公益財団法人　セコム科学技術振興財団
研究成果報告書

研究課題名

情報法学・マネジメント論と侵入防止技術の融合による超セキュア情報システム

Ultra-Secure Information Systems by Integrating Information Laws, Management Methodologies and Invasion Prevention Technologies

研究期間

平成 25 年　4 月　～　平成 29 年　3 月

報告年月

平成 29 年　6 月

研究代表者
東京大学　情報理工学系研究科　電子情報学専攻　教授
坂井　修一

Professor
Department of Information and Communication Engineering,
Graduate School of Information Science and Technology,
The University of Tokyo
Shuichi Sakai

Abstract

Along with the development of the information system as a social infrastructure, it is the pressing need for us all to ensure information security. In recent years, zero-day attacks and targeted attacks cause serious troubles such as leakage of important information and takeover of IT systems. Leakage of private information and invasion of privacy have become two of the most significant social problems. This research project aims to propose, design and verify innovative technologies, laws, policies and management systems in each field and to research and develop methods that comprehensively solve by the integration of the all fields.

The subject areas here are jurisprudence on information society, management systems, and information system engineering.

At the preparation stage, we conducted surveys in each field, concretely analyzed the most important problems, investigated the requirements of policies and technologies, proposed and preliminarily evaluated the basic ideas on both sides of the social science and the technology. In addition, we examined integration of the social science and the technology, and conducted case studies on cyber attack prevention and personal information protection, respectively, and made a prospect for the outcome of this research as a whole.

[Juriprudence]

The Japanese information law is based on the concept of respecting universal value of individual, the Personal Information Protection Commission takes a significant role in harmonization the rules of privacy and personal data protection with the ＥＵ and the United States. The Commission aimed to establish a system of executive cooperation with other countries, and have proposed a revision for such while maintaining to consider Japan's personal information protection legislation.

Meanwhile, in the background, the declining of the birth-rate and the elderly population in Japan has made the maintenance of the social security system getting structurally difficult. As individual burden increases day by day, the survival rights of individual are being threatened.

In order to maintain the social security system, increasing tax revenues through economic growth and securing financial resources are major issues. The "Big Data Business" is consider as one of the information technology (IT) industries that can contribute to such the growth. As such to promote the IT industry, innovation through research and development is required. It is a prerequisite to establish a legal system that secures freedom of academic and research, and to develop a legal framework to ensure distribution of information across the border as well as domestically. These prerequisites are reflected in the revised draft of the Personal Information Protection law.

[Management System]

In order to develop more effective information security management system, we took firstly a literature survey mainly focusing on the ISMS standards which has been rapidly developed since

around 2000. At the same time, we also made an investigation of actual practices by making enquires and interviews upon large sized commercial companies in Japan. Based on these preliminary surveys, underlying requirements, problems and our research focus for information security management are identified.

In addition, we examined international Enterprise Architecture standards and their consideration in information security to apply its intrinsic holism characteristic of EA as we thought the study of EA would enrich our research.

A mathematical risk analysis method and tangible governance process were developed as a result of these considerations, since we understood that the two prevalent key problems in this field are lack of objective risk analyses and malfunctions of senior officers' roles in information security management. Existing information security standards, related researches, actual information security system and incidents in Japan and U.S. government are also reviewed to verify our discussion.

On the ground of the above, we proposed a novel systemic approach of information security governance. Our result fills the gap which resides among existing standards, researches and practices. It clarifies the importance of information security to business, and provides a mean to complement the weaknesses of technology based security solutions. Although we also surveyed the situation of the latest security measures such as the Cyber Security Directive of the U.S. Obama Administration, it is almost omitted from our reports; their focus is put on critical infrastructure protection and information sharing for its purpose.

Our proposed approach of information security governance is applicable to information security management system in governments implemented under, for example, FISMA(Federal Information Security Modernization Act) or another similar information security management concepts like in Japan.

[Technology]

In security technology (especially intrusion prevention technology in this case), we analyzed cases of intrusions and information leaks from the past to the nearest, and also collected observation data of computer abnormal states. Based on these, we established the principles of an intrusion detection system and information leakage prevention platform, and specifically examined detection methods and countermeasures in case of intrusion. In order to comprehensively prevent data leakage and tampering, we focused on the following three subjects and conducted research.

The first is security assurance in the case where the system administrator and the right holder of the data are different. Protection from tampering of client information by a cloud provider and from illegal duplication of DRM contents by a user system are two of the examples. In this research, focusing on secure processor technology to solve such problems, we have developed the mechanism and organization of the VM secure processor "Sharkcage" based on the recent VM technology. By using the processor as the base of trust in the core of the computer system, it is proved possible to

guarantee that the intention of the legitimate right holder is properly reflected in processing. It realizes platform validity authentication and confidentiality / integrity of external data by appropriate cryptographic technology, and reduces the overhead of cryptographic processing by architectural technology to achieve both efficiency and security.

The second is to prevent from an intrusion exploiting carelessness of administrators and programmers. Virus infection and data alteration due to vulnerability, data stealing by the phishing site, system takeover by Trojan horses, Ransomware, etc. are getting fiecer and fiecer. The basic countermeasure technique was to record bit patterns and behavior patterns of the attack signals to create a database and quarantine attacks at the water's edge. However, it is currently quite difficult to cope with highly intentional and dangerous attacks, such as zero-day attacks and targetted attacks. In this research, we develop "information flow tracking technology" and realize a system that the computer constantly inspects the computer itself whether the operation the computer is about to do is intended by the rightful right holder, and detects the attack.

The third is to protect against social hacks exploiting how people use IT systems. Even if security measures are correctly taken on the system, intrusions from the interface of physical world / virtual world have been rapidly increasing, exploiting people's way of using IT devices such as passwords carelessly written down or easily guessable by IoT sensors, and of carelessly using a malicious wireless router pretending to be legitimate. It is expected that these kinds of attacks will become more and more universal and advanced as the information platform gets smaller and more wireless. In this research, we developed a human computer interaction (HCI) technology that allows users to log in and connect to IoT devices and computer systems intuitively for users. Based on user's location information and gestures, it can connect securely without making a password to wireless routers, IoT devices, household appliances, etc.

[Integration]

As for the integration of research fields, we examined what juriprudence, management, and technologies should do for zero-day attacks, targetted attacks, personal information leakage and copyright infringement, based on the latest results of each field and each new role sharing, and cooperation.