記者説明会資料

２００４年１１月　５日
独立行政法人　国民生活センター　企画調整課

個人情報を聞き出す「フィッシング」詐欺に要注意

フィッシング（phishing[1)]）とは、金融機関やオンラインショップなどからのEメールを装い、住所、氏名、銀行口座番号、クレジットカード番号、有効期限、ID、パスワードなどの個人情報を返信もしくは入力させてそれらの情報を入手し、金銭を詐取する行為である。

フィッシングの具体的な方法としては、現在のところ、E メールの受信者に対して偽のウェブサイトへアクセスするように仕向け、そのウェブサイトを使って個人情報を詐取する方法（以下、ウェブサイト誘導型という）と、偽のウェブサイトに誘導せずに個人情報を入力した E メールを返信させて個人情報を詐取する方法（以下、E メール返信型という）の 2 つが知られている。フィッシングで使われる E メールやウェブサイトは本物によく似せて作られており、よく見ても本物と見分けがつかないほどのものもあるため、受信者は本物の企業からの E メールと誤信して個人情報を返信・入力してしまう。また、E メールの受信者がフィッシングであることに気づかない場合も多くあると推測されている（参考図）。

アメリカでは、フィッシングによる被害が急激に増加しており、FTC（連邦取引委員会）や司法省などの公的機関や NCL（アメリカ消費者連合）のような消費者団体の他にも、フィッシングに対抗するための業界団体が複数設立され、さまざまな活動を行っている。

また、日本でも YAHOO！JAPAN や JCB などの企業の名前を騙った E メールが既に報告されており、企業や警察庁・経済産業省では注意を呼びかけている。現在までのところ、日本で報告されているフィッシングは E メール返信型が中心であったが、ウェブサイト誘導型も目立ってきている。

国民生活センターにおいては、平成 16 年 10 月までのところ、フィッシングについて寄せられている情報や相談は少ない。しかし、インターネット上でフィッシングに使うための偽のウェブサイトを作るキットが公開されたことなどによって作成方法が広まっていることや、ドイツにおいて英語ではなくドイツ語で書かれたウェブサイト誘導型の E メールが報告されたことから、日本においても日本語で書かれたフィッシング目的の E メール・ウェブサイトが多く発生し、被害が増加する可能性が十分に考えられる。

そこで、フィッシングによる被害が広まる前に、消費者にフィッシングについて認識してもらうことを目的として、その特徴や内外の状況などの情報を提供し、あわせて消費者へのアドバイスを行うこととする。

１．フィッシングの被害

（１）国民生活センターに寄せられた事例

国民生活センターには、平成 16 年 10 月までに、以下のような相談が寄せられている。

・銀行からキャッシュカードについてたずねるメールが届き、個人情報を送信してしまった。至急、キャッシュカードの利用停止手続きを行った。
（40 歳代　男性　給与生活者）

[1)] フィッシングという言葉は、個人情報を「釣る」という意味の“fishing”と、洗練されたという意味の“sophisticated”をあわせた造語、あるいは“password harvesting fishing”の略語、あるいは“fishing”と“phreaking”（ハッキングを表す造語）をあわせた造語であるなど、その由来には諸説がある。

・実在する企業になりすました E メールを、夫が取引のメールだと思って、パスワード、暗証番号、ID、住所、氏名、電話番号、カードの下 4 桁を入力してしまったが、後で全く違うということがわかった。（20 歳代　女性　家事従事者）
・口座を開設していない銀行からＥメールが来る。Ｅメールの中にあるリンクにアクセスすると、クレジットカード番号や暗証番号、名前などの個人情報を記入するよう求められ、その画面から抜け出せないようになっている。これでは騙されてしまう人もいるのではないか。（40 歳代　女性　自営・自由業）

また、国民生活センターの職員のもとには金融機関を騙ったウェブサイト誘導型のフィッシング目的のＥメールと見られるものが複数寄せられている（参考資料１－１～３）。

（２）予想される被害例

フィッシングによって、消費者が受けるおそれがある被害には、次のようなものが考えられる。（ただし、ここにあげた例はあくまで一例であり、これらが被害のすべてというわけではなく、また、これら以外の被害を受けることも十分考えられる。）
・カード決済などの方法でネットショッピングをされる。
・ネットオークションに本人のふりをして出品し、代金を支払わせておいて商品を送らないという詐欺や、逆に商品を落札して商品を入手し、代金を支払わない「取り込み詐欺」をはたらかれ、加害者とされてしまう。
・ネット銀行で、本人の預金が他人の口座に振り込まれ、預金を移される。
・本人の ID やパスワードを使って、企業のネットワークシステムに入り込まれ、企業の情報を盗んだりした加害者とされてしまう。
・キャッシュカードやクレジットカードを偽造され、預金を引き落とされる。
・本人になりすまされて勝手にＥメールの送受信をされる。
・悪質な業者に名簿のような形で本人の情報を売り渡され、ダイレクトメールや勧誘電話などが増える。

