An Experience of Monitoring University Network Security Using a Commercial Service and DIY Monitoring

Masato Masuya
Kagoshima University
1-21-35 Korimoto, Kagoshima
Kagoshima 890-0065, Japan
+81-99-285-7474
masatom@cc.kagoshima-u.ac.jp

Takashi Yamanoue
Kagoshima University
1-21-35 Korimoto, Kagoshima
Kagoshima 890-0065, Japan
+81-99-285-7187
yamanoue@cc.kagoshima-u.ac.jp

Shinichiro Kubota
Kagoshima University
1-21-35 Korimoto, Kagoshima
Kagoshima 890-0065, Japan
+81-99-285-7474
kubota@cc.kagoshima-u.ac.jp

ABSTRACT
Monitoring network security of a university is one of the most important jobs for the network managers. Without the monitoring, it is hard to keep the network safe. It is common that the security policy of a university has the term which states that monitoring network security is a mandate. However it is very hard to monitor every part of a university's network by the limited number of staff and a limited amount of time and expense. In order to cope with these problems, we bought a commercial network security monitoring service for the doorway of our campus network and we are doing Do It Yourself (DIY) monitoring with free software for the inside of the network. By the commercial monitoring service, we could reach 24 hours a day and 365 days a year monitoring at the doorway. By the DIY monitoring, we could realize the precise monitoring of inside network, which is hard to realize by the commercial monitoring, because there are Network Address Translations (NATs). If an incident was found by the combination of these monitoring, we could deal with it as fast as we can. By these efforts, there was no serious incident such as unauthorized manipulation of important web pages by crackers and leaking serious personal information by using P2P file sharing software last year. In this paper, we report the experience of our monitoring.

Categories and Subject Descriptors

General Terms
Management, Security, Verification.

Keywords
Security, policy, monitor, audit, network, IDS, fire wall

1. INTRODUCTION
A campus network is one of the most important infrastructures of a university today. Every member of a university needs the campus network, whether s/he is a student, a faculty or an officer. A campus network is similar to a city. There are good packets and bad packets in the network just like there are good people and bad people in the city. There are also packets which came from out side of the campus. A manager of the campus network is similar to a police officer in the city. S/he has to keep the network safe. The patrol of the city by the police officer is corresponding to monitoring network security by the network manager. Monitoring network security is one of the most important jobs for the network managers today. Without monitoring network security, it is hard to keep the network safe. It is common that the security policy of a university has the term which states that monitoring network security is a mandate, as same as the law of the city. However it is very hard to monitor every part of a university's network by the limited number of staff and a limited amount of time and expense. In order to cope with these problems, we bought a commercial network security monitoring service for the doorway of our campus network and we are doing Do It Yourself (DIY) monitoring with free software for the inside of the network. By the commercial monitoring service, we could reach 24 hours a day and 365 days a year monitoring at the doorway. By the DIY monitoring, we could realize the precise monitoring of the inside network, which is hard to reach by using the commercial monitoring, because there are Network Address Translations (NATs). If an incident was found by the combination of these monitoring, we could deal with it as fast as we can. By these efforts, there was no serious incident such like unauthorized manipulation of important web pages by crackers and leaking serious personal information by using P2P file sharing software last year.

The rest of this paper is organized as follows. In section 2, a summary of the network and the security policy of our university is shown. In section 3, an introduction of the commercial monitoring is described. In section 4, a way of the DIY monitoring is presented. In section 5, we evaluate our monitoring. Then in section 6, related works are shown. Finally in section 7, we summarize this paper and present some possible future works.
2. NETWORK AND SECURITY POLICY
OF OUR UNIVERSITY

