1. Computer Virus Reported

(1) Summary for this Quarter

The number of the cases reported for viruses*1 in the third quarter of 2012 decreased from that of the second quarter of 2012 (See Figure 1-1). By virus type, **W32/Mydoom** was reported most. As for **XM/Laroux** which is a type of macro virus, although the number of the cases reported decreased from that of the second quarter of 2012, it had slightly been increasing since the second quarter of 2011 (See Figure 1-2). This is **due to the spread of infection by the subspecies of XM/Laroux.** Meanwhile, the number of the cases reported for **W32/Autorun** decreased to one-third of that of the second quarter of 2011. This is **because the "Autorun" function, which is often exploited for W32/Autorun infection, came to be disabled*2 automatically by a security patch for Windows.**

As for the number of the viruses detected*3 in the third quarter of 2012, **W32/Mydoom** accounted for over half of the total; it was on the increase (See Figure 1-3). On the contrary, **W32/Netsky** was on the decrease and in the second quarter of 2012 and later, it was outpaced by **W32/Mydoom** in **terms of both the number of the cases reported and the number of the viruses detected**. **W32/Mydoom and W32/Netsky attach copies of themselves to an e-mail attachment, with the goal of spreading infection to the recipients of such e-mail. It is assumed that there are still a large number of the servers and PCs that are infected with these viruses.** From the number of the viruses detected, we can see that many of those viruses reached a point within an inch of their target PCs. However, because the users of those PC were using antivirus software, they were able to prevent their infection.

As for the number of the malicious programs detected in the third quarter of 2012, **Invo,** which masquerades as a pay slip for a courier company overseas and attempts to infect PCs, **Adware,** which is a collective term for the programs that display advertising messages, and **Bancos,** which steals IDs/Passwords for online banking systems, were detected in large numbers. The number of the malicious programs detected as a whole has increased in this quarter (see Figure 1-4).

Most of these viruses and malicious programs use e-mails as their infection route (see Figure 1-6). **So, by properly using antivirus software, you can, nine out of ten, prevent the infection of those viruses. In addition, you should be careful with the opening of e-mail attachments and discard suspicious e-mails without reading them.**

*1 Number of the cases reported: If multiple reports submitted by the same person contained the same virus with the same detection date, they are counted as one report regarding that specific virus.

*2 IT Security Center, IPA "Let's disable the "Autorun" function for USB sticks etc. You can do it by applying Windows Update" (http://www.ipa.go.jp/security/txt/2011/03outline.html)

*3 Number of the viruses detected: indicates how many times a specific virus was detected according to the reports submitted.

* Number of the malicious programs detected: It refers to the summary count of malicious programs that were reported to IPA in that period and that do not fall in the category of computer viruses defined by the "Computer Virus Countermeasures Standard".

* Computer Virus Countermeasures Standard (Announcement No.952 by the Ministry of International Trade and Industry): final decision was made on Dec. 28, 2000 by the Ministry of International Trade and Industry (MITI), which was renamed the Ministry of Economy, Trade and Industry (METI) on Jan. 6, 2001.
"Computer Virus Countermeasures Standard" (METI)
http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm (in Japanese)

(2) Virus Infection Reported

In the third quarter of 2012, **two** virus infection cases were reported**: one for W32/Downad** and the other for **W32/Fujacks**. Infection routes were: "External media" (1 case) and "Unknown" (1 case). Infectious causes were: "The antivirus software's pattern files not updated" (1 case) and "Unknown" (1 case).

How these viruses were detected was: **"By antivirus software" (both cases); in one case, they were not detected by the previously-used antivirus software but the newly-installed one, and in the other case, they had not been detected first by the antivirus software in use because its pattern file had not been updated, but after the update, they were detected.**

In the light of these instances, it is essential to use the latest version of antivirus software and keep its pattern files up-to-date. It is also effective to perform multilateral scan by using online scan services provided by other security vendors.

(3) Number of the Cases Reported for Viruses

In the third quarter (July to September) of 2012, the number of the cases reported for viruses was **2,595**. The graph below (Figure 1) shows the trend in the quarterly (i.e., three months') figures.
As shown in Figure 1, the number of the cases reported in this quarter decreased slightly from that of the second quarter of 2012 (**down 65** from **2,660**).

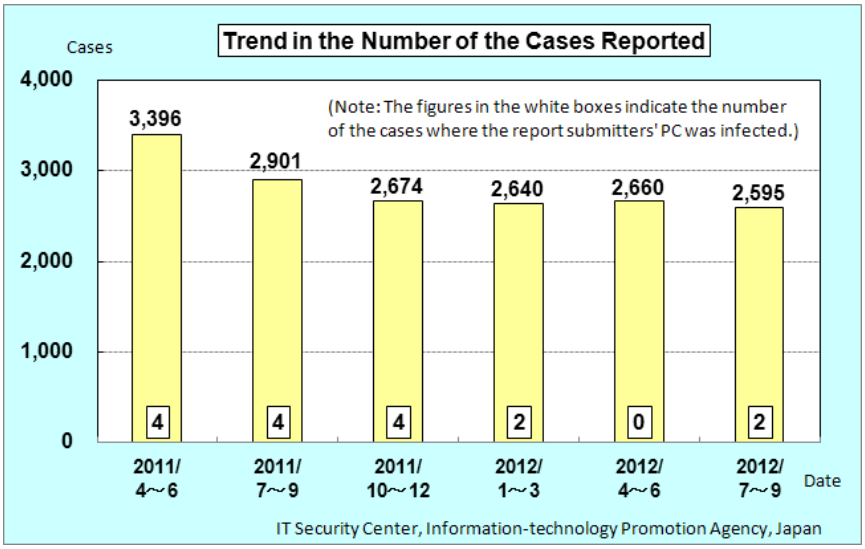


Figure 1-1: Trend in the Number of the Cases Reported (Quarterly Figures)

In the third quarter of 2012, **two** virus infection cases were reported. The name of the infecting viruses*[4] were **W32/Downad (1 case)** and **W32/Fujacks (1 case).** The details are as follows:

Table 1-1: Details of the Cases Reported for Virus Infection

Virus name	Type of repot submitter	Antivirus software	Infection route	Infectious cause	How it was detected	Actions taken
W32/Downad	General corporation	Installed	External Media	The antivirus software's pattern files not updated	By using the antivirus software with its pattern files updated	Initialization of that PC
W32/Fujacks	General corporation	Installed	Unknown	Unknown	By installing another antivirus software and performing virus scan	Installation of another antivirus software; scanning and cleaning by the software,

*4 For more details on the reported viruses, please refer to "The viruses that have been reported to IPA" (http://www.ipa.go.jp/security/virus/virus_main.html)

(4) Number of the Cases Reported (by Virus)

In the third quarter of 2012, **W32/Mydoom** was reported most (**591),** followed by **W32/Netsky** (**463**) and **W32/Autorun** (**175**) (See Figure 1-2).

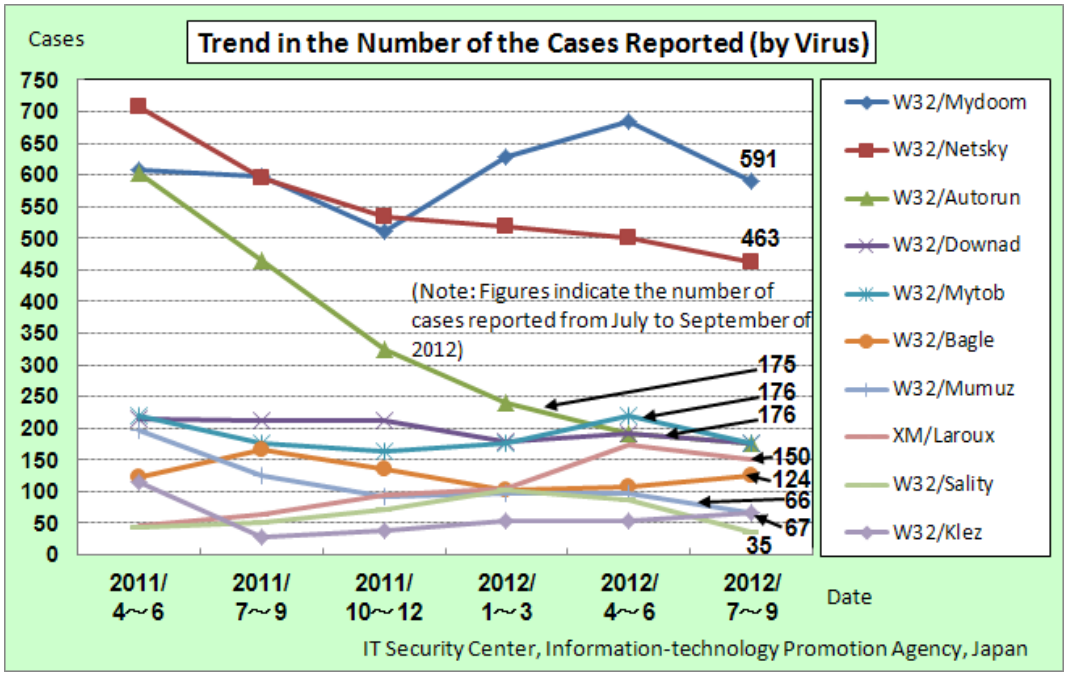


Figure 1-2: Trend in the Number of the Cases Reported (by Virus)

