KEK Security & CSIRT

Tadashi Murakami
KEK
Computing Research Center
/ CSIRT

Outline

- Introduction
  - KEK-CRC, KEK-CSIRT
- KEK network and security
- Situations of information security in KEK and Japan
- KEK CSIRT

First of all,

- I belong to Computing Research Center in KEK
  - Mainly, operate and introduce security infrastructure
  - Research and Development
- When a serious incident occurs, I devote in CSIRT works
- In these few years, I feel security circumstances get rapidly worse
- Unlike computer and network operations, I feel it is difficult to share failure experiences in computer security
  - directly associate to an organization’s weakness

Introduction

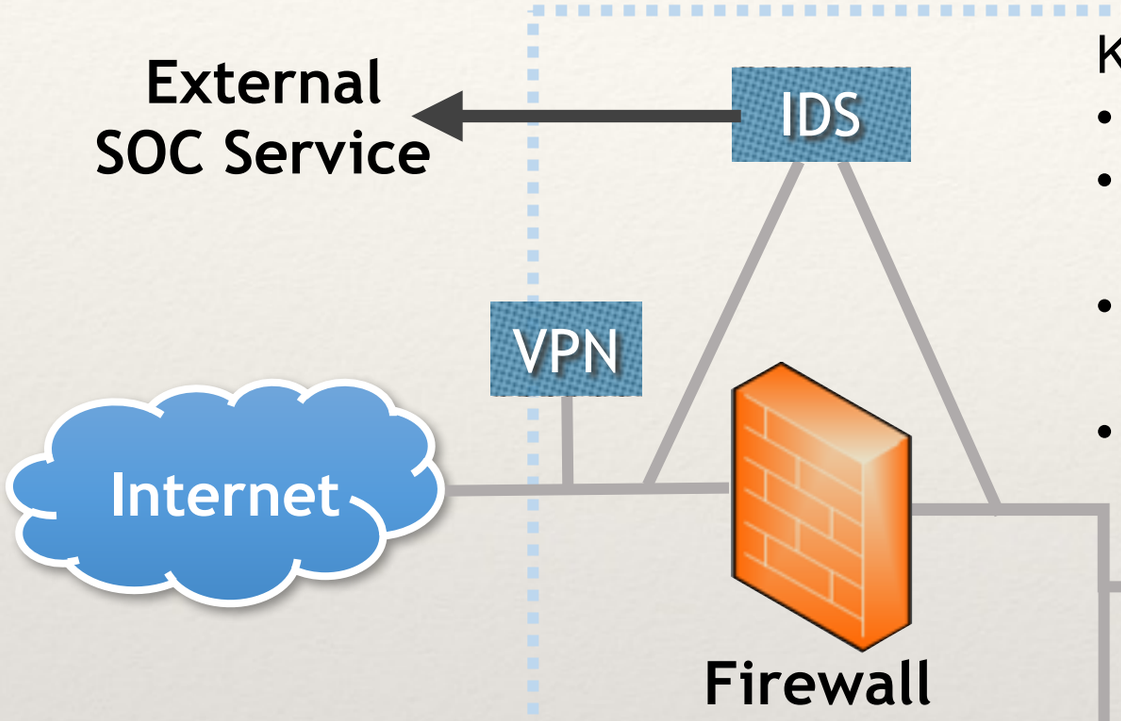
KEK-CRC, KEK-CSIRT

KEK CRC and CSIRT

- KEK Computing Research Center (CRC)
  - Mission: to provide IT infrastructures, computer systems, network, mail, web for various researches in KEK
  - Information security has been one of important missions in these years
  - KEK-CRC manages its own systems to provide services, but doesn't manage user's personal computer and their security risks
- KEK CSIRT (Computer Security Incident Response Team)
  - Mission: to defend information assets from inner/outer threats
  - KEK-CSIRT gives advices to users who are facing to security incidents
- KEK-CRC has been involved in CSIRT as an activity of security management
  - actually, a lot of human resources in CRC are introduced