Figure 1 shows a logical structure of our campus network. Our campus network consists of division networks and equipment such as routers, firewalls, Intrusion Detection Systems (IDS), NAT, DHCP (Dynamic Host Configuration Protocol) servers and others. The outside router, which is connected to the Internet directly, sends outbound packets from our campus to the Internet and receives inbound packets from the Internet. The outside IDS, which is connected to the line between the outside router and the firewall, monitors the traffic of the line. If it detects a suspicious activity, it reports the activity to network security specialists. The firewall filters out the unfavorable packets. The manager of our campus can add and delete the filtering rules easily using the web interface. The firewall also throws away e-mails with a virus. The middle router corrects the outbound packets from the division routers and sends them to the outside router. It also receives the inbound packets from the outside router and sends them to the appropriate division router. There are two kinds of division routers. One is the global address router and another is the private address router. An outbound packet from a global address network of a division is sent to the middle router by the division router (global) without any address translation. An inbound packet to the global address network of the division follows the reverse way. An outbound packet from a private address network is sent to the NAT by the division router (private). The NAT translates the packet’s source address to a global address. The NAT enhances security of the private networks because a malicious inbound packet is hard to intrude on the private network. The DHCP server provides IP address and other information to client computers in the private networks automatically. This allows the end users of the campus network easily connect their client computers. The inside IDS detects the malicious activity at the private networks and reports the activity to a manager.

In the dawn of the Internet, there were only colleagues and there was almost no malicious software at that time. However, every one is using the campus network today. There are computer viruses, spywares, phishing sites, botnets, illegal file sharing and others everywhere. In order to use the campus network peaceful and safely in such situation, there must be rules or a security policy.

Our security policy includes the following:

- The Computing and Communications Center is in charge of running, managing and maintaining the campus network. The center also has the responsibility for connecting the campus and the Internet.
- Each division has the responsibility for using the networks of the division.
- The center configures the campus network if a division requests it. In an emergency, the center can configure the network without the division,s request if the center judged that it is difficult to keep the campus network safe without the configuration.
- The center endeavors to reach 24 hours a day and 365 days a year monitoring at the doorway of our campus network.
- Using a P2P file sharing software is banned. It can be used if

![Figure 1. A Logical structure of our campus network](image-url)
the CIO allows it.

In order to connect a computer to the network of each division, the user of the computer has to complete an application which includes user’s name, user’s affiliation, the computer’s MAC address and other information. The user can use the division’s network if the manager of the division network accepts the application and the staff of the Computing and Communications Center configures the network to be able to use the computer on the network. This procedure is little bit cumbersome. We are also running the open network. Users’ PC laptops and others can be connected to the open network anytime without writing an application if the user has the account on the system from the Computing and Communications Center. In order to use the open network, the user has to follow the center’s policy. There are many access points of the open network in our campus. There are also wireless access points. In order to authenticate the user, there is the gateway with user authentication. The user of the open network is authenticated by the authentication web page which is shown to the user when s/he tries to display a web page at the first time after connecting the network. The gateway also has the function of NAT and DHCP.

3. COMMERCIAL MONITORING SERVICE

The security policy says “The center endeavors to realize the 24 hours a day and 365 days a year monitoring at the doorway of our campus network”. However, it is hard to reach this by us, Computing and Communications Center staff, only. We do not have enough time to monitor the network every day and every night. We also do not have enough money to employ a new person to do that. In order to monitor the network, there are IDSs and we have bought an IDS once. However, analyzing the output of the IDS was very hard. It produces big amount of log data. It was hard to choose which line of the data is important for us or not. We asked our university’s president to give us money for buying a commercial network security monitoring service. He gave us the money and we have started the monitoring August 2005. We had a short term test run during July 2005.

The commercial network security monitoring service does the following 24 hours a day, 365 days a year.

- Monitor our network using the outside IDS in our campus from their center.
- Analyze the output of IDS. There are network security specialists in the company and they analyze the output.
- Report to us the emergency and critical incidents when they find them.

The service also does the following.
- Write reports of our network security periodically.
- Send us news about network security.
- Maintain the IDS such as updating signatures.

When we receive an emergency incident report or a critical incident report, we tell it to the network manager of the applicable division and ask s/he to deal with the incident, or we add new filtering rule to the firewall.

