

月次報告書（2008年11月分）

フィッシング情報届出状況

2008年12月20日

目次

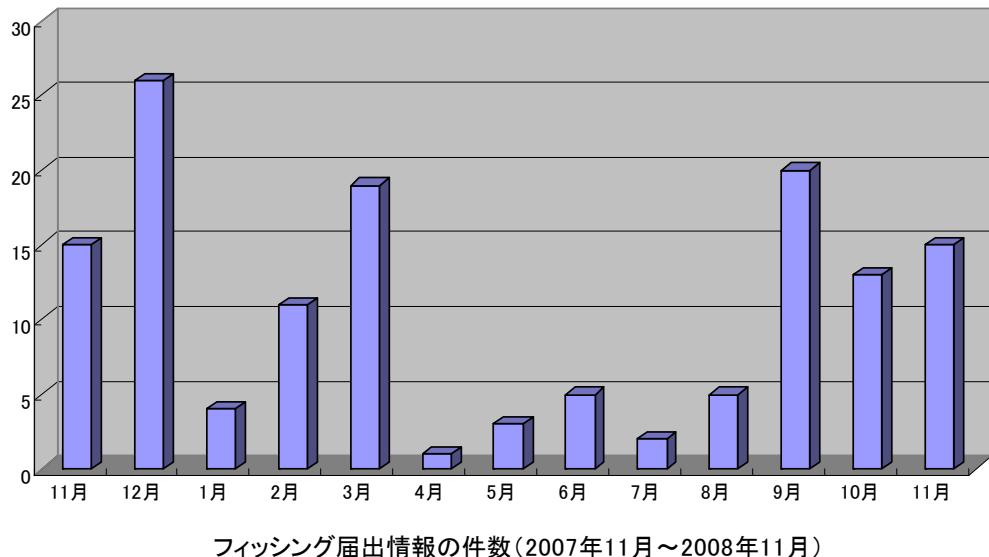
1. フィッシング情報届出状況	2
1.1. フィッシング情報届出状況	2
1.2. 業種別の状況	5
1.3. フィッシングサイトのホスト国	6
1.4. フィッシングメールの動向	7
1.5. フィッシングサイトの動向	14
1.6. フィッシング関連の不正プログラム情報	19
1.7. その他の動向	19
1.8. 総括	19

