フィッシング対策における技術・制度調査報告書
2008

平成２０年３月

フィッシング対策協議会

技術・制度検討ワーキンググループ

目　次

1. はじめに

平成１９年度のフィッシング対策協議会技術・制度検討ワーキンググループでは、次の２つのテーマに取り組んだ。

① 「フィッシング対策ガイドライン」の策定
② フィッシング攻撃の各段階において、前年度の調査で議論が十分には深化できていなかった３つの段階についての調査。

(1) フィッシング対策ガイドライン策定

事業者または消費者がフィッシングに対して講ずるべき適切かつ有効な対策の実施を図るための指針とすることを目的として「フィッシング対策ガイドライン」を検討・とりまとめた。

- 事業者にとっての予防策（事業者が被害に合う事象発生時の対応準備事項含む）
- 事業者が被害に遭った（なりすまされた）場合の対応
- 消費者にとっての予防策
- 消費者が被害に遭った場合の対応

「フィッシング対策ガイドライン」については本報告書とは独立したものとして別途まとめ公開するのでその資料を参照願いたい。

以降、本報告書では②の調査内容について整理する。

1.1 フィッシング攻撃の段階別検討

前年度（平成 18 年度）技術・制度検討ワーキンググループにおける調査の概要をまとめたものを表 1-1に示す。本表には前年度報告書中にある該当テーマに対応する資料番号も列を追加して記載した。

今年度は前年度で整理したフィッシング攻撃の段階において、議論が十分には深化できていなかった次の段階について調査整理した。

(1) ステップ１：メールの送信（悪質メールが届く段階）
(2) ステップ３：フィッシング攻撃の実行（Webサイトで機密情報入力を要請される段階）
(3) ステップ５：機密情報の入手（フィッシャーが機密情報を入手する段階）

表 1-1 技術的対策と法・制度面での対策のまとめ

ステップ	内容	技術的対策方法	法・制度面での対策	章/資料番号
0:フィッシングの準備	攻撃ターゲットの選別や電子メール送信のためのアドレス収集。類似ドメインの取得	類似ドメイン取得の監視	類似ドメイン取得の禁止 JPRS による類似ドメイン取得に関する注意喚起の提供	
1:メールの送信	フィッシングサイトに誘導するために詐欺メールの送信	ISP によるメールフィルタリング技術 送信者認証、メールの電子署名 *課題:迷惑メール用フィルタのため、フィッシングの場合フィルタの誤検知との見分けが付かない*	迷惑メール法、偽装メールに対する著作権法の適用 *課題: 送信者認証や電子署名の技術を推進する制度が必要とされる。*	2章 資料 A
2:ユーザがメールに反応	届いたメールを開封し、URL をユーザが実行	証明書付き電子メール	教育・啓発活動によるユーザの教育 フィッシング対策協議会の Web によるフィッシングの啓発活動	資料2
3:フィッシング攻撃の実行	偽装サイトにユーザが訪れる	クロスサイトスクリプティングの脆弱性の除去	偽装 Web に対する著作権法の適用	3章 資料 B
4:機密情報の送信	偽装サイトにユーザが個人識別情報を入力する	ユーザが容易にフィッシングサイトを見分けられるようにするための技術 ・フィッシング対策ツールバー ・実在性も保証する厳密な証明書(EV SSL) ・サイト画像認証 ・画像を利用したユーザ認証	*課題:制度面での技術の普及の後押しが必要*	資料2 資料5

ステップ	内容	技術的対策方法	法･制度面での対策	章/資料番号
5:機密情報の入手	偽装サイト上の収集された個人識別情報をフィッシャーが取得	マルウェアによる識別情報の盗み取りを防止するための技術 ・ソフトキーボード[1]、キーロガー[2]検知	*課題:個人識別情報の入手を罰する手段がない*	4章 資料Ｃ
6:機密情報の利用	個人識別情報を利用してユーザになりすましてサービスを利用	盗み出した個人識別情報を利用してもなりすましを出来ないようにするための技術 ・二要素認証 ・帯域外認証 *課題:コスト*	不正アクセス禁止法 *課題:制度面での技術の普及の後押しが必要*	資料3 資料4 資料6
7:不正行為の実行	クレジットカードの利用や預金の引き落としなど不正行為の実行	トランザクションの不正検知	現行の刑法に順ずる *課題:国際的な犯罪に対する国内法の限界*	資料6

