博士論文

Multi-level Empirical Studies on the Network Externalities of Information Security

(情報セキュリティのネットワーク外部性に関するマルチレベルの実証研究)

Jenjarrussakul Bongkot

ジェンチャラッサクン　ボンコット

Thesis Supervisor　Professor Kanta MATSUURA

指導教員　松浦 幹太　教授

December 12, 2014

Acknowledgement

First of all, I would like to express my deep gratitude to my supervisor, Professor Kanta Matsuura, for his kindness since my first day at Matsuura Laboratory. Under his supervision, he taught me how to deal with the research and gave me a number of opportunities to meet many well-known researchers in the research fields. He always encouraged and guided me with his meaningful advices throughout my Master and Doctoral courses. Without his kind supports, I would never have such a precious experience in my life.

I would like to thank my advisors, Professor Toru Asami and Professor Hiroshi Esaki for their valuable comments regarding my research direction. I would also like to express my special thanks to Professor Hideyuki Tanaka for his meaningful and valuable supports on my research.

I would like to express my sincere appreciation to Takahito Kikuchi, the owner of poitan.net, for his supportive information regarding loyalty program at poitan.net. Your supports are very meaningful to our study on firm-level network externalities.

My sincere thanks also go to Matsuura Laboratory's secretaries; Sae Nakano and Kayoko Ogura for their kind supports and encouragement. They always helped me every time I had problems while living in Japan. My life in Japan and Matsuura Laboratory would not be as smooth as I experienced without their helps.

I would like to express my appreciation to the past and present Matsuura laboratory's members; Takuro Hosoi, Satsuya Ohata, Feng Fei, Toshinori Usui, Kenjiro Nakata, Shiori Shinoda, Sun Da, Keisuke Katayama, Masahito Ishizaka, Takayoshi Hojo, Takao Murakami, Takahiro Matsuda, Peng Yang, Jacob Schuldt, Yasumasa Nakai, Yi Shi, Daiki Chiba, Shaojing Fu, Ken Ichikawa, Kenichi Yokote, Andreas Gutmann, and others, for their meaningful discussions and comments. Without everybody, I would not have such a remarkable time at Matsuura Laboratory. I would also like to thank my friends in Japan and those in Thailand for their helps and advices.

I would like to express my gratitude towards Tokyo Marine Kagami Memorial Foundation for the financial support and activities throughout my doctoral course. With supports from the foundation and its staffs, I could happily study in Japan.

Finally, my deepest thanks go to my family for their never ending love, support, and encouragement.

Abstract

Information technology (IT) is one of the role players nowadays. It is not only used to link businesses together, but also used to connect people from different parts of the world together. Such connectivity brings us a so-called *borderless* society which allows governments, businesses, and individuals to easily reach each other.

The expansion of the information network becomes an incentive for attackers to intrude into the system through system vulnerability and steal various kinds of information which is now considered as one of the valuable assets. With the interconnection between nodes in the network, security breaches at one of the nodes could affect other nodes via the interconnection.

Network externalities, thus, become one of very important topics in the field of information security. That is because the topic of network externalities is a study that focuses on consequence effects from the action of an individual on others. Actually, this is how the economic concepts are applied to the field of information security.

This thesis introduces our analyses regarding problems of network externalities in the field of information security. The analyses were conducted at two levels: national level and firm/operator level. The findings from our study show several important implications of the information security.

In the study regarding network externalities in the national level, we analyze the interdependency under information security risks. We use a two-step approach to analyze both sectoral and regional interdependencies under information security risks. In addition, the result collection process was introduced to suggest some empirical findings. Then we clarify the characteristics of interdependencies of information security from both sectoral and regional viewpoints. After that, the changes of interdependency after the occurrence of the Great East Japan Earthquake in March 2011 were also emphasized in our analyses. Furthermore, the analyses were done in both sectoral and regional perspectives.

According to our results in the sectoral perspective, the demand-side sectors can be classified into five classes due to their characteristics. In addition, most of the Japanese industries fall into the classes where consideration on interdependency from the regional perspective is required. In the regional perspective, the results of the analysis show that economic scale of a region has great influence on the characteristics of interdependency. The analysis results under the impact from the earthquake show importance of critical sectors. Furthermore, once such a disaster occurs, the damage to the information security could be expected in the area where the disaster occurs, as well as the region with the largest economic scale.

In the study regarding network externalities in the firm or operator level, we introduce an approach to analyze the security and the interconnectivity of the Japanese loyalty programs (LPs). Available online systems for the loyalty programs allow points or miles of loyalty programs to be considered as virtual currencies. Therefore, liquidity is what we consider besides security efforts and actual security levels of the loyalty program systems.

After that *linear regression analysis* is used to find implications regarding security and liquidity. In our work, we focus on the origin loyalty program since illegal exchanges originate from compromised LP accounts. We found that liquidity is significant to the impact on the loyalty program systems once the security incidents occur. Furthermore, we also found supportive evidences of an importance of network externalities from our analyses. The results also suggest operators of the loyalty programs to implement stronger security-related requirements for their systems. In addition, consideration on the level of security of their partners' systems is also recommended.

After studying network externalities in both national and firm/organization levels, we discuss more about network externalities. By this, we show how knowledge from our study at the national level can be used to provide more useful information and suggestions. We use the case of the network of loyalty programs as our example. To do so, we consider the average size of the expense on security countermeasures, the value of information security measure, and the sectoral characteristics of industries where the loyalty programs are operated. From our discussion, we found that industry 20, which includes airlines, might be the weakest link in the network of the Japanese loyalty programs. Operators from this industry are suggested to take actions in order to improve the security of their loyalty program systems. However, we still suggest other industries to pay attention to the matter of information security.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Overview and Motivation

Information technology (hereafter, IT) brings the convenience to all levels of organizations, firms, and individuals. It is a backbone of speedy and flexible communication, as well as various kinds of transactions worldwide. With these benefits, IT becomes one of the basic infrastructures among all sizes of businesses. The number of recent internet users, which includes users from a worldwide organizations to end-users, is one of the evidences of this fact. There are almost 3,000 millions of the internet users around the world[75][1]. Not only the bright side, IT might lead to massive loss once an intrusion occurs in any system.

According to the trend of internet security threat in 2013 by Symantec[148], it seems that the worldwide situation is getting worse. Compared to the trend in 2012, the trend of 2013 shows that it is the year of mega breach. Due to this report, the number of security breaches has increased by 62%. The top cause of data breach in 2013 was hacking. The breached data created risks not only directly for the corporations but also for individuals through their personal information stored there. Furthermore, Symantec also reported that the trend of zero-day vulnerabilities was also increased by 61% in 2013. Zero-day vulnerabilities let attackers silently threaten the systems. Attacker seeks for poor patch management systems or websites before invading and creating loss to those victims. Spear-phishing campaign was another kind of attacks which shows high trend in 2013. They found that this type of attack increases by 91% compared to the number in 2012. The spear-phishing campaign is a type of targeted attacks that directly attempt at specific groups of users. According to an article by Information-technology Promotion Agency, Japan (IPA), incidents from targeted-attack emails is the most serious type of threat in Japan[72]. With such activities, attackers can eventually complete its goal of breaching into the targeted organization. Once one of the users in a particular group is infected, it becomes so risky, and other connected systems or users would also be affected. These are only examples which could mean that the existing security might be insufficient due to increasing number of internet security threats.

Economics can explain some incentives that stimulate the creation of security threats[60]. As an effect of the great recession [2], the number of cybercrimes had increased due to scarcity in economics. Generally, to spend monetary resources in information security, vendors or organizations would make their decisions according to their business's profitability from that

[1] Number from the access on Oct 14, 2014.

[2] The great recession is “officially lasting from December 2007 to June 2009” [76].

investment[138]. However, during the period of recession, the benefit of an investment in security might not be so attractive. Such facts give huge opportunities to cyber criminals.

To make IT-related activities and the systems secure, *information security* (hereafter, IS) becomes one of the important elements in IT systems. IS has its main objective to protect information and information systems[110]. It also aims to provide confidentiality, integrity, and availability of the information in the information system. However, due to an emergence of new attack techniques, attackers could threaten the information and the system through their vulnerabilities. When the system is breached, the three properties of information security are broken. Therefore, the loss from security incidents would be introduced to the owner of that information system. In addition, as information systems are used to link systems together, the loss from any attack on one of the systems could affect their connected systems. The problem associated with such an expansion of the effect is called the problem of *network externalities* in the field of *economics of information security.*

The study of network externalities is one of the four main research areas in the field of economics of information security[9][10]. Basically, the area of network externalities is a study on security-related consequence of action of an agent on economically unrelated others [3]. Due to the use of the internet, we can hardly say that there is no externalities among systems.

In a cyber network, actions of an individual can introduce side effects to others. The influence from the action could be either positive or negative. Under a scenario that two parties have interdependency between each other, security investment by one of the parties also benefits its partner[66]. Likewise, an attack at one of the parties also affects its partners. Let's consider the case when firm A invests in security techniques to enhance protection of its system. Once the system of the firm A becomes stronger, vulnerability of the system would be decreased. It also means that the system becomes harder to attack. Hence, the attacker would change its target to systems with weaker protection. Although the threat probability at the system of the firm A decreases, its neighbors' systems could become more risky. This is an example of the negative effect. By contrast, if the system of the firm A is the weakest link among their connected parties, stronger protection of the system of the firm A would increase the security of the whole network. This is an example of the positive effect.

There are many areas of study regarding security and the problem of network externalities. Some studies in network externalities focus on the benefit of sharing information among parties in the network[55][67][93]. Gordon et al. found that sharing information among parties helps firms with reducing their investment in information security[55]. Furthermore, the level of information security also increases by sharing information. Hausken shows that information sharing and security investment by each firm are important factors to the security of interconnected parties[67]. Some consider the effects by using epidemic risk model. Especially, they consider the effects as epidemic risks when they study problems caused by malware[42][91].From such studies, a consideration of the effect from epidemic risks could help the owner of the system make a decision to invest or not to invest in security countermeasures.

Other three main research areas are *misaligned incentives*, *economics of vulnerability*, and *economics of privacy.*

Misaligned incentives is a study which considers a hidden action problem when one of the parties, who want to transact, takes unobservable actions that affect the outcome. Anderson introduced issues of security misaligned incentives by using the case of UK retail banking

[3] Economics definition of *externality* given by Investopedia is "A consequence of an economic activity that is experienced by unrelated third parties" [76].

and the concept of moral hazard to explain the failures and frauds within the systems[7]. He found that rather than lacking protection, the failure comes from an improper use of the system by the bank. Another intuitive example is a situation from 2000, when users would not spend much money on antivirus software and attackers focused on well-known websites like Amazon and Microsoft[11]. In other words, this topic concerns failures from poor security management of the system owner since that responsible owner does not suffer from the failure but its customers or others suffer.

Economics of vulnerability studies on hidden vulnerability in the systems, released products, etc. Researchers in this area concern questions such as whether or not information of vulnerability should be disclosed, would it be better to secretly keep information of vulnerability, how to deal with insurance premiums based on firm's exposure data, etc. Miller states that "Vulnerability information is a time-sensitive commodity"[101]. That is, a specific vulnerability information becomes nothing once it is disclosed. Anderson mentioned an answer to the question "who (i.e. attacker or defender) would be benefited from disclosure of vulnerability information?" in 2005[8]. From his study, under ideal scenario, he shows that both attackers and defenders would be equally benefited. Beside vulnerability disclosure, there is a system which helps providing information regarding the vulnerability of the released software or a system. Such a system is called *vulnerability market*. The use of vulnerability market brings advantages to both vendors and users of the affected products[9].

Finally, economics of privacy is a study on privacy problems which come from erosion of personal information in the system. The researches in this area try to explain why privacy-enhancing technologies fail in the market. The economics of privacy has long been interested by economists and lawyers[3]. After few decades, privacy intrusions and privacy protection techniques were also expanded in mid 1990s along with the expansion of IT. The new economics of privacy with formal micro-economic modeling which explains privacy in different aspects emerged approximately from year 2000.

Personal information has its own value. Some researchers consider it as an economic goods[2]. Generally, personal information is said to be sold in two markets; market for personal information and market for privacy. The market for personal information utilizes personal information by dealing with customer data, as well as giving price for the information. On the other hand, the market for privacy emphasizes more on how to offer privacy protection technologies, as well as enhancing those technologies. For example, a research that focuses on questions such as why people care about privacy and its erosion[114]. To answer to this question, Odlyzko explains that there is a high incentive on price discrimination regarding personal information in the cyber space. This is the result from the fact that vendors have high motivation to reduce customers' privacy and gain more information from their customers. Vendors of the e-commerce services can be used as an example to support such scenario very well. Enzmann and Schneider introduce a technique for a secure and privacy-enhanced loyalty system[44]. They research on the system which is claimed to be a privacy-friendly loyalty systems. The online vendor can use this system to issue loyalty points. However, the points and the purchase are unconditionally unlinked so that the vendor cannot track its customers' behaviors. Then the system provides the customers better privacy than system without such techniques. Furthermore, concerns on the price discrimination also appear in many related works[30][118][145].

In our researches, our concern focuses on the issue of network externalities. Issues regarding network externalities motivate us since the interrelationship or connection between systems has been dramatically expanded. Information can be transferred to another side of the world in just a few seconds. With such convenience, information systems becomes one of the basic infrastructures in modern business. Therefore, we can also expect that an occurrence of security incident at a specific system could cause catastrophic loss and impact at any system in the world.

In order to protect the information, proper security management should be done at each level of the system. Security policy of higher-level organizations should be considered differently from security policy for end users. That is because the level of affordability and concern are expected to be different between levels. To give proper advice to firms or systems in each level, an empirical study regarding each specific concern is needed. Luckily, in Japan, official data regarding information technology and information security are publicly provided.

To deal with loss from security incidents, organizations in all levels, including individual, seek their way to properly manage their information security resources. They might purchase some devices or softwares to protect their information and information systems. Beside that, they might find better ways to detect intrusion and malicious codes. These are only few examples of how an owner of a system invests in security. However, with limitation of their budget, one might not spend enough. On the other hand, those who are risk-averse regarding security might spend too much on their systems. In many cases, the more investment does not always mean that the most secure system has been introduced. That is because it also depends on how well those security resources are managed.

As mentioned above, security incidents can occur at any level and any size of organizations, including individuals. We classify levels of organizations as in Fig.1.1.

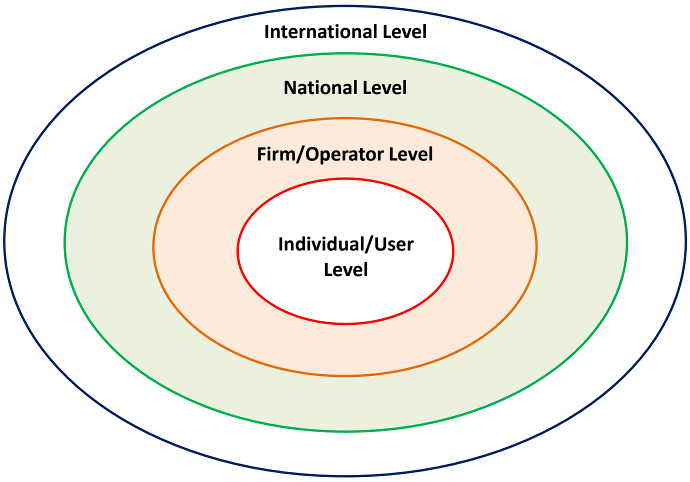


Figure 1.1: Multi-level of network externalities.

In Fig.1.1, the classification is done according to the size of elements in each level. However, the classification can be done from other perspectives. For example, in the second national strategy on information security ([109]), they consider level of organizations from the *national view point of Japan*. Thus, the classified level of elements in their strategy are Government agencies and local governments, Critical infrastructure, Enterprise, Individual, and Entity to entrust information[4]. For this case, the classification of elements in the strategy seems to be considered from the responsibilities of each element.

1.2 Outline and Summary of Contributions

In this thesis, we make contributions to the problems of network externalities in national and firm or operator levels. Fundamental knowledges and models regarding investment in information security are introduced in Chapter 2. These knowledges and models are important as they lead to several questions and inspire us to the information security-related issues (e.g. how to find proper proxy variable in our empirical studies) in our contributions. After that, we introduce our contributions according to their levels or sizes of the organizations.

- In Chapter 3, we focus on the topic regarding interdependency of the information security in sectoral and regional perspectives. We also study on the impact from the Great East Japan Earthquake on the interdependency of information security.

  In the context of an investment in information security, there are various concerns including problems of over- and under-investment in information security. To solve or reduce such problems, we must know the characteristics of the interdependency of information security between different industries, as well as regions. Knowing how information security of industries or regions connects between each other would help policy makers introducing more appropriate policies for the investment in information security. By contrast, it can also help predicting the impact when a serious security incident occurs at any system in the network.

  In our previous works (i.e. Publications 8 and 9), we found that the interdependency of the information security shows different characteristics industry by industry, and region by region. Information security in some industries shows high interdependency when tested with its own sector while some do not. In the case where high interdependency appears among firms in the same sector, the characteristic of regional interdependency will clearly show its importance.

  After the incident of the Great East Japan Earthquake in March, 2011, the empirical significance of each particular interdependency characteristics observed from our analysis before the quake is unfortunately reduced. Therefore, we conduct the analysis with a consideration on the impact from the quake regarding the interdependency of the information security. As a result, we could introduce some empirical findings from this analysis.

- In Chapter 4, we turn our attention into the security issues of network externalities in the firm-level. In this chapter, we focus on the security of the Japanese loyalty programs.

  Generally, loyalty programs are widely used as marketing tools to enhance customer's loyalty behaviors. Memberships of loyalty programs worldwide keep going in an increasing trend. This could be a result from increasing benefits of the point at each loyalty program. In addition, many companies which have never provided loyalty programs before considered to launch their programs[17].

[4] According to [109], Entity to entrust information is the one who "fully understand the possibility and take appropriate actions" when there is security incident such as information leakage or information stolen.

As stated above, since loyalty program is a marketing strategy, most of the researches on this topic are in the field of marketing. However, according to recent news, there are many incidents which attack loyalty systems through their online services. Such evidences show that there are security threats and vulnerabilities in the systems of loyalty programs. Beside that, the security issues on loyalty programs are not well-studied.

In our work, we analyze the Japanese loyalty program network. The loyalty point is considered as a virtual currency. Thus, we emphasize its liquidity which is an important property when talking about currency. We introduce the definition of liquidity of a loyalty program by considering the connection between loyalty programs in the network and their number of partners. To introduce security-liquidity implications, we also consider the security-related requirements at the system of 82 Japanese loyalty programs. This consideration is used to investigate the actual security level at each system.

- In Chapter 5, results from multi-level empirical studies are used to discuss more about network externalities regarding information security. Discussion in this chapter emphasizes how knowledge of multi-level network externalities can be used to provide more understanding to policy makers, IT practitioners, and those who are interested in information security. The findings from Chapter 3 are applied to the findings from Chapter 4. In addition, we consider how findings on network externalities from national level can be used to enrich our findings in the firm level. Discussion with consideration on the level of security expense and activities as well as discussion with consideration on the characteristics of interdependency are both focused.

  Besides the above two cores of consideration, we also introduce discussion in a general aspect in this chapter. The consideration on network externalities, threat, and vulnerability of information systems is what we want to share the idea.

Finally, the conclusion of this thesis and future directions are provided in Chapter 6.

Chapter 2

Investment in Information Security

2.1 Introduction to Investment in Information Security

The use of information technology becomes widespread and ubiquitous. Since IT resources become important and essential elements to businesses, the risks they create might become more and more important than its advantages[30]. One of the risks to IT is security breach, which eliminates or weakens three main information properties (i.e. confidentiality, integrity, and availability). Therefore, the investment in security countermeasures (e.g. spam filter, antivirus, intrusion detection system (IDS), and training and awareness measures, etc.) becomes necessary to protect those properties. However, it also brings questions such as *how much* firms should spend or invest in information security, as well as the study on optimal amount of investment in information security.

Generally, investment in economic perspective and investment in information security have some differences. Investment in economic perspective is defined as *an asset or item that is purchased with the hope that it will generate income or appreciate in the future*[76]. In other words, it aims to gain monetary benefits from the expenses. However, the investment in information security usually does not generate direct monetary benefits to the firm. Its main contribution is to *prevent potential economic loss from successful breaches*[71]. Fig.2.1 shows the image of their differences.

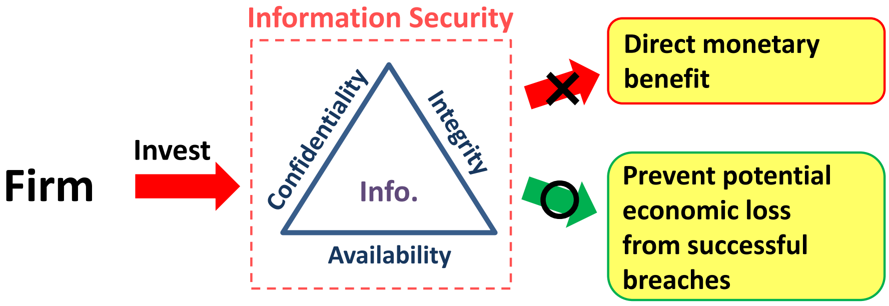


Figure 2.1: General concept of the investment in information security.

Firstly, we would like to introduce classical model in the field of investment in information security which focuses on the optimal investment. After that, we introduce extended or related literatures to show the usefulness of the basic model.

