

## コンピュータウイルス・不正アクセスの届出状況 [2006年10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10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:

「心当たりのないメールは、興味本位で開かず!にすぐ捨てよう!」

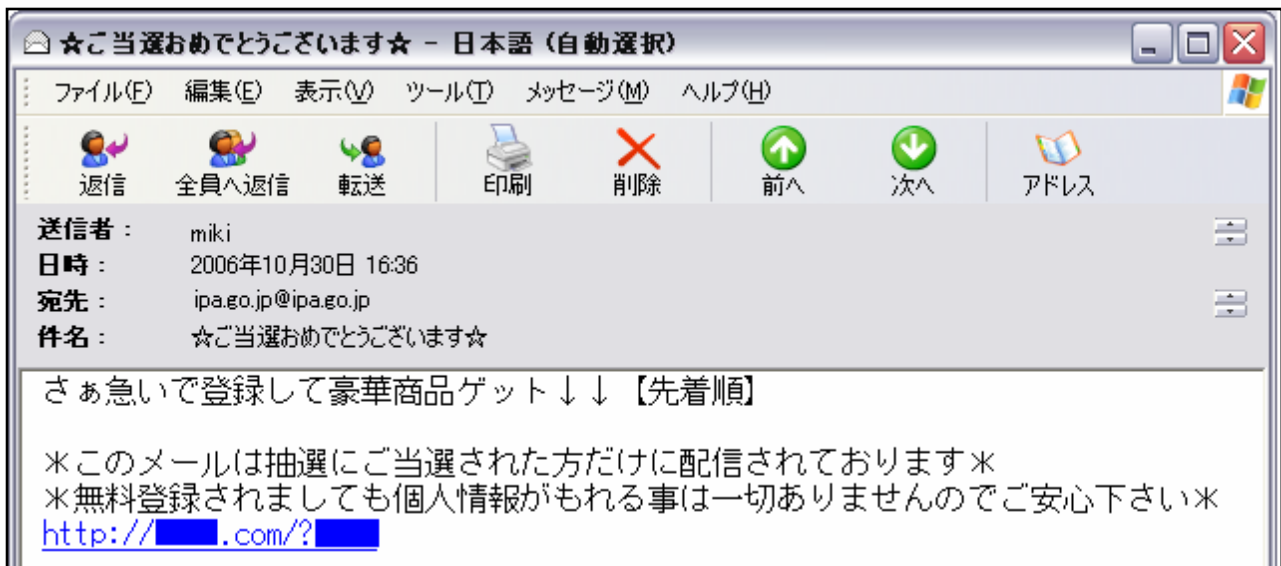
— 迷惑メールでウイルスなどの被害に遭わないように!! —

最近、見知らぬ差出人からの心当たりのないメールを受け取り、メール本文中に記載されているホームページのアドレスをクリックすることにより誘導されたホームページの表示に従ってクリックした結果、**ウイルスを取り込まれる被害に遭ったなどの相談が IPA に多く寄せられています。**(P9:3.相談受付状況 事例(i)参照)

届いたメールが自分に関係ないものと知りつつ興味本位で添付ファイルを開くことは、ウイルスに感染するなどの被害に遭う可能性が高くなります。また、**単なる広告メールのように見せかけて利用者を騙し、クリックさせてウイルスやスパイウェアなどを取り込ませるなど、手口が巧妙**になっています。

ひとたび感染するとパソコンを乗っ取られたり、あるいは、個人情報漏えいするなどの被害に遭う危険性があります。そもそも、どこの誰から届いたかわからない、自分に関係のないと思われる**怪しいメールは、本文を開いて見ることをせず、すぐに捨てる**ことが有効な対策となります。

怪しいメールには以下のようなものがあります。このようなメールが届いても、**リンクや添付ファイルをクリックすることなく、原則、すぐに捨てるように**しましょう。



その他、迷惑メールに使われる件名の実例

- VIP 会員特典の御連絡
- 業界ニュース最新号
- 新規お試しモニター募集!!
- 【緊急!大募集!! 目指せ月収 200 万円】
- 見事ご当選!! 商品券一万円☆ 等

迷惑メールなど、注意が必要なメールはその性質などにより概ね4つの種類に分類されます。

以下に4種類それぞれの主な特徴を記載します。また、これらの中には、ウイルスメールが紛れ込んでいる場合もあるので注意が必要です。

<b>(1) 無差別広告などの迷惑メール</b>	
事例	<ul style="list-style-type: none"><li>・ 件名から推測して自分が興味のない分野の広告と思われるメール</li><li>・ 同じところから繰り返し送られてくるメール</li></ul>
<p>これらの中には、本文中にホームページのアドレスが記載されていて、それを<b>クリック</b>することで<b>関係のないホームページへ誘導され、ウイルス感染等の被害に遭う</b>場合があります。</p>	
<b>(2) 差出人はいろいろ変わっているが本文が同じ内容のメール</b>	
事例	<ul style="list-style-type: none"><li>・ 差出人は異なっているが、同じ件名でメール本文が同じ内容のメール</li><li>・ 差出人も件名も異なるがメール本文が同じ内容のメール</li></ul>
<p>これらは、大量メール配信によって感染を拡げる<b>ウイルスによるメールの可能性</b>がありますので、開くとウイルス感染する恐れがあり注意が必要です。</p>	
<b>(3) 差出人が見知らぬ人で、内容にも覚えがないメール</b>	
事例	<ul style="list-style-type: none"><li>・ 自分のアドレスを登録した覚えのないところから来る広告などのメール</li><li>・ 懸賞に当選したなどの件名で届くメール</li></ul>
<p>これらは、ただで景品を取得できるように見せかけ、そのためには個人情報の入力が必要などと表示し、入力すると結果的にメールアドレスや氏名、住所などの<b>個人情報</b>を詐取されてしまう場合があります。</p>	
<b>(4) 差出人は知り合いであるが、件名が妙なものや普段と何か違うと感じられるメール</b>	
事例	<ul style="list-style-type: none"><li>・ 普段日本語でしかやりとりをしていない人から届いた本文が外国語のメール</li><li>・ 普段添付ファイルを送ってこない人から届いた添付ファイル付きのメール</li></ul>
<p>これらは、<b>差出人を詐称するウイルスが送信しているメールの可能性が高く</b>、添付ファイルを開くと被害に遭う場合があります。したがって、上記のようなメールが届いた場合は、差出人に電話等で内容を確認し、問題ないことがわかった上で開くようにしてください。</p>	

