不正メールの脅威の実例

5班
舟橋聖人
太田洋平
三島貴務
周億琳
アドバイザー教員：面和成

発表内容

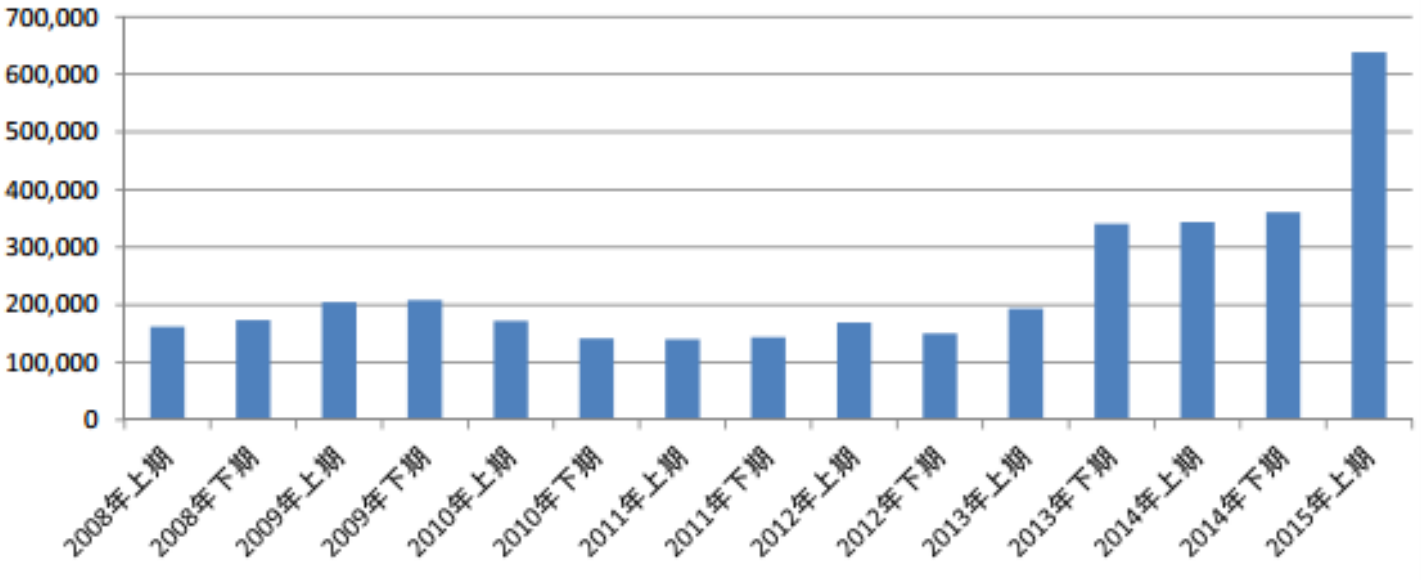
- 研究背景
  - フィッシングメールについて
  - マルウェア感染について
- 研究目的
- 実験概要
- 解析結果
  - 不正メールの特徴
  - 脅威の実例
    - Case1 Appleを装ったメール
    - Case2 ファイルやレジストリの書き換えを行うマルウェア
    - Case3 ウィズダムプロジェクト
- 考察
- まとめ

研究背景

近年、不正メールによる被害が拡大している

- フィッシング
- マルウェア感染
- スパムによる架空請求など

出典：フィッシング対策協議会



APWGへのフィッシングメール届け出件数

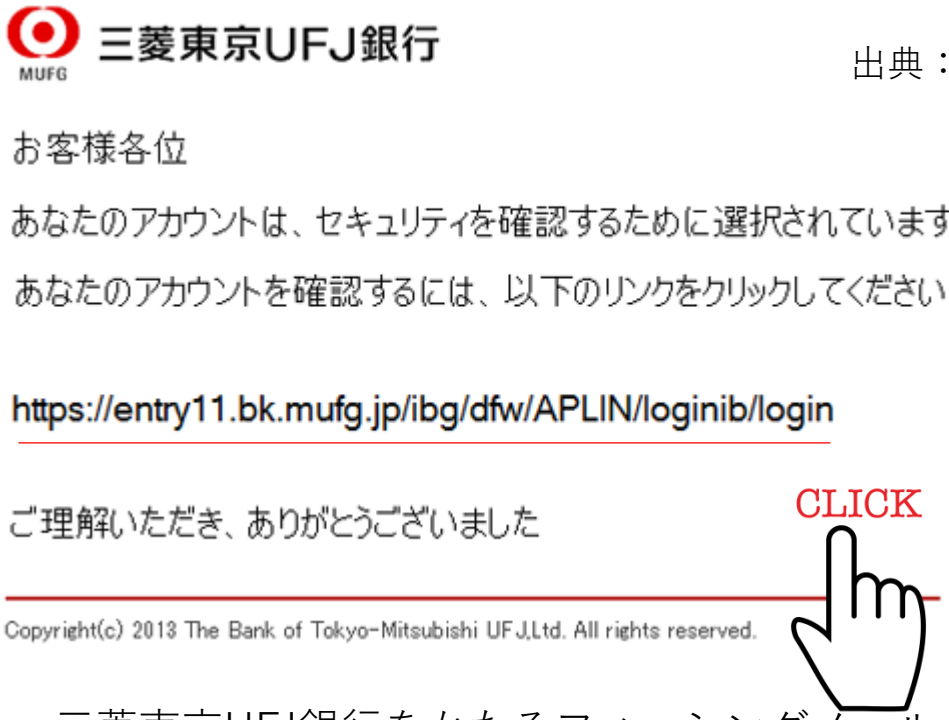
フィッシングメールについて

フィッシング(phishing)

金融機関などを装った電子メールを送り、氏名や口座番号クレジットカード番号などの個人情報を搾取する行為

電子メールの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

出典：フィッシング対策協議会



三菱東京UFJ銀行をかたるフィッシングメール

フィッシングメールについて

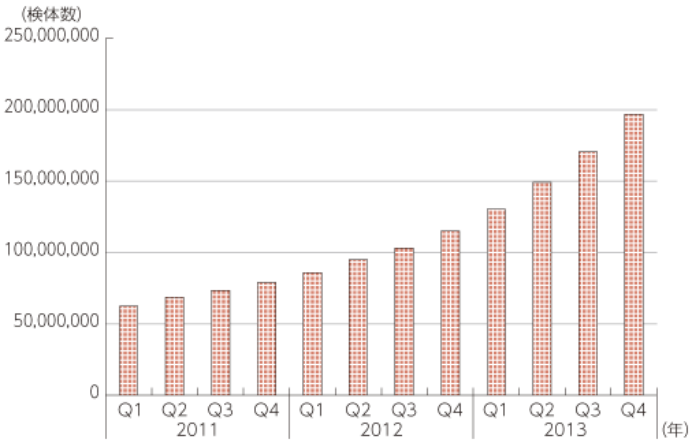
出典：フィッシング対策協議会

三菱東京UFJ銀行をかたるフィッシングサイト

マルウェア感染について

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

- ワーム
  - 独立したプログラムであり、ネットワークを介してPCからPCへ感染、ファイル破壊やシステムの異常終了等が発生する恐れ
- スパイウェア
  - ユーザーが知らない間に情報収集し、集めた情報をスパイウェア作成者に送信、パスワード等ユーザーの情報を悪用
- ランサムウェア（身代金要求型不正プログラム）
  - 感染したPCをロックしたりファイルを暗号化することで使用不可能にし、元に戻すことと引き換えに「身代金」を要求するプログラム



