情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Something missing in Cloud certification

A study on Third-party certification for cloud services

YONOSUKE HARADA

Professor, Graduate School of Information Security
INSTITUTE of INFORMATION SECURITY

Content

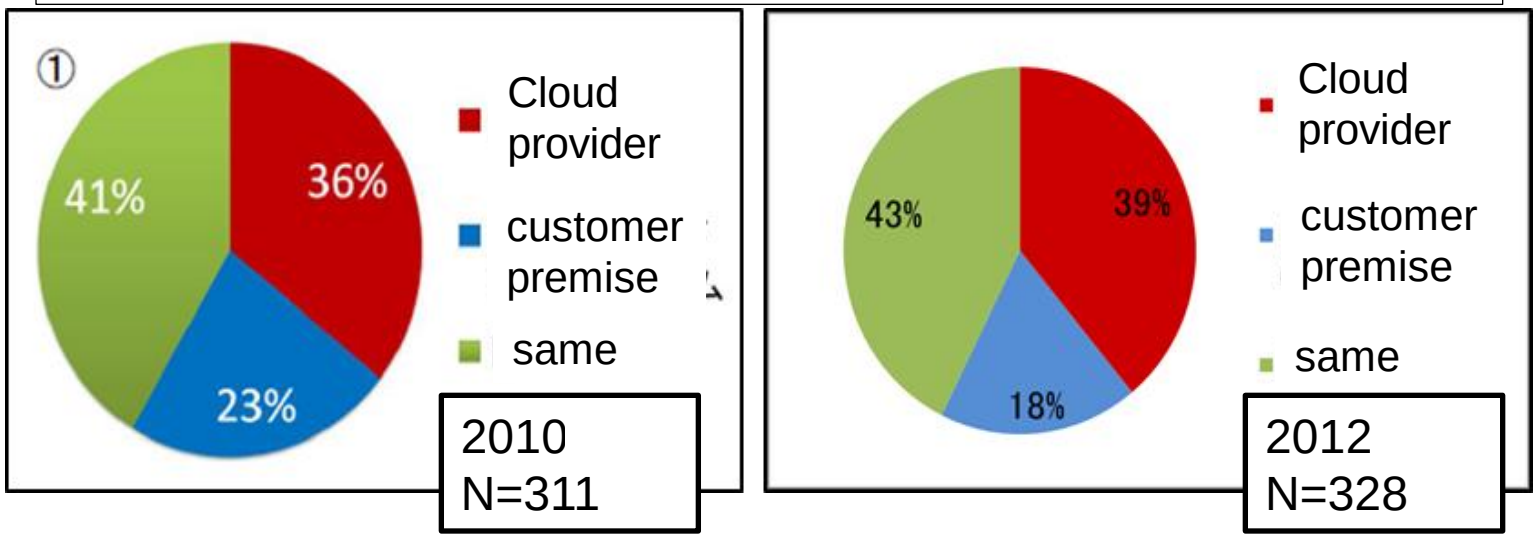
- Certification for cloud services are commonly used
  - Lessons learned from “First Server” incident
- Chain of trust for cloud services
  - customer organization needs trust from provider
  - accountability
- Proposal of new model to explain the gap between customer and cloud provider

Company-Customer perception

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Many of company customer feel bigger risk exists on cloud provider IT environment

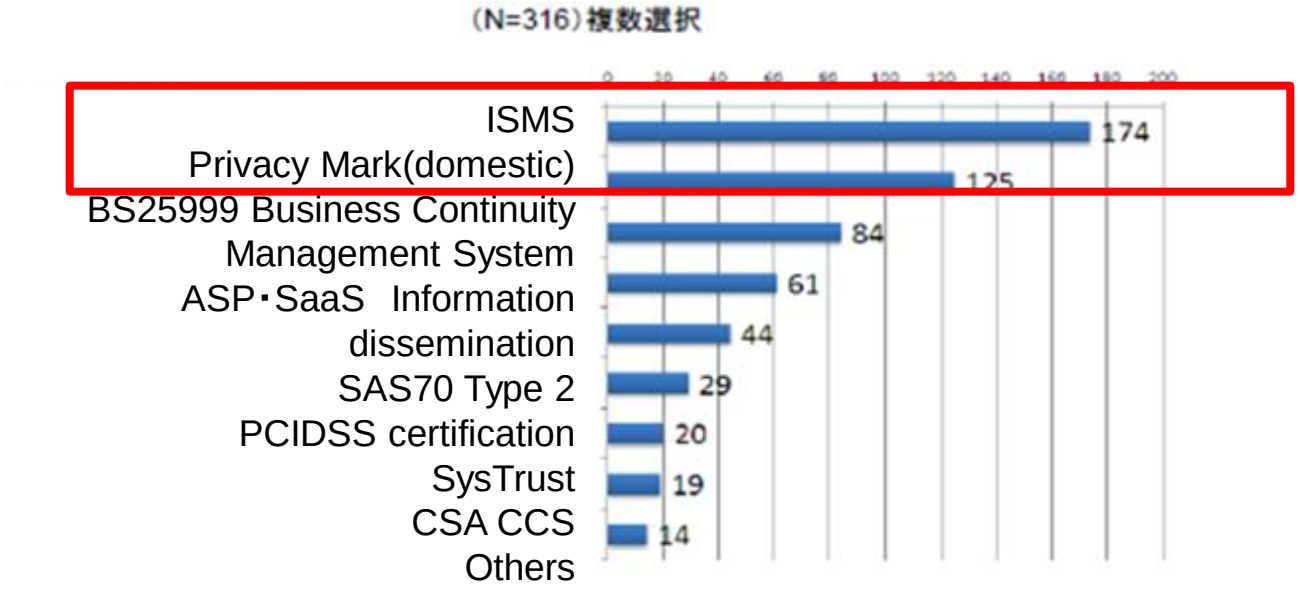
Comparison of risk perception of IT environment between customer premise or cloud provider



