Long-term experiences in keeping balance between safety and usability in research activities in KEK

Tadashi Murakami[1,*], *Fukuko* Yuasa[1,], *Ryouichi* Baba[1,], *Teiji* Nakamura[1,], *Kiyoharu* Hashimoto[1,], *Soh Y.* Suzuki[1,], *Mitsuo* Nishiguchi[1,], and *Toshiaki* Kaneko[1,]

[1]High Energy Accelerator Research Organization (KEK), Japan

Abstract. This work aims to provide KEK general-purpose network to support various research activities in the fields of high-energy physics, material physics, and accelerator physics. Since the end of the 20th century, on a daily basis, networks experience cyber-attacks and the methods of attack have rapidly evolved to become more sophisticated over the years. Security measures have been developed to mitigate the effects of cyber-attacks. While security measures may improve safety, restrictions might reduce usability. Therefore, we must keep a balance between safety and usability of the network for a smooth running of research activities.
Herein, we present our long-term experience with keeping a balance between safety and usability in KEK research activities. The key points are reasonably ensuring traceability and security management. We have been using security devices, such as firewalls, intrusion detection systems, and vulnerability management systems, to achieve a balance between safety and usability. Also, we present activities of the computer security incident response team (CSIRT) and collaborative activities among research organizations.

1 Introduction

In KEK, we provide a general-purpose network to support various research activities in the field of high-energy physics, material physics, and accelerator physics [1]. As shown in Figure 1, we continuously face difficult tradeoffs and are required to keep a balance between safety and usability when providing a network for the research activities. The safety aspect includes preventive and reactive protection, whereas usability aspect includes throughput, accessibility, privacy, and labor-saving. We achieve preventive protection using security devices. While restriction of network services/applications and network monitoring improves safety, excessive restrictions affect usability. Therefore, network monitoring should be carefully implemented to keep a balance between safety and usability.

In this paper, we present our long-term experiences in keeping a balance between safety and usability in KEK research activities. The principal focus of this work is ensuring traceability and security management in a reasonable manner. In Section 2, we describe our monitoring and blocking strategies with firewalls (FWs), intrusion detection systems, and manual protection. In Section 3, we describe our assessment strategies using vulnerability management system and user-friendly web portal site. In Sections 4 and 5, we describe computer security incident response team (CSIRT) activities within reactive protection and cooperative activities among research organizations.

[*]e-mail: tadashi.murakami@kek.jp

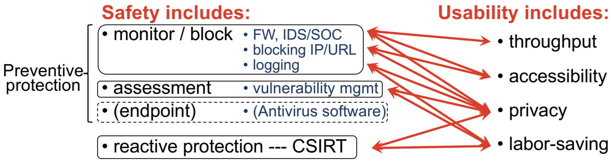


Figure 1: The tradeoff between safety and usability.

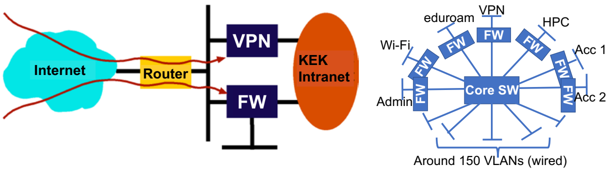


Figure 2: Firewall (FW) locations in KEK. Central FW between the Internet and intranet (left figure), and local FWs managed by each group (right figure).

2 Monitoring and blocking of network sessions

2.1 Firewalls: monitoring and blocking for safety and traceability

Firewalls (FWs) are one of our most essential devices for keeping a balance between safety and usability. Figure 2 shows FW locations in KEK. The central FW, which is shown on the left side of Figure 2, monitors all the connections between the Internet and our intranet, and it blocks suspicious addresses of internet protocol (IP), fully qualified domain name (FQDN), and uniform resource locator (URL). Several research groups have managed their own internal FWs, as shown in Figure 2–right figure, for their specific demands such as permitting access from only specific segments.

