平成１４年2月１６日

最新ウイルス事情

ＣＣ－ＮＥＴ　塚本

インターネットの普及に伴いウイルスは蔓延しています。
平成１４年１月に新規に発生したウイルスは３０件を数えました。
現在発見されているウイルスの数は Norton AntiVirus では 58,723 件です。

１．ウイルスの種類
破壊型
トラフィック負荷型(愉快犯)

２．なぜウイルスを作るのか
マイクロソフトの罪
Windows に標準搭載ソフトの脆弱製があり、
マイクロソフトへの警告または嫌がらせからウイルスを作るケースが多い
OutLook
OutLookExpress
Internet Explorer
MS Exchage

３．ウイルスに感染するには
添付ファイルを実行する。(ダブルクリック)
メールをプレビューするだけで感染
ホームページを閲覧するだけで感染

４．どうして防ぐか
アンチウイルスソフトを購入しパソコンにインストールする。
発売している会社は
http://www.symantec.co.jp/
http://www.trendmicro.co.jp/
http://www.nai.com/japan/
http://www.sophos.co.jp/
またはメールサーバにアンチウイルス対策を行う。
プロバイダーに加入の場合はプロバイダー次第であり、
企業サーバの場合には自社で購入しインストールする。
（年間コストは１００万円から１億以上でメールアドレスの数で決まります。）

５．ウイルスを作る目的は
インターネットの普及と共にウイルスをばらまく方法が簡単になり
また新聞などに取り上げられるケースも多く、世間が騒ぐのを見て楽しむ愉快犯が多い

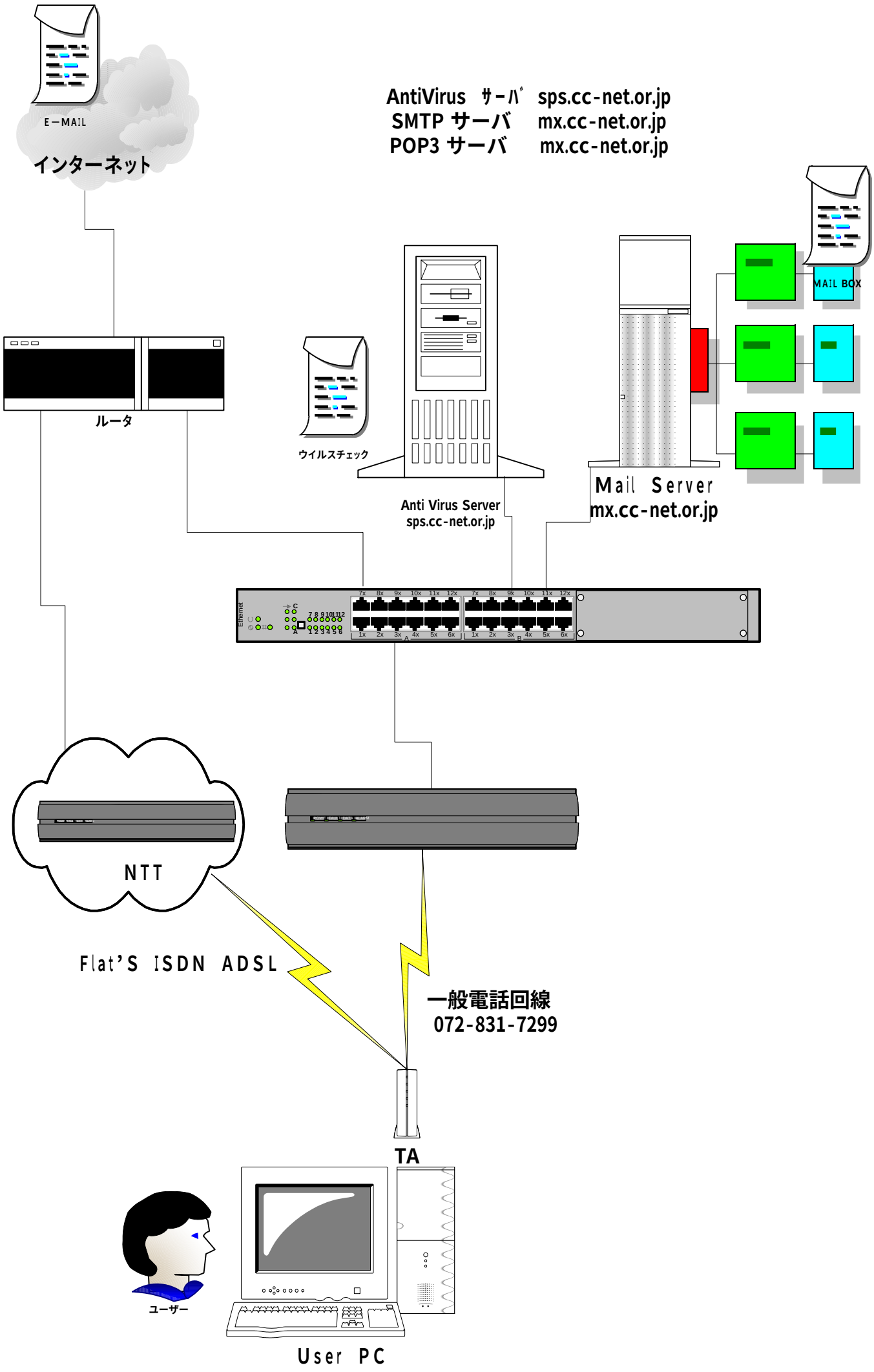
６．誰が作るのか
インターネット上にウイルスを作る方法のホームページがあり
そのページを参考にして学生が作成するケースが多い

７．名前の付け方は
アンチウイルスソフトを提供している会社が独自に名前を付けている。

８．ウイルスが届く仕組み？
最近はメールと共に送られてくるケースが大半であるが、
フロッピー、CD-ROM に住み着いているケースもある。

９．その他
ウイルスがばらまかれたときにすぐワクチンが出来るわけではない
ワクチンが出来るまでには時差があるのでその間に感染をする場合がある。

10.安全にインターネットを楽しむためには
ブラウザーを InternetExplorer から NetscapeCommunicator へ変更する。
メールソフトは市販品を使用し HTML 形式メールは使用しない
アンチウイルスソフトを使用する。


E－MAIL
インターネット
AntiVirus サーバ sps.cc-net.or.jp
SMTP サーバ mx.cc-net.or.jp
POP3 サーバ mx.cc-net.or.jp
MAIL BOX
ルータ
ウイルスチェック
Anti Virus Server
sps.cc-net.or.jp
Mail Server
mx.cc-net.or.jp
NTT
Flat'S ISDN ADSL
一般電話回線
072-831-7299
TA
ユーザー
User PC

FileName = Virus - Or.jp 02/02/12 18:09:36

 Subject: FOUND VIRUS IN MAIL from shihoko@fox.zero.ad.jp
    Date: Tue, 5 Feb 2002 07:27:14 +0900 (JST)
    From: postmaster@sps.cc-net.or.jp
      To: virusalert@sps.cc-net.or.jp

A virus was found in an email from:

shihoko@fox.zero.ad.jp

The message was addressed to:

-> info@cc-net.or.jp

The message has been quarantined as:

/var/virusmails/virus-20020205-072714-97322

Here is the output of the scanner:

>>> Virus 'W32/Badtrans-B' found in file
/var/amavis/amavis-07726338/parts/msg-97322-2.pif
>>> Virus 'W32/Badtrans-B' found in file
/var/amavis/amavis-07726338/parts/part-00001

Here are the headers:

------------------------ BEGIN HEADERS -----------------------------
Return-Path: <shihoko@fox.zero.ad.jp>
Received: from fox.zero.ad.jp (fox.zero.ad.jp [211.11.96.133])
    by sps.cc-net.or.jp (8.11.6/8.11.6av) with ESMTP id g14MRDA97319
    for <info@cc-net.or.jp>; Tue, 5 Feb 2002 07:27:13 +0900 (JST)
    (envelope-from shihoko@fox.zero.ad.jp)
Received: from aol.com (osaka1721-152057.zero.ad.jp [211.123.152.57])
    by fox.zero.ad.jp (8.9.3+3.2W/3.7W) with SMTP id HAA03402
    for <info@cc-net.or.jp>; Tue, 5 Feb 2002 07:27:00 +0900 (JST)
Date: Tue, 5 Feb 2002 07:27:00 +0900 (JST)
Message-Id: <200202042227.HAA03402@fox.zero.ad.jp>
From: "R□@u□q" <_shihoko@fox.zero.ad.jp>
To: info@cc-net.or.jp
Subject: Re:
MIME-Version: 1.0
Content-Type: multipart/related;
     type="multipart/alternative";
     boundary="====_ABC1234567890DEF_===="
X-Priority: 3
X-MSMail-Priority: Normal
X-Unsent: 1
------------------------- END HEADERS ------------------------------

FileName = 転送1 - From: Tsuka <tako@adonis.ne.jp> Adonis 02/02/12 18:13:50

V I R U S A L E R T

Our viruschecker found the

    'W32/Badtrans-B'
    'W32/Badtrans-B'

virus(es) in your email to the following recipient(s):

-> info@cc-net.or.jp

Please check your system for viruses, or ask your system administrator
to do so.

