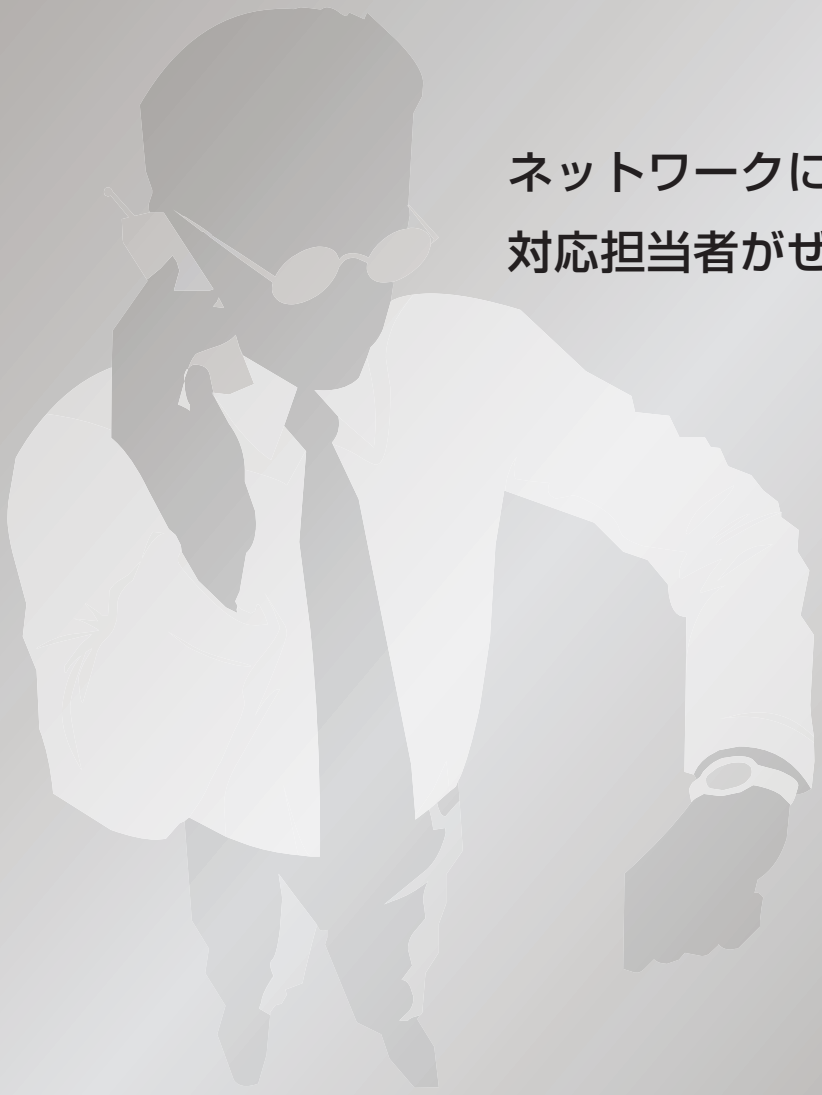
情報漏えい対応ガイド

【Winny・share 編】

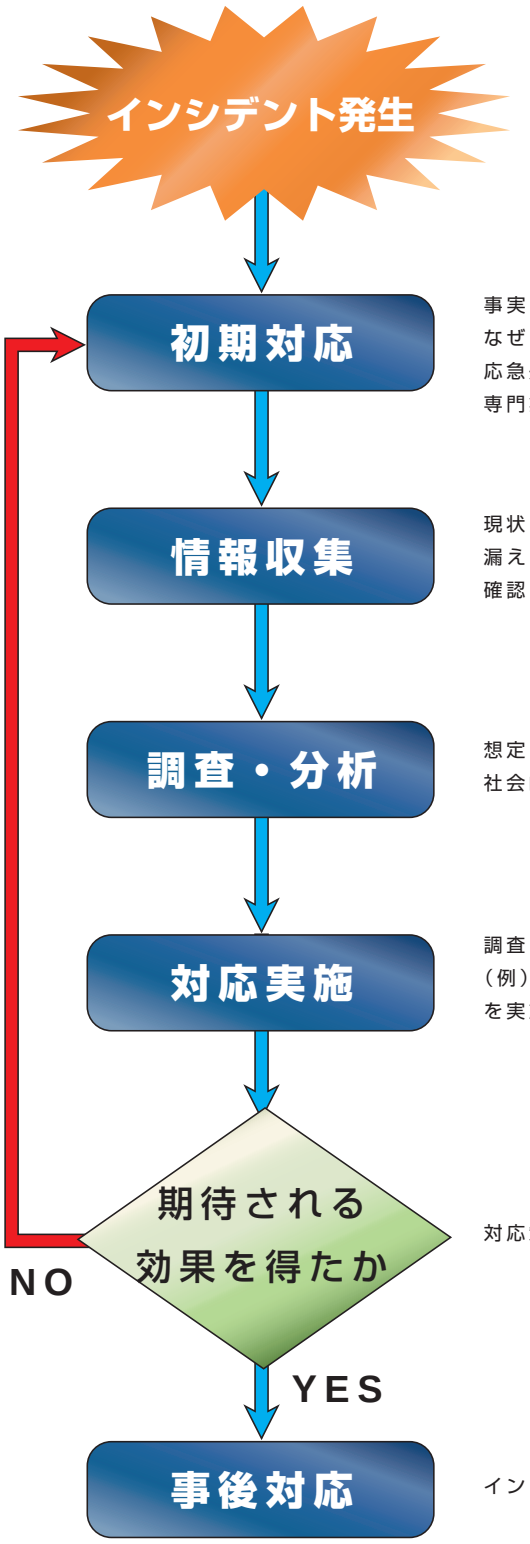


ネットワークに企業情報が流出！
対応担当者がぜひ知っておいて欲しい事項

NetAgent

目 次

【Winny・Share 情報漏えい対応ワークフロー】



事実を確認し、インシデントを 5W1H（いつ・だれが・どこから・なぜ・どうして・どのように）で確認する。
