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 2013

－　フィッシング被害の社会問題化　－

平成 25 年 6 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 年は我が国におけるフィッシングについてエポックメイキングな年であった。

2012 年 3 月、不正アクセス禁止法が改正され、同年 5 月 1 日から施行された。改正された不正アクセス禁止法では、他人の ID・パスワードの不正流通を防止することが主要な改正点であり、これはフィッシング行為の禁止・処罰を大きな目的としたものである。

一方で、2012 年のフィッシング件数は年初から前年度のトレンド通り高水準で推移したが、4 月以降はさらに活発化しており（特にフィッシングサイトの件数）、2013 年に入ってさらに件数が増加している（図 1-1）。

フィッシング対策協議会に対するフィッシング情報の報告件数は 2012 年度で、対前年度で約 66%増（2011 年度 498 件から、2012 年度 828 件）、フィッシングサイトの件数は、対前年度で 293%増（2011 年度 582 件から、2012 年度 2286 件）である。

一方で、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は、2012 年度は対前年度で 20%減少（2011 年度 147 件から、2012 年度 117 件）している。これは、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おり、注意を要する。

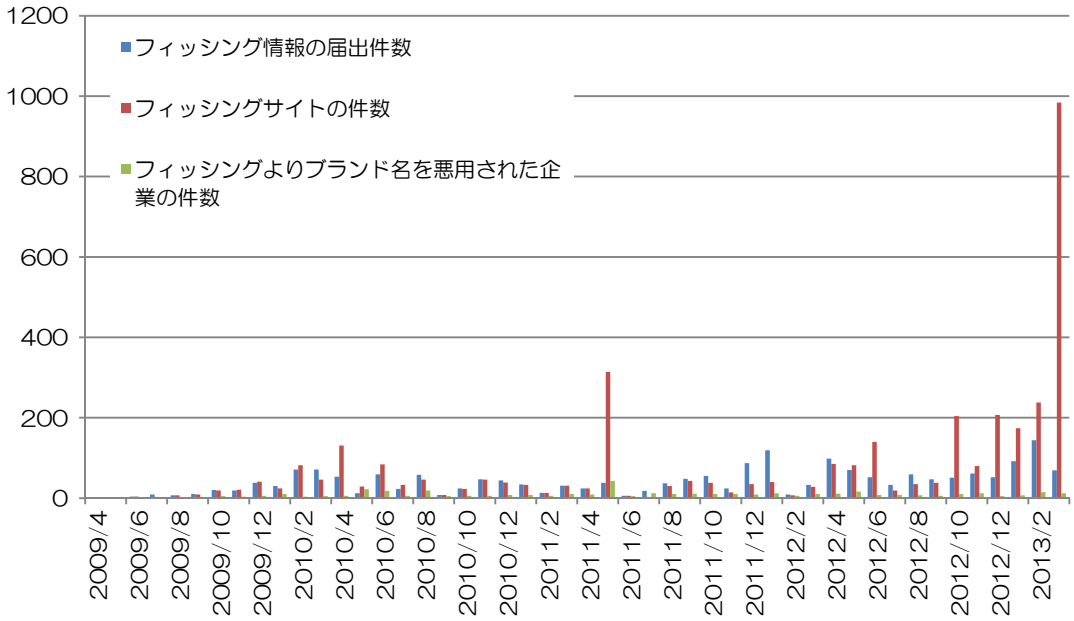

図 1-1　フィッシング対策協議会への届出件数等

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）は昨年度に比べて減少した（図 1-2）。また、その手口を見ると、2012 年（平成 24 年）はフィッシングは 18 件であり、比率は約 3%となっている（図 1-3）。

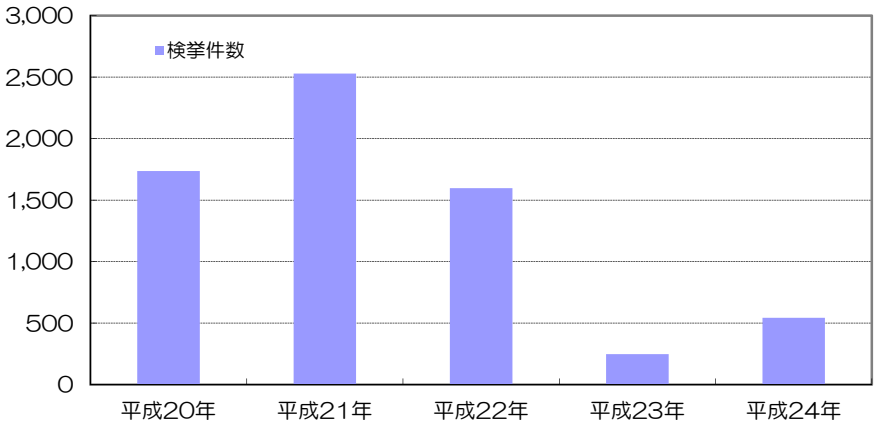

図 1-2　識別符号窃用（ID 窃盗）型不正アクセス行為の検挙件数[1]

[1] 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/h24/pdf041.pdf よりフィッシング対策協議会が作成

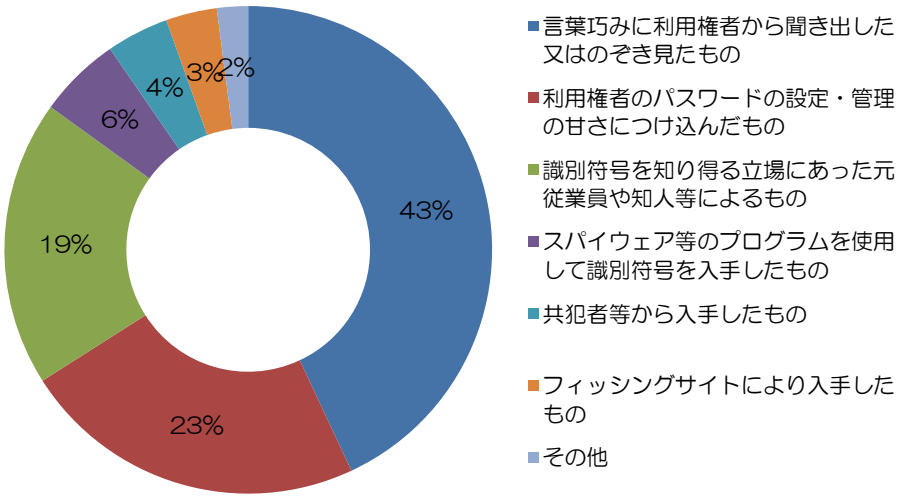

図 1-3　不正アクセス行為に係る犯行の手口の内訳[2]