世界のマルウェア検体の増加状況

総務省より

研究目的

そもそも
不正メールって？

危険そうだけど
よく分からない

自分は
大丈夫

大したことに
ならないはず

不正メールの脅威を認識し
意識の改善を目的

実験概要

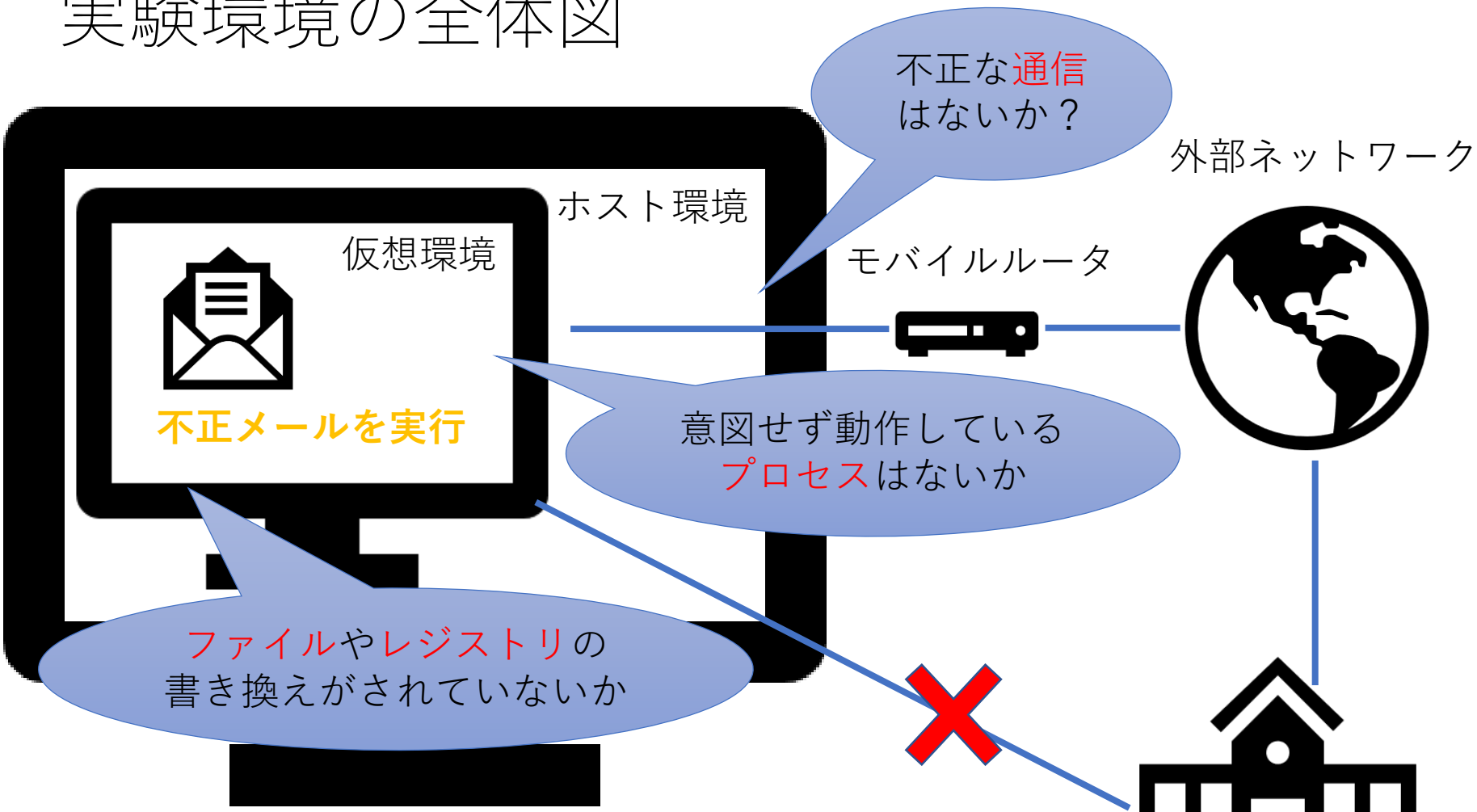
実際に届く不正メールの脅威を解析
- リンク先のWebサイト
- 添付ファイル

監視対象
- パケット：通信内容
- プロセス：実行中のプログラム
- ファイル：データ
- レジストリ：OSやソフトウェアの設定

調査する不正メール
- Webに公開しているアドレスに2ヶ月以内に届いたメール

不正メールの
詳細な挙動を知る

実験環境の全体図



- 仮想環境で不正メールを実行
- 筑波大学のネットワークは使用しない

実験環境

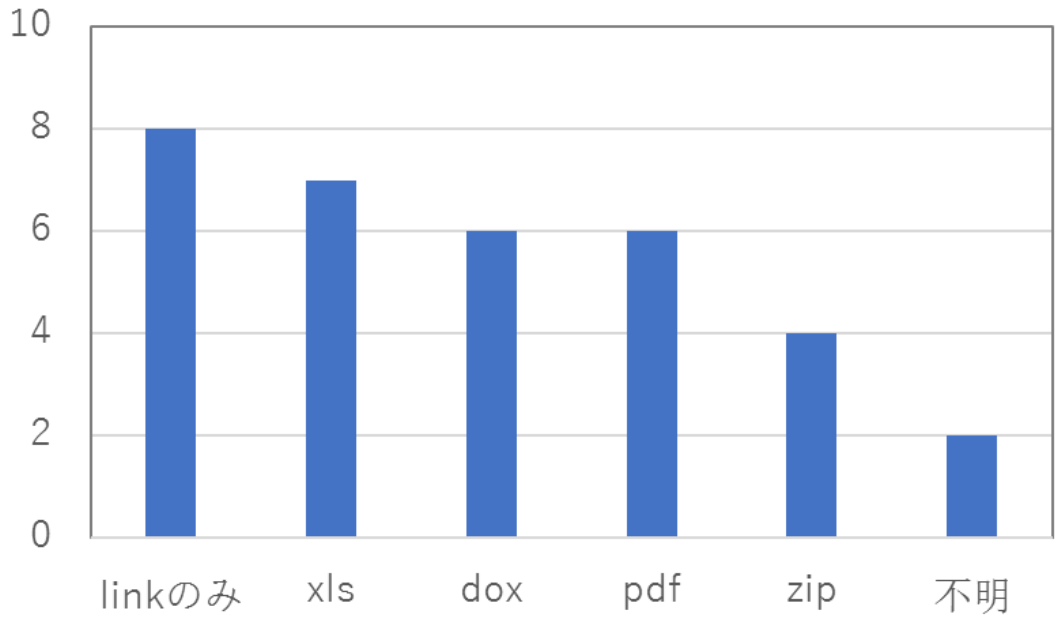
仮想化ソフトウェア	VirtualBox 5.1
ホストOS	Windows 7
ゲストOS	Windows 7, Windows 8
仮想環境の ネットワークアダプタ設定	NAT
パケット監視ソフトウェア	Wireshark 2.2.7
プロセス，ファイル， レジストリ監視ソフトウェア	Microsoft Process Monitor 2.95

[参考：本実験におけるルール]
1) ホストOSはWindowsアップデートを最新にしアンチウイルスソフトをインストール.
2) 実験用PCは，筑波ネットワークに一切接続しない.
3) 実験用PCをインターネットに接続する際は通信異常がないか常に監視する.
4) 不正メール（添付ファイル付き）は公開ネットワークに置かず，厳重に管理する.

