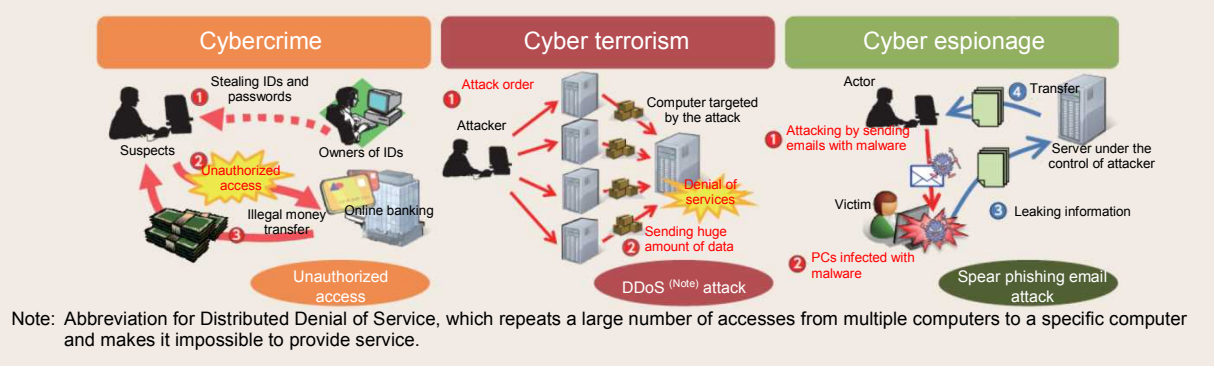
Chapter 3 Securing Safety in Cyberspace

Section 1: Threats in Cyberspace

The Internet has become recognized as a social infrastructure essential to people's lives and socioeconomic activities and cyberspace has become a part of people's everyday life. At the same time, threats in cyberspace are becoming increasingly serious. For example, cybercrimes such as illegal money transfers via online banking are frequently committed, and cyber-attacks including cyber terrorism which can cause the core systems of critical infrastructure to fail and paralyze social functions, and cyber espionage by which someone steals confidential information from government agencies and companies with advanced technology, are often carried out on a global scale.

Threats in Cyberspace



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

[Column] Computer Virus Demanding Ransom, "Ransomware"

Recently, there has been damage caused by a computer virus called "ransomware." Ransomware restricts the function of the infected computer, and demands that the user of the infected computer pay ransom in exchange for restoring a normal function of the computer.

In May 2017, computers of government agencies, hospitals, banks and companies in many countries were infected with ransomware called "Wannacry," and the infection was confirmed in Japan as well.

The police are striving to investigate the actual condition of the infection, and are making efforts to prevent the infection from spreading.

Section 2: Dealing with Threats in Cyberspace

1. Strengthening Comprehensive Cyber Security Measures

Dealing with threats in cyberspace has become a significant issue for all divisions of police, which requires the entire police force to strengthen their abilities to deal with such threats under a unified strategy. Therefore, in order to strengthen NPA's functions as headquarters for cyber security measures on the whole, the NPA has established the Director-General and the Director for cyber security that manage and coordinate various cyber security initiatives.

2. Measures against Cybercrimes

(1) Measures against Illegal Money Transfers via Online Banking

The total loss caused by illegal money transfers sharply increased to approximately 1,406 million yen in 2013, 2,910 million yen in 2014 and 3,073 million yen in 2015, which is the highest to date. However, the total loss significantly decreased in 2016 to approximately 1,687 million yen (decreasing by 45.1% as compared with the previous year) due to a decrease of the losses that Shinkin banks (a kind of Japanese depository institutions) incurred. The decrease of the losses is attributed to Shinkin banks' use of anti-virus software which detects access from computers infected with malicious programs.

