

# コンピュータセキュリティ動向調査報告書

## 2006 年上半期版

～ 情報漏洩動向報告 情報漏洩は増加傾向にあり ～



提供：株式会社ラック  
コンピュータセキュリティ研究所  
V1.2

初版 2006/10/10

# 目次

1. はじめに	3
2. 対象期間	3
3. 本書中の登録商標、商標	3
4. 総評	4
5. 検出困難なマルウェアの脅威 (ADSL 回線編)	6
5-1 一般家庭のパソコンに感染したマルウェアのうち 62.5%は対処困難	6
5-2 公開サーバへの攻撃傾向はウェブアプリケーション関連が増加	8
5-3 不正アクセスにおける今後の動向考察	9
6. 2006 年上半期セキュリティトピックス	11
6-1. 巧妙化し続けるマルウェアとその動向	11
6-1-1 日本特有のマルウェアに混乱する日本のネットワーク	11
6-1-2 人為的ミスによる P2P の事件・事故は増加傾向にあり	12
6-1-3 ワンクリックウェアの出現	13
6-1-4 スパイウェアが埋め込まれた詐称サイト	14
6-2 ウェブブラウザの 0-day 攻撃の可能性	17
6-2-1 ウェブブラウザを狙った巧妙な攻撃の増加	17
6-2-2 IE 以外のブラウザも注意が必要	17
6-2-3 ウェブブラウザを巡る今後の動向考察	18
6-3 ウェブアプリケーションにおけるセキュリティの現状	19
6-3-1 セキュリティ診断結果によると 96%が問題あり	19
6-3-2 ウェブアプリケーション開発の問題	21
6-3-3 ウェブアプリケーションを巡る今後の動向	22

## 1. はじめに

2006 年上半期セキュリティレポート（以降、本書）は、株式会社ラック（以降、弊社）コンピュータセキュリティ研究所（以降、CSL）が 2006 年 1 月～6 月（以降、対象期間）におけるコンピュータセキュリティの動向についてまとめたものである。

調査対象は、コンピュータセキュリティ全般としており、国内において注目を集めた事象や、組織・個人に対して今後影響があると考えられるものを選択している。本書では詳細な対策案まで記載しないが、今後のコンピュータセキュリティ対策の方向性を考えるうえでご活用頂けたら幸いである。

## 2. 対象期間

上半期は、以下の期間とする。

2006 年 1 月 1 日～2006 年 6 月 17 日

## 3. 本書中の登録商標、商標

本書中のシステム、および製品名は、一般に日本国、米国およびその他の国の製品メーカー各社、その子会社の登録商標または商標である。

## 4. 総評

個人情報保護法が施行され、早くも 1 年以上が経過したが、個人情報漏洩事件の報告件数は増加の一途を辿っている。発生した情報漏洩の主因は、いずれにおいても、人による不適切な操作や設定によるものが多いようだが、これは決して情報漏洩事件に限ったことではなく、人の介在が原因となった事件や事故は近年のセキュリティ業界全般において発生していると言える。その中でも、特に、外部からの不正アクセスによって情報が漏洩したセキュリティ事件に関して、キーワードを挙げると以下の 2 つがある。

(1) マルウェア (コンピュータウイルスに代表される悪性プログラム)

(2) ウェブアプリケーションの脆弱性の悪用

特に (1) のマルウェアについては、Winny がインストールされたコンピュータに感染する Antinny ウイルスの被害が大きく、一般紙だけでなく国家をあげて取り上げられるなど、社会的現象にまで発展した。

また、「スパイウェア」や「ボット」による被害も増加していると考えられる。これらのマルウェアは、専用の開発ツールが登場したことによって種類が爆発的に増加しており、定義ファイル型のウイルス対策ソフトウェアでは徐々に検出が困難になってきている。さらに、マルウェアの一種であるスパイウェアを忍び込ませる方法についても、人間心理の弱点をつくような、より巧妙な手口のものが増加している。CSL の調査結果では、インターネット上にある弊社の観測ポイントを行き交う通信のうち、不正な通信が約 7 割も占めていることが判明しており、利用者が気づかないうちにマルウェアやボットに感染している事例が非常に多いということが分かる。

(2) のウェブアプリケーションの脆弱性の悪用とは、電子商取引を行うウェブサイトのプログラム上の欠陥を突かれることを意味しており、個人情報漏洩事件の発生も顕在化している。さらに、CSL で調査した結果によると、被害を受けたサイトの多くで、漏洩発覚の約半年～2 年前にはサーバに既に侵入されていたことが判明しており、これも特徴の一つであると考えられる。このように、侵入されてから被害が判明するまでに多くの時間がかかっている理由としては、以下の二点が考えられる。

- ・ ウェブサイトの最前面に設置されているウェブサーバにしか注意を向けていなかった
- ・ ウェブアプリケーションの脆弱性に対する攻撃を検知する仕組みが実装されていなかった

対象期間中におけるセキュリティ事件の国内動向から分かるのは、セキュリティ事故・事件による被害者の対象が組織から個人へ変化している点が挙げられる。ウェブアプリケーションの脆弱性を狙った攻撃は、一見すると企業サイトのみが被害者のように見えるが、漏洩した情報はユーザ個人のものであることに目を向けると、企業だけではなく個人にも被害が及んでいるといえる。この傾向は、フィッシング詐欺やスパイウェアの手口が巧妙になっていることなどから、今後も

増加するものと予測する。また、フィッシング詐欺やワンクリック詐欺を実現するソフトウェア（以降、ワンクリックウェアと呼ぶ）のようなユーザの心理的な弱点をつくものと、ウェブブラウザの 0-day 攻撃の双方を悪用するものが増加しており、より一層、防御することが困難になっていくものと推測される。このような状況において、ビジネス、及び組織内の資産に対するリスクを軽減するためには、ユーザ制御、アクセス制御、IT リテラシーの向上、クライアント管理、脆弱性管理および対策、さらには、通信制御などをバランスよく実施する必要がある。つまり、ネットワークを含むシステムだけでなく、間に介在する人も含めた、全体的なリスク緩和策が必要であるといえる。

## 5. 検出困難なマルウェアの脅威（ADSL 回線編）

CSL の調査では、公開サーバへの不正通信の件数に関する傾向については、昨年度と大きな変化はないと考えている。しかし、攻撃者による攻撃件数とその他の不正通信件数を比較すると、ウイルスやワーム、ボットなどのマルウェアによる通信が圧倒的に多いという特徴が見受けられる。

CSL の検証環境にて、1 日に捕獲したマルウェアの検体のうち、62.5%がウイルス対策ソフトウェアでは検出不可能であった。マルウェアの種類が急増している現状において、新しいアプローチによって検出することが可能なウイルス対策ソフトウェアでなければ、これらのマルウェアの検出および駆除は困難だといえる。このように、マルウェアの通信が多いといった傾向は、今後もしばらくは変わらないと考えられるが、Cross Platform Shellcode<sup>2</sup>を悪用したウイルスの登場や、モバイル機器の普及などを鑑みることで、感染の方法や標的が変化する可能性はある。

