INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
第 07-13-108 号
2007 年 7 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［2007 年 6 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 6 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。

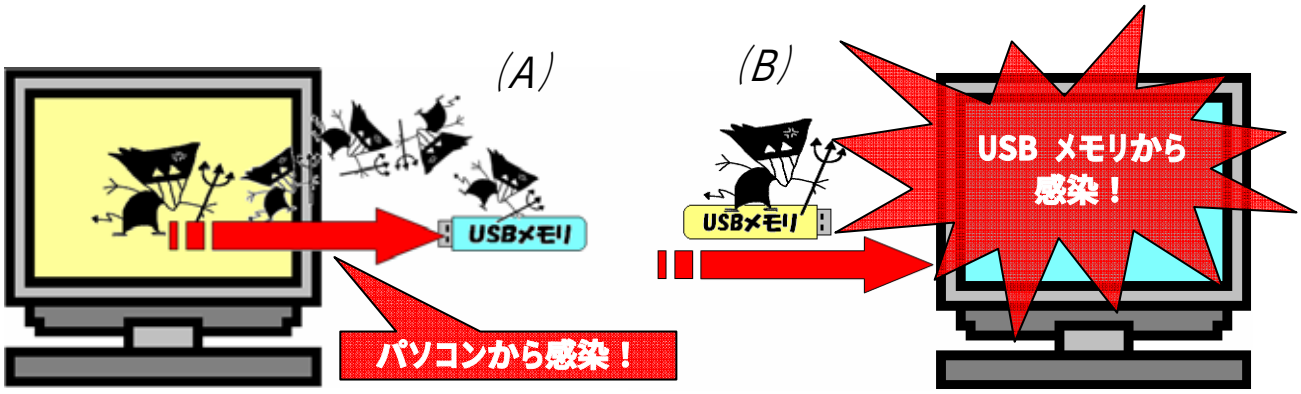
1．今月の呼びかけ

今月の呼びかけ：
「USB メモリを安易にパソコンに接続しないように！」
― USB メモリなどの外部記憶媒体からウイルス感染しないために！！ ―

(1)被害の状況

IPA へ 6 月に寄せられた相談の中に、「USB メモリをパソコンに挿したとたん、ウイルス対策ソフトがウイルスを検知した」といった内容の USB メモリに関する相談が多く見受けられました。

これらは、ウイルスがパソコンから USB メモリに感染し、その感染した USB メモリからパソコンへ二次感染して、感染が広まっている状況を示しています。さらに、5 月、6 月のコンピュータウイルスの発生状況を見ますと、USB メモリなどの外部記憶媒体を媒介して感染するウイルスが複数出現しています。



(2)USB メモリについて

USB メモリは、パソコンに USB ポートがあれば、そこに挿すだけで簡単に接続して使えます。このため、CD、FD(Floppy Disk)、MO(Magneto Optical Disk) などの、専用の読み書き装置がなければ使えないディスク媒体よりも、使い勝手の良い記憶媒体です。特に最近は、1G 以上の容量の大きいものもあり、比較的安価で小さく可搬性に優れるため、広く世間に普及しています。

手軽にパソコンに接続できて、サイズの大きいファイルも簡単に保存して持ち運べるのが USB メモリの大きな特徴です。しかし、**USB メモリそのものがウイルスに感染すると、ウイルスも手軽に持ち運べてしまう道具になりかねません。また、その USB メモリを他のパソコンに挿してしまうと、さらに感染を広げてしまう危険性があります。**

(3)対応策

USB メモリを利用する場合、USB ポート経由でウイルス感染の被害に遭わないために、以下の（A）と（B）のセキュリティ対策を行って下さい。

（A） USB メモリを挿して使用するパソコンのセキュリティ対策

基本的には、パソコン側のウイルス対策を実施するということです。最近では、USB メモリなど、外部に接続するドライブを探して感染するウイルスが見つかっています。

したがって、**自分の管理下にないパソコン(インターネットカフェ等にあるパソコンなど)に USB メモリを挿すことは、そのパソコンにセキュリティ対策が施されていないかも知れないので、USB メモリにウイルスが感染する可能性が高く、非常に危険です。**

そのパソコンに対して、ウイルスチェックを行うか、チェックができないのであれば、安易に USB メモリを挿すことはしない方が良いでしょう。

対策として、ウイルス対策ソフトのウイルス定義ファイルを最新の状態にして使用することはもちろん、Windows Update/Microsoft Update などでセキュリティホール(セキュリティ上の弱点)の解消も行っておくことが大事です。

USB メモリ等に感染する代表的なウイルスは以下のとおりです。

・W32/SillyFD-AA
このウイルスは、内蔵 HDD ではなく、USB メモリなどの外部に接続しているドライブを検索し、見つけた外部のドライブに自分自身をコピーし、Autorun.inf(自動起動)ファイルを作成します。
http://www.sophos.co.jp/security/analyses/w32sillyfdaa.html

・W32/LiarVB-A
このウイルスは、USB メモリなどの外部に接続しているドライブに感染します。見つけた外部のドライブに自分自身をコピーし、Autorun.inf ファイルを作成します。さらに、エイズと HIV について解説した HTML ファイルをパソコン側のシステムに保存します。
http://www.sophos.co.jp/security/analyses/w32liarvba.html

Autorun.inf (自動起動)ファイルとは、自動で起動させたい実行ファイル(拡張子が.exe のファイル)名を Autorun.inf ファイル内に設定しておき、その Autorun.inf ファイルが入った CD や DVD 等をパソコンに読み込ませると、自動で実行ファイルを起動させることができます。
通常 USB メモリでは、Autorun.inf ファイルは起動しません(Windows Vista の初期設定は除く)が、**USB メモリに感染するウイルスの中には、この Autorun.inf ファイルを作成し、ウイルス自身を自動で起動させようとするものもありますので、安心はできません。**

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
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
IPA -ボット対策について
http://www.ipa.go.jp/security/antivirus/bot.html

次に、パソコンにはウイルスがいないとわかった場合、以下の操作方法で安全に USB メモリを挿して、USB メモリのウイルスチェックを行ってください。

基本的に、**出所が不明の USB メモリを、そのまま自分のパソコンに挿すことは、大変危険です。**USB メモリにウイルスが感染している場合は、そのままパソコンにウイルス感染する可能性が高いので、安易に挿すことはすべきではありません。

