「 ウイルスによる機密情報流出対策」

毎日のようにマスコミを騒がせている機密情報や個人情報の流出。そのほとんどがファイル共有ソフト Winny(ウィニー)や Share(シャレ)で動作する暴露ウイルスによるものです。

情報漏えいによって損なわれる信用や長期にわたる対応策、訴訟リスクなど計り知れないダメージを被ることになります。不幸な事態を招くことのないように、まず敵を知り、的確な対策を講じましょう。情報漏洩でまず問題視されるファイル共有ソフトとは何か、暴露ウイルスとは何か、なぜ流出事件が減らないのか、どうすれば防げるか、Winny を例に解説します。

■とまらない情報流出

情報流出が、マスコミにひんぱんに登場するようになったのは 2005 年 3 月ごろからです。顧客情報、社員情報、内部資料、名簿、暗証番号、犯罪捜査資料など重大な影響を及ぼしかねないものが続々と流出して社会問題となっています。マスコミに登場しない個人や中小企業も合わせると、2006 年 3 月でおよそ 10 万件の情報流出があったといわれます。Winny と同様の機能を持つファイル共有ソフト Share でも、流出はおよそ 1000 件に達するといわれています。情報を流出させているのは、Winny や Share などのファイル共有ソフトで感染し、増殖するウイルスで、「暴露ウイルス」とか「さらし系ウイルス」と呼ばれています。感染したパソコンのデスクトップやマイドキュメント、メールファイル、さらに自分自身のコピーも入れて圧縮し、特定のファイル名を付けて共有ソフトのファイル公開機能を使ってネットワークに公開します。そのファイルは、Winny ユーザーの誰もがダウンロードすることができるようになります。当然ウイルスが含まれていますから、ダウンロードした人も感染する可能性が高くなります。

こうしてみると、ファイル共有ソフトではなくてウイルスが悪いのだから、ウイルスを止めれば解決するのではと考えたくなります。実際、このウイルスはほとんどの場合、市販のウイルス対策ソフトで検出し、削除することができます。ところが、流出は止まりません。後述しますが、暴露ウイルスは「ファ

イル共有ソフトの特徴」、「ユーザーの心理」、「Windows の機能」を巧みに利用して感染・増殖するのです。ウイルスによって流出した情報は、誰がダウンロードしたか、中継したかを特定することは難しく、回収・削除は不可能です。さらに始末が悪いことに、流出した情報は Winny ネットワーク内のコンピュータのキャッシュフォルダにコピーされるので、ダウンロードされ続けるかぎり、どこかのコンピュータに残り、いつまでたっても消えないのです。

したがって、流出した情報に長期的な対応が必要になります。「振り込め詐欺」などに悪用される可能性もあります。信用回復に時間を要するだけでなく、訴訟リスクの上昇、セキュリティ強化策など対応には多大なコストがかかります。個人ならば職を失うだけでなく、訴訟になればさらに深刻な事態を招くことになります。

「ファイル共有ソフト」、「暴露ウイルス」、「防止策」の順に説明しながら、そうならないためにどうすればよいか考えましょう。

※流出件数に関する参考(毎日新聞:2006/05/08)

【http://www.mainichi-msn.co.jp/keizai/it/jyouhou/news/20060507ddm001040145000c.html】

■ファイル共有ソフト Winny とは

Winny はインターネットを通じて不特定多数の Winny ユーザーとファイルを共有するための純国産のソフトです。

Winny を起動すると、Winny ネットワークと呼ばれる起動中の Winny で構成されるネットワークに参加することになります。PtoP(Pear to Pear)と呼ばれるネットワーク形態で、1 台 1 台がサーバ・クライアントの両方の機能を持ち、互いに助け合うように動作しますので、1 台あたりの負荷が小さくても、大きなネットワークとして機能します。IP 電話や Skype（スカイプ）も PtoP を採用しています。通信プロトコルは TCP で、データは共通鍵暗号化方式 RC4 で暗号化されています。

