IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2007 年 6 月 4 日
独立行政法人 情報処理推進機構

コンピュータウイルス・不正アクセスの届出状況［2007 年 5 月分］について

独立行政法人 情報処理推進機構（略称：IPA、理事長：藤原 武平太）は、2007 年 5 月のコンピュータウイルス・不正アクセスの届出状況をまとめました。

1．今月の呼びかけ

今月の呼びかけ：
「そのアプリケーションソフトには、セキュリティホールはありませんか？」
― セキュリティホール対策は、オペレーティングシステム(OS)だけではない！ ―

(1)アプリケーションソフトのセキュリティホールの現状

現在、一般で広く利用されているアプリケーションソフトの中には、セキュリティホール(セキュリティ上の弱点)(*1)が報告されているものが少なからず存在しています。また、悪意のある人がインターネットに接続されているコンピュータ上のアプリケーションソフト等にセキュリティホールが無いか、いろいろな手口で日々探しまわっています。

当機構への 4 月、5 月のウイルス・不正アクセスの届出の中でも、コンピュータを管理するアプリケーションソフトで発見されたセキュリティホールから侵入されて被害を受けたとの届出が目立ちました。

(2)アプリケーションソフトに潜むセキュリティホール

アプリケーションソフトとは、ワープロソフト、表計算ソフト、プレゼンテーションソフト、メールソフト、音楽や動画等を録画・再生するソフト、PDF ファイルを作成・表示するソフト等をいいます。これらのソフトは毎日のように利用されており、仕事や生活に必要不可欠なものとなっています。

このため、オペレーティングシステム(OS)だけでなく、パソコンに入っていてもこれまでほとんど利用していなかったものを含め、アプリケーションソフトにもセキュリティホール対策が必要であることを認識してください。日頃からアプリケーションソフトのセキュリティホール情報の有無を確認するなどして、セキュリティホール情報が発見された場合には、パッチ(修正プログラム)を当てるなどして、早急にセキュリティホールの解消を行う必要があります。

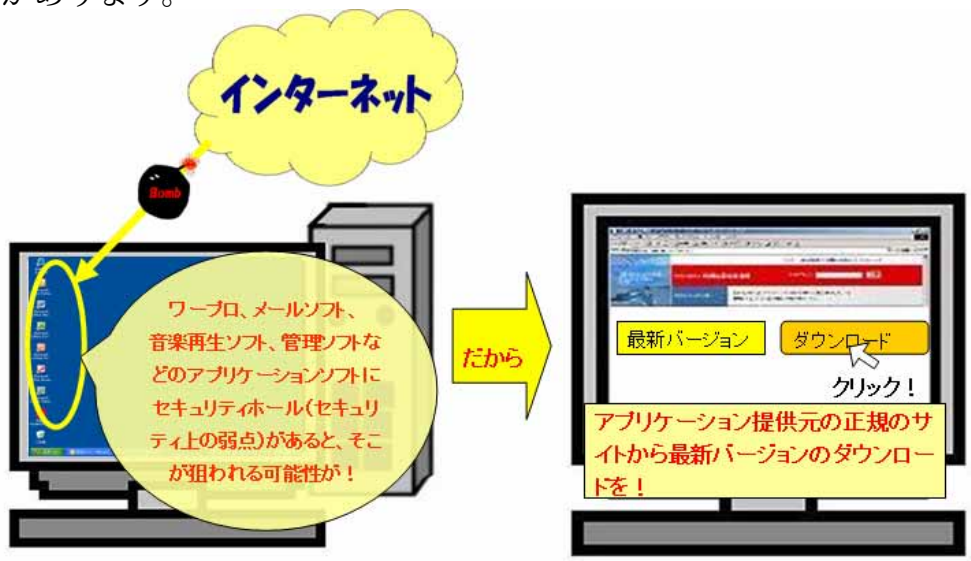


図 1：アプリケーションソフトの対策

(3)アプリケーションソフトのセキュリティホールにより想定される被害

当機構では経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」に基づき、アプリケーションソフト等のセキュリティホール関連情報の届出を受け付けており、四半期ごとに届出状況の報告を行っております。

その状況報告の 2007 年第 1 四半期(1 月～3 月)の報告によると、アプリケーションソフトのセキュリティホールを発見して届出を受け付けた件数は 36 件(2004 年 7 月からの累計件数 455 件)あります。その届出状況では、アプリケーションソフトにセキュリティホールがある場合にどのような被害が想定されるかをまとめており、主な想定される被害は以下のとおりとなっています。

- 任意のスクリプト(侵入者の意図する操作手続き)の実行
- 任意のコード(攻撃用プログラム)の実行
- 情報漏えい
- ID、パスワードの漏えい
- なりすまし
- サービス不能　　等

これらの被害を実際に受けた場合は、金銭的な損失や業務への影響等の被害だけでなく、「なりすまし」などによりいつの間にか、加害者となってしまうこともあります。

(4)アプリケーションソフトのセキュリティホール対策

上記(3)の様な被害に遭わないためには、セキュリティホールを解消する必要があります。そのためには、アプリケーションソフトのバージョン管理が重要になります。そこで以下の対策を行うことが必要となります。

a. アプリケーションソフトの入手は、必ず信頼できるところから正規のものを入手してください。アプリケーションソフトのバージョン情報は、アプリケーションソフトのヘルプで確認することが出来ます。

b. アプリケーションソフトを利用している間は、その提供元のアプリケーションソフトのバージョン更新履歴を定期的にチェックしてください。新しいバージョン情報が報告されている場合は、自分で新しいバージョンを入手して、安全に利用できる状態にしてください。

c. アプリケーションソフトの中には、新しいバージョンが出ると自動的に通知、更新をしてくれるものがあります。これを利用することにより、常に確実で安全に利用できる状態を保つことができます。特に最近のアプリケーションソフトには、自動更新機能が搭載されているものが増えてきています。

