ANTIPHISHING JAPAN フィッシング対策協議会 ▶ NEWS LETTER

APWG CeCOS II 特集（1）

APWG（Anti Phishing Working Group）主催「ネット犯罪対策運用サミット（CeCOS II ：The second annual Counter-eCrime Operations Summit)」報告

１．はじめに

世界的なネット犯罪対策コミュニティである米国 Anti Phishing Working Group(APWG)はフィッシング対策協議会の協力により、ネット犯罪対策を討議する国際カンファレンス「CeCOS II 東京：Counter eCrime Operation Summit」を、東京・赤坂のグランドプリンスホテル赤坂にて、2008年5月 26 日・27 日に開催した。 今回はこの会議の第１日目の内容について紹介する。当日の概観を示し、さらに特に選択した２つの発表についてより詳しく報告する。

APWG 会議としてアジア圏で初めて開催された CeCOSII 東京は、海外参加者とともに各報道関係者も数多く訪れた

写真　会場風景

２．初日概要

初日の冒頭におけるカンファレンスイントロダクションとして APWG 事務局長 Peter Cassidy 氏の挨拶から始まり、フィッシング対策協議会を代表し内田勝也氏（技術･制度検討 WG 主査、情報セキュリティ大学院大学教授）により日本におけるフィッシングや関連事件について概観された。日本ではフィッシング被害は米国に比べ非常に少ないが、携帯電話などでの被害を考えると、海外とは異なる形でのフィッシング詐欺が発生している状況が紹介された。

２．１「国際的なネット犯罪の展望」のセッション

(1)世界の法執行機関の展望：世界的規模のフィッシング問題（Ralf Zimmermann 氏、インターポール／フランス）

2005 年に開始した「Operation GoldPhish」では、首謀者の情報を共有するなど捜査官のプラットフォームを提供しており、インターポールと米国の協力で、エジプトの犯罪者 47

人を逮捕することが出来たという成功事例を説明した。今後の取り組みとして、ベストプラクティスの展開と、官民協力の推進を強調した。[詳細後述]

⑵ 国際的なフィッシングの調査結果（Greg Aeron 氏、Afilias／アメリカ、Rod Rasmuseen 氏、Internet Identity／アメリカ）

APWG の 2007 年のデータ等から整理された 52,000 個のユニークなドメイン名を分析した。全 273 の TLD（トップレベルドメイン）のうち、182 のドメインがフィッシングに使用されている。

近時はサブドメインにフィッシングの標的とした組織のブランドを組み込むケースが増えている。この理由として、サブドメインにはWHOIS[1]情報がない、無料である、リダイレクト[2]などに使いやすいなどがあり、サーバを停止させるのが困難であることが挙げられた。

⑶韓国レポート ＆ ケーススタディ(Terrence Park 氏、KrCERT／大韓民国)

韓国では、(サイト停止等対応する)フィッシングインシデントが 100 件／月となっている。本年、情報通信省が再編され、法律でもフィッシングの IP アドレスを停止することが出来るようになっている。人口の 1/3 が PKI を使用しているといわれ、その個人の証明書を含んで盗む手口事例などが紹介された。

⑷あなたのデスクトップや家の前、ペットをターゲットとする悪意のあるコード(Geok Meng Ong 氏、本城信輔氏、McAfee／アジアパシフィック)

各国あるいは各地域で利用されている検索エンジンやフリーソフトなどが攻撃のターゲットになっていると述べ、それらを悪用した標的型攻撃の事例を示した。

２．２「オンラインカスタマーの保護」セッション

⑴オンライン決済のセキュリティ事情　-livedoor、OnlineGame などの実例（片山昌徳氏、ビットキャッシュ(株)／日本)

決済関係の事業者としては、顧客が身に覚えのない取引に気づき事業者に相談があった時点でフィッシングなどのネット犯罪が発生していることを認識するため、フィッシング発生の最初の段階から 1～3 ヶ月ほど経過してしまっている。また、それまでに、いくつかの事業者（ショッピングサイト、カード会社、決済代行会社）が関連し、それぞれが被害者となってしまう。一方、各事業者はそれぞれ自身の範疇では問題なく処理をしていているということもあり、当事者が曖昧になりがちで事件を発生させないための対策活動へのモチベーションに課題がある。不正利用の情報収集は犯罪に巻き込まれたプレーヤー同士がいかに協力できるかにかかっている。