(5) Number of the Viruses Detected

In the third quarter of 2012, the number of the viruses detected was **69,738**, up **17,173** from **52,565** in the second quarter of 2012 (see Figure 1-3).

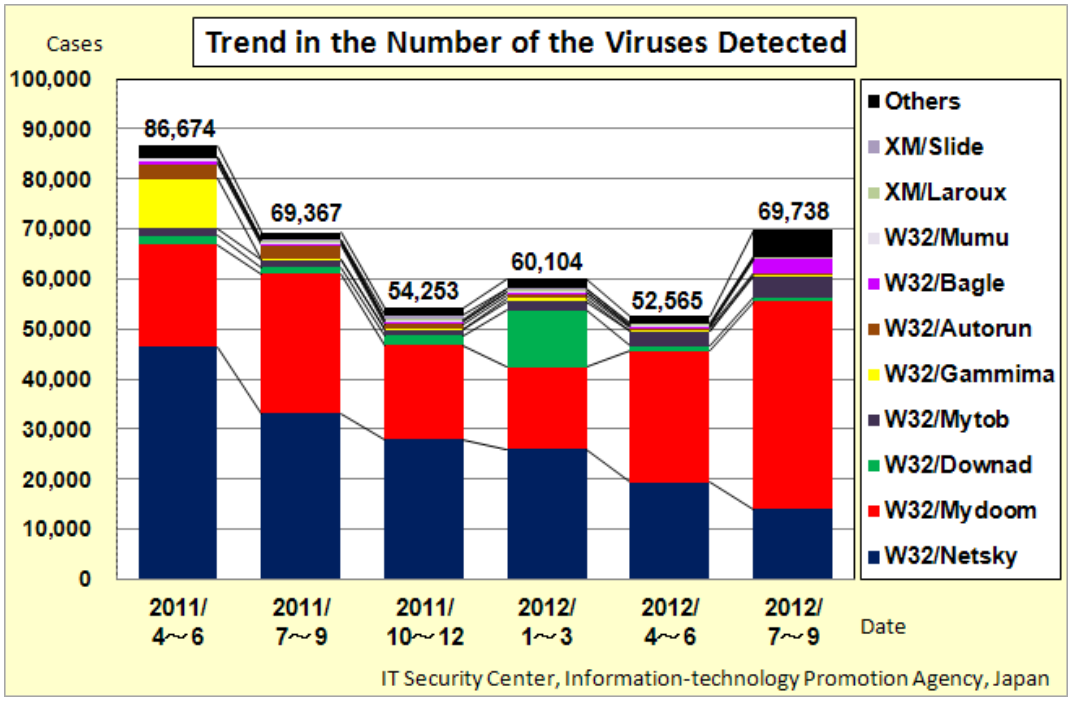


Figure 1-3: Trend in the Number of the Viruses Detected

(6) Number of the malicious programs detected

In the third quarter of 2012, the number of the malicious programs detected for top 10 malicious programs was **77,345**, up **9,630** from **67,715** in the second quarter of 2012 (see Figure 1-4).

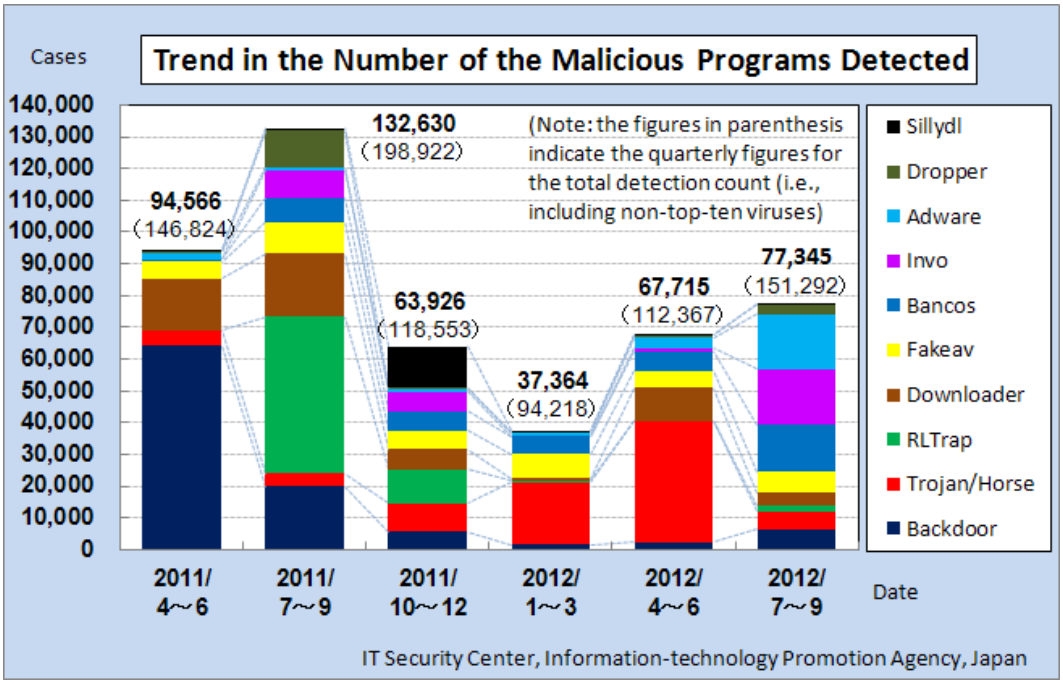


Figure 1-4: Trend in the Number of the Malicious Programs Detected

(7) Viruses Reported in the Third Quarter of 2012

79 types of viruses were reported in the third quarter of 2012, with 2,229 reports related to Windows/DOS, 343 reports to script virus and macro virus, 22 reports to PDA virus, and 1 report to Linux virus.

Note: Repot count includes that of the virus's subspecies. The symbol * indicates newly-discovered viruses.

i) Windows/DOS virus	Report count
W32/Mydoom	591
W32/Netsky	463
W32/Downad	176
W32/Mytob	176
W32/Autorun	175
W32/Bagle	124
W32/Klez	67
W32/Mumu	66
W32/Virut	42
W32/Fbound	41
W32/Gammima	38
W32/Sality	35
W32/Lovgate	27
W32/Funlove	26
W32/Chir	17
W32/IRCbot	15
W32/Fakerecy	12
Perl/Santy	10
W32/Dotex	10
W32/Mabezat	10
W32/Licum	8
W32/Antinny	7
W32/Korgo	7
W32/Imaut	6
W32/Palevo	6
W32/Fujacks	5
W32/Morto	5
W32/Parite	5
W32/Stuxnet	5
W32/Whybo	5
W32/Badtrans	4
W32/Sohanad	4
Cascade	3
W32/Allaple	3
W32/Rontokbro	3
W32/Stration	3
W32/Wapomi	3
W32/Almanahe	2
W32/Bugbear	2
W32/Hybris	2
W32/Mabutu	2
W32/Mota	2
W32/Nuwar	2
W32/Sobig	2
W32/Swen	2
W32/Bacterra	1
W32/Joydotto	1
W32/Looked	1

i) Windows/DOS virus	Report count
W32/Moega	1
W32/Nimda	1
W32/Ramnit	1
W32/Traxg	1
W32/Welchia	1
W32/Wergimog (*)	1
Wscript/Kakworm	1
Subtotal (55 types)	2,229