(5)アプリケーションソフトのセキュリティホール情報の収集

経済産業省では、アプリケーションソフト等のセキュリティホール関連情報流通の枠組みとして、官民連携による「情報セキュリティ早期警戒パートナーシップ」（以下、「枠組み」という）を構築しています。具体的な取り組みは以下のとおりです。この取り組みを活用してアプリケーションソフトのセキュリティホール情報の収集をすることができます。

a. IPA と有限責任中間法人 JPCERT コーディネーションセンター(JPCERT/CC)は、上述の枠組みに基づき、日本国内の製品開発者のセキュリティホール対応状況を公開するサ

イトとして、2004 年 7 月から JVN(Japan Vulnerability Notes)を共同で運営しています。
JVN では、この枠組みにより届け出られたアプリケーションソフト等のセキュリティホール情報を公開しています。これらのセキュリティホール情報には、JVN に登録している日本国内の製品開発者の対応状況も含まれております。対応状況には、セキュリティホールに該当する製品の有無、回避策や対策情報も含まれます。

b. また、JVN の中で日々発見されるアプリケーションソフト等のセキュリティホール情報を適宜収集・蓄積した「JVN iPedia 脆弱性対策情報データベース」を公開しています。
JVN iPedia は、JVN に掲載されるアプリケーションソフト等のセキュリティホール情報のほか、JVN 以外で公開される国内製品あるいは国内で広く利用されているアプリケーションソフト等の製品に対するセキュリティホール情報についても公開対象としています。
1998 年から発見されているアプリケーションソフトやオペレーティングシステム(OS)等のセキュリティホール情報を中心に約 3,500 件(2007 年 4 月公表時点)のデータを蓄積しており、以後も継続してデータの蓄積を進めています。
セキュリティホール情報は、アプリケーションソフト等の製品毎に「影響を受けるシステム」、「想定される影響」、「対策」等の情報を含みます。

その他、アプリケーションソフトのセキュリティ対策を強化するために、IT 及び情報セキュリティ関連のニュースサイト等をチェックして、利用しているアプリケーションソフトのセキュリティ関連情報等の収集を実施することをお勧めします。

参考 URL
JVN : http://jvn.jp/
JVN iPedia : http://jvndb.jvn.jp/

今月のトピックス

○ コンピュータ不正アクセス被害の主な事例 (届出状況及び被害事例の詳細は、5 頁の「3.コンピュータ不正アクセス届出状況」を参照)
・パスワードクラッキング攻撃を受け侵入された
・ウェブアプリケーションのぜい弱性を突かれて個人情報漏えい？！

○ 相談の主な事例 (相談受付状況及び相談事例の詳細は、7 頁の「4.相談受付状況」を参照)
・ワンクリック不正請求サイトの入り口がこんなところにも！
・ファイル交換ソフトでダウンロードしたファイルからウイルス感染

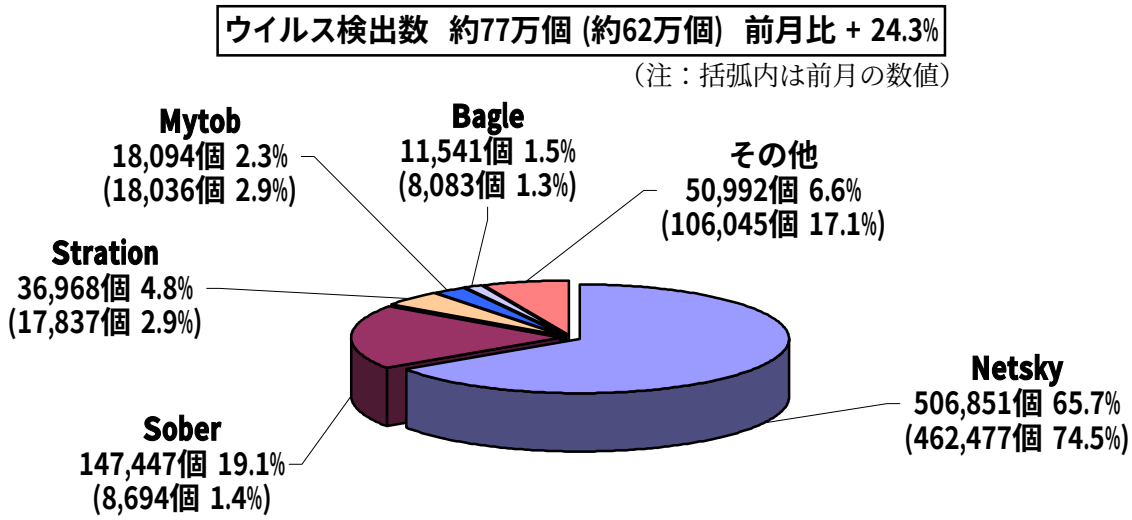
○ インターネット定点観測 (詳細は、別紙 3 を参照)
IPA で行っているインターネット定点観測について、詳細な解説を行っています。
・NetBIOS のぜい弱性を狙ったアクセスが増加！

