プレスリリース
第 09-32-159 号
2009 年 8 月 5 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 7 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 7 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

「知っていますか？“ゼロデイ攻撃”」
― 脆弱性対策の基本を理解しましょう ―

IPA では、ソフトウェアの提供元（ベンダー）から公開される脆弱性情報を分析して、緊急性が高いと判断したものを「緊急対策情報」として発信しています。7 月にマイクロソフト社から 4 件、アドビ社から 1 件と新たな脆弱性情報が公開され、IPA ではそのうちの 3 件 (※1) を、「緊急対策情報」として発信しました。これらの脆弱性はいずれも、修正プログラムが提供される前に脆弱性を悪用した攻撃が確認されていました。

脆弱性情報が公開されたら速やかに対応することが脆弱性対策の基本ですが、上述のようにその時点で修正プログラムが提供されていないこともあります。その場合でも、一時的な回避策が用意されていることがありますので、情報を注意深く確認することが重要です。

脆弱性対策の基本を正しく理解して、脆弱性を悪用した攻撃からパソコンを守りましょう。

※1：「Microsoft DirectShow の脆弱性（MS09-028）について」、「Microsoft Video ActiveX コントロール の脆弱性（MS09-032）について」、および「Adobe Flash Player 、Adobe Reader、Acrobat、Adobe AIR の脆弱性について」。

(1)「脆弱性」とは？

Windows や Mac OS などの OS やアプリケーションソフトの、セキュリティ上の弱点のことを脆弱性（vulnerability）と言います。脆弱性が解消されていない状態で、その脆弱性を悪用した攻撃を受けた場合、被害に遭うおそれがあります。脆弱性を悪用した攻撃への基本的な対策は、修正プログラムを適用し、脆弱性を解消することです。

IPA が従来から推奨している基本的なセキュリティ対策は、脆弱性を解消することと、ウイルス対策ソフトを最新の状態で使用することです。これはどちらか一方ではなく、両方を実施していないと効果がありません。たとえウイルス対策ソフトを最新の状態で使用していたとしても、脆弱性を解消していなければ、思いもよらない方法で外部からの侵入を許すことになる、ということです（図 1-1 参照）。

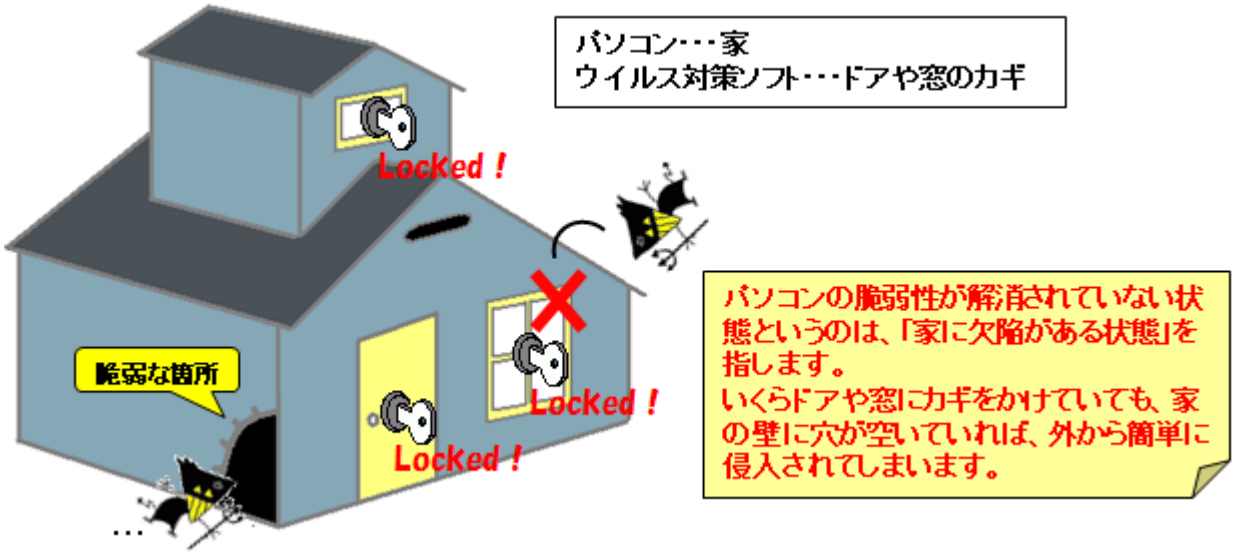


図 1-1：脆弱性を解消していないパソコンを家に例えた場合のイメージ図

(2)「ゼロデイ攻撃」とは？

「ゼロデイ攻撃」とは、あるソフトウェアの脆弱性が判明し、そのソフトウェアの修正プログラムがベンダーから提供されるより前に、その脆弱性を悪用して行われる攻撃のことを指します（図 1-2 参照）。

