



Fast, Frank, and Friendly  
Financials ISAC Japan



# Cybersecurity operation and management bird's-eye view from Japanese financial industry experience

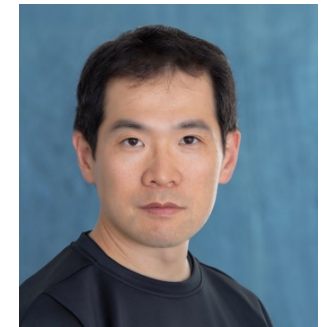
Keisuke Kamata

Executive Director / CTO

Financials ISAC Japan

HITCON 2022

# Me: Keisuke Kamata



- History

- Was national top 10 arcade gamer (teenager days)
- Worked for IT dev/ops : 3 yrs
- Start working for Cybersecurity in 2002 at JPCERT/CC
- Worked for MUFG Bank Cybersecurity Management Team: 2011-2014
- Establish Financials ISAC in 2014 (Cont)
- Establish Armoris in 2019 (Cont)

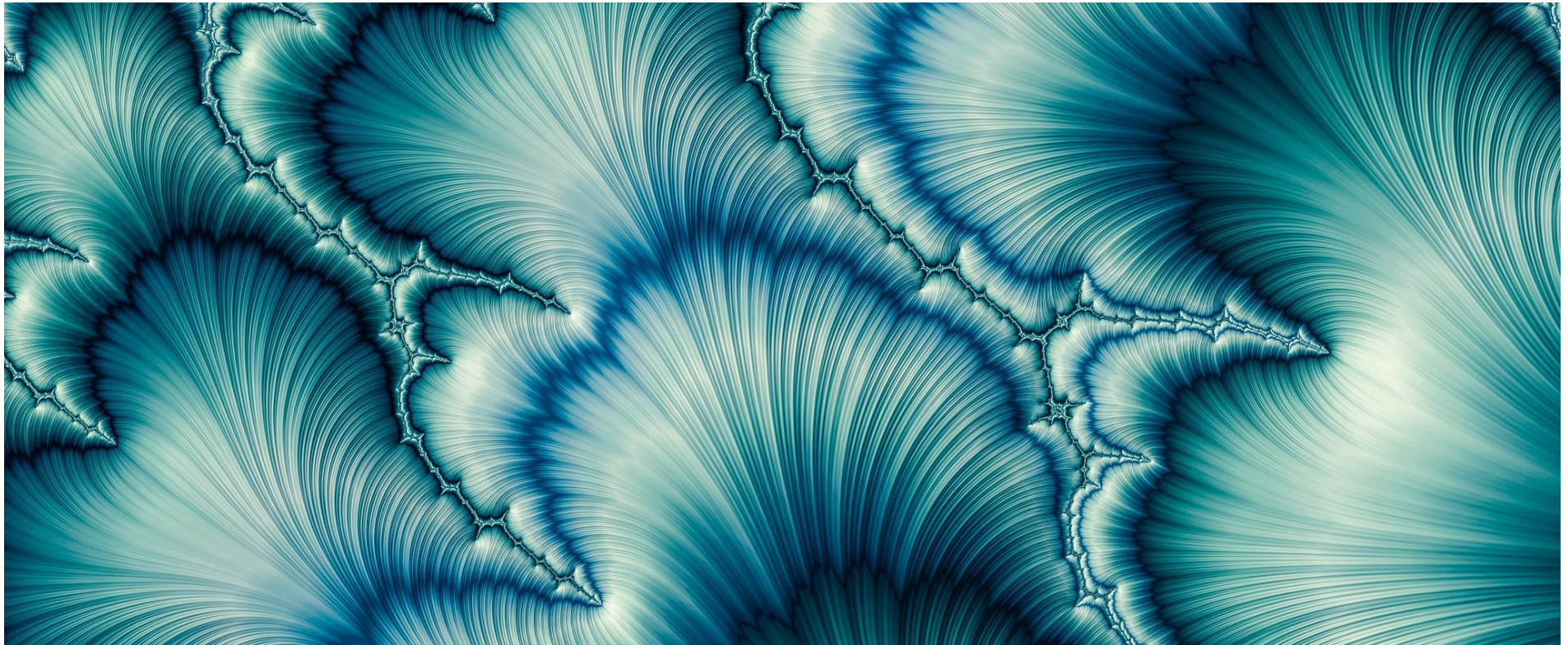
- Current positions

- Executive Director / CTO at Financials ISAC Japan
- Advisor to Financial Services Agency of JP gov
- Member of Cybersecurity HRD Committee of Cabinet
- Board Member / CTO at Armoris
- Cybersecurity Advisor to Ibaraki Police
- Cyclist (1200-1500km / month)