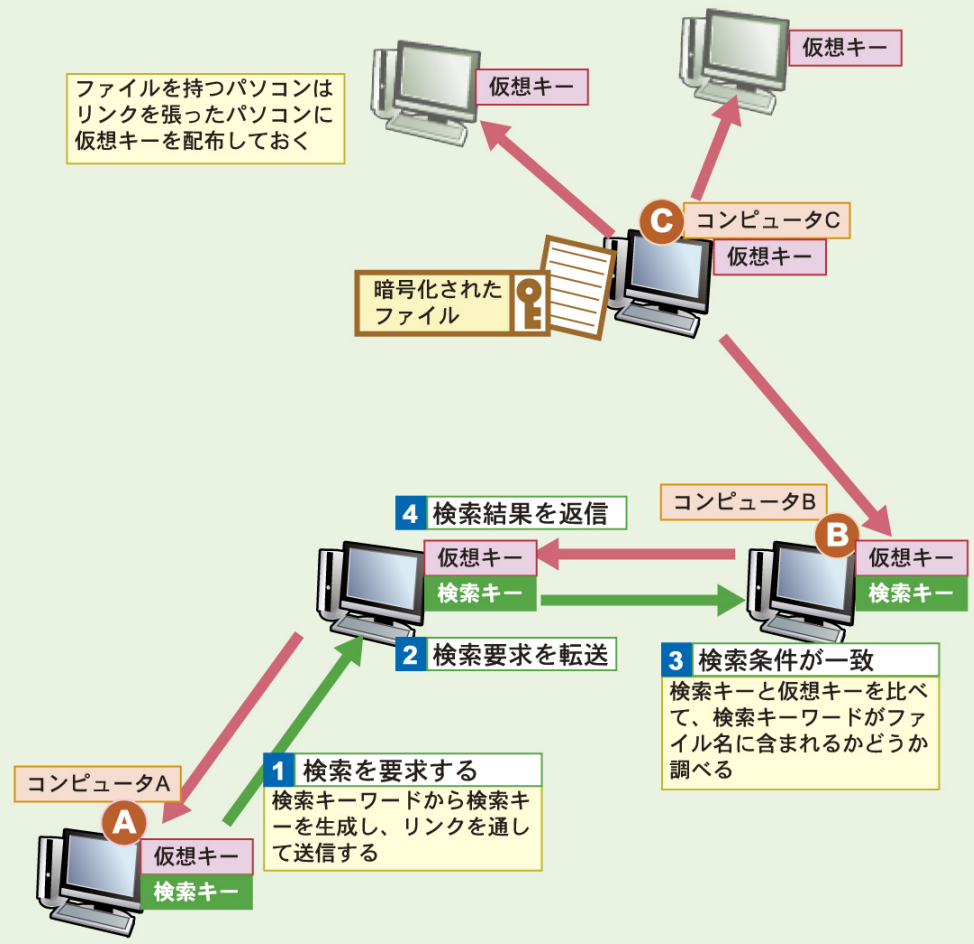
Winny の機能は、ファイルの「検索」「ダウンロード」「アップロード」です。それぞれの機能は次の通りです。

●ファイルの検索

検索を実行すると検索キーというリストが作られます。検索キーは Winny ネットワークに送信されます。応答したコンピュータ B は自分の持っているリストと照合します。このリストを仮想キーといい、公開されているファイル名とそのファイルを持っているコンピュータの IP アドレス、接続形態(ルータ経

由か直接か)などが記載されています。仮想キーの中に該当するファイルがなければ、別のコンピュータに問い合わせます。応答したコンピュータ B の仮想キーにあれば、「こういうファイルがある」とコンピュータ A に通知します。こうしてコンピュータ A には検索結果が表示されます。このとき、コンピュータ B は、自分の仮想キーの中に該当するものがあるというだけでファイルを持っているとは限りません。

