IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2006 年 2 月 3 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［2006 年 1 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、2006 年 1 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。

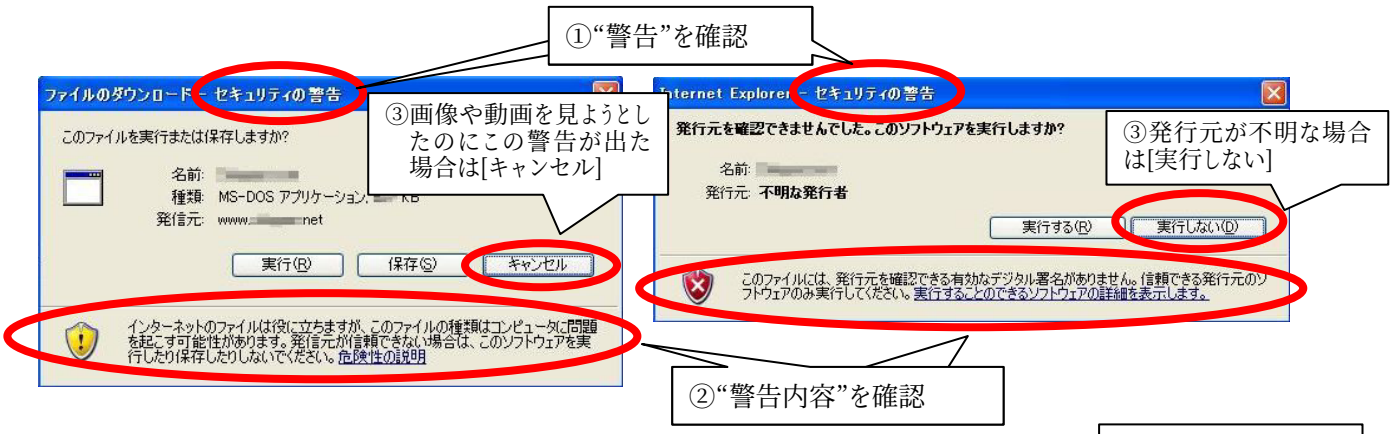
今月の呼びかけ：
「警告を無視すると不正プログラムがインストールされる？！」
―― 警告画面を軽視していませんか？ ――

最近、ホームページを閲覧していて、ブログや掲示板サイトに書き込まれているリンクや画像をクリックすることで、不正なプログラムをインストールされてしまったり、メールの添付ファイルを開いてウイルスに感染してしまったりという被害の相談事例が多く見受けられます。また、ウイルス対策ソフトやパーソナルファイアウォールソフトを導入していても、ウイルス感染や情報漏えいが起きるといった被害が後を絶ちません。

IPA に多く寄せられる相談として「ワンクリック不正請求」がありましたが、こうした事例を分析した結果、被害発生の過程においては何らかの“警告画面”が表示されていることが分かりました。つまり、利用者がその“警告”を軽視してしまったために被害に遭っていると推測されます。

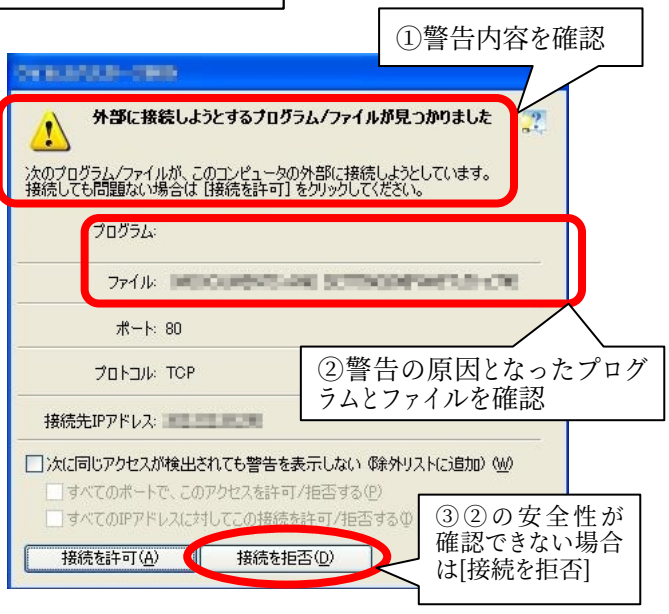
＜ウイルスやスパイウェアが埋め込まれる際の警告＞

画像や動画だと思ってファイルを開こうとした際に、次のような警告が出た場合は要注意です。この“セキュリティの警告”は、OS（Windows XP）がシステム保護のために発しているメッセージです。少しでも怪しいと思ったら、**ファイルの“種類”**や**ファイルの“発行元”**情報をチェックし、**安全が確認された場合以外は［実行］や［実行する］をクリックしてはいけません**。



