Efforts toward Information Leakage Prevention by the NEC Group -Information Leakage Prevention System "ARGUS" -

NEC is currently developing an information leakage prevention system (ARGUS: NEC Information Audit-trail & Guard System) that uses the new InfoCage series utilities as its core. The purpose of this system is to prevent information leakage incidents or to minimize their damages if they occur. These aims are achieved by using IT to permanently manage information flow, even when information is handled outside of the corporate office or by a third party in the office. Hitherto, the only means of prevention in such cases was to rely on the rules and ethical policies of the outside firms and their employees. ARGUS has already been introduced since the latter half of FY2006 in some NEC departments on a preliminary basis and its full scale domestic introduction throughout the NEC Group is scheduled for FY2007.

TAMURA Takashi
Manager,
Corporate IT Division,
NEC Corporation

KANDA Masahiko
Senior Manager,
Corporate IT Division,
NEC Corporation

Introduction

At NEC, we are developing the ARGUS information leakage prevention system as a defense against information leakage in the NEC Group (including contract firms such as cooperating firms). It is not possible to prevent information leakage incidents by simply relying on human behavior and awareness. The system aims at providing maximum defense using IT against information leakage incidents caused by human factors (by preventing them or minimizing damage if they occur).

In this article, we will introduce the background of the development of ARGUS, its objectives, summarize its functions and discuss its future perspectives.

Development Background

We have built and are operating a corporate network for the NEC Group called the NEC Intranet. We have already installed the following security measures:

(1) Security Enhancement of the NEC Intranet

Management of connections to commercial Internet sites, monitoring of the NEC Intranet status and access denial of PCs to the NEC Intranet that do not meet the required security standards, etc.

(2) Security Enhancement of the NEC Intranet Connected Devices

They include automatic application of security patches, automatic updating of anti-virus software and the introduction of PC encryption software, etc.

(3) Security Enhancement of Information in the NEC Intranet Environment

Encryption of files, restriction of file access, etc.

(4) Management of NEC Intranet Users

Integration of the IDs of all users based on personnel data and management of authorizations based on IDs.

However, due to the large number of tasks for which customers' confidential information is handled outside the offices, it has become necessary to adopt information leakage measures that cover the entire lifecycles of the information (input or compilation of the information to its disposal or return). These measures apply to contract firms as well as to the NEC Intranet.

Risk of Information Leakage

Fig. 1 shows the routes of information exchanges and the risk of leakage. As a result of surveys into past cases and the lessons learned from several projects, we have identified the following facts.

1) Information leakage incidents have two main causes, the theft/loss of a PC or mobile devices (USB devices) and data leakage by computer viruses on Peer to Peer file sharing sytems such as "Winny."

2) The employees of the contract firms obtain information in various ways, including direct acquisition from customers or customer systems, acquisition from NEC employees or

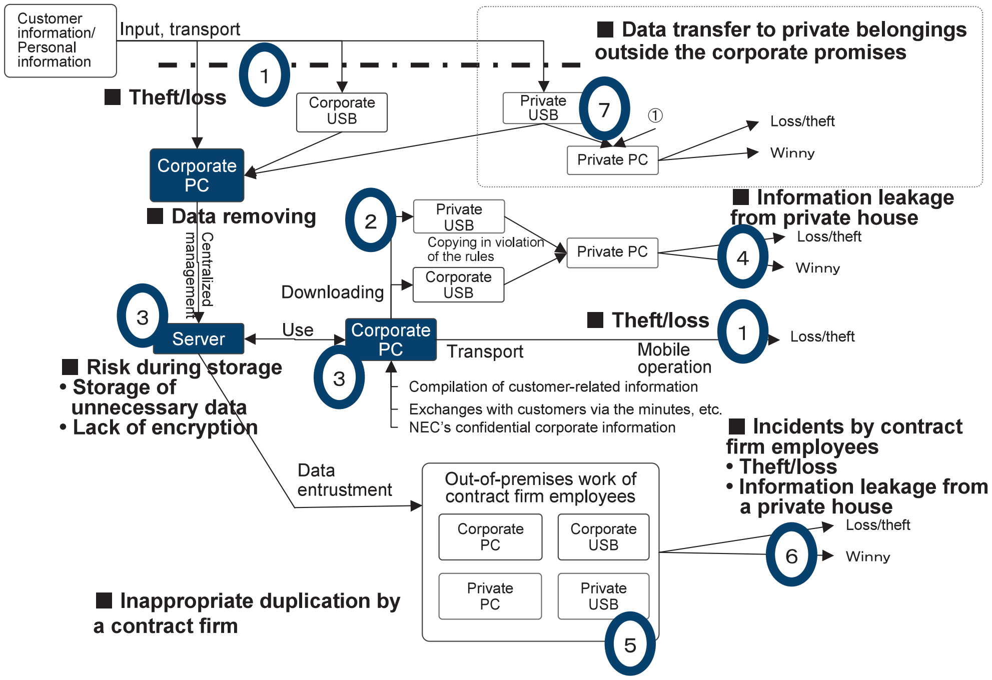
Customer information/ Personal information
Input, transport
■ Data transfer to private belongings outside the corporate promises
1
■ Theft/loss
Corporate USB
Private USB
7
①
Loss/theft
Winny
Private PC
Corporate PC
■ Data removing
2
Private USB
Copying in violation of the rules
Private PC
■ Information leakage from private house
Loss/theft
4
Winny
Corporate USB
Centralized management
Downloading
3
Server
Use
Corporate PC
■ Theft/loss
1
Loss/theft
Transport
Mobile operation
■ Risk during storage
• Storage of unnecessary data
• Lack of encryption
3
Compilation of customer-related information
Exchanges with customers via the minutes, etc.
NEC's confidential corporate information
■ Incidents by contract firm employees
• Theft/loss
• Information leakage from a private house
Data entrustment
Out-of-premises work of contract firm employees
Corporate PC
Corporate USB
Loss/theft
6
Winny
Private PC
Private USB
■ Inappropriate duplication by a contract firm
5

