フィッシング対策協議会
Council of Anti-Phishing Japan

Phishing trends in Japan

Council of Anti-phishing Japan
Shinichi Tankyo

Table of Contents

1. About Council of Anti-Phishing Japan(CAPJ)
2. Phishing Reports
3. Phishing Examples
4. Phishing Trends
5. Awareness Activities (STOP.THINK.CONNECT.)

About Council of Anti-Phishing Japan(CAPJ)

Organization Overview of Council of Anti-Phishing Japan

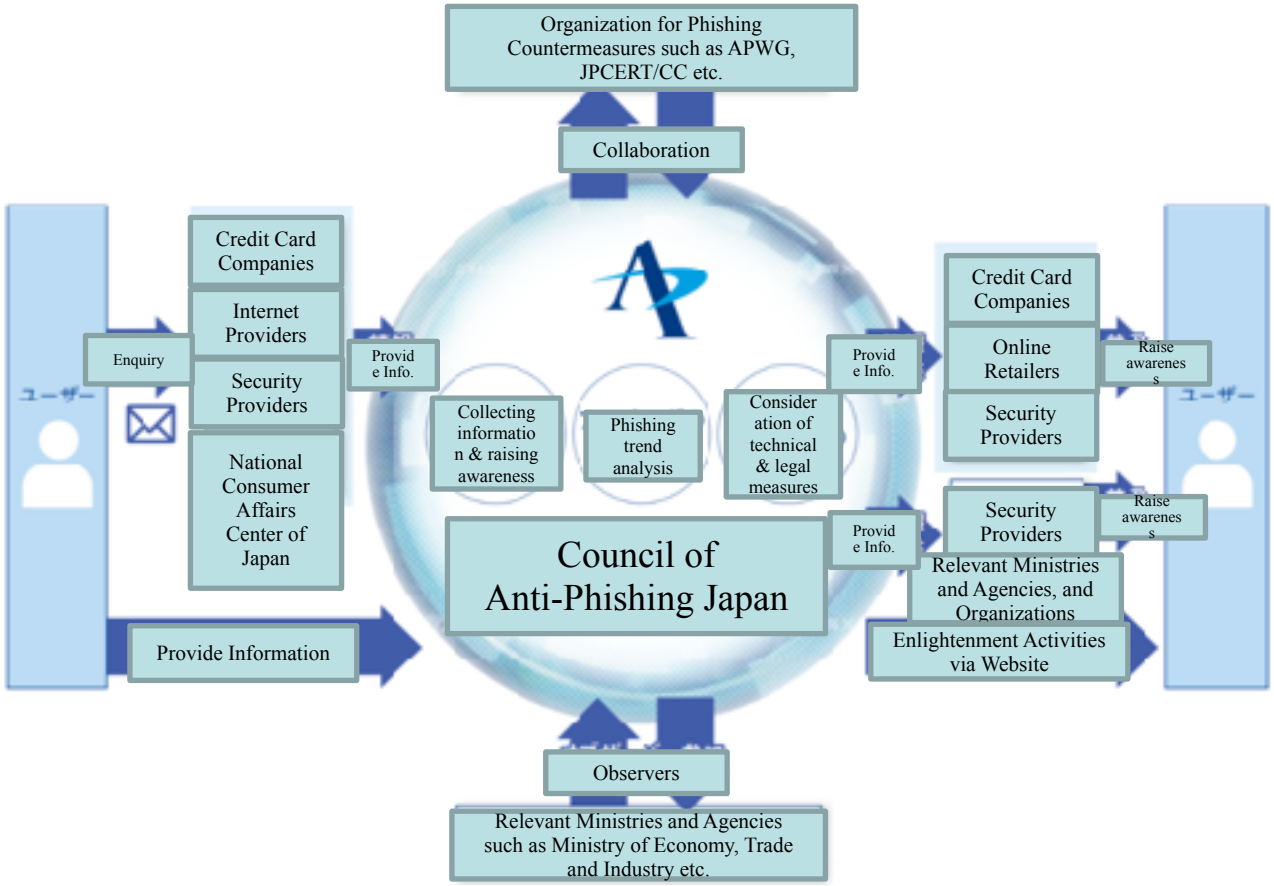
- Incorporation
  - 2005 Apr.
- Name
  - Council of Anti-Phishing Japan
- Purpose
  - Activity focused on gathering and providing information on phishing fraud cases and technical information to prevent phishing fraud in Japan.
- Member + Observer
  - 102

  Regular members: 75; research partners: 6; relevant organizations: 14

  Observer: 7

  Financial institutions, credit companies, online services, security vendors, etc.
- Chairman
  - Hisamichi OKAMURA
- Steering committee
  - Chairman: Takahiro Kato (Toppan Forms Co., Ltd.)
  - Vice Chairman: Yusuke Karasawa (Japan Digital Design Corporation/SourceNext Corporation)
- Office
  - JPCERT Coordination Center, Inc.

