Standardization Related to Electromagnetic Security

Tetsuya Tominaga†, Ryuichi Kobayashi, Hidenori Sekiguchi, and Shinji Seto

Abstract

This article describes standardization related to security issues arising from electromagnetic radiation (EMR), explains how EMR security is positioned within information security, and identifies trends in EMR security standardization in Japan and abroad.

1. Need for electromagnetic security

Information security is becoming increasingly important as we progress towards the information society. Rather than being just for financial systems, information security must now be considered in the construction of all data centers and communication facilities that operate authentication systems and conform to information management specifications. Physical security and electromagnetic security are often mentioned in information security specifications, as shown in **Fig. 1**. So far, however, no technical guidelines have been included. Furthermore, electromagnetic compatibility (EMC) specifications for data communication equipment in ordinary environments are being finalized in international and national specifications, and existing specifications are being applied. Those specifications, however, give permissible values for electromagnetic radiation (EMR) and EMR tolerance in ordinary usage environments; they do not cover the use of EMR in attacks or eavesdropping by malicious third parties.

Given this situation, we are getting involved in standardization activities in order to be able to provide safe and secure services to our clients by clarifying technical requirements, assessing risk, and taking necessary measures regarding EMR and EMR tolerance and information security. These activities are part of the research and development conducted in the Strategic Information and Communications R&D Promotion Programme (SCOPE) of the Ministry of Internal Affairs and Communications (MIC) in 2007.

In this article, we describe the topics of information security specifications that relate to security issues arising from EMR, explain how EMR security is positioned within information security, and identify the trends in EMR security standardization in Japan and abroad.

2. Information security specifications and EMC

General information security specifications include the well-known ISO/IEC 27001 [1] and ISO/IEC 27002 (17799) [2] published by the International Electrotechnical Commission (IEC) as the information security management system (ISMS) and ISO/IEC 15408 [3] information technology security evaluation criteria (ITSEC) and common criteria specifications.

The ISMS specifications are derived from BSI (British Standards Institution) BS7799 specifications and are equivalent to ITU-T (International Telecommunication Union, Telecommunication Standardization Sector) Recommendation X.1051 [4] in the field of telecommunication. These are information security management system specifications, and they are also being applied as an ISMS-compatibility evaluation

† NTT Information Sharing Laboratory Group
Musashino-shi, 180-8585 Japan

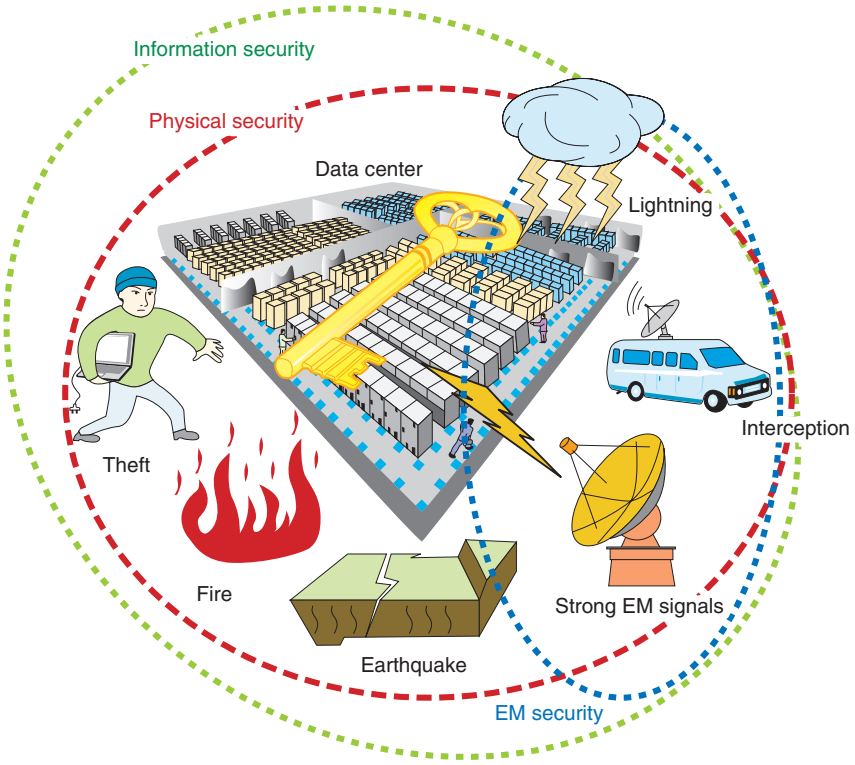


Fig. 1. Information security and electromagnetic (EM) security.

