INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
第 08-27-137 号
2008 年 12 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 11 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 11 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

「外部記憶メディアのセキュリティ対策を再確認しよう！」
― USB メモリ、便利のウラに落とし穴 ―

IPA に寄せられたウイルス届出のうち「USB メモリを経由して感染を広げるウイルス」の検出数が、9 月に 11,722 件、10 月に 62,555 件、11 月は 101,090 件と急増しています[図 1-1]。急増した原因の一つとして、**既存のウイルスに、USB メモリなど外部記憶メディアへの感染機能が新たに組込まれつつあること**が考えられます。ウイルスが外部記憶メディアに感染し、それによって他のパソコンへと感染していく手法や形態は、MS-DOS が主流であった当時に流行していたブートセクタ※感染型ウイルスとよく似ています。

USB メモリなどの外部記憶メディアは大容量化と低価格化が進み、利用機会が増えていますが、このようなメディアにおけるウイルス対策には、あまり意識が行き届いていないのが実情です。このため、ウイルスに感染した外部記憶メディアを安易にパソコンに接続してしまうことで、そのパソコンがウイルスに感染してしまうなど被害が拡大します。

以下の解説を参考にし、今一度 USB メモリなど外部記憶メディアのウイルス対策を見直しましょう。

※ブートセクタ：OS の立ち上げ時に必ず実行されるプログラムが格納されている、ハードディスクやフロッピーディスク上の領域のことです。この領域にウイルスが感染すると、パソコン起動時に必ず実行されるため、ウイルスにとっては都合の良い感染場所です。

(1)最近の届出・相談事例

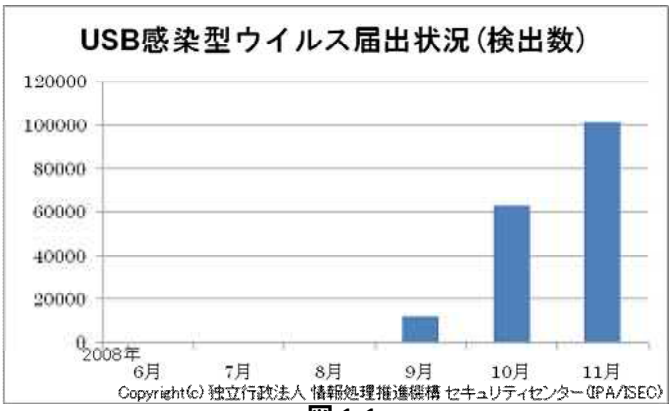

図 1-1

IPA に寄せられた届出・相談の中には、「USB メモリ内の、身に覚えのないファイルを興味本位でクリック。その後、SD メモリカードを接続したら、SD メモリカードにウイルスが感染した」、「データの受け渡しの為に、他人の USB メモリを自分のパソコンに接続したら、ウイルス感染した」という利用者の不注意の中でウイルス感染してしまったものがありました。また、「街のパソコン教室のパソコンに自分の USB メモリを接続してデータをコピーした。その USB メモリを職場で使っているパソコンに接続したら、ウイルスを検知した」など、USB メモリを公私混同で利用したために職場にウイルスを持ち込んでしまったという相談もありました。

(2)外部記憶メディアを経由して感染を広げるウイルスの概要

ウイルスが感染する外部記憶メディアとして USB メモリやメモリカード、USB 接続型外付けハードディスクなどがありますが、以降の説明では、「USB メモリ」を外部記憶メディアの代表例として、またこの USB メモリなどの外部記憶メディアに感染するウイルスを「USB メモリ感染型ウイルス」として説明します。

(a)感染の仕組み

Windows2000 以降には、パソコンに USB メモリが接続されると、その USB メモリの中に置かれたプログラムを自動的に実行する機能があります。USB メモリ感染型ウイルスは、この機能を悪用して感染活動を行います。

USB メモリ感染型ウイルスは USB メモリに感染する際、Windows エクスプローラからは見えない Autorun.inf というファイルを USB メモリ内に作成することで、ウイルス自身が自動実行される状態にします。

感染した USB メモリをパソコンに接続した時や、「マイコンピュータ」からディスクドライブのアイコンをダブルクリックした時に、USB メモリ内のウイルスが起動し、パソコンにウイルスが感染してしまいます[図 1-2(a)]。

また、ウイルス感染したパソコンに、別の USB メモリを接続すると、その USB メモリにウイルスが感染し、USB メモリ感染型ウイルスが拡散していきます[図 1-2(b)]。

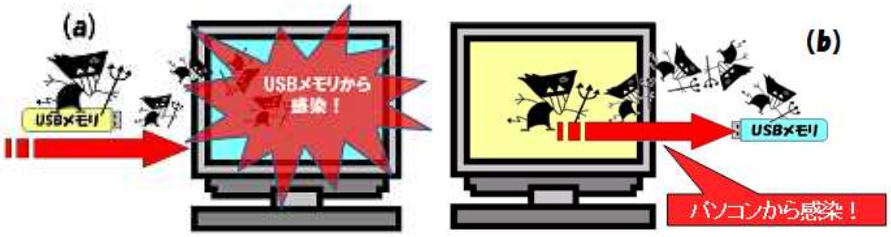

図 1-2 感染のイメージ図

(b)ウイルスの特徴

最近の USB メモリ型ウイルスは、その種類によって異なりますが、利用者による駆除や発見を困難にするために様々な偽装・妨害を行います。以下に、IPA に届けられた複数の USB メモリ感染型ウイルスの解析結果を基に、ウイルスの特徴を説明します。