KEK network and security

KEK network



KEK-CRC manages the local network and the Firewall

- manage a database of IP and MAC addresses
- MAC address registration is mandatory to use the network
- Firewall records every incoming and outgoing connections
- Services of DNS, DHCP, NTP, etc

DMZ network

Accessible from the Internet

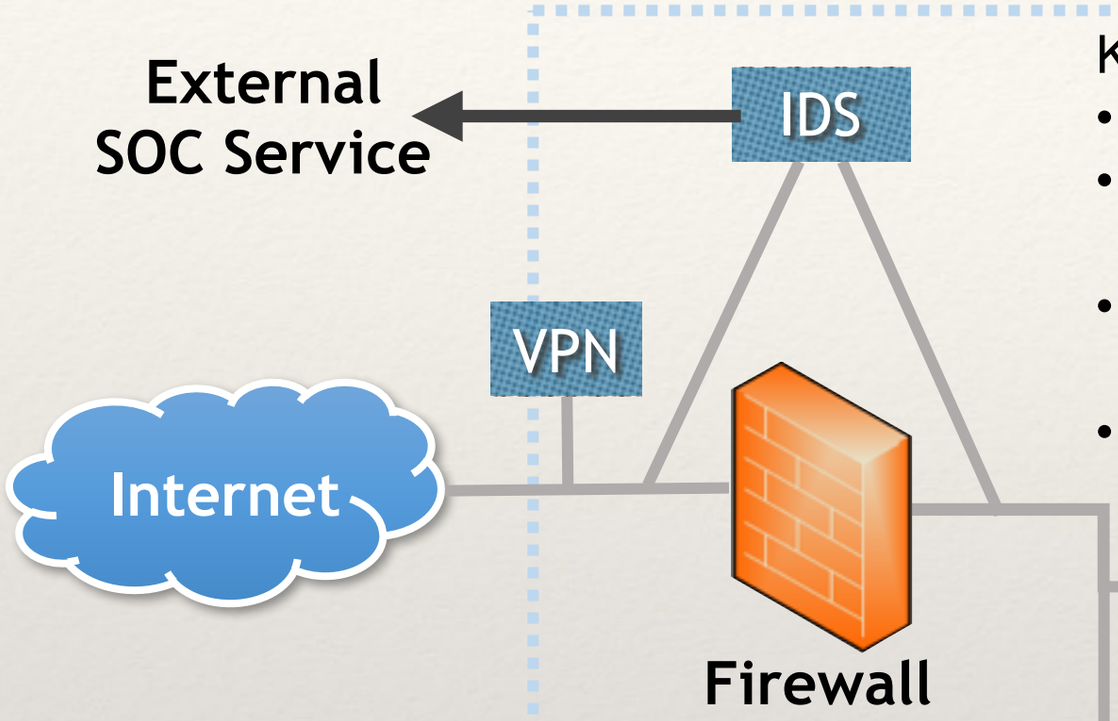
Intranet (multiple subnets)

About 7000 global IPs in 40 subnets
Some are gateways to bundle internal networks

To keep the network secure, we mainly manage and control MAC addresses:

- Each of registered MAC addresses also have user contact information
- Each of registered MAC addresses has a control frag whether a network connection is allowed

KEK network



KEK-CRC manages the local network and the Firewall

- manage a database of IP and MAC addresses
- MAC address registration is mandatory to use the network
- Firewall records every incoming and outgoing connections
- Services of DNS, DHCP, NTP, etc

DMZ network

Accessible from the Internet

Intranet (multiple subnets)

About 7000 global IPs in 40 subnets
Some are gateways to bundle internal networks

To keep the network secure, we mainly manage and control MAC addresses:

- Each of registered MAC addresses also have user contact information
- Each of registered MAC addresses has a control frag whether a network connection is allowed

