Terminology

A list of terms used in the five chapters of this special issue (5-1 to 5-9) and their explanations.

Technology Operation Centre An organization that remotely monitors, controls, and troubleshoots all technologies, including convention-related systems. It includes the Security Operations Centre.

Security Operation Centre An organization that detects, analyzes, and responds to cyber attacks and develops countermeasures to stop them. The structure and operational design varies depending on the organization, and please refer to each featured article for definitions in the Tokyo 2020 Games.

AD (Active Directory) A system developed by Microsoft to centrally manage user accounts and other information. In addition to on-premise type, cloud type services are also available in recent years.

Azure AD It is a type of centralized management system for user accounts and other information developed by Microsoft which is provided in the cloud.

Password Spraying Attack A type of attack in which login attempts are repeatedly made with different IDs and passwords to find a valid combination. To avoid detection, the process is carried out slowly, changing the ID and the IP from which the connection is made.

UTM (Unified Threat Management) A solution that integrates various functions such as firewalls, IPS/IDS, and security measures for the Web and e-mail. Since some applications require too much functionality, the Tokyo 2020 Organising Committee uses single-function solutions in combination with them.

Open Resolver A device that is configured to respond to DNS inquiries from the Internet. If the function is abused, there is a risk of being involved in cyber attacks.

Rule Based Filter A function that checks the contents of traffic and detects suspicious session based on a set of rules that determine whether they correspond to characteristics recognized as attacks.

Rate Based Filter A function that checks the frequency of access and detects as suspicious session when the access from a specific source to a specific destination exceeds a predefined threshold.

Reputation Based Filter A function that evaluates the connection source of communication based on attack cases, etc., and judges it to be distrustful when it has a bad reputation. For example, the connection source that has been involved in attacks in the past.

Credentials The information required to log into a system or get appropriate privileges, such as IDs, passwords, or other electronic information used internally by the system for authentication.

Vulnerability When used as a security term, it means security weakness including software bug and inappropriate configurations. It may also mean defect of operation procedure, lack of security implementation, and so on. In this article, vulnerability mainly means software bug and inappropriate configurations.

Zero-day Vulnerability Known security bugs in software for which no update have been provided. Attacks that target the period until the update is provided are called zero-day attacks.

DDoS (Distributed Denial of Service) Attack An attack in which malicious traffics are simultaneously sent from a large number of sources to exhaust various resources, such as communication capacity and computing power, to disturb the victim's service. DRDoS (Distributed Reflection Denial of Service) is also known for reflection attacks.

CDN (Content Delivery Network) A service that delivers Web content to end users from delivery servers distributed around the world. Often deployed to improve accessibility, it is also effective as a security measure.

SIEM (Security Information and Event Management) A solution that detects attacks or the threat of attacks by centrally aggregating logs and data output from security equipment and other devices, and by combining and analyzing them. Many of them have advanced visualization functions as well.

GDPR (General Data Protection Regulation) Regulations applied in May 2018 (after the PyeongChang 2018 Games) to strengthen and integrate the protection of all personal data within the European Union (EU). The systems of Tokyo 2020 Games are offered to users in the EU and therefore must comply with GDPR.

Zero-trust The concept of preventing threats by evaluated all access to system without distinguishing network boundaries, taking into account the possibility that has already been compromised.

OWASP Testing Guide The documents describing procedures and tools for web application security testing by OWASP (the Open Web Application Security Project), a worldwide community on the web security.

OSINT (Open Source Intelligence) A method of collecting target data from publicly available information sources.

Ambush marketing Marketing activities by an organization that is not an official sponsor by misleading consumers into believing that it is an official sponsor or by using intellectual property without permission.