In many cases, we tell the incidents to the division’s network manager of the applicable network and the incidents were cleared by the staff of the division. However, there were some cases that the destination address or the source address of the malicious packet was the translated address of our private address network or the open network. It is hard to identify the applicable host because the address is translated. The DHCP server also makes the problem difficult. We can not identify the applicable host by the IP address of the private network easily. There also can be malicious activity between hosts on our campus. The outside IDS can not detects this activity.

In order to deal with these problems, we are doing Do It Yourself (DIY) monitoring at the private network.

4. DIY MONITORING

We are identifying the IP addresses of the private networks before NAT translations, which cannot be made clear by the outside IDS. We are also detecting the port scanning on the inside of the network by virus-infected PCs and saving all log data by capturing all packets. We are doing these tasks at a mirror port in the inside of the campus network. The following equipment is used for our monitoring.

- DELL PowerEdge 850
- CPU: Pentium 4 512 2.8GHz
- Memory: 512MB
- HDD: SATA 160GB
- NIC: 1000Base-T (Broadcom BCM5721) x 2
- OS: SuSE Linux OSS 10.0

Four tools, argus, snort, tcpdump and ettercap, are used in this DIY monitoring. It is possible to choose any operating system on which these tools operate. In our experience, it takes less than one hour to install all of the operating system and these tools even if we installed them from scratch if we use the SuSE Linux OSS 10.0. In the case of hardware failure, we can hold down the interval without monitoring even if there is no cold standby hardware, because the constructing time is short.

The operating system SuSE Linux OSS 10.0 is an open source Linux which can be obtained from http://www.opensuse.org/ without expense. After the minimal installation of the SuSE Linux OSS 10.0, we installed the argus, the snort, the tcpdump and a development environment by using the administration tool YaST (Yet another Setup Tool). We downloaded and compiled ettercap NG-0.7.3 (http://ettercap.sourceforge.net/) in the next step. Finally, using YaST, we installed the libpcap, the libnet and the libtool, which are required to run the ettercap. If the ettercap already has been compiled on another PC, the installation is only installing the libpcap, the libnet and the libtool using the YaST and copying the ettercap from the PC.

4.1 Recording the traffic log with the Argus

The argus(http://www.qosient.com/argus/) is used for recording the traffic log. The argus(Audit Record Generation and Utilization System), which is developed by QoSient, LLC., is an open source
network monitoring tool. The argus consists of a tool to record traffic logs and a number of tools to analyze them. The amount of recorded data is small because it does not record all types of packets. In the case of Kagoshima University, the size of the compressed recorded data with bzip2 was about 500 Mbytes a weekday and about 200 Mbytes a holiday. It was about 10 Gbytes a month. At our university, it is also configured to record a part of the payload data of the packet in order to cope with the situation if our campus network is cracked. We only record the first 64 bytes of the each data. The total amount of the data can be reduced if we do not record the payload data.

We compress and save the log every hour by the argusarchive in the argus package. We divide the log into pieces because it takes too much time to analyze the log if the size of the log is large. The size of the each piece of the log when compressed with bzip2 is between 5 Mbytes to 50 Mbytes.

There are some tools to analyze the data. We usually use the ra command to analyze. The ra is a tool to print out the recorded log. Table 1 is an example of the output of the ra. Each line of the table shows the information about a captured packet.

In table 1, each field of the output is anonymous by using the ranonymize. The ranonymize is a tool to make each field of the time, the IP address, the source port in the argus record anonymous. It is useful in publishing papers and others.

The ra command prints all information out if it is executed without any option. The output of the ra can be controlled by its options or the same options as tcpdump. For example, in order to print out the lines about the packet whose destination port is SSH only, the command line will be like the following.

```
ra –nr argus.log – dst port 22
```

When we want to confirm the incident which is found by the outside IDS, we see the corresponding inside data. The data is extracted by the corresponding addresses or port by using the ra. The ra can read the log data file whether it is uncompressed or compressed if the format is gzip or bzip2. It is easy to analyze the past compressed log.