応急処置（Winny・Share の利用停止など）をする。
専門業者に対応を依頼する。

現状を確認する。
漏えいした情報が企業における重要情報か個人情報などであるかを確認し、影響を見積もる。

想定されるリスクを列挙し、対応の重要度を判定する。
社会的な影響の有無を確認する。

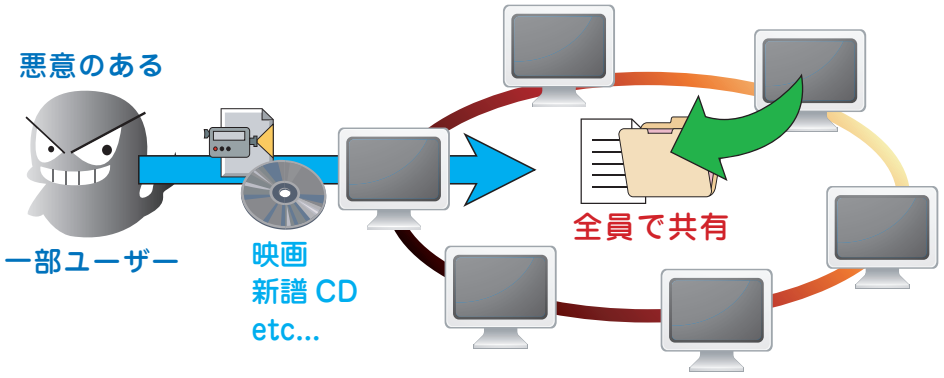
調査・分析によって得られた対応策を実施する。
（例）ネットワーク調査・端末調査・拡散防止サービスなどの対応策を実施する。