2.2 Gordon-Loeb Model

Gordon-Loeb model is a one-period economic model which emphasizes on the optimal amount for a firm to invest in information security in order to protect their information set[54]. This model becomes one of the classical and famous security investment models among IT practitioners and economists due to its simple and versatile nature[16]. Gordon-Loeb model focuses on the vulnerability of the information, as well as, potential loss that might occur if the information set is successfully breached. Gordon and Loeb consider and make assumption regarding the amount of investment under the *risk-neutral* criteria. In the context of economics, a risk-neutral investor concerns more about the expected return on his investment rather than the risk that he may be taking on[76].

According to their explanation, the information set is characterized by the following three parameters

1. λ: loss to the firms in a monetary unit
   The loss to the firms is conditioned on a breach occurring. In the model, the value of λ is assumed to have a fixed amount as estimated by the firms for simplicity. In addition, this amount of loss is finite and less than some very large numbers in order to make the assumptions under the risk-neutral criteria become realistic. [1]

2. t: the probability of threat occurring
   The probability of threat occurring is also called *threat probability* or simply *threat.* As this parameters is a probability, $0 \leq t \leq 1$. For simplicity, they assume that there is only a single threat to the information set.

3. v: the vulnerability
   In the model, the *vulnerability* is defined as *the conditional probability that a threat once realized would be successful.* Since the vulnerability is a probability, $0 \leq v \leq 1$.

In addition to the fact that they fix the amount of λ and assume that there is only a single threat in their model, they also simplify their model by assuming that the investment by the firms will affect nothing but the probability that the information set will be breached. Under this assumption, investment in information security will influence the vulnerability of information set but not the threat associated with the information set. Therefore, they define $L = t\lambda$ as the potential loss associated with the information set for simplicity.

According to the Gordon-Loeb model, let $z(\geqq 0\ )$ denote the monetary investment in security to protect the given information set. This value is measured in the same monetary unit (e.g. yen, dollar, etc.) used to measure the potential loss, L. Next, they define the function $S(z, v)$ or the security-breach probability function (hereafter, SBP function). Let $S(z, v)$ denote the probability that an information set with vulnerability v will be breached

[1] The risk-neutral investor is said to be a person who is indifferent to investments that have the same expected value, even though the investment may have varying amounts of risk. In other words, this group of investors concerns more about the expected return on their investment, rather than the risk they may be taking on[76].

after investing z. This is a conditional probability according to the realization of a threat and given that the firm has made a security investment of z. There are two main classes of the SBP function stated in the Gordon-Loeb model.

1. Class-I function

   $$S^I(z, v) = \frac{v}{(\alpha z + 1)^\beta} \tag{2.1}$$

   where $\alpha > 0$ and $\beta \geq 1$ are measures of the productivity of information security with respect to vulnerability reduction. For this class of function, the optimal level of information security investment equals zero until a threshold $v = 1/\alpha\beta L$ (hereafter, we will call this threshold as *threshold vulnerability*), and then increases at a decreasing rate.

   From this feature,they provide an implication that a firm should focus its investment on information set with high-vulnerability. The investment in information set where vulnerability is less than the threshold vulnerability will not give proper return to the firm. A firm trying to protect their information set from a targeted attack is an example of the supporting situation for this class of function[71].

2. Class-II function

   $$S^{II}(z, v) = v^{\alpha z + 1} \tag{2.2}$$

   where $\alpha > 0$ is a measure of the productivity of information security regarding vulnerability reduction. From their study, the optimal level of information security investment under this class of function shows its peak at a medium vulnerability.

   From their findings from the study on investment under this class of function, they suggest that a firm should focus its investment on information sets with midrange-vulnerabilities. The investment in information sets with very low or very high vulnerabilities will not be beneficial to the firms.

   Tanaka et al. give an additional explanation on this model in [151] as “the level of security investment influences expected loss most effectively with medium vulnerabilities. Such cases would make the information security investment become cost-effective”. Thus, the firms should invest in information set with that range of vulnerability. In addition to [151], an empirical study by Liu et al. in [94] also shows implications that support class-II function. The case that a firm with a high vulnerability faces a distributed attack is said to be an example of scenarios under the class-II function[71].

The amount of optimal investment with a focus on the effect of vulnerability and its subsequent implications are derived by solving the following maximization problem of *Expected Net Benefits from an investment in Information Security* (ENBIS):

$$ENBIS(z) = [v - S(z, v)]L - z \rightarrow \max \tag{2.3}$$

As a result, their analysis shows that the optimal investment is an increasing function of the level of vulnerability for the Class-I of SBP function. In addition, for the Class-II of SBP function, the optimal investment is not always increasing with the level of vulnerability. Instead, it initially increases and then decreases with the level of vulnerability.

2.3 Matsuura Model – An Extension of Gordon-Loeb Model

As stated above, the Gordon-Loeb model is basic and classic in the field of investment in information security, and there are plenty of researches which refer to the original Gordon-Loeb model. Matsuura model is one of those extension works.

Matsuura model focuses on productivities regarding both vulnerability and threat reductions[98]. The model considers an extension towards the formalization of the effect of the threat reduction. Moreover, a two-dimension space formed by both productivities is investigated in this work.

In this model, Matsuura assumes that the information security investment z can reduce the threat probability. Similarly to the Gordon-Loeb model, this model considers a situation under the risk-neutrality criteria. Furthermore, the threat reduction depends only on the investment z and the current level of threat probability t.

Matsuura explains differences between vulnerability reduction and threat reduction as follows: "vulnerability reduction is called when countermeasure of information security is introduced so that the *attack will fail.* On the other hand, threat reduction is called when countermeasure of information security is introduced so that the *attack will not occur*".

Then, to introduce implications regarding the optimal investment, the investment strategy is considered and discussed by solving the extended ENBIS maximization problem. The extended ENBIS is shown in (2.4).

$$ENBIS(z) = vt\lambda - S(z,v)T(z,t)\lambda - z \rightarrow \text{max}. \tag{2.4}$$

$T(z,t)$ denotes the probability that a threat occurring when the firm invests with an amount of z. It is called the security threat probability function (STP function, hereafter). In Matsuura model, $T(z,t)$ is defined as:

$$T(z,t) = t^{(\beta z+1)} \tag{2.5}$$

where $\beta \geq 0$ is a measure of the productivity of information security regarding threat reduction. α is vulnerability reduction productivity and β is threat reduction productivity.

The implications regarding the behaviors of the optimal level of investment z^* in Matsuura model are explained by the two-dimension space called *productivity space.* The two-dimension of the productivity space consists of the productivity of vulnerability reduction and the productivity of threat reduction. Thus, the productivity space explains the behaviors of the optimal level of investment z^* for different values of the productivity of vulnerability reduction and the productivity of threat reduction. The productivity space is divided into three areas as shown in Fig. 2.2.

The behaviors of the optimal level of investment z^* and advices on security investment in each area are explained as follows:

1. No-investment area
   This is an area where both productivities of threat reduction and vulnerability reduction are very low. Hence, there is no incentive for information security. The amount of optimal investment in this area equals zero.

2. Mid-vulnerability intensive area
   This area shows a similar feature to that in the case of Class-II function of the Gordon-Loeb model. This area falls into the area where productivity of vulnerability reduction

is high but productivity of threat reduction is low. The suggestion for this area is that the firms should focus their information security investment on information sets with midrange vulnerabilities.

3. High-vulnerability intensive area
   This area shows a similar feature to that in the case of Class-I function of the Gordon-Loeb model. This area falls into the area where threat reduction productivity is high. It suggests firms to focus their information security investment on information sets with high vulnerabilities.

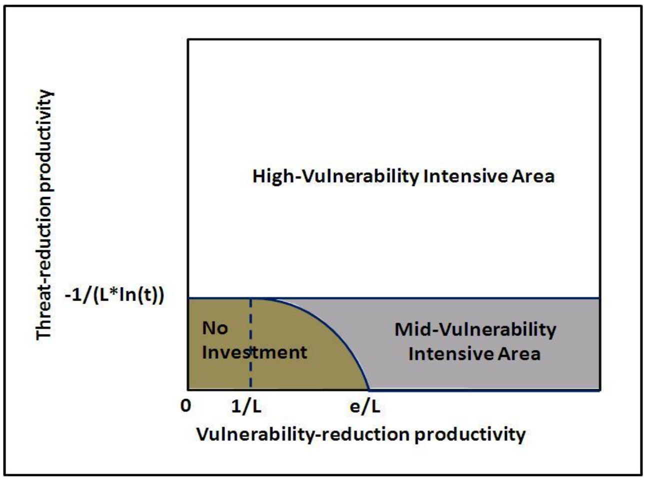

Threat-reduction productivity
-1/(L*ln(t))
High-Vulnerability Intensive Area
No Investment
Mid-Vulnerability Intensive Area
0
1/L
e/L
Vulnerability-reduction productivity

Figure 2.2: The productivity space and its three area of the behaviors of the optimal level of investment z^* for different values of the productivities of vulnerability reduction and threat reduction. Adapted from [98].

2.4 Information Sharing and the Investment in Information Security

One year after the introduction of the Gordon-Loeb model, Gordon et al. introduced their work regarding information sharing among firms in [55]. By using the framework in [54], they introduced implications regarding information sharing. They found that when security-related information (i.e. information of security threats and breaches) are shared, the overall information security costs could be reduced. Furthermore, information sharing might also raise the benefit to the network.

Beside the work by Gordon et al., findings by Gal-Or and Ghose on information sharing show interesting results[52]. In their work, the concept of game theory was used to introduce an analytical framework to find competitive implications about sharing security information and investments in security technologies. Beside the fact that security technology investments and security information sharing act as *strategic complements*, they also point that the benefit from the information-sharing between firms increases with the size of the firm. This supports an importance of a consideration on network externalities.

European union agency for network and information security (enisa) also emphasizes the importance of information sharing[43]. In their article, incentives to information sharing are divided into three levels: High, Medium, and Low. The interesting point is that the *economic incentives stemming from cost savings* is pointed out as the first incentive in the high level. Such consideration emphasizes what is stated in [54].

Information sharing is thus become one of what policy makers and practitioners consider. In 2002, the Sarbanes-Oxley Act of 2002 (a.k.a. SOX) was launched by the U.S. government[56]. Within this act, the corporations voluntarily disclose their information regarding information security activities. The introduction of this act shows a positive impact to the concern on information security.

Recently, National Institute of Standards and Technology (NIST) launched a draft version of *Guide to Cyber Threat Information Sharing*[79]. In this guide, information sharing is raised as one of the tools that help enhancing incident response actions. The information sharing acts as an important player since attackers often use similar techniques to attack multiple organizations. Therefore, information regarding security breaches becomes important. In order to select security-related information to share among organizations, they mention that firms that want to share the information should consider the following factors: risk of disclosure, operational urgency and need for sharing, benefits gained by sharing, sensitivity of the information, trustworthiness of the recipients, and methods and ability to safeguard the information.

Information sharing is also a topic included in the Japanese strategies regarding critical information infrastructure. The promotion of establishment of information sharing was firstly mentioned in *the First National Strategy on Information Security - "Toward the realization of trustworthy society"* which was introduced by Information Security Policy Council, the Ministry of Economy, Trade, and Industry (METI) in 2005[139][2]. According to this document, their primary objective is to strengthen the information sharing system among local governments[73]. The main responsibilities of the information sharing written in [73] are "to preemptive prevention of IT-mulfunctions and its expansion, prompt resumption, prevention of recurrence, and to improve the security level of all local governments". Although this topic was a tentative policy in the First National Strategy on Information Security[73], the information sharing system between local government offices in Japan was established by the end of 2006[109]. Recently, information sharing is also emphasized in *The Basic Policy of Critical Information Infrastructure Protection (3rd Edition)* by the Information Security Policy Council in 2014[74]. By this, topics such as enhancing the information sharing for more robust systems is set as one of the directions.

These are some interesting concerns on investment in information security behind our researches in multi-level network externalities in the information security.

[2] We refer to the English translated version which was published in 2006.

Chapter 3

The Empirical Study on Network Externalities in National-Level

3.1 Introduction

For our study in the national-level of network externalities, we focus on security concerns from the influence of information security risks. Motivated by the basic idea of investment in information security in Chapter 2 and the context of information sharing among parties in the network in [55][67][93], we expect that the security incidents would widely affect other parties in the network. Once a party in th network fails to protect its system from security breach, systems of its partner firms would also become risky to take the effect from that breach. This is how the problem of network externalities expands the effect from the security failures at one point to a larger scale.

Interdependency of information security is one of the main concerns in security economics. Empirical studies on interdependency of information security require two main groups of knowledge: knowledge from economic perspective and knowledge from information security perspective.

Information technology (IT) becomes one of the role players in supply chains [120][157]. That is because IT helps connecting businesses together. Firms can provide their services to respond to the need of their customers faster. Thus the interdependency between industrial sectors emerges. Many researches show that interdependency exists in many industrial sectors; For example, automotive: [82], computer: [33], financial services: [21], [47], [64], [97], and retail and logistics: [12], [29], [46], [53] [84]. Beside faster responses to the need of the customers, the satisfaction of the customers from the use of IT as a channel in the supply chains also relates to *customer loyalty*[53].

In the area of economics of information security, interdependency is very important, particularly in the context of network externalities[9]. Kunreuther and Heal applied Nash equilibrium to assess the interdependent security[86]. The impacts of network security vulnerabilities and supply chain integration on firms' incentives to their investments in information security were studied by Bandyopadhyay et al.[14]. They showed that the degree of network vulnerability or the degree of supply chain integration has relations to security investments. Hausken provided a framework in which two interdependent firms will be impacted both by security investment and by attacks if their interdependency increases[66]. Ogut et al. showed that the interdependency reduces firms' incentives to their investments in security technologies as well as to insurance coverage[116]. Tanaka studied economic interdependency between industrial sectors under the influence of the IT systems[150]; he assumed that a malfunctioning IT system in a firm will affect not only the economic activities of the firm but also those of its business partners. He then introduced the concept of ISBL (information security backward linkage) and analyzed interdependencies between firms in different sectors. Although he empirically assessed the influence of business locations on information security efforts in [149], he did not analyzed regional interdependencies in his ISBL study.

3.1.1 Our Contributions and Organization of the Chapter

In this chapter, we analyze the interdependency of information security from both sectoral and regional perspectives by using Japanese official datasets. Our main contribution is to show how the regional perspective is helpful in systematic analyses of interdependency. In other words, our contribution broadens the concept of the measurement methodology of interdependency by considering both sectoral and regional interdependencies of information security.

Due to the emergence of the Great East Japan Earthquake on March 11, 2011, the empirical significance of each particular interdependency characteristic observed from our analysis before the quake is unfortunately reduced. However, rather than being disappointed in the empirical analysis, we proceeded to extended analyses on the impact of the earthquake. Thus we suggest a wide variety of possibilities regarding extended studies based on the proposed methodology. This suggestion and some empirical findings in the earthquake analysis is our second contribution. Our study in the second contribution also emphasizes the usefulness of our extended approach since the preliminary purpose of the Inoperability Input-output Model (hereafter, IIM) is to analyze the effect from the damages.

We organize the rest of this chapter as follows: firstly, we summarize related works which are important to our study in Section 3.2. After that, we introduce the analysis methodologies in Section 3.3. Then we talk about the data we use in our study in Section 3.4. The study on the impact from the earthquake on sectoral and regional interdependency, and the results and discussion are explained in Section 3.6.2 and 3.6, respectively. Finally, we conclude this part of study in Section 3.7.

3.2 Related Literatures

First of all, we would like to introduced IIM which is one of important related studies. IIM is a Leontief-based infrastructure input-output model. It is introduced by Haimes and Jiang [61] in 2001. In particular, IIM can be used to quantify and address the risks from the intra- and inter-connectedness of infrastructures [152]. This model is used to ensure the integrity, as well as, the continued operability of complex critical infrastructures. Fig. 3.1 illustrates the concept of inter- and intra-connectedness of infrastructures in the IIM model.

In IIM, *inoperability* is defined as "*the inability of the system to perform its intended natural or engineered functions*"[63]. It can be referred as the level of the system's dysfunction. The main objective of their mode is to assess the impact of interdependencies between infrastructures on the system. The use of IIM in [63] focused on the *industry–by–industry* viewpoint. Summarized features and capabilities of the IIM in [63] show the usefulness of the IIM for the impact analysis of a terrorist attack. Thus interdependency between locations (i.e. regional perspective) was not considered in this work.

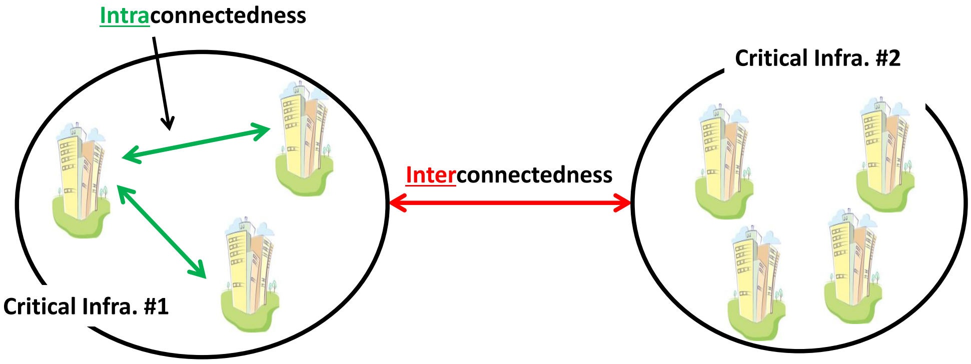


Figure 3.1: The concept of intra- and inter-connectedness of infrastructures in Inoperability Input-output Model (IIM) according to [152].

Another example of application where IIM shows its importance was introduced by Santos in 2012[135]. In this work, the concept of input-output framework is used to evaluate the economic impacts from disaster in Nashville metropolitan region in the USA. Discussion in this work is also done from the sectoral perspective. Ten industrial sectors are classified as critical sectors according to the results in this study.

Beside the use of IIM for static evaluation, Haimes et al. introduced *Dynamic IIM* in order to test interdependency with temporal dynamic behaviors of industry recoveries after damages. High-attitude electromagnetic pulse attack scenarios were used to evaluate the model regarding the dynamic IIM in [62].

Apart from the above applications, IIM framework can also be used to integrate analyses of systems from a hierarchical viewpoint where economic interdependency and physical interdependency are considered [152]. For this case, the hierarchical pyramid is introduced and used to show how economic and physical systems interact. There are six layers presented in this hierarchical pyramid. The six layers in the hierarchical pyramid from the top to the bottom are national security metric, sector , corporate or firm, facility, network, and system, respectively.

The IIM framework and the hierarchical pyramid can be applied in the analysis of interdependencies under the influence of information security where several interactions may be considered. In this case, the top half of the pyramid represents industry/regional/national-level economic metrics. Thus, it gives us a whole picture of national security. The bottom half of the pyramid represents plan-level process control system security metrics. This part is the foundation of SCADA[1] security. Thus SCADA is an example application where the IIM framework is applied to analyze interdependency in the information security perspective. In fact, the framework with hierarchies of cyber security metrics is used to show consequent risks from cyber attacks in an industrial sector such as Oil and Gas[115].

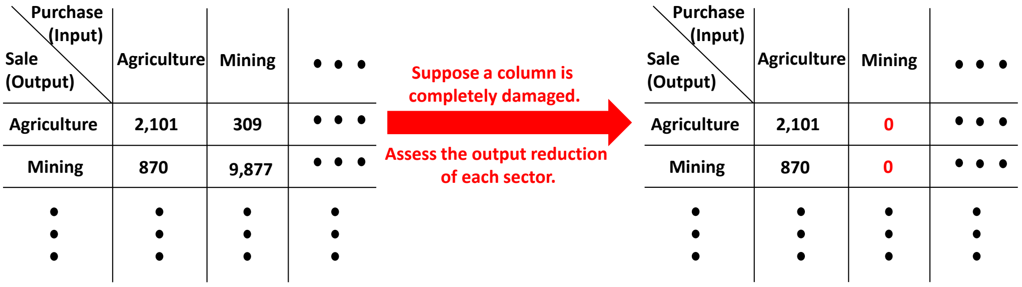
Although IIM provides features that support consideration from sectoral perspective, it still have some limitations. There are two main limitations of the existing works based on IIM. First, IIM does not distinguish differences between demand-driven perspective and supply-driven perspective. These two perspectives have different viewpoints since consideration from the demand-driven perspective represents a viewpoint from buyers while consideration from

[1] SCADA or Supervisory Control and Data Acquisition is used in the utilities industry in the U.S.

the supply-driven perspective represents a viewpoint from sellers. Another limitation is its lack of data regarding the level of IT dependency and information-security measures.

3.3 Methodology

In our study, we use a *two-step approach* to introduce our analysis methodology regarding Information Security Backward Dependency (hereafter, ISBD). The first step is about the analysis of cross-sectoral/regional interdependency as a basic economic analysis; we can conduct a sensitivity analysis by supposing a complete damage in a particular part of the input-output table. The second step is about the analysis of the interdependency under the influences of IT and information security (hereafter, IS); we can conduct a similar but different analysis by supposing that the damage depends on the level of IT dependency and the level of IS efforts. By this approach, interdependency under information security risks can be analyzed. Fig. 3.2 and 3.3 illustrate the concept of each analysis step respectively.

