Network Services Required for Business Operations Using Smartphones

● Motoyuki Kimura

Studies are in process to make use of smartphones and tablets, which have rapidly become widespread in the consumer market, as business tools for office work, customer contact operations and specialized operations in various work sites. Before smartphones can be used in such operations, however, issues must be resolved such as concerns about security and insufficient IT skills for their introduction and operation. To conduct specific studies on such introduction and operation, it must be understood that, in terms of using operations data, there are several different forms of smartphone application each with their own different issues. Based on that understanding, consideration must be given to factors including the content of operations, cost/deployment period, existing system environment and operational load to select the form of application and solution appropriate for the enterprise. This paper summarizes the forms of application of smartphones. It also presents network services capable of resolving issues that arise in using in-house Web applications such as information leakage and unauthorized connections, and adaptation of existing systems to smartphones, from the perspectives of devices, networks and applications. It also gives examples of their use.

1. Introduction

The volume of shipments of smartphones and tablets (hereafter "smartphones") is steadily increasing. Smartphones combine the convenience of the conventional mobile phones, such as high portability and fast start-up, with the convenience of PCs, including the ability to use full browsers to view websites and add functions by using applications registered with marketplaces on the Internet. They are also user-friendly with intuitive operations such as multi-touching and pinch-in/pinch-out. These merits are the major reason for their rapid diffusion in the consumer market.[1] Enterprises have high expectations for using smartphones as business tools. There are demands for "realization of a non-territorial office style of working for improving productivity," "making use of expressive screens and user interfaces (UI) for operations, especially customer contact operations" and "using mobile devices for reasons to do with work environments and work styles." Under these circumstances, enterprises are considering using such devices in various sites such as for office work that takes place outside or at home, customer contact operations in places of visiting customers or stores, and specialized operations in factories and hospitals.

Meanwhile, there are issues to be resolved before smartphones can be used in business operations. Especially obvious among them are concerns about security and insufficient IT skills for their introduction and operation. Since foreign-made devices and globally common OSes and applications are used compared with mobile phones that have been mainly used in Japan, from the perspective of security, this gives rise to concern about a significant increase in attacks on various vulnerabilities that the devices have, as with PCs. When a smartphone is lost, it may be used to gain unauthorized access to the internal information system of an enterprise and business data stored in the smartphone may be leaked. Many enterprises have therefore refrained from using smartphones in business operations until countermeasures are in place. In terms of insufficient IT skills, present difficulties are the need to comprehensively deal with devices, networks and business applications on the basis of mobile technology and the burden of maintaining a network connection environment and carrying out business application development for devices and OSes that require frequent updating.

To address this situation, Fujitsu has incorporated in FENICS II Universal Connect Mobile Browser Connection Service (hereafter "Mobile Browser Connection Service"), which is a remote access service for allowing internal Web applications to be used from outside via smartphones, its proprietary additional features from the perspective of devices, networks and applications. This service is an effective solution for enterprises considering using Web applications via smartphones. This is because it allows measures to be taken against information leakage in the event of loss or theft of devices without the burden of operation and management, and because smartphones can be quickly put to use without the need to modify the existing Web applications.

This paper first describes the forms of application of smartphones and their issues and the positioning of the Mobile Browser Connection Service. Then, it presents the solutions offered by this service and their benefits, followed by application examples.

2. Forms of application of smartphones and their issues

From the viewpoint of using business data, this section summarizes the forms of applying smartphones that are currently feasible and their issues in terms of security and system development (**Figure 1**).

1) Use of business data stored in devices

Business data are stored in the memory of smartphones and the stored information is viewed and processed offline with a connection to a network established only when required. Data can be comfortably used even when radio signals are weak because a network connection is not established while the device is in use.