注意：資料２～６は前年度（平成 18 年度）報告書に付属する資料番号を示し、２～４章及び資料 A～C は本報告書における章番号と対応資料番号を示す。

出典：フィッシング対策における技術・制度調査報告書 2007, フィッシング対策協議会

1 本来キーボードで行う入力処理を画面に表示したキーをマウスでクリックする等ソフトウェアで実現したもの
2 キーボードの入力を記録するもので、ユーザ入力情報を盗むことに悪用されることもある

2. ステップ1:メールの送信

フィッシング攻撃のステップ1にあたるメールの送信（悪質メールが届く）段階に関するテーマとして迷惑メール対策について、Japan Email Anti-Abuse Group（JEAG）のメンバによる講師により Outbound Port25 Blocking 及び送信ドメイン認証技術を中心に調査を実施した。

詳細は資料A「Outbound Port25 Blocking ＆ 送信ドメイン認証技術」を参照のこと。

2.1 迷惑メールをとりまく状況

迷惑メールは、単なる迷惑からより深刻な問題へと変化して来ている。例えばフィッシングなど個人情報の不正入手による直接的な金銭被害が発生しており、2006 年の金融被害額は 26 億ドルと予想されている(Gartner 2006.11.9)。迷惑メールはマルウェア配布の手段として利用されることもあり、これに感染すると、知らない間に（個人の PC が bot 化するなどにより）加害者になってしまう。一方、フィルタを回避するための技術も進化(image spam, 目くらまし words, botnet, etc)している。それに対して、迷惑メールフィルタの機能を強めると本来届かなくてはならないものが届かなくなる可能性がある。これは ISP として問題である。つまり False Positive（実際には正規の通信であるにもかかわらず、IDS/IPS が不正アクセスとして検知してしまう通信）はなるべく避けなければならない。

迷惑メール対策としてフィルタの他に、ブラックリスト（DNSBL/Real Time Black/Block List）の利用が増加している。これにも問題があり、例えば登録基準が曖昧で、その管理が継続されていない場合もある。また正規のものが登録された場合の送信側の被害が大きい、解除方針が不明瞭及び連絡先が分かりづらい等の問題点もある。そこで独自の Block Policy による防御も増える傾向にあるが、これは要因が複雑なためより解除が難しく、実務上非現実的であると考えられる。

2.2 フィッシングを防ぐためには

フィッシングの場合の大半が、メールを起点にしたものであることから、まずは迷惑メール対策を推し進める必要がある。そのためには、迷惑メールを受け取らないより、まず出さない（送らない）努力が必要である。その理由・根拠は次の通りである。

①受信側に届くまでの Internet 上を流れている→ 無駄な通信

②受信側でフィルタ等の対応をするにもコストが必要→ 受信設備の増加

③無駄なメールを無くすことにより正しいメールがきちんと届く仕組みを作る

④正しいメールはどれかを送信側が示すことが必要

メールのヘッダ情報は全て詐称可能であり、それが本当に正しいかは確認が難しい。そのような中で JEAG で取り組んでいるのが次の２つである。

■ OP25B (Outbound Port 25 Blocking)

■ 送信ドメイン認証(Sender Authentication Technology)

これらを日本国内にとどまらず、グローバルに普及させることが必要である。例えば海外にサ

ーバがある場合、国内だけで対処しても解決しない。

また、日本国内においてはフィッシングというよりは騙（かたり）り系が多く、ドメインの存在意義が成り立たなくなってきている。したがって、受信したメールが信頼出来るメールかどうかを判別する必要がある。

2.3 OP25B

(1) なぜ OP25B なのか

迷惑メールはどこから来るのかを考えてみる。「届く」と言うことは、誰かが「どこか」から送っているということであり、その発信源を調べて見た。その結果、ほとんどが ISP の動的 IP を発信源としていた、ということが分かった。そこで、「どこで止めるか?」を考えると、送信側で止める、送信させないということになり、この発想で出てきたのが Outbound Port 25 Blocking である。

(2) Outbound Port 25 Blocking (OP25B)

OP25B の実施方法は次の通りである。

・Source IP Address が動的 IP 、かつ、Destination Port が 25 である TCP トラフィックを遮断すること(JEAG Recommendation より)。

この OP25B の最大の特徴は、迷惑メールそのものを止めてしまうことである。これにより、動的 IP を Source IP とする spam（迷惑メール）が完全に止まることになる。OP25B は米国の大手 ISP で実施し効果が確認されており、日本では今日、大手の ISP 全てが実施するなど広まっており大きな成果を上げている。

