Cyber Security Incident Analysis by CAST

2021.6.30

Tomoko Kaneko

National Institute of Informatics(NII)/NTTDATA

NII
National Institute of Informatics

Self-Introduction

Tomoko Kaneko Ph.D(informatics)

- Specially Appointed Associate Professor, National Institute of Informatics(NII), Japan
- Working in NTTDATA inc. as a R&D Engineer
- Worked in Information Promotion Agency (IPA) in 2016-2019
- Certified Auditor of Information Security(CAIS)
- Researcher of Tokyo Denki Univ

Business experience:

- Air-to-Ground Airline communication system
- Pachinko prepaid-card system

(Experience of Security Attack)

Prof. Nancy Leveson

Research topic:

- Safety & Security Engineering
- Secure Development Methodology
- Quality Assurance of AI system
- Engineerable AI @eAI project

<STAMP Research>

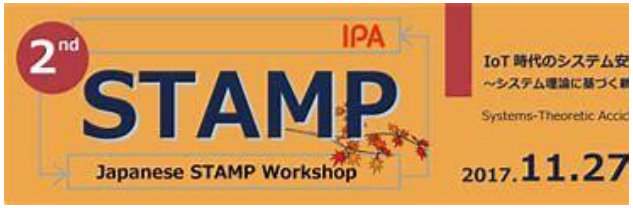
- STPA for Threat analysis
- CAST for Cyber-security Incident
- CAST for IT Operation Accident
- CAST for Autonoumous Driving Accident

History of STAMP Activities in JAPAN

Information Promotion Agency (IPA) promoted STAMP

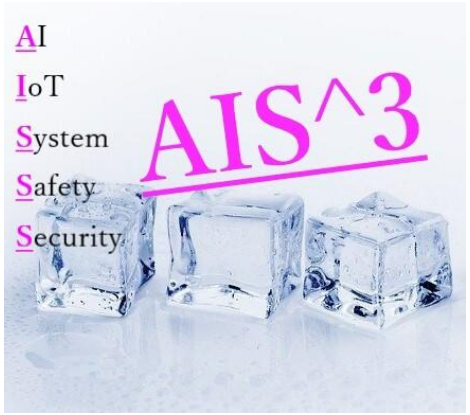
World authority of Safety

- STAMP （System Theoretic Accident Model and Process）
  by Prof. Nancy Leveson



STAMP Workbench

STAMP Support Tool for free



National Institute of Informatics

- The 1st Asian STAMP Workshop
- It was the 5th time STAMP Workshop in JAPAN last November!!
- We expand the scope of participation globally, set up an English session, and hold it as the first STAMP workshop in Asia.
- This year is a virtual workshop, so of course you can participate not only from Asia but also from all over the world. (Most of the participants are Japanese, but there are participants from India, Brazil, Thailand and Canada)..

Keynote Talk

:A Systems Approach to Safety and Cybersecurity: More Effective and Cheaper by Prof. Nancy G. Leveson

CAST Handbook translated in Japanese

http://psas.scripts.mit.edu/home/wp-content/uploads/2021/06/CAST_HandbookJPN.pdf

CAST HANDBOOK:

How to Learn More from Incidents and Accidents

日本語版 Ver. 0. 1

Nancy G. Leveson

Translators

Seiko Shirasaka / KEIO Univ.
Masa Katahira, Naoki Ishihama, Keichi Wada, Yasushi Ueda, Hiroki Umeda, Naoko Okubo, Nico Watanabe / JAXA
Ai Noumi / Sophia Univ.
Tomoko Kaneko / National Institute of Informatics
Yuko Fukushima / Nihon Unisys

MIT Partnership for Systems Approaches to Safety and Security (PSASS)

What's new? Home Research Materials People STAMP Workshop STAMP Tools Contact

Materials

CAST Handbook

The CAST Handbook provides practical guidance to help practitioners learn more from accidents.
- Download CAST Handbook in English
- Download CAST Handbook in Korean (translated by TTA)
- Download CAST Handbook in English-Korean (translated by TTA)
- Download CAST Handbook in Japanese (translated by KEIO Univ., JAXA, Sophia Univ., NII, Nihon Unisys)

STPA Handbook

We have written an STPA Handbook to help practitioners learn to use STPA.
- Download STPA Handbook in English
- Download STPA Handbook in Japanese (translated by JAXA)
- Download STPA Handbook in Chinese (translation by CAUC)
- Download STPA Handbook in Korean (translated by TTA)
- Download STPA Handbook in English-Korean (translated by TTA)

