Sustainable and Secured Computing Environment for ICT Education

Tomoaki Sato
C&C Systems Center
Hirosaki University
Hirosaki, Japan
E-mail: tsato@cc.hirosaki-u.ac.jp

***Abstract*— An ICT (Information and Communication Technology) education is widely performed at universities and the education using a student's own PC (Personal Computer) has been performed. The author performed computer literacy education and lectured for students who major in ICT using the PC. According to the results of ICT education, the problems are clarified. USB memory-based computing is proposed for the solution of the problems. The performance of USB memory-based computing is evaluated by using a test program. The results show that it is sustainable computing environment. A security system for ICT education using a student's own PC is introduced.**

Keywords-component; ICT education; Student's own PC; USB memory-based computing; Secured computing

I. INTRODUCTION

The appearance of computers and the Internet has a large influence on university education. The use of a computer enables easy creation of documents and diagrams and achieves vastly reducing time of data processing. The use of the Internet enables not only obtaining large amounts of information and easy information retrieval but also disclosing information to all over the world. Furthermore, the use of computers is demanded in a lot of classes for e-Learning or an interactive education.

Opportunities for use of computers at universities have increased. Therefore, the use of a computer at universities has changed from use in the computer room of a university to a personal computer that a student owns. As a result, ICT education using a student's own PC (Personal Computer) has been performed [1]. When the student's own PC is used in a conventional lecture, the conventional lecture can be changed into an interactive lecture. Learning the management technique of a PC is enabled by using it. Especially, it is very important for all students to learn security measures.

In this paper, ICT education by using the PC is introduced. The author performed computer literacy education and lectured for students who major in ICT using the PC. Experiences of establishment of support system and the model selection of the PC for education have been had. According to the results of ICT education, the problems are clarified. USB memory-based computing is proposed for the solution of the problems.

USB memory-based computing is a method of using a USB flush drive in place of the student's own PC. An operating system and application software are installed in the USB flush drive. It is used on various computers such as computers in a university, a home, an Internet Cafe, and so on. That is, it is used as a computer only for you. In addition, the operating system is free software based on Linux. Therefore, not only the operating system but also the word processor, the spreadsheet and the presentation software can be used free of charge. Additionally, it is possible to use it in old PC. It means a sustainable computer education and is feasible in a lot of regions.

This paper is organized as follows. Section II presents the outline and problems of ICT education using a student's own PC. Then, Section III describes USB memory-based computing for sustainable ICT education and it is evaluated. A security system for ICT education using a student's own PC that the author is developing is introduced on Section IV. In Section V, the conclusion is made.

II. ICT EDUCATION USING A STUDENT'S OWN PC

At a lot of universities, a student's own PC is used in classes [2]. Its usage is not only practice in a computer literacy class but also execution of interactive lecture using an e-Learning system. Study that uses the PC can use the same computing environment even in places other than the lecture room of the class.

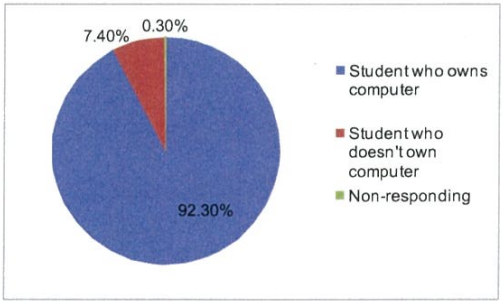

Fig. 1 Ratio of student who owns computer.

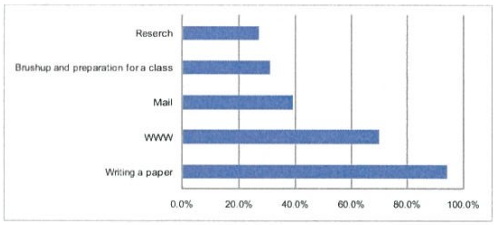

Fig. 2 Purpose of use.

