National Institute of Advanced Industrial Science and Technology
AIST

RISEC
Research Institute for Secure Systems

Security on cloud storage and IaaS

at Taiwan-Japan Workshop 2012/Nov/27
http://www.jst.go.jp/sicp/ws2012_nsc.html

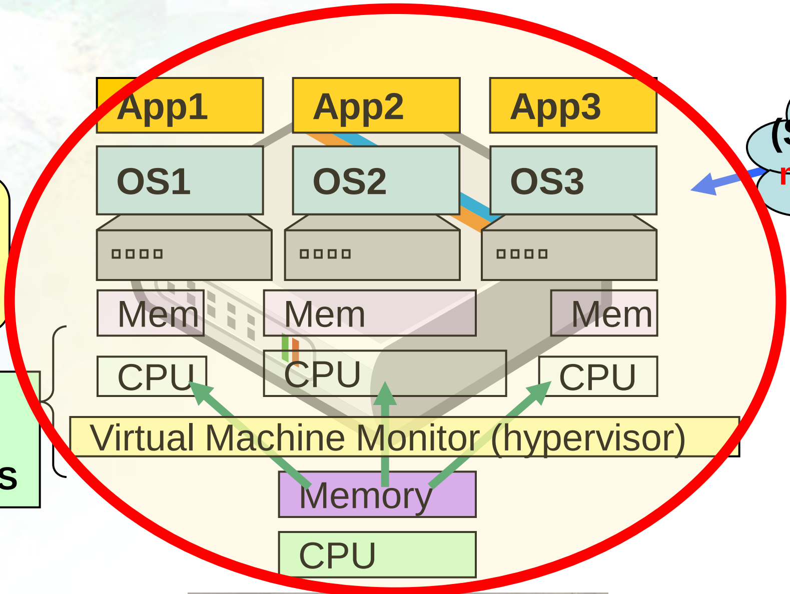
Kuniyasu Suzaki

Research Institute for Secure Systems (RISEC)
National Institute of Advanced Industrial Science and Technology (AIST)

National Institute of Advanced Industrial Science and Technology
AIST

Overview of Security on IaaS Cloud Computing

RISEC
Research Institute for Secure Systems



Internet
(Secure communication)
man in the middle attack

Formal Verification
To take high level EAL (Evaluation Assurance Level)

Software Vulnerability
- Hypervisor
- Management Host OS

Client User
- ID, Password, Secret Key management
- Software vulnerability Security update

Vulnerable (un-mature) safe

Security Guideline
- CSA (Cloud Security Alliance)
- Open Cloud Manifesto

Auditing Standard
- SAS70
- HIPAA

Data Management
- Information Leak
- Information Loss
- Information Erasure

Auditing
- Digital Forensic
- Log

My interests

- Sharing technologies (virtualization technologies) on IaaS are good for security?
  - Based on my papers [HotSec10], [EuroSec11], [EuroSec12]

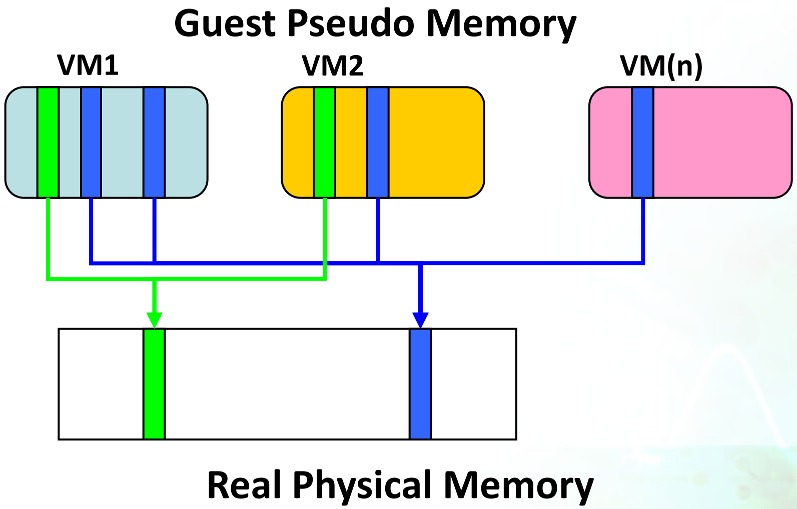
- Information leak / erase / loss on cloud storage
  - Funded by Strategic Information and Communications R&D Promotion Programme(SCOPE), Ministry of Internal Affairs and Communications (MIC).