（B）USB メモリのセキュリティ対策

USB メモリを挿した時に、すぐに実行ファイルが起動されない様に次の操作方法を行ってください。

(i). Windows Vista の場合

Windows Vista が初期設定のままだと、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は、いきなり実行ファイルが起動します。

キーボードの「Shift」キーを押下しながら、USB メモリをパソコンに挿せば、いきなり起動はされませんが、初期設定のまま、USB メモリをパソコンに挿すことは非常に危険です。確実に、自動で実行ファイルを起動しないために、以下の設定を行って下さい。

「 」→「コントロールパネル」→「ハードウェアとサウンド」→

「CD または他のメディアの自動再生」

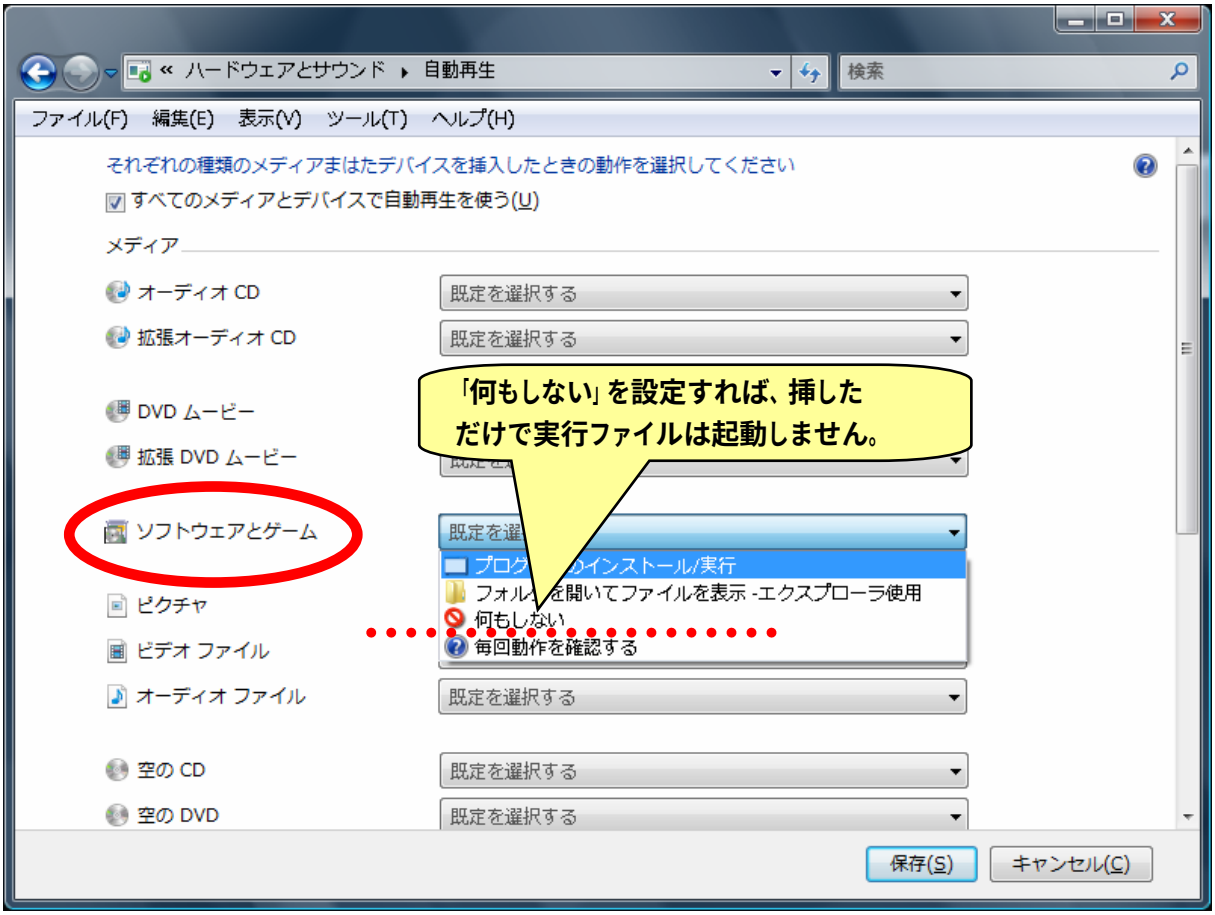


図 1-1. Windows Vista 「CD または他のメディアの自動再生」 設定画面

ウイルスプログラムは、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 ムービー等）も、同じ様に設定することをお勧めします。

(ii). Windows 2000／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、パソコンに挿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。