The investigation of the actual conditions of student life was executed in Hirosaki University in October, 2006 [3]. The author was a member of the investigative committee. Fig. 1 shows the PC ownership rates of students at that time. According to the results, most students own a PC. It is thought that the ratio of that now has risen further. The purpose of use of the PC is shown in Fig. 2. Writing a paper has the target majority. However, the purpose of use of the brushup and the preparation for a class is 31 % of the PC owners. Therefore, the use of the PCs for classes is very important.

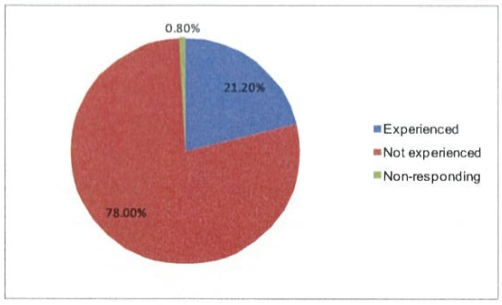

Fig. 3 Ratio in which trouble is experienced.

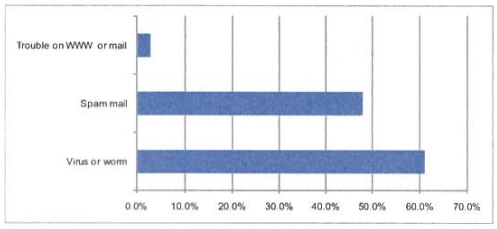

Fig. 4 Kind of Fig. 3.

Fig. 3 shows that the ratio to which the students experienced troubles concerning a PC. Moreover, Fig. 4 is the breakdown. These results mean that most students do not experience the troubles. However, for example, students of Department of Medicine treat important information on patients. In this case, troubles mean the serious issue. Therefore, information security education should be indispensable, and the action method should be learnt.

To learn an information security, the administration authority of a PC is needed. In general, students don't have the authority in PCs that a university owns and the PCs managed by s manager at the university. Thus, the students cannot freely install software in the PCs. However, in a student's own PC, it is enabled.

A. Use methods and problems of a studen't own PC

According to the web page of [2], at least 21 universities in Japan are performing ICT education using a student's own PC. Because the web page is written by using information open to the public on the Internet, it is assumed that it is performed at more universities. From the viewpoint of interactive education, iPhone [4] or iPad are used at some universities.

ICT education using a student's own PC has been performed at the university to which the author had belonged [1]. In the university, not only computer literacy and programming classes but also social investigation practice has used a student's own PC. The author took charge of classes concerning computer literacy, computing environment management, and computer architecture. In the computer literacy class, there is an advantage that its same environment can be used in places other than the university. In the class of computing environment management, the administration authority was used.

The author selected student's PC and constructed the system of the support. As a result, the following problems were clarified.

- When the worm such as Blaster is occurred, most PCs of the students were infected.
- The unification of models and Oss is difficult

When Blaster was generated, most of students did not execute windows update. As a result, because the traffic quantity by Blaster was increased, the classes that had used it was not able to be performed.

Exterminating of the worm was executed by all members of the faculty of the university. Considerable labor was used for that. In a university, the professional edition of windows is preferred because sharing files and printers is needed. Especially, the use of the same computing environment is indispensable in a computer literacy class. However, when a student buy a PC, it is difficult to understand it. Accordingly, reinstalling the OS of some PCs is demanded. And, it is difficult for the student the work.

It has been announced hard at the university that to buy the specified PC. The system of the support for the PC has been established. It has been operated by the students. External HDD has been prepared and the trouble of the PC is recovered by using the HDD. Problems in a software license have been solved by the school agreement of Microsoft. It means OSs and applications of Microsoft can be freely used.

III. USB Memory-Based Computing for Sustainable ICT Education

USB memory-based computing is a technique to achieve a computing environment for exclusive use of oneself. The technique is achieved by using a USB flush drive shown in Fig. 5. An OS is installed in the USB flush drive. Then, the OS is booted on various PCs and used. New applications can be installed in the USB flush drive. When Linux is used, the cost is free. In addition, Open Office can be used as alternative of Microsoft Office and a freeware. The cost of the USB flush drive is under JPY 2,000.

