EPC System for Safe & Secure Supply Chain and How it is applied

An Analysis from Japanese Cases

Tatsuya Inaba

Auto-ID Labs White Paper WP-BIZAPP-026

Tatsuya Inaba
Research Associate
Keio University

Contact:

Auto-ID Lab Japan
Keio University
5322 Endo, Fujisawa
Kanagawa 252-8520 Japan

Phone: +81 3 3516 0620
Fax: +81 3 3516 0652

E-Mail: info@autoid.sfc.keio.ac.jp
Internet: http://www.auto-id.jp/

Business Processes & Applications

Executive Summary

Threats in supply chains, such as counterfeiting, product piracy and product recall, are ubiquitous, and Japan is no exception to this trend. In addition, these threats are not limited to industrial products; supply chains of agricultural products are also under threat. In order to eliminate these threats, various efforts have been made, some of which are the applications enabled by the EPC System, a technology that connects the physical world with the information world.

In this paper, we first analyze safe and secure supply chain issues in Japan and identify the fundamental issues through abstracting these issues. Then, we analyze how the EPC System works effectively to deal with these issues and propose potential research topics that can enhance the security level of supply chains. Although this study starts from issues in Japan, since those issues can be generalized, the analyses and proposals are applicable to issues in other countries/regions.

1. Introduction

Safety and security of the supply chain is one of the concerns in Japanese society, and efforts to improve safety and security have been made by both public and private sectors for years [1][2][3]. The importance of safety and security of the supply chain is often argued in the context of food safety and security. This is because the society learned the importance from the past bitter experiences, such as the Bovine Spongiform Encephalopathy (BSE or Mad Cow Disease) epidemic and the fake labeling of agricultural products issues [4][5]. In the arguments of these issues, two points are often highlighted. The first is whether producers/manufacturers make products appropriately or not, and the second is whether the products are distributed securely. In addition, since we learned that the fact that authentic products are traded securely in the legitimate supply chain is not sufficient from the drug contamination case, the argument of the traceability after shipment from producers/manufacturers is included in the second point. We make these arguments as a background and categorize safe and secure supply chain issues into three: 1) issues about the authenticity of the products (counterfeit), 2) issues about the legality of the product trade (illegal trade), and 3) issues about the status of the product after shipment (wrong status).

Regarding the counterfeit issues, fake products made outside of Japan and brought to Japan becomes increasingly common these days. Since counterfeiting is sophisticated, the actual damage is not known. According the World Trade Organization (WTO), total damage of counterfeiting in Japan would be about 2.3 trillion Japanese yens [6]. In addition to this fake product issue, we include issues regarding labels on the product, such as re-labeling, substitution, fake labeling, as parts of counterfeit issues.

Illegal trade consists of gray market and black market, both of which are also problems in Japan. A gray market is created when products are sold in the different markets through different channels from the market and channels through which the original manufacturers and the authorized distributors intend to distribute. With the progress of international parcel services, e-business and Internet auction, the way products are shipped become dynamic and it is difficult for the original manufacturers and authorized distributors to keep track of their products, which could be a foundation of the gray market. Not only that, this complexity of the distribution channels also can cause emergence of the black market.

The ultimate goal of realizing safe and secure supply chains is to deliver safe and secure products to the end consumers. Because of this, the ability to guarantee the quality of the products and eliminate wrong status products even after shipment from the manufacturers or producers is crucial. Wrong status can be both a short term issue and a long term issue. For short term, wrong status could be expired products or mishandling of the inappropriate products, such that low quality products somehow enter the legitimate supply chain. On the

other hand, long term issues include the issue that products have some kind of defects that are not known now but will be known in the future. Contaminated drugs are a good example of this long term issue.

These are the issues about the “products,” which are categorized into “physical objects.” However, these issues are not limited to “physical objects”; both physical objects and information about the objects need to be considered to resolve these issues. As a technology to connect physical things with information, the EPC System is expected to solve these issues effectively and achieve the safe and secure supply chain.

In this paper, we will introduce emerging supply chain issues in Japan first, analyze the nature of these issues, and then explain how the EPC system improves safety and security of the supply chain effectively. In addition, we will propose types of measures to improve safety and security using the EPC system based on the characteristics of the products and supply chains, and briefly introduce potential research topics in the EPC system.

2. Issues in Japan

2.1. Counterfeit

Fake labeling of agricultural products

Fake labeling of agricultural products became famous when the Bovine Spongiform Encephalopathy (BSE or Mad Cow Disease) epidemic hit Japan. At that time, sales of Japanese beef plunged suddenly because people were afraid of eating beef. To help the industry the Japanese government decided to subsidize companies that deal with Japanese beef. The subsidy was paid corresponding to the amount of beef that the company had and the company had to dispose of the beef if it wanted to receive the subsidy. However one company that wholesaled both Japanese beef and imported beef illicitly put fake labels on the imported beef, claiming it to be domestic beef, in order to fraudulently exploit the subsidy. The case was found by inside information, and the company was condemned for the dishonesty. Moreover, people boycotted its products, and eventually the company had to leave the market [4]. This company was not the only case for this kind of exploitation of government subsidy; there are several similar cases in which companies put fake labels to get government money illicitly [5].

