「フィッシングの現状と対応」

渡辺弘美@JETRO/IPA NY

1. はじめに

米国では、2003 年ごろから「フィッシング（phishing）」と呼ばれるオンライン詐欺が流行している。

これは、実際に存在する企業からその企業の顧客向けに送られたように見せかけたメールを発信し、実在する企業とは別の偽のサイトへのアクセスを実行させ、クレジットカードの番号や、銀行口座の暗証番号などを、そのサイト上で入力させ、その情報を元に詐欺行為を行う犯罪である。

FTC（米連邦取引委員会）は、2003 年 7 月に初めてこの種の詐欺行為についての警告を発した。

また、対フィッシングの業界団体(APWG: Anti-Phishing Working Group)も組織されている。

フィッシングはメールを利用した行為ということで、スパムメールにとてもよく似ているとも言える。しかしスパムメール全てが詐欺ではないのに対し、フィッシングは当初より詐欺を目的にしていることが特徴で、この点ではいわゆる個人情報窃盗（ID セフト）のオンライン・メール版とも言える。

フィッシング「phishing」という言葉自体は割と最近のものだが、AOL、eBay、PayPal、Amazon などを巻き込んだいくつかの詐欺事件のおかげで広く知られつつある。

これは、クレジットカード番号や銀行口座の暗証番号など、金融機関にアクセスして操作するのに必要な個人情報を「釣りあげる（fishing）」ことと、言葉の上での掛け合わせとなっている。綴りが何故「f」ではなく、「ph」なのかは、「ユーザーを釣るための餌（メール）が『sophisticated』されている」」と解説されており、一般の辞書には載ってないようなインターネット上での特殊な隠語となっている。

また、語源には幾つか諸説があり、Phat(黒人のスラングで「いい女」を指す)や、Phish(ロックバンドの名前。Fish では商標やドメインが取りづらかったため、この表記を選んだと言われている）の語呂合わせという説もあるし、また「Password Harvesting Fishing」の略という説もある

なお、APWG では、1970 年代に電話のただ掛け装置を開発したハッカーの行為が「phreaking」として知られるようになったことから、一般的にハッカーは「f」を「ph」に置き換えるものであると説明している。

２．フィッシングの現状

(1) フィッシング被害の現状

Gartner 社が本年 5 月に発表した資料によると、推定 5700 万人の米国人がフィッシング詐欺のためのメールを受け取っており、2003 年の被害額は約 12 億ドルにのぼるという。この調査によると、3000 万人が「フィッシング攻撃を受けたことがある」と解答し、2700 万人が「それらしいものを見聞きした経験がある」という。このようなユーザーの 20%は、提示されているリンク先をクリックしており、更にその内の 3%がクレジットカード番号や、銀行口座の暗証番号などの重要な個人情報を、フィッシング用のサイト上で入力している。

フィッシングそのものは既に目新しいものではないが、最近大幅な増加を辿っており、同調査によると、フィッシングまたは同種のものと思われる行為の 3/4 以上は過去 6 カ月、16%は過去 7〜12 カ月に発生しているという。

また、APWG が本年 2 月に発表した資料によると、本年 1 月中だけでも 176 種類の新しいフィッシング・メールが報告されたという。また、APWG は本年 4 月中にユーザーから報告されたフィッシングに関する情報を集計して発表したが、それによると、新たに報告されたフィッシング詐欺は 1125 件。3 月中に報告された件数の約 3 倍になっている。

Tumbleweed Communications 社と APWG による調査によれば、本年 6 月のフィッシング攻撃は 1422 件であり、自動でスパム・メールを除去する機能を持つ ISP などに対抗するために、その 92%が送信元として偽りのメール・アドレスを使用していることが明らかになった。

通常、フィッシング行為は、最大 5%の成功率を達成しているという。

フィッシング攻撃サイトをもっとも多くホスティングしているのは米国で、全体の 1/4 以上を占める。フィッシング・サイトの平均寿命は 2 日強で、ハッキングした Web サーバーでフィッシング・サイトをホストしている割合は 25%であるという。

同調査では、1400 件の詐欺メールを分析した結果、メールの送信元認証技術が、不正のメールが受信箱に届くのを防ぎフィッシング攻撃の有効性を低下させるための重要なステップとなるという。

(2) フィッシングの手法

フィッシングの典型的な手順は以下の通りである。

まず、フィッシングを試みる人物(や団体)は、別途入手した不特定多数のインターネットユーザーに向け、有名企業からのものに見せかけたメールを送信する。

このメールリストは、ネット上にて無作為にメールアドレスを収集する事の出来るにアプリケーション・ソフトウェアより自動的に抽出されたものがほとんどであったが、近年ではより効率を高めるべく、更に入り組んだ手法をとるケースも多い。

それらのフィッシング・メール中には、ユーザーを現実に存在する企業のサイトにアクセスするように勧誘する内容が記載されている。ユーザーがリンクをクリックすると、その企業のサイトと間違えてしまうようなデザインの偽の WEB サイトへアクセスしてしまう(ユーザーを信用させるため、実際に本物のページを表示させ、その一部にのみ偽サイトの情報を表示するという場合もある)。表示された偽ページに個人情報を入力すると、その情報はフィッシャー(フィッシングを行おうとする個人やグループを指す)に送信される。

(3) フィッシング被害に遭う企業

フィッシング業者が入手した証明書がクレジットカードのものなら、リスクはカード発行者か小売店が負うことが多い。これは、フィッシングがＩＤセフトと見なされるためであり、よって被害が個人ではなく企業や事業者のものとなる。
また、大手のクレジットカード会社の場合には、フィッシングによって再発行しなくなった新しいカードに関して、カードそのものや暗証番号の制定や口座の確認などにかかる人件費など全てを含めておおよそ、$50 程の費用が発生するという。
なお、フィッシング・メールの詐称となった金融機関などによっては、これらの被害はユーザー自身が詐欺行為として認識し、避けるべき種類の問題とみなしており、金融機関の約款によっては、詐欺にあったユーザー自身がその損失を補填しなければならないとしている企業もある。

