FUJITSU

shaping tomorrow with you

FUJITSU Cloud Service K5

Security Related Information

Version 1.5
January 26, 2018
FUJITSU LIMITED

Foreword (1/2)

Purpose of This Document

These materials provide a security overview of K5 (formerly known as Fujitsu Cloud Service K5 (IaaS) and now known as K5) for business and customer negotiations.

Please note that these materials do not include information on the K5 PaaS.

Prerequisite Knowledge

The following basic knowledge related to system design and operation is required

- Basic knowledge related to OSs.
- Basic knowledge related to the Internet and intranets.
- Basic knowledge related to security.
- Basic knowledge related to system design & operations such as backup, monitoring, and redundancy.

Foreword (2/2)

FUJITSU

Registered Trademarks

- FUJITSU Cloud Service K5 is a registered trademark of FUJITSU Limited.
- Product names mentioned in these materials are trademarks or registered trademarks of each respective company.
- System names and product names may not be followed by trademark symbols in these materials.

Copyright, Trademark and Intellectual Property Rights

- These materials are protected by copyright, trademark and intellectual property rights. No part of these materials may be reproduced, modified, or reprinted in any form whatsoever (electronic or mechanical) without the express written permission of FUJITSU LIMITED.

Disclaimer

- These materials are based on information that was current at the time they were released.
- The information in these materials is provided for reference, and may be subject to change without prior notice.
- FUJITSU LIMITED in no way guarantees the accuracy, merchantability, or the suitability for use of these materials.

  There are no explicit or implicit guarantees or conditions regarding these materials.
- FUJITSU LIMITED takes no responsibility in relation to these materials.
- Fujitsu assumes no responsibility for infringement of any patent rights or other rights of third parties arising from the use of information in these materials.

Export Administration Regulation Declaration

- Exportation/release of these materials may require necessary procedures in accordance with the regulations of your resident country and/or US export control laws.

Revision History

Version	Date of Update	Content of Revision
1.0	May 11, 2017	First version
1.1	June 20, 2017	Added information regarding lightning countermeasures (p.15) and supplementary information regarding VLANs (p.22)
1.2	July 28, 2017	Made minor corrections (p.22, 27)
1.3	August 18, 2017	Made minor corrections (p.2, 17)
1.4	October 3, 2017	Made minor corrections (p.17) and updated description (p.33)
1.5	January 26, 2018	Modified diagram (p.22)

Index

FUJITSU

Chapter 1: Introduction

1.1 What is Information Security?

FUJITSU

In the "Information Security Guidelines" (*1 - 2) announced by OECD in 1992, the objective of information security is defined as follows:

"The objective of security of information systems is the protection of the interests of those relying on information systems from harm resulting from failures of availability, confidentiality, and integrity."

Confidentiality, integrity, and availability are defined as follows:

- Confidentiality : the characteristic of data and information being disclosed only to authorized persons, entities and processes at authorized times and in the authorized manner.
- Integrity : the characteristic of data and information being accurate and complete and the preservation of accuracy and completeness.
- Availability : the characteristic of data, information and information systems being accessible and usable on a timely basis in the required manner.

These are referred to as CIA, using the acronym in English, and are the "Three elements of information security".
In each element constituting a system, and in system operation, awareness of "the three elements of information security" and introduction of countermeasures is important to raise the security of an entire information system.

(*1) OECD Guidelines for the Security of Information Systems, 1992
http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.html
(*2) Digital Security Risk Management,2015 : The latest (2015) version of OECD's security guidelines
http://www.oecd.org/sti/ieconomy/digital-security-risk-management.htm

1.2 Concept of Information Security in the Cloud (1/2)

FUJITSU

When operating a system using the cloud, it is necessary to understand the cloud-specific information security concepts.

In the cloud (PaaS), system components managed by system administrators, are quite different from systems operating on-premises.

Components of a System (Comparison Aspect)	On-Premises	Cloud
Facilities where physical equipment is installed	Managed by system administrators belonging to information system departments	Managed by cloud service providers (Users are not involved)
Maintenance of physical equipment (Physical servers, network equipment, etc.)	Managed by system administrators belonging to information system departments	Managed by cloud service providers (Users are not involved)
Management of the virtualization platform	Managed by system administrators belonging to information system departments	Managed by cloud service providers (Users are not involved)
Operation and maintenance of OSs, middleware, business applications, etc.	Managed by system administrators belonging to information system departments	Managed by cloud service users (using cloud offering functions, standard OS functions, or third party software)
Network configuration such as firewalls	Managed by system administrators belonging to information system departments	Managed by cloud service users (using cloud offering functions, standard OS functions, or third party software)

1.2 Concept of Information Security in the Cloud (2/2)

FUJITSU

Pros and Cons of information system security control:

System Location	Pros	Cons
On-Premises	As system administrators can manage all of the system components constituting the information system by themselves, they can decide the security level required for the system by themselves and configure the system as necessary.	System administrators must configure and operate all system components constituting the information system by themselves.
Cloud	System administrators (of the cloud service user) are not responsible for the installation of physical devices and operations related to physical devices / virtualization infrastructure (such as responding to hardware failures and application of firmware / security patches). OSs, middleware, business applications, etc. need to be operated and managed by the system administrator as in conventional systems.	System administrators (of the cloud service user) must trust that the facilities managed by the cloud service provider, along with the physical devices / virtualization infrastructure, are operating properly and are managed securely.

In other words, when using a cloud service, it is necessary for the cloud service provider and cloud service user to cooperate to ensure the security of the overall system after understanding each other's mutual responsibilities.

