IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
第 08-11-126 号
2008 年 7 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［2008 年 6 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 6 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

「 自宅の無線 LAN のセキュリティ設定を確認しよう！」
― あなたの無線 LAN は本当に安全ですか？ ―

IPA に寄せられる一般家庭の無線 LAN に関する相談の中には、「無線 LAN が外部から不正アクセスされていないか不安になった」という内容のものが目立ちます。そのような相談者のほとんどは、セキュリティ設定が十分でない状態で無線 LAN を利用していました。

実際の相談として、「自宅のインターネットの通信速度が異常に遅くなった。試しに無線 LAN を外してみたら、明らかに通信速度が元に戻った」というものがありました。相談者の無線 LAN が何者かによって無断で利用され、通信を行われていた可能性が高いと言えます。

無線 LAN はケーブルを繋がずにネットワークを利用できるので非常に便利ですが、セキュリティ設定が十分でない場合、様々な被害に遭う危険性があります。

一般家庭で無線 LAN を利用している方は、この機会にセキュリティ設定を再確認して下さい。

(1)無線 LAN のセキュリティ対策の重要性

無線 LAN は、電波を使って無線 LAN アクセスポイント（以下、親機とする）と無線 LAN 機能を持つパソコンなど（以下、子機とする）との間で通信を行うネットワーク環境のことです。親機と子機の双方に設定をすることで、通信が可能になります。電波の届く範囲なら壁などの障害物を超えてどこでも通信が可能という便利さを備えています。しかし、その便利さとは裏腹に、悪意ある者から不正アクセスの対象として狙われ易い環境とも言えます。しかも、電波という、目に見えない通信経路を使うということは、侵入されていることさえも気付きにくいため、大きな脅威となります（図 1-1）。

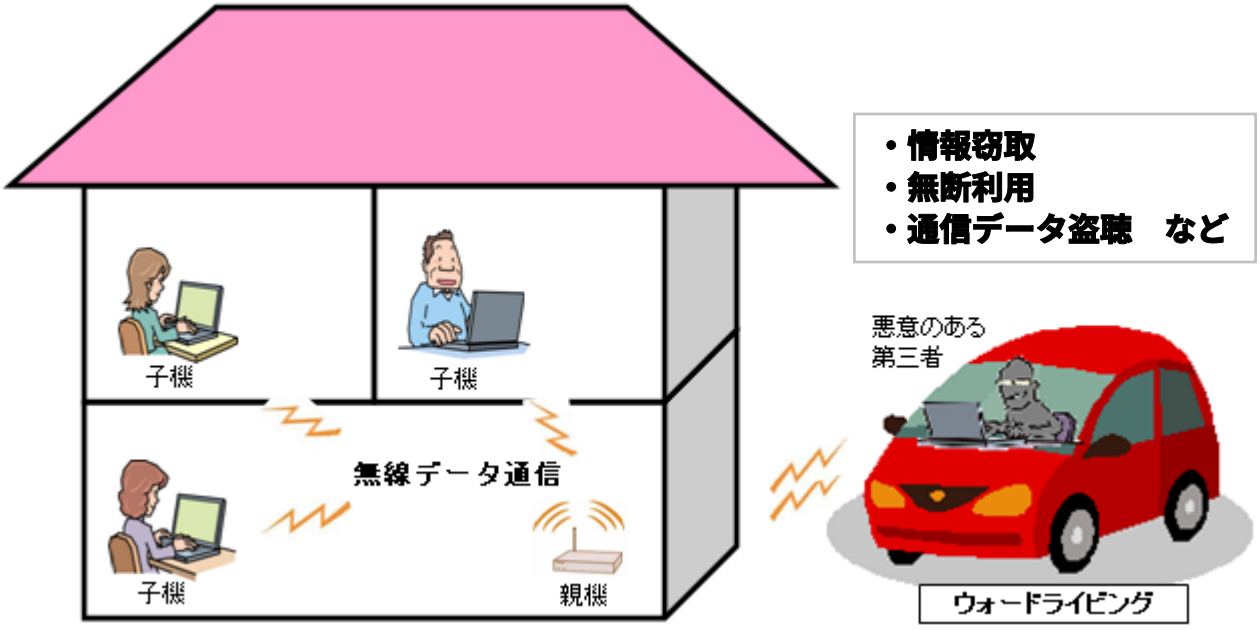

図1-1 無線LANの脅威

想定される被害として以下のようなことが挙げられます。

・無線 LAN 環境に侵入され、重要な情報を盗まれる。
・無線 LAN 環境を無断で利用される。
・通信データを盗聴される。

これらの行為の多くは、無防備な親機を介して行われます。悪意ある者は、ウォードライビング（War Driving）と呼ばれる行為によって、無防備な親機を探し回っています。こうして探索された無防備な親機が犯罪に利用されたと思われる事件がいくつか起きています。

