

2008年6月5日

フィッシング対策に関する事業者調査について

フィッシング対策協議会

フィッシング対策協議会(事務局:財団法人 日本情報処理開発協会 電子商取引推進センター)は、2007年11-12月に金融機関等フィッシング詐欺被害の対象となり得る事業者を対象とした「フィッシングに関する事業者調査」を実施し、その調査結果をまとめました。

調査の背景

米国 Anti-Phishing Working Group (APWG)によれば、フィッシング事例の報告件数は2万件/月を超えています。日本国内においても、フィッシング対策協議会へのフィッシング事例の報告件数は APWG より少ないものの、2007年夏頃より日本のインターネットバンキングをかたるフィッシング事例の報告や報道も増え、今後、米国と同様に事例や被害が増加していくことが懸念されます。

このような状況において、フィッシング詐欺に対する事業者側の対策の現状と動向を踏まえた、フィッシング対策協議会及び事業者における効果的施策検討に資することを目的として、この度「フィッシング対策に関する事業者調査」を実施しました。今回の調査では銀行などの金融機関に重点を置き、さらに通販/EC事業者なども対象とした調査を実施しました。

結果要旨

- フィッシング被害¹経験に関し「ほとんどの事業者が被害にあつたことがない(96.7%)」と回答しています。
- フィッシング被害防止の「対策をしている」と回答した事業者は72.2%でした。ただし回答者母数にはネット取引サービスを提供していない事業者(8.5%)も含まれるので、ネット取引サービス事業者内での比率はもっと多くなると考えられます。
- 採用している対策としては【SSL】(90.8%)が最も高く、【注意喚起や顧客啓発】(80.4%)が続き、それ以下を大きく引き離している。その後は【乱数表カード】(36.6%)、【フィッシング対策ツール・システム】(22.2%)、【ワンタイムパスワード】(19.6%)の順となります。
- 今後強化予定の対策手段としては、【ワンタイムパスワード】が27.8%と他のカテゴリより高く、【注意喚起や顧客啓発】(23.6%)、【EV SSL】が20.8%、【フィッシング対策ツール・システム】(17.9%)も、他のカテゴリより比較的高い結果となりました。
- フィッシング防止対策を実施する理由としては、「顧客に安心してサービスを利用いただくため」が92.8%と最も高く、「顧客を守るため」が87.6%で続き、顧客を重視した企業意識の高さが伺えます。

¹本調査における被害とは顧客の金銭的実害発生の有無には依らず、社名やサービス名等ブランドやログイン画面等が不正使用されたフィッシング詐欺行為が行われた場合としている。

す。

まとめと今後

本調査はブランドを偽られて使用されることによるフィッシング被害の対象となり得る金融機関、事業者及びその防御技術を開発・提供するベンダ等にとって、フィッシング対策推進の参考になると期待しています。

フィッシング対策協議会では、今回の調査結果から得られた情報をもとに、例えばフィッシング対策ガイドライン策定への反映等、効果的なフィッシング対策を促進するための活動を検討・実施してまいります。

報告書

「フィッシング対策に関する事業者調査」はフィッシング対策協議会のホームページ (<http://www.antiphishing.jp/>)にて6月5日より公開いたします。

お問合せ

本件に関するお問合せ先は次の通りです。

財団法人 日本情報処理開発協会 電子商取引推進センター内

フィッシング対策協議会事務局 山田、合原

TEL: 03-3436-7517, FAX: 03-3436-7570

e-mail: antiphishing-sec@ecom.jp

フィッシングとは

フィッシング (Phishing) とは、金融機関(銀行やクレジットカード会社)などを装った電子メールを送り、住所、氏名、銀行口座番号、クレジットカード番号などの個人情報を詐取する行為です。電子メールのリンクから偽サイトに誘導し、そこで個人情報を入力させる手口が一般的に使われています。

フィッシング対策協議会について

フィッシングに関する情報収集・提供、注意喚起等の活動を中心とした対策の促進を目的に設立された任意団体であり、金融業界、クレジットカード業界、ネットショッピング業界、対策事業者・対策機関などの事業者から構成されます。また、関係府省庁、関係対策機関がオブザーバとして参画しています。