＜不正アクセスの警告＞

特に通信操作をしていないような場面で、右図のような警告が出た場合には要注意です。この警告は、パーソナルファイアウォールソフトが発しているメッセージです。既に侵入済みのウイルスやスパイウェアが、パソコン外に情報を流出させようとしている可能性があります。このような問い合わせ画面が出て来た時は、プログラム名やファイル名をチェックし、本当に安全だと確認出来る時以外は［接続を許可］をクリックしてはいけません。



（ご参考）
IPA - 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
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
IPA - 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

1．コンピュータウイルス届出状況　－詳細は別紙 1 を参照－

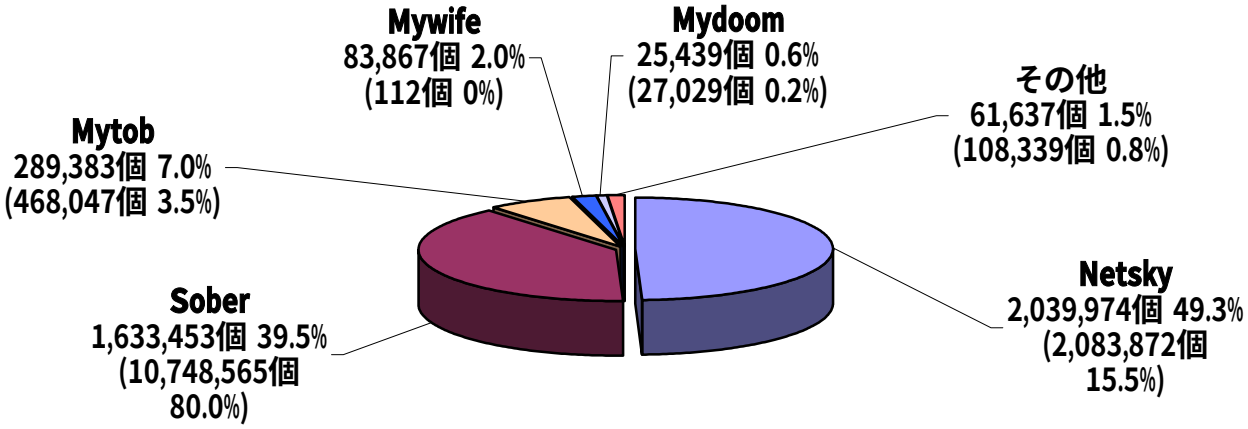
ウイルスの検出数(※1)は、**約 413 万個**と、12 月の約 1,344 万個から約 7 割の減少となりました。12 月に**大量のウイルスメールを送信して、全検出数を増加させた W32/Sober の特定亜種でした。当該亜種がメール送信活動を停止**したことにより、大幅な減少となりました。（＊W32/Sober の検出数は 12 月約 1,075 万個 から 1 月約 163 万個と約 85%の減少）
また、1 月の届出件数(※2)は、**4,499 件**となり、12 月の 4,293 件から 4.8%の増加となりました。

※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。
・1 月は、寄せられたウイルス検出数約 413 万個を集約した結果、4,499 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky で約 204 万個 、2 位は W32/Sober で約 163 万個、3 位は W32/Mytob で約 29 万個でした。**