DMZ User's Portal

Self security analysis and reporting service

- In KEK-DMZ network, about 400 hosts are located
  - managed by 100 users
- Each host has its own circumstances
  - It is difficult to settle security standards, because of too many circumstances …
  - Each owner of hosts has responsibility in security management
- We have a vulnerability scanner that evaluates each vulnerability in a score
  - If the score is over 1000, the vulnerability is regarded as severe
  - proprietary, rich functions
  - intricate to use

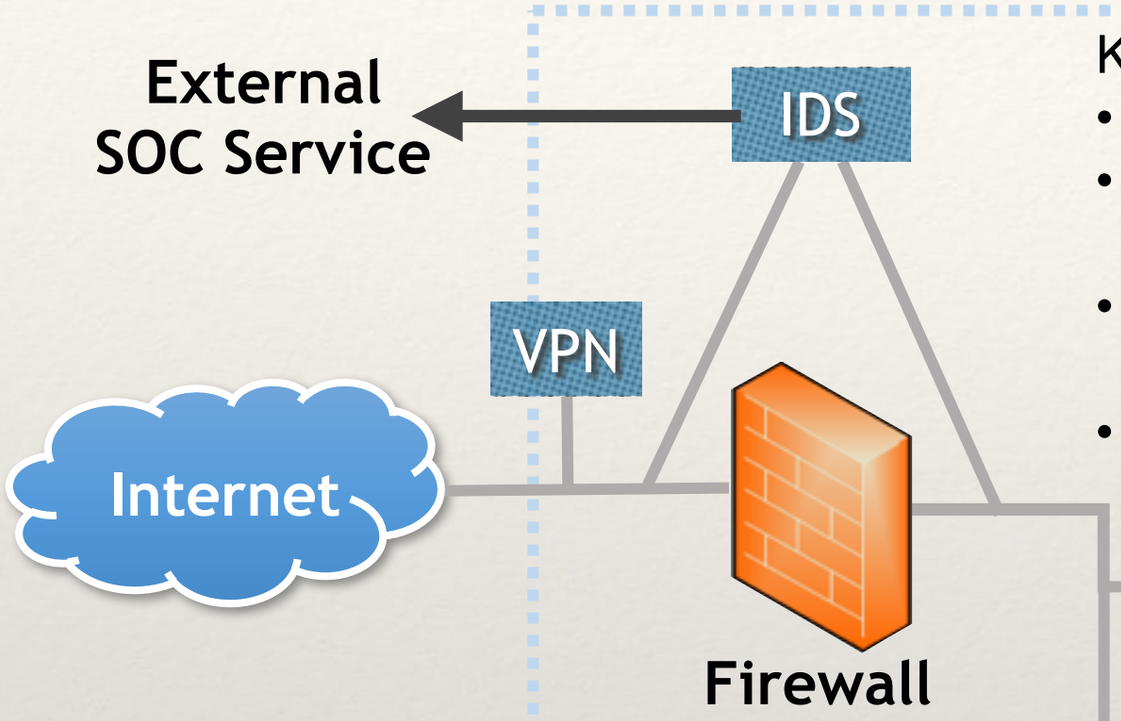
DMZ User's Portal

Self security analysis and reporting service

- DMZ User's Portal: for easy use
  - Run a security analysis of owner's host in one click
  - Download a report of the analysis
  - Submit the report
    - the internal security committee inspect the reports once a year
  - We developed a wrapper module for the vulnerability scanner
    - able to follow the upgrade of the vulnerability scanner
- Security management is done by each user
  - then, also introduced in J-PARC

- T.Murakami, et al. DBPowder: A Flexible Object-RelationalMapping Framework based on a Conceptual Model. the 37th IEEE COMPSAC 2013, Kyoto, Japan, pp.589–598, Jul. 2013. (acceptance rate 23%)
- T.Murakami, et al. Vulnerability Management by the Integration of Security Resources and Devices with DBPowder. Grid Camp and HEPiX Fall 2008, Oct. 2008.