対応策が有効に働き、事態の沈静化が行えたかどうかを確認する。

インシデント発生 再発防止策の検討

【Winny・Share とは】

Winny や Share と呼ばれるソフトウェアは、ネットワークを通じて、パソコン内の文書や画像などのファイルをそのネットワークの参加者全員が共有するためのもので、「P2P（Peer to Peer）」と呼ばれる仕組みを利用したソフトウェアです。この 2 つの P2P は日本製で使い易く、**国内では約 50 万人のユーザー**がいます。P2P は使い方によっては大変便利な技術なのですが、ここまで Winny や Share が流行した要因のひとつには、一部の悪意を持ったユーザーが映画や音楽、有償ソフトウェアなどといった「版権もの」を無料（違法）で共有するために利用していることが挙げられます。



【Antinny ウイルス】

そして「悪意」のある使い方をされているものには付きまといやすいことなのですが、Winny には害意を持った特有のウイルスが存在します。
それが暴露ウイルスとも呼ばれる「Antinny」です。現在のところ、流出事件を引き起こすこうした暴露系のウイルスが確認されているのは P2P だけで、流出事件のほとんどが Winny と Share という 2 つの P2P ネットワーク上で発生しています。Antinny ウイルスは、Winny や Share のネットワークを介して感染します。そして感染すると、このウイルスはそのパソコンの中にある画像や Office 書類ファイル、デスクトップなどをコピーし、まとめて Winny や Share のネットワーク上に公開するのです。つまり Antinny というウイルスは

「ユーザーが意図しないデータをネットワーク上にばら撒く」

ことを目的とした情報流出型のウイルスなのです。

【Antinny ウイルスによる被害】

Antinny ウイルスによって感染したパソコンの中に他人の画像や個人情報などのファイルが入っていた場合、ユーザー自身だけでなく他の人の情報までもが同時にネットワーク上に公開されてしまい、被害はユーザー本人のプライバシーのみに留まりません。

さらに悪いことに「事件」として扱われているケースの大半は

「勤務先の企業・団体の機密データが流出した」

「個人のプライバシーに関わるデータが流出した」

といった類の被害です。

【なぜ事故が起こるのか】

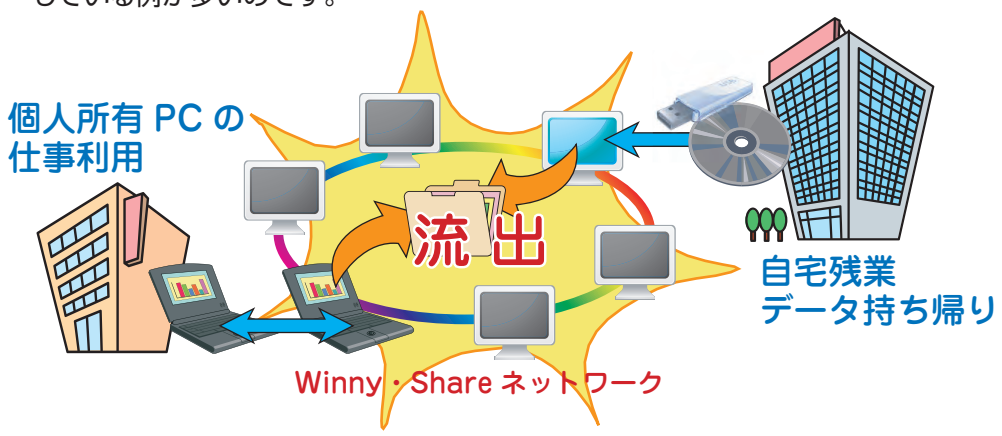
会社内のパソコンに対して Winny や Share をインストール、社内で使用されるといったケースはそう多くはありません。では、なぜ情報漏えい事故が後を絶たないのでしょう。

