

セキュリティ専門家人狼 (JIN-ROH)

SECWEARE  
WOLF

**JNSA** 特定非営利活動法人  
日本ネットワークセキュリティ協会  
Japan Network Security Association

March 9, 2018 (2nd Edition)

# Table of Contents

**1. What is the goal of this game?**

**2. Story**

**3. Game instructions and rules**

**4. Gameplay and strategies**

**5. For even more learning...**

\*The scripts necessary to progress through the game are listed on slides 41-48.

# The game has three goals #1

The first goal is to lower the learning threshold.



You can learn and remember difficult technical terms while playing.



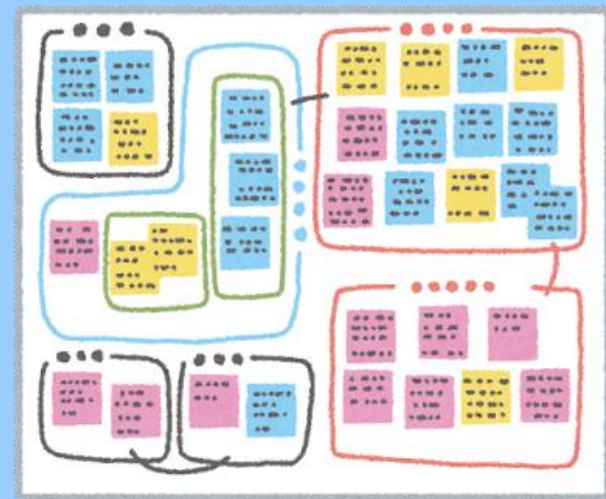
You can learn the roles necessary for a cybersecurity team.

# The game has three goals #2

The second goal is to learn how to communicate.



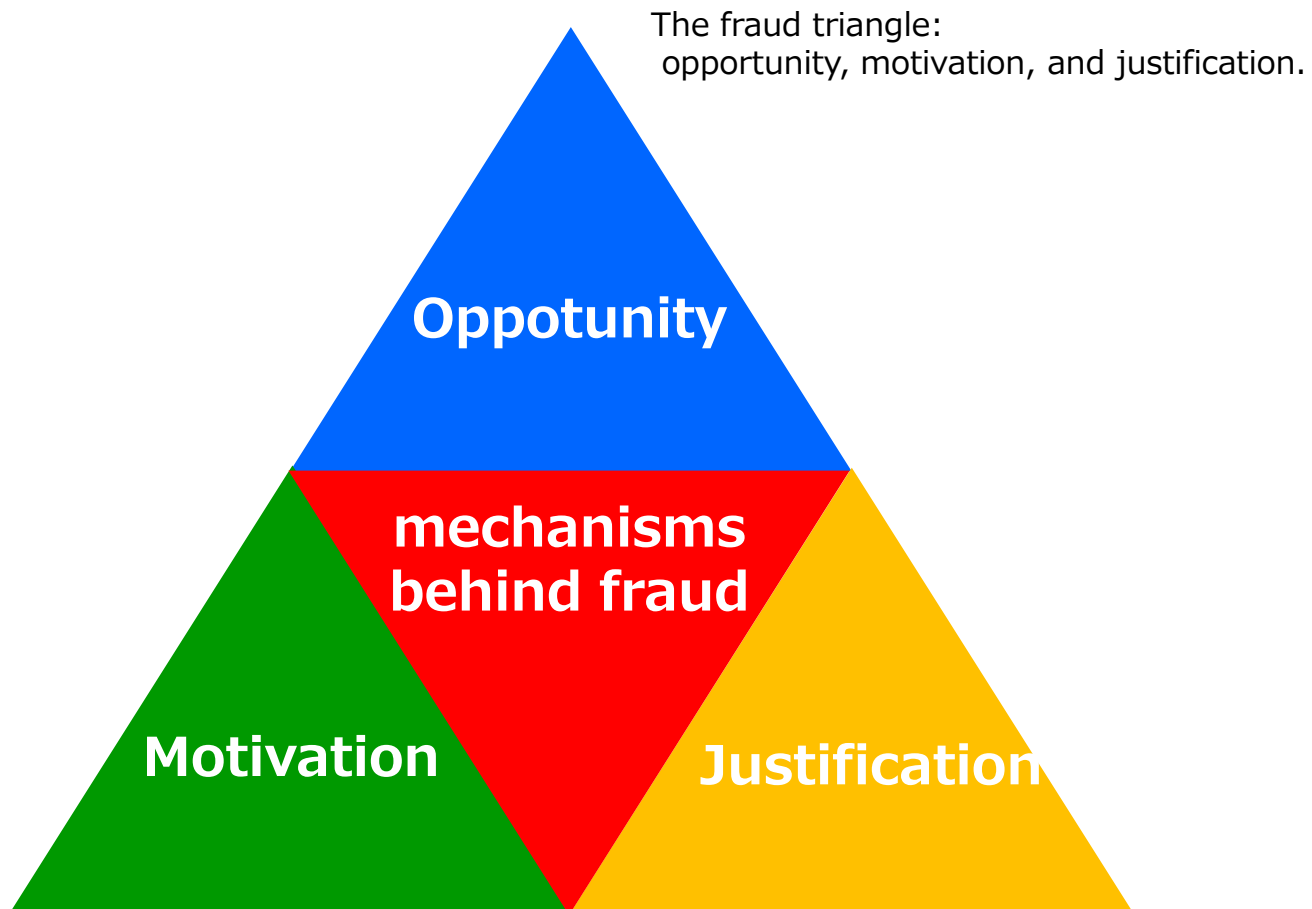
Players search for the necessary information by switching between jargon and normal speech.



Manage your limited information and use logic to discover the concealed information.

# The game has three goals #3

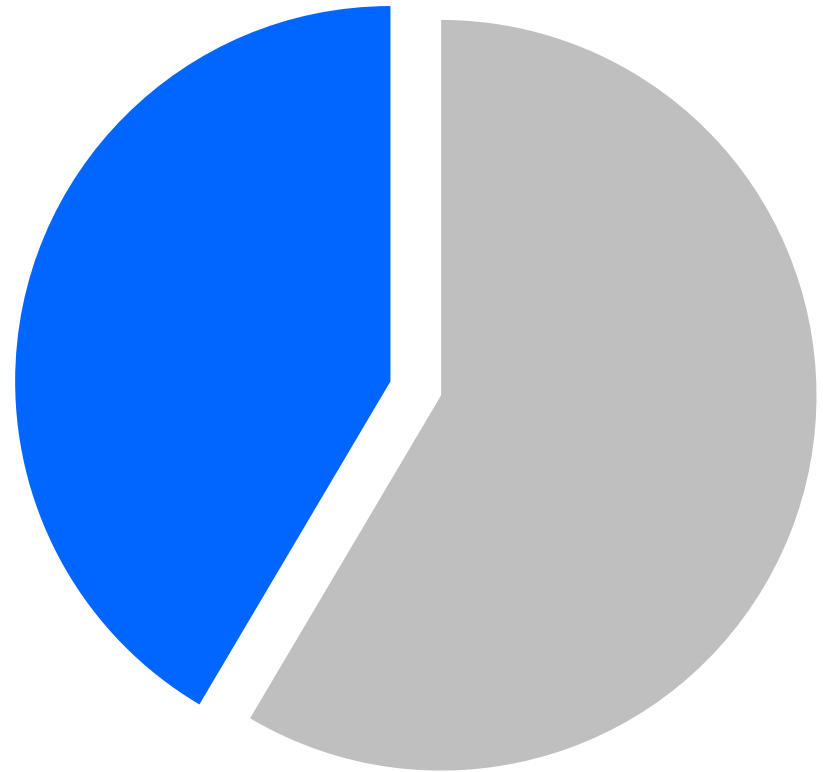
The third goal is learn the mechanisms behind fraud.



# Internal fraud report

The belief that human nature is fundamentally good does not work in internal fraud.

**Internal fraud  
due to bad  
intentions  
42.0%**



\*Quotation :

<https://www.ipa.go.jp/security/fy27/reports/insider/>

\*Make a graph using the published data

**Gameplay**  
**Before that...**



# What is “Werewolf”?

- Werewolf is a traditional analog card game in which players discover the truth about each other through conversation
  - In 1986, Dmitry Davidoff created the game Mafia as part in the psychology department of the Moscow State University of the then-USSR, and it's said that this is the first model of this game..
- Various arrangements have gone on sale.



