Cloud Security Threats & Countermeasures

November 29, 2011

Korea Internet & Security Agency

Jeong, Hyun Cheol

(hcjung@kisa.or.kr)

KISA 한국인터넷진흥원
Korea Internet & Security Agency

Contents

I. Overview and Characteristics of the Cloud Service

II. Security Threats to the Cloud Service

III. Security Measures of the Cloud Service

IV. Conclusion (Q&A)

I-1. The Cloud Service Concept

- **Cloud service**

  - A service that leases computing resources over the Internet, for which payment is made according to the amount of resources used.

- **The concept of the computing environment is changing from possession to online lease with the introduction of cloud computing.**

  - "The age of possession will come to an end, and the age of access will come," Jeremy Rifkin, The Age of Access.

<Existing IT environment>

<Cloud service environment>

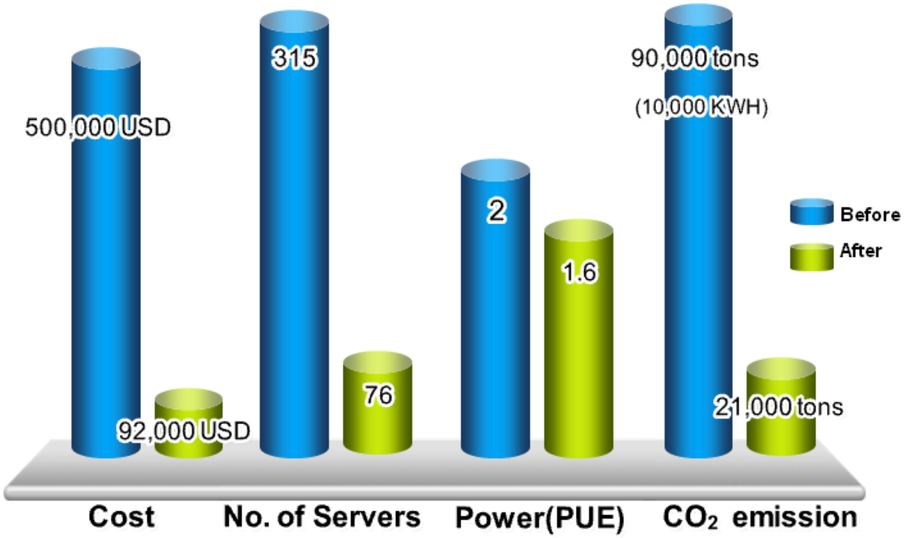
I-2. Overview

□ **Benefits of Cloud Computing → cost saving, energy efficiency and CO2 reduction**

□ **Considerations in moving to Cloud Computing: “Cost Reduction and Security Issues” are the top priorities**

Benefits of Cloud Computing

(Case of Korea Telecom)

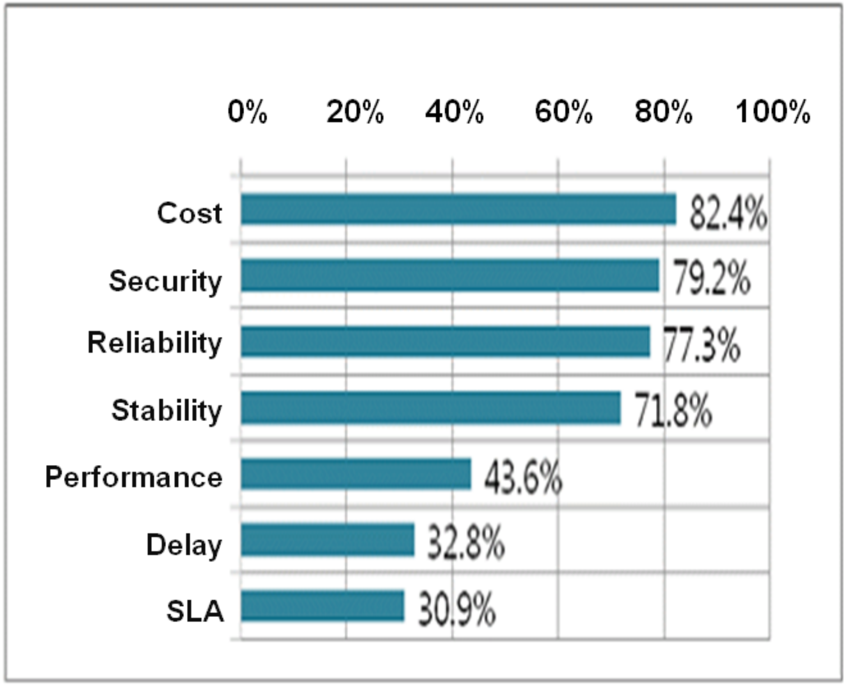


* PUE (Power Usage Effectiveness) = Total Facility Power / IT Equipment Power

o Results of applying cloud computing to KT's new services (2010)
(KT's own services, portals, web-hosting, domestic news media)

<Source: KT, Mar. 2011>

Considerations for Cloud Computing

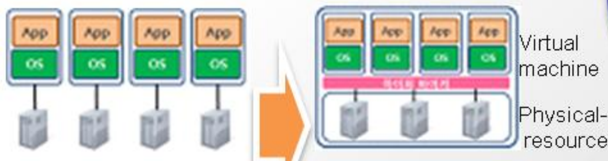


< Source: Nikkei Communications, Oct. 2009>

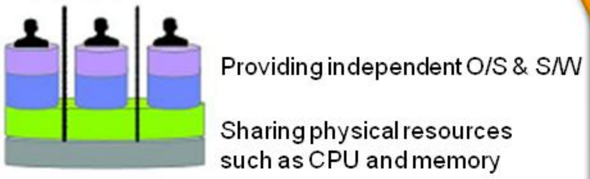
I-3. Characteristics of the Cloud Service – Security perspective