しかし、企業が被る被害は、被害金額などに代表される、具体的な形での財務的リスクだけには終わらない。
通常の金融機関は、利用者の意志に反する取引が発生した場合は、その大半の責任は利用者側には負わせない企業方針をとっているところがほとんどである。これは企業が自身の顧客と良好な関係を維持したいと考えているためであり、従来であればその経費が利益によってカバーできると考えられていたからであることは言うまでもない。
APWG は、その他の損失も多く存在しているという。これはフィッシングの攻撃により、企業が自社の WEB サイトを再構築する必要に迫られた場合、その改定期間中も自社の顧客の為に別途この問題に関しての連絡用窓口を設定する必要があることからも分かるが、これ以外にも事前には予測が不可能な、各種の追加費用も発生することが考えられる。被害者が増えればそのままコストが増えるのは当然であるとともに、大量な再発行作業が一時期に集中した場合は、他の業務にも支障を来すことになりかねないし、更には一時的な従業員の不足にもなりかねない。顧客との信頼関係や新規の営業などに支障を来すのは言うまでもなく、その被害額は計り知れないものとなる。このようにフィッシングは特に金融機関にとって重大な問題となっている。APWG の調べでは、複数のオーストラリアの銀行では、フィッシング関連の損失を補填する為に、200 万ドルの基金を設立しているという。

企業側の責任の範疇にあるかどうかの判断も徐々に変わりつつある。APWG の会員企業の中には、フィッシングの対象になったあげく被害が生じたとして、自社の顧客に訴えられた企業もあるという。しかし企業側から見れば、この訴訟の結果如何に関わらず、法的コストが生じ、更には企業としての名声にも大きな悪影響が発生するのは避けられない。

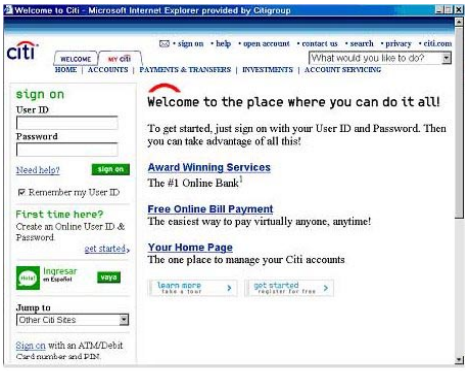
また企業側も将来の不測の事態に備えての準備も行い始めている。大きな被害が続出した eBay では、「一見 eBay から発信されたように見えるメールでも、実際にそうだとは限らない」と警告し、不測の事態に対しての自社責任を回避する余地を残す為、事前に警告を行っている。

フィッシングの標的とされた企業側から見ると被害は更に広がる可能性を秘めている。多くのフィッシャーは、詐欺行為を隠蔽する目的で、別途ハッキングをしてある第三者の Web サーバー上にてフィッシング用の Web サイトを公表する。

米国の法律の解釈如何では、このハッキングされた Web サーバーの運営者が、セキュリティ対策不足を理由に、訴訟の際の被告となる可能性も指摘されている。

Gartner 社の調査によれば、フィッシング・メールで　最も詐称が多かったのは、インターネットオークション最大手の eBay と同社の支払代行サービスの PayPal の利用者を対象にしたもので、また米国の大手金融機関の Citibank をターゲットにしたものも多かった。

一般にインターネット・ショッピングやオンライン・バンキングが普及するに連れて、経験の浅い消費者から重要な個人情報を引き出す方法も増加しつつある。最もターゲットになりやすいのは、オンラインでの各種の取引を開始してまだ間もない消費者達で、同社では、2003 年に新しくオンライン口座を開設したときに詐欺行為に遭遇した 400 万人の消費者のうち、約半数が、フィッシングメールも受信したと報告している。



Citibank を装うフィッシング・サイト

また、ソニーの名を語ったものも、既に 2003 年には出回っており、同年 7 月にはソニーの米国法人は、同社が発信元であるかのようなフィッシング・メールが存在することを発表し、警告を行った。

2003 年のクリスマス前には、VISA からのメールを装ったフィッシング詐欺メールが広まり、同年のホリデー・シーズンには、フィッシング・メールによる被害は、前年対比で 400%以上に増加した。

Gartner 社の Avivah Litan 氏は、インターネット・ユーザーが自身のマシンにタイプを行う文字をすべて記録するキーストローク・ロギングも急激に増えていると言い、消費者を犯罪に巻き込む可能性のある重大なセキュリティ問題はフィッシングだけではないと述べている。セキュリティ分野のアプリケーション・ソフトウェア開発会社の Webroot 社が行った調査では、使用されている PC の約 1/3 にキーストローク・ロギング用のソフトウェア・プログラムが存在していたという。

同氏は、加害者と被害者が、直接接触することが無く、また発覚するまでは同一の被害者に繰り返し被害を与えることが出来るなどの面から、IT 技術は加害者側にとっては、違法行為を行う際には有効な選択肢になるという。こうした問題を解決するには、銀行などのサービスの提供側が、顧客と安全な且つ密接な信頼関係を構築できるように、一段と高度なセキュリティ用の認証技術を開発するしかないと考えている。同氏は、インターネット上でも、コーラーID(発信者番号通知サービス)のようなものが必要だと言い、現時点で企業が採用できる最も簡単な方法は、自社サイトへ顧客がログオンする際に、複数の質問への回答を要求するものにすることだという。この方式は金融機関での初期の登録の際などには広く利用されている。

