16. Information Network Task Group

Overview

The information network is fundamental for the research activity. The advanced NIFS campus information network named “NIFS-LAN” is the information infrastructure which contributes to the development of nuclear fusion research. NIFS has 300 staffs and the number of PCs is near 3,000. Information Network Task Group (INTG) provides 1Gbps bandwidth to users’ PC. NIFS-LAN consists of three autonomous clusters which have their own purposes and usages as follows;

1. *Research Information Cluster* (Kiban-LAN) is the network of general use, and covers the campus whole region.
2. *LHD Experiment Cluster* (LHD-LAN) is provided for LHD experiment, and covers the building relevant to LHD experiment.
3. *Large-scale Computer Simulation Research Cluster* (PS-LAN) is provided in order to support the large-scale computer simulation research efficiently.

NIFS-LAN is connected to Science Information Network 4 (SINET4) managed by National Institute of Informatics. The block diagram of NIFS-LAN is shown in Fig. 1.

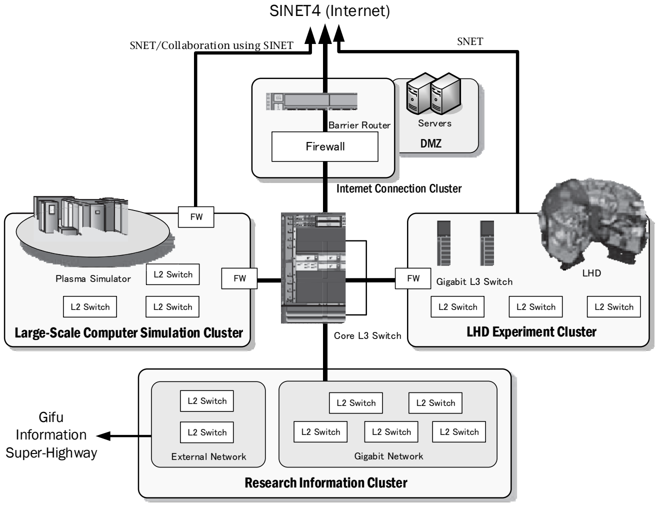

Fig.1. Block Diagram of NIFS Campus Information Network

Activities in FY2013

1) Operations and administrations of information network

a) The e-mail is a basic communication tool for the research activities. INTG has operated the mail server for NIFS to realize the effective communication. 64 new accounts (e-mail address) were created and 74 accounts were deleted and the mailing list service has also provided. 59 lists were created and 19 lists were deleted in FY 2013.

b) To manage the network, INTG has administrated the following information system;

* Routers and Layer 2 / Layer 3 switches
* Firewall
* SSL-VPN and Access Gateway server
* Mail, Mailing-list, DNS and DHCP servers

255 PCs were added to the DNS server and 89 PCs were deleted on Kiban-LAN and PS-LAN. 119 PCs were added and 92 PCs were deleted on LHD-LAN in FY 2013. INTG provided advice on information network and information systems to the staff of NIFS.

c) The TV conference system is a common tool for the remote conference. INTG has assisted 52 events which include Tokyo Event with TV conference in FY 2013.

2) Security incidents at NIFS-LAN

All of the security incidents were treated by INTG.

- The install of a malware by installing the freeware
- The install of a malware by browsing malicious web site
- Virus detection in the backup file
- E-mail which was forged to obtain user’s password
- Sending spam with SMTP-AUTH

Most virus infections cannot be prevented by the vaccine software even with latest virus definition file, because there is a wide variety of malformation virus which includes spyware and adware and the time to be change is very short. More attention is asked to prevent virus infection. The malware uses not only the flaws of the OS and the Web browser but also its plug-in software. We necessitate to pay more attentions to the update of the plug-ins.

The password is very important for using computers, especially mail server. The mail server selects whether the mail is spam or not with the account information of the sender. The user should use a strong password and should not use the same password as other system.

