"Cooperative Security" Breaks the Limits of Traditional Security Measures

NORIFUSA Masaya, GOTO Jun, MORINO Junichi, YANOO Kazuo, SAKAKI Hiroshi, TERASAKI Hiroshi

Abstract

Just as broadband networking, high-performance and light-weight laptops and useful applications have significantly improved enterprise IT environments, the targets and complexities of security management have also tended to increase significantly. Actions against security problems are now required to be performed in no delay. The resulting movement of information and its carrying devices have produced many security issues that cannot be dealt with by a single, static security countermesure. In order to deal effectively with this situation, this paper proposes the notion of “cooperative security.” Cooperative security allows security countermeasure utilities with different target domains to be mutually linked, thus achieving double or triple security management of the information and its carrying devices as well as maintaining a high security level for the enterprise. The new InfoCage series is a suite of utilities for implementing such management policies. It is also planned that “cooperative security” will be extended to the partner vendor products in order to enhance security linkages to the applications of other business fields such as paper documents and floor entrance/exit management systems, etc.

Keywords

cooperative security, coordination of security management, InfoCage series, linkages with partner vendor products

1. Introduction

The need for security measures has been recognized by a wide range of business users as a result of the widespread use of the Internet since the nineties. More than a decade has now passed since then and security has now become an important social issue that is recognized even by general users. At the same time its targets have become diversified and complicated to a degree that was unimaginable in the early days.

While security management has tended to increase the complexity, the opportunities needing demonstration of optimum security management such as auditing based on compliance and explanations of safeness to customers are increasing. This is a very big difference compared to past non-disclosed procedures and can be regarded as being likely to become a new constraint on the design of security measures from now on.

This paper analyzes the changes in security management methods up to the present, the current status of security measures and also discusses “cooperative security,” which is the means that we propose of applying consistent security management over a wide range of targets by reducing its complexity.

2. Changes and the Current Status of Security Requirements

In the initial period that businesses became capable of connecting to the Internet, the available aids for the business user were limited to E-mails and file transfers. Later, after the web technology was opened to the public, the disclosure of business information via the web has spread, gradually resulting in business activities becoming inseparable from the use of the Internet. Enterprises have now installed firewalls at the boundaries between their networks and the Internet, and are expanding their security coverage by introducing the VPN (Virtual Private Network), IDS (Intrusion Detection System), IPS (Intrusion Prevention System) and filtering gateways for use in taking measures on a per-application basis.

One of the security measures that do not derive from the Internet is the computer virus issue. The computer virus has existed since as early as the eighties, but it has now become a major threat involving any user of the Internet age, since the procedure of attaching files to E-mails became widely practiced. The viruses that are created merely for the enjoyment of the results of mischief have evolved into the worms that are accompanied by actual harm, and sophisticated techniques for penetrating PCs from networks has brought about new threats such as spyware and bots. As they do not destroy or alter the

PC data but act to attack other PCs or transfer internal information to them, these are often not noticed by the user of the infected PC.

One of the most active security measures in the recent Japanese market is that of information leakage countermeasures. While many of the traditional security measures assumed attacks to the network or the PC, information leakage countermeasures must be capable of managing internal offenses or information output from inside the organization, so they have to be based on an essentially different concept to those of the past. In many cases, information leakage occurs during an employee's normal use of PCs and their applications. It is also necessary to consider cases of theft of PCs that contain vital corporate data.

Many enterprises have been introducing security measure utilities according to the needs of the moment with the mobility factor becoming increasingly relevant. The users, PCs and information no longer remain in fixed positions but are frequently moved easily and instantly to locations with variable security levels (**Fig. 1**).

Due to rapid changes in the environment of management targets and the multiplication of the domains handled by security measure products, it has become extremely difficult to ensure consistent or complimentary security policies and functions and the only way possible for the present, is to resort to independent functions designed for individual purposes. The need to avoid unexpected security holes when management targets move beyond the boundaries of security management means that the work of IT administrators is becoming extremely complex and burdened.

3. Cooperative Security, Its True Value

Even when there are common functions shared by the utilities for preventing external attacks and those for preventing internal offences, they are managed essentially from different viewpoints. In fact, it cannot be guaranteed that the effects obtained from individual measures taken to permit user authentication, information access and data transmission or to deal with policy violations can avoid producing vulnerabilities in security management. This is especially so when the information moves across the boundaries between management targets, for example from the PC to the network. Even when individual products are provided with meticulously arranged functions, policy inconsistencies may lead to the creation of an unexpected management bypass.

