Migration of Internal Systems to FUJITSU Cloud Service K5

● Makoto Aizawa ● Tomohiro Kakuma ● Akinori Kanamaru

Fujitsu has embarked on migrating its internal systems integrated on a public cloud service, aiming to minimize system operation costs, as well as the cost and period of the development of new applications. In order to migrate the systems efficiently to a public cloud while ensuring operational security and safety, we have developed an internal cloud service. It can address various technical challenges in cloud computing, such as security enhancement as well as the development of a network environment for connecting to the cloud service (VPN connection), common shared infrastructure services, system-wide integrated infrastructure monitoring, and operational automation. An internal pilot system was introduced to assess and evaluate the migration operation, and we verified that the internal cloud service could achieve a 30% reduction in the cost of operating the infrastructure, while the new infrastructure would be introduced in a shorter period (to two weeks from four months). These are part of the efforts to integrate the internal systems on the FUJITSU Cloud Service K5, the core of FUJITSU Digital Business Platform MetaArc. This paper describes the initiative to develop the internal cloud service and the evaluation of the system migration using the pilot system, with its results. The paper also presents the total cloud-migration plan for Fujitsu's own internal systems, and the expected effects.

1. Introduction

Fujitsu's internal systems have undergone many improvements up to now to add the functions required. This has caused problems such as increased complexity of the system structure and "silos," or business systems unable to link up together because the systems are individually optimized. In addition, there were issues such as increased operation costs, system revisions for flexibly meeting business needs, and minimization of costs. To improve this situation, we have been working since FY2009 on company-wide information and communications technology (ICT) integration under the policy of overall optimization in two ways: server aggregation and application aggregation by virtualization. However, neither of them has produced satisfactory results up to now.

While efforts have been made to reduce the operation costs out of the ICT investment in internal systems by improving the efficiency of and automating operation monitoring, they have mostly remained at the same level. Fixed costs required for operation and maintenance account for 80% of all costs, which has made it impossible to appropriate the budget for strategic investment.

In this situation, for the purpose of fundamentally changing operation of the internal systems, we have started migrating the internal systems to a public cloud service called FUJITSU Cloud Service K5 (hereafter, K5),[1] which is the core of FUJITSU Digital Business Platform MetaArc.

This paper first describes approaches including the development of various infrastructure services and infrastructure operation for using internal systems on K5 with ensured safety and security while optimizing the costs. Next, it gives an explanation about security, performance, and other issues revealed by verifying and evaluating the migration to K5 using internal pilot systems and measures for resolving them. Lastly, it describes a plan for migrating internal systems to K5, which will start on a full-scale basis from now on.

2. Present condition of and issues with Fujitsu's internal systems

At Fujitsu, we have implemented since FY2009 server integration by virtualizing systems and aggregating applications (system restructuring). We have done so from the perspective of having overall optimization with the aim of improving system efficiency and reducing the total cost of ownership (TCO).

2.1 Server integration by virtualization

Fujitsu aggregated 5,808 servers including those of Group companies into 3,136 servers by the end of FY2015 using physical and virtual servers, which is a reduction of 2,672 servers. However, as compared with FY2011, about 60% are still physical servers and, even if virtualized, basically servers have only been aggregated for each business system, which is not sufficient as an efficiency improvement. In addition, virtualized physical servers have been designed to withstand the maximum peak load of the respective business systems. For this reason, the utilization rate in terms of average load is about 30% for the CPUs and 50 to 70% for the memory, which means that the resources are not effectively used.

2.2 Application aggregation (system restructuring)

Since FY2010, we have implemented innovations of processes for the individual business fields and operation segments to work on system integration and restructuring. However, the business process innovations have not progressed for cross-departmental functions and the existing practices are followed, which has caused a structure with the systems still linked together in a complicated manner. To aggregate applications, we have put an enterprise service bus (ESB) in place for standardizing data linkage. Such standardization requires mutual revision of systems and is significantly behind schedule due to the large scale of investment required.

