4-8 Electromagnetic Security

TANAKA Hidema

In this paper, we show the activity of research on the security analysis of electromagnetic emanation (electromagnetic security) between 2006 and 2009 in Security Fundamentals Group. The activity of electromagnetic security has two purposes; the development of evaluation method of amount of information leakage via electromagnetic emanation and the development of countermeasures against such threat. We proposed the evaluation method applying the estimation method of channel capacity of continuous channel. In particular, we focused on the threat of information leakage displayed on the monitor. Such threat is called as TEMPEST in general. And we developed the countermeasure on software (TEMPEST fonts) and it does not needs any devices. We move the technology to the venture company and they have commercialized it. At last, we successes the standardization of both of estimation method of information leakage and security level of countermeasure in ITU-T.

Keywords
Electromagnetic emanation, Electromagnetic security, Channel capacity, TEMPEST, Information leakage

1 Introduction

When we heard that displays of personal computers could be spied on by intercepting electromagnetic emanation, we thought it was only a theoretically feasible technology, and due to the cost of devices for such purpose (Fig. 1), it seemed to be an unrealistic threat; however, by the end of the first year of the second term, we recognized it as a realistic threat. Any electronic device generates noise according to the processing information, and the noise is emitted as electromagnetic emanation. Especially in terms of screen image, the system to reconstruct information is very simple, similar to television. However, it is more difficult to search for frequencies and appropriate bandwidths that contain sufficient screen image, and adjust vertical and horizontal synchronous frequencies. When these have been successfully found, screen image leakage through electromagnetic emanation becomes a serious threat. This is because electromagnetic emanation can be produced not only by direct emission into free-space, but also by conductive emission via power cable or LAN cable, and as a result, for example, it becomes possible to reconstruct screen image in a separate room in the building. In addition, various objects including window sash, metal door frame, and ceiling pipes of air-conditioning system can be used as an antenna. In some

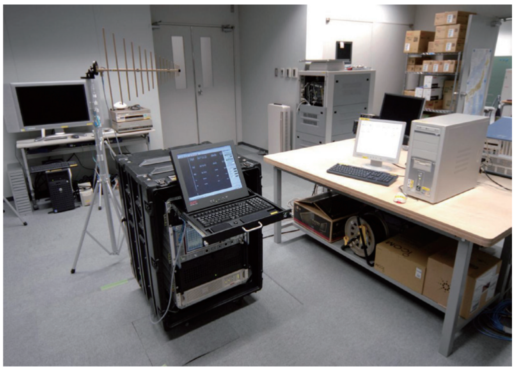


Fig.1 Tempest receiver FSET-22

cases, instead of spying the actual text, it may be only necessary to find out what kind of work or operation is performed. For example, touch panels are often used for ATM banking machines, and the input PIN code can be disclosed as screen image from the color change of the selected button. In the case of electronic voting, it is possible to grasp information on which candidate was voted for from a remote place. Thus, the most serious problem of this threat is that since human interface devices are targeted, the security cannot be established by cryptographic technologies, and information is leaked more directly. With the progress of our research, we discovered that it was possible to construct a device that can obtain sufficient information by combining consumer products as shown in Fig. 2.

The purpose of this research was the development of evaluation method of amount of information leakage via electromagnetic emanation and the development of countermeasure technologies against such threat. First, we developed a method to evaluate the frequencies that contain the most information and required bandwidth. We applied the calculation method of channel capacity of continuous channel to this method. However, since the received signals also include noise, we employed empirical rules of experimental results for the calculation of S/N. By analyzing this result and the characteristics of screen configuration that are more likely to emit electromagnetic emanation, we developed countermeasure technologies. While there are many hardware type countermeasure technologies that emit counter-electromagnetic waves (Fig. 3), our research is distinctive in providing software type countermeasures by filter software that changes the screen configuration. This is because we put our emphasis not only on devices designed to stay in a single location such as desktop PCs but also portable devices such as laptop PCs, as well as low installation cost, and ease of installation to the existing infrastructure.

It is also important to develop a method to evaluate whether countermeasure technologies provide sufficient security. For example, even though there is a countermeasure for the frequency band that is most suitable to obtain information, the information could be reconstructed by using the second best (or worse) frequency band. It was essential to take an EMC-like approach for this evaluation. Therefore, in our research it was important to link an information-theoretic approach, the viewpoint of security evaluation of cryptographic technology, and electromagnetic wave measurement technology, and it was conducted as a joint research by the Security Fundamentals Group and EMC Group. The final development of countermeasure technology has been commercialized by a venture company, and the evaluation method has been standardized by ITU-T.

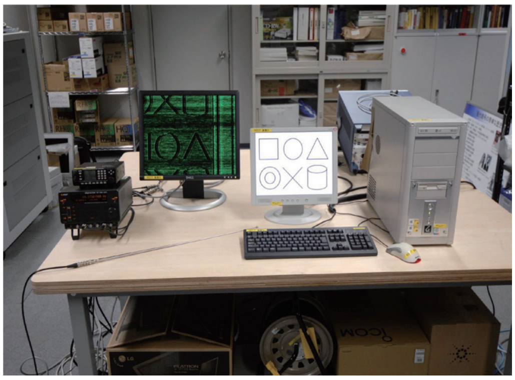


Fig.2 Easy-Tempest receiver

Combination of retail devices

Fig.3 Tempest countermeasure

Device I/F type

2 Evaluation of the amount of information leakage

2.1 Channel capacity

When a channel is given, the maximum amount of information that the channel can send is given by the channel capacity, and defined by the maximum mutual information between the sender and receiver. For an additive one-dimensional Gaussian channel with limited average power, given S denotes signal power, and N denotes noise power, channel capacity C is expressed as follows.

$$C = \frac{1}{2}\log_2 \frac{S+N}{N} \text{ [bit/symbol]} \tag{1}$$

In addition, for an additive Gaussian channel with limited bandwidth, given W denotes bandwidth, channel capacity is expressed as follows.

$$C = \frac{W}{2}\log_2 \frac{S+N}{N} \text{ [bit/sec]} \tag{2}$$

Channel capacity means the maximum amount of information that can be sent using the signal power and bandwidth which the sender secured in a channel where noise has a uniform distribution. The channel capacity allows the sender to increase the quality of communication by checking whether the channel is sufficient for the amount of information to be sent, or by improving the required signal power and bandwidth.

2.2 The amount of information leakage

In terms of the amount of information contained in the electromagnetic emanation from IT devices, we discuss its calculation methods based on the concept of channel capacity, based on the idea that the IT device and receiver are linked by a channel with limited bandwidth. As previously described, the theory of channel capacity is based on the sender's point of view, and the sender can adjust signal power and bandwidth in a channel where noise exists. The receiver should use a receiver with the bandwidth set by the sender in order to receive the amount of information that the sender intended to send.

