Secure Mobile Work Solutions That Exploit EMM

OIKAWA Tsuyoshi, YOSHIDA Kazumi

Abstract

To promote the Work Style Reform proposed by Japan's Abe administration, an ICT environment must be created that will allow people to work flexibly using various devices no matter where or when. However, it is expected that such a work style will increase the risk of cyberattacks, which makes sophisticated cyber-security critical to this endeavor. In this paper, we will discuss enterprise mobility management (EMM) solutions that ensure safe, reliable mobile work using smart devices. To illustrate how such a solution would work, we will review our own in-house case study, in which EMM was introduced at NEC.

Keywords

mobile security, mobile work, Work Style Reform, EMM, MDM, encryption

1. Introduction

The Abe administration in Japan is currently promoting what it calls Work Style Reform whose goal is to achieve dynamic engagement of all citizens. Many companies have already committed to pushing through this reform in their own workplaces and have begun to take measures to facilitate it, focusing in particular on mobile work that utilizes mobile devices and cloud services.

By introducing mobile work, companies will be able to offer diverse work styles to their employees. They can expand the spectrum of work styles by allowing their employees to work no matter where they are - which is ideal for workers unable to commit to fixed working hours due to the need to care for children or elderly parents, as well as for sales reps who need to access in-house resources from outside, just to name a few.

However, there are concerns that the introduction of mobile work may - in exchange for the improved convenience that it provides workers - pose security risks in the form of potential virus infection, data theft and loss of devices. This issue is now proving worrisome for information system administrators at many companies.

The ActSecure Mobile Platform Service Powered by VMware AirWatch (hereinafter referred to as the "Mobile Platform Service") that we will discuss in this paper is a service that helps achieve comprehensive management of a wide range of different devices and applications utilized for mobile work, while offering both convenience and security.

2. Overview of the Service

The Mobile Platform Service is an enterprise mobility management (EMM) service that integrates mobile device management (MDM) - which controls device conditions and system settings, mobile application management (MAM) - which controls applications used in devices, and mobile content management (MCM) - which protects local data and content.

It is compatible with a wide range of operating systems (Android, iOS, Windows, Mac OS, BlackBerry, etc.), and can be managed on a unified platform in an integrated fashion.

At the same time, users will be able to securely access the email accounts, address books, and schedules they

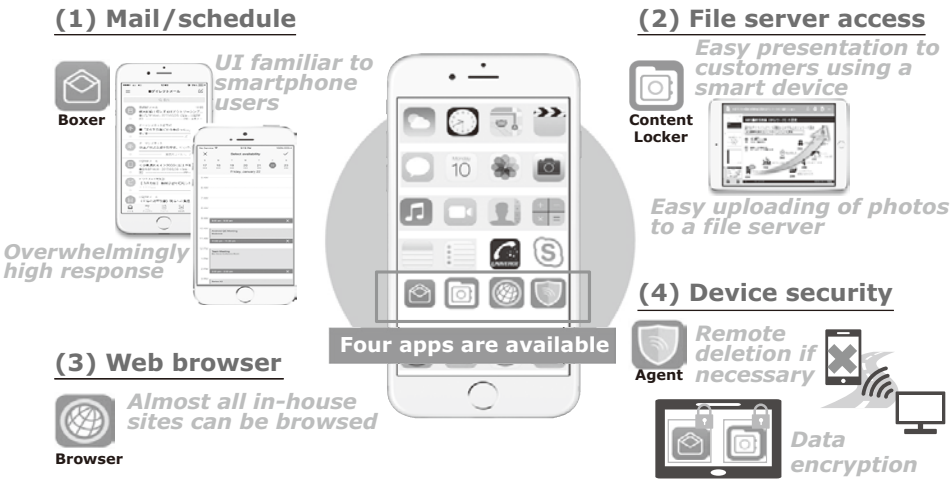

Fig. 1 Overview of the service used in-house at NEC.

use at the office via dedicated applications, thus improving operational efficiency.

As will be discussed in section 5 below, as part of NEC's commitment to the Work Style Reform we have decided to utilize the functions of this service in-house at NEC as a device management platform. We introduced the service on June 19, 2017 (**Fig. 1**).

Market demand for EMM has been rising every year, and it is expected that demand will continue to grow in the future. Given these market conditions, NEC plans to make this service available to its customers in the near future. The details and features of the service are described below.