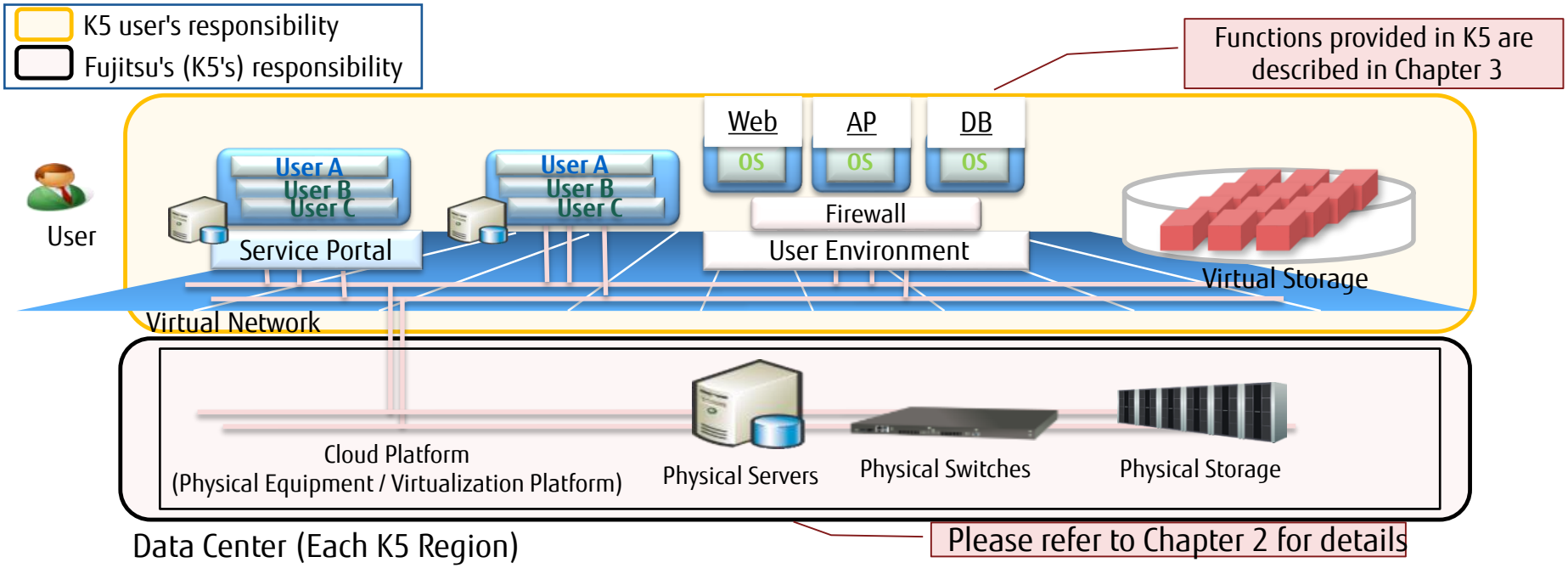
Such a model is common in the cloud, for example, Amazon's AWS has a model named "shared responsibility model."

Even when using K5 it is very important to understand this way of thinking.

1.3 K5 (IaaS) Division of Responsibilities in Service

- The division of responsibility in the K5 IaaS service is as follows:
  - Fujitsu (K5) is responsible for the facilities (data center), physical equipment, and the virtualization platform.
    Chapter 2 describes how Fujitsu ensures security for these facilities in K5.
  - K5 users are responsible for K5 service user management, configuration and operational management of each component (OS, middleware, storage, firewall, etc.) provided by the K5 service, and management and monitoring of business applications.
    Chapter 3 describes the functions provided in K5 in order to use these services securely.

Responsibility division when using K5 (IaaS) *



* Note: Official information is defined in the K5 terms of service.

FUJITSU

Chapter 2: Ensuring Security for the K5 Cloud Infrastructure

2.1 Summary

FUJITSU

This chapter describes the kind of technical / operational measures that are taken by K5 in the data center and cloud infrastructure components (physical servers, storage, network) in order to provide customers with the cloud infrastructure of K5 in a secure state, from the viewpoint of the "three elements of information security" below.

- Confidentiality (Measures against unauthorized access by third parties)
- Integrity (Prevention of data falsification, and trail management)
- Availability (Avoidance of single point of failure)

*Notes on the description in Chapter 2.

- The data center described in Section 2.2, is Eastern Japan Region 1.

  (In Japan, similar measures are being implemented for other regions.
  The measures are different for regions outside Japan.)
- Regarding the descriptions of the physical devices (network, storage, virtual servers, virtualization infrastructure) described in Section 2.3 and later, these refer to the computing, storage, and network used by the K5 standard service. The "Dedicated Physical Server Service" provided by K5 is not described in this manual.

2.2 Measures in K5 Data Centers (1/4)

FUJITSU

Confidentiality

Example Using the East Japan Region

The following measures are implemented at the K5 data center, to prevent third parties from physically entering the data center.

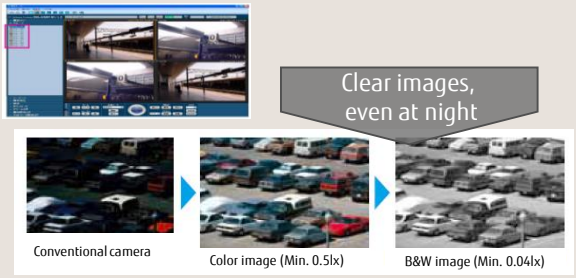
Infrared Sensor Monitoring Around the Data Center

- Infrared sensors are installed around the data center

If anything unusual is detected, it is automatically recorded on camera and security guards are sent immediately

High Precision Monitoring

- High-precision monitoring with advanced cameras, day and night
- Detect abnormal conditions using motion detection



24-hour Manned Monitoring

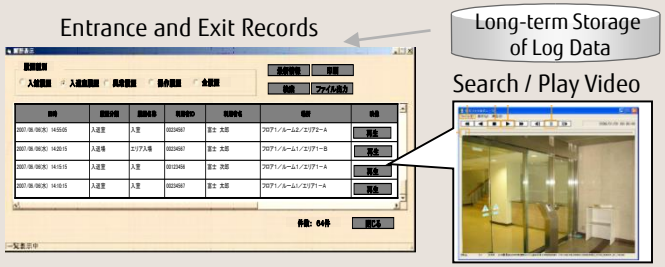
- Onsite monitoring 24 hours a day

Security guards on site 24 hours a day

*Crime prevention drills carried out twice a year in collaboration with the local police department

Log Management and Tracing Management

- All monitoring footage and entrance / exit logs are stored long-term
- Video log is searched in conjunction with authentication history



2.2 Measures in K5 Data Centers (2/4)

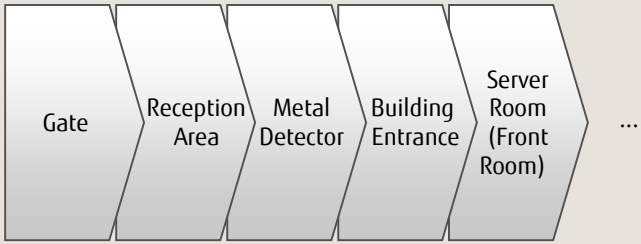
Confidentiality

Example Using the East Japan Region

The following measures are implemented to ensure only qualified personnel are able to access K5.

