不正メールの脅威の実例

リスク工学グループ演習第 5 班
舟橋聖人　三島貴務　太田洋平　周億琳
アドバイザー教員　面和成

1 背景・目的

近年，フィッシングメールやマルウェア感染といった不正メールによる特定の組織や個人を狙った情報窃盗等の被害が増加している[1].

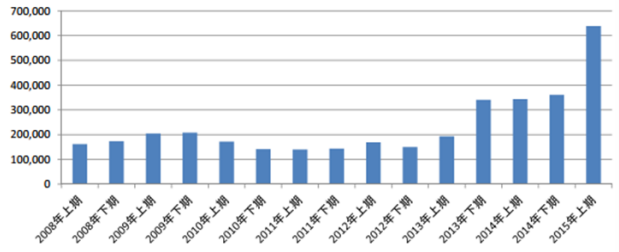


図 1 APWG へのフィッシングメール届け出件数[2]

このような不正メールの手口として，添付ファイルを開かせることでウイルスに感染させたり，特定のサイトに誘導したりすることで気付かれないようにウイルスを送りつけるなどが挙げられる[2]. また，正当な業務や依頼であるかのように見せかける件名や本文でメールを送りつけ，受信者が騙されやすいような仕掛けをしているので被害を受けやすい．これらの対策として，利用者は発信元に問い合わせるなどして受信したメールの信頼性を確認する，添付ファイルを開かない，リンク先を安易にクリックしないなど十分な注意を払う必要がある．しかし，「自分は大丈夫だろう」や「大したことにはならないに違いない」といった正常化の偏見を持っていることが多い．今回の目的として不正メールを実例に基づいて解析または分析することで，脅威を深く認識し，意識の改善を目指す.

2 不正メールについて

まず不正メールとは悪意のある第三者がウイルス等，何らかの手段で入手したメールアドレスを用いた”なりすまし”によるメールの総称であるが，例として以下の二つを紹介する.

1. フィッシング
金融機関などを装った電子メールで氏名や口座番号，クレジット番号などの個人情報を搾取するものである．特に添付されているリンクから偽サイトに誘導し，個人情報を入力させる手口が一般的である．図 2に実際にあったフィッシングメール・サイトの一例を示す.

図 2 三菱東京 UFJ 銀行をかたるフィッシングメールとフィッシングサイト[2]

2. マルウェア
コンピュータウイルスも含め，悪意を持つソフトウェアの総称であり，ワームやスパイウェア，ランサムウェアなどがある.

3 手法・手順

今回実験を行う際に安全に留意して行った．実験には実験専用の PC を用いて，不正メールは仮想空間上で実行し，筑波大学のネットワークは使用しないことにした．それらを考慮した実験手順を以下に示す.

1. ホスト環境(セキュリティ対策を行う)に仮想環境(脆弱性を残す)を作った.

2. 仮想環境上で不正メールを実行した際に意図せず動作しているプロセスはないか，もしあった場合はプロセスによりファイルやレジストリの書き換えが発生していないかを確認した．

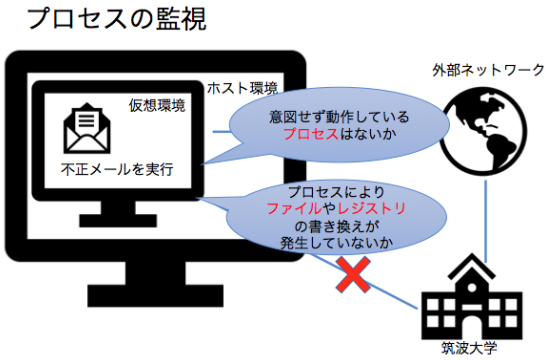


図 3 プロセス監視の模式図

3. 2 より不正な通信があった場合，どこと通信しているのか，通信内容は何であるかを確認した．ここでマルウェア的なウイルスの時は PC 内部にレジストリの監視とパケットの監視を両方行い，フィッシング的なウイルスの場合，PC そのものに及ぼす影響はないと考え，パケットの監視のみを行った．

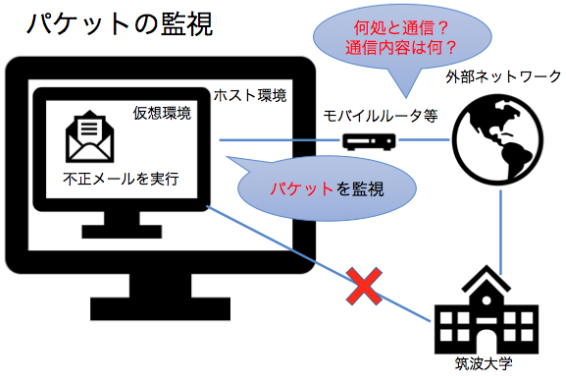


図 4 パケット監視の模式図

実験環境に用いた OS，ソフトを表 1 に示す．不正メールの解析対象は Web に公開しているメールアドレスに 2017 年 4 月 20 日から 6 月 20 日までに届いた 33 通とした．また，別途にいくつか解析対象外の不正メールの解析も行った．理由については後述する．

