社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2007－ＥＩＰ－36（２）
2007／5／25

フィッシング詐欺によるブランドへの影響に関する考察

荒金 陽助† 塩野入 理† 金井 敦†

† NTT 情報流通プラットフォーム研究所 〒239-0847 神奈川県横須賀市光の丘 1-1

あらまし オンラインサービスの普及に伴い，利用者のクレジットカード情報や金融情報などの個人重要情報をだまし取るフィッシング詐欺が社会問題化している．報道などにおいてもフィッシング詐欺による被害額などが話題となるが，その焦点は主として情報を窃盗されたユーザの損害に集まっていることが多い．しかし，被害者の意識から見れば，ターゲットとなったブランドを利用しようとした上での被害であり，今後そのブランドを利用しようとするモチベーションの低下につながることになりかねない．従って，被害者への損害補償やオンラインサービスの一時停止などの直接的被害だけではなく，長期的に顧客が離れていってしまうというリスクも考慮しなければならない．本稿では，知的財産としてのブランドへの攻撃という観点で，昨今のフィッシング詐欺の状況を概観するとともに，ブランドへの影響を考察する．

キーワード フィッシング詐欺，ブランド，アカウント情報

A Study for the Impact of Fishing on Brands

Yosuke ARAGANE†, Osamu SHIONOIRI†, and Atsushi KANAI†

† NTT Information Sharing Platform Laboratories, NTT Coporation
1-1 Hikarino-oka, Yokosuka, Kanagawa, 239-0847 Japan

Abstract According to the spread of online services such as online shopping, the phishing fraud has been famous crime which steals consumers' personal identity data and financial account credentials. In general, some reports about phishing damage describe on each customers' (users') economical damages. However, the customers' might have negative image not only on phishing crime but also on targeted brands. Therefore, there should be some negative influences to brand images by phishing fraud. There are some examples such as economical compensation for victims or online service suspension. However there is less discussion about escape of users in long term. In this paper, we explain about the environments around phishing fraud as a attack approach to a brand and discuss about phishing's influences to brand images.

Key words Phishing, Brands, Finacial Account

1. はじめに

ネットワーク環境の整備と普及および Web アプリケーションなどの開発によって，日常の様々な局面にオンラインサービスが浸透してきている．オンラインサービスではアクセス履歴や購買履歴，その他の様々な個人情報を駆使することでユーザに大きな利便性を提供している．オンラインサービスは従前のビジネスとは異なり，必ずしも店舗や流通網などのインフラを自前で用意する必要がないにも関わらず，アイデア次第によっては莫大な数のユーザを引きつけることが可能である．図 1 に B to C の電子商取引の市場規模の推移を示す [1]．

このようなオンラインサービスは，ユーザの口コミなどによって拡大することも多く，そのブランド性は必ずしも既存のブランド体系に依存するものではない．オンラインでの評判情報はプラス評価についてもマイナス評価についても爆発的に広がることが多く，ユーザの支持（プラス評価）を集めることで一気に巨大なマーケットを作り出すことも可能である．また，店舗を有する商取引では，商圏が自ずと定まり，それに従って市場規模も制限されることが多いのに対して，オンラインサービスでは距離的な制約はほとんど無く，また，国境も大きな障壁とはなり得ない．例えば，大手 EC サイトの eBay の登録ユーザ数は 2007 年 12 月末現在で 2 億 2200 万人であり，同社の決済事業部門である PayPal の登録ユーザ数は 1 億 7100 万人に達している．

図 1 に示すような B to C 電子商取引の急拡大は，新規ユーザを大量に生み出し，必ずしも十分なコンピュータリテラシ・ネットワークリテラシを持たないユーザを多く抱えることとなった．このような社会状況において，これらのユーザをター

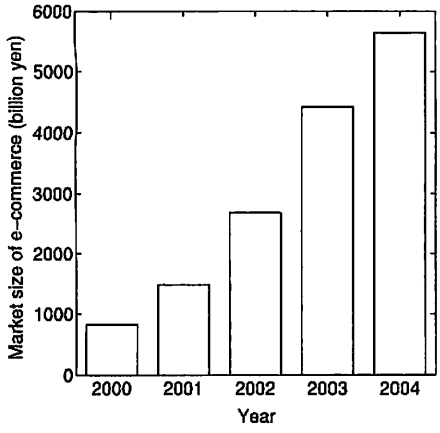

図 1　電子商取引の市場規模推移 [1]