Photo: Social Deduction Game Corner



Reference : 『ミラズホロウの人狼』, Dmitry Davidoff & Hervé Marly & Philippe des Pallières



# Examples of using the werewolf game



**素で出会う就活。**

就職活動で固い面談やテストをやっていると、無駄に緊張しませんか。そういう状態では、個々人の本来の力が発揮できません。また、ありのままの状態で個々人と企業のマッチングをしないと、入社後の不一致が起こりやすくなってしまいます。

素の状態でお互いを知りたい。その上で、ともに歩む仲間を探したい。

また、素で出会ったものを無駄にしないため、人狼で優秀な戦略を実践した人は一次選考を免除します。ぜひ会話型推理ゲームを楽しんでください。

**人狼 2015 採用**

新卒採用にゲームを導入！



情報処理学会第77回全国大会  
4ZC-03

**対話型ゲーム「人狼」を活用したグループディスカッションの練習方法の提案**

古川 裕賢<sup>1</sup> 中村 英夫<sup>2</sup> 山崎 善行<sup>3</sup>  
<sup>1</sup> 東京工科大学<sup>2</sup> 神奈川大学<sup>3</sup>

**1. はじめに**  
近年、就職活動の場において特定のテーマについて討論し、その結果や議論を評価するグループディスカッションを課する企業が増えている。しかし、就職活動の場にはたいてい対話型ゲームが少なく、評価が必ずしも公平であるとは言い難いという懸念がある。本論文では、対話型ゲーム「人狼」を用いて、就職活動の場でも活用できるグループディスカッションの練習方法を提案する。

**2. 人狼の概要**  
2.1. 人狼のルール  
グループディスカッションの練習を目的として、就職活動の場でも活用できる対話型ゲーム「人狼」を提案する。人狼は、プレイヤーがそれぞれ異なる役割を担い、議論を通じて自分の役割を果たすというゲームである。プレイヤーは、議論を通じて自分の役割を果たすために、他のプレイヤーの発言を聞き、自分の発言を調整する必要がある。人狼は、議論を通じて自分の役割を果たすために、他のプレイヤーの発言を聞き、自分の発言を調整する必要がある。

**3. 人狼の活用方法**  
3.1. 人狼の活用方法  
人狼は、就職活動の場でも活用できる対話型ゲームである。プレイヤーは、議論を通じて自分の役割を果たすために、他のプレイヤーの発言を聞き、自分の発言を調整する必要がある。人狼は、議論を通じて自分の役割を果たすために、他のプレイヤーの発言を聞き、自分の発言を調整する必要がある。

- Players make decisions during the werewolf game
- Measure communication training effectiveness through the werewolf game
- Propose an interactive werewolf game as a practice method for group discussions

Searchfield Inc. :  
Plant a werewolf among job applicants

A hot research topic for different academic fields



**Story**

# Story



A machine manufacturer that mainly works in B2B

Established in 2003

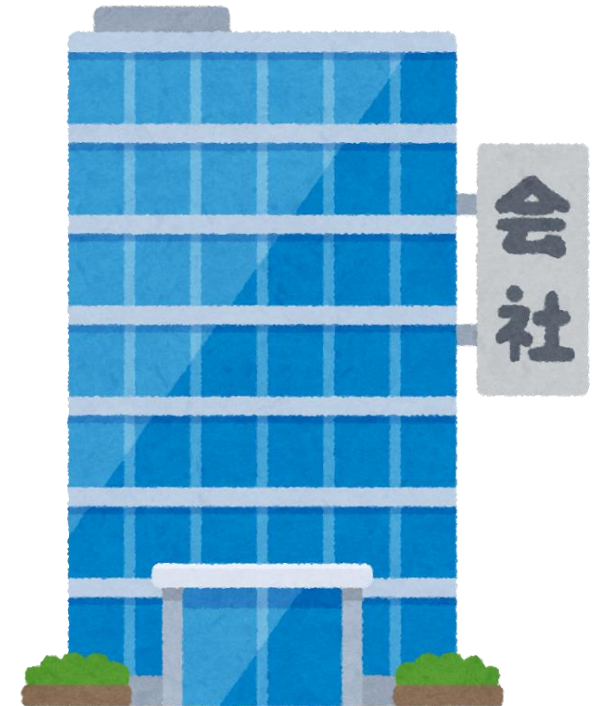
Yearly sales: 120 billion yen

14,000 employees

When the company was first established, it grew rapidly due to domestic demand for its strong technological strength.

However, the company's production hit its peak in 2008 and dropped sharply.

After that, international demand grew, leading to an improvement in performance.



# Story: Signs of fraud

## Worsening of the internal environment

- Unenforced rotation of human resources
- Decline in functional regulations due to the diversification of Recruitment
- Constant excess overwork
- Cycling between hiring and firing

### <Disparity between employees>

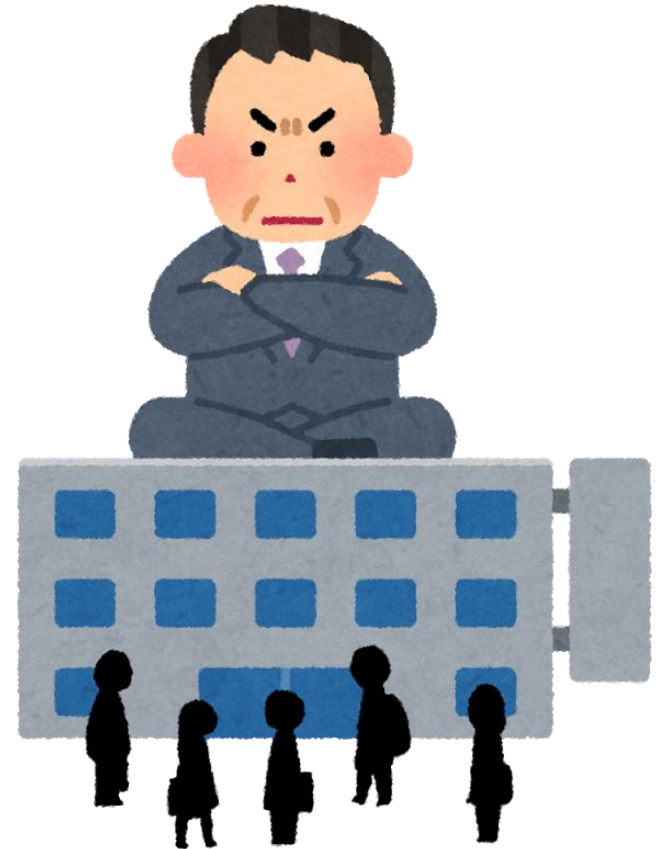
- Young management candidates aggressively being sent overseas
- Conceited senior employees dragging down the organization
- Superior departments and unnecessary departments
- Local employees of international subsidiary companies with different business manners



# Story: Signs of fraud

## Worsening of business management

- Intensification of industrial competition
- Unclear attitudes from administration
- Surrounded by yes-men
- High demands from stakeholders
- Delay in handling commands
- Inspections not being performed properly



# Transformation Time

Please think of the answers to these questions with the game's story in mind.

\*Decide on your answers before you take the card that tells you your job position.

Q1. How long have you been working at the company?

Senior employee (10-14 years)

Regular employee (5-9 years)

New generation employee (less than 1 year to 4 years)

Q2. What department do you belong to?

A superior department

Back office (administration)

An unnecessary department

Q4. How has your overtime been lately?

A little busy

No overtime lately (off-period)

May have gone over my limit



# Game setting:

## An explosion of dissatisfaction



### Lack of honesty

- Dissatisfaction with how one is treated
- Grudges towards the organization or bosses
- Black Hat Hackers in conspiracy

### An explosive rise in corrupt employees!




# Cyber Crime Team





# CSIRT Team, the opposition

**Notification Member**



**CSIRT Team**

Notification Members transmit information to the team and, when heavily influenced, adjust information for each specialist.

Japan Network Security Association.

**Forensic Engineer**



**CSIRT Team**

Forensic Engineers investigate the source of problems and sort through electronic information to discover evidence.

Japan Network Security Association.

**Researcher**



**CSIRT Team**

Researchers collect information, discover abnormalities in the system, and analyze the effects of the abnormalities.

Japan Network Security Association.

**Commander**



**CSIRT Team**

Commanders take control of the group after a problem appears and report important information to their team members.

Japan Network Security Association.

# Necessary employment conditions to execute roles

- The game is played based on assumed employment skills.



## ■ Assumed employment skills

- Knowledge of OS, commands, system files, programming languages, and logic
- Knowledge of vulnerability diagnoses.

# Necessary employment conditions to execute roles

- The game is played based on assumed employment skills.



## ■ Assumed employment skills

- Knowledge of basic security
- Media literacy to keep members from accepting news at face value
- The ability to properly read English

# Necessary employment conditions to execute roles

- The game is played based on assumed employment skills.



## ■ Assumed employment skills

- The ability to control systems when they fail
- Knowledge of the company's security architecture and business
- Skills proficient enough to communicate with management



# Game Story

*The corruption in white collar employees never ends...*

One night, corrupt employees illegally pilfered company secrets. They were dissatisfied with the way the company treated its employees and committed the crime with the help of black hat hackers. The corrupt employees try to pin the blame on those who hurt their self-esteem and continue to commit crimes each night.

Innocent employees are fired one after another...Just who are the corrupt employees?



# Game Story



## *Investigation and Interrogation of Suspects*

After the chain of crimes, the company's managers decided to create an investigative team called CSIRT, filled with security specialists who each had various specializations. The CSIRT Team set out to investigate and interrogate suspects.

In order to bring public order back to the company, the CSIRT Team made the harsh decision to lay off one person each day. Will they be able to eliminate all of the corruption and bring order back to the company?