表 1 実験環境

仮想化ソフトウェア	VirtualBox 5.1
ホストOS	Windows 7
ゲストOS	Windows 7, Windows 8
仮想環境の ネットワークアダプタ設定	NAT
パケット監視ソフトウェア	Wireshark 2.2.7
プロセス，ファイル， レジストリ監視ソフトウェア	Microsoft Process Monitor 2.95

4 解析結果

解析対象となった不正メールの内訳を図 5に示す．結果として，本文中にサイトの URL のみが貼り付けられているケースが多かった．しかし，サイトの URL はサイトが無くなっていたためアクセス出来ない場合がほとんどだった．この原因として不正メールの送信者が一定時間経過後に痕跡を消し，インターネットの取締などから免れるためであると考えられる．それにより，不正メールの実態が掴みづらい原因になっている．そのため，解析対象とは別途に受信後 24 時間以内に URL が添付された不正メールの解析を行った．その解析結果を 4.1, 4.3 に示す．

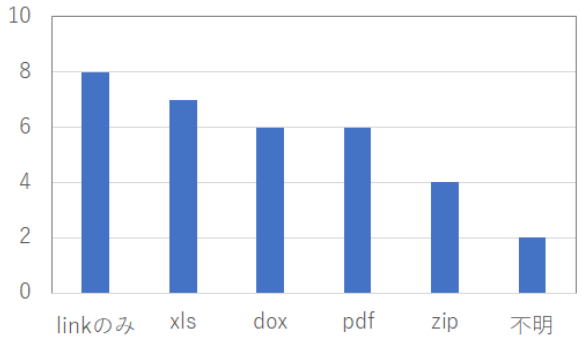
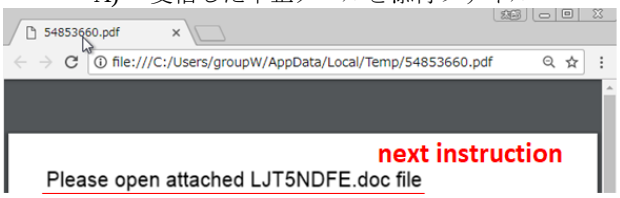


図 5 受信した不正メールの種類

不正メールの中には，図 6のように添付ファイルを開くと新たな指示があり，その指示に従っていくと危険性が増していくものもあった．不正メールの送信者が痕跡を分かりづらくするため，複数の動作を受信者に強いるようにしたためであると考えられる．

A) 受信した不正メールと添付ファイル



B) 開いた添付ファイルによる新たな指示

図 6 段階的な指示を出す不正メール

以上の結果の他に以下のような不正メールの特徴があった。

- 日本語が不自由なものが多かった（外国人が書いたためであると考えられる）
- マルウェアを添付したメールよりフィッシングメールの方がサイトへの誘導が巧妙だった
- マルウェア感染は通常のように PC を使用していても気づけないものが多かった

- 添付ファイルの拡張子を偽装しているものが多かった

不正メールを解析する中で得られた不正メールの脅威の実例を 4.1-3 で紹介する．

4.1 Apple を装ったフィッシング

メール内容

Subject: 警告 : あなたの盗難 ID は，認識されていないすべてのデバイスから iCloud に記録されました．
Date: 6 Sep 2017 01:36:33 +0200
From: Apple ID <Impoortanss-accountssummaryedes221@blackmates-kanjutkebod.mail.live.msn.hotmail.gmail.com>
To: [redacted]

Dear Client,

セキュリティ上の理由により, Apple ID がロックされています．
誰かが別の IP アドレスから Apple ID にログインしました．

日時： 6 September 2017, 07:15:35 GMT
デバイス： iPhone 7 plus
lP: 92.165.127.15 (United States)
オペレーティング· システム： iOS 10.3.3

あなたのアカウントはロックされています．あなたのアカウントを引き続き使用するには，下記のリンクをクリックして情報を更新してください．
更新したら，アカウントをもう一度使用し続けることができます．

ログインするにはここをクリック <http://bit.ly/2xMFb17>

アカウントにログインできない場合は，すぐにお知らせください． 重要なのは，誰もあなたの知らないうちにあなたのアカウントにアクセスしていないことを確認するためです．

SincereIy,

Apple Support

このメールに返信しないでください． 私たちと連絡を取るには，ヘルプと連絡先をクリックしてください．

Apple ID <http://bit.ly/2xMFb17>| Support <http://bit.ly/2xMFb17>| Privacy Policy <http://bit.ly/2xMFb17>
Copyright © 2017 Apple Distribution International.All rights reserved.

