IB3-2

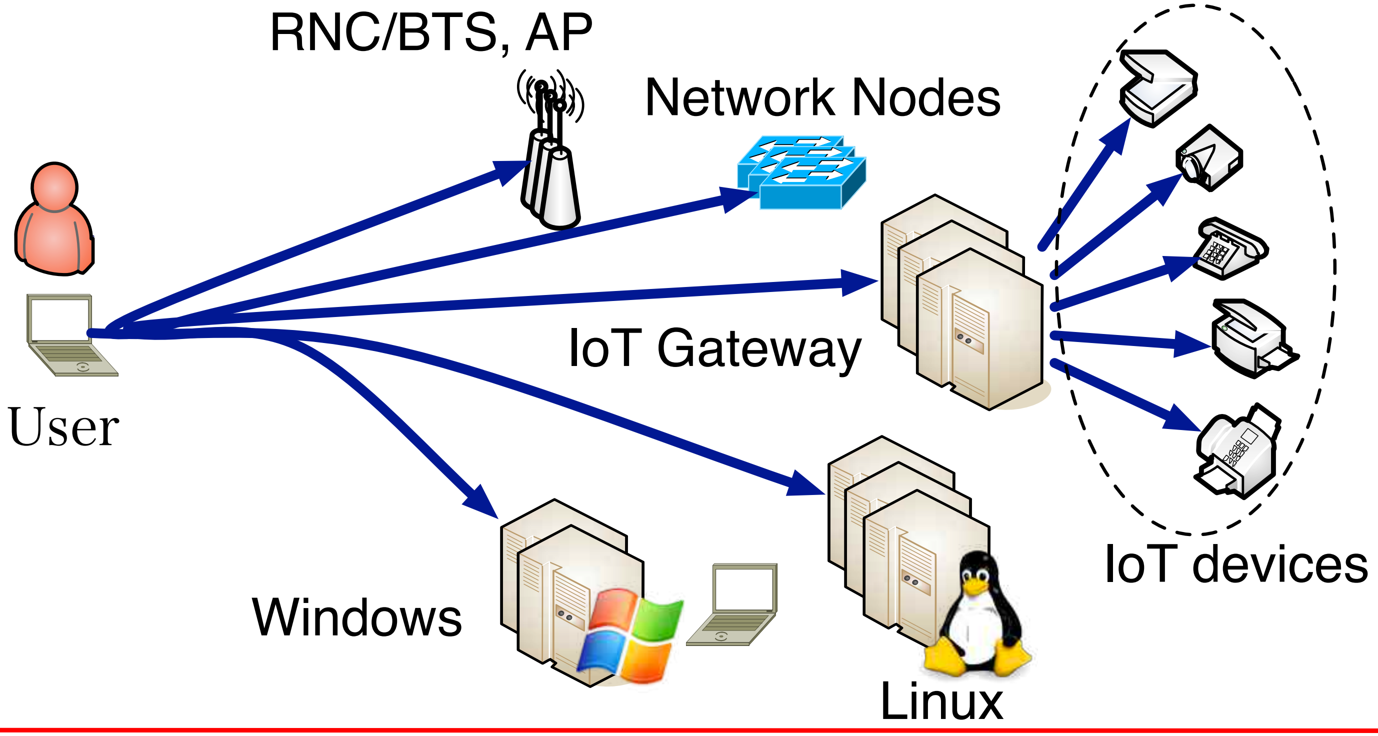
Environment independent IT-management for low-cost and robustness operation

Tsunemasa Hayashi

BOSCO Technologies

Topic area: ICT management

- Many type of services and devices has been deployed.
  -> Low Opex



Summary

- how management interface against number of components in ICT infrastructure are integrated into single management
- how the behavior against management interface is logged for each connection to the infrastructure
- operation correctness from logged session data
- the feasibility in a commercial environment with 100,000 nodes as ICT infrastructure