Survey result by Harada Lab. of Institute of Information Security in 2010 and 2012

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Many of Japanese customers(companies) use of ISMS and Privacy Mark certification when they procure IT services from third party



Certification is necessary for cloud provider selection

Survey result by Harada Lab. of Institute of Information Security in 2010

2. First Server Incident

- Loss of data (accidental deletion of entire customer data)

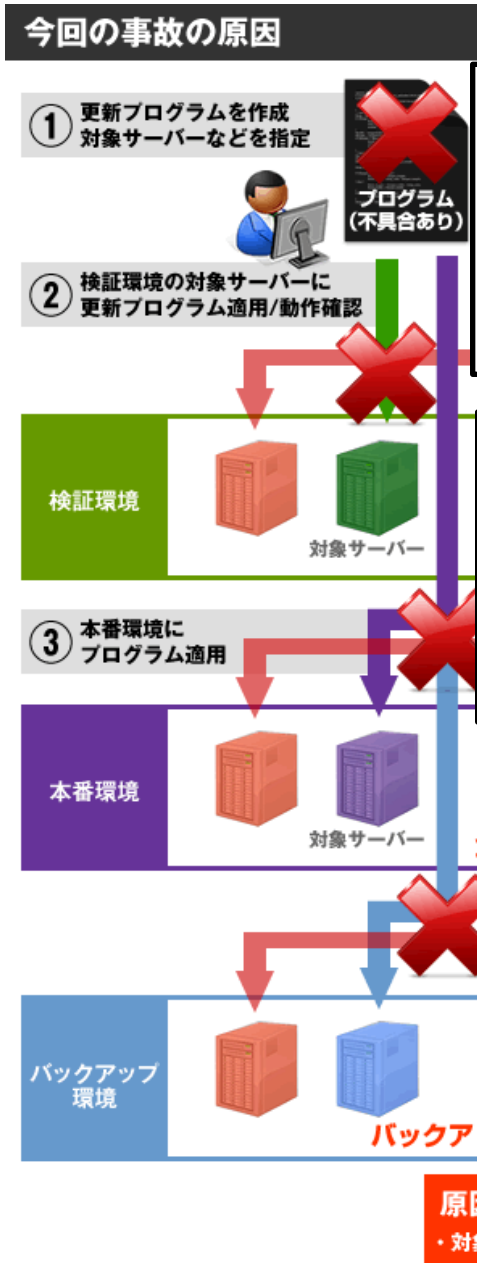
- Leakage of data (unintended data salvage)

Incident

- **Company**
  - **First server :** Rental server company (cloud provider)
- **Date**
  - 20th June, 2012 PM 1730-
- **Loss of data (servers)**
  - Entire data of User area
    - ◆Web and Mail server data
    - ◆database
  - Setting parameters
- **Affected number of business customers**
  - 5676 (about 20% of customers) companies and users
- **Major cause**
  - Human error and lack of management (manager’s supervisory)

Detail of Incident

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



Program update for vulnerability

Prepare automated macro command to update programs which utilizes file deletion after update completion of maintenance. (missing of macro command)

Lack of standard procedures for operation

Operators did not follow Prepare automated macro command to update programs which utilizes file deletion after update completion of No. (missing of macro command)

Loss of Back-up system and management

The system has designed to get back-up automatically at 6:00 AM. Operator first applied defect macro to production system and applied automatically to back-up systems and lost entire data.

