INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
第 09-19-151-2 号
最終更新日：2009 年 5 月 22 日
掲載日：2009 年 5 月 7 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 [2009 年 4 月分] について

IPA(独立行政法人情報処理推進機構、理事長：西垣 浩司)は、2009 年 4 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

**「USB メモリのセキュリティ対策を意識していますか？」**
**― USB メモリの安全な使い方を知ろう ―**

IPA ではこれまでに何度か USB メモリのセキュリティ対策に関する呼びかけを行っています。しかし、依然として USB メモリを介して感染するウイルスの相談や届出が寄せられています。

このような状況の中、USB メモリを介して感染を拡大するウイルスによる被害が、ここ最近、相次いで発生しています。2 月に、大学病院のシステムがウイルスに感染し、大規模なシステム障害が発生しました。ウイルスは、ネットワークを通じて 1,000 台以上のパソコンに感染し、感染源は USB メモリだったと報じられました。また、3 月には、地方自治体で同様のウイルスによる大規模なシステム障害が発生しました。

セキュリティ対策を意識しないで USB メモリを使用することは、思いがけない被害を招くことになります。USB メモリを利用する際のセキュリティ対策を改めて確認し、USB メモリの安全な使い方を知ってください。

### （1）USB メモリ利用時のセキュリティ対策の実態

「2008 年度第 2 回情報セキュリティに関する脅威に対する意識調査」で、USB メモリにおけるセキュリティ対策に関する質問を行いました。

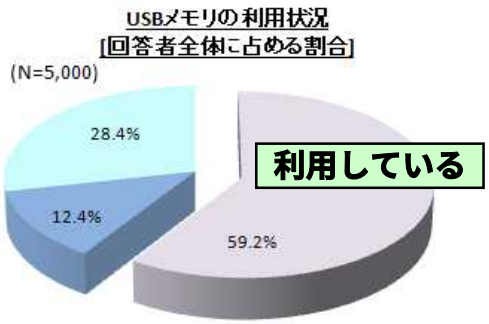



図 1-1: USB メモリの利用状況[回答者全体に占める割合]

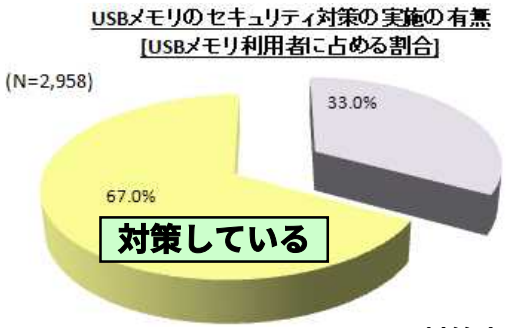



図 1-2: USB メモリのセキュリティ対策実施の有無 [USB メモリ利用者に占める割合]

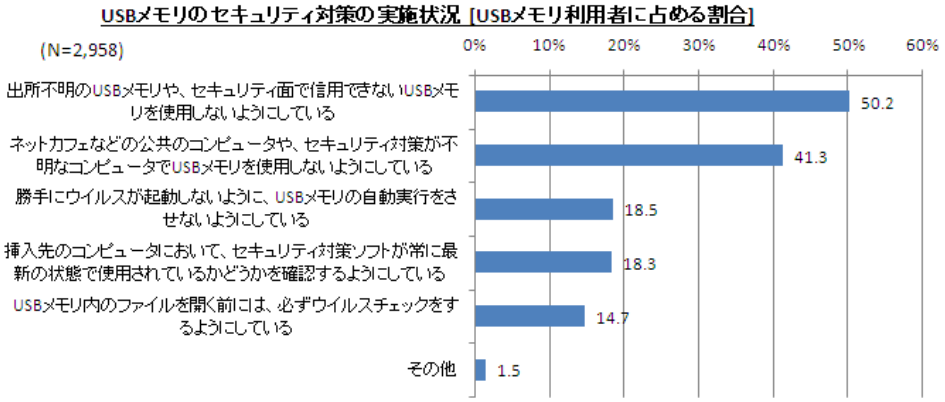



図 1-3: USB メモリのセキュリティ対策実施状況[USB メモリ利用者に占める割合]

図 1-1 によると、USB メモリの利用者の割合は、回答者全体の約 60%を占めています。また、図 1-2 によると、USB メモリ利用者の中で、USB メモリのセキュリティ対策を実施しているという利用者は 3 人中 2 人にとどまっているという結果が出ています。

(ご参考)

「2008 年度第 2 回情報セキュリティに関する脅威に対する意識調査」(IPA)

http://www.ipa.go.jp/security/fy20/reports/ishiki02

## (2) 利用面での対策

IPA では、従来から USB メモリについて、以下のような利用面での対策を実施することを推奨してきました。

- 自身が管理していないパソコンや不特定多数が利用するパソコンに、むやみに自身の USB メモリを挿さない。
- 自身が管理していない USB メモリや所有者不明な USB メモリを、むやみに自分のパソコンに挿さない。

しかし、図 1-3 の、USB メモリセキュリティ対策を実施している利用者の詳細をみると、「出所不明の USB メモリや、セキュリティ面で信用できない USB メモリを使用しないようにしている」や、「ネットカフェなどの公共のコンピュータや、セキュリティ対策が不明なコンピュータで USB メモリを使用しないようにしている」などの基本的な対策を行っている利用者が、半数程度、もしくはそれ以下という結果が出ています。

USB メモリを利用している利用者は、IPA が推奨する利用面での対策を行うことをお勧めします。

## (3) 技術的な対策指針

図 1-3 によれば、「勝手にウイルスが起動しないように、USB メモリの自動実行をさせないようにしている」といった対策を実施している利用者は、2 割にも満たないという結果が出ています。

