General Explanation
of Special Issue

NEC Group's Efforts in Information Security

In the new trend as exemplified by Web2.0, high reliability and high security is required more than ever for large-scale/complex business systems. Meanwhile, security threats are evolving at breakneck speed, making it necessary to have a system that allows any unexpected security threat to be countered much quicker than before to minimize the spread of that threat.
This special issue is aimed at introducing NEC's security technologies, products and solutions that address this problem. And this article serves to introduce summaries as well as the positioning of the various articles contained in this special issue.
In the category of key technologies we will introduce our latest technologies and products focusing on NEC's "Cooperative Security" architecture and our newest InfoCage series products. And in the category of solutions and case studies, we will talk about actual customer case studies as well as the information leakage countermeasures and strategies we have adopted at NEC.

Associate Senior Vice President,
NEC Corporation
OKADA Takayuki

1 New Trends in Information Systems

Information systems are continuing to progress by incorporating new computing and networking technologies, as well as new services that use these technologies. The permeation of broadband networks that have appeared on the scene in the last several years, as well as the spread of lightweight high-performance notebook PCs, have created a footing for a style of business activity that relies on accelerated new information systems. By virtue of the expanding NGN (Next Generation Network) infrastructure, ubiquitous technology-driven information systems will be spreading full-scale into the corporate environment. When you look at the spread of Web2.0 which was spearheaded by Google and Amazon, it can be said that outside of enterprises the e-business market has expanded explosively based on models that differ from conventional ideas. Moreover, new concepts related to the spread of software such as OSS (Open Source Software) and SaaS (Software as a Service) are being introduced, bringing about rapid change in software development and business styles. We believe this is the harbinger of innovative software products appearing one after the other, in step with the new age.

Even with companies that already own substantial amounts of conventional information system resources, the strong relationship between enterprises and the outside world brought about the shift to new information systems and their permeation will become the core of corporate activity. And in order to maintain and strengthen their innovativeness and competitiveness, leading-edge enterprises continue to have a strong desire to optimize corporate infrastructure including their computers, networks, and IT environments. Meanwhile, new software and hardware platforms are being launched in rapid succession by various suppliers. In the new trend as exemplified by Web2.0, high reliability and high security is required more than ever for large-scale, complex business systems. As shown in **Fig. 1**, sustaining high reliability and security in the large-scale/complex business systems that these developments will make possible, will be a factor that accelerates the shift towards a new environment.

For example, Web2.0 technology and services contain elements that can obscure the boundaries between the inside and outside of an organization, facilitating transparency of information exchange. Conventional information systems have a basic architecture that encloses an organization, but with Web2.0 the effectiveness of communication with the outside becomes a key point, needing radically different architectural prerequisites. The architecture required achieving high reliability and high security with this system is still in the development stage.

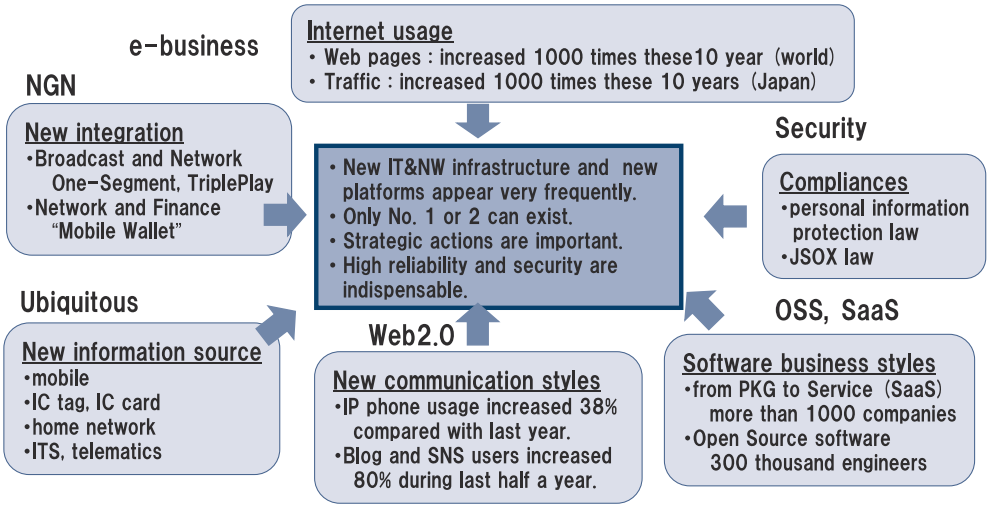

Fig. 1 New trends surrounding information systems.

Moreover, if OSS is adopted, system development will be based on coexisting in-house developed program code and open source program code, achieving overall high reliability and security of the entire system are issues that require full consideration.

Whenever a new technology arrives that can realize new information systems, technologies that give rise to new security threats also appear. Although it is difficult to predict what they will actually be like at this time, we can assume the following are highly probable: 1) within the scope of current technology there is likely to be an increase in threats that attack specific targets (e.g. spear type virus); and 2) we will see threats that enter the system in the conventional way but will carry out attacks that are difficult to detect through conventional technology (e.g. because their attack patterns are self-evolving).