Linux can be used on an old PC. That is, the old PC can be used until breaking down. On the other hand, Windows can be used for the support period. Because an OS and applications are installed in not a HDD but a USB flush drive, it can be easily used on various computers. Also when a computer breaks down, the correspondence is easy. As a result, this means a sustainable education in respect of cost can be established.

The problems of a student's own PC shown in Sec. II are solved by using it. The use of LINUX doesn't cause the problem in the CAL (Client Access License). Because it can be used on a PC in a university or an Internet Café, the computing environment for exclusive use of oneself is constructed without a PC for exclusive use of oneself.

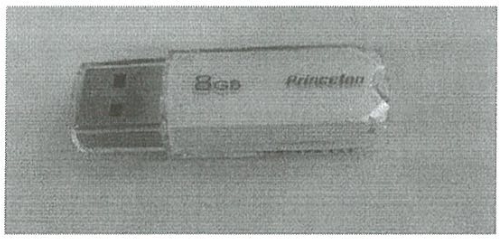

Fig. 5 USB flush drive.

A. Evaluation

The author evaluates it with a PC with low performance. For the evaluation, Linux on a USB flush drive and Windows XP Pro. on a HDD on the same PC are used. Table I shows the PC spec for the evaluation. To evaluate the performance, the program that calculates 30,000 digits of π is used. It is corded by using C language. Visual studio 2008 is used for the source file of Windows and gcc on Linux is used for the source file of Linux. Optimization option of the execution speed is used. In addition, processing times of starting and shutting are evaluated.

TABLE I
PC Spec for the Evaluation

Processor	VIA C7-M ULV 1.6 GHz
Memory	2GB
HDD	160 GB, Serial ATA 5400rpm
Original OS	Windows XP Professional SP3 Japanese Edtion
USB flush drive	Princeton PFU-2JUR 8GB
OS in the USB flush drive	Ubuntu 10.04 (Linux)

Performance evaluation results are shown in Fig. 6. According to the results, the computer by Linux on the USB flush drive works in 3.4 times high speed of the computer by MS Windows XP on a HDD. In other words, an old PC with LINUX can be used for ICT education. Another problem is reading and writing speed of a USB flush drive. The speed of the USB flush drive is slower than that of a HDD. Nevertheless, it is shown that the processing time of starting and shutting of the Linux system on the USB flush drive is faster than that of the Windows system on a HDD in Table II.

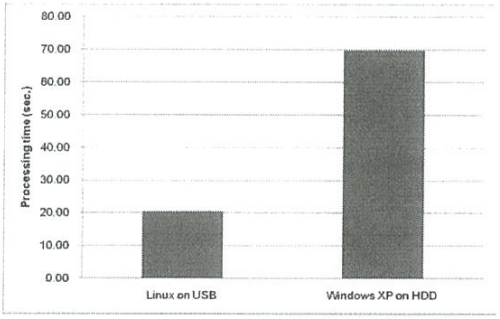

Fig. 6 Performance evaluation results.

TABLE II
Processing Time of Starting and Shutting of OS

Drive	OS	BIOS to Login	Login operation	Login to Connect to the Internet	Shutdown processing
HDD	Windows XP Pro.	50 sec.	20 sec.	115 sec.	45 sec.
USB	Ubuntu	80 sec.	20 sec.	40 sec.	37 sec.

IV. Security System for ICT Education Using a Student's Own PC

Even if the use of a student's own PC is in campus networks, it faces the danger of unauthorized computer access and computer viruses [5]. Incidents of copyright infringement by using a file exchanging software frequently occur. The use of the file exchanging software causes information leakage.

Therefore, measures for the software use are demanded [6]. For the measures, the author has developed a security system.

