Computer Security at KEK

Shigeo Yashiro[1]
Computing Research Center (CRC), KEK

1. Introduction

At KEK, Linux and UNIX are used as server hosts, while Windows and Macintosh are used mainly as client hosts. The Internet is indispensable for researchers to communicate with collaborators all over the world by using E-mail, to exchange information and data by using Web, and to execute remote programs.

As the Internet became a commodity, computer and network crimes have been increasing. Table-1 is a summary of security incidents from October 2001 to March 2002 reported by Information-technology Promotion Agency in Japan (IPA/ISEC). It shows that scanning and intrusion reached up to 75%, and E-mail related incidents of over 20%. Also, at KEK, the server hosts suffer port scanning, Denial of Service (DoS) attacks, and attacks to server programs. Very many SPAM E-mails and E-mails with computer virus are received. Figure-1 shows the security incidents from October 2002 to December 2003 at KEK.

Table 1 Major Security incidents in Japan (IPA/ISEC Apr. 2002)

Intrusion	17%	Linux, UNIX, Windows
Scanning	57%	
Worm	8%	Windows, Linux
Fake e-mail address	8%	
SPAM	2%	
E-mail relay	4%	Linux, Windows
Denial of Service (DoS) attack	1%	
others	4%	

It is important to guard our hosts and network against unauthorized access in order to properly maintain our research activity[1]. The difficulty is that the computers connected to the Internet can't be perfectly secure. What we can do is to keep them relatively secure. It would cost much time and money to make them more secure. We need to make some scheme to reduce security threats while balancing the cost for prevention against one that might be required when the system is cracked.

We must pay attention that we are not only victims of unauthorized access, but also that we might be regarded as being accomplices of computer crime if we leave unauthorized access free. The host might be used by a SPAM sender, a relay station for attacking, a proxy for http, a storage for improper copying, and so on.

2. Computer security incidents at KEK

2.1. Linux/UNIX server hosts

At KEK, three hosts were intruded through the SSH vulnerability from Dec. 2001 until March 2002. Eight hosts were attacked using SucKIT rootkit in April 2003. The sever programs, such as sendmail, apache, named, telnetd, ftpd, font server and smbd, were attacked and exploited from 1998 to 2003.

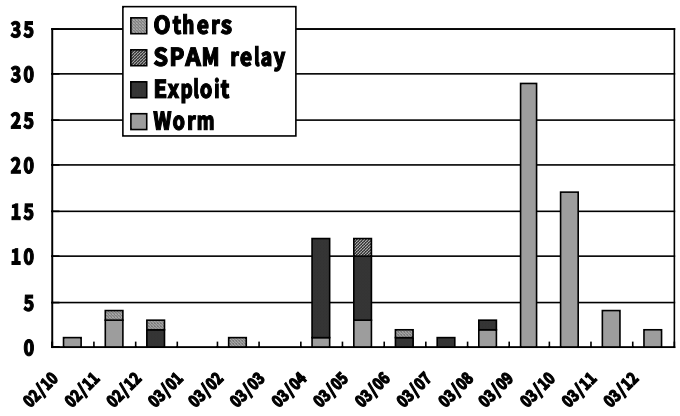

Figure 1. Recent security incidents at KEK

[1] Shigeo.Yashiro@kek.jp, http://research.kek.jp/people/yashiro/

In some cases, a network monitoring tool was installed to snatch user passwords. In other cases, the passwords in the /etc/passwd file were decoded by the cracking program. With a cracked user account, the cracker could login and attack a security hole of a program. Using this method, three hosts were cracked in 2001 and 2002.

Alerts on the security vulnerability are provided by security organizations, such as CERT/CC[2] and JPCERT/CC[3], and security companies. To minimize the risks of unauthorized access, it is important to update the software as soon as possible. Table-2 shows the Linux security hole warnings issued by KEK Linux-support[4].