国内では、2005 年に不正アクセス事件の犯人が、メールの本当の発信元を隠すために他人の親機を無断で経由して、ウイルスメールの送信に使っていたという事例がありました。2008 年 6 月には、他人の親機を無断で経由してインターネットの掲示板に脅迫文書を書き込んだとして、高校生が書類送検された事件が発生しています。

このような被害に巻き込まれないためにも、無線 LAN のセキュリティ対策には十分注意する必要があります。

(2)無線 LAN のセキュリティ設定

無線 LAN のセキュリティを適切に設定するには、多くの知識や管理の手間を必要とするために、一般の方にとっては非常に重荷です。この問題を改善するために制定された仕組みが、WPS（Wi-Fi Protected Setup）です。**WPS に対応した親機と子機同士であれば、複雑なセキュリティ設定項目をワンタッチで自動設定でき、簡単かつ安全にネットワークの接続が可能**となりますので、**一般家庭では WPS の使用をお勧めします**。

（i）これから無線LANを導入しようとしている方

WPS 対応の親機と子機を準備し、WPS によって自動設定することを推奨します。

（ii）既に無線LANを利用している方

現在お使いの親機と全ての子機が「WPSに対応しているか」を確認しましょう。WPSに対応していると分かった場合は、WPSの機能が使われているか（有効になっているか）を確認しましょう（図1-2）。もし使われていなかった場合は、WPSを使用するようにしましょう。

親機と、1台以上の子機がWPSに対応していれば、WPSを使用できます。しかし、現在お使いの**子機の中に、WPSに対応していないものがあった場合は、その子機に限っては設定を手動で行う必要があります**。「(3) 手動によるセキュリティ設定の手順」を参考にしてください。

また、親機と子機が**WPSに対応していない場合でも、無線LAN機器メーカー独自の自動設定機能を使える場合は、それを使用**してください。**メーカー独自の自動設定機能も使用できない場合は、設定を手動で行う必要があります**。

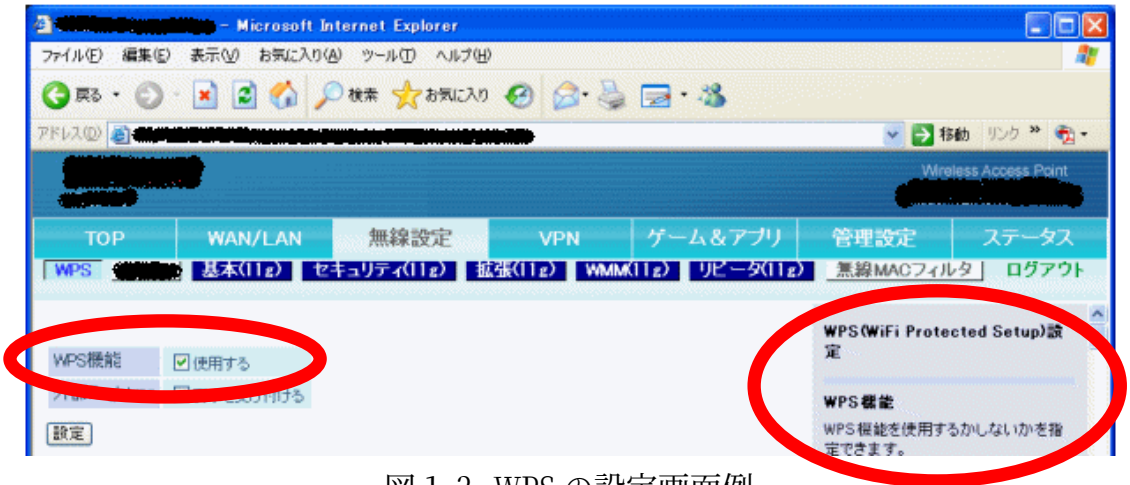

図 1-2　WPS の設定画面例

(3)手動によるセキュリティ設定の手順

セキュリティ設定の中でも、通信の途中で内容を見られたり改ざんされたりしないようにデータを変換処理する**暗号化方式がポイント**になります。この暗号化方式が強力でないと、短時間で通信内容が解読され盗聴されると同時に、認証が破られ、無断利用を許してしまいます。したがって、**適切な暗号化方式を選択することが最も重要になります。**

設定は、まず初めに親機の設定をしてから、次に子機側の設定を親機に合わせる、という手順となります。パソコン本体に無線 LAN 機能が内蔵されていない場合は、無線 LAN カードなどを子機として接続し、パソコンから設定します。

無線 LAN セキュリティ設定において**暗号化方式を選択するにあたり注意すべきことは、親機と子機の全てが、選択したい暗号化方式を選択可能であるとは限らない、ということ**です。

以下の手順で、適切な暗号化方式を選択してください。ここでは暗号化方式の適切な選択方法について親機の設定を例に説明しますので、子機も同様に設定してください。それぞれの暗号化方式の特徴については、以下の（ご参考）を参照して下さい。