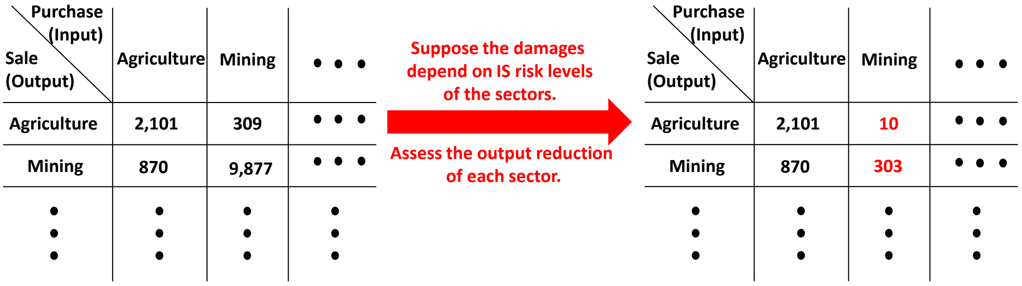


Purchase (Input) / Sale (Output)	Agriculture	Mining	• • •
Agriculture	2,101	309	• • •
Mining	870	9,877	• • •
⋮	⋮	⋮	⋮

Suppose a column is completely damaged.
Assess the output reduction of each sector.

Purchase (Input) / Sale (Output)	Agriculture	Mining	• • •
Agriculture	2,101	0	• • •
Mining	870	0	• • •
⋮	⋮	⋮	⋮

Figure 3.2: The concept of the analysis of cross-sectoral/regional interdependency as a basic economic analysis.



Purchase (Input) / Sale (Output)	Agriculture	Mining	• • •
Agriculture	2,101	309	• • •
Mining	870	9,877	• • •
⋮	⋮	⋮	⋮

Suppose the damages depend on IS risk levels of the sectors.
Assess the output reduction of each sector.

Purchase (Input) / Sale (Output)	Agriculture	Mining	• • •
Agriculture	2,101	10	• • •
Mining	870	303	• • •
⋮	⋮	⋮	⋮

Figure 3.3: The concept of the analysis of interdependency under the influence of IT and IS.

3.3.1 Structural Interdependency

From an economic viewpoint, structural interdependency can be assessed from two perspectives: a demand-driven perspective and a supply-driven perspective. In the case of demand-driven perspective, the assessment is done from the purchaser's viewpoint. By contrast, in the case of supply-driven perspective, the assessment is done from the producer's viewpoint.

The assessment methodology from demand-driven and supply-driven perspectives was initially proposed by Dietzenbacher and van der Linder in 1997 [34]. Their approach was used to measure the *inter-industry linkages* in a multi-sectoral framework. They analyzed the value of absolute *Backward Linkage* (BL) which reflects sectors' dependency on its *inputs* that they produced within the production processes. Another analyzed value is the value of absolute *Forward Linkage* (FL), which reflects sectors' dependency on its *outputs* that were sold by a particular industry to other production sectors as well as to itself.

In our work, we aim to find interdependency from the demand-driven perspective. Therefore, the concept of Backward Linkage or BL is focused in our study. There is another reason behind our consideration from the demand-driven perspective. That is, in an economic perspective, demand-side economics helps increasing the demand for goods and services or stimulate the economic growth without inflation[158].

Another important feature of our work is that we extend the basic definitions and concept in the Dietzenbacher and van der Linder's work so that both sectoral and regional interdependencies can be handled. Therefore, beside discussion from the sectoral perspective, we can also discuss from the regional perspective according to our results.

Observed Values

In [34], the input-output table is used to show relationships between industrial sectors. We extend their definitions by considering additional indices to indicate different regions. In other words, we consider an *inter-regional input-output table* $Z = (z_{q,i,r,j})$ where each intersection $z_{q,i,r,j}$ represents the economic transaction of goods and services purchased by demand-side companies of sector j in region r from supply-side companies of sector i in region q. Each transaction is valued as producers' prices. In our study, the combination of a region and a sector is called a *group*. When we talk about firms in a particular sector in a particular region on the demand side, we call the corresponding group as a *demand-side group*. Likewise, we define a *supply-side group*. In terms of the matrix structure, the four indices are used as follows:

$$Z =$$

$$\begin{pmatrix}
z_{1,1,1,1} & z_{1,1,1,2} & \cdots & z_{1,1,1,n} & z_{1,1,2,1} & z_{1,1,2,2} & \cdots & z_{1,1,2,n} & \cdots & z_{1,1,d,1} & z_{1,1,d,2} & \cdots & z_{1,1,d,n} \\
z_{1,2,1,1} & z_{1,2,1,2} & \cdots & z_{1,2,1,n} & z_{1,2,2,1} & z_{1,2,2,2} & \cdots & z_{1,2,2,n} & \cdots & z_{1,2,d,1} & z_{1,2,d,2} & \cdots & z_{1,2,d,n} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \cdots & \vdots & \vdots & \ddots & \vdots \\
z_{1,n,1,1} & z_{1,n,1,2} & \cdots & z_{1,n,1,n} & z_{1,n,2,1} & z_{1,n,2,2} & \cdots & z_{1,n,2,n} & \cdots & z_{1,n,d,1} & z_{1,n,d,2} & \cdots & z_{1,n,d,n} \\
z_{2,1,1,1} & z_{2,1,1,2} & \cdots & z_{2,1,1,n} & z_{2,1,2,1} & z_{2,1,2,2} & \cdots & z_{2,1,2,n} & \cdots & z_{2,1,d,1} & z_{2,1,d,2} & \cdots & z_{2,1,d,n} \\
z_{2,2,1,1} & z_{2,2,1,2} & \cdots & z_{2,2,1,n} & z_{2,2,2,1} & z_{2,2,2,2} & \cdots & z_{2,2,2,n} & \cdots & z_{2,2,d,1} & z_{2,2,d,2} & \cdots & z_{2,2,d,n} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \cdots & \vdots & \vdots & \ddots & \vdots \\
z_{2,n,1,1} & z_{2,n,1,2} & \cdots & z_{2,n,1,n} & z_{2,n,2,1} & z_{2,n,2,2} & \cdots & z_{2,n,2,n} & \cdots & z_{2,n,d,1} & z_{2,n,d,2} & \cdots & z_{2,n,d,n} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
z_{d,1,1,1} & z_{d,1,1,2} & \cdots & z_{d,1,1,n} & z_{d,1,2,1} & z_{d,1,2,2} & \cdots & z_{d,1,2,n} & \cdots & z_{d,1,d,1} & z_{d,1,d,2} & \cdots & z_{d,1,d,n} \\
z_{d,2,1,1} & z_{d,2,1,2} & \cdots & z_{d,2,1,n} & z_{d,2,2,1} & z_{d,2,2,2} & \cdots & z_{d,2,2,n} & \cdots & z_{d,2,d,1} & z_{d,2,d,2} & \cdots & z_{d,2,d,n} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \cdots & \vdots & \vdots & \ddots & \vdots \\
z_{d,n,1,1} & z_{d,n,1,2} & \cdots & z_{d,n,1,n} & z_{d,n,2,1} & z_{d,n,2,2} & \cdots & z_{d,n,2,n} & \cdots & z_{d,n,d,1} & z_{d,n,d,2} & \cdots & z_{d,n,d,n}
\end{pmatrix}$$

where we denote the number of regions by d and the number of sectors by n.

In addition to Z, the following values are directly observed from [102]:

Final demand: Final demand is denoted by matrix $F = (f_{q,i,r})$. From F, we obtain the following two vectors:

Regional final demand: $f^* = \left(f^*_{q,i}\right)$ where $f^*_{q,i} = f_{q,i,q}$.

Accumulated final demand: $\hat{f} = \left(\hat{f}_{q,i}\right)$ where $\hat{f}_{q,i} = \sum_{r=1}^{d} f_{q,i,r}$.

Import: Import is denoted by vector $m = (m_{r,j})$ where each element represents the absolute value of the import by each demand-side group. Normalization of the import vector m by the regional final demand gives the *import coefficient* matrix $B = (b_{q,i,r,j})$ where

$$b_{q,i,r,j} = \begin{cases} m_{q,i}/f^*_{q,i} & \text{if } r = q \text{ and } j = i \\ 0 & \text{otherwise.} \end{cases} \tag{3.1}$$

Export: Export is denoted by vector $e = (e_{q,i})$ where each element represents the value of the export by each supply-side group.

Value added: Value added is denoted by vector $c = (c_{r,j})$ where each element represents the value or tax added to the purchase by each demand-side group. From Z and c, we compute the gross output vector $g = (g_{r,j})$ where

$$g_{r,j} = \sum_{q=1}^{d} \sum_{i=1}^{n} z_{q,i,r,j} + c_{r,j} \tag{3.2}$$

represents the gross output to each demand-side group. Normalization of Z by the gross output gives the *input coefficient* which is denoted by matrix $A = (a_{q,i,r,j})$ where

$$a_{q,i,r,j} = z_{q,i,r,j}/g_{r,j}. \tag{3.3}$$

In order to extract the input coefficients inside each region, we define a matrix $A^* = \left(a^*_{q,i,r,j}\right)$ by

$$a^*_{q,i,r,j} = \begin{cases} a_{q,i,r,j} & \text{if } q = r \\ 0 & \text{otherwise.} \end{cases} \tag{3.4}$$

Backward Dependency

If all the deliveries to a demand-side group $(\overline{r}, \overline{j})$ are reduced to be zero by a disastrous event, the output from the group will be reduced. We compute such output reductions in order to study absolute backward linkages. The output reductions are given by $h - \overline{h}\left(\overline{r}, \overline{j}\right)$ where

$$h = \{I - [A - BA^*]\}^{-1} \left(\hat{f} - Bf^* + e\right), \tag{3.5}$$

$$\overline{h}\left(\overline{r}, \overline{j}\right) = \left\{I - \left[\overline{A}\left(\overline{r}, \overline{j}\right) - B\overline{A}^*\left(\overline{r}, \overline{j}\right)\right]\right\}^{-1} \left(\hat{f} - Bf^* + e\right), \tag{3.6}$$

and I is the identity matrix of the corresponding size. The matrices $\overline{A}\left(\overline{r},\overline{j}\right) = \left(\overline{a}\left(\overline{r},\overline{j}\right)_{q,i,r,j}\right)$ and $\overline{A}^{*}\left(\overline{r},\overline{j}\right) = \left(\overline{a}^{*}\left(\overline{r},\overline{j}\right)_{q,i,r,j}\right)$ are calculated from A and A^{*} as follows:

$$\overline{a}(\overline{r},\overline{j})_{q,i,r,j} = \begin{cases} 0 & \text{if } r = \overline{r} \text{ and } j = \overline{j} \\ a_{q,i,r,j} & \text{otherwise} \end{cases} \tag{3.7}$$

and

$$\overline{a}^{*}(\overline{r},\overline{j})_{q,i,r,j} = \begin{cases} 0 & \text{if } r = \overline{r} \text{ and } j = \overline{j} \\ a^{*}_{q,i,r,j} & \text{otherwise.} \end{cases} \tag{3.8}$$

Let vector $u(\overline{r},\overline{j}) = \left(u(\overline{r},\overline{j})_{q,i}\right)$ denote the backward dependency (BD) of a demand-side group $(\overline{r},\overline{j})$ on the supply-side groups. We can obtain $u(\overline{r},\overline{j})$ in terms of percentage by

$$u(\overline{r},\overline{j})_{q,i} = 100\frac{h_{q,i} - \overline{h}(\overline{r},\overline{j})_{q,i}}{g_{\overline{r},\overline{j}}}. \tag{3.9}$$

At this point, one can notice that the value of BD still has no influence from information security.

3.3.2 Interdependency under the Influence of Information Security

In this step, the influence of information security is added into the concept of BD shown in the above step. In [150], the ISBD vector of a demand-side group $(\overline{r},\overline{j})$ is defined as the BD vector computed by replacing (3.7) and (3.8) with

$$\overline{a}(\overline{r},\overline{j})_{q,i,r,j} = \begin{cases} (1 - s_i s_j)a_{q,i,r,j} & \text{if } r = \overline{r} \text{ and } j = \overline{j} \\ a_{q,i,r,j} & \text{otherwise} \end{cases} \tag{3.10}$$

and

$$\overline{a}^{*}(\overline{r},\overline{j})_{q,i,r,j} = \begin{cases} (1 - s_i s_j)a^{*}_{q,i,r,j} & \text{if } r = \overline{r} \text{ and } j = \overline{j} \\ a^{*}_{q,i,r,j} & \text{otherwise} \end{cases} \tag{3.11}$$

where s_i represents the security risk level of sector i. The values of security risk level are obtained from additional datasets [105], [134].

3.4 Data for Sectoral and Regional Interdependency

3.4.1 Inter-Regional Input-Output Table for 2005 [102]

In our study, inter-regional input-output table with 12 industrial sectors is mainly used. However, we also use the dataset of 53 sectors for further analyses on some sectors; sector of Agriculture and sector of Financial, insurance, and real estate. The list of the sectors is shown in Table 3.1.

In this dataset, Japan is divided into nine regions: Hokkaido, Tohoku, Kanto, Chubu, Kinki, Chugoku, Shikoku, Kyushu, and Okinawa. These regions are indexed by A, B, C, $\cdots$, and I, respectively. Regarding the economic scale, Kanto(C), Kinki(E), and Chubu(D) are the top three regions with high production values. On the other hand, Okinawa(I), Shikoku(G), and Hokkaido(A) are the bottom three regions with low production values.

Table 3.1: List of industrial sectors.

12 Industrial sectors			53 Industrial sectors	
Sector ID	**Sector name**		**Sector ID**	**Sector name**
01	Agriculture		0010	Agriculture
02	Mining		0020	Mining
			0030	Coal, oil, and natural gas
03	Manufacturing	Food & Beverage	0040	Food & beverage
04	Manufacturing	Metal	0170	Iron and steel
			0180	Nonferrous metal
			0190	Metal products
05	Manufacturing	Machinery	0200	General machinery
			0210	Office and service equipment
			0220	Industrial electrical equipment
			0230	Other electrical machinery
			0240	Household electric appliances
			0250	Telecommunications equipment and related equipment
			0260	Computer and accessories
			0270	Electronic components
			0280	Car
			0290	Other cars
			0300	Auto parts accessories
			0310	Other transportation equipment
			0320	Precision machinery
06	Manufacturing	Other	0050	Textile industry products
			0060	Apparel and other textile products
			0070	Lumbering, wood, and furniture
			0080	Pulp, paper, paperboard, and processed paper
			0090	Printing, plate making, and bookbinding
			0100	Chemical products
			0110	Plastics
			0120	Final chemical products
			0130	Pharmaceutical products
			0140	Petroleum and coal products
			0150	Plastic products
			0330	Other manufactured products
			0160	Clay products
			0340	Renewable resources and processing treatment
07	Construction		0350	Construction
08	Utilities		0360	Electricity
			0370	Gas and heat supply
			0380	Waste water treatment
09	Commerce & Logistic		0390	Commerce
			0430	Transportation
10	Financial, Insurance, and Real Estate		0400	Finance and Insurance
			0410	Real estate
			0420	Rental housing
11	ICT		0440	Other information and communications
			0450	Information service

Table 3.1: List of industrial sectors (Cont'd).

12 Industrial sectors		53 Industrial sectors	
Sector ID	**Sector name**	**Sector ID**	**Sector name**
12	Services	0460	Public service
		0470	Educational research
		0480	Health care and social security
		0490	Advertisement
		0500	Goods rental and leasing services
		0510	Other business services
		0520	Personal service
		0530	Other

From the sectoral perspective, the top three sectors with high production values are Services(12), Commerce&logistic(09), and Manufacturing-machinery(05), whereas Mining(02), Agriculture(01), and Utilities(08) are the bottom three sectors with low production values.

Table 3.2 and Table 3.3 show Japanese production values from regional and sectoral (12 sectors) perspectives, respectively. The exchange rate between JYP and USD was 76.75 JPY = 1 USD on Oct 19, 11. We use this exchange rate throughout the chapter.

Table 3.2: Regional production values in Japan according to [102].

Region name	**Region ID**	**Output (billion US$)**
Kanto	C	8,175.19
Kinki	E	3,042.11
Chubu	D	2,341.25
Kyushu	H	1,576.64
Chugoku	F	1,176.51
Tohoku	B	1,136.39
Hokkaido	A	684.96
Shikoku	G	508.69
Okinawa	I	116.78

3.4.2 The 2006 Survey of Information Technology [105]

The Survey of Information Technology is regular and very popular in Japan based on Statistics Law. Its 2006 version contains reliable data of 3,647 firms from 27 industries. We use the average number of IS measures deployed by the firms in each sector as a proxy of the level of IS in each sector. The IS measures are classified into four categories shown in Table 3.4.

We compute *IS multiplier* (denoted by m_i) which represents the normalized level of IS

Table 3.3: Japanese sectoral production values for 12 industrial sectors according to [102].

Sector name	**Sector ID**	**Output (billion US$)**
Services	12	3090.26
Commerce & Logistic	09	1916.02
Manufacturing-Machinery	05	1696.06
Financial, Insurance, and Real Estate	10	1404.47
Manufacturing-Other	06	1229.48
Construction	07	823.94
ICT	11	598.51
Manufacturing-Metal	04	593.76
Manufacturing-Food & Beverage	03	468.23
Utilities	08	349.05
Agriculture	01	171.40
Mining	02	13.14

measures. This variable is defined by

$$m_i = \mathrm{M}^*/\mathrm{M}_i \tag{3.12}$$

where M^* is the average number of deployed IS measures across all the sectors and M_i is the average number of deployed IS measures in sector i.

Although there are some similar surveys in other countries (e.g. 2005 CSI/FBI Computer Crime and Security Survey [57]), our dataset is more reliable and usable for empirical studies. First, let us recall the sample size and the coverage of industries of our dataset (3,647 firms from 27 industries). By contrast, [57] has approximately 700 samples, and its coverage of industries is questionable. Second, our dataset is more usable since we can see more detailed statistics regarding the deployment of IS measures. In particular, we can obtain not only the average number of deployed IS measures across all the sectors but also the average number of deployed IS measures in each sector.

Table 3.4: List of information security measures.

Category	Information security measures
Implementation of organizational measures	- Risk analysis - Security policy - Examination of specific measures based on security policy - Creation of information security report - Creation of Business Continuity Plan (BCP) - Deployment of an corporate-wide security management - Sectoral deployment of security management - Information security training for employees - Confirmation on information security measures of trading partners (including outsourcing)
Implementation of technical solutions/Defense measures	- Access control of important computer rooms - Access control of important systems - Data encryption (including Public Key Infrastructure (PKI)) - Firewall installation against external connection - Installation of ISO/IEC15408 certified product
System monitoring	- Installation of security monitoring software - Full-time monitoring by external professionals
Assessment	- Use of information security benchmark - Regular system auditing by external professionals - Regular system auditing by internal experts - Regular information security auditing by external professionals - Regular information security auditing by internal experts - Obtaining certification of information security management system (ISO/IEC27001)

3.4.3 Japan Industrial Productivity Database 2008 [134]

We use the data of *IT Capital Stock* and *non-IT Capital Stock* reported in [134] in order to estimate *the level of IT dependency* of each sector. Let t_i denote the level of IT dependency of sector i. We estimate the level of IT dependency by

$$t_i = \mathrm{IT}_i/(\mathrm{IT}_i + \mathrm{nIT}_i) \tag{3.13}$$

where IT_i denotes the IT capital stock of sector i and nIT_i denotes the non-IT capital stock of sector i. We then use

$$s_i = t_i m_i \tag{3.14}$$

as a proxy for the security risk level of sector i.

The level of IT dependency, the level of IS measure, and the IS multipliers computed from our dataset are shown in Fig. 3.4 and in Fig. 3.5, respectively. Finally, Fig. 3.6 shows the security risk levels of the 12 sectors.

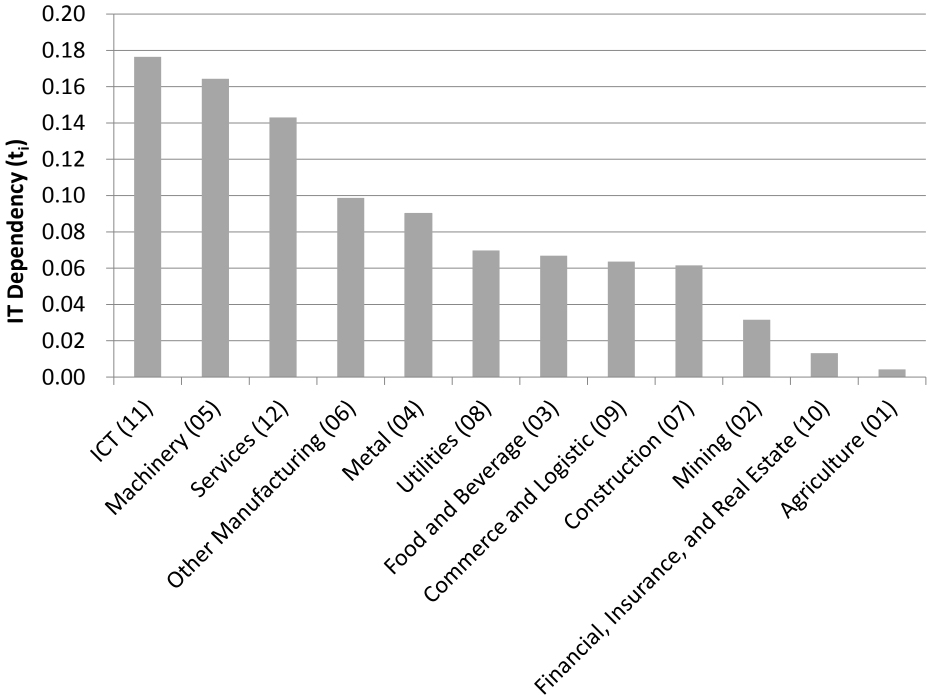


Figure 3.4: The level of IT dependency of 12 industrial sectors.