(i)ウイルスの種類によっては、ウイルスファイル自身のアイコンや属性情報を偽装し、図 1-3 のようにデータファイルとして見える場合があります。

図 1-3 属性が偽装された例

(ii)起動中のウイルス対策ソフトなどを強制終了させます。

(iii)さまざまな妨害行為を施します。

- Windows に付属している「コマンドプロンプト」、「タスクマネージャ」、「レジストリエディタ」などのプログラムファイルを別のファイルに書き換え、ウイルスの駆除や感染確認作業を妨害します。
- 複数のウイルスを同時に実行します。そのうちの 1 つのウイルスが終了させられても、他のウイルスが、止められているウイルスを再実行させることにより、ウイルスの駆除作業を妨害します。
- ウイルスファイル自身の日付情報を改ざんして、日付による検索を妨害します。また、ウイルスのファイル属性を「隠しファイル」として、ウイルス自身が見えないようにします。
- インターネットへの接続時に参照する特定ファイル(hosts ファイル)を改ざんし、ウイルス対策ソフトベンダなどのウェブサイトへの接続を妨害します。

(3)主な被害内容

パソコンがこのウイルスに感染した場合、現在では、

(i) 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

(ii)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

(iii)他のウイルスをダウンロードさせられる

などの被害が発生することを確認しています(全ての症状が出るとは限りませんし、今後は他の症状が出る可能性があります)。

(i)の結果、Windows がシステムファイルを修復しようとして、図 1-4 のダイアログが表示され、システム CD が要求される場合があります。

(ii)で盗まれたアカウント情報で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ります。

また、(iii)により、さらに悪質なウイルスをダウンロードさせられる可能性もあるため、非常に危険な状態になると言えます。

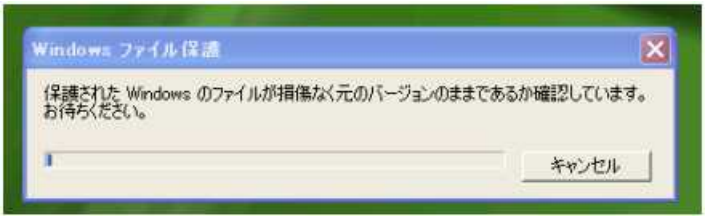

図 1-4 Windows ファイル保護メッセージダイアログ

(4)対策

(a)基本的な対策

パソコンがウイルスの感染被害を受けないための基本的な対策は、ウイルス対策ソフトのウイルス定義ファイルを常に最新の状態に更新して、リアルタイムのウイルス検知機能を有効にしておくことです。

また、パソコンだけでなく、USB メモリに対しても定期的なウイルスチェックの実施が必要です。

併せて、脆弱性を突かれてのウイルス感染を防ぐため、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。

(b)USB メモリの利用における対策

「(1)最近の届出・相談事例」にもあったように、利用者の不注意や利用目的の誤りによりウイルス感染、および感染の拡大を招くことがあります。USB メモリの利用においては、できる限り以下の原則に従いましょう。

(i)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。

(ii)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。

(iii)自宅から職場にウイルスを持ち込んだりしないよう、個人所有の USB メモリを会社のパソコンに接続しない、また、会社所有の USB メモリを自宅のパソコンに接続しない。

(5)USB メモリの自動実行を防止するための方法

USB メモリ感染型ウイルスは、Windows の自動実行機能を利用して感染することは、前述のとおりです。Windows の自動実行機能は利用者にとっては便利な機能ですが、ウイルスに悪用されると非常に危険であるため、USB メモリを接続しても自動実行しないように設定することをお勧めします。多少不便ですが、ウイルス感染の被害に遭わないためには有効な対策となります。

以下にその方法を説明します。

(a) Windows Vista の場合

パソコン画面のスタートボタンである「 」アイコンをクリック→メニューの中から「コントロールパネル」を選択→「ハードウェアとサウンド」項目の中の、「CD または他のメディアの自動再生」をクリックすると図 1-5 の設定画面が表示されます。

「自動再生」画面の「メディア」の種類には USB メモリはありませんが、「ソフトウェアとゲーム」設定項目で対応できます。「ソフトウェアとゲーム」設定項目をクリックし、その中から「何もしない」を選択し、最後に「保存」ボタンをクリックします。

一般にウイルスは、実行ファイル以外にも感染していることがありますので、他のファイル（オーディオファイル、ビデオファイル、DVD ムービーなど）も、同様に設定することをお勧めします。

