

IPA[®]

Information-technology Promotion Agency
IT Security Center

<http://www.ipa.go.jp/security/>

7 Articles for Virus Countermeasures

1

**Vaccine Software
Keep it Up-to-Date**

2

**Email Attachment Files
Should be Scanned**

3

**Downloaded Files
Should be Scanned**

4

**For Applications
Utilize Security Functions**

5

**Security Patches
Should be Applied**

6

**Symptoms of Virus Infection
Must not be Overlooked**

7

**In Case of Emergency
Data should be Backed Up**

IPA

Note: A poster showing “7 Articles for Virus Countermeasures” is available. The poster is used in “Teach Yourself Threats of Computer Viruses in 15 Minutes” (Moving contents that show how to develop and promote virus protection measures). It can be downloaded from the following URL:

<http://www.ipa.go.jp/security/y2k/virus/cdrom2/documents/7kajyou.pdf>

Reference: “Teach Yourself Threats of Computer Viruses in 15 Minutes”

<http://www.ipa.go.jp/security/y2k/virus/cdrom2/>

1. Vaccine Software ... Keep it Up-to-Date

To protect against viruses, antivirus software should be installed.

Those who are using antivirus software must perform scan using the latest virus-scanning engine and virus definition files.

Day by day, new viruses are detected one after another; even though some of them may look exactly the same as existing viruses, they are in fact subspaces of a specific virus. So the antivirus software should be kept updated so it can properly deal with such new viruses.

Generally, antivirus software has the automatic update function that keeps virus-definition files up-to-date. Turn on this function or manually update the files on a regular basis.

Some new computers have trial-antivirus-software pre-installed. Note, however, that after a specified period of time, those programs cannot be used or their definition files cannot be updated.

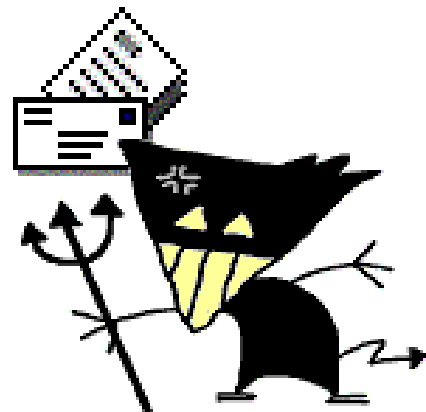
If you have no antivirus software at hand but can access the Internet, you can still use free-online scan services provided by some vendors (Refer to page 12). Note, however, that you cannot perform real-time checking, so it's recommended to install antivirus software.



2. Email Attachment Files ... Should be Scanned

Computer viruses are often contained in email attachments. Even if the email is from your close friend, scan the attached files for viruses before opening them.

The number of incidents caused by emails containing forged sender information is increasing. In order to protect your computer from such emails, you must also be careful with emails from unknown sources and forged service providers. When exchanging emails with your close friends and if it's necessary to attach a file, it's recommended to explain in the body of the email message that you have attached the file and what its contents are. When you have received an email with a file (or files) attached, you should scan the file for viruses before opening it. This step is necessary for better safety.



You should also be careful when the file extensions (the last three characters of a file name) listed below are used for attached files. Note, however, that Windows has the [Hide file extensions for known file types] option. It's recommended to disable it (Refer to page 5).

