プレスリリース
2006 年 6 月 2 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［2006 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、2006 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。

今月の呼びかけ：「有名企業等の名をかたった偽装メールに注意！！」 ― 添付ファイルを安易に開くな！ ―

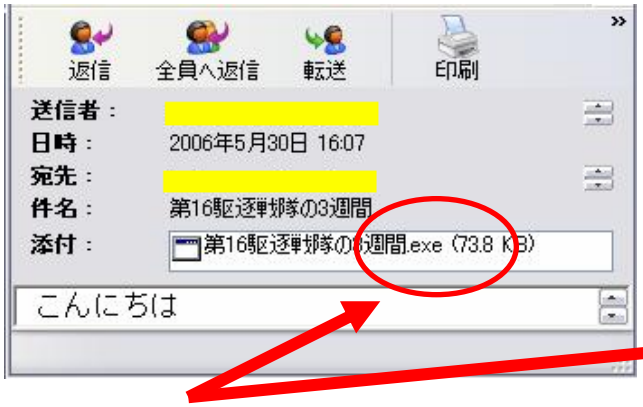
インターネットメールは、差出人アドレス欄（From 欄）に表示されるアドレスを詐称することが可能です。これまでにも、他人になりすましてメールを送るといったウイルスがありました。
2006 年 5 月には、防衛庁や日本経済新聞社といった有名組織になりすまし、特定の組織に対してウイルスを添付したメールが送りつけられるといった事例が立て続けに報道されました。

これらのケースは、新種ウイルスが送りつけられたものであったため、ウイルス対策ソフトの対応が遅れたものでした。このように、たとえウイルス対策ソフトを最新の状態にしていても検出されないことがあります。さらに、件名や本文が日本語で、偽のメールと気付きにくくなっていることもあります。仮に、差出人が信頼できる組織からのものであったとしても、添付ファイルがあった場合には、細心の注意を払い安易に開かないようにしましょう。

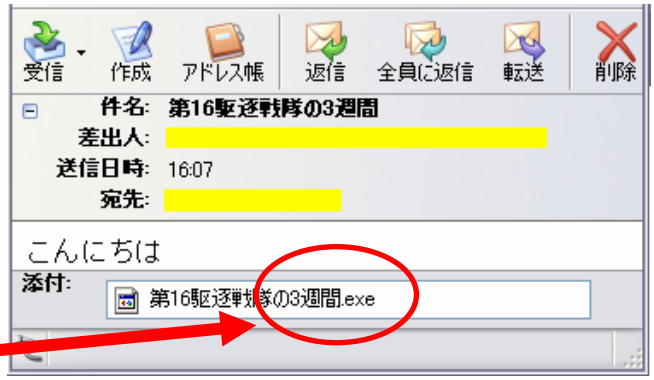
具体的には、メールの添付欄(下図参照)に表示されている名称を確認することが肝要です。例えば、末尾が「.exe」である場合は、ウイルスなどである可能性がありますので、原則として開かないようにしましょう。どうしても開く必要がある場合は、まずウイルス対策ソフトで検査する、さらに、検出されない場合であっても新種ウイルスの可能性もありますので、送信者に問い合わせる、などの注意が必要です。
この他、添付欄に表示されている名称の末尾が「.pif」、「.scr」、「.bat」、「.com」などの場合もウイルスの可能性がありますので、同様に注意が必要です。

【メールの添付欄の表示例】

例 1：メールソフト（Outlook Express）の表示例



例 2：メールソフト（Thunderbird）の表示例



ここに表示されている名称を確認。末尾が「.exe」になっている場合は要注意。

※ 最新版の Outlook Express には、メニューバーの[ツール]→[オプション]→[セキュリティ]タブに、「ウイルスの可能性がある添付ファイルを保存したり開いたりしない」という設定があります。Windows XP 以外の OS（Windows ME/2000 等）をお使いの方は、最新版の Outlook Express に更新することをお勧めします。

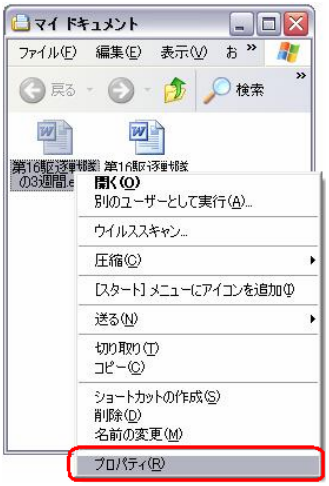
この設定を解除してしまうと、ウイルスの可能性があるファイルを開くことが可能になりますので、注意が必要です。
なお、Outlook Express を最新版にするには、[スタート]→[Windows Update]の手順で Windows Update のサイトから更新することができます。