system [5] in Japan. This management approach uses the plan-do-check-act cycle and refers to information system security management guidelines for enterprises and organizations. A feature of this standard is emphasis on operation and management regarding security in a sense broader than computers and networks: it provides a management method for assessing and coping with risk. In those specifications, EMR-related security is treated as part of physical security (theft, fire, water damage, etc.). References to EMR security include "An environment that minimizes damage from strong EMR must be constructed. If necessary, EMR shielding or other such measures shall be implemented." in X.1051 and "The environment shall be managed to minimize the risk of information leaks by radio-frequency emissions." in ISO/IEC 27002 (17799).

The approach in Japan is that "The party responsible for information system security shall institute measures for information leaks by EMR with respect to information systems that handle confidential information." as reflected in the Unified Standards for Information Security in Government Organizations (December 2005 version (first full published version)), for example. The handbook for that document mentions "This is an item for taking measures against the risk of information leaks by EMR emitted by display cables, etc. Specifically, the use of filters to reduce EMR is raised." For telecommunication, MIC's "Registration and Specification of Measures Against Data Communication Network Security and Reliability" (November 14, 2000) specifies that communication carriers are responsible for "taking measures to reduce EMR or to mask leaked EMR so that important data does not leak from the computers that control network functions."

In this kind of information security management, there is much mention of EMR security, and attention to information leaks in particular is advised.

Common criteria, on the other hand, are information security evaluation criteria. They are an international standard for security products (hardware or software) and for the development and construction of systems and their operation. They define the security function requirements for communication devices and other such security devices and they guarantee requirements for their implementation. Without these definitions, a device cannot be called *secure* for any given level of security. ISO/IEC 15408 provides the basis for such indexes of security.

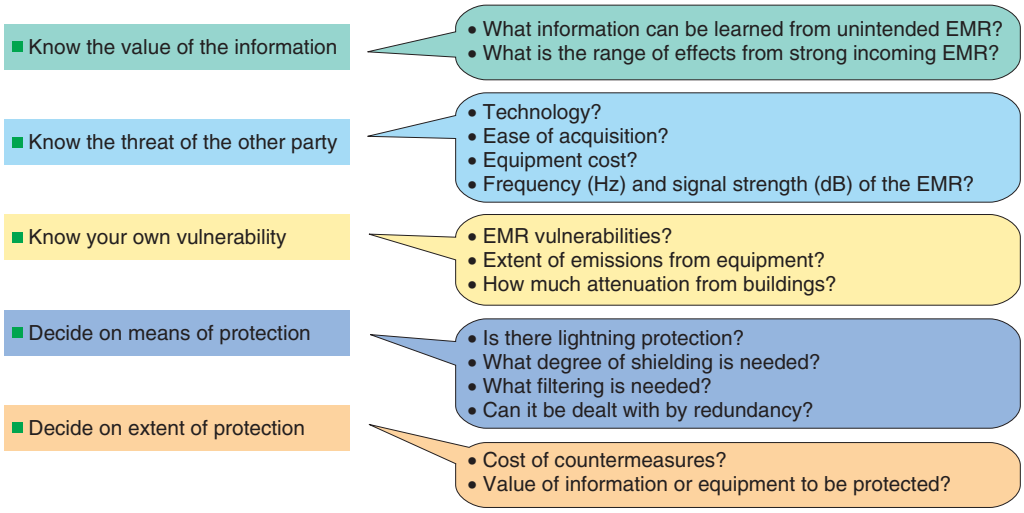


Fig. 2. Electromagnetic security risk assessment.

