Published October 1, 2003. Distribution restricted to Sponsors until January 1, 2004.

WHITE PAPER

Applying Auto-ID to the Japanese Publication Business

To Deliver Advanced Supply Chain Managment, Innovative Retail Applications, and Convenient and Safe Reader Services

Toshiharu ISHIKAWA, Yukiko YUMOTO, Michio KURATA, Makoto ENDO, Shingo KINOSHITA, Fumitaka HOSHINO, Satoshi YAGI, Masatoshi NOMACHI

AUTO-ID CENTER KEIO UNIVERSITY, 5322 ENDO, FUJISAWA, KANAGAWA, 252-8520, JAPAN

ABSTRACT

In recent years, because ofthe decrease in costs and increase in promotion activities by standard groups such as Auto-ID Center, RFID has been gathering greater interests from industries such as apparel, publication, appliances, and general household goods. Furthermore, RFID is considered to be more than just a tool for efficient logistics and commerce; it is one of the infrastructure technologies for ubiquitous computing society.

In particular, the publication industry has been proactive in adopting RFID in the areas such as logistics, anti-theft, marketing, and customer services. With the equipment vendors beginning to merge into this activity, it is hoped that the possibilities of RFID and its successful application be realized in the near future.

DNP, Sun, and NTT are cooperatively studying potential applications of Auto-ID technologies to Japanese publication business. The scope of the study includes distribution channels that span publishers, distributors, book stores, and readers, as well as the treatment of issues like privacy after a book has reached its consumer. This paper summarizes the activities and the findings thus far. The issues in Japanese publication business, possible solutions using Auto-ID technologies, and an experimental prototype system are described.

WHITE PAPER

Applying Auto-ID to the Japanese Publication Business

To Deliver Advanced Supply Chain Managment, Innovative Retail Applications, and Convenient and Safe Reader Services

Biography

Toshiharu ISHIKAWA
Associate Director

Toshiharu ISHIKAWA received his Bachelors and Masters from Tokyo Institute of Technology. He has worked for Central Research Laboratory of Dai Nippon Printing. co., Ltd. for 13 Years. He has stared RFID research in 1999 and has become a Deputy General Manager, RFID Business Center of Dai Nippon Printing. co., Ltd. has joined Auto-ID Center in 2001. He also has become an Associate Director, Auto-ID Center Japan in 2003.

Yukiko YUMOTO
Associate Director

Yukiko YUMOTO is the associate director of Industrial Deployment, Auto-ID Center Japan, and also a manager of Auto-ID project, solution practice operating, Sun Microsystems K.K.. She has experience of Sales Product marketing and development in CPG industry (Lion K.K.). She experienced asset inventory control as of Merchandiser/Buyer specialist. She moved to Motorola as QA of land mobile product service division, Information system service, project management in ERP system implementation. She moved to Boots company UK as IT operation manager, in Japan branch, responsible for product replenishment systems, etc.. In 1999, she moved to Manugistics Japan as Implementation consultant of Demand Planning module. She joined Sun Japan for provisioning Auto-ID system to research market deployment.

Michio KURATA,
General Manager, Dai Nippon Printing

Michio KURATA is a technical general manager, Advanced Technology Group, Communication & Information Operations, Dai Nippon Printing. He received his B.S. degree in Applied Physics from Waseda University. In 1979, he joined the central laboratory, Dai Nippon Printing. He moved the Communication and Information laboratory in 1983.

WHITE PAPER

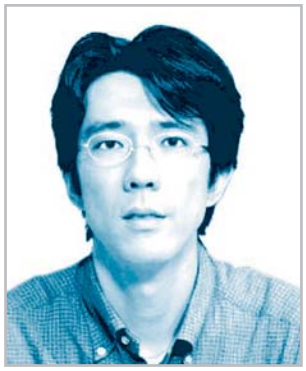
Applying Auto-ID to the Japanese Publication Business

To Deliver Advanced Supply Chain Managment, Innovative Retail Applications, and Convenient and Safe Reader Services

Biography

Makoto ENDO
Senior Research Engineer
NTT Corporation

Makoto ENDO is a senior research engineer, Ubiquitous Computing Project, Information Sharing Platform Laboratories, NTT Corporation.
He received the B.S. in Faculty of engineering from Musashi Institute of Technology, Tokyo, Japan. In 1990, he joined the Network Systems Development Center, Nippon Telegraph and Telephone Corporation, Tokyo, Japan. In 2002, he moved the NTT Information sharing Platform Laboratories.



Shingo KINOSHITA
Chief Research Engineer
NTT Corporation

Shingo KINOSHITA received his B.S. degree in Solid State Physics Engineering from Osaka University in 1991. In 1991 he joined the Information and Communication Systems Labs., Nippon Telegraph and Telephone Corporation, Yokosuka, Japan. He is a chief research engineer in the Information Security Project at NTT Information Sharing Labs. He has been engaged in the research and development of distributed computing systems, Internet protocols, especially reliable multicast protocol, information security. His recent interest is mainly ubiquitous security including RFID privacy. He is currently a member of IEEE Computer, IEICE and IPSJ Societies.

Fumitaka HOSHINO
Researcher
NTT Corporation

Fumitaka HOSHINO received his B.Eng. and M.Eng. degrees from Tokyo University, Tokyo, Japan, in 1996 and 1998, respectively. He is a Researcher in the Information Security Project at NTT Information Sharing Platform Laboratories.

WHITE PAPER

Applying Auto-ID to the Japanese Publication Business

To Deliver Advanced Supply Chain Managment, Innovative Retail Applications, and Convenient and Safe Reader Services

Biography

Satoshi YAGI
Research Engineer
NTT Corporation

Satoshi YAGI is a research engineer, Ubiquitous Computing Project, Information Sharing Platform Laboratories, NTT Corporation. He received his B.S. and M.S. in Electrical, Electronics and Computer Engineering from Waseda University, Tokyo, Japan, in 2000 and 2002, respectively. In 2002, he joined the NTT Information Sharing Platform Laboratories, Tokyo, Japan. He is a member of the Institute of Electronics, Information and Communication Engineers.

Masatoshi NOMACHI
Project Coordinator of Auto-ID Project
Sun Microsystems

Masatoshi NOMACHI is a project coordinator of Auto-ID Project, Solution Practice Operating, Sun Microsystems K.K.. He received his B.S. in Faculty of Environmental Information from Keio University, Tokyo, Japan. Since 2001, he has joined Auto-ID project, Sun Microsystems K.K..

WHITE PAPER

Applying Auto-ID to the Japanese Publication Business

To Deliver Advanced Supply Chain Managment, Innovative Retail Applications, and Convenient and Safe Reader Services

Contents

1. INTRODUCTION

In recent years, because ofthe decrease in costs and increase in promotion activities by standard groups such as Auto-ID Center, RFID has been gathering greater interests from industries such as apparel, publication, appliances, and general household goods.

In particular, the publication industry has been proactive in adopting RFID in the areas such as logistics, anti-theft, marketing, and customer services. In December 2002, an industry-wide group was established to study and promote the use of RFID as a replacement for bar codes. In March 2003, IC chip and other equipment vendors formed a technology consortium and began investigating technical issues. Topics of discussions in progress includes technical issues such as improving reading accuracy and methods for mounting tags to books, and business-oriented issues such as identifying problems at each of publisher, distributor, and book stores, industry-wide operating standards and application development.

DNP, the largest printing company in Japan, has made numerous system proposals incorporating Auto-ID technology to the study group. In addition, Auto-ID Center members, DNP, Sun, and NTT are cooperatively studying potential applications of Auto-ID technologies to Japanese publication business. The scope of study includes distribution channels that span publishers, distributors, book stores, and readers, as well as the treatment of issues like privacy after a book has reached its consumer. Also, a prototype system was developed and disclosed to the public during "Tokyo International Book Fair 2003," the largest industry exhibition (Tokyo Big Site April 24 through 27, 2003), to facilitate discussion between the industry and the consumers about the RFID vision. This prototype is built based on the core technologies of Auto-ID: EPC™ and Savant™.

This paper summarizes the activities of the aforementioned three companies. Section 2 is a brief introduction to Japanese publication industry, covering the market size, regulations, and issues. Section 3 shows "The big picture" of Auto-ID technology. How the technology may be applied to the Japanese publication industry and privacy issues that arise once a book is sold to a consumer are discussed in section 4. Section 5 describes the prototype system and its demonstration scenario.

2. PUBLICATION BUSINESS IN JAPAN

2.1. Overview

The Japanese publication industry is run by the following types of organizations: publishers that plan and edit, printers that print, wholesale merchants who acts as primary distribution hub, and book stores and kiosks that interfaces directly with the consumers. Each year, 70 thousand new books and 3,500 magazine titles are sold. Sixty five percentof this volume is sold through the "wholesale-to-bookstore" route. Figure 1 shows the system structure, and figure 2 shows the flow of books and information. 20% of the volume is sold through the "CVS (convenience store)" route. There are also other sales routes such as "co-op," "train station kiosk," and "specialty stores." Also, popularity of the Internet provided for the growth of the "net shop" route, which accounts for 1% of the volume.

In terms of regulation, there are two systems in place: "re-sale" and "commissioned sale." In short, these systems "control retail price" and "guarantee refunds for unsold books." These rules enables book stores to stock many books on their shelves without having to worry about unsold books. It also means that consumers can choose from a wide selection of books in any bookstore.