2．コンピュータウイルス届出状況　－詳細は別紙１を参照－

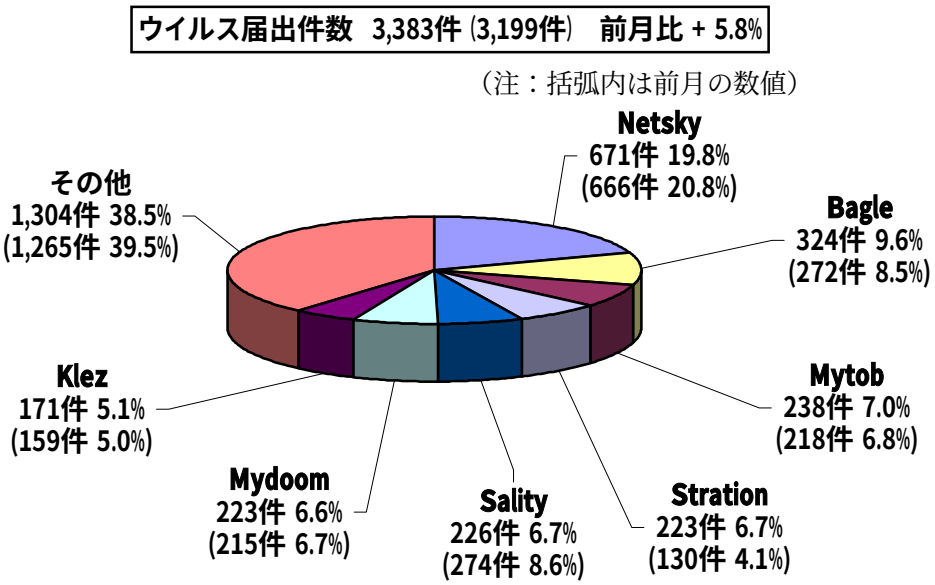
ウイルスの検出数(※1)は、**約 77 万個**と、4 月の 62 万個から 24.3%の増加となりました。
また、5 月の届出件数(※2)は、**3,383 件**となり、4 月の 3,199 件から 5.8%の増加となりました。

※1 検出数　：届出にあたり届出者から寄せられたウイルスの発見数（個数）
※2 届出件数：同じ届出者から寄せられた届出の内、同一発見日で同一種類のウイルスの検出が複数ある場合は、1 日何個検出されても届出 1 件としてカウントしたもの。
・5 月は、寄せられたウイルス検出数約 77 万個を集約した結果、3,383 件の届出件数となっています。

検出数の1位は、**W32/Netsky で約 51 万個 、2 位は W32/Sober で約 15 万個、3 位は W32/Stration で約 4 万個でした。**



図：2-1



図：2-2

3．コンピュータ不正アクセス届出状況（相談を含む）　－詳細は別紙 2 を参照－

不正アクセスの届出および相談の受付状況

		12月	1月	2月	3月	4月	5月
届出(a) 計		**10**	**32**	**23**	**13**	**15**	**19**
	被害あり(b)	9	22	14	9	12	13
	被害なし(c)	1	10	9	4	3	6
相談(d) 計		**40**	**52**	**50**	**43**	**31**	**37**
	被害あり(e)	23	25	28	20	20	21
	被害なし(f)	17	27	22	23	11	16
合計(a+d)		**50**	**84**	**73**	**56**	**46**	**56**
	被害あり(b+e)	32	47	42	29	32	34
	被害なし(c+f)	18	37	31	27	14	22

（1）不正アクセス届出状況

5 月の届出件数は 19 件であり、そのうち**被害のあった件数は 13 件**でした。

（2）不正アクセス等の相談受付状況

不正アクセスに関連した相談件数は 37 件（うち 7 件は届出件数としてもカウント）であり、そのうち何らかの被害のあった件数は 21 件でした。

（3）被害状況

被害届出の内訳は、**侵入 5 件、メール不正中継 2 件、アドレス詐称 1 件、その他（被害あり）5 件**でした。

侵入届出の被害内容は、フィッシング(*2)に悪用するためのコンテンツを設置されていたものが 2 件、外部サイトを攻撃するための踏み台になっていたものが 2 件、サーバ内データの破壊が 1 件でした。侵入の原因は、プログラムのぜい弱性(*1)を突かれたものが 3 件（サーバ管理ツール 2 件、コンピュータの遠隔操作ソフト 1 件）、パスワードクラッキング(*3)攻撃によるものが 2 件（うち SSH(*4)で使用するポート(*5)への攻撃が 1 件）でした。

(4) 被害事例

[侵入]