【添付されたファイルがウイルスの偽装かどうかを確認する方法】

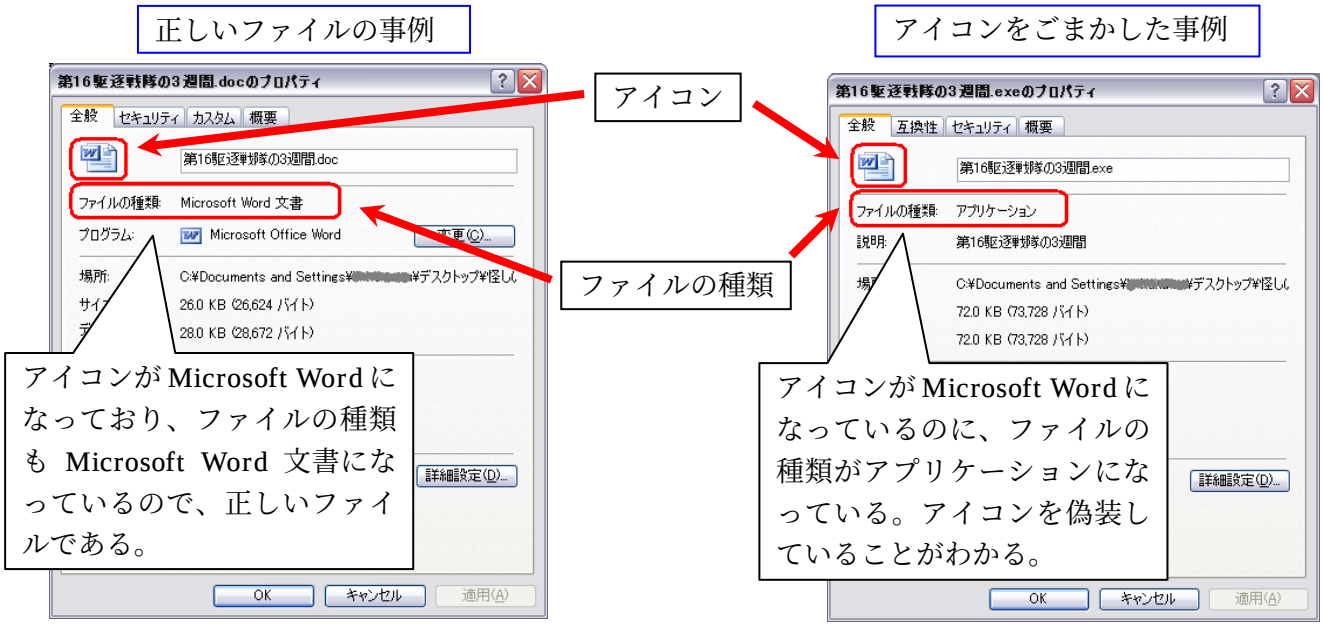
アイコン（パソコンの画面上でファイルの内容などを小さな絵などで表したもの）が偽装されていないかを見分ける方法として、右クリックして「保存」を選択し、添付ファイルを「マイドキュメント」などのフォルダにいったん保存した上で、ファイルの種類を確認する方法があります。（保存するだけではウイルスに感染しません。）

例えば、Microsoft Word（文書ファイル）のアイコンに偽装したウイルス（アプリケーションファイル）は以下のように見分けることができます。

上述の手順で保存したファイルを右クリックし、プロパティを表示します。「正しいファイルの事例」にあるように、Microsoft Word (文書ファイル)のアイコンに対し、正にワード文書であれば、ファイルの種類は必ず「Microsoft Word 文書」と表示されます。一方、アイコンをごまかした事例では、Microsoft Word (文書ファイル)のアイコンに対して、ファイルの種類が「アプリケーション」になったりしますので、偽装していることがわかります。このような、偽装しているファイルは決して開かずに削除するようにしてください。



保存した当該ファイルを右クリックして「プロパティ」を選択



その他、よく使われるファイルのプロパティを表示すると、以下の対応表のようになります。アイコ

ンとファイルの種類の対応が表に示されているものと異なる場合は、偽装されていることになりますので、開かないようご注意ください。特に、ファイルの種類が「アプリケーション」になっている場合は要注意です。

【アイコンとファイルの種類、プロパティ表示内容 対応表】

アイコン	ファイルの種類	プロパティでファイルの種類として表示されるもの
	画像ファイル	JPEG イメージ ビットマップ イメージ
	動画ファイル/音楽ファイル	ムービー ファイル Windows Media オーディオ/ビデオ ファイル　※注
	Microsoft Excel ファイル	Microsoft Excel ワークシート

