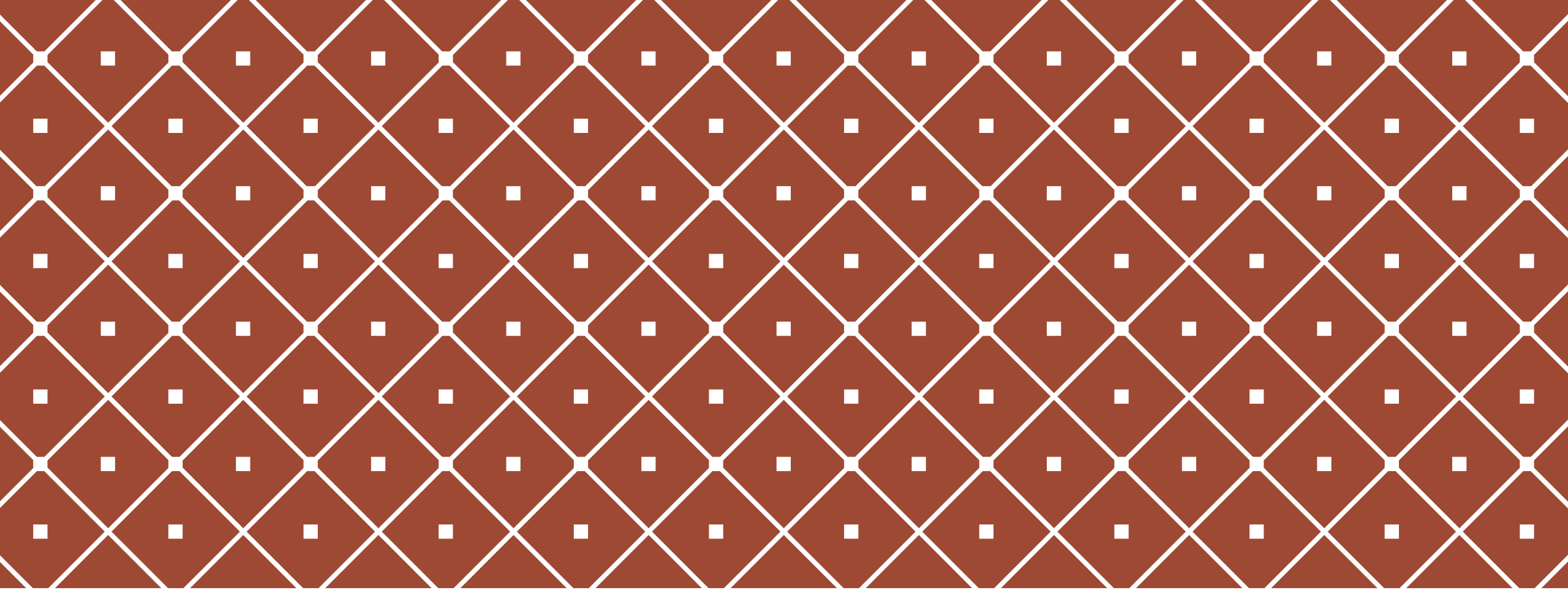


THINKING FROM INCIDENTS - SECURITY RESILIENCE

Tomoko Kaneko

AGENDA

I. Introduction.

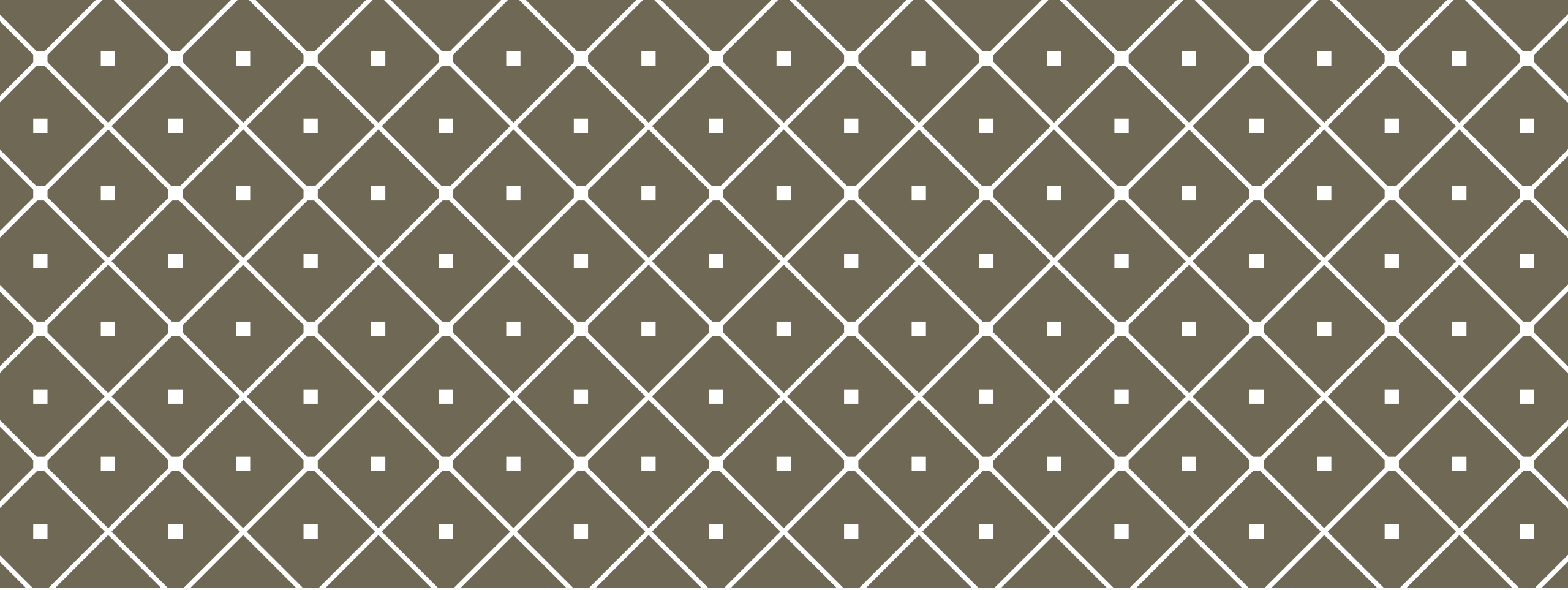
II. Related Work

III. Analysis and results applied to information security incidents
- A. Analysis Overview
- B . Purpose of the Analysis
- C. Case Study of Incident Analysis using FRAM
- D. Results of the case analysis using FRAM

IV. Evaluation experiment
- A. Features of FRAM as an accident analysis method
- B . Applicability and impact on security accident analysis.