(i) パスワードクラッキング(*3)攻撃を受け侵入された

事例	・サーバから通信ができなくなった上、アプリケーションが起動できなくなった。 ・ログ(*6)を調査したところ、インターネット側からアクセスを許可していたコンピュータ遠隔操作ソフトのサーバに数ヶ月前からパスワードクラッキング攻撃を受けており、結果としてログインを許していたことが判明。 ・OS のシステムファイルが破壊されたり、ルータ(*7)のファームウェア(*8)が書き換えられたりと、インターネット側から遠隔で破壊活動が行われていた。 ・コンピュータ遠隔操作ソフトへのログインアカウント(*9)に、推測が比較的容易なパスワードが設定されていたのが原因と思われた。
解説・対策	パスワード認証は、基本的には時間を掛ければ破られてしまうという大原則を認識しましょう。**ログのチェックをこまめに実施する**のはもちろんのこと、IP アドレスやドメインなどによる**接続許可制限を施したり、無制限にパスワードクラッキングされ続けないような対策**(一定回数のログイン失敗で、アカウントをロックするなど)をしたりすることが有効です。 (参考) IPA - 情報セキュリティ白書 2007 年版 http://www.ipa.go.jp/security/vuln/20070309_ISwhitepaper.html IPA - 安全なウェブサイトの作り方 改訂第 2 版 http://www.ipa.go.jp/security/vuln/websecurity.html

[その他(被害あり)]

(ii) ウェブアプリケーションのぜい弱性(*1)を突かれて個人情報漏えい?!

事例	・ログをチェックしていたら、大量のデータベースアクセスエラーが発生していたことが判明。 ・エラーの内容を確認したところ、エラー画面にはエラーメッセージとともにデータベース内に記録されている顧客の個人情報も表示されていたことが分かった。
解説・対策	侵入はされていなかったものの、**ウェブアプリケーションに対する SQL インジェクション(*10)攻撃を回避し切れず SQL クエリを実行されてしまい、想定範囲外のエラーを引き起こされていた**ものと推測されます。データベースアクセスエラーには、攻撃に役立つ情報が満載な上、様々な ID に対するエラー情報を収集すると、データベース内のデータをそっくりそのまま再構築することが可能になることもあります。**ウェブアプリケーションのぜい弱性を解消することが根本的な解決策となりますが、もしエラーを表示させる場合でも必要最小限の情報に留めることで、攻撃された場合でも被害を軽減できます**。 (参考) IPA - 情報セキュリティ白書 2007 年版 http://www.ipa.go.jp/security/vuln/20070309_ISwhitepaper.html IPA - 安全なウェブサイトの作り方 改訂第 2 版 http://www.ipa.go.jp/security/vuln/websecurity.html

4．相談受付状況

5 月の相談総件数は **814 件**でした。そのうち**『ワンクリック不正請求』に関する相談**が **185 件**（4 月：205 件）、**『セキュリティ対策ソフトの押し売り』行為**に関する相談が **19 件**（4 月：17 件）、**Winny に関連する相談**が **6 件**（4 月：7 件）などでした。

IPA で受け付けた全ての相談件数の推移

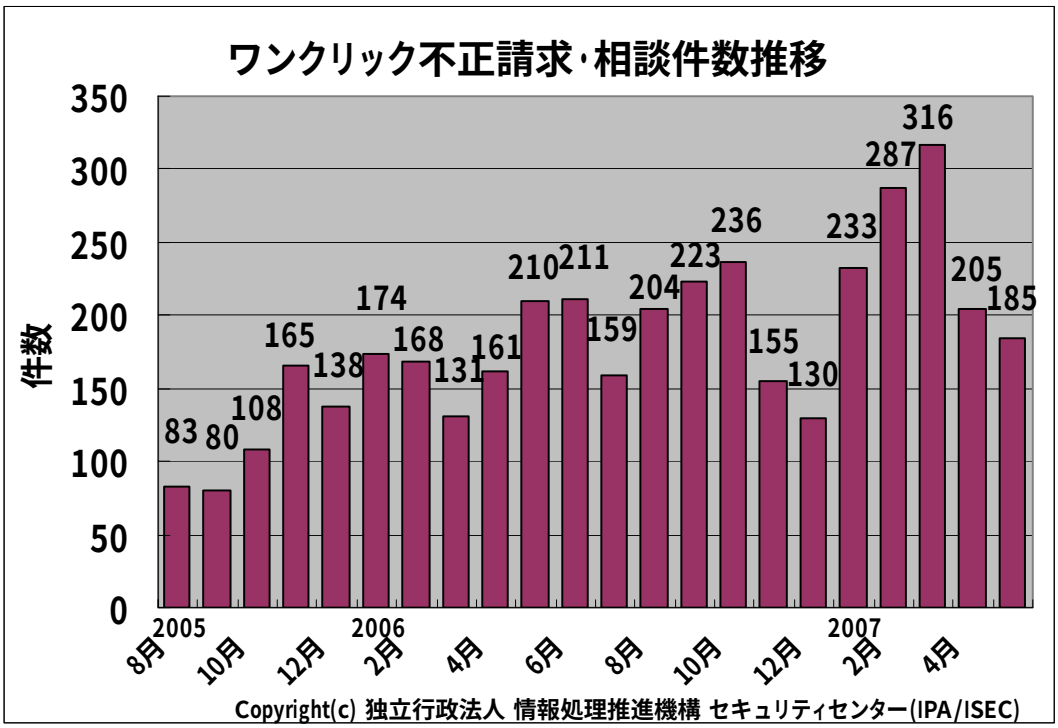
	12月	1月	2月	3月	4月	5月
合計	**680**	**946**	**1019**	**1127**	**827**	**814**
自動応答システム	394	582	603	697	486	484
電話	222	324	336	376	279	254
電子メール	59	39	75	54	58	69
その他	5	1	5	0	4	7