Anti-Phishing Working Group (APWG) について

Anti-Phishing Working Group (<http://www.antiphishing.org/>) は、顕著になりつつあるフィッシン

グや e メール・スプーフィングの問題に起因する個人情報の窃盗および詐欺行為の撲滅対策を中心課題として米国で活動する産業界連合団体です。この連合団体では、フィッシング問題について討議し、ハードおよびソフトのコスト面からフィッシングの問題範囲を定義し、問題解決のための情報と最良の実践例を共有するためのフォーラムを提供します。また、必要に応じ APWG はこれらの情報を司法当局と共有する意向を持っています。(APWG のレポートより抜粋)

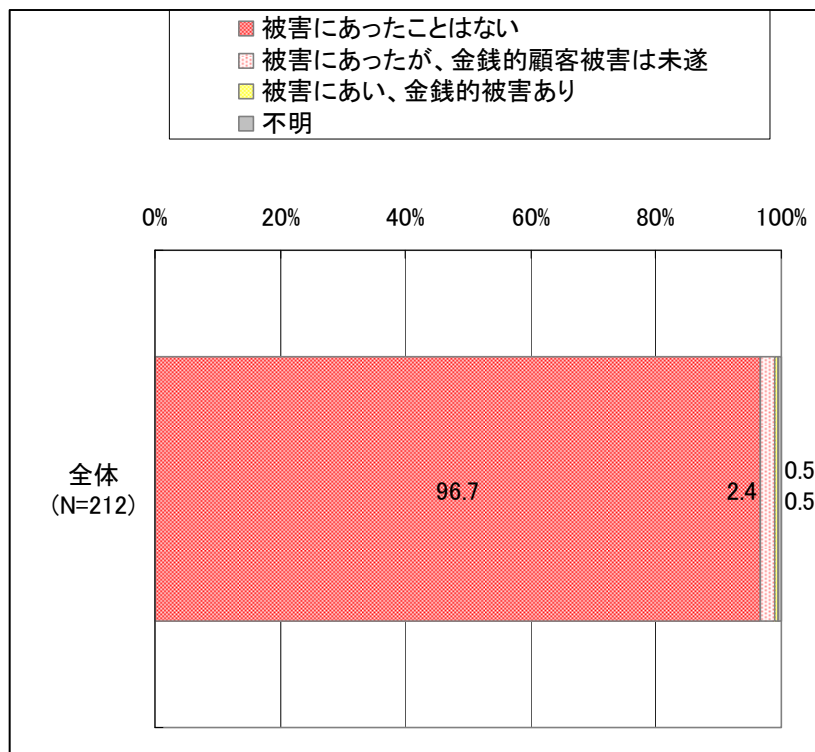
アンケート結果資料

1. 調査概要