セキュリティ専門家人狼 (JIN-ROH)

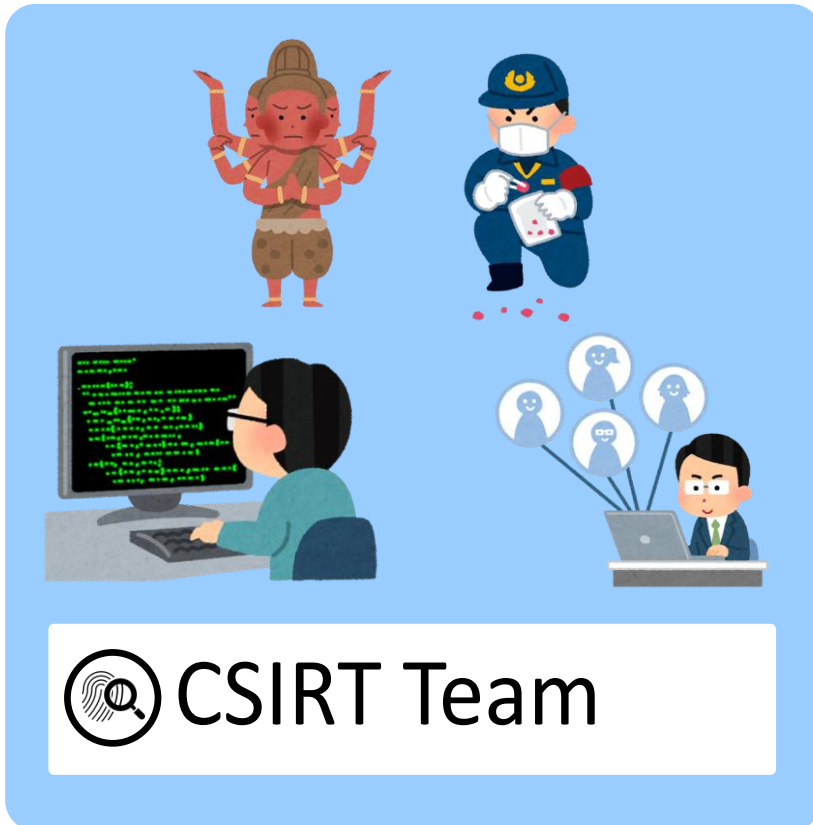
SECURE  
WOLF

# Rules



# The goal is for your team to win.

- Even if you've been dismissed from your team, if it wins, you also win.



# Conditions for Victory

## Conditions for the CSIRT Team to win

If the corrupt employees committing fraud due to dissatisfaction with their treatment within the company are found and dismissed, the CSIRT team wins.



Dismissal Dismissal



Dismissal

Dismissal

Dismissal

## Conditions for the Cyber Crime Team to win

If the number of corrupt employees committing fraud are the same as the number of CSIRT Team members, then the organization has been destroyed and the Cyber Crime Team wins.



Dismissal

Dismissal

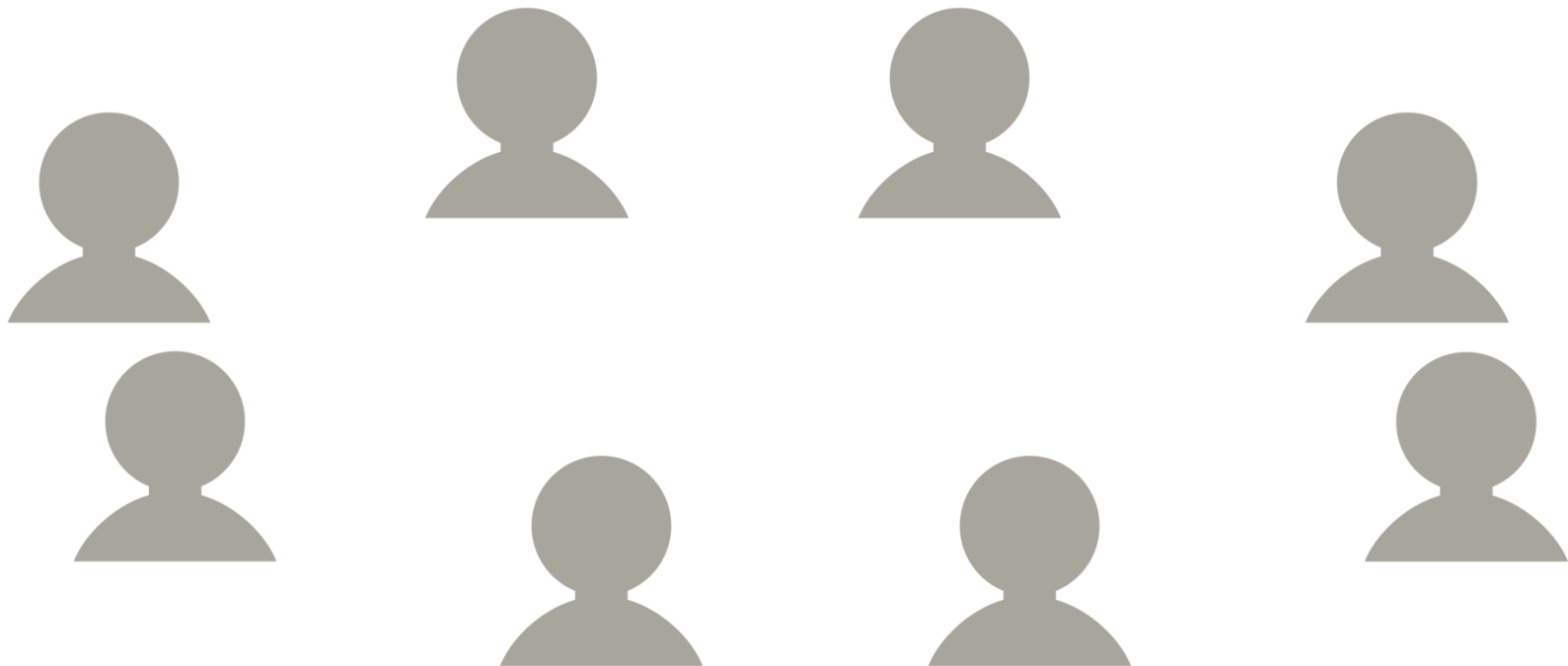


Dismissal

Dismissal

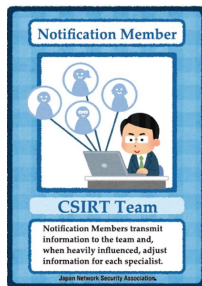
# Create Game Groups

- The game groups will be in circles.



# Confirm the Roles

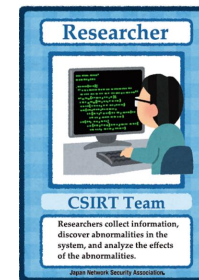
- Announce the combinations of this round (10 people, 1 team)



×4人



×1人



×1人



×1人



×1人



×2人

If there are uneven numbers, fix it by assigning roles like “one corrupt employee,” “one forensic engineer,” “(remaining number) notification members”

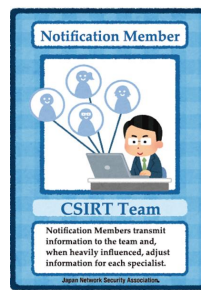
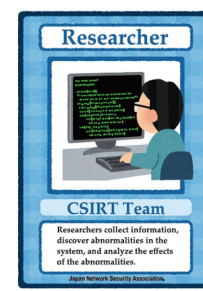
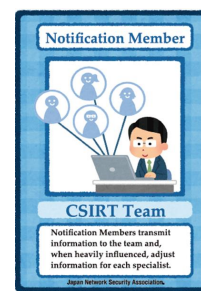
# Distribute Job Position Cards

- Each person gets one card.



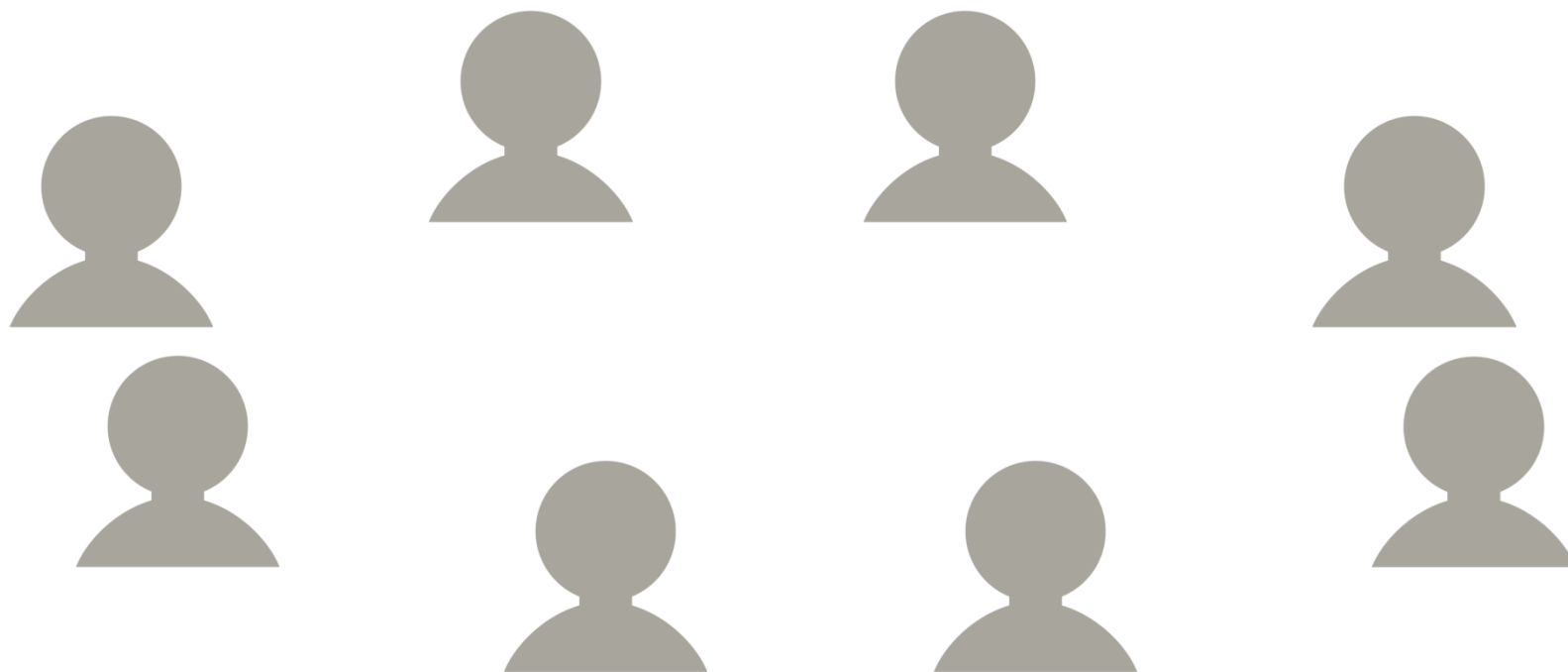
# Confirm Job Position Cards

- Make sure that the players have not revealed their job positions.