Site Map
- What's new?
- Home
- Research
- Materials (Handbook, Papers, Etc.)
- People
  - PSASS Structure
  - Research Associates, Students, and Visitors
  - Previous students and visitors
- STAMP Workshop
  - 2021 STAMP Workshop General Information
  - 2020 STAMP Workshop Presentations
  - 2019 STAMP Workshop Presentations
  - 2018 STAMP Workshop Presentations
  - 2017 STAMP Workshop Presentations
  - 2016 STAMP Workshop Presentations
  - 2015 Workshop Presentations
  - 2014 STAMP Workshop Presentations
  - 2013 STAMP Workshop

Acknowledgements:
I would like to thank several people who helped to edit this handbook: Dr. John Thomas, Andrew McGregor, Shem Malmquist, Diogo Castilho, and Darren Straker.

謝辞:
日本語版作成にあたり、以下の皆様のご支援に感謝申し上げます。
慶應義塾大学 白坂成功
宇宙航空研究開発機構 片平真史 石濱直樹 和田恵一 植田泰士 梅田浩貴 大久保梨思子 渡邉にこ
上智大学 能美亜衣
国立情報学研究所 金子朋子
日本ユニシス(株) 福島祐子

CAST evaluation experiment

Purpose

- Can the safety tool CAST be applied to the analysis of cybersecurity incidents?
- Is it effective?

- Analyze the incident report of AIST(National Institute of Advanced Industrial Science and Technology)
- The report summarizes the state of damage and causes of unauthorized access to the information system issued in February 2018 and summarizes information security measures.

* Assuming the analysis, the analyst is described in the report. Analyses are carried out after obtaining the results of investigations and other facts as known information.

CAST Procedure1: Assemble Basic Information

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)Than unauthorized access to AIST's information systems report on.

Identify system-level constraints

required to prevent hazards from identified hazards/hazard/safety constraints by gathering basic information

Accident/Incident	Hazard/Threat	Constraint
Unauthorized intrusion into the internal system	There is no defense in the route from the outside to the internal system	There is a defense in the route from the outside to the internal system
	Be attacked from the outside	Not attacked from the outside

Defining the range of systems and analysis involved in the loss

Create questions that require answers to explain why the event occurred

(to Explain what happened without conclusions or criticism)

The event chain and question generation analysis clarify What (what happened) and Why (what you want to clarify to determine the cause) and generate questions that may require answers to the survey results in response to the reasons for each event.