ゲットとして金融情報などの個人重要情報を盗み出すフィッシング詐欺が社会問題化している．フィッシング詐欺とは，クレジットカード情報や金融口座のアカウント情報など，個人の様々な重要情報を盗む犯罪であり，情報を送信させるための偽装ウェブサイト（フィッシングサイト）に被害者を誘導するために偽装電子メール（フィッシングメール）を用いること，およびこれらの偽装ウェブサイトと偽装電子メールにおいて，心理的および技術的手段を駆使することを特徴とする [2]．これらの手段が巧妙に使われることで，多くの被害者は被害に遭ったことすら認識することが難しい点もフィッシング詐欺の問題である．

このようなフィッシング詐欺に対して，主に Web ブラウザを対象として様々な対策手法が提案されている．悪意ある JavaScript を検知する手法 [3] や，ドメイン名，URL，リンク，画像の近似性をチェックする手法 [4]，Visual Hash を用いて正当サイトを証明する手法 [5] などが存在する．しかしながら，Wu らが述べているように [6]，フィッシング詐欺は人間自体をターゲットとしており(注1)，フィッシング詐欺における人間の行動や社会への影響を解析することも重要である．本論文では，フィッシング詐欺がターゲットとするブランドの視点からフィッシング詐欺を概観する．

なお，本稿で述べる “ブランド” には二つの意味がある．ひとつは，主に経済活動を行う主体としての企業を示す意味であり，もうひとつは，消費者が持つ企業イメージという意味である．前者は広義のブランドであり，後者は狭義のブランドであるとも言える．本稿では前者を “ブランド”，後者を “ブランドイメージ” として使い分けることにする．

以下，第二章では典型的なフィッシング詐欺の流れとその統計的特徴について述べ，第三章ではフィッシング詐欺とブランドとの関連性について議論する．

(注1)：“Phishing is an attack that directly targets the human being in the security system.”

2. フィッシング詐欺とその特徴

本章では，フィッシング詐欺の典型的な流れと，その統計的特徴について説明する．

2.1 典型的なフィッシング詐欺

インターネットバンキングを対象とした典型的なフィッシング詐欺の流れを図 2 に示し，そのプロセスを説明する．フィッシング詐欺師を M，預金者 A，銀行 B，第三者 C とする．

① サーバ乗っ取り

M は C の Web サーバの脆弱性等を利用して侵入し，自己の支配下に治める．

フィッシングサイトを構築するにあたっては，それが犯罪目的であるため，フィッシング詐欺師自身が管理をする（または借りている）サーバ上にそれを構築することはほとんど無い．多くは，ターゲットとするブランドとも全く無関係なサイトをクラックしてフィッシングサイトを開設する．わが国でも，公共機関や大学のサイトなどがクラックされ，フィッシングサイトを作成された事例が報告されている [7]．

② 偽 HP 作成

M は B の本物の Home Page (HP) に類似する偽 HP を作成する．偽 HP には「登録情報の更新」を求める記載がある．

ターゲットとするサイトと類似したサイトを作る際に，サイトの情報がデジタルデータであるため，容易にコピー可能であることもフィッシング詐欺の拡大を招いていると考えられる．

③ 偽 HP 公開

M はインターネットに接続された C の Web サーバ上で偽 HP を公開する．

ターゲットとするブランドとは無関係のサイトにフィッシングサイトを構築した場合でも，ディレクトリ名をそれらしい名称にしたりすることで，被害者を巧妙に騙すことも行われる．

④ 偽メール作成

M は偽 HP へのアクセスを誘引するメールを作成する．メールには「登録情報の更新」を求める記載がある．

様々な DM や実際の企業からの（正しい）お知らせメールが氾濫する今日において，それらの（正しい）メールの文面を参考に作成されたフィッシングメールを，その文面から偽メールだと判別するのは難しい．「メール発信者と称する企業が，クレジットカード番号を記入させることはない」，または，「重要事項を郵送ではなくオンラインで更新・確認させることはない」，などの企業の情報取り扱いポリシまで踏み込んだ高いコンピュータ/ネットワークリテラシーを必要とするからである．

⑤ 偽メール送信

M は B を送信元と偽ったメールを特定多数または不特定多数の第三者（A を含む）に大量送信する．

メールの送信元（from フィールド）は詐称することが技術的に容易であるため，受信者のメーラーにはインターネットバンキングの銀行や，オンラインサービス会社，クレジットカード会社の名称が発信者名として表示されることとなる．

