IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
第 07-14-109 号
2007 年 8 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［2007 年 7 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、2007 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

今月の呼びかけ：
「忘れずに、ネットと心のファイアーウォール※」
― 夏休みに、親子でパソコンの利用方法、セキュリティ対策を話し合おう！！ ―

※（情報セキュリティ標語 2007 大賞 北海道・遺愛女子高等学校 / 福士 彩織さん）

(1) 被害の状況

最近 IPA では、「子供がインターネットを利用していて、請求書が表示されるようになり、その画面が消えなくなってしまい、困っています」というような保護者の方からの相談を毎日のように受けています。これは、例としてアダルトサイトや出会い系サイトのような有害なサイト(以下「有害サイト」という)に、その危険性を知らずに興味本位で入り込んでしまった結果、パソコンに請求書を表示する不正プログラムが埋め込まれたためです。

(2) 予防策

この様な被害に遭わないためには、
(a)ウイルス対策ソフトを導入する。さらに、常に最新のパターンファイルに更新しておく。
(b)Microsoft Update や Windows Update、その他ソフトのアップデートを定期的に実施してセキュリティホールを解消する。
などの基本的な対策を実施するとともに、
(c)有害サイトに行かない、有害サイト内の写真や動画を安易にクリックしない。
(d)万が一有害サイト内の写真や動画をクリックして、セキュリティの警告画面が表示されても、無視をしないで内容を確認し、安易に不正プログラムをダウンロードしない。
などの心構えも重要です。

しかし、最善の予防策はインターネット上の有害サイトにはあらかじめアクセスできないようにしてしまうことです。**予防策に必要なものとしては、インターネット上に存在する有害な情報を遮断することができる対策ソフト（フィルタリングソフト）や、プロバイダによる有害サイト遮断サービス（フィルタリングサービス）があります。**保護者の方がこの様な予防策を行うことで、お子さんによる、インターネット上に公開されている有害な情報へのアクセスを未然に防ぐことができます。

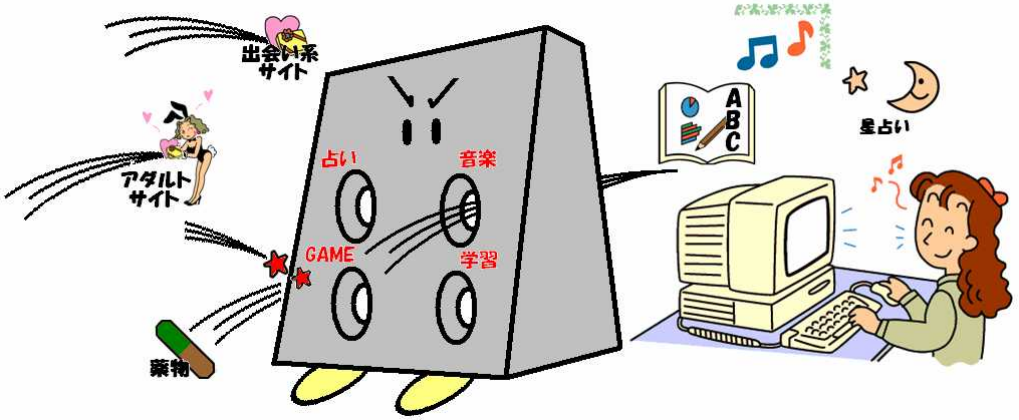


図1：フィルタリングソフトのイメージ

フィルタリングソフトは、ウイルス対策ソフトに含まれていたり、単体のソフトとして購入することが出来ます。導入する場合は、ご利用中のウイルス対策ソフトメーカー又は、販売店にご相談ください。

夏休みなど長期の休みに入り、家庭でパソコンやインターネットを利用する機会が増えます。**保護者の方は、お子さんがどのようにパソコンやインターネットを利用しているかを確認してください。また、以下のサイトを参照して、利用しているパソコンのセキュリティ対策を実施してください。その際に、親子でパソコンのセキュリティ対策やインターネットを安全に利用するための約束事を決めること**をお薦めします。

「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
「Windows Update 利用の手順」(マイクロソフト社)
http://www.microsoft.com/japan/security/square/guard/a04g11.asp
「クリックしただけで料金請求された場合の対応方法について」
http://www.ipa.go.jp/security/ciadr/oneclick.html

(3) 被害の解決策

請求書が表示された場合でも、慌てないようにしましょう。決してすぐに**お金を振り込んだり、請求書の連絡先にメールや電話で問い合わせをしたりしてはいけません。**一旦パソコンを再起動して、請求書が表示されるかを確認してください。再起動後に請求書が表示されなければ、そのまま無視してください。再起動後も請求書が表示される場合には、不正プログラムが埋め込まれていますので、以下の「システムの復元機能でシステムの状態を以前の正常な状態に戻す」を行ってください。それでも請求画面が消えない場合は、お使いのパソコンを初期化する必要があります。

(a) システムの復元機能でシステムの状態を以前の正常な状態に戻す

以下のマイクロソフトのホームページを参考にして、「システムの復元」機能を使用してシステムを請求書が表示される前の日に戻すことを行ってください。

ただし、選択した任意の日から現在までに行われた、OS の設定変更やソフトウェアのインストール、アップデート等をした場合は、それらの情報は消えてしまいますので、システム復元後に再度実施してください。

なお、選択した任意の日から現在までに作成した文書や送受信したメール情報並びにホームページへのアクセス履歴やお気に入りは消えません。

「システムの復元のやり方」
http://www.microsoft.com/japan/windowsxp/pro/business/feature/performance/restore.mspx

