

相次ぐ情報流出事件 暴露系ウィルスが与えた影響を振り返る

平成18年3月22日
インターネット協会評議員会

WEB110 吉川誠司

Winny経由での情報流出事件

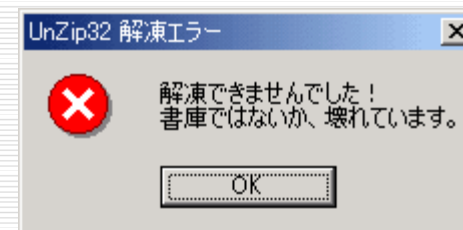
- 2006/3/16・・・愛媛県警、Nシステム情報流出か 車10万台ナンバー
 - 2006/3/15・・・空港の暗証番号流出、全日空機長の私物パソコンから
 - 2006/3/15・・・TBS出演者らの個人情報、「ウィニー」通じ流出
 - 2006/3/14・・・通知表80人分がネット流出・大津の教諭、ウィニー使う
 - 2006/3/9・・・富山市の病院で手術室の使用履歴2,873件が流出
 - 2006/3/8・・・NTT西日本でも顧客情報流出
 - 2006/3/8・・・住友生命、8000人分の個人情報流出
 - 2006/3/7・・・愛媛県警 被害者情報や殺人事件資料流出
 - 2006/3/5・・・岡山県警で1500人の捜査情報流出 被害者名など
 - 2006/3/1・・・海自の情報流出、昨年中に「秘」含む5件 空自でも
 - 2006/2/24・・・書記官PCから東京地裁の個人情報149件流出
 - 2006/2/24・・・NTT東西、フレッツユーザー約1,400件分の顧客情報が流出
 - 2006/2/22・・・受刑者情報の流出、5施設3380人分と判明
 - 2006/2/1・・・郵便局の顧客情報2800件、「ウィニー」通じ流出・千葉県
 - 2006/1/27・・・広島病院、ネットにデータ流出
 - 2006/1/20・・・筑波大の学生がウイルス感染、臨床実習の患者情報が流出
 - 2006/1/17・・・三井住友海上、業務委託先で590人分の個人情報漏洩
 - 2006/1/16・・・兵庫県養父市のCATV 7300人の個人情報流出
-

主な暴露ウィルスの種類とその動作

「Antinny.G」別名:キンタマウイルス

ワームは、感染コンピュータのデスクトップのスクリーンショットを収集し、JPEG形式で保存します。またレジストリ情報から登録者、組織、メールアドレスを取得しテキストファイルに保存します。そして取得したすべての情報をZIPまたはLZHファイルに保存し、Winnyの共有フォルダ内にコピーを作成します。

ワームが実行されると、右のメッセージボックスを表示します。



主な暴露ウィルスの種類とその動作

「TROJ_UPBIT.A」「Antinny.AB」「Antinny.AD」

別名: 仁義なきキンタマ

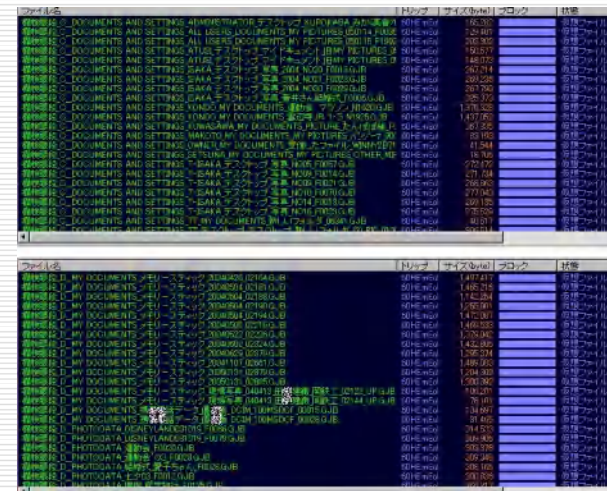
感染するとランダムな時間で感染者PCのスクリーンショットを公開する。データは「仁義なきキンタマ ○○のデスクトップ (yyyymmdd-hhmm).jpg」という形で流出。

「仁義なきキンタマ○○のドキュメント.zip」という形で、感染者PCのOutlook系メールファイル(.eml/.dbx)に加え、Excel(.xls)、Word(.doc)、PowerPoint(.ppt)、そしてテキストファイル(.txt)のデータまで流出する。