V. Conclusion

VI. Resilience Engineering and Security by Design



I. INTRODUCTION

- Self-introduction

Tomoko Kaneko, Ph.D. (Informatics)

・Executive R&D Specialist, NTT Data

・Researcher Information technology promotion Agency(IPA) *2016-2019

・Project Associate Professor, National Institute of Informatics（NII） *2021-2022

With Prof. Eric Hollnagel

- Chair, AI/IoT System Safety Symposium
- Chair, Safety & Security Subcommittee, SQiP Study Group, JUSE
- Researcher, Tohoku Koeki University
- Researcher, Cyber Security Research Institute, Tokyo Denki University
- Technical Committee Member, Intelligent Software Engineering Research Group, The Institute of Electronics, Information and Communication Engineers (IEICE)
- Secretary of IT Risk Studies Group, Japan Society for Security Management
- Certified Information Security Auditor (CAIS)

Research Interests: Safety & Security Safety of Machine Learning Systems

- Researcher, Information-technology Promotion Agency, Japan (2016-2019)

https://researchmap.jp/knktmk/(list of research achievements)

1990: Joined the development team for the Pachinko prepaid card incident, which became a social problem.
→ First large-scale security attack in Japan → Bitter experience of not being able to respond in any way

2003-2007: Institutionalized telework as an in-house volunteer → Tried and tested measures to prevent information leaks, conducted remote technology research, assessments, and demonstration experiments, and received the "Telework Promotion Award

2008-2014: Became the first female Ph.D. degree at the Graduate University of Information Security

2016-2019: Wrote "Development Guidelines for a Connected World" and other books, and engaged in the diffusion and development of system theory and resilience engineering of safety in IPA

SEC特別セミナー

破綻を回避するための レジリエンスエンジニアリング

～安全社会実現へのパラダイムシフト～

2017.1.12(木)

特別講演①：**エリック・ホルナゲル 氏**（南デンマーク大学 教授）
『レジリエンスエンジニアリング概説』

特別講演②：**中島 和江 氏**（大阪大学 医学部 教授）
『レジリエントヘルスケア実現に向けたチャレンジ』

パネルディスカッション

モデレータ：兼本 茂 氏（会津大学 教授）

パネリスト：北村 正晴 氏（東北大学 名誉教授）
野本 秀樹 氏（有人宇宙システム株式会社）
中島 和江 氏（大阪大学 医学部 教授）
小松原 明哲 氏（早稲田大学 教授）
古田 一雄 氏（東京大学 教授）
エリック・ホルナゲル 氏（南デンマーク大学 教授）

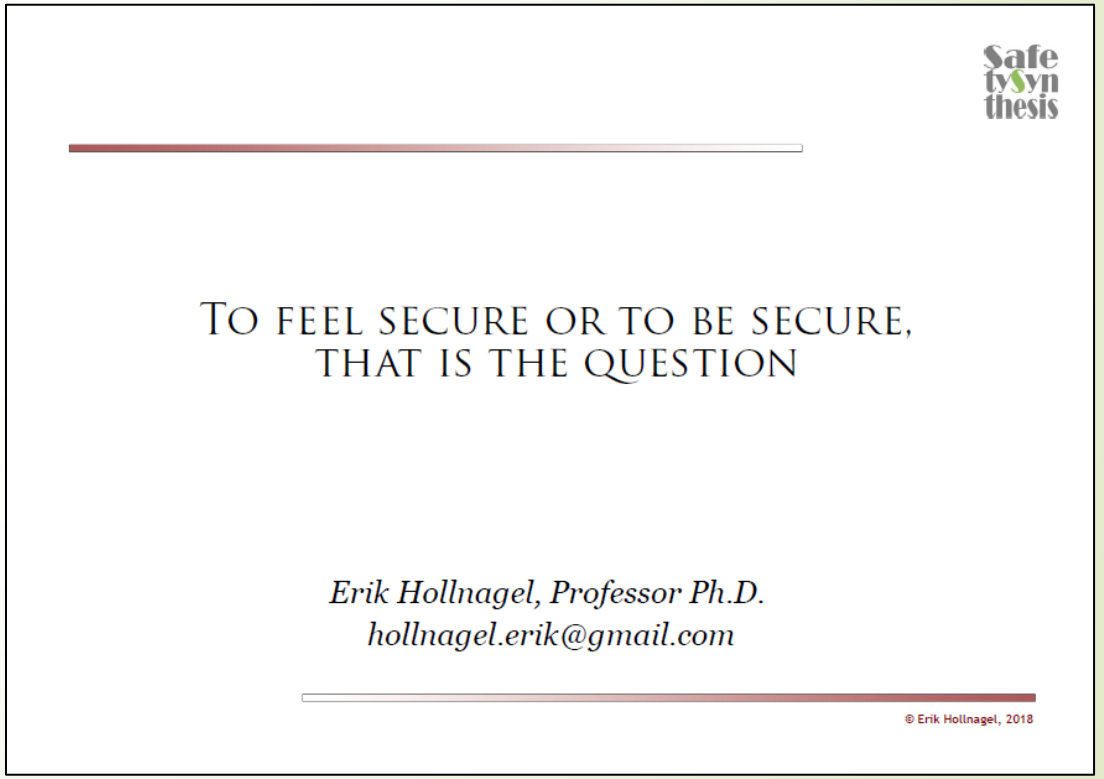
I was a staff member of this Japanese symposium in 2017. After the symposium, I had a chance to talk with Prof. hollnagel and asked him to talk about resilient security sometime.