### 5-1 一般家庭のパソコンに感染したマルウェアのうち 62.5%は対処困難（2006 年 6 月）

インターネットを行き交う通信には、ウイルスやワーム、ボットなどによる不正なものが非常に多く含まれているが、不正通信が含まれる割合を実際を知ることで、セキュリティ設定が不十分なコンピュータに対するリスクを試算することができる。そこで、CSL では、非公開サーバにおける 1 日あたりの通信量に対して、どの程度の不正通信が含まれるのかを調査した。

#### ■調査環境

##### サーバ環境

OS：FreeBSD（仮想 OS 環境）

CPU：Pentium3

Memory：256Mbyte

##### ネットワーク環境

ADSL を利用

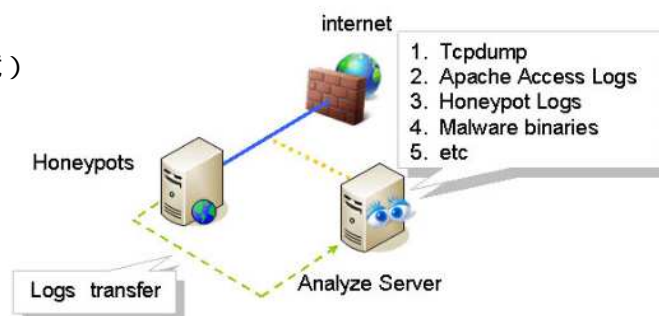


図 1 検証ネットワーク環境

<sup>2</sup> 異なる OS でシェルを起動させることが可能なコード

## ■調査結果

### (1) 通信量と不正通信の割合について

調査の結果、非公開サーバへの通信のうち、約 7 割（全 83507 パケット）で不正な通信の存在を確認した。一方、3 割程度となった正常なアクセスとしては、Googlebot<sup>3</sup>や NTP 等の通信であった。

図 2 に、1 日あたりに発生した不正通信の件数をポート別にまとめた。図 2 から分かるように、135/tcp、139/tcp、445/tcp を宛先ポートとする SMB<sup>4</sup>の通信が半数以上を占めており、さらに、それらの通信はマルウェアによるものであった。この結果は、IPA や JPCERT/CC 等で一般に公開されているインターネット定点観測の統計情報とほぼ一致する。このことは、IP アドレスが公開、非公開に関わらず、マルウェアに狙われ、知らず知らずに感染しているコンピュータが多数存在していることを意味する。

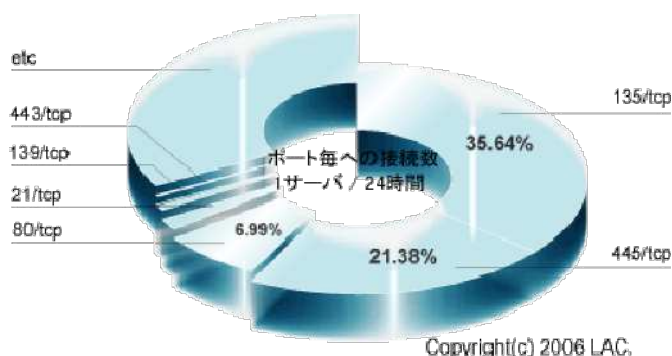


図 2 不正通信におけるポート別グラフ

### (2) マルウェアについて

これらのマルウェアに対し、ウイルス対策ソフトウェアをインストールした状態の一般コンシューマコンピュータがどの程度の耐久性を持つことができるかを調査した。調査の方法は、一般的に普及しているウイルス対策ソフトウェアによるマルウェア検出率について評価するものとした。

本調査中に取得した 24 種のマルウェアを、3 種類のウイルス対策ソフトウェアでスキャンした結果を図 3 に示す。図中の「Detected」は、1 種類のウイルス対策ソフトウェアでも検出できた割合を、「Undetected」は 3 種類全てのウイルス対策ソフトウェアが検出出来なかった割合を、それぞれ示している。

<sup>3</sup> ウェブからコンテンツを収集し、Google 検索エンジンのインデックスに登録しているプログラム。

<sup>4</sup> Windows 環境でネットワークを通じてファイル共有やプリンタ共有を実現するプロトコル。

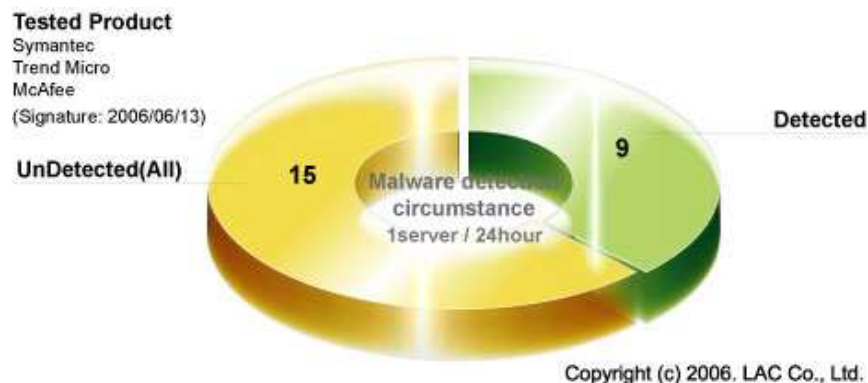


図3 マルウェア検出評価結果

調査の結果、検出可能であった検体は9体あり、残りの15体は検出することができなかった。検出できなかったであったマルウェアの多くは、ワームやボットに関連した rootkit やバックドアといったものであり、ワームやボットに感染後、対象のコンピュータにインストールされたものが殆どであった。このことから、一度ボットやワームに感染し、他のマルウェアをインストールされてしまうと、コンピュータを正常な状態に復旧することは非常に困難であることが分かる。

## 5-2 公開サーバへの攻撃傾向はウェブアプリケーション関連が増加

一般に公開されている統計情報<sup>5</sup>と弊社 JSOC（監視センター）の情報<sup>6</sup>を元に、公開サーバに対する不正アクセスの現状について考察する。

対象期間中におけるサーバへの不正アクセスについては、昨年、一昨年と同様にワームやボットによる 135/tcp、139/tcp、445/tcp 等の Microsoft Windows が利用するサービスポートへの通信が上位を占めている。これは、5-1 の調査結果とも一致している。また、公開サーバに対して注目すべき点は、マルウェア以外の攻撃として、22/tcp(ssh)や 21/tcp(ftp)へのブルートフォース攻撃<sup>7</sup>、RealVNC<sup>8</sup>への攻撃といった通信が多いことだ。いずれも、公開サーバにおいてメンテナンス作業時などで利用されるサービスであるが、不適切な設定によって運用している場合が多いため、標的とされていると考えられる。また、弊社 JSOC からの報告によると、ウェブアプリケーション

<sup>5</sup> <http://www.ipa.go.jp/security/ciadr/txt/list.html>、<http://www.cyberpolice.go.jp/detect/>

<sup>6</sup> [http://www.lac.co.jp/business/sns/intelligence/jsoc\\_report.html](http://www.lac.co.jp/business/sns/intelligence/jsoc_report.html)

