# §1. Information Network Task Group

Yamamoto, T.

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 1 Gbps 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.

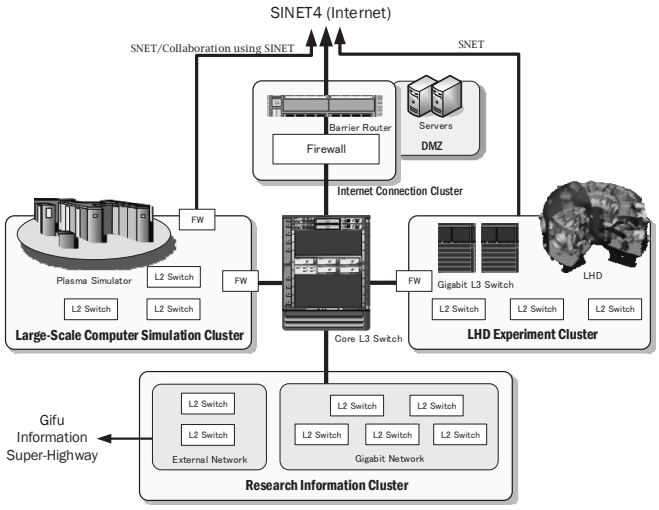


Fig.1. Block Diagram of NIFS Campus Information Network

Activities in FY2014

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. 58 new accounts (e-mail address) were created and 56 accounts were deleted and the mailing list service has also provided. 46 lists were created and 109 lists were deleted in FY 2014.

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

252 PCs were added to the DNS server and 86 PCs were deleted on Kiban-LAN and PS-LAN. 107 PCs were added and 101 PCs were deleted on LHD-LAN in FY 2014. INTG provided advices 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 7 events which include Tokyo Event with TV conference in FY 2014.

2) Security incidents at NIFS-LAN

All of the security incidents were treated by INTG.

- installs of a malware during the installation of a freeware
- installs of a malware with browsing malicious web site
- Virus detection which is in the backup file
- E-mail which was forged to obtain user's password

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 30 times in FY 2014.

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. 11 accounts were newly created, and 1 account was removed in FY 2014. The number of accounts for NIFS is 98 and the number of accounts for research collaborator is 50.

c) Malware protection system has been operated to detect the advanced persistent threat attacks and zero-day exploits. 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. 11 incidents were found in 70 notifications sent from this system in FY 2014.

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 is 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 terminals connected to LHD-LAN is 1267. 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. 35 accounts were newly created and 32 accounts were removed in FY 2014. The number of accounts for NIFS is 114 and the number of accounts for research collaborator is 5.

5) Notable activities in FY 2014

a) New security system on Kiban-LAN

The new quarantine system to whole Kiban-LAN has been started on September 2014. The news 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. About 1,600 MAC addresses are registered.

The quarantine network room was closed on December 2014 because the information outlet by their room offers the quarantine of their PC.

b) Upgraded the mail system on Kiban-LAN

The mail system has been replaced in FY 2014. The mail system is install on the virtual machine system which was installed in FY 2012. The mail system contains the antivirus service, the anti-spam service and the mailing list service. The user's mail spool size has been dramatically increased. The large attached file, more than 10 MB, is automatically replaced to a web link. The receiver can download the sender's file with the link.

The deploying of more secure login method is planned next year.

c) Lecture for information network and its security

Three lecture classes on the subject of the campus network of NIFS, information security and how to register the MAC address were delivered in FY 2014 and all of 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, about 370 members, who can register the MAC address of the PC to DHCP system in NIFS.

d) 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. 19 certificates were issued in FY 2014.

6) Others

- Replaced the edge switches in the guest house
- Updated the software of ISC BIND for fixing the security holes
- Closing the use of legacy OS, such as Windows XP
- Prepared the network environment for Mac OS X 10.10
- Maintained the wireless access points for the guests
- Surveyed the connectivity of the wireless access in LHD Lab. during the experimental campaign in FY 2014.
- Configured a route of L2VPN for thin clients of SOKENDAI
- Supported the network connection of PC for Kenzai-zyuku
- Provided and supported the network infrastructure for ITC-24