Script virus	Report count
VBS/Solow	12
VBS/LOVELETTER	7
VBS/Mondezimia	3
VBS/Freelink	2
VBS/Internal	2
VBS/Redlof	2
VBS/SST	1
Subtotal (7 types)	29

Macro virus	Report count
XM/Laroux	150
XM/Mailcab	134
XF/Sic	9
WM/Cap	6
X97M/Yini	6
W97M/Lexar	4
XF/Helpopy	2
W97M/Antisr1	1
W97M/Smac	1
WM/Wazzu	1
Subtotal (10 types)	314

ii)PDA	Report count
AndroidOS/Lotoor	11
AndroidOS/Adware	3
AndroidOS/Rootcage	3
AndroidOS/Fakeinst	2
AndroidOS/Rooter	2
AndroidOS/Fakeflash	1
Subtotal (6 types)	22

iii) Macintosh	Report count
None	

iv) OSS (OpenSourceSoftware):Unix including Linux and BSD	Report count
Linux/Adore	1
Subtotal (1 type)	1

< Reference information >
Windows/DOS Virus ... A virus designed to work in the Windows environment and the MS-DOS environment.
Macro Virus ... A virus designed to exploit the macro feature of Microsoft Word/ Excel etc.
Script Virus ... A virus written in a simplified programming language that does not require source code to be converted into machine code.

Note: denotation in the virus name column has the following meaning:

Code	Meaning
W32	Works in the Windows32- bit environment
XM	Abbreviated form of ExcelMacro for Microsoft Excel95/97
WM	Abbreviated form of WordMacro for Microsoft Word95/97
W97M	Abbreviated form of Word97Macro for Microsoft Word97
X97M	Abbreviated form of Excel97Macro for Microsoft Excel97
VBS	Written in Visual Basic Script(VBS)
Wscript	Works in the Windows Scripting Host environment (excluding VBS)
AndroidOS	Works in the Android OS environment
XF	Works under Microsoft Excel95/97. Abbreviated form of ExcelFormula

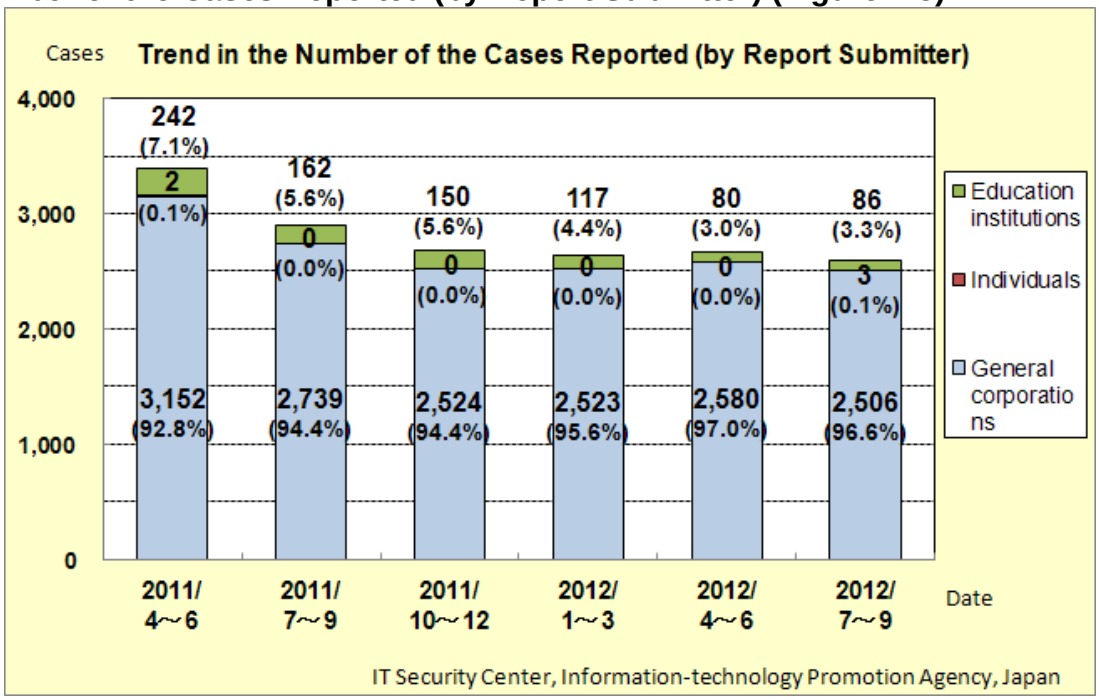
(8) Outline of the Viruses that Were Reported for the First Time to IPA in the Third Quarter of 2012

(1) W32/Wergimog (September 2012)

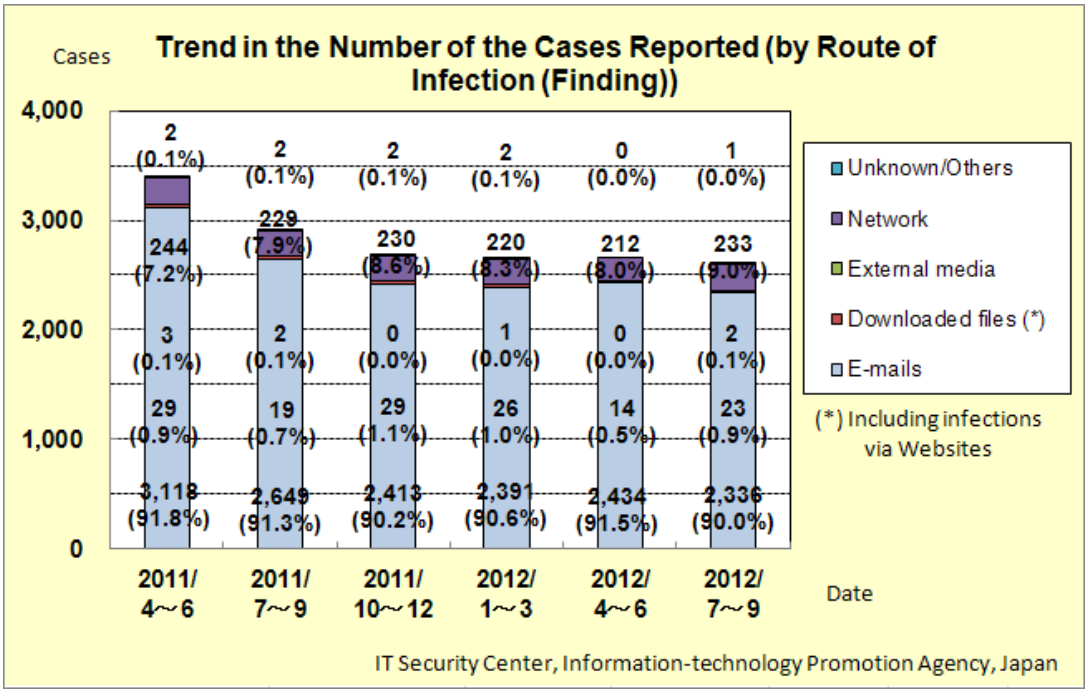
This virus spreads its infection via removable drives.

After the infection, it sets up a backdoor on that PC, steals the information stored, and transfers it to an external party. Some of the subspecies of this virus attempt to post themselves on multiple SNS sites.

