A Dynamic Access Control System based on Situations of Users

Hirokazu Hasegawa[1] and Hiroki Takakura[2]
[1]*Information Security Office, Nagoya University, Nagoya, Japan*
[2]*Center for Cybersecurity Research and Development, National Institute of Informatics, Tokyo, Japan*

Keywords: Cyber Security, Targeted Attacks, Network Separation, Access Control, Telecommuting, Working from Home.

Abstract: Recently, cyber attacks have been sophisticated and cause serious damages. As one of the solutions for mitigating the damages, the network separation and fine granularity of access controls are effective against attacks. However, the COVID-19 changes human work style, and telecommuting comes to be generally. It may give many chances to attackers for invading the organization's internal network by infecting user's vulnerable home terminals, which are out of control by the organization. To ensure the security of organizations, we propose a dynamic access control system based on the situations of users. The system evaluates communications based on the user's risk and the importance of resources in destination terminals. When a user connects to the organization network from the outside, the system dynamically changes the access controls according to the evaluation results. The such situation requires stricter access controls than usual ones. For example, the communication by the high-risk user and the communication to servers storing important resources are restricted. By applying such dynamic access controls, the system enables us to ensure our network security with maintaining the convenience of users telecommuting.

1 INTRODUCTION

Recently, cyber attacks have been so sophisticated that it is difficult to protect our networks completely. Especially, targeted attacks, which is one of the cyber attacks, cause serious damages. In the case of targeted attacks that target specific governments or companies and so on, its purpose is information theft or sabotage activities. To achieve the purpose, attackers investigate targets thoroughly in advance, and they prepare dedicated malwares for the targets. Such malwares slip through our traditional security measures for preventing the intrusion of malwares.

Because of such a situation, recent countermeasures has focused on the mitigation of damages by the attacks after the intrusion of malwares(Cichonski et al., 2012). A separated network is one of the most effective countermeasures for targeted attacks(Information-technology Promotion Agency, 2011). The separated network is a network design to separate the internal network into several segments and conduct fine access controls among separated segments. In the separated network, access controls among segments can restrain unintended communications by malwares. In addition, we can minimize the impact of the attack when we detect malwares because we can isolate infected hosts quickly. By applying the separated network, we can effectively prevent attacks regardless of the types of malwares. Recently, a lot of organizations apply such network design for security measures, and also the Cybersecurity and Infrastructure Security Agency recommends network segmentation and unnecessary communications limitation(Cybersecurity and Infrastructure Security Agency (CISA), 2020).

The separated network is an effective measure, however, it is heavy burden for network administrators to construct such network construction. To solve such a problem, we have proposed several systems to support the construction of the separated network. Our previous system judges the necessity of communications in the organization network based on the user's access authority to files stored in servers. If a user has no access authority against all files in the server, the system prohibits communication between the server and the user's equipment. Furthermore, we have also proposed a system that judges the necessity of communication based on the analysis of captured packets. Our previous systems make it possible to construct a separated network easily.

However, in 2020, the COVID-19 makes the change to human's work style. Almost all organi-

Hasegawa, H. and Takakura, H.
A Dynamic Access Control System based on Situations of Users.
DOI: 10.5220/0010327406530660
In *Proceedings of the 7th International Conference on Information Systems Security and Privacy (ICISSP 2021)*, pages 653-660
ISBN: 978-989-758-491-6

zations all over the world adopted telecommuting to reduce the risk of employee virus infection. Organizations were forced to construct the environments of the telecommuting quickly, therefore, many organizations adopted stopgap ways, e.g., employees are forced to connect their organization's network via VPN.. In such cases, the security level may reduce even if the separated network is constructed because the client terminals running the remote desktop may not secure.

To ensure the security of the organization network, we have to dynamically change the access controls based on the situation of the users not only on the necessity of the communication. In other words, we need to control the intensity of the access controls based on the situation. For example, we should restrict the communication by a user according to the situation of the user even if the communication is judged as necessary and permitted in the ordinary situation. However, it is difficult for network administrators to conduct such dynamic access controls.

Therefore, this paper proposes a dynamic access control system based on the situation of users. The system limits the communication according to the risk of a user and the importance of accessible resources. The system makes us possible to control access corresponding to various situations of the organization's employees and maintain the security of the networks even if the way of working changes.

