Anti-Phishing Working Group General Meeting

2006

Radisson University Hotel　米国フロリダ州オーランド
2006 年 11 月 14 日～15 日

主査代理参加・報告
坏　毅（株式会社　日立製作所）

Ⅰ．ミーティング趣旨

Anti-Phishing Working Group General Meeting は、フィッシング詐欺対策に取り組む世界最大の業界団体 Anti-Phishing Working Group（APWG）が主催するカンファレンスで、年 1 回、APWG 会員企業・団体に参加者を限定して開催される。内容は主にフィッシング詐欺に関する最新動向や研究・事例等に関する発表及びディスカッションから構成される。今年は米国フロリダ州のオーランドで開催され、米企業・政府関係者の他、イギリス・ドイツ・スペイン等のヨーロッパ勢、また韓国・日本等のアジア勢など世界中から約 200 人が参加した。カンファレンスでは、諸外国によるフィールドレポートとして、フィッシング詐欺における各国の状況・特徴が紹介されたほか、増加しつつあるドメイン名登録を利用した手口を防止するための対策、フィッシング詐欺において人的要因を考慮することの重要性と教育効果などに関する講演・議論が行われた。

本カンファレンスは基本的にベンダニュートラルなカンファレンスであるが、本年度はラウンドテーブルなどのプログラムが多く組み込まれ、ベンダや非営利団体、法執行機関など参加者が様々な立場から忌憚のない意見を活発に交わされ、随所に興味深いやり取りが見られた。

Ⅱ．セッション概要

第 1 日目（11 月 14 日）

1 日目は、フィッシングに関連する統計情報、諸外国の状況、さらに幾つかの主題に関するプレゼンテーションが行われた。以下に各セッションの概要を纏める。

① Statistical Overview & Interpretation

講演者：Bassam Khan氏（Cloudmark[1]）

米国における最近のフィッシング詐欺の動向に関する説明。Cloudmarkは 120 万を超えるデータソースから迷惑メール/詐欺メールに関するデータを集めており、そのメッセージは一日に 30 億を超える。フィッシング攻撃の発生数は、劇的ではないが少しずつ増えてきている。また、政府や企業によるフィッシング対策の実施やユーザへの啓蒙活動の浸透に伴い、犯罪者の手口も変化してきている。一つには、ターゲットの変化である。依然としてターゲットは金融関係のサイトが多い状況にあるが、これまでは大規模な金融機関が中心だったのに対し、小規模な金融機関を狙った手口が増えて来ている。その他の特徴としては、新しい攻撃手法の出現である。Vishing等の新しい手口が続々出て来ている（例：Asterisk PBXを利用したフィッシング[2]）。また、フィッシングに利用されるスパムメールの90%はボットネットから送られており、ボットネット対策が今後さらに重要となってくる。

[1] Cloudmark http://www.cloudmark.com/
[2] http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Schulman.pdf

質疑応答において、M&A とフィッシング詐欺の発生の統計的な関連性を問う質問がなされた。関係があるようであれば、M&A など企業の買収や統合が発生する場合、情報システムの統合等を騙ったフィッシング詐欺に気をつけるよう、先手を打って警告を発する事が可能なのでは、という趣旨。Khan 氏は、この 2 つに関しての調査は行っていないが、面白いアイデアであり、見てみる価値がありそうだと述べた。

② International Field Reports：諸外国の状況

【スペイン】講演者：Enrique González Ochoa（Panda Labs）

スペインにも世界的な銀行やマルウェアの作成者が存在し、金融機関をターゲットにしたフィッシング事件も数件発生している。しかし、全体としてはフィッシング以外の詐欺（送金したが商品が届かない等）が多い。スペインで特出しているのが宝くじ（lottery）に関するフィッシング詐欺である。宝くじはスペインで非常に人気がある庶民的なもので、海外でも人気がある（フランス、ドイツ、アメリカ、韓国 etc)。「おめでとうございます、宝くじに当選しました」というフィッシングメールは信じやすい傾向にある。2006 年 7 月には 300 人が逮捕され、50 ヶ国約 2 万人が被害にあっていた。

【イギリス】講演者：Colin Whittaker（APACS）

APACS（Association for Payment Clearing Services）は、イギリスの決済業務を担う共同機関であり、e-Banking Fraud Liaison Group を立ち上げ、顧客に被害を与える e-banking のインシデント調査、情報の共有、業界全体の動向把握に取り組んでいる。