New Security

@mini FRAMily in Japan 2018

Professor Hollnagel presents the world's first new security concept "Resilient Security" (*)

(*) *"TO FEEL SECURE OR TO BE SECURE, THATA IS THE QUESTION"*
Hollnagel, 2018



1st

2nd

3rd

日時：2019年11月26日（火）
10:00~18:00
場所：国立情報
会議室（東京都

Day 3：2020年11月12日（木）
13:00~16:40（FRAM
Workshop）

Day 5：2021年12月3日（金）
14:00~18:10（FRAM Workshop）

ptimising the
ex
s: using FRAM

r 氏（カーディフ大学

S】"A
is of
Systemic Potentials

I am here to say thank you from
the bottom of my heart.
I really appreciate Prof. Hollnagel
❤♡❤

Dr. Nomoto will give a digest report of this FRAMily2022 at the fourth symposium on November 30.
https://ai-iot-system-safsec.connpass.com/event/246280/

講演者：エリック・ホルナゲル氏（スウェーデン　ヨンショーピ

Resilience engineering argued that it is not multi-layered protective wall security, but the flexibility to change dynamically that enhances security.

Dr. Hollnagel noted that the biggest difference between Safety and Security is the "type" of threats that each has to deal with. Safety deals with Regular Threats (predictable threats such as component failure, control breakdown, etc.). Security, on the other hand, deals with Irregular Threats (threats that cannot be predicted, such as intrusion from unexpected routes).

For known threats, a strong defense wall is effective, and a strong system structure can protect the system from known threats, but it is "nearly impossible" to prepare system defenses in advance against unknown and unpredictable threats.

Resilient security does not add new defenses,
but rather emphasizes the four capabilities of Monitor, Respond, Learn, and Anticipate, as in resilience engineering, to achieve a secure environment by enhancing them as security-enhancing capabilities.

I argue that the four capabilities of Monitor, Respond, Learn, and Anticipate, as in resilience engineering, can be enhanced as security improvement capabilities to achieve a secure environment.

To confirm these claims,
I validated my resilient analysis based on the Functional Resonance Method (FRAM) with a case study of an incident report of a security incident at the National Institute of Advanced Industrial Science and Technology (AIST).

In this incident, unauthorized accesses were sequentially made to both (1) a mail system using cloud services and (2) an internal system built in monolithic form at AIST.

After presenting specific examples of this case study,
I hope to discuss "security and safety," "security by design," and "security resilience“ in the end.

Resilient security does not add new defenses,
but rather emphasizes the four capabilities of Monitor, Respond, Learn, and Anticipate, as in resilience engineering, to achieve a secure environment by enhancing them as security-enhancing capabilities.

I argue that the four capabilities of Monitor, Respond, Learn, and Anticipate, as in resilience engineering, can be enhanced as security improvement capabilities to achieve a secure environment.

Resilience engineering is one of the new safety theories for safely constructing complex socio-technical systems, and the author has been trying to apply resilience engineering to information security.

The National Institute of Advanced Industrial Science and Technology (AIST) has released a "Report on Unauthorized Access to Information Systems of AIST" (hereinafter, Report). An accident analysis by FRAM was conducted for this security incident case by researchers of the SQiP Study Group.

The purpose of this experiment

is to demonstrate the effectiveness of the analysis by extracting and analyzing problems from a different perspective than the traditional security analysis (report conclusions),

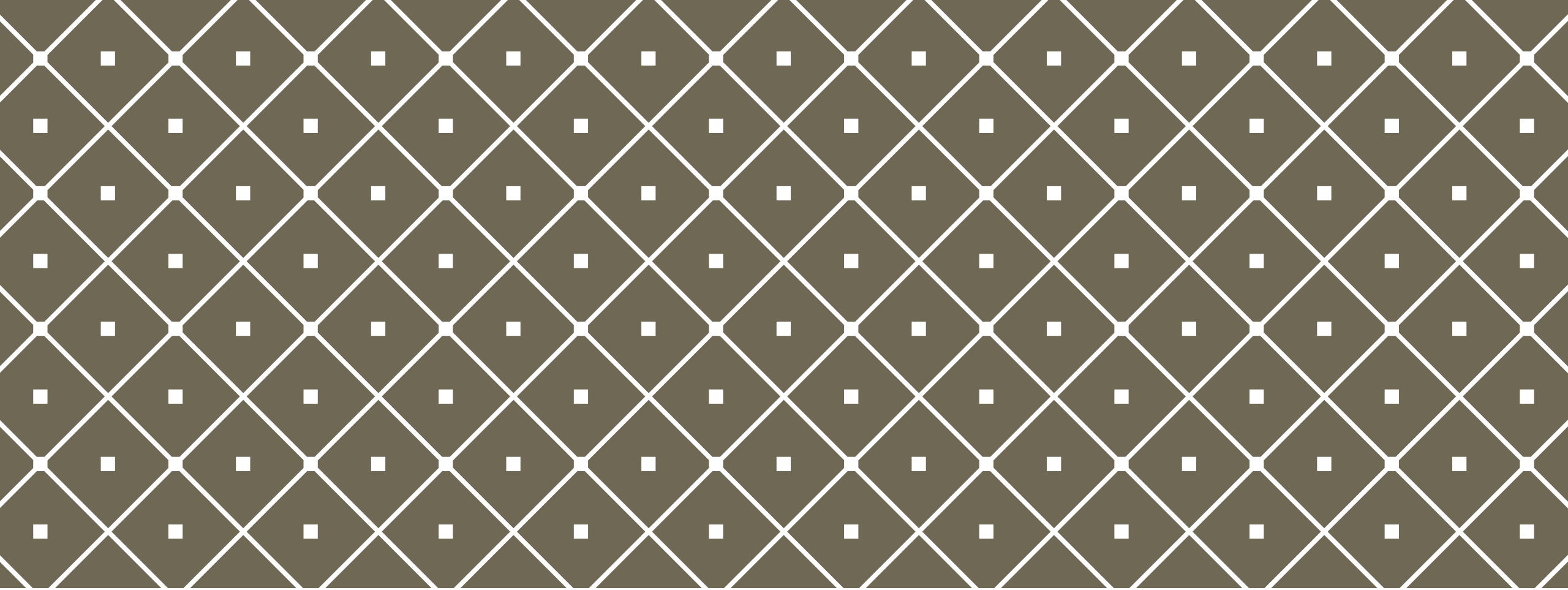
and to identify problems that are not apparent from the report content alone.