The rest of this paper is organized as follows: In Section II, we introduce related works. Section III presents the proposal system. In Section IV, we discuss the effectiveness of our proposed system. Finally, we conclude this paper in Section V.

2 RELATED WORKS

Because the separated network is effective in suppressing malware activities, many research works have done to construct separated networks.

Watanabe et al. proposed a VLAN configuration method(Watanabe et al., 2005). In this method, they focused on the frequency of communications. When a certain amount of traffic among terminals is observed, such terminals are coordinated into the same VLAN.

Nayak et al. proposed Resonance(Nayak et al., 2009) that is a framework of dynamic access controls based on the security policy. It also based on real-time monitoring, and it can isolate suspicious terminals.

As the system proposed by Tian et al. (Tian et al., 2019), Jinjing can read the network operator's intention and update network ACL configuration automatically.

In our previous work, we proposed the system supporting the construction of the separated network. The system refers to the employees' human resource information and their access authorities to resources in the organization, and it generates access controls based on the collected information automatically. Moreover, to increase the accuracy of the access control, the system also refers to the network traffic to judges the necessity of the communication.

However, these researches focus on preventing unnecessary or malicious communications, therefore, the communication judged as necessary is always permitted in the network. For example, although our previous system can follow the personnel changes or changes of access authorities and can dynamically update the access controls because it automatically generates access controls based on the collected information, the system always permits necessary communication.

On the other hand, as described in Section 1, we need flexible access controls according to the user's situation. There are many researches of constructing secure network for the Internet of Things (IoT) (Atlam et al., 2017)(Rath and Colin, 2017). The recent network situation, in which telecommuting forces almost every user to connect to the resources from the external network, is an unexpected structure in conventional networks. As with the IoT network, we need a new construction method of the secure network from the different viewpoint of conventional networks.

In recent years, methods of network configuration have been improving. As one of such methods, Software Defined Networking (SDN) is often studied. As Nguyen and Kim proposed(Nguyen and Kim, 2016), we can flexibly manage a large scale network, e.g., campus networks, by using SDN technics. By using such methods, we can configure the network flexibly. Therefore, we propose the method to judges the permission of users according to the situation.

3 PROPOSED SYSTEM

In this paper, we propose a dynamic access control system based on the situation of users. When a user connects to the internal network from the outside network via the internet, the system dynamically assigns the ACL different from the usual ACL.

3.1 Assumption

First of all, the proposed system assumes a network that is separated into several segments and managed fine access controls. For example, we assume the organization network constructed by our previous system, and all clients in the network can conduct only necessary communication.

As similar to the conventional networks, there are several ways for users to connect the resources on the separated network from the outside of the organization network. As one of the simple ways, for example, a user connects to the organization's internal network via VPN and uses his/her own client in the office by the remote desktop applications, e.g., Microsoft Remote Desktop. Otherwise, a user uses the terminal in the home by directly connecting to the organization network via VPN.

Because this paper focuses on the precise access control supposing telecommuting, the control to users at an office is out of scope. Thus, to simplify the discussion, it is assumed that all users connect to their office PCs by the remote desktop applications via VPN, and our system can identify their situation based on access information of VPN servers.

3.2 System Overview

The proposed system classifies the usually permitted communications concerning the connected user into three types shown below by evaluating the security risk of communication. According to the classified result, the system generates the new ACL automatically.

- Conventional
  Communication permitted like a user at the office.
- Temporal
  Communication permitted within a certain period. The period is automatically calculated by the proposed system.
- Restriction
  Communication permitted only when a responsible person permits.

3.2.1 Evaluation of Communications

The system evaluates the security risk of each communication usually permitted to conduct by a user and decides its type based on the evaluation results. The system defines the RC_c as the risk of communication c. To evaluate RC_c, the system applies two factors, i.e., risk of users and importance of resources.

The first factor is the risk of users because a security incident is sometimes caused by human error. To calculate the risk of users, the system uses the mail quarantine log and the security log. The mail quarantine log indicates the volume of deleted malicious messages. If the volume of deleted malicious messages against the user is high, the user has a high risk of malware infection. The security log includes various logs concerning the user. In this paper, we take the incident logs that the user caused, malicious activities, and the learning state of the information security seminar. However, the system can apply various types of information to calculate the risk depending on the actual environment. If a user caused a security incident previously, the system considers the user as high risk. Similarly, the malicious activity of the user, e.g., he/she neglects to perform security updates, is taken into account in risk calculation. In addition, the system checks the learning state of employee education about information security by the organization, and the system treats the user as high risk if the user has not taken the education.