There is another fake labeling case as well. In Japan, locations and species of the agricultural products become the “brand,” in just the same way as the SONY brand for televisions and Toyota for automotives. Each brand has its reputations, most of which are deliciousness of the brand product. Therefore, even though they may look exactly the same,

the consumer is willing to pay more money to Kobe Beef than the beef from an unknown region. There are several famous brands in most of the agricultural products, and, because of the higher margin that they can get by dealing with these famous brands, producers are working hard to keep the quality of the products and the image of the brands. However, since it is difficult to tell the difference, say, between two pieces of meat, malicious producers, wholesalers, repackagers, and/or retailers put fake labels on the packages and mislead consumers [5].

Putting aside the issue that this fake labeling is done by producers, because it is more of an ethical issue than a safe and secure supply chain issue, there are still many issues in this fake labeling: Companies in the supply chain can easily remove the labels from what they buy from their suppliers and put fake labels onto them. If there is a mechanism to stop this fake labeling, not only industrious producers of the brand products can secure their brand and get fair profits but also consumers can buy products after confirming that what they buy is what they see on the labels.

Fake Products

Fake products cause tremendous damage to both consumers and manufacturers of the products. According to JETRO (Japan External Trade Organization), a broad range of products, such as electronic home appliances, machine tools, auto-parts, office equipment, motorbikes, toys, cosmetics, and food, are being counterfeited [7]. There are two main characteristics in the Japanese fake product cases: 1) fake products of the Japanese manufacturers' brand are made in the foreign countries and sold in both foreign and domestic market, and 2) fake products of the foreign manufacturers, such as luxury goods manufacturer, are made in the foreign countries and sold in the domestic market. Since fake products are made in foreign countries in both cases, anti-counterfeit measures taken by the Japanese government is to work on the countries in which fake products are made to settle intellectual property legislations and enforce strict regulations, and to work together with the international community to develop international laws and guidelines for these fake product issues. At the same time, the government as well as industry organizations produce public campaigns and educate consumers not to buy fake products [8].

At the same time, the private sector is also taking anti-counterfeit measures. A common approach is to use physical anti-counterfeit measures, such as holograms and invisible ultra-violet ink [9][10]. Although they are effective to some extent, these physical anti-counterfeit measures are also copied by the counterfeiters. Since Auto-ID technology is said to be effective for anti-counterfeit, expectations of the technology are high in many industries. Recently the electronic appliance industry started a new consortium called the Home Appliance Electronic Tag Consortium. The goal of this consortium is to develop industry rules and guidelines about how to use RFID, and it is said that one of the purposes is to study how RFID can be used for anti-counterfeit [11].

2.2. Illegal trade

Gray market

If the market is different, the price of the same product, even though they are in the same condition, may not be the same. This difference mainly comes from the difference in tariffs and exchange rates. This price differentiation was not a big issue when the distribution of the products was controlled by the manufacturers and the authorized distributors. However, with the development of the Internet and the progress of the transportation network, the movement of both humans and products is becoming dynamic, and, as a result, products are sold in many markets through the channels that the original manufacturers and the authorized distribution channel companies do not intend. This kind of practice is called parallel import; and this unintended distribution has brought many consequences; such as deteriorating distributor relations, brand image, profits, sales force morale, and customer service efforts; and is becoming a major issue [12][13][14].

In addition to these gray market issues caused by parallel import, there is another gray market issue that is created by the discount stores that buy excess inventory from the authorized distribution channel companies with cheaper wholesaler price and sell them to consumers with discount price. Whether this practice becomes an issue or not is dependent on each industry. For example, in the home electronic appliance industry, these kinds of discount stores became one of the major distribution channels for the manufacturers; manufacturers and discount stores became interdependent. Now those discount stores realize low cost procurement by directly purchasing products from manufacturers instead of buying excess inventory from the authorized distribution channels. It is not gray anymore. In other industries, on the other hand, manufacturers are still making efforts not to lower brand image caused by the proliferation of the unintended cheap products in the market and trying to maintain the authorized distribution channel [15].

Although it is not necessarily illegal as indicated in its name, gray market can become a barrier for the manufacturers that want to deliver safe and secure products to the end customers. In this sense, we will argue that this gray market phenomenon is a kind of safe and secure supply chain issue in this paper.

Black Market

Although national television networks sometimes broadcast news about criminal organizations that steal luxury cars and smuggle them to foreign market or sell them as used cars [16][17], the black market, in which stolen and illegal products are traded, is not an immediate threat to ordinary people in Japan. However, it is not something that we can ignore completely because it is said that shoplifted products are sometimes sold in the secondary market, which can be categorized as a black market issue. All kinds of goods sold in stores can become a target for shoplifting, but, among them, books are a major target for

shoplifters. According to the statistics from the Ministry of Economy, Trade and Industry, the average damage of shoplifting is about 2.1 million Japanese yens per book store. Considering the fact that the number of the book stores in Japan is about 80,000, the total damage of shoplifting adds up to 150 billion Japanese yens [18]. Since selling the stolen books is not a major reason for the shoplifting, it is not likely that this huge amount of books floods into the legitimate market. However, since the secondary market for books has been well developed in Japan, the possibility of the stolen books' re-entering the market is high.

