Architecture of Data Network for the Tokyo 2020 Games

KUROMIYA Takayuki

Abstract

In the Olympic and Paralympic Games, it is essential to establish a highly reliable data network for the stakeholders to realize the safe and secure operation of the Games. In the Olympic and Paralympic Games Tokyo 2020, we revised the configuration of the past Games and constructed three logical networks divided by users and applications. This article summarizes the concepts and implementation methods for ensuring the efficiency, reliability, flexibility, and scalability of the data network for the Games, taking into account the service characteristics that are particular to the Games. The article also examines key architectural points for the Olympic and Paralympic Games Tokyo 2020.

Keywords：Data Centre, WAN, LAN, Security, Remote Access VPN, Wi-Fi

1. Introduction

When the Organising Committee developed the data network that would serve as the operational infrastructure for the Olympic and Paralympic Games Tokyo 2020 (Tokyo 2020 Games), it was required not only to provide robust and stable services that would not interfere with Games operations but also to keep up with the highly uncertain Games planning and stakeholder usage requirements until just before the actual event. Following these subjects, the basic policy was to ensure that construction and operation costs are appropriate (efficiency), availability and security are assured (reliability), and changes can be made flexibly (flexibility and scalability). The system was architected and built-in cooperation with the NTT Group, the telecom service partner of the Games.

First, from the standpoint of efficiency, the system was designed to be superimposed on a single large-scale network which is highly reliable, rather than providing independent networks separately for each of the various systems and services involved in Games operations. It was also assumed that the requirements of the many stakeholders using the network would continue to be added and changed until just before the Games, so we paid attention to the flexibility and scalability of the network to absorb these changes in requirements.

On the other hand, because of its large scale, the basic design had to be completed more than two years before the Games, taking into account the lead time required for its verification and construction. The basic design of the data network for the Games was completed in April 2018 actually, but the requirements had not been completed at that time and the assumed parameters were calculated based on information mainly from past Games.

This article introduces the architecture of the data network for the Games built on these backgrounds from both physical and logical perspectives.

2. Physical Network

2.1 Overall Configuration of the Infrastructure

In consideration of efficiency through improved operability and standardized security policies, external

KUROMIYA Takayuki
Technology Services Bureau, The Tokyo Organising Committee of the Olympic and Paralympic Games

The Journal of The Institute of Electronics, Information and Communication Engineers, Vol.105, No.8, Supplement, pp.22-31, August 2022

