INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
第 09-01-140 号
2009 年 1 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 [2008 年 12 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：西垣 浩司)は、2008 年 12 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

「ウイルス感染の危険と隣り合わせの状況を知ろう！」
― 従来の常識が通用しないほど、感染の手口が巧妙になっています ―

2008 年のウイルスの傾向を振り返ると、感染の手口が巧妙になってきたことが挙げられます。今までは安全と言われていた PDF（Portable Document Format）ファイルや Word ファイル等のデータファイルにウイルスが潜んでいたり、有名な企業のウェブサイトが改ざんされ、そのページを閲覧したパソコンにウイルスを取り込ませる仕掛けになっていた事例が確認されました。また、普段何気なく利用している USB メモリを介してウイルス感染する事例もありました。このように、いつの間にかウイルスに感染してしまう危険性と隣り合わせの状況へと変化しました。

これらの手口によってウイルスに感染すると、オンラインゲームのアカウント情報（ID やパスワード）を盗まれ、ゲーム内のアイテムを窃取される、パソコン内の重要なファイルを削除され、システムが破壊されるといった被害が起きることがあります。

ウイルス感染の被害に遭わないよう、新しい感染の手口を認識し、ウイルス対策の基本を再確認しましょう。

（1）巧妙化するウイルス感染の手口

2008 年を通してウイルス感染の傾向を分析すると、従来は安全と考えられていた対象が、巧妙になったウイルスにより、もはや安全ではなくなってしまったといえます。その結果、以前よりも注意すべき対象が増え、対策が行き届かないケースも想定されます。次項に特徴的な傾向を 3 つ紹介しますので、感染の手口を認識してください。

（a）PDF ファイルや Word ファイルでも感染！

従来、危険なファイルといえば拡張子が exe といったアプリケーションファイルでしたが、今では PDF ファイルや Word ファイルも危険なファイルとなっています。

従来	PDF や Word などのデータファイルは比較的安全。アプリケーションファイルがメールに添付されていたら危険。
現在	PDF や Word などのデータファイルにもウイルスが潜んでいるケースがある。

メールの添付ファイルを開く場合、拡張子を確認し、exe だったら危険、pdf や doc であれば安全という認識がありました。しかし、データファイルを閲覧するために利用するソフトに脆弱性（ぜいじゃくせい）があり、それを悪用することで、ウイルスに感染させる手法が出現しています。

実際に、特定の組織をターゲットにして攻撃を行う標的型攻撃に利用されたケースが確認されています。

（ご参考）
「公的機関になりすましたメールに注意してください！！」（2008 年 5 月の呼びかけ）
http://www.ipa.go.jp/security/txt/2008/05outline.html#5

「オフィスソフトの文書ファイルにウイルスが！」（2008 年 4 月の呼びかけ）
http://www.ipa.go.jp/security/txt/2008/04outline.html#5

（b）有名な企業や組織のウェブサイトが改ざんされ、それを見ただけでウイルス感染！

有名な企業や組織のウェブサイトといえば管理が行き届いた信頼できるサイトとして、ウイルスに感染する事態が発生するとは想像もしません。しかし、安全と思われているサイトであっても改ざんされ、ウイルスに感染させるための仕掛けが埋め込まれてしまうケースが 2008 年に多発しました。

そのような改ざんされたウェブサイトは、利用者が見ただけでウイルスに感染してしまう危険性があります。見ただけで感染してしまう原因は、Internet Explorer といったウェブサイトを閲覧するためのブラウザソフトに脆弱性があり、それを悪用しているからです。

従来	有名企業のウェブサイトは信頼できるので安全。怪しいサイトに近づかなければ大丈夫。
現在	有名企業のウェブサイトであっても改ざんされた結果、ウイルスに感染する危険性がある。

（ご参考）
「いつも見ていたウェブサイトなのにウイルス検知？」（2008 年 3 月の呼びかけ）
http://www.ipa.go.jp/security/txt/2008/03outline.html#5

（c）USB メモリを介してパソコンにウイルス感染！

USB メモリやメモリカードなどの外部記憶メディアは、大容量化と低価格化が進み、データの持ち運びやバックアップに利用する機会が増えています。この便利な USB メモリを悪用し、感染を拡大するウイルスが 2008 年後半、急速に増加しました。

普段、何気なく利用している USB メモリに、ウイルスが潜んでいるという危険性を知らない利用者が多いと推測されます。このような利用者が、ウイルスに感染した USB メモリをパソコンに接続すると、パソコンにウイルスが感染し、さらに、感染したパソコンに別の USB メモリを接続すると、そこにも感染します。このように、USB メモリを介して次々と感染が拡大することになります。

従来	1990 年代、フロッピーディスクを介して感染するウイルスが流行した。
現在	USB メモリを介して感染するウイルスが出現し、USB メモリ経由でデータをやり取りする際にもウイルス感染の危険が潜んでいる。

（ご参考）
「外部記憶メディアのセキュリティ対策を再確認しよう！」（2008 年 12 月の呼びかけ）
http://www.ipa.go.jp/security/txt/2008/12outline.html#5

（2）ウイルス感染時の被害事例

ウイルスに感染することにより発生する被害事例としては、次のケースが確認されています。近年のウイルスの傾向としては、パソコン内の情報を盗むことや感染したパソコンを二次利用することなどを目的としたケースが増えています。

[ケース 1]：標的型攻撃で利用されたウイルスの症状

感染したウイルスが、悪意ある者が用意したインターネット上のサーバにアクセスし、そのサーバに利用者のパソコン名、OS のバージョン、IP アドレスなどの情報を送信します。また、このサーバから感染したパソコンに対して、次のような命令を出すことが可能となり、情報漏えいやパソコン内のファイルが削除されるといった被害が発生する危険があります。

・ パソコン内のドライブ、フォルダ、ファイルの一覧の送信
・ 任意のファイルの送受信、変更、削除
・ パソコンでのコマンドの実行とその出力結果の送信
・ プログラムの実行

[ケース 2]：ウェブサイトに仕掛けられたウイルスや USB メモリ感染型ウイルスの症状
これらのウイルスに感染すると、パソコンに以下の被害が発生する危険があります。

