“Cooperative Security” Dealing Flexibly with Business Environments

MIURA Kazuki

Abstract

Recently, security measures are influenced by the open implementation of IT systems. What kinds of security measures and support products are required to effectively and flexibly enhance such systems when customer systems are becoming so diversified? This paper discusses the “cooperative security” based InfoCage, which has been developed in order to deal with the needs and issues related to security measures that affect individual products and persons, as well as the overall governance of individual organizations.

Keywords

security, cooperative security, information leak, outflow, InfoCage, WORKS, safety, security, flexibility

1. Introduction

Many IT systems still operate and administer businesses using general-purpose machines. Actually, most of the businesses conducted up to the present have been conducted using general-purpose machines.

At NEC, the PC-8800 series was released initially to target personal entertainment, but the subsequent PC-9800 series began to be used in a business environment. This was still in the age in which the OS was DOS.

At the time Microsoft started the sale of Windows 3.1, vendors including NEC began to market TCP/IP communication software. Subsequently, the release of Windows 95 accelerated the volume of network connections, making it a natural social phenomenon to connect a PC to the network.

Security measures were not a common practice in the age in which the PC was not connected to the network. Closed general-purpose machines and PCs were installed in the operator room and measures against information leaks and other security issues consisted of the management of entrance to the operator room. Entrance to this room was by key and the entrance and exit were recorded in a ledger, which is a paper medium.

At the time open IT systems began to be introduced extensively in businesses, thanks to the ease of installation and low costs, everyone felt the convenience of the open IT systems.

On the other hand, this convenience also provided an opportunity for crackers to satisfy their desire for conquest by manipulating data. Crackers were initially simply criminals who enjoyed the reactions their victims to what they had done. However, they began to notice that the systems contained important data and this could be sold to others in order to yield profits.

We can say that it was at this point that the endeavors of businesses for improving the security of their open IT systems started to become a serious issue.

2. The Present Status of Security Measures and the Needs and Issues That Concern Them

The security measures of businesses are most often applied at the gateways, which are the points of connection to the Internet.

The gateway begins with a firewall, and important data is protected in the DMZ (De-Militarized Zone). In general open IT system environment, important data is placed in the DMZ together with the web server, the mail server, the DNS server, etc. The web server is divided into the AP and DB server layers, the former working to balance access control and the latter for keeping important data.

Past security attacks were often targeted at the DMZ. At present, however, the security measures are inadequate if they are taken only to protect the servers in the DMZ, this is mainly for the following two reasons;

1) Dissemination of the ubiquitous society (ADSL, wireless LAN);

2) Dissemination of E-mails.

In the past, with the ordinary open systems the security had been protected to a certain degree by using business applications of 3-layer construction or by limited access to the web system. Nevertheless, as the dissemination of the ubiquitous network infrastructures has tended to make PCs more mobile and the dissemination of E-mails has made contents more mobile, the potential of infection by viruses or worms has become much higher than in the past.

Security measures for IT systems are taken by imaging the servers, networks and PC clients. Vendors providing network

devices are developing and marketing a large number of security-enhanced products, PC clients are more often bundled together with anti-virus products and more and more businesses have introduced IDS (Intruder Detection Systems) and IDP to protect their DMZs. But are all of theses really enough as security measures?

Past security measures might be the tasks only of the professionals among the professionals. Daily enforcement and virus/worm countermeasures resulted in severe labor and cost loads for the managers and administrators of systems. The IDS is a good method for monitoring network packets but it is accompanied with too many incidents in its actual operations. This makes it necessary for precise knowledge to identify which incidents might affect the system.

Today, security measures are being diversified, and a time for learning and education is essential for improving the skills of system managers who are fighting the crackers by taking full command of more advanced techniques than before.

The security measures are a source of concern for any system manager who wishes to improve operational efficiencies. A review of the operation process is possible by using the best practices released for this purpose such as the ITIL and there are also "Service Support" systems for use in routine system administration and user support and "Service Delivery" for use in longer-term planning and improvement. However, the ITIL handles security in a separate framework and this has become another source of concern for system managers.

The current needs lie in easy installation and administration. In addition, if the security can be enhanced without modifying the existing system, it is possible to upgrade the IT system into a more secure system without wasting customer assets.

Since each vendor providing security products operates from a different position of strength to other vendors, products from diverse vendors are often installed in a single customer system. The labor involved in the management and administration of such systems tends to be very large, making this one of the important issues to be solved by us at NEC.

