IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
第 07-15-110 号
2007 年 9 月 4 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 8 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 8 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：

「 何かなぁ？ 開いた時には、もう遅い※1 」
― 迷惑メール※2 は、クリックせずにゴミ箱へ！！ ―

※1（情報セキュリティ標語2007 中学生の部 銀賞 千葉県・匝瑳市立八日市場第二中学校 / 伊藤 友美さん）
※2 UBE (Unsolicited Bulk Email) 一般に spam メール(スパムメール)とも呼ばれます。

8 月に IPA へ寄せられた届出や相談の中で、「迷惑メールの中に書いてあるリンク先をクリックしたところ、ウイルス対策ソフトが警告を表示した」など、迷惑メール経由でウイルス感染の被害に遭いそうになったという内容のものが数多くありました。
これらは、ウイルス対策ソフトを装備していたため、感染を免れた例ですが、予防対策をとっていないと警告も出ないため、ウイルスに気付かずに感染してしまうケースが多くあると考えられます。

（1）迷惑メールはどうして届く？

迷惑メールとは、**「受け取る側の意思に関係なく、一方的に送られてくるメール」**のことを言います。ボットなどのウイルスに感染したパソコンから大量に送られて来ることが多くなっています。
送り先メールアドレスをランダムに自動作成するツール等を使い、不特定多数の相手にメールを送る場合もあります。このため、メールアドレスを誰にも知らせていなくても迷惑メールが届いてしまうことになります。

（2）迷惑メールをクリックすると…

迷惑メール経由でウイルス感染する主なケースとしては、以下のようなものがあります。
・中身がウイルスである添付ファイルをクリックして、ウイルス感染
・メールの本文中に書かれているリンク先や、本文中に貼りつけてある画像などをクリックし、ウイルスが埋め込まれているウェブサイトに誘導されて、ウイルス感染
以下に、迷惑メール経由でウイルス感染する事例を紹介します。

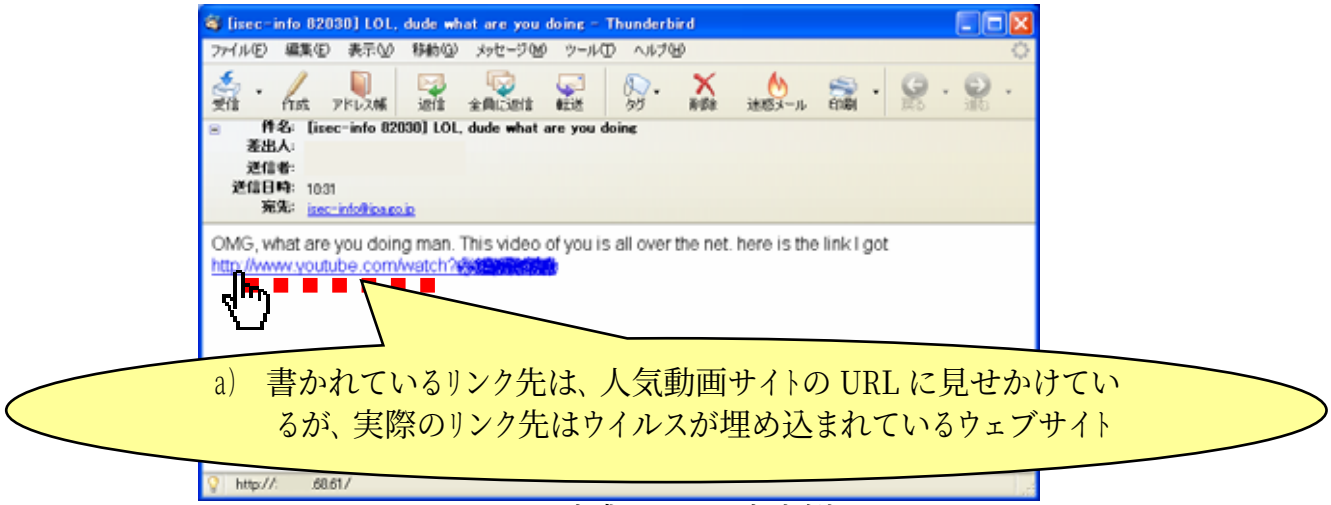


図 1-1 迷惑メールの本文例

図 1-1 は、メールの本文に書かれているリンク先をクリックすることにより、ウイルスが埋め込まれているウェブサイトに誘導されるケースです。

メールの本文（図 1-1 参照）には、**「キミが映っている動画ファイルがネットに流れているよ！ボクが見つけたリンク先はここ」**というような、メールを受け取った人の興味を引くようなことが書いてあり、本文中に書かれているリンク先をクリックさせようとしています。

このリンク先は、見た目には人気動画サイトの URL[a] ですが、このリンク先をクリックすると、人気動画サイトに似せた、実際はまったく違うウェブサイト（図 1-2 参照）に誘導されてしまいます。そこからさらにリンク先[b]を**クリックすることにより、ウイルスがダウンロードされ、警告を無視して実行することでウイルスに感染してしまいます。**