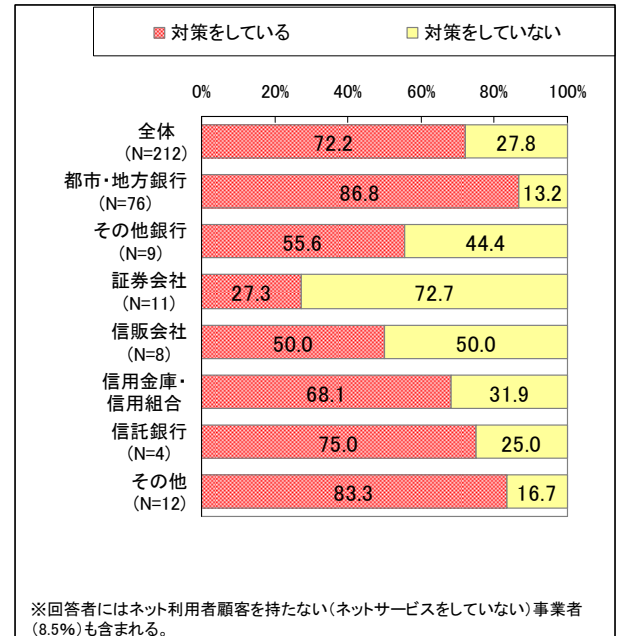
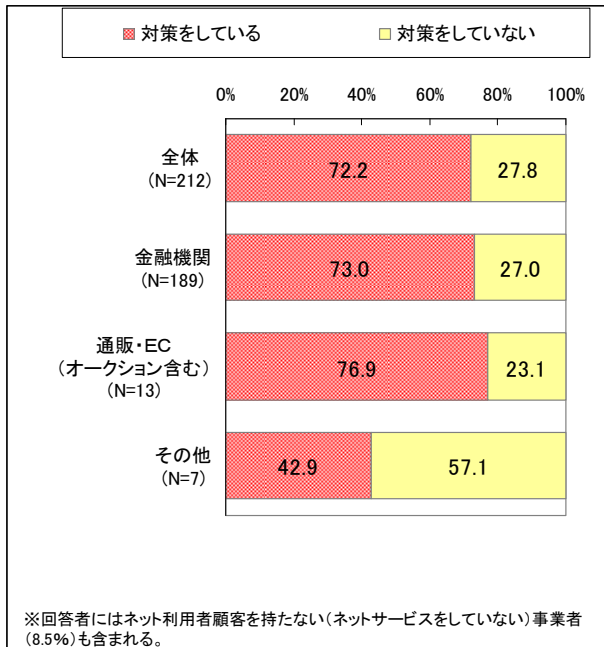
- (1) 調査方法: 郵送調査(一部電子メールによる調査票調査)
- (2) 調査対象: フィッシング被害の対象となる事業者
- (3) 調査期間: 2007年11月7日~12月17日
- (4) 依頼方法: 事前依頼電話架電または業界団体経由
- (5) サンプル数: 212件(調査票発送/配信 665件)

2. アンケート結果概要

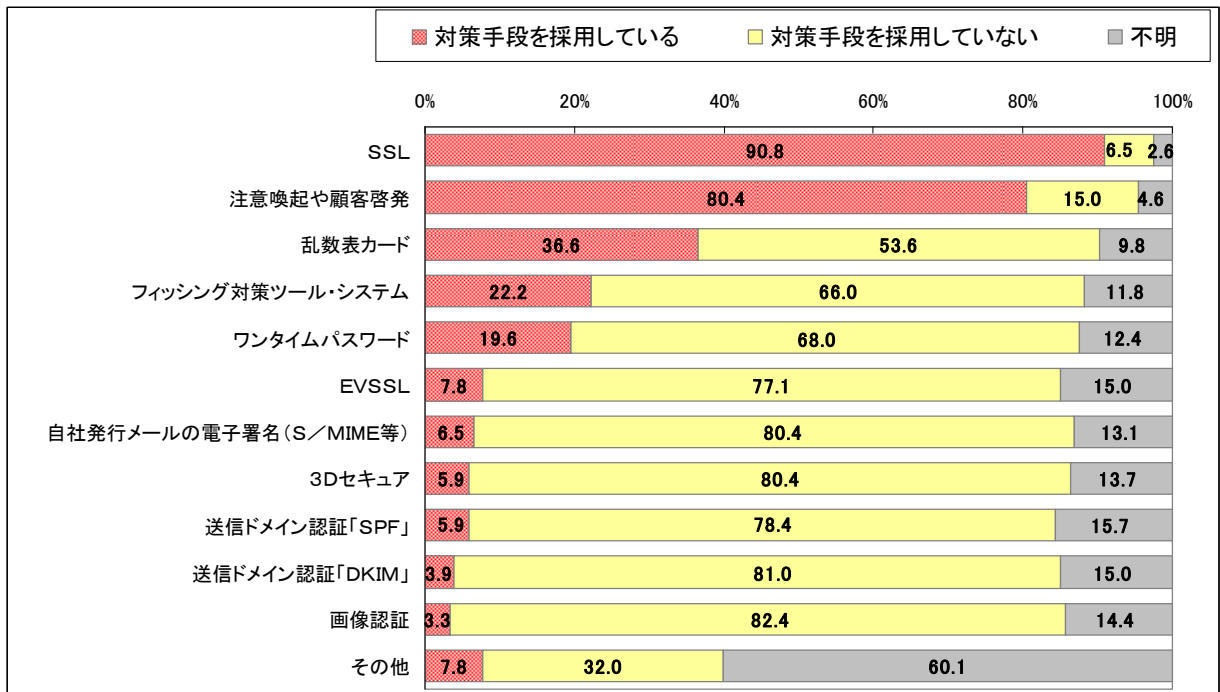
(1) 事業者の被害経験に関し、ほとんどの事業者が「被害にあったことがない(96.7%)」と回答しているが、「被害にあったが、金銭的顧客被害は未遂」(2.4%(5件))、「被害にあい、金銭的被害あり」(0.5%(1件))という事業者も存在する。



