第22部

ネットワーク管理とセキュリティ

Glenn Mansfield Keeni、角田 裕

第１章　Introduction

The WIDE-Netman-WG has been carrying out research and development to make the Internet more manageable and secure. In the quickly evolving Internet the major shift is towards mobility on one hand and advanced applications on the other hand. The quick evolution has given rise to new requirements particularly in the area of network monitoring and management.

The WG has examined the issue of accuracy and consistency of measurements in systems that are widely deployed. Syslog forms an important part of 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.

Finally, the WG has examined the issue of evaluation of NMS systems.

第２章　Accuracy and consistency of network measurements

The quality and nature of statistics obtained from network monitoring and management have significant implications in accounting, operations, security and quality of service management. The WG took a closer look at the requirements of monitoring and management in the context of the future Internet and emerging applications and examined the limitations of current practices.

The WG showed that the limitations essentially stem from the timestamp attribute of a statistic. Without an implicit or explicit timestamp the usability of a statistic is severely limited especially as the network gets mobile and highspeed and, as more advanced applications appear. The results are published in [20].

第３章　Managing syslog

The WG discussed the necessity and importance of monitoring and managing logging systems. Log messages are generated by operating systems and applications. These 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 that generates, relays, collects and archives log messages, 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. In the Internet, some progress has been made towards the standardization of the syslog protocol but, to date, the management aspect of syslog has been neglected, for all practical purposes. The WG presented the basic design of a Management Information Base module which will make it possible to monitor and manage a syslog system using standard management protocols. A prototype implementation of the MIB has been carried out. A prototype syslog management application is developed to demonstrate management of syslog configuration in an enterprise. The results are summarized in [21].

第４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. The WG continued to examine the information that can be mined from the network about network devices and their activities. This is an ongoing activity.

第５章　Evaluating the performance of NMS systems

The WG discussed a framework for the performance evaluation of NMS systems. The framework is based on passive packet monitoring. Preliminary experiments show that the proposed framework can detect the effect of caching at agent side. This is also an ongoing activity.

第６章　Plans for 2015.

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 framework to evaluate the performance of NMS systems.