3. Birth of "Cooperative Security" InfoCage

If security measures are taken individually, point by point and the system uses diverse products from a variety of vendors, it would be a great advantage for the customer to implement a new security system by closely connecting the existing measures and products. This is because security may be significantly improved by utilizing the existing environment.

InfoCage includes a line of point security measure products that are selected to comply with the viewpoints of "Server," "Network," "PC clients" and "File (Contents)" (**Fig. 1**).

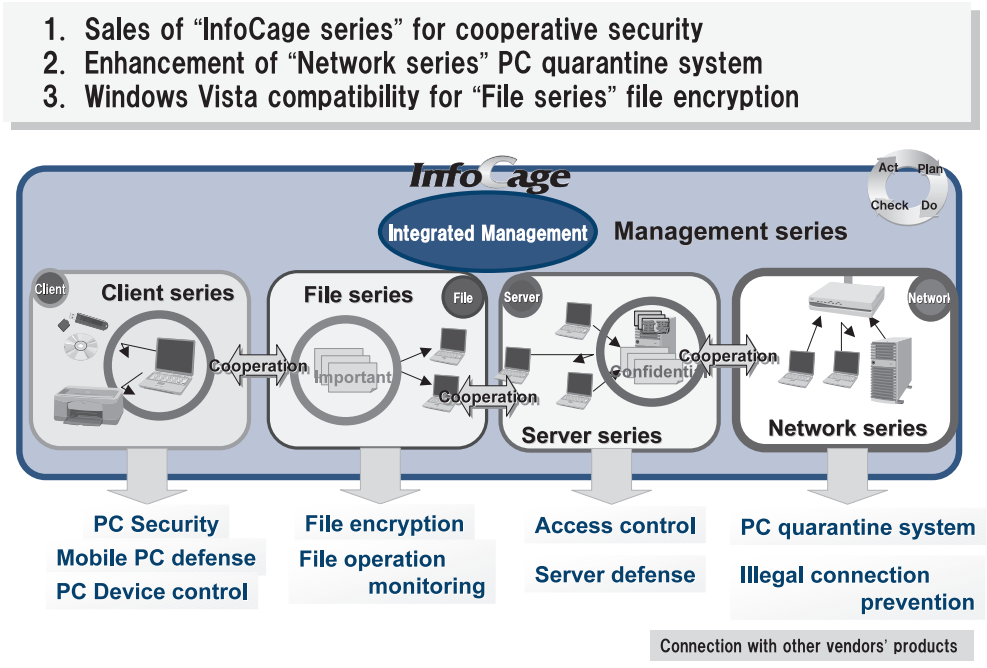

Fig. 1 InfoCage system.

When the market situation is considered, it would not be a wise practice for NEC to develop anti-virus products. The basic concept of InfoCage is that the IT system should connect and cooperate with the products of those vendors who make their products according to de-facto standards, so that provision of the same business environment may be continued.

The keyword of "flexibility" of the "REAL IT PLATFORM" Vision corresponds to the "cooperative" keyword of InfoCage. It is this flexibility that enables easy expansion and modification without discontinuing the system operation. InfoCage offers equivalence to the security technology as well as to the virtualization technology.

The "Safety" of the "REAL IT PLATFORM" should be provided as a security foundation. Technology for improved reliability and avoidance of system shutdowns due to failures or troubles may reside not only in the domain of hardware and clustering technology. In the domain of security, it is reflected as the zero-defect or failsafe type of concept that is feature of the InfoCage products.

"A safe business environment" - this means a "securely" usable platform and a simple IT system without complexity of operation.

4. Examples of "Cooperative Security" Implementation Technologies

What kind of security foundation does the "Cooperative Security" InfoCage provide and how does it enable linkage with the products of other vendors?

With PC clients, typically the foundations are the firewall and anti-virus functions that are the functions of Windows OS. This is because of considerations in prioritizing the market situation.

Microsoft is expected to continue its OS security enhancements in the future and may implement an all-in-one product offering the PC client security measures as standard functions like TCP/IP networking. InfoCage offers "authentication," "encryption," "policy setup/application" and "trace logging" for PC security. In the future, there may be a potential for a joint development of products with Microsoft.

Within the network there are a large number of network devices. The OPSEC port shutdown that features a firewall and session disconnection per TCP/IP is one of the strong points of IDS, and the InfoCage Illegal Connection Protection (previously called WebSAM SecureVisor) is a simplified version of IDS. These functions are also released as hardware appliances called InterSec/NQ30b.