On the other hand, signal power and noise power co-exist when receiving electromagnetic emanation, and it is the receiver who determines which is signal and which is noise. In addition, the performance of channel depends on the S/N ratio or bandwidth of the receiver which has been set up by the receiver. Thus, when receiving electromagnetic emanation, only the channel one-sidedly determined by the receiver can be established.

Figure 4 shows an example of electromagnetic waves emitted from a PC measured by frequency domain. The bandwidth of the measuring instrument (spectrum analyzer) was set to 10 [MHz]. Previous experiments showed that screen image can be successfully reconstructed at the frequency of 285 [MHz][1], and it is considered that the emanation at the frequencies between approximately 277 [MHz] and 293 [MHz] contains screen image (signal), and other frequencies are noise. In addition, we give an example of electromagnetic emanation measured by time domain. Figure 4 plots the maximum electromagnetic emanation shown in Fig. 5.

Given $S(f)$ denotes signal power at the frequency of f, and $N(f)$ denotes noise power, then channel capacity C at the range of frequency $[f_1, f_2]$ (provided $f_2 > f_1$) is given by the

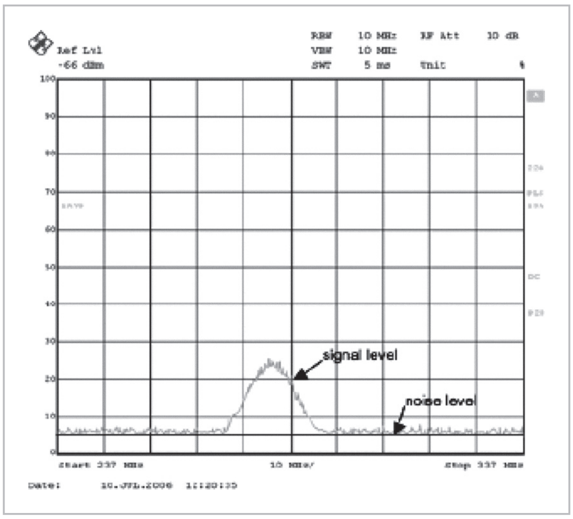


Fig.4 *Measurement result of electromagnetic emanation by spectrum analyzer (frequency domain)*

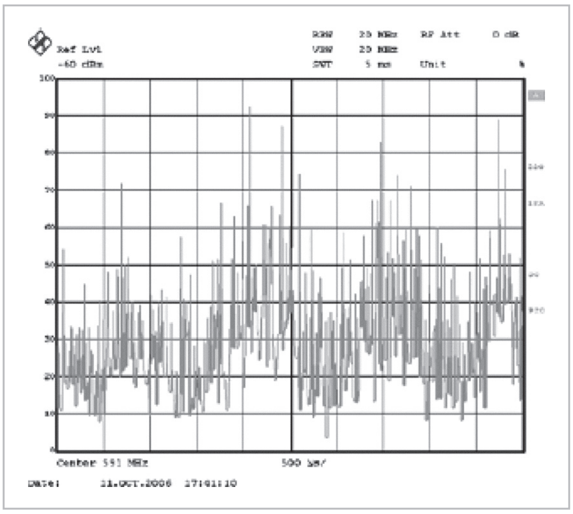


Fig.5 *Measurement result of electromagnetic emanation by spectrum analyzer (time domain)*

maximum value of mutual information I per unit time.

$$I = W \int_{f_1}^{f_2} \log_2 \frac{S(f)+N(f)}{N(f)}\, df \text{ [bit/sec]} \qquad (3)$$

On the other hand, when receiving electromagnetic emanation, since $S(f)$ and $N(f)$ are determined by the bandwidth and the S/N ratio of the receiver, it is apparent that the receivable information is smaller than I which is computed by the equation (3). Therefore, the mutual information of the equation (3) is the same as the channel capacity to receive electromagnetic emanation. However, as previously described, since its property is different from channel capacity, the amount of information defined by the equation (3) is referred to as “the amount of information leakage per unit time” and denoted by the symbol L in this paper, in order to distinguish it from the original sense of mutual information and channel capacity.

In addition, if the bandwidth of the receiver is set to W, and given f_0 denotes the receive frequency, the range of receive frequency is given by $[f_0 - W/2, f_0 + W/2]$.

2.3 The relation between the amount of information leakage and receiver bandwidth

We defined the amount of information leakage by the equation (3), and as the amount of information that the receiver can obtain via electromagnetic emanation. The amount of information emitted from the source of electromagnetic emanation per unit time is hereafter referred to as the amount of targeted information, and denoted by A [bps]. In addition, given L [bps] denotes the amount of information leakage, and if the channel satisfies the relation of (amount of targeted information A)< (amount of information leakage L), the receiver is able to obtain all the amount of targeted information within a unit time.

The S/N ratio is determined by the specific performance of the device or environment, and the receiver cannot adjust the value. Therefore, the amount of information leakage is determined by the bandwidth of the receiver only. The bandwidth of the receiver has an influence on the S/N ratio and time to establish amplitude. The larger the bandwidth is, the more improvement in the S/N ratio can be made, and the shorter the time to establish amplitude becomes; therefore, a wider bandwidth is more effective to receive electromagnetic emanation. However, receivers with more than 20 [MHz] bandwidth are categorized as high-priced devices, and commonly available receivers are around 10 [MHz]. In addition, when wider bandwidth is used, the receivers will receive a wider range of signals in addition to the signals that are meaningful for them. As a result, although the S/N ratio in terms of signal reception is improved, the S/N ratio in terms of receiving meaningful information could become worse.

Moreover, the setting for required bandwidth could vary depending on the property of the receiving signals. For example, when receiving one-off information such as an authentication signal of a non-contact type smart card or keyboard stroke information, a deficit of received information may result in a fatal error in obtaining the information. However, when receiving screen image of a static image display, the deficit of received information can be corrected or modified to some degree, since highly correlative information is repeatedly sent. Therefore, it is necessary to set an appropriate bandwidth based on the amount of information and property of the signals of the source of the receiving information and the amount of information leakage.

2.4 Verification by experiment on reconstruction of screen image

Experiment summary

In this section, we verify the validity of the calculation of information leakage, based on the experiment in which we displayed a static image on a laptop PC and reconstructed the screen image using electromagnetic emanation from the main body. A static image shown in Fig. 6 was displayed on the screen of the PC, and electromagnetic emanation was received by a probe that was coherent to the main body. The relation of targeted information, receiver, and the channel between them in this experiment is shown in Fig. 7.