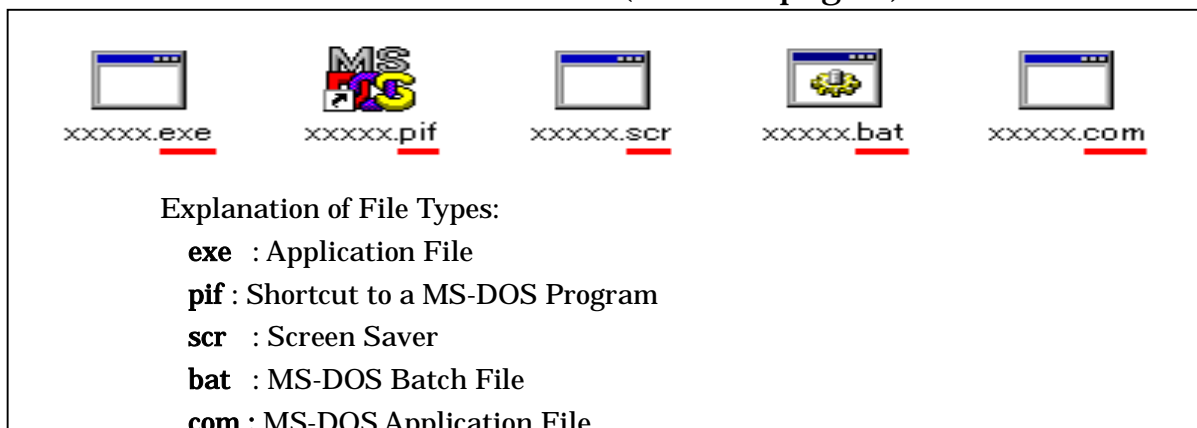


Figure 1

Files with these extensions are executed right after they are opened. If the files contain a computer virus, your computer might be infected with it and suffer damage, such as leakage of personal information, destruction of hard drive, etc., and in the worst case, entire controls of your computer might be taken over.

Depending on the virus, file icons might be forged or double extensions applied to make you think they are authentic ones.

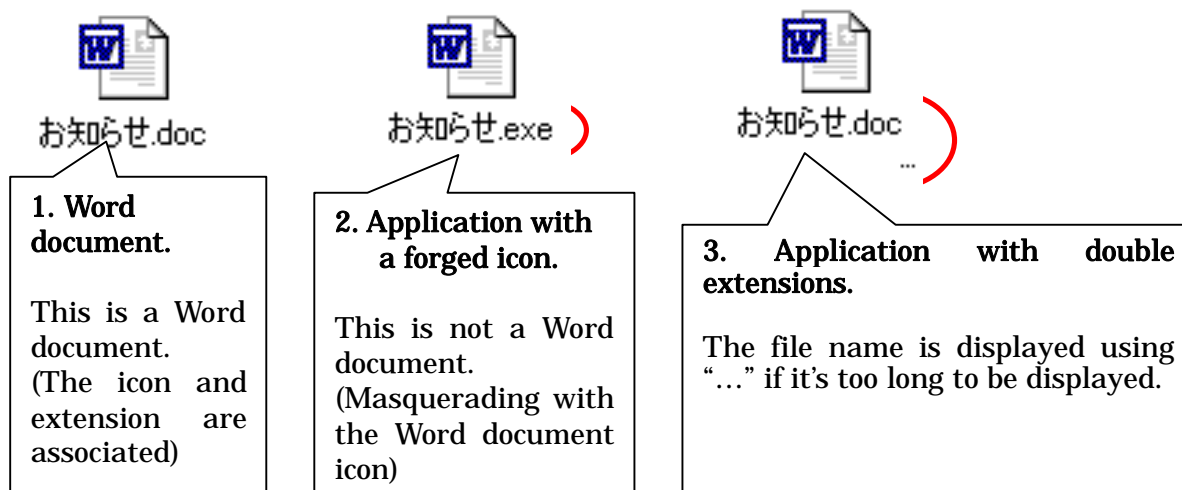


Figure 2

Figure 3

Figure 4

Word document files should look like Figure 2. On the contrary, applications with forged icons will appear as in Figure 3, and applications with double extensions in Figure 4.

Figure 5 shows what the window looks like when you have received an email with a file (as shown in Figure 4) attached.



Figure 5

There are several ways to check the file types.

For example, in the case of Figure 2 and Figure 3, right-click on the file icon and select [Properties (R)] from the pop-up menu.



Figure 6 File's properties

Figure 7 File' Properties

Settings to Show Hidden File Extensions

By default, Windows does not show file extensions. In order to display them, open the [My Computer] or [Explorer] window, select [Tools (T)] > [Folder Options (O)], click the [Display] tab, and uncheck the [Hide file extensions for known file types] option. (Figure 8 is for Windows XP)