KEK network



KEK-CRC manages the local network and the Firewall

- manage a database of IP and MAC addresses
- MAC address registration is mandatory to use the network
- Firewall records every incoming and outgoing connections
- Services of DNS, DHCP, NTP, etc

DMZ network

Accessible from the Internet

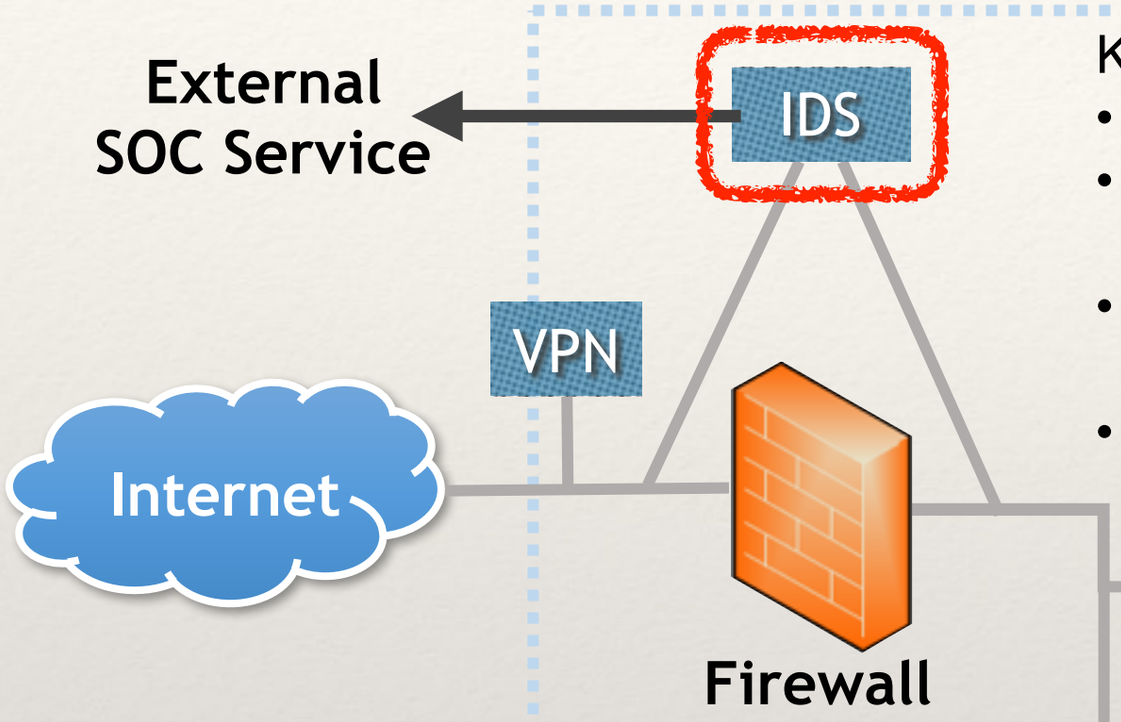
Intranet (multiple subnets)

About 7000 global IPs in 40 subnets
Some are gateways to bundle internal networks

To keep the network secure, we mainly manage and control MAC addresses:

- Each of registered MAC addresses also have user contact information
- Each of registered MAC addresses has a control frag whether a network connection is allowed

KEK network



KEK-CRC manages the local network and the Firewall

- manage a database of IP and MAC addresses
- MAC address registration is mandatory to use the network
- Firewall records every incoming and outgoing connections
- Services of DNS, DHCP, NTP, etc

DMZ network

Accessible from the Internet

Intranet (multiple subnets)

About 7000 global IPs in 40 subnets
Some are gateways to bundle internal networks

