Smart Device Management/Security Solutions Regardless of OS or Carrier

SAITO Yoshihiko, NEZU Satoshi, ISHIBASHI Takeshi

Abstract

The rapid dissemination of smart devices in recent years has been changing usage from the initial personal use to business use. However, smart devices are often involved in incidents such as theft or loss, so terminal management and security measures are indispensable for business use. This has led to the growth of security management operations and has made them an important issue.

NEC supports enterprises introducing smart devices by preparing a comprehensive, far-sighted range of smart device management and terminal security solutions. This paper introduces details of these solutions.

Keywords

smart device, security, MDM, antivirus measures, Android, iOS
application management, 24h-365d contracted operational support, LCM, on-premise, cloud-based service

1. Introduction

As the business use of smart devices (smartphones and tablet terminals) is spreading, mobile device management (MDM) is now recognized as an indispensable management tool that is being actively introduced.

The market is now flooded with a large number of MDM products. Their functions are enhanced day by day and MDM coverage is also expanding. NEC's 3rd Carrier Services Division has commercialized the highly competitive MDM product (NC7000-DM Lite; hereafter "DM Lite") as part of our MDM business strategy, which also provides a cloud-based service using the DM Lite (NEC Mobile Security Pro; hereafter "NMSPro"). These product and service will be advanced continually in the future.

The characteristics of the DM Lite are described in sections 4 and 5 below, the NMSPro is described in section 6, and the NEC Mobile Security LCM (hereafter "LCM"), a service for the general support of smart mobile use by enterprises, is explained in section 7.

2. Market Trends of MDM

MDM was marketed originally as a security countermeasure to handle losses of smartphones and tablet terminals, following their increased business use, and its main purpose was to lock a terminal or to initialize (it clear data) remotely.

However, as the actual use of MDM increased among enterprises, the required functions did not remain simply as terminal locking or initialization. The operational requirements of the businesses to be conducted by enterprises were now added. Specifically, terminal status management, asset management and application distribution have now entered the category of MDM functions.

3. MDM at NEC

3.1 MDM product (NC7000–DM Lite)

In order to respond to the diversifying market needs, we commercialized an MDM product called NC7000-DM Lite and we are currently advancing its enhancement.

We have previously launched a server product (NC7000-DM) that is used for management and control of feature phones by communications carriers. This product has actually been operated in carrier-grade large-scale environments. It has been developed making full use of the "expertise (large-scale/large-capacity) of NEC, which has been continuing R&D for carrier-oriented businesses over many years." This expertise is also applied to NEC in-house and has led to the commercialization of the NC7000-DM Lite as a product that can be introduced in general enterprises as well as for communications carriers.

3.2 MDM Services

At NEC, we started provisions of two cloud-based MDM services based on DM Lite in February 2012.

(1) NEC Mobile Security Pro (NMSPro)

NEC 3rd Carrier Services Division implements the NMSPro (packaged solution service) as a menu supported service that does not need customization and enables immediate start up.

(2) Smart device management service

NEC IT Services Operations Unit implemented the Smart Device Management Service (SI type) with a menu that enables system integration (SI) such as linkages with business applications and backbone systems at the time of a service introduction.

4. Features of NC7000–DM Lite Product

The most useful four features of the DM Lite are the following (**Fig. 1**).

(1) Multi-user compatibility

The first is the multi-user compatibility. Since a "one terminal per person" environment is not always possible in enterprises, the need for shared use is very high, particularly among business terminals. The DM Lite is designed to authenticate each user of a dedicated home application and sets the usable applications and functions according to the authority of each user.

(2) Operations management functions in pursuit of usability

The second feature is the pursuit of usability of operations management functions. One example is the profile distribution function. Some MDM products set the profile information per each terminal.

However, in the case of the DM Lite, provided that a profile including the usable applications and security policy is set per department or group, a user belonging to a specific group can automatically apply that profile to the terminal he or she uses.