イギリスではフィッシング詐欺による被害が増加しており（9 月に 1,400 件超)、直接の被害額だけででも 2006 年度上半期で 2,250 万ポンドにのぼる（2005 年度上期は 1,450 万ポンド)。これだけフィッシングが増加しているにもかかわらず、ユーザのオンラインバンキングの利用者は年々増加しており、ある調査結果でも利用者の信頼が低下する傾向はみられていない。なお、最近の攻撃の傾向として、マルウェアの進化やボットネットやルートキットの利用など、フィッシング攻撃の進化が見られる。その他のイギリスにおける動向は以下。

- 攻撃手法としては、メールや Web サイトの詐称が最も多く、次にキーロガーが多い。
- イギリスでは金融機関の規模に関係なく、平等にターゲットになっている。
- 犯罪組織は東欧（ロシア、ルーマニア、ウクライナ）がほとんどで、最近は西アフリカからの攻撃も増えている。
- APACS の調査によれば、21 歳以下の若い世代、また女性が引っ掛かりやすい。
- 新しいソーシャルエンジニアリング手法として、Targeted Phishing、Vishing、SMiShing などが出現している。特に Targeted Phishing（パーソナライズされたフィッシングメール）は成功率が数倍高い。
- ユーザへの教育はあまり効果があがっていない。

・ フィッシング詐欺と関連して、イギリスではmule recruitment[3]の広告が増加している。

【日本】講演者：Yurie Ito（JPCERT/CC）

言語の壁や銀行が顧客との連絡手段に電子メールをあまり利用していないことなどからか、日本では金融機関をターゲットにしたフィッシング詐欺はあまり横行していない。しかし、日本のサーバがフィッシングサイトのホストとして使われるケースは増加している。日本で見られるフィッシング詐欺の傾向は以下。

・ ターゲットは主にギャンブルサイト
・ メールではなく、郵送でフィッシングサイトへの URL を含む CD-ROM を送付
・ 「ワンクリック詐欺」又は「ツークリック詐欺」
・ 偽セキュリティソフト（フェイクウェア）の押し売り

【ドイツ】講演者：Dr. Waldemar Grudzien（Bundesverband Deutscher Banken e.V.）

ドイツでは、伝統的なフィッシング攻撃（10%程度）からマルウェアを利用した攻撃（90%以上）に移行してきている。ドイツではオンラインサービスを提供する銀行のほとんどがPIN/TAN[4]による認証サービスを提供していたが、フィッシング詐欺によって盗まれ悪用されるのを防ぐための新たな措置としてiTAN[5]の利用が広がっている。2006 年には完全にiTANに移行される見込みである。その他の対策として、顧客への教育の実施や早期警告システムの整備を進めており、また携帯電話を利用したmTAN[6]による認証サービスも 2 つの銀行に導入されている。また、ドイツのオンラインバンキングサービスでは、銀行規則により、2 ファクタ認証（ひとつは動的な要素による認証）が必須となっている。

今後は、mTAN のさらなる普及、ドイツの電子署名法に準拠する資格証明書を利用した電子署名などの準備を検討している。また施策としては、対策をよりハイレベル（国家・グローバルレベル）の取り組みにエスカレーションすること、フィッシング対策ハンドブック等の配布による普及啓蒙の促進、関係者間の協力体制の強化等が挙げられる。

【韓国】講演者：Terrence Park（KrCERT/CC）

韓国はまだあまりフィッシングのターゲットになっていない。韓国では Financial

[3] フィッシング詐欺で入手した ID とパスワード等を使って送金を行うのに、フィッシャー（フィッシング詐欺犯）の口座ではなく、送金先口座を提供する人間（mule）を雇い、その口座に送金を行う。Mule は手数料を差し引いて残りをフィッシャーの国外口座に送金する。殆どの場合 mule も騙されており、警察が追跡した場合のスケープゴートにされる。
[4] 取引時に、PIN（パスワード）の他に、TAN（Transaction Number：取引番号）の入力を求める。TAN のリストは金融機関から紙文書として発行される為、盗み難い。
[5] indexed TAN。TAN にそれぞれインデックス番号が付記されており、取引時には当該取引を実行するのに必要な TAN が金融機関側からインデックス番号で指定される。
[6] mobile TAN。オンラインで TAN を要求すると、サーバで TAN を生成し、顧客の携帯電話に SMS で送信される。

Supervisory Service（FSS）が金融セクタに対して厳格なセキュリティ規則を定めており、銀行は PKI による公開鍵証明書の利用を要求されている。近年の問題としては、セキュリティ専門家が確保できない中小企業の存在やソーシャルエンジニアリングの高度化等が挙げられる。韓国では、対策として以下のような施策を取っている。