1. フィッシング情報届出状況

1.1. フィッシング情報届出状況

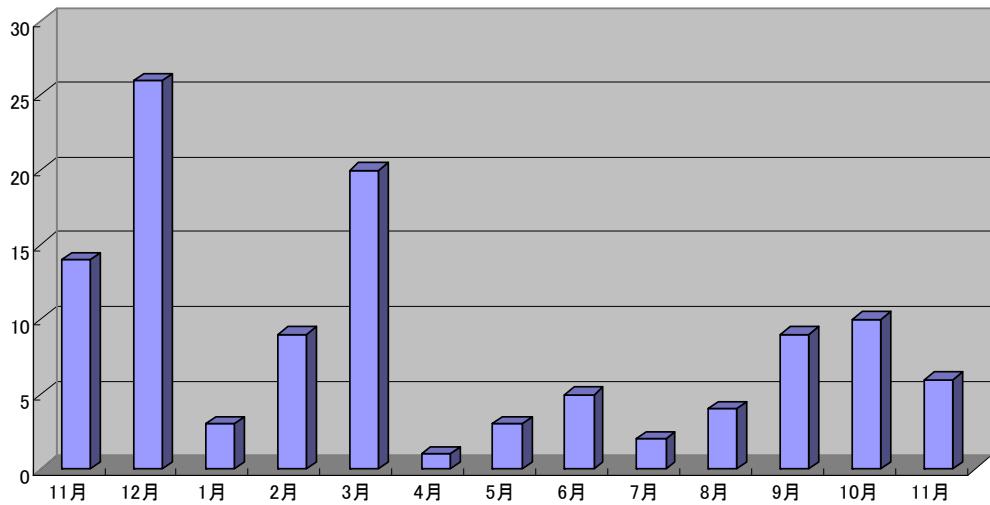
- ・ フィッシングメール届出件数： 15 件

2008 年 11 月度におけるフィッシング情報の届出件数は、前月度より 2 件増加し 15 件となりました。過去 1 年間の平均を上回っています。



・ フィッシングメールの件数： 6 件

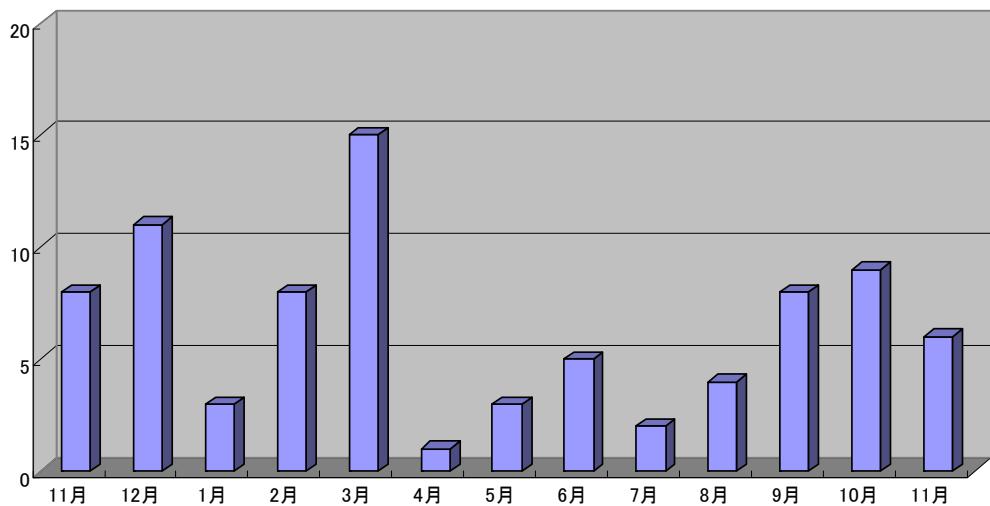
2008 年 11 月度に報告されたフィッシングメールの件数は、前月度より 4 件減少し 6 件となりました。過去 1 年間の平均を若干下回っています。



フィッシングメールの件数(2007年11月～2008年11月)

・ フィッシングサイトの件数： 6 件

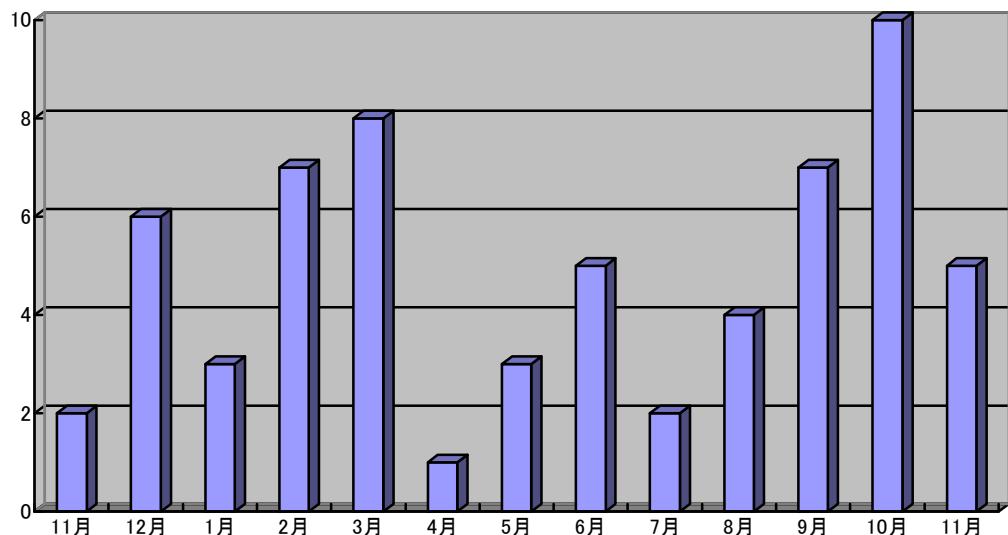
2008 年 11 月度に報告されたフィッシングサイトの件数は、前月度より 3 件減少し 6 件となりました。過去 1 年間の平均とほぼ同じです。



フィッシングサイトの件数(2007年11月～2008年11月)

