Feasibility Verification of Access Control System for Telecommuting by Users Reliability Calculation

Atsushi SHINODA[1], Hirokazu HASEGAWA[2], Yukiko YAMAGUCHI[3], Hajime SHIMADA[3], Hiroki TAKAKURA[2]

[1]Graduate School of Informatics, Nagoya University, Japan
mail: shinoda@net.itc.nagoya-u.ac.jp

[2]Center for Strategic Cyber Resilience R&D,
National Institute of Informatics, Japan

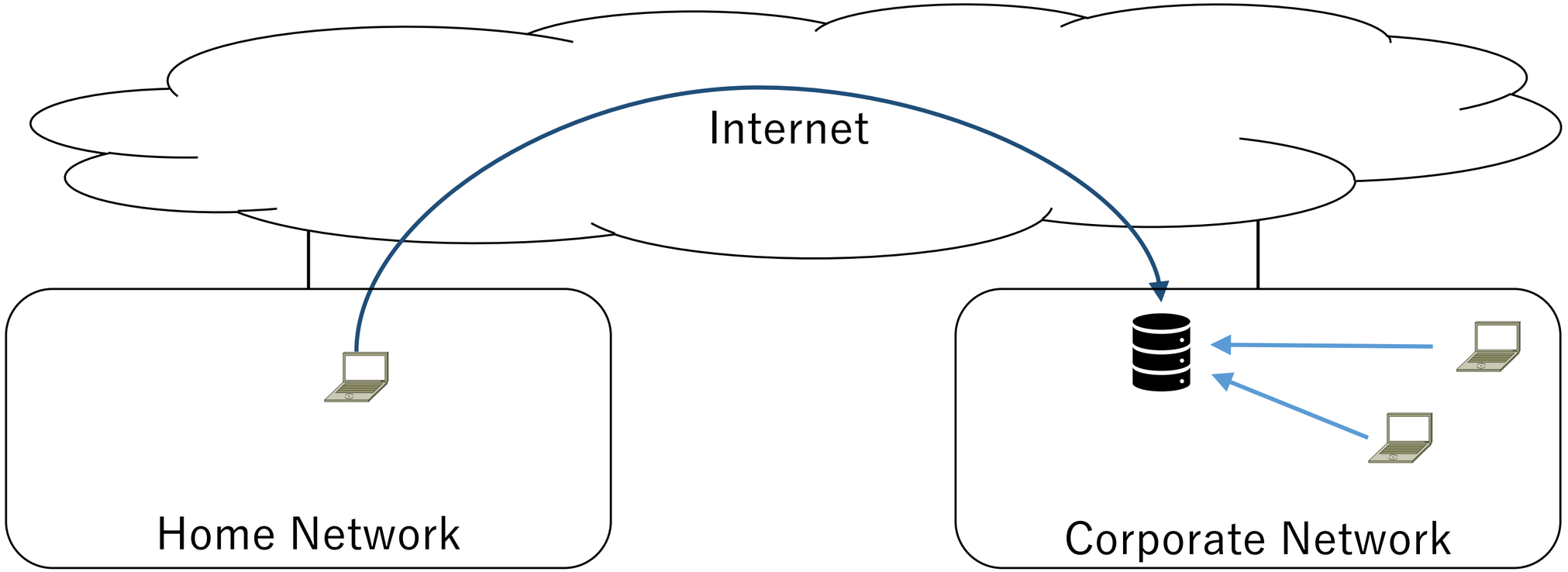
[3]Information Technology Center, Nagoya University, Japan

Presenter Self Introduction

- Name: Atsushi SHINODA
- Affiliation:
  - 2nd year master's student at Nagoya University in Japan,
  - Graduate School of Informatics,
  - Department of Computing and Software Systems,
  - Shimada laboratory
- Research Topic:
  - Network Security

