

コンピュータウイルス・不正アクセスの届出状況 [2007 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:藤原 武平太)は、2007 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: その巻

「ファイル共有ソフト、それでもまだ使い続けますか？」
一向に無くならない情報漏えい

IPA には毎月、「Winny 経由で会社の情報が漏れてしまったが、どうしたらいいですか？」とファイル共有ソフトを介した情報漏えいに関する相談が相当数寄せられています。これらのほとんどが Winny を利用して感染を拡大する W32/Antinny というウイルスに感染することにより発生しています。

企業の機密情報や個人情報などが漏えいする事故が相次いでいるなか、それでも一向にファイル共有ソフト利用者が減っていません。それは、ファイル共有ソフトや情報を漏えいさせるウイルスが持つ危険性が正しく理解されていないためです。ユーザ自身の興味本位による行動がこのような被害を招いていることを認識して、自身の行動に注意していただくようお願いします。

(1) ファイル共有ソフトとは？

ファイル共有ソフトには代表的なものとして、(i)Winny、(ii)Share、(iii)Cabos、(iv)LimeWire などがあります。ある調査によると、Winny 利用端末は、2007 年 8 月末の時点で約 34 万台、Share 利用端末は約 15 万台とのことです。これら多数のユーザ間で、ファイルが共有されるのです。

これら多くのファイル共有ソフトでは、公開したいファイルを置くフォルダは、自分で設定します【図 1-1】。つまり、**利用者の操作ミスや設定の誤り一つで公開したくないファイルを公開してしまい、情報が漏えいする可能性があります。**「公開」フォルダに置かれたファイルは、ファイル共有ソフトを利用している不特定多数のユーザ同士で共有されるため、**その行き先が分からなくなってしまう**。その上、ファイルが多くの利用者にダウンロードされてしまうと、回収が事実上不可能になってしまいます。



図 1-1: Winny ネットワーク例

このように、ファイル共有ソフトの利用には多くの危険を伴います。よって、**単なる興味本位で利用することは絶対に慎まなくてはなりません。**

(2) 情報を漏えいさせるウイルスとは？

ファイル共有ソフトを利用して情報を漏えいさせるウイルスの多くは、「お宝画像」、「個人情報」のような多数の人が興味をもつ単語を含むファイル名で出回っています。ユーザがファイル共有ソフトを利用してそれらのファイルをダウンロードし、ファイルを開くことにより、情報を漏えいさせるウイルスがユーザのパソコンに感染してしまいます。

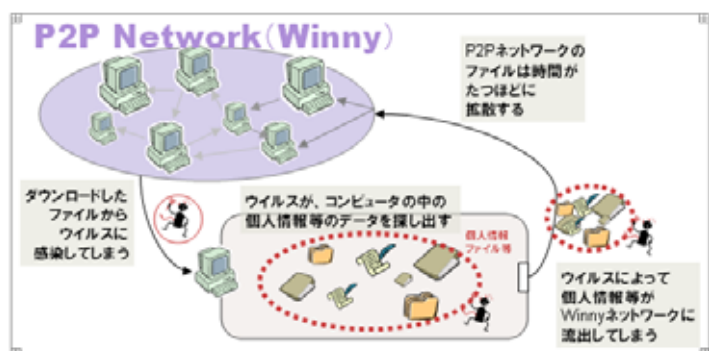


図 1-2: ファイル共有ソフトによる情報漏えいの例

パソコンに感染したウイルスは、パソコン内の送受信メール、ワープロ、表計算の文書、画像や動画ファイル等の各種の情報を一つのファイルとしてまとめ、公開フォルダにコピーしてしまいます。また、この過程でウイルス(自分自身)を紛れ込ませます。

こうして、**ウイルスがパソコンの中から各種の情報をファイル共有ネットワークに流出させて情報漏えい**が起きることになるとともに、**情報を漏えいさせるウイルスもファイル共有ネットワークに広がって行きます。**

(3) ファイル共有ソフトによる情報漏えい事故に至る想定事例

(a) 会社のルールを破って仕事のデータを自宅に持ち帰り、ファイル共有ソフトを利用している私用パソコンに**仕事のデータをコピーして仕事をしたために、会社のデータが漏えい**しまった。

(b) ファイル共有ソフトを利用しているが、USB メモリや、ポータブルハードディスクなどの外部記憶メディアの中の情報は大丈夫だろうと思い、**パソコンに接続して情報が漏えい**してしまった。