・ フィッシングによりブランド名を悪用された企業の件数： 5 件

2008 年 11 月度にブランド名を悪用された企業の件数は、前月度より 5 件減少し 5 件となりました。

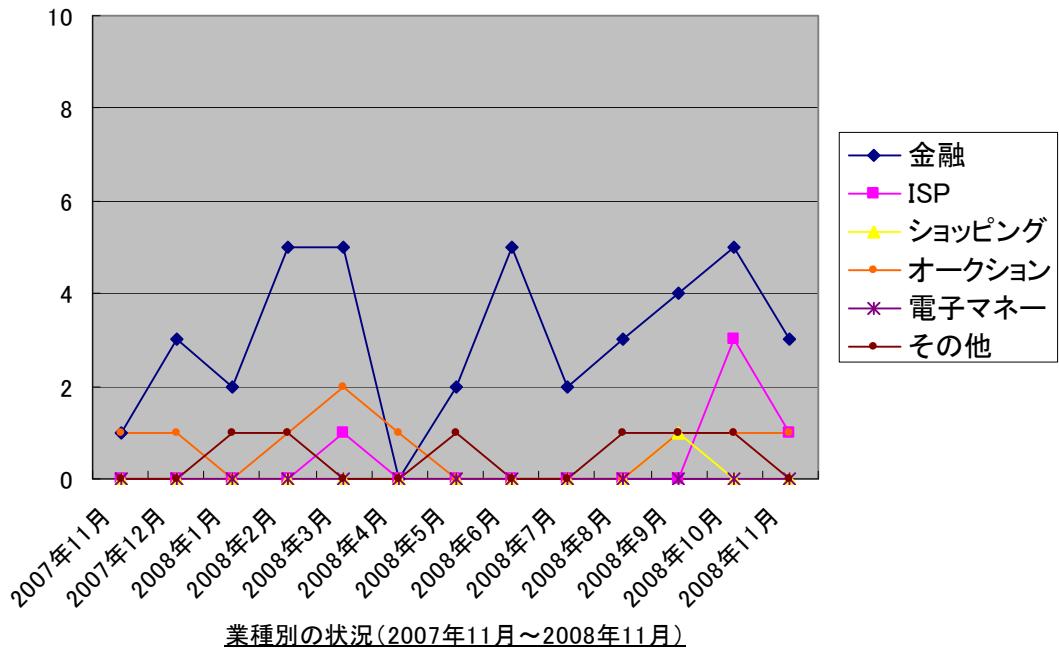


フィッシングによりブランド名を悪用された企業の件数(2007年11月～2008年11月)

・ もっともフィッシングに利用される WEB サイトが多かった国： アメリカ (2 件)、日本 (2 件)、ロシア (1 件)

