



# Automation of Network Operations by Cooperation between Anomaly Detections and Operation Logs

**Naoki Yoshida, Shingo Ata,  
Graduate School of Engineering, Osaka City University  
Hiroki Nakayama, Tsunemasa Hayashi  
BOSCO Technologies Inc.**

# Introduction

---

- Network management becomes more important to save a safe and secure ICT infrastructure
- Automation of the management is a big challenging for future networks
  - It is difficult to take appropriate actions **against rapid, complicated, and diverse** variation of behaviors in networking
  - Shortage of experts in network operations and management

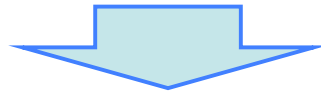
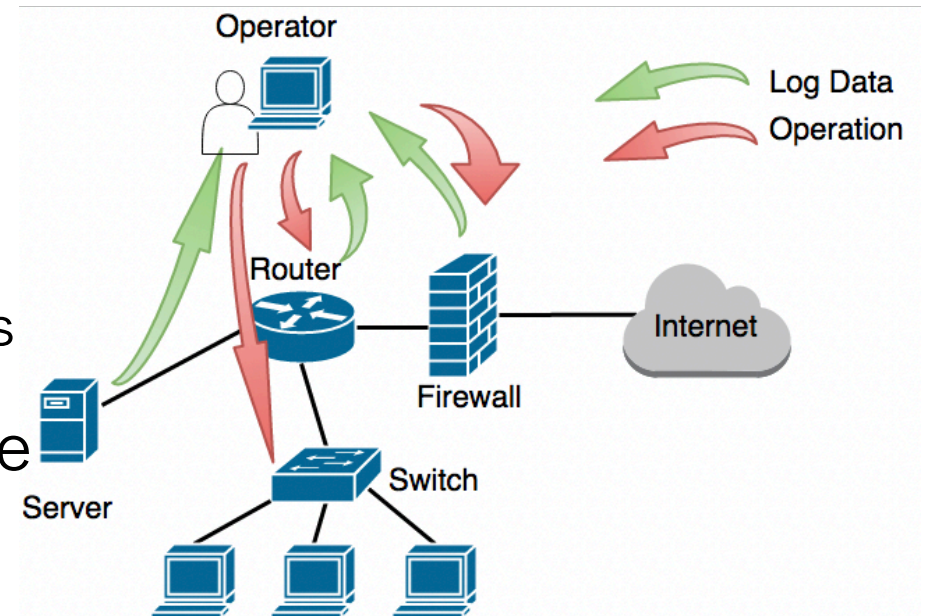
# Introduction

---

- We propose a new framework for automating operations and management of ICT infrastructure, by combination of both networking/system incidents and records of operations.
- Our framework focuses on the integration of various types of log data.
- We demonstrate an implementation of our framework by using honeypots and ssh-based agents.

# Conventional Operation

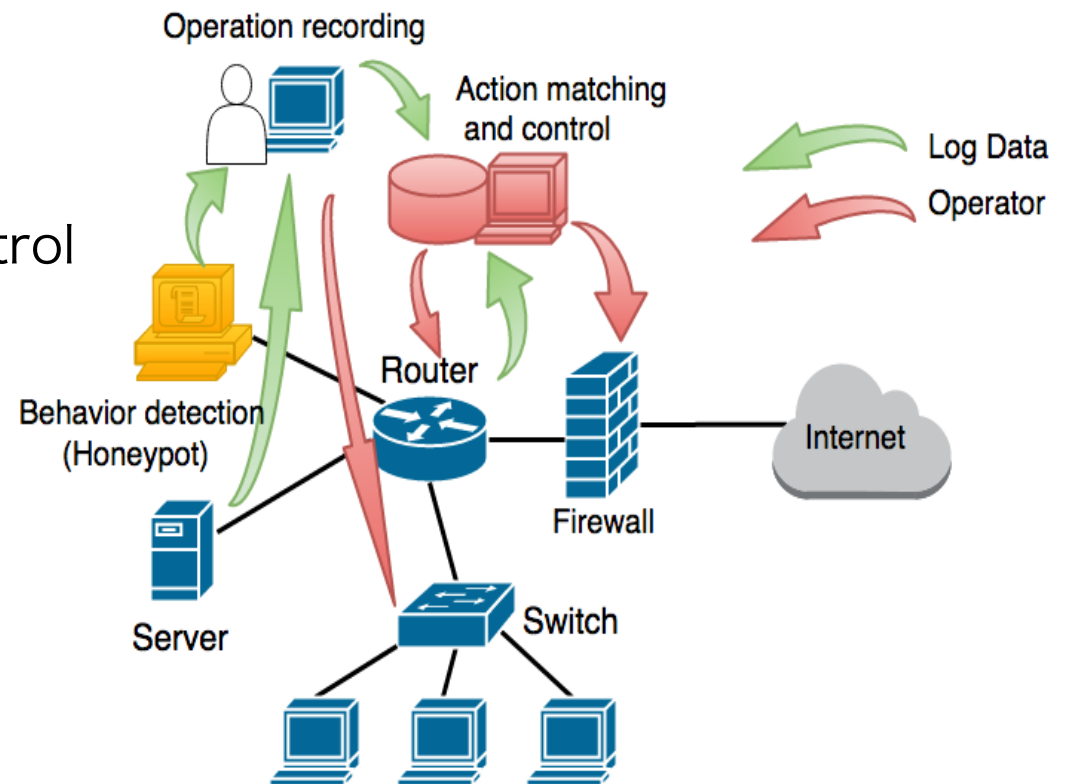
- Operators
  1. Collect logs from devices
  2. Analyze a huge volume of log based on experience
  3. Execute appropriate operations
- However the complexity of the system is increasing