Sharing Technology

- Sharing is a key technology on Cloud computing, because it can reduce costs. It offers pseudo physical devices and shares same parts of devices.
  - Virtual Machine
    - VMware, Xen, KVM, etc.
  - Storage deduplication
    - Dropbox, EMC products, etc.
  - Memory deduplication

Memory Deduplication

- Memory deduplication is a technique to share same contents page.
  - Mainly used for virtual machines.
  - Very effective when same guest OS runs on many virtual machines.
- Most memory deduplication are included in virtual machine monitors with different implementations.
  - VMware, Xen, and KVM have own memory deduplication



Is Memory Deduplication good or bad for security?

(1) Good

- From logical sharing to physical sharing [HotSec10]

(2) Bad

- Cross-VM Side Channel Attack [EuroSec11]
  - Cause Information leak

(3) Good or Bad

- Affects to current security functions (Address Space Layout Randomization, Memory Sanitization, Page Cache Flushing) [EuroSec11]

(1) Logical Sharing

- Current OSes use logical sharing technique to reduce consumption of memory.
  - “Dynamic-Link Shared Library”
- Unfortunately, it includes vulnerabilities caused by dynamic management.
  - Search Path Replacement Attack
  - GOT (Global Offset Table) overwrite attack
  - Dependency Hell
  - Etc.

(1) Solution, and further problem

- These vulnerabilities are solved by static-link in general, but it increase consumption of memory.
  - Fortunately, the increased consumption is mitigated by **memory deduplication** on IaaS.
  - It looks easy to solve the problem, but …
- Current applications assume dynamic-link and are not re-compiled as static-link easily.
  - Dynamic-link is used for avoiding license contamination problems. The programs includes “**dlopen()**” to call dynamic link explicitly.

(1) From Logical sharing to physical sharing

- Instead of static link, we proposed to use "*self-contained binary translator*" which integrates shared libraries into an ELF binary file. [HotSec'10]
  - The ELF binaries become fatter than static link, but the redundancy is shared by physical sharing (memory deduplication).

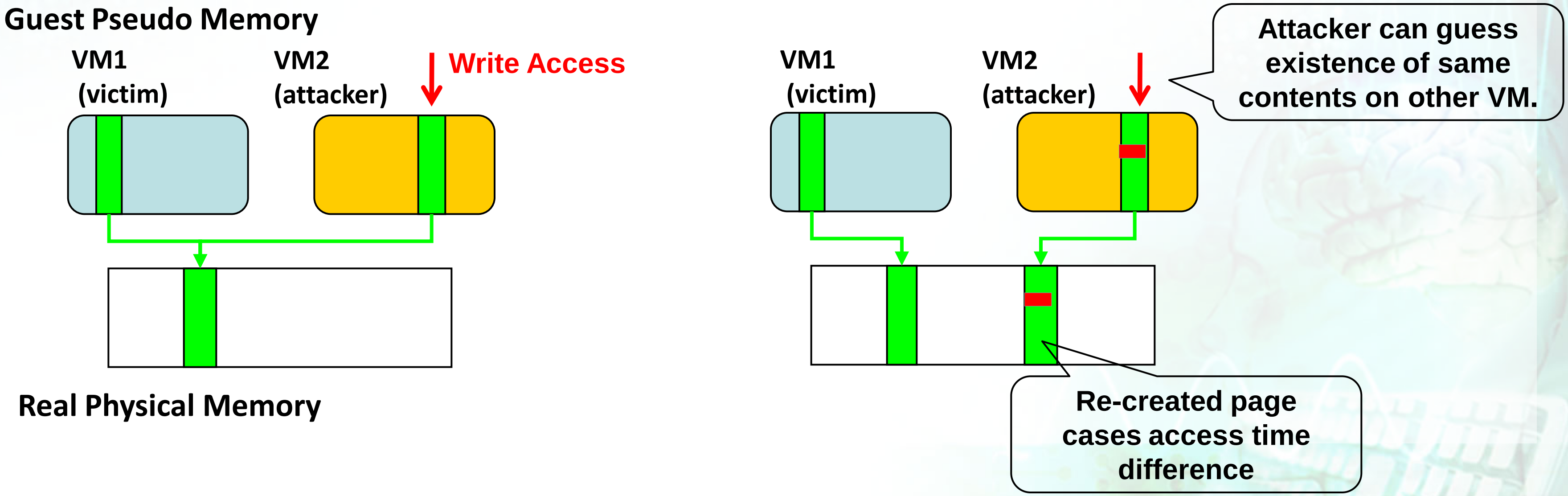
- OSes on a cloud can increase security.

(2) VM Side Channel Attack

- Memory deduplication is vulnerable for side channel attack.
  - The vulnerable is caused by Copy-On-Write of memory deduplication.
  - Copy-On-Write is a common technique to manage shared contents, but it became a Covert Channel for Information Leak.