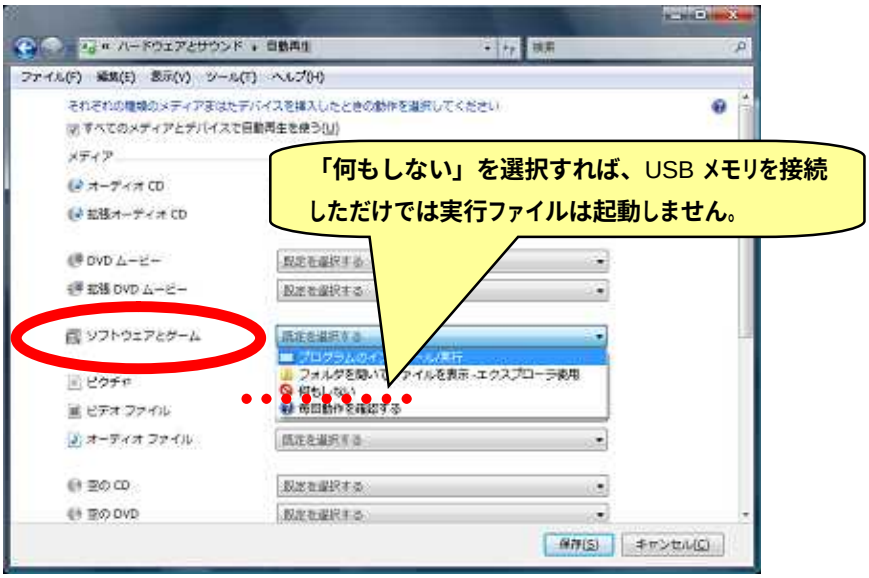

図 1-5 Windows Vista 「CD または他のメディアの自動再生」設定画面

ただし、Windows Vista には、2008 年 7 月にマイクロソフトが公開した、「Windows エクスプローラの脆弱性により、リモートでコードが実行される(MS08-038)」という脆弱性が存在することに注意する必要があります。この脆弱性を解消していない場合、上記の設定を行っていても、USB メモリ内に Autorun.inf ファイルと実行ファイルが存在すれば、USB メモリを接続すると自動的に実行ファイルが起動されてしまいます。

従って、設定変更とともに、必ずマイクロソフトからこの脆弱性に対する更新プログラムを入手し、脆弱性を解消することが必要です。また、確実に実行ファイルを自動起動させないためには、現在公開されているすべての重要な脆弱性について、Windows Update を実施し解消してください。

「Windows エクスプローラの脆弱性により、リモートでコードが実行される」脆弱性の解説
http://www.microsoft.com/japan/technet/security/bulletin/ms08-038.mspx

(b)Windows XP の場合

USB メモリ内に、Autorun.inf ファイル と実行ファイルが入っている場合でも、パソコンに接続した時点ですぐに実行ファイルが起動することはありません。しかしながら、「マイコンピュータ」から、USB メモリを認識したドライブをダブルクリックすると、実行ファイルが起動してしまいます。もし、USB メモリにウイルスが感染していた場合、パソコンにもウイルスが感染してしまう恐れがあります。

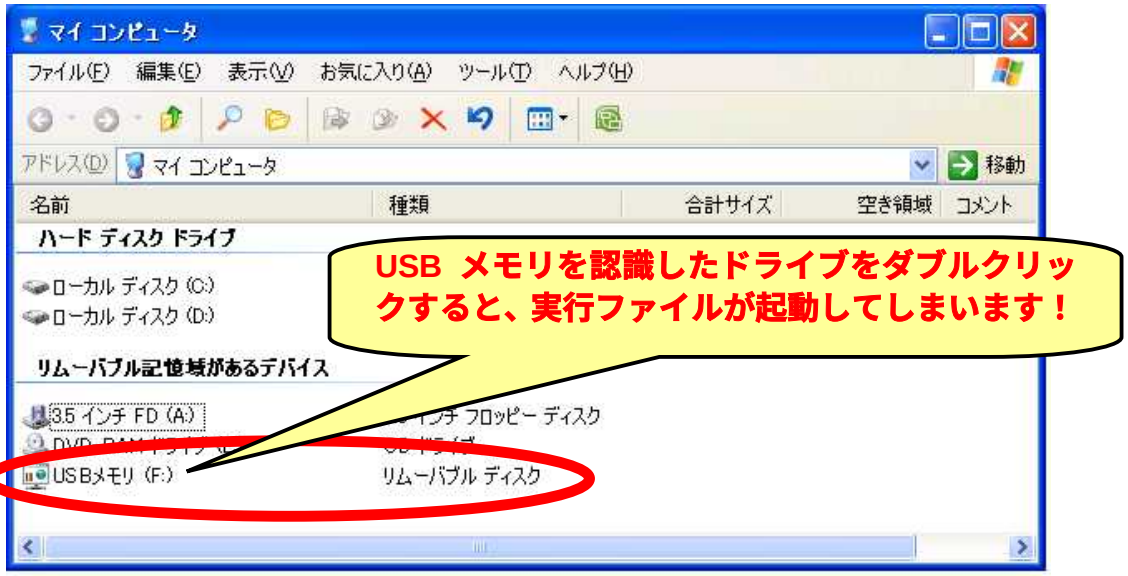

図 1-6 マイコンピュータ画面

この問題を解決する更新プログラムが 2008 年 9 月に Microsoft から公開されました。

「Windows で強制"無効"に自動実行レジストリキーを修正する方法」
http://support.microsoft.com/kb/953252/ja

「Windows XP 用の更新プログラム(KB950582)」
http://www.microsoft.com/downloads/details.aspx?FamilyId=CC4FB38C-579B-40F7-89C4-1721D7B8DAA5

この更新プログラムを適用することにより、USB メモリ内のプログラムが自動実行されないようになります。適用すると、図 1-6 の USB メモリを認識したドライブをダブルクリックしても自動実行されずに、図 1-7 のようにドライブの中身が見えるだけ、となります。

