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 2012

― 新たな脅威の動向とそれに向けた対策と課題 ―

平成 24 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

2009 年の後半から、我が国におけるフィッシングの報告件数が増加している（図 1-1）。

2011 年度の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対前年度で約 23%増（2009 年度 283 件から、2010 年度 406 件、2011 年度 498 件）、フィッシングサイトの件数は、対前年度で約 13%増（2009 年度 260 件から、2010 年度 516 件、2011 年度 582 件）である。これは、2009 年度の傾向が継続しており、フィッシングサイトのテイクダウンを回避するなど、フィッシング手法の高度化や、関与する犯罪者の増加を反映しているものと考えられる。

さらに、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、2009 年度は前年から減少したのに対して、2011 年度は対前年度で 24%増加（2009 年度 46 件、2010 年度 119 件、2011 年度 147 件）している。これは、有名なサイト、つまり犯罪者から見た場合、効率的な一部の著名サイトを騙るフィッシングサイトが多かったのに対して、2011 年度は国内の金融機関をかたるフィッシングサイトが増加したことなど、フィッシングの対象となるブランド数がさらに増えつつあることを示しており、注意を要する。

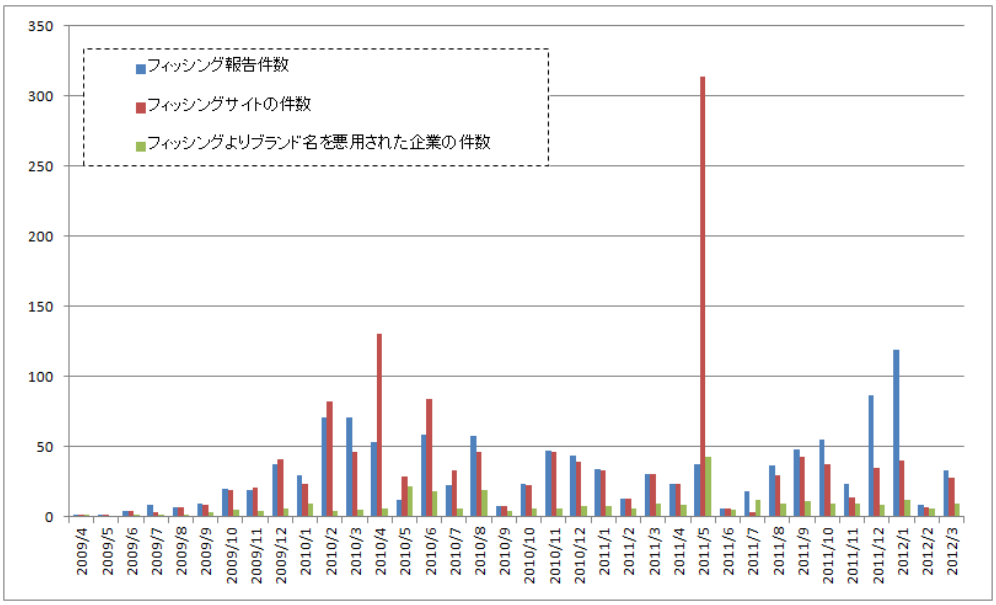


図 1-1　フィッシング対策協議会への届出件数等

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、平成 23 年はフィッシングが一番多く（25%）となっている（図 1-3）。