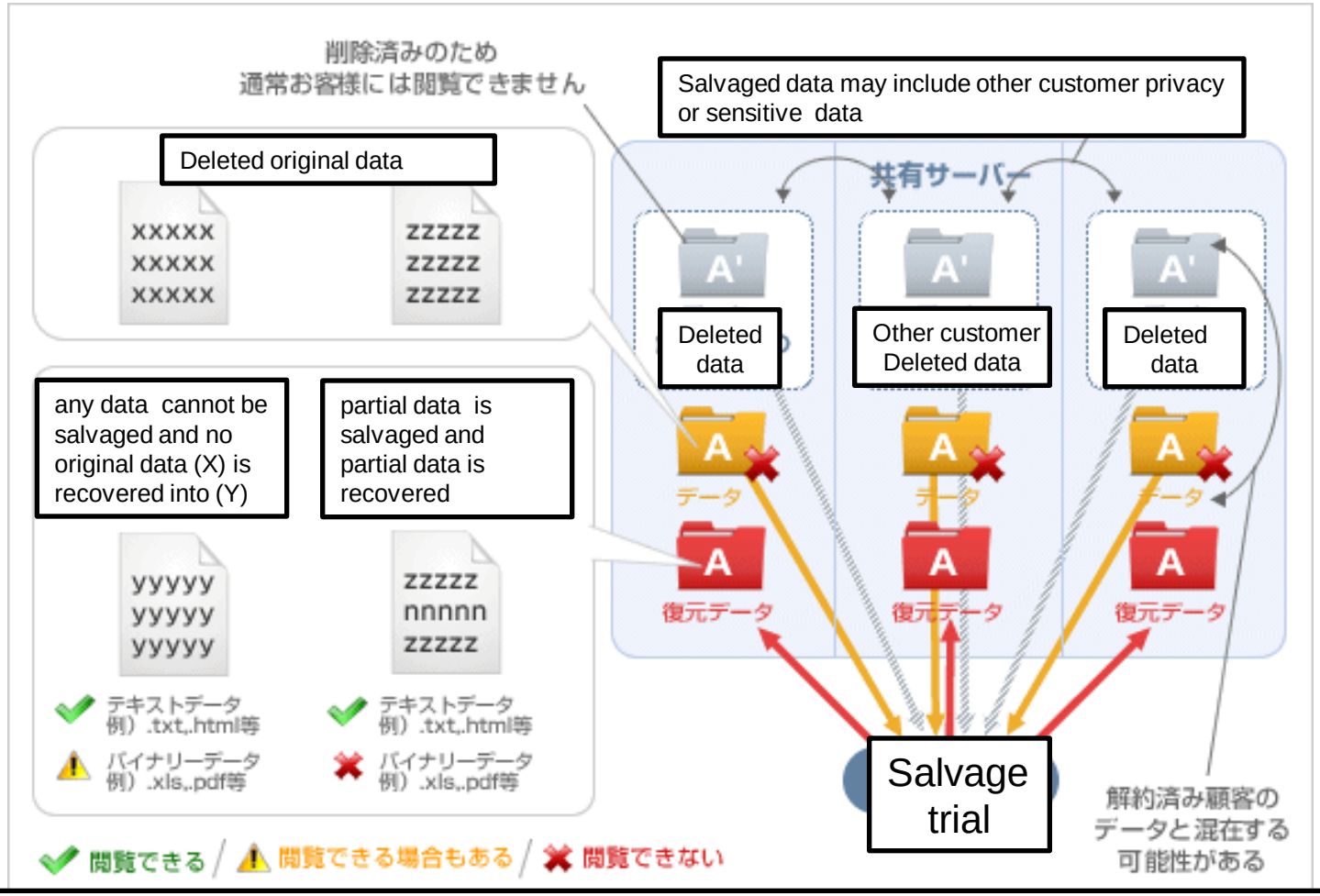
http://support2.fsv.jp/urgent/report.html

Detail of Incident

- **Operator has not followed the operation manual and supervisor knew his activity because of effectiveness**
- **Operator applied his previous automated updating commands without checking**
  - Operator usually automates procedures applying patches and deleting unnecessary files and directory. He utilized previous macro command he developed. He had not noticed the mistake to delete entire all directory.
- **Lack of testing procedure after update**
  - The operation manual mandates first test patches in a test server and evaluate. He did not check after patch application. He continued applying his program to the production servers.