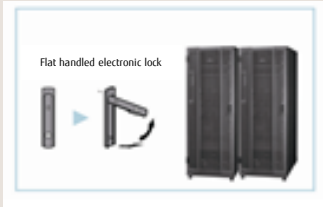
Setting of Security Areas

- There are multiple security areas set in the data center
- Visitors can only enter the areas to which they have been granted access



Rack Security

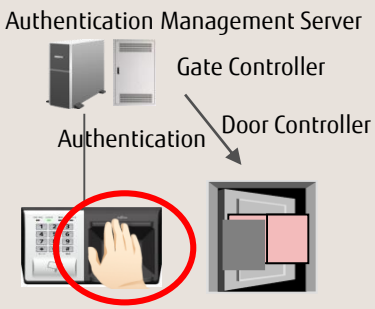
- Rack locking / unlocking management uses palm vein authentication
- Data center-provided racks use electronic locks



Entry Control

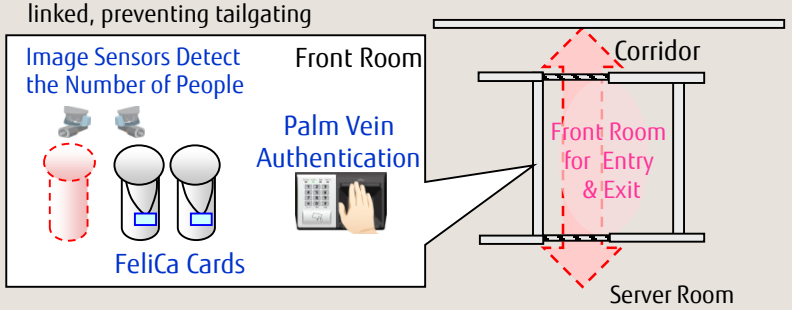
- Biometric authentication is performed using palm vein authentication

Authentication accuracy of palm vein authentication = False acceptance rate 0.00008% or less (one in 1.25 million people)



Tailgating Prevention

- FeliCa cards, flow line cameras, and biometric authentication are linked, preventing tailgating



2.2 Measures in K5 Data Centers (3/4)

FUJITSU

- Integrity

Example Using the East Japan Region

  - K5 access log management for the Cloud infrastructure

Access log management is implemented to prevent operators who have valid access rights from modifying and/or leaking data of K5 cloud platform, intentionally or accidentally.

If a failure or a security incident occurs in K5, the root cause analysis carried out using these logs and appropriate measures are taken. This log data is not provided to K5 users, because these access logs are confidential information of the K5 cloud platform.

Categories of Logs	Definition	Log Details
1) Management status	Log information to confirm whether the information security management system and management process are working properly.	Logging of the details of each internal action, and the approval histories.
2) Control status	Log information to confirm whether individual security measures are working properly.	Logging of the activities of security measures for customer's common functions and the physical infrastructure environment.
3) Security violation detection	Log information to notify that individual security measures are facing a threat due to unauthorized acts.	Logging of unauthorized access to the system platform detected by IDS (Intrusion Detection System).
4) Assurance of traceability in security incidents	Log information to confirm the details of security incidents and the influence, after unauthorized acts are performed.	Preparation for retrospective investigation by storing the logs of 1), 2), and 3) above, for a long period of time.

2.2 Measures in K5 Data Centers (4/4)

FUJITSU

Availability

Example Using the East Japan Region

The following measures are being taken so that users can use resources on K5 when they need to.

- In Japan, K5 is operated at a data center that is equivalent to Tier 3 or higher, and various measures are taken such as earthquake countermeasures, water-related damage countermeasures (flooding, leakage, water shortages, condensation), power failure measures, fire countermeasures, etc.
- Multiple facilities with separate power supply systems and air conditioning facilities are offered as availability zones to enable continued operation even if an availability zone goes down.
- We provide K5 service in multiple regions (data centers) to provide a mechanism for business continuity even when wide area failures occur.

Earthquake Countermeasures

- Seismic isolation (building and utility equipment).
- Supporting base is a strong stratum of laminar gravel soil.

Measures Against Water-related Damage

- First floor is 3.7 m above sea level
- Water leakage sensors
- Stockpile of 1,400 tons of water for air conditioning
- Dedicated temporary holding boxes
  (with condensation prevention using temperature adjustment)

Measures Against Power Failures

- Separated substations, dual routed power
- Redundant UPSs provided
- In-house power generation facilities, 1,000 kl stockpile of heavy oil (final stockpile) and supply contract (3rd party)

Fire Countermeasures

- N2 (Nitrogen) fire suppression
- Ultra high sensitivity smoke sensors
- Situated near the fire department (minimum time to arrival: 7 minutes, joint training conducted twice a year)
- Lightning countermeasures (Protection level I, JISA 4201)

(*1: The term "Tier 3" mentioned here is based on the data center facility standards defined by the Japan Data Center Council (JDCC)).
For details, please refer to the JDCC Guidelines for Data Center Facility Standards
http://www.jdcc.or.jp/english/fs.html

2.3 Measures Regarding K5 Network (1/2)

FUJITSU

Confidentiality

As measures against external electronic intruders (such as hackers) the following steps are taken for the K5 cloud infrastructure.

- Attempts at unauthorized external access to the K5 cloud platform are monitored by IDS devices. When an access attempt is suspected as being unauthorized, stakeholders are automatically notified, and are asked to take countermeasures, as defined in the operation rules.

  The monitoring of unauthorized access by IDS is not provided for individual K5 customer environments.
- Before the K5 service is made available to customers, the K5 platform is audited by the security department of Fujitsu Limited, and it is confirmed that there are no known vulnerabilities from the viewpoint of third party organizations who are not involved in K5 development activities.

2.3 Measures Regarding K5 Network (2/2)

FUJITSU

- Integrity
  - Encryption of network communication

All communication within K5 is encrypted, except some communications which cannot be unencrypted due to operational requirements of the K5 platform. However, we plan to encrypt those unencrypted communications in the future.

Note

Although all communication related to operation of the K5 cloud platform is encrypted, this does not mean that there is an encryption function provided for the communication performed by K5 users.

- Availability
  - Redundancy of network devices

In the K5 cloud platform, physical network devices are in redundant configurations. All of the K5 network devices are generally redundant, and the network nodes which are not redundant are monitored at all times, and if a failure is detected the affected node is quickly replaced with a working network node.

In addition, the devices connecting K5 to the Internet are also in redundant configurations. However, when a failure occurs on a device connecting to the Internet, it is necessary to switch routing, so temporary disconnection may occur.

2.4 Measures Regarding K5 Physical Storage (1/2)

FUJITSU

- Confidentiality
  - Limits on physical access to physical storage

In order to prevent theft of the physical disk drives used for physical storage, the racks containing physical storage are locked with electronic locks. It is not possible to access physical storage unless a qualified person performs biometric authentication and unlocks the electronic lock of the rack.

  - Measures against information leakage using physical disk encryption

Disks stored in physical storage are encrypted using storage devices (Self-Encrypting Drives), and encryption keys are strictly managed using a key management server. Encryption keys cannot be extracted from disk drives.