従来、我が国はフィッシング被害について、諸外国よりも影響が少ないと言われてきた。しかし、2012 年は我が国の銀行等を中心に多くのフィッシング被害が発生するとともに、不正アクセス禁止法改正に伴い、フィッシング犯として初の逮捕者が出た。2013 年もこのトレンドが継続しており、フィッシング対策はインターネット関連事業者はもちろん、インターネット利用者にとっても喫緊の課題となっている。

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、2011 年 4 月から 2012 年 9 月までのフィッシング情報の届出件数において、フィッシングメールの件数としては横ばい傾向にあるものの、2011 年 11 月からフィッシングサイトの件数が大きく増加している。（図 1-4）。その為、引き続き注意が必要である。

[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/h24/pdf041.pdf よりフィッシング対策協議会が作成

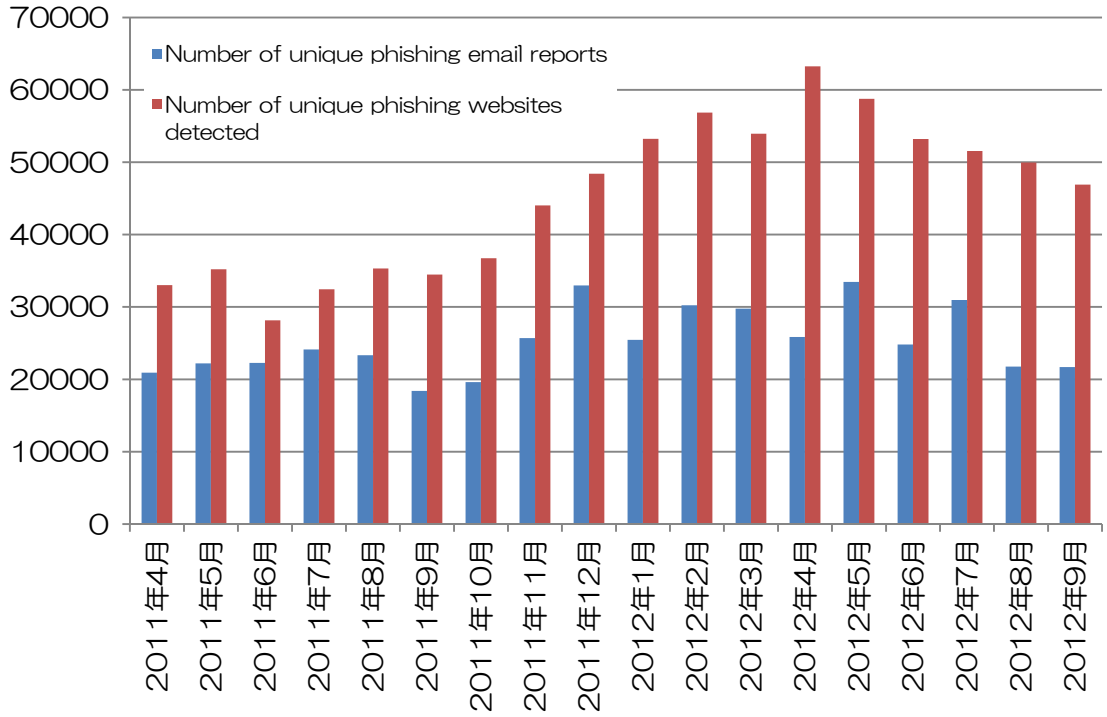

図 1-4　APWG への届出件数等[3]

[3] APWG (Anti-Phishing Working Group), " Phishing Attack 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. 巧妙化するフィッシング手口

2012 年はオンライン犯罪（とりわけインターネットバンキングを狙う犯罪）にとって、特徴的な事件や新たな技術が散見される年であった。年初から夏場にかけて大手金融機関を標的とするフィッシングが断続的に発生し、6-7 月期には総額約 2,950 万円の不正引き出しが発生するという事件に発展した。(2012 年 8 月 29 日 警察庁)

この時期のフィッシングは、不正なサイトを立ち上げて ID/パスワード情報などを入手するという標準的な手法が多く見られた。しかしその後、HTML メールに不正サイトのコンテンツを貼り付けたり、ISP の CGI プログラムを悪用したサイトなども発生し、その手法は多様となった。

図 2-1 ゆうちょ銀行をかたるフィッシングサイト[4]

2012 年のオンライン犯罪で最も特筆されるべき事件は、10-11 月頃に発生した、ポップアップ画面を表示させてインターネットバンキングの情報を盗み

[4] フィッシング対策協議, http://www.antiphishing.jp/news/alert/20121029.html

取ろうとする犯罪（通称：ポップアップ型フィッシング詐欺）であろう。この犯罪には、ポップアップを表示するためにマルウェア(トロイの木馬など)が利用されており、それらに感染した消費者のパソコンで不正なポップアップが表示され、そこから ID/パスワード情報などが窃取され、不正な振込や送金が発生する事件となったと考えられている。この手法は金融機関を装う偽メールやフィッシングサイトの設置を必要とせず、正規のインターネットバンキングサイトへのアクセス時に、不正なポップアップ画面を表示させるという点で実に巧妙であった。発表されている情報によれば、この様な事例は全部で 7 つ（住信 SBI ネット銀行、みずほ銀行、三井住友銀行、三菱東京 UFJ 銀行、ゆうちょ銀行、楽天銀行、三菱 UFJ ニコス）の金融機関の顧客に対して行われたことが確認されている。そのうち数社では不正な引き出しも確認されている。(総被害額は 420 万円(2012 年 11 月 9 日　警察庁)

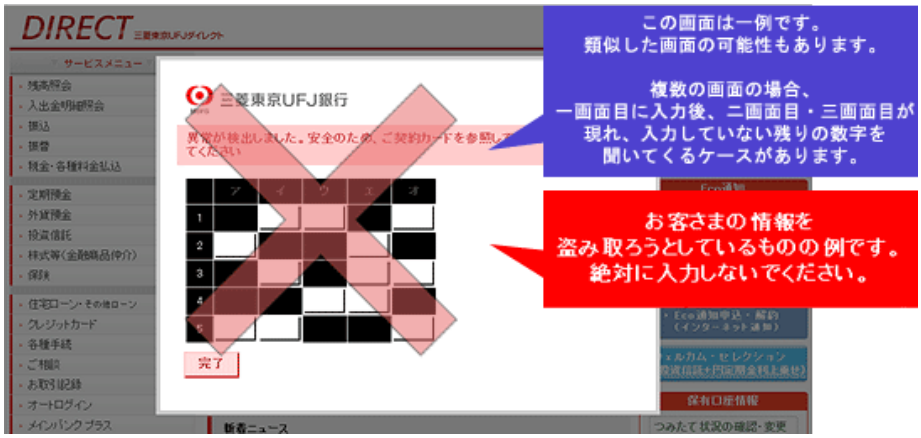

図 2-2 三菱東京 UFJ 銀行を装った偽画面の一例[5]