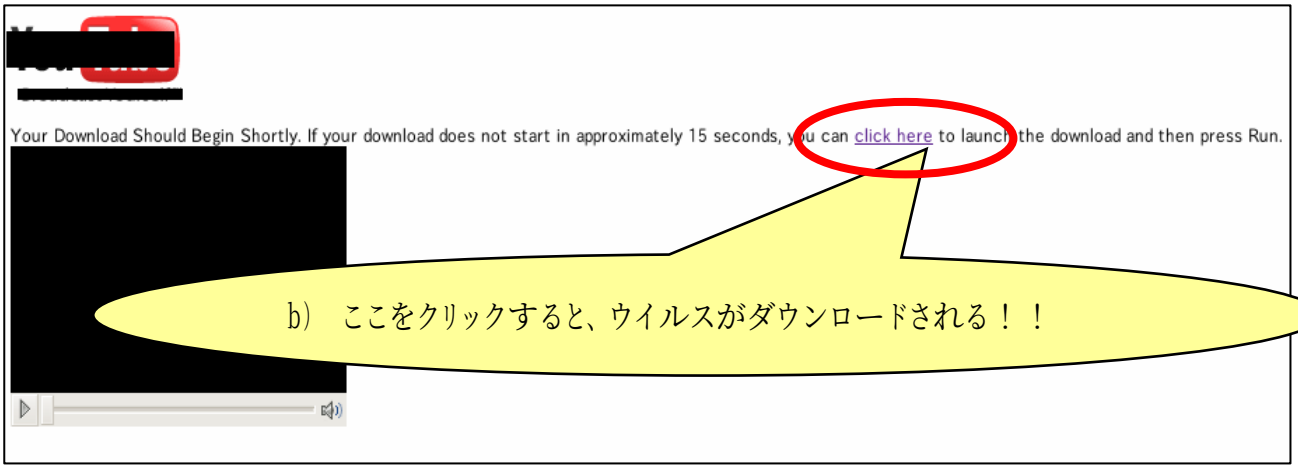


図 1-2 リンク先にある悪意あるウェブサイト

IPA がこのウイルスを入手し解析したところ、ウイルス自身をウイルス対策ソフトに見つからないように隠蔽する機能を有していることを確認しました。このためパソコンがこのウイルスに感染してしまうと、利用者はウイルスに感染したことに気がつかない可能性があります。

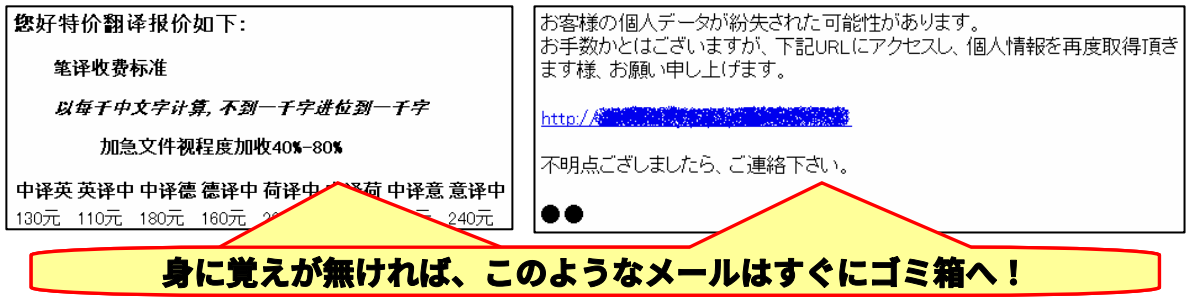
ウイルスがパソコンに感染すると、パソコン内の個人情報が盗まれたり、第三者への迷惑メール送信の踏み台にさせられる等の被害に遭ってしまいます。

（3）迷惑メールへの対処

最近では、インターネット接続サービス業者（プロバイダ）でも、インターネット利用者に迷惑メールが届かないように対策を行なっていますが、完全ではありません。このためどうしても迷惑メールは届くことがあります。

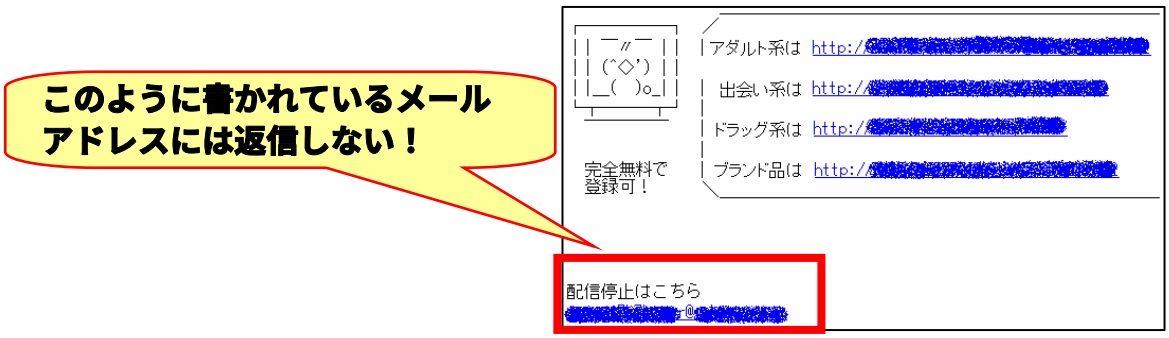
迷惑メールは、相手がメールを開きたくなるような件名や本文を記述したり、添付ファイルを開きたくなるような名前をつけたりして送ってきますので、その誘惑に負けないようにしましょう。
例えば、迷惑メールを開いてしまう理由として、以下のような例が挙げられます。

- **メールのタイトルや文中に、自分の興味を引く内容が書いてあったので、ついメールを開いてしまい、文中に書いてあるリンク先を、興味本位でクリックしてしまった。**
- **送信者の名前が友達と同じだったので、友達からのメールと思い、何の疑いもなく添付されているファイルをクリックしてしまった。**
- **添付されているファイルが何なのか見たくて、ついクリックしてしまった。**



迷惑メールまたは迷惑メールと思われる怪しいメールへの対処は、読まないで開かずにゴミ箱へ捨てる（削除する）ことです。

また、上述したように迷惑メールを送信する側は、相手を特定しないでとにかく大量にメールを送るわけですから、信頼できる相手ではありません。”メール拒否はこちら“や、”配信停止はこちら”などと書かれているメールアドレスには絶対に返信をしないで下さい。返信することにより、こちらのメールアドレスが特定されることになり、さらに迷惑メールが届く可能性があります。



