迷惑メールが名簿を盗む？！

ー情報セキュリティとトラブル対策のために

講師：寺田 慶治（NPO 情報セキュリティフォーラム、（有）コンピュメンター）

１ 狙われる情報

福祉関連会社「コロニーワイズ」（東京都港区）による詐欺事件で、聴覚障害者から金をだまし取ったとして詐欺罪に問われた元同社社員、町田栄子（57）と長男、訓清（29）両被告の判決公判が３日、東京地裁で開かれた。井口修裁判長は栄子被告に懲役６年（求刑懲役８年)、訓清被告に懲役５年（同懲役６年）の実刑判決を言い渡した。

判決によると、栄子被告らは平成 16 年２月～17 年９月、同社社長の小林洋子被告（56）＝公判中＝と共謀し、会社の資金繰りが破綻（はたん）していることを隠して、聴覚障害者に手話でうその投資話を持ちかけ、13 人から計 1 億 1600 万円をだまし取った。

（2007 年 12 月３日産経ニュース）

情報漏洩などによる名簿はこうした犯罪に使われる可能性があります。彼らはその名簿を高値で取引しています。

こうした情報漏洩は、インターネットを通じてメールや Web をきっかけとして起こります。自分たちが扱っている情報がどれだけ大事なもので、責任を持って扱わなくていけないのか（個人情報保護法など関連法を参考に）考えてみましょう。

１-１ 情報漏洩はなぜ起こるのか？

・第三者が悪意を持って公開する

他人の個人情報などを掲示板に掲載するケースが頻発しています。ちょっとした他人とのトラブルがこうしたケースに発展する場合があるようです。

・第三者が保有するデータが不注意により流出する

名簿などの入力をボランティアの方に頼んだりしていませんか？ボランティアの方に情報の取り扱いに関する話をしていますか？データのコピーは簡単にできます。ちょっと目を離したすきに簡単に盗まれることがあります。

・自身が運営する Web から不注意により流出する

Web サーバーの構成（中のファイルなど）をちゃんと把握していますか？公開しないデータを置いてありませんか？リンクが張られていなくてもロボット検索エンジンでファイルの存在がわかってしまいます。

・不正アクセスにより意図的に持ち出される

自前あるいはレンタルサーバーのセキュリティ対策はしっかりしていますか？レンタルサーバーの料金の違いはそうした部分に反映されます。利用料金が単に安いからと言ってセキュリティ対策がきちんとされているかどうかチェックしましょう。

インターネットに接続すると言うことは外部へアクセスできるだけでなく、外部か

ら自分のところへもアクセスが可能になると言うことです。きちんとしたセキュリティ対策がなされていないと簡単に外部からあなたのパソコンへアクセスされてしまいます。

・個人情報収集目的のサイトに騙される

懸賞やモニター募集に安易に応募していませんか？どこが何の目的でやっているのかを理解しないと、情報収集だけのためにやっているケースもたくさんあります。懸賞やモニター募集に応募したとたんに迷惑メールが増えたと言うケースがたくさんあります。

こうして盗まれた情報は、冒頭にあげた犯罪などの対象として使われたりするケースがあります。

１-２ 個人情報保護法

個人情報の有用性に配慮しながら、個人の権利利益を保護することを目的として2005 年 4 月より施行されました。個人情報の取扱いに当たっては、個人情報の「保護」と「活用」のバランスを図ることが重要と考えられます。
個人情報保護法の義務の対象である「個人情報取扱事業者」は、個人情報データベース等を構成する個人情報によって特定される個人の数の合計が、過去６か月以内のいずれの日においても 5,000 を超える者とされますが、それ以外の場合でも、義務は発生しませんが、「個人情報は、個人の人格尊重の理念の下に慎重に取り扱われるべきものであることにかんがみ、その適正な取扱いが図られなければならない」（法第３条）という個人情報保護法の基本理念を尊重して、個人情報の保護に自主的に取り組むことが望ましいところです。

ここで言う個人に関する情報とは、氏名、性別、生年月日、職業、家族関係などの事実に係る情報のみではなく、個人に関する判断・評価に関する情報も含め、個人と関連づけられるすべての情報を意味します。死者に関する情報については保護の対象とはなりませんが、同時に生存する遺族などに関する情報である場合（例：死者の家族関係に関する情報は、死者に関する情報であると同時に、生存する遺族に関する情報である場合がある）には、その遺族などに関する「個人情報」となります。
映像や音声であっても、それによって特定の個人が識別できる場合には、「個人情報」に該当します。