自動実行機能とは、USB メモリをパソコンに挿した際、または USB メモリを認識したドライブをダブルクリックした際に、ファイルが自動的に実行される Windows の機能のことです。この機能のことを Autorun(オートラン)機能と呼ぶ場合もあります。

USB メモリを介して感染を拡大するウイルスは、接続対象のパソコンに感染するために自動実行機能を悪用します。このようなウイルスの感染を防ぐ確実な対策の一つとして自動実行機能の無効化があります。

この対策は、現在 USB メモリを利用していない利用者でも、今後、自身のパソコンに USB メモリを挿すことはないと言い切れない場合は、実施しておくことをお勧めします。

## (4) USB メモリの自動実行機能を無効化する方法

2009 年 2 月 24 日にマイクロソフト社から自動実行機能の無効化を適切に行うための更新プログラム、および手順が公開されました。

(ご参考)

「Windows の自動実行機能を無効にする方法」(マイクロソフト社)

http://support.microsoft.com/kb/967715/ja

今回は、上述の情報を基に、USB メモリの自動実行機能の無効化を実施する利用者を増やし、安全に USB メモリを利用してもらう目的で、この対策についての詳細な手順を説明することとします。

Windows のバージョンによって手順が異なりますので、自身のパソコンに対応した手順に従って実施してください。Windows のバージョンの確認方法については以下のサイトを参照してください。

(ご参考)

「Windows のバージョン確認方法」(マイクロソフト社)

http://www.microsoft.com/japan/security/bulletins/ver_win.mspx

Windows のバージョンを確認した上で、自身のパソコンに対応した方法で自動実行機能の無効化を実施してください。各バージョンに対応した方法については以下の表 1-1 に従ってください。

なお、以降で解説する方法を実施することで、USB メモリ以外のすべての外部記憶メディアにおいても、自動実行機能を無効化することになります。すなわち、CD や DVD の自動実行機能も無効化されることになりますので、注意してください。

表 1-1: USB メモリの自動実行機能を無効化する方法に関する Windows のバージョン毎の対応表

| Windows のバージョン | Vista Ultimate | Vista Business | Vista Home Premium | Vista Home Basic | XP Professional Edition | XP Home Edition | 2000 |
|---|---|---|---|---|---|---|---|
| | 方法 A | 方法 A | 方法 B | 方法 B | 方法 C | 方法 D | 方法 C |

また、これらすべての方法において、処置を誤ると深刻な問題が発生することがあります。処置を実施する際には十分注意してください。万一に備えて、以下のサイトを参考に、事前に「システムの復元」のポイントを作成してください。問題が発生した場合でも、処置前に作成した復元ポイントを指定して、「システムの復元」を実施することで状態を復元することができます。

(ご参考)

Windows Vista のシステムの復元の解説（マイクロソフト社の「PC とーく」の情報）

http://support.microsoft.com/kb/934854/ja

「システムの復元　Windows XP」（マイクロソフト社）

http://www.microsoft.com/japan/windowsxp/pro/business/feature/performance/restore.mspx

**(a)Windows Vista の場合**

＜共通＞

Windows Vista の場合、「CD または他のメディアの自動再生」(※)の「ソフトウェアとゲーム」項目の設定(図 1-4 参照)によって、USB メモリを挿した時の動作が決定されています。しかも前回 USB メモリを挿した時の動作によってその設定が変更されますので、本来、利用者は毎回この設定を確認する必要があります。そこで、USB メモリを挿した時に、勝手にプログラムが自動実行されないようにするためには、ここで設定するのではなく、以下に述べる方法で自動実行機能を根本的に無効化することが適切な方法です。

まず、前提条件として Windows Vista 用の更新プログラム(KB950582)が適用されている必要があります。適用されている更新プログラムの確認方法については以下のサイトを
参照してください。

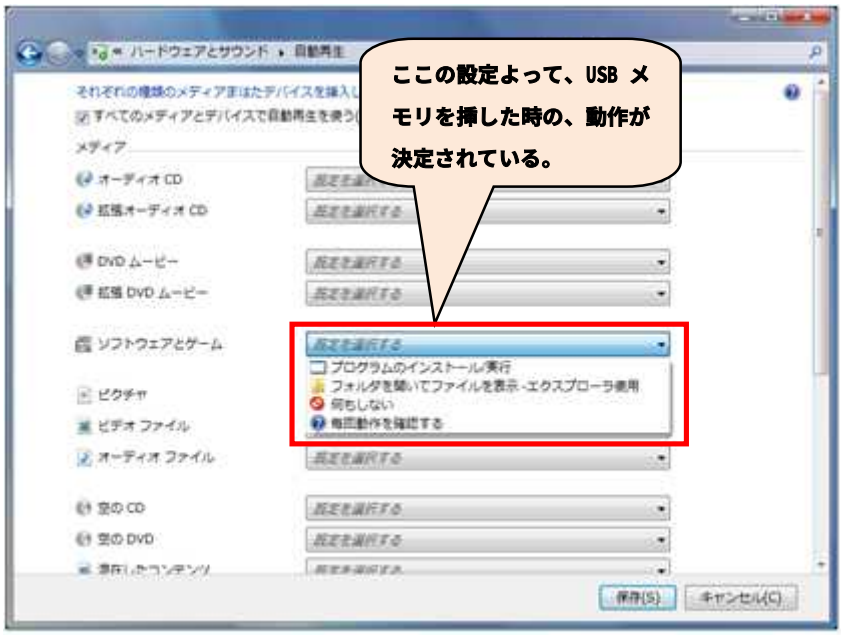



図 1-4:Windows Vista の「CD または他のメディアの自動再生」の設定画面例

※「CD または他のメディアの自動再生」：「スタート」ボタンをクリック→「コントロールパネル」をクリック→「ハードウェアとサウンド」項目の中の、「CD または他のメディアの自動再生」をクリックすると図 1-2 の設定画面が表示されます。