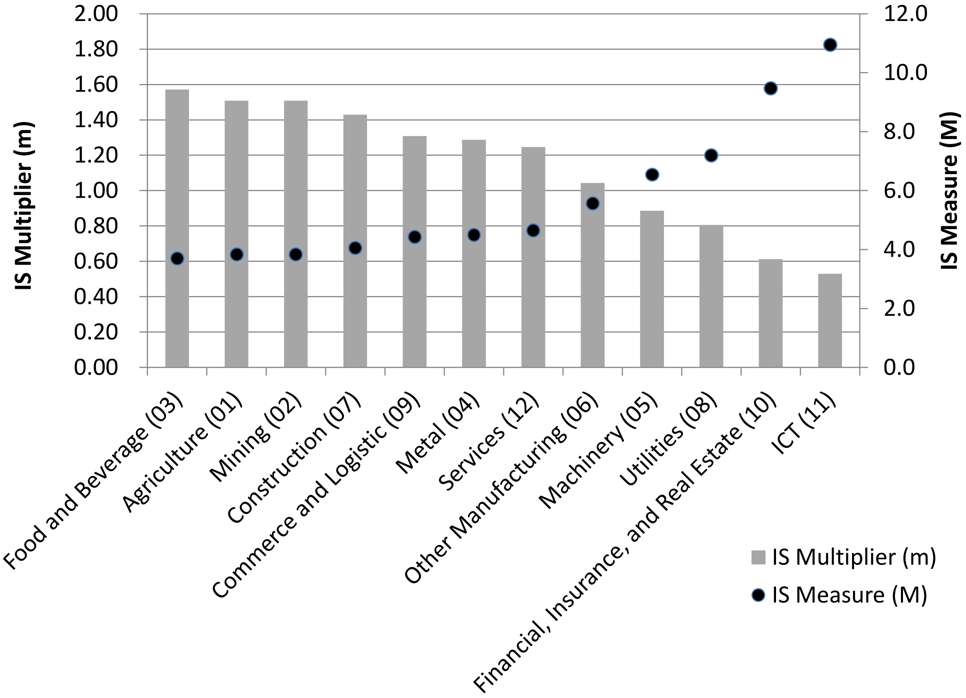


Figure 3.5: The level of IS measure and the IS multipliers of 12 industrial sectors.

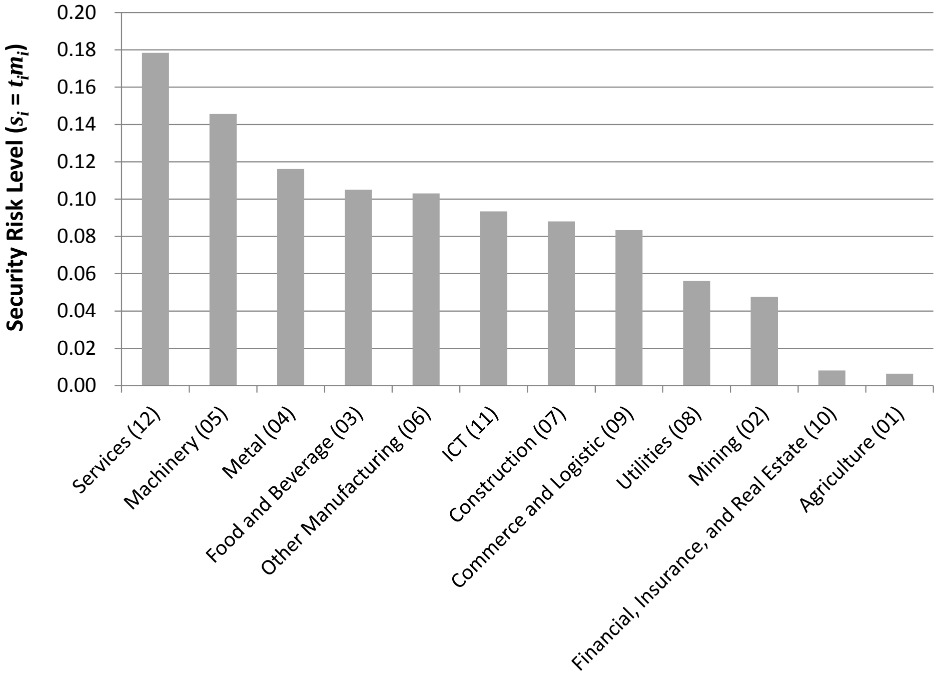


Figure 3.6: Security risk levels of 12 industrial sectors.

3.5 The Analysis on the Impact of the Earthquake

At 14:46 p.m. on March 11, 2011, The Great East Japan Earthquake hit Tohoku region with magnitude 9.0. This massive earthquake also triggered tremendous and powerful Tsunami waves which left dreadful damages. The cabinet office, Government of Japan, defined seven prefectures as disaster areas regarding this earthquake [24]. Among them, the three most significantly damaged prefectures are in Tohoku region. The Cabinet office defined the following two cases of damages.

Case 1: refers to the damage directly by the earthquake, and

Case 2: refers to the damage by the earthquake and the consequent Tsunami.

Shinozaki et al. estimated the damage on ICT-related private capital stock due to the Great East Japan Earthquake in [142]. Their result shows that the damage from this disaster is expected to be around 2.5-4.4 trillion yen in total.

We study the impact of the Great East Japan Earthquake by using the methodology in Section 3.3 with a modification based on the following two additional datasets:

1. **Special cabinet meeting material on monthly economic report due to the earthquake** [24]
   This report is available few weeks after the earthquake by the government. We obtain the overall damage on capital stock, D^{all}, from this dataset.

2. **Gross capital stock by industry** [23]
   We use the values of gross capital stock of year 2009, which was the newest at the time we estimated the impact of the earthquake. Therefore, the employed dataset of gross

capital stock would be closer to the data in our first additional dataset mentioned above. We obtain the nationwide capital stock, C_n, from this dataset.

Now let us describe the extended analysis. First, in the analysis regarding the structural interdependency, we use

$$\overline{z}_{q,i,r,j} = \begin{cases} (1 - R_r)z_{q,i,r,j} & \text{if } r = \text{Tohoku} \\ z_{q,i,r,j} & \text{otherwise} \end{cases} \tag{3.15}$$

instead of $z_{q,i,r,j}$. Here, R_r is a "regional ratio of damage" of region r defined by

$$R_r = D^{all}/C_r \tag{3.16}$$

where C_r represents the capital stock of region r estimated by

$$C_r = \frac{P_r}{P_{total}} \cdot C_n \tag{3.17}$$

and P_r is the production value of region r, and P_{total} is the total production value of all regions. P_r and P_{total} are observed from the inter-regional input-output table [102].

Second, in the analysis regarding ISBD, we estimate the damage on IT systems, D^{IT}, by

$$D^{IT} = D^{all}t_{\text{total}} \tag{3.18}$$

where t_{total} is the ratio of IT capital stock given by

$$t_{\text{total}} = \text{IT}_{\text{total}}/(\text{IT}_{\text{total}} + \text{nIT}_{\text{total}}) \tag{3.19}$$

where IT_{total} denotes the total amount of IT capital stock, and $\text{nIT}_{\text{total}}$ denotes the total amount of non-IT capital stock.

To further investigate the effects from investment in information security, we assume that the investment will reduce the damage from disasters such as earthquakes. In particular, we assume that a pre-disaster investment in information security helps improving the amount of damage from the disaster by a certain *degree of improvement*, Deg. So we replace R_r in (3.15) with

$$\tilde{R}_r = (1 - \text{Deg})D^{IT}/C_r \tag{3.20}$$

in our analysis. We set the degree of improvement as 10% (therefore, Deg=0.1) as our first estimation. However, the same methodology can be used for more detailed analysis with different degrees.

3.6 Results and Discussions

3.6.1 Sectoral and Regional Interdependency

First, we analyze the sectoral and regional interdependencies before the earthquake. The dataset with 53 industrial sectors is used to analyze more details of Agriculture(01) and Financial, insurance, and real estate(10) because these two sectors showed very low values of ISBD in the analysis based on the 12-sector dataset.

Suppose that we want to see the BD between a *pair* of groups (a supply-side group and a demand-side group). By using a heuristic threshold ISBD=0.01%[2], we say "dependent" if ISBD is larger than or equals to this threshold, and "not dependent" otherwise. We count the number of dependent pairs to see regional and sectoral interdependencies.

[2] In our raw result, the average mean value of ISBD is 0.00754%. By considering this mean value and the standard deviation, we set the threshold.

Sectoral Interdependency

The results regarding sectoral interdependency can be summarized by Table 3.5. Different symbols indicate different levels of interdependency as follows. For example, let us look at the sixth row of Table 3.5. The i-th element of this row shows the level of interdependency between the demand-side sector Manufacturing-Other(06) and the supply-side sector i. When we evaluate the interdependency level of this element, we compute the ISBD for each of the $9 \times 9 = 81$ pairs of (demand-side group in Sector 06, supply-side group in Sector i), and count the number of "dependent" pairs. The result of this counting is shown in the last row of Table 3.6. The largest element in this last row is the sixth row, and its value is 56. Then we compute the ratio of "the value of each element of this row" to this highest value. If the ratio is larger than or equals to 50%, we use the sign "$\circ\circ$" in the corresponding element in Table 3.5. Likewise, we use "$\circ$" if the ratio is between 10% and 50%. We use "$\bullet$" if the ratio is non-zero but less than 10%. Finally, we use "$-$" if the ratio is zero. Since $(0/56, 2/56, 0/56, 8/56, 0/56, 56/56, 2/56, 9/56, 28/56, 11/56, 10/56, 22/56)$ $= (0, 0.036, 0, 0.143, 0, 1, 0.036, 0.161, 0.500, 0.196, 0.179, 0.393)$, the sixth row of Table 3.5 is

$$(-, \bullet, -, \circ, -, \circ\circ, \bullet, \circ, \circ\circ, \circ, \circ, \circ).$$

Table 3.5 shows that supply-side sectors of Manufacturing-other(06), Commerce& logistic(09), and Services(12) are the sectors highly depended by demand-side sectors. We call these three sectors as *critical sectors* or *influential sectors*. These three industries are critical sectors when the issue regarding interdependency of information security is emphasized. Furthermore, this issue has high relationship to the problem of network externalities. Demand-side sectors have high opportunities to be affected by security incidents in these critical sectors. That is, once security breaches occur to the system in a critical sector, impacts from the security incidents likely expand and show high effect through connectivities between systems of supply-side and demand-side sectors.

According to [73], critical infrastructures in their document refer to "*the basic for people's social lives and economic activities and the most important task is to ensure stable services by protecting them from any threats.* Thus we could see that the definition of the critical infrastructures by the government is considered more in the general aspect even when they talk about information systems. That is they do not only considered in terms of interdependency of information security but also in a broader sense.

Although the industrial sectors which are classified as critical infrastructures were not clearly mentioned in [73], 10 industrial sectors which are critical infrastructures in terms of information system and information security were mentioned in the Second National Strategy on Information Security[109]. These 10 sectors are Information and communication, Finance, Aviation, Railroad, Electricity, Gas, Government, Medical treatment, Water service, and Logistic[3]. Compared to our findings, the critical infrastructures mentioned in [109] are also included in our three critical sectors; Aviation, Railroad, and Logistic are included in industry 09 (Commerce & Logistic), and Medical treatment is included in industry 12 (Services).

Although industry 06 was not included as a critical infrastructure in [109], the Information Security Policy Council decided to add three more industries as critical sectors in the year 2014[74]. This decision was made based on a lesson learned from the past experiences including

[3] The total number of industries and how to classify industries were not mentioned in [109].

the effect from the Great East Japan Earthquake[4]. The three additional industries in [74] are Credit card services, Chemical industries, and Petroleum industries. According to the List of Industrial Sectors in Table 3.1, Chemical industries and Petroleum industries are sub-industries in industrial sector 06 (Manufacturing-Other) which we classified as *critical sectors* due to our result. In addition, interestingly, the main reason to add Petroleum industries into a critical infrastructure is that it has *interdependency with the current Critical Information Infrastructure sectors*. Such a reason helps emphasizing the importance of consideration on interconnectivity between systems or the topic regarding network externalities.

Likewise, Table 3.5 shows that demand-side sectors of Machinery(05) and Services(12) are the most *influenced sectors*. Thus, if we consider demand-side sectors, these two industries likely obtain high impact compared to other demand-side sectors. This high impact is realized not only from the fact that they are the most influenced sectors but also from their characteristics of interdependency (i.e. high self-dependency and high interdependency with the critical sectors) which we introduce in the next paragraph.

By observing Table 3.5 in more detail, we can classify demand-side sectors into the following five classes.

Class 1: *Sectors which show high interdependency* ***when and only when*** *tested with the critical sectors.* Mining(02) and Utilities(08) belong to this group.

Class 2: *Sectors which show high interdependency when tested with its own sector and* ***all*** *of the critical sectors.* Manufacturing-Food&beverage(03), Manufacturing-Machinery(05), Commerce&logistic(09), ICT(11), and Services(12) belong to this group.

Class 3: *Sectors which show high interdependency when tested with its own sector and* ***not all but some*** *of the critical sectors.* Manufacturing-Metal(04) and Manufacturing-other(06) belong to this group.

Class 4: *Sectors which shows little interdependency when tested with supply-side sectors.* Although sector of Financial, insurance, and real estate(10) belongs to this group, our detailed analysis by using the 53-sector dataset shows that sub-sector Financial and insurance(0400) shows characteristics similar to those of Class 3.

Class 5: *The rest of the demand-side sectors.* Agriculture(01) and Construction(07) belong to this group. These two sectors show no interdependency when tested with its own sector.

We can see that the demand-side sectors with high self-dependency (i.e. the sectors in Class 2 and Class 3) do not show high interdependency with non-critical sectors. Since investment advices regarding self-dependency and critical sectors are trivial, they need to learn from the analysis of regional interdependencies. Paying attention to the fact that majority of sectors belong to these two classes, we notice the importance of regional interdependency analysis.

[4] The effects from the Great East Japan Earthquake which were mention in [74] are system outage and data loss during the disaster. In our opinion, the case of system outage is quite close to our consideration on the loss or damage from the earthquake.

Table 3.5: Summary of sectoral interdependency of information security.

Demand-side sector name (ID)	Sector ID of supply-side sector (Sector ID)											
	01	02	03	04	05	06	07	08	09	10	11	12
Agriculture(01)	–	–	–	–	–	–	–	–	–	–	–	–
Mining(02)	–	–	–	○	–	○○	–	○	○○	○	●	○○
Manufacturing-Food &beverage(03)	○	–	○○	○	–	○○	–	○	○○	○	○	○○
Manufacturing-Metal(04)	–	–	–	○○	–	○○	○	○	○○	○	○	○
Manufacturing-Machinery(05)	–	–	–	○○	○○	○○	●	○	○○	○	○	○○
Manufacturing-Other(06)	–	●	–	○	–	○○	●	○	○○	○	○	○
Construction(07)	–	–	–	○○	○	○○	–	○	○	○	○	○
Utilities(08)	–	–	–	–	–	○○	○	○	○○	○	○	○○
Commerce&logistic(09)	–	–	–	–	○	○○	●	○	○○	○	○○	○○
Financial, insurance, and real estate(10)	–	–	–	–	–	–	–	–	–	–	–	○○
ICT(11)	–	–	–	–	–	○○	●	○	○○	○	○○	○○
Services(12)	●	–	○	○	○○	○○	○	○	○○	○	○	○○

Table 3.6: Number of dependent pairs for demand-side sector of Manufacturing-Other (06).

Demand-side region name (ID)	Number of dependent pairs for each supply-side sector (Sector ID)											
	01	02	03	04	05	06	07	08	09	10	11	12
Hokkaido (A)	0	1	0	0	0	6	0	1	2	1	1	2
Tohoku (B)	0	0	0	1	0	6	0	1	3	2	1	2
Kanto (C)	0	0	0	1	0	7	1	1	2	1	1	2
Chubu (D)	0	0	0	3	0	6	0	1	3	2	2	3
Kinki (E)	0	0	0	1	0	7	1	1	3	1	2	2
Chugoku (F)	0	0	0	1	0	6	0	1	4	1	1	3
Shikoku (G)	0	0	0	0	0	6	0	1	5	1	1	3
Kyushu (H)	0	0	0	1	0	6	0	1	4	1	1	3
Okinawa (I)	0	1	0	0	0	6	0	1	2	1	0	2
Total	0	2	0	8	0	56	2	9	28	11	10	22

Regional Interdependency

The results regarding regional interdependency can be summarized by Table 3.7 where different symbols indicate different levels of interdependency in the same way as in the sectoral interdependency analysis. In Table 3.7, we can see the economic scale of a region has a great influence on the characteristics of the interdependency, and most of the results are intuitively easy to accept; for example, on the supply-side, Kanto (economically largest region) is the most influential. In other words, Kanto is the region where information security of demand-side of all regions including itself highly rely on.

As a remarkable (somewhat counter-intuitive) point, on the demand-side, Tohoku (economically middle sized) has the same features (i.e. less influenced) with that of Kanto. That is information security of Tohoku relies on smaller numbers of region compared to other regions except Kanto.

Also, the features regarding highly influenced sectors are quite different from those of highly influenced regions. From the regional perspective, we found that highly influenced regions likely have small economic scales. By contrast, from the sectoral perspective, the two highly influenced sectors, Machinery(05) and Services(12), have large economic scales.

Table 3.7: Summary of regional interdependency of information security.

Demand-side region name (ID)	Region ID of supply-side region (Region ID)								
	A	B	C	D	E	F	G	H	I
Hokkaido(A)	○○	○	○○	○	○	○	●	●	–
Tohoku(B)	●	○○	○○	○	○	●	–	●	–
Kanto(C)	●	●	○○	○	○	●	●	●	–
Chubu(D)	●	●	○○	○○	○	○	●	○	–
Kinki(E)	●	●	○○	○	○○	○	●	●	–
Chugoku(F)	–	●	○○	○	○	○○	●	○	–
Shikoku(G)	–	●	○○	○	○○	○	○○	○	–
Kyushu(H)	–	●	○○	○	○	○	●	○○	–
Okinawa(I)	●	●	○○	○	○	○	●	○	○○

3.6.2 Impact of the Earthquake

Based on the government's announcement about the damage mentioned in Section 3.5, we set the following four testing scenarios:

Case 1a: Full damage from the earthquake. The full amount of nine trillion yen is used as the damage value.

Case 1b: Damage from the earthquake with some reduction by investment in information security. The amount of nine trillion yen with 10%-reduction is used as the damage value.

Case 2a: Full damage from the earthquake and the consequent Tsunami. The full amount of 16 trillion yen is used as the damage value.

Case 2b: Damage from the earthquake and the consequent Tsunami with some reduction by investment in information security. The amount of 16 trillion yen with 10%-reduction is used as the damage value.

In each of the four cases, we did the following.

1. Count the number of dependent pairs (demand-side group in Tohoku and supply-side group in Sector i) before the earthquake, N_i.
2. Count this number after the earthquake, N'_i.
3. Compute the reduction of this number (i.e. $N_i - N'_i$). We refer to this reduction as the number of *missing* dependent pairs.

We obtained Table 3.8 by the above procedure. The reduction of interdependency occurs more likely with the following sectors: Financial, insurance, and real estate(10), Manufacturing-other(06), and Commerce&logistic(09). It should be noted that Manufacturing-other(06) and Commerce&logistic(09) are critical sectors identified by the basic analysis in 3.6.1 but that Financial, insurance, and real estate(10) is not a critical sector. However, sub-industries in Financial, insurance, and real estate(10); Finance and Credit card services, are classified as critical infrastructure in [109] and [74], respectively. The above characteristics are not changed by the reduction of damages by prior security investment.

Table 3.8: ISBD reduction (in terms of the number of *missing* dependent pairs) from the sectoral perspective in the investigation of the impact of The Great East Japan Earthquake.

	Supply-side Sector ID												
	01	02	03	04	05	06	07	08	09	10	11	12	Total
Case 1a	0	0	1	0	1	5	0	1	3	9	2	0	22
Case 1b	0	0	1	0	1	5	0	1	3	9	2	0	22
Case 2a	0	0	1	2	2	6	1	4	7	10	5	0	38
Case 2b	0	0	1	2	2	6	1	4	7	10	5	0	38

Likewise, in each of the four cases, we did the following.

1. Count the number of dependent pairs (demand-side group in Tohoku and supply-side group in Region q) before the earthquake.
2. Count this number after the earthquake.
3. Compute the reduction of this number. We refer to this reduction as the number of *missing* dependent pairs.

We obtained Table 3.9 by the above procedure. The reduction of interdependency is concentrated on two patterns: one is between sectors inside Tohoku(B), and the other is between sectors in Tohoku(B) and those in Kanto(C). Thus, the earthquake impacted the most damaged region (Tohoku) and the economically largest region (Kanto) most significantly. This feature is not changed by the reduction of damages by prior security investment.