In this situation, we have decided to take the opportunity of migrating internal systems to public cloud service K5 to work more drastically on server integration and application aggregation by virtualization as described earlier. In order to achieve this, we have started providing an internal cloud service with strengthened security measures and appropriate operation costs. And we also have started verifying and evaluating migration to a public cloud by using internal pilot systems.

3. Standardization with internal cloud service

To run internal systems on K5, we have put in place an operational environment to ensure the information security rules and operational quality and adjust the operation costs. In addition, for phased migration in the next five years, we have designed and constructed an internal cloud service capable of standardizing and automating operation of internal data centers including network connection between existing data centers and K5, and connection of the corporate intranet and K5 that makes it possible for internal offices to use systems.

3.1 Dedicated domain for internal systems

For a domain provided for each K5 contract, we have put in place an environment exclusively for internal systems including security (such as access control and antivirus measures), network connection, and common services. By constructing and providing an internal cloud service in this way, we have realized a service that can be used safely and securely with appropriate operation costs even on a public cloud. An overview of a dedicated domain for internal systems is shown in **Figure 1**.

The following describes the security, access control, antivirus measures, network connection, and common services that constitute the internal cloud service.

3.2 Concept of security in virtualized environment

K5 provides defense in depth for all zones based on the concept of "zero trust," or the idea that there is no secure area either internally or externally, and has been designed to deal with targeted attacks and other threats.

As development work requires immediacy, we have designed K5 to be able to change the security level of the servers used for the business and product development.

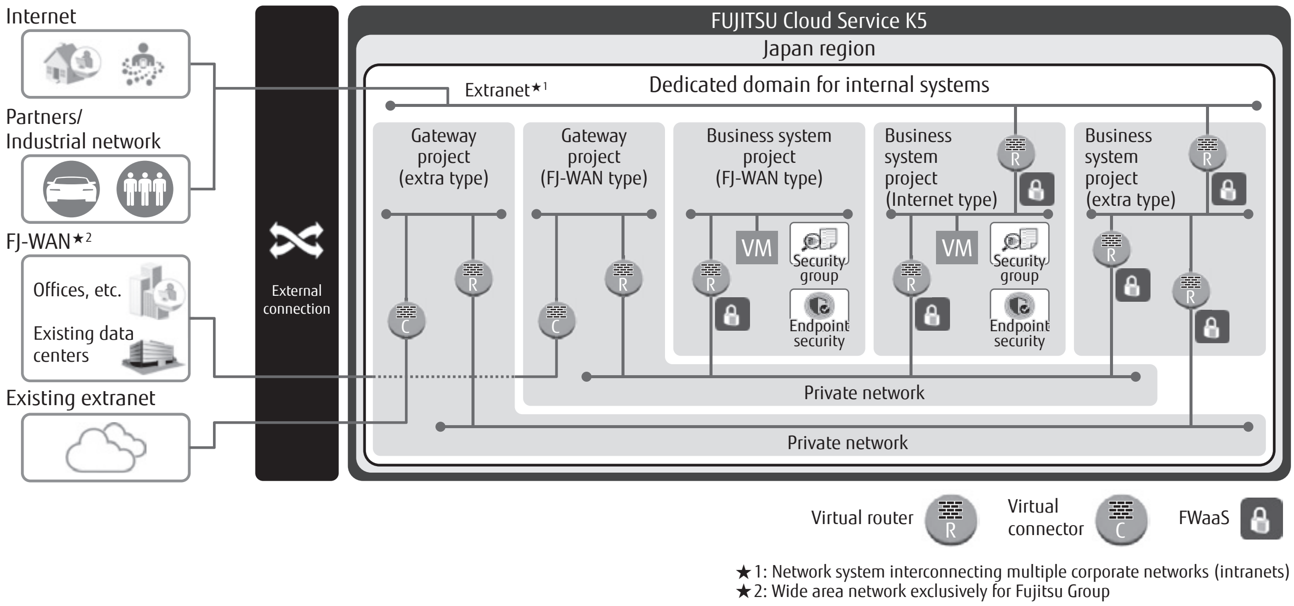

Figure 1
Overview of dedicated domain for internal systems.