<sup>7</sup> 暗号やログイン情報等のように一つの答えを解読するため、推測出来る全ての解答例を片っ端から試していく攻撃。非常に効率が悪い方法。

<sup>8</sup> ネットワークに繋がった他のコンピュータの画面を遠隔操作するソフトウェア。

ンを狙った攻撃が昨年より増加傾向にある。特に、PHP のプログラムの欠陥を狙ったワームも一般的に知られるようになり、セキュリティ機器の運用や、各サーバに対しての対応がますます難しくなってくる。

### 5-3 不正アクセスにおける今後の動向考察

昨今の不正アクセスに関する動向をみると、傾向が変化しているといえる。2004 年までは、OS やソフトウェアの脆弱性を悪用されて侵入を許してしまう傾向が強かったが、2005 年からは、ウェブアプリケーションのプログラム上の欠陥や、サーバの設定不備といったシステム管理者や運用者が管理する領域に対する攻撃が増加してきた。また、従来のような愉快犯や政治的な理由による攻撃に加え、電子マネーやリアルマネートレーディングなどの金銭を目的とした攻撃が増加している。それらを含め、近年どのような変化があったのかを、(1) 攻撃者、(2) 攻撃対象、(3) 攻撃ツールの 3 つの観点から考察してみる。

#### (1) 攻撃者の変化

弊社の緊急対応サービス（個人情報 119）や JSOC からの報告によると、2001 年～2004 年までは、愉快犯による不正アクセスが比較的多数を占めていた。しかし、日常生活に必要な様々な取引が電子化されたことで、犯罪行為も愉快犯から金銭を狙ったものに変化を遂げてきた。このような傾向は、今後も増加することは間違いないだろう。

#### (2) 攻撃対象の変化

インターネットで電子商取引を行っているサイトが狙われる傾向にある。これは、弊社の緊急対応サービス（個人情報 119）を提供した実際の事故（被害）のうち、電子商取引を行っているサイトでの被害の割合が増加したことからも裏付けられる。その背景には、電子マネーやモバイル機器が普及し、それに対応したサービスが広がっていることが関係していると考えられる。つまり、サービス提供側が間口を広げると、攻撃者もそこを狙ってくるといえる。

図 4 のように、フィッシング詐欺を行う犯人は、フィッシングサイトを構築するために、「企業等のサイトに侵入する行為」と、コンシューマを騙し「フィッシングサイトに誘導する行為」の両方を行う。サーバへの侵入とコンシューマへの受動的攻撃の両方を行うことで、売買する価値のある情報を入手している。

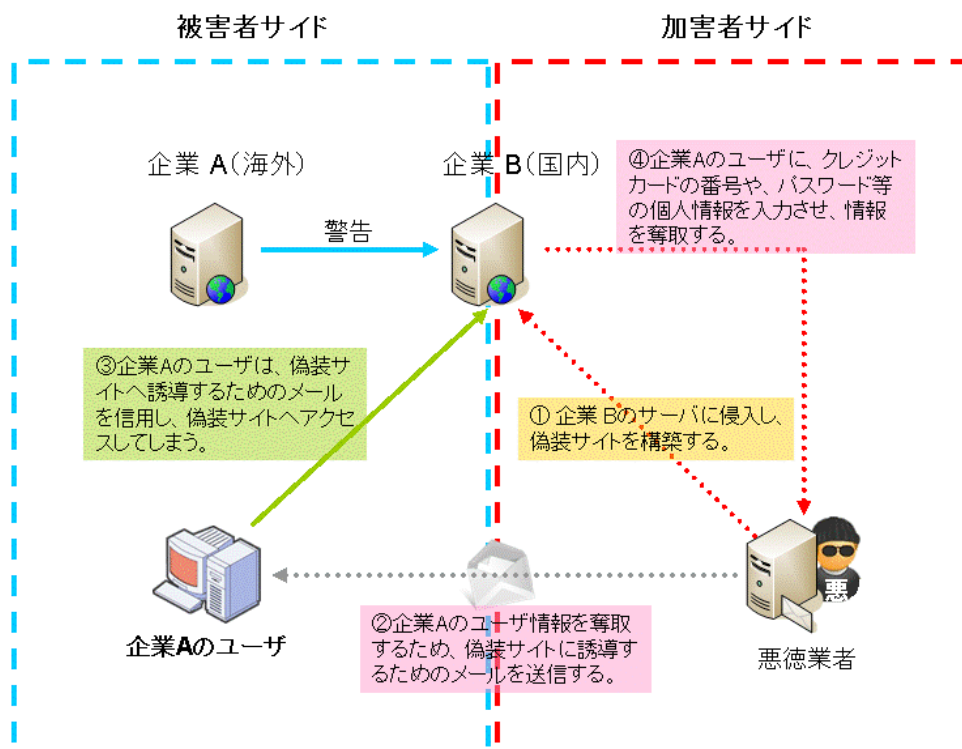


図4 フィッシング詐欺の加害者と被害者の関係

### (3) 攻撃ツールの変化

統合型の攻撃ツールが充実した機能を持つようになり、容易に第三者のコンピュータを攻撃することが可能になった。統合型攻撃ツールのひとつは、Exploit Scanner 等と呼ばれ、悪用したい脆弱性に対する攻撃が成功した後、実際に行いたい操作や動作を選択するだけで、標的コンピュータに侵入することが可能である。また、もうひとつの代表的なツールが、スパイウェア配布サイトの作成ツールキットのような、金銭目的で利用するツールの登場である。これらツールは、ウェブブラウザに対する攻撃ツールとして洗練されており、被害者側による対応が困難になるといえる。

これら3つの観点から、今後も攻撃はより一層巧妙化し、従来のセキュリティ製品では防御が困難になってくると考えられる。今までのような、攻撃元と攻撃先のための単純な関係だけではなく、より複雑な攻撃経路を介し、その通信経路上においても検出が困難になってくる。つまり、セキュリティ製品の機能や性能と現実の攻撃の間にある格差を、運用方法や人がどこまで埋められるかが重要になってくると言える。

## 6. 2006 年上半期セキュリティトピックス

### 6-1. 巧妙化し続けるマルウェアとその動向

Antinny ウイルス<sup>9</sup>をはじめとし、国産ウイルスが問題となっているが、これらのウイルスは、Winny ネットワークの特性や、地域性が意図的に考慮されており、Winny ユーザが油断して実行ファイルのクリックを許してしまうような工夫がなされていた。このような手法は、スパイウェアなどにも見られ、マルウェアを用いた犯罪手口は日々巧妙化しているようだ。

#### 6-1-1 日本特有のマルウェアに混乱する日本のネットワーク

Antinny、山田オルタナティブ<sup>10</sup>といった、海外ではあまり見られないマルウェアが日本国内に出現している。P2P ネットワークを介して感染するウイルスは決して新しいものではないが、感染後にコンピュータ上の情報を公開してしまう動作は特徴的なうえに、個人情報保護法施行直後といった日本固有の時期的な要因からも影響のあるマルウェアであったといえる。

特に、山田オルタナティブは、ウェブサーバプログラムとして動作し、感染したコンピュータ上の全ファイルをコンテンツとして公開する。さらに、感染したコンピュータの IP アドレスを特定の電子掲示板に書き込んでしまうため、たとえ ADSL ルータなどの配下にあり、インターネットからのアクセスを許可していなくとも、Universal Plug and Play(UPnP)<sup>12</sup>を利用することで外部からのウェブサーバアクセスを可能としてしまう。