This is not only possible at the time of the initial setting. In the case of transfer or addition of employees, simply reflecting the information in the profiles, the latest profile is applied automatically thanks to the communication between the terminal and server. This system can reduce the operations management items and thereby reduce the operations load.

(3) Security enhancement by linkage with NEC terminals

The third feature is the linkage with NEC-made terminals. Specifically, linkage is possible with the MEDIAS, LifeTouch and business terminals.

In general, MDM controls devices using APIs (Application Programming Interfaces), which are made public by OS and terminal manufacturers. In such case, MDM can only control devices within the certain level of their performance.

An enterprise that requires particularly strict security can take stronger measures by adopting the combination of NEC-made terminals and the DM Lite, which is shown in **Fig. 2** .

The Inhibition of OS version upgrading and USB connection are also functions that are essential for business use in preventing illegal use. The collection of terminal usage logs is also one of the main functions of the MDM, and DM Lite is capable of collecting more detailed information than ordinary MDM systems.

(4) Anti-malware measures

The fourth feature is the anti-malware measures. The MDM terminal, application management function, antivirus function and URL block are integrated so that all can be controlled from a single console.

Should a virus be detected on a terminal, the notification is automatically displayed on the DM Lite management screen, so that the administrator can identify what is detected and at which terminal in real time.

Integration of the anti-malware measures and the MDM contribute greatly to a reduction in the management burden.

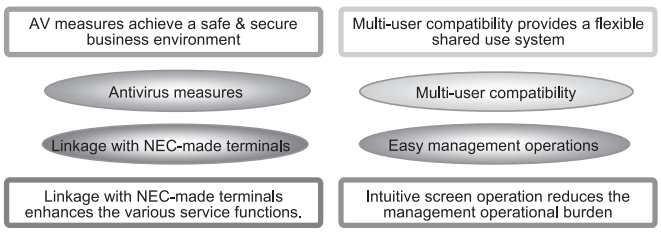

Fig. 1 Four features of DM Lite.

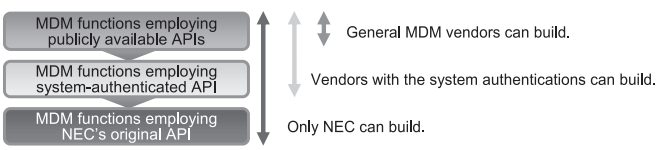

Fig. 2 NEC terminal linkage of DM Lite.

The anti-virus function and the URL block that are integrated with the DM Lite are the products of Webroot, Inc., which is an American software manufacturer. The Webroot products are highly evaluated for the absence of pressure on the device resources, lightness, quick search and low battery consumption.

5. Future of DM Lite

The following function extensions are planned for the DM Lite.

(1) Multi-device/multi-OS compatibility

The DM Lite is already compatible with Android and iOS terminals, and measures are being advanced for compatibility with Windows (it is planned to provide Windows with the lock function for use in the case of loss).

To make the DM Lite capable of providing the same wide range of features as the MDM system, e.g. the capability for taking quick measures in the case of the launch of a new terminal, or upgrading of an OS version, upgrading will be prepared.

(2) Prevention of iOS configuration profile deletion

Various MDM products for use in managing the iPhone and iPad are already marketed, but their common problem is that effective management becomes impossible if the configuration profile that requires to be controlled is deleted. Also, if the configuration profile is deleted, it is necessary to reconfigure the initial setting of the terminal. To solve this problem, the configuration profile deletion prevention function will be provided before the end of March 2013. This function will allow enterprise administrators to manage iOS terminals securely and safely.

(3) Quarantine function

Accessing corporate networks or systems from smartphones is increasing. For this case, the MDM alone is inadequate and a quarantine function is required.

DM Lite manages the profile application situation, and the terminal quarantine status, such as for a malware invasion, and prepares the web API according to the quarantine status. When it is linked with a quarantine server, the smart devices accessing the corporate network can refer to the quarantine status of the DM Lite for a quarantine check.

As an optional function, the DM Lite alone can disconnect the Wi-Fi connection when the quarantine status is NG (Not Good).

