1. Computer Virus Reported

(1) Summary for this Quarter

The number of the cases reported for viruses*[1] in the first quarter of 2013 decreased from that of the fourth quarter of 2012 (See Figure 1-1).

As for the number of the viruses detected*[2] in the first quarter of 2013, **W32/Mydoom** accounted for **three-fourths of the total** (See Figure 1-2). Compared to the fourth quarter of 2012, however, **both W32/Mydoom and W32/Netsky showed a decreasing trend.**

When we looked into the cases reported for **W32/Netsky**, we found that in most of those cases, the virus code had been corrupted, for which the virus was unable to carry out its infection activity. So, it is unlikely that the number of cases involving this virus will increase significantly in the future

As for **W32/IRCbot**, **it has greatly decreased from the level of the fourth quarter of 2012. W32/IRCbot** carries out infection activities by exploiting vulnerabilities within Windows or programs, and is often used as a foothold for carrying out "Targeted Attack". It is likely that that there has been a shift to attacks not using this virus.

XM/Mailcab is a mass-mailing type virus that exploits mailer's address book and distributes copies of itself. By carelessly opening this type of email attachment, the user's computer is infected and if the number of such users increases, so will the number of the cases reported.

As for the number of the malicious programs detected in the first quarter of 2013, **Bancos,** which steals IDs/Passwords for Internet banking, **Backdoor**, which sets up a back door on the target PC, and **Webkit**, which guides Internet users to a maliciously-crafted Website to infect with another virus, were detected in large numbers. Apart from **Bancos**, however, all of them showed a decreasing trend (see Figure 1-3).

As for **Bancos**, in the first quarter of 2013, it was detected in large numbers in March 2013. One possible reason for this increase is that: the attacker may have waited for such busy period (i.e., the end of the quarter) to come and then carried out mass-mailing against unspecified people.

Meanwhile, **Fakeav**, which is a collective term for fake security software, marked a significant decrease. It is likely that regarding the way to infect with fake security software, there has been a shift from "an attack by email" to "Drive-by-Download" attack against Web audiences. Meanwhile, **reports on a malicious program "Trojan/MBRKill" (described as "Trojan.Jokra" in those reports [The number of the cases reported: 2, the number of the viruses detected: 3]), which is said to have been used for a large-scale cyberattack against Republic of Korea, were submitted to IPA in March 2013.** If infected with this malicious program, **the data on that computer's HDD might be wiped out.**

It is highly likely that **around the time the damage was caused in Republic of Korea, this malicious program entered Japan as well.**

From the number of the viruses detected and the number of the malicious programs detected, we can see that many of them 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.**

Most of these viruses and malicious programs use emails as their infection route (see Table 1-2). **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 email attachments** and **discard suspicious emails without reading them. To counter "Drive-by-Download" attack, which exploits vulnerabilities within operating system (OS) and application software, it is**

essential to keep your OS and application software up-to-date. Be careful not to use older versions.

*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 Number of the viruses detected: indicates how many viruses were detected according to the reports submitted

*3 Number of the malicious programs detected 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 revision 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 first quarter of 2013, no virus infection case was reported.
Still, PC users are required to maintain their information security, by implementing anti-virus measures and other security measures.

(3) Number of the Cases Reported for Viruses

In the first quarter (January to March) of 2013, the number of the cases reported for viruses was **1,803**. The graph below (Figure 1-1) shows the trend in the quarterly (i.e., three months') figures.
As shown in Figure 1-1, the number of the cases reported in this quarter decreased from that of the fourth quarter of 2012 (**down 653** from **2,456**).

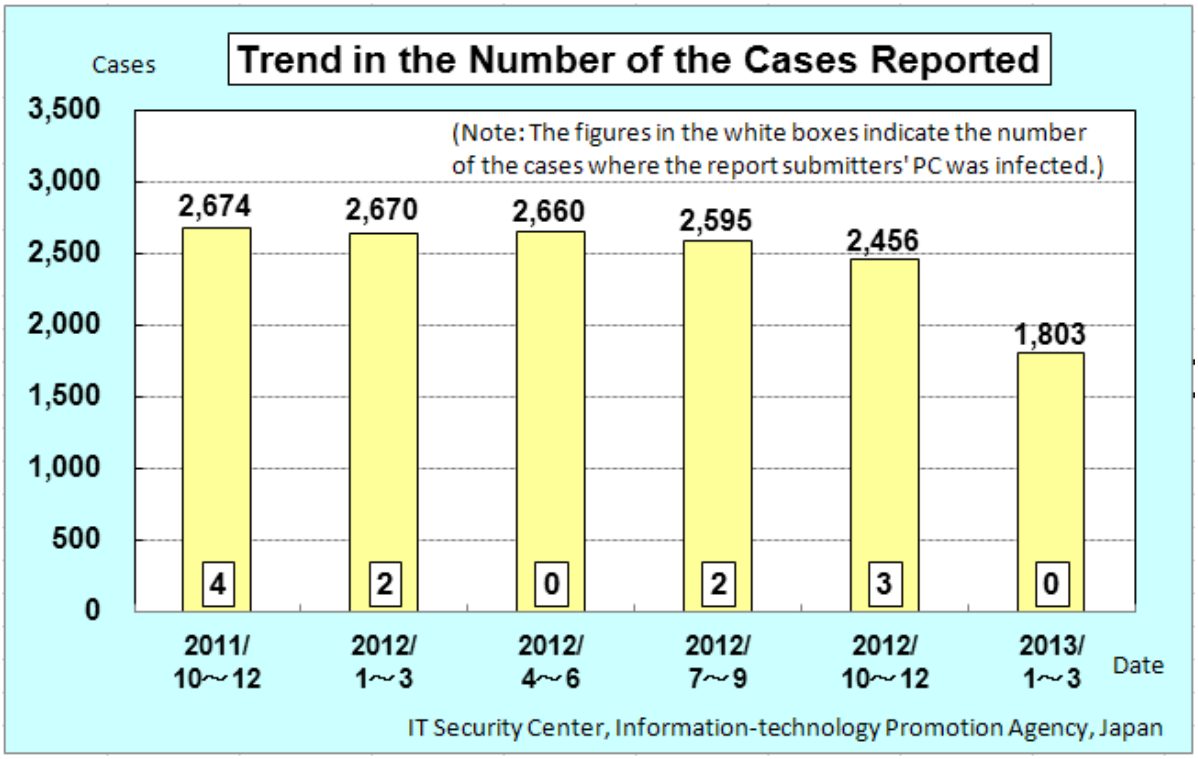

Figure 1-1: Trend in the Number of the Cases Reported (Quarterly Figures)

(4) Number of the Viruses Detected

In the first quarter of 2013, the number of the viruses detected was **56,210**, down **11,323** from **67,533** in the fourth quarter of 2012 (see Figure 1-2).