以上の例の内、いわゆる迷惑(広告)メールには、「配信不要の場合はこのアドレスへ返信メールにて連絡してください。」等のメッセージの記述とともに連絡先のメールアドレスが文末に記載されていることがあります。このメッセージを信用して、配信拒否のための返信メールを送信することは、無差別に送ってきている相手に、わざわざ自分のメールアドレスが実在していてちゃんと使われていることを知らせることになり、さらに迷惑メールが増えるなど、悪用される可能性を増やすこととなります。決して返信するなど考えずに、心当たりのないメールには一切対応せず、無視することが重要です。

# 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**117万個**と、9月の105万個から11.5%の増加となりました。  
また、10月の届出件数(※2)は、**3,696件**となり、9月の3,551件から4.1%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です。

・10月は、寄せられたウイルス検出数約117万個を集約した結果、3,696件の届出件数となっています。

検出数の1位は、**W32/Netsky**で約**78万個**、2位は**W32/Stration**で約**22万個**、3位は**W32/Mytob**で約**4万個**でした。

**ウイルス検出数 約117万個(約105万個) 前月比 + 11.5%**

(注：括弧内は前月の数値)

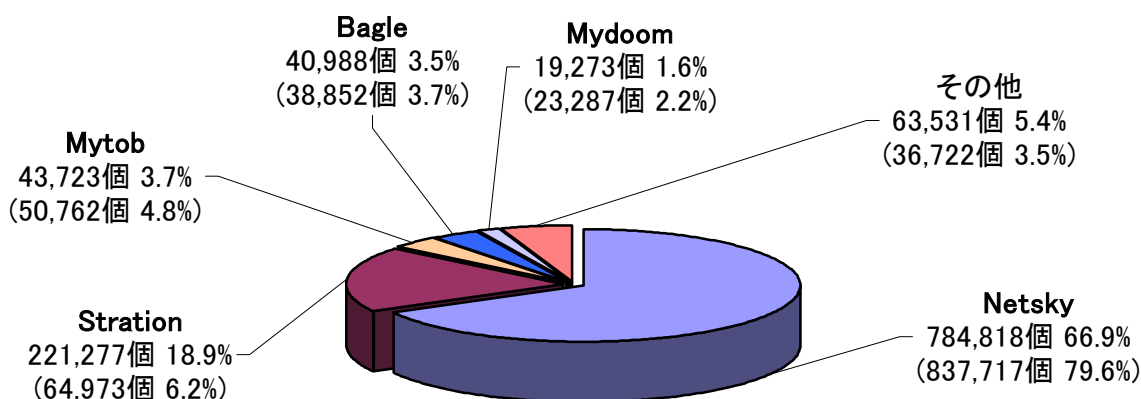


図:1-1

**ウイルス届出件数 3,696件(3,551件) 前月比 + 4.1%**

(注：括弧内は前月の数値)

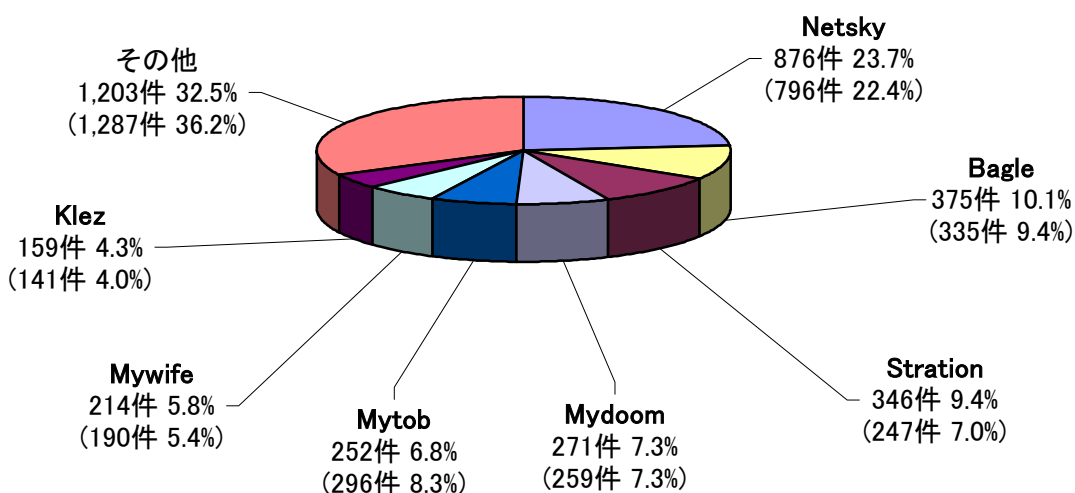


図:1-2

## W32/Stration の蔓延に注意

2006年8月に発生した W32/Stration の亜種が9月に引き続き10月も多数出現し、出回っていますので、注意が必要です。

このウイルスは、メールの添付ファイルにより拡散します。その添付ファイルを開くとウイルスに感染することになり、アドレス帳に保存されているメールアドレス宛に同様のウイルスメールを送信することになってしまいます。