APWG は、メール認証の標準規格を一層厳しく制定することにより、フィッシングを始めとする各種の詐欺行為の抑制につながると述べている。

(4) 最新の事例

以前は、フィッシングは、フィッシング・メールによるものが中心であったが、最近ではより巧妙な手段により、個人情報を入手しようとしているケースも多い。

（事例１）求人情報を利用した事例

2003 年 3 月にはオンライン就職情報サイトの大手である Monster.com がフィッシング詐欺の対象となった。同社はこのほどユーザー向けに送信したメールの中で、個人情報を入手する目的で偽の求人情報が掲載されていると警告。同社は個人情報盗難を防ぐため、応募に際して社会保障番号やクレジットカード番号、仕事に関係ない情報などを明かすことは避けるよう警告を発している。

（事例２）YahooID、パスワードを入力させる事例

Yahoo! の ID やパスワード、暗証番号（セキュリティキー）を入力させて情報を引き出そうとする Web 上の掲示板が報告されたという。これは Yahoo!とは関係ない Web サイトの掲示板で、ユーザーの Yahoo! ID、パスワードの入力を要求するものであり、同社により既に警告が成されている。Yahoo! の ID や暗証番号

は個人オンクレジットカード番号などに直結するものではないが、複数の情報を組み合わせることや、Yahoo!のショッピングサイトなどでの情報を入手することによって、最終的な被害に結びつくことがあるという。

（事例３）Explorer を利用した事例

2004 年 6 月 11 日には、US-CERT が、Microsoft の Internet Explorer に、フィッシングに利用される可能性のあるバグが存在すると発表した。この種のバグは通常のフィッシング攻撃に比べ、防止策が困難だという。しかし同社は 2 月には、対抗手段が取られた Internet Explorer を公開し、配布を始めている。新しい仕様では、ユーザー名やパスワードを含めたこれらの情報を入力できる形式の URL へは、クリック後もアクセスできないよう修正されており、この種の形式の URL を入力してサイトを表示させようとした場合、ブラウザのタイトル・バーにはエラーが表示されるようになっている。

またブラウザではなく、入手したい個人情報を入力するオンライン・フォームを含んだ HTML 形式のメールを送るフィッシング手法もある。メール上のフォームに情報を入力した後に送信ボタンを押すと、個人情報は加害者の指定するサイトへ送られることとなる。

（事例４）プログラムを活用する事例

また、個人情報を盗むプログラムをメールに添付して送りつける方法も出現した。メールに添付されたアプリケーション・プログラムを実行すると、クレジットカード番号や銀行口座の暗証番号などを入力する画面が表示される。

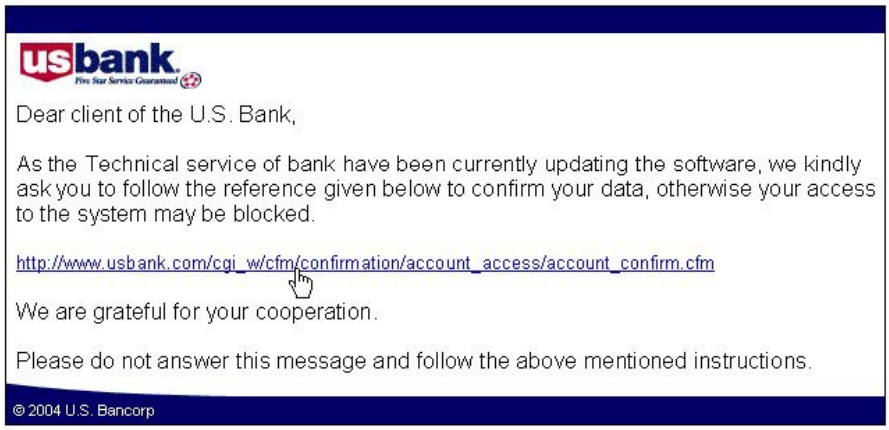
その画面に入力した個人情報は、加害者の指定するサイトへ送信されることとなる。類似系のものとしては、メール中のリンクをクリックすると、情報を盗むようなプログラムがダウンロードされるものもある。被害者自身によってダウンロードされたそのプログラムを実行すると、加害者が入手したい個人情報の入力画面が表示される。

この種のプログラムには、ユーザーのキー入力を記録する、所謂「キーストローク・ロギング・プログラム」が混在されていることもある。同様にスパイ・ウェアやアド・ウェアを見えないようにとダウンロードし、インストールを終える場合もある。更にひどい場合は、PC の基本システムにダメージを与えることの出来る悪質なプログラムやスクリプトが Web サイトに巧妙に設定されていることもあるという。

（事例５）メールソフトウェアのセキュリティホールを利用する事例

また、メールソフトウェアのセキュリティホールを利用するものもある。これはメールソフトウェアのステータス・バーをよく似た形で偽装するもので、Microsoft 社の Outlook Express のセキュリティホールを利用するプログラムが組み込まれている。この偽装が行われた場合には、Outlook Express のステータス・バーに、実在する大手金融機関などの URL が表示される。ユーザーが該当個

所をクリックした場合は、その金融機関とは全く関係の無い、フィッシングのために立ち上げられた偽の WEB サイトへ誘導されてしまう。



↑US bank を装い、Outlook Express のセキュリティホールを付くように細工されたフィッシング用のメールの一例

（事例６）オンラインショップを装う事例

最近ニューヨーク市近郊に出現し、被害報告が多くなってきているケースは、オンラインショップを装ったサイトによるフィッシング行為である。

まず、詐欺を行う側は、良くあるようなオンラインショップ・サイトを立ち上げ、そこに通常のオンラインショップのように各種の商品を並べておく。そのオンラインショップでは、その時点でもっとも人気のある商品を、どこよりも安価で掲載し、入手が困難な商品の在庫が豊富であるかのようにしてあり、購買意欲をそそるような体裁をとる。そしてユーザーはそのオンラインショップで購買を行い、サイト上でクレジットカードの情報や住所電話番号など、必要な情報を入力することとなるが、しかしその商品は多くの場合注文後に在庫不足であり、発送が遅れるなどという通知がショップ側より返答されてくる事となる。多くのユーザーはそこで注文をキャンセルするか、またはサイト側より注文のキャンセルを通知され、一旦はここで商取引が終了したかに見える。しかしサイト上で入手したクレジットカード情報や個人情報を元に、そのサイトとは何の関係もないところでカードが使用され、後日クレジットカードの利用明細が消費者宛に郵送された時点で初めて詐欺行為が発覚する。