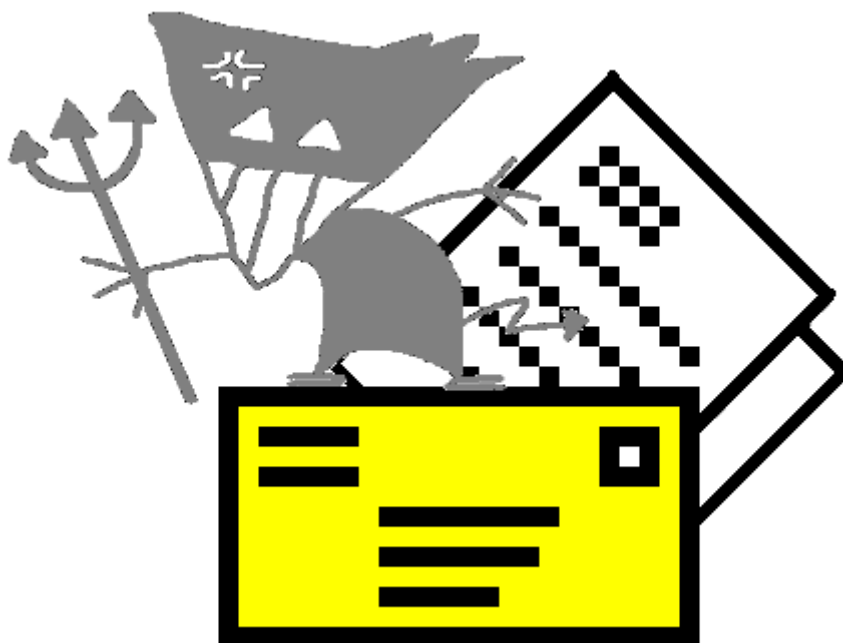
Figure 8

[Five points for handling email attachments]

- (1) Be careful with email attachments from unknown sources.**
- (2) Do not be fooled by the appearance of attachment files.**
- (3) Be wary of suspicious files attached to emails even though they are from your friends.**
- (4) Do not send a plain text that can be included in the body of an email message as an attachment file.**
- (5) Learn about how email attachments are handled by different email programs.**

<http://www.ipa.go.jp/security/antivirus/attach5.html>

Note: It is important to understand how email attachments are handled by the email program you are using. For example, some programs automatically save attachment files in certain folders upon receiving them. When using such programs, you need to make proper settings to ensure that, when emails and attachment files containing a computer virus are deleted, their copies in the designated folders are also deleted.



3. Downloaded Files ... Should be Scanned

Various files such as image files, music files and video files can be downloaded from the Internet, but there is a possibility of a malicious program or instruction code being embedded in those files. To avoid this, be sure to scan downloaded files before using them.



Similarly, files on external recording media (such as floppy disks, CDs, etc) should be scanned for viruses if the source of the media is unknown.

Wonderful Present?

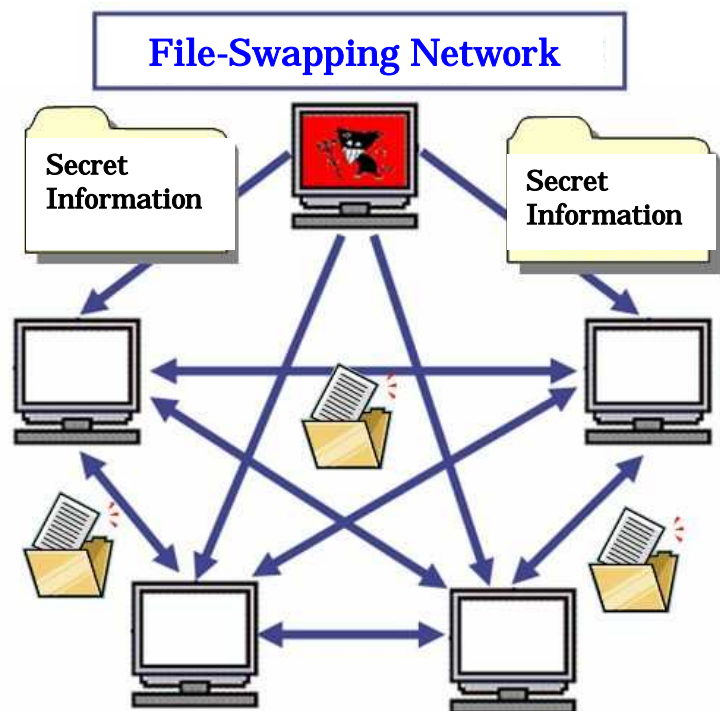


Also, when downloading files, be sure that the Web site is secure. You should not download any files from suspicious Web sites, including the sites whose URLs are advertised in SPAM mails.

