

コンピュータウイルス・不正アクセスの届出状況 [2008 年 10 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 10 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

「偽の警告を見分けよう！」
あなたのセキュリティ対策ソフトは本物ですか？

「セキュリティ対策ソフトの押し売り」に関する IPA への相談件数が、9 月に 50 件と急増し、10 月も 31 件ありました。「セキュリティ対策ソフトの押し売り」とは、突然画面に「Warning!」や「ウイルスが発見されました」などの偽の警告メッセージを表示させ、セキュリティ対策ソフトを購入させようとする行為です。

偽の警告メッセージは、パソコンに埋め込まれた不正なプログラム(広い意味でウイルスとみなす)によるものです。一旦このようなウイルスを埋め込まれると、パソコンの動作が不安定になる場合があり、最悪の場合、初期化を余儀なくされるなど、被害内容が深刻化しています。

以下の解説を参考にし、自分のパソコンに当てはまる例がないか確認しましょう。

(1)ウイルス感染の仕組み

「セキュリティ対策ソフトの押し売り」に関する IPA への相談は以前からありましたが、ウイルス感染の仕組みが以前とは異なってきています。以前はユーザがバナー広告(ホームページ上にある画像広告)に表示された偽の警告メッセージをクリックして、ウイルス感染してしまう事例が多くありました。

しかし、最近はユーザが、迷惑メールに添付されてきたファイルを不用意に開くことで、このウイルスに感染する事例が多く見受けられます。実際に IPA に届出のあった、ウイルスが添付されていたメールの内容を図 1-1 に示します。

IPA に届出のあったウイルスの集計結果からも、そのようなウイルスが多く出回っていることが裏付けられます(図 1-2 参照)。

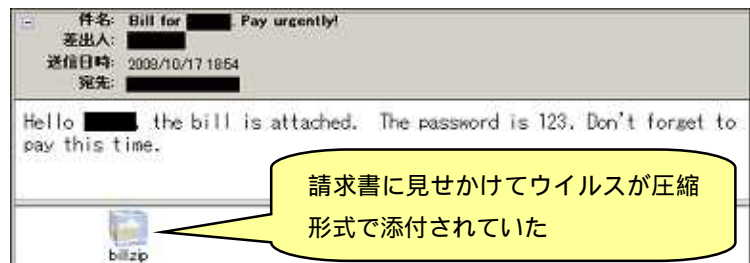


図 1-1：ウイルスが添付されたメール本文の例

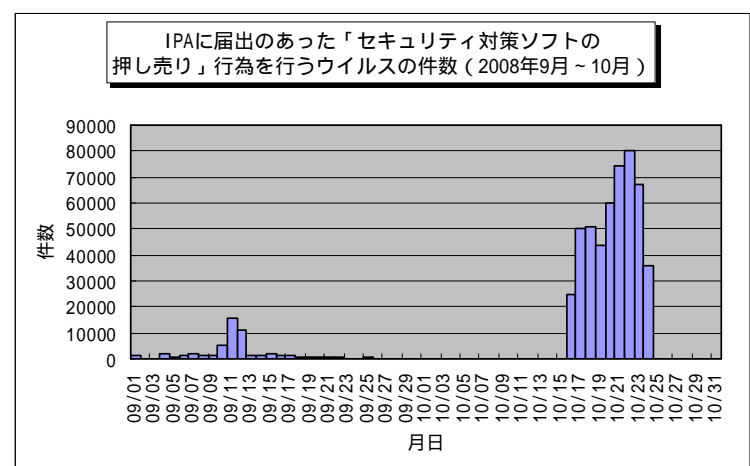


図 1-2：IPA に届出のあった「セキュリティ対策ソフトの押し売り」行為を行うウイルスの件数

「セキュリティ対策ソフトの押し売り」行為を行うウイルスは、信頼できるセキュリティ対策ソフトを常に最新の状態で使用していれば、メール受信時に検知できるため、ほとんど防ぐことができます。よって、このウイルスへの基本的な対策としては、第一に信頼できるセキュリティ対策ソフトを使用し、そのパターンファイルを常に最新の状態にしておくことが重要となります。しかし、検知をすり抜けてしまうウイルスもあるため、油断は禁物です。ウイルスの特徴を知るなど、日頃からの注意が必要です。

(2) 「セキュリティ対策ソフトの押し売り」行為を行うウイルスの特徴

(a)主な症状

お使いのパソコンに「セキュリティ対策ソフトの押し売り」行為を行うウイルスが感染してしまった場合、パソコンに以下のような症状が出るため、これらを基にウイルスに感染しているか判断することができます。

