

2008年9月10日

「フィッシング対策ガイドライン」の発表について

～ 日本初のフィッシング詐欺対策指針 ～

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)では、フィッシング詐欺被害の対象となり得るサービス事業者および消費者に対する「フィッシング対策ガイドライン」を策定しましたので、公表いたします。

特徴

- ・業種を特定せず、事業者、消費者両面の観点からフィッシング対策について総合的にまとめたガイドラインとして日本で初めてのものです。
- ・実施の重要度を次の3段階で参考表示し、事業特性等により適用範囲を調整できるようにしてあります。(◎:実施すべき ○:実施を推奨 △:場合によっては実施すべき)
- ・検討メンバーは銀行、クレジットカード会社、情報セキュリティ会社、大学の有識者、JPCERT コーディネーションセンタなど各界にわたり、また、経済産業省などの政府機関においてもオブザーバとして参加協力を得ました。また実際にフィッシングに被害に遭い、その対策実施経験のある銀行やISP 関係者の意見も取り入れるなど、実践的な内容となっています。

位置付け

フィッシング対策協議会では消費者がフィッシングの被害にあわないために留意すべきことをまとめた「被害にあわないための5カ条」¹をまとめ、啓発リーフレットやホームページなどを通じ提供してきました。しかしながら、次のような事項に対しても指針があることが望まれていました。

- 消費者が被害にあったとき、何を、どのような優先順位で実施するか
- 事業者として顧客の啓発、フィッシング被害²を未然に防ぐ予防措置など事前にどのような体制整備すべきか
- 事業者が被害に遭ったとき、迅速かつ的確な対応をとれるようにするため何を、どのような優先順位で実施するか

本ガイドラインは、このような事項を検討する際に参考としていただけるよう、わかりやすく記述することに配慮するとともに、実践的な内容となっています。

ガイドライン入手先

「フィッシング対策ガイドライン」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9月10日より公開いたします。

お問合せ

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

¹ 「被害にあわないための5カ条」: <http://www.antiphishing.jp/gokajou.html>

² 事業者にとっての被害とは、その社名やブランド名を騙(かた)られ、フィッシング行為に使用される場合も含む。

策定の背景

米国 Anti-Phishing Working Group (APWG) によれば、APWG に寄せられる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に寄せられるフィッシング事例の報告件数は APWG と比べれば少ないものの、2007 年夏頃より日本人を対象としていると考えられる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が増えてきています。また、2008 年に入ってから、従来の銀行・クレジットカード会社・ネットオークションをかたる事例以外に SNS サイトやインターネットサービスプロバイダ、携帯電話会社など多様な業種の事業者をかたるフィッシング事例が観測されるようになってきており、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。

このような状況の中、フィッシング詐欺被害を未然に防ぎ、また被害が発生した場合の被害拡大を効果的に抑止することを目指し、フィッシングによる被害を受ける可能性のあるサービス事業者及び一般消費者がフィッシングの手法により不正に利益を得ようとする者に対して講じておくべき対策について、適切かつ有効であるという観点から選択・整理し、提示することを目的に、2007 年度より検討を行ってまいりました。

ガイドランの内容

本ガイドラインでは次の4つの場面から実施項目を規定しその内容を解説しています。

場面	内容
サービス事業者におけるフィッシング詐欺対策	
①フィッシング詐欺被害を抑制するための対策	フィッシング被害を未然に防ぐ予防措置など事前行うべき体制整備等の要件と解説
②フィッシング詐欺被害の発生を迅速に検知するための対策	フィッシングの発生から検出までのタイムラグを短くするための要件と解説
③フィッシング詐欺被害が発生してしまった際の対策	フィッシングサイトのテイクダウン活動とその方法、注意勧告(窓口準備、顧客への通知)、関係機関への連絡などの実施要件と解説
消費者におけるフィッシング詐欺対策	
①フィッシング詐欺への備え	「被害にあわないための5カ条」の中で特に重要な3項目について、具体的にどうすれば良いかの要件と解説
②フィッシング詐欺に遭ってしまった時	消費者が被害に遭ったときの、対処手順の整理と解説

まとめ

フィッシング対策協議会では、本ガイドラインを活用して、サービス事業者の方々におかれまし

では自社サービスにおけるフィッシング対策の促進・充実を図っていただき、消費者の方々におかれましてはフィッシング詐欺に対する正確な知識を持つことで必要な対策を確実に行っていただくこと、及び、事業者・消費者双方が的確な対策をとることによってフィッシング被害の抑制・最小化に資することを期待しています。