Issues with use include the fact that business information is stored in devices and information leakage in the event of theft or loss may lead to serious consequences. This generates the need to use Mobile Device Management (MDM) for remote device locking, data deletion and memory encryption. To allow devices owned by individuals to be used in business operations, users must agree to such management and data must be backed up. In addition, when the enterprise's original business application is used for processing business data rather than general-purpose applications such as mailers and groupware preinstalled in devices or offered on the market, they must develop the application

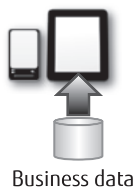
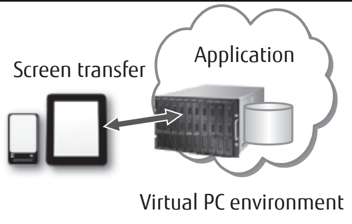
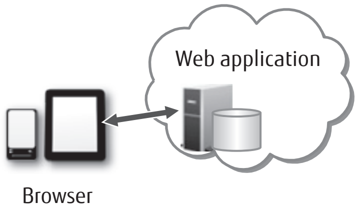
	1) Use of business data stored in devices	2) Use of thin client system (virtual PC system)	3) Use of Web applications in center
Image			
Major benefits	• Offline use allowed even in weak radio signal environment	• Information not stored in devices • Implementation of same business as with office PC	• Information not stored in devices • Inexpensive availability simply by network connection
Major issues	• Device management required because of serious consequences caused by information leakage due to theft or loss • Need for development of applications to handle business data	• Degraded response, unauthorized connection and tapping via communication paths • Same screen as PC (not easy to operate) • Cost of environment construction	• Browser cache remaining • Degraded response, unauthorized connection and tapping via communication paths • Same screen as PC (not easy to operate)

Figure 1
Forms of application of smartphones in use of business data.

from scratch according to the device OS and maintain operations whenever the OS is updated.

2) Use of thin client system (virtual PC system)

This is a form in which, on the premise of a network connection, business data processing is centralized on a virtual PC environment (server) constructed in the center. When in use, the desktop screen of the virtual PC is transferred to a mobile device and the mobile device only shows the result of processing on the screen without storing any business information. This reduces the risk of information leakage in the event that the device is stolen or lost. For business data processing, all applications ordinarily running in the desktop environment can be used.

For use, there are issues including a possible connection to the network by malicious users, tapping via communication paths, degraded response due to mobile communication delays and use of the same screen as a PC without consideration given to operability. While it does not require a business application to be developed for mobile use, a thin client system must be constructed if one does not exist, and this is very expensive.

3) Use of Web applications in center

On the premise of a network connection, specific Web applications in the center are used to process business data. For use, an environment allowing an always-on network connection is required but no business information is stored in a device, which reduces the risk of information leakage in the event of theft or loss. In addition, this form is less expensive than using a thin client system if existing Web applications can be used.

Issues with use include the fact that data may remain in the Web browser cache, a network connection might be made by malicious users, and tapping via communication paths could occur. In addition, an ability to operate the relevant Web applications in the browser installed in a device and screen and response suited to the device size must be taken into consideration.

In this way, the three forms of application have their own benefits and issues and enterprises must decide which one to adopt in view of the business operations to conduct using smartphones, cost, deployment period, existing system environment and burden of operation. Paying insufficient consideration to these points may cause excessive investment and increased burden of operation, leading to an inability to produce sufficient results. The next section describes how to resolve the issues that arise when the application form 3), or use of Web applications with smartphones, is adopted. It is an effective solution for enterprises wishing to implement security measures as inexpensively as possible without the burden of operation and maintenance or to quickly put smartphones into use without modifying the existing Web applications.

3. Solution with Mobile Browser Connection Service and its benefits

This section describes how to use the Mobile Browser Connection Service as a solution to issues with use of Web applications in the center by smartphones, which is mentioned in the previous section, and its benefits (**Figure 2**).