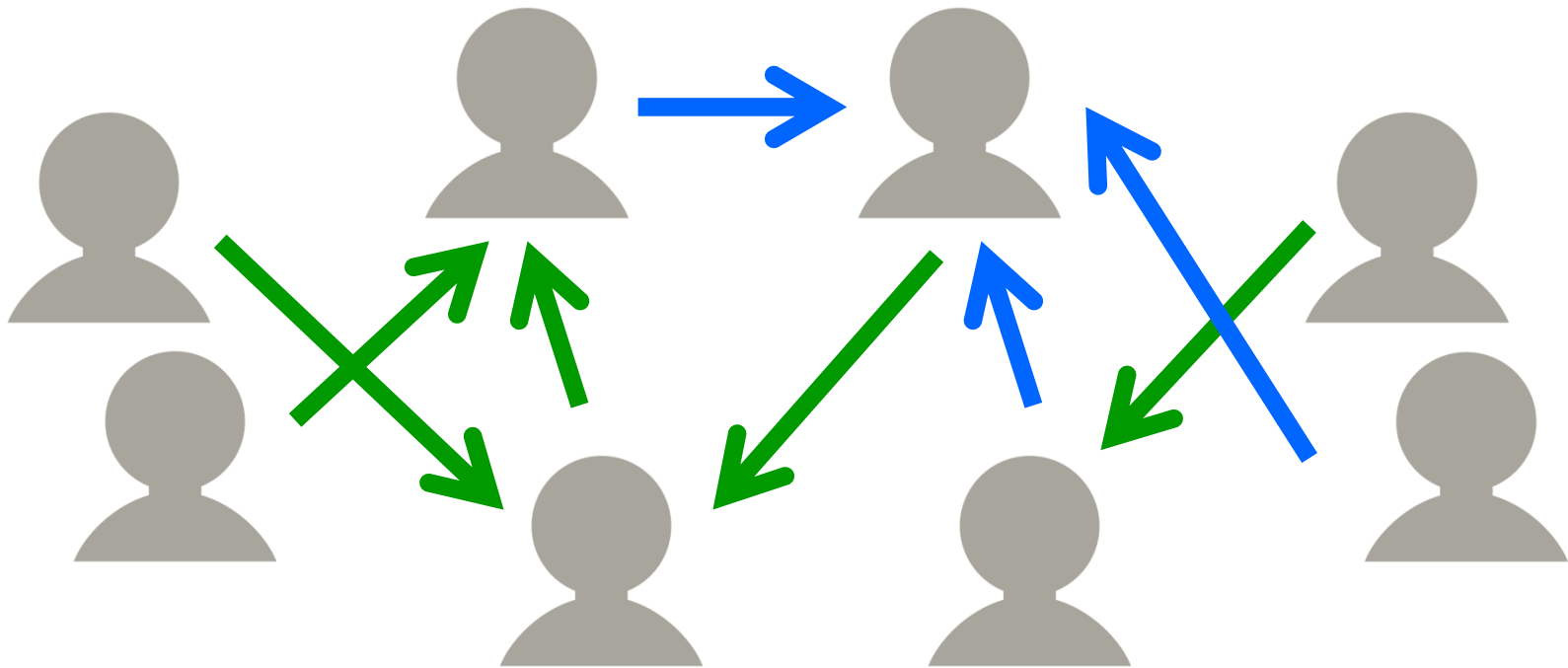
# Suspect Interrogation

- CSIRT members will guess who the unhappy employees are through interrogations.
- The corrupt employees will participate in discussions in a non-suspicious manner.



# Investigation: Deciding the Dismissal

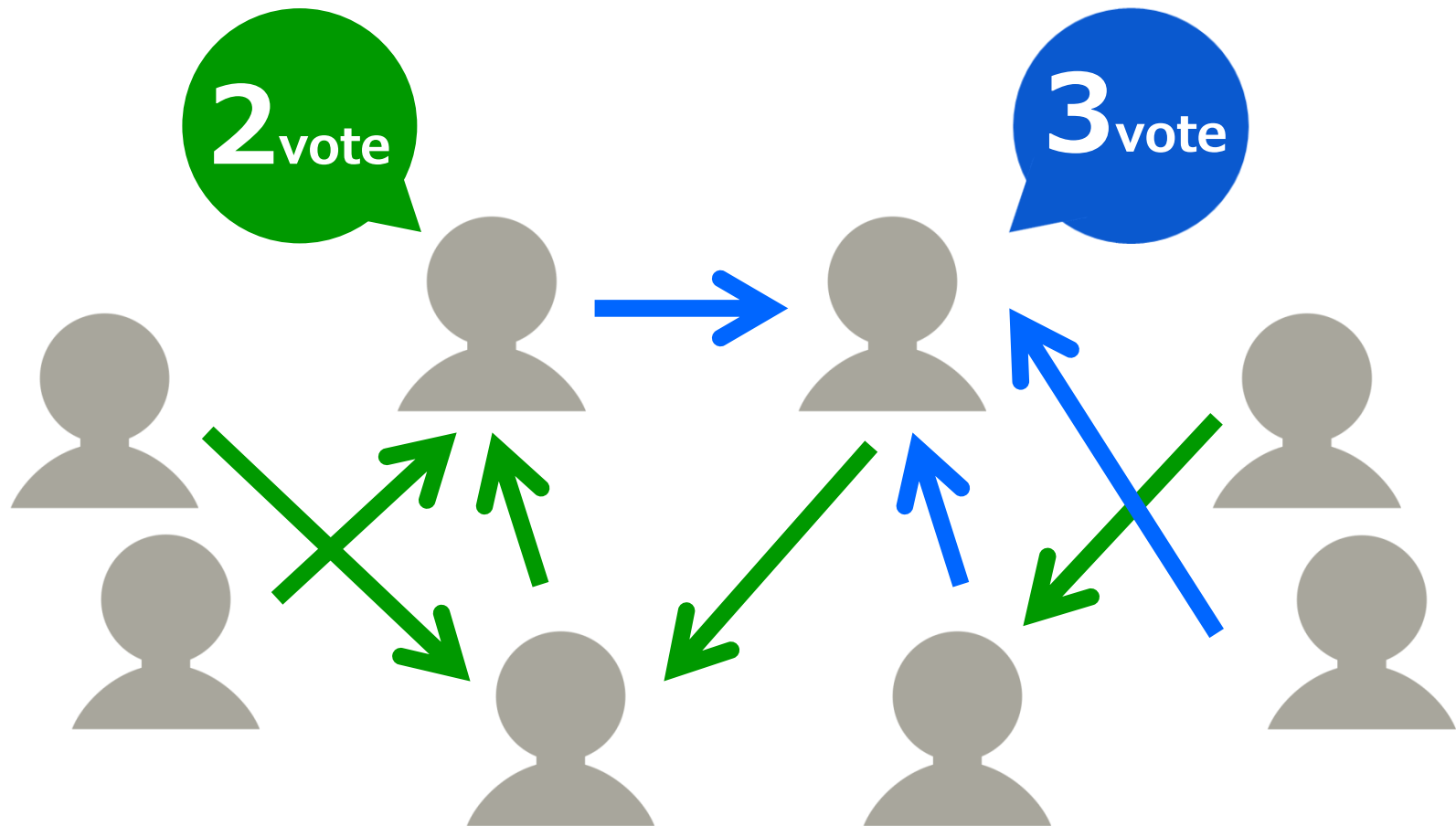
- The most questionable person (the person who is the most dissatisfied) will be decided through a vote.





# Investigation: Dismissal

- The player who has the most votes will be dismissed.



# Secret Expert Investigation

- The following job positions will have expert investigations conducted late at night.

**Forensic Engineer**




**CSIRT Team**

Forensic Engineers investigate the source of problems and sort through electronic information to discover evidence.

Japan Network Security Association.

**Researcher**



**CSIRT Team**

Researchers collect information, discover abnormalities in the system, and analyze the effects of the abnormalities.

Japan Network Security Association.