これらのウイルスは、P2P ネットワークからダウンロードしたファイルを実行することによって感染する場合が多いが、電子掲示板からのダウンロード事例も報告されている。現在のところ、Antinny、山田オルタナティブは、愉快犯的な側面が強いと考えられている。

---

<sup>9</sup> Winny がインストールされているコンピュータに感染し、Winny ネットワークに感染したコンピュータのスクリーンショットや、デスクトップ上やマイコンピュータフォルダ内の個人情報をアーカイブし、流出させるウイルス。

<sup>10</sup> Winny がインストールされているコンピュータに感染し、感染したコンピュータの IP アドレスを 2ch 等の掲示板に書き込む。感染したコンピュータは、ウェブサーバが起動されてしまい、コンピュータの中身が閲覧やダウンロードが出来るようにされてしまう。

<sup>12</sup> パソコンや周辺機器、AV 機器、電話、家電製品等の機器をネットワークを通じて接続し、相互に機能を提供しあうためのプロトコル仕様。

## 6-1-2 人為的ミスによる P2P の事件・事故は増加傾向にあり

情報漏洩事件でさかんに取り上げられていた Winny や Share などの P2P ソフトウェアは、決して新しい技術を使ったものではなかった。しかし、無料で電子データがダウンロードできるという利便性から利用者が増大した。また、Winny および Share を利用することでコンピュータに潜入・感染を成功させたウイルスによって、大量に流出した個人情報に興味をもつことによって、さらに利用ニーズが増加した。

### (1) Winny を巡る動向

2006 年 1 月～6 月においては、Winny および Share からの情報漏洩事件が相次いで報告された。Winny を巡る動向について付録 1 にまとめた。

表 1 から分かるように、2006 年に入り、Winny を取り巻く環境は大きく変化したといえる。また、各セキュリティ製品ベンダから次々と対策ツールが公開された。しかし、いずれの対策案も製品単体では完全に防ぎきることが出来ず、未だに Antinny ウイルスに感染するユーザが後を絶たない。さらに、Winny のプログラム自体にも脆弱性が発見され、更なるマルウェアの散布が危惧された。

現在、Winny の通信自体を制御する傾向にあり、Winny を利用することが徐々に難しくなっている。しかし、Share のように Winny を参考に作成されるソフトウェアが登場するなど、今後も同様のソフトウェアが開発される可能性があり、別の通信経路を使うことで制御を回避することができる。なお、Share に関しては、暗号化された通信内容が既に解読されているが、Share の開発自体は継続されているため、さらなるバージョンアップによって回避される可能性が残っている。

### (2) P2P 技術における今後の動向考察

相次ぐ個人情報漏洩事件によって、P2P ソフトウェアの印象が悪いように感じるが、技術的には注目すべき点が多々あると考える。

海外では、P2P 技術を利用したビジネスや製品が普及しつつあり、日本に登場するのも時間の問題である。そういった意味では、P2P ソフトウェアは、これからが全盛といえるのかもしれない。しかしながら、ここで懸念されるのは、普及した場合に Winny と同様にセキュリティ事故が発生する可能性があるという点である。即ち、P2P ネットワーク用のマルウェアが大量に作成される可能性があるため、Antinny ウイルスと同様に、多くの感染者が出ることが推測される。P2P は、信用された者同士での利用が

考えられるため、比較的容易に利用者を油断させることができ、その結果、マルウェアを実行させることも、信用されているならばさほど困難ではないと考えられる。

### 6-1-3 ワンクリックウェアの出現

国内において、ワンクリックウェアと呼ばれるスパイウェアが確認され、流行しつつある。ワンクリックウェアはワンクリック詐欺に利用されるため、このように呼ばれている。ワンクリック詐欺は、アダルトサイトといった年齢制限を設けているウェブサイトで良く見られる詐欺手法である。この詐欺手法の手順は次の通りである。

- (1) 年齢制限を設けている Web ページを表示させる際にダイアログでこっそりと有料である旨を記載し、ユーザに同意させる
- (2) ユーザが同意すると、アニメーション GIF、Flash を表示し、あたかも個人情報を取得されたかのように錯覚させる
- (3) IP アドレス、プロバイダといった情報を表示させ、登録が完了したとし、ユーザに登録料を入金させる

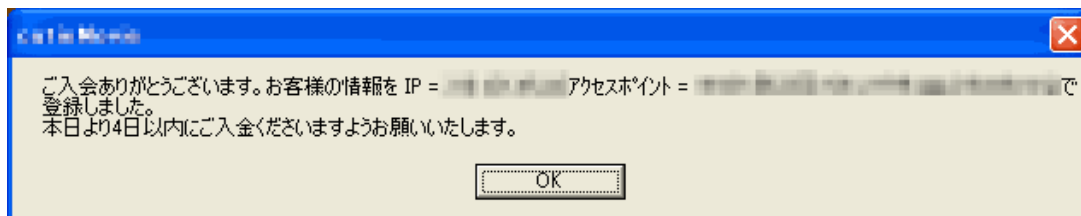


図5 ワンクリック詐欺

ワンクリックウェアは、手順の(1)の段階で簡単にインストールされてしまう。ワンクリックウェアは、アイコンが動画ファイルを想起させるようなものに偽装されており、容易に実行させるような工夫がなされている。インストール後は、定期的にポップアップで入金を促すメッセージを表示させる。

また、インストールさせるまでの動作や挙動は、海外のスパイウェアと類似している。しかし、スパイウェアのようにコンピュータ上の情報を外部に転送するのではなく、明示的に入金を促すことで心理的な動揺を誘い、金銭を得ようとする点が大きく異なる。

このような心理的な誘導は、電話での架空料金請求や、携帯電話メールなどで悪用された手法が応用されていると推測される。

心理面を狙った攻撃は、古典的な手法ではあるが、いつの時代でも効果的な方法といえる。そのため、ワンクリックウェアのようなマルウェアは、今後も増加傾向にあると推測される。こういった「罠」に引っかからないためには、URL フィルタリング等を導入することで、ユーザに注意を促したり、閲覧自体を抑制することが、有効な対策の一つといえる。

#### 6-1-4 スパイウェアが埋め込まれた詐欺サイト

特定サイトの詐欺や、悪質なコンテンツの無断借用等が増加している。スパイウェアの感染経路を考えた場合、フィッシング詐欺の流行や、昨年話題になった代表的な著名サイトのコンテンツへの混入等を踏まえて推測すると、最も感染率が高いと推測されるのが「日常的に利用されているサイト」であることが分かる。代表的なサイトとしては、総合的な情報を提供するポータルサイトなどが挙げられるが、特に、アクセスの多いサイトでは、詐欺サイトが確認されており、フィッシング詐欺やスパイウェアの散布等に悪用されていることは周知の事実であろう。

これら詐欺サイトにおいて、マルウェアを散布しているサイトの統計について、某ポータルサイトにおける詐欺サイトを巡回し、スパイウェアが混入されているサイトの数を調査した結果を図 6 に示す。