それは、顧客データや機密文書等といった「被害規模の大きな情報」が漏えいした事故の多くが、

「自宅に持ち帰って自分のパソコンで仕事をしたデータ」や

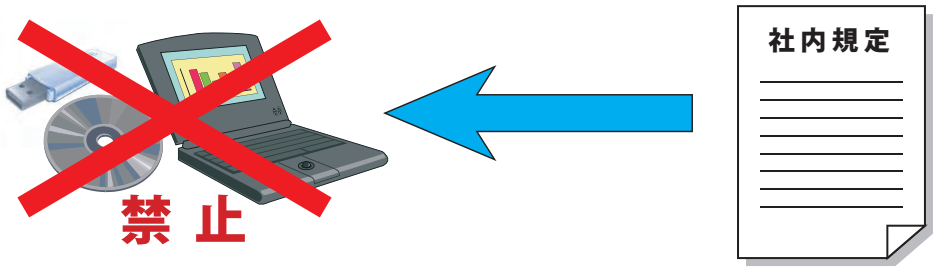
「仕事に使っている個人所有のノート PC」

からの情報流出なのです。つまり、いくら社内のシステムを強化したとしても情報漏えい事故が起こる場所は社内とは限らず、むしろ自宅など他の場所で発生している例が多いのです。



【事故を防ぐには】

情報漏えい事故の原因は「社外に持ち出された機密データ」の存在にあります。しかもこれは所謂スパイ行為とは異なり、その人の善意、厚意に基づく自宅残業や個人資産（パソコン）の業務への提供といった「悪意のない外部持ち出し」がほとんどなのです。こうした事故を予防するために、まず内部規定などでデータの社外への持ち出し、そして個人所有パソコンの仕事利用を禁止し、データ管理を徹底する必要があります。



また、それだけでは完全とは言えません。それに加えて、実際の勤務にあたって各社員が自宅に社内の機密データを持ち出したり、個人のパソコンを仕事に使ったりといったことをする必要のない勤務体系・勤務体制の確立も重要です。
そして万全を期すためには、今後の持ち出しを止めるだけでなく、過去すでに持ち出されてしまっているデータについても回収・消去といった対策を講じる必要があります。

【コレクターの特徴】

Winny や Share のコレクターの特徴について知っておくことは、対策を考える上で重要なことだと考えます。ここでは特に企業・団体に関する情報流出の場合に注意すべきコレクターのパターンについて紹介します。

1．企業情報や個人情報の流出に特別の興味を抱いている。

暴露系ウィルスによる流出ファイルを意図的に収集しており、発見した情報を匿名掲示板などに書き込む（全員ではないが）。その書き込まれた情報を見た別のユーザーがそのファイルを検索し、更に拡散が広まるケースが多いのです。
そのため、一旦このユーザー層の手に流出ファイルが渡ると、ネットワーク上からファイルが消えるまで非常に長い時間を要することになります。更に一旦ネットワーク上からファイルが消えても、流出事件が一般へ公表された後に、再びそのファイルが公開・共有される可能性もあります。

2．発見したファイルを、その中身が分かりやすいように、より具体的な名前（社名等）をつけ、別のネットワーク（Winny なら Share、Share なら Winny）にまたがって流出させる。

したがって、Winny・Share 両方のネットワークを並行して調査することが実態把握のためには重要となります。

Winny 調査サービス・Share 調査サービス
http://forensic.netagent.co.jp/

【事前対策で重要なこと】

P2P ネットワークは基本的に外部からのコントロールが不可能なネットワークですので、**情報漏えいが起きてしまってからでは、対策として出来る事は自ずと限られます**。万が一の際は、まず実態を把握することが重要ですが、流出によって被害を受ける可能性のある当事者（お客様）の方々に対して、状況報告とこれからどういった対策を講じるのか、その結果受けることになるであろうメリットとデメリットを提示しながら、お客様の納得のいく報告と対策を行うことが何より重要となってきます。

Winny・Share に起因する情報漏えい事故は、実は完全に防ぐことが可能な類の事故であるということをご存じでしょうか? 単に社内ネットワークに対するセキュリティ製品・サービスの導入で防ぐ、という方法だけで対策を図っても、ポイントのずれた対策となりかねず、残念ながらそれだけではこの類の流出事故を防ぐことは出来ません。
流出してしまってから「しまった」では遅すぎるのです。しかし人間が関わる以上「100% 絶対に情報が漏えいしない対策・システム」などというのは不可能です。利便性を高めるための IT であるにもかかわらず、情報セキュリティ対策を強化し続けたあまり営業活動が阻害されてしまっては本末転倒です。
対策で何より大切なのは