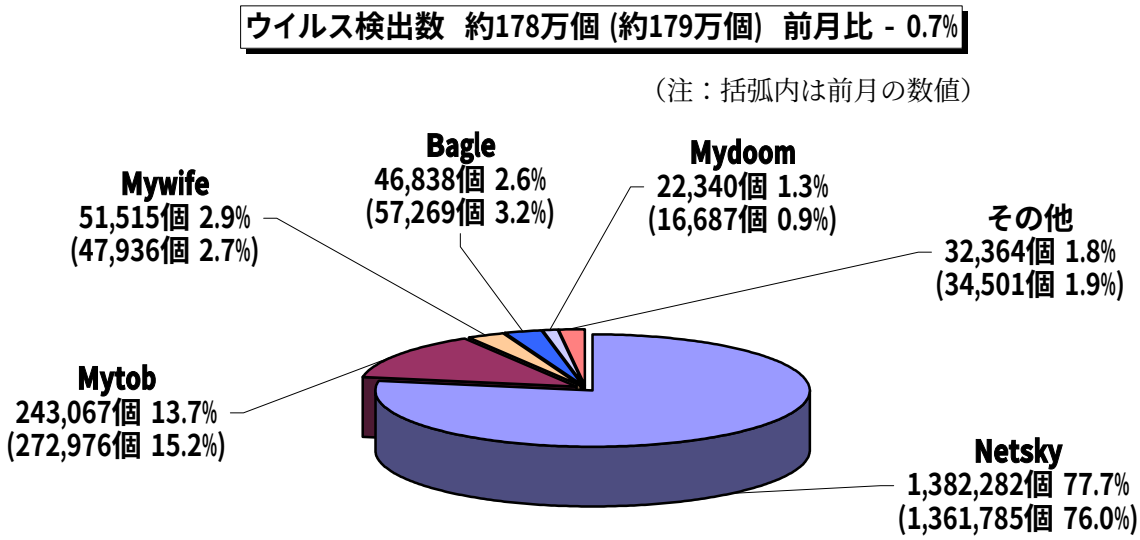
注：初期設定であれば、この他に、「Windows ビデオ/オーディオ ファイル」、「MP3 オーディオ ファイル」、「MIDI ファイル」、「AIFE オーディオ ファイル」、「AU オーディオ ファイル」、「Microsoft テレビ録画ファイル」があります。

1．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 178 万個**と、4 月の 179 万個から同水準での推移となりました。
また、5 月の届出件数(※2)は、**3,651 件**となり、4 月の 3,537 件から 3.2%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 178 万個を集約した結果、3,651 件の届出件数となっています。

検出数の1位は、**W32/Netsky** で**約 138 万個 、2 位は W32/Mytob** で**約 24 万個、3 位は W32/Mywife** で**約 5 万個でした。**



図：1-1

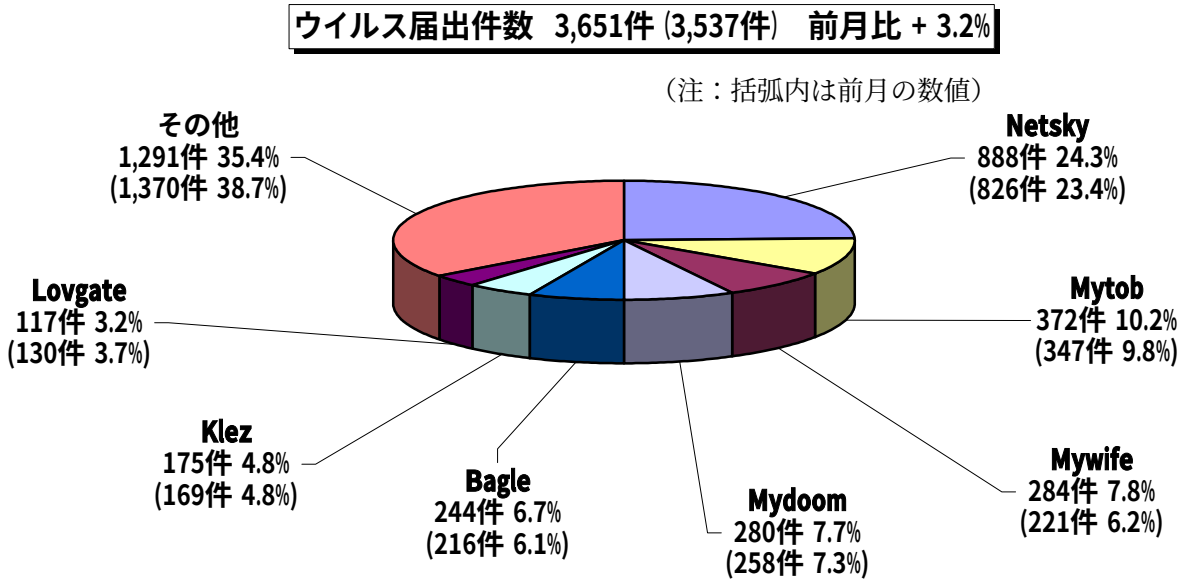


図:1-2

2．スパイウェアについて

スパイウェア(*1)による相談事例として、アダルトサイト等で画像や動画と思ってクリックしただけで、スパイウェアが取り込まされる等のいわゆるワンクリック不正請求に関するものが継続して多数(200 件以上) 寄せられています。

このような被害事例では、セキュリティ警告を無視して、自分でスパイウェアを取り込んでしてしまっているケースが多いようです。

動画や画像を表示するだけであれば、下図のようなセキュリティの警告画面は表示されません(まず図2-1の警告画面が表示されます。このとき「実行」を選択すると図2-2の警告画面が表示されます)。

少しでも怪しいと思ったら、ファイルの「種類」やファイルの「発行元」の情報をチェックし、安全が確認された場合以外は [実行] や [実行する] をクリックしないようにしましょう。

