

「IPv4 アドレス枯渇対応タスクフォース」 発足の背景と今後の活動

タスクフォース代表/東京大学 情報理工学系研究科 教授 江崎 浩

目的はIPv6 普及ではなく IPv4 枯渇への対応

インターネットとは、自律的に運用されるコンピューターネットワークを相互接続したネットワークのネットワークである。インターネットの父と呼ばれる Dr. Robert Kahn が「インターネットは、論理的なアーキテクチャであり、スイッチやルーターで形成された物理的なネットワークのことではない。インターネットは、デジタル情報が透明に流通する"コモンズ"の環境を提供する基盤である」と述べている通り、誰でも自由に利用できるのがインターネットの特徴である。

これを実現するためには、グローバルな IP アドレスの存在が暗黙の前提となっていた。IP アドレスの不足に対応することを主な目的として IPv6 技術の標準化と製品開発が展開されてきたが、IPv6 技術の普及よりも早く、現在のインターネットで最も広く利用されている「IPv4 アドレス」が枯渇の危機を迎えつつある。このような状況に対応するために、われわれは総務省およびテレコム/インターネット関連12団体とともに「IPv4 アドレス枯渇対応タスクフォース」¹⁾を、2008年9月6日に設立した(2008年10月6日時点で14団体に増加)。

本タスクフォースの活動目的は「IPv6の導入・普及」ではなく、「IPv4 アドレスの枯渇への対応」にある。すなわち、これから2~3年後には、新規のグローバル

IPv4 アドレスの取得が困難となることが確実となってきた。それまでに、IPv6の導入と完全な移行は事実上不可能であり、IPv4 グローバルアドレスが枯渇した状況においても、一般ユーザーの方々がサービスの低下や障害を経験されないような対応を、サービスの提供者側が適切に行う必要がある。

情報同期と協力関係を確立する必要

サービスの提供者側において、最も影響を受けるのは「新規ビジネス」の展開を目指す事業者と、今後ビジネスの拡大を目指す事業者(=すべての事業者)となる。さらに、すべてのステークホルダーが少なからぬ影響を受け、現在、十分な量の IPv4 グローバルアドレスを保持している事業者においても、影響が発生することを十分に認識しなければならない。すでに、IPv4 アドレスの枯渇の問題は、経済活動に少なからぬ影響を及ぼすことが OECD においても認識されるに至っている。

このような現状に対しては、すべてのステークホルダーが情報の同期と協力関係を確立して対応することが必要となる。具体的には、システムのオーナー、システムインテグレーター、システムオペレーター、ネットワークプロバイダー、ICT 機器ベンダー、ICT ソフトウェアベンダー、一般ユーザー、企業ユーザー、あるいは投資家やアナリストになる。これら、すべ

でのプレーヤーにとって、今回の問題は、システムネットワーク関連事業の変革と創成の可能性が存在するという意味においては、ビジネスチャンスと捉えることもできるだろう。

既存事業者への優遇措置は期待することが難しく、既存事業者も少なからぬ影響を受ける。また、IPv4 アドレスの取引市場は構築される可能性は十分にあるが、この取引市場からの IPv4 アドレスの新規調達を前提とすることはリスクが伴うこととなるだろう。さらに、IPv4 アドレス枯渇の対応の遅れは、システムネットワークのセキュリティ問題となる可能性もすでに指摘されている。このように、ネットワーク関連の事業者は、今回の問題を、事業継続と事業発展に関する「リスク管理」としてとらえる必要があると考えられる。

各ステークホルダーへのメッセージ

以下に、各ステークホルダーに対する本タスクフォースからのメッセージを列挙することとする。

- ① ISP : IPv4 アドレスの枯渇に対し、キャリアグレード NAT の導入が行われることが考えられるが、これはあくまで暫定解にしかならず、IPv6 Only サーバーの導入への対応を行わざるをえない。
- ② iDC、ASP、CSP : サーバーには、グローバルアドレスが必要であるため、IPv4 アドレスの枯渇に伴って、最も困るのが