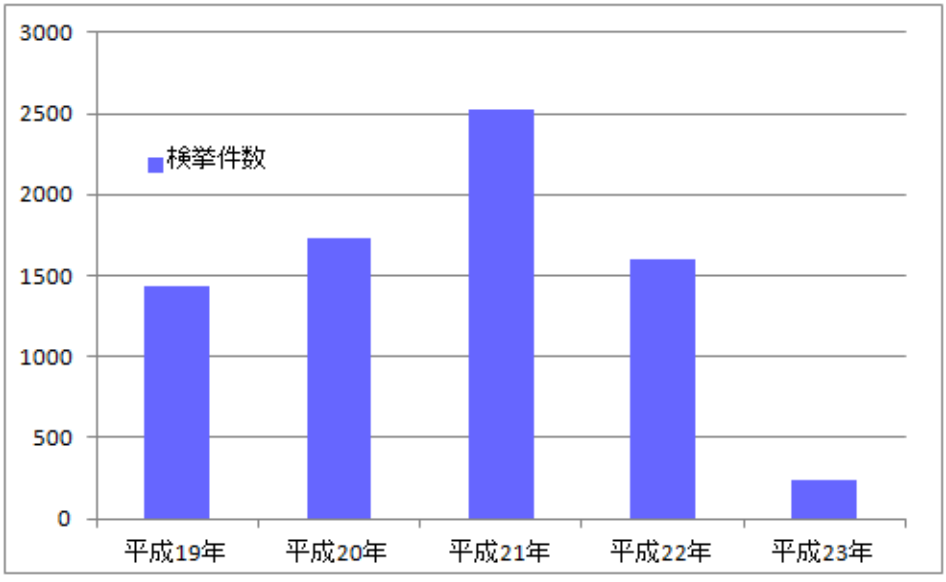


図 1-2　識別符号窃用（ID 窃盗）型不正アクセス行為の検挙件数[1]

[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/h23/pdf041.pdf よりフィッシング対策協議会が作成

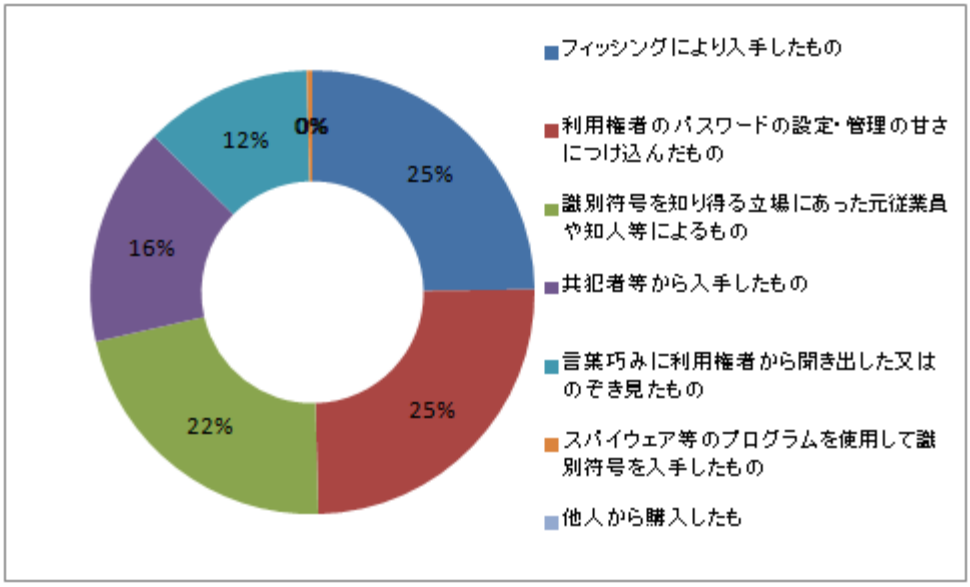


図 1-3　不正アクセス行為に係る犯行の手口の内訳[2]

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が、2009 年末から 2010 年前半にかけてフィッシングの報告が急増した。2011 年度は、5 月に多くのフィッシングサイトが見つかったが、全体的には、見つかる月に波があるものの、コンスタントにフィッシングの報告が続いている。事業者はもとより、一般消費者おいても、フィッシングの脅威に対する正しい知識を普及させることが、被害の拡大の防止には欠かすことができない。

1.2. 海外の状況

米国で設立されたフィッシング対策問題に関する国際組織 APWG（Anti-Phishing Working Group）の調査によれば、2010 年 7 月から 2011 年 6 月までのフィッシング情報の届出件数において、2011 年 3 月にフィッシングサイト件数が大きく増加はしているものの全体としては横ばい傾向にある。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/h23/pdf041.pdf よりフィッシング対策協議会が作成

