In-house Practice of Cloud-based Authentication Platform Service Focusing on Palm Vein Authentication

● Yuko Suzuki ● Atsuko Niigata ● Masayuki Hamada

Fujitsu has been working on constructing a cloud-based authentication platform service that provides multiple means of high-security authentication, making use of device characteristics. In this service, the central role is played by palm vein authentication, which Fujitsu has cultivated up to now. This service is realized by cross-functionally bringing together knowledge relating to biometrics and authentication services at Fujitsu. Fujitsu intends to offer it to customers and society after it has been thoroughly utilized and brushed up by in-house practice. The authentication means offered include biometrics such as palm vein, iris, and fingerprint authentication and one-time password (OTP) not requiring dedicated devices. In addition, as authentication federation interfaces, multiple standard protocols including Security Assertion Markup Language (SAML) are available. This paper describes the safe and secure authentication features offered by this cloud-based authentication platform service, mainly including Fujitsu's palm vein authentication technology, which can boast of having one of the highest authentication accuracies in the industry.

1. Introduction

The number of victims of cyber attacks has been growing in recent years. In order to counterattack, multi-layered protection is necessary by enhancing features such as malware detection, network security, and tracing. Authentication is one of the most crucial defense mechanisms against spoofing offenders. Fixed password authentication is no longer a reliable option (**Figure 1**).[1] Meanwhile, other options such as IC cards, public key infrastructure (PKI), and one-time password (OTP) with hardware tokens are not proving very popular, hindered by additional operational cost and complexity and onerous handling of dedicated devices, together with the risk of having such cards and devices lost or stolen. On the other hand, customers, particularly corporate or organizational users, demand an accessible and secure environment in which their systems can be deployed using smartphones and cloud-based services, from outside like from their homes or while on the road. In order to leverage the advantages of cloud services, such an environment must also offer ready-to-use usability as well as connectivity with existing in-house systems (**Figures 2** and **3**).[2]

Considering these requirements, authentication needs to tackle the following three major challenges:

1) High security and convenience,
2) Flexibility to secure connection to various services,
3) Configuration of authentication that can be readily available when needed.

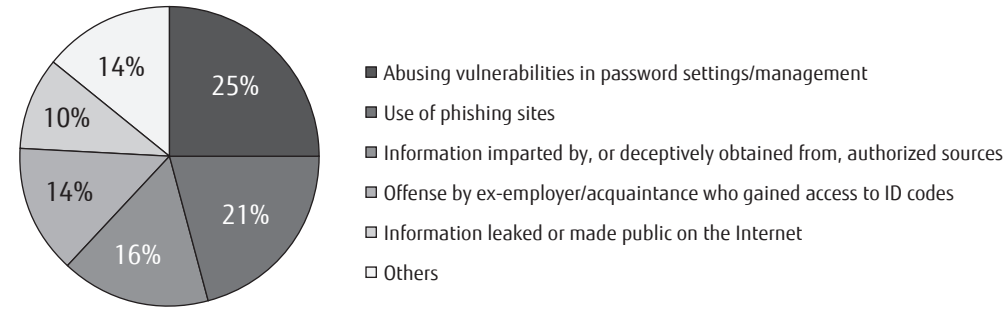
These are also challenges faced by Fujitsu itself; while the currently implemented authentication system that combines IC cards and PKI is secure, it lacks the flexibility to quickly adapt to evolving work-styles.

Biometric authentication is a promising option to tackle challenge 1). Fujitsu can boast of having palm vein authentication technology[3),4)] with world-leading accuracy. Palm vein authentication offers both easy operation, as users only need to place their palm on sensors, and robust security performance as it is almost impossible to copy palm vein patterns. To address the second challenge, there needs to be an authentication federation interface that can integrate more and more standard authentication protocols, offered as a service. In order to develop an open and secure work environment, both of these two points described above must come in one package. As for the third challenge, a

