

# Integrated Security Management Service

Authors: Akira Tanaka\* and Fujii Seiji\*\*

## 1. Introduction

This paper describes the managed security monitoring service that MIND has provided since 1998 and the integrated security management service that MIND started as a business in fiscal 2005. It then describes the information security forecast system that MIND and Mitsubishi Electric Information Technology R&D Center are jointly developing as an expansion of these services, with the aim of releasing the system in fiscal 2007.

## 2. MIND Managed Security Service

This service provides a total security package ranging from construction, operation, monitoring and support of the system to be monitored, to the collection and analysis of security information. This service is run from the Integrated Control Center where security expert engineers monitor security operations 24 hours/365 days a year. This service consists of professional operations, education and information provision, consulting, and construction, all of which constitute the life cycle of information security.

## 3. Integrated Security Management Service

An overview of the integrated security management service is shown in Fig. 1. The integrated security management service was started as an improvement on the MIND managed security service. In this integrated service, a total optimization security monitoring service was started in fiscal 2005, and a proactive security monitoring service is now being developed, toward introduction in fiscal 2007.

ment service is shown in Fig. 1. The integrated security management service was started as an improvement on the MIND managed security service. In this integrated service, a total optimization security monitoring service was started in fiscal 2005, and a proactive security monitoring service is now being developed, toward introduction in fiscal 2007.

### 3.1 Total optimization security monitoring

A typical company has many IT systems, and needs to maintain and improve the entire security management level. The integrated security management service was designed in response to increasing demands for monitoring system operations broadly throughout a company as well as conventional optimization of individual systems.

In order to achieve these services, individually managed security information items (Intrusion Detection System [IDS]/Intrusion Prevention System [IPS] alarm/log, firewall log, system security setting, vulnerability information and security diagnosis results, etc.) are gathered by the Security Information Management (SIM) system.

The correlation analysis function of SIM was used

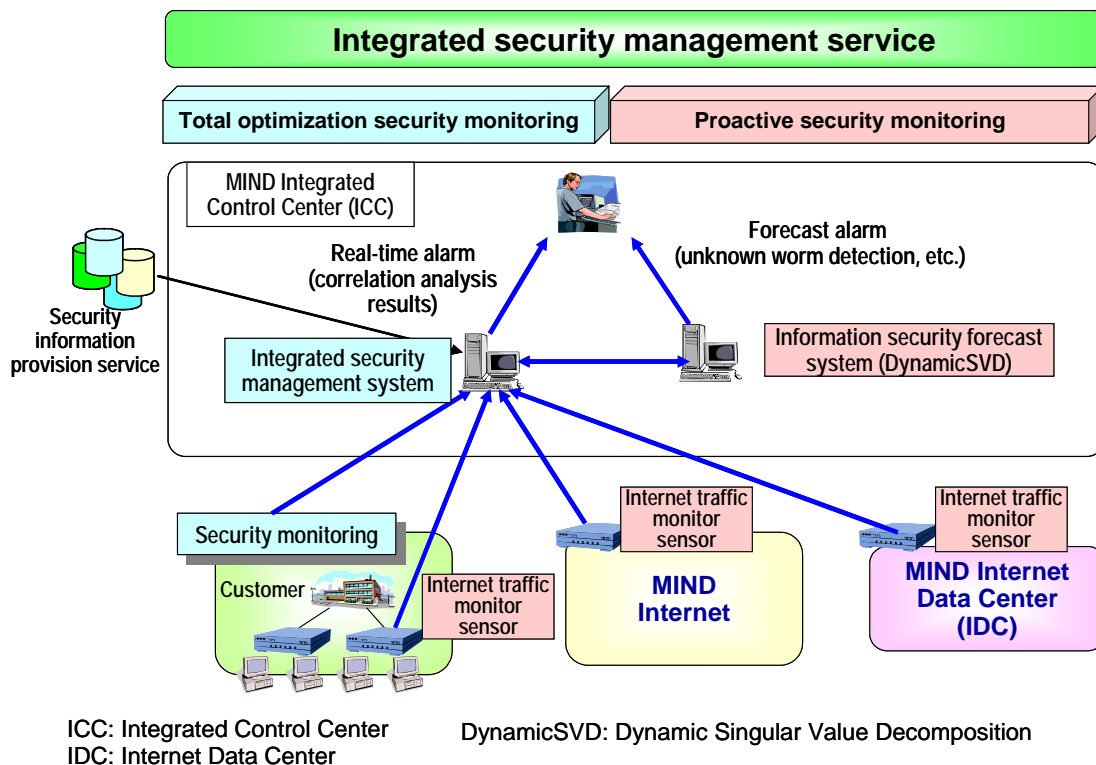


Fig. 1 Integrated security management service

to define the expertise of security expert engineers accumulated in past service operations as rules of this function, and then the gathered security information items are automatically monitored and analyzed based on the rules.

### 3.2 Proactive security monitoring

In this planned service, proactive monitoring provides added value by using the security log and system information gathered, to achieve total optimization.