解析結果

解析対象となった不正メール（33通）

- リンクのみ…8つ
- xlsファイル…7つ
- doxファイル…6つ
- pdfファイル…6つ
- zipファイル…4つ
- 不明(拡張子なし)…2つ



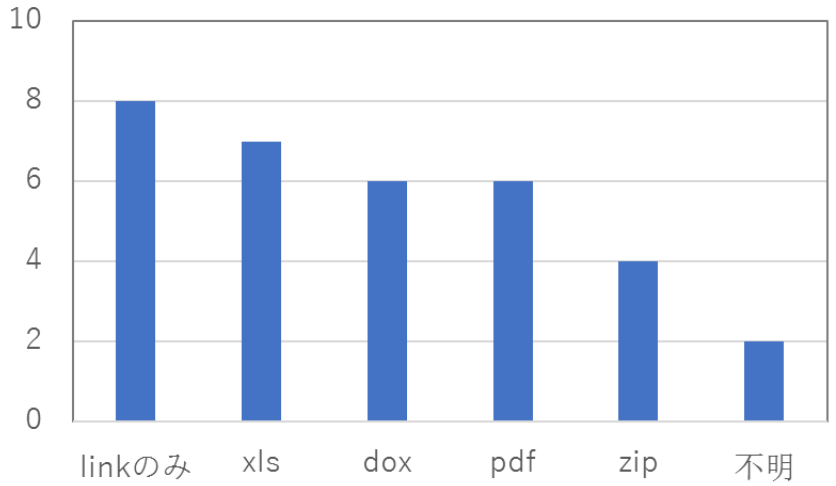
受信した不正メールの種類

不正メールの特徴

- URLのみが添付されているものはリンク先のサイトにアクセスできない場合がほとんどだった
  - ➢ 不正メール送信者が痕跡を消すために削除していたためか

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

→Case1、Case3

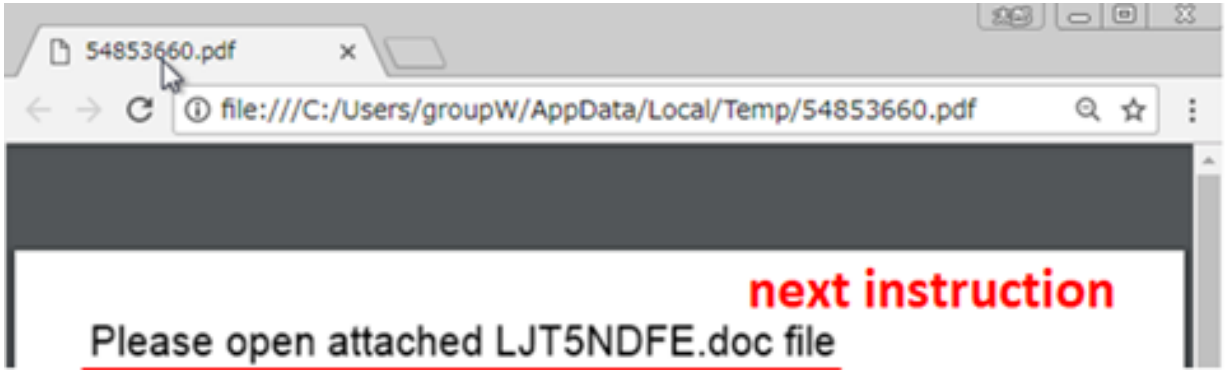


受信した不正メールの種類

不正メールの特徴

- 段階的な指示を出す不正メール

受信した不正メールと添付ファイル



開いた添付ファイルによる新たな指示

- 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か

不正メールの特徴

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
- 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

実例の紹介

- Case1 Appleを装ったメール
- Case2 ファイルやレジストリの書き換えを行うマルウェア
- Case3 ウィズダムプロジェクト

Case1：Appleを装ったメール①

- 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:

A pple ID <Impoortanss-accountssummaryedes221@blackmates-kanjutkebod.mail.live.msn.hotmail.gmail.com>

- To:

[redacted]

Case1： Appleを装ったメール②

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
IP: 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.

Case1： Appleを装ったメー

クリック

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
確認するためです．

クリックするだけなら
大丈夫というわけではないので注意

Sincerely,

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>

ページ内のリンクは
自身へのもの

Appleのすべての

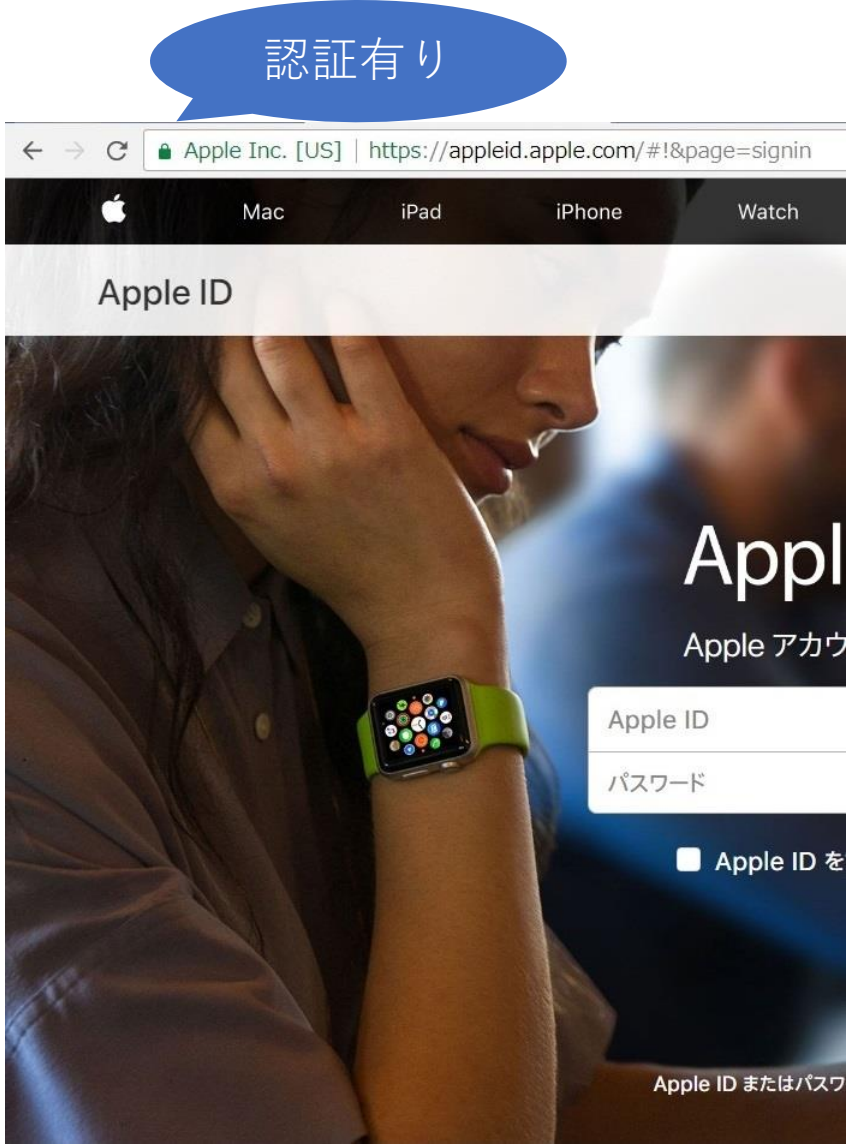
単一のApple IDとパスワードにより、すべてのAppleサービスにアクセスできま