Security measures in the past have consisted of rushing together countermeasure products specific to incidents after they actually occur, in a patchwork manner. When one considers the spread of new information systems as introduced in this article earlier, simply applying security measures based on conventional standards will not enable the benefits of new information systems to be realized. Although it is difficult to set up a complete solution in advance to counter a threat that is nearly impossible to predict, it is possible to systematically implement countermeasures much quicker than before to squelch the spread of an unpredicted threat once it strikes. At NEC, we have decided to develop the architecture that will answer this problem, and widely incorporate it into our security measure products. This is the essence of the content that we would like to convey to you in this special edition.

2 NEC's Efforts in Information Security

At NEC, in order to address the innovations associated with the new trend in information systems, we have developed our information security strategy and architecture. Parts of this were announced to the public in September and November 2006. First, in September we announced NEC's original "Cooperative Security" architecture, as well as our flagship product in the information security field, the new InfoCage series. This is our product line that offers integrated management of the information resources within a company, from paper documents to digital data and networks, and provides mutual and automatic integration of the security functions of PCs and servers, etc., based on "Cooperative Security."

The information security products up until now have consisted mainly of single function products that offered solutions for individual problems, and how they were used in combination was left up to the user or system integrator. As a result, security vulnerability existence became an issue depending on how they were combined, and there was always a possibility of information leakage when it moves from one product to another across one security management territory.

Enterprises that are done with ordinary information security measures will have to be applying thorough information management aimed at strengthening internal IT asset controls. From the use of individual countermeasure products, to entry/exit control and computer log-in control, business system access control, unauthorized access countermeasures, information leakage countermeasures, digital data management and cabinet management, there is a strong desire to develop total solutions that encompass all of these. The new InfoCage series we are

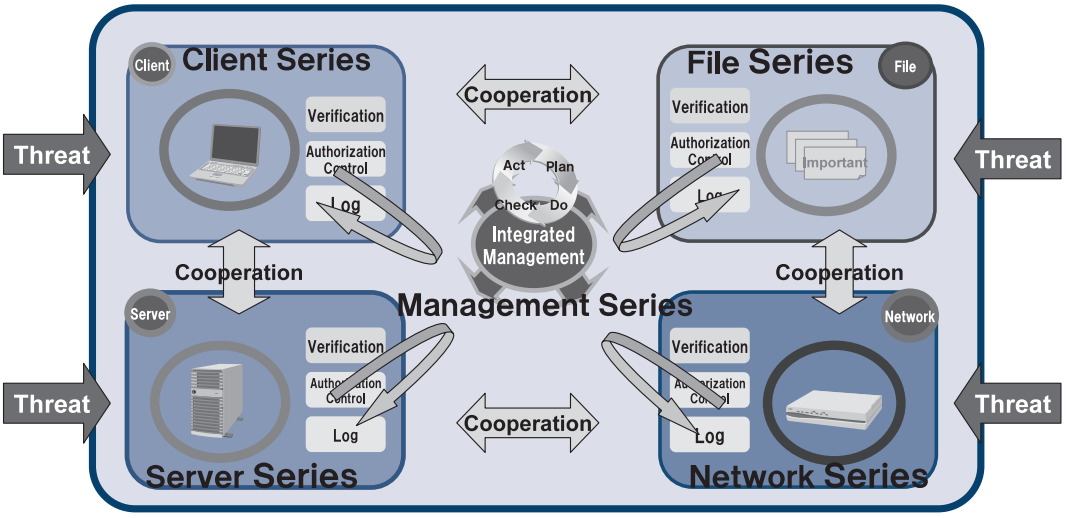

Fig. 2 New InfoCage Series.

introducing is a renewal of our previous InfoCage system, in order to meet this market demand.

As you can see in **Fig. 2**, our new products are comprised of 5 groups. Namely they are the "Client Series" which performs encryption and authentication of clients such as PCs; the "File Series" which encrypts files and contents as well as folder verification; the "Server Series" which controls the removal of data from the server; the "Network Series" which performs carry-in PC detection and blocking as well as network management and the "Management Series" which integrates and controls management information (verification ID, access log) for each of the above mentioned products. Through this, it is possible to achieve well-balanced security countermeasures at each layer of content, PC, server, and network. In terms of implementation, it is possible to continue running the current system while phasing-in a system environment that prevents information leaks. Starting with the release of "PC Security," a core product of our "Client Series," in November 2006, we plan to incrementally roll out our entire product line.

