

ECOM News

Headline

- The Fifth Planning Committee Meeting for FY 2006
- “Eighteenth ECOM Seminar” Lecture Outline
 - Measures for Promoting RFID Tags and Their Possible Utilization-
- “Nineteenth ECOM Seminar” Lecture Outline
 - Special Seminar in Commemoration of the First “Information Security Day” –
- Announcement of the “21st ECOM Seminar”
 - Recent Trends in Overseas E-Commerce-

The Fifth Planning Committee Meeting for FY 2006

—Drawing up the Activity Plan (Draft) for FY 2007—

The Fifth Planning Committee Meeting - February 23, 2007

At the meeting, Masahiko Fujihara, Information Economy Division Director of the Commerce and Information Policy Bureau at Ministry of Economy, Trade and Industry reported on the current status of the initiative for new RFID tags and e-commerce. We also had discussions about the activity plan (draft) for FY 2007 proposed by the secretariat and activity themes proposed by members.

1. Status Report on the Initiative for New RFID Tags and E-Commerce

We had a report on the results of interviews conducted in industries (regarding the current status and problems of EDI and RFID tags), common problems, and strategies for the future with regard to the initiative for new RFID tags and e-commerce.

2. Activity Plan for FY 2007

(1) Activity themes and plans proposed by the secretariat

An overall summary of activities conducted by the Special Committee regarding RFID Tags and Traceability was given, and proposals were made concerning new projects of the committee such as work-related training and sensor networks.

(2) Activity themes proposed by member companies

Member companies made proposals concerning RFID tags, sensor networks, information security, and the utilization of IT (Web 2.0), and the proposals were explained in detail.

(3) The secretariat will make necessary adjustments by the next committee meeting.

3. Summary of the Activity Report for FY 2006

We explained the initial activity plan drawn up at the beginning of the fiscal year and the results of activities expected at the end of the year.

4. Schedule for the Future

The sixth committee meeting is scheduled for March 20 to hear an activity report (draft) for FY

2006, prepare a financial statement (predicted results) for FY 2006, and discuss the activity plan (draft) and budget (draft) for FY 2007.

Plans were made to finalize the activity plan and budget for FY 2007 at the meeting of the Board of Directors held on March 29.

“Eighteenth ECOM Seminar” Lecture Outline

–Measures for Promoting RFID Tags and Their Possible Utilization–

On Thursday, February 1, 2007, we held a monthly ECOM seminar on the theme shown under the title above in Kikai Shinko Kaikan Building (3-5-8, Shibaura Koen, Minato-ku, Tokyo). A total of 160 participants attended the seminar, including ECOM members and other visitors.

At the seminar, we had a report on the program launched by the Ministry of Economy, Trade and Industry with an aim of creating infrastructures that allow RFID cards to be used across companies, industries, and countries. We also had other reports on projects for lowering the price of RFID tags, developing new technologies, creating international standards, and promoting field trials. We handed out “ECOM RFID tag admission tickets” to participants. These tickets are being developed in the ECOM field trial program.

◆ Lecture 1

“Measures of the Ministry of Economy, Trade and Industry for Promoting RFID Tags”

Masahiko Fujihara
Director
Information Economy Division
Commerce and Information Policy Bureau
Ministry of Economy, Trade and Industry

[Project for Promoting RFID Tags]

The effective utilization of RFID tags is expected to improve efficiency and create new services in user industries in Japan, as well as help maintain and improve the global competitiveness of these industries. RFID tags have the following characteristics as compared with bar codes: (1) The tags can contain large quantities of information; (2) The tags are writable; (3) Information in the box can also be read; and (4) The tags allow users to identify a number of products at one time from a distance. How widely are RFID tags currently used? RFID tags are mostly used for practical purposes in closed fields within industries where the tags can be recycled, and not in open fields across companies where the tags could be treated as disposable items. Therefore, it is essential to promote RFID tags in transactions between companies, and METI has undertaken projects for “creating international standards” for RFID tags, “reducing the price (Hibiki Project)” and “promoting field trials in industries.”

• Creating International standards

Since Japan adopts a free trade system

and many Japanese companies are engaged in international business, we need to create international standards for RFID tags. Important elements of the international standards for RFID tags are the “product code” and “communication protocol.” METI submitted a proposal to ISO for using a unified “product code”, and it was approved at an ISO meeting in March 2006. And since there were different standards for the “communication protocol” used for UHF-band RFID tags, METI and user industries around the world called for the unification of standards, and in 2006 unified international standards were finally adopted.

• Reducing the Price (Hibiki Project)

The goal of this project was to lower the price of UHF-band RFID tags, which range from several tens to several hundreds of yen a piece down to five yen a piece. To develop a five-yen inlet (a device consisting of an IC chip and antenna) and an IC chip for the reader/writer, we developed technologies for manufacturing low-cost antennas, low-cost installation, and downsizing a UHF-band IC chip that meets international standards. As a result, we were able to achieve our goal in two years from August 2004 to July 2006.

• Field Trials in Industries

In 2003, four industries participated in field trials to use UHF-band RFID tags. In 2004, seven industries participated in trials to use RFID tags in supply chains across companies, followed by trials conducted in 2005 on using RFID tags in actual business processes in a number of industries and

calculating the return on investment. In the RFID tag project for 2006, we “developed an RFID tag system that meets the need for security,” and conducted “field trials to create international standards” and “field trials to check how to use multi-codes and tags.”

[Current Status and Problems of RFID Tags and E-Commerce]

To meet the challenges facing economic society in Japan (such as radically improving productivity using IT, developing measures for environmental problems such as global warming, recycling products and controlling chemical substances, and ensuring product safety), efforts are needed to share information across boundaries between existing industries and businesses. IT development in recent years has achieved valuable results for these efforts. There is an urgent need for industries to create a system for sharing data that will serve as a “new social infrastructure for the information economy.”

The main purposes of the “new social infrastructure for the information economy” are: (1) To use infrastructures for next-generation e-commerce through RFID tags and the Internet to share information and create a linkage between systems inside and outside companies, and (2) To create a system that provides the benefits of sharing information to a wide range of companies by promoting projects jointly conducted by companies across related industries rather than by individual companies. We will develop the “Initiative for New RFID Tags and E-Commerce” to create these new infrastructures. To achieve our purposes, we are comparing notes with business leaders to examine project plans for the “new social infrastructure for the information economy,” developing tools for using systems across industries (creating standards, developing technologies, and conducting trials), drawing up “guidelines” to promote collaboration between businesses and industries, creating organizations for new projects, and developing environments for encouraging small- and mid-sized companies to participate.