また、フィッシングは、消費者のみならず、ターゲットとなった企業に対しても顧客に補償するための費用や ID やパスワードを再発行するための費用、詐欺犯に対する調査や訴訟費用の負担などといった損害を与えることが予想される。

２．フィッシングの現状

（１）アメリカにおける状況

アメリカでは、フィッシングによる被害が急激な増加を見せている。アメリカの調査会社 Gartner,Inc.の調査によれば、アメリカでは明らかにフィッシング目的のＥメールを受け取ったと認識しているインターネットユーザーが約 3000 万人おり、フィッシングのようなものを経験したと感じているユーザーもさらに約 2700 万人いる。そして、これらのうちの約 19%（約 1100 万人）がＥメールに記載された偽のウェブサイトのリンクをクリックし、さらに、約 3%（約 178 万人）が偽のウェブサイト上で個人情報を入力してしまっている。また、フィッシングがアメリカの銀行やクレジット会社に与えた損害額については、2003 年で約 12 億ドルにのぼると推定されている。

フィッシング対策を行っている団体である Anti-Phishing Working Group（APWG）が出した 2004 年 7 月の報告によれば、7 月中に新しく発見されたフィッシング目的のＥメールは 1974 種類で、前月に比べ 40%近く増加している。最も多くフィッシングのターゲットとされた企業は Citibank であり、以下 U.S.Bank , eBay , PayPal , AOL（America Online,Inc.）と続き、金融関係の企業が多い。最も多くフィッシングに使われているウェブサイトのサーバーがあるのはアメリカで、以下韓国、中国、ロシアといった順に続いている。そのようなウェブサイトの存続期間は、平均で 6.1 日であるが、最も長いも

のでは１ヶ月ほどアクセスできたものがあった。なお、APWG は、ウェブサイト（http://www.antiphishing.org）でフィッシングに関する情報を掲載している。

こうした状況に対し、FTC ではフィッシングの仕組みや被害を防ぐためのアドバイスなどを“FTC Consumer Alert”として公表している。また、アメリカ司法省（Department of Justice）でも、フィッシング目的のＥメールに応答することの危険性やフィッシングが法律に反するかどうか、フィッシングにどのような対策をとればよいかなどについて述べたフィッシングに関する特別報告書を公表し、消費者に注意を呼びかけている。小売、通信、金融、ハイテク業界の企業 14 社は、フィッシングを含むインターネット上の詐欺行為に対抗するための団体 TECF（Trusted Electronic Communications Forum）を設立し、国際的な技術標準仕様の策定や各国政府への働きかけといった活動を行っている。また、全米規模で活動する消費者団体である NCL は、フィッシングに大きな関心を持ち、様々な活動を行っている。NCL の NFIC/IFW（詐欺情報センター/インターネット詐欺監視データベース）によると、フィッシングの項目を設けた昨年 12 月以来、フィッシングによる被害の報告はインターネット詐欺のうち 4 番目に多い。NCL は企業と連携してフィッシングに関する公共広告に乗りだし、新しいウェブサイト（http://www.phishinginfo.org）を開設した。そのウェブサイトでは、騙されないための注意や被害に遭った場合の相談先といった情報を掲載している。

（２）日本における状況

日本では、JCB クレジットカードセンターを装ったＥメールが確認され、株式会社ジェーシービーが注意を呼びかけている他、ヤフー株式会社でも YAHOO！JAPAN からであるかのように装ったＥメールについて注意を喚起している。日本クレジットカード協会（JCCA）を装ったＥメールも確認されており、JCCA では注意を呼びかけている。また、銀行やクレジットカード会社などにおいても、自社や JCCA などを装ったＥメールについて注意を呼びかけているところである。