The authentication keys used in encryption authentication for self-encrypting drives are stored on a key management server, so if a disk is physically removed from physical storage the data on it cannot be decrypted.

If exchange or disposal of disks is performed, those disks are not physically destroyed, but they are disposed of in a state where it is impossible to recover data from them.

Note

Encryption is performed for entire disks. When a K5 user handles data on a virtual server, it can always be viewed in a transparent state and consideration of encryption is not necessary.

If it is necessary to encrypt information on individual virtual servers on K5, the K5 user needs to consider their own data encryption method.

2.4 Measures Regarding K5 Physical Storage (2/2)

FUJITSU

- Integrity
  - Log management of storage operations

    K5 informs stakeholders when prohibited operations and management operations (removal of disks, etc.) for storage are detected. The event logs related to storage operations are stored for a certain period of time, and it is possible to investigate the root cause of prohibited operations.

- Availability
  - Redundancy of storage disks

    The redundancy configuration of storage disks in K5 is equivalent to RAID 6.

  - Data replication of object storage

    Data on object storage is automatically replicated to a different AZ in the same region using data duplication. Data multiplexing is not performed for block storage.

2.5 Measures Regarding K5 Physical Servers (1/2)

- Confidentiality
  - Access to servers is restricted

    In order to restrict physical access to K5's server equipment to only qualified people, the racks containing servers are locked with electronic locks. Servers cannot be accessed physically, unless a qualified person performs biometric authentication to unlock the electronic lock of the rack.

  - Remote access to servers is restricted

    In addition, remote access to K5 server equipment is strictly restricted to only qualified personnel, with no access for unauthorized third parties.

2.5 Measures Regarding K5 Physical Servers (2/2)

FUJITSU

- Integrity
  - Anti-virus protection

Security checks such as checking for viruses and vulnerabilities are carried out frequently for the devices used in K5 development and K5 operation activities, to prevent virus infections during operation of the K5 cloud infrastructure. This prevents tampering, leakage, and damage to the K5 cloud infrastructure resulting from virus infections.

Note

The measures above only apply to the K5 cloud infrastructure. For the resources managed directly by K5 users, such as the virtual server of K5 users, it is necessary for the users to take their own anti-virus measures.

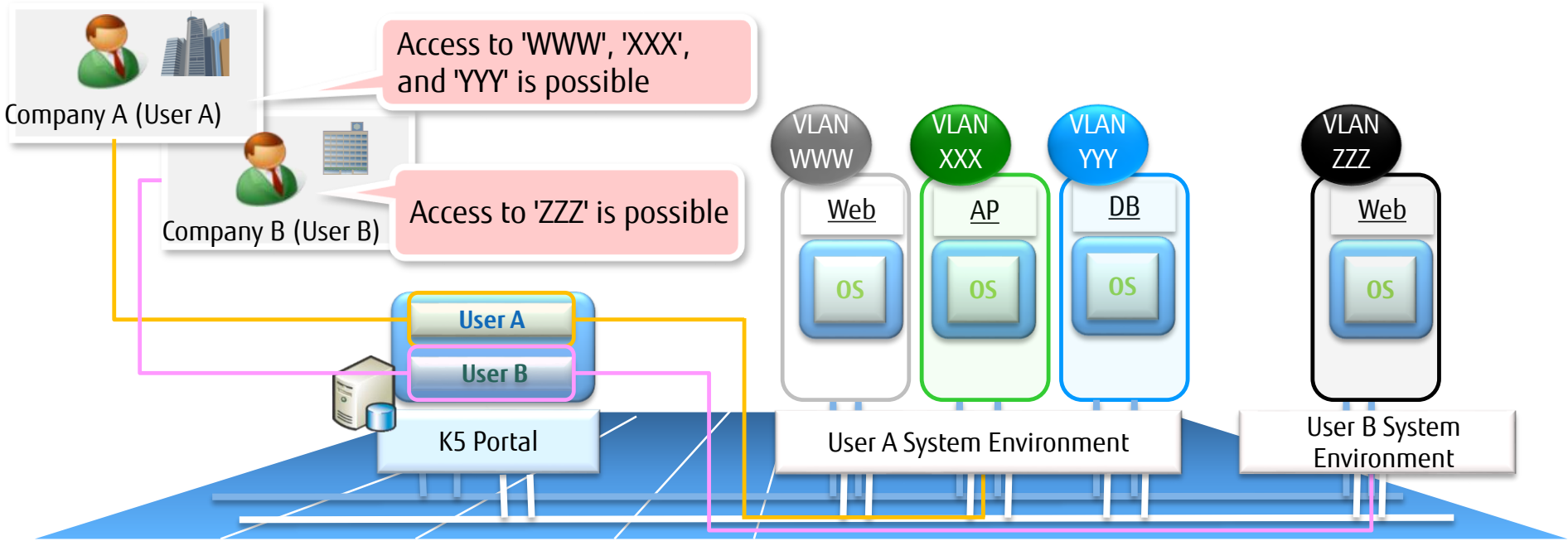
- Availability
  - Redundant server power supply

In addition to the duplication of the power supply of server itself, power supply equipment is also duplicated. UPSs are also installed to provide a backup power supply.

2.6 Measures Regarding K5 Virtualized Infrastructure (1/2)

- Confidentiality
  - Partitioning by VLAN (isolation)

In K5 IaaS, the network and the virtual server environment are shared by multiple customers, but individual environments are logically separated. Therefore customers using K5 will not see any data or transferred information of other customers.
* Administrator communication (monitoring, etc.) and user communication also use separate VLANs.



2.6 Measures Regarding K5 Virtualized Infrastructure (2/2)

- Integrity
  - Response in case a vulnerability is found in the virtualized infrastructure

    The dedicated security department of Fujitsu are constantly monitoring vulnerability information relevant to the virtualized infrastructure of K5. If a vulnerability is found in the virtualized infrastructure used in K5, the K5 development team is notified. Following the investigation of the applicability of the vulnerability to K5 functions and services, the appropriate security patches are quickly applied.

- Availability
  - Auto failover function of virtual servers

    If the physical host machine in data center is stopped, due to a failure or some other reason, the virtual servers running on that host machine can be automatically moved to another host machine, enabling continuity of operation without any auto scaling. Since this function cannot be used at the same time as the auto scale function, it is up to the K5 user to decide whether or not to use this function.