Second incident

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



Recovery from deleted files cause mess. All recovered User files are accessible from all users

Third party assessment
Lack of Governance

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- **Ignorance of standard operation in the manual**
- **No management oversight and conduct**
  - Lose communication between management and operators
  - Operator did not wait for management approval for critical operation
  - Operator did not report to the management after the outage
- **No incident manual for data deletion and other problems**
  - Operators are confident enough having no major problems since business start. They think themselves confident enough tackle without any written manual.
- No education for critical operation and risk avoidance
  - Operator did not follow operation manual
  - Operator has no knowledge recovery of data and tried to recover by utilizing free salvage software to recover
  - Operator did not understand future “risk” with salvage activity

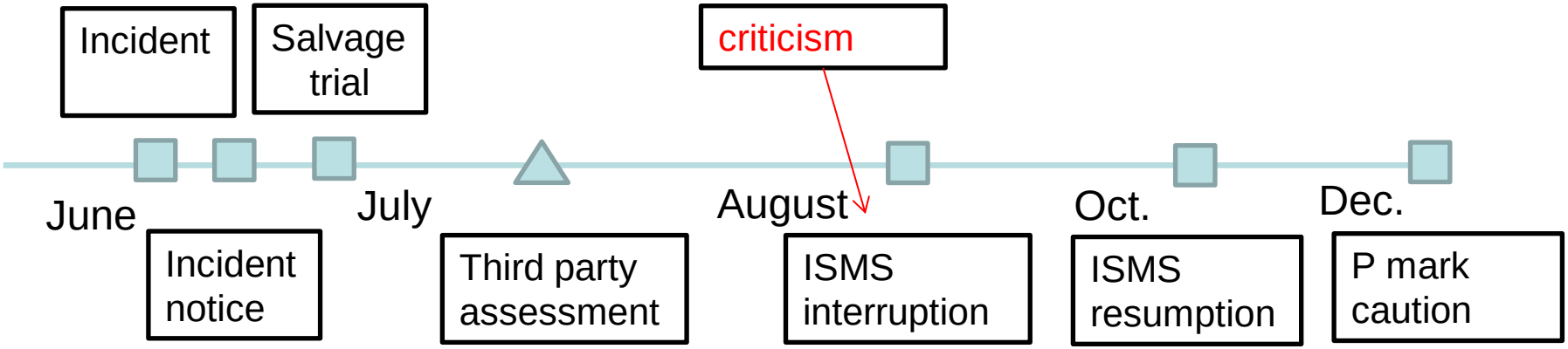
Discrepancy of certification and reality

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- First Server acquired certifications ISMS and Privacy Mark
  - Discrepancy between their daily conducts and ISMS requirement
- Certifications are used for users' "trust" and good appearance
  - Customers believe their data is protected as private information
  - Identified private information is about company staffs

Time Line of incident

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



Poor sanction for certification

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- First Server was banned ISMS certification from August to October
  - Sanction looks weak against incident
- First Server was not banned Privacy Mark because of small amount of leakage
  - Identified private information is company staff which are protected
  - Service does not include back-up (contract)

Use of Certification for marketing

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- “certification” is good tool for sales and advertisement
  - ISMS
  - Privacy Mark (domestic privacy and private information protection certification)
- Customer trust on “certification”
  - Good explanation of provider selection
  - Accountability to their end-users (chain of trust relations)