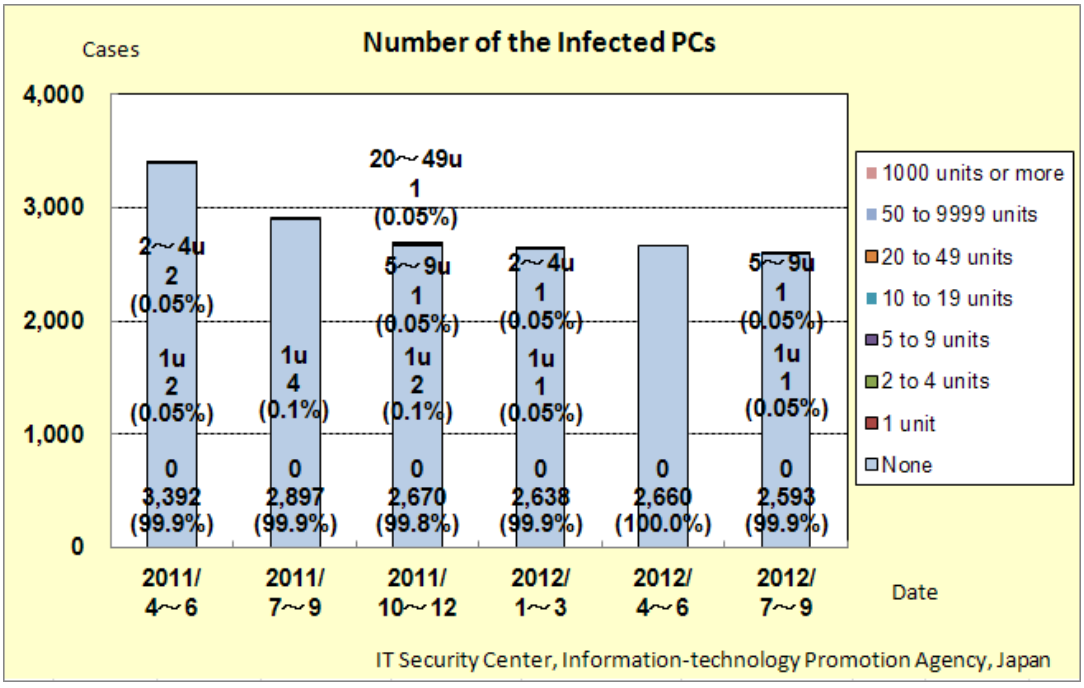
(9) Number of the Cases Reported (by Report Submitter) (Figure 1-5)



(10) Number of the Cases Reported (by Route of Infection (Finding)) (Figure 1-6)



(11) Number of the Infected PCs (Figure 1-7)



Computer Virus Incident Reporting Program

This program was established and enforced in April 1990 by the Ministry of Economy, Trade and Industry (METI) according to its computer virus prevention guidelines and encourages those who detected computer viruses to report them to IPA so that the recurrence or the spread of such infection can be prevented.

While IPA responds individually to each report submitter, it also establishes countermeasures against virus incidents, based the reports submitted. Submitted reports are carefully handled to protect the privacy of report submitters and used solely for the purpose of analyzing damage situation and periodically releasing our findings.

Computer Virus Prevention Guidelines:

Established on July 7, 1995 (Ministry of International Trade and Industry (MITI) release No. 429)
Revised on September 24, 1997 (MITI release No. 535)
Final revision on December 28, 2000 (MITI release No. 952)

The One Designated by the Minister of Economy, Trade and Industry:

January 5, 2004 (METI release No. 2)

2. Unauthorized Computer Access Reported

(1) Summary for this Quarter

Compared to other years, what stood in this quarter was the increase in the number of the cases reported for web defacement. Historically, every summer, we had some international incidents and therefore, summer is a period in which cyber attacks from neighboring countries tend to occur. In the past, however, not many reports concerning website defacement were submitted in this period to IPA. But this quarter, as shown in the graph below, we saw a sharp increase in the number of the cases reported for website defacement*[1]. Such defacement was thought to part of protest from neighboring countries over the sovereignty of some islands*[2].

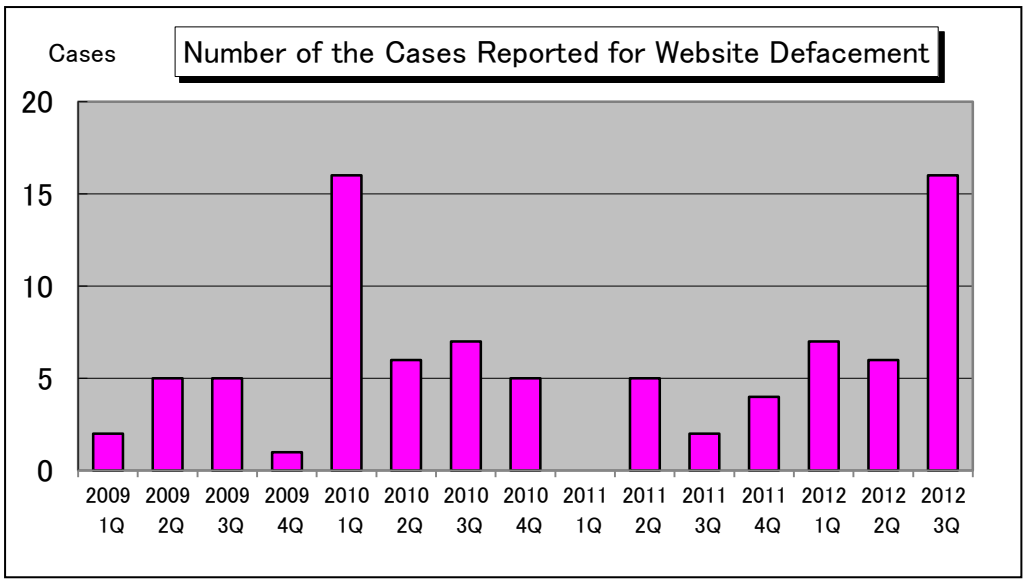


Figure 2-1: Trend in the Number of the Cases Reported for Website Defacement

Some organizations suffered not only website defacement but also DoS attack, theft of information, etc. Especially in this quarter, the number of the cases reported for DoS attack (4 in total) drew our attention (see Table 2-1). Some of them have been identified as attacks from neighboring countries and thought to have been carried out in parallel with website defacement.

According to various news reports, as for a series of website defacement cases that took place in this time, many of them were against government-affiliated organizations, but IPA received such reports from private companies and academic institutions as well. As there is a possibility that every site in the nation might become the target of such attacks, system administrators should understand this present situation, check the following points and implement comprehensive measures.

- Are strict control over and appropriate settings of IDs and passwords done?
- Are security holes eliminated? (NB: if security patches are not applicable, operational workaround should also be included)
- Are appropriate settings of routers and firewalls etc done? Are access control settings done?
- Are access logs regularly checked?

Apart from pretest-motivated website defacement, there is another type of website defacement whose purpose is to redirect the visitors to a phony website which is designed to infect visitors' PC with a virus, and such defacement is continuously taking place. For many of those cases, causes remain unknown. But if the site visitors had implemented fundamental security measures on their PC, they would have been able to escape such damages. While it is imperative that security on the part of websites be enhanced, PC users should also implement security measures without negligence

- Update your operating system and application software (e.g., apply Windows Update/Office Update)
- Set and manage your passwords (e.g., use complex passwords; do not tell them to others, do not

use the same password for multiple sites)

- Make use of routers and personal firewalls
- Check for the encryption setting of your wireless LAN (if possible, use WPA2 instead of WEP)

*1 The increase in the number of the cases reported in the first quarter of 2010 was due to the prevalence of a series of technique: (i) infecting visitors' PC with a virus through 'drive-by-download, (ii) stealing their FTP account by using the virus, (iii) defacing another Website by using those accounts, and (iv) embedding 'drive-by-download' in order to spread the virus infection

*2 Right now, only three cases have been identified as attacks from neighboring countries and other cases are under investigation; however, given the fact that the number of such cases has sharply increased compared to the rest of quarters, It is assumed that the other cases were also of that sort.

(2) Damage Instance

[Intrusion]

（i）A vulnerability in our Server was exploited and its Web pages were defaced

Instance	- On Twitter, a teacher of our school found a tweet saying that our school's web pages were defaced. Upon checking it, we found that our school's front page's content had been replaced with a picture containing Arabic. - An investigation revealed that the front page was altered to refer to others sites and display any pictures contained. Fortunately, it was not something that causes virus infection to visitors, so the Website visitors had no damage. - A vulnerability in CMS*3 plug-in which we were using on our Website for server management was exploited and the front page was defaced. - We are planning to upgrade our CMS to the latest version.

*3 CMS (Content Management System): Web application software which enables users to manage their Website contents (text and pictures) in a comprehensive manner.

