- Regarding cyberspace, while it has become a public space where all citizens participate and engage in important socio-economic activities, there has been an increase in the occurrence of cyber incidents with more sophisticated and serious methods.
- Incidents of unauthorized access attempting to steal information have occurred. Furthermore, there has been a sharp increase in credit card fraud and online banking fraud. Additionally, the number of ransomware attacks remains at a high level, indicating an extremely serious situation that continues unabated.

◆Situation regarding unauthorized access aimed at stealing information

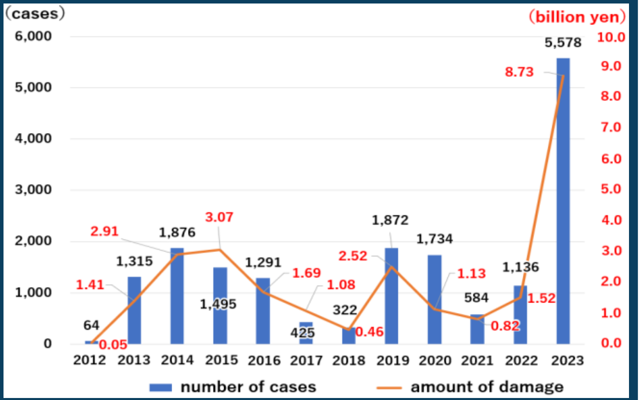
Notable incidents

- In October 2023, an academic institution in Japan announced that as a result of spear-phishing attacks, computers used by staff were infected with malware, leading to unauthorized access. There is a possibility that personal information may have been leaked around May 2023.
- In November 2023, a research and development institution in the aerospace sector in Japan revealed the possibility that unauthorized access was made to the organization’s intranet management server around the summer in 2023.

◆Situation regarding online banking fraud

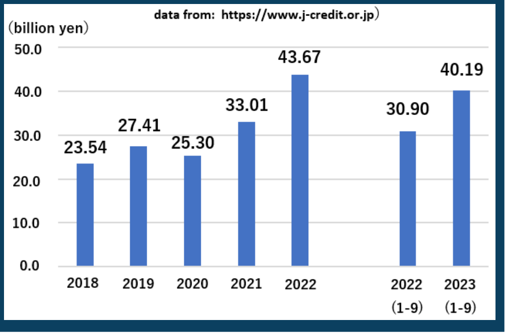
Trend of incidents and damage caused by online banking fraud

- The number of the online banking fraud cases was 5,578, with a total damage amounting to approximately 8.73 billion yen.
- The number of cases increased by 4.9 times compared to the previous year. The total damage also increased by 5.7 times, both reaching record highs.



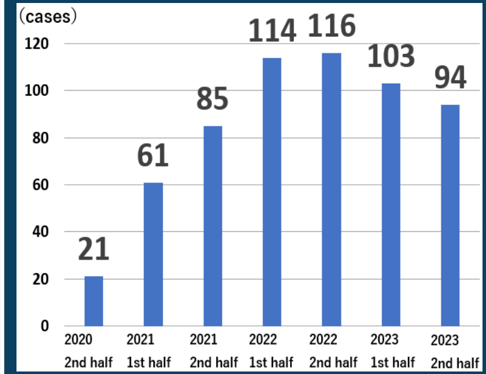
Trend of credit card fraud losses

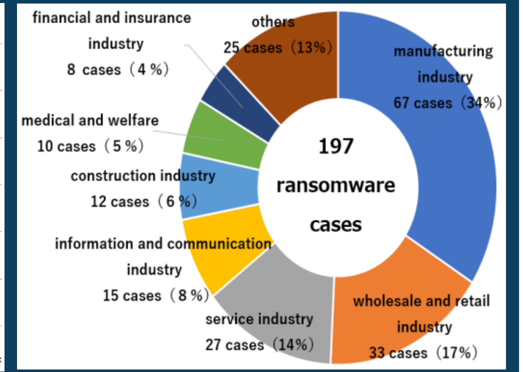
- The credit card fraud losses from January to September 2023 amounted to approximately 40.2 billion yen, showing an increase compared to the same period of the previous year and continuing to remain at a high level.
- The majority of the damage was caused by credit card number theft. The main method was to steal credit card numbers by phishing, and impersonate the cardholders.



◆Situation of damage caused by ransomware and similar attacks

- The number of ransomware cases was 197, remaining at a high level.