(c) 家族で共用しているパソコンでは、ファイル共有ソフトを使用していないので安心だと思っていた。しかし、**自分以外の家族がこっそりファイル共有ソフトを使っているのを知らずに、そこで仕事を行い、重要ファイルを残したままにして、情報が漏えい**してしまった。

(d) 重要情報を保存したパソコンを譲渡する時、その情報が入ったファイルは**全て消したつもりだった。しかし、そのファイルが一時保存領域などに残っていたため、その後そのパソコンを入手した人がファイル共有ソフトを使用して、消したはずの重要ファイルの情報が漏えい**してしまった。

(e) 中古パソコンを入手して利用していたが、**以前の利用者がファイル共有ソフトを削除せずに残っていた事**を知らず、重要な情報が漏えいしてしまった。

以上のようにファイル共有ソフトによる情報漏えいは、思いがけないことで起きることが想定されますので、いくら注意をしても**ファイル共有ソフトを利用し続ける限りは、情報漏えい事故はなくなりません。**

このため IPA では従来から「**ファイル共有ソフトを使用しないで下さい**」と呼びかけておりますが、再度注意喚起をします。

参考:

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

今月の呼びかけ：その式

「ウイルスの見分け方を再確認しよう！」 騙されないための対策例

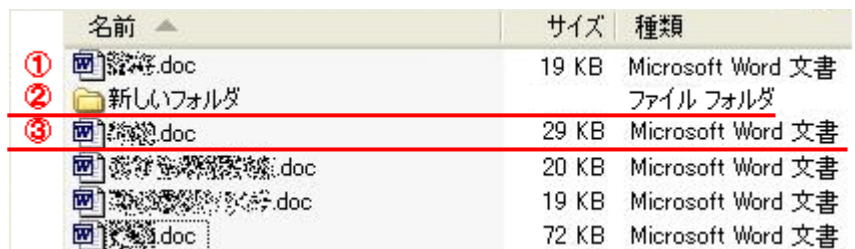
ウイルス感染への予防策として、「セキュリティホール対策(OS や各種アプリケーションのアップデート)の実施」、「ウイルス対策ソフトの利用と定期的なパターンファイルの更新」を行うのは当たり前です。最近のウイルスは亜種が多く、日々新しいウイルスが作られています。

インターネットなどから入手したファイルをウイルス対策ソフトでスキャンして、“ウイルスが検知されなかったから安全”とは限りません。

(1)ウイルスの見分け方

ファイルの見た目に巧妙な仕掛けがされている場合があります。一看すると、アイコンはフォルダに見えますが、実はウイルスであるというように、**ファイルの見た目を偽装しているのです**。偽装を見抜くには、ファイルの拡張子を確認する必要があります。

【図 1-3】は、ウイルスに感染していない正常な状態の例です。【図 1-3】の は種類が「**ファイルフォルダ**」で、フォルダには拡張子は付きません。 のファイルは、名前の欄に表示されているファイル名の**拡張子が「.doc」**で、**種類が「Microsoft Word 文書」**となっています。

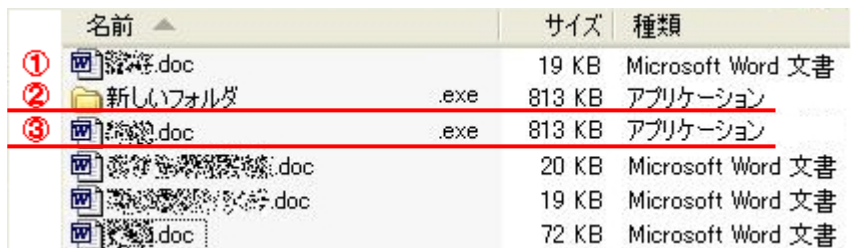


名前	サイズ	種類
① 123456789.doc	19 KB	Microsoft Word 文書
② 新しいフォルダ		ファイル フォルダ
③ 123456789.doc	29 KB	Microsoft Word 文書
123456789.doc	20 KB	Microsoft Word 文書
123456789.doc	19 KB	Microsoft Word 文書
123456789.doc	72 KB	Microsoft Word 文書