(3) 普及の状況

2004 年秋の日本における spam メールの状況を見ると次の顕著な特徴があった。

・発信源：ISP の動的 IP

・受信者：携帯電話

現在は当時とは異なる特徴を示している。

その後次のような変遷をした。

・ 2005.8 OP25B に対する総務省見解の公表
　→携帯宛限定 OP25B の普及が進む

・ 2006.2 JEAG Recommendation 発表
　→完全な OP25B の普及が進む

・ 現在 JEAG 内の OP25B 実施率、ほぼ 100%達成
　→日本の OP25B は「完成期」を迎えている
　→spam 発信源は海外へ

このような流れの中で Spam の発信国ランキングを世界的に見ると、日本は 2007 年秋頃より

ベスト１２のランク外となった。

2.4 送信ドメイン認証

迷惑メールの対策には、送信ドメイン認証という方法もある。これは、「送信者情報を詐称出来ない仕組みの導入が必要」との考え方によるもので、次の２通りの仕組みが挙げられる。

① SMTP AUTH

これは送信者を認証する技術で、ISP 側のメールサーバで誰が送ります、と宣言してから送るという仕組みである。

②送信ドメイン認証技術

これは、例えば KKI.com のメールサーバはこれです、と宣言することにより、それ以外から来たメールはドメインを詐称して送っていると判断できるようにするものである。

2.5 送信ドメイン認証技術

送信ドメイン認証技術の要点は次の通りである。

・ 送信側がドメイン単位でメール送信元情報を表明する
・ 受信側が正規のメールサーバから出たものかを認証する
・ 送信側と受信側で協力して初めて成立する技術である
・ 既存のメール配送の上位互換として存在する

また、送信ドメイン認証技術には大きく分けて次の二つの種類（方式）が存在している。

①送信元をネットワーク的に判断するもの
（SPF：Sender Policy Framework）

②送信時に電子署名をメールに付与するもの
（DKIM：DomainKeys Identified Mail）

2.5.1 SPF

送信ドメイン認証の一つであるSPFの仕組みを資料Aのスライド２０に示す。まず、DNSサーバに送信メールサーバのドメイン名（例：example.com）とIPアドレスの対を登録しておく。そして、ユーザがfoo@example.comというアドレスからメールを送ると、受け取った受信メールサーバはメールの送り元がどこかを（ドメイン名により）DNSサーバに尋ねる。するとDNSサーバはexample.comのIPアドレスを返す。メールが送られてきた元のIPアドレスとDNSサーバから返されたIPアドレスの整合チェックをかけてOKであれば正規のサーバから送られたメールとみなす。一方、迷惑メール送信者がfoo@example.comというメールアドレス（ドメイン）をかたって、本来でないサーバからメールを送信すると、DNSサーバへの照会で得られるIPアドレスと送信元サーバのIPアドレスが違うアドレスになるので、そのメールはアドレスを詐称しているものと判定できる。

2.5.2 送信ドメイン認証の普及状況

WIDE プロジェクトは、JPRS と共同研究契約を結び、2005 年 4 月から送信ドメイン認証の普及率測定を実施しており、その調査結果を資料 A のスライド２１に示す。着実に国内の SPF の記述率は増えており、2007 年 6 月末現在、約 6.84%まで普及している。

2.5.3 課題

送信ドメイン認証普及にむけての課題としては次のとおり認識されている。

・ 送信ドメイン認証の仕組み、影響及び効果が認知されていない。
・ 社内へ十分説明出来ない。もしくは、そもそも十分理解していない。
  - 導入のインパクト、影響、等
・ (技術自身新しいものであるため) SPF の記述方法や設定方法などを説明する媒体が無い (少ない)。
  - 記述したくても、記述方法が判らない為、導入できない
・ 受信側の対応が少なく、書くメリットがない。
  - 実影響が出ていない為
  - 認証結果をどう扱うかが不明確。(pass と none の区別がない)
・ メールを受信するエンドユーザに効果を訴求しづらい。
  - エンドユーザへの効果に対して、導入の障壁が高い。
  - 顧客にとってどのようなメリットがあるのか見えにくい。

2.5.4 普及に向けて

送信ドメイン認証（SPF）の普及に向けて次のように進めていただきたいと考えている。

① メール送信側でまず導入すべき
② 送信側の SPF の導入は容易
  DNS への SPF レコード追加で済む
③ 利用者に応じて導入技術を判断
  - それぞれの長所、短所を把握して判断
  - ビジネスとしての連絡や情報提供に使うメールは DKIM を用いる