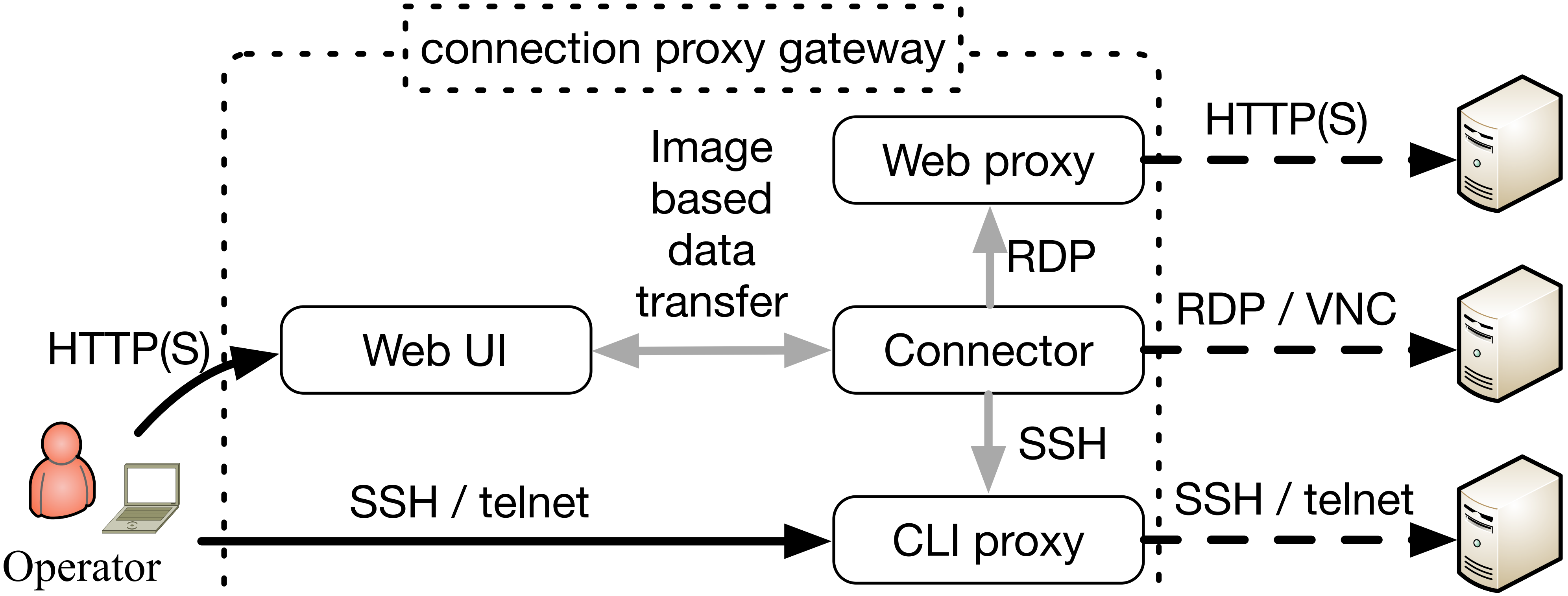
Background

- microservices to quickly provide various kinds of service deployments
- several kinds of infrastructure orchestration tools are becoming ready on commercial environment
- Quickly deploy not only applications but also for network elements
- Just push code or configuration without human operation on the provisioning phase
- still required to access ICT infrastructure directly on the management phase
- harder to check what is going on when problem occurred in target service
- human operation error is still the critical factor of service failure

Proposal overview

- investigated protocol-based connection integration system as connection proxy gateway
- integrate all the management interface into single management system
- provide logging management operations
- provide connection restriction features