Table 2 Linux security hole warnings issued by KEK Linux-support

2002	May	sudo, mozilla
	June	kernel, apach, openssh
	Aug	glibc
	Sep	slapper worm via OpenSSL
2003	Mar	sendmail
	Apr	sendmail
	May	kernel
	Jun	Samba
	Aug	wu-ftpd
	Sep	sendmail, openssh
	Oct	KDE
	Nov	XFree86
	Dec	kernel

2.2. Windows desktop PC

Computer viruses and worms[5] are major security incidents for Windows. Most of the worms are received in E-mail attachments and are activated when a file is opened with an application program, such as Microsoft Word. The worm reproduces E-mails and sends them to addresses obtained from the address list saved in the desktop computer. Table-3 gives the alerts from F-secure Co. Every month several viruses are found.

The worms found at KEK since August 2001 are listed in Table-4. Blaster and Welchi in 2003 are network worms, by which many hosts were tainted. Others are E-mail worms.

Table 3 Virus alerts from F-secure Co.

	E-mail worm	Other worm
2003 Mar.	Ganda, Lovgate	Deloder (Network worm)
May	Kickin, Fizzer, Lovgate, Palyh, Holar	
June	Sobig.C, Bugbear, Sobig.E	
Aug.	Mimail, Sobig.F	Blaster(Lovsan), Welchi (Network worm)
Sep.	Swen (Email, IRC, shares and P2P)	
Oct.	Flea, Sober	
Nov.	Mimail	
Dec.	Sober.C (German email worm)	Scold (Outlook worm)
2004 Jan.	Xombe, Dumaru, Mydoom (Email and Kazaa worm)	
Feb.	Doomjuice, Bagle[-E], Netsky.C, Mydoom.F	
Mar.	Bagle.[F-U], Netsky.[D-Q], Sober.D, Witty	

[2] http://www.cert.org/

[3] http://www.jpcert.or.jp/english/index.html

[4] http://ccwww.kek.jp/kek/root/linux-support/ (in Japanese)

[5] A virus is a program that modifies other programs, while a worm is a kind of virus that propagates from a computer to another computer.

Table 4 Computer worms found at KEK

2001	Aug.	CodeRed
2002	Jan.	MyParty
	Apr.	Nimda
	Apr.	CodeRed
	Jul.	Frethem.J@mm
	Sep.-Oct.	Nimda
2003	Aug.-Nov.	Blaster, Welchi (Network worm)
2004	Mar.-Apr.	Bagle, Netsky

Vulnerability attacks have a cycle: a vulnerability is found, an update program is developed, a security note and the program are released, the program is disassembled by crackers, a new worm is created, and it is distributed. This cycle is becoming very short; for example, the Blaster worm was detected about only a month after the security patch was released, while the Nimda worm was detected about one year after the security patch was released.

At KEK, several months ago, it was after an anti-virus database was developed that a new virus was detected. During these months, a new virus was received as soon as it was distributed, and before the database was developed. The chance of infection increased.

Other security incidents than viruses at KEK are listed in table-5. Windows users need to pay attention to information on the vulnerability provided by Microsoft[6], or by the security companies.

Table 5 Recent attacks to Windows at KEK

Feb. 2002	MS IE buffer overflow
July 2003	MS HTML converter buffer overflow
Jan. 2003	MS SQL slammer worm

2.3. Security incidents with E-mail at KEK

There are three major problems with using E-mail: receiving viruses in E-mail attachments, receiving SPAM mail from various sites, and SPAM mail distributed with fake KEK E-mail addresses.

Viruses arrive from various sites, which reproduce virus mail, or attack other hosts. Viruses detected by the KEK E-mail system *PostKEK* are shown in Figure-2. Most of the viruses in August and September 2003 were Sobig.F, those in January 2004 are Mydoom, and those in March 2004 were Netsky and Bagle.

3. Activity for computer security

3.1. Working group

Security Working Group(WG) was organized in 1998 to examine security incidents. The group consists of CRC staff members as well as representatives of users. In April 2003, the group was reorganized to the Information Security Management Group. The missions of the group are as follows.

