フィッシング対策協議会
Council of Anti-Phishing Japan

フィッシングレポート 2014

－　急増する不正送金とフィッシング　－

平成 26 年 7 月

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

目次

1. フィッシングの動向

1.1. 国内の状況

2012 年に大きく増加したフィッシング被害は、2013 年に入ってさらに急増しており、深刻化している。特に問題になっているのは、昨年のフィッシングレポート 2013 で指摘したマルウェアを用いた手法による被害である。

警察庁の発表[1]によれば、インターネットバンキング利用者の口座情報を様々なウイルスやマルウェアを用いて盗み取り、利用者の口座から不正送金する事件が急増した。2012 年には 64 件、約 4,800 万円だった被害額が、2013 年には 1,315 件、約 14 億 600 万円に増加し、前年比 29 倍に達した。

フィッシング対策協議会の統計でも、2013 年のフィッシング届出件数は年初から前年度を上回る水準で推移し、7 月以降届出件数が急増した。これは、オンラインゲームを対象としたフィッシングの届出が急増したためである。さらに 11 月以降はさらに増加しているが、これはオンラインゲームに加え金融機関を対象としたフィッシングの届出が増加したためである。（図 1-1）。

フィッシングサイトの件数も増加しているものの、届出の増加割合に比べると増加率は低い。これはフィッシング手法の多様化を反映しているものと考えられる。

フィッシング対策協議会に対するフィッシング情報の届出件数は対前年度で約 17 倍以上（2012 年度 828 件、2013 年度 15,171 件）と急増した。一方でフィッシングサイトの件数(2012 年度 2,286 件、2013 年度 2,522 件)、ブランド名を悪用された企業数(2012 年度 117 件、2013 年度 136 件)は、前年に比べそれほど大きな変化はなかった。フィッシングの対象となるブランド数は頭打ちの傾向にあること、つまり犯罪者がターゲットとするブランドが固定化しつつあることを示している。

[1] 警察庁，平成 25 年中のインターネットバンキングに係る不正送金事犯の発生状況等について，
https://www.npa.go.jp/cyber/pdf/H260131_banking.pdf