「サーバー事業者」である。少なくとも、IPv4アドレスの枯渇後しばらくは、IPv4グローバルサービスを提供できないIDCは、提供可能なIDCに比べてビジネスチャンスに少なからぬ差が発生してしまうことが推定される。

③ SaaSの事業者：SaaSへの移行が困難になる可能性も存在する。

④ 機器ベンダー、アプリケーションベンダー：Multiple-NATとMulti-Prefixへの対応を行わないと製品の不具合とされる可能性が存在する。

問題解決支援のための具体策

このような状況に対して、タスクフォースに参画する14団体は連携し、その問題解決の支援を推進する予定だ。

具体的には、①全体課題リストの作成と管理、②関係団体への広報啓発活動、③質問窓口の連携、④テストベッドの企画と運営、⑤教育プログラムの企画・開発と運営、⑥セキュリティ対策の課題検討と啓発、⑦システムインテグレーター等、これまで関わりが少なかったセグメントへのリーチである。

特に、教育プログラムの作成は急務であり、最初のプログラムの企画と実施を、11月25日(火)から東京秋葉原で開催されるInternetWeek2008⁽²⁾において計画している。また、教育プログラムは、.comマスター、シスコアカデミー、マイクロソフトなど、技術資格関連のプログ



「IPv4アドレス枯渇対応タスクフォース」発足式に集まった人々



活動趣旨と参加団体を記したオブジェ

ラムとの連携・協調を積極的に推進する予定。

関係各位のご協力とご尽力に感謝ならびに期待するとともに、今回の対応がわが国の国際競争力の向上に貢献することを期待している。

IPv4 アドレス枯渇対応 タスクフォース参加団体

IPv6普及・高度化推進協議会
(会長：慶應義塾大学 教授 村井純)
財団法人インターネット協会
(IAJapan/理事長：日本電気 社長 矢野薫)
次世代IX研究会
(Distix/代表：東京大学 教授 江崎浩)
情報通信ネットワーク産業協会
(CIAJ/会長：富士通 会長 間塚道義)
社団法人テレコムサービス協会
(会長：ITホールディングス 会長 中尾哲雄)
社団法人電気通信事業者協会
(TCA/会長：ソフトバンクモバイル株式会社

社長兼CEO 孫正義)
財団法人電気通信端末機器審査協会
(JATE/会長：東京大学名誉教授 齊藤忠夫)
社団法人日本インターネットプロバイダー協会
(JAIPA/会長：ディー・エヌ・エー 渡辺武経)
社団法人日本ケーブルテレビ連盟
(JCTA/理事長：唐澤俊二郎)
財団法人日本データ通信協会
(NIC/理事長：森 清)
社団法人日本ネットワーク
インフォメーションセンター
(JPNIC/理事長：早稲田大学教授 後藤滋樹)
日本ネットワーク・オペレーターズ・グループ
(JANOG/会長：池尻雄一)
日本UNIXユーザ会
(jus/会長：湯川隆広 創夢)
WIDEプロジェクト
(代表：村井純 慶應義塾大学教授)

- (1) IPv4 アドレス枯渇対応タスクフォース
<http://www.v6pc.jp/v4exh/index.phtml>
(2) InternetWeek2008
<http://internetweek.jp/>

日本の技術者へのメッセージ 「P2P基本提言」の概要

東京大学 情報理工学系研究科 教授 江崎 浩

NPO法人ブロードバンド・アソシエーション(理事長:板谷 駿一氏)では、P2P技術のような革新的な技術を社会が抑圧するのではなく、その可能性を社会が認め、自身の成長とイノベーションのために御することの必要性をうたった提言書をまとめた。2008年9月18日にその内容を公開するとともに、9月22日に東京大学においてシンポジウムを開催し、その趣旨と関連する研究活動の報告を行った。