その他の有効な対応策として、使用しているメールソフトについて、電子メールの本文が HTML 形式(Hyper Text Markup Language： ウェブサイトなどの表示形式を利用したメール)の場合、HTML を実行できない設定にする、ウイルスの可能性がある添付ファイルを開かない設定にする等の方法があります。

最後に以下の基本的な対策も忘れずに行ってください。

- ◆ セキュリティホール対策(OS や各種アプリのアップデート)の実施
- ◆ ウイルス対策ソフトのパターンファイルの更新

「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
「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
「IPA -ボット対策について」
http://www.ipa.go.jp/security/antivirus/bot.html
「ワクチンソフトに関する情報」
http://www.ipa.go.jp/security/antivirus/vacc-info.html
「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

「迷惑メール対策」（経済産業省）
http://www.meti.go.jp/policy/consumer/tokusyuu/meiwakumail-main.htm
「迷惑メール情報提供受付」(財団法人　日本産業協会)
http://www.nissankyo.or.jp/spam/index.html
「迷惑メール相談センター」（財団法人　日本データ通信協会）
http://www.dekyo.or.jp/soudan/index.html

2．IPA で行っているウイルス対策の取り組みに関連した情報の紹介

1）情報漏えい発生時の対応ポイント集

-情報が漏えいしてしまった時、何をすべきか!! -

本小冊子は、情報漏えいインシデント対応マニュアルを整備していない中小企業などにおいて、情報漏えい事故が発生した場合、何をする必要があるか、何に気をつけなければいけないかを経営者をはじめとする対応チームの方々が短時間に理解し、速やかに適切な対応ができるように分かりやすく解説しています。

URL　http://www.ipa.go.jp/security/awareness/johorouei/

2）2006 年 国内における情報セキュリティ事象被害状況調査報告書

本調査は、最新の情報セキュリティ関連の被害実態及び対策の実施状況を把握するため、企業･自治体を対象に郵送によるアンケート調査を行い、その結果を公開しています。

URL　http://www.ipa.go.jp/security/fy18/reports/virus-survey/press.html

3）情報セキュリティに関する新たな脅威に対する意識調査(2006 年度第 2 回)

近年、コンピュータウイルスだけでなく、フィッシング詐欺やスパイウェア、ボット等、新たな脅威が出現し、被害を生じさせています。このような状況を受け、PC インターネット利用者へのウェブアンケートを通じて、新たな脅威に対する認知度、理解度、対策の実施状況等の実態を調査し、その結果を公開しています。

URL　http://www.ipa.go.jp/security/fy18/reports/ishiki02/index.html

4）ZHA(Zero Hour Analysis)に基づくウイルス情報 iPedia

収集したウイルス検体について挙動分析を行い、その概要を“ウイルス情報 iPedia”として広く一般に公開しています。

URL　https://isec.ipa.go.jp/zha-virusdb/web/Top.php

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「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た

･オンラインゲーム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）

･メールの本文にあったリンクをクリックしたら、ウイルス警告が！

○ 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。

･Trend Micro 社サーバ版ウイルス対策ソフトのぜい弱性を狙ったアクセスが、一時的に増加！

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 49 万個**と、7 月の 51 万個から 4.3%の減少となりました。
また、8 月の届出件数(※2)は、**2,806 件**となり、7 月の 3,069 件から 8.6%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。
・8 月は、寄せられたウイルス検出数約 49 万個を集約した結果、2,806 件の届出件数となっています。

検出数の1位は、**W32/Netsky** で**約 42 万個 、2 位は W32/Zhelatin** で**約 3 万個、3 位は W32/Mytob** で**約 2 万個でした。**