１-３ 被害者が加害者に

情報漏洩の怖いところは、一度漏洩した情報はまず回収困難であると言うことです。万が一被害が発生した場合、その管理責任を問われるケースもあります。その場合、情報漏洩の被害者であったものが一瞬にして加害者になってしまうのです。法律的責任だけでなく損害賠償を求められるケースもこれまで多く発生しています。

２ 変なところ（Web）へ行かないから大丈夫

「迷惑メールも来るけどそんなところへ行かないから大丈夫」と思っていませんか？最近の手口は巧妙になってきてメールを見ただけでウィルスやボットなどに感染する可能性もあります。
ウィルスやボットがどんなものでどんなことをするのでしょうか？

２-１ ウィルス、ボットとは？

・他のプログラムに寄生しシステム破壊活動などをするウィルス
・自己増殖をし自己プログラムをメールなどを勝手に送信して繁殖するワーム
・単独で破壊活動をするトロイの木馬
・ユーザーの知らない間にパソコンに入り込みクレジットカードの情報やパスワードなどの個人情報を収集し、特定のサーバーに送信するスパイウェア
・インターネットを通じて悪意を持った攻撃者が、ユーザーのパソコンを外部から遠隔操作するボット（フィッシング、スパム、DDoS 攻撃、個人情報漏洩などに利用される）

２-２ ウィルスなどの感染原因

・メールに添付される
　最も多い感染原因。Word や Excel のファイルに仕込まれている場合がある。
・HTML メールに仕込まれる
　Web のページのような形のメール。閲覧した時点で感染する場合がある。
　また、リンク先が偽装されていたりしてフィッシングサイトなどに誘導されるケースもある。
・P2P ファイル交換ソフト
　最も危険なもの。官庁や企業などの情報漏洩のほとんどはこれが原因。そもそもそこで扱われているものは、音楽、映画、ゲーム、パソコンソフトなど違法なものがほとんど。絶対に使ってはいけない。
・外部からのメディア
　USB メモリや CD/DVD、フロッピーディスクを外部から持ち込まれるケースもあります。

３ ウィルス対策ソフトを入れているから大丈夫

本当に大丈夫ですか？ウィルス対策ソフトの更新はもちろん OS のアップデートもしていますか？今自分たちが使っている OS のバージョンは知っていますか？
いつも使うメールソフトの名前やバージョンは知っていますか？
何もしないでそのまま使っていると格好の標的になります。
最低限、必要な対策を考えてみましょう。

３-１ コンピュータを最新状態にする

Windows をはじめとする各種 OS やソフトウェアには「セキュリティホール（ぜい弱性）」と呼ばれるシステム上の欠陥や仕様上の問題点が発見されることがあり、このような場合には製品の開発元から修正プログラムが公開されます。ソフトウェア等のセキュリティホール（ぜい弱性）によってウィルスに感染したり、コンピュータが悪用されたりする場合が多くあることから、セキュリティホール（ぜい弱性）を修正せずにそのまま利用することは非常に危険です。
特に Windows は利用者も多いせいもあり、一番狙われています。もちろん Mac でも安全とは言えません。**「Microsoft Update （Windows Update）」を最低でも毎月必ず実施**するようにしましょう。

３-２ ウィルス対策ソフトを必ず導入する

ウィルス対策ソフトを利用してコンピュータウィルスに感染する危険性を軽減することが重要です。また、ウィルス対策ソフトを利用していても、ウィルス定義ファイルの更新期限が切れていたり、定期的な更新を行っていない場合には新種ウィルスに対応することができません。**ウィルス対策ソフトは常に最新の状態に保ち、定期的にコンピュータをスキャン**することによって、ウィルスに感染していない事を常に確認しましょう。

３-３ パーソナルファイアウォールを利用する

最近の OS やウィルス対策ソフトウェアには、パーソナルファイアウォール機能を備えたものが多くなってきています。パーソナルファイアウォール機能を適切に利用することによって、利用しているコンピュータに対する意図しない通信を検出・遮断することができます。ボットをはじめとする多くのウィルスは、このようなユーザーが意図しない通信を利用して感染および活動をするため、パーソナルファイアウォールを導入することによって、意図しない通信からコンピュータを守りましょう。

