Network Security in SPring-8

The network system is one of the most important infrastructures that enable the continuous operation of SPring-8. Not only SPring-8 staff but also many experimental users from outside access various network services provided by SPring-8. A secure network system contributes to the stable operation of SPring-8. We will discuss the outline of the SPring-8 network system in this text.

The SPring-8 network system consists of three network zones: a public network for office work, a beamline user network and a control network. Figure 1 shows an overview of the network system of SPring-8. The public network provides services such as mail servers, web servers and a wireless network system. We constructed the wireless network and the guesthouse network under an authentication system. When users access the wireless or guesthouse network, only authorized users can access the public network and the Internet through the authentication system. We have several access policies for each access point. For instance, the access from the guesthouse to unauthorized network resources is restricted. To maintain the security of the access points, we have recently installed a wireless network-monitoring tool, using which we can detect network abuse such as rogue access points.

The beamline user network was constructed for users' experiments. Various experimental control and data acquisition systems are operated on the network. As shown in Fig. 2, the beamline user network is isolated from external networks such as the Internet and the public network by using NAT (network address translation). We introduced VLAN (virtual local area network) technology to build a logically independent and flexible network system. The access from one VLAN to other VLANs is restricted by IP filtering through a core switch. Additionally, by introducing an IPS (intrusion protection system) we can remove network threats that are caused by computer worms. When the IPS detects malicious activity, it prevents the spread of worms by dropping or rejecting the unauthorized connection.

The control network is used for the operation of accelerators and beamlines. The network is strictly protected because its importance to SPring-8 by a firewall system. However, if a recovery procedure from outside SPring-8 is needed in the case of machine trouble, we must access the control network

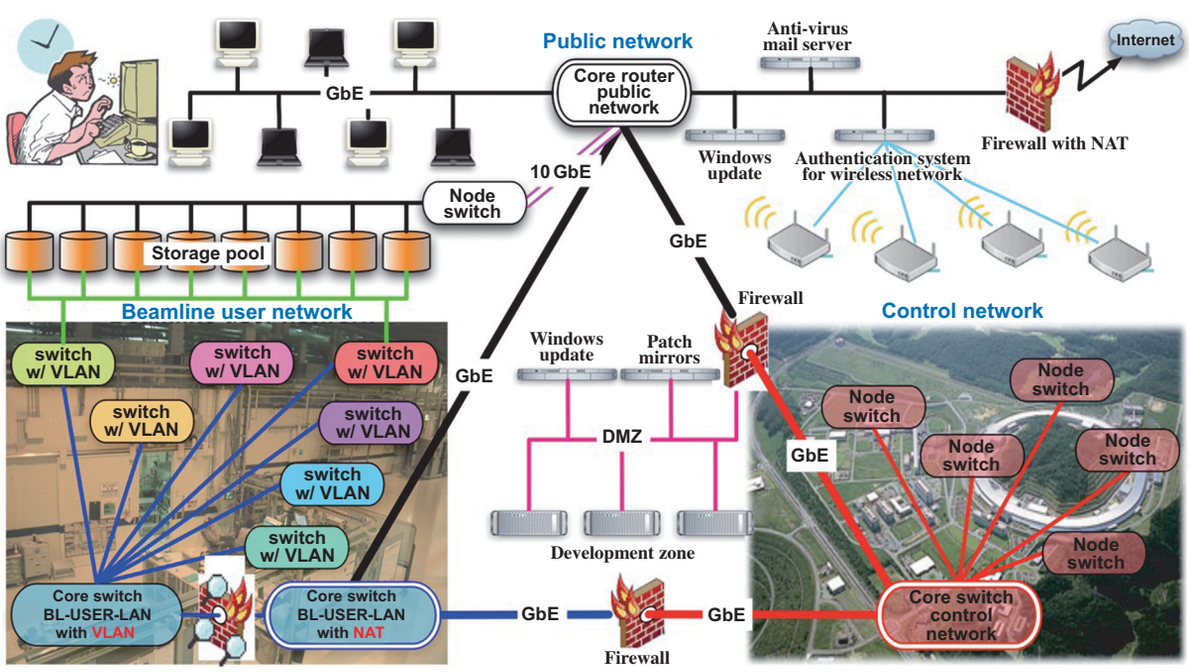

Fig. 1. Schematic view of the SPring-8 network system. The network is divided into three networks: a public network, a beamline user network and a control network.