Figure 1:

Delivery
Send back

BOOK DISTRIBUTION (WHOLESALER, BOOK STORE ROUTE) SYSTEM

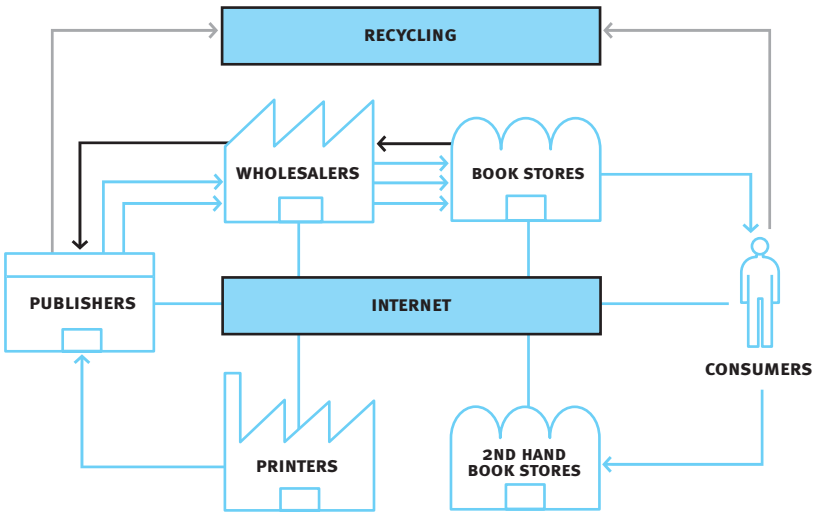
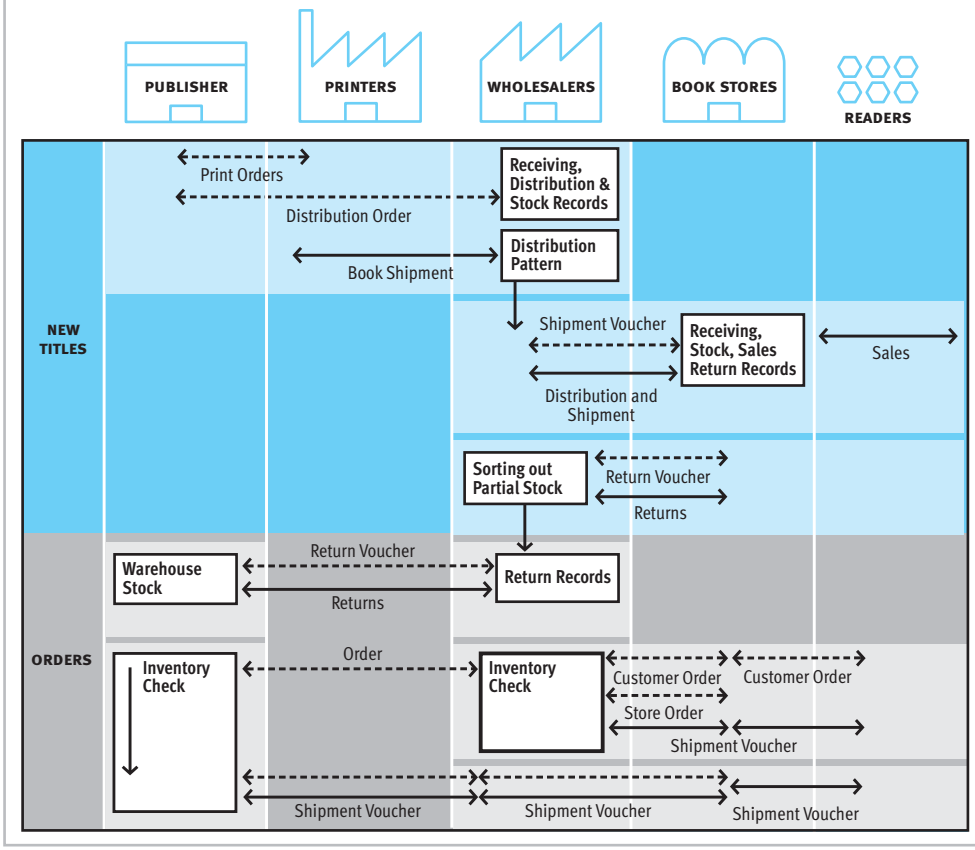


Figure 2:

Flow of Information
Flow of Goods

BOOK DISTRIBUTION (WHOLESALER, BOOK STORE ROUTE) FLOW OF GOODS & INFORMATION



As far as a publisher is concerned, only one copy of a book may be consumed by a single reader. Thus they forecast demands in attempt to provide books that sell well in a timely manner. In this sense, accuracy of information on current demand, sales forecast, and inventory is a key element in achieving business success.

In the “wholesale-to-bookstore” route, wholesale merchants determine the number of new books to stock in each book store by considering factors like the store's location, size, past sales record, and the types of consumers. Currently, however, it is difficult to accurately grasp such properties for 20 thousand book stores across the country, resulting in lost sales opportunities, excess inventory, wasteful transportation, and mounds of returned books (books 40%, magazines 30%).

Furthermore, new problems have arisen in recent years. Shoplifting for the purpose of reselling and fraudulent transactions such as returning books past its return deadline has become rampant. Also, libraries buying many copies of best seller titles and the increase in number of comic book coffee shops has lead to decreased sale of new titles.

2.2. Market Size

Total sale of published goods in 2002 was 2.3 trillion yen, indicating decrease for five consecutive years since 1997. There are 4,400 publishers and 40 wholesale merchants, and 80% of them are based in Tokyo. There are 20 thousand bookstores, and the number is on a decreasing trend, but the floor space is increasing. This indicates that while small bookstores are closing down, big shops remain or are getting bigger. Each year, more than 70 thousand new titles, 1.3 billion books, and 4.4 billion magazines are delivered to store shelves. Of these, 0.8 billion books and 3.2 billion magazines are sold for 950 billion yen and 1.44 trillion yen, respectively.

“Wholesale-to-bookstore” route accounts for 65% of all publication distribution. 80% of these are shipped from Tokyo. A large wholesale merchant handles 2 million books and 4.5 million magazines every day. Shipment of such volume is handled by carriers contracted for each region.

2.3. Current Issues

Existing issues in the publication industry can be organized into three categories: logistics, promotion and marketing, and customer services.

Logistics can be divided into three areas. First is the efficient shipment of new titles. For each bookstore, the wholesale merchant must sort and box the items to be shipped. Currently, this task is done by hand using barcode, but there is increasing pressure to make this more efficient. Second is the order processing, which is a coordinated effort between a bookstore and a wholesale merchant. Although parts of this task is slowing becoming online, it has not reached the point where inventory at the wholesale merchant and the publisher can be directly queried. The third area is the inventory management within a bookstore. There is much room for improvement in backyard tasks such as verification of received books, inventory checks, and returning of unsold books. Also, the burden of guarding against shoplifting is increasing.

To gather information for promotion and marketing, one must go to the shops where books and consumers meet. Currently, lack of marketing information is preventing effective selling. Also, because publishers cannot easily know inventory state and “what's selling well” at the shelves in real time, they often fall into situation where well-selling titles are also the ones that get returned the most.

Traditional reading from printed books still plays an important role in enhancing imagination and literacy. Nowadays, however, there are more occasions to read digitally displayed text from sources such as the Internet. In times when the revenue from books is decreasing, it is hoped that new reader services using the network will help boost its sales by making purchases more convenient for consumers.

Note: sales figures in this section were excerpt from [1].

3. WHAT IS AUTO-ID?

3.1. Overview

Auto-ID (Automatic Identification) is one of the RFID technology standards developed and promoted by Auto-ID Center. The scope of this standard covers basic and communication technologies for network systems that identify, track, and record objects and their movement. In Auto-ID, each object has an RFID tag. Ultimately, recognition and system entry of the information in these tags are done without human intervention. The system, in turn, has tracking, monitoring, and processing capabilities to realize automatic object identification.

Auto-ID Center

Auto-ID Center [2] was founded in 1999 at Massachusetts Institute of Technology (MIT). Since then, leading companies from various industries assist its activities. Auto-ID Center is founded as one of the UCC (Universal Code Council) activities for next-generation barcode, and is designing foundation systems and standards for object identification and tracking technologies used in global supply chains. A technology for mapping trillions of objects like merchandise, products, parts, pharmaceutical goods, to their associated information – the goal of Auto-ID Center is to establish standards that gets adopted and used by companies world wide.

3.2. Auto-ID Technical Overview

EPC™ (Electronic Product Code)

EPC™ [3] is the format, proposed by Auto-ID Center, for unique identifier to be associated with an object. Contrast to barcode, which was a standard for identifying the type of a product, EPC™ standard enables unique identification of each individual object (Figure 3).

Figure 3

EPC™ CODE SAMPLE (96 BITS)

RFID (Radio Frequency Identification) Tag/RF Reader

RFID tag is a package that contains an IC chip and an antenna [11]. A RF reader can obtain information in the IC chip via radio communication, without making a physical contact with the tag. For wide adoption of Auto-ID, the price of a tag must fall from current 50 cents to below 5 cents.
RF reader identifies RFID tags, and communicates with them using various methods. Currently, a RF reader costs about $1,000. In the future when readers become widely deployed, the price is expected to fall below $100. RF readers that can identify RFID tags at different frequency band is also expected.

Savant

As the most advanced facet of Auto-ID technology, Auto-ID Center is developing software technology called Savant [4]. A savant collects, accumulates, and processes EPC™ data from one or more RF readers. It adjusts inadvertent multiple readings of a tag, and performs tasks according to the acquired information such as archive, transfer, and inventory control.

Savant consists of three key elements: EMS (Event Management System) that provides Java API for different RF readers, RIED (real-time in-memory data structure) that manages event information, and TMS (Task Management System) that provides external interface for task management.

ONS (Object Name Service)
ONS (Object Name Service) [5] is a technology that maps an EPC™ code to its associated information. ONS server, upon request from a Savant, shows the location of the information for a given EPC™ code. Auto-ID Center is developing ONS with the assumption that its load will be more than that of domain name service (DNS) used in the Internet.

PML (Physical Markup Language)
Information associated with a given EPC™ is described in PML (Physical Markup Language) [6]. PML is based on widely-used XML (eXtensible Markup Language), and is designed to be world-wide standard language for describing information about an object such as product name, size and current state (location, owner, etc.).

4. APPLICABILITY OF AUTO-ID

4.1. Scope of Application and its Methods

As discussed in section 2.1, book distribution entails many complex tasks like package inspection, sorting, inventory management, order and return processing, marketing research, and anti-shoplifting countermeasures. RFID is a tool for silent commerce – a way to get these tedious and complex tasks done automatically without human intervention.

A RFID tag is embedded into a book when it's bound, and the information about the book is entered into a database. The database is updated each time the book is shipped from, and returned to a wholesale merchant. By displaying the book in a shelf that has an antenna, a bookstore can track its inventory. In this way, distribution and sales history of each book can be captured accurately, authors and publishers can obtain marketing information in real time, and wholesale merchants can grasp the inventory in circulation. In a bookstore, shelves of sold books can be replenished quickly, and effective anti-theft countermeasures may be put into place. Consumers can use RFID to easily access information related to a book. It also becomes easier to build and organize one's private library. By accurately tracking the circulation route of each book, technical solutions may be possible to address the problems associated with used book stores, libraries, and comic book coffee shops.

By using RFID, the real world of objects and the world of information may be unified seamlessly, and each participant, be it an author, a publisher, a vendor, or a consumer, can get information relevant for that participant from databases connected to a network.

