

Computer Virus/Unauthorized Computer Access Incident Report – April 2009

This is the summary of computer virus/unauthorized computer access incident report for April 2009 compiled by IPA.

I. Reminder for the Month

**“Are you always recognizing the security measures for USB memory?”
- Let s double check the secure use of USB memory -**

Up to current, IPA has been warning variety level of computer users the necessity of security measures relevant to USB memory. Unfortunately, we still have number of consultations and reports relevant to the virus infected via an USB memory. Bad to worse, such damages caused by that virus which enlarges infection via an USB memory are continually reporting: For example, in February, the system in an academic medical center was infected by virus that caused severe system failures. The virus infected over 1,000 computers via a network: lately, it was realized that the infection source was from an USB memory. The same virus also led another severe system failure in a municipal government in March.

Absent any of security measures from your mind will lead unanticipated damage (s). Why don't you recognize the security measures upon utilizing USB memory and double check the secure use of USB memory with us.

(1) Current Status of Security Measures Upon Using USB Memory

Follows, we summarized the responds to the small questionnaires relevant to the security measures for an USB memory in the “2nd Awareness Survey about the Threats relevant to Information Security in 2008” conducted by IPA.

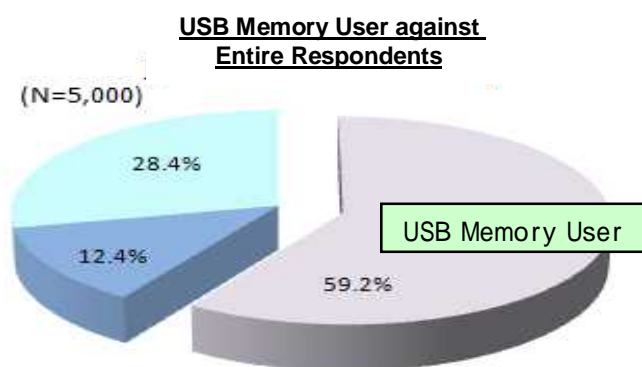


Chart 1-1: USB Memory User (Ratio against entire respondents)

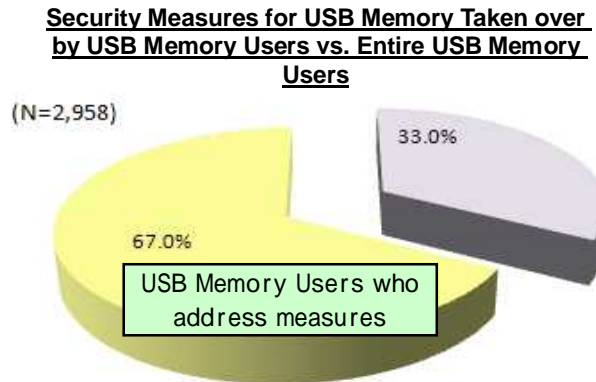


Chart 1-2: Security Measures for USB Memory taken over by USB Memory User

Security Measures for USB Memory Actually Conducted by the Respondents who Use USB Memory

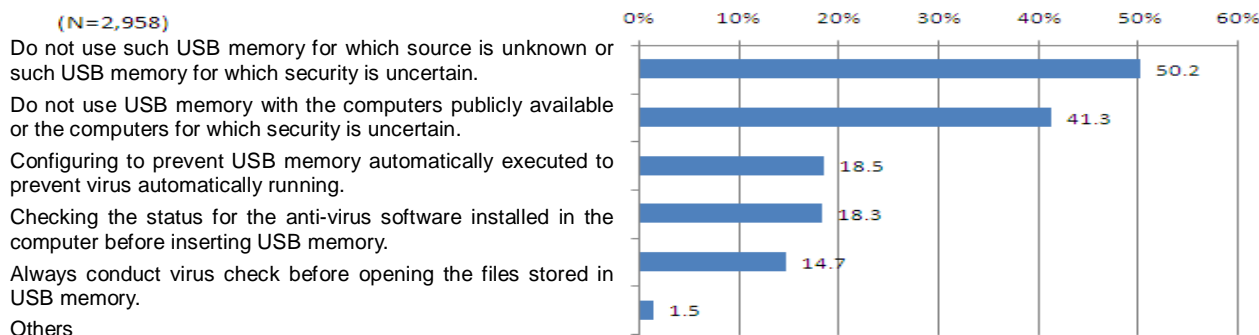


Chart 1-3: Security Measures for USB Memory Actually Conducted by USB Memory Users

According to the Chart 1-1, the ratio for USB memory users took over about 60% against entire respondents. In addition, the Chart 1-2 shows that the users who conduct security measures for USB memory retained 2/3 for the entire respondents who use USB memory.

<Reference>

The "2nd Awareness Survey about the Threats relevant to Information Security in 2008" conducted by IPA (in Japanese)

<http://www.ipa.go.jp/security/fy20/reports/ishiki02>

(2) Security Measures Upon Using USB Memory

IPA occasionally recommended users to conduct following security measures upon utilizing USB memory.