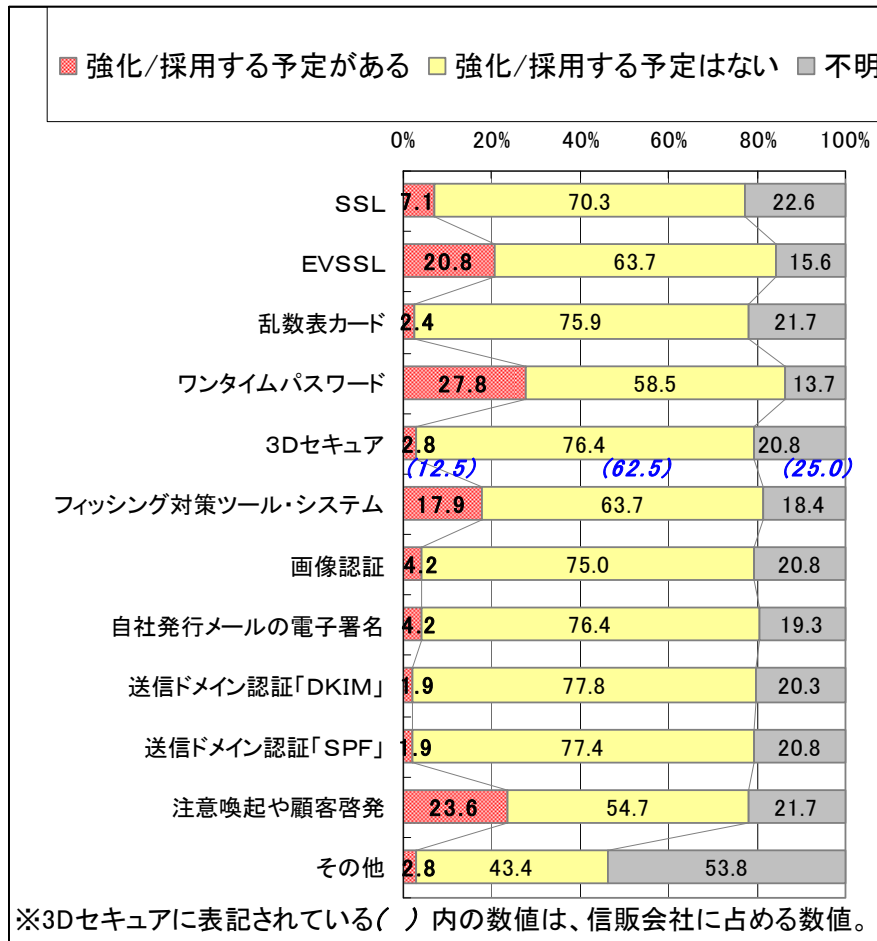
(2)フィッシング被害防止の「対策をしている」(72.2%)と回答した事業者は7割である。(但し回答者にはネット取引サービスを提供していない事業者も8.5%含まれる)。都市銀行は86.8%が被害防止対策済みとなっている。