図 1-3: 正常なファイルの例

【図 1-4】はウイルスに感染した状態の例です。【図 1-4】の のファイルは、【図 1-3】の と同じなので、正常なファイルです。

しかし、 と の名前の欄に表示されているファイル名の**拡張子が「.exe」**となっており、**種類が「アプリケーション」**となっています。



名前	サイズ	種類
① 123456789.doc	19 KB	Microsoft Word 文書
② 新しいフォルダ	.exe 813 KB	アプリケーション
③ 123456789.doc	.exe 813 KB	アプリケーション
123456789.doc	20 KB	Microsoft Word 文書
123456789.doc	19 KB	Microsoft Word 文書
123456789.doc	72 KB	Microsoft Word 文書

図 1-4: ウイルスファイルの例

この二つのファイルが、アイコンをフォルダや Word 文書に見せかけたウイルスの典型的な例です。

ファイルの種類を正しく見分ける知識を身につけないと、ウイルスと知らずに開いてしまい、感染してしまいます。しかし Windows の初期設定では**拡張子が表示されない**ようになっています。拡張子を確認するためには、以下の手順で設定を変更して下さい。

(a)Windows XP の場合

マイコンピュータもしくはエクスプローラのメニューバーから[ツール] - [フォルダオプション] - [表示]タブを選択し、[登録されている拡張子は表示しない]のチェックを外す

(b)Windows Vista の場合

スタートボタンから[コントロールパネル] - [デスクトップのカスタマイズ] - [フォルダオプション] - [表示]タブを選択し、[登録されている拡張子は表示しない]のチェックを外す

設定を変更した後、再度ファイル名を確認して【図 1-4】の や の特徴を持つファイルが見つかったら、**直ぐに削除してください(ゴミ箱に移動した後、ゴミ箱を空にする)**。

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でデータが改ざんされた

相談の主な事例 (相談受付状況及び相談事例の詳細は、9 頁の「4.相談受付状況」を参照)

- ・Antinny ウイルスが検出された
- ・出会い系サイトに登録したら一方的にメールを送られ続けている

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。

- ・Windows Messenger サービスを悪用したアクセスに注意!

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 60 万個と、10月の50万個から18.5%の増加となりました。
また、11月の届出件数(2)は、2,351件となり、10月の2,419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を。
・11月は、寄せられたウイルス検出数約60万個を集約した結果、2,351件の届出件数となっています。