architecture of connection proxy gateway

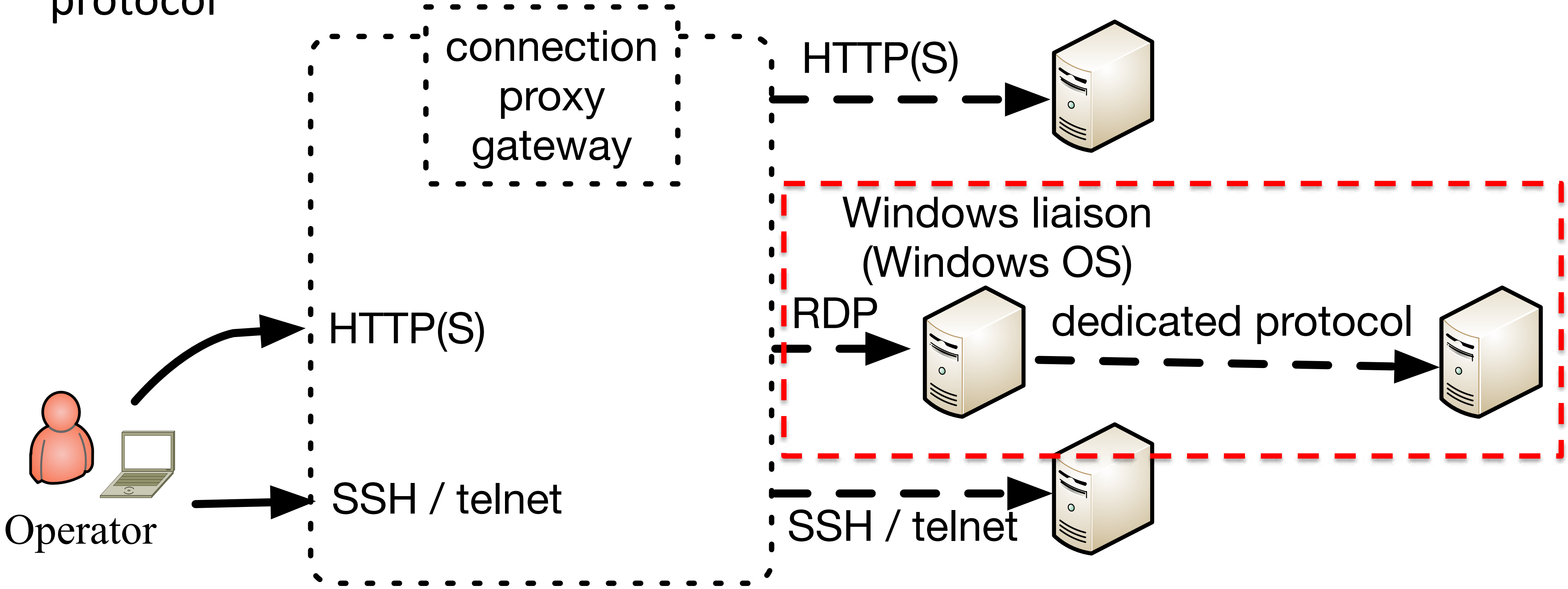


Issues on this architecture

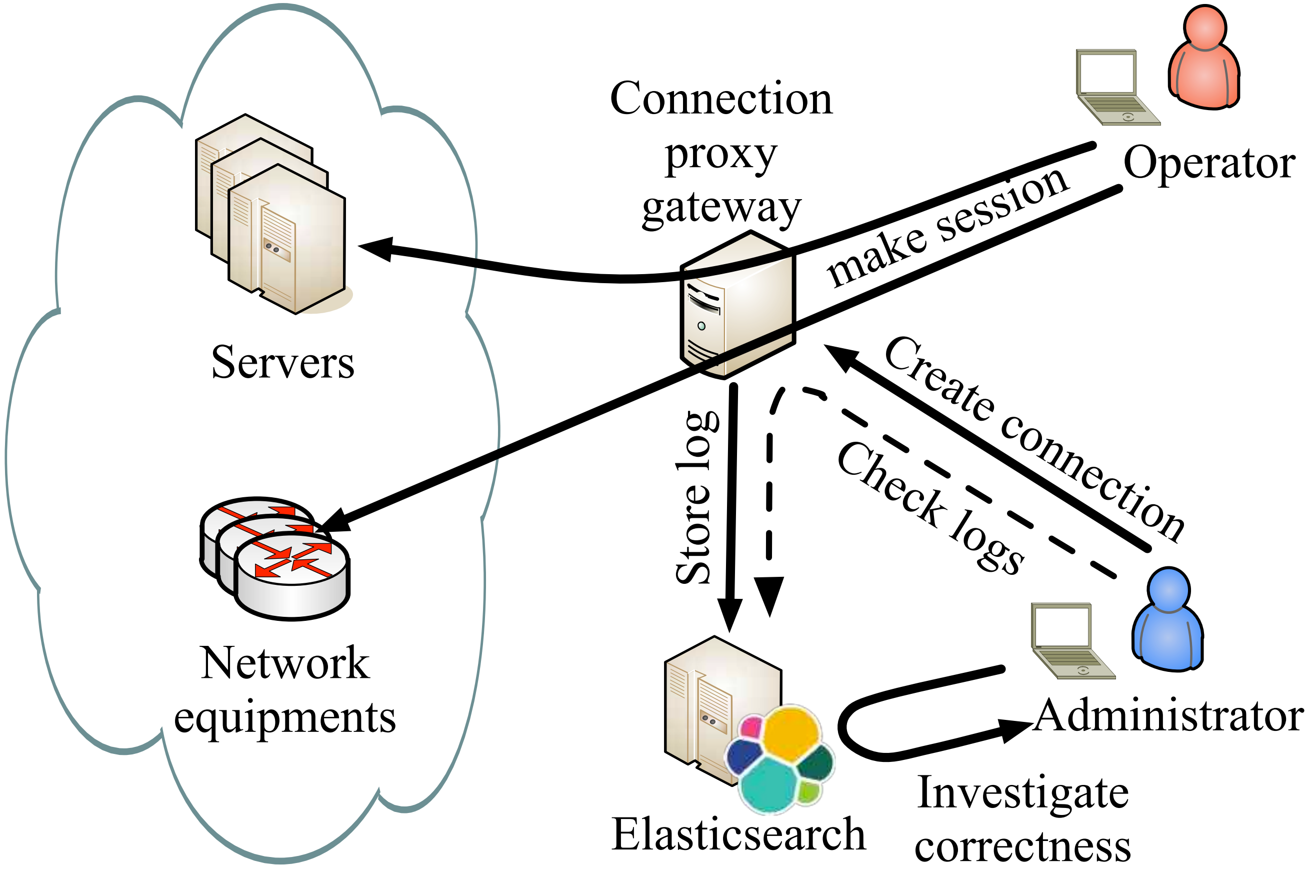
- cannot support application dedicated protocol (e.g.) between vSphere Client and vCenter server
- integrate “Windows OS” into the connection proxy gateway as liaison

Enhanced architecture for dedicated protocol

- RDP protocol from the Connector are transfer to the application dedicated protocol