3.3 Access control

Internal systems are managed by a domain in units of user project. This user project ensures security by combining different types of access control, e.g., network access control by Firewall as a Service (FWaaS) and server access control by security groups.

FWaaS is applied to the virtual router of a user project. And it controls external connections and communications between projects by specific IP addresses (or subnets) or ports (whitelist method). As with a conventional firewall (FW), security is strengthened by restricting the administrative authority of FWaaS to the internal cloud service operation department.

Security groups play a role of a FW that controls internal and external traffic according to the application of virtual machines (VMs) such as Web and database (DB). Specifically, they control the receiving ports of VMs themselves according to the Ingress (inbound communication) rule and control communications transmitted from the VMs themselves according to the Egress (outbound communication) rule. By restricting the administrative authority for the security groups to the center operation SE, operation with security of a single server maintained is ensured. The configuration of access control is shown in **Figure 2**.

3.4 Antivirus measures

In accordance with the information security rules for internal systems, endpoint security (an antivirus measure) is implemented. As antivirus software, McAfee's products have been employed and incorporated into a common project that can be communicated with from individual projects, thereby providing the antivirus function for the respective business systems (operation, development/verification, and department servers).

3.5 Security self-check

For devices that are directly accessed from the Internet, security diagnosis is regularly conducted for the purpose of ensuring security.

3.6 Network connection with corporate intranet

We have aimed to ensure the linkage with existing data centers and system migration efficiency and improve the efficiency of network bandwidth management. To this end, we have designed the service so that a gateway project can be constructed for sharing by the router (L3 switch) for corporate intranet connection. This has made it easy to connect to a network covering individual projects and the corporate intranet,

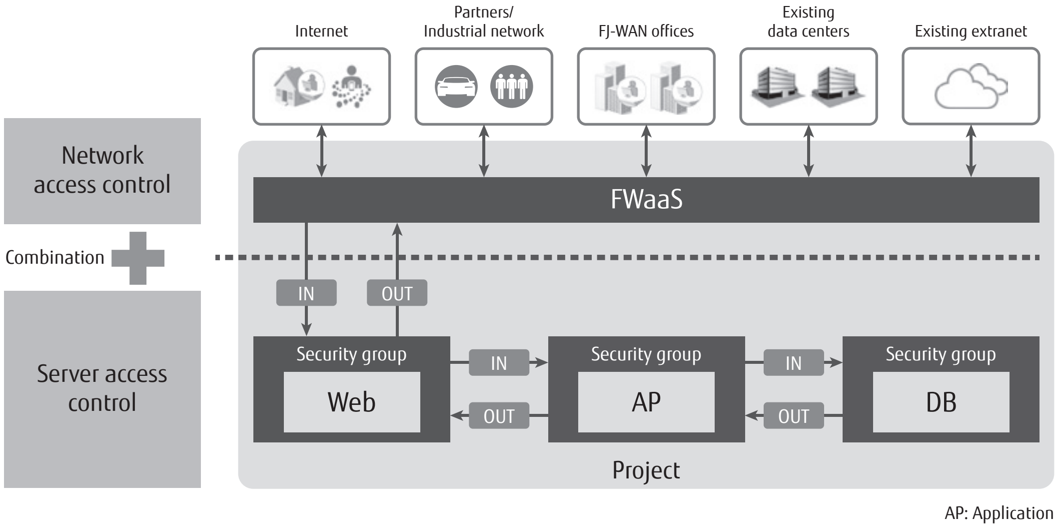

Figure 2
Configuration of access control.

and also made it easy to manage that network.

3.7 Common shared infrastructure service environment

To improve the efficiency of infrastructure operation of internal systems, we have developed and provided the following common services.