また、亜種の中には、ウイルスの作者が用意したと推測されるサイトへアクセスさせ、勝手に感染したPCにスパイウェアなどをダウンロードする機能を持ったものなどもあり、情報漏えいが生じるなどの被害に遭う可能性があります。

さらに、ルートキット<sup>(\*)</sup>も同時にコンピュータにインストールするため、感染してからでは発見することが困難になります。また、見た目にはわかる症状もでないため、感染していることに気付かず、ウイルスメールを撒き散らし続けることになってしまいます。

感染してからでは対処が困難になるなど、被害が拡大する恐れがありますので、メールの添付ファイルを安易に開くことは決してしないようにしてください。

以下に最近出回っている W32/Stration の亜種の件名、添付ファイル名の例を示します。

	件名	添付ファイル名
(1)	This is not shown on TV.	picture3135.zip
(2)	This is not shown on TV.	picture7484..gif. exe
(3)	Livan War real pictures.	picture2812..bmp. exe
(4)	This must be seen by everyone.	picture6720..jpg. exe
(5)	Server Report	text.txt.exe
(6)	URGENT NEWS!	last.exe
(7)	ATTN	about me.exe
(8)	NEWS!	latest news.exe
(9)	READ AND RESEND ASAP!	truth.exe

上記(2)、(3)、(4)の例では、二重拡張子のファイル名を用いて、さらに間にスペースを入れて、末尾の拡張子「.exe」に気付かせないようにし、画像ファイルに見せかけています。

他の例では、News と称して注目させるような件名や添付ファイル名を用いているケースもあります。

(参考)

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

<http://www.ipa.go.jp/security/txt/2006/10outline.html>

## 2. 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

	5月	6月	7月	8月	9月	10月
<b>届出<sup>(a)</sup> 計</b>	<b>13</b>	<b>22</b>	<b>15</b>	<b>50</b>	<b>46</b>	<b>22</b>
被害あり <sup>(b)</sup>	6	20	8	30	21	15
被害なし <sup>(c)</sup>	7	2	7	20	25	7
<b>相談<sup>(d)</sup> 計</b>	<b>23</b>	<b>32</b>	<b>31</b>	<b>24</b>	<b>35</b>	<b>53</b>
被害あり <sup>(e)</sup>	11	19	18	13	26	37
被害なし <sup>(f)</sup>	12	13	13	11	9	16
<b>合計<sup>(a+d)</sup></b>	<b>36</b>	<b>54</b>	<b>46</b>	<b>74</b>	<b>81</b>	<b>75</b>
被害あり <sup>(b+e)</sup>	17	39	26	43	47	52
被害なし <sup>(c+f)</sup>	19	15	20	31	34	23

### (1) 不正アクセス届出状況

10月の届出件数は22件であり、そのうち被害のあった件数は15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53件（うち11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37件でした。

### (3) 被害状況

被害届出の内訳は、**侵入8件、ワーム感染1件、DoS攻撃1件**などでした。

侵入届出の被害内容は、ウェブページの改ざんが3件、他サイト攻撃の踏み台になっていたものが2件、フィッシングに悪用するためのコンテンツを設置されていたものが1件、などでした。侵入の原因として、SSH<sup>(\*)2</sup>で使用するポート<sup>(\*)3</sup>へのパスワードクラッキング<sup>(\*)4</sup>攻撃を受けてパスワードが破られた事例が1件ありました。

その他の被害として、ウェブメールなどのアカウント<sup>(\*)5</sup>が何者かによって勝手に使われ、登録してあった本人のデータを改ざんされたりメールを削除されたりしたという事例が3件ありました。

## 被害事例

### [侵入]

#### (i) SSH<sup>(\*)2</sup>で使用するポート<sup>(\*)3</sup>への攻撃

<b>事例</b>	<ul style="list-style-type: none"><li>・サーバの環境構築中、何らかの外的要因にて作業がストップしてしまった。</li><li>・調査したところ、SSH で使用するポートに対して SSH ログインのパスワードクラッキング<sup>(*)4</sup> 攻撃を受けており、最終的にパスワードを破られてサーバに侵入されていたことが判明。</li><li>・さらに、サーバ内にボット<sup>(*)6</sup> やポートスキャンツール<sup>(*)7</sup> を置かれ、起動されていた。外部サイトへの DoS 攻撃<sup>(*)8</sup> ツールを設置しようとした形跡もあった。また、サーバ内で起動されたプログラムがウイルスに感染しており、サーバ内の他のファイルにもウイルス感染が広がっていた。</li></ul>
<b>解説・対策</b>	<p>パスワードクラッキング<sup>(*)4</sup> の際には自動攻撃ツールが用いられるためか、SSH で使用するポート<sup>(*)3</sup> が狙われる機会はなおも多いようです。そもそも、SSH によるリモート接続が本当に必要なものなのか、そのメリット・デメリットについて議論しましょう。SSH を利用する場合、パケットフィルタリングの実施や IDS<sup>(*)9</sup> /IPS<sup>(*)10</sup> の導入なども大事ですが、まずは<b>日々アクセスログ<sup>(*)11</sup> 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。SSH 運用時には、ログインの際に公開鍵認証<sup>(*)12</sup> などの強固な認証を採用することを推奨</b>します。</p> <p>(参考)</p> <p>IPA - 今月の呼びかけ(7 月分) 「パスワードを一つ残らず、きちんと管理しましょう！」 <a href="http://www.ipa.go.jp/security/txt/2006/07outline.html">http://www.ipa.go.jp/security/txt/2006/07outline.html</a></p> <p>IPA - 安全なウェブサイトの作り方 <a href="http://www.ipa.go.jp/security/vuln/20060131_websecurity.html">http://www.ipa.go.jp/security/vuln/20060131_websecurity.html</a></p>