3. ステップ3:フィッシング攻撃の実行

ステップ３にあたるフィッシング攻撃の実行（Web サイトで機密情報入力を要請される）段階に関するテーマとしてクロスサイトスクリプティングを中心に高木浩光氏(産業技術総合研究所)の講師により検討を行った。また、当日は当該テーマに限らずフィッシング対策全般についても検討を行った。その概要を次に記すが具体的には資料 B「正しいフィッシング対策について」を参照のこと。

3.1 フィッシング対策の方向性

正しいフィッシング対策としては次の３つの方向での活動が要求される。

・ Web の正しい利用方法の理解の普及
・ 技術的欠陥（脆弱性）の排除
・ 技術的解決策

3.2 啓発活動

啓発のための解説には適切でない、または誤った内容のものがあり、これらは、啓発コンテンツ作成を広告会社等に丸投げし、その内容が技術的専門家にチェックされていないことが原因と想像される。また専門家自身もフィッシング対策についてただしく理解してないと見られる例も存在する。

適切な解説コンテンツを作るには、企画の最初の段階から技術的専門家もチームに参画し制作を進める必要がある。また、利用マニュアル作成者やサイト設計者向けに要点を独立行政法人産業技術総合研究所（産総研）から次のサイトで公開しているので、啓発コンテンツの制作にあたって参考にしていただきたい。

「安全なWebサイト利用の鉄則」http://www.rcis.aist.go.jp/special/websafety2007/

ここで示している鉄則の要点は次の通りである。

- 初めて訪れたサイトの場合
  - サイト運営者のことを知っている場合
    - その運営者のドメイン名を既に知っている場合
      - アドレスバーのドメイン名を確認する
    - その運営者のドメイン名をまだ知らない場合
      - SSL のサーバ証明書の内容を確認する
  - サイト運営者のことをまだ知らない場合
    - （信用できる運営者か見極める）
- 再度訪れたサイトの場合
  - アドレスバーのドメイン名を確認する

3.3 技術的欠陥の排除

脆弱性など技術的欠陥によるフィッシング被害を防ぐためには、責任分解点を明確にして取り組むべきである。

(1) アドレスバー偽装、錠前アイコン偽装

これらに対しては Web ブラウザベンダーの責任であり、アドレスバーや錠前アイコンを正しく確認できないようなものは、ブラウザとして欠陥があるという共通認識がある。そしてブラウザの脆弱性として発見され次第修正が行われている。

(2) クロスサイトスクリプティング攻撃

クロスサイトスクリプティング攻撃に対しては Web サイト運営者に責任がある。クロスサイトスクリプティングは Web アプリケーションの脆弱性によるものであり、修正すべきものである。

(3) 本物サイトが偽ページに改ざん

これも Web サイト運営者の責任であり、そもそもあってはならないことである。

(4) Pharming（ファーミング）の手口

Pharming（ファーミング）の手口に対しては、これは消費者の責任である。消費者がスパイウェア等に感染するようなミス操作をしては如何ともしがたい。

3.3.1 事業者での対策

事業者のとるべき対策（Web サイト及びメール配信のあるべき姿）として次のものがある。

(1) Web サイトの構成のあるべき姿

- アドレスバーやステータスバーを隠さない
- 入力ページを https:// にする
- 正規のサーバ証明書を購入して SSL を運用する
- サービス提供者が保有するドメイン名を使う
- まぎらわしくないドメイン名を使う
- サイトからクロスサイトスクリプティング脆弱性を排除する

(2) メール配信のあるべき姿

- HTML メールを送らない
- デジタル署名のないメールを送らない

3.3.2 クロスサイトスクリプティング

クロスサイトスクリプティング脆弱性（「XSS 脆弱性」）とは CERT/CC が 2000 年 2 月に勧告

（CERT Advisory CA-2000-02 “Malicious HTML Tags Embedded in Client Web Requests”）したもので、Cookie 漏えい、セッションハイジャック攻撃の危険があるとして国内では比較的よく知れ渡り対策が進んだものである。しかし、もう一つの脅威がある。それは、本物サイトの画面上に偽ページを差し込まれる、というものである。これはサーバ内の記憶データが改ざんされるわけではない。外部からの入力を差し込んで表示する動的なページで、適切な作り方をしていないと、JavaScript をページ内に差し込まれ、悪意あるサイトからジャンプしてきた場合に起きるというものである。