The system defines RU_u as the risk of the user u. In addition, the system uses M_1 as the parameter for the maximum value of RU_u. To simplify the discussion of the paper, we set 100 to M_1. In this paper, we use the mail quarantine log, the incident log, the malicious activities, and the learning state, and we call each of these is a user concerning content.

To calculate the RU_u, the system calculates that 100 (the parameter M_1) divides by the total number of the user concerning contents in advance, and it treats the calculated number as the maximum value of the risk of each user concerning contents. In this paper, we use four user concerning contents, therefore, the maximum value of each risk comes to 25. Then, the system calculates each risk of the user concerning contents.

As the risk of malicious messages, the system applies the ratio of malicious messages to total receiving messages. Therefore, the system obtains the risk of malicious messages by the multiplication of the ratio of malicious messages and 25 (the maximum value of the risk).

Then, as the calculation of risk of the incident log which the user caused, the system checks all incident logs. Generally, the incident log includes the contents of the incident and its severity. According to the level of severity, the system calculates the risk of incidents caused by the user. The system divides the maximum value of the risk of a user concerning content by the total number of such levels. Then, by multiplication of the calculated number and the level of the severity, the system calculates the risk value of the incidents. For example, as shown in Figure 1, when an organization defines the 4 levels of severity, the system calculates the sum of 1, 2, 3, and 4, and divides 25 by it.

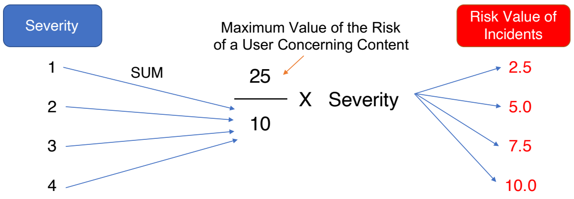


Figure 1: Calculation example of the risk of incidents.

Then, the risk value of each incident level obtained by the multiplication of the calculated number and the level of the severity. If the incident report concerning the user is detected, the risk value of the incident is added regardless of the number of incidents.

The malicious activity of the user directly indicates the credit of the user. If the user conducted malicious activity, even if it is once, the system adds the maximum number of the risk.

Generally, an organization conducts the education of basic knowledge about information security to employees. The system simply judges the risk of users by checking whether he/she attended the lecture or not. The style or contents of education depends on the organization. Therefore, the system calculates that 25 divides by the total number of educations conducted by the organization, and it obtains the risk of the learning state by multiplication of the calculated number and number of the absence of the user.

The system obtains the RU_u by the sum total of the user concerning contents. ($0 \leq RU_u \leq 100$)

The second factor is the importance of resources. Generally, an organization assigns importance to each file treated in the office. Based on the importance, the access authority is assigned. For example, only a responsible person can treat a confidential file, which has very high importance. The system defines the I_r as the importance of the resource r, and sets its minimum value to zero and maximum value to M_2. Similar to M_1, we set 100 to M_2 in this paper. The system converts the value of the importance of the resource r decided by the organization to I_r by adjusting a ratio.

Finally, the system earns RC_c by Equation (1).

$$RC_c = RU_u \times I_r \quad (0 \leq RC_C \leq 10000) \tag{1}$$

By using obtained RC_c, the system decides the access control of communication c. To decide the access control, network administrators have to set and adjust two parameters, i.e., th_1 and th_2, in advance according to the security policy of the organization.

The th_1 is the threshold to treat communication as holding a certain risk. Only when RC_c is less than th_1, communication c is permitted access similar to regular permission.

The th_2 is the threshold to judge whether the system permits communication or not. If the RC_c is higher than th_2, the system decides that the communication c has high risk, and judges to restrict it. Only when a responsible person permits communication, the system resumes permission of the communication.

If the RC_c is higher than th_1 and less than th_2, the system permits communication for a certain period. The system defines the permitting time PT_c as a period for permitting communication c, and it calculates the permitting time by Equation (2).

$$PT_c = \frac{1}{RC_c} \times T \tag{2}$$

In this equation, the T is the parameter to adjust the permitting time according to the work style of the organization. The value of T is different for each organization. For example, in an organization in which users need to exchange big size data, the network administrator set a big value to the T.