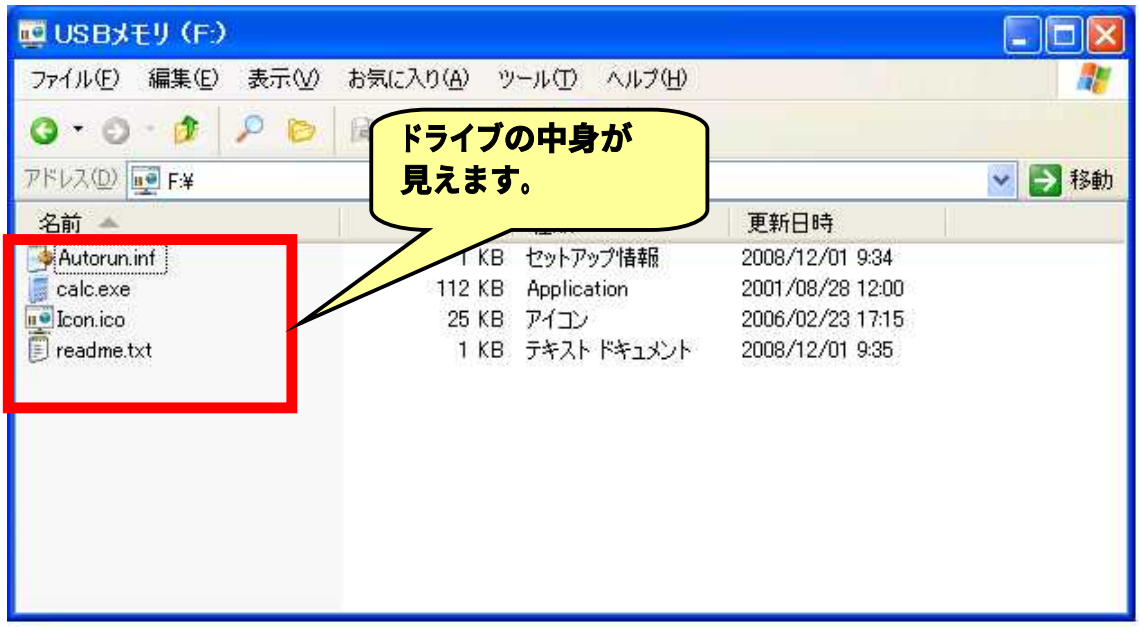

図 1-7 Windows エクスプローラ画面

自動実行を無効化したパソコンに USB メモリを接続した場合でも、リムーバブルディスクとして認識したドライブに対して、必ずウイルス対策ソフトで、ウイルスチェックを実施してから利用してください。併せて、Windows エクスプローラから USB メモリを認識したドライブの中身を見て、身に覚えの無い、怪しいファイルがないかを確認しましょう。怪しいファイルがあった場合、決して開かずに、すぐに削除してください。自身で判断がつかない場合は、詳しい人に聞くなどしてください。

(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、8 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
・オンラインゲームサイトで、自分のアカウントが乗っ取られた

○ 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「4.相談受付状況」を参照)

・USB メモリ内に、身に覚えのない怪しいファイルがある
・ファイル共有ソフトでダウンロードしたファイルがウイルスだった？

○ 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。

・22/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 25.6 万個と、10 月の約 27.2 万個から 6%の減少となりました。
また、11 月の届出件数(※2)は、1,830 件となり、10 月の 1,839 件から同水準での推移となりました。

※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。
・11 月は、寄せられたウイルス検出数約 25.6 万個を集約した結果、1,830 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 万個 、2 位は W32/Autorun で約 10 万個、3 位は W32/Mytob で約 4 千個でした。