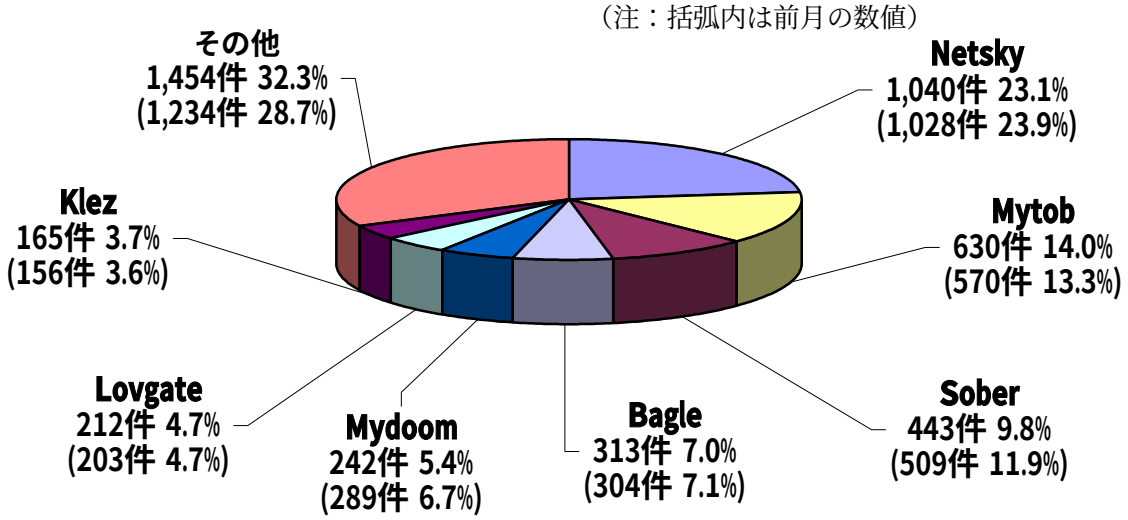
ウイルス検出数　413万個(1,344万個)　前月比 - 69.2%

（注：括弧内は前月の数値）



ウイルス届出件数　4,499件（4,293件）　前月比 + 4.8%

（注：括弧内は前月の数値）



2．スパイウェアについて

アダルトサイトで画像をクリックしただけでスパイウェア(*1)がインストールされ、普段使用しているメールアドレスが抜き取られるといった相談事例が昨年から増加しています。アドレスが盗まれた結果、不正な請求書がメールで送られてくるといった被害が発生しています。

以下に掲げる対策を実施すると共に、安易にダウンロードしない等の注意を払い、被害に遭わないようご注意ください。

(1) スパイウェア対策ソフトを利用し、定期的な定義ファイルの更新およびスパイウェア検査を行う
(2) コンピュータを常に最新の状態にしておく
(3) 怪しいサイトや不審なメールに注意する
(4) コンピュータのセキュリティを強化する
(5) 万が一のために、必要なファイルのバックアップを取る

スパイウェア対策のしおり
http://www.ipa.go.jp/security/antivirus/shiori.html

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

		8月	9月	10月	11月	12月	1月
届出(a) 計		**41**	**31**	**22**	**24**	**25**	**50**
	被害あり(b)	12	16	15	15	19	13
	被害なし(c)	29	15	7	9	6	37
相談(d) 計		**43**	**30**	**35**	**30**	**25**	**43**
	被害あり(e)	23	16	25	18	15	23
	被害なし(f)	20	14	10	12	10	20
合計(a+d)		**84**	**61**	**57**	**54**	**50**	**93**
	被害あり(b+e)	35	32	40	33	34	36
	被害なし(c+f)	49	29	17	21	16	57

(1) 不正アクセス届出状況

1 月の届出件数は 50 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 43 件（うち 6 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 23 件でした。

（3）被害状況

被害届出の内訳は、**侵入 11 件、その他(被害あり)2 件**でした。

侵入届出のうち、SSH(*2)で使用するポート(*3)への攻撃を受けた結果侵入されたという届出が 3 件、Web サーバに侵入されてフィッシングに悪用するための Web コンテンツを設置された届出が 2 件、XML-RPC(*4)の PHP(*5)実装ライブラリの脆弱性を突かれて侵入されたという届出が 2 件ありました。

被害事例

[侵入]

