

Computer Virus/Unauthorized Computer Access Incident Report

- December 2009 -

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

I. Reminder for the Month

- Be sure to look back over the past 2009 to verify YOUR security measures -
 “Do not forget the evil hands behind you – adequate security measures is the best medicine*”

* The 5th IPA Information Security Catch-phrase and Poster Contest in 2009: The Catch-phrase won among junior-high school students

Looking back to the virus infection mechanism over the entire 2009, one can be said that their infection mechanism was further sophisticated with widely differentiated aspects than the one recognized in 2008. The virus which infects the computer who browsed via business/private websites previously altered or those which enlarge infection via outside memory media such as USB memory, etc. are still spreading.

In this way, the virus (es) infected to computers enlarges damages to the other computers, attempts to download different virus (es), etc. that would cause not only to the computer previously infected, but also the other computers.

To prevent such damages, let’s look back to the symptoms caused by virus in 2009 to verify YOUR security measures with us by reviewing their infection mechanism.

(1) The Major Symptoms and their Countermeasures

For here, we will pick up/describe 4 types of peculiar symptoms caused by virus in 2009. Their countermeasures will follow respectively.

- (a) Infected by virus upon browsing websites run by business or private previously altered.**
- (b) Infected by virus via outside memory media such as USB memory, etc.**
- (c) Infected by virus via the file appended to e-mail (“falsified security measures software” type of virus, spear type of virus mails targeting specific business, etc.)**
- (d) Infected by virus, etc. induced to malicious website (s).**

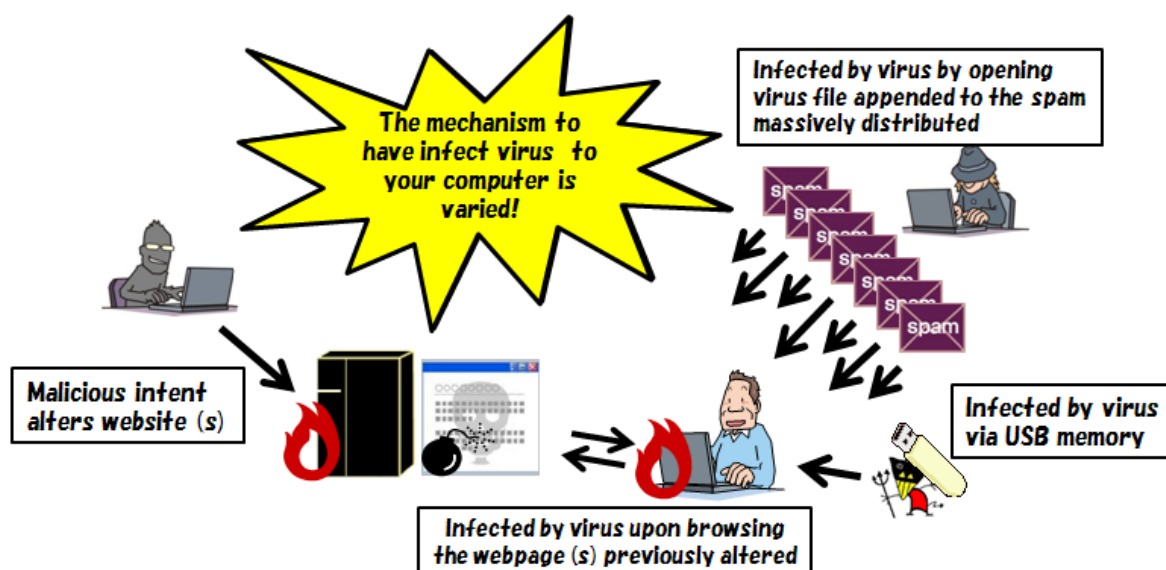


Chart 1-1: Variety of Mechanisms to Infect Virus to your Computer (Image)

(a) Infected by virus upon browsing websites run by business or private previously altered.

The malicious intent who fraudulently accesses to the website with the ftp* account information (user ID, password, etc.) stolen from the website manager alters the webpage so that those who browse the webpage will be infected by virus. It is identified that a computer infected by virus (i.e., spyware) is exploited as the one of the means to steal ftp account information. What if there is vulnerability (ies) (“security hole” in another word) in those who browsed website (s) previously altered, it will be exploited to infect virus to their computers. Once infected, the virus may cause different damages: stealing the account information for online banking, online games, etc. are the part of example. In addition, the virus destructs important files stored in their computers and/or may cause variety of damages. This virus broke out from May to June 2009 all over the world. Once everybody believed that their activities were terminated, however, it regained to enlarge infection on or after November 2009. Here in IPA, such reports and asking consultations relevant to this virus that “the modified website previously altered was again altered”, “virus was detected immediately after accessed to a certain website (s)”, etc. are rushed every day. Accordingly, website managers and website users should conduct following countermeasures without fail.

* File Transfer Protocol to be used to transfer files via a network.

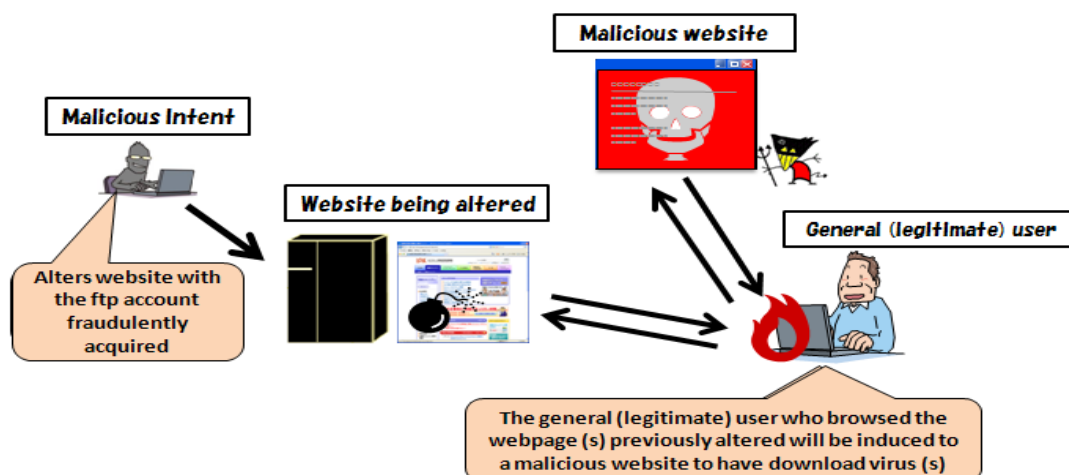


Chart 1-2: The Infection Mechanism

<The countermeasures for website manager>

- Be sure to check out the entire contents of the website you are managing if such script whether you do not know is NOT embedded.
- Be sure to check out the ftp access logs whether anybody is NOT accessed in the time and date while you were not accessing.
- Be sure to use IP address to restrict access to those computers that can be accessible via ftp.
- Be sure to employ/operate website alteration detection system/service.

