Practical Introduction of CoreBoot® and STRAGEX

Kenji Motohashi†*, Kimihiro Iwasaki, Akira Yonahara, Akihiro Hayakawa, and Masaomi Nakajima*

Abstract

This article introduces CoreBoot®*, a network booting thin client commercial product that prevents information leaks, reduces operating and management costs, and provides high usability. It also describes the STRAGEX system, which served as the basis of CoreBoot and was introduced internally at NTT Data as a trial.

1. CoreBoot

CoreBoot is a network-booting thin client product that uses an iSCSI (Internet small computer system interface) storage system. It is a functionally enhanced version of the STRAGEX system developed by NTT Information Sharing Platform Laboratories, but made simpler and more convenient.

2. CoreBoot features

There have been numerous information leak incidents in recent years, so sufficient measures against information leaks must be taken because they can have major effects on a company's trustworthiness and credibility, and hence on its continued existence. However, measures taken to prevent information leaks usually increase the company's operating and management costs. Furthermore, some security systems may interfere with the proper operation of applications and peripheral devices and thus reduce usability. CoreBoot solves this problem by providing functions that prevent information leaks, reduce operating and management costs, and achieve high usability.

2.1 Prevention of information leaks

CoreBoot prevents information leaks in three ways: (i) it is a diskless system, having no local hard disk, so information cannot leak when a personal computer (PC) is lost or stolen; (ii) the use of floppy disk drives, USB (universal serial bus) drives, and other such devices can be restricted, so that unauthorized removal of information via external memory devices is prevented; and (iii) central management of programs prevents failures to apply operating system (OS) or security software patches, so the latest anti-virus measures are always in place. A breakdown of the causes of information leaks and those that CoreBoot can prevent is shown in **Fig. 1**. Introducing CoreBoot can eliminate the causes of about 70% of all information leaks.

2.2 Reduction of operating and management costs

CoreBoot reduces operating and management costs by applying maintenance results on a single Core-Boot terminal to all of the terminals, accomplishing instant setup of a new CoreBoot terminal, and keeping data in a central storage device so that data backup and recovery is simple. Moreover, the server is accessed only during boot-up; after booting, the

---

† NTT DATA Research and Development Headquarters
Koto-ku, 135-8671 Japan
Contact: coreboot@am. nttdata.co.jp

* CoreBoot® is a trademark of NTT Data Corporation in Japan. The corporate names and product names that appear in this article are the trademarks or registered trademarks of the respective companies.
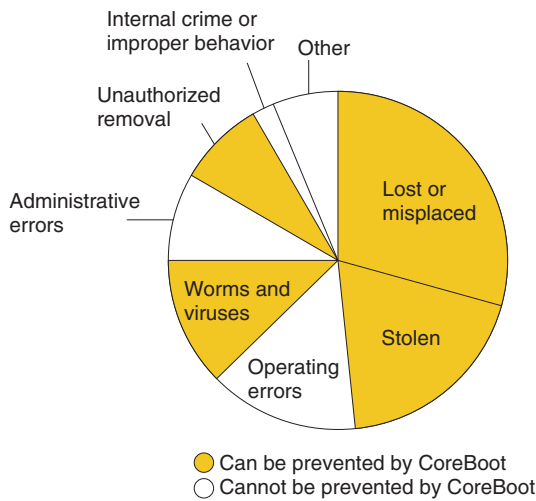
*Japan Network Security Association
From the 2006 Information Security Incident Survey Report in Japan

Fig. 1. Causes of information leaks and proportions prevented.
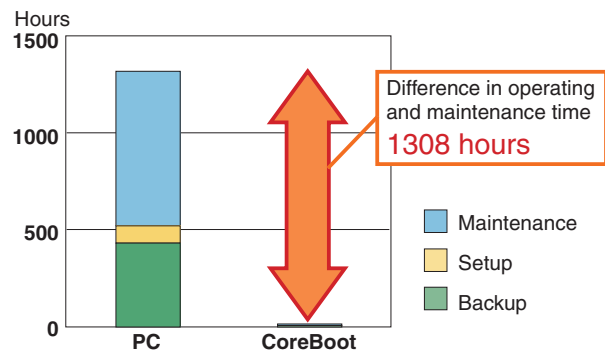

Conditions

Maintenance
-Security patches for OS or application.
-Applications are upgraded or installed once a year.

