2008年上半期の個人情報漏えい

止まらない情報漏えい と やめられない Winny

株式会社ディアイティ
セキュリティ被害調査WGメンバー　山田　英史

本誌の読者はご存知と思われるが、JNSAセキュリティ被害調査WGでは年間の個人情報漏えいを集計分析した結果を報告書として毎年公開している。2002年度に個人情報漏えいの集計を開始してから、インシデント件数は個人情報保護法が完全施行された2005年をピークに2006年と2007年と若干の減少傾向にある。当WGの集計は、報道機関などにより公表された情報に基づくため、世の中の関心が薄れることで集計件数が減少するであろうことは予想していた。しかし、現実には思っていたほど大幅な減少は無く、2006年以降も一定の報道件数が保たれていることは想定外であった。個人情報漏えいも、他の不祥事と同じく組織にとって一般的なリスクとして認識されたのであろうということを、2007年度の報告書では述べている。

2008年はインシデント件数が増加？

さて、2008年も残りわずかになった。年が明けると、当WGでは恒例となった前年の個人情報漏えいの集計と分析を始めるのだが、対象の件数が多いことから昨年からは半年毎に集計するようにしている。したがって、実はすでに2008年の1月から6月の上半期の集計結果が手元にある。

まだインシデントを時系列に並べただけで内容を精査していないため、個人情報以外の情報漏えいが含まれていたり、同じ事案をダブルカウントしているなどの誤差があることを前置きした上で、2008年上半期の集計結果を触りだけ紹介したい。

まずインシデント件数だが、2007年が通期で864件だったのに対し、おどろくべきことに2008年は上半期だけで700件を超えている。前述したように精査していないので最終的には件数が減ることになると思われるが、このままのペースで行くと通期では2007年のインシデント件数を超えるのは確実だろう。現時点で数字だけが一人歩きすると困るため具体的な数字は出せないが、2008年は漏えい人数（被害者）1名～数名の小規模なインシデントが占める割合が高いようだ。漏えい元の業種を見ると「公務（他に分類されないもの）」の比率が最も高く、この業種では漏えい人数が少数の場合でも公表する傾向が強いため、それが全体のインシデント件数を引き上げる要因になっていると思われる。

次に漏えい原因はどうだろうか。2007年は上位5位までの合計が全体の80%を占めていたが、2008年上半期は上位4位が全体の80%以上を占めている。また、2008年上半期は「誤操作」が大きな割合を占めているのだが、これはある特定の機関が大量に誤配送を発生させたことに影響された結果である。「管理ミス」は相変わらず上位に位置するが、これは例年通り金融機関が年度末の情報資産棚卸しの際に、保管しているはずの伝票等がなくなっていることに気がつくというケースだ。

表1：2007年と2008年の漏えい原因上位5位の比較（件数割合）

順位	2007年（通期）	2008年（上半期）
1位	紛失･置忘れ	誤操作
2位	管理ミス	管理ミス
3位	誤操作	盗難
4位	盗難	紛失･置忘れ
5位	ワーム･ウイルス	不正な情報持ち出し

繰り返しになるが現時点での集計は上半期までのものであり精査もしていないため、通期で集計・分析した結果は上記の結果と大きく離れている可能性もあるので、当WGの2008年度の報告書が公開されたら是非ともご確認いただきたい。

Winnyは相変わらず

ところで、2008年上半期の集計で気になる点がひとつある。それは、Winny等ファイル交換ソフトでの漏えいが40件強と、全体の6%ほどを占めることだ。なお、その内Shareによるものが4件とLimeWireによるものが1件ある。

どうも数字だけ見ると少ないように感じるが、これだけ新聞沙汰になっているにもかかわらずいまだ利用している人がいるということは理解に苦しむ。これらのソフトを使ったことがない人にとっては不思議でならないだろう。

では、なぜ利用がやめられないのか、簡単にいうとそれは趣味の世界だからだ。体に悪いことは分かっていてもタバコや深酒がやめられないのと同じで、頭で分かっていても好きだからどうしようもないのだ。会社が社員に対し自宅でのWinnyの使用を禁止しても、実際どれだけの効果があるか疑問である。

やはり、大半の利用者は「自分は大丈夫」と思って(信じて)使い続けているはずだ。社員に対してWinny等による情報漏えいの危険性を説くときは、組織の問題として捉えるのではなく、漏えいさせた本人の個人の問題として認識させないと危機感は生まれないのではないだろうか。

というわけで、ファイル交換ソフトの危険性について個人の問題として感じてもらうための助けになることを期待して、漏えい元の当事者がどのような顛末をむかえるのか、実際の現場の例を紹介してみたいと思う。

Winnyが危険と言われる訳

いろいろな媒体でWinnyの仕組みは紹介されているので、ここではポイントだけ整理してみたい。Winnyはサーバを介さずPC間でファイル交換する機能を提供するソフトである。Winnyでは送信元PCと受信元PCは直接データを転送するのではなく、他のWinnyユーザのPCを幾つか経由してファイル交換する(図1)。その時、ファイル交換を希望したPCだけでなく中継したPCにも当該ファイルがキャッシュされ、以降公開される。複数のPCを中継することで、ファイルの提供者の匿名性を確保すると伴に、キャッシュにより情報を広く拡散させることで検索・ダウンロードの効率を上げる効果がある。