Security measures such as firewalls offer immediate protection against unauthorized access and known worm-type virus attacks via the Internet. As shown in Fig. 2, however, if an unknown attack can be detected immediately it occurs, effective measures can be quickly taken to prevent the damage from spreading.

To achieve proactive monitoring of unknown attacks, an information security forecast system is being researched and developed.

## 4. Information Security Forecast System

The information security forecast system consists of the new algorithm DynamicSVD (Dynamic Singular Value Decomposition), a function for taking quick action based on the evaluation by the algorithm, and a function that interfaces with SIM.

### 4.1 Information security forecast function

The information security forecast function learns the normal network traffic status and detects abnormal traffic to help DynamicSVD ensure early detection of invalid traffic that occurs just prior to an unauthorized access. DynamicSVD has the following features:

- (1) High-speed processing  
The information security forecast algorithm Dy-

amicSVD was developed based on the Incremental SVD that speeds up Singular Value Decomposition (SVD) developed by Mitsubishi Electric Research Laboratories, Inc. (MERL), which is Mitsubishi Electric's research and development center in the U.S. This algorithm enables real-time analysis of even time-series data such as network monitoring data.

- (2) Improved detection accuracy  
With SVD, continuous analysis of network monitoring data adversely affected the performance of attack detection. To prevent this deterioration of detection performance, data is analyzed while deleting unnecessary past network monitoring data.
- (3) Verification result

In order to verify the validity of DynamicSVD that has the above features, the following network monitoring data items were analyzed using DynamicSVD to verify that an unknown attack can be detected:

- (a) Lincoln Laboratory (U.S.) IDS evaluation data
- (b) JPCERT/CC Internet traffic monitor data
- (c) MIND Internet traffic monitor data

Figure 4 shows the result of analyzing MIND Internet traffic monitor data in (c). The analysis using DynamicSVD achieved detection in just one third of the time required by the threshold method.

### 4.2 Future development

Customers demand security monitoring that can promptly detect unknown attacks and respond quickly. This section describes the function that is being developed to achieve this.

