# 第19部

# ネットワーク管理とセキュリティ

Glenn Mansfield Keeni, Hiroshi Tsunoda

## 第１章　Introduction

The WIDE-Netman-WG has been carrying out research and development to make the Internet more manageable and secure. Syslog plays an important role in management and security of the ICT infrastructure. The WG continues to work on monitoring and managing Syslog. Mining for information, the WG examined network traffic traces to discover patterns of activities in the network. The WG is looking at the security aspect of Internet of Things (IoT). Applications of IoT cover wide areas including transportation, healthcare, and the home. These critical IoT applications require a high level of security.

## 第２章　Managing syslog

The WG has discussed the necessity and importance of monitoring and managing logging systems. Log messages contain important information about the health and operation of the system. The messages are also of great significance for security management, audit-checks, and forensics in an intranet. So, a logging system must be monitored and managed just like any other component of the ICT infrastructure, to ensure that it is operating normally i.e., the logs are being collected and archived as desired. The WG reviewed and revised the basic design of a Management Information Base (MIB) module which will make it possible to monitor and control syslog applications. The latest document is published as an internet draft [25]. The WG will continue to review and refine the MIB and experiment with prototype implementation of the MIB.

## 第３章　Mining for events in network traffic traces

The WG attempted to detect events by examining network traffic traces. The traffic traces were from the darknet and from the operational Internet. The concept of traffic stability was used in the analysis. Analysis results showed that some suspicious events like backscatters, scans, DDoS attacks were found from darknet. Moreover, the WG found strange fluctuations in ICMP traffic from darknet and investigated ICMP traffic from the point of view of volume, source and destination hosts, and ICMP header contents. The results are summarized in papers [26][27]

The WG will continue to examine the information that can be mined from the network about network devices and their activities.

## 第４章　Operational model for secure Internet of Things

The WG proposed a simple operational model for IoT, namely the societal model [28]. The basic concept of the model is borrowed from human society - infants are protected by adults. This natural security mechanism works very well for IoT networks which seem to have inherently weak security mechanisms. The WG discussed the requirements of the societal model [29]. The WG is working on a proof-of-concept implementation for examining its feasibility.

## 第５章　Management information bases for multicast in BGP/MPLS L3 and L2 VPN

The BGP (Border Gateway Protocol) Enabled ServiceS (BESS) working group in IETF is working on defining, specifying, and extending network services based on BGP. As one of the BGP-based services, multicast in BGP/MPLS (Multi-Protocol Label Switching) Layer 3 (L3) and Layer 2 (L2) VPN (Virtual Private Network), is proposed. BESS working group is working on providing data models for modeling, managing, and operating such services. The netman WG has volunteered to work as document editor and MIB Doctor on the standardization of the monitoring and control aspect of the proposed multicast in BGP/MPLS L3 and L2 VPN protocols.

## 第６章　Plans for 2017.

The WIDE-Netman-WG will continue the investigation on data collection on a large scale and from small devices. We will be focusing on

a. a management framework of a syslog logging system
b. mining for events in network traffic traces
c. a security model for Internet of Things
d. monitoring and control for multicast in BGP/MPLS L3 and L2 VPN