撃メールとは？
  - ④ 標的型攻撃メールの特徴
  - ⑤ 「だましのテクニック」の着眼点
  - ⑥ 「だましのテクニック」の事例
  - ⑦ 特に注意すべきこと
  - ⑧ 身に付けておくべき基礎知識と予防対応

(1)訓練告知

- 告知から訓練メール送信まで、一定期間開けることで記憶を薄れさせることを期待

(2)訓練メール送信

- 複数の種類の訓練メールを用意(2017年度4種類)し、受信時に訓練メールであることを分かりづらくする
- 一方で、業務上の混乱を避けるために
  - ✓ 誤ってURL等アクセスしてしまった場合、訓練メールであることがすぐに分かるようにする
  - ✓ 当初は訓練メールの内容に関係する部署へ事前通知（2017年度は事前通知なし）
- 訓練メールの内容は後程、紹介

(3)アンケート

- 訓練メール受信後の行動を把握することが重要

(4) フィードバック研修

- フィードバック研修受講者は、各部署で選任されたセキュリティ担当者
  - ✓ 自部署へ戻って、講師役としてメンバーへ説明することを依頼

- フィードバック研修の柱
  - ① 背景
  - ② 事例
    - ✓本学へ送付された不審メール数と事例
    - ✓事務系PCでのマルウェア感染事例
  - ③ 標的型攻撃メール訓練
    - ✓目的、実施概要・結果、考察、今後について
  - ④ 不審メール受信時・開封時の適切な行動とは？
  - ⑤ 不審メール等の各種セキュリティ情報

（参考）アンケートから見る訓練受講者の反応

- 当初、訓練受講者の反応が懸念されたが、実施してみると想像以上に好評価

- ✓ 一般的な研修と比較して「意識が高まった」「再認識した」という肯定的な回答が多く得られたのが特徴
- ✓ アンケート回答者の７割は、訓練の実施に肯定的
- ✓ ４人に１人は、定期的に訓練を実施を希望
- ✓ 頻度を増やして実施した方がよいという要望は、約２%しかなかったことから、年に１回の訓練頻度が、適切
- ✓ 「箇所内でも話題にすることで情報セキュリティへの意識が高まるのも実感ができた。」
- ✓ 「日頃気を付けているものの、まだ十分ではないことが多いため、こうした研修でさらに意識を高めていきたい。」
- ✓ 「学生スタッフも含め日ごろから情報セキュリティに対して意識を高めるよい機会となりました。」

グループワーク

早稲田大学での訓練の流れ

- 業務用PCを利用する職員、派遣等を対象に実施

(0) オンデマンド事前学習
- ✓ 原則、着任時に視聴を依頼

↓

(1) 訓練告知
- ✓ 訓練実施2週間前程度に告知
- ✓ いずれは告知なしで実施予定

↓

(2) 訓練メール送信
- ✓ 複数の種類の訓練メールを用意し、種類別に時間間隔を開けて送信

(3) アンケート
- ✓ 訓練メール受信後の行動調査
- ✓ 回答率は6割程度

↓

(4) フィードバック研修
- ✓ 実際の感染事例紹介
- ✓ 訓練結果の報告

訓練の目標

- 巧妙化が進む標的型攻撃に対応した訓練メール
  ✓新たな攻撃メールに対応したコンテンツの充実を図る。

- サイバー攻撃への耐性強化を目的に「感染**予防**対応」、「感染**拡大防止**対応」の視点で2つの目標を設定

① 訓練メールのURLアクセス・添付開封率の低減

✓サイバー攻撃の脅威に対する「意識(気づき)」を持つこと
✓標的型攻撃メールの見分け方の「知識」定着を図ること
✓不審メール受信時の適切な行動をとること

② 訓練メールのURLアクセス・添付開封者全てが適切な行動をとる

訓練の概要

- **作成種類：** ４種類（４文×1タイプ（URL））
- **件名　　：** ①メールが管理ポリシーに抵触している恐れがあります。
  ②【重要】ISO9001の改定に伴う影響について
  ③【至急】職場環境調査の実施について
  ④【重要】情報システム端末に関わる緊急調査の実施について
- **差出人　：** ①情報セキュリティ対策委員会 <secure.taisaku.waseda@gmail.com>
  ②社会連携推進室 <syakai.renkei.waseda@gmail.com>
  ③職場環境改善委員会 <syokuba.kaizen.waseda@gmail.com>
  ④情報セキュリティ対策委員会 <secure.taisaku.waseda@gmail.com>
- **内容　　：**

✓ 「だましのテクニック」の着眼点、そのほかの気づきのポイントを複数含んだ訓練メール文を作成
✓ それぞれメール文中の**URLをクリックして確認するように促すタイプ**として作成
✓ 差出人メールアドレスとして**フリーメールのアカウント**を取得
✓ 本学ドメイン**を偽装**したドメインを取得し、**偽装URL**を使用

訓練の文例

標的型攻撃・模擬メールの見分け方のポイント

差出人："情報セキュリティ対策委員会"<secure.taisaku.waseda@gmail.com> ⑦
宛先　：●●●●@xxxxx.xx.xx
CC　：
件名　：メールが管理ポリシーに抵触している恐れがあります。

平成３０年1月１９日

メール送信者様

貴殿が送信したメールが、管理ポリシーに抵触している恐れがあります。詳細については、以下のURLを早急に確認し、管理者に問い合わせてください。⑨ Ⓐ

今一度、送信日時・宛先・件名から、送付したメールが問題ないかご確認ください。Ⓑ

<メールはこちら> Ⓒ
http://docs.weseda.jp/s/ner134nuk7520lia7195t45mik145eg565uok65ata879giket65465uoy
<http://docs. weseda.jp/entry/?～～～～～> ⑫