検出数の1位は、W32/Netskyで約51万個、2位はW32/Lookedで約2万個、3位はW32/Mytobで約1.8万個でした。

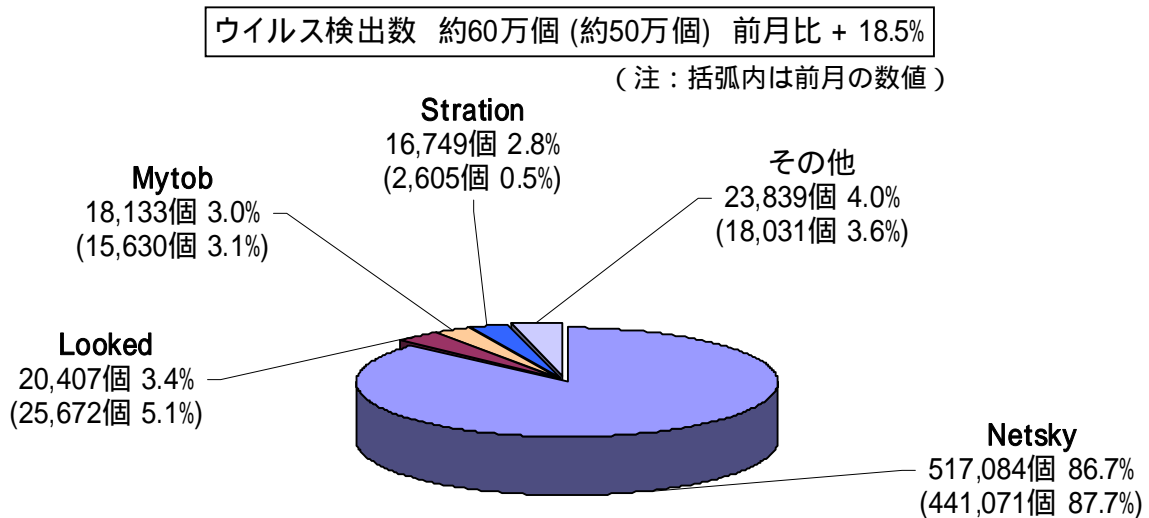


図 2-1

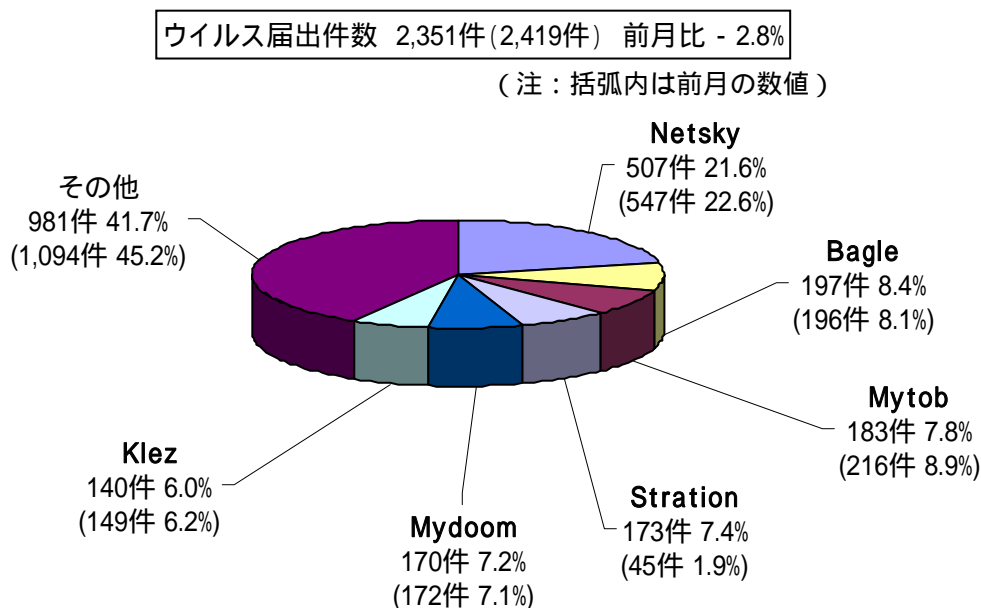


図 2-2

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 -

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	41	10	16	10	10	15
被害あり ^(b)	36	8	13	8	9	11
被害なし ^(c)	5	2	3	2	1	4
相談^(d) 計	27	25	23	27	37	31
被害あり ^(e)	11	11	15	12	22	17
被害なし ^(f)	16	14	8	15	15	14
合計^(a+d)	68	35	39	37	47	46
被害あり ^(b+e)	47	19	28	20	31	28
被害なし ^(c+f)	21	16	11	17	16	18

(1) 不正アクセス届出状況

11月の届出件数は15件であり、そのうち被害のあった件数は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31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17件でした。

(3) 被害状況

被害届出の内訳は、**侵入6件、DoS攻撃1件、アドレス詐称1件、その他(被害あり)3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、などでした。侵入の原因は、パスワードクラッキング攻撃によるものが3件、サーバOSその他アプリケーションのぜい弱性放置によるものが3件、などでした。

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。

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 攻撃でデータが改ざんされた

事例	<ul style="list-style-type: none">・データベース内データのウェブ表示でエラーが発生。・データベース内のデータ 1000 箇所以上に、見覚えのない文字列 【<script src="http://(省略).net/0.js"></script>】が追記されていることを発見。・正規の手続きを踏んでデータ書き込みした場合に更新される情報が、更新されていなかった。他の何らかの方法で書き込まれていたということ。・データベースサーバは、外部(インターネット)からは直接アクセス出来ないところに配置してある。通常はウェブサーバ上のウェブアプリケーションを介してアクセスする。・SQL インジェクション対策が一部で未対応であったことが原因と思われた。
解説・対策	<p>ウェブサーバ上のウェブアプリケーションにぜい弱性があったため、SQL インジェクション攻撃の被害を受け、結果的にデータベース内のデータが機械的に改ざんされてしまった例です。このサイト以外にも同様の被害事例が多数見受けられましたので、攻撃者はぜい弱性があるサイトを無差別的に攻撃している模様です。</p> <p>ぜい弱性を攻撃されると、改ざん・消去のみならず、閲覧も可能ですから、情報漏えいにつながる恐れがあります。SQL インジェクション対策に漏れがないか、再度確認をしましょう。</p> <p>(参考)</p> <p>IPA - セキュアプログラミング講座(Web アプリケーション編) http://www.ipa.go.jp/security/awareness/vendor/programmingv2/</p> <p>IPA - 安全なウェブサイトの作り方 改訂第2版 http://www.ipa.go.jp/security/vuln/websecurity.html</p>