・ Windows が正常に動作するために必要なシステムファイルが破壊される
　破壊された結果、Windows がシステムファイルを修復しようとして、システム CD が要求される場合がある。
・ オンラインゲームサイトのアカウント情報（ID やパスワード）が盗まれる
　盗まれたアカウント情報でオンラインゲームに不正アクセスされ、ゲーム内の通貨や、手に入りにくいアイテムなどを失ってしまう可能性がある。
・ 他のウイルスをダウンロードさせられる
　悪質なウイルスをダウンロードさせられる可能性もあり、どのような機能を持ったウイルスがダウンロードされるか不明なため、想定される被害は多岐に渡る。

（3）基本的な対策

ウイルスによる感染被害を未然に防ぐための対策として、ウイルス対策ソフトの活用と脆弱性の解消が挙げられます。これらの技術的な対策は、セキュリティ対策の基本となりますので、必ず実施するようにしてください。

（a）ウイルス対策ソフトの活用

ウイルス対策ソフトをインストールし、ウイルス定義ファイルを常に最新の状態に更新、リアルタイムでウイルスを検知する機能を有効にして利用するようにしてください。

さらに、1 週間に 1 回程度、パソコン内を定期的にウイルスチェックすることをお勧めします。

（b）脆弱性を解消する

PDF ファイルに潜むウイルスに感染する、ウェブサイトを見ただけで感染するといった被害は、アプリケーションソフトに脆弱性があるために発生します。PDF 閲覧ソフトやブラウザソフト等のアプリケーションを最新版に更新することにより、可能な限り脆弱性を解消してください。また、Windows 等の OS にも脆弱性が存在します。Windows Update を利用して、同様に脆弱性を解消しておきましょう。

（4）新しい手口への対策

上述の基本的な対策だけでは、(1) で紹介した新しい感染の手口による被害を防ぐには不十分です。(2) で紹介した被害に遭わないため、技術的な対策に加え、日頃から以下のようなことにも注意を払い、新しい手口への対策を実施してください。

（a）信頼できない、出所不明なファイルは開かない

普段やり取りがない送信者から届いたメールの添付ファイルや怪しいウェブサイトからダウンロードしたファイルなど、信頼できないファイルにはウイルスが潜んでいる可能性が高いです。ウイルス対策ソフトで検知されないからといって、ファイルの内容を開いて確認する必要はありませんので、決して開かないようにしてください。

（b）警告を無視しない

Window XP や Vista には、アプリケーションを実行しようとしたとき、「セキュリティの警告」を表示してくれる機能があります。不意にこの警告が表示された場合、それを無視して実行すると、ウイルスに感染するなどの被害に遭ってしまいます。「セキュリティの警告」が表示された場合は、自

分の意図した作業かどうかを確認し、判断できないときはキャンセルするようにしてください。

（c）自身が管理していない USB メモリは使わない

USB メモリ等の外部記憶メディアを介したウイルス感染が増加しています。感染被害に遭わないための最低限の心掛けとして、

- 自身が管理していない USB メモリや所有者の不明な USB メモリは、自身のパソコンには接続しない。
- 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は、自身の USB メモリを接続しない。

といった点に注意するようにしましょう。

以上（3)、(4）の対策は、単独に実施していても効果は限定的です。それぞれを組み合わせて総合的に実施することで、新しい感染の手口にも対応することができます。できる限りの対策を実施し、感染被害を未然に防ぐようにしてください。

(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
「メールの添付ファイルの取り扱い 5 つの心得」
http://www.ipa.go.jp/security/antivirus/attach5.html
「スパイウェアガイド」
http://www.shareedge.com/spywareguide/index.php
「Microsoft Update と Windows Update の利用の手順」(マイクロソフト社)
http://www.microsoft.com/japan/athome/security/mrt/wu.mspx

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、6 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らしい
- オンラインゲームサイト内のデータが改ざんされた

○ 相談の主な事例 (相談受付状況及び相談事例の詳細は、8 頁の「4.相談受付状況」を参照)

- USB メモリにデータを入れて持ち帰ったら、自宅のパソコンでウイルス検知
- 不正アクセスされたら、パソコンは初期化？

○ 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。

- 脆弱性を突くウイルスによる攻撃と思われる 445/tcp へのアクセスに注意！

2．コンピュータウイルス届出状況　－詳細は別紙 1 を参照－

(1)ウイルス届出状況

ウイルスの検出数(※1)は、約 17.3 万個と、11 月の約 25.6 万個から 32.5%の減少となりました。
また、12 月の届出件数(※2)は、1,795 件となり、11 月の 1,830 件から 1.9%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。

- 12 月は、寄せられたウイルス検出数約 17.3 万個を集約した結果、1,795 件の届出件数となっています。

検出数の 1 位は、W32/Netsky で約 14.4 万個 、2 位は W32/Autorun で約 1.3 万個、3 位は W32/Mydoom で約 4 千個でした。