図1 検索の概念図

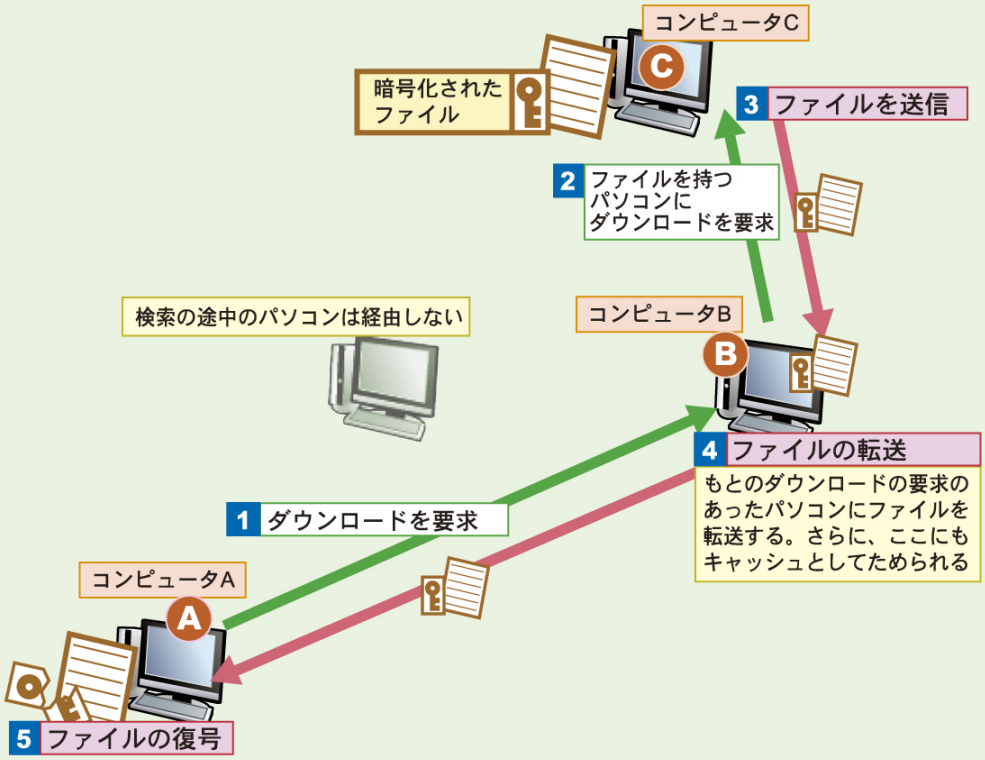


●ダウンロード（ファイルの入手）

検索結果から必要なファイルを選んで、ダウンロードを開始します。まず、コンピュータ B にダウンロードを要求します。コンピュータ B は、コンピュータ C からダウンロードを開始します。ダウンロードされたファイルはコンピュータ B のキャッシュフォルダに蓄えられ、ここで仮想キーのファイルのありかを示す IP アドレスをコンピュータ B のものに書き換えて、コンピュータ A に転送します。コンピュータ A は目的のファイルをキャッシュフォルダにダウン