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

フィッシング対策の促進を目的に設立された任意団体であり、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に行っています。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、対策ベンダなどの事業者から構成され、また、関係府省庁、関係機関がオブザーバとして参画しています。（<http://www.antiphishing.jp/>）

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。（APWG のレポートより抜粋）

〈参考資料〉

フィッシング対策ガイドライン(抜粋)

フィッシング対策ガイドラインの要件一覧(付録)、図表などを紹介します。

①サービス事業者が考慮すべき要件一覧

【 顧客が正規メールとフィッシングメールを判別可能とする対策 】

- ◎顧客に送信するメールには電子署名を付与すること
- ◎外部送信用メールサーバを送信ドメイン認証に対応させること
- ◎顧客に送信するメールでは定型的な様式を用いること
- ◎サービス事業者が顧客に送信するメールは TEXT 形式とすること
- ◎顧客にメール送信する状況及び内容を周知しておくこと

【 顧客が正規サイトとフィッシングサイトを判別可能とする対策 】

- ◎Web サイトの安全性を確保すること
- ◎Web サイトの正当性に係る情報を十分に提供する画面とすること
- ◎重要情報を入力するページは SSL/TLS で保護すること
- ◎Web サイト運営者の連絡先及びガイダンス等、顧客に間違いなく情報を伝える必要のあるページは SSL/TLS で保護すること
- ◎正規 Web サイトのドメイン内設置サーバの安全性を確認すること
- 正規サイトの全てのページに顧客に対する脅威の状況を表示する
△認証画面には顧客個別のマーク等を表示できるようにする

【 フィッシング詐欺被害を拡大させないための対策 】

- ◎資産の移動に限度額を設定すること
- ◎資産の移動時に顧客に通知を行うこと
- 正規 Web サイトにアクセス可能な端末を制限すること
- 携帯電話によるサービス利用は顧客の選択制とすること
- 機微情報を変更するページへの移動には複数要素認証を要求すること
- 重要情報の表示については制限を行う
△特別な認証方法を採用する場合には、その方式に特有のぜい弱性対策を行うこと
△正規サイトログイン時の認証要素としてワンタイムパスワードを利用すること

【 ドメイン名に関する配慮事項 】

- ◎顧客の認知しているサービス事業者名称から連想されるドメイン名とすること
- ◎悪用される可能性の高い類似ドメインを保有しておくこと
- ◎使用するドメイン名と用途の情報を顧客に周知すること
- ドメイン名に見た目が紛らわしい文字を含めないこと

【 組織的な対応体制の整備 】

- ◎フィッシング詐欺対応に必要な機能を備えた組織編制とすること
- ◎フィッシング詐欺に関する報告窓口を設けること
- ◎フィッシング詐欺発生時の行動計画を策定すること
- ◎フィッシング詐欺及び対策に関わる最新の情報を収集すること
- ◎フィッシングサイト閉鎖体制の整備をしておくこと
- フィッシングサイトアクセスブロック体制の整備をしておくこと

【 顧客への啓発活動 】

- ◎顧客が実施すべきフィッシング詐欺対策啓発活動を行うこと
- ◎フィッシング詐欺発生時の顧客との通信手段を整備しておくこと

【 フィッシング詐欺被害の発生を迅速に検知するための対策 】

- Web サイトに対する不審なアクセスを監視すること
- △フィッシング詐欺検出サービスを活用すること

② フィッシング詐欺被害が発生してしまった際の対策（対応フロー）

- (1) フィッシング詐欺被害の発見
- (2) フィッシング詐欺被害状況の把握
- (3) フィッシング詐欺被害対応活動
 - ・フィッシングサイトテイクダウン活動
 - ・フィッシングメールに対する注意勧告
 - ・関係機関への連絡、報道発表
- (4) 生じたフィッシング詐欺被害の回復措置
- (5) 事後対応

③消費者が考慮すべき要件一覧

【 フィッシング詐欺 】

- ◎機微情報の入力を求めるメールを信用しない
- ◎メールに記載される差出人名称は信用しない
- ◎怪しいメールの判断基準を知る

【 電子メール本文中のリンクの扱い 】

- ◎電子メール本文中のリンクには原則としてアクセスしない
- サービス事業者からの通知メール形式を TEXT 形式に設定する
- リンク先で機微情報の入力を求められた場合には、電話等でサービス事業者に真偽を確認する