(a) To analyze security incidents.
(b) To establish a security policy and an action program.
(c) To provide security information to KEK staff.

The group established a security policy in 1998[2]. According to the group's decision, a network monitoring system was employed in 1998. A security audit of E-mail servers was executed in 2001. Security Task Force was organized in CRC to make dispositions for introducing a firewall system in 2001[3]. A new KEK Information Security Policy was

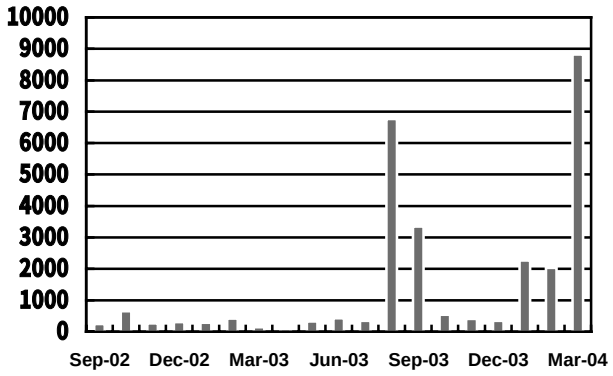

Figure 2. E-mail with virus detected by PostKEK

[6] http://www.microsoft.com/security/

established and a firewall system was employed in 2003.

The security information and alerts are delivered to users by E-mail. Two mailing lists, for computer users and for system administrators, are maintained. A web page *KEK Computer Security*[7] provides the security information and security patches. The web page is accessible only from the inside of KEK. Seminars on security, Linux management, Windows Update, and so on are held since 1999.

3.2. Solutions to improve security

The WG established security policy, guidelines, and action program to prevent attacks and intrusions. The solutions are, network base solution, host base or application base solution, and user base solution.
The solutions for Linux host and Windows host are explained separately in this paper. The description of host base solutions doesn't distinguish servers from client desktop hosts because major parts are the same between them.

3.3. Network base solutions

Before 1998, most of all the computers had global IP address and accessible from all over the world. As the Internet became popular, attacks and unauthorized access increased at KEK.
We reviewed whether all hosts need to be accessible from outside of KEK. The result showed that because many hosts are for client use, they need to access outside of KEK, but need not to be accessed from outside.

The WG made a decision to classify the hosts into *incoming*, *outgoing*, and *KEK local* classes. The *incoming* class is accessible from outside and can access the Internet . The *outgoing* class can access the Internet, but can not be accessed from it. The *KEK local* class is for Intranet use. This restriction reduces the number of accessible hosts from outside of KEK. Still, there exists a problem. If an incoming host is cracked, it attacks the outgoing hosts.

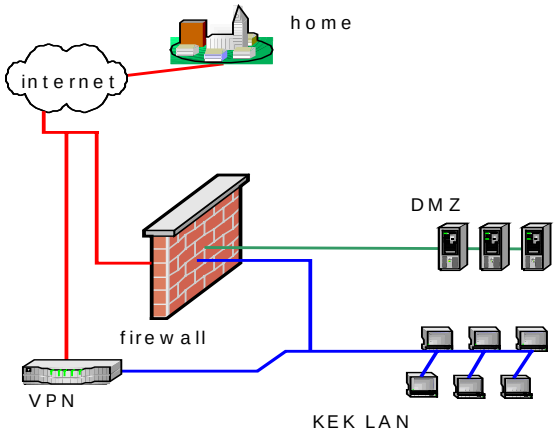

Figure 3 Outline of KEK network

An Intrusion Detection System(IDS) was employed to monitor the packets in June 1998.
A firewall system has been working since September 2003(Fig.3). The *incoming* hosts were moved to the DMZ area when the firewall was installed. The *outgoing* class was separated from the *incoming* class to make it more secure. A MAC address certification system has also been working since August 2003.