当時の Yahoo!メールの XSS 脆弱性を突いて、yahoo.co.jp ドメインの画面上に偽コンテンツを表示させていた、という日本語フィッシング事例が 2005 年 11 月に発生している。

3.4 技術的解決策

フィッシングに対する技術的解決策として次のものがある。

(1) EV-SSL

ホワイトリスト方式の一つであり、サイト運営者の信頼性を専門機関が審査認定する。（サイト実在性の審査基準が厳格であることなどに起因し）正当なサイトのすべてが利用できるわけではない、という欠点がある。

(2) ツールバーによる利用者補助

ブラックリスト方式、特徴検出（IE 7、Firefox 2）するものや、ドメイン名の視認性向上（各種 Firefox アドオン等）を図るもの及び信頼するドメインの登録・確認ツール（「Petname Tool」）などがある。

(3) パスワード自動入力ツール

「PwdHash」(Stanford)、「Passpet」(UCB)等のツールがこの分類に相当するものとしてある。

(4) ログイン認証方式の改善

この方式をとるものとして、産総研－ヤフー共同研究の事例がある。

3.4.1 産総研とヤフーが提案する新認証プロトコル

ここで提案している新認証プロトコルは、長期的展望に立った抜本的解決策であり、HTTP Auth（「Basic認証」等）の拡張である「HTTPパスワード相互認証プロトコル」[3]というもので

[3]『「HTTP パスワード相互認証プロトコル」は、Web システムでのフィッシング攻撃を防止するための、新しい認証プロトコルです。この認証プロトコルは PAKE と呼ばれる暗号・認証技術に新たな手法で改良を加え、ウェブの標準プロトコルである HTTP および HTTPS に適用したもので、ユーザーがパスワードでサイトの真偽性を確認できる仕組みを提供することによりフィッシングを防止します。』（「フィッシング対策のための HTTP 相互認証プロトコル」,産業技術総合研究所,より）

ある。この新認証プロトコルはIETFに提案中であり 2010～2011 年頃にRFC化を目指し、その後、各ブラウザへの標準搭載へ、という展開を計画している。

このプロトコルによる認証方式を採用し、（現状の）フォーム認証を使うことをやめることにより、フィッシング被害を防止する。また同時に、Web アプリケーションの脆弱性も減らせ、Web アプリケーションのログイン機能実装が容易になるという利点もある。

4. ステップ5:機密情報の入手

ステップ５にあたる機密情報の入手（フィッシャーが機密情報を入手する段階）に関するテーマとして、フィッシャーによる盗難情報伝送の方法とその追跡について、カスペルスキーラブスジャパンにおける調査･事例に基づいて解説された。

以下､その内容を紹介するが併せて資料 C｢フィッシャーの追跡　現状と課題｣を参照されたい。なお｢(　)｣内に示す数字は資料 C における対応スライド番号を示している。

講師は次の通りである。

・スーパーバイザー: Michael Molsner ((株)カスペルスキーラブスジャパン CIO)

・プレゼンター/本稿執筆: 林 裕子 ((株)カスペルスキーラブスジャパン Coordinator)

4.1 序

フィッシングは、国境を越えた世界的な脅威となっている。日本においてフィッシングはさほどの被害を生んでいないと言われるが、これは日本の企業や団体をかたるフィッシングのケースがさほど多くないという意味である。日本のサーバにフィッシングサイトがホストされてしまうケースは、決して少なくない。フィッシングサイトを置かれるということは、そのサーバに脆弱性が存在すること、またはセキュリティ対策が十分でないことを示す。つまり、そのサーバはフィッシングサイト設置以外にも悪用される可能性を持っている。または、すでに悪用されているかもしれない。フィッシングの被害に遭わないように一般ユーザの啓蒙をうながす必要性もさることながら、サーバ管理側/サービス提供者の側にも十分な危機管理意識と状況の理解が必要とされる。

今回の講義のテーマとしては、フィッシング攻撃のステップ 5「フィッシャーが機密情報を入手する段階」が与えられているが、これに留まらない内容となっていることをはじめにお断りしておきたい。具体的には、盗まれた情報がフィッシャーの手にわたる過程を説明し、フィッシャーを追跡する方法をいくつか紹介した。また、フィッシングサイトの閉鎖について説明し、今後の課題を提示した(2)。