■ Prosecuted unauthorized accesses in 2014

Identity theft	336
Security hole	2

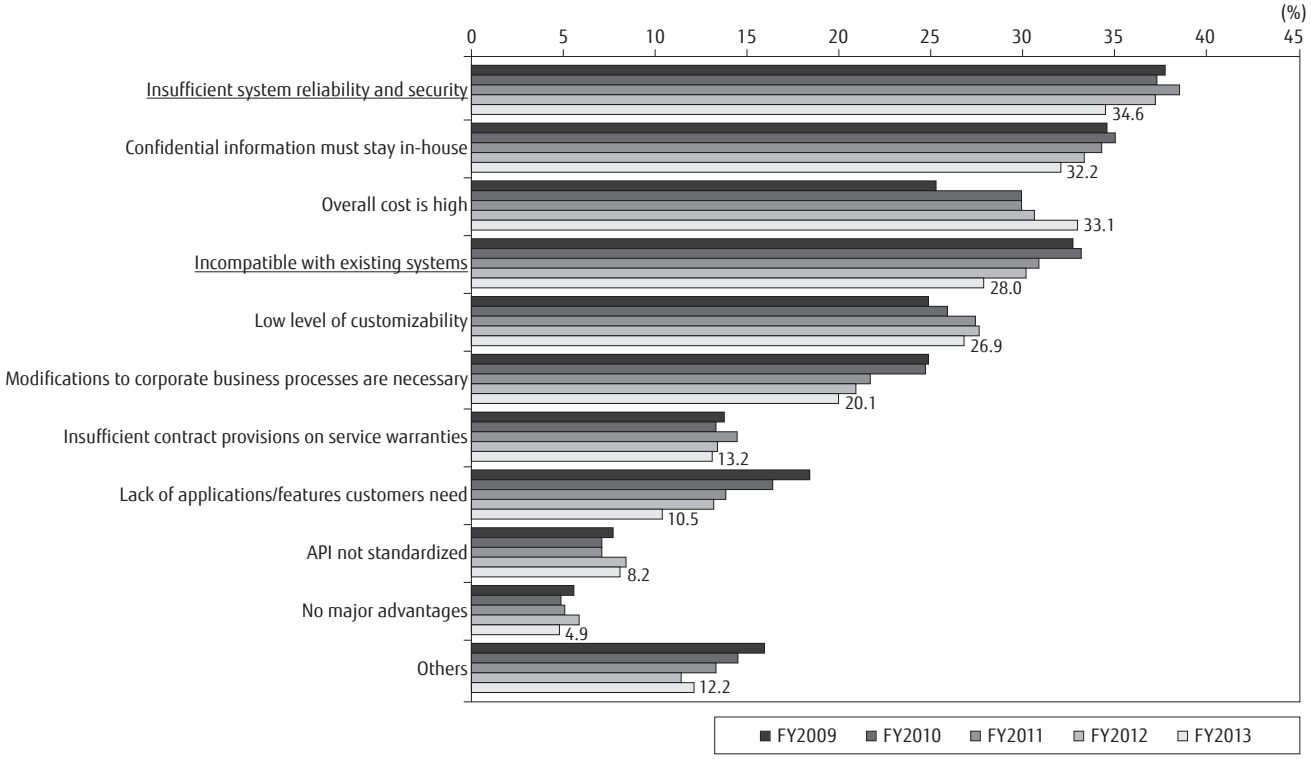
■ Types of identity theft in 2014



Most cases of identity theft are attributed to abuses of fixed ID passwords

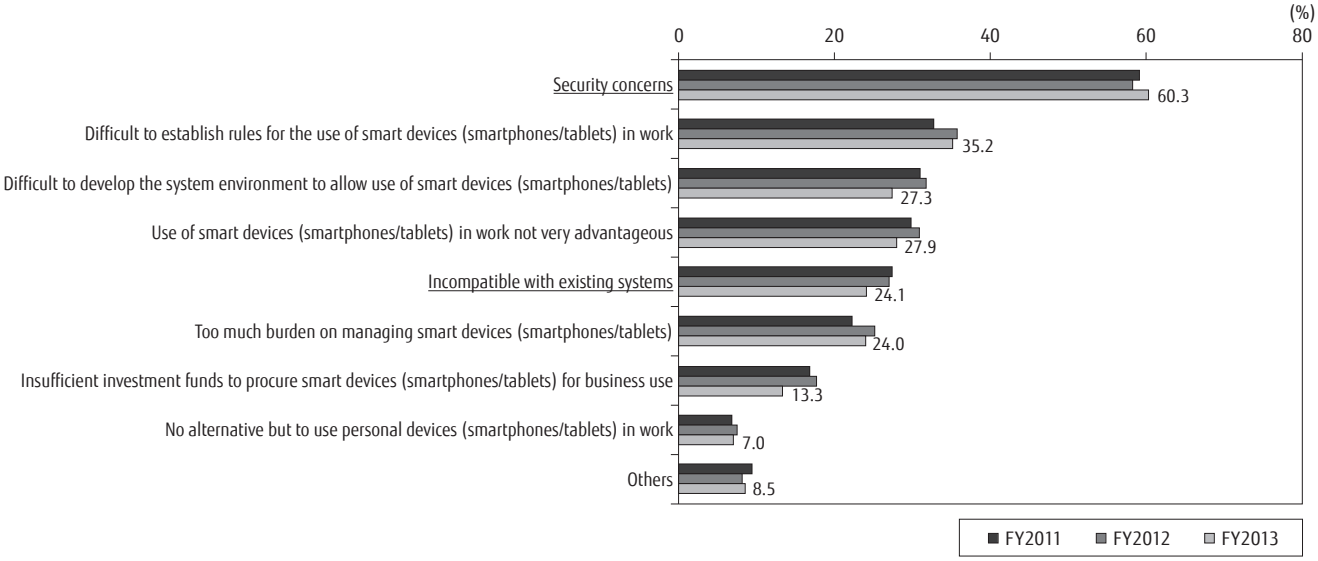
Data based on "Incidence of unauthorized accesses in 2014 and system engineering against Internet access control technology" by Ministry of Internal Affairs and Communications of Japan