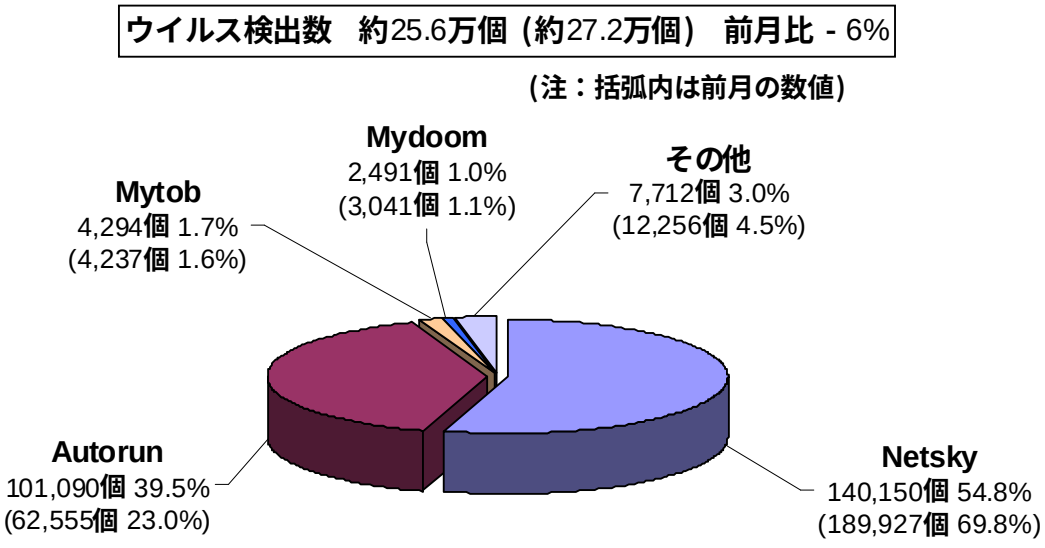

図 2-1

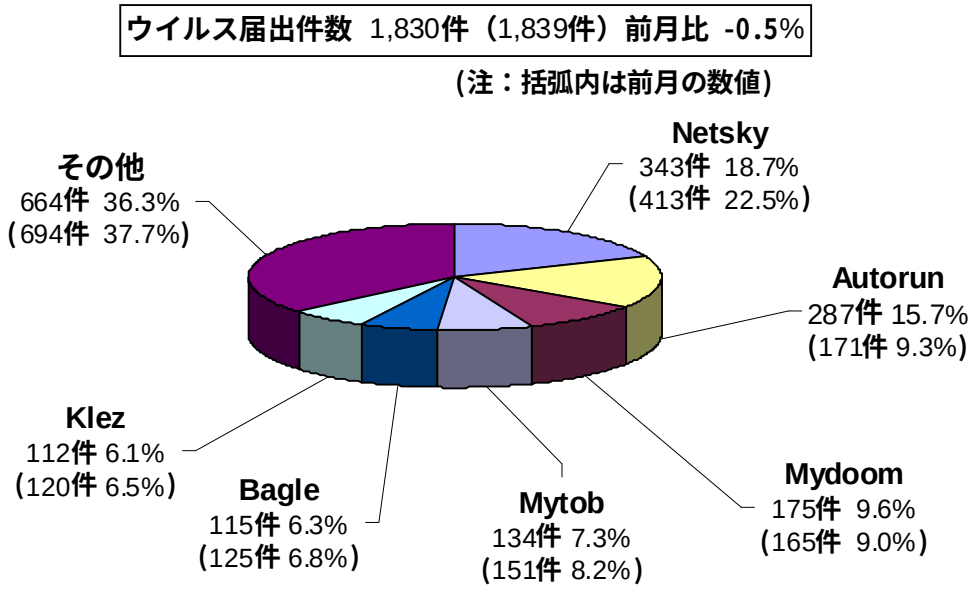

図 2-2

(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 月には、10 月に多数寄せられた FAKEAV がほとんどなくなり、その他の不正プログラムの検知数も激減しました（図 2-3 参照）。

このように減少した要因のひとつとして、不正プログラムの配信元がネットワークから遮断されたことが挙げられます。

（ご参考）

迷惑メールの流通量が 75%減、悪質業者に対するネット遮断が奏功

http://itpro.nikkeibp.co.jp/article/NEWS/20081113/319233/

現在は検知数が少ない状況となっていますが、今後、いつ急増するかわかりませんので、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。

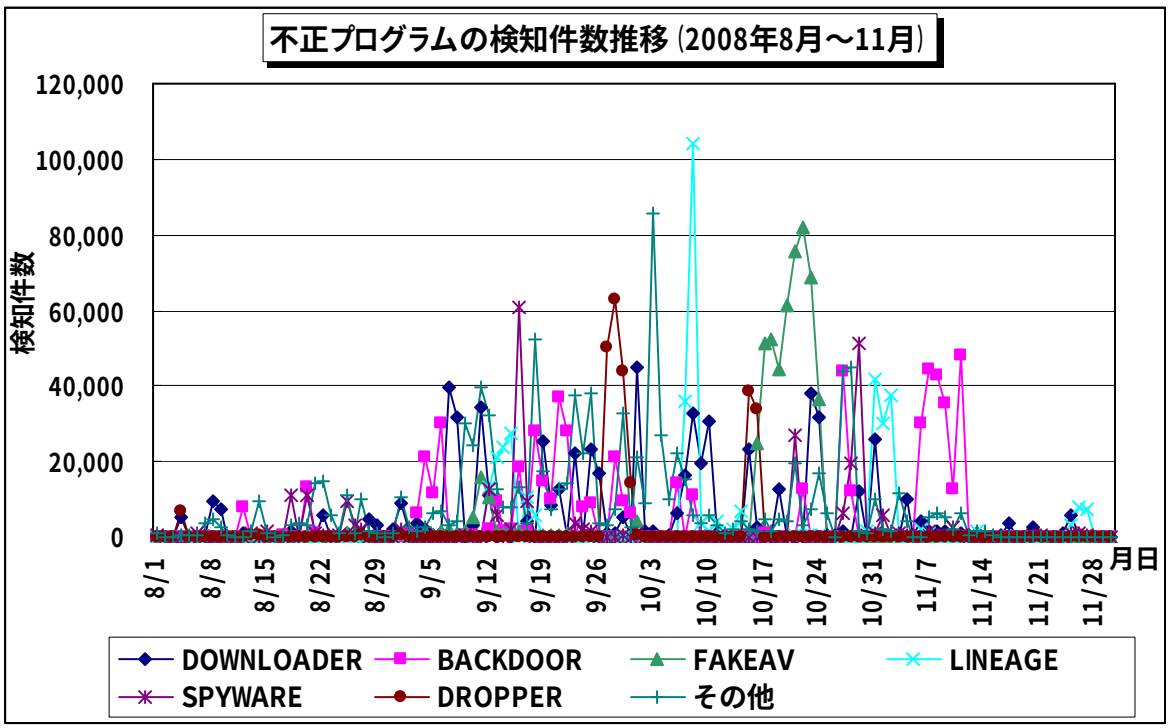

図 2-3

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

		6月	7月	8月	9月	10月	11月
届出(a) 計		13	19	15	14	17	18
	被害あり(b)	11	18	10	12	12	12
	被害なし(c)	2	1	5	2	5	6
相談(d) 計		36	49	25	38	58	39
	被害あり(e)	15	26	13	20	22	19
	被害なし(f)	21	23	12	18	36	20
合計(a+d)		49	68	40	52	75	57
	被害あり(b+e)	26	44	23	32	34	31
	被害なし(c+f)	23	24	17	20	41	26

(1)不正アクセス届出状況

11 月の届出件数は 18 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 39 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 5 件、DoS 攻撃が 1 件、その他(被害あり)6 件でした。

侵入届出の被害は、他サイト攻撃などの踏み台として悪用されたものが 4 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(残りの 1 件は原因不明)。

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 4 件(オンラインゲーム 4 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