3.2.2 Example of Evaluation

We introduce the example of an evaluation. As shown in Figure 2, we assume two users. In the organization, the severity of the incident is assigned to 4 levels similar to Figure 1.

The user A receives 1,500 messages including 30 malicious messages, and he has no concerning incident log and malicious activity. In addition, he completely attended the learning by the organization. In this situation, the RU_A comes to be 0.5.

On the other hand, the user B receives 800 messages including 40 malicious messages, and he caused the incident in which severity is 4. Moreover, he conducted the malicious activity in advance, and he was absent from three lectures. The risk of the user B is high, and the RU_B comes to be 51.25.

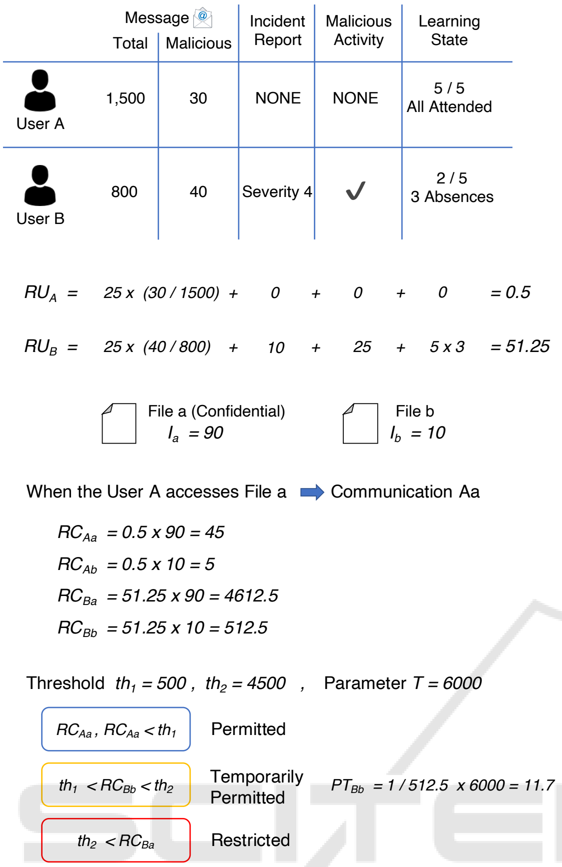
When the user A and the user B access the file a and the file b, the system calculates the risk of such communication. For example, the organization assigns $I_a = 90$ and $I_b = 10$.

In this case, the risk of communication RC is calculated, as shown in Figure 2. In addition, the organization sets value of each parameter as shown in Table 1.

Table 1: Value of parameters.

Parameter	Value
th_1	500
th_2	4500
T	6000

Finally, the system decides that the communication from the user A to the file a and the file b is permitted and the communication between the user B and



	Message Total	Message Malicious	Incident Report	Malicious Activity	Learning State
User A	1,500	30	NONE	NONE	5 / 5 All Attended
User B	800	40	Severity 4	✓	2 / 5 3 Absences

$RU_A = 25 \times (30 / 1500) + 0 + 0 + 0 = 0.5$

$RU_B = 25 \times (40 / 800) + 10 + 25 + 5 \times 3 = 51.25$

File a (Confidential) $I_a = 90$

File b $I_b = 10$

When the User A accesses File a → Communication Aa

$RC_{Aa} = 0.5 \times 90 = 45$

$RC_{Ab} = 0.5 \times 10 = 5$

$RC_{Ba} = 51.25 \times 90 = 4612.5$

$RC_{Bb} = 51.25 \times 10 = 512.5$

Threshold $th_1 = 500$, $th_2 = 4500$, Parameter $T = 6000$

$RC_{Aa}, RC_{Aa} < th_1$ Permitted

$th_1 < RC_{Bb} < th_2$ Temporarily Permitted $PT_{Bb} = 1 / 512.5 \times 6000 = 11.7$

$th_2 < RC_{Ba}$ Restricted

Figure 2: Example of the evaluation.

the file b is permitted for 11 minutes. The communication between the user B and the file a is restricted by the system.