「P2P基本提言」の要旨

以下が、本提言書の要旨である。

- ① インターネットにおける問題を解決する手段として、P2P技術にはさまざまな可能性がある。これは今後のインターネット社会にとって不可欠な技術である。P2P技術は商用化の時代へ突入しており、社会的インフラとして積極的に取り入れられるべきである。
- ② P2P技術に関連して問題となった事項は、すべてP2P技術の本質的問題ではなく、しかも、現在、商用で用いられているP2Pネットワークでは解決済みである。
- ③ 日本における先進的なソフトウェア開発、とくにP2P技術の開発は、種々の裁判例により萎縮しており、世界的に立ち遅れている。日本の技術発展のためには、技術者が安心して開発できる環境を実現しなくてはならない。
- ④ P2P技術の開発をめぐる、現在も法的問題等の課題があり、このような問題

を速やかに解決すべく、立法を含めた是正手段が講じられるべきである。

「インターネットにおける中立性」とP2P技術

本提言は、「インターネットにおける中立性」を維持し、インターネットの継続的な成長と発展を実現するために、P2P技術が必須の技術であること、およびその発展の必要性と可能性を、インターネットに関連するステークホルダーの皆さんと共有し、健全な研究開発と導入、ならびに利用を推進することを目的としている。

「インターネットにおける中立性」においては、人々は、自由にコモンズに資する情報通信資源を利用する権利を持ち、情報通信資源を持つものはその資源がコモンズに資する場合には、公正なルールに従って、これを利用可能にする義務を持つ(排他性の否定)。

- ① 消費者は、適法なインターネット・コンテンツの選択とアクセスの権利を有する。
- ② 消費者は、法律の要件に従うことを要件として、自らが選択するアプリケーション、サービスを運営する権利を有する。
- ③ 消費者は、ネットワークに害を及ぼさない適法な機器とネットワークを接続する権利を有する。
- ④ 消費者は、ネットワークプロバイダー、アプリケーションプロバイダーとの競争に参画する権利を有する。

上記の原則に従うべきとのコンセンサ

スがインターネットの運用者や利用者間で共有されているにもかかわらず、P2P技術の利用に関しては、わが国とそれ以外の国々では、その扱いが大きく異なる。具体的には、P2P技術を適用したアプリケーションは、必要以上にその使用が制限されているとともに、その研究開発活動自体が抑制・制限、あるいは否定される現象が見られる。

以下、本提言書の内容の概要を簡単に説明する。

技術、経済の両面でP2Pは有効

P2P、とくにP2Pを用いたファイル共有アプリケーションが生成するトラフィックが、インターネット上を流れるトラフィックの大部分を占めるとの認識が一般化しているようだが、ある研究報告では、すでに消費者の需要は、高品質なインタラクティブコンテンツへと急速にシフトしていることが、具体的な商用ISPのトラフィックデータの解析から示されつつある。

また、国際線における、海外からわが国に流入するトラフィックの超過現象は、すでに国内のプロバイダーにとって大きな負担となりつつある。この問題は、グローバルな視点でのP2P技術の導入により解決することが可能となるかもしれない。P2P技術が、資源の効率的活用、耐故障性の向上、システムの大規模化への対応、新規サービスの導入障壁の低減などに貢献する可能性を持つことは、専門

知識を持つ技術者の間では、すでに広く認識されている。P2P技術を積極的に利用した大規模なコンテンツ配信サービスの効率化が商用システムにおいて実現されており、その有効性を技術面、経済面の両方で証明している例も多数報告されている。

正しく理解したい「著作権侵害」 「情報漏えい」問題

P2P技術が、技術開発の意図とは離れて、著作権侵害や情報漏えいと、直接的に関連して取り上げられる場合が見受けられる。著作権侵害や情報漏えいはP2P技術によって発生したのではなく、P2P以外の通常の情報通信システムにおいても同様に発生していることを正確に理解する必要がある。

情報漏えいは、P2P技術を用いない従来のクライアント・サーバー型システムにおいても頻繁に発生しており、古くは電子メールを介したウイルスに起因する情報漏えいなどが存在する。著作権侵害の問題も同様に、P2P技術を適用しないシステムにおいても頻繁に発生しているのが実状である。