- Do not insert your USB memory to such computers managed by the others or such computers who used by unspecified majority.
- Do not insert such USB memory managed by the others or such USB memory for which owner is unknown to your computer.

However, according to the Chart 1-3, those users who conduct fundamental security measures such as "Do not use such USB memory for which source is unknown or such USB memory for which security is uncertain", "Do not use USB memory with the computers publicly available (such as those in net café, etc.) or the such computers for which security is uncertain" resulted about a half or the less against the entire respondents who use USB memory.

Accordingly, we encourage those users who use USB memory are to conduct the security measures upon using USB memory recommended by IPA.

(3) Policy for Technical Security Measures

According to the Chart 1-3, those users conducting "Configuring to prevent USB memory automatically executed to prevent virus automatically running" were less than 20%. The automatically execution feature is the one of Windows functions with which file is automatically executed upon inserting USB memory or double clicking the drive which recognizes USB memory. This function is also referred as Autorun feature.

Such virus which enlarges infection via an USB memory exploits the Autorun feature to infect such computers for which an USB memory to be inserted. The one of effective measures to prevent infection by that virus is to disable Autorun feature.

We encourage those users are to conduct above mentioned measures who are not currently using USB memory, but those may use it in future.

(4) How to Disable Autorun Function of USB Memory

There publicized the Security Updates and its procedures how to adequately disables Autorun feature by Microsoft on February 24, 2009.

<Reference>

How to correct "disable Autorun registry key" enforcement in Windows (Microsoft)

<http://support.microsoft.com/kb/967715/en>

Based on the information above, we describe detailed procedures about the measure: this is to increase the users who will disable Autorun feature relevant to USB memory in number and to achieve further secure use of USB memory.

However, the procedures may vary depending on which Windows version you are using; accordingly, be sure to follow to the procedure supported by your computer. To make it sure what supporting procedure is available for your computer, please refer to the following URL.

<Reference>

How to Check Most Suitable Supporting Procedures for your Computer (Microsoft) (in Japanese)

http://www.microsoft.com/japan/security/bulletins/ver_win.mspx

Upon disabling Autorun feature for your computer, be sure to identify your Windows version to what procedure is available for your computer. Following Chart 1-1 will tell you which method will support what Windows version. In addition, once you disable Autorun features with the one of methods described below, it means that you will disable not only Autorun feature for USB memory, but also all of outside memory media: that is, Autorun features for CDs and DVDs will also be disabled, so please be noted.

Table 1-1: Cross Reference for the Windows Versions and the Procedures Disabling Autorun Feature for USB Memory Supported

Windows Versions	Vista Ultimate	Vista Business	Vista Home Premium	Vista Home Basic	XP Professional Edition	XP Home Edition	2000
	Method A	Method A	Method B	Method B	Method C	Method D	Method C

Please be cautious as you may face difficulties if any of measures above wrongly addressed. In case of accident/incident, be sure to create the points for “system restoration” by referring following URLs in case something happens. In this way, you can smoothly move to the “system restoration” session by specifying the restoration point being set before you initiate any of procedures above.

<Reference>

Description about System Restoration for Windows Vista (Information cited from “PC talk” by Microsoft) (in Japanese)

<http://www.support.microsoft.com/kb/934854/ja>

“Using System Restore” (Microsoft)

<http://www.microsoft.com/japan/windowsxp/pro/business/feature/performance/restore.mspx>

(a) For Windows Vista User

<Common Concept>

As for Windows Vista, the behavior upon inserting USB memory will be determined depending on how the “Auto play for CD or the other media” (*) in the “Software and Games” editor (See the Chart 1-4) is configured.

That is, the configuration may be updated depending on the behavior when an USB memory was previously inserted so that the user needs to check this configuration every time. Accordingly, to make the Autorun feature fundamentally disabling, you should take following method rather than configuring it in the editor screen shown in the Chart 1-4.

First of all, it is necessary that the security updates for Windows Vista (KB950582) is applied in advance. The method how to check the security updates applied, please refer to the following URL.

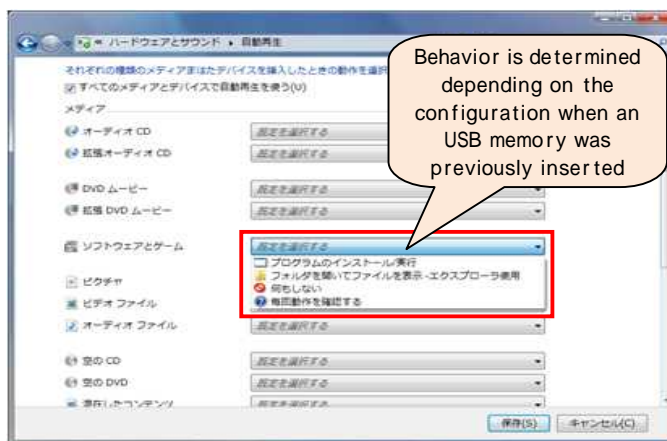


Chart 1-4: Sample Configuration for “Auto Play for CDs or the other Media” for Windows Vista

* The configuration screen shown in the Chart 1-4 will be appeared as you start to click “Start” button, “Control Panel” and then “Auto play for CD or the other media” in the “Hardware and Sound” items in turn.