2.3. Wrong status

Infection caused by contaminated blood or blood-origin drugs

Transmission of HIV and other blood-borne viruses through blood transfusions or the use of human origin drugs became a huge social problem in Japan, too [19]. To respond to the situation, the industry and the government have been tightening the quality check of the raw materials of the drugs, which are human and animal blood or organs, in order to stop manufacturing contaminated products. Also they have developed after infection action rules and regulations. Those include identifying the root cause of the infection and affected patients, and treating them as soon as possible.

What makes this issue more complicated is the existence of the infectious prion diseases, such as Variant Creutzfeldt-Jakob Disease (vCJD). vCJD is said to be a disease when a human is infected with BSE. Although researchers are working hard to investigate the infectious mechanism and the treatment, since so far the number of patients is not so many, the entire process of studying the disease is not as smooth as is expected. One of the characteristics known so far is the long latency period that the disease has. The exact period is not clear, but it is said to be as long as 20 years [20][21]. This piece of information gives a tremendous impact to the community because the effects of long latency period may grow exponentially. When one patient who is given human or animal origin drugs is found to be infected with vCJD, the possibility of having other patients is high; those who took the same drug could be infected. However, since the latency period is so long, it is difficult to envision the entire impact by only using conventional record retention system. The long latency period also becomes a cause of secondary and tertiary infections, assuming that the patients may donate their blood and organs.

To respond to the current and future problem, the Ministry of Health, Labor and Welfare issued a new regulation enacted on July 31, 2003. In the new regulation, manufacturers of human origin drugs have to retain information of their customers, which are pharmacies and hospitals, for thirty years, and pharmacies and hospitals that used the drugs have to retain information about their patients for ten years. Manufacturers also have to retain customer information for ten years if the drug is of animal origin [22][22].

The existing concept of drug recall is to collect defective drugs from the drug market. This process is not perfect but effective considering the nature of the current drug problem. However, this recall process may not work well for the contaminated drugs that can cause diseases like vCJD, whose infectious mechanism is not totally known and latency period is very long. Other measures such as new government regulations as well as new technologies such as Auto-ID technology will be required to effectively minimize the impact of this kind of diseases.

3. Nature of the Issues

3.1. Analysis of threats of safe and secure supply chain

This subsection explores the nature of the safe and secure supply chain issues and how the EPC System can work effectively on the nature of the issues.

Figure 1 depicts a supply chain from producer/manufacturer to consumer. This figure is showing the entities in the supply chain and the general flow of products but is not limiting the relations of each entity. For example, a producer/manufacturer may ship directly to its consumers in some cases, and a wholesaler may sell products to another wholesaler in other cases. In addition, there might be a case in which a person may buy products from a retailer and sell them through an internet auction. At the time the person and the retailer work as a retailer and a wholesaler, respectively.

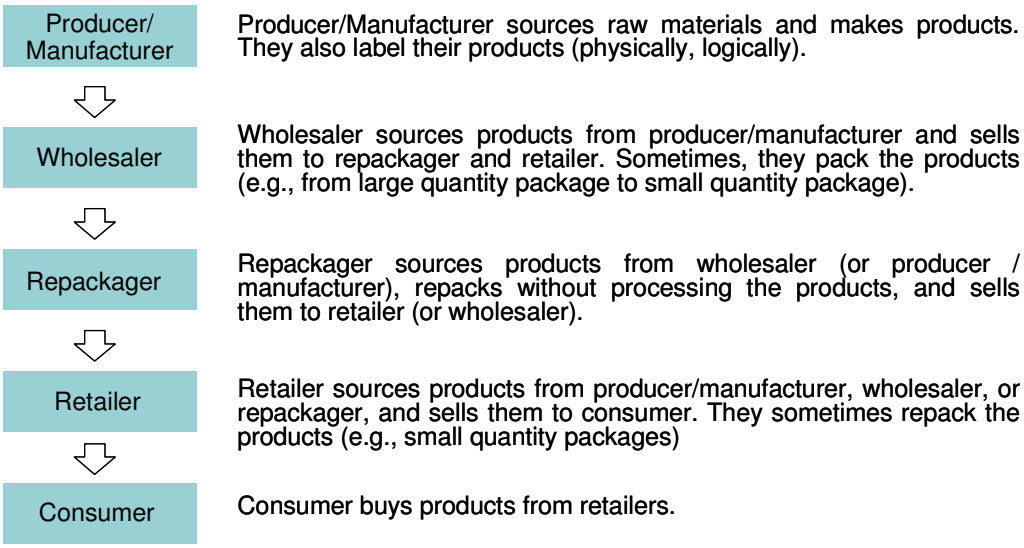

Figure 1 Supply chain

Each entity in the supply chain has its own vulnerabilities in terms of safety and security of the supply chain (Table 1). Although it is not necessarily illegal, we include gray market issues as parts of safe and secure supply chain issues because 1) these issues cause both manufacturers and consumers problems and 2) we believe that supply chain members should be notified of the risk of the products before they actually sell them to their customers.

