FOR IMMEDIATE RELEASE

"Decentralized Security Operation" that realizes prompt incident response by cooperation between multiple security-response teams

Enabling rapid detection of and countermeasures against cyber-attacks by industry-university collaboration

Tokyo, February 5, 2018 --- Keio University and Hitachi, Ltd. (TSE: 6501, Hitachi) today announced that establishment of a testing environment based on a new concept, "decentralized security operation" that provides swift incident response to increasingly sophisticated and large-scale cyber-attacks through collaboration between multiple security response teams such as SOC[1] and CSIRT.[2] The testing environment verified that by automating the process of "requesting investigation by a specialized team upon detection of an incident, and sharing of the analytical data" which previously required human intervention, it was possible to complete this process within one second. Keio University and Hitachi will now intend to pursue research for the practical application of this concept to contribute to the realization of security operations that will assure the stable operation of societal infrastructure systems.

The speed of cyber-attacks is increasing yearly, and the risk of multi-point attacks over a short period of time is also increasing. Further, with the progress of the cloud and BYOD,[3] the targets which need to be protected have also grown from the system of one's own organization to the cloud or personal terminals, so innovative security measures are required.

Keio University and Hitachi began research collaboration for IT security management and personal information protection against cyberattacks[4] in February 2016. The knowledge accumulated by Keio University over 25 years of contributing to the advancement of the Internet, and Hitachi's knowledge in building societal infrastructure and preventing or responding to security incidents, were brought together to conceive the new concept, "decentralized security operation", and develop one of its core technologies, "dynamic authentication-authorization technology." Key features of "decentralized security operation" and "dynamic authentication-authorization technology" are as described below:

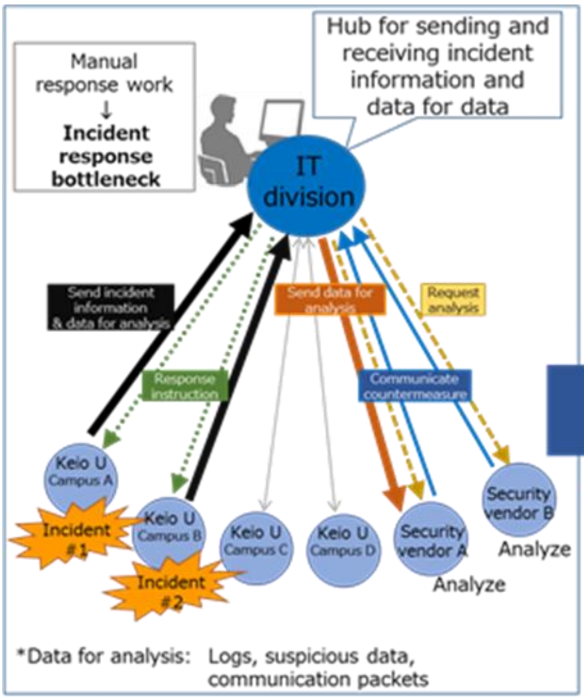
1. Decentralized security operation

In conventional incident response, incident information and analytical data (logs, suspicious data, and communication packets) are aggregated by a specific security-response team acting as a hub, and requests for analysis and analysis data are sent to multiple security response teams by human operators (Figure (a)). Under the new concept of “decentralized security operation,” instead of having a specific security response team handling all incident responses, security response teams within each organization (e.g. a cloud provider) autonomously responds to incidents in a decentralized manner, calling on collaboration when and where necessary.

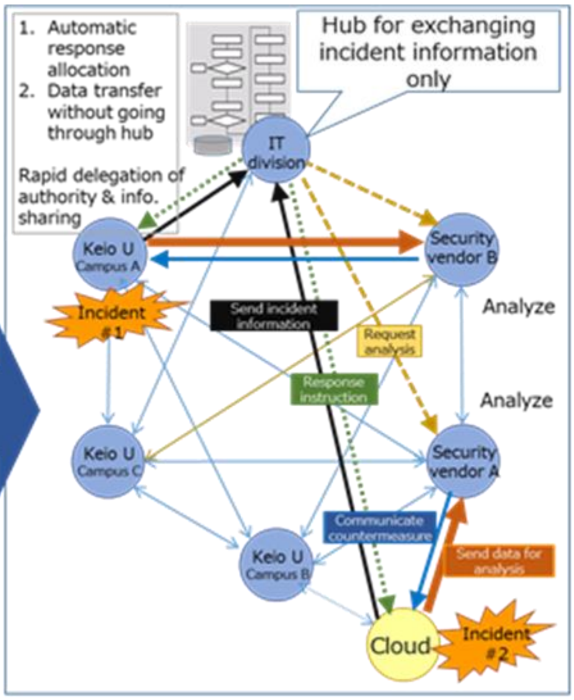
2. Dynamic authentication-authorization technology