Table 1 shows economic impact expected of RFID deployment. At the first stage, 240 billion yen of cost may be cut due to reduced theft and efficient circulation. At the next stage, effective marketing and CRM may lead to increased revenue. Each RFID element currently costs about 100 yen, but development is under way to reduce this to less than 5 yen. If six billion books are printed annually, then the increase in annual cost would be 6 billion x 5 = 30 billion yen. However, if 240 billion is saved as mentioned above, return on investment is sufficiently large.

Table 1

ECONOMIC EFFECTS EXPECTED OF RFID USE		
Current Situation	– Whole sales volume = 20 billion – Theft volume = 1.5% ↓ **= $300 million**	– Sent back volume = 6 billion – Unauthorized return book volume = 3% ↓ **= $ 180 million**
Target of the 1st Step Trial ↓	1. Reducing these losses by tag sensing 2. Well-organized inventory control through on-line SCM system	Reduce useless delivery by 25% **= $ 1.5 billion**
Future Target	3. Further effectiveness in Effective Marketing by Customer Relationship Management	

Circulation and Inventory Management

By applying RFID to supply chain management, one can expect increased efficiency in tasks like (1) inspection, (2) inventory management, and (3) return processing. By expanding this effect to cover all of circulation, the amount of inventory in circulation can be optimized, and supply chain lead-time may be reduced. Once RFID becomes widely deployed and information shared among companies, new business models may emerge. Following sections elaborate on the effects on tasks (1) through (3) mentioned above.

1. Inspection

Traditional barcode-based (e.g. ISBN) inspection procedure can be made more efficient by using RFID. Inspection occurs at many points. At the beginning of a book's lifecycle (publisher, printers, wholesale merchants), the subject of inspection is “many of the same thing.” Near the end of a book's lifecycle (book store, used book shops, libraries, etc.), the subject is “few of many things.” Inspection also takes place when books are returned.

In any case, by reading RFID tags, inspection can be done without opening the outside package. By comparing the manifest of the package against information read by RF reader, one can determine whether something is missing or is in excess. To achieve the same goal without RFID, one must open the package and verify each of its contents by hand. RFID makes inspection more efficient by eliminating human intervention and errors.

2. Inventory Management

In many situations, “theoretical inventory” is used in place of the actual inventory. Theoretical inventory is derived from actual inventory (which is sparsely verified) and transaction records. In reality, the theoretical amount differs from the actual amount due to factors such as errors during inspection and record keeping, lost merchandise, and theft. This difference is reconciled once or twice a year when an actual inventory count is taken. Similar situation is true for location management. Even for the same products, if the condition of sale differs, management becomes very costly. Currently, differences in terms and conditions are managed using a paper slip that gets bound with each book. Although existing systems have significantly increased efficiency from fully manual record keeping, they have not completely done away with paper slips because bar codes cannot manage each book individually.

RFID will change the inventory control methods, and improve accuracy and efficiency. For example, RF readers can be embedded into display shelves so that the inventory of the merchandise on the shelves is constantly kept up to date. Efficient inventory control methods enable more flexible operation. The cost of managing paper slips can be eliminated by maintaining the information together with RFID on a database. Then, by share this information among the companies on the book supply chain, decisions like “when to re-print” can be made quickly.

3. Return Processing

Return processing, more than any other task, requires attention to individual item. A bookstore must select books to return based on terms and return deadline, and send them to the wholesale merchant. Wholesale merchant, then, must verify validity of returned items. These tasks, currently done for each item by hand, can be greatly facilitated by RFID. In a bookstore, selection of return books can be done as a part of inventory management. Wholesale merchant can validate returned items quickly, easily, and accurately.

Prevention of Illegal Circulation

A rule of book selling in Japan stipulates that a new title is stocked on bookstore shelves for 105 days. After that, the books are returned to the wholesale merchant. However, selecting books approaching their return deadline from a vast volume of books in a store is tedious work and occasionally, books that has not reached its deadline may get mixed into return stock. There have been malicious cases where a store bought back used books, and returned them as unsold stock. Also, considering the volume and variety of books a wholesale merchant handle, it is unrealistic for them to accurately inspect each returned book.

With RFID, each item can be individually identified, and its circulation record be retrieved. This is an extremely efficient way to determine if a book has reached its return deadline, or if it was sold previously.

Marketing and Customer Services

In traditional marketing, price and quantity data from POS systems were collected and analyzed based on day-of-week and time-of-day, and then a sales trend hypothesis was defined and evaluated. However, POS data does not reflect the process that consumers went through to pick each item, and thus is insufficient for fully understanding the consumers.

Auto-ID technology may provide a revolutionary solution to address this problem. RFID tags embedded in a book is read by RF readers, installed throughout a bookstore, and the information is stored in a database. This information represents the movement, in real time, of the book within the bookstore that can be used to analyze, for example, trends in browsing habits. In this way, popular genre may be quickly identified and effective marketing campaign can be launched. Furthermore, because the movement of a book also represents the movement of the consumer within a bookstore, it may be possible to obtain hints for more attractive and effective display or shelf organization.

Accumulated data may also be fed back to the consumers in forms like “top ten ranking” or “what's related.” If such data can be shared by the entire publication industry, it may prove to be a key factor in revitalizing the industry.

Countermeasures Against Shoplifting

In recent years, the ratio of damages due to lost merchandise is rapidly worsening, and has become a significant burden on book store revenue [7]. There are many causes for lost merchandise, but the major factor is shoplifting, where the number of cases and damage has increased dramatically. According to a survey of 2,530 book stores, conducted by the Ministry of Economy, Trade and Industry, damage per shop due to shoplifting is 2.1 million yen per year, which is equivalent to one to two percent of the annual revenue [8]. Because the margin gained by a book store is also one to two percent, this is an issue of critical importance [9]. Also, shoplifters have become more organized. Acting as a group, they steal not one or two books, but a shelf at a time. It is no longer a matter of impulse of an individual.

It is said that the reason for the increase in such malicious theft is that books can be turned into cash easily at used book stores [10]. Used bookshops have their place in collecting and recycling books that otherwise would be discarded. However, it is also undeniable that they induce malicious theft. The most

popular target for theft is new comic book titles, for which used bookshops pay a relatively high price. It is not a coincidence that rapid growth of used bookshops and the dramatic rise in shoplifting damage happened at the same time [9]. Although someone bringing in tens of new comic titles is suspicious, unless there is clear evidence that the comics were stolen goods, a used bookshop cannot refuse to buy them.

Auto-ID technology provides a fundamental solution against shoplifting. For example, by applying "book tracking" as mentioned above, it is easy to implement a mechanism to detect suspicious behavior, like many books being taken from a shelf at once, in real time. Upon detecting such an event, an alarm can be sounded in the backyard to alert store staff. In other words, Auto-ID system is taking place of security guards in constantly watching the store. In addition sounding an alarm in the backyard, a voice such as "thank you" may be played near the suspect's shelf. In general, bookstores tend to be indifferent about browsing consumers. As this disregard may, in part, be inducing shoplifting, it would be an effective deterrent to plant in consumer's mind the notion that the store do care, and that there are defense mechanisms in place.

Furthermore, if used bookshops have access to circulation information, they can identify stolen merchandise quickly and easily, and refuse to buy them. By moving away from the traditional model, where bookstores took the risk of theft, to the industry-wide cooperation model, damages from shoplifting can be greatly reduced.

Customer Services
Information such as identification and sales record of an individual book may be used to realize enhanced customer services. For example, if a RF reader is installed in a customer's home, it can be used to access online services provided by the publishers such as lottery, point service, e-books, user registration, and bulleting boards. Also, the store that sold the book can be found from the sales record of the book. Thus, customized services can be provided by the store as well. This type of service is not only beneficial to consumers, publishers and book stores can use them as Marketing tools.

In the future, if the issues such as RF reader cost and customer's privacy are resolved, it is likely that RF readers will permeate to various places such as every home and many attactive services will be created. Particularly, in Japan, Internet access from mobile phones equipped with a camera and IrDA is very popular. A mobile phone with an embedded RF reader may be introduced.

4.2. RFID Privacy Consideration

What Privacy Issues are there with RFID?
The Auto-ID Center's RFID does not implement any access control in order to reduce cost. RF readers can read EPC™ codes of an object containing an EPD code, however, unprotected information is limited by the EPC™ code only. Information associated to the EPC™ code, such as product tracking history and preservation state, is maintained inside a network, and is protected by Internet security technologies. Furthermore, by policy, no information that can link to personal information about a buyer or an owner is to be managed. Yet, the ability to read EPC™ code alone, can lead to privacy issues. These issues can be categorized into two types: (1) leakage of information about personal properties, and (2) activity monitoring and personal identification by ID tracking.

1. **An EPC™ code contains maker code and type of item, so it may be possible to obtain information about someone's personal properties. It is conceivable that there is information that one would not want to disclose, such as the type of medication, clothes and under garments, expensive items, bills, and books which reflect the preference and thought of their owners.**

2. If a piece of personal information gets linked with an item by some methods, **then the activity of the person may be possible to track by tracking the purchased item. In particular, artifacts that one wears to keep close (clothes, shoes, jewelry, bags, etc.) may be senitive.** This risk is not specific to EPC™ code, but applies to any RFID that always returns identical unique ID. Furthermore, once an ID of a person's item is linked to information identifying that person, the same link can be established with the ID of every other possession. Then, it becomes impossible to prevent being tracked. With the exception of dictionaries, books generally are not carried on one's person for any extended period. Thus the risk of being tracked for a long time because of a book is relatively low. Yet, the thread needs to be carefully evaluated.

3. Becomes a real threat when personal information is linked to an item, information is fraudulently circulated, and the person owns the item for some extended period of time. In this sense, the possibility of (2) becoming a threat is less than that of (1). Nowadays, with more incidents of shoddy management of personal information by companies, and circulation by unethical roster vendors, these risks must be carefully considered.

Kill Feature and its Issues

With features like access control and mutual authentication between IC card and its reader, existing IC cards used for personal identification and payment are designed with security in mind. They also have relatively large memory capacity, and some of the "data-carriage" type RFID, that can hold circulation route and other information, also support access control. In contrast, RFID that aims for low-cost, such as the one used by Auto-ID, serves its primary purpose, enable automatic identification of things, and does not support any security feature.

The only security measure supported by Auto-ID Class I chip [11] is the "Kill" feature. The purpose of this feature is to disable RFID functionality, for example, at the time of purchase. A disabled tag cannot be re-enabled.

Consumers would find the kill feature intuitive, and thus easy to accept. However, killing a tag nips the bud of future potential use of RFID, such as consumer services (e.g. limited offer, automatic replenishment ordered by a refrigerator, expiration date and product recall alarm, personal library management, etc.), use by resellers, and recycling. Publication business, in particular, have many post-sale users (libraries, used book shops, etc) who expect RFID tags to be fully functional.

