Activities for Information Security Against Electromagnetic Radiation from Telecommunication Facilities

Kimihiro Tajima†, *Yoshiharu Akiyama, Tetsuya Tominaga, and Tadahito Aoki*

Abstract

NTT Group takes countermeasures against electromagnetic compatibility (EMC) problems in order to ensure that networks and services are highly reliable and secure. This article introduces recent activities for information security against electromagnetic emissions and for the immunity of telecommunication facilities based on the application of EMC technology.

1. Introduction

NTT Group takes countermeasures against electromagnetic compatibility (EMC) problems in order to ensure that the network infrastructure and communication services that run on it are highly reliable and secure. It regulates the EMC conditions of telecommunication equipment and terminal equipment by means of "NTT Internal Standards for EMC" and "NTT-TRs for EMC" for procurement (TR: technical requirements) and regulates test methods and limits for testing emissions, immunity, and overvoltage [1]. In EMC research, it has been reported that in some cases information technology equipment (ITE) such as personal computers leaks information via unintended electromagnetic waves radiated mainly from displays [2]. NTT R&D is investigating countermeasures against information leakage problems like this based on the use of EMC technologies.

NTT Group released "Promoting NTT Group's Medium-Term Management Strategy" in November 2005. It shows a "Roadmap for building the next-generation network (NGN)" and "Development plan of ubiquitous broadband services" [3]. We are aiming to enable 20 million subscribers to use innovative ubiquitous broadband services very safely and securely by promoting rapid progress of the optical access network and IP-based services by 2010 (IP: Internet protocol).

The NGN is expected to provide connectivity anytime and anywhere (fixed mobile convergence) and various application services combining telephony, Internet access, and video distribution (triple play) and to stimulate the development of new broadband businesses (ubiquitous broadband services) such as video conferencing, telemedicine, and electronic numbering of products and documents using radio frequency identification (RFID). NGN service has been running successfully since its start in March 2008 [4].

Although information and communications technology (ICT) has improved the quality and convenience of people's lives, maintaining the information security of broadband networks that are opened for the Internet is becoming a big problem these days. Social problems on the Internet, such as spoofing, illegal access (intrusion), falsification, information exploitation, and tapping, are becoming serious. Anyone could suffer from these threats if no countermeasures against them were taken. Telecommunication

† NTT Energy and Environment Systems Laboratories
Musashino-shi, 180-8585 Japan

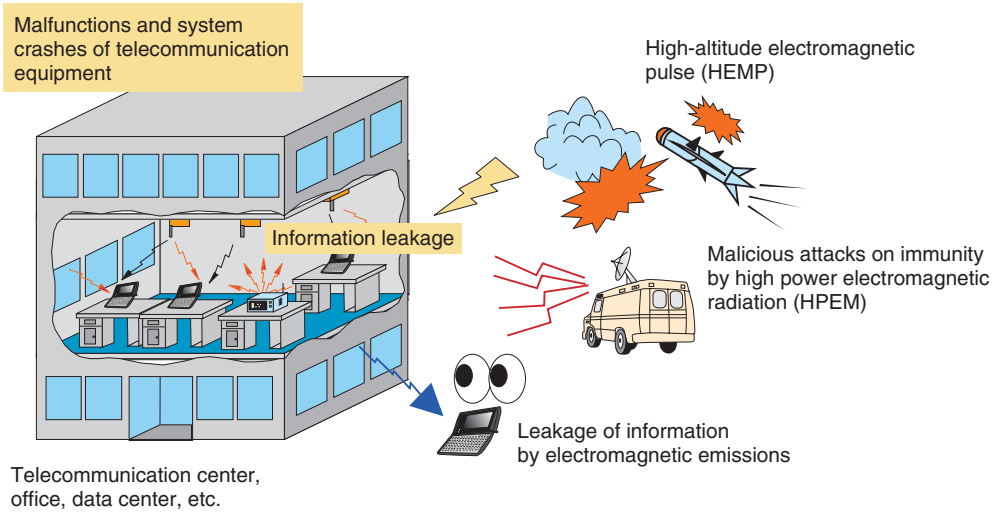

Fig. 1. Threats to information security against electromagnetic emissions and to immunity.

carriers can take countermeasures against these risks on their networks [5]. Against this backdrop of social problems, on April 2006, the Information Security Conference for Telecommunications (ISeCT) was established and Information Security Management Guidelines for Telecommunications (ISM-TG) were enacted [6]. However, because network terminals like personal computers (PCs) in particular are owned by users and they are used under various circumstances, we think that it will be difficult to keep security against intentional exploitation of information. Information security against electromagnetic radiation from electronic apparatus and protection against malfunctions caused by malicious exposure by high-power electromagnetic radiation (HPEM) are called *information security against electromagnetic emissions and immunity*. "Security Guidelines relating to Electromagnetic Emission and Immunity Outline" were established by the Information Security Technology study group in 2003. These guidelines regulate countermeasures and testing methods for electronic apparatus [2].