こうした動きに加えて、6 月 4 日には警察庁が“いわゆる「フィッシング」事案への注意喚起について”を公表し、7 月 7 日には経済産業省も“「フィッシング」詐欺にご注意ください”を公表し、消費者に対し注意を呼びかけている（参考資料２）。

現在までのところ、日本で報告されているフィッシングはＥメール返信型が中心であったが、ウェブサイト誘導型も目立ってきている。

（３）フィッシング拡大の懸念

フィッシングは、世界的に広がりつつある。日本では、ウェブサイト誘導型のフィッシングはまだ少ないが、イギリスの法人向けウイルス/スパム対策会社 Sophos Plc.は、本物そっくりの銀行のウェブサイトが簡単に作れるという「フィッシングサイト構築キット」がインターネット上で公開されているのを確認した、と発表している。フィッシングを行うための技術がこのような形で広まれば、今後さらにフィッシングが増加するのではないかという危惧が持たれている。また、フィッシングの方法もさまざまな情報技術と結びついて今後さらに高度化し、広まっていくことが懸念されている。

地域的にみると、これまではアメリカやイギリス、オーストラリアなど英語圏の金融機関がフィッシングのターゲットとなっていたが、最近はブラジルやドイツなどの英語圏以外の地域の金融機関もターゲットとされるようになってきている。ドイツの Postbank は、いくつか文法的な誤りのあるドイツ語で書かれたフィッシング目的のＥメールが送信されていたことを明らかにし、注意を呼びかけている。

これまで、日本において確認されているウェブサイト誘導型のＥメールやウェブサイトの多くは英語で書かれており、入力するよう指示される個人情報もアメリカの社会保障番号（SSN）や母親の旧姓（MMN）など、日本では入力を求められないような情報が入っていたため、偽物であることに気づきやすく、被害に遭いにくくなっていたと考え

られる。しかし、今後、日本においても日本語で書かれたフィッシング目的のEメール・ウェブサイトが多く発生し、被害が増加する可能性は十分に考えられる。

３．消費者へのアドバイス

（１）被害に遭わないために

・金融機関などは個人情報についてEメールを使ってたずねることはしない、ということを理解しておく。
・個人的・金銭的な情報をEメールで送信しない。Eメールは個人情報を送信するのに安全な方法ではないことを理解しておく。
・取引等のために、企業のウェブサイトを使ってそのような情報を提供したい場合は、入力画面上の鍵マークや「https:」で始まるURLなど、そのウェブサイトが安全であるという目印を確認してからにする。ただし、鍵マークなどのセキュリティアイコンを偽造している場合もあるので、目印を過信しない。
・Eメールの添付ファイルにウイルスが存在することもあるので、疑わしいEメールの添付ファイルを不用意に開かない。また、常に最新のウイルス対策ソフトを使う。

（２）個人情報を聞き出すようなEメールが届いた場合

・このようなEメールには応答しない。Eメールの文中に「カードが使えなくなります」などと慌てさせるような記述や、「○○が当たりました」というような記述があっても、その内容を冷静に確認する。
・Eメールに含まれているリンクをクリックしない。本物の企業のウェブサイトからロゴなどをコピーし、それをフィッシング目的のEメールやウェブサイトに置き換えることは簡単にできる、ということを理解しておく。
・Eメールの内容の真偽を確認したいときは、メッセージの中に含まれるリンクをコピーして貼り付けたりしない。新たにブラウザを開いてEメール送信元の企業の正しいウェブアドレスを自分で入力するか検索エンジンで検索した上で、その企業のウェブサイトにアクセスして問い合わせたり、その企業の本物の電話窓口に電話をして確認する。

（３）届いたEメールや、Eメールに含まれるリンクを開いた先のウェブサイトに個人情報を入力してしまった場合

・名前を使われた本物の企業に連絡する。金融機関の場合はすぐに利用停止手続きをとる。
・クレジットカードの利用明細や銀行口座通帳などを定期的にチェックして、身に覚えのない取引（振込・引き落とし等）がないかどうか確認する。身に覚えのない取引に気づいたら、カード会社や銀行にすぐ連絡し、内容を確認する。
・消費生活センターに相談する。
・金銭を騙し取られるなどの被害を受けたら、警察に届け出る。