For these reasons, it is very much desired to achieve low cost, post-sale use of RFID, and privacy protection. [12] through [17] are examples of research in progress.

Operational approaches

A radio shield may be used to prevent an ID from leaking without disabling a RFID tag. Many bookstores in Japan provide paper covers for customers who ask for them. If radio shield were embedded into each of these covers would prevent ID from being eavesdropped. Simply removing the cover will allow the RFID tag to be used again. Although primitive, this is effective and intuitive as it is suggestive of "hiding the title," which is the purpose of the covers themselves. Some of the down sides are, that covers are used only on relatively small books, not all book stores have them, and the cost of embedding radio shields.

Following sections introduce some technical solutions.

NOTE: as mentioned earlier, privacy protection technologies are still under investigation at Auto-ID, and are neither standardized nor implemented. The position of the techniques described below is trial research.

Technical Solution 1

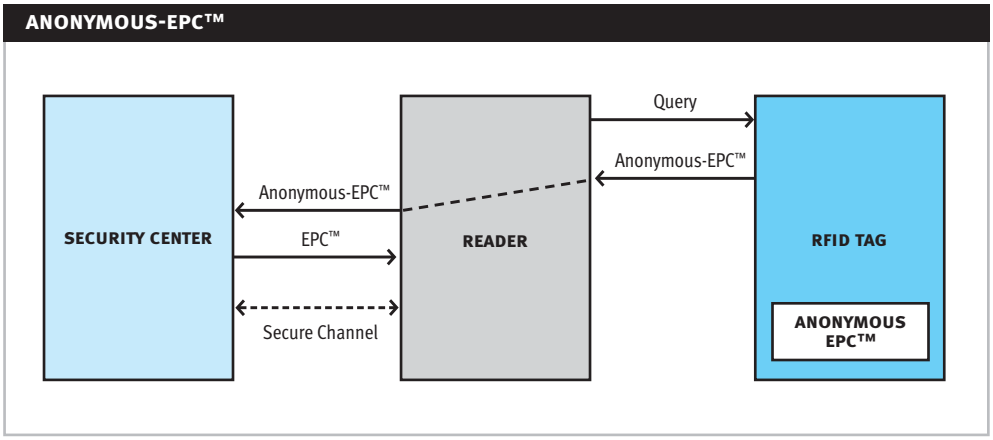
PREVENTING LEAKAGE OF INFORMATION ABOUT PERSONAL PROPERTIES

The method described in this section is applicable to RFID that only has ROM capability. With this limitation, only (1) leakage of information about personal properties, can be addressed. As books reflect preferences and ideals of their owners, high demand is believed to exist to hide their titles from strangers.

Anonymous-EPC™

By storing anonymous (by encryption, for example) EPC™ in RFID, information leakage can be stopped without using any access control circuitry. The Anonymous-EPC™ is converted to regular EPC™ by a trusted security center. Only the readers that have proper clearance may request conversion of Anonymous-EPC™ (Figure 5).

Figure 5



When a reader accesses the security center, a secure channel is used to authenticate the reader. In this way, only authorized readers will be able to obtain the EPC™. By allowing the owner to set access control list, readers owned by those other than the owner may be granted access. This technique only requires that RFID tags contain Anonymous-EPC™. Low cost privacy assurance is achieved by storing only Anonymous-EPC™ in RFID and using existing Internet security technologies to control access of readers to security centers.

There are three ways that an EPC™ may be anonymized.

1. Randomize. Choose an arbitrary random number as Anonymous-EPC™, and have the security center map the random number to the corresponding regular EPC™. This method allows the Anonymous-EPC™ to be variable in length. On the other hand, having to do table lookup at security centers limits scalability.

2. Common key encryption. Anonymous-EPC™ is generated by encrypting the regular EPC™ by a common key. Security centers decrypt the Anonymous-EPC™, and return the regular EPC™. Compared to public key encryption, this method generates shorter Anonymous-EPC™, and thus can be decrypted quickly. Also, unlike randomized EPC™, this method does not limit scalability. On the other hand, this method generally requires longer Anonymous-EPC™ than randomized EPC™, but shorter Anonymous-EPC™ is possible, even with the same length key, by using an encryption algorithm with a shorter block size [18]. Also, in contrast to public key encryption, to keep key management costs low, the security center must perform all encryption processing, these operations results high computational load which may not be trivial.

3. Public key encryption. RFID holds the Anonymous-EPC™, which is generated by encrypting regular EPC™ by a public key. Upon request, security centers decrypt the Anonymous-EPC™. This allows each vendor to freely encrypt EPC™ using a public key, so that there is no single entity burdened with all the computation. As for encryption algorithm, to achieve sufficient cryptographic strength, RSA would require Anonymous-EPC™ to be several kilobits, which is far too long compared to the regular EPC™ sizes of 64/96 bits. Elliptic curve cryptography can achieve similar strength while limiting the length of Anonymous-EPC™ to about 320 bits.

In our prototype, we implemented randomized EPC™ and public key encrypted EPC™. Public key encryption algorithm is EC-ElGamal. Also, by using OEF [19], developed by NTT, for elliptic curve cryptographic computation, decryption at security centers is accelerated.

Technical Solution 2

ADDRESSING ID TRACKING PROBLEM

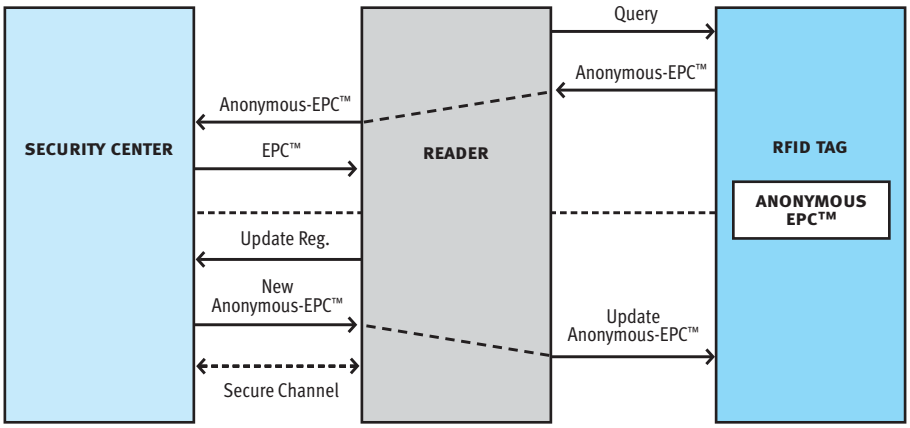
This section describes a method, using a rewritable memory like EEPROM, to address issue (2) ID tracking. The Anonymous-EPC™ technique discussed above is effective against issue (1), leakage of information about personal properties, it does not solve the ID tracking problem. This is because, even if EPC™ is anonymized, the value read from RFID is always the same, which is sufficient for tracking purpose. An effective countermeasure for this problem is re-encryption of Anonymous-EPC™ using probabilistic public-key cryptosystem. Roughly speaking, probabilistic encryption is a public-key cryptosystem whose goal is that "no information" about the plaintext should be computable from the ciphertext. "No information" means that it is infeasible to know whether given two ciphertexts have the same plaintext or not without secret. Therefore there are many possible encryptions of each plaintext. Some probabilistic public-key cryptosystem have re-encryption function, which transforms a given ciphertext into other encryption of the same plaintext without knowing any secret. By re-encrypting a RFID tag returns a different value each time it is read, making evasion from ID trackers possible. Security centers can continue to decrypt Anonymous-EPC™ exactly as mention above, without additional computational overhead. If, however, re-encryption were done inside a RFID, then the cost of each tag would increase.

To keep the RFID tag cost low, re-encryption should be done somewhere outside of the tags, where implementation cost is low, and tags must have rewritable ROM so that updated Anonymous-EPC™ can be stored. There is additional cost associated with using rewritable ROM and its controller, but this is significantly less than that of re-encryption circuitry.

The protocol is as follows (figure 6).

Figure 6

UPDATING A ANONYMOUS-EPC™



Step 1
A reader sends re-anonymizing request for a Anonymous-EPC™ to the appropriate security center. The security center authenticates the reader using existing Internet security technologies.

Step 2
The security center generates and returns a new Anonymous-EPC™. The method for generating a new Anonymous-EPC™ depends on the anonymizing method used.

- for randomized EPC™, security center will generate another unique Anonymous-EPC™.
- for common key encryption, security center will pad the regular EPC™ with a random number, and encrypt the entire sequence to generate a new Anonymous-EPC™.
- for public key encryption, use an algorithm with re-encryption characteristics, such as EC-ElGamal algorithm, to generate a new Anonymous-EPC™. In this case, re-encryption need not be done at the security center, but may be done at the reader because the key for encryption is public [13]. Discusses the method for public key re-encryption at the point-of-sale terminal to protect privacy of RFID attached to currency notes.

Step 3
The reader writes the new Anonymous-EPC™ into the RFID tag. For methods (b) and (c), it would be more effective if the keys are updated at the same time.

By sparse updating Anonymous-EPC™ in this manner, long term tracking may be avoided. In reality, however, there are operational issues that need to be considered, such as the frequency and cumbersomeness of updates. In order to address these issues, we are studying a new scheme where ID can be updated every time [22].

Other Security Features
In addition to privacy protection, we considered signed EPC™ to detect duplicate and fake EPC™. For digital signature algorithm, we use ECAO [20], developed by NTT, based on elliptic curve cryptography. ECAO generates a message-recovery type signature. That is, EPC™ data can be embedded into its signature. This method consumes about 80 bits less than an attach type signature algorithm that attaches the signature to EPC™ data. To alleviate the overhead of authenticating signed EPC™, use of 160 bits signatures by Boneh's short signature [21] method would be effective, yet relatively slow.