「絶対に流出させてはいけない情報の範囲を明確に定める」
「そのデータを社外に持ち出さない、持ち出させない」
「そのためのルールを作成し、システムでそれを支える」

という点にあります。
つまり、絶対に流出してはならない重要な情報、そしてそれを含んだファイルが社外には存在しない、という状況を作り、それを保つ。そのための対策をいかに実施するのかという点が何より重要なのです。

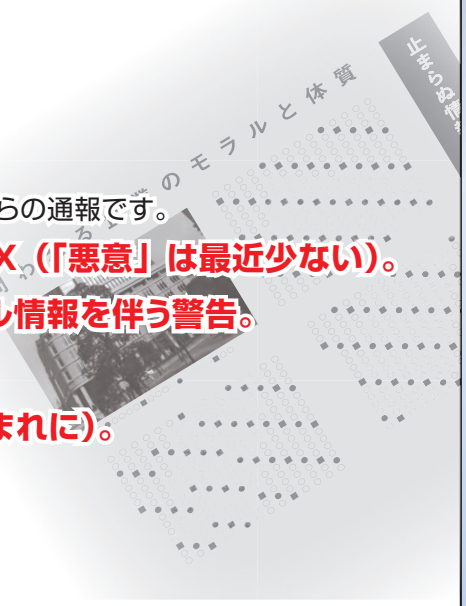
2-2

情報漏えい事故を防ぐために
～万全を期すためには～

【企業・団体が最優先で対応すべきこと】

もし万が一、情報が流出してしまったら…
その事実が発覚するのは、多くの場合、外部からの通報です。

善意・悪意の第三者からのメール・FAX（「悪意」は最近少ない）。
監督官庁から注意喚起または、ファイル情報を伴う警告。
匿名掲示板への書き込み。
流出させた本人からの自己申告（ごくまれに）。
マスコミからの問い合わせ。



【流出が発覚したら】

企業情報の Winny・Share ネットワークへの流出事故が発生したとき、やるべきこととやってはいけないことがあります。

※あくまでも流出が確認されてからの話ではあるのですが、残念ながら第三者からの通報で発覚した場合、ほぼ確実に流出していると考えてほぼ間違いないと考えられます。

・被害者の救済

流出情報によって被害を受けた個人・組織に対し、事実を伝え、直接謝罪するとともに、対処方法や考えられるリスクを教える等、適切な支援を行う必要があります。

・被害拡大の防止

流出情報が拡散することで、悪意を持ったユーザーの手に情報が渡る可能性も高まり、二次被害の発生確率も高まります。一旦流出した情報ができるだけ拡散しないよう、手を打つ必要があります。

・二次被害の防止

情報流出によって被害を受ける可能性のある個人・組織に対し、事実を伝え、自己防衛を促すなど、二次被害の防止に努める必要があります。但し、Winny·Share の特性上、ネットワークに流出情報が存在する時点で公表という手段をとると一部のユーザーがファイルを入手することで拡散が促され、被害を拡大させることがあります。

過去、流出の事実を公表することを最優先に考え、行動されている事件も少なくないのですが、そのタイミングによって結果的に公表することが被害を更に拡大してしまう場合が非常に多く、それが Winny・Share による情報流出の最大の特徴であることをご理解ください。

過去、流出の事実を公表することを最優先に考え、行動されている事件も少なくないのですが、そのタイミングによって結果的に公表することが被害を更に拡大してしまう場合が非常に多く、それが Winny・Share による情報流出の最大の特徴であることをご理解ください。

【流出が発覚した直後にやってはいけないこと】

【1】

Winny・Share を利用してネットワークを調査し、流出ファイルを確認すること。

きわめて効率が悪い上、Winny・Share の仕様上、ダウンロードしているファイルは自動的にアップロードされます。この時点で拡散がさらに拡がり、自分で被害を拡大させたことになってしまいます。

