Appendix

Key features of the Cyber Security Factory

1. Security Operations Center function (SOC)

   Professional security personnel will provide round-the-clock security surveillance of customers' networks and websites and promptly report unauthorized access and possible malware (malicious software) infections.

   The "cyber incident on-site intervention service" for providing initial response to emergencies and a variety of forensic services for investigating malware sources and information leakage will be offered through the SOC.

2. Human Resource Development

   The Cyber Security Factory will provide cyber training services for appropriately handling cyber attacks. It will contribute to raising the technical level of security personnel in customers' computer security incident response team (CSIRT)*, as well as help train security engineers, which are chronically lacking in number.

   Furthermore, the Cyber Security Factory will be staffed with personnel from Cyber Defense Institute (CDI), Infosec Corporation (Infosec), whose shared knowledge and work experience will enable the grooming of qualified security professionals.

3. Cyber intelligence function

   The Cyber Security Factory will collect evidence on cyber attacks as well as investigate the latest attack methods and malware trends. Knowledge gained from the investigations will be used in development of new products and in information-provision services, such as infiltration tests of customer's systems, which are aimed at assessing vulnerability through simulated attack trials carried out from the attacker's point of view. This will enable flexible responses to various attack threats, which are increasing everyday and expanding their targets.

***

Note:

*Computer Security Incident Response Team (CSIRT)

A team of computer security specialists established within a company