---

[1] IP アドレスやドメイン名の登録者などに関する情報を、インターネットユーザが誰でも参照できるサービス

[2] Web 上で、ある URL から他の URL に転送させること

⑵オンラインゲームというヴァーチャル世界が持つネット犯罪を含む現状と課題(植田修平氏、日本オンラインゲーム協会（JOGA)、 増村洋二氏、NHN Japan(株）／日本)

オンラインゲームの業界では、ゲーム内のお金やアイテムを現実世界の現金で取引する仕組み（Real Money Trade）に関連して不正行為が行われることが問題になっている。JOGA では不正行為を防ぐ対策を検討しており、ユーザ協力、ルール策定、技術的対策及び組織的対策の各面での諸施策を紹介し、併せて今後の必要な対策と対応を整理した。

⑶フィッシングに陥らないための教育(Steve Sheng 氏、カーネギーメロン大学／アメリカ)

社会心理学手法によりフィッシング対策のための教育のあるべきアプローチを示し、その具体事例として、擬似的啓発用フィッシングメールを送る方法と、ゲームから学ぶ方法を紹介した。[詳細後述]

２．３「ネット犯罪の技術 - ネット犯罪のレスポンス」セッション

⑴ウェブアプリケーションセキュリティ最新動向(金床氏、JUMPERZ.NET／日本)

IE8 や Firefox3、Flash Player の最新バージョンやマイクロソフトの Silverlight など、ウェブに関連する新たな技術が登場している。これらの技術のセキュリティについて、クロスドメインアクセスや DNS Rebinding、UPnP の悪用といった攻撃手法との関連について解説された。

⑵フィッシングエクストリーム(Michael Molsner 氏、(株)Kaspersky Labs Japan／日本)

フィッシングに用いられるサーバ側の状況を多くの事例を通して報告された。極めてまれなフィッシングサイト（実在の銀行や警察関連のサイト）の実例が報告された。また、犯罪者が改ざんしたサーバに残されていた、メールアドレスやウェブサイト、その他具体的なデータの事例も紹介された。

⑶共通データフォーマットを通じたネット犯罪に関する国際協力レスポンスのコーディネーション（Pat Cain 氏、APWG／アメリカ）

APWG では現在のところ情報共有が定着しており、継続的な業務効率と実用性の向上に努めている。APWG がリードし、新しい APWG レポジトリで使われている情報共有フォーマットの標準化のための取り組みについて報告された。APWG と研究パートナーで現在進行中の新しい共有手法に関する解説とそれに対する期待や効果についても報告された。

２．４「Birds of a Feather」セッション

次の２つのテーマについて、２つのグループに別れ自由討議が行われた。

・金融分野に関する事象の情報共有について

・教育：世界が次のステップを踏むためにどうするべきかについて

３．世界の法執行機関の展望：世界的規模のフィッシング問題

Ralf Zimmermann, インターポール

インターポールは、フランスのリヨンに拠点を置く世界 186 カ国の警察で構成された組織である。

法執行機関と民間のコミュニケーションが不足しており、こういった発表の場も一つの機会であると述べた。世界人口の 1/5 がネットに繋がっており、世界の電力消費の１％がコンピュータに費やされ、IPv6 やグリッドコンピューティングでインターネットの速度が 30 倍にもなろうとしている中で、銀行強盗といった物理的な犯罪の減少に比べ、オンライン犯罪が増加している。オンライン犯罪は、マネーロンダリングや児童ポルノ、ドラッグなどの犯罪とも結びついており、深刻な問題である。

近時においては、被害者が気づかないような、マン・イン・ザ・ミドル（中間者）攻撃が行われたり、銀行のホームページの HTML やロゴが同梱されたフィッシングキットが出回ったりするなど攻撃手法が高度化している。また、Fast-Flux という DNS プロキシを盾に自分の存在を隠す手法も使われている。特に、RockPhish キットと呼ばれるものは、ルーマニアの犯罪組織が裏にいるのではないか、というところまで突き止めている。こうした犯罪の多くは、児童ポルノ、重要インフラなどの分野における法の未整備を悪用している。また、盗難したカード情報、ID 等をオンライン上で売買している。