Council of Anti-Phishing Japan's Activity



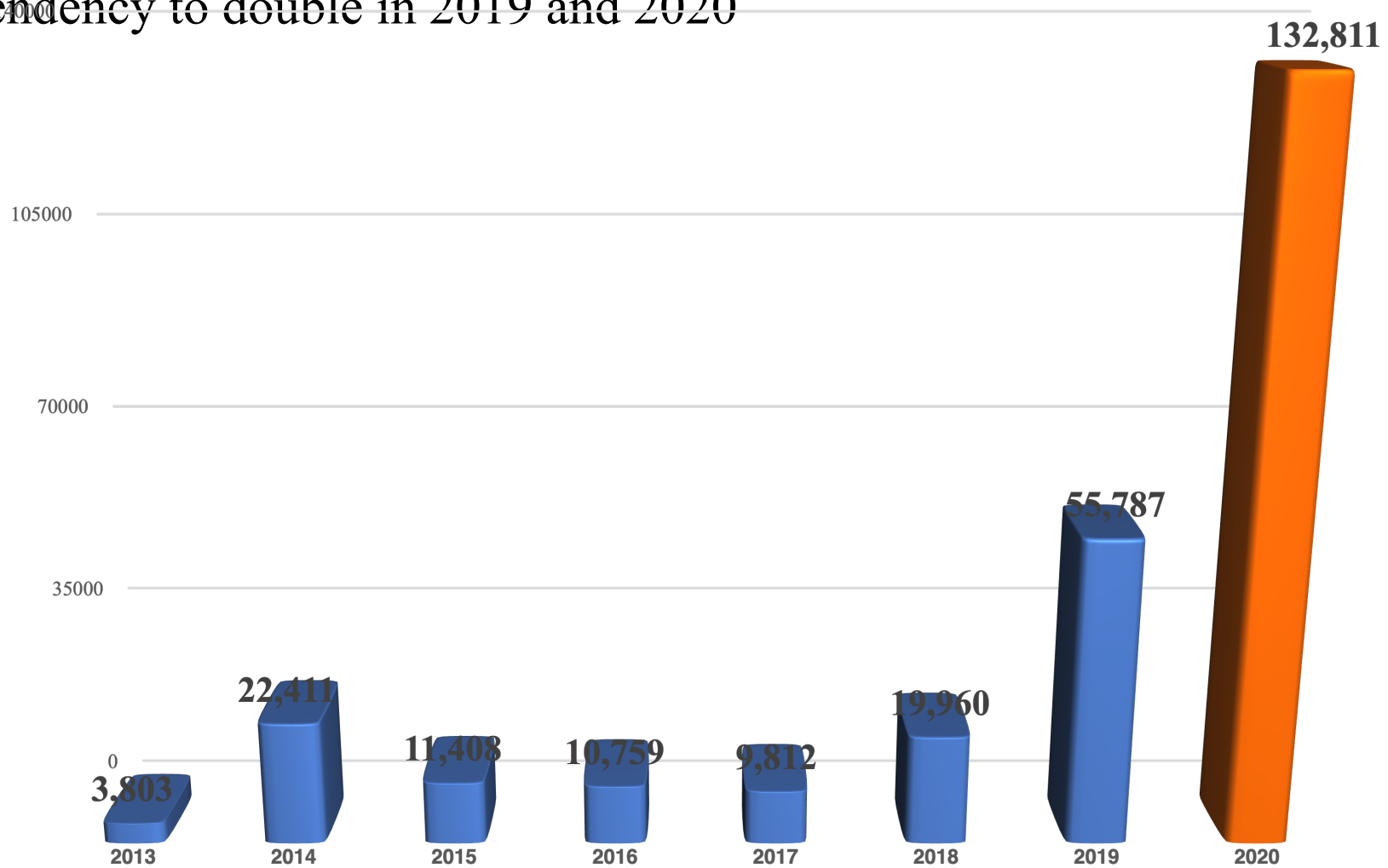
Posting Information	■Emergency Information/ Announcements ■Revised Guideline (WG activities) ■Phishing Report etc.
Exchange Information among members	■General Meeting/Information Exchange Meeting ■Study Group ■Working Group Activities etc.
Academic Research	■Early Detection of Phishing Site ■Full Picture of Phishing Scams
Awareness-Raising Activities	■Phishing Measures Seminar ■STOP, THINK,CONNECT