(b) パソコンの初期化

パソコンを購入した時の状態に戻す作業を実施します。

実際の作業方法は、購入時に添付されている説明書に記載されている「購入時の状態に戻す」等の手順に沿って作業してください。

作業する前に重要なデータを外部媒体等に必ずバックアップしてから作業を行って下さい。

（情報セキュリティポスター2007 大賞　佐賀県・弘学館中学校 / 諸隈 幸宏さん）

IPA では、「第 3 回　情報セキュリティ標語・ポスター」を募集しています。この夏休みを利用して御家族で話し合った内容を元に、情報セキュリティに関する標語やポスターに応募してみてはいかがでしょうか。締め切りは、2007 年9月10日(月)です。

「第３回 情報セキュリティ標語・ポスター」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：2007年7月１日(日)～2007 年9月１０日(月)
応募方法：電子メール、ＦＡＸ、郵送
　　詳しくは、下記のホームページをご参照下さい。
　　http://www.ipa.go.jp/security/event/hyogo/2007/boshu.html
賞　　金：大賞（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）、その他、参加企業賞あり

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　山田／岸原
Tel:　03-5978-7508
Fax:　03-5978-7518
E-mail:　isec-hyogo@ipa.go.jp

問い合わせ受付時間 9:30 - 18:30 月曜日～金曜日
（祝祭日、振替休日を除く）

2. システム管理者の方へ、夏季休暇における対策のお願い

夏季休暇は、システム管理者が不在になる場合が予想され、ひとたびウイルス・ワーム感染や不正アクセスによる Web 改ざん・メール不正中継などの被害に遭うと不在期間中に被害範囲が拡大する可能性があります。

システム管理者の方は、ファイアウォールなどを適切に設定し、攻撃に対して確実に検出・対応できるようにするとともに、必要な修正プログラムを的確に適用するなど、日常のセキュリティ対策内容を再度確認して頂き、可能な対策を実施して、万全の体制を整えてください。

また、休暇中に自宅へパソコンを持ち帰るユーザも多くいると推測されるため、休暇明けの出勤時にはパソコンのワクチンソフトを最新の定義ファイルに更新した上でインターネットへ接続させ、必ずウイルスチェックをしてから LAN に接続させてください。さらに、新種ウイルスや新たなセキュリティホールが公開されていないか、情報収集を行い、必要があれば迅速に対策を実施するとともに、ユーザへ通知するなどを徹底するようにしてください。

その他、以下の対策情報などを参考に休暇に入る前に、対策の実施、体制の確立をしてください。

「情報セキュリティ対策実践情報」
http://www.ipa.go.jp/security/awareness/administrator/administrator.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、7 頁の「4.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、ボットを設置された
- SNS のアカウントが誰かに乗っ取られた

○ 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「5.相談受付状況」を参照）
- 金融情報サイトを見ていたらウイルス警告が！
- 不正アクセスされているとの警告が出る

○ 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。
- アプリケーションソフトウェアのぜい弱性を狙ったアクセスが増加！

3. 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 51 万個**と、6 月の 50 万個から 3.4%の増加となりました。
また、7 月の届出件数(※2)は、**3,069 件**となり、6 月の 2,898 件から 5.9%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。
・7 月は、寄せられたウイルス検出数約 51 万個を集約した結果、3,069 件の届出件数となっています。

検出数の1位は、**W32/Netsky で約 44 万個 、2 位は W32/Mytob で約 1 万個、3 位は W32/Stration で約 1 万個でした。**