Table 1 Threats of supply chain security and entry points of them

		Producer/ Manufacturer	Wholesaler	Repackager	Retailer	Consumer
Counterfeit	Fake label	✖		✖		
	Adulteration	✖		✖		
	Re-label		✖		✖	
	Substitute		✖		✖	
	Fake product		✖	✖	✖	
Illegal trade	Stolen		✖	✖	✖	
	Gray market		✖	✖	✖	
Wrong status	Scrapped		✖	✖	✖	
	Recall/Contamination	✖		✖		

3.2. Analysis of securing supply chain applications

3.2.1. Basic applications

In order to realize safe and secure supply chains, companies have to do two types of verifications, physical verification and informational verification, with three applications. Firstly, each entity of the supply chain must verify the authenticity and appropriateness of the products (hereafter "status verification") on hand in order not to catch problematic products (On-site status verification). This practice includes both physical verification, such as checking if the packaging is broken, and information verification, such as the serial number verification. It is also important for consignees to verify the products they will receive before they physically receive the products by getting prepositioning information about the products from shippers, such as serial number and certificates (Track). Secondly, each entity of the supply chain as well as regulatory bodies must identify the entry point of the problematic products, assess the impact of the case, eliminate the products, and expose the parties that introduced the problematic products. This can be implemented by accumulating the track information (Trace).

Table 2 Basic applications for securing supply chain

APPLICATION	VERIFICATION TYPE	DESCRIPTION
On-site status verification	Physical	Verify authenticity by checking the ingredient of the product (component elements, DNA etc.), verify packages for broken packaging, broken seals etc.
	Informational	Verify status by checking information about the products, such as serial number, certificate, trade history, etc
Track	Informational	Verify status by checking prepositioning information
Trace	Informational	Identify suspicious products, eliminate the products, and stop proliferation of the products

3.2.2. Analysis of intentional mislabeling by Manufacturer/Producer

In the case that the producer/manufacturer labels their products (either physically or logically) and that the products are shipped directly to their customers, if the producer/manufacturer ships low quality products or substandard products, saying that they are appropriate, it is impossible to detect the problem by solely using informational status verification. For example, if a producer of Kobe beef falsely sells normal beef as Kobe beef, downstream members of the supply chain can not recognize the issue, and other physical status

verification measures, such as DNA testing, may be required. Considering the difficulty of using physical status verification measures at the individual consumer level, government and/or industry bodies need to implement effective measures. For example, government agencies or organizations from the public sector sample the product and check the status, or issue the licenses to the authorized producers/manufacturers if it meets a certain qualification; or trusted third parties certify the authenticity of both producers/manufacturers and their products so that consumers can have information to judge the quality of the products. As analyzed different nature of the fake labeling done by producer/manufacturer, we put these issues out of scope of this study.

Table 3 Threats of the supply chain security and entry points of them (Revised)

		Producer/ Manufacturer	Wholesaler	Repackager	Retailer	Consumer
Counterfeit	Fake label	(Out of scope)		✖		
	Adulteration	(Out of scope)		✖		
	Re-label		✖		✖	
	Substitute		✖		✖	
	Fake product		✖	✖	✖	
Illegal trade	Stolen		✖	✖	✖	
	Gray market		✖	✖	✖	
Wrong status	Scrapped		✖	✖	✖	
	Recall/Contamination	✖		✖		

3.3. Measures to enable suggested applications

3.3.1. Mass serialization

In order to verify the legitimacy of the product status, the ability to uniquely specify the individual products with unique identifiers or serial numbers is essential. Moreover, to have a

unique identifier itself can show the authenticity of the product to some extent. The problem of the unique identifier will be discussed in the next subsection.

3.3.2. Verification by using information

Importance and constraints of physical status verification

In the previous subsection, we explained that to specify the individual product is crucial for product status verification and that mass serialization is necessary for this purpose. One verification method is a physical status verification, with which those who check the product status confirm the physical characteristics of the products, such as breaks of the shrink wrap and clarity of the hologram. However, it is not enough because these physical characteristics can also be copied by parties such as criminal organizations. Moreover, to check these physical characteristics may delay the speed of the supply chain, which can undermine the benefit of using RFID. Therefore, informational verification, especially using automated data capturing, is required.

Status verification by using information

Introduction of information to verify the legitimacy of the product status can improve the verification speed and accuracy of verification, but to introduce a new concept, “information” in this case, will add a new vulnerability because this “information” could be wrong. Therefore, it is necessary to verify the status of the “information” as well.

There are several pieces of information that can be used for product verification. One fundamental one is the unique identifier. However, if the unique identifier is scanned by anyone, it is easily duplicated. In the case that the numbering scheme is too simple, identifiers may be forged by malicious parties. In order to improve security levels regarding this unique identifier, it is necessary to employ some kind of access control and encryption technologies when identifiers are read. In addition, to manage the lifecycle of unique identifiers and to verify the legitimacy of the identifiers including detecting duplication will be necessary to improve the security level. Related information of the products is also used for status verification. It includes information such as certificates and trade history of the product. Just the same as unique identifiers, this information also needs to have its status verified its status before it is used for product status verification.