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。

4. 相談受付状況

11月の相談総件数は911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**264件**(10月:369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**14件**(10月:16件)、Winnyに関連する相談が**31件**(10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

		6月	7月	8月	9月	10月	11月
合計		932	1162	1013	910	1128	911
	自動応答システム	537	694	593	544	669	520
	電話	339	402	374	310	397	337
	電子メール	53	65	43	55	57	52
	その他	3	1	3	1	5	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)

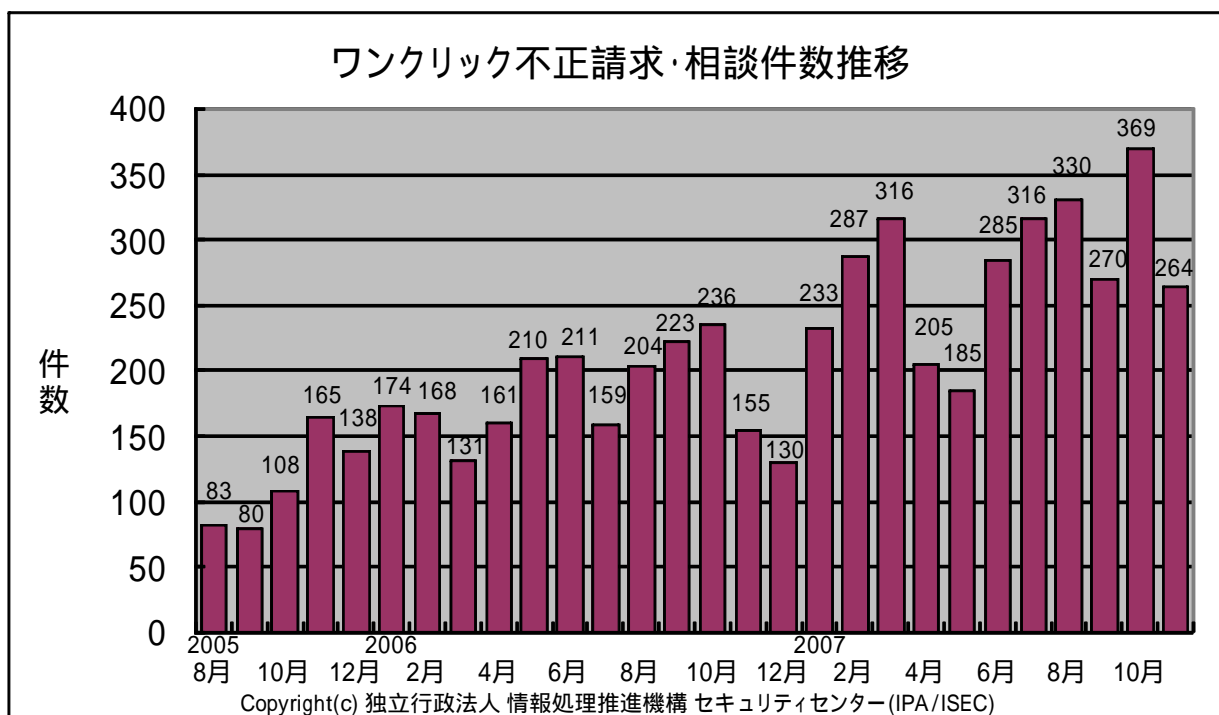
FAX: 03-5978-7518 (24時間受付)

「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。

(参考) 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) Antinny ウイルスが検出された

相談	つい先日までファイル共有ソフト share を使っていた。ダウンロードしたファイルは、必ずウイルス対策ソフトでチェックしてから開いていた。ある日、これまでと異なるウイルス対策ソフトでチェックしたら Antinny ウイルスが数種類検出された。ウイルスはすぐ削除してしまった。ファイル共有ソフトも、今では削除してしまっている。情報漏えいしているのか？
回答	検出されたウイルスは Winny の動作を悪用して情報漏えいさせるものでした。しかし、 現時点では検出できないウイルスに感染していたことも考えられるため、安心はできません。 ファイル共有ソフト share を削除していなければ、share の動作を悪用されての情報漏えいの有無は確認できましたが、今となってはどうすることもできません。 二次被害を想定した対策が望まれます。 (ご参考) IPA - 「情報漏えい発生時の対応ポイント集」 http://www.ipa.go.jp/security/awareness/johorouei/