ポップアップを表示するためにマルウェアは諸外国、特に欧米では”Banking Trojan(オンラインバンキングを狙うトロイの木馬)”と呼ばれ、多くの被害をもたらしてきた。2012 年はこれらの被害が日本に及びはじめた。2011 年に有名な多機能 Banking Trojan である「Zeus」のソースコードが流出してから、これまでに無い低価格版や多様な機能パッケージとなった亜種が流通し利用される傾向にある。

[5]三菱東京 UFJ 銀行、http://www.bk.mufg.jp/info/phishing/ransuu.html

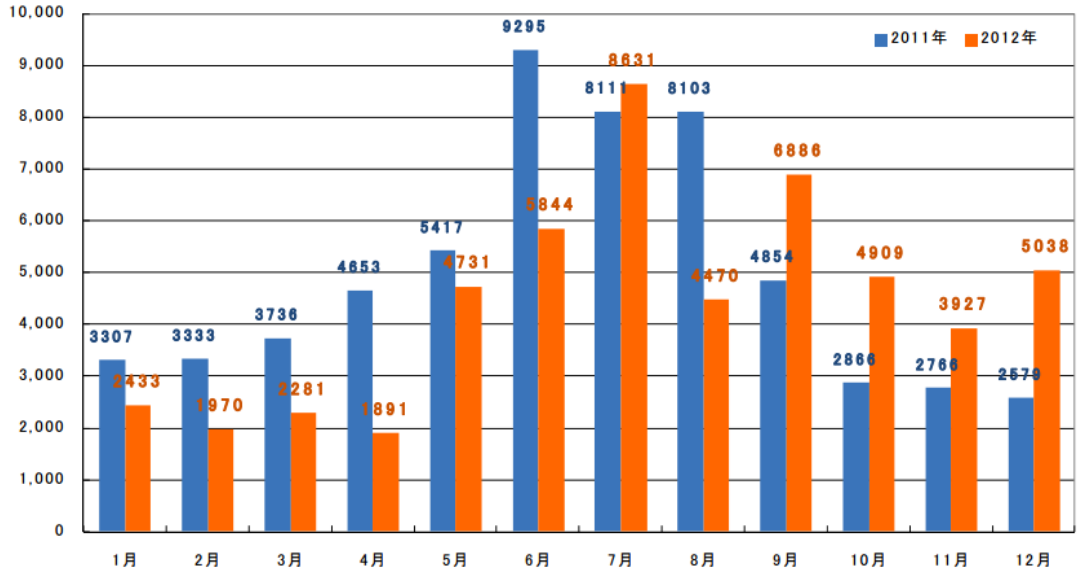

図 2-3 トロイの木馬による月間攻撃数の推移[6]

中でも、2012 年に特に目立ったのは、トロイの木馬「Citadel」であろう。Citadel は Zeus の基本的な機能を踏襲していることも特徴としてあげられるが、最大の特徴は、その卓越したサービスであろう。アンダーグラウンドの世界では、自らトロイの木馬のコードを開発しない犯罪者も多い。彼らのような犯罪者のために、FaaS (Fraud as a Service) が発達してきており、テクノロジーが簡単に金で手に入る時代になっている。Citadel の開発グループは、質問にタイムリーに答えるという通常のサービスの他に、利用者（恐らく犯罪者）同士が情報を共有するコミュニティも提供している。オープンソースのコードがその開発者のサポートやコミュニティで急速に品質が向上していくように、Citadel のコードもその品質が向上している。犯罪者はこの Citadel を利用して諸外国の銀行を狙い始めている。日本のオンラインバンキングサービスを狙ったものも確認されており、今後さらなる注意が必要なトロイの木馬である。

このような犯罪者によるフィッシングやトロイの木馬の被害に合わないようにするにはどうしたらよいのだろうか。

(1) 対策

犯罪者はトロイの木馬のようなマルウェアを用いた複合的な手法によって、思いもよらない新しい手口を次々と編み出してくるため、消費者自身の目視に

[6] RSA, Monthly AFCC NEWS Vol.67, http://www.rsa.com/japan/pdf/solutions/AFCC_news/AFCCNews_130312.pdf

よるフィッシングサイトの判断や、セキュリティソフトの機能に頼るような、従来の知識、手法だけでは被害を防ぐことが困難になっている。

今後消費者が、被害に会わないようにするためには、以下のような対策が必要と考えられる。

1） OS やアプリケーションの脆弱性に関する修正プログラムを迅速に適用する。

マルウェアの感染は、ドライブバイダウンロードによる OS、主要アプリケーションの脆弱性を利用した手口が主流となっており、特に脆弱性を突いた攻撃は、セキュリティ対策ソフトだけでは保護できないケースもあるため、常に最新の脆弱性パッチを適用しておくことが肝要である。

2） セキュリティソフトのプログラムアップデート、パターンファイルは最新のものにしておく。

犯罪者は常にセキュリティソフトに検出されない工夫をマルウェアに施している。検知エンジンのアップデートやパターンファイルのこまめな更新は不可欠である。まして、対策ソフトの期限切れなどは絶対に無いよう注意したい。

3） 金融機関が消費者に対して行わない事を把握しておく。

金融機関が消費者に対して電話やメールで暗証番号を聞いたり、第 2 認証情報 (第二暗証、第三暗証など)の全ての情報を入力させたりすることはない。犯罪者の巧妙な騙しのテクニックにひっかからないよう、判断規準となる知識を持っておく必要がある。

4） 最新のフィッシング手口に関する情報に関心を持ち、予備知識を得ておく。

「私は騙されない」「対策をしているから大丈夫」といった過信が最も大きな落とし穴。どのような対策にも完全なものは無いという意識を持ち、危険性の発見、判断がつくように、新しい手口に関する予備知識を得ておくことが重要である。

