Systematized Method of Measuring Emanation Security and Trends in Research on EMSEC Standards in Japan

Ministry of Defense, Technical Research and Development Institute
5-1 Ichigaya-Honmura-cho, Sinjyuku-ku, Tokyo 162-8830, Japan
Dr. Kazuo Uchiyama

1 Introduction

Although cellular phone, electronic toll collection (ETC) and radio frequency identification (RFID), which emit electro-magnetic waves improve our daily lives, threats due to emanation (Tempest) from electronic appliances includes PC and faxes are becoming more common.

However, Tempest standards have been established by the U.S. military ; there are no clear guidance for measuring and evaluating Tempest in Japan. Under these circumstances, Japan's Defense Agency (Ministry of Defense since January 2007) has been studying Emanation Security. As a result, National Defense Standards (NDS C 0013) was established in June 2003, and standards for commercial electronic appliances were established by the New Information Security Research Group (IST) in November 2004.

In this year's EMC 2009 Kyoto conference, the background to and concept for quantitatively evaluating emanations are presented, and also perspectives on future evaluations and measurements of emanation security are described.

The meaning of technical term is clarified in this report. Tempest means that information recovery includes unintentional RF emanation when daily business is conducted, and the prevention of these unintentional RF emanations.

2 Systematized measurement and evaluation of emanation security

NDS C 0013 "Test and evaluation method for emanation security" has an open scope of measurements, and methods, except for the section on thread estimates. Because we at the Ministry of Defense would like to know about emanation security standards and countermeasures as well as the general public.

In this section, the concept of NDS standards and comparison with the IST standard are considered.

2.1 Concepts for evaluating and measuring emanation security

There are seven prerequisites for the NDS C 0013 including scope, target appliances, information, spatial limitations, methods, standard values, and confirmation of the effectiveness of measurement values. Communication security generally involves four factors including encryption, record medium storage, communication-line security, and radiation, which includes conduction. This standard covers the scope of emanation security except for floppy disks; magnetic disks, and CD-ROMs. However, the radiation generated by operating these record media in personal computers (PC) is included in emanation security.

This standard covers almost all IT appliances such as PCs, faxes, and printers. Some appliances including routers and secured telephones that only transmit electronic data and control signals are excluded. The standard values according to the frequency are defined as Full Tempest (2-m standard), Relaxed Tempest (20-m standard), and

Table 1 Test frequency range for EMSEC equipment[1)]

Maximum frequency on test equipment (fs)	Upper test frequency
Below 30 MHz (<)	1 GHz
30 MHz - 300 MHz	3 GHz
300 MHz - 1.24 GHz	12.4 GHz
1.24 GHz - 5 GHz	10 GHz or max. value above 5fs
5 GHz - 12.4 GHz	40 GHz or max. value above 5fs

the 100-m standard. The emanation security standard involves testing and measuring both conductive and radiation leakage. This standard for conductive leakage covers all frequency ranges that are used in power cables and signal cables for IT appliances.

Recent IT appliances are high-performance and the clock frequencies of PCs, especially, have reached the gigahertz-frequency level. Under these circumstances, we considered expanding the future frequency region; so that this standard could cover a wide range between 100 kHz and 40 GHz. However, this range cannot be applied to the radiation emitted from the antenna of communication radios. Table 1 lists the test frequency ranges of target appliances. At present, there are no PCs that have a clock frequency beyond 12.4 GHz; however, this standard has defined the upper-limit frequency that covers emanation in the high-frequency region for the time being. As recent IT appliances, especially, PCs run in the higher-frequency regions, the test-frequency should be revised.

2.2 Consideration of standard values for commercial use

Concrete numerical values that are related to defined standard values for threat are not available; however, the concept to define standard values is available. This subsection describes the 20-m Relaxed Tempest standards using commercial values include those for antennas, and compares these with commercial standard values defined by IST.

Emanation radiating from IT appliances can be categorized into both repeatedly generating and unexpectedly generating types. The former involves frequency fluctuations generated by the raster scan method on PCs and the latter involves signals generated suddenly in bursts. The standards defined for the former involve repeated emanation values and those for the latter involve unrepeated emanation values.

Figure 1 is a flow diagram for calculating the standard value of emanation. Equation 1 is the formula to calculate emanation.

Eml= ((S/N)'sl – Gds - Gps) +Ns – Gas + 20log (ds/dm) + 20log (f) + 10log (Zm) – 68.55

····· (Equation 1)

Table 2 lists the parameters for the numerical model that enables the standard value for emanation to be calculated. The attenuation characteristics of emanation transmissions were approximated calculated by using free-space transmission.