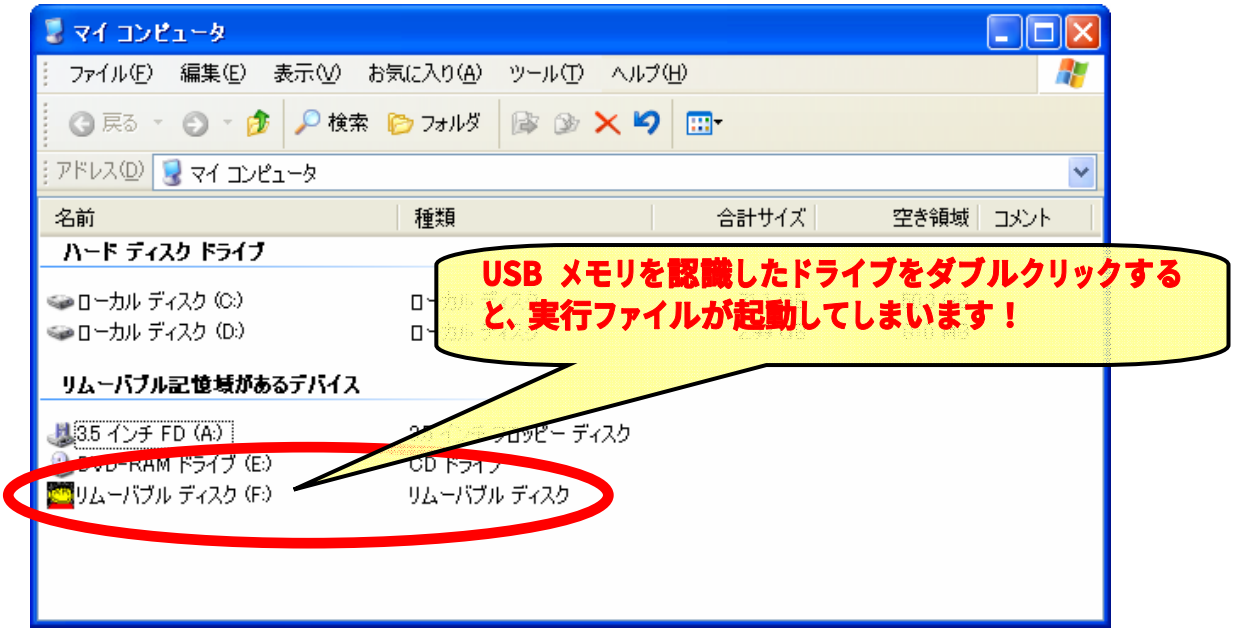


図 1-2. マイコンピュータ画面

ダブルクリックする前に、USB メモリを認識したドライブに対して、ウイルス対策ソフトで、ウイルスチェックを行ったり、Windows エクスプローラーから、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。

Windows エクスプローラーの表示は、マイコンピュータを開いて、「表示」→「エクスプローラーバー」→「フォルダ」をクリックします。
Windows エクスプローラー画面から向かって左側の画面(図 1-3.参照)より、USB メモリを認識したドライブをクリックすると、ドライブの中身(図 1-4.参照)が見えます。

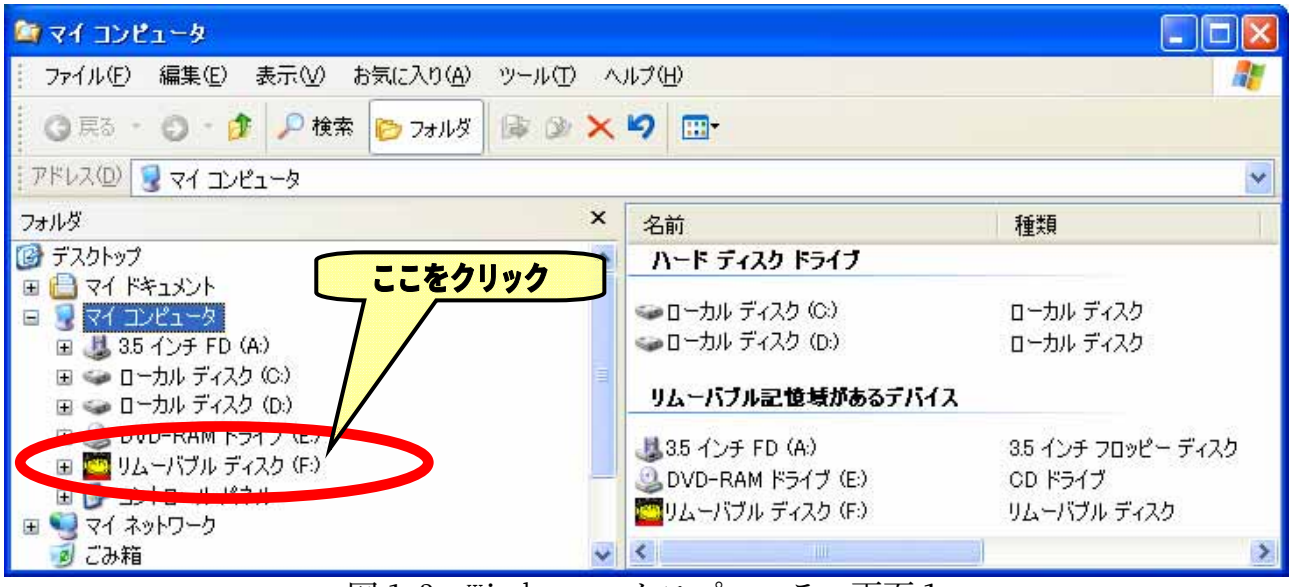


図 1-3. Windows エクスプローラー画面 1

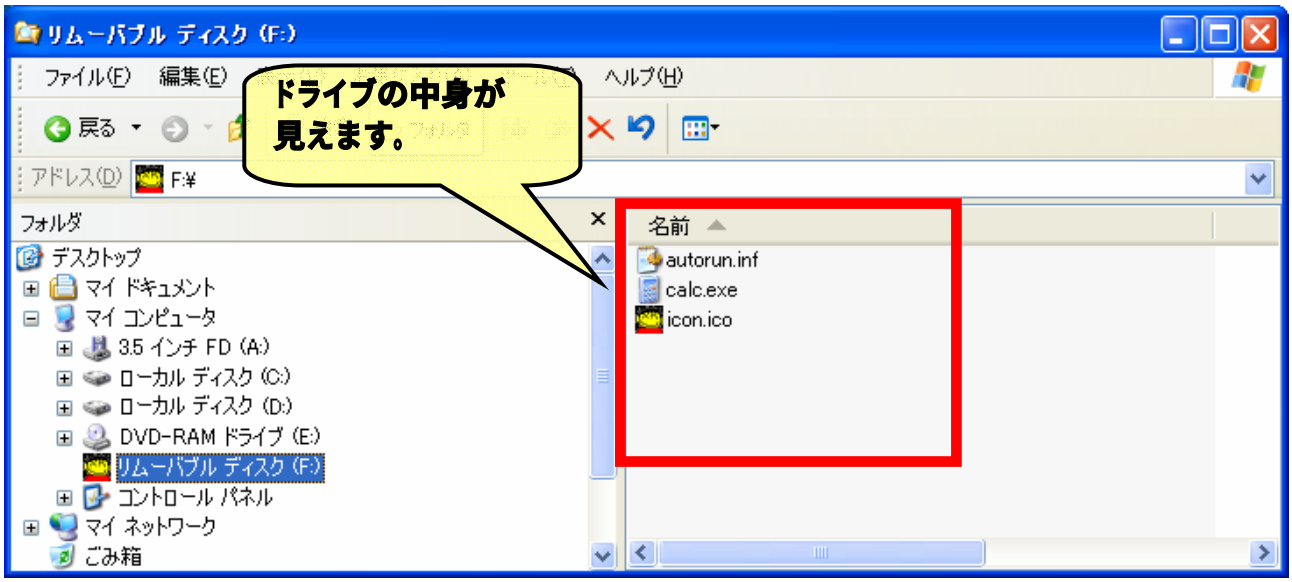


図 1-4. Windows エクスプローラー画面 2

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)