Currently, the concept of ISO/IEC 15408 is also being applied in the procurement of products for the electronic government project in Japan. Procurement is restricted to vendors that create a security target that satisfies ISO/IEC 15408.

In FIPS-140-2 [6], which are security specifications for encryption equipment published by the National Institute of Standards and Technology (NIST) of the USA, FCC Part 15 describes the need for general EMC specifications for measures against unintentional radiation. The FIPS-140-2 FAQ (frequently asked questions and answers) published by NIST will be supplemented after information about robustness against intentional radiation has been obtained from EMC experts, and ultimately, side-channel attacks and other encryption-breaking techniques that use EMR will also become topics [7].

Thus, information security management systems are required to implement EMR security risk evaluation and countermeasures. There is a need, however, for standardization of technical requirements for actual implementation of risk evaluation and countermeasures, as shown in **Fig. 2**, rather than reference to EMR security specifications that are to be described later.

3. Trends in EMR security standardization

3.1 Terminology of EMR security

EMC technicians researching and developing countermeasures against EMR-induced malfunctions of electronic devices and damage to devices caused by electrical surges, etc. are intimately familiar with the vulnerability of electronic devices to EMR and this research has a long history. There are three broad classes of EMR for security purposes: emissions from nuclear explosions, intentional strong EMR, and information leaks via EMR. Matters related to international EMR are being standardized in the IEC SC77C specifications and ITU-T SG5 Recommendations, in which we are also participating. The standards and Recommendations use various abbreviations and terms of their own, so there is some confusion in the terminology. Below, we explain some key terms.

The effect of strong EMR from a high-altitude nuclear explosion on devices and systems is called nuclear electromagnetic pulse (NEMP) or high-altitude electromagnetic pulse (HEMP).

The effects of strong EMR and intentional radiation are referred to as high-power EMR (HPEM), high-power electromagnetic (HPM), or intentional electromagnetic interference (IEMI). Information leaks via undesired EMR from electronic devices, which can reveal information displayed on a personal computer screen, keystroke information, or data sent to a printer, are most often referred to as TEMPEST. In the glossary of RFC (Request for Comments) 2828 published by IETF (Internet Engineering Task Force), TEMPEST is defined as “a nickname for specifications and standards for limiting the strength of electromagnetic emanations from electrical and electronic equipment and thus reducing vulnerability to eavesdropping. This term originated in the U.S. Department of Defense.” Another recommended term is *emanation*, which is defined as “a signal (electro-

Table 1. IEC SC77C existing specifications related to HEMP.

Document number	Title
61000-1-3	The Effects of High-Altitude EMP (HEMP) on Civil Equipment and Systems – First Edition
61000-2-9	Section 9: Description of HEMP Environment – Radiated Disturbance Basic EMC Publication First Edition
61000-2-10	Description of HEMP Environment – Conducted Disturbance – First Edition
61000-2-11	Classification of HEMP Environments – First Edition
61000-4-23	Test Methods for Protective Devices for HEMP and Other Radiated Disturbances – First Edition
61000-4-24	Test Methods for Protective Devices for HEMP Conducted Disturbance Basic EMC Publication – First Edition
61000-4-25	HEMP Immunity Test Methods for Equipment and Systems – First Edition
61000-4-32	High-altitude electromagnetic pulse (HEMP) simulator compendium – First Edition
61000-5-3	HEMP Protection Concepts – First Edition
61000-5-4	Immunity to HEMP – Specifications for Protective Devices Against HEMP Radiated Disturbance – Basic EMC Publication – First Edition
61000-5-5	Specification of Protective Devices for HEMP Conducted Disturbance – Basic EMC Publication First Edition
61000-5-7	Degrees of protection provided by enclosures against electromagnetic disturbances (EM code)
61000-6-6	HEMP immunity for indoor equipment – First Edition

Table 2. IEC SC77C existing specifications related to HPEM.

Document number	Title
61000-1-5	High power electromagnetic (HPEM) effects on civil systems
61000-2-13	High-power electromagnetic (HPEM) environments – radiated and conducted
61000-4-33	Measurement methods for high power transient parameters

magnetic, acoustic, or other medium) that is emitted by a system (through radiation or conductance) as a consequence (i.e., byproduct) of its operation, and that may contain information (see TEMPEST)". It is also referred to as electromagnetic emanation security (EMSEC) and emanation security (EMSEC).