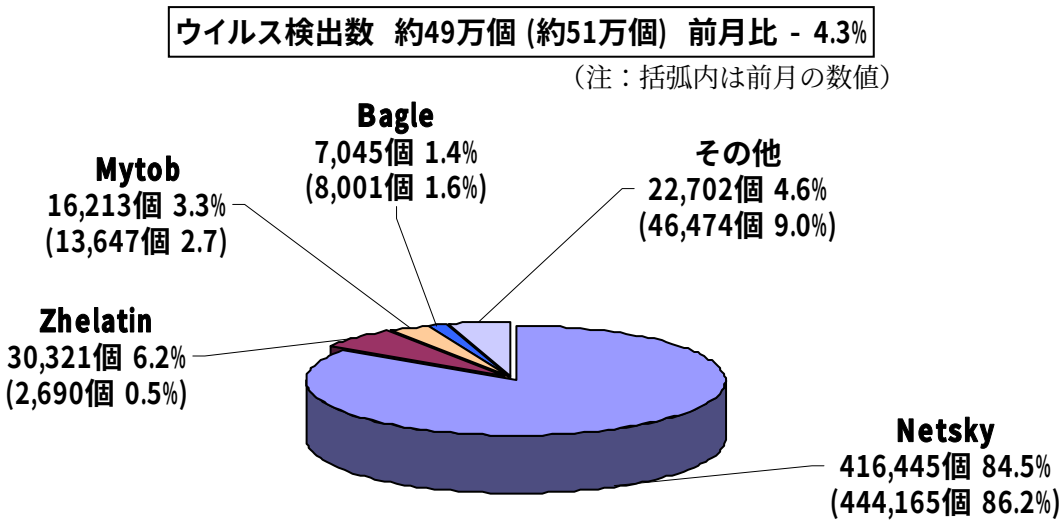


図 3-1

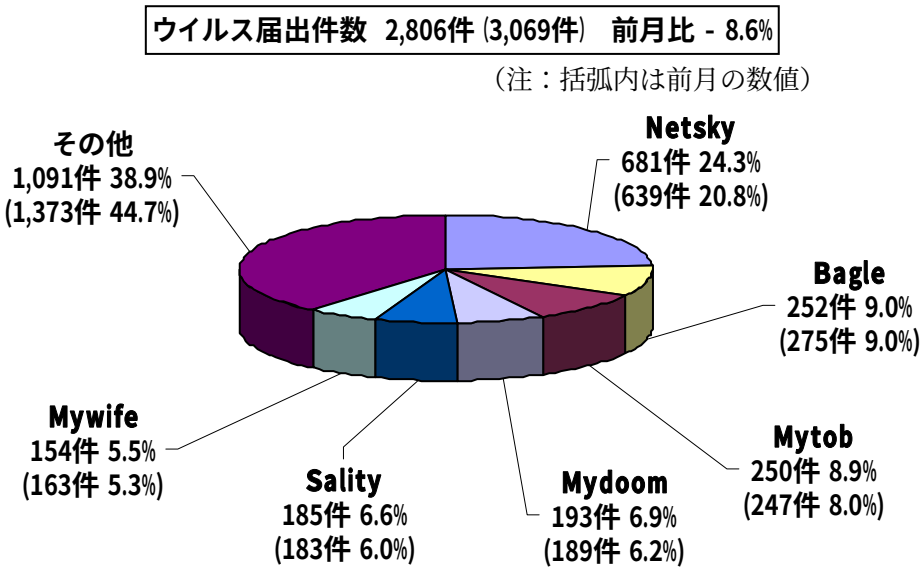


図 3-2

(参考)

本年1月以降から届出されている検出数が減少していますが、考えられる理由としては、昨年12月より開始された総務省／経済産業省の合同プロジェクトである「ボット対策事業*1)」の活動が多少影響しているのではないかと考えられます。

それは、このプロジェクトは、現在社会に対してウイルスを大量に感染させている原因のひとつである「ボット」を撲滅することを目的としているため、その効果が表れてきたからだと考えられます。

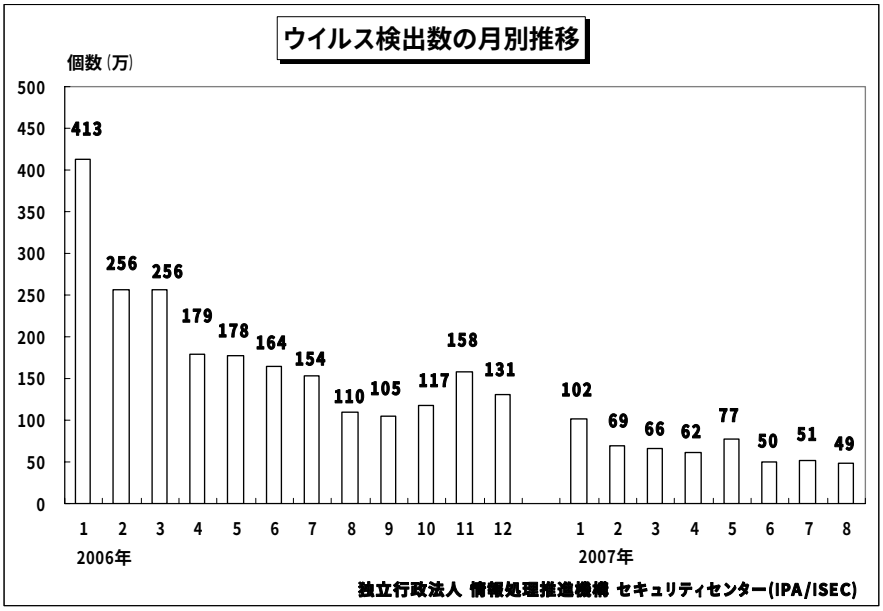


図 3-3:ウイルス検出数の月別推移

*1)ボット対策事業

サイバークリーンセンター (https://www.ccc.go.jp/) は、総務省と経済産業省の合同プロジェクトであるボット対策事業を運営しています。インターネットにおける脅威となっているボットの特徴を解析するとともに、ユーザのコンピュータからボットを駆除するために必要な情報をユーザに提供する活動を行っています。

具体的には、ボット感染ユーザへ個別のメールによる注意喚起を行い、サイバークリーンセンターのサイトに駆除手順の説明ページを設け、併せて、感染したボットに対応した駆除ツールのダウンロード提供を行っています。

IPA は、サイバークリーンセンターに「ボット感染予防推進グループ」として参加しており、セキュリティベンダと連携して広く一般ユーザにおけるボット感染予防策の強化及び再発防止に取り組んでいます。本プロジェクトにて収集したボットを、セキュリティベンダに対して検体として提供し、各社の対策ソフトのパターンファイルへの反映を促進しています。これにより、対策ソフトのパターンファイルを最新のものに更新すれば、対策ソフトは本プロジェクトで収集したボットを検出することができるようになり、感染予防の向上を図ることができます。

活動実績

7月の活動実績は、以下の通りです。

- 注意喚起をした感染ユーザ数
  7月　8,681 人、活動開始(2006 年 12 月 15 日)からの累計 27,329 人

- 一般公開サイトからの駆除ツールダウンロード総数
  7月　32,788 回、活動開始からの累計 164,561 回

- 本プロジェクトにて収集した検体数
  7月　13,437 個、活動開始からの累計 83,240 個

本プロジェクトにて収集され、参加しているセキュリティベンダに提供された検体のパターンファイルへの反映率は、参加ベンダ平均で、98.7%となっています。

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

		3月	4月	5月	6月	7月	8月
届出(a) 計		**13**	**15**	**19**	**41**	**10**	**16**
	被害あり(b)	9	12	13	36	8	13
	被害なし(c)	4	3	6	5	2	3
相談(d) 計		**43**	**31**	**37**	**27**	**25**	**23**
	被害あり(e)	20	20	21	11	11	15
	被害なし(f)	23	11	16	16	14	8
合計(a+d)		**56**	**46**	**56**	**68**	**35**	**39**
	被害あり(b+e)	29	32	34	47	19	28
	被害なし(c+f)	27	14	22	21	16	11