【 パソコンを安全に保つために 】

- ◎最新のセキュリティパッチを確実に適用する
- ◎マルウェア対策ソフトウェアを適切に用いる

- ◎類似性評価によるフィッシングメール判別機能を活用すること
- ◎Web ブラウザにフィッシングサイト判別機能を組み込み活用すること

【 アカウント情報の管理 】

- ◎アカウント ID/パスワードはサービス事業者別に設定すること
- ◎アカウント管理ソフトウェアを導入する
- ◎全てのアカウントについて緊急連絡先を把握しておくこと

④消費者がフィッシング被害に遭ってしまった時の対応

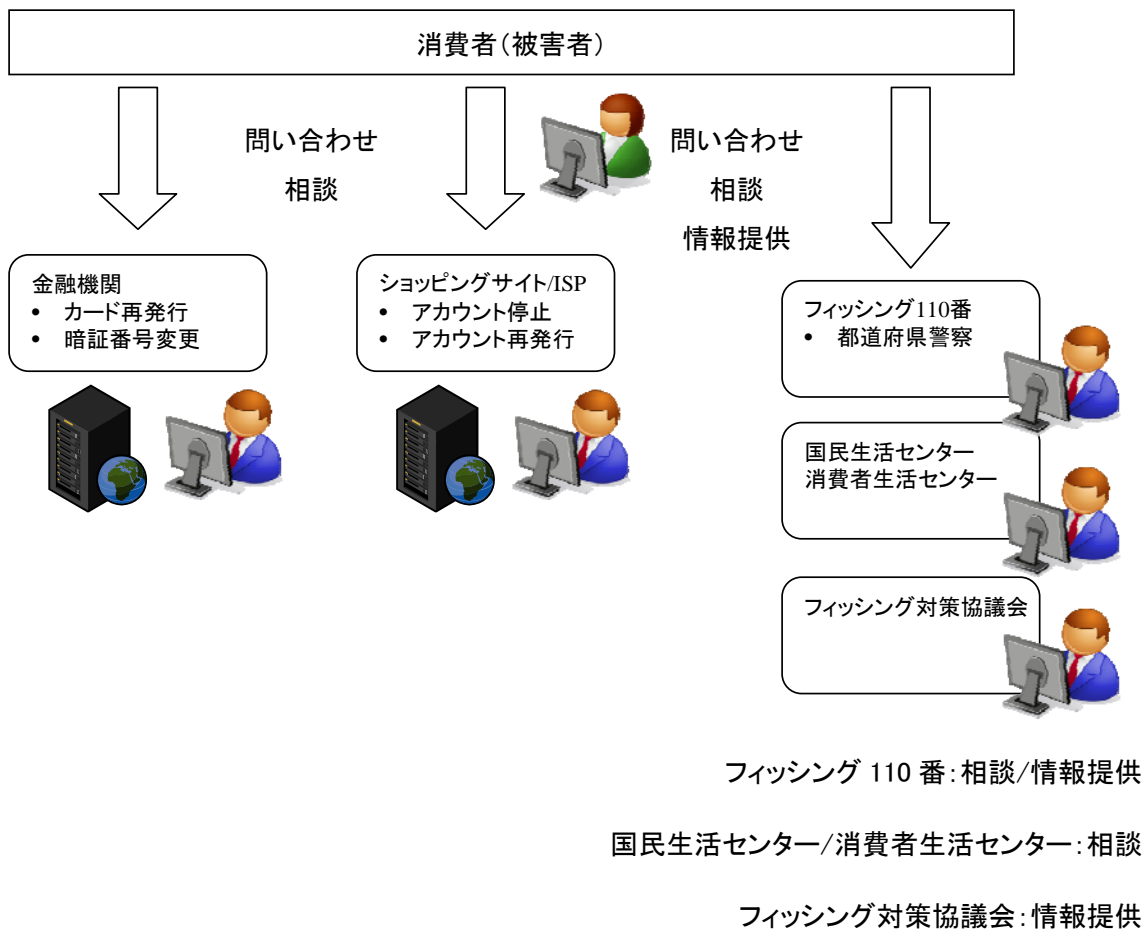


図 消費者がフィッシング被害に遭ってしまった時の対応内容

以上