このような行動を取り、常にネット犯罪への関心と警戒意識を維持することが、フィッシング被害から身を守るため必要であると考えられる。

[本稿執筆担当：水村明博（EMC ジャパン株式会社）]

2.2. ポップアップを使ったフィッシング詐欺

(1) 概要

2012 年 10 月頃から国内金融機関をかたるフィッシングサイトのうちに、ポップアップメッセージを利用する手口が確認された。

ユーザが正規のインターネットバンキングサイトにログインした後に、ブラウザ上に第 2 認証情報（乱数表や合言葉など）の入力を促すポップアップメッセージが表示（図 2-4）され、あたかも正規サイトが入力を促しているようにユーザに見せかけ、第 2 認証情報などの詐取を試みる手口である。ユーザがサイトにログインした後にポップアップメッセージが表示されるため、URL からは不正であることを判別することが困難である。

図 2-4 不正なポップアップ画面イメージ（ゆうちょダイレクト）

これは利用者の端末がウイルスに感染していて、特定のサイトを閲覧時にあらかじめ用意された不正な Javascript を挿入することによって行われる。このような行為を行うウイルスは特に”Banking Trojan”などと呼ばれ、欧米においては数年前から被害が多数報告されていた（図 2-5）。

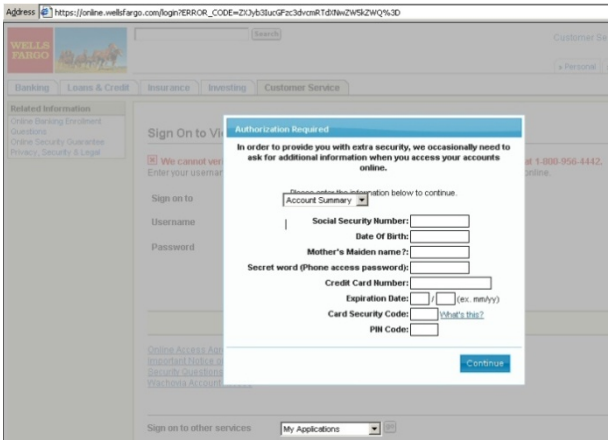

図 2-5 不正なポップアップ画面イメージ（海外事例）[7]

[7] http://blog.webroot.com/2010/08/20/a-cave-monster-from-hell-wants-your-financial-data/

(2) 対策と課題

ポップアップを使ったフィッシングについては URL から不正な表示であることを判別することは不可能であるため、その対策についてはまず利用者への啓発活動を十分に行う必要がある。啓発活動において特に重要なのは以下の 2 点である。

① ウイルス対策の重要性の周知

利用する端末を安全に保つことの重要性は、ポップアップを使ったフィッシング手口の増加により、さらに高まった。端末がウイルスに感染している場合には、どのように利用者がフィッシングサイトに注意を払っても無意味となるからである。フィッシャーは、ポップアップを表示せずとも、キーボード入力からオンラインバンキングの認証情報を盗むことが可能である。海外で流行している”Banking Trojan” が日本のオンラインバンキング、オンラインサービスの認証情報をターゲットに加えたという事実をふまえ、あらためてセキュリティ対策の基礎である、ウイルス対策ソフトを利用し、パターンファイルをアップデートすることが重要であることを、サービス事業者がサービス利用者に訴えることが必要である。

② 第 2 認証情報 (第二暗証、第三暗証など)の取り扱いについて周知

いかなる場合であっても、第 2 認証情報を全て入力させることはないということを利用者に対して十分に周知することが必要である。ポップアップを使ったフィッシングが確認された国内の銀行などでは速やかにこの周知が行われた。このような注意は、フィッシャーがポップアップを表示させるであろう直前、つまりオンラインサービスであればログイン画面に掲載すべきである。

以上、利用者への啓発をオンラインサービス事業者やセキュリティベンダー、関係機関が繰り返すことが被害の拡大防止にもっとも効果的であるとかんがえるが、加えてオンラインサービス事業者による監視については以下の点を留意いただきたい。一つ目は手口はかならずしもポップアップとは限らないということである。2012 年後半に確認されたのは Javascript でポップアップを表示させる手口であったが、既に海外では正規の HTML コンテンツ中にフィッシャーの管理するサーバに情報を送信するフォームを埋め込む手口が確認されており、今後も手口は変わっていくことが予想される。ポップアップ表示に対する注意をよびかけるあまり、ポップアップ表示でなければ安全というミスリードがおきないように配慮をする必要がある。二つ目はユーザアクティビティの監

視である。具体的にはオンラインサービスのログ中に利用者からの存在しないコンテンツへのアクセスがあった場合には特に注意が必要である。フィッシング対策協議会では、ポップアップ表示によるフィッシング事例で埋め込まれた Javascript を確認したが、その一部はサーバ上の存在しないコンテンツへのアクセスが確認されている。サーバのログを確認し、存在しないコンテンツへのアクセスを素早く見つけることで、同様のフィッシングの発生をより早く把握することが可能と考える。

3. その他の攻撃手法

3.1. モバイルフィッシング

(1) 概要

フィッシング対策協議会では、2011 年 5 月に公開した「フィッシングレポート 2011」において、スマートフォンの普及が急激に伸びると予想されるため、新たな脅威の動向としてモバイルフィッシングを取り上げた。2012 年度、スマートフォンは当時の予測を上回るスピードで普及しつつある。（図 3-1）キッズやシニア世代向けスマートフォンも発売され、全ての世代において普及が進んでいる。（図 3-2）

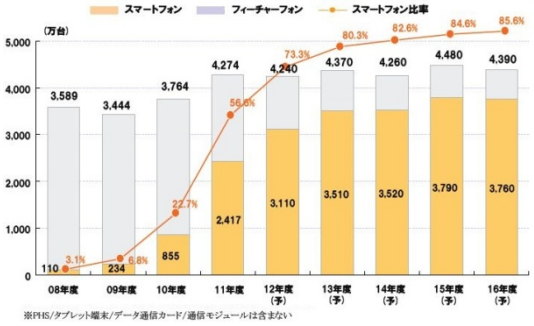

図 3-1 国内スマートフォンの出荷台数推移・予測[8]