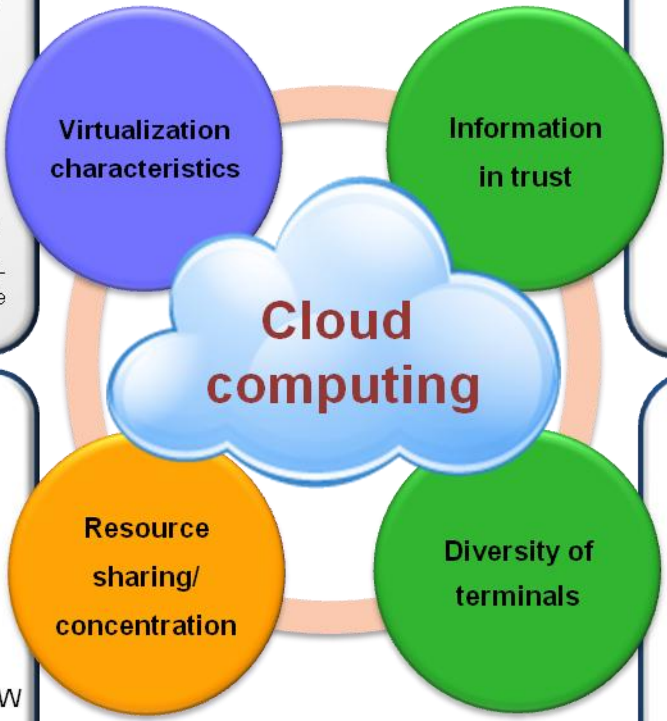
- **Integrating/Redistributing physical resources logically**

- Online provisioning of physical resources
- Increasing resource utilization efficiency



- **Virtual resources are allocated independently but physical resources are shared**


Providing independent O/S & S/W
Sharing physical resources such as CPU and memory



Virtualization characteristics

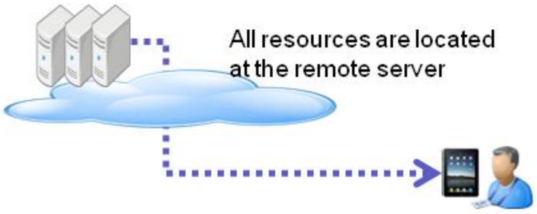
Information in trust

Cloud computing

Resource sharing/ concentration

Diversity of terminals

- **All users' resources are located at the cloud server managed by the service provider**



- **Accessing from various terminals such as smart-phones and tablet PCs, besides regular PCs.**

II-1. Are Cloud Services Safe?

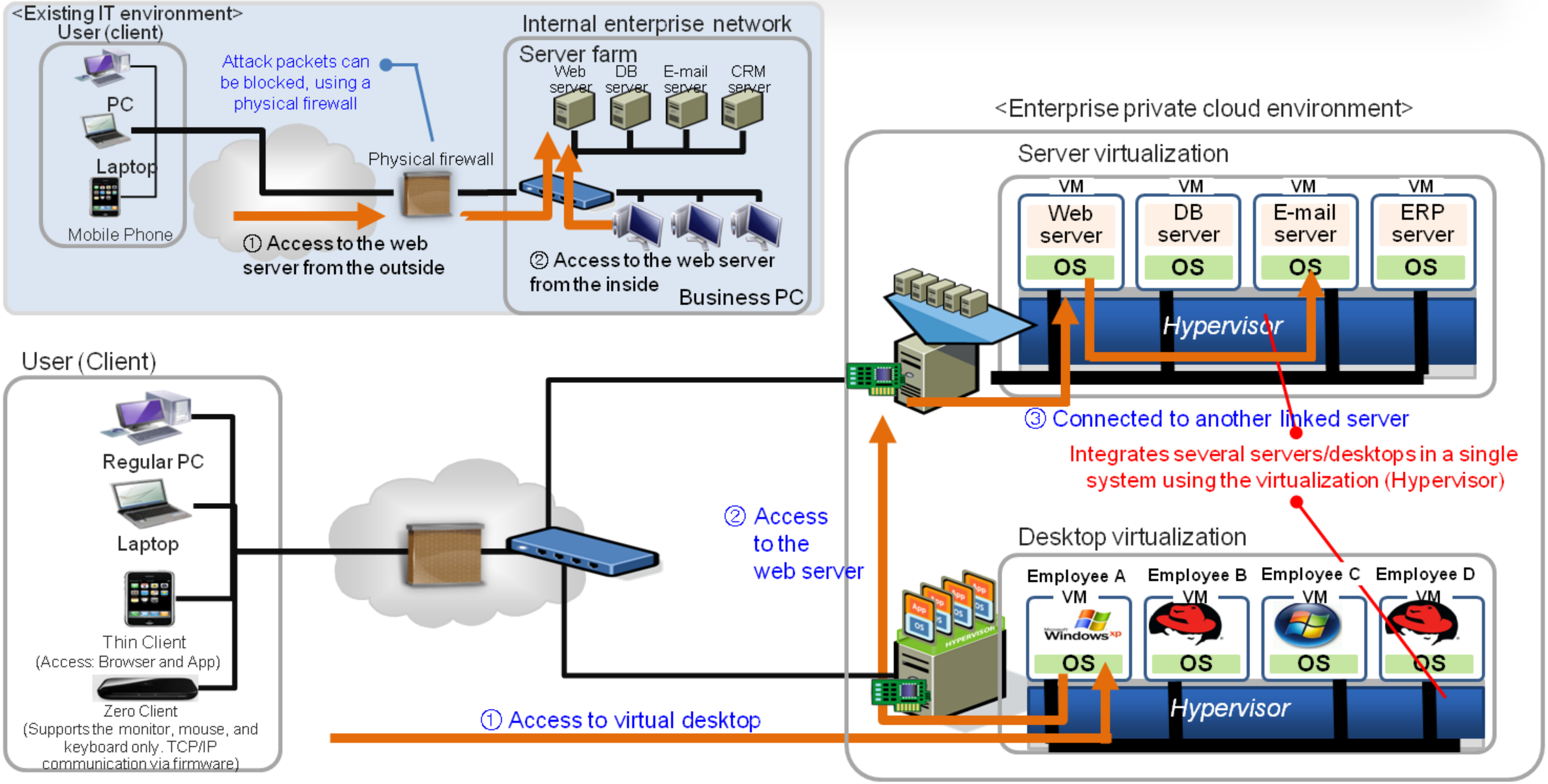
- **Safer!**
  - Services are safer because they are under the professional security management and control of the cloud service provider.
  - The service provider provides the security control service , using security equipment like firewall, IDS, and DDoS prevention devices.
  - Complete maintenance and control by professionals.