- (1) Early detection

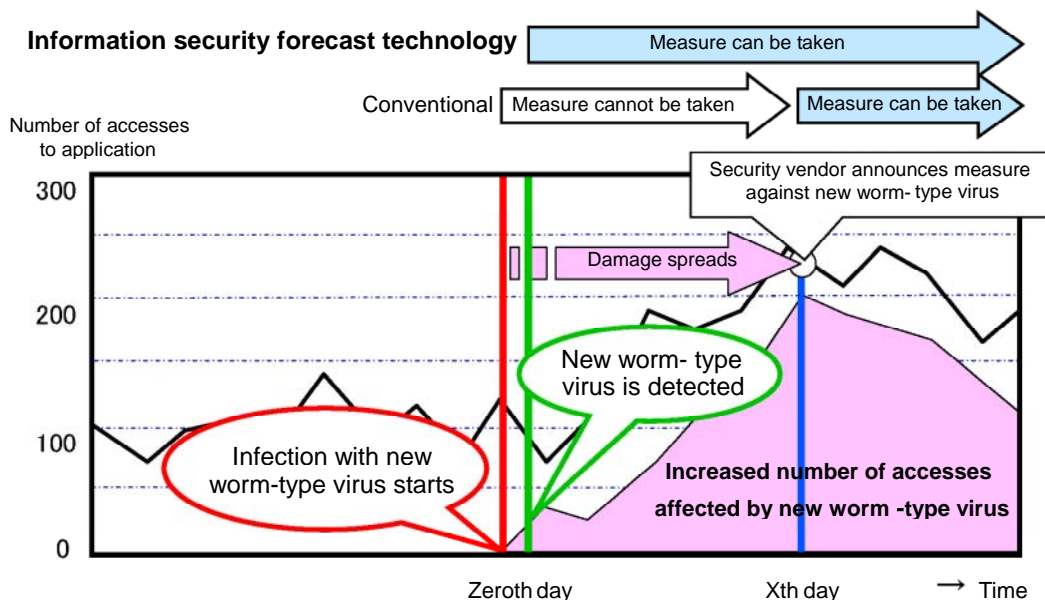


Fig. 2 Timing of unknown worm detection

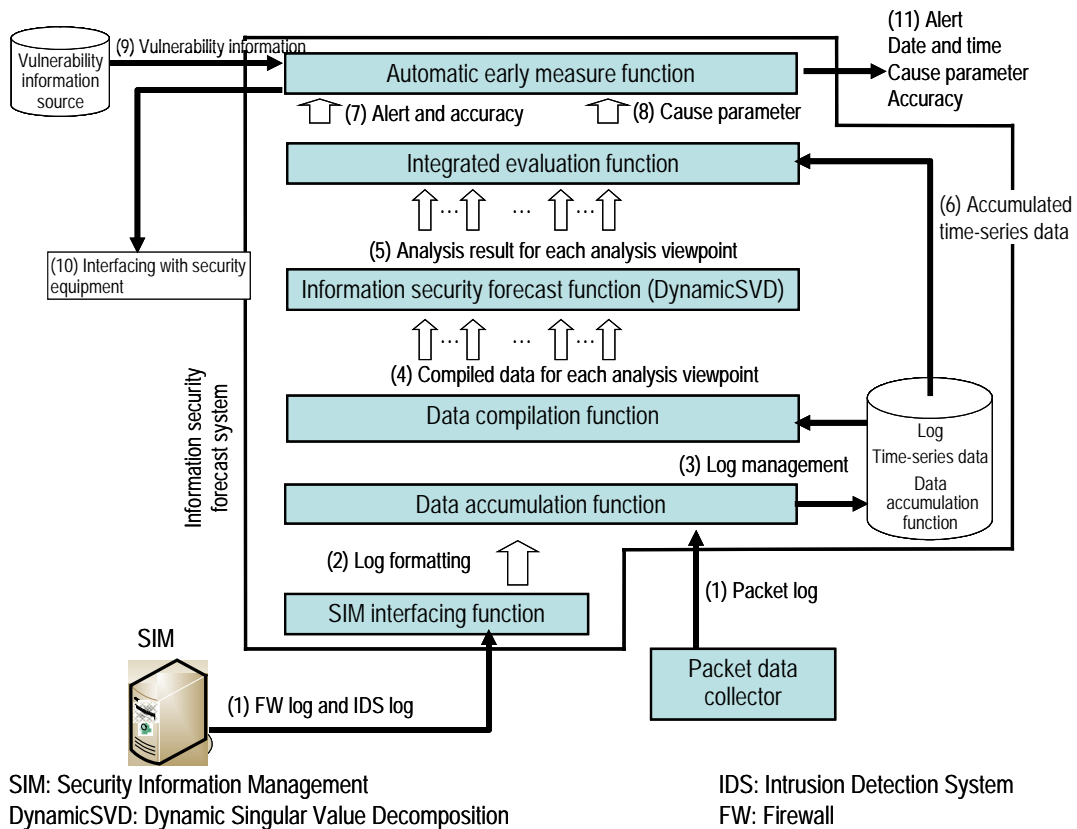


Fig. 3 Data flow diagram of information security forecast system

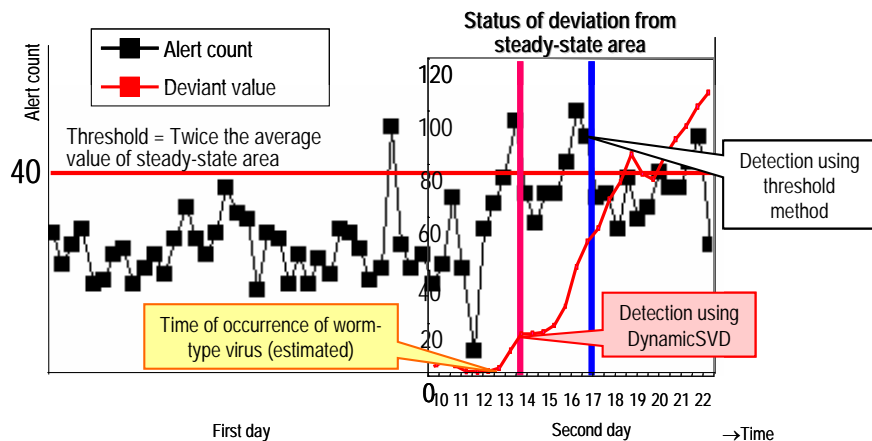


Fig. 4 Difference in detection time between methods for detecting unauthorized access

In order to use the information security forecast system for the integrated security management service, interfacing with SIM is required. We therefore developed the SIM interfacing function to collect a huge amount of SIM logs without hindering operation of the security monitoring system.

(2) Specified measure

In order to take action quickly, the cause of the abnormality and information on how to correct it are required. We are developing an automatic early measure function that uses the security

equipment installed at the monitored target to take measures according to the information provided by the integrated evaluation function and publicly available vulnerability information.

References

- (1) Hiroyuki Sakakibara et al.: Proposal of Unauthorized Access Analysis System Using Internet Traffic Monitor, the 68th National Convention of Information Processing Society of Japan 2006, 5E-3 (2006)

- (2) Norio Hirai et al.: Proposal of Unauthorized Access Analysis System Using Internet Traffic Monitor – Analysis Technique for Network Log to Detect an Abnormality Caused by Worm Attack, the 68th National Convention of Information Processing Society of Japan 2006, 5E-4 (2006)
- (3) Hiroyuki Sakakibara et al.: Unauthorized Access Analysis System Using Internet Traffic Monitor, the 38th Computer Security Group Research Seminar of Information Processing Society of Japan, 2007
- (4) Kazuhiro Ono et al.: Evaluation Technique for Network Abnormality Detection Using Principal Component Analysis, Symposium on Cryptography and Information Security 2007, 1F2-1 (2007)