誤解釈の是正と立法を含む 諸制度の改善必要

われわれが最も危惧すべき点は、P2Pシステムの提供者に対する著作権侵害等

の責任を問う裁判例や、P2Pファイル共有ソフトウェアの開発者に対する刑事立件などを通じて、ソフトウェア技術者、さらには企業の経営者とその研究開発を委縮している状況にある。インターネットにおいて、キャッシュ保持による著作権侵害責任を恐れるあまり、他国と比べ通信に偏りが著しくなっている状況は、その一例と言えるだろう。P2P技術の発展が効率のよいコンテンツ流通インフラを実現し、結果的にコンテンツホルダーにより多くの利益をもたらすことになるということに対する理解が、残念ながらわが国の産業界に不足しているように思われる。

また、P2P技術の開発と、P2Pシステムを違法ビジネスに利用する行為は、正確に分離して考えなければならない。このような、誤った司法的解釈を是正し、わが国の国際競争力の向上の観点から、立法を含めた諸制度の改善を行うべきである。本提言書が、このような活動を推進する契機となることを期待している。

P2P 関連問題研究会メンバー

江崎浩(東京大学・委員長)
石川宏
(NTTアドバンステクノロジ・副委員長)
斉藤賢爾(慶應義塾大学)
津田大介(IT・音楽ジャーナリスト)
石橋聡(NTT)



NPO法人ブロードバンド・アソシエーションのホームページ

伊勢幸一(ライブドア)
壇利光(弁護士)
古川享(慶應義塾大学)
持田侑宏(フランステレコム)
安田浩(東京電機大学)
山下達也(NTTコミュニケーションズ)
吉開範章(日本大学)
早稲田祐美子(森・濱田松本法律事務所)
飯野嘉郎(ブロードバンド・アソシエーション)

NPO法人ブロードバンド・
アソシエーション

<http://www.npo-ba.org/>

ネットの未来を創るベンチャー企業が世界中から終結「TechCrunch50」カンファレンス参加報告

株式会社インプレスR&D インターネットメディア総合研究所 堀田有利江

新興企業の登竜門「TechCrunch50」

2008年9月8日から10日、米国サンフランシスコで、いま最もホットなIT系ベンチャー企業が集まる「TechCrunch50」が開催された。

入場料が2995米ドル(約30万円以上)という高額にもかかわらず、世界中から1700人以上が集まり、会場は熱気と躍動感で包まれていた。

同カンファレンスでは、事前に応募があったスタートアップ企業の中から、面白い内容のサービスをもつ企業を審査員が選考し、カンファレンス当日、選ばれた企業がプレゼンテーションデモを行う。今年は、応募総数約1000社の中からファイナリスト52社が選抜され、自社サービスを紹介した。

日本からの参加企業

今年は初めて、日本からも3社がノミネートされ、熱気高まる会場でデモを行った。

ファイナリスト52社に勝ち残り、1000人を超える聴衆の前でデモを行った日本企業のサービスは下記の3つだ。

Rinen「OpenTrace」

環境レーティングシステムと称したこのサービスは、商品を原材料までさかのぼって、産地からの輸送にかかる燃料まで含めた商品単体の環境負荷を割り出すウ

ェブのサービス。企業はその結果を刷り出したステッカーを商品に貼って環境の取り組みをアピールできる。

頓知(Tonchidot)「Sekai Camera」
iPhone専用のソーシャル・タグ・ツール。詳細は後述する。

日立製作所「Gazopa」
類似画像検索エンジン。日立制作所の社内ベンチャーが立ち上げた。「形状」を検索キーとして世界中のウェブサイトから集めた画像から似た画像を探し出してくれる。

そのほか、下記の2社がデモ出展し、日本からは全部で5社が参加した。

Adlib「Waget」
モバイル向け店舗・レストラン情報提供。ユーザーがその店の電話番号を件名としてWagetにメールすると、URL、地図、割引クーポンなどがメールで返信されてくる。また、ユーザー自身が情報をデータベースに追加できる。