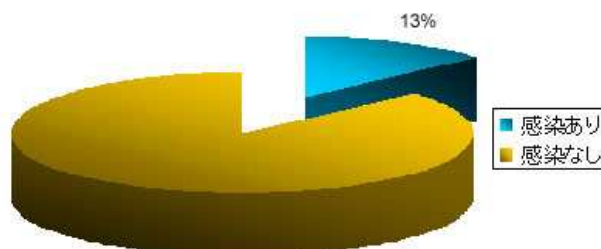


図 6 某ポータルサイトのスパイウェア混入傾向

さらに、スパイウェアに感染した際の経路について調査した結果、全てポップアップ広告であることが判明した。最近のウェブブラウザが備えるポップアップ制御機能は、スパイウェア対策として有効に機能しているといえる。

#### 6-1-5 マルウェアを巡る今後の動向考察

ボットやワームは、能動的に動作する上、感染速度が速い。したがって、感染したコンピュータを内部ネットワークに持ち込むことで感染が拡大することが多く、企業にとっては非常に影響度の大きいマルウェアだといえる。これに対し、スパイウェアなどの受動的に動作するマルウェアは、悪意のあるサイト等に誘導するためにワンクリックが必要となるため、影響度が見えにくい。しかしながら、現在のところはボットほどの影響度ではないと考える。

近年、OS やシステム側のセキュリティ対策も進み、ボットやワームによる感染が困難な環境になってきていると言われているが、ボットやワームに感染しているコンピュータは依然多いと考えられる。この傾向は、OS やハードウェア自体が、ファイアウォール機能やマルウェア検出などのセキュリティ機能を備えるようになるまで続くのではないだろうか。

また、受動的な動作をするマルウェアに関しては、ランサムウェア<sup>13</sup>にしばしば見られるように、ユーザを脅すことでスパイウェア対策ソフトウェアを装い、マルウェアをインストールするよう誘導するものや、ウイルス対策ソフトウェアを装ったスパイウェアのように、ユーザを安心させてインストールさせようとするものが主流になりつつある。こういった、ユーザを誘導する行為は、国や地域の文化に依存する手法が多いため、日本国内においても同様のマルウェアが作成される可能性があるのではないだろうか。また、ボットとスパイウェアに共通する点は、いずれも金銭目的で作成されているということである。そのため、これらのマルウェアは常に進化し、より巧妙になっていくと考える。

---

<sup>13</sup> 知らず知らずのうちにインストールされ、ソフトウェア等売りつけるマルウェア。

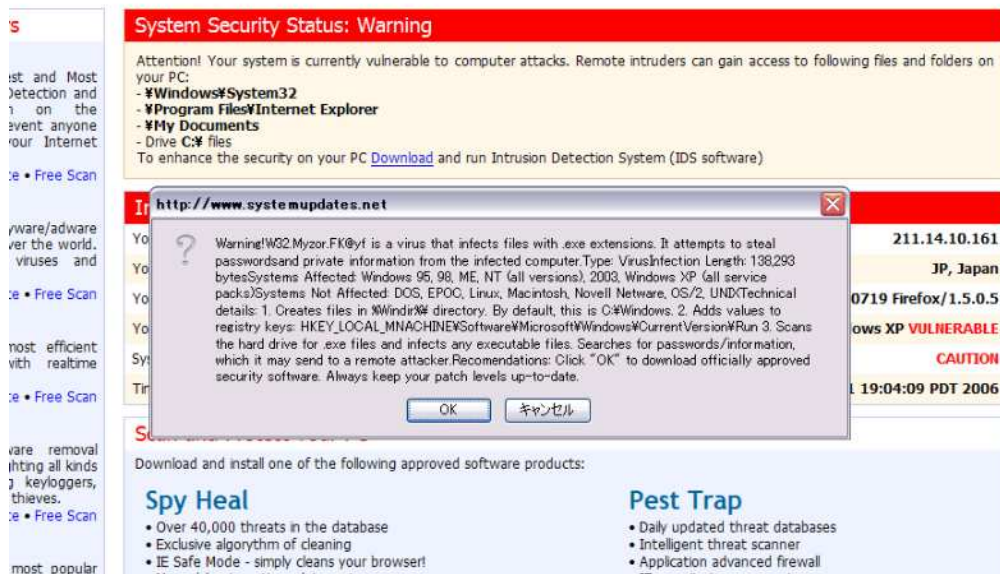


図 7 ランサムウェアの事例

## 6-2 ウェブブラウザの 0-day 攻撃の可能性

情報漏洩の原因の一つとして、ウェブブラウザにおいて脆弱性を悪用される可能性がある。これらの脆弱性は、メールなどで悪意のあるサイトに誘導することで悪用されることが多い。その代表例として挙げられるのがスパイウェアである。標的とされる代表的なウェブブラウザとして、Microsoft 社 Internet Explorer (以下、IE) や Firefox、Opera、Safari などがある

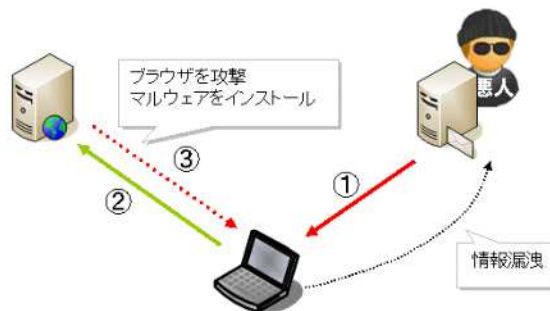


図 8 ブラウザの脆弱性の悪用例

### 6-2-1 ウェブブラウザを狙った巧妙な攻撃の増加

2005/06 ~ 2006/05 の間で IE に発見された脆弱性を表 1 にまとめた。(付録 1 参照) 表 1 において注目すべき点は、修正パッチが提供される前に攻撃手法が公開された脆弱性があるということである。

また、表 2 (付録 2 参照) から分かるように、依然として修正パッチが提供されていない脆弱性も存在する。脆弱性自体は外部から直接任意のコードを実行できるわけではないため、受動的攻撃によりユーザのコンピュータを不正操作することになる。例えば、ニセモノのホームページやメール本文に誘導先のリンクを張っておくことで、悪意のあるサイトへ訪問させる。そして、リンク先のホームページにおいて、IE の脆弱性を悪用し、スパイウェアなどのマルウェアをインストールする。

### 6-2-2 IE 以外のブラウザも注意が必要

IE の脆弱性に関しては 6-2-1 に述べた通りである。他のブラウザの状況について、Firefox を例にとって述べる。

Firefox は、Mozilla Foundation によって開発されているブラウザであり、IE とは異

なるレンダリングエンジン<sup>14</sup>が採用されている。このため、IE で発見された脆弱性の影響を受けることはない。しかし、Firefox においても脆弱性は多々あり、それらを表 3 にまとめた(付録 3 参照)。

Firefox においても 0-day ツールは存在し、スパイウェアサイト作成ツールキットに含まれている。攻撃ツールの有無で危険度を判定するのであれば、どちらも同じと言える。

### 6-2-3 ウェブブラウザを巡る今後の動向考察

最近の傾向として、ウェブブラウザ単体でセキュリティの強化が図られてきており、特に 2006 年現在でも大半のシェアを占める Microsoft 社の IE7 では、大幅なセキュリティ強化を図られようとしている。