※ IPA では、コンピュータウイルス・不正アクセス、Winny 関連、その他情報セキュリティ全般についての相談を受け付けています。
メール：virus@ipa.go.jp（ウイルス）、crack@ipa.go.jp（不正アクセス）、
winny119@ipa.go.jp（Winny 緊急相談窓口）、isec-info@ipa.go.jp（その他）
電話番号：03-5978-7509（24 時間自動応答、ただし IPA セキュリティセンター員による相談受付は休日を除く月～金の 10:00～12:00、13:30～17:00 のみ）
FAX：03-5978-7518（24 時間受付）

※ 「自動応答システム」：電話の自動音声による応対件数
「電話」：IPA セキュリティセンター員による応対件数

※ 合計件数には、「不正アクセスの届出および相談の受付状況」における『相談(d) 計』件数を内数として含みます。

（参考）ワンクリック不正請求相談件数の推移

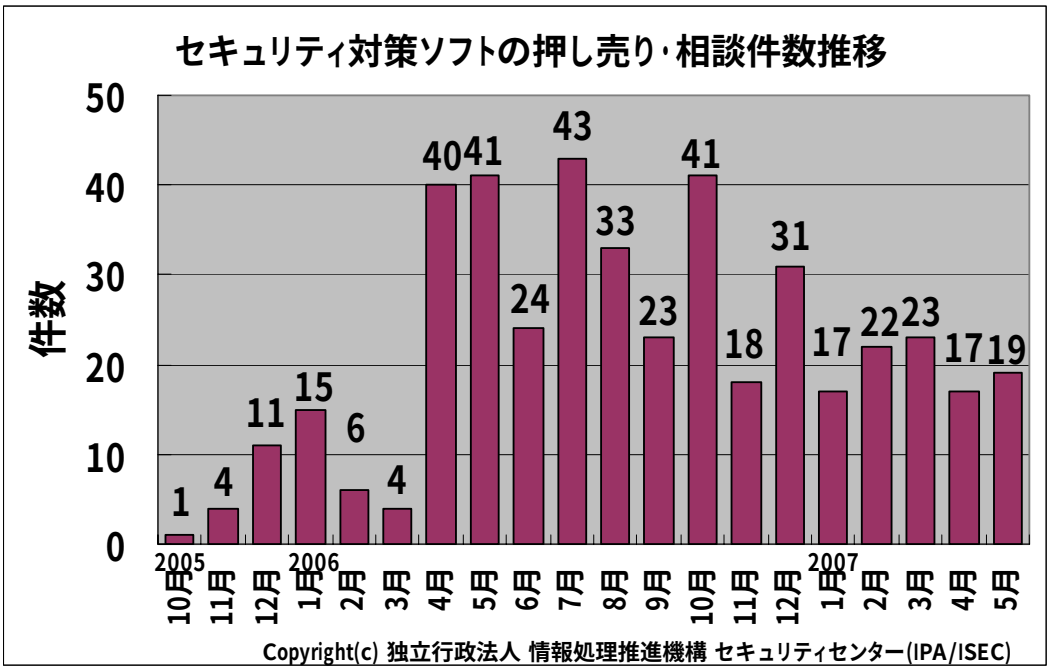


ワンクリック不正請求についての対策については下記をご参照ください。

・コンピュータウイルス・不正アクセスの届出状況[9 月分および第 3 四半期]について
2. ワンクリック不正請求
http://www.ipa.go.jp/security/txt/2006/10outline.html

・コンピュータウイルス・不正アクセスの届出状況[8 月分]について
2. 依然として相談の多いワンクリック不正請求による被害
http://www.ipa.go.jp/security/txt/2006/09outline.html

（参考）セキュリティ対策ソフトの押し売り・相談件数の推移



セキュリティ対策ソフトの押し売り行為については下記をご参照ください。

・2006 年 5 月の呼びかけ:「セキュリティ対策ソフトウェアの押し売りに注意！！」
http://www.ipa.go.jp/security/txt/2006/05outline.html

主な相談事例は以下の通りです。

(i) ワンクリック不正請求サイトの入り口がこんなところにも！

相談	ニュースで話題になっていた**ジェットコースター事故のことを知りたくて検索サイトで調べていた**ら、事故映像を掲載しているというサイトがリスト内にあった。早速クリックしてみたら、個人が開設しているブログサイトだった。ニュースを一通り読み進め、「衝撃映像はこちら」というリンクがあったのでクリックしたら、有名な動画投稿サイトらしき画面に遷移した。プレイボタンをクリックしたら「規約に同意されますか？」という画面が出て、**安易に「はい」をクリックしてしまったら、何かデータをダウンロードされたような画面が表示され、さらに入会金 50,000 円の請求書が表示された**。
回答	アダルトサイト以外でも、**“芸能人裏情報”や“衝撃映像”といった誘い文句で待ち受けている悪質なワンクリック不正請求サイトが存在しています**。検索でヒットしたサイトは、安全なものばかりではないことを十分認識し、注意してアクセスしなければなりません。さらに、興味本位でどんどんクリックして先に進むのは控えましょう。**請求書画面が出現する前に、必ず“年齢認証”や“入会規約”などの確認画面があるはず**です。そこには、その先で提供されるサービスが有料であることが明示されているケースがほとんどです。**クリックする前に、画面に表示されているメッセージをしっかりと読むことも、被害を防止するために重要な心掛けとなります**。 （ご参考） IPA - 「巧妙化するワンクリック不正請求の手口！！」 http://www.ipa.go.jp/security/txt/2005/11outline.html#5