Architecture of typical implementation

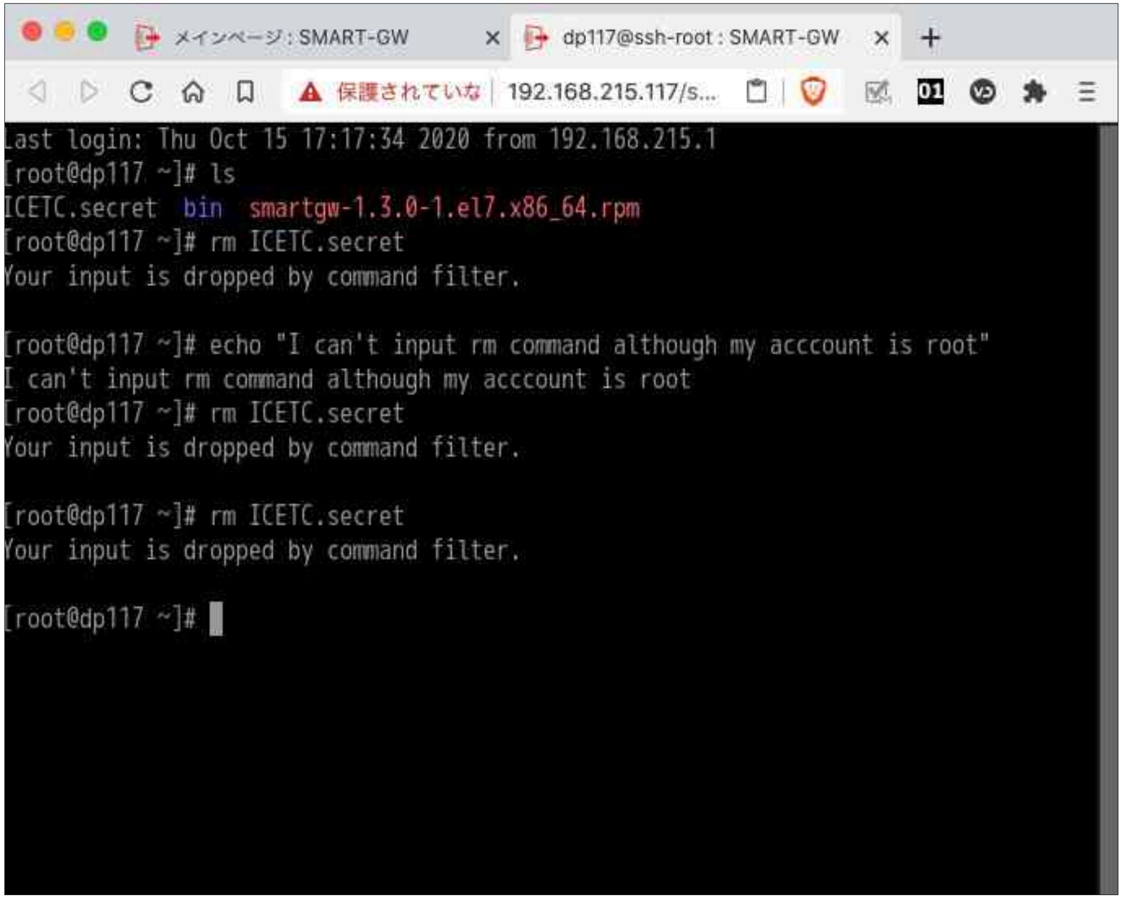


mitigates human operation error on ICT infrastructure

1. Create connections dynamically for user based on service deployment
2. Design human operation for login to ICT infrastructure
3. RDP or SSH or HTTP session against ICT infrastructure via Web UI
4. Check and investigate logged session data