- Name resolution service: Domain Name System (DNS)
- Time synchronization service: Network Time Protocol (NTP)
- Proxy service: access to external Web
- Mail service: mail relay
- Infrastructure monitoring service: server monitoring
- Log management service: server and other log management
- RBA service: Systemwalker Runbook Automation (RBA), automation of maintenance such as patch application

Above all, the infrastructure monitoring, log management, and RBA services have been designed and constructed to be capable of dynamically dealing with an increase or decrease in the number of devices corresponding to OpenStack-based auto-scaling and failover.

3.8 Infrastructure monitoring service

The auto-scaling, failover, etc. mentioned above need system operation monitoring functions for the cloud function and not provided as the standard service of K5 and the system monitoring functions have been constructed and provided as a common service for internal systems.

This service uses Systemwalker Centric Manager (CMGR) incorporating Zabbix, a product of Zabbix LLC, to realize automatic addition of targets of monitoring for auto-scaling. And it uses Systemwalker Service Quality Coordinator (SQC) to monitor server resources and ensure good performance of Fujitsu's middleware. The configuration of the common shared infrastructure service environment is shown in **Figure 3**.

3.9 Provision of self-service portal

To decrease the time required for VM deployment and further reduce the operation costs, we have provided a self-service portal that uses internal cloud service management (CSM) products. The self-service portal makes it possible to smoothly implement future migration of internal systems in addition to improving the efficiency of VM deployment operations, which are based on manual labor.

We have attempted to reduce the operation costs by incorporating the configuration work required for VM deployment to achieve efficient operation of internal systems on a public cloud. In VM use for the purpose of development, VM deployment and disposal operations occur frequently, but implementing them by manual labor has its limits. Accordingly, for efficient

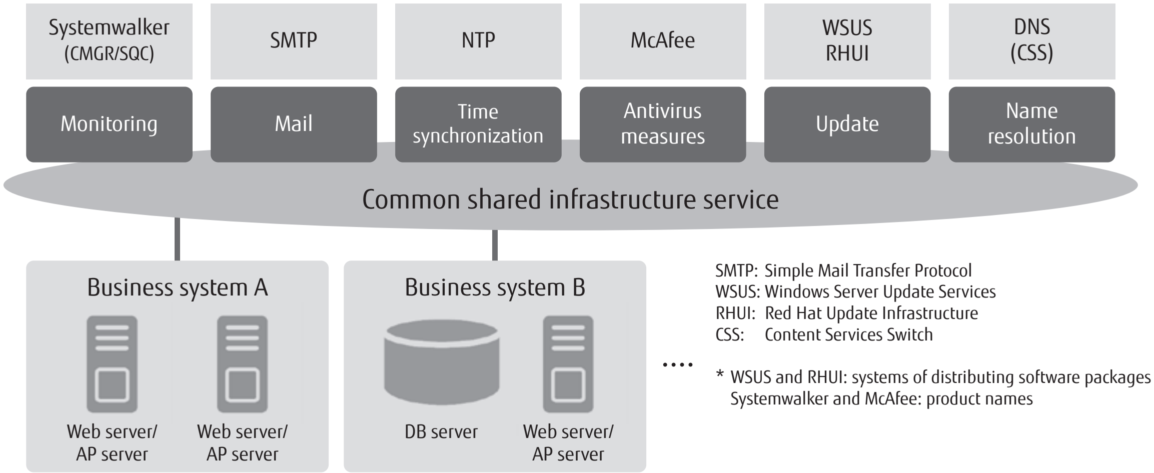

Figure 3
Configuration of common shared infrastructure service environment.

product development, Fujitsu is working to provide a self-service portal at as early a stage as possible.

4. Global ICT governance

This section describes the global expansion of the internal cloud service. We have constructed an internal cloud service on K5 provided in Japan. The K5 provides common services for ensuring appropriateness of the operation costs with the information security rules for internal systems of Fujitsu. And this service standardizes and automates infrastructure operation of internal data centers. From now on, we will gradually migrate internal systems to K5 starting in Japan.