IE 7 に関して、公開されている技術資料からセキュリティ面に関連する機能は以下の通りである。(一部を抜粋)

- ・ ActiveX オプトイン(マルウェア対策)
- ・ クロスドメインスクリプト対策(XSS 対策)
- ・ Windows Defender との連携(マルウェア対策)
- ・ フィッシング詐欺検出機能(フィッシング対策)
- ・ Web 閲覧履歴、キャッシュなどの簡単削除機能(個人情報の保護)

「技術概要：Microsoft Windows Internet Explorer 7」より

<http://www.microsoft.com/japan/windows/ie/ie7/technology/default.msp>

これらの機能を見ると、マルウェア、フィッシング詐欺、個人情報の漏洩など一通りの対策が施されていると考えられる。しかし、IE7 に実装されるマルウェアやフィッシング対策機能は基本的にブラックリスト方式であるため、検出に限界があり、併せて別の対策も実施することが望ましい。

---

<sup>14</sup> 一般的に、文字コードで指定されたデータを、画像や映像、レイアウトされた文章に変換するソフトのことを指す。

### 6-3 ウェブアプリケーションにおけるセキュリティの現状

昨年から、ウェブアプリケーションの脆弱性が原因となったセキュリティ事件が多発している。安全性を重視するシステム管理者やセキュリティ担当者と、利便性を重視するウェブアプリケーション開発者との意識に格差があるためと考える。

#### 6-3-1 セキュリティ診断結果によると 96%が問題あり

昨年、商用サイトの個人情報漏洩事件をきっかけに、「SQL インジェクション」が話題になり、ウェブアプリケーションの安全な実装がより一層求められるようになった。その理由のひとつとして、ウェブアプリケーションは、ウェブサーバとその背後にあるデータベースサーバとの連携を担っている場合が多いという点が挙げられる。ウェブアプリケーションに脆弱性があると、それを悪用することで重要情報が保存されている可能性の高いデータベースサーバに直接アクセスし、個人情報などを奪取することができてしまう。このような攻撃を受けた場合、サイト運用者はウェブサーバ単体に注視してしまい、データベースサーバの異変に気付かないことが多い。その結果、最も価値の高いデータベースサーバの被害に気付くまでに時間を要してしまうといった問題がある。

2006年1月～6月の間で実施した弊社脆弱性診断サービスの結果から、約75サイトをサンプリングし、分析した結果を図9、図10に示す。

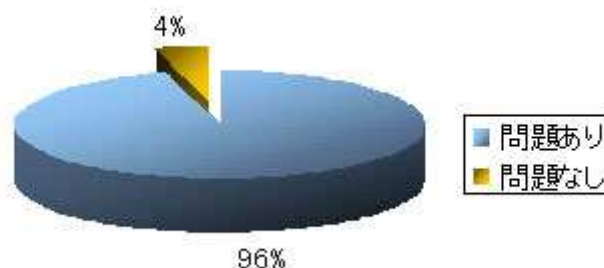


図9 ウェブアプリケーション脆弱性診断による問題の有無

図9の結果によると、全体の約96%のサイトがウェブアプリケーションに問題を抱えていることが分かる。あくまでサンプリング数値ではあるが、殆どの商用サイトがウェブアプリケーションに何らかの問題を抱えていることになる。過去の傾向と今回の結果を比較してみても、余り変化していないことがさらに分かった。それだけウェブアプリケーションに対する脆弱性対策の進行度合いは低いといえるが、これは非常に大きな問題と考える。

図 9 で示したウェブアプリケーションに問題を抱えるサイトについて、その問題の内訳を図 10 に示す。

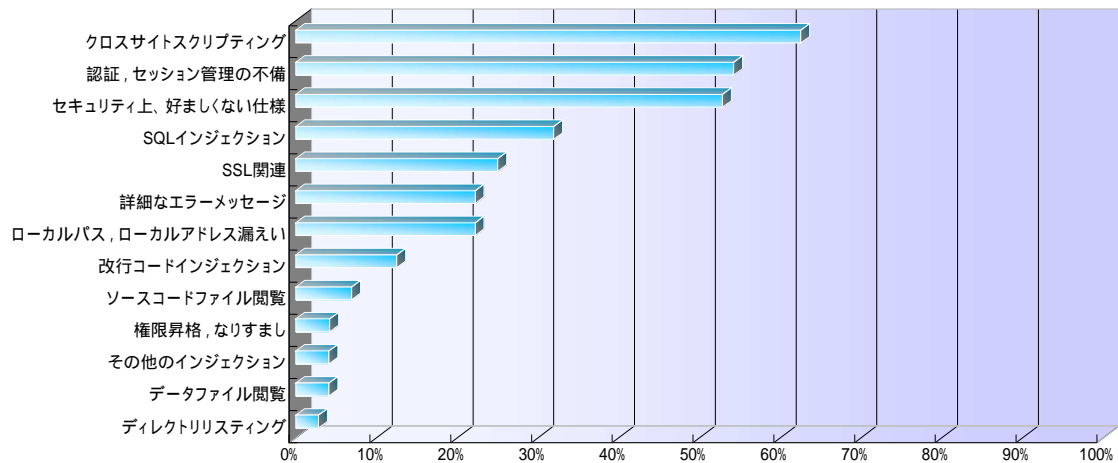


図 10 検出されたウェブアプリケーションの問題

半数以上のサイトにおいて、「クロスサイトスクリプティング」、「認証、セッション管理の不備」、「セキュリティ上、好ましくない仕様」といった問題点が見つかることが図 10 から分かる。

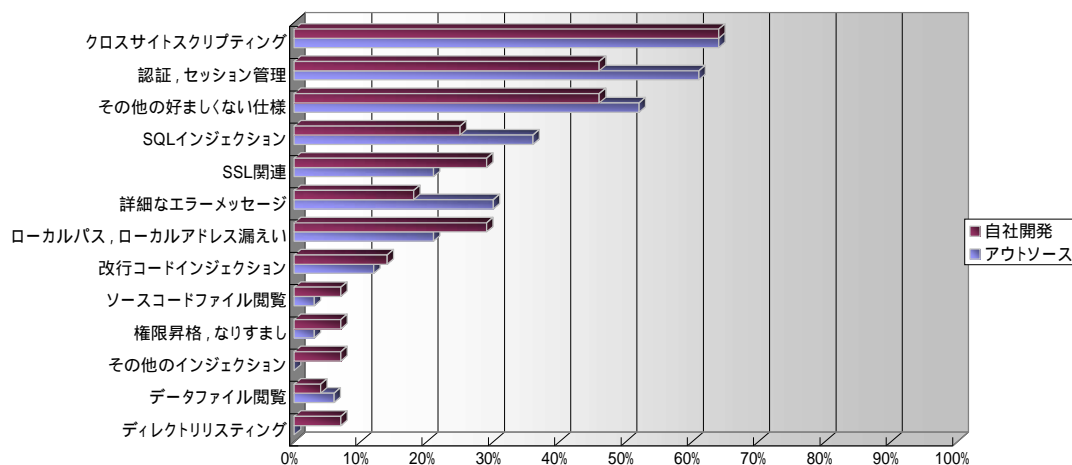
さらに、これらの問題点を持つウェブアプリケーションでは、複数の問題も併せて抱えていることが多い。