- (i)タスクバーに見覚えのないアイコンができていて、そこから「ウイルスに感染しています」などといった警告メッセージが表示される。

例



- (ii)突然、見覚えのないウイルス対策ソフトがウイルスチェックを始める。

例



その他の「セキュリティ対策ソフトの押し売り」行為を行うソフトの起動画面については、以下を参照ください。

「セキュリティ対策ソフトの押し売り」行為を行うソフトの起動画面例

http://www.ipa.go.jp/security/txt/2008/documents/infection_images.html

- (iii)デスクトップの壁紙が勝手に変更されている。元に戻せない場合もある。

例



(iv)その他

- ・デスクトップ上に見覚えのないアイコンができています。
- ・ウェブブラウザの起動時に最初に表示される「スタートページ」が変更されている。 など

(b) 「セキュリティ対策ソフトの押し売り」行為を行うソフトの名称

IPA に寄せられた 「セキュリティ対策ソフトの押し売り」に関する相談事例の中で、IPA が認識しているソフトの名称を以下の表 1-1 に記載しました。ただし、これらは「現状の主なもの」であり、自身のパソコンに入っている怪しいソフトと同じ名称がこの表に記載されていなくとも、それで安全であるという証明にはなりませんので、注意してください。

表 1-1：「セキュリティ対策ソフトの押し売り」行為を行う主なソフトの名称

AdvancedPrivacyGuard	Alphawipe	AntiSpyware	AntiSpywareExpert	AntiVirus2008
AntiVirus XP 2008	Doraibuhogo	DriveCleaner	HadodoraiBugado	NetTurboPro
SpyDajaba	Spyware Remover	SupaShuri	VirusRemover2008	VirusVanguard
WinAntiSpyware	WinAntiVirus	WinAntivirusPro2006	WinAntivirusPro2007	WinFixer
WinXProtector 2.1	XPAntivirus	XPSecurityCenter		

(c) 「セキュリティ対策ソフトの押し売り」行為の事例

参考として、ウイルス感染から「セキュリティ対策ソフト」を購入させるまでの流れの一例を、以下に紹介します。

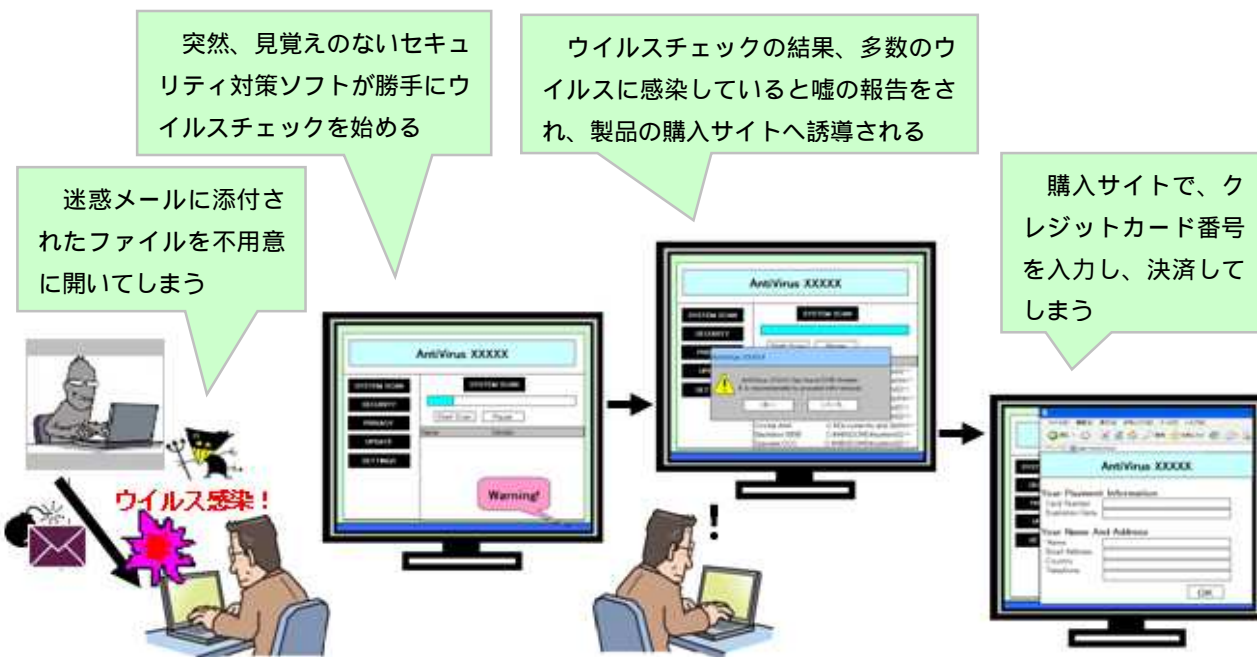


図 1-3：最近の「セキュリティ対策ソフトの押し売り」行為の一連の流れの例

(d) ウイルス感染以外の注意

今回の呼びかけは、「セキュリティ対策ソフトの押し売り」行為を行うウイルスに関する注意喚起ですが、ウイルス感染とともにさらに 1 点注意すべきことがあります。それは、「セキュリティ対策ソフトの押し売り」行為を行うウイルスをばら撒くような悪意のある者の最終的な目的は、ほとんどの場合「信頼できないセキュリティ対策ソフト」を購入させて金銭を得ることであるという点です。