フィッシング対策協議会
Council of Anti-Phishing Japan

Reception Status of Phishing Reports

Number of Phishing Reports (Year)

- Rapid increase since 2018
- Tendency to double in 2019 and 2020

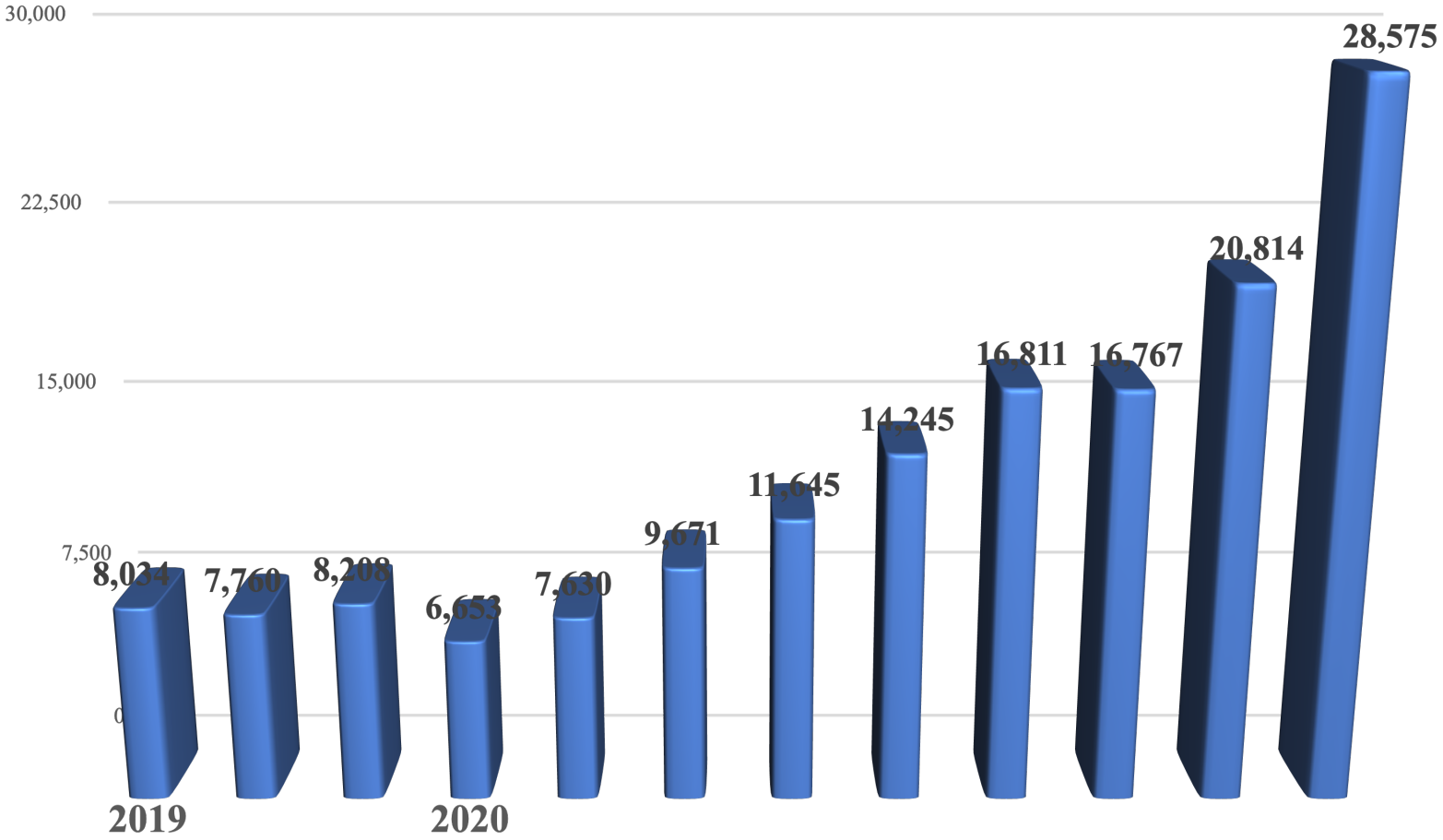


Source: Council of Anti Phishing Japan

フィッシング対策協議会
Council of Anti-Phishing Japan

Number of Phishing Reports (Monthly, 2020)