Figure 1
Prosecuted unauthorized accesses and offense types of identity theft attacks.



Source: FY2014 Development of information economic society infrastructure in Japan - Survey report, Ministry of Economy, Trade and Industry of Japan

Figure 2
Changing challenges in introducing and using cloud computing systems.



Source: FY2014 Development of information economic society infrastructure in Japan - Survey report, Ministry of Economy, Trade and Industry of Japan

Figure 3
Challenges in incorporating smartphone/tablet use in work environment.

cloud-based authentication service is the direction to take. In order to achieve these, at Fujitsu we have decided to build a new authentication platform through a collaboration of relevant divisions, and pilot it internally before offering it to our customers.

In this paper, we will describe the challenges in terms of Fujitsu's in-house authentication practices and the project to address these challenges. We will then explain the introduction of a new authentication service and its effectiveness, and present our future tasks in preparing for the solution to be offered to our customers.

2. Challenges deriving from changing work-styles

At Fujitsu, authentication has been unified into two systems: PKI-card authentication (for high-level security) that uses IC cards with embedded PKI secret keys, and ID-password authentication (for basic-level security) by ActiveDirectory. The method used depends on the required level of information confidentiality. However, changes in work-styles in recent years have given rise to the three challenges stated in the introduction.

1) High security and convenience

To create an environment that allows access to more than calendar entries and/or e-mails, smart-device accessibility will be further enhanced to include access to a company's internal information, which requires a high-security authentication system. Currently available is PKI-card authentication, in which the user takes out a card and places it over a smartphone while entering a personal identification number (PIN) to decrypt the secret key. This method significantly compromises the smart device's ease of use and possibly the work efficiency. Furthermore, there is a high chance of losing the card. Therefore, a new system is needed that provides robust security while keeping the level of usability intact.

2) Flexibility to secure connection to various services

Fujitsu operates a closed work system, and it is in theory possible to employ a unified authentication ID system by integrating a uniquely developed authentication federation interface. Even with the introduction of cloud-based services, the IDs should be centrally managed, but such a control would be difficult to implement with a unique authentication method. In order to upscale the work process environment, we need to provide an environment that is able to connect securely to diverse services.

3) Configuration of authentication that can be readily available when needed

As work and workers globalize, internal information as an asset also needs to be protected by globally invariable security measures. Ideally, the authentication process should be easy to use for anyone irrespective of the countries or work systems in which it is deployed. To achieve this, we need a system to easily and quickly roll out the Japan-made authentication service to overseas bases.

Given the above three challenges, we aimed to develop an authentication platform service based on the following three concepts:

- Biometric authentication that is both highly secure and easy to use,
- Support for multiple authentication federation standards,
- Cloud-based service that is ready to use.

3. Platform development for commercialization

For the platform development, we had a cloud-based commercial service in mind rather than simply developing a system for in-house use. Biometric authentication technology that employs palm veins or irises and cloud-based services are Fujitsu's strong point. The idea was to rigorously enhance this combination for the authentication platform, through in-house testing, and develop the model further to define the service so that it can be offered to customers as it is. Meanwhile, the above-stated challenges were also discussed in a division related to the security business to develop a solution. We then launched a cross-division project between the ICT Division and Security Business Division, and commenced a joint development project. This project is an embodiment of FUJITSU Security Initiative[5] in the sense that the ICT Division and Security Business Division are collaborating in the development, having commercialization in mind from the beginning.