ウイルス検出数　約51万個（約50万個）　前月比 + 3.4%

（注：括弧内は前月の数値）

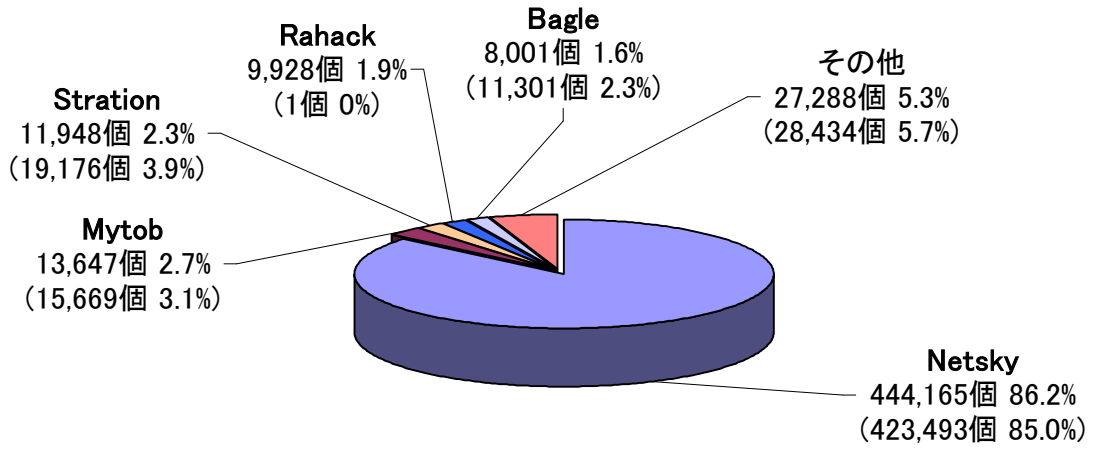


図:3-1

ウイルス届出件数　3,069件（2,898件）　前月比 + 5.9%

（注：括弧内は前月の数値）

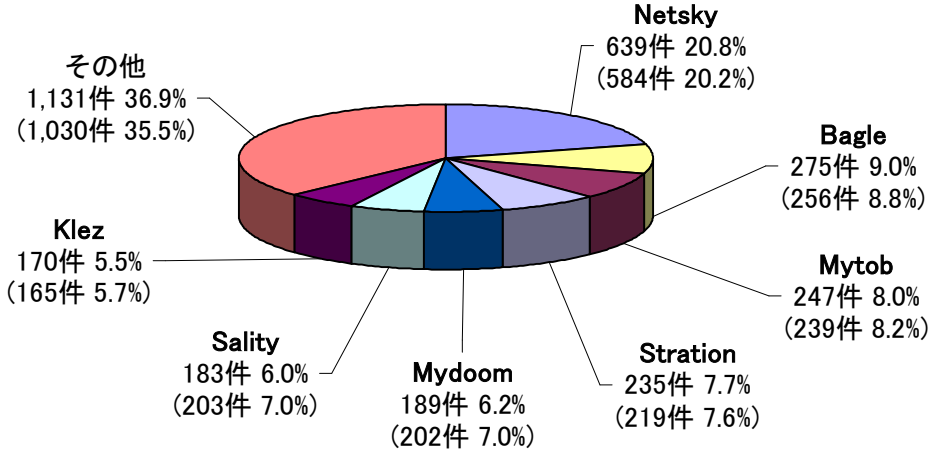


図:3-2

4. 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

		2月	3月	4月	5月	6月	7月
届出(a) 計		23	13	15	19	41	10
	被害あり(b)	14	9	12	13	36	8
	被害なし(c)	9	4	3	6	5	2
相談(d) 計		50	43	31	37	27	25
	被害あり(e)	28	20	20	21	11	11
	被害なし(f)	22	23	11	16	16	14
合計(a+d)		73	56	46	56	68	35
	被害あり(b+e)	42	29	32	34	47	19
	被害なし(c+f)	31	27	14	22	21	16

(1) 不正アクセス届出状況

7 月の届出件数は 10 件であり、そのうち**被害のあった件数は 8 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 25 件（うち 1 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 11 件でした。

(3) 被害状況

被害届出の内訳は、**侵入 3 件、その他（被害あり）5 件**でした。

侵入届出の被害内容は、外部サイトを攻撃するための踏み台になっていたものが 2 件、フィッシング(*1)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、パスワードクラッキング(*2)攻撃によるものが 2 件などでした。

（4） 被害事例

［侵入］

（i） SSH(*3)で使用するポート(*4)への攻撃で侵入され、ボット(*5)を設置された

事例	・朝出社したら、社内ネットワークが異常。調査したところ、あるサーバが大量の不審なパケットを送信していたことが判明。 ・SSH で使うポートへパスワードクラッキング(*2)攻撃を受け侵入されていた。ボットが埋め込まれ、外部と通信をしていた。さらにウェブサイトのコンテンツも改ざんされていた。 ・業務上の都合で一時的に ftp サービスを外部に公開していたが、**ftp 用のポートのみ開いたつもりが、全てのポートが開放されていたのが原因**と思われた。
解説・対策	**非定常作業だったため、チェックが行き届かなかった**ようです。このように、わずかな油断でも攻撃者は見逃しません。たとえ一時的でも外部にサービスを公開する際は、**チェックリストなどを利用して設定ミスが生じないよう、細心の注意を払いましょう**。 （参考） IPA － 情報セキュリティ白書 2007 年版 http://www.ipa.go.jp/security/vuln/20070309_ISwhitepaper.html

［その他（被害あり）］

（ii） SNS(*6)のアカウントが誰かに乗っ取られた

事例	・SNS のサービスを利用している。ある日突然、パソコンからのログインができなくなった。 ・ケータイからはログインできたが、利用者情報が、身に覚えの無いパスワードとメールアドレスに勝手に変更されていた。
解説・対策	今までも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事例がありました。最近話題の SNS にも多くの人が集まるため、悪意のあるユーザに狙われてしまう傾向にあります。パスワードは推測されにくいものにするとともに、**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**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。 （参考） IPA － 今月の呼びかけ（2006 年 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！」 http://www.ipa.go.jp/security/txt/2006/07outline.html

5. 相談受付状況

7 月の相談総件数は**1,162 件**と、集計を始めてから最高の件数でした。そのうち**『ワンクリック不正請求』に関する相談**が**316 件**(6 月:285 件)で今までの最悪値に並び、**『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**16 件**(6 月:12 件)、**Winny に関連する相談**が**19 件**(6 月:11 件)などでした。