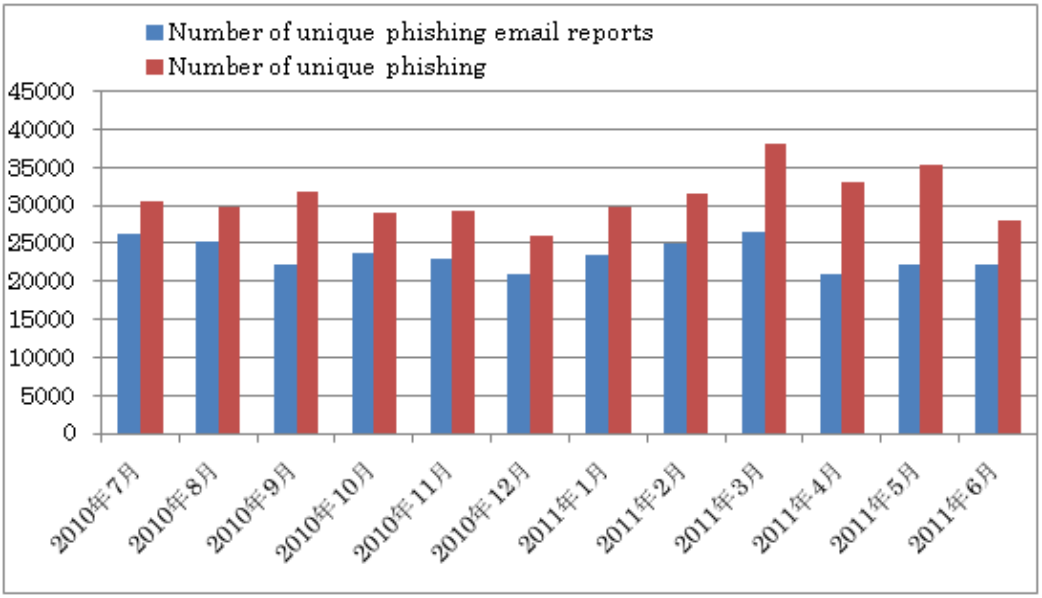


図 1-4　APWG への届出件数等[3]

[3] APWG (Anti-Phishing Working Group), "Phishing 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. 新たな脅威の動向

フィッシングとは、つまるところ、ID 窃盗を行うための手法の一つである。フィッシング対策協議会では、従来型のフィッシングに留まらず、様々な ID 窃盗の手法について動向把握につとめている。そのような活動を通して、フィッシング対策協議会が 2011 年でも脅威となる事例として「銀行の第二認証情報を詐取するフィッシング」と「Zeus - Banking Trojan」の 2 つを取り上げた。以下にそれぞれについて解説を行う。

2.1. 銀行の第二認証情報を詐取するフィッシング

(1) 概要

金融機関をかたるフィッシングは、以前より確認されていたが、2011 年 7 月末に国内の金融機関をかたり、乱数表や第二暗証番号などの第二認証情報を詐取するフィッシングが見つかった。この第二認証情報を詐取する方法は、従来からあるフィッシングサイトへ誘導する方法とは異なる、新たな手法が使われていた。それは実行ファイル(Exe ファイル)を使用した手法である。これは、電子メールに実行ファイル(Exe ファイル)が添付されており、受け取った人が、そのファイルを開くと、プログラムが起動し、ログイン ID やパスワードとともに、第二認証情報の入力を促す画面が現れる。(図 2-1)

図 2-1　第二認証情報の入力を促す画面

誤って、ログイン ID やパスワード、乱数表を入力し、画面下にある「送信ボタン」を押すとフィッシャーが用意したサーバへデータが送信されてしまう。この実行ファイルは一見技術的に高度な手法に見えるかもしれないが、常に単純なプログラムでできている。またいくつか見つかった実行ファイルを確認したが、金融機関で正規に使われている乱数表と桁数が異なっていたり、別の銀行で使用した実行ファイルを流用したために、一部にロゴとは別の銀行名が記載されていた物もあった。

なお、従来からあるフィッシングサイトへ誘導するメールや html 形式で送られるタイプなどいくつか見つかっているが、実行ファイルが添付されたメール同様、第二認証情報を記入する欄が現れることを確認している。このような第二認証情報を詐取するフィッシングは複数の金融機関で確認されていたことから、協議会では被害拡大を防ぐ目的で注意喚起を発行し、一般消費者向けに注意を呼びかけた。

(2)　複数の融機関に対するフィッシングの推移

協議会に届けられたフィッシング報告を分析した結果、この第二認証情報を詐取するフィッシングは、概ね以下のような推移で複数の金融機関に対して行われていた事を確認している。(図 2-2)