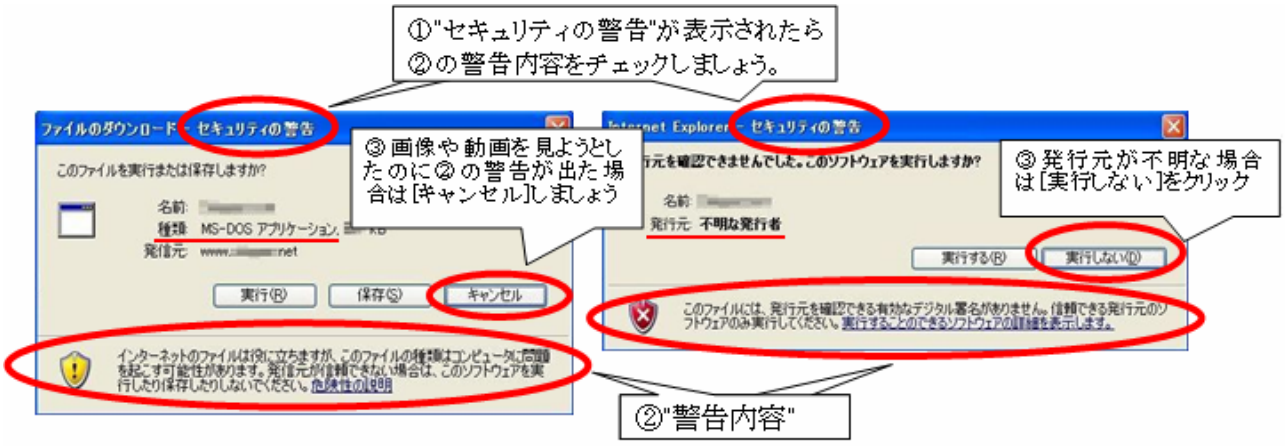
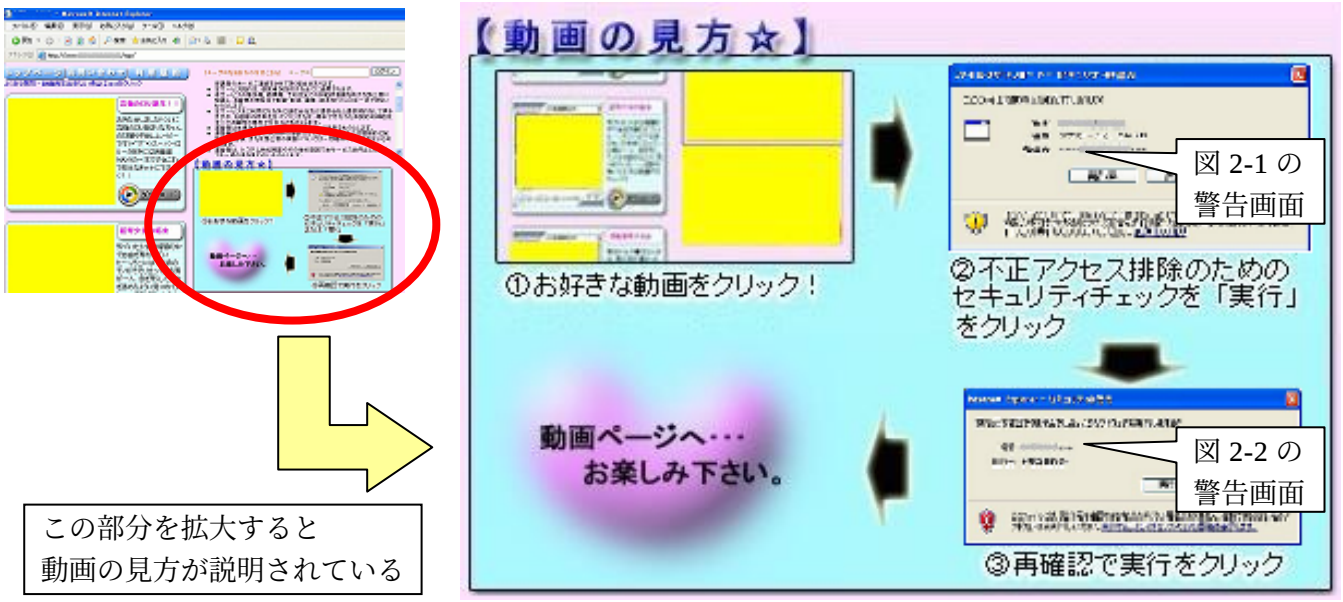


図:2-1　　図:2-2

実際の相談の中には、以下のような悪意あるサイトの表示内容によって誘導され、被害に遭ったという事例もあります。

これは、動画だと偽ってプログラム（スパイウェア）を埋め込ませるために、Windows が表示するセキュリティの警告に対して、実行を選択するよう促すものです。この手順通りに進めると、動画は再生されずに、自らスパイウェアを取り込んでしてしまうことになります。

【スパイウェアを埋め込ませるため、ユーザに Windows が表示する警告を無視するように誘導している悪いサイトの例】



図：2-3

上述の事例で紹介したスパイウェアは、動画の画面そのもの(図 2-3 における①の黄色の部分)に埋め込まれています。黄色の部分をクリックすると、Windows のセキュリティ機能により図 2-1 の警告画面が表示されます。その警告画面で、「実行」をクリックするように仕向けています。「実行」をクリックすると、図 2-2 にある Windows からの再警告が表示されます。