Generally the amount of information [bps] of VGA signal is computed as follows.

The number of colors [bits]
× total pixels [dots] × frame rate [fps] (4)

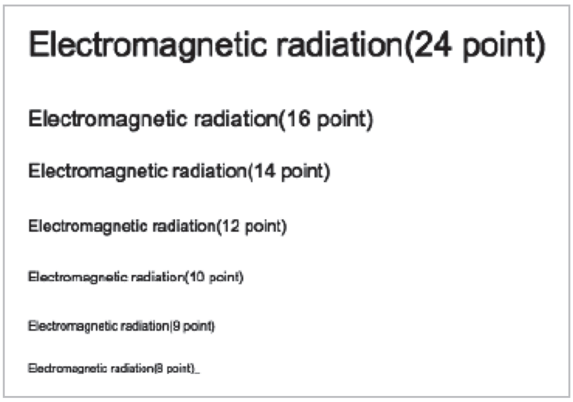
"Total pixels [dots] × frame rate [fps]" is also called the dot clock frequency. The specification of the measured display was set to 24 [bit] color, total pixels of 800×600 [dots], and frame rate of 60 [fps], therefore, the amount of targeted information A is computed as follows.

$$A = 24 \times (800 \times 600) \times 60 = 691 \text{ [Mbps]} \quad (5)$$

Measurement results

The measurement results when the bandwidth was set to 10 [MHz] and 20 [MHz] are shown in Figs. 8 and 9, respectively. From these results, it is apparent that the established channel has the larger amount of information leakage when the bandwidth was 20 [MHz] than when it was 10 [MHz].

To compute the amount of information leakage from these results, let L_{10} denote the amount of information leakage when the



Electromagnetic radiation(24 point)

Electromagnetic radiation(16 point)

Electromagnetic radiation(14 point)

Electromagnetic radiation(12 point)

Electromagnetic radiation(10 point)

Electromagnetic radiation(9 point)

Electromagnetic radiation(8 point)_

Fig.6 *Displayed image on target PC*

Characters only. Black figure on white background

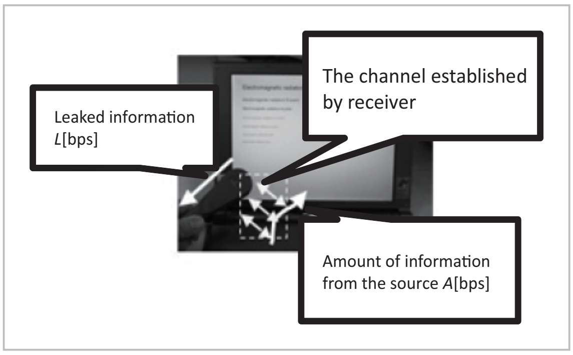

Leaked information
L[bps]
The channel established by receiver
Amount of information from the source A[bps]

Fig.7 *The relation between target information and receiver on the channel*

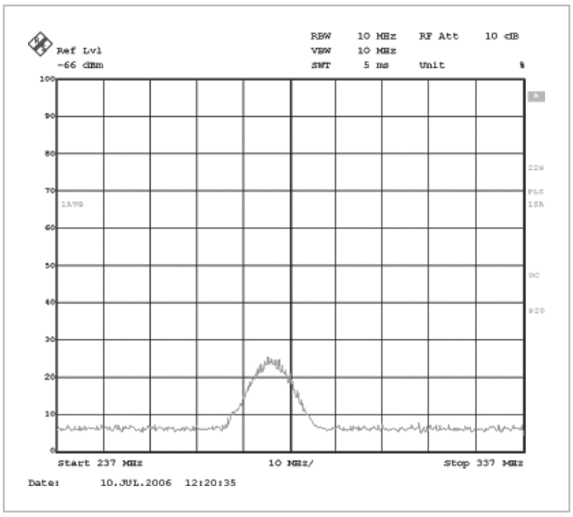


Fig.8 *Measurement result of electromagnetic emanation from target PC (Bandwidth 10[MHz], frequency range 237 – 337[MHz])*

bandwidth is 10 [MHz], and let L_{20} denote the amount of information leakage when the bandwidth is 20 [MHz].

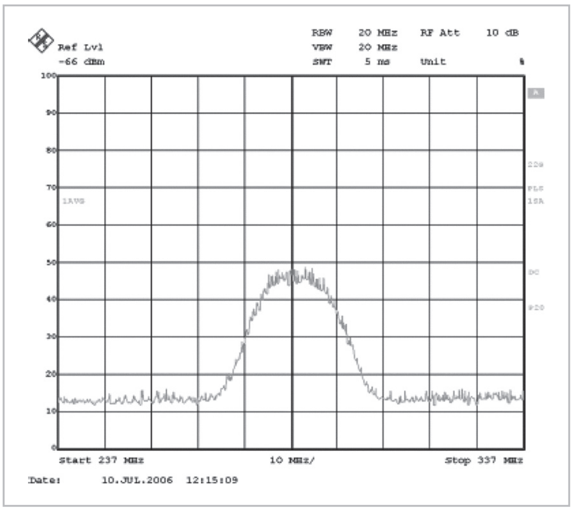


Fig.9 Measurement result of electromagnetic emanation from target PC (Bandwidth 20[MHz], frequency range 237 – 337[MHz])

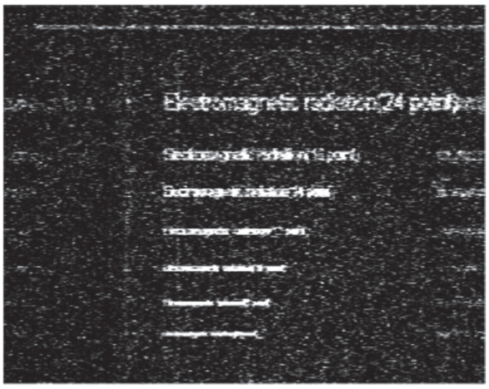


Fig.10 The reconstructed image with bandwidth 10[MHz]

Without image processing unit

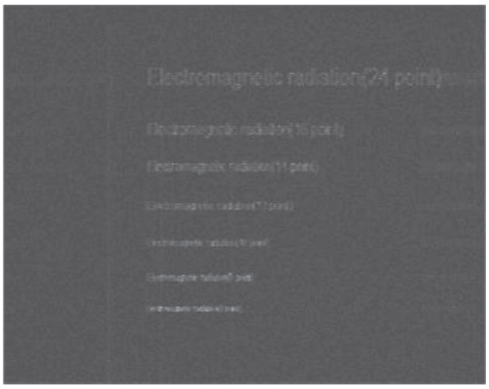

Electromagnetic radiation(24 point)
Electromagnetic radiation(16 point)
Electromagnetic radiation(11 point)

