




Topic III: A New Framework of Collaboration between Industry, Academia and Government to Cope with Threats in Cyberspace

(1) Current Threats and the Need for Additional Undertakings

Although Japan achieved some positive results in its efforts dealing with threats in cyberspace, these efforts focused on measures against each specific case that had happened. Japan has not yet been able to take proactive and comprehensive measures against the ever-shifting pattern of threats to ensure future threats to be neutralized before it happens. Industry, academic institutions, and law enforcement agencies such as the police, were playing key roles in coping with cyber threats while accumulating a wealth of knowledge and experience in dealing with them. However, each of these sectors was acting independently in promoting their various measures. Sufficient efforts were not made for the coordinated integration and analysis of such knowledge and experience in order to formulate effective countermeasures. In the Strategy to Make Japan "the Safest Country in the World", approved by the Cabinet in 2013, and also at the Advisory Council for NPA on Cyber Security⁹, it had been noted many times that a new organization needed to be created. The National Cyber-Forensics & Training Alliance (NCFTA) in the United States of America, a non-profit organization attaining positive results within the framework of collaboration between industry, academia and government, was suggested as a model.

Chart III-1 Challenges in dealing with threats in cyberspace

 Industry	<p>◆ Having knowledge and real-time information of the threat from cyberspace</p> <p>However, No effective measures, such as arrest of suspects, are available.</p>
 Academic institutions	<p>◆ Having high level skills and knowledge from research.</p> <p>However, Have no real experience handling threats in cyberspace</p>
 Law enforcement agencies	<p>◆ It is possible to make a specified case that is related to a specific threat ineffective by understanding the details through investigation and other police activities</p> <p>However, The threat of the entire scope of cyberspace has not been thoroughly understood</p>

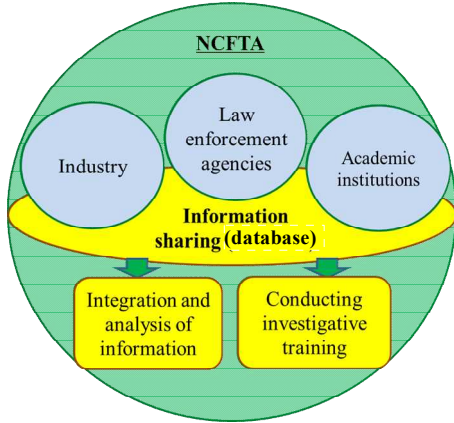
(2) Outline of the NCFTA

With the aim of effectively coping with increasingly complex threats in cyberspace, the NCFTA was established in 1997 in the U.S.A. The NCFTA brings together law enforcement agencies, private industry, and academia to share and analyze real-time information on the threats, so that multiple sectors can work jointly towards cyber threats.

The results that the NCFTA obtains by integrating and analyzing the information it collects are provided to law enforcement agencies and private companies. The NCFTA also has training programs for investigators. The NCFTA's proactive and comprehensive efforts within the framework of collaboration between industry, academia and government have produced positive results. For example, the NCFTA helped seize criminal proceeds and prevent potential losses in the investigation of cyber financial crime. The NCFTA is highly admired inside and outside the U.S.A., with initiatives modeled after the NCFTA having been undertaken in other countries.

⁹: The Advisory Council on Cyber Security has been held by the NPA since FY2001 to generate discussion by experts on cooperation between industry and government agencies, particularly the police in order to ensure the security and reliability of info-communications network.