Based on this case, the following research questions are set up and verified.

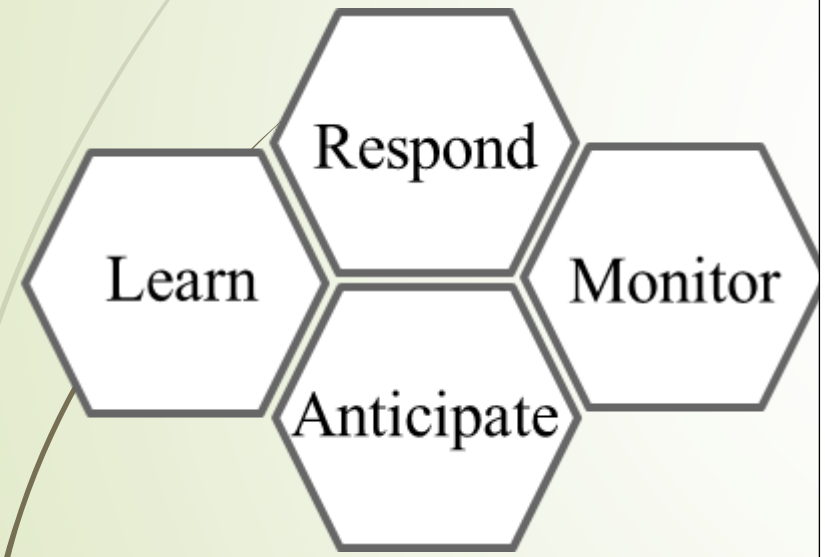
Q1: What are the characteristics of FRAM as an accident analysis method?

Q2: FRAM is a safety accident analysis method, but can it be applied to security accident analysis?

Safety here is being protected against non-malicious hazards, such as accidental errors and failures, while security is being protected against malicious threats.



Ⅱ. RELATED WORK



Monitor: the ability to detect signs of danger

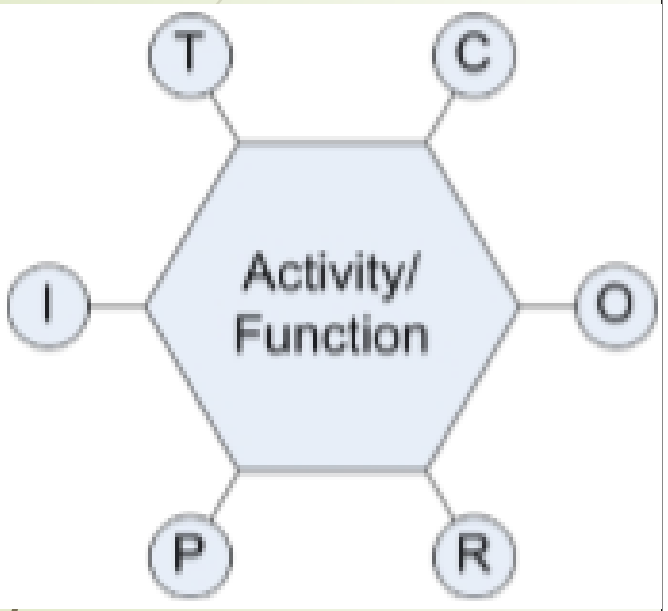
Respond: The ability to react quickly to warning signs

Learn: the ability to learn from past successes and failures

Anticipate: Ability to predict future risks

Four capabilities of Resilience Engineering

These 4 capabilities need to be a safe and secure system.



Input (I) Triggering of the function

Output (O) Output of a function

Preconditions (P) Pre-conditions before function execution

Resources (R) Resources to be consumed or conditions for function execution

Time (T) Time constraints on function execution

Control (C) Conditions that manipulate

Six Aspects of FRAM

So I applied fram analysis to security incidents

III. ANALYSIS AND RESULTS APPLIED TO INFORMATION SECURITY INCIDENTS

Outline of unauthorized access to information systems from outside

Date and time: February 6, 2018
As the main information system of AIST

- Mail systems using cloud services
- unauthorized access to both internal systems that are built on their own.

(1) Stealing the login ID of an employee
(2) Password detection by password trial attack
(3) Illegal offender to internal system using login ID and password of staff
(4) Stepping on internal system servers
(5) stealing or browsing files stored on multiple servers of the mail system and internal system. A series of fraudulent acts were carried out.
(6)Unauthorized access to AIST's information systems.

C. Case Study of Incident Analysis using FRAM

[Step 0] Recognize the purpose of FRAM analysis

FRAM will be used to explain the details of the accident and to generate countermeasure plans for the accident case described in the report by the National Institute of Advanced Industrial Science and Technology.

Based on the results of this experiment, the roles and characteristics of each component that makes up the information system are identified to discuss the characteristics of applying FRAM to the problem.