In order to avoid unlawful computer accesses, an IDS (Intrusion Detection System) has been used in wired LAN. And it that applies the function to defend is an IPS (Intrusion Protection System). The IDS is categorized into a network-based IDS (NIDS) and a host-based IDS (HIDS). The NIDS installed to dedicated network computers at companies and universities makes the real-time analysis of flowing packets and detects unauthorized computer access. The drawback of these processes is that they take long delay to treat large packets. This is hard to solve even if cutting edge high-performance network computers are used for the network-based IDS. Thus, it is not almighty for unlawful computer accesses. Unfortunately, unauthorized computer access once exceeded the network-based IDS invades computers in LAN. The access acts violently among computers within those networks. At present NIDS for WLAN has been announced only by IBM in November 2003. This has a problem similar to conventional IDS [7].

The HIDS to be installed in individual host computers for personal uses is really promising for the protection of each of them. However, the HIDS so far developed is software that works statically in checking falsified files, information set on operating systems, and process information. Thus, conventional HIDS lacks real-time response and has poor ability to analyze packet. To solve such issues, we have proposed H-HIDS (Hardware-based HIDS).

H-HIDS furnishing the function of both the NIDS and the HIDS is logic-based HIDS achieved by FPGA (Field programmable gate array) and can easily achieve the IPS function. This is reconfigurable hardware. Basic algorithms of conventional HIDS have been made use of to the Netlist of FPGA. In designing H-HIDS, we aim to achieve more advantageous features with less power than conventional HIDS. Intrusion detection processing on logic requires cipher such as WEP (Wired Equivalent Privacy) and CRC (Cyclic Redundancy Check) at high-speed with less-power consumption. Power consumption is one of most important properties for a mobile computer and PDA (Personal Digital Assistance) driven by a battery. The analysis of a detailed packet level is crucial for fulfilling these requirements.

The Network-based IDS is practically limited by the performance of processing computer. Thus, it is hard to process all the packet analyses with the increase of the amount of packet. In [8], a detection technique by the traffic pattern was described. However, it is necessary to analyze all packets in detail to do more accurate detection.

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

A. Intrusion Detection Logic

H-HIDS has IDL (Intrusion Detection Logic). The IDL of NIC that plays in part the function of network-base IDS should process the packet analysis more than three layers of OSI (Open Systems Interconnection) layer model.

After manufacturing custom design VLSI processor cannot change hardware, it cannot add a limitation to a specific protocol and a new function. Therefore, it cannot be used for IDL. Then, the hardware processing that is only software becomes possible by using FPGA as for IDS. The TCP/IP Flow Monitor circuit [9] was achieved with FPGA for such reasons.

The host-based IDL is really useful for packet analysis and port monitoring. Port monitoring so far supported by OS watches port access whose number is used for specifying network applications such as mail, web, and DNS according to TCP/IP and UDP/IP. Then, the function of port monitoring gives response for network applications that makes the user-specified ports active and the other ports inactive. Since the built-in hardware IDS gives immediate response, it is also helpful for host computers to forbid unauthorized access. Besides, the monitoring function is effective for Denial of Service (DoS) attack that sends a burst of packets such as Smurf and SYN FLOOD to computers.

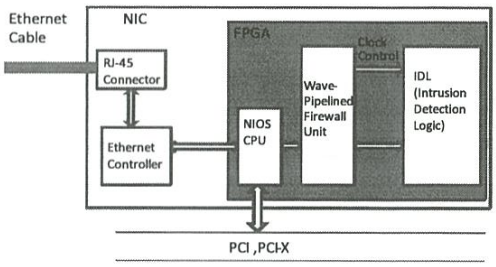

Fig. 7 Hardware Structure of H-HIPS.

Fig. 7 shows hardware structure of H-HIPS for Ethernet. The IDL of H-HIPS solves the problem of software IDS. In addition, it is cost-effective. The cost of FPGA chip is 22 US dollars or less in the scale of 250,000 unit volumes [10]. Thus, the IDL can be introduced in an individual environment such as a Wireless LAN. Moreover, it can cover a large-scale network because the packet analysis function of conventional network-based IDS is distributed by each host.