Recently, personal data and confidential data of enterprises have been compromised due to a computer virus exploiting file-swapping software (such as Winny).

Once the stolen information is posted on the Internet, the diffusion of the information is technically unavoidable, which may bring serious troubles.

The virus "Antinny" spreads its infection by distributing virus files using a file-swapping software called "Winny". Files obtained using the file-swapping software must also be scanned to avoid any trouble.



4. For Applications ... Utilize Security Functions

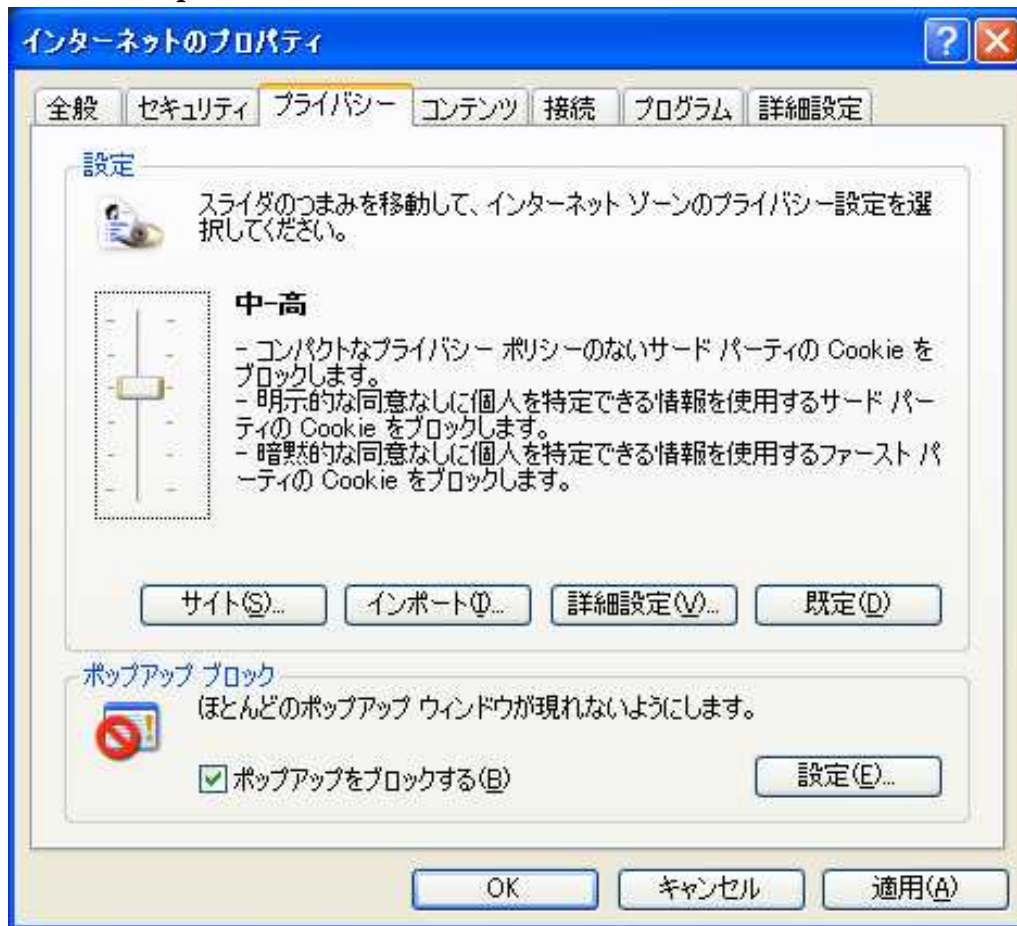
When using mailer software to send or receive emails, or a web browser to access Web sites on the Internet, **utilize the security functions/settings supplied with the application software.**