Lecture

◆ Lecture 2

“Examples of Using and Introducing RFID Tags”

Masatomo Takemoto
Research Director
Next Generation
Electronic Commerce Promotion
Council of Japan

RFID tags are now beginning to be used for practical purposes within companies and organizations. Nevertheless, the tags are rarely used for supply chains across different companies and industries. To promote the use of RFID tags, we need to solve specific problems: (1) RFID tags are expensive; (2) There are no international standards for these tags; (3) The issue of privacy may arise in the future. Moreover, no unified rules regarding RFID tags will become established unless collaborative efforts are made across all industries to create rules; (4) ECOM organized working groups to find answers to these problems.

[Field Trials in Industries]

In 2003 we conducted field trials in four user industries to use RFID tags for practical purposes. These trials demonstrated that UHF-band RFID tags perform superbly under certain conditions in terms of read distance, diffraction, and read accuracy.

In 2004 we used RFID tags to promote restructuring in seven industries. The

department industry and apparel industry started using RFID tags immediately after the trial. Based on the results of this trial, we conducted cross-sectional analyses of the background and purposes of using RFID tags, the specifications of RFID tag systems, and methods of operating tag systems in production, distribution, and sales. The ECOM Report for 2005 summarizes the analysis results. The specifications of RFID tags used in trials conducted in 2004 differed from one industry to another. Accordingly, there is a need to establish standards across industries and make rules about how to enforce these standards. Our trials have achieved some results, including saving labor for receiving deliveries, shortening the time for product inspection, and increasing sales by preventing lost sales opportunities. As a result, RFID tags were recognized as an efficient technology for creating a smooth flow of products that leads to an overall optimization of business, and a means of maximizing efficiency in economic and business activities.

In 2005, field trials with RFID tags were conducted to achieve four goals. One goal was to improve the read rate, which requires a good environment for the reader. We examined how to make it easier to read RFID tags in order to improve the reliability of reading RFID tags. We also tried various methods to improve the read rate. For example, in the electronics industry, we worked out a method of reliably reading the tag of a product placed on a worktable without changing the flow of operations. In the automotive parts industry, we devised a method of reading tags when the operation slows down. In the copy machine industry, we employed a method of reading tags for film cases as stretched film was being wound on a drum. Moreover, we also devised methods of reading a number of tags at one time.

It will be necessary in the future to use tags with different frequency bands as well as bar codes all at the same time in the management of distribution and other processes. In that case, we will encounter compatibility problems between different makers and frequencies. To use these

different systems simultaneously, it is essential to develop middleware, and for that reason we plan to conduct global trials in various areas including the ASEAN region for the project in 2006 with the aim of creating international standards for middleware.

[\[ECOM Voluntary Project for 2006](#)

[“Trial with RFID Tags,” Outline of the Seminar Attendance Management System\]](#)

We planned this project to conduct an trial by ECOM using an application that allows everyone to enjoy the benefits of RFID tags together. The trial was conducted as follows: At the reception desk, the receptionist checked the name of each visitor on the PC screen, and passed each person's attendance card (RFID tag) over the reader/writer to establish a link between the reception number and RFID tag. This procedure makes it possible to keep track of the comings and goings of visitors with attendance cards by using the reader/writer installed at the entrance of the seminar hall. While our trial was conducted for a free seminar this time, the seminar attendance management system using RFID tags may also be used for checking billing at the entrance and the leaving of visitors at pay seminars.



Attendance card (RFID tag) being handed out

◆ Lecture 3

“Projects for Utilizing RFID Tags”

Kazuhiko Wakaizumi

[Using RFID Tags Across Borders]

Contemporary Japan depends greatly on trade. Therefore, RFID tags must be developed so that tags from Japan can be read overseas and tags from overseas can be read in Japan.

[Two Aspects of RFID Tags]

RFID tags are characterized as a medium that stores the identifier of a product and as a data carrier that stores product information other than such identifier. C1G2 is a standard that unifies these two aspects, and provides for UII (identifier) and user memory.

[Development of RFID Tag Infrastructure]

An identifier identifies a product as a unique entity in the world. The ISO/IEC 15459 series was developed to identify a product despite differences in code systems. Japan has made proposals about Part 4: Individual items and Part 6: Product groupings (product groups, lots, and batches). Part 4 has already been approved and Part 6 is awaiting a final vote.

[Development of Application Standards]

A joint working group for ISO/TC104 and ISO/TC122 is engaged in defining five standards about the "usage" of RFID tags. Four of the five standards other than ISO17363 support ISO/IEC 18000-6TypeC (UHF) and/or 18000-3Mode3 (13.56 MHz).

[Effective Use of User Memory]

Results of a questionnaire survey on users conducted by EPC Global and attempts by companies to store information other than product IDs in RFID tags in past trials both suggest that there is a compelling need for user memory. ISO/IEC JTC1/SC31/WG2 define ISO/IEC15434 to store data in user memory in a format compatible with EDI.

[Varieties of RFID Tags and Development of a Unified Interface]

Due to differences in characteristics between products and in such circumstances as laws governing radio use between countries and areas, RFID tags with different

specifications may be used for different types of products. To reduce the burden that these differences may impose on applications, we are examining the possibility of standardizing specifications for middleware, so that information on an RFID tag can be transmitted via a unified interface to applications using different air interfaces (including frequencies).

[RFID Tags and Privacy]

When RFID tags become widely used and readers/writers readily available in the future, some unethical people may attempt to read the IDs of other people's belongings without the owner's consent or obtain personal information about the owners from stolen IDs, and thus violate privacy. Definitions of privacy vary depending on the values held by individuals. We also need to respect other cultures and religions when using RFID tags for international purposes.

Products with RFID tags provide a useful system for the caretakers of those who need protection such as children. However, those who believe they have the "right" to act anonymously may consider these tags an invasion of privacy. Technologies expected to provide important tools for protecting privacy are being developed, such as functions for stopping certain RFID tag actions in a reversible way.

◆ Lecture 4

"Outline of Project for Developing UHF-Band RFID Tag Technologies"

Atsushi Honzawa
Senior Engineer
Products Operation
Tracing & Tracking Systems Division
Hitachi, Ltd.