図 1-2：「ゼロデイ攻撃」

以下に、具体的な事例として、7 月に確認された「Microsoft Video ActiveX コントロールの脆弱性」（MS09-032）を例に「ゼロデイ攻撃」を説明します。

＜時系列＞

［発生日不明］

今回の脆弱性を悪用した攻撃が発生した（図 1-3 の①）。

［2009 年 7 月 6 日（米国時間）］

今回の脆弱性を悪用した攻撃の発生が確認され、マイクロソフト社より「Microsoft Video ActiveX コントロールの脆弱性」（MS09-032）に関する脆弱性情報が公開された。この時点で修正プログラムは提供されなかったが、暫定措置として攻撃の回避策が提示された（図 1-3 の②）。

［2009 年 7 月 14 日（米国時間）］

マイクロソフト社より、MS09-032 に関する脆弱性情報の更新と、修正プログラムが提供された（図 1-3 の③）。

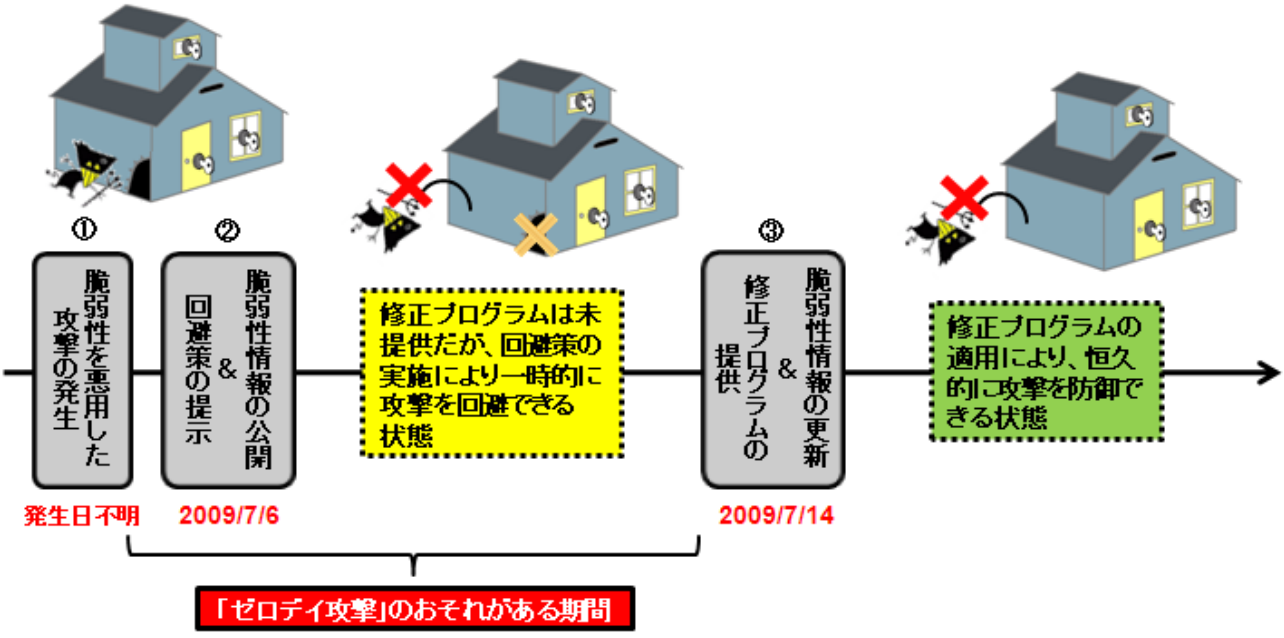


図 1-3：脆弱性 MS09-032 への対応状況〈時系列推移〉

今回の事例は、実際に脆弱性情報が公開される前に攻撃が発生していました（図 1-3 の①）。パソコン利用者は 7 月 6 日の脆弱性情報の公開時（図 1-3 の②）に提示された回避策を知ってすぐに実施し、その後の 7 月 14 日の脆弱性情報の更新時（図 1-3 の③）に提供された修正プログラムをすぐに適用していれば、攻撃を防御できました。

しかし、脆弱性情報が公開されたことを知らなかったために、脆弱性対策を実施出来なかったパソコン利用者は、攻撃を受けていた可能性があります。

次項で説明する注意点を参考に「ゼロデイ攻撃」への対策を実施してください。

（ご参考）

「Microsoft Video ActiveX コントロールの脆弱性により、リモートでコードが実行される」（マイクロソフト社）
http://www.microsoft.com/japan/technet/security/advisory/972890.mspx