As security improves, it became harder to access server systems, such as the IMAP server, KEK local web pages and SSH servers, from outside of KEK. The VPN is employed as a solution.

3.4. Solutions for E-mail system

Security requirements from users with an E-mail system are to block viruses in attachments, to block SPAM mail, and to prevent fake KEK E-mail addresses.

To block viruses and worms, anti-virus software was employed in PostKEK in August 2002. The software is working very well. When it detects viruses, it inserts a warning into the E-mail subject. But it's not almighty. New viruses which appear one after another will not be detected. There are E-mail servers operated by research groups, some of which are without anti-virus software. To avoid infection in all cases, the most secure solution is to verify the truth of the E-mail before opening attachments. It is important to verify the sender name, to verify the history in mail headers, and to verify that the attachment is the requested one. If it is doubted in any degree, it should not

[7] http://ccwww.kek.jp/cn-security/index-e.html, access allowed only to the clients inside of KEK.

be opened.

Filtering SPAM mail on PostKEK is difficult. SPAM sites are frequently changing, and a SPAM site for a user may not be the one for another user. The solution to this problem is under investigation.

There is no idea to prevent fake KEK E-mail addresses used in SPAM mail. It is easy to fake an E-mail address, and once it is dispatched, no mail software can check it. One just notices that his/her E-mail address is faked only when he/she receives returning error mail or receives a claim to a SPAM mail. In many cases, claim mails are created automatically and the sender address is a mail administrator. One does not need to reply to this type mail. In some cases, the receiver writes a claim manually, with anger and with little knowledge of the E-mail system. In this case, one needs to apologize and explain that it's a fake.

Table 6 Samples for using the APT in RedHat Linux9 at KEK

```
configuration file /etc/apt/source.list
    rpm http://reflx1.kek.jp apt/9 os updates
    rpm http://apt.freshrpms.net redhat/9/i386 freshrpms
    #rpm-src http://apt.freshrpms.net redhat/9/en/i386 ....
update of packages
    # apt-get update
    # apt-get upgrade
```

3.5. Host base solutions for Linux

The security guideline at KEK requires computer owners to keep all of their computers on a secure network, including desktop PCs as well as server hosts.

It is mandatory to apply the newest security patches. They are issued frequently, as shown in table-2. A tool, *APT*[8], for Debian and RedHat Linux is helpful. It detects, downloads, and installs update packages. Table-6 is a sample of using the APT, a configuration file and APT commands for RedHat Linux9 to access the APT server at KEK.

To minimize vulnerabilities, the following implementations are required:

(a) To check the server services and close unnecessary ones.

(b) Access control to the service ports with *iptables*[4] and *tcpwrappers*

Table-7 is a sample of checking the running services, and of inactivating the running *sendmail* service.

Table-8 is a sample of the /etc/sysconfig/iptables file based on the iptables file in Red Hat Linux 9. (1) is the changing default value for INPUT to a secure side, DROP. From the next line, the necessary ports are opened one by one. (2) is to accept the ICMP packets for ping. (3)-(6) are for connection with the name server (suppose to be 130.87.56.2). (7) is to accept the udp123 from the NTP server (suppose to be 172.30.32.102). This line is needless in the RedHat 9 Linux, since it is added automatically at the startup time of the NTPD. (8) is to accept the SSH connection from everywhere, while (9) is to accept only from inside of KEK. It might be better for maintenance to limit hosts with TCPWRAPPERS rather than to limit them here. (10) and (11) are for the E-mail service. Some sendmail requires tcp113 of (12). (13) is to use a printer (suppose to be 130.87.32.65). (14) is for the Web service. (15) and (16) are for the SMB service; this sample allows access from 130.87.57.44. (17)-(20) are for the NFS service; this sample allows access from 130.87.57.44.