As a telecommunication carrier, NTT is focusing on ITE such as telecommunication equipment installed in telecommunications buildings and the access network and terminal equipment like notebook PCs which are highly mobile and bought on the open market. We are also studying information security against electromagnetic radiation from telecommunication equipment and protection against its malfunction due to HPEM. This article introduces these information security activities aimed at providing telecommunication services safely and securely.

2. Information security against electromagnetic emissions and immunity

Here, we assume that there are two main threats to information security from electromagnetic emissions and to immunity (**Fig. 1**).

(1) Leakage of information by electromagnetic emissions

Information is obtained from weak electromagnetic radiation from telecommunication equipment (including terminals).

(2) Malicious attacks on immunity by high-power electromagnetic waves

Malfunctions or system crashes are caused by malicious exposure to HPEM.

The dangers of information leakage by electromagnetic emissions include (1) unintentional emanations conveying image information emitted from the displays of information technology equipment, such as PCs, and from laser printers, IC cards, and card readers and (2) exploitation of information in databases handled by servers at public key infrastructure (PKI) centers and financial data centers. It has been reported that even if the level of such electromagnetic radiation is below the limits regulated by the Voluntary Control Council for Interference by Information Technology Equipment (VCCI), information can be obtained from the weak signals at some distance [7], [8].

As threats of malicious HPEM attacks on immunity, we consider the intentional irradiation of telecommunication equipment by HPEM from high-power transmitters, such as intentionally altered radio trans-

mitters and radars (radio detection and ranging), microwave ovens, high-voltage apparatus for self-defense (e.g., tasers), and surge generators for testing.

As a first step toward countermeasures against these electromagnetic information security problems, NTT has developed the iDC shielded vault (iDC: Internet data center) as a high-security electromagnetic-radiation-shielded room [9]. The appearance of the iDC shielded vault is shown in **Fig. 2**. The vault is based on 19-inch cabinet racks, which are common in data centers and server rooms. It can withstand an earthquake intensity of 6 on the Japanese seven-point seismic scale without collapsing. A simple metal panel joining method produces an electromagnetic radiation shielded room that has a shielding factor of 50 dB or more, while being light and inexpensive. Including the construction cost, it can be made for a cost ranging from 1/2 to 1/5 of the cost of existing methods. The number of racks can be changed to accommodate changes in the number of machines, which ensures easy expandability—something that has previously been difficult for shielded rooms. The double-door construction guarantees that rack doors can be opened and closed while maintaining higher shielding performance than previous room facilities. That construction also prevents electromagnetic leakage and electromagnetic attacks during maintenance work. A security cabin (private room) can also be created by adding locks.

As a second step, we have developed an active device to protect information displayed on a PC against eavesdropping (**Fig. 3**) [10]. We need to develop countermeasures appropriate for the user's circumstances because it is difficult to prevent the leakage of electromagnetic radiation in the case of ITE with man-machine interfaces like notebook PCs. Our device is directly connected to the video display connector of a PC and it picks up the video signals to regenerate the dot clock signal. This dot clock signal is modulated to actively generate masking signals that are fed to the PC and to the video display terminal. These masking signals prevent others from eavesdropping on leaking signals. This device is much more effective for a wide frequency band and for mobile applications than the shielding technique because we can install the countermeasures at the source of leakage signals without having to tune it to the characteristics of the target PC.