［Malicious Program Embedded］

（ii）A backdoor was placed on our server, which was then used for scanning another host

Instance	- We were notified by an external party that suspicious access attempts were being made from an IP address of our school. - So we scanned the server to which that IP address is assigned by using multiple antivirus software and found that a backdoor*4 had been placed in the Windows folder. Furthermore, the system's hidden folder contained a vulnerability scan tool called "DFind"*5. - We don't know how the backdoor was placed. We are running Apache, PHP, MySQL and WordPress on the server and none of them had been upgraded to the latest version, so it is possible that any vulnerability was exploited.

*4 Backdoor: This is a door to allow an intruder to a computer to break it again at a later time and it is placed covertly (i.e., without its administrator noticing it) on the target computer.

*5 DFind: This is a tool to scan computer vulnerabilities. It can scan multiple server software for the presence or absence of certain behaviors as well as their vulnerabilities.

(3) Number of the Cases Reported for Unauthorized Computer Access

The number of the cases reported for unauthorized computer access in the third quarter (July-September quarter) of 2012 was 38, about 181 percent over the previous quarter level. The

number of the cases involving actual damages was 36, about 240 percent over the previous quarter level

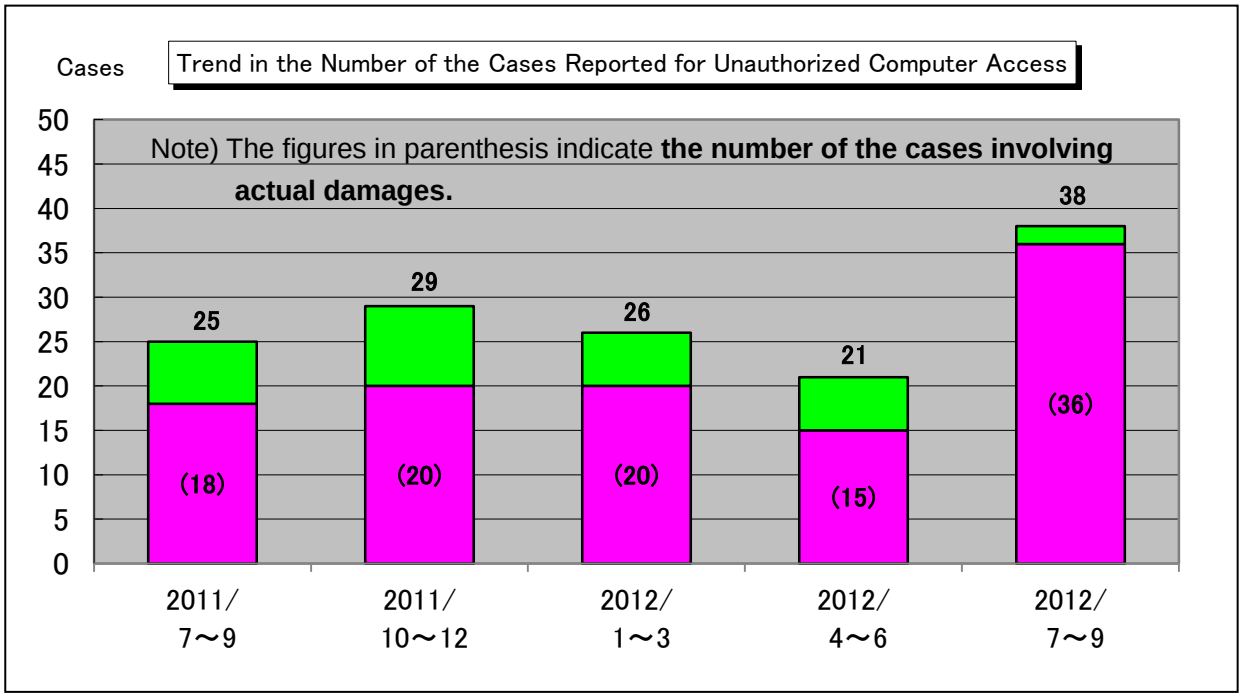


Figure 2-2: Trend in the Number of the Cases Reported for Unauthorized Computer Access

(4) Number of the Cases Reported for Unauthorized Computer Access (by Type)

The number of the cases reported for unauthorized computer access in the third quarter of 2012 was 38 (21 in the previous quarter). Among them, 36 cases (15 cases in the previous quarter) involved actual damages, accounting for 95 percent of all the cases reported. Actual damages in this context are caused by: "Intrusion", "Unauthorized mail relay", "Worm infection", "DoS", "Spoofed address", "Spoofing", "Malicious code embedded" and "Other factors (with damage)", and the number of the cases involving actual damages is calculated by summing up the number of the cases reported for each one of them.

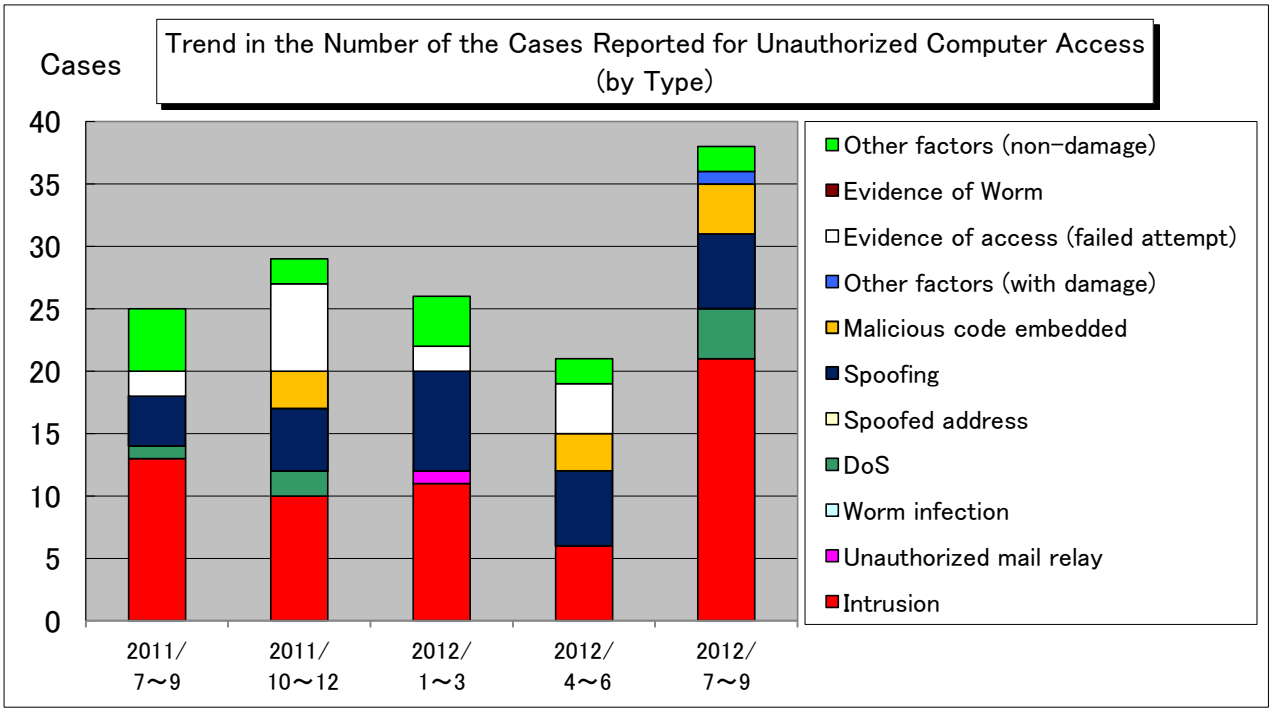


Figure 2-3: Trend in the Number of the Cases Reported for Unauthorized Computer Access (by Type)

Table 2-1: Trend in the Number of the Cases Reported for Unauthorized Computer Access (by Type)

	3rd Qtr. 2011		4th Qtr. 2011		1st Qtr. 2012		2nd Qtr. 2012		3rd Qtr. 2012	
Intrusion	13	52.0%	10	34.5%	11	42.3%	6	28.6%	21	55.3%
Unauthorized mail relay	0	0.0%	0	0.0%	1	3.8%	0	0.0%	0	0.0%
Worm infection	0	0.0%	0	0.0%	0	0.0%	0	0.0%	0	0.0%
DoS	1	4.0%	2	6.9%	0	0.0%	0	0.0%	4	10.5%
Spoofed address	0	0.0%	0	0.0%	0	0.0%	0	0.0%	0	0.0%
Spoofing	4	16.0%	5	17.2%	8	30.8%	6	28.6%	6	15.8%
Malicious code embedded	0	0.0%	3	10.3%	0	0.0%	3	14.3%	4	10.5%
Other factors (with damage)	0	0.0%	0	0.0%	0	0.0%	0	0.0%	1	2.6%
Evidence of access (failed attempt)	2	8.0%	7	24.1%	2	7.7%	4	19.0%	0	0.0%
Evidence of Worm	0	0.0%	0	0.0%	0	0.0%	0	0.0%	0	0.0%
Other factors (non-damage)	5	20.0%	2	6.9%	4	15.4%	2	9.5%	2	5.3%
Total	**25**		**29**		**26**		**21**		**38**	

Note: shaded regions indicate **the cases involving actual damages**. All the ratios shown in the Table above are rounded to one decimal place, so they may not add up to 100 percent.