In addition, since all or part of the information used to verify the product status is supposed to be managed by using network resources, the availability of the network at each check point in the supply chain is also important. Types of network availability are 1) always available (on-line), 2) sometimes available (on/off-line), and 3) not available (off-line). Security levels will become lower according to this order. This is because supply chain members need to use real time information when they verify the information legitimacy but they can not do so

without the network. In addition, it is necessary to guarantee the authenticity of the information that links unique identifiers to network resources and information.

Track and trace enabled by the related information

We proposed three applications for product status verification in the previous subsection: on-site status verification, track, and trace. These three applications, especially track and trace, require information to uniquely identify the product (unique identifiers), and to describe the attributes of the product (related information). Regarding tracking, originally it is used to streamline the shipping process, and it also improves the accuracy of the shipment. In this case, unique identifiers will be sent from a shipper to a consignee by using communication systems such as EDI. The consignee uses this information to confirm whether the product is what it ordered, prepare for receipt of the shipment, and to trigger permission of the new orders from its customers. This is a short description of tracking applications for shipment, but tracking for product verification can be implemented easily by adding a few more processes, such as verification of the unique identifiers and certificate/trade history documents, to this tracking for shipment processes.

Trace, on the other hand, is an application using the product trail archive. Therefore, once you use unique identifiers and product related information for tracking, you can implement trace by just archiving the same information. There are several ways to implement trace, and they are categorized based on the location of the archive information. This difference also affects the speed of the retrieval and difficulty of the implementation. These are three different types of trace:

- store information about track in one place and retrieve trace information (Centralized),
- store information about track in each of the supply chain member and retrieve trace information by visiting each member with the unique identifier as a key (De-centralized), and
- circulate trace information with the product and retrieve trace information by checking locally stored information (Pedigree).

Each measure has its own advantages and disadvantages and is chosen based on the requirements from the product and the industry.

As explained here, track and trace applications to verify the status of the products, can be implemented by using unique identifiers and related information that describes attributes of the products.

3.3.3. Tampering and re-labeling alert

In the previous subsection, we explained that it is essential to check the appearance of the products, such as tampering and re-labeling, in terms of product status verification and that this check has a down side for slowing down the speed of the supply chain if it is done through human intervention. In order to resolve this disadvantage, it will be useful to detect package tampering automatically, alert and convert the change into information signals. This automatic detection can be done with RFID tags. One example of this kind of tags is the type used for international shipments, such as e-seals. E-seals can emit signals when they detect tampering of the container [23][24].

3.4. Mapping measures to supply chain issues

Based on the argument in this section, we map security measures (3.3) onto potential threats in the supply chain (2). Table 4 shows the relation.

Table 4 Measures to secure supply chain

		Measures covered by the EPC System			Measures not covered
		Mass serialization	Related information	Tamper & Relabel alert	Physical verification
Counterfeit	Fake label	✖	✖		
	Adulteration	✖	✖		
	Re-label			✖	✖
	Substitute			✖	✖
	Fake product	✖	✖	✖	✖
Illegal trade	Stolen	✖	✖		
	Gray market	✖	✖		
Wrong status	Scrapped	✖	✖	✖	✖
	Recall/Contamination	✖	✖		

3.5. Functions of the EPC System necessary for safe and secure supply chain

In the previous section, we explained that there are three effective measures in securing supply chain. They are:

1) to introduce unique identifiers for confirmation of individual products (Mass serialization),
2) to confirm the legitimacy of the product status by using information including both unique identifiers and related information such as certificate and trade history (Related information), and
3) to detect breach of the products and/or product packaging by automatically alerting and converting physical changes into information (Tampering and re-labeling alert).

Then what kind of functions are required for the EPC System to realize these measures? Table 5 shows the relation between proposed measures and components that constitute the EPC System.

Table 5 Mapping of security measures to EPC System components

SECURITY MEASURES		EPC	Tag	Reader	Middle ware	EPC-IS	ONS
Mass serialization	Encryption	✖	✖	✖	✖		✖
	Access control		✖	✖	✖		
	ID management					✖	✖
Related information	Electronic document verification					✖	
	Product status management					✖	✖
Tamper & Relabel alert	Tamper proof tag	✖	✖	✖			

This map is also used to make decisions when a company has to prioritize security measures for its products. For example, if a product has characteristics that the number of shipments is many but the price is not high, then naturally the manufacturer will take low functionality/low price tags with high functionality network system because the more it ships its products, the higher the total cost of the system becomes. This is just one example for the product characteristics, but characteristics of the supply chain, including network availability, also affect the choice of the security measures. In the next chapter, we will qualitatively analyze

what kind of measures companies should take in order to make their supply chain safe and secure.

4. Choice of security measures

There are several measures to secure supply chain, and these measures are different in their effect, cost, and difficulty of implementation. Each measure has its own advantages and disadvantages, and companies choose measures considering the characteristics of the product and its supply chain to make the effect feasible and sufficient. In addition, the availability of the network is also important when companies select security measures as explained in the previous chapter. In this chapter, we will analyze the relation between these characteristics and security measures.

4.1. Relation between characteristics of product and security measures

Products have many characteristics that will affect the choice of security measures. They are:

- products sold with outer package (e.g., cosmetics, drugs) and without outer package (e.g., auto parts, second hand distribution of luxury goods),
- products with different monetary value, and
- products that have privacy issues with non line of sight read (e.g., drugs).