ロードします。ダウンロードが終了すると暗号化されたデータを復号してダウンロードフォルダに保存します。

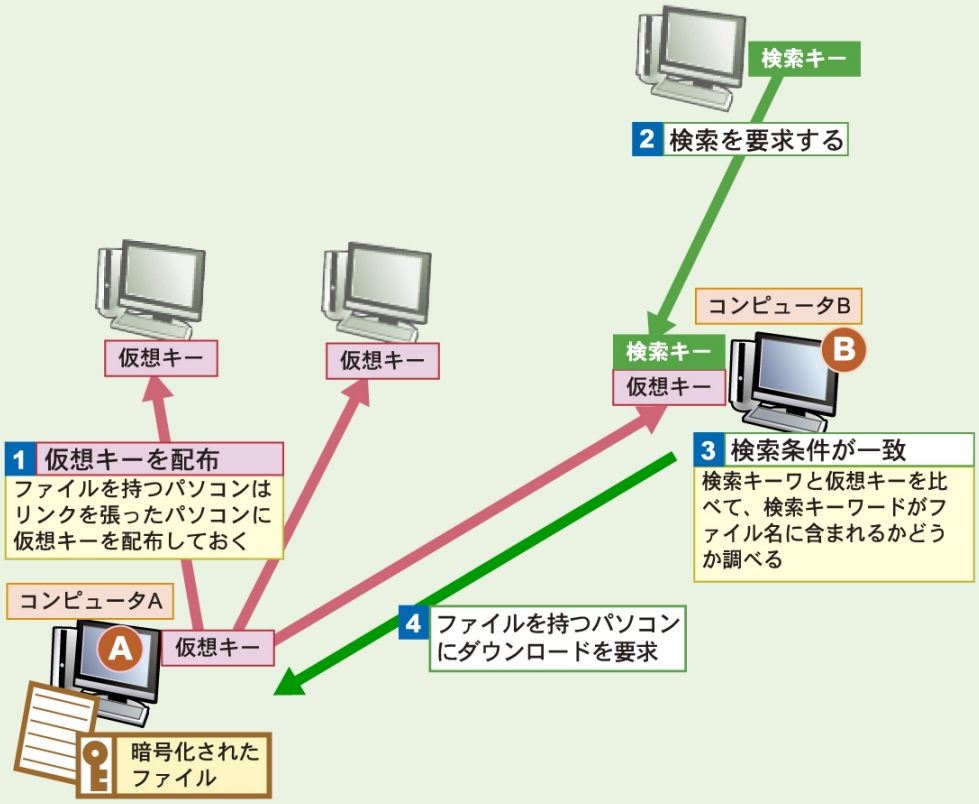
図2 ダウンロードの概念図



●アップロード（ファイルの公開）

公開したいファイルをアップロードフォルダに保存します。キャッシュフォルダに保存されているファイルも公開されるファイルと同じに扱われます。Winny はファイルが公開されると、検索キーと照合するための仮想キーを作って Winny ネットワークに送信します。応答したコンピュータは自分の仮想キーにそのデータを加えます。後は、誰かが検索し、ダウンロードするのを待ちます。

図3 アップロードの概念図



●匿名性と帯域の有効利用

Winny の動作の中にファイル公開の匿名性と帯域を確保するため工夫が盛り込まれています。検索やダウンロード時に、要求元のコンピュータ A には、コンピュータ B の IP アドレスしか分かりません。途中のコンピュータなどのキャッシュフォルダに保存されるので、コンピュータ B も本来のファイルの持ち主がコンピュータ C かどうかは分かりません。しかも、よくダウンロードされるファイルは、より多くのコンピュータのキャッシュに保存され、より近くのコンピュータからダウンロードでき、帯域を有効に利用できるようになります。Winny ネットワークを構成する個人のコンピュータは、電源が切れていたり、Winny が起動していなかったりすることがあります。その場合にも、多くのコンピュータにファイルがあれば、ダウンロードには困らないのです。

■暴露ウイルスとは

Winny などのファイル共有ソフトを通じて感染し、増殖し、数々の情報流出を引き起こす暴露ウイルスの代表的なものが Antinny G(アンティニージー)と山田ウイルスです。どちらも特別に強力な感染力やウイルス対策ソフトを欺くような技を持っているわけではなく、ほとんどの場合、一般に流通しているウイルス対策ソフトで検出し、駆除することができます。

●Antinny G

Winny でダウンロードされるファイルは ZIP 等で複数のファイルやフォルダを圧縮したものが多く、Antinny G はそうしたファイルの中に EXE(実行形式)ファイルで紛れ込んでいます。そのファイルをダブルクリックすることで、Antinny G は起動し活動を開始します。

デスクトップやマイドキュメントの jpeg や Word、Excel、PowerPoint、Access のデータファイル、さらに、Outlook Express のメールのデータなどのファイルを 1 まとめにして zip で圧縮し、その中にウイルス自身のコピーも潜り込ませます。できあがった zip ファイルに独特のファイル名をつけて、Winny のアップロードフォルダに保存し、Winny ネットワークにファイルを公開します。Winny と同等の機能を持ち、より匿名性が高いといわれる Share でも同じように動作する Antinny G が出ています。

●山田ウイルス(山田オルターナティブ)