- セキュリティ啓蒙・教育
  - パンフレットの配布
  - フラッシュ・アニメーションを用いた教材
  - セキュリティ情報サイトの提供
  - 相談窓口の提供：インシデントの報告から助言の提供まで、幅広く対応
- Malicious Code Finder（悪質プログラム探知ツール）の開発
- 中小企業支援策として、脆弱性検査サービス（ウェブサーバの脆弱性を検査するサービス）、ウェブアプリケーション・テンプレート（基本的なセキュリティ機能を盛り込んだサンプルコード）を提供
- IODEF ベースの情報共有システムをテスト中（2007 年後半迄に終了予定）

③ Crimewareラウンドテーブル

パネリスト：Zulfikar Ramzan（Symantec）、Dan Hubbard（Websense）、Cristine Hoepers（Brazil CERT）、Jason Milletary（CERT/CC）、Richard Wang（SophosLab US）

本ラウンドテーブルでは、犯罪に利用されるクライムウェアの現状と傾向について、関係者によるプレゼンテーションとパネルディスカッションの形式で進められた。

ウィルスやワーム等のマルウェアの作成が、当初（1986～2000 年頃）の愉快犯によるものから、近年（1990 年代後半～）は犯罪者による“ビジネス”へと性格が変わっている。犯罪者が新しいタイプのクライムウェアを次々と生み出す一方で、ユーザの理解不足及び対策不足、効果的な抑制手段の欠如から困難な闘いを強いられている現状が報告された。

クライムウェアは、ここ数年、無差別に、かつ劇的に増加している。その背景には、インターネットバンキングの世界的普及により詐欺や ID 窃取の市場が肥大化し、収益性が非常に高い活動となっていることがあげられる。クライムウェアによるインシデントの状況は下記。

【クライムウェアによるインシデントの状況】（Symantec の ISTR の調査）

- 一日平均 57,000 台のボット PC が活動しており、6 ヶ月間で 4,696,000 台の PC が発見された。また、6300 台の制御サーバを特定。
- ボットに感染している PC の所在地は、中国が最多（20%）、次に米国（19%）と続く。日本は 10 位で 2%。一方、制御サーバの所在地は、米国が最多（42%）と圧倒的。
- ネットワーク上を流れる電子メールの 54%はスパムであり、スパムの発信国は米国が 50%以上で圧倒的に多く、日本は 8 位で 3%。さらにスパムの 122 通に 1 通はマルウェ

アを含んでいる。

- マルウェアの増殖手段としては、SMTP が圧倒的に多く、次に P2P やリモートからの脆弱性攻撃等が多い。
- マルウェアのトップ 50 のうち、30 は個人情報の窃取を目的としたものである。
- 毎日 6000 程度の DoS 攻撃が検知されており、その数も増加傾向にある。ターゲットとなる国は米国が最も多く（54%）、次に中国の 12%。攻撃元も米国が最多（37%）、次いで中国（10%）となっている。

また、クライムウェアの技術的な進化として、クライムウェアの検知・停止を回避、または困難する技術の実装が進んでいる。ホストやドメイン登録を冗長化してサイトの停止を困難にしたり、その存在（プロセスやファイル）を隠すルートキット（haxdooor etc.）、アンチウイルスやパーソナル FW をバイパスするトロイの木馬なども存在。その他、クライムウェア対策を困難にしている点として以下が挙げられる。

- マルウェアのボリュームが膨大、ゼロデイ攻撃の普及
- マルウェアによるサイバー攻撃の更なる高度化
- セキュリティパッチが提供されてもユーザが充てない
- ウェブ 2.0 といった、ユーザが作成したコンテンツの普及（セキュリティの無保証）
- RSS フィードの普及によるマルウェアの自動ダウンロードの潜在性
- ウィルス対策ソフトのウィルス認識率の低さ
- ユーザへのアンケート調査によれば、ウィルス対策ソフトを導入しているのは 70%。そのうちの 30%は定義ファイルを全く更新していない

パネルディスカッションでは、マルウェアへの取り組みが「負け戦」であると思うかが議論された。パネリストの総意は負け戦とは考えないが、状況は厳しいというもの。マルウェアの発展を抑制していくためには、マルウェアの作成が割に合わない（ビジネスにならない）ようにすること、罰則が厳しく且つ迅速に実行されるようにすること（裁判に何ヶ月も何年も掛かるようでは駄目）、国際的な司法・警察の管轄権の明確化等が必要である。また、教育にあたっては、「セキュリティ意識の自覚（awareness）」が「教育（education）」に付随するものではないということを認識すべきとの見解が同意を集めた。

④ Law Enforcement, Regulation and Public Policy Precipitates of Phishing

講演者：Jonathan Rusch（US Department of Justice）、Donald Saxinger（Federal Deposit Insurance Corporation）