ウイルス検出数　約17.3万個（約25.6万個）　前月比 - 32.5%

（注：括弧内は前月の数値）

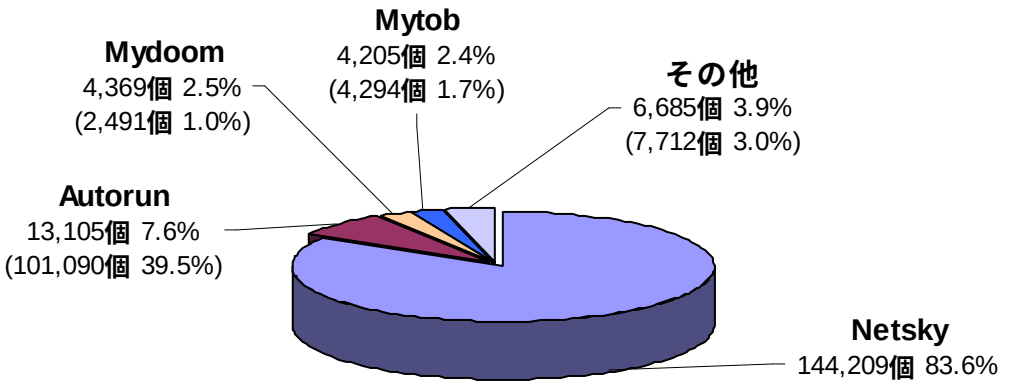


図 2-1

ウイルス届出件数　1,795件（1,830件）前月比 **-1.9%**

（注：括弧内は前月の数値）

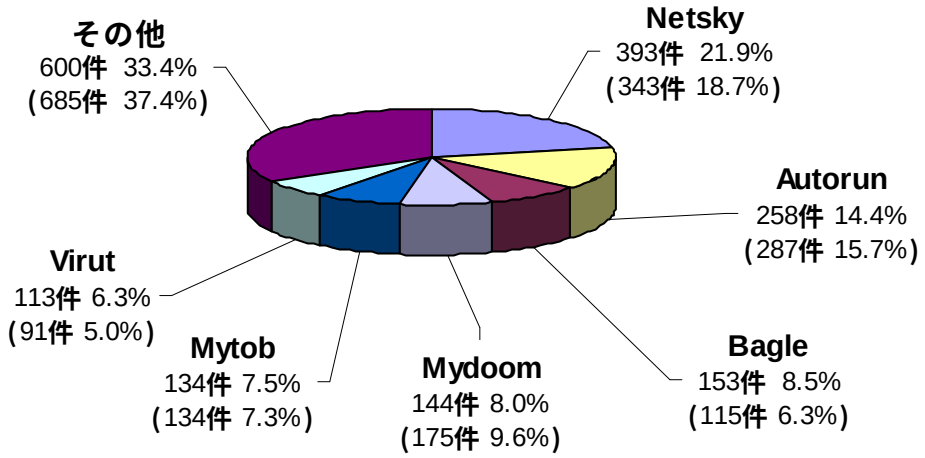


図 2-2

(2)不正プログラムの検知状況

バックドアやスパイウェア等の不正プログラムの検知件数が、2008 年 9 月に急増し、10 月も高水準で推移しました。しかし、11 月中旬以降は、急増する前の水準に戻り、FAKEAV や LINEAGE の検知件数がほとんどなくなりました（図 2-3 参照）。

不正プログラムの検知状況は少なくなっていますが、いつ急増するか予測できませんので、添付ファイルの取り扱いには継続して注意するようにしてください。

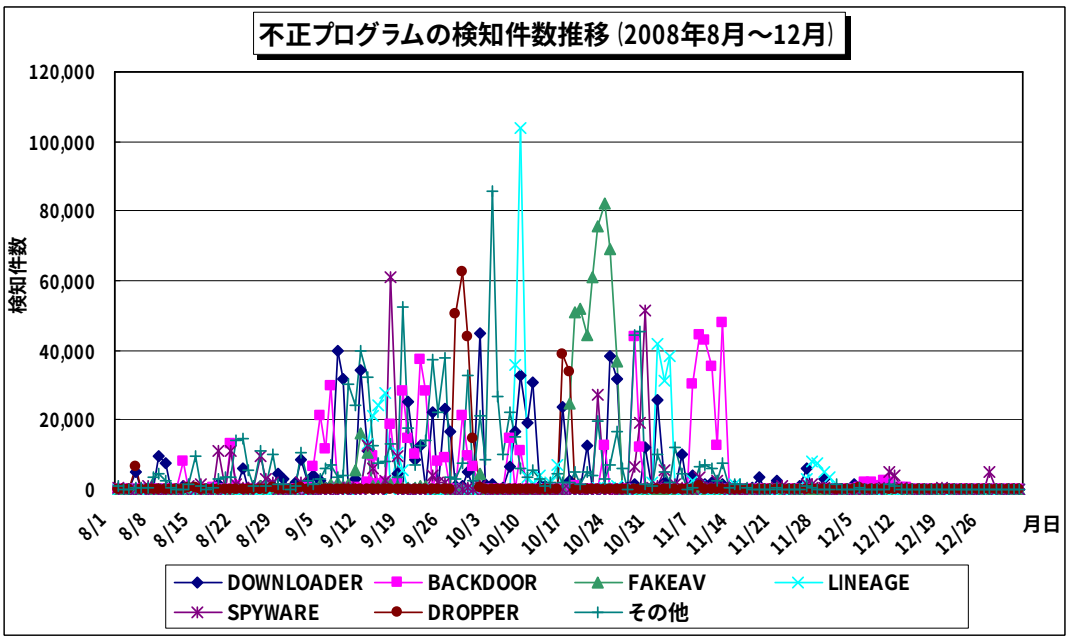


図 2-3

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

		7月	8月	9月	10月	11月	12月
届出(a) 計		19	15	14	17	18	10
	被害あり(b)	18	10	12	12	12	7
	被害なし(c)	1	5	2	5	6	3
相談(d) 計		49	25	38	58	39	38
	被害あり(e)	26	13	20	22	19	19
	被害なし(f)	23	12	18	36	20	19
合計(a+d)		68	40	52	75	57	48
	被害あり(b+e)	44	23	32	34	31	26
	被害なし(c+f)	24	17	20	41	26	22

(1)不正アクセス届出状況

12 月の届出件数は 10 件であり、そのうち何らかの被害のあったものは 7 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 38 件(うち 5 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 19 件でした。

(3)被害状況

被害届出の内訳は、侵入 7 件でした。

侵入届出の被害は、SQL※インジェクション※攻撃を受け、結果としてデータベース内のデータを改ざんされたものが 3 件、その他脆弱性を突かれて侵入され、システム内でコマンドを実行されたものが 2 件、他サイト攻撃などの踏み台として悪用されたものが 1 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 件でした。侵入の原因は、脆弱性を突かれたことによるものが 5 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)。

※SQL (Structured Query Language)：リレーショナルデータベースマネジメントシステム(RDBMS)において、データの操作や定義を行うための問合せ言語のこと。
※SQL インジェクション：データベースへアクセスするプログラムの不具合を悪用し、正当な方法以外でデータベース内のデータを閲覧したり書き換えしたりする攻撃のこと。
※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。
※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らしい

