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 2011

― 新たな脅威の動向とそれに向けた対策と課題 ―

平成 23 年 5 月

フィッシング対策協議会

技術・制度検討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急増している（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 2011 年 2 月までで、既に対前年度で約 33%増（2009 年度 283 件から、2010 年度 375 件）となっている。また、フィッシングサイトの件数は、対前年度で約 86%増（2009 年度 260 件から、2010 年度 485 件）となり、届出件数以上の増加となっている。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、2010 年度は対前年度で 139%増加（2009 年度 46 件から、2010 年度 110 件）している。これは 2009 年度は有名なサイト、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、2010 年度はフィッシングの対象となるブランド数が増えつつあることを示しており、注意を要する。

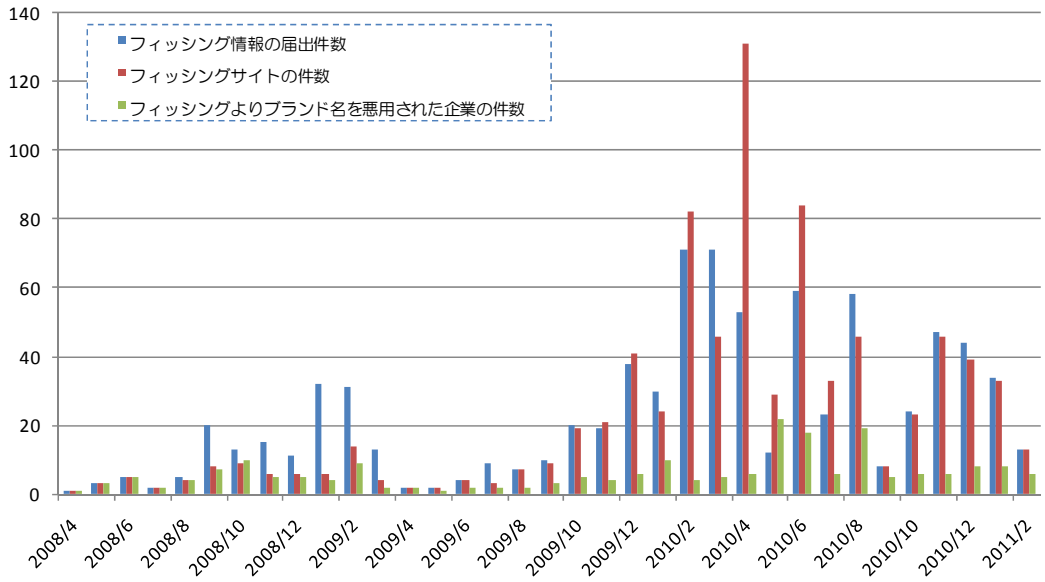


図 1-1　フィッシング対策協議会への届出件数等

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が引き続き高い水準にある（図 1-2）。また、その手口を見ると、平成 22 年はフィッシングが大半（88％）となっている（図 1-3）。

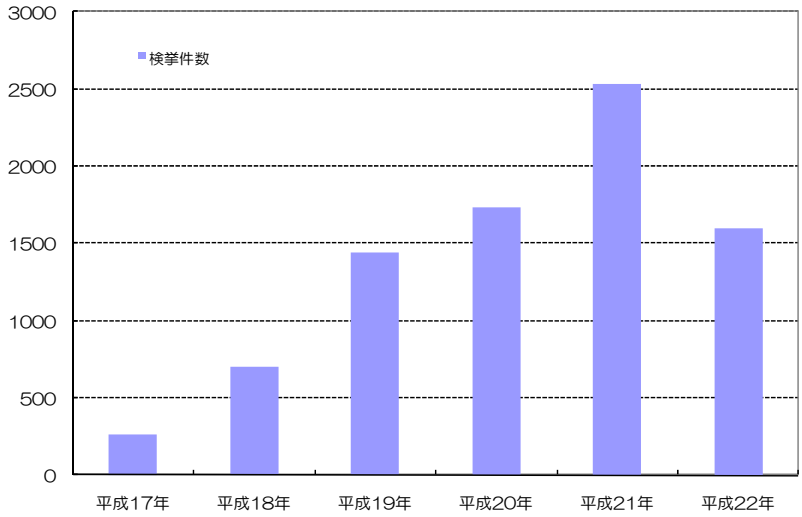


図 1-2　識別符号窃用（ID 窃盗）型不正アクセス行為の検挙件数[1]