オンライン詐欺や ID 窃取に関連する、米国をはじめとする法執行機関の取り組み状況、および連邦預金保険公社（FDIC）によるガイドラインの策定に関する講演。

米国ではフィッシング詐欺、オンライン詐欺に関連して多くの犯罪者を逮捕している。多数のサイバー犯罪には地理的境界線が無く、フィッシングを含めた ID 窃盗の捜査には、ローカル、州、国を超えた司法・警察の協力が有益かつ不可欠となる。例としては、FBI がつい最近ポーランド当局と協力し、ID 窃盗団の摘発に成功している（Operation Cardkeeper）。また、米国では 2006 年 5 月に大統領令（EO）により ID 窃盗に対する連邦政府の取り組みを強化するためのタスクフォース（Identity Theft Task Force）が設立された。この TF の主な狙いは、ID 窃取防止に関わる米政府の取り組み改善に関する戦略計画の立案であり（2007 年 2 月を目処）、司法・警察機関による取り締まりの強化、一般大衆の教育促進、政府機関の情報対策強化のほか、法律の制定などの検討を進めている。

一方イギリスでは、先週「Fraud Act of 2006[7]」が可決された。同法はこれまで複数法の中でバラバラに取り扱われていたID窃盗を一つの法律で包括的に規定、取り締まるもので、例えばID窃盗を目的とするツールの所有に最高 5 年の禁固刑、ツールの作成に最高 10 年の禁固刑を課している。また、世界的には、2004 年にユネスコが国連にID窃盗に関する専門家委員会の設置を求めたのに応え、UNCCIEGFCMFI（United Nations Crime Commission Intergovernmental Expert Group on Fraud and the Criminal Misuse and Falsification of Identity）が設立された。UNCCIEGFCMFIでは、国連加盟国の政府及び民間セクタに対して、各国のID詐欺やオンライン詐欺の状況、体制や法制度を含めた取り組みに関するアンケートを実施している（回答期限は 2007 年 1 月のミーティング）。今後調査結果を活用し、警察、司執行機関による国際的な協力体制（関係者の連絡先等の明確化等）や民間セクタとの協力体制の確立を推進し、またID窃盗事件の扱いに関するガイドラインやベストプラクティスを策定し、ポリシーや捜査手法等のベンチマークとして利用されることが期待される。

連邦預金保険公社（FDIC）では、2004 年よりID窃取に関する様々な調査を行ってきており、2005 年 10 月には「FFIEC Authentication Guidance[8]（Authentication in an Internet Banking Environment）」、2006 年 8 月には「Authentication FAQs[9]」を策定した。FDICでは、金融機関に対して、リスクの高いトランザクション（顧客情報へのアクセス、ファンドの移動等）での複数ファクタの認証、及び階層化されたセキュリティを要求してきており、対象を消費者向けのサービスにも広げている。業界の動向として、中小規模の金融機関のほとんどがTSP（Technical Service Provider）を利用してオンラインバンキングのサービスを提供しており、「Authentication FAQs」ではTSPを利用する際の配慮事項等も記載されている。なお、TSPは様々な認証ソリューションを提供しており、例えば一般消費者の認証手

[7] 「Fraud Act of 2006」http://www.opsi.gov.uk/ACTS/acts2006/ukpga_20060035_en.pdf

[8] 「FFIEC Authentication Guidance」http://www.ffiec.gov/pdf/authentication_guidance.pdf

[9] 「Authentication FAQs 」http://www.fdic.gov/news/news/financial/2006/authentication_faq.pdf

段として複数デバイスの選択を提供したり、またバックエンドの振る舞い分析と組み合わせた認証ソリューション等も提供したりしている。

⑤ Practicum on Phish Data: Distinguishing Phish from Generic Spam for Alerting & Forensic Applications

本セッションでは、スパムやフィッシングメールへの対抗策として 2 つの取り組みが紹介された。以下にそれぞれのプロジェクトの概要を示す。

【SpotSpam】講演者：Thomas Rickert（German Internet Service Provider's Association）

SpotSpam は、EU やマイクロソフトの後援を受けているプロジェクトで、国際的なスパム事例のデータベースを構築し、脅威分析や、法執行機関、ISP による対策の支援に利用することを目的としている。この背景には、(1) スパムが国境を越えた国際的なスコープを持つ一方、警察・司法機関による国際的な情報共有は遅れていること、(2) スパム被害者である個々のユーザが訴訟を起こすことが難しいこと、などが挙げられる。また、SpotSpam は、スパム事例を広く集め、ISP 等の団体がスパマーに対して訴訟を起こす際に必要な証拠を提供することも目的とする。下記に情報収集の流れを示す。