⑥ 偽メール受信

A はフィッシングメールを受信する．

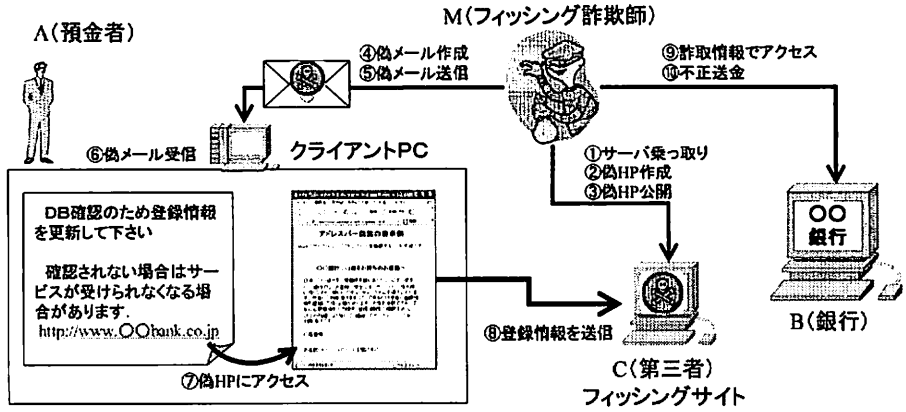

図 2　典型的なフィッシング詐欺の流れ

上記のような送信元の詐称や，サブジェクトの文面に「緊急のお知らせ」などの注意を喚起するような文面や詐称する企業名が記載されたりしているために，受信者は詐称企業からの読むべきメールであると誤認する．その結果，メール一覧の中から本文を閲覧するようそのメールを選択してしまうことになり，より高度な詐称の手口（記述）が駆使されているメール本文に誘い込まれてしまう．

⑦　偽 HP にアクセス

A は受信したメールの記載内容を信じてその指示に従い偽 HP にアクセスする．

フィッシングメールの発信者および内容を信頼し，メール内のリンクをクリックすることで，利用者は詐称された企業のサイトだと誤認したままフィッシングサイトに誤誘導されることになる．

⑧　登録情報を送信

A は偽 HP の記載内容を信じて ID，パスワード等の A の個人情報を偽 HP に自ら入力する．

フィッシング詐欺師はフィッシングメールから自然な流れで，被害者が個人情報を入力・送信するようにし向ける．詐取対象となる情報は，オンラインサービスのアカウント情報の他に，換金性の高いクレジットカードの情報や個人を特定する情報となるソーシャルセキュリティナンバー（社会保障番号：米国）などの情報が含まれることが多い．

⑨　詐取情報でアクセス

M は B のインターネットバンキング HP にアクセスし，A の ID，パスワード等をシステムに入力する．

オンラインサービスのアカウント情報であれば，そのオンラインサービスへのログインがこれに該当する．

⑩　不正送金

B は A になりすまし，A の口座から預金を M の管理下にある他の口座等へ送金する．

フィッシング詐欺師が情報を犯罪組織に売り渡すことで利益を得るケースも多い．

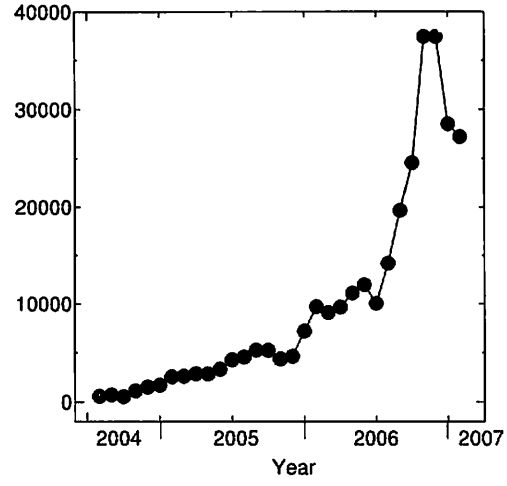

図 3　新たに発見されたフィッシングサイト数 [2]