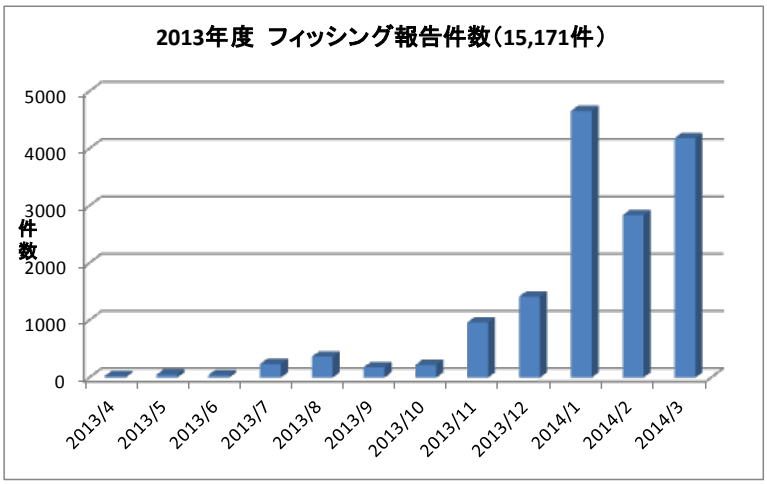


図 1-1　フィッシング報告件数

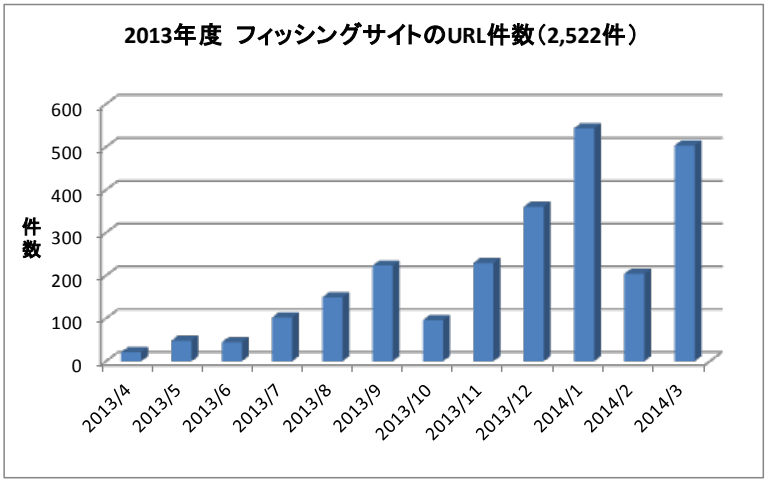


図 1-2　フィッシングサイトの URL 件数

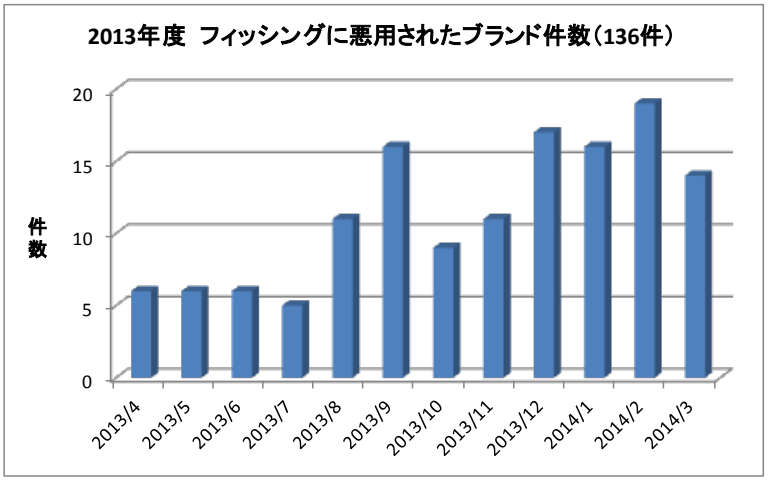


図 1-3　フィッシングに悪用されたブランド件数

また、国家公安委員会・総務省・経済産業省の発表によれば、警察庁に報告のあった不正アクセス行為として、識別符号窃用型不正アクセス行為（ID 窃盗による不正アクセス行為）は昨年度に比べて増加した（図 1-4）。また、その手口を見ると、2013 年（平成 25 年）のフィッシングは 9 件であり、比率は約 1%となっている（図 1-5）。

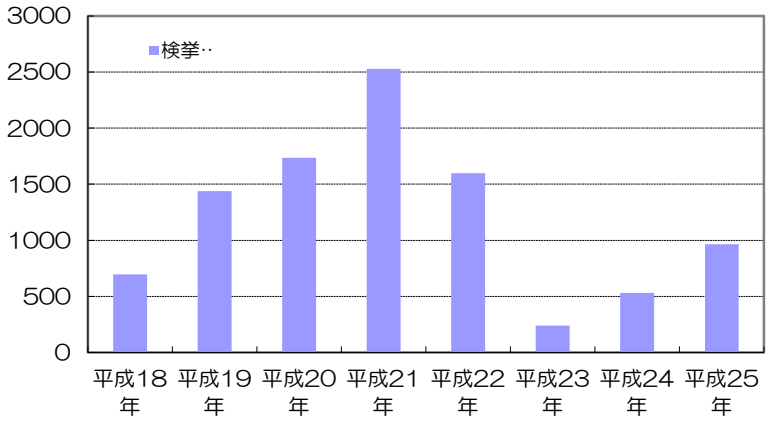


図 1-4　識別符号窃用（ID窃盗）型不正アクセス行為の検挙件数 [2]

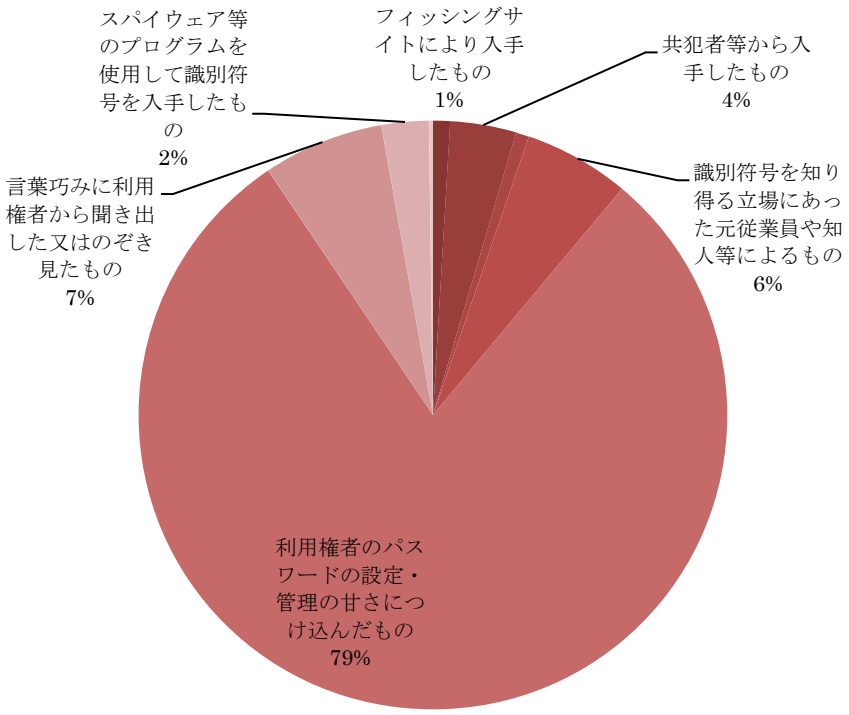


図 1-5　平成 25 年 不正アクセス行為に係る犯行の手口の内訳 [3]

[2] 国家公安委員会・総務省・経済産業省,「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」,等、http://www.npa.go.jp/cyber/statics/h25/pdf041.pdf よりフィッシング対策協議会が作成
[3] 同上

冒頭でも述べたように、我が国におけるフィッシング被害は深刻な状況にある。被害金額という観点から特に問題となっているのは、マルウェアを利用した手法による不正送金被害である。この手法は従来の狭義のフィッシング対策だけでは対処することが出来ないため、事業者はもちろん利用者の総合的なセキュリティ意識の向上がこれまで以上に求められている。

1.2. 海外の状況

米国で設立されたフィッシング問題に関する国際組織 APWG（Anti-Phishing Working Group）の調査によれば、2013 年のフィッシング届出件数は、年初減少傾向にあったものの 4 月以降急増し過去最高に達した。またフィッシングサイトの件数についても年初来現象傾向にあったものが 7 月から急増し過去最高に近い水準に達した。（図 1-6、1-7、1-8）。引き続き注意が必要である。