The advantages are that feedback from users and operators can be incorporated early in the designing stage, that having commercialization as the goal helps to eliminate problematic peculiarities, and that the resulting product for customers is based on practical knowledge gained through actual use.

4. Accommodating the internal ICT situation

There were several points to consider before applying the authentication platform based on the above-mentioned three major concepts. One of them was the fact that a wide variety of devices were in use for business within the Fujitsu Group. Furthermore, one person would carry several devices, which are employed for different tasks or in different situations. It would be ideal to roll out the biometric authentication to all such devices by equipping them with biometric sensors, but that is not realistic given that there would be some 100,000 prospective users to account for. This being said, security cannot rely on password-based authentication forever, as it has already been found vulnerable. We therefore developed a system which allows biometric authentication to be deployed as the main authentication security option, but with a selection of appropriate authentication methods depending on the device characteristics, from non-device-dependent authentication methods such as OTP (one-time password) as a software token (**Figure 4**). Although the alternative authentication method is not as robust as the biometric one, this system at least offers security and usability that is better than fixed password authentication. This system may have the drawback that the operator must bear the burden of user support, but users can simply benefit from the easy authentication system to use.

5. New authentication platform and its effectiveness

Given the above descriptions as the background, we have developed a new authentication platform based on the three major concepts, and it is being subjected to a practical trial at Fujitsu today (**Figure 5**).

- Infrastructure: Fujitsu Cloud platform
- Authentication methods: palm vein, fingerprint, and OTP {time-based one-time password (TOTP), software token}
- Authentication method under consideration for enhancement: iris recognition
- Authentication federation interface: Security Assertion Markup Language 2.0 (SAML 2.0), REST API, agent-based proxy authentication,
- Authentication federation interface under consideration for scaling: OpenID Connect, OAuth 2.0

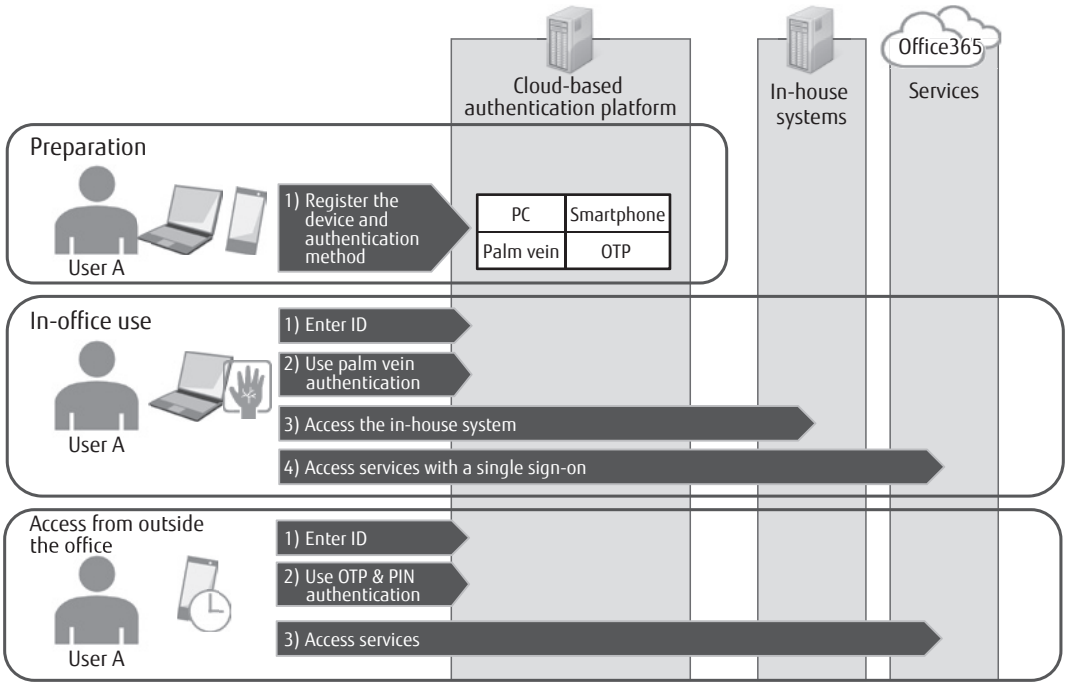


Figure 4
Authentication methods adopted by device characteristics.

