第23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 forms an important part of management and security in the ICT infrastructure. The WG has taken a closer look at the status of Syslog management. Mining for information, the WG focused on network traffic traces to discover patterns of activities in the network. The WG is focusing on the security aspect of Internet of Things (IoT). Applications of IoT cover wide areas including transportation, healthcare, and the home. Such critical IoT applications require high level 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 presented the basic design of a Management Information Base modue which will make it possible to monitor and control syslog applications in an internet draft [68]. This document defines managed objects representing the following elements.

- The configuration and status related details of each syslog application.
- The statistics on syslog messages received, processed locally, and relayed by each syslog application.

The WG is currently working on a prototye implementation of the MIB.

(Please refer wide-paper-netman-syslog-mib-draft-00.txt) [http://www.ietf.org/id/draft-tsuno-syslog-mib-01.txt]

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.
The results are summarised in papers [69, 70, 71]

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

第4章　Security model for Internet of Things

The WG proposed a security model for Internet of Things. The basic concept of the model is borrowed from our human society. The elements of this model are members, behaviors of each member, and notification methods. All of these must be well-defined. The notification method is a key element. The WG is considering that syslog will play an important role as a candidate for light-weight and standardized notification method. The basic idea is discussed in [72]. This is an ongoing activity.

第5章　Plans for 2016.

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

a. a management framework of syslog logging system
b. mining for events in network traffic traces
c. a security model for Internet of Things