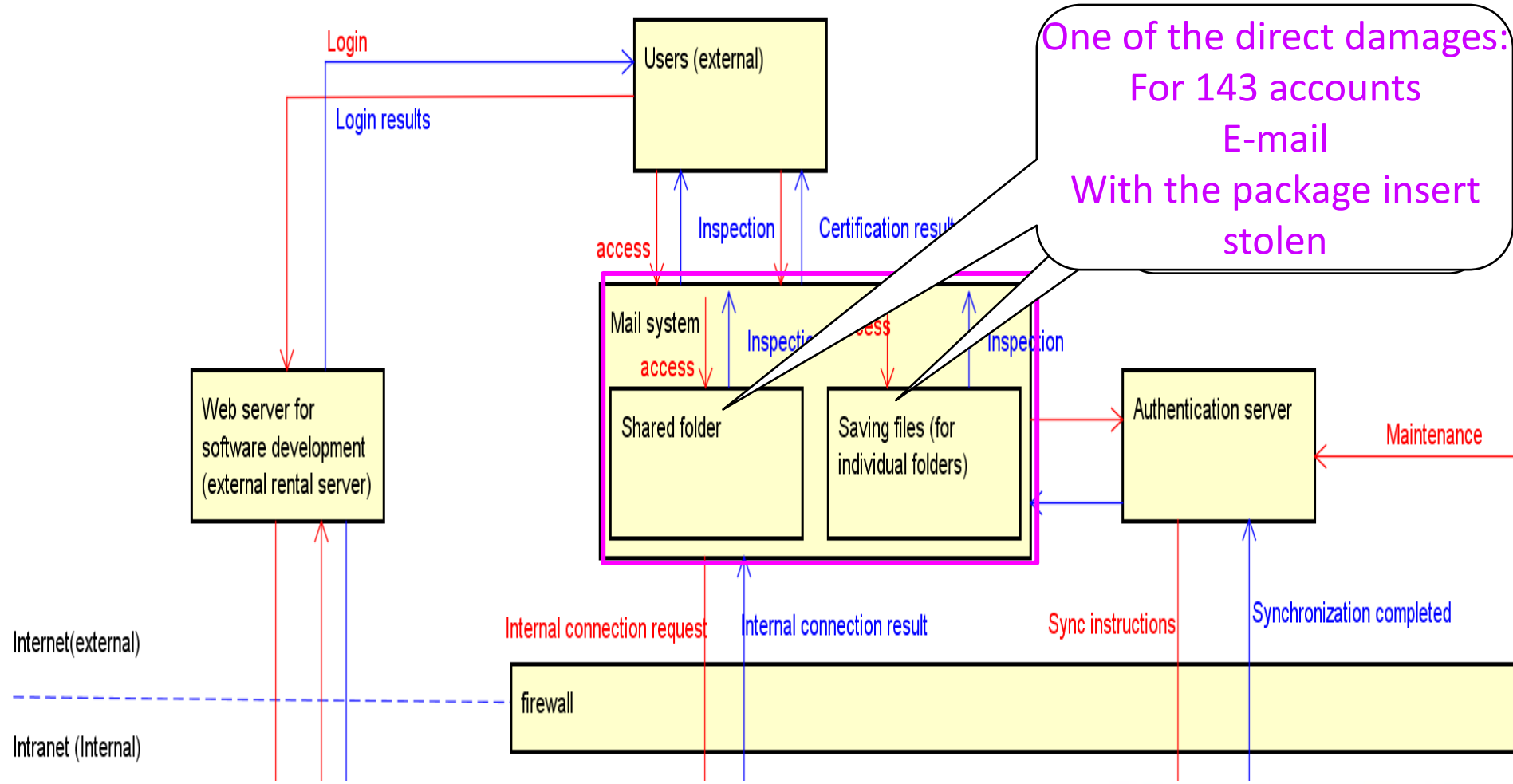
What-Why

It is not

Who-Why analysis

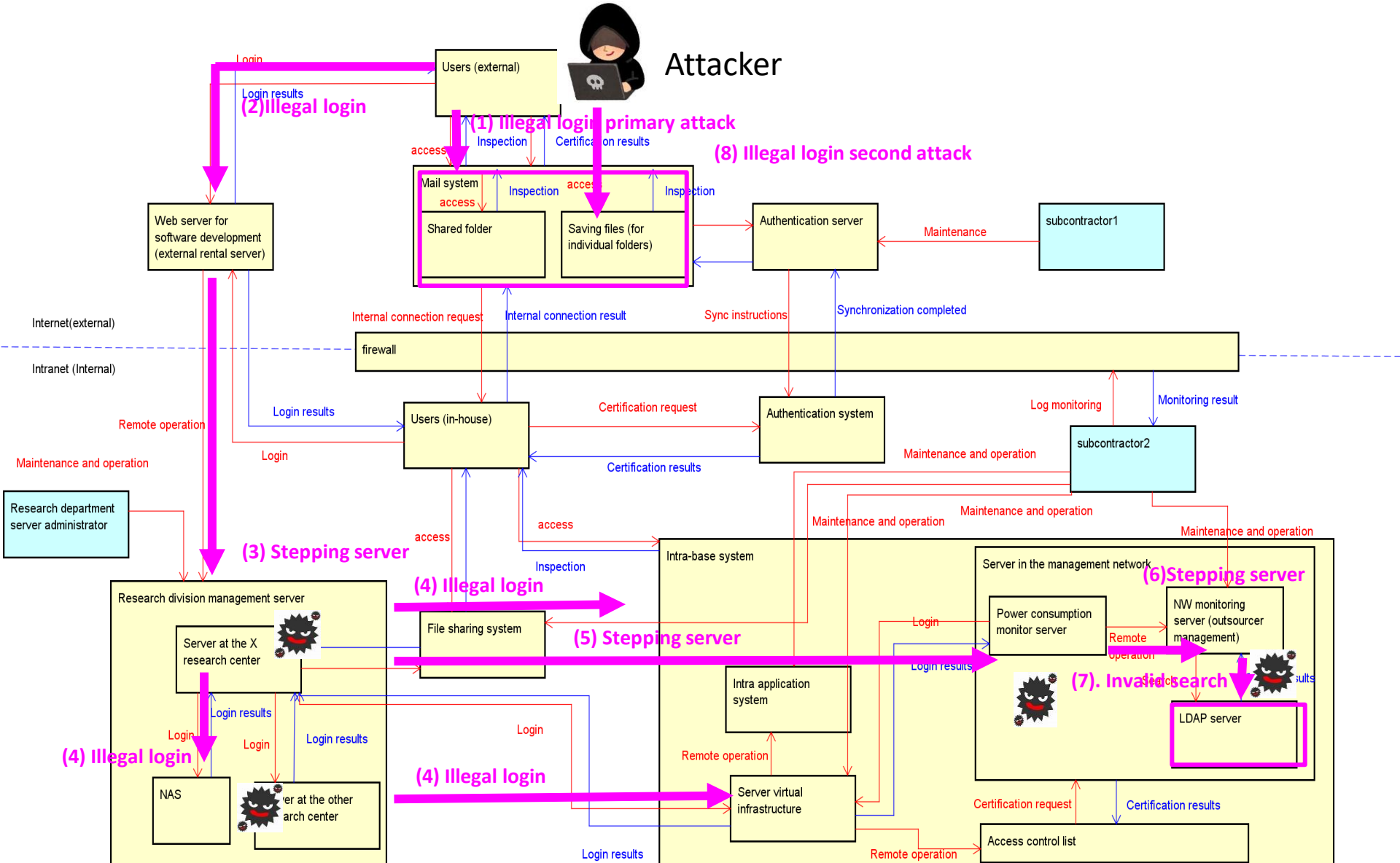
ID	Event occurring in systems and operation and maintenance that is close to the loss （What？What happened	Create questions that may need to be answered to explain why each event occurred （Why？Desired to clarify the cause of the accident.
1	<Accident 01> An attempted password attack (Blue Force attack) was carried out on an authentication server built on an external network.	<Detection and analysis> Q1-1. Why did you not detect a password attempt attack? <Prepare> Q1-2. Why was the authentication server built in an external network? Was the risk considered? Q1-3. Why was the address of the authentication