<Reference>

The method how to check if the security updates are adequately installed – for Windows Vista User” (Microsoft) (in Japanese)

http://www.microsoft.com/japan/security/bulletins/inst_history_vista.msp

Upon confirmed that the above mentioned security updates are adequately applied; then initiate to disable Autorun features with the following <Method A> if you are a Windows Vista Ultimate or a Windows Vista Business user.

<Method A>

1. Click the “Start” button and then enter “Gpedit.msc” in the “Start to Search” box to display Local Group Policy Object editor. When administrator password is required, click “OK” button following to the password: if you are asked to confirmation, just click “Continue”. If you do not know about the administrator password, check the password with your administrator.
2. Click the “Computer Configuration”, “Administrative Template” and “Windows Configuration” in turn and then click the “Policy for Auto Play”.
3. Double click “Disabling Auto Play Feature” in the configuration window to display the Configuration editor for the “Policy for Auto Play” (See the Chart 1-5).
4. Click the “Enabled” button in the Configuration editor and then select “All Drives” in the “Disabling Auto Play Feature” to disable Autorun feature for all the drives.
5. Click the “OK” button and then exit from Local Group Policy Object Editor.
6. Restart your computer.

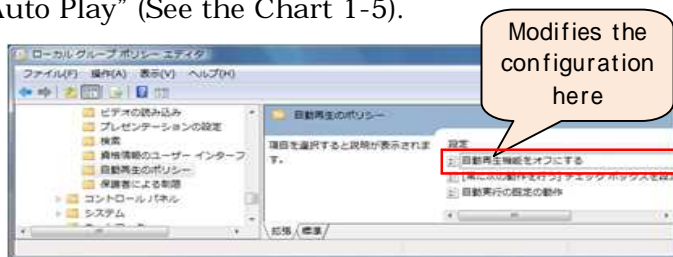


Chart 1-5: The Group Policy Object editor for Windows Vista (Sample)

In the cases of Windows Vista Home Basic and Windows Vista Home Premium, <Policy A> is not available as the Group Policy Object editor is not usable: however, the Autorun feature can be disabled if you can modify registry information. The <Method B> underneath is the other method that can disable the Autorun feature as well.

<Method B>

1. Click the “Specify File to Execute” button follows to the “Start” button. Enter “regedit” in the “name” box and click “OK” to display the Registry editor.
2. Click following folders in turn in the Registry editor: “HKEY_LOCAL_MACHINE” (*), “SOFTWARE”, “Microsoft”, “Windows”, “CurrentVersion”, “Policies” and finally “Explorer”.
3. Right click the “Explorer” to select “New”, “DWORD (32-bit) value” in turn from the menu to configure “NoDriveTypeAutoRun” as the “new value” newly created within the folder. Right click “NoDriveTypeAutoRun” again to select “Edit” from menu (See the Chart 1-6).
4. To disable all the Autorun features, you need to enter “0xFF” in the “Value Data” box.
5. Click “OK” and exit from the Registry editor.
6. Restart your computer.

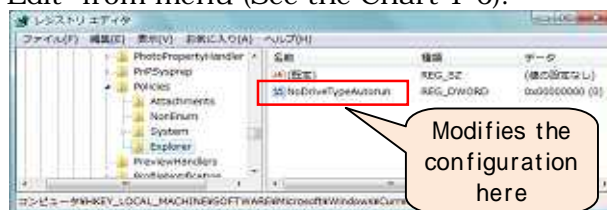


Chart 1-6: The Registry editor for Windows Vista (Sample)

(*) To disable the Autorun feature on all users' machines, "HKEY_CURRENT_USER" was replaced by "HKEY_LOCAL_MACHINE". (May 22, 2009)

By conducting either the method <A> or described above, the potential risk caused by virus will be eliminated regardless how you'd configured in the "Auto Play for CD or the other Media" as none of configuration editor for Autorun will be appeared even you insert your USB memory.

(b) For Windows XP and Windows 2000 User
 <Common Concept>

As for Windows XP and Windows 2000, any of programs will not automatically run even you insert your USB memory in your computer; however, when you double click the drive that recognizes USB memory from "My Computer", some program may be run (See the Chart 1-7). To eliminate this risk, disabling Autorun feature is helpful.

First of all, it is necessary that security updates either for Windows XP and Windows 2000 (KB967715) or common security updates (KB953252) is applied in advance. The method how to check the security updates applied, please refer to the following URL.