事例	・自組織で運用しているウェブサーバが、外部からアクセスできないとの連絡を受けた。 ・サーバを調査したところ、特権ユーザアカウントのパスワードが変更されていて、ログインできないことが判明。 ・その後の調査で、おそらく SSH で使うポートにパスワードクラッキング攻撃を受け、弱いパスワードが破られて侵入されたらしいことが分かった。さらに、SSH スキャナを埋め込まれていた。 ・通常は、SSH で使うポートに外部から接続を許可する IP アドレスを限定していた。しかし、非定常作業の際に一旦アドレス限定を外し、作業完了後もそのままにしていたことが、攻撃を受けるきっかけであった。
解説・対策	非定常作業だったため、**作業後、IP アドレス限定設定を元に戻すのを忘れてしまったこと**と、**アカウントのパスワードが強固ではなかった**ことの複合要因で起きてしまった事例です。 対策が抜かりなく行えるように、**作業手順書や作業チェックリストなどを準備する**のも一つの手です。 (参考) IPA - 安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/websecurity.html

[侵入]

(ii) オンラインゲームサイト内のデータが改ざんされた

事例	・オンラインゲームサイト運営者が、自身のサイトの表示不具合を確認。 ・調査したところ、当該サイトで動いているウェブアプリケーションから参照するデータベース内のデータに、html タグが埋め込まれるという改ざんがされていることが判明。 ・改ざんの結果、当該サイトにアクセスしただけで、ウイルスが仕込まれているサイトに誘導されるようになっていた。当該サイトと提携している他のゲームサイトからのアクセスでも、同様の被害に遭うようになっていた。 ・ウェブアプリケーションに、SQL インジェクションの脆弱性があったことが原因。
解説・対策	オンラインゲームサイトは、多くの人がアクセスしてくるため、サイトを改ざんし、ウイルスサイトへ誘導するための“踏み台”として狙われることが多いようです。 **最大の対策は、脆弱性を作り込まないこと**、です。次の資料を参考にしてください。 (参考) IPA - ウェブサイト運営者のための脆弱性対応ガイド http://www.ipa.go.jp/security/fy19/reports/vuln_handling/ IPA - 安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/websecurity.html

4．相談受付状況

12 月の相談総件数は 839 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 194 件(11 月：144 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 13 件(11 月：28 件)、Winny に関連する相談が 6 件(11 月：5 件)、などでした。(「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」に関する相談は 0 件)

表 4-1　IPA で受け付けた全ての相談件数の推移

	7月	8月	9月	10月	11月	12月
合計	1,387	1,616	2,154	1,171	713	839
自動応答システム	817	994	1,302	677	363	458
電話	500	548	755	441	288	331
電子メール	70	69	93	47	62	49
その他	0	5	4	6	0	1