- **More vulnerable!**
  - Security threats due to the characteristics of cloud computing, such as resource sharing and virtualization.
  - The current security level is insufficient, and security should be strengthened.
  - Poor maintenance, malicious passenger, and crew mistakes.

VS.

II-2. Security Threats to Cloud Services (1) - Vulnerability of the Virtualization Infrastructure

There are security threats in the internal area of virtualization that cannot be protected by physical security equipment, as the existing IT environment is changing into the virtualization-based cloud environment.



Attack packets can be blocked, using a physical firewall

① Access to the web server from the outside

② Access to the web server from the inside

③ Connected to another linked server

Integrates several servers/desktops in a single system using the virtualization (Hypervisor)

② Access to the web server

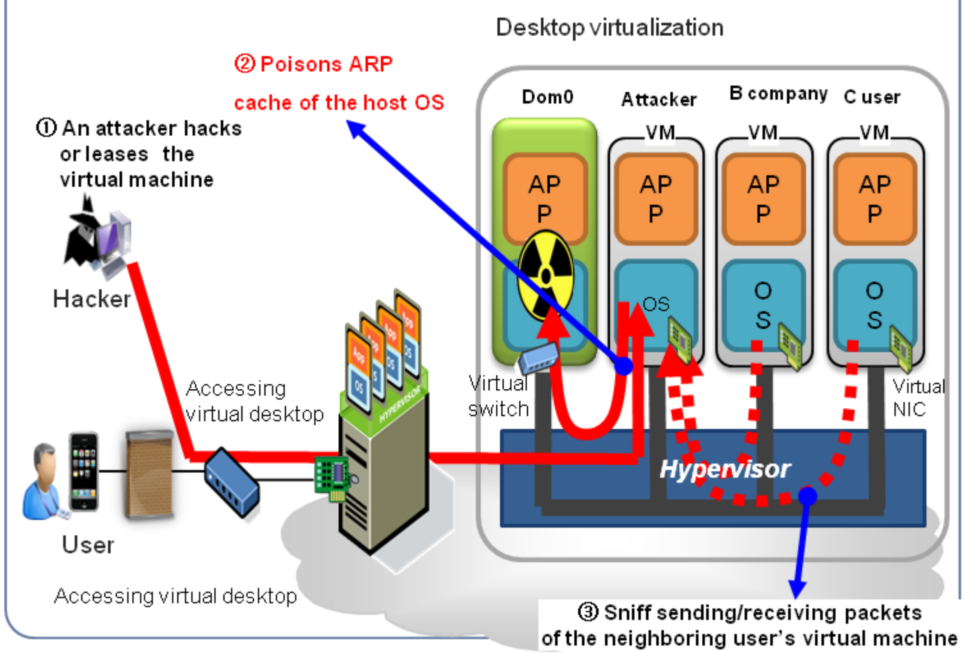
① Access to virtual desktop

II-2. Security Threats to Cloud Services(1) - Vulnerability of the Virtualization Infrastructure

Attack paths can be diverse, as the user's virtual machines are interconnected, using virtualization technology

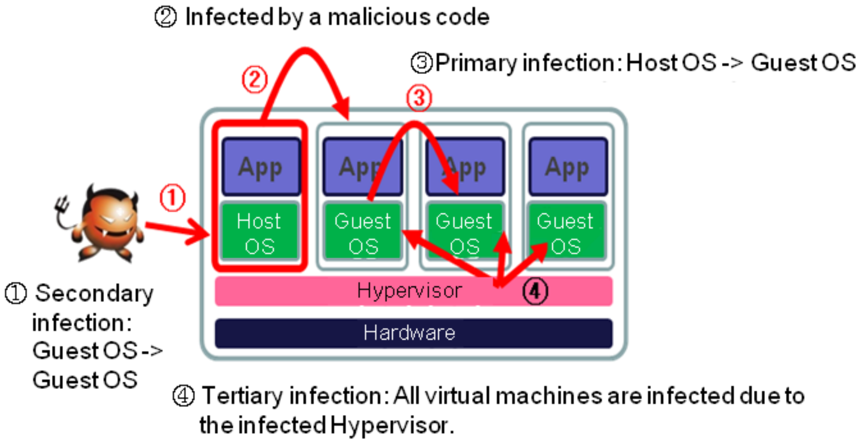
(Easy to hack, launch a DDoS attack, or spread malicious codes)

