第36号　発行日 2018年8月1日

vol.36

c l i c k !

情報処理センター通信

CONTENTS

◆ 特集

● フィッシングメールの見分け方

フィッシングメールというのは、偽のWebサイト（フィッシングサイト）に誘導して、ユーザ名やパスワードなどを盗み取ろうとする詐欺メールです。販売サイトでパスワードを盗まれれば勝手に発注されてしまうかもしれないし、メールサーバでパスワードを盗まれればメールが盗み見られるだけでなく本人になりすましてメールを送られてしまうかもしれません。フィッシングメールに限らずネットワーク犯罪は巧妙化の一途をたどっており、フィッシングメールを100%見分ける方法は残念ながらありませんが、あまり手間をかけず、かなりの程度見分けることはできます。この記事では、その方法をご紹介します。

チェックポイントは次の3つです。1つでも明確に「おかしい」と判断した場合、フィッシングメール（あるいはその他の迷惑メール）と見なして無視して下さい。

1) 件名やメールの内容・宛先が怪しくないか

日本語がおかしい、会員でないのにメールが来ている、個人情報なのに同報メール（To:に複数のアドレスがある）になっている等、怪しさはいろいろです。アナログですが大事な点です。フィッシングメールの場合、相手を不安にさせて情報を入力させようとするのが常套手段です。

2) 送信元（From:）アドレスのドメイン名が正しいか

メールアドレスのうち、末尾で組織を表わすのがドメイン名です（学芸大なら"u-gakugei.ac.jp"）。例えば、アマゾンからのメールならドメイン名は"amazon.com"のはずで、違う場合はおかしいと判断されます。

3) メール本文中のリンク先URLのドメイン名が正しいか

メール本文中のリンクをクリックさせ、偽のWebサイトに誘導するのがフィッシングメールの狙いです。偽のWebサイトは本物そっくりに作ることができるため、見た目で真偽を判断するのは困難です。リンク先のURLは、リンクの上にポインタを持っていくと（クリックはしないように！）、ステータスバーに表示されます。例えば、アマゾンからのメールならURLのドメイン名は"amazon.com"のはずで、違う場合はおかしいと判断されます。ただし、正当なメールでも短縮URL（例えば"bit.ly"）など別のドメインを使っている場合もあり、判断を面倒にしています。

では、実例を見てみましょう。例に挙げるのは、情報処理センター宛てに届いた、アップル社を騙ったフィッシングメールです。アップル社のドメイン名は"apple.com"です。

1) 件名やメールの内容・宛先が怪しくないか

件名は"アラート:あなたのアカウントは閉鎖されます。"で、本文中に"リカバリアカウント"というリンクが1つあり、フィッシングメールらしさが感じられるものの、微妙です。ただ、よく見ると次の問題があります。

・宛先が複数並び、同報メールになっている。

・本文に"アマゾンアカウントで何ができるか的を絞ってください"とあり、アップルかアマゾンか訳が分からない。

ここでNGと判定して構いません。今回は、例として先に進んでみましょう。

2) 送信元(From:)アドレスのドメイン名が正しいか

送信元アドレスは"noreply@email.apple.com"で、問題なさそうです。ここは「自称XXX」のようなもので、表面的に偽装されています。"apple"のl(小文字のエル)をI(大文字のアイ)に変えた、"apIe"のような騙しもあります。

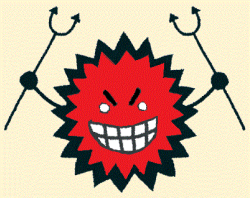
3) メール本文中のリンク先URLのドメイン名が正しいか

リンク"リカバリアカウントのURLは"http://pdate-security-supprt-appeld.com/"で、ドメイン名が全く違います。短縮URLでもなく、明確にNGです。

例では比較的分かりやすいものを取り上げましたが、より巧妙で紛らわしいものもあります。フィッシングメールに騙されないよう、基本として知っておきましょう。

● ウイルスの症状

ウィルスに感染すると、以下のように**ウイルス対策ソフトが反応し通信を切断します。**



ただ最近のウイルスは感染しても**症状が出にくいものが増えています。**

ウイルス対策ソフトが検知できなかった場合、症状でわかる例として以下のようのものがあります。
● 特定のサイトにアクセスできない。
（特にセキュリティ関係、ウイルス対策メーカーサイト、Microsoftなど）
● お気に入りやツールバーが勝手に追加されている。
● インターネットが遅い、接続・切断をくり返す。
（＃これは微妙です。Trafficが増えただけの遅延かもしれません。）
● 通信や起動中でないのに、ネットワーク機器やハードディスクのアクセスランプが点滅する。

ランサムウェアのようにはっきり乗っ取られたことがわかるケースもあります。
ランサムウェアとは感染したPCをロックしたり、ファイルを暗号化したりすることによって使用不能にしたのち、元に戻すことと引き換えに「身代金」を要求する不正プログラムです。昨年流行したWannaCryがその一種です。

ウイルスに対応するには、ウイルス対策ソフトを最新にすることが重要ですが、完全に防ぐには下記のような方法しかないのかもしれません。
・映画(Enemy of the State)にもあったように、ネットワークを遮断する。
・どうしても使う必要があるなら、感染しても困らない空のPCでネット接続する。