2.2　フィッシング詐欺の統計的特徴

フィッシング詐欺について様々な観点で調査を行っている Anti-Phishing Working Group (APWG) のレポートの概要を表 1 に示す．

APWG に報告されただけでも 1ヶ月間で 27000 以上のサイトが新たに発見されており，870 サイト/日以上のペースでフィッシングサイトが開設されていることが分かる．この "新たに見つかるフィッシングサイト数" の時間推移を図 3 に示す．2004 年の 10 月には 1142 サイト/月であったものが，2005 年の 12 月で 7197，そして 2007 年 1 月で 27221 と 24 倍近い伸びとなっている．推移としては完全な単調増加ではないため，2006 年末からの減少が各種対策や啓蒙活動の成果なのか，誤差の範囲に過ぎないのかは予断を許さないが，サイバー犯罪の一つとして対策の緊急度が増していると思われる．

一方，フィッシング詐欺がターゲットとするブランド数は 135 ブランドであったが，そのうちの上位 80%は 10 のブランドに集中している．また，フィッシングサイトの寿命はわずか 4 日

表 1　APWG レポートの概要 (2007 年 1 月) [2]

contents	value
Number of unique phishing sites received in January 2007	27221
Number of brands hijacked by phishing campaigns in January 2007	135
Number of brands comprising the top 80% of phishing campaigns in January 2007	10
Country hosting the most phishing websites in January 2007	United States
Contain some form of target name in URL	24.5%
No hostname just IP address	18 %
Percentage of sites not using port 80	3.0%
Average time online for site	4.0 days
Longest time online for site	30 days

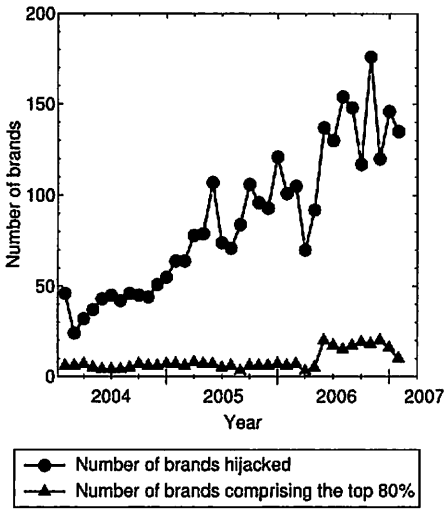

図 4　フィッシング詐欺のターゲットとなったブランド数 [2]

であり，フィッシングサイト閉鎖などの対策が困難な状況となっている．

3. フィッシングとブランド

本章では，フィッシング詐欺とそれがターゲットとするブランドとの関係について考察する．

3.1 数の論理としてのブランド

フィッシング詐欺のターゲットとなったブランド数の推移を図 4 に示す．

ターゲットとなったブランド数は着実に増加を続けており，3 年前（2004 年初頭）と比較して約 3 倍となる 150 ブランド前後で推移している．しかしながら，上位 80%を占めるブランド数は総ブランド数に比例して変動してはいない．これがブランドに関するフィッシング詐欺の特徴である．

二章で示したように，フィッシング詐欺は主として電子メールによって被害者に偽装メール（フィッシングメール）を送るところからそのプロセスが始まる．このフィッシングメールを受け取った被害者は，メール内に記載されたブランドから送られてきたメールであると誤認して，メールに記述されている指示に従い，ブランドのオンラインサービスのアカウント情報やクレジットカード情報などを送信してしまう．その結果としてフィッシング詐欺師は情報を取得し，それを使って不正な利益を得ることになる．ここで，フィッシング詐欺師が得る利益 V は以下のように定式化することが可能である．

$$V = N_a \times p_0 \times p_1 \times C \tag{1}$$

ここで N_a はフィッシングメールを送った人数，p_0 はフィッシングメール受信者が偽装ブランドの利用者である確率，p_1 は利用者が騙される確率，C は詐取した情報一つから得られる利益である．総利益 V を向上させるためには，これらのパラメータの値を上げることが必要となる．その一つとして，フィッシングメール受信者が偽装ブランドの利用者である確率 p_0 を向上するアプローチがある．このためには，利用者の多い巨大ブランドをターゲットとすることで p_0 の値を確保することが行われる．その結果として，図 4 に示すように少数のブランドがターゲットとして狙い打ちされる傾向が生まれることとなる．

3.2 スピアフィッシング

式 (1) に示す V を増加させるための手段として，他の手口も出現してきている．そのひとつがスピアフィッシングである．スピアフィッシングとはフィッシングメールの宛先を特定のブランド利用者に絞って行わるフィッシング詐欺である．スピアフィッシングの登場の背景にはいくつかの理由が考えられる．