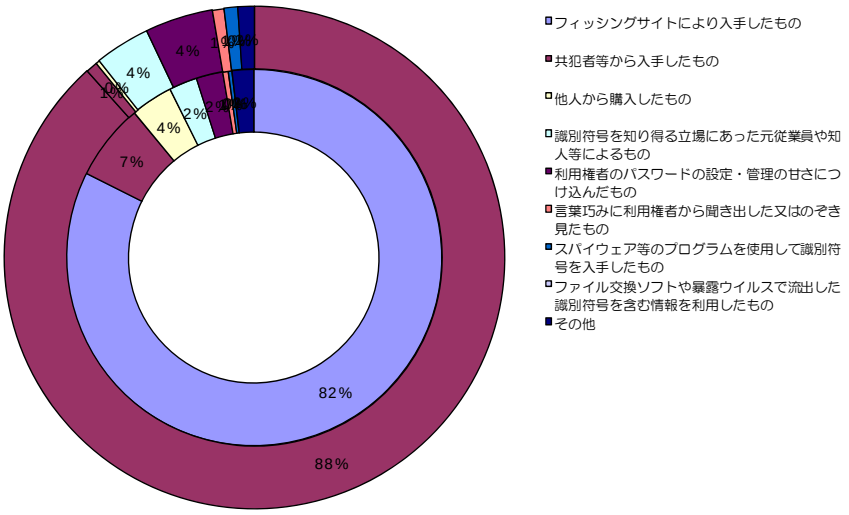


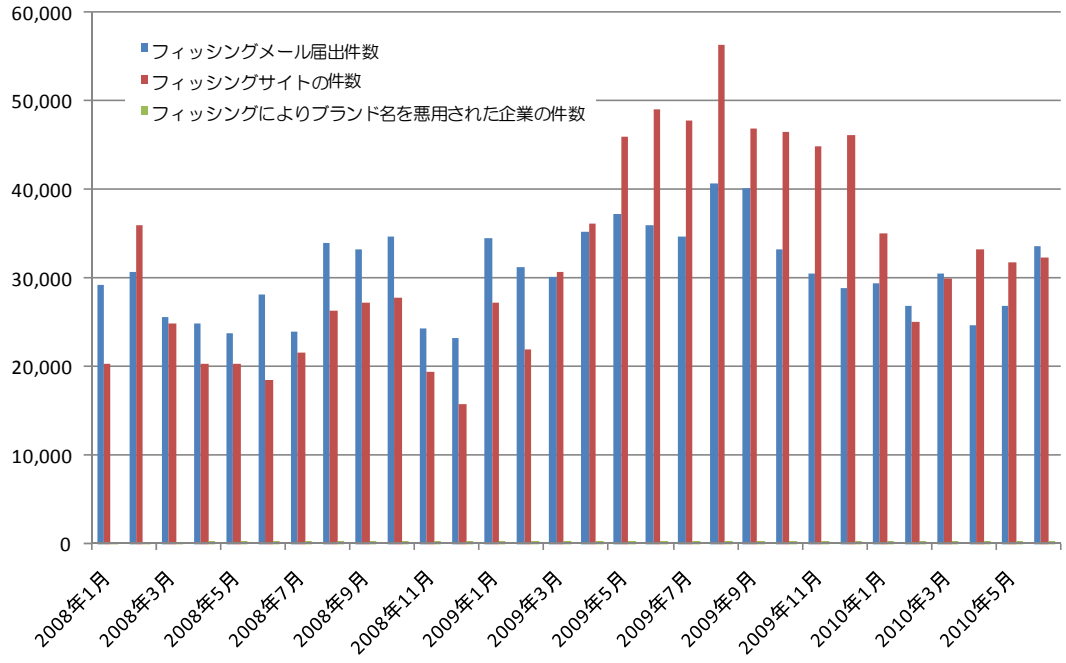
図 1-3　不正アクセス行為に係る犯行の手口の内訳[2]