The analysis tool which we secondly use well is the ramon command. This tool allows us to get information on hosts whose inbound or outbound traffic are larger than others. For example, in order to know the top 10 hosts whose traffic is larger than others, the following command line is used.

```
ramon –M TopN –N 10 –nr argus.log
```

Table 2 shows the output of the command line. The time and addresses are ranonymized.

If the traffic of a host is heavy and lasts for a long time, there is a large possibility that a P2P file sharing software is used on the host or the host is an unauthorized server.

<table>
<thead>
<tr>
<th>Time</th>
<th>Source IP Address</th>
<th>Source Port</th>
<th>Dest IP Address</th>
<th>Dest Port</th>
<th>Protocol</th>
<th>Flags</th>
<th>Seq.</th>
<th>Ack.</th>
<th>Size</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/10/07 4:08:49</td>
<td>100.132.8.56549</td>
<td>56549</td>
<td>197.2.37.2.80</td>
<td>FIN</td>
<td>754</td>
<td>621</td>
<td>10</td>
<td>12</td>
<td>75</td>
<td>FIN</td>
</tr>
<tr>
<td>05/10/07 4:08:49</td>
<td>1.1.62.1.40050</td>
<td>40050</td>
<td>100.0.13.1.80</td>
<td>RST</td>
<td>1340</td>
<td>18135</td>
<td>18</td>
<td>33</td>
<td>13024</td>
<td>FIN</td>
</tr>
<tr>
<td>05/10/07 4:08:49</td>
<td>100.0.85.1.56409</td>
<td>56409</td>
<td>197.0.4.5.80</td>
<td>FIN</td>
<td>2867</td>
<td>13024</td>
<td>10</td>
<td>12</td>
<td>75</td>
<td>FIN</td>
</tr>
<tr>
<td>05/10/07 4:08:49</td>
<td>100.0.132.8.56550</td>
<td>56550</td>
<td>197.2.37.2.80</td>
<td>FIN</td>
<td>753</td>
<td>621</td>
<td>6</td>
<td>7</td>
<td>75</td>
<td>FIN</td>
</tr>
<tr>
<td>05/10/07 4:08:49</td>
<td>100.0.27.12.56337</td>
<td>56337</td>
<td>197.0.3.4.60341</td>
<td>CON</td>
<td>92</td>
<td>54</td>
<td>1</td>
<td>1</td>
<td>5</td>
<td>FIN</td>
</tr>
<tr>
<td>05/10/07 4:08:49</td>
<td>100.0.11.15.56595</td>
<td>56595</td>
<td>197.0.33.4.80</td>
<td>FIN</td>
<td>1937</td>
<td>76538</td>
<td>29</td>
<td>56</td>
<td>75</td>
<td>FIN</td>
</tr>
<tr>
<td>05/10/07 4:08:49</td>
<td>100.0.119.1.46783</td>
<td>46783</td>
<td>100.0.50.4.80</td>
<td>FIN</td>
<td>600</td>
<td>771</td>
<td>4</td>
<td>5</td>
<td>75</td>
<td>FIN</td>
</tr>
<tr>
<td>05/10/07 4:08:49</td>
<td>100.0.132.8.56551</td>
<td>56551</td>
<td>197.2.37.2.80</td>
<td>FIN</td>
<td>750</td>
<td>620</td>
<td>6</td>
<td>7</td>
<td>75</td>
<td>FIN</td>
</tr>
<tr>
<td>05/10/07 4:08:49</td>
<td>100.1.52.1.59998</td>
<td>59998</td>
<td>197.0.70.2.80</td>
<td>FIN</td>
<td>1468</td>
<td>1127</td>
<td>5</td>
<td>4</td>
<td>1468</td>
<td>FIN</td>
</tr>
<tr>
<td>05/10/07 4:08:49</td>
<td>100.0.27.4.57374</td>
<td>57374</td>
<td>197.0.53.1.80</td>
<td>FIN</td>
<td>646</td>
<td>700</td>
<td>5</td>
<td>4</td>
<td>646</td>
<td>FIN</td>
</tr>
