2006年度情報漏えいによる被害想定と考察
～Winnyインシデント、本当のところ～

株式会社ラック 研究開発本部 主管研究員
JNSA セキュリティ被害調査 WG メンバー　丸山　司郎

1. はじめに

JNSAの政策部会に所属するセキュリティ被害調査ワーキンググループでは、2002 年度より毎年、国内における情報セキュリティインシデント(事件・事故)の調査を行い、集計結果を分析し公表してきた。本年も個人情報漏えい事件・事故の調査分析を行い、つい先日、2007年7月23日に「2006年度 情報セキュリティインシデントに関する調査報告書」としてJNSAのWebサイトに公開したところである。

近年の調査報告書においては、各年度における特徴的なセキュリティインシデントをよりくわしく解説する「付録」を添付しており、本稿は、2006年度の報告書の付録として、最も特徴的なセキュリティインシデントである、Winnyネットワークにおける情報漏えいインシデントを統計的な視点から分析したものである。

1.1　2006年 最悪の情報漏えいインシデント

2006年における個人情報漏えいインシデントの中で最も特徴的なものが、WinnyなどのP2Pソフトを利用することで暴露ウイルスに感染し、プライベート情報や仕事上の情報をインターネット上にばら撒いてしまった事件である。

この問題は、すでに一般紙を含む、数多くのメディアで取り上げられており、その法的な是非論や、ソフトウエアおよび利用者の善悪の検討はここでは省くが、本稿ではWinnyやShareに関して報道されたインシデントを集計することで情報セキュリティインシデントとしての特徴を明らかにし、今後の情報セキュリティ対策の一助となることを目指す。

1.2　調査対象、調査方法

本稿は「2006年度 情報セキュリティインシデントに関する調査報告書」を作成する過程で収集した、2006年1月1日から2006年12月31日までに新聞やインターネットニュースに報道された個人情報漏えいインシデント情報の中から、Winny、Shareなどファイル交換ソフトを利用し、ウイルスに感染し情報漏えいを起こしたインシデントを抜き出し、漏えい人数、漏えい原因、漏えい経路、漏えいした組織の業種などにより特徴を分析している。

ファイル交換ソフト上でウイルスに感染し、漏えいしている情報は、月に1000件以上といわれている。ここではその中でも、漏えいした情報の中に個人情報が含まれており、かつ、メディアに取り上げられたものを主に対象としているため、ファイル交換ソフトによるインシデント全体を対象とした分析とはなっていない点をご了承いただきたい。

2. Winnyを媒介とするウィルス

2.1　ウイルスの悪質化

Winnyネットワークで感染するウイルス(Antinny)の原型は、2003年8月に発生しているが、実際に情報の暴露機能をもったタイプは、2004年3月頃から発生している。その後、様々な亜種が作られ、より感染しやすく悪質な暴露型ウイルスへと成長しており、さらには、Antinny以外の種類(山田ウイルス、ヌルポース、ドクロウイルスなど)も発生してきている。

表1:暴露型ウイルス成長の流れ

時　期	ウイルス	特　徴
2003/8	初代Antinny	Winnyのキャッシュフォルダ中のファイルのみを消去
2004/3	暴露型ウイルスAntinny.G	感染したPCのデスクトップ画面をjpegにするとともに、デスクトップ上にあるファイルをzipに圧縮し、Winnyネットワークに漏えいさせる。
2004/8	ヌルポース	水曜日または日曜日の午後11:45にPCが起動されているとCドライブ全てを削除
2004/11	仙台ギャラクシーエンジェルズ	IEのお気に入り、Outlook Expressのメールデータを漏えいさせる機能が追加される

2005/3	欄検眼段	デジタルカメラの映像を漏えいさせる機能が追加
2005/3	仁義なき○○○○	Office系のドキュメントや2chへのKakikomi.txt、Winnyの検索履歴と共有ファイル名を漏えいさせる機能が追加
2005/4	山田ウイルス	感染するとhttpサーバーを立ち上げ感染PCのHDD内容やスクリーンショットを外部から見えるようにし、2chに自分のリモートホストアドレスを書き込む
2006/1	ほぼ完成型 Antinny	Windowsの"システムの復元"機能を無効化し、DOC、XLS、EML、PPT、DBX、TXT、PDFといった拡張子のファイルや、Winnyの検索履歴、IEのお気に入りや履歴を ZIP ファイルに固めてWinnyに漏えいさせる
2006/1	ドクロウイルス	Winnyのみでなく、Shareでも感染を広げる