（1）不正アクセス届出状況

8 月の届出件数は 16 件であり、そのうち**被害のあった件数は 13 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 23 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 15 件でした。

（3）被害状況

被害届出の内訳は、**侵入 9 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 8 件、などでした。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 6 件などでした。

※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。
※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。
※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	･IDS※が、組織外部への SSH スキャンのアクセスを検知した。 ･調査したところ、組織内のあるサーバが SSH で不正にログインされ、SSH スキャンツールを埋め込まれていたことが判明。 ･外部からの **SSH 接続は公開鍵認証※方式**としていたが、**パスワード認証方式も有効になっていた**。
解説・対策	**IDS が有効に活用されている例**と言えます。残念ながら侵入を防ぐことはできませんでしたが、**問題の早期発見により被害の拡大が防ぐことができました**。この事例では、セキュリティ強化のために**公開鍵認証方式を採用していましたが、同時にパスワード認証も有効になっていた**のに気付きませんでした。さらに**推測が容易なパスワードを使用していたアカウント※があった**ため、パスワードクラッキング攻撃でパスワードが破られてしまっていました。**SSH を使用している場合は、認証の方式について、再度確認しましょう**。 (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

※IDS (Intrusion Detection System)…システムに対する侵入／侵害を検出･通知するシステムのこと。
※公開鍵認証…秘密鍵と公開鍵との鍵のペアを使用して、暗号化と復号を行う方式のこと。
※アカウント (account)…コンピュータやネットワーク上の資源を利用出来る権利のこと。

[その他（被害あり）]

(ii) オンラインゲームのアカウントが誰かに乗っ取られた

事例	･いつもプレイしていたオンラインゲームの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」とエラーが出て、ログインできなくなっていた。 ･ゲーム管理者に連絡してパスワードを再発行してもらい、ログインしてみたが、所持していたゲームのアイテムが全て無くなっていた。 ･ゲーム管理者に調査を依頼したところ、何者かが本人に成りすましてログインしていた形跡があったことが判明。なぜパスワードが破られたのかは不明。
解説・対策	人気のあるオンラインゲームでは、アイテム欲しさに、悪意のあるユーザが他人のアカウントを狙う事件が時折発生しています。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。 最近は、ウイルスに感染したために、パスワード情報が外部に漏れてしまった事例もあります。この場合、**パーソナルファイアウォールなどのソフトを導入し、自分で許可したプログラムしかインターネットに接続しないように設定しておく**ことで、万が一ウイルスが仕込まれてしまったとしても、パスワードなどの重要情報が外部に送信されることを予防することが出来ます。 (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

8 月の相談総件数は **1,013 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 **330 件**（7 月：316 件）と、今までで最高の件数を更新しました。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 **13 件**（7 月：16 件）、**Winny に関連する相談**が **6 件**（7 月：19 件）などでした。

IPA で受け付けた全ての相談件数の推移

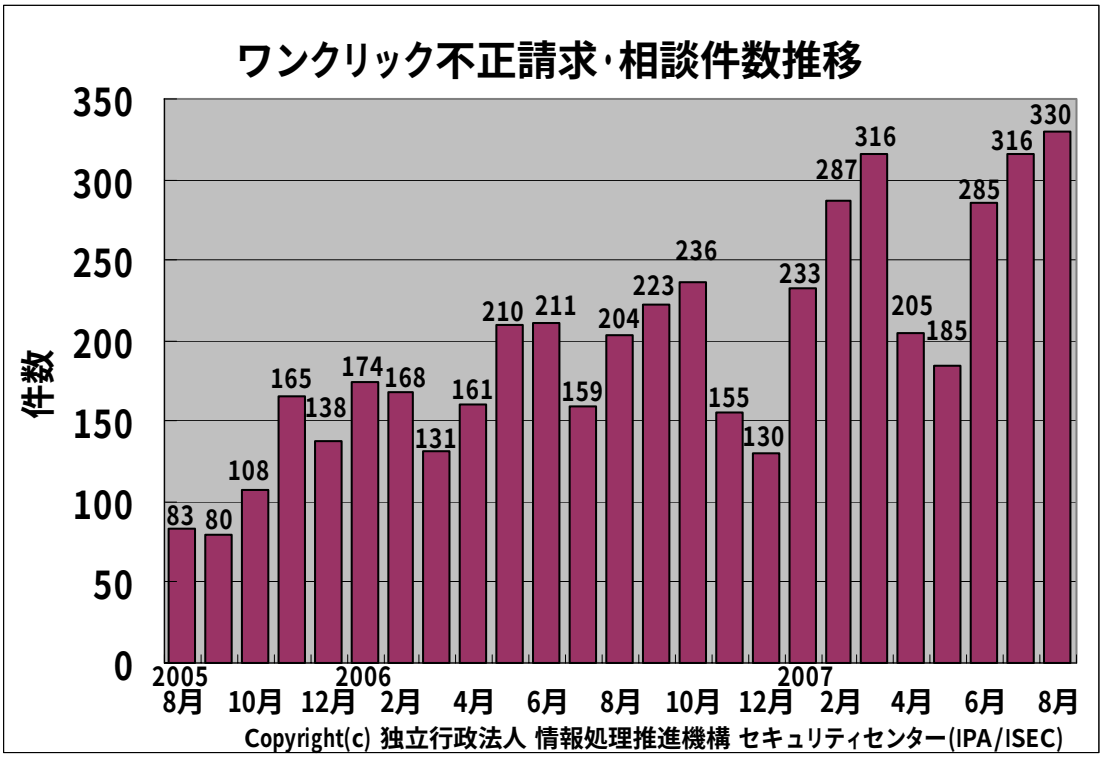
	3月	4月	5月	6月	7月	8月
合計	**1127**	**827**	**814**	**932**	**1162**	**1013**
自動応答システム	697	486	484	537	694	593
電話	376	279	254	339	402	374
電子メール	54	58	69	53	65	43
その他	0	4	7	3	1	3