(ご参考)
「更新プログラムが正しくインストールされたか確認する方法 - Windows Vista の場合」(マイクロソフト社)
http://www.microsoft.com/japan/security/bulletins/inst_history_vista.mspx

以上の更新プログラムが適用されていることを確認した上で、Windows Vista Ultimate、および Windows Vista Business の場合は、以下の＜方法 A>で自動実行機能を無効化させます。

＜方法 A＞

1.[スタート]ボタンをクリックし、[検索の開始] ボックスに「Gpedit.msc」と入力し、Enter キーを押し、ローカルグループポリシーエディタ画面を表示させます。管理者のパスワードを要求するダイアログボックスが表示された場合は、パスワードを入力して [OK] をクリックし、確認を要求するダイアログボックスが表示された場合は [続行] をクリックします。パスワードがわからない場合は、管理者にパスワードを確認してください。
2. [コンピュータの構成]、[管理用テンプレート]、[Windows コンポーネント] を順に展開し、[自動再生のポリシー] をクリックします。
3. 詳細ウィンドウ領域で、[自動再生機能をオフにする] をダブルクリックし、設定画面を表示させます。(図 1-5 参照)。
4. 設定画面の中の[有効] をクリックし、[自動再生機能をオフにする] ボックスの [すべてのドライブ] を選択し、すべてのドライブで自動実行を無効にします。
5. [OK] をクリックしてから、ローカルグループポリシーエディタ画面を終了します。
6. コンピュータを再起動します。

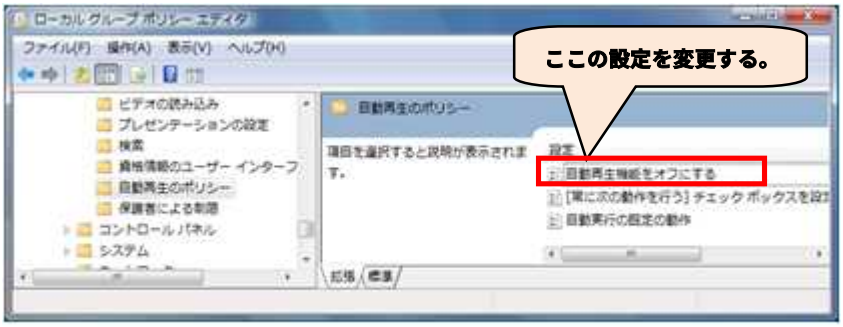


図 1-5:Windows Vista のグループポリシー画面例

Windows Vista Home Basic、および Windows Vista Home Premium の場合は、グループポリシーエディタ画面が利用できないため、＜方法 A＞は使えませんが、レジストリ情報を変更することで自動実行機能を無効化させることができます。
以下の＜方法 B＞で自動実行機能を無効化させます。

＜方法 B＞

1. [スタート] ボタンをクリックし、[ファイル名を指定して実行] をクリックします。[名前] ボックスに「regedit」と入力し、[OK] をクリックし、レジストリエディタ画面を表示させます。
2. レジストリエディタ画面で次のフォルダを見つけ、クリックします。
[HKEY_LOCAL_MACHINE](※) → [SOFTWARE] → [Microsoft] → [Windows] → [CurrentVersion] → [policies]→[Explorer]
3. [Explorer] を右クリックし、メニューから[新規]－[DWORD(32 ビット)値]と選択し、フォルダ内に作成された[新しい値]に[NoDriveTypeAutoRun] と設定します。[NoDriveTypeAutoRun] を右クリックし、メニューから、[修正]を選択します(図 1-6 参照)。
4. すべての自動実行機能を無効化するには、[値のデータ] ボックスに「0xFF」と入力します。
5. [OK] をクリックしてから、レジス

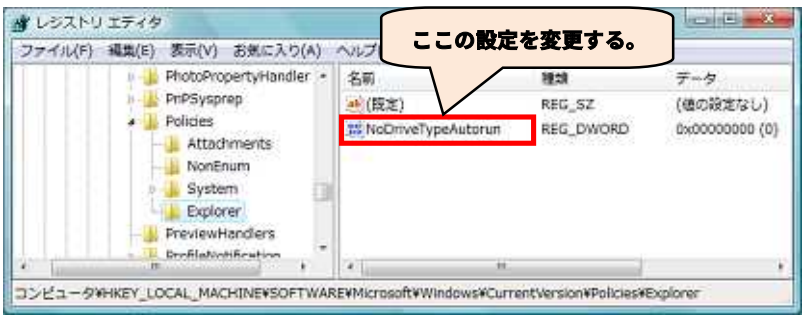


図 1-6:Windows Vista のレジストリエディタ画面例

トリエディタ画面を終了します。

6. コンピュータを再起動します。

※パソコンの全てのユーザに対して、自動実行機能を無効化させるため、[HKEY_CURRENT_USER]から、[HKEY_LOCAL_MACHINE]に変更。(2009 年 5 月 22 日修正)

以上のいずれかの方法を行うことで、「CD または他のメディアの自動再生」の設定に関係なく、USB メモリを挿しても常に自動再生の画面さえも出力されなくなるため、ウイルスが自動実行される危険性は解消されます。