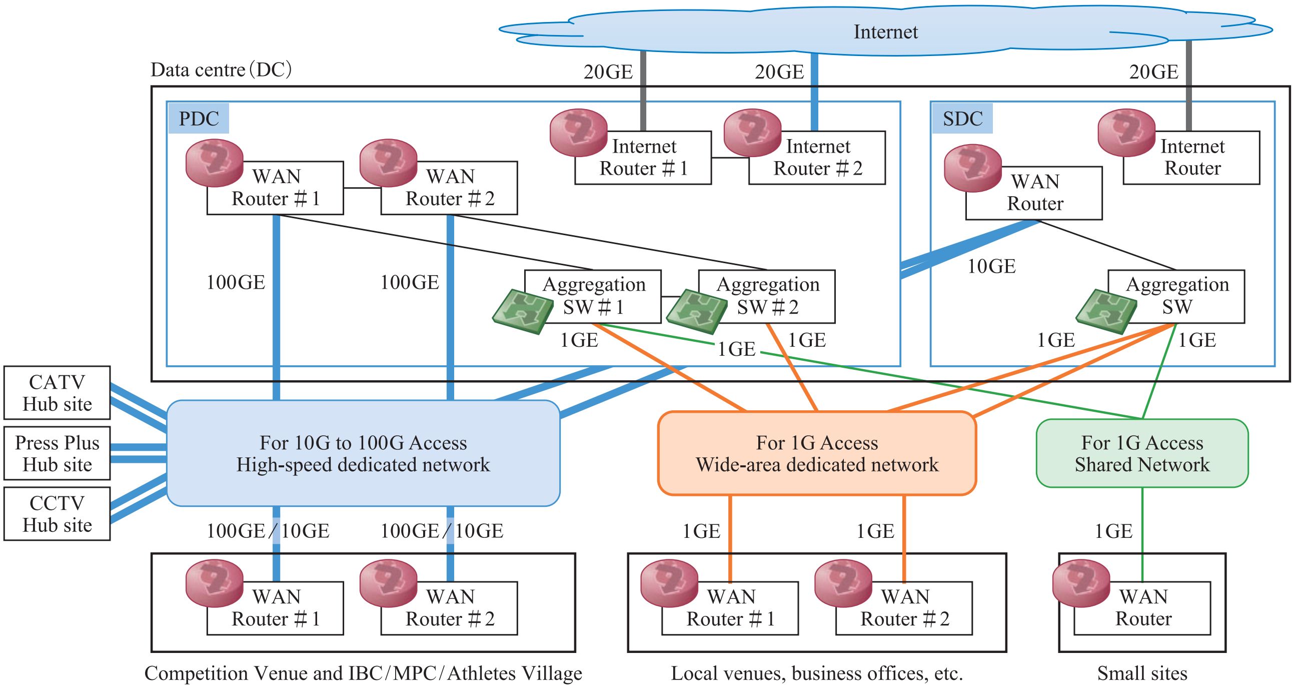

Figure 1 Overview of the Core Configuration of the Data Network for the Games A star topology to connect the venues and the Internet via DC (with exceptions).

communications such as Internet connections were routed through Data Centres (DC) in principle. As a result, the server system was centralized in the DC which was a hub to connect the various venues with a star topology.

The DCs themselves were also made redundant, with a Primary Data Centre (PDC) in Tokyo and a Secondary Data Centre (SDC) in Saitama to ensure the reliability of the entire data network for the Games.

The backbone had sufficient capacity with a bandwidth of 100 Gbit/s, and we adopted a 20 Gbit/s Internet access service that was expandable to make it flexible and scalable enough to absorb a variety of user requirements (Figure 1).

However, some telecom services on this communication network such as CATV (video distribution), Press Plus (photo data transmission), and CCTV (security surveillance cameras), required a large amount of communication data with specific venues other than the DC. If that traffic was to go through the DC, further WAN access line bandwidth and consequent higher performance equipment (i.e., additional modules) shall be required at the DC. Therefore, these telecom services were exceptionally designed in a star topology with a specific venue as a hub for each service to reduce equipment costs.

■ Terminology

Dark fiber Optical fibers laid by telecommunications carriers and leased in fiber units. The user (borrower) is responsible for maintenance and management such as fault detection.

MPLS Multi-Protocol Label Switching. A technology that adds labels to packets to achieve high-speed transmission over a network without referring to IP headers.

IDS/IPS Custom Signatures Intrusion Detection System/Intrusion Prevention System : A system that creates its signatures to provide accuracy, speed, and coverage for attacks that cannot be detected or prevented by security vendors' signatures.

UTM Unified Threat Management. Unified Threat Management, integrates and manages multiple security countermeasures to protect the network from various threats in web access and e-mail.

2.2 Data Centre Configuration

The data centre (DC) had to integrate communications from all venues and to provide connectivity to the outside of the Games network. DC was one of the essential components for providing basic network services (L2 authentication, DHCP, DNS, etc.) to each venue, requiring a robust and flexible design.

As described in section 2.1, PDC and SDC were established as a disaster countermeasure, but the functions accommodated would not be divided up