（i） SSH(*2)で使用するポートへの攻撃

事例	・ネットワーク監視装置が、内部サーバから外部ネットワークに向けての頻繁な SSH アクセス試行を検知した。 ・当該サーバのログ(*6)を確認したところ、外部のサーバに対して不正な SSH 接続を試みていた（外部サイト攻撃のための踏み台にされていた）。 ・使用されていないテスト用アカウント(*7)が残っていた。そのアカウントのパスワードが脆弱であったため、破られて侵入されてしまった。
解説・対策	テスト用とは言え、安易なパスワードを付与すると比較的容易にパスワードが破られてしまう恐れがあります。このケースでは特に、**用が済んだテスト用アカウントを放置してしまったために管理の目が行き届かず、攻撃の標的として狙われた**ものと思われます。管理者は、アカウントの登録状況をしっかりと監視する必要があります。しかしながら、ネットワーク監視装置の導入によって、被害を最小限に食い止めることができています。**SSH 運用時には、ログインの際に公開鍵認証(*8)などの強固な認証を採用することを推奨します**。 （ご参考） IPA - セキュアな Web サーバの構築と運用 ～ ユーザ認証 http://www.ipa.go.jp/security/awareness/administrator/secure-web/chap6/6_userauth-1.html

(ii) フィッシング詐欺に使用されるコンテンツ設置および個人情報の流出

事例	・自社の Web サイトにアクセスすると、本来のページではなく、某有名ショッピングサイトを模した偽のページが表示されることを確認（外部から通報あり）。 ・当該の偽ページ（フィッシング詐欺に悪用することを目的としたと考えられる）データは、自社の Web サーバ上に置かれていた。さらに、パスワードが勝手に変更されていて、サーバ管理者はサーバにログインできなかった。 ・ファイアウォールを設置しておらず、かつソフトウェアを最新の状態にしていなかったのが原因と思われた。 ・侵入されたサーバには個人情報が保存されていたため、これらの情報が外部に流出した可能性もある。
解説・対策	フィッシング詐欺に悪用するための偽コンテンツデータを Web サーバに設置されていました。侵入された原因は、セキュリティホールを解消せずに放置していたことのようです。被害に遭わないためにも**日頃から脆弱性情報に気を配り、セキュリティパッチをタイムリーに適用していくことが、最も基本的かつ重要な対策となります**。さらにこの事例では、たまたまサーバ内に個人情報が保管されていたため、それらの流出や二次被害にまで頭を悩ませることになってしまいました。**重要な情報の保管場所やセキュリティ対策内容について改めて確認しましょう**。 （ご参考） IPA - 安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/20060131_websecurity.html

(iii) XML-RPC(*4)の脆弱性を突かれた侵入

事例	・Web サーバに侵入され、ホームページを改ざんされていた（外部から通報あり）。 ・Web サーバに組み込んでいた PHP(*5)用ライブラリ中の「XML-RPC の脆弱性」を突かれたのが原因。 ・問題となったライブラリは、使用されていなかった。
解説・対策	**システム運用上、必要の無いファイルがサーバ内に存在し、かつそのファイルに脆弱性が存在していた**ため、虚を衝かれた格好になったと思われます。**不要なファイルはサーバ内に置かない、不要なサービスは停止する、などといった基本的な対策が重要です。** （ご参考） IPA - 安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/20060131_websecurity.html 高度なセキュリティ対策を施していても、一箇所、弱い部分があるとそこから侵入されてしまいます。**抜けの無いセキュリティ対策とするためにも、セキュリティ監査など、第三者によるチェックを受けるなどの措置が有効です**。 （ご参考） 経済産業省 - 情報セキュリティ監査企業台帳 http://www.meti.go.jp/policy/netsecurity/is-kansa/

4．相談受付状況

1 月の相談件数は、**748 件**でした。そのうち、アダルトサイトを閲覧した後に「振り込め詐欺」のメールを送りつけられるなど、いわゆる**『ワンクリック不正請求』に関する相談**は相変わらず非常に多く、**173 件**もありました。また、ワンクリック不正請求に関する相談のうち **9 割近くが、スパイウェアなどの不正なプログラムを埋め込まれたケース**となっています。＜ワンクリック不正請求相談件数推移…7 月：28 件、8 月：83 件、9 月：80 件、10 月：108 件、11 月：165 件、12 月：138 件＞。