<The countermeasures for website users>

- Be sure to resolve vulnerability (ies) or security hole (s) in application software you are using.

<Reference>

- “JVN iPedia Vulnerability Countermeasure Information Database”

<http://jvndb.jvn.jp/en/>

- Be sure to maintain your signature files always up-to-dated that can be adequately leveraged whenever you need.

Following URL is another source for both website managers and website users.

<Reference>

“Isn’t your website being altered?” (Reminder for June 2009)

http://www.ipa.go.jp/security/english/virus/press/200906/E_PR200906.html

(b) Infected by virus via outside memory media such as USB memory, etc.

The damage caused by virus is enlarged via outside memory media, such as USB memory (hereafter refers to USB memory). When you connect such USB memory already infected by virus to your computer, Windows auto run function will be exploited by the virus (i.e., your computer is also get infected). Once infected, the virus enlarges infection to the computer linked to a network or the other USB memory (ies) connected to the computer previously infected. Some viruses may lower the computer’s performance. Such damage was initially reported on or around November 2008: from February to May 2009, those computers for private sectors and municipal governments got involved significant damages. To fight against such virus, following countermeasures are effective.



Chart 1-3: Virus Infection via USB Memory (Image)

<Countermeasures upon using USB memory>

- Do not insert such USB memory you are not managing to your computer carelessly.
- Do not insert your USB memory to the computer you are not managing/ those computers to be used by unspecified majority with ease.
- Do not insert the USB memory you OWN to the computer located in your work place; do not insert such USB memory to be used in your work place to your home computer carelessly.

<Via Windows configuration (Disabling the auto run function in Windows)>

- We encourage you to disable your auto run function by configuring Windows: This helps to stop infection even if you inserted such USB memory previously infected by virus to your computer by mistake. Please refer to the following URL how to disable the auto run function. If you are a Windows 7 user, please refer to Windows Vista.

<Reference>

“Are you always recognizing the security measures for USB memory?” (Reminder for April 2009)

http://www.ipa.go.jp/security/english/virus/press/200904/E_PR200904.html

To ensure whether your auto run function is disabled, following tools can be useful: if not, you can also refer how to alter the configuration. Please use this as the one of the means to prevent virus infection via USB memory.

<Reference>

MyJVN Security Configuration Checker (in Japanese)

<http://jvndb.jvn.jp/apis/myjvn/#CCCHECK>

(c) Infected by virus via the file appended to e-mail (“falsified security measures software” type of virus, spear type of virus mails targeting specific business, etc.)

This symptom is to have user (i.e., addressee) clicks virus file appended to e-mail (usually spam) to infect the virus to his/her computer.

As the one of its instances, such virus file appended to e-mail (spam) which spoofing to be an actual research institution was sent to a specific business (es) in June 2009: this mail was seemed to be alerting the epidemic of H1N1, the new flu virus, but was actually a computer virus (i.e., spear type of attack). From September to December 2009, we identified such file previously infected by “falsified security measures software” type of virus appended to e-mail (i.e., spam) spoofing to be Microsoft who notifying (updated) security measures information was massively distributed in relatively extensive area. Moreover, we also identified that suspicious mail spoofing to be a governmental organ was sent to cryptography relevant project parties.

In this case, some documentation technologies (i.e., part of social engineering technique) were used to have the addressees forcibly opening the mail and its attachment to derive necessary information.

To address such symptoms, please be cautious with the following items:

<Spam handling>

- If you received a file appended e-mail from the sender who rarely communicates with, do not immediately open either the mail or the attachment; do not click the link (s) written in the mail body either. Though you received a mail from one of your acquaintances, do not immediately open it and check it with the sender directly if you feel somewhat suspicious.
- If you feel suspicious, never, ever open them and immediately delete them.

Even you feel curious with either the mail subjects or its contents, it is important not to immediately open the mail or its attachment carelessly. Physical number of spam is expected to increase taking advantage such news people mostly interested in, seasonal events, etc. As you already know that there scheduled Winter Olympic games, Succor World Championship, etc. in 2010. Accordingly, it is expected that the physical number of spam will be increased before or after such national events: BE CAUTIOUS.

<Reference>

“The threat relevant to falsified security measures software enlarges again!” (Reminder for October 2009)

http://www.ipa.go.jp/security/english/virus/press/200910/E_PR200910.html

“Be cautious with the computer virus which masquerading to be the alert for H1N1 flu virus!” (Reminder for May 2009)

http://www.ipa.go.jp/security/english/virus/press/200905/E_PR200905.html

(d) Infected by virus, etc. induced to malicious website (s).

This is the method to have a curious user click the link (s) with such phrase “Click here for further details” on show business news, animation posting site (s) and information site (s) for anime/games: the user will be induced to a malicious site and infected by virus while he/she does not know. Often times, such site is designed to have user his/herself downloads virus.

Most of malicious websites are continually displays billing statement for the adult site the user signed up with (while he does not know), automatically appears unwanted ads relevant to adult site over and over, etc. We had so many consultations relevant to the billing statement which stayed on the user’s screen in 2009 as well as we did in 2008. Following are the effective measures for such symptoms.