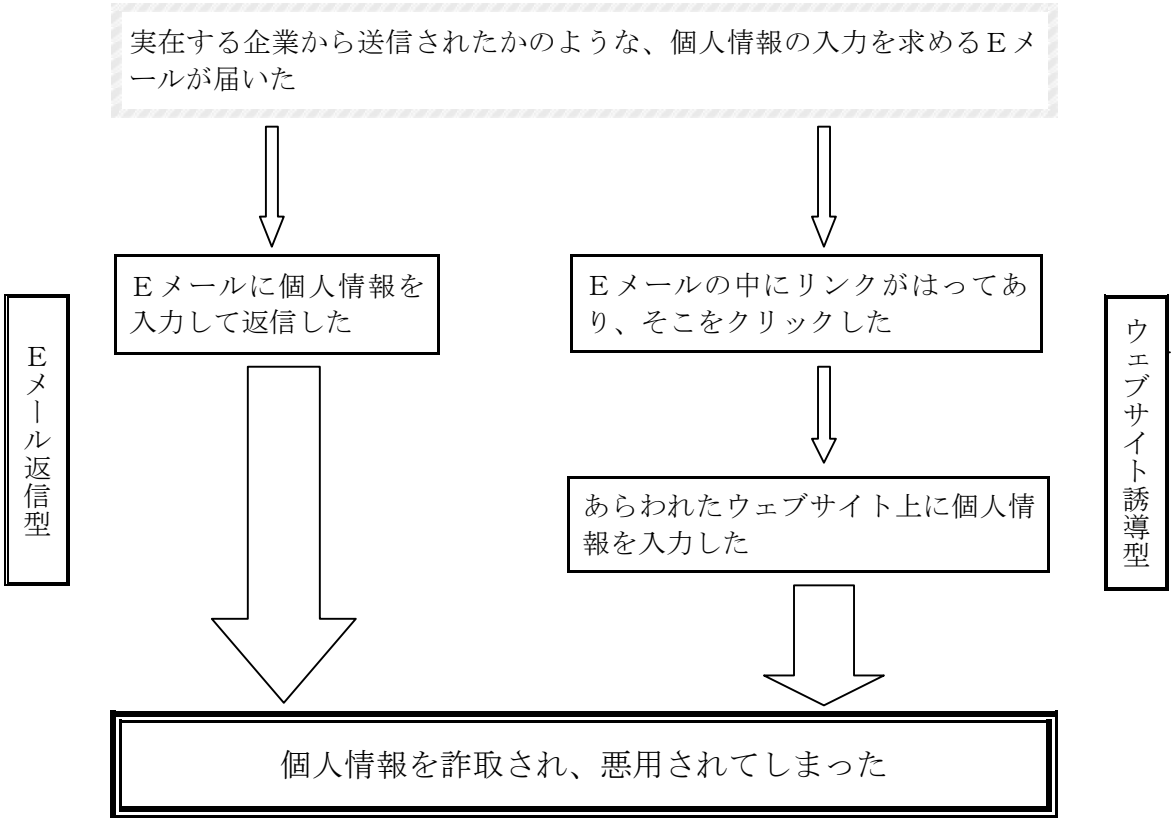
＜参考文献＞

・Anti-Phishing Working Group “Phishing Attack Trends Report-July 2004”，August 2004
・Department of Justice Criminal Division “SPECIAL REPORT ON “PHISHING””，2004
・Federal Trade Commission “How Not Get Hooked by a ‘Phishing’ Scam”，June 2004
・Federal Trade Commission “Is Someone “Phishing” for Your Information？”，June 2004

・Litan,Avivah “Phishing Attack Victims Likely Targets for Identity Theft” Gartner,Inc.， May 2004
・National Consumers League “Group Warns Consumers Not to Take the Bait in Phishing Scams”， August 2004
・National Fraud Information Center/Internet Fraud Watch “January-June 2004 Internet Fraud Statistics”， August 2004
・Sophos Plc. “Do-it-yourself phishing kits found on the internet, reveals Sophos”， August 2004

参考図

【「フィッシング」詐欺の流れ】



本件問い合わせ先

企画調整課：03－3443－6284

参考資料１－１

実在する金融機関から来たかのように装ったEメールの例。Citibankの顧客に対して「最近、顧客の個人情報を盗もうとする事件がたくさん起きています。あなたの口座を守るために、銀行に届けてある内容の詳細を確認してください。この確認は必須のものであり、もしこれをただちに行わない場合は、あなたの口座は一時的に停止されます。」と書いて受信者の不安をあおり、リンク先のウェブサイトへ誘導している。

Dear CitiBank customer,

Recently there have been a large number of identity theft attempts targeting CitiBank customers. In order to safeguard your account, we require that you confirm your banking details.