ここで問題になるのは、中継したPC上において、持ち主の意思に関係なく様々なファイルを公開して

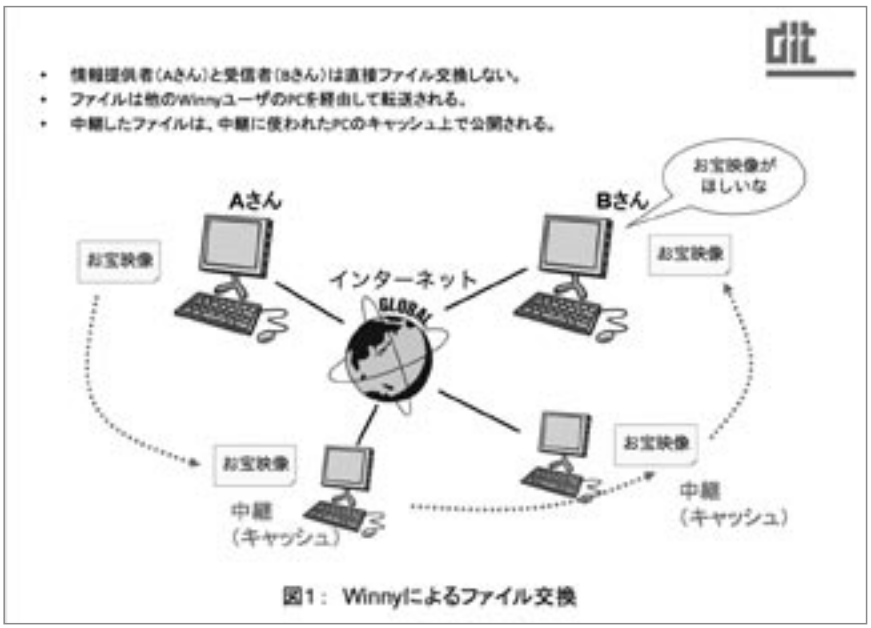

図1: Winnyによるファイル交換

しまうことだ。キャッシュで公開しているファイルには違法に収集した著作物も含まれる。したがって、Winnyを使うということは、暴露ウイルス感染による情報漏えいと、著作権侵害という2つのリスクを負うこと意味する。ただし、WinnyやShareユーザの大半は違法なファイルを自覚的に交換しているはずなので、ここでは情報漏えいの危険性にフォーカスする。

Winnyが危険と言われる訳

WinnyとShareで情報漏えいが多いのは、これらソフトの脆弱性を悪用する暴露ウイルスが数多く出回っているからだが、ではなぜその2つのソフトにウイルスが多いのか。両ソフトの技術的特性に理由がある。WinnyとShareは共に、どのファイルを公開するか等の設定情報をテキストファイルで保持するようになっている。設定をテキストで持っているがためにウイルスが利用し易く、そのために両ソフトを狙った暴露ウイルスが多く作られているのだ。特にWinnyは脆弱性が改善されることが期待できないため、より危険だといえるだろう。

さて、暴露ウイルスに感染したら、どのような情報が漏れるのだろうか。図2は暴露ウイルス体験ツールで擬似的に漏えいさせた情報の例(一部)である。文書ファイルだけでなく画像・映像・メール・IEお気に入り等あらゆるものが漏えいする。それらは、ZIP圧縮ファイルとして一括して漏えいするため(ウイルスの種類によってZIP以外もある)、ほとんどの場合、ファイル名やそこに含まれる住所録やメールや写真画像などから漏えい元の個人が特定できる。

情報漏えいする人のプロファイル

Winny等で被害の大きな情報漏えいを起こすのはどのような人物なのだろう。幾つかの事例から以下のような人物像が浮かび上がる。

・男性
・30代半ば～50代
・既婚者
・几帳面でまじめ
・コンピュータにいくらか精通している

意外に30代半ば～50代の中堅社員や課長クラスの人が多い。その年代の人たちは、4～5年前まで会社の資料を持ち帰って家で仕事をするのが普通

図2: Winnyにより漏えいする情報(一部)

だった。そのため、今でも家に会社の資料が保管されている可能性が高い。当時から使っている自宅のPCにWinnyをインストールしたところ、暴露ウイルスに感染し、消し忘れたあるいは存在を忘れていた会社の資料が流出するというパターンが多いようだ。現実に最近流出したファイルでも作成は4～5年前という情報が良く見つかる。

また、ある程度コンピュータに詳しく、自分は危険性を認識した上で上手く使っているという自信をもっている人も多い。実際に、ある会社の情報システム管理責任者が漏えいを起こしたケースもあった。

多くのWinnyの利用者は、好きな分野のファイルは徹底的にコレクションし、収集したファイルを分類整理するような几帳面さが見られる。仕事にも普段まじめに取り組んでいる人が多い。