IPA で受け付けた全ての相談件数の推移

		8月	9月	10月	11月	12月	1月
合計		**629**	**554**	**606**	**673**	**653**	**748**
	自動応答システム	376	337	357	379	391	425
	電話	179	144	165	220	194	228
	電子メール	67	72	82	66	66	87
	FAX・他	7	1	2	8	2	8

※ IPA では、コンピュータウイルス・不正アクセス、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）
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。

主な相談事例は以下の通りです。

（i）賞金が当たったとのメールが・・

相談	突然、「100万円当選しました」というメールが届いた。空メールを送ると返信メールが届くので、そこに必要事項を記入し再度送信すれば100万円が振り込まれるというシステムとのこと。銀行口座番号を入れてメールを送ったがいまだ100万は振り込まれず、当選のお知らせメールだけが毎日のように届く。
回答	単なる偽の懸賞の当選メールであり、**氏名や銀行口座番号などを詐取するためのフィッシング詐欺の一種**であると思われます。身に覚えの無い怪しいメールの内容は安易に信じることはせず、**“罠かもしれない”と常に疑って掛かる必要があります**。特に、個人情報を入力するような場面では、注意が必要です。

(ii)ウイルス感染で個人情報が流出した・・

相談	Winny を使っていて、ウイルスに感染した。ウイルスによって、自分の住所や名前を始めとしたプライベート情報が流出してしまった。どうすればよいか。
回答	**ファイル交換ネットワークに流出してしまったデータの回収は、事実上不可能**と言えます。ファイル交換ソフトを使用するにあたっては、こうした危険と隣り合わせであることを再度認識し、**ウイルス対策ソフトを導入するなど、セキュリティ対策を万全にしましょう**。 (ご参考) IPA - ファイル交換ソフト使用上の注意事項 http://www.ipa.go.jp/security/topics/20050623_exchange.html

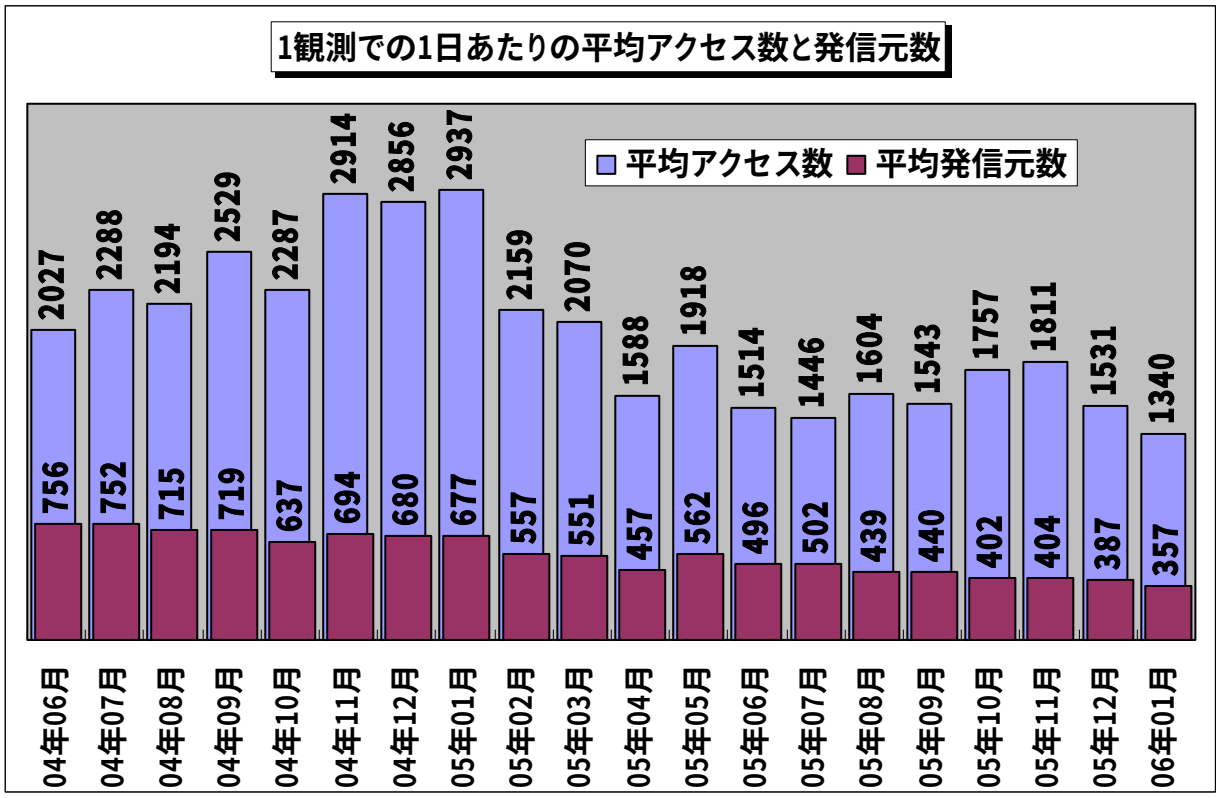
なお、依然として多数の相談件数を占めるワンクリック不正請求に関する対策情報は、以下のサイトに掲載しておりますので、ご参照ください。

