




A File Access Permission Management System to Realize Task Transfer during Cyber Attacks

Hidetoshi Kawai 

Department of Informatics, The Graduate University for Advanced Studies, Tokyo, JAPAN
e-mail: h-kawai@nii.ac.jp

Masahito Kumazaki , Hirokazu Hasegawa , Hiroki Takakura 

Center for Strategic Cyber Resilience R&D, National Institute of Informatics, Tokyo, JAPAN
e-mail: {kumazaki, hasegawa, takakura}@nii.ac.jp

Masahiko Kato

Department of Health Data Science, Juntendo University, Chiba, Japan
e-mail: m.kato.ug@juntendo.ac.jp

Abstract—When a cyberattack happens to any company, they often disconnect the attacked device or all of the devices in the department where the attack device belongs from the internal network. The primary objective of this study is to improve business continuity. In this paper, we propose a system for file access management under cyberattack. The system is designed to allow the transfer of file access permissions from a cyberattack victim to other employees. The system uses victim file information and staff information, and determines who to transfer authority to based on the file's content and importance, as well as the individual's expertise and reliability.

Keywords—Cyber Attacks; File access permissions; Reliability; Expertise; Business Continuity.

I. INTRODUCTION

When a cyber attack happens to any company, they often disconnect the attacked device from the internal network to respond to the incident. Sometimes, they have to disconnect multiple devices, and all operations using those devices will be suspended. However, in the case of the infrastructure, e.g., medical, transportation, electric power, communication, and so on, suspension of the attacked device may cause serious damage to our society. Therefore, the primary objective of this study is to improve business continuity under cyber attacks.

In the military, if a superior officer is injured and unable to continue their duties, their subordinates are promoted to take over to continue their work. Applying this to a company under cyberattack, the tasks previously handled by the compromised employee would be continued by their subordinate, who gets promoted. However, this method might not work if the subordinate does not have sufficient skills to perform those duties. Additionally, since these tasks are recorded in files, it is important to manage the file access permissions.

In this paper, we propose a file access permission management system under cyber attacks. The system aims to distribute the work of the employee who was attacked to others. First, it determines whether a subordinate can take over tasks based on the file content, considering factors like confidentiality. If it is decided that a subordinate can handle a file, that file is then assigned to an individual based on its importance,

the employee's individual expertise, and their reliability, thus determining who will take over the superior's duties.

The outline of this paper is as follows. We introduce previous research related to file access permission management in Section II. Section III describes the proposed system, and Section IV explains the implementation plan, how to evaluate a pilot. In Section V, we discuss what needs to be improved in the pilot. Finally, we present our conclusion and future works in Section VI.

II. RELATED WORK

It is important to protect sensitive information in every company and organization. A lot of methods to determine individual access privileges have been developed until today. Discretionary Access Control (DAC) has been used for a long time. DAC lets resource owners decide who can access their work. It is a flexible way to control who can access resources like files and databases because owners can give or take away permissions from other users [1]. Mandatory Access Control (MAC) is also used for accesses to highly confidential information in critical environments like military ones. MAC needed to have flexible access control mechanism with the development of computing technology [2]. However, DAC and MAC are not suitable for today's complex organizations [3]. So, the method called Role-based Access Control (RBAC) was proposed by Ferraiolo and Kuhn in 1992 [4] to solve the problem. This access control method centralizes management by role, and cannot be delegated between users without authority. Thus, it improved the file management efficiency compared to MAC and DAC. After that, RBAC has been studied using various approaches because researchers aimed to achieve one that reflected changing organizational circumstances. Julisch and Karjoth [5] presented an automated method for determining access permissions for new users or users whose roles have changed within an organization, focusing on the assignment of appropriate access rights. The proposed method assesses the access rights of similar users and decides new access permissions for new people in department positions. Moreover,

Privacy-aware Role-Based Access Control (P-RBAC) was proposed by Qunet al. as an evolution of RBAC [6]. It aimed to apply restrictions required by privacy laws and internal policies in an organization to RBAC.