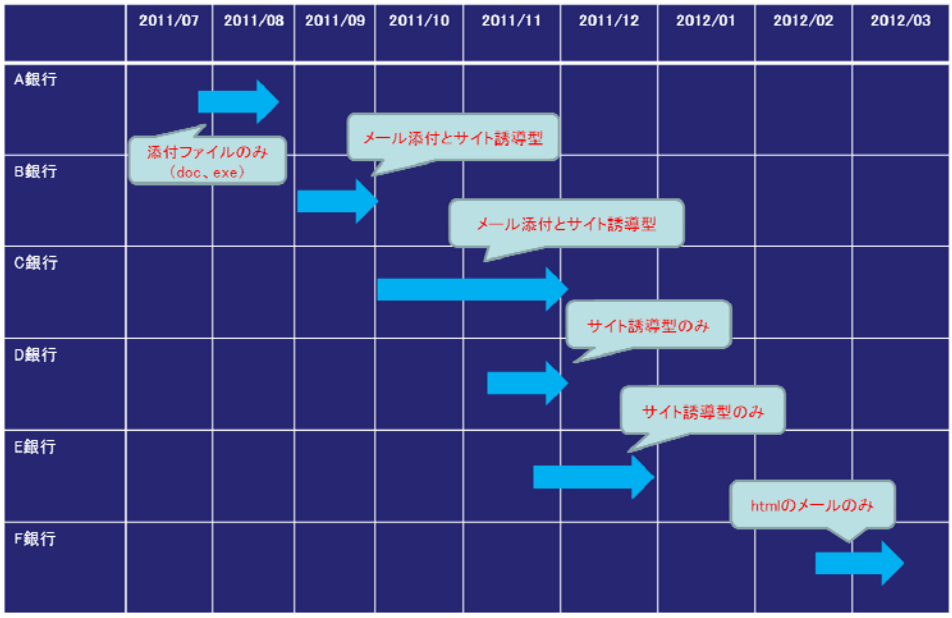


図 2-2　複数の金融機関に対するフィッシング

特徴としては、約１～２ヶ月の周期で、次々と別の金融機関へ推移すること、また、フィッシャーが使用するフィッシングサイトのドメインが「●●.com」や「●●.net」といったように、他の金融機関のフィッシングサイトで使用したドメインを転用する事例も確認している。さらに、フィッシングメールの本文に、稚拙な表現や漢字の誤記などが含まれることがあるのが特徴的である。

(3) 対策と課題

フィッシングサイトは、正規サイトの画像やロゴなどでコピーすることで簡単に作成可能のため、事前にフィッシングサイトが作成されることを防ぐのは難しい。その為、対策としては事後対策となる「フィッシングサイトが公開された場合にどう対応するか」といった事を中心に考える必要がある。具体的には、どのようにフィッシングに関する情報収集を行い、ユーザに対してどのように周知を行うか、またフィッシングサイトの停止を外部専門家へ依頼するか、などについて事前に検討しておくことで、迅速な対応が可能となり、結果としてユーザの被害低減が期待できる。
今回、第二認証情報を詐取するフィッシングでは、第一報の多くは、実際にフィッシングメールを受け取ったユーザから協議会に届けられたものであった。金融機関側でも、ユーザへの注意喚起や問い合わせ窓口は用意し、その存在を日頃から周知することが大切である。またその際に、可能であればユーザの手元に届いたフィッシングメールを元文のまま(本文や添付ファイルなど全て)手に入れる事ができるよう、ユーザに呼びかけることが望ましい。
また、フィッシングが発生している事をいち早くユーザへ伝えるためにも、twitter やニュース配信サイトなどへ情報を配信し、広く周知することが重要である。なお、第二認証情報を詐取するフィッシングは 2012 年 3 月現在も続いており、引き続き注意が必要である。

2.2. Zeus - Banking Trojan

(1) 概要

皆さんは、Zeus（ゼウス）と聞いて何が浮かび上がってくるでしょうか？
インターネットで検索してみると、ギリシア神話に登場する全知全能の神が多く上がってくるようです。その言葉の力強さにあやかった製品やサービスなども見受けられますが、コンピュータウイルス[4]に関連する言葉として紹介

