解説

狙われる個人情報
―巧妙化するネット詐欺と新たな脅威―

多摩大学教授　齋藤　裕美

1．シフトする攻撃方法

これまでのサイバー犯罪では，コンピュータやWebサイトの脆弱性を利用した攻撃が多かった。これまでは利用者の約9割がオペレーティングシステム（OS）としてMicrosoft Windowsを利用していたが，現在ではネットワークに接続されるデバイスの種類は多様化し，様々なソフトウェアやOSのバージョンが登場していることから，半数以上の利用者が単一のプラットフォームを利用しているといった状況ではなくなった。2019年5月のOSのシェアを見てみると，現在でも88.9%がMicrosoft Windowsではあるが，バージョン別のシェアでは，Windows 10とWindows 7がシェアを二分し，さらにWindows 8.1やWindows XPの利用者もいる（図1）[1]。Apple社のMacOSも10.14と10.13がそれぞれ混在しており，すなわち，従来の脆弱性攻撃ツールを利用した攻撃手法が効率的ではなくなったということを意味している。

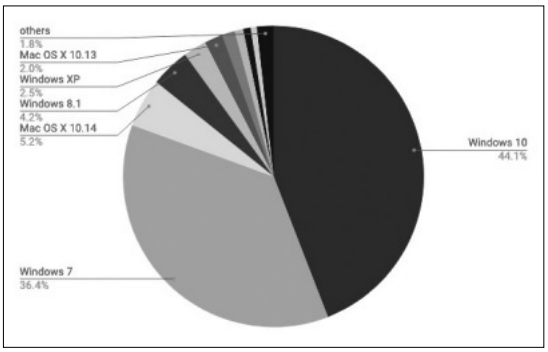

図1　2019年4月デスクトップOSバージョン別シェア
（出典：マイナビニュース）

そのため，サイバー犯罪者は，コンピュータやWebサイトの脆弱性ではなく「人の脆弱性」を狙うソーシャルエンジニアリングの手法を用いた攻撃に切り替えてきている。

2018年には，フィッシングサイトに誘導された利用者数が前年の約2.45倍増加しており（図2）[2]，また国内でのフィッシング詐欺の届け出件数も2018年は前年よりも約2倍増加している[3]。

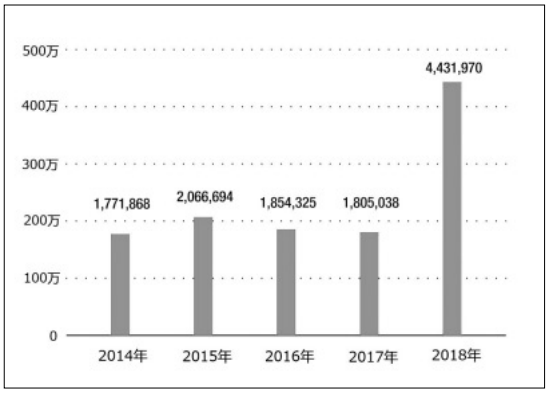

図2　フィッシングサイトに誘導された国内利用者数の推移
（出典：トレンドマイクロ株式会社）

2．フィッシング詐欺の多様な手口

(1) フィッシングメール

通常，フィッシング詐欺は電子メールを介して行われるが，近年では電子メール以外にもSMS（Short Message Service。携帯電話同士で電話番号を宛先にしてメッセージをやり取りするサービス）やIM（Instant Message。インスタントメッセンジャーに接続している利用者同士でリアルタイムに短いメッセージをやり取りするサービス），音声通話など様々な通信形態に拡大している。