Table 3.9: ISBD reduction (in terms of the number of *missing* dependent pairs) from the regional perspective in the investigation of the impact of The Great East Japan Earthquake.

	Supply-side Region ID									
	A	B	C	D	E	F	G	H	I	Total
Case 1a	3	8	5	3	2	0	0	1	0	22
Case 1b	3	8	5	3	2	0	0	1	0	22
Case 2a	3	14	11	3	6	0	0	1	0	38
Case 2b	3	14	11	3	6	0	0	1	0	38

3.7 Conclusion

In this chapter, we present our empirical study on sectoral and regional interdependencies under the influence of information security in Japan from the demand-side perspective.

In our main study, first, the economic scale of a region has a great influence on the characteristics of the interdependency. For example, security problems of economically larger supply-side regions tend to affect demand-side firms more significantly. Second, we observed that there are three supply-side sectors which are *critical* in the sense that information security problems in the three sectors can highly affect the demand-side sectors. These three critical sectors are also included as *critical infrastructures* in [109] and [74]. In addition, industrial sector of Manufacturing - Other (06) was additionally mentioned in 2014 as critical infrastructure due to its interdependency with other existing critical infrastructures. Such an evidence from the government helps emphasizing the importance of our findings in this work. Another common feature of the three critical sectors (Manufacturing-other, Commerce and logistic, and Services) is that they have high self-dependency.

As an extended study, we investigated the impact of the Great East Japan Earthquake by evaluating interdependency reductions caused by the earthquake. Four testing scenarios are introduced in this part. The results are consistent with the results of our main study; the role of the critical sectors is very important in Japan. We also found that the earthquake impacted the most damaged region (Tohoku) and the economically largest region (Kanto) most significantly. These features are not changed by the reduction of damages by prior security investment.

Both in the basic study and in the extended study, we can see that considering not only sectoral perspective but also regional perspective is very helpful in empirical analyses related to the interdependency under the influence of information security. One main supporting reason to this point is the differences between the characteristics of sectoral and regional interdependencies. Especially, the case of how economic scale affects the characteristics of each type of interdependency. By analyzing sensitivity of the interdependency to changes in an inter-regional input-output table in a wide variety of scenarios, there are many possibilities of more extended studies based on our methodology. For instance, an analysis regarding a large-scale earthquake in Kanto expected in the near future would bring important implications and suggestions since there are many predictions about such earthquakes.

One might notice that the datasets we used in this chapter contain data between 2005-2009. However, our preliminary results show that the characteristics of interdependency under the influence of information security in Japan are highly influenced by the economic scale. Such finding means that economic activity is one of the most important factors to the future impact on the information security.

In addition to the above reason, we also found a similar trend of the IS measure when the data of 26 industrial sectors in [104] is used for the calculation [5, 6]. Fig. 3.7 shows the level of IS measure and the IS multipliers of 26 industrial sectors in 2012.

Let us compare the values of IS measure from the calculation in the year 2006 (shown in Fig. 3.3) and 2012. According to our results, we found that industries with high IS measure (i.e. industries that deployed more IS measures) in 2012 are sectors which likely had high IS measure in 2006. For example, the results of sector of Information services (industry 19 in Fig. 3.7) in 2012 and sector of ICT (industry 11 in Fig. 3.3) in 2006, and the results of sector of Financial and insurance (industry 23 in Fig. 3.7) in 2012 and sector of Financial, insurance, and real estate (industry 10 in Fig. 3.3) in 2006. The results of both industries show high IS measures in both years. Likewise, industries with low IS measure in 2012 are sectors which likely had low IS measure in 2006. For example, the results of sector of Manufacture of food, beverages, tobacco, and feed (industry 01 in Fig. 3.7) in 2012 and sector of Food and beverages (industry 03 in Fig. 3.3 in 2006.

As a result, we did not conduct any reanalysis by using newer data.

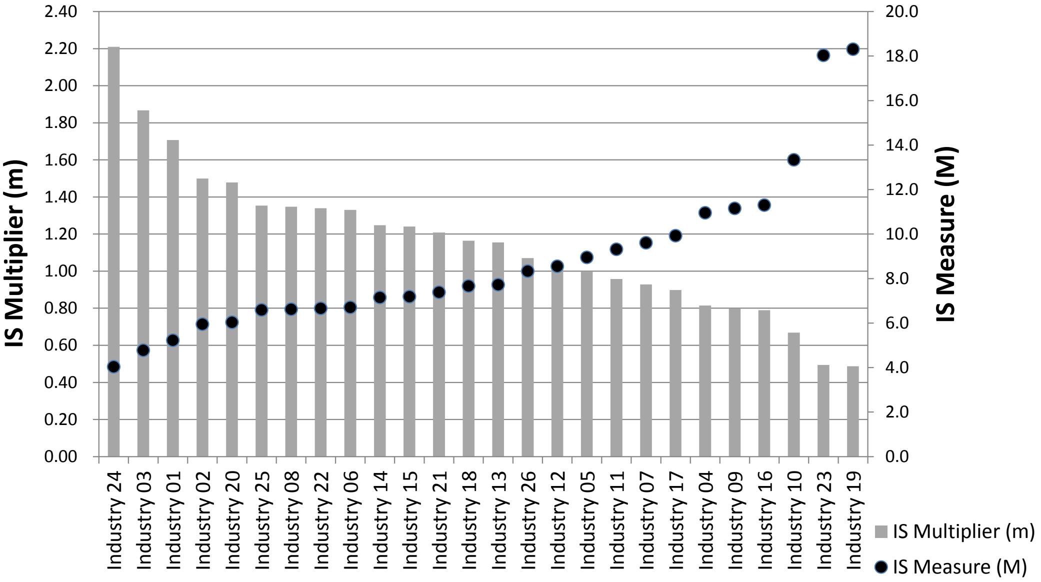


Figure 3.7: The level of IS measure and the IS multipliers of 26 industrial sectors. The results shown in this graph are calculated from the data of year 2012 provided in [104]. The names of industries shown in this table are provided in Table 4.2 in Chapter 4.

[5] Due to the limitation of our dataset in year 2012, we cannot calculate the values for 12 industries.

[6] Since we pay attention on information security, we decided to calculate the value of IS measure to the security-related trend.

Chapter 4

Security of the Virtual Currency

4.1 Introduction

For our study in the firm-level, we focus on security concerns in Japanese loyalty programs. Virtual currency (hereafter, VC) is an important medium of exchange for both virtual and physical goods and services[156]. Virtual property and currency can have economic value outside virtual economies. Trade of virtual goods for government-issued currencies (e.g. Japanese yen(¥) , US Dollar($), etc.) leads to some types of cybercrime. For example, trade of stolen precious items in online game, trade of stolen loyalty points in the dark online site, etc. In [156], virtual currency is generally classified into three categories: closed-flow, hybrid-flow, and opened-flow.

Closed-flow In the case of closed-flow, there is no interaction between virtual currency and real currencies or goods. The virtual currency in this category has no value in the real environment. Therefore, virtual environment is the only space where users can use their virtual currency.

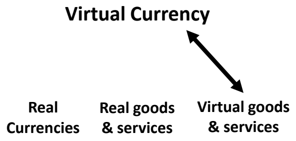
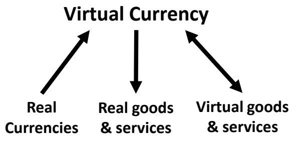
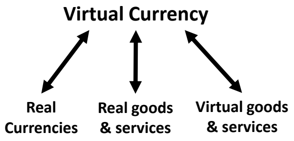
Hybrid-flow In the case of hybrid-flow, the virtual currency can be used to purchase both virtual and physical goods or services. However, virtual currencies in this category cannot be directly converted into real currencies.

Opened-flow In the case of opened-flow, users can spend their virtual currency to buy both virtual and physical goods or services. In addition, they can directly convert their possessed virtual currencies in this type into real currencies.

Illustrations of these three types of virtual currency and their examples are given in Table 4.1.

Although VC shows its importance in many applications and businesses, its insufficient concern on security management leads to some kinds of economic crimes in which cyberspace acts as the main environment. Such problems introduce various consequential researches. Due to our knowledge, there are many studies which focus on security risks in virtual economics. Since hybrid-flow and opened-flow virtual currencies are related to online activities, many researchers, including those who work on security-issues, pay attention to them. According to our survey, we found that virtual currency in massively multiplayer online games (MMOGS) and massively multiplayer online role-playing games (MMORPGS), which are hybrid-flow

Table 4.1: Three types of virtual currency and their examples according to [156].

Closed-flow	**Hybrid-flow**	**Opened-flow**
 Virtual Currency Real Currencies Real goods & services Virtual goods & services	 Virtual Currency Real Currencies Real goods & services Virtual goods & services	 Virtual Currency Real Currencies Real goods & services Virtual goods & services
– Virtual money in games	– Virtual money earned by completing tasks (Online survey, visit site, watching an advertisement, etc.) – Virtual money in massively multiplayer online role-playing games	– Crypto-currency (e.g. BitCoin, Ripple, Litecoin, etc.)

virtual currencies, and one of crypto-currencies (i.e. Bitcoin), which is an opened-flow virtual currency, are the areas to which security researches mainly pay attention.

Several studies considered massively multiplayer online games (MMOGS) in their works. Bardzell et al. surveyed some security vulnerabilities in MMOGS in general[15]. In their work, they also discussed how an attacker cheats the system by using online frauds such as phishing and click-fraud. By emailing phishing emails to the players of the game, the attacker could collect users' credentials. The attacker might use those personal information to impersonate and conduct some types of cybercrimes. Some studies considered massively multiplayer online role-playing games (MMORPGS), where players use Avatar such as Second Life (SL) and World of Warcraft (WW)[27], [81], [85]. Irwin and Slay show that MMORPGS can be used for some economic crimes[77]. In their work, they focus on money laundering and terrorism financing detection. Kiondo et al. explored some security risks in virtual economies with SL[83].

Bitcoin is another well-known actively studied virtual currency beside MMOGS and MMORPGS, In fact, Bitcoin is the most famous virtual currency among approximately 500 virtual currencies worldwide [1]. The most important property which makes Bitcoin becomes popular and attractive is the feature that provides anonymity to its users.

Christin conducted a comprehensive measurement analysis of Silk Road; an online marketplace where Bitcoin can be used for payment[28]. He analyzed description of goods, pictures, item categories, and other information which are available at Silk Road to show characteristic of this online marketplace. According to his study, many available goods on Silk Road are illegal. Such finding could be a result from the main feature of Bitcoin (i.e. availability of anonymity to users). Plohmann and Gerhards-Padilla focused on the concept of botnet-related money-making where Bitcoin plays an important role[121]. In their work, they analyzed the case of *Miner Botnet* which is a type of Botnet with a feature of mining Bitcoin. The results from their study support that this Botnet focuses on Bitcoin according to the analysis of the activities created by this Botnet.

[1] Number as of Oct 27, 2014 from [31].

Tyler and Christin studied the risk of exchanges between Bitcoin and real currency[106]. From their study, they found that famous Bitcoin exchange sites are more likely suffered from security breach. The case of Bitcoin suspension at Mt.Gox in August 2013 and a consequential bankruptcy of Mt.Gox in February 2014 could be good examples regarding this concern[48][69][88]. Especially, a remarkable one is the case of the bankruptcy of Mt.Gox in February 2014 where a huge amount of Bitcoin is said to be stolen by hackers[99]. Bitcoin is closer to real currency in terms of its liquidity than the virtual valuables (e.g. precious items) in online games.

Loyalty program (hereafter, LP) is another type of virtual currency located between online games and Bitcoin. It is used in selected environments from both virtual and physical spaces. Retail stores, credit card companies, airline companies, hotel chains and so on often use LPs to increase motivation of their customers. Beside that, many operators also introduce LPs as a tool of online advertisement . Since the main goal of LP is to increase customers' repeat-purchase behavior, there are many studies on LP in the economic aspect. Those studies mostly focus on customer behavior and effective LP management such as [19], [41], [90], [129], [155]. There are also empirical studies on this topic. For example, [89] shows that customer-oriented firms most likely adopt LPs. According to our survey, security aspects of LPs are not really well studied. Several evidences of security incidents at LPs in this chapter emphasize the necessity of consideration and study on the LP from security aspects.

4.1.1 Our Contributions and Organization of the Chapter

In Japan, LP is very popular and its liquidity is high; there is even an LP information website called *Poitan* (Point Exploration Club - ポイ探)[2]. At Poitan, information of more than 200 LPs in Japan is provided. This number is about 40-50% of numbers of crypto-currency worldwide [3]. The LPs supported there are widespread in terms of their parent businesses: airline companies, electronics discount shops, convenience stores, and so on. Poitan shows information such as estimated real-currency values of LP points, exchange/conversion rates between different LPs, and how long the conversion would take. Suppose that a consumer would like to convert a certain amount of ANA (All Nippon Airways, a star alliance member) miles, say, 20,000 miles, into JAL (Japan Airlines, a one-world alliance member) miles. In response to this query, Poitan shows all the possible conversion routes. For example, on Nov 27, 2014, Poitan showed that the following example was the route with the best rate for this conversion:

- By redeeming at ANA's website, one can convert 20,000 ANA miles (estimated value is 30,000JPY (Japanese Yen)) into 4,000 ANA Visa Card points (estimated value is 20,000JPY). This would take about 28 days.

- Likewise, at ANA Visa Card, one can convert 4,000 points into 25,000 NTT Docomo points[4] (estimated value is 25,000JPY). This would take about 60 days.

- By redeeming at NTT Docomo's website, 25,000 NTT Docomo points can be converted into 12,000 JAL miles (estimated value is 18,750JPY). This would take about 60 days.

[2] "Poi" is from "point" and "tan" is from "tanken", a Japanese word which means exploration.

[3] Number of crypto-currency worldwide as of Nov 27, 2014 from [31] is 533.

[4] NTT Docomo is the famous mobile phone operator in Japan.

Thus, the customer has to spend 148 days in total to change their 20,000 ANA mileages into 12,500 JAL mileages. According to Poitan, this route was the possible route which customer can earn the highest amount of mileage at JAL on the query day. In addition, Poitan also allows their customers to select the route ordered by the amount of point, the number of program in the route, and the number of required duration (i.e. days) for the exchange. By exchanging points between programs, the customer has to consider about a *trade-off* between estimated value and expiration date of the points. That is, although customer might lose some amount of estimated value of points after the exchange, their exchanged points will be updated with a new expiry date at the terminal loyalty program. Therefore, the loss in value of points is then changed into a longer available time of the points.

LPs in Japan are still increasing such redeeming options, and thus getting more and more popular and liquid virtual currencies. By increasing redeeming options, LP operators could attract new customers and keep their current customers. On the other hand, increasing option becomes one of the incentives to malicious people to attack the LP system. However, their security issues have not been well established and studied.

In this chapter, we investigate Japanese LP systems with focuses on their liquidity, their operating firms' security efforts, and the LP systems' actual security levels. The rest of this chapter is structured as follows. In the next section, we talk about LP in general, and show some recently reported security incidents of LPs. The situation of LPs and their security incidents are not limited to LPs in Japan. The overall image of LPs will emphasize the need of study from the information security aspect. In Section 4.3, we analyze the Japanese LP network. By this analysis, LPs from different industries are connected according to the industry of their operator. Then, in Section 4.4, we talk about liquidity from both economic and cyber viewpoints. In addition, we also show the evaluation of liquidity of the LP points. The official security-related data in industry-wise level is shown in this section. We then proceed to a detailed network analysis and a security analysis of selected LP systems in Section 4.5. In the security analysis, we consider requirements at registration, authentication, and back-up authentication systems (e.g. password recovery protocols) of LPs to observe their actual security levels. Based on our intuition that the attackers would pay more attention to more liquid LPs, we consider a basic model to derive security-liquidity implications and conduct a linear regression analysis in Section 4.6. After that, we introduce additional linear regression models to derive implications regarding impacts from the security incidents and partnership in Section 4.7. Finally, we conclude our study in Section 4.8.

4.2 Loyalty Programs and Security Incidents

Loyalty program is a marketing activity whose main objective is to encourage customers' *loyalty behaviors* by rewarding them[140]. The rewards usually take the form of *reward currency* or *point*. However, there are also other forms of reward due to differences of business[113]. For example a "buy 10, get 1 free" campaign at a coffee shop, or a present of travel set from cosmetic brands. Smith lists 52 ways of LP strategies that differentiate the LPs[144]. For example, rewards are given when customers share products or brand's news via social media (found in industry such as film corporation), when customers connect their social account to the brand's account (found in industry such as cosmetic), when customers write product reviews (found in industry such as e-commerce and electronic retailer), when some amount of goods are purchased (found in industry such as cosmetic), etc. These are only few marketing strategies which operators use to promote more brand loyalty.

Loyalty program is said to have advantages to beat price promotion strategies[141]. That is because the price promotion strategy is temporary and provides lower loyalty behavior. On the other hand, firms which operate LPs can gain more information about their customers' behaviors[40]. In fact, this point is another main purpose that motivate vendors to provide loyalty programs. These data would give more opportunities to the vendors to understand more about their customers[119]. Furthermore, vendors can use their customers' data and behaviors to refine their business strategies[44]. The analyzed customers' data could be used to tailor more attractive campaigns in the future.

Many LP operators also cooperate with their business partners so that rewards can be exchanged between different LPs. Liquidity of the reward currencies is thus increased. However, this is not the only strategy that operators use. For example, some LPs allow their customers to earn and spend their points at variety of participating shops[119]. Such strategy is said to be popular outside the U.S. In addition, some reward points can be redeemed to obtain both virtual and physical goods or services.

4.2.1 Worldwide Situation of Loyalty Programs

Despite the cooperative strategy, the world trend of the number of LP memberships is also interesting.

In the U.S., according to a report in COLLOQUY talk[17], the total number of LP memberships is more than 2.6 billion in 2012 after 26.7% growth from 2010. This increasing number of LP memberships also brought the average number of LPs per U.S. household to 21.9 from 18.4 in 2010. This growth is said to be a result from the gradual recovery rate from the recession during 2007-2009 and the introduction of new programs, especially by companies or operators which had never operated LPs before. Fig. 4.1 shows the trend of the number of membership in the U.S. between 2000 and 2012.

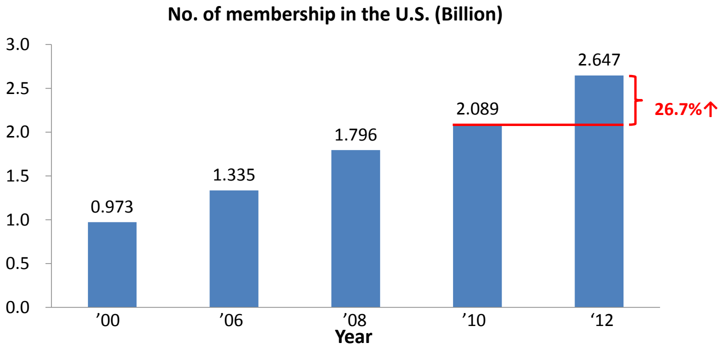


Figure 4.1: Number of membership in the U.S. according to [17](unit in Billion people).

In addition to the number of memberships, there is also a web provider who similarly provides information of LPs.This website is called "Web Flyer". It is operated by Frequent Flyer Services; an operator in the U.S.[49]. Although this website provides information such as general information of a specific LP, award/upgrade index, and mileage converter, it only focuses on the LPs in less varieties of industry (i.e. airline and hotel). Furthermore, users of the Web Flyer cannot manage their possessed points, while poitan allows their users to do so once they become its member.

According to another report in COLLOQUY talk of the same year, 90% of Canadian customers belong to at least one LP[18]. This number is very high compared to the rate of 74% in the U.S. However, due to the report, the average number of LPs per Canadian household has dropped 7.5% from 2010. The report claims that the main part of this declination rate comes from demographic factors; 1.) The 7% increment of the number of households with steady figure of membership. 2.) An immigration-driven growth of population. Other factors are such as privacy concerns, and similarity of the benefits from different LPs. Thus, LPs are still popular among Canadian customers in spite of the slightly decreasing trend. Fig. 4.2 shows the trend of the number of membership in Canada.

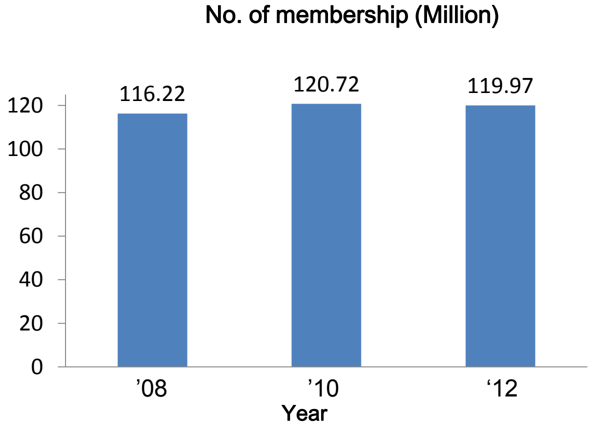


Figure 4.2: Number of membership in Canada according to [18](unit in Million people).

What about LPs in Europe? Although loyalty program marketing is quite new in Europe, it is estimated that roughly 80% of shoppers in Europe belong to at least one LP[95]. In addition, one-third of those European shoppers use two or more LPs.