一部報道(*1)によれば､流通している実行形式ファイルの内60%以上にウイルスが含まれていると言われている。

つまり、WinnyやShare ネットワークは、根本的な著作権違反の問題も含め、その存在自体が裏社会を形成しているものと考えられる。

3. 分析

3.1　月別の情報漏えい件数

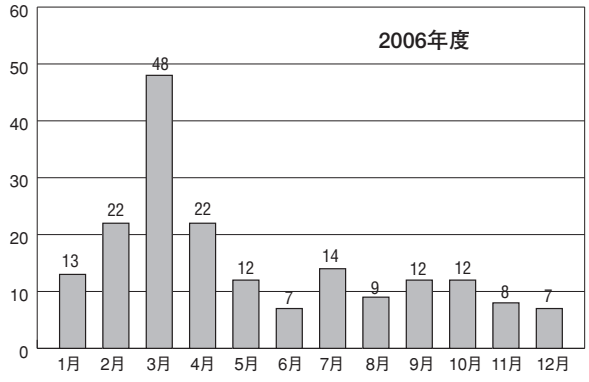

図 1:ファイル交換ソフトによる月別インシデント件数

2006年におけるファイル交換ソフト起因によるインシデントは186件であり、インシデント総件数993件に対し約19%を占める。昨年(2005年)が29件／1099件で約3%だったことを考えると件数、割合とも大幅な増加となっており、その要因としては、以下のものが考えられる。

- 一般紙やテレビでもファイル交換ソフトが報道されることで認知度が上がり、利用者が増加した。
- ファイル交換ソフト上で、蔓延するウイルスが巧妙になりかつ種類が増加した。
- ファイル交換ソフト利用者のウイルスへの感染率が高まり、流通しているファイル中のウイルス含有率が高まった。

次に、月毎の発生件数を見ると、毎月7件以上がコンスタントに報告されているが、3月が48件と突出していることが分かる。この要因としては、以下のものが考えられる。

- 3月にウイルスの新種が登場し、感染する人が増加した。
- 世間での報道や注意喚起を契機に、3月に各組織が内部を調査した結果、過去にウイルスに感染し、情報漏えいしていることが判明したものを含めこの時点で公にされた。

3.2　業種

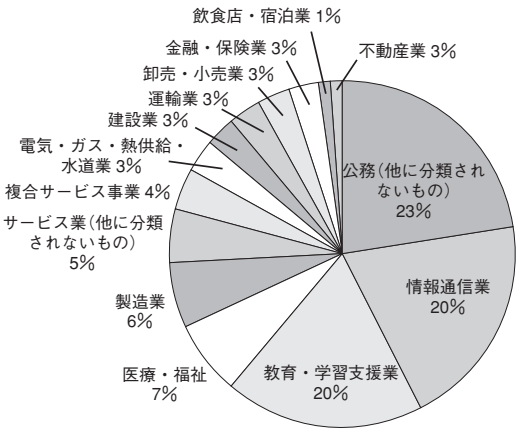

図 2:業種別のファイル交換ソフトによるインシデント件数

(*1)　IT Pro「Winny ネットワークはやっぱり真っ黒，NTT コミュニケーションズの小山氏に聞く」
http://itpro.nikkeibp.co.jp/article/Interview/20070413/268234/

個人情報や機密情報が含まれるデータを自宅に持ち帰り、私有PC上で扱うことが多い業種が、上位を占めているものと思われる。

情報漏えいインシデント全体の業種別の漏えい事故件数と比較すると、金融・保険業の割合が大きく減り(14.0%→2.7%)、教育・学習支援業(11.1%→18.8%)、医療・福祉(4.2%→7.0%)の割合が多くなっている。

一番多い「公務(他に分類されないもの)」(22.6%：42件)の内訳としては、県・市･町による漏えいが16件ともっとも多く、消防署・同組合による漏えいが11件と次いでいる。この理由としては、以下の点が想定される