Chart III-2 Structure of the NCFTA



(3) A New Framework of Collaboration between Industry, Academia and Government in Japan

I. Establishment of JC3

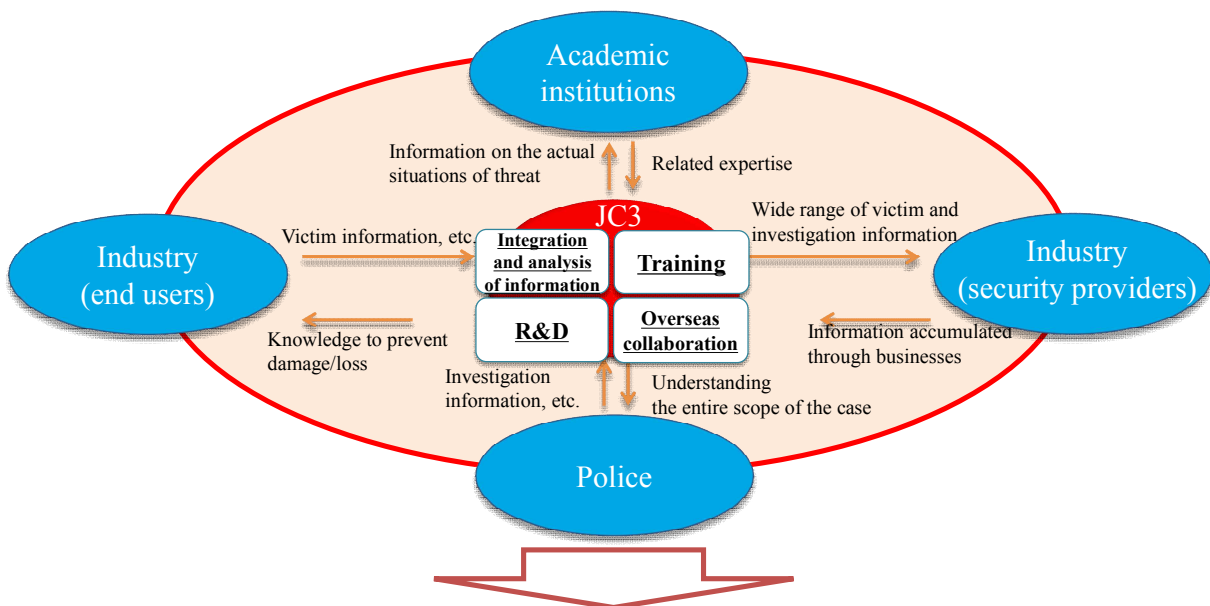
After considering the circumstances, the NPA and other entities deliberated on the establishment of a new organization, resulting in the establishment of the Japan Cybercrime Control Center (JC3). The center started operations on November 13, 2014.

At the JC3, the separate information and expertise of industry, academia and government agencies are collated and the results are provided to each sector to identify any sources of threats in cyberspace. The JC3 aims to prevent cybercrimes by mitigating and neutralizing cyber threats. By providing the

public with the information that the JC3 integrates, the JC3 helps create a safe and secure Internet environment for the public. In order to maximize its potential, the JC3 is building relationships with the NCFTA and other organizations overseas for the purposes of sharing information and cooperating with each other.

II. Cooperation between the Police and the JC3

In January 2013, the police formulated the Immediate Action Program for the Reinforcement of the Abilities to Cope with Cybercrimes. Based on this program, the police have been strengthening partnerships with private businesses in order to cope with cybercrimes. After the inauguration of the JC3, the police began to use the JC3 as a hub for collaborating with an increasing number of partners in industry and academia on a routine basis, not just cooperating with individual companies after each case but also aiming at the development of a new framework of collaboration between industry, academia and government. At a forum held by the JC3 in February 2015 and other opportunities, the police have actively exchanged views and information with experts from industry and academia regarding financial crimes, information leakage and other issues.



Understanding the entire scope of the threat in cyberspace enables the addressing of issues

It is expected that close cooperation with the JC3 will make it possible for the police to take proactive and comprehensive measures against threats in cyberspace. For example, information about malware will be integrated at the JC3 from industry, academia and government agencies for analysis to identify the relevant command-and-control servers. This will enable the police to exercise their statutory authority of investigation for neutralizing these servers and preventing any potential losses. The police will in turn 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. Efforts will be accelerated toward the creation of a safe and secure cyberspace by adequately and promptly utilizing information shared through the JC3 for effective police operations.



JC3 Forum 2015