The log facility is useful for debugging. The target LOG outputs the log message into the /var/log/messages file. A sample is as follows:

```
-A INPUT -s 130.87.56.2 -j LOG
```

Table 7 Samples for checking running services

```
Check the services
    # /sbin/chkconfig –list
Stop/start a running service
    # /sbin/chkconfig sendmail off
    # /sbin/chkconfig sendmail on
To activate/inactivate at boot time
    # /sbin/service sendmail stop
    # /sbin/service sendmail start
```

[8] http://freshrpms.net/apt/

Table 8 A sample of the iptables configuration

```
*filter
:INPUT DROP [0:0]                                                                          (1)
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Lokkit-0-50-INPUT - [0:0]
-A INPUT -j RH-Lokkit-0-50-INPUT
-A FORWARD -j RH-Lokkit-0-50-INPUT
-A RH-Lokkit-0-50-INPUT -i lo -j ACCEPT
-A RH-Lokkit-0-50-INPUT -p icmp -j ACCEPT                                                  (2)
-A RH-Lokkit-0-50-INPUT -p tcp --sport 53 -s 130.87.56.2 -j ACCEPT                         (3)
-A RH-Lokkit-0-50-INPUT -p tcp --sport 42 -s 130.87.56.2 -j ACCEPT                         (4)
-A RH-Lokkit-0-50-INPUT -p udp --sport 53 -s 130.87.56.2 -j ACCEPT                         (5)
-A RH-Lokkit-0-50-INPUT -p udp --sport 42 -s 130.87.56.2 -j ACCEPT                         (6)
-A RH-Lokkit-0-50-INPUT -s 172.30.32.102 -p udp -m udp --sport 123 --dport 123 -j ACCEPT   (7)
-A RH-Lokkit-0-50-INPUT -p tcp -m tcp -- dport 22 -j ACCEPT                                (8)
-A RH-Lokkit-0-50-INPUT -s 130.87.0.0/255.255.0.0 -p tcp -m tcp --dport 22 -j ACCEPT       (9)
-A RH-Lokkit-0-50-INPUT -p tcp --dport 25 -j ACCEPT                                        (10)
-A RH-Lokkit-0-50-INPUT -p tcp --sport 25 -j ACCEPT                                        (11)
-A RH-Lokkit-0-50-INPUT -p tcp --dport 113 -j ACCEPT                                       (12)
-A RH-Lokkit-0-50-INPUT -p tcp -s 130.87.32.65 --sport 515 -j ACCEPT                       (13)
-A RH-Lokkit-0-50-INPUT -p tcp --dport 80 -j ACCEPT                                        (14)
-A RH-Lokkit-0-50-INPUT -p tcp --dport 137:139 -s 130.87.57.44 -j ACCEPT                   (15)
-A RH-Lokkit-0-50-INPUT -p udp --dport 137:139 -s 130.87.57.44 -j ACCEPT                   (16)
-A RH-Lokkit-0-50-INPUT -p udp --dport 111 -s 130.87.57.44 -j ACCEPT                       (17)
-A RH-Lokkit-0-50-INPUT -p tcp --dport 111 -s 130.87.57.44 -j ACCEPT                       (18)
-A RH-Lokkit-0-50-INPUT -p udp --dport 1024 -s 130.87.57.44 -j ACCEPT                      (19)
-A RH-Lokkit-0-50-INPUT -p udp --dport 2049 -s 130.87.57.44 -j ACCEPT                      (20)
```

Table-9 is a sample of the TCPWRAPPERS configuration. In this sample, the default is turned to be secure by adding a line into */etc/hosts.deny* file. The allowed services and IP addresses are listed in */etc/hosts.allow* file. The sample accepts access to any services from *localhost* and the access to SSH from inside of KEK. It works with no operation when the parameter for the SSH is changed. In the sample, sendmail and NFS lines are included with the comment sign #. If a sendmail or a NFS line is changed, restart of the sendmail/NFS daemon is required. In this case, editing the /etc/sysconfig/iptables file may also be required.

If the host accepts the remote login, only the SSH is allowed to enforce the secure connection. To accept public-key-authentication or not is a choice. The point is that the administrator of the host can't check the key with a null passphrase of a client. Among the hosts, public-key-authentication is allowed, and a more secure remote access environment can be made using the ssh-agent.

