△▼△▼△▼△▼△▼△▼△▼△▼△▼△

個人情報保護法・施行後の課題と対応
～企業を守るセキュリティから顧客を守るセキュリティへ（フィッシング詐欺を題材に）～

日本ユニシス株式会社　小芝卓宏氏

個人情報保護「法」への対応とその後

私は入社以来システムエンジニアをしているが、2004 年から個人情報保護を中心にセキュリティ対策サービスを担当している。

個人情報保護法の趣旨は、個人情報の有用性に配慮しつつ個人の権利を保護すること。個人情報を正しく使ってビジネスをすることが目的であって、企業を縛ることが本質的な目的ではない。これは非常に重要なことだが、割と勘違いをしている方が多いように思う。セキュリティに関することは、個人情報保護法には「個人データの漏えい滅失または棄損の防止、その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない」（第 20 条）ということしか書かれていない。経済産業省のガイドラインには、もう少し細かく組織的、人的、物理的安全管理措置について示されているが、それでもわかりにくいので、具体的にどうすればいいのか、私たちは職業的にやってきた。

例えば企業は、先ずは従業員の教育が一番重要であるとか、入退出管理をしたいと考える。それを物理的な技術で全てカバーしようとすると莫大な金額がかかってしまうので、一番重要なところを押さえてやっていくという形になる。私共は、セキュリティ診断をまずやった上で、こんなシステムを入れましょうという提案をしていたが、今年の4月以降、そのような仕事は減るだろうと思っていた。しかし、予想に反して全く減らなかった。社内の規則作りは今年の４月に駆け込みでやったが、実際のITセキュリティ対策は、あまり進んでいないのかもしれない。

私は偶々東京駅からバスに乗ることが多いのだが、個人情報保護法完全施行前の 2004 年 10 月に、バスの中でアナライザソフトを使い、八重洲口近辺で無線 LAN のアクセスポイントを探してみた。すると、暗号化などのセキュリティ対策をしていない無線 LAN が本当にたくさんあった。それから約一年後、法完全施行後にこのセミナーの講師をすることになり、同じ場所でもう一度調べてみたが、実態はあまり変わっていないことがわかる。多少の入れ替わりはあるが、同じアドレスがあったりする。

今、個人情報保護の法律に準拠することと、現実のセキュリティを守ることの両方が求められている。規則やマネジメントシステムは、情報漏えいそのものの防止を保証してくれるわけではない。法対応のためにやらなければならないことと、現実に起こるリスクを把握した上でリスクをのむということと、最低限打てる手は打っておくというこの3点が重要である。

以上のような、「企業を外敵から守る」、あるいは「企業内部からの情報漏えいを防ぐ」、という観点の情報セキュリティに関しては、対策の実態はともかく、その必要性に関しては、個人情報保護法の完全施行を契機に広く世間の認知を得てきたように見える。しかし今後の情報セキュリティには、それに加えて「顧客を守る」という観点が重要になってくるものと考える。そのひとつの題材として、最近流行している「フィッシング詐欺」を取り上げたい。

フィッシング詐欺の現状と傾向

フィッシング詐欺は、ネット版の振り込め詐欺と言える。今までのネット犯罪は、会社の Web サイトに攻撃をしかけ、データの盗用や改ざんをするということが主体だったので、それに対抗するために ISMS の認証取得などで防衛していた。しかしフィッシング詐欺は全く違う。犯人が会社の Web サイトを偽装し、顧客が詐欺サイトと気付かず諸手続をすると、個人情報が抜き取られる。被害があれば、顧客は会社に文句を言う。文句を言われた会社は何のことかわからない。そこで初めてフィッシング詐欺だということがわかる。

事件になって報道されると、会社の情報システム対策が問われるが、その時点では既に犯人は詐欺サイトを閉鎖していることが多く、対策が難しい。ここが企業の一般的な情報セキュリティ対策とフィッシング詐欺対策の違う点だ。

アメリカでは 2003 年頃からフィッシング詐欺による被害が増えており、億円単位の被害があると言われている。日本でも 2004 年から話題になってきている。

日本のフィッシング詐欺事例

ビザ・インターナショナルというカードの決済会社がフィッシング詐欺に遭った事例を紹介しよう。最初に、セキュリティ強化やサービスの継続と偽った、ロゴなどを盗用したメールが来て、詐欺サイトの URL にメール受信者を誘導する。そしてカード番号や有効期限、パスワードを入力するようにし向ける。詐欺サイトは、メニューバーから Visa の実際のサイトにリンクするなど、本物のサイトのように偽装されている。本物のビザ・インターナショナル・アジアのサイトはシンガポールにあるが、この詐欺サイトはルーマニアにあった。

フィッシング詐欺の実行犯は、かなり綿密な計画を立て、準備している。どの会社をターゲットにし、どんな情報を狙うかなど、かなり練っている。フィッシング詐欺

をする人をフィッシャーと言うが、フィッシャーは PDCA サイクルを確実に回す。職責にも社会規範にもしばられない。対策製品や情報を堂々と入手できるので、それに対していくらでも先手を打つことができる。普通の社会人だとそうはいかない。自己の職責に基づいて、社会規範に則って仕事をする。また、プランとドゥはともかく、チェックとアクションが難しいということが往々にしてある。