(i) 暗号化方式にはいくつか種類がありますが、**WPA2-PSK**という最もセキュリティ強度が高い方式を選択してください。その中から、“AES暗号を使うWPA2-PSK”という意味である「**WPA2-PSK（AES）**」という方式を選択することを推奨します。しかし、親機によってはWPA2-PSKに対応していないものもあります。対応しているかどうか、自身で判断がつかない場合は取扱説明書を確認するか、メーカーへ問合わせてください。
暗号化方式を選択したら、「(4)パスワードの設定」に進んでください。

(ii) WPA2-PSKに対応していない場合は、次善の策として**WPA-PSK**という方式を選択してください。WPA-PSKには、AES暗号を使う「**WPA-PSK（AES）**」とRC4暗号を含んだ技術であるTKIPを使う「**WPA-PSK（TKIP）**」という2種類の方式があり、通常はセキュリティ強度が高い「**WPA-PSK（AES）**」という方式を選択することを推奨します。親機と子機とが接続できないなどの問題が生じた場合に限り、「**WPA-PSK（TKIP）**」を選択してください。
暗号化方式を選択したら、「(4)パスワードの設定」に進んでください。
しかし、WPAはWPA2よりセキュリティ強度が劣りますので、あくまでもWPA2対応機へ移行するまでの“つなぎ”としての役割であるという認識を持って使用して下さい。

(iii) WPA2-PSKとWPA-PSKに対応していない場合でも、**内部ソフトウェアのアップデートによりWPAに対応できるものもあります**。詳細については、メーカーのホームページなどで確認しましょう。**WPAに対応できない場合は使用しないで下さい**。

以上のように、**親機と子機が対応している暗号化方式を確認し、その中から最もセキュリティ強度の高いものを選択する**、という流れになります。

なお、**親機と全ての子機とが、選択したい暗号化方式に対応していなければなりません**。つまり、WPA2-PSK（AES）を使いたい場合は、親機と全ての子機が WPA2-PSK（AES）に対応していることが条件です。

(4)パスワードの設定

WPA2-PSKやWPA-PSKでは、無線LANの盗聴や無断利用を防ぐためのパスワードを設定します。WPSで設定した場合は、パスワードも自動で設定されます。**パスワードを手動で入力する際は、容易に推測されることを防ぐため、以下の注意事項に従ってください**。

(i) 英語の**辞書に載っている単語を使わない**
(ii) **大文字、小文字、数字、記号の全てを含む**文字列とする
(iii) 文字数は**最低でも20文字**（半角英数字＋記号の場合。最大で63文字）

(ご参考)

暗号化方式の種類

現在使われている、3 つの無線 LAN の暗号化方式の特徴は以下の通りです (表 1-3)。

(i) WEP (Wired Equivalent Privacy)

WEPは、無線LANの世界で最初に登場した暗号化方式です。今までに以下のようないくつかの欠点が見つかっているため、**現状では使用することを推奨しません**。

(a) 暗号化に使う鍵データの生成方法が単純であるため、解析が容易であること。
(b) パスワードを変更しない限り、暗号化に使う鍵は同じものが使用され続けること。
(c) (a) および (b) が原因で、暗号化方式そのものが既に解読されていること。
(d) 通信データの改ざん検知ができないこと。

(ii) WPA (Wi-Fi Protected Access)

WPAは、欠点が多いWEPの代わりとして考えられた方式です。新たに**TKIP** (Temporal Key Integrity Protocol) と呼ばれる技術が採用され、WEPの欠点として前述した (a)、(b)、(d) が改善されています。しかし、暗号強度に直接影響する暗号技術がWEPと同じままであるため、**暗号化方式として万全とは言えません**。一般家庭向けのモードとしては、簡易認証方式として**PSK** (Pre-Shared Key) を使う**WPA-PSK**があります。

(iii) WPA2 (Wi-Fi Protected Access 2)

WPAの改良版であるWPA2では、より強力な暗号技術である**AES** (Advanced Encryption Standard) を採用しているため、**WEPやWPAの欠点が全て解消されている**と言えます。一般家庭向けのモードとしては、簡易認証方式として**PSK** (Pre-Shared Key) を使う**WPA2-PSK**があります。**一般家庭においては、暗号化方式としてWPA2-PSKが最も強力であり、安全**です。

表1-3 無線LANで用いられる暗号化方式の比較

	WEP	WPA	WPA2
暗号の解読	比較的容易	困難	現状は不可能
暗号キーの生成方法	単純	複雑	複雑
暗号キーの更新機能	なし	あり	あり
暗号技術	RC4	RC4	AES
データ改ざん検知	なし	あり	あり