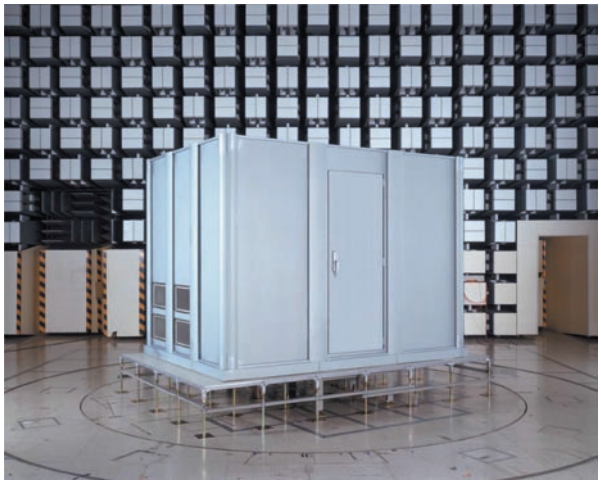

Fig. 2. Appearance of iDC shielded vault.

3. Standardization activities for information security against electromagnetic emission and immunity

X.1051 produced by ITU-T SG17 (ITU-T: International Telecommunication Union, Telecommunication Standardization Sector; SG: Study Group) received consent as ITU-T standardization in 2004. This is a global recommendation in the telecommunication and information industries about how to manage information security in facilities and infrastructure such as telecommunication and data centers [11]. It is based on ISO/IEC17799, which was established as a practical standard for information security management in the electrical and electronics fields in 2000. In Japan, "Information Security Management System Guidelines for Telecommunications (ISMS-TG)" were published by a study group organized by the Ministry of Internal Affairs and Communications in 2006. ITU-T SG5 is promoting the standardization of practical testing and countermeasures as the SG5 K.sec series in information security against electromagnetic emissions and immunity.

In the general meeting of ITU-T SG5 in Geneva in February 2008, the draft recommendation "Application of requirements against high-altitude electromagnetic pulse (HEMP) to telecommunication systems" underwent technical discussion and it is scheduled to receive consent this year. The topic continues to be discussed as a draft of K.hpem: "Application of requirements against HPEM to telecommunication systems"[12], the draft of K.sec: "Guide for the application of electromagnetic security requirements" and

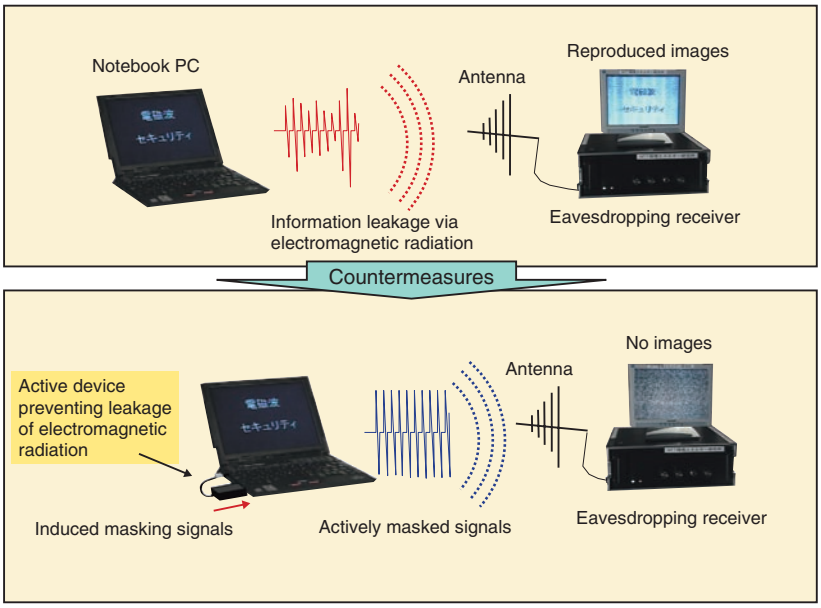

Fig. 3. Active device preventing leakage of electromagnetic radiation.

the draft of K.leakage: "Test method and requirements against information leak through unintentional EM emission", aiming to receive consent by 2010. In addition, K.secmiti: "Test method and requirements against information leak through unintentional EM emission" will be discussed in SG5 from now. The Telecommunication Technology Committee (TTC) of Japan aims to standardize that recommendation in Japan.

NTT Group is also trying to make guidelines for information security against electromagnetic emissions and immunity that comply with the ITU-T standard.

4. Conclusion

This article introduced activities for information security against electromagnetic radiation from telecommunication facilities. It would appear that information security against electromagnetic radiation is becoming more and more important as one aspect of information security management in the general sense. NTT Group is trying to improve the performance of countermeasure and evaluation technologies and to promote standardization in order to offer telecommunication services safely and securely.