For your reference, here are the headers from your email:

------------------------ BEGIN HEADERS -----------------------------
Return-Path: <info@cc-net.or.jp>
Received: from aol.com (c196002.ppp.asahi-net.or.jp [210.155.196.2])
    by sps.cc-net.or.jp (8.11.6/8.11.6av) with SMTP id g0A73HT91472
    for <info@cc-net.or.jp>; Thu, 10 Jan 2002 16:03:17 +0900 (JST)
    (envelope-from info@cc-net.or.jp)
Date: Thu, 10 Jan 2002 16:03:17 +0900 (JST)
Message-Id: <200201100703.g0A73HT91472@sps.cc-net.or.jp>
From: "Support" <support@cyberramp.net>
To: info@cc-net.or.jp
Subject: Re:
MIME-Version: 1.0
Content-Type: multipart/related;
     type="multipart/alternative";
     boundary="====_ABC1234567890DEF_===="
X-Priority: 3
X-MSMail-Priority: Normal
X-Unsent: 1
------------------------ END HEADERS -------------------------------

2001年3月21日

用語集

Access 97 マクロウイルス

感染対象: MS Access 97 以降、すべての OS
言語: VBA マクロ言語
複製: 感染データベースが開かれた際、他の Access データベースファイルに感染。
命名方法: Sophos Anti-Virus で、この種のウイルス名は、"AM97/" で始まります。"A97M"、"AM" などを使用するウイルス対策ベンダーもあります。
例: この種のウイルスを表示する

TOP

AppleScript ワーム

説明: AppleScript は、Macintosh OS のデフォルトバッチ言語です。したがって、Macintosh マシンにインストールされるアプリケーションの大半は、AppleScript を使ってスクリプトを作成できます。AppleScript ワームは、AppleScript の機能を使って他のマシンに感染したり、自らを送信するため、メールアプリケーションにスクリプトで指示を出すワームです。
命名方法: Sophos Anti-Virus で、この種のワーム名は、"AplS/" で始まります。
例: この種のワームを表示する

TOP

Basic Input Output System (BIOS)

説明: BIOS は、PC の電源を入れた際、一番最初に実行するソフトウェアです。したがって、マシンが作動するためには不可欠で、BIOS が存在しないとマシンは実質上使用できません。
BIOS は、マザーボードにある、電源が切断されても、その内容が保存される特別のチップに保存されています。これは、常に BIOS が存在することを保証するのが目的です。

注: 多くのコンピュータでは、BIOS 製造元が提供するソフトを使って、BIOS をアップグレードすることが可能です。更に、W95/CIH-10xx などのウイルスによって破壊されることも可能で、場合によってはマシンを起動できなくなることがあります。BIOS チップを取り替えることができない場合 (はんだ付けで固定されている BIOS チップもあります)、マシンのマザーボードを交換することが必要な場合さえあります。

TOP

CMOS 設定

説明: CMOS 設定は、根本的なシステム環境設定情報を維持保存し、マザーボードの特別なチップ内に保存されています。このチップは、通常、電池によって電源が供給されているため、マシンの他の部分とは独立して作動することができるので、電源を切った場合でも、システムクロックを維持するなどの操作を行います。
また、CMOS 設定は、どのようなディスクがマシンにインストールされているか、起動時にパスワードが必要か、マシンの起動にはどのデバイス (例: フロッピーディスク、ハードディスク、CD-ROM、ネットワーク) が必要かなどを記録します。マシンの CMOS 設定が不正確な場合、マシンが正常に作動しない場合があります。
一部のウイルスや Troj/KillCMOS-E などのトロイの木馬は、わざとこれらの設定を破損し、マシンが作動しないようにしようとします。
CMOS 設定を修正するのは通常簡単なことですが、その方法はマシンによって異なります。ご不明な点は、マシン付属のマニュアルや製造元の Web サイトをご参照ください。

注: CMOS 設定の一つに、"ブートシークェンス" と呼ばれるものがあります。これは、マシンがフロッピーディスクを使って起動を試みるかどうかを決定するものです。誤って、フロッピーディスクを使ってマシンを起動した場合、Form などのブートセクタ感染型ウイルスに感染してしまう可能性があるので、常にマシンがハードディスクから起動するようこの設定を変えることをお勧めします。安全対策ガイドラインをご参照ください。

TOP

Corel Script ウイルス

感染対象: すべての OS で実行している Corel SCRIPT ファイル

言語: Corel SCRIPT マクロ言語

複製: 感染スクリプトが実行されると、他の Corel SCRIPT ファイルに感染します。

命名方法: Sophos Anti-Virus で、この種のウイルス名は "CSC/" で始まります。

TOP

DOS 実行ファイル感染型ウイルス

感染対象: DOS/Windows 実行ファイル

複製: 他の実行ファイルに感染。ウイルスの中には、メモリに常駐して、実行時に他のプログラムに感染するものもあります。積極的に他のファイルを検出して、それに感染するウイルスもあります。

命名方法: この種のウイルスに関する標準の命名法はありません。

例: この種のウイルスを表示する

TOP

DOS ブートセクタ感染型ウイルス

感染対象: ハードディスクの DOS ブートセクタ（別名 DOS ブートレコード）と、フロッピーディスクのブートセクタ。
フロッピードライブから起動するように設定されている Intel 互換性の PC すべてに感染可能です。
Windows NT のように、より安全な OS には感染可能ではあるが、ウイルスの複製を妨げることが考えられます。

言語: Intel 80x86 アセンブラ

複製: 感染マシンが起動した際、メモリにロードし、その後、マシンで使用するフロッピーディスクすべてに感染します。感染フロッピーディスクを使って起動したマシンは、感染してしまいます。

命名方法: この種のウイルスに関する標準の命名法はありません。

例: この種のウイルスを表示する

Excel 97 マクロウイルス

感染対象: MS Excel 97 以降、すべての OS

言語: VBA5 以降のマクロ言語

複製: 感染ドキュメントが開かれると、ウイルスコードのあるフォーミュラシートがディレクトリ XLSTART にあるファイルにコピーされます。他のファイルを開いた際、このファイルは自動的にロードされます。
XM97/Papa などのウイルスは、Outlook などのメールプログラムを使って、アドレス帳にあるメールアドレスに自動的に感染ファイルを送信します。

命名方法: Sophos Anti-Virus で、この種のウイルス名は "XM97/" で始まります。"X97M" を使用するウイルス対策ベンダーもあります。

例: この種のウイルスを表示する

Excel フォーミュラウイルス

感染対象: MS Excel 5 以降、すべての OS

言語: Excel フォーミュラ言語

複製: 感染ドキュメントが開かれると、ウイルスコードのあるフォーミュラシートがディレクトリ XLSTART にあるファイルにコピーされます。他のファイルを開いた際、このファイルは自動的にロードされます。

命名方法: Sophos Anti-Virus で、この種のウイルス名は "XF/"、あるいは "XF97/" で始まります。

Excel マクロウイルス

感染対象: MS Excel 5 以降、すべての OS

言語: VBA3 マクロ言語

複製: 感染ドキュメントが開かれると、ウイルスコードのあるフォーミュラシートがディレクトリ XLSTART にあるファイルにコピーされます。他のファイルを開いた際、このファイルは自動的にロードされます。

命名方法: Sophos Anti-Virus で、この種のウイルス名は "XM/" で始まります。（旧式名として、"Excel" で始まるものもあります。）

例: この種のウイルスを表示する

JavaScript ウイルス

感染対象: JavaScript スクリプトファイル、埋め込みスクリプトのある HTML ファイル、Microsoft Outlook、Internet Explorer

言語: JavaScript

複製: ファイル内に自らを挿入。

命名方法: Sophos Anti-Virus で、この種のウイルス名は "JS/" で始まります。

例: この種のウイルスを表示する

TOP

JavaScript ワーム

感染対象: JavaScript スクリプトファイル、埋め込みスクリプトのある HTML ファイル、Microsoft Outlook、Internet Explorer

言語: JavaScript

複製: IRC、Outlook、あるいは Windows のネットワーク機能を使って、複数のユーザーに感染ファイルのコピーを電子メール送信したり、ネットワークを介して自らをコピーします。

命名方法: Sophos Anti-Virus で、この種のワーム名は "JS/" で始まります。

例: この種のワームを表示する

TOP

Linux ワーム

感染対象: Linux ネットワークに接続しているマシン。

複製: Linux ワームは、ネットワークコードにある脆弱性を利用して、Linux を実行している遠隔のコンピュータに未許可のアクセスを行います。アクセス後は、感染対象にする新たなマシンの検索を開始し、しばしば、ネットワークトラフィックが増加することより、初めその存在が認識されます。ユーザー介入を必要としないので、この種のワームは、インターネットに常設しているマシン間で迅速に感染を広げます。

命名方法: Sophos Anti-Virus で、この種のワーム名は "Linux/" で始まります。"Unix" を使用するウイルス対策ベンダーもあります。

例: この種のワームを表示する

TOP

Macintosh ファイル感染型ウイルス

感染対象: Macintosh

複製: 多様な方法で他の Macintosh ファイルに感染。

命名方法: Sophos Anti-Virus で、この種のウイルス名は "Mac/" で始まります。

TOP

Macintosh ワーム

感染対象: Power Macintosh

複製: QuickTime AutoPlay 機能を使って、感染フロッピーディスクが挿入された際、それを自身にコピーし、または、それに自らをコピーします。

命名方法: Sophos Anti-Virus で、この種のワーム名は "Mac/" で始まります。

TOP

Macromedia Flash 感染型ウイルス

感染対象: Flash 5 プレーヤー関連の Macromedia Flash ファイル

複製: 通常、Flash ファイルの始めにあるスクリプトに自らをコピーして複製。

例: この種のウイルスを表示する

TOP

mIRC、pIRCH スクリプトワーム

感染対象: IRC を実行しているシステム
言語: IRC Script
複製: SCRIPT.INI ファイルに変更を加え、IRC に自らのコピーを配布させる実行ファイル。
命名方法: Sophos Anti-Virus で、この種のワーム名は "mIRC/"、あるいは "pIRC/" で始まります。

TOP

Office 97 マクロウイルス

感染対象: MS Office 97 以降、すべての OS
言語: VBA5 以降のマクロ言語
複製: 二つ、あるいは複数の Office コンポーネントに感染。多くは Word と Excel に感染するが、 PowerPoint、および Project ファイルにも感染する場合があります。
命名方法: Sophos Anti-Virus で、この種のウイルス名は "OF97/" で始まります。
例: この種のウイルスを表示する

TOP

PalmOS 実行ファイル感染型ウイルス

感染対象: PalmOS Palm リソース (PRC) ファイル
複製: この種の既存ウイルスのすべては、感染する目的で他の Palm リソースファイルを積極的に検索します。
命名方法: Sophos Anti-Virus で、この種のウイルス名は "Palm/" で始まります。