It is difficult for operators to analyze logs in a short time

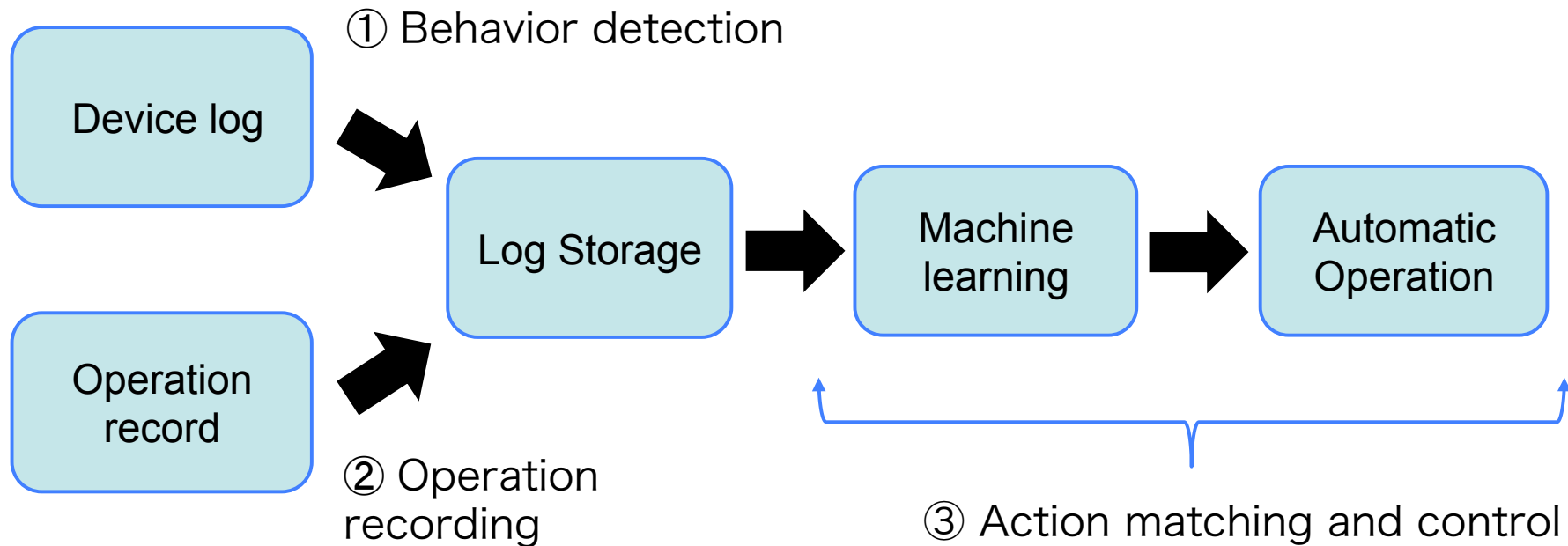
# Proposed Framework

- Our framework consists of 3 parts
  1. Behavior detection
  2. Operation recording
  3. Action matching and control





# Proposed Framework



# Behavior Detection

---

- Device logs
  - Just collecting the log data makes the number of logs enormous and increases the risk of missing important information.
  - The types of logs are various (syslog, ids alerts, SNMP, etc.).
  - A single system like conventional anomaly detection devices, cannot detect information on unknown threats

In order to collect and manage information,  
device logs are sent to the log storage.