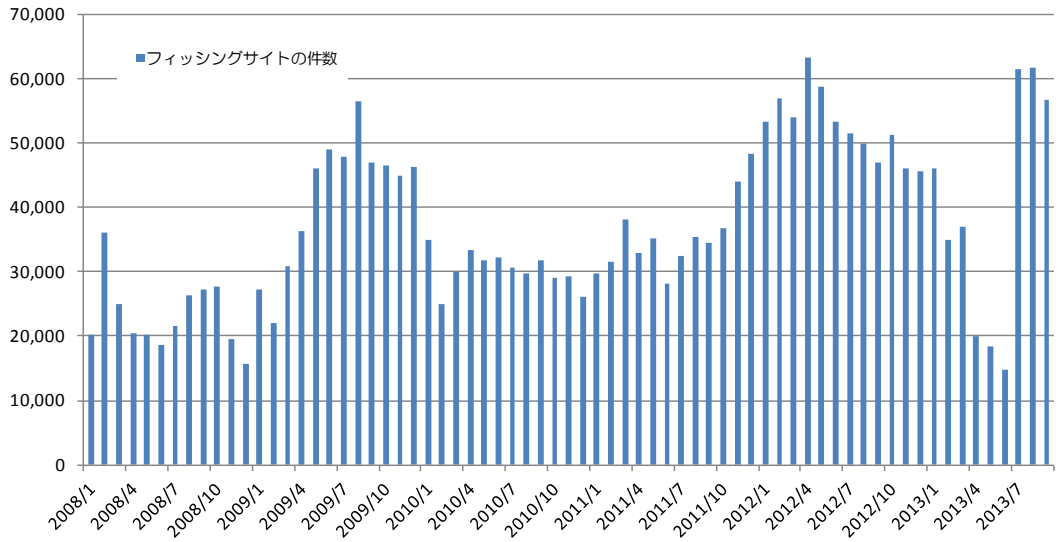


図 1-6　フィッシングサイトの届出件数 [4]

[4] APWG (Anti-Phishing Working Group), "Phishing Activity Trends Report"、http://www.antiphishing.org/index.html、よりフィッシング対策協議会にて作成

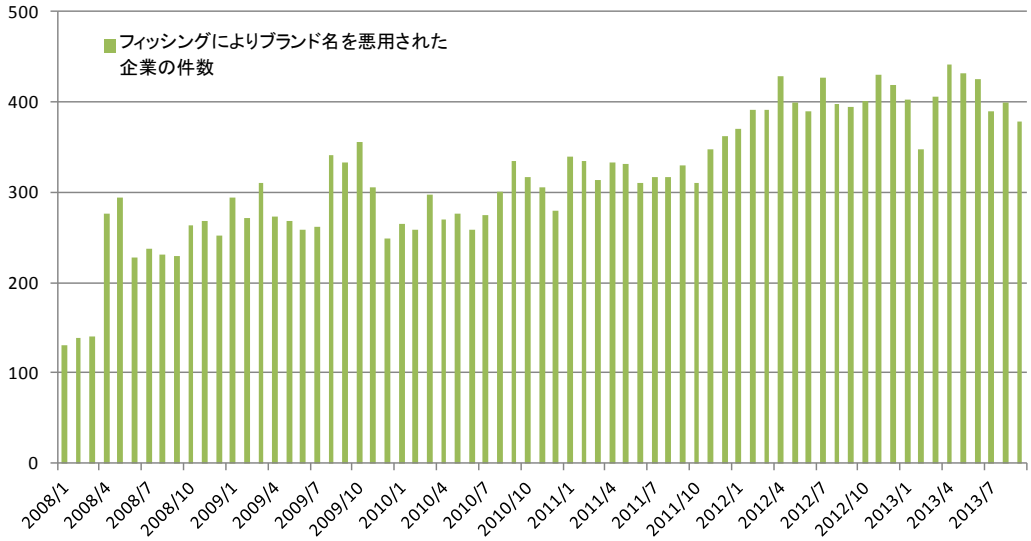


図 1-7　フィッシングによりブランド名を悪用された企業の件数 [5]

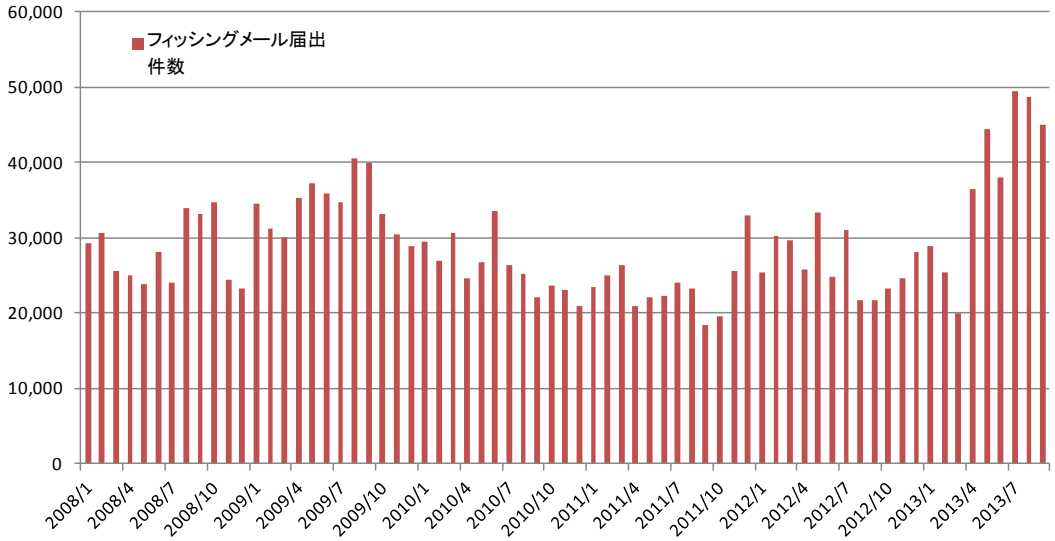


図 1-8　フィッシングメール届出件数 [6]