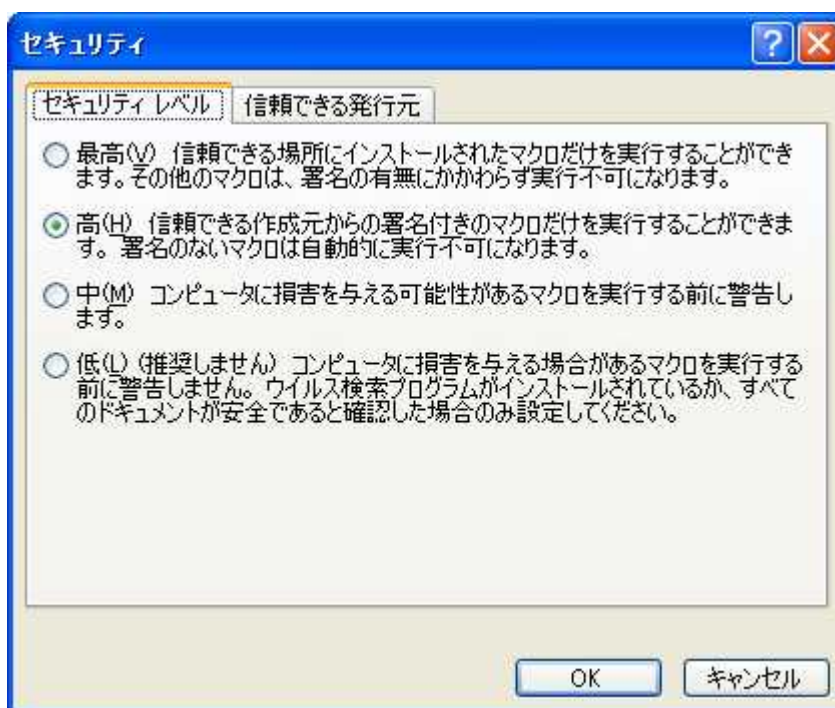
For example, when you are using Microsoft Internet Explorer, you can set security levels on the Options window (Select [Start] > [Settings] > [Control Panel] > [Internet Options]) (The figure below shows an example with Windows XP.) In this case, it's recommended to set the security level to "Medium".



As a mean to protect your computer from Spyware, it is also recommended to set the privacy level to “Medium - High” or higher. (The figure below shows an example with Windows XP)



Although macro-type viruses (*3) may seem obsolete, your computer can still be infected with such viruses by opening MS Word or Excel files containing malicious macros. To avoid this, disable the automatic execution of macros (by selecting [Tool(T)] > [Option(O)] > [Security] > [Macro Security] for Word2003.)



This setting will protect your computer from viruses that can cause a serious damage.

5. Security Patches ... Should be Applied

Recent viruses exploit vulnerabilities (or security holes) in the operating systems and application software. If there is any vulnerability, your computer can be infected with viruses only by **previewing emails** or **accessing the Internet**.

For example, vulnerability in mailer software allowing the automatic execution of attachment files can be exploited by viruses, which can cause a broader damage. Such vulnerabilities are detected at short intervals, so it is important to periodically visit the vender's Web site and check for any related information on the application (in particular, mailer software and browsers) you are using, and then apply the latest security patch available.



Depending on the vulnerability, your computer can be infected with viruses only by accessing the Internet. The virus “W32/MSBlaster” (detected in August 2003), “W32/Welchia”(August 2003) and “W32/Sasser” (May 2004) are well-known for causing computers to keep rebooting.

A computer virus called **Bot (*5)**, which has become a topic of conversation, can spread its infection via the Internet.

Windows users should periodically perform the Windows Update/Microsoft Update, or turn on the Automatic Update feature. You can apply the latest patches provided by Microsoft for their operating systems, Internet Explorer, and Office products.

- Windows Update
<http://windowsupdate.microsoft.com/>
- Office Update
<http://office.microsoft.com/ja-jp/officeupdate/>
- Microsoft Update
<http://update.microsoft.com/microsoftupdate/>

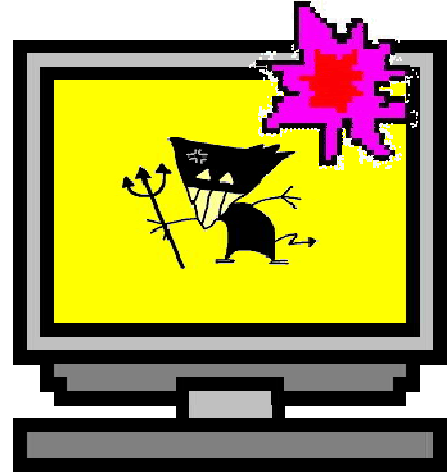
For information on how to apply the Windows Update, Office Update, and Microsoft Update, please refer to the following Web sites:

- How to apply the Windows Update
<http://www.microsoft.com/japan/athome/security/sechome/tool/mbsa4.mspx>
- How to apply the Office Update
<http://www.microsoft.com/japan/athome/security/sechome/tool/mbsa5.mspx>
- How to apply the Microsoft Update
http://www.microsoft.com/japan/athome/security/update/j_musteps.mspx

6. Symptoms of Virus Infection ... Must not be Overlooked

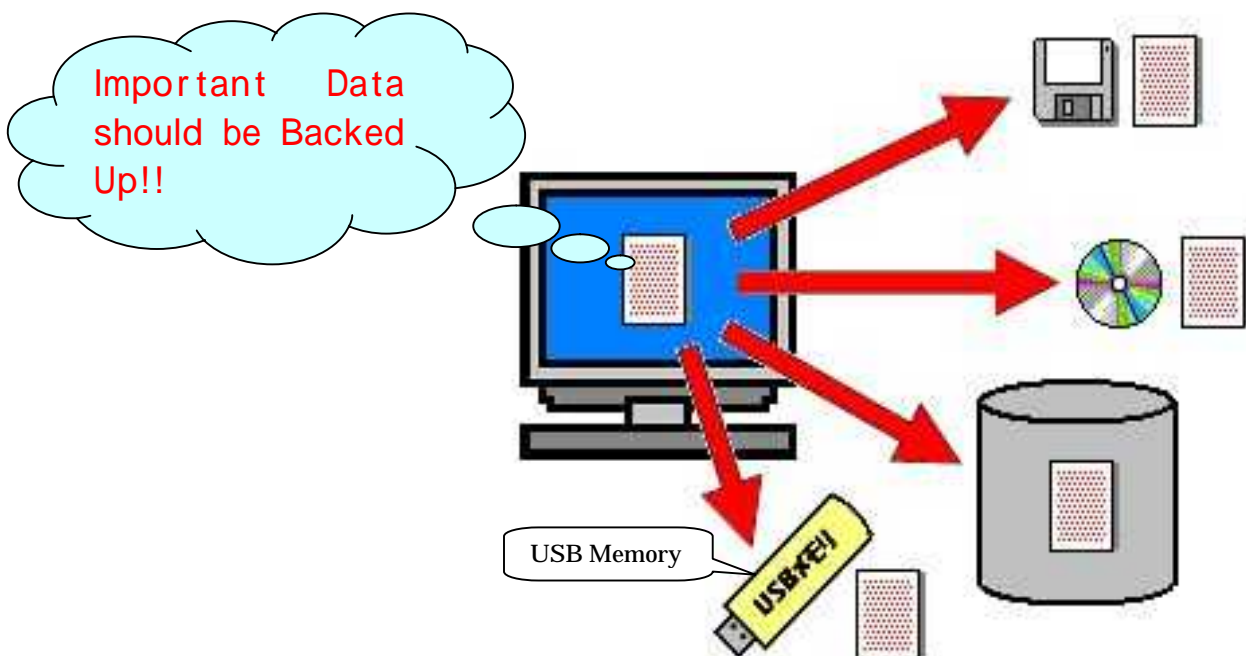
If you have encountered symptoms listed below, your computer may have been infected with computer viruses. Do not overlook them and scan your computer for viruses.

- (1) System or application software often gets hosed (freezes), or the system does not start.
- (2) Files disappear. Unknown files exist.
- (3) Strange icons appear on the task bar.
- (4) Attempts are made to access the Internet without any operation.
- (5) Emails are sent without the user's consent.
- (6) Can intuitively sense that there is something wrong with the computer.



7. In Case of Emergency ... Data should be Backed up

Data corrupted by viruses cannot be restored by using antivirus software. Make it a rule to back up data on a regular basis so you can restore the system from any damage caused by virus infection. In addition, keep in a safe place the original CD-ROMs of application software. Should the contents of the hard drive be damaged, you can restore them using the CD-ROMs.



8. Should Your Computer be Infected with a Virus ...

Scan your computer for viruses using the latest virus definition files. If you have been able to identify the name of the virus but do not know how to eliminate it, visit the Web site of your antivirus software manufacturer and look for information related to the virus, and then follow the instructions presented on the Web page.