[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」, http://www.meti.go.jp/press/20110303004/20110303004.pdf 等、より株式会社三菱総合研究所が作成
[2] 同上

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。2010 年度末にかけて緩やかに減少してきてはいるものの、引き続きコンスタントに被害が報告されている。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、2009 年のフィッシング情報の届出件数は前年比約 23%増、同フィッシングサイトの件数は約 80%増であるなど、引き続き脅威が高まりつつける状況にある。2010 年については、半年分しか数値が公表されていないため正確な比較は不可能であるが、2009 年に比べて、届け出件数・サイト件数については減少、ブランドを悪用された企業数は横ばいの傾向にある。



2. 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、より株式会社三菱総合研究所が作成

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 年に重要性が増すと考える新たな課題として「モバイルフィッシング」と「短縮 URL」の 2 つがあげられる。以下にそれぞれについて解説を行う。

2.1. モバイルフィッシング

(1) 概要

日本では、携帯電話を通じてメールや Web を利用することが諸外国と比較して多いとされている(*1)。特に近年は、Android 搭載端末・iPhone の登場により、スマートフォンの出荷台数が急激に伸び、2010 年度の出荷台数は 675 万台、前年比約 2.9 倍のペースで増えている(*2)。

(*1)http://pewglobal.org/files/2010/12/Pew-Global-Attitudes-Technology-Report-FINAL-December-15-2010.pdf “Cell Phones, Internet Usage”

(*2)㈱MM総研調べ(10 年 12 月時点)

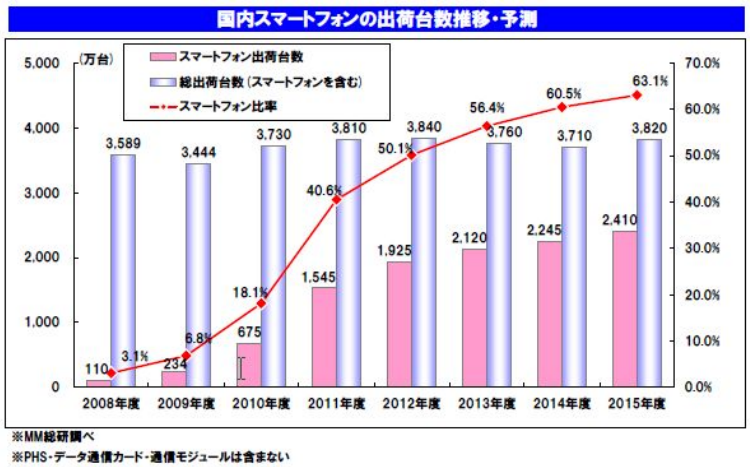


図 2-1　国内スマートフォンの出荷台数推移・予測

急激な利用拡大にもかかわらず、脅威への対処は十分ではない。携帯/スマートフォンの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(*3)、入力インターフェースの関係で携帯向け Web サービスでは

パスワードのセキュリティレベルが低いこともある(*4)。また、ユーザも若年層が多いためセキュリティ意識も低めである。フィッシングサイトも出現しており、すでに隠れた被害者が増え始めていることが推測される。

重ねて、モバイル端末のトレンドが携帯からスマートフォンへ推移したことで、「OS そのものの脆弱性をつく攻撃」や「ダウンロードアプリを利用したマルウェア」といった新たな脅威も出現している。実際にアプリによる被害報告も出始めており、今後のフィッシング被害の中心となってくることが予想される。

なお、これらの脅威への対策についても全く進んでいないわけではなく、携帯キャリア自身のみならず、サードパーティーによる対策ソリューションが登場しつつある。今後も様々な対策ソリューションが登場すると思われ、注目が必要である。

(*3)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、ブラウザ画面が小さい/URL が表示されない/証明書の表示が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