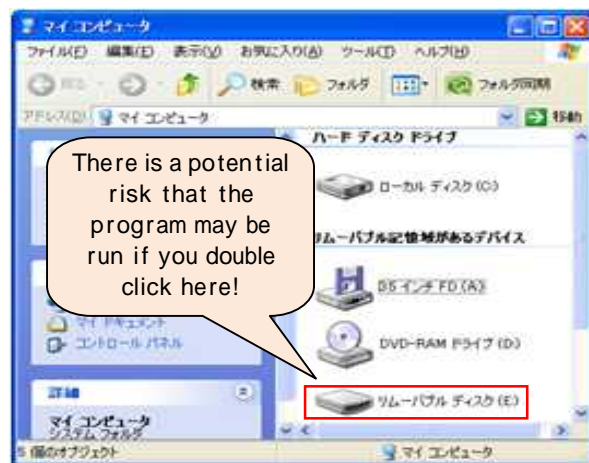


Chart 1-7: My Computer Screen for Windows XP (Sample)

<Reference>

The method how to check the security updates be properly installed" (Microsoft) (in Japanese)

http://www.microsoft.com/japan/security/bulletins/inst_history.msp

Upon confirmed that the above mentioned security updates are adequately applied; then initiate to disable Autorun features with the following <Method C> if you are a Windows XP Professional Edition or a Windows 2000 user.

<Method C>

1. Click the "Specify File Name to Execute" button follows to the "Start" button. Enter "Gpedit.msc." in the "name" box and then click "OK" to display the Group Policy editor.
2. Click the "Computer Configuration", "Administrative Template" in turn and eventually click the "System" (See the Chart 1-8).
3. Double click the "Turn-off Auto Play" in the configuration window to display Configuration editor (in Windows 2000, "Turn-off" is used instead of using "Disabling" for the "name" for the Policy Configuration editor).
4. Click the "Enabled" button in the Configuration editor and then select "All Drives" in the "Turn-off Auto Play" box to disable Autorun feature in all the drives.

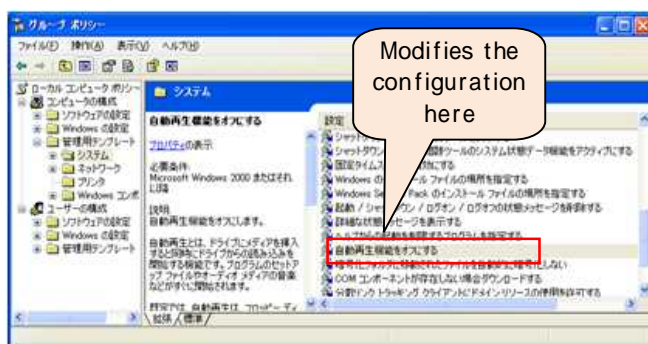


Chart 1-8: The Group Policy editor for Windows XP (Sample)

5. Click “OK” and then exit from the Group Policy editor.

6. Restart your computer.

As for the Windows XP Home Edition, <Method C> is not available as the Group Policy editor is not usable: however, you may be disable the Autorun feature by modifying the registry information. The <Method D> underneath is the other method that can disable the Autorun feature as well.

<Method D>

1. Click the “Specify File Name to Execute” button follows to the “Start” button. Enter “regedit” in the “name” box and click “OK” to display the Registry editor.
2. Click the following folders in turn in the Registry editor: “HKEY_LOCAL_MACHINE” (*), “SOFTWARE”, “Microsoft”, “Windows”, “CurrentVersion”, “Policies” and eventually “Explorer”.
3. Right click the “Explorer” to select “New” and “DWORD Value” in turn from the menu to configure “NoDriveTypeAutoRun” as the “new value” newly created within the folder. Right click “NoDriveTypeAutoRun” again to select “Edit” from the menu (See the Chart 1-9).
4. To disable the all Autorun feature, enter “0xFF” in the “Value Data” box.
5. Click “OK” and then exit from the Registry editor.
6. Restart your computer.



Chart 1-9: Registry Editor for (Sample)

(*) To disable the Autorun feature on all users’ machines, “HKEY_CURRENT_USER” was replaced by “HKEY_LOCAL_MACHINE”. (May 22, 2009)

By conducting either the method <C> or <D> described above, the potential risk caused by virus can be eliminated: none of programs will be executed even you double click the drive which recognizes USB memory from “My Computer” – there only appears the list of files.

<Reference>

IPA – The Seven Anti-virus Requirements for Computer Users

<http://www.ipa.go.jp/security/antivirus/7kajonew.html>

IPA – The Five Anti-Spyware Measures for Computer Users (in Japanese)

<http://www.ipa.go.jp./security/antivirus/spyware5kajyou.html>

II. Reporting Status of Computer Virus - further details, please refer to the Attachment 1 -

The detection number ^(*) in April was **about 156T** (March: about 119T): increased 31.1%. In addition, the reported number ^(*) in April was **1,438** (March: 1,674): decreased 14.1%.

^(*) Detection number: Reported virus counts (cumulative) found by a filer.

^(*) Reported number: Aggregated virus counts. Viruses of same type and their variants reported on the same day are counted as one case number regardless how many viruses or the actual number of viruses is found by the same filer on the same day. In April, the reported number was 1,438 and the aggregated virus count was about 156T. *(From the May '08 report, we use "T (thousand)" instead of using "M (Million)" to show the detection number of virus in detail.)*

The worst detection number was **W32/Netsky** with about **105T**; **W32/Downad** with about **40T** and **W32/Mytob** with about **3T** subsequently followed.