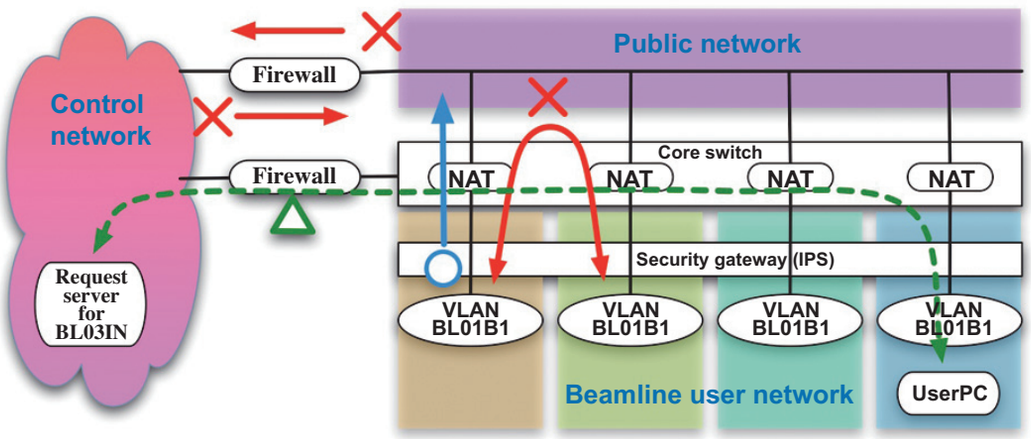

Fig. 2. Beamline user network isolated by using NAT and VLAN. The IPS prevents computer worms from spreading.

from outside. Thus, we constructed a remote maintenance mechanism, WARCS (wide area remote control system), which is able to access the higher-security control network. Figure 3 shows an overview of WARCS. WARCS comes under the scrutiny of the shift leader of the SPring-8 operators. WARCS is implemented by a network tunneling application, Zebedee, to bypass the firewalls system. The shift leader can control and monitor the access of WARCS. For a security reasons a one-time password is used to access the control network. By introducing WARCS we have acquired a safe remote maintenance scheme. The ability to conduct remote beamline experiments will be advanced on the basis of the technology of WARCS.

Network technology has progressed rapidly in recent years, during which many security threats have developed then been fixed, which has created a vicious circle of network development. It is difficult to achieve a good balance between security and user friendliness. At SPring-8, we are maintaining a secure network by conducting advanced research on network technology.

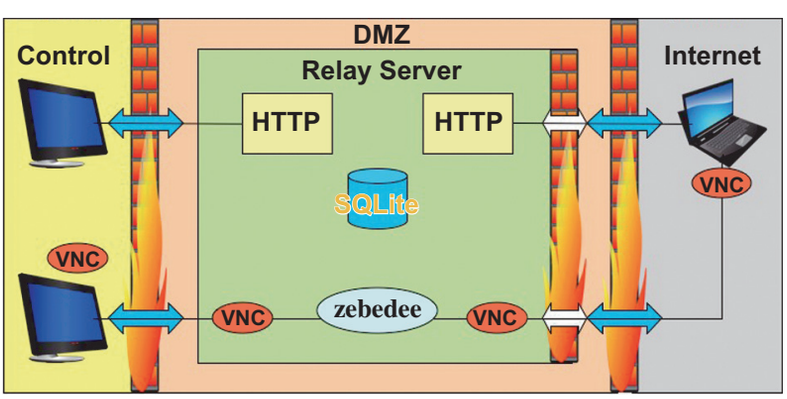

Fig. 3. Overview of WARCS, which realizes safe remote access by using the network tunneling technique.

Toru Ohata* and Miho Ishii

SPring-8 / JASRI

*E-mail: ohata@spring8.or.jp