**(b)Windows XP、および Windows 2000 の場合**

＜共通＞

Windows XP、および Windows 2000 の場合、USB メモリをパソコンに挿すときにプログラムが自動実行されることはありませんが、「マイコンピュータ」から USB メモリを認識したドライブをダブルクリックすると、プログラムが実行される危険性があります(図 1-7 参照)。この危険性を解消するためには、自動実行機能を無効化することが適切な方法です。

まず、前提条件として Windows XP 用更新プログラム(KB967715)、もしくは Windows 2000 用更新プログラム(KB967715)、もしくは更新プログラム(KB953252)が適用されている必要があります。適用されている更新プログラムの確認方法については以下のサイトを参照してください。

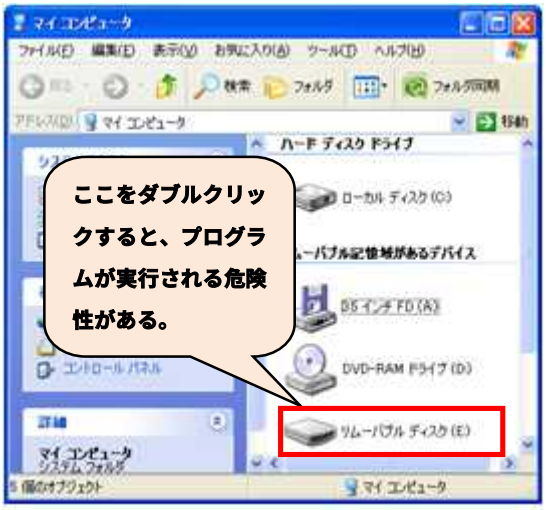



図 1-7:Windows XP のマイコンピュータ画面例

(ご参考)

「更新プログラムが正しくインストールされたか確認する方法」(マイクロソフト社)

http://www.microsoft.com/japan/security/bulletins/inst_history.mspx

以上の更新プログラムが適用されていることを確認した上で、Windows XP professional Edition および、Windows 2000 の場合は、以下の＜方法 C＞で自動実行機能を無効化させます。

＜方法 C＞

1. [スタート] ボタンをクリックし、[ファイル名を指定して実行] をクリックします。[名前] ボックスに「Gpedit.msc」と入力し、[OK] をクリックし、グループポリシー画面を表示させます。
2. [コンピュータの構成]、[管理用テンプレート]を順に展開し、[システム] をクリックします(図 1-8 参照)。
3. 設定ウィンドウで、[自動再生機能をオフにする] をダブルクリックし、設定画面を表示させます。(Windows 2000 では、ポリシー設定の名前は [自動再生機能を無効にする] です。)
4. 設定画面の中の [有効] をクリックし、[自動再生機能をオフにする] ボックスの [すべてのドライブ] を選択し、すべ

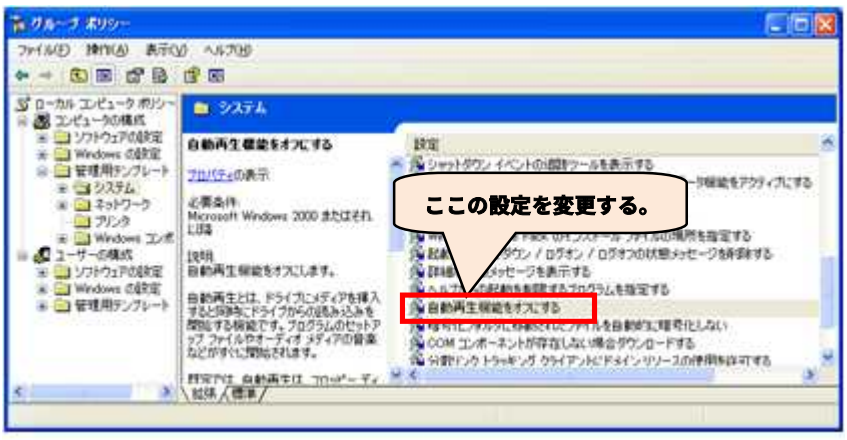



図 1-8:Windows XP のグループポリシー画面例

てのドライブで自動実行を無効にします。

5. [OK] をクリックしてから、グループポリシー画面を終了します。
6. コンピュータを再起動します。

Windows XP Home Edition の場合は、グループポリシー画面が利用できないため、＜方法 C＞は使えませんが、レジストリ情報を変更することで自動実行機能を無効化させることができます。
以下の＜方法 D＞で自動実行機能を無効化させます。

＜方法 D＞

1. [スタート] ボタンをクリックし、[ファイル名を指定して実行] をクリックします。[名前] ボックスに「regedit」と入力し、[OK] をクリックし、レジストリエディタ画面を表示させます。
2. レジストリエディタ画面で次のフォルダを見つけ、クリックします。
   [HKEY_LOCAL_MACHINE](※) → [SOFTWARE] → [Microsoft] → [Windows] → [CurrentVersion] → [policies]→[Explorer]
3. [Explorer] を右クリックし、メニューから[新規]－[DWORD 値]と選択し、フォルダ内に作成された[新しい値]に[NoDriveTypeAutoRun] と設定します。[NoDriveTypeAutoRun]を右クリックし、メニューから、[修正]を選択します(図 1-9 参照)。
4. すべての自動実行機能を無効化するには、 [値のデータ] ボックスに「0xFF」と入力します。
5. [OK] をクリックしてから、レジストリエディタ画面を終了します。
6. コンピュータを再起動します。