【2】

情報を流出させた本人に直接 PC 提出の依頼を行うこと。また、PCを確保に出動する際に本人に事前通知すること。

個人 PC には多かれ少なかれ他人の目に触れさせたくないものが入っている。ましてや情報流出の疑いを持たれているとなれば、高い確率で証拠隠滅が図られ、後々の調査に支障をきたす。

【3】

本人の同意書を取らずに、個人所有のPCを確保や調査をすること。

情報流出の疑いがあるといえども、PC は個人の所有物であり、勝手に確保はできません。またプライバシーの問題も軽視する訳には行きません。事後の問題発生を避けるためにも事前に調査の同意書を取り、プライバシーに配慮する必要があります。対象のPCが家族などで共有されている場合、基本的には全員の同意書が必要となります。

【4】

情報を流出させたPCに対し、ウィルス対策ソフトを起動し、ウィルスの駆除を行うこと。

PC を起動させた時点、ファイルにアクセスした時点で、ファイルのタイムスタンプが書き換えられ、証拠が意図せずに隠滅してしまいます。

【実態の把握】

流出事故の実態を把握する為には、まず何より「何が流出しているか」の把握が最優先です。この場合、実際にネットワークから流出ファイルを取得するか、流出させたパソコンそのものを調査して内容を確認するかの2つの方法しかありません。実は、これまで多くの事故を起こした会社はここでつまずいているケースが多いのです。

P2P ネットワーク上からファイルを取得する為には Winny・Share ノード（Winny・Share ソフトの起動可能なパソコン）が必要ですが、前述のように Winny・Share を迂闊に使ってしまうとその仕様によって、Winny・Share が「ダウンロードしている途中のファイル」は同時に（ダウンロード中のファイル=完全ではない一部分のデータの状態でも）自動的にアップロードされネットワーク上に共有されますから、そのせいで更に被害の拡散を拡大させてしまいます。

また、そのデータを流出させた疑いのあるパソコンの調査を実行するには、専門のツールと技術、経験を必要とします。パソコン内のファイルは電源を入れたり切ったりするだけでもデータが書き換えられるようになっているので、不用意に触ると証拠となるデータが消える可能性があります。

◆ フォレンジック調査

流出の疑いのあるPCの調査を行う場合、PCのハードディスクを調査する場合、対象となるハードディスクの保全（複製）を行い、複製側の調査を行う。緊急でPCの調査を行う必要のある場合は、専用の書込み禁止装置、またはソフトウェアを使用し、証拠となるデータの改ざんを防ぐことが必要である。

http://forensic.netagent.co.jp/

いずれにしてもこうした実態を正確に把握する際は、事後のことを考えても作業を専門家に任せた方が確実でしょう。ただし緊急対応などで作業する場合は、作業した内容の記録を 5W1H 形式で取るようにしましょう。

【初期対応】

では具体的に、情報の流出が確認された際には、まずどのような対応をすべきなのか、その内容を見ていきましょう。

Winny・Share への情報流出に対する対応

1．Winny・Share ネットワークへの流出が確認された場合、**その規模や原因を特定**する必要があります。それには、端末（パソコン）とネットワーク両面からの調査が有効です。
ネットワーク調査により流出ファイルを特定すれば、その流出の規模と状況を把握することが可能となり、高い確率で流出元となったパソコンの所有者も特定することが出来ます。そのパソコンを確保し、専門の調査を実行すれば、流出の経緯、内容なども把握することが可能になります。