[Step 1] Identify and describe functions

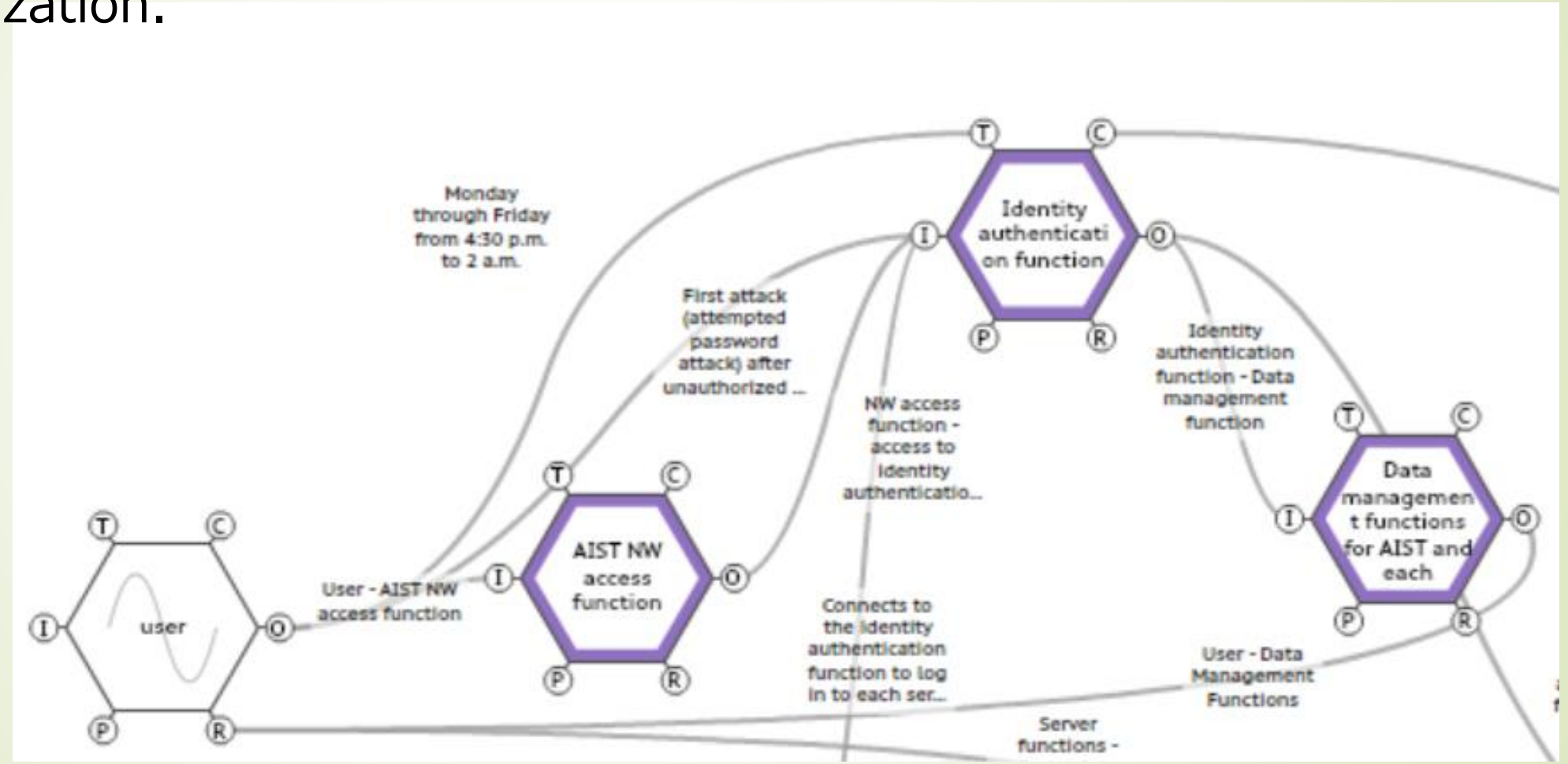
For each component identified in Step 1, extract functions. At this time, if there are functions with similar characteristics in other components, abstract and define them as one function. The abstraction is as follows.

■ Concept of Abstraction

- The information leakage started with an attack on identity authentication, so we will focus on the "identity authentication function" and the "data management function of AIST and each research department".
- The access to AIST's internal NW (business system and servers/NAS of each research department) is focused on as one function as the "AIST NW access function" because the source of the information leak was an external server of ISM X.

[Step 2] Identification of variations

Visualize the defined functions by connecting them to other functions and summarizing them in a FRAM diagram.
The tool for visualization is FMV [6]. FMV [6] is used as a tool for visualization.



[Step 3] Aggregation of fluctuations

The visualized model is looked at from a bird's eye view, and attention is paid to functions with structural characteristics such as a large number of connections and the existence of loops. Among these functions, select the function that is a success factor and designate it as the core function. Conversely, consider whether there are any aspects in which the central function is a weak point.

In this case, the attack path is simulated as it occurred (Fig. 3). As a result, it is checked whether the targeted function in the attack path is the core function. To loosely couple the functions between the business system and the research department, an "inter-site connection function" should be introduced. Specifically, the NWS of the business system and the research department should be separated from each other.