IPA「不正アクセス対策のしおり」
http://www.ipa.go.jp/security/antivirus/documents/4_fusei_v3.pdf
IPA「無線 LAN 利用環境のための運用上のセキュリティ対策」
http://www.ipa.go.jp/security/fy18/reports/contents/enterprise/html/411.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、6 頁の「3.コンピュータ不正アクセス届出状況」を参照)
・SQL インジェクション攻撃によってデータベースが改ざんされた
・ネットオークションで、誰かが自分になりすまして勝手に出品

○ 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 メモリにウイルスが感染？
・迷惑メール本文にあったアドレスをクリックしたら請求書メールが来た

○ 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。
・DoS 攻撃（SYN Flood 攻撃）の影響と思われるアクセスに注意！

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 23.6 万個**と、5 月の約 20 万個から 18.2%の増加となりました。
また、6 月の届出件数(※2)は、**2,002 件**となり、5 月の 1,737 件から 15.3%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。
・6 月は、寄せられたウイルス検出数約 23.6 万個を集約した結果、2,002 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 20.5 万個 、2 位は W32/Mywife** で**約 1.4 万個、3 位は W32/Mytob** で**約 4 千個でした。**

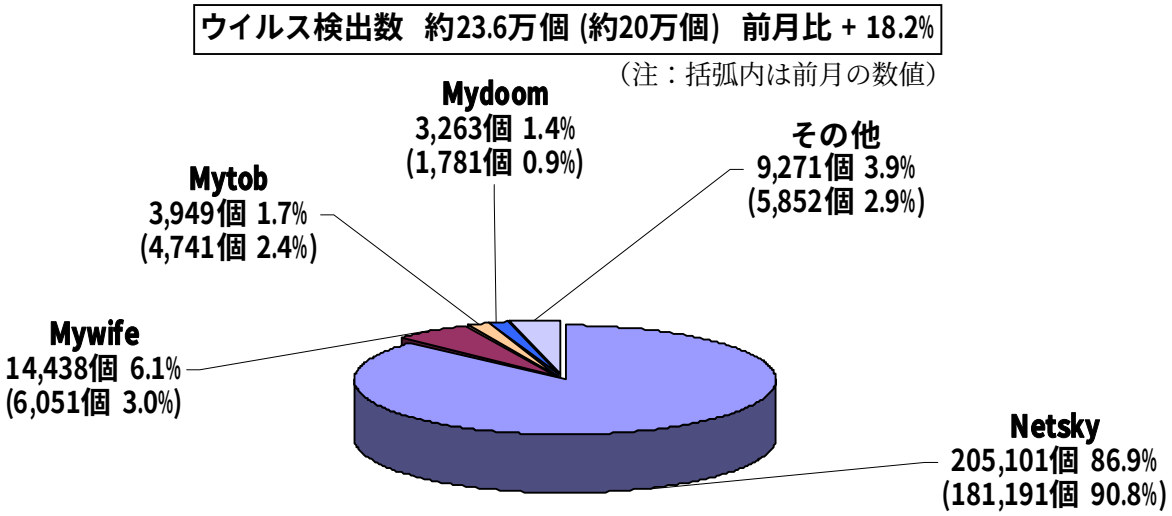

図 2-1

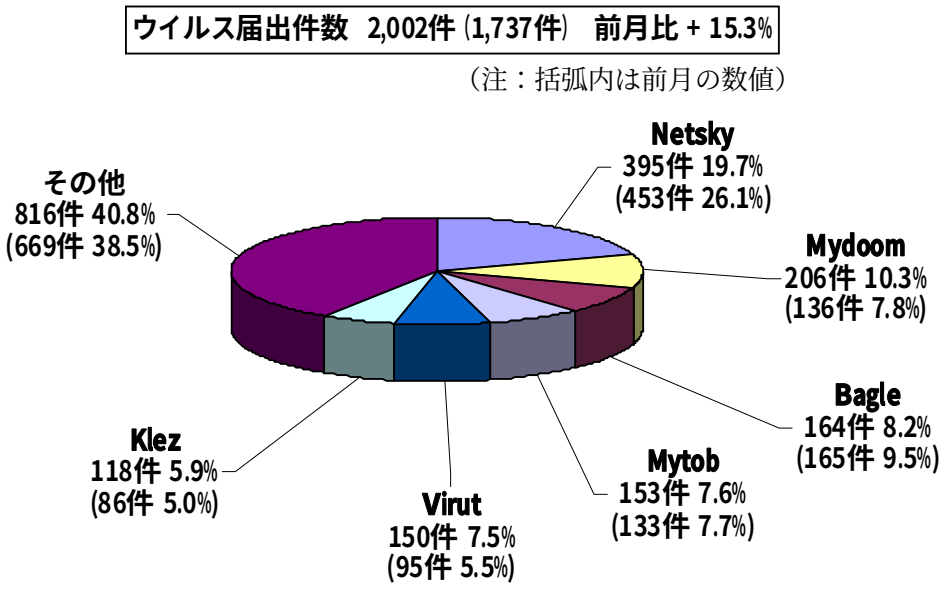

図 2-2

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

		1月	2月	3月	4月	5月	6月
届出(a) 計		**8**	**4**	**19**	**14**	**4**	**13**
	被害あり(b)	7	4	13	10	4	11
	被害なし(c)	1	0	6	4	0	2
相談(d) 計		**24**	**29**	**35**	**56**	**37**	**36**
	被害あり(e)	15	10	15	31	18	15
	被害なし(f)	9	19	20	25	19	21
合計(a+d)		**32**	**33**	**54**	**70**	**41**	**49**
	被害あり(b+e)	22	14	28	41	22	26
	被害なし(c+f)	10	19	26	29	19	23

（1）不正アクセス届出状況

6 月の届出件数は 13 件であり、そのうち何らかの被害のあったものは 11 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 36 件（うち 3 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 15 件でした。

（3）被害状況

被害届出の内訳は、**侵入 6 件、DoS 攻撃が 3 件、その他（被害あり）2 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て結果としてウェブページコンテンツを改ざんされてしまったものが 1 件、他サイト攻撃の踏み台として悪用されたものが 4 件、などでした。侵入の原因は、脆弱性によるものが 2 件（ウェブアプリケーション 1 件、その他ツール 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※によるものが 4 件、でした。