### [その他]

#### (ii) アカウント<sup>(\*)5</sup>を勝手に使われた

<b>事例</b>	<ul style="list-style-type: none"><li>・大手ポータルサイトで作成した自分のアカウントにログインしようとしたら、「パスワードが間違っています」となり、ログインできなかった。</li><li>・当該ポータルサイトのアカウント作成の際に、作成者のメールアドレスとして登録していた他のフリーメールアカウントにアクセスしてみたら、当該ポータルサイトの“登録メールアドレス変更確認”通知が届いていた。</li><li>・さらに、当該ポータルサイトのオークションサービスで、自分のアカウントから身に覚えの無い品物が出品されていることを確認。</li></ul>
-----------	--

解説・対策	<p>最近、大手のポータルサイトにおいて無料で取得できるアカウントが、第三者に勝手に使われてしまったという被害届出が多くなっています。ウェブメールの送受信ボックスが空になっていた、など単なるいたずらと思われるものもありますが、金銭が絡むオークションなどでは詐欺に悪用される例もあるため、引き続き注意が必要です。パスワードは推測されにくいものにするとともに、<b>特に用事が無くても定期的にアクセスし、勝手に使われていないかどうか確認する</b>と良いでしょう。定期的にパスワードを変更することも、有効な対策となります。また、スパイウェアによってパソコン内の ID/パスワード情報を盗み出されるケースもありますので、ウイルス/スパイウェア対策ソフトによるチェックも欠かさないようにしましょう。</p> <p>(参考)</p> <p>IPA - 今月の呼びかけ(7月分) 「パスワードを一つ残らず、きちんと管理しましょう！」 <a href="http://www.ipa.go.jp/security/txt/2006/07outline.html">http://www.ipa.go.jp/security/txt/2006/07outline.html</a></p>
-------	--

### 3. 相談受付状況

10月の相談総件数は**1,002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**236件**(9月:223件)と、先月に更新した最高件数をさらに上回る最悪の件数を記録しました。その他の内訳は、『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**41件**(9月:23件)、Winnyに関連する相談が**12件**(3月:196件、4月:83件、5月:28件、6月:15件、7月:12件、8月:14件、9月:9件)などでした。

#### IPAで受け付けた全ての相談件数の推移

	5月	6月	7月	8月	9月	10月
<b>合計</b>	<b>846</b>	<b>773</b>	<b>767</b>	<b>793</b>	<b>933</b>	<b>1,002</b>
自動応答システム	484	423	444	460	575	580
電話	295	283	257	280	302	326
電子メール	63	64	66	48	51	93
その他	4	3	0	5	5	3

※ 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)、

winsky119@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)

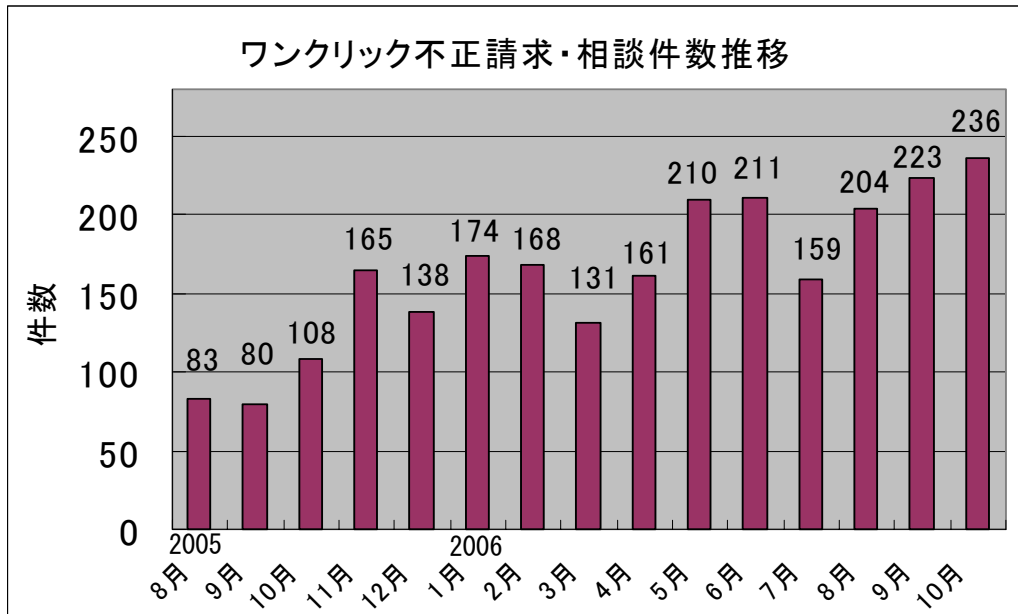
FAX: 03-5978-7518 (24時間受付)

※ 「自動応答システム」: 電話の自動音声による対応件数

「電話」: IPAセキュリティセンター員による対応件数

※ 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<sup>(d)</sup>計』件数を内数として含みます。