- 業務上、満足のいく台数やスペックのPCが配備されておらず、私有PCを持ち込んで使用している。
- 残業の規制が強いため、自宅に持ち帰って作業をすることが多い。
- 漏えいした場合に話題になりやすく、公表される可能性が高い。

2位の「情報通信業」(20.4%：38件)が多い理由としては、以下のものが想定される。

- ファイル共有ソフトに関する情報を入手しやすい。知る機会が多い。
- ファイル共有ソフトを使用するための難解なシステム設定作業を行なう能力がある。

3位の「教育・学習支援業」(18.8%：35件)の内訳としては、小学校が11件と最も多く、次いで、高校、塾の5件が続いている。この業種が多い理由は、公務と同様であると想定される。

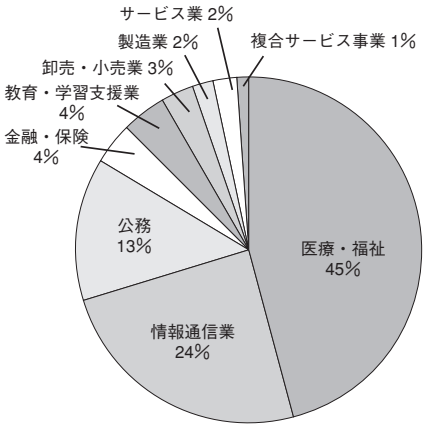

図 3:業種別のファイル交換ソフトによる漏えい人数

業種別の漏えい人数の合計を分析すると、件数では4位の「医療・福祉」が、47.7%（271,258人）と1番多い。これは、「医療・福祉」においてある大規模な漏えいインシデントが起こったことに起因している。

「情報通信業」の漏えい人数が24.4%（148,158人）と2番目に多く、インシデント件数が1番多かった「公務」と順位が逆転している。「情報通信業」は、業種上、取り扱う情報量が多いためと考えられる。

3.3 漏えいの当事者のプロファイル

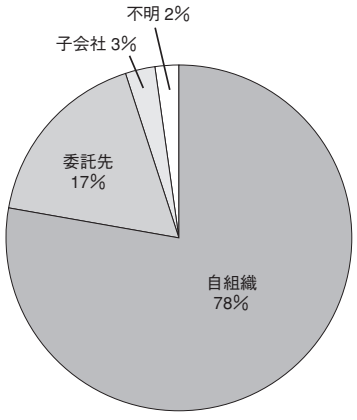

図 4:当事者の所属組織

漏えいインシデントを起こした当事者と、インシ

デントを公表した組織上の所属との関係を表したグラフが図 4である。

公表した組織(会社や団体)に直接所属する者が漏えいの当事者である場合が一番多く、146件：78.5%を占めている。調査前の想定では、委託先や子会社などのセキュリティポリシーが徹底されていない組織が、インシデントを起こしている可能性が高いと考えていたが、外部ではなく内部の人間が問題を起こしているケースが多いことがわかる。

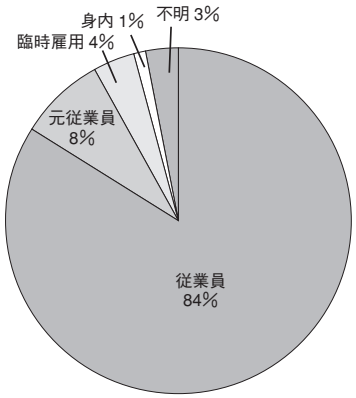

図 5:当事者の雇用形態

次に、漏えいインシデントを起こした当事者と、自分の所属する組織との雇用形態を表したグラフが図 5である。

インシデントを起こした組織(会社や団体)に直接所属する者が漏えいの当事者である場合が一番多く、157件：84.4%を占めている。こちらも調査前の想定では、臨時雇用や、すでに退職した元従業員など、セキュリティポリシーが徹底されていない者がインシデントを起こしている可能性が高いと考えていたが、本来、インシデントの発生が直接所属する組織の業績や、自分の関連する業務内容に影響を与えるため、情報の取り扱いには細心の注意を払うはずの内部の人間が、問題を起こしているケースが多いことがわかる。