Tradeoffs exist while operating FWs in a network. One such tradeoff is that FWs can constitute bandwidth bottleneck in a network. Another is that fine segmentation increases the operation cost in terms of management of filter rules and packet monitoring, which prevents a quick response and results in error-prone operations. Another tradeoff is the fact that FWs can monitor users' behavior, thereby limiting their privacy.

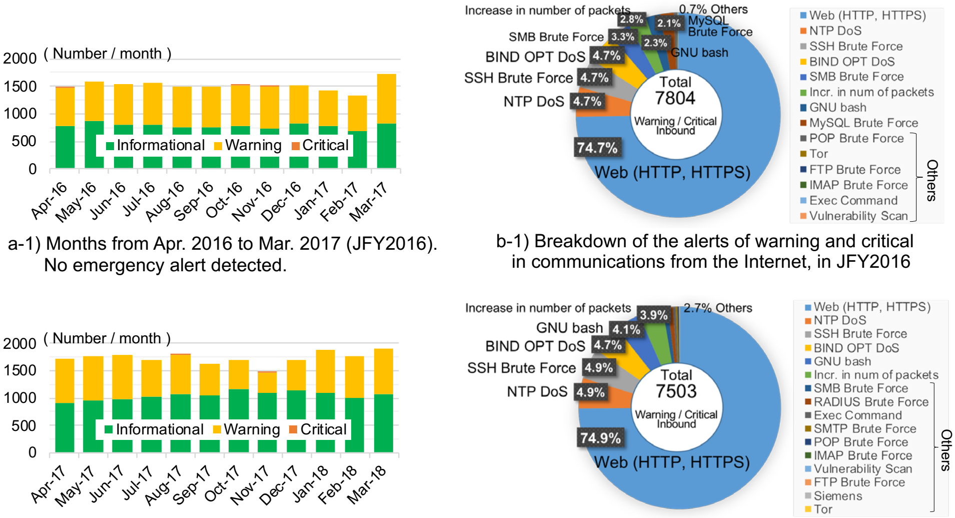
To manage these tradeoffs, we have adopted a step-by-step strategy, with respect to throughput, accessibility, and privacy. In 2002, we introduced a central FW in the zone boundary between the Internet, Demilitarized Zone (DMZ), and the intranet. In 2004, we added FWs to separate the wired network from the wireless network and Virtual Private Network (VPN). After that, we added separations for IPv6, eduroam[1], a network for Japan Proton Accelerator Research Complex (J-PARC), and others. Moreover, a few of the high-performance computing groups and large-scale experimental groups have installed dedicated FWs, which they manage.

Due to performance issues, it has been difficult for the central FW and other FWs to differentiate each wired network segments. We are planning to upgrade to more powerful FWs that can differentiate each wired network segments in September 2018. In this way, we will continue to operate FWs, one of our most important tool for network security, in a step-by-step strategy to manage the tradeoffs.

2.2 Intrusion Detection System (IDS): Collaboration with external Security Operation Center (SOC) service for safety

We introduced an IDS device for reactive defense and traceability. We did not adopt an Intrusion Prevention System (IPS) because it was difficult for the IPS to ensure the desired levels of throughput and accessibility in our environment. In the operation of the IDS, the

[1] Eduroam is an international roaming service for educational institutions.



a-1) Months from Apr. 2016 to Mar. 2017 (JFY2016).
No emergency alert detected.

b-1) Breakdown of the alerts of warning and critical
in communications from the Internet, in JFY2016

a-2) Months from Apr. 2017 to Mar. 2018 (JFY2017).
No emergency alert detected.

b-2) Breakdown of the alerts of warning and critical
in communications from the Internet, in JFY2017

Figure 3: Number of alerts from the SOC service categorized by the severity of the situation. a-1) and a-2) show the number of alerts from the SOC service, and b-1) and b-2) show the breakdown of warning and critical alerts in communications from the Internet.

system mirrors and monitors every packet from/to the Internet. The IDS generates a large number of alerts. For example, in April 2017, IDS generated 2.0×10^6 alerts. Further analyses by experts are mandatory to figure malicious communication from this vast number of alerts.