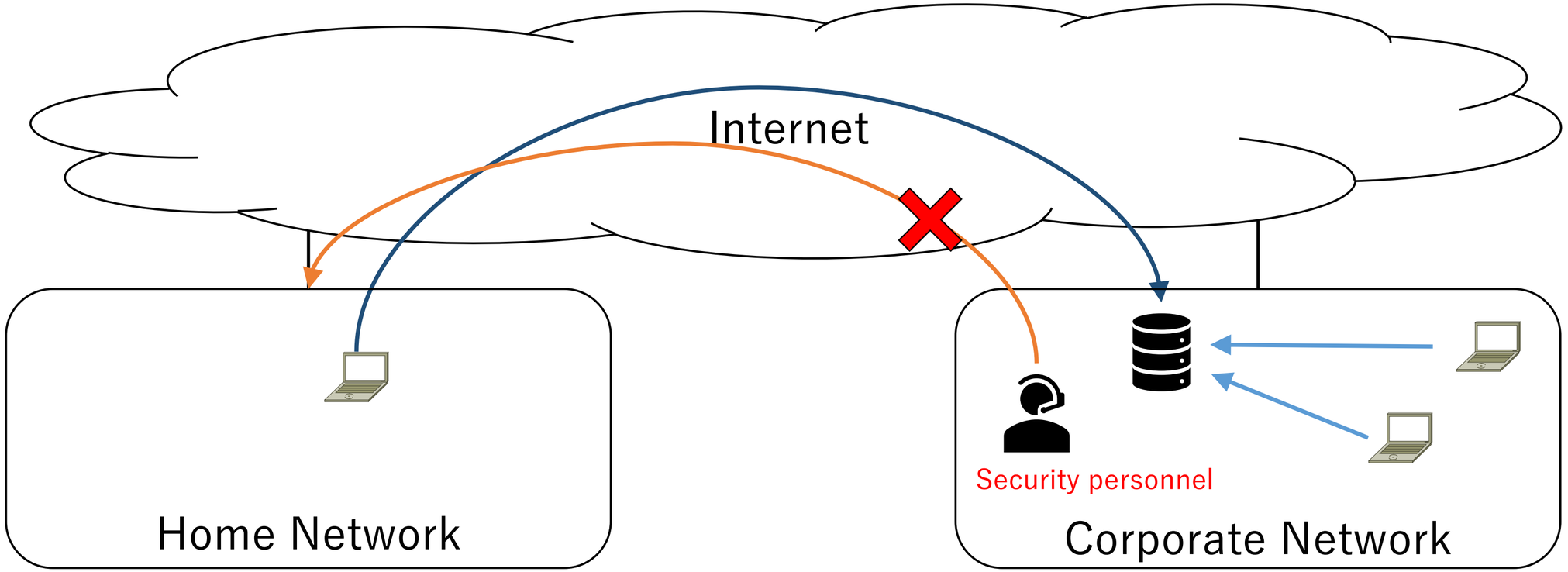
Background: Increasing Telecommuting

- Increasing Telecommuting
- User can connect remote terminals to corporate-network