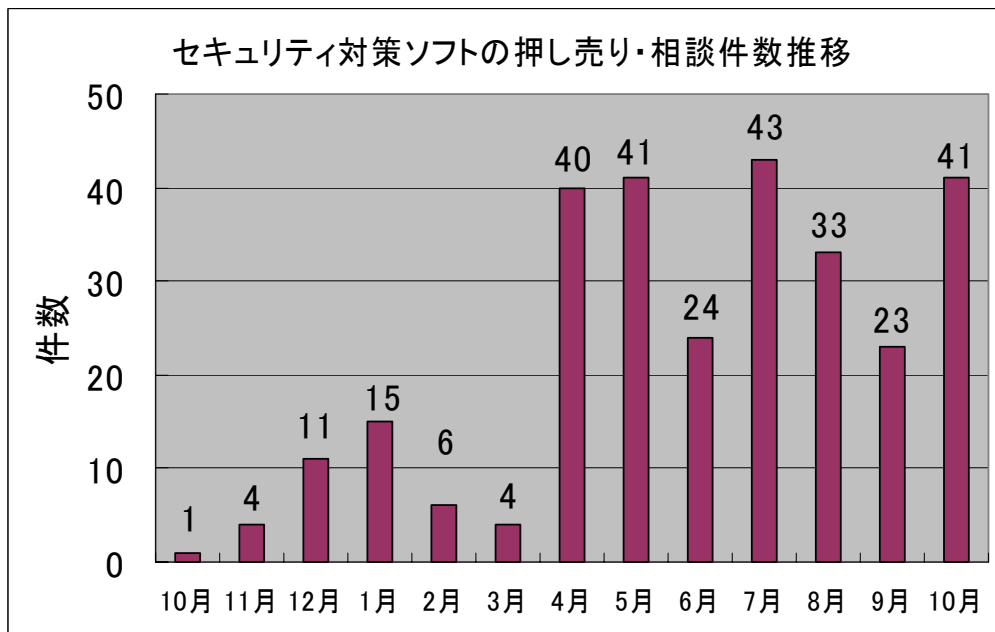
### (参考) ワンクリック不正請求相談件数の推移



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。

- 2006年2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?!」  
<http://www.ipa.go.jp/security/txt/2006/02outline.html>
- 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) 日本語の怪しいメールに添付ファイルが・・・

<p>相談</p>	<p>次のようなメールが届いた。差出人とは面識が無いので、添付ファイルは開かずに放置している。念のためウイルスチェックをしたが、何も検出されなかった。</p> <p>From:admin@●.●.jp To:●@●.co.jp Subject:あなたのパソコンがウイルスに感染している恐れがあります こんにちは。 私は(株)▲▲ ■■部の●田 ●●と申します。 弊社のサーバーコンピュータのログを調査しておりましたところ、あなたのコンピューターと思われる IP アドレスから 1 秒間に数十回もの不正アクセスを確認いたしました。 現在、弊社のサーバーは正常に稼働できない状態となっております。 これはあなたのコンピューターに仕掛けられたウイルスプログラムによる攻撃であると考えられます。 お送りしました delete_virus.exe ファイルを用いてウイルスを早急に削除されますよう、お願い申し上げます。 なお、この状態を放置されますと不正アクセス禁止法違反および威力業務妨害で司法手段に訴える可能性も検討しております。 早急に、対処されますようお願い申し上げます。 それでは、失礼いたします。 ウイルスの削除の仕方 1.パソコンの任意のフォルダに delete_virus.exe をコピーする。 2.delete_virus.exe をダブルクリックする。 ***** ●田 ●● 株式会社 ▲▲ ■■部 XXX-XXX-XXXX (代) admin@●.●.jp *****</p>
<p>回答</p>	<p>添付されていたファイルを改めてチェックしたところ、トロイの木馬型ウイルスが検出されました。今回のケースは、悪意のある人物が特定の宛先を狙ってウイルスを仕込もうとしている可能性があります。<b>身に覚えの無い差出人からのメールには注意し、特にファイルが添付されている場合は絶対に開かずに、メールごと削除してください。</b>メール本文は、添付ファイルを開かせようとして巧妙な言い回しになっている場合がほとんどですので、決して鵜呑みにすることのないよう、注意しましょう。</p>