[5] APWG (Anti-Phishing Working Group), "Phishing Activity Trends Report"、http://www.antiphishing.org/index.html、よりフィッシング対策協議会にて作成
[6] APWG (Anti-Phishing Working Group), "Phishing Activity Trends Report"、http://www.antiphishing.org/index.html、よりフィッシング対策協議会にて作成

2. 手口の変化・影響の拡大

2.1. 不正送金被害の拡大

2012 年に大きく増加したフィッシング被害は、2013 年に入ってさらに急増しており、深刻化している。特に問題になっているのは、昨年のフィッシングレポート 2013 で指摘したマルウェアを用いた手法による被害である。

インターネットバンキングに係る不正送金事件は、平成 24 年には 64 件、約 4,800 万円だった被害額が、平成 25 年には 1,315 件、約 14 億 600 万円の被害が発生しており、前年比 29 倍に達した。（図 2-1）

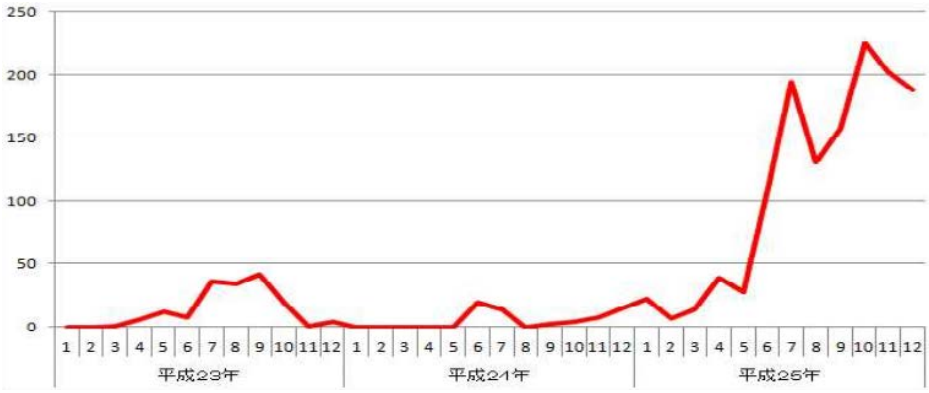


図 2-1　インターネットバンキングに係る不正送金事犯の月別発生件数 [7]

同様に、金融庁 [8]によれば、平成 25 年度（4～9 月）において発生したインターネットバンキングに関する被害件数は 640 件、被害金額は約 5 億 8 千万円に達している。顕著なのは、偽造・盗難キャッシュカード、盗難通帳等による預金等の不正払戻し等の被害に占める、インターネットバンキングの占める割合である。平成 24 年度は 3%に満たなかったものが（5,009 件中 145 件）、平成 25 年は 26%以上（2,390 件中 640 件）に達している。

被害急増を受けて、金融庁や金融機関、警察が中心となり注意喚起を行っているが、手法も巧妙化しており、依然として被害はおさまっていない状況にある。また、専用のウイルス対策ソフトやフィッシング対策ソフトを無償配布する金融機関も出てきている。また、認証の強化としてワンタイムパスワードの利用も進んできている。

---

[7] 出典：警察庁，平成 25 年中のインターネットバンキングに係る不正送金事犯の発生状況等について，
https://www.npa.go.jp/cyber/pdf/H260131_banking.pdf
[8] 金融庁，偽造キャッシュカード等による被害発生等の状況について，
http://www.fsa.go.jp/news/25/ginkou/20140219-1.html

■コラム：金融端末への攻撃

「あれっ　なんかカード入りにくいな。　あっ入った。飲み会に遅れちゃう。急いで行かないと。暗証番号は〇〇〇〇、金額は 3 万円と。」

鈴木さんはコンビニエンスストアの ATM から引き出した現金を持って夜の街に消えてゆきました。

数日後、鈴木さんの携帯電話が鳴りました。

「鈴木様の携帯電話ですか？こちらはニッポンクレジットカードです。先ほど△△（外国国名）でキャッシングサービスを受けられましたでしょうか？」

「えー何言ってるんですか？　ずっと東京ですよ。カードもここにあるしキャッシングなど受けていません！」　「いったいどうゆうこと？？？？」

昨年、金融機関が発行したキャッシュカード・クレジットカードが偽造され不正にキャッシングサービスを受けられる被害が多発しました。

捜査当局の調べで、鈴木さんが利用した ATM のカード挿入口にペンギンのクチバシの様なパーツが取り付けられ、磁気データを読み取られて偽造カードが作成されていました。さらに、引き出した現金を入れるための封筒がまとめてある ATM 横のボックスの底には暗証番号を入力するパネル盗撮用のカメラが！