(2) Copy-On-Write (COW)

- When a write access is issued to a deduplicated page, a same contents page is created and accepts write access. This action is logically valid, but …
- ***Write access time difference*** between deduplicated and non-deduplicated pages due to copying.



Attacker can guess existence of same contents on other VM.

Re-created page cases access time difference

(2) Attacking problem

- Cross VM side channel attack looks simple, but there are some problems.

  ① 4KB Alignment problem

  - Attacker must prepare exact same pages in order to guess victim’s contents.

  ② Self-reflection problem

  - Caused by redundant memory management on cache and heap. Attacker has a false-positive result.

  ③ Run time modification problem

  - Caused by swap-out, etc. Attacker has a false-negative result.

- The attacking methods and countermeasure are mentioned in [EuroSec11].

(3) Affects of OS Security functions on memory deduplication

- Modern OSes have security functions that modify memory contents dynamically.
  1. Address Space Layout Randomization (ASLR)
  2. Memory Sanitization
     - Pages are zero-cleared. Increase deduplication.
  3. Page Cache Flushing
     - Useful to remove redundant pages.
- These security functions are affected by memory deduplication.

(3) Affects on Security Functions

- ASLR looks to be independent of memory deduplication because the contents are not changed on memory. However it increased consumption of memory, because It made different page tables.
- Memory Sanitization and Page Cache Flushing increase zero-cleared pages and help memory deduplication. However, the costs are heavy and they decreased performance severely.

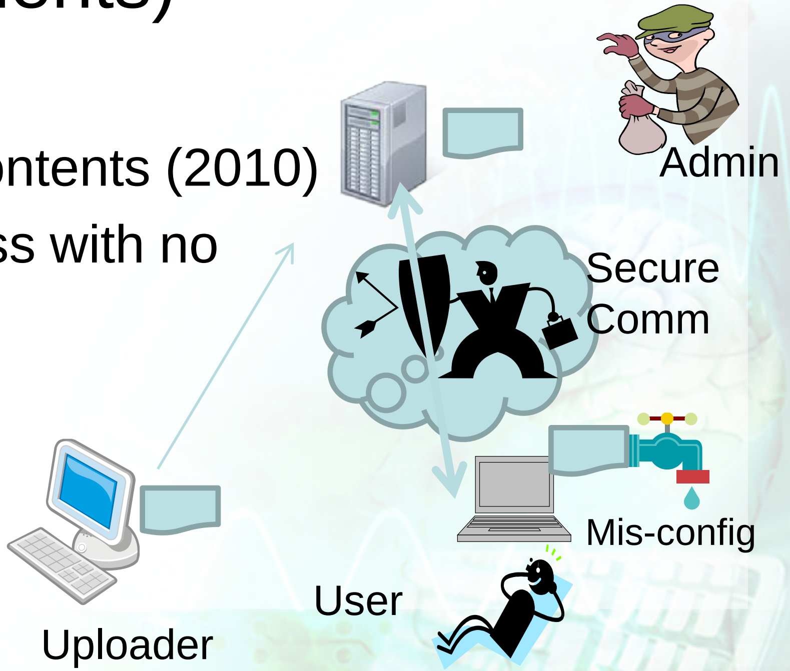
The detail is written in my paper [EuroSec'12]

Summary: OS on sharing technology

- Memory deduplication on cloud computing have a potential to change the structure of OS from the view of secuirty.
  - It will differ from OSes on devices (PC, Smartphone, etc), because OSes interact each other on IaaS.
- The OS on IaaS should take care of security and performance on the environment which shares resources with others.

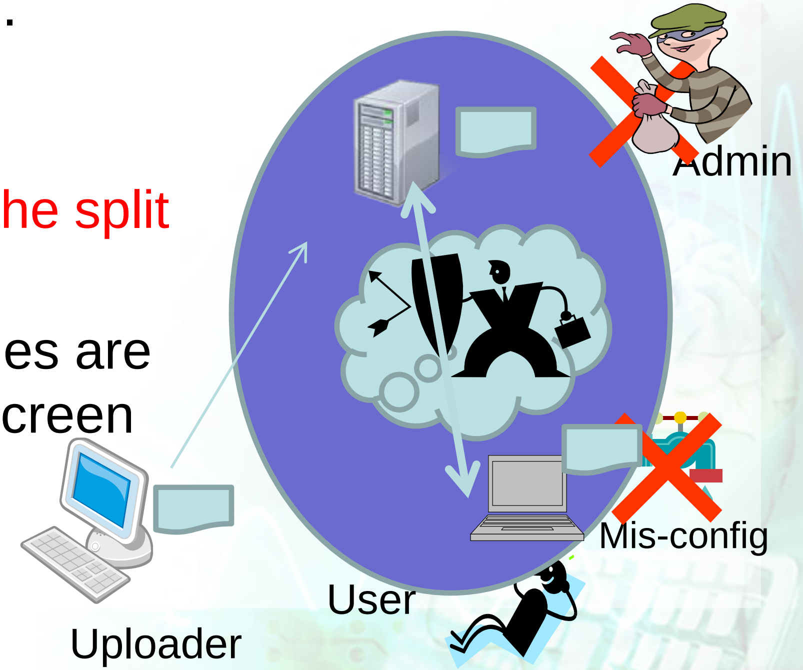
Data management Problem Information Leak