信頼のおけるセキュリティ対策ソフトのベンダーの場合、上記の(c)の事例のように、急に警告メッセージを出したり、突然勝手にウイルスチェックを行うことは通常あり得ません。突然、警告が表示されても、それを鵜呑みにして慌ててお金を支払うようなことはせず、周囲の詳しい人や国民生活センターなどの相談窓口にご相談する、などといった対応が重要です。

IPA に寄せられた相談の中には、クレジットカード番号を入力し決済してしまった事例や、本物のセキュリティ対策ソフトと思い込んで、そのまま使い続けていた事例もありました。ウイルス感染の対策とともに十分な注意が必要です。

(3)ウイルス感染時のパソコンの復旧方法

ウイルスに感染してしまった後に、信頼できるセキュリティ対策ソフトでウイルスを駆除したとしても、ウイルスによって変更されてしまったシステムの設定などは元に戻りません。

この場合は、以下の「システムの復元」を実施してください。それでも症状が改善されない場合、もしくは、「システムの復元」が失敗した場合は、パソコンの初期化を実施してください。

(a)システム復元による復旧

Windows XP や Vista には、パソコンの動作が不安定になるなど、使用するのに支障がある場合に、以前の状態に戻すことができる「システムの復元」という機能があります。これは Windows が、任意の日を自動的に選んで保存しているシステムの情報を基に、パソコンの状態を戻すというものです。

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」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、アプリケーションソフトウェアのインストール、アップデートなどをした場合は、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。

「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>

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

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

(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初期化という作業を実施します。

実際の作業方法は、取扱説明書に記載されている「購入時の状態に戻す」など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(USB メモリや CD-R、外付け HDD など)にバックアップしてから作業を行ってください。

(4)被害を未然に防ぐための対策

今後、このような被害に遭わないために、以下のことを心掛けてください。

(a)迷惑メールへの対処

迷惑メールに添付されてくるファイルを不用意に開かないことが、ウイルス感染を予防する上で最も重要です。

また、迷惑メールを認識して遮断、削除できる迷惑メールフィルタリング機能を利用することも有効です。迷惑メールフィルタリング機能は、メールソフトに備わっている場合や、プロバイダ^(*)のサービスで提供している場合があります。

それでも遮断されない迷惑メールは、開かずに捨てることを心掛けてください。

(b)脆弱性(ぜいじゃくせい)^(*)の解消

脆弱性を突かれてウイルスに感染しないように、お使いの OS、アプリケーションを常に最新の状態に更新して、脆弱性を可能な限り解消してください。

(c)信頼できるセキュリティ対策ソフトの導入

お使いのセキュリティ対策ソフトが信頼できるものかどうか判断がつかない場合は、「(2)『セキュリティ対策ソフトの押し売り』行為を行うウイルスの特徴」を参考にする、詳しい人に聞くなどして、必ず確認をしてください。

どのセキュリティ対策ソフトを購入したらいいか判断できない場合は、パソコンショップなどの販売員に確認して、パッケージ版を購入することをお勧めします。

(*1)プロバイダ

ISP(インターネットサービスプロバイダ)のこと。インターネットに接続するためのサービスなどを提供する事業者。

(*2)脆弱性(Vulnerability)

一般にソフトウェアなどのセキュリティ上の弱点を指します。セキュリティホール(Security Hole)とも呼ばれます。

(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>

「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.mspix>

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「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サイトで、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、9 頁の「4.相談受付状況」を参照)

- ・ ネットでウイルス対策ソフトを購入した後、パソコンの調子が悪い
- ・ ファイル共有ソフトでダウンロードしたファイルを開いたらパソコンの調子が悪い

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。

- ・ 135/tcp、139/tcp 及び 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 27 万個と、9 月の約 22 万個から 23.7%の増加となりました。
また、10 月の届出件数(²)は、1,839 件となり、9 月の 1,875 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を。

- ・ 10 月は、寄せられたウイルス検出数約 27 万個を集約した結果、1,839 件の届出件数となっています。

検出数の 1 位は、W32/Netsky で約 19 万個、2 位は W32/Autorun で約 6 万個、3 位は W32/Mytob で約 4 千個でした。

ウイルス検出数 約27万個 (約22万個) 前月比 +23.7%

(注：括弧内は前月の数値)