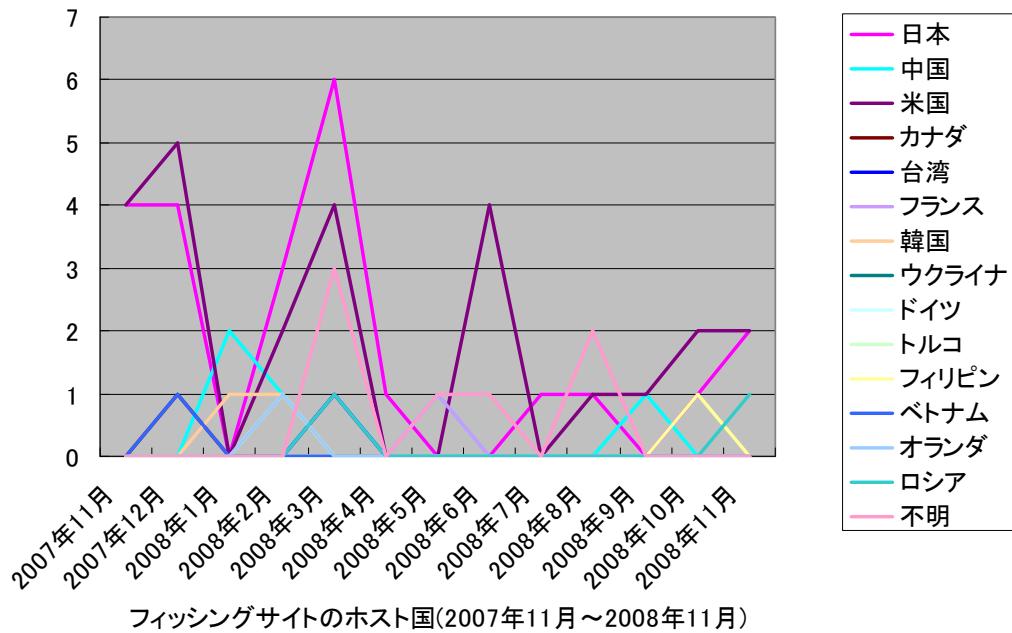
1.2. 業種別の状況

2008年11月度に標的となった業種は、金融が3件、ISPが1件、オークションが1件でした。



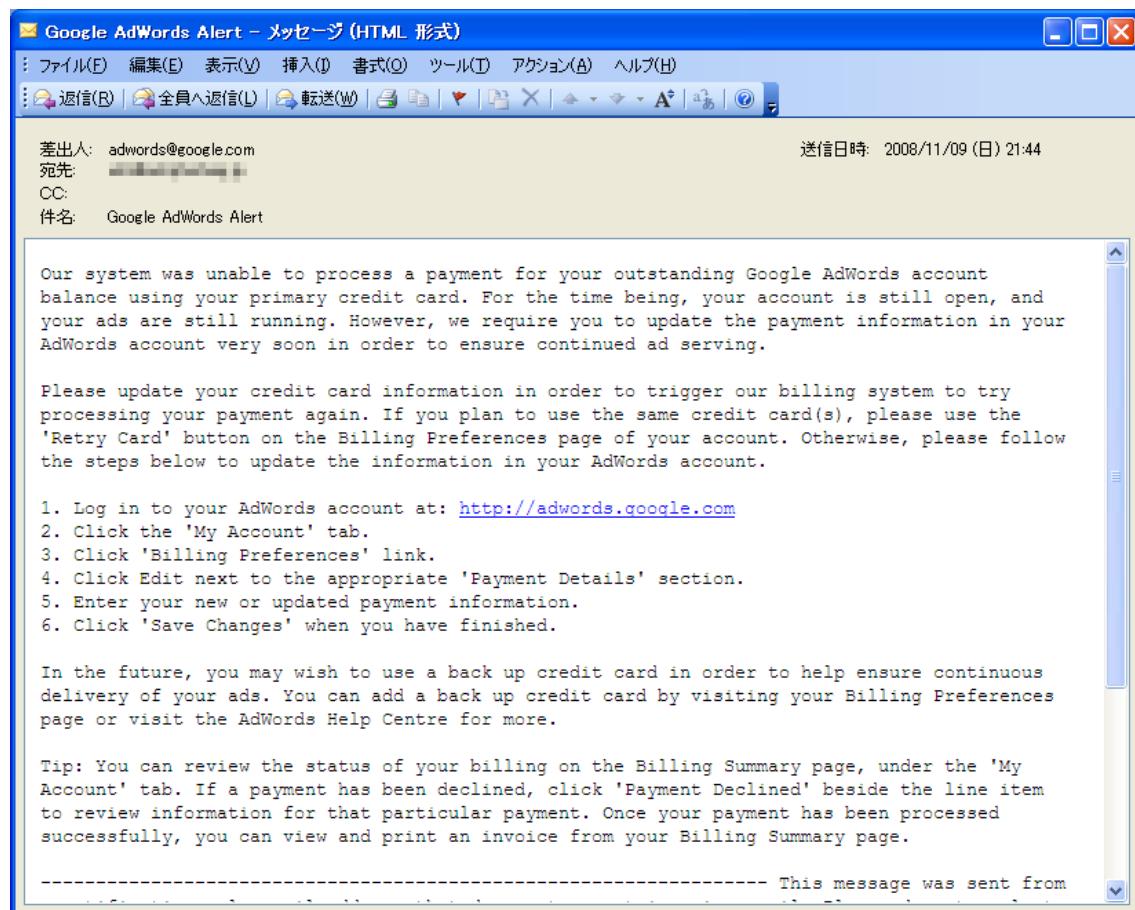
1.3. フィッシングサイトのホスト国

2008年11月度に報告されたフィッシングサイトは、アメリカで2件、日本で2件、ロシアで1件ホスティングされていました。

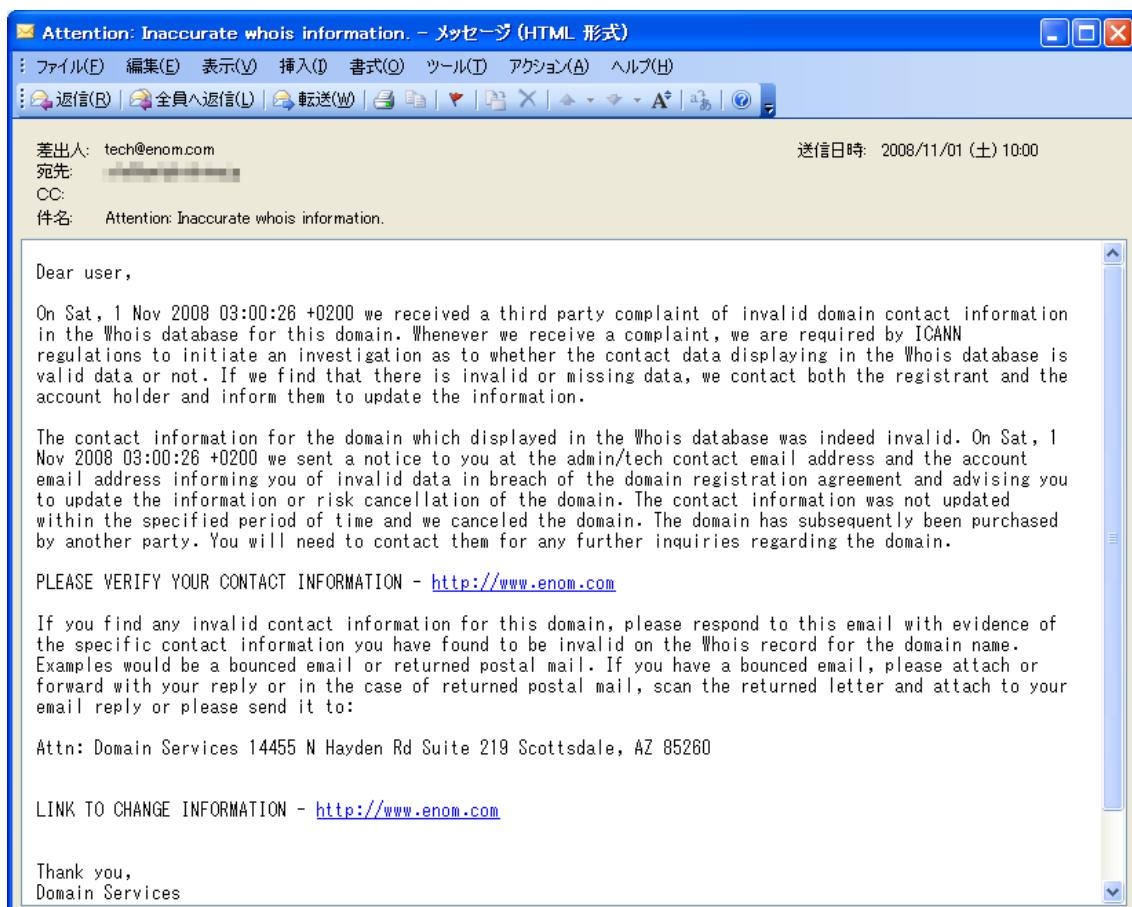


1.4. フィッシングメールの動向

「Google AdWords」をかたるフィッシングメールが確認されました。差出人は「adwords@google.com」、件名は「Google AdWords Alert」で、英語で書かれたHTML形式のメールになっています。メールは、「Google Adwords」の支払いプロセスが実行できないなどとして、クレジットカード情報入力の偽サイトへ誘導しようとします。