Winny でダウンロードされるファイルに紛れ込んで、Antinny G と同様の方法で感染することもあれば、メールに添付されたファイルを不用意に開くことで感染することもあります。感染すると、HTTP サーバソフトをインストールし、HTTP サーバとしてコンピュータの HDD をインターネット上に公開します。同時に感染したコンピュータへのリンクを 2 チャンネルなどの掲示板に書き込みます。感染したコンピュータは、持ち主の知らない間にインターネットに公開され、誰でもアクセスすることができるようになります。

■どうして防げないか

Antinny G も山田ウイルスも EXE(実行形式)ファイルで、ダブルクリックしなければ起動しません。しかも、ウイルス対策ソフトで対応できるのに、現実には流出が止まりません。これが、「ファイル共有ソフトの特徴」と「ユーザーの心理」、そして「Windows の機能」を巧みに利用する暴露ウイルスの怖さです。

●ファイル共有ソフトの特徴

ダウンロードには時間がかかるので、複数のファイルをダウンロード指定しておき、ダウンロードが始まったら、後は Winny に任せておき、多数のファイルがダウンロードフォルダに保存されるのを待ちます。ユーザーはその間、寝ていたり他のことをしているケースがほとんどです。ところが、この使い方ではダウンロード時にウイルス対策ソフトを起動しておくと、ウイルスを含むファイルが勝手に削除されたり、警告を発したまま回答待ちの画面で止まったりします。そこで、ファイルの入手を優先するユーザーは、Winny 使用時にはウイルス対策ソフトをオフにしてしまい、ウイルスへの門を開いてしまいます。

しかも、ファイル共有ソフトのファイル公開機能は強力で、アップロードフォルダに保存するだけで、ファイルを公開できます。動作中は HDD へのアクセスが頻繁に発生するので、アクセスランプ点滅は当たり前で、裏でウイルスが動いていてもユーザーには分からないのです。

●ユーザーの心理

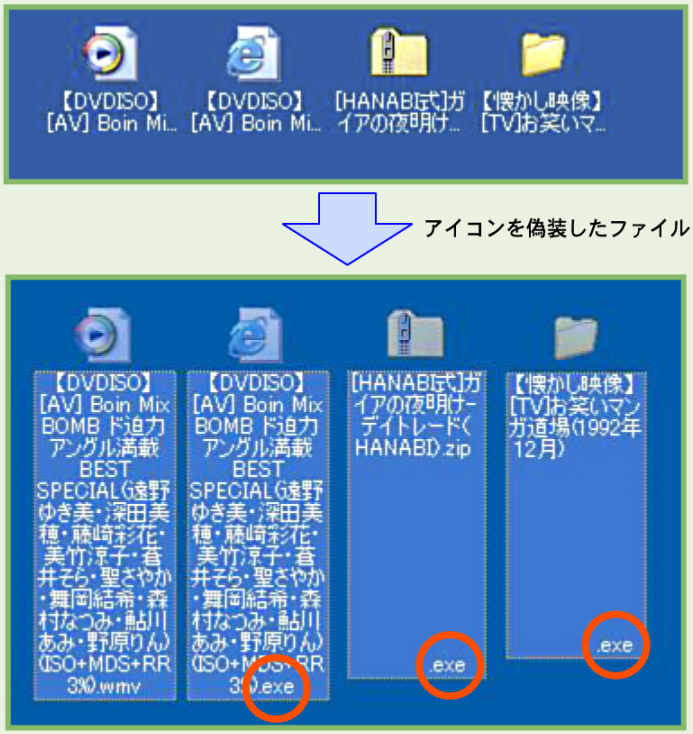
誰がファイルを公開したかわからないような匿名性が高いファイル共有のネットワークでは、流通するファイルのほとんどが、映画・TV ドラマ・音楽・コミック・写真集など著作権法に違反してデータ化されたものです。そうしたファイルを入手したくて多くの人が Winny を利用しています。ファイルを手に入れたいという意欲が先行し、ウイルス対策は邪魔者になります。