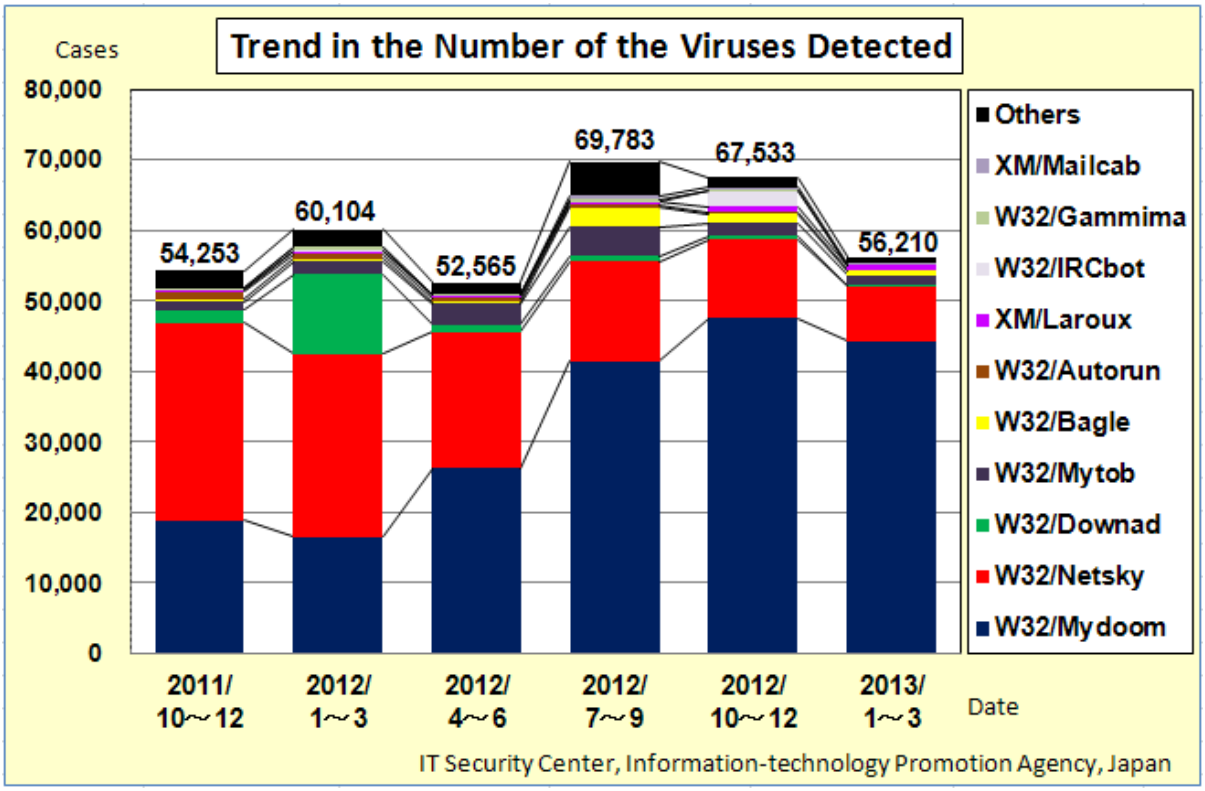

Figure 1-2: Trend in the Number of the Viruses Detected

(5) Number of the malicious programs detected

In the first quarter of 2013, the number of the malicious programs detected for top 10 malicious programs was **23,617**, down **13,863** from **37,480** in the fourth quarter of 2012 (see Figure 1-3).

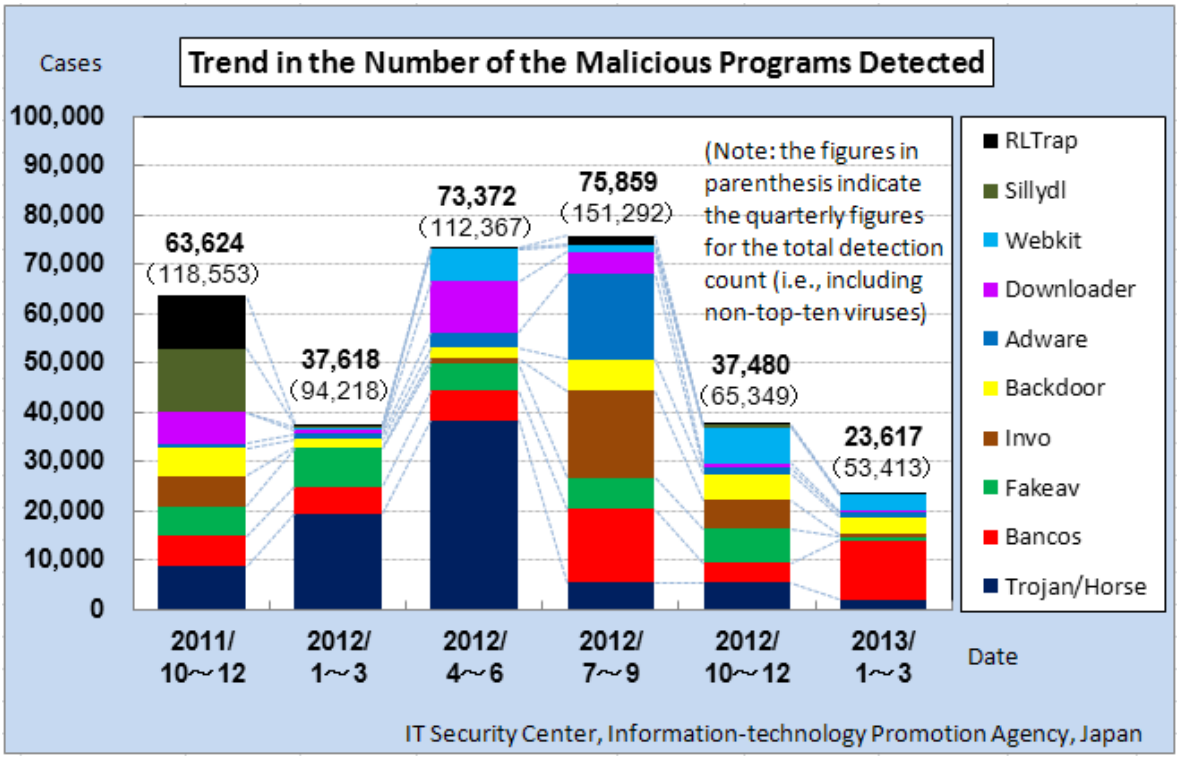

Figure 1-3: Trend in the Number of the Malicious Programs Detected

(6) Viruses Reported in the first quarter of 2013

76 types of viruses were reported in the first quarter of 2013, with 1,589 reports related to Windows/DOS, 197 reports to script virus and macro virus, and 17 reports to PDA virus.