(5) Number of the Cases Reported for Unauthorized Computer Access (by Cause) (Only for the Cases Involving Actual Damages)

Of the 36 cases involving actual damages, **7 cases were caused by "Older version used/patch not applied", 3 cases by "Poor ID & password management", and 3 cases by "Inappropriate setting"**.

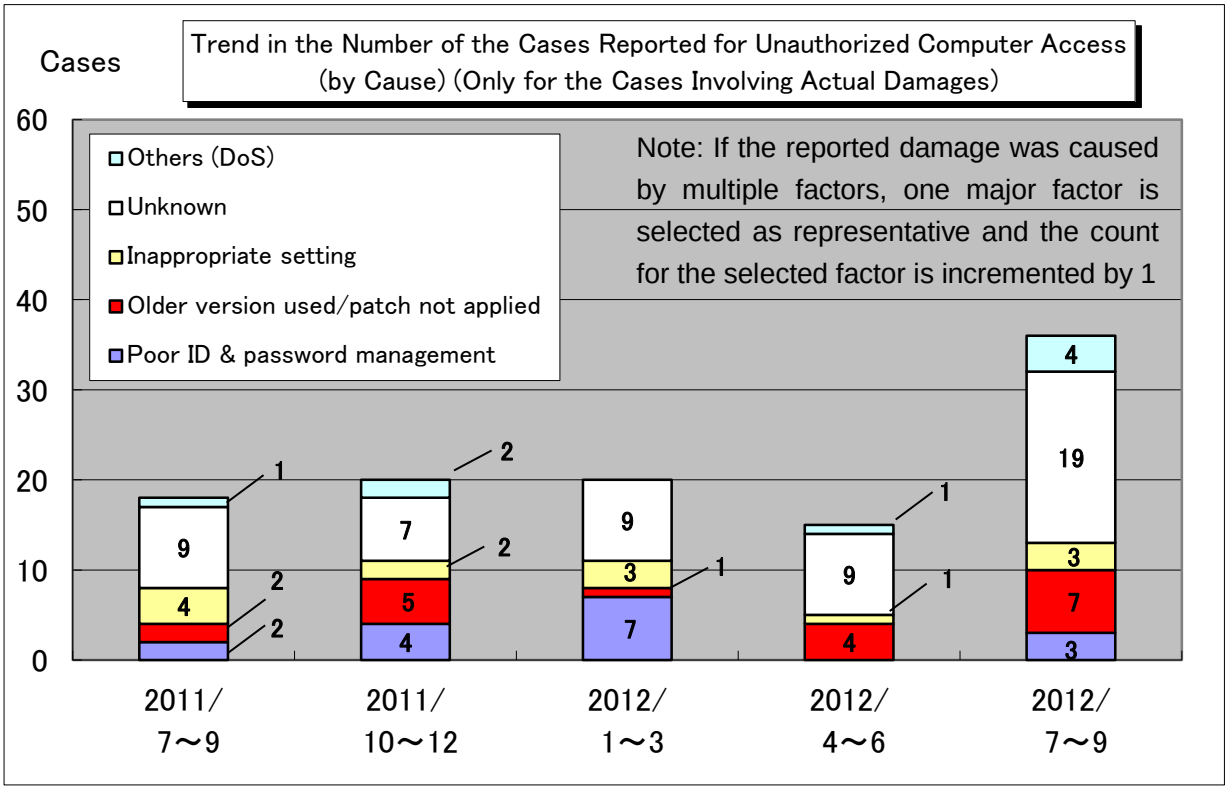


Figure 2-4: Trend in the Number of the Cases Reported for Unauthorized Computer Access (by Cause)

(6) Number of the Cases Reported for Unauthorized Computer Access (by Report Submitter)

Breakdown of the report submitters is as follows:

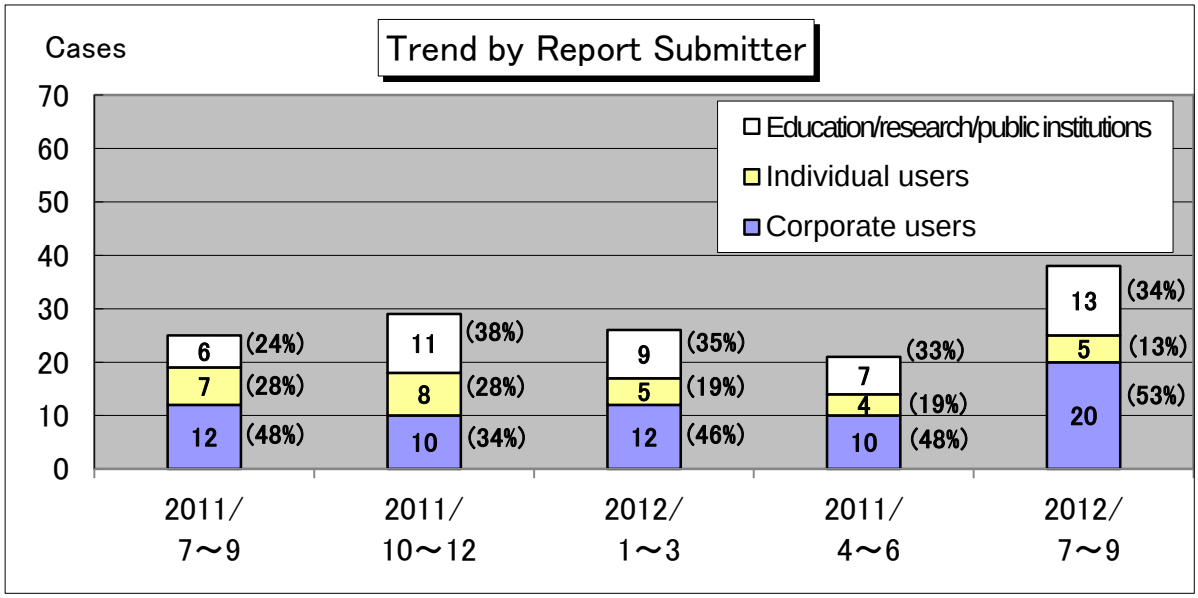


Figure 2-5: Trend in the Number of the Cases Reported for Unauthorized Computer Access (by Report Submitter)

Unauthorized Computer Access Reporting Program

This program was established and enforced in August 1996 by the Ministry of Economy, Trade and Industry (METI) according to its unauthorized computer access prevention guidelines and encourages those who suffered from unauthorized computer access to report them to IPA so that recurrence or the spread of such incident can be prevented.

While IPA responds individually to each report submitter, it also establishes countermeasures against unauthorized computer access, based on the reports submitted. Submitted reports are carefully handled to protect the privacy of report submitters and used solely for the purpose of analyzing damage situation and periodically releasing our findings.