事例	・自組織で運用しているウェブサーバが、とある迷惑メール発信元ブラックリストに載ったという連絡を受けた。 ・サーバを調査したところ、ログが消された上、メールサーバとしての設定が施され、メール送信サーバとして稼働されていたことが判明。 ・その他、いくつかのシステムコマンドが削除されていたり、不正なプロセスが稼働していたりしたことも分かった。 ・SSH で使用しているポートから侵入されたらしい。ボットらしきプログラムを埋め込まれ、迷惑メール発信の踏み台として悪用されていたようだ。
解説・対策	SSH で使用しているポートからパスワードクラッキングで侵入され、乗っ取られてしまった典型的な例と言えます。 **自組織が管理する IP アドレスが迷惑メール発信元としてブラックリストに載ってしまうと、本来の正しいメールサーバから発信されたメールも、相手側メールサーバによって拒否されてしまう可能性があります。**相手側にメールが届かないなどの事故が頻発する場合は、このような事例もあるということを念頭に置いて、調査を進めるべきでしょう。 パスワード認証は、時間を掛けられればいつかは破られる、という原則を再認識しましょう。ログのチェック、接続許可制限などの対策が有効ですが、**SSH 運用時には、ログインの際に公開鍵認証※などの強固な認証の採用を推奨**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

※公開鍵認証：公開鍵と秘密鍵のペアでユーザ個人の認証を行う方式のこと。

[なりすまし]

(ii) オンラインゲームサイトで、自分のアカウントが乗っ取られた

事例	・オンラインゲームサイトにログインしようとしたら、「パスワードが違います」となり、ログインできなかった。 ・サイト運営会社に問い合わせたところ、何者かが本人になりすましてログインし、パスワードを変更してアカウントを乗っ取っていたことが判明。 ・さらに、ゲーム内で有料コンテンツを勝手に購入されていたことも判明。 ・今思えば、色々なウェブサイトを閲覧中に怪しいリンクをクリックしたり、怪しいファイルを開いたりしており、それが原因でウイルスに感染していたのかもしれない。
解説・対策	**ある特定のゲームサイトへのログイン ID とパスワードを盗むウイルスが存在します。**サイトでのゲームプレイ中、**チャットで話して仲良くなった相手から示されたサイトにアクセスした際に、そのようなウイルスに感染することがあります。**また、**「便利なツールだ」と言われてインストールしたツールが、実はそのようなウイルスだったということもあります。**ゲームプレイ中は慎重に行動しましょう。もちろん、ウイルス対策ソフトの導入も、有効な対策となります。 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。 (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

11 月の相談総件数は 713 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 144 件(10 月：305 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 28 件(10 月：31 件)、Winny に関連する相談が 5 件(10 月：5 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(10 月：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

	6月	7月	8月	9月	10月	11月
合計	1,211	1,387	1,616	2,154	1,171	713
自動応答システム	693	817	994	1,302	677	363
電話	456	500	548	755	441	288
電子メール	60	70	69	93	47	62
その他	2	0	5	4	6	0