Therefore, we used an outsourced security operation center (SOC) service that provides a 24h 365 days human-based alert-log analyses. Although the IDS generated an average of 2.0×10^6 alerts per month, the SOC drastically reduces the number of alerts to about 1500 per month. When the SOC detects a malicious communication based on the analyses of IDS alerts, the severity of alert defines the next course of action. For alerts categorized as "Emergency" or "Critical," the SOC blocks the IP, and informs us. When we receive such an alert, we initiate a security incident response with the owner of the network device. While alerts categorized as "Warning" or "Informational" are not regarded as critical events, they are useful as reference information for the SOC to specify the real critical events.

Figure 3-a-1 and 3-a-2 shows the number of alerts from the SOC service categorized by the severity. Figure 3-b-1 and 3-b-2 indicates a breakdown of the alerts of warning and critical in communications from the Internet. Three-quarter of the alerts were related to the web. In the remainder of a quarter, two-thirds of the alerts were related to network time protocol (NTP), secure shell (SSH), and Domain Name System (DNS). From April 2017 to March 2018 (JFY2017), the SOC service noticed four "Critical" alerts, and no "Emergency" alerts were generated.

From the overall results, the SOC has been successful in detecting real malicious communications from plenty of alerts generated by the IDS. However, there is a possibility to overlook malicious communications, and it is difficult to inspect that.

2.3 Proactive protection: IP blocking and URL filter

We used the filtering list of malicious URLs that are automatically updated daily by the FW vendor. The list is categorized into various groups, including malware, gambling, and phishing. We selected one or more groups to protect our network automatically from the

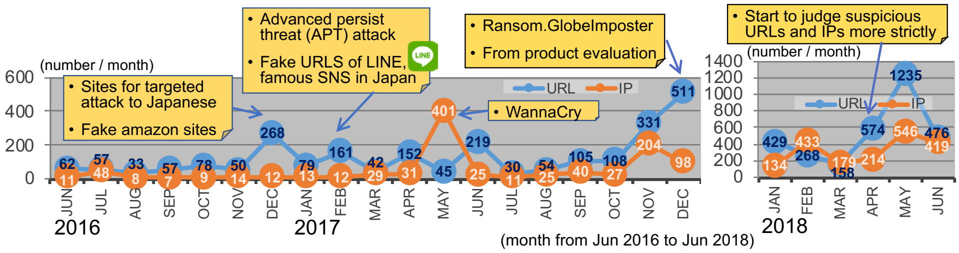


Figure 4: Number of manually blocked URLs and IPs. The blue graph shows the number of URLs and the red graph shows the number of IPs.

URLs within the groups. Users of wireless and VPN networks tend to be more vulnerable than users of wired local networks because wireless and VPN users are more likely to use the network for daily activities. Then, we assigned a greater number of groups and protect wireless and VPN networks to prepare against risks.

The filtering list is useful, but we cannot rely entirely on this list because it includes a significant amount of false-positive and false-negative URLs. For instance, some important academic sites were flagged as malicious that is false-positives while some malicious sites were not flagged as malicious that is false-negatives. In both cases, domestic sites tend to be misjudged more easily.

To manage these tradeoffs, from June 2016, we started adding URLs and IPs manually to supplement the vendor's filtering list. Figure 4 shows the monthly summary of the number of addresses (URLs and IPs) blocked manually. We gathered addresses of malicious sites from public agencies[2], commercial SOCs, websites, KEK administrative division[3], and so on. In December 2017, there were more than 500 blocked addresses.

There were no requests to reopen the manually-filtered URLs and IPs in the two years following June 2016. Conversely, there were four requests to reopen the false-positive vendor-based filtered URLs from June 2016 although we employed only a few groups that could be regarded as malicious from the filtering list. It is acceptable for us to receive four requests in two years. However, the addition of a greater number of groups warrants more careful consideration and analyses on our part.