TOP

PowerPoint 97 マクロウイルス

感染対象: MS PowerPoint 97 以降、すべての OS
言語: VBA5 以降のマクロ言語
複製: あるアクションが起きた場合、ウイルスは実行され、他の PowerPoint ファイルやメインテンプレート (Blank Presentation.pot) に感染。 感染テンプレートより作成された、新しいプレゼンテーションファイルも感染します。
命名方法: Sophos Anti-Virus で、この種のウイルス名は "PM97/" で始まります。"PP97M" を使用するウイルス対策ベンダーもあります。

TOP

Unix ワーム

感染対象: Unix ネットワークに接続しているマシン
複製: Unix ワームは、バッファ・オーバーフローと呼ばれる、ネットワークコードにある脆弱性を利用して、Unix を実行している遠隔のコンピュータに未許可のアクセスを行います。 アクセス後は、感染対象にする新たなマシンの検索を開始し、しばしば、ネットワークトラフィックが増加することより、初め、その存在が認識されます。 ユーザー介入を必要としないので、この種のワームは、インターネットに常設しているマシン間で迅速に感染を広げます。
命名方法: Sophos Anti-Virus で、この種のワーム名は "Unix/" で始まります。
例: この種のワームを表示する

TOP

Visual Basic Script ウイルス

感染対象: Visual Basic スクリプトファイル、埋め込みスクリプトのある HTML ファイル、Microsoft Outlook、Internet Explorer

言語: Visual Basic Script

複製: 他の実行ファイルに多様なメカニズムで感染。VBS/Dismissed-B などのウイルスは、Outlook を使って電子メールで感染ファイルを配布。

命名方法: Sophos Anti-Virus で、この種のウイルス名は、"VBS/" で始まります。

例: この種のウイルスを表示する

TOP

Visual Basic Script ワーム

感染対象: Visual Basic スクリプトファイル、埋め込みスクリプトのある HTML ファイル、Microsoft Outlook、Internet Explorer

言語: Visual Basic Script

複製: IRC や Outlook を使って、複数のユーザーに感染ファイルのコピーを電子メール送信します。

命名方法: Sophos Anti-Virus で、この種のワーム名は "VBS/" で始まります。

例: この種のワームを表示する

TOP

Win32 実行ファイル感染型ウイルス

感染対象: MS Windows 95/98/Me/NT/2000 PE (Portable Executable) ファイル

複製: 多様な方法で、他の実行ファイルに感染。
W32/ExploreZip などのウイルスは、Outlook や他のプログラムを使って、電子メールで感染ファイルを配布したりもします。

命名方法: Sophos Anti-Virus で、この種のウイルス名は "W32/" で始まります。(旧式名として、"Win32" で始まるものもあります。)

例: この種のウイルスを表示する

TOP

Win32 ワーム

感染対象: Windows 95/98/Me/NT/2000 ネットワークに接続しているマシン

複製: Win32 ワームは、Windows ネットワーク API、MAPI 機能、あるいは Microsoft Outlook のような電子メールクライアントを使って感染を広げます。このワームプログラムが添付されたメールを作成したり、送信されるメールに自らを添付したりします。 ワームが作成したメールは、しばしば、添付ファイルを起動して、興味深いことや重要なことを見るよう受信者に促します。

命名方法: Sophos Anti-Virus で、この種のワーム名は "W32/" で始まります。"Win32" などを使用するウイルス対策ベンダーもあります。

例: この種のワームを表示する

TOP

Windows 95 実行ファイル感染型ウイルス

感染対象: MS Windows 95/98/Me PE (Portable Executable) ファイル

複製: 他の実行ファイルに感染します。メモリに常駐して、他のプログラムが実行された場合、それに感染するものもあります。 積極的に他のファイルを検出して、それに感染するウイルスもあります。
W95/Babylonia などのウイルスは、更に電子メールでも感染ファイルを配布します。

命名方法: Sophos Anti-Virus で、この種のウイルス名は "W95/" で始まります。(旧式名として、"Win95" で始まるものもあります。)

例: この種のウイルスを表示する

TOP

Windows 98 実行ファイル感染型ウイルス

感染対象: MS Windows 98 PE (Portable Executable) ファイル
複製: 他の実行ファイルに感染します。メモリに常駐して、他のプログラムが実行された場合、それに感染するものもあります。積極的に他のファイルを検出して、それに感染するウイルスもあります。
命名方法: Sophos Anti-Virus で、この種のウイルス名は "W98/" で始まります。(旧式名として、"Win98" で始まるものもあります。)
例: この種のウイルスを表示する

TOP

Windows NT 実行ファイル感染型ウイルス

感染対象: MS Windows NT/2000 PE (Portable Executable) ファイル
複製: 多種の方法を使用して、他の実行ファイルに感染します。
命名方法: Sophos Anti-Virus で、この種のウイルス名は "WNT/" で始まります。(旧式名として、"WinNT" で始まるものもあります。)

TOP

Windows 2000 実行ファイル感染型ウイルス

感染対象: MS Windows 2000 PE (Portable Executable) ファイル
複製: 他の実行ファイルに感染します。メモリに常駐して、他のプログラムが実行された場合、それに感染するものもあります。積極的に他のファイルを検出して、それに感染するウイルスもあります。
命名方法: Sophos Anti-Virus で、この種のウイルス名は "W2K/" で始まります。

TOP

Word マクロウイルス

感染対象: すべての OS にある MS Word の全バージョン
言語: Word Basic マクロ言語 (Word 6 と Word 95 で使用される。)
複製: 感染ドキュメントが開かれると、ウイルスコードを持つマクロがグローバルテンプレート (通常 NORMAL.DOT) にコピーされます。それ以外のドキュメントは、開いた際、このファイルより自動的にウイルス性マクロをロードします。
命名方法: Sophos Anti-Virus で、この種のウイルス名は "WM/" で始まります。(旧式名として、"Winword" で始まるものもあります。)
例: この種のウイルスを表示する

TOP

Word 97 マクロウイルス

感染対象: MS Word 97 以降、すべての OS
言語: VBA5 以降のマクロ言語
複製: この種のウイルスの中には、Word マクロウイルスと同様、ウイルスコードを持つマクロをグローバルテンプレート (通常 NORMAL.DOT) にコピーするものもあります。しかし、この感染方法は、MS Office 97 SR1 以降では作動しません。
最近のこの種のウイルスの大半は、ウイルスコードのあるマクロを他のファイルにコピーし、別のドキュメントを開いた際、それを取り入れるため、グローバルテンプレートに変更を加えます。
命名方法: Sophos Anti-Virus で、これらのウイルス名は、"WM97/" で始まります。"W97M" を使用するウイルス対策ベンダーもあります。
例: この種のウイルスを表示する

TOP

Word 97 マクロワーム

感染対象: MS Word 97 以降、すべての OS

言語: VBA5 以降のマクロ言語

複製: MS Outlook などのメールプログラムを使用して、アドレス帳にあるメールアドレスに、自動的に感染ファイルを送信します。この種のワームの多くは、Word 97 マクロウイルスと同様の方法で複製します。

命名方法: Sophos Anti-Virus で、これらのワーム名は、"WM97/" で始まります。"W97M" を使用するウイルス対策ベンダーもあります。

例: この種のワームを表示する

TOP

Word 2001 マクロウイルス

感染対象: Apple マシン上の MS Word 2001

言語: VBA6 以降のマクロ言語

複製: この種のウイルスの中には、Word マクロウイルスと同様、ウイルスコードを持つマクロをグローバルテンプレート(通常 NORMAL.DOT)にコピーするものもあります。これらのウイルスの大半は、既存の Word 97 ウイルスが Word 2001 でも作動するように変換されたものです。しかし、たいがいのペイロードは Intel 特有であり、作動しません。

命名方法: Sophos Anti-Virus で、この種のウイルス名は "WM97/" で始まります。"W97M" を使用するウイルス対策ベンダーもあります。

TOP

恐怖メール

説明: 起きるかもしれない脅威に対して、大袈裟に警鐘を鳴らす警告メッセージ。

TOP

誤警告

説明: ファイルがウイルス感染している、という誤った報告。

TOP

誤解

説明: しばしば、誤ってコンピュータウイルスに関連付けられ問題。

TOP

コンパニオンウイルス

感染対象: すべての OS

複製: コンパニオンウイルスは、自分自身、あるいはターゲットのファイルのファイル名を変更し、ユーザーに、正規のプログラムでなく、ウイルス自身を実行させようとします。例えば、GAME.EXE というファイルを攻撃しているコンパニオンウイルスは、そのファイル名を GAME.EX に変更し、自らのコピーを GAME.EXE という名前で作成します。または、単に、自らの名前を GAME.COM に変更して、ユーザーがコマンドラインから 'GAME' を実行することを見込む場合もあります。OS は、GAME.EXE でなく、GAME.COM を実行します。

命名方法: この種のウイルスに関する標準の命名法はありません。

例: この種のウイルスを表示する

TOP

ジャンクデータ

説明: 様々な理由から、ウイルスとして機能しなくなったファイル。Sophos Anti-Virus は、統一性を保つため、この種のファイルを検出します。

命名方法: Sophos Anti-Virus で、この種のファイル名は "Junk/" で始まります。

TOP

ジョーク

感染対象: ウイルスやトロイの木馬と間違われる可能性のある、無害なジョークプログラム。

複製: 複製しない。

命名方法: Sophos Anti-Virus で、この種のファイル名は "Joke/" で始まります。

例: この種のプログラムを表示する

TOP

チェーンレター

説明: 受信したメールを他のユーザーに転送するよう促すメール。

TOP

テストファイル

感染対象: ウイルス対策ソフトのテストに使用される標準ファイル。

複製: 複製しない。

TOP

デマウイルス

説明: 存在しないウイルスに対する警告。通常、知っている人すべてに警告を転送するよう促します。

TOP

トロイの木馬

感染対象: 本来の目的を隠して、ゲームやソフトウェアのアップデート版のように見せかける悪質なプログラム。ゲームのように見えるプログラムが、ファイルを削除したり、システムにウイルス感染したり、システムセキュリティを弱めたりする場合もあります。

複製: 複製しない。

命名方法: Sophos Anti-Virus で、この種のウイルス名は "Troj/" で始まります。

例: トロイの木馬を表示する

TOP

ドロッパー

説明: システムに、ウイルス、ワーム、あるいはトロイの木馬を置くために、特別に作成されるファイル。ファイルの種類は、ウイルス、ワーム、あるいはトロイの木馬とは違う場合もあります。