Table 9 A sample of the tcpwrappers configuration

```
/etc/hosts.deny sample
        ALL: ALL
/etc/hosts.allow sample
        ALL: 127.0.0.1
        sshd: 130.87.
        ## If TCPWRAPPERS is included.
        #sendmail: 130.87. localhost local_host_name
        ## NFS, If TCPWRAPPERS is included.
        #portmap: 130.87.32.99
```

The system log is important to detect irregular or unauthorized accesses to the host. The log check software, such as *logwatch*, *logcheck*, or *logsurf*, helps to analyze the accesses. If required, it is possible to keep old logs by editing the files in the directory /etc/logroted.d/. To protect the logs from deletion by an intruder, sending logs to a remote host is effective. The

syslogd has this option.

If a host accepts login users, user account management, such as password robustness checks and validity checks of an account, is indispensable.

Not only the hosts on the DMZ, but also the hosts on the Intranet, are to be kept at a high security level. There is a possibility of an inside menace or accidental attacks.

Since November 2001, a Linux-support service is employed to support Linux users and administrators. The service covers mainly Red Hat Linux and Turbo Linux, consultation on Linux, providing security information by E-mail and by web pages. Red Hat security patches are available from the Web.

3.6. Host base solutions for Windows

It is the first step for improving security to apply new security patches which are provided frequently. The list of patches are on the Microsoft web space[9]. The tools *Windows Update* or *Office Update* download and install appropriate updates. The Microsoft *Software Update Services*[10] (SUS) was implemented at KEK in 2004 for automatic updating of Windows 2000 SP3 and Windows XP.

To minimize vulnerabilities, it is efficient to check the server services and stop unnecessary ones.
Access control of the service ports is available with *Windows Firewall*, supported in Windows 2000. The software does not support filtering by IP addresses. Other good filtering software exist, such as Norton Internet Security, Kerio Personal Firewall, and so on. For mobile PCs, the software is indispensable, to connect to the dial-up or the wireless LAN of the open spaces.

Anti-virus software is mandatory for Windows PCs to prevent viruses. Even though the software is employed in the PostKEK system, viruses are received not only by E-mail, but also by Web, USB sticks, and so on. Since the virus database is essential to the software, it is important to keep it up-to-date, to meet the new viruses that regularly appear. To avoid a risk in any case, it is the best choice not to open unexpected attached files. The default value of an E-mail client is to be changed not to open attached Office files and HTML files automatically. If there is an accessible Linux desktop, it is a better choice to open MS-word files with *Open Office*[11]. Carefulness will save the host and time. Anti-virus software also detects other types of network worms, such as the famous Blaster, which propagates through security hole of network programs.

The tutorials[5] and the documents on Windows security can be obtained from the Web.

3.7. User base solutions

For a user who has an account of a computer, there are two things that need attention. One is to keep the password secure. To reduce the risk of the password being cracked, strings hard to guess and hard to be broken should be chosen[12]. The password should be kept

Table 10 A sample of the public key authentication with SSH2

```
Step1: On a client host, make a key pair.
       [lune]$ ssh-keygen -t dsa
Step2: Put the generated public key into the
        "authorized_keys2" file on the SSH server host.
      [lune]$ scp id_dsa.pub soleil:.ssh
      [soleil]$ cd .ssh
      [soleil]$ cat id_dsa.pub >> authorized_keys2
      [soleil]$ chmod 600 authorized_keys2
Step3: Remote login with public key authentication.
      [lune]$ ssh soleil
      Enter passphrase for key '/home/monkey/.ssh/id_dsa':
```

[9] http://www.microsoft.com/technet/security/CurrentDL.aspx
[10] http://www.microsoft.com/security/guidance/prodtech/SUS.mspx
[11] http://www.openoffice.org/
[12] http://security.web.cern.ch/security/passwords/

secret in all cases. Even if a person says he is a system administrator and needs to know a user's password for a bug fix, one should not tell him the password. A real administrator never inquires a user's password. The only thing he does is to reset a user's password. It's also most important not to save the password in a computer file, unless it is encrypted.