<Anti-virus measures against malicious website (s)>

- Do not click link (s) carelessly with your simple curiosity.
- Do not either click a link or go forward if you feel somewhat suspicious.
- When you click the word “Download” on movies or image (s) in a malicious website (s), there will be appeared the “security warning” window shown in the Chart 1-4. In another words, if movies and images are legitimate, the “security warning” will not be appeared.

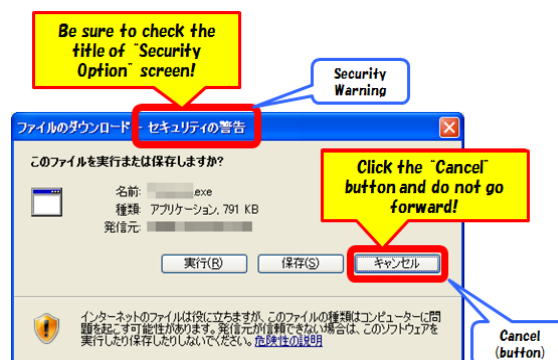


Chart 1-4: “Security Warning” Window for Internet Explorer

What if you click the “Run” button though the “security warning” is appeared, you will download virus by yourself and get infected.

In case the billing statement relevant to an adult site cannot be wiped off from your screen, please refer to the following URLs for specific handling.

<Reference>

“Security warning relevant to One-click Billing Fraud” – updated on December 3, 2009 (IPA)(in Japanese)

<http://www.ipa.go.jp/security/topics/alert20080909.html>

“Ensuring security on the Internet is your own responsibility!! It is you who’d clicked “Yes” (Reminder for November 2009)

http://www.ipa.go.jp/security/english/virus/press/200911/E_PR200911.html

“Isn’t your browser being hijacked?” (Reminder for August 2009)

http://www.ipa.go.jp/security/english/virus/press/200908/E_PR200908.html

(2) Common Security Measures

In the previous section, we described peculiarities of the viruses and their infection mechanism in 2009 respectively; their infection mechanism is very much sophisticated/common that does not allow users recognize that they are infected.

When infected, users may infect virus to the other users’ computers while they do not know; those who believe to be the casualties who got damages caused by virus turned to be the victimizer who causes to infect virus to the other users’ computers, etc. Accordingly, if not recognized that they are infected, every user may have a chance to be the victimizer who causes significant damage (s) to the other users’ computers.

Such threat (s) caused by virus will be open ended – accordingly, to prevent from virus infection, do not connect to the Internet with the computer for which security is insufficient or do not insert your USB memory easily.

Most of all the damages caused by virus infection can be preventable if every user practices the minimal/fundamental security measures described below without fail.

<Fundamental security measures>

- Be sure to update your OSs (operating system) you are using to resolve vulnerability (ies) (security hole (s)) in your computer as far as possible. Be sure to apply the modification programs to update your application software such as the Internet browser, mailing software, animation viewer, document file viewer, etc. installed to your computer as default to resolve vulnerability (ies) (security hole (s)) as well.

- Be sure to update the signature files for your anti-virus measures software you are using to be able to adequately leveraged whenever you need.

For your further security, be sure to back up your important data to the outside memory media (we encourage you to use optic media such as CD-R, external HDD, etc.) in case your computer does not behave properly because of virus, etc.

<Reference>

Microsoft Update helps keep your computer current

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

JVN Vulnerability Countermeasure Notes

<http://jvn.jp/en/>

Brochures for security measures (IPA)(in Japanese)

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

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

(1) Reporting Status of Virus

The detection number of virus (*1) in December was about 66T: decreased about 5.7% from about 70T in November. In addition, the reported number of virus (*2) in December was 981: 13.9% decreased from 1,140 in November.

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

(*2) 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 December, the reported number was 981 and the aggregated virus count was about 66T.

The worst detection number was for W32/Netsky with about 54T: W32/Mydoom with about 4.4T and W32/Whybo with about 3.3T respectively followed.

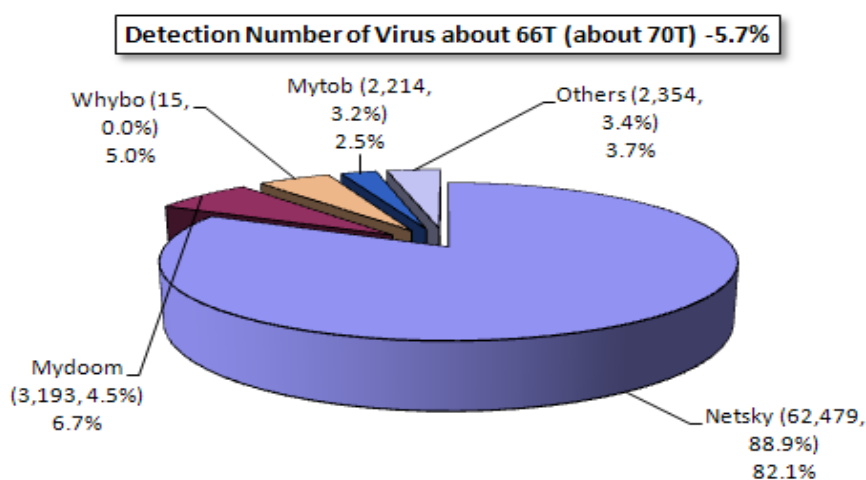


Chart 2-1: Detection Number of Virus

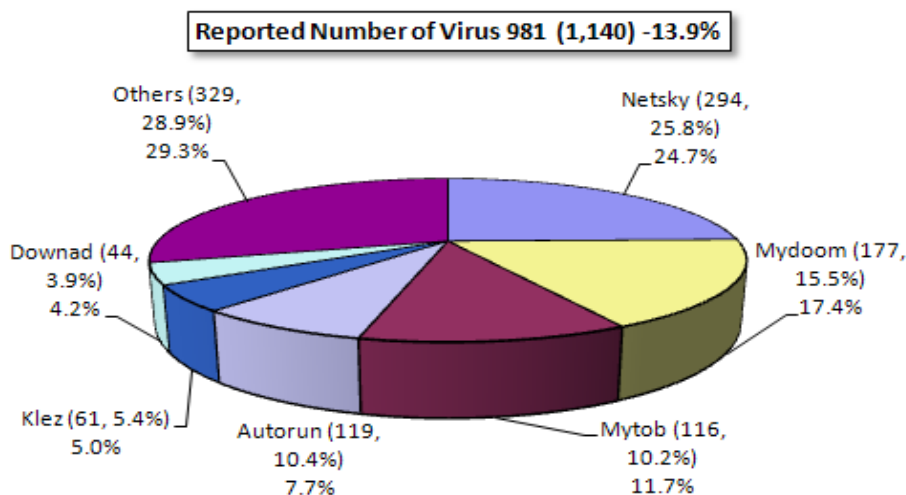


Chart 2-2: Reported Number of Virus

(2) Detection Status of Falsified Program

The detection number of the “falsified security measures software” type of virus (FAKEAV) drastically increased in September 2009 is decreasing: as of now, they are rarely identified (See the Chart 2-3).