Packet sniffing via the virtual network


Desktop virtualization
② Poisons ARP cache of the host OS
① An attacker hacks or leases the virtual machine
Hacker
Dom0
Attacker VM
B company VM
C user VM
AP P
AP P
AP P
AP P
OS
O S
O S
Virtual switch
Virtual NIC
Hypervisor
Accessing virtual desktop
User
Accessing virtual desktop
③ Sniff sending/receiving packets of the neighboring user's virtual machine

Hacking among virtual machines

- When a Hypervisor machine is hacked, control over the entire virtual machine will be lost.
- If a particular virtual machine is infected by a malicious code, it can spread to the inside of the virtual environment.
  ※ All virtual machines establish communication via Hypervisor.


② Infected by a malicious code
③Primary infection: Host OS -> Guest OS
②
③
①
App
App
App
App
Host OS
Guest OS
Guest OS
Guest OS
Hypervisor
④
Hardware
① Secondary infection: Guest OS -> Guest OS
④ Tertiary infection: All virtual machines are infected due to the infected Hypervisor.

II-3. Security Threats to Cloud Services(2) – Information access by the unauthorized user due to resource sharing

A large amount of customer information is concentrated in the data center, and unauthorized users can access the information due to a configuration error or weak password. It is difficult to understand in which cloud server the user information is stored, backed up, and accessed, and who is accessing the information.

- **Risk of information access by unauthorized customers**

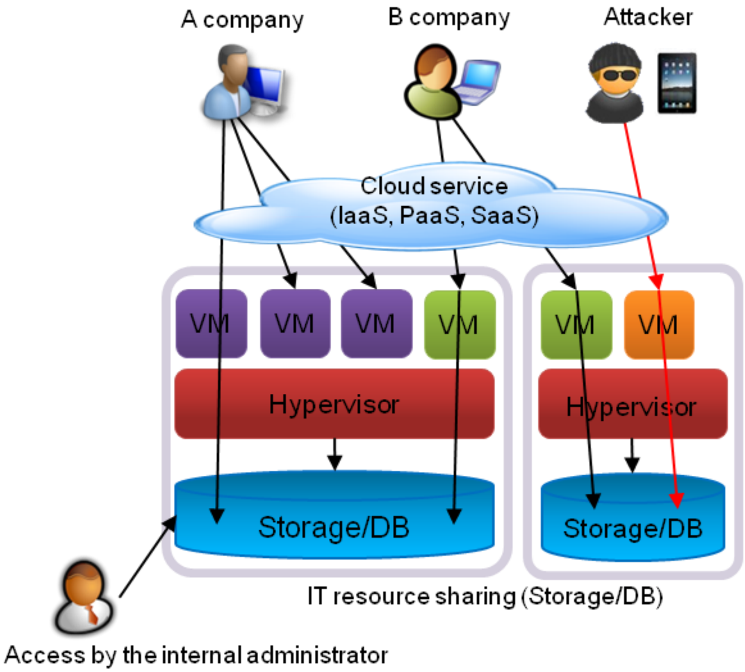
  ※ As a large amount of customer information is concentrated, and other customer's information is mixed in the data center, unauthorized persons can access the information due to a configuration error or weak password.
  (Example: Enterprise information was disclosed due to an MS BPOS configuration error.)

- **Information leakage caused by mobile device loss, theft, or account theft**

  ※ Various mobile devices are used to access the cloud server, such as smart-phones.

- **Customer information damage, misuse, and leakage caused by the insider**

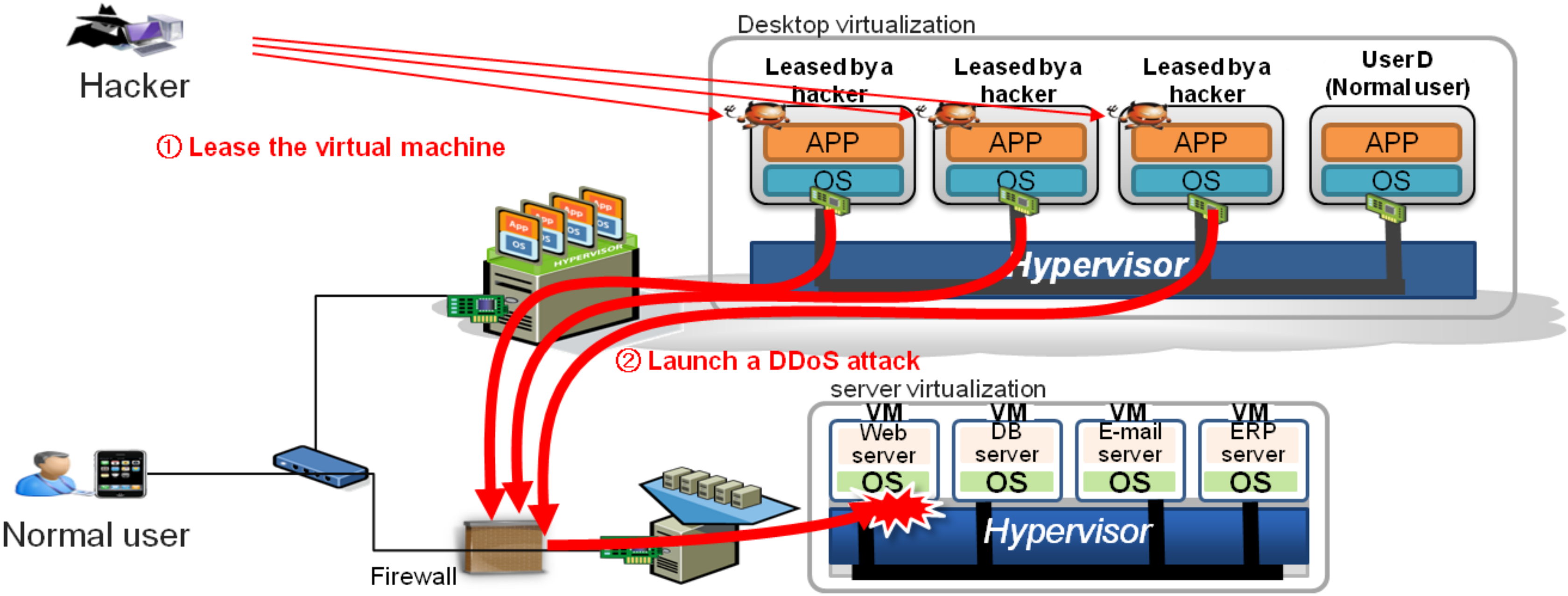
  ※ Customers cannot recognize the threat, if an insider performs poor management or tries to damage or disclose information intentionally.