Lessons learned from incident

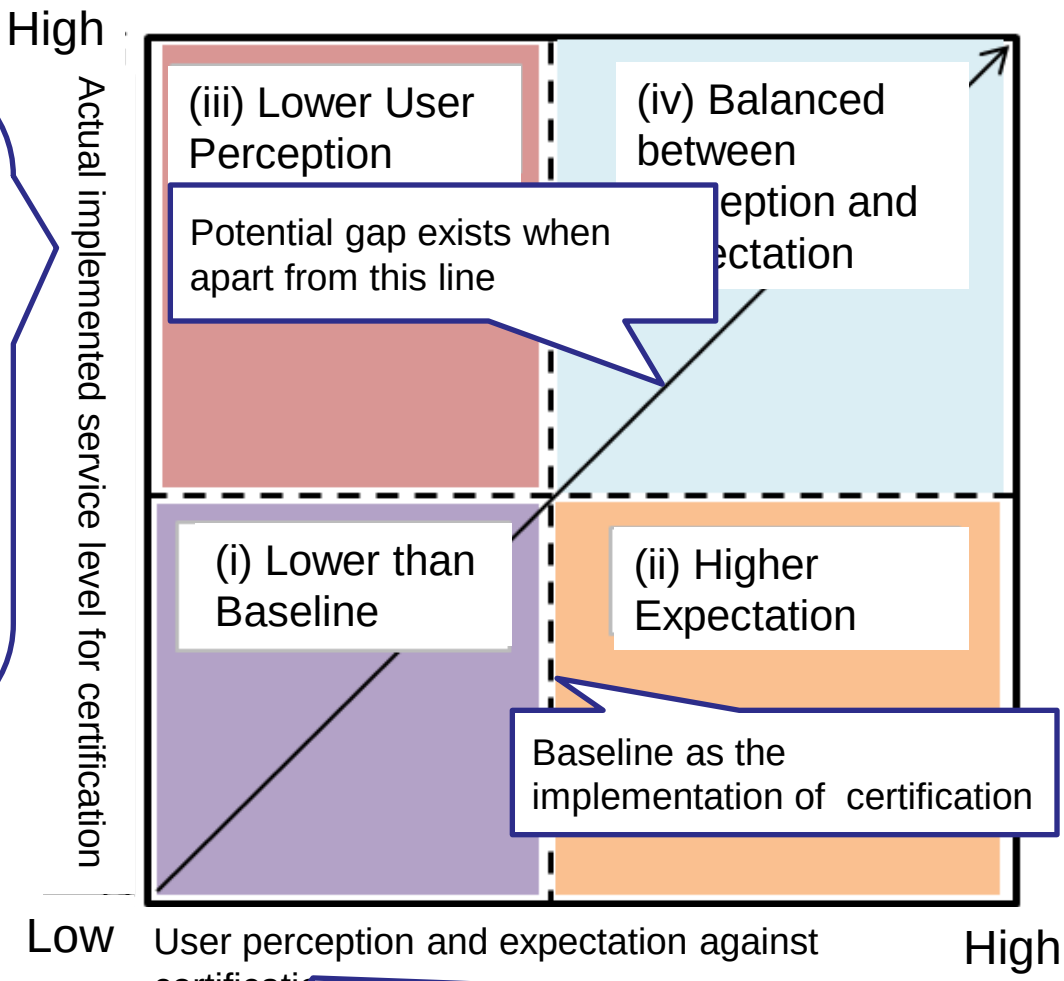
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- Importance of understanding “certification”
  - Provider has certified its implementation of ISMS as entire business
  - Customer understand ISMS certification as the protection of date from various risks
- “certification” does not mean “trustworthy” service
  - Provider use “certification” for marketing
  - Customer use “certification” for trust

Gap model : information asymmetry

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- Understanding of requirement for certification system
- Perception and Penetration
- Clearness of definition
- Accountability
- Customer responsibility
- …etc