## Operation Recording

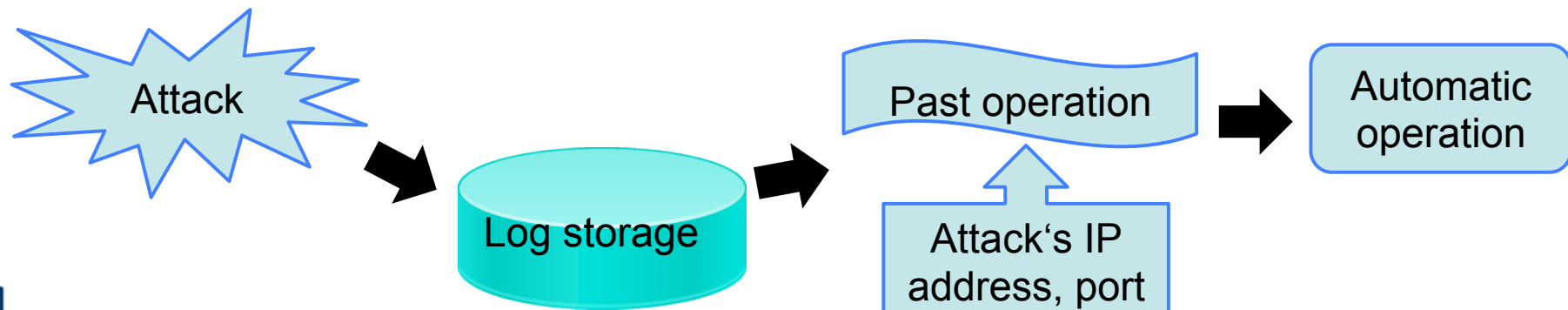
---

- We use the operator's command to perform the operation **suitable for the various environment.**
- We need the records of the operation  
(ex. the time, commands, authentication information, etc.)
- We use SMART Gateway<sup>[1]</sup>.
- The administrator can record all the operations by operating the terminal via the SMART GW when performing operations on the device.

[1] <http://www.bosco-tech.com/smart-gw/>

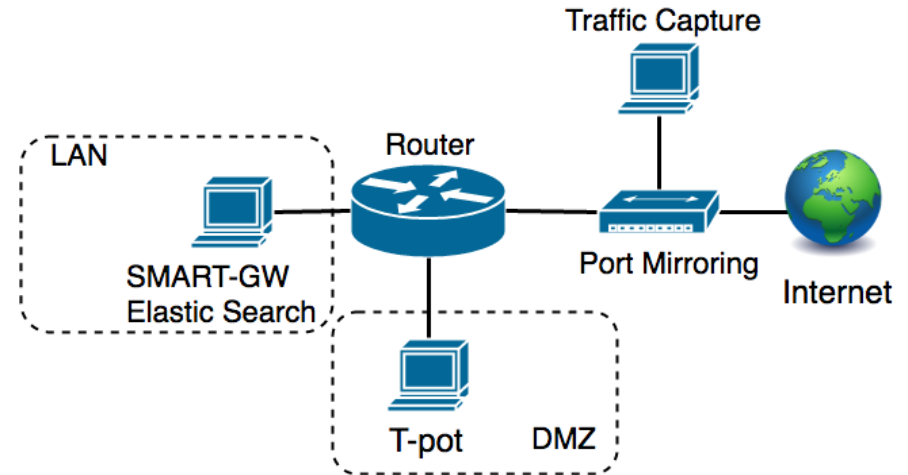
## Action Matching and Control

- The log data accumulated in the storage is searched at regular intervals.
- When there is an operation that coped with the same behavior in the past, the parameter obtained from the new log is applied to the variable, and the action is taken automatically.