B. Firewall Unit

Fig. 8 shows the outline of the firewall for H-HIPS [11]. Table I is the controlled ports for lap-top computer, mobile phone, or PDA (Personal Digital Assistant), and they are at least needed. Because the firewall unit is developed by FPGA, the change of ports is very easy.

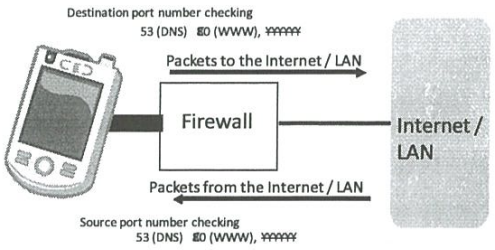

Fig. 8 Firewall for H-HIPS.

TABLE III
CONTROLLED PORTS

Function	Port Number	Binary
NOP	0	0000000000000000
SMTP	25	0000000000011001
DNS	53	0000000000110101
HTTP	80	0000000001010000
POP3	110	0000000001101110
HTTPS	443	0000000110111011

V. CONCLUSION

In this paper, USB memory-based computing has been proposed for the solution of problems on ICT education using a student's own PC and sustainable ICT education. Linux operations on the USB flush drive and MS Windows XP Professional operations on the HDD were evaluated by the pi calculation of 30 million digits on same PC. As a result, it was shown that the Linux operations on the USB flush drive are more high-speed than the MS Windows XP Professional operations on the HDD. It means USB memory-based computing is applicable on an obsolete PC. The security system in campus networks for a student's own PC was introduced. Our future works are an investigation of the sustainability of server systems and network systems.

ACKNOWLEDGMENT

This work has been supported in part by Grant-in-Aid for Young Scientists (B) (21700064) from Ministry of Education, Culture, Sports, Science and Technology, Japan.

REFERENCES

[1] K. Satoh, "The Specification for Educational Environment with Note PCs of its Application Study," *Social Information*, Vol. 13, No. 1, pp. 29-63, 2003.

[2] H. Nagataki. (2010, August). Summary of Using a Student's Own PC in an Educational Institution. [Online]. Available: http://www.okayama-u.ac.jp/user/nagataki/notePC.html.

[3] Hirosaki University, *Investigative Report of the Actual Conditions of Student Life*, Hirosaki University, 2007.

[4] Y. Miyajima, and Y. Iijima, "The objectives and influences of iPhone use in the school of social informatics at Aoyama Gakuin University," *Computer&education*, No. 28, pp. 4-10, 2010.

[5] 4a-T. Sato and M. Fukase, "Hardware Approach for Unauthorized Computer Access and Computer Virus in Wireless Campus LAN," *Journal for Academic Computing and Networking*, No. 9, pp. 15-26, 2005.

[6] T. Sato, S. Imaruoka, and M. Fukase, "FPGA Implementation of Winny Detection in a Campus Networks," *Journal for Academic Computing and Networking*, No.12, pp. 68-74, 2008

[7] T. Sato and M. Fukase, "Reconfigurable Hardware Implementation of Host-Based IDS," *Proc. of the 9th Asia-Pacific Conference on Communication*, Vol. 2, pp. 849-853, 2003.

[8] Y. TAKEI, K. OHTA, N. KATO, and Y. NEMOTO, "Detecting and Tracing Illegal Access by using Traffic Pattern Matching Technique," *Trans. of IEICE*, Vol. J84-B, No. 8, pp.1464-1473, 2001.

[9] D.V. Schuehler, and J. W. Lockwood, "TCP Splitter: A TCP/IP Flow Monitor in Reconfigurable Hardware," *IEEE Micro*, vol. 23, No. 1, pp. 54-59, 2003.

[10] EE Times. (2010, August). Lower Cost Drives New FPGAs. [Online]. Available: http://www.eeproductcenter.com/printableArticle.jhtml?printable=true&articleID=22103038.

[11] Sato, T., Imaruoka, S., and Fukase, M. (2009) Verifying firewall circuits by wave-pipelined operations, *Proc. of IEEE TENCON 2009*, pp. WED3.P.14.1 -WED3.P.14.6.