なんと ATM にスキミング装置が取り付けられていたのです。

鈴木さんがカードを使ったとき「カード入りにくいな」と感じたのは、通常利用時と違う装置に挿入していたからなのです。

カードをとりまく犯罪は、盗難・紛失、偽造、あるいはカード番号の盗用と様々なケースがありますが、思いもよらない新しい手法を用いられ被害が発生してしまうのです。

このコラムをご覧のあなた　昨日感じた違和感、何かに巻き込まれていませんか？

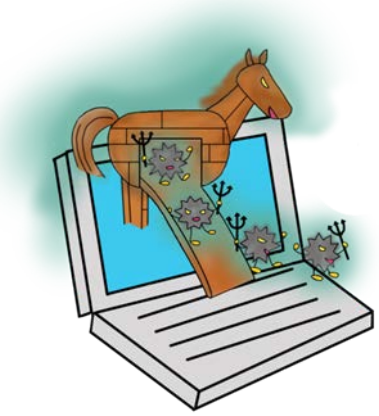
[鈴木 哲治 株式会社ジャックス]

2.2. マルウェアを用いたフィッシング被害の拡大

2013 年は、オンライン犯罪 (特にインターネットバンキングを狙う犯罪) から守る側にとって大変厳しい年になった。その内容については前述(不正送金被害の拡大)の通りであるが、その手法は 2012 年に既にその活動が明らかになっていた Citadel を始めとするトロイの木馬によるものである。Citadel は 2012 年末に地下市場から姿を消したと言われているが、往年の有名なツールである Zeus をもとにしたトロイの木馬だけあって、2013 年も引き続き犯罪者に利用されていたようだ。

Banking Trojan (主に銀行を狙うトロイの木馬) は、Zeus から SpyEye、Citadel など新たな種類が発見されてきており、Citadel の次のトロイの木馬が一体何になるのかセキュリティベンダも目をこらしている。2013 年は大きくその活動が認められていないが、いくつかのトロイの木馬の名前があげられる。

ひとつは、KINS という名のトロイの木馬の存在が明らかになったことである。KINS は 2013 年の初頭から地下市場に出始めたと言われる、Zeus や SpyEye の機能を持ち合わせて進化したトロイの木馬とされている (当の KINS 開発者のコメントではスクラッチから開発した新作と強調されているようである)。KINS は Citadel やそれ以前の犯罪者に必要とされていた機能を包含しており、主に下記のような特徴がある。その他にも、Windows 8 への対応や bootkit*1 機能への対応を試みているようで今後も進化を続けそうなトロイの木馬である。また発見時点ではサンプルの数が非常に少ないため、アンチウイルス・マルウェアの検知率が低く、ボット化の成功率が高いという犯罪者側の利点もある。



KINS が持つ主な機能

- メインファイルと DLL ベースのプラグインからなる Zeus や SpyEye 同様のプログラム構造
- Zeus や SpyEye と互換性のある HTML インジェクション機能
- SpyEye と同様の対アンチウイルス・マルウェア機能

- RDP (Remote Desktop Protocol) での動作
- Zeus, SpeEye 同様な、技術的に高度な知識が不要であるコントロールパネルなど

KINS は、FaaS (Fraud as a Service) としても市場へ浸透しようとしている。2013 年 3 月頃から犯罪者の攻撃用のパッケージとして販売が開始されているようで、洗練度合いが高い。例えば、犯罪者が使用中のトロイの木馬 (亜種) を、アンチウイルス・マルウェアが検知できるかを確認できたり、ドロップサイトや指令サイト等にトロイの木馬を配置する際に、ドメインが取り締まり側のブラックリストの対象になっていないかを確認することができる。

もう一つは、スマートフォンをターゲットとしたトロイの木馬であろう。スマートフォンを狙うトロイの木馬については 2011 年頃から頻繁にとりあげられるようになり、ユーザへのデバイスの浸透を背景にいくつかのトロイの木馬が話題となった。


Copyright right holders of the [Android robot] is Google

日本でもトロイの木馬の機能を含む偽スマートフォンのアプリケーションがいくつか見られるようになってきたが、特に狙われているのは Android を搭載したスマートフォンである。名称は様々であるが、2013 年に主に話題になったものとして、スマートフォンの管理者特権を奪うもの、SMS メッセージの送受信をコントロールするもの等があった。管理者特権を奪われると、デバイス上の情報の殆どが盗まれる危険性がある上、アプリケーション一覧に表示されないというステルス性の高さがあるため感染を発見するのが困難である。また、SMS が操作されると、ワンタイムパスワードの送受信を SMS で実施している場合にはトロイの木馬によって認証が横取りされる結果となる。これらはオンライン犯罪に使われるという意味では非常に危険である。

オンライン犯罪に利用されるトロイの木馬は、一般のユーザが知らないところで進化し続けている。対象のデバイスの広がりや感染させるための手口の巧妙化が進んでおり、意図しないトロイの木馬のインストールが日々行われている状況である。ユーザはアンチウイルス・マルウェアのソフトウェアをインストールしておくことはもちろん、タイムリーにアップデートしておくことが求められる。また、Android においては、アプリケーションに対するアクセス許

可を必ず確認して、アプリケーションの動作から考えて不要と思われるアクセス権限に注意する。そして、万が一に感染したことを考えて、オンラインバンキングの画面で要求される項目がいつもとおかしかったり、あるいは過剰な情報要求と感じた場合は、その時点でアクセスを中止して銀行のホームページを確認したり、相談窓口に連絡するなどの冷静な対処がその後の被害を未然に防ぐ策となる。

[水村 明博 EMC ジャパン株式会社]

■コラム：**Facebook** の危険性

Facebook は便利なツールです。自分の友達が 100 人、その先の友達も 100 人とすると、100 x 100 = 10,000 のネットワークになります。連絡が途絶えていた高校時代の友人を探したり、思いがけない出会いがあり使っていて楽しいツールです。しかし、この“便利さ”が使い方を誤ると意図していないことに巻き込まれる危険があるのです。