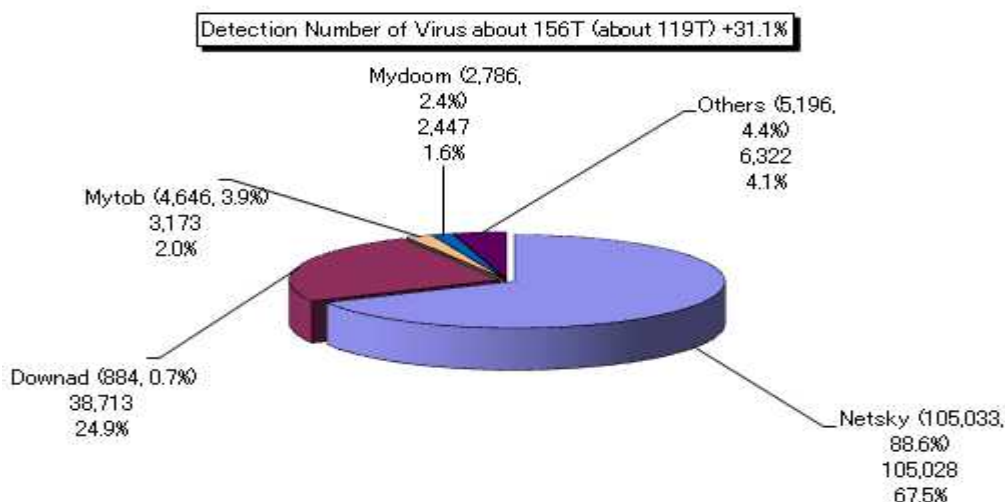


Chart 2-1: Detection Number of Virus
(Numbers in parenthesis are for the previous month)

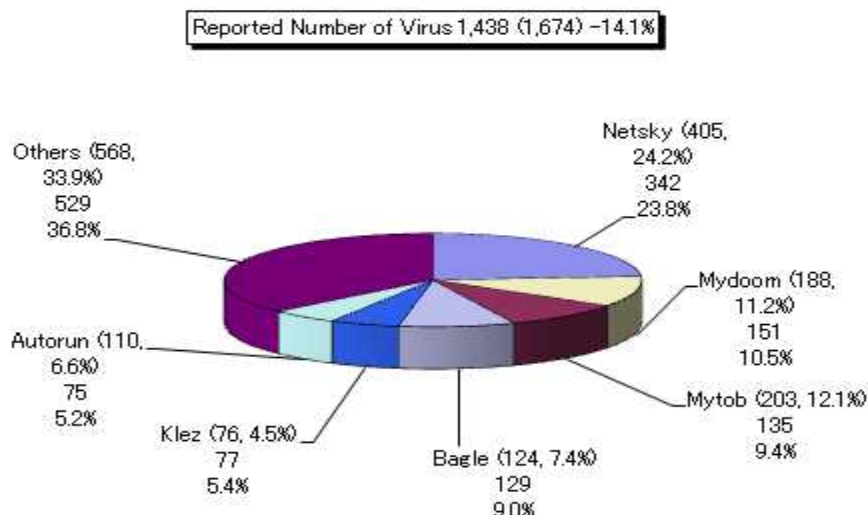


Chart 2-2: Reported Number of Virus
(Numbers in parenthesis are for the previous month)

III. Reporting Status of Unauthorized Computer Access (includes Consultations) –
Please refer to the Attachment 2 for further details –

Chart 3-1: Report for unauthorized computer access and status of consultation

	Nov.	Dec.	Jan. '09	Feb.	Mar.	Apr.
Total for Reported (a)	18	10	10	9	20	9
Damaged (b)	12	7	7	6	13	6
Not Damaged (c)	6	3	3	3	7	3
Total for Consultation (d)	39	38	29	35	40	39
Damaged (e)	19	19	13	14	11	11
Not Damaged (f)	20	19	16	21	29	28
Grand Total (a + d)	57	48	39	44	60	48
Damaged (b + e)	31	26	20	20	24	17
Not Damaged (c + f)	26	22	19	24	36	31

(1) Reporting Status for Unauthorized Computer Access

Reported number in April was 9: Of 6 was the number actually damaged.

(2) Accepting Status for Consultation relevant to Unauthorized Access

The consultation number relevant to unauthorized computer access was 39: Of 11 was the number actually damaged.

(3) Status of Damage

The breakdown for damage reports included **intrusion** with **3**, **masquerading** with **1**, **embedding of malicious codes** with **1**, etc. As for the damage caused by intrusion included: located the contents that were not intended by the manager of the web server with 2 (of 1 was for the contents to be exploited for phishing*), located malicious codes on the server with 1, etc. The causes for the intrusion were: insufficient security configuration with 1, seemed to be a password cracking* attack to the port used by SSH* with 1, etc (the cause for the rest of 1 was not yet identified).

* Phishing: the one of illegal activities to exploit the IDs and passwords from those users who'd opened/browsed either mails or web pages spoofed to be a substantial business such as legitimate financial institution, etc.