Migration of internal systems is not limited to within Japan but will be implemented at a global level. For that reason, it is necessary to conform to the regulations and institutions of the respective countries and regions and provide an internal cloud service on K5 outside Japan. The know-how for construction and operation of the internal cloud service constructed in Japan will not only accelerate migration of internal systems outside Japan to K5 but also allow internal data centers to be operated at a global level, which has not been realized up to now. These are of great significance also in terms of realizing ICT governance at a global level and are goals that should be accomplished at any price.

5. Verification and evaluation by internal pilot systems

Aiming for full-scale migration of internal systems to K5, we conducted migration verification in advance by using two systems (pilot systems). This section describes an approach for effectively utilizing the K5 functions and resources, and issues with and measures for migration.

5.1 Outline of pilot system migration

Two systems—the ICT Investment Budget Management System and Integrated Asset Management System for managing ICT devices—were specified as pilot systems and the auto-scaling function and multi-tenant products were used for aggregating six VMs to three at minimum. An outline of the pilot system migration is shown in **Figure 4**.

5.2 Utilization of auto-scaling function

The pilot systems had load variations between normal time and peak time and the system configuration assumed peak time up to now. This means that there was a surplus in the resources at normal time. If the system configuration for normal time is the basis of the resources that can be augmented at peak time according to the load, the resources can be effectively utilized.

As a result of investigating the CPU utilization rate of the pilot systems, it was found that there was high load on the system that occurred regularly such as

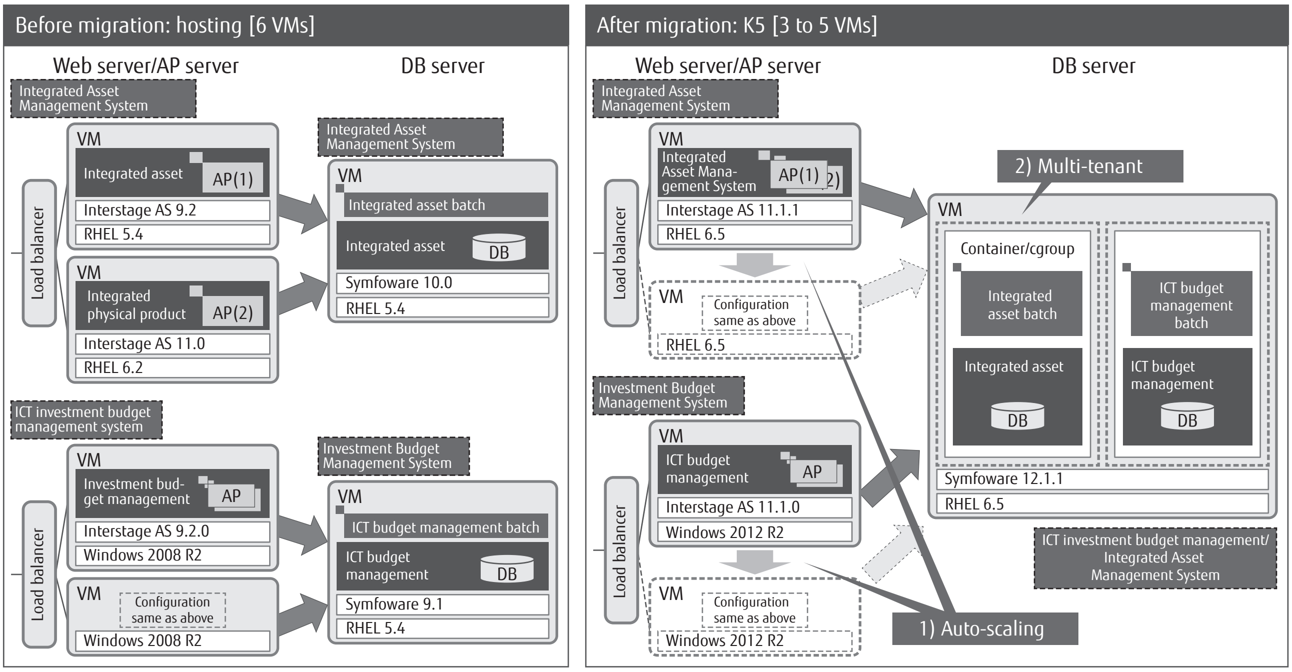

Figure 4
Outline of internal pilot system migration.