This process is mandatory, and if not completed within the nearest time your account may be subject to temporary suspension.

To securely confirm your Citibank account details please go to:

https://web.da-us.citibank.com/signin/scripts/login/user_setup.jsp

Thank you for your prompt attention to this matter and thank you for using CitiBank!

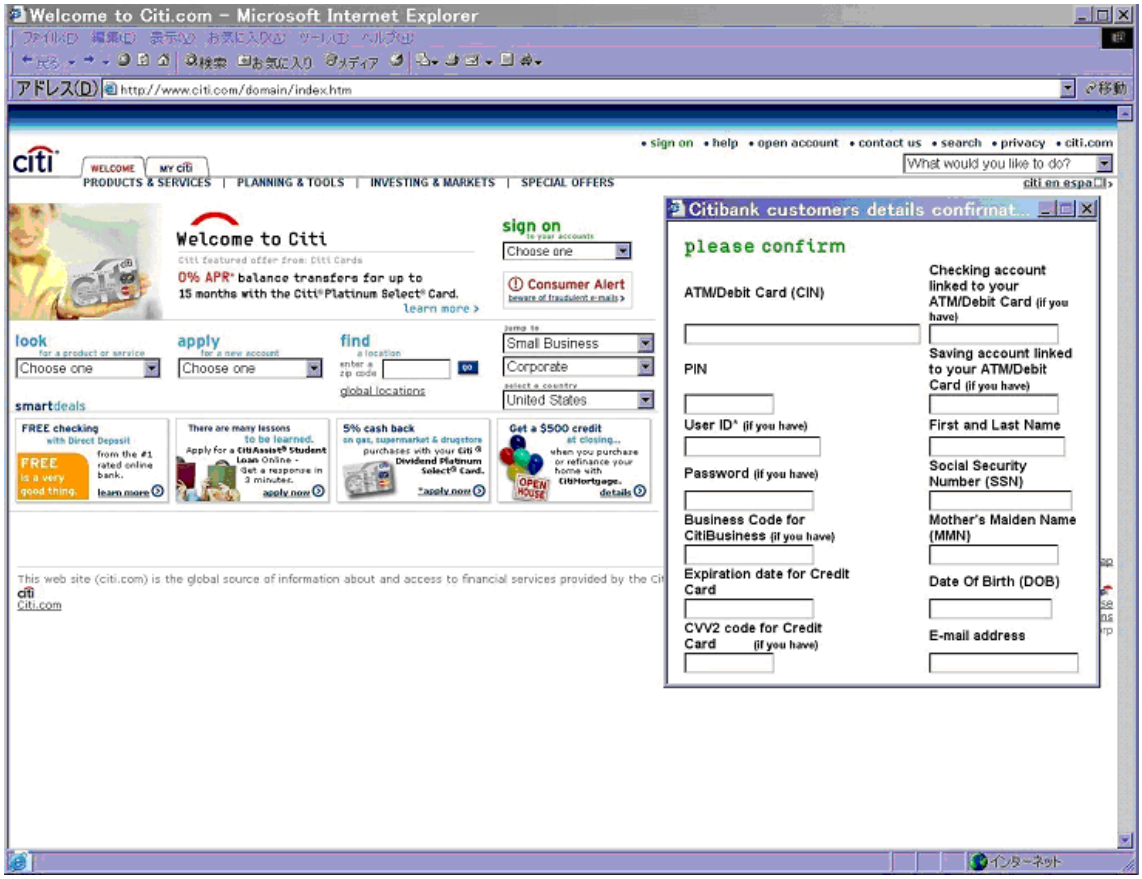
Citi® Identity Theft Solutions

Do not reply to this email as it is an unmonitored alias

A member of citigroup