Apple IDの詳細›

Appleを偽装した
フィッシングサイト

偽物

認証有り



本物

見た目による判断はあてにならない

ログインする

- 偽物ページは架空のIDとパスワードでログインできる
- ただし入力したIDとパスワードのペアは収集されると考えるのが自然

Apple IDで管理できるもの

メール，連絡先，バックアップデータ，

クラウド上のデータ（写真など），支払情報など


保護された通信 | https://appid-accnts-jp51212521616763422.com/Login.php?sslchannel=true&sessionid=g3Hry9uNm6wJ7dIsj1if…
Mac
iPad
iPhone
Watch
TV
Music
Support
Apple ID
サインイン
Apple IDを作成する
よくある質問
このApple IDはセキュリティ上の理由でロックされています。
サインインする前にアカウントのロックを解除する必要があります.
アカウントのロック解除
Apple IDまたはパスワードをお忘れですか？

保護された通信 | https://appid-accnts-jp51212521616763422.com/Step1.php?a@aaa&Account-Unlock&sessionid=41fX7aXuYKUaoHci…

アカウントのロック解除の名目で
個人情報を入力

続ける 当社のサービスを使用して、アカウントのセキュリティを維持するための検証を行う必要があります。 確認プロセスが完了するまでアカウントは無効になります

個人情報

- ファーストネーム
- ミドルネーム（オプション）
- 苗字
- 生年月日
- 電話番号
- 住所欄
- 町/都市
- State/Province

次

次ページでカード情報を入力
（キャプチャは事故により紛失）

Apple IDにTwo-Factor認証を使用してアカウントをより安全に保つ<

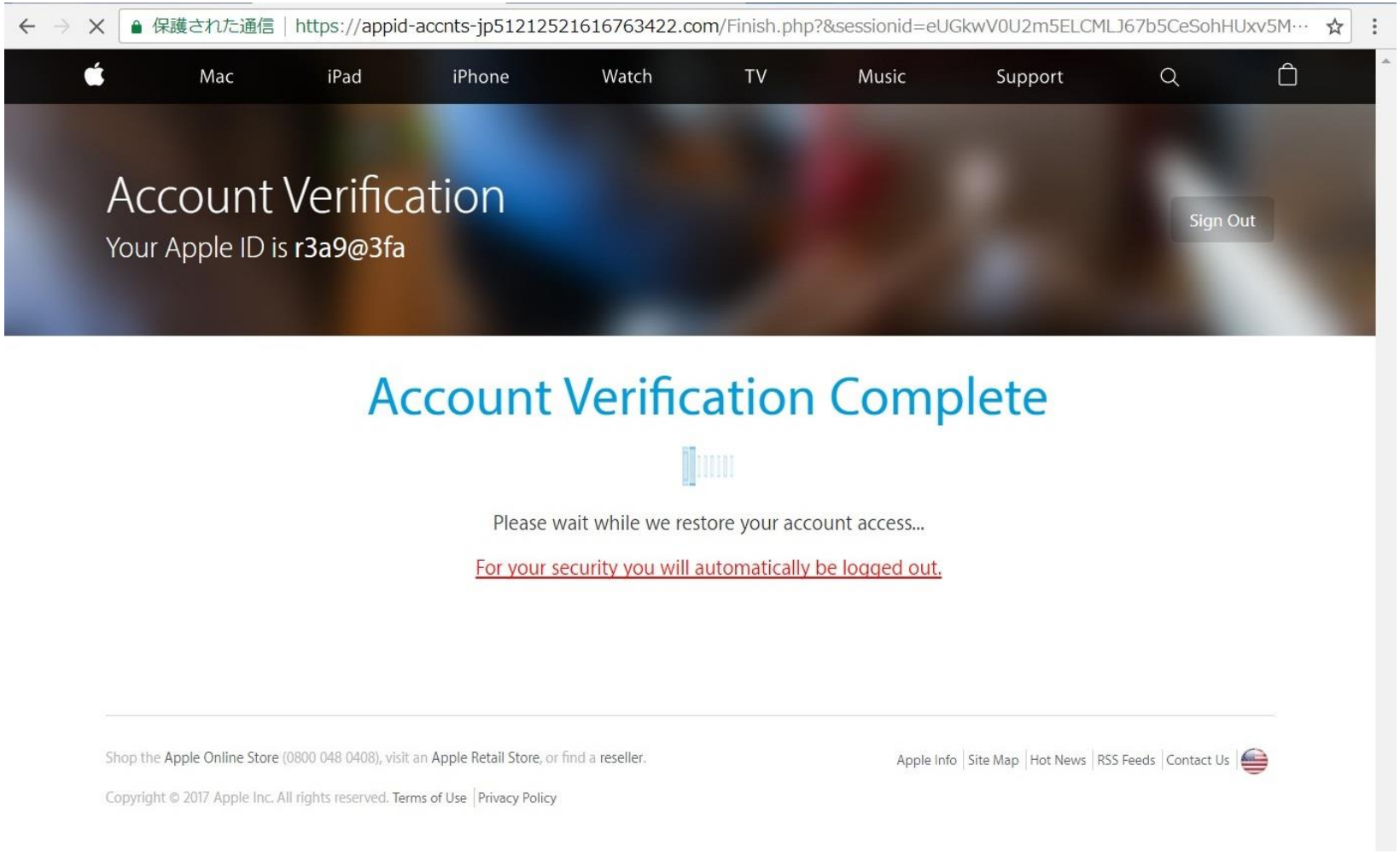
セキュリティの質問を選択

母親の旧姓

- セキュリティに関する質問を選択
- 母親の旧姓
- 運転免許証番号
- パスポート番号

フィニッシュ

二要素認証の回避



すべての入力が終わると自動的に本物のAppleのページへ移動する

その後

個人情報を入力後にメールにあるリンク
http://bit.ly/2xMFb17
をクリックすると本物のAppleページへ移動するようになる
（入力前と入力後で挙動が異なる）