# Agenda

- Introduction
- Case study
- Lessons Learned
- Conclusion

# Introduction



# Japanese financial industry cybersecurity

Role	Organization	Logo
Regulation/Policy	Financial Services Agency Bank of Japan NISC (cabinet office)	
Guideline	Associations for "Bank" "Securities" "Insurance" "Credit card" etc  FISC for computer system  Fintech, Cryptocurrency	
Operational	Financials ISAC Japan	

# Concept form history: 自助・共助・公助



# About: Financials ISAC Japan



Financials ISAC Japan was established in 2014 as a "Mutual Help (共助)" body for financial institutions. 427 members.



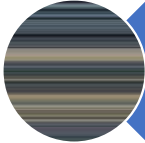




Recognize cybersecurity as "cooperation" not as "competition."  
Financial institutions helping each other for secure financial industry.



What we do? : Develop best practice, Industry wide exercise, Hands on Training, Seminar, Workshop, Annual conference, Information sharing

# Trend: Cyber Threat Landscape in JP financial industry

-  Sophisticated attack (APT) to cryptocurrency industry
-  Fraud money transfer (Bank, Payment, Securities, Insurance)
-  Business / Service suspension by DDoS etc
-  Information leakage through cloud services
-  Ransomware incidents?



# Who are attackers, and what is motivation?



Hackers



Hacktivist



Criminals



Nation state



Teenagers



Insiders

# Case study



# 1. Phishing

- Attackers launch phishing site to steal customer information from financial institutions (FIs)
- Bank or payment companies are main target but we see securities and insurance companies are becoming target



# Phishing site analysis

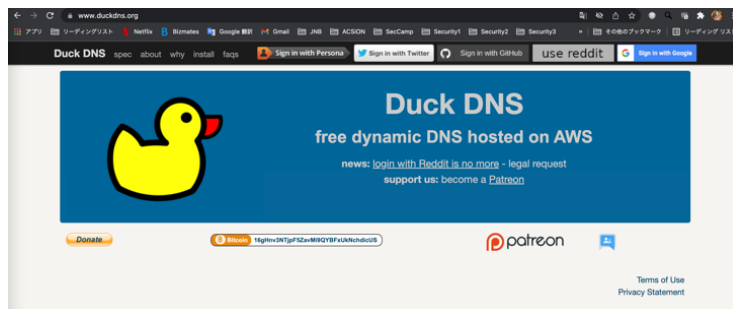
- Over 10000 phishing site observed per month
  - Mobile companies, large bank, credit card companies are major target
  - Top3 target is like 80% of 10000
- Domain registration companies like duckdns, webnic, namesilo, godaddy are mainly used.
  - Those are not major in Japan
- 4 hosting companies are use 80% of those phishing site

# Phishing site analysis (cont.)

- Major top level domains are "org" "com" "cn" "top" "xyz"
  - .jp is very little (less than 1%)
- Most of phishing site is using HTTPS and lets encrypt is 99%
- Why mobile companies are major target?
  - Large customer volume
  - Their own payment service
  - eSIM?

# Phishing site analysis (cont..)

- Using Dynamic DNS service to create unlimited numbers of URLs
- Redirect to same IP address phishing site
- We see like bit.ly → Dynamic DNS URL → phishing site redirection



# Phishing site analysis (cont...)

The screenshot shows a web browser with the URL `https://dzuzhazfm.duckdns.org`. The page has a white background with a grey header. Below the header, there is a login form with the title "ログイン". It contains a text input field with the email address "wazaok02@gmail.com" and an orange button labeled "次へ". Below this, there is a section for "au IDはau以外の方もご利用いただけます。" with an orange button labeled "au IDを新規登録する" and a link "au IDとは".