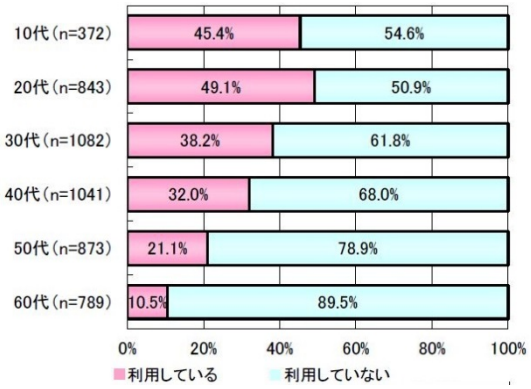

図 3-2 スマートフォンの利用状況[9]

(2) 被害の状況

スマートフォンの急激な普及により、攻撃者たちのターゲットもスマートフォンに向けられ、不正アプリが急増している（図 3-3）。ワンクリック詐欺アプリや、「セーフ・バッテリー（電池長持ち）」「電波改善」「安心ウイルススキャン」などとユーティリティアプリやセキュリティアプリを装って利用者を騙し、個人情報を収集するアプリなど、攻撃の手法が進化している。
スマートフォンが攻撃を受けた結果、以下のような被害が想定される。

---

[8] MM 総研調べ「2012 年度上期 国内携帯電話端末出荷状況」（2012/11/1）

[9] 独立行政法人 情報処理推進機構「2012 年度情報セキュリティの脅威に対する意識調査」（2012/12/11）

・メール、電話帳、端末情報（電話番号、端末番号、他）などが漏えいする
・端末の GPS 情報が窃取され所有者の行動情報が漏えいする
・端末をコントロールする権限を窃取され、遠隔操作されたり、有料サービスを悪用される

電話帳が漏えいした場合、不正アプリを使用した本人が被害を受けるだけでなく、友人・知人の情報が攻撃者の手に渡ってしまうことが大きな問題である。Web メールやショッピングサイト、携帯キャリアなどの各種サービスでは、ID にメールアドレスや電話番号を使用している場合も多い。攻撃者がメールアドレスや SNS のアドレス、電話番号を入手すれば、パスワードのみを探り当てれば不正アクセスが可能となる。安易なパスワードは、攻撃ツールを使って容易に解読でき、電話帳に住所や誕生日・記念日などの情報まで登録していると、パスワード推測に、多くのヒントを与えることになりかねない。トレンドマイクロの調査（図 3-4）によるとスマートフォン利用者の 50%が電話帳に 100 人以上登録しているという。1 人の不注意が多くの友人・知人に迷惑を掛けることになりかねない。

本項では、2012 年度に発生した新たな攻撃・脅威について報告する。

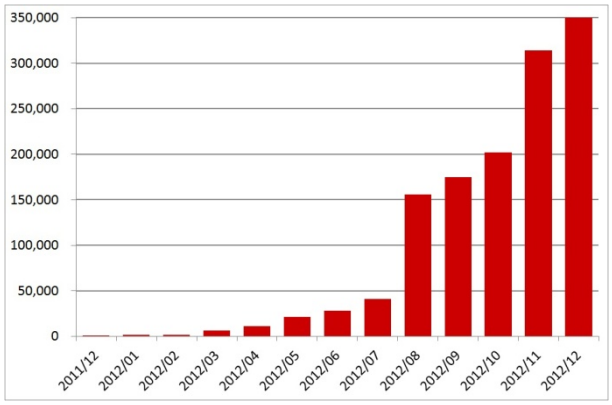

図 3-3 Android 端末に感染する不正アプリ数[10]

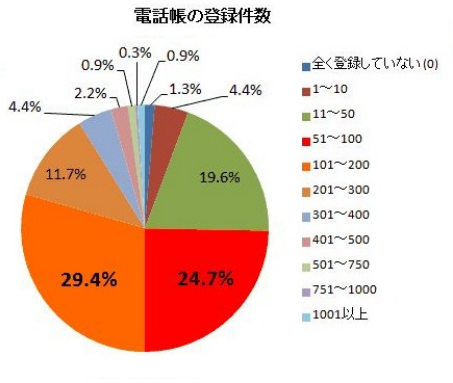

図 3-4 スマートフォンの電話帳の登録件数[11]

（不正アプリによる電話帳等の漏えい）

[10] トレンドマイクロ株式会社「2012 年度インターネット脅威年間レポート」（2013/1/10）
http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20130107041500.html
[11] トレンドマイクロ株式会社「スマートフォンの利用実態調査」（2012/12/25）
http://jp.trendmicro.com/jp/about/news/pr/article/20121221094239.html

端末情報や電話帳のデータが漏えいした場合、想定される被害を予測してみる。2012 年にワンクリック詐欺を目的とした不正アプリが報告された。[12] 従来報告されているワンクリック詐欺は、PC 上からブラウザで詐欺サイトにアクセスするため、メールアドレスなどが攻撃者に自動的に漏えいすることはない。しかしスマートフォンの場合、攻撃者はアプリをインストールさせることにより、定期的にブラウザを起動して請求画面を表示する例が確認されている。バイブレータ機能によりスマートフォンを振動させたりして恐怖を煽り金銭を要求する。さらには電話番号やメールアドレスを入手し、SMS やメールにより請求を行ったり、電話を掛けてくる（ワン切りも含め）ことも想定される。

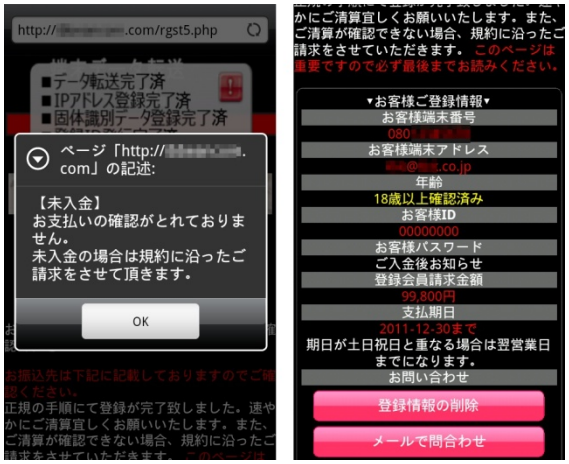

図 3-5 不正アプリから電話番号が表示される請求画面

図 3-6 偽 Google Play へ誘導するメール

また、攻撃者はターゲット名簿を作成する手段として不正アプリを活用している可能性がある。2012 年 7 月より報告されている事例では、「セーフ・バッテリー（電池長持ち）」「電波改善」といったスマートフォンの機能を補うユーティリティアプリを装った不正アプリが報告されている[13]。これらの不正アプリはいずれのスマートフォンにおいても、「お使いの端末は未対応のためご利用いただけません」というメッセージを表示し、利用者にアプリの終了を促す。すなわち最初からスマートフォンの機能を補う意図は一切なく、一連のアプリ名称は利用者を騙すためだけにつけられた悪質な宣伝文句に過