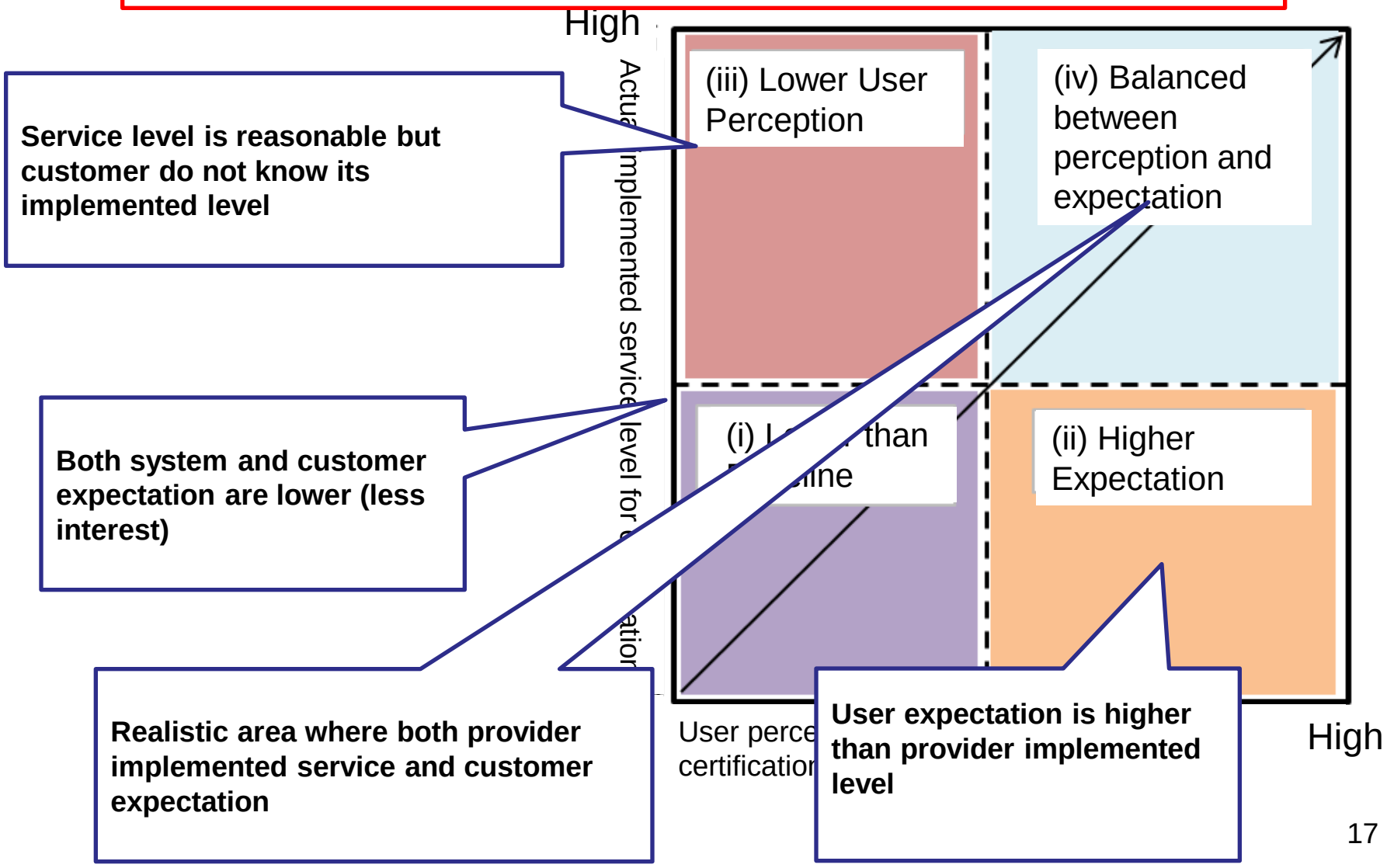


How certification system is used to fulfill user expectation and accountability?

Gap model

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Four areas for consideration