そこでさらに「実行」をクリックするよう誘導しています。ここで「実行」をクリックすると、スパイウェアを自ら取り込んでしまうことになります。Windows のセキュリティ機能が正常に働いて警告を出しているのですが、この仕組みを逆手にとって、手順を示すことにより大丈夫だから「実行」を押して先に進ませて、スパイウェアを取り込ませようとする悪質なやり方です。

（ご参考）

今月の呼びかけ：「警告を無視すると不正プログラムがインストールされる？！　」
― 警告画面を軽視していませんか？ ―　　【2006 年 1 月分】
http://www.ipa.go.jp/security/txt/2006/02outline.html
スパイウェア対策のしおり
http://www.ipa.go.jp/security/antivirus/shiori.html

※4. (i) の相談事例もご参照ください。

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		**25**	**50**	**26**	**38**	**15**	**13**
	被害あり(b)	19	13	15	10	7	6
	被害なし(c)	6	37	11	28	8	7
相談(d) 計		**25**	**43**	**42**	**24**	**27**	**23**
	被害あり(e)	15	23	24	12	15	11
	被害なし(f)	10	20	18	12	12	12
合計(a+d)		**50**	**93**	**68**	**62**	**42**	**36**
	被害あり(b+e)	34	36	39	22	22	17
	被害なし(c+f)	16	57	29	40	20	19

（1）不正アクセス届出状況

5 月の届出件数は 13 件であり、そのうち**被害のあった件数は 6 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 23 件（うち 2 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 11 件でした。

（3）被害状況

被害届出の内訳は、**侵入 4 件、DoS 攻撃 1 件、アドレス詐称 1 件**でした。

侵入届出の内訳は、SSH(*2)で使用するポート(*3)への攻撃を受けた結果侵入されたというものが 2 件、フィッシング(*4)に悪用するための Web コンテンツを設置させられていたというものが 1 件、などでした。

被害事例

[侵入]

(i) SSH(*2)で使用するポート(*3)への攻撃

事例	・「同組織内にあるサーバを攻撃しているようだ」との通報を受けたため調査したところ、大量の SSH(*2)アクセスログ(*5)を発見。 ・テスト用に作り、後で削除する予定だったアカウント(*6)のパスワードが破られ、サーバにログインされていたことが判明。 ・ログによれば最初の侵入から数日後、侵入されたサーバから、1 時間程度の間に 1 万通を超えるメールが発信されていた。そのほとんどが宛先不明のエラーメールとして返送されてしまい、最終的には被害を受けた組織のメールサーバがダウンした。発信されたメールは、文面からしてフィッシング(*4)目的と思われた。 ・本来の意図とは違い、ルータの設定が外部からの SSH アクセスを許可するようになっていたため攻撃に晒されて、その結果侵入を許していた。以前、ルータの設定をリセットした際に、設定し直すのを怠っていたのが原因と思われた。
解説・対策	この事例では、**ルータの設定不備**と**脆弱なパスワードを持った不要アカウントの存在**という、2 つの事象が重なったのが原因となっています。さらに、**フィッシングメール送信の踏み台**にされていましたから、一歩間違うと社会的責任を問われかねませんでした。**日々アクセスログをチェックして一刻も早く攻撃の兆候を掴み、必要な対策を講じることが重要です**。なお、相変わらず、SSH で使用するポートが狙われる機会が多いようです。**SSH 運用時には、ログインの際に公開鍵認証(*7)などの強固な認証を採用することを推奨します**。 (参考) IPA - 安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/20060131_websecurity.html

[DoS 攻撃(*8)]

（ii） メール不正中継を狙った攻撃？

事例	・テスト中のサーバのログチェック中、メールサーバへの執拗なアクセスを発見。 ・その後、ログの量が極端に増加したため、攻撃であると判断。サーバのパフォーマンスが著しく低下した。 ・アクセス内容を解析した結果、メールの不正中継を試みていたと思われた。さらに、管理者権限でのログイン試行も認められた。（全て未遂）
解説・対策	この事例では、**テストとはいえ適切な設定で実施していたようで、侵入もメール不正中継も許していなかったのが幸いでした**。特に、メール不正中継を防止するためには、必要が無いならネットワーク外部からメール送信サーバを使えない設定にすることが最も有効です。なお、DoS 攻撃(*8)を受けてしまった時に迅速な対応を取るためには、**IDS(*9)や IPS(*10)といった侵入検知システムの導入による、攻撃の早期検知**が重要です。 （参考） IPA - UBE（迷惑メール）中継対策 http://www.ipa.go.jp/security/ciadr/antirelay.html IPA - コンピュータ不正アクセス被害防止対策集 http://www.ipa.go.jp/security/ciadr/cm01.html#DoS

4．相談受付状況

5 月の相談総件数は **846 件**と、相変わらず高水準で推移しています。そのうち、**『ワンクリック不正請求』に関する相談**が **210 件**（4 月：161 件）と、統計を取り始めた昨年からでは最高の件数を記録しました。また、セキュリティ対策ソフトの押し売りのような行為に関する相談は **41 件**（4 月：40 件）と、先月に引き続き多く寄せられました。その他は、**Winny に関連する相談**が **28 件**（3 月：196 件、4 月：83 件）などでした。