IPA で受け付けた全ての相談件数の推移

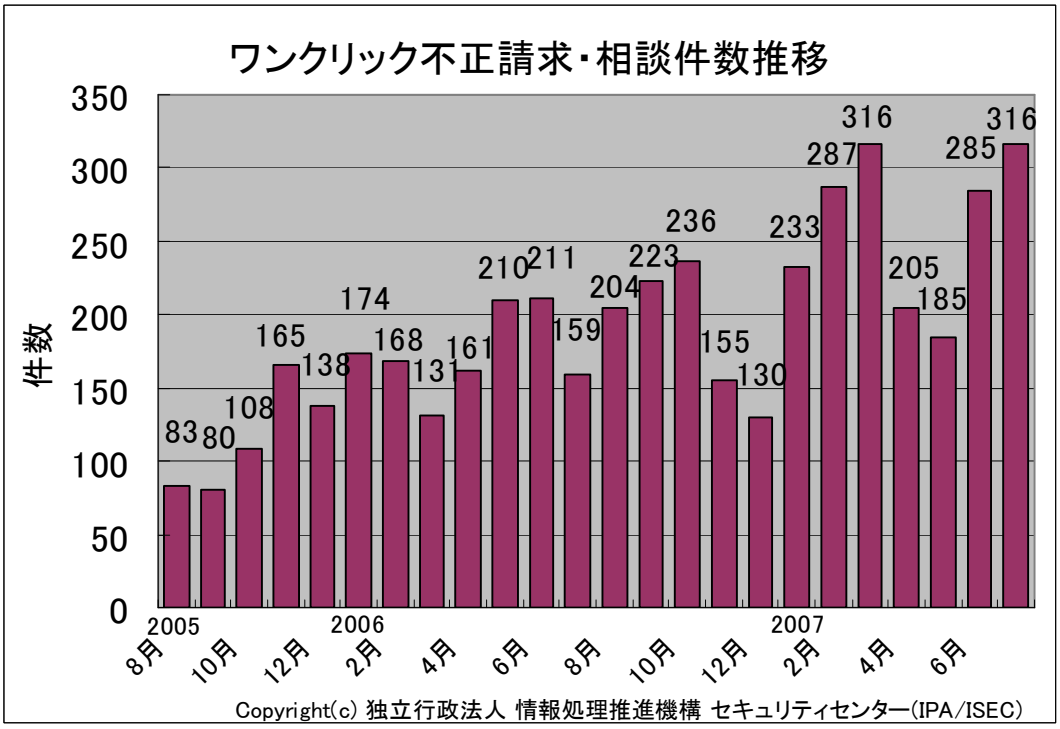
	2月	3月	4月	5月	6月	7月
合計	1019	1127	827	814	932	1162
自動応答システム	603	697	486	484	537	694
電話	336	376	279	254	339	402
電子メール	75	54	58	69	53	65
その他	5	0	4	7	3	1

※ 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)、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。

(参考) ワンクリック不正請求相談件数の推移

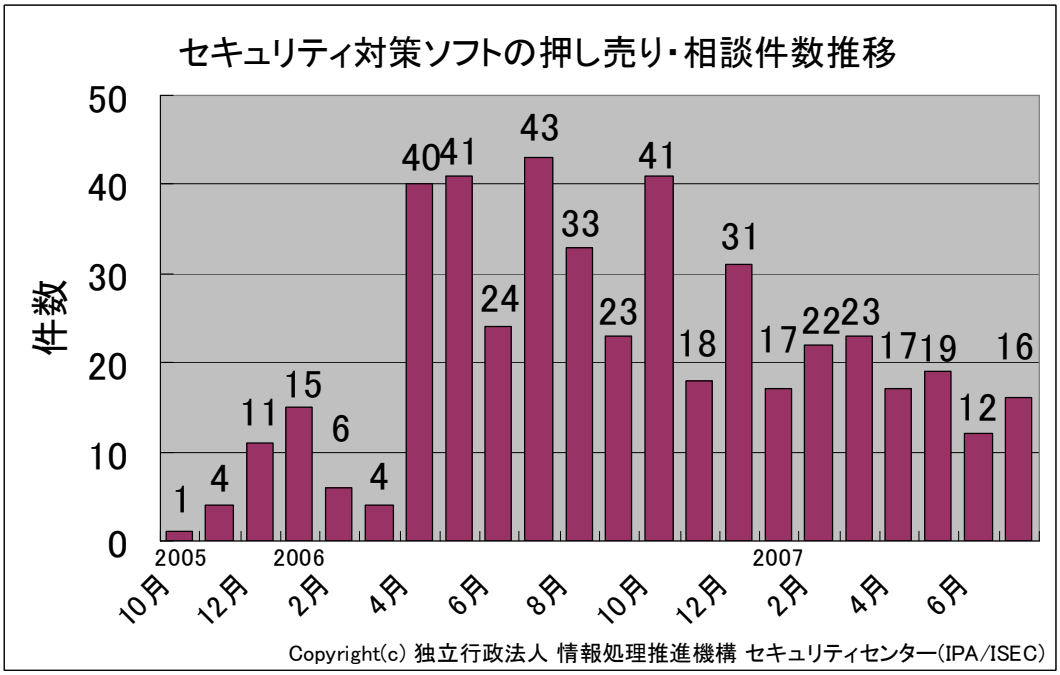


ワンクリック不正請求についての対策については下記をご参照ください。

・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）金融情報サイトを見ていたらウイルス警告が！

相談	いつも見ている有名な金融情報サイトをある日開いたら、ウイルス対策ソフトが警告を発した。どうしたらよいのか。
回答	ウイルス対策ソフトによって、ウイルス感染は防がれたはずです。が、念のためパソコン内を手動でウイルスチェックしてみましょう。このケースでは、**サイトが侵入、改ざんされて、サイトにアクセスしたパソコンにウイルスをダウンロードさせてしまうようになっていた**のです。しかし、**適切なウイルス対策を実施していれば問題はありません**。 （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