もうひとつは、野次馬的な利用です。相次ぐ情報流出で報道されている情報を見たいという目的で利用する人です。例えば、2006 年 3 月の海上自衛隊の情報流出ではマスコミで報道される前には数十人だった情報の所有者が、報道後には 100 倍に増えました。こうした利用者は、ふだんコンピュータを使っており、自分だけは大丈夫というという意識があります。しかし、慣れが油断を生むことも多いようです。

●Windows の機能

Winny で入手した ZIP ファイルを解凍したら、次のようなファイルやフォルダが表れました。

図4 偽装アイコン



慣れた人でもフォルダアイコンに対する警戒心は低いでしょう。見慣れた HTML や zip ファイルのアイコンは、ほとんど反射的にダブルクリックしてしまいそうです。でも、これらの一部は偽装されたアイコンで、EXE(実行)ファイルです。

Windows は長いファイル名の表示を省略しますので、拡張子が EXE であることに気が付かないかもしれません。ダブルクリックすると、「不正な、、、、」などのそれらしいメッセージを表示しますが、その時、すでにコンピュータは感染しています。

■どう防ぐか

ぷららネットワークスは、「Winny による情報流出を防ぐ」目的で、加入者が Winny を利用した場合、通信を遮断する措置を行いました。しかし、総務省は「Winny による信号かどうか調べる際にプロバイダーは通信の中身を一部解読することになる」という理由で憲法違反(通信の秘密の保護)のおそれがあるという判断を示しました。Winny の使用は自己責任で、という見解です。

●最良の策とは

「ファイル共有ソフトを使わない」ことです。企業レベルでは次のような施策が考えられます。

・ファイル共有ソフトの使用ならびにインストールの禁止
・ファイル共有ソフトの監視・動作停止・削除の実施
・上記ルールの徹底と罰則の強化

また、データを持ち帰って自宅のコンピュータで仕事をしたり、私物のコンピュータを持ち込んで業務を行った結果、情報流出させる例が後を絶ちません。そのためには

・仕事と個人のコンピュータの区別
・自宅の個人用のコンピュータから業務用のデータをすべて消去する
・やむをえず持ち出して処理するときはデータを暗号化して保存する

●最終的にはユーザー自身の問題

情報流出を教訓に Winny の使用を禁止したところ、ある社員が Winny をアンインストールして Share をインストールし、再び情報を流出させた例があります。体制やしくみを強固に作っても、最終的には使う人の問題です。残念なことに Winny や Share ネットワークを流通するデータは違法性の強いデータがほとんどです。そして、多くの人がそうしたファイルを入手するために利用しています。興味本位で流出情報を見るために利用する人も少なくありません。ほしいものを入手することを最優先にし、ウイルス対策を無視した結果、ウイルスへの感染が増え、情報流出が繰り返される悪循環になっています。

ファイル共有ネットワーク上で流通している違法性の強いデータや流失データを入手したり、公開する行為は犯罪です。法人情報だけでなく、コンピュータの HDD の内容がネットに公開されたら、自分だけでなく家族や友人、知人の電話番号やメールアドレスなどの個人情報の流出もありえます。詐欺被害、訴訟リスク、失業、逮捕などファイル共有ソフトの利用は大きなリスクを伴います。最終的にユーザー自身と周囲の人々にツケが回ってきます。本当にそれ

だけのリスクを冒してでも必要な情報かどうかを考えるべきでしょう。

●ウィニー対策参考 URL(2006 年 5 月 24 日現在)

・Winny&暴露ウイルスのここが知りたい--- 日経 NETWORK スペシャル・エディション
【http://itpro.nikkeibp.co.jp/article/COLUMN/20060419/235637/】

・特番サイト(Winny)ウィニー問題
【http://itpro.nikkeibp.co.jp/winny/index.html】

・情報処理推進機構:セキュリティセンター
【http://www.ipa.go.jp/security/index.html】

・内閣官房 情報セキュリティセンター
Winny を介して感染するコンピュータウイルスによる情報流出対策について
【http://www.nisc.go.jp/press/inf_msrk.html】