Such malicious programs are distributed over and over as the attachment file to e-mail: as you can see from the Chart 2-3, their movements are artificial as they drastically increased/decreased in certain periods, etc. We assume that they are distributed by bot virus: accordingly, we cannot foresee when they will be increased. Users are to pay due care continuously with their movements.

In the Cyber Clean Center (CCC), they provide anti-bot measures and their removal tools. To NOT being a victimizer who distribute virus while you do not know, be sure to conduct adequate security measures to prevent infection by bot: ensuring that your computer is free from bot virus and/or never, ever downloading falsified program is essential.

<Reference>

“The Knowledge how to prevent infection” (CCC)

<https://www.ccc.go.jp/knowledge/> (in Japanese)

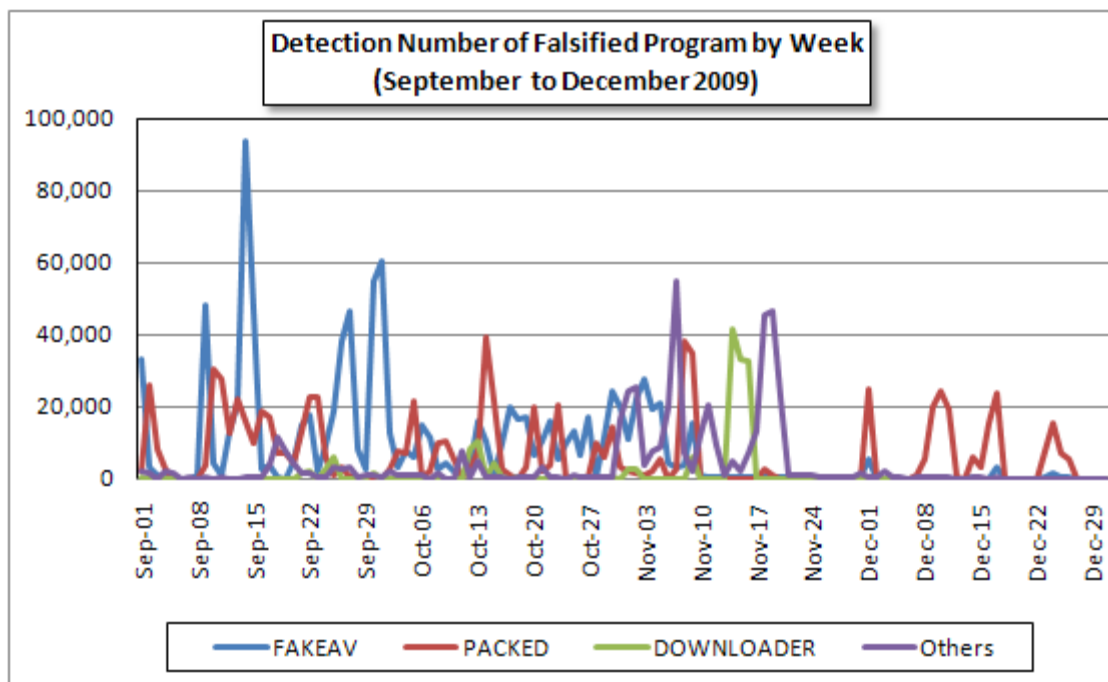


Chart 2-3: Detection Number of Falsified Program by Week (September – December 2009)

III. Reporting Status of Unauthorized Computer Access (includes Consultations) –

Please refer to the Attachment 2 for further details –

Chart 3-1: Reported Number for unauthorized computer access and the status of consultation

	July	Aug.	Sep.	Oct.	Nov.	Dec.
Total for Reported (a)	14	20	11	21	11	9
Damaged (b)	6	12	8	14	6	6
Not Damaged (c)	8	8	3	7	5	3
Total for Consultation (d)	24	39	44	34	34	22
Damaged (e)	3	17	13	11	14	14
Not Damaged (f)	21	22	31	23	20	8
Grand Total (a + d)	38	59	55	55	45	31
Damaged (b + e)	9	29	21	25	20	20
Not Damaged (c + f)	29	30	34	30	25	11

(1) Reporting Status for Unauthorized Computer Access

Reported number in December 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 **22** (of **5** were also counted as reported number): Of **14** was the number actually damaged.

(3) Status of Damage

The breakdown for the damage reports were **intrusion** with **1**, **spoofing** with **2** and **others (damaged)** with **1**. The damage relevant to intrusion included: insertion of malicious codes to webpage with 1, deletion of address information within a web server to distribute mail magazine to subscribers with 1, disabling of firewall software/file alteration with 1. The causes for the intrusions were: the computer to be used to update webpage was infected by virus and ftp account information was stolen with 1, exploited vulnerability (ies) in CGI (common gateway interface) to be used for mail magazine with 1. The other 1 has not yet identified.

As for the damage for “masquerading”, someone spoofing to be the legitimate user who actually signed-up with logged in to use on-line services without asking with 2 (online game with 1, et al).

(4) Damage Instance

[Intrusion]

(i) Falsified codes were inserted to website ...