FUJITSU

Chapter 3: K5 Functions Provided for Secure Usage

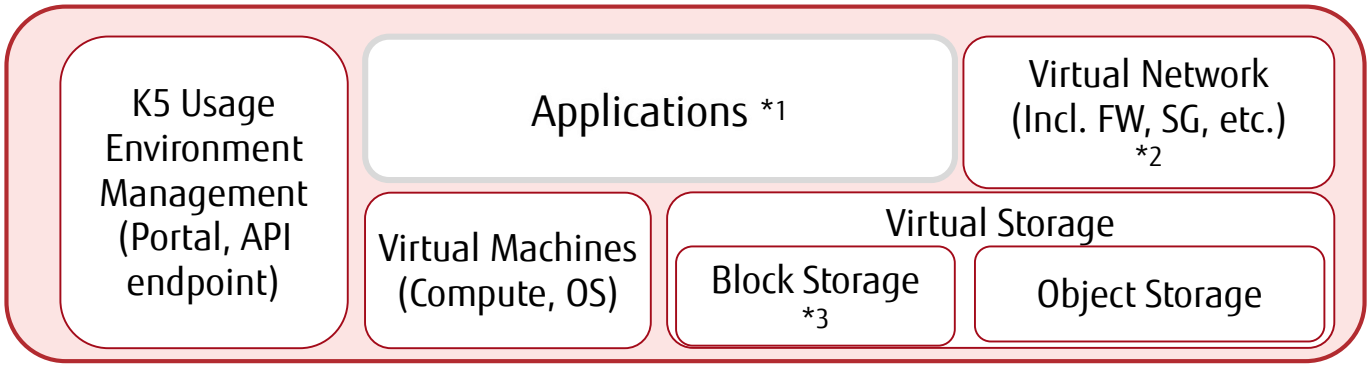
3.1 Summary

Users of K5 need to secure the OS and the other items shown below in their own K5 Tenant environment using functions provided by either K5, OS functions, or third party software.

*Please note that not only functions provided by K5 but also various other functions must be used in combination in order to enhance the security of the entire system. Consideration equivalent to that for conventional countermeasures for an on-premises system is also necessary.

In Chapter 3, we introduce the functions provided by K5 to enable secure use of K5.

Details of individual functions and design guidelines are not described in this chapter. Please see the K5 (IaaS) Features Handbook and other chapters of SE handbook, etc. Also, some of the K5 services, such as the database service, the mail delivery service, and the PaaS service are not described in this chapter.



*1: There is no description in this chapter as K5 does not provide the security function.
*2: FW: Firewall
SG: Security group
* 3: Attached to servers for use.
System storage (for the system area)
Expansion storage (for the data area)

3.2 Security Functions Related to K5 Usage Environment Management

FUJITSU

Security related functions for the K5 usage environment management function (portal and API endpoint) are described below.

K5 Service / Function Name	Summary	Expected Effects in Terms of Security
K5 User management function	This function enables creation of users to access the services and resources on K5 and the setting of appropriate operational authority based on each user's role.	By setting the appropriate authority settings, it is possible to prevent damage to systems by third-parties, through acts such as deleting K5 resources.
Certificates and password authentication	It is possible to select from the following two authentication methods for logging in to the K5 portal and obtaining tokens for in order to execute APIs. (1) Password authentication (2) Certificates and password authentication	When authentication method (2) is selected, as authentication requires 2 factors, it is possible to prevent access by unauthorized users.

3.3 Security Functions Related to the K5 Virtual Machine Environment

FUJITSU

Security related functions for K5's virtual machine environment are described below.

K5 Service / Function Name	Summary	Expected Effects in Terms of Security
SSH login to virtual servers using the key pair management function	This function enables registration and management of key pairs for SSH communication when creating virtual servers.	By using the key file of the key pair when connecting to a virtual server, it is possible to login using SSH or to obtain login information. As an ID and password are not used, the risk of servers being hacked using brute force attacks can be reduced.
Provision of update server for virtual machines	We provide OS patch application environments (WSUS / RHUI / yum).	It is possible to apply OS patches and updates on K5.
Trend Micro Deep Security as a Service (DSaaS) option	Provides the following functions to virtual servers: - Anti-virus function - Firewall function for servers - Log monitoring function - IDS / IPS functions for servers - Web reputation function - Change management function for virtual servers	Using the functions on the left you can improve the security of virtual servers.

3.4 Security Functions Related to K5 Virtual Storage

FUJITSU

Security related functions for K5's storage are described below.

Block Storage

K5 Service / Function Name	Summary	Expected Effects in Terms of Security
Snapshot function	This function enables creation of a snapshot of in-use block storage.	In case of an unexpected event such as data corruption, it is possible to restore the data on the storage disk from the snapshot.
Virtual server image management	This function enables creation and management of virtual server images from the system storage of a virtual server.	When it is necessary to rebuild a virtual server for some reason, it is possible to create a new server using an virtual server image acquired in advance.

Object Storage

K5 Service / Function Name	Summary	Expected Effects in Terms of Security
Access policy configuration	It is possible to configure read / write access authority for object storage.	It is possible to prevent data access from third parties that do not have the appropriate authority to access the object storage.

3.5 Security Functions Related to K5 Virtual Networks

FUJITSU

Security related functions for K5's virtual networks are described below.

K5 Service / Function Name	Summary	Expected Effects in Terms of Security
IPsec VPN function	This provides the IPsec VPN gateway function for connecting to on-premises environments or for system connection between regions.	Use of a VPN connection using IPsec between a K5 user 's IPsec gateway and a K5 virtual router makes it possible to reduce the risk of attack from a third party on the communication route.
SSL-VPN function	The SSL-VPN connection function is provided to enable secure login and management operations for the virtual servers built on a system.	By using SSL encrypted communication between remote access terminals and K5 it is possible to use VPN connections to reduce the risk of attack from a third party on the communication route.
Private connection options	These options provide functions for establishing private connections between K5 and the user's individual environments such as hosting environments and on-premises environments.	By using private connections it is possible to reduce the risk of attack from a third party on the communication route.
Firewall service	This service provides packet filtering capabilities to the virtual router.	By blocking unauthorized communication with the virtual router it is possible to prevent unauthorized access by a third party to the system.
Security group function	This function enables users to perform packet filtering on the ports connected to the virtual server. It is also possible to group defined and configured rule settings.	By blocking unauthorized communication with virtual servers it is possible to prevent unauthorized access by a third party to the system.

FUJITSU

Chapter 4: K5 Security Promotion Framework and Efforts

4.1 Security Promotion System (1/3)

■Organizational Approach to Information Security

Based on the basic global cloud information security policy and management standards, the FUJITSU Cloud Service K5 continuously operates in accordance with the operational procedures (which reflect the unique requirements of each country), which are followed by operators who have been trained with systematic security education.

In addition to the technical measures used to protect user's information assets, Fujitsu also takes preventive measures for service operation, such as limiting the use of terminals, assigning access rights, and managing logs of operator access.

In the event of a security problem, Fujitsu will identify the event and investigate the root cause, and promptly respond in a systematic manner minimizing the damage and keeping it local without letting it spread.