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

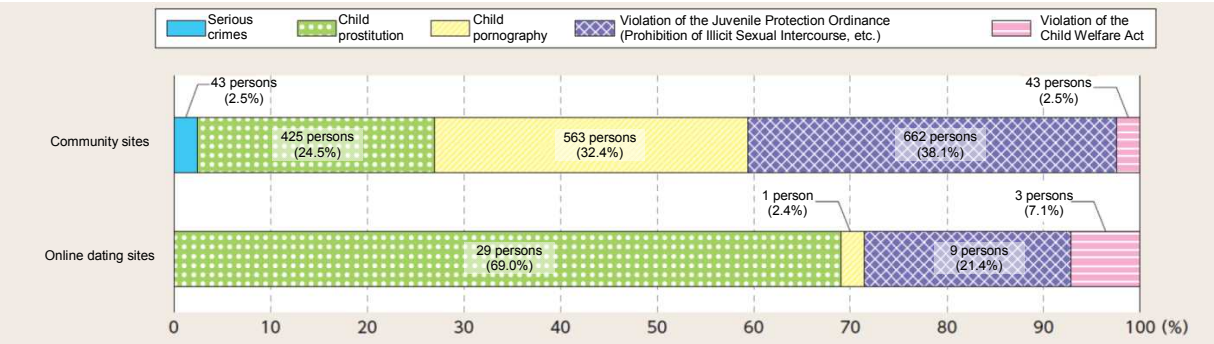
The number of children becoming victims of crimes attributable to community sites has been increasing since 2008, reaching the highest record level of 1,736 in 2016.

On the other hand, the number of children becoming victims of crimes attributable to online dating sites has been decreasing since the revision of the Act on Regulation on Soliciting Children by Using Opposite Sex Introducing Service on Internet in 2008, and the number was 42 in 2016. The decrease stems from the revision of the Act. The revised Act obligates online dating business operators to notify a local public safety commission of items the Act stipulates, that facilitates a good grasp of the actual condition of online dating business operators and to prevent children from becoming victims of crime.

As part of the measures to prevent children from becoming victims of crimes attributable to the use of community sites, the police, as to the size of website operators and what the operators provide, are promoting enhancement of website monitoring including checking posted contents and pushing website operators to introduce effective "Internet zoning". In addition, the police are conducting thorough crackdowns on unregistered malicious online dating site operators which do not make notifications required by the Act, and those who conducted prohibited solicitation activities on online dating sites as measures to prevent children from becoming victims of crimes attributable to online dating sites.

Furthermore, the police are conducting cyber guidance on community sites and online dating sites and promoting measures, such as dissemination of the use of filtering services mainly for smartphones and awareness raising for children, their parents and those concerned with their school, efforts at preventing children from becoming victims of crime.

Number and Ratio by Crime on Child Victims of Crimes involving Community Sites and Online Dating Sites (2016)



3. Measures against Cyber-Attacks

The NPA and prefectural police have units responding to cyber-attacks, and each division of the NPA and prefectural police is collaborating to promote elucidation of the actual condition of cyber-attacks and prevention of damage due to cyber-attacks. The police are also working on measures such as strengthening of cooperation on investigation and information gathering with foreign security intelligence agencies, and establishment of cooperation with the private sector to foil damage due to cyber-attacks to deal with ever-changing situations over cyber-attacks.

4. Promoting Public-Private Sector Collaboration

(1) Council for Countermeasures against Cyber Terrorism

The police have set up the Council for Countermeasures against Cyber Terrorism that consists of critical infrastructure operators which might be a target of a cyber-attack, and conduct joint drills, assuming that cyber-attacks will take place, as well as provide information on threats of cyber-attacks and information security, hold seminars by experts from the private sector and urge information exchange and information sharing among member business operators.

(2) Collaboration with the Japan Cybercrime Control Center

The Japan Cybercrime Control Center (JC3), launching its operations in 2014 as a new framework of industry-academia-government collaboration in Japan, aims to identify the source of threats, by collecting and analyzing information and intelligence provided from businesses, academic community and governmental agencies, and returning results of the analysis to them, and to prevent cyber incidents taking place, by mitigating and neutralizing the source. The police contribute cybersecurity efforts made in industry and academic community, sharing information on investigation with the JC3, and make efforts to build safe and secure cyberspace by making use of information with promptness and accuracy shared with the JC3 for police activities.