<tr>
<td>05/10/07 4:08:50</td>
<td>100.0.132.8.56552</td>
<td>56552</td>
<td>197.2.37.2.80</td>
<td>FIN</td>
<td>755</td>
<td>617</td>
<td>6</td>
<td>7</td>
<td>755</td>
<td>FIN</td>
</tr>
<tr>
<td>05/10/07 4:08:50</td>
<td>100.0.43.7.56770</td>
<td>56770</td>
<td>197.0.20.2.80</td>
<td>FIN</td>
<td>950</td>
<td>16999</td>
<td>11</td>
<td>16</td>
<td>950</td>
<td>FIN</td>
</tr>
<tr>
<td>05/10/07 4:08:50</td>
<td>100.0.7.8.70704</td>
<td>70704</td>
<td>197.0.2.3.80</td>
<td>FIN</td>
<td>1459</td>
<td>643</td>
<td>5</td>
<td>4</td>
<td>1459</td>
<td>FIN</td>
</tr>
<tr>
<td>05/10/07 4:08:50</td>
<td>100.0.119.1.46791</td>
<td>46791</td>
<td>100.0.50.4.80</td>
<td>FIN</td>
<td>592</td>
<td>748</td>
<td>4</td>
<td>5</td>
<td>592</td>
<td>FIN</td>
</tr>
<tr>
<td>05/10/07 4:08:50</td>
<td>100.0.27.4.57376</td>
<td>57376</td>
<td>197.0.167.1.80</td>
<td>FIN</td>
<td>679</td>
<td>547</td>
<td>5</td>
<td>4</td>
<td>679</td>
<td>FIN</td>
</tr>
<tr>
<td>05/10/07 4:08:50</td>
<td>100.0.108.1.57882</td>
<td>57882</td>
<td>197.2.14.2.554</td>
<td>CON</td>
<td>6366</td>
<td>260379</td>
<td>105</td>
<td>214</td>
<td>6366</td>
<td>CON</td>
</tr>
<tr>
<td>05/10/07 4:08:50</td>
<td>100.0.119.1.46793</td>
<td>46793</td>
<td>100.0.50.4.80</td>
<td>FIN</td>
<td>600</td>
<td>771</td>
<td>4</td>
<td>5</td>
<td>600</td>
<td>FIN</td>
</tr>
<tr>
<td>05/10/07 4:08:50</td>
<td>100.0.113.6.56324</td>
<td>56324</td>
<td>197.0.23.28.57154</td>
<td>CON</td>
<td>226</td>
<td>124</td>
<td>4</td>
<td>2</td>
<td>226</td>
<td>CON</td>
</tr>
<tr>
<td>05/10/07 4:08:50</td>
<td>100.0.132.8.56553</td>
<td>56553</td>
<td>197.2.37.2.80</td>
<td>CON</td>
<td>749</td>
<td>620</td>
<td>6</td>
<td>7</td>
<td>749</td>
<td>CON</td>
</tr>
<tr>
<td>05/10/07 4:08:50</td>
<td>100.0.11.15.56596</td>
<td>56596</td>
<td>197.0.14.10.80</td>
<td>RST</td>
<td>574</td>
<td>58</td>
<td>4</td>
<td>1</td>
<td>574</td>
<td>RST</td>
</tr>
<tr>
<td>05/10/07 4:08:50</td>
<td>100.0.11.15.56597</td>
<td>56597</td>
<td>197.0.14.2.80</td>
<td>FIN</td>
<td>62</td>
<td>232</td>
<td>1</td>
<td>4</td>
<td>62</td>
<td>FIN</td>
</tr>
<tr>
<td>05/10/07 4:08:50</td>
<td>100.204.1.56641</td>
<td>56641</td>
<td>197.1.121.3.80</td>
<td>CON</td>
<td>675</td>
<td>279</td>
<td>4</td>
<td>2</td>
<td>675</td>
<td>CON</td>
</tr>
</tbody>
</table>
For the doubtful host, we analyze the traffic with the ra and confirm whether it is suspicious traffic or not. The ra hosts command is a useful tool for confirming whether the P2P file sharing software is used or not. This tool is used to print out the hosts list. For example, the hosts, which are only communicating with the host 100.0.109.3, are printed out by the following command line.

```
rahosts –nr argus.log – host 100.0.109.3
```