その他（被害あり）の被害として、ネットオークションサイトに本人になりすまして何者かにログインされ、勝手に商品を出品されていたものが 2 件ありました。

※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）SQL インジェクション攻撃によってデータベースが改ざんされた

事例	・外部公開している動画サーバで、動画が見られなくなっていたので調査したところ、動画へのリンクページに、不審な外部サイトの JavaScript を実行するためのスクリプト記述が挿入されていたことが判明。 ・さらに調査を進めたところ、ＳＱＬインジェクション攻撃を受け、ウェブアプリケーションの脆弱性を突かれてデータベースのデータが改ざんされていたことが判明。 ・ウェブアプリケーションの脆弱性対策は、データベースサーバ導入時の 2004 年に実施してから、以降は実施していなかった。
解説・対策	ウェブアプリケーションの脆弱性を突く攻撃手法は日々、新しいものが生み出されています。**脆弱性対策は、一度実施したら終わりではありません。定期的に脆弱性検査を受け、新たな脆弱性が生じていないか、確認しましょう**。また、日々のログを確認し、攻撃を受けていないか、侵入を許していないかも、こまめにチェックしましょう。 （参考） 安全なウェブサイト運営入門 http://www.ipa.go.jp/security/vuln/7incidents/ ウェブサイトの脆弱性検出ツール iLogScanner http://www.ipa.go.jp/security/vuln/iLogScanner/

（ii）ネットオークションで、誰かが自分になりすまして勝手に出品

事例	・ネットオークションで使っている ID が使えなくなった。 ・事務局に問い合わせたところ、自分の ID から偽ブランド品が多数出品されていたため、ID の利用が停止させられていたことが判明。 ・出品の手数料として、自分に数万円の請求が来た。
解説・対策	ネットオークションの不正では、他人の ID を悪用して本人になりすますことがほとんどです。商品取引に直接絡む金銭の問題以外にも、手数料請求などで、本来の ID 所有者に被害が生じる場合があります。**オークションをしばらく利用しない場合でも、時々オークションサイトにログインして、不正が行われていないか確認するようにしましょう**。被害を受けたら、すぐにサイト管理者に通報するとともに、警察機関に被害届を出しましょう。 （参考） 警察庁 － インターネット安全・安心相談 http://www.cybersafety.go.jp/

4．相談受付状況

6 月の相談総件数は **1211 件**であり、2005 年に統計を取り始めてから最多となりました。そのうち**『ワンクリック不正請求』に関する相談**が **372 件**（5 月：320 件）となり、**過去最多記録を更新**しました。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 **14 件**（5 月：1 件）、**Winny に関連する相談**が **4 件**（5 月：8 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

	1月	2月	3月	4月	5月	6月
合計	**408**	**350**	**654**	**938**	**1080**	**1211**
自動応答システム	219	192	373	514	649	693
電話	151	110	214	335	379	456
電子メール	38	47	66	87	48	60
その他	0	1	1	2	4	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）、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。