・サーバが他サイト攻撃のための踏み台として使われていた
・WebDAV の設定ミスでウェブサイトが改ざんされた

○ 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)

・ボットに感染している？！
・家族共用パソコンのデスクトップに見知らぬアイコンが‥

○ 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。

・Windows Messenger サービスを狙ったアクセスに注意！

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 50 万個**と、5 月の 77 万個から 35.5%の減少となりました。
また、6 月の届出件数(※2)は、**2,898 件**となり、5 月の 3,383 件から 14.3%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。
・6 月は、寄せられたウイルス検出数約 50 万個を集約した結果、2,898 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/Stration** で**約 2 万個、3 位は W32/Mytob** で**約 1.6 万個でした。**

ウイルス検出数　約50万個 (約77万個)　前月比 - 35.5%

（注：括弧内は前月の数値）

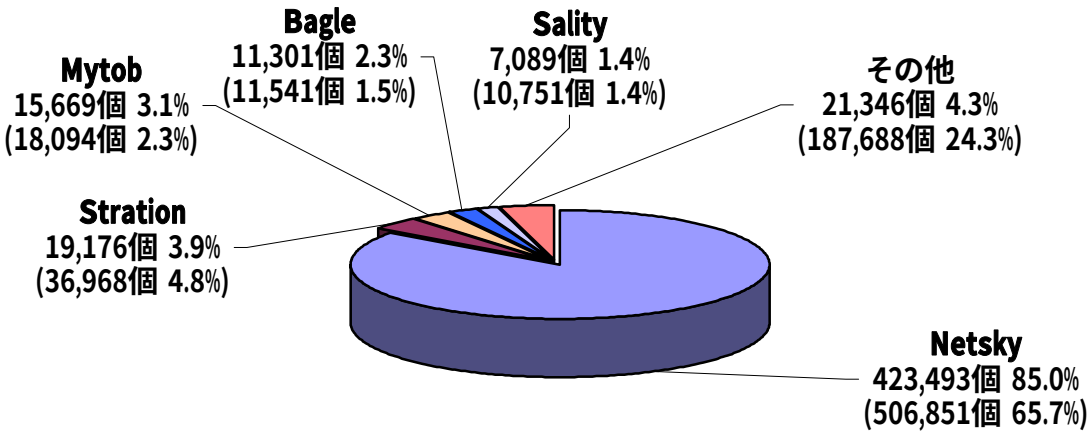


図:2-1

ウイルス届出件数　2,898件 (3,383件)　前月比 - 14.3%

（注：括弧内は前月の数値）

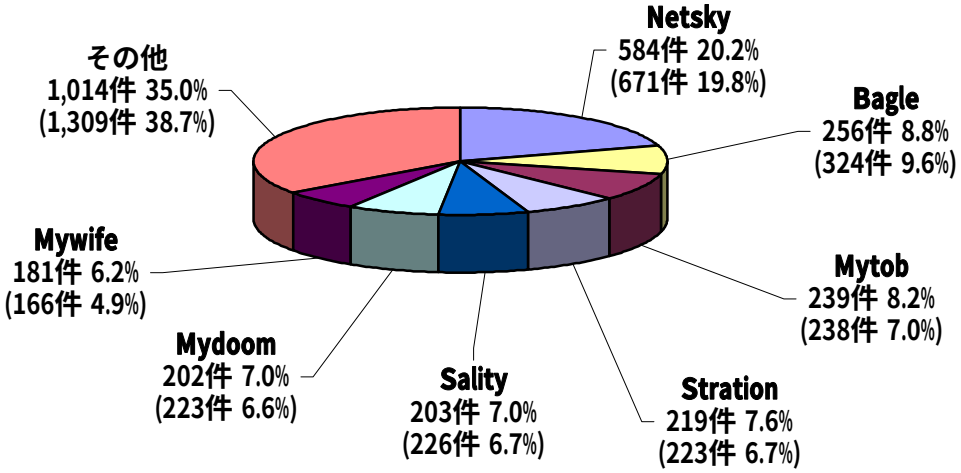


図:2-2

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

		1月	2月	3月	4月	5月	6月
届出[a] 計		**32**	**23**	**13**	**15**	**19**	**41**
	被害あり[b]	22	14	9	12	13	36
	被害なし[c]	10	9	4	3	6	5
相談[d] 計		**52**	**50**	**43**	**31**	**37**	**27**
	被害あり[e]	25	28	20	20	21	11
	被害なし[f]	27	22	23	11	16	16
合計[a+d]		**84**	**73**	**56**	**46**	**56**	**68**
	被害あり[b+e]	47	42	29	32	34	47
	被害なし[c+f]	37	31	27	14	22	21

（1）不正アクセス届出状況

6 月の届出件数は 41 件であり、そのうち**被害のあった件数は 36 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 27 件（うち 2 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 11 件でした。

（3）被害状況

被害届出の内訳は、**侵入 6 件、アドレス詐称 2 件、その他（被害あり）28 件**でした。

侵入届出の被害内容は、ウェブサイトのコンテンツ改ざんが 1 件、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 1 件、サーバ内データの書き換え 2 件、などでした。侵入の原因は、プログラムのぜい弱性[*1]を突かれたものが 3 件（ウェブサーバ 1 件、その他アプリケーション 2 件）、設定不備によるものが 2 件、などでした。

(4) 被害事例

[侵入]