Note: Repot count includes that of the virus's subspecies. The symbol * indicates newly-discovered viruses in the first quarter of 2013.

i) Windows/DOS virus	Report count
W32/Netsky	440
W32/Mydoom	367
W32/Autorun	129
W32/Mytob	125
W32/Bagle	114
W32/Downad	106
W32/Klez	58
W32/Mumu	42
W32/Gammima	23
W32/Virut	17
W32/Funlove	15
W32/IRCbot	12
W32/Sality	11
Perl/Santy	9
W32/Antinny	9
W32/Lovgate	9
W32/Palevo	9
Wscript/Kakworm	9
W32/Fujacks	8
W32/Fakerecy	5
W32/Looked	5
W32/Badtrans	4
W32/Parite	4
W32/Bacterra	3
W32/Harakit	3
W32/Myparty	3
W32/Ramnit	3
W32/Stration	3
W32/Stuxnet	3
W32/Witty (※)	3
W32/Zafi	3
Stoned	2
W32/Allaple	2
W32/Imaut	2
W32/Mywife	2
W32/Sober	2
W32/Sobig	2
W32/Waledac	2
Diskkiller	1
W32/Aliz	1
W32/Brid	1
W32/CIH	1
W32/Chir	1
W32/Dorkbot	1
W32/Dupator	1
W32/Gaobot	1
W32/Hybris	1
W32/Lunalight	1

i) Windows/DOS virus	Report count
W32/Mabutu	1
W32/Magistr	1
W32/Nimda	1
W32/Opaserv	1
W32/Rontokbro	1
W32/Sohanad	1
W32/Traxg	1
W32/Valla	1
W32/Wapomi	1
W32/Whybo	1
W32/Xpaj (※)	1
Subtotal (59 types)	1,589

Script virus	Report count
VBS/LOVELETTER	3
VBS/SST	3
VBS/Solow	3
VBS/Freelink	2
VBS/Internal	1
VBS/Redlof	1
Subtotal (6 types)	13

Macro virus	Report count
XM/Laroux	100
XM/Mailcab	70
XF/Sic	5
XF/Helpopy	3
W97M/Relax	2
X97M/Divi	2
W97M/Melissa	1
W97M/X97M/P97M/Tristate	1
Subtotal (8 types)	184

ii)PDA	Report count
AndroidOS/Lotoor	14
AndroidOS/Fakeinst	2
AndroidOS/Rootcage	1
Subtotal (3 types)	17

iii) Macintosh	Report count
None	

iv) OSS (OpenSourceSoftware):Unix including Linux and BSD	Report count
None	

< 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

(7) Outline of the Viruses that Were Reported for the First Time to IPA in the First Quarter of 2013

(1) W32/ Witty (January 2013)

This virus infects computers by exploiting vulnerability within the security software "BlackICE" via network. After the infection, it sends copies of itself to multiple IP addresses and ports at random through a UDP port 4000.

Since this virus resides in only the memory unit, computer users can prevent its infection activity by rebooting their computer.

(2) W32/Xpaj (January 2013)

This virus spreads its infection via removable drives.

After the infection, it encrypts itself and infects files whose extension is "dll", "exe", "scr" or "sys". Furthermore, it guides Internet users to a maliciously-crafted Website.

Some of the subspecies of this virus infect the computer's HDD's master boot record. This means that the virus is activated before the operating system is up, making it harder for the computer user to clean it,

(8) Number of the Cases Reported (by Report Submitter) (Table 1-1)

	2011/ 10～12	2012/ 1～3	2012/ 4～6	2012/ 7～9	2012/ 10～12	2013/ 1～3
General corporations	2,524	2,523	2,580	2,506	2,367	1,946
	(94.4%)	(95.6%)	(97.0%)	(96.6%)	(96.4%)	(97.8%)
Individuals	0	0	0	3	4	0
	(0.0%)	(0.0%)	(0.0%)	(0.1%)	(0.2%)	(0.0%)
Educational institutions	150	117	80	86	85	43
	(5.6%)	(4.4%)	(3.0%)	(3.3%)	(3.5%)	(2.2%)
Total	2,674	2,640	2,660	2,595	2,456	1,989

(9) Number of the Cases Reported (by Route of Infection (Finding)) (Table 1-2)

	2011/ 10～12	2012/ 1～3	2012/ 4～6	2012/ 7～9	2012/ 10～12	2013/ 1～3
Emails	2,413	2,391	2,434	2,336	2,230	1,796
	(90.2%)	(90.6%)	(91.5%)	(90.0%)	(90.8%)	(90.3%)
Downloaded files(*)	29	26	14	23	29	23
	(1.1%)	(1.0%)	(0.5%)	(0.9%)	(1.2%)	(1.2%)
External media	0	1	0	2	3	2
	(0.0%)	(0.0%)	(0.0%)	(0.1%)	(0.1%)	(0.1%)
Networks	230	220	212	233	194	168
	(8.6%)	(8.3%)	(8.0%)	(9.0%)	(7.9%)	(8.4%)
Unknown/Others	2	2	0	1	0	0
	(0.1%)	(0.1%)	(0.0%)	(0.0%)	(0.0%)	(0.0%)
Total	2,674	2,640	2,660	2,595	2,456	1,989

(10) Number of the Infected PCs (Table 1-3)

	2011/ 10～12	2012/ 1～3	2012/ 4～6	2012/ 7～9	2012/ 10～12	2013/ 1～3
None	2,670	2,638	2,660	2,593	2,453	1,989
	(99.9%)	(99.9%)	(100.0%)	(99.9%)	(99.9%)	(100.0%)
1 unit	2	1	0	1	2	0
	(0.1%)	(0.0%)	(0.0%)	(0.0%)	(0.1%)	(0.0%)
2 to 4 units	0	1	0	0	1	0
	(0.0%)	(0.0%)	(0.0%)	(0.0%)	(0.0%)	(0.0%)
5 to 9 units	1	0	0	1	0	0
	(0.0%)	(0.0%)	(0.0%)	(0.0%)	(0.0%)	(0.0%)
10 to 19 units	0	0	0	0	0	0
	(0.0%)	(0.0%)	(0.0%)	(0.0%)	(0.0%)	(0.0%)
20 to 49 units	1	0	0	0	0	0
	(0.0%)	(0.0%)	(0.0%)	(0.0%)	(0.0%)	(0.0%)
50 to 9999 units	0	0	0	0	0	0
	(0.0%)	(0.0%)	(0.0%)	(0.0%)	(0.0%)	(0.0%)
1000 units or more	0	0	0	0	0	0
	(0.0%)	(0.0%)	(0.0%)	(0.0%)	(0.0%)	(0.0%)
Total	2,674	2,640	2,660	2,595	2,456	1,989

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

The number of the cases reported for unauthorized computer access in the first quarter (January to Marc) of 2013 was **27** (36 in the previous quarter (October to December of 2012)). Among them, **18** cases (14 cases in the previous quarter) were caused by **"Intrusion"**, **5** cases (12 cases in the previous quarter) by **"Spoofing"**, and **2** cases (3 cases in the previous quarter) by **"Malicious code embedded"**.

Among the 18 cases involving "Intrusion", most of them (15 cases) involved "Web defacement".

In the first quarter of 2010, so called "Gumbler"*[1] become prevalent and in the third quarter of 2012, a Website defacement thought to have been done by neighboring countries as part of their protest over the sovereignty of some islands stood out in number, which contributed the increase in the number of the cases reported. Both of them contributed to the increase in the number of the cases reported. Unlike the above-mentioned period, in this quarter, we have not seen such characteristic causes as: "prevalence of infection by a specific virus" or "detection of a critical vulnerability within the Web server". However, the number of the cases reported in this quarter was close to that of the above-mentioned period.