# Implementation

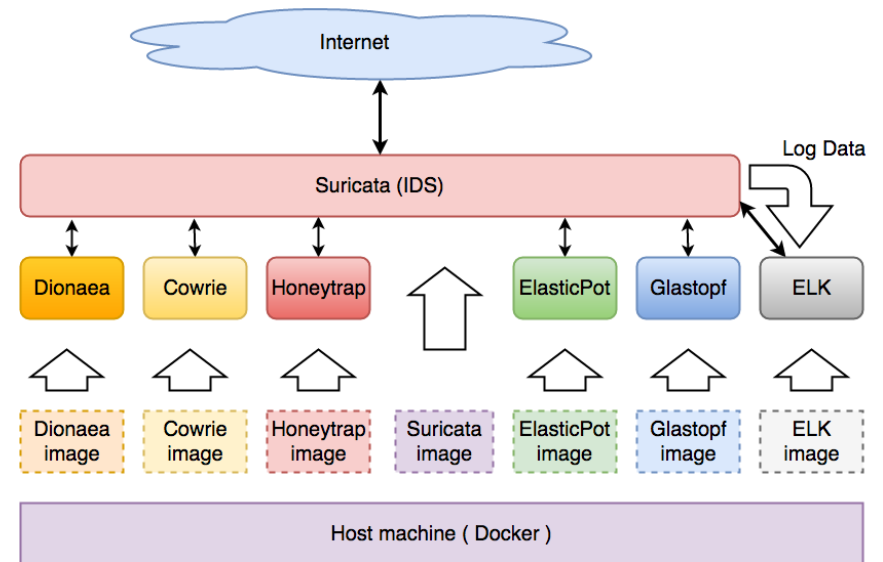
- The right figure is our experimental environment.



- T-pot

It is a multi-honeypot platform.

We use it as **Behavior Detection**.



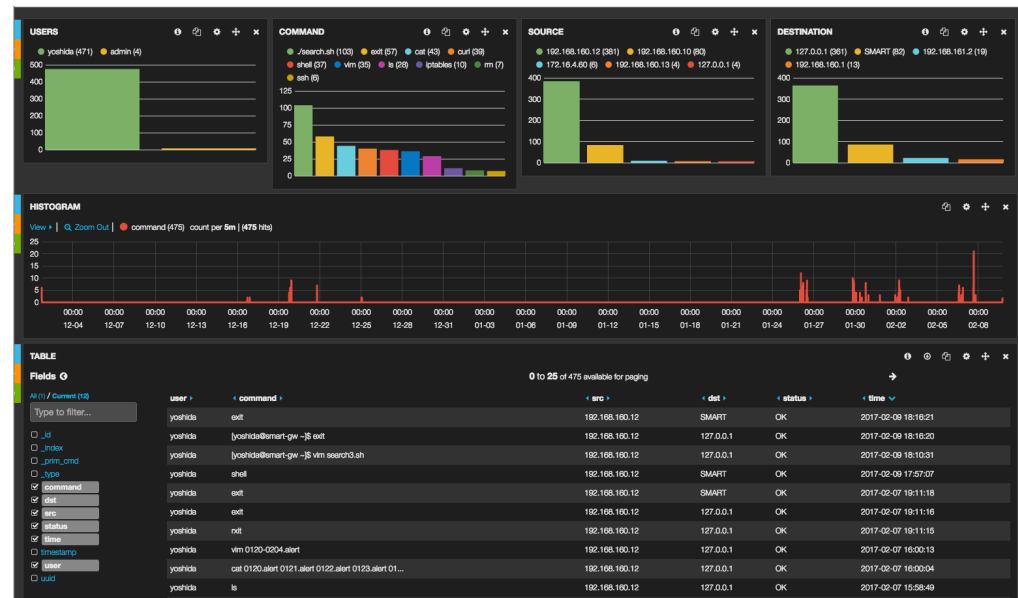
# Implementation

- SMART Gateway

It records operational commands to servers and network devices (ex. the time, the executed command, the authentication information).

We use it as

Operation Recording.



# Implementation

---

- Action matching and control

- 1) Log Search

The logs are sent to Elasticsearch.

If similar attacks and operations have been done in the past, replace the variables and apply the same operation.