先月に引き続き、「Enom.com」をかたるフィッシングメールが確認されました。差出人は「tech@enom.com」、件名は「Attention Inaccurate whois information.」で、英語で書かれたHTML形式のメールになっています。メールは、ドメインの連絡先情報が無効であるという苦情を受けたため、ICANNの規則によって調査を開始しなければならぬとし、登録情報の更新のためとして偽サイトへ誘導しようとします。



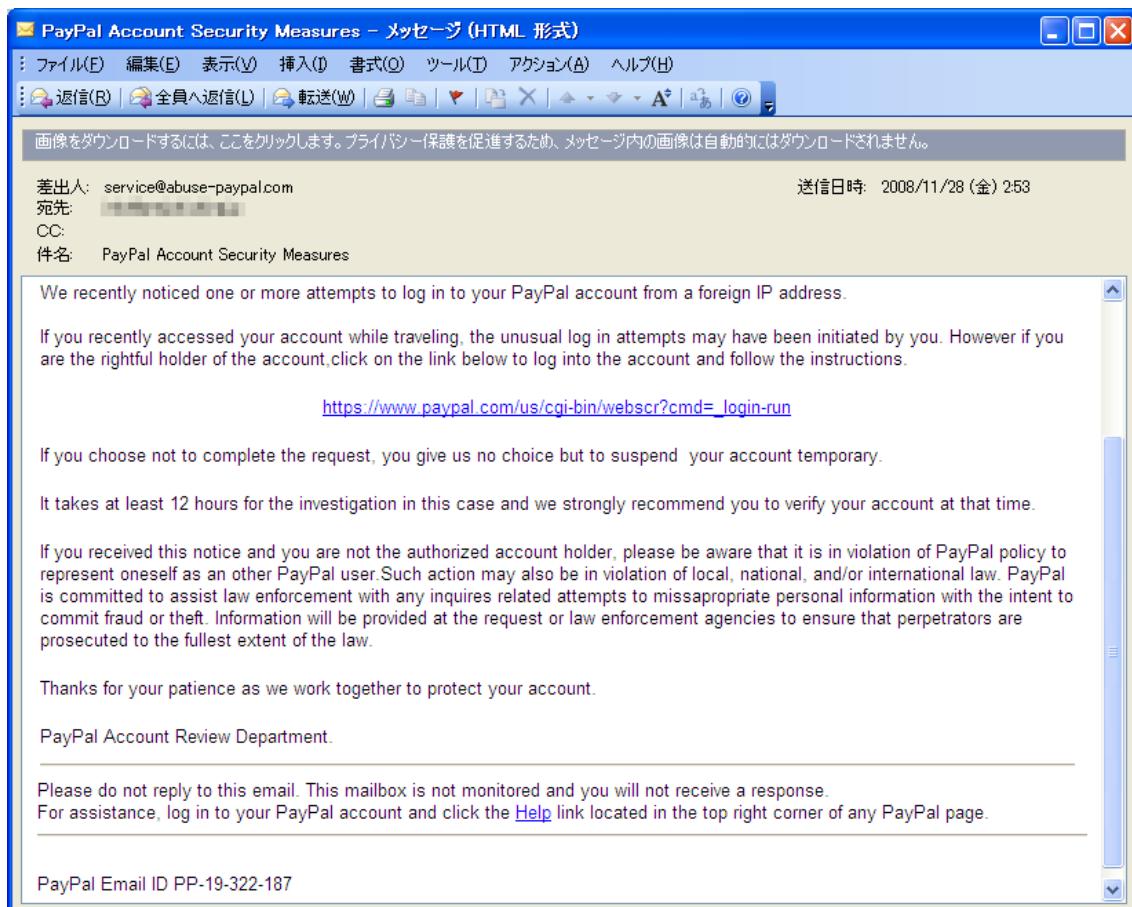
今月新たに、「ジャックス」をかたるフィッシングメールが確認されました。差出人は「gensen@nifty.com」、件名は「■ ジャックスカード おまとめローン 実施中！！」で、日本語で書かれたテキスト形式のメールになっています。メールは、キャッシング詐欺サイトを宣伝し、個人情報を入力させる偽サイトへ誘導しようとします。