In UK, according to the information provided by SAS[5], almost 95% of UK consumers possess at least one loyalty card[136]. Sixty-Five percent of UK customers join three or more LPs. Interestingly, the active customers, who regularly use their LPs, are as high as 88%. And 40% of UK customers say they are less likely to visit retailers with no LP.

LPs are also very popular in Japan. LP is well-known in Japan as a *point system*. Many shops and services from various types of businesses provide their customers a point card. According to Poitan.net, there are more than 200 active LPs in Japan. As of July, 2014, 272 LPs are covered by Poitan system. Two hundreds and thirty three of them are active domestic LPs. These are LPs which are operated by Japanese operators. In addition, due to the raw data provided by Poitan, there are 320 registered LPs at Poitan from April, 2006 to July, 2014 in total. In 2012, Japanese Statistics Bureau survey did a survey about household

[5] SAS Institute for advanced analytics, business intelligence, data management, and predictive analytics.

expenditure which includes the use of e-money and point cards[6][147]. In our study, we do not omit the e-money in our analysis since many LPs allow their customers to exchange their collected points into e-money. Furthermore, redeeming points to e-money, which includes gift vouchers, is one of the popular transactions. In addition, many LP-related cyber incidents with this type of illegal exchange exist.

The report by Japanese Statistics Bureau shows an increasing trend of the use of both e-money and point cards. 74.6% of 30,000 Japanese households possess point cards in 2012 (increased from 72.1% in 2011). And 38.7% of the same group of Japanese households possess e-money cards in 2012 (increased from 35.6% in 2011).

Beside the Japanese official statistical data, raw data from Poitan also shows a similar trend. According to the raw data from Poitan, we investigate the number of members at its site from May 2006 to August 2014. From their data, we found that the number of members keeps increasing. Especially, the number of memberships shows a prompt increment between April and December 2009. This is the similar period when LP members in the U.S. increased due to a recovery from the economic recession in 2007-2009. In addition, the promptly increasing number might also come from an influence of the media according to the site owner. This trend of members at poitan.net is shown in Fig. 4.3. The number of members at poitan.net as of August 17, 2014 is 108,964 people. About 1,068 people become members at poitan.net every month [7].

From the above evidences, the increasing trend of LP and its popularity could motivate malicious parties. Therefore, malicious parties can have an incentive to break into LP systems, abuse their extended services, and obtain benefits.

4.2.2 Security Incidents and Problems in Loyalty Programs

There are many reports and articles about security incidents related to LPs. Loyalty-card fraud (sometimes called Affinity-card fraud) is different from credit-card fraud[126]. The main difference is the retrieved information from Loyalty-card fraud could be used for identity theft. Identity theft lets an attacker easily impersonate the cardholders and break into the corresponding online systems. In addition, it could also let attackers trace the victim's routine and/or behavior which leads to other types of crime.

On the other hand, loyalty-card fraud also raises a large and potentially damaging financial risk for the provider of the loyalty programs[154]. The providers could lose the trust from their customers as well. According to [45], it is said that the breach of loyalty data would have a significant impact on the brand. The brand damage can be even fatal.

Airline industry is one of the well-known participating industries in loyalty marketing. In fact, point from the airline or mile is said to be *the fourth-biggest currency in the world in 2013*[59].

There are plenty of alerts from several airlines which are related to security incidents that occurred with frequent flyer accounts. With frequent flyer programs, generally, attackers attack the system by taking advantages of system's weakness such as weak login credentials, and phishing campaigns[92]. Attackers could, then, utilize the account owner's collected miles in various redemption ways. Many airlines also put on alert and advisory on their website

[6] Definition of *point card* in this report excludes paper-based stamp cards.

[7] Median = 518 people/month, Minimum number of new member = 65 people/month, and Maximum number of new member = 23,329 people/month.

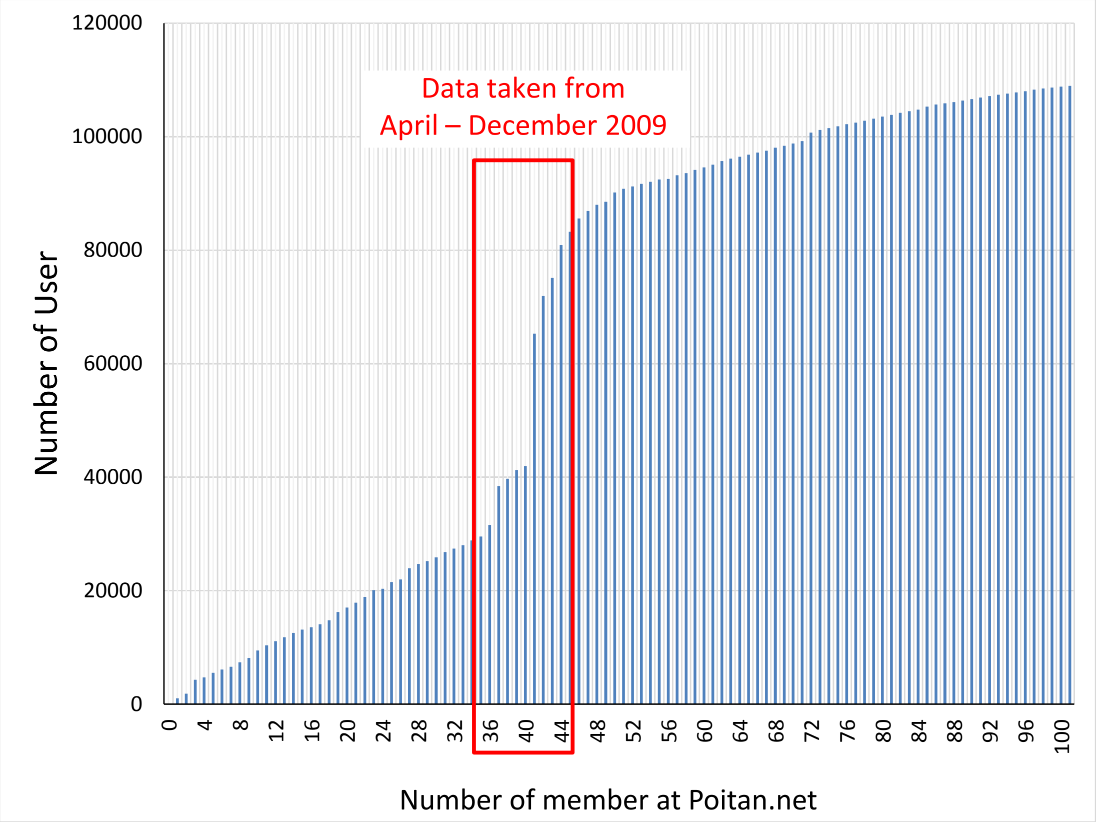


Figure 4.3: Number of member at Poitan.net from May 2006 to August 2014. Data sequence = every 30 days. The number of x-axis refers to data taken date in raw data provided by Poitan.

regarding this topic. For example, there are such announcements by U.S. airways [8], Delta airlines [9], and British airways [10].

Security of the LP is also one of the concerns in hotel industry. During the panel discussion in a conference for hotel industry at the beginning of 2014[13], gift-card and LP frauds are picked up in the discussion. They mentioned that "*as the points have been paid for before reaching the hotel, it's easy for partners (i.e. hotels) to cover their eyes to potential fraud.*". According to the recent news, there was an incident in October 2014 with the Hilton HHonors[1]. In this case, it is reported that hacker maliciously accessed into the members' account and redeemed reward points. 250,000 points of one of the victims are said to be stolen and used to reserve numbers of hotel rooms at Hilton[32]. In addition, the post fraudulent charges for more rewards points on credit cards that attached to the Hilton Honors programs were also reported[20].

In Britain, Tesco, a well-known supermarket chain, also experienced irregular activities in 2013[80]. At that time, some amounts of gift vouchers from accounts of Tesco's Clubcard

[8] http://www.usairways.com/en-US/contact/scamalert.html. Last assessed on Feb. 9, 2015.

[9] http://www.delta.com/content/www/en_US/traveling-with-us/advisories/phishing-email-alert.html. Last assessed on Feb. 9, 2015.

[10] http://www.britishairways.com/travel/flightops/public/en_gb?p_faqid=4290. Last assessed on Feb. 9, 2015.

members were spent by malicious parties. Some members also reported that some parts of their account information are slightly changed. Since they did not respond to any phishing e-mails, some members believed that their accounts have been compromised through the vulnerability of the LP system.

In addition, according to many news, security incidents on LP are usually related to identity thefts. In March 2014, Canadian police investigated a scamming case in which the suspects used fraudulent credit cards[26]. Their revealed investigation result shows that this scam included illegal redemption of the credit card points for gift cards.

Recently, there are several reports about security incidents related to LPs in Japan too. For example, in 2012, there was a report from G-Point about unauthorized accesses[50]. G-Point is a Japanese well-known online-based point system website. At G-point, besides earning points when shopping, members at this system can also earn points by completing tasks online. According to the report, 59,044 IDs at this site were compromised and points from 447 accounts were illegally used to obtain Amazon gift vouchers. The damages of this incident cost 1,617,525 JPY (or 15,808 USD[11]). In April 2013, there was a news about T-Point[137][12] when it was attacked by unauthorized accesses from both domestic and oversea origins. In this incident, points from at least 299 member accounts were illegally transferred to several different accounts. In December 2013, two Chinese college students were arrested due to the Rakuten point exchange fraud[107][13]. They bought an ID-Password list from someone through the Internet, accessed some accounts by using the list, and converted Rakuten points into e-money. JAL experienced malicious redemptions in February 2014. Some of the FFP (frequent flyer program) accounts were compromised and their JAL miles were used to obtain Amazon gift vouchers[78]. In a similar manner to that in the JAL's incident, ANA also experienced malicious redemptions in March[6]. Some of its frequent flyer member's accounts were attacked by unauthorized accesses and their mileages were illegally turned into iTunes gift codes. From many cases in Japan, it seems that malicious activities usually break into the system by unauthorized access at the customers' accounts. Then, points are usually turned into some types of e-money which can be used to purchase a wide variety of goods and services online.

However, other types of the malicious activities also occur to LP systems in Japan. An example is information leakage from attacks. According to the news in September 2014, there was a security breach at the JAL's system[153]. This security breach is said to be a result from infected computer terminals within its network. In this incident, personal information of between 110,000 and 750,000 members of JAL frequent flier club was stolen. Although JAL said that neither credit card number nor passwords were leaked, personal data such as names, addresses, genders, and workplace were said to be leaked. Anyway, the case of information leakage at JAL by the security breach at the LP system was not the first case. Such incidents also happened to other mileage clubs as well (e.g. [70]).

From the above examples, we can see that the security of LP systems becomes an important issue. The security incidents do not only introduce economic loss but also reduce trustworthiness of the LPs and their operators.

[11] Exchange rate on Feb 1, 2014. 98 JPY = 1 USD. We use this rate throughout the chapter.

[12] T-Point is a well-known and popular LP jointly operated by convenience stores, petroleum stations, pharmacies, an online shopping mall, and so on.

[13] Rakuten is a large e-commerce and information portal.

4.3 Japanese Loyalty Programs and their Networks

As stated in Section 4.2.1, there are more than 200 LPs in Japan. In addition, according to a report by the Nomura Research Institute (NRI), the gross amount of issued LP points in Japan is estimated to be over one trillion yen (or 9.8 billion US$) in 2013[112] [14]. This number is said to be the result of recovered business conditions from the Great East Japan Earthquake in 2011 and the increased number of the loyalty cards. NRI also expects that the number will keep raising in the future.

By using Poitan[122], we overview LPs in Japan. LPs supported at Poitan are categorized into 16 groups based on the types of shops or services: airlines, banks, books/CD/DVD, petroleum stations, shared point (common point system or inter-firm point system), credit card, e-money (digital cash implemented by using rechargeable IC cards), electronics retail stores, hotel chains, online shopping, online point exchange system, telecommunication (telephone companies and Internet service providers), supermarkets, railway companies, travel agencies, and others[15]. In our study, we re-categorize LPs as shown in Table 4.2 so that we can use the governmental statistics[103] in our subsequent analysis on the security and liquidity of LPs. To do so, we consider the industry of each LP's operator by focusing on their main business. For example, *ANA Mileage Club* is operated by All Nippon Airway Co.,Ltd. The main business of All Nippon Airway Co.,Ltd. is airline which belongs to industry 20: Transportation and postal activities in Table 4.2. Therefore, we assign ANA Mileage Club into industry 20: the industry of transportation and postal activities.

At Poitan, we collect the information of 247 LPs [16]. Among them, 207 LPs (84% of the 247 LPs) are operated by Japanese firms and are still active. After that, we classify these 207 LPs according to the re-categorized list of industries. As a result, we found that these LPs are operated by firms from nine industries:

Industry 09:	Manufacture of electrical machinery, equipment and supplies
Industry 13:	Miscellaneous manufacturing industries
Industry 16:	Electricity, gas, heat supply and water
Industry 17:	Video picture, sound information, broadcasting and communication
Industry 19:	Information services
Industry 20:	Transportation and postal activities
Industry 22:	Retail trade
Industry 23:	Finance and insurance
Industry 26:	Miscellaneous non-manufacturing industries

Unsurprisingly, these nine industries are those that have high interaction with customers or so-called *customer-oriented* industries[51], [146]. Fig. 4.4 shows the number of loyalty programs which are operated by Japanese operators from each industry.

[14] According to the report, the estimated amount comes from the investigation among 11 types of business; electronics retail store, credit card, mobile phone, petroleum station, supermarket, airline, convenience store, department store, online shopping, drugstore, and dining.

[15] Group of *Others* includes department stores, pharmacies, and fashion shops.

[16] Available LPs on poitan.net as of November 2013.

Table 4.2: List of industries conforming to the governmental statistics[103][*].

Industry ID	Industry Name
01	Manufacture of food, beverages, tobacco and feed
02	Manufacture of textile mill products
03	Manufacture of pulp, paper and paper product
04	Manufacture of chemical and allied products
05	Manufacture of petroleum, coal and plastic products
06	Manufacture of ceramic, stone and clay products
07	Manufacture of iron and steel
08	Manufacture of non-ferrous metals and fabricated metal products
09	Manufacture of electrical machinery, equipment and supplies
10	Manufacture of information and communication electronics equipment
11	Manufacture of transportation equipment
12	Miscellaneous machinery, equipment and supplies
13	Miscellaneous manufacturing industries
14	Agriculture, forestry, fisheries, cooperative association and mining
15	Construction
16	Electricity, gas, heat supply and water
17	Video picture, sound information, broadcasting and communications
18	Newspaper and publishing
19	Information services
20	Transportation and postal activities
21	Wholesale trade
22	Retail trade
23	Finance and insurance
24	Medical and other health services (exclude national services)
25	Education (exclude national services) and learning support
26	Miscellaneous non-manufacturing industries

[*] We use the Japanese-English contrast table in [127] when we translate the names of some industries.

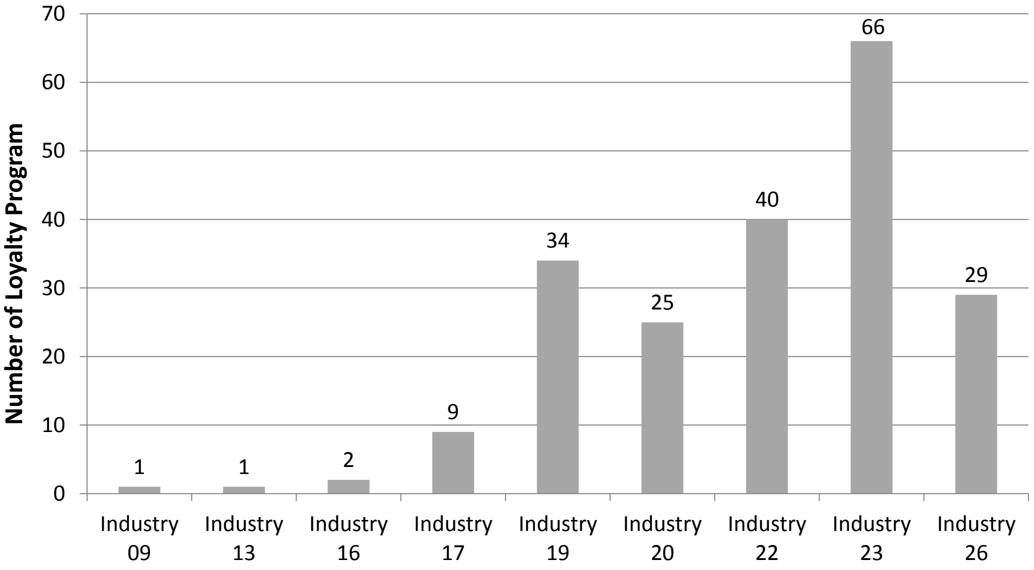


Figure 4.4: Number of loyalty programs in each industry.

Next, in Fig. 4.5, we draw a graph of the Japanese LP network. This graph of the Japanese LP network is the network in industry-level. We draw a graph of the Japanese LP network in the following way:

- Prepare nine nodes corresponding to the LPs of the above identified nine industries.
- If the points of an LP can be converted into those of a different LP but not vice versa, we say there is a *one-directional flow* from the node of the former LP to that of the latter. If the points of an LP can be converted into those of a different LP and vice versa, we say there is a *bidirectional flow* between the corresponding nodes. Thus we consider three types of flows between nodes: one-directional flow, the opposite one-directional flow, and bidirectional flow.
- Depending on the pattern of mutual exchange of LP points, classify edges between nodes into three: edges of Group 1, edges of Group 2, and edges of Group 3.

Group 1: Between the two nodes connected by the edge, there are all the three types of flows. In Fig. 4.5, we use a thick black line to represent such edges.

Group 2: Between the two nodes connected by the edge, there are two types of flows. The possibilities are *one-directional flow and the opposite one-directional flow* and *one-directional flow and bidirectional flow.* In Fig. 4.5, we use two arrows to represent such edges; one-directional flows are dash or dot black arrows, and bidirectional flows are dash gray arrows.

Group 3: Between the two nodes connected by the edge, there is only one type of flow. In Fig. 4.5, we use a single black arrow to represent such edges.

Fig.4.6 illustrates the patterns of edges of these three groups.

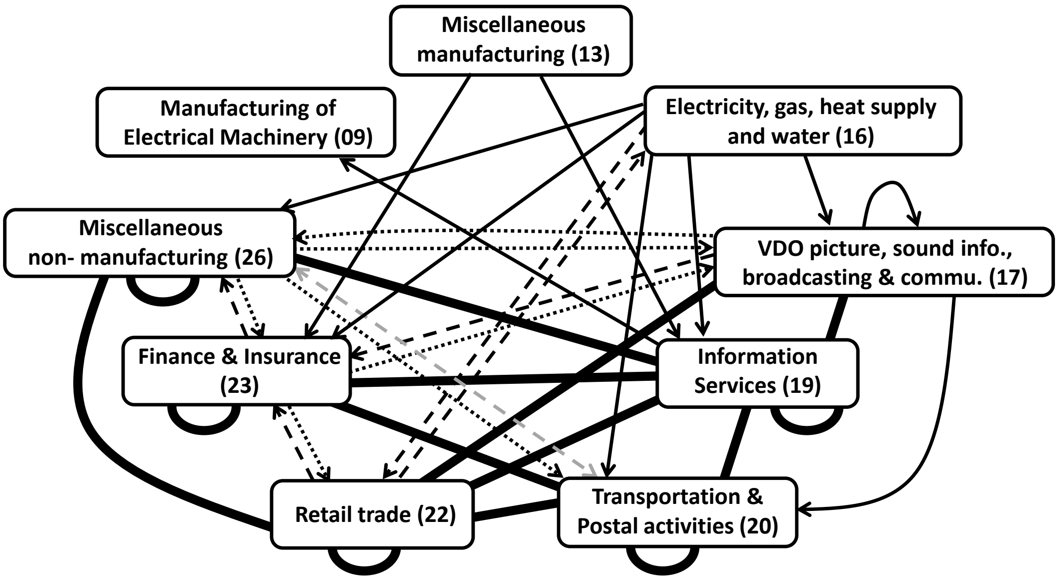
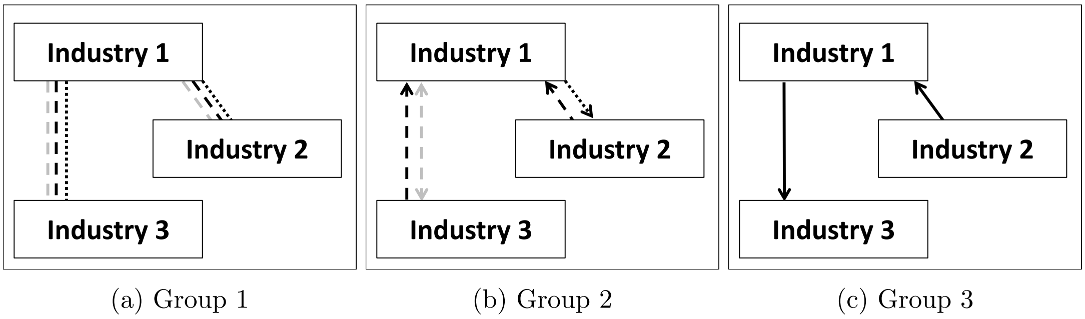

Miscellaneous manufacturing (13)
Manufacturing of Electrical Machinery (09)
Electricity, gas, heat supply and water (16)
Miscellaneous non- manufacturing (26)
VDO picture, sound info., broadcasting & commu. (17)
Finance & Insurance (23)
Information Services (19)
Retail trade (22)
Transportation & Postal activities (20)

Figure 4.5: Japanese loyalty-program (LP) network focused on the nine industries and convertibility of the LP points.