[Outline of the Secure RFID Tag Project]

The Secure RFID Tag Project is being conducted to address the needs and challenges of user industries in field trials. Based on ISO-18000-6TypeC, we are working to provide supplementary functions needed for secure tags. To provide these supplementary functions, we are: (1) developing a tag IC chip that has a function to

protect privacy and business information, and (2) examining and testing methods of operating a secure RFID tag system (measures for plugging security holes). We have manufactured IC chips for trials and are assessing their system applicability in three industries.

[\[Protocol Specifications of Secure RFID Tags\]](#)

The IC chips currently used for tags become unusable for secondary distribution or maintenance once a kill command (which invalidates tags) is executed or tag data deleted. To overcome this drawback and develop technologies for protecting privacy, we studied how to prohibit the reading of a tag or limit the communication distance when the tag is handed out to a consumer, and then restore it to the original state upon entry of a password by an authorized user. We were able to prohibit writing to the user bank in tag memory, but unable to prohibit writing to or reading from specific areas within the user bank. To resolve this problem and protect business information, we developed a method of dividing a user bank into a number of areas so as to prohibit reading and writing in each area. This method allows us to set two different types of prohibition: permanent prohibition and temporary prohibition that can be lifted by using a password.

[\[Outline of the Secure RFID Tag System\]](#)

When RFID tags become usable across the entire life cycles of products, tag passwords may be stolen, allowing unauthorized access to the information, tampering with RFID tag data, or unauthorized copying of the data.

To address these problems, we have examined and developed a system to evaluate secure RFID tags. We are now using this system to evaluate RFID tags in certain industries such as the publishing and consumer electronics.

RFID tags are typically protected by passwords these days. However, if a common password is used throughout an industry, and subsequently exposed, a wrongdoer may tamper with or invalidate the information of many tags by using the same password. For this reason, it was necessary to use different passwords for different tags in

our project to minimize risk. Based on the model of security management employed in an industry that plays a leading role in introducing RFID tags, we examined the specifications and methods of mounting RFID tags, mounted a security module for generating passwords on terminal devices, and managed to create a secure and efficient RFID tag system that can be accessed only by authorized users.

[\[Evaluation of System Applicability\]](#)

The system applicability of "IC chips for secure RFID tags" and the "secure RFID tag system" developed in our project is being evaluated in three industries. To test our system, we assumed different players (manufacture, distribution, sales, maintenance and recycling) and different data sets for different industries. Based on these assumptions, we examined the operating procedures for tag memory developed in our project (functions for protecting privacy and business information). To evaluate the functions and performance of our system, we used the secure RFID tag system under circumstances pertaining to each industry for managing tags equipped with newly developed functions.

[\[Example: Application for Protecting Privacy and Business Information in the Publishing Industry\]](#)

To respond to the publishing industry's need to limit consumer access to RFID tag information without preventing used book stores and libraries from reading sales information and check-out information, we developed methods of prohibiting the reading of specific parts of information and preventing unauthorized access from a long distance by reducing the communication distance allowed for tags. To meet the need to check whether a book can be returned (and prohibiting tampering with return information), we devised a means of dividing the user area of an RFID tag and developed technology to prohibit writing to each segment of the area and lift that prohibition by using a password. Using these applications, we are working to evaluate our developed technologies to protect privacy and business information.

◆ Lecture 5

“Outline of Project for Establishing International standards”

Takeo Seraku
RFID Consulting Team
Next Generation
Infrastructure Research Group
Mitsubishi Research Institute, Inc.

[Outline of the Project]

We conducted three sets of trials in Southeast Asian countries on RFID tags that require international collaboration: Lane 1 (BtoG), Lane 2 (BtoB), and Lane 3 (BtoC). To “make Japan’s presence known in the RFID tag business” among Asian countries, we organized several workshops in the field and presented the results of trials conducted on RFID tags in Japan, examples of application, and projects concerning RFID international standards.

[Lane 1]

We conducted trials to study the efficiency of checks on imported products made by SIRIM (Standard and Industrial Research Institute of Malaysia) for import and export control, with the aim of improving efficiency in the procedures for product certification. Our trials were conducted using telephone devices. We sealed containers with RFID seals and sent data about the content separately to simplify procedures for checking the content of containers. More specifically, we exported products from Japan to Malaysia using containers sealed with RFID seals and sent information to SIRIM regarding the names and quantities of products declared when exported from Japan. By using the information received, SIRIM was able to reduce the number of processes required to check the content of containers stored in warehouses. As a result, the time required for import procedures was reduced by up to three days. In our trials, RFID seals were used for checking the content of containers against the information received. We used dummy RFID seals along with normal seals to confirm proper functioning.

[Lane 2]

The goals of our trials in Lane 2 were threefold: To improve the efficiency in international distribution, check the international standards for applications, and test the performance of Hibiki chips (μ -Chip Hibiki). We conducted trials in the trade lanes (between warehouses) used for international distribution from the country to Japan, and affixed Hibiki chips to packages and package layers to check the effectiveness of Hibiki chips in distribution processes and test chip performance. We also checked some guidelines of the Home Appliance Industry Consortium in our trials using home fax machines. To improve the level of distribution service, we examined how to avoid errors by using shipment information. As for distribution operation service, we studied on destination information management of each pallet and tag management of recycled pallets. We examined such technical questions as how read accuracy is affected by the position of tags and antennas, and the relation between the durability of Hibiki tags and the location of pallets within a container. We also examined how to use tags for improving the efficiency of the packing process.

[Lane 3]

We conducted field trials in electric appliance stores in Thailand, Malaysia, and Singapore to increase over-the-counter marketing accuracy and advertise RFID tags made in Japan. We used such products as plasma display TVs, washing machines, and refrigerators in our trials. In the sales promotion field trial, we read RFID tags affixed to products and advertisement panels for products using a mobile information terminal with a tag reader (or monitor terminal) to display product information on a monitor terminal screen. We kept logs of the RFID tags on a PC used for tag management and analyzed these logs to show that the information can be used as survey data for understanding market trends and consumer preferences.

[Designing and Development of RFID Middleware]

ISO initiated discussions about international standards for middleware last

year. To make these standards suitable for the functions and performance required by Japanese industries to make efficient use of RFID tags, Japan is drafting the specifications for middleware and developing software to check the functions and performance of RFID applications. Since the current data description method to user memory is not suited for handling large quantities of data at high speed in manufacturing and distribution processes, Japan is proposing the addition of a more flexible method (profiling method) of reading and writing to the list of existing methods.