偽物ページ（履歴に残っている）は
数日以内に消滅を確認

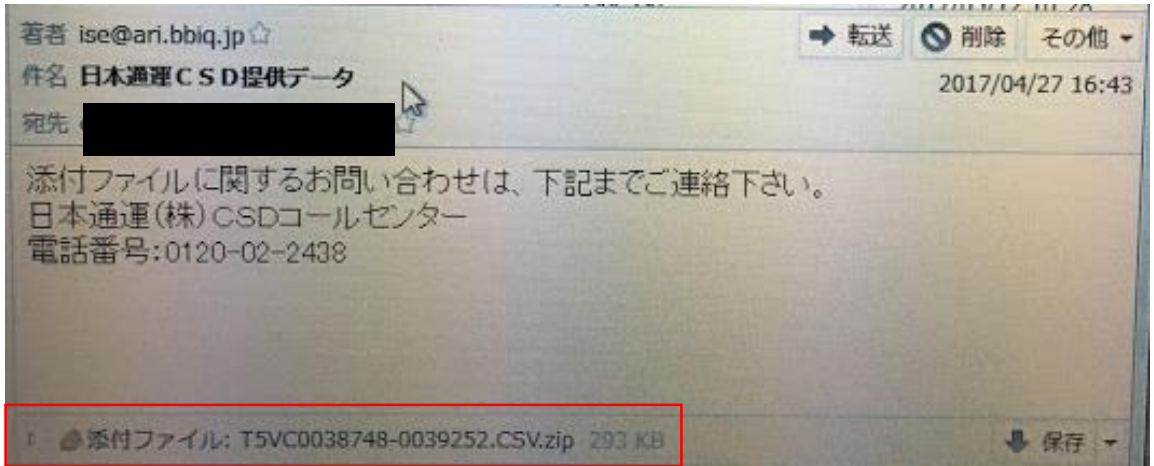
フィッシングサイトの解析結果

- 多くのフィッシングサイトは
  メールが来た数日後には消える（分析回避のためか）
- 見た目での判断は難しい
  （本物を徹底的に模倣している）
- 細部までこだわって作成されている
- https通信で安全そうに見える
- 騙されたことに気づかせない工夫がある

Case2：レジストリやファイルの書換えを行うマルウェア

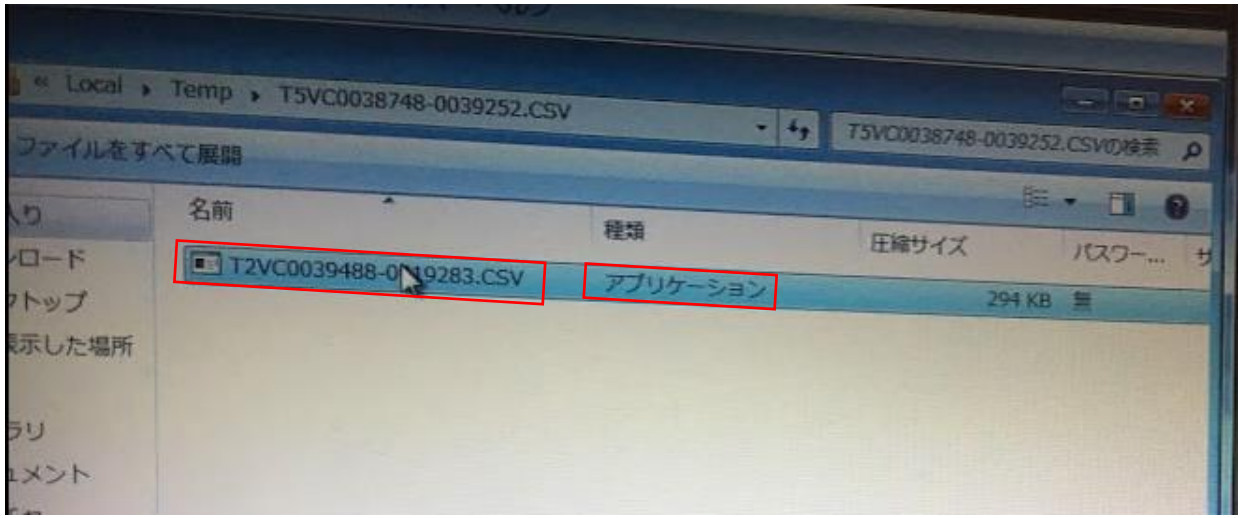
- Subject:　日本通運CSD提供データ
- Date:　Thu, 27 Apr 2017 08:43:09 +0100
- From:　ise@ari.bbiq.jp
- To: [redacted]

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



Case2：レジストリやファイルの書換えを行うマルウェア

- zipファイルを解凍すると拡張子をcsvに偽装したexeファイルが現れた
- exeファイルを実行するとファイルやレジストリが書き換えられた（Windows error ratingの無効化など）
- 実際に使用していても、目に見える悪影響は生じなかった
  （感染には気づけない）



Case3 ：ウィズダムプロジェクト

- 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

Case3 ：ウィズダムプロジェクト

- 会員登録をすると40分程度の動画の視聴を促された
- 動画は全5話（今回、視聴したのは1話のみ）
- 敢えて、全5話の動画を視聴させ、最後まで見てしまう騙しやすい人間をピンポイントに狙う詐欺のようなものか