[12] トレンドマイクロ株式会社「スマホを狙ったワンクリックウェアを確認。執拗に請求画面を表示し、電話番号の流出も／トレンドマイクロ セキュリティ ブログ」（2012/1/11）http://blog.trendmicro.co.jp/archives/4714

[13] トレンドマイクロ株式会社「アドレス情報を効果的に盗み取るスマホ向け脅威「ANDROIDOS_CONTACTS」ファミリを確認／トレンドマイクロ セキュリティ ブログ」（2012/9/11）
http://blog.trendmicro.co.jp/archives/5931

ぎない。アプリ終了を促す画面の裏では、電話帳を取り込み、攻撃者が用意した外部のサーバに送信しているのである。

（偽マーケット）

スマートフォンのアプリは、通常オフィシャルサイトから入手する。iPhone(iOS)であれば Apple Inc.が提供する「App Store」のみであるが、Google Inc.が提供する Android は自身が運営する「Google Play（旧 Android Market）」のみならず、通信事業者[14]やコンテンツホルダー[15]などの事業者がアプリの配布・販売を行うマーケットプレイス事業に参画している。このため、アプリをダウンロードする際は、アプリの安全性について審査を行っているマーケットを選択することが一つの目安となる。
また、攻撃者は信頼されたマーケットと混同させることを目的としてデザインや名称を模したマーケットへ誘導する事例が報告された[16]。2013 年 1 月「Gcogle Play」（2 文字目が「o」ではなく「c」）と Google Play を模した Web サイトに個人情報を搾取する不正アプリが掲載された。（2013 年 1 月 15 日時点では名称が変更されている[17]）なお、このアプリは個人情報を暗号化（SSL）して外部のサーバに送信している特長がある。

（クラウドを利用した ID 管理アプリ）

Web メールやショッピングサイトなどで使用する ID とパスワードは、サービスごとに、別々とすることを、フィッシング対策協議会では呼びかけている。利用しているサービスが多いほど、利用者は混乱を避けるために URL・ID・パスワードを一括管理できるアプリ（以下、ID 管理アプリ）を使用することが容易に推測される。ID 管理アプリの中には、クラウドを使用して、データをクラウド上で管理するものも多くある。スマートフォンはパソコンに比べ、保存できるデータ容量が少ないためクラウドサービスを利用する利用者が多い傾向にある。また、ID 管理アプリや各種のクラウドサービス、およびクラウドに保存したデータはパソコン、スマートフォン、タブレットなど複数のデバイスで使用することを考えるとクラウドの活用は、利便性が高い。しかし、この数年報じられている通り、クラウドサービスや会員制サービス

[14] KDDI 株式会社が運営する「au Market」、株式会社 NTT ドコモが運営する「d マーケット」、ソフトバンクモバイル株式会社が運営する「ソフトバンク ピックアップ」など
[15] 株式会社バンダイナムコゲームスが運営する「バナドロイド」、株式会社スクウェア・エニックスが運営する「SQUARE ENIX MARKET」など
[16] 株式会社シマンテック「Android.Exprespam の出現は地検の不起訴が引き金か／　シマンテック　セキュリティレスポンスブログ」（2013/1/8）
http://www.symantec.com/connect/ja/blogs/androidexprespam
[17] 株式会社シマンテック「Android.Exprespam の作成者グループ、Gcogle Play から「ANDROID EXPRESS の PLAY」にリニューアル／シマンテック　セキュリティレスポンスブログ」（2013/1/15）
http://www.symantec.com/connect/ja/blogs/androidexprespam-gcogle-play-android-express-play

を狙った不正アクセスにより、情報漏えい事件が多発していることも事実である。各種サービスの ID とパスワードを管理しているクラウドサービスが不正アクセスにより、被害を受けたら影響は甚大となる。

ID 管理アプリがデータをスマートフォン上に保存している場合であっても、そのデータ自体を、ストレージサービスのようなクラウドに預けた場合も、同様である。（2012 年 8 月 Dropbox が不正アクセスにより、社員のフォルダへ侵入されユーザ情報が漏えいする事件が発生し、二重認証などの対策が講じられた事例もある）

（SNS）

従来のフィッシング詐欺の手口は、攻撃者が差出人を詐称したメールを送り、受信者が攻撃者が用意した偽の Web サイトへアクセスして、ID やパスワード、口座番号などを入力することで、これらの情報が搾取される。

昨今、SNS（ソーシャル・ネットワーキング・サービス）は全世界の多くの人々に利用されている。スマートフォンは画面が小さいとはいえ、常時インターネットに接続されているため、移動中でも確認でき、スマートフォンで撮影した写真を簡単に投稿できるなど、パソコンより便利な面も多く、スマートフォンでの利用が進んでいる。

IPA では SNS のサービス連携について注意を呼びかけている[18]。例えば、Twitter には、「ツイート（つぶやき、投稿）」と「フォロー」という仕組みがある。「フォロー」とは、他の利用者のツイートを自分のタイムラインに表示することでいち早く他の利用者のツイートを見ることができる機能である。被害の事例として攻撃者（X）が Twitter 上でツイートし、それをフォローしている利用者（A）が、連携サービスを利用すると、利用者（A）をフォローしている他の利用者（B）に、連携サービスが（A）の代わりに勝手に書き込んだツイートが載ってしまう。攻撃者（X）は、当初は興味を引く話題を提供して、フォローする利用者を集めた後、フィッシングやウィルスをダウンロードさせるようなツイートを書き込むことで、被害が拡大する。なお、連携サービスを利用したとしても、連携サービス側に、ID やパスワードが漏えいすることはない。

一般的にメールより SNS から発信される情報の方が、被害に遭いやすい。これは、SNS は利用者自身が相手を信頼していることに起因すると言われる。しかし、SNS における公開の範囲に"友達の友達"というカテゴリーがある。

[18] 独立行政法人 情報処理推進機構 2012 年 10 月の呼びかけ「SNS におけるサービス連携に注意！ 」～ あなたの名前で勝手に使われてしまいます ～（2012/10/1）

JNSA の報告[19]によると、Facebook の友達の平均は 130 人、“友達の友達”は 8500 人にもなり、全てが信頼できるアカンウトであるとは限らず、無制限の公開と変わりはないと言う。