※ 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。

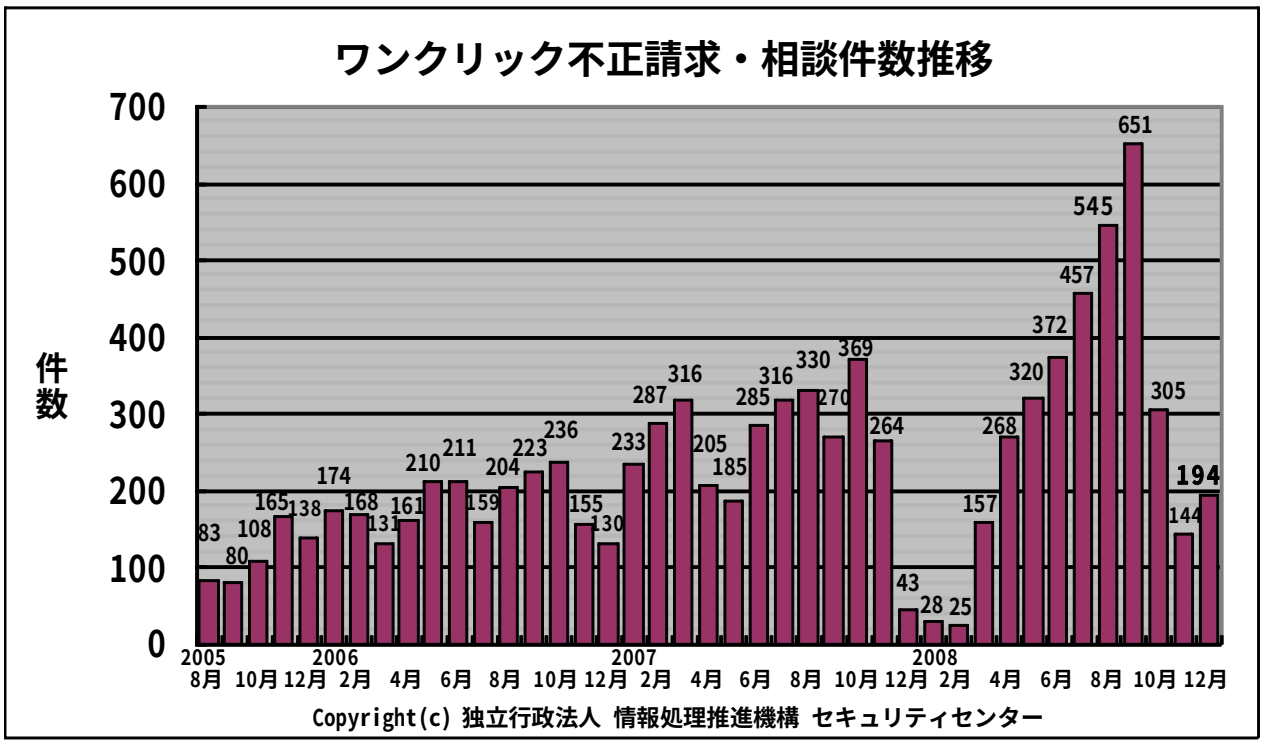


図 4-1　ワンクリック不正請求相談件数の推移

主な相談事例は以下の通りです。

(i) USB メモリにデータを入れて持ち帰ったら、自宅のパソコンでウイルス検知

相談	学校で使っているパソコン(A 社製ウイルス対策ソフト入り。契約切れ)から、学校で管理している USB メモリにデータをコピーした。自宅に持ち帰り、自宅のパソコン(B 社製ウイルス対策ソフト入り。契約期間内)に USB メモリを接続したら、ウイルスが検知された。どうして、学校のパソコンではウイルスが検知されなかったのか。 その後、同じ USB メモリを自宅パソコンに接続しても、何も警告が無い。どうなっているのか。心配である。
回答	ウイルス定義ファイル更新の**契約の切れたウイルス対策ソフトでは、日々新しく出現するウイルスの新種を検知することができません。**また、製造元の異なるウイルス対策ソフトでは、一方では検知可能でも他方で検知できるようになるまでには時間が掛かるものもあったりします。なお、**その後自宅パソコンで警告が出ないのは、USB メモリ内にあったウイルスが検知され、駆除されたため**です。パソコンにウイルスは感染していませんので、安心してください。 (ご参考) IPA - **呼びかけ：「外部記憶メディアのセキュリティ対策を再確認しよう！ 」** http://www.ipa.go.jp/security/txt/2008/12outline.html

(ii) 不正アクセスされたら、パソコンは初期化？

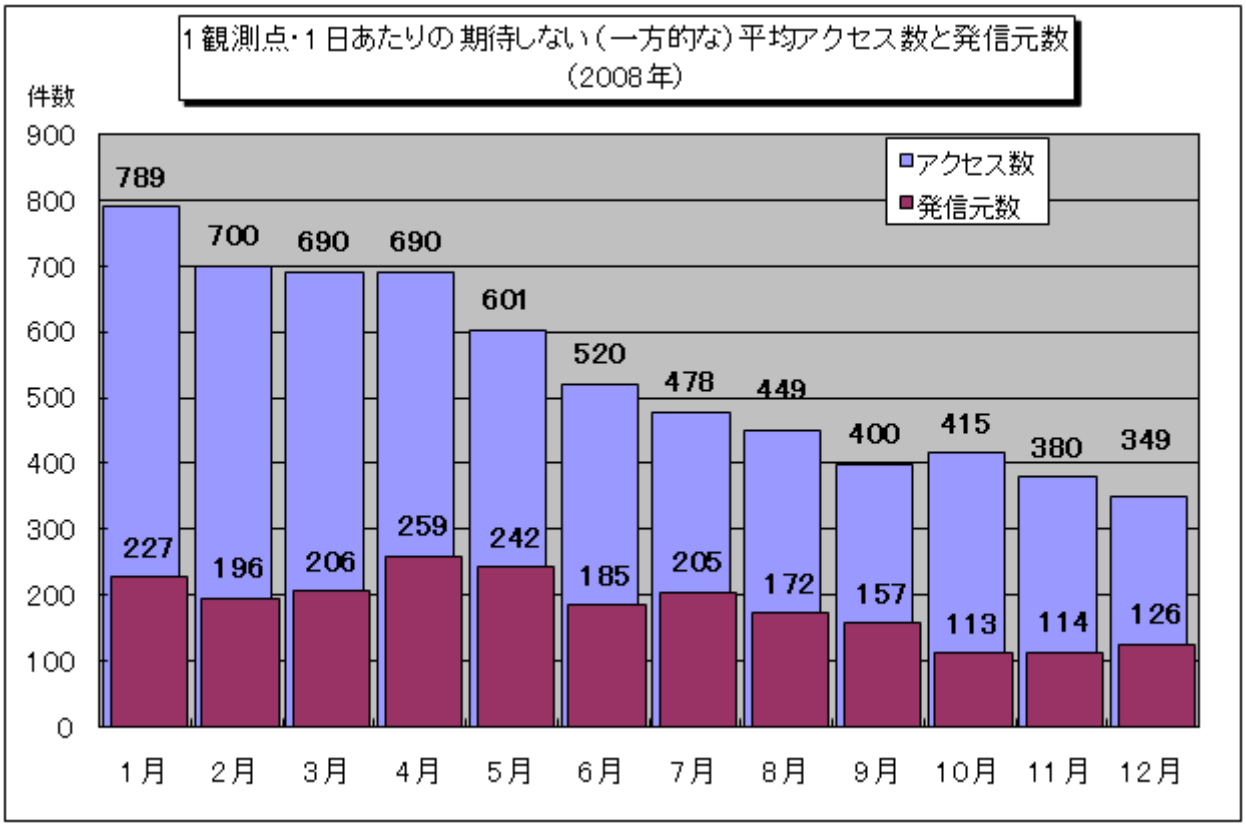
相談	パソコンの調子が、何となく悪い気がする。パソコンの中身を、誰かに見られているような感じがする。ルータを使い、ウイルス対策ソフトは常にウイルス定義ファイルを最新にして使い、パーソナルファイアウォールも入っている。ある人から、「不正アクセスされている可能性が高いから、初期化を勧める」と言われた。なぜですか？
回答	新種のウイルスなど、ウイルス対策ソフトでも見付けられないものは存在します。**ウイルスチェックをすり抜けてパソコンに入り込んだウイルスは、セキュリティ関連のソフトの動きを止めたり、外部から他の未知のウイルスをダウンロードして来たりします。** このことから、パソコンの動きが明らかにおかしい場合は、ウイルスに感染していたり、外部から操られていたりする可能性が高いと言えます。しかし、**それらの異変がチェックできていないということは、他の方法でも影響範囲の判別が困難だということです。**よって、パソコンを初期化し、全てをリセットするのが最善策と言えます。 (ご参考) IPA - **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

5．インターネット定点観測での 12 月のアクセス状況

インターネット定点観測(TALOT2)によると、2008 年 12 月の期待しない(一方的な)アクセスの総数は 10 観測点で 108,338 件、総発信元(※)は 38,976 箇所ありました。平均すると、1 観測点につき 1 日あたり 126 の発信元から 349 件のアクセスがあったことになります。