◆ Lecture 6

Outline of “Project for Interoperable Operation of Multi-Code Systems”

Yutaka Ukon
Senior Resercher
Advanced Technology
Nihon Unisys, Ltd.

[Platform for Interoperable Operation of Multi-Code Systems]

A multi-code system consists of a number of identification codes, such as EPC, ucode, proprietary codes, and new standard codes that will be created in the future.

The existence of multiple codes is one factor hindering the promotion of RFID tags, since it makes companies hesitant to use RFID tags in not knowing which code system to choose. To overcome this drawback, we developed a “system platform for interoperable operation of multi-codes” that automatically sorts out EPC, ucode, and unique codes. We conducted field trials using the platform. The API (application program interface) of the platform enables the user to operate applications regardless of the code system employed. We also conducted trials to demonstrate possible multi-code system operation in an interoperable way, and assured companies that the code system adopted at the outset does not impose any restrictions on subsequent expansion or interoperable operation of the system.

The distribution of goods and identification

of persons and locations are expected applications of this platform for interoperable operation of multi-code systems. For example, there is a need to read multiple codes at retail stores to deal with goods that were source-tagged in production lines. In areas related to traceability, we also need to use a multi-code system to identify vehicles and parts, and keep replacement records for the regular maintenance of vehicles and aircraft. When identification codes become widely used for goods and locations in the future, in order to create code-free applications for managing the relation between these goods and locations, multi-code systems will be required as infrastructures in ubiquitous society. By operating multi-code systems in an interoperable way, we will be allowed to disregard code differences between applications and eliminate the need to change the keys of a database when linking to a different code system.

A multi-code identifier (MCI) is a code to identify code systems. This is a variable length code, but only the 8-bit code was tested in our trials. Since MCI a variable length code, it can be used to identify a large number of any code system that may be created in the future. To distinguish code systems in our trials, we employed a method of identifying a code system upon entering an information system space. There are many methods of identifying a code system at the entrance of an information system space, such as identification using readers, frequencies, and instructions via the API.

The API used for the platform has functions for reporting events, requesting event information, and requesting information from the information server.

[Open Field Trials]

In our open field trials (ORF and TRONSHOW), we displayed information on different areas (how many people of what business are in which area) and distributed the information via e-mail to cell phones (by providing information relevant to each area for cell phones). We asked each participant in the field trial to choose either ucode, EPC, or a unique code at the time of application,

and handed out RFID tags on the day of the field trial. The purpose of the trial was to demonstrate that by using our platform for the interoperable operation of multi-code systems, we could provide e-mail service for users who use different codes.

We installed 10 tag readers and used UHF bands to conduct the ORF open trial. We disclosed the API to the public and wrote additional applications required for the field trial, such as programs for locating persons and drawing distribution maps. We used HF

bands to conduct the TRONSHOW open trial and demonstrated that it is possible to communicate with ubiquitous communicators (UC) using multi-code. We also organized a point rally and used the event database to check whether participants visited 20 different places.

We need to achieve a consensus and adopt a basic policy about the methods that we used in our trials (especially regarding MCI).

“Nineteenth ECOM Seminar” Lecture Outline

- Special Seminar in Commemoration of the First “Information Security Day” -

On Tuesday, February 6, 2007, we held a monthly ECOM seminar at Kikai Shinko Kaikan (3-5-8, Shiba Koen, Minato-ku, Tokyo) in commemoration of the first “information security day” (February 2) established this year. We had a total of 144 participants, including members of ECOM and supporting organizations, and other visitors.

At this seminar the lecturers spoke about information security policies and measures aimed at creating a safe and secure environment for e-commerce, projects conceived from the perspective of users, and security measures to be adopted by companies and organizations.

Session 1 Information Security Policies And Measures

◆ Lecture

“Trends in Information Security Policies in Japan”

Hideki Kanai
Assistant Director
Office of IT Security Policy
Commerce and Information Policy Bureau
Ministry of Economy, Trade and Industry

[Rapid Development of IT and New Threats]

The rapid development of IT poses new threats to security. Unlike the case of using regular dedicated lines, it is totally unpredictable to whom we are connected through the Internet. The Internet extends across organizations, borders, and time, linking us to people with good intentions as well as those with bad intentions. And because the Internet is faceless, we are also confronted with an ever-increasing number of problems, such as tampering with information, spoofing, attacks, and invasion from outside.

[Unified and Cross-Sectional Promotion System for Safety Measures Implemented by the Japanese Government]

In February of last year, the Information Security Policy Council drew up the “First Master Plan for Information Security.” This three-year medium- to long-term plan outlines a basic strategy for the future. We also formulated “Secure Japan 2006” as an annual plan for 2006 to (1) “create a system for implementing security measures in the

government and private sector” (133 measures) and (2) “improve the level of security management in the government and private sector” (26 measures).

[Changing Threats to Information Security and Measures Implemented by METI]

The Ministry of Economy, Trade and Industry created a system in the 1990s for reporting computer viruses and unauthorized access, conducted fixed-point observation of the Internet in 2000, and in 2003 developed a vigilance system. The reported number of security holes in vigilance partnerships totaled 1,178 (as of January 12, 2007), which suggests that the system helps curtail security problems. Given the increasing number of bot attacks that have become more sophisticated and dangerous in recent years, METI has launched a project to provide information about countermeasures against bots in collaboration with related organizations.

[Promotion of Organizational Measures]

Among the major causes of attacks and accidents that threaten information security are such internal factors as system operation and management problems, and the leakage and infringement of information from inside. Therefore, it is essential to take organizational measures to ensure security in addition to technological measures. More specifically, we are promoting the following measures: (1) Implementing information security management systems, (2) Implementing information security monitoring systems, and (3) Establishing information security governance. We are also planning to provide “System Management Standards:

Supplementary Version (Guidance on IT Control Concerning Financial Reports)” for companies using “System Management Standards” to offer practical guidance on introducing IT control concerning financial reports.