- Exceeded 20,000 per month in August 2020

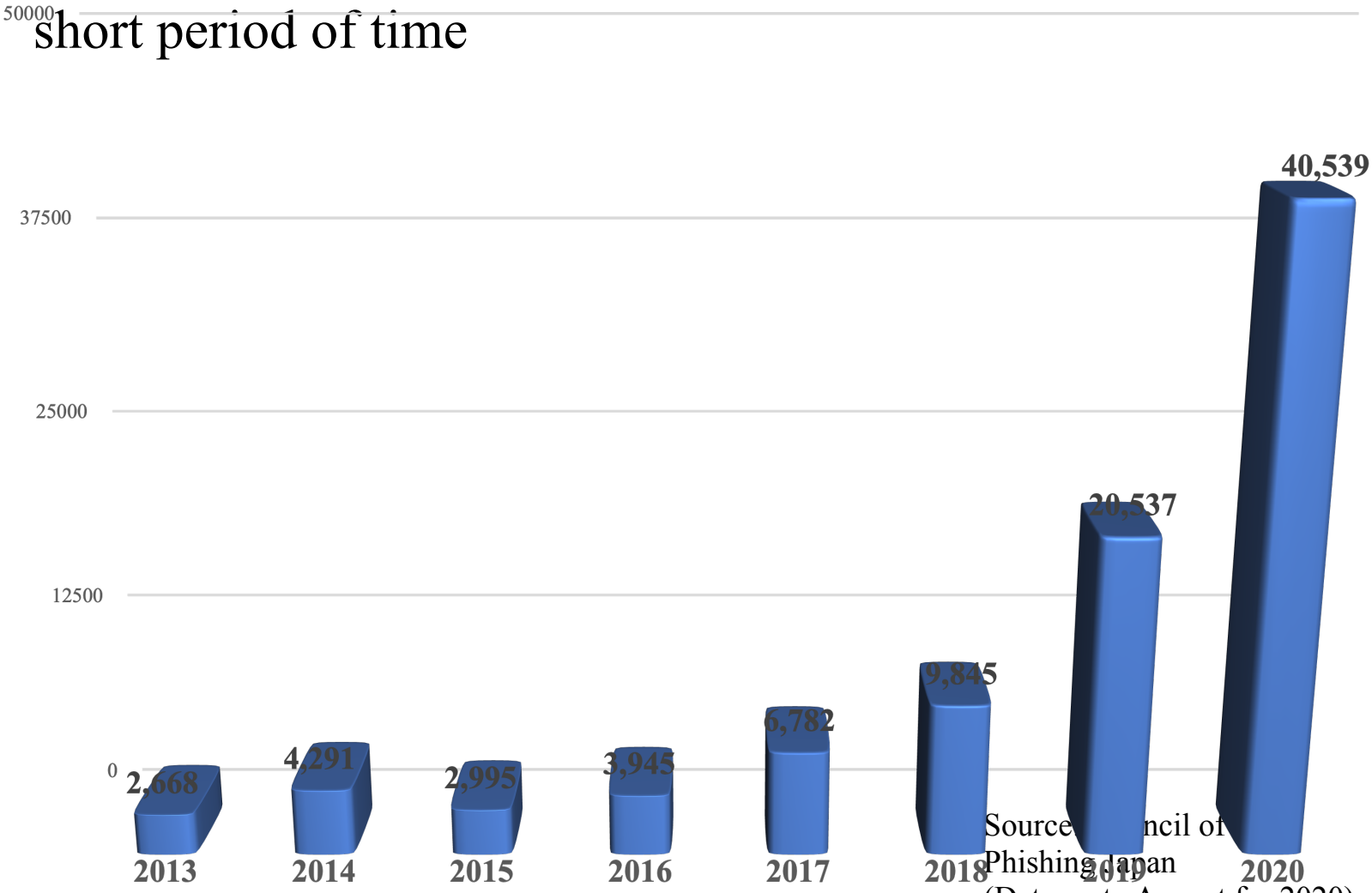


Source: Council of Anti Phishing Japan

フィッシング対策協議会
Council of Anti-Phishing Japan

Number of URLs (Year)