また、少数ではあるが、「データファイル閲覧」、「ディレクトリリスティング」など、本来ユーザが閲覧できない情報が閲覧できてしまう問題を抱えるサイトも確認されている。これらの脆弱性は、リモートから権限が奪取されるような致命的な脆弱性ではないため比較的軽視されてしまう傾向にあるが、クロスサイトスクリプティングなどはフィッシングサイトにも悪用されている脆弱性であり、5-3でも説明したような問題が出てくるため注意が必要である。

### 6-3-2 ウェブアプリケーション開発の問題

ウェブアプリケーションの開発は、全ての組織において同一の方針で行われているわけではない。例えば、組織内で開発を行う部署が無い場合は開発をアウトソースすることもあるだろう。本項では、環境が異なる場合のウェブアプリケーションの品質に関して、どのような違いが出ているのかを考察する。

図 12 は、弊社で提供中のホームページ情報漏えい診断サービスの統計結果から、自社開発を行った場合とアウトソースした場合について、脆弱性が含まれる割合を調査したものである。



この結果によると、クロスサイトスクリプティングに関しては、自社開発とアウトソースの両方において、高い数値となっていることから、対策についてあまり考慮されていないことが分かる。さらに、クロスサイトスクリプティングの脆弱性が存在するアプリケーションのうち、約 70% が SQL インジェクションの脆弱性を併せ持っていた。

さらに図 13 は、業界別にクロスサイトスクリプティングと SQL インジェクションの統計を示したものである。この結果によると、業界とは関係なくクロスサイトスクリプティングの脆弱性が多く存在していることが分かる。

一方、ここで注目すべき点は、SQL インジェクションの有無である。SQL インジェクションはサービス業や金融業に多く、さらにクロスサイトスクリプティングを併せ持っていることが多い。

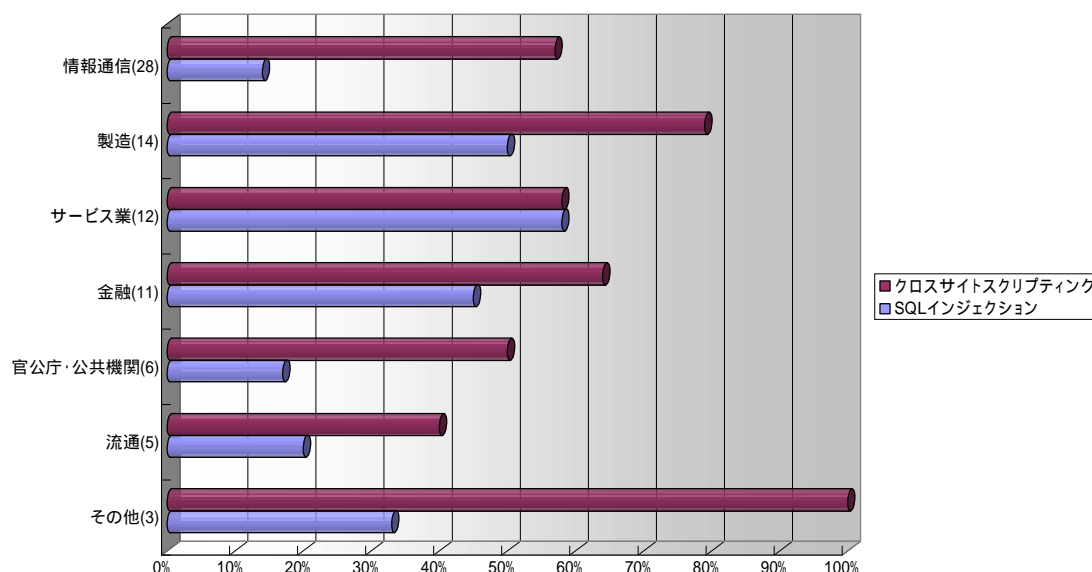


図 13 業界別統計

### 6-3-3 ウェブアプリケーションを巡る今後の動向

今後のウェブアプリケーションを取巻く環境を考えた場合、しばらくの間はウェブアプリケーションのプログラム上の欠陥を悪用した攻撃が続くと推測する。

私たちの日常生活は、コンピュータやモバイル機器、携帯電話の小型高性能化、複数のアクセス手段の普及等の進歩により、徐々にオンライン化している。これらの機器がネットワークに接続する先には、多くの場合でウェブアプリケーションが存在する。それだけ、世の中にはウェブアプリケーションが溢れており、今後も増加する傾向にある。

次に、ウェブアプリケーションを狙った攻撃の傾向が今後どうなるのか考察してみると、弊社JSOCではSQLインジェクション攻撃が依然として増加傾向にあることや、インターネット上に新たなSQLインジェクション攻撃ツールが公開され続けていることから、今後も攻撃が減少する可能性は低いと考える。

また、クロスサイトスクリプティングのような受動的攻撃に悪用される脆弱性も増加傾向にある。これらの脆弱性は、ウェブサイトとサイトのユーザ双方に対して仕掛けることで攻撃(犯罪)が成立するため、影響度を正確に把握することは困難である。しかしながら、主にフィッシングサイトをはじめとするような金銭目的のサイトにユーザを誘導するためにウェブアプリケーションの脆弱性が悪用され続けるとしたら、これらの悪意あるサイトの増加に比例して、ウェブアプリケーションの脆弱性への攻

撃はさらに増加する可能性がある。

最近では、スパイウェアサイト作成ツールキットやフィッシングサイト作成ツールキットが存在し、自動で悪意のあるサイトを作成することが可能であるため、急速に悪意のあるウェブサイトが増加することが懸念される。