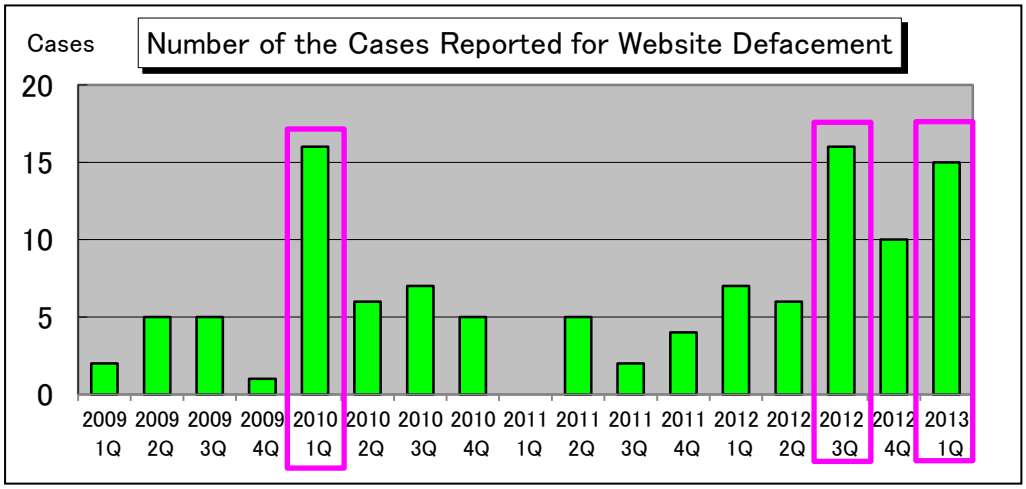

Figure 2-1: Trend in the Number of the Cases Reported for Website Defacement

As for the causes of Website defacement, "Unknown cause" accounted for **the majority** (see Figure 2-4). Among identified causes are: **brute force attack against the administrative privilege account; and vulnerabilities within CMS*[2] and server management tools being exploited.** In fact, their causes **vary**. There was also a report on Website defacement by an attacker who stole a FTP account. So, we assume that "Gumbler" (which became prevalent in the first quarter of 2010) or something of its kind is still being used.

Meanwhile, JPCERT/CC issued a security alert on defacement against the Websites where a server management tool "Parallels Plesk Panel" is used*[3] IPA also received reports on and inquiries about a maliciously-crafted Apache module embedded in a Website where "Parallels Plesk Panel" is used. It's not clear whether "Parallels Plesk Panel" is attributable, but those using this tool for their Websites are encouraged to update the tool to the latest version.

As for Website defacement, before and in the previous quarter, IPA received reports on a Website alteration whose purpose was to show protesting messages from neighboring countries, but in this quarter, no such case was reported. In this quarter, however, **"Our Website has been altered into a virus distribution site" accounted for half of the cases reported**. This suggests that besides a direct attack against Internet users, an indirect attack in which an attacker alters a legitimate Website so that visitors suffer certain damage is also becoming prevalent.

To effectively counter Website defacement as an organization, efforts from both system administrators and PC users are required: while **system administrators should implement countermeasures on the server(s) they are responsible for, PC users should also take necessary steps on their PC** so that they can protect their PC in case they visit a defaced Website.

Below are examples of effective, fundamental security measures. Make sure that each item is being implemented as planned.

Countermeasures on Servers (Countermeasures for System Administrators)

- **Perform strict control and settings of IDs and passwords**
- **Eliminate security holes (including operational workaround if no patch is applicable)**
- **Perform appropriate settings and access control of routers and firewalls**
- **Perform periodical access log checking**

Countermeasures on PCs (Countermeasures for Individual Users)

- **Keep your antivirus software up-to-date**
- **Update your OS and application software (e.g., by applying Windows Update and Office Update)**
- **Perform appropriate password settings and control (make them complex, do not tell them to others, do not use the same password for multiple purposes etc.)**
- **Make use of routers and personal firewalls**
- **Check for your wireless LAN encryption settings (When possible, use WPA2 instead of WEP)**

*1 An avenue to cause the infection and spread of a virus. It takes place as follows: "The PC of a visitor to a Website is infected with a virus through "Drive-by-Download" attack; "The virus steals his FTP account"; "By using this account, the attacker alters another Website and other PCs accessing it are also infected through "Drive-by-Download" attack"

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

*3 "A security alert on the use of an older version of 'Parallels Plesk Panel'" by JPCERT/CC
https://www.jpcert.or.jp/at/2013/at130018.html

(2) Damage Instance

(i) A large volume of communication is done by our server, causing trouble to other organizations

Instance	- We were notified by the hosting service company in use: "A large volume of inbound and outbound communication is taking place. Especially, the volume of the outbound communication is extremely large." - The originator of such outbound communication was our company's DNS server and its destination was UDP53 port, which is typically used by DNS. - Of course, such communication is not the one our company intended. - We asked the hosting service company to look into the matter, but the result of their investigation was: "unknown cause".

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

The number of the cases reported for unauthorized computer access in the first quarter (January to March) of 2013 was 27, about 75 percent over the previous quarter level. The number of the cases involving actual damages was 27, about 79 percent over the previous quarter level