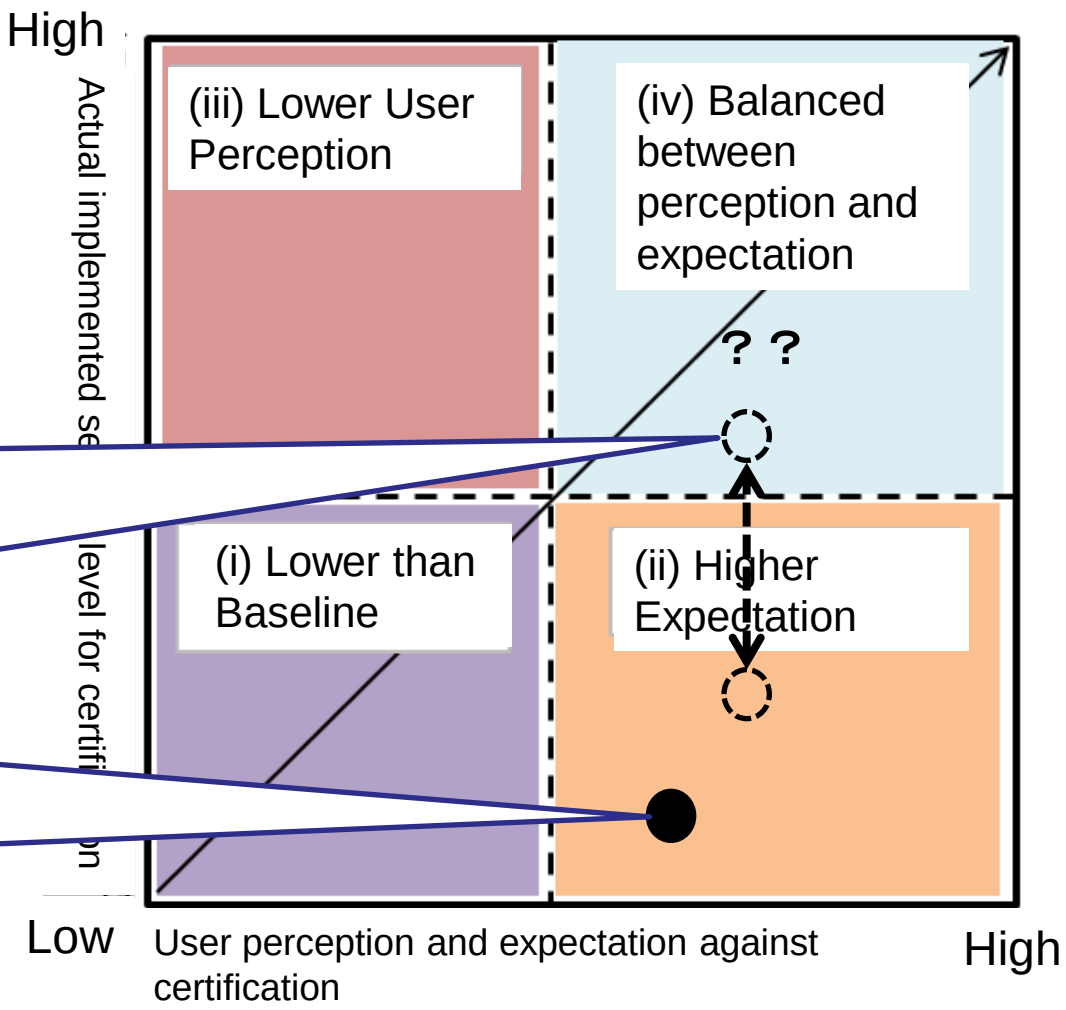
Gap model

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Higher Expectation should be adjusted

・ISMS
SOA(statement of Applicability) should be exposed to customers
⇒Implemented ISMS management and controls to reduce risk should be disseminated

・Privacy Mark
Definition should be matched between provider and customers



Gap model

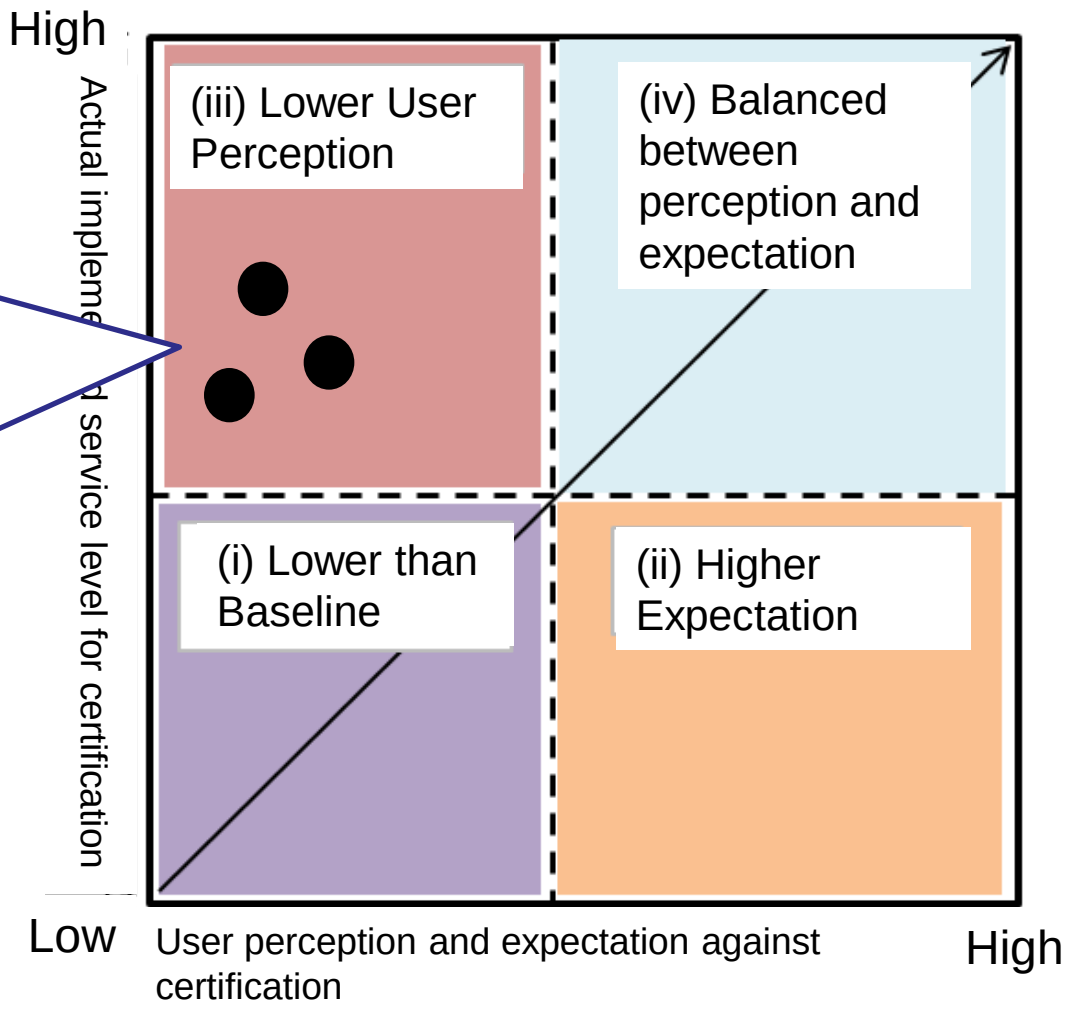
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- Provider incentive is small because of its cost does not match with investment

