Chapter 3 Securing Safety in Cyberspace

Section 1 Threats in Cyberspace

1 Characteristics of Threats in Cyberspace

The Internet has become recognized as a social infrastructure essential to citizens' lives and socioeconomic activities. Today, while cyberspace has become a part of citizens' daily lives, cybercrimes such as online banking fraud are frequently committed, and cyber attacks including cyber terrorism and cyber espionage are often carried out on a global scale. Thus, threats in cyberspace are becoming serious. During 2014, the techniques used for cybercrimes such as online banking fraud and spear phishing email attacks were found to have grown more vicious and sophisticated, and the presence of "crime infrastructure" in cyberspace, including malicious proxy servers, was confirmed. In addition, new techniques and services that have the potential to be used by individuals for crimes in cyberspace arose, as seen in the case where an individual used a 3D printer to manufacture a homemade handgun. Much harm was caused by unauthorized login attacks and by the provision of privately recorded sexual images. Thus, there was a tendency for Internet use to lead to an increased risk of Internet users' involvement in crimes.

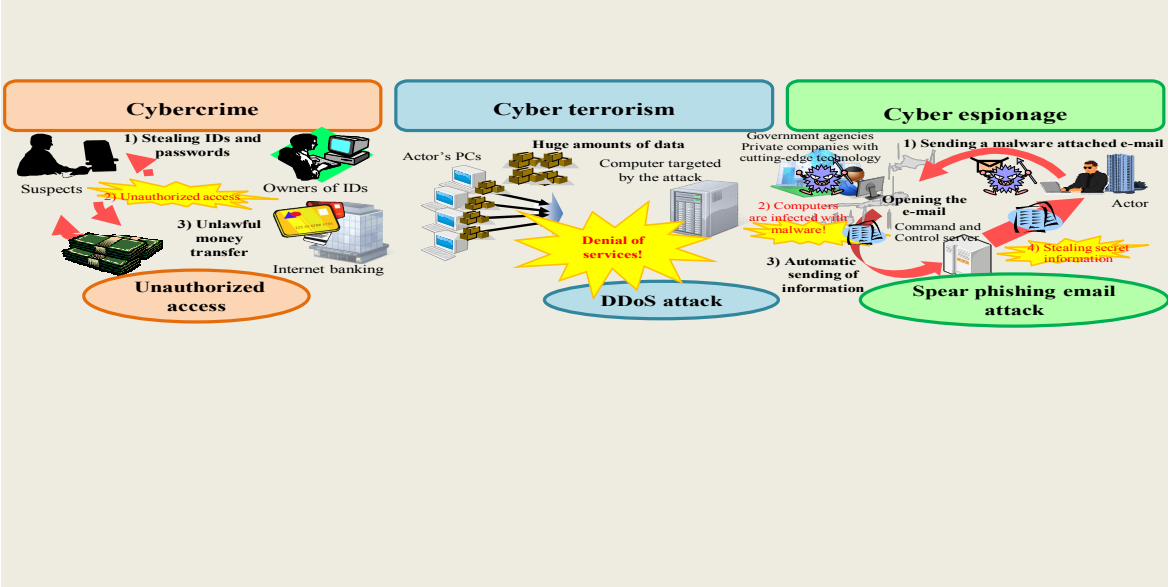
2 Cybercrime

In 2014, the number of cleared cases for cybercrime was 7,905, a year-on-year decrease of 208 cases.

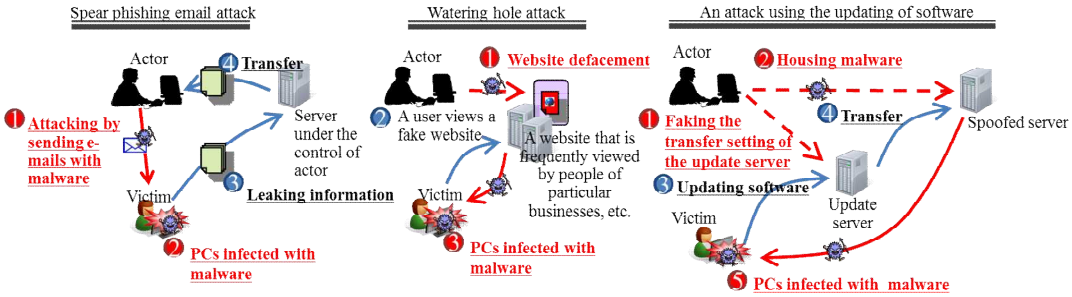
3 Cyber Attacks

In recent years, cyber attacks have been occurring in Japan against entities such as government agencies and private companies, and the techniques used are becoming more ingenious. In particular, threats of cyber terrorism, which is an electronic attack causing the core systems of critical infrastructure malfunction and paralyze social functions, and cyber intelligence, which is espionage operation using information and communication technology, are becoming problems that may impact the country's public safety and security.