3-4 インターネット接続にブロードバンドルータを利用する

ルータがなくパソコンが直接インターネットに接続する構成では、パソコンにセキュリティホール（ぜい弱性）がある場合、外部からの感染攻撃により数分で感染してしまう恐れがあります。
ブロードバンドルータを介して接続することにより、ルータの NAT 機能が外部からの感染攻撃を防いでくれるため、感染しにくい安全な環境を構築することができます。

3-5 HTML 形式の電子メールはプレビューしない

HTML メールとは、ホームページのように文字の色や大きさを自由に変えたり、絵や写真を貼りつけたり、他のホームページに飛べるようにできるなど、大変便利なものです。ホームページだけではなく、メールソフトにも HTML を使える機能が付いていて、まるでホームページを見ているかのようなメールを送ることもできます。
しかし、この機能を悪用して、HTML メールを開いただけ、あるいはプレビューしただけで感染するウィルスも蔓延しています。ですから、HTML メールを見ない・使わないように設定しましょう。

3-6 添付ファイル付きの電子メールには十分気をつける

見知らぬメールの添付ファイルを安易に開いてはいけません。また、画像や文書を装った実行形式のファイルも存在するため、ファイルの種別だけで安全性を判断することはできません。差出人を知人や職場のアドレスに偽ってウィルスに感染させようとするメールもあるため、知人からのメールであっても不審な点がある場合は差出人に確認するなど十分に注意してください。

3-7 ID とパスワードによる認証と強固なパスワードを使用する

コンピュータを利用する場合は、必ず ID とパスワードによる認証を行うようにしましょう。ID とパスワードによる認証を行うことによって、第三者が無断でコンピュータを使用するのが難しくなります。また、パスワードは名前や誕生日など他人に推測されやすいものはさけ、記号などを含んだできるだけ長い文字列としましょう。

４ 万が一、事件事故に遭遇したらどうしたら良いか考えていますか？

さまざまな対策をしても 100%安全と言うことはありません。どうしたら最善最良の対策が取れるか具体的に考えてみましょう。

４-１ 早急に対応する

ウィルスなどに感染していることが判明したら、すぐインターネットや LAN の接続から外しましょう。二次感染をできるだけ防ぐことが重要です。すでに述べたように被害者が加害者に変身してしまう可能性が高いからです。

どう対応していいか分からない場合は、パソコンに詳しい人や関係機関に相談しましょう。

情報漏洩の場合
　最寄りの警察署、消費生活センター等
コンピュータウィルス、不正アクセスの場合
　独立行政法人情報処理推進機構（http://www.ipa.go.jp/）

４-２ 対応策を作成しておく

さまざまなケースを想定して、常日頃から管理、対策、連絡先などをまとめておきましょう。一度作成すれば良いというわけではなく随時見直しが必要です。

自分たちの組織でどのような情報を扱っているのか？
管理はどのようにしているのか？
　例えば名簿（紙）、コンピュータ本体内のデータ、CD/DVD、フロッピー等何で保存しているのか？ どこにしまってあって鍵などかけてあるのか？誰が取り扱えるのか？責任者は誰か？等々
これらを列記して、盗難・紛失、漏洩など想定されるケースを考えてみましょう。
そしてそれらを防ぐにはどのような方法を取ればいいのか考えてみましょう。

寺田 慶治（てらだ けいじ）
（有）コンピュメンター 社長、NPO 法人りんぐりんく理事、
JD 情報通信委員、パソコンボランティア「ドリームナビゲーター横浜」副代表
東京都立工科短期大学電気電子工学科卒業 卒論「マイコンの教育的利用」（現首都大学東京）
半導体メーカー代理店技術営業、厨房機器メーカー技術担当などを経て独立。パソコン・ネットワーク関連の仕事以外にパソコンボランティアをパソコン通信の時代から始める。さまざまな地域活動や青少年育成活動にも参加。
日本福祉大学通信教育学部福祉経営学部医療・福祉マネジメント学科在学中。
[資格]
福祉情報技術コーディネーター1 級
情報セキュリティ検定 1 級、個人情報保護士、システムアドミニストレーター
[所属団体]
NPO 法人情報セキュリティフォーラム、U-Kanagawa 推進協議会、Internet Society