3.3 Architecture

Figure 3 shows the architecture of the proposed system. The system consists of seven modules and one database.

3.3.1 Log-on/out Detector

First of all, when a user connects to the VPN server in the office, the log of the connection is sent to the Log-in/out Detector module. If the received log indicates the log-in of the user, the module sends the log-in information which includes the user's information to the User's Risk Calculator module. On the other hand, if the log indicates the user's log-out, the module sends the log-out information to the Termination Manager module.

3.3.2 User's Risk Calculator

User's Risk Calculator calculates the risk of users. When the module receives the user's log-in information, it investigates the human resource information and his/her client information by using the directory service server.

Then, the module finds out the mail quarantine log in the mail gateway for a certain period, e.g., 1 month, to investigate the reception of malicious e-mails against the user's e-mail address. Moreover, it receives the security log concerning the user from the database in the network. The security log includes the previous incident report, malicious activity, and learning state of the seminar about information security.

By using the obtained information, the module calculates the risk of the user. Finally, it sends the risk of the user in addition to the human resource information and client information to ACL's Risk Calculator.

3.3.3 ACL's Risk Calculator

ACL's Risk Calculator calculates the risk of access controls concerning the user's client. When it receives client information, it finds concerning access controls that permit access to the resources about the client from the applied ACL. Moreover, it investigates the importance of each resource in which each access control permits access from the clients.

After the investigation of resource importance, the module calculates the risk of each access control. Then, if the calculated risk of access control exceeds the threshold th_1, the module generates the new ACL, which does not include the access control permitting access to the resources.

In addition, the module investigates the recent access situation to the resources from the client by using mirrored packets stored in Packet Collector. Even if the risk of access control does not exceed the threshold, the system restricts the communication when the client has not accessed the resources.

If the risk of access control is less than the threshold th_2, the module calculates the permitting time in order to permit the communication for a short period when the user tries to communicate.

Finally, the module registers the generated new ACL and the permitting time to Dynamic ACL DB and sends it to Configurator, and then, Configurator configures the network equipments in the organization.

3.3.4 Packet Collector

Packet Collector module receives mirrored packets in the network and stores them in the database. When