また、更に巧妙なのは、一回の被害を得に低額にすることによって、消費者から長期に渡って詐欺行為を行おうとするところも増えてきており、一回の被害金額が 10 ドル以下というものを、数カ月以上の長期に渡って詐欺行為を行うところも目立ち始めている。このような場合は、仮のオンラインショップの有償のダイレクトメールの受領サービスを購入したことになっていたり、格安の旅行や商品の優先購入券を得られるなどという、一見通常の商行為に見せかけているケースも多い。

ニューヨーク市を中心とした近郊に住む、アメリカン・エクスプレス・カードのユーザーを中心に詐欺行為と見られる業務を行っている、Reservationrewards.com 社のトラブルはこの手法の典型的な事例である。同社は登記上はコネチカット州に拠点を構えていることとなっているが、多くの被害者からの電話問い合わせには全く応答しない状況であり、また自動応答の電話に自身の情報を入れないと個人のクレームに対応しないシステムを採択しており、これがまた新たな被害の元となっていると非難されている。同社の行為はネット上でも非難の対象となっており、多くの被害者が自身の経験を語っている。同社の詐欺行為による被害金額は、その多くが 7 ドルとなっており、非常に少額ではあるが、長期に渡って被害を受けている消費者が多く、同社への苦情は非常に多い。しかし金額が少額であることと、長期に渡っての被害ということで、過去の被害額をクレームすることが困難なことも多く、被害は増え続けているという。この場合も、被害者の多くはクレジットカードでの購買をオンラインショップで行ったと見られており、しかし当該のショッピングサイトは、表向き同社とは関係がないこととなっており、またこれらのサイトは短期で閉鎖となりまた新たな名称の元での営業を始めるということを繰り返しており、被害者による届出後の警察による捜査も困難を極めているという。

↑Reservationrewards.com 社の WEB サイト

（事例７）大統領選挙に便乗した事例

メールの為のフィルタリング用ソフトウェアを提供する、SurfControl 社の発表によると、本年 7 月末から 8 月始めにかけて、民主党候補のケリー陣営を騙るフィッシング・メールが発見されたという。

これは大統領候補への寄付を呼びかけるメールの体裁を採っており、献金を行おうとする一般選挙民に対して、フィッシングを行おうとするものである。

政治絡みであること、現時点で実際に選挙運動中であること、更には対抗する両党それぞれに熱狂的な支持者が居ること、それぞれの候補が著名人であることなどが相乗効果となり、警戒心が低くなった被害者から個人情報を盗んだり、実際に寄付をそのままだまし取ろうとする。

これは、これまでの一般的なフィッシングの手法と同じで、候補者からのメッセージを装ったメールにより、潜在的被害者である支持者達に、選挙運動支援のように見せかけたWEBサイトを訪問してもらい、献金や寄付をするように呼びかけるものである。発見された偽サイトは、米国内のものとともに、インドにサーバーが設置されているものもあり、いずれも各候補とは無関係のサイトである。

選挙活動はこの後もしばらく続くことから、大統領選挙に便乗したフィッシング行為は、今後更に増加するものと予想されており、このように時期的に違和感も持たれにくい。同社は、国家行事などを装った詐欺行為は今後一層の留意が必要と見なしている。

同社とともにこの種のメールの為のフィルタリング用ソフトウェアを開発している MailFrontier 社が行った調査によると、インターネット・ユーザーのうち、30%弱の人がフィッシングなどの詐欺行為を行うためのメールと、金融機関などから送られて来る、本物のメールによる企業からのメッセージを区別出来ないという。

（事例８）偽物と判断つかない高度な事例

2004年4月にはAPWGがフィッシングの新たな手口を警告した。

これは米国の大手金融機関であるCitibankの利用者を対象としたフィッシング行為である。まず偽のWEBサイトへ誘導するメール自体には目新しさはない。しかし誘導先の偽のWEBサイトへアクセスすると、ブラウザのアドレス・バーにJavaScriptを使って実際のアドレス・バーを表示させないよう細工が施されており、さらにJavaScriptとフレームタグで作成した偽のアドレス・バーには、偽のURLを表示させる。偽のアドレス・バーにはCitibankのサイトであるかのように表示が出ており、一見しただけでは正規のCitibank社のサイトにアクセスしたかのように見える。このとき偽のアドレス・バーにそれらしいURLが表示されていても、実際にアクセスしているのは偽のWEBサイトなので、ブラウザ隅に表示されるべき、SSL通信していることを示す鍵マークが表示されないままである。また、この偽のページ画面から別のページに移動しようとしても、偽のアドレス・バーは表示されたままで、本物のアドレス・バーと同じように機能する。もし偽のアドレス・バーに直接URLを入力した場合はそのURLのページに移動できる（しかし別のページに移動しても、画面上ではタイトル・バーに「Welcome to Citi」と表示されたままである）。このため、ユーザーは偽のアドレス・バーが表示されていることになかなか気が付かない。

APWGは、今回の手法について、これまで確認した中で最も洗練された方法の一つとし、特に警告を発している。

３．フィッシングへの対応

(1) 企業による対応

フィッシングの被害件数増加にともない、インターネットサービスプロバイダ、ソフトウェアベンダー、セキュリティ会社、クレジット会社など各大手 IT 企業は、インターネット利用者への教育と、こうした被害を防ぐ方法の考案に力を入れている。