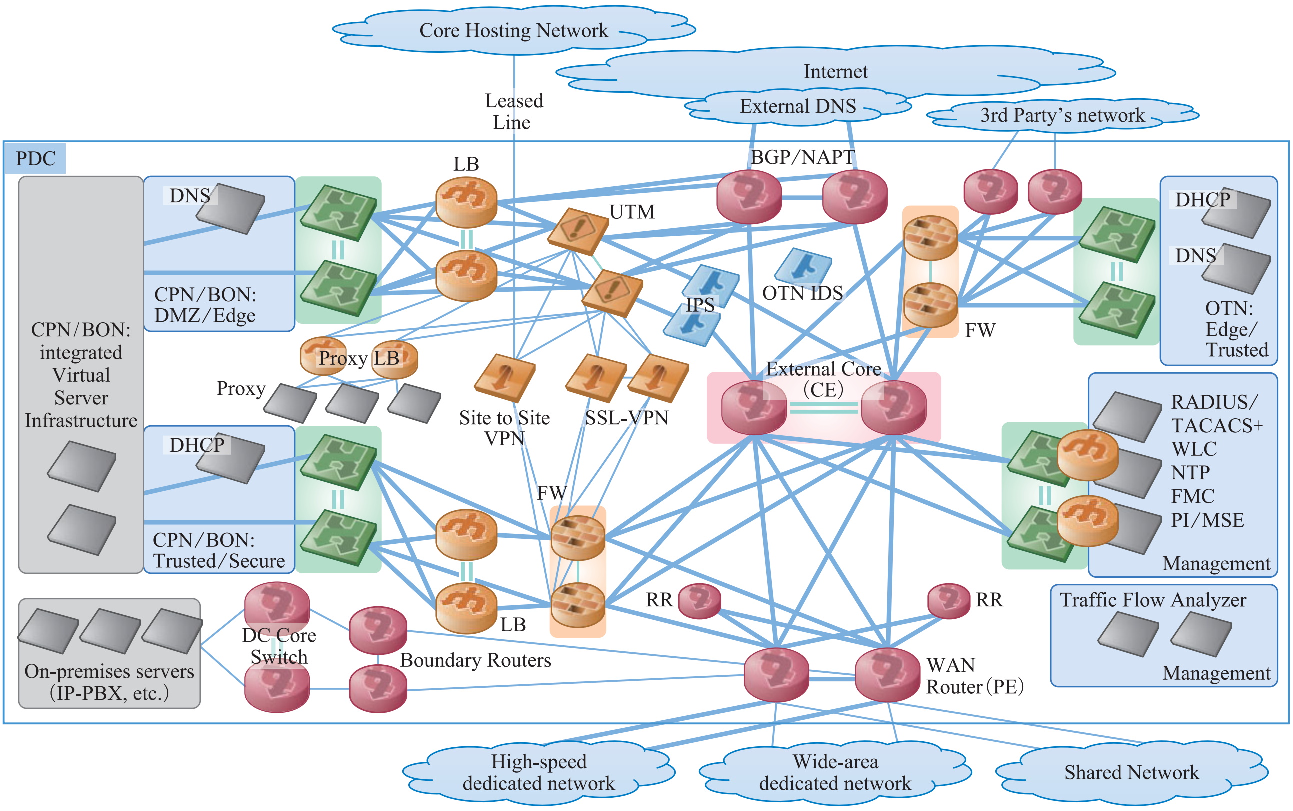

Figure 2 PDC Configuration with All Equipment Redundant To assure stable operation of the PDC independently, the enclosures and power supplies of all devices in the PDC are redundant to ensure reliability. (The SDC is omitted in this figure.)

between the two DCs and the PDC shall be operated independently under normal circumstances. For this reason, all equipment in the PDC should be redundant, and even within the equipment, all line cards, interfaces, and power supplies were redundant to ensure reliability (Figure 2). We decided that redundancy within the SDC would not be required for cost-effectiveness. At the Games time, 45 racks for the PDC and 20 for the SDC were working.

2.3 Wide Area Network (WAN) between Venues

In the past Games, WAN was sometimes built up from scratch laying dark fiber (Terminology) to connect the venues. For the Tokyo 2020 Games, however, high-quality and highly reliable network services provided by NTT East and West were available, and from the perspective of construction and operation costs, we combined three types of commercial line service ranging from 1 to 100 Gbit/s to connect between venues and DCs.

For the connection to each venue, the bandwidth was estimated according to the size and role of the venue based on the past Games experience, and we used different access line services considering whether the redundancy and CPN (see 3.1 (1) Competition Network) existed in the venue were mandatory or not (Table 1). IBC and MPC of the "main venues" in Table 1 refer to International Broadcast Centre and Main Press Centre respectively. The venue patterns are described in section 2.4.

Especially, at important venues such as competition venues, there were not only two WAN lines installed but also redundancy was thoroughly implemented at all access sections, NTT receiving stations, relay sections, and receiving equipment to ensure network reliability. Figure 3 shows an overview of the configuration of Pattern 1 (large-scale venues such as IBC and MPC) as an example.

In the case the distance between two venues was sufficiently close and they could share the network devices at the venues, we defined it as a "precinct venue" and integrated WAN access lines and extended LAN for greater efficiency. In some venues that had existing Internet access available, we used VPN technology to connect to the PDC by using those facilities without installing an exclusive data network for the Games.

We adopted MPLS (Terminology) in the backbone of the

Table 1　WAN Circuits and Major Venue Patterns

Pattern	Access Line Bandwidth	WAN Redundancy	CPN	Number of Venues	Major venues
Data network for the Games (connected to DC)					
1	100 Gbit/s	Yes, different stations	Yes	3	IBC, MPC
2	10 Gbit/s	Yes, different stations	Yes	34	Competition Venue
3	10 Gbit/s	Yes, same station	No	3	IOC Hotel
4	1 Gbit/s	Yes, different stations	Yes	4	Local Qualifying Venue
5	1 Gbit/s	Yes, same station	No	4	Office
6	1 Gbit/s	No	None	6	Bus depot
Internet					
7	1 Gbit/s	—	—	28	Vehicle waiting area
8	Use existing facilities at the venue			15	General hotel