II-4. Security Threats to Cloud Services(3) – Large scale damages due to information concentration.

Customer information concentrated in cloud servers → Exploited as a target of hacking and DDoS attack, or as a transit point. If an infringement incident occurs, all user services can be stopped consecutively and large-scale damages can be caused.

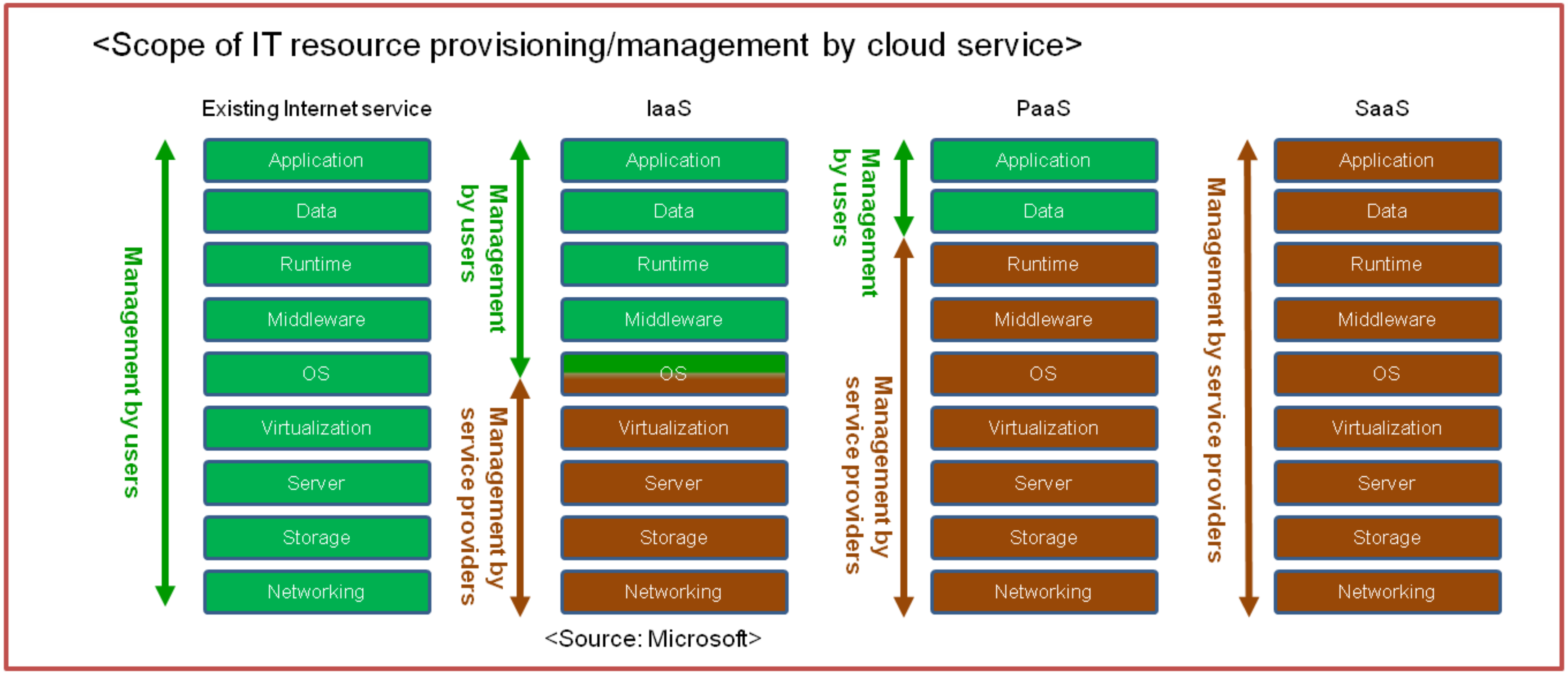
- 190 services were paralyzed simultaneously due to an 11-hour system error at Amazon (April 2011)
- If the service fails, customers cannot identify the reason quickly.
  - ※ Service provider dependent service structure (Services cannot be used until the service provider restores or applies the patches.)
  - ※ If the cloud server is paralyzed, damages can grow, such as service interruption time and scope.
- The service can be exploited as a target of cyber attacks such as DDoS attacks, or attack transit point.