① Compliant
　↓ 被害者がスパムを報告
② National Spambox（当該国のナショナルデータベース）
　↓ ナショナルデータベースから国際データベースに報告をフォワード
③ SpotSpam（国際的データベース）
　↓ 訴訟の原告となる企業・団体、検察当局などが集められたデータを利用
④ 被害を受けた ISP、企業・団体、警察・司法機関

既にプロトタイプが公開されているが、一つの問題として、EU にはデータ保護指令（95/96/EC）があり、個人に係る情報の第三者（国）への提供に制限があるため、情報の国際的な流通にあたっては慎重な確認が必要である。

【PILFER】講演者：Ian Fette（Carnegie Mellon University）

フィッシングメールに特化したフィルタリングツールとして、カーネギーメロン大学の PILFER（Phishing Identification by Learning on Features of Email Received）の取り組みが紹介された。

年々スパムフィルタの技術も高度化（ニューラルネットワークや学習アルゴリズムの利用等）してきているが、フィッシングメールは頻繁にこのフィルタリングをパスしてしま

う。彼らは、フィッシングメールの特徴を抽出することからはじめ、PILFER では独自のフィッシングメール分析アルゴリズムを実装した。フィッシングメールの以下の特徴を探す。

- HTML メールであること
- URL ドメインの登録期間
- javascript の存在
- メール内の URL リンク数やドメイン数、URL 内のドット（.）数、または IP ベース URL
- 特定単語（link, click here 等）にリンクされた URL のモーダル性
- 表記される URL と実際の URL（href タグ記載の URL）が不一致

テストにおいて、PILFER のフィッシングメール認識率は 93%と非常に高く、誤認率も false positive が 0.1%、false negative が 7%と低かった。なお、false negative は既存のスパムフィルタと組み合わせる事で 2%まで押さえることが可能であるとのこと。

⑥ ケーススタディ：eBay/PayPal

講演者：Mike Vergara（PayPal）

本セッションでは、PayPal におけるフィッシング詐欺の被害、対策の現状が紹介された。eBay と PayPal はフィッシング攻撃の No.1 のターゲット。これは両社のユーザが合わせて 3 億人超であること、多様な支払方法を扱い、お金のフローが流動的であること、誰もが参加できること等が原因と考えられる。幸いこれまでに大規模なフィッシング被害が発生したことはないが、フィッシング詐欺による電子商取引に対する長期的な悪影響について懸念される。

電子メールについては完全にコントロールすることは困難であり、ブロッキング対策として以下に取り組んでいるが、ユーザーフレンドリーなソリューションの開発を業界全体で検討していく必要がある。

- SPF/Sender ID
  → 実装済。ただし、ISP の数の多さ等から、効果が期待できる程度の導入には時間がかかると思われる
- DK/DKIM
  → 実装に向けて準備中。目標は全てのメールに署名が付けられ、署名がないメールはブロックすること。ただし、署名の検証法など検討事項も残る。

第 2 日目（11 月 15 日）

2 日目は4つの主題に関して、主にラウンドテーブルが行われた。各セッションについて、パネリストのプレゼンテーション及びパネルディスカッションの概要を下記に纏める。

⑦ ポリシー・ラウンドテーブル：Weaponized Domain Names

パネリスト：Jorge Aguila（e-la Caixa CSIRT）、Ben Butler（GoDaddy.com）、Dan Whetzel（VeriSign）、Brad Keller（Wachovia Corp.）、John Crain（ICANN）、Jon Nevett（ICANN）

本ラウンドテーブルでは、増加傾向にあるドメイン名を悪用したフィッシング詐欺の手口、および対策について論じられた。ドメイン名を悪用したフィッシング詐欺が急増しており、2006 年 10 月に確認されたフィッシングサイトの 56%がドメイン名を悪用している。その傾向としては、フィッシングに利用される TLD（Top Level Domain）も多様化が進んでおり、また.com 以外の（62% → 10%程度）.edu、.info といった他の GTLD や CCTLD の悪用が多く見られるようになってきている。下記、ドメイン名を悪用した典型的な手口の例を示す。

- スペル違いを巧妙に隠す　例：vvellsfargo.com（正：wellsfargo.com）、citilbank.com
- 信頼されそうなそれっぽいドメイン名　例：accountvalidator.com, onlineaccess.net
- ホスト名を加えて、本物らしく見せる
  例：http://chase.com.account-secure-logon.com
- 正しいドメイン名のカントリーコードだけを変える
- スパムフィルタをすり抜けるため、ワイルドカード DNS、rotating DNS、エイリアス等を利用