ISP など、Web でサービスを提供する企業も対抗策を考慮することは重要である。多くの企業が WEB サイトの運営をアウトソーシングしている為、アドレスバーを表示しないシステムを採択しているケースが多い。これはもし表示された場合には。その企業のドメインではない別の URL が表示されるためで、自社の顧客に不安を与えてしまいかねないためである。しかしこの状況がアドレスバーが非表示でも不自然に感じないことと繋がっており、結果としてフィッシングの成功を後押ししていることは否めない。

悪質なフィッシャーは、実際は偽の WEB サイトにアクセスする URL でも、ブラウザのステータス・バーに、詐称する企業の本来の URL が表示されるように偽装を施しているものもある。このような場合の対抗策は、すぐにブラウザの Back ボタンか、ホーム・ボタンをクリックすることしかないが、この場合も対抗策としては完全ではない。

APWG によれば、APWG の会員は大手金融機関やフォーチュン 500 企業などのいわゆる一流企業だが、会員企業の多くはフィッシングに関する話題の中で言及されることすら嫌がるという。従って対応も遅れがちになるのは否めないし、大規模に警告を発することも躊躇する傾向が多々見られる。

技術的見地に立てば、フィッシングメール自体は一つのメールにすぎず、従来のスパムメールの範疇に区分されるものである。従って、WEB サイトやメールのフィルタリングといった従来からあるスパムメール対策と同様のツールが有効である場合も多い。

また、現時点で実際に効果があると考えられている対策は、各 WEB サーバーの管理者が、頻繁に DNS をスキャンし、自分たちのドメインと似たドメインが登録されていないか調べることだと APWG は述べている。2003 年 12 月に VISA がターゲットになったとき、フィッシング業者は visa-security.com というドメインを使っていた。また、過去に航空券を購入した e チケットの利用者に e-ticketmarketing.com 等というドメインでフィッシング・メールを送るところも出てきている。

一方、大手の主要銀行の多くでは、自社から発信するメールに、電子署名を加えるようにするところが増えてきており、これは顧客でもあるインターネット・ユーザーに、きちんと自社の署名されたメールと、そうでないものとを識別する事を勧める啓蒙活動に繋がるケースが多い。代表的なフィシイングの被害企業で

ある eBay は、この種の活動を具体化し実行しているが、他の多くの民間企業は対策が遅れている。

以下、主な企業の個別具体的な対応状況を紹介する。

・ISP

既に Yahoo、Microsoft、EarthLink、America Online、British Telecom、Comcast といった大手インターネット・サービス・プロバイダ(ISP)数社は、メールのフィルタリングや送信に関する具体的な技術的ガイドラインを制定するために提携をしている。更に EarthLink は、フィッシング対策ソフトの導入に向け積極的に取り組んでいると発表した。

APWG のデイビット・ジェバンス会長によれば、フィッシング・メールやスパム・メールといった、メールを利用した詐欺行為の最大の弱点の一つは、メール送信者のアドレスを偽造していることにあるという。現在でも、身元確認を行なうための最新技術は数多く用意されており、更に高度なものも開発されている。近い将来にはそれらの技術利用により、フィッシング・メールを始めとするネットを経由し、メールを利用した攻撃を、インターネットの利用者に届かないようにすることは可能だという。

・VeriSign

米 VeriSign は本年 6 月にメールのセキュリティを確保する「Email Security Service」を発表した。

このシステムを導入する企業は、メールを悪用して拡大するコンピュータウイルスやスパムメールを遮断することで、企業に勤務する従業員の生産性を向上させ、悪意のあるメールにより引き起こされる無意味なトラフィックや無駄なストレージ消費を抑制できるという。

Email Security Service では、独自な幾つかの学習機能を有し、その他にも複数のアンチ・ウイルス・プログラムを使用し、コンピューターウイルスを自動的にスキャンする機能を持つ他、セキュリティレベルに対する規定値をドメインレベルで適用することが可能で、指定されたドメイン名を利用して送受信されるメールに対し、各種のチェックを行うことが可能であるという。

またメール・サーバーが障害を起こした際には、VeriSign 社の別のネットワークへ自動的に切り替えて SMTP 接続を提供し、メールの送受信に支障が出ないようにする機能も持つ。更にはユーザーが不審なメールを自身の PC 内で確認する前に、別途用意された隔離されているエリア内で事前に閲覧もできる。

VeriSign 社は、フィッシング行為から企業を守る「Anti-Phishing Solution」の提供を始めており、「防御、検知、対応、分析、報告という五つの要素を統合したソリューションによって、企業がフィッシングの被害に遭わないように支援する」という。

VeriSign 社の Security Services 部門、担当執行バイス・プレジデントの Judy Lin 氏は、「企業や金融期間、e コマース業者などは、インターネット上に

おける知名度向上の為、数百万ドルという投資を行ってきている。フィッシング行為はその知名度を逆手にとり、企業の顧客を欺く行為であり、企業のブランド・イメージや評判に悪影響を与える」という。このため、同社は自社の顧客でもある企業の利益を守るため、相手先企業のオンライン上の決済プロセスやセキュリティ・ポリシーに関してコンサルティングを行う他、より厳しい認証サービスを提供し、流出した重要な個人情報が悪用されないようにする。またインターネット上の不正なWebサイトや、メールの検知を継続し、それらを発見した場合は、当該のISPと協力し、サイトを閉鎖する。同様にドメイン名やディレクトリに関するノウハウを活用し、フィッシングの被害を最小限に抑える為、クライアント企業に最新のフィッシング情報や対策を提供する。