Phishing site and login  
(you can input wrong ID/PW)



The screenshot shows the "My Y!mobile" payment page. The URL is `https://dzuzhazfm.duckdns.org/unist`. The page has a red header with "My Y!mobile" and "未払い金のお支払い". Below the header, there is a section for "支払い方法の選択". It contains a table with columns "未払い金額", "支払い期限", and "請求金額". The table shows a total of 40,000 yen due by 2021年11月26日. Below the table, there are three radio button options for payment methods: "コンビニ(セブンイレブン)", "ネットバンキング(Pay-easy)", and "電子マネー (iTunes ギフトカード)". The "電子マネー" option is selected. There is a red button at the bottom labeled "お支払い手続きを続ける".

You can choose "iTunes card"  
Only at payment method



The screenshot shows the iTunes gift card selection page. The URL is `https://dzuzhazfm.duckdns.org/itunes`. The page has a white background with a blue header. Below the header, there is a section for "iTunes ギフトカードでお支払い". It contains a form with a "ギフト券番号" input field and a "金額" input field. The "ギフト券番号" field contains "A0A1B2C3D4E5F6G7" and the "金額" field contains "10000". Below the form, there is a table with columns "ギフト券番号" and "金額". The table shows five rows of gift card numbers and amounts, all set to 10000. Below the table, there is a section for "お申し込み金額", "ギフト券総額合計", and "不一致". The "お申し込み金額" is 40000円, the "ギフト券総額合計" is 40000円, and the "不一致" is 0円. There is a red button at the bottom labeled "お支払いへ進む".

Input iTunes card serial  
(wrong number is acceptable)

# Phishing site analysis (cont....)

- You go phishing site, input ID/PW and login
- Asking you to go to ATM to make payment