**Commander**



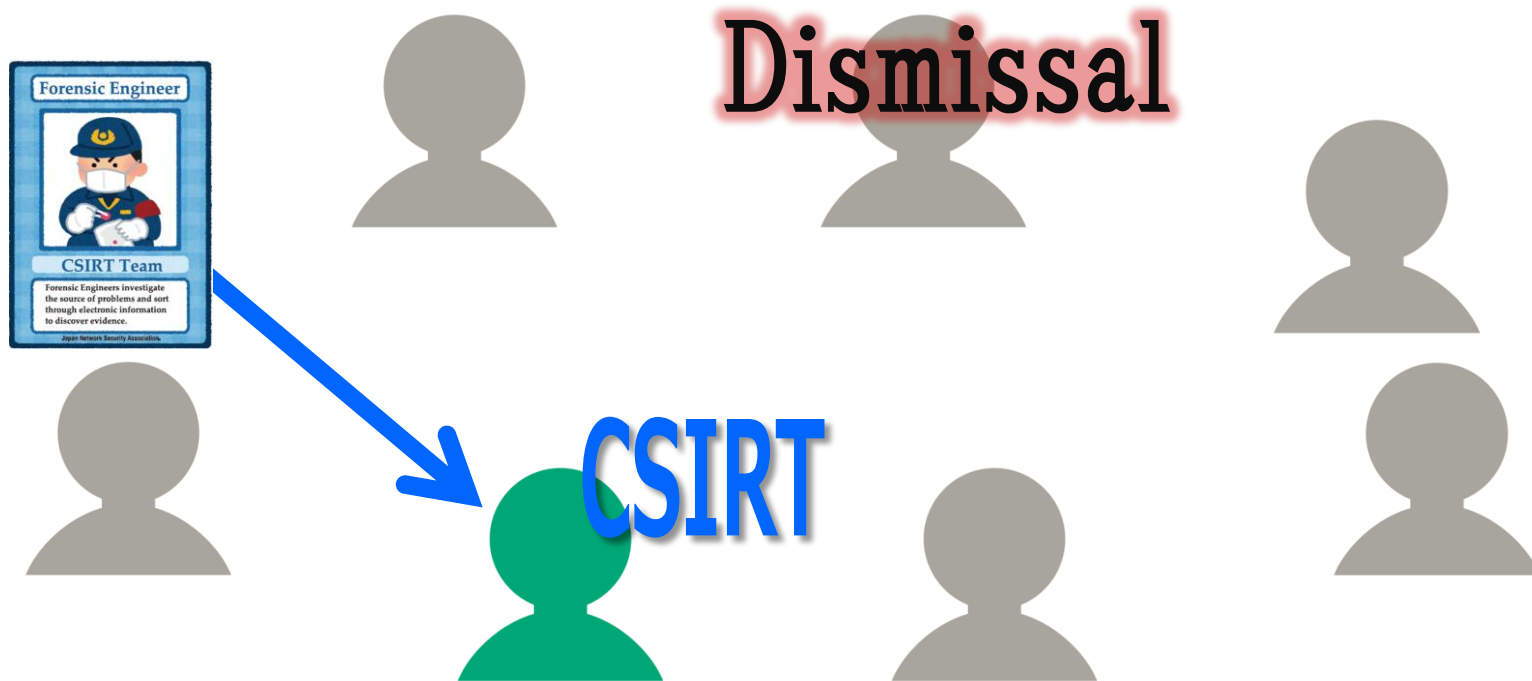
**CSIRT Team**

Commanders take control of the group after a problem appears and report important information to their team members.

Japan Network Security Association.

# Expert Investigation: Forensic Engineer

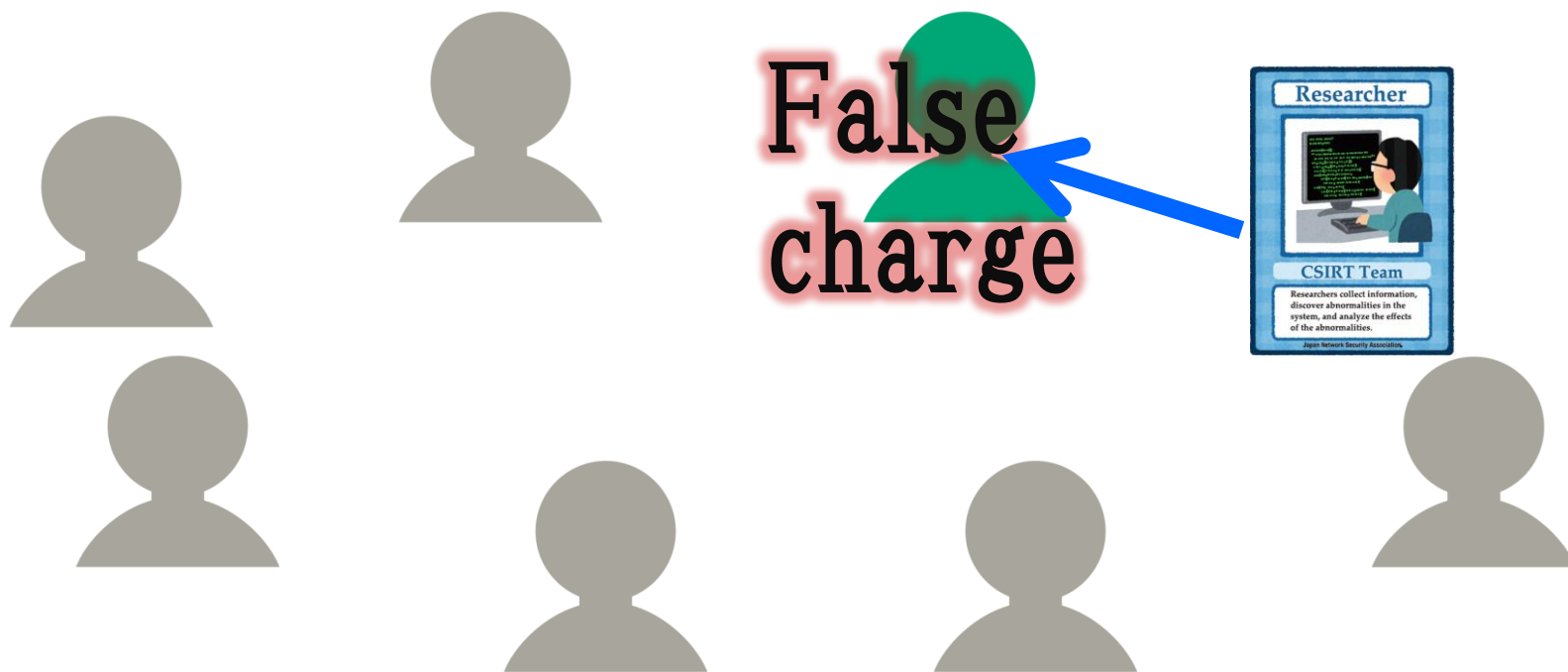
- The forensic engineers will conduct an investigation for evidence late at night.
- They can learn the truth about which team one person belongs to.



# Expert Investigation: Researcher

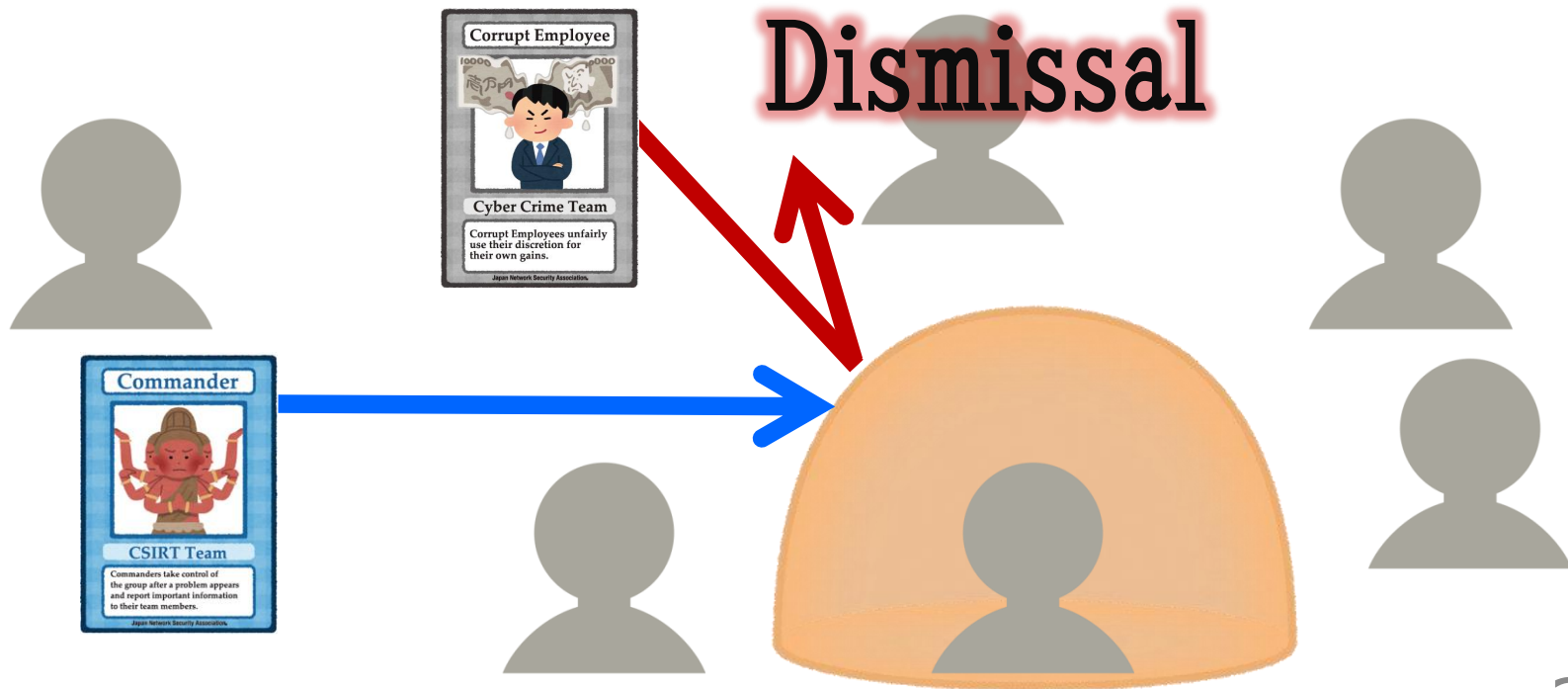


- The researchers will conduct a follow-up investigation late at night.
- They can learn the truth about the employee that was just dismissed (whether they were corrupt or not).