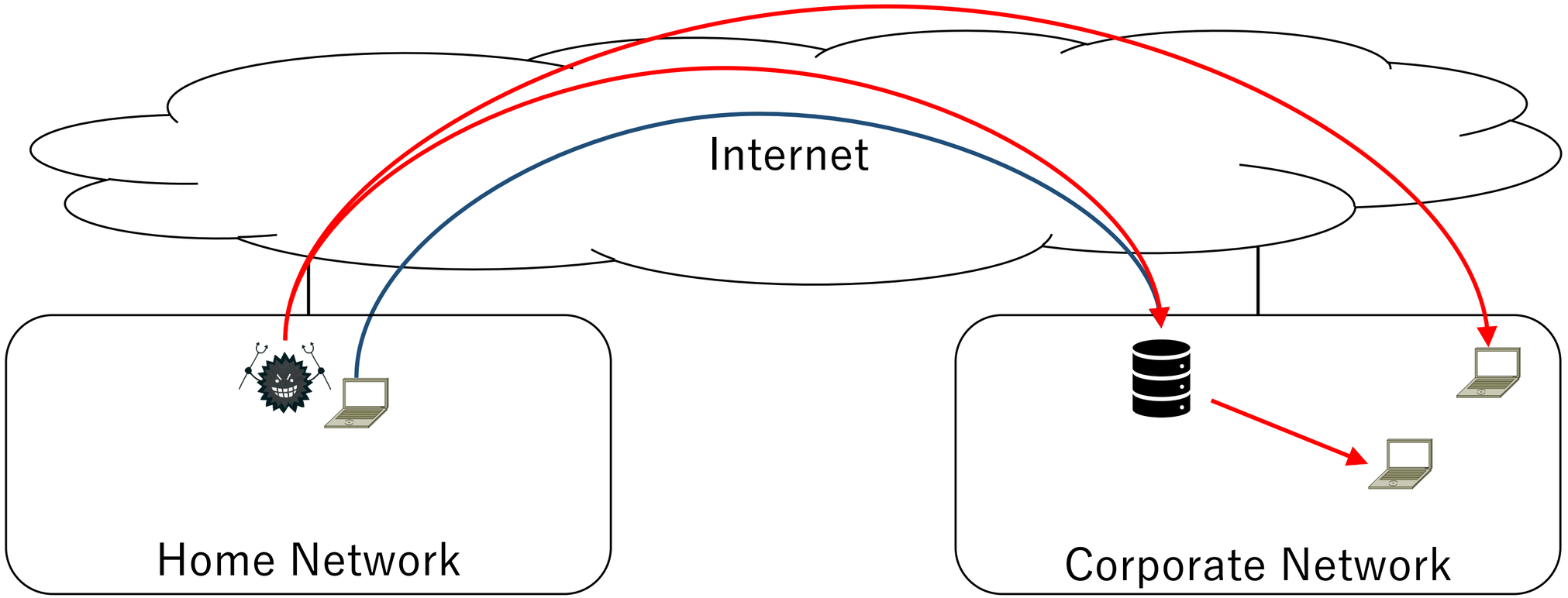
Background: Increasing Telecommuting

- Corporate security personnel cannot manage or supervise
  - The home network or terminal (remotely connecting to cooperate network)
  - Making situation dangerous



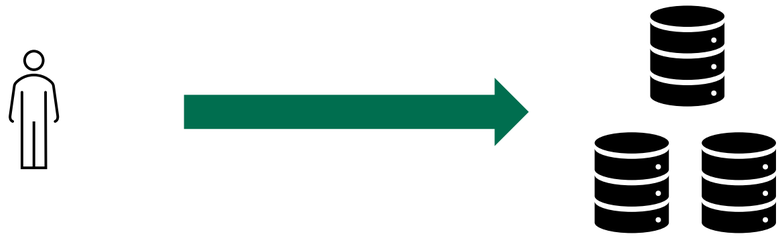
Background: Risks of Telecommuting

- Corporate networks are more dangerous than ever
  - Telecommuting requires further security enhancements
  - Often the security enhancements decrease business efficiency



Previous Research: Systems for Enhancing Network Security

- Access control system for telecommuting communications based on user reliability [1]



