ABSTRACT
The Nara Institute of Science and Technology (NAIST) user authorization management system for network accesses (NAS) was designed and developed as a campus-network management system for administrators who are not information and communications technology (ICT) experts. Student residents have successfully operated the system in the dormitory network since November 2002, in the staff accommodation network by residents since June 2003, and as the component of the Guesthouse Network Management System by office helpers since June 2004. In Japan, administration of the system is performed by volunteer instructors and students for various reasons, which includes inadequate budget allocation and human resource constraints, and insufficient provisions for the system maintenance. Designing a system for the system administration volunteers is not easy because of their wide-ranging technical levels and unstable joining period. In our development, we defined the following minimum requirements for the system design:

1. The system does not require a full understanding of the management logic for daily operation.
2. No special operations are required even after the base operating system is updated (i.e., application of security patches).
3. The control logic can be modified easily by the administrators when the network administration policy changes.
4. The system can be operated in an open-source UNIX-like environment.

In this paper, we describe the development and deployment of our system in the campus and clarify the advantages and disadvantages of the system. We will also discuss various issues in system operation of the dormitory network by student residents, e.g., what has happened to this network in the two years operation.

Categories and Subject Descriptors
C.4 [Performance of Systems]: Reliability, availability, and serviceability;
K.6.2 [Installation Management]: Performance and usage measurement;
D.4.6 [Security and Protection]: Access controls

General Terms
Management, Design, Reliability

Keywords
Campus-network, Authorization, Voluntary-management

1. INTRODUCTION
NARA INSTITUTE OF SCIENCE and TECHNOLOGY (NAIST), a national university composed solely of graduate schools, has promoted advanced research since October 1991. NAIST also educates accomplished individuals to help in the development of
society based on the advancement of science and technology. At NAIST, the standard period for completion of a master's program is two years, and the completion period of a doctoral program is three years. NAIST promotes three graduate courses: Information Science, Biological Sciences, and Materials Science. In April 2005, NAIST had 1094 student and 405 faculty. The budget is about 10.1 billion yen [4].

The Information Technology Center (ITC) of NAIST provides the MANDARA network of campus networks [6]. As part of the network in MANDARA, NAIST provides three networks, the dormitory network [7], the staff accommodation network, and the guesthouse network [5]. Volunteer residents and office helpers administer these networks.

In this article we will discuss how to design and construct the authorization management system for these networks.

2. PROCESS
2.1 Why We Needed to Develop the NAS
Before deployment of the system, NAIST provided only the dormitory network in MANDARA. The dormitory network did not have an authorization management system. In other words, NAIST provided only a voluntary management method that had residents submit notices to ITC's administrator. In 2002, we encountered network abuse and we needed to strengthen the accountability and traceability process. We had to also provide network training to the residents.

2.2 Requirements
The requirements of the system included two main issues. One issue was ITC's order, which means accountability and traceability, and volunteer residents’ enlightenment activities for network usages. Another issue was low burden sharing for the system administration, because volunteer residents sometimes had insufficient experience in the system administration. We proposed the following requirements to ITC and volunteer residents:

2.2.1 Definition of requirements of the system development
2.2.1.1 Accountability and traceability
1. Registration defined as building a relation between residents' client equipment and network id (i.e., IP-address) by resident authentication.
2. A unit of control defined as a network ID.
3. The system will make observations of client equipment activation.
4. Management defined as registration, authorization control, and logging transactions of usage.

2.2.1.2 Low burden sharing for the system administration
1. The system is a simple structure for stability, robustness, and easy maintenance.

2. The system is easy to use for users and administrators.
3. The system is easily upgradeable, which means the system needs to be easy to modify the control function, the authentication logic, and the user-interface function.
4. The system is easily migrated, which means the system is low dependency on the components’ structure of data and function migration.

2.3 Development
2.3.1 Specification
We decided to use a management framework for DHCP, and a client equipment id for MAC Addresses. Access control was used as a trigger to initiate or renew that lease of DHCP; which means, we did not choose PPPoE, 802.1x, etc., because the system needed to have simple architecture for system maintenance. Also, other solutions needed expensive equipment for the development.

We choose Web-UI for registration of user interfaces, because Web-UI does not need to know resident usage. Before registration, the initial users were guided to the registration form (captive portal). Figure 1 shows the outline of the NAS.

2.3.2 Implementation
The design was aimed at simplicity and portability, because the system administrator volunteers' sometimes preferred different base systems (i.e., OS). We designed the system by shell-scripts and typical commands. We developed the system on RedHat Linux. Figure 2 to Figure 4 shows diagrams of the NAS.
2.4 Deployment
First, in October 2002, we deployed the NAS to the dormitory network. Integrators were the Second Author and the volunteer student residents. The system’s host OS was Debian GNU Linux, because, a volunteer system administrator preferred that operating system. When the system was upgraded in April 2003, the host OS was changed to FreeBSD 4.x. At that time, the reason for this upgrade also was that the volunteer system administrator preferred to use FreeBSD 4.x. Secondly, in May 2003, we deployed the NAS to the staff accommodation network with FreeBSD 4.x. Integrators were staff accommodation’s residents and student volunteers. Finally, in June 2004, we deployed a component of the Guesthouse Network Management System with FreeBSD. Integrators were the Second Author and student volunteers. The authentication method was RADIUS. In March 2005, the campus authentication infrastructure changed from NIS to MIT Kerberos V + LDAP. In March 2004, we also fitted the systems to the new authentication infrastructure.

Figure 3. Block diagrams of the Registration Sub System.

Figure 4. Block diagrams of the Accounting Sub System.

3. CHALLENGES
Sometimes, we see a problem within the system development. Before the development, the specification and system policy was ill-argued. In addition, the project was no budget for the development and deployment, and insufficient mutual
understanding for the development with ITC staff and volunteered administrators. Fortunately, we were able to purchase a new PC for the gateway in the dormitory network. At deployment, we needed to detect the faked DHCP Server (e.g., AirMac Express, Extreme), because our network switches were not able to support L2-layer management. During operation, we often had problems with the network switches, with the need to detect infected viruses or worms, and the abused P2P nodes. For about a year after the start of the operation, the staff were discussing the managements’ policy usage of the network, and discussing administrative issues. During that first year, the residents questioned the changes of the administrative policy.

4. RESULTS
Since November 2002, the NAS has successfully operated in the dormitory network.[3]. We also deployed NAS to the staff accommodation network in June 2003 and as a component of the Guesthouse Network Management System in June 2004 [2]. Figure 5 shows the dormitory network’s activity. Capability of registration is 619. Mean value of registration was 486. Mean value of residents’ utilization was 119. Figure 6 shows states of mailing-list of administration. The number of total of mail was 3231 from October 2002 to March 2005. The figure shows issues of problems for the administration and management system. Primary, we needed to discuss the management policy with the volunteer administrators and the ITC staff. During operation, sometimes we needed to modify the system for function enhancements. Fortunately, aim of design was correct, the system proofed to theses claims.

5. LESSONS LEARNED
The NAS is satisfied of the results that were achieved, since these were part of the original specifications. Perfect system developing has never been seen before [1]. In this project, we confirmed that volunteers were able to be used to assist the system administrators. We still need to learn more about self-reliance. We need to learn more about human development for system management of the association of voluntarily. Currently, we have some technical issues. Figure 6 appear clearly following:

1. We need to develop a monitoring method for the network equipments’ health in the dormitory.
2. Sometimes, we need to ‘fake’ the detection of the DHCP Server until the network switches will be upgraded.
3. We need to develop a detection method for the Virus and Worm crime hosts and abuse hosts [8].

6. REFERENCES