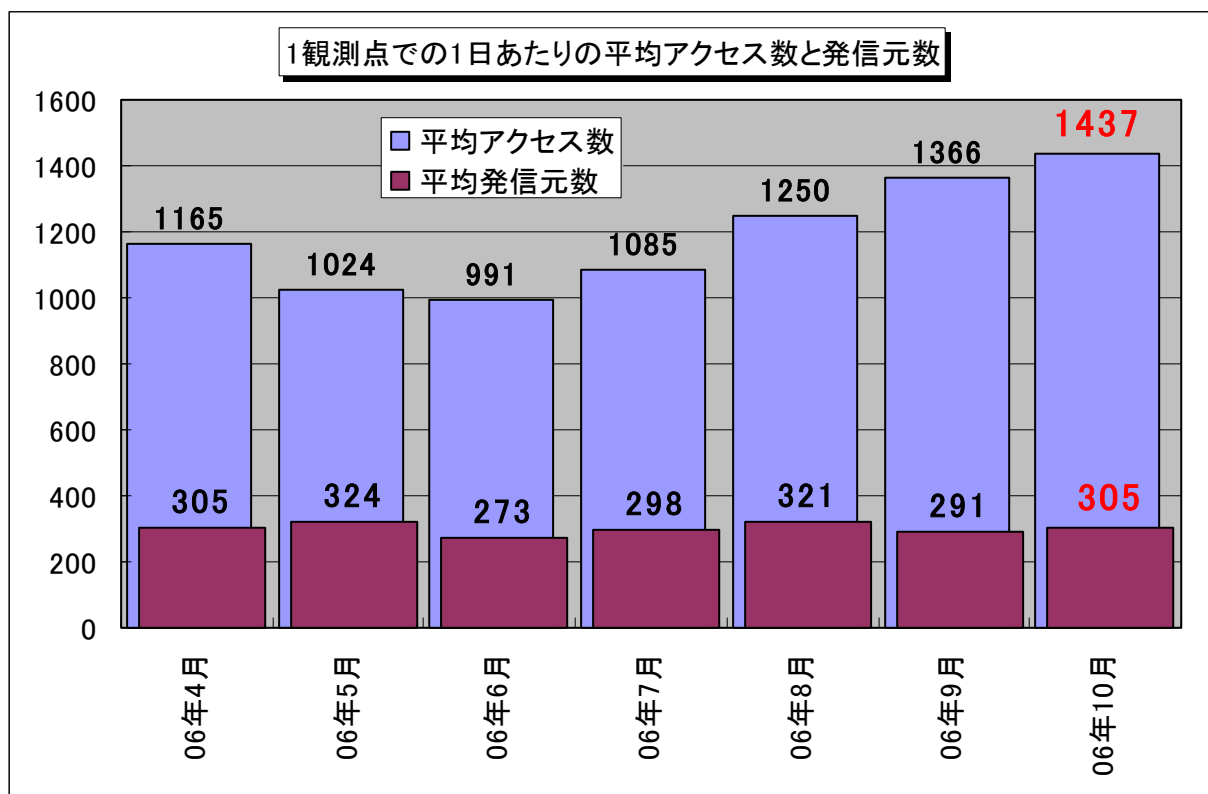
(ii) Winny で情報流出しているか確認できるか？

相談	以前 Winny を使っていた際、Antinny ウイルスに感染していたことが分かったので、Winny を使うのを止めた。ウイルスは駆除済みであるが、情報が流出しているかどうか調べる方法は無いか。パソコン内には、会社の情報もあったので心配。
回答	<p>一般の個人にとっては、<b>情報流出の有無を調べることは非常に難しいこと</b>です。専門の業者のサービスを利用するという選択肢もありますが、恐らく個人で支払うには非常に厳しい額になると思われます。<b>まずは自社や影響が及ぶと思われる関係先に一刻も早く報告し、善後策を検討しましょう。</b></p> <p><b>ファイル共有ネットワークに流出してしまったデータの回収は、事実上不可能</b>と言えます。ファイル共有ソフトの利用は、こうした危険と隣り合わせの行動であることを改めて認識しましょう。</p> <p>(ご参考)</p> <p>IPA - Winny による情報漏えいを防止するために <a href="http://www.ipa.go.jp/security/topics/20060310_winny.html">http://www.ipa.go.jp/security/topics/20060310_winny.html</a></p> <p>IPA - パソコンユーザのためのウイルス対策 7 箇条 <a href="http://www.ipa.go.jp/security/antivirus/7kajonew.html">http://www.ipa.go.jp/security/antivirus/7kajonew.html</a></p>

## 4. インターネット定点観測での10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10月の期待しない(一方的な)アクセスの総数は、10観測点で**416,676件**ありました。1観測点で1日あたり**305**の発信元から**1,437件**のアクセスがあったこととなります。

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、305人の見知らぬ人(発信元)から、発信元一人当たり5件の不正と思われるアクセスを受けている**ということになります。



【図 4.1 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4月～2006年10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4.1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、7月以降増加傾向です**。全体的なアクセス内容については、定常化していると言えます。

10月のアクセス状況は、全体的には9月とほぼ同じ状況ですが、ファイル交換関連と思われるポートへのアクセスが多い月でした。図4.2と図4.3を比較すると、これらのアクセスの多さが分かります。これらのファイル交換関連と思われるポートへのアクセスについては、統計情報から除外していますが、今月のトピックとして、これらのアクセスについて状況を説明します。