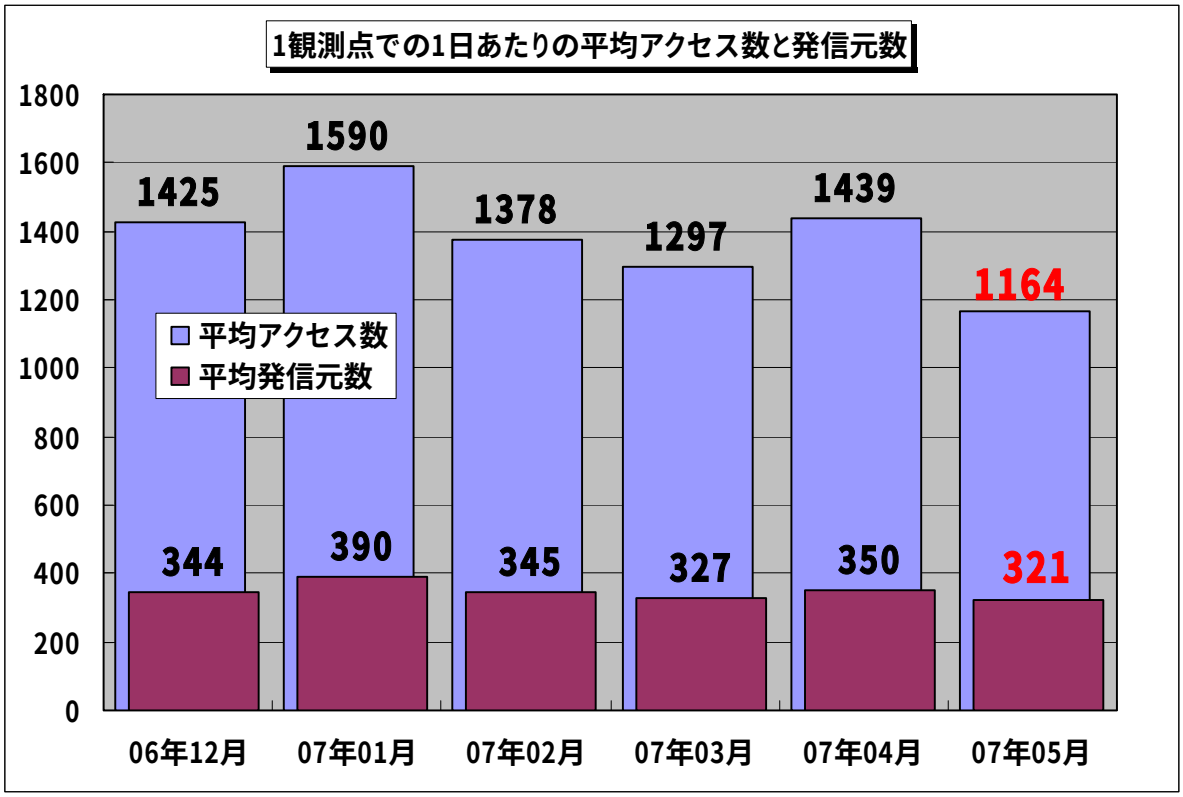
(ii) ファイル交換ソフトでダウンロードしたファイルからウイルス感染

相談	① 友人に勧められ、パソコンにファイル交換ソフト（**Winny と Share**）をインストールして使っていた。動画プレーヤーが動かなくなったり、セキュリティ対策ソフトがエラーを出すようになったりしたので、無償のウイルスチェックでスキャンしたところ、600 ものファイルが 3 種類のウイルスに感染していた。 ② パソコンに外部から侵入されてパソコンの設定を変更されてしまったらしく、インターネットに接続できなくなった。ファイル交換ソフト**Cabos**を利用しており、ダウンロードしたファイルを開いていたせいでウイルス感染したのか。 ③ **Winny** でダウンロードしたファイルを開いたら、多数のファイル（動画やプログラムなど）が某アニメーションキャラクターの画像ファイルに置き換わっていた。ウイルス対策ソフトでは何も検知されない。
回答	ファイル交換ソフトを使う上での脅威として、**暴露型ウイルスの他にファイルを破壊（上書き）するタイプのウイルスも存在します**。出所の不明なファイルを開くことは、ウイルス対策の観点で見れば最も危険な行為です。ウイルスに感染したくないのであれば、**ファイル交換ソフトの利用を止めることも有効な対策の一つです**。何か問題が発生してからでは、取り返しがつきません。 （ご参考） IPA – Winny による情報漏えいを防止するために http://www.ipa.go.jp/security/topics/20060310_winny.html

5．インターネット定点観測での 5 月のアクセス状況

インターネット定点観測(TALOT2)によると、2007 年 5 月の期待しない（一方的な）アクセスの総数は、10 観測点で **209,499 件**ありました。1 観測点で 1 日あたり **321** の発信元から **1,164 件**のアクセスがあったことになります。

TALOT2 での 1 観測点の環境は、インターネットを利用される一般的な接続環境と同一なので、インターネットを利用される皆さんの環境へも同じくらいの一方的なアクセスがあると考えられます。言い換えれば、**あなたのコンピュータは、毎日、平均して、321 人の見知らぬ人(発信元)から、発信元一人当たり 4 件の不正と思われるアクセスを受けている**と言うことになります。