The overall results show that this manual filtering works successfully with careful operation to manage the tradeoffs between the false-positives and false-negatives.

2.4 Logging IP traffic for traceability

Using the central FW, logs of IP connections were stored for traceability. When a security incident occurs, in many cases we initiate an incident response by investigating the connection logs. If there is any mistake in logging, the incident response is flawed from the outset.

Figure 5 shows the number of traffic logs from the central FW. For example, in December 2015, in one week the log files generated contained 720 million records amounting to 215GB of storage space. The number of logs continues to increase, and it is difficult to estimate

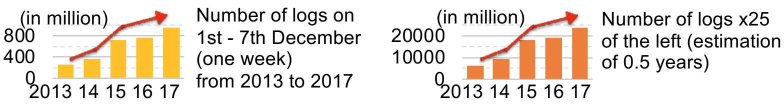
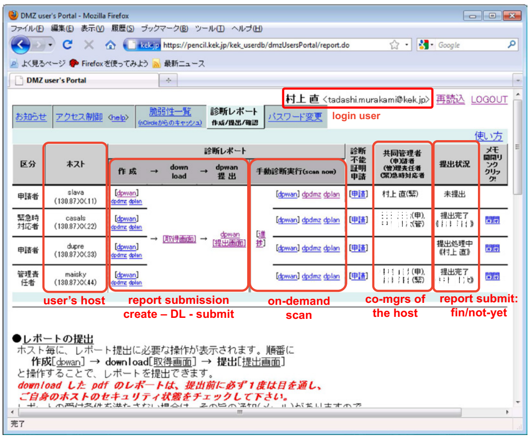


Figure 5: Number of traffic logs from central FW.

[2] JPCERT/CC, IPA, NII-SOCS, MEXT, and so on.

[3] An email attack notification system in KEK administrative division has been working. We receive about one notification per two days.


DMZ user's Portal - Mozilla Firefox
ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)
kek.jp https://pencil.kek.jp/kek_userdb/dmzUsersPortal/report.do
Google
よく見るページ Firefox を使ってみよう 最新ニュース
DMZ user's Portal
村上 直 <tadashi.murakami@kek.jp> 再読込 LOGOUT
login user
お知らせ アクセス制御 <help> 脆弱性一覧 (nCircleからのキャッシュ) 診断レポート 作成/提出/確認 パスワード変更
使い方
user's host
report submission
create – DL - submit
on-demand
scan
co-mgrs of
the host
report submit:
fin/not-yet
完了

区分	ホスト	診断レポート 作成 →	 down load →	 dpwan 提出	手動診断実行(scan now)		診断不能証明申請	共同管理者 (申)請者 (管)理責任者 (緊)急時対応者	提出状況	メモ開閉リンククリック!
申請者	slava (130.87.XX.11)	[dpwan] dpdmz dplan	→ [取得画面] →	dpwan [提出画面]	[進捗]	[dpwan] dpdmz dplan	[申請]	村上 直(緊)	未提出	
緊急時対応者	casals (130.87.XX.22)	[dpwan] dpdmz dplan				[dpwan] dpdmz dplan	[申請]	[illegible](申), [illegible](管)	提出完了 《[illegible]》	開閉
申請者	dupre (130.87.XX.33)	[dpwan] dpdmz dplan				[dpwan] dpdmz dplan	[申請]		提出処理中 《村上 直》	開閉
管理責任者	maisky (130.87.XX.44)	[dpwan] dpdmz dplan				[dpwan] dpdmz dplan	[申請]	[illegible](申), [illegible](緊)	提出完了 《[illegible]》	開閉

●レポートの提出
ホスト毎に、レポート提出に必要な操作が表示されます。順番に
作成[dpwan] → download[取得画面] → 提出[提出画面]
と操作することで、レポートを提出できます。
download した pdf のレポートは、提出前に必ず1度は目を通し、
ご自身のホストのセキュリティ状態をチェックして下さい。

Figure 6: Main page of DMZ User's Portal.