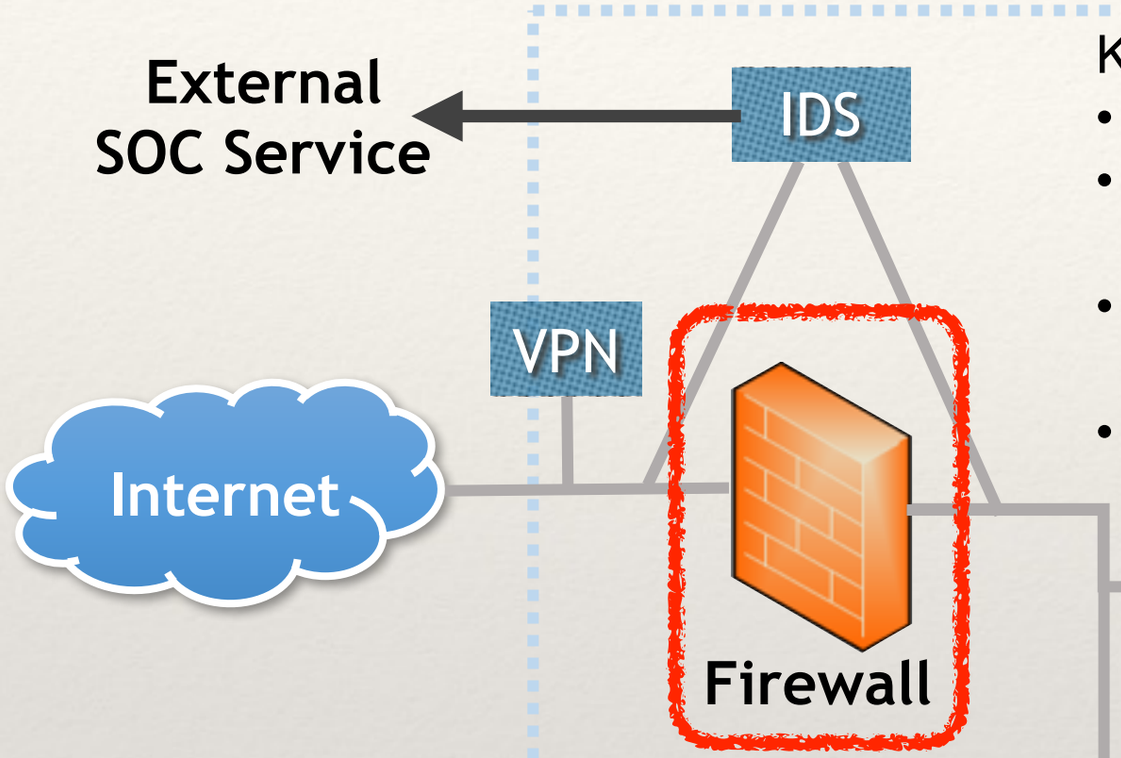
To keep the network secure, we mainly manage and control MAC addresses:

- Each of registered MAC addresses also have user contact information
- Each of registered MAC addresses has a control frag whether a network connection is allowed

IDS: Collaboration with external SOC service

- IDS: McAfee Network Security Platform (NSP)
  - Security operation center (SOC) service in outsource
    - log analyses (24 hours, 365 days)
      - When a malicious communication is detected,
        - SOC blocks the IP
        - SOC tells us
        - We contact with the owner and start the security incident response
      - We also monitor the logs

KEK network



KEK-CRC manages the local network and the Firewall

- manage a database of IP and MAC addresses
- MAC address registration is mandatory to use the network
- Firewall records every incoming and outgoing connections
- Services of DNS, DHCP, NTP, etc