Targeted IT appliances included PCs. The limitation value of 20 m for the Relaxed Tempest was use to calculate emanation with Equation 1 using antenna gain obtained from the catalogue

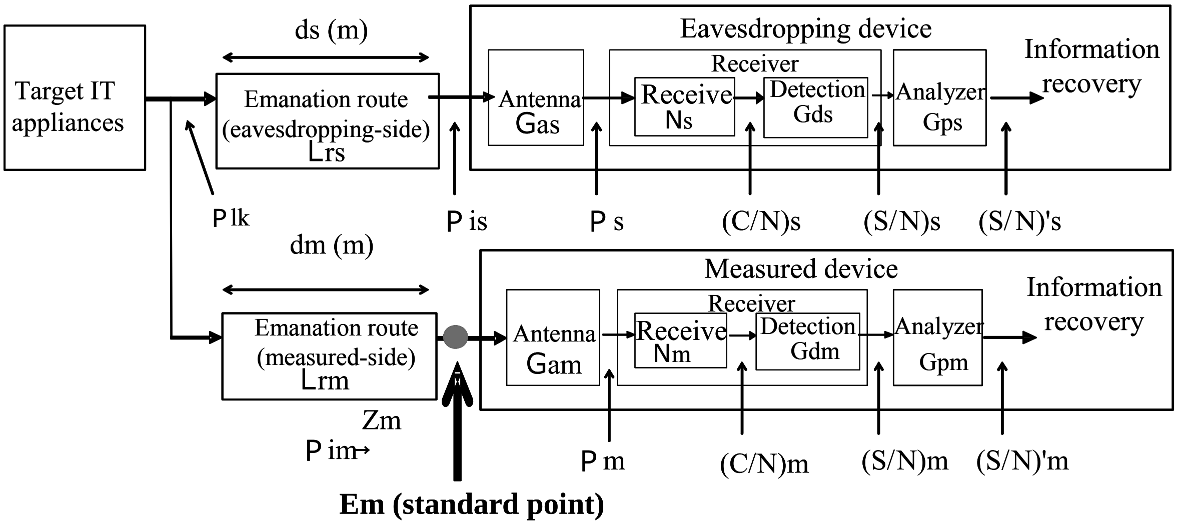

Figure 1 Eavesdropping model on EMSEC3)－5)

Table 2 Parameters for calculating of EMSEC standard values[3) - 5)]

Symbols	Items	Units	Equations or basic prerequisites	Appendix
Eavesdropping side, prerequisites				
(S/N)'sl	Signal to noise ratio (After analysis)	dB	Estimated from experimental results	
Gps	Analyzed gain	dB	Gps = 10log$\sqrt{\ }$(Num)	
Num	Number of analyse	th		
Gds	Detected gain	dB	AM detected wave	
Ns	Receiver noise power	dBm	Ns = 10log(K･Ts･Bs)+Fs+30	
K	Boltzman factor	J/K	Constant	
Ts	Receiver temperature	K	Room temperature (300 K)	
Bs	Receivable bandwidth	Hz	Same prerequisite to obtain signal bandwidth of emanation	
Fs	Noise factor	dB	Realistic value	
Gas	Antenna gain	dBi	Maximum gain at all frequencies under antenna scale limitations	
Lrs	Quantative value of emanation attenuation	dB	Lrs = 20log(4πds/λ)	
ds	Emanation transmission	dB	Setting prerequisite	
Measured side, prerequisites				
Lrm	Conductive transmission	dB	Worst-case scenario	
dm	Emanation transmission	m	Setting prerequisites	
Zm	Spatial impedance	Ω	Zm=Zom=120π　(dm＞λ＞2π)	Far field
Zm	Spatial impedance	Ω	Zm=(λ/2π･dm)･Zom(dm＞λ＞2π)	Near field

value. However, the limited value of 20 m is discrete because the frequency parameter is defined as discrete. As a result, the standard values for commercial use were obtained from line approximation. Figure 2 compares the standard values for emanation at a receivable bandwidth of 100 kHz that I calculated these with the IST standard value in 2004. The IST standard has defined 3 MHz as the value at the receivable bandwidth. The EMSEC guidelines explain why