- Information leak does not occur on network.
  - Secure communication (ssh, SSL/TLS, etc) is established between client and server, and it is not easy to attack.
- Most information leaks on cloud storage occur on both edge machines (servers and clients)
  - On server
    - Gmail Administrator read use's contents (2010)
    - Dropbox had a bug to allow access with no pass word (2011)
  - On Client
    - P2P File sharing
    - (Japanese "Winny") (2003 ~)

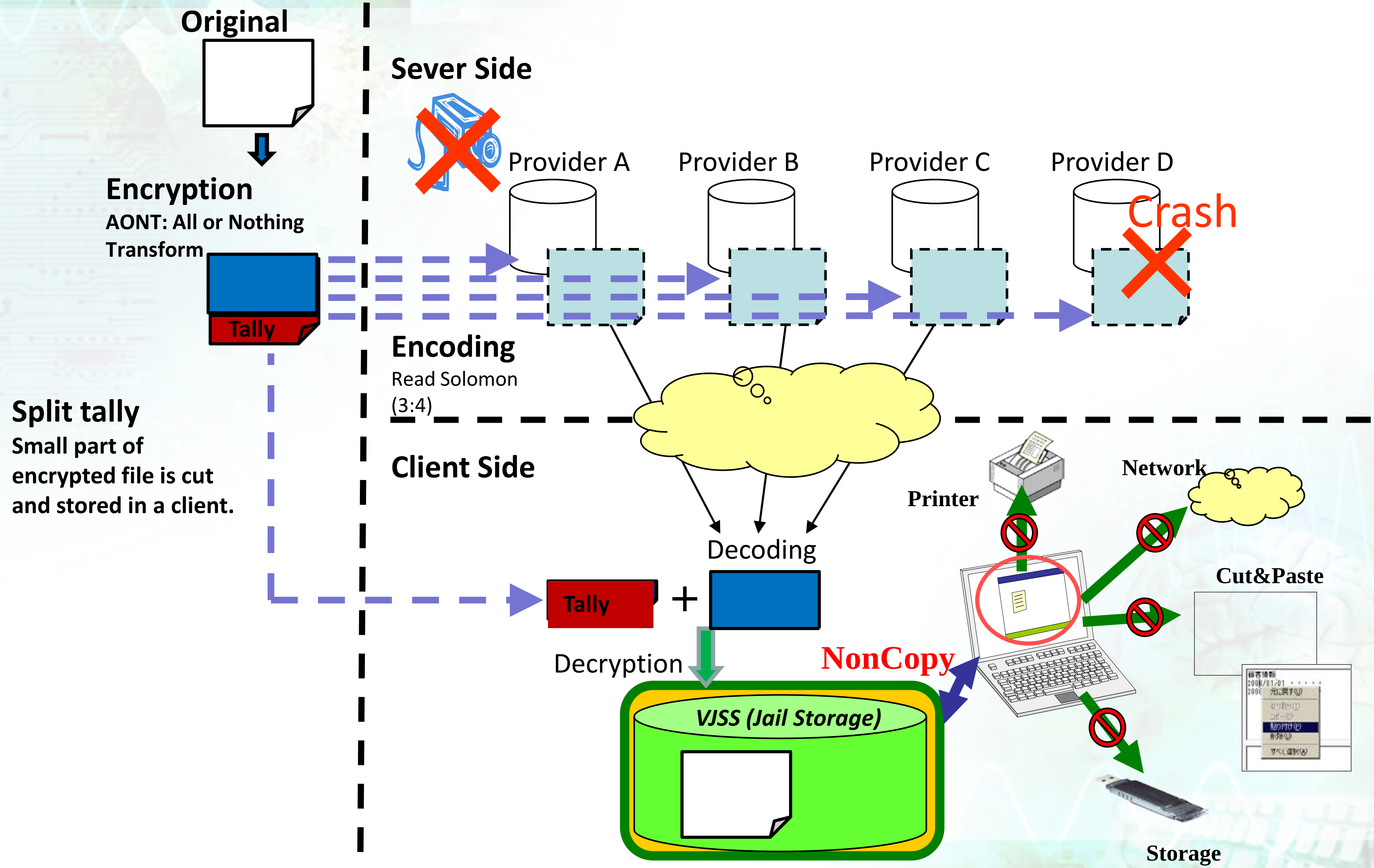


Our proposal

- Virtual Jail Storage System (VJSS)
  - On Server:
    - Data are encrypted and cut a split tally.
    - It mean that whole content of file are not upload. Even if the all uploaded data are gathered, the full contents are not reconstructed.
    - Data are also coded by Reed-Solomon and uploaded on some servers. It works for fault tolerance.
  - On Client:
    - Original file is reconstructed with the split tally.
    - Files are under access-control. Files are prohibited copying, printing, and screen cut&paste.



Overview of VJSS



Original

Encryption

AONT: All or Nothing Transform

Tally

Split tally

Small part of encrypted file is cut and stored in a client.

Sever Side

Provider A

Provider B

Provider C

Provider D

Crash

Encoding

Read Solomon (3:4)

Client Side

Decoding

Tally +

Decryption

NonCopy

VJSS (Jail Storage)

Printer

Network

Cut&Paste

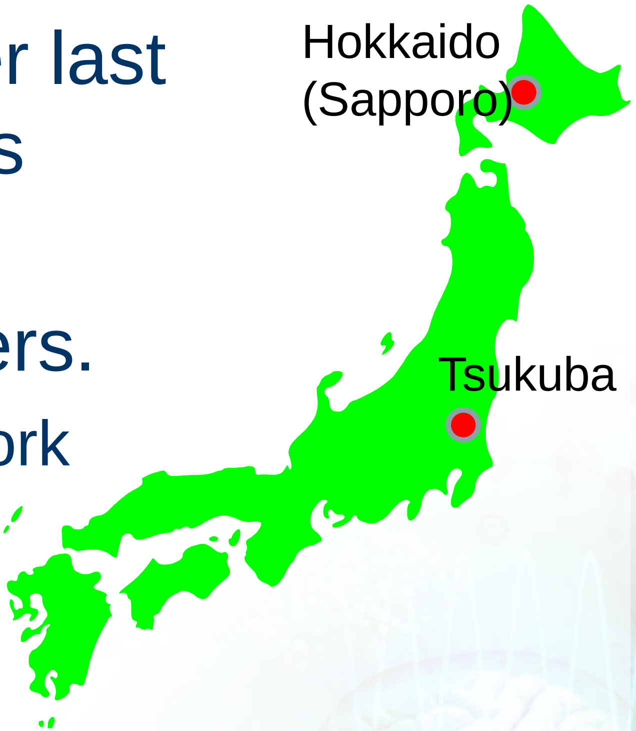
Storage

National Institute of Advanced Industrial Science and Technology
AIST

Deploying Plan (Against Disaster)

Research Institute for Secure Systems