主な暴露ウィルスの種類とその動作

「**TROJ_ANTINNY.C**」通称「**欄検眼段**」(リャンクーガンドウ)
 デジカメ画像データをWinnyネットワークに流す

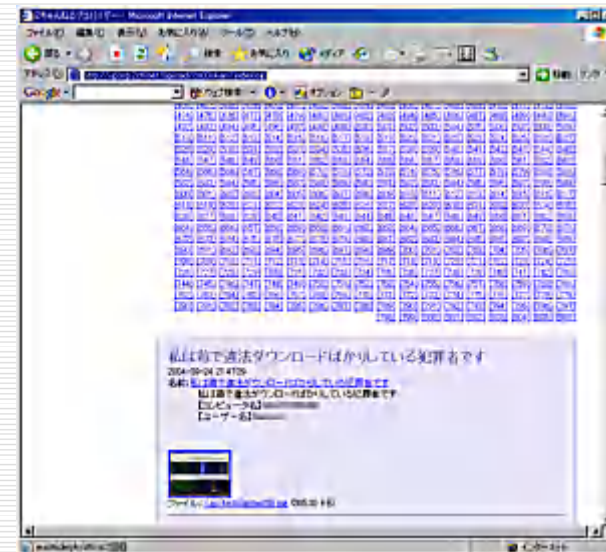
感染するとHDD中にある「DSC*.JPG」ファイルを探し出して、「フォルダ名_ファイル名からDSCを除いたもの.GJB」という形式で、新規に作成したWinnyのアップロードフォルダ(c:¥temp000)にそれらをコピーする。



主な暴露ウィルスの種類とその動作

「Trojan.Upchan」別名: 苺キンタマ、アップチャン 2004/09/27
デスクトップ画像を2ちゃんねるにアップロードするウイルス

感染したPCのデスクトップ画像を2ちゃんねるプロバイダーのアップローダーに自動的に送信するほか、Webサイト「BBS TABLE for 2ch」に掲載された2ちゃんねるの各掲示板をランダムに選択し、感染したPC名やユーザー名、アップローダーに送信されたデスクトップ画像のURLを掲載する。



このウイルスは常に、互いに監視しあう2つの同一プロセス(ウォッチャー)を実行しているため駆除が困難。

主な暴露ウィルスの種類とその動作

「Trojan.Exponny」別 名: エックスポニー, イーエックスポニー
ローカルドライブを全公開するWinny用ウイルス。2006/03/17

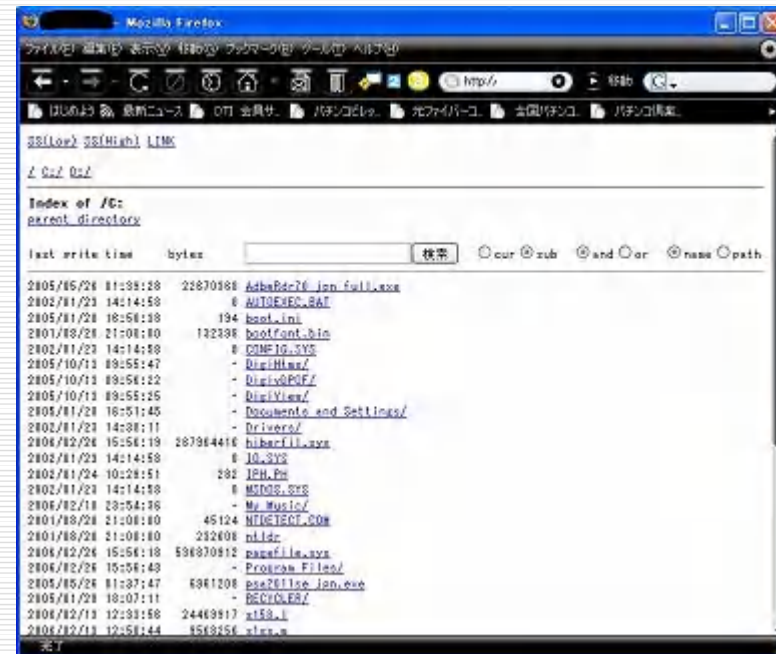
Exponnyは、所有するコンテンツをWinnyネットワークで共有するための設定を変更し、ローカルドライブ全体をWinnyネットワークに公開する。さらに、感染者のデフォルトのメールアドレスを検索し、[UPALL] ID=[メールアドレス]という情報を「SYSTEM.INI」ファイルに追加する。これにより感染者のメールアドレスが知られる恐れもある。