4.2 フィッシングの概要

フィッシングの概要については、ここでは説明を割愛する。フィッシングの流れについてはスライド 3、フィッシングサイト事例についてはスライド 4～5 を参照されたい。なお、ここで紹介するフィッシングの流れは、本講義を進める上での便宜的なものであり、本協議会で使用する各ステップとは必ずしも対応していないことをご了承いただきたい。

4.3 盗まれた情報とフィッシャーの追跡

4.3.1 フィッシングサイトの実体

フィッシングサイトは、フリーの Web ページサービスを利用して開設されることもあるが、脆弱なサーバに仕掛けられることが多い。サーバのセキュリティホールを突いて、管理者の知らない間にフィッシングサイトが仕掛けられる。

近年は、組織的なフィッシングが増える傾向にある。そのひとつに、ボットネットを利用したフィッシングがある。ボットネットを介して、スパム配信やフィッシングサイト設置が自動的かつ高速に行われるようになった。

フィッシングサイトの存続期間が長いほど、フィッシングの効果は高まる。フィッシャーは、Fast-Flux などのテクニックを使ってサイトの長期存続をはかっている。

近年めだっているのが組織的な犯罪者集団によるフィッシングであり、著名なものは"Rock-Phish"と呼ばれる集団である。フィッシング情報データベースである PhishTank には、多数のフィッシングサイトが日々報告されている(8)。フィッシングサイトをできるだけ迅速につきとめて閉鎖することが、被害拡大を防ぐのに欠かせない。

4.3.2 フィッシャーの手口

フィッシャーを追跡するためには、その手口を知る必要がある。よく見られるのは、脆弱なサービスが稼働するサーバにフィッシングサイトが仕掛けられるケースである(9、10、14)。たとえば、セキュリティホールを通じてバックドアが仕掛けられ、これを通じてフィッシングサイトが置かれる(11～13)。直観的なユーザインターフェイスを備えたバックドアツールが流通しており、さほどスキルのない人間でも簡単にマルウェアをアップロード可能となっている。

かつて、ハッカーは高いスキルを持ち、政府系サイトへ侵入することを一種のステータスと考えていたが、近年ではハッカーのプロフィールも変化してきた。スキルの高くない犯罪者が増え、また名声のためにハッキング行為に及ぶのではなく実利を求める犯罪者が増えた。その一端をうかがわせるのが、とある IRC チャネルで弊社アナリストがハッカーと交わした会話である。このハッカーはこう述べている「(政府系サイトへ侵入することに)特別な意味はない。仕掛けられるところに仕掛けて金を稼ぐだけだ」(15)。

なお、スライド 10 の例は米国某州の小さな信用組合のフィッシングサイトである。フィッシングサイトで名前を騙られるのは大手企業がほとんどであったが、最近は、知名度のない小規模な企業のフィッシングサイトも増えている。

フィッシングサイトを通じて取得された情報は、フィッシャーへメールで送られる。リアルタイムで送られるケースと、サーバ上に置かれたファイルに情報をためておいて一括でメール送信するケースとがある。スライド 16 では、ユーザが入力した情報が一覧になっている様子がわかる。

フィッシングサイトの開設に使われたパッケージは、開設後に削除されることが多いが、その

ままサーバ上に残されていることもある。パッケージ内には、フィッシングで獲得した情報の送り先その他の重要なデータが眠っている。しかし、こうしたパッケージは、フィッシングサイトを閉鎖するときにまとめて削除される。フィッシャーの追跡やフィッシング被害の捜査に役立つと考えられるこの情報を、活用できないものだろうか。

サーバ上のフィッシングサイトパッケージ(アーカイブ)に格納されていたフィッシャーのメールアドレスを取り出し、リスト化したのがスライド 17 である。フリーの Webmail サービスがフィッシャーによって利用されることが多い。こうしたメールアドレスを Webmail サービス提供者へ報告し、停止してもらうことで、フィッシャーへ情報がわたるのを阻止できる。

ごくレアケースながら、こうしたデータから犯罪者を特定できることもある。たとえば、弊社で見つけたメールアドレスから、欧州で個人商店を営む特定の人物に行き当たった(19、20)。この情報は、現地の警察にレポートされた。

4.3.3 Rock-Phish

フィッシング犯罪は、組織化されて大規模にわたる傾向にある。全世界で観測されるフィッシング犯罪のおよそ半数は、"Rock-Phish"と呼ばれる集団に起因すると見られている(21)。その実体は不明だが、ロシアをベースに活動する、きわめてスキルの高い少数精鋭集団であるとされる。ボットネットや Fast-Flux を使った、効率よい組織だったフィッシング活動に特徴がある。