命名方法: この種のウイルスに関する標準の命名法はありません。

TOP

バッチファイル感染型ワーム

感染対象: DOS、Windows 95/98/Me/NT/2000 ネットワークに接続しているマシン

複製: バッチファイルワームは、遠隔マシンの共有エリアを探し、それに自らをコピーして感染を広げます。

命名方法: Sophos Anti-Virus で、この種のワーム名は、"Bat/" で始まります。

例: この種のワームを表示する

マスターブートセクタ感染型ウイルス

感染対象: ハードディスクのマスターブートセクタ (別名、マスターブートレコード) と、フロッピーディスクのブートセクタ。
フロッピードライブから起動するように設定されている Intel 互換性の PC すべてに感染可能です。
Windows NT のように、より安全な OS には感染可能ではあるが、ウイルスの複製を妨げることが考えられます。

言語: Intel 80x86 アセンブラ

複製: 感染マシンが起動した際、メモリにロードし、その後、マシンで使用するフロッピーディスクすべてに感染します。感染フロッピーディスクを使って起動したマシンは、感染してしまいます。
フロッピードライブから起動できないようにマシンの BIOS 設定を変更した場合、この種のウイルスはマシンに感染できません。

命名方法: この種のウイルスに関する標準の命名法はありません。

例: この種のウイルスを表示する

TOP

参照:

- わかりやすいコンピュータウイルス [PDF]
- ウイルス情報:ウイルス解析
- ウイルス情報:ニュース

TOP

2002年1月に Sophos に報告されたウイルスのトップ10

順位	前月の順位	ウイルス名	割合
1	1	W32/Badtrans-B	61.1%
2	新規	W32/MyParty-A	4.3%
3	3	W32/Magistr-B	3.6%
4	4	W32/Sircam-A	2.9%
5	7=	W32/Nimda-A	2.3%
6	新規	W32/Maldal-G	1.6%
7	5	W32/Magistr-A	1.4%
8=	再規	W32/Gokar-A	1.3%
8=	新規	W32/Klez-E	1.3%
10	7=	W32/Nimda-D	1.0%
その他			19.2%

- トップ10ウイルスの画像 (GIF、EPS)
- 自社 Web サイトに、ライブウイルス情報を掲載する

月ごとのトップ10ウイルス

2002 年 1 月 OK

6ヶ月ごと、または1年ごとのトップ10ウイルス

2001年に Sophos に報告されたウイルスのトップ10 OK

TOP

クイック検索 Go

SOPHOS ANTI-VIRUS

ウイルス情報 ホーム 検索 お問い合わせ

ホーム ➤ ウイルス情報 ➤ ウイルス情報フィード

ウイルス情報フィード

Web サイトに最新のウイルス、トロイの木馬、ワーム情報を掲載する？
Sophos Anti-Virus のウイルス情報フィードを利用すれば、ご自分の Web サイトに、ウイルス脅威に関する、便利で最新の情報を簡単に掲載することができます。

また、このサービスは無料となっています！

最新ウイルス警告10種類	
2月8日	XM97/Divi-AQ
2月7日	W32/Klez-G
2月6日	WM97/Comical-A
2月5日	W32/Tariprox-B
1月30日	WM97/Jedi-P
1月28日	Troj/Msstake-A
1月28日	Troj/Download-A
1月28日	VBS/Haptime-Fam
1月28日	W32/MyParty-A
1月25日	WM97/Falcon-A
資料提供：Sophos Anti-Virus	
この情報を自分のサイトに追加する	

2002年1月 トップ5ウイルス	
1	W32/Badtrans-B
2	W32/MyParty-A
3	W32/Magistr-B
4	W32/Sircam-A
5	W32/Nimda-A
資料提供：Sophos Anti-Virus	
この情報を自分のサイトに追加する	

最新ウイルス警告5種類	
2月8日	XM97/Divi-AQ
2月7日	W32/Klez-G
2月6日	WM97/Comical-A
2月5日	W32/Tariprox-B
1月30日	WM97/Jedi-P
資料提供：Sophos Anti-Virus	
この情報を自分のサイトに追加する	

2002年1月 トップ10ウイルス	
1	W32/Badtrans-B
2	W32/MyParty-A
3	W32/Magistr-B
4	W32/Sircam-A
5	W32/Nimda-A
6	W32/Maldal-G
7	W32/Magistr-A
8=	W32/Gokar-A
8=	W32/Klez-E
10	W32/Nimda-D
資料提供：Sophos Anti-Virus	
この情報を自分のサイトに追加する	

ウイルス情報フィードについて

以下のボタンをクリックして、登録フォームにご入力いただきますと、簡単な HTML コードを電子メールで送信致します。また、お好みの色や外観で、ご自分のサイトに最新ウイルス情報を含める方法もご案内致します。

一度、このコードをご自分の Web サイトに導入すれば、それで操作は終わりです！
ウイルス情報は、最新のもので自動的にアップデートされます。

現在、以下の2種類のウイルス情報をご自分の Web サイトに掲載できます：

- 最新ウイルス警告
- 先月、最も報告件数の多かったウイルス

W32/Badtrans-B

別名

I-Worm.BadtransII, WORM_BADTRANS.B

種類

Win32 ワーム

検出

ウイルスに対する保護を提供する、ウイルス ID（IDE ファイル）は、**最新のウイルス ID** ページよりご利用になれます。このウイルス ID は、Sophos Anti-Virus 2002年1月 (3.53) バージョンに組み込まれました。

弊社では、このワームのユーザー環境での感染報告を多数受けております。

詳細

W32/Badtrans-B は MAPI を使用して感染を広げる電子メール送信型ワームで、自らを、本文のない電子メールとして、感染マシンにある電子メールアドレスに送信します。

ワームは、自らを送信するためのアドレスを、アドレス帳より探します。更に、インターネットのキャッシュフォルダ、及び "マイ ドキュメント" フォルダにある Web ページ内も探します。

感染マシンにあるメールに返信する場合、ワームは、そのメールの From: フィールドに、感染ユーザーのアドレスを使用します。それ以外の場合は、以下のいずれかのアドレスを使用します:

" Anna" <aizzo@home.com>
"JUDY" <JUJUB271@AOL.COM>
"Rita Tulliani" <powerpuff@videotron.ca>
"Tina" <tina0828@yahoo.com>
"Kelly Andersen" <Gravity49@aol.com>
" Andy" <andy@hweb-media.com>
"Linda" <lgonzal@hotmail.com>
"Mon S" <spiderroll@hotmail.com>
"Joanna" <joanna@mail.utexas.edu>
"JESSICA BENAVIDES" <jessica@aol.com>
" Administrator" <administrator@border.net>
" Admin" <admin@gte.net>
"Support" <support@cyberramp.net>
"Monika Prado" <monika@telia.com>
"Mary L. Adams" <mary@c-com.net>

この電子メールは、Outlook Express 5 の一部のバージョンにある既知の脆弱性を利用して、添付ファイルを自動的に実行します。Microsoft 社は、この脆弱性に対応するパッチをリリースしています:
http://www.microsoft.com/japan/technet/security/frame_prekb.asp?sec_cd=MS01-027 よりダウンロード可能です。（このパッチは、このワームが利用する脆弱性を含む、Microsoft 社製品にある複数の脆弱性を修正します。）

ワームは、感染マシン上のメールを読んで、それに "返信" することによって件名を作成します。例:

Re: <感染マシンにあるメールを読んで取得した件名;

電子メールアドレスが、インターネットのキャッシュフォルダや "マイ ドキュメント" フォルダにある Web ページにて見つけたものの場合、件名は、単に、"Re:" となります。

このワームは、感染した添付ファイルのファイル名を、3つの構成部分から任意に作成します。最初の部分は、以下のリストより選択されます:

CARD
DOCS
FUN
HAMSTER
NEWS_DOC
HUMOR
IMAGES
info
ME_NUDE
New_Napster_Site
PICS
README
S3MSONG
SEARCHURL
SETUP
Sorry_about_yesterday
stuff
YOU_ARE_FAT!

2番目の部分は、以下のリストより選択されます:

.DOC.
.MP3.
.ZIP.

(なお、ワーム内にバグがあるため、".ZIP." が選択されることはありません。)

最後の部分は、以下のリストより選択されます:

pif
scr

結果として、添付ファイルのファイル名の種類は多数に上ります。例:

card.DOC.pif
docs.DOC.pif
fun.MP3.pif
HAMSTER.DOC.PIF
Humor.MP3.scr
IMAGES.DOC.pif
Me_nude.MP3.scr
New_Napster_Site.MP3.pif
Pics.DOC.scr
README.MP3.scr
S3MSONG.DOC.scr
SEARCHURL.MP3.pif
SETUP.DOC.scr
Sorry_about_yesterday.MP3.pif
Sorry_about_yesterday.MP3.scr
stuff.MP3.pif

YOU_ARE_FAT!.DOC.pif
YOU_are_FAT!.MP3.scr

添付ファイルが実行された場合、ワームは自身を Windows **ディレクトリや** Windows **のシステムディレクトリへ** kernel32.exe **というファイル名でコピーし、レジストリキー** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce **を変更して、次回** Windows **が起動した際に、このワームが実行されるように設定します。なお、ワームが、**Windows **や** Windows **のシステムディレクトリに自らのコピーを作成していない場合、このレジストリキーは、元の添付ファイルを指定します。**

また、ワームは、 kdll.dll **という名前のファイルをドロップ（作成）します。これは、パスワードを盗むトロイの木馬、** Troj/PWS-AV **です。**

W32/Badtrans-B **は、トロイの木馬** Troj/PWS-AV **を使用して、**Windows **システムディレクトリ内の** cp_25389.nls **というファイルに、ユーザーのキー操作をログします。このログは暗号化される場合があります。**