- フィッシングメールの宛先であるメールアドレスの収集にはコスト(注2)が生じるため，効率のよいフィッシング詐欺のためには V を減少させずに N_a を減少させたい．そのために，$p_0 \simeq 1$ となるようなメールアドレスの集合を確保することで，N_a が減少しても $N_a \times p_0$ が減少しないようにする．2004 年の CardSystem Solutions 社による四千万件以上のクレジットカード情報の漏洩に伴って，特定カード会社のカード保有者に対してそのカード会社を名乗るスピアフィッシングが仕掛けられた事例が報告されている．
- N_a が少ないと言うことは，発送するフィッシングメールが少ないことを意味する．現在，世界各国で SPAM 対策を謳った法案が出てきており，大量のメールを送信することは，それに比例したリスクを負うこととなる．また，SPAM フィルタが普及してきており，フィッシングメールを大量に送ることで SPAM フィルタベンダの目にとまる確率が高くなり，フィル

(注2)：業者から購入するのであれば直接的コストだが，フィッシング詐欺師が自ら収集する場合でも作業コストが発生する．

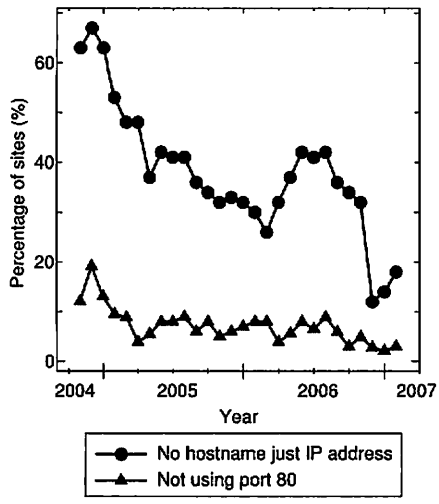

図 5　フィッシングサイトのネットワーク的特徴 [2]

タのルールに追加される可能性が高まることとなる．そこで，N_a を減ずることで，法や SPAM フィルタの目をかいくぐるようにする．

- 特定の企業情報を詐取して転売を狙う，より組織的で経済効果の大きいフィッシング詐欺が発生してきている．目的としている情報を持っているのは標的としている企業の従業員であり，また情報を盗み取ったことが発覚していないこと自体にも価値がある(注3)ため，標的を絞ったフィッシングが行われることになる．企業のネットワークに侵入するために，ネットワーク管理者を装って従業員にアカウントを知らせるよう依頼するフィッシングなどが知られている．

既存研究においても自分が会員であるまたは知っているブランドに対してはフィッシング詐欺への耐性が低くなることが報告されており [8], [9]，スピアフィッシングは p_0 を上昇させるためにフィッシングメールの宛先を絞ることで，結果として p_1 も増加させていると考えられる．このように巨大ブランドを狙わなくとも効果的に犯罪を行うことの出来る手法が開発されたことで，様々なブランドに対する攻撃が発生し，その結果として図 4 の 2006 年半ばから示されるように，上位 80%を占めるターゲットブランド数が増加する傾向にあるとも考えられる．

3.3　踏み台としてのブランド

図 2 に示すように，フィッシングサイトは他のサイトを乗っ取って設置されることが多い．本節では，数値データからこの傾向を探ることとする．

図 5 にフィッシングサイトのネットワーク的特徴を示す．図 5 には，フィッシングサイトの URL に IP アドレスが含まれる割合と，80 番以外のポートを使用しているフィッシングサイトの割合が示されている．これはどちらも減少傾向にあるが，これには様々な要因が考えられる．

まず IP アドレスに関しての理由としては，URL 内の IP アドレスに対する利用者の意識変化と，フィッシングサイトの設置場所の変化が挙げられる．巨大ブランドのサイトのほとんどは，そのブランド名を関したドメインを URL としているものが多く，ブラウザのアドレスバーに IP アドレスが並ぶことはほとんど無い．また，ウィルスが設置されているサイトやワンクリックサイトなどの利用者に危害を与えるサイトが IP アドレスを含む URL を使っていたこともあり，IP アドレスを含む URL に対して利用者が警戒感を持つようになってきている．フィッシングサイトの設置場所の観点からは，フィッシング詐欺の摘発が進んだことで，リスクを負ってまで自らサイトを構えるフィッシング詐欺師が減少し，他の無関係のセキュリティ強度の低いサイトを乗っ取って設置するケースが増大したことが IP アドレスをふくむ URL の減少の理由としてあげられる(注4)．サイト名はターゲットとなるブランド名とは無関係になるが，アルファベットの羅列としてはすぐに見分けが付かないことと，サイト名以下のディレクトリ名などをブランド名と関連づけることで p_1 を向上させることが可能である．