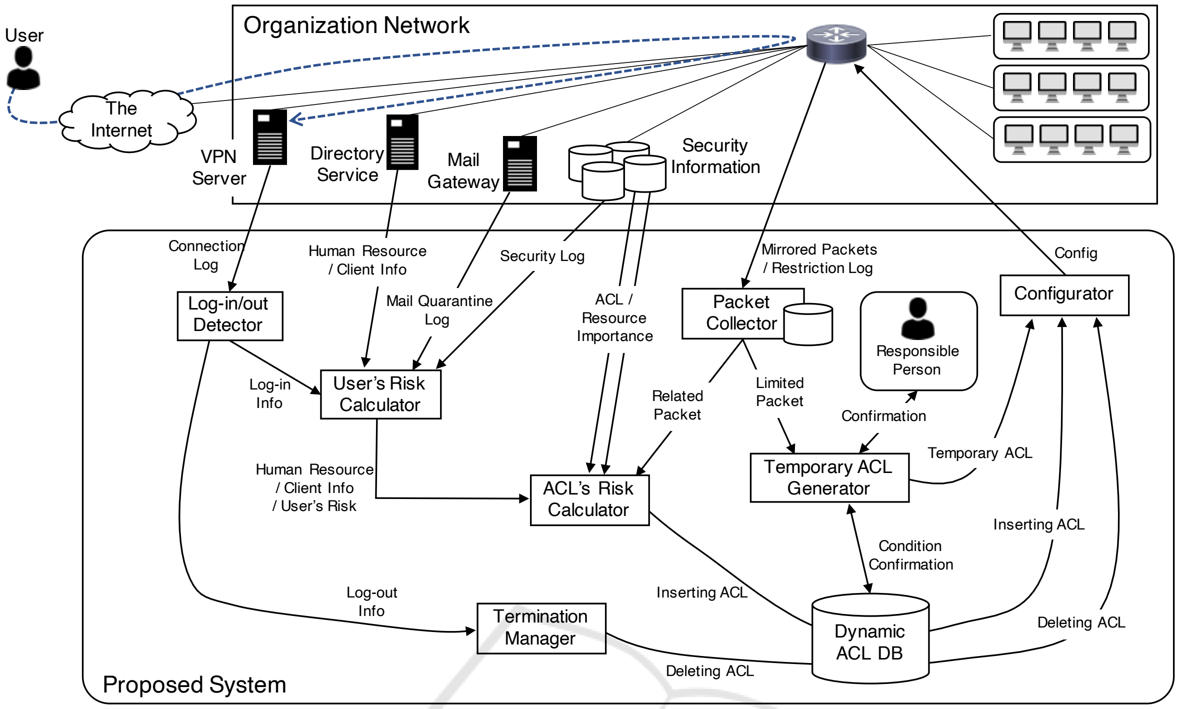


Figure 3: Architecture of the proposed system.

ACL's Risk Calculator finds the packets concerning the client, Packet Collector finds them from the database and sends the found packets to ACL's Risk Calculator module.

In addition to the mirrored packets, the module receives restriction logs of network equipments. The logs include the communication restricted by the proposed system, and a part of them will be permitted for a short period. When the communication is restricted by the ACL generated by the proposed system, the module sends the log of such communication to Temporary ACL Generator module.

3.3.5 Temporary ACL Generator

Temporary ACL Generator module receives packets which restricted by the proposed system, and then, it inquires the condition of permission about such packet to Dynamic ACL DB.

If the permitting time is registered, the module sends the ACL including permission of the restricted communication to Configurator and it measures the time. After the permitting time passes, the module sends the new ACL to Configurator again in order to restore the ACL.

On the other hand, if the permitting time is not registered, such communication is judged should be restricted by the proposed system. If the communication is usually permitted for users at office, the system asks a responsible person whether permit or not. If permitted, the module sends new ACL to Configurator module.

3.3.6 Termination Manager

When Log-in/out Detector module confirms the log-out of a user, it sends such log-out information to Termination Manager module. Termination Manager module finds the access controls concerning the user from Dynamic ACL DB, and then, it deletes found access controls from Dynamic ACL DB and sends a new ACL to Configurator module to restore the original ACL.

4 VERIFICATION OF THE PROPOSED SYSTEM

In this section, we discuss about verification of the proposed system. As a verification experiment, we compare the proposed system to simple separated network and flat network in the assumed scenario. We assume the scenario that a user, who is judged to have a high risk and his home device is infected by malware, telecommutes by connecting to the internal network via VPN. In addition, the attacker remotely controls the infected host to attack organization's internal network.

4.1 Security Effectiveness

From the viewpoint of security effectiveness, we discuss resource protection and harmful effects on other devices. Figure 4 shows the accessible area from a user.

When an organization does not apply the separated network, the user can communicate with all other terminals. In this case, all terminals have the risk of attack via the internal network connection. In addition, the attacker can access resources to which the user has access authority and resources with no authentication, therefore, a lot of resources have the risk of leakage.

On the other hand, if the separated network is constructed, the proposed system supposes such networks, the attacker can access to the only user concerning servers and terminals. In other words, the number of terminals which has the risk to be targeted by the attack decreases. Besides, only the resources that authorize the user are communicated by the user's terminal. The separated network can reduce the risk of attacks.

By the proposed system, accessible resources and terminals are strictly limited. Only ordinarily used resources that have moderate importance are accessible by the user. The high important resources are protected by access controls.

When the user works at the office as usual, we have several chances to detect the malicious activities controlled by external attackers targeting important resources by the IDS or the network quarantine logs and so on. However, when the terminal in the office is remotely controlled from the user's home, it is difficult to distinguish whether it is conducted by the genuine user or the attacker. Therefore, the communication limitation according to the situation of the user is effective.

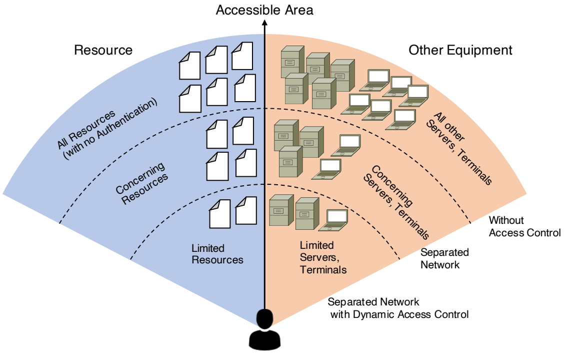


Figure 4: Accessible resources and equipments from a user.