但し、技術的にも、規則上でも対策が困難なケースとして、すでに退職した正社員から漏えいしているケースも8%存在しており、過去の契約を含めた対応が必要となっている。

3.4　漏えいした情報のタイプ

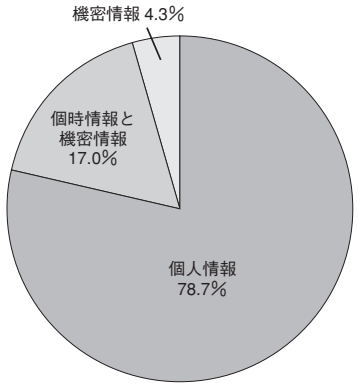

図 6:漏えい情報における個人情報と機密情報

漏えいした情報の種類としては、圧倒的に個人情報が多く、95.7%となる。これは、個人情報が漏えいした場合に、一般に公表されるケースが多くなっており、結果として個人情報漏えいインシデントの発生情報を得やすいためと考えられる。

一方、個人情報が含まれず、機密情報やプライベートな情報のみが漏えいした場合には、企業として公表する義務もなく件数が少なくなっているものと考える。

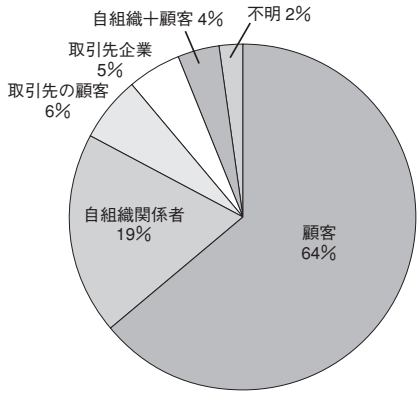

図 7:個人情報の管理責任組織との関係

表 2:個人情報の管理責任組織との関係

組織との関係	説　明	割合	件数
顧客	自社の顧客、または生徒など	64.5%	120件
自組織関係者	自組織の所属員、自社社員、学校教員など	19.4%	36件
取引先の顧客	自社が業務を委託されている、取引先の管理する顧客	5.9%	11件
取引先企業	取引先企業の担当者	4.8%	9件
自組織＋顧客	自組織の所属員と、自組織の顧客	3.8%	7件
不明	—	1.6%	3件

次に、漏えい元組織と漏えい情報の関係を図 7、表 2で表す。

ここからも、自社の顧客など自分に責任のある個人情報を漏えいしている割合が高いことが伺える。

3.5　原因と経路の分析

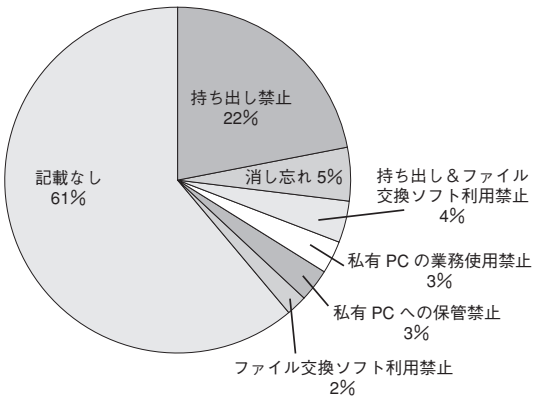

図 8:漏えい原因に占める、違反内容

公表された情報の中になんらかの規則違反があったと記載されているインシデントを抜き出し、分類したグラフが図 8である。

主な規則違反を以下に挙げる。

◉ 業務場所からの持ち出し禁止規則の違反
◉ 情報削除指示の違反、情報の消し忘れ
◉ ファイル交換ソフトの使用禁止規則の違反
◉ 私有PCの業務使用禁止規則の違反
◉ 私有PC上への業務データ保存禁止規則の違反

上記の何らかの規則に対して違反があったと記載されていたインシデントが38.9%（72件）あり、残りの61.1%には明確な規則違反に関する記載がなかった。

これは、Winnyなどのファイル交換ソフトという新たな脅威に対する、組織としての対応が追いついていないことを如実に表しているものと考えられ、想定される原因は以下のようになる。