Instance	<ul style="list-style-type: none"> -The webpage I am managing was not properly displayed: they were turned into garbled characters. -Study was conducted: it was realized that the php files, etc. to be used to update the site was altered: in the event, HTML file which includes malicious codes are also appeared on my webpage (usually, such event should have been done covertly). -The computer to be used to update the webpage was infected by virus: one could be assumed that the ftp account information was stolen when updated the site and having been fraudulently accessed. -This was addressed to restrict the computer to be used to update the site.
----------	--

[Spoofing]

(ii) Points were fraudulently cashed in an online point service site ...

Instance	<ul style="list-style-type: none"> -I am signing up a point-service with which I can exchange points into cash and/or goods. -One day, I am unable to log-in to the service site: upon inquired it to the site manager, my mail address used to sign up with the site was changed with the different one which I do not know. -In addition, all the points I'd saved was already exchanged to e-money (5,000jpy worth) by someone.
----------	---

IV. Accepting Status of Consultation

The gross number of consultation in December was 1,794. The consultation relevant to “**One-click Billing Fraud**” was **576** (November: 903). The others included the consultation relevant to “**Hard selling of falsified anti-virus software**” with **7** (November: 6), the consultation relevant to “**Winny**” with **6** (November: 0), the consultation relevant to “**the suspicious mail sent to specific organization to collect specific information/data**” with **1** (November: 0), etc.

Table 4-1: Gross Consultation Number Accepted by IPA over the Past 6 Months

	July	August	Sept.	Oct.	Nov.	Dec.
Total	1,708	1,792	1,653	2,049	2,315	1,794
Automatic Response System	923	1,015	915	1,157	1,340	1,138
Telephone	736	702	676	843	918	602
e-mail	47	68	60	45	53	52
Fax, Others	2	7	2	4	4	2

*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. Reporting Status of Unauthorized Computer Access” and “IV. Accepting Status of Consultation”.

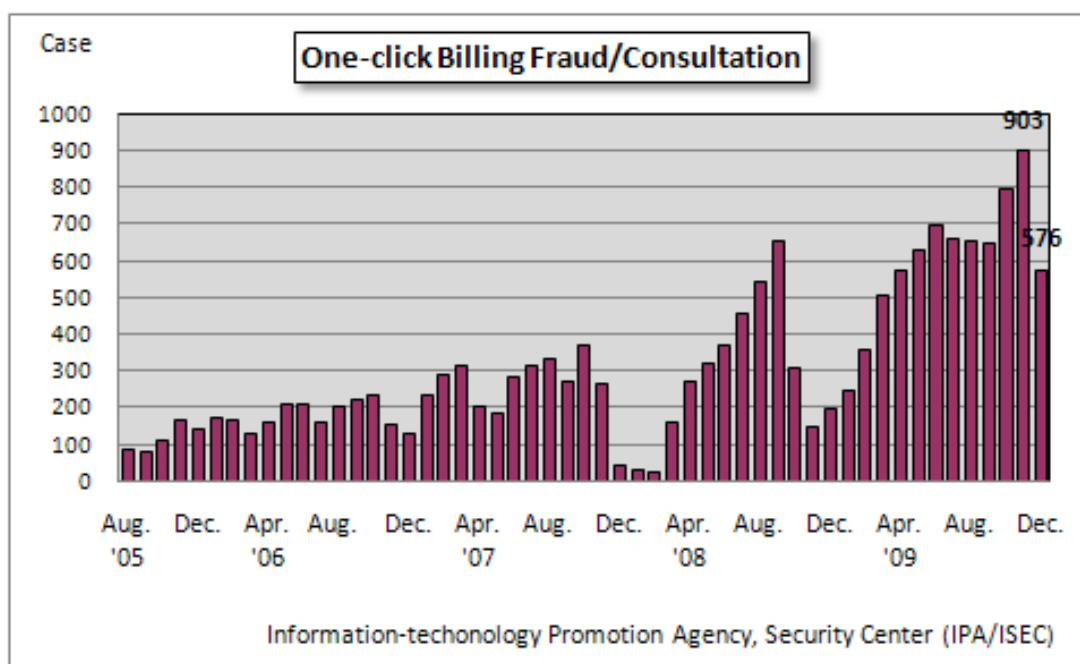


Chart 4-1: One-click Billing Fraud/Consultation

The major consultation instances are as follows.

(i) I do not have to conduct Windows Update if my anti-virus measures is sufficient ...?

<p>Consultation</p>	<p>I do install anti-virus software in my computer so that I think I do not need to conduct Windows Update. Though Windows Update is still necessary, do you mean that any of anti-virus software cannot perfectly block virus? Since I feel troublesome to conduct Windows Update, I do not want to do if possible.</p>
<p>Response</p>	<p>Windows Update is the fundamental part of anti-virus countermeasures. Windows Update is to modify the potential part which may cause troubles relevant to security (i.e., vulnerability or security hole). Accordingly, resolving of vulnerability is the base of the entire security measures. For your information, anti-vulnerability measures needs be conducted not only for Windows, but also for all application you are using. As for major applications such as Adobe Flash Player, etc., IPA provides such tool that can automatically check your version information.</p> <p><Reference> “MyJVN Version Checker” released (IPA) http://www.ipa.go.jp/security/english/vuln/200911_myjvn_vc_en.html</p>

(ii) As I opened the file obtained via a file sharing software, number of files (icons) is replaced by octopus icons ...?

<p>Consultation</p>	<p>Consultation 1: I'd downloaded a movie file via a file sharing software. When I opened, movies and images stored on my computer were overwritten by octopus icons.</p> <p>Consultation 2: I'd downloaded a file for screen saver via Winny. When I opened, all of the files including movies were overwritten by squid icons. I did checked with or without virus, nothing was detected.</p>
<p>Response</p>	<p>You were fooled by the file name or their appearance: we diagnose that you may have been downloaded virus file by yourself and then infected. As with the “Harada virus” we'd taken up in our February 2008 report, this virus is the one of “destruction” type of virus so that it will be difficult to restore back your data as they were.</p> <p>For your information, other than “destruction” type of virus such as the “Harada virus”, several black “disclosure” type of virus such as Antinny, etc. are also distributed.</p> <p>Accordingly, it is necessary that users including you are to recognize that the file sharing network which unspecified majority users participate is indeed risky. If you do not want to infect by virus, it is better not to use any of file sharing software as far as possible.</p> <p><Reference> “Be Minded, Idleness is the VIRUS’ Workshop” (Reminder for January 2008) http://www.ipa.go.jp/security/english/virus/press/200801/E_PR200801.html</p>

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

According to the Internet Monitoring (TALOT2), the total of unwanted (one-sided) number of access in December was **176,871** for the 10 monitoring points and the gross number of source* was **76,781**. That is, the number of access was **571** from **248** source addresses/monitoring point/day.