# Expert Investigation: Commander

- The commanders will conduct a protective investigation late at night.
- They can prevent one employee other than themselves from being accused of a crime by a corrupt employee for one turn.



# Actions of the Cyber Crime Team

- Aim for destruction by bluffing the organization into chaos





# Criminal Acts: Corrupt Employees

- They commit fraud late at night.
- They decide which player to accuse with false charges.



**Dismissal**

**Dismissal**

# Double-dealing Black Hat Hackers

- Black Hat Hackers only win if the Cyber Crime Team wins.
- During the expert investigations, they are judged to be part of the CSIRT Team.



**Dismissal**



**CSIRT**





# Start the SECWEREWOLF

# Directions for the Record keeper



The time for the first instance of fraud has arrived. Other than the facilitator and the record keeper, all other players should close their eyes and bow their heads.

The record keeper will record on a sheet of paper who is playing which role.

Corrupt employees, please raise your heads, open your eyes, and raise your hand.

Corrupt employees, please close your eyes and bow your heads.

Black Hat Hackers, please raise your heads, open your eyes, and raise your hand.

Black Hat Hackers, please close your eyes and bow your heads.

Commanders, please raise your heads, open your eyes, and raise your hand.

Commanders, please close your eyes and bow your heads.

Researchers, please raise your heads, open your eyes, and raise your hand.

Researchers, please close your eyes and bow your heads.

Forensic Engineers, please raise your heads, open your eyes, and raise your hand.

Forensic Engineers, please close your eyes and bow your heads.



# Suspect Interrogation

Record keeper, have you recorded all of the roles for the participants?

Everyone, raise your heads and open your eyes.

It seems there are corrupt employees who are dissatisfied among us.

We will now conduct suspect interrogations for five minutes.

We will conduct suspect observations and gather information through the fraud triangle theory and by using investigative interrogation techniques.

Participants can speak the truth or lie.

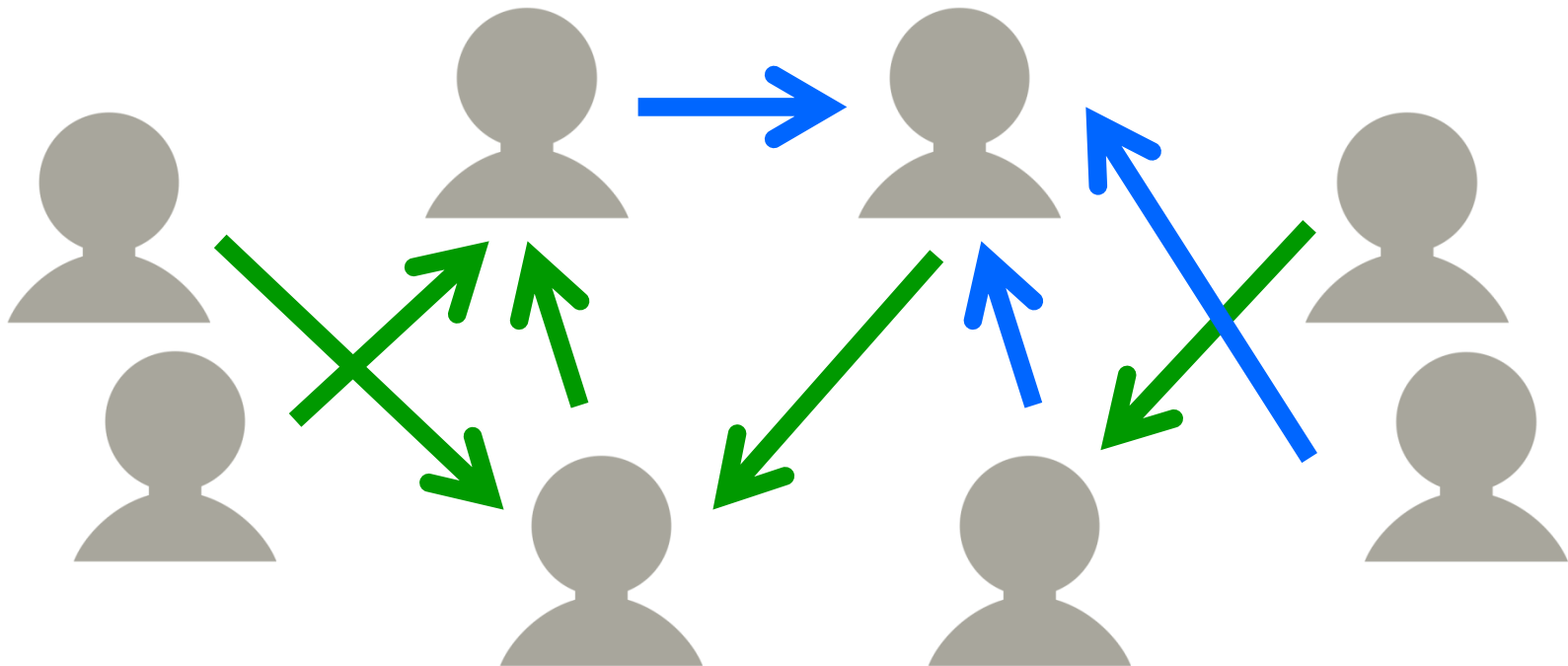
However, you cannot show your job position card until the end.



セキュリティ専門家人狼 (JIN-ROH)

**SEC WERE**  
**WOLF**

If there is a tie, please conduct a final vote to decide on one person to dismiss.



# Secret Expert Investigation

Once again, night has fallen. It seems like there are still corrupt employees in our midst.

Everyone, close your eyes and bow your heads.

Record keeper, please note which players the facilitator indicates through gestures during the expert investigation.

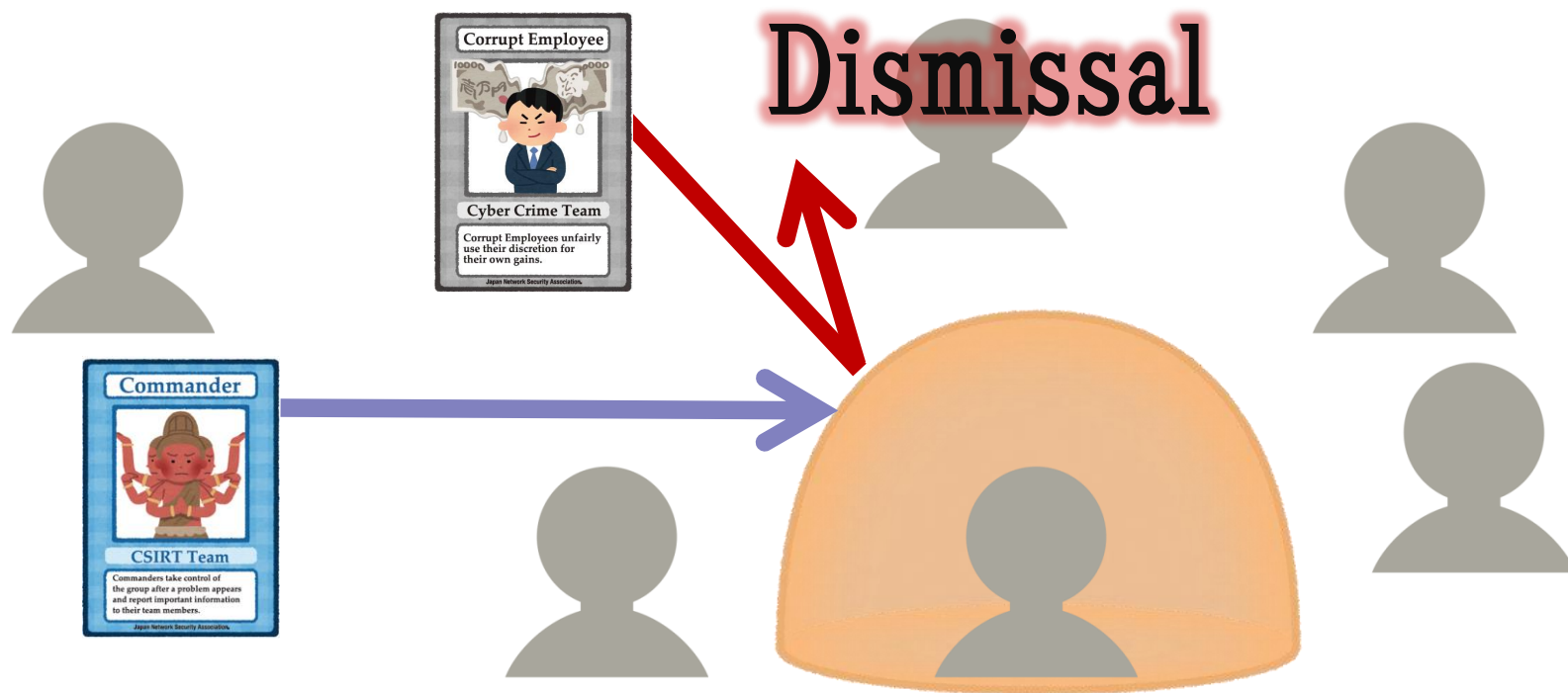
Researchers, please open your eyes. There will be a follow-up investigation. This is the role of players who were dismissed in the previous investigation.