IPA で受け付けた全ての相談件数の推移

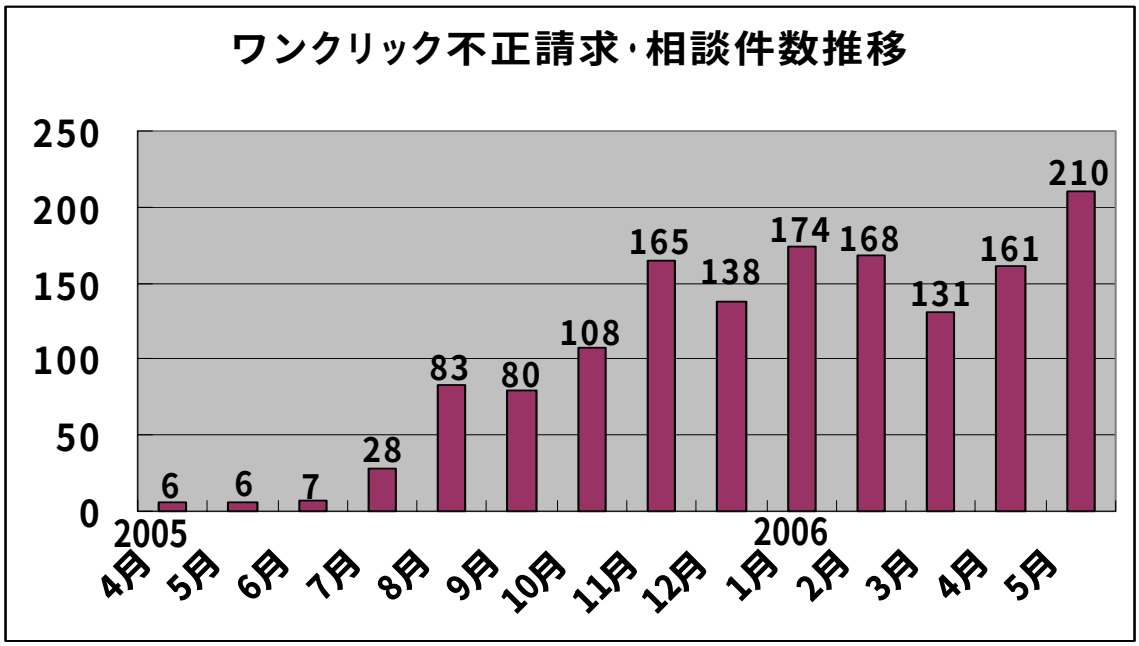
		12月	1月	2月	3月	4月	5月
合計		**653**	**748**	**834**	**1056**	**904**	**846**
	自動応答システム	391	425	479	659	510	484
	電話	194	228	258	296	306	295
	電子メール	66	87	90	99	86	63
	その他	2	8	7	2	2	4

※ 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。

ワンクリック不正請求相談件数の推移



主な相談事例は以下の通りです。

(i) アダルトサイトでワンクリックしたら・・・

相談	ネットサーフィンをしていてたまたま訪れたアダルトサイトで、画像をクリックしたら勝手に入会登録されたようで、料金請求書が表示された。その後、数日経つとメールで請求書が送られて来たり、パソコン上に数分おきに請求書が表示されたりする。複数のウイルス対策ソフトでスキャンしても、何も検出されない。パソコンを初期化するしかないのでしょうか。
回答	最近の多くの相談例を見ていると、違うアダルトサイトでも、仕込まれる不正プログラムの特徴が似通っていることが分かります。ウイルス対策ソフトで何も検出できなくても、**請求書に書かれている「サイト名」「サービス名」「連絡先」などの情報が分かれば、ほとんどの場合は不正プログラムを特定し削除できます**。あきらめずに、IPA セキュリティセンターに相談してください。 また、Windows XP や Me であれば、**「システムの復元」機能を使うと、当該アダルトサイトを訪れる以前の状態に戻すことができる場合があります**。Windows XP であれば、 [スタート]－[すべてのプログラム]－[アクセサリ]－[システムツール]－[システムの復元]で、実行できます。 （被害を未然に防ぐための対策は、本紙 2. スパイウェアについて を参照）