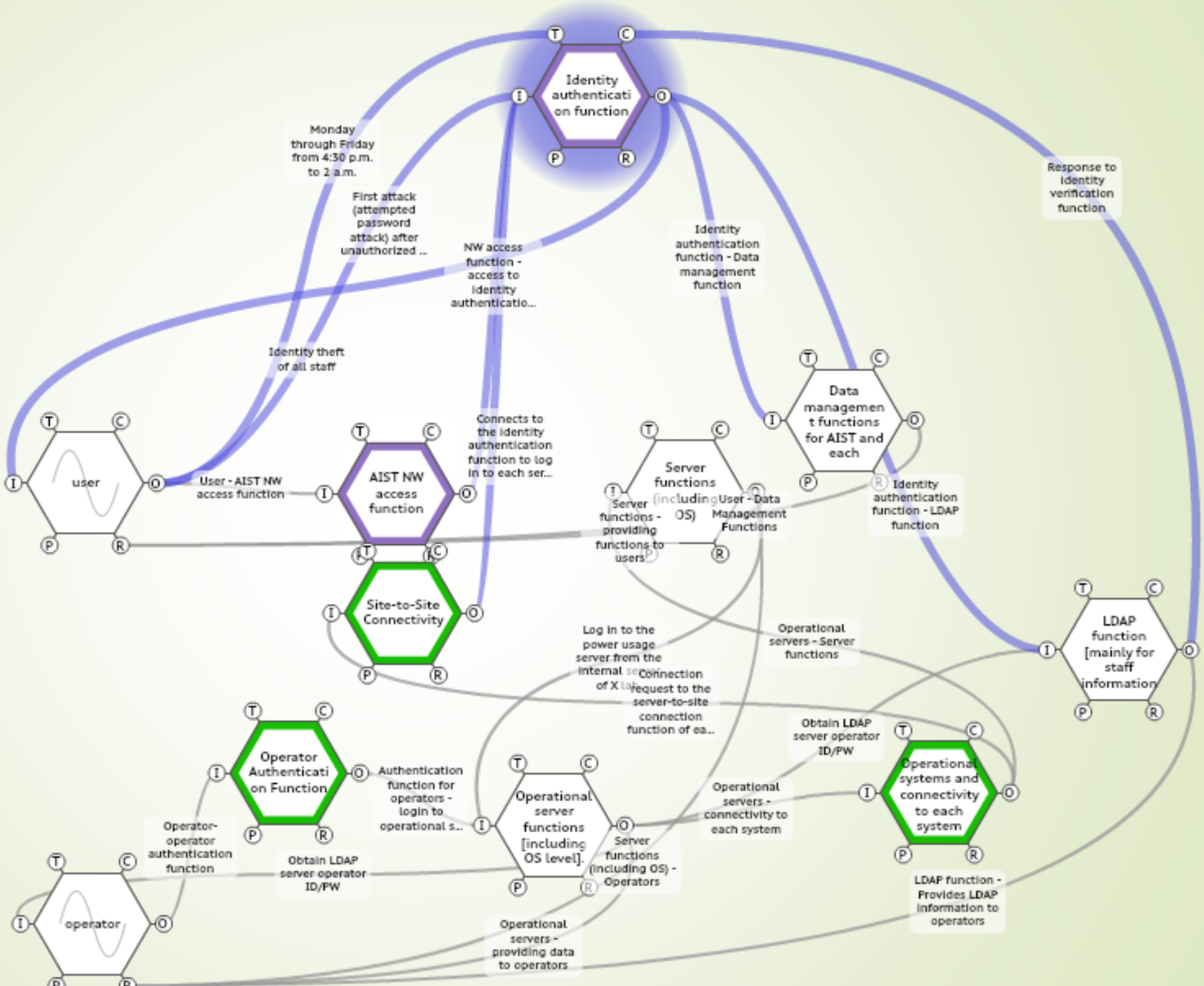


Fig.3. AIST FRAM Analysis Figure(Step3) : Simulate attack paths with FRAM

[Step 4] Results of Analysis

Overlook the model while focusing on the central function defined in Step 3, and add functions for countermeasures to the model so that the central function does not become a weak point. In addition, add resilient countermeasure plans by adding functions that apply to the four capabilities of resilience (Fig. 4).