[Promotion of Technological Measures]

To help create a safe and secure IT society, we need to encourage the wider use of safe IT products in our society, create infrastructures for more advanced electronic authentication systems, and promote research and development to support these infrastructures. To achieve these goals, we are promoting development of the following: (1) Systems for third-party evaluation and certification of information security technologies (such as IT products, encryption technologies, encryption modules, and information systems), (2) Research and development related to information security technologies, and (3) Infrastructures for electronic authentication systems that authenticate users and information by electronic means (with field trials conducted on cross-sectional infrastructures for next-generation authentication systems).

◆ Lecture

“Development of a Vigilance System for Computer Security: Bots Prevention Project”

Takayoshi Shiigi
Senior Analyst
Coordination Center
JPCERT

[What is a Botnet?]

A botnet is a network created by viruses called bots. Unlike ordinary viruses and worms, bots can be controlled and managed remotely (via IRC and P2P), and are provided with a number of their own functions, such as contagion (finding security holes, hijacking, and social engineering), collecting information (including account information), attack (DDoS attack), and self-defense (such as encryption). A bot launches a range of operations such as DDoS attack and spam mail from large number of infected PCs under

the direction of one person. Since many source programs for bots are released to the public, there are millions of bot subspecies. They “hide” in PCs to continue operating in a stable environment. Unlike other viruses, botnets are bought and sold as self-functioning systems.

[Changing Threats]

As assets on the Internet increase in value and more people begin using the network, more threats are being targeted at real society. While the techniques used for invasion and contagion, such as attacks on known security holes and social engineering, have not changed in most cases, these techniques are being combined and used in a more sophisticated manner. Moreover, in various situations, many recent viruses employ techniques for hiding, encryption, and obfuscation. These viruses are able to detect debuggers and virtual environments, and obstruct the operation and updating of anti-virus software.

[Programs by JPCERT/CC]

Under current circumstances, the costs and risks involved in virus attack are low while the values of assets and profits obtained are high. JPCERT/CC is therefore implementing programs that forces attackers to face an increase in the costs and risks, and a decrease in the values and profits through such measures as incident responses, the distribution of information on security holes, and analysis of malware.

[Bot Prevention Project]

The Bot Prevention Project being jointly conducted by the Ministry of Internal Affairs and Communications (MIC) and METI is aimed at developing measures for protecting against bot infection, eliminating bots, and minimizing their damage (by circulating information about bot prevention, issuing warnings, conducting surveys and analyses of bot programs, developing preventive measures, improving measures against bot infection, and preventing recurrence). Cyber Clean Center (<https://www.ccc.go.jp/>) was created as the portal site for the Bot Prevention Project. JPCERT/CC serves as the bot program analysis group that

examines bot viruses, analyzes the characteristics of bot programs, studies methods of analysis, and develops and provides tools for eliminating bots.

◆ Lecture

Security Evaluation and the Benchmark for Information Security Management

Yasuko Kanno
Chief Advisor
IT Security Center
ISEC

The IT Security Center of Japan's Information-Technology Promotion Agency (IPA) is developing various security measures, such as protection against security holes, viruses, and unauthorized access, as well as evaluating and certifying security and studying encryption technology.

[Viewpoints and Methods of Security Evaluation]

IPA provides a number of security evaluation tests. Some of these tests evaluate the state of security management in an organization (such as through ISMS adequacy level evaluation, information security audits, and benchmarks for information security management), while other tests evaluate security products (using the IT security evaluation and certification system, and encryption module testing and certification). These tests are intended to: (1) check the level of security management implemented in a company and the effectiveness of security measures adopted, (2) provide explanations about security measures implemented in the company, (3) check the level of security management implemented by subcontractors and subsidiary companies, and (4) check whether security products provide necessary security functions.

[Benchmark for Information Security Management]

* <http://www.ipa.go.jp/security/benchmark/index.html>

METI proposed the Benchmark for Information Security Management in the

“Study Report on Information Security Governance in Companies” as one of the tools for promoting information security governance in companies. IPA developed this self-diagnosis tool that can be used on a Web page, and has provided it since August 2005. A diagnosis given by this tool can be used to check a company's level of security management and that of its subcontractors as well.

To obtain a diagnosis of a company's security management and provide advice about security measures, the user answers a total of 40 questions on the IPA website (25 questions about information security management by the user's company in Part 1, and 15 questions about the company profile in Part 2). Based on answers to the 15 questions in Part 2, the company is categorized as belonging to one of the following groups: (1) Companies that must maintain a high level of security, (2) Companies that must maintain a normal level of security, or (3) Companies for which there is no urgent need to implement security management. A desired level of security is given for each group to provide companies with a benchmark for examining security measures suited to their particular level in order to optimize security costs.

The 25 questions in Part 1 are based on detailed guidelines (127 items) prescribed in the ISMS Certification Standards, Version 2.0. Answers to these questions are used to calculate the total score for a company's security management, along with radar charts showing differences from the desired level of security, the average levels of other companies in the same group, and average levels of other companies in the same industry. The desired security level is calculated based on the empirical data of thousands of companies. Companies are recommended to use this tool for self-diagnosis and improve their levels of information security management.

Session 2 New Risks for Users

◆ Lecture

"Information Security Risks Revealed by User Trouble"

Yuri Harada
Director
EC Network

EC Network is a private organization established in April 2006 to create an "e-commerce market that consumers can trust and use without trouble" based on the results of trials conducted by the ECOM Net Shopping Dispute Consulting Office. EC Network provides consulting, mediation (ADR: alternative dispute resolution), and information services for members with regard to their e-commerce transactions. In August of last year, it also began to play a part in an international relation project of METI for settling disputes with overseas transaction partners.

[Cases of Disputes]

Case 1: Credit card charges for shopping and auction entries by total strangers

We have many cases of trouble regarding "credit card charges for shopping by strangers." Circumstances differ depending on certain characteristics of the victims, such as whether they have families, the products purchased, and the settings of service sites.

Case 2: Unauthorized use of credit cards

Under current rules, credit card charges for spoofing shopping can basically be billed to the member store of the credit company and settled the following month.

Case 3: Security software and lottery tickets purchased on overseas websites

Policies regarding the cancellation of credit card charges and refunding for high-pressure sales of security software differ between credit card companies. Whether the loss can be recovered differs from one case to another.

Case 4: Spyware on adult sites

Properly updated security software will normally give a warning about spyware on adult sites used in "one-click fraud." Those failing to take proper precautions for security will likely be victimized.