Focusing on the fact that previous studies assumed that no cyber attacks had occurred, McGraw proposed a new access-control approach called Risk-Adaptable Access Control (RAdAC). RAdAC dynamically weighs mission importance against security risk and chooses the best information-sharing decision for each situation [7]. However, the system proposed by him has low adaptability to general organizations because it was developed for the military.

III. PROPOSED SYSTEM

A. Overview of the Proposed System

We propose a file access permission management system to improve business continuity under cyber attacks. Figure 1 shows the concept of the proposed system in this paper.

When a victim device of a cyber attack is isolated from the network, the user of the device cannot push his work forward. It may not only be his problem but also cause a delay or business suspension in his department. Therefore, the system ensures business continuity in the department by dividing his work to other persons in his department. The proposal system determines a substitute person and changing access permissions from the victim to him for all files to which only the victim has access permission.

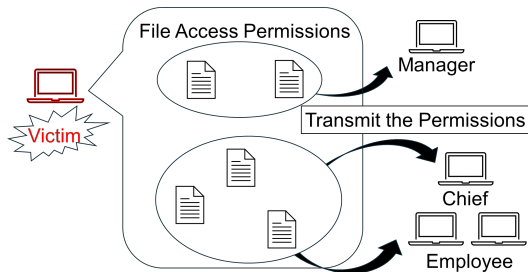


Figure 1. Concept of the Proposed System.

B. Assumption

In order to determine the substitute worker of each file, the system uses information about files and staff. The detailed assumptions in this paper are listed below.

1) *Victim File Information*: The file information includes the list of victim's files with each file's data, importance, expertise it requires, and access permitted information. The victim's file is a file only the victim has write permission to. We describe the details of file's importance and expertise below.

- **File Importance**

File Importance is based on three values, Confidentiality, Integrity, and Availability. It decides what positions have access to files according to the importance.

- **File Expertise**

This expertise is the value that reflects the level of skill required to operate files. This value is decided by the owner who has the file access permissions.

2) *Staff Information*: The Staff Information consists of name, staff ID, department, post, IP address, reliability, and user expertise. IP address and staff ID are linked and managed on the Asset Management DB. Moreover, Staff Information without IP address is consolidated and stored in the Human Resources Information DB. In particular, we describe the reliability and expertise below.

- **Reliability**

Reliability is a score that quantifies each user's level of security awareness and risk. Shinoda et al. proposed a method to calculate the reliability based on multiple indicators [8]. In this method, Carelessness, Awareness of Efforts to Secure, and Security Skill Levels are used for the calculation of reliability. The Carelessness is calculated based on the results from the Security Surprise Test, URL Filtering Detection, and Incident History. The Awareness is determined based on the Progress Rate of Security Training Courses and the response of the Security Surprise Test. The User Skill Level is decided based on the Test Result Scores during Security Training Courses and the result of the Security Surprise Test. We assumed that Reliability of each user has been calculated in advance using this method and is available as part of the Staff Information.

- **User Expertise**

User Expertise refers to very high domain-specific competence relative to peers with the same tasks in a specific domain [9]. In other words, User Expertise represents how skilled a person is at their job compared to their colleagues. For example, an employee in the Development department needs programming skill, technical knowledge, and more. User Expertise indicates these values per employee in this example. It is assumed that User Expertise related to the duties of the department to which each user currently belongs is calculated and included in the staff information.

C. Architecture

Figure 2 shows the architecture of the proposed system. The system consists of three modules, Information Collector, Access Permission Allocator, and OverWriter. These modules play a role in collecting information about users and files, deciding new file access permissions, and overwriting the new permissions. The Access Permission Allocator module consists of five components: Contents Classifier, Importance Classifier, Expertise Classifier, Reliability Classifier, and File Permission Decider. Figure 3 shows these components in the Access Permission Allocator.