- **Executive commitment**
- **Roles and organization**
- **Information management classification**
- **Compliance**
- **Security control measures**
- **Vulnerability diagnosis**
- **Risk assessment**
- **Monitoring and auditing**
- **Service desks, etc.**

Global Common Rules

Based on ISO 27000s, NIST(*1), ENISA(*2), Guidelines of the Cloud Security Alliance, etc.

*1 National Institute of Standards and Technology
*2 European Network and Information Security Agency

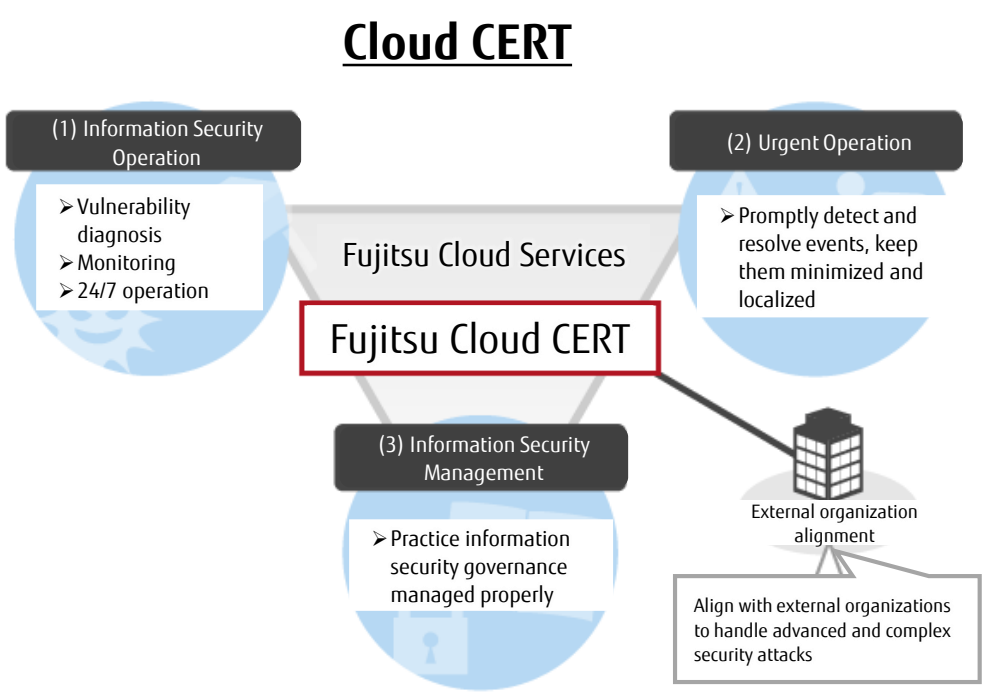
4.1 Security Promotion System (2/3)

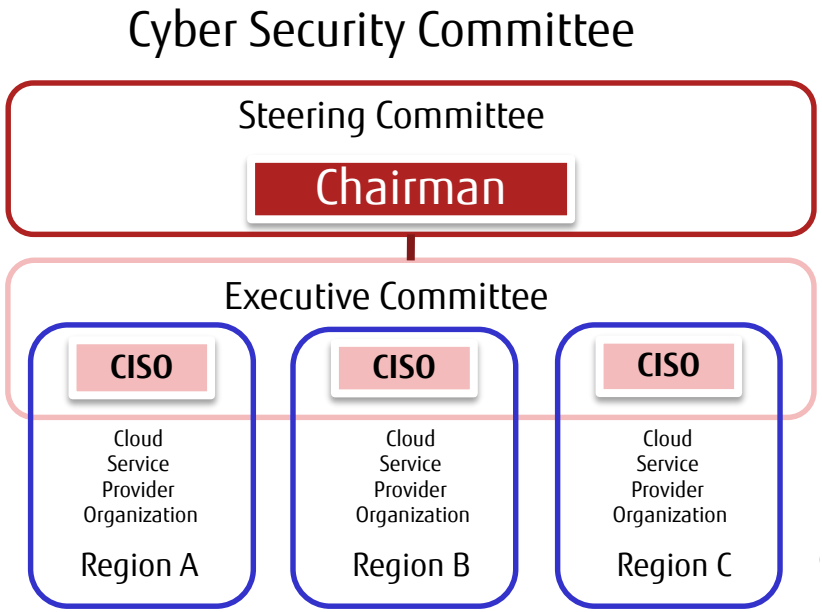
■Establishment of a Specialized Cloud Security Organization

We strive to prevent and detect security threats (cyber terrorism, unauthorized use, information leaks, etc.) in FUJITSU Cloud Service K5. If any security problems occur, the cloud security specialist team "Fujitsu Cloud CERT" responds promptly. We provide a trusted (highly reliable) service.

Fujitsu Cloud CERT is a skilled security team specializing in cloud computing. We monitor 24 hours a day, 365 days a year, and protect the FUJITSU Cloud Service K5 infrastructure from security threats.
If any security accidents are detected, we will respond promptly to solve any problems.

In addition, we have established an internal cyber security committee to properly manage "people", "assets", and "information" in FUJITSU Cloud Service K5 and ensure that information security governance is applied.





4.1 Security Promotion System (3/3)

FUJITSU

■ Cooperation with External Security Incident Teams

By coordinating with external security incident systems, we are able deal with security issues in terms of sophistication and complexity from a global perspective.

- FIRST (Forum of Incident Response and Security Teams)
  Provides support for sharing and providing information on security incidents. There are more than 300 member companies registered, including CSIRT members in 67 countries and regions.
  Global members: Cisco, Intel, Microsoft, IBM, HP, etc.
  Japanese members: Rakuten, KDDI, RICOH, and Panasonic. etc.

- JPCERT/CC (JPCERT Coordination Center)
  An organization that collects information on events related to computer security generated via the Internet, provides incident support, provides computer security related information, and is a representative CSIRT in Japan.

- Japan CSIRT Council (CSIRT: Computer Security Incident Response Team)
  Work to realize an organization with tight coordination between affiliated teams in order to enable rapid resolution of computer security incidents.
  Members: Japan IBM, Hitachi, LAC, Rakuten, Yahoo, NRI SecureTechnologies, NEC Group, and IIJ Group, etc.

4.2 K5 Security Operation (1/4)

■Vulnerability Diagnosis, Monitoring and Detection

FUJITSU Cloud Service K5 has information security measures such as vulnerability diagnosis and monitoring of the K5 platform in place, and operates the system 24 hours a day, 365 days a year.

- Vulnerability Diagnosis

Every day, the Security Operation Center (SOC) diagnoses vulnerabilities of the FUJITSU Cloud Service K5 platform. If a problem occurs, the SOC consults and discusses with related departments and coordinates with the security patch management system.