Case 5: Mail addresses disclosed by being

misplaced in the CC or e-mail destination entry

We have had cases where companies misplaced the mail addresses of customers in the CC or e-mail destination entry instead of BCC when sending mail messages to a large number of customers. As a result, customers who sent return mail had their interest and concerns disclosed to a large number of other customers. While it is certainly true that consumers need to exercise due caution in sending e-mail, companies also need to adopt appropriate measures to avoid these careless errors, such as using special mail software for business purposes.

[Recent Trouble]

Business models like affiliate shopping and drop shipping that provide individuals with the opportunity to earn income over the Internet are attracting the attention of many users. We will be required to make increasingly difficult judgments as to what form of protection should be provided for consumers in the future. While fewer acts of fraudulent auctions are occurring thanks to the introduction of more advanced methods of authentication and the mandatory escrow system, a growing number of fraudulent acts are being committed in transactions other than auctions. We have seen cases where users, upon reading a bulletin board, agreed to put goods up or provide a bank account for an auction, and were made to participate in fraud. There is also a need to improve the level of morality among consumers.

◆ Lecture

"Sophisticated Phishing Frauds"

Futoshi Nakata
Manager
Information Collection/ Provision WG
Antiphishing Japan
(SecureBrain Corporation)

[Examples of Phishing]

In November 2004, a Japanese phishing site disguised as the site of a major credit

card company appeared on the Internet, claiming phishing victims for the first time in Japan. There were 37 cases of illegal cash withdrawals made via Internet banking last year (from April 2005 through March 2006), resulting in damage totaling 30 million yen.*¹ Around October of last year, a man who created a fraudulent website to illegally obtain bank account passwords was detected and arrested by members of the Metropolitan Police Department's High-Tech Crime Prevention Center. A fraud group whose members included students and even housewives was subsequently uncovered. A 14-year old boy who studied phishing techniques all on his own and sent phishing mail to members of an Internet game to obtain their IDs and passwords was caught by the police and reported to the Public Prosecutors Office.

[Techniques Used in Phishing Fraud]

Phishing refers to the act of stealing personal information by impersonating a credible organization such as a financial institution (like a bank or credit card company). Phishers disguise themselves as representing real companies and send e-mail or create fake home pages for fraudulent purposes. It is very difficult to see through their disguises at first glance. Various techniques are used for phishing. These include placing a fraudulent website address in an innocent-looking e-mail message, attaching a faked address bar to a copy of the home page of a credible organization, and hacking a server with security holes to create a phishing site or use it to send phishing mail. One technique known as "cross-site scripting" conducts phishing via the credible websites of other people. Malicious code and spyware are also used to obtain personal information.

[A Recent Incident and Measures to Be Adopted for the Future]

In July of last year, a phishing scam committed by using techniques for "man-in-the-middle attack" was exposed in a major bank in the United States. These techniques provide the means of committing phishing fraud even where one-time passwords—considered a means to ensure security—are used. Phishers use a variety

of sophisticated techniques to deceive consumers, which makes it difficult to prevent phishing scams. Websites that are exploited by phishing and must be closed are often hosted in countries not associated with the companies running these websites. Thus, it is not always easy to obtain a complete picture of phishing organizations. For these reasons, we must work in collaboration with police organizations to provide effective countermeasures.

*1: Results of a questionnaire survey on "illegal cash withdrawals via Internet banking" by the Japanese Bankers Association

◆ Lecture

"Current Status of Spyware"

Koji Nonoshita
WG Leader
Antispyware Promotion WG
NPO Japan Network Security Association
(Webroot Software K.K.)

[Changes in the Motivation of Attackers]

In the past some computer engineers and experts conducted attacks on computers out of interest or for fame. Nowadays, in contrast, many attackers and criminals (including amateur hackers and script kiddies) form groups and use tools developed by experts to illegally obtain personal profits. Spyware is often used as a tool in these attacks.

[Spyware Business]

The short history of spyware dates back to 1999, when Dash.com began providing a tool bar called "dashBar." This was initially adware for marketing via the Internet for the purpose of collecting information about users. However, many spyware vendors followed in its wake. Today's spyware business accounts for 11% of advertising business on the Internet, with total sales of this business believed to amount to 2 billion dollars. A large number of people are involved in the business, including the providers of products and services, adware vendors, owners of websites, and advertisers. The system is complex, but these people all work in

collaboration. For example, unidentified affiliators who help users install software using whatever means available are paid money for their installation services.

[Current Status of Spyware]

According to a survey conducted by Webroot in December of last year using "Spy Audit" (a free spyware detection tool), the top 10 spyware applications in the adware sector included SystemDoctor 2006 (second place) and DriveCleaner (third place). These applications start scanning your computer the moment you click a button such as "free." Both display a message stating that your computer has a serious infection, thus prompting you to install security software with the price charged to your credit card. Messages used to be displayed in English, but in recent years are being replaced by Japanese.

In the Trojan horse category, Trojan-Downloader-Zlog was tops followed Trojan Hachilem. Both applications are distributed as movie codec. The former downloads malware on your PC, while the latter is "one-click ware" that charges you a registration fee for an adult site.

[What's Happening?]

The spyware business is becoming a global business. Sites that look like Japanese sites often originate in countries other than Japan. Security applications sold by fraudulent high-pressure sales techniques are obviously developed overseas with Japan as the target. Most Trojan horses targeted at the accounts of Japanese gamers are hosted on overseas websites in China, Taiwan, and other countries. These applications use sophisticated techniques and disguise themselves as ordinary software applications. Moreover, many subspecies are posted as advertisements, bulletin boards, or blogs, and hidden on innocent-looking sites, making it difficult to detect using anti-virus tools. Therefore, precautions need to be taken even when installing security software.

Session 3 Projects in Companies and Organizations (1: Organizational Measures)

◆ Lecture

"Importance of Information Security Management"

Masahiro Hoshi
Senior Researcher
Assessment Group
ISMS Promotion Office
IT Management Center
JIPDEC

[Outline of the Information Security Management System (ISMS)]

Since information provides a foundation for organizational activities, properly protecting it is essential. A security problem or accident causes great damage to an entire company or organization. Therefore, we need to consider information security as a problem related to the management (administration) of a company or organization as a whole. The information security management system provides an effective means of solving this problem.