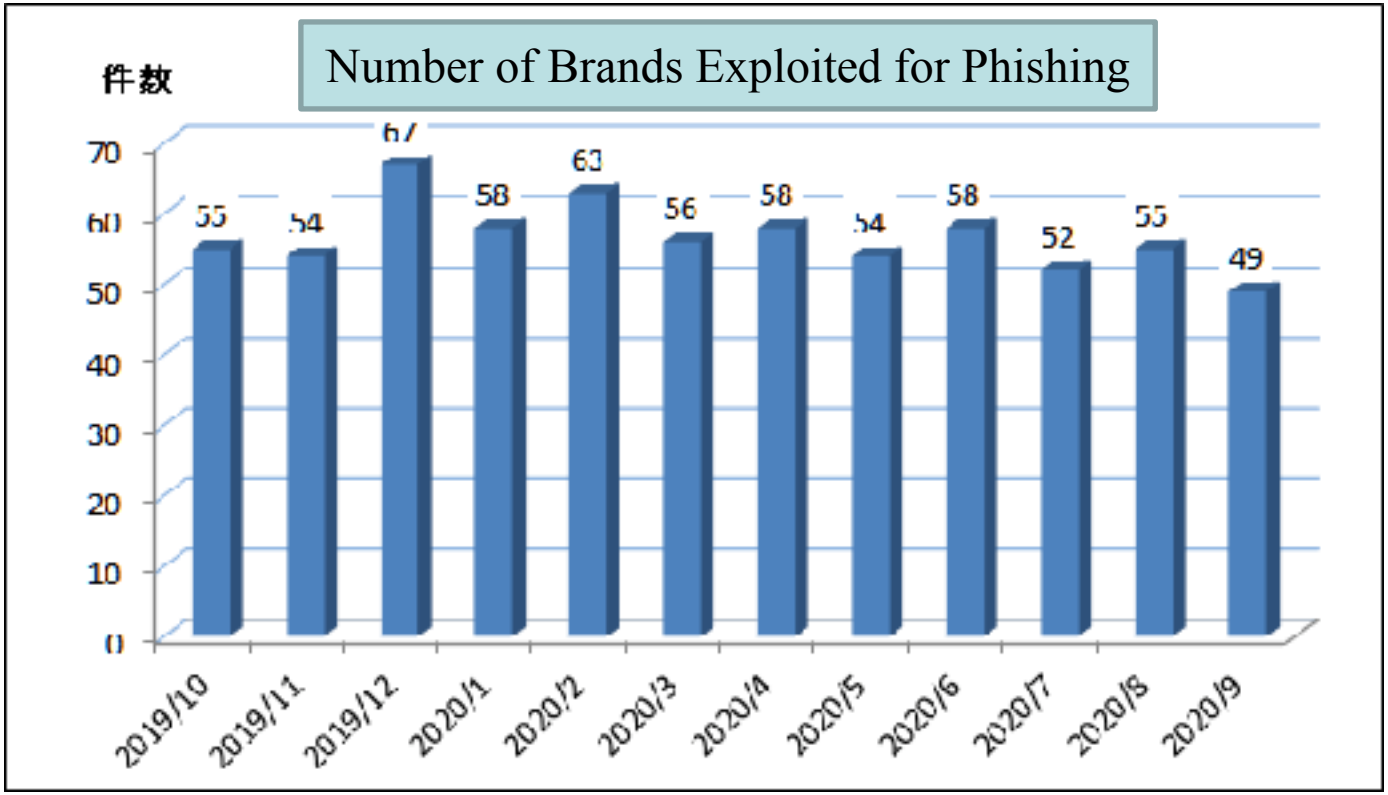
- Increase in phishing sites operating in different domains in a short period of time



Source: Council of Anti-Phishing Japan
(Data up to August for 2020)

By Brand (Monthly, 2020)

- No significant fluctuation in the number of brands misused
- In September, the top four brands of Amazon, Rakuten, Mitsui Sumitomo Cards, and LINE account for approximately 93.2% of the total number of reports.