問題は、フィッシング詐欺等、何か問題が発生したとき対応が遅いドメイン登録事業者の存在である。フィッシャーはこうした事業者を選んでドメイン登録に利用しており、これらの事業者をどう改善していくかが大きな課題となる。こうした事業者のほとんどは、問題が発生した場合の連絡先が明確でなかったり、対応チーム（abuse dept.）が確立していないなどインシデント対応体制が整備されていない。事業者の間でこの問題を検討するポリシーグループの設立も議論されたが、現状のステータスは不明である。また、事業者にとっては、フィッシング報告自体の信憑性が問題となる。フィッシングサイトでないと知りつつも、知的財産権の侵害等、あるサイトを撤去させるために虚偽の報告をしてくることなどもあり、報告を鵜呑みにできない事情もあるとのこと。いずれにしても、事業者ごとに異なるインシデント報告・対応に係わるポリシーや基準を改善するための対策が必要となる。具体的な案は以下。

- Internet Corporation for Assigned Names and Numbers（ICANN）のポリシー・基準に組み込む。認定要件に追加する。

→ 非常に時間が掛かるほか、登録事業者の反発も予想される。また、CCTLD 登録事業者は ICANN の管轄でない為、そちらへの効果が期待できない。

・ APWG が登録事業者に対して「この事業者は（インシデント対応がしっかりしており）大丈夫」という認可を発行する。
・ PDRP（Phraud Dispute Resolution Policy）の策定
ICANN が策定した UDRP（統一ドメイン名紛争処理方針）同様のポリシーを作成する。

なお、APWG としても、この問題に関するワーキンググループの立ち上げが会員に問われた。ワーキンググループは ICANN と協力し、ICANN が登録事業者と開くミーティングに参加し、事業者がフィッシャーに悪用されるのを防ぐ手助けを提供していくことを検討。

⑧ <u>テクニカル・ラウンドテーブル：**Countering Botnet Scourges**</u>

パネリスト：David Dagon（Georgia Institute of Technology）、Rick Wesson（Alice's Resister）、Joe Stewart（SecureWorks）、Gary Warner（PIRT）、Richard Perlotto（ShadowServer）、Dave Monnier（REN-ISAC）、Jordan Medlen（Sago Networka）、Scott Chasin（MX Logic）

本ラウンドテーブルでは、DDoS 攻撃やスパムメール等の発信源・中継点として脅威を増すボットネットについて、現状と対策が論じられた。ボットネットが犯罪者にとって貴重なツールとして重宝され続ける背景には、ID 搾取といった犯罪行為がもたらす利益がマイクロソフト等の成功企業の純益を軽く数倍上回るビジネスであることが挙げられる。ボットマスターによるボットネット制御の手口も、ボットネット対策の強化に伴い進化している。最近では IRC の利用が廃れ、より特定が困難な HTTP や P2P を利用するケースが目立つようになってきている。冒頭に行われたボットネットの紹介では、現状の対策が功を奏していない理由とその対策として、以下が挙げられた。

【理由】
・ マルウェアの量が膨大すぎる
・ 報告が乏しい（報告を促すインセンティブや報告しなかった故の罰がない）
・ 報告（警告）が無視される・活用されない
・ 関係者間のコミュニケーションが欠如している
・ ポリシーや手順が不適切

【対策】
・ ボットネット対策・対応に関するガイドラインを提供する
・ 報告を義務付ける
・ グローバルレベルでの対策を検討する
・ インターネットの一部（感染部分）を隔離する方法を確立する
・ 電子メールをよりセキュアにする

ラウンドテーブルではこれらの状況を踏まえ、人々に行動を促し、また対策の有効性を評価するための方法が議論された。ジョージア工科大学の David Dagon 氏からは、ボットネットに対処していくためのアプローチとして、伝染病への感染と引っ掛けた 3 つのアプローチが紹介された。

１．Epidemiological Models
分析にあたっての伝染病の「SIRモデル」[10]の利用。ボットネットはコンピュータの電源が切られている間は機能しないため、通常のSIRモデルに人々がコンピュータを使用しない睡眠時間帯（世界各地の夜中にあたる時間帯）という変数を追加。分析においては、マルウェアをインターネットに流すタイミング、対策を取るタイミング、コンピュータの地理的状況の推移を考慮に入れておくことが重要。

２．Surveillance Studies
伝染病の勃発を監視する世界的ネットワーク網にならい、マルウェア監視と探知されたマルウェアの情報を共有することは有益である。Dagon 氏は、マルウェア情報の共有のためのマルウェアデータベースを構築している。

３．Population Estimate
感染するコンピュータを見ていると、同じコンピュータ群が何度も繰り返し感染していることがわかる。こうしたコンピュータ（セキュリティパッチを当てていない等）を見積もることで、集中的に対策を取るべき対象が明らかになる。