The Information Security Management System (ISMS) is an effective method to implement information security management. It provides technological measures designed to solve specific security problems, as well as a means of determining the level of security required for organizational management based on a self-assessment of risks. This system helps develop a security management plan and allocate resources for managing an organization. The basic purpose of ISMS is to ensure security for information assets that must be protected while maintaining a proper balance between the confidentiality, integrity, and availability of that information. ISMS evaluates the effectiveness of management measures adopted following risk management.

[Advantages of Development and Operation ISMS]

ISMS development and operation offer the following advantages: (1) It helps create a comprehensive security system for the

management and administration of technological and human resources by improving the skills of employees, clarifying responsibilities, providing emergency measures, and by improving general abilities, (2) It provides efficient security measures such as a cost-efficient system for managing assets based on a comprehensive standpoint, and forms a solid foundation for risk management. ISMS certification will help a company gain public confidence in its information security system, and improve its business competitiveness by qualifying for projects that require certification.

[\[Outline of the ISMS Conformity Assessment System\]](#)

The ISMS Adequacy Level Evaluation System is a third-party certification system for management that meets international standards for information security. It is based on JIS

Q27001 (equivalent to international standard ISO/IEC 27001). The system is designed to improve the overall level of information security in Japan, and also achieve a level of information security that meets international standards and gains the trust of other countries. ISMS standards (Version 2.0) that have been effective since 2003 will be abolished in November of this year, so there is a need to comply with JIS Q27001 by then. There were 1,959 companies certified by ISMS as of January 2007, with about two-thirds of these companies in the Kanto area.

◆ Lecture

“Program for Protecting Personal and Business Information by Matsushita Electric Industrial”

Kenny Koike

Manager

Information Security Planning Group
Matsushita Electric Industrial Co. Ltd.

[\[Basic Guidelines\]](#)

Matsushita Electric Industrial established its Information Security Office in 2004 to conduct a program designed to improve the company's worldwide level of information

security. The purpose of this program is to improve the level of information security by protecting customers and employees, continuing business activities on a solid foundation, and using information in a secure environment. Our basic ideas to achieve those purposes are: (1) maintain information security under common global rules, (2) apply the same rules to all executives and employees regardless of status, and (3) provide training (for education) programs and administer appropriate punishment to those who violate the rules.

[\[Global Promotion System\]](#)

We are formulating a global policy based on the abovementioned purposes and ideas regarding information security. The global policy consists of mainly three sections: “personnel security,” “physical security,” and “IT security.” We are working in collaboration with related groups to implement specific measures for management. To provide experts required to maintain information security on a global level, we have chosen 30 members from the Information Security Office staff, 300 from among those who are in charge of the domains of various areas and offices (150 from Japan and 150 from overseas), and 3,000 members from among those who are in charge of branch factories and offices (one member per 100).

[\[Improvement of Information Assets Identification and an Information Security Management Cycle\]](#)

To improve the program for information security, we are carrying out the following three activities; (1) identify information assets that must be protected, (2) manage the information assets under a management cycle (PDCA), (3) make preparations to avoid dangers that threaten our information security.

[\[Training, Education, and Audits\]](#)

For educational purposes, we distribute security guidebooks (regarding practical training for beginners, training on personal information protection, and global practical training). We also conduct e-tests, put up posters, and display advertisements on Internet log-in screens to promote information security. Guidebooks, training videos, and posters are

all provided in multiple languages, including English, Chinese, and local languages. In addition to these promotion activities, the Information Security Office conducts audits, coupled with internal audits in each domain, autonomous inspections conducted by each branch office, and self-inspection at work to improve a management cycle for information security.

Session 4 Projects in Companies and Organizations
(2: Security Tools and Examples)

◆ Lecture

“Examples of Secret Sharing Schemes and Applications”

Yutaka Yasukura
President/ CEO
Global Friendship Inc.

Our company (GFI) has been primarily engaged in the development of information security technology based on secret sharing schemes. In 1999 we succeeded in commercializing the world's first fully proprietary secret sharing scheme, which is making contribution to the society.

[What is Advanced Encryption?]

The term “advanced encryption” itself is difficult to understand. It may give the impression that some clever IT experts are trying to deceive non-experts. A code cannot be broken as long as it is created and used in accordance with the encryption theory. In other words, the encryption theory allows us a theoretical possibility of maintaining perfect secrecy. Meanwhile, codes that are available on the market provide only a limited level of security by increasing computational complexity. In other words, there is no code sold on the market that satisfies theoretical conditions 100 percent, but codes that exceed an adequate level of computational complexity or are evaluated by a third party as offering adequate performance are accepted as codes that meet the advanced encryption standard.

[What is a Secret Sharing Scheme?]

Our company undertook the development of secret sharing schemes to avoid the risks involved in centralized information systems. Encryption schemes assume perfect key management to encode and decode information, whereas secret sharing schemes provide a means of restoring original information from a fixed number of sets of decontextualized information without using secret keys. A secret sharing schemes protects classified information by dividing it into a number of “shares.” It uses a well-known method of matching “tallies” as employed in Stevenson's *Treasure Island* to restore a map. In today's society as well, checks and bills continue to be used as in the past. Given the long time that people have used these methods, the methods are easily “understood and adopted” by the public. Guidelines for laws concerning the protection of personal information in business and industry (issued by METI in October 2004) explicitly state that personal information should be protected “regardless of whether or not encrypted.” The Commentary on the Unified Guidelines for Information Security Management in Government Organizations (published by the Cabinet Secretariat Information Security Center in December 2005) also states that “administrative officials who transport confidential digital records should use the required level of encryption to encrypt the information, and divide it into a number of sets to be transported through different channels.” Secret sharing is a method of managing information created from human wisdom that complements existing encryption technology.

[Examples, Applications, and Challenges for the Future]

We are able to cite several examples of secret sharing technology, such as GFI acquiring ISMS certification for its company information management system that was created using a secret sharing scheme (GFI electronic tally or “e-Tally”). The Personal Information Protection Project conducted by the Ministry of Internal Affairs and Communications also adopted our solution, which was made possible by the GFI e-tally.

There are currently more than 2 million licenses and we have yet to receive customer complaints. Our product has therefore achieved good results so far. Government offices and companies that have a keen interest in compliance have already introduced the e-tally in their systems. To promote appropriate use of the technology, we must develop various applications in the future. We will work in collaboration with our supporters to create a market for Japanese products that meet global standards.