※ 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



主な相談事例は以下の通りです。

(i) メールの本文にあったリンクをクリックしたら、ウイルス警告が！

相談	身に覚えの無いメールが届いた。ある会員制サイトからのもののようで、「あなたのログイン情報が 24 時間で無効になるので、更新してください」というメールであった。そのメール本文内に書かれていたリンクをクリックしたら、ウイルス対策ソフトがウイルスを検知した。 +-----受信メール例-----+ "MP3 World" <*****@***.***.**> 送信者: User ***** <*****@***.**.**.*****.net> 2007/08/22 08:03 Greetings, We are so happy you joined MP3 World. Member Number: 272761797951 Your Login ID: user6104 Password ID: du556 Your temporary Login Info will expire in 24 hours. Please login and change it. Use this link to change your Login info: **http://***.***.193.70/** Enjoy, New Member Services MP3 World
回答	リンク先のサイトにウイルスが仕込まれている場合があります。**見知らぬ人からのメールや迷惑メールなどの本文中にあるリンクは、不用意にクリックしてはいけません**。Windows やウイルス対策ソフトを最新の状態にしていない場合、クリックしただけで、ウイルス感染してしまうこともあります。 （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

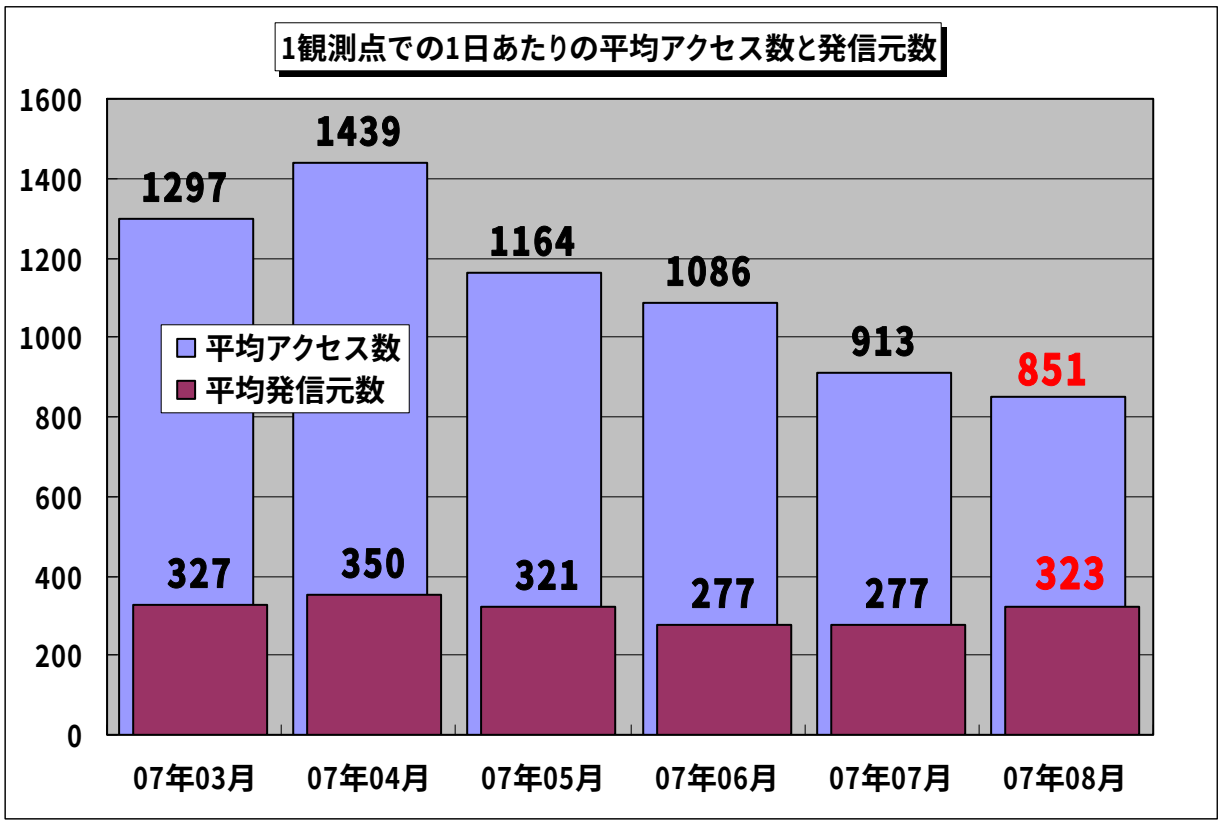
(ii) もらったファイルを開いても良いか？

相談	友人から譲り受けた CD-ROM の中に、大量のファイルが入っている。念のため、ウイルス対策ソフトでチェックしてみたが、ウイルスなどは何も検出されなかった。この場合、ファイルを開いていっても本当に大丈夫か？
回答	その友人が、どこからファイルを入手したのかが問題です。**出所の不明なファイルを開くことは、ウイルス対策の観点で見れば最も危険な行為**と言えます。ウイルスに感染したくないのであれば、不用意にファイルを開くことは止めましょう。何か問題が発生してからでは、取り返しがつきません。 なお、ウイルス対策ソフトでも検知できないウイルスも存在します。**出所不明なファイルは、ウイルスチェックするまでもなく、削除するのが賢明**です。 （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

6．インターネット定点観測での 8 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 8 月の期待しない（一方的な）アクセスの総数は、10 観測点で **263,940 件**ありました。1 観測点で 1 日あたり **323** の発信元から **851 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、323 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。