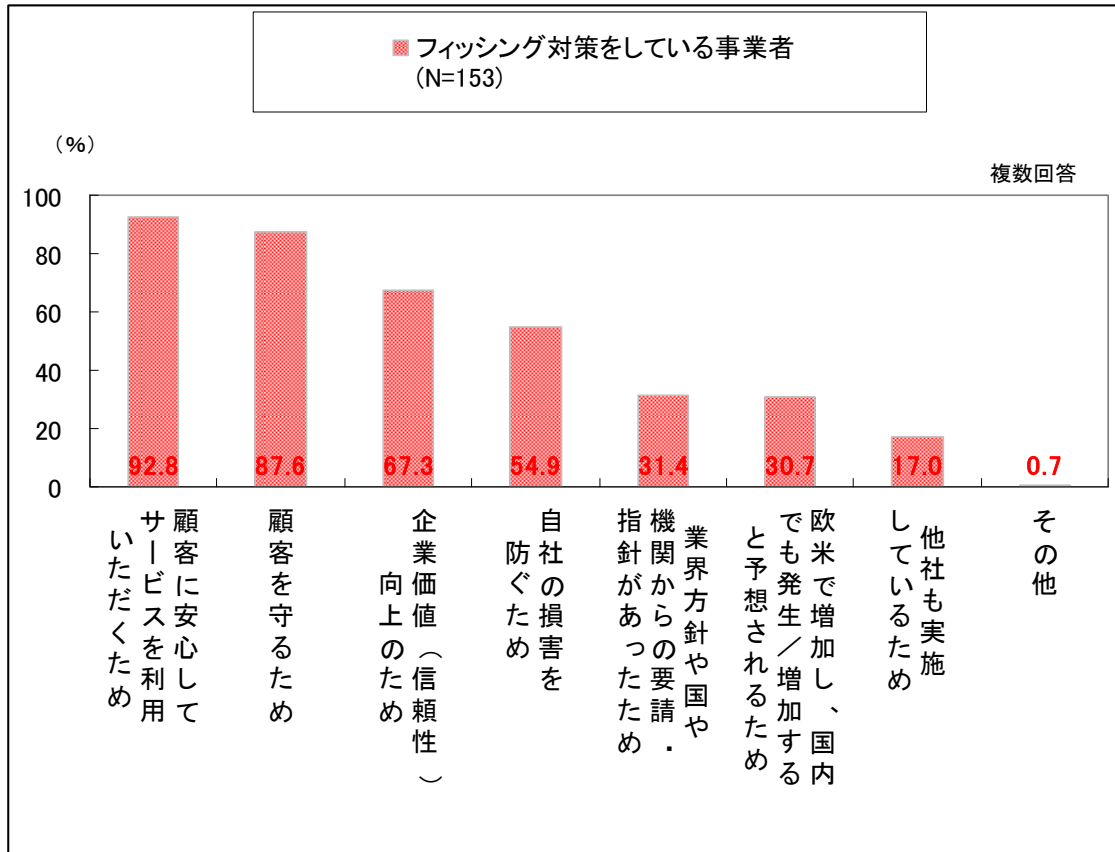
(3)採用している対策としては【SSL】(90.8%)が最も高く、大多数の事業者が採用している。【注意喚起や顧客啓発】(80.4%)が続き、それ以下を大きく引き離している。【乱数表カード】(36.6%)、【フィッシング対策ツール・システム】(22.2%)、【ワンタイムパスワード】(19.6%)と続く。



(4) 今後強化／採用する予定の対策としては、【ワンタイムパスワード】は「強化／採用する予定がある」(27.8%)が他のカテゴリより高く、【注意喚起や顧客啓発】(23.6%)、【EV SSL】(20.8%)、【フィッシング対策ツール・システム】(17.9%)も、他のカテゴリより比較的高い。



(5)フィッシング防止対策を実施する理由としては、「顧客に安心してサービスを利用いただくため」(92.8%)が最も高く、後に「顧客を守るため」(87.6%)が続き、顧客を重視した企業意識の高さが伺える。



以上