W32/Badtrans-B **は、このログを、以下のメールアドレスのいずれかに送信しようとします：**

ZVDOHYIK@yahoo.com
udtzqccc@yahoo.com
DTCELACB@yahoo.com
I1MCH2TH@yahoo.com
WPADJQ12@yahoo.com
fjshd@rambler.ru
smr@eurosport.com
bgnd2@canada.com
muwripa@fairesuivre.com
rmxqpey@latemodels.com
eccles@ballsy.net
suck_my_prick@ijustgotfired.com
suck_my_prick4@ukr.net
thisisno_fucking_good@usa.com
S_Mentis@mail-x-change.com
YJPFJTGZ@excite.com
JGQZCD@excite.com
XHZJ3@excite.com
OZUNYLRL@excite.com
tsnlqd@excite.com
cxkawog@krovatka.net
ssdn@myrealbox.com

駆除

W32/Badtrans-B **の除去方法をご覧ください。**

参照：

- **新種ユーザー環境ウイルス、無料通知サービスに登録する**
- **自社** Web **サイトに、ライブウイルス情報を掲載する**

W32/Goner-A

別名

I-Worm.Goner, Gone, W32/Goner@MM, Pentagone, pentagon

種類

Win32 ワーム

検出

ウイルスに対する保護を提供する、ウイルス ID（IDE ファイル）は、**最新のウイルス ID** ページよりご利用になれます。このウイルス ID は、Sophos Anti-Virus 2002 年1月 (3.53) バージョンに組み込まれました。

弊社では、このワームのユーザー環境での感染報告を多数受けております。

ご注意：Sophos Anti-Virus は、2001年12月5日 0時45分より W32/Goner-A を検出しています。この IDE ファイルは、このワームがドロップ（作成）する mIRC スクリプトも検出するよう、2001年12月5日 21時00分に更新されました。

詳細

W32/Goner-A は、GONE.SCR という添付ファイルとして、電子メールを経由して感染を拡大します。このファイル名は、スクリーンセーバー装うために使用されています。このワームは、以下の特徴を持った電子メールとして到着します：

件名：Hi

本文：
How are you ?
When I saw this screen saver, I immediately thought about you I am in a harry, I promise you will love it!

W32/Goner-A は、感染したマシンにインストールされているアンチウイルス製品を無効にしようとします。これは、以下のプロセスを探し出すことにより、実行します：

_AVP32.EXE,
_AVPCC.EXE,
_AVPM.EXE,
APLICA32.EXE,
AVCONSOL.EXE,
AVP.EXE,
AVP32.EXE,
AVPCC.EXE,
AVPM.EXE,
CFIADMIN.EXE,
CFIAUDIT.EXE,
CFINET.EXE
CFINET32.EXE,
ESAFE.EXE,
FRW.EXE,
IAMAPP.EXE
IAMSERV.EXE
ICLOAD95.EXE,
ICLOADNT.EXE,
ICMON.EXE,
ICSUPP95.EXE,
ICSUPPNT.EXE,
LOCKDOWN2000.EXE,
NAVAPW32.EXE,
NAVW32.EXE,
PCFWallIcon.EXE,
TDS2-98.EXE,
TDS2-NT.EXE,
SAFEWEB.EXE.
VSHWIN32.EXE,
VSECOMR.EXE,
VSSTAT.EXE,
WEBSCANX.EXE,
ZONEALARM.EXE.

上記プロセスのいずれかを探し出した場合、そのプロセスを停止するよう試みます。また、ワームは、これらの名前のファイルを含んだディレクトリ内にあるすべてのファイルを削除しようとします。そして Windows が次回起動する際に、残っているファイルをすべて削除するよう、wininit.ini というファイルを作成します。

弊社では、感染したマシン上の Sophos Anti-Virus が最新のバージョンで、それが正しく動作しているかを確認するよう推奨しています。

このワームは C:\SAFEWEB\ にあるすべてのファイルを削除します。

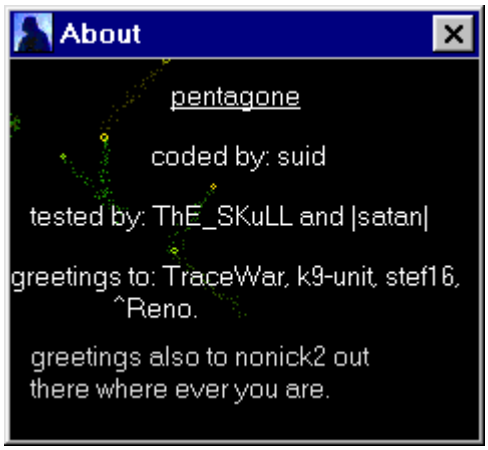
また、インターネット・リレー・チャット クライアントである mIRC にも感染します。REMOTE32.INI という名の mIRC スクリプトファイルを mIRC フォルダへドロップ（作成）し、感染したユーザーが mIRC を使用した際に、REMOTE32.INI 内にあるスクリプトが起動されるよう MIRC.INI ファイルへセクションを追加します。

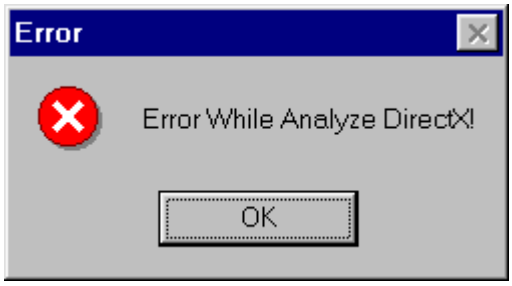
また、メッセージプログラムである ICQ も感染の手段として使用されます。

更にワームは gone.scr というファイル名で自身のコピーを Windows のシステムディレクトリに作成します。Windows が再起動されるたびに毎回実行されるよう、ワームは、自身のファイル名を含むレジストリキーを以下に作成します。

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

ワームが初めて実行されると、短いメッセージを含む画像に続いて、偽りのエラーメッセージが表示されます。これは、受け取ったスクリーン・セーバーは本物で、何らかの理由で実行が中断されたと思わせるよう、ファイルを受信したユーザーをだますためのものです。





駆除

W32/Goner-A の除去方法をご覧下さい。

参照:

- 新種ユーザー環境ウイルス、無料通知サービスに登録する
- 自社 Web サイトに、ライブウイルス情報を掲載する

クイック検索 Go

SOPHOS ANTI-VIRUS

JS/Gigger-A

種類

JavaScript ウイルス

検出

ウイルスに対する保護を提供する、ウイルス ID（IDE ファイル）は、**最新のウイルス ID** ページよりご利用になれます。このウイルス ID は、Sophos Anti-Virus 2002 年3月 (3.55) バージョンに組み込まれます。

現時点で、弊社へのユーザー環境感染報告は、一件にとどまっています。

詳細

JS/Gigger-A は JavaScript ウイルスで、以下のいずれかの特徴を持った電子メールとして到着します：

件名：Outlook Express Update
本文：MSNSofware Co.
添付ファイル：Mmsn_offline.htm

または、

件名：*recipient@Address*（つまり、受信者のメールアドレス）
本文：Microsoft Outlook 98.
添付ファイル：Mmsn_offline.htm

実行されると、ウイルスは、以下のファイルを作成しようとします：

C:\Bla.hta
C:\B.htm
C:\Windows\Samples\Wsh\Charts.js
C:\Windows\Samples\Wsh\Charts.vbs
C:\Windows\Help\Mmsn_offline.htm

また、拡張子が INI または HLP であるファイルが含まれるフォルダに、Script.ini というファイルを作成します。 これらのファイルは、mIRC/Simp-Fam として検出されます。

ウイルスは、HTM、HTML、ASP ファイルに感染し、また、以下の行を C:\Autoexec.bat に追加しようとします：

Echo y|format c:

これにより、文字「Y」を「Yes」として使用している Windows のバージョンで、起動時に C: ドライブのフォーマットを実行しようとします。

JS/Gigger-A は、ユーザーのアドレス帳内のすべての宛先に自身を送信し、以下のレジストリキーを作成します：

HKCU\Software\Microsoft\Windows Scripting Host\Settings\Timeout
HKCU\Software\TheGrave\badUsers\v2.0

そして、'NAV DefAlert' という値を以下のレジストリに追加します：

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

このウイルスには、"This virus is donation from all Bulgarians" という文が含まれています。

参照：

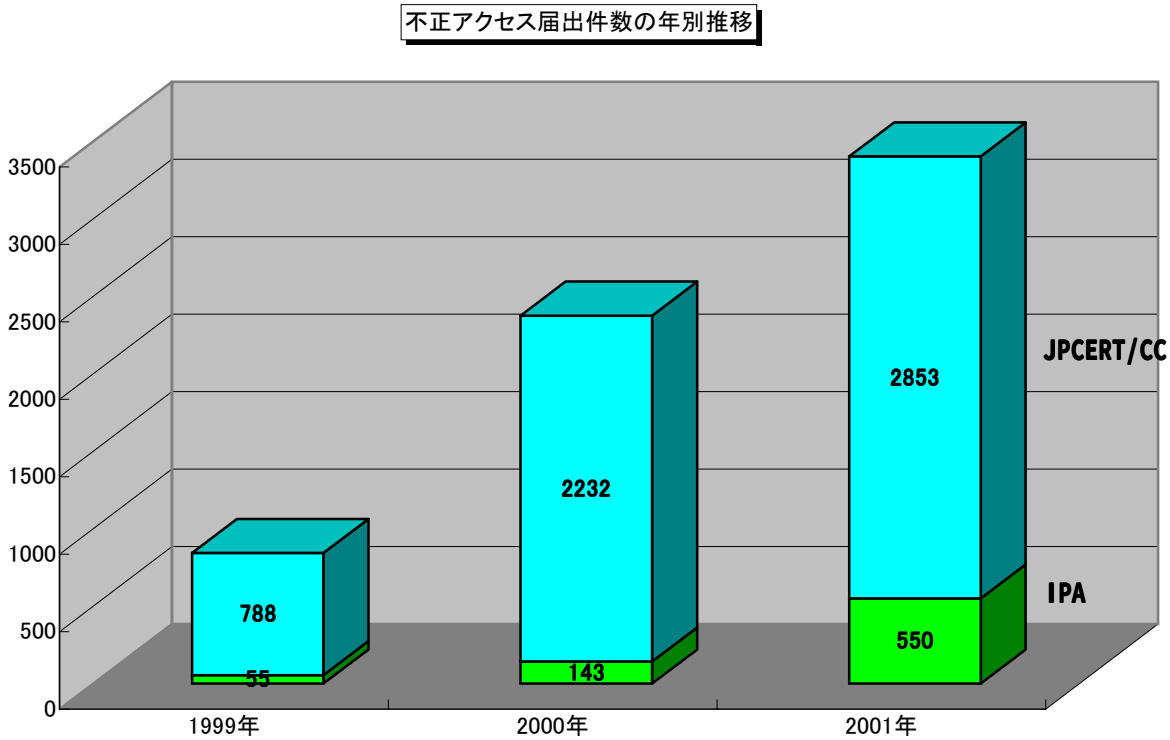
2001 年不正アクセス届出状況

2002 年 2 月 1 日
情報処理振興事業協会
セキュリティセンター(IPA/ISEC)