### 4.2 Detection with the snort

The outside IDS is used for intrusion detection. The inside IDS is mainly used for detecting the use of P2P file sharing software and the port scanning caused by the virus infected host which scan the ports of Windows file sharing. For the P2P file sharing software, we use signatures provided from [http://www.bleedingsnort.com/](http://www.bleedingsnort.com/), with the default signature which is included in the snort package. We only record the detected log by the command line “snort –A fast –N” because the log data are record by the argus.

### 4.3 Real time monitoring

For confirming both the running viruses and P2P file sharing software, we use mostly ettercap and tcpdump. The ettercap enables us to do real time confirmation of the monitoring data in the console windows. After logging in the inside IDS, we can start it by the command line such like the following.

```
ettercap –i eth0 –C
```

It is possible to monitor the particular port only. For example, in order to monitor the TCP80, we execute the following command line.

```
ettercap –i eth0 –C //80.
```

### 5. EVALUATION

Figure 2 shows the number of incidents which are reported to us by the commercial security monitor service from July 2005 to April 2006. The scale at left vertical axis shows the number of informational and warning incidents. The scale at right vertical axis shows the number of critical incidents. July 21-31 was the term of the test run of the service.

Informational incidents are network activities such as a horizontal scan. It can be malicious activity or happen by a normal usage of the network. Warning incidents are malicious activities such as a port scan from outside. If it seems that someone in the outside found out the security hole in the inside, it is a critical incident. An emergency incident is the incident such as hosts in the inside doing a DDOS attack.

There was no emergency incident from the start of the service until now as of May 2006.

There were twelve critical incidents during July 21-31. Seven of them were botnet activities which use the IRC. We closed the IRC port of the outbound packet at the firewall. Recently, there were VNC scanning around the world. The monitoring service tells us that one of our hosts was compromised. So we closed the VNC port of the inbound packet at the fire wall.

<table>
<thead>
<tr>
<th>StartTime</th>
<th>Addr</th>
<th>InPkt</th>
<th>OutPkt</th>
<th>InBytes</th>
<th>OutBytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>92/12/17 18:11:10</td>
<td>100.0.109.3</td>
<td>10</td>
<td>1412506</td>
<td>1585</td>
<td>285866399</td>
</tr>
<tr>
<td>92/12/17 18:11:10</td>
<td>100.0.180.2</td>
<td>1412472</td>
<td>2</td>
<td>285856404</td>
<td>180</td>
</tr>
<tr>
<td>92/12/17 18:10:23</td>
<td>100.0.22.1</td>
<td>344996</td>
<td>255709</td>
<td>330205889</td>
<td>56096096</td>
</tr>
<tr>
<td>92/12/17 18:11:03</td>
<td>100.0.226.5</td>
<td>207719</td>
<td>104849</td>
<td>2951056645</td>
<td>6009744</td>
</tr>
<tr>
<td>92/12/17 18:10:19</td>
<td>100.0.6.2</td>
<td>173980</td>
<td>137312</td>
<td>153268511</td>
<td>11088610</td>
</tr>
<tr>
<td>92/12/17 18:10:25</td>
<td>100.0.66.2</td>
<td>153522</td>
<td>131473</td>
<td>119039634</td>
<td>140703717</td>
</tr>
<tr>
<td>92/12/17 18:10:44</td>
<td>100.0.154.3</td>
<td>281549</td>
<td>73</td>
<td>129133500</td>
<td>12136</td>
</tr>
<tr>
<td>92/12/17 18:10:44</td>
<td>100.0.251.1</td>
<td>0</td>
<td>281551</td>
<td>0</td>
<td>129133856</td>
</tr>
<tr>
<td>92/12/17 18:11:37</td>
<td>100.1.49.3</td>
<td>178694</td>
<td>58911</td>
<td>246874565</td>
<td>3494347</td>
</tr>
<tr>
<td>92/12/17 18:23:55</td>
<td>197.1.34.4</td>
<td>76070</td>
<td>150923</td>
<td>4306076</td>
<td>214723227</td>
</tr>
</tbody>
</table>