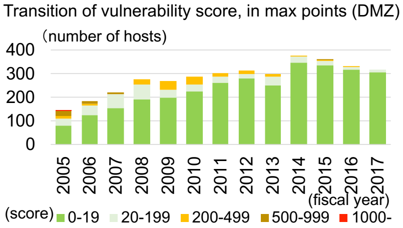


Figure 7: Transition of vulnerability score in terms of maximum points in DMZ.

the number of logs in the future. For traceability, multiple copies of the logs were stored in multiple measures on different servers, including Syslog by syslog servers managed by technical operating staffs, Syslog servers managed by authors, log replication using Gfarm [2] with compression by gzip (under 10% size), secure copy (SCP) from central FW every hour, and log analysis application. Log analysis is essential, but in our environment, proprietary tools are unsuitable from the viewpoint of performance or annual cost.

In summary, log analysis is crucially important at the beginning point of the incident response. Thus, we take multiple measures to store the logs. We have to deal with the increasing size of logs year by year.

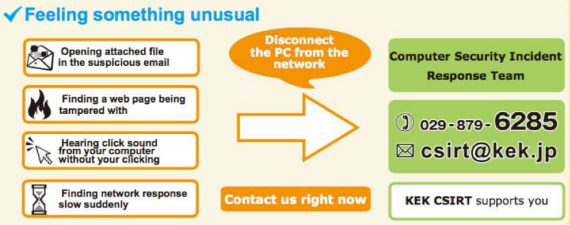
3 Assessment: Vulnerability management to maintain the server environment efficiently

In KEK, various research groups engage in various fields of physics. They need services that are not covered by the standard services provided by the computing research center. Moreover, it is difficult to set security standards because each of the hosts has its own circumstances such as historical reasons.

The KEK-DMZ network consists of more than 300 individual hosts (DMZ hosts) managed by about 100 administrators. Administrators of DMZ hosts (DMZ admins) have their own responsibilities in security management such as access control, security patch, and vulnerability management. We have a vulnerability scanner, which is used to analyze hosts and evaluate each one's vulnerabilities in the form of a score. The scanner is proprietary and has rich functions, but it is too intricate for non-security-experts.

To solve the above problems, we incorporated the vulnerability scanner into developing a site named DMZ User's Portal in 2007 [3–5]. Since then, we have operated and improved the portal.

We developed a web site and a wrapper module for the vulnerability scanner; the wrapper module adds tolerance to the change of specification in the vulnerability scanner. Figure 6 shows a screen of the main page of DMZ User's Portal. With this portal, DMZ admins can use the vulnerability scanner easily with one click to run a security analysis of the owner's host. The result can be downloaded as a PDF report. The scanner automatically scans all DMZ hosts weekly to find vulnerabilities and evaluate by scoring them. If the score of more than 1000 point is detected, the detected vulnerability is regarded as severe, and the portal sends an email alert. In this way, security management can be executed by each DMZ admin.



✓ Feeling something unusual

- Opening attached file in the suspicious email
- Finding a web page being tampered with
- Hearing click sound from your computer without your clicking
- Finding network response slow suddenly

Disconnect the PC from the network

Contact us right now

Computer Security Incident Response Team

☎ 029-879-6285
✉ csirt@kek.jp

KEK CSIRT supports you

Figure 8: Extract from the security leaflet "KEK computer security 11 Best Practices" issued in 2017 for foreign researchers.

In 2011, we extended the portal and introduced it into a network for J-PARC, a joint site with KEK. In 2017, we introduced the portal to a network for HEPnet-J, another joint site with KEK.

We have performed annual security self-inspections since 2007. In these self-inspections, DMZ admins use DMZ User's Portal themselves to check their hosts, and submit reports. Our security management committee inspects the submitted reports. Figure 7 shows the transition of vulnerability score in terms of maximum points in DMZ. In 2005, more than 25% of the hosts had vulnerability scores higher than 200 points. Since then, the number of hosts with high scores has gradually decreased. Especially after 2014, hosts with low scores (green) became the majority in number, and the hosts that have higher than 200 points have accounted for less than 5% of the total.