(i) サーバが他サイト攻撃のための踏み台として使われていた

事例	・組織外部から「貴方の組織内のパソコンから、SSH(*2)で使用するポートへパスワードクラッキング(*3)攻撃を受けている」との苦情メールが入った。 ・調査したところ、2 台の Linux マシンに侵入された形跡を発見。内 1 台にパスワードクラッキングツールを埋め込まれ、他サイト攻撃の踏み台として使われていたことが判明。どちらのマシンも、パスワードクラッキングを受けた形跡は無く、ID/パスワード共に一度の入力でログインに成功していた。 ・Linux マシンに接続し端末として使用していた Windows マシンを調査したところ、ウイルス対策ソフトの機能が無効にされた上、キーロガー(*4)を含むルートキット(*5)を埋め込まれていた。
解説・対策	侵入者は、ネットワーク内に侵入した際にすぐサーバへの侵入を試みず、まずはサーバへのアクセスがあると予想される端末マシンを狙ったと思われます。そして何らかの方法によって**ウイルスやルートキットを埋め込み、キーロガーを使って、端末からサーバへのログイン入力文字列を盗み見た**のでしょう。そうすることで、サーバへのログインは難なく出来ていました。このように、**最近は侵入の手口が巧妙かつ複雑化しています**。侵入者は、弱点を確実に狙ってきます。ネットワーク機器、サーバから端末まで抜けの無い、**総合的なセキュリティ対策が重要**になっています。 (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

(ii) WebDAV(*6)の設定ミスでウェブサイトが改ざんされた

事例	・ウェブサイトのトップページが改ざんされているとの連絡が、組織外部から入った。 ・調査したところ、ウェブサーバ内の複数のファイルが改ざんされ、関連するログ(*7)は削除されていたことが判明。その他、スクリプトが書かれたファイルも埋め込まれていた(ただし、スクリプト実行は失敗していた)。 ・WebDAV 機能を使っていたが、**利用者認証の設定にミス**があり、接続許可の無い人間によって外部から侵入され、ファイル操作されていた。
解説・対策	公開サーバは常に狙われています。**外部に向かってサービスを公開する場合、アクセス制限の設定には細心の気配りが必要**です。利用者をアカウントで区別するのはもちろんのこと、IP アドレス範囲を指定した**パケットフィルタリングも不正アクセスを防ぐための一つの対策として有効**です。 (参考) 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

4．相談受付状況

6 月の相談総件数は **932 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 **285 件**(5 月：185 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 **12 件**(5 月：19 件)、**Winny に関連する相談**が **11 件**(5 月：6 件) などでした。

IPA で受け付けた全ての相談件数の推移

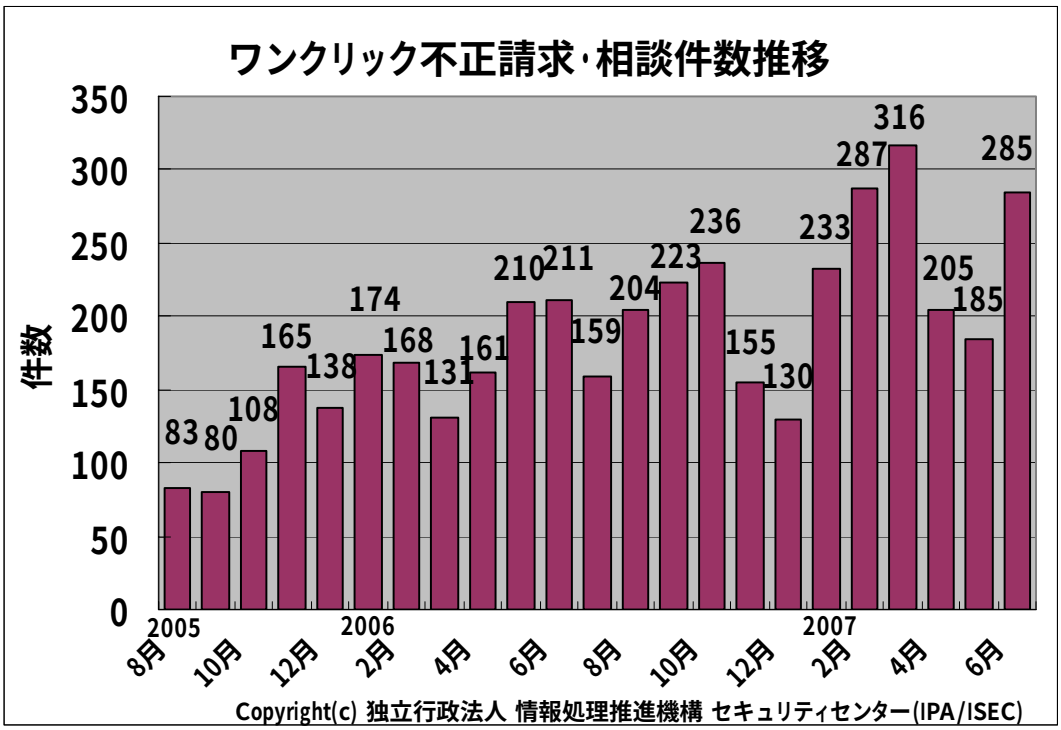
	1月	2月	3月	4月	5月	6月
合計	**946**	**1019**	**1127**	**827**	**814**	**932**
自動応答システム	582	603	697	486	484	537
電話	324	336	376	279	254	339
電子メール	39	75	54	58	69	53
その他	1	5	0	4	7	3

