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

コンピュータの原理原則に着眼したセキュリティカーネル技術とその応用に関する研究

Research on Security Kernel Technology which is based on the Principles of Computer, and its Application

研究期間

平成26年　4月　～　平成30年　3月

報告年月

平成30年　6月

研究代表者

東京電機大学 サイバー・セキュリティ研究所 副所長
上野 洋一郎

Associate Director, Tokyo Denki University Cyber Security Laboratories
Yoichiro UENO

Abstract

Tokyo Denki University Cyber Security Laboratories and F.TRON Inc collaborate on research and development of the Security Kernel Technology, which is based on the principles of computer. The Security Kernel Technology may get some lead in malwares.

The principles of computer is based on execution order and protection ring mechanism of CPU. Protection ring of CPU has 4 levels (Ring 0 – 3) and Ring 0 is the level with the most privileges. The privileges of machine language instructions are defined by current protection ring level of CPU. Currently, all application programs are executed in Ring 3, and kernel code of operating systems are executed in Ring 0. If malwares run as application program which is executed in Ring 3, operating system with privilege of Ring 0 should be able to detect and control such malwares. However, as operating system have to communicate with all applications and have some security holes, most malwares try to get highest privilege of Ring 0 via security holes. If some malwares get the Ring 0, they may hide themselves and have some bad influence on operating system.

If someone want to separate security soft from all bad influence of malware, they have to provide the higher privilege to security soft than operation system.

In the principles of computer, the Security Kernel Technology is loaded to the main memory and booted before operating system, for getting protection privilege of Ring 0. Then, the Security Kernel Technology loads operating system code to the main memory and start in Ring 2. So, computers with the Security Kernel Technology assure higher privilege to the Kernel Security Technology than operating system and application programs. And, the Kernel Security Technology places oneself in the memory area, which are not able to recognize from operating system. Therefore, all programs under operating system can't access to the Kernel Security Technology and such computers becomes safety.

All computers with the Kernel Security Technology are able to form a new safety overlay network on the Internet, with mutual authentication and unique cryptography. In such overlay network, we should place the Secure Space which is consists of some servers. These servers provide network services only to computers within overlay network. This overlay network with the Kernel Security Technology and Secure Space will be realize the reliable and safety network service foundation over the Internet.