Setup
-There is an annual 10% turnover in users due to personnel changes.
-20% of the terminals are replaced by new ones during the year

Backup
-OS snapshots and data backup are done once a week.

Fig. 2. Reduction in operating and maintenance time.

only direct access is to a highly reliable storage device, so system downtime is greatly reduced. The results of a CoreBoot trial calculation involving the operation and management of 100 PCs and 100 users over a period of one year are shown in **Fig. 2**. The introduction of CoreBoot reduced operating and management time by 1308 hours over the year.

2.3 Good usability

With CoreBoot, applications run by making the greatest possible use of the central processing unit, memory, and graphics card on a diskless PC, so processing-intensive applications that have complex screen output, such as three dimensional computer-aided design (3D CAD) programs run without problems. Peripheral devices such as scanners and handsets also operate without problems because the applications run on a diskless Windows-based PC. Furthermore, the system lets users access their own 'My Documents' folder and desktop environment, no matter which CoreBoot terminal the user logs in on.

3. CoreBoot application fields

CoreBoot is most effective in an environment where there is control over the applications and types of terminals used, such as a CAD environment, a call center, or the computer room of a school or university. Of those application fields, it is best suited to the CAD environment, which requires a high-performance, high-reliability, and high-definition system.

4. CoreBoot development

When developing CoreBoot, we listened to the opinions of customers and the people that constructed and operated the STRAGEX system, and we added the following functions to make a mature commercial product.

4.1 Redesigned user interface

We worked together with our in-house user interface design team to develop an administration screen that can be used even by unskilled operators. First, we identified the characteristics of CoreBoot management of the OS, terminals, and user information, and we optimized the menus and input of information from the operator's viewpoint. We also introduced a universal design to achieve an intuitive user interface.

4.2 Integration of the storage functions

Previously, the operator had to use the administration screens of both STRAGEX and the storage device, but CoreBoot integrates the backup and data restoration tasks, which are essential to system operation, into the CoreBoot administration screen. As a result, the operator can perform all operations from the CoreBoot administration screen alone, which simplifies the system operation task and eliminates mistakes in the operation of the storage device (**Fig. 3**).
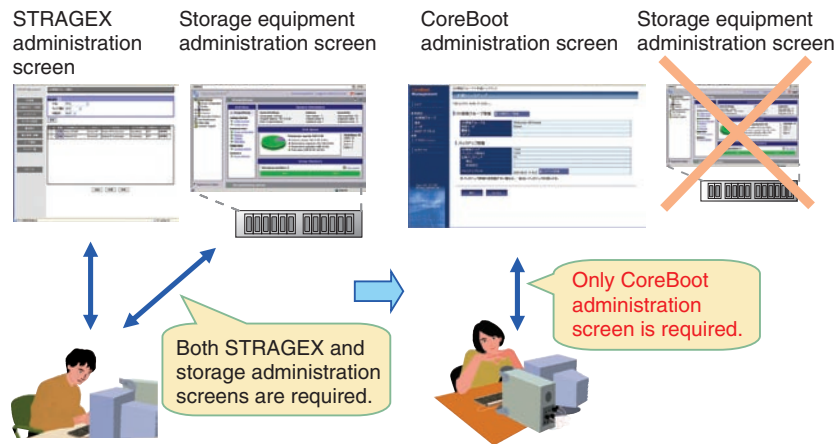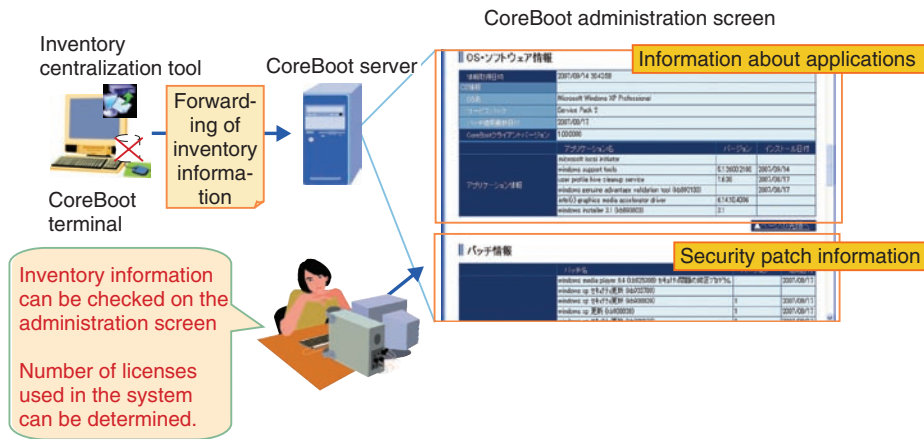
Fig. 3.   Integration of storage function.