フィッシングメールで偽装される送信元には大手IT企業や金融機関，携帯電話会社などがあり（図3）[2]，そのブランド名を悪用された企業の数

は増加傾向にある（図４）[3]。

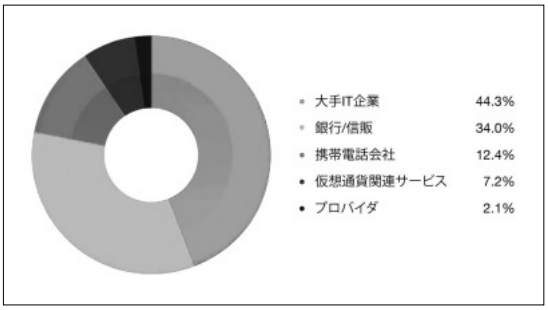

図３　偽装された送信元別割合（n＝97）
（出典：トレンドマイクロ株式会社）

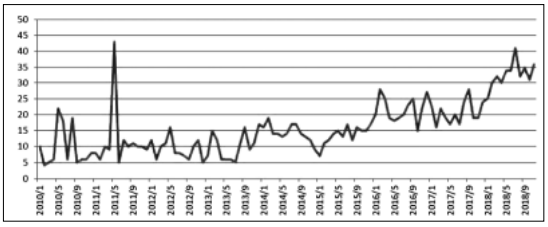

図４　ブランド名を悪用された企業数
（出典：フィッシング対策協議会）

フィッシングメールの特徴は，件名に「重要」や「緊急」など受信者に対応を迫る文言を入れていたり，本文が「アカウントの閉鎖」や「パスワードの初期化」，「不正ログイン」，「クレジットカードの使用不可」など受信者の不安を煽る内容になっていたりなど，受信者の冷静さを奪い，焦燥感によって咄嗟の行動を引き出そうとしている点である（図５）。

図５　筆者が受信したフィッシングメールの例

フィッシングメールから誘導されるフィッシングサイトではWebの認証情報やクレジットカード情報などが狙われており，とりわけWebの認証情報はクレジットカード情報を含む様々な個人情報に紐付いていることから，金銭に直結するクレジットカード情報と同様に狙われている。

(2) 偽装SMS

2018年は宅配の荷物の不在通知を偽装したSMSも急激に拡散している（図６）。

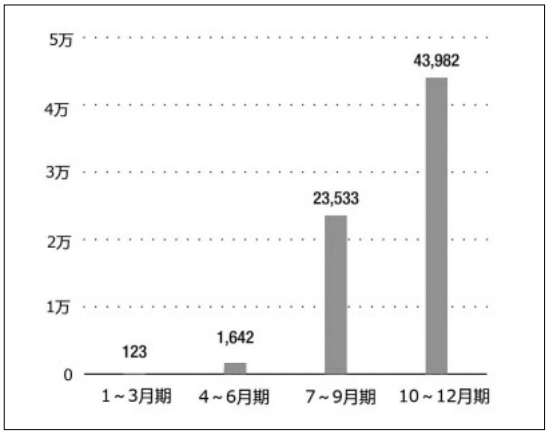

図６　偽装SMSから不正サイトへアクセスした利用者数
（出典：トレンドマイクロ株式会社）

大手宅配便事業者もそのサイトで注意を呼びかけているが[4]，偽装される宅配便事業者が複数になるなど，いまだに増え続けている状況である。

偽装SMSから不正アプリをインストールさせるサイトに誘導していることから，不正アプリの拡散も増えており，2018年の不正アプリ検出台数

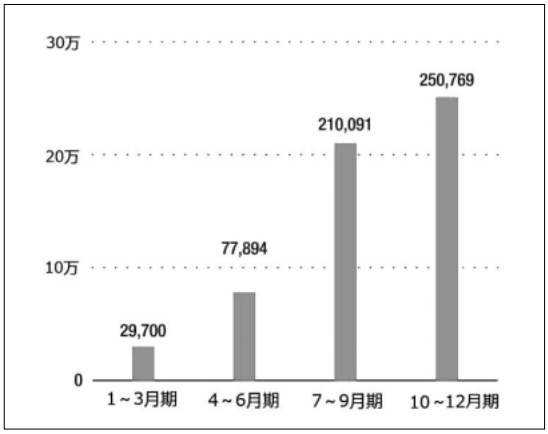

図７　不正アプリの検出台数
（出典：トレンドマイクロ株式会社）

は25万件を超えている（図７）。

IPAによれば，不正アプリの権限として，端末のステータスとIDの読取り，電話番号発信や発信先の変更，SMSの送受信，録音，連絡先（アドレス帳）の読取り，SDカードのコンテンツの読取りや変更・削除，画面ロックの無効化，実行中のアプリの取得，他のアプリの終了や他のアプリの上に重ねての表示，端末のスリープの無効化など多岐にわたっていることが報告[5]されており，こうした権限によってスマートフォンを不正に操作されたり，スマートフォン内の情報を外部に送信されたりする可能性がある。

さらに，トレンドマイクロ株式会社によれば，端末内にインストールされている正規の銀行アプリを偽物とすり替え，ネットバンキングの認証情報を詐取したり，携帯電話会社のキャリア決済を不正利用したりなどの活動が報告されている[6]。

不正アプリのインストールを防ぐためには，スマートフォンのセキュリティ設定等で，あらかじめ提供元の不明なアプリのインストールをさせない設定にしておくことが効果的である。提供先不明のアプリのインストールを不許可に設定しておくと，万が一不正アプリをインストールしようとしても，いったん警告が表示される。その時点でインストールをキャンセルすればよい。また，不正アプリは公式のアプリマーケットからは配信されていないため，公式マーケット以外からアプリをインストールしないように注意する。