【図 5.1　1 観測点での 1 日あたりの期待しない(一方的な)アクセス数および発信元数】

2006 年 12 月～2007 年 5 月までの各月の 1 観測点での 1 日あたりの平均アクセス数および、それらのアクセスの平均発信元数を図 5.1 に示します。

2007 年 5 月のアクセス状況は、全体的に 4 月と同じで定常化していると言えます。

注意）

5 月は TALOT2 システム保守の為、5 月 1 日から 5 月 18 日までの観測データで発表しておりますことをご了承下さい。

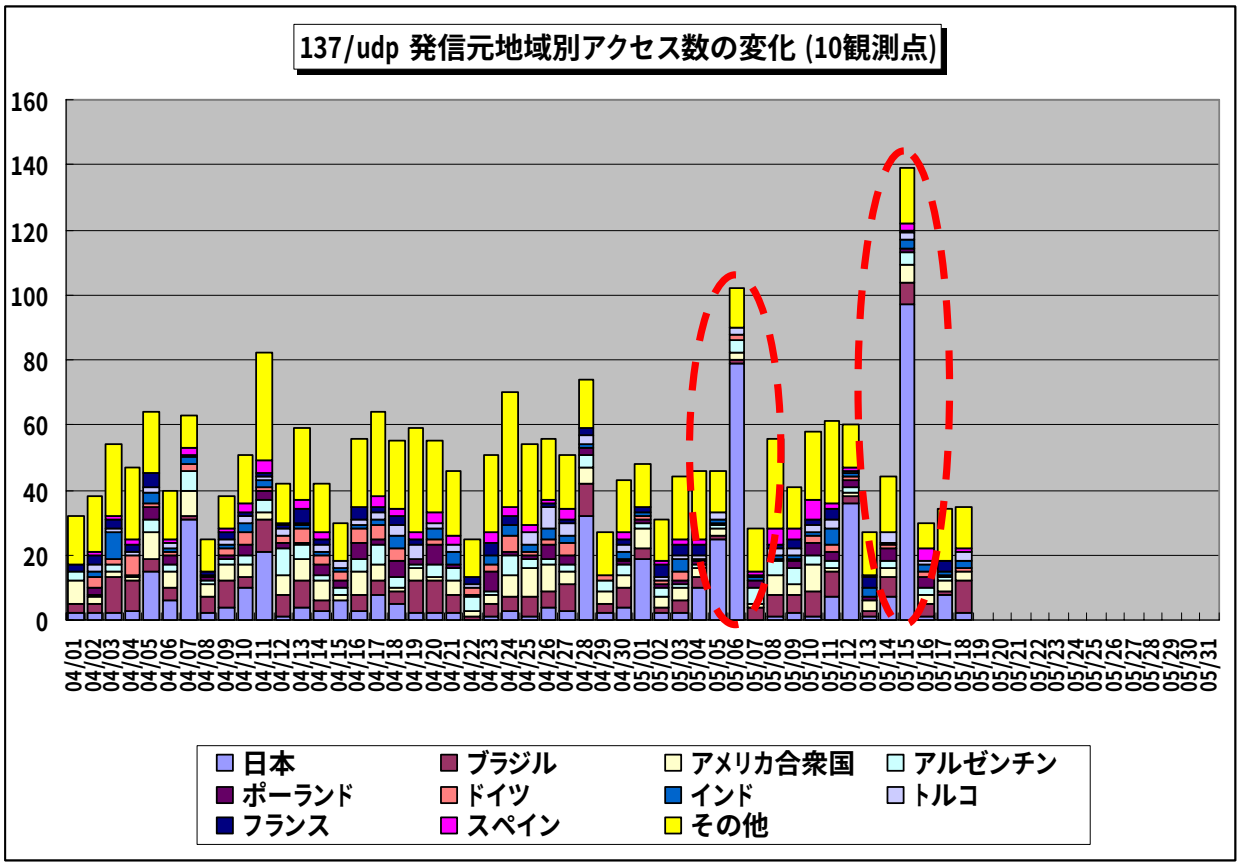
(1) NetBIOS※のぜい弱性を狙ったアクセス

5 月は観測データが少ない中で、137/udp ポートへのアクセスが目立ちました。これはネットワークサービスである、NetBIOS※ の Windows のぜい弱性を狙ったアクセスと考えられます。

図 5.2 に、2007 年 4 月から 2 ヶ月間の、137/udp ポートへの発信元地域別アクセス数の変化を示します。

<参考情報>

■ NetBIOS の問題により、情報が漏えいする。(MS03-034)
http://www.microsoft.com/japan/technet/security/Bulletin/MS03-034.mspx



【図 5.2　2007 年 4 月～5 月の 137/udp ポートへの発信元地域別アクセス数の変化】

※ NetBIOS（ネットバイオス：Network Basic Input/Output System）
ネットワーク上でプログラムが使用する関数。Windows では、NetBEUI（ネットビューイ：NetBIOS Extended User Interface）プロトコルと組み合わせて、小規模なネットワーク環境で使用される。

以上の情報に関して、詳細はこちらのサイトをご参照ください。

別紙 3_インターネット定点観測（TALOT2）での観測状況について
http://www.ipa.go.jp/security/txt/2007/documents/TALOT2-0706.pdf

---

『他機関・ベンダーの各種統計情報は以下のサイトで公開されています。』

@police：http://www.cyberpolice.go.jp/
トレンドマイクロ株式会社：http://www.trendmicro.com/jp/
マカフィー株式会社：http://www.mcafee.com/japan/