一方，ポート番号については，他のサイトを乗っ取って設置されたフィッシングサイトが多くなったことが主要因であると考えられる．待ち受けポート番号を変更することはフィッシング詐欺師が立ち上げたサーバであれば容易であることから，その減少は，フィッシング詐欺師が立ち上げたサーバの減少に影響を受けたと考えられる．なお，乗っ取ったサイトにおいてフィッシングサイトの存在が露見しないように異なったポート番号を利用している，という理由も考えられる．しかし最近では，サイトが設置されている Web サーバとは別にファイアウォールサーバなどを設置するケースが増えており，主要因ではないと思われる．

このような，乗っ取り型フィッシングサイトの間接的影響として，フィッシングサイト生存期間の短縮が進んでいる．図 6 にフィッシングサイトの平均生存期間の変化を示す．

2004 年後半と比較して 2 日以上も平均生存期間が短縮されており，フィッシングの短期決戦型の傾向が強まっていると考えられる．これには大きく二つの理由が考えられる．ひとつは，摘発可能性を低くする目的である．フィッシングでは，サイトの設置や詐取した情報の伝達において，様々な手法を用いることで追跡を困難としていることが多い．しかしながら，より多くの情報量を残すことで摘発可能性が高まるため，可能な限り早期に情報および活動の痕跡を消去することが望ましい．もうひとつは長期にわたってフィッシングサイトを開設するメリットが少ない，という理由である．被害者の行動として，フィッシングメールを読んだ直後にフィッシングサイトへのアクセスが増加し，それ以降は急激に減少することが考えられる．これ

(注3)：例えば企業の戦略情報を考える．新商品情報など機秘情報が競合他社に漏れたことが発覚した場合，競合他社が対策を打ってくることは明らかとなる．そこで，さらなる対策を考えて戦略を練り直すことで，競合他社の対策の効果を減じようとする．しかし，戦略情報が漏れていることが発覚していなかった場合には戦略の練り直しは発生せず，競合他社の対策は大きな効果を上げることが期待できる．

(注4)：とは言え，ターゲットとするブランド名と酷似したドメインを取得するフィッシングサイトも依然存在する．

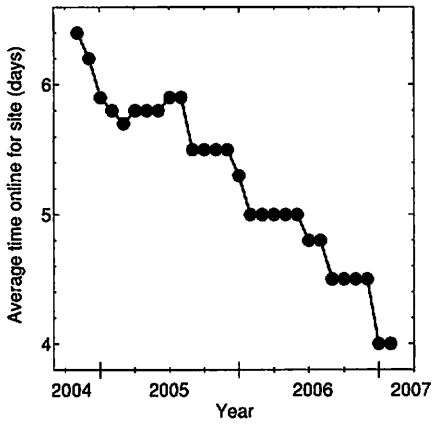

図 6 フィッシングサイトの生存期間 [2]

には，2 章で述べた緊急性を煽る文面も影響を与えていると思われる．また，ブラックリストを使ってフィッシングサイトを警告するブラウザが多数出てきており，ブラックリストに載ったフィッシングサイトへのアクセスは極端に減少すると想定される．日数が経つにつれてブラックリストに登録される可能性が高まるため，短期間でフィッシング詐欺のプロセスを完了させる意識が強まると考えられる．

3.4 ブランドへの被害

このようなフィッシング詐欺によるブランドへの被害は決して少なくない．現時点での我が国の状況においては，単に被害者の損害であるという見方が多いが，欧米諸国などでは様々な被害が報告されている．

まず，被害者の損害に対する保険の支払いが挙げられる．50 ドルルールや 50 ポンドルールなど形態は違えど被害者の損害を補償する制度が設置されている例が多い [10]．この場合，その損害は銀行またはクレジットカード会社などが被害者に対して補償するが，その資金は保険会社より提供される．従って短期的には保険会社の損害であり，長期的には保険金の値上がりによってブランドの損害に反映される．