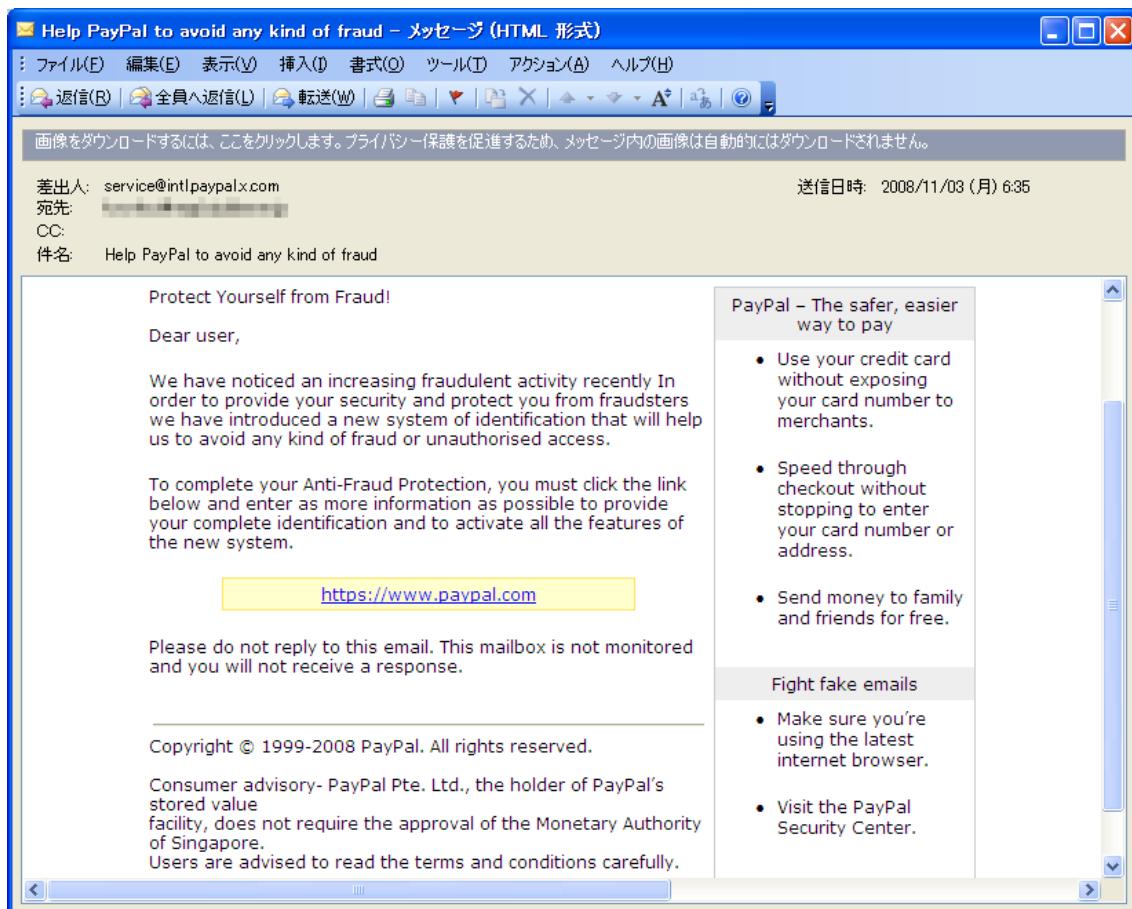
「オリコ」をかたるフィッシングメールが確認されました。差出人は「gen5454@nifty.com」、件名は「■ オリコグループのネット専用キャッシング」で、日本語で書かれたテキスト形式のメールになっています。メールは、キャッシング詐欺サイトを宣伝し、個人情報を入力させる偽サイトへ誘導しようとします。



先月に引き続き、「PayPal」をかたるフィッシングメールが確認されました。差出人は「service@abuse-paypal.com」、件名は「PayPal Account Security Measures」で、英語で書かれたHTML形式のメールになっています。メールは、ユーザの「PayPal」口座に外国からログインがあり、ユーザが正規の利用者か確認するためとして口座情報の入力偽サイトへ誘導しようとします。