例えば、2013 年の年末に流行った Facebook の人気アプリで自分新聞というのがあります。これは 2013 年で最多の“いいね”を獲得した記事や月間で人気があった自分の記事をまとめた“自分新聞 ”をまとめるサービスです。サービス自体は良くできているのですが、サービスを使うために“ハーバード流宴会術”と“Omiai”Facebook ページに対して“いいね”を押す必要があります。Facebook の広告に自分の名前やプロフィール写真などがマッチングサイトの広告に利用される可能性があります。このサービスは“自分新聞”作成後当該サイトに対して“いいね”を取り消すことができるので違法性を問うことは難しいですがほとんどの人はそういったことに気づかず放置してしまうのではないでしょうか？

Facebook では、普段とは違う場所や端末からログインしたなどの理由でアカウントがロックされてしまうことがあります。救済措置として、「友達の助けを借りる」という機能があります。友達３人に向けて「セキュリティコード」が送信され、それらが入力されれば本人確認とみなし、再びアカウントにアクセスできるようになります。しかし、この一見便利な機能が、アカウント乗っ取りの手段として悪用される可能性があります。３つ以上の「なりすましアカウント」を友達として承認してしまい、さらに Facebook に登録しているメールアドレスを知られてしまうと、「セキュリティコード」を使って登録メールアドレスとパスワードが変更され、アカウントが乗っ取られてしまいます。アカウントが乗っ取られると、自分の友達に対して商用サイト（有料の出会い系サイトなど）への誘導・勧誘が行われるかもしれません。

Facebook へのアクセスに使う機器を限定し、公開範囲を特定の人に限定するなど使い方には十分注意しましょう。

[花村 実 EMC ジャパン株式会社]

3. 新しい対策の動向

3.1. サービス提供側の対策

近年、セキュリティ対策として、多層防御の重要性が言われているように、オンライン口座乗っ取りに対する対策としても、一つの対策で保護することは難しい。

米国のGartnerは金融機関における、不正ソフトウェアによるオンライン口座乗っ取りの対策技術として、「The Five Layers of Fraud Prevention and Using Them to Beat Malware」という資料で、下記の 5 層の対策を紹介[9]している。

第 1 層：エンドポイントでの保護
第 2 層：オンライン上のやりとりに着目した保護
第 3 層：ユーザと口座取引に着目した保護
第 4 層：ユーザと口座取引の複数の取引チャネルでの動きに着目した保護
第 5 層：口座取引やお金の動きなど金融機関、小売店などでのすべての動きに着目した保護

下に行くほど、複数のデータの相互相関が必要となり、分析するデータ量も多くなり、実現の費用も多くなる。

FS-ISACが公開している「Account Take Over and Online Fraud Response White Paper」[10]においても、オンライン口座乗っ取り詐欺の検出方法として、第 1、第 2、第 3 層に相当する顧客エンドポイントによる方法とサーバ側による方法が紹介しています。以下に、各層での対策の概要を紹介しますが、技術のみでの保護は難しく、監視チームの編成など、運用体制の方が重要で、FS-ISACのWhite Paperでもその多くを運用面にさいている。

<u>第 1 層：エンドポイントでの保護</u>

オンライン銀行利用者が使っているエンドポイントおよび利用者の状況に対応したウイルス対策以外のエンドポイントでの防御技術です。下記のような技術が含まれ、製品としての実装も存在する。

なお、単一の技術だけでなく、下記の複数の技術を組み合わせることによって、エンドポイントでの対策をよりセキュアにすることが可能です。

[9] https://www.gartner.com/doc/1646115
[10] http://www.fbiic.gov/public/2011/jun/RESPONSE_%2020110614.pdf

- ソフトウェアベースのセキュアブラウジング

サンドボックス技術やカーネルフックの保護技術などを使って、不正ソフトウェアによる利用者が利用しているブラウザソフトウェアのハイジャックを防ぐブラウザ

- USB で動作する安全なブラウザを提供

安全なブラウザを USB など別デバイスから起動し、安全なブラウザを提供する

- 帯域外認証とトランザクションの検証

利用者が使っている PC 以外の経路を使って、振り込み時の金額、振込先を確認する。あるいは、振り込み時の金額、振込先に電子署名など、メッセージ・ダイジェストをつけ、経路上での変更を検知できるようにする。

- エンドポイントデバイスの識別

いわゆるリスク認証と呼ばれるもので、利用者が普段利用しているデバイス以外からの利用があった場合を識別する。

第 2 層：オンライン上のやりとりに着目した保護

ユーザと IP アドレスの実際の通信と Web のトラフィックを分析することにより、不正を検知する技術です。多くの場合、不正プログラムが行うトランザクションの流れや実施のタイミングは、人が行うものと比較すると違う点があり、その点を利用して不正を検出する技術で、次の第 3 層による方法より、展開が早く、不正ソフトウェアによる詐欺の検知において、効果を上げることができる。

第 3 層：ユーザと口座に着目した保護

オンラインなど単一の取引におけるユーザの行動パターンの傾向などを含めて、下記のようなデータから通常ではない顧客行動を特定し、盗まれた認証情報による不正アクセスの検知において、効果を上げることができる。

- 顧客のアクセスパターン（日中にアクセスする時間帯、1 週間のうちでアクセスする日など）
- アプリケーション内での活動内容（明細を参照、取引の実行など）
- コンピュータの情報（IP アドレス、ブラウザータイプ）
- コンピュータの位置情報（IP アドレスから派生した GeoIP データ）
- 取引フロー