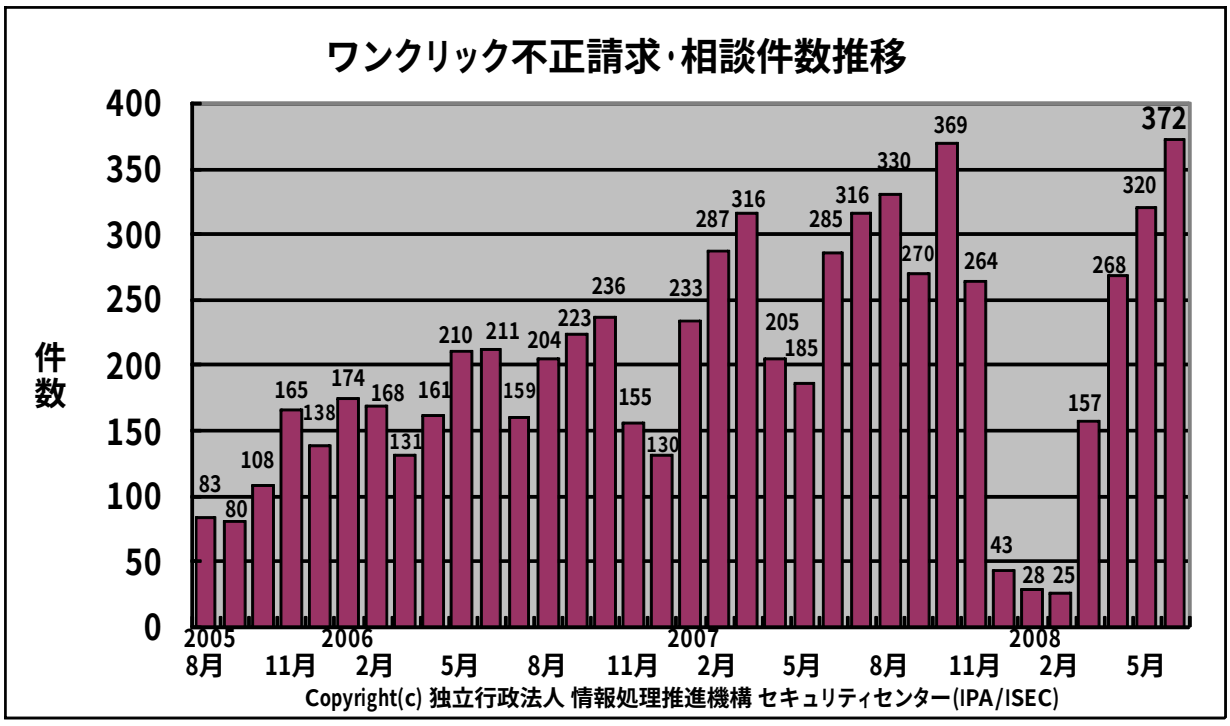

図 4-1　ワンクリック不正請求相談件数の推移

主な相談事例は以下の通りです。

(i) USB メモリにウイルスが感染？

相談	自分の USB メモリに、ウイルスが感染していると言われた。気持ち悪いので、初期化（フォーマット）しようと思う。ウイルスが感染していたとしても、フォーマットすればウイルスは消えますか？
回答	**USB メモリをフォーマットすれば、USB メモリ内にあるファイルは全て削除されます**。ウイルスに感染していたとしても、それらも含めて全て削除されます。 ただし、**ウイルスに感染しているパソコンでフォーマット作業をしても、フォーマット完了直後に再度ウイルスに感染してしまいます**。よって、フォーマット作業をする際は、適切なウイルス対策がなされており、ウイルスに感染していないパソコンを使用する必要があります。 （ご参考） 呼びかけ：「USB メモリを安易にパソコンに接続しないように！」 http://www.ipa.go.jp/security/txt/2007/07outline.html

(ii) 迷惑メール本文にあったアドレスをクリックしたら請求書メールが来た

相談	身に覚えのない女性名の差出人で、メールが届いた。迷惑メールだとは思ったが、ちょっと興味がわいて、メール本文中にあるアドレスをクリックしてホームページを見てしまった。その後、当該ホームページを見たということで、請求書メールが届いた。請求書内には、自分が当該ホームページを見た際の自分の IP アドレスが記載されていた。IP アドレスから、自分の住所や名前などの個人情報が業者に知られてしまいますか？
回答	プロバイダのサービスを利用している個人ユーザであれば、自ら個人情報を相手に伝えていない場合、**個人情報はプロバイダが洩らさない限り、相手には伝わりません**。また、**プロバイダには個人情報保護の義務があるため、警察機関などからの正当な要請がない限り、個人情報を相手に伝えることはありません**。つまり、今回の件では、業者に個人情報が伝わっていないと思われます。 （ご参考） 財団法人日本データ通信協会　迷惑メール相談センター http://www.dekyo.or.jp/soudan/

5．インターネット定点観測での 6 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 6 月の期待しない（一方的な）アクセスの総数は 10 観測点で **156,012 件**、総発信元数(※)は **55,589 箇所**ありました。1 観測点で見ると、1 日あたり **185** の発信元から **520 件**のアクセスがあったことになります。

総発信元数（※）：TALOT2 にアクセスしてきた発信元の総数。なお、同一発信元から同一観測日・観測点・ポートにアクセスがあった場合は 1 つの発信元としてカウント。