※ 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

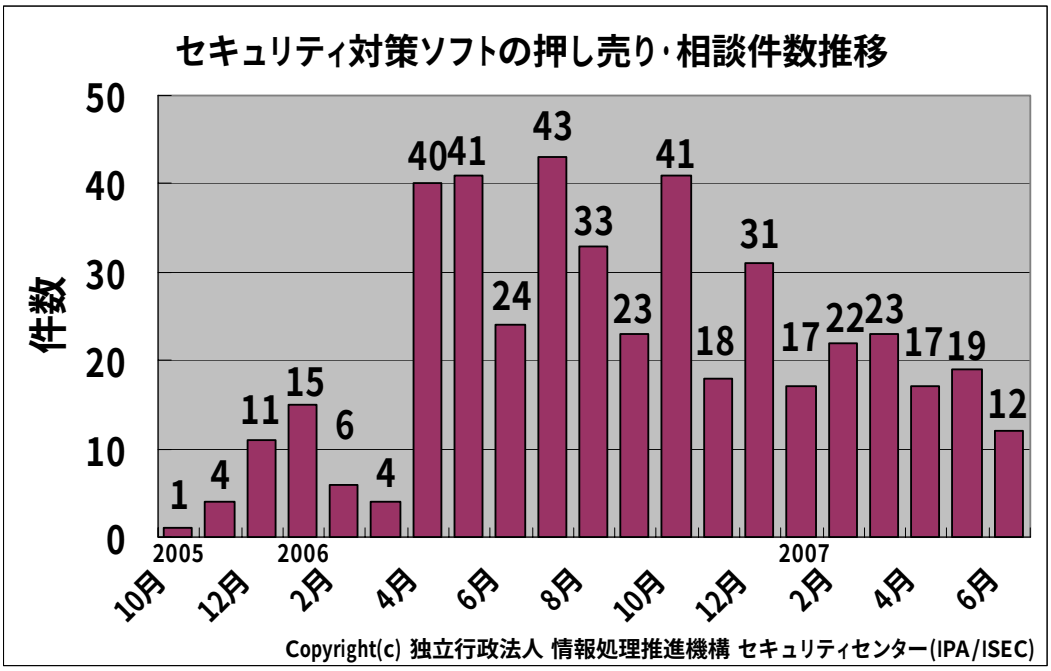


ワンクリック不正請求についての対策については下記をご参照ください。

・コンピュータウイルス・不正アクセスの届出状況[9 月分および第 3 四半期]について
2. ワンクリック不正請求
http://www.ipa.go.jp/security/txt/2006/10outline.html

・コンピュータウイルス・不正アクセスの届出状況[8 月分]について
2. 依然として相談の多いワンクリック不正請求による被害
http://www.ipa.go.jp/security/txt/2006/09outline.html

（参考）セキュリティ対策ソフトの押し売り・相談件数の推移



セキュリティ対策ソフトの押し売り行為については下記をご参照ください。

・2006 年 5 月の呼びかけ:「セキュリティ対策ソフトウェアの押し売りに注意！！」
http://www.ipa.go.jp/security/txt/2006/05outline.html

主な相談事例は以下の通りです。

(i) ボットに感染している？！

相談	自分が契約しているプロバイダを通じて、サイバークリーンセンター（CCC）というところからメールが届いた。「あなたのパソコンにボットが感染している」といった主旨。メールに書かれていた手順に従ってボット駆除ツールをダウンロードし、対処した。今後はどうすれば良いのか。
回答	**CCC ではプロバイダの協力を得てボットに感染しているパソコンの所有者に対して、メールで「感染している事実」を通知し、ボット駆除を促すという活動を実施しています**。今後は、**ウイルス対策ソフトを導入**するとともに、**OS を常に最新の状態に保つ**（Windows Update などを実施）ことを基本として、**「怪しいサイトには近づかない」「出所の不明なファイルは開かない」**ことを心掛ければ、ウイルスに感染する可能性を最小限にできるでしょう。 （ご参考） サイバークリーンセンター（総務省・経済産業省 連携プロジェクト） https://www.ccc.go.jp/

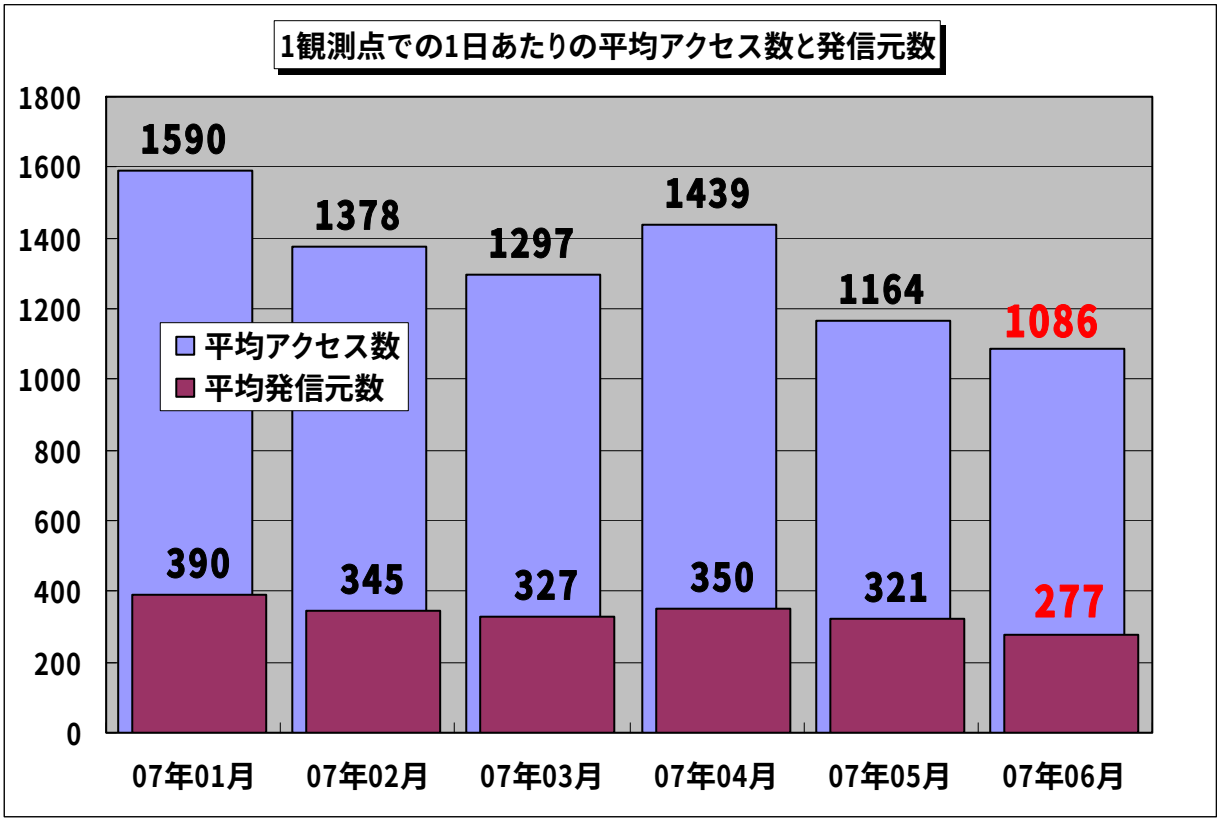
(ii) 家族共用パソコンのデスクトップに見知らぬアイコンが・・

相談	家族で共用しているパソコンで、ある日、デスクトップに見知らぬアイコンがあるのに気付いた。「**Cabos**」「Setup」など。これはウイルスによる仕業なのか？
回答	恐らく、他の共用者がソフトウェアをインストールしたものと思われます。ところで、**Cabos はファイル交換（共有）ソフトです。使い方を誤ると、パソコン内のデータがインターネットに流出してしまいます**。ウイルスに感染しても、自分の意思に反してデータが流出してしまう場合があります。このような**潜在的危険性があることを、パソコンの共用者に分かってもらう必要があります**。自分の知らないうちにデータが流出しないようにするため、**共用パソコンにはファイル共有ソフトはインストールすべきではありません**。 （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 6 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 6 月の期待しない（一方的な）アクセスの総数は、10 観測点で **293,252 件**ありました。1 観測点で 1 日あたり **277** の発信元から **1,086 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、277 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 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 1 月～2007 年 6 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、緩やかですが減少傾向にあるようです。