For example, even when data transmission is controlled using security measures software on the PC, certain violations may occur due to the PC or the user. Such violations might

The traditional concept of security measures

Traditionally, security measures have been to apply one-issue or unidirectional countermeasures to each target to be protected. However, as the protection targets have become more diversified (including information, networks, IT assets, etc.) and ubiquitous (movements with mobile PCs, mails and USB memories), methods of adopting one-issue and unidirectional countermeasures are approaching the limits.

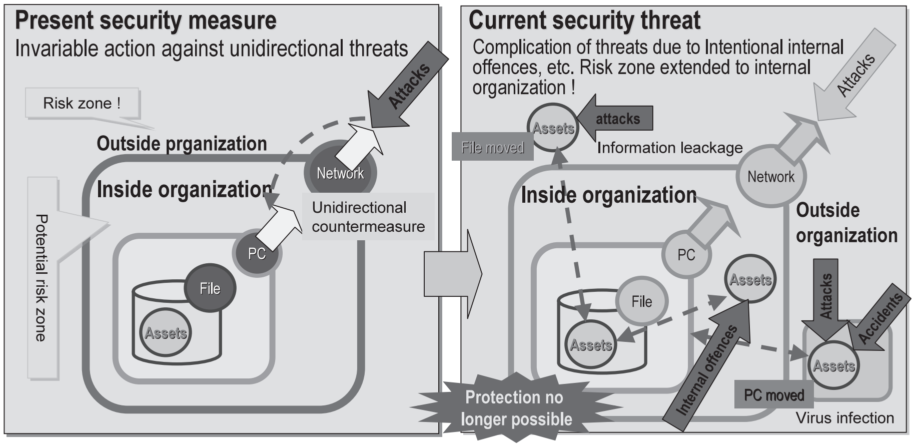


Fig. 1 Imbalance between security threats and countermeasure coverage.

take place when spyware is activated or the user leaks information intentionally. In such cases, spreading of the damage can be prevented by adopting measures such as a firewall capable of shutting down all communications from the PC.

The notion of “cooperative security” lies in preventing omissions in security management by running the security measures, which usually function for closed, individual targets, via security management linkages that also cover multiple targets in the surrounding environment. Traditional security measures have been aimed exclusively at individual targets and have achieved prevention, detection and defense against threats represented in each policy. As a result, if a preventive action is invalidated or a defensive function is annulled when a threat is detected, the effect of threat detection cannot be used effectively, and it has been necessary to resort to other countermeasures that are prepared separately elsewhere. In addition, the conditions needed for threat detection have had limitations if applied only to individual functions. However, cooperative security can detect threats in individual management targets, judge the situation by combining them and inform the defense functions of other management targets in real time. This makes it possible to have consistent security measures function over a wide range, such as throughout an entire intranet organization.

Coordination functions for preventing the omission of measures are determined by the threats, countermeasures, effects of countermeasures, conditions invalidating the effects and threat transformations. **Table** shows examples.

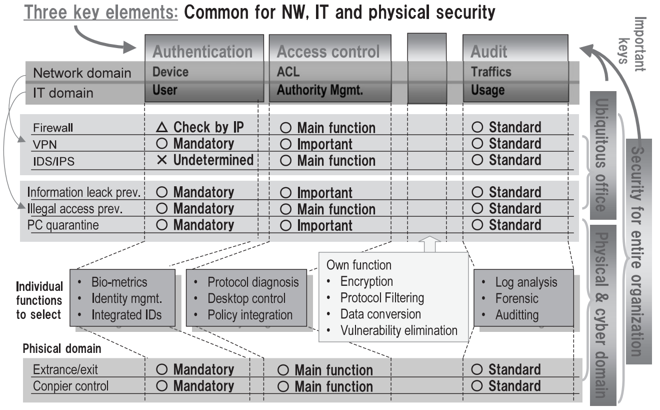
Coordination functions first utilize the functions that are applied commonly as security measures. Many security measures are based on the management of authentication, access control and computer forensics as shown in **Fig. 2**. Reliable rigorous authentication and access control based on the reliable authentication IDs make it possible to prevent many such abuses.

The four main targets of security management in the enterprise IT environment are; “file (content),” “PC (client),” “server” and “network.” These four target domains cover

Table Relationships between threats, countermeasures, effects of countermeasures, invalidation of effects and auxiliary measures.