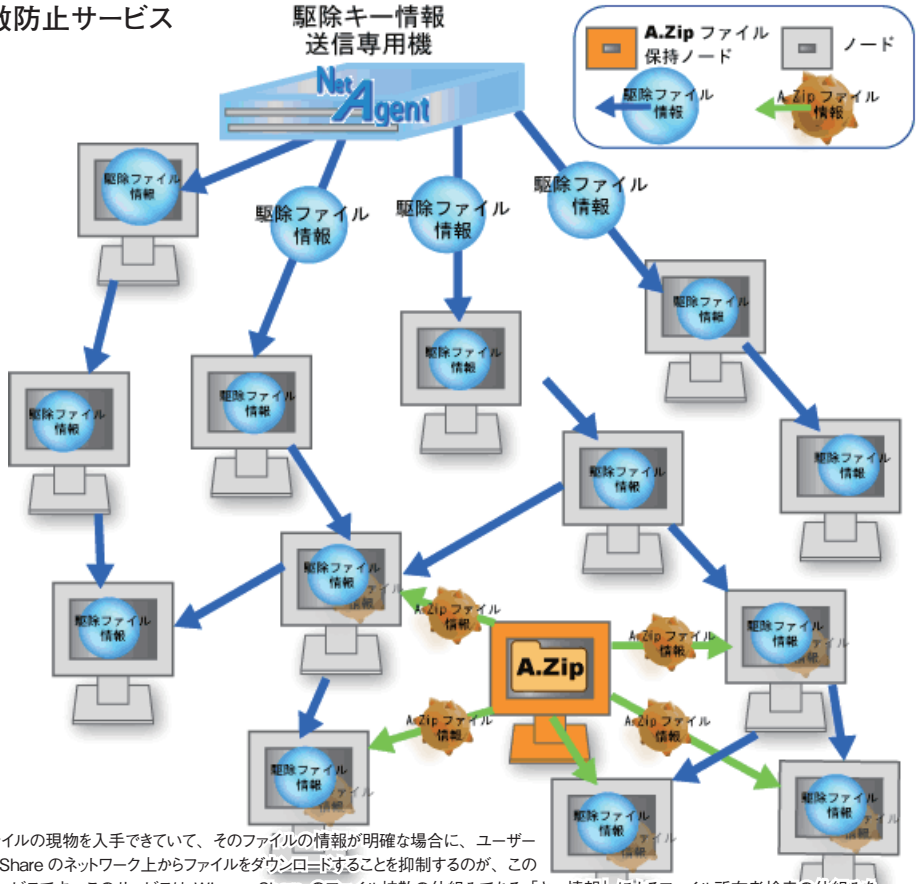
2．流出した情報の内容、漏えいの規模と状況によって対応策は変わってきます。ファイル所有者に対し法的措置を検討することから、場合によってはその流出をあえて放置・黙認することまで、**取るべき対応策は流出したデータの範囲やその重要性、緊急性などによって様々**です。
ともあれ、流出事故によって被害者となる（可能性を含め）お客様を守るということを最大の優先事項として行動するのは当然のことです。

3．流出したその情報によって被害者になる可能性のある全てのお客様に対し、速やかに事実の通知をする必要があります。
ただし、Winny・Share ネットワークの特性上、不用意にメディア等への公表という手段をとってしまうと流出情報が更に拡散することになり、二次的な被害の拡大へとつながる可能性が極めて高くなることを踏まえ、企業・団体の監督官庁等と協議の上、**状況を見ながら対応する必要**があります。

【被害拡大の防止】

Winny・Share による漏えい情報は永久に消えないとか、やがて消えるとか、色々と言われています。では流出してしまった情報（ファイル）を回収、もしくは抹消することは実際には可能なのでしょうか? いったん掲示板などで話題になり、流出ファイルの存在が広範囲に知られてしまったファイルは、相当の長期間、複数のユーザーによって共有し続けられるという傾向が強いようです。また、沈静化した後も再び話題になることが多く、以前ファイルを入手した者が再びネットワーク上で公開し結果として長期間にわたってネットワーク上に存在し続けます。最も広範囲に拡散するのが、メディア、マスコミに対する公表です。特に TV で取り上げられた場合、流出したファイルの拡散・コピーが1日で1000件を超えるケースがあり、この場合には流出ファイルがネットワーク上から完全になくなることはまず期待できません。もし流出した情報の権利者に法的措置を講じる用意があり、法的にもその権利が発生する場合（弁護士の判断が必要）、該当するデータをネットワーク上から削除することができる可能性はあります。