IPA - 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

5．インターネット定点観測での１月のアクセス状況

インターネット定点観測(TALOT2)によると、2006 年 1 月の期待しない（一方的な）アクセスの総数は、10 観測点で **415,438 件**ありました。1 観測点で 1 日あたり **357** の発信元から **1,340 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、357 人の見知らぬ人(発信元)から、発信元一人当たり 4 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】

2004 年 6 月～2006 年 1 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 1 に示しています。この図を見ると、期待しない（一方的な）アクセスは、発信元数も含めて、緩やかに減少傾向にあるようです。

1 月のアクセス状況は、あいかわらず、Windows の脆弱性を狙っていると思われる不正なアクセスが多いようです。特にアクセス数の多い 135(TCP)ポート,445(TCP)ポートへのアクセスは、Windows の脆弱性を狙っています。また、最近は、ウイルス対策や不正アクセス対策を勧めるポップアップメッセージやネットサーフィン時のアドウェアによるポップアップ広告等も多いので、これらの内容に騙されないように注意して下さい。

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/2006/documents/TALOT2-0602.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/jp/default.asp

『用語の解説』

(*1) スパイウェア（spyware）
利用者の個人情報やアクセス履歴などの情報を詐取し、利用者以外のものに自動的に送信するソフトウェア。

(*2) SSH (Secure SHell)
ネットワークを介して別のコンピュータにログインしたり、遠隔地のマシンでコマンドを実行したり、他のマシンへファイルを移動したりするために使うプロトコルもしくはプログラムのこと。ネットワーク上を流れるデータは暗号化されるため、インターネット経由でも一連の操作を安全に行なうことができる。

(*3) 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。

(*4) XML-RPC（eXtensible Markup Language - Remote Procedure Call）
XML を利用してインターネット上で RPC を実行するためのプロトコル。RPC とは、ネットワーク上のコンピュータを利用してプログラムを処理させる手続きのこと。

(*5) PHP（PHP: Hypertext Preprocessor）
動的な Web ページの生成に適した、汎用のスクリプト言語のこと。HTML 記述内に埋め込むことができる。

(*6) ログ（log）
コンピュータの利用状況やデータ通信の記録のこと。一般的に、操作を行った者の ID や操作日時、操作内容などが記録される。

(*7) 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、または利用する際に必要な ID のこと。

(*8)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。

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

お知らせ

『情報セキュリティ対策ベンチマークシステム』の紹介

IPA では、**「情報セキュリティ対策ベンチマークシステム」**を Web サイト上に公開しております。
情報セキュリティ対策ベンチマーク
http://www.ipa.go.jp/security/benchmark/

本システムは、企業を対象としたもので、セキュリティ対策状況及び企業情報に関する設問(計40 問)に答えることにより、セキュリティ対策の取組状況を自己採点できるシステムです。

診断結果は、「貴社のスコア」と「望まれる水準」とが同時に表示され、各社が優先的に取り組むべきセキュリティ対策項目が明らかになります。また、推奨される取り組み事例も提示しますので、今後の対策を強化する上での具体的な改善策がわかります。

30 分程度で自己採点できますので、ぜひ、今後のセキュリティ対策の参考とすべく、ご活用ください。