スマートフォンがネットに繋がってきており、世界の携帯電話の普及が 26 億台に達している状況下（注：国際電気通信連合のまとめによると、契約台数は 2007 年末で 33 億台を突破）において、Bluetooth 通信で感染を広めるマルウェアも登場していることを懸念し、問題解決においては、テレコムや金融などの各業界の協力が不可欠であると考えている。

インターポールが注力している犯罪領域として、1. 公安・テロ、2. ドラッグ・犯罪組織、3. 人身売買・児童性的虐待、4. 逃亡犯の捜査、5. 金融・ハイテク犯罪の５つが挙げられる。

2005 年に、各国の警察、法律、産業、科学などの業界でフィッシングに関する情報共有を行なうプロジェクト「Operation GoldPhish」を開始し、国境を越えて犯罪首謀者の情報を共有するなど捜査官のプラットフォームを提供している。こうした活動の成果として、インターポールと米国、エジプト当局の協力により、エジプトの犯罪者 47 人を逮捕することが出来き、これは一つの成功事例である。

現状、フィッシングサイトの 40%はアジア地域でホスティングされている。今後は、アフリカにシフトしていくのではないかと推測している。

最後に、今後の取り組みとして、蓄積したベストプラクティスの展開と、官民協力の推進が必要と考える。

４．フィッシングに陥らないための教育　～Teaching Johnny Not to Fall for Phish～

Steve Sheng, カーネギーメロン大学

コンピュータやインターネットに詳しくない一般ユーザに対するフィッシング詐欺に巻き込まれないようにするための教育方法は難しい。CeCOS II ではこの教育分野に関し、カーネギーメロン大学にて Steve Sheng 氏らにより研究された社会心理学に基づく教育方法が紹介された。Steve Sheng 氏はこの中で紹介されるオンラインゲーム「Anti-Phishing Phil」をデザインしている。

セキュリティ分野教育がうまくいかない理由として次が挙げられることがある。

・ユーザは必ずしもインターネットや PC に十分な知識やスキルを持ってるわけではない

・コンピュータセキュリティは一般ユーザが理解するには複雑すぎる

・ユーザ教育は不適切な方法で実施されがち

ここで述べるアプローチでは、ユーザは訓練され、またユーザ教育はフィッシング技術に対処させることができるものである、という立場をとっている。

フィッシング等セキュリティ上の問題はコンピュータウィルス検出のように可能な限り自動化すべきであるが、フィッシングにはどうしても完全には自動検知できない場合があり、ユーザ教育（啓発）が必要である。このユーザ教育に関して次の課題がある。

（1） ユーザはシステムに対し知識をほとんど持ってない

2 年前に行った調査では、フィッシングの意味を知っているユーザは半数しかなく、55%は怪しい見え方をする URL にまったく気が付いたことがなかった。このことからもユーザ教育がいかに難しいか分かると思う。ただし、2 年前に比べ最近の認知度傾向は良化していると思われる。

（2） ある種の詐欺への知識は別のタイプの詐欺には応用されない

例えば一部の人々は金融サイトでのフィッシングについては知識があったとする。その知識があるにも関わらず Amazon をかたるフィッシングにはまったく警戒心なく情報を出してしまう、ということがある。我々の調査でもう一つ分かったことは、ユーザの 80%がフィッシングリンクのついた e-mail をクリックすることによってなんらかの情報を出した経験があるということである。また、ユーザは各々独自の対策を考えており、それぞれのやり方で自分の身を守ろうとしている。画面の見え方や、その見え方によって何を感じるかで考えている。例えばこの Web サイトは自分の使っている銀行のものと似ているな、また銀行から e-mail が来ることはよくある、だからこの e-mail は本物に違いないと判断してしまう、ということがある。