ATMトップ画面からメニュー選択  
ATMトップ画面から「税金・料金払込」を選択してください。



収納機関番号の入力  
「収納機関番号」58091を入力してください。



お客様番号の入力  
「お客様番号」2131478205を入力してください。



確認番号の入力

「確認番号」758369を入力してください。



申込内容の確認

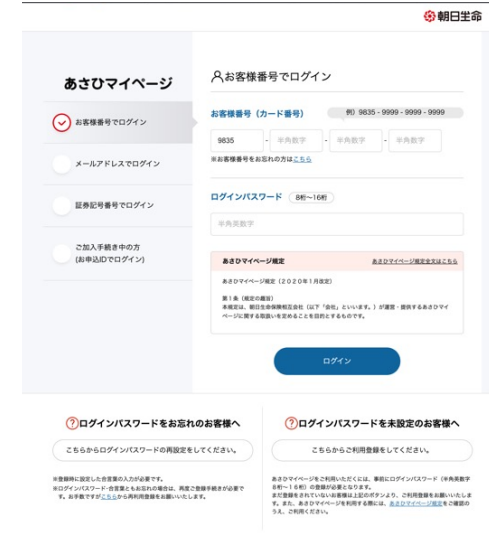
申込内容をご確認ください。

お支払い方法の選択

お支払い方法「現金」もしくは「キャッシュカード」を選択してください。



# Life insurance company phishing

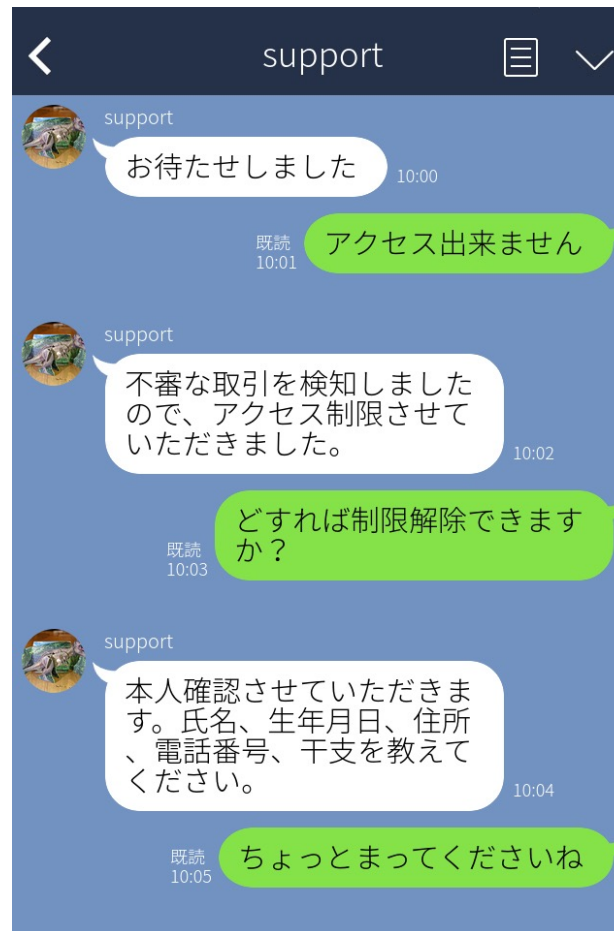


# Customer support chat

Thank you for waiting

We detect suspicious behavior and account suspended.

We need to confirm your identity. Tell us your "name" "birth date" "address" "phone number" "oriental zodiac"

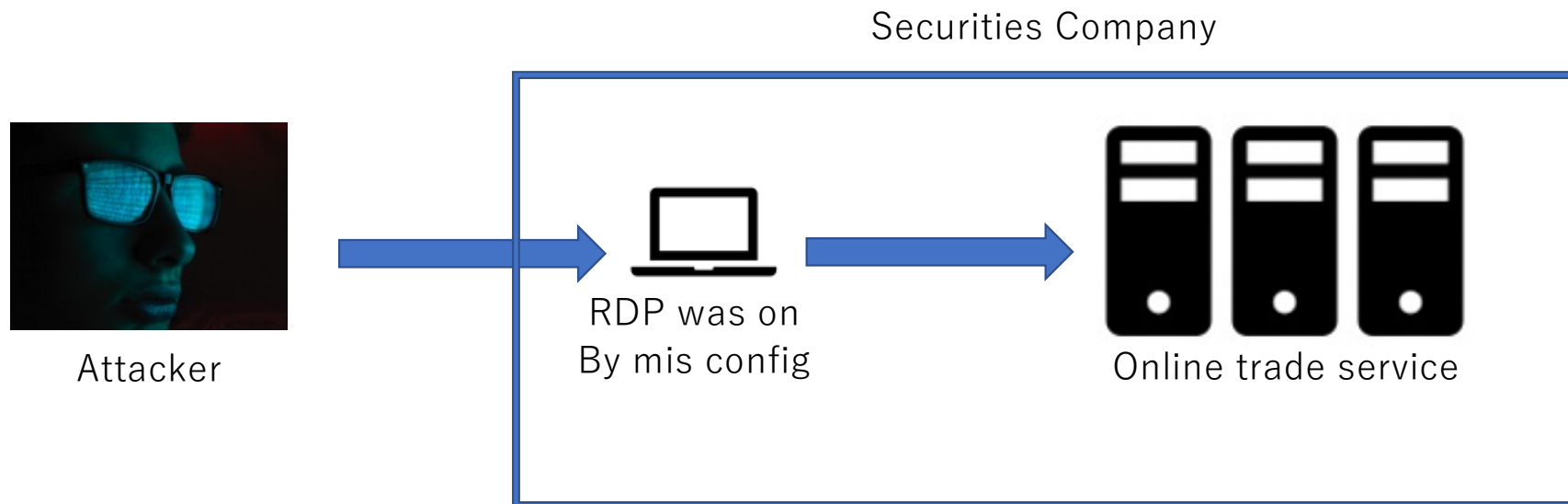


I can not access

What should I do?

Please wait...

