Implementation: Oct. 2005

NTT DATA Successful Implementation of X-FORT

*X-FORT rename as TotalSecurityFort in Japan

NTT Data Coporation

Section Manager of NTT DATA, Masaki Yamaoka

Former Section Manager of NTT DATA, Inoue Katsushi

NTT Data is the top system integrator in Japan and was formerly the computer department of Nippon Telegraph and Telephone Corporation. It is currently still a member of the NTT Group. NTT Data had two major information security incidents in the past and was immediately required to implement solutions to prevent such incidents from occurring again. Hence, NTT Data selects information security products by insisting that "NTT Data will not be able to continue doing business if it cannot develop a way to manage data that is written to external storage devices".

Background and information security concept

Mr. Inoue: NTT Data had two major personal data leaks in the past. The first was on December 10, 2003 when a contractor's laptop containing customer information was stolen. Even though the data leakage incident was before the Personal Information Protection Act took effect, we still implemented concrete and thorough measures for personal information management. We also reduced the number of personnel with access rights and actively provided employee training, using comprehensive measures to prevent data leakage incidents from occurring again.

Unfortunately, a second data leakage incident occurred in May 2005. This time the incident did not involve customer information, but rather the information of NTT Data employees. The data leakage was caused by a common flash drive being lost. From these two data leakage incidents we learned the lesson that "we must have comprehensive prevention measures, even if it means spending money." This is because simply

implementing our information security policy did not produce ideal results, and instead became a burden and caused fear among employees. Another important issue is that "internal information control must be properly implemented", whether or not writing/bringing out data is allowed must be correctly determined to control our information flow. Flash drives with large storage capacity, in particular, can be used to store a variety of information, but it is hard to determine exactly what information was stored once the flash drive is lost.

Information is an important asset to enterprises. These assets allow enterprises to further increase its work efficiency, productivity, and innovation abilities, and also create new customer value. Information needs to be properly managed and correctly used. Incorrect use or accidentally handing it over to persons without access right may result in substantial loss. Hence, a key point of information security is to find a balance between two seemingly conflicting conditions using high standards. Every company in the NTT Data Group shares the same information security concepts, and strives to ensure the overall group's information security, so as to correctly share and use information.

Key factors of solution selection

Both data leakage incidents were caused by a flash drive, which can easily store over 10,000 entries of personal information. Hence, the top priority when selecting a solution is restricting the writing of data to external storage devices (including CD-ROMs). Furthermore, employees may have administrator permissions in Windows, which will allow them to easily remove control software; but not giving users administrator permissions will make it difficult for them at work. Therefore, control will only be meaningful if there is a powerful system that gives users administrator permissions but prevents them from removing restrictions, and when all external storage devices, Internet access, and Bluetooth can be controlled.

Mr. Inoue: Putting a blanket ban on writing data is not feasible at work. Companies in the group can use a file share server for specific customers, but it isn't that easy when it comes to regular customers. If it is necessary to take out data for work, an appropriate person should be responsible for review, and the time that approval is given must be documented. Salespeople can simply fill out an application form and affix the seal of approval. But this approach will not be strictly executed after a few days, and the following situations may occur: "Let me complete the application form later!" or "I need to go out now, it's not a big deal if I come back later for the seal of approval!" If a data leakage incident were to occur at this time, we would not be able to clearly explain the cause.

Having an automatic recording function is extremely important if we want to clearly know what information was leaked in a data leakage incident. Even though backing up and recording the contents of files that are written each time is also a feasible approach, it will only make work more difficult than it needs to be. Also, it would be even better if the files were written with the approval of the supervisor on other devices or via electronic review. When selecting a solution, X-FORT was the only solution capable of providing all of these functions.

X-FORT allows security rights to be flexibly set based on the work requirements of different employees. Besides prohibiting all access, it also allows information to be brought out when necessary. X-FORT

achieves a delicate balance between ensuring information security and allowing correct use and sharing of information.

Other factors of solution selection

Mr. Inoue: We didn't notice the variety of functions offered by X-FORT until after we began using it. In addition to general control functions, it also has remote control functions with file deployment for executing programs on users' computers, and also for managing computer software and hardware assets. It is a comprehensive solution with complete functions, and that is one of its greatest features.

At the time, we planned to complete implementation within six months. NTT Data is a special company and its R&D Department uses numerous domains, which are not necessarily centrally managed, so a considerable number of X-FORT servers are needed for management. Since the number of computers installed with the client end is in the tens of thousands, integration of the client end is not an easy task either. The key to shortening the time for implementing X-FORT is its centralized and intuitive management interface that enables flexible and detailed control. Administrators can user their mouse to check items and set access rights on the control panel of the graphical interface. Individual and organization access rights can be set based on the system environment and applied to computers and users. Software agents can even be remotely deployed, simple and fast. (Installation on 500 computers only takes about 50 minutes using remote operations. The actual results may vary with the environment.)

Explanation and announcement to employees

Mr. Inoue: X-FORT has a wide variety of functions and allows various records to be accessed. Almost all computer operations can be recorded. Some people will still ask: "Is this system used by companies to manage employees?" From a company's perspective, the system reduces the risk of data leakage, and allows the company to verify the channel of information outflow when a data leakage incident occurs. We want to let employees understand the meaning of implementing an information security system, and tell our employees that "This system was implemented to protect employees". If a data leakage incident occurs, employees will be able to explain the act of "bringing out information" was due to work requirements, and we will be able to know what data was written. Employees do not need to try to remember exactly what data was written, reducing unnecessary trouble and lifting the burden on them mentally. The advantage of implementing X-FORT is that it protects employees and the company at the same time.

Overview and results of implementation

Mr. Yamaoka: X-FORT was installed on about 30,000 computers as mentioned above, expanding from Tokyo throughout the nation. In addition to the basic network, there are also many departmental and R&D networks, so the number of X-FORT servers exceeds 200.

Mr. Yamaoka: With regard to applications, the reading and writing of data on external storage devices

such as flash drives are categorically prohibited. However, when there is no choice but to use flash drives, permission may be obtained from the manager to use flash drives. X-FORT has an audit function that can be used to send records back to the X-FORT server, so that records of data writing, Web browsing, software installation, and hardware changes can be accessed from the file server. It can also control the execution of P2P software such as Winny and Share. Different user rights can be set for control or records based on different situations.

Mr. Yamaoka: Portable storage devices such as flash drives are almost never used in the company. Before implementing X-FORT, small portable storage devices were frequently used and losing such devices created the possibility of data leakage. Employees were unable to use flash drives after X-FORT was implemented, and they thus began considering how to safely transmit information. This not only reduced the risk of data leakage caused by losing storage devices, but more importantly caused every employee to consider how to safely use information.

Mr. Inoue: The effective use of X-FORT naturally prevents data leakage and unintentional data writing. It is also very useful for keeping records during work. In other words, if the writing of data was reviewed and carried out according to work procedures, then “when,” “who,” and “what” data was written can be proven. It can also be used to prove that someone didn't do anything wrong. Only one entry out of many records needs to be found to prove that something wrong was done, but all records need to be accessed and reviewed to prove that nothing wrong was done. For example, X-FORT can access execution records of different programs to prove that prohibited applications were not executed. Also, X-FORT can access files read/write records and file operation records through My Network Places, and can also record file access by monitored users on the file server to prove that no files were copied. F

** Reference from Japanese version.*