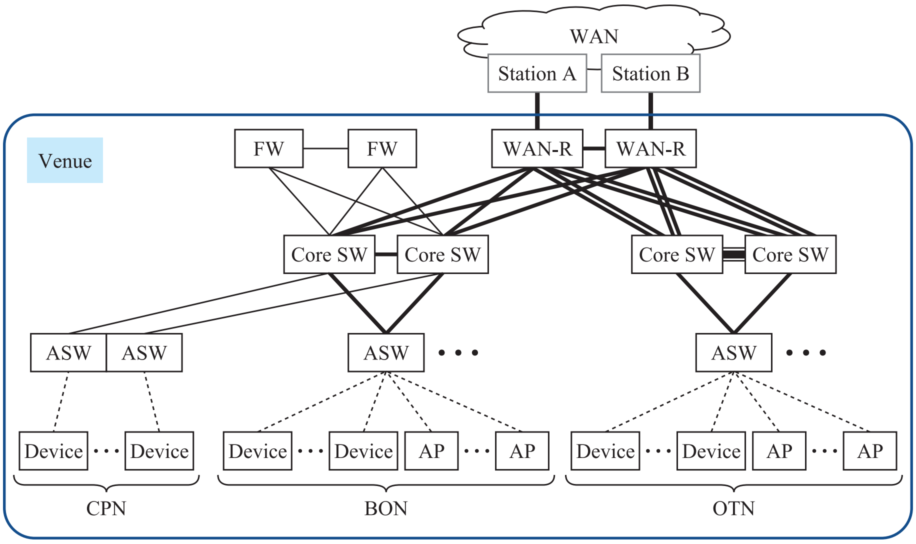

Figure 3　Brief Overview of the Pattern 1 Venue　Important venues such as the Competition Venue ensured reliability by making all WAN/LAN components redundant.

WAN between the DC and the venues referring to its operational experience and scalability in past Games. The WAN routers at each venue worked as MPLS-VPN provider edges and used OSPF routing. Priority control was applied to the backbone, while bandwidth control was not applied to the access section, providing a circuit with sufficient bandwidth.

2.4　Venue Patterning

Connectivity to the event data network was required not only at competition venues, but also at non-competition venues such as operation centres, training venues, and facility sites, which were a mixture of large and small venues.

However, in an environment such as the Olympic and Paralympic Games where multiple competitions are held simultaneously, the key point is to standardize the design and operation, aiming for total optimization rather than individual optimization for each venue. Based on this concept, as shown in Table 1, we created several venue patterns, selected device models for each pattern, and utilized them as a reference design to minimize the number of exceptional cases.

The effectiveness of this patterning and standardization was developed as the Games approached. Even when a change for the network configuration in one venue was required due to a sudden additional requirement from stakeholders just before the Games, we did not need too much time for re-design because we should only expand the network to the other venue that had a similar pattern. At the same time, necessary equipment could be quickly deployed by converting spare equipment from other nearby venues.

The Technology Operation Centre (TOC), which centrally managed trouble handling during the Games time, needed to know the configuration of each venue and its status in real-time, and this patterning enabled prompt and accurate restoration measures to be taken in cooperation between the TOC and venues when trouble occurred.

2.5 Construction of LAN within the Venue

Since many of the Tokyo 2020 venues used existing buildings and facilities, we were required to carry out the network installation after installing temporary facilities (power supply, fixtures, etc.) at each venue, resulting in a short construction period of one to two months. In particular, the large venue such as MPC, where the actual length of tenancy was very limited, we had to meet the tight time constraints by using free time on weekends and late at night to install cables little by little in the backyard that could not be seen about six months before the Games.

In addition, if we were required some changes in service requirements or additional cabling after the start of use, there would be limited time to implement them before the Games. Therefore, in consideration of availability, scalability, and operability, a standard configuration was adopted as much as possible in the LAN as well as the pattern of the venue.

Table 2 shows the total amount of equipment and materials installed in the LAN construction for all venues, including the Athletes Village as the representative of large venues, and the National Stadium which was the largest venue among the competition venues.

To construct these facilities in a short period and at multiple geographically separated venues simultaneously, a total of approximately 2,000 workers worked day and night until the last minute before the Games, and as a result, no venues experienced schedule delays in installation.

Table 2 Amount of Equipment and Cables Installed

	Total of all venues	Athletes Village	National Stadium
Racks	1,400	106	92
Routers	150	2	2
Firewalls	150	2	2
L3 Switches	500	14	4
L2 Switches	7,000	814	373
Wi-Fi AP	11,100	5,080	270
ptical fiber	1,400 km	46 km	134 km
UTP cable	4,450 km	233 km	460 km

3. Logical Network

3.1 Logical Partitioning of the Games Data Network

After discussions with Atos, the integrator, we defined the data network for the Tokyo 2020 Games as consisting of the following three logical networks.

(1) Competition Network (CPN)

This network is necessary for using the systems required for operating the Games and the competition. High availability and reliability are of utmost importance, and logical isolation from other networks and the Internet is mandatory. Atos determined the communication requirements and security measures, and NTT installed and operated the network based on these requirements.