Fig.11 The reconstructed image with bandwidth 20[MHz]

Without image processing unit

$$L_{10} = W\int_{280}^{290} \log_2 \frac{S(f)+N(f)}{N(f)}\, df \text{ [Mbps]} \qquad (6)$$

$$L_{20} = W\int_{275}^{295} \log_2 \frac{S(f)+N(f)}{N(f)}\, df \text{ [Mbps]} \qquad (7)$$

Since the amount of targeted information is 691 [Mbps], based on the assumption that the static image will not change, it will take about 25 seconds to receive the whole screen image when the bandwidth is 10 [MHz], and about 7 seconds when the bandwidth is 20 [MHz], in order to reconstruct the screen image. On the other hand, since Fig. 6 is a black and white binary image, it is a 1 [bit] color image, and therefore, the amount of targeted information can be regarded as about 29 [Mbps]. Although it is a black and white image in terms of device specification, it is sent as 24 [bit] information. This means that 24 [bits] are used to send 1 [bit] of information, which can be regarded as a very redundant communication. Considering the property of the displayed screen image, it is appropriate to regard it as a 1 [bit] color image as described latter, and we consider the bandwidth of 10 [MHz] is sufficient to receive the information.

Comparison of the amount of information leakage and reconstructed image

Figures 10 and 11 show the image reconstructed from the screen image by adding vertical and horizontal synchronous frequencies to the received signals. Image processing such as integration (averaging) of multiple frames has not been applied to these results.

Therefore, these reconstructed images consist of about 28 [Mbits] of information when the bandwidth is 10 [MHz], and about 101 [Mbits] of information when the bandwidth is 20 [MHz]. They contain about 0.97 [bits] per 1 [dot] pixel of information when the bandwidth is 10 [MHz], and about 3.5 [bits] when the bandwidth is 20 [MHz]. As previously described, since it is regarded as a black and white binary image, the obtained reconstructed image was fairly clear even with the bandwidth of 10 [MHz] and without averaging process.

Note that the reconstructed image was slightly shifted vertically and horizontally because of the subtle differences in vertical and horizontal synchronous frequencies. It is also possible that noise from the equipment for reconstruction had influenced the image quality. For this reason and due to printing issues, it may be more difficult to read the examples of reconstruction in this paper than in reality.

3 Reconstruction of screen image

The equipment that displays the targeted screen image generates horizontal and vertical synchronous frequencies, and even though it complies with the same VESA standards, there is a margin of error within a range that does not affect the image quality. Since the error varies depending on device, it can be used to obtain information from a specific device. Therefore, even in an office environment where devices from the same manufacturer and of the same model type are running at once, counter-intuitively, it is possible to narrow down the target and reconstruct screen image.

Moreover, there are various methods to receive electromagnetic emanation to reconstruct screen image, including a method that uses antenna to intercept electromagnetic emanation that propagate through free-space, and a method to intercept through power cables. However, the required frequencies and bandwidth varies in accordance with the quality of electromagnetic emanation.

Following this, we assumed some cases to verify the feasibility.

Equipment

In the experiment, we used ROHDE & SCHWALZ FSET22 as a Tempest receiver and FrameControl ver. 4.24 as an image processing application. The specifications of FSET22 are given in Table 1.

Table 1 *Specification of FSET22*

Frequency range	100 Hz ∼ 22 GHz
Frequency resolution	0.1 Hz
Bandwidth	10 Hz ∼ 500 MHz in steps of 1/2/5
Average noise level	< -142 dBm (1 MHz)

FrameControl supports processing of signals from FSET22 at 256 frames/3s. The performance of the image processing application has a significant influence on image reconstruction by Tempest. The image processing application used in the experiment integrates images of 256 frames in order to eliminate noise and create clear images. As for the antenna and probe for reception, we used an Anritsu MP666A logarithm periodic antenna (20 to 2000 MHz), an Anritsu MA2601B/C near-magnetic field probe (5 to 1000 MHz), and a TOKIN EIP-100 injection probe (80 KHz to 30 MHz).

The targets were a SONY VAIO laptop computer (hereafter “VAIO”), IBM ThinkPad (hereafter “IBM”), and a CRT display connected to a typical desktop PC (hereafter “CRT”). We used the CRT to compare with an LCD display. This is because we considered that a CRT emits stronger unintentional electromagnetic waves than an LCD.

Experiment Environment

Based on the following attack scenarios, we conducted the experiments using a near-magnetic field probe, antenna and injection probe.

- The attacker set up a near-magnetic field probe close to the targeted PC (i.e. under the desk).
- The attacker attempted to intercept the electromagnetic waves emitted from the targeted PC from the adjacent room or outside by using an antenna.
- The attacker attempted to intercept through the power cable of the targeted PC from a different room in the same building.

We consider that the closer to the last scenario, the more serious the realistic threat becomes. On the contrary, the closer to the first scenario, the shorter the distance to the target becomes, and therefore, the clearer the images can be intercepted.

Experiment using a near-magnetic field probe

In this experiment, we set a near-magnetic field probe close to the targeted PC and attempted interception. The reconstructed images are shown in Fig. 12. Since there was no difference between the results of the VAIO and IBM, the result of the VAIO is omitted here. In addition, the parameter values of the Tempest receiver are given in Table 2. The characters are clearly legible in the results shown in Fig. 12. If the text has specific meaning, it will be possible to understand the meaning even if a few characters are unrecognizable.

The following experiments also judges success or failure of the experiments by the legibility of characters; however, the legibility varies largely depending on person, and it is easier to read characters on the screen of the Tempest receiver than in the printed image. Moreover, since the screen of the Tempest receiver does not display a static image, it is difficult to print it. On the contrary, if receivers watch the screen for a long time, they will get used to it, and they will be able to recognize the characters more easily.