主な暴露ウィルスの種類とその動作

「TROJ_AGENT.AZW」通称:山田オルタナティブ 2006/3/3

感染したPCは、WebサーバーとしてHDDの全内容をインターネット上に公開する。また、ほかの感染PCのリンク集も自動生成して公開する。P2Pソフト「Winny」だけでなく、メールの添付ファイルやWebサイトからのダウンロードで感染する可能性があるためWinny利用者以外も注意。



警察庁が緊急通達「私物PCでもWinny厳禁」

警察庁は3月7日、全国の警察本部に対して、公務だけでなく私物のPCについてもP2Pソフト「Winny」の使用を禁止する緊急対策を通達した。

警察庁では公私で使うPCでWinnyを使用禁止するとともに、公務による使用承認を受けていないPCおよび外部記録媒体で警察情報を取り扱うことを禁止する。また、自宅で使うすべてのPCの自己点検を義務づけ、Winnyや警察情報が保存されている場合はすみやかに削除するよう求めた。自己点検については、報告書を提出させる。公務での使用を届け出していないPCについては、警察情報をすべて削除した上で撤去させる。

そのほか、公務で使用するPCを許可なくインターネットに接続することを禁止するほか、PCを外部に持ち出す際は許可を得るとともに、警察情報を暗号化させるなど管理を徹底させる。

ウィニー使われぬと誓約書、岡山県警が全職員から

(読売新聞)2006年 3月13日

私物パソコンに入れたファイル交換ソフト「Winny(ウィニー)」が原因で捜査資料がインターネット上に流出した問題で、岡山県警は全職員約3300人にウィニーを使わないなどとする誓約書を提出させ、自宅の私物パソコンの点検も始めた。

警察庁の指示を受けた措置で、誓約書には、捜査資料を自宅に持ち帰らないことも盛り込んでいる。私物パソコンは、ノート型は署などに持参させ、「セキュリティー指導員」が点検。デスクトップ型の場合は自宅に出向き、調べている。

「ウィニー使いません」 愛媛県警、全職員に誓約書

(共同通信)2006年 3月10日

愛媛県警警部(42)のパソコンから捜査資料がインターネットに流出した問題で、県警は10日、全職員約2700人にウィニーなどのファイル交換ソフトを使わないなどとする誓約書を書かせると発表した。

誓約書は(1)公務に使うパソコンやフロッピーディスクなどを許可なく外部に持ち出さない(2)私物パソコンであってもファイル交換ソフトを入れないの2項目。

官用パソコン緊急購入 5万台 情報流出で防衛庁

朝日新聞(2006年 3月14日)

自衛隊の秘密情報などが隊員の私物パソコンからファイル交換ソフト「ウィニー」でインターネット上に流出した問題で、防衛庁は14日、再発防止のための検討会を開き、対策として官用パソコン約5万6000台を緊急購入することを決めた。

同庁は職務で私物パソコンを使用することを禁止する方針を固めており、官用パソコンを増やす必要があると判断した。持ち運びが困難なデスクトップ型を中心に、本年度予算を使い、来年度中に配備する予定だ。

防衛庁によると、全自衛隊員ら約26万人を対象にパソコンの使用状況を調査した結果、約12万台の私物パソコンが職務で使用されていたことが判明。

うち約80台でファイル交換ソフトが使われていたが、現在はすべて削除されているという。

借り上げ私物PC全廃へ ウィニー対策で神奈川県警

朝日新聞(2006年 3月8日)

ファイル交換ソフト「ウィニー」を入れた警察官の私物パソコンから捜査情報が相次いでインターネット上に流出した問題で、神奈川県警の井上美昭本部長は8日の記者会見で、職員が公用に使うパソコンのうち「公用借り上げ」の私物パソコンを07年末までに全廃する考えを明らかにした。井上本部長は「職場の私物パソコンをなくして情報管理の徹底を図りたい」と述べた。

県警職員が仕事に使っている約1万2700台の公用パソコンのうち、「公用借り上げ」の私物パソコンは約5700台。県警は、交代制の職場もあるため約1万台の公用パソコンがあれば私物を借り上げなくても職務に支障がないとみており、07年末までに不足分数千台を新たに購入する方針だ。

米信用調査会社に個人情報漏洩で過去最大の課徴金

読売新聞（1月27日）

米連邦取引委員会（FTC）は26日、大量の個人情報漏えいが昨年に見つかった信用調査会社「チョイスポイント」（米ジョージア州）に対し、総額1500万ドル（約17億5000万円）の課徴金支払いを命じた。