*Gross number of source: the gross number of the source accessed to 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.

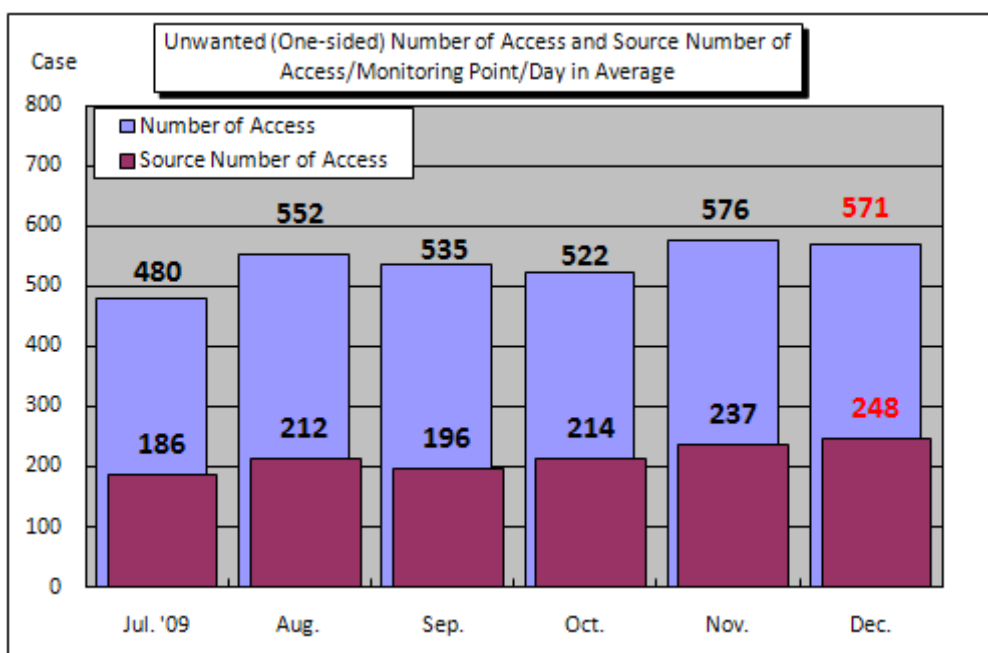


Chart 5-1: Unwanted (One-sided) Number of Access and Source Number of Access/Monitoring Point/Day in Average

The Chart 5-1 shows the unwanted (one-sided) number of access and source number of access/monitoring point/day in average from July to December 2009. Both unwanted (one-sided) number of accesses in December were shifted almost of the same level from those in November.

The Chart 5-2 shows the comparison of number of access classified by destination (by port) in November and December. The access to the port 139/tcp was about 22% increased than the one in November since the access to this port from domestic was increased from the end of November and this tendency was remained in December. The cause of the source number of access increased from domestic in this period has not yet been identified.

In addition, the access to the port 10538/udp which has rarely observed heretofore was significantly increased on December 14. What did this access intend for has not yet been identified, but this was the source number of access which could be monitored only at a specific single monitoring point from severa sources.

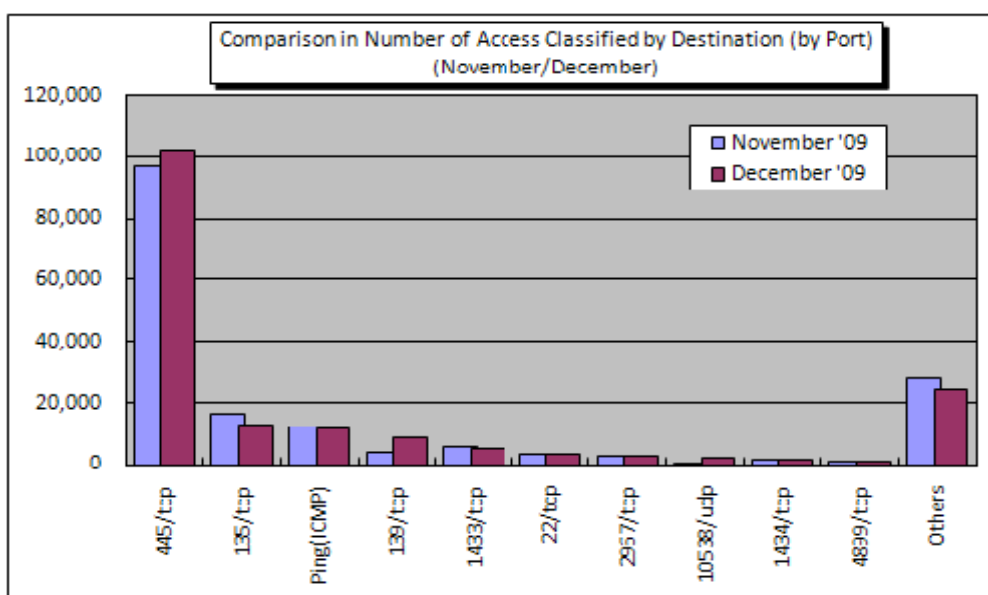


Chart 5-2: Comparison in Number of Access Classified by Destination (by Port) (November/December)

(1) Accessing Status in 2009

The Chart 5-3 shows the unwanted (one-sided) number of access and source number of access/monitoring point/day in average from January to December 2009. Looking back to 2009, the number of access topped in February was once decreased, but was again gradually gotten back to the same level as it was in February.