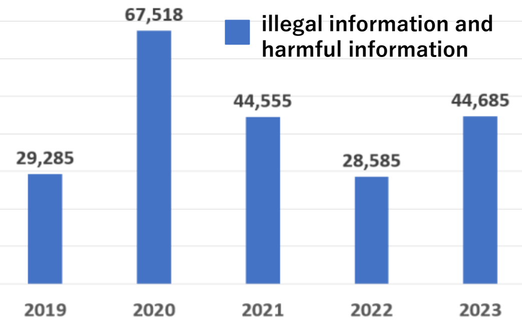


- In addition to damage caused by ransomware, a new method involving the theft of data without encryption and demanding ransom (known as ‘no-ware-ransom’) has been identified with 30 cases confirmed.

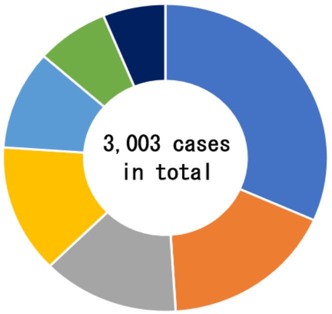
◆Situation of illegal and harmful information on the Internet

Handling of illegal and harmful information in IHC

- The Internet Hotline Center (IHC) accepts reports of illegal information, serious-crime-related information, and information that may incite suicide on the internet, and reports them to the police while also requesting deletion from internet service providers and site administrators.
- Based on the operational guidelines of the IHC, the analysis resulted in the identification of 44,685 pieces of information judged as illegal or harmful. Among these, there were 4,876 cases of serious-crime-related information reported to the IHC for the first time in 2023.



◆Situation of cleared cyber incidents



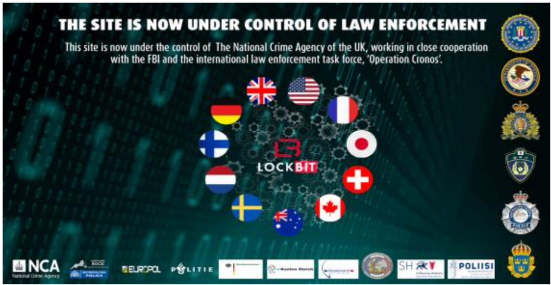
- 🟦 computer fraud : 950 cases (31.6%)
- 🟧 violation of Act on Prohibition of Unauthorized Computer Access : 521 cases (17.3%)
- ⬜ fraud : 409 cases (13.6%)
- 🟨 violation of Act on Prevention of Transfer of Criminal Proceeds : 405 cases (13.5%)
- 🟦 unauthorized creation or use of electromagnetic records : 313 cases (10.4%)
- 🟩 theft : 218 cases (7.3%)
- ⬛ others : 187 cases (6.2%)

◆Main measures implemented by police

- In February 2023, the National Police Agency (NPA) expanded the scope of the information dealt with in the Internet Hotline Center and the Cyber Patrol Center to include serious-crime-related information. Additionally, in September 2023, the NPA further strengthened the operational framework related to measures against illegal and harmful information by adding recruitment information for criminal actors to their handling scope.
- In April 2023, the NPA signed a memorandum of understanding with the Japan Medical Association, in order to proactively prevent cyber incidents such as ransomware in medical institutions and to facilitate swift reporting and consultation to the police in the event of an incident.
- In September 2023, the NPA released the joint cybersecurity advisory with NISC, as well as FBI, NSA, and CISA in the U.S. regarding cyber attacks conducted by the China-linked cyber actors known as ‘BlackTech’.
- In February 2024, in collaboration with the FSA, the NPA requested to the financial institutions for strengthening measures against illicit transfers to cryptocurrency exchange service providers.

◆Main activities of the National Cyber Unit

- As a result of the National Cyber Unit’s efforts to promote international joint investigations with Europol and others, in February 2024, law enforcement agencies in related countries arrested two suspects believed to be members of the cyber attack group LockBit, which is responsible for ransomware attacks on companies worldwide. Furthermore, they conducted raids on servers and other infrastructure used by the group and displayed a ‘splash page’ on leak sites.



THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT

This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, ‘Operation Cronos’.

Threats in Cyberspace in 2023

Cyber Affairs Bureau
National Police Agency of Japan
March 2024