FTCの課徴金としては過去最大額となる。このうち罰金は1000万ドルで、残り500万ドルは被害者への補償に充てられる。

チョイスポイントは、正規の顧客を装った不正利用者に16万3000人分もの個人情報を誤って流し、米国で個人情報保護法制を強化する動きの発端となった。

個人情報漏えい、1年以下の懲役・自民が保護法改正案

日経新聞(2月15日)

自民党の情報漏えい罪検討プロジェクトチームは15日、個人情報保護法改正案の概要をまとめた。業務上知り得た個人情報を漏らした民間企業の従業員に「1年以下の懲役または50万円以下の罰金」を科す。公明党と協議し、3月中に議員立法で国会に提出、早期成立を目指す。

対象は(1)5000件以上の個人情報を保有する個人情報取扱事業者(2)取扱事業者から個人データの取り扱いを受託した業者——の従業員と元従業員。業務で知り得た個人情報を「自己または第三者の不正な利益を図る目的」で漏洩(ろうえい)した場合に罰則を科す。報道機関や政治団体への個人情報提供は対象外。

欄検眼段(リャンクーガンドウ)による流出事件

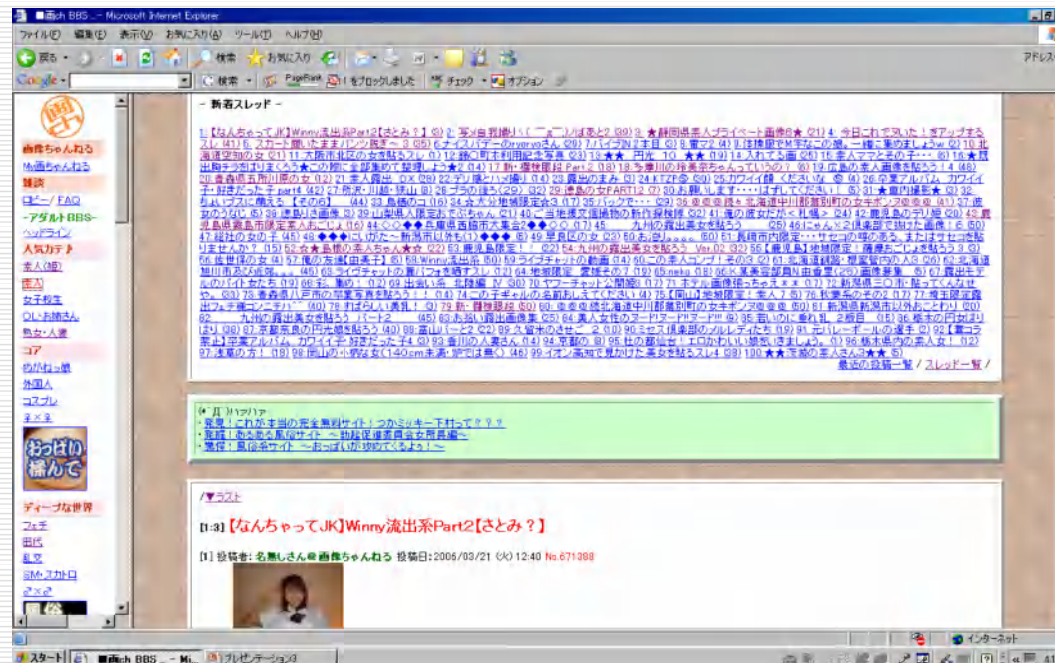
ネット大騒ぎ…元国税庁職員のハメ撮り写真流出
(ZAKZAK 2005/3/28)

記事引用:

決定的なのは、約150枚にもものぼるエロ&ハメ撮り写真。
焼き肉店のテーブルの下から彼女らしき女性のパンチラを狙ったショット
や、自宅での脱衣シーン、生挿入の一部始終から目隠しして手を縛って
SMエッチする姿が赤裸々に写し出される。もちろん、ノーカット。イケメン
ゆえか、少なくとも4人の女性とカラんでいた。