1) *Information Collector*: First, the administrator who manages this proposed system inputs the IP address of the victim device in the Information Collector Module when an attack is detected (Figure 2 - I). By using the IP address of the victim's device, Asset Management provides this module with the staff ID of the device owner who was attacked (Figure 2 - II, II'). Subsequently, it obtains victim information about Reliability, Department, and Post with staff ID from Human Resources Information (Figure 2 - III, III'). Using the staff ID, it searches the file server for files only the victim has

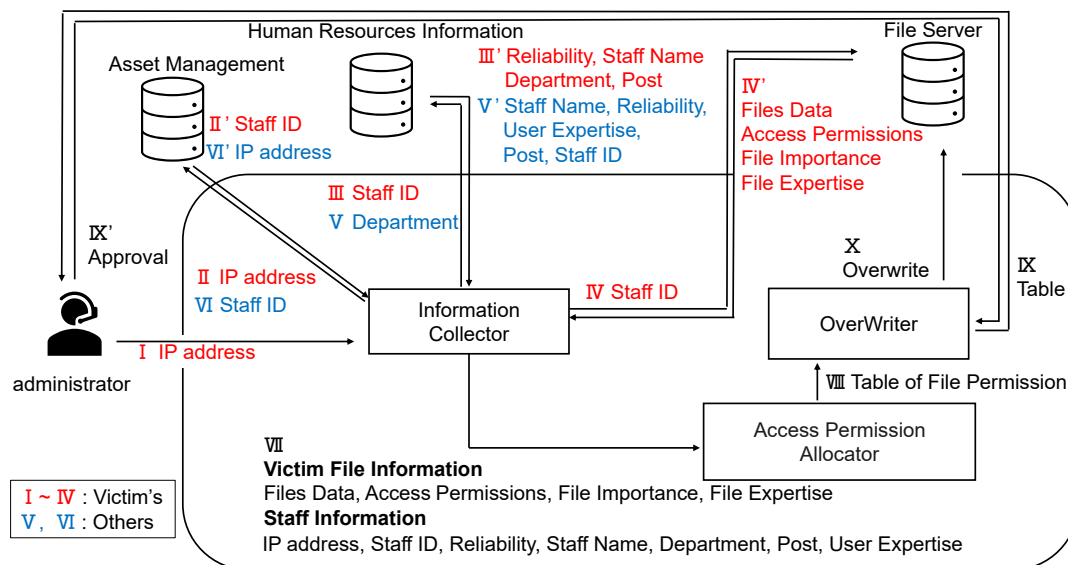


Figure 2. Architecture of the Proposed System.

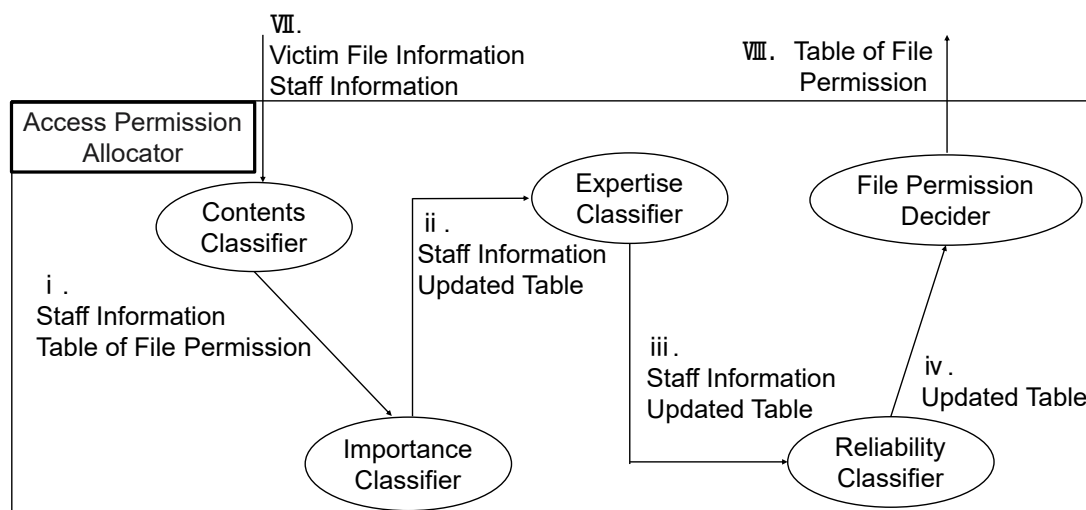


Figure 3. Components in Access Permission Allocator.

permission to write to and gathers the files found together with their importance and expertise information (Figure 2 - I V, IV'). Based on the gathered files, it generates Victim File Information.