Highly reliable users — Many accessible resources

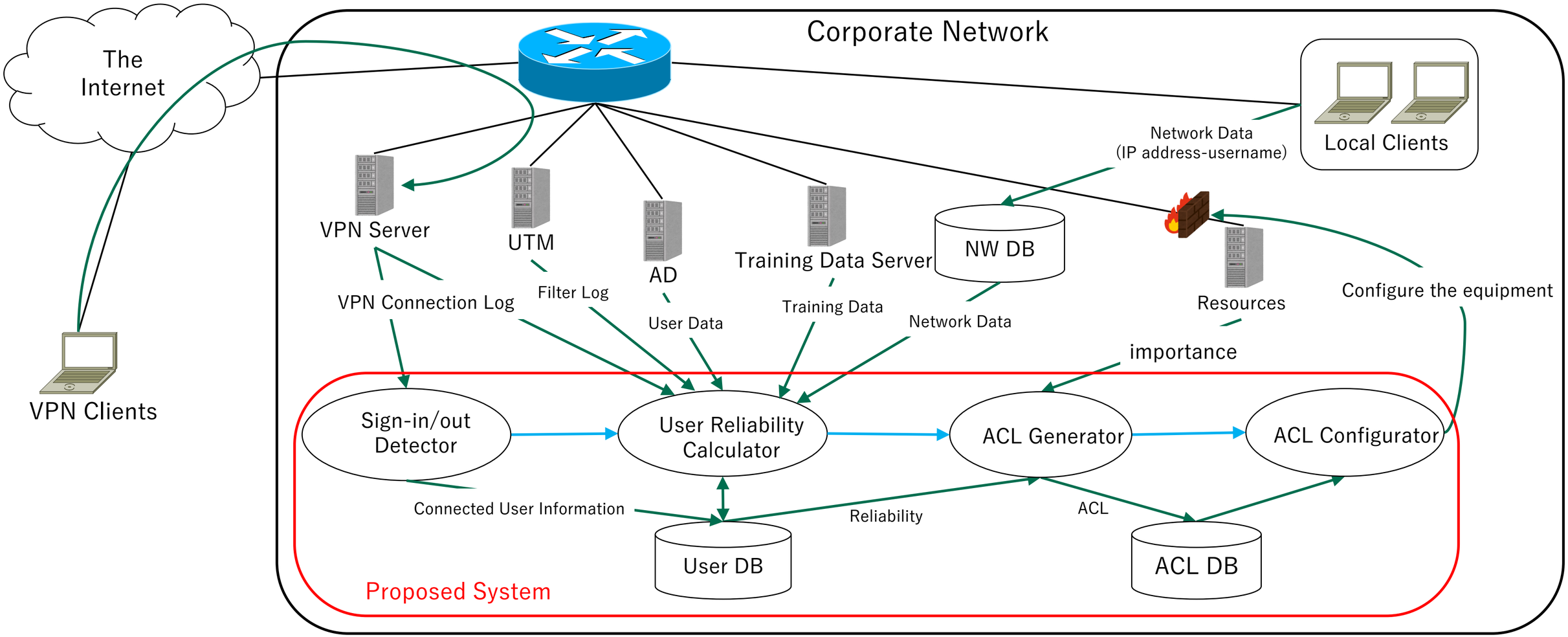
Low reliable users — Less accessible resources

[1] Hasegawa et. al., “A Dynamic Access Control System based on Situations of Users,” International Conference on Information Systems Security and Privacy 2021.

Previous Research: Systems for Enhancing Network Security

- Access control based on user reliability and resource importance by users connecting VPN.
  - User Reliability
    - Indicator based on users' daily behavior regarding information security
      - Progress rate of security training / Security test scores
      - History of security incident
      - Result of security surprise test
      - Result of URL filtering detection etc.
  - Resource Importance
    - Indicator based on the impact of a data breach/loss
      - Customer privacy information -> High importance etc.