Mulodo「Deckkr」
Firefox 3のエクステンション。タブやウィンドウを切り換えなくてもいろいろなウェブの閲覧ができる。

これらの中で、iPhoneのカメラを利用し、そこに写る目の前の現実世界とそれ

に関する情報をタグで結ぶ「Sekai Camera」の井口尊仁氏のプレゼンテーションは特に鮮烈で、印象深かった。

同サービスを利用し、iPhoneのカメラを通して自分の周辺の現実世界を見ると、周辺にあるものやサービスに関する情報が、ポップアップで表示される。

たとえば、秋葉原でこのサービスを利用すると、周辺にある電化製品店から提供されているディスカウント商品情報や、商品に関する詳細情報を取得したりできる。また、秋葉原を背景に、自分の好きなアニメキャラクターと一緒に写真を撮り、それを友人とシェアしたりもできる。

技術的には、位置認識技術、加速度センサー、タグなどを利用し、その場所と関連するネット上のデータを連動させており、同サービスの応用範囲や用途は幅広そうだ。

数多くのベンチャー企業を見ていると、過半数はどうしても、どこかで以前見たことがあるような内容のサービスが多かったりする。しかし、「Sekai Camera」は、全く斬新かつクリエイティブな印象を与え、満場の大喝采を浴びた。

日本のネット企業の歴史に残るプレゼン

舞台には、プレゼンを行うベンチャー企業に加えて、それらサービスに対して賛否評論を言う専門家パネリストもいるのだが、他の参加企業にはもっと辛口なコメントをする専門家パネリストも、うち



会場入り口



各社がプレゼンを行うステージの様子

一人が、グーグルに買収される可能性があるのではといったことを言及するほどだった。

これに対し、同じくパネリストとして参加していたO'Reilly Mediaのティム・オライリー氏はもう少し辛辣な質問を投げかけた。

しかし、井口氏は吉本風の切り返して、会場を爆笑の渦に巻き込んだ。同サービスは、後日、現地のさまざまなメディアやブログでも取り上げられ、今回最も愉快で話題になったサービスの一つとって間違いなだろう。

ティム・オライリー氏の質問に対し、井口氏の回答は技術面での詳細説明を端折った部分があったため、中には、「Sekai Camera」の技術的な実現性を疑問視する声もあったが、iPhoneアプリの未来の可能性をいち早く垣間見せてくれたという点で、注目度は高かった。

同社のデモは、日本のネット企業の海外市場における可能性を強烈に感じさせてくれた。

米国に渡る日本のネット企業の歴史に残る一幕だったようにも思う。

【ファイナリストの52社】

<http://www.techcrunch.com/2008/09/08/announcing-the-techcrunch50-finalists/>

【Sekai Cameraのデモの様様】

<http://www.techcrunch50.com/2008/conference/presenter.php?presenter=71#video>

【TechCrunch日本語ページ】

<http://jp.techcrunch.com/>



デモ展示場の様子



日立からはGazopaの名前で社内ベンチャーが参加



日本から参加したTonchidotの井口氏。個性あふれる存在感を見せた



パネリストとして参加していたティム・オライリー氏が疑心暗鬼に投げかける質問に対し、井口氏は個性あふれる回答で会場を笑いの渦に巻き込んだ



米国でもモバイル向けサービスを提供する企業が増えてきた



新たなSNSの形を提案する企業

フィッシング詐欺の被害状況と警戒すべき新手法 事業者とエンドユーザーがとるべき対策は？

JPCERTコーディネーションセンター 早期警戒グループ 情報セキュリティアナリスト 小宮山 功一朗

「フィッシング」とは

攻撃者が正規のサイトを模した偽サイトにユーザーをおびき寄せ、個人情報やクレジットカード番号などを入力させる詐欺の手口をフィッシングと呼ぶ。この際、詐欺に用いられる偽サイトをフィッシングサイトと呼んでいる。