・Microsoft―NCFTA

本年7月、Microsoft社はフィッシング詐欺に対抗するため、4万6000ドル相当のソフトウェアと、フルタイムのアナリスト1名を無償で提供すると発表した。

同社からこの提供を受けることになるのは、米連邦捜査局（FBI）とNational White Collar Crime Center、カーネギーメロン大学、ウェストバージニア大学が共同で設立したNational Cyber-Forensics & Training Alliance(NCFTA)という組織である。同社のInternet Safety Enforcementグループのシニア研究員Stirling McBrideは「これは個人情報窃盗や、フィッシングに関する情報を収集し、共有するための組織である」と述べている。フルタイムのアナリストは、同社のこのグループから派遣されるという。

同社のアナリストは、NCFTAがCan-Spam Act（後述）違反や、フィッシングなどのインターネット犯罪に関連するデータを理解するのを手助けすると述べている。更にはNCFTAと協力して、警察当局が的確な専門資料を入手可能なように取りはからう他、警察機構関係者向けのトレーニングや専用のプログラムの構築にも協力する予定だ。

またMicrosoft社では、Sasserなどの悪質なプログラムの作者に関する情報を提供した者に、懸賞金を支払うプログラムも実施している。

更に同社は本年2月に、ウイルスを含む悪質なメールやスパムメールに対抗するための技術を発表した。この技術を取り込んだWindows XP のSP2バージョンでは、「Windows Firewall」「Windows Security Center」、Internet Explorerの機能強化といったセキュリティ機能を新たに導入している。

また同社は、各種のスパムメールへの対抗策として、「Exchange Edge Services」について明らかにした。これは SMTP リレー機能をもつことが特徴で、SMTPリレーの他にも、迷惑メールの配信阻止を自動で行える機能も持ちメール処理速度を向上するとともに、より一層の効率化が図れるという。

この「Exchange Edge Services」技術には、米Brightmail社、GFI Software社、Network Associates社、Sybari Software社、Symantec社、Trend Micro社とともに、スペインのPanda Software社等が、Microsoft社と協力をしていくという。

さらに同社は、「Coordinated Spam Reduction Initiative（CSRI）」という各種のスパムメールの削減をめざし、メールの発信元の身元確認を行うことの出来る技術を発表した。この技術は、一般の電話回線における、コーラーID(発信者番号通知サービス)のメールでの実現を目指すものであり、偽の送信元 IP アドレスを騙ってメールを送信するスプーフィング(spoofing)対策上効果がある。

この種の技術は現在も複数開発が行われており、フィッシングの対象となった企業では、今後実用段階になった時点から、順次採用されていくものと見られている。eBay は現時点から既にこの種の技術の必要性を重要視し、将来の顧客の理解を得ることを目的としてその導入に関して肯定的な意見を積極的に主張し続けている。

・DELL

PC メーカーの Dell は、フィッシング等のインターネット上の犯罪を避けるための、顧客向け教育プログラムを発表した。

・MasterCard

クレジットカード大手の MasterCard 社は本年 6 月 22 日に、増加の一途を辿るインターネットを利用した犯罪行為、特にフィッシングに対抗する対応策を発表した。同社は、セキュリティ・ソフトウェア・開発会社の米国 NameProtect 社と協力し、インターネットを利用した犯罪や詐欺行為に関与する人を追跡すると述べた。この取組みは個人情報窃盗や、不正に入手したクレジットカード情報の転売といった犯罪行為に対抗するものだ。これは特にフィッシングに注力して行われると言い、カリフォルニア州、サンディエゴで開催された、MasterCard の「Global Risk Management Symposium」で発表された。

同社は同時に、全米郵政検査公社や米財務省を含む、複数の連邦政府機関からこの件についての協力を得られていることを発表した。同社は世界各国で 2 万 1000 の金融機関と取引を行っており、彼らとの迅速に連携がこの取組みにととっては重要な項目であるという。この提携の特徴は、被害が発生した後に犯人を追い詰めるのではなく、重要な個人情報にアクセスされる前に、フィッシング行為を行おうとする犯人らに対抗することである。同社は、NameProtect 社のソフトウェアを利用し、偽物の WEB サイト等、フィッシング行為が行われる可能性の高い事象がネット上に発見された場合に、犯罪が起こる前、もしくはその初期の段階でそれを突き止めることを目指す。最終的には、捜査当局と協力の上、インターネットのユーザーが被害に遭う前に犯罪を抑制したいと述べている。

・Barclaycard

2004 年 7 月、英国 Barclaycard 社は、英国内 5000 人の自社の顧客に対し、クレジットカードおよびデビット・カードのカード・リーダーを配布した。これはカードを利用した不正行為や、カード所有者がフィッシング攻撃の脅威から守ることが目的だ。このカード・リーダーには、数字を入力するキーボードと、小型の液晶画面を持ち、これまでの、利用者による署名に代わる方法として、クレジ

ットカードやデビットカードで既に採用されている「IC チップと暗証（PIN）番号」による技術を用い、カード内のデータを読取る機能を備えている。
この新しいシステムをサポートする WEB サイトから商品を購入する場合、利用者はこれまでの e コマースサイトと同様に、自身のクレジットカードやデビットカードの情報を入力する。その後 WEB サイト側からは、このカード・リーダーが生成する特別なパスワードを入力するように要求される。この時点でユーザーは、カード・リーダーに自身のカードを差し込み、新たなパスワードを生成するため、従来の暗証番号を入力する。すると、このカード・リーダーは、新たなパスワードを生成し表示する。この新しく生成されたパスワードをオンラインでの購買に利用することにより、ユーザーはインターネットを介して暗証番号そのものを送信したり、電話で通信販売サービスを利用する時に、暗証番号を押す操作をする必要がなくなる。このカード・リーダー配布プロジェクトで、Barclaycard 社と技術提携をしている nCipher 社は、クレジットカード被害の 35%～40%は、カードの所有者自身が、支払い処理の現場に居合わせない取引（つまりは通信販売やインターネットでの購買）によって発生しているという。
　nCipher 社の Carter 氏によると、Mastercard 社は、今後も各加盟店に対し、この新しいカード・リーダーによる新システムを導入するよう、積極的に勧誘していく予定だという。加盟店側にとっては、このシステムの導入は不正取引の負債を被ってしまうことによる経費負担の軽減につながる。「現時点では、法的面からも企業ポリシーの面からも、被害の責任を取っているのは商店側だ。しかし彼らが新カード・リーダーを導入すれば今後はこの種の責任から免れられる。そしてその手間は非常に小さいものである」と Carter 氏は述べている。