(3) 偽装警告

特定の個人宛に送信されるフィッシングメールや偽装SMSだけでなく，Webサイトを閲覧している際に表示される警告メッセージを経由してフィッシングサイトに誘導したり，偽のセキュリティソフトウェアを購入させたりする手口も増加している（図８）。

また，画面に表示された連絡先へ電話をかけさせ，オペレーターの遠隔操作による有償サポート契約へ誘導する手口も報告されている[7]。

偽装警告は，Webサイトの閲覧中に突然，「ウイルス感染」や「システム破損」など閲覧者の不安を煽る警告画面やポップアップが表示され，さらに「〇秒以内に対応しないとデータが全て削除される」などすぐの対応を迫る内容になっており，さらに，閲覧者を信用させるために，それらの画面に実在の企業のロゴマークが使われているケースもある（図９）[7]。

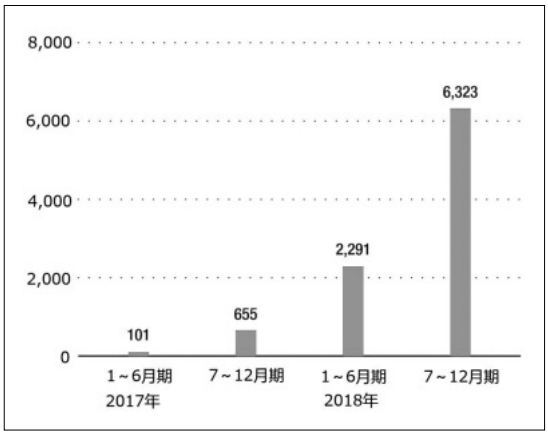

図８　偽装警告の問合せ件数
（出典：トレンドマイクロ株式会社）

図９　偽装警告の例
（出典：IPAセキュリティセンター）

自らが購入してインストールしたセキュリティソフトウェアによる警告ではない場合には偽装警告である可能性が高いため，警告画面の表示に安易に従わず，画面を閉じてから，既に導入しているセキュリティソフトウェアでスキャンするなど落ち着いて対応することが必要である。

(4) セクストーションスパム

セクストーションスパムとは，アダルトサイトへのアクセスログや閲覧時の状況を録画した動画を周囲に流布しないことを条件に仮想通貨の支払

いを求めるメールで，性的脅迫と言われる手口の一種である。

これまでは，SNSや出会い系サイト等で知り合った特定の標的に対して行うものであったが，2018年頃から不特定多数の利用者に対してメールを送信するスパムと化している。

アダルトコンテンツの閲覧など誰もが秘匿しておきたいプライバシーを周囲にばらまくという脅迫で不安に陥れ，また周囲に相談しにくい内容であることや支払い可能な金額であることなどから，脅迫者の要求を受け入れてしまうケースも多い。

3．狙われる個人情報と対策

フィッシングサイトが狙う個人情報は主としてWebの認証情報である。一般にアカウントとパスワードの組合せで認証するが，利用者の多くは，各自が利用している複数のWebサイトで同じアカウントとパスワードを使い回しているケースが多く，また昨今ではアカウントをメールアドレスとしているWebサイトも多いことから，パスワードひとつを入手すれば，そこから複数のWebサイトにアクセスすることもでき，またメールアカウントを乗っ取ることもできる。

これまではこうした不正ログインや乗っ取りなどを防ぐためにパスワードの定期的な変更が推奨されてきたが，2017年に米国国立標準技術研究所（NIST）からWebサービス提供者はパスワードの定期的変更を要求するべきではないとのガイドラインが示された[8]。内閣サイバーセキュリティセンター（NISC）でも，利用者に対してパスワードの定期的変更よりも，流出時に速やかに変更する旨が示されている[9]。

パスワードの使い回しは，パスワードを忘れてログインできなくなることを防ぐための方策であろうが，近年はセキュリティ強度の高いパスワードを自動生成し，かつそのパスワードを管理するアプリケーションなども登場しているので，そのようなアプリケーションを利用するとよい。

4．学校組織が持つ個人情報

教育機関が保有する個人情報には様々なものがあるが，中でも児童・生徒・学生のテスト結果など学業成績に関する情報や健康診断結果など保健医療に関する情報は価値の高いセンシティブ情報であり，今後，そうした生徒の個人情報が狙われることも予測されている[10]。そのようなセンシティブ情報も含めて教育機関のオープンネットワーク環境上で管理されているケースもあり，教育機関で個人情報を管理する担当者は，データベースセキュリティを強化する必要がある。