(2) Back Office Network (BON)

This is an office network for Tokyo 2020 Organising Committee staff to use business applications, Internet access, printers, etc., to carry out their work. As the number of staff members continued to increase toward the Games, the BON needed to be flexible enough to expand its capacity accordingly. Many servers providing business applications were installed, and the communication requirements between servers and clients were implemented by the "Allowlist" method. The system also had a multi-layered security defense system, including endpoints, to reduce and avoid various security risks.

(3) Olympic Technology Network (OTN)

The OTN is a network that serves as the infrastructure for accommodating various telecommunication services and systems provided by each FA (Functional Area, the organising committee's internal event management function) for stakeholders other than spectators. Since the number of users is large and various usage patterns are possible, the configuration should be kept as simple as possible. And as the systems using this OTN are implemented individually, they are grouped and logically divided by VRF (Virtual Routing and Forwarding) to assure the independence of each system.

3.2 Zone Design and Inter-zone Communication

Based on the security policy of the Tokyo 2020 Games, the CPN/BON/OTN were each segmented into eight zones (Table 3), and inter-zone communication was strictly managed by the Allowlist as shown in Table 4. In the OTN, we integrated some zones (Shared and Unmanaged) in consideration of the characteristics of the services provided and redefined separately for the Shared Internet and the Dedicated Internet.

3.3 Security Measures

The Olympic and Paralympic Games are particularly vulnerable to cyber-attacks, and it was a massive challenge how to protect against cyber-attacks. Therefore, as shown in Table 5, security threats and their countermeasures were studied and designed, and we adopted a suitable solution for each. In particular, we paid attention to avoid the reputational risks of the attackers, like leakage of sensitive information, attacks on external networks, and attacks from the inside based on what is now known as a zero-trust concept.

Table 3 Security Zones Definition

Zone	Definition
DMZ	An external zone, for assets being exposed to zones hosting 3rd party devices.
Edge	An external zone, for assets requiring outbound connectivity to 3rd party devices.
Trusted	The "default" trusted zone, most assets used internally in the network are in this zone.
Secure	The most secure and isolated zone, reserved for sensitive data storage.
Managed	The zone including all assets which owned by and operated by Organising Committee staff or assimilated.
Shared	The zone including all assets which owned by Organising Committee, connected to ODN (including through a VPN, see 2.3.6), but not operated by Organising Committee and instead used by 3rd parties.
Unmanaged	The zone including all unmanaged (i.e. 3rd party owned) end-user devices.
Untrusted	All other assets and 3rd party network, including Internet.

All telecommunications equipment had been fortified with unified hardening using the Organising Committee's Configuration Standard and took countermeasures at Layer 2 and Layer 3 against malicious attacks.

The communication control was implemented based on the inter-zone communication flow described in 3.2 by the Allowlist, which permitted only the minimum necessary communication. As a result, this list totaled 400,000 lines.

The management and operation of this list were significantly complicated, but we coped with this by devising process management and auditing methods. For details, please refer to 2-3 of this special issue.

The security measures taken for each logical network are summarized below.

(1) Security Measures for CPN/BON

We implemented a multi-layered defense in the network with multiple security measures including the DNS layer, application layer, and endpoints to counter targeted attacks. In addition, we conducted a correlation analysis of security information and event management logs and implemented a detection function using flow information for Layer 2 repetitive malicious communications between terminals to improve the detection capability of security threats. In the BON used by the organising committee staff, a proxy was installed to SSL traffic decryption to the Internet, providing audit function by URL filtering, anti-virus, and Sandbox. NTT had implemented a mechanism to create and apply its IDS/IPS custom signatures(Terminology), for threats that could not be detected by the standard functions of security equipment, thereby enhancing detection and

Table 4 Security Zones Flow Design Allowable/unallowable intercommunication between the segregated zones is defined, where "Yes" is allowed, "No" is not allowed, and "Avoid" indicates that IT services should be designed not to require using the related traffic flow.

↗	Secure	Trusted	DMZ	Edge	Managed	Shared	Unmanaged	Untrusted
Secure	Yes	Yes	Avoid	Avoid	No	No	No	No
Trusted	Yes	Yes	Yes	Yes	Yes	No	No	No
DMZ	No	Yes	Yes	Avoid	Avoid	Avoid	Avoid	Avoid
Edge	No	Yes	Avoid	Yes	Yes	Yes	Yes	Yes
Managed	No	Yes	Yes	Yes	Avoid	No	No	Yes
Shared	No	No	Yes	No	No	Avoid	Yes	Yes
Unmanaged	No	No	Yes	No	No	No	Avoid	Yes
Untrusted	No	No	Yes	No	No	No	No	N/A