(3) 対策と課題

「フィッシングレポート 2011」にて、スマートフォン特有のフィッシング対策を紹介した。

スマートフォンの急激な利用拡大にもかかわらず、標準メーラーやブラウザでは正当なメール/サイトかどうかの確認がしにくく[20]、ダウンロードしたアプリでは情報の送信先や送信する情報が暗号化されているかどうか確認が困難であり、改善が待たれるところである。

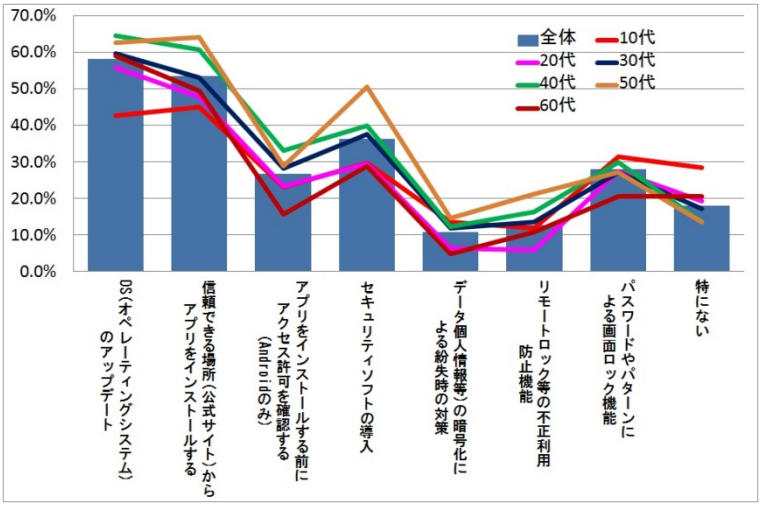

図 3-7　スマートフォンのセキュリティ対策の実施状況[21]

「OS をアップデートする」「アプリはオフィシャルサイトから入手する」「セキュリティソフトの導入」などは、浸透しつつある（図 3-7）が、さらなる啓発が必要である。特にスマートフォンの経験が浅い、キッズやシニア世代の利用者に対しては、パソコンや携帯電話との違いを理解して対策を実施してもらいたい。

前述のワンクリック詐欺アプリを含め不正アプリへの対策としては、「アプ

[19] JNSA（NPO 日本ネットワークセキュリティ協会）「SNS の安全な歩き方」（2012/11/19）

[20] 携帯やスマートフォンでは、メール受信にあたって電子署名を確認できないことが多い。また、ブラウザは画面が小さい/URL が表示されない/証明書が表示できない（もしくは容易ではない）といった理由により、本物のサイトであるという確認がつきにくい

[21] 独立行政法人 情報処理推進機構「2012 年度情報セキュリティの脅威に対する意識調査」（2012/12/11）より執筆者にて作成

リをインストールする前に、アクセス許可を確認する」ことで防げる可能性がある。電話帳にアクセスする必要があるのか？ネットワーク通信が必要なのか？インストールするアプリの機能から想像してみることも対策の一つである。また、フィッシング詐欺が本物とそっくりの Web サイトに個人情報を入力させる手法であるが、同様に Google Play などの信頼できるマーケットの偽サイトやメジャーなアプリの偽アプリも出現している。疑問に思うものは、インストールする前に、アプリ名などにて検索を行い評判を調べるなど、慎重に対応してほしい。

[本稿執筆担当：本多規克（アルプスシステムインテグレーション株式会社）]

3.2. SNS

ソーシャルエンジニアリングとは、技術的な方法では無く、社会的な方法(人の心理的な隙やミスを狙った方法)を使用し、情報を聞き出したりする行為である。一般的には、電話で取引先などをかたり情報を入手しようとしたり、また宅配業者などをかたり住所などを聞き出すといった行為の事を言うが、最近では、もっと手軽に情報を入手できる方法がある。それはソーシャルネットワークサービス(以下、SNS)などに掲載してる内容から情報を入手する方法である。例えば、サイバー犯罪者は、SNS で公開されている情報から生年月日や連絡先、友人や知人など多くの情報を入手可能である。また、サイバー犯罪者は、友人や知人になりすましてフィッシングメールを本人に送付することも可能である。普段はフィッシングメールにだまされない人でも、友人や知人などを装っているため、誤ってフィッシングメールに騙される。

3.3. QR コード

QR コードを使用したフィッシングサイトへの誘導といった手法がある。この手法は、以前からある方法ではあるが、街中や空港といった人通りの多い所に貼られているキャンペーンポスター等で使用されている QR コードの上に、サイバー犯罪者が、偽の QR コードのステッカーを貼ることで、携帯電話やスマートフォンなどで読み込んだ人々を、偽のキャンペーンサイトへ誘導することが可能となる。こういった一見地味と思える手法で、個人情報を取られるケースも考えられる。

4. コラム

4.1. 株式会社セガにおけるフィッシング対策事例

従来、フィッシングには電子メールを用いたフィッシングサイトの告知が良く知られている方法である。

しかし最近では多様化しており、株式会社セガ（以降、セガ）のオンラインサービスアカウント窃取をねらった過去の事例では

・　掲示板サイト、SNS 等での書き込み、誘引

・　ゲーム内チャット機能を使用

といった手法も報告されている。

サービスの性格上、該当のフィッシングサイトで ID とパスワードを入力すればゲーム内で使用するアイテムをプレゼントするという宣伝が用いられることが多い。

また、フィッシングサイトは無料で使用できるウェブホスティングサービス上にセガのサイト内 html ソースや画像をコピーし、ID とパスワードの入力欄のみ変造するという手法が良く取られている。

このようなフィッシングに対し、セガではオンラインサービスを行っているウェブサイトおよび登録者に宛てた電子メールにてフィッシング等を含めたアカウントの窃取に対し常時注意喚起を行っている。

実際にフィッシングサイトが確認された場合は、すみやかにウェブサイトと電子メール、またゲーム画面上にテロップ(字幕)表示させることによって注意喚起を行い、被害が広がらないよう対策を行っている。

図 4-1 セガによる告知の例

なお、情報をフィッシング対策協議会に報告している。セガではフィッシング対策協議会と連携し、早期のフィッシングサイトの早期閉鎖や情報共有などを実施している。

[本稿執筆担当：簀本輝夫（株式会社セガ）]