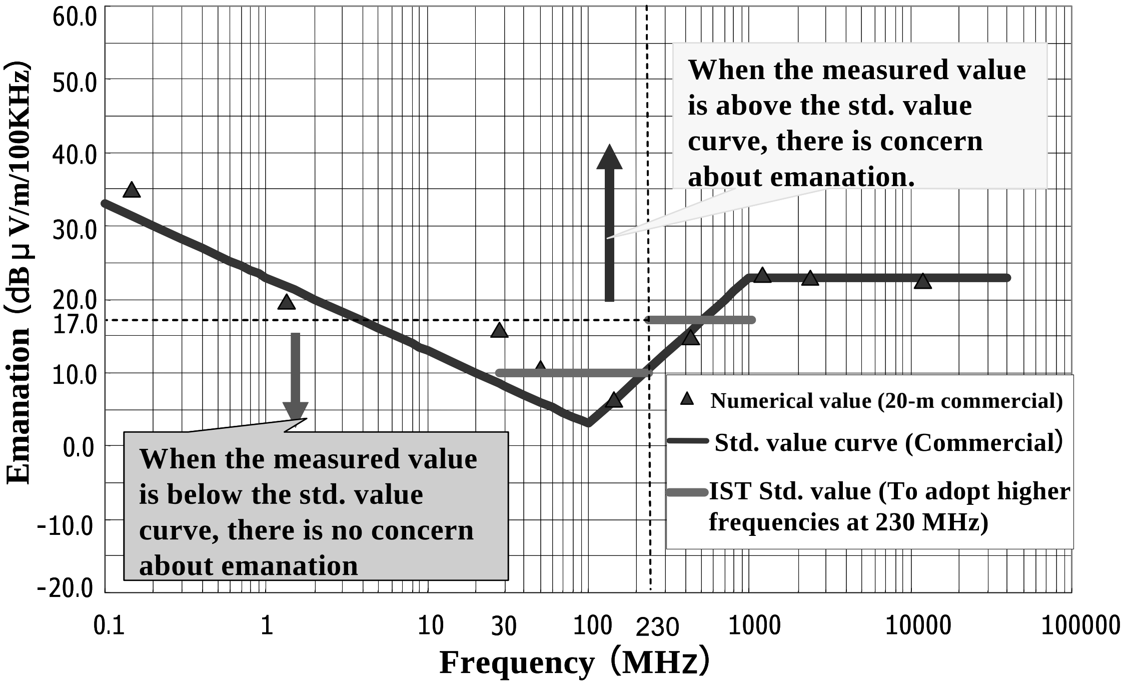

Figure 2 Comparison with IST std. value and EMSEC value for commercially available equipment [2) – 5)]

the receivable bandwidths have been defined as 100 kHz and 3 MHz because they are almost the same as those for commercial appliances including spectrum analyzers set an upper frequency limit of 3 MHz. Appliances above a receivable bandwidth of 10 MHz are not produced or sold on the domestic market, according to EMSEC and I think the trade-off between economics and utility is a serious problem, because there is some information that is not include in the 3-MHz emanations. Receivable bandwidth in the future would have to shift to broader-bandwidth-emanation regions. The receivable bandwidths in NDS C 0013 are defined as 100 kHz and 10 MHz. When the standard value and IST standard value correspond to the measured value, the frequency-characteristic curve of the standard value or IST standard value is beyond the measured frequency-characteristic curve, and the concern about information leakage caused by emanation disappear.

IST defined the standard value as 10 dBμV/m in frequencies between 30 MHz and 230 MHz, 17 dBμV/m in frequencies between 230 MHz and 1 GHz. This is because the International Special Committee on Radio Interference (CISPR) test method was introduced, and it only defined PC and did not include faxes. The IST standard has become more relaxed than the one I calculated in the 30-MHz and 230-MHz, and 230-MHz and 500-MHz frequency regions. However, these values have been increased to cover the 500-MHz and 1-GHz frequency regions. The upper limit of frequency region in the IST standard is 1 GHz, and there is some possibility this upper limit will be revised because the clock frequency of IT appliances has tended to shift to higher-frequency regions. The upper limit for frequency tends to be in line with the radiation control value for EMC, which has been defined by the Voluntary Control Council for Information Technology Equipment (VCCI).

However, the basic model for standard value should be encouraged despite the fact that it is less relaxed for commercial use than military applications. The RF security guidelines recommend conducting EMSEC (Tempest) countermeasures in e-government (electronic government) and commercial fields by using IST standard. But this standard value presents some problems. First, the standard value was obtained solely from experimental results using PCs in an RF anechoic chamber. Second, the frequency range was limited to 30 MHz - 1 GHz, which is relatively narrow. Third, as the receivable bandwidth has been defined as 100 kHz and 3 MHz, both standard values and frequency ranges might create problems with applying an equivalent such as NDS C 0013 to e-government and commercial facilities.

3 Perspectives and Conclusion

Although EMSEC research in Japan has lagged behind that in the United States and Europe, we have at last established NDS and IST standards. “The ubiquitous society” in which we can communicate anyone, anywhere, and at any time is here today, but problems with information security including EMSEC continue to be pressing issues. After this, this old but new problem as explained by the Japanese proverb of “温故知新：Onko Tishin”, means new research topics are found when we scrutinize old ones. It is my sincere belief that more attention should be given to EMC and EMSEC (Tempest).

References

1) Ministry of Defense standards, NDS C 0013, Test method for Emanation Security, Japan Association of Defense Industry

2) Radio-frequency security guideline, New Information Security Research Group, Nov. 2004

3) K. Uchiyama, Information leakage by the emanation RF and how to evaluate it, Japan Defense Technology Journal, Feb. 2005, pp. 4-13

4) K. Uchiyama, Information security for emanation security and NDS standard, EMC journal Japan, Jan. 2006, pp. 124-140

5) K. Uchiyama et al. The concept and systematized method of EMSEC, The 2008 annual meeting record I.E.E Japan, Vol. 1, pp. S2(8) - S2(11), Fukuoka, Japan, Mar. 2008