このメールに記載された短縮された URL をクリックすると本物と見分けの付かない偽のサイトに飛ばされる（図 7）．本物のサイト（図 8）と外見のみで見分けることはほぼ不可能であるが, ID とパスワードに適当な文字列を入力することで次のページへ進むことができること，よくある質問などのリンク先は準備がされてなく，すべて自分自身へのリンクが貼られていることなどから偽物であることが判断できる．何よりも URL が Apple のものではない．適当な文字列を入力しログインする（ここで ID とパスワードのペアが漏れる）と，アカウントのロック解除を名目に，個人情報（氏名，生年月日，電話番号，住所）とカード番号（番号，期限，セキュリティコード）の入力を促される（図 10）．ある程度の入力チェック機能があり，クレジットカードの桁数などが間違っていると再入力を求められる．

図 7 偽物の Apple のホームページ（上部にメニューバーがないのはキャプチャミス）

図 8 本物の Apple のホームページ

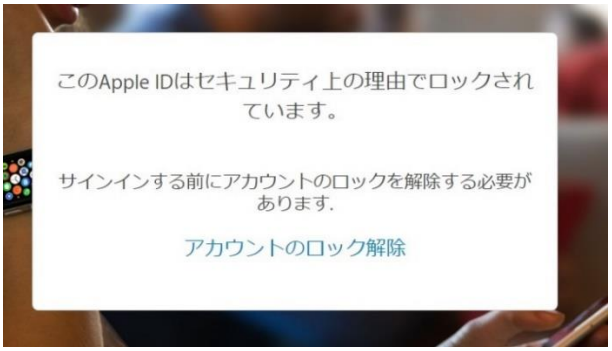


図 9 細部への工夫

図 10 個人情報入力画面

すべての入力を終えると，セキュリティのためログアウトしますと表示され，本物の Apple ページへと飛ばされた．

興味深いのは，一度個人情報とカード番号を入力した後に，メールのリンクをクリックすると偽物ではなく本物の Apple のページへと飛ばされるようになることである．また，この数日後に偽物のページは削除された．被害者に詐欺にあったことを気づかせない工夫や痕跡を残さないための工夫がみられた．

4.2 レジストリやファイルの書換えを行うマルウェア

メール内容

Subject:	日本通運 CSD 提供データ
Date:	Thu, 27 Apr 2017 08:43:09 +0100
From:	ise@ari.bbiq.jp
To:	[redacted]

添付ファイルに関するお問い合わせは，下記までご連絡下さい．
日本通運（株）CSD コールセンター
電話番号：0120-02-2438

このメールには添付ファイルとして，zip ファイルが添付されている．zip ファイルを解凍すると拡張子を csv と偽造した exe ファイルが現れる．これは圧縮形式を用いることによりパターンマッチングによるウイルス検知を回避することを目的としていると推測できる．

Windows8 の環境でこの exe ファイルを実行すると，ファイルやレジストリの書き換えが発生した．具体的には，エラー報告や診断サービスを提供する Windows Error Reporting 機能の無効化や，DLL インジェクションの攻撃対象として報告されている sysmain.sdb[3]の書き換えなどが行われた．しかし実験の期間内にはこのプログラムによる不審なパケット通信は観測されず，プログラム実行時に数秒ほど処理が重くなることを除いてはコンピュータに悪影響を及ぼさず，何を目的としたものであるかは特定できなかった．

この例の他にも添付ファイルを実行すると，レジストリなどの書き換えが発生しているのにもかかわらず目に見える悪影響が発生せず，感染しているという実感がわかないものが多数あった．

時間を置いた後の悪意ある動作や，マルウェアによる仮想環境の検知などが考えられるが，感染していることに気づくことが出来ないマルウェアが多数存在することには注意せねばならない．

4.3 ウィズダムプロジェクト

メール内容

Subject:	参加申請（無料）→7 万円プレゼント
Date:	Sep, 12 Apr 2017 15:39
From:	mail@pc-bigs.net
To:	[redacted]

下記 URL から『特設サイト』へ飛び，
プロジェクトへの参加申請手続き（無料）を行うと
今日から毎日 7 万円を差し上げます．
参加申請手続きは 30 秒，
長くても 1 分で完了しますので今のうちに
行っていただくようお願い致します．
参加申請手続きはこちら

http://tinyurl.com/y775477a

…続く

メールで述べられていたプロジェクトの名前は「ウィズダムプロジェクト」と呼ばれ，登録して指示に従うと 1 年後には 1 億円を手に入れられるという趣旨であった．

このプロジェクトにメールアドレスを用いて参加登録を行うと，ある動画を視聴するように促された．動画は約 40 分程度のもので YouTube にアップされていた．この動画ではプロジェクトの趣旨，1 億円を手に入れるための大まかな流れ等が説明されていた．この動画の視聴が終わると次回の動画の予告があり，予告によると動画視聴日の次の日に第 2 話がアップロードされるということだった．