3. Features of the Service

The features of this service are described below.

(1) Plentiful compatible devices

The policy commonly known as BYOD or "bring your own device" - which encourages employees to bring their personal devices to their workplace - has become increasingly widespread. As a result, the types of devices used for work at any given company have multiplied rapidly, creating headaches for administrators as they try to develop robust systems to manage all these different devices. The result is increased stress on servers as the number of processes grows and a decline in the level of security for each device.

Our Mobile Platform Service is compatible with a tremendous number of devices and operating systems. It makes it possible to provide standardized security levels for numerous devices - including BYOD devices - on a unified platform. The service is also built to respond immediately to OS updates, so changes to any device will not affect how it is managed.

(2) Secure utilization of mobile devices in an offline environment

When the dedicated apps offered by the Mobile Platform Service are used, data such as mail and files are stored in the mobile device's local memory. This allows users to access the data even when they are in a weak signal environment or on an airplane, for example.

System administrators are not normally inclined to look favorably on the idea of storing critical data in the local memory of mobile devices as it vastly increases the risk of information leakage. However, the dedicated Mobile Platform Service apps all comply with FIPS 140-2, and data stored in local memory are protected by AES 256-bit encryption, achieving a configuration with high security.

Security can be made even more robust by making passcode entry mandatory whenever a dedicated app is used. Since the encrypted data cannot be viewed in any app other than the dedicated app, security is maintained even if the data is leaked (**Fig. 2**).

(3) Universal device administration policy

The downside of the anytime, anywhere work environment made possible by mobile devices is that it can easily lead to employees being overworked as they find themselves forced to work overtime in order to complete a specific task for which they are responsible. The excess physical and mental stress caused by overwork can lead to fatigue, burnout, and other health issues.

As will be discussed in section 4 below, our Mobile

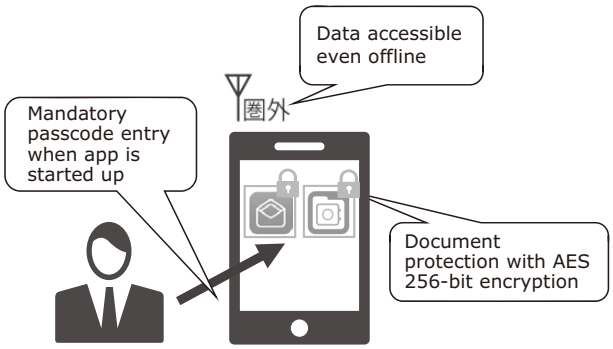

Fig. 2 Features available when browsing data.

Platform Service can restrict the use of specific functions and applications according to time and location, making it possible to prevent overwork.

Another problem inherent in mobile work is that unfettered use of mobile devices at work by employees can create vulnerabilities, leading to security-related accidents.

To deal with this, the Mobile Platform Service enables the administrator to set in detail the policies with which the connected devices must comply. For instance, the administrator can fine-tune the settings such as requiring password entry to lock the device, making passwords eight characters or more mandatory, and prohibiting the rooting of Android OS or the jailbreaking of iOS - both of which remove user privileges and enable software to operate in a way not intended by developers.

4. Details of the Service

So far, we have reviewed the features of the service. In the following section, we will examine the functions of the Mobile Platform Service in more detail.

(1) Mobile device management (MDM) functions

MDM functions include remote wipe and remote lock which are typically used when the device is lost, as well as restriction of usable functions depending on time and location. In other words, the administrator can fine-tune operations on the device side according to company policy. For example, it is possible to prohibit picture taking (camera functions) in specific premises and emailing outside business hours.

The Mobile Platform Service also offers a portal site called the Self Service Portal (SSP), which allows users to perform remote wipe and remote lock on their own.

If a user loses their mobile device, this helps reduce the risk of information leakage by reducing the time until the data on that device is deleted - something that tends to take considerable time conventionally - while reducing the number of jobs that administrators have to handle.

(2) Mobile application management (MAM) functions

A dedicated user application called App Catalog allows administrators to install various required applications and business applications developed in-house on a standardized platform, while being able to manage installation conditions and version information in detail. As long as the devices are owned by their companies and compatible with automatic installation and update, the administrators can set the devices so that specified applications are automatically installed and updated - which will reduce the user task load.