第 4 層：ユーザと口座の複数の取引チャネルでの動きに着目した保護

ユーザや口座の振る舞いを監視し、オンラインや実店舗での利用状況などの

相関を取ることによって、怪しい取引を検出する。

第 5 層：口座取引やお金の動きなど金融機関、小売店などでのすべての動きに着目した保護

金融機関内での振る舞いだけでなく、外部での組織の関係やそれらの属性なども分析し、共謀での犯罪活動を検出する。

不正プログラムによるオンライン口座乗っ取り対策の導入としては、まずは、第 1 層と第 2 層の対策が比較的容易に導入できて、効果的である。第 1 層の技術的対策の多くは、顧客クライアントへの適用が必要なため、顧客全体への浸透が難しいが、防御としての確実性は、高い。フィッシングに効果が高い帯域外認証はいくつかの金融機関では導入され、実際導入後のフィッシングが減るなど高い効果を上げている。一方、MITM にも効果があるトランザクションの検証については、金融機関から配布されているトークンにはすでにその機能を有しているものの、日本においては実際の使用例はまだ見ないようである。

第 2 層の対策技術は、サーバ側で行うため、顧客クライアントソフトへ依存しないため、顧客全体へすぐに適用可能で、顧客の PC のリスクの存在を検出するという点では効果的で、すでに導入している金融機関でも効果が出ているようである。しかし、リスクを取り除くという点では、顧客 PC への対策が必要で、防御の観点では難しい。

したがって、第 1 層と第 2 層の技術的対策を組み合わせて行うことが望ましい。

[野々下 幸治 トレンドマイクロ株式会社]

■コラム　個人情報を不用意に投稿する世代への対策

インターネット上に個人情報を公開し過ぎる傾向「over-sharing」は年々強まっています。

アリストテレスは著書『政治学』において「人間は自然にポリス（社会）的な動物である」と定義しています。この定義に言われるとおり、我々は本質的に良いニュースについて声を出して叫びたいと、認識して欲しいと共有することを願っています。

しかし、行動による影響を理解せずに、不用意に共有を行うことは自らを危険にさらすことになるだけです。

Twitter 上に投稿されているカード番号を含むクレジットカード画像

Twitter 上に iTunes Card のアクティベーション番号を公開した事例。投稿時には番号のモザイク処理なし。

「Facebook」や、「GREE」、「mixi」などのソーシャルネットワークサービスの登場は、共有欲求を加速させました。マイクロブログサイト「Twitter」や写真共有サイト「Instagram」上には、自ら自身の身分証明書やクレジットカードの写真を投稿している様子が多数確認出来ます。中には、用途について理解できず不注意でプリペイドカード「iTunes Card」のアクティベーション（機能の有効化）番号を投稿している事例も確認されています。

こうした状況を歓迎しているのはサイバー犯罪者のみです。不注意なユーザによるこうした個人情報の投稿は彼らにとって「宝の山」です。事実、「NeedADebitCard」と呼ばれる一覧表も作成されています。

これら新たなリスクについて利用者を保護していくには、技術による対策もさることながら、適切な教育機会の提供と継続した注意喚起が必要であるといえます。

これまでに発生したトラブルの例とそれが招いた結果について振り返る機会を提供することも対策の一つになり得ると言えそうです。

ファミマTカード番号の取扱いとSNS上などでのファミマTカード券面画像公開に関するお願い

いつもファミリーマートならびにファミマTカードをご利用いただきありがとうございます。

ファミマTカードの券面に記載されているクレジットカード番号、T会員番号、及びご氏名は会員様にとって大切な情報です。

特に、TwitterやFacebook、ブログなどでファミマTカード券面の画像を掲載される場合、クレジットカード番号、T会員番号、及びご氏名が判明する形での掲載は、大事な情報が不特定多数の方に見られてしまうことになります。
つきましては、もし掲載される場合は、クレジットカード番号、T会員番号、及びご氏名（下の赤枠部分）が判明しないように隠してから掲載くださいますようお願い申し上げます。

株式会社ファミリーマートによるカード券面画像公開に関する注意喚起

オバマ大統領の声明で「全米サイバーセキュリティ意識向上活動」として認められているインターネットを安全に使うための消費者向けセキュリティ普及啓発活動「STOP. THINK. CONNECT.」では、インターネットやウェブサイトにアクセスする前に「ちょっと立ち止まって、(例えば、そのウェブサイトにアクセスすることで)何が起こるか考える」意識を持つよう呼びかけています。

活動の一環として「安全なオンライン生活習慣のためのヒント&アドバイス」（http://stopthinkconnect.org/tips-and-advice/japanese-tips-and-advice/）情報が提供されています。

このような最新の情報を取得し、安全にインターネットを利用する新しい方法についてアンテナをはりつづけていることが、かしこいネットユーザへの近道です。

[林 憲明 トレンドマイクロ株式会社]

3.2. 様々なフィッシング対策用コンテンツ

近年、インターネットを利用したサービスも増え続けており、サービスを利用する消費者がフィッシング詐欺の被害に合うというニュースやメディアなどの報道も後をたちません。

フィッシングの動向で国内のフィッシング状況について説明しているとおり、2013 年のフィッシング報告件数、フィッシング URL 件数が急増しています。また、従来の金融機関をかたるフィッシング事例のほかに、オンラインゲームサービスや SNS、プロバイダの Web メールのアカウント詐取を目的とした多様なフィッシング事例が観測されるようになっており、今後もフィッシング事例や被害が増加・巧妙化していくことが懸念されます。このような現状を踏まえ、事業者側の対策も重要であるが、利用者へのフィッシング対策を促進することが重要と考えられています。