* SSH: The one of protocols to communicate with the computer remotely via a network.

* Password Cracking: The activity to analyze/parse the other person's password illegally. Brute Force Attack (Exhaustive Search Attack) and Dictionary Attack are the well-known methods. The program for cracking activity is also existed.

(4) Damage Instance

[Intrusion]

(i) Server was intruded by the attack to the port used by SSH...

Instance	<ul style="list-style-type: none">- The server for my department was fraudulently accessed so communicated from the in-house Data Center Division.- In the event of the study, some malicious codes located in the “/home/tomcat/.bot” directory is identified.- The cause seems that the server was conducted by password cracking attack to the port used by SSH and the password was analyzed.- We used more than 8 characters for the password, though.
----------	--

(ii) Phishing site was located...

Instance	<ul style="list-style-type: none">- We are using a rented server. One day, “there may be some fraudulent contents on that server” so communicated from that rental business.- In the event of the study, some malicious contents to be exploited for Phishing located on that server were identified.- The study was really a challenging that we could not identify the fundamental cause as the logs were already deleted and the default commands such as ps and ls, etc. were altered with the fraudulent ones.
----------	---

IV. Accepting Status of Consultation

The gross number of consultation in April was 1,668. Of the consultation relevant to “One-click Billing Fraud” was 572 (March: 503), consultation relevant to “Hard selling of falsified anti-virus software” was 3 (March: 3), consultation relevant to “Winny” with 4 (March: 6), were realized. (The consultation relevant to “the suspicious mail sent to specific organization to collect specific information/data” was 0 (March: 1).

Chart 4-1: All the Consultation Number Accepted by IPA over the Past 6 Months

	Nov.	Dec.	Jan. '09	Feb.	Mar.	April
Total	713	839	960	1,051	1,406	1,668
Automatic Response System	363	458	529	521	758	962
Telephone	288	331	390	472	597	651
e-mail	62	49	39	57	49	55
Fax, Others	0	1	2	1	2	0

*IPA consults/advises about computer viruses, unauthorized computer accesses, problems relevant to Winny as well as the other information concerning overall security issues.

Mail: virus@ipa.go.jp for virus issues, crack@ipa.go.jp for crack issues, winny119@ipa.go.jp for emergent consultation relevant to Winny, fushin110@ipa.go.jp for suspicious mail handling and isec-info@ipa.go.jp for other security relevant issues.

Tel.: +81-3-5978-7509 (24-hour automatic response; in person consultation by an IPA Security Center personnel is available from Mon. – Fri., 10:00 – 12:00, 13:30 – 17:00.)

Fax: +81-3-5978-7518 (24-hour automatic response)

*"Automatic Response System": Numbers responded by automatic response

*"Telephone": Numbers responded by the Security Center personnel

*The Total case number includes the number in Consultation (d) column of the Chart in the “III. Reported Status for Unauthorized Computer Access” and “IV. Accepting Status of Consultation”.