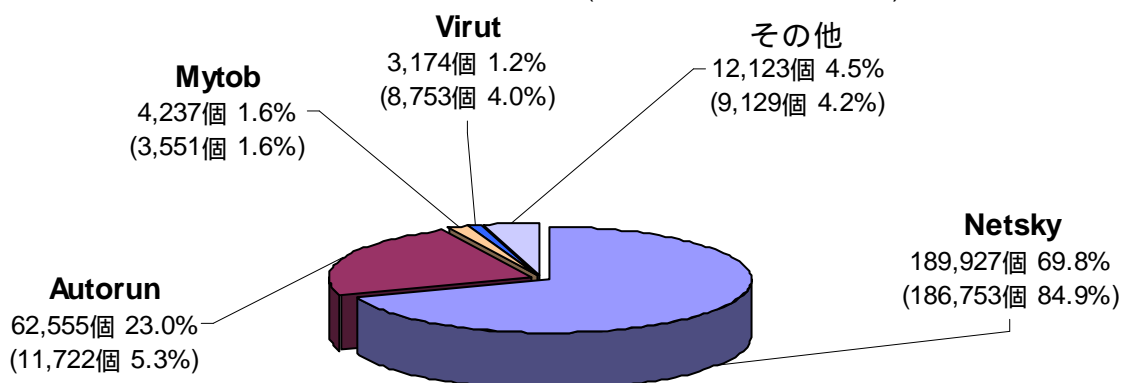


図 2-1

ウイルス届出件数 1,839件 (1,875件) 前月比 -1.9%

(注：括弧内は前月の数値)

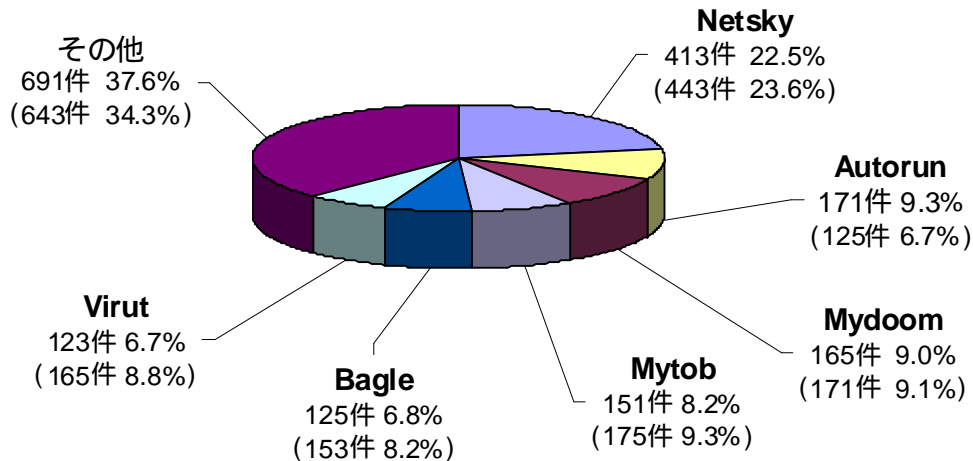


図 2-2

(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 月以降に増加しています(図 2-3 参照)。10 月には、「1.今月の呼びかけ」でも紹介したように、「セキュリティ対策ソフトの押し売り」行為を行う FAKEAV が急増しました。これは、バナー広告により感染に導く従来の手法から、メールの添付ファイルを用いて感染に導く手法に変化していることが原因といえます。FAKEAV に感染すると、ほとんどのケースで復旧には初期化が必要になるなど、深刻な被害が発生していることから、今回、不正プログラムが増加している状況を示し、注意を促すこととしました。

これらの不正プログラムは、メールの添付ファイルとして多数出回っており、図 2-3 からわかる通り、特定の期間に急増するなど、不自然な傾向が見取れます。このことは、ボット等によりメール配信が行われている可能性があることを示しており、ボットに感染しているか確認するとともに、不正プログラムを取り込まないように、添付ファイルには十分注意してください。

(ご参考)

「感染防止のための知識」(サイバークリーンセンター)