References

[1] T. Aoki, K. Tajima, T. Tominaga, and R. Kobayashi, "Electromagnetic Compatibility Standards and Their Application in NTT Group," NTT Technical Review, Vol. 5, No. 12, 2007, https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200712sf1.html
[2] http://www.j-netcom.co.jp/ist/index.html (in Japanese).
[3] http://www.ntt.co.jp/about/keieisenryaku.html (in Japanese).
[4] S. Miura, "NTT's Activities to Promote the Advance of the Ubiquitous Broadband Society," Vol. 6, No. 4, Apr. 2008.
[5] A. Goto, "Developing High-security Technology for High-reliability Networks," NTT Technical Review, Vol. 6, No. 6, 2008, https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200806lab.html
[6] http://www.fmmc.or.jp/news/H63index.html (in Japanese).
[7] Y. Yamanaka, H. Ohno, and M. Hattori, "Reconstruction of information by receiving unwanted emission from information technology equipment," IEICE Technical Report, EMCJ2004-140, pp. 55–60, 2005.
[8] H. Sekiguchi and S. Seto, "Proposal of an information signal measurement method in display image contained in electromagnetic noise emanated [*sic*] from a personal computer," 2008 IEEE International Instrumentation and Measurement Technology Conference, May 2008.
[9] http://www.ntt.co.jp/news/news04/0409/040927.html
[10] Y. Suzuki, R. Kobayashi, M. Masugi, K. Tajima, and H. Yamane, "Development of Countermeasure Device to Prevent Leakage of Information Caused by Unintentional PC Display Emanations," EUROEM 2008 European Electromagnetics, Lausanne, July 2008.
[11] ITU-T SG17, "Recommendation X.1051 (07/04): Information security management system—Requirements for telecommunications (ISMS-T)," Approved in July 2004.
[12] ITU-T SG5, "Draft text of K.hemp: Application of requirements against HEMP to telecommunication systems," TD698 rev. 2, Geneva, Swiss, Feb. 2008.

Kimihiro Tajima
Senior Manager, Research and Development Planning Department, NTT.

He received the B.E. and M.E. degrees from the Department of Electronics at Kumamoto University, Kumamoto, in 1986 and 1989, respectively. He joined NTT Telecommunications Networks Laboratories in 1989. He has been engaged in studies on optical-scheme-based measuring methods in the EMC field, development of mobile communication systems using infrared rays for EMC, etc. He is a secretary of the Japanese National Committee of CISPR Group A and of the Technical Committee on Electromagnetic Compatibility of the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan. He is a member of IEEE. He moved from the EMC Technology Group, Energy Systems Project, NTT Energy and Environment Systems Laboratories, to his current department in July 2008.

Yoshiharu Akiyama
Senior Research Engineer, Research Planning Section, NTT Energy and Environment Systems Laboratories.

He received the B.E. degree in communication engineering from the University of Electro-Communications, Tokyo, in 1990. Since joining NTT in 1990, he has been researching EMC of broadband communications such as wireless local area networks, digital subscriber lines, and power line telecommunication.

Tetsuya Tominaga
Senior Manager, Research Planning Section, NTT Information Sharing Laboratory Group.

He received the B.E. and M.E. degrees in mechanical engineering from Doshisha University, Kyoto, in 1989 and 1991, respectively. Since joining NTT Telecommunication Networks Laboratories in 1991, he has been researching and developing electromagnetic environment systems and telecommunication equipment protection against lightning surges. He is the Rapporteur of ITU-T SG5 Question 15. He is a member of IEICE, the Robotic Society of Japan, the Institute of Electrical Engineers of Japan (IEEJ), and IEEE. He moved from the EMC Engineering Group, Technical Assistance and Support Center, Maintenance and Service Operations Department, Network Business Headquarters, NTT East, to his current department in August 2008.

Tadahito Aoki
Project Manager of the Energy Systems Project and Senior Manager, Research Planning Section, NTT Energy and Environment Systems Laboratories.

He received the B.E. and M.E. degrees in electrical engineering from Shinshu University, Nagano, and the Dr.Eng. degree in electrical and electronics engineering from Kyushu University, Fukuoka, in 1983, 1985, and 2000, respectively. He joined NTT Electrical Communications Laboratories in 1985. His research interests are in environmental protection and power electronics technologies. He is a member of IEICE, IEEJ, and IEEE.