◆ 拡散防止サービス



流出したファイルの現物を入手できていて、そのファイルの情報が明確な場合に、ユーザーが Winny・Share のネットワーク上からファイルをダウンロードすることを抑制するのが、この拡散防止サービスです。このサービスは Winny・Share のファイル拡散の仕組みである「キー情報」によるファイル所有者検索の仕組みを利用したサービスで、対象となる流出ファイルと同じ『情報』を持つ「拡散防止キー」をネットワーク上に大量に配布することで、流出ファイルのダウンロード成功率を 1/100 から 1/1000 に低減させることが出来ます。

http://forensic.netagent.co.jp/winny_kakusan.html

4

まとめ ～いま、何をすべきか～

【まとめ】

Winny・Share ネットワークへの情報漏えい事故のそもそもの原因は、企業や団体によって直接管理されていない「個人所有のパソコン上に、本来は在るべきではない機密情報が存在する」という状況を生み出した事実に他なりません。
また、いくら Winny や Share の使用を禁止しても、こういった P2P ソフトには冒頭で述べた通り本来は大変便利な技術（BB ブロードキャスト等、他のサービスにも広く用いられている技術）なのです。そもそもソフトウェア自体に「違法性」はなく、使用禁止の徹底は現実的に不可能です。

前述の【事前対策で重要なこと】に記載の通り、対策で何より大切なのは

「絶対に流出させてはいけない情報の範囲を明確に定める」
「そのデータを社外に持ち出さない、持ち出させない」
「そのためのルールを作成し、システムでそれを支える」

という点に尽きます。
絶対に流出してはならない重要な情報を含んだファイルが、社外には存在しない状況を保つための対策、が何より重要なのです。

【会社概要・お問い合わせはこちら】

ネットエージェント株式会社
情報漏えい対策室

住所：東京都墨田区江東橋4-26-5　東京トラフィック錦糸町ビル9階
TEL：03-5625-1245　／　FAX：03-5625-9008

URL：http://www.netagent.co.jp/
e-mail：forensics@netagent.co.jp

【ネットエージェント株式会社 情報漏えい対策関連製品】

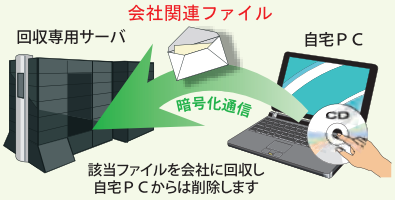
【1】

◆ USB 関所守

USB 関所守は USB メモリ等の外部ストレージからの情報漏えいを防ぎます。個々の PC にはインストール不要で購入後すぐ USB メモリ禁止環境が構築できます。また事前に会社用として登録した USB メモリのみ使用できるようにできます。
USB 関所守を持ち出して一度適応させておけば、持ち出し用のノート PC を外に持ち出し中であっても制限が有効になっています。会社に戻ってきたとき私用 USB を使っていないかもチェック可能です。さらに USB 関所守は Winny を始めとした P2P ソフトなどの実行を禁止してくれます。もちろん設定を変更するソフトも禁止です。
また私物の USB メモリなどで情報漏洩があった場合、全社的にスキャンして、私物 USB メモリの使用者と、メーカ名や型番をあぶりだします。

http://www.netagent.co.jp/usb_ng.html

【2】



◆ Winny 特別調査員2

Winny 特別調査員2は、会社から配布された「調査員CD」を社員が個人（自宅）のパソコンにセットするだけで、インストールすることなく動作します。
セットされたパソコンの内部から会社関係のファイルを自動的に見つけ出し、会社のファイル回収専用サーバにそのファイルを回収（アップロード）します。同時に、自宅のパソコンからは、もし仮にファイル復旧ソフトを使ったとしても、ファイルが復活できないような形で完全に削除します。これによって、過去すでに持ち出されてしまっている機密データによる情報漏えい事故が発生する可能性をなくします。

http://www.netagent.co.jp/winny_check2.html