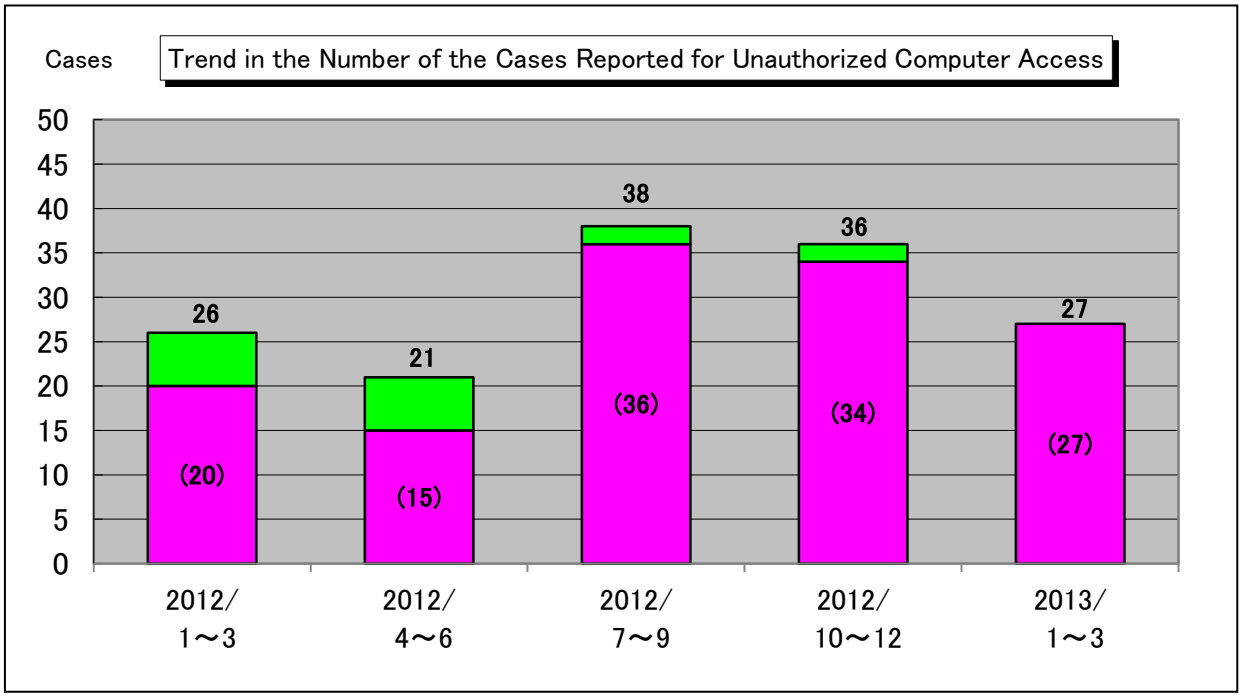

Figure 2-2: Trend in the Number of the Cases Reported for Unauthorized Computer Access

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

The number of the cases reported for unauthorized computer access in the first quarter of 2013 was 27 (36 in the previous quarter). Among them, 27 cases (34 cases in the previous quarter) involved actual damages, accounting for 100 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.

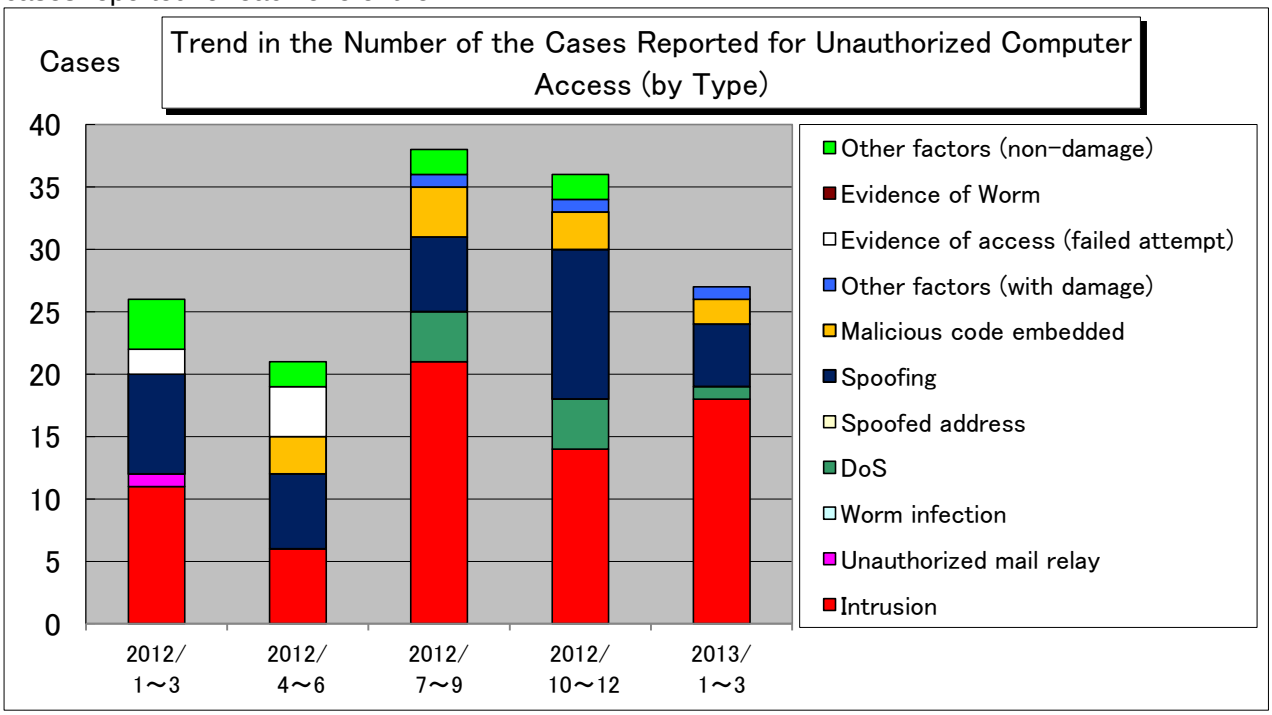

Figure 2-3: Trend in the Number of the Cases Reported for Unauthorized Computer Access (by Type)

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	11	42.3%	6	28.6%	21	55.3%	14	38.9%	18	66.7%
Unauthorized mail relay	1	3.8%	0	0.0%	0	0.0%	0	0.0%	0	0.0%
Worm infection	0	0.0%	0	0.0%	0	0.0%	0	0.0%	0	0.0%
DoS	0	0.0%	0	0.0%	4	10.5%	4	11.1%	1	3.7%
Spoofed address	0	0.0%	0	0.0%	0	0.0%	0	0.0%	0	0.0%
Spoofing	8	30.8%	6	28.6%	6	15.8%	12	33.3%	5	18.5%
Malicious code embedded	0	0.0%	3	14.3%	4	10.5%	3	8.3%	2	7.4%
Other factors (with damage)	0	0.0%	0	0.0%	1	2.6%	1	2.8%	1	3.7%
Evidence of access (failed attempt)	2	7.7%	4	19.0%	0	0.0%	0	0.0%	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)	4	15.4%	2	9.5%	2	5.3%	2	5.6%	0	0.0%
Total	**26**		**21**		**38**		**36**		**27**	

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, **5 cases were caused by "Older version used/patch not applied", 2 cases by "Poor ID & password management", and 2 cases by "Inappropriate setting"**.