Create a Control Structure for system and operational maintenance



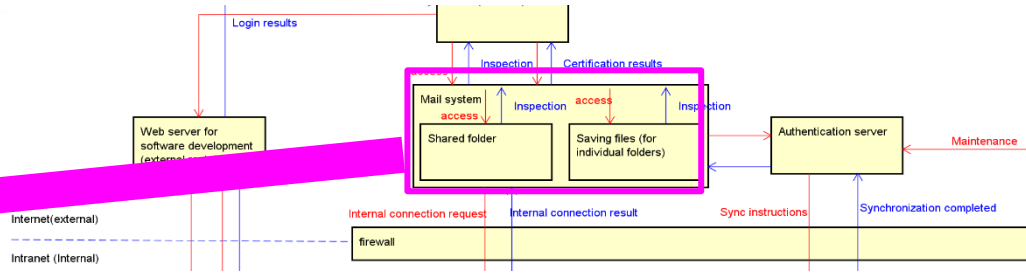
Modeling existing control structures

You can follow the flow of cyber security attacks with CS diagram components, control actions, and feedback flow.



Analysis at the Physical component level

Example of Mail system



<Responsibility for security>

・Collate user ID and password on the authentication server and grant access permissions only to users whose matching result matches

<Unsecure control actions>

(1) Nothing was done for a login attempt failure of the same user ID. Accessing

<Process/Mental Model Defects>

(1) suspicious password attempts were not included in the scope of the Integrated Network Monitoring. There was no control over

<Decision-Making Situations and Background>

(1) The authentication server was managed by another maintenance contractor and was located outside the AIST network.

Analysis at the abstract component level

(Abstract Events)	Responsibility for safety	Unsafe control actions
Unauthorized access to the mail	・The authentication server matches the login ID and password	・For multiple automated login attempts, the matching result was successfully returned. ・Illegal login information was used.

An abstract event is not a component alone, but an event involving multiple components and is analyzed based on four perspectives:
safety responsibility, unsafe control actions, process/mental model defects, and decision-making situations and backgrounds.

System overview analysis

Analyze system impact from 186 defects

The results of the experiment

Comparison with AIST report

Cause of the damage		AIST	CAST
(1) System and equipment problems	Mail system login method	○	◎
	External sites that were associated with internal servers	○	◎
	wide-area, flat internal network	○	○
	Insufficient monitoring of internal networks	○	○
	Existence of an administrative network server without access restrictions	○	◎
	Vulnerability of information devices	○	○
2) Password and encryption key management and strength issues		○	◎
(3) Problems with the management of the subcontractor		○	○
4) Management Issues		○	◎

CAST can find more concrete cause of damage than AIST report.

Conclusion

Can CAST be applied to the analysis of cyber security incidents?

→Yes ！ ！

→ However, it can be used, but it is necessary to consider the difference between safety and security terms and targets.

Is it effective?

→Definitely Yes ！ ！

Let's use it together and realize safety and security!

ACKNOWLEDGMENTS

The experiment in this presentation was done with the researchers of Japan Society for Science and Technology Software Quality Management Study Group Safety & Security WG.

I would like to express sincere gratitude to the researchers and eAI project.

Q&A

Thank you for your attention