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。

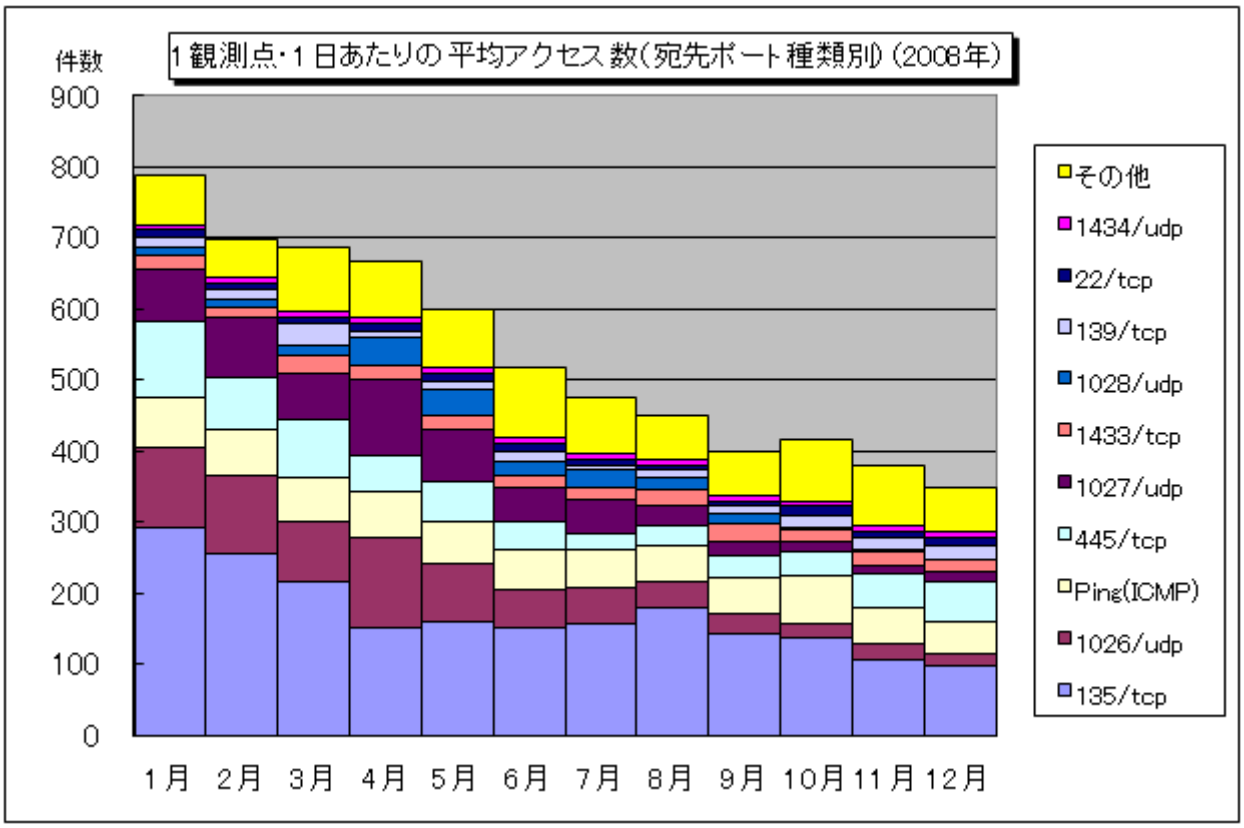


【図 5-1 1 観測点・1 日あたりの期待しない(一方的な)平均アクセス数と発信元数】

2008 年 1 月～2008 年 12 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。この図を見ると、12 月の期待しない(一方的な)アクセスは 11 月と比べて若干減少しました。年間を通してみると、減少傾向にあると言えます。

2008 年の各月の 1 観測点・1 日あたりの平均アクセス数を宛先ポート種類別で表したものを図 5-2 に示します。この図を見ると、全体のアクセス数の推移において支配的と言える 135/tcp、1026/udp へのアクセスの減少が目立っており、それがアクセス数全体の減少に影響していると言えます。

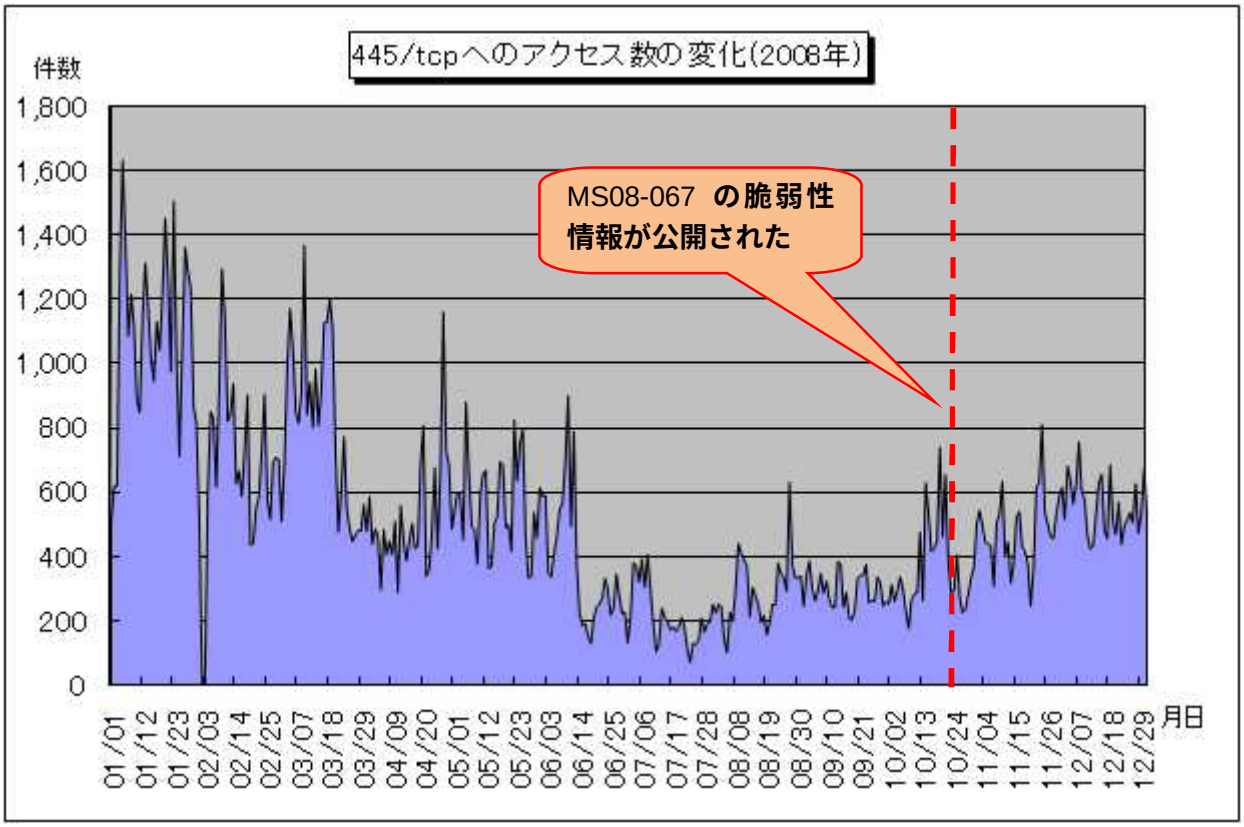
135/tcp は Windows の脆弱性を狙った攻撃を行う際に狙われる可能性が高いポートであり、1026/udp は 1027/udp とともに Windows のメッセンジャサービス機能を利用して、悪意あるメッセージを送りつける際に狙われる可能性が高いポートです。