情報処理振興事業協会（略称ＩＰＡ・村岡茂生理事長）は、2001 年 1 月～12 月の不正アクセス届出データを集計した。

1.届出件数

2001 年の年間届出件数は 550 件となり、前年（2000 年）の届出件数 143 件に対して約 3.8 倍まで急増した。増加の要因としては、個人ユーザの常時接続環境の普及やワームの出現によるものと推測される。なお、下記グラフは、過去 3 年間に IPA セキュリティセンター及びコンピュータセキュリティインシデント報告の受付窓口となっている JPCERT/CC*1 が受け付けた届出件数注 1) の推移を示したものである。



*1) JPCERT/CC: コンピュータ緊急対応センター(http://www.jpcert.or.jp)
コンピュータセキュリティインシデントについて、報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討と助言などを、技術的な立場から行なっている民間の非営利団体。また、Scan 等の弱点探索に関する情報も傾向分析しており、Web やメーリングリストによりその情報を公開している。

注 1)上記グラフの件数は、受付基準が異なる IPA 及び JPCERT/CC が受け付けた届出・報告の件数であり、実際のアタックの発生件数や、被害件数を類推できるような数値ではない。

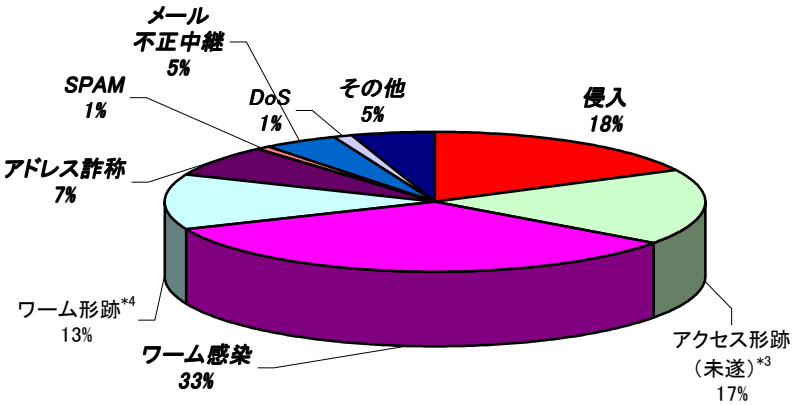
IPA と JPCERT/CC は、「情報セキュリティ・インシデントへの組織的対応セミナー」の共同開催や情報化月間の時期に IPA が経済産業省と共催で実施している「情報セキュリティセミナー」に講師として参加してもらうなど、相互に協力し、日本国内におけるインシデントマネジメントに関する情報提供やユーザに対する、普及啓発等を行っている。

以下、IPA への届出内容について述べる。

2.届出種別

IPA に届けられた 550 件のうち実際に被害に及んだケースが**約７割**に及んでいる。特に 2001 年は Sadmind/IIS、CodeRed、Nimda など既知の**セキュリティホール**[*2]を悪用したワームの出現により、ワーム感染及びワーム形跡（未感染）に関するものが全体の**約 46%**を占め、不正アクセス届出増加の要因の一つとなっており、今後新たな脅威として捉える必要がある。

2001年不正アクセス届出状況



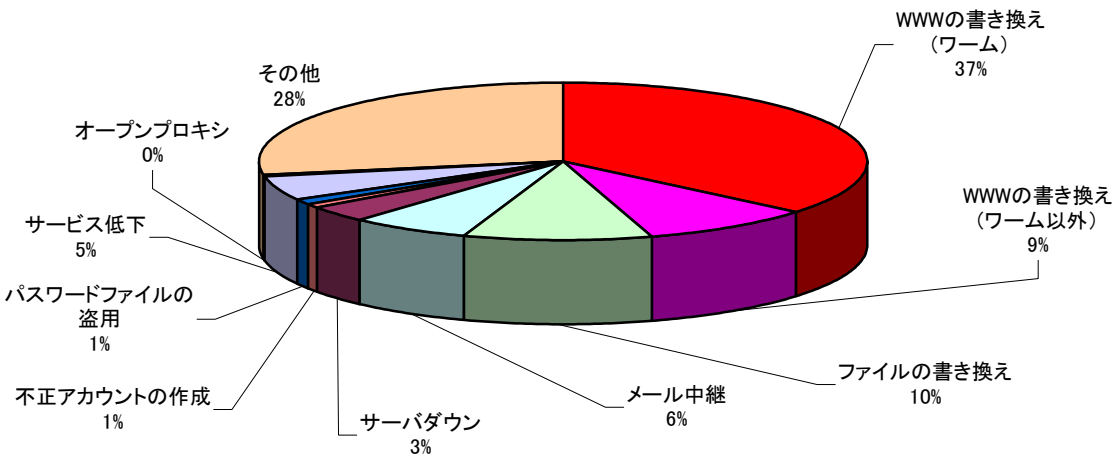
届出種別	2000 年	2001 年
侵入	43	97
アクセス形跡（未遂）*3	24	96
ワーム感染	0	184
ワーム形跡*4	0	71
アドレス詐称	26	39
SPAM	3	5
メール不正中継	41	25
DoS(サービス妨害)	6	5
その他	4	28
合計*5	147	550

*2) セキュリティホール:アプリケーションのセキュリティ上の欠陥
*3) 「アクセス形跡（未遂）」はサーバのログやファイアウォールのログに不正アクセスの痕跡があったもの
*4) 「ワーム形跡」はワームによるアクセスを検知したが、感染の被害を受けなかったもの
*5) 届出種別の合計は種別の重複があるため届出件数とは必ずしも一致しない

3.被害内容

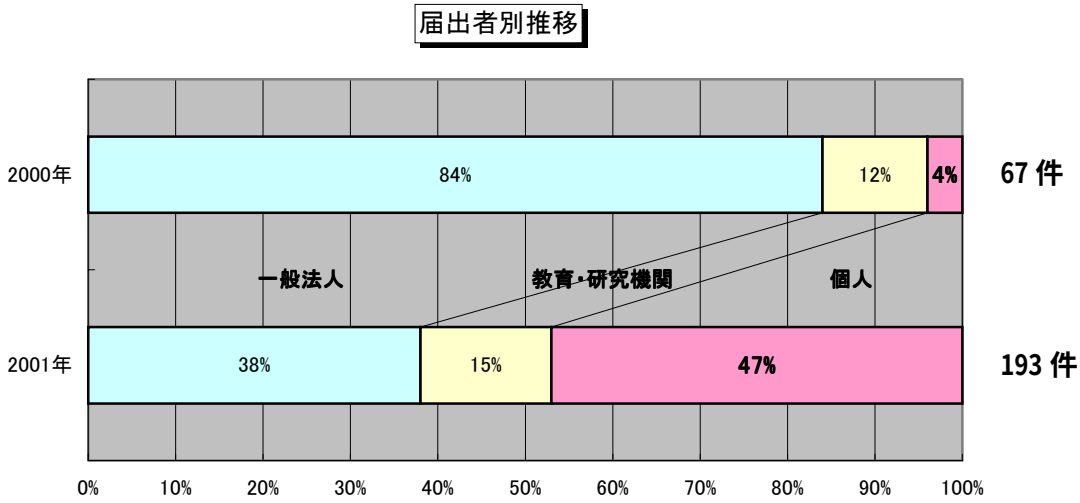
届出のうち実際に被害に及んだケースに関する被害内容の分類である。**半数近くが WWW サーバの書き換え**の被害であり、その要因としては、やはり**ワーム感染**によるものが多く、全体の約４割を占める。ワームに感染した場合には、自らが感染元となり、**被害者から加害者へ立場が逆転する場合もある**事を理解する必要がある。

2001年被害内容分類



4.届出者の分類

侵入及びアクセス形跡における届出者別の内訳は、**個人からの届出の割合が 2000 年の 4%から 2001 年は一気に 47%まで増加した**。その要因として、個人ユーザにおける ADSL などの常時接続環境の普及と**パーソナルファイアウォール**[*6] の普及が背景にあると考えられる。



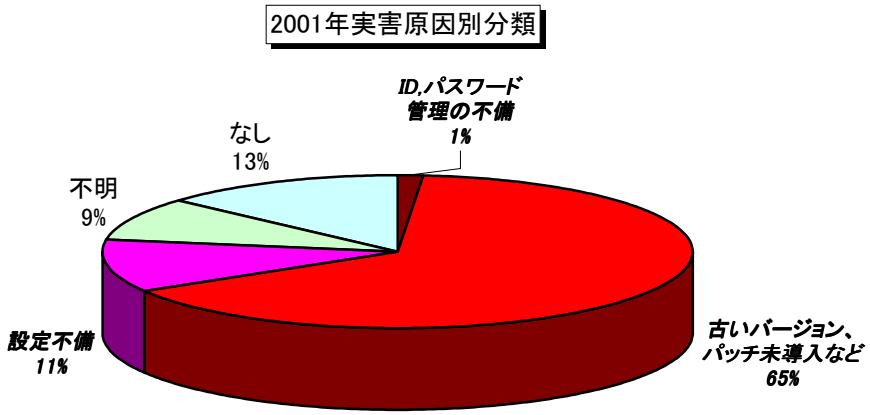
しかし、これらはパーソナルファイアウォール等により対策を施していたため、そのログデータにより不正アクセスに気づいた例であり、**何ら対策を行っていない場合には気づかないケースが多い**と推測される。