2007 年 6 月のアクセス状況は、全体的に 5 月と同じで定常化していると言えます。Windows のぜい弱性を狙った、135/tcp、445/tcp のアクセスは相変わらず多い状況の中、Windows Messenger サービスを悪用してポップアップメールを送信する、1026/udp、1027/udp のアクセスが増加しました。

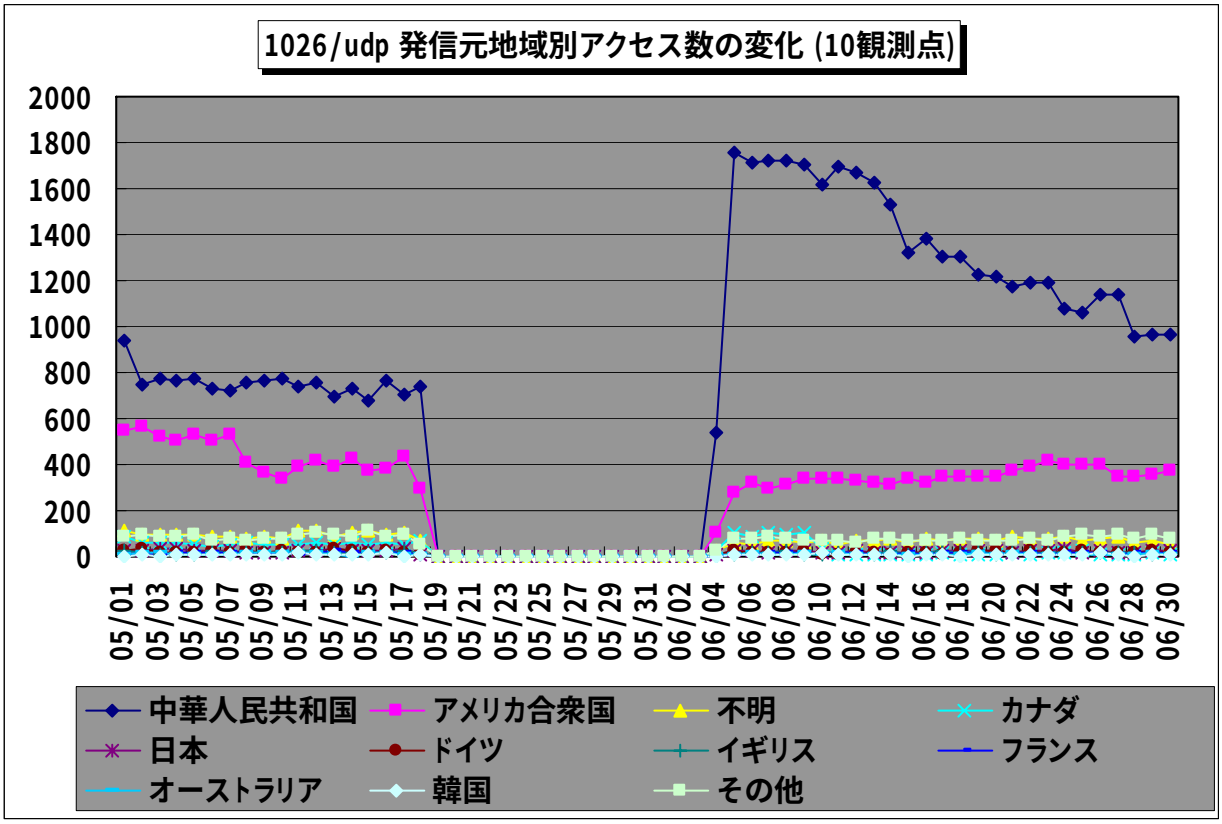
注意）

6 月 1 日から 3 日までは TALOT2 システム保守の為、6 月 4 日から 6 月 30 日までの観測データで発表しておりますことをご了承下さい。

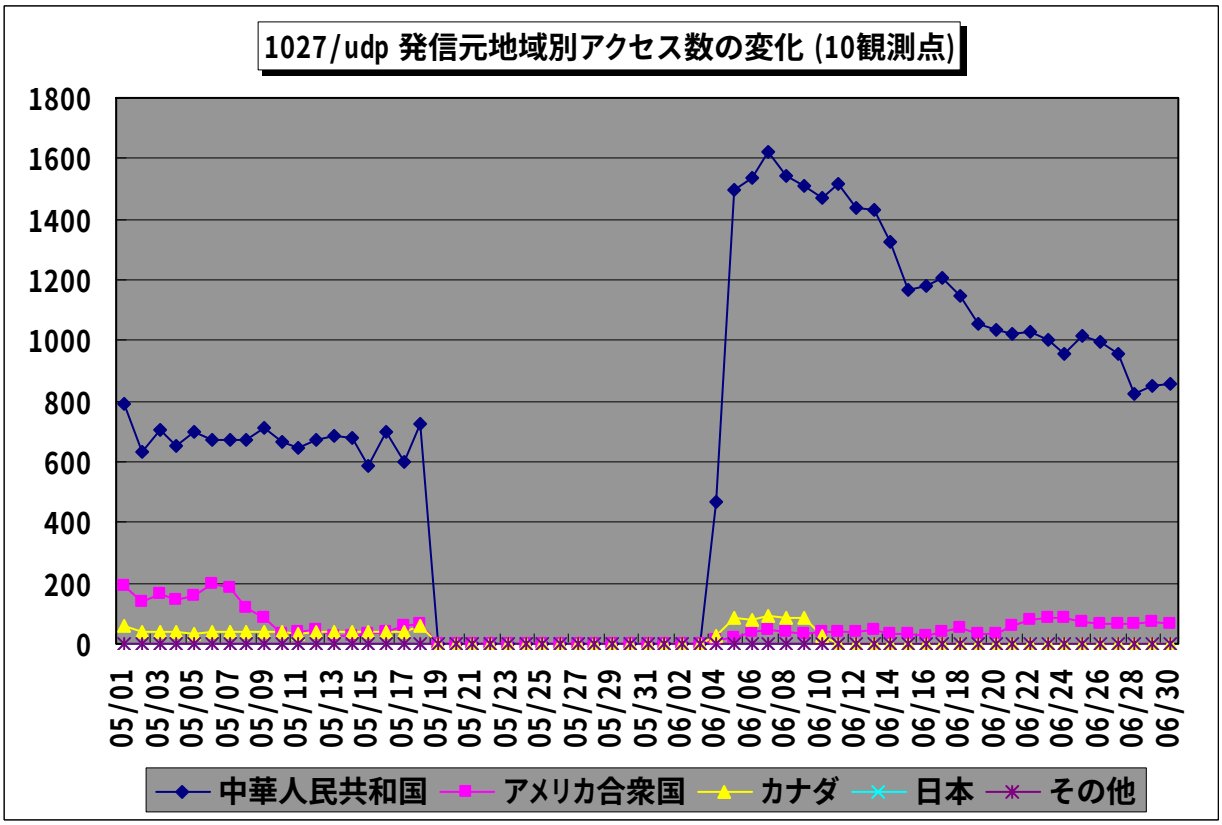
（1）1026/udp、1027/udp ポートを狙ったアクセス

2007 年 6 月の、1026/udp、1027/udp ポートのアクセスは、2007 年 5 月と比べると、約 2 倍近くのアクセス数がありました。これらのほとんどが中国からのアクセスです。

図 5.2、図 5.3 に、2007 年 5 月から 2 ヶ月間の、1026/udp、1027/udp ポートへの発信元地域別アクセス数の変化を示します。



【図 5.2　2007 年 5 月～6 月の 1026/udp ポートへの発信元地域別アクセス数の変化】



【図 5.3　2007 年 5 月～6 月の 1027/udp ポートへの発信元地域別アクセス数の変化】

これらのアクセスは、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す。ただ、メッセージが表示されるには、いくつかの条件がある為、全てのコンピュータに表示されるわけではありません。

このように送られてくるポップアップメッセージは、スパムメッセージのようなものが多いので、無視をしていれば問題はありませんが、Windows Messenger サービスの脆弱性のセキュリティパッチが適用されていないと、リモートからコードを実行される危険性があります。セキュリティパッチが適用されているか確認を行ってください。

<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.mspx

最近では、この様な Messenger サービスを使って、ウイルスが送られてきたり、フィッシングサイトに誘導するものもあります。Messenger サービスを使用しているコンピュータのセキュリティ対策を、再確認されることをお勧めします。

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/TALOT2-0707.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/

『用語の解説』

(*1) **ぜい弱性** (vulnerability)
情報セキュリティ分野においては、通常、システム・ネットワーク・アプリケーションまたは関連するプロトコルのセキュリティを損なうような、予定外の、望まないイベントにつながる可能性がある弱点の存在や、設計もしくは実装のエラーのことを言う。セキュリティ上の設定が不備である状態を指す場合もある。一般に、セキュリティホール (security hole)と呼ばれることもある。