[4] 厳密にはトロイの木馬はコンピュータウイルスとは区別されているが、目的が悪意のあるものが殆どなため、一般的にはコンピュータウイルスとして認知されている。

されている例が多くあります。検索結果の紹介文には、パソコンからの駆除方法や対策、官公庁や企業のコンピュータが被害を受けたというニュース記事まで、あまり良くないイメージで出ていることがわかります。そう、何を隠そうこの Zeus はコンピュータウイルスの一種である「トロイの木馬(Trojan)」として有名なのです。
トロイの木馬が有名になったのは、恐らく 2000 年頃にネットワークを経由してパソコンへ侵入するために仕掛けたバックドアタイプのものです。”タイプ”という言葉を使ったのは、トロイの木馬にはいくつか”タイプ”があるためです。

トロイの木馬のタイプ (例)

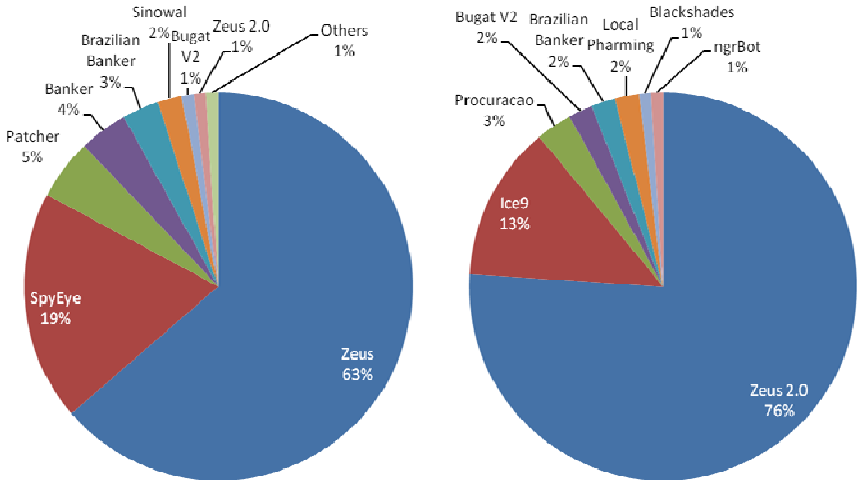
1	Banking Trojan	インターネット・バンキングなどで金融機関にアクセスするためのユーザ情報（主にユーザ名とパスワード）を盗み取るタイプ。
2	Data-Destruction Trojan	ユーザのパソコンに保管されたファイルを消去したり壊したりするタイプ。仕掛けた後にユーザを脅すなどする犯罪者の手口がある。
3	DDoS Trojan	犯罪者が他のコンピュータを攻撃するための踏み台としてユーザのパソコンを、利用するタイプ。
4	Downloader	サーバからファイルをユーザのパソコンにダウンロードさせるだけのタイプ。ダウンロードするファイルがウイルスなどの場合は問題になる。
5	Remote Access Trojans	ユーザのパソコンが、犯罪者によってコントロールされるタイプ。

なかでも「Banking Trojan」(バンキングトロージャン)は、フィッシング詐欺とならんで、昨今の金融機関が提供するオンラインサービスへの脅威となっています。Banking Trojan の行動は、インターネット・バンキングなどにアクセスするためのユーザ情報を犯罪者に送信したり、最先端のものでは消費者（ユーザ）によるオンラインバンキングの処理を横取りして、リアルタイムに犯罪者の意図する口座へ送金してしまうものまであります。普段はユーザのパソコンに潜んでおり、定期的に犯罪者が準備するアップデートサーバに密かにアクセスすることで、アンチウイルスソフトウェアに捕らえられるのを極力、防いでいます。
Banking Trojan にもいくつか種類がありますが、特に多いのはこの章のタイ

トルにもなっている Zeus です。Zeus は 2011 年にソースコードが公になったため、犯罪者が改良を加えた亜種が増加し、犯罪者が Zeus を利用するためのツールやサービスが次々と提供されるようになっていることがわかっています。

(2) 消費者（ユーザ）へ広がりと被害の状況

Banking Trojan には様々な種類があります。そのなかでも Zeus がそのトップシェアと考えられますが、2011 年から 2012 年初頭にかけて、そのシェアを拡大しつつあります。(図 1 の Ice9 Trojan も Zeus の派生版と考えられています)