このような課題から、どのようにすべきかを次に示す。

1）トレーニング用メッセージを初心者向けにデザインすべきである。
　例えば教材で示すメッセージはできるだけ簡素化する。

2）一般的な知識を教えるべきである（特定の事例を教えるのではなく）。

3）ユーザの考え方を適切な方法に導くようにしなければならない。

一方、現在一般に行われている教育実施アプローチとして次のものがある。

・集合教育（費用がかかる。非常に多数の人数への拡大が困難。）

・Web 上に教材を掲載する

・セキュリティ注意喚起アプローチ（企業等 Web での注意喚起などはあまり読まれていない。）

・フィッシング IQ テスト（ユーザをより疑い深くする。見えているサイトがすべてフィッシングサイトでないかと疑うようになる。）

なぜ、上記のようなアプローチが無視されるのかということに関し、次のような要因が考えられる。

・読むものが長すぎる

・自分たちには関係ないものだと思っている

・既に騙されない方法を知っていると思い込んでいる

（実は自信を持っている人ほど、引っかかりやすいということが分かっている）

・テストだけでは学習とはならない

そこで、教材のデザインとしては次のように作成すべきである。

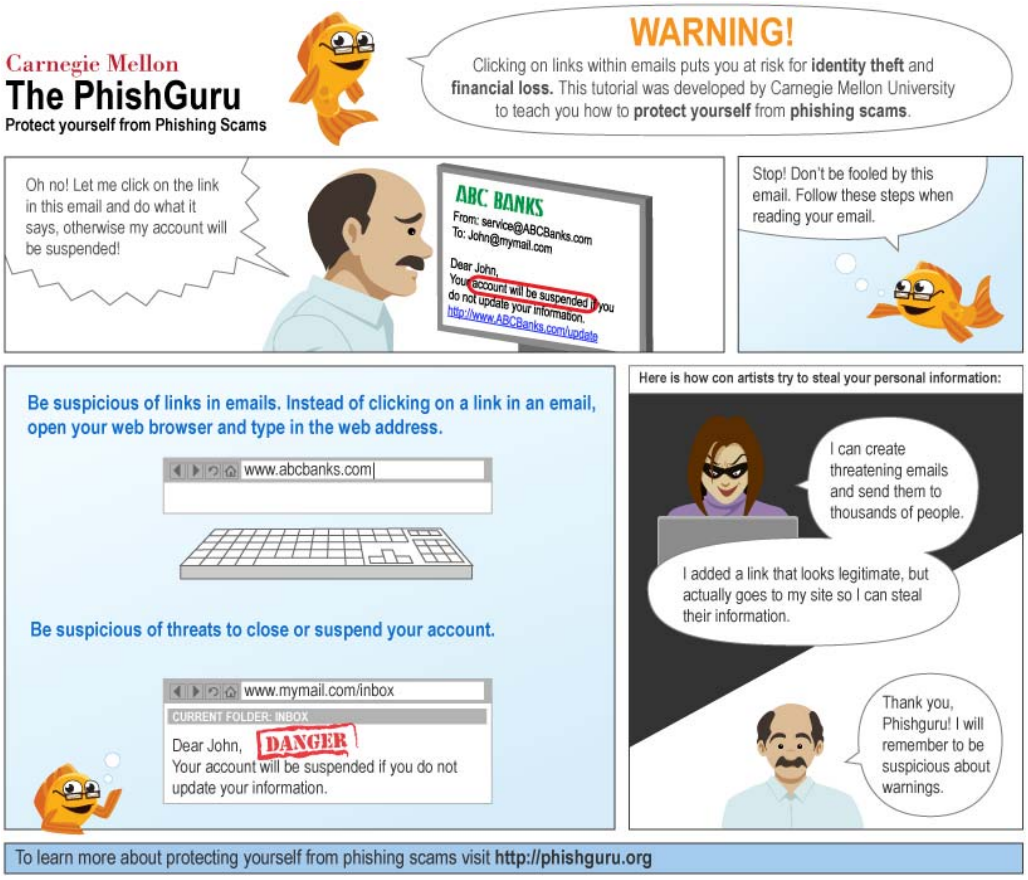
・できるだけ短く、集約されたものにすること

・楽しく、関与度を高めた形で強く動機付けをすること

また教育の形態としては、ユーザが受けやすい環境に合わせて提供することが重要である。例えば研修のためにわざわざ別の場所に行かなくてすむようにすることが望ましい。

以上のような観点から考え作成した教材を２つ紹介する。

１つ目は、教育用の擬似的フィッシング攻撃の e-mail をユーザに送る。その e-mail にだまされた場合のその擬似フィッシング Web サイトに、啓発用メッセージを表示する。そのメッセージを図 A に示す。