Previous Research: Overview of the System

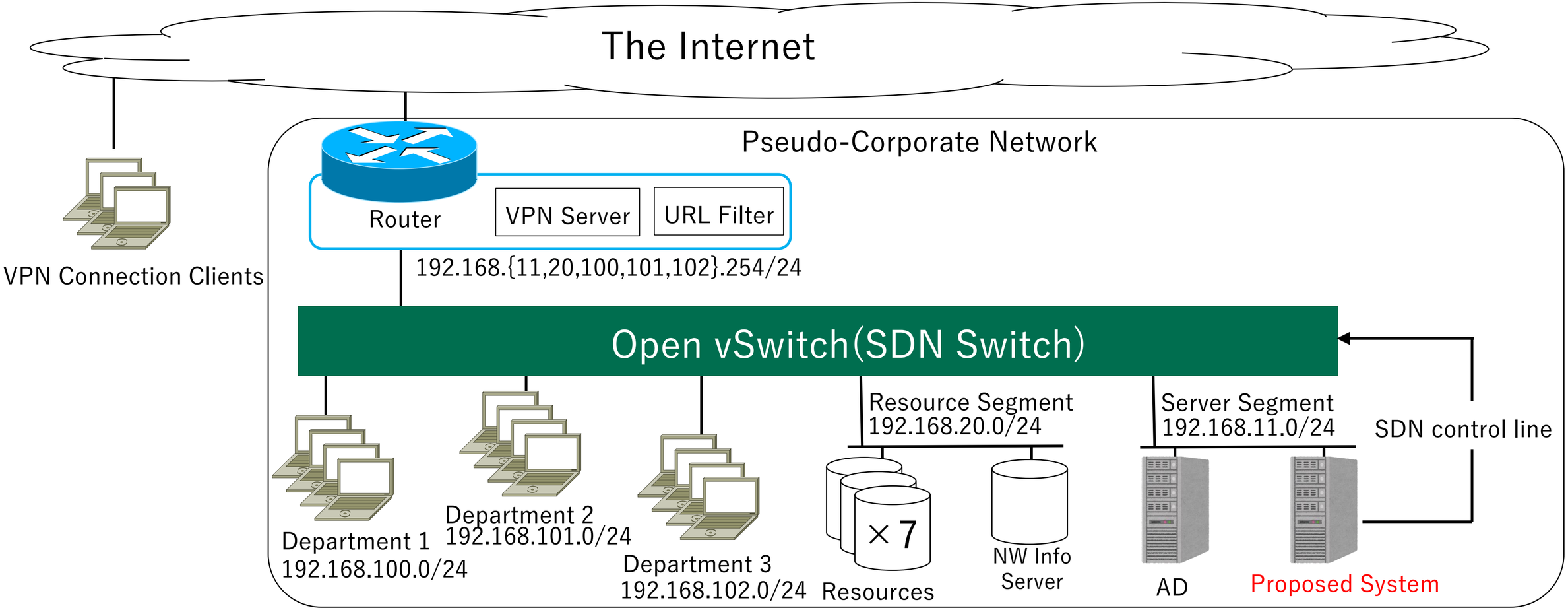


名古屋大学 NAGOYA UNIVERSITY

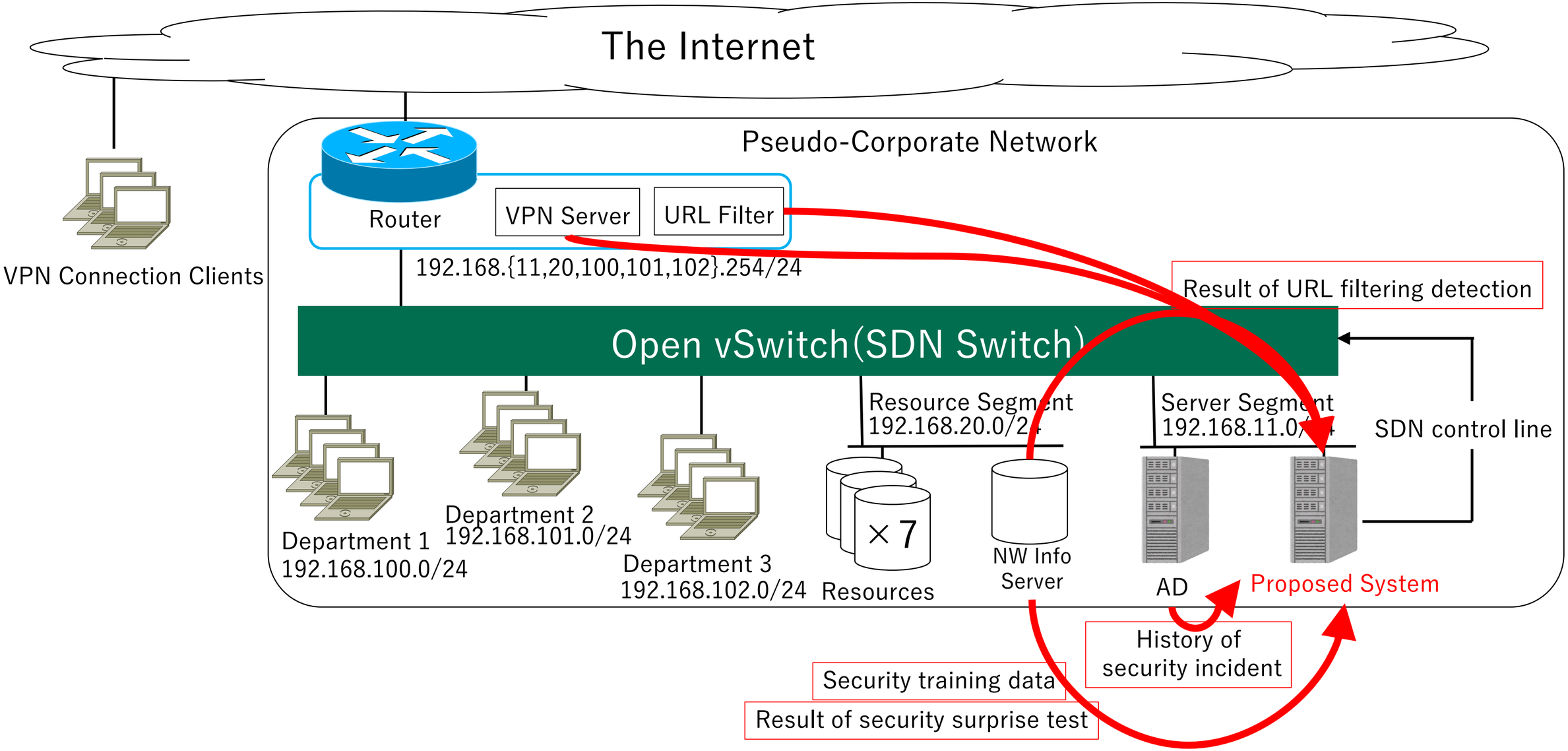
This Research: Feasibility Verification of the System

- Implement the system on a pseudo-corporate network and calculate user reliability has not been verified
- The system performance is important
  - Especially, when the VPN connected, followings are started
    - Collecting data for user reliability indicator
    - Calculating user reliability
    - Conduct access control by SDN

Implementation of the Proposed System



Collecting Data for User Reliability Indicators



名古屋大学 NAGOYA UNIVERSITY

Calculating User Reliability and Conducting Access Control

In User Reliability Calculator,

- Standardizing each user reliability indicator
- Calculating user reliability from average of the indicators with weighting

In ACL Generator,

- Compare each user's reliability with all resource importance
  - IF (user.reliability – resource.importance > threshold), then
    - access_rule = ALLOW; (Note: Default access rule is DENY)