(a) Group 1 (b) Group 2 (c) Group 3

Figure 4.6: Three groups of edges between nodes.

4.4 Liquidity

In this Section, we explain general definitions of liquidity in economic and cyber perspectives. After that, we explain how we consider liquidity of the Japanese loyalty programs in our study.

4.4.1 General Definitions of Liquidity in Economic and Cyber Perspectives

In economics, liquidity is a characteristic possessed only by perfectly marketable assets[68]. An asset is said to have liquidity if its price is not affected when bought or sold in the market [76]. A study by Adrian and Shin introduces a new definition of liquidity: the rate of growth of aggregate balance sheets[4]. They explained the effect of monetary policy on overall liquidity conditions. European central bank mentions that liquidity is a *flow concept* in financial systems[111]. It also has the ability of realizing the flow. Liquidity is also important in the area of foreign exchange market. Mancini et al. explain in [96] that liquidity of foreign exchange could also affect issues such as insurance premium, appreciation of the low or high interest rate currencies, etc. Liquidity is thus becoming a topic discussed in a wider spectrum.

In the cyber world, online services such as online auction, exchanges, and e-marketplace increase liquidity, and there is a view that more secure systems provide higher liquidity[143]. Under such explanations, the level of liquidity depends on the number of channels where services are available online. With an increasing number of channels for online transaction, liquidity is getting higher and vulnerability of the organization is increased[58]. Beside the number of channels, making cyber transaction also provides anonymity to the transaction[22]. With more efficiency of the cyber transaction system, the scale of network becomes larger. The cyber transaction system then becomes popular among users. Thus, with larger numbers of users, the system becomes more liquid. This is one of the evidences that liquidity shows its importance in cyber finance. Regarding cyber applications and liquidity, topics on security, trust, and risk management become fundamental research items there.

Beside online services, crypto-currency is another area where liquidity is very important. Among hundreds of crypto-currencies, Bitcoin is one of the most popular currencies. Bitcoin is a particular implementation of crypto-currency. It is a decentralized currency which means there is no backup or control by the central bank. By using a peer-to-peer approach, user can transfer a portion of electronic cash to another without sending through any financial institution[108]. According to the mechanism of Bitcoin, it is said to provide "*true anonymity* to its users[87]. This is one of the most important advantages of the crypto-currencies. In addition, this property motivates more users to use crypto-currencies.

In one of the recent news, the chief economist of Citibank says that crypto-currencies like Bitcoin have something in common as of gold[159]. That is "*Bitcoin has to be mined, is limited in supply and has no significant utility*". There are several different views about liquidity of Bitcoin. In a country where the liquidity of real currency is problematic (e.g. Iran), Bitcoin becomes an important way of making transactions especially with business partners abroad[128]. In such cases, Bitcoin is considered highly liquid. However, in general, disadvantages of Bitcoin are discussed from the viewpoint of its limited liquidity[39]. Online currency exchange sites like Mt.Gox and Tradehill also consider this point. In the case of Tradehill, it even paused the exchange services for Bitcoin[65]. However, since Bitcoin is a decentralized currency and there are several exchange sites that support exchanges between Bitcoin and real currencies[88], the collapse of Mt.Gox in February 2014 did not affect the use and exchange of Bitcoin at other sites. At the time when the price of Bitcoin fell below 400 US$ at Mt.Gox, the value of Bitcoin at the other famous Bitcoin exchange sites such as Bitstamp[17] were around 650 US$. Therefore, it seems that effect from an incident at one of the exchange sites does not destroy the whole liquidity of this cryto-currency. As a result, by observing the discussions on the liquidity of Bitcoin, it is easy to notice that liquidity is also an important research topic regarding cyber services.

According to definitions of liquidity in economic and cyber perspectives, we explain how we consider and calculate the liquidity of loyalty programs in our work in the next subsection.

4.4.2 Liquidity of the Japanese Loyalty Programs in Industry-Level

Liquidity in the economic viewpoint is the ability of an economic agent to exchange his or her existing wealth for goods and services. And liquidity in cyber space refers to the availability of various kinds of online services. Therefore, in our study, we define *liquidity of the loyalty program* with following definition.

Definition 1. *Liquidity of the loyalty program is an ability that customer can exchange his or her points between different loyalty programs.*

From our definition of the liquidity of the LP, we consider two main factors when we calculate the liquidity scores. These two factors are *the number of corresponding type of the edges (or edge score)* and *average number of partner LPs.*

First of all, let's take a look at an overview of the liquidity of Japanese LPs' network. We evaluate the liquidity of LPs based on the classification of the edges in Fig. 4.5 and the number of their partner programs. In the industry-level, the number of corresponding type of the edge is the number of existing edge types which connect to a focusing industry. The average number of partner LPs is calculated by finding average number of partner LPs from all LPs in a focusing industry. For ease of recognition, we introduce four liquidity levels: Low (L), Medium-Low (ML), Medium-High (MH), and High (H). The evaluation process is as follows.

1. For each node (i.e. each industry), see if each type of edge is connected. Do this check for the three types of edges, and represent the results in the second column of Table 4.3 by using a three-dimensional vector where "1" denotes that the corresponding type of edge is connected and "0" denotes that the corresponding type of edge is not connected. Let x denote the number of connected edge types. For example, the node corresponding to the industry ID 09 (Manufacturing of Electrical Machinery) has an edge of Group 3 but does not have the other two types. In this industry, x=1. Likewise, the node corresponding to the industry ID 16 (Electricity, gas, heat supply and water) has edges of Group 2 and Group 3 but does not have an edge of Group 1. In this industry, x=2.

2. Compute the average number of partners (denoted by y) regarding the LPs in a node. This result is shown in the third column of Table 4.3.

3. Define *liquidity score* as xy.

   Ranges of four liquidity levels according to our calculated results are as follows.

[17] Bitstamp is an European firm.

4. If $0 \leq xy \leq 15$, we say the liquidity is low (L). If $15 < xy \leq 23$, we say the liquidity is medium-low (ML). If $23 < xy \leq 30$, we say the liquidity is medium-high (MH). Finally, if $30 < xy$, we say the liquidity is high (H). The final column of Table 4.3 shows the results.

Table 4.3: Liquidity of LPs by industry.

Industry ID	**Direction of Flows between Nodes (edges)**	**Number of Partners**		**Liquidity**
		Average number	**SD (σ)**	
09	[0,0,1]	2.0	n/a*	L
13	[0,0,1]	2.0	n/a*	L
16	[0,1,1]	6.0	1.4	L
17	[1,1,1]	15.2	14.2	H
19	[1,0,1]	14.2	16.9	MH
20	[1,1,1]	10.7	20.2	H
22	[1,1,1]	6.8	9.2	ML
23	[1,1,1]	9.0	7.1	MH
26	[1,1,1]	5.7	4.8	ML

*There is only one loyalty program.

4.5 Security of the Loyalty Programs

In this section, we firstly introduce security-related data of industries which provide loyalty programs. After that, we show actual security levels of the LP systems.

4.5.1 Security-related Data of LP Operating Firms in Industry Level

As we mentioned in Chapter 2, the investment in information security has a different objective compared to an investment in a general perspective. Therefore, in our analysis, we focus on economic data related to information security issues.

The Japanese data regarding security issues can be retrieved from *Survey on information processing: result detail part 3*[104]. This annual data is published by Ministry of Economy, Trade and Industry (METI) and publicly accessible. In this work, we refer to available data of year 2012 which is the newest data at the time we conducted this analysis. The data by METI is classified by industry. Firms are categorized into 26 industries in this data. Therefore, this data is in industry-level. We focus on information security-related data regarding size of capital stock, number of enterprise that faced security incidents, size of damage from security incidents, and size of expense of security countermeasure.

In terms of economics, capital refers to "financial assets of the firm"[76]. It also includes "factories, machinery, and equipments which are owned by firms and used in their productions". The provided data of capital size in [104] comes as the number of firms according to the range of the capital size. Therefore, we utilize the data by calculating the average size of capital per firms for each industry. Although the value of the income by each industry might reflect the demand from customers, the capital size would reflect more about the size of the industry due to its definition in the economic perspective stated above. In our case, we consider that LPs must be implemented based on some kinds of network- or IT-related systems which the operators must consider to invest as a part of their production (or business strategy). Therefore, we assume that the security effort or investment should also be considered based on the size of industry.

The issues of security incidents asked in this survey are system troubles, system halt, DoS attack, spam mail, unauthorized access, computer virus, and information leakage. We consider the number of firms which answered that they experienced security incidents.

Since there are different numbers of firms in each industry, we consider average size of damage from security incidents and average size of expense on security countermeasures, which are values per firm in each specific industry. That is, we use the same value for each firm in the same industry. For the nine industries that operate loyalty programs, the obtained data is shown in Table 4.4.

Table 4.4: Security-related data of industries in which Japanese firms operate LPs.

Industry ID, Liquidity	**Average Capital Size (in US$)**	**Number of Enterprises that Faced Security Incidents**	**Average Size of Damage from Information Security Incidents (in US$)(*)**	**Average Size of Expense on Security Countermeasures (in US$)(**)**
09, L	35,731,889$	22	12,740$(0.04%)	70,970$(0.20%)
13, L	16,454,683$	30	4,696$(0.03%)	74,118$(0.45%)
16, L	42,958,816$	10	2,450$(0.01%)	112,006$(0.26%)
17, H	13,720,000$	26	2,940$(0.02%)	70,155$(0.51%)
19, MH	10,942,132$	100	47,367$(0.43%)	151,341$(1.38%)
20, H	15,186,573$	40	7,525$(0.05%)	47,753$(0.31%)
22, ML	15,434,475$	76	8,003$(0.05%)	40,286$(0.26%)
23, MH	74,246,974$	59	12,658$(0.02%)	235,716$(0.32%)
26, ML	9,779,476$	98	2,975$(0.03%)	60,422$(0.62%)

The exchange rate between Yen to US dollar is 0.98 Yen/US$ (Rate as of Feb 1, 2014.). We use this exchange rate throughout the chapter.
*Ratio of average size of damage to average capital size.
**Ratio of average size of expense on countermeasure to average capital size.

One may expect that higher liquidity would imply larger security investments because such LPs would need higher security. On the other hand, one may expect that higher liquidity would imply larger damages because more attackers would choose such LPs. Table 4.4 supports neither of them because there is no definite tendency.

4.5.2 Actual Security Level of the Japanese Loyalty Programs

One possible way to evaluate the security strength of each loyalty program is to observe its actual security level. According to Section 4.2.2, many of security incidents at LP systems occur by unauthorized accesses. It means that the attackers would seek security vulnerability in the systems to get the access. Security engineers provide some technologies so that attacks will fail. This is vulnerability reduction in the context of a security investment model[98]. In addition, they provide other technologies so that attacks will not occur. This is threat reduction in the context of the security investment model. Since both reductions are important in the evaluation of actual security levels in an empirical study, we examine the following three processes.

Registration plays an important role in threat reduction since more strict requirements in this process bring stronger traceability; this is easy to see if, for example, we compare *registration processes requiring a physically authenticated ID* with *registration processes requiring just an active e-mail address where a free-mail address is allowed.* Traceability is important to realize a deterrent.

Authentication (login) plays an important role in vulnerability reduction since most LP systems accommodate general consumers whose literacy regarding password security is not really high. If an authentication process requires correct CAPTCHA inputs,[18] this process can contribute to threat reduction, too, due to the increasing cost of attacks. CAPTCHA is said to be one of the actions which LP operators should use to protect their systems against hacking bots and scripts[32].

Back-up authentication (e.g. password recovery) is important from the viewpoint of usable security. It should be noted again that most LP systems accommodate general consumers. They tend to require usable mechanisms as a failure mode (e.g. how to do when they forget their passwords). Since attackers would break the weakest part of a system, security of back-up authentication processes should be analyzed when we consider vulnerability reduction.

In this section, we show an example of actual security level of each loyalty program. Firstly, we select representative LPs for the nine industries focused in the previous sections (i.e. the industries which have active LPs operated by Japanese firms). Our selection is made based on existing surveys regarding the use of LPs and related customer behaviors in Japan[35], [36], [37], [38], [130], [131], [132], [133]. After that, we investigate their security-related processes stated above and consider their actual security levels. During our observation, we investigate security-related items which are appeared on the website for each process. The resultant list of selected LPs are as follows:

Industry 09:	Sony point
Industry 13:	QooPo
Industry 16:	Switch! point
Industry 17:	Softbank point
Industry 19:	T Point, PeX, G-Point
Industry 20:	ANA Mileage club, JAL Mileage bank, Suica point[19]
Industry 22:	Matsumoto Kiyoshi, Yamada Denki point[20]
Industry 23:	Mitsui Sumitomo Card (credit card company)

[18] CAPTCHA (Completely Automatic Public Turing tests to tell Computers and Humans Apart)[5] is a mechanism to avoid inputs by automated attack tools. A popular example is a text CAPTCHA which asks a user to input the texts which are displayed in a distorted manner.

[19] Suica point is operated by JR East, a big railway company in the eastern part of Japan.

[20] Yamada Denki is a big electronics retail store chain.

Industry 26: Ponta (convenience store and its partners)

In each system of the above selected LPs, we manually investigated the requirements in the three processes to see their security.[21]

Before showing the result of this investigation in the subsequent subsections, let us overview the network of the selected LPs in Fig. 4.7 where each node indicates each LP. We draw an arrow if point conversion in that direction is possible. Each arrow has the following two labels.

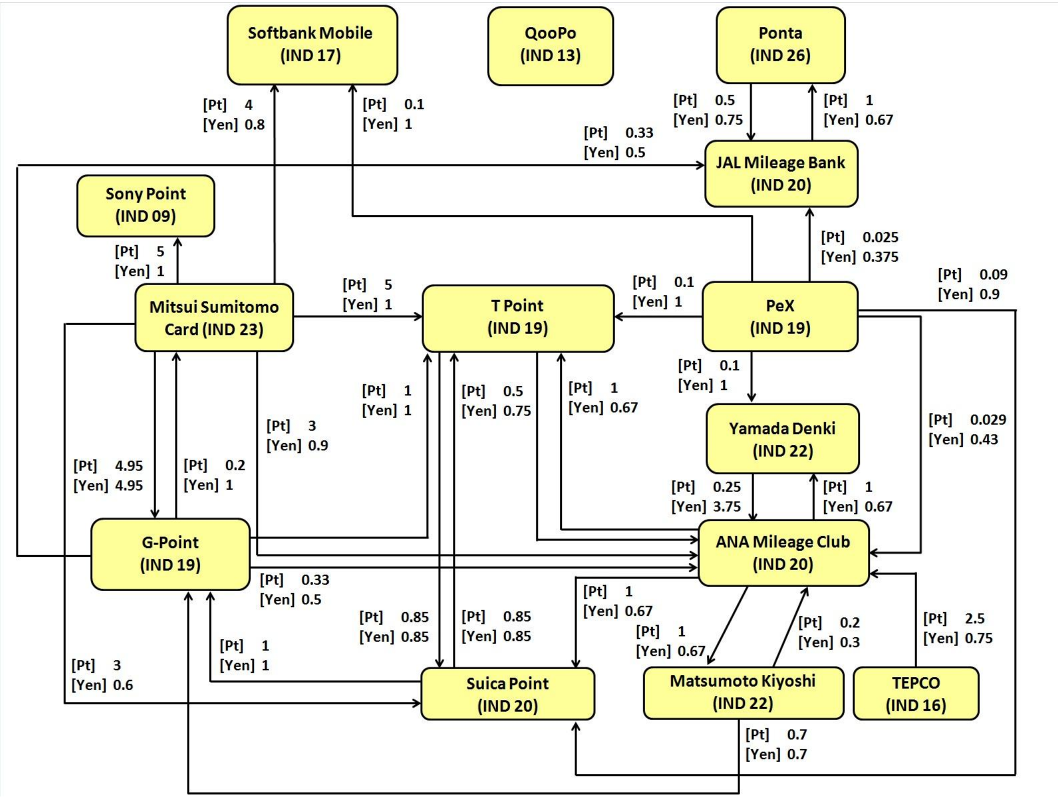


Figure 4.7: Network of selected loyalty programs from different industries.

Nominal rate of exchange: `[Pt]` is a rate of exchange in terms of the nominal amount of points (i.e. *the amount of points of the destination LP* divided by *the amount of points of the original LP*). For example, 10,000 T-points can be converted into 5,000 ANA miles, and hence the arrow from T Point to ANA Mileage Club is labeled `[Pt] 0.5`.

Actual rate of exchange: `[Yen]` is a rate of exchange in terms of the estimated real-currency values (i.e. *the estimated real-currency value of the points of the destination LP* divided by *the estimated real-currency value of the points of the origin LP*). For example, 10,000 T-points can be converted into 5,000 ANA miles. At Poitan[122], the estimated real-currency value of 10,000 T-points is 10,000 JPY, and the estimated real-

[21] We do not analyze the security of QooPo and Switch! point due to some operational difficulties. We use these two LPs only for drawing the LP network in Fig. 4.7.

currency value of 5,000 ANA miles is 7,500 JPY. Therefore, the arrow from T Point to ANA Mileage Club is labeled `[Yen] 0.75`.

In this study, we refer to the value of estimated real-currency value of point at each LP which is provided by Poitan. According to [162], value of the estimated real-currency value of point at poitan.net is calculated as follows:

$$\text{value of 1 point} = \frac{\text{value of redeemed goods or service}}{\text{number of required point}}. \tag{4.1}$$

The investigation results are shown according to the processes.

4.5.3 Registration Requirements

Table 4.5 shows the result of our investigation about what are required in the registration process. "Y" indicates that the corresponding information is required in the registration process. "Y*" indicates that the corresponding information is an option (i.e. customers do not have to provide the information but they can do so optionally.). Lastly, "–" indicates that the corresponding information is not required during the registration. The column of Softbank Point in Table 4.5 is n/a (not applicable) because its registration process is not online; the registration for LP online access is automatically done when a person becomes a customer through an offline process.

One may wonder why the symbol "Y" in the row of personal information is not classified into several different security levels since there are a wide variety of such information (e.g. first name, last name, gender, date of birth, postal address, email address, phone number (fixed and/or mobile), and so on) and the trustworthiness of the information would depend on its certification method. For example, one may expect that personal information used in LPs of airline companies would be well certified based on photo IDs. However, in Japan, we do not need to show such IDs when boarding domestic flights. Although mileage cards are sent to registered postal addresses, one can live in cheap apartment houses without rigorous IDs. Likewise, the weakest type of personal information is considered to be on a similar security level regardless of industry. Therefore, we just use the same symbol "Y" in this row.

An additional security mechanism, CAPTCHA, is used by the LPs in Industry 19 (medium-high liquidity) and the LPs in Industry 09 (low liquidity). Another countermeasure is *URL for further process*. If this is deployed, the LP's portal does not provide the URL for registration. Instead, the registration URL is e-mailed to the user. This countermeasure is used by LPs of various liquidity levels.

In conclusion, we did not find definite relationship between the liquidity and the security level of registration.

4.5.4 Authentication Requirements

All the systems use ID and password. Difference is in the types of IDs, as shown in Table 4.6. "Y" indicates information required during authentication. "Y†" indicates *one-out-of-the-two* requirements; that is, in the cases of Sony Point and T Point, either registered e-mail address or physical card number is required (users can make a choice by themselves). Finally, "–" indicates information that is not required during the authentication.

Although actual security enhancement is questionable, some LP operators with high or medium-high liquidities use their own type of ID. For example, since the use of nicknames can enhance user anonymity, the risk of abusing liquidity can get higher.

4.5.5 Back-up Authentication Requirements

As shown in Table 4.7, back-up authentication requirements of the LP systems are quite different system by system. The definition of each symbol in In Table 4.7 (i.e. symbols "Y", "Y†", and "–") are used in the same way as in Table 4.6. For this process, we did not analyze Suica Point due to some operational difficulties at the time we investigated the system. The LP of Mitsui Sumitomo card requires users to restart from the registration without offering a back-up authentication mechanism. According to our investigation, the result suggests that heuristics of back-up authentication has not been established yet.

Table 4.5: Requirements for registration.

Industry ID and Liquidity	09 L	17 H	19 MH			20 H			22 ML		23 MH	26 ML
Name of loyalty program	Sony Point	Softbank Point	T Point	PeX	G-Point	ANA Mileage Club	JAL Mileage Bank	Suica Point	Matsumoto Kiyoshi	Yamada Denki	Mitsui Sumitomo Card	Ponta
Necessity of physical card	–	n/a	Y	–	–	Y	Y	Y	Y	–	Y	Y
Terms and conditions on personal information	Y	n/a	Y	Y	–	Y	–	Y	Y	Y	Y	–
Personal Information	–	n/a	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Affiliation	–	n/a	–	–	Y*	Y*	Y*	–	–	–	–	–
Length of password	6–10	n/a	from 6	8–16	8–36	4	6	6–8	4–8	6–20	6–8	from 8
CAPTCHA	Y	n/a	Y	Y	Y	–	–	–	–	–	–	–
URL for further process	Y	n/a	–	Y	–	–	–	–	–	Y	–	Y
Answer to secret question	–	n/a	–	Y	–	–	–	–	–	–	–	–

Table 4.6: Types of required user IDs in authentication process.