II-5. Security Threats to Cloud Services(4) - Unclear responsibilities and complex policies

□ It is difficult to assign the responsibility for security, as the subject of IT resource management differs, depending on the service model.

□ It is impossible to clarify where the responsibility lies, as service access environments and terminals are diverse, and complex security policies should be applied.



<Scope of IT resource provisioning/management by cloud service>

Existing Internet service	IaaS	PaaS	SaaS
🟩 Application	🟩 Application	🟩 Application	🟫 Application
🟩 Data	🟩 Data	🟩 Data	🟫 Data
🟩 Runtime	🟩 Runtime	🟫 Runtime	🟫 Runtime
🟩 Middleware	🟩 Middleware	🟫 Middleware	🟫 Middleware
🟩 OS	🟩🟫 OS	🟫 OS	🟫 OS
🟩 Virtualization	🟫 Virtualization	🟫 Virtualization	🟫 Virtualization
🟩 Server	🟫 Server	🟫 Server	🟫 Server
🟩 Storage	🟫 Storage	🟫 Storage	🟫 Storage
🟩 Networking	🟫 Networking	🟫 Networking	🟫 Networking

Management by users
Management by users
Management by service providers
Management by users
Management by service providers
Management by service providers

<Source: Microsoft>

II-6. Cases of Cloud Service Incidents

Q. What have been the causes of known cloud service incidents up to now?

A. Incidents occurred due to the carelessness of the administrator, natural disasters, and program errors.

Case	Date	Type	Content
Google	SEP. 2009	Service failure	Gmail service failed for 2 hours continuously.
	FEB. 2011	Data loss	500,000 users' e-mails and address books were deleted.
MS	SEP. 2010	Service failure	Smart-phone service "Sidekick" stopped.
	OCT. 2012	Data leak	Enterprise information was disclosed to others due to a service environment setting error.
eBay	SEP. 2008	Service failure	Service failed for 2 hours due to a Paypal payment system error.
Amazon	AUG. 2011	Service failure	Amazon EC2 failed due to an electrical outage caused by lightning strikes (thousands of companies in European countries could not access the service for 2 days).

III-2. Development Prospects for Cloud Security Technology

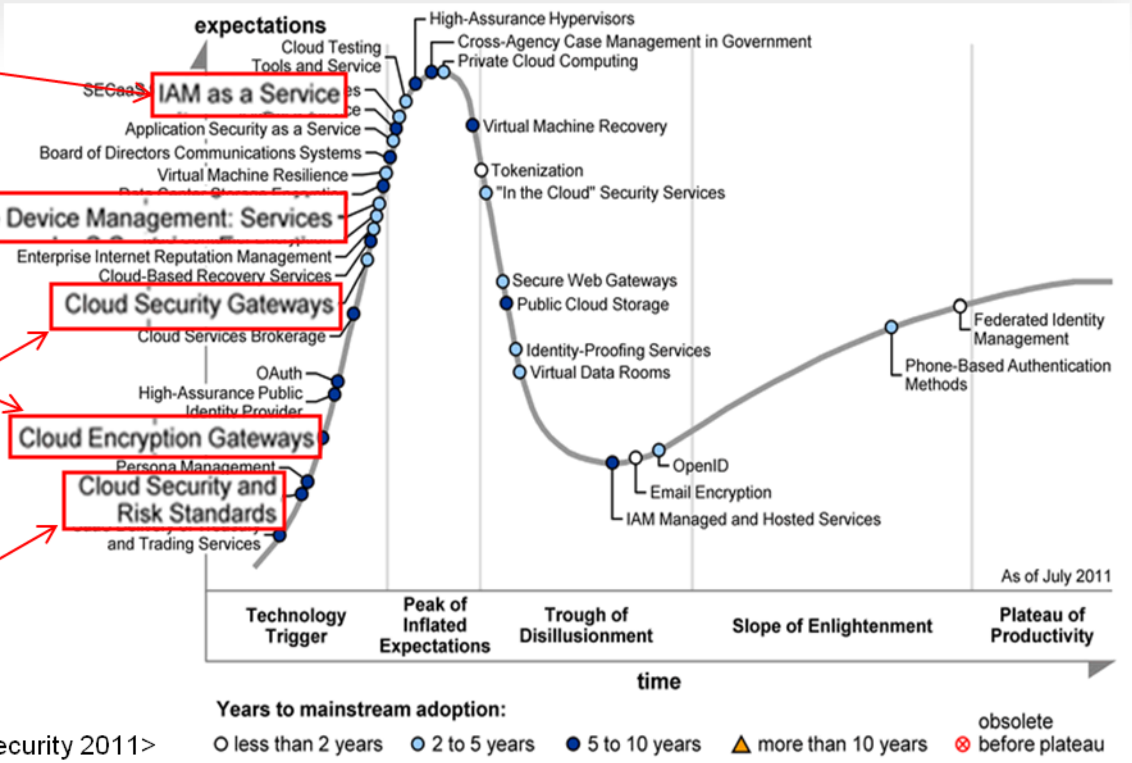
- **Application of existing technologies → Security technologies exclusive for cloud services (For the Cloud)**
  - ❖ Cloud dedicated security technologies such as Hypervisor security technology and cloud encryption technology have emerged..
- **Provides security technologies in the cloud environment (In the Cloud)**
  - ❖ The existing security system itself becomes the cloud service, such as IAM (Identity & Access Management).