that on the closing day for the ICT investment budget, and a high load on the system generated irregularly. Changes in the CPU utilization rate are shown in **Figure 5**. We have realized an appropriate VM configuration (streamlining of resources) by combining dynamic scale-out when a load exceeds the threshold and systematic scale-out by the schedule according to changes in the CPU utilization rate.

5.3 Utilization of multi-tenant products

The DB server was adapted for multi-tenant use by the FUJITSU Software Symfoware Server Consolidation Option function and the control group (cgroup) function of Red Hat Enterprise Linux (RHEL) 6.5 to aggregate the DB servers for the two pilot systems.

We have set the CPU use ratio for the individual systems. While processing takes place within the predefined range at high load (utilization rates of all CPUs are 100%), at normal time (utilization rate of any one CPU is less than 100%), CPU utilization exceeding the set ratio is possible. CPU utilization rate changes for the two systems are shown in **Figure 6**.

5.4 Security measures with standard policy application

Up to now, the corporate intranet had been positioned as a secure environment but K5 implements security measures based on the concept of zero trust. The present pilot systems oblige the SE to carry out new tasks such as examination of all communication information in and outside the systems for setting communication policies required to create security groups. To deal with this, we have divided the communication policies into information that can be grasped by data center engineers such as that between existing internal data centers (standard policies) and information that can be grasped by the SE. And we applied centralized management to and automated the former, thereby successfully reducing the respective tasks of the data center engineers and the SE. With the pilot systems, the number of communication policies to be examined by the SE has been reduced to 482 from 1,389.

5.5 Multiplexing for maintaining performance

As part of TCO reduction, K5 applies the standard configuration such as OS and middleware standardization and provision of patterns for combining the

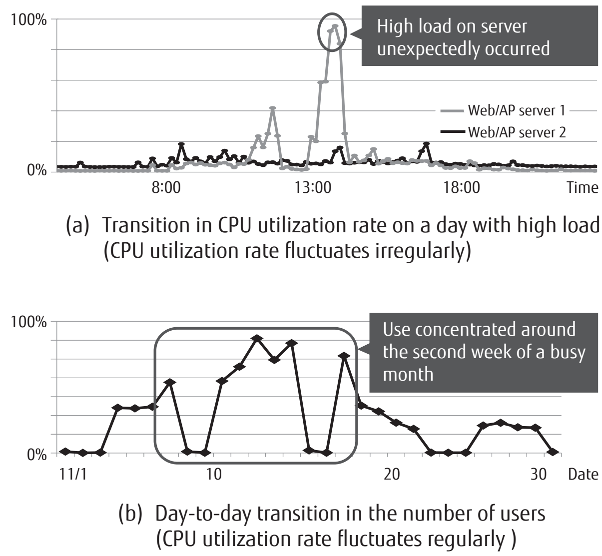

Figure 5
Transition in CPU utilization on internal pilot systems.