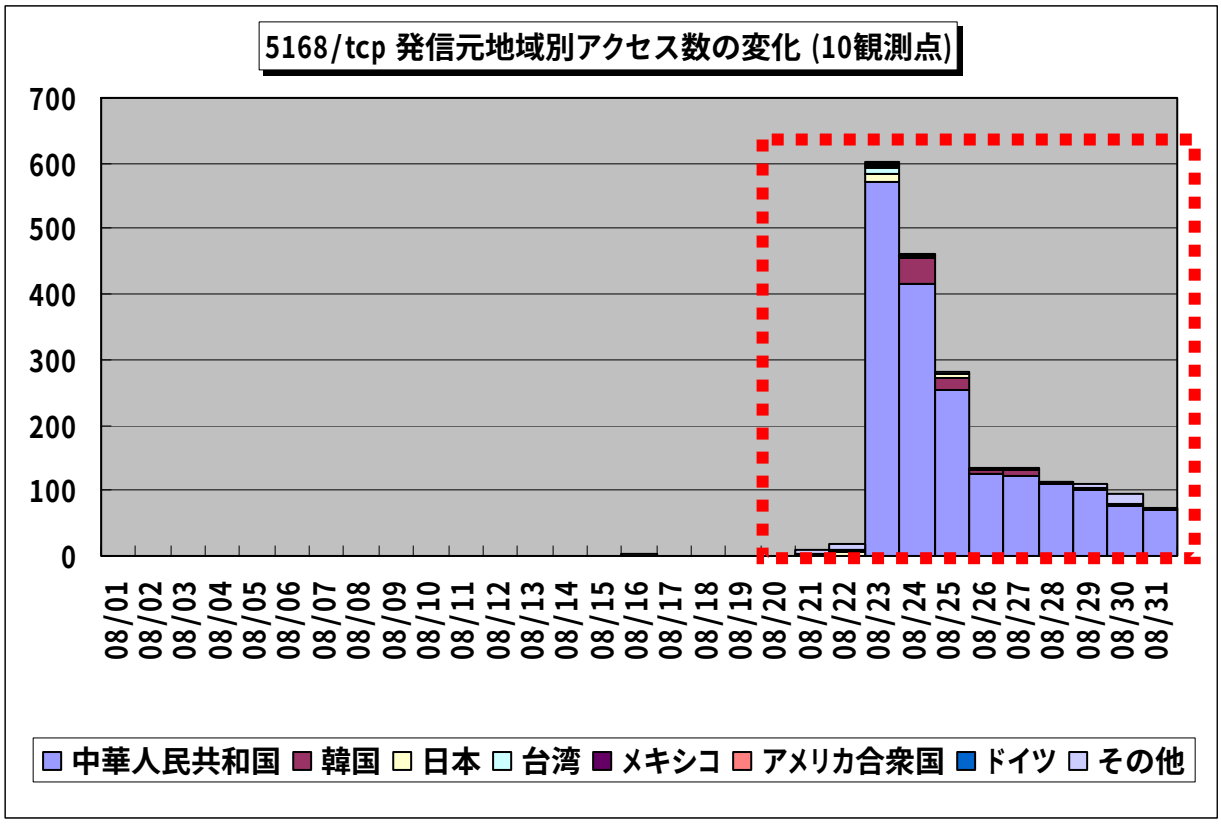
【図 6-1　1 観測点での 1 日あたりの期待しない(一方的な)アクセス数および発信元数】

2007 年 3 月～2007 年 8 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ります。

2007 年 8 月のアクセス状況は、全体的に 7 月と同じで定常化していると言えます。その中において、Windows Messenger サービスを悪用してポップアップメッセージを送信する、1026/udp、1027/udp、1028/udp のアクセス合計数が、全体のアクセスの 4 分の 1 を占めました。また Trend Micro 社の、サーバ版ウイルス対策ソフトの脆弱性を狙ったと思われるアクセスが、一時的に多くありました。

(1) トレンドマイクロ社サーバ版ウイルス対策ソフトのぜい弱性を狙ったアクセス

トレンドマイクロ社から、サーバ版ウイルス対策ソフトのセキュリティパッチが発表された頃から、このソフトが管理用として使用する、5168/tcp ポートのアクセスが一時的に増加しました。



【図 6-2 2007 年 8 月の 5168/tcp ポートへの発信元地域別アクセス数の変化】

これは、トレンドマイクロ社のサーバ版ウイルス対策ソフトの脆弱性を狙ったアクセスと思われますが、現在は収まった感じに見受けられます。

しかしながら、この様な脆弱性情報が出されると、忘れた頃にまた同じ脆弱性を狙った攻撃が起こりますので、該当ソフトウェアをお使いの方は、以下の参考情報より早めの対応を行うことをお勧めします。

なお、該当ソフトウェアはサーバで使用するソフトウェアですので、対応にはシステム管理者の指示に従って下さい。

(参考情報)