Location of Threat	Threat details	Countermeasure against threat	Case in which countermeasure is effective	Case in which countermeasure is invalidated	Method of recovering from the invalidation of countermeasures
PC	Information spread by worm or virus	Elimination of worm or virus in a gate	When the data is not encrypted	When a new worm or virus without a registered signature is used	① Isolation of PC. ② Server access control.
PC	Carrying of infected PC	Identification of infection status using a PC quarantine system	When the quarantine agent is introduced in the PC	When the quarantine agent is stopped	③ Elimination of worm or virus in a gate ④ Isolation of PC
PC, file	Carrying out of file through the network	Inhibition of program startup using remote desktop, etc.	When the access authority to share information is enhanced	When the program is started after changing the program name	File encryption and access authority management
PC, file	Carrying out filing using a removable medium	Automatic encryption of files written in an external storage device	When the user is authenticated, if the PC is used by only one user	When an authorized PC with which authentication is omitted is abused	Isolation of removable medium
PC, file	Transmission of files by attachment to E-mails	Encryption of all important files	When the file is used in the range for which the encryption key can be used	When the file is stored temporarily in plain text for editing, etc.	⑤ Filtering of plain text mails in the mail server ⑥ Locking of PC communications
Server	Operation by an illegal user	Use of multiple authentication elements such as IC cards	When authentication is performed for an individual	When an IC card is shared	Enhancement of authentication conditions and access management
Network	Data bugging on WAN	Encryption of communication with SSL or IPSEC	In an environment in which VPN can be created	Management of communications beyond the decryption device	Encryption of files

The threat of information being spread due to a worm or virus is dealt with by getting rid of them using a firewall or gateway. However, the countermeasures cannot be effective when a new virus without a registered signature is used. In such a case, the spread of the virus can be prevented effectively by additional measures such as isolation of the infection source PC from the network (①) or restriction of the client from accessing the server (②). For a threat caused by an infected PC, defense is provided by using the PC quarantine system. However, this countermeasure loses its effectiveness if the quarantine agency ceases to operate. In such a case, it is effective to take additional measures such as the elimination of the virus by firewall or gateway (③) or identification of communications from the infected PC in the gateway and isolating that PC (④). Attachment of files to E-mails is a general practice, but a file edited on a PC is usually left as a plain text. To prevent a PC from transmitting such a non-encrypted file in an E-mail, it is very effective to detect the attached plain text file in the file server (⑤).



	Authentication	Access control		Audit
Network domain	Device	ACL		Traffics
IT domain	User	Authority Mgmt.		Usage
Firewall	△ Check by IP	○ Main function		○ Standard
VPN	○ Mandatory	○ Important		○ Standard
IDS/IPS	× Undetermined	○ Main function		○ Standard
Information leack prev.	○ Mandatory	○ Important		○ Standard
Illegal access prev.	○ Mandatory	○ Main function		○ Standard
PC quarantine	○ Mandatory	○ Important		○ Standard
Extrance/exit	○ Mandatory	○ Main function		○ Standard
Conpier control	○ Mandatory	○ Main function		○ Standard

Fig. 2 Mutual linkages between security measures.

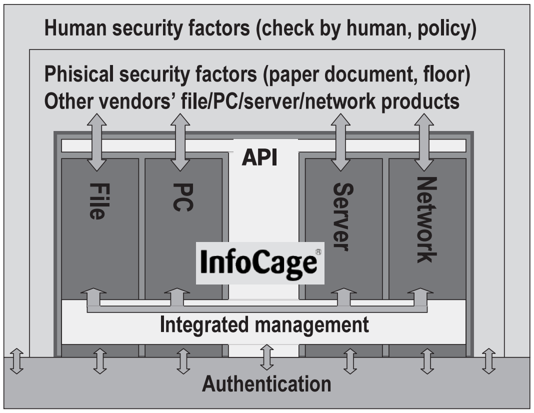

Human security factors (check by human, policy)
Phisical security factors (paper document, floor)
Other vendors' file/PC/server/network products
API
File
PC
Server
Network
InfoCage®
Integrated management
Authentication

Fig. 3 Cooperative security around InfoCage.

almost all of the important security measures used at present. In addition to these, extended management targets also include the "paper document (physical)," "entrance/exit gate (physical)" and "user IDs (human)." Coordination of security measures among these is performed by layering the measures, placing measures that can be electronically and automatically coordinated in the inner positions of the layers and placing the measures that necessitate human intervention in outer layers. Namely, the "file" measures are placed in the innermost position, the "PC" and "server" measures are placed outside of these, the "network" is placed in the outer layer, and the "paper documents" and "entrance/exit gate" measures are placed in the outermost layer. The "human" measures are associated with all of these but are placed in the outermost layer because they are dependent on human intervention, and function as the last resort of the security measures. This layered structure means that an omission in the measures produced in an inner layer may be dealt with in the outer layers.