Fig. 1 Information exchange routes and leakage risks.

from project servers.

3) Information is duplicated or processed as required before it is finally handed to the employees of the contract firms.

4) Absence of protection of the environment is one of the major causes of incidents (and increase of the consequent damage).

We have also identified that information is taken out in the following ways.

(1) In Many Cases, It Was Necessary to Take out Information for Use in Tasks.

① For development at the contract firms.

② For maintenance of the customer systems.

③ For delivery of the data to the customers.

(2) There Were Many Cases in Which the Necessity of Taking Information out Was Admitted But Information Was Taken out Without Observing the Related Rules.

① Taking out without following the official procedures.

② Taking out without leaving a record.

③ Use of private PCs or mobile devices.

(3) Cases in Which Information That Is Not Necessary for Tasks Is Taken out and the Files Are Stored in PCs, Thus Contributing to Spreading the Damage.

① Taking out all of the information regardless of its necessity or non-necessity.

② Retention of redundant information without deleting it.

System Objectives

Based on the above analyses, we set as our objectives for the NEC Group, the implementation of a system that provides the following functions designed to prevent information leakage incidents.

(1) Coverage of All Firms and Organizations Handling Information of the NEC Group

These should include the NEC Corporation, affiliated firms, cooperating firms and sub contract firms.

A systematic countermeasures should be implemented to manage information exchanges with contract firms and subcontractors, for which no effective measure exists in the past.

(2) Management throughout the Information Lifecycle

The system should protect information throughout the lifecycle from input/compilation to utilization/storage and return/disposal, and should also be capable of management and the tracing of information.

Efforts toward Information Leakage Prevention by the NEC Group -Information Leakage Prevention System "ARGUS" -

(3) Integrated Information Management and Fail Safe Measures

The system should protect information that must be stored in file server/storage services and manage them properly. Only that information required for specific work should be downloaded for use when necessary. Non-encrypted files should be encrypted/encapsulated automatically.

(4) The Use of IT for the Enhancement of Governance of the NEC Group

The system should enable enforcement of management policies with regard to information and mobile device. It should also be capable of centralized management of PC usage and file access logs and of retrieving them as required.

Functions and Configuration of ARGUS

ARGUS is composed of; (1) ARGUS Clients; (2) ARGUS servers; (3) Corporate ARGUS Center and; (4) file server/storage servers (**Fig. 2**).

(1) ARGUS Client

The ARGUS Client is installed in each of the management targeted client PCs. It executes user operation monitoring, USB device control, file encryption/encapsulation, file transfer to file server/storage server and recording of file operation logs according to the policies distributed by the ARGUS policy management server.

A file created on an ARGUS Client is given an attribute that inhibits any person other than the file creator from opening, so that no third party can open the file even if it is leaked.

For a case in which it is required to share a created file, the file is placed in a “confidential folder.” As a result, the file is given an attribute that permits only specified persons to open, and encrypted/encapsulated and stored in the file server/storage server.

The ARGUS Client also features a special encryption/encapsulation function (export function) for information handed over to contract firms. This function makes it possible to hand over a file only for use in a specified environment by specifying the environment. The file cannot be opened in a non-specified environment so that further leakage of information can be prevented.

(2) ARGUS Servers

The ARGUS servers include log management servers, policy management servers and file management servers.