情報セキュリティ対策委員会⑬<secure.taisaku.waseda@gmail.com>

標的型攻撃・模擬メールの見分け方のポイント

今回送信したメールは、訓練用として以下の「だましのテクニック」の着眼点とそのほかの気づきポイントを設定してあります。

「だましのテクニック」の着眼点

① 知らない人からのメールだが、メール本文のURLや添付ファイルを開かざるを得ない内容（内部文書を装ったメール）
⑦ フリーメールアドレスから送信されている
⑨ 日本語の言い回しが不自然である（誤字がある（くだだい⇒ください））
⑫ 表示されているURL（アンカーテキスト）と実際のリンク先のURLが異なる
⑬ 署名内容が間違っている（実在しない組織である）

そのほかの気づきのポイント

A．早急に確認せよと急がせようとしている。
B．あからさまにURLアクセスを働きかけている。
C．URLが見慣れないものである。（「waseda.jp」ではなく「weseda.jp」）

このようなポイントに今後留意していただくとともに怪しいメールが届いたら、 URLをクリック（添付ファイルの場合は開封）してはいけません。標的型攻撃メールの疑いが強い場合は、速やかに削除してください。標的型攻撃メールの疑いが強い場合は、速やかにセキュリティ担当者へ報告し、対応の指示を受けましょう。

※「だましのテクニック」の着眼点はCourse N@viの「事務系における情報セキュリティ対策研修」、「標的型攻撃メールの基礎知識と予防」で確認ください。

訓練の文例

標的型攻撃・模擬メールの見分け方のポイント

差出人："社会連携推進室"<syakai.renkei.waseda@gmail.com> ⑦
宛先　：●●●●@xxxxx.xx.xx
CC　：
件名　：【重要】ISO9001の改定に伴う影響について

平成３０年1月１９日

各位 ④

２０１５年に、ISO9001が改定されました。これに伴う業務への影響について調査を行い、その結果を第１報として公開しました。各位におかれましては、内容をよくお読みいただき、自分の業務がどのようにかわるのかを確認してください。 Ⓒ

また、併せてアンケートを実施します。実際のQMSの改定は、この結果を加味しながら実施します。期間は平成３０年１月２６日までとなりますので、早めに回答してください。 Ⓐ

http://docs.weseda.jp/s/ner134nuk7520lia7195t45mik145eg565uok65ata879giket65465uoyh Ⓑ
<http://docs.weseda.jp/entry/?～～～～～> ⑫

以上

⑬
社会連携推進室<syakai.renkei.waseda@gmail.com>

標的型攻撃・模擬メールの見分け方のポイント

今回送信したメールは、訓練用として以下の「だましのテクニック」の着眼点とそのほかの気づきポイントを設定してあります。

「だましのテクニック」の着眼点

① 知らない人からのメールだが、メール本文のURLや添付ファイルを開かざるを得ない内容（内部文書を装ったメール）
④ 組織全体への案内
⑦ フリーメールアドレスから送信されている
⑫ 表示されているURL（アンカーテキスト）と実際のリンク先のURLが異なる
⑬ 署名内容が間違っている（実在しない組織である）

そのほかの気づきのポイント

A．期限を設定し、急がせようとしている。
B．URLが見慣れないものである。（「waseda.jp」ではなく「weseda.jp」）
C．業務に連携していると気を引いている。

このようなポイントに今後留意していただくとともに怪しいメールが届いたら、 URLをクリック（添付ファイルの場合は開封）してはいけません。標的型攻撃メールの疑いが強い場合は、速やかに削除してください。標的型攻撃メールの疑いが強い場合は、速やかにセキュリティ担当者へ報告し、対応の指示を受けましょう。

※「だましのテクニック」の着眼点はCourse N@viの「事務系における情報セキュリティ対策研修」、「標的型攻撃メールの基礎知識と予防」で確認ください。

不審メールを受信した場合の対応例

- 不審メールを受信した場合、以下の対応を周知

A)「だましのテクニック」の着眼点に複数合致している。
B)業務上、添付ファイルを開封（本文中に記載のURLへアクセス）する必要がある。

✓ **A)、B)のいずれにも当てはまる不審メールを受信した場合**
- 添付ファイルを開封（URLアクセス）せずに、担当者を通じて以下へ連絡
- 口頭等により箇所内で情報共有
- 担当者が不在の場合は、本人より連絡

✓ **B)の内容であるが、A)の判断に迷う不審メールを受信した場合**
- 添付ファイルを開封（URLアクセス）せずに、情報部門へ連絡

✓ **A)のみに当てはまる不審メールを受信した場合**
- 当該メールは原則として削除
- 口頭等により部署内で情報共有
- 情報部門への連絡は不要

不審メールの添付ファイル開封（URLアクセス）した場合の対応例

- 不審メールの添付ファイル開封（URLアクセス）をした場合、以下の対応を周知

✓ 担当者を通じて情報部門へ連絡
✓ 口頭等により部署内で情報共有
✓ 担当者が不在の場合は、本人より連絡

- 情報部門が管理するセキュリティ機器でマルウェアを検知した場合、当該PCをネットワークから遮断

- メール利用者の感染に至った状況や箇所内での対応状況を把握し、適切な対応および情報共有を目的として報告書を提出

本学の事例が皆様の参考になれば幸いです。

ご静聴ありがとうございました。