5. PROTOTYPE SYSTEM

5.1. Overview

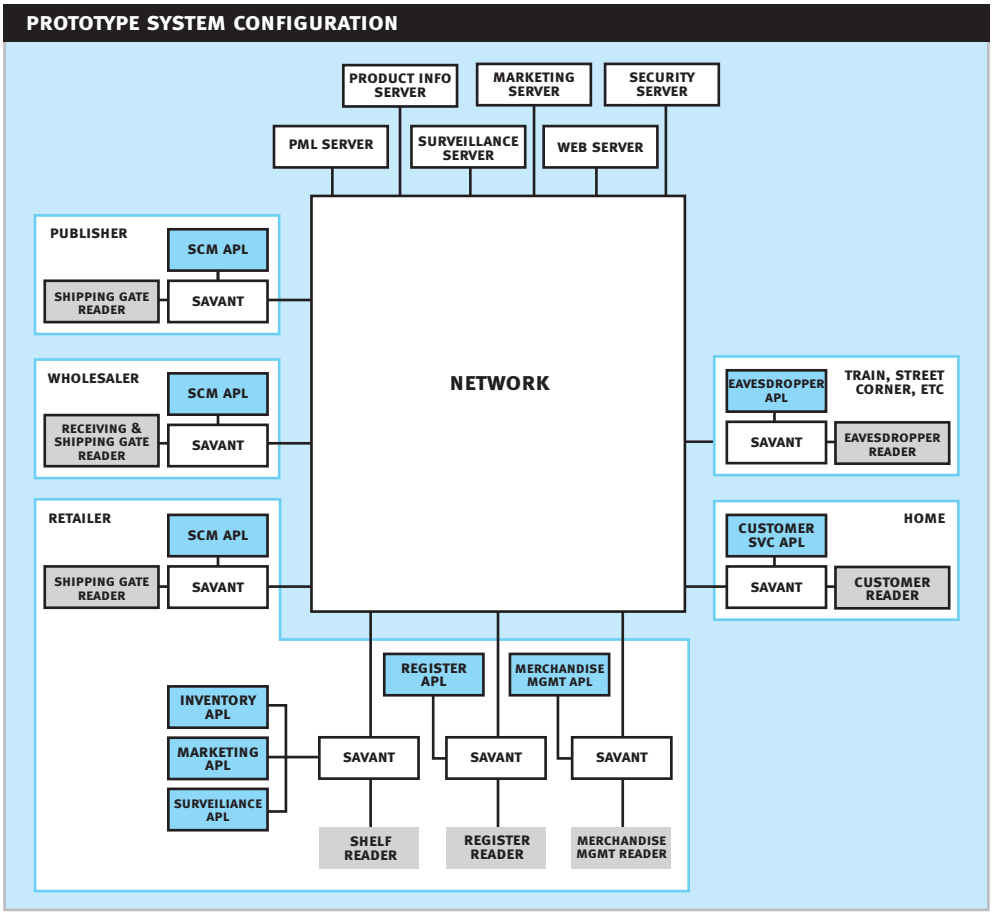
System Configuration
DNP, Sun, and NTT cooperatively developed a prototype system targeted for the publication business. The system covers scenarios for all participants in the business, namely publishers, wholesale merchants, bookstores, and consumers. The actual scenarios implemented includes circulation management between publishers, wholesale merchants, and book stores, automatic inventory control inside a book store, marketing (consumer tracking within a book store), shoplift prevention, shopping history management, and customer services. In addition to these applications, a privacy protection system was also developed.

The purpose of this prototype is twofold. First, is to clearly identify technical issues associated with applying Auto-ID technology to publication business through evaluation of features and performance. Second is to clearly identify real-world operational issues by providing a working ground for discussion by publication industry personnel and consumers.

Figures 7 and 8 shows the exterior and the configuration of the prototype system, respectively. The numbers in the figure 8 indicate the following: (1) circulation management among publishers, wholesale merchant, and book stores, (2) inventory in a book store, (3) marketing, (4) shoplift prevention, (5) cash register, (6) merchandise management, (7) customer services, and (8) privacy protection.

Figure 7: Prototype System Exterior

Figure 8: Corresponds to the numbers in Table 1



Section 5.2 describes each of the above scenarios in detail. Table 2 shows the distribution of development tasks among the three companies.

Table 2

DEVELOPMENT RESPONSIBILITIES		
TASK		**OWNER**
Application Scenario Design		Dai Nippon Printing
Hardware	– RFID	Dai Nippon Printing
	– Smart Shelves	Dai Nippon Printing
Software	– SCM	Sun Microsystems
	– Store Inventory	Sun Microsystems
	– Store Marketing	NTT Corporation
	– Store Anti-theft	NTT Corporation
	– Cash Register	NTT Corporation
	– Merchandise Mgmt.	NTT Corporation
	– Customer Services	NTT Corporation
	– Privacy Protection	NTT Corporation

RFID and Smart Shelves

The specification of the RFID tags used in the prototype is shown below. Figure 9 shows a book with a tag attached to it.

Figure 9: Book with a RFID Tag

RFID TAG
Accuwave by Dai Nippon Printing, K. K.

IC: Philips I-CODE SL-I
RFID Antenna size: 76 x 45 mm
Method of attachment: by adhesive
epc: UID (64 bits) or set to 64 bits in user area

Two types of smart shelves were developed for the prototype.

1. Prototype 1
Prototype 1 smart shelf uses mid-range readers that are approved by Japanese radio law at the time when development was began. Each antenna was dedicated to a given application. Figure 10 shows the exterior of this shelf.

Table 3

PROTOTYPE 1	
RF reader:	Feig MR100 (output fixed to 1 W)
Antenna:	Feig pad antenna (340x240 mm), passive resonance antenna used to extend effective range
Number of books detectable:	20 per shelf
Number of shelves:	two for insertion, one for stacking

2. Prototype 2
Prototype 2 smart shelf uses long range readers to improve the number of objects that can be read at one time. For cost cutting measure, one reader multiplex among five antennas. As shown in figures 11 and 12, passive antennas are placed not only to extend effective range, but also to adjust shift in resonance point that occurs from mutual inductance among nearby RFID tags when many tags enter the communication range. The placement of antennas and the shelf exterior are shown in figures 13 and 14, respectively.

Table 4

PROTOTYPE 2	
RF reader:	Feig MR100 (output fixed to 1 W)
Antenna:	Feig pad antenna (340x240 mm), passive resonance antenna used to extend effective range
Number of books detectable:	20 per shelf
Number of shelves:	two for insertion, one for stacking