DMZ network

Accessible from the Internet

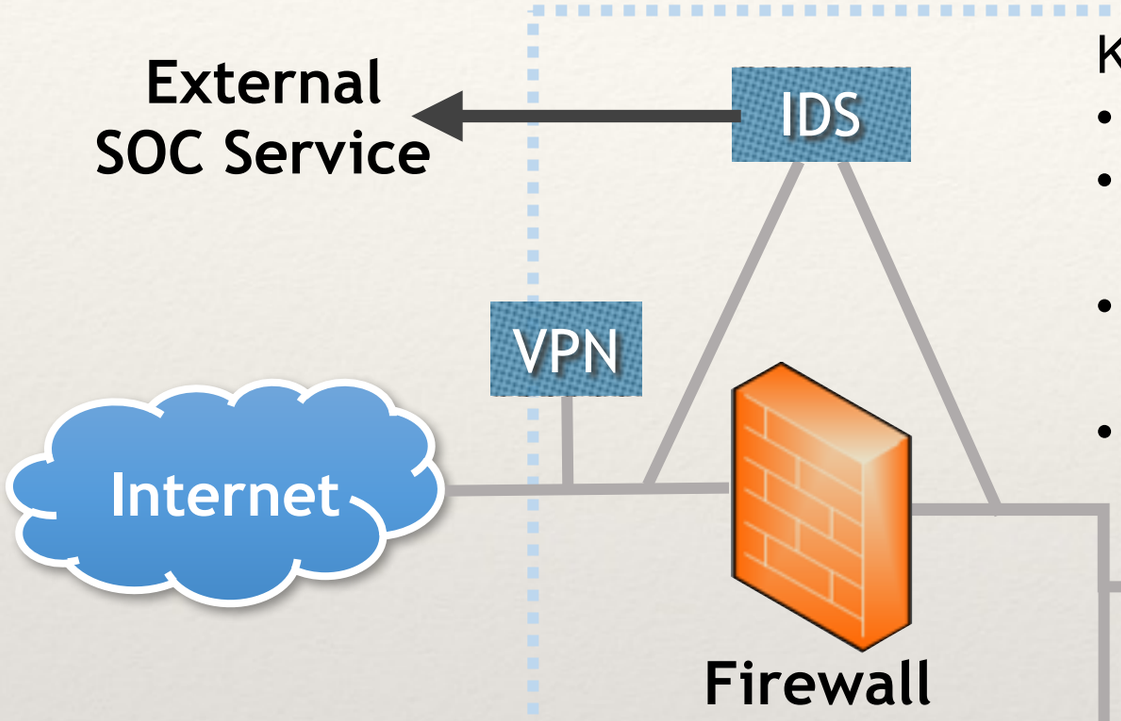
Intranet (multiple subnets)

About 7000 global IPs in 40 subnets
Some are gateways to bundle internal networks

To keep the network secure, we mainly manage and control MAC addresses:

- Each of registered MAC addresses also have user contact information
- Each of registered MAC addresses has a control frag whether a network connection is allowed

KEK network



KEK-CRC manages the local network and the Firewall

- manage a database of IP and MAC addresses
- MAC address registration is mandatory to use the network
- Firewall records every incoming and outgoing connections
- Services of DNS, DHCP, NTP, etc

DMZ network

Accessible from the Internet

Intranet (multiple subnets)

About 7000 global IPs in 40 subnets
Some are gateways to bundle internal networks

To keep the network secure, we mainly manage and control MAC addresses:

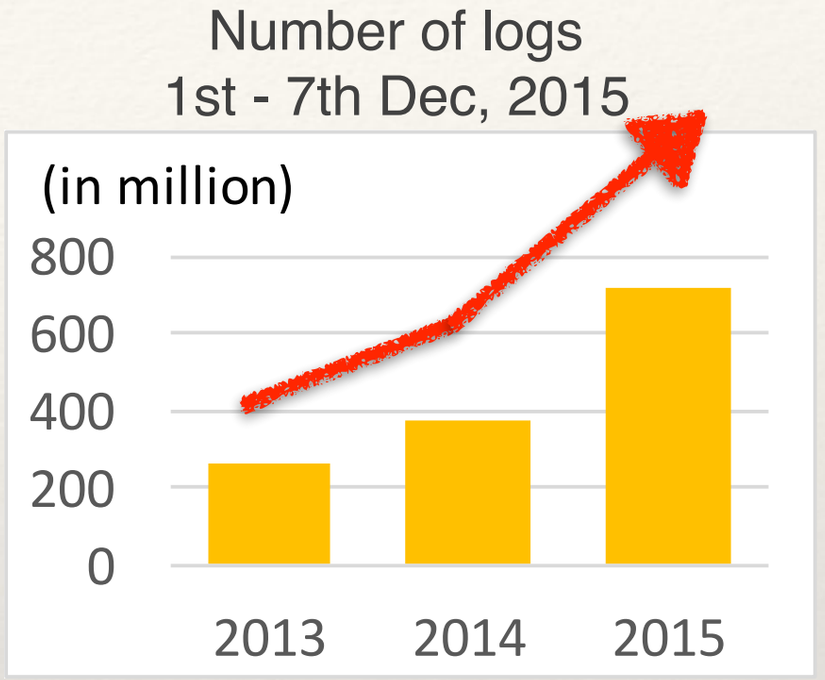
- Each of registered MAC addresses also have user contact information
- Each of registered MAC addresses has a control frag whether a network connection is allowed

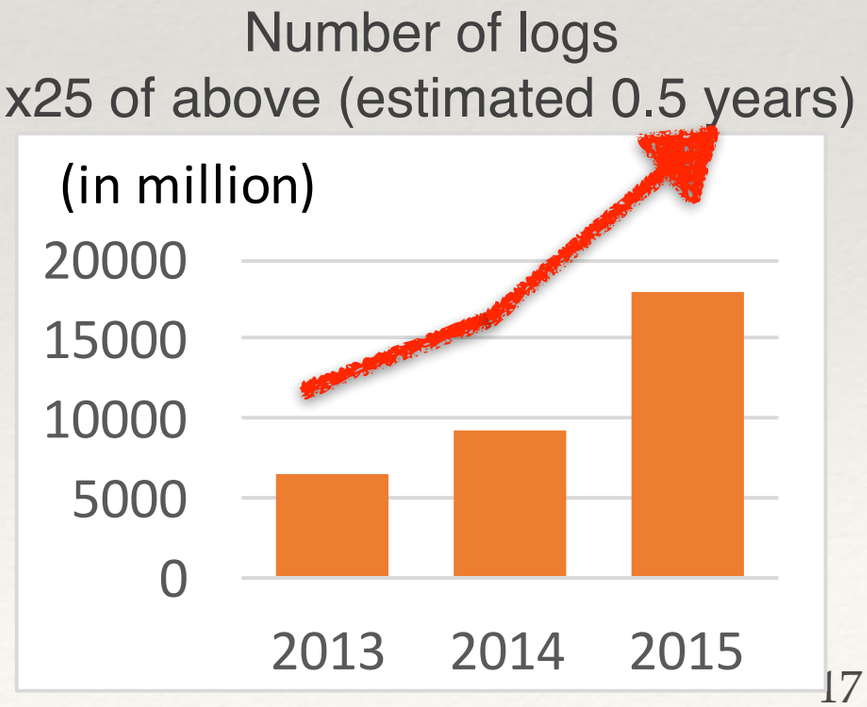
Firewall

- Firewall: PaloAlto
- monitor all connections between Internet and intranet
- block suspicious IPs, FQDNs, URLs
- Automatic block of suspicious URLs
  - In wireless connections and VPN
- logging IP connections: next slide

Firewall: logging IP connections

- 800 million in 1 week
  - Increasing, and we cannot estimate the future
- Log analysis is important, but
  - proprietary tool does not fit in performance and/or annual cost
  - For previous FW products, I developed a log collector tool for Oracle
    - enjoyed SQL analyses
    - but does not fit to the current FW…
    - in current, designing a new scheme