Packaging of the product is one important factor when companies select security measures. When products are usually shipped without outer packages, the company has to consider the possibility of the tag detachment. Rather than sticking a tag on the product, it may be effective to embed a tag into the product or directly engrave/inscribe the necessary information onto the product so that the binding between the product and the unique identifier and related information can be guaranteed. The impact here is that if the company chooses a solution that uses engraved two-dimensional barcodes as a carrier of unique identifiers, it can not use high functionality that can be provided by RFID tags and has to rely on the network system for high functionalities such as tag data encryption.

Next is the monetary value of the product. When comparing high and low functionality, it is more expensive to use the high functionality tags than the low functionality ones. Although it depends on the number of products to be shipped and the level of the required security, relatively expensive products may justify the use of high functionality (expensive) tags, whereas low functionality (cheap) tags will be used for relatively cheap products. If you need

to meet a security level for the supply chain system, more sophisticated functionality is required for the network system of the low functionality tag solution than that of the high functionality tag solution.

Privacy and security issues will become important if the information stored in the tag can be easily read without any access control. Suppose a manufacturer makes controlled drugs like morphine and it adopts to use low functionality RFID tags that do not have access control functionality, anyone can get the tag information by just scanning the tags, and the possibility of the theft by criminal organizations will become higher. In such a case, the company should pay more attention to the security and should choose high functionality tags that have access control functionality or at least remove product information from the unique identifier so that companies that do not have business contracts with the manufacturer cannot identify the product type.

4.2. Relation between characteristics of supply chain and security measures

Supply chains also have many characteristics that will affect the choice of security measures. They are:

- simple distribution (e.g., fresh produce)
- complex distribution (e.g., medical equipment, parallel import)
- secondary distribution (e.g., internet auction)

In the simple distributions, since originally the number of participants is small and the distribution route is rather static, the possibility of having adverse events will be small. Therefore, relatively low security solutions will be sufficient for this kind of distribution. Whereas, in the complex distributions, since not only the total length and time of the product movement will be long but also the route becomes dynamic, the chances of counterfeited product entry and parallel import product entry will become higher. In the distribution that has these characteristics, the assumption that the network connectivity is always available may not be true all the time. Therefore, solutions with high tag functionality and low network dependency will be feasible.

In the secondary distribution, such as Internet auction, it is also expected that products are routed dynamically. But if ordinary consumers are assumed to work as either wholesalers or retailers, high functionality tag solution may not be appropriate. This is because high functionality tag solution is effective in securing the information stored in the tag with technologies like access control, but the solution requires complex network system including expensive high functionality readers. As a result, consumers can not read the information stored in the tag, update the status of the unique identifiers and related information, or verify

the status of the product. In such a case, a solution with which a unique identifier can be read easily and the product is verified easily is required even if the security level might be sacrificed to some extent.

4.3. Relation between network dependency and security measures

We touched a little on the importance of the network availability in analyzing characteristics of the supply chain. In this subsection, we will show the relation between network availability and possible security measures thoroughly.

Table 6 Network availability and security measures

SECURITY MEASURES		NETWORK AVAILABILITY		
		Off line	On & Off	On line
Mass serialization	Schematic	✖	✖	✖
	Encryption		✖	✖
	Access control		✖	✖
	ID management (cached)		✖	✖
	ID management (real time)			✖
Related information	Electronic document verification		✖	✖
	Product status management (cached)		✖	✖
	Product status management (real time)			✖
Tamper & Relabel alert	Tamper proof tag	✖	✖	✖

Off-line means that measures do not require network access. For example, to verify whether a tag can be read with a legitimate identifier that follow the identifier's schematic rule and to detect whether the product package is broken or not can be a basis of entire security measures. On/off-line means that the system has network access but not always available. In this case, measures that use network access can be used, but the security level is not as high as that of on-line. The reason why the security level is considered to be low is because the network is used to exchange access control key and verify against a list of illegitimate (or

legitimate) identifiers, but real time information is not always available to check the legitimacy of identifiers, including identifier duplications. Lastly, on-line means that network, and consequently necessary information, is always available and higher security can be achieved.

As shown in the table, the choice of the security measures depends on availability of the network. For example, if a high functionality solution with tag encryption is adapted in a supply chain without network availability, the solution will work so long as the encryption is not broken, but once it is broken, it can not change security keys through network and therefore, the security level becomes extremely low. A similar problem is the security level of the network, since all the measures that use the network access assume the security of the network itself, the security level of the measure becomes lower if the network is not secure enough because secret information could be exposed to unknown third parties. Therefore, if companies in the supply chain can not implement sufficient network security because of some constraints, the entire security level of the supply chain will be lower.

5. Potential research topics

The effectiveness of the EPC System to realize the safe and secure supply chain was explained in section 3, but the EPC components that have been standardized or are being standardized may not be sufficient to realize all the measures proposed in the chapter. That is, studies regarding the EPC System must be done to realize the proposal. Moreover, these studies are not enough; business rules and guidelines, such as document formats to exchange related information, will be necessary in order to implement the security measures. In this chapter, we will introduce potential research topics in both EPC System components and outside of EPC System components.