Figure 10

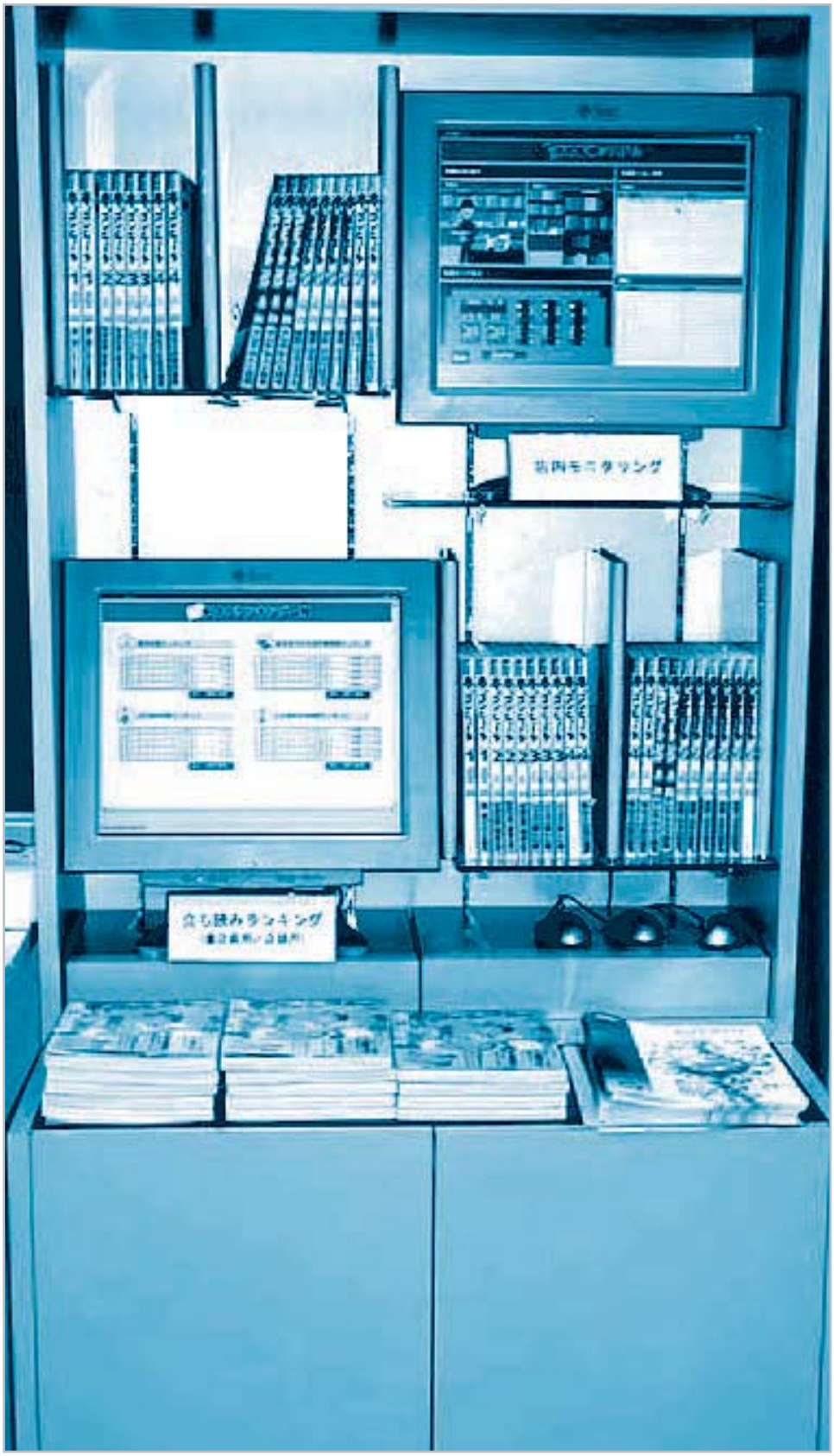


Figure 11

INSERTION SHELF

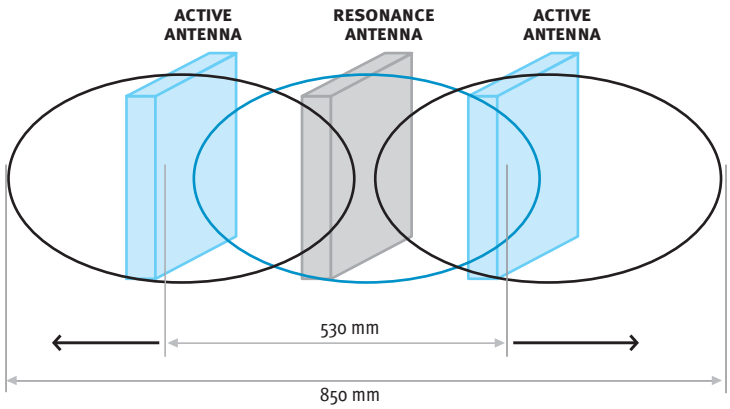


Figure 12

STACKING SHELF

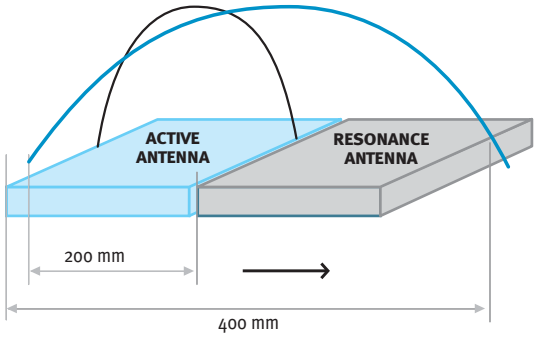


Figure 13

ANTENNA PLAMENT

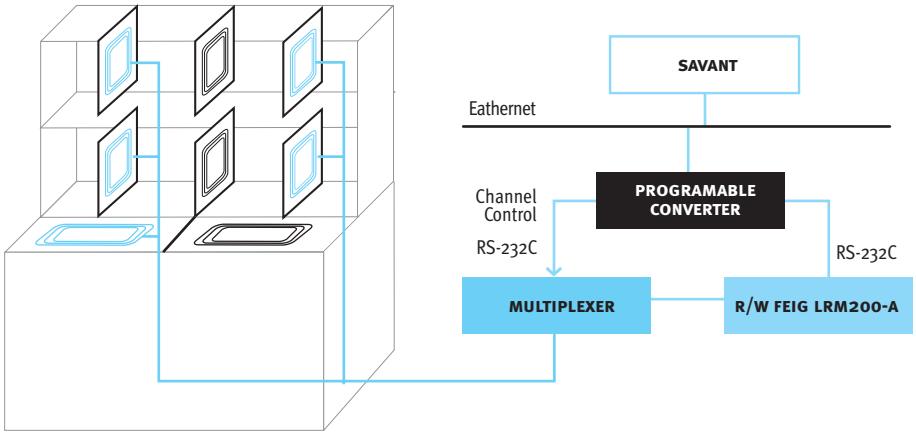


Figure 14

SMART SHELF (PROTOTYPE II)

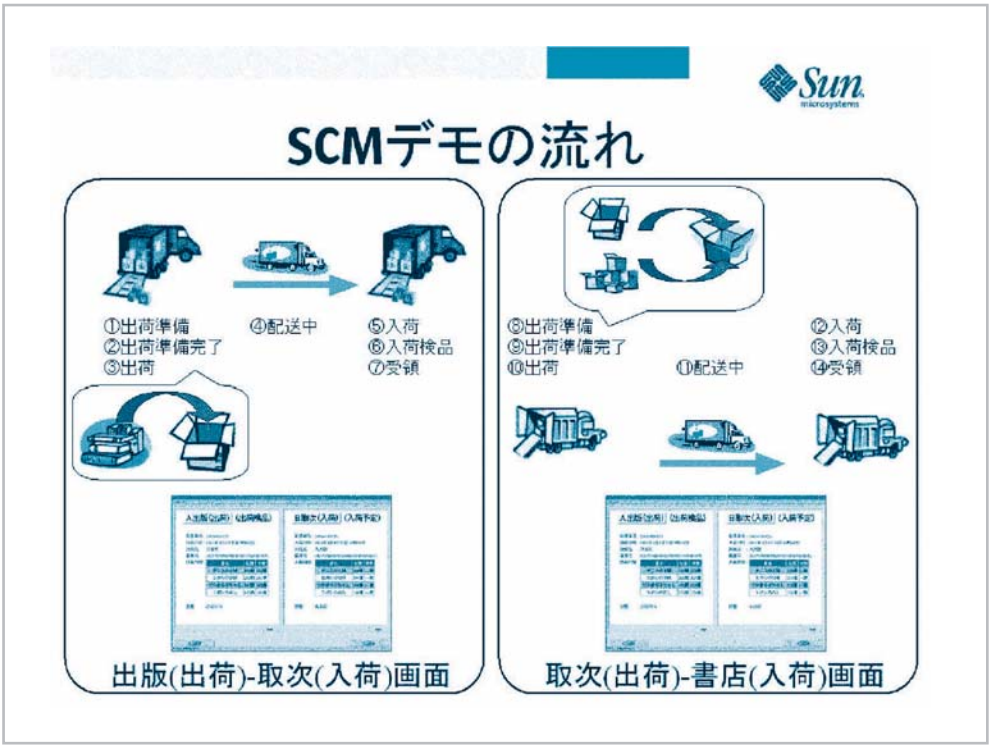
5.2. Demonstration Scenarios

1. SCM

Auto-ID provides for more efficient operations by each of the participants in publication industry, as well as a solution for optimal supply chain, which requires cooperation by all of the participants. The prototype system demonstrates applications of Auto-ID to distribution tasks along the supply chain from publishers, through wholesale merchants, to book stores.

This scenario consists of two processes: the distribution process from publishers to wholesale merchants, and that from wholesale merchants to book stores. These processes, in turn, consist of four steps: (1) outbound merchandise inspection, (2) shipment, (3) inbound merchandise inspection, and (4) reception. Also, as shown on figure 15, the prototype follows the actual operation that merchandise shipped from publishers are first unpacked and sorted at wholesale merchant before being shipped to bookstores.

Figure 15: SCM Demo



At step (1) outbound merchandise inspection, a RFID tag is attached to the outside of the package, and is associated with the list of the package's contents, which was checked against the RFID of the items that are actually packed (Figure 16). Once the package is verified and leaves the outbound inspection gate of the publisher, the status of the package become (2) “in transit.” At this point, information such as departure time and expected time of arrival may be shared among the shipper and the receiver. When the package arrives at the wholesale merchant, (3) inbound merchandise inspection takes place, and detects any discrepancies in the packages contents (figure 17). Because Auto-ID identifies individual item, it can detect the change even if a book has been replaced with a different copy of the same title. Once the package passes inbound inspection, its contents will be (4) received. In the prototype system, the reception status, like shipping status, is shared in real time between the shipper and the receiver.

Figure 16: Shipment Inspection

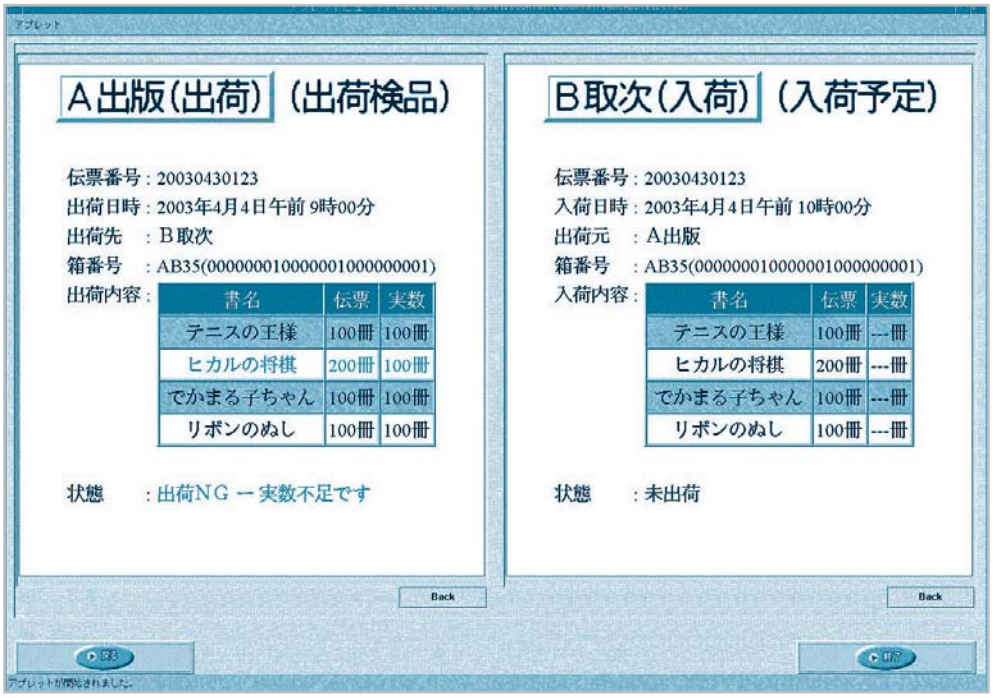
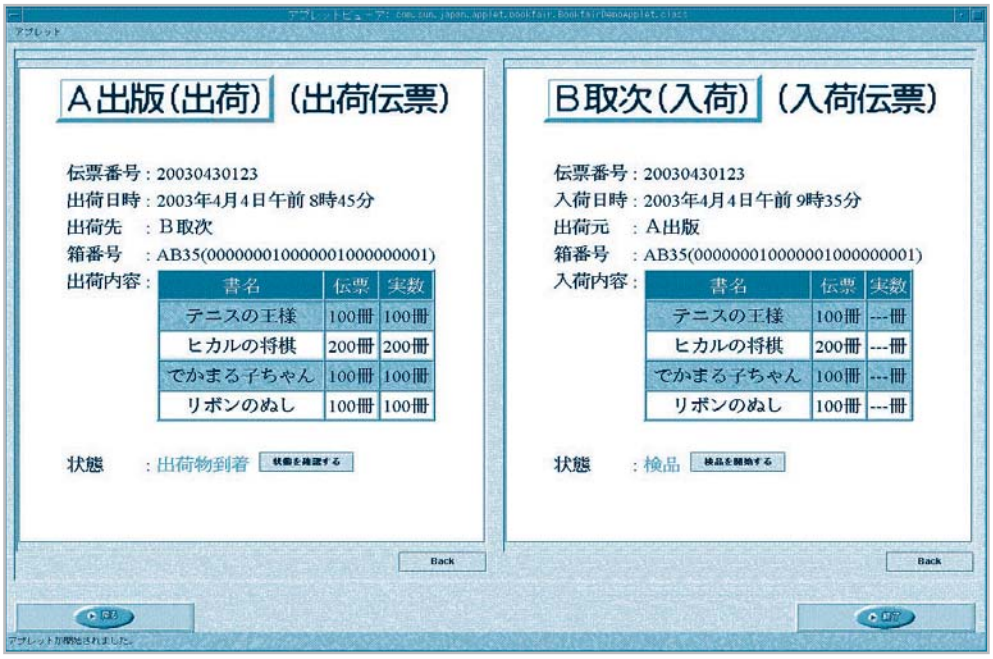