3.1 Security measures

1) Dedicated browser that does not leave business data in devices

When using a pre-installed browser such as Safari, downloaded information that is stored in the cache or cookies remains in the device. It is not realistic for the user to delete such information every time the device is used for business purposes. The specialized browser developed by Fujitsu (hereafter "FENICS Browser") automatically deletes this information when a browser is closed. To display a document attached to Webmail, the FENICS Browser stores the relevant data in a temporary area inaccessible by the user and managed by the browser and automatically deletes the data when the browser is closed or a certain period of time has elapsed. In addition, copying and pasting of text shown on the screen and registration and editing of bookmarks are restricted and the browser is automatically closed when other applications are used, which means that no business data are left in the device. This browser ensures that business information is not left in the device and eliminates the fear of information leakage even if the smartphone is lost.

2) Strong authentication

To connect from a smartphone to an internal network, the pre-registered device ID and the device ID acquired by the browser using JavaScript are compared in addition to ID and password validation, and

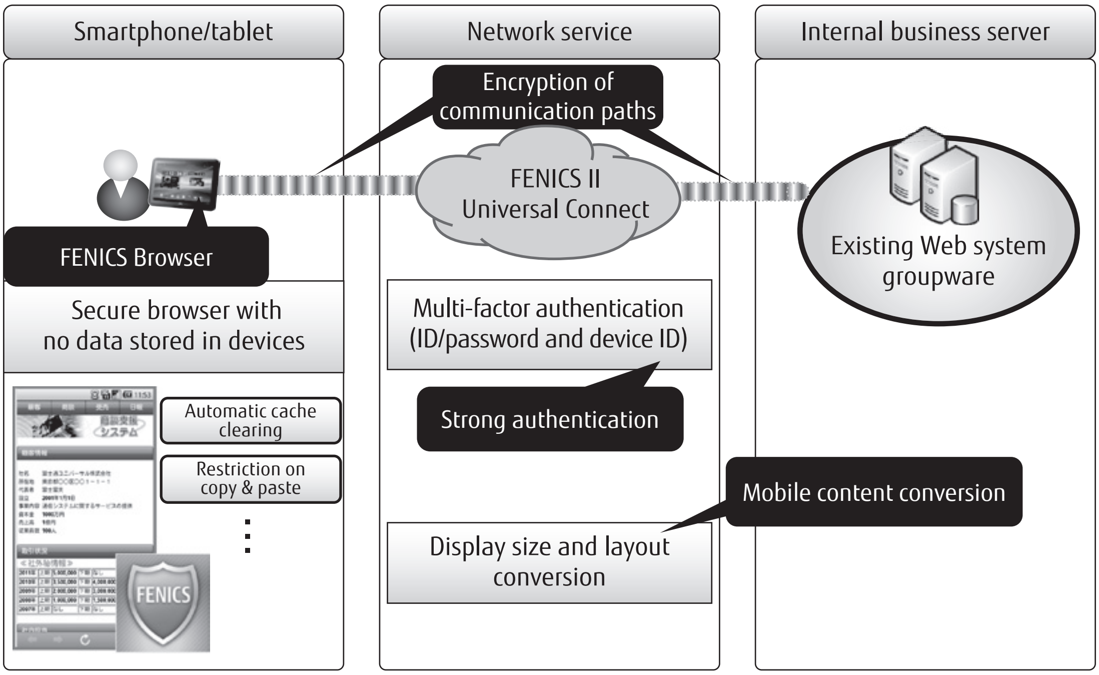

Smartphone/tablet
Network service
Internal business server
Encryption of communication paths
FENICS II Universal Connect
FENICS Browser
Existing Web system groupware
Secure browser with no data stored in devices
Multi-factor authentication (ID/password and device ID)
Strong authentication
Automatic cache clearing
Restriction on copy & paste
FENICS
Mobile content conversion
Display size and layout conversion

Figure 2
Mobile Browser Connection Service/FENICS Browser.

this provides authentication by multiple checks. In addition, connection to the internal network is permitted only via the FENICS Browser described in 1). This prevents connections to the network being made by unauthorized users, unauthenticated devices and standard browsers. Furthermore, in view of the trouble of entering IDs and passwords with smartphones, a proxy authentication mechanism is provided in which the IDs and passwords entered at the time of connection to the internal network are used to access Web applications with authentication.