◉ 私用PCを職場に持ち込んで業務に使用している。（業務用PCが不足している。）
◉ 自宅への業務の持ち帰りが恒常化している。（業務情報の持ち帰り、自宅PC上で業務作業が行われている。）
◉ 業務用PCが私的に利用されている。（私用PCと業務用PCとの境界があいまいである。）
◉ 社内の規定整備が追いついていない。

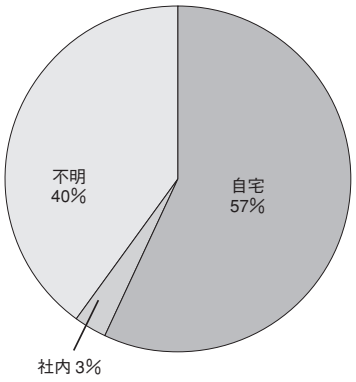

図 9:漏えいが発生した場所

社内でファイル交換ソフトを使い、情報漏えいした件数はほとんどない。自宅での利用つまり、他人の目の触れないプライベートでのインターネット利用が57.0%（106件）と過半数を占めている。

記事や公表された内容から漏えいの発生場所が

読み取れないインシデントは「不明」に分類したが、そのほとんどのインシデントの説明内容には「私用PCで」や「メディアにより持ち出した」などの記載があった。そのため「不明」としたインシデントのほとんどのものは、「社内」ではなく、他人の目の触れない「自宅」に近いプライベートな環境より漏えいしたと考えられる。

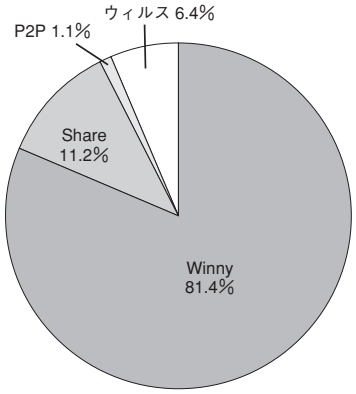

図 10：漏えい経路

情報漏えいが発生した際に利用していたファイル共有ソフトは、圧倒的にWinnyが多い。P2Pと分類したものは、ファイル交換ソフトと記載があるがその種類が不明なものであり、ウイルスと分類したものは、ファイル交換ソフトの利用に関しての記載がないものである。実際はこれらも、Winnyまたは、Shareのいずれかを利用していたものと考えられる。例外としては、1件のみLimeWireの設定ミスがある。

4. まとめ

つい先日、情報漏えいをしたことで自殺者がでたという報道があったが、Winnyネットワークでの情報漏えいインシデントは後を絶たない。一度、インシデントの当事者となった場合には、組織内に留まることも出来ず、さらには、住んでいる所も追われるような失態を、日本中にばら撒くことになる。

しかし、Winnyに代表されるファイル交換ソフトを使う当事者は、そこで流通するファイルに、ある程度の違法性があることを承知の上で行なっている確信犯であり、アンチウイルスソフトを使っているからウイルスに感染しない、実行ファイルをクリックしなければ感染しないなどの迷信めいたものに頼って、自分が当事者になり悲惨な末路を歩むことになることを想像できないでいる。

これまでの分析から、ファイル交換ソフトを使うことによる情報漏えいインシデントの特徴を整理すると次のようになる。

① 今のところ、ファイル交換ソフトを使うこと自体には違法性がないことから、組織としても明確に禁止できないでいる。
② 従来にないタイプの脅威であり、組織としての対応がとれないうちに広範囲に広まってしまった。
③ 日本型ワークスタイルの特徴である、以下のような自発的な業務遂行があだになっている。
・仕事のために私用PCを持ち込んで業務を行なう。
・業務時間中に終わらない仕事を、家に持って帰って行なう。

この分析結果からすると、組織がポリシーを整備し、正しい対応を自組織の構成員に示すことで、数々の悲惨な事故を減らせる可能性が高いことがわかる。企業などの組織は、自社の社員に対して、仕事の仕方、PCの使い方、ファイル交換ソフトの倫理観に関して明確な方針を示す義務があり、早急に実施していただくことをお願いしたい。