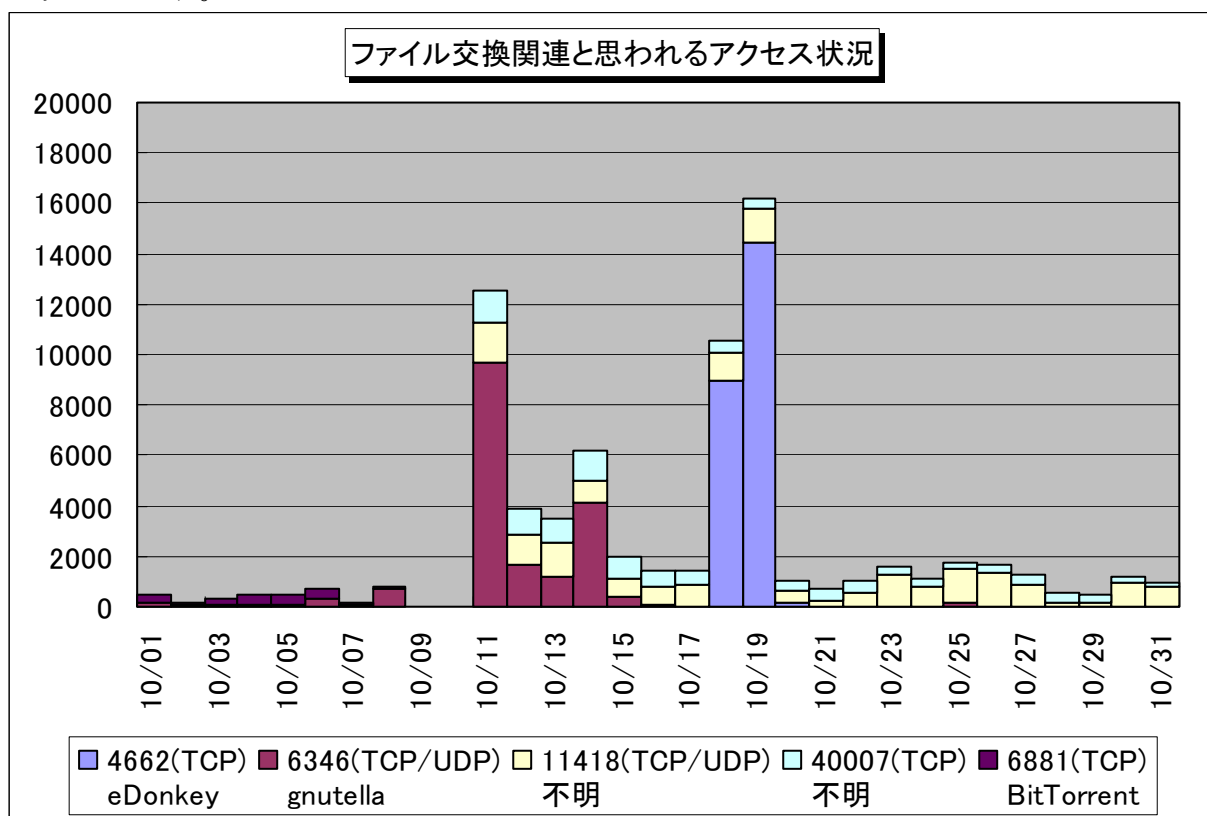
はじめにファイル交換について説明します。ファイル交換とは、ファイル交換ソフトを利用して特定のコンピュータどうしで直接ファイル(データ)を交換することです。

ファイル交換の方法にはいろいろありますが、ファイル交換を行うための情報を管理するサーバを中心としたファイル交換ネットワークを組む方式と、ファイル交換ソフトを介して数多くのコンピュータがファイル交換ネットワークを組む方式がほとんどです。

ファイル交換を行うコンピュータは、一般的に、そのコンピュータが使っているIPアドレスによっ

て特定されます。交換できるファイルの情報と、この IP アドレスの情報等がファイル交換ネットワーク上を流れることになります。

ところで、一般的なインターネットの利用者のコンピュータは、利用するプロバイダを介してネットワーク上の空いている IP アドレスを動的に割り当てられるのが普通です。そのため、ファイル交換を利用するコンピュータの IP アドレスも、ネットワークとの接続を行うたびに、違う IP アドレスになります。このため、ファイル交換を行っていたコンピュータがネットワークから切断されても、ファイル交換ネットワーク上には、以前使っていた IP アドレスの情報が残ってしまう場合があります。この残ってしまった IP アドレスが、同じプロバイダ内の違う利用者のコンピュータに割り当てられ、このコンピュータに対して、同じファイル交換を利用する別のコンピュータからファイル交換の接続要求(アクセス)がくることになります。以下に示すアクセスのほとんどが、このような状況で発生したアクセスと考えられます。



【図 4.2 2006 年 10 月のファイル交換関連と思われるアクセス数の遷移】

これらのアクセスの発信元については、以下の通り

- ・ 4662(TCP)ポートへのアクセスの発信元はスペイン方面がほとんど(図 2.1.2 参照)
- ・ 6346(TCP/UDP)ポートへのアクセスの発信元は日本国内がほとんど
- ・ 11418(TCP/UDP)ポートへのアクセスの発信元は台湾方面がほとんど
- ・ 40007(TCP)ポートへのアクセスの発信元も日本国内がほとんど
- ・ 6881(TCP)ポートへのアクセスの発信元も日本国内がほとんど

でした。

著作権のあるデータ(ファイル)を非合法にファイル交換する人たちがいるため、最近ではサーバを中心に持つタイプのファイル交換では、サーバが閉鎖に追い込まれたり、違法なファイル交換を行った人が逮捕されたりという事件も起こっています。