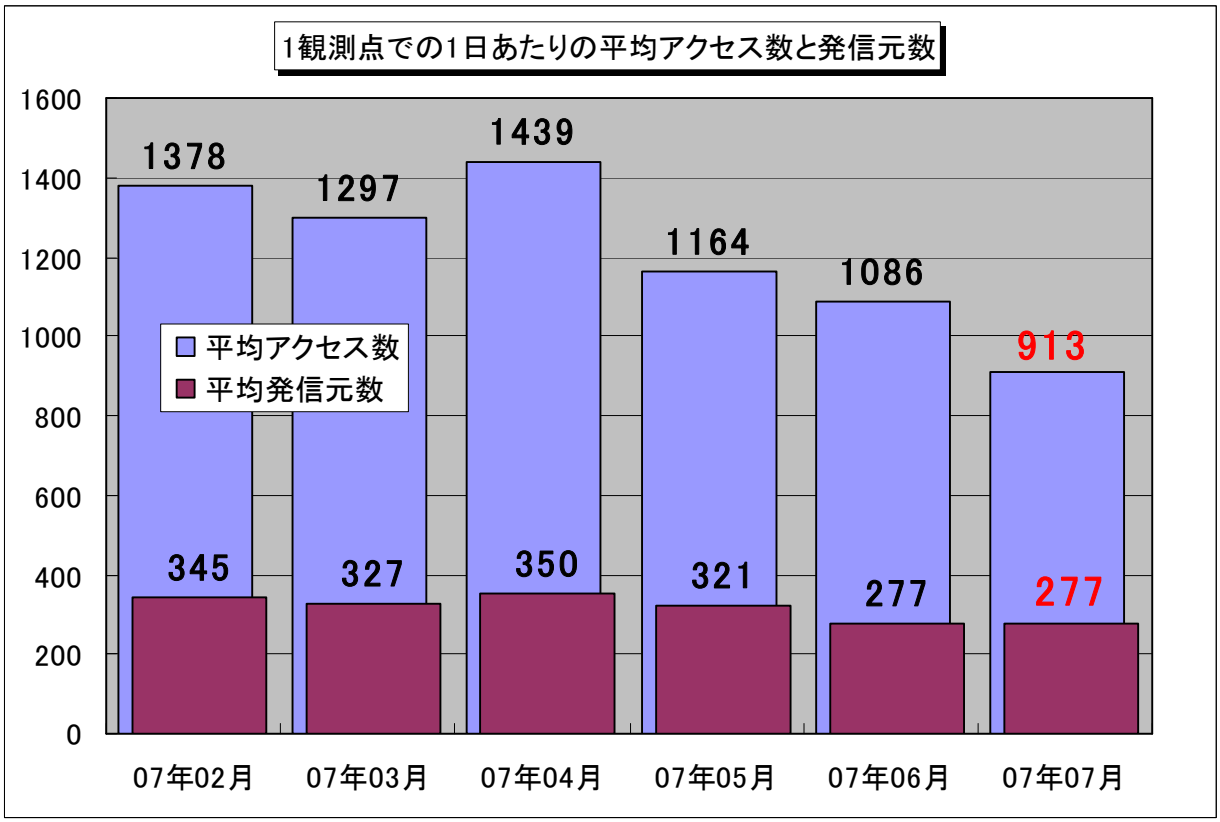
（ii）不正アクセスされているとの警告が出る

相談	ウイルス対策ソフトが、「不正アクセスされています」と警告を出す。処理方法が分からない。インターネットにつながらない。無線 LAN を使っているが、それが原因か。
回答	**無線 LAN は、セキュリティ設定をおろそかにすると簡単に侵入を許してしまいます**ので、注意が必要です。**無線 LAN アクセスポイントと、パソコン側の無線 LAN アダプタの設定を確認**しましょう。**工場出荷時の設定をそのまま使うことなく、自身で変更**しましょう。**特に、暗号化は必須**です。また、アクセスポイントの識別子（SSID）を外部に発信しない（ステルス設定などと呼ばれる）ことで、脅威に晒される機会を減らすことができます。 （ご参考） IPA - 無線 LAN のセキュリティに関する注意 http://www.ipa.go.jp/security/ciadr/20030228wirelesslan.html

6. 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、2007 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 **282, 889 件**ありました。1 観測点で 1 日あたり **277** の発信元から **913 件**のアクセスがあったことになります。

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、277 人の見知らぬ人(発信元)から、発信元一人当たり 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。