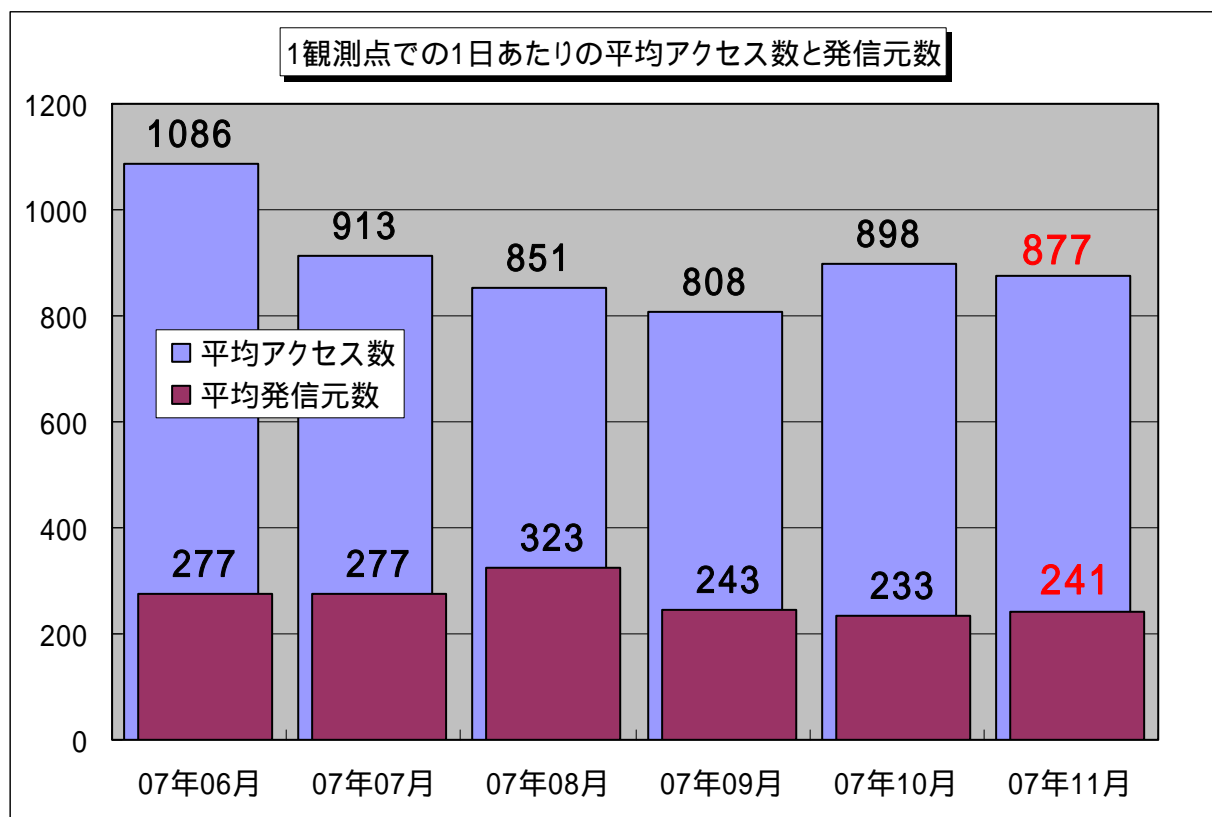
(ii) 出会い系サイトに登録したら一方的にメールを送られ続けている

相談	インターネットの出会い系サイトに登録した。後で考え直し、登録を解除しようと申し出たが、業者側が対応してくれない。そのサイトから、毎日大量の案内メールが送られてくる。どうすれば良いか。
回答	悪質な業者だと、素直に話を聞き入れてくれる可能性は低いでしょう。まずは、 メールをフィルタで振り分けて無視しましょう。恒久的対策としては、メールアドレスを変更することになります。 今後は、 信頼できるか分からない業者には、不用意にアドレスを教えないことが一番の予防策 となります。どうしても相手にアドレスを教えなくてはならない場合は、念のため、変更もしくは削除しても良いアドレスを教えるのが良いでしょう。