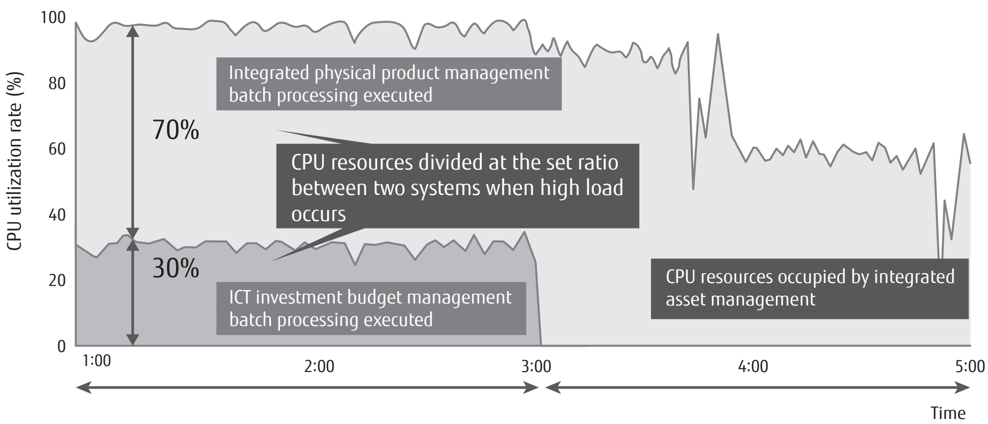

Figure 6
Transition in CPU utilization rate observed during occurrence of system high load.

number of CPU cores and memory. The server specifications (CPU frequency) adopted for K5 are about 50 to 70% those of conventional products. Accordingly, when the processing speed decreases due to the low CPU frequency, improvement of the application is required. The performance degradation that occurred in the pilot systems has been dealt with by improving the application to multiplex processing (to effectively use the number of cores).

5.6 Results of verification by using pilot systems

With the internal pilot systems, the number of VMs has been halved from that before migration by utilizing the auto-scaling function and multi-tenant products. In addition, a 30% reduction in operation person-hours has been achieved by standardizing the system-wide integrated infrastructure monitoring and operational automation. Furthermore, the period required for introducing the infrastructure has been reduced to 1/8 (to two weeks from four months) because of the elimination of the sizing and procurement tasks generated during system construction. The results of efforts for K5 migration are shown in **Figure 7**.

6. Plan for migration of internal systems to K5 and expected effects

We started migrating internal systems in Japan to K5 on a full-scale basis in FY2015 and 19 systems are in operation as of the end of FY2015. Currently, to complete the plan for migration of the internal systems in Japan and overseas to K5 within the next five years, we are conducting a survey on the actual conditions for all internal systems. In addition to the mission-critical systems, there are multiple individual development cloud environments for the purpose of business and product/solution development (with approximately 13,000 VMs). For these development cloud environments, we are cooperating with various departments to work on migration to K5.

Fujitsu announced in February 2015 that it would achieve a TCO reduction of approximately 35 billion yen as the entire group by migrating all of the group's internal systems in Japan and overseas to the next-generation cloud platform.[2] The biggest effect of migrating internal systems to a cloud is reduced procurement of infrastructure equipment such as servers, storage, and networks and infrastructure construction and operation tasks. This can reduce the infrastructure construction and operation costs. Scalability can also be taken advantage of for flexibly changing resources according to the amount of operations. This allows the amount of resources to be reduced from that for peak time of operations to that for normal time and the infrastructure operation costs can be reduced. In addition, it eliminates the need for individually maintaining infrastructure of internal systems, leading to a reduction in labor costs for internal ICT personnel. The personnel conventionally engaged in ICT operation have the know-how and expertise developed through internal practice. Shifting the work that has been done by them to maintain infrastructure to a different kind of work raises expectations for a secondary effect—a contribution to business. However, there are also challenges in carrying out cloud-migration of internal systems. Many of the systems planned for migration to a cloud are of the Infrastructure as a Service (IaaS) type that use a platform of hardware, OS, middleware, etc. And reducing the operation costs for applications that have become complex through many improvements requires measures to be taken.