In ACL Configurator,

- Setting access rules by SDN

Experiment

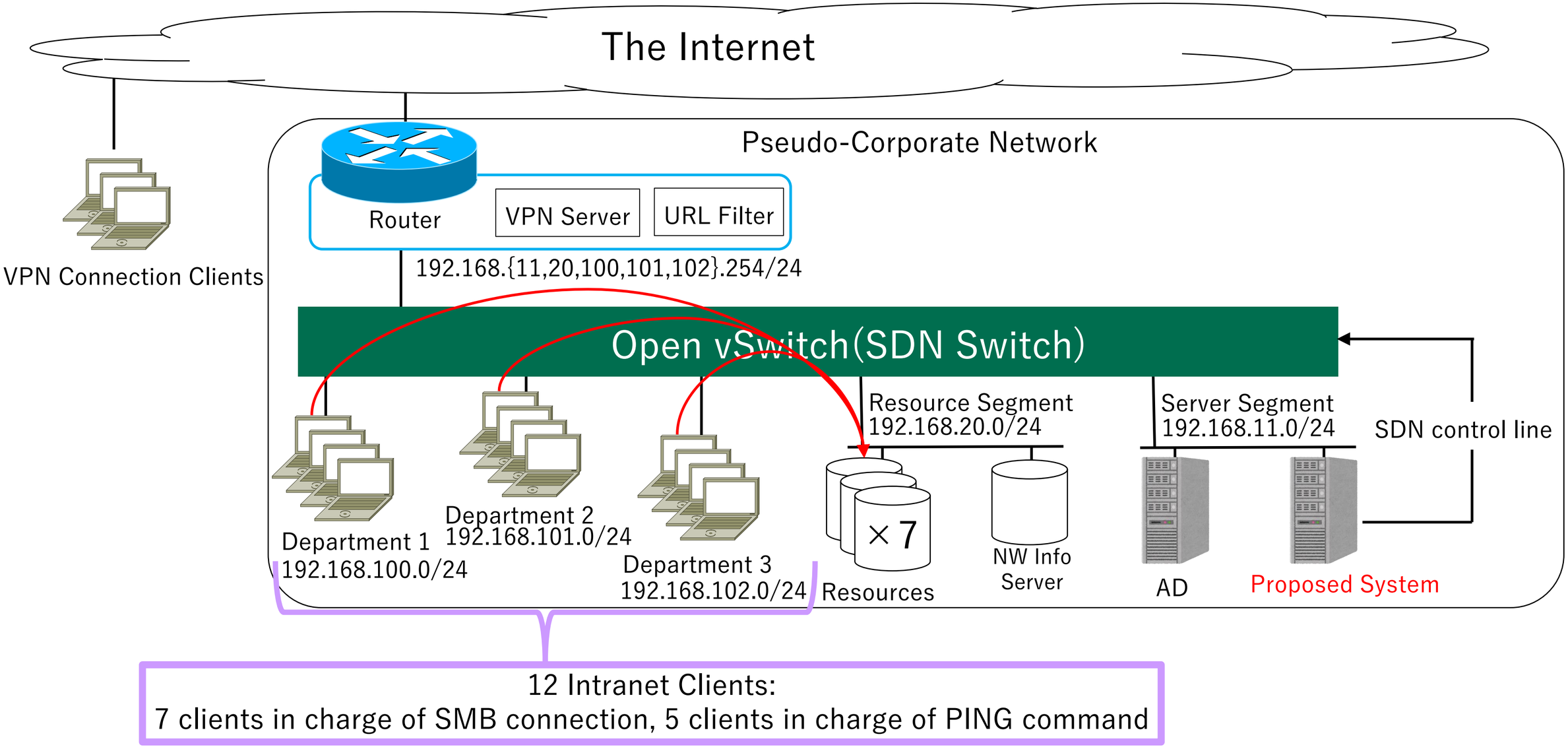
Verification experiments for the proposed system

- Conducted on a pseudo-corporate network

Measuring VPN and SMB connection waiting time

- 2 patterns of VPN multi connection
  - **Sequential** : increasing the number of VPN connecting terminal one by one
  - **Simultaneous** : connecting VPN at same time for all terminals
- 2 patterns of load traffic at network
  - **None** : there is no traffic between internal client to Resources
  - **Heavy** : large traffic by PING,SMB between internal client to Resources

Experimental Network (Intranet Traffic: **Heavy**)