(If the player was a Corrupt Employee, make an L with your fingers, like a gun. If they were a Notification Member, a Forensic Engineer, a Researcher, a Commander, or a Black Hat Hacker, raise your thumb.) Researchers, please close your eyes.

Forensic Engineers, please open your eyes. We will survey the evidence. Please pick the player to investigate. That player fulfills this role. (If the player is a Corrupt Employee, make an L with your fingers, like a gun. If they are a Notification Member, a Forensic Engineer, a Researcher, a Commander, or a Black Hat Hacker, raise your thumb.) Forensic Engineers, please close your eyes.

# Expert Investigation: Commanders

Commanders, please open your eyes. There will be a protective investigation.  
Please choose the player you want to protect from being charged with a crime.  
However, you cannot choose the same player as the last turn nor can you choose yourself.  
Commanders, please close your eyes.  
\*The record keeper will record who the commander chose on the record sheet.



# Criminal Acts: Corrupt Employee

Corrupt Employees, please open your eyes. It is time to commit a criminal act.

Who is it that hurt your self-esteem? Please decide on who to charge with a false crime.

Corrupt employees, please close your eyes.

\*The record keeper will record who the corrupt employees chose on the record sheet.





# Directions for the Record Keeper



Everyone, raise your head and open your eyes.

Record keeper, please tell everyone who was blamed for a crime by the Corrupt Employees in the previous fraud turn.

“It was OO,” or “There was no one,” (if the commanders’ protection worked).

The dismissed person will step away from the table and watch what happens.

Players, please analyze the situation from the point of view of “opportunity,” “motivation,” and “justification.”

Record keeper, please announce the remaining number of players on each team.

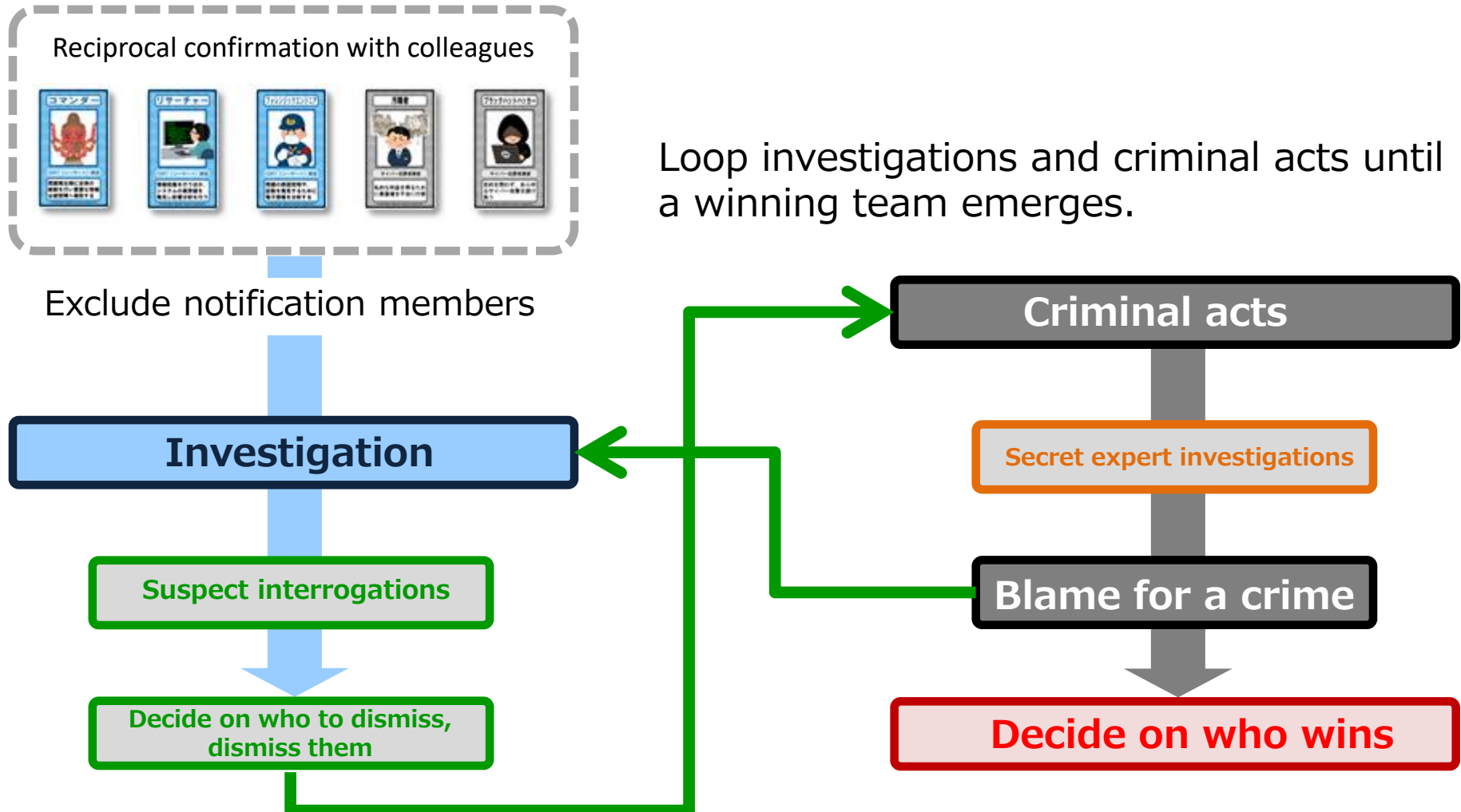
There are X players remaining on CSIRT Team and X players remaining on Cyber Crime Team.

\*Double-check the conditions for victory (slide 26)

Continue the game (return to slide 43)



# Game Progress

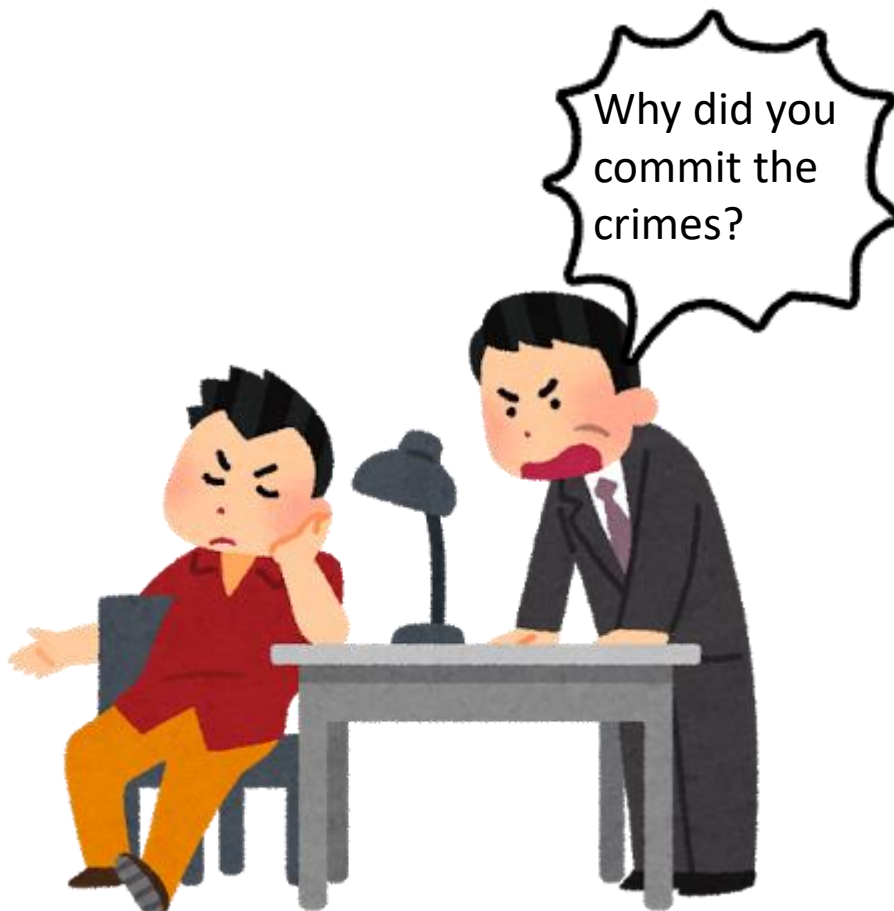


# Interrogation Techniques



# Differentiate Between the Innocent and Criminals

## The corrupt employees will not confess!



Tempt them into telling the truth.  
\*Search for the unrelenting truth.  
\*The interrogator will inquire about the crime while speaking the truth.

### Banned phrases :

"Did you do it?"  
\*Avoid using language that will make the suspect emotional.  
\*Once the suspect has denied committing fraud, it is difficult to overcome the situation.

# Examine the Suspect's Facial Expressions and Body Language

**Learn how to tell who is innocent.**



- They will be shocked when they are accused of a crime.
- They will be openly angry and will strongly deny they are guilty.