The second important thing is to make a secure remote access. Network packets might be monitored from somewhere. To protect the password from eavesdropping, SSH should be used. Scp, sftp, slogin, and X-port forwarding are substituted for ftp, telnet, and xhost. If the speed of file transferring using the SSH is too slow, it's worth trying *blowfish* authentication. A sample is as follows:

```
$ scp –c blowfish source_file target_file
```

Table-10 gives samples of public key authentication with SSH2. Step1 is a key pair generation on a client host. Step2 is used to copy the generated public key to the SSH server host. On the host, the key is saved in the $HOME/.ssh/authorized_keys2 file. The public key authentication is now available. Step3 is remote login from the SSH client host with public key authentication. It works well if the prompt for the passphrase is displayed. If not, the trace list displayed with the following command will be helpful to check the reason:

```
$ ssh –v soleil
```

Table 11 Samples of .htaccess files

.htaccess for the limitation by IP address

```
< limit GET POST >
order deny,allow
deny from all
allow from .kek.jp .ac.jp
< /limit >
```

.htpasswd for the limitation by password

```
AuthType Basic
AuthUserFile /home/my_home/public_html/users
< limit get posts >
require user john paul
< /limit >
```

The points to consider about viruses and E-mails are explained in 3.6. Similarly, there may be viruses in downloaded files from Web. It is important to copy software and files from trusted sites, such as official vendors. Other things to consider are how to reply to the dialogue box displayed by some site, to enable Java and JavaScript or not. In general, it's safer to reply *no* to uncertain sites, disable Java and JavaScript when accessing unreliable sites.

If Web[6] space is acquired, the points to be nervous are not to violate software licenses and copyrights, and to be careful not to expose local documents to world wide. Access control is available with .htaccess and .htpasswd files in the document directory. Two types of limitations are available. One is by domain name or by IP address, and the other is by password. Table-11 shows samples. A password file for the limitations is created with a htpasswd command:

```
$ htpasswd -c $HOME/public_html/users john
```

4. Summary

There are no security incidents with Linux or UNIX hosts, since a firewall is activated. Security at KEK has been improved. To keep this security level of the hosts at least as it is, it is required to make continuous effort to apply new update programs as soon as they are released.

The anti virus software in PostKEK blocks thousands of viruses. Although this is very useful, still each user should not forget to exercise attention against new viruses in attachments, which will sometimes get through the check. The most secure solution is to be cautious not to open uncertain E-mail attachments.

Our next theme concerning security is how to make secure distributed computing systems, and how to block SPAM mail.

Acknowledgement

The author thank to Prof. Setsuya Kawabata for useful discussions. The author also thanks the members of working groups, especially Prof. Fukuko Yuasa, Mr. Teiji Nakamura, Mr. Kiyoharu Hashimoto and Prof. Hiroshi Mawatari, who are members from Computing Research Center. The figures are provided by courtesy of Ms. Tomoko Oshikubo and Dr. Kouichi Murakami.

References

[1] Practical Unix & Internet Security, Simson Garfinkel, Gene Spafford, Alan Schwartz, O'Reilly & Associates, Inc.
[2] KEK internal 99-3 (in Japanese)
[3] KEK internal 2001-15 (in Japanese)
[4] netfilter/iptables FAQ, http://www.netfilter.org/documentation/FAQ/netfilter-faq.html
[5] Microsoft Application Center 2000 Resource Kit Chapter 12 - Security: For Administrators and Developers, http://www.microsoft.com/technet/prodtechnol/acs/reskit/acrkch12.mspx
[6] Web Security, Privacy & Commerce, Simson Garfinkel, Gene Spafford, O'Reilly & Associates, Inc., 2001