Experiment using an antenna

Interception using an antenna is considered to be a more realistic threat than interception using a near-magnetic field probe. In this experiment, we attempted interception 4 [m] away from the targeted PC. The experiment was conducted in a location with good visibility in the elevator hall of the third floor of Building No.5, at NICT Koganei Head Quarter. Since the experiment that targeted the IBM failed, Fig. 13 only shows the reconstruction results of the VAIO and CRT, and Table 3 gives the parameter values for the Tempest receiver. The reason why the experiment for the IBM failed was probably due to device specific problems. Multiple previous experiments demonstrated that the strongest electromag-

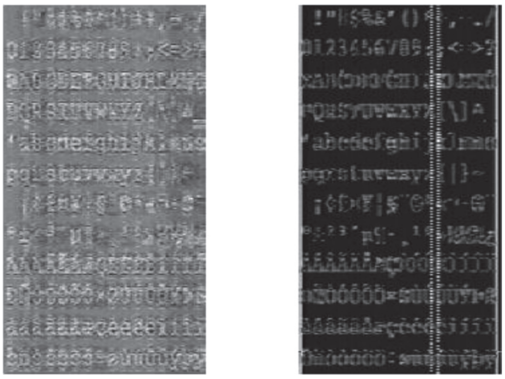


Fig.12 *The reconstructed image using near-magnet field probe (using 128 frame averaging)*

Left=IBM, Right=CRT

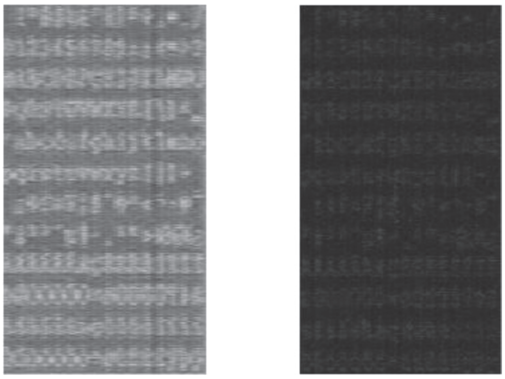


Fig.13 *The reconstructed image using antenna from 4[m] distance (using 128 frame averaging)*

Left=VAIO, Right=CRT

Table 2 *The parameter values in experiment using near-magnetic field probe*

	Frequency [MHz]	Bandwidth [MHz]
IBM	461.2	20.0
CRT	57.4	20.0

Table 3 *The parameter values in experiment using antenna*

	Frequency [MHz]	Bandwidth [MHz]
VAIO	844.8	20.0
CRT	973.2	20.0

netic waves were emitted from the hinges of a laptop PC. While the hinges of the IBM are made from metal, they are plastic in the VAIO and many other laptops. In addition, from our experience, thin LCD displays emit very strong electromagnetic waves. Although the intercepted images were less clear than the ones in the experiment using a near-magnetic field probe, there was no problem with recognizing the characters on the actual Tempest receiver.

Experiment using an injection probe

Attack scenarios using an injection probe are considered to be the most realistic threat. This is because emitted electromagnetic emanation propagate almost without being attenuated within the same building, and the attacker has a smaller risk of being noticed. In one of these experiments, we set a probe 30 [cm] away from the targeted PC, and in another we set it over a 30 [m] extension cable.

There was no difference in the results of these experiments. Figure 14 shows the reconstructed image of CRT when 30 [m] extension cable was used, and Table 4 shows the parameter values for the Tempest receiver. Although we expected that screen image could not be obtained from the VAIO and IBM due to AC adapter issues, the experiments were successful. However, the experiment using an injection probe tended to add more noise compared to other two experiments, and in some cases the averaging process increased noise and made it more difficult to recognize characters. Nevertheless, similar to other experiments, characters were generally legible.

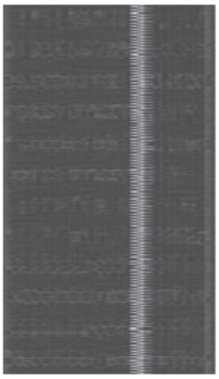


Fig.14 The reconstructed image using injection probe from 30[m] distance (using 128 frame averaging)

Table 4 The parameter values in experiment using injection probe

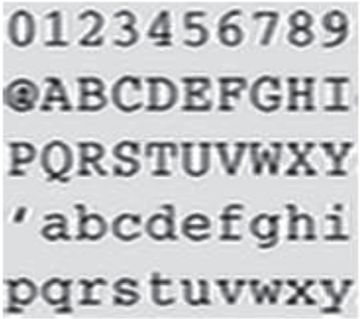
	Frequency [MHz]	Bandwidth [MHz]
CRT	23.8	20.0

In addition, although when using an antenna or a near-magnetic field probe, the results varied depending on position or orientation, when using an injection probe over a power cable, stable results were obtained. The result was not affected by distance if it was 30 [m] or so. This also confirmed that interception using an injection probe is the most serious threat.

4 Development of countermeasure technology

Analysis of Tempest fonts

Tempest fonts are created by removing the top 30% of horizontal frequency components from the image of the source fonts by using a discrete Fourier transform[2]. This is based on the fact that the top 30% of horizontal frequency components affects the reconstruction of image in Tempest. The interception experiment described in **3** actually targeted these Tempest fonts. Figure 15 shows enlargement image of Tempest fonts. It shows dither around the outlines of characters (white block-like



0123456789
@ABCDEFGHI
PQRSTUVWXY
'abcdefghi
pqrstuvwxy

Fig.15 Enlargement image of Tempest fonts

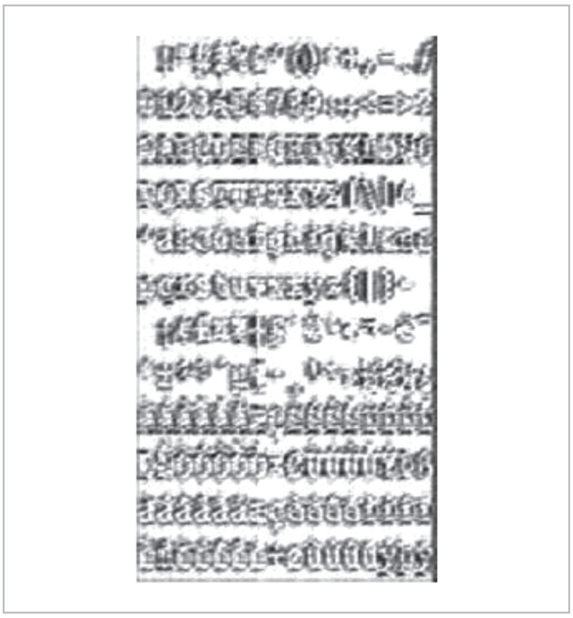


Fig.16 Black/White contrary processed image of left image in Fig. 12

patterns around the characters). In addition, another processed image is shown in Fig. 16.

This image is a simple inversion of black and white, and we can see the dither has been clearly reproduced. This helps to maintain the shape of characters and makes the characters legible in the reconstructed image. The characters consisting of straight lines tend to keep their shapes better, and are more easily recognized. In the experimental result of Kuhn and Anderson[2], the characters disappeared completely; however, as our experiment shows, the characters actually become legible by enhancing dither. This is probably because image processing technology has improved since Kuhn and Anderson conducted their experiments.