“Dynamic authentication authorization technology” a core technology for decentralized security operation, standardizes the functions required for incident response such as information gathering and analysis, and enables the mutual confirmation of functions held by each security response team in real time. As a result, it is possible to automatically share analytics or entrust functions (authorize actions) such as processing to specialist teams. Further, with each new discovery of organization involved, it is possible to realize security measures quickly by automating the full process from authorization to approval (authentication) by organization involved in sending and receiving data (Figure (b)).

To verify the effectiveness of this technology, the incident analysis data monitored by the Keio University Information Technology Center was sent to the SOC for research at Hitachi’s Open Lab Yokohama.,[5] to establish an environment for entrusted data analysis. Results from the evaluation which commenced in November 2017, confirmed that the series of processes from incident detection to requesting analysis which depending on the skill level of the operator could take from a few minutes to a few hours, could be completed within one second.



Figure(a) Conventional security operation



Figure(b)Decentralized security operation with
Dynamic authentication-authorization
technology

Keio University and Hitachi will continue to develop technologies to realize decentralized security operation using the testbed developed, and will propose these technologies to the Nippon CSIRT Association[(6)] as a countermeasure for increasingly threatening cyber-attacks, and thus contribute to the realization of security operation for stable operation of societal infrastructure systems.

These accomplishments will be presented at the Internet and Operational Technology Study Group meeting of the Information Processing Society of Japan, to be held on 6 March 2018.

(1) SOC: Security Operation Center. An organization that monitors and analyzes cyber-attacks and various security incidents
(2) CSIRT: Computer Security Incident Response Team
(3) BYOD: Bring Your Own Device. Individuals such as employees of organizations bring their own information terminals to work for work purposes.
(4) 29 February 2016 News Release: Keio University and Hitachi to commence joint research in the area of cyber security for a "Super Smart Society"
http://www.hitachi.com/New/cnews/month/2016/02/160229.html
(5) 30 November 2016 News Release: Hitachi's cutting-edge technologies to be available for prototyping with customers in a new open-laboratory
http://www.hitachi.com/New/cnews/month/2016/11/161130.html
(6) Nippon CSIRT Association website
http://www.nca.gr.jp/en/index.html

About Keio University

Keio University is a private, comprehensive university with six major campuses in the Greater Tokyo area along with a number of affiliated academic institutions. Keio was founded in 1858, and it is Japan’s first modern institution of higher learning. Founder Yukichi Fukuzawa, a highly respected educator and one of the most important intellectuals of modern Japan, aspired for Keio to be a pioneer of new discoveries and contribute to society through learning. Guided by Fukuzawa’s founding principle of learning that is based on *jitsugaku*, or “science”, Keio will continue to cultivate knowledge and wisdom to face the challenges of tomorrow.
https://www.keio.ac.jp/en/

About Hitachi, Ltd.

Hitachi, Ltd. (TSE: 6501), headquartered in Tokyo, Japan, delivers innovations that answer society’s challenges. The company’s consolidated revenues for fiscal 2016 (ended March 31, 2017) totaled 9,162.2 billion yen ($81.8 billion). The Hitachi Group is a global leader in the Social Innovation Business, and it has approximately 304,000 employees worldwide. Through collaborative creation, Hitachi is providing solutions to customers in a broad range of sectors, including Power / Energy, Industry / Distribution / Water, Urban Development, and Finance / Government & Public / Healthcare. For more information on Hitachi, please visit the company's website at http://www.hitachi.com.