(*4)サイトのパスワードも入力を簡単にするため、文字数が少なかったり、数字だけの場合も多い

(2) 被害の状況

以下のようなサイト・アプリが登場しており、実際の被害が出始めていると推測される。

（フィッシングサイト）

フィッシング対策協議会では 2009 年 12 月下旬より、「モバゲータウン」など 4 ブランドの携帯サイトを装ったフィッシングを確認している。ユーザにキャンペーン応募などのリンクをクリックするよう促す。正規のサイトからのメールと混同したユーザがクリックすることでメールアドレスが攻撃者に知られてしまう。（図 2-2）

（フィッシングアプリ）

Android 上で動作するアプリケーションでは、2010 年 1 月 Android Market（Google 社が運営するアプリケーション配信サイト）で、オンラインバンキングアプリケーションに見せかけてパスワードなどの情報を盗み出す不正なアプリケーションが販売されていたことを F-Secure が発見した。問題のアプリケーションは、09Droid という匿名の開発者の名前で Android

Market に登録され、50 以上の金融機関名を騙り、オンラインバンキングの Web インターフェースを表示するだけで実際の取引には利用できず、ユーザ名やパスワードなどの情報が盗み出された可能性があるという。（図 2-3）（マルウェアアプリ）

Android Market 上でマルウェアも報告されている。2010 年 8 月に F-Secure が発見した「Tap Snake」や、Kaspersky labs が発見した「Movie Player」等である。「Tap Snake」は、一見するとゲームアプリケーションであるが、起動すると定期的に位置情報を作成者に送信する。ゲームを終了しても、バックグランドで動作し、位置情報を送信し続ける。「Movie Player」は起動すると、有料情報提供サービス（プレミアム SMS）に SMS が送信され、ユーザには利用料が課金されてしまう。

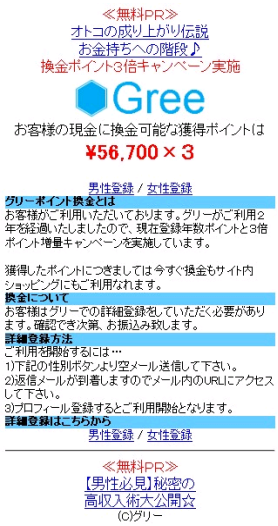


図 2-2　GREE を騙る、フィッシングサイサイト

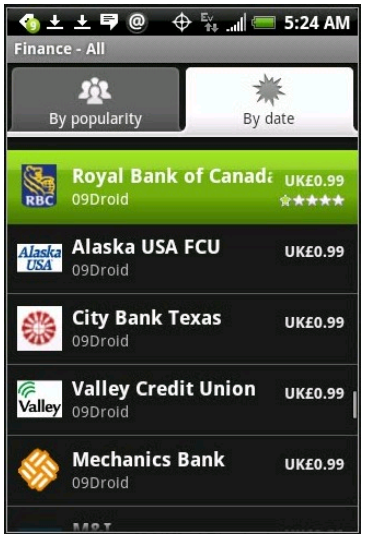


図 2-3「09Droid」が開発者したアプリケーション

なお、KDDI 研究所が 2010 年 7 月に Android Market から無作為に 646 個アプリケーションを調査したところ、約 17.2%のアプリケーションが電話番号や端末識別番号(IMEI)を、約 15.2%のアプリケーションが位置情報を、約 11.6%のアプリケーションが電話帳やアドレス帳を読み出す可能性があったと報告している。（図 2-4）