「マイクロソフト セキュリティ情報 MS09-032 - 緊急」（マイクロソフト社）
http://www.microsoft.com/japan/technet/security/bulletin/MS09-032.mspx

「Microsoft Video ActiveX コントロール の脆弱性（MS09-032）について」（IPA）
http://www.ipa.go.jp/security/ciadr/vul/20090707-ms-activex.html

（3）「ゼロデイ攻撃」を受けないための注意点

「ゼロデイ攻撃」を受けないためには、ベンダーから公開される脆弱性情報を十分理解し、適切に対応することが重要です。IPA などが発信する「緊急対策情報」や JVN などの脆弱性情報ポータルサイトも参考にしてください。（2）の事例のように、脆弱性情報の公開時には修正プログラムが提供されていない場合でも、一時的な回避策が提示されていることがあります。ただし、実施することで特定のサービスが利用できなくなるなどの影響が出る場合がありますので、実施する際は十分注意が必要です。万が一具体的な回避策が提示されない場合は、当該ソフトウェアを一時的に使用しないなどの対応が有効です。その後、正式な修正プログラムが提供された際には、直ちに適用することも忘れないでください。

以上のように、脆弱性に適切に対応するためには、日頃から脆弱性情報を収集することが重要です。また、併せてウイルス対策ソフトを最新の状態で使用し、攻撃を防御することも重要です。

以下に有効な情報収集の方法を示します。

（i）メールマガジンを利用した情報収集

パソコン利用者が使用している OS やアプリケーションソフト・セキュリティ対策ソフトのベンダー、パソコンメーカーなどがメールマガジンのサービスを提供している場合、それを利用することで、負担なく脆弱性に関する情報を得ることができます。マイクロソフト社の場合は、以下の URL からメールマガジンの購読申し込みが行えます。

また、IPA では、ベンダーから公開される脆弱性情報を分析して、緊急性が高いと判断されたものを「緊急対策情報」としてウェブサイトから発信するとともに、メールマガジンでその情報を配信しています。

（ご参考）

「セキュリティ ニュースレター」（マイクロソフト社）
http://technet.microsoft.com/ja-jp/security/cc307424.aspx

「情報処理推進機構　新着情報メール配信」（IPA）
http://www.ipa.go.jp/about/mail/

（ii）ウェブサイトからの情報収集

パソコン利用者が使用している OS やアプリケーションソフト・セキュリティ対策ソフトのベンダー、パソコンメーカーなどのウェブサイトで、脆弱性に関する情報が得られる場合がありますので、定期的に参照することをお勧めします。マイクロソフト社の場合は、以下の URL が参考になります。

また IPA では、ベンダーから公開される脆弱性情報を分析して、緊急性が高いと判断されたものを「緊急対策情報」としてウェブサイトから発信しています。日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供している JVN などの脆弱性情報ポータルサイトも参

考になります。

（ご参考）
「セキュリティ TechCenter」IT プロフェッショナル向け（マイクロソフト社）
http://technet.microsoft.com/ja-jp/security/default.aspx

「セキュリティ At Home」一般家庭向け（マイクロソフト社）
http://www.microsoft.com/japan/protect/default.mspx

「緊急対策情報・注意喚起 一覧」（IPA）
http://www.ipa.go.jp/security/announce/alert.html

「JVN（Japan Vulnerability Notes）」（脆弱性情報ポータルサイト）
http://jvn.jp/

（iii）補足・解説記事

その他の方法として、ニュースサイト（特に IT 系）やポータルサイトに掲載される記事を参考にすることが挙げられます。脆弱性に関する情報が掲載されることがありますので、そこから有益な情報が得られる場合もあります。

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（届出状況およ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）
- cgi の脆弱性を突かれて侵入され、バックドアを設置された
- オンラインゲームサイトで、ゲーム内で使うアイテムや所持金を盗まれた

○ 相談の主な事例 （相談受付状況および相談事例の詳細は、8 頁の「4.相談受付状況」を参照）
- 外部公開サーバや企業内パソコン・ネットワークのセキュリティ対策はどうすれば？
- ウイルス対策をやりたがらない知り合いがいる

○ インターネット定点観測（10 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。
- 4899/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－

ウイルスの検出数（※1）は、**約 8 万個**と、6 月の約 8.7 万個から 14%の減少となりました。
また、7 月の届出件数（※2）は、**1,256 件**となり、6 月の 1,460 件から 8%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。
・7 月は、寄せられたウイルス検出数約 8 万個を集約した結果、1,256 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 7 万個**、2 位は **W32/Mydoom** で**約 4 千個**、3 位は **W32/Mytob** で**約 3 千個**でした。