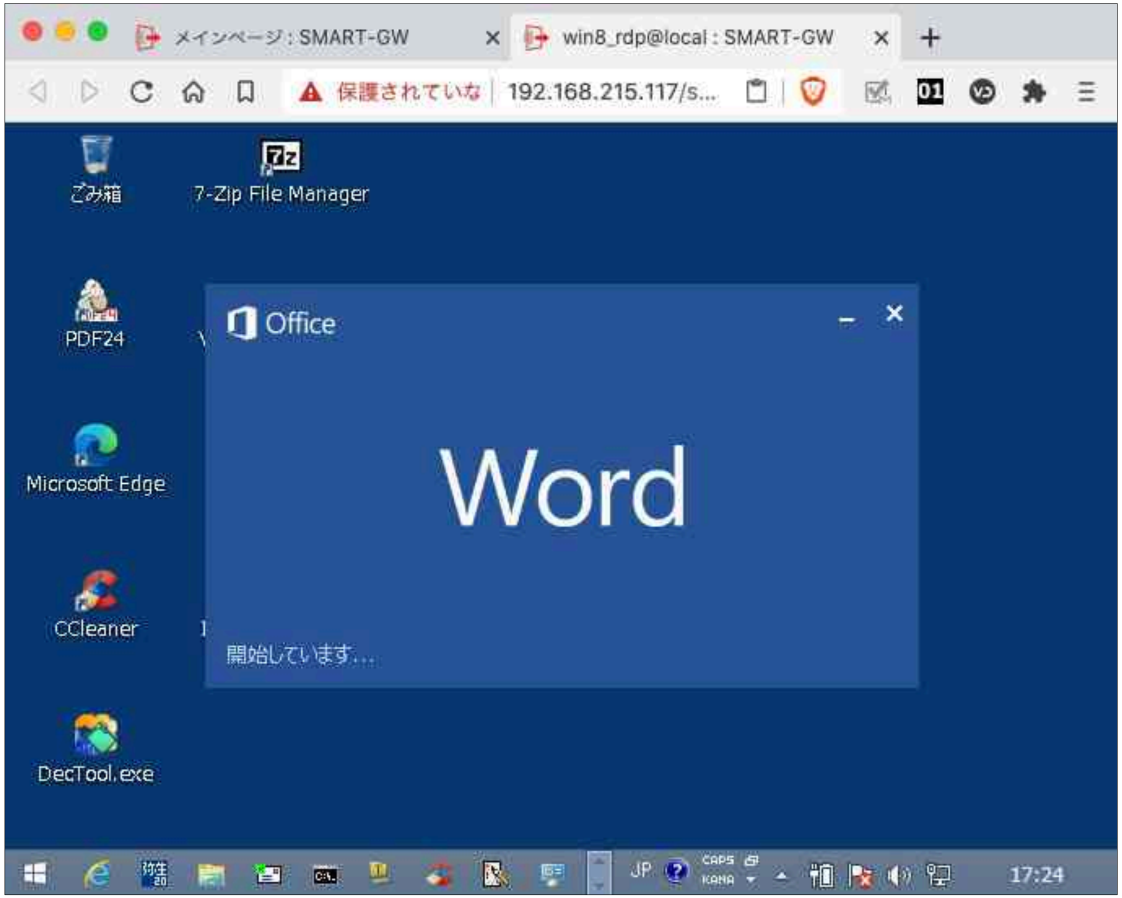
Results

SSH connection via Web UI

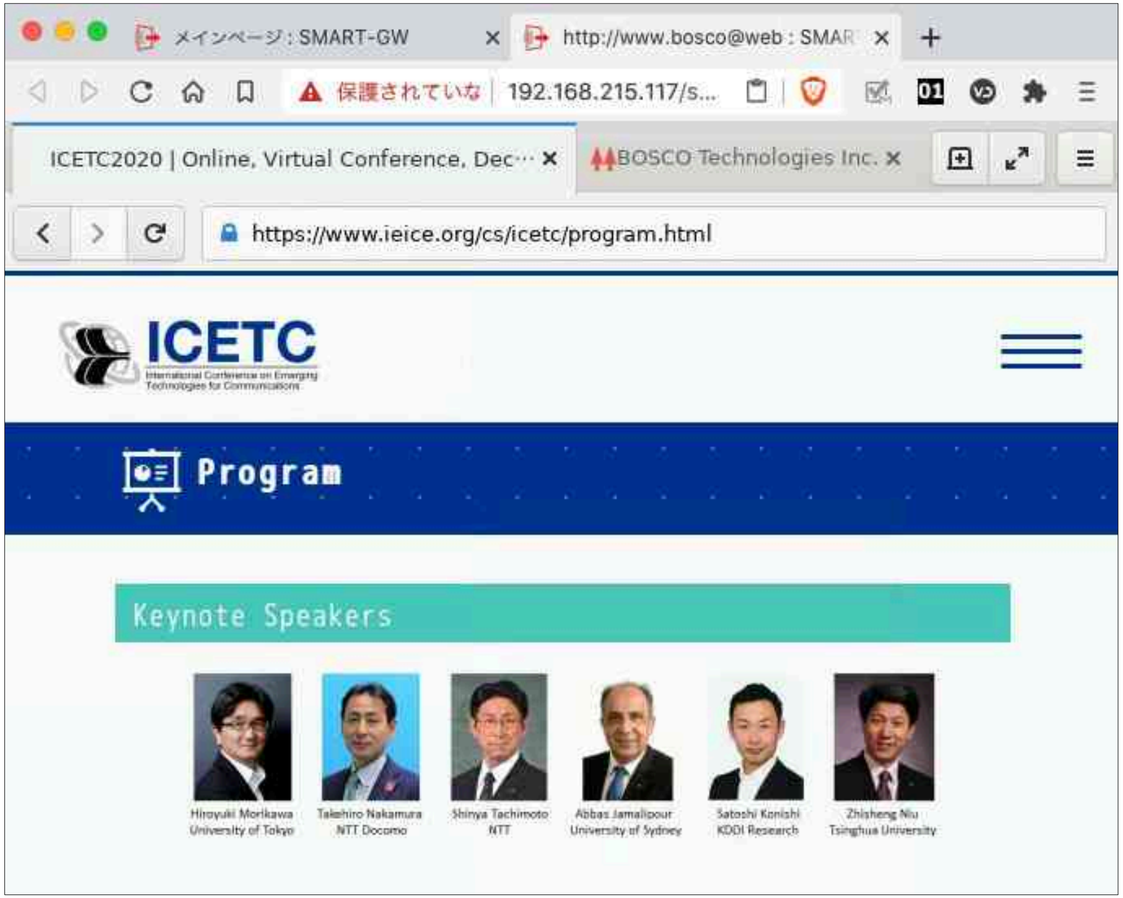


```
Last login: Thu Oct 15 17:17:34 2020 from 192.168.215.1
[root@dp117 ~]# ls
ICETC.secret  bin  smartgw-1.3.0-1.el7.x86_64.rpm
[root@dp117 ~]# rm ICETC.secret
Your input is dropped by command filter.

[root@dp117 ~]# echo "I can't input rm command although my acccount is root"
I can't input rm command although my acccount is root
[root@dp117 ~]# rm ICETC.secret
Your input is dropped by command filter.

[root@dp117 ~]# rm ICETC.secret
Your input is dropped by command filter.

[root@dp117 ~]# 
```

RDP connection via Web UI



HTTPS connection via Web UI



メインページ : SMART-GW

http://www.bosco@web : SMAR

保護されていな 192.168.215.117/s...

ICETC2020 | Online, Virtual Conference, Dec···

BOSCO Technologies Inc.