- 2) Automatic Operation

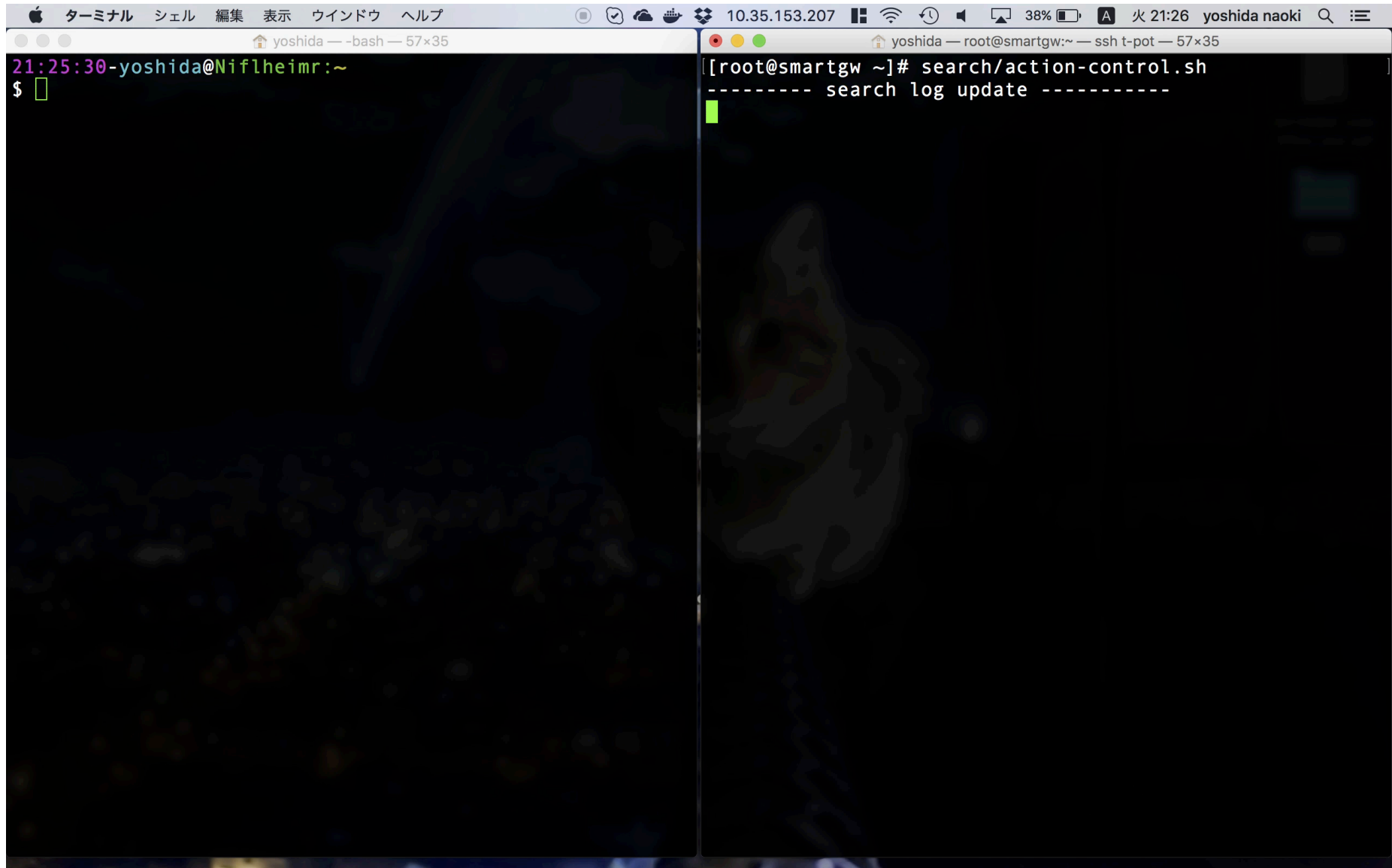
It is necessary to login to the operation target device and execute the command.

We implemented SSH-based agent with SMART-GW.

## Verification

---

- We confirmed the basic function of our framework  
First, the attack logs and the operation record are accumulated,  
and a correspondence table is created.  
Second, We confirmed that attack logs can be automatically  
detected when the next attacks are recorded.  
Finally, it confirmed that the associated operation is  
automatically reproduced after reflecting new attack log.



```
ターミナル シェル 編集 表示 ウィンドウ ヘルプ 10.35.153.207 38% 火 21:26 yoshida naoki
yoshida -- -bash -- 57x35
21:25:30-yoshida@Niflheimr:~
$

yoshida -- root@smartgw:~ -- ssh t-pot -- 57x35
[root@smartgw ~]# search/action-control.sh
----- search log update -----
```

## Conclusion

---

- We propose a framework on automation of management operation by linking the anomaly detection with the operation log.
- We showed that the operation can be applied automatically by our framework.
- Future works
  - We will introduce a machine learning method to automate linking anomaly detection and operation records.



---

**Thank you for listening!**