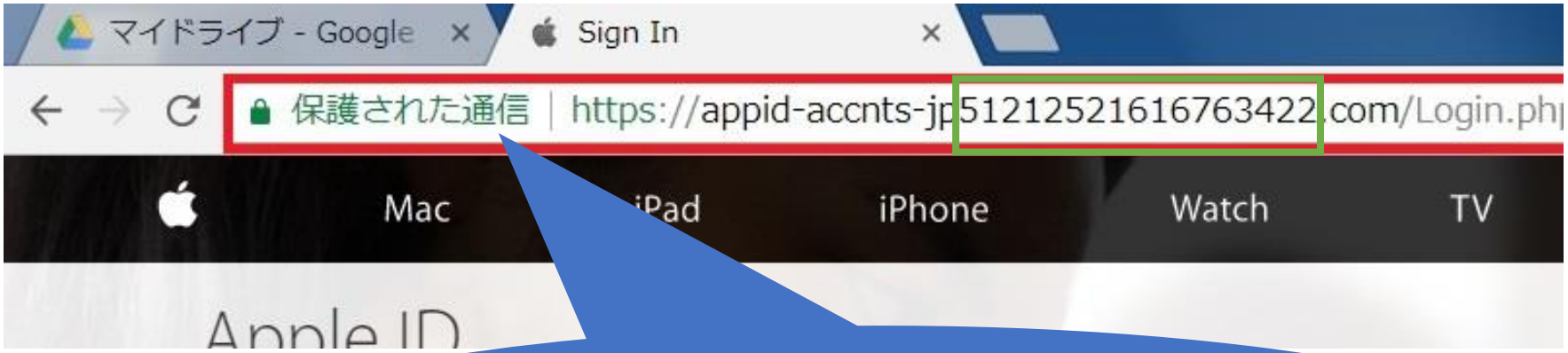
ウィズダムプロジェクト登録画面

説明動画（第1話）

解析結果の考察

<フィッシィングサイト>

- 今回のケースはURLが不自然だったので、URLで判断することが可能か
- しかし、有名でないサイトでは判断が難しいと感じた



通信が保護されていても（https通信）
悪意のあるサイトかもしれない

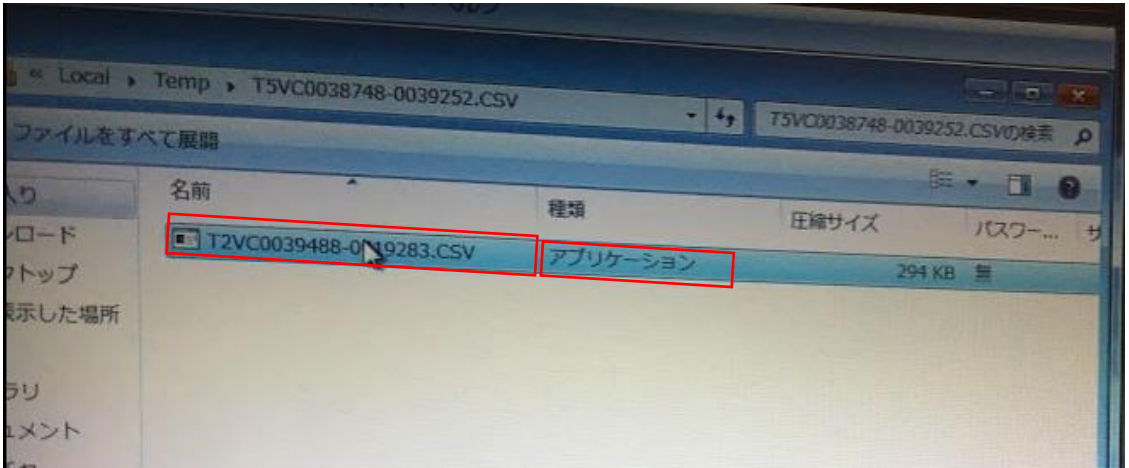
解析結果の考察

<マルウェア>

自分のPCが感染しているかどうか分からなかった

感染しても多くの人は気づかない
そもそもマルウェアに感染しないことが重要

危険なファイルの拡張子の偽装（Case2）



exeファイルは警戒されやすいが、csvファイルはより実行されやすいと感じた

まとめ

不正メールの脅威を認識し、意識の改善を図る

解析

<解析結果よりわかったこと>

- 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、一定時間通過後に削除された
- フィッシィングサイトは緻密に作られており、見た目だけで本物か偽物かを判断するのは難しかった(Appleのサイトなど)
- マルウェアではより感染させやすくするために添付ファイルの拡張子を偽装しているものがあった

<今後の課題>

- 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

最後に

今回の実験は
・大学のネットワークを利用しない
・不正メールの実行は仮想空間上で行う
・悪質な通信がないか常に確認する
等、安全に留意して行いました

参考文献

[1] 日本フィッシング対策協議会

https://www.antiphishing.jp/consumer/abt_phishing.html

[2] Norton Blog, マルウェアとウイルスの違い

https://japan.norton.com/malware-virus-difference-2041

[3] TREND MICRO

http://www.trendmicro.co.jp/jp/security-intelligence/threat-solution/ransomware/index.html