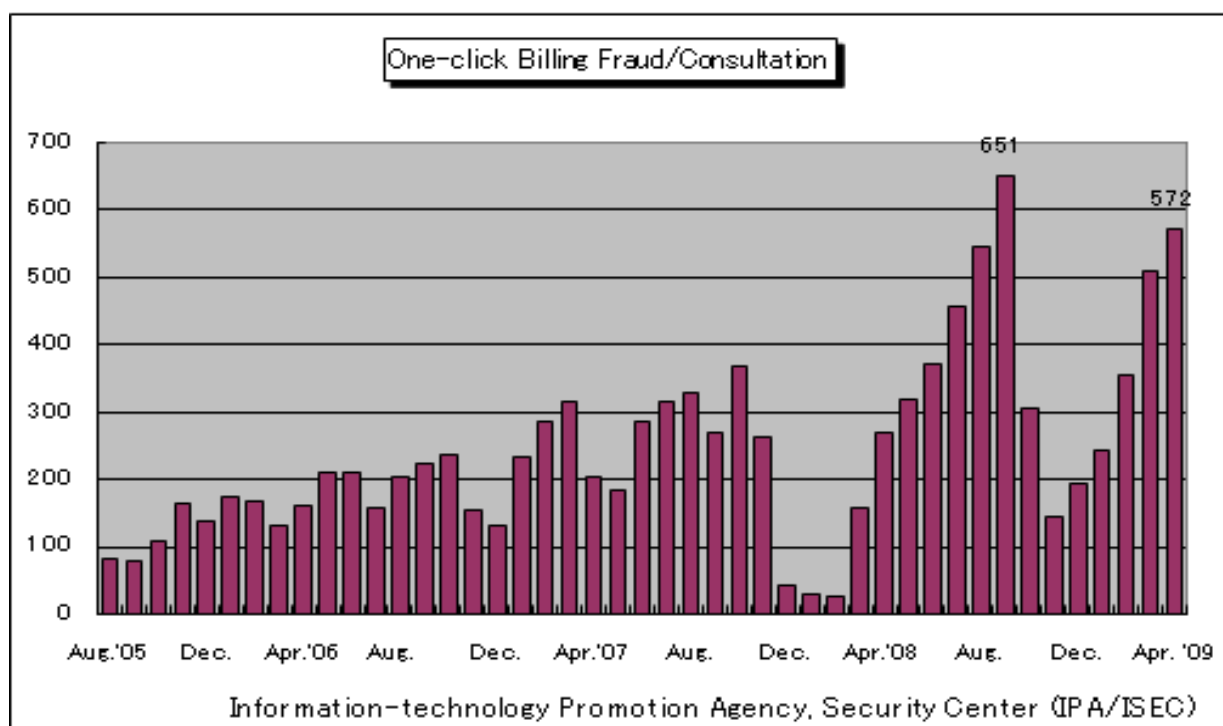


Chart 4-1: One-click Billing Fraud/Consultation

The major consultation instances are as follows.

(i) I may be infected by virus via the attachment file to suspicious e-mail...?

Consultation	I received a mail which I do not know via a free web mail. I saved the attachment file to the mail and opened it as none of virus was detected by the anti-virus software installed in my computer; however, there appears error display all over the screen thereafter. Am I infected by virus? My computer is already initialized.
Response	<p>Upon checked the subjected file with several anti-virus software, there detected virus with number of software. Though nothing was detected with the anti-virus software A, but some virus may be detected by the anti-virus software B. Specifically, the attachment file to an e-mail that you do not know or the file for which source is unknown should not be opened till with or without of virus is identified.</p> <p>If you need to open it, we encourage you to check with or without of virus with several anti-virus software. "VIRUS TOTAL" is the one of recommended services that can parse suspicious file via on-line. This is free and with or without of virus can be identified using about 40 types of anti-virus software simultaneously.</p> <p><Reference> VIRUS TOTAL http://www.virustotal.com/</p>

(ii) I may be fraudulently accessed...?

Consultation	<p>It seems that my computer was fraudulently accessed and is being hijacked for several years. The symptoms are:</p> <ul style="list-style-type: none"> - The activity of my anti-virus software is interrupted and disabled. - When I attempt to shut down, my computer warns that "someone is still logging-in". <p>Can you tell me what shall I do? I am subscribing radio LAN service.</p>
Response	<p>According to the condition you'd explained to us, it seems to be hard to explore the fundamental cause: accordingly, we encourage you to initialize your computer any way with the following procedures to identify matters.</p> <ul style="list-style-type: none"> - Initialize your computer and router. Use wired LAN, rather than radio LAN. - Connect your computer to a network to maintain your OSs and anti-virus software always up-to-dated. - Install trustful software only such as package software as minimum as possible. - You can browse trustful site only such as news site, etc., but should avoid to log in to the site in where requires you to sign-up. Also you need to avoid writing messages on e-bulletin, etc. - See how they work. If nothing specific can be identified, you can increase the software you want to install one by one. - Again, see how they work. If no problem, you can log in only to trustful site (s). <p><Reference> IPA-Seven Rules of Virus Countermeasures for PC Users http://www.ipa.go.jp/security/english/virus/antivirus/7RulesV.html</p>

V. Accessing Status Captured by the Internet Monitoring (TALOT2) in April

According to the Internet Monitoring (TALOT2), the total of unwanted (one-sided) number of access in April was **110,995** for the 10 monitoring points and the gross number of source* was **41,366**. That is, the number of access was **370** from **138** source addresses/monitoring point/day.

*Gross number of source: the gross number of the source accessed the TALOT2. In addition, the source will be counted as 1 if accessed from identical source in the same day to the same point/port.

Since each monitoring environment for the TALOT2 is nearly equal to the general connection environment used by the Internet; it can be considered that the same amount of unwanted (one-sided) access can be monitored for the general Internet users' connection environment.