<https://www.ccc.go.jp/knowledge/index.html>

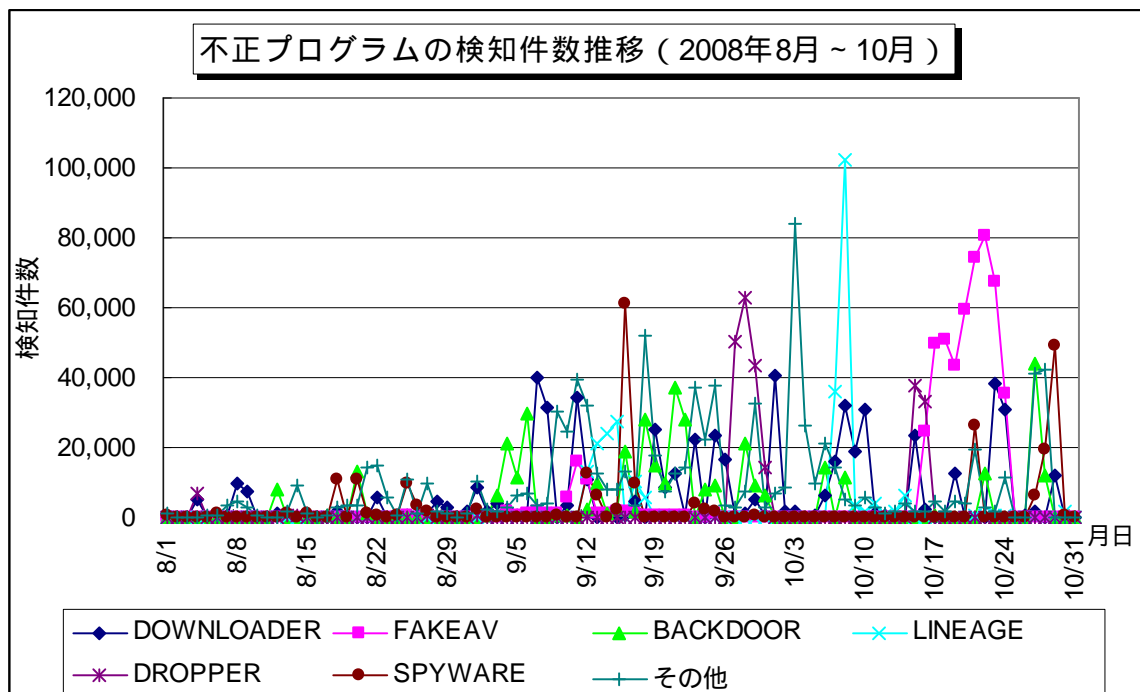


図 2-3

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

		5月	6月	7月	8月	9月	10月
届出^(a) 計		4	13	19	15	14	17
	被害あり ^(b)	4	11	18	10	12	12
	被害なし ^(c)	0	2	1	5	2	5
相談^(d) 計		37	36	49	25	38	58
	被害あり ^(e)	18	15	26	13	20	22
	被害なし ^(f)	19	21	23	12	18	36
合計^(a+d)		41	49	68	40	52	75
	被害あり ^(b+e)	22	26	44	23	32	34
	被害なし ^(c+f)	19	23	24	17	20	41

(1)不正アクセス届出状況

10月の届出件数は17件であり、そのうち何らかの被害のあったものは12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58件(うち7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22件でした。

(3)被害状況

被害届出の内訳は、**侵入4件、アドレス詐称が1件、その他(被害あり)7件**でした。

侵入届出の被害は、他サイト攻撃の踏み台として悪用されたものが3件、SQL インジェクション攻撃を受けて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1件でした。侵入の原因は、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2件、脆弱性を突かれたことによるものが2件でした。

その他(被害あり)の被害として、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が5件(ネットオークション2件、オンラインゲーム1件、ウェブメール1件、その他1件)、などがありました。

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。

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(総当たり攻撃)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	<ul style="list-style-type: none">・ウェブサイト閲覧者(顧客)から「ウェブサイトの商品紹介ページにアクセスすると、商品には関係がないと思われる文字列が表示され、同時に、身に覚えのないアダルトサイトに飛ばされてしまう」といった報告があった。・サーバのログを調査したところ、SQL インジェクション攻撃を受け侵入を許し、データベース内のデータ(商品マスタ情報)が改ざんされていたことが判明。・改ざん内容は、アダルトサイトへ飛ばすための JavaScript の記述を埋め込むというもの。・サーバ上で動いていたウェブアプリケーションに、脆弱性があったことが原因と思われる。
解説・対策	<p>問題のあったサイトは、ウェブサイトアクセスして来た顧客のリクエストに応じて、データベースで管理している商品情報を、随時ピックアップして見せる、という仕組みになっていました。</p> <p>ショッピングサイトでは個人情報や金融情報を扱うことが多いため、特に問題が大きくなりがちです。ウェブサイト上で商品を販売するようなサイトがこのような改ざん被害を受けると、次のような影響が出る可能性があります。</p> <ul style="list-style-type: none">・サイトにアクセスして来た顧客のパソコンが、ウイルスに感染する。・復旧のためサイトを一時的に閉鎖するなど、ビジネス上の損失が出る。・ショッピングサイトとしての信用に傷が付く。 <p>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)</p> <p>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/</p> <p>IPA-安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/websecurity.html</p>

[なりすまし]

(ii) ネットオークションサイトで、誰かが自分になりすまして勝手に出品

事例	<ul style="list-style-type: none">・オークションサイトから「メインメールアドレスが変更されました」との通知メールが届いた。・不審に思い、当該サイトにログインして確認したところ、身に覚えのないアドレスが登録されていた。・ログイン履歴を確認したところ、オークションページを閲覧した履歴があったため、自分のアカウントの出品/入札状況を確認。その結果、身に覚えのない商品が勝手に出品されていたことが判明。・すぐに出品を取り消し、当該サイトのログインパスワードも変更した。しかし、出品手数料が数千円も請求されている。
解説・対策	<p>何者かが、パスワードを推測してログインに成功したものと思われます。対策として、複雑なパスワードを設定することが重要ですが、他のサイトのサービスと全く同じパスワードを使用していると、それらが手掛かりとなり、芋づる式にパスワードが破られてしまうこともあるようですので、注意が必要です。</p> <p>オークションサイトやオンラインバンキングサイトでは、サイトに登録された情報が変更された場合に確認通知メールを送れるようになっていることが多いようです。普段から、携帯電話のメールアドレスを登録しておく、万が一の不正が行われた際の変更通知にも早く気付くため、有効な策の一つと言えます。</p> <p>不正に気付いたら、すぐにサイト運営元と、警察に連絡しましょう。</p> <p>(参考)</p> <p>警察庁 - インターネット安全・安心相談 http://www.cybersafety.go.jp/</p>

