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. At the same time, today, cybercrimes such as online banking fraud are frequently committed, and cyber attacks including cyber terrorism, which is an electronic attack causing the core systems of critical infrastructure malfunction and paralyzes social functions and cyber espionage, in which confidential information from government agencies and companies with advanced technology are stolen, are often carried out on a global scale. Thus, threats in cyberspace are becoming serious.

2 Cybercrime

In 2015, the number of cleared cases for cybercrime was 8,096, a year-on-year increase of 191 cases.

3 Cyber Attacks

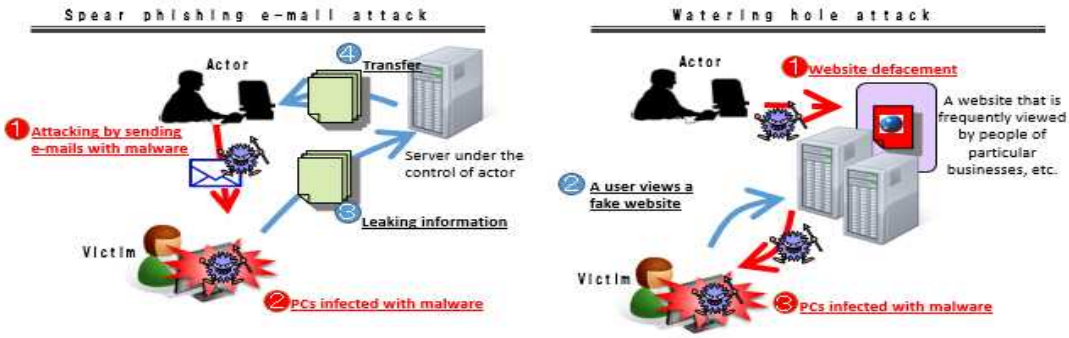
Threats of cyber terrorism and cyber espionage aiming at stealing confidential information such as advanced technology, which can be converted to military technology and the national strategy in diplomatic negotiations are becoming problems in many countries around the world.

Also, in view of the fact that the threats of terrorism against Japan have become a reality, that can be a preparation for physical terrorism, there are risks of cyber

Threats in cyberspace

1: Abbreviation for Distributed Denial of Service, that repeats a large number of accesses from multiple computers to a specific computer and make it impossible to provide service.

Modus operandi of cyber espionage



intelligence that intrude the system of important infrastructure companies and steal information on the security system.

Section 2 Dealing with Threats in Cyberspace

1 Measures against Cybercrimes

(1) Measures against Online Banking

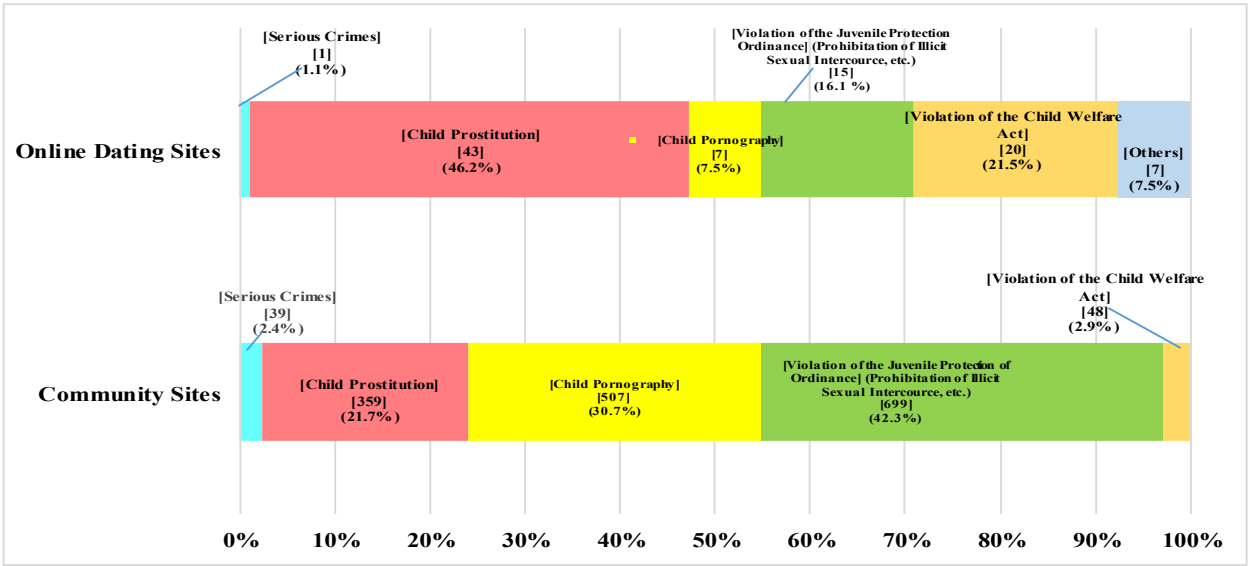
The total loss caused by illegal money transfers sharply increased to approximately 1,406 million yen in 2013, and approximately 2,910 million yen in 2014. Although the total loss decreased somewhat in the second half of 2014, it increased again in the first half of 2015, reaching approximately 3,073 million yen in the year, which is the highest to date. In addition, in 2015, loss extended to credit unions, agricultural cooperatives and other financial institutions, in particular, the loss to corporate accounts of credit unions sharply increased and major banks were damaged frequently from April, thus the situation is becoming serious. Besides, the account holders of the illegal beneficiaries are characterized by a high proportion of those with Chinese nationality.

The police arrested 160 persons who were involved in illegal money transfers during 2015. 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 2008. 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", and furthermore, are promoting publicity and public relations and educational activities for the purpose of further spreading and of preventing crimes involving children. The police are making these efforts in collaboration with related government ministries and agencies and other organizations.

Number and ratio by crime on child victims of crimes involving online dating sites and community sites (2015)



Section 3 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, and the police are carrying out various efforts such as establishing a framework for personnel exchanges and information sharing on new types of malware.

In addition, at the Japan Cybercrime Control Center (JC3) whose operations started in 2014 as a new framework of collaboration among industry, academia and government agencies in Japan, the separate information and expertise of industry, academia and government agencies are collated and the results are provided to each sector to identify any source of threats in cyberspace. The JC3 aims to prevent cybercrimes by mitigating and neutralizing cyber threats. The police share information related to their investigations of the threats with the JC3 to contribute to the efforts by industry and academia to enhance cyber security while working to build safe and secure cyberspace by adequately and promptly utilizing information shared through the JC3.