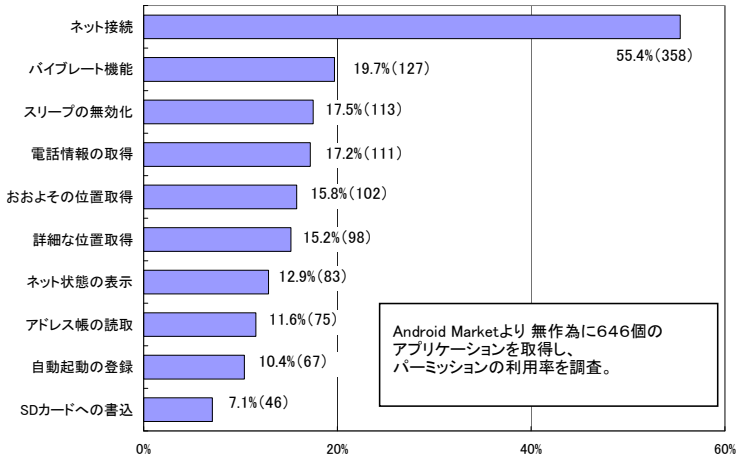


図 2-4　アプリケーションの利用パーミッション調査（KDDI 研究所）

(3)　対策と課題

各分野において、以下のような対策および課題が考えられる。

（Web）

フィッシング対策として Web 上で個人情報を入力する際に確認すべき事項は、携帯/スマートフォンであっても、PC と同じである。メールの送信元、アクセスする URL（端末により違いがあるがポップアップで確認できる場合も多い）、証明書の表示などは最低限確認する必要がある。なお、端末によっては、各情報の確認手順が面倒であったり、場合によっては情報が確認できないケースもあり、端末の製造元と連携して解決する必要のある課題である。

（メール）

キャリアが提供する迷惑メール対策の利用を推奨する。なお、モバイル端末でメールを確認する際には S/MIME などの電子署名が施されていても検証が行えない場合があることは、今後の課題である。

（Android）

開発が容易（オープン性）で配布も自由である Android は攻撃者にとって、より効率的な端末である。使用者が多いことは、比例して被害にあるユーザが多いことを意味する。セキュリティの意識が低いまま利用すると、被害に直結しかねないという認識を持つ必要がある。

（各ベンダーによる対策ソリューション）

Android 向けセキュリティソフトの開発も各ベンダーにより進められている。入手可能なソリューションについては適宜検討をすべきである。

（キャリアの対策ソリューション）

各キャリアが提供しているAndroid向けのセキュリティサービスを利用するのもよい。NTT ドコモでは、メールウィルスチェック、SP モードフィルタ（URL フィルタリング）を、ソフトバンクモバイルでは、スマートフォン基本パック（アプリケーション、受信メールの添付ファイル等のウィルスチェック等）を提供している。

（アプリの利用）

アプリケーションを利用する際は、AppleStore、ドコモマーケット（NTT ドコモが動作確認したアプリケーションを掲載）、au one Market（KDDI がセキュリティ検査を実施したアプリケーションにマークを付けるサービス）などできるだけ信頼できる所から入手することが賢明である。

（OS）

OS の脆弱性を付く攻撃も予想される。スマートフォンでは、OS のアップデートはユーザ自身で行う必要がある。ただし、種類によってはアップデート作業が繁雑であり、リテラシーの高くないユーザにとって敷居が高いケースがあることは課題である。

[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）宮本和明（株式会社 HDE）]

2.2. 短縮 URL

(1) 概要

メディアを大きく賑わせている北アフリカや中東での政変に Facebook が大きな影響を与えているという報道を目にした方も多いと思われる。Facebook は現在世界規模で急速に利用が拡大しており、登録者数は 6 億人にも及ぶという。しかし、新しい情報メディアの台頭は、新たなフィッシング脅威にもつながっている。今回は、Facebook や Twitter に代表されるソーシャル･ネットワークで使われている短縮 URL を利用したフィッシング詐欺について紹介する。

そもそも、短縮 URL とは、字数制限がある中に長い URL を埋め込むために工夫されたサービスである。例えば Twitter の場合、一回の投稿は 140 文字までという制限があるが、その中で 100 文字近くを URL が占めてしまうと書きたいことが書けない。そこで、リンク先の URL を 20 文字程度に変換したものが、短縮 URL である。こうすることで、投稿者は URL の文字数を気にせず、記事の中で外部サイトを参照することができる。