・Network Associates
　米 Network Associates 社は本年 3 月より同社のクライアントである企業をはじめとし、各企業および個人にフィッシング対策を指南すると発表した。
　同社は、企業および個人がフィッシング行為から情報を守るための対策を「Anti-Phishing: Best Practices for Institutions and Consumers」という資料ににまとめ、同年 3 月 15 日に発表した。
　企業や個人がフィッシング行為の具体的な内容を把握することでその被害を最小限に抑え、今後の更なる攻撃に対応できるようにするのが目的であるという。
　同社が勧める主な対策は以下のとおり。
　（企業向けの対策）
- 合法なメールとフィッシングを混同しない為、ポリシーを策定し、インターネット・ユーザーに周知徹底させる
- 受信メールが合法的であることを検証する技術的手法を確立する
- Web サイト上での認証を強化する
- 自社の Web サイトがフィッシング行為に利用されないよう、常にネット上を監視する
- アンチ・ウイルス、コンテンツ・フィルタリング、アンチ・スパムなどの技術的手段を導入する

（個人向けの対策）

- 悪意のあるメール、または不正なメールを自動的に遮断する
- 悪意のあるアプリケーション・ソフトウェアを自動的に検出および削除する
- 悪質な業者への重要な機密情報の送信を自動的に防止する
- 受信メールが合法的であるかどうか分からない場合には、その送信元とされる企業などに直接確認を行う

(2) 企業間連携による対応

企業間連携による対応としては前述の APWG による取り組みがある。民間企業の対策の遅れをカバーするために、APWG ではあらゆるケースに関しての被害状況などの報告を受け付け、有効な対応策の実施に役立てたいとしている。また、APWG はフィッシング問題に対してきちんとした認識をもち、具体的かつ有効な対策を求める企業には、APWG に参加すればメリットがあるとしている。APWG の会員になれば、同業者や過去に被害にあった企業を参照することが可能であるし、他のいくつかの業界組織とも連携しているため、より幅広い情報を収集できる。APWG は、フィッシング事業者が偽名で加盟しないようにするための最低限の審査を経た企業であれば、どのような業種でも海外に拠点を持つ企業でも会員になれるという。APWG は各地で定期的に会合なども行っており、情報収集や交換などとともに、企業へ対する啓蒙活動なども行っている。

前述の APWG 以外にも企業間連携による動きがある。

本年 6 月 1 には、小売業、金融機関及びそれに類するサービス業、通信関連、IT 技術業界の各企業が、メールや電子商取引を悪用してのフィッシング等の詐欺行為などに対抗する為の団体「Trusted Electronic Communications Forum（TECF）」を発足させた。

TECF は、フィッシングを始めとする、インターネットを利用しての個人情報窃盗を行おうとする相手に対して、それらの行為によるリスクの低減を目的とする任意団体である。潜在的な被害者であるインターネットの利用者や、詐称の対象となる可能性のある企業をフィッシャーより守るため、国際標準となる基準の制定作業も進めるという。TECF は、フィッシングそのものとともに、スプーフィングもその対象に加えることとしている。

TECF 会長の Shawn Eldridge 氏は、フィッシングなどによる個人情報窃盗の被害は、既に年間数 10 億ドルにのぼり、フィッシングがインターネットとそのユーザー、更には企業に対する信頼感を失墜させていると声明を発表した。

（TECF の設立メンバー企業）

オランダの ABN AMRO 社。
米国 AT&T Wireless 社。Best Buy 社。Charles Schwab 社。CipherTrust 社。DirecTV 社。E*Trade 社。Fidelity Investments 社。GE Access 社。IBM 社。National City Bank 社。PostX 社。Siebel Systems 社。
英国 HSBC 社、Royal Bank of Scotland 社。

TECF と APWG との違いは、APWG はポリシーに注力しており、問題の定性的や定量的な側面を規定している。TECF は技術標準策定と米国政府への働きかけをその活動の中心とするとされている。

(2) 政府の対応

本年 7 月 15 日には米国のブッシュ大統領が、フィッシング等を中心とする、各種の身元詐称行為を刑事罰に処することの出来る法案に署名し、法案を成立させた。Identity Theft Penalty Enhancement Act（ITPEA）と呼ばれるこの法律は、犯罪目的で他人の個人情報を所有すること、もしくはその目的での個人情報の窃盗行為に対する刑罰のガイドラインを制定している。

この法案では、ID セフトに対して執行猶予を容認しない懲役 2 年の刑事罰が制定されており、テロリスト事件と関係が認められた場合は更に 5 年の刑期が自動的に追加となる。

この法案の主要な推進者だったウイスコンシン州の共和党下院議員、James Sensenbrenner は、テロ組織が身を隠しながら活動するために ID セフトに力を入れていると言い、テロ問題以外でも、米国ではこれらセフト窃盗による被害が増えており、早急な対策が必要であると主張してきた。

警察機構の構造から、罰則が緩やかだったことも今回の法案制定の大きな理由の一つだ。米国では州内の犯罪は各自治体が。州をまたぐ場合には FBI が捜査を担当するが、ID セフト事件は、犯人と被害者が離れて存在する傾向にあるため、これまで捜査の迅速性や、立件から起訴までが難しいことが多かった。