If you have no antivirus software at hand but can access the Internet, you can still use free-online scan services provided by some vendors to identify the name of the virus. If identified, look for the information on the virus and follow the instructions presented on that Web page.

Online scan services provided by major antivirus software vendors are as follows:

- Symantec Security Check
<http://www.symantec.com/region/jp/securitycheck/>
- Trendmicro Online Scan
<http://www.trendmicro.co.jp/hcall/>
- McAfee Free Scan
<http://www.mcafeesecurity.com/japan/mcafee/home/freescan.asp>

If you have further questions, contact the “IPA Computer Virus 911 call” service, where you can consult IPA consultees about virus-related problems.

IPA Computer Virus 911 Call Number

Feel free to ask questions about computer viruses.

03-5978-7509

(Japanese only)

Weekdays: 10:00 - 12:00, 13:30 - 17:00

You can e-mail to the following address:

virus@ipa.go.jp

9. References

For further information, please refer to the following materials:

Careless Downloading can Cause Considerable Damage

<http://www.ipa.go.jp/security/topics/malicious.html>

- Notes on Using File-Swapping Software

http://www.ipa.go.jp/security/topics/20050623_exchange.html

- Virus Protection Measure Check Sheets

<http://www.ipa.go.jp/security/virus/beginner/check/check.html>

- Information on Antivirus Software

<http://www.ipa.go.jp/security/antivirus/vacc-info.html>

- Security at Home: Protect Your Computer (Microsoft)

<http://www.microsoft.com/protect/computer/default.mspx>

- “Enhancing Security for Your Browser and Emails” (Microsoft)

<http://www.microsoft.com/japan/security/incident/settings.mspx>

10. Terminology

(*1) SPAM Mail

Also called Unsolicited Bulk Email (UBE). Emails containing identical or nearly identical messages that are sent to any number of recipients for commercial, religious, or harassing purposes.

(*2) File-Swapping Software

A software program that makes a user's files available to other users for download over the Internet.

(*3) Macro-Type Virus

A macro virus that infects Microsoft Word documents and Excel spreadsheets. If you open a document or spreadsheet that is infected with this virus, Word or Excel itself is also contaminated. Virus-infected files that are attached to emails or saved on recording media (such as floppy disks, magneto-optical disks etc) become the source of another infection.

(*4) Vulnerability

Vulnerability in terms of information security is a security hole that may degrade the security level of systems, networks, applications and protocols, which can bring unexpected, unwanted events, or design and implementation errors. Vulnerabilities are classified into “vulnerabilities in the operating systems”, “vulnerabilities in applications”, etc. Inadequate security settings are also referred to as vulnerability. In general terms, it is called “security hole”.

(*5) Bot

A computer virus designed to control computers (infected with this virus) from an external source via a network (or the Internet). It waits for instructions from the external source and upon receiving them, performs programmed tasks. The name “Bot” was derived from “Robot”, as its functions are similar to those of robots.

11. Major Antivirus Software Vendors (Based on reports submitted to IPA)

Ahnlab.Inc

URL <http://global.ahnlab.com/>

Main Product: Virus Block

Aladdin Japan

URL <http://www.eAladdin.com/esafe/> (Israel Site)

Main Product: eSafe

Symantec

URL <http://www.symantec.com/> (US Site)

Main Product: Norton Internet Security, Norton Antivirus, Norton Antivirus for Mac

Sophos

URL <http://www.sophos.com/> (UK Site)

Main Product: Sophos Anti-Virus

Trendmicro

URL <http://www.trendmicro.com/en/home/us/enterprise.htm> (US Site)

Main Product: Virus Buster, Inter Scan

Japan F Secure

URL <http://www.f-secure.com/> (Finland Site)

Main Product: F-Secure Antivirus

McAfee

URL <http://www.mcafee.com/us/> (US Site)

Main Product: VirusScan, GroupShield



IPA[®]

Information-technology Promotion Agency
IT Security Center

2-28-8, Honkomagome, Bunkyo, Tokyo, 113-6591 Japan

TEL 81-(0)3-5978-7508

FAX 81-(0)3-5978-7518

E-mail virus@ipa.go.jp (Virus) crack@ipa.go.jp (Hacking)

URL <http://www.ipa.go.jp/security/>

Issued August 1, 2006 Issue No.4