(2) 被害の状況

2009 年ごろから、人気のブランドを騙ってフィッシングサイトに誘導する短縮 URL を埋め込んだ記事を投稿する、新手のフィッシング攻撃が登場している。昨年 8 月の米国での報道によると、マクドナルド社を騙ったある記事の中のフィッシングサイトへのリンクをクリックしたユーザはおよそ 32,000 人にも上り、その半数近くはアクセス先がフィッシングサイトであることに気づきもしなかったという。

(3) 対策と課題

アクセスする前にアクセス先の URL、とりわけドメインを確認する、というのは、フィッシング詐欺に遭わないための、いわば「いろはの”い”」である。この基本を手軽に守ることができるように、最近のブラウザソフトの多くは、アクセスしたサイトの危険度を視覚化する機能が用意されている。セキュリティソフトも、アクセスしようとした URL がブラックリストに含まれていると警告を表示する（レピュテーション機能）。こうした業界を挙げた対応が一定の成果を挙げ、外見だけを似せた、ドメイン名などはまるで異なるフィッシングサイトに単純に誘導しようとするフィッシング攻撃の成功率は下がってきていると考えられる。

しかし、短縮 URL に変換されてしまうと、すべての URL はどれも http://bit.ly のような同じドメインで始まり、それに続く文字列も変換されてしまう。つまり、URL を見ただけでは、リンク先が不審なサイトかどうか見分けがつかなくなってしまう。悪意を持ったサイトへのリンクの遮断をシステム的に行うのを困難にしている理由は、他にもある。Twitter によく見られるブラウザ以外の専用クライアントソフトを使っていると、ブラウザソフトのために用意された既存のフィッシング対策のセキュリティ機能は働かない。

さらに、多くのユーザがソーシャル･ネットワーク･サイトへのアクセスに利用している携帯電話、とりわけスマートフォンでは、リスクはさらに高まる。スマートフォンは、PC とほとんど同じことができるにもかかわらず、PC のようにはセキュリティ対策が充実していない。ブラウザには、アクセス先のレピュテーション機能も含まれておらず、トロイの木馬などへの感染を防ぐためのセキュリティソフトも実績が少なく、効果は未知数の部分も残されている。セキュリティソフトを導入していないスマートフォンユーザもまだ少ないと思われる。このように、脆弱性を残した中で、利用者が急増しているスマートフォンは、サイバー犯罪者たちにとって、格好の標的である。

事業者側でも、短縮URLの内包する潜在的なリスクについて理解しており、すでに対策が講じられている。短縮 URL サービスを提供しているTineyURL.com では、実際にアクセスする前にアクセス先の内容を確認するためのプレビュー機能を提供している。Twitter も、2010 年 4 月から、Twitter 経由のリンク先に不正サイトがないか、同社の信頼安全性部門が監視するという、新しいフィッシング対策機能を開始している。短縮対象が Twitter に限定されたり、利用環境が IE や Firefox に限定されたりといった制限があるが、短縮URLを送ると危険度を判定してくれるサービスもいくつか始まっている。とはいえ、こうした対策だけで、ユーザが何の不安もなく短縮 URL をクリックできるかといえば、そうもいかない。

そうなると、ユーザには、本当に信頼できるサイト以外アクセスしないといった慎重さが求められるわけであるが、サイバー犯罪者たちは、逆にユーザが思わずアクセスしたくなるような餌を周到に用意してきている。例えば、冒頭で取り上げた中東情勢なども巧妙に利用される恐れがある。2008 年の年末に、イスラエルで政府とハマスの武力衝突が発生した際、一部のサイバー犯罪者たちは驚くほど迅速な対応を見せた。短時間のうちに CNN.com を巧妙に模したフィッシングサイトから動画再生ソフトを騙ったトロイの木馬を配布する準備を整え、そこに誘導するための大量のスパムメールを大量に配布した。当時はメールが使われたが、もしも今日 Facebook などのソーシャル･ネットワークを使って、こうした攻撃が行われれば、被害は格段に増える恐れがある。それは、人々は一般にソーシャル･ネットワークの中の情報を他の情報以上に信じやすい傾向にあるためである。