Unauthorized Computer Access Prevention Guidelines:
Established on August 8, 1996 (Ministry of International Trade and Industry (MITI) release No. 362)
Revised on September 24, 1997 (MITI release No. 534)
Final revision on December 28, 2000 (MITI release No. 950)
The One Designated by the Minister of Economy, Trade and Industry:
January 5, 2004 (METI release No. 3)

3. Consultations

(1) Summary for This Quarter

The number of the cases consulted for virus and unauthorized computer access in the third quarter (July-September quarter) of 2012 was **2,819**, **717** of which were related to **"One-click Billing Fraud"** (compared to 693 in April-June quarter); **95** to **"Fake Security Software"** (compared to 57 in April-June quarter); **19** to **"Winny"** (compared to 13 in April-June quarter); **6** to **"A Suspicious E-Mail Sent to a Specific Organization to Collect Specific Information/Data"** (compared to 7 in April-June quarter)

Among the cases consulted for virus and unauthorized computer access, those related to "One-click Billing Fraud" has remained at the same level since the first quarter of 2012. **In these days, the number of the cases consulted for "One-click Billing Fraud" against smartphone has been increasing**, but they are still fewer than that of "One-click Billing Fraud" against PCs. However, when we look at the trend in the number of the consulted cases that contained the keyword "smartphone", we can see that the number has been increasing, so smartphone users should watch out for "One-click Billing Fraud" as well.

Furthermore, in these days, the number of the cases consulted for social network has also been increasing. When we look at the trend in the number of the consulted cases that contained the keyword "social network service", we can see the number has also been increasing in recent years.

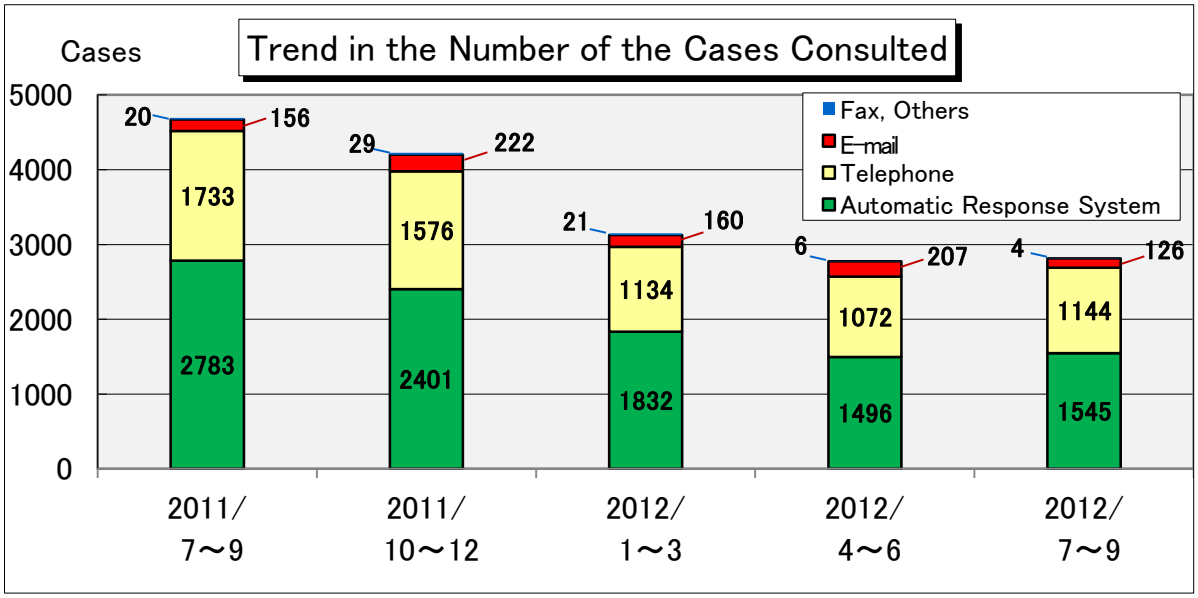


Figure 3-1: Number of the Cases Consulted for Virus and Unauthorized Computer Access

Table 3-1 Number of the Cases Consulted for Virus and Unauthorized Computer Access

	Jul. to Sep. 2011	Oct. to Dec. 2011	Jan. to Mar. 2012	Apr. to Jun. 2012	Jul. to Sep. 2012
Total	4692	4228	3147	2781	2819
Automatic Response System	2783 (59%)	2401 (57%)	1832 (58%)	1496 (54%)	1545 (55%)
Telephone	1733 (37%)	1576 (37%)	1134 (36%)	1072 (39%)	1144 (41%)
E-mail	156 (3%)	222 (5%)	160 (5%)	207 (7%)	126 (4%)
Fax, Others	20 (0%)	29 (1%)	21 (1%)	6 (0%)	4 (0%)

(2) Consultation Instances

Major consultation instances are as follows:

（i） An error mail for an e-mail which I haven't sent arrived at my mailbox

What was consulted	Since yesterday, an error mail titled "Mailer Daemon" began to arrive at my mailbox and the number of such mail has reached one hundred. From the error message, I could see that an e-mail had been sent from my address to an unknown address. I checked my transmission history but could not find such e-mail. Why does the thing like this happen? (I've cleaned a virus recently, but I don't know if there is anything to do with this problem)
Response	There are three possible causes: 1. Your e-mail address was spoofed (impersonation); 2. Your e-mail account was used by an unauthorized person (spoofing through password cracking); 3. Your PC was infected with a Spam delivery virus. Even after cleaning that virus, you had the same symptom, right? So, it is less likely to be case 3. First, you should immediately change the password for your e-mail account. If you stop receiving such error mail, it is more likely to be case 2. If you continue to receive such error mail, it is more likely to be case 1; in this case, it is difficult to stop e-mail address spoofing. **So, consider changing your e-mail address.** If it turns out to be the case 2, it is the case of **unauthorized access**, so please **submit a report to IPA.** <Reference> About reports on unauthorized computer access http://www.ipa.go.jp/security/ciadr/index.html (in Japanese)

（ii） While using mail software, the message "You are going for registration for the certificate"

What was consulted	When I try to send/receive an e-mail, the message "Adding a security exception" appears. Below the message "You are going for registration for the certificate", there are "OK" and "Cancel" buttons. Should I select "Cancel"? I'm using SSL for the connection to my provider's mail server,
Response	At this stage, **we cannot identify its cause, so do not click "OK"**. Such messages may appear due to the following reasons: ・ The certificate issued by your provider's mail server was expired; ・ Your provider's mail server's host name was changed; ・ Your provider's mail server had some sort of problem; ・ Your PC's mail software's settings were changed First, check for your PC's clock time. **If the clock time is out of alignment, the validity of the certificate cannot be checked** and therefore, such message may appear. If the clock time is correct, **consult your provider**. They may have knowledge on the same symptom. If it doesn't fall into any one of the cases listed above and you find no explicit change in the settings of your PC and mail software, **consult IPA again**. <Reference> "Worry-Free Information Security Consultation Service" http://www.ipa.go.jp/security/anshin/ (in Japanese)

(3) Analysis of the Cases Consulted

We graphed the number of the cases consulted for "One-click Billing Fraud" for the second quarter of 2005 and the subsequent quarters. In November 2007, a site operator carrying out "One-click Billing Fraud" by using several consent screens was **arrested**; for a while afterwards, the number of the cases consulted for "One-click Billing Fraud" decreased, but after the turn of the year, it began to increase again.

In September 2008, the site operator was **ruled guilty** and after that, **the number of the cases consulted decreased** temporarily again; however, about half a year later, it began to increase again and surpassed the level before the first decrease.

In October 2010, IPA posted FAQ in its Website and after that, the number of the cases consulted for "One-click Billing Fraud" decreased again.

In the end of 2011, a man conducting "One-click Billing Fraud" was **arrested on multiple charges** and after that, the number decreased further; but given the fact that **IPA is still receiving certain number of such inquiries**, it is obvious that "One-click Billing Fraud" cases are still going on.

Since the end of 2011, the number of inquiries from smartphone users about "One-click Billing Fraud" has also been increasing.