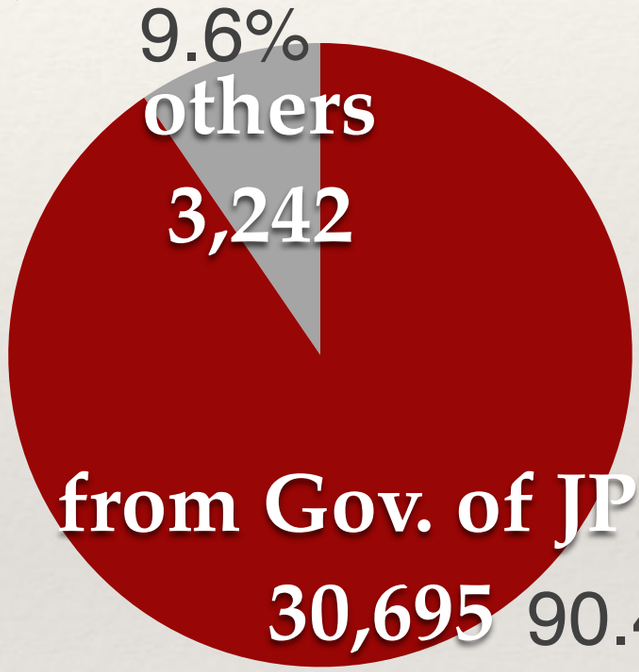


Situations of information security in KEK and Japan

Situations of information security

- KEK's budget mainly comes from the grants of the government of Japan — more than 90%
- Japan Government is anxious about any incidents
  - e.g., subtle and malicious targeting attacks are also succeed in Japan in these years
    - in fluent Japanese (e.g., Emdivi)
  - If a serious incident is occurred, managers have to apologize (or "shazai") in public
- We also have to be anxious about any incidents
  - Note that more than 90% of budget comes from grants of the government

KEK Annual budget plan 2015
unit: 1 million yen (about 10 thousand $)
total 33,937



Example: Situations of information security

- e.g., when KEK causes a serious security incident,
  - We have to report the incident immediately to the government
  - In the final report,
    - Measures for preventing recurrence are always required
    - arrange meetings three or more times
  - New preventing recurrences will be added one by one

- If serious security incidents continue to occur,
  - The government will think that we cannot continue quality management

KEK CSIRT

KEK CSIRT: Members & Responsibility

- Members & Responsibility
  - 6 regular members
- When in a serious incident,
  - 3 or more occasional members devote to the incident response
    - investigation
    - for the government: preventing recurrence, three-or-more-time meetings, etc
- Sometimes, more than one serious incident occurs in a same time
  - 6 or more occasional member have to devote
  - challenge for KEK CSIRT

Responsibility	
primary responsible	**1**
occasional responsible	**5**
project specific	*5*
Total	**6** + *5*

Associations in security and CSIRT

- It is important to associate among organizations to share information about security
  - unofficial or underground included
- We have relationships with other organizations in two domestic associations:
  - NCA (Nippon CSIRT Association)
    - sharing ideas about CSIRT activities
    - among various kinds of organizations of 137 teams (as of Apr 2016)
  - SWS (Security WorkShop)
    - RIKEN, Spring-8, RCNP, KEK, etc.
    - association among research organizations
    - have annual workshop to share unofficial information

I want to know …

- In research institutes, freedom and independence is crucially important, but sometimes security measurements conflict them
- Have you adopted any restrictions in these years, in considering, or already introduced?
  - We introduced automatic URL blacklist in WLAN subnets in 2015, and considering to introducing in whole LAN
  - We hesitate to introduce security agent software (except for AntiVirus) to user's PCs, due to the difficulty to get into user environments
    - If you have any successful case, I'd like to know know-hows
- Unlike computer and network operations, I feel it is difficult to share failure experiences in security. Do you have any way to share?

Thank you !

Danke schön !