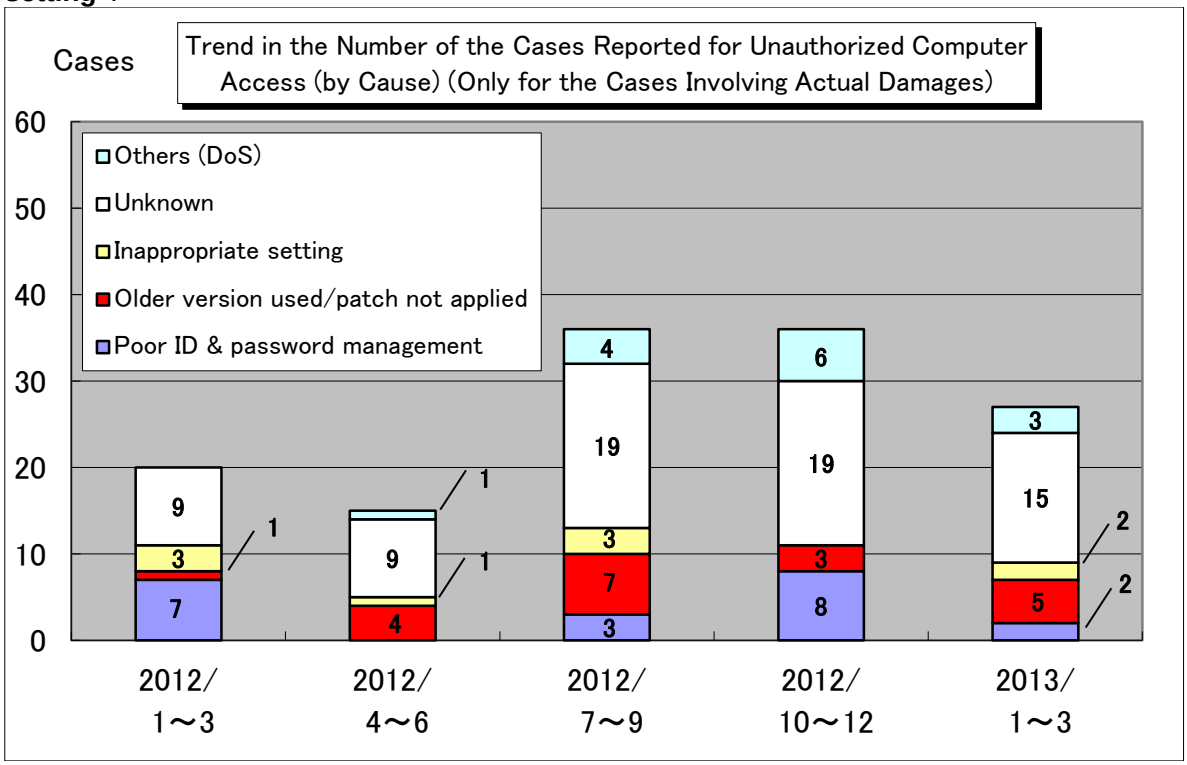

Figure 2-4: Trend in the Number of the Cases Reported for Unauthorized Computer Access (by Cause)

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

Breakdown of the report submitters is as follows:

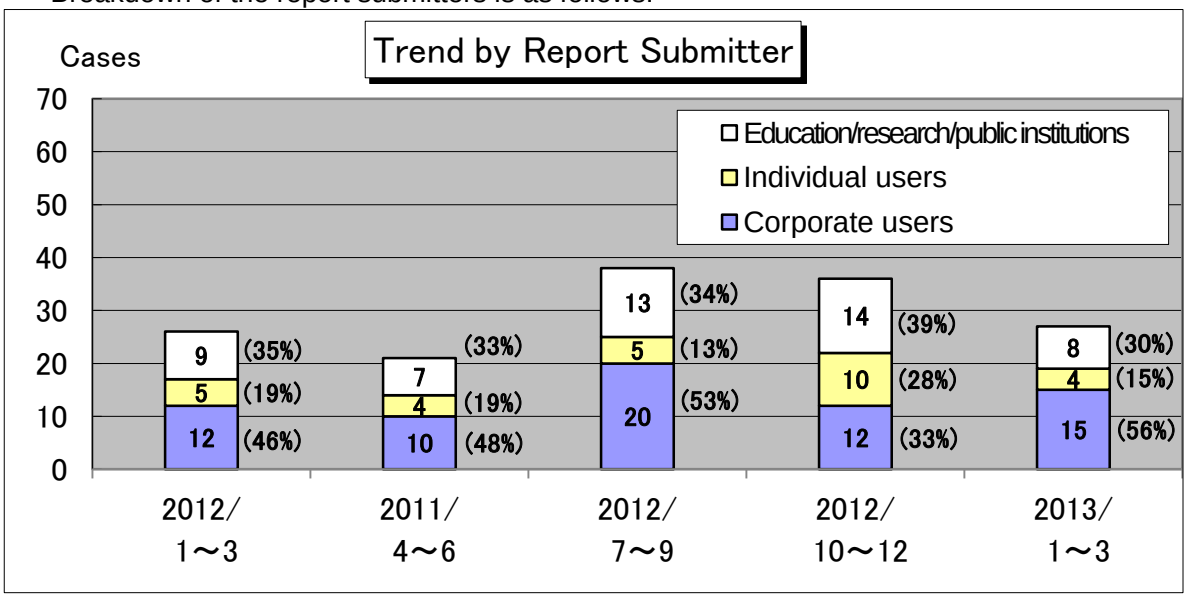

Figure 2-5: Trend in the Number of the Cases Reported for Unauthorized Computer Access (by Report Submitter)

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 first quarter (January to March) of 2013 was **3,300** (3,203 in the previous quarter (October to December 2012)), **721** of which were related to **"One-click Billing Fraud"** (659 in the previous quarter); **179** to **"Fake Security Software"** (116 in the previous quarter); **22** to **"Winny"** (51 in the previous quarter); **18** to **"A Suspicious E-Mail Sent to a Specific Organization to Collect Specific Information/Data"** (18 in the previous quarter)

The trend of the first quarter of 2013 was: "One-click Billing Fraud" showed a moderate up-and-down trend but has remained roughly flat (see Figure 3-2). Meanwhile, **the number of the cases consulted for "Fake Security Software" showed an explicit, increasing trend** (see Figure 3-3)**.** The number of the cases consulted for "Smartphone" is also on the increase, reflecting ever-increasing smartphone users

Furthermore, compared to the same period last year (the first quarter (January to March) of 2012), the number of the cases consulted in this quarter was more or less the same. But when we focused on the period between the second quarter (April to June) of 2012 and the first quarter of 2013, we could see the number **keep increasing slightly** (see Figure 3-1 and Table 3-1).