4.2. スマホアプリの課題～スマートデバイスによるインターネット接続時の留意点

1．Web サイトの正当性確認について

ネットバンキングやネットショッピング等ネット経由で経済取引を行う場合には、SSL/TLS 接続により接続先 Web サイトが正当なサイトであることを確認する必要がある。

Web サイト正当性確認方法としては、以下(1)および(2)を行うのが通例である。

(1) Web サイトの URL を確認する

URL 中のホストネーム、ドメインネームが正しいことを確認する。

(2) Web サイトのサーバ証明書を確認する（図 4-2 参照）

基本的には、サーバ証明書に記載されている、CN（Common Name：一般名称）、O（Organization：組織）、OU（organization Unit：部門）等が正しいことを確認する。また、URL 中のホストネーム、ドメインネームが CN の値と一致していることを確認する。

図 4-2　サーバ証明書記載事項表示の例

しかしながら、スマートデバイスによっては標準ブラウザであっても(2)のサーバ証明書記載事項を

確認できないものが存在する。この場合、URL の確認程度でしか接続先の正当性を確認できないので注意を要する。

なお、サーバ証明書記載事項を確認できない場合の代替方法として、以下のような方法を紹介している Web サイトも存在する（図 4-3 参照）。

① SSL サーバ証明書を利用した通信であることを示す錠前マークが表示されていること。

② アドレスバーの上部の文字が緑色になっていること。

図 4-3　代替方法としてブラウザのアドレスバー表示を確認する例

2．重要なアプリの正当性確認について

スマートデバイス用の重要なアプリ、例えば銀行アプリの中には、資金移動等の作業を銀行サーバと通信しながらアプリ内で完了させるものが存在する。この場合、利用者は取引実行にあたり URL の確認やサーバ証明書の確認ができないので接続先の正当性確認ができない。

そのため利用者はアプリを全面的に信用して取引を実行せざるを得ないので、アプリは必ずオフィシャルサイトから入手しなければならない。

3．正当なアプリが抱える脆弱性を狙った攻撃の可能性について

正当なアプリであったとしてもそのアプリに脆弱性を含んでいる可能性を否定することはできない。脆弱性を抱えたアプリを使い続けることによる機微な情報の漏えい被害を予測してみる。ハノーバー大学とマールブルク大学の研究者チームは、Google Play ストアで 1 万 3,500 本の無料アプリについて、SSL/TLS が安全に実装されているか調査した。その結果、1,074 本のアプリが「認証時にあらゆる証明書、またはあらゆるホスト名を受け入れてしまう SSL 処理のコードが含まれているため、中間者攻撃に対して潜在的な脆弱性を持っていることを報告[22]している。こうした脆弱性のあるアプリを放置した場合、攻撃者が偽のサイトを用意し、そのサイトに対して機微な情報（個人情報など）を送信してしまうおそれがある。

機微な情報が他のアプリからも参照可能な場所（SD カードや他のアプリも参照可能な領域下にあるファイル/データベース）に保存されており、かつ暗号化されていない状態にあったアプリが報告[23]されている。こうした脆弱性のあるアプリを放置した場合、不正アプリが参照可能な機微な情報を読み取り、攻撃者の用意したサイトへ情報を送信してしまうおそれがある。

[22] ACM 会議「Why eve and mallory love android: an analysis of android SSL (in)security」（2012/10/23）, http://dl.acm.org/citation.cfm?id=2382205

[23] Skype「[Fixed] Privacy vulnerability in Skype for Android」（2011/4/15）, http://blogs.skype.com/2011/04/15/privacy-vulnerability-in-skype/

一部のアプリには他のアプリに対して自身の機能を自由に呼び出し可能な状態で公開しているものがある。こうしたアプリにおいてアクセス制限を行っていない場合、開発者の意図とは異なる形で不正アプリに正当なアプリの機能が悪用される可能性がある[24]。

ここにあげたシナリオは一例にすぎない。現時点において、個別アプリの脆弱性を狙った動きは極めて少数である。しかしながら、数百万の利用者を抱えるアプリも多く存在している。こうした中で、個別アプリの脆弱性を狙った攻撃が広まる可能性は否定できない。

アプリが抱える脆弱性そのものについては、利用者が対策を行うことは困難であり、開発者の努力を要するものである。開発者はアプリのセキュア設計に心掛け、脆弱性を作り込まない努力をすべきである。また利用者は OS が提供するアプリの自動更新、通知機能を活用し、脆弱性が報告されているアプリを使い続けることを避けるべきである。

4．偽 WiFi ポイントへの接続の脅威について

スマートデバイス、特にスマートフォンは利用者が手に持って移動しながらネット接続する機会が多いので、意図せず偽 WiFi ポイントに接続させられてしまう可能性がある。この場合、正しい URL（または IP アドレス）で接続していても偽サイトに誘導され、中間者攻撃される可能性があるので注意が必要である。この場合においても接続先の正当性確認は SSL／TLS 接続の上、サーバ証明書の確認が必要であるが、上記 1 のようにブラウザによっては確認できない場合もある。

従って、WiFi 接続する場合は、信頼できるアクセスポイントのみを利用することが肝要である。

[本稿執筆担当：八津川 直伸（日本ユニシス株式会社）、林 憲明（トレンドマイクロ株式会社）]

[24] JVN#31860555「twicca におけるアクセス制限不備の脆弱性」（2012/3/13）, http://jvn.jp/jp/JVN31860555/

5. まとめ

2012 年度は我が国においてもフィッシング被害が社会問題化した年として記憶されることになった。

特に 2012 年末に立て続けに発生したネットバンク不正送金事件は、マルウェアを利用した ID やパスワードなどの個人情報を詐取する事例である。このような手法は、昨年度の本レポートで注意を呼び掛けていたものであるが、それが実際に被害が発生したことは残念というほかはない。

昨今の状況を鑑みるに、海外で用いられた手法が日本に持ち込まれるリードタイムはますます短くなってきており、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。特に、今後利用者の増加が見込まれるスマートフォンなどのモバイルデバイスについては、従来の PC を想定した対策が通用しない点があることから、協議会としても注意深く動向を観察するとともに、必要となる対策についてはガイドライン等の改訂により対処していくことが重要と認識している。

（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
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
松田 知行	ネットスター株式会社
八津川 直伸	日本ユニシス株式会社
佐々木 智彦	楽天株式会社
山本 和輝	BB ソフトサービス株式会社
本多 規克	アルプスシステムインテグレーション株式会社
林 憲明	トレンドマイクロ株式会社

【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

【事務局】

一般社団法人 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