Fast-Flux とは、ひとつのドメインに複数の IP を割り当て、短期間で IP をローテーションする方法である(22)。ドメインに割り当てられる IP セットは、必ずしも固定ではない。したがって、ドメインの追跡は非常に難しい。Fast-Flux を利用したフィッシングサイトは長いあいだ存続する傾向にあり、フィッシング被害の危険性が高まる。

Rock-Phish によるフィッシングサイトの主な特徴は、次のとおりである(23)。

1)意味のない、機械的に生成されたことをうかがわせるドメイン名を持つ、

2)同じ名前のフィッシングディレクトリが複数のドメインに仕掛けられている

実際の Rock-Phish サイトの例を、スライド 23 に挙げた(注: これらは、すでに閉鎖されている)。フィッシングホストの情報を得るため、フィッシングメールに埋め込まれた URL(例: http://www.ukbusiness.hsbc.com.doran4.xz.cn/bibauth/formStart/)からフィッシングドメイン(例: http://doran4.xz.cn)を取り出して直接アクセスしても、ホストがロックされていて情報が見えない(24)。しかし、フィッシングドメインの後ろにフィッシングディレクトリ名を追加してアクセスすると(例: http://doran4.xz.cn/bibauth/formStart/)、フィッシングサイトが表示される(25)。これが実際のフィッシングホストである。

フィッシングメールに埋め込まれた URL からドメインを割り出すだけでなく、ひとつのフィッシングドメインから類似の名前を持つ別のドメインを探し出すこともできる。無作為に見えるフィッシングドメイン名の数値を別の数値に置き換え(例: fk6krt.hk→fk7krt.hk)、既知のフィッシングディレクトリ名を追加してアクセスを試みることで、未報告の(しかし稼働中の)フィッシ

ングサイトを見つけだせる。(27、この手法で見つかって PhishTank に報告されたフィッシングサイト)。

4.4 日本のフィッシングサイト事例

海外のサーバ事例を取り上げてきたが、日本のサーバも例外ではない。日本企業が名前を騙られるフィッシング事例は海外ほど多くはないが、日本のサーバに海外のフィッシングサイトが仕掛けられるケースは多々ある(28)。PhishTank のレポート(29)および APWG レポート(30)によれば、2007 年 7 月にフィッシングサイトが多く置かれた国の第三位は日本である。

2007 年秋は、フィッシング関連の報道が続いた(31、33)。最初に紹介する 2 例(31)では、いずれも大学のサーバに海外の金融関連企業のフィッシングサイトが置かれていた。一方の例では、企業側からフィッシングサイトの閉鎖を求めるメールが届いて、大学側が不正サイトの存在に気づいている。もう一方の例では、過去にもフィッシングサイトが仕掛けられたことがあったにもかかわらず、セキュリティ対策が不十分であったために再発の事態を招いた。

フィッシングで名前を騙られる企業の代表的なものは、金融関連企業とオークションサイトである(32)。2007 年 10 月には、国内オークションサイトの ID とパスワードを不正入手して闇サイトで販売したとして、日本で逮捕者が出た(33)。逮捕容疑は、不正アクセス禁止法である。容疑者が他人名義で所有していた口座には約 1000 万円が振り込まれており、不正入手した ID とパスワードは 1 件あたり 25000～30000 円で売買されていたという。この事件では、福岡・熊本・岡山・茨城の 4 県警からなる合同捜査本部が容疑者逮捕にこぎつけた。

4.5 フィッシングサイトの閉鎖(Take Down)

被害を最小限に抑えるには、フィッシングサイトの速やかな閉鎖が求められる。フィッシングサイト情報を入手したら、フィッシングサイトが置かれているホストの管理者、またはそのページをホストしている ISP へただちに連絡する必要がある(34)。弊社では PhishTank への報告を行っている(35)。

しかし、サイト管理者の連絡先を突き止めるのは容易ではない。連絡先を明記しないサイトは多く、Whois 情報すら登録していないサイトもあるため、連絡先を突き止めるだけで多くの時間が費やされる。ネット不正使用に関する窓口へ送ったメールが「フィッシングメールと思われるので受け付けられません」という理由で返ってきたこともあった(36)。弊社では、フィッシングサイトを見つけた場合にサイト管理者へ通知しているが、日本のサーバにフィッシングサイトが見つかった場合には JPCERT/CC へも合わせて通知し、情報の登録をお願いしている。