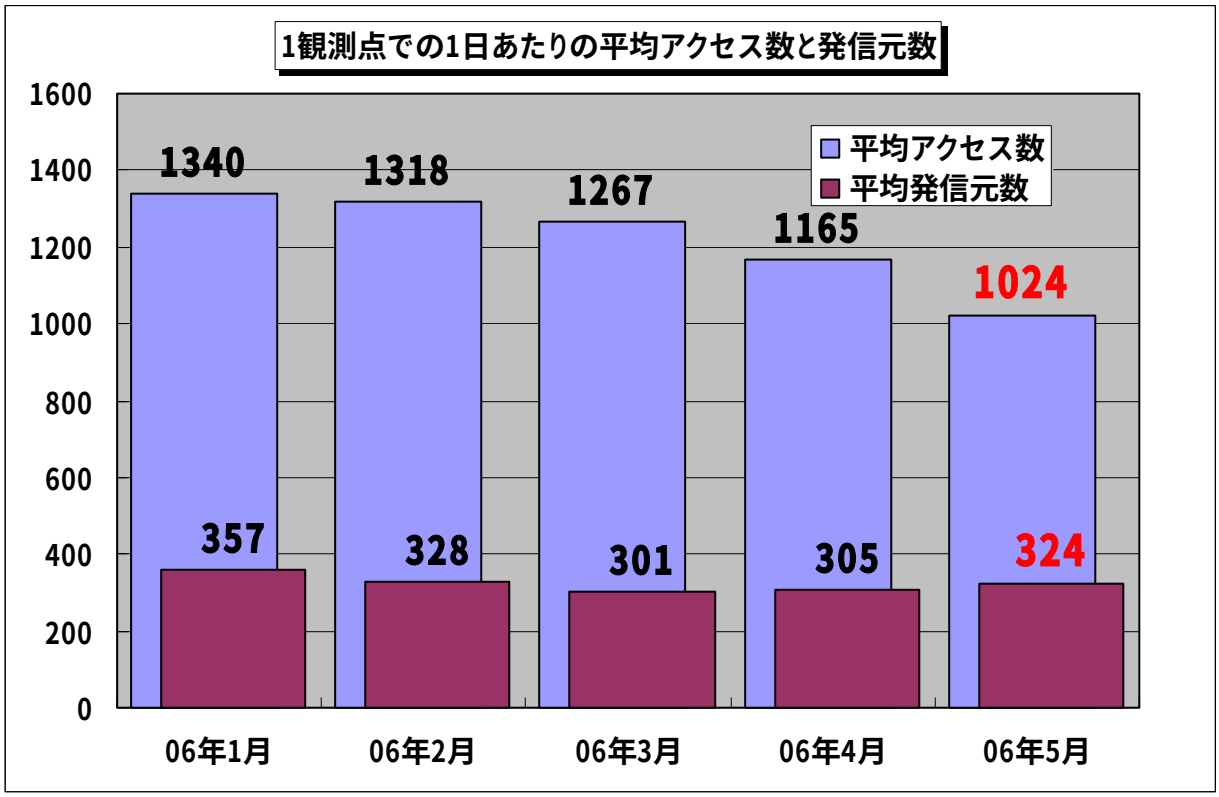
(ii) 怪しいメールの本文にあったリンクをクリックしたら・・

相談	見知らぬ人から怪しいメールが届いた。本文中に「**当選しました！　ここをクリックしてください**」などというリンクがあったのでクリックしたら、そのサイトにジャンプして「**入会完了**」と表示された。退会しようとしてメールで連絡したが、返事は無い。その後、出会い系サイトの勧誘メールがたくさん届くようになった。
回答	悪意のある Web サイトには、多くの危険が潜んでいます。そういったサイトへ誘導するために、人間の興味を惹くような題名や内容のメールが不特定多数のアドレス宛に送信されているようです。つまり、怪しいサイトのみならず、怪しいメールにも危険が潜んでいるのです。**見知らぬ人から届いた“怪しい”メールは、内容までは確認しても、本文中のリンクはクリックしてはいけません**。悪意のあるサイトに誘導され、ウイルスやスパイウェアなどの不正プログラムを埋め込まれる可能性があります。(関連情報：　本紙冒頭　今月の呼びかけ　を参照) なお、届くようになってしまった**迷惑メールは、技術的には送信自体を止められませんので、「送信を止めさせる」手立てが必要**です。メールヘッダ情報を基に送信元コンピュータ情報を割り出し、**送信元コンピュータが所属するネットワーク（プロバイダなど）の管理者宛に対処を依頼する**ことになります。 また、「特定電子メールの送信の適正化等に関する法律(平成 14 年法律第 26 号)」によれば、以下の機関が相談･問い合わせ･情報提供機関として指定されています。 (ご参考) ･出会い系サイトなどの迷惑メールに関する相談など (表示義務違反メールなどに関する情報提供、電話相談) 財団法人日本データ通信協会　迷惑メール相談センター(総務省指定機関) http://www.dekyo.or.jp/soudan/top.htm ･物品の販売などの商取引に関する迷惑メールに関する相談など (再送信禁止義務違反メールの情報提供) 財団法人日本産業協会(経済産業省指定機関) http://www.nissankyo.or.jp/

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、2006 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 **317,490 件**ありました。1 観測点で 1 日あたり **324** の発信元から **1024 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、324 人の見知らぬ人(発信元)から、発信元一人当たり 3 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 1 月～2006 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 1 に示します。この図を見ると、**期待しない（一方的な）アクセスは、緩やかに減少傾向にあるようです**。アクセス内容については、定常化していると言えます。

5 月のアクセス状況は、4 月とほぼ同じ状況です。Windows の脆弱性を狙っていると思われる不正なアクセスが多いようで、これらのアクセスの多くは、ボット(*11)に感染したコンピュータから送信されていると思われます。

特にアクセス数の多い 135(TCP)ポート,445(TCP)ポートへのアクセスは、Windows の脆弱性を狙っています。また、Windows Messenger サービスを悪用したポップアップスパムメッセージの 1026(UDP)/1027(UDP)ポートへのアクセスは、継続しています。