先月に引き続き、「Paypal」をかたるフィッシングメールが確認されました。差出人は「service@intl.paypal.x.com」、件名は「Help PayPal to avoid any kind of fraud」で、英語で書かれたHTML形式のメールになっています。メールは、近年のフィッシング詐欺の増加に伴い、「PayPal」に新規のセキュリティシステム導入が予定されており、システムの有効化のため登録作業が必要だとして偽サイトへ誘導しようとします。



先月に引き続き、「Yahoo! オークション」をかたるフィッシングメールが確認されました。先月出回っていたフィッシングメールと文面、書式が似ており差出人は「cly35860@pop26.odn.ne.jp」、件名は「Yahoo!オークションのご利用に関するお知らせです。※重要！！」で、日本語で書かれたテキスト形式のメールになっています。メールは、Yahoo!オークションを引き続き利用するためにYahoo! JAPAN ID ユーザーアカウント更新手続きが必要だととして偽サイトに誘導しようとします。



1.5. フィッシングサイトの動向

「Google Adwords」をかたるフィッシングサイトは、正規のログインサイトを装いGoogleアカウントの登録メールアドレス、パスワードを盗み出そうとします。サイトはアメリカのサーバでホスティングされていました。

The screenshot shows a fake Google AdWords landing page. At the top left is the Google logo with 'AdWords' underneath. To the right is a language dropdown set to 'English (US)'. A large blue button on the right says 'Try AdWords now'. Below the button, there's a link to 'Sign in to Google AdWords with your Google Account'. On the left, there's a diagram showing a hand cursor pointing at a box labeled 'Your ad here' which contains the URL 'www.your-company-site.com'. The diagram also shows a search results page with ads and a building icon. On the right, there's a section for logging in with fields for 'Email' and 'Password', and a 'Sign in' button.

The screenshot shows a 'Learn about AdWords' page. On the left, there's a sidebar with links: 'How it works', 'Reach more customers', 'Costs and payment', 'For local businesses', and 'Success stories'. The main content area has several sections: 'You create your ads' (with a link to 'Get keyword ideas'), 'Your ads appear on Google' (with a link to 'See your ad on Google'), 'You attract customers' (with a link to 'Create your ad'), and 'Sign up now | Next topic»'. There are also two small images of Google search results pages, one for 'Keywords' and one for 'Your ad appears beside relevant search results'. A green hand cursor points at the 'Create your ad' link in the 'You attract customers' section.

「Enom. com」をかたるフィッシングサイトは、正規の Enom. com サイトを装いアカウントの登録 ID、パスワードを盗み出そうとします。サイトはアメリカのサーバにホスティングされていました。

The screenshot shows the Enom.com website. At the top, there's a blue header bar with the Enom logo, navigation links like 'Register', 'Transfer', 'Whois', and a search bar. Below the header, there's a main content area divided into two sections: 'New to eNom?' on the left and 'Log-in to your Account' on the right.

New to eNom?

Apply for an eNom reseller account - it's a breeze to set up and manage all of your domain names and services.

- ▶ **Account Manager**
Easy management of your domain names, hosted or not.
- ▶ **Versatile Product Suite**
A full product suite is available to you to better maintain your accounts.
- ▶ **FREE Services**
eNom offers FREE Services that are available to you as well!

ICANN ACCREDITED

[Learn more](#)

Log-in to your Account

Enter your Log-in ID and Password.

Log-in ID:

Password:

Remember my Log-in ID
 Keep me logged-in on this computer.

log-in

By logging in to this site you agree to all the [terms & conditions](#).

[log-in help](#) | [lost password?](#)

At the bottom of the page, there are links for 'About Us', 'Help', 'Careers', 'Services', 'News', 'Pricing', 'Statistics', 'Maintenance', 'Press Releases', 'Whois', and 'Site Map'. There are also sections for 'Awards & Achievements' (with logos for ICANN, BBB, and Registrar Reseller) and 'Payment Options' (with logos for PayPal, VISA, MasterCard, American Express, and Discover). A copyright notice at the bottom states 'Copyright © 1998-2008 eNom Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Policy](#)'.

「ジャックス」をかたるフィッシングサイトは、融資の自動診断としてメールアドレス、名前、携帯電話番号などを盗み出そうとします。サイトは日本のサーバにホスティングされていました。

参考情報)

【ご注意】弊社名および弊社と紛らわしい名を名乗る団体について（ジャックス）

http://www.jacccs.co.jp/information/attent_ruiji.html

The screenshot shows the homepage of the JACCS Corporation website. The header includes the company logo, navigation links for HOME, ご利用方法, 商品のご案内, and 会員様ログイン, and links for 会社概要, Q & A, プライバシーポリシー, and キャンペーン情報.

The main content features a large image of a man in a suit looking up at a modern building, with the text "毎日の暮らしの中に、いつもジャックス". To the left is a sidebar with links for お申し込み, Q & A, プライバシーポリシー, and 会社概要.