(*2) **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。通信上のデータはすべて暗号化されるため、Telnet のようにデータが平文で通信されるプロトコルに比べて、安全性が高い。SSH の利用に際しては、いくつかの認証方式を選択することが可能だが、パスワード認証は総当り攻撃などにより認証を突破されてしまう可能性があるため、公開鍵認証を用いることが推奨される。

(*3) **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。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。
＊:総当り攻撃
システムのパスワードを発見するために、パスワード文字列として可能な組み合わせをひとつずつ試す攻撃。「ブルートフォース」には、「力ずく」という意味が込められている。
＊:辞書攻撃
パスワードを破るために、辞書にある単語などを片端から試行する攻撃方法のこと。

(*4) **キーロガー** (key logger)
キーボードから入力された情報を記録するプログラムのこと。

(*5) **ルートキット** (rootkit)
攻撃者がコンピュータに侵入した後に利用するためのソフトウェアをまとめたパッケージのこと。一般的には、ログ改ざんツールやバックドアツール、改ざんされたシステムコマンド群などが含まれる。

(*6) **WebDAV** (Web-based Distributed Authoring and Versioning)
http (hypertext transfer protocol) を拡張し、ウェブブラウザからウェブサーバ上のファイルやフォルダの編集やバージョン管理などができるようにした仕組みのこと。

(*7) **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。

■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

お知らせ

「第 3 回 情報セキュリティ標語・ポスター」募集のお知らせ

コンピュータウイルスやコンピュータへの不正な侵入などの被害にあわないために、「情報セキュリティ対策」の意識を高めるための標語及びポスターを、全国の小学生・中学生・高校生から募集します。入選作品は、報道発表し、IPA のホームページにも掲載します。

募集期間：2007年7月 1 日(日)～2007 年9月１０日(月)
応募方法：電子メール　isec-hyogo@ipa.go.jp
ＦＡＸ　　03-5978-7518
郵　送　　〒113-6591　東京都文京区本駒込 2-28-8
情報処理推進機構（IPA）　セキュリティセンター
情報セキュリティ標語・ポスター事務局　宛
詳しくは、下記のホームページをご参照下さい。
http://www.ipa.go.jp/security/event/hyogo/2007/boshu.html
賞　　金：大賞（10 万円)、金賞（7 万円)、銀賞（5 万円)、銅賞（3 万円）
韓国情報保護振興院(KISA)賞（賞品)、その他、参加企業賞あり

お問い合わせ先
標語・ポスター募集に関するお問い合わせ先はこちらです。
独立行政法人 情報処理推進機構　セキュリティセンター　山田／岸原
Tel:　　03-5978-7508
Fax:　　03-5978-7518
E-mail:　isec-hyogo@ipa.go.jp

問い合わせ受付時間 9:30 - 18:30 月曜日～金曜日
（祝祭日、振替休日を除く）