さらに、ファイル交換を介した情報漏えいの問題も多発しているため、ファイル交換を問題視する傾向もあるようです。

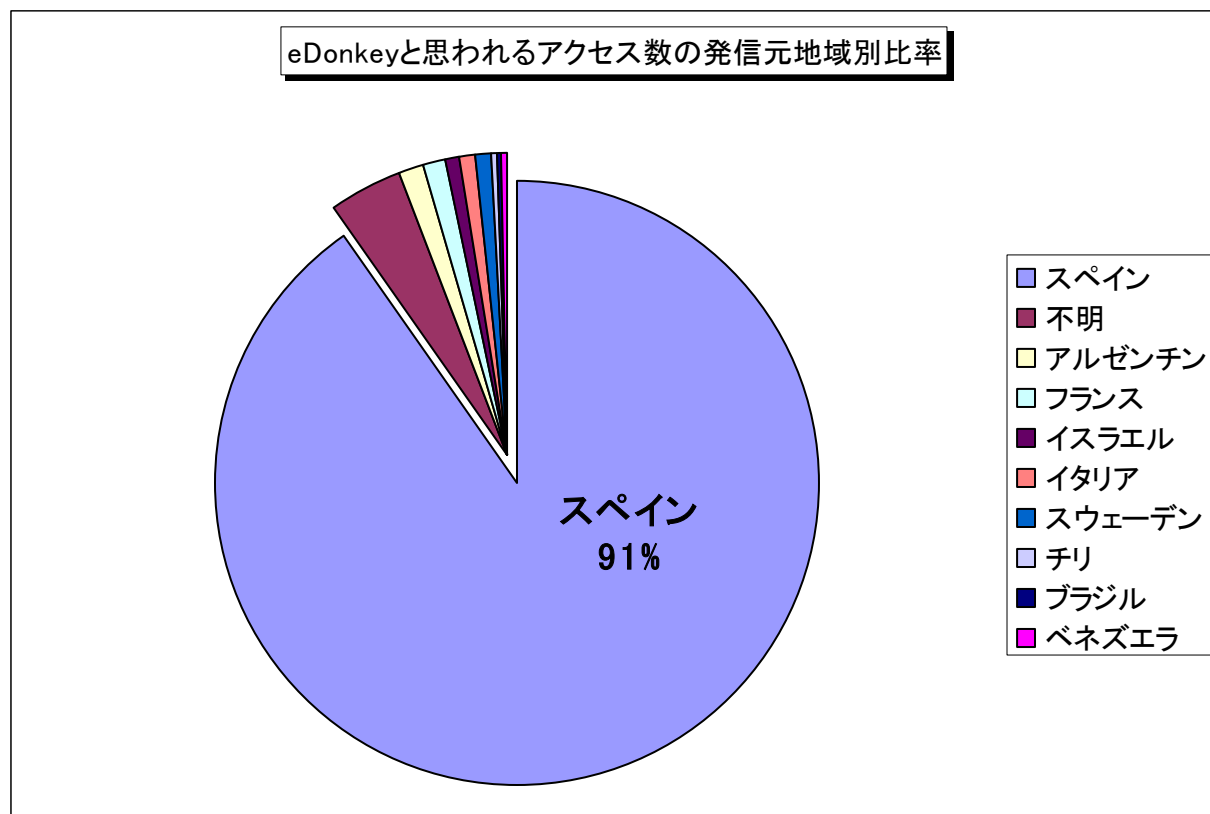
図 4.2 に示した、一番アクセス数の多かった 4662(TCP)は、eDonkey と呼ばれるファイル交換ソフトを利用したアクセスのようです。eDonkey については、欧州を中心に eDonkey のサーバの閉鎖やファイル交換ソフトの配布停止となったために、残ったサーバが閉鎖される前に、駆け込み的に

ファイルをダウンロードしようと、急激にアクセスが増加したものと考えられます。

#### 参考情報

■ 国際レコード産業連盟、違法ファイル交換に対し 17 カ国で 8,000 件の訴訟 (2006/10/18)

<http://internet.watch.impress.co.jp/cda/news/2006/10/18/13661.html>



【図 4.3 eDonkey とと思われるアクセス数の発信元地域別比率】

特定のIPアドレスに、このようなアクセスが集中すると、ほとんどDoS攻撃を受けている状況となります。このようなアクセスは、ほとんどがファイル交換を自動化した場合に発生するものであり、ファイル交換の利用者の方には、このような状況を理解いただき、ファイル交換の接続先の確認をあらかじめ行ってから、アクセスするように心掛けていただきたいと思います。

さらに、ファイル交換を介した情報漏えい問題も多発していますので、利用者には、ファイル交換の仕組みをご理解いただき、さらなる注意を払っていただきたいと思います。

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/TALOT2-0611.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) ルートキット (rootkit)

攻撃者がコンピュータに侵入した後に利用するためのソフトウェアをまとめたパッケージのこと。一般的には、ログ改ざんツールやバックドアツール、改ざんされたシステムコマンド群などが含まれる。

### (\*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) 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。総当た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。

#### \*:総当たり攻撃

何らかの規則にしたがって、文字の組み合わせを総当たりで試行する攻撃方法のこと。いわゆる力づくの攻撃方法のことで、ブルートフォース攻撃ともいう。

#### \*: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。

### (\*5) 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。

### (\*6) ボット (bot)

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。

### (\*7) ポートスキャンツール

サーバ内で動作しているアプリケーションや、OS の種類の情報などから、セキュリティホールを探すためのツール。侵入の準備行為に利用されることが多い。

### (\*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) **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。

(\*12) **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。

■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**

**「情報セキュリティ標語・ポスター2007」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：2006年12月1日(金)～2007年3月31日(土)

応募方法：電子メール・FAX・郵送（詳細はホームページにて近日公開予定）

賞金：特賞（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）

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・中山

Tel: 03-5978-7508

Fax: 03-5978-7518

E-mail: isec-hyogo@ipa.go.jp

## お知らせ



### 『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)**」をウェブ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)

<http://www.ipa.go.jp/security/benchmark/>

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。

## お知らせ

### IPA では、対策のしおりシリーズを提供しています！

情報セキュリティ対策のための「ウイルス対策のしおり」、「ボット対策のしおり」、「スパイウェア対策のしおり」、「不正アクセス対策のしおり」、「情報漏えい対策のしおり」を作成・提供しております。

本対策のしおりは、一般のご家庭や企業（組織）内でパソコンをご利用する方々を対象に、情報セキュリティ上の様々な脅威への対策を分かりやすく説明したものです。気軽に読んでいただけるよう、挿絵を多用し、それぞれの脅威の概要、仕組み、対策を理解し、把握できるように工夫しております。これらの脅威への対策を実践するために、ぜひご活用ください。

#### 対策のしおりシリーズ

- (1)ウイルス対策、(2)スパイウェア対策、(3)ボット対策、(4)不正アクセス対策、および
- (5)情報漏えい対策

<http://www.ipa.go.jp/security/antivirus/shiori.html>