既に大学では，この数年サイバー攻撃を受けており，2017年には島根大学や大阪大学が，2018年には新潟大学が被害を受けている。島根大学の場合には学生の個人情報が外部から閲覧可能な状態になり，大阪大学の場合は学生や教職員など最大７万件ほどの個人情報が流出，新潟大学の場合はランサムウェアに感染したことで業務ファイルが使用できない状態になったと報道されている。

また，ビジネスメール詐欺やCEO詐欺と呼ばれる標的型攻撃メールの一種として，大学教職員をターゲットとしていると推測される文面による高度な標的型攻撃メールが確認されており，2016年に富山大学が受けたサイバー攻撃では，教員や非常勤職員宛に届いた標的型攻撃メールに添付されたファイルを非常勤職員が開封したため，PCがマルウエアに感染し，その結果，外部サーバとの不審な通信や不審なファイルの作成が確認されている[11]。

サイバー攻撃だけでなく，教育機関からの個人情報流出は毎年200件弱発生しており，2017年度には公立学校だけで12万６千人分の個人情報が流出している[12]。その原因の70%は「紛失・置き忘れ」と「誤配付」であり，教職員一人ひとりが生徒や保護者の個人情報の取扱いに十分注意する必要がある。

また，学校の公式サイト等で生徒の活動の様子などを伝える際，生徒の容貌等が識別できる写真を使用することにも注意が必要である。性犯罪等

に巻き込まれるケース以外にも，ドメスティックバイオレンス等で別居や離婚などした家庭の生徒の写真から転居先を特定されるなどのケースも考えられる。容貌等が識別できない程度にぼかす，画素数を落とすなどの工夫が考えられる。

5．おわりに

人間の心理を突いたソーシャルエンジニアリングの手法を用いた攻撃は巧妙化してきており，次々に新しい手口が出てきている。また人間の「うっかり」を原因とする個人情報流出も変わらず発生している。

日常の業務に追われるなかで不断の注意をすることは難しい面もあるが，預かっている生徒と同様に大切な生徒の個人情報を守るためにできることを学校全体で考えていく必要があろう。

［1］後藤大地．“Windows10シェア増加”．マイナビニュース．2019-05-05．https://news.mynavi.jp/article/20190505-817788/,(参照2019-07-20)．

［2］2018年年間ラウンドアップ 騙しの手口の多様化と急増するメールの脅威．トレンドマイクロ株式会社，2019，p.5.

［3］フィッシング対策協議会ガイドライン策定ワーキンググループ．フィッシングレポート2019．フィッシング対策協議会．2019．p.1.

［4］“ヤマト運輸の名前を装った迷惑メールにご注意ください”．ヤマト運輸．2018-12-12．http://www.kuronekoyamato.co.jp/ytc/info/info_181212.html,(参照2019-07-20)．

［5］IPA（独立行政法人情報処理推進機構）セキュリティセンター．“宅配便業者をかたる偽ショートメッセージに関する相談が急増中 誘導されるままAndroid端末にアプリをインストールしないように！”．IPA．2018-08-08．https://www.ipa.go.jp/security/anshin/mgdayori20180808.html,(参照2019-07-20)．

［6］前掲書2，p.17.

［7］IPAセキュリティセンター．“偽のセキュリティ警告によって有償の「ソフトウエア購入」や「サポート契約」をしてしまう相談が増加中 インターネット利用中に表示される偽の警告画面にだまされないで！”．IPA．2018-07-18．https://www.ipa.go.jp/security/anshin/mgdayori20180718.html,(参照2019-07-20)．

［8］NIST SP800-63B（電子的認証に関するガイドライン）．2017-06.

［9］“インターネットの安全・安心ハンドブック Ver.4.03”．NISC．2019-06-18．https://www.nisc.go.jp/security-site/handbook/index.html,(参照2019-07-20)．

［10］2016年情報セキュリティ予測．ウォッチガード・テクノロジー・ジャパン株式会社．2015-12-22．https://www.watchguard.co.jp/contents/docs/resource/2016_Predictions_jp.pdf,(参照2019-07-20)．

［11］富山大学水素同位体科学研究センターに対する標的型サイバー攻撃について（概要）．富山大学．2016-10-11．https://www.u-toyama.ac.jp/news/2016/doc/1011.pdf,(参照2019-07-20)．

［12］平成29年度学校・教育機関における個人情報漏えい事故の発生状況．教育ネットワーク情報セキュリティ推進委員会．2018-11-30．https://school-security.jp/pdf/2017.pdf,(参照2019-07-20)．