3.2 Trends in international standards

IEC discussion of HEMP ended with SC77C, the publication of which was completed in 2003. Since 2004, documents related to HPEM have appeared in succession. ITU-T SG5 has been discussing matters relating to EMR security since the 2005–2008 session, and many draft Recommendations have been submitted. Below, we describe the trends and main content of these international specifications [8].

3.2.1 IEC standards

IEC SC77C has gone furthest in standardization related to EMR security. Existing specifications related to HEMP and HPEM are described in **Tables 1** and **2**, respectively. As we see from Table 1, most of the documents related to HEMP have been made into standards. The specifications for consumer systems are complete and standardization for HPEM is currently moving forward. The divisions of the IEC 61000 series are Part 1: Requirements, Part 2: Environment, Part 4: Testing and Measurement, Part 5: Installation Guidelines, and Part 6: Other. The HEMP specifications are also divided in the same way.

At least the following three documents are need for testing device tolerance to HEMP. IEC 61000-4-25 specifies HEMP immunity testing methods, IEC6100-2-11, as shown in **Table 3**, indicates building and enclosure protection levels, and IEC 61000-6-6 specifies the testing that accords with those levels. Examples of immunity levels at enclosure ports are given in **Table 4**. The pulse testing described in 1.1 is peculiar to HEMP, and the testing level decreases according to the shielding characteristics of the protection level. The electrostatic testing described in 1.2, on the other hand, tests a phenomenon that is not caused by HEMP, so it is specified as a constant value for all protection levels. Documents 61000-2-9 and 61000-4-25 specify various testing waveforms, but 61000-6-6 describes only the pulse testing of 1.1 as a HEMP-specific test. We believe that is because EMC testing and compatibility are made clear in other IEC documents. This pulse test is a special test. Document 61000-4-32 introduces a test site for it and indicates that testing can be performed even without test devices.

Table 3. Protection concepts and definitions (IEC6100-2-11).

Concept class	Description of protection	Shielding (dB)	Filtering (dB)
1A	Buildings or structures whose above-ground parts are constructed of wood, bricks, or concrete blocks and have no rebar or have large doors or windows with no clear shielding	0	0
1B	Buildings or structures whose above-ground parts are constructed of wood, bricks, or concrete blocks and have no rebar or have large doors with no clear shielding, but have lightning protection (unfiltered overvoltage protection)	0	20
2A	Buildings or structures whose above-ground parts are constructed of reinforced concrete or buried brick	20	0
2B	Buildings or structures whose above-ground parts are constructed of reinforced concrete or buried brick and have lightning protection (unfiltered overvoltage protection)	20	20
3	Shielded enclosure with minimum RF shielding, typical device cabinet that has small gaps, and ordinary lightning protection and EMI filtering	20	40
4	Shielded enclosure with intermediate level of RF shielding and well-bonded at entry and exit points. Ordinary lightning protection and EMI filtering	40	40
5	Good RF shielding and protected at entry and exit points (overvoltage protection and filtering)	60	60
6	High-quality RF shielding and protected at entry and exit points (overvoltage protection and filtering)	80	80

RF: radio frequency

Table 4. Immunity levels at enclosure ports.

Test	Radiated disturbance and electrostatic discharge	Basic standard	Criterion	Protection concepts of buildings					
				1A	1B	2	3	4	5-6
1.1	Electromagnetic pulse: 2.5/25 ns	IEC 61000-4-25	B	50 kV/m	50 kV/m	5 kV/m	5 kV/m	Optional 500 V/m	Not required
1.2	Electrostatic discharge	IEC 61000-4-2	B	8 kV	8 kV	8 kV	8 kV	8 kV	8 kV

For the implementation of countermeasures, 61000-5-4 and 61000-5-5 describe shielding, filters, and overvoltage protection elements in fine detail. Those two documents can be used by EMC technicians as countermeasure textbooks.