ほとんどの人は、故意ではなく意図せず漏えいしていまっているので、ある意味被害者でもある。

情報漏えいの顛末

一度漏えいした情報は形を変えながらコピーされ続ける。Winnyで流出した情報は、すぐさまShareにコピーされShare経由で拡散し、2ちゃんねる等の掲示板でも公表される。多くの場合、漏えい元組織（実際にはその組織に所属する個人が漏えい元だが）が自ら検知することは無く、匿名の警告FAXが送られてきたり、掲示板等を見て発見した親会社や取引先から通知されて初めて漏えいに気付くことになる。

この時点で、漏えい情報が保全されていれば、漏えい元組織は自らの分析で漏えい元となった人物を特定できていることが多い。漏えい情報の中身が自己の組織に関わるものだけであれば、内々に対処して終わるのだが、漏えい情報に親会社や取引先の内部情報が含まれている場合は、それら関係者から正式な報告を求められることになる。報告は客観的な内容を求められるので、インシデントレスポンスやフォレンジックを行なうベンダーに調査を依頼することが多い。調査依頼を受けたベンダーは、WinnyやShareのネットワークを監視し、本当に漏えいしているのかを確認し、漏えいしている場合はファイルを保全し、何人くらいがダウンロードして、何人くらいがキャッシュで公開しているのかといった漏えい規模を分析する。

さらに、実際に漏えいしている場合は、流出者を特定する証拠を用意した上で、次のような手続きで流出元のPCを差し押さえる。（あくまでも一例）

(1) 就業時間中に直属の上司含め、多数の関係者で流出者を取り囲む。
(2) 流出者には、自宅で使用しているPCの提出をお願いする。この時、自宅に電話はさせず会社のPCも使わせないようにする。
(3) 車を使い、流出者の自宅へ移動してPCの回収に向かう。
(4) できれば上司だけでも一緒に部屋まで入れてもらい、PCや外付けディスクを確認しながら回収する。部屋に入れてもらえない場合は、3分以内というように時間を制限する。
猶予を与えるとディスクを壊したり、別のPCやディスクを代わりに提出する可能性が高くなる。
(5) 流出者本人もいっしょに、回収したPCや外付けディスクとともに引き揚げる。
(6) Explorer等を操作しただけでも証拠（記録）が変化するため、引き揚げたPCは立ち上げず、専用の装置で内蔵ディスクの複製を取り、解析は複製に対して行なう。複製をとった後にPCは所有者へ返す。

残念ながら、この時、ほとんどの情報流出者は全てを話さず幾つかの事実を隠す。全てが露呈すると仕事も家庭も失うことが想像できるからだ。別のPCやディスクを提出して時間を稼ぎ、その間に本当のディスクをフォーマットしたり物理的な破壊を試みたりする。しかし、引き揚げたPCを解析すると隠している物が分かるので、いずれ本物を提出することになる。初期の調査や保全で、会社は相当な出費をしているのだが、破壊されたディスクの復旧などを行なうとさらに数百万円の出費になる。

情報漏えいにより関係者が大きな経済的損失や精神的苦痛を被り係争まで発展する場合を除き、会社

は流出者を必要以上に罰することは無い。しかし、証拠隠滅を図り余計な出費を会社にさせた場合はいくらか厳しい処分が下されることになるだろう。

また、Winny等ファイル交換ソフトを使っている人は、ほとんどの場合アダルト情報を収集しており、解析の過程でその人の趣味嗜好だけではなく性癖まで知ってしまうことになる。知られた方も知ってしまった方も、相手に対する接し方はそれまでの通りとはいかなくなる。ほとんどの場合、故意ではない情報漏えいでクビにするほどの厳罰を会社が下すことはないが、流出者本人が会社にいづらくなることが多いようだ。

さらに、家庭でも「お父さんがWinnyを使っていた」という事実により家族の接し方が変わってしまい、発覚以後互いに気まずくなることもあると聞く。

状況によりインパクトは異なるとは思うが、情報を流出させた時点で会社での地位も家庭での立場も失い未来はなくなるということをWinnyユーザは覚悟しておくべきだろう。

今一度チェックを

ファイル交換ソフトによる情報漏えいの対策はいくつも考えられるが、まずは自宅のPCに会社の情報を保管しないことだろう。先にも述べたが、故意にデータを保管していることは少なく、保管したこと自体忘れていたり、削除したつもりが予想しなかったフォルダに残っていたりすることで被害に結びつく。

以前削除したという方も、今一度自宅のPCの中をチェックしていただきたい。

情報漏えいに責任を感じて自殺した人もいる。自分だけは大丈夫という根拠の無い自信は持たず、すべてを失い未来がなくなる前に、Winnyを使うということの問題をまじめに考えていただきたい。

チェックリスト(データだけでなく文書も含む)

□	自宅のPCのあらゆるフォルダをチェックして会社の業務情報が無いことを確認した
□	メール(添付ファイルを含む)にも業務情報はなかった
□	外付けディスクやUSBメモリにも業務情報はなかった
□	業務情報が家の中で放置されていなかった
□	引出や本棚に昔の紙資料がなかった
□	上記は記憶ではなく、実際に確認した
□	インターネットの脅威と被害について家族とも話し合った
□	情報の取り扱いについて、家族にも注意するように伝えた