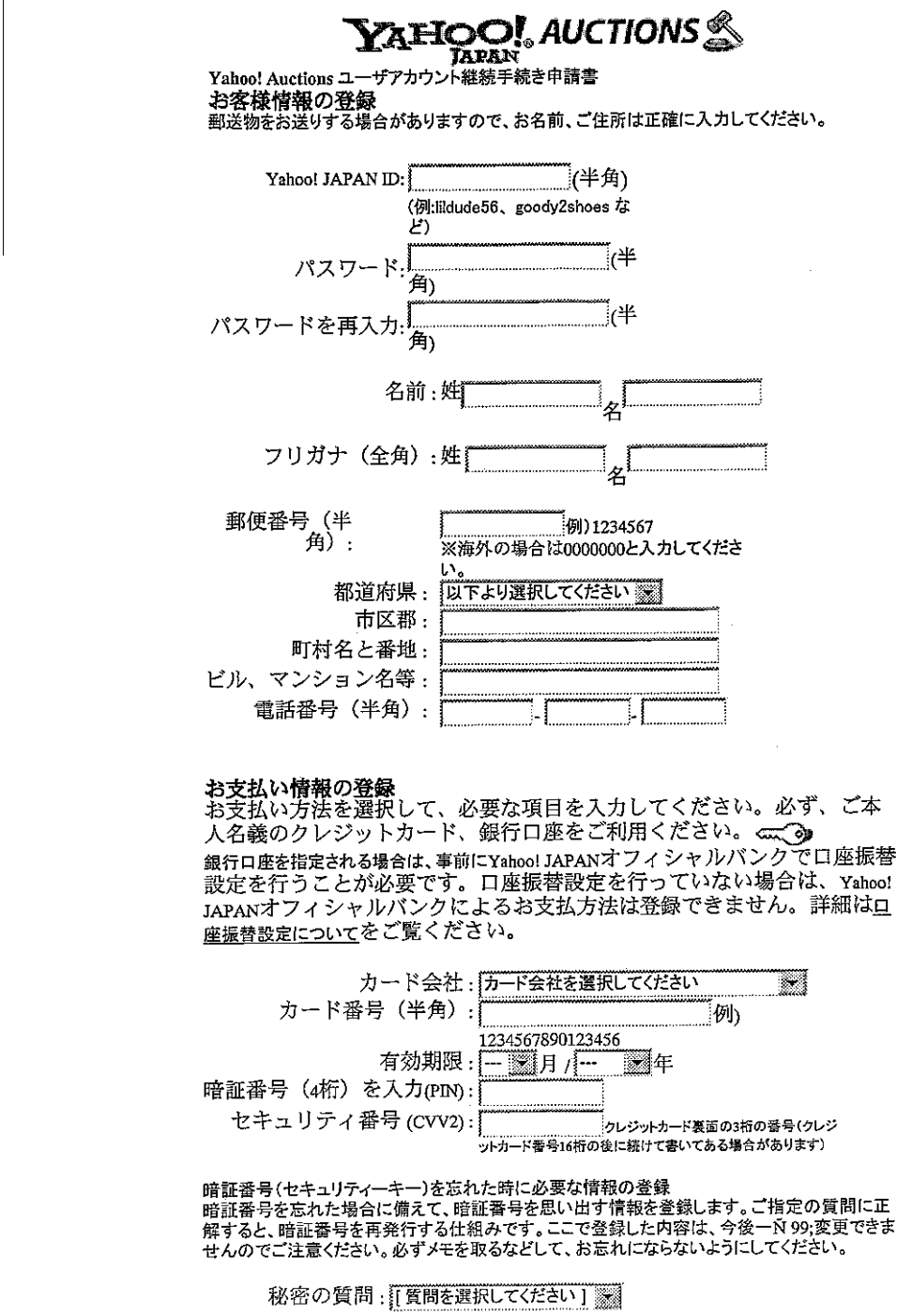
参考資料１－２

参考資料１－１にあげたＥメールの中にあるリンクをクリックすると現われる、偽のウェブサイト。画面の右には、カード番号・暗証番号・ユーザーID・パスワード・クレジットカードの有効期限・口座番号・氏名・社会保障番号・母親の旧姓・誕生日・Ｅメールアドレスといった個人情報を入力させるポップアップウィンドウが出ている。



参考資料１－３

日本語で書かれたフィッシング目的の入力フォームと見られる例。



YAHOO! JAPAN AUCTIONS

Yahoo! Auctions ユーザアカウント継続手続き申請書

お客様情報の登録

郵送物をお送りする場合がありますので、お名前、ご住所は正確に入力してください。

Yahoo! JAPAN ID: (半角)
(例:lildude56、goody2shoes など)

パスワード: (半角)

パスワードを再入力: (半角)

名前 : 姓 名

フリガナ（全角）: 姓 名

郵便番号（半角）: 例)1234567
※海外の場合は0000000と入力してください。

都道府県 : 以下より選択してください

市区郡 :