A central box titled "自動診断" contains a form for a loan application. It includes fields for 希望金額 (Loan amount), メールアドレス (Email address), お名前 (Name), 携帯電話番号 (Mobile phone number), 生年月日 (Date of birth), お住まいの地域 (Residence area), and ご連絡可能な時間帯 (Available time for contact). A note at the bottom states "* 全て入力せんと、自動返信できません". Buttons for 診断 (Diagnose) and 取消 (Cancel) are at the bottom.

To the right of the diagnosis form is a red warning box titled "こんな手口に注意!" containing the text: "悪質な振込み詐欺の被害が急増しています。090金融などにご注意下さい。"

「オリコ」をかたるフィッシングサイトは、融資のお試し診断としてメールアドレス、名前、携帯電話番号などを盗み出そうとします。サイトは日本のサーバにホスティングされていました。

参考情報)

当社名称及び当社の類似名称を名乗る金融業者（オリコ）
http://www.orico.co.jp/school/security/info_01.html

The screenshot shows a web page for 'Orico Group Network専用キャッシング'. The header includes the Orico logo and the text 'オリコグループ ネット専用キャッシング'. The left sidebar has a vertical navigation menu with links: HOME, ご利用方法, 商品のご案内, シュミレーション, お申し込み, 会員様ログイン, Q&A, プライバシーポリシー, and 会社概要. Below this is a contact information section with address, phone number, and fax number. The main content area features a photograph of a laptop keyboard and a CD. A promotional message reads: '新規ご契約のお客様には、もれなく5万円分の商品券をプレゼント!!'. There are two main informational boxes: 'お試し診断' (Diagnostic Test) and 'キャンペーン情報' (Campaign Information). The 'お試し診断' box contains fields for希望金額 (Loan Amount), メールアドレス (Email Address), お名前 (Name), 携帯電話番号 (Mobile Phone Number), 生年月日 (Date of Birth), お住まいの地域 (Residence), and ご連絡可能な時間帯 (Available Contact Time). It also includes a note: '* 全て入力せんと、自動返信できません' and buttons for '診断' (Diagnose) and '取消' (Cancel). The 'キャンペーン情報' box contains text about interest rates and application times. At the bottom right, there is a 'ご注意' (Attention) box warning about phishing attempts. The footer contains the copyright notice: 'Copyright(c)2008 ORICO SHINPAN All Rights Reserved.'

「PayPal」をかたるフィッシングサイトは、正規の PayPal ログインサイトを装い、アカウントの登録メールアドレス、パスワードを盗み出そうとします。サイトはロシアのサーバにホスティングされていました。

Sign Up | Log In | Help | Security Center | Search

PayPal U.S. English ▾

Home | Personal | Business | Products & Services

Account login 

Email address

PayPal password

Log In

Forgot your [email address or password?](#)

New to PayPal? [Sign up](#)

Did you know?



With PayPal, you can pay with a credit or debit card, bank account or PayPal balance.

About | Accounts | Fees | Privacy | Security Center | Contact Us | Legal Agreements | Developers | Jobs | Merchant Services | Mobile | Plus Card | Referrals | Shops | Mass Pay



Copyright © 1999-2008 PayPal. All rights reserved.
[Information about FDIC pass-through insurance](#)

Home | Personal | Business | Products & Services

1.6. フィッシング関連の不正プログラム情報

特にありません。

1.7. その他の動向

US-CERT（米政府系組織のコンピュータ緊急事態対策チーム）は、米国の連邦準備制度をかたるフィッシングメールについて警告を行いました。メールには、フィッシング詐欺の発生が報告されており、詳細情報として、PDF の脆弱性を悪用する不正な Web サイトの URL が記載されています。

関連 URL :

U.S. Federal Reserve Fraudulent Email Scam 2008/11/13 (US-CERT)

http://www.us-cert.gov/current/archive/2008/11/18/archive.html#u_s_federal_reserve_phishing

Bogus Federal Reserve Sites Deliver PDF Exploit 2008/11/13 (TrendLabs)

<http://blog.trendmicro.com/bogus-federal-reserve-sites-deliver-pdf-exploit/>

1.8. 総括

今月度は、新たに「ジャックス」をかたるフィッシングメールおよびサイトを確認しました。同様にクレジットカード会社をかたるものとして「オリコ」のフィッシングも確認されており、両方ともメール、サイトが非常に良く出来ているため、ログイン、パスワード等の入力を行わないよう引き続き十分な注意が必要です。

その他のフィッシングは以前から出回っている「Google Adwords」、「Enom.com」、「PayPal」、「Yahoo! オークション」などでメールの内容、サイトも同じものでした。但し、サイトのホスティング場所は変わっており、今後もホスティング場所を変えながら同様のブランドをかたるフィッシング詐欺が繰り返されることが予想されます。