◆ 情報処理センターレポート

● 第15回国立大学法人情報系センター協議会参加報告

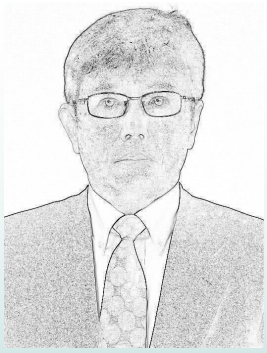
2018年6月29日（金）、鹿屋体育大学において第15回国立大学法人情報系センター協議会総会が開催され、本学からは宮寺センター長、森本教授、および情報基盤課職員2名が参加しました。

今回の統一テーマは『情報セキュリティ対策の運用と課題』でした。CSIRTの構築と運用、NIIのセキュリティ運用連携サービス（NII-SOCS）の開始などを経て、参加大学の情報セキュリティ対策はどのような状況にあるのか、情報や課題を共有するとともに、今後の在り方について検討しました。

午前中の分科会では、話題提供した4大学が各々の情報セキュリティ対策の現状と課題について報告があり、その後のパネルディスカッションでも参加大学を交えて忌憚のない意見交換が行われました。
午後の総会では、文部科学省研究振興局参事官（情報担当）付学術基盤整備室長（丸山修一氏）より「学術情報基盤整備の動向について」という演題で、国立情報学研究所所長（喜連川優氏）、国立情報学研究所学術基盤推進部長（漆谷重雄氏）他2名より「国立情報学研究所の事業について」という演題で、講演がありました。
その後議事に移り、議題、報告事項の後、各地区幹事校が取りまとめた地区報告がありました。今年度は本学が幹事校だったため、宮寺センター長が登壇し報告しました。
夕方からは情報交換会が催され、鹿屋市全面協力のもと盛大な会となりました。

【参考】鹿屋体育大学スポーツ情報センター　情報系センター協議会
http://itec.nifs-k.ac.jp/nipc/

●情報処理センター教職員紹介



情報処理センターの荒木です。4月から技術補佐員として勤務しています。

30年以上も昔、大学は文学部卒なのですが、在学中にかじったコンピュータプログラミングが面白くて、システム開発の会社に入りました。某総合商社の子会社です。当時（今も？）、「プログラマー35歳定年説」がささやかれていましたが、システムを作って納めるという仕事をしているとプログラミング以外のノウハウも身に付くもので、プログラマーを40歳くらいで卒業した後も失職せずに済んでいます。その後何回か転職し、前職は国会図書館にいました。国会図書館の書庫の広さには定評がありますが、学芸大の敷地の広さはそれ以上です。

締め切りに追われるプログラマーは卒業しましたが、仕事で使うツールは今でもプログラミングしています。国会図書館時代は、画像処理のツールをPython（パイソン）という言語で作っていました。国会図書館と画像はあまり結びつかないと思いますが、紙の劣化に備えてデジタル化を進めており、大量のスキャン画像を保有しています。ちょうど、深層学習（Deep Learning）が注目され始めた頃で、Python言語と画像処理は深層学習の主流になりました。深層学習のライブラリはオープンソースで多数公開されていて、中身の数学的な詳細が分からなくても使えます。その恩恵で、仕事で取り組んだ画像補正（視認性の低いスキャン画像をくっきりさせる）も、そこそこの成果を得ることができました。

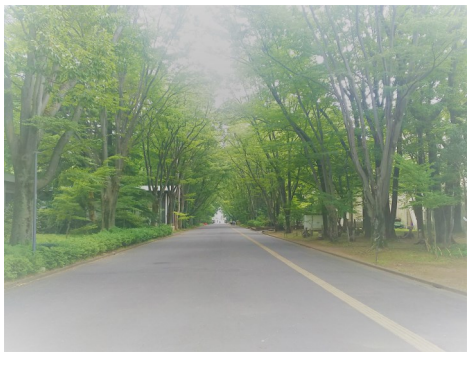
どうぞ、よろしくお願いします。

編集後記

今年は春も夏も例年よりも早く訪れたように感じます。最近では「猛暑」ではなく「酷暑」と言われるほどの気温が続いています。先の見えない暑さで、既に秋が待ち遠しいですが…確か今年の初めは史上最大の寒波と言っていたはずで、ちょうどいい暑さ寒さにならないでしょうかね。

さて、今回は特集として「フィッシングメールの見分け方」について掲載しました。前回も話題にしましたが、メールによる詐欺やウイルス感染被害は未だになくなりません。オレオレ詐欺の被害者アンケートでは、実に半数以上が「自分は大丈夫だと思っていた」と答えています。自分は大丈夫、ではないのです。自分の判断能力を過信せず、そこそこ疑う心が必要です。とはいえ、そんな世の中になったのも悲しいことです。

この暑さで、ついにサーバ室のエアコンが壊れました。室外機がヤラれました。学内ではあちらこちらで同様の被害があるとのこと。これを機会に本学でもテレワークやりませんか。（前）



国立大学法人　東京学芸大学

情報処理センター

☐TEL　042-329-7710　　☐FAX　042-329-7711

☐URL　http://www.u-gakugei.ac.jp/~ipcenter/

☐E-mail　ipcenter@u-gakugei.ac.jp