以上

## 付録1 Winny 対策動向

日付	内容
2004/2/17	NetAgent 社から Winny 通信を遮断できる One Point Wall がリリース。
2004/12/22	Whizzy R&D 社から Winny ネットワークに偽造ファイルをばらまく「コンテンツシェルタ」がリリース。
2005/10/06	ASCII 出版社より「Winny の技術」が出版。
2005/10/12	MS 社より、「悪意のあるソフトウェアの削除ツール」が Antinny に対応。
2005/12/05	NTT コミュニケーション社の「OCN PC パトロール」が Winny の検出機能を実装。
2005/12/26	ネットエージェント社が「Winny 調査サービス」を開始。
2006/02/07	Fortinet 社から Winny に対応した新ファームウェア FortiGate の FortiOS3.0 がリリース。
2006/02/16	ISS 社から Winny を検知するシグネチャがリリース。
2006/03/02	トレンドマイクロ社が「ウイルスバスター コーポレートエディション」で Winny 対策ツールを同梱。
2006/03/02	高木氏のブログで「Winny の Down フォルダをインターネットゾーンにする」が提案される。
2006/03/11	アンラボ社から「ウィニーウイルス」専用ワクチンがリリース。
2006/03/15	安倍官房長官が Winny を介した情報漏えいについて記者発表で言及。
2006/03/15	ネットエージェント社から Antinny 感染履歴調査ツールをリリース。
2006/03/16	ぶららネットワークス社が Winny 通信の完全規制を発表。
2006/03/16	アップデートテクノロジー社からウィニーSTOPパーがリリース。
2006/03/17	アークン社の AntiMalware が Winny の検知に対応。
2006/03/18	アットマーク IT で「グループ・ポリシーで Winny の実行を禁止する」が提案される。
2006/03/22	ウェブセンス社が Winny の起動を停止する Websense Web Security Suite Lockdown Edition をリリース。
2006/03/23	Symantec 社 から Winny 検索ツールがリリース。
2006/03/24	IPA が Winny 緊急相談窓口を設置。
2006/03/24	Symantec 社 から Antinny 駆除ツールがリリース。
2006/03/27	「カスペルスキー アンチウイルス 5」において、Winny がリスクウェアとして検知。
2006/04/11	住商情報システムズ社を通じて、eEye 社から Winny Scanner、Winny Monitor がリリース。
2006/04/12	McAfee 社から Winny を検知するシグネチャがリリース。
2006/04/12	eEye 社 鶴飼氏による Winny 通信の解読方法が公開される。
2006/04/21	ニフティ社がファイル交換ソフトの通信速度を制限することを発表。4/28 から適用。
2006/04/21	eEye 社 から Winny の脆弱性についてのアドバイザリがリリース。
2006/05/2	「止めるぞ！情報漏えいセミナー」が開催された。
2006/05/15	この講演において、金子氏より情報漏えい対策として Upfolder.txt の監視が提案された。
2006/05/17	カーネギーメロン大学日本校オープンカンファレンス - 匿名 P2P ネットワークにおける情報漏洩対策を考える - が開催された。
2006/05/16	hi-ho 社が大量のデータ通信に対して通信利用規制することを発表。6/30 から適用。
2006/05/18	ぶららネットワークス社が総務省の指示により、Winny 通信の完全規制について再検討。
	Juniper 社の IDP で Winny 検知に対応。
2006/06/01	YAMAHA 社より、ヤマハルーター「Winny フィルタ機能」搭載した β ファームがリリース。
2006/06/06	Cisco 社が Cisco IDS/IPS で Winny Activity シグネチャが追加。

## 付録2 Internet Explorer の脆弱性一覧 (2006年6月現在)

発見年月日	パッチ	パッチリリース日	セキュリティホール名称
2006/4/27	-	-	Microsoft Internet Explorer Improper mhtml URL Redirection Information Disclosure Vulnerability
2006/4/22	MS06-021	2006/6/14	Microsoft Internet Explorer OBJECT Tag Handling Memory Corruption Vulnerability
2006/4/11	MS06-013	2006/4/11	Microsoft Internet Explorer Improper HTML Parsing Memory Corruption Vulnerability
2006/4/11	MS06-013	2006/4/11	Microsoft Internet Explorer Multiple Memory Corruption Vulnerabilities
2006/4/11	MS06-013	2006/4/11	Microsoft Internet Explorer Memory Corruptions and Improper HTA Execution Vulnerabilities
2006/4/11	MS06-013	2006/4/11	Microsoft Internet Explorer Erroneous IOleClientSite Data Security Restriction Bypass Vulnerability
2006/4/11	MS06-013	2006/4/11	Microsoft Internet Explorer Incorrect Domain Identification Information Disclosure Vulnerability
2006/4/11	MS06-013	2006/4/11	Microsoft Internet Explorer Unspecified Address Bar Spoofing Vulnerability
2006/4/4	MS06-021	2006/6/14	Microsoft Internet Explorer Improper swf File Handling Address Bar Spoofing Vulnerability
2006/3/22	MS06-013	2006/4/11	Microsoft Internet Explorer HTML Objects Handle Unexpected Method Calls Memory Corruption Vulnerability
2006/1/26	MS05-054	2005/12/13	Microsoft Internet Explorer ActiveX Kill Bit Check Bypass Vulnerability
2006/1/7	MS06-004	2006/2/14	Microsoft Internet Explorer WMF File Rendering Memory Corruption Vulnerability
2005/12/13	MS05-054	2005/12/13	Microsoft Internet Explorer Arbitrary Code Execution and Information Disclosure Multiple Vulnerabilities
2005/11/30	MS06-021	2006/6/14	Microsoft Internet Explorer CSS Import Information Disclosure Vulnerability
2005/11/6	-	-	Microsoft Internet Explorer Improper Status Bar Display Spoofing Vulnerability
2005/10/11	MS05-044	2005/10/12	Microsoft Windows FTP Client Improper Filename Validation Vulnerability
2005/8/9	MS05-038	2005/8/9	Microsoft Internet Explorer COM Objects Memory Corruption Vulnerability
2005/8/9	MS05-038	2005/8/9	Microsoft Internet Explorer Web Folder Behaviors Cross-Domain Scripting Vulnerability
2005/7/17	MS05-038	2005/8/9	Microsoft Internet Explorer Malformed JPEG Image Parsing Denial of Service Vulnerability
2005/6/29	MS05-037	2005/7/13	Microsoft Internet Explorer javaprxy.dll Handling COM Object Heap Overflow Vulnerability
2005/6/21	-	-	Multiple Web Browsers Dialog Box Spoofing Vulnerability
2005/6/14	MS05-025	2005/6/14	Microsoft Internet Explorer pngfilt.dll PNG Rendering Buffer Overflow Vulnerability

付録3 対象期間中の Firefox の脆弱性一覧

発見年月日	Fixed	Fix 版リリース日	セキュリティホール名称
2006/4/24	1.5.0.3	2006/5/2	Mozilla Firefox designMode Deleted Object Reference Vulnerability
2006/4/13	1.0.8	2006/4/13	Mozilla Firefox Improper Popup Window Handling Secure Site Spoofing Vulnerability
2006/4/11	1.0.8 1.5.0.2	2006/4/13	Mozilla Firefox prior to 1.5.0.2 Memory Corruption and Security Bypass Vulnerabilities
2006/4/11	1.0.8 1.5.0.2	2006/4/13	Mozilla Firefox prior to 1.0.8/1.5.0.2 Multiple Vulnerabilities
2006/4/11	1.0.8	2006/4/13	Mozilla Firefox prior to 1.0.8 Memory Corruption and Privileged JavaScript Execution Vulnerabilities
2006/4/11	1.0.8	2006/4/13	Mozilla Firefox prior to 1.0.8 Multiple Cross-Site Scripting Vulnerabilities
2006/4/11	1.0.8 1.5.0.2	2006/4/13	Mozilla Firefox Changing Input Type Arbitrary File Steal Vulnerability
2006/4/11	1.5.0.2	2006/4/13	Mozilla Firefox Faster History Mechanism XUL Content Windows Spoofing Vulnerability
2006/4/11	1.0.8	2006/4/13	Mozilla Firefox Improper Image Context Menu Save Executable File as Image Vulnerability
2006/2/2	1.0.8 1.5.0.1	2006/4/13 2006/2/1	Mozilla Products Memory Corruption and JavaScript Injection Vulnerabilities
2006/2/2	1.5.0.1	2006/2/1	Mozilla Firefox/Thunderbird 1.5 Memory Corruption and Security Restriction Bypass Vulnerabilities
2006/1/19	-	-	Mozilla Firefox -moz-binding Property Cross-Domain Scripting Vulnerability