ソーシャル･ネットワークの情報の多くは、自ら選択してつながった相手からもたらされることを考えると、無理からぬ部分もあるかもしれない。サイバー攻撃の脅威は、トロイの木馬の攻撃力や感染力だけではなく、サイバー犯罪者たちのソーシャル・エンジニアリングを駆使する力やスピード感とも大いに関係してくる。彼らは、攻撃をしかける準備を日頃から周到に行っていて、市民の関心あるいは不安につながる世界の重要な関心事に素早く反応する。今この瞬間も、リビア情勢やニュージーランドの地震など、多くの人が関心を持ちそうなニュースに短縮 URL を組み合わせたフィッシング攻撃が続々と発生していても、何の不思議もない。

より容易に短縮 URL の参照先の安全性を確認できる仕組みなど、関連ソフトウェアにおけるソーシャル･ネットワーク･サービス対応の充実が待たれるところであるが、ユーザが常に脅威を頭の片隅において慎重に行動することを忘れない必要がある。

[本稿執筆担当：水村 明博（EMC ジャパン RSA 事業本部）]

3. 総合的対策の確立に向けた課題

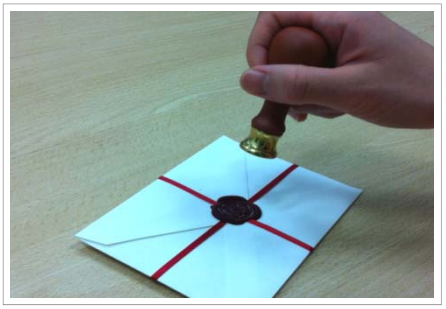
3.1. 技術的対策

(1) DKIM

・電子メールにおけるフィッシング詐欺対策

依然として電子メールがフィッシング詐欺の主な入り口となっている。この理由の一つとして、電子メールの差出人が容易に詐称されてしまう事があげられるが、この課題に対しては比較的古くから対策が取られてきた。

技術的対策のアイデアは、中世ヨーロッパで行われていたサイン入りの手紙をロウで封緘し、差出人を示すスタンプを押す事で身元の詐称および途中の改竄を防いだ事をコンピューターに代行させたもの、と考えると理解しやすい。



電子メールに対してデジタル署名（サイン）を入れ、それを受取人が確認する事で差出人の詐称を防ぐという対策は、Cisco Systems が中心となって進められた。これは IIM（Identified Internet Mail の略）と呼ばれる。これとは別に、Yahoo!が中心となって進められた DomainKeys では、電子メール本文とドメイン情報を一括したデジタル署名（封緘とスタンプ）を確認し、身元の詐称を防ぐものである。

これらの技術はフィッシング詐欺対策として取られてきた側面が大きいが、迷惑メール対策としても応用が可能である。現在、これら２つの技術の長所は DKIM（ディーキム：DomainKeys Identified Mail の略）と呼ばれる技術に統合されている。

・DKIM の課題

2010 年 11 月「Japan DKIM Working Group (略称; dkim.jp)」が設立され送信・受信双方の事業者による本格的な DKIM 普及活動が始まったが、DomainKeys や SPF（Sender Policy Framework の略）など先行する送信ドメイン認証技術に比べ、普及の度合いには依然大きな開きがある。

DKIM は DomainKeys とよく似ているが、より詳細な情報を使ってデジタル署名を作成することが可能であり、より進歩したデジタル署名の検証ポリ

シーを使用することができる。しかし、これらが原因となって DKIM 導入を複雑・難解と感じさせる面があるかもしれない。

だが、フィッシング詐欺を目的とした電子メールの「なりすまし」が巧妙化している中、それを見破るための最新技術である DKIM の導入は、電子商取引をはじめとするビジネス環境の信頼性確保のために必須であろう。

これらを踏まえ、DKIM 普及への課題とは、

- □ 電子メール送信側、受信側、双方の取り組み
- □ DKIM 導入の容易さの改善
- □ DKIM 導入メリットの訴求

であると言える。

[本稿執筆担当：宇佐見 洋志（ヤフー株式会社）、加藤 孝浩（トッパン・フォームズ株式会社）]