被害の形はさまざまであるが、たとえば、インターネットバンキングの認証情報が盗まれると、その情報を悪用されて銀行口座から預金を引き出されてしまう。また、インターネットオークションサイトの認証情報が盗まれ、その情報を利用して架空の出品や入札が行われるなどという被害が国内においても実際に発生している。

本記事は、コンピューターやネットワークについてある程度の知識を持つ読者を対象に、国内外のフィッシング被害の現状と最近の傾向、そしてとるべき対策について解説する。

フィッシング被害の現状

米国でのフィッシング被害

米国 連邦取引委員会において確認されたインターネットによる詐欺の被害総額は、2005年3.3億ドル、2006年5.9億ドル、2007年5.2億ドルだった¹⁾。米国では、確認されたフィッシングサイトの数、フィッシングサイトにユーザーをおびき寄せるメール(フィッシングメール)の数はいずれ

も上昇している。自動化ツールによりフィッシングのプロセスが効率化され、攻撃者によってマネーロンダリングの手法も確立されるなど、フィッシングが「金銭詐取を目的」として、「組織的に行われる犯罪」であるという実態が鮮明に浮かび上がってきている。

国内でのフィッシング被害

これに比して、日本を含めた東アジアでのフィッシング被害は、非常に緩やかに推移している。図1は、JPCERT/CCに寄せられたフィッシングの届け出件数の推移であるが、2006年から現在まで大きな変化がないのが見てとれる。(図1参照)

諸外国のような大規模な被害が発生していない原因としては、言葉の壁や現金による取引を好む商習慣が考えられる。また、日本においては振り込め詐欺やワンクリック詐欺による被害が依然として多く、相対的に手間のかかるフィッシングは攻撃者にとって効率がよい手法とは考えられていない可能性もある。

個々の事例を確認していくと、14歳の男子中学生がオンラインゲーム会社のWebサイトを模したフィッシングサイトを公開した事例²⁾もあり、諸外国とはフィッシングの動機・性質に差異があるように思われる。また、国内のポータルサイト、ISPやSNSなどのユーザーを狙ったフィッシングも確認されている。

注意すべきフィッシングの新手法

国内のフィッシングによる金銭被害が諸外国に比して少ないとはいえ、警戒すべき変化がいくつかある。ここでは「スピア・フィッシング」と「ヴィッシング(Vishing)」および「ファストフラックス(FastFlux)」という3つの手法についてご紹介する。

スピア・フィッシング

不特定多数を対象にメールを送り、そのうちの何%かが騙されることを期待して行われる通常のフィッシングに対して、あらかじめターゲットを限定し、ターゲットに応じて件名や文面を工夫するタイプのフィッシングをスピア・フィッシングと呼ぶ。たとえば企業の重役宛てに、裁判所からの召喚状を装ったメールが送られるなどの事例が確認されている。

スピア・フィッシングの存在がメディアなどで取り上げられるようになったのは2005年頃であるが、日本でも中央省庁や大企業にスピア・フィッシングが試みられたことが明らかになっている³⁾。フィッシングにソーシャルエンジニアリングの手法を取り入れることで、攻撃成功率が4倍になるという海外での研究⁴⁾もあり、企業等の組織において「不審なメールは開かない」という原則を再度徹底する必要があるといえる。

ヴィッシング(Vishing)

既存のフィッシングでは、フィッシングサ

イトの入力フォームにユーザーが秘密情報を入力するように仕向ける手法が一般的だった。これに対して、近年国内でも「ヴィッシング(Vishing)」という手法が確認されている。これはユーザーを特定の番号に電話させるように仕向け、録音された応答メッセージにより秘密情報を入力するよう誘導するものである。この場合、フィッシングメールにはURLではなく電話番号が記載されている。Webサイトに設けられたフォームへの入力には警戒をしているユーザーでも、電話ということで油断してしまい、被害にあう可能性がある。

ファストフラックス(Fast Flux)