3) Encryption of communication paths

Communication from devices to Web applications on the internal network takes place via Fujitsu's data center responsible for authentication as described above. In the process, communication on the Internet from devices to the Fujitsu data center is encrypted with SSL and a virtual private network (VPN) or leased line is used from the Fujitsu data center to the corporate network, which eliminates concerns about tapping via communication paths.

3.2 Utilization of existing Web applications

1) Operations/views and UIs of existing Web applications

Existing Web applications have layouts and UIs intended for PCs and using them as they are on smartphones may pose difficulties such as poor visibility and unsuitability for touch operation.[2] The mobile content conversion feature developed by Fujitsu uses screen display rules suited for mobile operation requirements such as "elements shown on one screen should be as simple as possible" and "methods of presentation should eliminate screen transition" to convert existing Web applications for displaying with the FENICS Browser. While attention must be paid to the device specifications and mobile line bandwidth, description conversion to HTML5 is possible for representing on smartphones the existing rich content realized by JavaScript and Flash. This allows content to be used on smartphones with views and UIs suited for devices without the need to modify the existing Web applications.

2) Response

The amounts of communication data can be reduced by optimization such as automatically deleting unnecessary graphic data according to rules established with customer enterprises, and this allows applications to be used with a comfortable response time.

4. Examples of use of service

This section presents representative examples of using this service out of the more than 1000 smartphone cases to which Fujitsu has given assistance up to now.

1) Use of groupware and e-mail with smartphones (**Figure 3**)

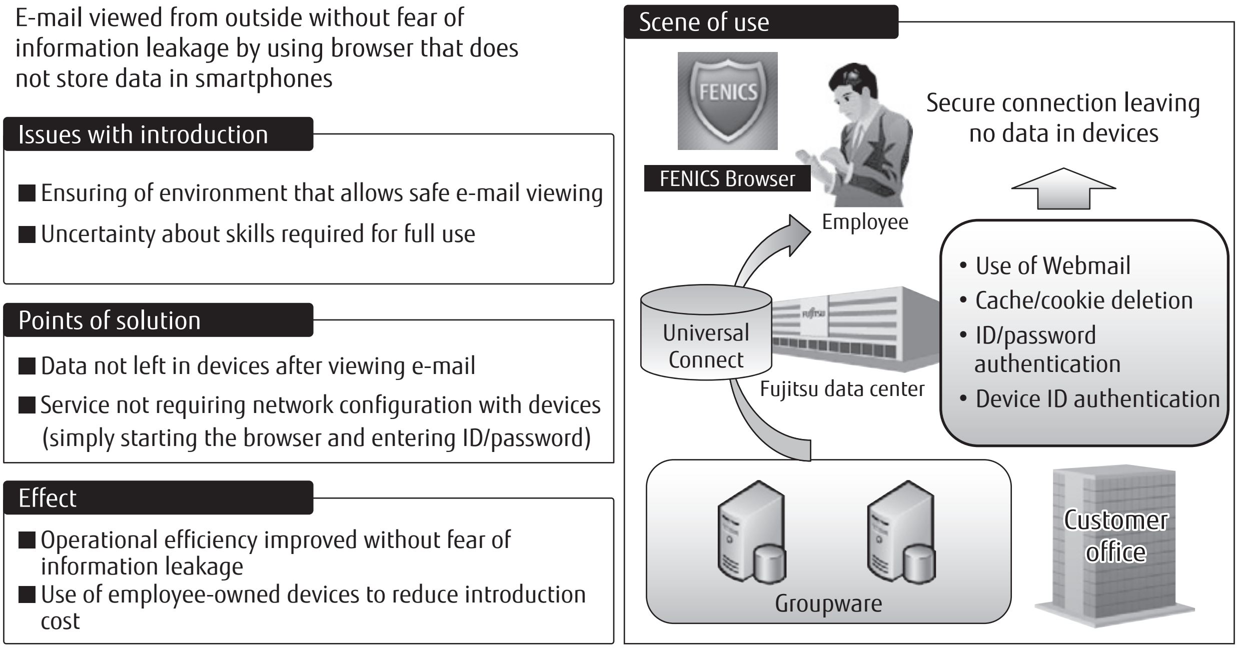
While this is a need that has existed since the age of feature phones, many enterprises wish to use groupware and e-mail on smartphones. It is possible to meet this need by using mobile PCs but there are restrictions such as start-up time and ensuring enough work space, which makes it unsuitable for information checks carried out in short periods of spare time and small spaces. Moreover, use of mailing software in a device synchronized with an internal server gives rise to concern about information leakage. By introducing the Mobile Browser Connection Service, groupware and e-mail can be used without the fear of information leakage and operations can be made more efficient, especially those of the sales department which involve a lot of outside work. It is raising expectations also from the perspective of business continuity (BC) as a means of business communication when it is difficult for workers to come into the office. At present, an increasing number of enterprises are considering using this service including using it with individually owned devices that do not easily allow data to be deleted in an emergency such as theft and deciding to introduce this service.