https://www.ieice.org/cs/icetc/program.html

ICETC

International Conference on Emerging Technologies for Communications

Program

Keynote Speakers

Hiroyuki Morikawa
University of Tokyo

Takehiro Nakamura
NTT Docomo

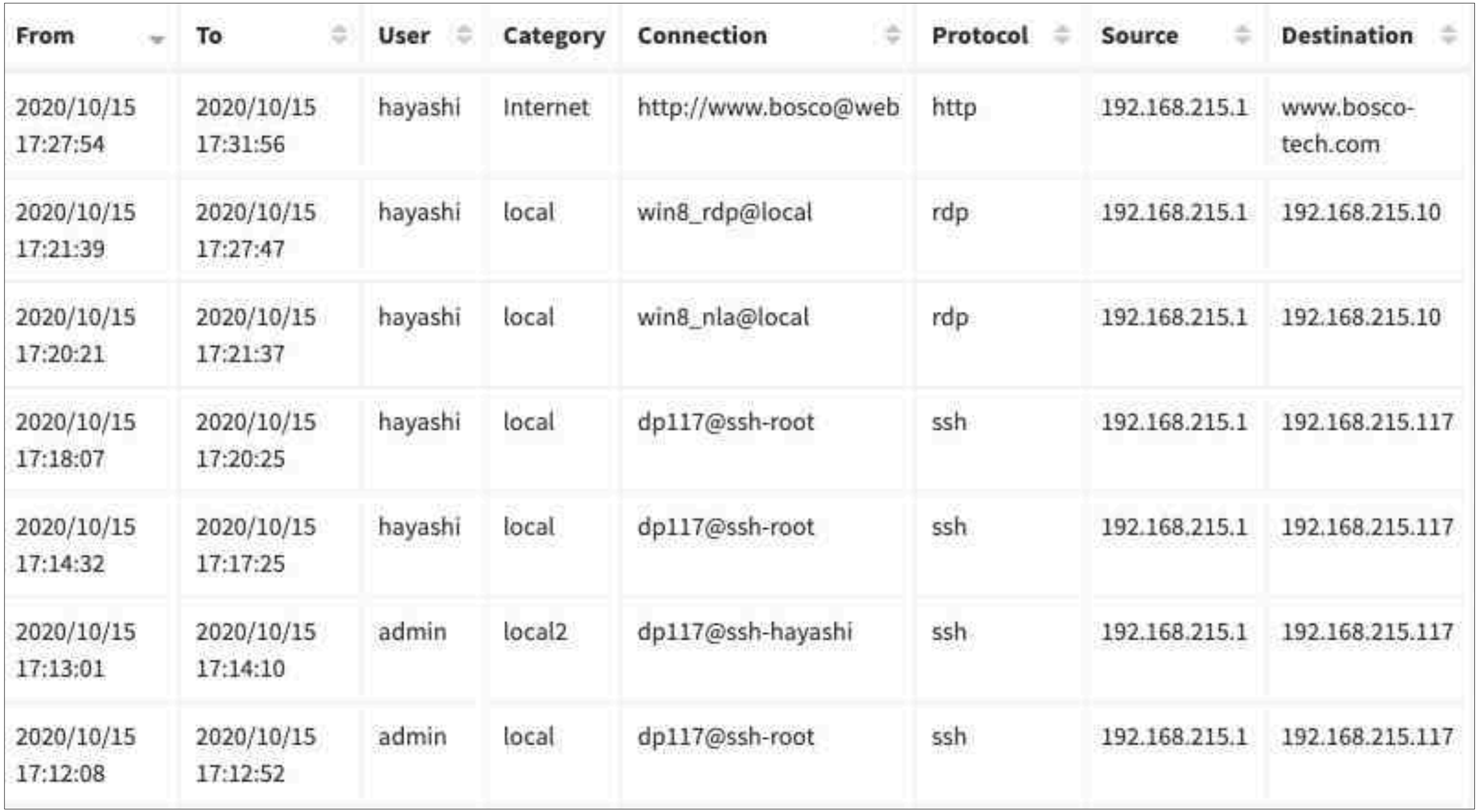
Shinya Tachimoto
NTT

Abbas Jamalipour
University of Sydney

Satoshi Konishi
KDDI Research

Zhisheng Niu
Tsinghua University

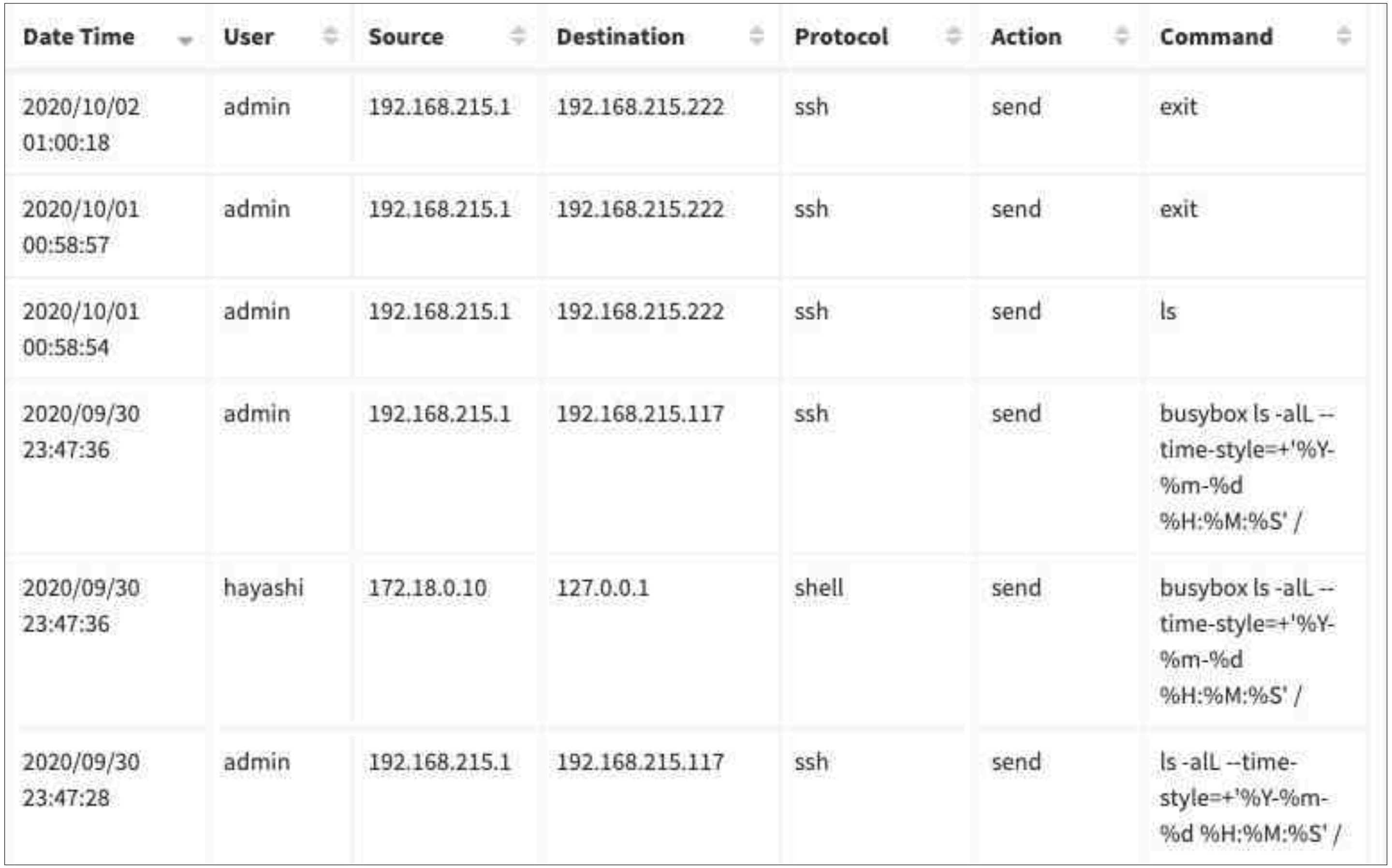
Session log



From	To	User	Category	Connection	Protocol	Source	Destination
2020/10/15 17:27:54	2020/10/15 17:31:56	hayashi	Internet	http://www.bosco@web	http	192.168.215.1	www.bosco-tech.com
2020/10/15 17:21:39	2020/10/15 17:27:47	hayashi	local	win8_rdp@local	rdp	192.168.215.1	192.168.215.10
2020/10/15 17:20:21	2020/10/15 17:21:37	hayashi	local	win8_nla@local	rdp	192.168.215.1	192.168.215.10
2020/10/15 17:18:07	2020/10/15 17:20:25	hayashi	local	dp117@ssh-root	ssh	192.168.215.1	192.168.215.117
2020/10/15 17:14:32	2020/10/15 17:17:25	hayashi	local	dp117@ssh-root	ssh	192.168.215.1	192.168.215.117
2020/10/15 17:13:01	2020/10/15 17:14:10	admin	local2	dp117@ssh-hayashi	ssh	192.168.215.1	192.168.215.117
2020/10/15 17:12:08	2020/10/15 17:12:52	admin	local	dp117@ssh-root	ssh	192.168.215.1	192.168.215.117