この他、Alice's RegisterのRick Wesson氏より、ネットワークマネージャがネットワークの状況を分析し、ボットネットを探知できるツールが紹介された（1 ヶ月以内には、ドメイン登録事業者がフィッシングサイトを特定するのに役立つツールも完成する予定[11]）。また、インターネット上のマルウェアの監視団体であるShadowServerのRichard Perlott氏は、フィッシングの監視や対策に取り組んでいるのがほぼボランティアでやっている業界団体であることを指摘し、こうした人々が活動を続けていける程度の支援を政府や企業が行うべきだと勧告した。

パネリストによるディスカッションで論題となったのは、「誰がセキュリティ対策に関する責任を負うか」であった。最も効果的な手段が取れる位置にいる ISP の名がまず挙がったが、メンバからは ISP にだけ責任を負わせるのはどうかという意見が多く聞かれた。やはり最終的エンドユーザが使用するコンピュータに対する責任を負うべきであるが、ユー

[10] S（susceptible：感染しやすい状態）、I（Infected：感染した状態）、R（resistant：抗体を持った状態）。ワクチン接種によって免疫をつけても、効果が薄れて再感染したり、新しいウィルスに感染する等、SIRを繰り返すことになる。
[11] 詳細はwww.support-intellegence.com参照。

ザは対策を行う知識も意志もないのが実情。サービスを提供する ISP 側が「ユーザのコンピュータに脆弱性がある場合、対策を取るまでネットワークには接続させない」といった対応や、それを後押しするような法規則の制定も提案された（例えば、「社会基盤であるインターネットの安全性を守るため、接続するコンピュータは一定のセキュリティを確保していなければならない」など)。これら対策の是非については賛否が分かれた。

⑨ サーチ・ラウンドテーブル：Behavioral Vulnerabilities and Human Factors

パネリスト：Jeff Wilbur（Iconix)、Dr. Lorrie Cranor（Carnegie Mellon University)、Dr. Markus Jacobsson（Indiana University)、Dan Schultzer（Financial Services Technology Institution）

セキュリティは技術だけでなく、セキュリティ技術を効果的に使うことができるかという人的要因に大きく拠る。本ラウンドテーブルでは、ユーザの行動や考え方に焦点を当て、どのようなメールの文面、Web デザイン、状況において、ユーザがフィッシング詐欺に引っ掛かり易いかという研究結果が発表された。調査では、ユーザが極めて主観的かつ曖昧な基準でフィッシングの「フィッシングっぽさ」を判断していること、教育にも方法により効果が見られる等の結果が示された。

インディアナ大学の Markus Jacobsson 博士は、様々な種類のフィッシングメールを見せ、それぞれのフィッシングらしさを「絶対フィッシングメール」から「絶対本物のメール」の 5 段階で評価するよう被験者に依頼した。調査結果でみられるユーザの判断基準は以下。

【本物だと判断する要素】
- パーソナライズされている（XX 様、と個人名明記で送付）
- メール内のリンク上にマウスが掛かると URL がポップアップで表示される
- Verisign ロゴが貼付してある（他の証明書ベンダのロゴでは効果なし）
- クリック先のウェブサイトに著作権等、法的文言がきちんと掲載されている
- 差出人が個人名（「カスタマーサービス」等だけでなく、「カスタマーサービス担当 XX」）
- 強制（「～してください。さもないと・・・」ではなく、任意（「確認してみてください」）
- 電話等でのフォロー

【フィッシングメールだと判断する要素】
- スペルミスがある（ユーザは非常に敏感）
- URL が架空っぽい、または IP アドレスである
- 「このメールは本物です」と書かれている、または安全性を強調している
- クリック先のウェブサイトのデザインが素人っぽい

また、カーネギーメロン大学の Lorrie Cranor 博士は、コンピュータに詳しくない一般人を被験者として、セキュリティ機能や教育によってフィッシングメールへの対応に違いが

出るか等の実験を行った。Cranor 博士の調査結果は以下。

- 金融関係の情報を開示するよう求められて、おかしいと感じると答えたのは全体の 55%（約半数はおかしいとも思わない）
- あるタイプのフィッシング詐欺について知っていても、他のタイプのフィッシング詐欺に対してはその知識は活かされない
- メールの送信元が自分の取引企業（口座を持っている等）であれば怪しいとは思わない
- 電子証明書の期限切れ等のポップアップは良くわからないから無視する
- ツールバーのフィッシングサイト監視ツールに頼る
  （ただし、ツールバーのフィッシングサイト認識率は全体的に低いのも事実）
- 教育資料を読んだ直後であれば、フィッシングへの判断力が飛躍的に向上する