3) Security improvements at Kiban-LAN

To keep the high-level security, Kiban-LAN has utilized the firewall and other security equipment. The following activities had been performed to maintain the network security.

a) Owners who bring their PC from outside of NIFS-LAN are requested to make a security check before connecting PC to NIFS network. The quarantine network room was offered for such a security check and INTG assists the quarantine processing to be sane. This room was used more than 100 times in FY 2013.

b) Secure Socket Layer-Virtual Private Network (SSL-VPN) is a kind of VPN, which uses a web browser as a client's software. The SSL-VPN in the NIFS has the function to check the security level of the client before VPN connection is established. The user needs the One-Time Password token as the authentication. 22 accounts were newly created, 123 accounts were renewed, and 3 accounts were removed in FY 2013. The number of accounts for NIFS is 99 and the number of accounts for research collaborator is 43.

c) Malware protection system has been installed to detect the advanced persistent threat attacks and zero-day exploits in FY 2013. This system detects the download of a malware, such as virus, adware, spyware, Trojan horse and unwanted software, and finds the connections between PC which the malware had been installed in and central and command server.

4) Security improvements at LHD-LAN

a) LHD-LAN is requested as the highly secure network because of LHD experimentation. A PC should be checked with the staff of INTG before connecting to LHD-LAN. The staff checks whether OS and the virus definition file are recently updated or not. The status of vaccine software on users' PC are monitored during the connection to LHD-LAN. If the warning message on the monitor is found, the staff warns the user to check his/her PC. The number of PCs connected to LHD-LAN is 1261. Before the LHD experiment campaign, the security condition of every PC is checked with the criterion described above by the monitor system.

b) The Access Gateway is operated to permit the connection from Kiban-LAN to LHD-LAN. After the user authentication, Access Gateway adds the temporary access-list of the firewall for the connections from the experimenter's host to the server in LHD-LAN. 20 accounts were newly created and 19 accounts were removed in FY 2013. The number of accounts for NIFS is 107 and the number of accounts for research collaborator is 14.

5) Notable activities in FY 2013

a) Upgraded the edge and security system on Kiban-LAN

The core system on Kiban-LAN had been replaced to introduce 10 Gbps networks in FY 2012. The edge system has been installed and being connected to core system with multi 10 GbE links in FY 2013. The bandwidth for users increased to 1 Gbps because the new edge system offers 10/100/1000BASE-T ports to users. The additional ether network module has been installed to core switch to gain the redundancy.

The edge system consists of 62 L2 switches, optical fiber and UTP cables. The single mode optical fibers have been newly wired between buildings to connect distributed edge switches and the core switch with 10GBASE-LR. The UTP cable in Research Building I has been rewired with category 6 cable to ensure the connection of 1GbE.

The new quarantine system has been prepared. The security check is automatically done when the user connects a PC to information outlet and then the PC is connected to the pre-specified VLAN. MAC address registration is needed for all of PC includes fixed IP address. The guest user can connect a PC to the external network without the registration. The deploying of the new quarantine system to whole Kiban-LAN is planned next year.

Two physical servers have been added to the virtual system for network services to support new quarantine system and others.

b) Lecture for information network and its security

Five lecture classes on the subject of the campus network of NIFS, information security and how to register the MAC address were delivered in FY 2013 and 226 staffs joined. This lecture was held under "Information Security Policy" with the Information Security Committee. Only the attendance of this lecture can be the MAC address registrar, 153 members, who can register the MAC address of the PC to DHCP system in NIFS.

c) SSL Certificate distribution by UPKI initiative

University Public Key Infrastructure Initiative (UPKI initiative) operated by NII provides universities and institutes with a digital certificate free of charge. A digital certificate is mainly installed on the web server. 8 certificates were issued in FY 2013.

6) Others

- Maintained the wireless access points for the guests
- Prepared the network environment for Windows 8
- Updated the software of ISC BIND for fixing the security holes
- Reconfigured the connection for RMSAFE network, Super Conducting Magnet System Laboratory and R & D Laboratory
- Upgraded the license of LHD Access Gateway to allow more simultaneous connections.
- Installed the information outlets in the rooms of LHD control Building
- Supported the network connection of PC for Kenzai-zyuku
- Provided and supported the network infrastructure for ITC-23

(Yamamoto, T.)