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、2007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263,077件ありました。1観測点で1日あたり241の発信元から877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、241人の見知らぬ人(発信元)から、発信元一人あたり約4件の不正と思われるアクセスを受けている**ということになります。



【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】

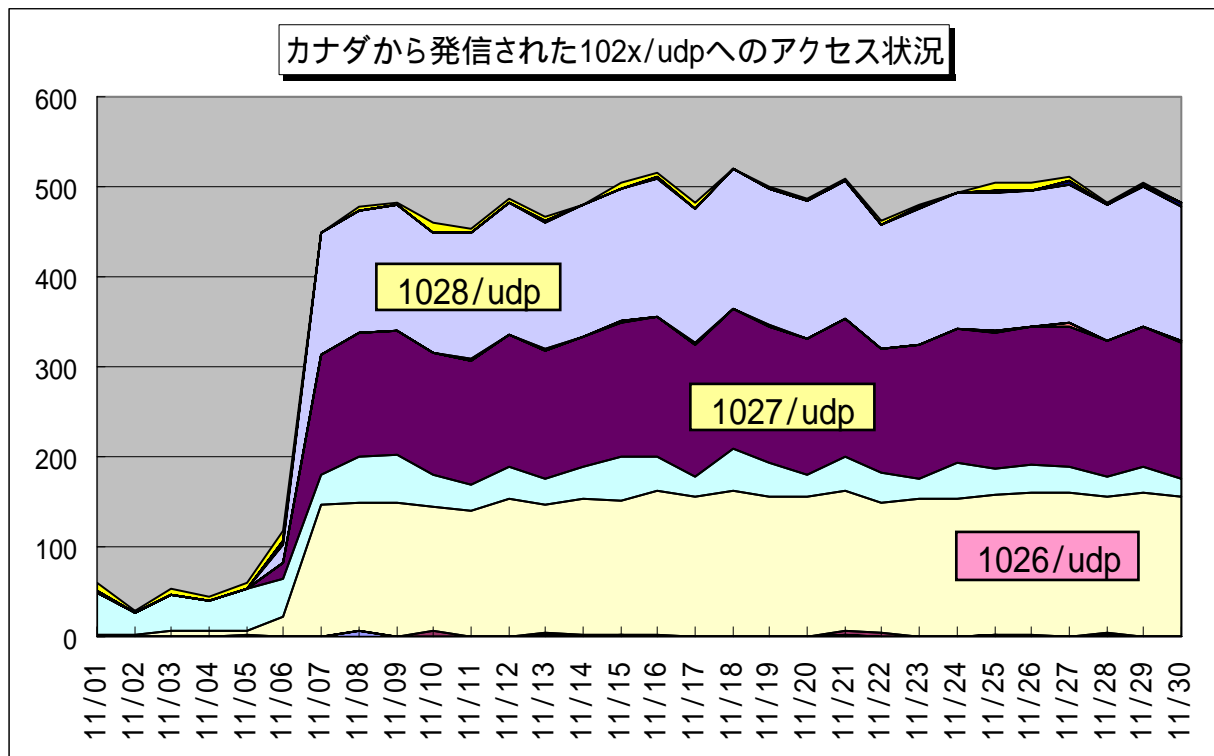
2007年6月～2007年11月までの各月の1観測点での1日あたりの平均アクセス数および、それらのアクセスの平均発信元数を図5-1に示します。この図を見ると、期待しない(一方的な)アクセスは、10月とほとんど同じ傾向にあります。

2007年11月のアクセス状況は、10月と比べても変わりなくほとんど同じ状況でした。その中で、Windows Messenger サービスを悪用してポップアップメッセージを送信するアクセスの内、1028/udpが増加しました。