◆ Lecture

“Secret Sharing for Long-Term Storage of Large Quantities of Data”

Naohiko Mori
Senior Manager
Security Project
Innovative IP Architecture Center
NTT Communications Corporation

[Secret Sharing Scheme]

Secret sharing schemes (SSS) are used to divide confidential information into different “shares” owned and managed by many individuals and restore the original information from a certain number of these shares. It is believed that these methods were originally developed to safely store data of relatively small size such as the secret keys used for codes.

[Using Electronic Data for Long-Term Storage of Information]

In recent years, the “long-term and safe management of electronic data” has become a serious challenge for companies, given the expanding amounts of electronic data owned by companies (due to growing needs to save paper documents on computers and achieve compliance) and higher levels of security required for such electronic data (such as protection against leakage and disasters).

The method of secret sharing that we developed randomizes confidential information and stores it in three separate shares. Since it allows high-speed data processing using logical operations, it can handle large-size data. Even if one share

gets lost, the original information can be restored from the other two shares (availability), and as long as genuine random numbers are used to randomize the information, it is impossible to restore the original data using any single one of the shares (confidentiality).

This method is used for storing a company’s electronic data, makes it possible to store divided data in three separate locations, and provides an effective measure for recovery in case of a disaster. Since the original information cannot be restored unless two shares are put together, entrusting data centers with the task of storing the shares involves no risk of exposing information and also provides an effective means of preventing insiders from leaking information.

[Attempts to Reduce the Amount of Storage Data]

The method of secret sharing that we developed has one drawback in creating three sets of data, each of which is the same size as the original data. One of these shares contains random numbers used to randomize the information, and we are working to overcome the drawback of our method by taking advantage of this characteristic. More specifically, we are trying to work out a method that combines pseudo and genuine random numbers so that we can ensure greater safety than when only using pseudo random numbers, and make the size of data smaller than when using only genuine random numbers.

◆ Lecture

“Attempts to Improve Information Security in Daily Business Operations by Ricoh Company: Improving Security and Reducing TCO by Integrated Management of OA Equipment”

Toshihiro Suzuki
General Manager
IT/S Planning Office
Information Technology & Solution Division
Ricoh Company, Ltd.

[Outline of Information Security Management by Ricoh Company]

The Ricoh Group developed a plan to create an information security management system (ISMS) in September 2002. We aimed to achieve the following goals to improve the level of security and increase the business value of the Ricoh Group as a whole: (1) To bear full corporate social responsibility as a member of society (by thoroughly implementing risk management); (2) To develop and provide strategic products and systems (by encouraging the acquisition of ISO15408 certification); and (3) To develop a solution business (by providing consulting services and know-how tool). In 2004, 91 Ricoh Group companies in Japan obtained certification. In 2005, six overseas factories obtained ISMS certification, and in 2006 two sales companies in Europe acquired ISMS certification. In August 2006 we also published the "Rico Group Information Security Report 2006."

[Value of Information Security for Companies]

The meaning of "Information Security" for companies is to provide valuable information for appropriate users and to promote the use of information while improving information security. For example, we disclose technological information of electronic components/ parts not only to the group companies but also to our clients, which makes responses to the RoHS directives quicker and more appropriate. Needless to say, we are careful only to disclose the information necessary in order to improve security.

[Measures for Routine Operations]

In relocating to a new head office, we adopted the following measures to strengthen security: (1) Integrated management using employee IC cards (to manage the comings and goings of employees, PC log-ins, and authentication

for OA equipment), (2) Integration of servers, and (3) Centralized management and "universalization" of OA equipment (using common MFPs throughout the entire office by integrating the functions of copy machines, printers, faxes, and scanners, making output printable from any MFP on any floor of the building, managing print logs using IC cards to prevent leaving printouts in machine trays, and using paperless fax machines).

The "universalization" of OA environment is the same thing as using location-free printing, which eliminates the need to use printers on other floors and reset PCs each time the layout is changed. It also greatly reduces user workload since full support is provided for equipment maintenance and troubleshooting. And since an employee is required to display an IC card to remove printouts from machines, the risks of leaving printouts in machine trays and taking the wrong printouts were eliminated.

[Improvement of TCO and Environment in the New Head Office]

These measures brought about quantitative effects, such as reduced paper costs through the centralized management of OA equipment and curtailed electric power consumption by IT equipment under centralized management, which alone lowered total annual costs by about 26 million yen per year and decreased environmental impact (CO2 emissions) by 318.2 tons per year. The initial number of man-hours required for introduction and maintenance of the new environment for PCs and printers, operation and maintenance of OA equipment, and introduction and maintenance of servers totaled 3,354 hours, but the annual man-hours required for actually running the office were reduced by 2,179 hours per year, thus yielding a high return on investment.

Announcement of the “21st ECOM Seminar” –Recent Trends in Overseas E-Commerce–

Improvements in information technology and proliferation of the Internet have caused the e-commerce market to rapidly expand around the world. At this seminar, reports were presented on the development of e-commerce overseas and the latest market trends. We have focused on the United States, the pioneer in e-commerce, and China, which is achieving spectacular growth, and examined the current status of e-commerce and major market trends in detail.

Date and Time: Wednesday, March 7, 2007 14:30 – 16:40

Place: Kikai Shinko Kaikan, Sixth Floor, Room 6-66 (3-5-8, Shiba Koen, Minato-ku, Tokyo)

▼ Program

14:30-15:30	Lecture 1 “Current Status and Future Prospects of E-Commerce in the Global Market”
15:30-15:40	Break
15:40-16:40	Lecture 2 “Recent Trends in E-Commerce in China”
16:40-16:50	Questions and Answers

From the Secretary-General

▼ I have not worn my coat since the beginning of the last week in February. On the first day I thought I may have been too hasty in making the decision, but signs of spring are already in the air. ▼ February turned out to be a month of seminars, with eight being held including local seminars. (Some seminars are summarized in the News above.) We would like to thank those people who took the trouble to deliver lectures, make arrangements for the seminars, and participate in the programs. Thank you all very much. ▼ We began discussing the Activity Plan for FY 2007 at the Fifth Planning Committee Meeting (on 2/23), and plan to hold discussions about the Activity Plan (draft) and budget (draft) at the next Planning Committee Meeting (on 3/20) and meeting of the Board of Directors (on 3/29). ▼ We have only another month left before the end of the fiscal year, and the Secretariat of each group is now in the final stages of organizing the results for this year. We will send you a report on these results. We hope our report will live up to your expectations. (Kataoka)