「Fast Flux 手法」とは、フィッシングサイトをより長い時間インターネット上で活動させるために攻撃者が用いる技術の一つだ。攻撃者は、特定のホスト名に、数多くのIPアドレスを短い有効期限で設定する。これにより、たとえばその一つのIPアドレスが到達不能になっても、残る多くのホストでフィッシングサイトの稼働を続けることができる。

関係組織が連携して、このような有害サイトを停止(テイクダウン)させる努力をしているが、Fast Flux 手法を使った有害サイトでは、IPアドレスが次々と変更されることで、対応が困難な状況になっている。JPCERT/CCに寄せられるフィッシングサイトの報告の中にも、Fast Flux 手法が用いられたケースが確認さ

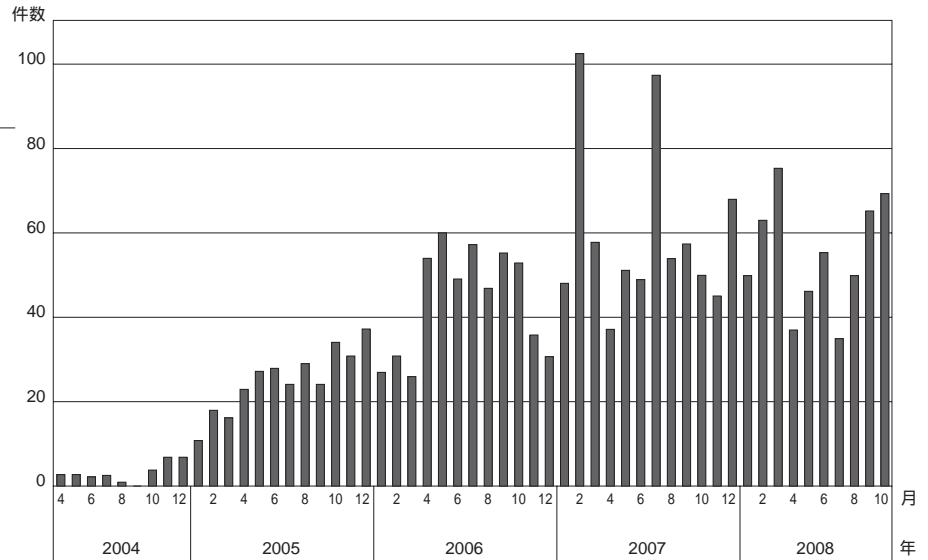


図1 フィッシング報告件数の月次推移

れている。Fast Flux 手法がさまざまな有害サイトの停止を難しくしている状況から、ICANN等も対応の検討を始めている⁵⁾。

フィッシング対策

フィッシングの手口は日々巧妙になっており、対策を行う側の裏をかくような手法がいくつも確認されている。ここでは関係組織の取り組みに加えて、エンドユーザーやオンラインサービス事業者がとるべき対策について簡単に解説する。

関係機関の取り組み

フィッシングへの対策のため、現在も多くの組織や企業がさまざまな活動を行っている。ここではそのごく一部を紹介する。

APWG (<http://www.apwg.org>)

APWGは、フィッシングやクライムウェア対策に関する情報共有を目的に2003年に発足した非営利のワーキンググループである。会員は大学などの研究者、オン

ラインサービス事業者、CSIRT、法執行機関などさまざまである。年に2回行われる会合、および参加者向けメーリングリストではフィッシングに関する最新の情報が交換されている。日本からはJPCERT/CCなど数組織が参加、協力している。

フィッシング対策協議会

(<http://www.antiphishing.jp/>)

日本国内でのフィッシングに関する情報収集や制度/技術の検討を目的に2005年に設立された。現在30近い企業が参加し、定期的にフィッシング対策について協議を行っている。また協議会のWebサイトでは、ユーザーに対する啓発活動の一環として、フィッシングの具体的な事例を紹介している。

JPCERTコーディネーションセンター

(JPCERT/CC) (<http://www.jpccert.or.jp>)