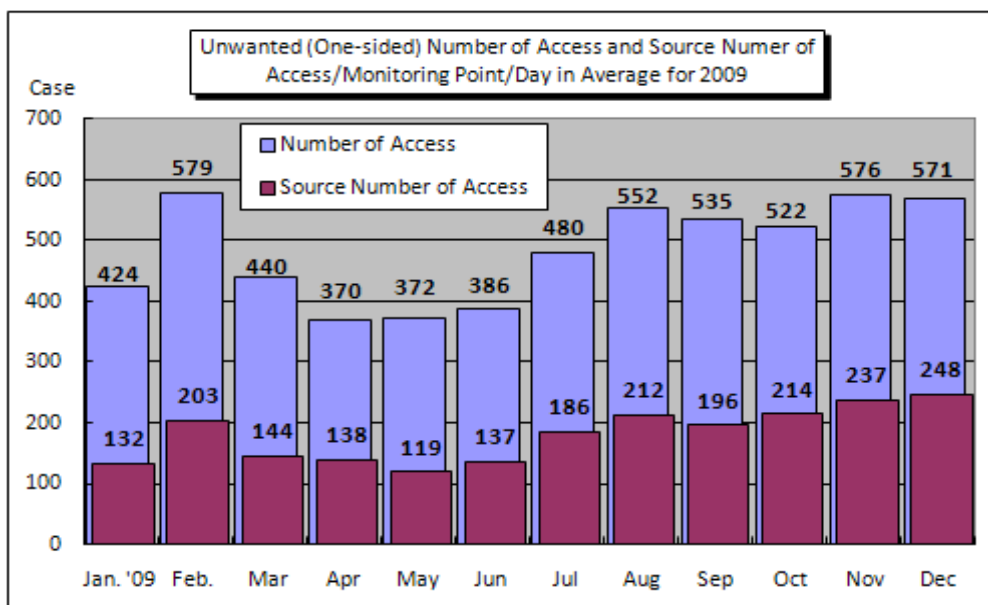


Chart 5-3: Unwanted (One-sided) Number of Access and Source Number of Access/Monitoring Point/Day in Average for 2009

The Chart 5-4 refers the number of access classified by destination (by port) in the Chart 5-3 above. According to this chart, the number of access to the port 139/tcp which once was taken over against the entire number of access was gradually decreased: in contrary, the access to the port 445/tcp showed significant increase; in the event, access to this port was taken over more than a half against the entire number of access.

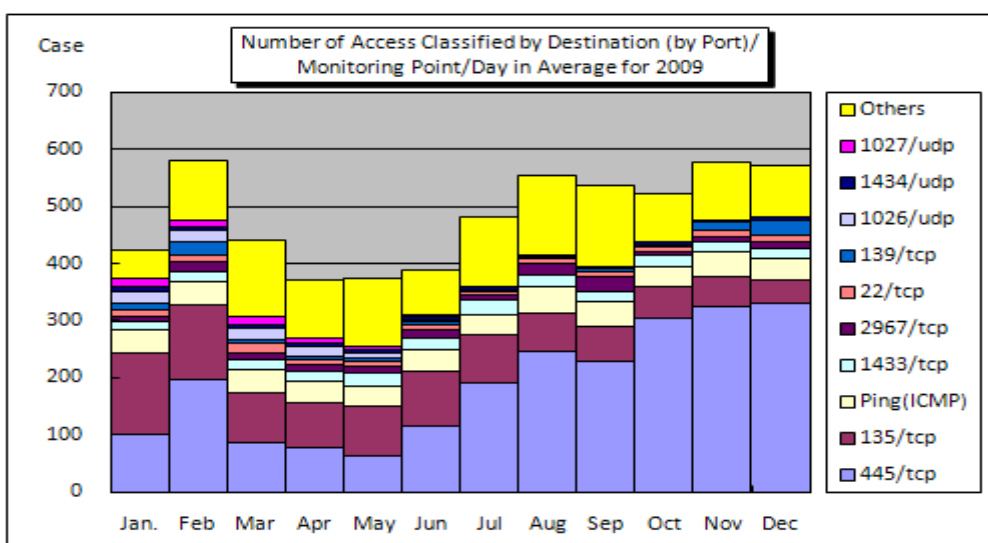


Chart 5-4: Number of Access Classified by Destination (by Port)/Monitoring Point/Day in Average for 2009

The Chart 5-5 shows the comparison in number of access classified by destination (by port) for 2008 and 2009. The number of access to the port 445/tcp was drastically increased about 500,000 cases than the one in 2008 (3.8 times higher). In contrary, the number of access to the port 135/tcp was significantly decreased about 33T than the one in 2008 (48%). In addition, drastic decrease could also be seen in both the number of accesses to ports 1026/udp and 1027/udp since the accesses to both ports could rarely be monitored since middle of June 2009.

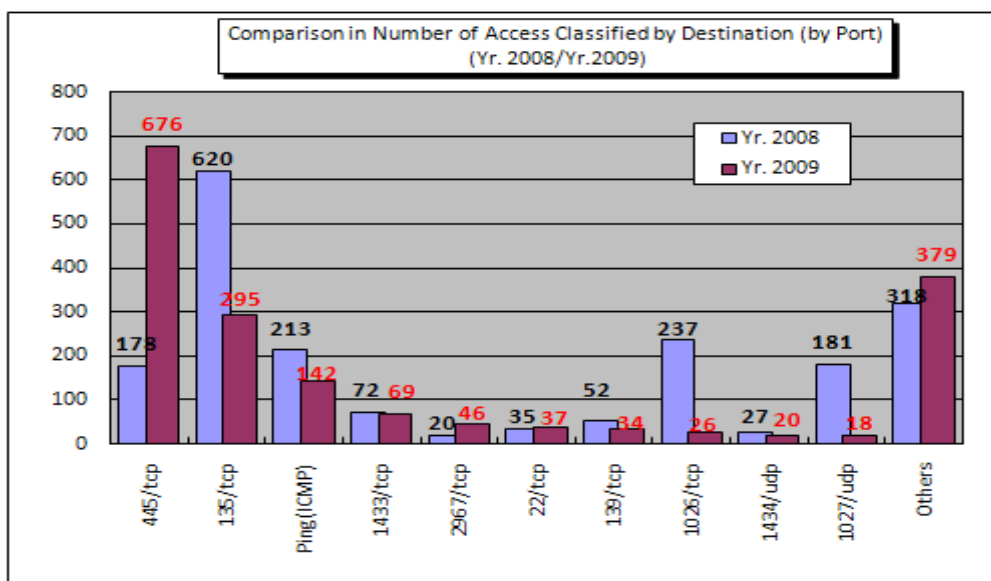


Chart 5-5: Comparison in Number of Access Classified by Destination (by Port) (Yr.2008/Yr.2009)