IB3-2

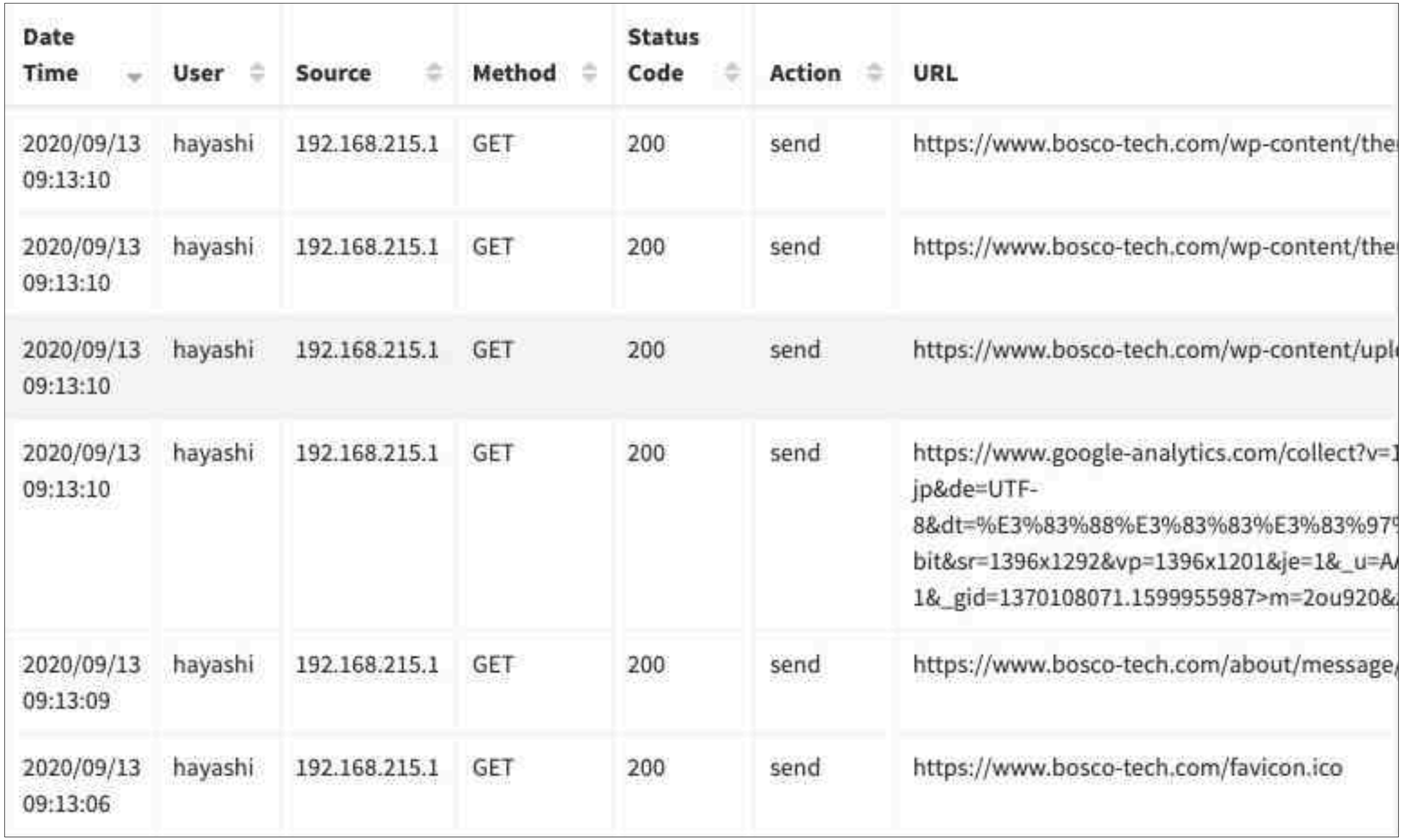
Command log



Date Time	User	Source	Destination	Protocol	Action	Command
2020/10/02 01:00:18	admin	192.168.215.1	192.168.215.222	ssh	send	exit
2020/10/01 00:58:57	admin	192.168.215.1	192.168.215.222	ssh	send	exit
2020/10/01 00:58:54	admin	192.168.215.1	192.168.215.222	ssh	send	ls
2020/09/30 23:47:36	admin	192.168.215.1	192.168.215.117	ssh	send	busybox ls -alL --time-style=+'%Y-%m-%d %H:%M:%S' /
2020/09/30 23:47:36	hayashi	172.18.0.10	127.0.0.1	shell	send	busybox ls -alL --time-style=+'%Y-%m-%d %H:%M:%S' /
2020/09/30 23:47:28	admin	192.168.215.1	192.168.215.117	ssh	send	ls -alL --time-style=+'%Y-%m-%d %H:%M:%S' /