フィッシング詐欺の対象や手法は刻々と変わる。一度狙われたところは対策をし、防御を強めるので、フィッシャーにとっては「効率」が悪くなる。今までは大手の銀行やカード会社など、有名企業がターゲットにされていたが、米国の例では、最近は地方の信用組合など、必ずしも知名度の高くない Web サイトもターゲットになってきている。

フィッシング詐欺へ対抗するには？

世間で言われているフィッシング詐欺への対策法は、実際にできるのか疑問が多い。例えば「不審なメールが来ても、リンクはクリックしないように」と言われても、不審でないところがフィッシング詐欺の一番重要なところなので、セキュリティ担当者はともかく、一般の人が見抜くのは難しい。

多くのフィッシング詐欺は、メールがきっかけになることが多いので、メールの出自を明らかにするということが行われつつある。このサーバはきちんとメールを発信するサーバだということを公表し、正式に登録されたところから来たメールならば安心だという考え方。しかし、堂々と名乗ってくるフィッシング詐欺メールには無効。他に、Web の出自を明らかにする方法がある。サーバ証明書、SSL など、鍵のマークが目印だ。これは必要だが、紛らわしいドメイン名には対処できないし、技術的には偽装することが可能。また、個人認証を高度化する方式がある。例えばネット銀行では、2 桁の数字を 2 回入れるという方法を採っている。この他にも様々あるが、これで完全という対策はない。しかし無駄なわけではなく、一つ一つには意味があるので、やらないよりはやった方がいい。

フィッシング詐欺対策ソフトーフィッシュウォールー

フィッシング詐欺の対策法のひとつの紹介をする。「フィッシュウォール」というソフトを使用すると、ツールバーにその Web サイトが存在している場所の国名と国旗、実際にアクセスしている Web サイトのドメイン名が表示される。このツールは、詐欺サイトかどうかを自動的に判断することはできないが、アドレスバーの偽装など、普通のサイトはしないようなことを検知した場合は赤信号が出る。また、フィッシュウォールに対応した正規のサイトなら青い信号が点灯する。これを使うと、詐欺サイトに誘導されたときに気がつく可能性が高い。このソフトは、セキュアブレインという会社がクライアントに無償で配っている他、メーカーPC へのプリインストールを進めている。

フィッシュウォールは、サーバとクライアント（ユーザー）と公開鍵サーバの 3 つから成っている。サーバに対して、ユーザーが自分に固有の暗号化された識別情報をあらかじめ納めておき、サイトにアクセスした時、それを見せてもらうことで、確かにいつも自分が見ている正しいサイトだということが確認できるという仕組み。偽物のサイトは、画面はそっくりでも自分の認証情報がないので、青信号がつかない。

認証にも片方向の認証と双方向の認証があり、フィッシュウォールのような双方向の認証が最後に残るのではないか。

様々なフィッシング対策

他に最近話題なのは、インターネットエクスプローラーの次のバージョンで搭載されるマイクロソフトフィッシングフィルターというソフト。これは、ブラックリストとホワイトリストによる制御。まず、安全であることが確認されているサイトのリストを作成し、ユーザーのパソコンに保存して定期的にアップデートする。サイトを訪問すると、そのアドレスがリストにあるかどうか絶えずチェックされる。このリストにない場合にはフィルターがサイトを解析し、フィシングサイトに共通する特徴がないかどうかを調べ、疑わしい場合には、フィッシングサイトである可能性が高いとの警告を表示する。

アンチスパイウェア、アンチスパムもフィッシング対策の一つとして使われているが、これもブラックリストに含まれている場合は警告を発す。しかし、ブラックリストを使う方法は精度に問題がある。というのは、偽サイトは平均寿命が約 5 日。計画的なフィッシャーは、最大限に収穫するまでサイトを開設しているわけではなく、一定の成果を上げればサイトを閉鎖してしまう。ブラックリストに載っているサイトは、本物の会社の Web サイトがクラックされて、ブラックリストの中に入ってしまっているということが多い。

フィッシング対策ソフトで大事なことは、「使い勝手が良いこと」と、「汎用的であること」と、「単純であること」。セキュリティ製品は、ものによってはいちいち起動、停止、再起動などが必要なこともある。認証の度に普通のパスワードではない特別なコードを必要とするものもあるが、ユーザーにとっては使いにくい。使いにくいソフトウェアは、結局は使われなくなってしまう。また、最近は多くの人がアンチウイルスソフトを入れているので、

それで対処できることは、運営会社が対策を取らなくても済むこともある。

おわりに

一番重要なのは、基本的な情報セキュリティ対策、個人情報保護である。フィッシュウォールといえども、正規のWebサイトの中に偽のコンテンツがあるという状態には対応できない。基本ができていないと、どんなセキュリティツールを使っても意味がない。これは個人ユーザーの場合も同じ。偽のフィッシュウォールを先にインストールされてしまったらどうしようもない。

個人のレベルではアンチウイルス、アンチスパイウェアソフトをきちんと使う必要があり、企業では自社のサイトや自分の運営するWebサイトが改ざんされないように運営していくことが大切。個人情報保護法にきちんと準拠して、趣旨に乗っ取って対策を行っていれば、フィッシング詐欺などのインターネット犯罪に遭う確率を減らすことができるだろう。