4. 相談受付状況

10月の相談総件数は1171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**305件**(9月:651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**31件**(9月:50件)、Winnyに関連する相談が**5件**(9月:4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**3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

		5月	6月	7月	8月	9月	10月
合計		1080	1211	1387	1616	2154	1171
	自動応答システム	649	693	817	994	1302	677
	電話	379	456	500	548	755	441
	電子メール	48	60	70	69	93	47
	その他	4	2	0	5	4	6

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対応件数

「電話」：IPAセキュリティセンター員による対応件数

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。

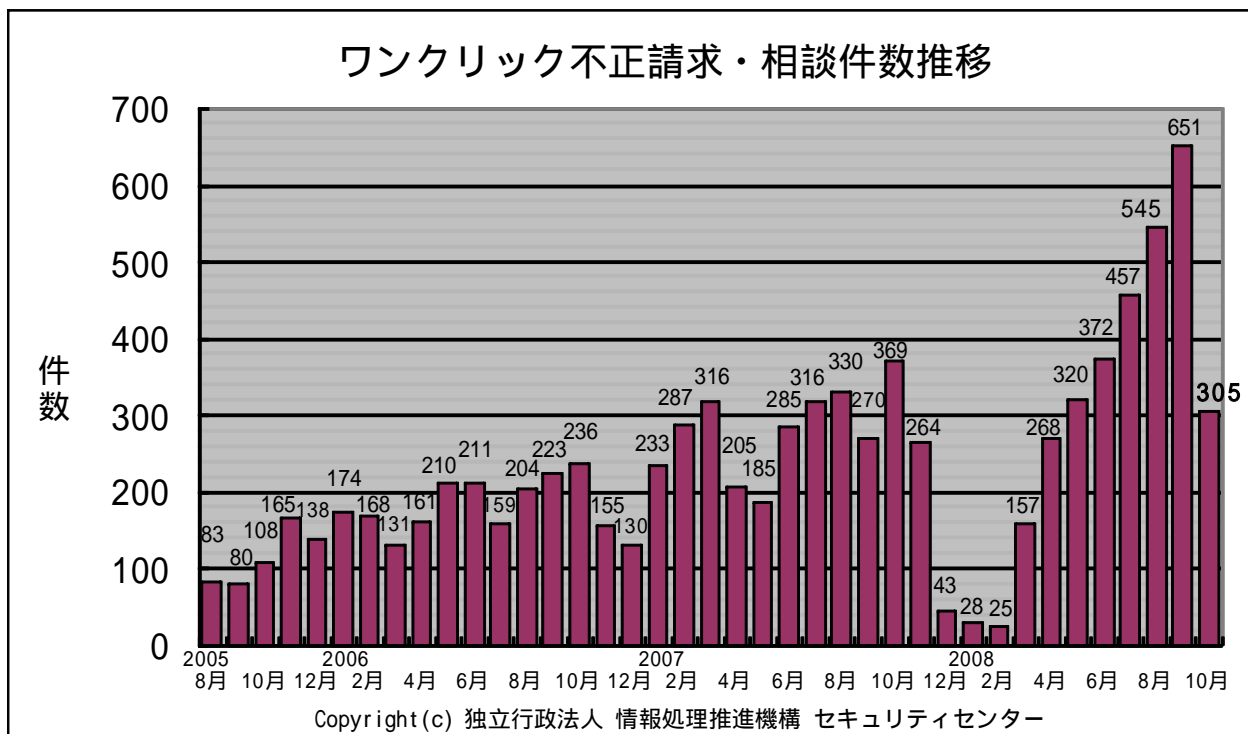


図 4-1 ワンクリック不正請求相談件数の推移

主な相談事例は以下の通りです。

(i) ネットでウイルス対策ソフトを購入した後、パソコンの調子が悪い

相談	ウイルス対策ソフトを新たに購入しようとして、ネットで検索。良さそうなものを見付けてダウンロード、インストールした。その際、クレジットカードで決済をおこなった。その後、パソコン起動時に【warning! spyware detected on your computer...】などと表示されたり、起動に時間が掛かるようになったり、時々パソコンが不安定になって使えなくなったりする。
回答	信頼できないウイルス対策ソフトを誤って購入してしまったものと思われます。ウイルス対策ソフトのような名前に見えても、不正なプログラムであることがありますので、注意が必要です(「1. 今月の呼びかけ」参照)。 どのセキュリティ対策ソフトを購入したら良いか判断できない場合は、安易にネットでダウンロード版を購入せず、パソコンショップなどの店頭で販売員に確認するなどしてパッケージ版を購入した方が良いでしょう。