With the InfoCage network series, design is often conducted on a per-hub, switch or segment basis. InfoCage not only develops the sensors for dealing with this design, but also enhances linkages through collaboration with various vendors.

With the InfoCage server series, classified servers are thoroughly protected based on a concept close to the Linux security setup or SecureOS and the network is often multiplexed in order to ensure its reliability and continuity. The risk of information outflow from servers increases if the network security setup is flawed or vulnerable. When the 3-layer structure of the present open IT systems is considered, this design may be effective when it is used between the AP and DB servers. Naturally, there are no problems with its use between the PC client and the server, including the web, AP and mail server.

With the InfoCage file (content) series, linkage with various products is performed through encryption. Because the encryption of InfoCage is linked and cooperated with the products from other vendors, contents such as files cannot be decrypted even when they outflow. Linkage with gateway-type products also makes it possible to implement a linkage for "not to allow non-encrypted data leaks outside."

5. The Goal of "Cooperative Security"

"Cooperative Security" InfoCage is either linked to or is incorporated as a part of other products. This is not limited only to the case of IT systems, but is also applied to the physical security measures taken in current business environments and offices. As seen with the entrance/exit management of a building or in integrated ID management using ID cards, the ideal and goal is that enhanced security is incorporated as a part of daily life, without making users conscious of it.

If IT infrastructures are well prepared, InfoCage products dealing with various security measure points can be distributed and applied without the need for installing applications, following the ideas for SOA or SaaS, and security enhancement may be implemented as the "REAL IT PLATFORM." This is "Cooperative security."

However, there are still some areas that can be dealt with only by NEC. One of them is the area of integrated management. The integrated management products that can monitor and control security products from various vendors will promote cooperation between InfoCage and the security operations management solution WebSAM, thus enabling continual improvement of the IT system as well as "comfort" (**Fig. 2**).

◆Dynamic "Cooperation" of IT and physical measures improves the overall security of the organization.
◆ "Cooperation" with partner products improves the security at low costs, based on the existing environment and something extra.

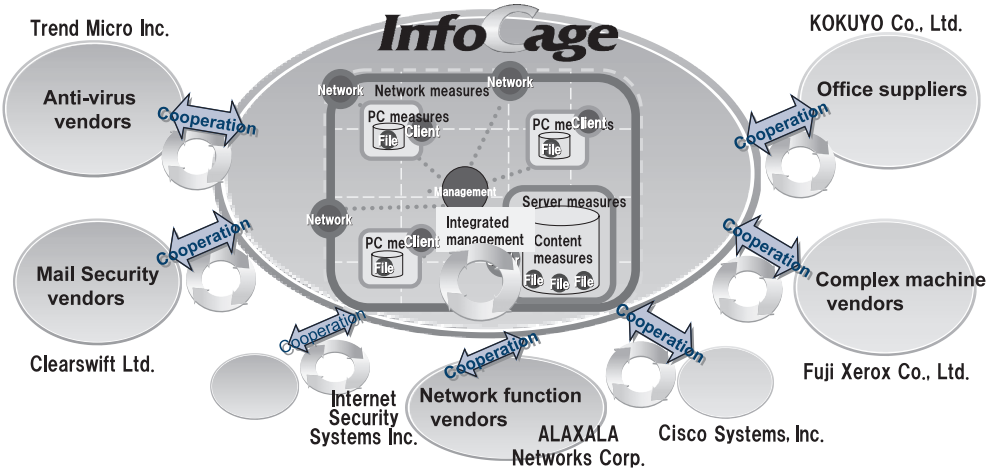

Fig. 2 "Cooperative Security" concept of NEC.

6. Conclusion

Recently in the domain of internal governance, the general governance of IT is often focused exclusively on the topic of operations management. Security is equipped with the function for tracing logs. However, the necessity of identifying and "visualizing" system status by detecting its components and of enforcing a long-term improvement program according to the current status of governance are applicable to security measures as well as to the operational management.

In the future, we will offer InfoCage WORKS products that can closely link with strategic partner products and pioneer cooperative business models and offer them to the emerging market.

The "Cooperative Security" product, InfoCage implements a safe business environment by providing "flexibility," "safety" and "comfort" as part of the "REAL IT PLATFORM."

Author's Profile

MIURA Kazuki
Manager,
First System Software Division,
System Software Operations Unit,
NEC Corporation