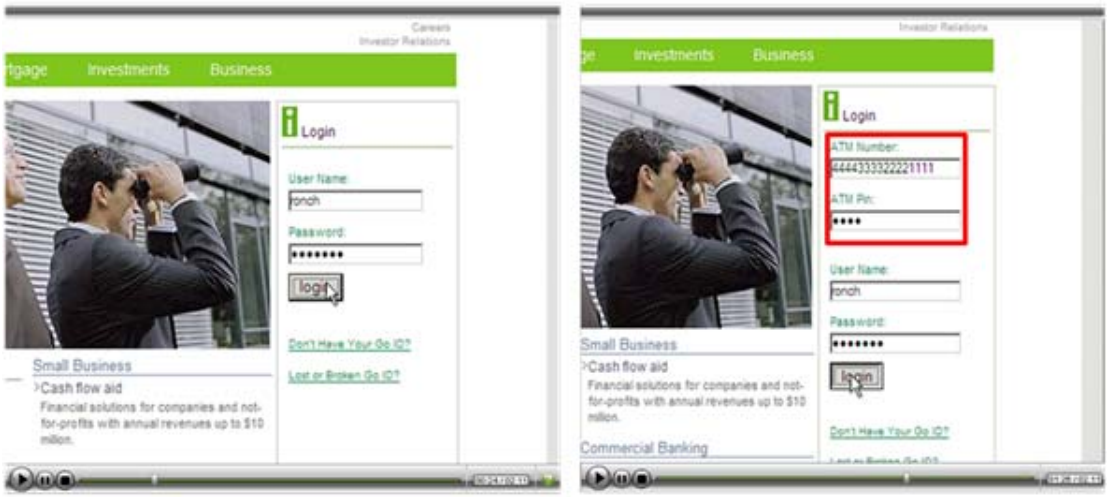


2011 年 第 1 四半期　　2011 年 第 4 四半期

Banking Trojan の種類比較

RSA Anti Fraud Command Center 提供

Zeus は HTML インジェクションと呼ばれる方法でユーザの目を欺くことを得意としており、本来インターネット・バンキング等では要求されていない項目（例:通帳番号や ATM の暗証番号）を画面上に表示して入力を促したり、画面表示そのものを変えたりすることができます。例えば、不正な宛先に送金しているにも関わらず、正常に処理が終了したように見せる画面を表示する等です。これによりユーザは、オンラインバンキングのウェブサイトが正しく表示していると勘違いさせられ、安心して情報を入力してしまい、被害が広がります。



HTML インジェクションにより ATM 番号と PIN(暗証番号)の入力を求める例（赤い四角内）

警察庁の発表[5]によれば、2011 年（3 月末以降 11 月 24 日まで）の不正プログラムによる犯行の被害は 54 金融機関の 136 口座で、約 2 億 8,200 万円に及ぶことがわかりました。一部の被疑者も逮捕されているようですが、全てが検挙されているわけではないようです。
金融庁や全国銀行協会等の関連団体では、銀行に対するより一層の注意喚起やセキュリティの向上を検討しているようです。また関係法令である不正アクセス禁止法の改定も 2012 年 2 月 21 に閣議決定されるなど、取り締まりの向上にむけた取り組みが各所で行われています。

(3) 対策と課題

ユーザの対策は、トロイの木馬を検知するためのセキュリティソフトウェア（一般的にはアンチウイルスソフトと呼ばれることが多い）がインストールされたパソコンを利用したり、信頼できないサイトからのファイルのダウンロードやそのプログラムの実行をしたりしないなど基本的なことが考えられます。しかし、犯罪者側もユーザを騙すためのテクニックや、セキュリティソフトウェアに発見されることを防ぐための機能を向上させているため、うっかり情報を入力してしまうミスを防ぐことや、ソフトウェアをタイムリーにアップデートさせられるかどうかが課題となります。
オンラインバンキングの画面で求められる入力項目がいつもと違う、あるいは過剰な情報要求だと思った場合は一旦アクセスを中断して、銀行のホーム

[5] 出典:インターネットバンキングに係る不正アクセス禁止法違反等事件の発生状況等について (2011.12.15 警察庁)http://www.npa.go.jp/cyber/warning/h23/111215_1.pdf