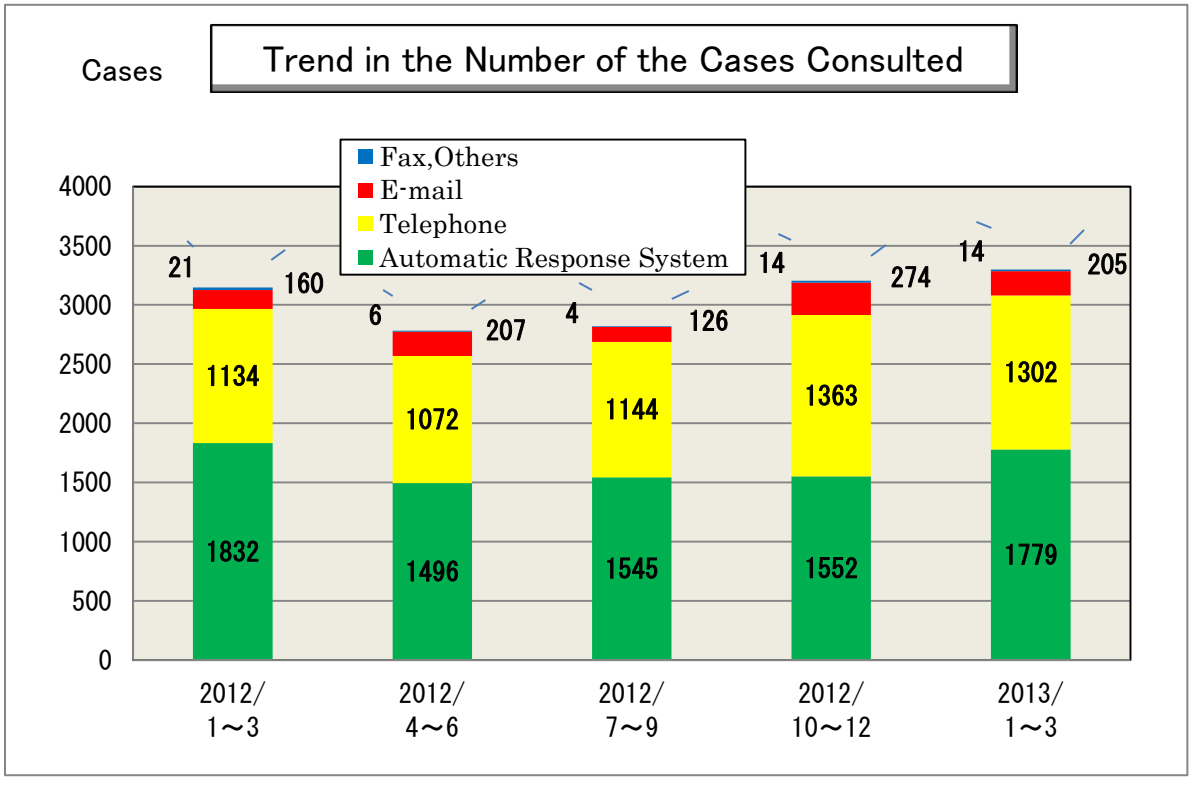

Figure 3-1: Number of the Cases Consulted for Virus and Unauthorized Computer Access

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

	2012/ 1～3		2012/ 4～6		2012/ 7～9		2012/ 10～12		2013/ 1～3	
Total	3147		2781		2819		3203		3300	
Automatic Response System	1832	(58%)	1496	(54%)	1545	(55%)	1552	(48%)	1779	(54%)
Telephone	1134	(36%)	1072	(39%)	1144	(41%)	1363	(43%)	1302	(39%)
E-mail	160	(5%)	207	(7%)	126	(4%)	274	(9%)	205	(6%)
Fax, Others	21	(1%)	6	(0%)	4	(0%)	14	(0%)	14	(0%)

(2) Consultation Instances

Major consultation instances are as follows:

（i） As a result of downloading a suspicious software, my PC began to malfunction

What was consulted (Case 1)	**I cannot access the Internet** ・ When I booted my PC, a pop-up window appeared and unknown software began to scan the PC and displayed a message: "A large number of viruses have been detected!!" ・ When I tried to access the Internet, this software displayed a warning screen, saying "You are trying to access a suspicious Website," and I could not access the Internet.
What was consulted (Case 2)	**Files were deleted and nothing could be done** ・ When I booted my PC, an unknown pop-up window appeared, and I found that most of the desktop icons, installed programs and created files had gone away. ・ I tried to perform "system restoration", which was detailed on IPA's Website, and clicked on the "Start" button and "All programs", but inside the submenu was almost empty. So nothing could be done.
What was consulted (Case 3)	**My PC went off and I was asked for money to improve the symptom** ・ Now I live in Germany. The PC in use seems to have been infected with a virus and when I booted it, a pop-up window appeared, saying "This is German police. You have accessed a suspicious Website, so pay us 100 Euro as a fine!" ・ I fell into the situation in which no further operation could be performed. ・ I tried "system restoration" by referring to IPA's Website, but despite booting my PC in safe mode, the above window appeared and I could not proceed further.

Response	We assume that you are suffering from the virus called "Fake Security Software" This type of software has a screen structure similar to legitimate security software and may seem useful in the eyes of the users. However, it issues a phony warning message to get the user to purchase a product. If you see a window that encourages such purchase, do not enter your credit card number or other personal information. Should you enter such information, consult your credit card company and the consumer affairs bureau. Just in case, consider changing your credit card number. As for the infected PC, **the most reliable way to fix it is to perform initialization**. But for those who do not want to perform initialization, IPA recommends that they implement "System restoration", with which then can get their PC back to the state before the infection. To prevent the recurrence of a problem like this in the future, be sure to keep your OS and application software and antivirus software up-to-date. <Reference> ・"Endless incidents caused by a virus issuing a fake warning" http://www.ipa.go.jp/security/txt/2012/03outline.html (in Japanese) ・"How Is Fake Security Software Installed?" - Let's learn the fundamental countermeasures and carry out Internet surfing in a secure manner - http://www.ipa.go.jp/security/txt/2013/04outline.html (in Japanese)

(3) Analysis of the Cases Consulted

As for the number of the cases consulted for **virus and unauthorized computer access**, once it showed a decreasing trend after peaking in the third quarter (July to September) of 2010 (6,667), but **in and after the second quarter (April to June) of 2012, it showed a slightly increasing trend** (See Figure 3-1 and Table 3-1). Below are possible reasons.

Figure 3-2 shows a graph for the number of the cases consulted for "One-click Billing Fraud", which takes a large share of the number of all the cases consulted. For **the number of the cases consulted for "One-click Billing Fraud"** once it showed a decreasing trend after peaking in the third quarter of 2010 (2,560), but **in and after the first quarter (January to March) of 2012, it remained roughly flat.**

Meanwhile, for the number of the cases consulted for "Fake Security Software", .it has been gradually increasing since the second quarter of 2012 (See Figure 3-2). This may have contributed to the slightly increasing trend since the second quarter of 2012.

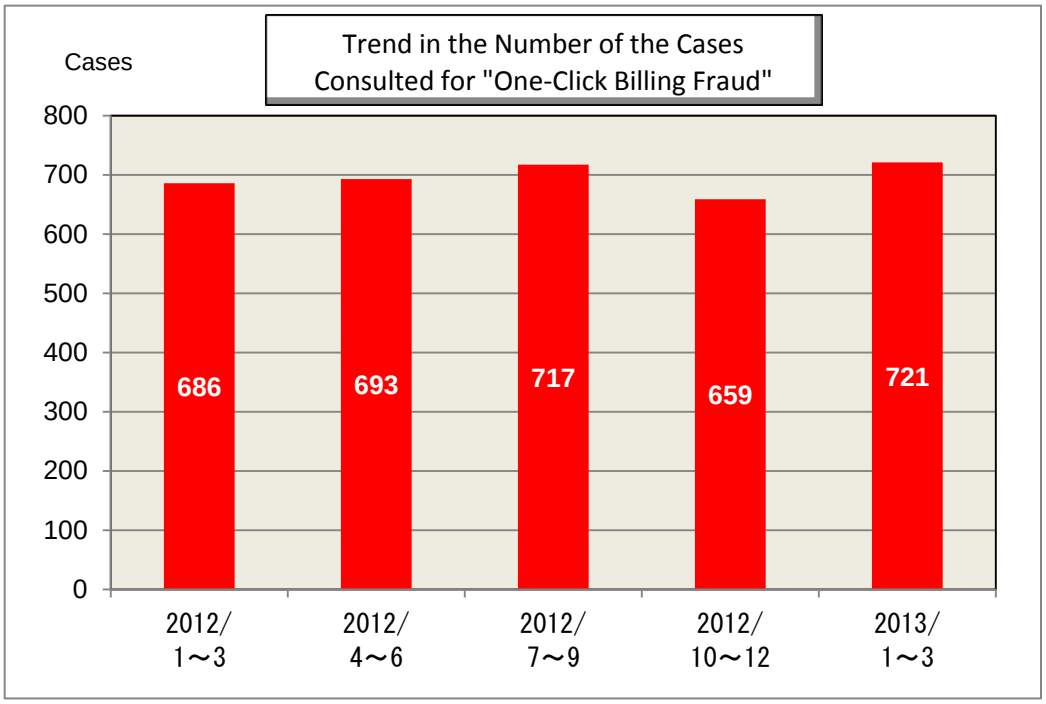

Figure 3-2: Trend in the Number of the Cases Consulted for "One-Click Billing Fraud"