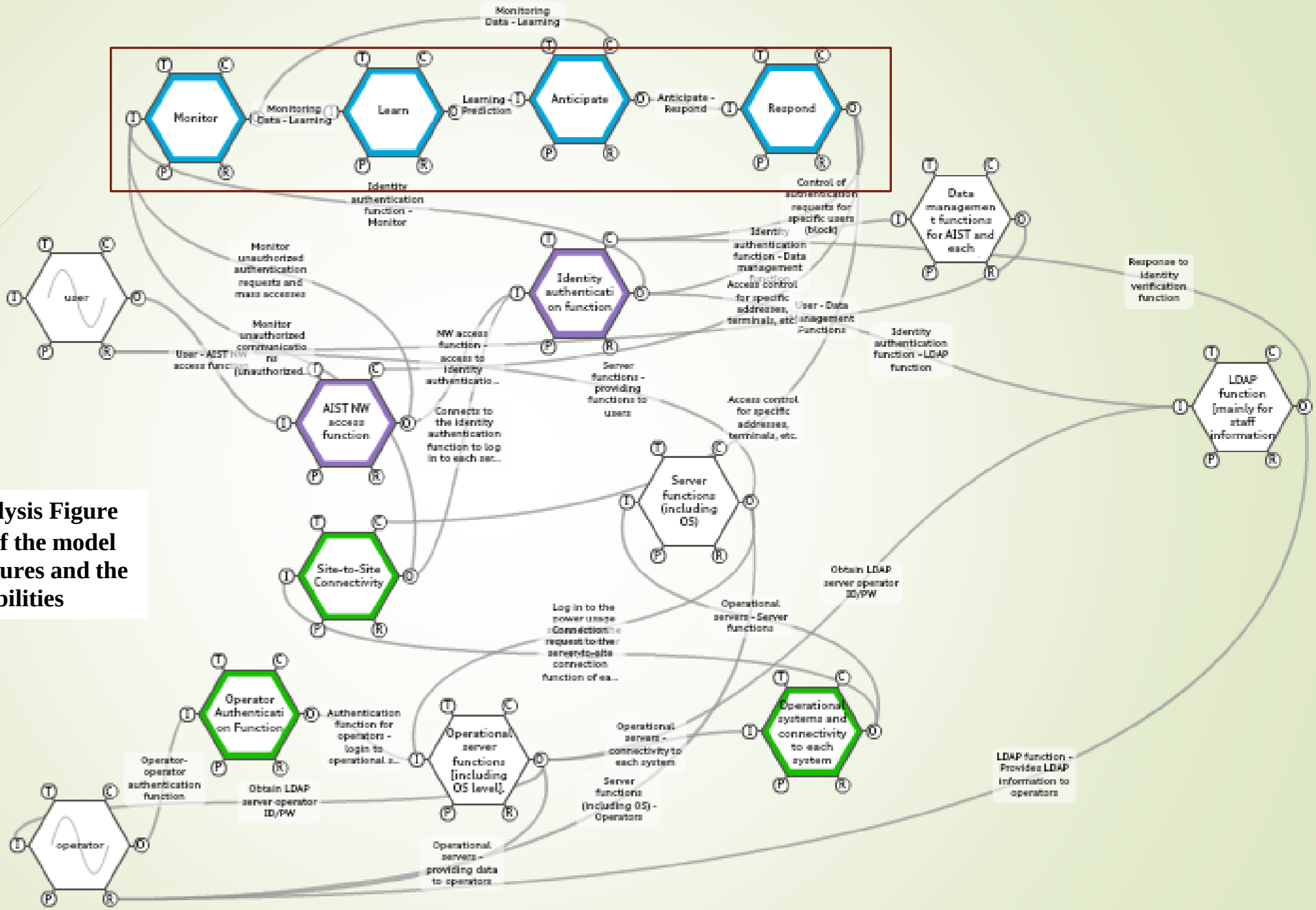


Fig.4. AIST FRAM Analysis Figure (Step5): Re-visualization of the model with proposed countermeasures and the addition of four capabilities

■Concept of Improvement

- To make the operation system loosely coupled with the servers and nodes directly used by users such as staff members, a "connection function from the operating system to each system" (specifically, a FW or NW device between the operation system server and the business system/ servers in each research department) should be introduced between the operating system functions and the functions related to users. Logins from the servers of each research department to the operating system servers/NW devices are prohibited. In addition, an "authentication function for operators" will be introduced.
- Before users such as staff connect to the "Authentication function", they must go through the "AIST NW access function".
- To loosely couple the functions between the business system and the research department, an "inter-site connection function" will be introduced. Specifically, the NWs of the business system and the research department should be separated, and a FW or NW device should be introduced to connect from one research department to the server or business system of another research department.

D. Results of the case analysis using FRAM

Step 1 was conducted to define functions such as identity authentication and data management functions for AIST and each department. Based on the concept of abstraction, several functions were combined into a single function, for example, a function for authenticating the identity of the user when using the mail server, using the business system, and logging into the server managed by each department, each of which has the same characteristics.

Based on the visualization in Step 2, in Step 3, the two functions, the personal authentication function and the data management function for AIST and each department, have many connections with each function, and in fact, users and administrators can access data assets and staff information relatively freely, resulting in success in terms of convenience in operation. Therefore, these two functions were chosen as the core functions.

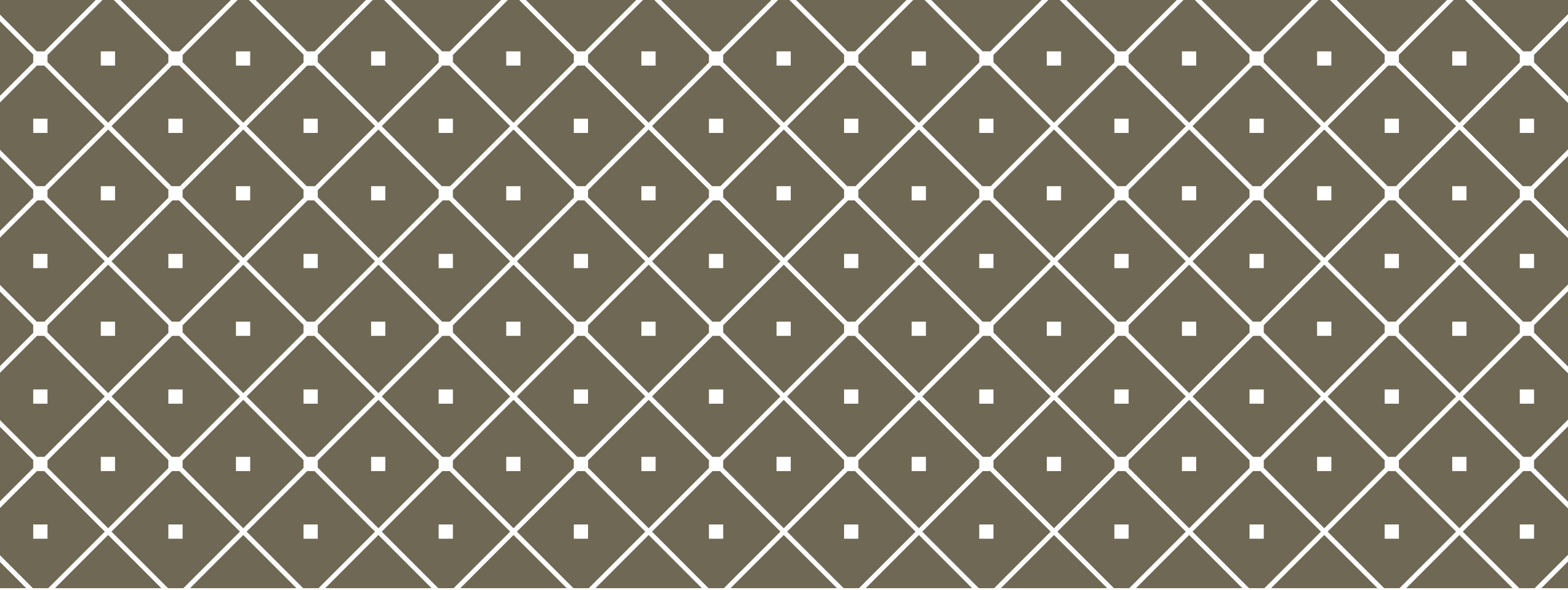
On the other hand, the direct access nature from the Internet of the identity authentication function was a critical path that could be freely attacked by malicious external users. The data management functions of AIST and its divisions could be logged in from servers used by researchers in each research division, and it was possible to log in one after another from server to server. These characteristics made the system vulnerable from an attacker's perspective.

As a result of simulating the attack paths at the time of the incident, it was found that, at many stages, attacks were made against the central function of the system, the identity authentication function, and the data management functions of AIST and each department.