(ii) ファイル共有ソフトでダウンロードしたファイルを開いたらパソコンの調子が悪い

相談	Cabos というファイル共有ソフトで音楽データを複数ダウンロードした。そのうちの一つをダブルクリックしたら、何やら英語のメッセージウィンドウが出て来た。そのウィンドウは、閉じようとしても閉じられない。さらに、壁紙が勝手に変更されていた。パソコンを再起動したら、Windows が起動し切らないうちに、再起動を繰り返してしまう。パソコンの操作が全くできなくなってしまった。
回答	このような状況になった場合、影響範囲が不明確なため、パソコンを初期化することをお勧めします。音楽データに見えたファイルが、実はウイルスであった可能性が高いです。特に、映画・音楽・書籍をコピーしたような、違法に流通しているデータと思わせるような名前のファイル内に、ウイルスが含まれている傾向がありますので、注意が必要です。 違法行為を止めるのはもちろんですが、ウイルス感染予防のためにも、出所の不明なファイルを開いたら何が起こるか分からないという根本的な危険性を、改めて認識し直すべきです。安易に興味本位でファイル共有ソフトを使うことは、厳として慎むべきです。 (ご参考) IPA - Winny による情報漏えいを防止するために http://www.ipa.go.jp/security/topics/20060310_winny.html

5. インターネット定点観測での10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10月の期待しない(一方的な)アクセスの総数は10観測点で128,667件、総発信元()は34,926箇所ありました。1観測点で見ると、1日あたり113の発信元から415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。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向的アクセスがあると考えられます。

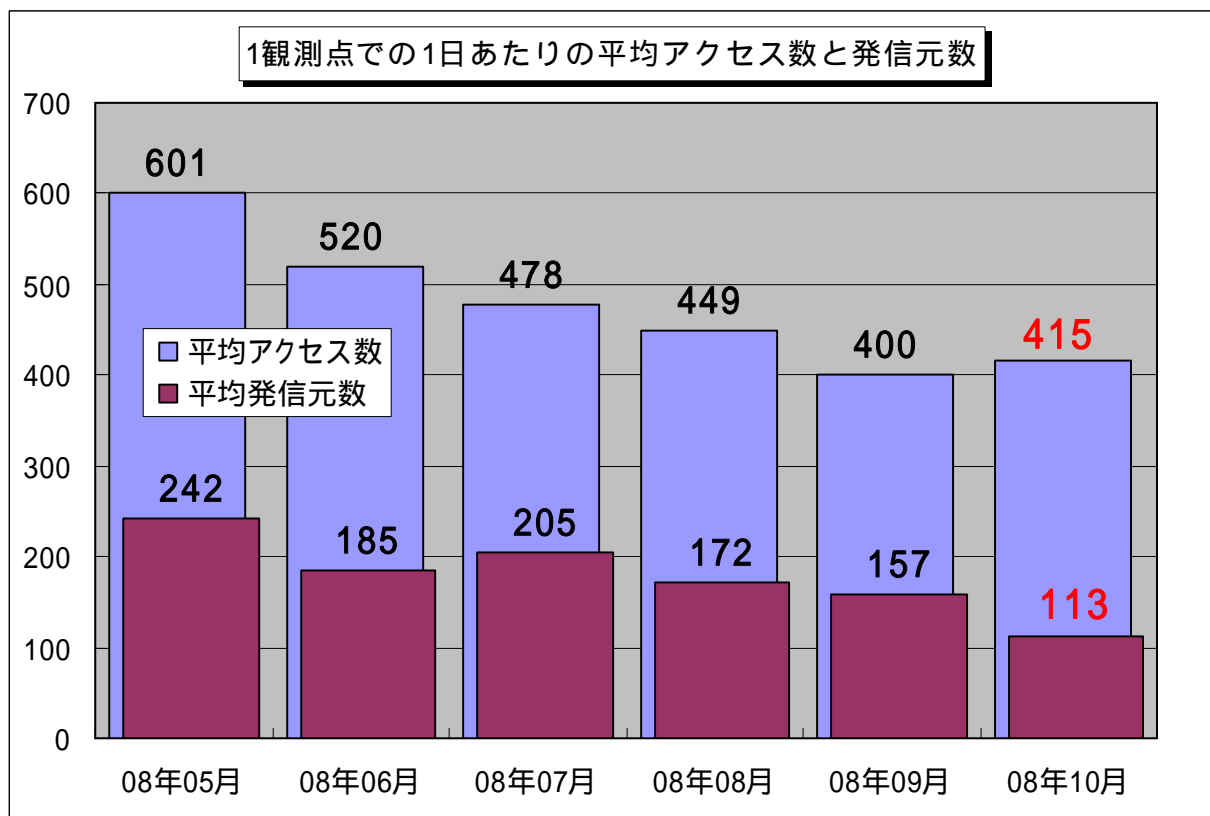


図5-1：1観測点での1日あたりの期待しない(一方的な)アクセス数および発信元数

2008年5月～2008年10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、10月の期待しない(一方的な)アクセスは9月と比べて若干増加しました。過去6ヶ月を通してみると、これまでの減少傾向が一段落した格好です。