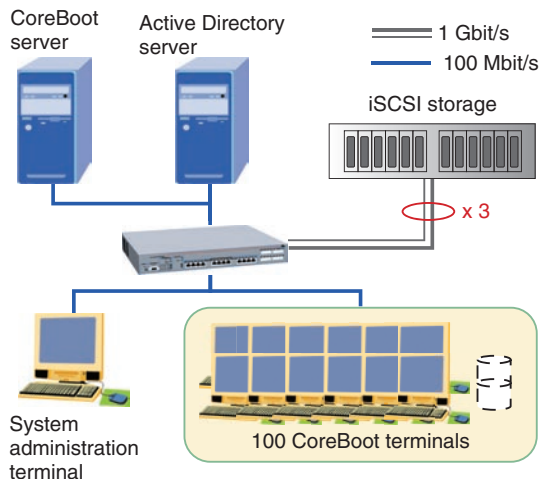Fig. 4.   Addition of inventory function.

Fig. 5.   CoreBoot system configuration example.

4.3   Addition of an inventory function

The operator manages the OS and the applications, so he or she must understand their installation and know about security patches. CoreBoot adds to the administration screen a function for aggregating and listing information such as the types and names of machines, application names, and Windows security patches (**Fig. 4**). The CoreBoot administration screen can also display the number of terminals on which each application is installed so that the operator can quickly and easily determine how many licenses are being used.

5.   CoreBoot configuration example

A system configuration example with 100 Core-Boot terminals is shown in **Fig 5**. For ordinary office work, a single iSCSI storage unit can handle up to

Table 1.   CoreBoot operating environment.

| Coreboot server	OS	RedHat Enterprise Linux 5.0
Active Directory server	OS	Windows Server 2003
iSCSI storage	Product	Dell EqualLogic PeerStorage series
System administration terminal	Browser	Internet Explorer 7
CoreBoot terminal	OS	Windows XP Professional SP2 Windows XP Professional x64 SP2
	Network	PXE 2.1-compliant network interface card (100 Mbit/s or faster)
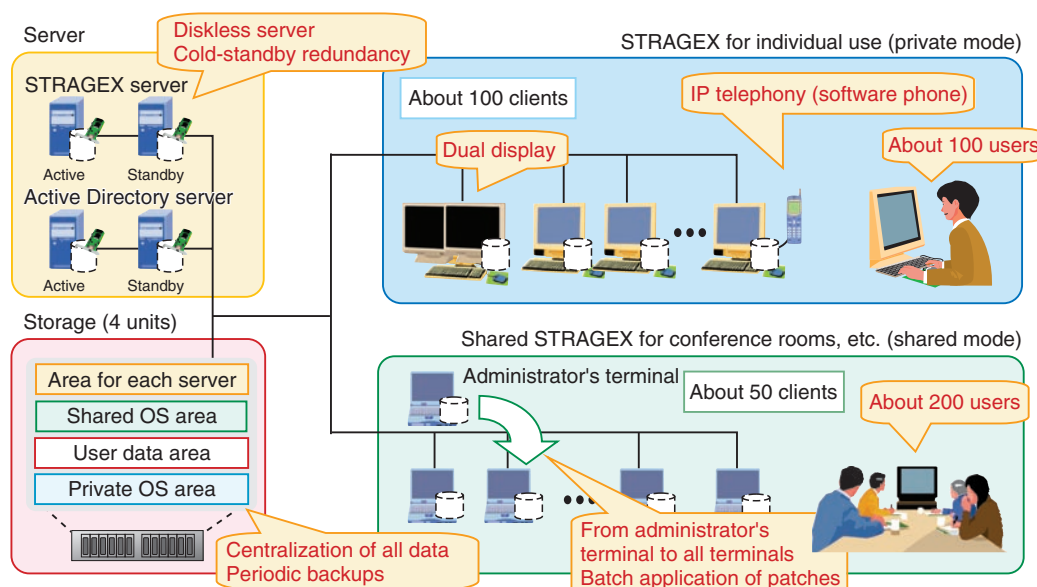
Fig. 6.   Configuration of the Toyosu Building STRAGEX system.