(4) Linkage with an authentication function

The user authentication of the DM Lite-dedicated home application can be linked to the authentication product (NC7000-3A) of the NEC's 3rd Carrier Services Division in order to implement a more secure environment. This linkage also makes it possible to implement single sign-on (SSO) and thereby improve the convenience of terminal users.

In addition to the authentication linkage, we are ready to plan linkages with both NEC and non-NEC products to offer solutions that can meet the needs of enterprises more effectively.

6. Features of NEC Mobile Security Pro (NMSPro)

The NMSPro is a cloud-based service, so customers do not have to prepare servers and other devices in order to introduce MDM. They can use the MDM service soon after they apply for the service. Even after introducing the MDM service, the fact that the NMSPro is a cloud-based service allows it to deal with an increase in the number of users without need for a server upgrade. Furthermore, when the LCM service described in section 7 is used, a speedier MDM introduction is possible without increasing workload.

7. Total Support of Smart Device Lifecycle

NEC offers the DM Lite as a secure product for smart devices and the NMSPro as a cloud-based service. However, for actual use by enterprises, the emergency lock function in the case of a terminal loss during non-business hours, as well as the policy establishment and terminal initial settings at the time of terminal introduction are additionally necessary.

NEC does not limit its products to the provision of solutions, but will also provide the LCM suitable for actual operations per enterprise for the total support of smart device lifecycles.

The LCM deploys the following menus

- Policy establishment support
- 24h-365d contracted operational support.
- Operations analysis
- Data recovery
- Terminal initial settings (kitting)
- Help desk

- Spare device provision
- Usage fee analysis

7.1 Introduction Support

One of the traditional issues in the introduction of smart devices in enterprises is the increase in the workload on the system department managing the smart devices.

When introducing smart devices, it is required to establish a smart device security policy and operations rules; and to perform kitting of the introduced terminals according to the business form and method of usage of the enterprise introducing them.

The LCM service has already been introduced in a wide variety of business types. Our SE specialists of the LCM support the establishment of an 'optimum policy' and 'operational rules' via their expertise.

For the kitting, NEC has expertise as a terminal manufacturer and also possesses large-scale kitting centers in several locations across Japan, so the introduction of even thousands of terminals is possible.

7.2 Operational Support

Even after the terminals have entered the operational phase, there are still many issues, so the system department of the enterprise should be ready to accept emergency notices day and night in order to prepare for emergencies; including the loss of a terminal by an employee. It is also necessary to prepare a system for handling inquiries from employees who are not yet accustomed to using smartphones.

The LCM can respond to terminal lock and wipe (data erasure) requests in the 24h-365d system by substituting the system department that manages the terminals. SE specialists offer technical support to enable safe, secure use of smart devices by all employees.

Other services additionally available include the arrangement of substitute terminals in case of a terminal failure, data erasure before terminal disposal, and terminal usage fee analysis.

Via menus offering various services, the LCD provides comprehensive support for safe, secure use of smart devices by all employees, while minimizing the workload of the system department that manages the smart devices.

8. Hybrid Solutions for Smart Devices

Many of the enterprises that have introduced smart devices are still only capable of using smartphones in reading E-mails and documents and in placing phone calls. To deal with this current status, NEC is planning to deploy the NEC Enterprise Suite (hereafter "ESuite"), which provides general enterprise solutions for smart devices developed besides the DM Lite/NMSPro, and is not limited to those in the security domain.

In addition to the DM Lite/NMSPro, the ESuite provides various solutions, including the NEC Cloud Authentication (authentication and ID management), the NEC Cloud Smartphone (virtual smartphone) and solutions that are applicable to enterprise systems, such as quarantine, VPN and asset management solutions, as well as the Smart Communicator Catch! (communication support,); which is a communication tool for promoting business efficiency improvements using smart devices (**Fig. 3**).