ページを確認したり、問い合わせるなど冷静な対処をする必要があるでしょう。

インターネット・バンキングなどのサービスを提供する企業は、トロイの木馬の発生をいち早く検知するためのサービスや取り組み、可変式パスワード導入などによるユーザ認証の強化、送金・振込処理の監視強化などがセキュリティ対策として求められます。
セキュリティ対策を講じた場合、ユーザの手間が増えることもあります。利便性を損なわない対策の導入とのトレードオフを模索することが課題となります。

[本稿執筆担当：水村明博（EMC ジャパン株式会社 RSA 事業本部）]

3. 総合的対策の確立に向けた課題

3.1. 技術的対策

(1) フィッシング URL 共有

・背景

一般社団法人 JPCERT コーディネーションセンター（以下、JPCERT/CC）が発表しているインシデントレポートによると、2010 年 1 月から 12 月までの期間に受け付けた、国内のブランドを装ったフィッシングサイトに関する報告件数が増加している。これは国内の金融機関や SNS、オンラインゲームなど様々な業種のフィッシングが数多く報告されているためである。報告された事例では、設置されるコンテンツや手口が類似していることから、なんらかの攻撃ツールが広く流通している可能性があるほか、最近では、スマートフォン利用者を狙った新たな手口も確認されている。

JPCERT/CC では報告を受けたフィッシングについて、ISP 等にフィッシングサイト停止の依頼をおこなっている。サイトの停止については ISP やその他の関係者の協力により、停止に繋がる場合が多いが、停止まで長い期間を要する場合も存在するのが現状である。

JPCERT/CC の 2011 年度フィッシング稼働状況によると、フィッシング報告を受領をしてからサイトの停止を確認するまで 1 日で約 70%が停止し、3 日で約 90%のフィッシングサイトが停止することがわかる。（図１）

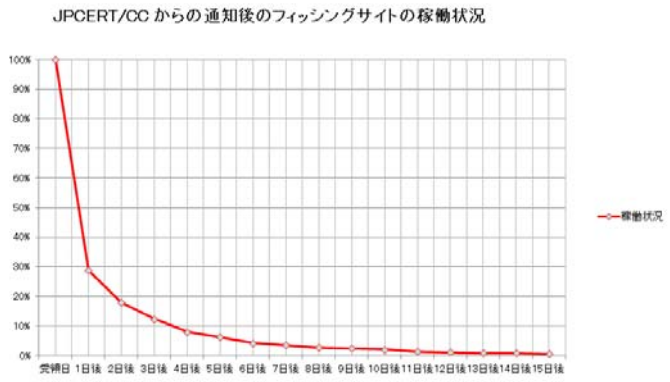


図１：フィッシング稼働状況

しかしながら、裏を返せば 3 日以上稼働しているフィッシングサイトが 10%程度あることも言える。このフィッシングサイトが稼働している間にユーザが誤ってアクセスした場合に、フィッシングサイトにアクセスさせない

よう消費者を保護する取り組みの一つにフィッシング URL 共有がある。
　フィッシング URL 共有とは、フィッシング検出機能を備えているアプリケーション（ウェブブラウザやウイルス対策ソフト）へフィッシングサイト URL を実装（ブラックリストへの登録など）することで、フィッシング機能を有したアプリケーションはブラックリストをもとにアクセスの遮断判定を行う。主要なウェブブラウザはこのフィッシング検出機能が備えられており、ユーザが誤ってフィッシングサイトにアクセスした場合にはブラックリストを参照し、そのフィッシングサイトの URL が登録されていればアクセスを遮断したあとに警告メッセージを表示させる。（図２）