【図 5-2 1 観測点・1 日あたりの平均アクセス数（宛先ポート種類別）（2008 年）】

(1) 脆弱性を突くウイルスによる攻撃と思われる 445/tcp へのアクセス数の増加

2008 年の 445/tcp へのアクセス数の変化を、図 5-3 に示します。2008 年の 445/tcp へのアクセス状況は、7 月頃まで減少傾向を示していましたが、その後、緩やかに増加傾向を示し、12 月末の時点でもその傾向が続いています。



【図 5-3 445/tcp へのアクセス数の変化（2008 年）】

このアクセス数の増加について原因は定かではありませんが、10 月頃からの増加に関しては、日本時間の 10 月 24 日にマイクロソフトから緊急に発表された、MS08-067 の脆弱性に関連した攻撃が影響していた可能性があります。マイクロソフトの情報によると、脆弱性情報が公開される 2 週間ほど前から、この脆弱性を突いた攻撃がすでに行われていたとのことです。

＜参考情報＞

■「Server サービスの脆弱性により、リモートでコードが実行される」（マイクロソフト）
http://www.microsoft.com/japan/technet/security/bulletin/ms08-067.mspx

この脆弱性情報の公開以降、445/tcp へのアクセス数の増加は、定点観測を行っている他の組織においても観測されており、この脆弱性を突くウイルスによる感染の試みであった可能性があります。また、実際に、この脆弱性を突くウイルスや攻撃ツールの存在が確認されています。

日頃から脆弱性情報には十分注意し、新しい脆弱性情報が公開されたら、速やかに対処することが基本的な対策となります。

＜参考情報＞

■「TCP 445 番ポートへのスキャン増加に関する注意喚起」
http://www.jpcert.or.jp/at/2008/at080019.txt

■「脆弱性 （MS08-067：CVE-2008-4250）を悪用したハッキングツールを確認」
http://blog.trendmicro.co.jp/archives/2115