Currently, the focus of SC77C has shifted to HPEM, and the documentation for the overview, environment, and measurement methodology has been completed. Documentation for testing methods and countermeasures, etc. is planned for future work. In the same way as for HEMP, specifications that deal with only the introduction of testing sites are being formulated.

3.2.2 ITU-T Recommendations

In Topic 15 of ITU-T SG5 (Study Group 5), discussion on Recommendations related to EMR security in telecommunications began in 2005. As shown in **Table 5**, five documents are planned for publication as Recommendations. As described in section 2, the work is proceeding from the viewpoint that intermediate technical documents on information security and EMR security are needed. To enable the necessary risk evaluation to be performed when implementing X.1051, which is a Recommendation on the management of information security, work is proceeding on K.sec as an overview of security phenomena involving EMR and an introduction to Recommendations that must be referred to for coping with that risk. Recommendations that allow various levels of testing and countermeasures according to the risk evaluation, including ordinary EMC and lightning, are planned. K.hemp is planned as a Recommendation that includes no new testing at all to avoid redundancy with the IEC specifications. The plan is to gather the many IEC documents that concern HEMP into a single volume and compose a Recommendation for only the protection criteria and device immunity levels for when countermeasures are implemented. K.hpem is planned as a Recommendation that

Table 5. ITU-T SG5 topic 15 Recommendation schedule.

Document	Recommendation title	Timing
K.sec	Guide for the application of electromagnetic security requirements – Basic Recommendation	2010
K.hemp	Application of requirements against HEMP to telecommunication systems	2008
K.hpem	Application of requirements against HPEM to telecommunication systems	2008
K.leakage	Test method and requirements against information leakage through unintentional EM emission	2009
K.secmiti	Mitigation methods against EM security threats	2011

introduces many kinds of equipment that emits strong EMR, gives examples of electric field strength at various distances, etc. to allow risk evaluation, and presents the corresponding levels of countermeasures. International specifications concerning information leaks are not yet complete. The first one is expected to be K.leakage. Many information security specification documents mention the leaking of information via EMR, but it is not possible to move forward with specific countermeasures because there are no technical guidelines. K.leakage, however, is planned to include measurement methods [9]–[11] and permissible values [12], [13]. Finally, K.secmiti is planned to be a Recommendation concerning methods for countering threats to EMR security.

3.2.3 Trends in Japan

There are no published domestic specifications in Japan. The IEC SC77C Japan National Committee and the EMR Security Committee of the IEE are at the investigative stage. On the other hand, the Information Security Technology Study Group (IST), an independent organization in Japan, distributed EMR Security Guidelines to its members in September 2003 and the document is currently published on its Web site [13]. The document is organized as Introduction (chapters 1 and 2), Application Scope (chapter 3), Cited Specifications (chapter 4), Definitions (chapter 5), General Criteria (chapter 6), Criteria for EMR Leak Countermeasures (chapter 7), Criteria for Intrusive EMR (chapter 8), and Criteria for Construction Work and Design (chapter 9). Commentary 1 describes a typical model for an electronic government system. It is currently the only document concerning EMR information leaks that includes testing methods.

4. Conclusion

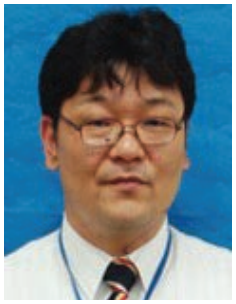
We have shown that information security specifications often urge the implementation of EMR security measures, speak of the need to treat failures caused by EMR as part of security, and speak of the importance of clarifying the technical criteria for evaluating such security risks. We have also explained the status of standardization activities in IEC and ITU-T.

Acknowledgment

This research and development was done as part of the R&D for SCOPE run by MIC.