A 州に住む人が B 州に住むフィッシング犯の被害に遭った場合、両州の警察が捜査を開始する。しかしその警察機構同士のせめぎ合いから捜査の進展がスムーズに行くことは困難だとされている。その結果重罪の可能性が高いにも関わらず、軽微な罰則で処理されることがこれまでは多かったという。

ITPEA では、厳しい連邦法の導入で、より多くのケースを起訴に持ち込むのが狙い。悪質な ID セフト事件は、組織的な犯行であるケースが多く、その全貌を徹底して追求できるようにすることが目的である。

またこれに先立ち、スパムメールを制限する法案も本年から施行されている。これは、迷惑メール対策法案と呼ばれ、通称 CAN-SPAM 法と呼ばれる。CAN-SPAM 法の内容は一部の反スパム推進派が要求していたほどに厳しくはなく、詐欺的な宣伝目的のメールでなければ罰則はなく、また、受信者が以後の受け取りを拒否の意思を示すことにより送信を停止するオプトアウト方式を採用していることが非難の対象となっている。また、FTC による反スパム対策用のリスト(do-not-spam List)の作成を認めてはいるが義務付けてはいない。

また、州政府レベルでは、昨年 9 月にカリフォルニア州で成立した反スパム法については、他州以上に対象が広範であることから、スパムメールの発信業者から、米国憲法で保障された権利を侵害するという訴訟が起こされる可能性が指摘されており、同様の理由から通信販売の民間企業などからも、長年慣れ親しんだ

これまでの商慣行を著しく疎外するものとして苦情が申し立てるだろうと考えられている。

(3) 利用者による対応

益々増大するフィッシングを防止する方法は、スパムメールの際と同様に、技術面からの改善、法整備の充実が図られつつあるが、APWG では技術面での対抗策だけではフィッシング対策としては不十分であると述べている。これは、現時点での最高の技術力をもってしても、詐欺行為に利用される WEB サイトの排除は困難であるためである。

APWG によれば、通常 Web サイトや Web ページを切断するには、19 時間から 6 日半の時間を要するという。また対象となる Web サイトが海外にある場合は、時差や法の違い等の問題などから、作業に要する所要時間は一層長くなる。現実にはフィッシングの為にハッキングにあった Web サイトの多くが、東ヨーロッパや東南アジアに集中しており、これらの地域で日常的に使用される言語が英語でないことから、やりとりには更に時間がかかることが多い。このような状況では、WEB サイトを閉鎖するまでのの被害が更に増え続けることとなる。だまし取られた資金は、秘密主義を採る幾つかの国の金融機関を経由し、それらを幾つも経過する間に洗浄され(マネー・ロンダリング)、結果として資金の移動状況を確認することが不可能となる。APWG の調べでは、現実にこれまでにフィッシング詐欺の関係者を訴追できたことは一度もないという。結局、被害者にならないために取れる対策のうち、インターネット・ユーザーが採ることの出来る手段で最も効果的なのは、疑わしい Web サイトにアクセスをしないことである。

連邦取引委員会(FTC)ではフィッシングによる被害を避けるために、次のことに留意するよう消費者に伝えている。

・個人情報を入力するよう催促するメールが来た場合は、直接そのメールに返事をしたり、そのメールに記載されていたりリンクが張られているサイトを訪れないようにする。

・その上で、そのメールの差出人となっている企業へ電話連絡や直接訪問によりその内容をきちんと確認をすること。もしくは改めて URL を入力した上で訪れることの出来る、その企業の本来の Web サイトからしかるべき確認を行う。

・またインターネット上でクレジットカード番号や、銀行口座の暗証番号等の重要な個人情報を入力する際には、WEB サイト上で SSL が使用されていることを確認すること。

・更にはクレジットカードの利用明細等に未確認の利用金額が記載されていないかを確認する。

（参考資料）

http://www.consumer.gov/idtheft
http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm
http://www.antiphishing.org/

http://en.wikipedia.org/wiki/Phishing
http://www.antiphishing.org/word_phish.html
http://www3.gartner.com/5_about/press_releases/asset_71087_11.jsp
http://www.tumbleweed.com/company/press_releases/2004/index.html
http://news.sel.sony.com/pressrelease/3817
http://help.monster.com/besafe/
http://home.reservationrewards.com/
http://www.ripoffreport.com/reports/ripoff66519.htm
http://www.mailfrontier.com/press/press_phishtest.html
http://www.antiphishing.org/phishing_archive/Citibank_3-31-04.htm
http://news.com.com/Alliance+turns+up+heat+on+spam/2100-1032_3-5243727.html?tag=nl
http://www.verisign.com/corporate/news/2004/pr_20040628.html
http://www.microsoft.com/presspass/press/2004/jul04/07-21NCFTAPR.asp
http://news.com.com/Microsoft%27s+bounty+hunter/2008-7355_3-5228216.html?tag=nl
http://www.microsoft.com/exchange/techinfo/security/EdgeServices.asp
http://news.com.com/Dell+wants+to+teach+Web+surfers+a+security+lesson/2100-1009_3-5276639.html?tag=nl
https://programs.regweb.com/mastercard/risk2004/
http://news.com.com/2100-7348-5243302.html
http://www.barclaycard.co.uk/
http://www.ncipher.com/
http://news.zdnet.co.uk/internet/security/0、39020375、39159671、00.htm
http://www.mcafee.com/us/default.asp
http://www.tecf.org/resources/press/2004_06_16
http://dw.com.com/redir?destUrl=http%3A%2F%2Fthomas.loc.gov%2Fcgi-bin%2Fbdquery%2Fz%3Fd108%3Ah.r.01731%3A&siteId=3&oId=2100-1028-5270077&ontId=1023&lop=nl_ex
http://www.techweb.com/wire/story/TWB20040616S0009

このレポートに対するご質問、ご意見、ご要望がありましたら、
hiroyoshi_watanabe@jetro.go.jpまでお願いします。