In this way, user-based quality management of DMZ hosts has been successful with the help of DMZ User's Portal.

4 Reactive protection: incident-response after compromise and targeted email attacks

4.1 KEK CSIRT

We started KEK CSIRT in 2012. The mission of our team is to defend information assets from inner and outer threats. To meet this objective, our team advices users when they are facing security incidents. Figure 8 shows an extract from the security leaflet issued in 2017.

When a security incident occurs, our team provides the initial responses that include investigations, analysis, and prevention of damage from spreading. After that, our team contacts users to devise with the users a recovery plan and measures for recurrence prevention. Then, the users and our team implement the plan as well as the measures.

Although it is important to keep the network environment safe, very severe measures for security also reduce the flexibility of the network environment. Such a non-flexible network would be unsuitable for a research institute. Hence, KEK CSIRT is always faced with trade-offs. Another important point is our activities are based on trust relationships with network users. We respect the users' privacy, and we always interact with users, as opposed to operating in a command-hierarchical manner. Without trust from the users, we cannot proceed with an appropriate incident response, which itself poses a risk in terms of keeping security.

4.2 Fight against targeted email attacks

Email is one of the most attractive services for attackers. Figure 9 shows statistics of the KEK main email server, PostKEK. The left graph presents the total number of emails and spam messages. According to this graph, most of the emails are spam. The right graph presents the number of emails detected as viruses by the built-in antivirus software in PostKEK.

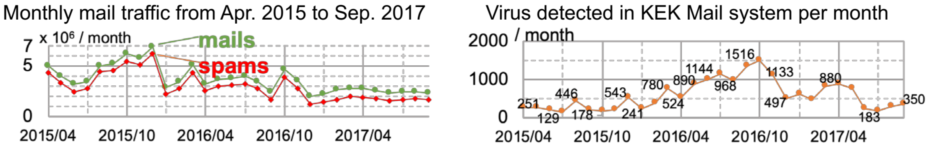


Figure 9: Statistics of the KEK main email server, PostKEK.

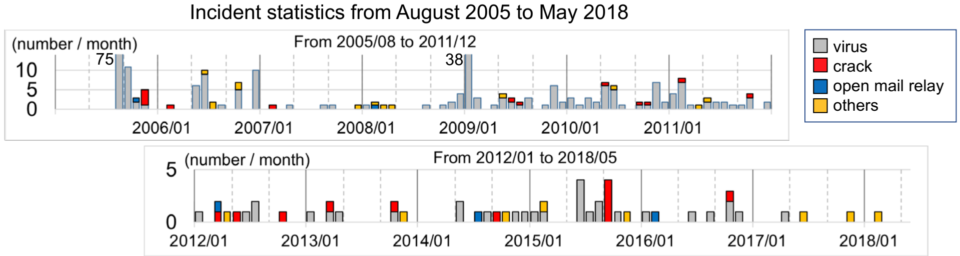


Figure 10: Incident statistics from August 2005 to May 2018. The graph shows the number of reports submitted by users who take incident responses from KEK CSIRT due to illegal access. In these years, the number of reports has remained relatively small.

These days, we occasionally receive sophisticated targeted emails in fluent Japanese using the names of well-known companies[4]. Another example is a password reset fraud emails that sent from someone masquerading as a KEK email administrator to KEK email accounts.

To make matters worse, academia has become a target now. In January 2017, a notification email from a fake Japanese funding agency for researchers (JSPS) was sent to researchers. The email contained a notice about funding, and a malicious zip file was attached to the email. Because notices about funding are important to every researcher who receives funding, it is impossible to ignore such a notice without consideration, even if it is suspicious.

Because it is difficult to protect against such attacks by using an email security appliance and endpoint antivirus software, an annual drill has been performed for user training. In the drill held in 2017, the training emails were sent twice in a few weeks, to about 1600 email accounts of PostKEK. Although the opening rate of the emails seems an easy-to-understand quantitative indicator at a glance, we believe that the email-opening rate itself does not have much meaning because the rate depends on content. The important thing is to ensure that email users have continuous chances to aware that emails have to be handled with care.