フィッシングが国をまたいで行われることも、迅速なサイト閉鎖の障害となる(37、38)。被害側の国とサイトが置かれたサーバのある国との間で対応に温度差がある、時間的なロスが出るなどである。インターネットに国境はないが、現実世界には存在する。セキュリティ関係者側の国際連携が求められる。

セキュリティが侵害されたサーバは、フィッシング以外にもさまざまな脅威の温床となりうる。ひとつのサーバにフィッシングサイトがいくつも置かれる(39)、フィッシングサイトの他にトロイの木馬が仕掛けられる(41)、スパムメール配信の足場になる、などの例は枚挙にいとまがない。したがって、フィッシングサイトを削除しても、たとえばバックドア(40)がサーバ上に残っていれば、バックドアを通じて何度でもフィッシングサイトが仕掛けられてしまう。脆弱性を解消するための対策を採らない限り、根本的な解決にはならない。

4.6 何が必要か(まとめ)

では、フィッシング被害を抑え、フィッシングサイトを閉鎖し、フィッシャーを追跡するには何が必要なのか。サイトの閉鎖やフィッシャーの追跡には、多くの時間と労力が必要である。フィッシング対策協議会の活動をはじめとした対応は始められているものの、まだ十分とはいえない。ポイントは、大きく 2 つに分けられる(42)。

4.6.1 効果的な啓蒙活動

1)一般ユーザへの啓蒙活動: フィッシング対策協議会が現在取り組んでいる課題のひとつである。

2)サーバ/サイト管理者、サービス提供者への啓蒙活動: 流れる水は水源を閉じなければ止まらない。サービス提供者やサーバ/サイトの管理者、保有者に対しても、自らのシステムを責任持って管理し、最新のセキュリティ状態を保つ必要性を認知させたい。

4.6.2 法整備および関係機関の連携

フィッシング対策に関する法の整備と、セキュリティ会社同士または諸機関との連携の強化が求められる。フィッシングに関するデータを持っている人たち(セキュリティ会社や研究者)、実効能力を持つ各種機関(法的機関や警察当局など)の間に協力体制ができれば、より高い効果を得られる。同時に、セキュリティ会社間、研究者間、法的機関間の連携も必要である。国内オークションサイト絡みでの容疑者逮捕は、4 県警による連携捜査の結果であり、協力体制の必要性を端的に示すように思われる。

上記の問題は、日本国内に限った話ではない。ネットセキュリティにおいてもインターポールのような組織が実効性を持つ必要性が高まっており、国際間においても密な連携が必要とされている。

5. 技術制度検討ワーキンググループメンバ

技術制度検討ワーキンググループメンバ構成は次の通りである。

区分	氏名	所属
主査	内田　勝也	（情報セキュリティ大学院大学）
副主査	野々下　幸治	特定非営利活動法人日本ネットワークセキュリティ協会(ウェブルート・ソフトウェア株式会社)
	岩尾　健一	RSA セキュリティ株式会社
	山口　朗	株式会社オリエントコーポレーション
	石田　公孝	有限会社ストーンズインターナショナル
	内田　浩示	全国銀行協会
	加藤　孝浩	トッパン・フォームズ株式会社
	國米　仁	株式会社ニーモニックセキュリティ
	秋山　卓司	有限責任中間法人　日本電子認証協議会
	冬木 啓介	特定非営利活動法人日本ネットワークセキュリティ協会(NRI セキュアテクノロジーズ株式会社)
	畑崎 晃盛	特定非営利活動法人日本ネットワークセキュリティ協会(株式会社ジャパンネット銀行)
	青木　雄一	サイバートラスト株式会社
	浅井　英里子	マイクロソフト株式会社
	吉浦　裕	（電気通信大学）
	三田　英之	ブレインズ株式会社
オブザーバ	宮崎　清隆	有限責任中間法人 JPCERT コーディネーションセンター

資料

本報告書に関する関連資料は次の通りであり、これらは別ファイルとして掲載する。

資料 A 「Outbound Port25 Blocking & 送信ドメイン認証技術」, 本間 輝彰・櫻庭 秀次 (JEAG Board Member), 2007

資料 B 「正しいフィッシング対策について」, 高木浩光氏（産業技術総合研究所）, 2007

資料 C 「フィッシャーの追跡　現状と課題」, (株)カスペルスキーラブスジャパン, 2007