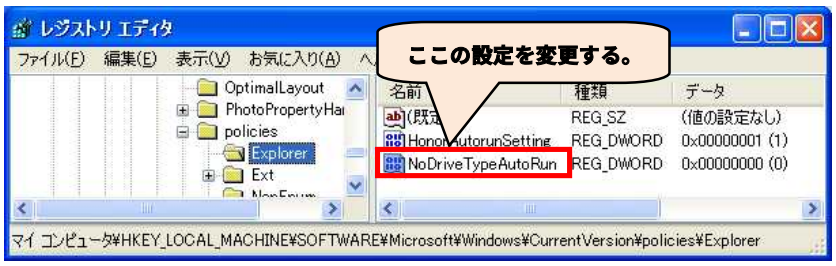



図 1-9:Windows XP のレジストリエディタ画面例

※パソコンの全てのユーザに対して、自動実行機能を無効化させるため、[HKEY_CURRENT_USER]から、[HKEY_LOCAL_MACHINE]に変更。(2009 年 5 月 22 日修正)

以上のいずれかの方法を行うことで、「マイコンピュータ」から USB メモリを認識したドライブをダブルクリックしてもプログラムは実行されず、ファイルの一覧が表示されるだけとなりますので、ウイルスが自動実行される危険性は解消されます。

(ご参考)
「パソコンユーザのためのウイルス対策 7 箇条」
http://www.ipa.go.jp/security/antivirus/7kajonew.html
「パソコンユーザのためのスパイウェア対策 5 箇条」
http://www.ipa.go.jp/security/antivirus/spyware5kajyou.html

## 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、8 頁の「3.コンピュータ不正アクセス届出状況」を参照)
- SSH で使用するポートへの攻撃で侵入された
- フィッシングサイトを設置された

○ 相談の主な事例 (相談受付状況及び相談事例の詳細は、10 頁の「4.相談受付状況」を参照)
- 怪しいメールの添付ファイルを開いたらウイルス感染？
- 不正アクセスされているかも知れない

○ インターネット定点観測(12 頁参照。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。

## 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 15.6 万個と、3 月の約 11.9 万個から 31.3%の増加となりました。**
**また、4 月の届出件数(※2)は、1,438 件となり、3 月の 1,674 件から 14.1%の減少となりました。**

※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。
・4 月は、寄せられたウイルス検出数約 15.6 万個を集約した結果、1,438 件の届出件数となっています。