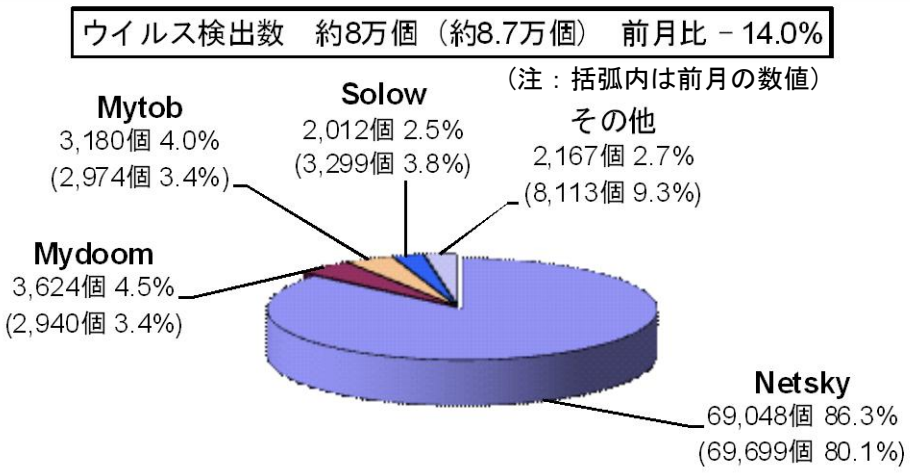


図 2-1：ウイルス検出数

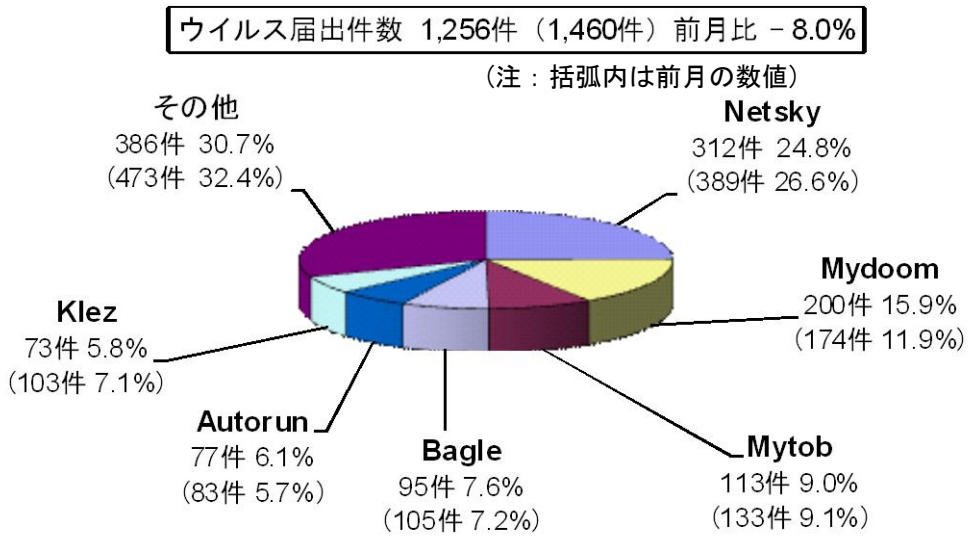


図 2-2：ウイルス届出件数

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

		2月	3月	4月	5月	6月	7月
届出(a) 計		9	20	9	8	7	14
	被害あり(b)	6	13	6	6	6	6
	被害なし(c)	3	7	3	2	1	8
相談(d) 計		35	40	39	45	35	24
	被害あり(e)	14	11	11	16	9	3
	被害なし(f)	21	29	28	29	26	21
合計(a+d)		44	60	48	53	42	38
	被害あり(b+e)	20	24	17	22	15	9
	被害なし(c+f)	24	36	31	31	27	29

（1）不正アクセス届出状況

７月の届出件数は 14 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 24 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３件でした。

（3）被害状況

被害届出の内訳は、**侵入２件、アドレス詐称１件、なりすまし３件、**でした。

「侵入」の被害は、バックドア※プログラムを埋め込まれたものが 1 件、ウェブページ内に不正なスクリプトを埋め込まれていたものが１件、でした。侵入の原因は、cgi※の脆弱性を突かれたことによるものでした（残りの１件は原因不明）。「なりすまし」の被害は、オンラインサービスのサイトに本人になりすまして何者かにログインされ、サービスを勝手に利用されていたもの(オンラインゲーム 3 件)でした。

※バックドア（backdoor）：コンピュータシステムへの侵入者が侵入後、そのシステムに再侵入するために準備する仕掛けのこと。
※cgi（Common Gateway Interface）：ウェブサーバが、クライアントからのリクエストに応じてウェブサーバ上でプログラムを動作させ、その処理結果をクライアントに送信するための仕組みのこと。

（4）被害事例

[侵入]