Table 5　Security Threats to Be Considered and Countermeasures

Security Threats	Examples of Cyber Attack	Security Countermeasures			
		Use of cloud/ISP services	Security features to be deployed on the network	Considerations for Network Design	Considerations for Network Operation
Hijacking of user privileges, etc.	・Attacks exploiting vulnerabilities Acquisition of authorization/authentication information through malware infection	・Cloud-based DNS communication control	・ACL ・URL filter ・IPS/IDS (including custom signatures) ・Anti-virus, Sandbox ・SSL decryption, AD authentication	・NAPT/NAT, uRPF ・Zone design, IP address design ・Logical network segregation by VRF/VLAN ・Communication control within the same VLAN and between VLANs ・Server fortification, Data encryption	・SIEM, security operations ・ID/password management ・Visualization of communication inside the data network ・Vulnerability management of servers/network devices ・Flow information analysis (Security detection)
	・Spoofing	—	—	・Network log tracking environment (Syslog, internal DNS, NTP, FW, etc.) ・Terminal authentication, user authentication ・DHCP, AD	・SIEM, security operations ・Two-factor authentication for remote access ・ID/password management
Information theft	・External communication of stolen information after malware infection	・Cloud-based DNS communication control	・ACL ・URL Filter ・IPS/IDS ・SSL decryption, AD authentication	—	・SIEM, security operation ・Flow information analysis (security detection)
	・Sniffing packet by man-in-the-middle attacks, etc.	—	—	・Wireless LAN countermeasures (countermeasures against rogue APs) ・Encryption of remote access communication for maintenance	—
All Internet connectivity disconnected or delayed	・DoS attacks exploiting vulnerabilities	—	・IPS/IDS	—	・Vulnerability management of server/network equipment
	・DDoS attacks	・DDoS countermeasures by ISP	・IPS	—	・ACL deployed when mitigation bandwidth is exceeded
	・Bandwidth shortage on WAN circuit at venues	—	—	・Logical network segregation by VRF/VLAN ・Communication control within the same VLAN and between VLANs ・Rate Limit/QoS deployment	・Flow information analysis (Visualization of communication inside the data network)
	・BGP route hijacking	—	—	—	・Operation handling by ISP (specific contract)
	・Attacks on external DNS	・Cloud migration of authoritative name server ・Cloud migration of cache DNS	—	—	・Handling by authoritative name server provider ・Handling by cache DNS provider

protection capabilities.

(2)　Security Measures in OTN

The OTN had a wide variety of applications, and it was necessary to select security measures to be implemented to ensure the availability of the service. In addition to network access restrictions, blocking malicious communications by DNS and security detection using flow information were introduced among the measures applied in the BON. It enabled the avoidance