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、185 人の見知らぬ人(発信元)から、発信元一人当たり約 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。

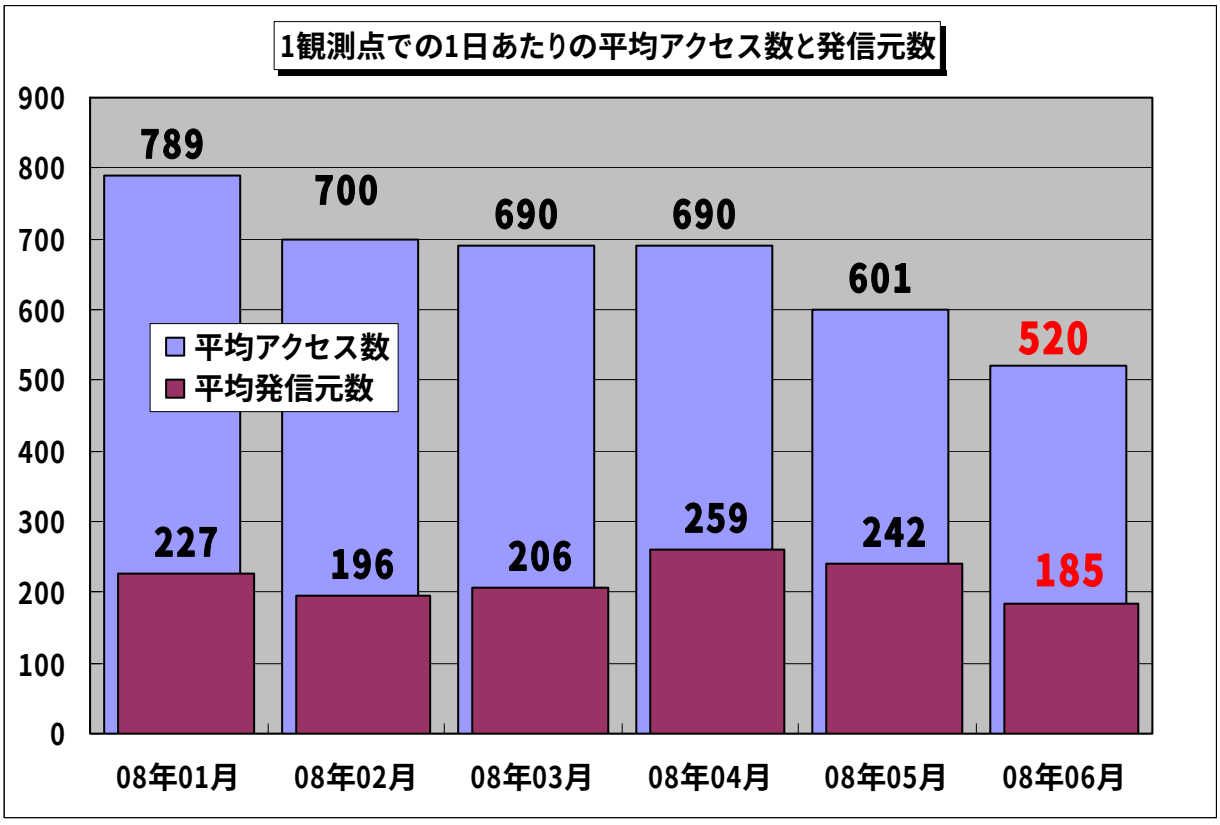

図 5-1：1 観測点での 1 日あたりの期待しない(一方的な)アクセス数および発信元数

2008 年 1 月～2008 年 6 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 5-1 に示します。この図を見ると、6 月の期待しない（一方的な）アクセスは 5 月と比べて減少しており、過去 6 ヶ月間を通してみても、徐々に減少傾向を示していると言えます。

（1）DoS 攻撃（SYN Flood 攻撃）(*1)の影響と思われるアクセス

6 月の後半に香港方面の通信事業者を狙った DoS 攻撃（SYN Flood 攻撃）の影響と思われるアクセスが 2 箇所の観測点で確認されています。これらのアクセスは宛先ポート 829/tcp 及び 881/tcp（発信ポートは 80）への SYN+ACK パケットでした。

TALOT2 で使用しているアドレスが、攻撃者が発信元詐称に利用したアドレスと一致した為に、標的となった企業からの SYN+ACK パケットが大量に届いたということです。その時の時間単位のアクセス状況を図 5-2 に示します。