5.1. Mass serialization

ID Encryption

When companies verify the product status by using information, to keep the legitimacy of the unique identifiers is crucial. If it is read by anyone and duplicated easily, the entire security measures proposed in chapter 3 are undermined. Even if a malicious third party gets the identifier from the tag, but if it is encrypted and the party can not decrypt and get the real unique identifier that is used to connect the identifier with the object, companies can reduce the risk of counterfeiting. Encryption alone does not solve identifier duplication, but at least obscuring identifier schema will prevent malicious parties from generating schematically

legitimate identifiers. Therefore, with the help of identifier duplication check, which is a function of the identifier management, companies can improve security level of supply chains.

The mechanism is also effective for some of the privacy issues. One of the privacy concerns is that anyone who has an RFID reader may be able to get the information of the product you have through casual contact. But if the identifier is encrypted and does not have any meaning by itself, that will solve this casual contact privacy issue.

Access control

The same problem described in the ID encryption part can be solved by implementing access control to the tag. By access control, tag access is only allowed to the supply chain members and/or the authorized parties. Through this access control, not everyone can get the information stored in the tag, and the possibility of duplication and forging by malicious third parties will become lower.

Moreover, just the same as ID encryption, this access control function is also effective in dealing with privacy concerns. One of the strong solutions to protect privacy in the current RFID implementation is the function to kill the tag (i.e. to render it permanently inoperable), e.g. at the checkout, when the products are bought by consumers. But if the access of the tag is properly controlled, consumers do not need to kill the tag and they may be able to utilize tag information in maintaining the products, collecting the quality information, and recycling the product.

Regarding methods of access control, access control technologies developed for the Internet security and smart card security can be applied to this RFID security.

Identifier management

ID encryption and access control are the measures to prevent unique identifiers from being exposed unnecessarily, but this identifier management is a measure to deal with after exposure or in the case of no access limitation to tags. Even if identifiers are not protected with encryption or access control, furthermore if there is a mechanism to detect duplicates and wrong status (e.g., identifiers of stolen products are found or identifiers of used and scrapped products are found), it will improve safety and security of the supply chain because the possibilities of suspicious activities or system errors are high in those cases. The mechanism will require network services to manage the lifecycle of the identifier as well as requiring new functionality from the EPC System components.

5.2. Related information to secure supply chain

Electronic document validation

It is useful to use product related information, such as certificate and trade history to secure the supply chain. However, this information could also be counterfeited or duplicated; therefore, measures to prevent these malicious activities need to be identified and eliminated. Unfortunately current EPC System does not have functionalities to exchange this kind of related information; therefore, it is necessary either to standardize this information within the EPC System or to develop industry standards by analyzing business processes to secure the supply chain. One example of this related information is the electronic pedigree document discussed in the Healthcare and Life science Business Action Group (HLS BAG) at EPCglobal [27].

Product status management

Just the same as the argument in 5.1, even after shipment, products in the wrong status should be eliminated from the supply chain. Wrong status includes product recall and expiry. In order to realize this function, information about the products need to be exchanged. This exchange of the related information can be done by using EPC-IS, a component in the EPC System, but business processes that are out side of the EPC System standards scope also need to be agreed among the companies in the supply chain.

In addition, trade history information is not always queried and updated through the network considering the availability of the network. One of the current EPC System's design policies is to limit functions of tags in order to make them cheap and to control related information using the network, such as the internet [28]. But even without network connectivity, companies may have to verify the status of the products, and, in such a case, some amount of information might be stored in the tags for redundancy purpose. With the new air protocol, user memory areas became available, but guidelines of how to use the user memory, including memory allocation and fine-grained access controls, should be necessary to use the storage capacity in these tags [29].

ONS Security

As analyzed in 3.3, to guarantee the authenticity of the information that links the unique identifiers with network resources is necessary. In the EPC System, the only resolver function currently provided is the Object Naming Service (ONS), which does not have the mechanism to authenticate both client and network resource information. If the supply chains are static and members of the supply chain have settled business deals, this resolver function might not be required; however, if the transaction is dynamic, securing the resolver mechanism becomes mandatory. It is planned that 'EPC Discovery Services' will provide serial-level lookup services for tagged objects throughout their lifecycle. Massive scalability, secure access controls, authentication and the ability to prevent unauthorized data mining of the serial-level tracking data are some of the business requirements for Discovery Services.

5.3. Tampering and re-labeling alert

Tamper-evident tag

In case a unique identifier of the product is attached not directly to the product but the package of the product, managing the information about the product is not enough to guarantee the safety and security of the product. This is because the package may be opened and the product inside is switched for other products. Of course this package tampering may be detected through manual checks, but, since it will delay the supply chain process, some measures to detect package tampering and send it to the system managing the supply chain is required. With this function, package tampering will be detected without spoiling the merits of the RFID system.

6. Conclusion

In this study, we explored issues that threaten supply chains in Japan, analyzing the nature of the issues, and showed the potentials of using the EPC System as a solution to the issues. In arguing how the EPC System is used to secure the chain, we proposed three potential applications to make supply chain safe and secure and explained how each application is effective in addressing supply chain vulnerabilities. Moreover, we showed the relation between characteristics of the supply chain factors, such as products, distribution, and network availability and the recommended measures. We also introduced potential research topics to realize the proposed applications.