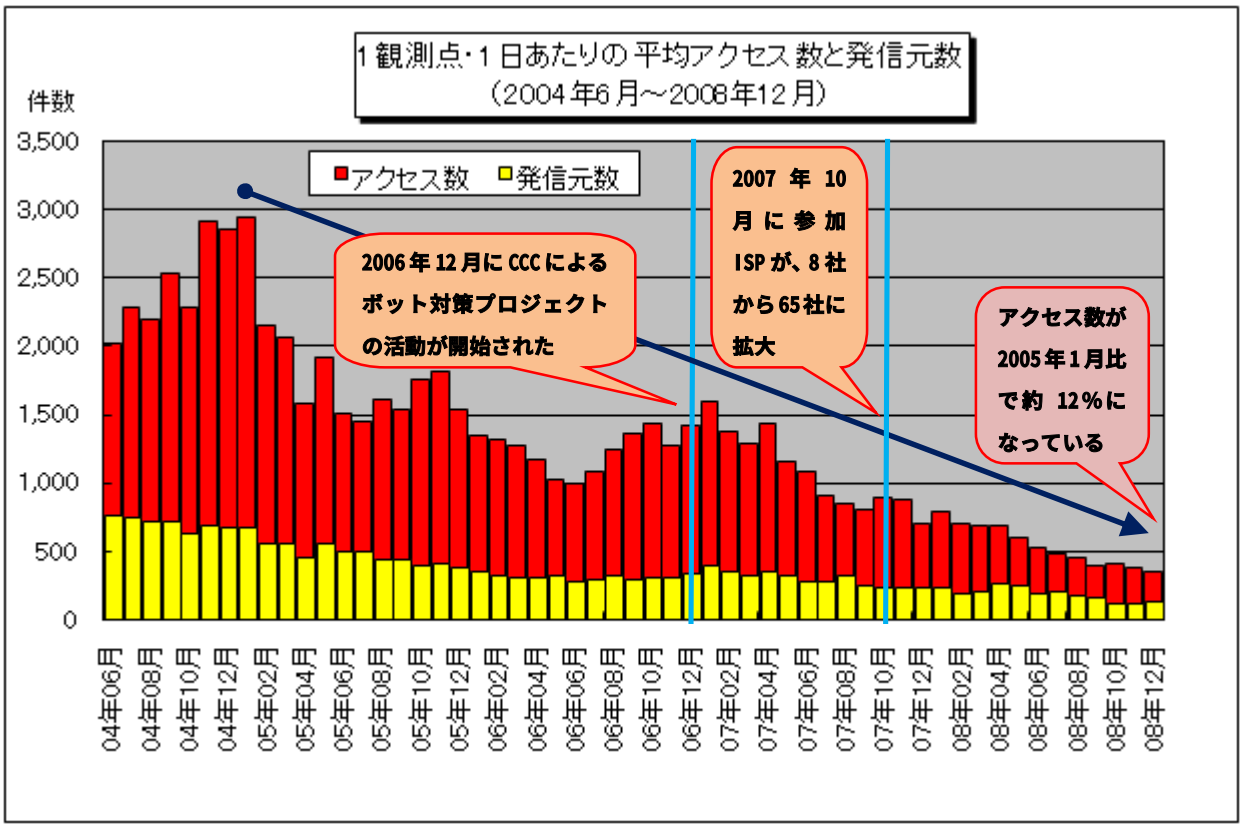
(2) 定点観測を開始してから 2008 年 12 月までのアクセス状況

TALOT2 による定点観測を開始した 2004 年 6 月から 2008 年 12 月までの、1 観測点・1 日あたりの平均アクセス数と発信元数を図 5-4 に示します。2008 年 12 月の平均アクセス数は、2005 年 1 月比で約 12%になっています。このうち 2006 年 12 月からの減少傾向については、その頃に活動が開始された CCC（サイバークリーンセンター）によるボット対策プロジェクトの活動の効果が、要因の一つとして挙げられます。

CCC では、ボット検体の収集・解析、ボット駆除ツールの作成・配布、プロジェクトに参加している ISP(インターネットサービスプロバイダ)を通じて、ボットに感染していると思われるユーザへの注意喚起といった活動を行っています。また、2007 年 10 月には、プロジェクトに参加する ISP が 8 社から 65 社へ大幅に拡大されました。これによって、さらに 2007 年 10 月以降の国内からのアクセス数の減少につながっています。

＜参考情報＞

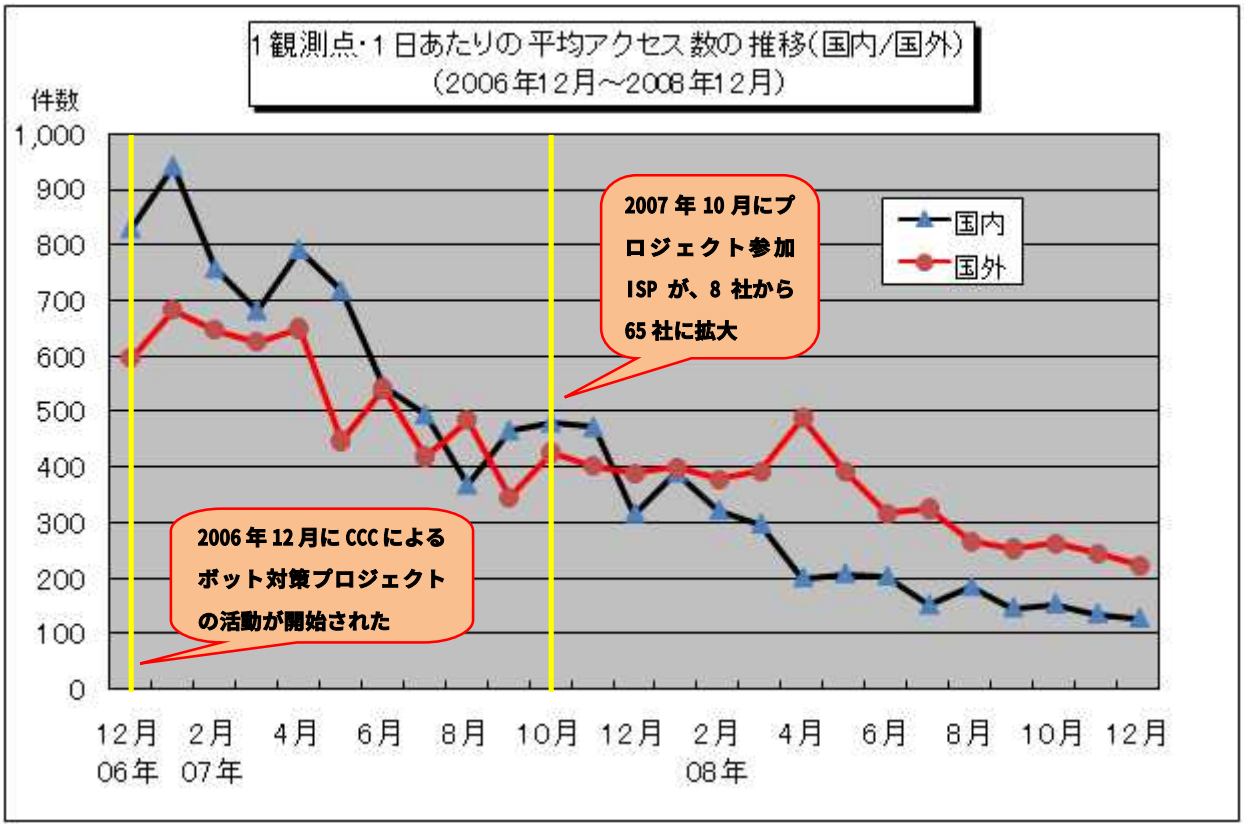
■総務省・経済産業省 連携プロジェクト Cyber Clean Center
https://www.ccc.go.jp/



【図 5-4 1 観測点・1 日あたりの平均アクセス数と発信元数（2004 年 6 月～2008 年 12 月）】

CCC が活動を開始してから 2008 年 12 月までの、国内からと国外からの平均アクセス数の推移を図 5-5 に示します。この図を見ると、国内・国外ともにアクセス数が減少していますが、国内からのアクセス数の減少の方がより顕著です。

このことからも、国内のボットの駆除を進めている CCC の活動が効果を上げていると思われます。



【図 5-5 1 観測点・1 日あたりの平均アクセス数の推移（国内/国外）（2006 年 12 月～2008 年 12 月）】

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/2009/documents/TALOT2-0901.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
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／大浦
Tel:03-5978-7527 Fax:03-5978-7518
E-mail: isec-info@ipa.go.jp