In the future, we plan to verify "modernization," in

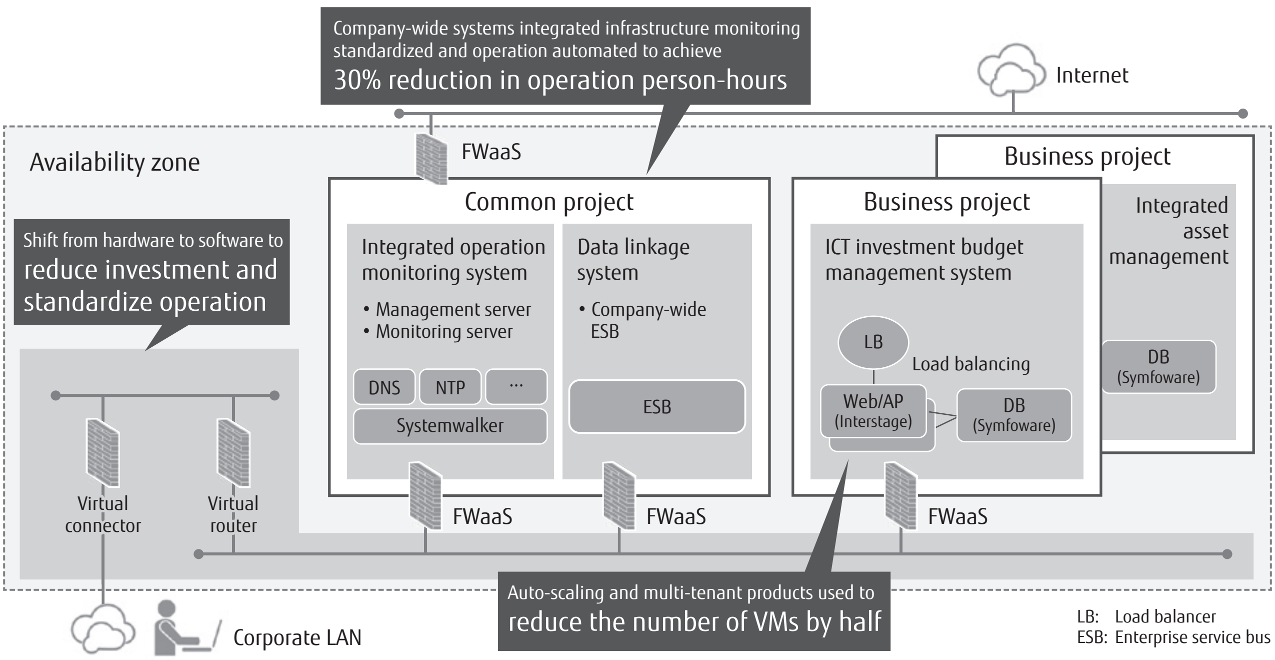

Figure 7
Results of verification by using pilot systems.

which legacy systems are taken down once to construct on a cloud only those systems that are really necessary. We will also verify system reconstruction in conjunction with business strategies and a cloud-native development methodology that utilizes Platform as a Service (PaaS) in line with them. In this way, we will standardize and automate applications for reducing the TCO.

7. Conclusion

This paper presented an internal cloud service for aggregating and integrating internal systems to a public cloud and verification and evaluation of cloud-migration using internal pilot systems and its effects.

As we migrate internal systems to K5 on a full-scale basis and operate them in the future, we will enhance the internal cloud service and accumulate a large amount of knowledge and know-how by applying IaaS and PaaS provided on K5 to internal systems. We believe this will not only to lead to an improvement in K5 quality and enhancement of new products and services including PaaS, but also will definitely contribute to Fujitsu's cloud business. Needless to say, using in advance a cloud service to be offered to customers should make it possible to provide customers with the value of knowledge and know-how obtained internally in addition to a feeling of security in use of the service. To that end, we are committed to successfully completing the project of migrating the internal systems to K5 to be implemented in the entire Fujitsu Group.

References

1) Fujitsu: Fujitsu Launches MetaArc, Its Digital Business Platform.
http://www.fujitsu.com/global/about/resources/news/press-releases/2015/0929-01.html
2) 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

Makoto Aizawa
Fujitsu Ltd.
Mr. Aizawa is currently engaged in the promotion of migration of internal systems to K5.

Tomohiro Kakuma
Toyama Fujitsu Ltd.
Mr. Kakuma is currently engaged in the planning and design of internal cloud services.

Akinori Kanamaru
Fujitsu CIT Ltd.
Mr. Kanamaru is currently engaged in the planning, development and operation of intellectual property systems and corporate common systems.