4. Implementation of Cooperative Security

The cooperative security till the physical and human layers can be implemented by using the InfoCage series utilities including the security measures products for "file (content)," "PC (client)," "server" and "network" and the integrated management tool providing policy management and coordination engine as the InfoCage core products and linking them with the supplemental products including the extended target products from vendors other than NEC (**Fig. 3**).

Linkage between the InfoCage series utilities can be implemented dynamically and closely thanks to the integrated management tool, while the linkage is begun with that between each utility from another vendor and one of the InfoCage utilities. This is the basic configuration. For example, the coordination with the anti-virus utility is managed by the InfoCage PC security product, and that with the firewall is managed by the InfoCage network security utility. The result of the coordination between each pair of utilities is sent to the integrated management tool through each InfoCage utility and then the integrated management sends the details of the coordination to other InfoCage utilities.

We are planning to offer an API between each utility from other vendors and the integrated management tool in order to enhance the coordination more powerfully than that available with the basic configuration. This will for example make it possible when the firewall detects a bot attack, to inform the integrated management tool of the event through the API so that the PCs and servers under the InfoCage control can also take countermeasures against the bot behavior.

5. Examples of Cooperative Security Application

The following figure (**Fig. 4**) shows an example of a cooperative security application. Here, it is assumed that policy inhibits the transmission of an E-mail outside the enterprise by attaching a non-encrypted file to it and that an E-mail was transmitted with an attached non-encrypted file by violating the rule.

① The mail server checks whether or not the file attached to every E-mail it receives is encrypted.

② When the mail server detected that a non-encrypted file was attached to an E-mail addressed to an outside address, it

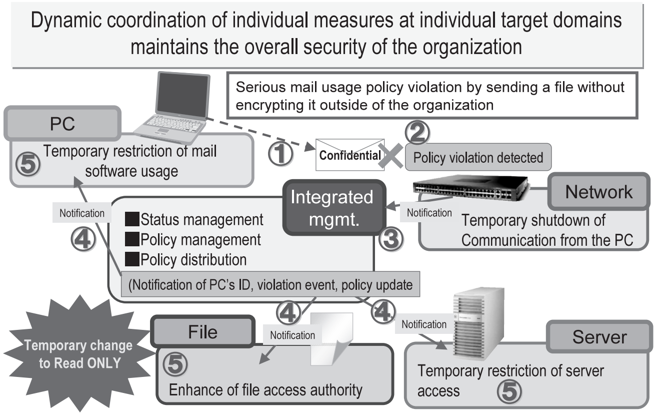

Dynamic coordination of individual measures at individual target domains maintains the overall security of the organization
Serious mail usage policy violation by sending a file without encrypting it outside of the organization
PC
⑤ Temporary restriction of mail software usage
①
Confidential
②
Policy violation detected
Integrated mgmt.
Network
Notification
Temporary shutdown of Communication from the PC
③
Notification
④
■Status management
■Policy management
■Policy distribution
(Notification of PC's ID, violation event, policy update
④
④
Temporary change to Read ONLY
File
Notification
⑤
Enhance of file access authority
Notification
Server
Temporary restriction of server access ⑤

Fig. 4 Example of a joint operation with cooperative security.

stops the transfer of that E-mail.

③ The mail server informs the InfoCage integrated management utility that it has stopped an E-mail.

④ When this information is sent to the integrated management tool, it sends a coordination notification to the associated InfoCage utilities.

⑤ The products receiving the notification execute the cooperative security actions, e.g.;

a) The network temporarily shuts down the communication from the PC;

b) The mail server temporarily denies access from the PC;

c) The authority for decoding encrypted files is voided temporarily;

d) The main client is temporarily prevented from starting up.

6. Toward More Advanced Cooperative Security

Cooperative security can improve the security level of an enterprise because it facilitates in-house security management, maintains a high security level across a wide area and enables transition to a coordinated environment by extensively utilizing an existing one. More advanced coordination is possible by adopting either of two kinds of orientations. One of these is to enhance the coordination with extended target systems including;

① linkage with the firewall;
② linkage with the IPS;
③ linkage with the networking device;
④ linkage with the access management device,
⑤ linkage with the PC security software;
⑥ linkage with the copier;
⑦ linkage with the office equipment.

Enhancement is also possible by developing cooperative security partner programs with the vendors of the above products.

The other orientation is to implement cooperative security across more than one organization. Even within a single enterprise, different security management methods are used between different locations or between affiliated firms. However, people from different organizations often work together on a single project, sharing important information regarding the project and bringing it back to their organizations with variable security management levels. In such a system, the probability that information leakage might occur in an organization with minimal security management is very high.