Thus, generation of dither could reduce the security against Tempest, therefore, we presumed that it could be improved by eliminating dither. In this paper, we discuss the application of a Gaussian filter as a method to eliminate dither without losing the property of Tempest fonts. High frequency content of the image is caused when the correlation between neighboring pixels is low. Since a Gaussian filter increases the correlation of neighboring pixels, the generated frequency content will not be greater than the one removed by discrete Fourier transform.

Discrete Fourier transform and Gaussian filter smooth out the entire image, and as a result the whole image will be blurred. Therefore, this process is not suitable for the characters in the font we are discussing here, and it is necessary to find a parameter setting that maintains the legibility without losing effectiveness against Tempest. In this paper, we investigated experimentally and determined the most suitable setting as radius 3.0 pixels and threshold 25.0 pixels.

On the other hand, the effect of the Gaussian filter can be evaluated by the amount of information leakage from the equation (3). Based on Fig. 17, we verify the effectiveness of countermeasure technology using a Gaussian filter. The image processed from Fig. 17 with a radius of 1 [pix] is referred to as processed image 1 (Fig. 18). The image processed from Fig. 17 with a radius of 2 [pix] is referred to as processed image 2 (Fig. 19). Due to the nature of paper, it is difficult to see the differences in Figs. 17 to 19; however, the effect of process is apparent when observing the degree of vagueness in the bottom text (8-point) and the degree of smoothness of edges in the top text (24-point). Processed image 2 showed more clear differences and looked more blurred on the screen, and it seems more difficult to recognize the text smaller than 10-point. In addition, the text seems blurred even in 24-point.

We conducted experiments to reconstruct the screen image of these images by intercepting emitted electromagnetic waves. The specification of the display card of the measurement target was 24 [bit] color image, total pixels of 800 × 600 [dot], and frame rate of 60 [fps]. We used the receive frequency of 335.4 [MHz] and the bandwidth of 20 [MHz], and attached an injection probe to a VGA cable to attempt the interception.

Analysis based on the amount of information leakage

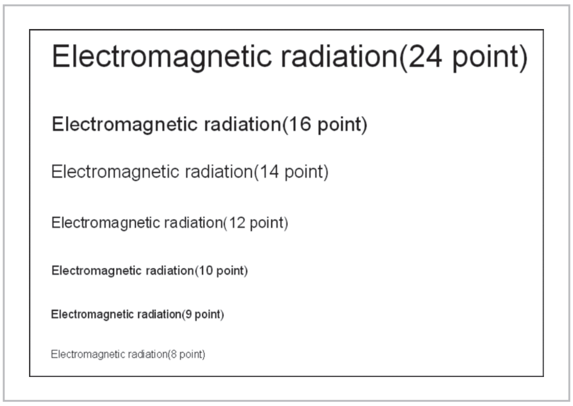
In this section, we compare the source image and processed image 2 based on the amount of information leakage. Since the source image is a black and white binary image, the amount of targeted information of the source image A_0 is assumed as a 1 [bit] color image and computed as follows.

$$A_0 = 1 \times (800 \times 600) \times 60 = 29 \text{ [Mbps]} \qquad (8)$$

On the other hand, since gradation was produced by a blur effect in processed image 2, it is a 256 gray scale image (8 [bit] intensity image). Therefore, the amount of targeted information A_2 is assumed as an 8 [bit] color image and computed as follows.

$$A_2 = 8 \times (800 \times 600) \times 60 = 232 \text{ [Mbps]} \qquad (9)$$

The result of measurement of electromagnetic emanation is shown in Figs. 20 and 21, respectively. Based on these results, L_0, the amount of information leaked from the source image, and L_2, the amount of information leaked from processed image 2, are computed


Electromagnetic radiation(24 point)

Electromagnetic radiation(16 point)

Electromagnetic radiation(14 point)

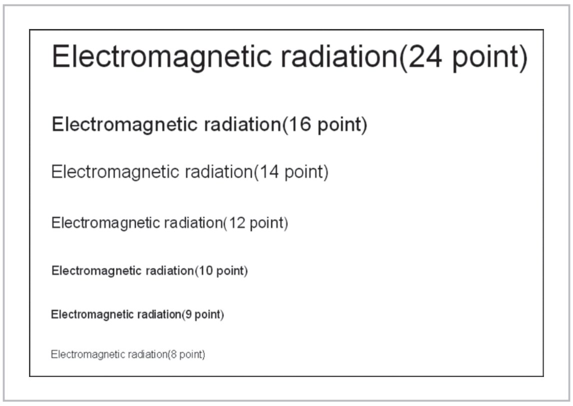
Electromagnetic radiation(12 point)

Electromagnetic radiation(10 point)

Electromagnetic radiation(9 point)

Electromagnetic radiation(8 point)

Fig.17 Source image


Electromagnetic radiation(24 point)

Electromagnetic radiation(16 point)

Electromagnetic radiation(14 point)

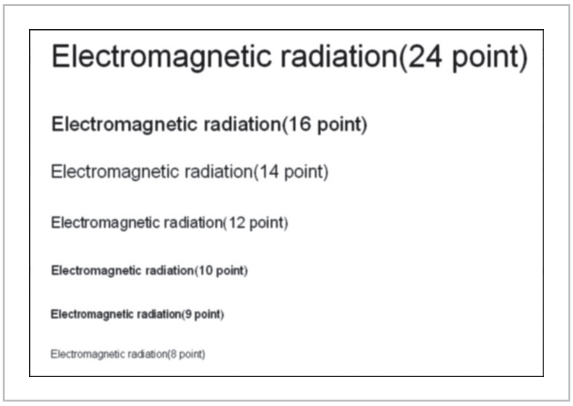
Electromagnetic radiation(12 point)

Electromagnetic radiation(10 point)

Electromagnetic radiation(9 point)

Electromagnetic radiation(8 point)

Fig.18 Processed image 1


Electromagnetic radiation(24 point)

Electromagnetic radiation(16 point)

Electromagnetic radiation(14 point)

Electromagnetic radiation(12 point)

Electromagnetic radiation(10 point)

Electromagnetic radiation(9 point)

Electromagnetic radiation(8 point)

Fig.19 Processed image 2

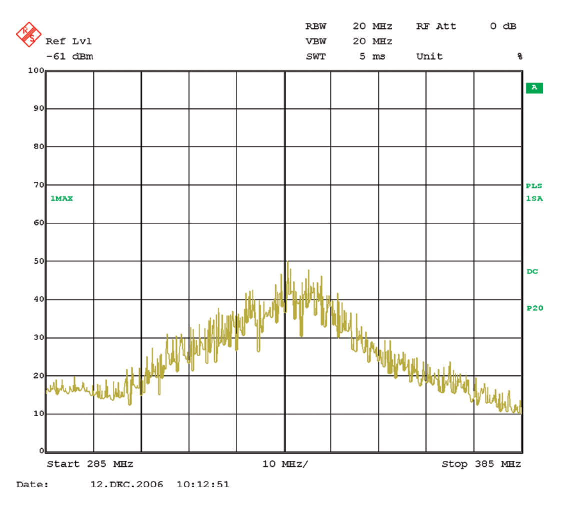


Fig.20 Measurement result of electromagnetic emanation by spectrum analyzer (Source image)