第 2 話以降は動画を視聴したり，受信したメールを開いたりせず無視したため，最後まで指示に従うとどうなるかは分からなかった（動画は段階的に 5 話までアップロードされていた）．

このプロジェクトでは敢えて段階的に動画を視聴させることで，最後まで説明を聞いた騙されやすい人をピンポイントで狙う詐欺のようなものであったと考えられる．

図 11 ウィズダムプロジェクト会員登録画面

図 12 ウィズダムプロジェクトの概要説明の動画

5 被害低減に向けて-対策

本稿ではいくつか不正メールの脅威の実例を紹介した．不正メールの脅威を調べていく中で得られた，不正メールから身を守るための方策を述べる．

まず，フィッシングサイトについて．図 7 と図 8 を見ると，偽物と本物のサイトを見た目で判断することは非常に難しい．しかし，フィッシングサイトの URL は本物のサイトの URL と異なる．

本物のサイト：
https://appleid.apple.com/#!&page=signin
偽物のサイト：
https://appid-accnts-jp51212521616763422.com/

例えば，よくネットバンキング等を利用する人はログインの度に必ず URL をチェックする癖を付けることでフィッシングメール・フィッシングサイトによる被害を受けなくなる可能性が非常に高くなる．たとえフィッシングサイトに誘導されても URL が違うことによってすぐに気づくことができると考えられるからである．

次に，マルウェア感染について．マルウェアに感染させられるようなサイトや実行ファイルにアクセスしても，PC が感染しているかどうか分からない場合がほとんどだった．そのため，現実においても感染しても気づかないケースがほとんどであると考えられる．この対策として，そもそもマルウェアに感染しないようにすることが挙げられる．例えば，使用している OS やソフトウェアを常に最新の状態にしておくことや，セキュリティソフトを使用するなどの対策できる．

しかし，マルウェアやフィッシングサイトは日に日に進化している．現在どのようなマルウェアが流行しているか知るだけでも被害低減の対策になり得ると考えられる．

6 まとめ

本稿では不正メールの脅威を認識し，意識の改善を図るために不正メールの解析を行った．

不正メールの解析は安全に留意して行った．具体的には，大学のネットワークを使用しない，不正メールの実行は仮想空間上で行い悪質な通信がないか監視する等の対策をした．

不正メールの解析により，不正メールからアクセスできるネットワーク上の不正なサイトは多くの場合，一定時間経過後(24 時間程度か)に削除されることが分かった．これは不正メールの送信者が痕跡を消してネットワークの取り締まりを免れるためだと考えられる．

Apple を装った不正メールでは，フィッシングサイトに誘導され Apple ID やクレジットカード番号の入力を求められた．このフィッシングサイトは緻密に作られており，見た目だけで本物の Apple のサイトと見極めるのは困難であった．

日本通運を装った不正メールでは zip ファイルを解凍して得られた exe ファイルを実行することでレジストリやファイルの書き換えが行われた．解析上でレジストリが書き換えられても PC 使用時に目に見える悪影響を及ぼすことはなかった．このため，PC がマルウェアに感染しても気づかない可能性が高いこと考えられる．

以上の解析を経て，被害低減のために以下のような対策を行うのが望ましい．バンキングサイト等のログイン時は必ず URL の確認を行うことである。これにより，フィッシングサイトによる被害の対策ができる．フィッシングサイトはサイトの見た目を模倣できても URL までは一緒にできないからである．また，マルウェアに感染してもほとんどの場合は気づかないと考えられるため，OS やソフトウェアを常に最新の状態にしておくなど，日頃の対策が重要であると考えられる．

最後に本稿では，OS による脆弱性の違いや，アップデートあり・なしによる感染のしやすさ等の解析ができなかった．そのため，マルウェアに感染する不正メールなどを異なる環境下で実行し，挙動を解析することで PC の環境による不正メールのリスク評価ができると考えられる．以上が今後の課題であり，来年以降のグループ演習での解決を期待したい．

参考文献

[1]. 経済産業省 日本ネットセキュリティー協会, http://www.jnsa.org/ikusei/spam/07_01.html, 2017 年 10 月 12 日確認
[2]. 日本フィッシング対策協議会, https://www.antiphishing.jp/consumer/abt_phishing.html, 2017 年 10 月 12 日確認
[3]. Windows Shim Database (SDB) Parser (shims), https://www.tzworks.net/prototype_page.php?proto_id=33, 2017 年 10 月 12 日確認