※ 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。

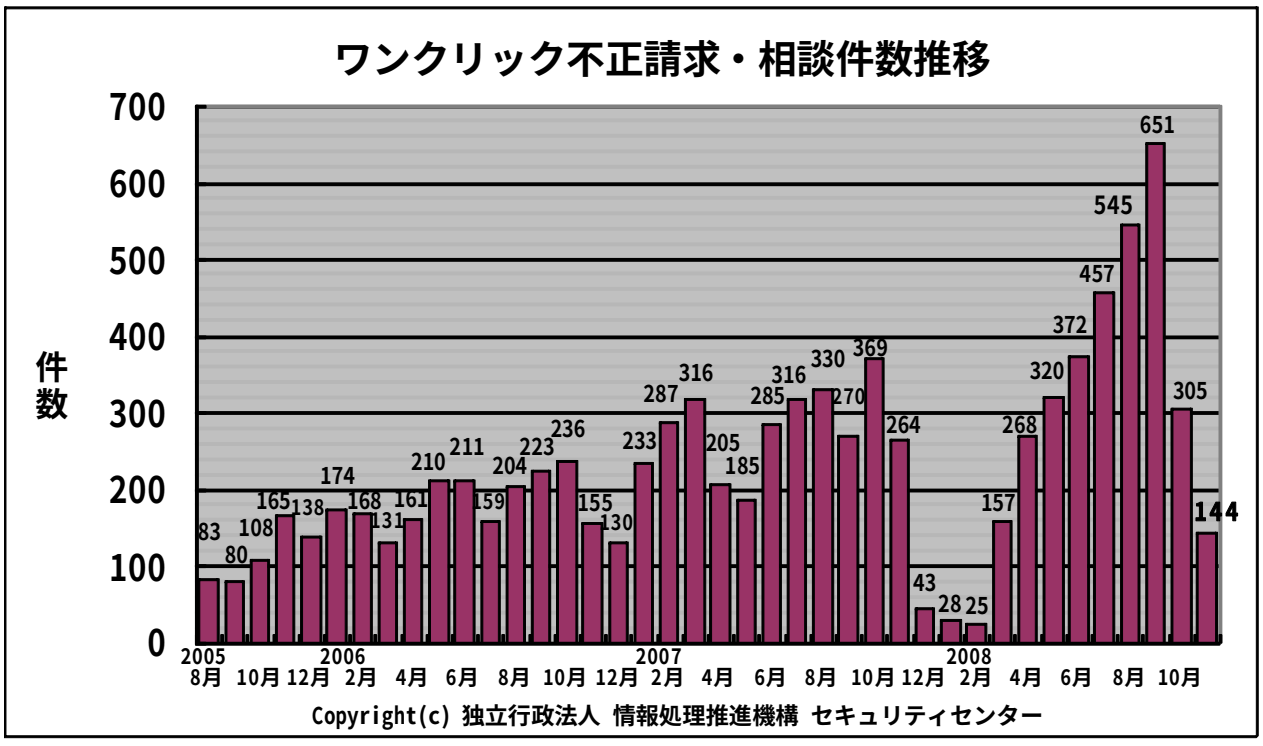

図 4-1　ワンクリック不正請求相談件数の推移

主な相談事例は以下の通りです。

(i) USB メモリ内に、身に覚えのない怪しいファイルがある

相談	職場で使っている USB メモリの中に、「sizhu.exe」という身に覚えのないファイルを見つけた。これはウイルスなのか。手持ちのウイルス対策ソフトでは、何も検知されなかった。
回答	疑問に思ったことは、すぐに検索サイトで調べてみましょう。今回の場合、「sizhu.exe」というファイル名そのものをキーワードで検索すると、このファイル名を名乗るウイルスが存在することが分かります。さらに、ウイルス対策ソフトベンダが提供するウイルス情報によれば、USB メモリなど外部記憶メディアを介して感染を広げるタイプのようです。つまり、今回見つけたファイルは、ウイルスである可能性が非常に高いと言えます。このファイルを、できるだけ多くのウイルス対策ソフトで検査してみることをお勧めします。「VIRUS TOTAL」は、オンラインで疑わしいファイルを解析してくれるサービスです。無償で、同時に 30 種類以上のウイルス対策ソフトによるチェックが可能です。 (ご参考) VIRUS TOTAL http://www.virustotal.com/jp/

(ii) ファイル共有ソフトでダウンロードしたファイルがウイルスだった？

相談	パソコンが起動する際、壁紙がいつもと違って青くなっており、さらに英語で「Spyware・・」などと書かれていたのに気づいた。Windows が立ち上がった後には、英語でウイルス対策ソフトのようなものの購入を勧めるような警告画面が出るようになった。自分には身に覚えが無かったため、このパソコンをいつも使っている子どもに事情を聴くと、Cabos というファイル共有ソフトで何やらファイルをダウンロードし、ファイルを開いた後にこうなったらしい。ウイルスに感染したのか。
回答	Cabos でダウンロードしたファイルが、「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だったようです。しかし今回はそのことよりも、複数人で共用しているパソコンでファイル共有ソフトが使われていたことの危険性を認識すべきです。即ち、ファイル共有ソフトの存在を知らずにパソコン内に機密情報を保管していると、それらが意図せずにファイル共有ネットワークに流出してしまう可能性があるということです。親として、ファイル共有ソフトの危険性をお子さんに教育することも必要です。違法行為を止めさせ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 11 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 11 月の期待しない(一方的な)アクセスの総数は 10 観測点で 113,906 件、総発信元※は 34,179 箇所ありました。平均すると、1 観測点につき 1 日あたり 114 の発信元から 380 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。

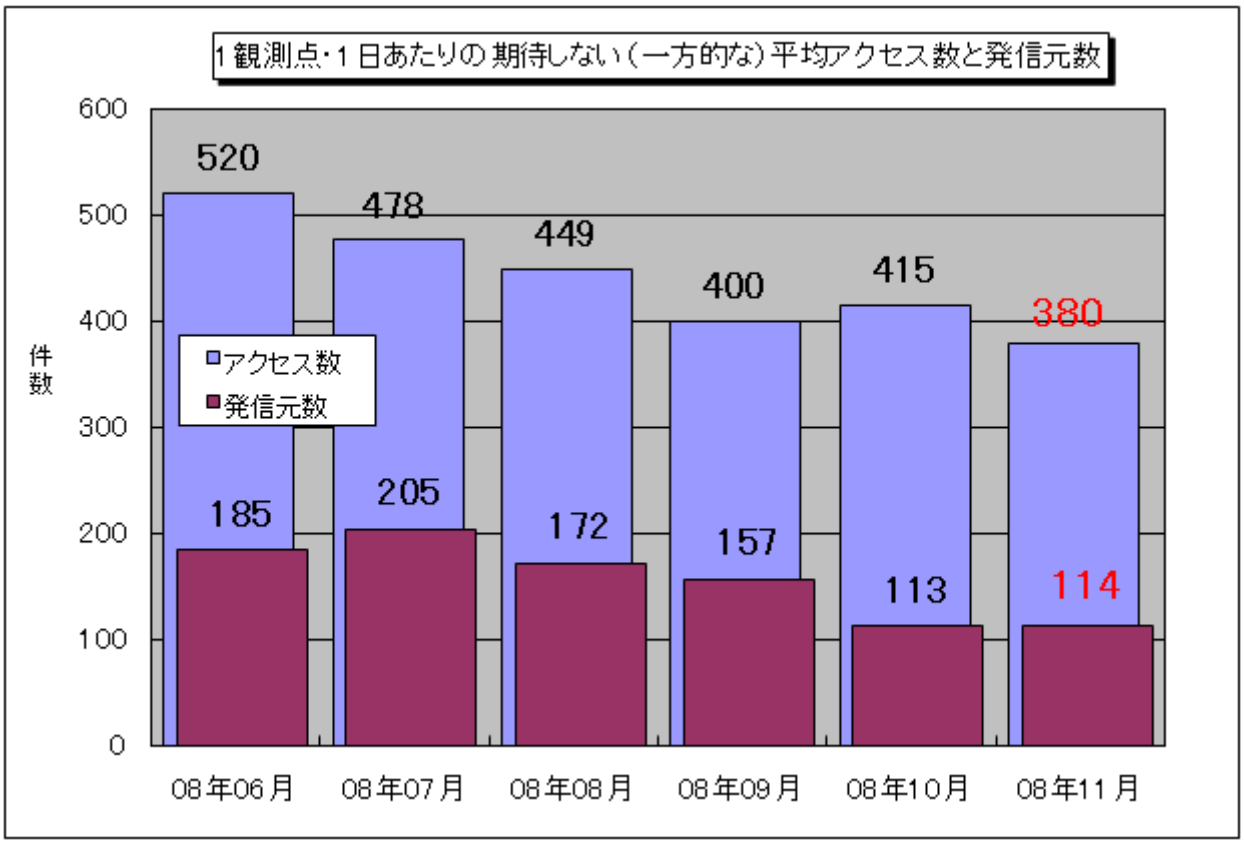

図 5-1： 1 観測点・1 日あたりの期待しない(一方的な)平均アクセス数と発信元数

2008 年 6 月～2008 年 11 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、11 月の期待しない(一方的な)アクセスは 10 月と比べて若干減少しました。過去 6 ヶ月を通してみると、減少傾向にあると言えます。