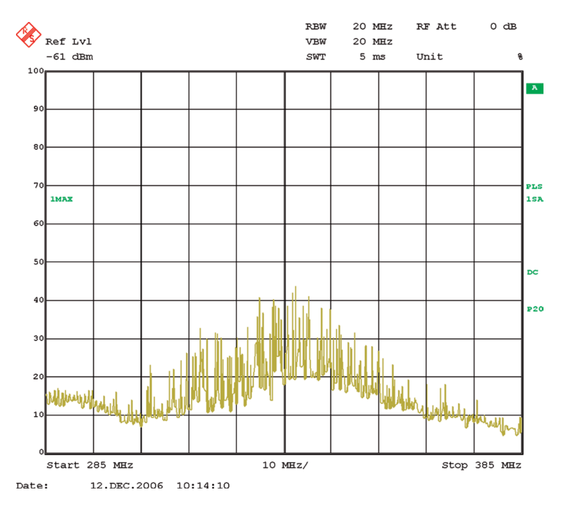


Fig.21 Measurement result of electromagnetic emanation by spectrum analyzer (Processed image 2)

as follows.

$$L_0 = W\int_{325.4}^{345.4} \log_2 \frac{S(f)+N(f)}{N(f)}\,df \tag{10}$$
$$= 83.1\,[\text{Mbps}]$$

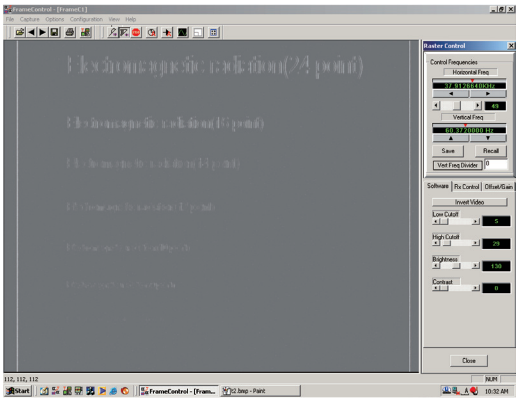
$$L_2 = W\int_{325.4}^{345.4} \log_2 \frac{S(f)+N(f)}{N(f)}\,df \tag{11}$$
$$= 49.8\ [\text{Mbps}]$$

These results yield $L_0 > A_0$, and when an averaging process is not performed, the reconstructed image consists of about 2.9 [bits] of information per 1 [dot] per unit time. We confirmed that the source image was legible without an averaging process from an information-theoretic standpoint. In addition, $L_2 < A_0$ is given, and in terms of processed image 2, when an averaging process is not performed, the screen image of 8 [bits] per 1 [dot] should be constructed from about 1.7 [bits]; therefore reconstruction will not be satisfactory due to the missing information. However, when an averaging process is performed, the information will be multiplied by the number of used frames. In the case of processed image 2, since eight frames were used, it is expected to increase to 1.7 × 8 [bits] and the reconstruction will be successful; however, we did not reach this result.

Analysis based on image processing

Figure 22 shows the reconstructed image of processed image 2, and Fig. 23 shows a brightness histogram of processed image 2. These show that the source image had been converted to a black and white binary image, and the processed image to a 256 gray scale-level image. In previous image reconstruction experiments, electromagnetic emanation was observed most at the point where white changes to black (or black changes to white) in an image. A Gaussian filter gives a blur effect at the changing point of white to black (or black to white) and generates gradation. Therefore, the image will gradually change, such as "white – white gray – black gray – black", rather than steeply change such as "white to black". As a result, electromagnetic emanation will become smaller and the reception level will become lower, thus the reconstruction will be more difficult. This can be confirmed from the observation results by spectrum analyzer shown in Figs. 20 and 21.

Incidentally, electromagnetic waves are emitted from the part of an image where the color information changes. For example, consider the bottom straight line of the numeric character 2. Electromagnetic waves are emitted at the point where the color changes from the white of the background to the black of the character, and will not be emitted until the color changes back to the white of the background. In other words, since electromagnetic waves are not received from the part of an image where no horizontal color change occurs, that part will not appear in the reconstructed image. Thus, screen image is already missing from the source information at the point at which it affects electromagnetic ema-



Horizontal Freq: 37.9126640KHz, 49

Vertical Freq: 60.3720000 Hz

Vert Freq Divider: 0

Low Cutoff: 5

High Cutoff: 29

Brightness: 130

Contrast: 0

112, 112, 112

Fig.22 Reconstructed image of processed image 2

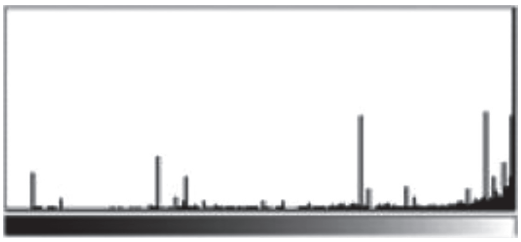
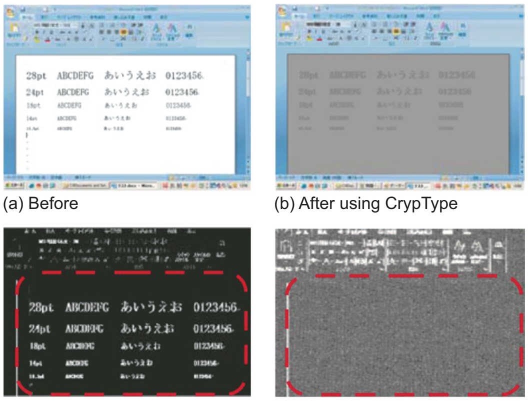


Fig.23 Histogram of processed image 2

nation. Therefore, it is not possible to reconstruct the screen image completely by accumulating and averaging A/L information only.