Existing security system itself becomes the cloud service

Management technology for Mobile devices

Appearance of dedicated cloud security technology

Movement to standardize cloud security features

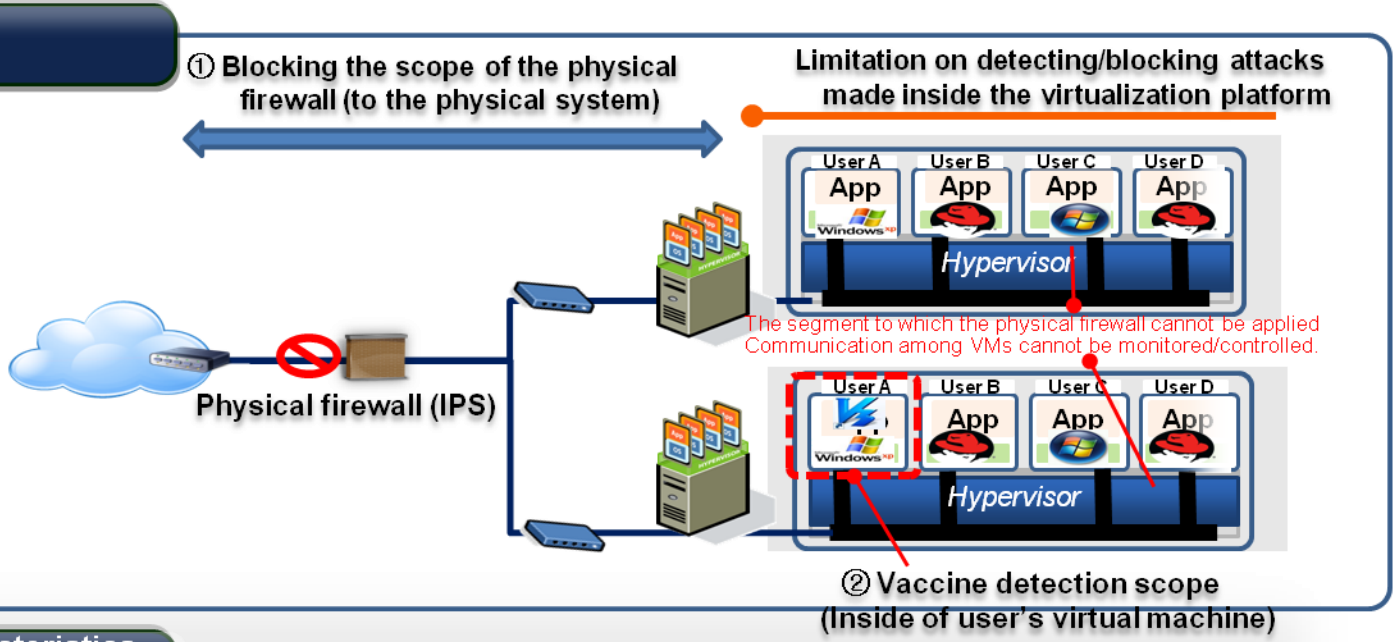


<Source: Gartner, Hype Cycle for Cloud Security 2011>

III-3. Cloud Security Technology – Virtualization intrusion detection/blocking

Limitations of existing network security equipment

Focusing on the outside-inside boundary


① Blocking the scope of the physical firewall (to the physical system)

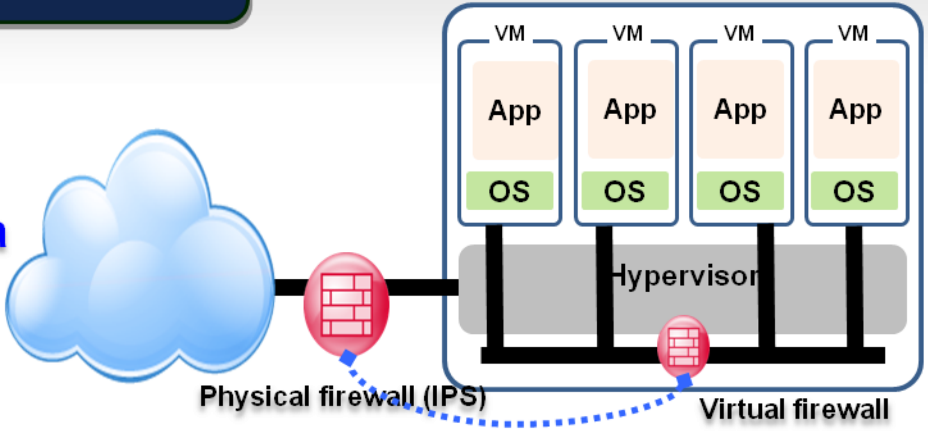
Limitation on detecting/blocking attacks made inside the virtualization platform

The segment to which the physical firewall cannot be applied
Communication among VMs cannot be monitored/controlled.

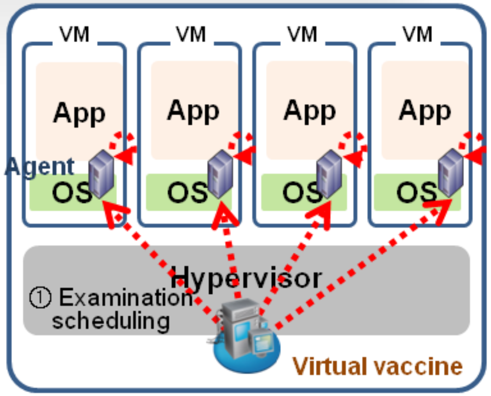
② Vaccine detection scope
(Inside of user's virtual machine)

Security considering the characteristics of cloud services

Security of the virtualization area inside the cloud service



Virtual firewall
(Detecting/Blocking attack traffic via the channel among VMs.)