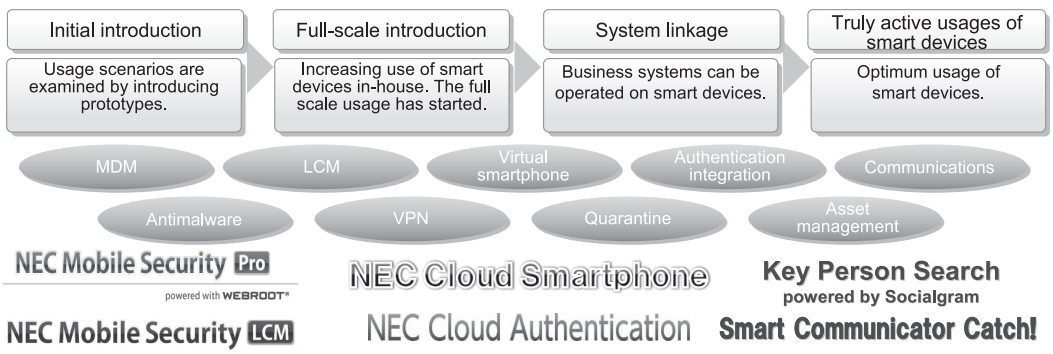

Fig. 3 Smart device introductory steps and correlations between solutions.

By combining these solutions, we offer comprehensive support for various usages of smart devices including the BYOD (Bring Your Own Device) in enterprises.

9. Conclusion

Smart devices free the work styles of employees from conventional work on PCs and deskwork and change them to those not restricted in location and time. This change is expected to give rise to widely variable new usage scenarios in realizing predictions. We intend to continue our technical development program in achieving an increasingly active usage of smartphones.

Authors' Profiles

SAITO Yoshihiko
Manager
3rd Carrier Services Division
Carrier Services Operations Unit

NEZU Satoshi
Manager
3rd Carrier Services Division
Carrier Services Operations Unit

ISHIBASHI Takeshi
Assistant Manager
3rd Carrier Services Division
Carrier Services Operations Unit

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese

English

Vol.7 No.3 Smart Device Solutions

Remarks for Special Issue on Smart Device Solutions
NEC Group Paves the Way for Smart Devices

◇ Papers for Special Issue

Service platforms

Smart Device Management/Security Solutions Regardless of OS or Carrier
Solutions Supporting the Utilization of Smart Devices: System Introduction Case Studies
Authentication Solution Optimized for Smart Devices
“Smart Mobile Cloud” Contributing to the Use of Smart Devices
“BIGLOBE Cloud Hosting” Supports Building of High Quality Services
“Contents Director,” Content Distribution Service for Smart Devices
UNIVERGE Mobile Portal Service: A Smart Device Utilization Platform Optimized for BYOD
Remote Desktop Software that Supports Usability of Smart Devices
SystemDirector Enterprise - A Business System Construction Platform to Facilitate Development of Applications Compatible with Smart Devices
Smart Device Content Distribution Platform Service Using the BIGLOBE Hosting

Smart devices

Overview of “LifeTouch” Series Android Tablets
VersaPro Type VZ - A Windows 8-based, Large-screen Tablet PC
Development of an Android-based Tablet(Panel Computer series)

Solutions

ConforMeeting: A Real-time Conference System Compatible with Smart Devices for Conducting Paperless Meetings
BusinessView Maintenance Work Solutions Utilizing Smartphones
Application of the UNIVERGE Remote Consultation Solution to Elderly Care
Introduction of the GAZIRU Image Recognition Service
Tablet Concierge- An Ultimate Customer Service Solution -
Development of a Business Systems Template for Use with Smart Devices
Introduction of Video Communications Cloud Services Compatible with Multiple Devices

Technical researches

Towards a User-Friendly Security-Enhancing BYOD Solution
Implementing Secure Communications for Business-Use Smart Devices by Applying OpenFlow
Human-Computer Interaction Technology Using Image Projection and Gesture-Based Input
Noise Robust Voice UI Technology and Its Applications

◇ General Papers

Efforts to Solve the Congestion Problems of Mobile Communications Services during Major Natural Disasters

Vol.7 No.3
March, 2013

Special Issue TOP