In Step 4, the model was overhauled, and to make a loosely coupled state between the functions of the operating system and the functions directly used by the staff, "a function to connect the operational system to each system" was added as a countermeasure between the functions of the operating system and the functions for staff.

Furthermore, as functions corresponding to "Monitor" and "Learn" among the four capabilities, "Monitor," which takes communication and authentication processing status from each function as input, and "Learn," which learns based on information collected by the monitor and outputs blocking requests to each function according to the results, were added.

I then looked over the model diagram with the added and modified functions and confirmed that the weaknesses of the central functions had been overcome.



IV. Evaluation experiment

A. Features of FRAM as an accident analysis method

Q1: What are the characteristics of FRAM as an accident analysis method?

From the results of the case study analysis using FRAM, we were able to create several countermeasure proposals, including the AIST NW access function.

These countermeasure proposals were created by focusing on the two functions with the largest number of connections in the FRAM model, and by focusing on weak points in the critical paths around these functions and were made possible by the structural visibility unique to FRAM analysis.

From this fact, I believe that FRAM analysis has effective application characteristics for accident analysis of information systems.

B. Applicability and impact on security accident analysis.

Q2: FRAM is a safety accident analysis method, but can it be applied to security accident analysis?

As one of the information security incidents, the AIST report on preventing unauthorized access due to authentication information leakage could be analyzed by FRAM.
Countermeasures or workarounds for the case where IDs and passwords for identity authentication have been compromised before the attack could include the introduction of password strings with formatting conditions and periodic password changes to strengthen them.

However, in the overview of the model in Step 4, no weaknesses or countermeasures for password strength were considered. This is because the FRAM analysis focuses on the continuous interaction between functions, and tends not to focus on processes that occur only once at a specific time, and therefore, the process at the time of password initialization was not incorporated into the model.

In this case, countermeasures can be taken by monitoring and learning.

Input to the learning process as a characteristic pattern of a malicious third party.

Since the learning process has already learned the access pattern by the relevant user, it detects a mismatch between the malicious access pattern and the learned pattern and outputs a blocking request to the identity authentication function.

The above flow prevents unauthorized access due to the leakage of authentication information.

V. Conclusion

In this paper, I introduced resilience engineering and the FRAM methodology. FRAM is a method used to find hazards through the resonance of functions in chaotic situations, such as the behavior of a Mars rover. It is suitable for dynamic control systems.

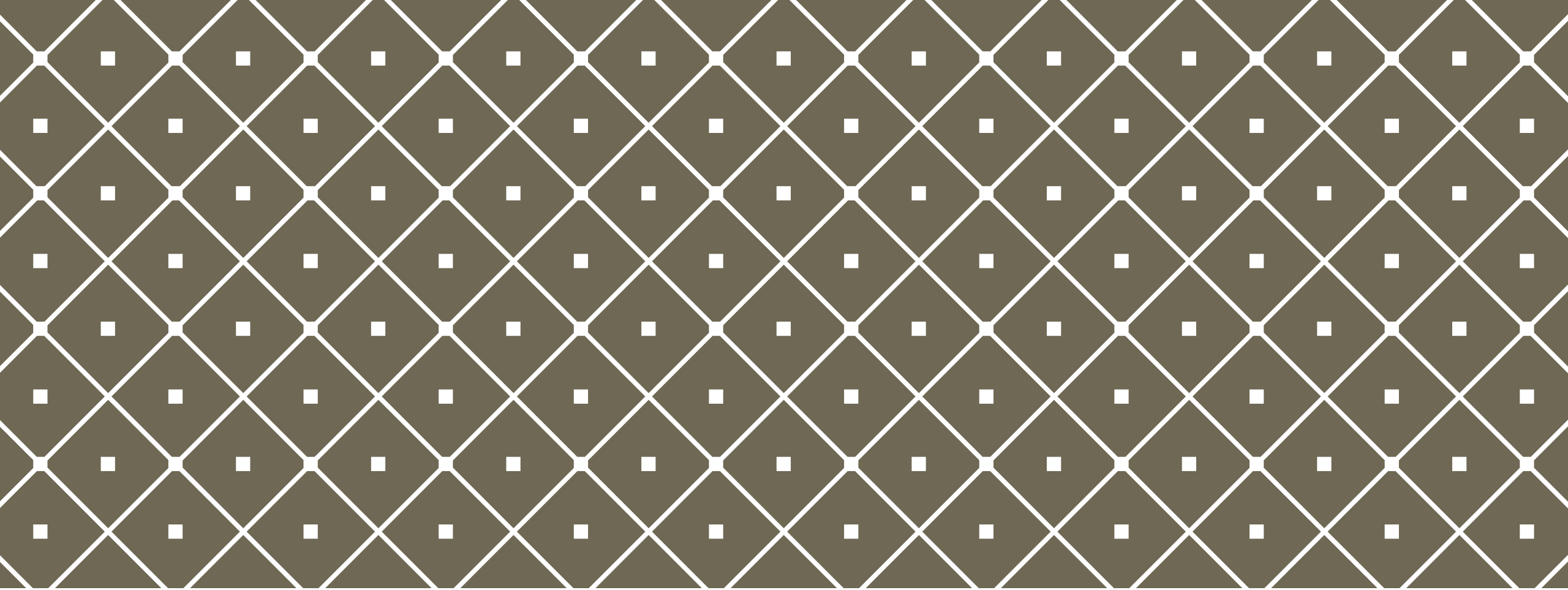
The case study of IT security incident analysis was presented, and it is expected to be applied to dynamic control systems such as automated driving. Because the method will be more effective if it is applied to dynamic control systems, such as automated driving systems.

Q&A

Please feel free to ask me anything.

Acknowledgement

This research was supported by the JST Project for the Creation of a New Society JPMJMI20B8 and the Grant-in-Aid for Scientific Research on "Establishment of a Method for Analyzing Accidents in Socio-Engineering Systems by System Theory (21K21301)".



DISCUSSION: RESILIENCE ENGINEERING AND SECURITY BY DESIGN

THANK YOU FOR YOUR ATTENTION.