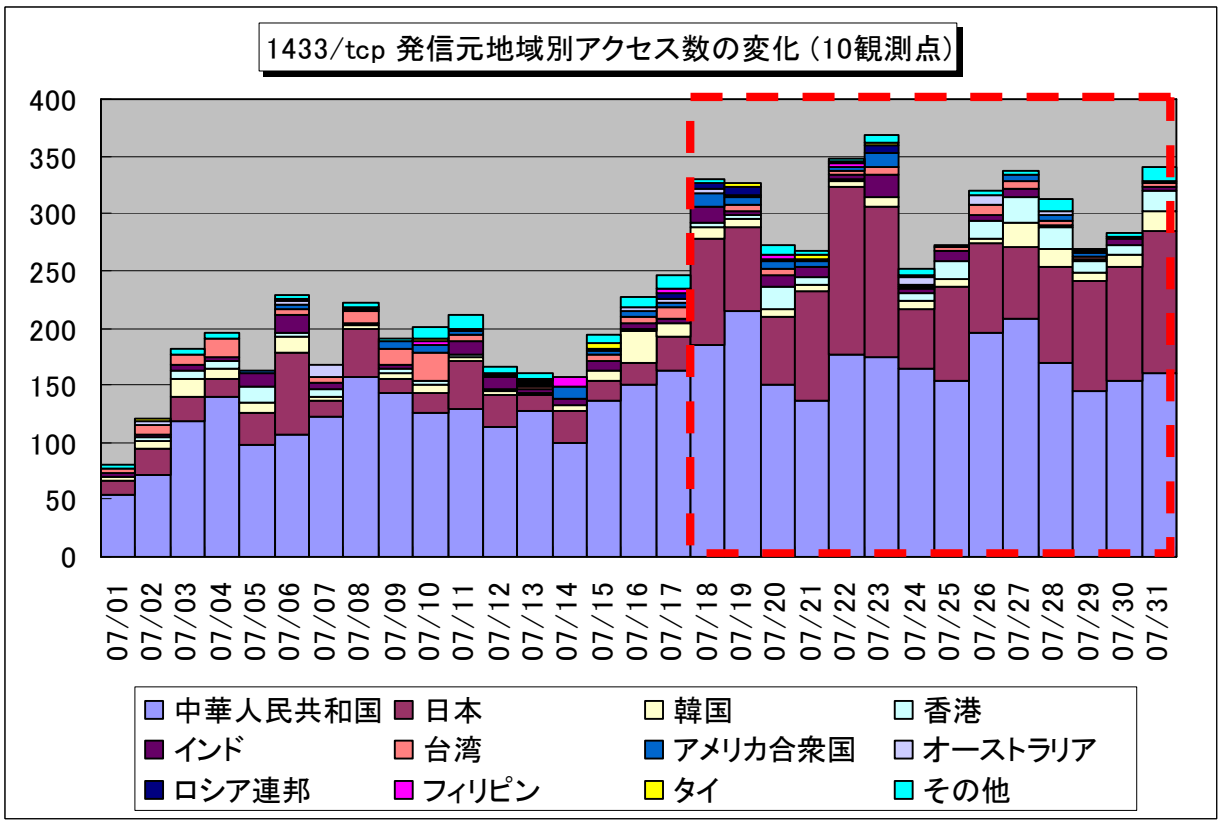
【図 6.1　1 観測点での 1 日あたりの期待しない(一方的な)アクセス数および発信元数】

2007 年 2 月～2007 年 7 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 6.1 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、緩やかですが減少傾向にあるようです。

2007 年 7 月のアクセス状況は、全体的に 6 月と同じで定常化していると言えます。その中において、Microsoft SQL Server のぜい弱性を狙った、1433/tcp のアクセスや、Symantec 社のセキュリティ対策ソフトのぜい弱性を狙った、2967/tcp のアクセスなど、アプリケーションソフトウェアのぜい弱性を狙ったアクセスが増加しました。

(1)　アプリケーションソフトウェアのぜい弱性を狙ったアクセス

2007 年 7 月の後半辺りから、1433/tcp ポートのアクセスが増加しました。これは、Microsoft SQL Server のぜい弱性を狙ったもので、主に中国や日本からのアクセスです。



【図 6.2　2007 年 7 月の 1433/tcp ポートへの発信元地域別アクセス数の変化】

日本からのアクセスの中には、Windows のぜい弱性を狙った、135/tcp、139/tcp、445/tcp を同時に狙ったアクセスも多いことから、ボット(*5)に感染したコンピュータからの感染活動（ボットの感染を広げようとしているアクセス）と思われます。

日本以外のアクセスを見てみると、中国、韓国、香港などからは、Symantec 社のセキュリティ対策ソフトのぜい弱性を狙った、2967/tcp や、MySQL（オープンソース SQL データベース）の稼動するサーバを狙った、3306/tcp を同時に狙ったアクセスもあります。（図 6.3、6.4 参照）