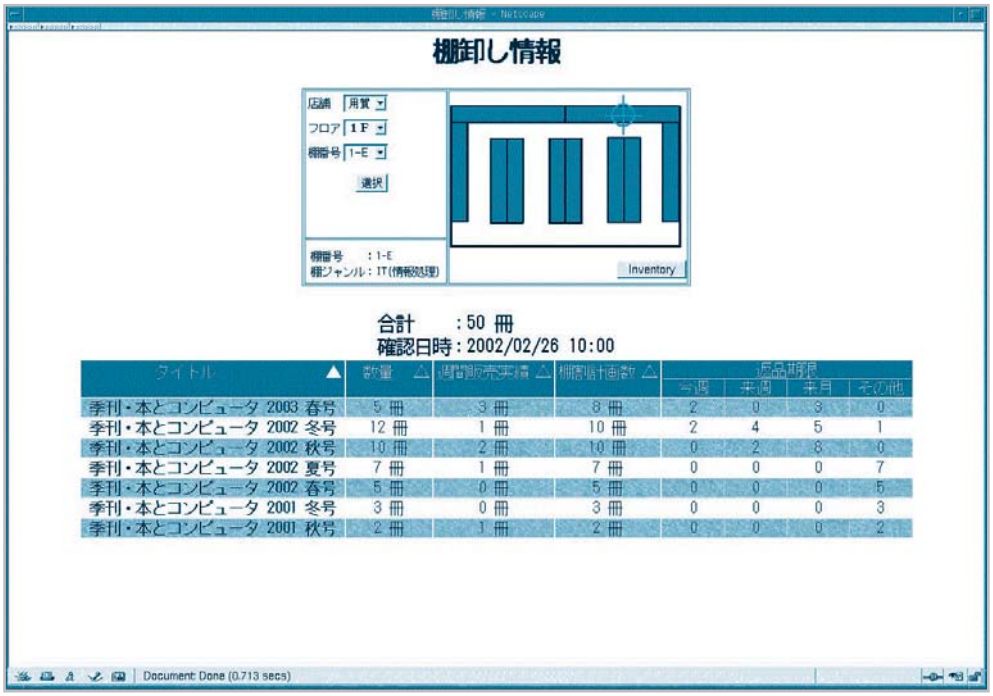
Figure 17: Receive Inspection



2. Taking an Inventory at a Book Store

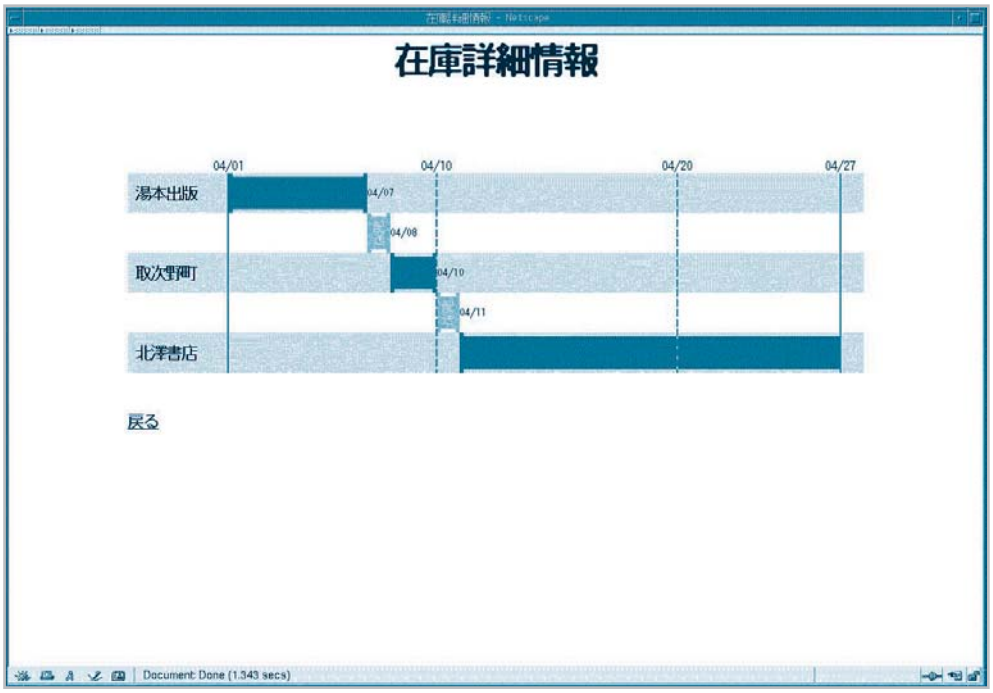
Using tagged books and smart shelves, an inventory may be taken at any time. In addition, automatic identification of in-stock books by smart shelves greatly reduces the time required to take an inventory. On the prototype system, an inventory may be taken at a click of a button. It will read the tags of the books on the shelves, tally up the numbers, and displays each title on screen, along with the number of copies in stock, number of copies sold, number of time that it was browsed, from where it was ordered, return deadline information (Figure 18).

Figure 18: Inventory Demo



For each book that has undergone inventory, its information is managed together with other information gathered from its supply chain. As an example, the prototype system can display the distribution history for each book.

Figure 19: Book Circulation History



3. In-Store Marketing

The prototype system collects three types of information that were unavailable from traditional POS systems: browse count, average browse time, and average time for a sale. They are collected in real time by following the movement of each book in a bookstore, “top five ranking” for each data is displayed (Figure 20.)

Figure 20: Rankig Display

Clicking on an entry will show the information about the selected book, including graphs showing its rank for past 30 days.

4. Shoplift Prevention

The prototype implements monitoring system to track customer behavior based on movement of each book – removal from, and return to a shelf, purchase, etc.

Upon removal of a book from a shelf, monitoring displays show the information about the book and an indication that it is being browsed (Figure 22). When the customer buys the book, the display shows an animated indication (Figure 23).

When a large quantity of books are removed from a shelf simultaneously, the display shows an indication that a possible shoplifting is taking place, and at the same time, the smart shelf plays a “Thank you” sound (Figure 24).

Figure 21: Graph Display

Figure 22: Browse Screen

Figure 23: Sale

Figure 24: Removal of Many Books

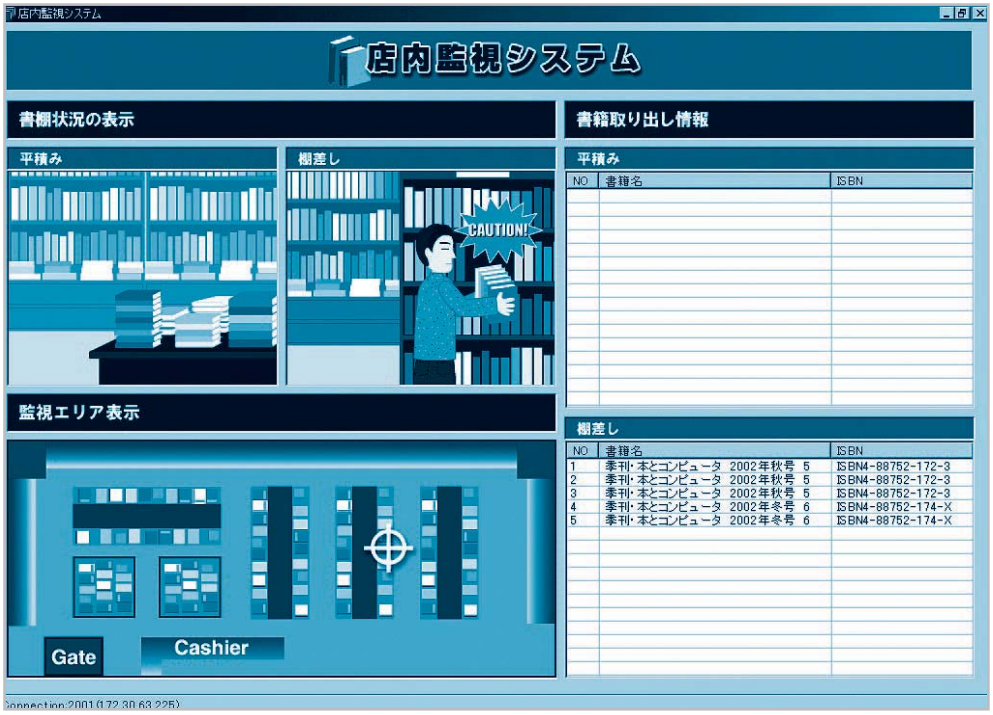


Figure 25: Check-out

5. Cash Register

During check-out with barcodes, each item must be read individually. In the prototype, multiple items can be read at a time, have information for each item (price, tax, etc.), and tally up the results quickly.

6. Merchandise Management

Traditionally, each participant in book distribution route individually maintained information about the same merchandise (date received, return deadline, sales record, etc.). The prototype implements a mechanism that consolidates merchandise management into a single database on a network, with each item searchable by using EPC as the key.

With the prototype, one can easily verify information, like date received and return deadline, by passing an item through a reader, instead of having to shuffle through paper slips by hand (Figure 26). This scheme has other potential uses, such as verification of sales of record by a used book shop.

7. Customer Services

Of the many conceivable customer services, the prototype implements some that publishers may provide to customers who purchased their books.

By holding up a purchased book to readers located in a store or in a home, the EPC is sent to the publisher's web site through a savant (figure 27), allowing access to reserved services (figure 28), such as e-book offers, special coupons, bulletin boards, next-issue information, and online registration.

Access to reserved services may be restricted on per-book basis, depending on the sales record or book type. For example, the prototype does not allow access to reserved services to unpurchased books such as those that were stolen (figure 29).