4.2 Accessibility Effectiveness

From the viewpoint of accessibility effectiveness, the proposed system can provide effective access control. Generally, to ensure security, organizations restrict the communication to important information by telecommuting. Such restriction is conducted under uniform conditions against all users in the organization. It can protect important information, however, the convenience of users decrease.

There are low-security awareness users in the organization, therefore it is effective against such users. However, for high-security awareness users, it is an onerous restriction. In the assumed scenario, the infected terminal is restricted to access the important information, however, other terminals are similarly restricted to conduct communication.

The proposed system judges access controls according to the situation of users, therefore, it can apply flexibly access controls. For example, the high-security awareness user can access the resources from home almost the same as the office. On the other hand, a low-security awareness user is restricted to access the resources, however, the methods of temporary permission of communication and permission by a responsible person can improve the convenience of users and business continuity.

5 CONCLUSIONS

In this paper, we proposed a dynamic access control system based on the situation of users. The COVID-19 changes the human work style, and working from home comes to be a more generic style. To ensure the organization's network security to which a lot of clients connect from home, we have to flexibly change the access controls in the network according to the situation of users. The proposed system makes such dynamic access control possible by evaluating the risk of the user and the importance of communication destination resources. Based on the evaluation results, the system dynamically changes the permission of communication, i.e., no change, permitting for a certain period, restricting. We can reduce the risk of attack against important resources, and ensure the security of organization networks.

In future works, we will implement the system and deploy it to a large-scale experimental network for evaluation of the system. In addition, we will extend the system to focus on the access authority of files. When a server stores a high important resource, the proposed system may restrict the communication between a user and the server even if the user wants to access the other low important resource because the proposed system focuses only on the network access controls. To solve such a problem, we will extend the proposed system to conduct more flexible controls by collaborating network access and user's access authority to resources.

ACKNOWLEDGEMENT

Part of this work is supported by the Cabinet Office (CAO), Cross-ministerial Strategic Innovation Promotion Program (SIP), "Cyber Physical Security for IoT Society" (funding agency: NEDO).

REFERENCES

Atlam, H. F., Alenezi, A., Walters, R. J., and Wills, G. B. (2017). An overview of risk estimation techniques in risk-based access control for the internet of things. In *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security - IoTBDS,*, pages 254–260. INSTICC, SciTePress.

Cichonski, P., Miller, T., Grance, T., and Scarfone, K. (2012). Computer Security Incident Handling Guide. *NIST Special Publication 800-61 Revision 2*.

Cybersecurity and Infrastructure Security Agency (CISA) (2020). Alert (AA20-280A) Emotet Malware. URL: https://us-cert.cisa.gov/ncas/alerts/aa20-280a [accessed: 2020-10-29].

Information-technology Promotion Agency, J. (2011). Design and Operational Guide to Protect against "Advanced Persistent Threats" Revised 2nd edition. URL: https://www.ipa.go.jp/files/000017299.pdf [accessed: 2020-10-29].

Nayak, A. K., Reimers, A., Feamster, N., and Clark, R. (2009). Resonance: dynamic access control for enterprise networks. In *Proceedings of the 1st ACM workshop on Research on enterprise networking*, pages 11–18.

Nguyen, V.-G. and Kim, Y. (2016). Sdn-based enterprise and campus networks: A case of vlan management. *JIPS*, 12(3):511–524.

Rath, T. A. and Colin, J.-N. (2017). Adaptive risk-aware access control model for internet of things. In *2017 International Workshop on Secure Internet of Things (SIoT)*, pages 40–49. IEEE.

Tian, B., Zhang, X., Zhai, E., Liu, H. H., Ye, Q., Wang, C., Wu, X., Ji, Z., Sang, Y., Zhang, M., et al. (2019). Safely and automatically updating in-network acl configurations with intent language. In *Proceedings of the ACM Special Interest Group on Data Communication*, pages 214–226.

Watanabe, T., Kitazaki, T., Ideguchi, T., and Murata, Y. (2005). A Proposal of Dinamic VLAN Configuration with Traffic Analyzation and Its Evaluation Using a Computer Simulation (in Japanese). *IPSJ Journal*, 46(9):2196–2204.