（i）cgi の脆弱性を突かれて侵入され、バックドアを設置された

事例	・IDS（侵入検知システム）が、OS コマンドインジェクションと思われる攻撃アクセスを検知した。 ・調査したところ、ウェブサーバ上で利用していた cgi プログラムの脆弱性を突かれ侵入され、madshell と呼ばれる、バックドア機能を持つ php のシェルプログラムを埋め込まれ、実行されていたことが判明。 ・当該サーバは、再構築することにした。
解説・対策	幸い、**検知が早かったため、被害を最小限に食い止めることができた**事例です。**脆弱性の解消は、最も基本的なセキュリティ対策**です。外部にサービスを提供するサーバであれば、一通りの対策が済んだ時点で、第三者による**脆弱性検査を受けることをお勧めします**。 （参考） IPA - 安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/websecurity.html 経済産業省 - 情報セキュリティ監査企業台帳 http://www.meti.go.jp/policy/netsecurity/is-kansa/

[なりすまし]

（ii）オンラインゲームサイトで、ゲーム内で使うアイテムや所持金を盗まれた

事例	・自分が登録しているオンラインゲームのサイトにログインした際、自分のキャラクターが所持していたアイテムやお金が全て無くなっていることに気付いた。 ・履歴などを調査したところ、誰かが自分になりすましてログインし、他のキャラクターへアイテムなどを勝手に譲渡していたらしいことが判明。 ・原因は不明。
解説・対策	何らかの理由により、パスワードが破られてしまったようです。簡単に破られないように、**複雑なパスワードを設定することが重要**です。また、**パスワードを盗み取るウイルスに感染したことによる被害も発生**しているようです。IPA や、ゲーム運営会社のサイトからの注意喚起情報などを参考にして、ウイルス対策を確実に実施しましょう。 被害に遭ってしまったら、サイト運営者や警察機関に相談しましょう。 （参考） IPA からの呼びかけ - 「 今一度、パスワードを点検しましょう！ 」 http://www.ipa.go.jp/security/txt/2008/10outline.html 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 警察庁 - インターネット安全・安心相談 http://www.npa.go.jp/cybersafety/

4. 相談受付状況

7 月のウイルス・不正アクセス関連相談総件数は **1,708 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 **657 件**（6 月：694 件）となり、**過去 2 番目に多い件数**となりました。その他は、**『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 **6 件**（6 月：6 件）、**Winny に関連する相談**が **6 件**（6 月：13 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 **1 件**（6 月：0 件）、などでした。

表 4-1　IPA で受け付けた全てのウイルス・不正アクセス関連相談件数の推移

	2月	3月	4月	5月	6月	7月
合計	1,051	1,406	1,668	1,765	1,898	1,708
自動応答システム	521	758	962	992	1,081	923
電話	472	597	651	710	777	736
電子メール	57	49	55	58	37	47
その他	1	2	0	5	3	2