(1) 22/tcp へのアクセス

TALOT2 には、管理上、SSH(*1)を利用している観測点があります。その観測点の 22/tcp (SSH で利用されるポート)に対してアクセス(*2)を行う発信元数が、11 月 20 日に急増したのち、緩やかに減少していきました。

TALOT2 では攻撃の内容を解析していないため、断定はできませんが、このアクセスは日本時間の 11 月 15 日に公開された SSH の脆弱性を突く、攻撃を行うための探索行為であった可能性があります。

＜参考情報＞

■「SSH 通信において一部データが漏えいする可能性」(JVN)
http://jvn.jp/niscc/CPNI-957037/

TALOT2 で SSH を利用している観測点の 22/tcp へのアクセスの発信元数の変化を図 5-2 に示します。

(*1) 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。

(*2)SSH を利用している観測点に対する 22/tcp への観測データは、アクセスに対する応答を行わない他の観測データとは異なるため、統計情報からは除外してあります。

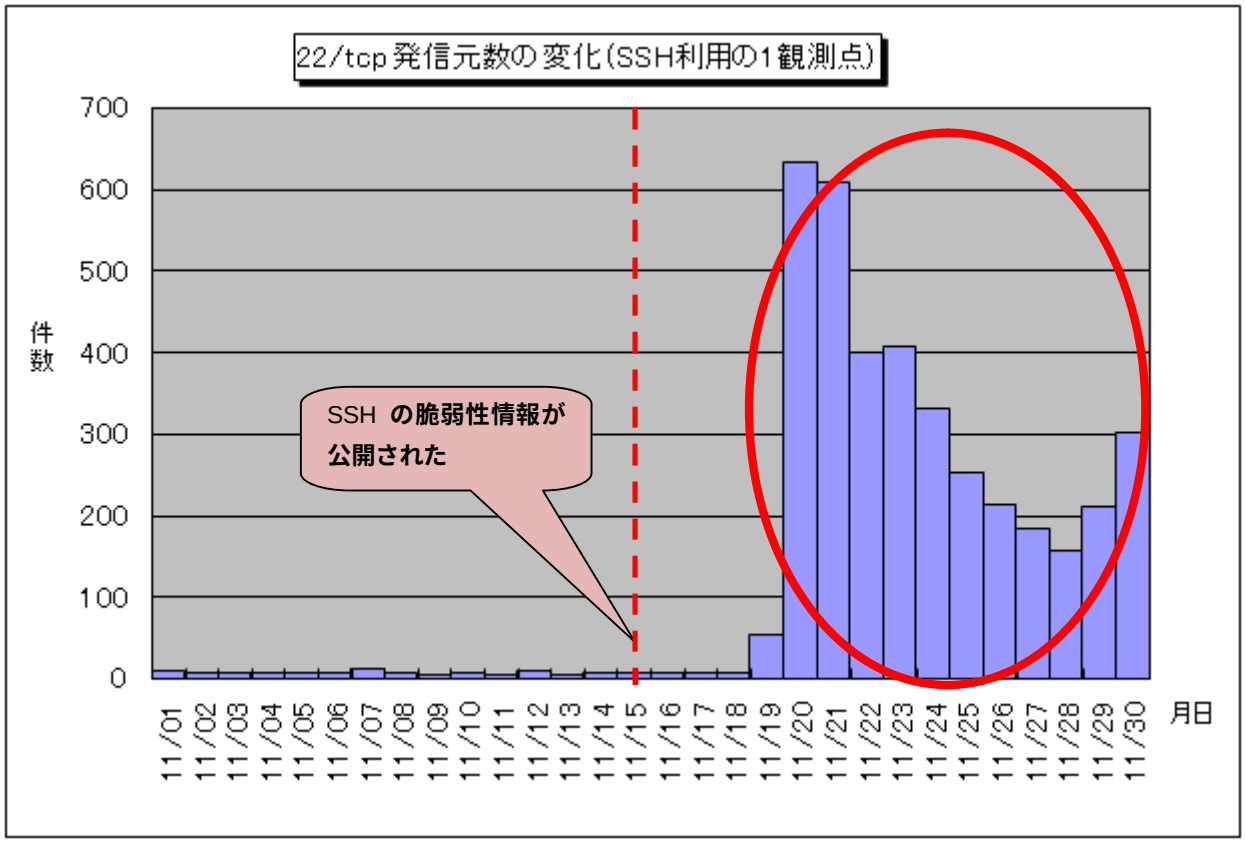

図 5-2： 22/tcp 発信元数の変化（SSH 利用の 1 観測点）

脆弱性情報が公開されると、短期間でその脆弱性に関連したアクセスが増えることがあります。サーバ管理者の方は、日頃から JVN などの脆弱性対策情報ポータルサイトを確認して、お使いのシステムの脆弱性対策を迅速に行えるようにしてください。

＜参考情報＞

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

■「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/TALOT2-0812.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