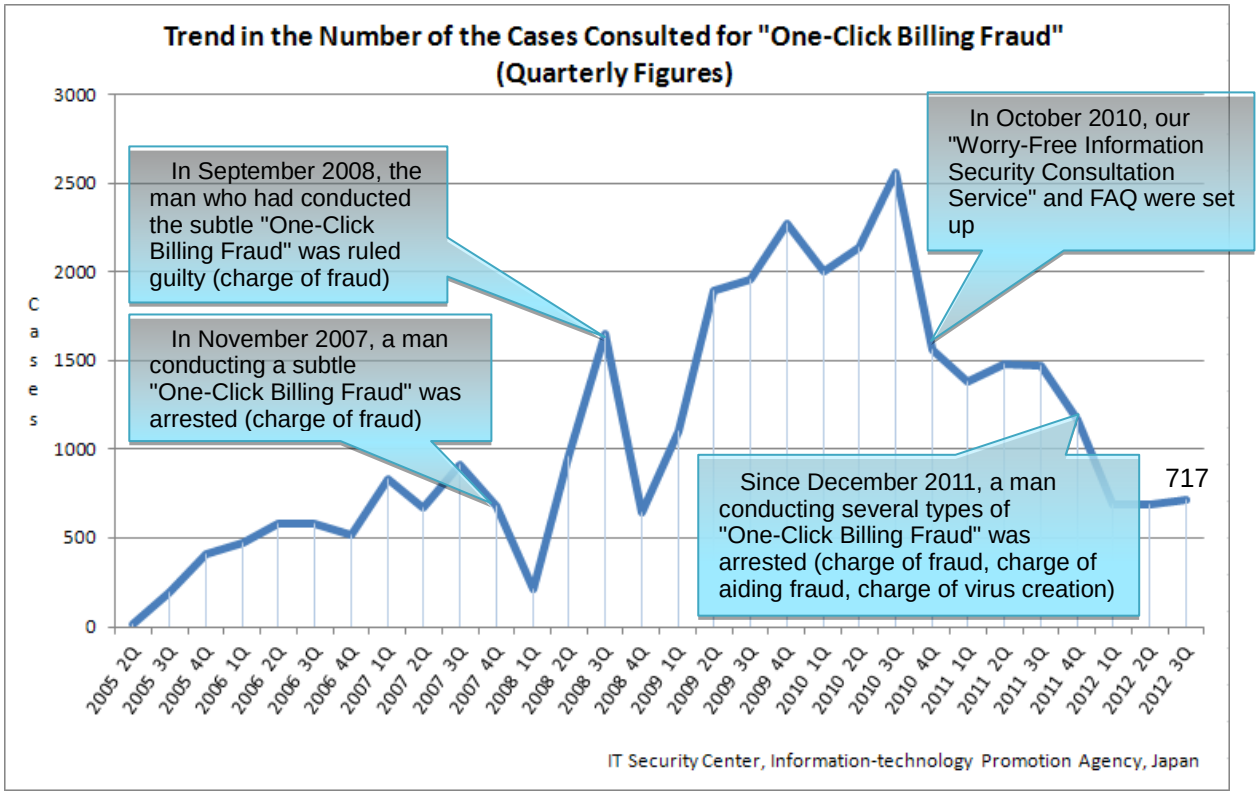


Figure 3-2: Trend in the Number of the Cases Consulted for "One-Click Billing Fraud"

Then we tallied the number of the cases that contained the keyword "smartphone" on a quarterly basis. The result is shown in Figure 3-3. From this result, we can see that along with the increase in the number of smartphone users, IPA began to receive certain number of inquires. The number of such inquires is expected to increase further, backed by the popularization of smartphone.

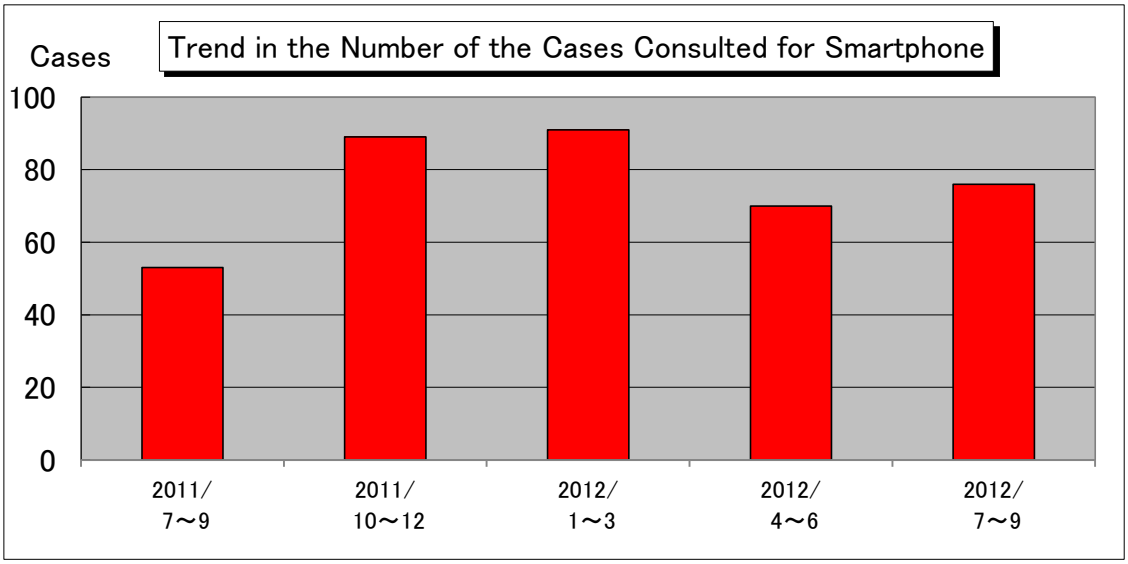


Figure 3-3: Trend in the Number of the Cases Consulted for Smartphone

Figure 3-4 shows the tarried number of the cases related to social network. From this result, we can see that in recent years, the number of inquires about social network has been increasing. Recently, IPA received an increasing number of inquiries from the people, saying: "My PC was infected with a virus while using social network"; "Suffered from an unauthorized login"; "Received a suspicious message", "Without my knowing, an e-mail was sent from my address" are increasing. Along with the popularization of smartphone, social network has now become a major instrument of communication, and the number of inquiries about social network is expected to increase further in the future.

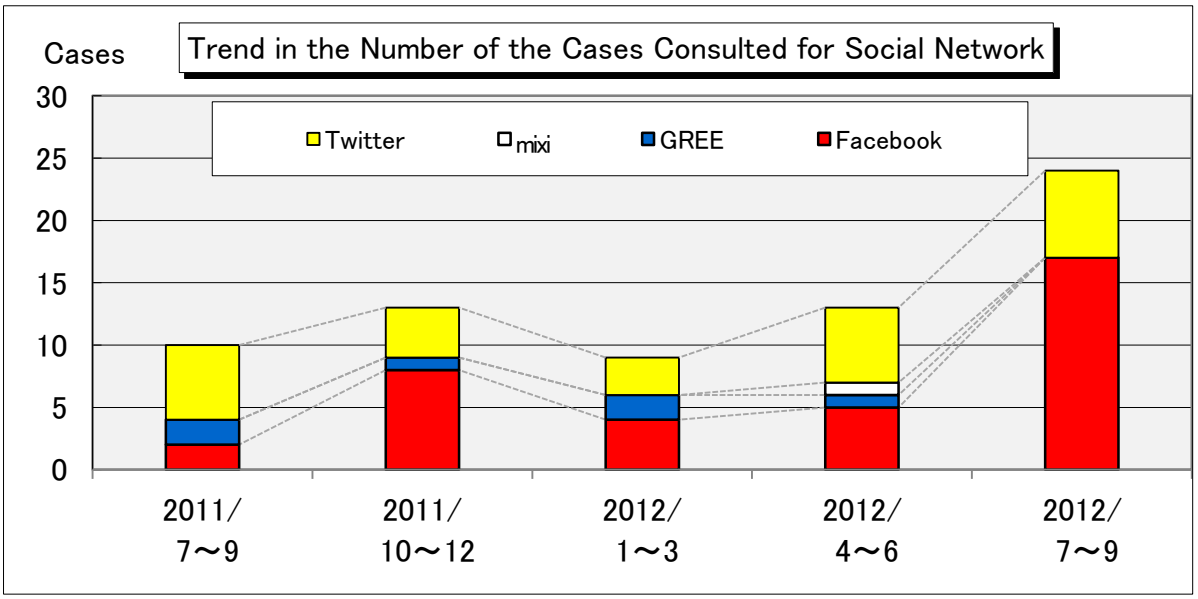


Figure 3-4: Trend in the Number of the Cases Consulted for Social Network

Inquiries to:
IT Security Center, Information-technology Promotion Agency, Japan (IPA/ISEC)
Kagaya/Aoki
Tel: +81-3-5978-7591; Fax: +81-3-5978-7518;
E-mail:isec-info@ipa.go.jp