Table 2. An output of the ramon command

![Figure 2. Security incidents of our university reported by the commercial service.](image-url)
less than 9960 times. This host was scanned much more in fact. The SSH brute force attack was not detected by the commercial monitoring service.

There was a host that had a weak password. The host was compromised at that time. We have found the host and coped with this as fast as we could. A simple and effective way against the SSH brute force attack is to use another port except TCP port 22. We have closed the TCP port 22 at 12:00 on February 2nd, 2006. Though the TCP port 22 is scanned even now, there has been no compromised host since closing it. We have informed the network managers of all division of the attack and the fact that one host has been compromised before closing the port. Consequently, it was relatively easy to agree with the managers about closing the TCP port 22.

We also found eleven P2P file sharing software activities from April to May 2006 by using the DIY monitoring. They were six BitTorrent and five LimeWire activities. The BitTorrent has been generally used for distributing large volume open source software, such as Linux distributions. However, students were downloading and/or uploading copyrighted music files. We reported the use of P2P file sharing software to the faculty staff so that they can counsel the students to avoid doing illegal activity.

We found many incidents by these efforts. Most of them were dealt with immediately after the find. There was no serious incident such as unauthorized manipulation of important web pages of our university until May 2006. There was no leaking of serious personal information by using P2P file sharing software. We think that it is because we dealt with the malicious activity, in co-operative with the manager of applicable division network, as fast as we can before the activity becomes serious.

6. RELATED WORKS
In the RFC1359[1], “Monitoring of the network” is an operation service of the network of an institution. Someone in the institution should do the monitoring. When the RFC was made, monitoring was mainly used for detecting the mechanical fault of the network and getting the information for improving the network. However, monitoring is important for security today.

Running a PDCA cycle, which includes making a security policy, is common work for the network managers of universities today[4]. In order to run the PDCA cycle, we have to get the cost for it. We show a way to get the cost for campus network security and a way to realize a low cost security monitoring.

There are many arguments against monitoring P2P file sharing software usage[2][3]. Monitoring the software usage can be violation of human rights and academic freedom. However, there were many serious private information leaks by using a P2P file sharing software in Japan recently[7][8]. There were also governmental security information leaks. Japanese government asked all Japanese to do not use the software March 2006[6]. In Japan, monitoring the P2P file sharing software usage is a means to keep our privacy.

Madigan and others estimated the cost of non-compliance[8], the cost of using the commercial security monitoring service and others for network security including anti-virus software on our campus is much less than the cost of their estimation.

7. CONCLUSIONS
We succeeded to prevent serious security incidents by combining the commercial security monitoring service and the DIY monitoring last year. In order to continue the commercial service, we must keep the cost for it. In order to continue the DIY monitoring we must keep our time and cost for it. We can reduce the burden of network managing a little bit by these efforts. However it is still heavy for us. We would like to reduce our burden much more.

8. ACKNOWLEDGMENTS
We thank network managers and users of all divisions of Kagoshima University. Without their cooperation and efforts, we could not keep our network safe and comfortable.

9. REFERENCES