In addition, the module collects Staff Information of all members in the same department as the victim by victim's department (Figure 2 - V, V'). It sends all the ID of collected Staff Information to Asset Management DB and receives the IP addresses if their device (Figure 2 - VI, VI'). Finally, the module sends Staff Information consisting of the victim and all members of his department with their device's IP address and Victim File Information to the Access Permission Allocator module (Figure 2 - VII).

2) *Access Permission Allocator*: The module consists of five components and Figure 3 shows the structure of the module. Each component performs classifying the victim’s file permissions to decide new permissions according to the

information received from previous module. The details are as follows.

- Contents Classifier

This component classifies the file access rights according to the file contents and makes a table of new file permissions. Files that only victim can access include highly classified information. For instance, that needs approval of the position above the victim, is recorded in the minutes of the executive meeting, and more. Of course, there is also no classified information. For this reason, we have to check these files, whichever victim's subordinates can access or not, based on the contents of victim's file in Staff Information (Figure 3 - i). In order to analyze the contents, this component utilizes Large Language Model (LLM) because it is so difficult to analyze them that are not standardized format and written in natural language. That is why this component uses LLM

to analyze the contents and this module makes a table of individuals who may be granted file access permission, and sends it next to the components.

- Importance Classifier

This component modifies the importance of files that are allowed to pass file permissions to subordinates by the previous component. When the victim cannot use his device and his subordinates have to operate his work, there are gaps in access permissions based on file importance. So, this component temporarily changes his file importance and determines the extent to which permissions are to be redistributed among his subordinates. In order to do it, the component decreases the importance of the file by one level and eliminates the gap. At last, the component updates the table received from the previous module and sends it to the next component (Figure 3 - ii).

- Expertise Classifier

Expertise Classifier Component decides someone who is not enough to operate the victim's file based on the expertise his subordinates have. This process narrows down the candidates to whom file permissions may be distributed based on the user expertise, and file access permissions will be distributed only to staff who meet the required technical capabilities. In addition, the required technical level is determined for each file, and this value is compared with the staff's expertise to determine whether to grant access to the file. The component then changes the table to show this process and sends it to the next component (Figure 3 - iii).

- Reliability Classifier.

This component decides his subordinates are not reliable according to the reliability score because this component aims to prevent them from distributing file permissions to low trust staff by narrowing them. It compares victim's Reliability Score with his subordinate's score and update the table from previous component (Figure 3 - iv).

- File Permission Decider

The above components have been narrowed down the victim's subordinates to whom file access permissions are distributed. This component decides who will have access to the files in accordance with the amount of work for an individual. This decision is reflected in a table, and the component updates the table that links the IP addresses of the devices owned by each subordinate. Finally, this component sends it to the OverWriter module (Figure 3 - VIII).

3) *OverWriter*: OverWriter module receives the table from Access Permission Allocator module (Figure 2 - VIII), and sends it to the administrator who manages the system to get approval. After he approves it, the module replaces the victim's file permissions with the new one (Figure 2 - IX, IX', X).

IV. EVALUATION

The proposed system is still in the idea stage and has not yet been implemented. Therefore, we conducted a simulation to verify the system. This paper discusses its expected results.

A. Evaluation Method

Figure 4 shows the network of an assumed experimental organization. There are five devices and people in each of the two departments. We assume the section manager of department A is attacked, and our proposed system will distribute file access permissions from the section manager to others. In addition, victim file information is on the File Server, and his files are categorized into three levels of importance based on the policy of Information-technology Promotion Agency, Japan (IPA) [10]. The IPA has stipulated that the importance of a file is determined by assessing it on a three-level scale for each of the criteria of confidentiality, integrity, and availability, and then determining the importance based on the maximum value of each of these levels. He deals with six files, and these files consist of two of each file with a level one, level two, and level three importance. Moreover, the Asset Management DB is on the Asset Management Server, and the Human Resources Information DB is on the Human Resources Information Server, as shown in Figure 4. Especially, Table I is a part of staff information in the Human Resources Information DB and represents the personnel deployment in the organization.