Threats in cyberspace



Modus operandi of cyber espionage



Section 2 Dealing with Threats in Cyberspace

1 Measures against Cybercrimes

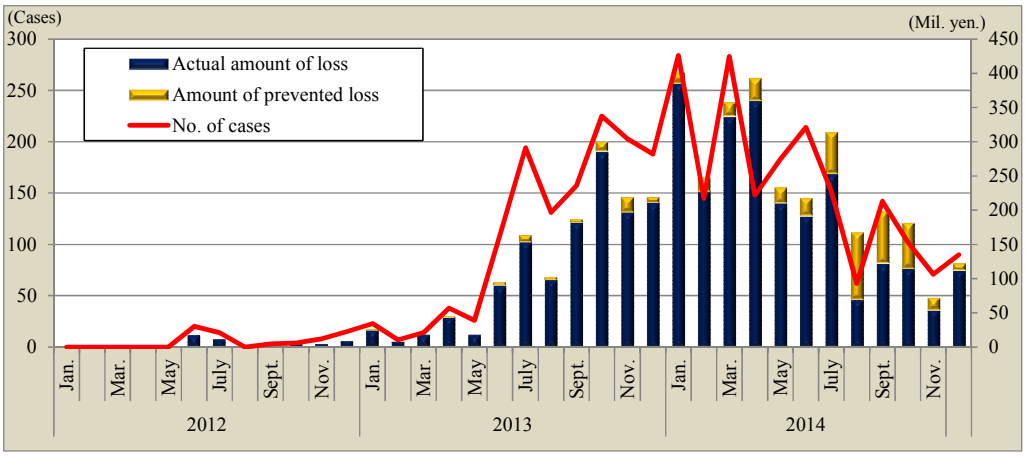
(1) Measures against Online Banking

The total loss caused by illegal money transfers has sharply increased since 2013, reaching about 2,910 million yen in 2014, which is the highest to date. The police arrested 233 persons who were involved in illegal money transfers during 2014. In addition, the police have, in collaboration with private companies, implemented preventive measures such as requesting financial institutions to strengthen the security capacity of online banking.

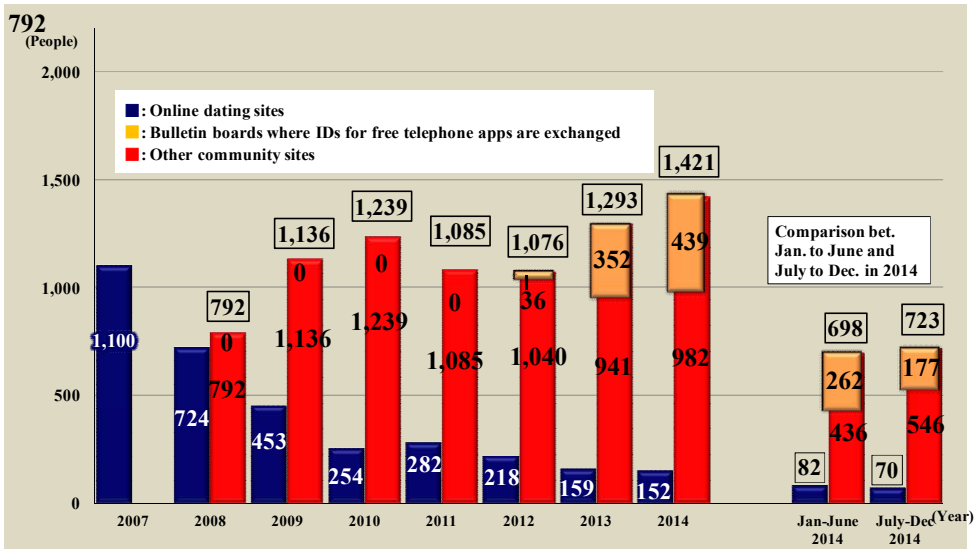
(2) Measures against Crimes Arising From Online Dating Sites and Community Sites

The number of children becoming victims of crimes involving online dating sites has shown a decreasing trend while the number of children becoming victims of crimes arising from community sites has shown an increasing trend since 2013, due to the increase in the number of victims of crimes involving online bulletin boards where IDs for free-telephone apps can be exchanged. To prevent crimes involving children's use of community sites, the police are promoting the enhancement of website monitoring and are making efforts to introduce effective "Internet zoning", in addition to promoting publicity and public relations and educational activities for the purposes of further spreading filtering and of preventing crimes involving children. The police are making these efforts in collaboration with related government ministries and agencies and other organizations.

Trends in the number of online banking fraud by month



Trends in the number of child victims of crimes involving online dating sites and community sites



Note: Statistics of other community sites is available since 2008.

Section 3 Promoting Collaboration between Government and Private Sector against Threats in Cyberspace

1 Promoting Collaboration between Government and Private Sector against Threats in Cyberspace

In order to counter the threats in cyberspace, it is necessary to collaborate with private companies. Therefore, the police are establishing a framework to cooperate with entities such as private companies and are utilizing their knowledge to prevent harm caused by cybercrimes and cyber attacks and to ensure an accurate response in the event of an incident.

Framework for countermeasure with private sectors