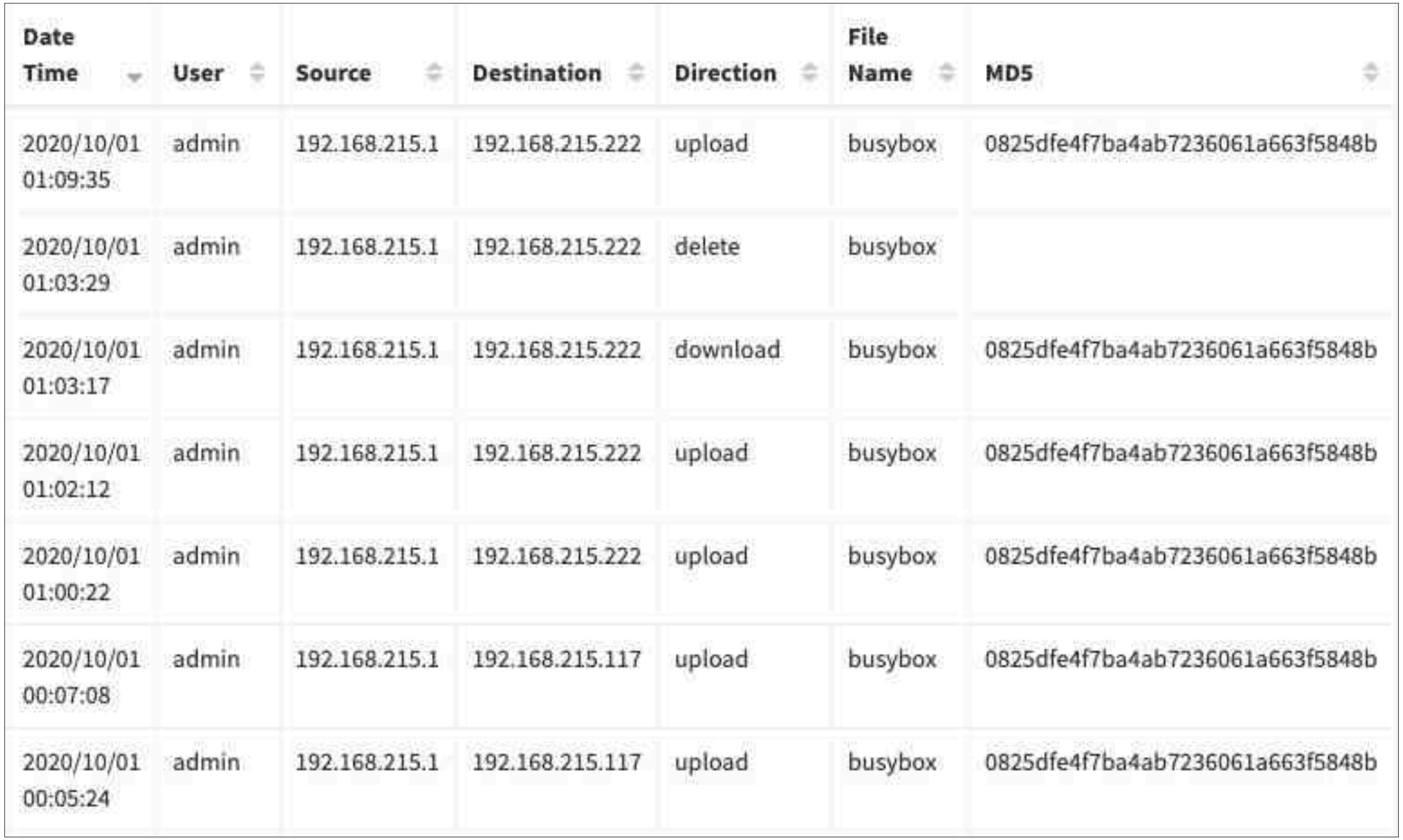
IB3-2

URL request log



Date Time	User	Source	Method	Status Code	Action	URL
2020/09/13 09:13:10	hayashi	192.168.215.1	GET	200	send	https://www.bosco-tech.com/wp-content/the
2020/09/13 09:13:10	hayashi	192.168.215.1	GET	200	send	https://www.bosco-tech.com/wp-content/the
2020/09/13 09:13:10	hayashi	192.168.215.1	GET	200	send	https://www.bosco-tech.com/wp-content/upl
2020/09/13 09:13:10	hayashi	192.168.215.1	GET	200	send	https://www.google-analytics.com/collect?v=1 jp&de=UTF-8&dt=%E3%83%88%E3%83%83%E3%83%97 bit&sr=1396x1292&vp=1396x1201&je=1&_u=A 1&_gid=1370108071.1599955987&gtm=2ou920&
2020/09/13 09:13:09	hayashi	192.168.215.1	GET	200	send	https://www.bosco-tech.com/about/message
2020/09/13 09:13:06	hayashi	192.168.215.1	GET	200	send	https://www.bosco-tech.com/favicon.ico

File transfer log



Date Time	User	Source	Destination	Direction	File Name	MD5
2020/10/01 01:09:35	admin	192.168.215.1	192.168.215.222	upload	busybox	0825dfe4f7ba4ab7236061a663f5848b
2020/10/01 01:03:29	admin	192.168.215.1	192.168.215.222	delete	busybox	
2020/10/01 01:03:17	admin	192.168.215.1	192.168.215.222	download	busybox	0825dfe4f7ba4ab7236061a663f5848b
2020/10/01 01:02:12	admin	192.168.215.1	192.168.215.222	upload	busybox	0825dfe4f7ba4ab7236061a663f5848b
2020/10/01 01:00:22	admin	192.168.215.1	192.168.215.222	upload	busybox	0825dfe4f7ba4ab7236061a663f5848b
2020/10/01 00:07:08	admin	192.168.215.1	192.168.215.117	upload	busybox	0825dfe4f7ba4ab7236061a663f5848b
2020/10/01 00:05:24	admin	192.168.215.1	192.168.215.117	upload	busybox	0825dfe4f7ba4ab7236061a663f5848b

operation correctness or illegal / irregular from the session logs

1. Aggregate the number of occurrences per command
2. Apply a heuristic algorithm with log (count +1) to the number of appearances

the value of p is less than 1%

		Evaluation data		
		User A	User B	User C
Training data	User A	0.9998	0.0082	0.0000
	User B	0.0000	0.4980	0.0000
	User C	0.0000	0.0000	0.9503

Conclusion

- client-less and centralized connection management against ICT infrastructure
  -> protocol-based connection integration system to manage the infra.
- each logging feature records user behavior in detailed level
  -> distinguish normal operation from operation log
- Feasible in a commercial environment with 100,000 (capability 400,000)
  -> can handle 10,000 SSH, RDP and HTTPS sessions at the same time

IB3-2

BOSCO Technologies