References

[1] ISO/IEC 27001: 2005, “Information Security Management Systems—Requirements”.
[2] ISO/IEC 27002: 2005, “Information Technology—Security Techniques—Code of practice for information security management”.
[3] ISO/IEC 15408-1: 2005, “Information Technology—Security techniques—Evaluation criteria for IT security—Part 1: Introduction and general model”.
[4] ITU-T, X.1051, “Information Security Management System—Requirements for Telecommunications (ISMS-T)”.
[5] JIP-ISAC210-2.0, “ISMS Guide (ver. 2.0),” Japan Information Processing Development Corporation (JIPEDC), April 2003, http: //www.isms.jipdec.jp/doc/JIP-ISMS100-20.pdf (in Japanese).
[6] FIPS PUB 140-2, “Security Requirements for Cryptographic Modules,” National Institute of Standards and Technology (NIST), 2001, http: //csrc.nist.gov/cryptval/140-2.htm
[7] S. Oyama, “From the Latest Research in EMR and Information Security,” 2008 IEEJ Symposium, S2-6 (in Japanese).
[8] T. Tominaga, “Domestic and Foreign Specifications Relevant to EMR and Information Security,” 2008 IEEJ Symposium, S2-3 (in Japanese).
[9] T. Tozaka, Y. Yamanaka, and K. Fukunaga, “Evaluation of Reproducibility of Data Based on Radio Emission from Printers,” 2008 IEEJ Symposium, S2-7 (in Japanese).
[10] H. Sekiguchi and S. Seto, “Methods of Evaluating Leaking of Personal Computer Monitor Image Information from Electromagnetic Noise,” 2008 IEEJ Symposium, S2-9 (in Japanese).
[11] Y. Suzuki, M. Masugi, K. Tajima, and H. Yamane, “Countermeasures for Information Leaking from Personal Computers by EMR,” 2008 IEEJ Symposium, S2-8 (in Japanese).
[12] K. Uchiyama, “Systematizing Methods for Measuring EMR Leaks and an Approach to them—An approach to setting specifications modeled on the NDS specifications,” 2008 IEEJ Symposium, S2-4 (in Japanese).
[13] “EMR Security Guidelines,” Information Security Technology Study Group, October 8, 2004, http: //www.j-netcom.co.jp/ist/ist-glv3.pdf (in Japanese).



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 IEEE, the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan, the Institute of Electrical Engineers of Japan (IEEJ), and the Robotic Society of Japan. 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.

Ryuichi Kobayashi
Senior Research Engineer, Energy Systems Project, NTT Energy and Environment Systems Laboratories.

He received the B.E., M.E., and Dr.Eng degrees in electronic engineering from the University of Electro-Communications, Tokyo, in 1991, 1993, and 2008, respectively. He joined NTT Telecommunications Networks Laboratories in 1993. Between 1997 and 2006, he worked at the Technical Assistance & Support Center, NTT East, and found solutions to EMC trouble in the field. Currently, he is studying EMC measurement methods and sensors. He has participated in ITU-T SG5 since 1997. He is currently the Rapporteur for two issues related to EMC problems in telecommunication centers and homes. His research interests are measurement methods for electromagnetic noise and electromagnetic environments. He is a member of IEEE and IEICE.

Hidenori Sekiguchi
Expert Researcher, Security Fundamentals Group, Information Security Research Center, National Institute of Information and Communications Technology (NiCT).

He received the B.S., M.S., and Ph.D. degrees from the Department of Electrical and Electronic Engineering, Chuo University, Tokyo, in 1994, 1996, and 2003, respectively. Since joining NiCT in 2005, he has been researching information security caused by electromagnetic environments. He is currently Associate Rapporteur of ITU-T SG5 Question 15. He is a member of IEEE, IEICE, and IEEJ.

Shinji Seto
Expert Researcher, Security Fundamentals Group, Information Security Center, NiCT.

He received the B.E. degree in electrical engineering from Osaka Prefectural University, Osaka, in 1961. After he joined the Defense Systems Engineering Department at Mitsubishi Electric Corporation (MELCO) in 1961, he performed theoretical and experimental investigations in areas such as wave propagation, antennas, radio receivers and transmitters, electronic countermeasures, electronic counter-countermeasures, and electromagnetic data security, TEMPEST. As a Senior Engineer at MELCO, he was responsible for electronic warfare systems from large radio systems and computer systems. He has contributed to the development of several national defense standards as the Chairman. Since he was invited by NiCT to be an expert researcher in 2005, he has published more than 50 technical papers.