To help prevent information leakage, MAM can prohibit installation of specific applications and can also restrict data exchange between business applications and personal applications, thereby helping improve security.

(3) Mobile content management (MCM) functions

A variety of MCM functions are available, including one that lets users browse files stored on in-house servers and one that lets them browse sites on intranets. The former is achieved by the dedicated viewer application called Content Locker, which uses the previously discussed encryption method. Using Content Locker, users can browse local files securely even when offline. For secure access to sites on intranets, users can use a web browsing application called VMware Browser.

While it is commonly believed that the best way to ensure security is simply to avoid storing data on mobile devices altogether, the Mobile Platform Service is based on the concept that security can be ensured by properly encrypting data on mobile devices. This allows employees to take full advantage of the improved convenience - including offline usability - that downloading to mobile devices offers without compromising security.

5. In-house Introduction at NEC

As already mentioned in section 2, the functions of the Mobile Platform Service were deployed at NEC on June 19, 2017 and have been in use ever since. The details of the service and its introduction are discussed below.

(1) Reasons for the introduction

In recent years, the need to be able to use smart devices in places where the network environment is unstable - for example, during overseas business

trips - is increasing, This prompted NEC to look at ways to realize a secure, mobile-compatible service that would enable users to use their mobile devices anytime, anywhere, without compromising security. At the same time, NEC group member companies - including ones overseas - were pushing for a standardized platform that would streamline operations and facilitate data sharing. To meet these various needs, we decided to introduce the Mobile Platform Service because it was able to offer both the convenience of offline usability and the flexibility of global usability.

(2) Scope of usage and terminals

All employees, including NEC group company employees, can use this service. As for the terminals, both company-owned devices and BYOD devices are supported. However, a BYOD device can only be deployed only after the implementation of comprehensive security measures that meet the same security standards applied to company-owned terminals, and after the devices have been configured to ensure that confidential personal information cannot be collected from those devices.

(3) NEC in-house policies incorporated in the service

In addition to mandatory security requirements such as device password setting and storage encryption, we are also trying to improve convenience by ensuring that intra-office wireless LAN profiles are automatically distributed so that when users enter the offices, their devices are automatically switched to in-house wireless LAN.

We believe that this service has had a significant impact on convenience. As a matter of fact, we are now receiving comments from employees of various NEC group companies, saying that efficiency has been improved thanks to offline usage capability, that operability is excellent, and that it is very easy to use. But what these workers appreciate above all is that they only have to carry one device.

We are planning to expand the scale of this service up to 30,000 users from the current 20,000 users by implementing global introduction in the future.

6. Future Prospects

(1) Integration with other products

Thus far, we have discussed the secure use of mobile devices facilitated by the Mobile Platform Service. We believe that in the future we will be able to further leverage the capabilities of this service to address a wider range of issues through integration and collaboration with various other products and solutions. This will help meet the needs of customers who are facing the problem of limited applicability of the current service due to the obstacle of imperfect security of mobile devices.

(2) Model deployment using NEC as a reference

This service can offer so many functions that it is expected that some customers will be unable to decide which or how many functions they need and the extent to which selected functions should be deployed. Currently, we are looking into the possibility of providing a comprehensive service that includes consulting and advice on introducing the service using our own in-house deployment at NEC as a reference model.

(3) Overseas deployment

For the time being, this service will be available only in Japan. However, we are planning to introduce this service overseas in the future.

In fact, we are planning to continue using this service as the standardized device management platform at NEC and will be deploying it globally as well. Our goal is to make it available to overseas customers as soon as possible.

7. Conclusion

Mobile devices have become indispensable in modern business. Expanded utilization of BYOD devices makes it imperative that companies deploy a system capable of managing a variety of devices in order to ensure data security.

The Mobile Platform Service introduced in this paper allows administrators to perform detailed, flexible management of devices without forcing users to sacrifice convenience. While positioning this as a platform for future mobile work, NEC will continue to address various customer needs through reference utilization for in-house usage and combinations with other products and services.

Authors' Profiles

OIKAWA Tsuyoshi
Smart Networks Division

YOSHIDA Kazumi
Manager
Smart Networks Division

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.12 No.2 Cybersecurity

- Building Futureproof Security to Support Business Safety and Reliability -

Vol.12 No.2
January 2018

Special Issue TOP