(1) 135/tcp、139/tcp 及び 445/tcp へのアクセス

10月14日から22日にかけて全体的にアクセス数が増加しました。このうち135/tcp、139/tcp及び445/tcpへのアクセスに関しては、10月15日に発表されたマイクロソフトの脆弱性(ぜいじゃくせい)情報の中の、Windowsの脆弱性を狙った攻撃が含まれていた可能性があります。

図5-2に135/tcp、139/tcp及び445/tcpへのアクセス数の遷移を示します。

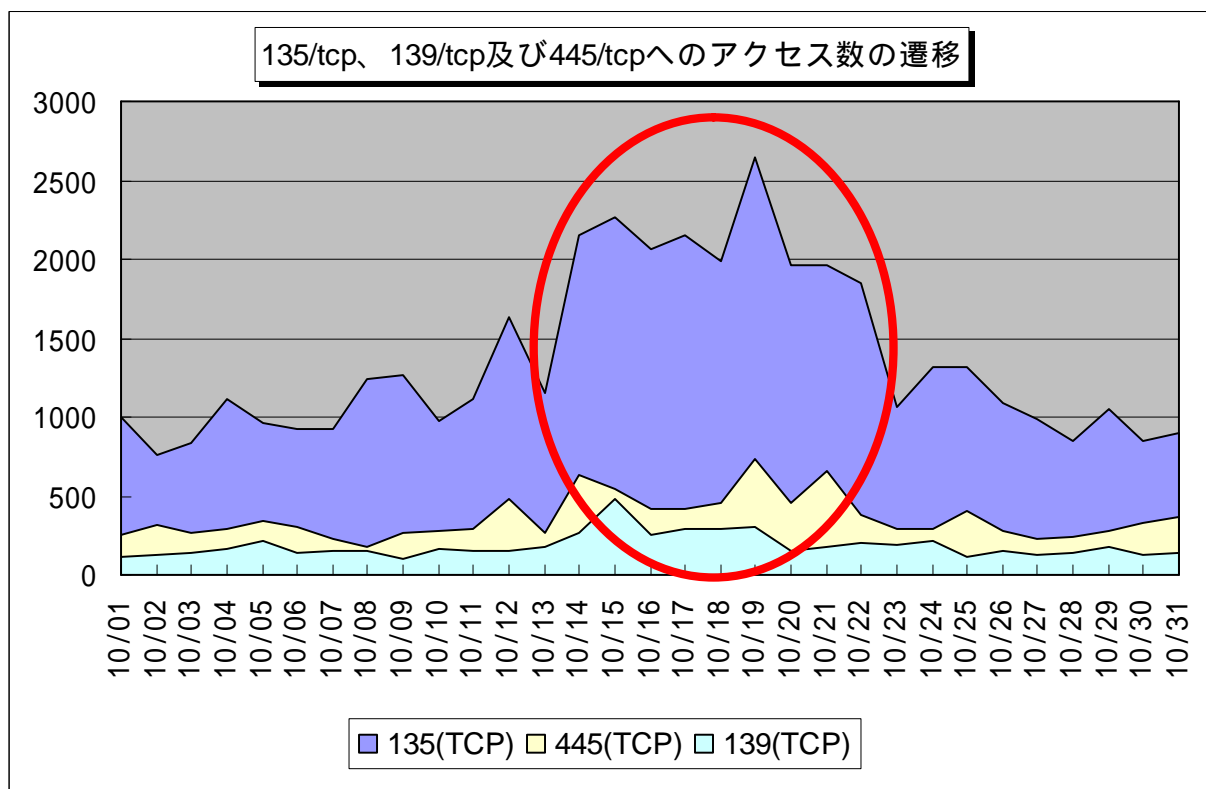


図5-2：135/tcp、139/tcp及び445/tcpへのアクセス数の遷移

OSやアプリケーションの脆弱性を解消し、常に最新の状態で使うことは、セキュリティ対策の基本です。

Windowsには、更新情報を通知させる設定(自動更新機能)があります。この機能を利用している方は、更新情報が通知されたら、すぐに更新作業を行うように心掛けてください。

この機能を利用していない方は、以下のマイクロソフトのホームページを参考にして、利用するようにしてください。

また、業務サーバなどのように停止が困難なサーバであっても、メンテナンスのための時間を確保するなどして、確実に脆弱性を修正するようにしてください。

<参考情報>

「自動更新機能で常に最新のWindows XPを使おう」(マイクロソフト社)

<http://www.microsoft.com/japan/windowsxp/security/au.mspx>

Windows Vistaの自動更新機能の解説(マイクロソフト社のWindows Vistaまるわかりガイドの情報)

<http://www.microsoft.com/japan/windows/using/windowsvista/guide/security/update.mspx>

また、更新情報の通知が行われないアプリケーションなどについても、専用サイトなどで脆弱性情報をこまめに確認し、更新作業が手遅れにならないように十分ご注意ください。

<参考情報>

「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>

「JVN iPedia 脆弱性対策情報データベース」
<http://jvndb.jvn.jp/>

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/TALOT2-0811.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@jpa.go.jp