**検出数の 1 位は、W32/Netsky で約 10.5 万個、2 位は W32/Downad で約 4 万個、3 位は W32/Mytob で約 3 千個でした。**

**ウイルス検出数　約15.6万個（約11.9万個）　前月比 +** 31.3%

**(注：括弧内は前月の数値)**

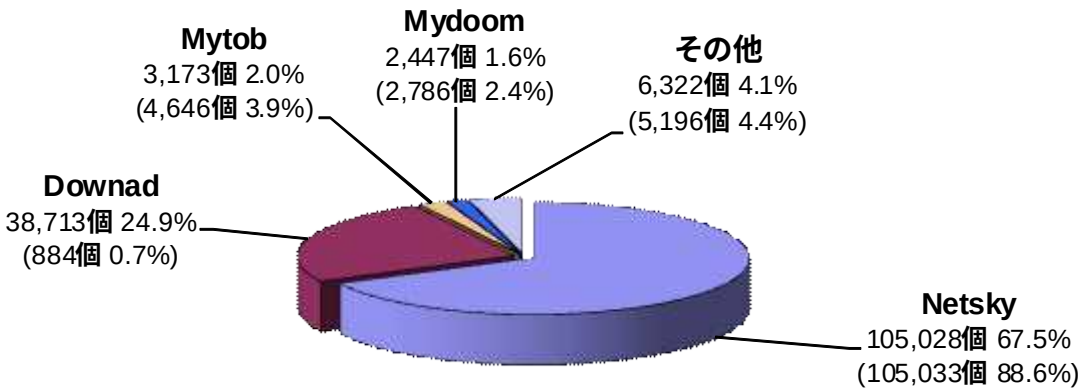



**図 2-1：ウイルス検出数**

**ウイルス届出件数** 1,438**件（**1,674**件）前月比** - 14.1%

**(注：括弧内は前月の数値)**

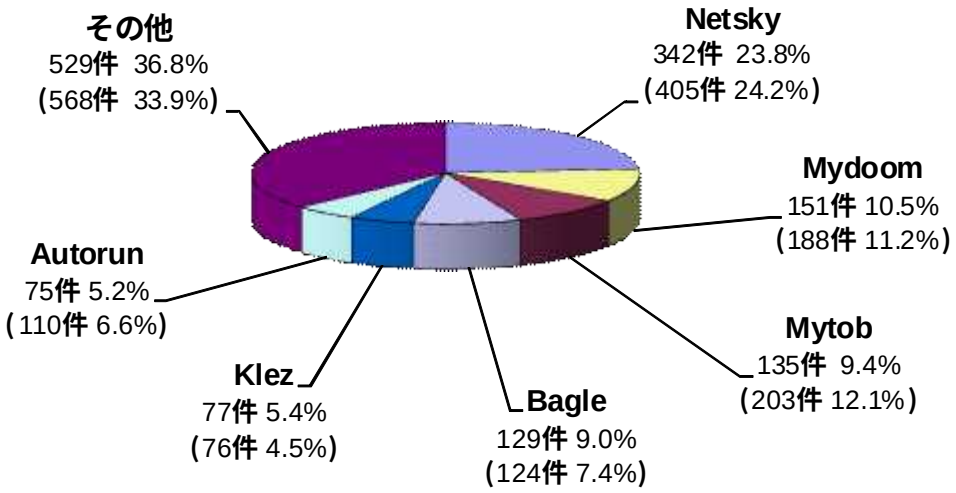



**図 2-2：ウイルス届出件数**

## 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－

**表 3-1　不正アクセスの届出および相談の受付状況**

| | | 11月 | 12月 | 1月 | 2月 | 3月 | 4月 |
|---|---|---|---|---|---|---|---|
| 届出(a) 計 | | 18 | 10 | 10 | 9 | 20 | 9 |
| | 被害あり(b) | 12 | 7 | 7 | 6 | 13 | 6 |
| | 被害なし(c) | 6 | 3 | 3 | 3 | 7 | 3 |
| 相談(d) 計 | | 39 | 38 | 29 | 35 | 40 | 39 |
| | 被害あり(e) | 19 | 19 | 13 | 14 | 11 | 11 |
| | 被害なし(f) | 20 | 19 | 16 | 21 | 29 | 28 |
| 合計(a+d) | | 57 | 48 | 39 | 44 | 60 | 48 |
| | 被害あり(b+e) | 31 | 26 | 20 | 20 | 24 | 17 |
| | 被害なし(c+f) | 26 | 22 | 19 | 24 | 36 | 31 |

### (1)不正アクセス届出状況

4 月の届出件数は 9 件であり、そのうち何らかの被害のあったものは 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 39 件であり、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 3 件、なりすまし 1 件、不正プログラム埋込 1 件、**などでした。

「侵入」の被害は、ウェブサーバ上に運営者が意図しないコンテンツを設置されていたものが 2 件(内 1 件はフィッシング※に悪用するためのコンテンツ)、不正プログラムを置かれていたものが 1 件、でした。侵入の原因は、セキュリティ設定の不備が 1 件、SSH※で使用するポートへのパスワードクラッキング※攻撃と思われるものが 1 件、でした(残りの 1 件は原因不明)。

※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ウェブページを装い、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。
※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。
※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。ブルートフォース攻撃(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。

## (4)被害事例

### [侵入]

#### (i) SSH で使用するポートへの攻撃で侵入された

| | |
|---|---|
| 事例 | ・社内のデータセンター部門からの連絡で、自部門のサーバが不正アクセスを受けていたことが判明。<br>・調査の結果、「/home/tomcat/.bot」ディレクトリに不正なプログラムが置かれているのを発見。<br>・SSH で使用するポートにパスワードクラッキング攻撃を受け、パスワードが破られたのが原因と思われた。<br>・パスワードは 8 文字以上にしてあった。 |
| 解説・対策 | パスワード認証は、時間を掛ければいつかは破られる、という原則を再認識しましょう。ログのチェック、接続許可制限などの対策が有効ですが、SSH 運用時には、ログインの際に公開鍵認証※などの強固な認証の採用を推奨します。<br>(参考)<br>IPA - 安全なウェブサイトの作り方<br>http://www.ipa.go.jp/security/vuln/websecurity.html |

※公開鍵認証…公開鍵と秘密鍵のペアで利用者個人の認証を行う方式のこと。

#### (ii) フィッシングサイトを設置された

| | |
|---|---|
| 事例 | ・サーバをレンタルで利用している。ある日、レンタル業者から、「不正なコンテンツが置かれているのでは？」との連絡があった。<br>・調査したところ、ウェブサーバ上にフィッシングに悪用するための不正なコンテンツを設置されていたことが判明。<br>・ログが消されていた上に、ps や ls などの基本コマンドが不正なものに置き換えられていたために調査が難航し、結局、原因究明には至らなかった。 |
| 解説・対策 | システムコマンドが不正なものに置き換えられていますので、ルートキット※を埋め込まれている可能性が非常に高いと言えるでしょう。この場合、侵入・改ざんの影響範囲を正確に把握することが困難ですので、サーバは再構築することが基本となります。なお、サーバ再構築後は、脆弱性の解消・不要なプログラムの削除・不要なサービスの停止を確実にするとともに、ログのチェックを密にして侵入の兆候に一刻も早く気付くことが大切です。<br>(参考)<br>IPA - 安全なウェブサイトの作り方<br>http://www.ipa.go.jp/security/vuln/websecurity.html |

※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。動作中のプロセスやファイル、システム情報などを不可視化し、これらツール群の存在が利用者に察知されないようになっていることが多い。

## 4．相談受付状況

4 月の相談総件数は 1,668 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 572 件(3 月：503 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 3 件(3 月：3 件)、Winny に関連する相談が 4 件(3 月：6 件)、「情報詐取を目的として特定の組織に送られる不審なメール」に関する相談が 0 件(3 月：1 件)、などでした。

表 4-1　IPA で受け付けた全ての相談件数の推移

| | 11月 | 12月 | 1月 | 2月 | 3月 | 4月 |
|---|---|---|---|---|---|---|
| 合計 | 713 | 839 | 960 | 1,051 | 1,406 | 1,668 |
| 自動応答システム | 363 | 458 | 529 | 521 | 758 | 962 |
| 電話 | 288 | 331 | 390 | 472 | 597 | 651 |
| 電子メール | 62 | 49 | 39 | 57 | 49 | 55 |
| その他 | 0 | 1 | 2 | 1 | 2 | 0 |

※ 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)、fushin110@ipa.go.jp(不審メール 110 番)、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。