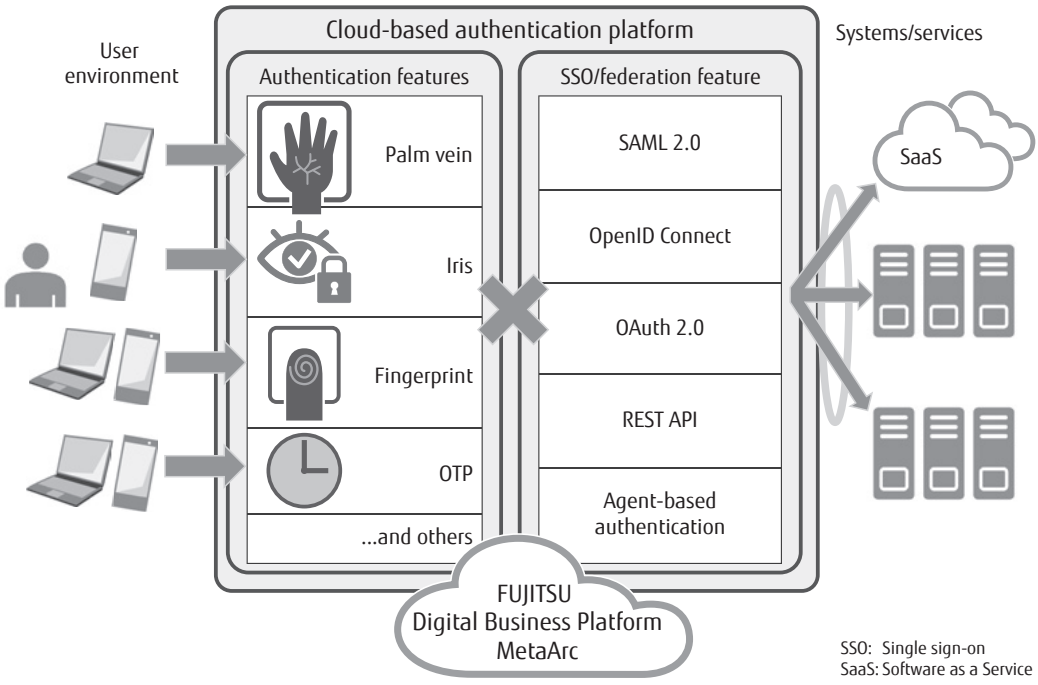


Figure 5
Major features of new authentication platform.

This authentication service is developed with the following systems of in-house information and office-entry security:

- Virtual desktop service,
- Web-based business system,
- Windows log-on,
- Remote access,
- Wireless LAN, etc.

Once commercially launched, the platform will offer the following benefits:

- High-security without compromising the convenience of smart devices: to establish work-styles with safety, security, and utility,
- Flexible selection of high-security authentication methods according to the devices used: to leverage existing devices,
- Rich authentication federation interfaces allow access to various cloud-based services.

6. Future plan

The future developments envisaged for this authentication platform are described below.

1) Application to in-house virtual desktop service authentication

The in-house trial of the system was begun in January 2016, and will be fully implemented by March 2017. The interface employs SAML, and offers biometric and OTP authentication services (**Figure 6**).

2) Application to in-house work system

Fujitsu will be migrating its in-house systems to its proprietary cloud platform FUJITSU Digital Business Platform MetaArc[6] over the next five years.[7] Thus, we will apply the new authentication platform to the work systems as they are transferred.

3) Commercialization of the service

We plan to commercially offer the platform thus developed through in-house trial as one-stop authentication for the MetaArc. Further improvement to the platform and feature enhancements will also be subjected to in-house trials before being made commercially available.

4) Feature enhancement

To meet the Fujitsu Group's unique needs, we will develop a risk-based authentication feature and realize personal-device inclusion (bring your own device: BYOD), and roll it out to overseas offices.