The log management servers collect logs from PCs periodically and store the logs in the corporate log management

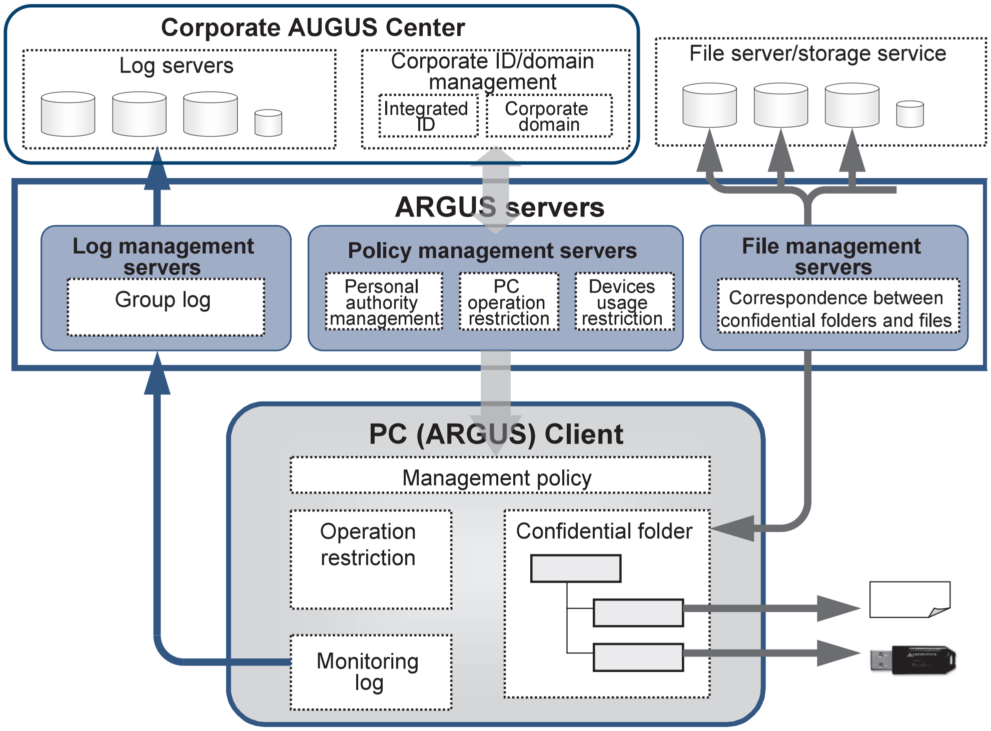

Fig. 2 Functional configuration of ARGUS.

server.

The policy management servers download management policies to the managed PCs in order to enforce divisions rules. For example, it can force the control for inhibiting the use of USB devices other than those specified by the corporation by distributing a management policy.

The file management server maps the linkage to the virtual folders in the ARGUS Clients with the file server/storage services that are the actual file storage locations.

(3) Corporate ARGUS Center

The Corporate ARGUS Center performs centralized management of the logs and the governance of the whole NEC Group. The ARGUS servers manage the personnel (IDs) by linking with the corporate ID/domain management.

(4) File Server/Storage Service

This is the location for storing the files that have been encrypted/encapsulated by the ARGUS Clients. The operations on encrypted/encapsulated files are recorded in the operation logs.

Effects of Introduction

Table below shows the risk control measures implemented by ARGUS for each of the risks depicted in Fig.1.

The basis of management by ARGUS is to store encrypted/encapsulated files in safe servers and to take out the required information only for the required period.

In other words, the management by ARGUS begins with storing whatever information is acquired in a secure PC or mobile devices temporarily and then storing it in the file server/storage server via the ARGUS servers. This enables effective management and tracing to be performed by ARGUS.

Table Risk control measures of ARGUS.

No.	Risk	Risk Control
①	Theft/loss	■ Encryption/encapsulation of all the customer information, personal information and confidential corporate information to prevent opening by a third party. ■ Permission to use only those USB devices specified by the corporation.
②	Data leakage	■ Permission to connect only those USB devices and peripheral devices specified by the corporation. ■ Monitoring of operation logs for the detection and recording of illegal operations.
③	Risks during storage	■ Forced encryption of non-encrypted files. ■ Automatic file deletion according to the terms of storage.
④	Information leakage from private houses	■ Encryption/encapsulation of all the customer information, personal information and confidential corporate information in order to prohibit opening by a third party.
⑤	Inappropriate duplication by contract firms	■ Encryption/encapsulation of exported information. ⇒ Usage permitted only in approved environments.
⑥	Incidents by contract firm employees • Theft/loss • Information leakage from private house	■Encryption/encapsulation of all customer information, personal information and confidential corporate information to prohibit opening by a third party. ■Encryption/encapsulation of exported information.

Future Plan

NEC began the preliminary introduction of ARGUS in selected departments during the latter half of FY2006. Following its introduction in support of projects with an especially high information leakage prevention requirement during FY2006, we plan to first of all start full scale domestic introduction in FY2007 followed by introductions through the entire NEC Group.