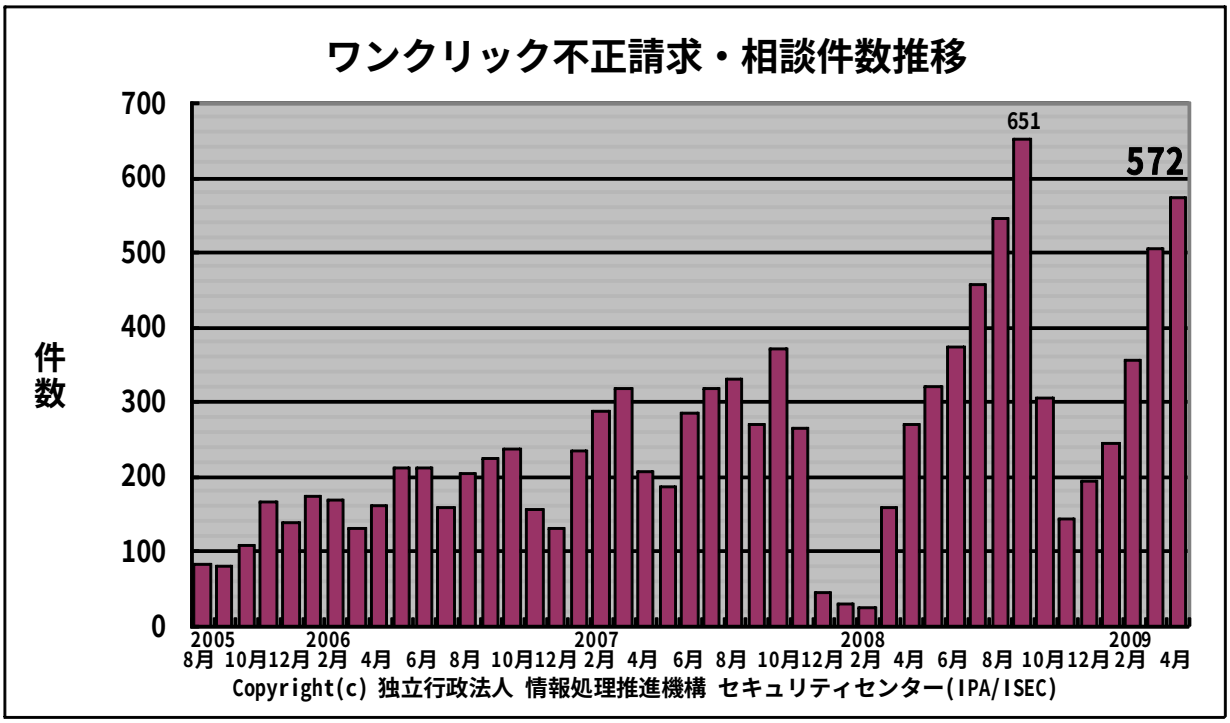



図 4-1　ワンクリック不正請求相談件数の推移

主な相談事例は以下の通りです。

### (i) 怪しいメールの添付ファイルを開いたらウイルス感染？

| | |
|---|---|
| **相談** | 無料で使えるウェブメールで、身に覚えのないメールが自分宛に送られて来た。そのメール添付ファイルをウイルス対策ソフトでチェックしたら問題無かったので、ファイルを保存して開いたら、デスクトップ一面にエラー表示がたくさん出て来るようになった。ウイルスに感染したのか。パソコンは、初期化した。 |
| **回答** | 当該ファイルを様々なウイルス対策ソフトでチェックしたところ、複数のソフトでウイルスを検知しました。あるウイルス対策ソフトで何も検知されなくても、他のウイルス対策ソフトではウイルスとして検知される場合があります。特に、**身に覚えのないメールの添付ファイルや出所の不明なファイルなどは、ウイルスチェックなどする以前に、開こうとしてはいけません。**<br>もし、どうしても開く必要がある、ということであれば、当該ファイルをできるだけ多くのウイルス対策ソフトで検査してみることをお勧めします。「VIRUS TOTAL」は、オンラインで疑わしいファイルを解析してくれるサービスです。無償で、同時に 40 種類程度のウイルス対策ソフトによるチェックが可能です。<br>(ご参考)<br>VIRUS TOTAL<br>http://www.virustotal.com/jp/ |

### (ii) 不正アクセスされているかも知れない

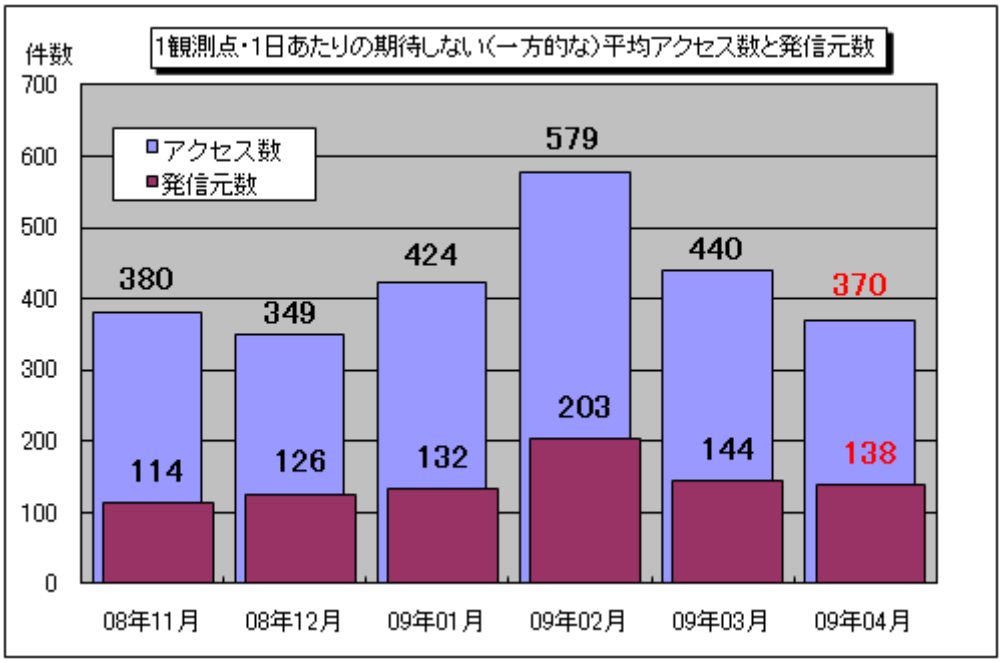
| | |
|---|---|
| **相談** | 数年前から、不正アクセスを受けてパソコンを乗っ取られていると思う。症状は、<br>・ウイルス対策ソフトの動きを無効化される<br>・パソコンをシャットダウンしようとすると、「誰かログインしている」と出る<br>どうすれば良いか。無線 LAN を利用している。 |
| **回答** | 今のままだと**原因究明は難しいため、一度パソコンを初期化し、以下の手順で様子を見ることで、問題を切り分けていくことをお勧めします。**<br>・パソコン、ルータを初期化。無線 LAN は使用せず、有線 LAN で。<br>・ネットにつなぎ、OS やウイルス対策ソフトをアップデートして最新状態に。<br>・パッケージソフトなど信頼出来るソフトのみ、必要最小限入れる。<br>・ウェブ閲覧は、ニュースサイトなど、信頼のおけるサイトを見るだけにし、会員制サイトへのログインや、掲示板への書き込みなどは避ける。<br>・しばらく様子を見て、問題が無いようだったら一つずつインストールするソフトを増やす。<br>・問題無いようだったら、信頼おけそうなサイトにはログインして様子を見る。<br>(ご参考)<br>IPA - パソコンユーザのためのウイルス対策 7 箇条<br>http://www.ipa.go.jp/security/antivirus/7kajonew.html |