2) Face-to-face operations using tablets (**Figure 4**)

The financial and service industries in particular need to use tablets instead of mobile PCs for face-to-face operations including making presentations of their products and services, estimating charges and accepting applications for subscription at stores and places where customers visit. Using tablets allows enterprises to give more effective and easier-to-understand explanations to customers and inputting data in devices is more efficient as compared with mobile PCs. As a result, the time required to close deals can be reduced and more customers can be served, which means there are greater business opportunities for enterprises. More and more enterprises are considering using tablets in their operations in a short time and at low cost and introducing this service, which makes the most of the existing business Web applications.

5. Conclusion

This paper has shown that the Mobile Browser


E-mail viewed from outside without fear of information leakage by using browser that does not store data in smartphones

Issues with introduction
- ■ Ensuring of environment that allows safe e-mail viewing
- ■ Uncertainty about skills required for full use

Points of solution
- ■ Data not left in devices after viewing e-mail
- ■ Service not requiring network configuration with devices (simply starting the browser and entering ID/password)

Effect
- ■ Operational efficiency improved without fear of information leakage
- ■ Use of employee-owned devices to reduce introduction cost

Scene of use

Secure connection leaving no data in devices

- Use of Webmail
- Cache/cookie deletion
- ID/password authentication
- Device ID authentication

Figure 3
Use of groupware and e-mail with smartphones.