※ 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。

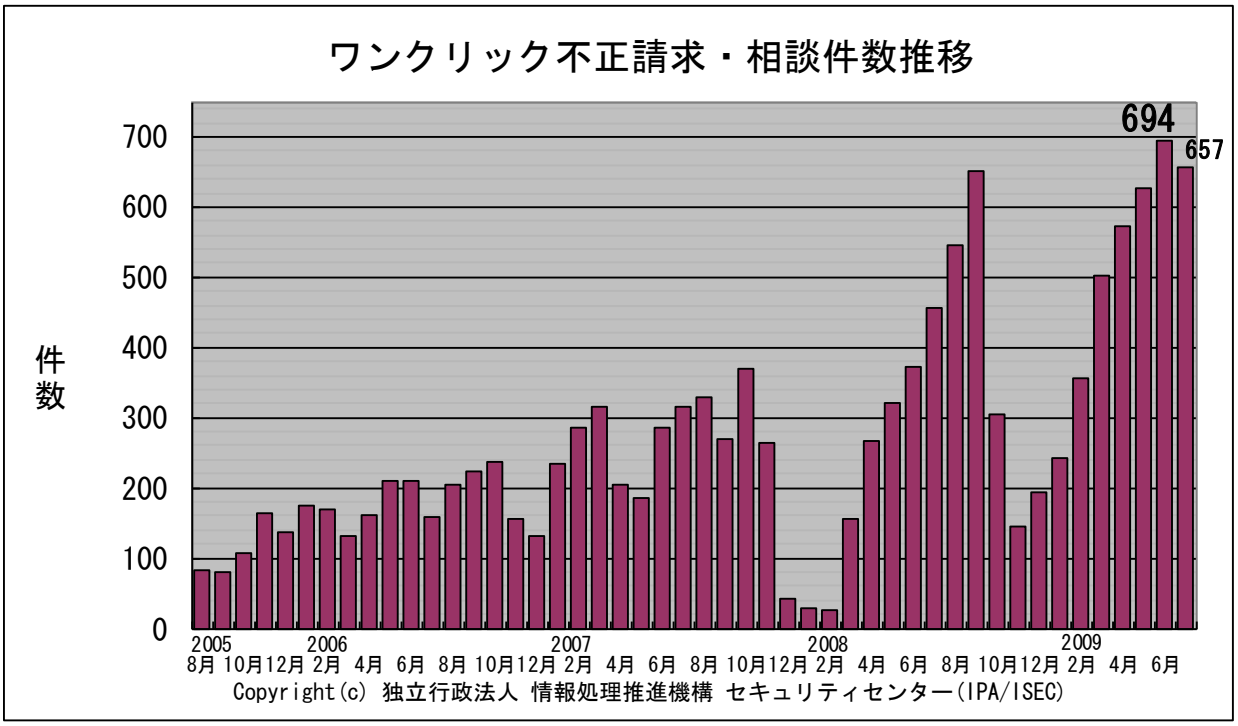


図 4-1：ワンクリック不正請求相談件数の推移

主な相談事例は以下の通りです。

（i）外部公開サーバや企業内パソコン・ネットワークのセキュリティ対策はどうすれば？

相談	社外に公開するサーバや、社内のパソコンやネットワークのセキュリティ対策を検討しています。一般的には、どのようなセキュリティ対策をどの程度実施すればいいのでしょうか。
回答	それぞれの企業・組織に適するセキュリティ対策の内容は様々ですので、一概には言えません。**まずは現状把握から始め、その結果を踏まえ、自社に最適な対策方法を検討するのが良いでしょう**。当機構から、ガイドラインを公開しておりますので、参考にしてください。 （ご参考） IPA - 中小企業の情報セキュリティ対策ガイドライン http://www.ipa.go.jp/security/fy20/reports/sme-guide/press.html

（ii）ウイルス対策をやりたがらない知り合いがいる

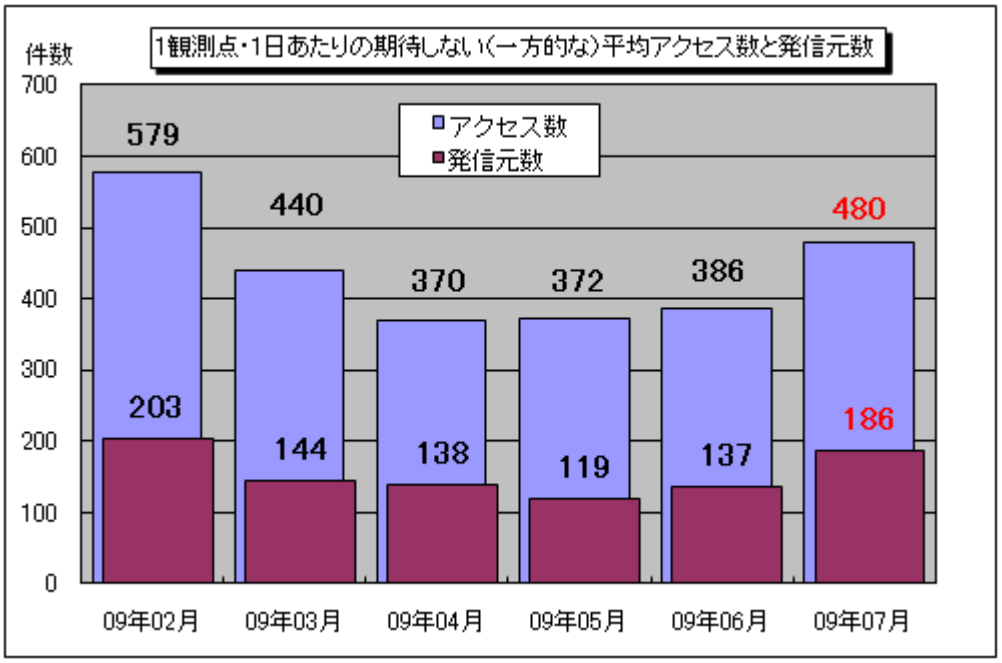
相談	知り合いに、パソコンのウイルス対策を実施するように勧めているが、 ・ウイルス対策ソフトを入れると動作が重くなるからイヤ ・お金が掛かるからイヤ ・ウイルス感染したって、パソコン内に重要なデータは無いから問題ない と言って、ウイルス対策ソフトすら導入しようとしない。知り合いをどうやって説得したら良いでしょうか。
回答	**ウイルス感染したままパソコンを使っていると、ウイルスが迷惑メールを勝手に送信したり、他のサイトを攻撃したりするなど、加害者になってしまう可能性があります**。その場合、プロバイダから警告が届くことや、一方的に接続を拒否されることがあります。**ネット社会の秩序を正常に保つためには、パソコン利用者一人一人がセキュリティ意識を持ち、適切な対策を実施する必要がある**、ということを説得材料にしてみてはいかがでしょうか。IPA では、対策実施の際に役立つ資料を用意していますので、活用してください。 （ご参考） IPA - 対策のしおり　シリーズ http://www.ipa.go.jp/security/antivirus/shiori.html