Source: Council of Anti Phishing Japan

Phishing Examples

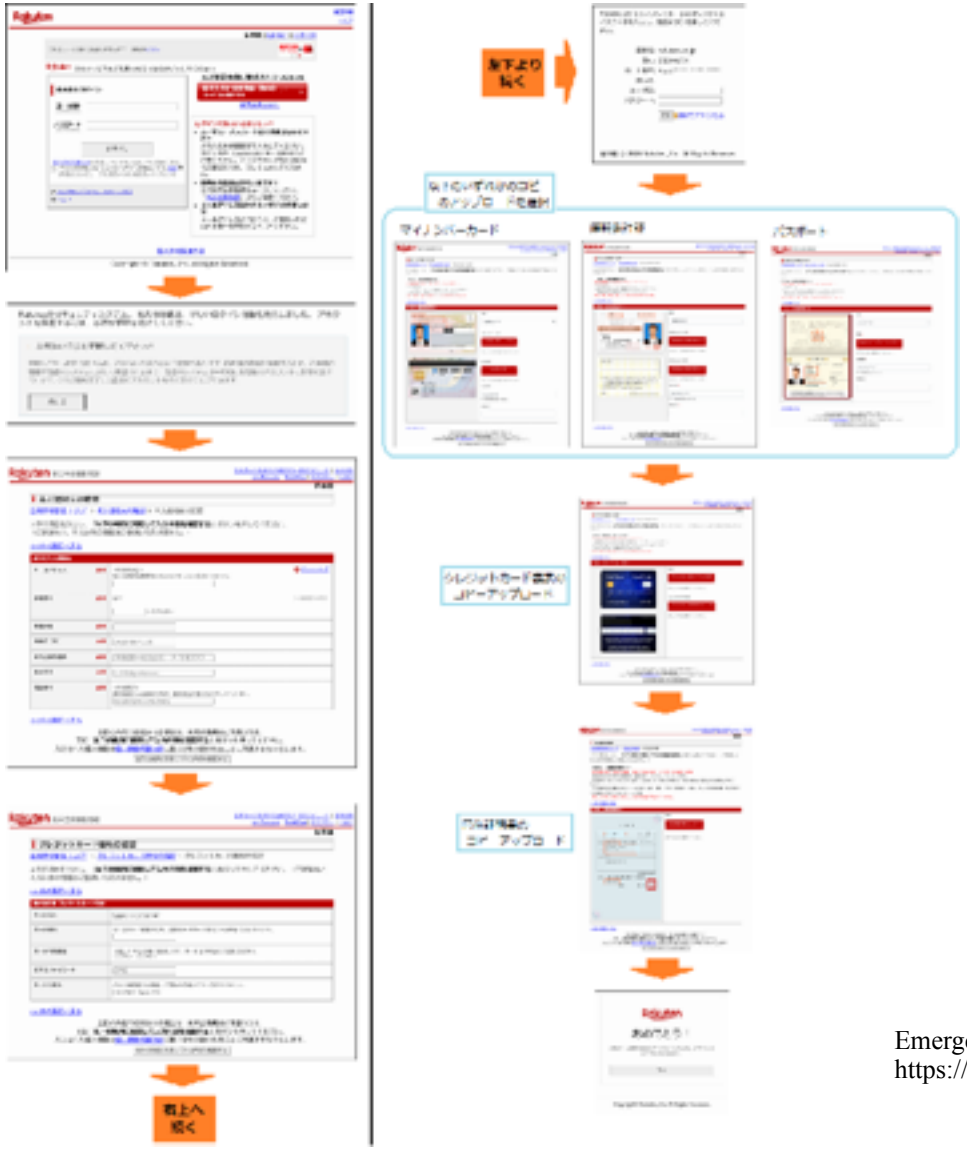
Fake Ads Guidance

- Fake ads that appear in Google searches

Example of a fake advertisement directed to phishing site

Emergency: phishing BTCBOX (2020/09/28)
https://www.antiphishing.jp/news/alert/btcbox_20200928.html

Phishing Sites collect a lot of Information



- Exploited information

1. ID/password
2. Address, Date of Birth, Telephone Number
3. Credit card information
4. 3D Secure ID/password
5. Copy of my number card, driver's license or password
6. Copy of the credit card
7. Copy of the residence certificate

Emergency information: phishing to make Rakuten (2020/06/25)
https://www.antiphishing.jp/news/alert/rakuten_20200625.html

Phishing Trends

Recent Delivery of Phishing E-mails

- Mass-delivery phishing e-mails
  The following two types of bulk distribution are noticeable

  - Delivery using spambots
    - Transmit from IP addresses in and out of the country, direct delivery
    - The sender's e-mail address can vary (proprietary domain)
    - Be distributed over and over to a large number of destinations in the same text or URL
    - Recipients of the same domain often list their email addresses

  - Distribution via facilities (servers) of domestic operators
    - The sender's e-mail address may be spoofed, but it uses its own domain and the company's domain.
    - Passing and Sending SMTP Authentication as a Regular User
    - There are cases where a contract is made with a business operator and cases where a exploited account is thought to be used.
    - The originator was from CN, HK, TW in the scope of the search
    - The source IPs were registered in some DNSBL

Destination Phishing URL

- Specify phishing site directly
  - To acquire many domains and build phishing sites at the same time
- Cases involving multiple redirects
  - It is usually about two steps. Many of Apple's phishing sites are multi-tiered.
- Use of shortened URLs
  - Twitter, Linkedin, bitly, GoDaddy, Frama.link, ・・・・・・