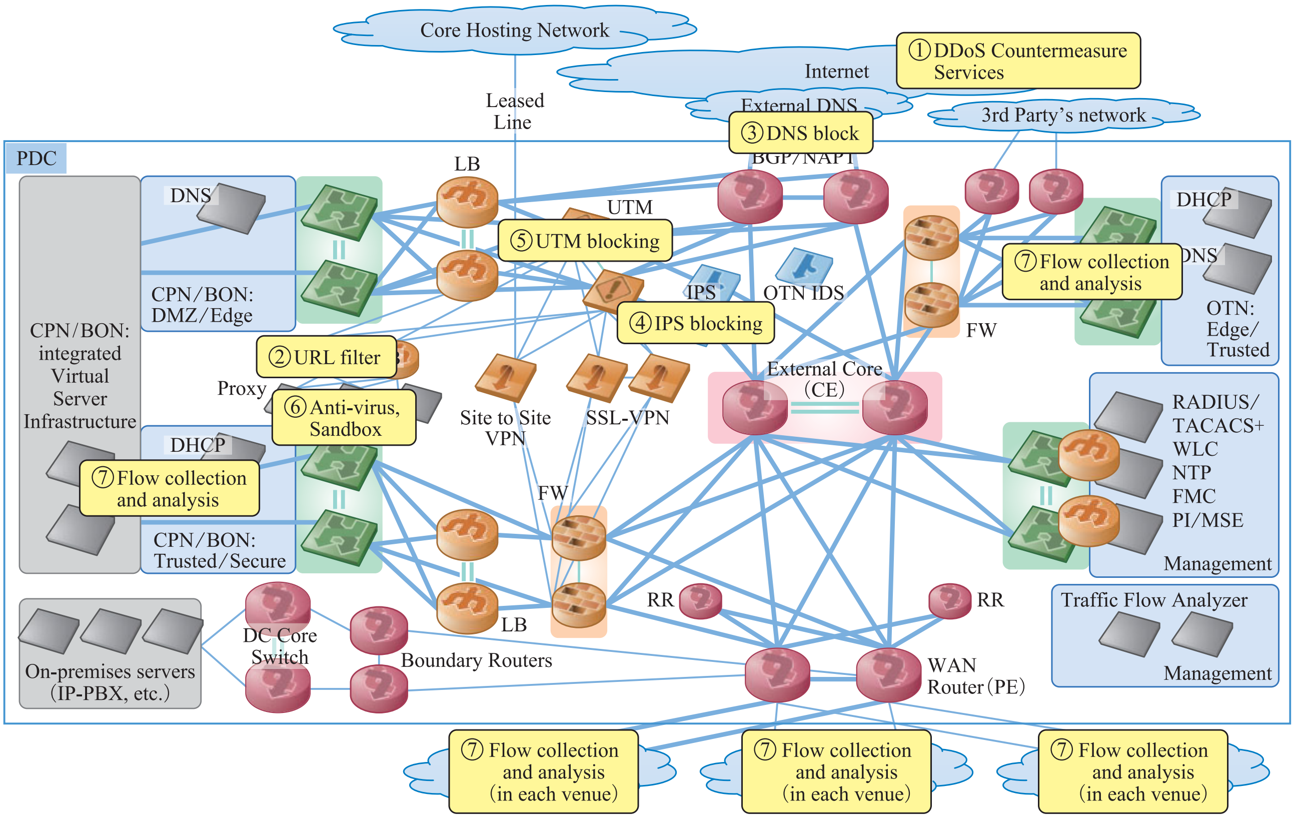

Figure 4　Deployment of Security Solutions　Multiple security solutions deployed in a multi-layer, and necessary blocking configuration put in each time by analyzing detected security events.

of attacks from OTN-connected terminals to external networks and the detection of malicious communications to internal servers and the Internet.

In implementing each solution, as shown in Figure 4 ① to ⑦, we adopted a multilayer defense and multi-vendor approach and selected products from different manufacturers for multiple layers against DDoS attacks, DoS attacks, targeted attacks, and so on. In operation, the firewalls and UTM(Terminology) devices at the entrance and exit of each network detected some security events, and we analyzed flow information collected at multiple points to minimize security risks by applying blocking configuration as Denylist to unauthorized flows.

These security measures through strict communication requirement management, visualization, and careful auditing were the cornerstones of a robust data network for the Games.

3.4　Management Network

We implemented the "management network" to efficiently perform a series of operation and maintenance tasks, such as prompt issue detection and restoration by monitoring the normality of its components so that we promptly coped with all incidents on the Games data network.

We must perform these tasks continuously without depending on the failure of a specific function of the Games data network. Considering cyber security attacks, which were assumed to be the greatest threat, the main components of the management network were closed with physically independent. Furthermore, since it is a significantly important network because it reaches all communication devices in the Games network, it has implemented the same level of security measures as the main body of the Games data network in terms of Allowlist control, log monitoring, endpoint management, and internal control. As a result, we could perform remote configuration changes of communication devices, and verification of the settings when responding to user requirements at the venue securely and smoothly by network monitoring from the TOC.

In addition, although not used during the whole Games time, we also prepared a backup network to ensure that the event of a failure of the management network itself would not disrupt the operation and maintenance work.

3.5 Wireless LAN (Wi-Fi)

Wireless LANs (Wi-Fi) are in greater demand than wired LANs, and the provision of an adequate Wi-Fi environment for all parties involved was considered essential for the success of the Tokyo 2020 Games.

We installed a Wireless LAN Controller (WLC) in the DC for integrated management of all Wi-Fi access points (APs), and scalability in channel design when additional APs were needed.

Because of the wireless nature of the Wi-Fi network, there was much concern about its availability and performance, so we introduced an integrated management system that could detect rogue APs and check signal strength and heat maps.

However, since the Wi-Fi in the Athletes Village was predominantly used by athletes to connect only to the Internet, we incorporated the Wi-Fi service for small offices provided by NTT as part of the OTN, rather than central management by the WLC. This enabled the reduction of equipment costs for APs (as shown in Table 2, the Athletes Village alone accounted for more than 40% of the total number of APs at all venues).

In some cases, a higher-than-expected number of Wi-Fi terminals were connected simultaneously in some venues, resulting in deficient performance and connection difficulties, which we manually adjusted and resolved eventually. Please refer to 2-4 of this special issue for more details.

Wi-Fi technology is advancing rapidly. We had to re-examine the product version in cases where the connection method assumed in the design phase did not match the specifications of the latest terminals brought in at the venue and we could not absorb it by any configuration changes. Even for a temporary established network for an event, it is critical to keep up with new technologies when the operation period gets longer.

3.6 Remote Access VPN

In the organising committee, which was rapidly expanding in preparation for the Games, we introduced a remote access VPN so that staff members could connect to the BON for their work even when they were out of the office. Terminal authentication was mandatory to connect to the BON, and L2 authentication was required for the data network for the Games in offices and venues, while remote access VPN authentication from outside the office.