5. インターネット定点観測での 7 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 7 月の期待しない（一方的な）アクセスの総数は 10 観測点で **148,935 件**、総発信元（※）は **57,687 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 186 の発信元から 480 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。



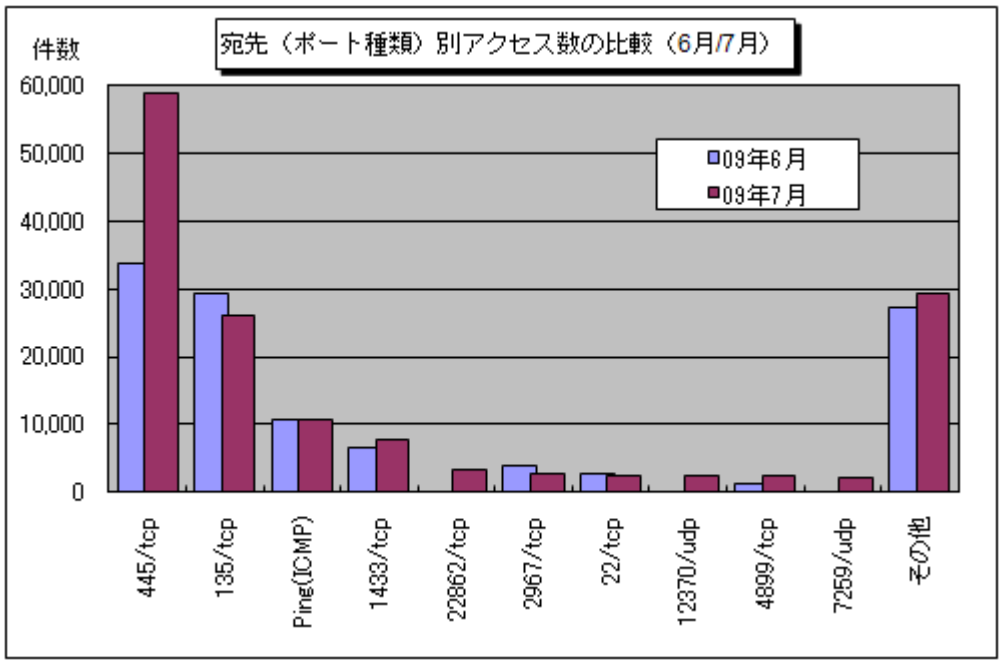
【図 5-1：1 観測点・1 日あたりの期待しない（一方的な）平均アクセス数と発信元数】

2009 年 2 月～2009 年 7 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。7 月の期待しない（一方的な）アクセスは、6 月と比べて増加しました。

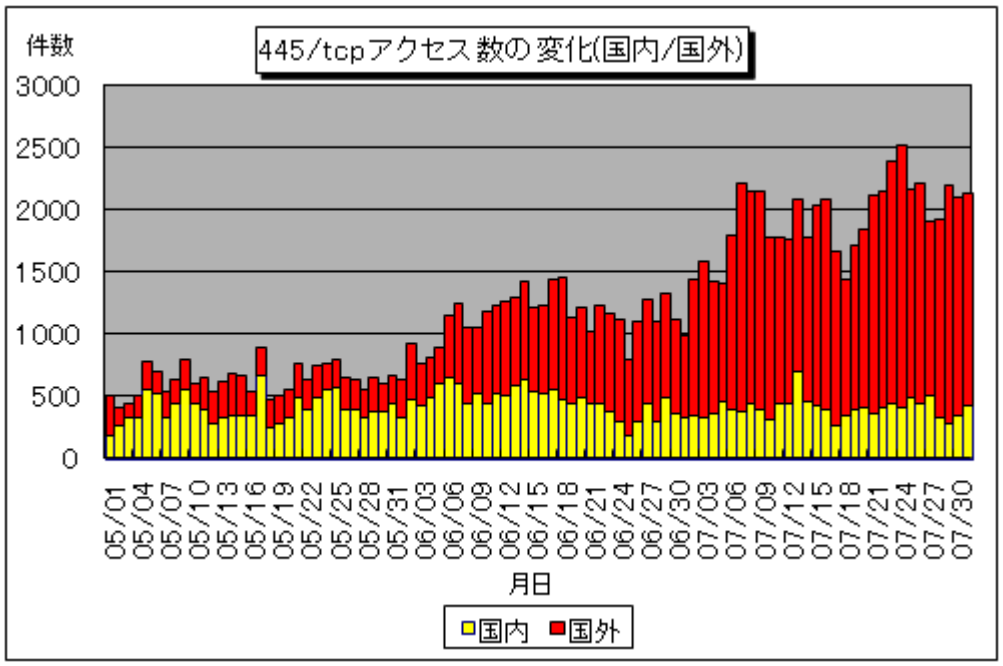
6 月と 7 月の宛先（ポート種類）別アクセス数の比較を図 5-2 に示します。