Although we analyzed both supply chain issues and the EPC System as a solution, more careful and quantitative analysis is required to apply the EPC System to an actual issue because each case must have different supply chain members, damage structure, and urgency; and these factors are interdependent. One of the important factors is the security level that the system needs to realize. Of course, it is better if members of the chain can achieve the level, but, even if they can not, they may lower the possibility of having adverse events to some extent.

This section started from the introduction of the supply chain issues in Japan, but, since these issues can be applied to other parts of the globe, we believe all the arguments made in this paper will be useful when analyzing the safe and secure supply chain issues throughout the world.

References

[1] Nikkei Ryutsu Shimbun MJ, “e-retail special – IT as enabler of safe and secure life, Food traceability is available at store front,” September 21, 2005 (in Japanese)

[2] Nikkei Ryutsu Shimbun MJ, “e-retail special – RFID is coming! Attendees are counted by using RFID embedded ticket at EXPO,” September 21, 2005 (in Japanese)

[3] Nikkei Sangyo Shimbun, “SANRIO called for help to combat counterfeit products to customs offices,” August 29, 2005 (in Japanese)

[4] Nikkei Shimbun, “Snow Brand Food decided liquidation,” April 27, 2002 (in Japanese)

[5] Nikkei Shimbun, “Reasons of stumble (1) Trust toward food manufacturers,” August 13, 2002 (in Japanese)

[6] Sankei Shimbun, “Japanese government asks China for strict law enforcement to IPR abuse,” December 4, 2001 (in Japanese)

[7] Intellectual Property Rights Department JETRO Beijing, http://www.jetro-pkip.org/ (in Japanese)

[8] Japan Ministry of Economy, Trade and Industry, “Issues and measures for counterfeit products,“ October 16, 2002 (in Japanese) http://www.kantei.go.jp/jp/singi/titeki/dai7/7siryou4.pdf

[9] SECUTAG, http://www.secutag.com/

[10] Hewlett-Packard, UV/IR Invisible Ink System, http://www.hp.com/oeminkjet/products/C6121A/overview.html

[11] Nikkei Ryutsu Shimbun, “Home appliance industry set up a consortium to study RFID – Four companies including SONY will develop industry guidelines,” November 30, 2005 (in Japanese)

[12] P. E. Chaudhry, M. G. Walsh, “Gray Marketing of Pharmaceuticals,” Journal of Health Care Marketing Fall 1995 Vol. 15, No.3 pp.18-22

[13] M. B. Myers, “Incidents of Gray Market Activity Among U.S. Exporters: Occurrence, Characteristics, and Consequences,” Journal of International Business Studies 30.1 (First Quarter 1999): pp. 105 – 128

[14] S. Tamer Cavusgil, Ed Sikora, “How Multinationals Can Counter Gray Market Imports,” Columbia Journal of World Business Winter pp. 75 – 85

[15] K. Tsuchida, “A study of discrimination of sales in E-Business and limitation of re-selling,” Waseda Hougakkai, Waseda Hogaku Vol 76(3) March 20, 2001 pp 209 – 238 (in Japanese)

[16] Nikkei Shimbun, “Arrest organized crime of automotive. Damage is JPN 1 billion and 46 are arrested,” October 10, 2005 (in Japanese)

[17] Nikkei Shimbun, “Worst record of automotive theft. 64,000 cases a year,” January 20, 2004 (in Japanese)

[18] Japan Ministry of Economy, Trade and Industry, “Survey for shoplifting at bookstore,” October 25, 2002 (in Japanese)

[19] Defense council for Osaka HIV law suit, International Conference for AIDS caused by drug contamination, Tokyo, Sairyu-sha, November 20, 1998 (in Japanese)

[20] BBC, "vCJD may take 30 years to show," BBC News, March 22, 2001, http://news.bbc.co.uk/1/hi/health/1235241.stm

[21] Japan Ministry of Health, Welfare and Labor, “(Draft) Regulation for human and animal origin drugs record retention,” January 10, 2003 (in Japanese)

[22] Japan Ministry of Health, Labor, and Welfare, Pharmaceutical Affairs Law, 2002, §68.9 (in Japanese)

[23] R. Hadow, “E-seals and RFID,” The Journal of Commerce, October 24, 2004 p58

[24] P. Tirschwell, “Container seals: Here they come,” The Journal of Commerce, September 19, 2005, p52

[25] Y. Yamada, “Marking technology trend and point of utilizing marking technology,” Tool Engineer, September 2005 pp84-85 (in Japanese)

[26] S. Brandner, “Privacy as an after thought,” NetworkWorld, March 1, 2004 p.24

[27] EPCglobal, Healthcare Life Science Business Action Group (HLS BAG), http://www.epcglobalinc.org/action_groups/hls_bag.html

[28] Auto-ID Center, “The Networked Physical World,” White Paper, http://www.autoidlabs.org/whitepapers/mit-autoid-wh-001.pdf

[29] EPCglobal, EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz Version 1.0.9, http://www.epcglobalinc.org/standards_technology/EPCglobal2UHFRFIDProtocolV109122005.pdf, January 2005