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/2006/documents/TALOT2-0606.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/jp/default.asp

『用語の解説』

(*1) スパイウェア (spyware)
利用者や管理者の意図に反してインストールされ、利用者の個人情報やアクセス履歴などの情報を収集するプログラム等。

(*2) SSH (Secure SHell)
ネットワークを介して別のコンピュータにログインしたり、遠隔地のマシンでコマンドを実行したり、他のマシンへファイルを移動したりするために使うプロトコルもしくはプログラムのこと。ネットワーク上を流れるデータは暗号化されるため、インターネット経由でも一連の操作を安全に行なうことができる。

(*3) 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。

(*4) フィッシング (Phishing)
正規の金融機関など実在する会社のメールや Web ページを装い、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。

(*5) 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。

(*6) 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、または利用する際に必要な ID のこと。

(*7) 公開鍵認証
公開鍵と秘密鍵のペアでユーザ個人の認証を行う方式のこと。公開鍵はサーバ側で管理し、秘密鍵は個人で管理し、これらによりユーザ認証を行う。

(*8) DoS 攻撃 (Denial of Services)
サーバに大量のデータを送って過大な負荷をかけ、サーバのパフォーマンスを極端に低下させたり、サーバを機能停止に追い込んだりする攻撃のこと。

(*9) IDS (Intrusion Detection System)
システムに対する侵入／侵害を検出･通知するシステムのこと。システムを監視し、セキュリティポリシーを侵害するような行為を検出した場合に、その行為を可能な限り早く管理者に伝えるとともに、調査分析の作業を支援するために必要な情報を保存･提供することが目的である。

(*10) IPS （Intrusion Prevention System）
システムに対する侵入／侵害を阻止するシステムのこと。異常を検知した際に自動的に通信を停止する機能を有したものであり、一般的には IDS の発展形と言える。

(*11)ボット
コンピュータウイルスの一種で、コンピュータに感染し、そのコンピュータを、ネットワーク(インターネット)を通じて外部から操ることを目的として作成されたプログラムのことである。

■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

『自社のセキュリティ対策自己診断テスト』
～ 情報セキュリティ対策ベンチマーク ～

IPA では、**「自社のセキュリティ対策自己診断テスト（情報セキュリティ対策ベンチマーク）」**を Web サイト上に公開しております。

自社のセキュリティ対策自己診断テスト（情報セキュリティ対策ベンチマーク）
https://isec.ipa.go.jp/benchmark-new/

本システムは、企業を対象としたもので、セキュリティ対策状況及び企業情報に関する設問(計40 問)に答えることにより、セキュリティ対策の取組状況を自己採点できるシステムです。

診断結果は、「貴社のスコア」と「望まれる水準」とが同時に表示され、各社が優先的に取り組むべきセキュリティ対策項目が明らかになります。また、推奨される取り組み事例も提示しますので、今後の対策を強化する上での具体的な改善策がわかります。

30 分程度で自己採点できますので、ぜひ、今後のセキュリティ対策の参考とすべく、ご活用ください。

「情報セキュリティ標語 2006」の入選作品

これは、コンピュータウイルスの感染やコンピュータへの不正な侵入、 ワンクリック詐欺などの被害に遭わないよう、 特に若年層の「情報セキュリティ対策」の意識を高めるために、本年 3 月より全国の小学生・中学生・高校生から募集していたもので、全国 118 の小・中・高等学校の中から 1,101 件の応募があり、以下の 10 作品が入選しました。

区分	作品	学校 / 受賞者氏名
大賞	ネットで繋がる無限の世界　明暗決めるはあなたの手	神奈川･慶應義塾湘南藤沢高等部 / 清水　優香子（しみずゆかこ）
高校生の部		
金賞	人々の　意識で変わる　セキュリティ	埼玉県･県立越谷北高等学校 / 浅井　慧（あさいあきら）
銀賞	ケータイは持って天国　落として地獄	岐阜県･県立可児工業高等学校 / 田口　史武（たぐちふみたけ）
銅賞	手軽でも　忘れるなかれ　セキュリティ	埼玉県･立教新座高等学校 / 松下　成昭（まつしたしげあき）
中学生の部		
金賞	ネットワーク　便利と危険は　紙一重	茨城県･つくば市立吾妻中学校 / 藤井のど佳（ふじいのどか）
銀賞	情報は　流れだしたら　止まらない	埼玉県･三郷市立早稲田中学校 / 増田　恵子（ますだあやこ）
銅賞	気をつけよう　インターネットの落とし穴	兵庫県･加古川市立中部中学校 / 遠入　和也（えんにゅうかずや）
小学生の部		
金賞	ぼくだけは　感染しないよ　大間違い	岐阜県･大垣市立墨俣小学校 / 古澤健太郎（ふるさわけんたろう）
銀賞	パスワード　ともだちにだって　ないしょだよ	愛知県･名古屋市立滝ノ水小学校 / 森　明日翔（もりあすか）
銅賞	セキュリティ　あなたが守る　あなたの身	千葉県･千葉市立若松台小学校 / 山崎　緑（やまざきみどり）