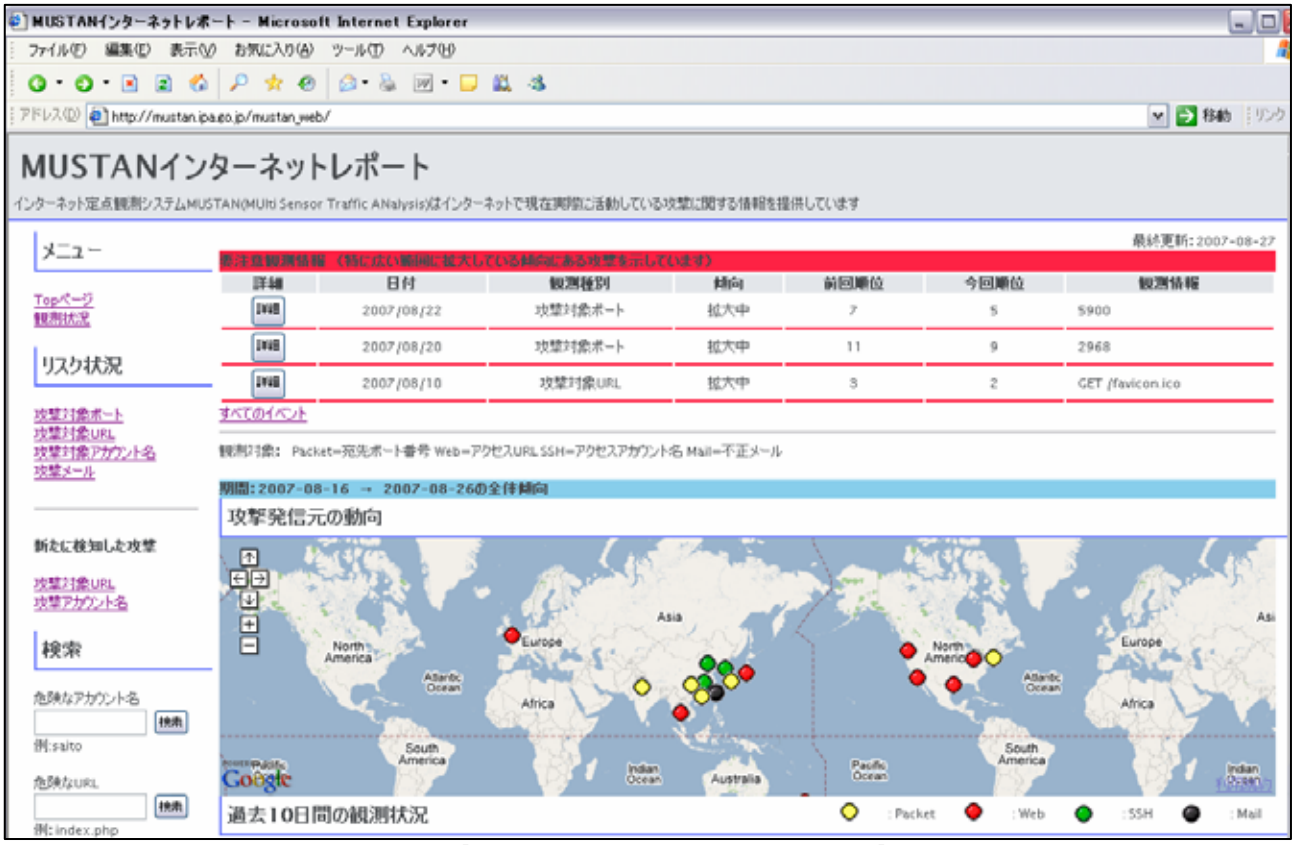
- ServerProtect for Windows/NetWare 5.58 用 Security Patch 2(Build_1185)適用のお願い (Trend Micro 社)
  http://www.trendmicro.co.jp/support/news.asp?id=1003
- TCP 5168 番ポートへのスキャン増加に関する注意喚起 (JPCERT/CC)
  http://www.jpcert.or.jp/at/2007/at070019.txt
- JVNTA07-235A Trend Micro ServerProtect に複数の脆弱性
  http://jvn.jp/cert/JVNTA07-235A/

(2) インターネット定点観測システム MUSTAN(Multi Sensor Traffic Analysis) について

MUSTAN は、インターネットで現在実際に活動している攻撃に関する情報を提供しています。実際に広範囲に流行しており、ネットワークユーザが特に注意すべき

- ◆ 新しい
- ◆ 活発な
- ◆ 活発化している

不正アクセスを自動的に検知･報告するシステムとして運用しています。



【図 6-3 MUSTAN TOP ページ】

● 機能概要

定点観測システム MUSTAN は、インターネット上に配置されたセンサによってインターネットに広がっている攻撃を監視しています。監視対象は以下の 4 つです。

- ポートへの不正なアクセス
- HTTP による不正なウェブアクセス
- SSH アカウントへの不正なログインの試み
- 不正なメール

観測された情報を分析し、発信元の数の増加をいち早く検知することで、流行の広がりを確認できます。

合わせて、過去 10 日間の攻撃発信元の動向や、各攻撃の状況が確認できます。

(1) 要注意観測状況

要注意情報では、観測対象不正アクセスの発信元を分析し、その数が特に**大きな増加傾向**を示しているものを抽出しています。ここに警告されている不正アクセスは、当該ポート、関連する URL について、**自サイトでの利用状況**を特に注意する必要があります。

[詳細]ボタンから、その不正アクセスの数、発信元の広がり状況を確認することができます。

(2) リスク状況

リスク状況は、要注意ほどの緊急度ではありませんが、上昇傾向にある不正アクセス、および新規に観測された不正アクセスを示しています [地図]ボタンから、発信元の広がり状況を確認することができます。

(3) 新しいウェブ攻撃

新規に観測されたウェブアクセスの状況を示しています。**ウェブアプリケーションに対する新たな攻撃のバリエーション**などを示しています。 この情報から自サイトで利用しているウェブアプリケーションの URL などを確認することで、関連するウェブアプリケーションの攻撃の有無を検索できます。

(4) 新しい攻撃アカウント

新規に観測された攻撃に利用された SSH アカウントを示しています。自サイトで利用している SSH 用アカウント名などを入力することで、関連の攻撃の有無を検索できます。

(5) 検索機能

MUSTAN が観測した攻撃に使用されている SSH アカウント名、ウェブアプリケーションの URL、ポート番号が検索出来ます。

(6) 要注意情報の XML 出力

MUSTANが観測、解析し、特に広い範囲に拡大している傾向にある攻撃の情報をXMLファイルとして取得できます。

IPAでは、本システムを6/29より運用を開始しています。インターネット上で発生している不正アクセスの状況を把握するために、ご利用下さい。

http://mustan.ipa.go.jp/mustan_web/

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/TALOT2-0709.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