よって、特に常時接続環境においては個人ユーザでも不正アクセスの危険にさらされているという認識を持ち、**パーソナルファイアウォールなどによる対策は必須**である。

＊6）パーソナルファイアウォール：
個人のコンピュータがネットワークを介して外部から不正に操作されたり侵入されたりする事を防ぐためのソフトウェア又はハードウェアのこと。最近では、ウイルス対策用のソフトと一体で販売されている事が多い。

5.被害原因

実際に被害にあった届出を原因別分類に見ると、**「古いバージョン、パッチ未導入など」「設定不備」など基本的な(既知の)対策をとっていれば被害を未然に防げたケースが全体の約 8 割**を占めた。特にワーム感染においては、Microsoft 社の IIS[*7] (Web サーバ) や Internet Explorer(ブラウザ)などのセキュリティホールが原因の被害が多かった。



従って、今後の不正アクセス対策として、システム管理者はサーバにインストールされている OS やアプリケーションに関する**セキュリティ情報の収集**及び**セキュリティパッチ**[*8] **適用**と**設定見直し**が必須である。（対策方法については「6．対策情報　システム管理者向け」参照のこと）

また、個人ユーザにおいても**ブラウザなどのバージョンを確認**し、**バージョンアップ**と**セキュリティ設定の確認**が必要である。また、ワクチンソフトなどのアプリケーションについてもコンピュータにプレインストールされたままの状態やインストールしただけの状態ではなく、**パターンファイル等の更新（アップデート）**が必要である。（対策方法については「6．対策情報　エンドユーザ・ホームユーザ向け」参照のこと）

*7)IIS:Internet Information Server 又は Service の略

*8)セキュリティパッチ:セキュリティ上の欠陥を修復するプログラム

6．対策情報

上述のように、基本的な(既知の)対策をとっていなかったために被害にあってしまったものが多くなっている。下記ページなどを参照し、今一度状況確認・対処されたい。

システム管理者向け

- 「セキュリティ対策セルフチェックシート」
  http://www.ipa.go.jp/security/ciadr/checksheet.html
- 「コンピュータ不正アクセス被害防止対策集」
  http://www.ipa.go.jp/security/ciadr/cm01.html
- 「セキュリティ脆弱性情報」
  http://www.ipa.go.jp/security/news/news.html

エンドユーザ・ホームユーザ向け

- 「個人ユーザの Web サーフィン、メール利用などに係わる脅威（危険性）に対する対策」
  http://www.ipa.go.jp/security/ciadr/cm01.html#user
- Internet Explorer のバージョンアップ方法
  Windows Update にアクセスして最新のバージョンにする。又は
  「ホームユーザ向けセキュリティ対策早分かりガイド」よりダウンロードする。
  http://www.microsoft.com/Japan/enable/products/security/verslist.asp?prod=032
- Microsoft 社製品セキュリティ対策情報　「ホームユーザ向けセキュリティ対策早分かりガイド」
  http://www.asia.microsoft.com/japan/enable/products/security/

ウイルス対策を含むセキュリティ関係の情報・対策などについては、下記ページを参照のこと。
「IPA セキュリティセンタートップページ」
http://www.ipa.go.jp/security/

2002年 2月 7日
情報処理振興事業協会
セキュリティセンター(IPA/ISEC)

コンピュータウイルスの届出状況について

1. 2002年 1月のウイルス届出状況

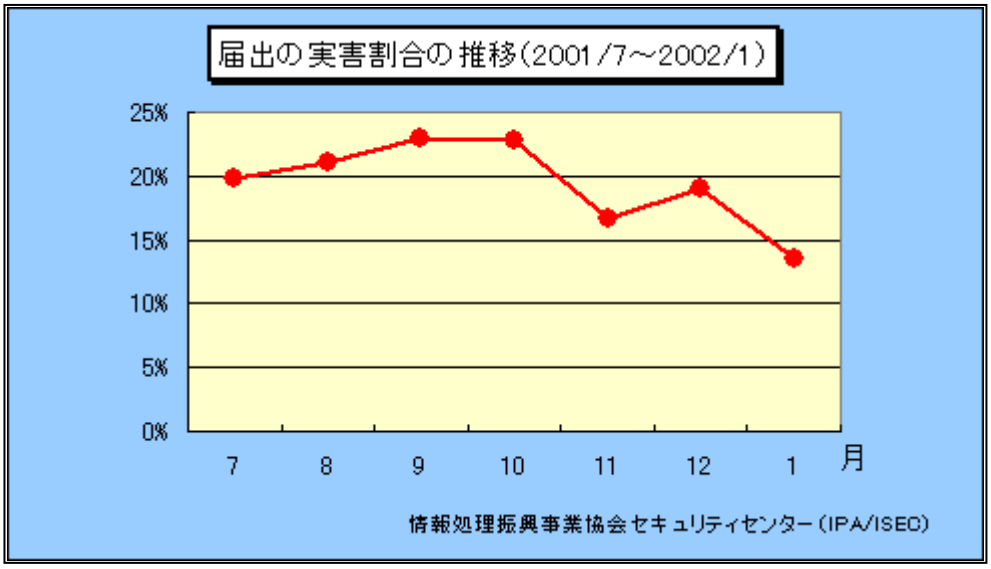
情報処理振興事業協会セキュリティセンターは、2002年 1月の届出状況をまとめた。

1月の届出件数は**2,283件**と昨年の月平均（2,021件）を上回っており、引き続き高水準となっている。

2. 今月の特記事項

W32/Badtrans蔓延状況続くが実害率は減少傾向へ！！

昨年末猛威を振るった**W32/Badtransウイルスの亜種は、1月も1,381件**（12月2,701件）と届出全体の6割を占めており、依然として蔓延している状況が伺える。
しかし、**実害率は14.3%と12月の20.1%から5.8ポイント減少**しており、セキュリティホールの解消などの対策が浸透してきている状況が伺える。**1月の届出全体の実害率も13.6%（12月19%）**と2,000件を超えた月（過去7回）のうち最低の数値となった。



図：W32/Badtarnsのウイルスメールのプレビュー画面

ホームページアドレスに見せかけたW32/Myparty ウイルス出現

このウイルスは、添付ファイル名が『www.myparty.yahoo.com』で**リンクのように見える**ため、つい開いてしまうケースが見受けられる。
添付ファイルを開くと感染し、ウイルスを添付したメールが送信される。このような**添付ファイルの見た目に騙されうっかり開かないよう**十分注意されたい。

W32/Mypartyのメール受信画面の一例

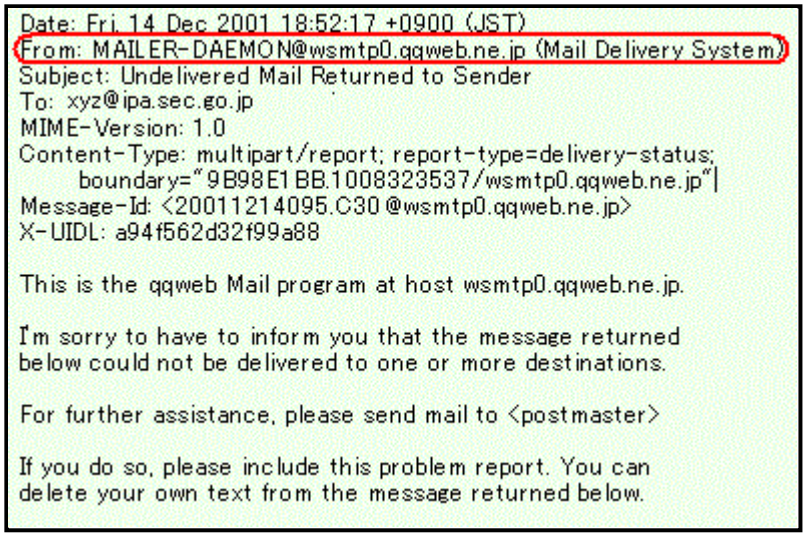
今月の呼びかけ：「ウイルス感染の兆候を見逃すな！！」
ーワクチンソフトで確認をー

メール機能悪用ウイルスに感染すると、たちまち**被害者からメールをばら撒く加害者に**なってしまうので、早急に修復を行う必要がある。
下記のような感染の兆候が現れた場合、**最新のウイルス検出データファイル（※）に更新したワクチンソフトによる検査**を行い、ただちにウイルス名を特定し、対処することが肝要である。
また、**更新は日頃から最低週1回**は行うべきである。（企業においては毎日更新や、1時間ごとに更新トライを行っている例もある。）

※ウイルス検出データファイルは、メーカーにより「定義ファイル」、「パターンファイル」、「シグネチャファイル」など呼び名が 異なるので、マニュアル等を参照されたし。

感染の兆候例：「MAILER-DAEMON」というメールアドレスからメールが**数多く届く**。

このような**不達の案内のメールが数多く届くとき**は、ウイルスが自動的に送信した メールが宛先不明で返信されたケースがほとんどである。
なお、メール機能悪用ウイルスの多くは、 メールソフトの送信記録に履歴を残さないので、 ユーザにとってはウイルスが送信したことを確認できない。


Date: Fri, 14 Dec 2001 18:52:17 +0900 (JST)
From: MAILER-DAEMON@wsmtp0.qqweb.ne.jp (Mail Delivery System)
Subject: Undelivered Mail Returned to Sender
To: xyz@ipa.sec.go.jp
MIME-Version: 1.0
Content-Type: multipart/report; report-type=delivery-status;
boundary="9B98E1BB.1008323537/wsmtp0.qqweb.ne.jp"
Message-Id: <20011214095.C30@wsmtp0.qqweb.ne.jp>
X-UIDL: a94f562d32f99a88

This is the qqweb Mail program at host wsmtp0.qqweb.ne.jp.

I'm sorry to have to inform you that the message returned
below could not be delivered to one or more destinations.

For further assistance, please send mail to <postmaster>

If you do so, please include this problem report. You can
delete your own text from the message returned below.