- Japan had a heavy natural disaster last year. The deploying plan considers location against disaster.
- Collaborate with Japanese providers.
  - Hokkaido Telecommunication Network
    - Tokyo - Hokkaido(Sapporo) 1,000km
  - Dream Arts Okinawa
    - Tokyo - Okinawa 1,500km
- Severs for VJSS will be located at the southern and northern edges of Japan in order to prevent natural disasters.



Okinawa
Taiwan

Information Erase (Planned)

- Most users want to erase uploaded data completely, after the service is terminated.
- Unfortunately most provider cannot guarantee that all uploaded data are removed.
  - Even if uploaded data are encrypted, the data may be decrypted by brute-force attack.
- Our VJSS is a little bit advanced, because it keeps split tally in a client. Even if all uploaded data are decrypted, all contents are not disclosed.

Information loss (Planned)

- Hosting services have to prevent data loss, but some incidents occurred.
    - T-Mobile Sidekick lost user’s data (2009).
    - Japanese provider FirstServer lost user’s data (2012).
- Most information loss incidents were caused by operation mistake.
- VJSS has data redundancy by Reed-Solomon error correction, but it is not enough.
- We propose to use append-only file system on Cloud Storage.
    - Most data will be shared by deduplication technology.

Conclusion

- Sharing technology (deduplication) on IaaS has a potential to change the structure of OS on it.
- Many people want to use cloud storage, but they are afraid of information leak/erase/loss.
  - Virtual Jail Storage System (VJSS) prevents information leak from a server and a client. VJSS plans to treat information erase and loss.