TABLE I. PART OF STAFF INFORMATION

| Staff ID | Staff Name | Post | Department |
|----------|------------|-----------------|------------|
| A1 | | Manager | A |
| A2 | | Section Manager | A |
| A3 | | Chief | A |
| A4 | | Employee | A |
| A5 | | Employee | A |

B. Expected Results

In this subsection, we explain about the expected results and the interim one. Access Permission Allocator module receives victim file information and staff information from Information Collector module, and outputs the table of file permission to OverWriter module. Table IV is the output from Access Permission Allocator module, and Table II and Table III are the interim table from any components in this module.

Table II is the interim table generated by Reliability Classifier components. Components from Contents Classifier to Reliability Classifier decide someone who cannot access the victim's files following file contents, file importance, user expertise, and reliability, and this table reflects these decisions. The details are shown below.

- File 1 :

People without Manager whose staff ID is A1 cannot access the file based on file contents, file importance, user expertise, and reliability.

- File 2, 3, 4 :

Only employees whose staff ID are A4 and A5 cannot access these files.

- File 5, 6 :

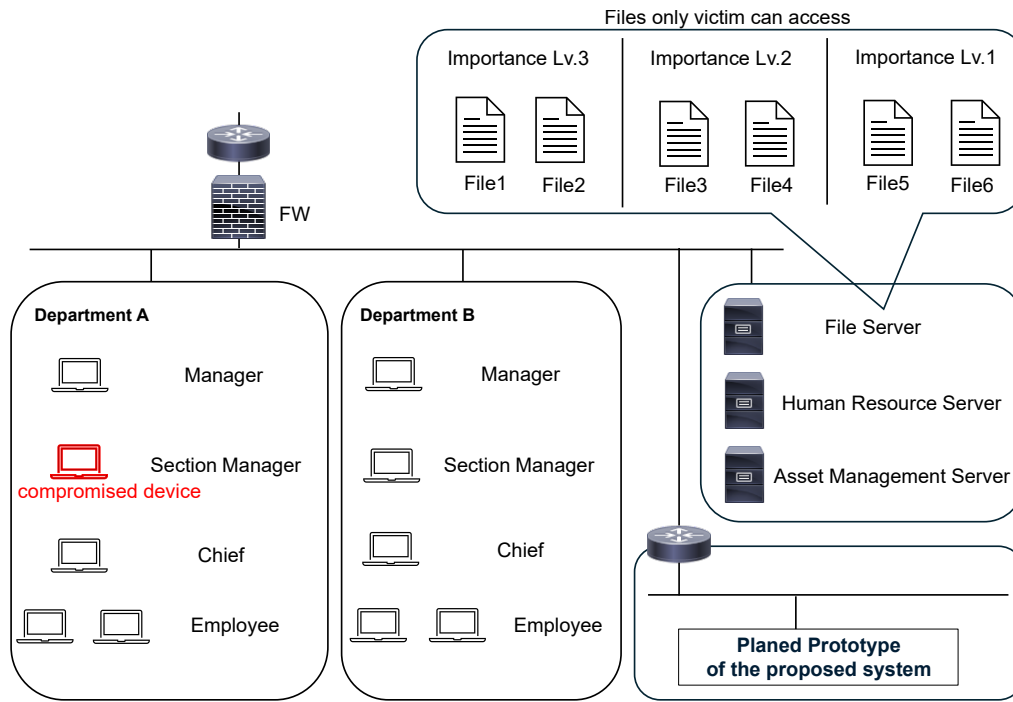


Figure 4. Assumed Experimental Network.