3.2. 制度的課題

(1) 教育制度

本項では、フィッシング詐欺に対する教育制度の現状について報告する。文部科学省は 2003 年、高校過程の必修教科として「情報」3 科目（情報 A、情報 B、情報 C）を新設し、以来「教育制度」としての情報教育に対する関する関心が高まっている。

また、フィッシング詐欺が契約に関する詐欺行為の一形態であるとするならば、「社会」や「家庭」の科目において行われている消費者教育についても留意すべき教育制度であろう。

ここでは、文部科学省の「高等学校学習指導要領　第 10 節　情報」から教育制度の現状について考察する。これによれば、同学習指導要領においてフィッシング詐欺の学習について明示な規定はされていないものの、「情報化の進展と社会への影響」の項目が挙げられており、情報化が社会に及ぼす影響を、情報通信ネットワークなどを活用して調べたり、討議したりする学習を取り入れるよう示唆されている。

実際に学校教員が授業カリキュラムを作成する際には、各教科書出版社が提供する「教科書対応関連リンク集」などが大きな影響を与えることになるであろう。そこで、出版社 7 社（実教出版、開隆堂、教育出版、啓林館、数研出版、第一学習社、日本文教出版）が掲載する情報について分析を行っている。

各社が記載するセキュリティに関する事項としては、主にコンピュータを利用する上で必要なモラルやマナー、コンピュータウィルス対策、パスワー

ドの管理などがあげられる。特にコンピュータウイルス対策については授業運営に必要と思われる参考情報の入手がしやすい環境下にあると考える。しかしながら、これらのセキュリティ項目はフィッシング詐欺と大きく関係するところではあるが、直接的に「フィッシング」の用語を用いてその脅威について学習の必要性を記述している情報は確認するに至っていない。また、「フィッシング対策協議会」サイトの紹介など本協議会の取り組みについて紹介している状況を確認するに至らなかった。

学校教員は消費者教育において、都道府県、市からの支援を受けらことも可能であろう。教科書副教材として活用可能な教育資料（パンフレット）の配布は多くの都道府県において行われており、そのほとんどがデジタルデータとしてダウンロード可能な状態で提供されている。

また、教科の授業以外でも、通信会社、消費生活センターなどの外部専門家を招いた講演に関する実施機会が設けられており、消費者リテラシーを高める教育制度が提供されていると考える。

しかしながら、これら消費者教育においてフィッシング詐欺についてどのように取り扱いが行われており、十分な教育がなされているか否かについては判断することができない。

フィッシング詐欺においては、すでに広く知られているサイバー犯罪手法のみならず、より巧妙化した手口が複雑に関連し、一つの犯罪行為が成立している。こうした現状を広く知らせるのにまだ十分でない面もあり、今後も、学校をはじめとする教育の場において本協議会をはじめとするフィッシング詐欺対策に関する取組を積極的に展開していくとともに、教職員/保護者等を対象とした研修会なども様々な場で開催されるよう、啓発に努めていく必要があると考える。

これらを踏まえ、フィッシング対策協議会が抱える教育制度に関する課題とは、

- □ 本協議会の実施する取り組みに対するさらなる周知
- □ 被害状況を踏まえた学習指導要領に対する提言
- □ 教育制度を支援するサポート体制の提供

であると言える。

[本稿執筆担当：林 憲明（トレンドマイクロ株式会社）]

以上

3.3. まとめ

2010 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、昨年同様、クレジットカード会社を騙ったフィッシングサイトが多く見つかっている。また、オンラインゲームや携帯ゲーム、震災に乗じた日本赤十字社など国内ブランドを騙ったフィッシングサイトも見つかっている。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、特に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策定が必要と考えている。

（空白）

フィッシング対策協議会　技術・制度検討ワーキンググループ
構成員名簿（改訂版）

（敬称略・順不同）

【主査】

内田 勝也	中央大学 研究開発機構

【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
遠藤 績穂	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	株式会社日立情報システムズ
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