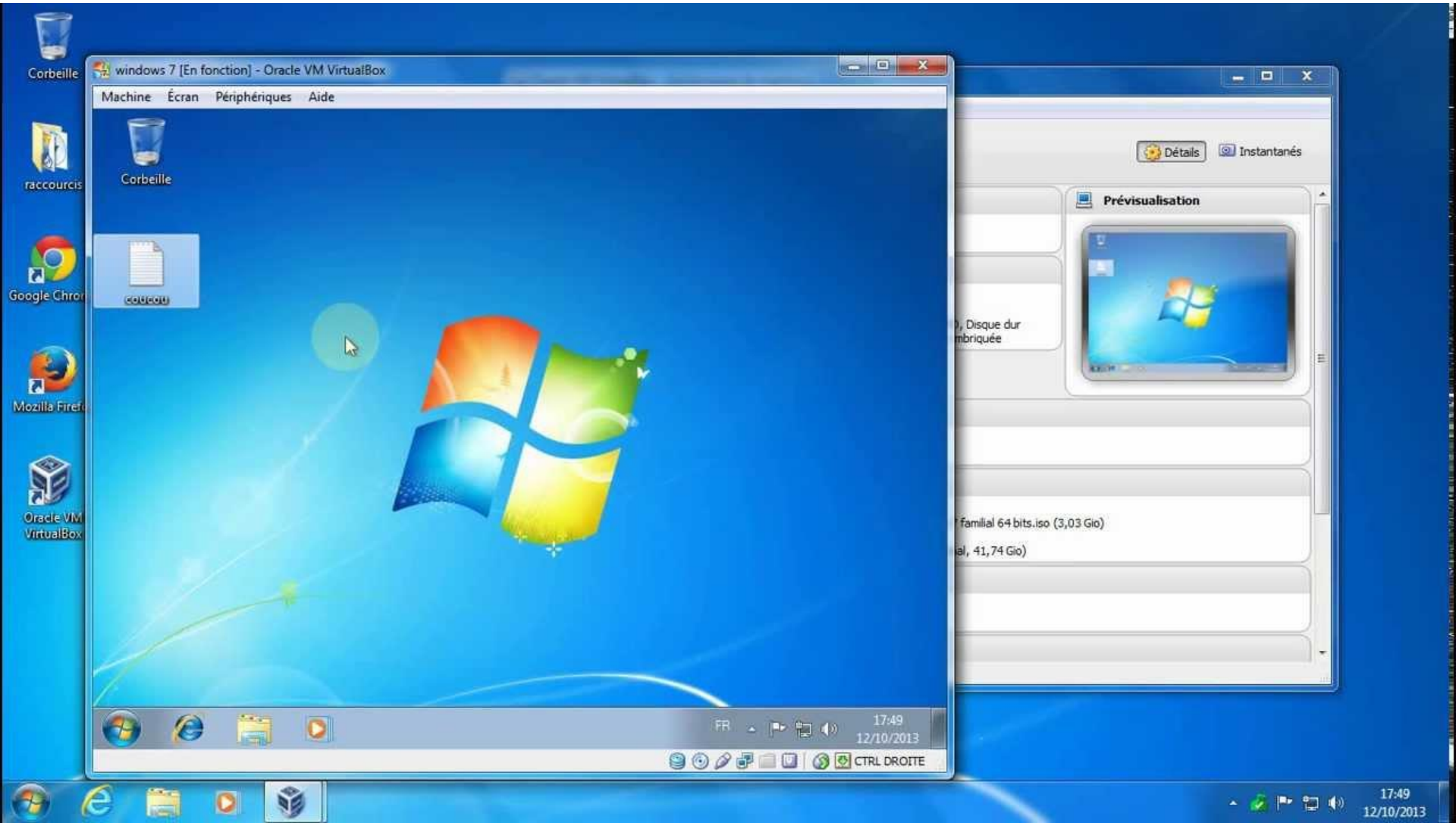
[4] Canon ITソリューションズ

https://eset-info.canon-its.jp/malware_info/term/detail/00107.html

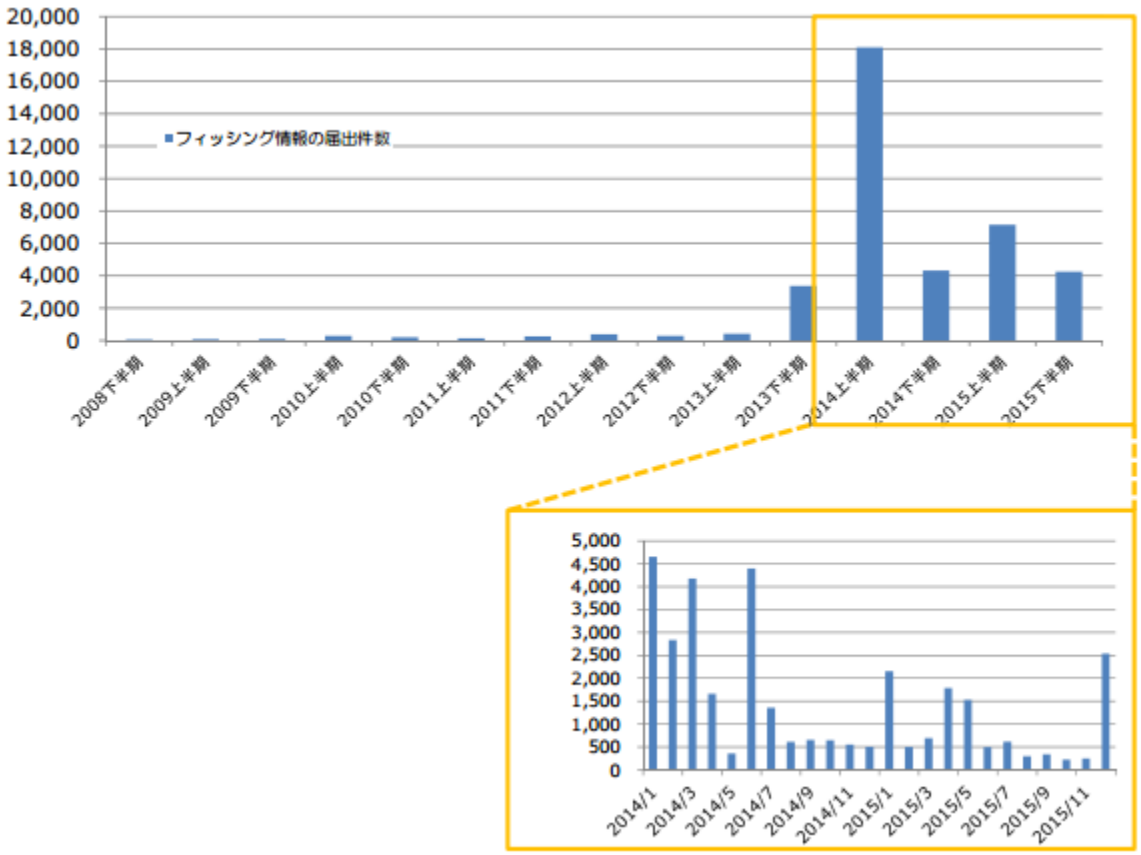
[5] 総務省

http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h26/html/nc143210.html

Virtual Boxについて



日本でのフィッシングメール被害



日本でのフィッシングメール届け出件数

日本のフィッシングメール被害

出典：フィッシング対策協議会
フィッシングレポート

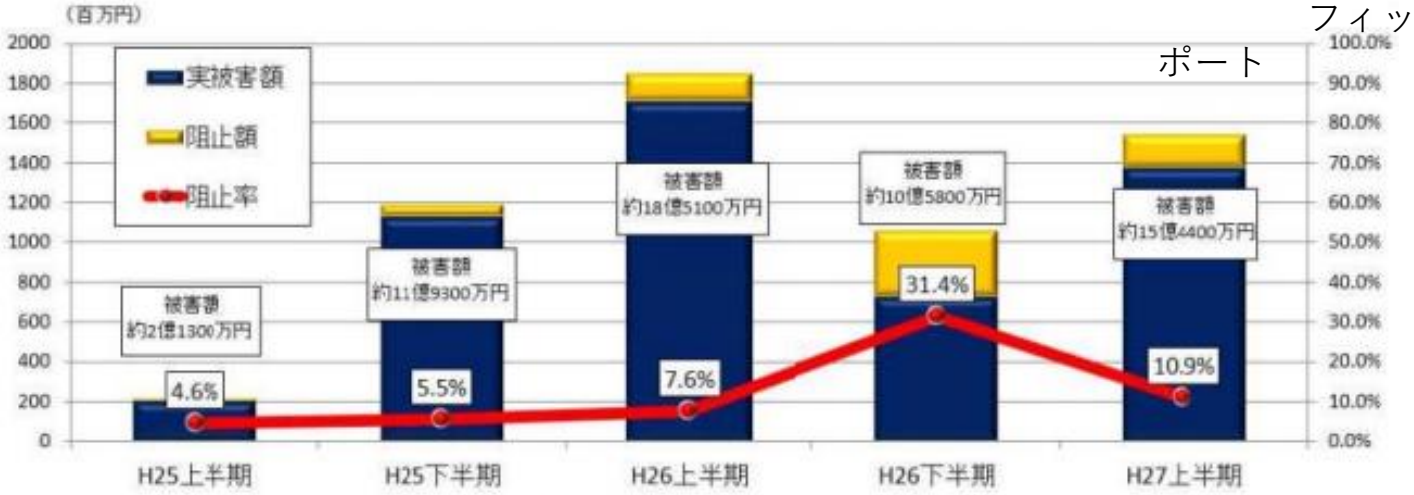
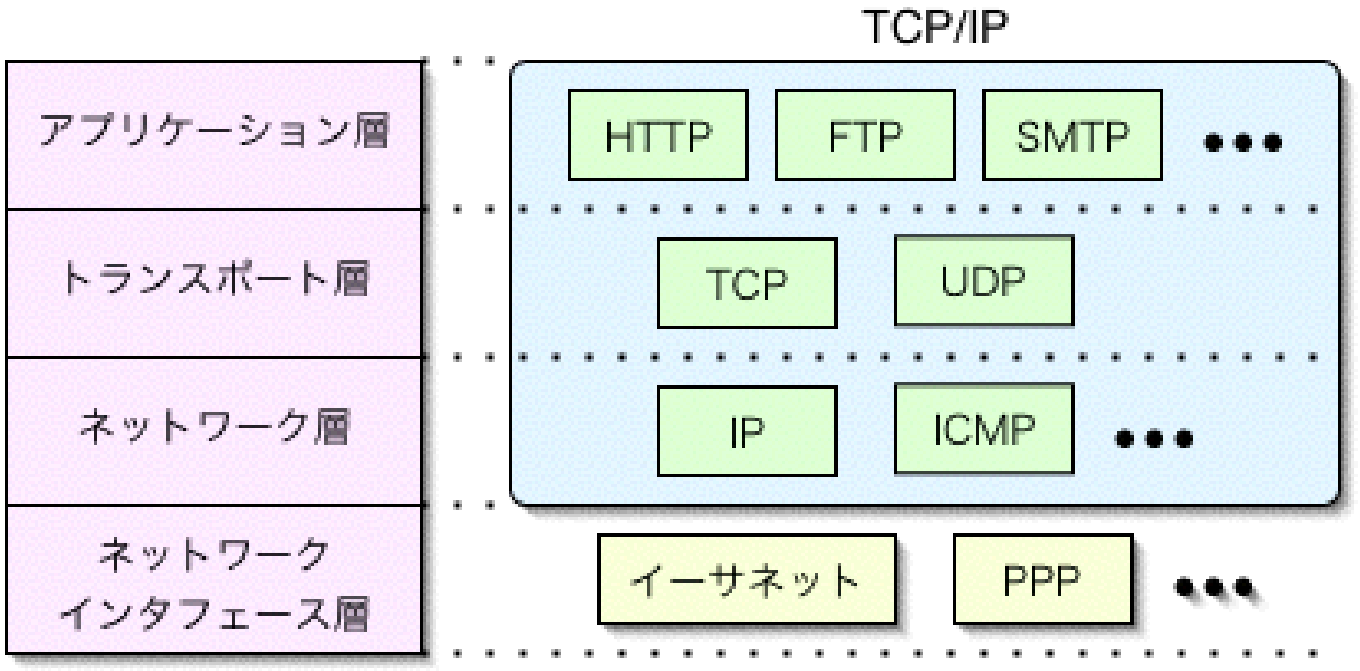