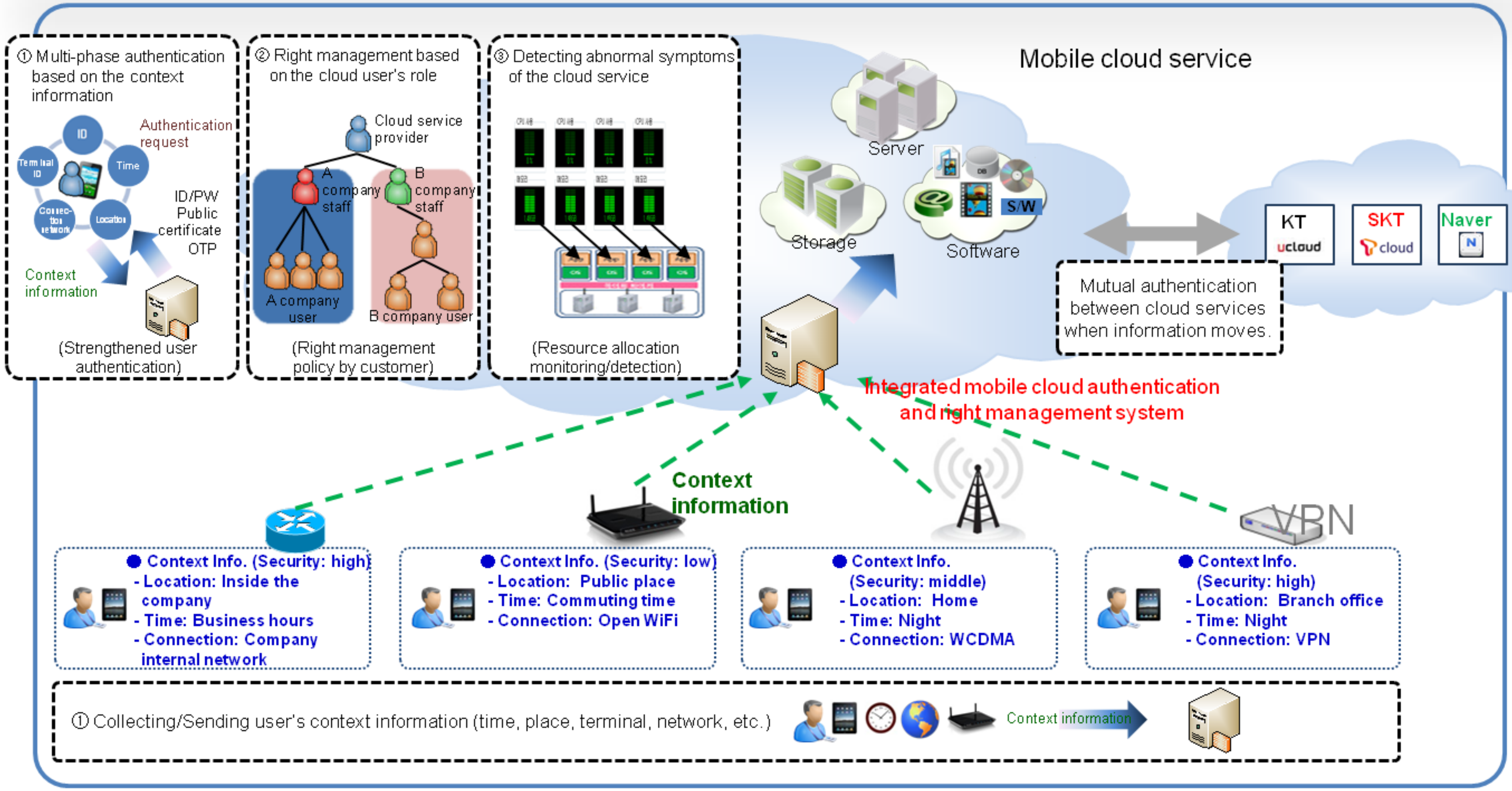


② Virus/Malicious detection by virtual host

Virtualization system vaccine

III-4. Cloud Security Technology – Mobile cloud authentication/right management technology

- Collecting information on the user's access, such as connection time and location (home, office, etc.), using a mobile device.
- Providing different authentication and the right management, depending on the access context information -> Technology that analyzes abnormal symptoms in accessing cloud resources.



① Multi-phase authentication based on the context information

(Strengthened user authentication)

② Right management based on the cloud user's role

(Right management policy by customer)

③ Detecting abnormal symptoms of the cloud service

(Resource allocation monitoring/detection)

Mutual authentication between cloud services when information moves.

Integrated mobile cloud authentication and right management system

- Context Info. (Security: high)
  - Location: Inside the company
  - Time: Business hours
  - Connection: Company internal network
- Context Info. (Security: low)
  - Location: Public place
  - Time: Commuting time
  - Connection: Open WiFi
- Context Info. (Security: middle)
  - Location: Home
  - Time: Night
  - Connection: WCDMA
- Context Info. (Security: high)
  - Location: Branch office
  - Time: Night
  - Connection: VPN

① Collecting/Sending user's context information (time, place, terminal, network, etc.)

IV. Conclusion

- "Security" must be considered first when introducing the cloud service.
- Stronger security is required, as the information of many customers is concentrated in the same data center.
- Safer services can be provided through professional security management.
- However, existing security + ∝ security is required, considering the characteristics of the cloud service such as resource sharing and virtualization.