国内の事業者や業界団体は利用者向けのフィッシング対策の普及啓発コンテンツを作成しているので、いくつかのフィッシング対策コンテンツを紹介します。

■全国銀行協会「金融犯罪にご用心！」インターネットで行われる金融犯罪 [11]

全国銀行協会が金融犯罪に巻き込まれないために公開している啓発コン

[11] https://www.zenginkyo.or.jp/topic/hanzai/case09/index.html

テンツで、その中でフィッシング詐欺については、「犯罪の概要」、「犯罪の手口」、「犯罪の防止策」、「犯罪の事例」にカテゴリ分けされており、フィッシング詐欺の手口の紹介から対策・事例がわかりやすく紹介されており、さらに全国銀行協会のマスコットキャラクターである BANK-KEN のワンポイントアドバイスが掲載されている。

図 3-1　金融犯罪にご用心！

■クレジットカード協会「いつもキミをまもりたいから」[12]

日本クレジットカード協会がクレジットカードの不正使用を防止するために、消費者に対してフィッシング詐欺の注意すべき事例や要点をまとめたアニメ動画で、劇中に「被害防止の 5 つのお願い」としてフィッシング対策を紹介している。

図 3-2　いつもキミをまもりたいから

[12] http://www.jcca-office.gr.jp/consumer/stopphising.html

■フィッシング対策協議会「STOP!フィッシング詐欺について」[13]

フィッシング対策協議会がフィッシング対策の促進を目的として提供しているフィッシング対策教育コンテンツで、「フィッシング詐欺って何？」や「フィッシング詐欺事例」、「フィッシング詐欺対策力診断」、「被害にあわないための 5 カ条」、「フィッシング詐欺に気付いたら」を公開している。

図 3-3　STOP!フィッシング詐欺について

[JPCERT/CC]

[13] https://www.antiphishing.jp/stop_phishing/

■コラム　フィッシングの分類

フィッシングは大きく分けると、ネットワークを利用したものと、電話機などの物理的機器を利用したものに分類することが出来る。

ネットワークを利用したフィッシングについては、その犯行の端緒によってまず分類することができる。具体的には以前より大半を占めるメールと、最近増えてきているウェブを用いたものである。

被害者に送信されるメールを端緒とするものであっても、Web に誘導する場合と、メールの添付ファイルなどによりトロイの木馬（マルウェア）に感染させようとするものがある。

メールを介して Web 上のフィッシングサイトに誘導させるものが、いわゆる狭義のフィッシングである。

■ネットワーク利用				
	■メール利用			
		ウェブ利用		
			狭義のフィッシング	
			フリーダイヤル利用	
			ワンクリック詐欺	
				携帯電話利用
				ウェブ利用
		トロイの木馬（マルウェア：Malicious Software）		
			ターゲット型（スピア型）	
			無作為型	
				キーロガー/スパイウェア
	■ウェブ			
		トロイの木馬（Downward 型マルウェア：Malicious Software）		
■物理的機器の利用※				
	■Voice Phishing（ビッシング： Vishing）			
		振込詐欺(電話 ＆ ATM 等の利用)		
		ID 盗難		

※「ATM スキミング」により、カード情報や暗証番号等を盗取する方法があるが、広義のフィッシングとして分類するには無理があるため、分類から外した。

[内田 勝也 情報セキュリティ大学院大学名誉教授，事務局]

4. まとめ

2012 年後半から急激に増加したフィッシング被害は、2013 年に入っても減少するどころか増加を続け、その被害は拡大の一途である。特に金融機関における不正送金は大きな問題となっている。

2013 年に多発したネットバンク不正送金事件の多くは、マルウェアを利用したフィッシング事件である。このような手法は、一昨年度、昨年度のフィッシングレポートで警戒を呼び掛けていたものであるが、被害が相次いでいるのは残念というほかはない。

また手法の高度化・精緻化が進んでいることも特徴的である。悪用を防ぐために本レポートでは触れていないが、各オンラインバンキングのサービスの特色に合わせて、攻撃手法をカスタマイズするなど、より巧妙かつ悪質になってきている。利用者・事業者ともに、常日頃からの情報収集や迅速な対応がより重要になってきている。

これらの現状に対しては、協議会は今後も動向に関する最新情報を収集し、新たな手法に対する技術的対策などを検討する必要がある。

（空白）

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
構成員名簿

（敬称略・順不同）

【主査】

内田 勝也	情報セキュリティ大学院大学名誉教授

【副主査】

野々下 幸治	トレンドマイクロ株式会社

【構成員】

水村 明博	EMC ジャパン株式会社
花村 実	EMC ジャパン株式会社
早川 和実	NTT コミュニケーションズ株式会社
加藤 孝浩	トッパン・フォームズ株式会社
長谷部 一泰	アルプスシステムインテグレーション株式会社
八津川 直伸	日本ユニシス株式会社
山本 和輝	BB ソフトサービス株式会社
林 憲明	トレンドマイクロ株式会社
鈴木 哲治	株式会社ジャックス
伊東 達彦	一般社団法人全国銀行協会

【オブザーバ】

経済産業省商務情報政策局情報セキュリティ政策室
株式会社みずほ銀行
株式会社三菱東京 UFJ 銀行
株式会社三井住友銀行

【事務局】

JPCERT コーディネーションセンター
株式会社三菱総合研究所