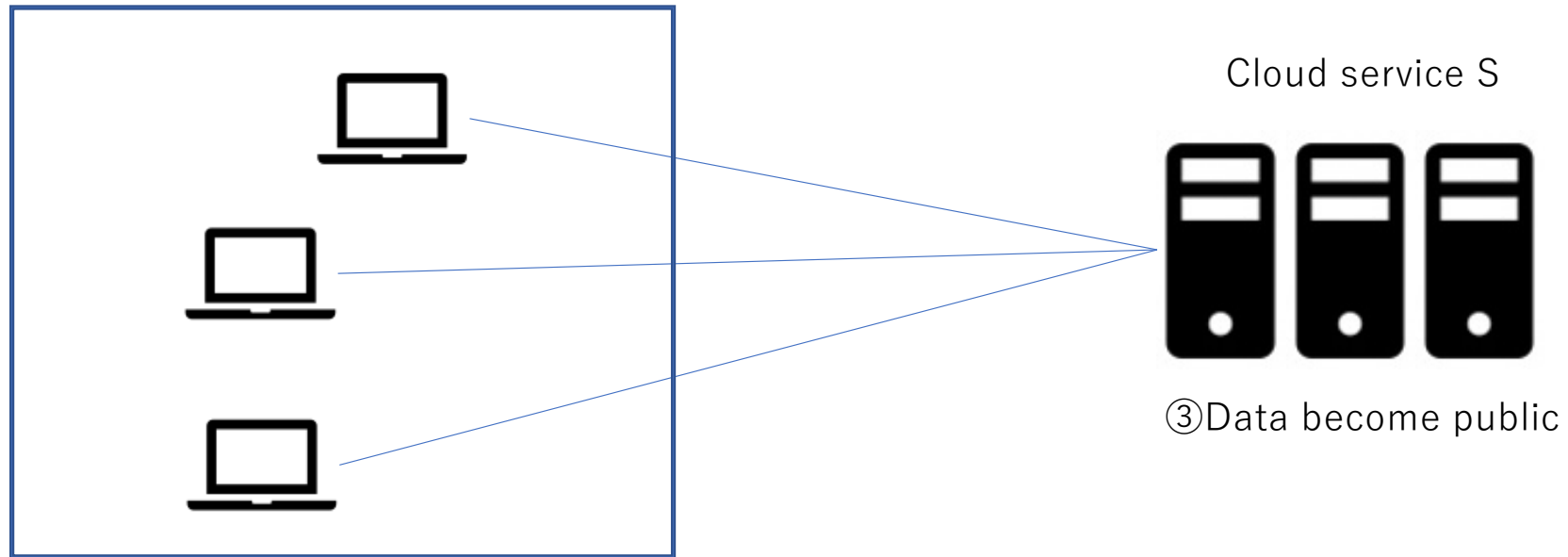
## 2. Ransomware incident



1. Their initial plan did not use the Internet
2. Change the network configuration
3. Wrongly open RDP without proper access control

# 3. Cloud service access control

② Many customers did not understand



① Notice configuration change

What we do for it?



# 1. Phishing

- Create small technical group to develop and distribute phishing site detection tool for F-ISAC Japan members
  - Provide hands-on training for in-house monitoring
- Tor node server list to monitor suspicious IP access
- Daily/timely information sharing in the community
  - About new phishing site
  - How we respond to it?

## 2. Ransomware

- It is recognized serious case but we dont see many victim cases like other industries
- We keep gathering global trend
- Business viewpoint
  - Can we pay or not?
  - What we do if the business suspended? (BCP)

# 3. Cloud service access control

- Discuss and create guideline for cloud service access control.
- Discuss with cloud service provider what and how we should have done
- Organize technical seminar for members



# Conclusion



# PPT Analysis



# People

- Is security team understand "current situation" ?
- Do they have enough knowledge and experience?
- Do they have "good" information source and peers?
- How is corporate internal communication?
- We do "mis-configuration"

# Process (Organization)

- Corporate security policy and enforcement
- Do we really know our "IT assets" throughout company?
- How strong is the IT/Security division?
- Is your CxO really understand cyber risk?

# Technology

- Small thing cause big problem like RDP case
- In-house vs Outsource
- Daily operation, devsecops, agile
- Technical people can help non-technical people

# People again

- Need more people?
- Technical skill vs management skill
- Communication with CxO
- Help each other and sharing helps industry

Thank you for your attention!