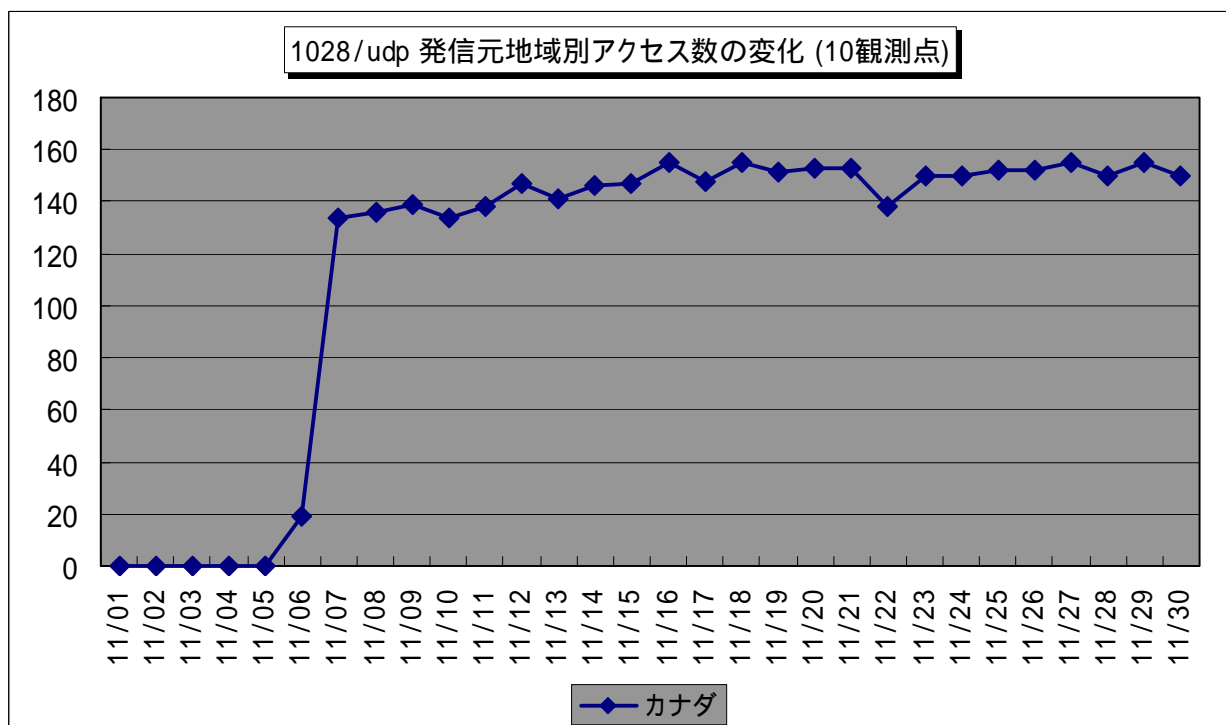
(1) Windows Messenger サービスを悪用したアクセスの発信元状況

Windows Messenger サービスを悪用してポップアップメッセージを送信するアクセスは、1026/udp、1027/udp、1028/udp に対して行なわれますが、11 月は 1028/udp に対するアクセスが多く見受けられました。

これらの発信元は、そのほとんどがカナダからで、1026/udp、1027/udp に対するアクセスも、アクセス数 1 位の中国(中華人民共和国)に次いで、多く見受けられます。(図 5-2 参照)



【図 5-2 2007 年 11 月 カナダから発信された 102x/udp へのアクセス状況】



【図 5-3 2007 年 11 月 1028/udp 発信元地域別アクセス数の変化 (10 観測点)】

これらのアクセスは、迷惑メールと似ていて、Windows Messenger サービスを悪用してポップアップメッセージを送りつけてくるもので、「コンピュータに重度の障害が発生しました」旨の嘘の内容で脅し、特定の URL をクリックさせようとしています。

ほとんどがスパムメッセージと思われるので、無視をしていればよいのですが、迷惑メールの様に増加していく可能性もあります。

この様なアクセスへの対策としては、Windows Messenger サービスを停止することを勧めます。ただし、企業内 LAN 等で使用しているコンピュータの場合は、システム管理者の指示に従って下さい。

(参考情報)

インターネット広告を含む Messenger サービスウィンドウが表示される

<http://support.microsoft.com/kb/330904/ja>

また、Windows Messenger サービスのぜい弱性のセキュリティパッチも発表されていますので、適用されているか確認を行なうこともお勧めします。

(参考情報)

メッセンジャ サービスのバッファオーバーランにより、コードが実行される。(MS03-043)

<http://www.microsoft.com/japan/technet/security/Bulletin/MS03-043.msp>

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/TALOT2-0712.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 / 宮本

Tel:03-5978-7527 Fax:03-5978-7518 E-mail:isec-info@ipa.go.jp