5 Commercialization and standardization activity

As previously described, we found that a Gaussian filter that removes the top 30% of horizontal frequency components of screen image was an effective countermeasure. When this method is applied in practice, it is necessary to store pre-processed image information. The Tempest font in the previous research[3] is one such example, and pre-processed fonts are available in some roman fonts. However, it is very difficult to create such data for the Japanese language, since there are so many different characters. In addition, as we already pointed out, reading the information of characters is not the only problem regarding information leakage. In order to solve these issues comprehensively, we developed a middleware that generates electromagnetic noise using software and performs real-time filtering. In this application, we developed a font decoration software called CrypType that is especially effective for text display[4]. This software solves the problem of losing legibility when a Gaussian filter is applied to fonts directly. We implemented it in Microsoft Office Word2007 using the OpenXML format. Figure 24 demonstrates the effect of the software. As Fig. 24 shows, it is possible to reconstruct the screen image for the unprocessed part of the Word screen by intercepting electromagnetic waves; however, no information is leaked for the processed part. In addition, since this is real-time processing, it can be used as a countermeasure against averaging process, and will be fully effective when applied to user interfaces such as touch panels. The software has been jointly developed with Beyond IT Co., Ltd., and it received the Microsoft Innovation Award[5][6].


28pt ABCDEFG あいうえお 0123456
24pt ABCDEFG あいうえお 0123456
18pt ABCDEFG あいうえお 0123456

(a) Before

(b) After using CrypType

(c) Reconstruction image of (a)

(d) Reconstruction image of (c)

Fig.24 *The demonstration of effect of CrypType*

The relevant standardization organizations for electromagnetic security is ITU-T (International Telecommunication Union Telecommunication Standardization Sector), and its recommendation X.1050. It provides specifications for information security management system which are applied to various system security management guidelines. In 2005, ITU-T SG5 (Sub Group 5) started an argument regarding electromagnetic security in telecommunications in their Question 15, and it was published as a recommendation in 2009.

- K.sec: Guide for the application of electromagnetic security requirement
- K.hemp: Application of requirements against HEMP to telecommunication systems
- K.hpem: Application of requirements against HPEM to telecommunication systems
- K.leakage: Test method and requirements against information leak through unintentional EM emission
- K.secmlti: Mitigation methods against EM security threats

K.leakage is the first international standard for information leakage. Although various documents point out the threat of information leakage via electromagnetic waves and the necessity of countermeasures, K.leakage is the almost the only standard that indicates specific technology policy. The achievement of our research has been developed in relation to the measurement methods[7]-[9] and tolerance.

6 Conclusion

This paper outlined the achievements

of research on electromagnetic security of the Security Fundamentals Group between FY2006 and FY2010. In fact, we also conducted joint research with EMC Group on measuring methods, but it is omitted due to the limits of space, and we described quantitative evaluation methods of the amount of information leakage via electromagnetic emanation, covering from the theoretical arguments to demonstration experiments.

As for electromagnetic security related activities, we conducted not only the reproduction of screen images, but also experiments in which we observed electromagnetic emanation generated by keyboard strokes to identify keys, as well as executing attacks by observing electromagnetic emanation that are generated when a SUICA is read. Moreover, as for screen image leakage, we conducted experiments by bringing in an actual ATM banking machine (Fig. 25), and we found that activities such as inputting a PIN code can be intercepted even by simple measuring equipment. Thus, there is the apparent possibility of attacks against electronic devices and infrastructures used in real life; however, considering the impact to the society, we had to be very careful in presenting our findings.

Originally it was difficult to execute Tempest against laptop PCs, but it became easier as years go by. This is partly because interception technologies have been improved, but it is also because laptop PCs became thinner and thinner every year. Especially, thinner displays do not provide enough magnetic protection, and emit larger electromagnetic emanation. One of the other reasons is that their structure was easy in accordance with price reductions. We also attempted to intercept mobile phone screens, but were not successful in this research period. This was because it was extremely difficult to find synchronous frequencies from mobile phone screens which existed around 2006. However, screen display of smart phones, which have been spreading rapidly, comply with VESA standards similar to laptops, and we are concerned that they may be easily intercepted.

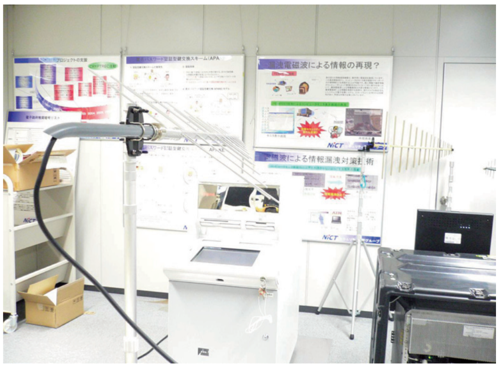


Fig.25 Experiment of ATM

This research has demonstrated academic achievements, brought the technology into commercialization, won two competitive external research funds, and has been standardized internationally: the result we have achieved in four years in a small group is extremely fruitful.

Acknowledgements

We would like to extend our gratitude to then Expert Researcher Dr. Hidenori Sekiguchi and then Short-Term Researcher Shinji Seto. While we succeeded to increase our limited budget by winning external funds such as SCOPE, it produced a lot of paperwork that distracted our research and experiments, and their vigorous cooperation was valuable in completing this work. We would also like to extend our gratitude to Mr. Tetsuya Tominaga (NTT East). Last, but not least, we would like to thank then EMC Group Leader Dr. Yamanaka, then Senior Researcher Dr. Fukunaga, and then Expert Researcher Dr. Tosaka.

References

1 H.Tanaka, "Evaluation of Information Leakage via Electromagnetic Emanation and Effectiveness of Tempest," IEICE - Transactions on Information and Systems archive Vol. E91-D Issue 5, pp. 1439–1446, May 2008.

2 M.G.Kuhn and R.J.Anderson, "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations," Information Hiding 1998, Lecture Notes in Computer Science Vol. 1525, pp. 200–210, Springer- Verlag, 1998.

3 True Type Tempest font, SearchFreeFont.com

4 Security Sangyo Shinbun(2007.9.25).

5 Monthly ASCII(2007.12).

6 Sekigutchi and Miyata, "THE DEVELOPMENT OF A TEMPEST SOFTWARE, CrypType," 2008 IEICE Technical Committee Meeting – A-7-4, Engineering Sciences Society, 2008.

7 Tosaka, Yamanaka, Fukunaga, and Hattori "An evaluation method of reconstruction of printed image by measuring disturbance from laser printer," 2008 EIC Annual Conference, S2-7, 2008.

8 Sekiguchi and Seto "Evaluation Method of information leakage for Display image Reconstructed from Electromagnetic Noise of Personal Computer," 2008 EIC Annual Conference, S2-9, 2008.

9 Suzuki, Masugi, Tajima, and Yamane, "Counter measure against Information leakage via electromagnetic emanation from PC," 2008 EIC Annual Conference, S2-8, 2008.

(Accepted June 15, 2011)

TANAKA Hidema, *Ph.D.*

Director, Security Fundamentals Laboratory, Network Security Research Institute

Information Security, Cryptographic Technology, Information Theory