Multiple Stages of Phishing Sites

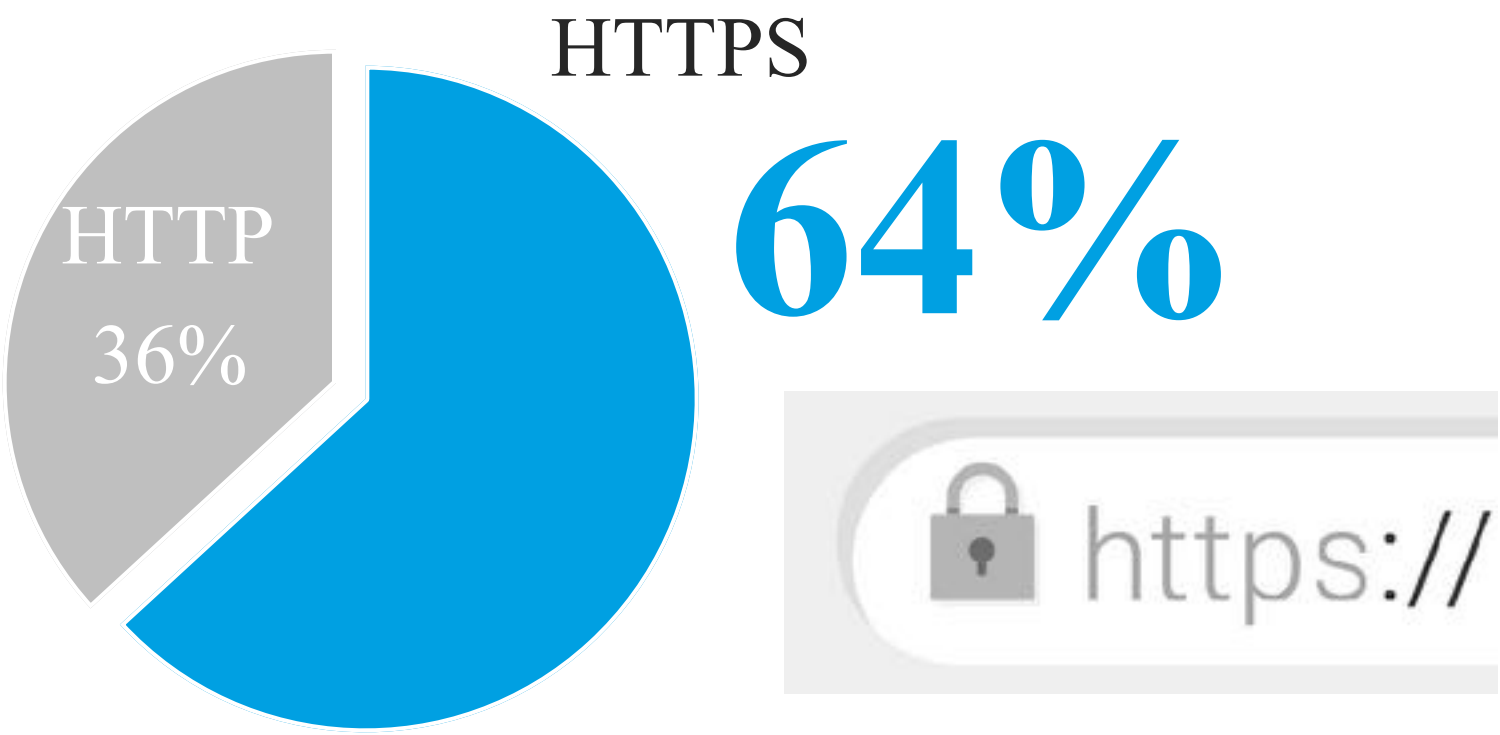
- Leading to phishing sites via abbreviated URLs and relay sites

No	Description	Example Redirect Transitions
1	Destination URL in the mail	http://aqq22.asrksssnsifsada.org/
2	Relay site	http://165.22.53.5/bangkol
3	Relay site	https://sebujakeosk.biz/account1.php
4	Phishing sites	https://anjro04218-accoi.dynv6.net.anjro04218-accoi.dynv6.net/yoibosku/?reset

- Even if the phishing site is closed, the forwarding site remains for a long time, and the new phishing site is linked to the forwarding site