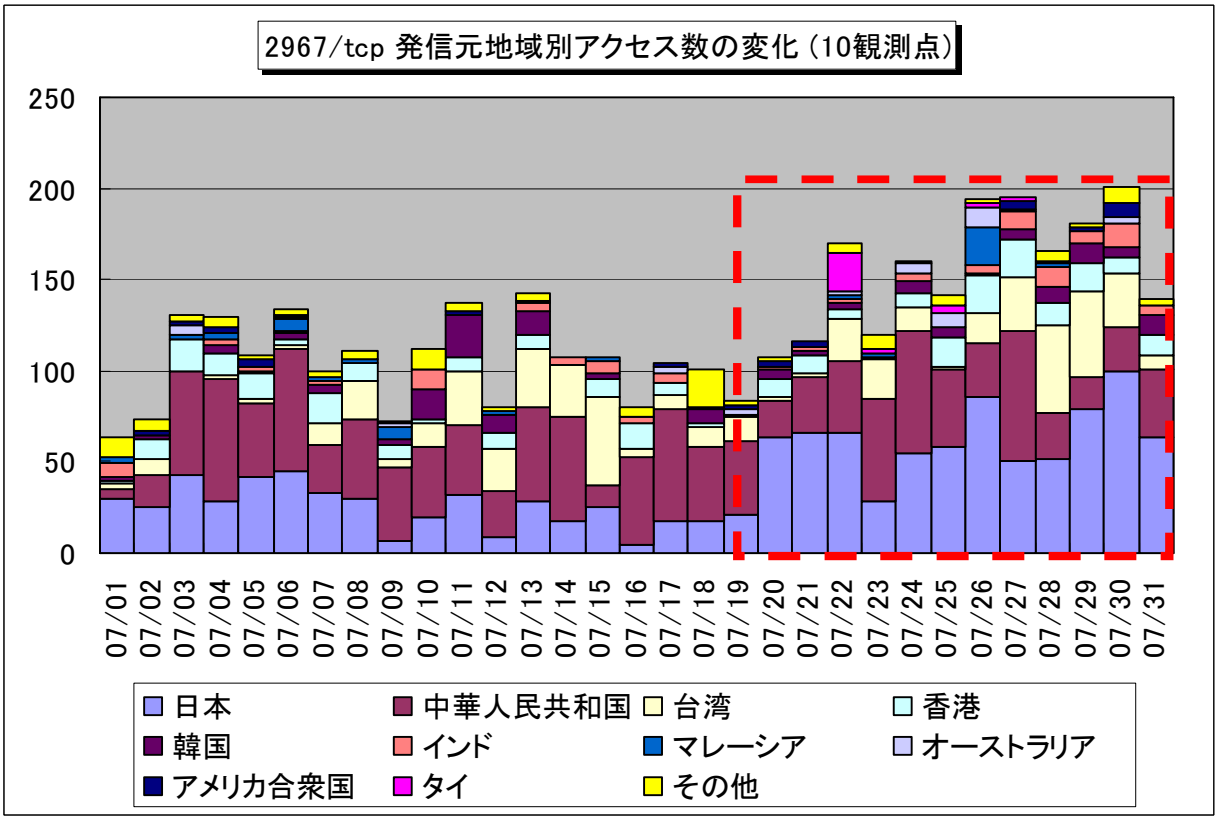
これらのアクセスは、日本で感染活動しているボットとは異なる種類のボットに感染したコンピュータからの感染活動と思われます。これにより、未だにボットに感染しているコンピュータが多いことが伺えます。

ボットは、感染していることに気づきにくいウイルスです。下記のサイトより、駆除ツールをダウンロードし、手順にしたがってボットの駆除を実行することをお勧めします。

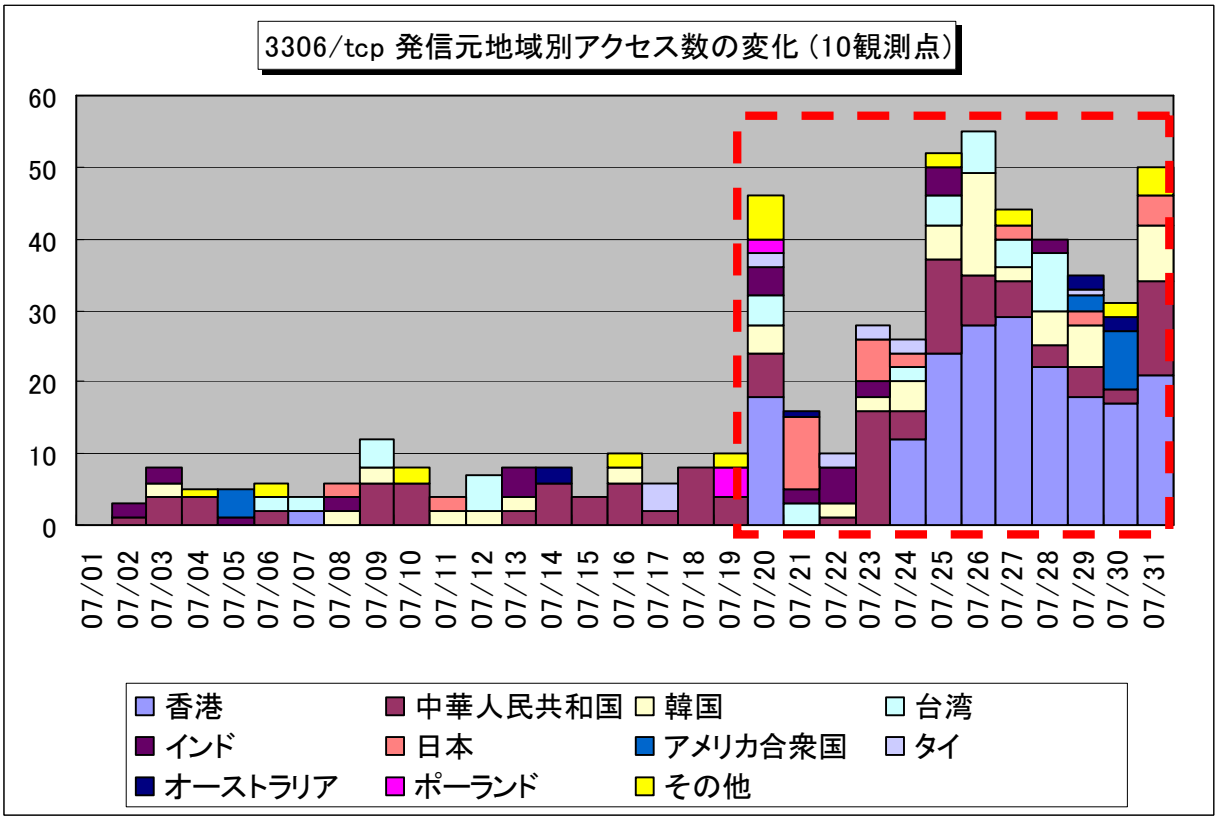
（参考情報）

■ ボットの駆除手順
https://www.ccc.go.jp/flow/index.html

■ 2007 年 6 月度　サイバークリーンセンター活動実績
https://www.ccc.go.jp/report/200706/0706monthly.html