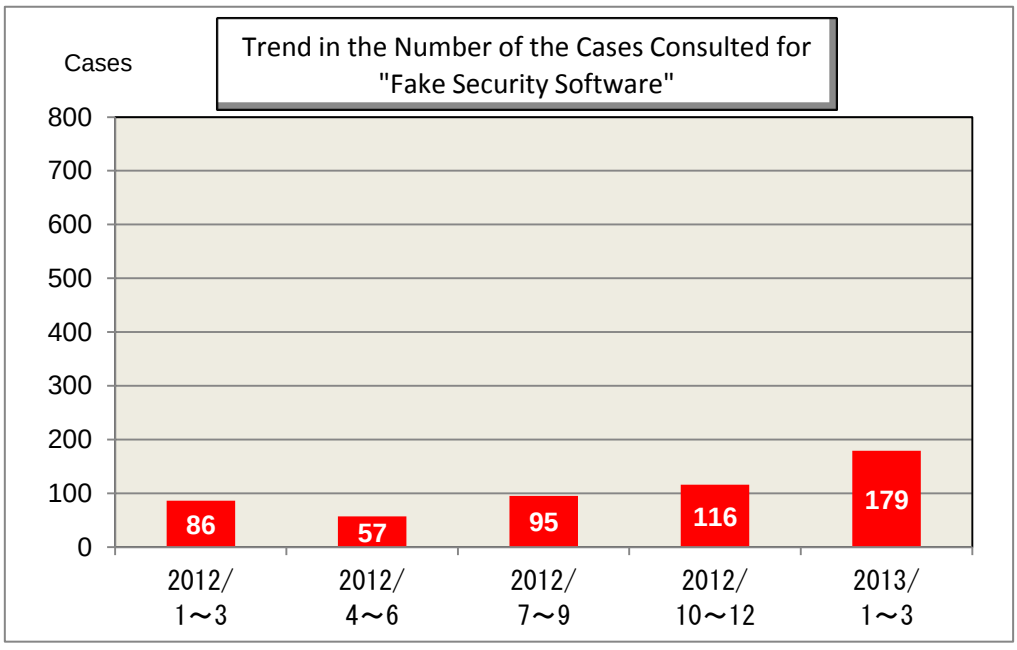

Figure 3-3: Trend in the Number of the Cases Consulted for "Fake Security Software"

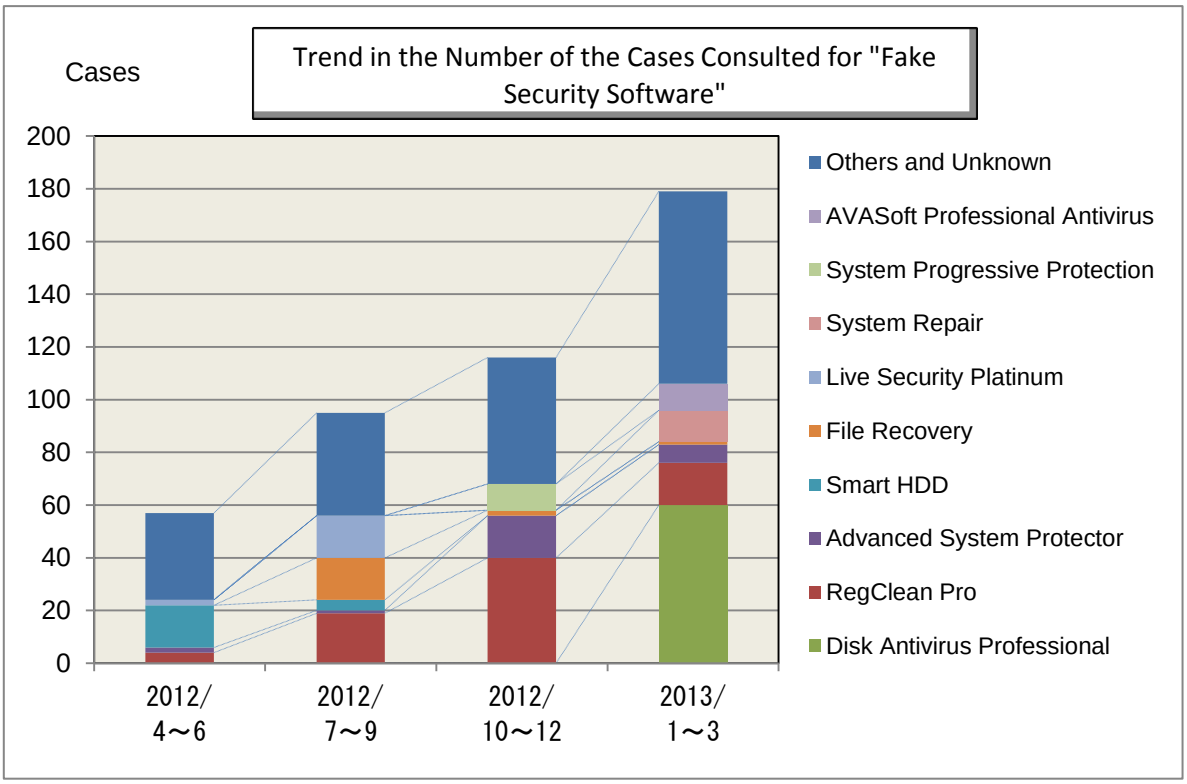

Figure 3-4: Trend in the Number of the Cases Consulted for "Fake Security Software" (in Detail)

Fake security software of recent years may impede the normal behavior of browsers or other programs so that their users cannot access the Internet, or change the attributes of an important file so that it cannot be seen or backed up. Thus they are becoming more malicious.

Figure 3-4 shows the quarterly figure for the tarried number of the cases related to fake security software, whose number of the cases consulted has been increasing since the second quarter (April to June) of 2012.

The fake security software names that have been reported to IPA between April 2012 and March 2013 vary greatly (approximately 70 types.) We can see that such a wide variety of fake security software emerged and gone away during this period.

Especially in this quarter (January to March 2013), the number of the cases consulted for "Disk Antivirus Professional" reached 60, which is an outstanding figure. Since March 2013, the number of the cases consulted for "AVASoft Professional Antivirus" , which has a similar screen structure, has been increasing. From its screen structure, we can see that this software falls into the same category as "Disk Antivirus Professional". It is expected that the number of the cases consulted for this software will increase.

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