Figure 26: Product Verification

Figure 27: Publisher Web Site (purchase check)

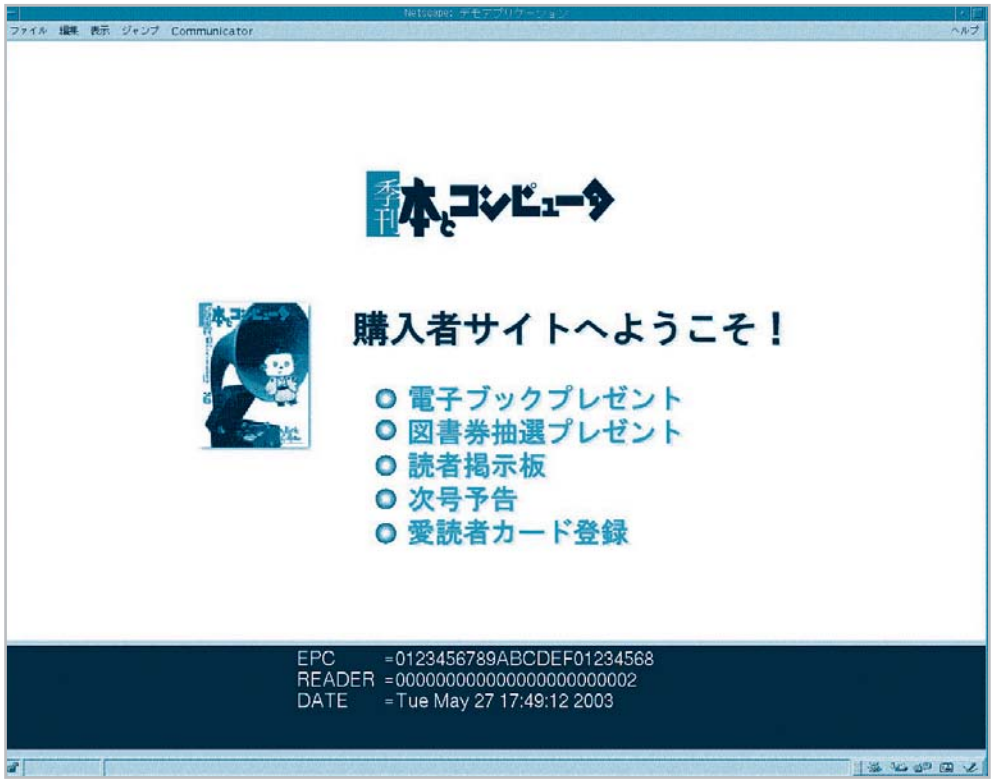


Figure 28: Publisher Web Site (Authentication Successful)

Figure 29: Publisher Web Site (Authentication Failed)

8. Privacy Protection

Of the two privacy issues described in section 4.2, the prototype implements protection against (1), leakage of information on personal properties.

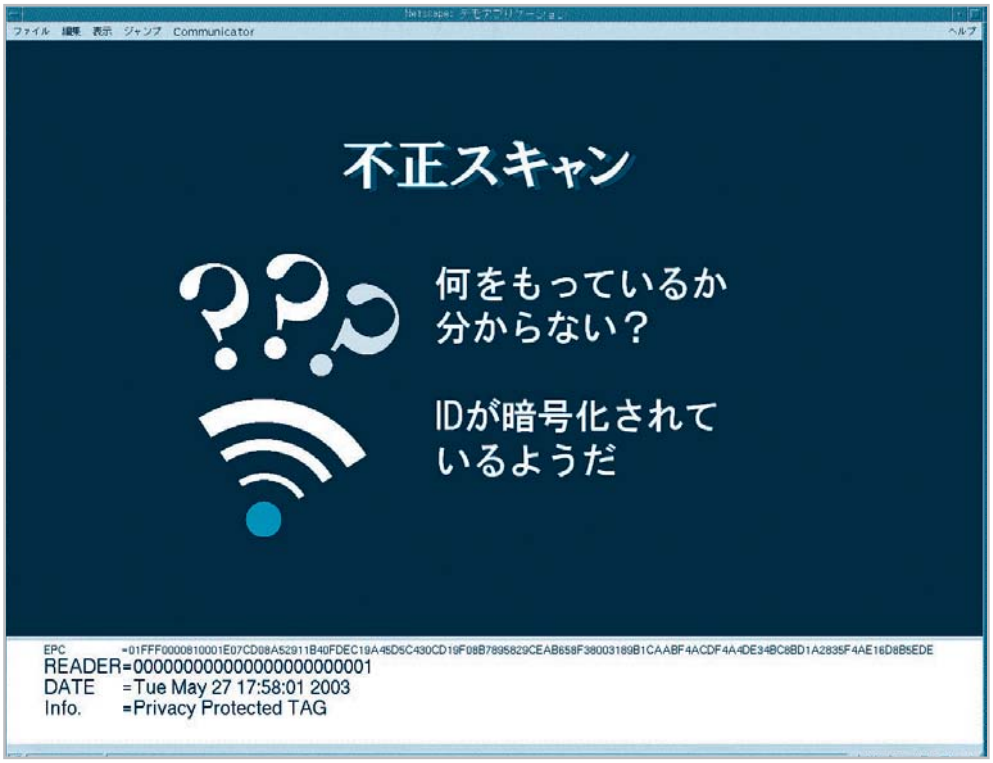
As shown in figure 30, having a book with RFID that contains regular EPC™ allows an eavesdropper to read the EPC™, and find out the title of the book. Having an obstacle, or being sufficiently far from the reader prevents eavesdropping. Disabling the RFID tag at the time of sale also prevents eavesdropping, but it also prevents post-sale uses of the tag, mentioned above.

On the other hand, if the RFID tag of the book contains a Anonymous-EPC™, as discussed in 4.2, it becomes impossible for an eavesdropper to discover the book's title because the EPC™ is encrypted (figure 31). Even in this case, reserved services can be accessed by using the customer's reader, or readers that are registered with the security center (figure 28).

Registered readers sends the Anonymous-EPC™ to the security center via a savant. The security center replies with a decrypted EPC™ only if the reader has been authorized. In this way, the privacy is maintained while reserved customer services are still available.

Figure 30: Successful Eavesdropping

Figure 31: Failed Eavesdropping



6. CONCLUSION

This paper presented the results of the cooperative experiment conducted by DNP, SUN, and NTT. The issues existing in the Japanese publication business are addressed and the exploration ofhe applications of Auto-ID technologies were explored in order to solve them. The study covered the entire distribution channel, from publishers, through wholesale merchants and bookstores, to consumers, as well as the privacy issues after a book reaches its consumer. The study showed that Auto-ID technologies provides for very effective solutions to many problems in the industry. To verify and demonstrate potential solutions, a prototype system for a representative was developed. The prototype provided a open ground for discussion, and the evaluation of its features and performance revealed new technical and operational issues. As we strengthen our relationship with the publication industry, these issues and the input that we gained from the discussions will be addressed in future studies.

7. REFERENCES

1. **Understanding Distribution in Publication Industry.**
   Yokuwakaru Shuppan-Ryuutsuu no Shikumi, Mediapal, April 2003.

2. **Auto-ID Center.**
   http://www.autoidcenter.org

3. **D. L. Brock, "The Electronic Product Code (EPC™) – A Naming Scheme For Physical Objects".**
   White Paper MIT-AUTOID-WH-002, MIT Auto-ID Center, Jan. 2001.

4. **Oat Systems & MIT Auto-ID Center, "The Savant – Version 0.1 (Alpha)".**
   Technical Manual, MIT-AUTOID-TM-003, MIT Auto-ID Center, Feb. 2002.

5. **Oat Systems & MIT Auto-ID Center, "The Object Name Service – Version 0.5 (Beta)".**
   Technical Manual, MIT-AUTOID-TM-004, MIT Auto-ID Center, Feb. 2002.

6. **D.L. Brock, T.P. Milne, Y.Y. Kang & B.Lewis, "The Physical Markup Language".**
   White Paper MIT-AUTOID-WH-005, MIT Auto-ID Center, Jun. 2001.

7. **Newspaper of Newspapers.**
   ("Shinbun-no-shinbun"), 2001/11/09
   Five Publishers asked to Counter Comic Theft [in Japanese].

8. **Ministry of Economy, Trade, and Industries, 2002/10/15,**
   "Results of Survey on Theft in Book Stores" .
   http://www.meti.go.jp/policy/media_contents/downloadfiles/1024Manbiki_gaiyou.pdf
   [in Japanese].

9. **Nihon Keizai Shinbun, 2003/05/11, "Sunday Nikkei: Eyes Behind Book Shelves".**
   [in Japanese].

10. **Bunka Tsuusin, 2001/11/12, "Five Comic Book Publishers Asked to Counter Theft"**
    [in Japanese].

11. **"860MHz–960MHz Class I Radio Frequency Identification Tag Radio Frequency& Logical Communication Interface Specification Proposed Recommendation, Version 1.0.0"**
    Auto-ID Center Technical Report MIT-AUTOID-TR-007, November 2002.
    http://www.autoidcenter.org/publishedresearch/mit-autoid-tr007.pdf

12. **S. A. Weis, S. Sarma, R. Rivest & D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems".**
    First International Conference on Security in Pervasive Computing, 2003.

13. **A. Juels & R. Pappu, "Squealing Euros: Privacy Protection in RFID-Enabled Banknotes".**
    In R. Wright, ed., Financial Cryptography 2003 Springer-Verlag, 2003.

14. **S. A. Weis, "Security and Privacy in Radio-Frequency Identification Devices".**
    Masters Thesis. MIT. May, 2003.

15. **A. Juels, R.L. Rivest & M.Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy,"**
http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/blocker/blocker.pdf
In submission. 2003.

16. **A. Juels, "Privacy and Authentication in Low-Cost RFID Tags".**
http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/pt-rfid/pt-rfid.pdf
In submission. 2003.

17. **S. Kinoshita, F. Hoshino, T. Komuro, A. Fujimura & M. Ookubo, "Nonidentifiable Anonymous-ID Scheme for RFID Privacy Protection".**
Computer Security Symposium 2003, Oct. 2003 [in Japanese].

18. **L.R. Knudsen, "The Security of {Feistel} Ciphers with Six Rounds or Less".**
Journal of Cryptology: the journal of the International Association for Cryptologic Research, vol. 15, no. 3, pp. 207-222, 2002.

19. **T. Kobayashi, H. Morita, K. Kobayashi & F. Hoshino, "Fast Elliptic Curve Algorithm Combining Frobenius Map and Table Reference to Adapt to Higher Characteristic".**
EUROCRYPT '99, May 1999 Proceedings, Lecture Notes in Computer Science, vol. 1592, pp. 176-189, 1999.

20. **M. Abe & T. Okamoto, "A Signature Scheme with Message Recovery as Secure as Discrete Logarithm".**
ASIACRYPT '99, November 1999 Proceedings, Lecture Notes in Computer Science, vol. 1716, pp. 3 78—389, 1999.

21. **D. Boneh, H. Shacham & B. Lynn, "Short signatures from the Weil pairing".**
ASIACRYPT '01, pages 514-532, LNCS no. 2139, 2001.

22. **M. Ohkubo, K. Suzuki & S. Kinoshita, "Cryptographic Approach to "Privacy-Friendly" Tag".**
To be appeared in RFID privacy workshop @ MIT.

Designed by Foxner. www.foxner.com