公益財団法人 セコム科学技術振興財団

（平成 23 年度～平成 27 年度）

次世代ネットワークにおける持続的標的型攻撃の検出手法の開発

Development of Detection Methods for Advanced Persistent Attacks on the Future Network

2016 年 6 月

研究代表者

国立情報学研究所　教授　高倉 弘喜

National Institute of Informatics, Professor, Hiroki Takakura

Because of rapid sophistication of Cyberattacks, it is quite difficult for conventional countermeasures to sense their existence not only to block them. With rapid growth of application of Internet Technology, such as IoT, existing countermeasures which are basically designed for personal computers and servers have reduced their effectiveness. By considering explosive increase of the number of information devices, it becomes unfeasible that single monitoring point investigates all kinds of communication among all of them.

To solve these problems above, in the next generation network environment where various types of devices are connected, it is mandatory to develop techniques which can sense the existence of silent activity of a cyberattack, grasp the damage situation caused by the attack and continue our operation with suppressing the damage. Furthermore, new technology is required to extract suspicious devices by performing cross-certification among devices.

In this research, we proposed the following methods to satisfy the requirements.

- A malicious communication detection algorithm designed for the future network, e.g., HEMS(Home Energy Management System)
- A malware classification algorithm based on behavior analysis of malware communication
- An information device trace system for the future network where automatic IP address assignment mechanism will be adopted, e.g., SLAAC (StateLess Address AutoConfiguration)
- A network management support system to detect suspicious activities and suppress the damage of the attacks.
- A cross certification protocol among devices with the least disclosure of secret information

Most of these methods has been evaluated by using real dataset on our laboratory LAN or university network. In addition, we plan to evaluate the methods on huge size academic networks and improve them.