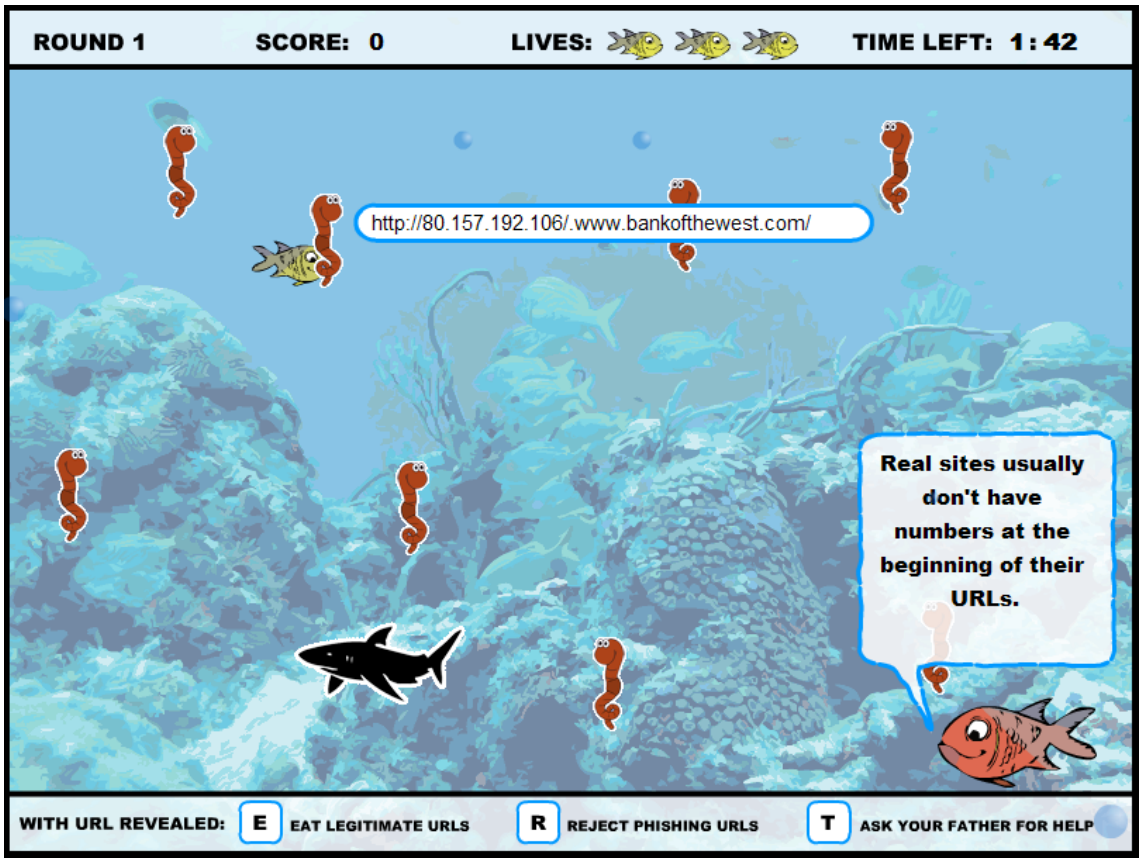
擬似フィッシング e-mail の URL をクリックするとまずこの画面「フィッシング詐欺から身を守れ」が出る。

出所：Teaching Johnny not to fall for Phish, APWG CeCOS II, Steve Sheng, 2008

図 A　教育用擬似フィッシングメールから誘導されるサイトの啓発メッセージ例

この手法が効果的な理由は、擬似フィッシングに引っかかったことが、フィッシングに注意する動機付けになるからである。また、この教材は学習科学に立脚して作成されたものである。

もう一つは、Anti-Phishing Phill と呼ばれるユーザ参加型の娯楽性のあるゲームの形態をとったものである。それを図 B に示す。



URL のアドレスに数字が用いられているケースを信用しないよう教示している

出所：Teaching Johnny not to fall for Phish, APWG CeCOS II, Steve Sheng, 2008

図 B　ゲーム型の教材例（Anti-Phishing Phill）

このゲームの教材により初心者ユーザの 47%、平均的知識を持つユーザで 25%の試験成績の改善が見られた。また被験者は 1 週間後でも内容を覚えており、このゲームを体験したのは今日までの 3 ヶ月 52,000 人以上である。

5．（参考）CeCOSII のホームページ

http://www.antiphishing.org/events/2008_operationsSummit_jp.html