The remarkable peculiarity in the TALOT2 in 2009 is the drastic increase of number of access to the port to 445/tcp. The access to this port is having been gradually increased on or after October 24, 2008 (Japan time), the date when vulnerability information relevant to Windows (MS08-067) was publicized. The Chart 5-6 shows the shift in number of access to the port 445/tcp since October 2008.

There identified such virus attacks to the port by exploiting this vulnerability so called Downad (alias name: Conficker) on or after this vulnerability was publicized and the damage caused by

this virus is frequently reported from both domestic and overseas. This virus also provides such mechanism which infect outside memory media such as USB memory, etc. Since there identified its variants as well, every user has to continually watch over this virus hereafter.

<Reference>

Microsoft Security Bulletin MS08-067 - Critical

<http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx>

“Vulnerability in Server Service in Windows (MS08-067)” (IPA)(in Japanese)

<http://www.ipa.go.jp/security/ciadr/vul/20081024-ms08-067.html>

“Is Vulnerability in your Computer Adequately Resolved?” (Reminder for January 2009)

http://www.ipa.go.jp/security/english/virus/press/200901/E_PR200901.html

Other than the vulnerability described above, there publicized another vulnerability information which exploits the access to the port 445/tcp on October 14, 2009 (Japan time). In this way, there were number of activities deemed to be attack to the vulnerabilities eventually increased the number of access to the port 445/tcp.

<Reference>

Microsoft Security Bulletin MS09-050 - Critical

<http://www.microsoft.com/technet/security/bulletin/MS09-050.mspx>

“Vulnerability in SMBv2 in Microsoft Windows (MS09-050)” (IPA)(in Japanese)

<http://www.ipa.go.jp/security/ciadr/vul/20091014-ms09-050.html> (in Japanese)

* The maintenance period for the TALOT2 was fallen on from February 6 to 9 so that the system did not work.

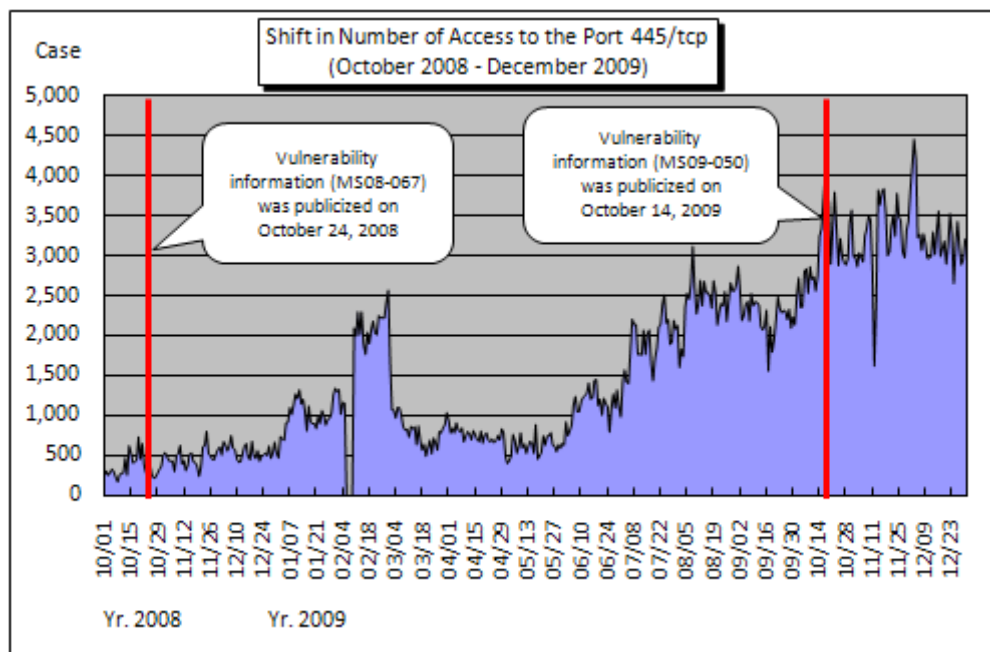


Chart 5-6: Shift in Number of Access to the Port 445/tcp (October 2008 – December 2009)

The fundamental measure to prevent the damage caused by the attack which exploits vulnerability (ies) in Windows is to immediately apply the modification program provided by Microsoft every month successfully. It is also essential that your anti-virus software is always up-to-dated to prevent damages caused by virus infection.

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/200912/documents/TALOT2-0912.pdf>

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

<http://www.ipa.go.jp/security/english/virus/press/200911/documents/summary0912.pdf>

Attachment_1 Computer Virus Incident Report

<http://www.ipa.go.jp/security/english/virus/press/200911/documents/virus0912.pdf>

Attachment_2 Unauthorized Computer Access Incident Report

<http://www.ipa.go.jp/security/english/virus/press/200911/documents/crack0912.pdf>

Attachment_4 Computer Virus Incident Report 2009

<http://www.ipa.go.jp/security/english/virus/press/200812/documents/virus2009.pdf>

Attachment_5 Unauthorized Computer Access Incident Report 2009

<http://www.ipa.go.jp/security/english/virus/press/200809/documents/ua2009.pdf>

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

JPCERT/Coordination Center (CC):

<http://www.jpCERT.or.jp/>

@police:

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

Council of Anti-Phishing Japan:

<http://www.antiphishing.jp/>

Symantec:

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

Trendmicro:

<http://www.trendmicro.com/en/home/us/home.htm>

McAfee:

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

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