100 CoreBoot terminals. A line capable of at least 100 Mbit/s is recommended for the link between the CoreBoot terminals and the switch.

The specifications of the CoreBoot operating environment are given in **Table 1**. CoreBoot is compatible with the Dell EqualLogic PeerStorage series of highly reliable iSCSI storage systems. In addition, the CoreBoot terminals are not dedicated hardware, but ordinary Windows-based PCs that have had the hard disk removed.

6. Introduction of STRAGEX at NTT DATA

About 150 STRAGEX terminals were introduced in a trial at the NTT DATA Toyosu Center Building Annex (Toyosu Building) on October 16, 2006. Currently (January 2008), about 200 persons in the Research and Development Headquarters are also using the system. The system configuration is shown in **Fig. 6**. The main objectives of introducing STRAGEX were to build up experience with a large-scale STRAGEX deployment and to implement a new work style and work place (WS & WP).

Since we previously had no experience of large-scale introduction aimed at commercialization of the STRAGEX system, either inside or outside the company, we introduced about 100 STRAGEX terminals for individual use at the users' desks as an example of large-scale introduction with the dual purpose of gaining experience at introducing large-scale systems and promoting the use of the system. At the same time, a working group for revising the style of office work was set up in an office of the Data Research and Development Headquarters with the objective of implementing a new WS & WP, so secure and easily managed PCs had to be installed in conference rooms and other shared spaces. Therefore, we proposed the installation of STRAGEX terminals and set up about

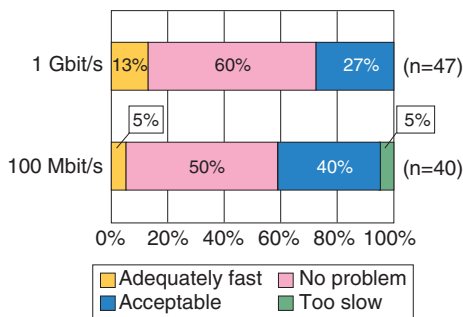Fig. 7.   STRAGEX terminals in a shared space.

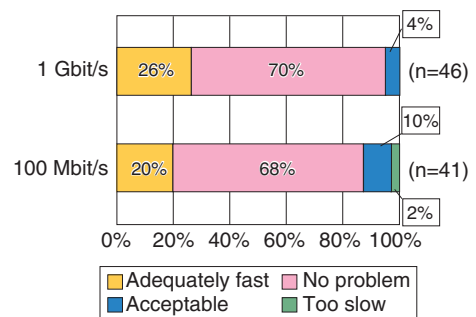Fig. 8.   Questionnaire results for startup time.

Fig. 9.   Questionnaire results for terminal speed.

50 STRAGEX terminals for shared use.

Below, we describe how the introduction of the STRAGEX system in the Toyosu Building prevented information leaks, reduced operating and management costs, and provided high usability.

6.1   Prevention of information leaks

The shared STRAGEX terminals were installed in shared spaces (**Fig. 7**), so there was some risk of theft or loss. However, because STRAGEX terminals do not have hard disk drives, the theft or loss of a PC did not lead to any information leakage. In addition, since the administrator enforced the application of security patches and the updating of virus definition files, there were no cases of infection by worms or viruses.

6.2   Reduction of operating and management costs

Operating and management costs were reduced as expected, and the time required for maintenance and setup was greatly reduced. However, the operators said that the STRAGEX system itself required spe-

cialized knowledge and operating experience. Another point was that the many operations to be performed on the administration screen of the storage device led to mistakes in operation. In particular, mistakes in the operation of the storage device system were fatal to the system, so the users requested improvements in that respect. We incorporated this feedback into Core-Boot when we decided to make an improved version of STRAGEX.