7. Conclusion

This paper described a new cloud-based authentication platform and service that will mainly employ palm vein authentication. This service will help to ensure a safe and secure work environment that is accessible from outside the company utilizing smartphones and cloud-based services. The challenge at

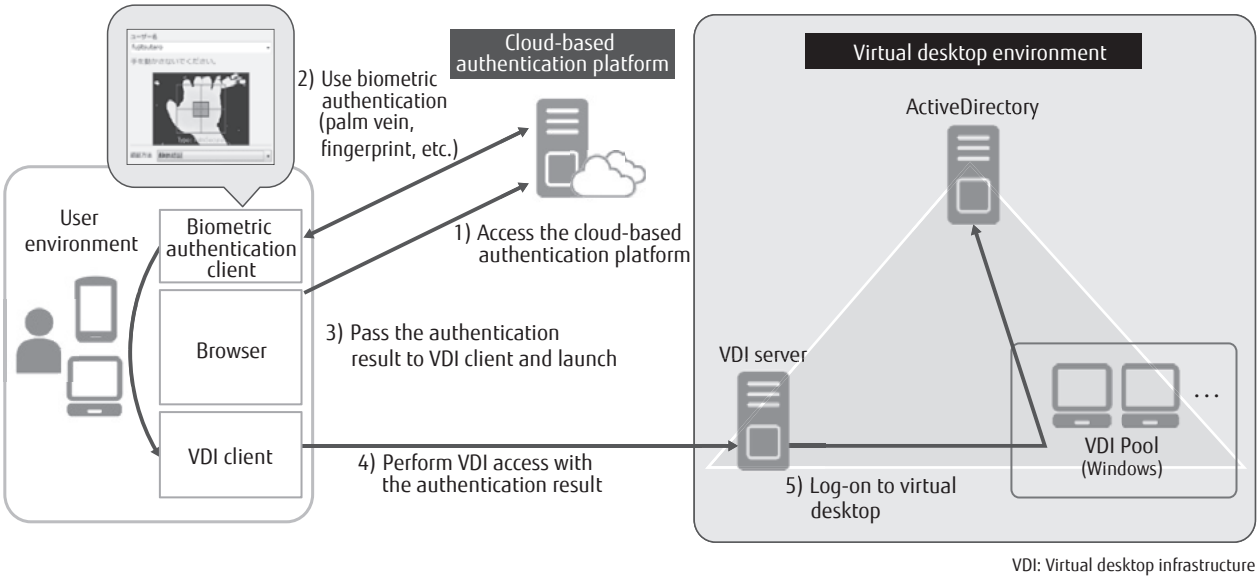


Figure 6
Application to virtual desktop environment.

hand is to smoothly migrate Fujitsu's several hundred in-house systems onto this service platform. The know-how gained through this practice will be a valuable resource for future services for our customers. With its 170,000 employees and several hundred in-house systems spread across the world, the Fujitsu Group can be seen as one big trial ground. Piloting the services in-house before launch should also allow us to accumulate debugging experience, improvements, and know-how, bringing great benefits to our customers. We will continue to work on challenges and improve services through these in-house pilot exercises.

References

1) Ministry of Internal Affairs and Communications: Incidence of unauthorized accesses and research and development about Internet access control function in 2014 Appendix 1 "Incidence of unauthorized accesses" (in Japanese).
http://www.soumu.go.jp/main_content/000347975.pdf
2) Ministry of Economy, Trade and Industry: FY 2014 Development of information economic society infrastructure in Japan-Survey report (in Japanese).
http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/pdf/H26_report.pdf
3) Fujitsu: Fujitsu PalmSecure.
http://www.fujitsu.com/global/solutions/business-technology/security/palmsecure/
4) Fujitsu: With Fujitsu's Palm Vein Authentication, people only need to hold their hand over the sensor!
http://journal.jp.fujitsu.com/en/2014/09/16/01/
5) Fujitsu: Security.
http://www.fujitsu.com/global/vision/2015/products/security/
6) Fujitsu: Digital Business Platform MetaArc.
http://journal.jp.fujitsu.com/en/metaarc/
7) Fujitsu: Fujitsu to Migrate All Internal Systems to a New Cloud Platform.
http://www.fujitsu.com/global/about/resources/news/press-releases/2015/0218-01.html

Yuko Suzuki
Fujitsu Ltd.
Ms. Suzuki is currently engaged in the project on in-house implementation of ID authentication platform based on biometric authentication technology.

Atsuko Niigata
Fujitsu Ltd.
Ms. Niigata is currently engaged in the project on in-house implementation of ID authentication platform, mainly in charge of the platform development and application to virtual desktop service.

Masayuki Hamada
Fujitsu Ltd.
Mr. Hamada is currently engaged in the project on in-house implementation of ID authentication platform, mainly in charge of the OTP authentication system and application to web-based work systems.