The key to the implementation of cooperative security across different organizations begins above all the coordination of ID management (**Fig. 5**). User authentication methods of different organizations are allowed to be different. However, the relationships between user IDs must be managed strictly so that the project information can be handled without degrading the security management level, whether a user conducts work in another organization or in his or her own organization. It is also important that the user IDs recorded in usage forensics should be traceable to a single person if they are used by a single person.

This kind of cooperative security is possible thanks to the linkage of InfoCage utilities with ID access management ones that are equipped with a function for enabling the mutual use of IDs (ID federation function).

7. Conclusion

This paper has explained the basic concept and superiority of "cooperative security" and the method of its implementation. Since security managed on a per-product or per-function basis has limitations, if coordination of security management between security products is applied it will be possible to recover any omitted countermeasures at another location by coordinated products. Security management will thus be maintained at a high level, even when changes in threats or system utilization conditions have led to the elimination of individual countermeasures. Now that the entire range of management homogeneity from information leakage to general internal governance is being expanded, we believe that the method of maintaining security based on the coordination of PCs and networks on an all-organization scale best meets the trends of the times.

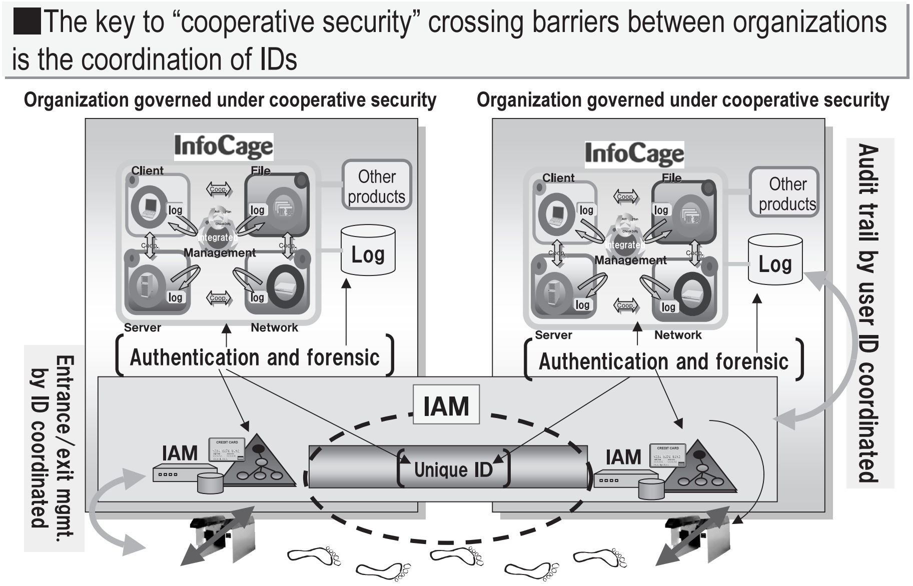

The key to "cooperative security" crossing barriers between organizations is the coordination of IDs
Organization governed under cooperative security
Organization governed under cooperative security
InfoCage
Client
File
Coop.
log
Integrated Management
Server
Network
Other products
Log
Authentication and forensic
IAM
Unique ID
Entrance/exit mgmt. by ID coordinated
Audit trail by user ID coordinated

Fig. 5 More advanced cooperative security across different organizations.

In order to apply cooperative security measures across multiple organizations such as for firms within a business group, it is necessary to expand the range of coordination of ID management methods or linkages by using more information devices. This issue is a key to the notion of security management and we are pursuing in depth studies in this regard. Cooperative security begins with the introduction of InfoCage products as the core solution. However, the management range should expand step by step so that security management may eventually be shared by crossing barriers between organizations.

Authors' Profiles

NORIFUSA Masaya
Executive Expert,
First System Software Division,
Systems Software Operations Unit,
NEC Corporation

GOTO Jun
Assistant Manager,
First System Software Division,
Systems Software Operations Unit,
NEC Corporation

MORINO Junichi
Staff,
First Systems Software Division,
System Software Operations Unit,
NEC Corporation

YANOO Kazuo
Assistant Manager,
Internet Systems Research Laboratories,
Central Research Laboratories,
NEC Corporation

SAKAKI Hiroshi
Staff,
Internet Systems Research Laboratories,
Central Research Laboratories,
NEC Corporation

TERASAKI Hiroshi
Assistant Manager,
System Platform Software Development Division,
Solution Development Laboratories,
NEC Corporation