- Monitoring and Detection

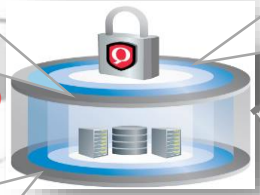
We conduct monitoring of attempted unauthorized access and malware on a 24x7 basis. If there are any problems detected, we will share information with the related departments, coordinate and investigate promptly, and we will also analyze the relationships between logs and events and report our findings.

■ Vulnerability Diagnosis

Fujitsu's Security Operation Center (SOC) is constantly operational. Daily diagnosis of the K5 platform is carried out and coordinated with the patch management system.

■ Collect / Analyze / Manage Vulnerability Information

Information on cloud service platform vulnerabilities is constantly collected and the analysis of their threat levels is applied to modification and patch management.



Fujitsu
Cloud CERT

■ Monitoring and Detection

- Monitor malware and attempts at unauthorized access
- Analysis of the relationships between logs and events

4.2 K5 Security Operation (2/4)

FUJITSU

■ Establish Process for Collecting, Analyzing and Managing Vulnerability Information

We have established a process which involves constant collection of vulnerability information on the FUJITSU Cloud Service K5 platform, carrying out of analysis by the dedicated team "Fujitsu Cloud CERT", performance of triage based on the level of impact, and reflection on change management / patch management.
We provide trusted (highly reliable) public cloud services to users by implementing vulnerability countermeasures against the FUJITSU Cloud Service K5 infrastructure based on change management and patch management.

Vulnerability Information Collection

- Collect feeds from about 100 overseas / domestic sites
- Individual acquisition of "JPCERT / CC early warning information"
- Collect JPCERT / CC VRDA * feeds

*Vulnerability Response Decision Assistance

Impact Analysis

Analysis process
- Triage (by impact)
- Determine relevant / irrelevant details of the product

Analysis scheme
- Handled by the dedicated risk control team

Change Management/Patch Management

Final decision at CAB*

- Security-Sub CAB considers priority

*Change Advisory Board

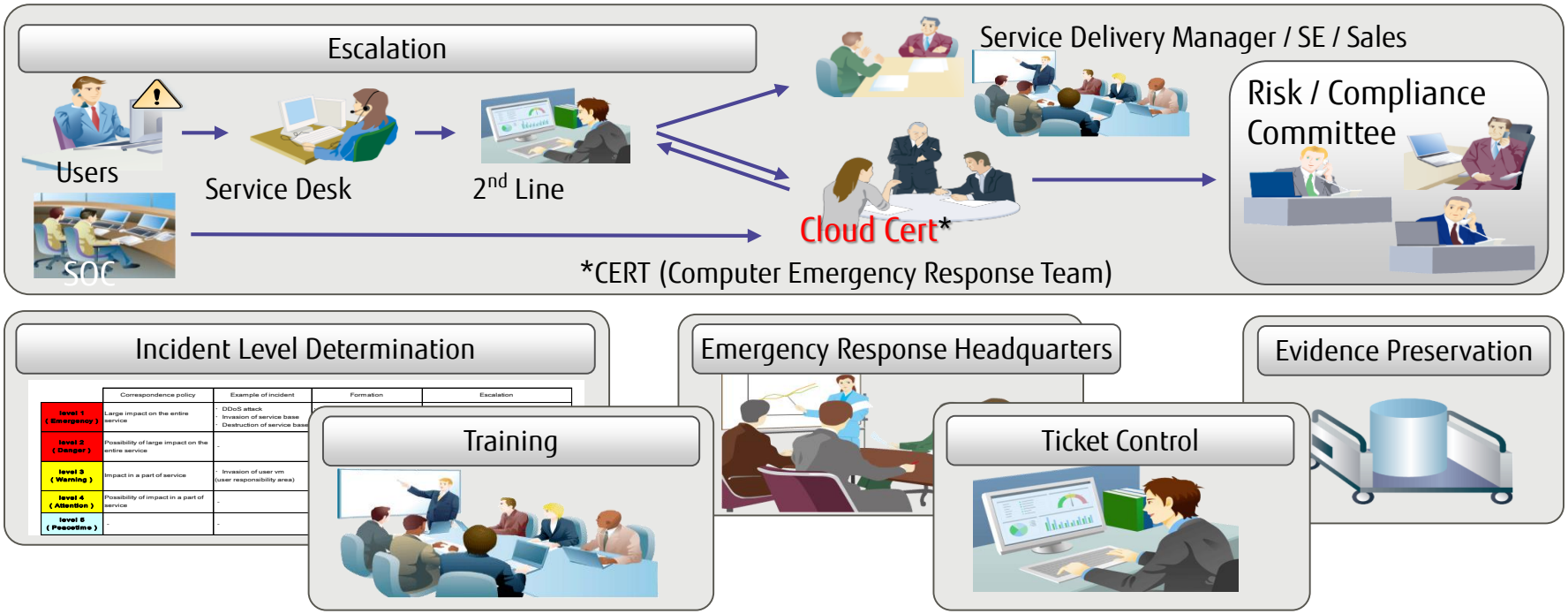
4.2 K5 Security Operation (3/4)

■ Implement Prompt and Reliable Incident Management

FUJITSU Cloud Service K5 initiates a pre-defined response process upon the occurrence of a security incident, and in the event of a security incident, we will promptly identify, resolve and localize the event.

When a user informs us of a security incident regarding the FUJITSU Cloud Service K5 infrastructure (excluding problems unique to the user's system), the information is quickly escalated from the front line to the back end, and is also escalated to the specialist team. The team conducts incident-level triage, confirms events, determines the impact (the degree of influence) and establishes a Cloud Security Committee if necessary.