「MAILERーDAEMON」から送信されたメール受信画面

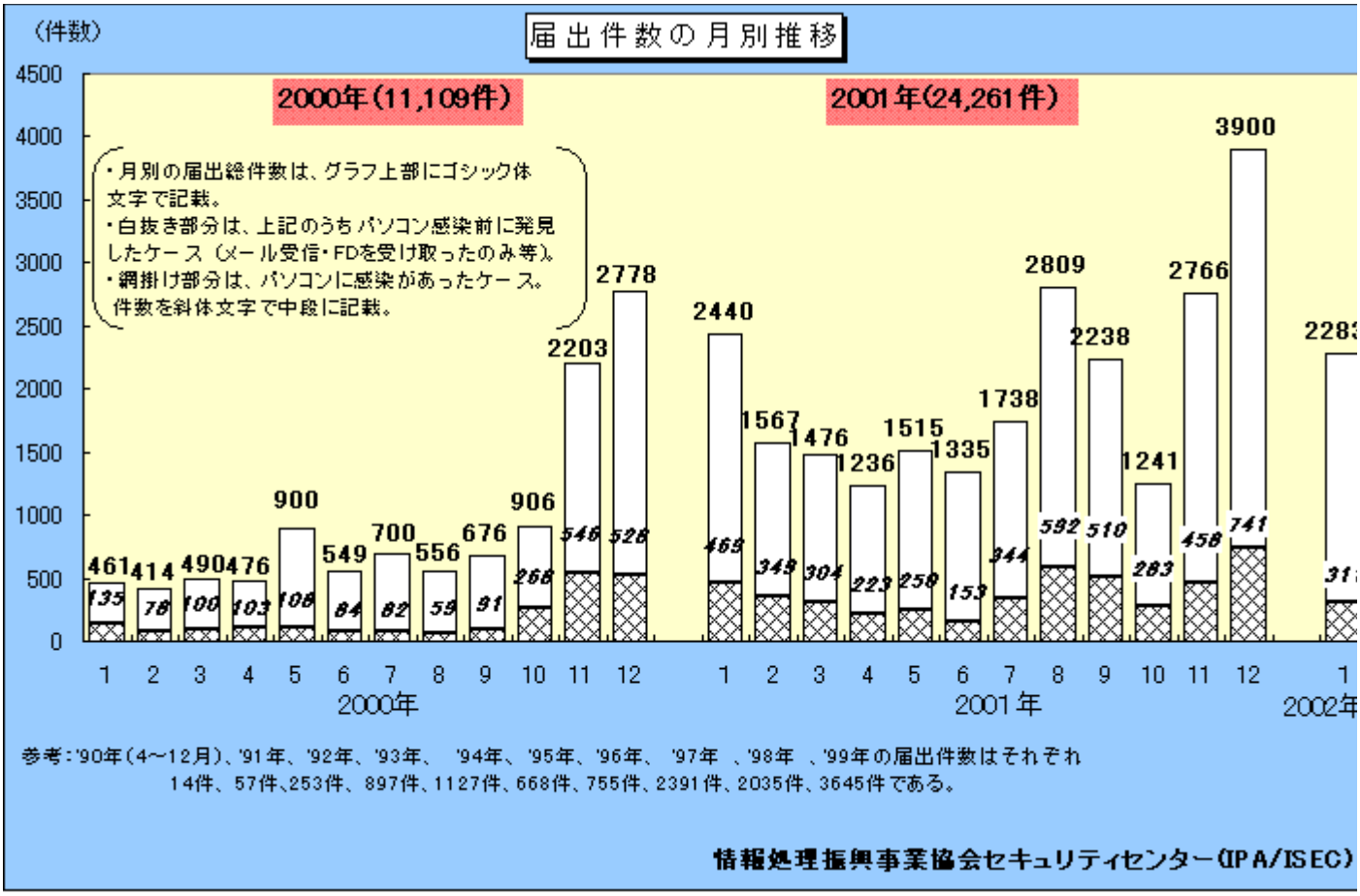
その他のよくある感染の兆候：

1.パソコンを起動するとダイアルアップ接続の画面が表示され、**何度も**インターネットに接続しようとする。

2.メールの送受信に**異常に**時間がかかるようになった。

3.ホームページを見ているときやアプリケーションを起動したとき、**頻繁に**強制終了が発生するようになった。

3. ウイルス届出の詳細



1) 1月、届出のあったウイルスは37種類であった。
(Windows、DOS及びUNIXウイルス2,174件、マクロウイルス及びスクリプトウイルス109件、Macintoshウイルスが0件。)(※)印は、1月の新種ウイルスを示す。

Windows、DOSウイルス	届出件数	マクロウイルス	届出件数
W32/Badtrans	1381	XM/Laroux	41
W32/Hybris	151	XM/VCX.A	16
W32/Magistr	138	X97M/Divi	15
W32/Aliz	109	W97M/Marker	6
W32/Myparty(※)	107	W97M/Melissa	5
W32/Sircam	88	W97M/Titch	4
W32/Nimda	70	W97M/Groov	1
W32/MTX	29	W97M/Opey	1
W32/Klez	27	W97M/Proverb	1
W32/Goner	23	W97M/Vmpck1	1
W32/Zoher	21	X97M/Barisada	1
W32/Shoho(※)	6	スクリプトウイルス	届出件数
W32/CIH	4	VBS/Haptime	11
Anti-CMOS	3	VBS/LOVELETTER	3
Form	3	VBS/SST	2
W32/Funlove	3	VBS/Homepage	1
W32/Msinit	3	UNIXウイルス	届出件数
W32/Ska	3		なし
W32/QAZ	2		
Cascade	1	Macintoshウイルス	届出件数
W32/Fix2001	1		なし
W32/Navidad	1		

注） ウイルス名欄で、各記号はそれぞれの下記ウイルスを示す。

記号	対象ウイルス
WM	MSword95 (WordMacroの略)
W97M	MSword97 (Word97Macroの略)
XM、XF	MSexcel95、97 (ExcelMacro、ExcelFormulaの略)
X97M	MSexcel97 (Excel97Macro)
W97M/X97M/P97M	MSword97、MSexcel97、MSpowerpoint97 (Word97Macro、Excel97Macro、PowerPoint97Macroの略)
W32	Windows32ビット環境下で動作
VBS	VisualBasicScriptで記述
Wscript	WindowsScriptingHost環境下で動作 (VBSを除く)
Solaris	Solaris環境下で動作

2) 届出の届出者別件数は次のとおりである。一番多い届出は、一般法人ユーザからのもので、65.2%を占めている。

届　出　者	届　出　件　数			
	2002/1		2001年合計	
一般法人ユーザ	1,489	65.2%	17,332	71.4%
教育･研究機関	327	14.3%	1,286	5.3%
個人ユーザ	467	20.5%	5,643	23.3%

3)届出の地域別件数は次のとおりである。関東地方が最も多く、続いて近畿地方、中部地方の順となっている。

地　域	届　出　件　数			
	2002/1		2001年合計	
北海道地方	38	1.7%	506	2.1%
東北地方	73	3.2%	882	3.6%
関東地方	1,326	58.1%	16,291	67.1%
中部地方	208	9.1%	2,360	9.7%
近畿地方	430	18.8%	2,589	10.7%
中国地方	18	0.8%	387	1.6%
四国地方	29	1.3%	399	1.6%
九州地方	161	7.0%	847	3.5%

4)届出から感染経路を区分けすると次の表のようになる。 海外からのメールも含めたメールにより感染したケースが最も多く、届出件数の約99.4%を占めている。

感　染　経　路	届　出　件　数			
	2002/1		2001年合計	
メール	2,251	98.6%	17,790	73.3%
海外からのメール	19	0.8%	3,791	15.6%
ダウンロード (※)	1	0%	593	2.4%
外部からの媒体	11	0.5%	655	2.7%
海外からの媒体	0	0%	22	0.1%
不明･その他	1	0%	1,410	5.8%

(※) ホームページからの感染を含む

5)届出のあったウイルスが感染させたパソコンの台数は次のとおりである。感染台数の欄0台は、ＦＤのみの感染またはファイルのみの感染を示し、事前の検査により、パソコンに感染する前にウイルスを発見したものである。

感　染　台　数	届　出　件　数			
	2001/12		2001年合計	
0台	1,969	86.2%	19,585	80.7%
1台	276	12.1%	3,733	15.4%
2台以上 5台未満	26	1.1%	528	2.2%
5台以上 10台未満	5	0.2%	190	0.8%
10台以上 20台未満	5	0.2%	93	0.4%
20台以上 50台未満	2	0.1%	74	0.3%
50台以上	0	0%	58	0.2%

特定日発病ウイルスについて

ウイルスの被害の拡大を防止する意味から、今回は、IPA/ISEC に届出されたウイルスの中で、2月8日～ 3月31日に発病する可能性がある主なウイルスを下記に掲げたので注意されたい。(参考：特定日発病ウイルス［ウイルスカレンダー］)

VBS/Haptime	2月11日、3月10日

コンピュータウイルスに関する届出制度について

コンピュータウイルスに関する届出制度は、経済産業省のコンピュータウイルス対策基準に基づき、'90年4月にスタートした制度であって、コンピュータウイルスを発見したものは被害の拡大と再発を防ぐために必要な情報をＩＰＡ に届け出ることとされている。
ＩＰＡでは、個別に届出者への対応を行っているが、同時に受理した届出等を基に、コンピュータウイルス対策を検討している。また受理した届出は、届出者のプライバシーを侵害することがないように配慮した上で、被害等の状況を分析し、検討結果を定期的に公表している。

○コンピュータウイルス対策基準
・通商産業省告示第139号　平成 2年 4月10日制定
・通商産業省告示第429号　平成 7年 7月 7日改訂
・通商産業省告示第535号　平成 9年 9月24日改訂
・通商産業省告示第952号　平成12年12月28日改訂

問い合わせ先：ＩＰＡセキュリティセンター (IPA/ISEC)
(ISEC：Information technology SEcurity Center)
TEL：03-5978-7508　FAX：03-5978-7518
E-mail：virus@ipa.go.jp　相談電話：03-5978-7509　URL：http://www.ipa.go.jp/security/