JPCERT/CCは、フィッシングだけでなくインターネットを介して発生するさまざまなコンピューターセキュリティインシデントの報告を受け付け、対応を支援する

非営利の組織である。海外関連組織との緊密な協力関係を活用し、2004年からフィッシングサイトの停止コーディネーションを行っている。また、停止コーディネーションの実態からフィッシングの傾向を分析し、その結果に基づく啓発活動を行っている。またAPWGやフィッシング対策協議会にオブザーバーとして参加し、対策の現場からの知見を伝えている。

エンドユーザー向けの対策

エンドユーザーがフィッシングによる被害にあわないために、気をつけるべき基本的な原則は、以下の2つである。

①自分が利用するサービスが使用するドメイン名を知っておくこと

自分が利用するサービス(インターネットバンキング、オークション)が使用するドメイン名を事前に確認しておく。利用者向けのカードや郵送物には多くの場合ドメイン名(URL)が印刷されている。記載がない場合、電話などで問い合わせしておく。

②情報入力時にアドレスバーに表示されたURLを確認し、正規サービスのドメイン名であることを確認すること

オンラインサービス等で他人には知られたくない情報を入力するときは、URLを確認し、①で確認したドメイン名と異なっている場合には閲覧や情報入力を中止すること。

以上の2つを徹底するだけでも、現在行われているフィッシングの大半を見破る

ことが可能だ。エンドユーザー向けに啓発活動を行う際には、この点を強調することが有効であると考えられる。

事業者向けの対策

諸外国でのフィッシングの現状を観察すると、フィッシングや不正利用対策を十分に行っている企業のWebサイトは、そうでない企業と比較して狙われにくいという傾向がある。オンラインサービス提供事業者は、みずからのWebサイト等について、フィッシングに悪用されそうなデザインや機能(たとえば、Webサイトでアドレスバーを隠す等)を用いない工夫を行うことが大切である。

事業者が行うべき対策については、フィッシング対策協議会が2008年9月に公開した「フィッシング対策ガイドライン」に網羅的に解説されている。その中から、自社が目指すセキュリティレベルに応じて、効果的な対策を実施するとよい。

まとめ

現在のところ、国内でのフィッシング被害は、諸外国との比較においては小規模である。しかしながら、インターネットバンキングやオンラインでの買い物などインターネット上での商取引が一般的になるにつれ、そのユーザーを騙そうとするフィッシングが増えていくことが予想される。現在、業界団体/セキュリティベンダー/先進的なオンラインサービス事業者等が協

力してフィッシング対策に取り組んでいるが、フィッシングは、セキュリティ関係者だけが努力をして解決できる問題ではない。インターネットを利用する一人ひとりがフィッシングやオンライン詐欺について正しい知識を持ち、それを自らの顧客や、周囲のユーザーに適切に伝えていくことが重要である。

(1)Consumer Sentinel Annual Fraud and Identity Theft Reports

<http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinelcy2007.pdf>

(2)14歳の男子中学生の事例
平成18年のサイバー犯罪の検挙および相談状況について(警察庁/2007年2月)

URL : <http://www.npa.go.jp/cyber/statics/h18/pdf34.pdf>

不正アクセス行為の発生状況およびアクセス制御機能に関する技術の研究開発の状況(総務省/2007年2月)

http://www.soumu.go.jp/s-news/2007/070222_3.html

(3)警察を標的にしたスパイ型フィッシングメールが増加(警察庁の坂明氏講演、ITpro掲載記事/2006年5月29日)

<http://itpro.nikkeibp.co.jp/article/NEWS/20060529/239209/>

(4)Social Phishing, Indiana University (Dec 12, 2005)

<http://www.indiana.edu/~phishing/social-network-experiment/phishingpreprint.pdf>

(5)ICANN Fast Flux PDP WG

<https://st.icann.org/pdp-wg-ff/index.cgi>

(6)フィッシング対策ガイドライン(フィッシング対策協議会/2008年9月10日)

http://www.antiphishing.jp/antiphishing_guide_press.pdf