FOR IMMEDIATE RELEASE

Hitachi Begins Trial for Sharing Cyber Threat Data with HP

Tokyo, October 6, 2015 --- Hitachi, Ltd. (TSE: 6501) today announced that it has begun trials for sharing cyber threat data, such as emerging threats and attack methods to IT systems, with Hewlett-Packard Company. In this way, Hitachi will be able to assess up-to-date cyber threat situations and analyze cyber-attacks with higher accuracy, accelerating its effort to actualize advanced responses to cyber attacks by sharing cyber threat data with CSIRTs (Computer Security Incident Response Teams) of other companies and organizations, and by enhancing security-related services.

In recent years, not only corporate IT systems but also critical social infrastructure are facing a growing risk of cyber attacks, with their techniques becoming more complex and tenacious. Consequently, it is becoming necessary to identify the cause of cyber attacks and threat actors' identities through collecting and analyzing more information to find clues. However, only victims get a "full picture" of specific attack methods and its damage, and the amount of information one company can gather is limited in both terms of quality and quantity. Behind this development it is becoming a social issue to establish an efficient information-sharing scheme between security-related companies and organizations.

Hitachi has either prevented or defended against cyber attacks through HIRT (Hitachi Incident Response Team)[*1], its internal security expert group, and has continued efforts to share cyber threat data between companies and other organizations, establishing the "HIRT Lab" in the Research & Development Group in October 2013.

At the same time, HP is advancing a progressive approach in the security field by utilizing its security information sharing platform, "HP Threat Central," and sharing cyber threat data with other companies and organizations globally.

Amid these developments, Hitachi has formed a Global Threat Intelligence Alliance with HP. Hitachi and HP will share various types of data such as emerging threats, attack methods and possible targets[*2]. Hitachi will also consider the use of shared data in the field, as well as technical and practical issues. The information will be shared based on the STIX (Structured Threat Information eXpression)[*3] and the TAXII (Trusted Automated eXchange of Indicator Information)[*4], which are standard

technological specifications designed to enable information sharing for cyber threats.

“Targeted attacks are becoming more pervasive and the evolving nature of threats continues to be a top security challenge facing organizations around the world,” said Ted Ross, Director, Threat Intelligence, Security Research, HP. “Information sharing is fundamental to staying a step ahead of adversaries, advancing security intelligence and quickly isolating threats to predict threats and protect our most valuable data.”

“Hitachi will share cyber threat data with CSIRTs of other companies and security-related organizations,” said Shuji Senoo, Senior Director, Advanced Security Technology Operations, Cloud Services Division at Hitachi. “In this way, the Company will contribute to more sophisticated society-wide cyber security capabilities by enhancing methods to detect and prevent cyber attacks while minimizing its impacts on organizational activities.”

Moving forward, Hitachi will actively collaborate with CSIRTs in Japan and other countries, utilizing knowledge and data-sharing schemes learned from the trial with HP. The Company will also accelerate its efforts to improve its security-related services, such as system operations & monitoring services as well as cyber attack investigation & response services by the SHIELD SOC[*5]. By this means, Hitachi will fulfill its social responsibility to protect critical social infrastructure.

*1 HIRT (Hitachi Incident Response Team), Hitachi Group’s CSIRT, is an organization responsible for the efficient provision of security vulnerability information and incident response information to all divisions in the Hitachi Group, and supports the promotion of measures to defend the Group from external and internal vulnerabilities and incidents.

*2 Shared information will be anonymized to prevent to identify attribute information such as name of victims.

*3 STIX (Structured Threat Information eXpression): A XML specification to represent cyber attacks. MITRE Corporation, a non-profit organization which implements technical supports, research & development for the U.S. government, led development of its specifications to describe indicators of cyber attacks and to share information about the attacks.

*4 TAXII (Trusted Automated eXchange of Indicator Information): A specification which defines transfer protocols to exchange data about indicators which describes cyber attacks. The U.S. Department of Homeland Security (DHS) led development of the specifications centering at MITRE Corporation.

*5 SHIELD SOC: The security operations center of Hitachi Systems, Ltd., a wholly owned subsidiary of Hitachi, Ltd.

Hitachi Incident Response Team website
http://www.hitachi.com/hirt/

About Hitachi, Ltd.
Hitachi, Ltd. (TSE: 6501), headquartered in Tokyo, Japan, delivers innovations that answer society’s challenges with our talented team and proven experience in global markets. The company’s consolidated revenues for fiscal 2014 (ended March 31,

2015) totaled 9,761 billion yen ($81.3 billion). Hitachi is focusing more than ever on the Social Innovation Business, which includes power & infrastructure systems, information & telecommunication systems, construction machinery, high functional materials & components, automotive systems, healthcare and others. For more information on Hitachi, please visit the company's website at http://www.hitachi.com.

# # #

Information contained in this news release is current as of the date of the press announcement, but may be subject to change without prior notice.