次にサービス運営への影響が挙げられる．フィッシング詐欺によりオンラインバンキングが一時閉鎖に追い込まれた銀行が出現している [11]．これがオンラインショッピングの企業であったならば，その企業の全業務が停止することになり，機会損失も含めてその損害は莫大なものとなる．また，メール中にフィッシングサイトへのリンクを持つフィッシングメールの存在により，正規の企業が送るメールの中に自社サービスへのリンク URL を記述しにくくなっている，という問題も発生している．

最後に，ブランドイメージへの悪影響が挙げられる．現時点では，フィッシングのターゲットとなることはある意味巨大ブランドの証でもあるが，それが頻発するようになると利用者の信頼に与える影響が無視できなくなる．問題の放置または被害者等への対応ミスによるブランドイメージの失墜や，信頼崩壊によっていつの間にか顧客が離れていってしまうという現象が起こりかねない．また，フィッシングサイトの踏み台となったブランドについても影響は少なくない．これは，フィッシング詐欺師によってサーバが乗っ取られたことを意味するため，そのブランドのセキュリティレベルが疑われることとなる．これらブランドイメージへの被害は，その他の被害と比較して定量的な評価が行いにくいため軽視されがちであるが，長期的な影響を考えた際には大きなインパクトがあると考えられる．

4. おわりに

本論文ではフィッシング詐欺プロセスの説明を行うとともに，フィッシング詐欺がブランドに与える影響について考察した．一般的にフィッシングは，巨大ブランドをターゲットとすることで大きな利益を上げようとしてきたが，昨今の傾向としてスピアフィッシングなどフィッシングメールを送る対象（フィッシングを仕掛ける対象）を絞ることで成功率を上げるような手口が散見されてきており，今後は巨大ブランドだけではなく様々なブランドに対してフィッシングの脅威が現実となってくることが考えられる．このようなフィッシングにより，損害額補填やサービスレベルの低下といった被害だけではなく，ブランドイメージの失墜や顧客の離散を招く可能性も考えられる．

文　献

[1] 経済産業省・ECOM・NTT データ経営研究所, “平成 16 年度電子商取引に関する実態・市場規模調査”, http://www.meti.go.jp/press/20050628001/e-commerce-set.pdf, 2005.

[2] Anti-Phishing Working Group, “Phishing Activity Trends Report for the Month of January, 2007”, APWG Web Page, http://www.antiphishing.org/

[3] O. Hallaraker and G. Vigna, “Detecting malicious JavaScript code in Mozilla”, Proceedings of the 10th IEEE International Conference on Engineering of Complex Computer Systems(ICECCS'05), pp.85-94 Jun. 2005.

[4] N. Chou, R. Ledesma, Y. Teraguchi and J.C. Mitchell, “Client-side defense against web-based identity theft”, 11th Annual Network and Distributed System Security Symposium (NDSS '04), San Diego, February, 2004.

[5] Rachna Dhamija and J. D. Tygar, “The Battle Against Phishing: Dynamic Security Skins”, Proceedings of the Symposium on Usable Privacy and Security (SOUPS), 2005.

[6] M. Wu, R.C. Miller and S.L. Garfinkel, “Do Security Toolbars Actually Prevent Phishing Attacks?”, Conference on Human Factors in Computing Systems(CHI2006), 2006.

[7] 三重県 総合企画局 広聴広報室, “三重県「ｅ－デモ会議室」におけるサーバへの不正アクセスについて”, 三重県 Web サイト（報告書）, http://www.pref.mie.jp/TOPICS/2005070370.htm, 2005. spoofing.htm, 2004.

[8] T. Jagatic, N. Johnson, M. Jakobsson and F. Menczer, “Social Phishing”, http://www.indiana.edu/ phishing/social-network-experiment/phishing-preprint.pdf, 2005.

[9] Rachna Dhamija, J. D. Tygar and Mrti Hearst, “Why Phishing Works”, Proceedings of the Conference on Human Factors in Computing Systems (CHI2006), 2006.

[10] 杉浦宣彦, “海外調査報告～預金者への補償のあり方と偽造予防策について～”, 金融庁 偽造キャッシュカード問題に関するスタディグループ 資料, Mar. 2005.

[11] 中山靖司, “インターネットバンキングを取り巻く犯罪動向”, 日本銀行 随時公表資料, Jan. 2006. pdf26.pdf.