TABLE II. ACCESS OR NOT TABLE BY RELIABILITY CLASSIFIER

| | Staff in Department | | | |
|-------|---------------------|----|----|----|
| Files | A1 | A3 | A4 | A5 |
| File1 | - | x | x | x |
| File2 | - | - | x | x |
| File3 | - | - | x | x |
| File4 | - | - | x | x |
| File5 | - | - | - | - |
| File6 | - | - | - | - |

√ : access, x : no access,
- : undecided

TABLE III. ACCESS OR NOT TABLE BY FILE PERMISSION DECIDER

| | Staff in Department | | | |
|-------|---------------------|----|----|----|
| Files | A1 | A3 | A4 | A5 |
| File1 | √ | x | x | x |
| File2 | x | √ | x | x |
| File3 | x | √ | x | x |
| File4 | √ | x | x | x |
| File5 | x | x | √ | x |
| File6 | x | x | x | √ |

√ : access, x : no access,
- : undecided

All staff have the potential to access these files. But they have not had these file access permissions yet.

Table III is the interim table generated by File Permission Decider based on the workload in order to prevent imbalances in workload. In this process, this module receives the Table II, decides the permissions, and updates Table III with Table II. Moreover, the components linked file access permissions with staff information like Table IV, and output it to OverWriter Module.

V. DISCUSSION

The previous studies mentioned in Section II are for access control systems under normal conditions [1]–[5]. On the other

TABLE IV. OUTPUT OF FILE ACCESS PERMISSIONS

| Files | Post | Name | Staff ID | IP Address |
|-------|----------|------|----------|---------------|
| File1 | Manager | | A1 | 192.0.2.11/24 |
| File2 | Chief | | A3 | 192.0.2.12/24 |
| File3 | Chief | | A3 | 192.0.2.13/24 |
| File4 | Manager | | A1 | 192.0.2.14/24 |
| File5 | Employee | | A4 | 192.0.2.15/24 |
| File6 | Employee | | A5 | 192.0.2.16/24 |

Note ; IP addresses listed in this table are illustrative examples.

hand, our proposed system is beneficial in dealing with any incidents. Moreover, it is useful that the system is introduced to many organizations because the previous system proposed by McGraw in 2010 aimed at military organizations [7]. The proposed system is designed for an on-premises environment in this paper. But it is possible to redesign the system for cloud computing in mind, and all kinds of organizations can adopt the system. The system has not yet been implemented in this paper. But there are potential challenges and limitations. These details are below.

A. Decrease in resources of the devices

It is less likely to expand cyber attacks from one compromised device, like a springboard attack because the device cannot use files by the proposed system in this paper. But there are possibilities of the reduction of the no affected devices by other attack vectors.

Moreover, when a staff member is attacked and everyone above him is also attacked, the problem arises with Contents Classifier component because it cannot distribute file access permissions that record highly confidential information to his subordinates. Therefore, we should prepare solutions for the management of the number of devices and improve the system.

B. The staff's past expertise

We proposed a system targeted at staff within a single department. This system utilizes the user expertise that would be required within a department. However, there are employees moving from one different department to another one. When such a movement occurs, the expertise that was required in the previous department should be reflected in user expertise.

C. Timing of file access permission transfers

In this paper, the administrator who is responsible for the proposed system approves the table sent from OverWriter module. The access permissions are transferred when the module overwrites the file server after approval.

This transfer is most likely to occur while a compromised device is manipulating data. At that time, the device's access right is revoked, making differences between the data stored on file server and edited on the device. Consequently, managing this difference becomes essential because the edited data may contain malware.

To address these issues, we propose storing the edited data in a temporary location such as a quarantine folder. The system should scan the data for malware and retain it for a predetermined period to allow detection of unknown threats. Only after confirming that no problems exist, should it be written back to the original folder as a derived file. This system ensures both consistency and authenticity.

D. Execution time

Since the system has not yet been implemented, the following issues are anticipated regarding system execution time. There is a possibility that an attacker could edit and save the contents of files using an infected device while the proposed system

is running. Especially, this problem is likely to occur when system execution times are long.