## 5．インターネット定点観測での 4 月のアクセス状況

インターネット定点観測(TALOT2)によると、2009 年 4 月の期待しない(一方的な)アクセスの総数は 10 観測点で 110,995 件、総発信元(※)は 41,366 箇所ありました。平均すると、1 観測点につき 1 日あたり 138 の発信元から 370 件のアクセスがあったことになります(図 5-1 参照)。

総発信元(※)：TALOT2 にアクセスしてきた発信元の総数。同一発信元から同一の観測日・観測点・ポートに複数アクセスがあった場合でも、発信元数は 1 としてカウント。

TALOT2 における各観測点の環境は、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。

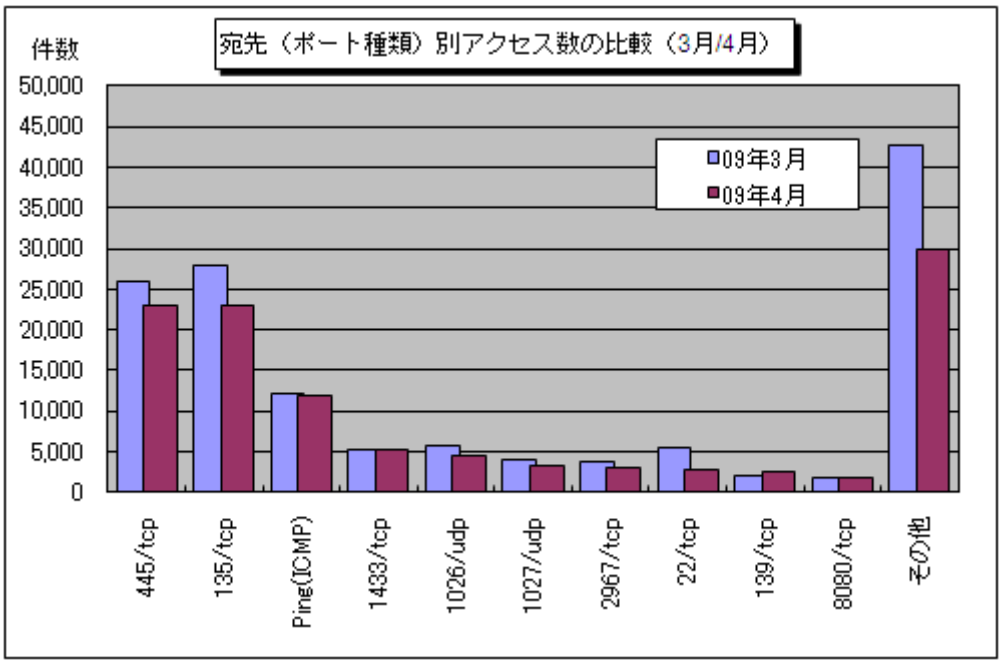



【図 5-1 1 観測点・1 日あたりの期待しない(一方的な)平均アクセス数と発信元数】

2008 年 11 月～2009 年 4 月までの各月の 1 観測点・1 日あたりの平均アクセス数とそれらのアクセスの平均発信元数を図 5-1 に示します。4 月の期待しない(一方的な)アクセスは 3 月と比べて減少しました。

3 月と 4 月の宛先(ポート種類)別アクセス数の比較を図 5-2 に示します。

アクセス数の上位 10 ポートにおいて、3 月と比較して大きく変化があったポートはありませんでした。平均アクセス数の減少に影響を与えたのは、上位 10 ポート以外のポートへのアクセスであり、3 月に比べて、約 1 万 3 千件の減少(3 月比で約 70%)となりました。これは、3 月に、1 観測点においてのみ、一時的に観測されていた原因不明のアクセスが複数あったのに対して、4 月には同様のアクセスが観測されなかったことが影響しています。




**【図 5-2 宛先(ポート種類)別アクセス数の比較(3 月/4 月)】**

**以上の情報に関して、詳細はこちらをご参照ください。**

**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/2009/documents/TALOT2-0905.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/

**■お問い合わせ先**
IPA **セキュリティセンター　花村／加賀谷／大浦**
Tel:03-5978-7527 Fax:03-5978-7518
E-mail: isec-info@ipa.go.jp