『用語の解説』

(*1) **ぜい弱性** (vulnerability)
情報セキュリティ分野においては、通常、システム・ネットワーク・アプリケーションまたは関連するプロトコルのセキュリティを損なうような、予定外の、望まないイベントにつながる可能性がある弱点の存在や、設計もしくは実装のエラーのことを言う。セキュリティ上の設定が不備である状態を指す場合もある。一般に、セキュリティホール (security hole)と呼ばれることもある。

(*2) **フィッシング** (Phishing)
正規の金融機関など実在する会社を装ったメールを利用して偽のウェブページに誘導し、それを見た利用者の ID やパスワードなどを詐取しようとする行為のこと。「釣り」を意味する「fishing」が語源だが、ハッカーの命名規則に則って"f"を"ph"に置き換えたという説、「洗練された」という意味の英語 "sophisticated"と"fish"とを組み合わせた造語という説、"password harvesting fishing"の短縮形という説、などがある。

(*3) **パスワードクラッキング** (password cracking)
他人のパスワードを、解析するなどして探り当てること。総当り攻撃や辞書攻撃といった手法があり、クラッキング用のプログラムも存在する。
＊:総当り攻撃
システムのパスワードを発見するために、パスワード文字列として可能な組み合わせをひとつずつ試す攻撃。「ブルートフォース」には、「力ずく」という意味が込められている。
＊:辞書攻撃
パスワードを破るために、辞書にある単語などを片端から試行する攻撃方法のこと。

(*4) **SSH** (Secure SHell)
ネットワークを介して遠隔のコンピュータと通信するためのプロトコルの一つ。通信上のデータはすべて暗号化されるため、Telnet のようにデータが平文で通信されるプロトコルに比べて、安全性が高い。SSH の利用に際しては、いくつかの認証方式を選択することが可能だが、パスワード認証は総当り攻撃などにより認証を突破されてしまう可能性があるため、公開鍵認証を用いることが推奨される。

(*5) **ポート** (port)
コンピュータが外部との情報の受け渡しの際に使う、コンピュータ内の各種サービス窓口のこと。ポートは 0 から 65535 までの値が使われるため、ポート番号とも呼ばれる。

(*6) **ログ** (log)
コンピュータの利用状況やデータ通信の記録のこと。一般的に、操作を行った者の ID や操作日時、操作内容などが記録される。

(*7) **ルータ** (router)
異なるネットワークを接続したり中継したりする通信機器のこと。

(*8) **ファームウェア** (firmware)
コンピュータやその他電子機器の基本的制御を行うために、機器内に組み込まれたプログラムのこと。ハードウェアとソフトウェアとの中間的な存在ということで、こう呼ばれている。

(*9) **アカウント** (account)
コンピュータやネットワーク上の資源を利用出来る権利のこと。

(*10) **SQL インジェクション** (SQL injection)
データベースアクセスのために SQL 文を用いるプログラムにおいては、SQL 文を構成する際、プログラム中の式の値を SQL 文に埋め込む場合には、引用符で括られる文字列について、引用符が含まれているならばそれをエスケープ処理しなければならない。これを怠ると、正当なデータに対して SQL 文の実行がエラーとなる不具合が生じる。このバグが悪意ある者によって与えられ得る文字列を扱う箇所に存在すると、それはセキュリティ上のぜい弱性となる。攻撃者が悪意あるコマンドを与えると、データベースの内容を改ざんや情報を盗み出されるなどの被害が生じる。このような攻撃を SQL インジェクション攻撃と呼び、その原因箇所を同ぜい弱性と呼ぶ。

■お問い合わせ先
独立行政法人 情報処理推進機構 セキュリティセンター
花村／加賀谷／宮本
Tel:03-5978-7527 Fax:03-5978-7518 E-mail:isec-info@ipa.go.jp

お知らせ

「第 3 回 情報セキュリティ標語・ポスター」募集のお知らせ

コンピュータウイルスやコンピュータへの不正な侵入などの被害にあわないために、「情報セキュリティ対策」の意識を高めるための標語及びポスターを、全国の小学生・中学生・高校生から募集します。入選作品は、報道発表し、IPA のホームページにも掲載します。

募集期間：2007年7月 1 日(日)～2007 年9月１０日(月)
応募方法：電子メール　isec-hyogo@ipa.go.jp
ＦＡＸ　　03-5978-7518
郵　送　　〒113-6591　東京都文京区本駒込 2-28-8
情報処理推進機構（IPA）　セキュリティセンター
情報セキュリティ標語・ポスター事務局　宛
詳しくは、下記のホームページをご参照下さい。
http://www.ipa.go.jp/security/event/hyogo/2007/boshu.html
賞　　金：大賞（10 万円)、金賞（7 万円)、銀賞（5 万円)、銅賞（3 万円）
韓国情報保護振興院(KISA)賞（賞品)、その他、参加企業賞あり

お問い合わせ先
標語・ポスター募集に関するお問い合わせ先はこちらです。
独立行政法人 情報処理推進機構　セキュリティセンター　山田／岸原
Tel:　　03-5978-7508
Fax:　　03-5978-7518
E-mail:　isec-hyogo@ipa.go.jp

問い合わせ受付時間 9:30 - 18:30 月曜日～金曜日
（祝祭日、振替休日を除く）