【図 6.3　2007 年 7 月の 2967/tcp ポートへの発信元地域別アクセス数の変化】



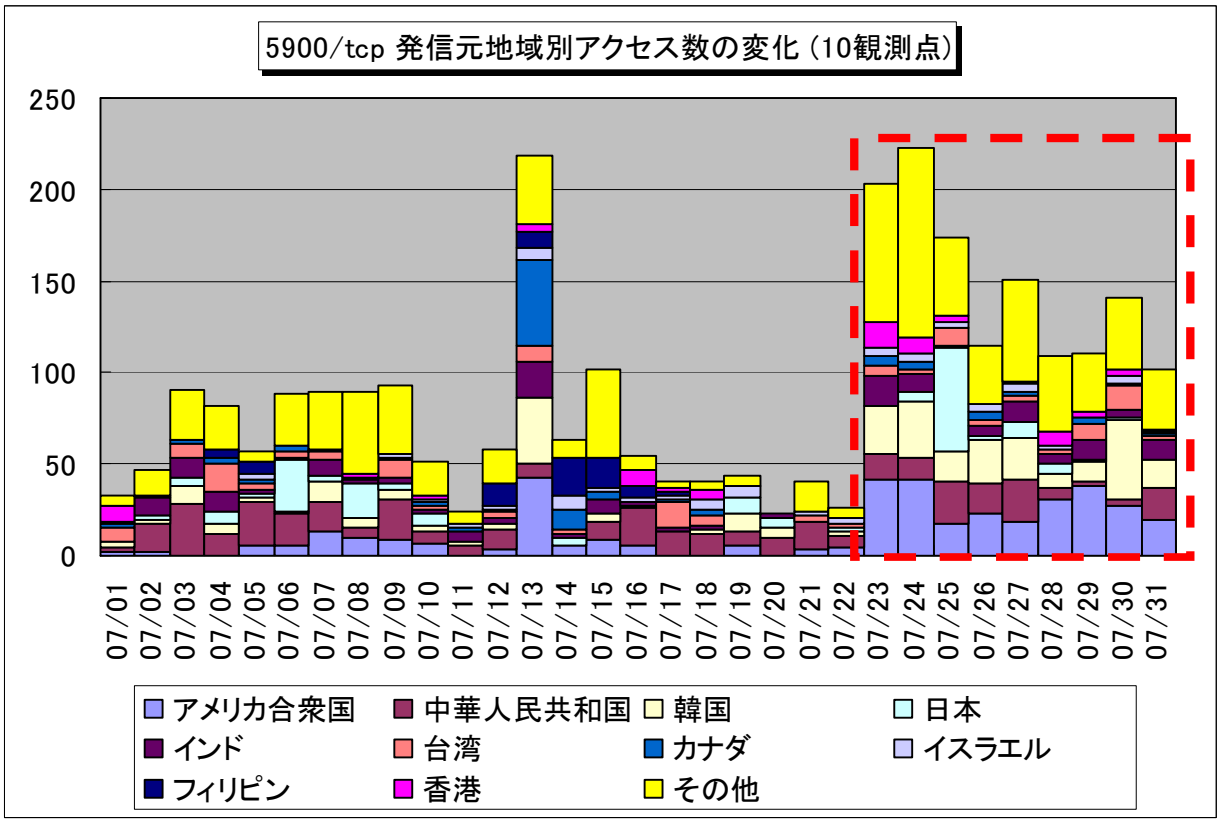
【図 6.4　2007 年 7 月の 3306/tcp ポートへの発信元地域別アクセス数の変化】

このほかに、リモートアクセスツール RealVNC のぜい弱性を狙っていると思われる 5900/tcp ポートへのアクセスについても、同じタイミングで増加しました。（図 6.5 参照）

このアクセスは、リモートから攻撃先のコンピュータへ侵入を試みるものであり、このようなツールを利用して、サーバを運用しているシステムの管理者は、運用方法の再点検やぜい弱性の解消を怠らないようにして下さい。

（参考情報）

■ JVNVU#117929 RealVNC Server に認証回避が可能な脆弱性
http://jvn.jp/cert/JVNVU%23117929/index.html



【図 6.5　2007 年 7 月の 5900/tcp ポートへの発信元地域別アクセス数の変化】

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/2007/documents/TALOT2-0708.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) **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。「釣り」を意味する「fishing」が語源だが、ハッカーの命名規則に則って"f"を"ph"に置き換えたという説、「洗練された」という意味の英語 "sophisticated"と"fish"とを組み合わせた造語という説、"password harvesting fishing"の短縮形という説、などがある。

(*2) **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。
＊:総当り攻撃
システムのパスワードを発見するために、パスワード文字列として可能な組み合わせをひとつずつ試す攻撃。「ブルートフォース」には、「力ずく」という意味が込められている。
＊: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。

(*3) **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。通信上のデータはすべて暗号化されるため、Telnet のようにデータが平文で通信されるプロトコルに比べて、安全性が高い。SSH の利用に際しては、いくつかの認証方式を選択することが可能だが、パスワード認証は総当り攻撃などにより認証を突破されてしまう可能性があるため、公開鍵認証を用いることが推奨される。

(*4) **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。

(*5) **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。

(*6) **SNS** (Social Networking Service/ Site)
インターネット上に構築された、人と人とのつながりを円滑にするようなサービスのこと。一般的に、会員制でコミュニティ型である。

■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