4.3 Incidents statistics

Figure 10 shows the incident statistics in KEK from August 2005 to May 2018. The graph shows the number of reports submitted by users whose computers underwent incident responses from KEK CSIRT owing to illegal access. Although the frequency of cyber-attacks has increased over the years, the number of incident responses remained relatively small. Notably, we have been able to decrease the number of incidents in the recent ten years. Hopefully, our strategy has been working well, with users' improvement of self-conscious of security. However, sometimes, the general opinion in Japan demands "zero risks," and *the goal* of zero incidents is not achieved at all.

5 Cooperative activities

Each organization has confidential information related to security, which includes crucial for many organizations. Therefore, it is important to build trust relationships among the orga-

[4] e.g., Japan postal service, AppIe, Amason, NTT-X (Japanese online shop), credit-card company, ...

nizations to facilitate the exchange of confidential information. We have relationships with other organizations mainly in two domestic associations: NCA (Nippon CSIRT Association,) and SWS (Security WorkShop).

NCA shares ideas about CSIRT activities among various organizations via frequent meetings. In April 2016, the number of CSIRT teams stood at 137. The number increased to 222 in April 2017. KEK is the first academic team to have joined NCA in 2012. In 2016, there were three academic CSIRT teams. In 2017, the number has increased.

SWS establishes an association among research organizations through an annual workshop for sharing unofficial information. SWS started in 1999, and their first meeting was held in KEK. The members include RIKEN, SPring-8, RCNP, and KEK.

6 Summary

We are constantly facing difficult tradeoffs and are required to keep a balance between safety and usability in research activities. In this paper, we presented our long-term experiences about keeping a balance between safety and usability in terms of KEK research activities in a reasonable manner.

While monitoring and blocking transactions, we operate FWs, IDS, commercial SOC service, and manual blocking operations. Tradeoffs exist while operating FWs and IDS in a network. Safety enhancements often conflict with throughput, accessibility, and privacy. During vulnerability management, we operate a vulnerability scanner. However, tradeoffs also exist where safety enhancements often conflict with privacy and labor-saving.

To manage these tradeoffs, we adopted the step-by-step strategy to provide the desired throughput, accessibility, privacy, and labor-saving.

In monitoring and blocking, we introduced measures in a step-by-step manner. We introduced auto-blocking with care and care. The operation was successful and there were only a few requests to reopen blocked addresses. During vulnerability management of the DMZ network, we developed and operated a portal that facilitates easy use of our vulnerability scanner. In addition, we have had annual security self-inspections. In the basis of step-by-step strategy operations above, CSIRT activities are important for reactive protection. In CSIRT activities, a trust relationship with the network users is crucial.

7 Future plan

Our network and security infrastructure was renewed according to a new lease contract in September 2018. In the new infrastructure, FWs perform more powerfully. Therefore, we have just started separating wired network segments into several groups. We need to investigate the effects of the separation.

Our vulnerability management has been successful for 13 years. On the other hand, it became difficult for the vulnerability scanner to detect severe vulnerabilities. Therefore, we decided to replace the vulnerability scanner with a more powerful and complex one. The new scanner tends to detect more vulnerabilities which contain false-positives. We also need to investigate and review the performance of the new vulnerability scanner.

References

[1] F.Yuasa, et al, *HEPiX Fall/Autumn 2017 Workshop* (2017)

[2] O.Tatebe, et al, New Generation Computing **28**, pp 257 – 275 (2010)

[3] T.Murakami, *CHEP 2018* (2018) (to be appeared)

[4] T.Murakami, *IEEE/ACIS ICIS 2008*, pp. 127 – 132 (2008)

[5] T.Murakami, T.Amagasa, H.Kitagawa, *IEEE COMPSAC 2013*, pp. 589 – 598 (2013)