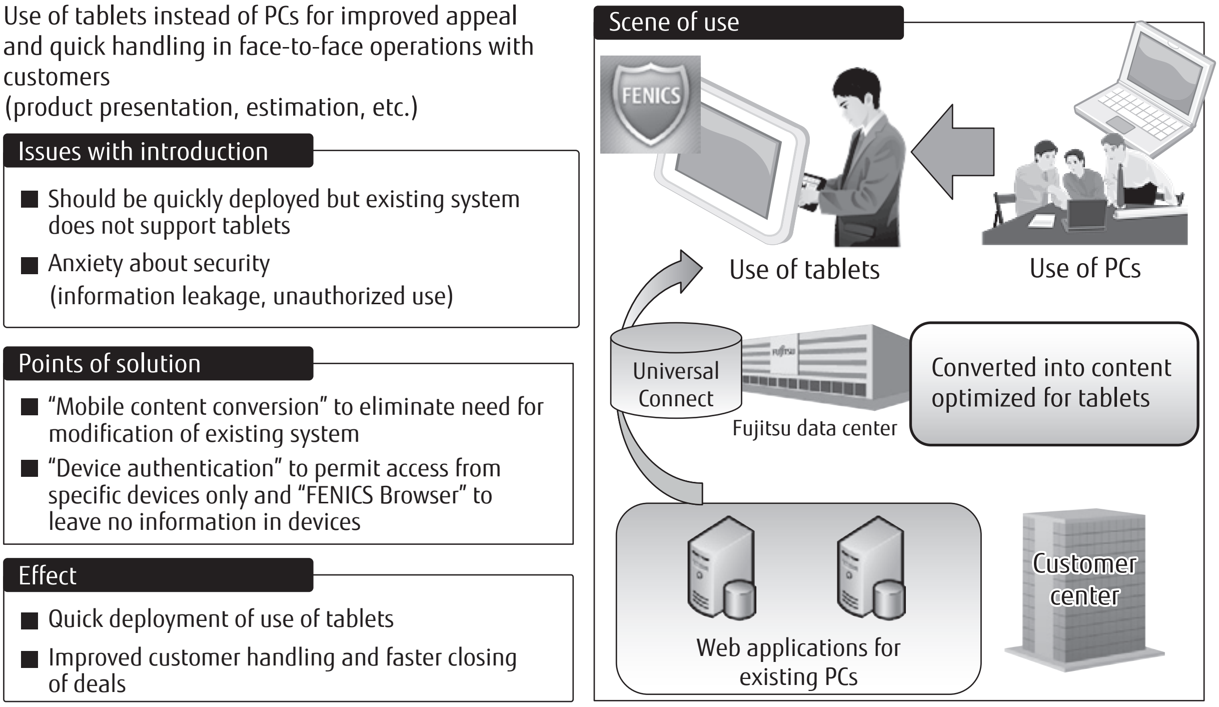

Use of tablets instead of PCs for improved appeal and quick handling in face-to-face operations with customers
(product presentation, estimation, etc.)
Issues with introduction
■ Should be quickly deployed but existing system does not support tablets
■ Anxiety about security
(information leakage, unauthorized use)
Points of solution
■ "Mobile content conversion" to eliminate need for modification of existing system
■ "Device authentication" to permit access from specific devices only and "FENICS Browser" to leave no information in devices
Effect
■ Quick deployment of use of tablets
■ Improved customer handling and faster closing of deals
Scene of use
FENICS
Use of tablets
Use of PCs
Universal Connect
Fujitsu data center
Converted into content optimized for tablets
Web applications for existing PCs
Customer center

Figure 4
Use of tablets for face-to-face operations.

Connection Service provides an effective solution to problems with using smartphones in business operations for enterprises, as security measures against information leakage from devices and unauthorized network connection in the event of theft or loss, and in terms of utilizing the existing Web applications. However, it needs further enhancement such as applying access policies to devices and incorporating a quarantine function for virus-infected devices to make it a service capable of comprehensive and efficient operation and management. The FENICS Browser must be able to keep up with the latest models and OSes including Windows 8. For additional features in view of applications for content conversion, their roles and functions are expected to change due to the development of HTML5 and the spreading use of mobile devices in enterprises, and so we must pay attention to the trends.

Fujitsu intends to continue enhancing network services for smartphones that are desired by enterprises from a comprehensive perspective that covers the devices, applications used and operation as well as safety and convenience of network connections. In this way, we will help our customers to achieve work style innovation and expand their business.

References

1) S. Sano: Medium-term Forecast of the Smartphone/Tablet Market. MCPC Mobile Solution Fair 2011 seminar lecture material (in Japanese).
http://www.mcpc-jp.org/news/pdf/20111125_fair11.pdf

2) K. Nagai: Smartphone Selection and UI (in Japanese).
http://thinkit.co.jp/story/2011/01/19/1964

Motoyuki Kimura
Fujitsu Ltd.
Mr. Kimura is currently engaged in planning and sales promotion of network services.