E. Limitations

- Limitations of administrator

In this paper, the system requires an administrator to review and approve its contents before overwriting the file server with the determined file permissions table. However, he is primarily responsible for managing the proposed system and is likely unfamiliar with the detailed operations within the company. Therefore, the ideal method for this process would be for the victim, who was originally responsible for the tasks, to review and approve the content of the generated table. On the other hand, the challenge is that the victim's computer has been compromised by the cyberattack, making it impossible to facilitate this review.

- On-premise experimental environment

We assume an experimental organization that manages data in an on-premises environment. An advantage using the environment is that data management can be completed within a company. On the other hand, in order to reduce the efforts or costs of operations in an on-premises environment, many organizations are using the data management system in cloud. Compared with on-premises environments, cloud-based data management systems can cause problems with communication delay. Therefore, it is necessary to evaluate the proposed system under a cloud environment.

VI. CONCLUSION AND FUTURE WORK

We proposed a system for file access management under cyberattack that aims to improve the business continuity in this paper. We expect that the system is effective from the perspective of flexibly changing access permissions under cyber attacks and being adaptable to a variety of organizations. However, we have not implemented the system and conducted verification of the effects. Future work will involve developing the system and conducting experiments to assess the effectiveness, limitations, and robustness of the system under cyber attacks.

ACKNOWLEDGEMENTS

This work was supported by JST K Program Grant Number JPMJKP24K3, Japan.

REFERENCES

- [1] D. D. Downs, J. R. Rub, K. C. Kung, and C. S. Jordan, "Issues in discretionary access control", in *1985 IEEE Symposium on Security and Privacy*, 1985, pp. 208–208. DOI: 10.1109/SP.1985.10014.
- [2] J. H. Jafarian, M. Amini, and R. Jalili, "A dynamic mandatory access control model", in *Computer Society of Iran Computer Conference*, Springer, 2008, pp. 862–866.
- [3] A. Gabillon, "Web access control strategies", in Jan. 2011, pp. 1368–1371, ISBN: 978-1-4419-5906-5. DOI: 10.1007/978-1-4419-5906-5_664.
- [4] D. F. Ferraiolo and D. R. Kuhn, "Role-based access controls", in *Proceedings of the 15th National Computer Security Conference*, Baltimore, MD, USA: National Institute of Standards and Technology (NIST), Oct. 1992, pp. 554–563.

- [5] K. Julisch and G. Karjoth, *Method and apparatus for automated assignment of access permissions to users*, US Patent 8,826,455, 2014.
- [6] Q. Ni et al., “Privacy-aware role-based access control”, *ACM Transactions on Information and System Security (TISSEC)*, vol. 13, no. 3, pp. 1–31, 2010.
- [7] R. W. McGraw, “Risk-adaptable access control (RAdAC)”, in *Proceedings of the NIST & NSA Privilege Management Workshop*, Paper originally presented September 2009; online PDF accessed June 2025, Gaithersburg, MD, USA: National Institute of Standards and Technology, 2010, pp. 1–10.
- [8] A. Shinoda, H. Hasegawa, H. Shimada, Y. Yamaguchi, and H. Takakura, “Feasibility verification of access control system for telecommuting by users reliability calculation”, in *Proceedings of the Eighteenth International Conference on Systems and Networks Communications*. International Academy, Research, and Industry Association, Nov. 2023, pp. 16–22.
- [9] D. P. Köhler, A. Rausch, T. Biemann, and R. Büchsenschuss, “Expertise and specialization in organizations: A social network analysis”, *European Journal of Work and Organizational Psychology*, vol. 34, no. 2, pp. 282–297, 2025.
- [10] S. C. Information-technology Promotion Agency Japan (IPA), *Risk analysis sheet: Information security measures guidelines for small and medium-sized enterprises, version 3.1, appendix 7*, Guideline, https://www.ipa.go.jp/security/sme/f55m8k000000587z-att/outline_guidance_risk.pdf, Last accessed: June, 2025, Tokyo, Jul. 2024.