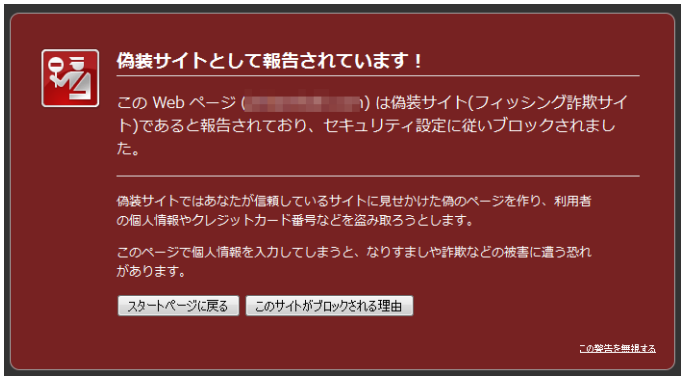


図２：フィッシング検出機能（例：Firefox）

・フィッシング対策協議会の取り組み

　協議会では、2010 年 2 月からフィッシング対策機能を有している製品を開発している会員企業などに対して、消費者から協議会に報告いただいたフィッシングの URL を共有する取り組みを始めている。このような取り組みを拡大し、ブラウザベンダや大手セキュリティソフトベンダとの連携を強化することが消費者保護の観点から推進すべき課題の１つと考えられる。

3.2. 国際的な取り組み

(1) STOP THINK CONNECT

米国 APWG (Anti-Phishing Working Group) と NCSA (National Cyber Security Alliance) などがリードするインターネットを安全に利用するための啓発キャンペーンに「STOP.THINK.CONNECT[6]」がある。

・「STOP」
メッセージ: インターネットは便利であるが、一般社会と同様、そこには危険もあります。どのような危険があるかを知り、解決策をどのように見つけるかについて、一旦、立ち止まって調べましょう。

・「THINK」
メッセージ:フィッシング詐欺にひっかからないためには、様々な警告の見極め方を知る必要があります。警告を確認したら、これから取ろうとする行動がコンピュータやあなた自身の安全を脅かさないか考えましょう。

・「CONNECT」
メッセージ:危険を理解し、十分な対策をとれば、インターネットをより信頼できるようになるでしょう。

これらのシンプルな啓発メッセージをキャンペーンに参加する複数の企業や組織が、組織の壁を越えて同じメッセージを繰り返し消費者に伝えることで、いままで各社によって表現がまちまちであったセキュリティ啓発メッセージが統一され、より消費者に理解されやすいものとなることが期待されている。この国際的な啓発キャンペーンに参加するべく、フィッシング対策協議会では国際連携 WG を設立し、STOP THINK CONNECT の日本展開について検討している。

6 http://stopthinkconnect.org/

3.3. まとめ

2011 年度を通してフィッシングサイトの件数は、横ばい傾向にあるが、国内の金融機関を騙ったフィッシングサイトや SNS サイトを騙るフィッシングサイトが多く見つかっている。第二認証情報を詐取するフィッシングでは、フィッシングサイトに誘導させる手法以外に、メールに実行ファイルを添付し、その実行ファイルを開くと、ログイン ID やパスワードとともに第二認証情報の入力を促すタイプの新たな手法が使用されていた。また、オンラインゲームやプロバイダのウェブメールなど国内ブランドを騙ったフィッシングサイトも引き続き見つかっている。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。新たな手法や国内ブランドが狙われていることから、昨年度公開した一般消費者保護を主軸とした、消費者向けガイドラインの改訂が必要と考えている。

（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(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】

白石 知宏	アグスネット株式会社
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
水村 明博	EMC ジャパン株式会社
宮本 和明	株式会社 HDE
柿沼 靖雄	エヌ・ティ・ティ・コムウェア株式会社
永塚 淳	エヌ・ティ・ティ・コムウェア株式会社
前田 典彦	株式会社 Kaspersky Labs Japan
石丸 傑	株式会社 Kaspersky Labs Japan
佐藤 克洋	株式会社カービュー
橋本 小月	株式会社カービュー
松本 義和	サイバートラスト株式会社
谷田部 茂	シスコシステムズ合同会社
石田 公孝	有限会社ストーンズインターナショナル
伊東 達彦	一般社団法人全国銀行協会
加藤 孝浩	トッパン・フォームズ株式会社
林 憲明	トレンドマイクロ株式会社
岡本 勝之	トレンドマイクロ株式会社
秋山 卓司	一般社団法人日本電子認証協議会
國米 仁	株式会社ニーモニックセキュリティ
高橋 大洋	ネットスター株式会社
長谷部 一泰	ネットスター株式会社
丹京 真一	株式会社日立システムズ
望月 貴仁	ヤフー株式会社
戸田 薫	ヤフー株式会社
宇佐見 洋志	ヤフー株式会社

【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】

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