町村名と番地 :

ビル、マンション名等 :

電話番号（半角）: - -

お支払い情報の登録

お支払い方法を選択して、必要な項目を入力してください。必ず、ご本人名義のクレジットカード、銀行口座をご利用ください。

銀行口座を指定される場合は、事前にYahoo! JAPANオフィシャルバンクで口座振替設定を行うことが必要です。口座振替設定を行っていない場合は、Yahoo! JAPANオフィシャルバンクによるお支払方法は登録できません。詳細は口座振替設定についてをご覧ください。

カード会社 : カード会社を選択してください

カード番号（半角）: 例)
1234567890123456

有効期限 : -- 月 / --- 年

暗証番号（4桁）を入力(PIN) :

セキュリティ番号 (CVV2) : クレジットカード裏面の3桁の番号（クレジットカード番号16桁の後に続けて書いてある場合があります）

暗証番号（セキュリティーキー）を忘れた時に必要な情報の登録
暗証番号を忘れた場合に備えて、暗証番号を思い出す情報を登録します。ご指定の質問に正解すると、暗証番号を再発行する仕組みです。ここで登録した内容は、今後一Ñ 99;変更できませんのでご注意ください。必ずメモを取るなどして、お忘れにならないようにしてください。

秘密の質問 : [質問を選択してください]

秘密の質問の答え：
※「全角ひらがな」か「全角カタカナ」で設定してください。
生年月日：---------- 年 --- 月 --- 日

万一、必要な情報（秘密の質問の答え、生年月日）も思い出せない場合は、公的機関が発行した身分証等をご郵送いただく場合がありますので、ご注意ください。

次へ | キャンセル

「次へ」ボタンを押すと、Yahoo!ウォレットに登録されます。登録手続き完了後、確認メールが届きます。請求書及び領収書などは発行いたしません。
Yahoo!ウォレットの詳しいガイドラインはこちらをご覧ください。

ご登録のお支払方法にご請求できなかった場合にコンビニでのお支払いなどをご案内する場合がございます。

Yahoo! JAPANが提供する商品やサービスの代金のお支払いは、Yahoo!ウォレットに保存されているクレジットカードまたは銀行口座からお支払いいただきます。
また、Yahoo! JAPANの提携先が提供する商品やサービスについて、ユーザーがYahoo!ウォレットに保存されているお支払い方法を指定された場合は、Yahoo! JAPANが代金の収納を代行します。

このページは、情報を暗号化して送受信するSSL（Secure Sockets Layer）技術によって保護されています。

参考資料２

平成１６年6月４日
警　　察　　庁

いわゆる「フィッシング」事案への注意喚起について

１　「フィッシング（Phishing）」とは

「フィッシング（Phishing）」とは、銀行等の企業からのメールを装い、メールの受信者に偽のホームページにアクセスするよう仕向け、そのページにおいて個人の金融情報（クレジットカード番号、ＩＤ、パスワード等）を入力させるなどして個人の金融情報を不正に入手するような行為であり、その情報を元に金銭をだまし取られる被害が欧米を中心に広まっています。今後、日本においても同種の形態による被害が予想されるところです。

２　注意喚起

不自然な形で個人の金融情報（クレジットカード番号、ＩＤ、パスワード等）を聞き出そうとするメールに対しては、メールを送信してきたとされる企業の実際のホームページや窓口に問い合わせて確認するなどご注意下さい。

また、金銭をだまし取られるなど被害を受けた場合は最寄りの警察署までご相談下さい。

平成１６年７月７日
経済産業省

「フィッシング」詐欺にご注意ください

銀行、カード会社等からのメールを装い、メールの受信者に偽のホームページにアクセスするよう仕向け、個人の金融情報（クレジットカード番号、ID、パスワード等）を入力させるなどして個人の金融情報を不正に入手し、その情報を元に金銭をだまし取る行為（いわゆる「フィッシング（Phishing）詐欺」）が米国で広まっており大きな被害が発生しています。今後、日本においても同様な詐欺行為による被害が予想されます。

つきましては、不自然な形で個人の金融情報（クレジットカード番号、ID、パスワード等）を聞き出そうとするメールに対しては、メールを送信してきたとされる企業の実際のホームページや窓口に問い合わせて確認するなどご注意下さい。

<title>個人情報を聞き出す「フィッシング」詐欺に要注意</title>