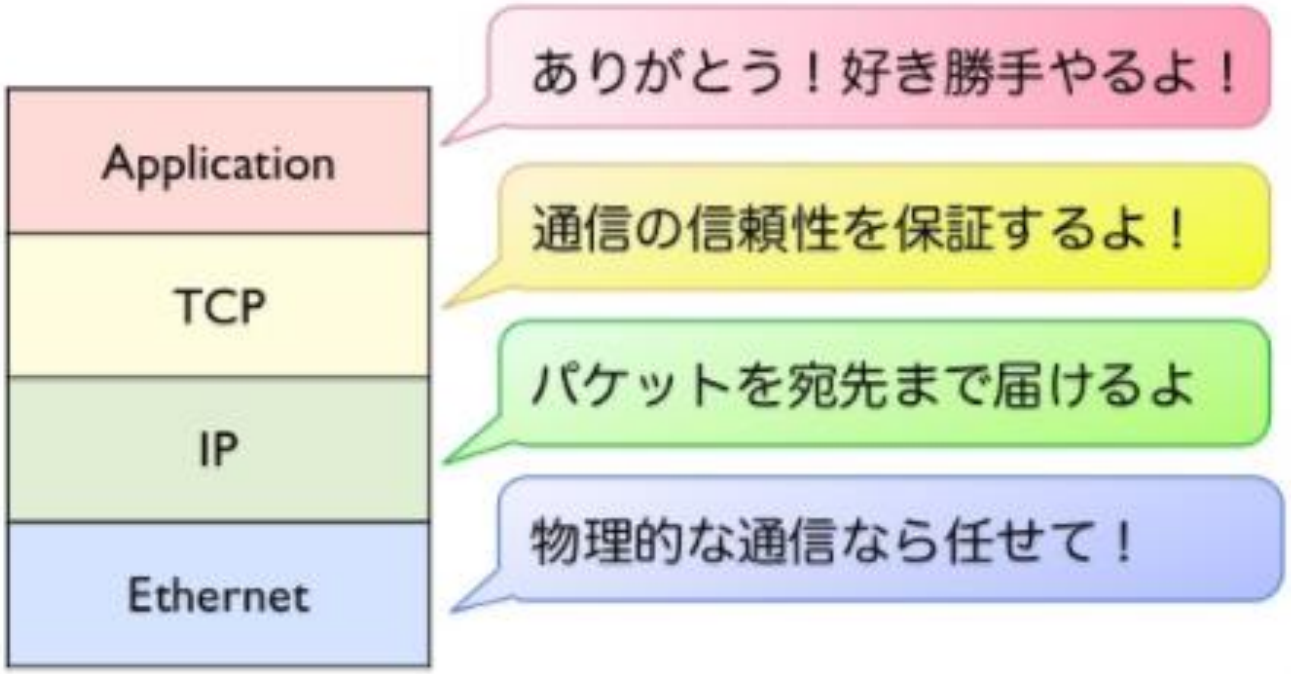
図 2.2-1 不正送金阻止状況[9]

通信について



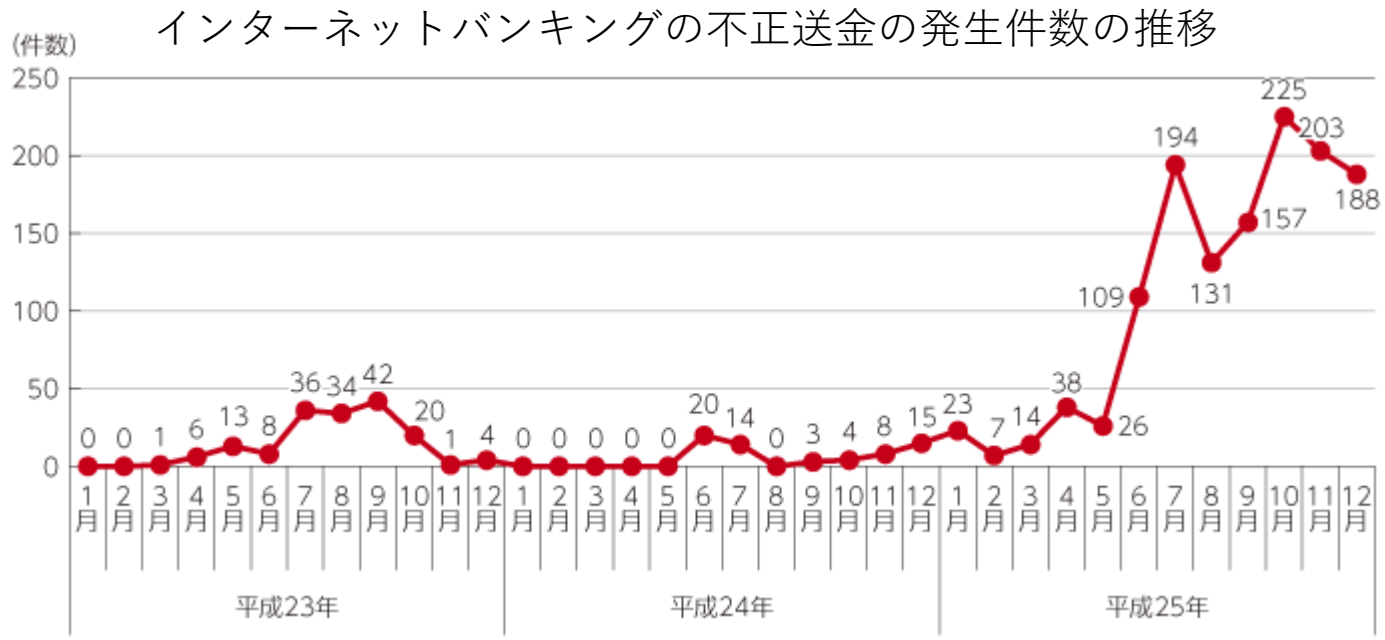
http://www.techscore.com/tech/Java/JavaSE/Network/1/

通信について



https://www.slideshare.net/yuyarin/ss-39737250

インターネットバンキング被害



総務省

コンピュータウイルスによる被害額

情報処理推進機構(IPA)の被害額算出モデルにおいて
ウイルス感染による1企業当たりの被害額

中小規模企業・・・430万円
大手・中堅企業・・・1億3000万円

グループ演習シラバス

- **授業概要**
- 3-4 名の学生グループ毎にリスク工学に関する特定の課題を選択し,アドヴァイザー教員のもとで,グループとして問題の把握,分析,考察を行い,結果をまとめる.