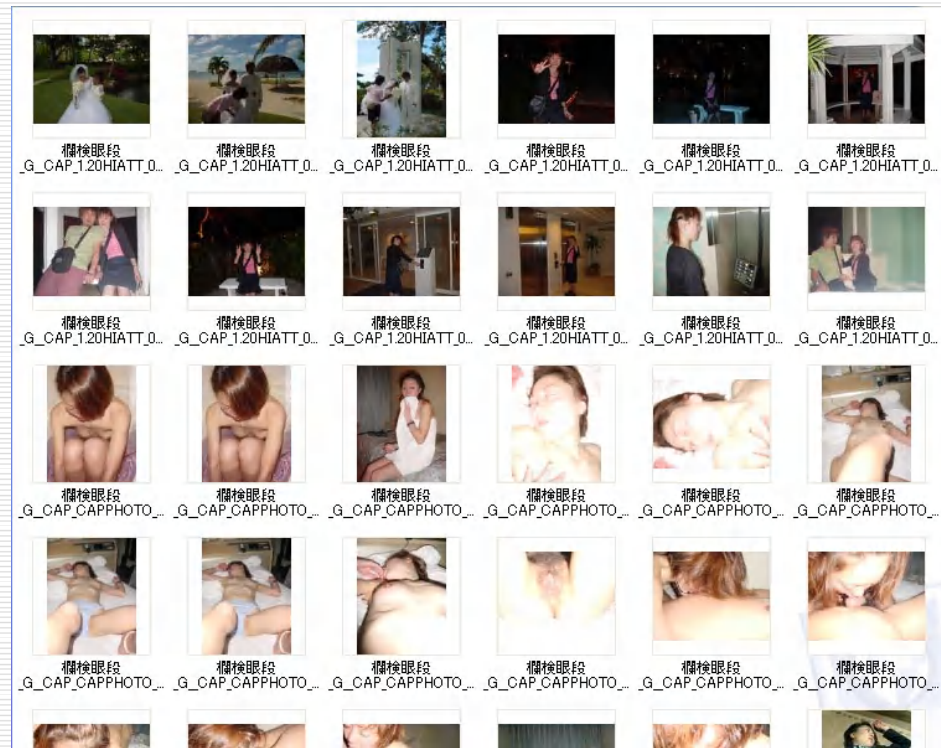
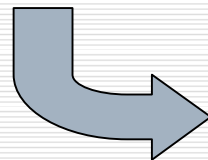
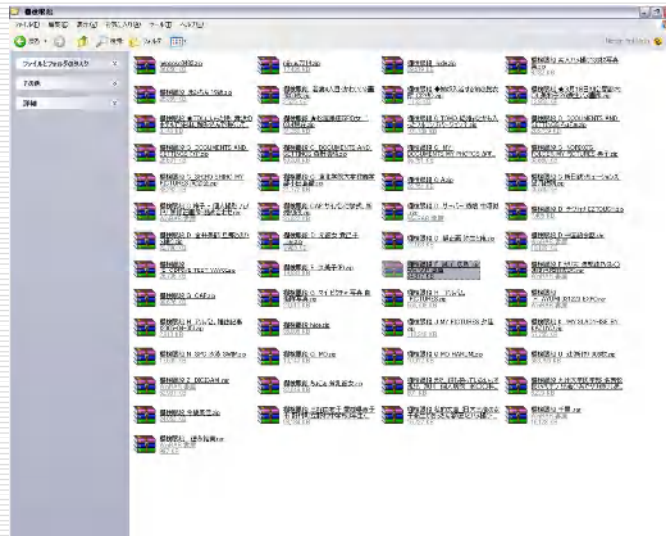
欄検眼段(リャンクーガンドウ)による流出事件

Winnyネットワークからインターネットへの拡大
 欄検眼段等による流出画像を集める画像掲示板



欄検眼段(リャンクーガンドウ)による流出事件

欄検眼段等により流出した画像



仁義なきキンタマによる流出事件

センセイのタマゴがハメ撮り大放出、四十七士の末裔

ZAKZAK 2006/01/06

(記事より抜粋)

8年にわたって衆院議員の秘書を務め、九州の県議選にも立候補した政治家のタマゴが、約500枚のハメ撮り写真などをネット上に大流出させていたことが分かった。

流出データの中には選挙事務所や街頭演説、選挙ポスター、名刺などが含まれ、年明け後に「センセイのハメ撮りが流出した」と、一部ネット上で話題となっていた。「さらに画像を詳しく解析したところ、同じデジカメでハメ撮りした女性とは別の女性とのデートを同時期に撮影していた。また県議選のデータの中には、事務所スタッフをダブルベッドに座らせて撮影したものがあつた」(ITライター)といい、2股どころか3股をかけていた可能性も浮上している。

仁義なきキンタマによる流出事件

2ちゃんねるニュース板でのお祭り～個人情報晒し