7 月は 6 月に増加した 445/tcp へのアクセスがさらに増加していました。6 月にアクセス数が増加したのは国外からのアクセスが増加したためでしたが、7 月も継続して国外からのアクセスが増加していました（図 5-3 参照）。その原因については特定できておりませんが、6 月同様、特定の発信元からのアクセス回数が増加したわけではなく、国外からの発信元数自体がさらに増加したことでアクセス数の増加につながっていました。

また、6 月は全く観測されなかったポートへのアクセスが、複数のポート（22862/tcp、12370/udp、7259/udp など）で観測されました。これらのポートへのアクセスが何を目的としたものだったかは不明ですが、いずれも特定の 1 観測点のみで観測されたアクセスでした。



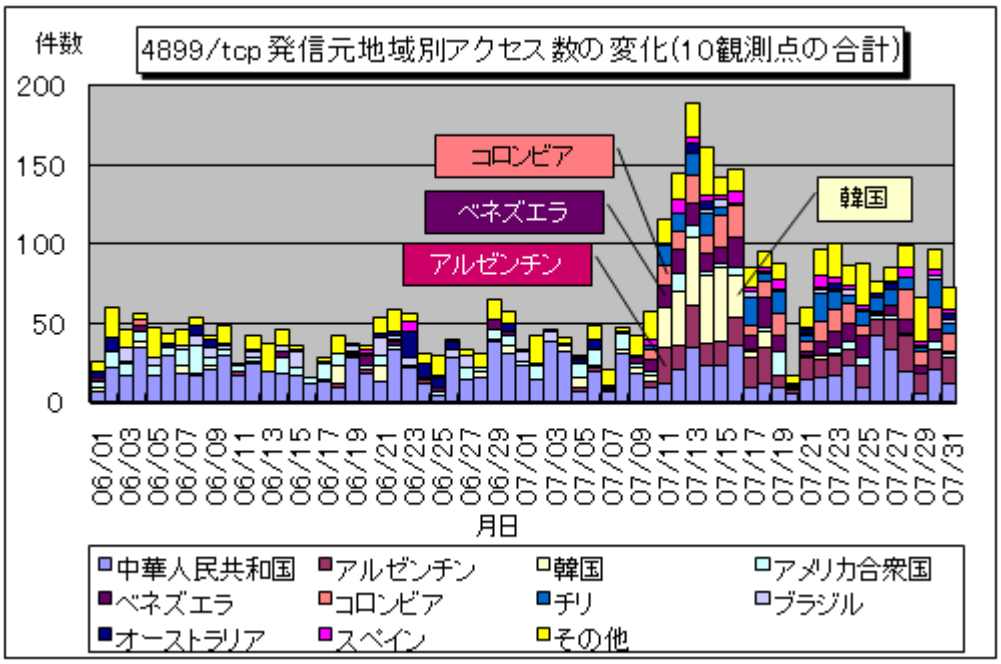
【図 5-2：宛先（ポート種類）別アクセス数の比較（6 月/7 月）】



【図 5-3：445/tcp アクセス数の変化（国内/国外）】

（1）4899/tcp へのアクセス

7 月の中頃に、一時的に 4899/tcp へのアクセスが増加した期間がありました。これは、韓国の 1 つの発信元からのアクセスと、アルゼンチン、ベネズエラ、コロンビアなどの南米地域の多数の発信元からのアクセスが増加したためです（図 5-4 参照）。



【図 5-4：4899/tcp 発信元地域別アクセス数の変化（10 観測点の合計）】

南米地域の発信元からの 4899/tcp へのアクセスの増加は、定点観測を行っている他の組織でも観測されており、広い範囲で同様の事象が発生している可能性があります。

4899/tcp は、Famatech 社のリモートコントロールソフトウェア Radmin が使用するポートとして知られています。

Radmin の利用者は、4899/tcp に対して、接続を許可していない発信元からのアクセスが来ていないかを確認し、状況に応じてアクセス制限（接続を許可する IP アドレスの範囲を絞るなど）や、接続認証の強化を行ってください。

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/TALOT2-0908.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