※このアクセスは直接的な攻撃を狙ったアクセスではなく統計情報にそぐわない為、集計からは除外しています。

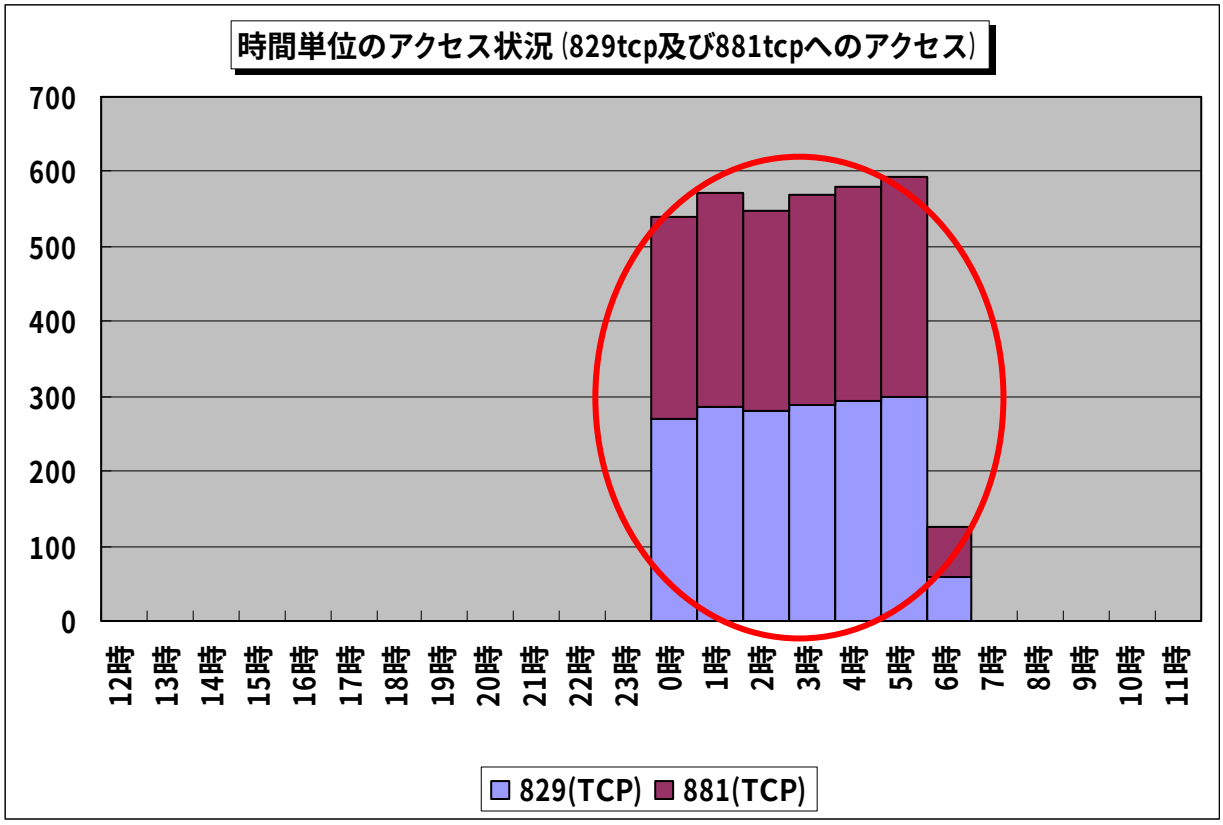

図 5-2：香港方面への SYN Flood 攻撃のバックスキャッタ (*3)

TALOT2 が観測点として使用しているアドレスは、不定期に変更しています。今回取得した 10 箇所のアドレスのうち、2 箇所もこの攻撃に利用されていたということは、他にも利用されていたアドレスが多数あると推測されます。

このように本人が攻撃対象として狙われていなくても、不正なアクセスを受信することがあるので、外部からの不要なポートがファイアウォールでフィルタリングされているか確認することをお勧めします。

(*1):DoS 攻撃（SYN Flood 攻撃）

「サービス妨害攻撃」Denial of Service の略からＤｏＳ攻撃と呼ばれ、標的マシンにおけるサービス機能を停止または低下させる攻撃のこと。このＤｏＳ攻撃の１つに、標的マシンに「過負荷を与える攻撃」として SYN Flood 攻撃があります。これは、標的マシンに対して発信元アドレスを詐称した SYN パケット(3 ウェイ・ハンドシェーク(*2)での接続確立の最初に送られるパケット)を大量に送りつけ、確立途中状態の接続を大量作成するものです。

(*2):3 ウェイ・ハンドシェーク

TCP で通信を行う際に、最初に行われる通信確立のための手順を、3 ウェイ・ハンドシェークと言います。この手順により、通信を行う相手同士が通信の準備ができたことを確認できるわけです。

以下に A と B の通信確立の手順を示します。

①A から B へ SYN パケットの送信

②B から A へ ACK+SYN パケットの送信

③A から B へ ACK パケットの送信

これで、AB 双方の通信が確立されます。

(*3):バックスキャッタ

DoS 攻撃（SYN Flood 攻撃）において攻撃者が詐称した発信元アドレスに、標的マシンから大量の SYN+ACK パケットが返信されてくることです。

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/2008/documents/TALOT2-0807.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