Due to operational cost and construction period constraints, we planned not to install an official data network for the Games at each venue until just before the Games (April-May 2021). And implementation of remote access to the BON was necessary to conduct preparatory work at each venue for test events, which were to be held in the summer of 2019.

For the security level enhancement, this remote access VPN system required multi-factor authentication combining SSL certificates, passwords, and phone notifications to mobile terminals when connecting, as well as quarantine based on how the OS patch, antivirus software, and pattern file were applied in the PC. The system also performed quarantine based on the OS patch application, antivirus software activation, and the pattern file, and disconnects the VPN or updates the client terminal if necessary. In addition, the personal firewall function installed on the terminals applied appropriate policies, and we implemented an Always-on feature to force remote access when we ran the PC outside the office.

In this way, we had implemented a flexible and secure remote access VPN as of the summer of 2019, when preparation activities for the Games were in full swing at each venue. As the number of teleworkers at home surged in 2020 with the spread of the COVID-19 infection, this remote access service unintendedly became the most critical to help us survive the unprecedented postponement of the Games by a year.

Due to the declaration of a state of emergency in April 2020, nearly all of the approximately 3,500 staff members were connected simultaneously (Figure 5) from their homes, while we initially expected the maximum number of simultaneous connections to be

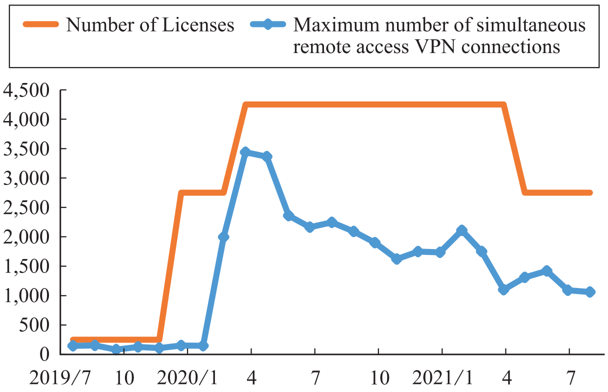

Figure 5 Maximum Number of Simultaneous Remote Access VPN Connections The figures plotted for the day with the largest number of simultaneous connections in each month. In April 2020, almost all staff were to use remote access, so additional licenses were procured quickly to accommodate this change.

around 2,500. We quickly established a telework environment for the staff by procuring additional licenses and making capacity design changes including revising the split tunneling target to improve performance. Please refer to 2-6 and 2-9 of this special issue for details.

4. Summary/Conclusion

The most important aspect of the data network developed for the Tokyo 2020 Games was to ensure reliability through stable operation while considering efficiency. For this reason, we did not deliver the latest technologies basically but were very conscious of implementing technologies with practical experience. In addition, since various parties from around the world brought in a wide variety of terminals, the architecture itself had to be flexible enough to meet their requirements, and the engineers operating it had to be able to respond quickly and reliably.

However, when the postponement of the Games came out, we suddenly had to figure out the massive issue of how we should keep the data network for the Games that had already started the operations toward the summer of 2020 for one more year. We evaluated and analyzed various risks which equipment and services becoming obsolete and cyber-attacks being higher developed, and implemented appropriate countermeasures after considering its cost and lead time. As a result, we could keep operating the data network for the Games without any problems until 2021, which contributed to the success of the Games.

If the Games had been scheduled for 2021 from the beginning, it could be possible that the Games data network would have been designed and implemented with a different architecture. However, the postponement of the Games by one year did not result in fatal flaws or significant design revisions, and the network was able to operate stably with the same architecture as initially designed until after the postponement. It was only thanks to many engineers of the telecommunication service and equipment partners of the Tokyo 2020 Games, who contributed their expertise and knowledge to design and deploy the network considering the flexibility and easy operations.

The IOC initially warned us that “the Olympics is NOT a technology showcase,” and the data network for the Games and its design engineers, who would play a fundamental role in the Games, had faithfully adhered to that warning and provided the infrastructure to support the Games. They had been working steadily and invisibly.

Please refer to 2-6 of this special issue for the actual operations and performance of the data network during the Tokyo 2020 Games time.

(Received February 28, 2022 ; Revised March 15, 2022)

KUROMIYA Takayuki

Mr. Kuromiya received his M.S. in Information Science and Technology from Tohoku University in 1998 and joined Nippon Telegraph and Telephone Corporation (NTT) in the same year. Since then, he has been engaged mainly in the implementation and operation of a dedicated global network for manufacturing enterprises. In January 2015, he was seconded to the Tokyo 2020 Organising Committee as the Director of Telecom Business Promotion, Technology Services Bureau.