Also in November 2006, we announced the establishment of "InfoCage WORKS" for our collaboration program with partner companies, in an effort to strategically promote the collaborative operation between security products. By establishing a mutually complementary relationship on security measures between InfoCage and the main products of our partner companies, it will be possible to apply the high-level security management enabled by "Cooperative Security" to a broader area, thus allowing us to provide information security to our customers in a more solid fashion (see **Fig. 3**). This system provides 3 levels of corporation: 1) performing mutual security feature verification between products; 2) enabling collaborative operation between products; 3) performing co-development by way of close-knit collaboration between products. As of November 2006 when the announcement was made, about ten companies including Trend Micro Incorporated, KOKUYO S&T Co., Ltd. and Clearswift Corporation had collaborated.

Besides this, we also announced two other products. One is "SECUREMASTER," our new product in the IAM (Identity & Access Management) field that is critical for "Cooperative Security" to be able to transcend organizational boundaries. And the other is the "Agent-less PC quarantine system" which makes it unnecessary to install software into your PCs to perform PC security status verification. "SECUREMASTER" offers a system of API and connectors to provide ID-level integration with the security products of our partner companies. Based on a track record as No.1* in the quarantine tool market, the "PC quarantine system" is being offered with a broadened range of cooperative products.

By utilizing our line of cooperative products, it is possible to offer various security solutions and services. And by virtue of the security products by partner companies that support our "Cooperative Security," it is possible to offer solutions tailored to the environments of our customers.

3 Structure of This Special Issue

In this special issue, we have gathered articles that cover the NEC group's latest activities in "information security in enterprises," by introducing our technologies, products, solutions, and case studies in this field. It is structure as follows.

The category of key technologies will focus on the product

* "2006 Network Security Business Survey" (Fuji Chimera Research Institute, Inc.)

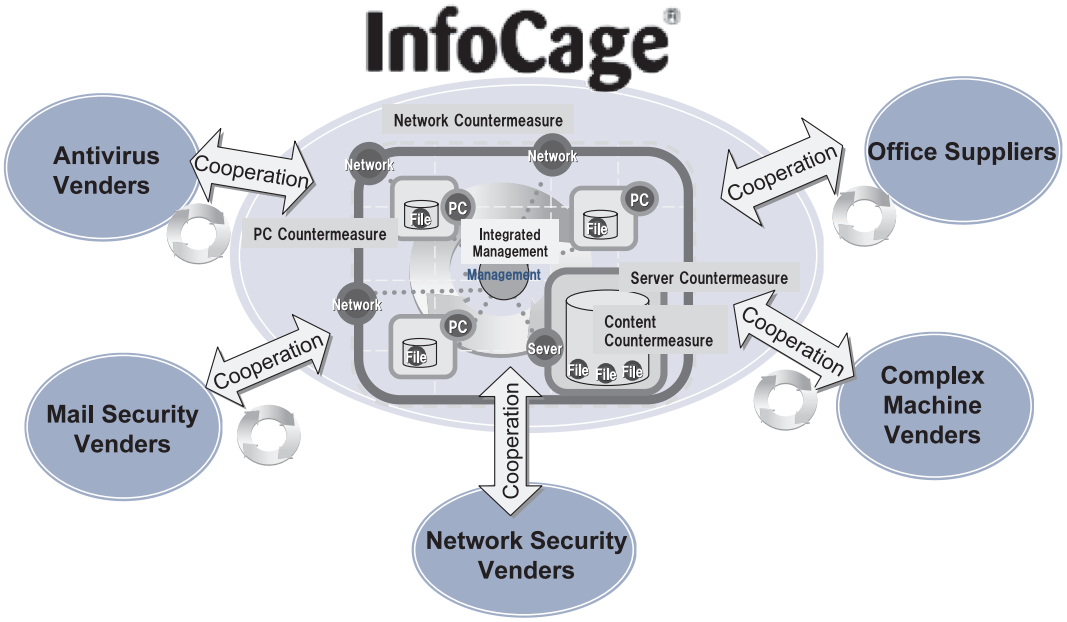

Fig. 3 "Cooperative security" with our partner enterprises.

line that will enable "Cooperative security" as well as other products and technologies that can be integrated with them. First, in "Cooperative security Breaks the Limits of Traditional Security Measures," we explain the concept of Cooperative security and offer specific examples. In "Quarantine Network in the Age of Internal Governance," we explain about the quarantine system that achieves access control in response to the security level of the Intranet-connected equipment that constitutes the core of InfoCage's Network Series. In "Internal ID Management in the Age of Internal Governance," we explain about the verification technology that is the common foundation for cooperative type security, as well as our product for this purpose, SECUREMASTER. In "Employment of Contents Security in Business Environments," we explain about the security technology centered on digital documents, as well as its product, the InfoCage File Series. And in "System Cooperation between Entrance/exit and Information Security," we will explain about the IC card based entry/exit management system. Here, we will introduce the system used to manage the entry/exit of all NEC employees and visitors.

The category of Case Studies contains one explanation. In "Efforts toward Information Leakage Prevention by the NEC Group," you will find introductions regarding the design policy and architecture of NEC's internal information security system, as well as its management methods.