教育に関しては、効果がある事は確かだが、問題はどうやってユーザに教育資料を読ませるかである。実験環境では強制だが、実際にはユーザが自ら時間を削って教育資料を読む事はない。教育目的のフィッシングメールの送信も手段の一つ。例えば、ユーザがメール内の URL をクリックすると「貴方はフィッシング詐欺に引っ掛かりました」といった警告及び啓蒙サイトに誘導することが考えられる。

いずれにせよ、ユーザは知識も乏しく騙され易く、経験から学ぶこともあまりない。メール＋電話という 2 段構えで詐欺が行われた場合、被害率が急増する可能性が高いのも脅威である。企業側では、ユーザ側の考え方や情報の捉え方に十分配慮した URL（ドメイン名）やメールの文言、ウェブサイトのデザイン、サーバ側での確実なセキュリティ対策の実装等が求められる。またユーザに対しても、辛抱強く教育を行っていくことが大事である。

⑩ Counter-e.Crime Data Resources, Tools, Techniques and Schema

講演者：Pat Cain（APWG）、kent Davidson（APWG/ioflux）、Dave Jevans（APWG）

本セッションでは、APWG で進めている、インシデントの報告や情報交換のためのデータフォーマットの策定、インシデント報告及び対応にあたっての連絡先データベースの紹介が行われた。

【データ交換フォーマットとリポジトリ】

フィッシング・インシデントに関する情報交換をスムーズにするため、APWG では情報交換用のデータフォーマットとして、Incident Object Description and Exchange Format（IODEF）の活用に取り組んでいる。IODEF は CSIRT がインシデントの情報を共有するためのデータフォーマットのための規定であり、用語や記述すべき内容、サポート要件等が定められている。APWG では、IODEF を利用して、サイバー犯罪やフィッシング詐欺に関する情報を共有し、データベースとして、アクセスできるようにしていく予定。

【連絡先データベース】

連絡先データベースは、フィッシング・インシデントの報告、関係者への通知を迅速に行うための APWG のシステム。APWG メンバにフィッシング等のインシデント関係で連絡を取りたい場合、企業・団体名から担当者が特定でき、電子メール等が送れるようになっている。メンバは担当者や連絡先に変更が生じた場合、データベースを更新して常に最新の連絡先情報を維持するよう求められる。データベースは現在まだ開発中。来週中、遅くとも 11 月中には完成し、メンバに公開される予定。

Ⅲ．所感

ミーティングには 1 日目、2 日目両日とも 200 名ぐらいのメンバが参加しており、また質問も活発に飛び交い、フィッシングに対して各企業・各団体が非常に真剣に取り組んでいる姿勢がうかがえた。一方でアジアからの参加者は日本及び韓国だけであり、かつ取り組み状況等からも欧米諸国とアジアの間では明らかにフィッシングに対する取り組みに温度差が存在するように感じた（そもそも被害が少ないのが根底にあるが)。

フィッシングの攻撃が従来のソーシャルエンジニアリング的な詐欺行為からボットやクライムウェアを活用したより技術的な方向に進化しており、対策もより複雑、かつ広範囲な業界・関連団体の協力が不可欠な状況になっている。特にクライムウェアを利用したフィッシング被害の拡大は深刻な状況になりつつあるように感じられた。こういった状況において、欧米諸国の政府・業界団体では、フィッシング/ID 窃盗に関する取り締まりを強化する法整備やガイドラインの策定、さらには情報共有のための協力体制作りが積極的に進められており、これら関係者による問題解決に向けた意欲が強く感じられた。特に FDIC の「FFIEC Authentication Guidance」やドイツにおけるオンラインバンキング関連の規則、また英国における「Fraud Act of 2006」など、法令関連の整備やガイドラインの策定が進んでいることに注目されられた。

一方で、フィッシング対策には従来同様の根気強い教育・啓蒙活動、またはタイムリーな警告の発信が重要であることも事実であり、そういう意味では、Human Factors のような調査・研究もフィッシング対策を考える上で、また教育手段を考える上でも非常に有益であると考えられる。やはりフィッシング対策の最後の砦はユーザ自身であり、Vishing 等電話を活用した新しい手口に関しても普及啓蒙やユーザへの教育が不可欠であると考えられる。

日本国内においては、幸いフィッシング詐欺が欧米ほど深刻化していない状況にあるが、今年一年での英国やドイツ等での状況などから推測しても、日本でも「フィッシング対策協議会」のような活動を通して、さらなる情報連絡・連携体制の構築、人的資源の共有等を進めていく必要があると考える。

以上