# Observe the Suspect's Facial Expressions and Body Language

## Guilty parties will be silent.



- Their lips will be pulled into a thin line.  
They will look stressed or anxious.  
There are behavioral tendencies, such as touching their mouths.
- Their voices may be pitched higher and their tone of voice might change.  
This indicates that they are losing their ability to stay calm.
- They will weakly deny their crimes.  
They will repeat the same words over and over (to buy time).  
Their words may be shortened.  
They may become vague.  
They may try to explain themselves instead of denying what's in front of them, and they may participate less.

# Strategies for Discerning Players' Job Positions

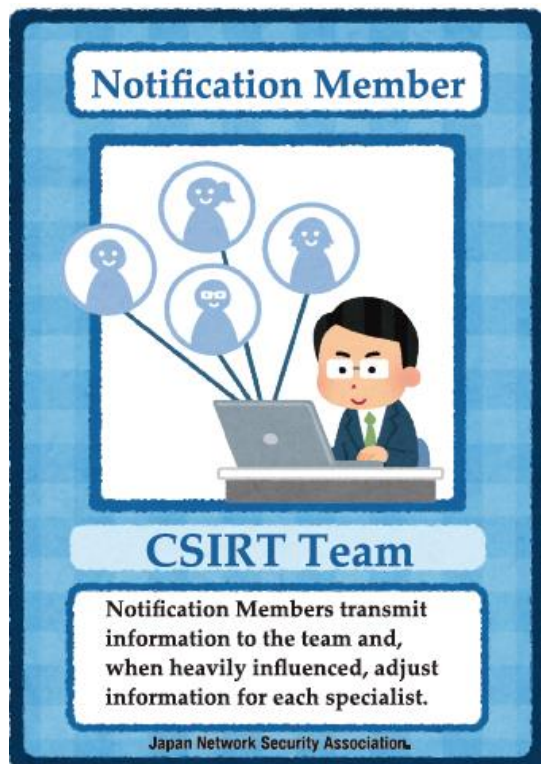
CSIRT Team Version





# Honestly and assertively...

Notification members are forbidden to deceive anyone.



- When they can't get any information (normal times), they take the initiative to gather information themselves.
- They propose a joint struggle after finding the stakeholders.
- They recognize suspicious behavior.

# Ask for Help from Commanders

Hint at the evidence surveillance skills you hold and request help from other players.



- Actively participate starting from the second turn
- Search for people whose positions cannot be uncovered through interrogations
- Prove that you have legitimate evidence-gathering skills by reasoning out the fraud committed by Corrupt Employees.

# Verify the Authenticity of Proof

Verify the abilities of the forensic engineer



- Devote yourself to discovering corrupt employees using espionage activities.
- Devote yourself to being an inspector of the forensic engineer's ability to survey evidence if they are suspicious.

# Decide Who to Protect

Take everything into account and perform triage.



- The ability to screen the importance of who to protect is important.
- The forensic engineer's protection priority level is high.
- The strategy of appointing someone in the CSIRT Team to decide who will be protected is also effective.

# Strategies for Discerning Players' Job Positions

Cyber Crime Team Version





# Test Secret Maneuvers Based on Skill

Make them think you have expert investigation skills.



- Pretend to be a Forensic Engineer or Researcher.
- Get protected by commanders.
- Effectively use being judged as a CSIRT member during the investigation.

# Deceive the CSIRT Team

Accuse players with abilities that are unfavorable to you of false charges.



- Commit fraud and lead the CSIRT Team to chaos.
- Strategic betrayal is also effective.
- Aim for the victory of the Cyber Crime Team through friendly fire.



# Reference Materials

For even more study...



# Social Engineering

- A method to steal important information for attacks and fraud without using any IT techniques.
- You can take advantage of many people's mental gaps and behavioral mistakes.

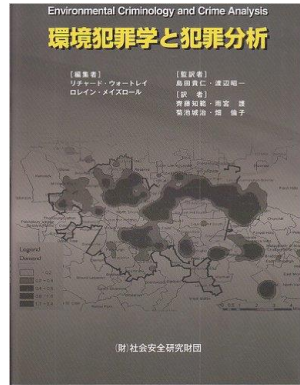


# Criminal Profiling

- Criminals tend to have certain behaviors in common.
- If a crime has happened, there will be signs or traces left behind.



# Applying situational crime prevention methods

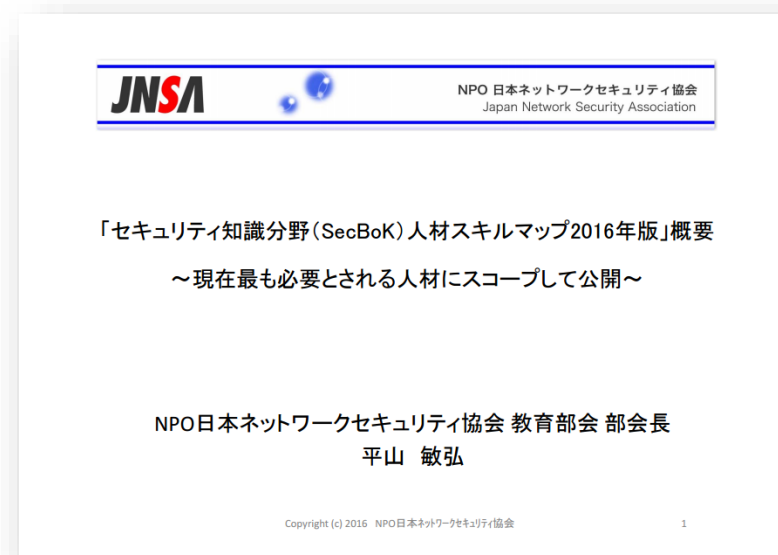


(財)社会安全研究財団 2010年  
『環境犯罪学と犯罪分析』

## 状況的犯罪予防における25の技法

Twenty Five Techniques of Situation Prevention

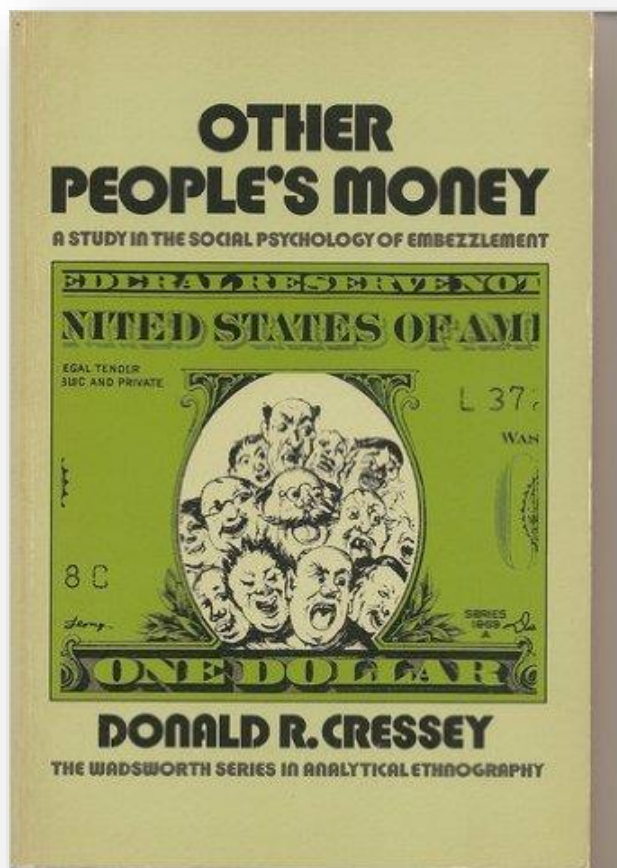
Increase the Effect	Increase the Risk	Reduce the Rewards	Reduce Provocations	Remove Excuses
犯行を難しくする	捕まるリスクを高める	犯行の見返りを減らす	犯行の挑発を減らす	釈明させない
対象を防御的に強化する	監視者を増やす	標的を隠す（存在がわからない）	欲求不満やストレスを減らす	規則を決める
施設への出入りを制限する	自然監視を補佐する	対象を排除する（存在をなくす）	対立（紛争）を避ける	指示を提示する
出口の検査	匿名性を減らす	所有者の特定	誘惑や興奮の低減	良心に警告する
犯罪者をそらす	現場管理者の利用	市場を阻止	仲間からの圧力を緩和する	遵守を補佐する
道具や武器を制御する	フォーマルな監視体制を強化する	便益を与えない	模倣犯を阻止する	薬物・アルコールを規制する



日本コンピュータセキュリティインシデント対応チーム協議会  
『CSIRT人材の定義と確保(Ver.1.5)』

特定非営利活動法人 日本ネットワークセキュリティ協会  
『セキュリティ知識分野 (SecBoK) 人材スキルマップ2017年版』

# The fraud triangle



クレッシー・ドナルド・R 1953年『他人の金 (Other People's Money)』フリープレス社、ニューヨーク (New York: Free Press)

特定非営利活動法人 日本ネットワークセキュリティ協会  
『内部不正対策 14 の論点』



# Points for countermeasures and concrete plans to enact

IPA

## 組織における 内部不正防止ガイドライン



独立行政法人 情報処理推進機構

独立行政法人情報処理推進機構  
『組織における内部不正防止ガイドライン 第3版（2015年3月改訂）』

JNSA

## 内部不正対策 ソリューションガイド



2013 年 12 月 26 日

特定非営利活動法人  
日本ネットワークセキュリティ協会

1

特定非営利活動法人 日本ネットワーク  
セキュリティ協会  
『内部不正対策ソリューションガイド』



\\ We're always tweeting the latest information! //

Follow us!→@Sec\_JINROH



#SECWEREWOLF'  
s official account