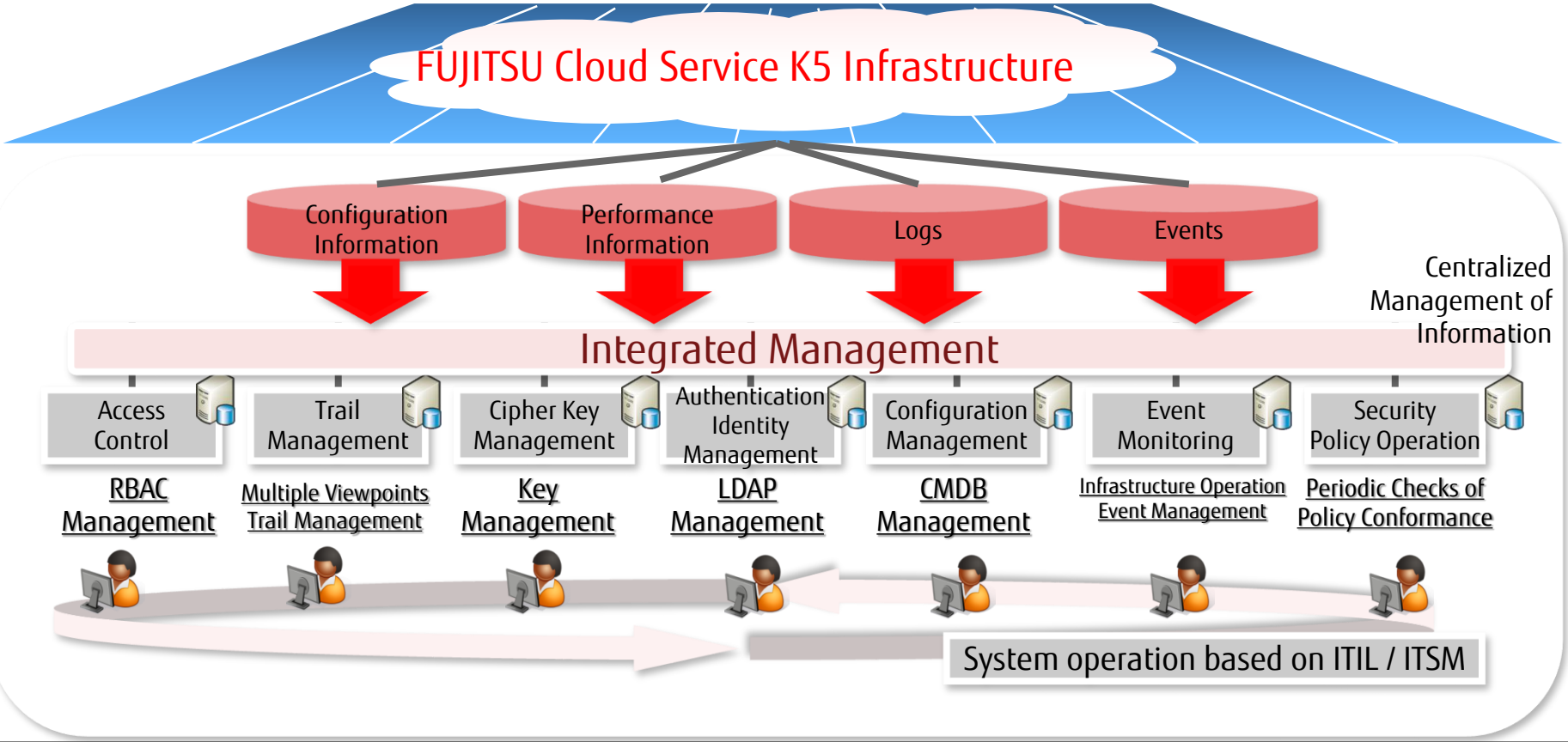
We regularly conduct training and perform operation drills so that we can act promptly, confirm collaboration with related departments, set up an emergency response headquarters, and preserve evidence when a security incident occurs.



4.2 K5 Security Operation (4/4)

■ Centralized Management of Information

Through integrated management of "configuration information", "performance information", "logs", and "events" of the FUJITSU Cloud Service K5 infrastructure, we have established a system that enables us to visualize issues and respond promptly to any problems that may occur.
The K5 cloud platform constantly monitors the status of each resource device (physical server, network, storage etc.) related to the infrastructure, the network usage status, the API acceptance status, etc. and manages capacity and the network in order to maintain the service. We monitor the FUJITSU Cloud Service K5 infrastructure but we do not monitor the resources of individual users.



Appendix: Glossary (1/2)

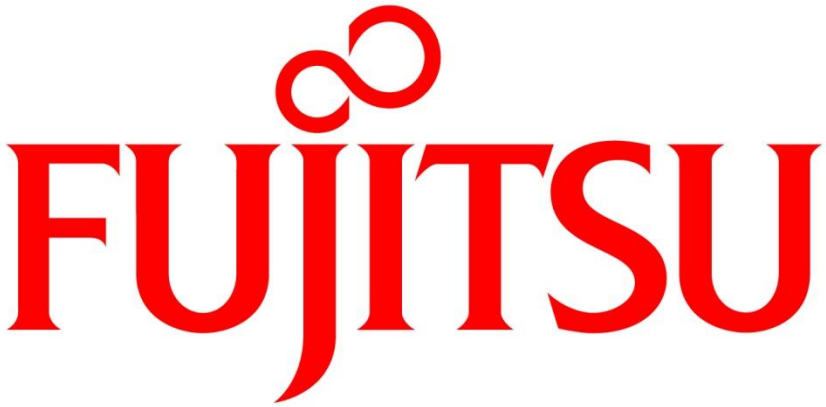
FUJITSU

Term	Description
API endpoint	The connection destination that clients use to access APIs.
auto failover	A mechanism that automatically restarts the service on other hardware when trouble occurs on the hardware being used to provide a service.
auto scaling	A function that automatically increases and decreases the number of virtual servers used based on conditions such as the system load.
availability zone	The unit in which the physical equipment such as data center equipment and equipment for providing services is shared.
block storage	Devices that can be used for system storage and additional storage.
CMDB	Configuration Management DataBase. A database used to manage the information (configuration management) regarding all of the components necessary to provide a service.
external network	A network prepared by K5 for connection to the Internet.
firewall service (FW)	Packet filtering rules for virtual routers.
internal network	A network that is not connected to the Internet.
key pair	The combination of a public key and a private key that is used when logging in to a virtual server with SSH or encrypting a random Windows password. Only public keys are registered on virtual servers.
object storage	Storage that saves in units of objects (composed of contents and metadata).
port	A network interface that performs linking with IP addresses in order to connect resources such as virtual servers to a network.
RBAC	Role-based access control. Access control that enables flexibility through the use of roles.
region	A unit used to geographically divide a country or areas within a country.
security group	A function that groups the rules used to perform packet filtering for the ports connected to a virtual server.
snapshot	An image of block storage taken at a particular point in time. Snapshots can be used as backups.

Appendix: Glossary (2/2)

FUJITSU

Term	Description
Subnet	A logical subdivision of a network. Provides private IP address management, DHCP functions, and routing management for deployed resources.
tier	Data center facility standards decided by the JDCC (Japan Data Center Council). Data centers are divided into tiers 1 - 4, with 4 being the most reliable.
virtual network	A virtual network used for communication between resources such as virtual servers. They are created on a subnet basis.
virtual router	A function that connects an external network and a network, or a pair of networks.
virtual server image (image)	A function that enables easy replication of deployed virtual servers through the use of templates with all of the server-specific information deleted.



shaping tomorrow with you