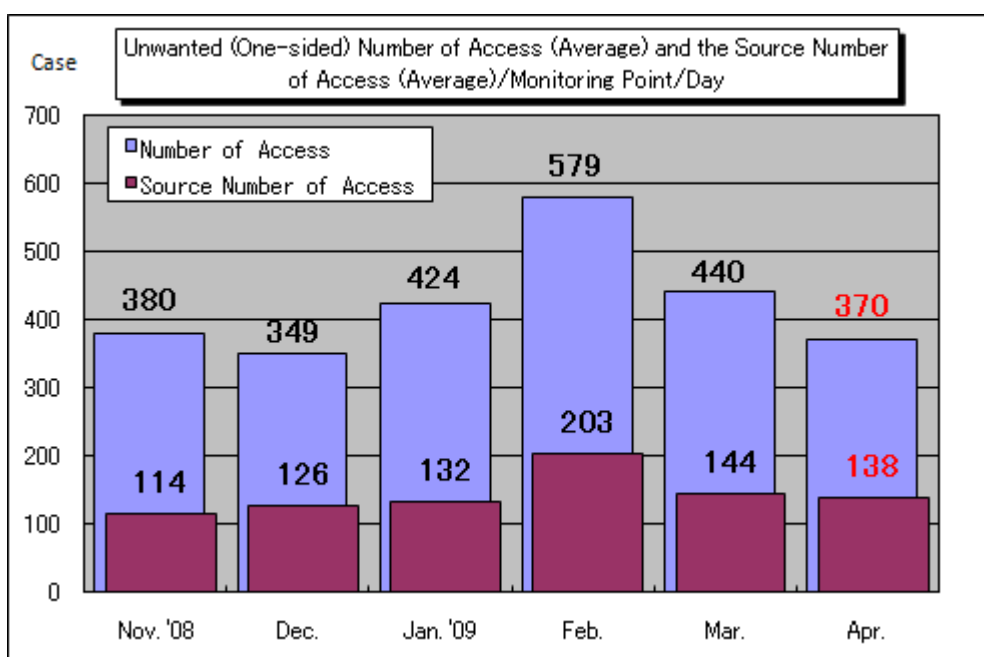


Chart 5-1: Unwanted (One-sided) Number of Access and the Source Number of Access/Monitoring Point/Day

The Chart 5-1 shows the unwanted (one-sided) number of access (average) and the source number of access (average)/monitoring point/day from November 2008 to April 2009. Both the unwanted (one-sided) number of accesses (average) in April were decreased compared with the ones in March.

The Chart 5-2 shows the comparison of number of access classified by destination (port type) in March and April.

None of the 10 frequently accessed ports was drastically shifted in number from March. The cause mostly affected the frequently accessed ports to decrease was the accesses to the ports other than the 10 frequently accessed ports: the number of access (average) lessened about 13T (decreased about 70%) from March. Another reason was that there observed several accesses for which cause was unknown in March: however, in April, such access was not observed.

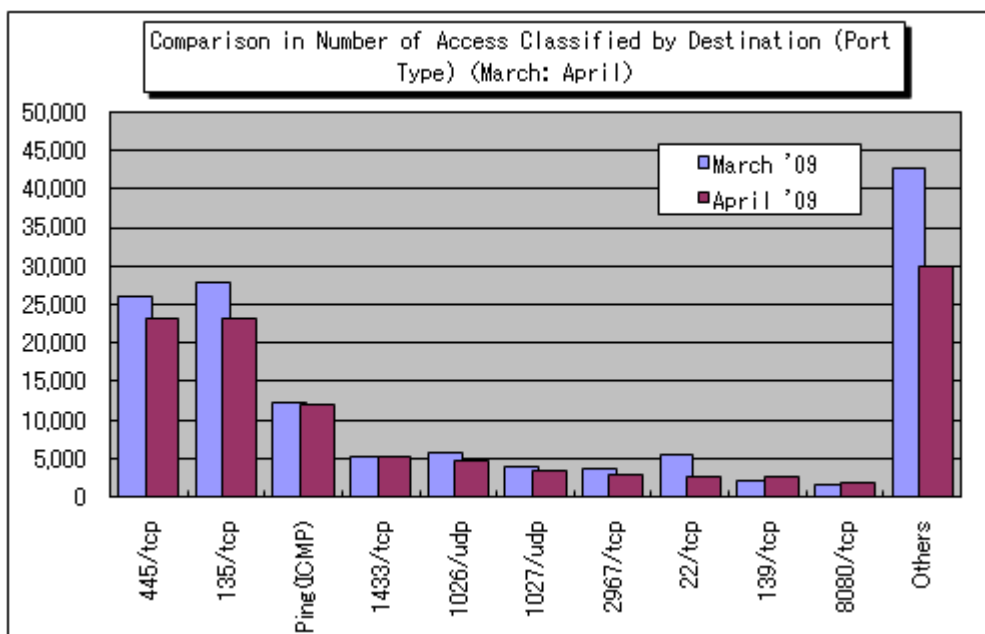


Chart 5-2: Comparison in Number of Access Classified by Destination (March: April)

For more detailed information, please also refer to the following URLs.

Attachment_3: Accessing Status Captured by the Internet Monitoring (TALOT2)

<http://www.ipa.go.jp/security/english/virus/press/200904/documents/TALOT2-0904.pdf>

Summary Reporting Status for Computer Virus/Unauthorized Computer Access for December

<http://www.ipa.go.jp/security/english/virus/press/200904/documents/summary0904.pdf>

Attachment_1 Computer Virus Incident Report

<http://www.ipa.go.jp/security/english/virus/press/200904/documents/virus0904.pdf>

Attachment_2 Unauthorized Computer Access Incident Report

<http://www.ipa.go.jp/security/english/virus/press/200904/documents/crack0904.pdf>

Variety of statistical Information provided by the other organizations/vendors is available in the following sites.

@police: <http://www.cyberpolice.go.jp/english>

Trendmicro: <http://us.trendmicro.com/us/home/>

McAfee: <http://www.mcafee.com/us/>

Symantec: <http://www.symantec.com/>

Inquiries to:

Information-Technology Promotion Agency, Security Center

Hanamura/Kagaya/Ooura

Tel.: +81-3-5978-7527

Fax: +81-3-5978-7518

E-mail: isec-info@ipa.go.jp