⇒potential incentives should be prepared by authorities

⇒reduce a cot of “certification”

Example: PCIDSS



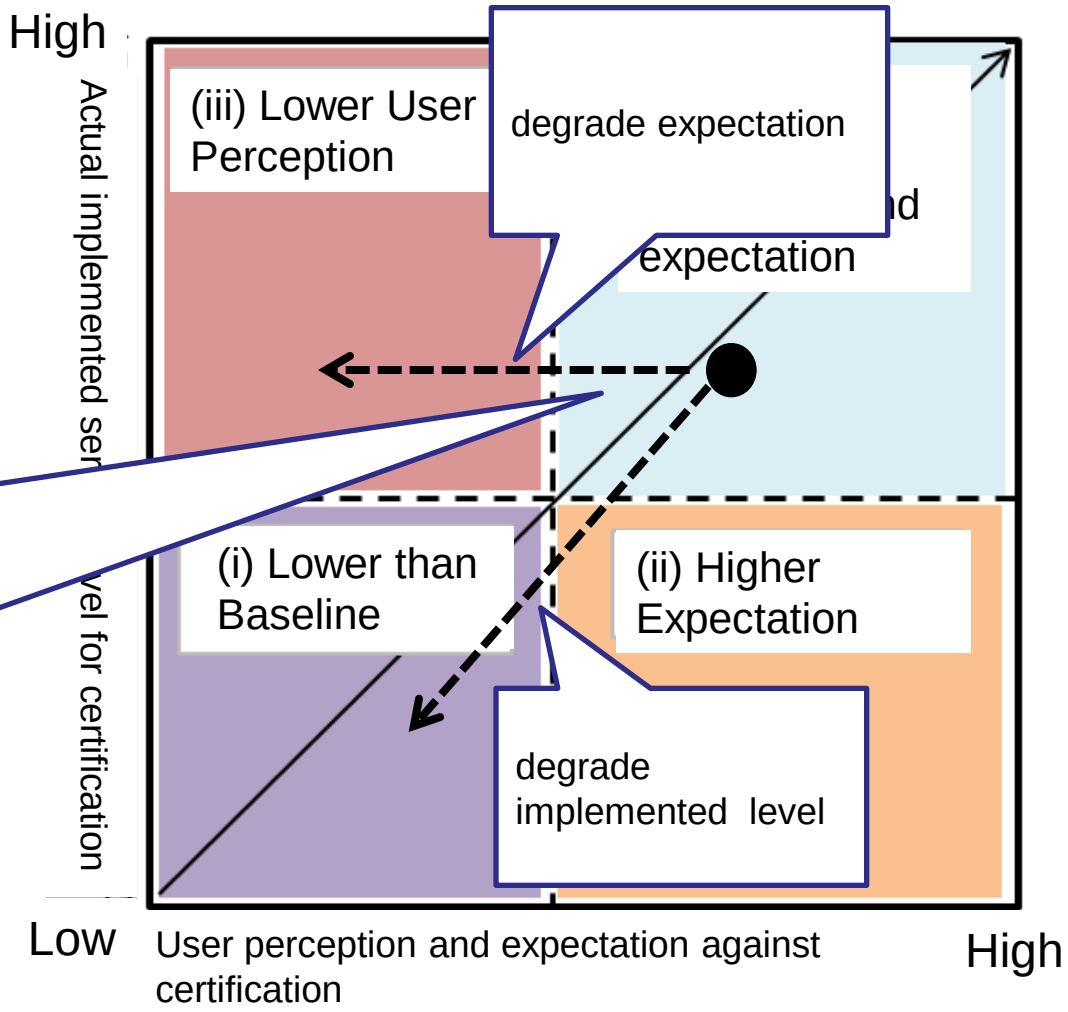
Gap model

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Potential Risk for Certification

No cloud specific certification

(iv) looks best positioning but may sift to (ii) or (iii) according to the lower investment by provider and the higher expectation / perception change



6 Conclusion

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- Current ISMS and Privacy Mark has revealed that information asymmetry between provider and customer.
  - Missing peace exists between customer expectation/perception and provider implementation/investment
- The trend is apparent for cloud service.
  - The certification should be neutral between user excessive expectation and provider lower implementation.
  - Current certification is not enough to fill the gap for cloud services
- New model should be designed for accessing gap between customer and provider implementation.
- The third party organization may balance user expectation and provider implementation.

Thanks
for more information

yo-harada@iisec.ac.jp