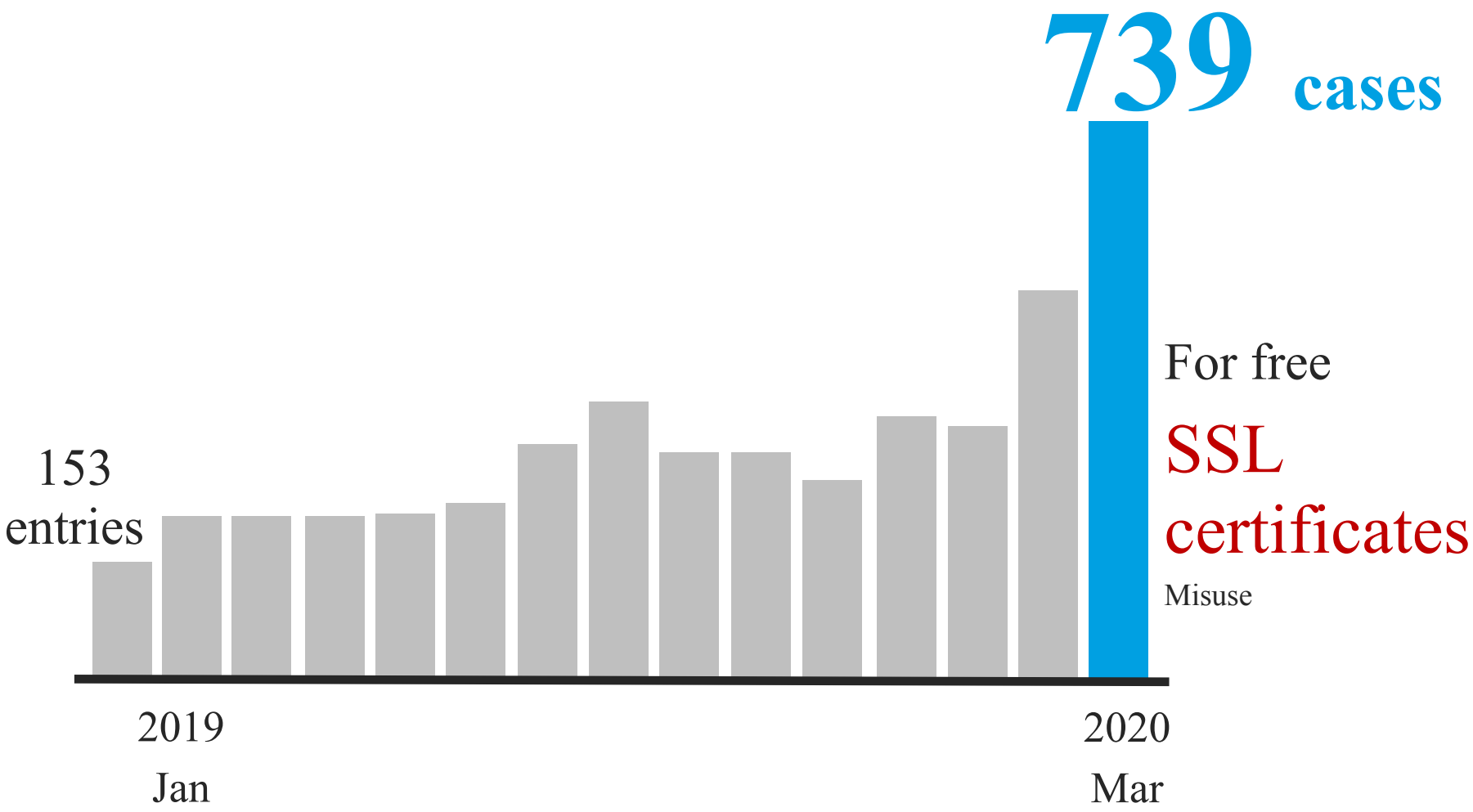
Phishing Sites With Server Certificates that Begin With https://

- Server certificates are often used on phishing sites and https are often used



Survey conducted from January to March 31, 2020

Phishing Sites Hosted on HTTPS



The usage of Let's Encrypt is very high

Improved phishing technics

- More natural Japanese language usage due to improvements in machine translations.

- Understanding of Japan's current culture and social dynamics
  - Amazon, Rakuten, LINE, are being targetted
  - Usage of Japanese fonts(used to be other Asian fonts)
  - Domestic delivery agent phishing SMS

Awareness Activities

For enhancing cyber security
Awareness campaign

STOP 立ち止まる | THINK 考える | CONNECT™ 楽しむ

STC Awareness Working Group of the Council of Anti Phishing Japan

STOP THINK CONNECT

Thank You for Your Attention.

- Phishing Information
  - Facebook
    https://www.facebook.com/StopThinkConnectJapan/(Link)
  - Twitter
    @antiphishing_jp

- Phishing Reporting Contacts
  - Mail to "mailto:info@antiphishing.jp"!
  - For details, "https://www.antiphishing.jp/contact.html"

For phishing sites in the JP domain
Contact the council!
If you receive an inquiry from JPCERT or the council, please respond.

Thank you !

フィッシング対策協議会
Council of Anti-Phishing Japan