6.3   Good usability

To check STRAGEX for usability, we conducted a questionnaire survey of the users. In the results given below, *n* indicates the number of meaningful responses.

The results of the questionnaire given to the individual users of STRAGEX regarding the startup time and post-startup terminal speed are shown in **Figs. 8** and **9**, respectively. The values of 1 Gbit/s and 100 Mbit/s are the line speeds between the STRAGEX terminal and the switch. From Figs. 8 and 9, we can see that most responses regarding the startup time were "No problem" or "Acceptable". For the terminal
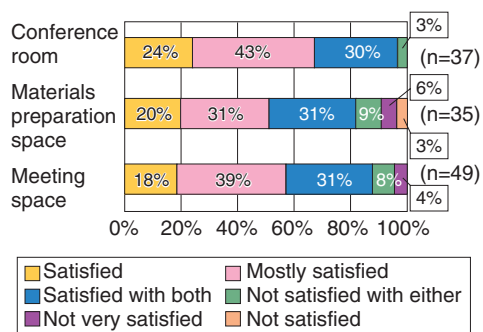
Fig. 10.   Questionnaire results for satisfaction.

speed after startup, nearly all of the responses were "No problem". In particular, most of the responses were that, after startup, the performance was not inferior to PCs that boot from a local hard disk for both line speeds.

The results of the questionnaire given to all employees of the Research and Development Headquarters concerning satisfaction with the shared STRAGEX system (**Fig. 10**) reveal that most were "Satisfied", "Mostly satisfied", or "Satisfied with both" cases. Most of the users said that they were able to access materials from meeting spaces without preparation or that they were able to use their own 'My Documents' folder and desktop environment from any STRAGEX terminal, so the effects targeted by the working group were achieved.

7.   Future development

We intend to promote CoreBoot aggressively to customers in the application fields that it is suitable for and we will aim for the top market share for thin clients in CAD environments in particular. For the next phase of development, we plan the achieve compatibility with NetApp storage systems and Windows Vista. There is a web page describing the functions of CoreBoot in detail [1].

Reference

[1]   http://www.coreboot.jp/ (in Japanese).

Kenji Motohashi
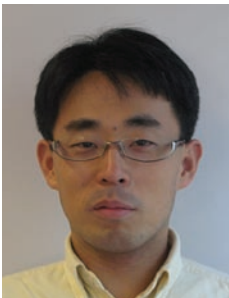Research and Development Headquarters, NTT DATA.
He received the B.E. degree in computer science and the M.E. degree in communications and integrated systems from Tokyo Institute of Technology, Tokyo, in 2003 and 2005, respectively. He joined NTT DATA in 2005. He has been engaged in developing thin client systems.

Akihiro Hayakawa
Manager, Research and Development Headquarters, NTT DATA.
He received the B.S. and M.S. degrees in mathematics from Tokyo University of Science, Tokyo, in 1991 and 1993, respectively. He joined NTT DATA in 1993. Since then, he has been engaged in research on QoS control in IP networks and network security.

Kimihiro Iwasaki
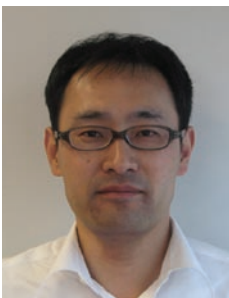Research and Development Headquarters, NTT DATA.
He received the B.E. and M.E. degrees in computer science from Tokushima University, Tokushima, in 1996 and 1999, respectively. He joined NTT DATA Research and Development Headquarters in 1999. He has been engaged in R&D of public key infrastructure and development of thin client systems.

Masaomi Nakajima
Senior Manager, Research and Development Headquarters, NTT DATA.
He received the B.E., M.E., and Ph.D. degrees in engineering from Waseda University, Tokyo, in 1986, 1988, and 1999, respectively. He joined NTT DATA in 1988. He has been engaged in R&D of multimedia systems and security platforms.

Akira Yonahara
Senior Expert, Research and Development Headquarters, NTT DATA.
He received the B.E. and M.E. degrees in engineering from Tohoku University, Miyagi, in 1996 and 1998, respectively. Since joining NTT DATA in 2004, he has been engaged in developing network security systems and thin client systems.