12 Intranet Clients:
7 clients in charge of SMB connection, 5 clients in charge of PING command

名古屋大学 NAGOYA UNIVERSITY

Experimental Results

Traffic Load	None				Heavy			
Multi Type	Sequential		Simultaneous		Sequential		Simultaneous	
Protocol	VPN	SMB	VPN	SMB	VPN	SMB	VPN	SMB
Client 0	0.681	3.093	0.718	6.460	0.723	17.192	1.044	28.613
Client 1	0.657	3.311	0.654	6.616	0.555	17.211	0.668	28.522
Client 2	0.797	2.970	0.685	6.535	0.654	17.342	0.668	28.814
Client 3	0.598	3.292	0.594	6.631	0.591	17.502	0.576	28.544
Client 4	0.664	3.269	0.675	6.640	0.601	16.989	0.680	28.651
Client 5	0.645	3.233	0.660	6.630	0.584	17.241	0.666	28.512
Client 6	0.796	2.943	0.760	6.358	0.696	17.087	0.695	28.554
Client 7	0.669	3.268	0.622	6.677	0.634	17.398	0.622	28.647
Client 8	0.330	3.367	0.312	3.212	0.297	17.086	0.317	16.549
Client 9	0.782	2.946	0.690	6.416	0.616	17.120	0.710	28.639
Client 10	0.360	3.210	0.326	3.207	0.331	17.106	0.337	16.773
Client 11	0.622	3.332	0.704	6.211	0.581	17.291	0.679	28.641
Average	0.634	3.186	0.617	5.966	0.572	17.214	0.639	26.622

Experimental Results

Traffic Load	None				Heavy			
Multi Type	Sequential		Simultaneous		Sequential		Simultaneous	
Protocol	VPN	SMB	VPN	SMB	VPN	SMB	VPN	SMB
Client 0	0.681	3.093	0.718	6.460	0.723	17.192	1.044	28.613
Client 1	0.657	3.311	0.654	6.616	0.555	17.211	0.668	28.522
Client 2	0.797	2.970	0.685	6.535	0.654	17.342	0.668	28.814
Client 3	0.598	3.292	0.594	6.631	0.591	17.502	0.576	28.544
Client 4	0.664	3.269	0.675	6.640	0.601	16.989	0.680	28.651
Client 5	0.645	3.233	0.660	6.630	0.584	17.241	0.666	28.512
Client 6	0.796	2.943	0.760	6.358	0.696	17.087	0.695	28.554
Client 7	0.669	3.268	0.622	6.677	0.634	17.398	0.622	28.647
Client 8	0.330	3.367	0.312	3.212	0.297	17.086	0.317	16.549
Client 9	0.782	2.946	0.690	6.416	0.616	17.120	0.710	28.639
Client 10	0.360	3.210	0.326	3.207	0.331	17.106	0.337	16.773
Client 11	0.622	3.332	0.704	6.211	0.581	17.291	0.679	28.641
Average	0.634	3.186	0.617	5.966	0.572	**17.214**	0.639	**26.622**

Considerations

- In the **Sequential**,
  - The difference of SMB time was no more than 1 second.
  - The SMB connection time did not depend on the order of VPN connections.
- In the **Simultaneous**,
  - Some clients (Client: 8, 10) took the same time as in the **Sequential**.
  - However, other clients took twice as long.
    - Due to the processing of simultaneous VPN connection
- In **Heavy** load,
  - There are significant delay about 17s in **Sequential** and 26s in **Simultaneous**.
- For the intranet traffic,
  - The proposed system has almost no effect both **Sequential** and **Simultaneous**.

Conclusion

Verify the feasibility of the proposed system

- Implementation of access control system based on User Reliability
- Calculating user reliability and conduct access control
- Delay can be acceptable except for excessive intranet traffic

Future Works

- The exact validation of user reliability calculation has not been carried out
  - Reliability indicators should be based on as many indicators as possible
- Impact verification for larger networks
  - Increaseing in the number of objects under management may affect delay