Industry ID and Liquidity	09 L	17 H	19 MH			20 H			22 ML		23 MH	26 ML
Name of loyalty program	Sony Point	Softbank Point	T Point	PeX	G-Point	ANA Mileage Club	JAL Mileage Bank	Suica Point	Matsumoto Kiyoshi	Yamada Denki	Mitsui Sumitomo Card	Ponta
Registered email address	Y†	–	Y†	Y	–	–	–	–	–	Y	–	–
Physical card number	Y†	–	Y†	–	–	Y	Y	–	Y	–	–	Y
Others	–	Mobile number	–	–	Self registered nickname	–	–	Self registered nickname	–	–	System generated ID	–

Table 4.7: Requirements during back-up authentication processes.

Industry ID and Liquidity	09 L	17 H	19 MH			20 H			22 ML		23 MH	26 ML
Name of loyalty program	Sony Point	Softbank Point	T Point	PeX	G-Point	ANA Mileage Club	JAL Mileage Bank	Suica Point	Matsumoto Kiyoshi	Yamada Denki	Mitsui Sumitomo Card	Ponta
Registered email address	Y†	–	Y†	Y	Y	–	–	n/a	Y	Y	n/a	Y
Physical card number	Y†	–	Y†	–	–	Y	Y	n/a	Y	–	n/a	Y
Others	–	Mobile number	–	–	–	–	–	n/a	–	–	n/a	–
Firstname & lastname	–	–	–	–	–	–	Y	n/a	–	–	n/a	Y
Date of birth	–	–	Y	–	–	Y	Y	n/a	–	Y	n/a	Y
Registered phone number	–	–	–	–	–	Y	–	n/a	–	–	n/a	Y
Type of registered phone number	–	–	–	–	–	Y	–	n/a	–	–	n/a	–
CAPTCHA	–	–	–	Y	–	–	–	n/a	–	–	n/a	–
Security code	–	Y	–	–	–	–	–	n/a	–	–	n/a	–
URL for further process	Y	–	Y	Y	–	Y	Y	n/a	Y	Y	n/a	Y
Time-limitation of the URL	Y	–	Y	Y	–	Y	Y	n/a	–	Y	n/a	Y
Token's period	24 hrs	–	24 hrs	7 days	–	24 hrs	24 hrs	n/a	–	1 hr	n/a	24 hrs

4.6 Security-Liquidity Implications

As we can learn from the examples in Section 4.2.2, illegal exchange of LP points are often used in LP security incidents. Therefore, intuitively, an attacker would have higher incentive to compromise the LP which has higher liquidity. In this section, we investigate a relationship between security and liquidity by linear regression analysis.

4.6.1 Data

There are many factors that could increase an impact from security incident at the LP. Financial damage is a basic factor when we consider the impact from a security incident in general. In addition, we focus on popularity of the LP because popular LPs would not only have large news values but also be preferred by attackers.

At Poitan, based on the monthly statistics of queries, we can see the top 20 popular LPs or LP pairs as shown in Table 4.8. The "Utilized pair of exchange" column in Table 4.8 shows the top 20 queries made at Poitan in April 2014[125]; exchange of T Point into ANA mileage is the most frequently queried pattern. The "Origin LP" column in Table 4.8 shows the top 20 LPs which were used as the origins of the exchanges in queries made at Poitan in April 2014[124]; exchange of T Point into something else is the most frequently queried pattern when we focus on the origin. Likewise, "Destination LP" column in Table 4.8 shows the top 20 LPs which were used as the destinations of the exchanges[123].

We select 82 Japanese LPs or 33% of Japanese LPs available at Poitan as our samples in this study so that most of the top 20 rankers are included and each of the security analyses explained in Section 4.5 can be done in most of the samples.

We use the following proxy variables in our analysis:

1. Impact from incidents
   Since illegal exchanges originate from compromised LP accounts, we focus on the "Origin LP" ranking, and observe the ranking score, $rank_i$, of LP$_i$ ($i = 1, 2, \cdots, 82$) by using the following table.

Rank as the origin LP	Score
1–5	5
6–10	4
11-15	3
16-20	2
out of rank	1

   And then, we calculate the impact proxy as follows:

   $$impact_i = damage_{IND_i} * rank_i \tag{4.2}$$

   where

i	is	the index of each selected LP.
IND_i	is	the industry ID of the industry LP$_i$ belongs to.
$damage_{IND_i}$	is	the average amount of damage from incidents in industry IND_i.
$rank_i$	is	the ranking score of LP$_i$.

   The impact from 4.2 is the value in firm-level.

Table 4.8: Rank of Loyalty Programs (April 2014).

Rank	Utilized pair of exchange	Origin LP	Destination LP
1	T Point → ANA	T Point	ANA
2	G Point → ANA	ANA	JAL
3	PeX → ANA	Rakuten	Rakuten
4	Habitas → ANA	JAL	T Point
5	Rakuten → ANA	G Point	Amazon Gift Voucher
6	T Point → JAL	PeX	Rakuten Edy
7	G Point → JAL	NTT Docomo	G Point
8	ANA → JAL	Hapitas	Ponta
9	ANA → Rakuten	Ponta	PeX
10	Net Mile → ANA	Net Mile	NTT Docomo
11	PeX → JAL	Mitsui Sumitomo Card	Suica Point
12	Rakuten → JAL	Credit Saison	Suica
13	JAL → ANA	JCB Card	Cash (Rakuten Bank)
14	Ponta → JAL	Biccamera	WAON
15	Hapitas → JAL	American Express	nanaco Point
16	NTT Docomo → JAL	Life Card	Biccamera
17	nanaco Point → ANA	Macro Mill	Yodobashi Camera
18	Ponta → ANA	Yamada Denki	nanaco
19	Credit Saison → ANA	Diners Club	WAON Point
20	ANA → T Point	nanaco Point	United Airlines

2. Liquidity
   We calculate an LP-wise (i.e. firm-level) liquidity score $liquidity_i = xy$ by using a similar methodology to that used in sub-Section 4.4.2. In our study, we classify liquidity into two types; *unweighted liquidity score* and *weighted liquidity score.*

   (a) Unweighted liquidity score
   In particular, we firstly consider the edge types between LP$_i$ and LPs from the nine industries which operate LPs and obtain the value of x. The existing type of edges between nodes is counted as one for all types. That is the edge of group 1, the edge of group 2, and the edge of group 3 have the same weight of 1. We then obtain the value of y by counting the number of the exchange partners of LP$_i$.

   As state above, the weight of the edge of group 1, 2, and 3 in unweighted liquidity score are the same. Thus, the definition of liquidity score might be incomplete. Therefore, we introduce weighted liquidity score to enhance our definition of liquidity.

   (b) Weighted liquidity score
   For the weighted liquidity score, the three groups of edges are re-classified into five groups as shown in Fig. 4.8. We add consideration on the number of arrows and the direction of each arrow when we consider the weighted liquidity score. As a result, the edge of group 2 is re-classified into two groups of 2.a and 2.b. Likewise, the edge of group 3 is re-classified into two groups of 3.a and 3.b. A five-directional vector is used instead of a three-directional vector mentioned in sub-Section 4.4.2.

   The weight of each group is calculated as follows:

$$weight_g = arrow_g * direction_g \tag{4.3}$$

   where

g	indicates an edge group (1, 2.a, 2.b, 3.a, or 3.b).
$weight_g$	is the weight of the group g.
$arrow_g$	is the number of arrows in group g.
$direction_g$	is the number of existing direction(s) of arrows in group g.

   There are two types of weighted liquidity score in our study.

   i. Weighted liquidity score type I
   In this type of liquidity, we consider the exchangeability of the points between LP$_i$ and the nine industries. We check if each type of edges in five-directional vector is connected between LP$_i$ and the nine industries or not. If connected, we set the value of the corresponding component in the five-directional vector to be 1. Otherwise, we set the value to be 0. Finally, the value of x' in weighted liquidity score type I is calculated as follows:

$$x' = \sum_g (\text{existence of edge of group}g * weight_g). \tag{4.4}$$

   For example, suppose an LP is connected with three industries through an edge of Group 1 and two industries through an edge of Group 3.b. In this case, the corresponding five-directional vector is [1,0,0,0,1]. Therefore, the value of x' is (1*12) + (1*1) = 13. Suppose that another LP is connected with just

one industry through the edge of Group 1 and just one industry through the edge of Group 3.b. In this case, the corresponding five-directional vector is also [1,0,0,0,1] and the value of x' is (1*12) + (1*1) = 13. As a result, under this detailed definition, there is no difference between an LP which connects to many industries through a specific group of edge and an LP which connects to only one industry through a specific group of edge.
Similarly to the unweighted liquidity score, we obtain the value of y by counting the number of the exchange partners of LP$_i$. The liquidity score in this case is defined as $x'y$.

ii. Weighted liquidity score type II
In the weighted liquidity score type II, beside consideration on the exchangeability of the point between LP$_i$ and the nine industries, we also consider how many industries are connected with LP$_i$ through a particular edge group. In particular, the value of each component in the five-directional vector refers to the number of partner industries are connected to LP$_i$ through a specific group of edge type. The value of x' in weighted liquidity score type II is calculated as follows:

$$x' = \sum_g (\text{the number of industry that connected to LP}_i \text{ through edge of group} g * weight_g). \tag{4.5}$$

For example, suppose an LP is connected with three industries through an edge of Group 1 and two industries through an edge of Group 3.b. In this

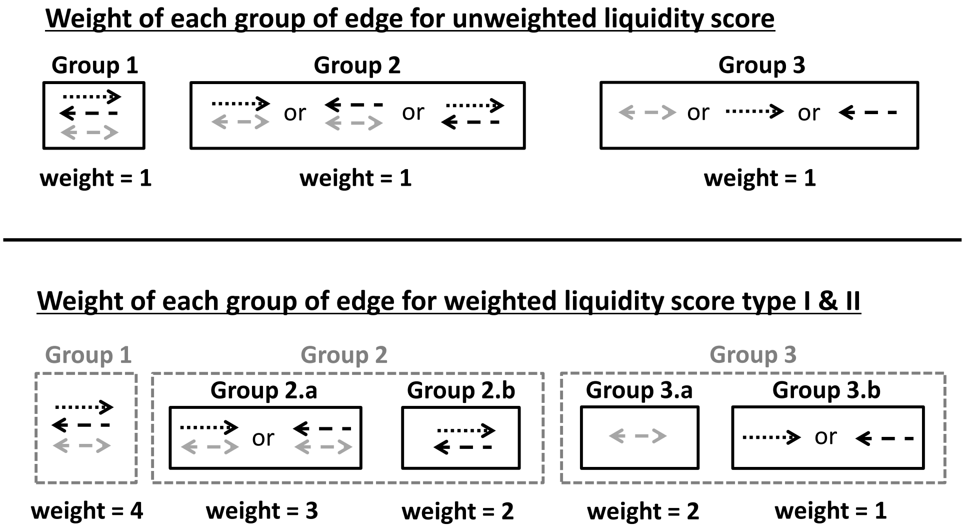


Figure 4.8: Groups of edges between node for unweighted liquidity score and weighted liquidity score. Black dotted arrow refers to a flow of *coming in only*. Black dashed arrow refers to a flow of *going out only*, And Gray dashed arrow refers to a flow of *both directions* where points can be exchanged back-and-forth between LPs in the two industries.

case, the corresponding five-directional vector is [3,0,0,0,2]. Therefore, the value of x' is (3*12) + (2*1) = 38. Suppose that another LP is connected with just one industry through an edge of Group 1 and just one industry through an edge of Group 3.b. In this case, the corresponding five-directional vector is also [1,0,0,0,1] and the value of x' is (1*12) + (1*1) = 13. Hence, this detailed definition shows differences between an LP which connects to many industries through a specific group of edge and an LP which connects to only one industry through a specific group of edge.

Similarly to the unweighted liquidity score and weighted liquidity score type I, we obtain the value of y by counting the number of the exchange partners of LP$_i$. The liquidity score in this case is defined as $x'y$.

3. Security score

In Section 4.5, we investigated a lot of security-related requirements in the registration process, the authentication (login) process, and the back-up authentication process of each LP. In this section, we focus on the important requirements listed below.

Process	Requirements
Registration	– Trusted information (e.g. certified information, security code, information which is matched to certifiable document). – Necessity of physical card or account. – Implementation of additional security techniques (e.g. CAPTCHA, secret question).
Authentication (login)	– Data which increases difficulty to log into the account. (e.g. mobile number, physical card number, system generated ID).
Back-up authentication (password recovery)	– Trusted information. – Physical card or account number.

We compute the security score, $secscore_i$, of LP$_i$ as follows:

$$secscore_i = \frac{\text{the number of satisfied requirements in LP}_i}{\text{the number of requirements about which we can obtain data regarding LP}_i}. \tag{4.6}$$

For example, let us consider Table 4.9. In this case, $secscore_1 = 5/6 = 0.83$ and $secscore_2 = 2/5 = 0.40$.

Table 4.9: Security requirements (n/a means that data is unavailable). The value of 1 indicates that the corresponding requirement is satisfied. The value of 0 indicates that the corresponding requirement is not satisfied.

	Security-related Requirements					
	Registration			Login	Back-up authentication	
	Trusted information	Physical card or account	Implementation of security techniques	Data which increase difficulty	Trusted information	Physical card or account number
LP_1	1	1	1	0	1	1
LP_2	0	1	n/a	0	0	1
LP_3	0	0	0	0	0	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮
LP_n	0	1	0	n/a	n/a	n/a

4.6.2 The Model

Based on the viewpoints mentioned at the beginning of Section 4.6, we firstly examine the following two hypotheses:

Hypothesis 1. *The impact from security incidents on an origin LP would be reduced if the LP operator implements stronger security requirements in registration, authentication (login), and back-up authentication processes.*

Hypothesis 2. *The impact from security incidents on an origin LP would be increased if the LP has higher liquidity.*

We use the following linear regression model to test the above two hypotheses.

$$impact_i = \beta_0 + \beta_1 expense_i + \beta_2 liquidity_i + \beta_3 secscore_i \tag{4.7}$$

where $expense_i$ is the average size of expense on countermeasures in the industry which LP_i belongs to.

4.6.3 The Analysis of Basic Model with Unweighted Liquidity Score

We begin our analysis from the case when we consider only the existence of a specific group of edge. This analysis of basic model is used to give basic ideas regarding importance of security and liquidity of the LP.

Verifying the Data

Firstly, we verify the independence of the explanatory variables in the model by checking their correlation coefficients. We found that the correlation coefficients are very low; the correlation coefficients between *expense* and *secscore*, *expense* and *liquidity*, and *secscore* and *liquidity* are 0.272064, 0.040581, and -0.044189, respectively. Thus, we can confirm that our explanatory variables are mutually independent.

Result of the Regression Analysis

The result of the linear regression analysis of our basic model is shown in Table 4.10.

Table 4.10: The results of the linear regression analysis of the model with unweighted liquidity score.

Variables	Coefficient	p-value
Intercept	4311.91	0.6401
expense	0.19	0.0027***
liquidity	643.69	$3.49e^{-9}$***
secscore	-30138.18	0.0115**
R^2	0.449729	
DW-Stat	1.276663	

** indicates significance at 5% level.
*** indicates significance at 1% level.
DW-Stat is the value of *Durbin-Watson statistic.*
The value closes to 2 means the problem of auto-correlation is unlikely occurred.

Regarding the statistical significance, we can see that p-values are very low for all of the explanatory variables. That is, all explanatory variables in our model are significant. The negative sign of the coefficient of *secscore* implies that satisfying more security requirements would reduce the impact from security incidents. Hence, Hypothesis 1 is supported.

Next, let's consider liquidity. The positive sign of the coefficient of *liquidity* implies that higher liquidity would increase the impact from security incidents. In addition, the p-value of *liquidity* is extremely low. Hence, Hypothesis 2 is also supported.

Although the p-value of *expense* shows significance of this variable, we do not provide a corresponding hypothesis this time. That is because we used not LP-wise but industry-wise data for *expense*.

4.6.4 The Advanced Analysis of the Basic Model with Weighted Liquidity Score

From sub-Section 4.6.3, we show that liquidity and security-related requirements of LPs are important. In this sub-Section, we conduct further analyses with weighted liquidity scores type I and II to check the significance and appropriateness of our enhanced definition of liquidity. We test the model (4.7) with both types of weighted liquidity score.

1. Advanced analysis of the basic model with weighted liquidity score type I

Verifying the Data

Similarly to the analysis in sub-Section 4.6.3, we firstly verify the independence of the explanatory variables in the model by checking their correlation coefficients. The correlation coefficients between *expense* and *secscore*, *expense* and *liquidity*, and *secscore* and *liquidity* are 0.272064, 0.016007, and −0.070313, respectively. These values are still very low. Thus, we can also confirm that our explanatory variables for this set of data are mutually independent.

Result of the Regression Analysis

The result of the linear regression analysis from our basic model with weighted liquidity score type I is shown in Table 4.11.

Table 4.11: The results of the linear regression analysis of the model with weighted liquidity score type I.

Variables	Coefficient	p-value
Intercept	8218.59	0.3716
expense	0.20	0.0020***
liquidity	96.30	$7.57e^{-9}$***
secscore	−28664.13	0.0173**
R^2	0.438508	
DW-Stat	1.388232	

** indicates significance at 5% level.
*** indicates significance at 1% level.

The p-values of all explanatory variables are very low. This means that all explanatory variables are significant to the model. We will discuss more about the result from this analysis after introducing the results from the advanced analysis of the basic model with weighted liquidity score type II.

2. Advanced analysis of the basic model with weighted liquidity score type II

Verifying the Data

We also verify the independence of the explanatory variables in the model with weighted liquidity score type II by checking their correlation coefficients. The correlation coefficients between *expense* and *secscore*, *expense* and *liquidity*, and *secscore* and *liquidity* are 0.272064, 0.00587, and −0.026415, respectively. These values are still very low. Thus we can confirm that our explanatory variables for this set of data are also mutually independent.

Result of the Regression Analysis

The result of the linear regression analysis of our basic model with weighted liquidity score type II is shown in Table 4.12.

Table 4.12: The results of the linear regression analysis of the model with weighted liquidity score type II.

Variables	Coefficient	p-value
Intercept	9381.22	0.3118
expense	0.21	0.0014^{***}
liquidity	49.76	$1.73e^{-8***}$
secscore	-32429.46	0.0078^{***}
R^2	0.426248	
DW-Stat	1.231269	

*** indicates significance at 1% level.

Similarly to the advanced analysis with weighted liquidity score type I, the p-values of all explanatory variables in this analysis are very low. Such results mean that all explanatory variables are significant to the model.

3. Comparison of the results
Compared to the result from our preliminary analysis in Table 4.6.3, the results from the advanced analyses with more detailed definitions of liquidity in Table 4.11 and Table 4.12 support the hypotheses stronger. Thus LP operators should be more highly motivated to tackle cyber security issues.

   The results of the advanced analysis support both hypotheses 1 and 2 stronger than the preliminary analysis. Especially, the result from the analysis with weighted liquidity score type II where the significance of *secscore* is raised. In addition, this variable is directly related to the security of the LP systems. Such results imply and emphasize the necessity of stronger security in LP systems.

4.7 The Implications of the Impact from Security Incidents and Partnership

The analyses of security-liquidity implication in Section 4.6 show the importance of liquidity, as well as, the importance of security level of the LP systems. In this section, we would like to emphasize the problem of network externalities of information security. To do so, we analyze the impact from security incidents which occurs at the systems of both origin LPs and destination LPs. We consider the scenarios when there are security incidents at the origin or destination LPs. Under scenarios in this section, we also expect that the impact at a specific system could affect its partner systems.

For this analysis, we use the same dataset which we used when we tested hypotheses 1 and 2 in Section 4.6. That is, the data of *expense*, *liquidity*, and *secscore* are data which belong to the origin LP. We select the detailed definition of liquidity score (i.e. weighted liquidity score type II) for the analyses in this section as the result from the analysis with weighted liquidity score type II raises the importance of the variable *secscore*.

4.7.1 The Model

Based on our objectives described at the beginning of this section, we examine the following hypotheses:

Hypothesis 3. *The impact from security incidents on an origin LP would be increased if the incident occurs at a destination LP with which they have partnership.*

Hypothesis 4. *The impact from security incidents on destination LPs would be increased if the incident occurs at an origin LP with which they have partnership.*

Hypothesis 5. *The liquidity and security level of the origin LP would give an indirect effect on its partners via impacts from security incidents.*

Hypotheses 3 and 4 are used to study the effect of the partnership between LPs. In addition, these implications are used to emphasize the issues of network externalities in the economics of information security when the incident occurs at one of the systems in the network.

Hypothesis 5 is also used to emphasize the topic regarding network externalities in the economics of information security. From this hypothesis, we expect that the vulnerability in a specific system could affect other systems via interconnectivity initiated between them. Differently from hypotheses 3 and 4, we would like to raise an importance of the investment in information security by the operator of each system in this hypothesis.

We use the following two linear regression models to test the above three hypotheses.

$$impact\_org_i = \beta_0 + \beta_1 impact\_dest_j + \beta_2 expense_i + \beta_3 liquidity_i + \beta_4 secscore_i \tag{4.8}$$

$$impact\_dest_j = \beta_0 + \beta_1 impact\_org_i + \beta_2 expense_i + \beta_3 liquidity_i + \beta_4 secscore_i \tag{4.9}$$

where

i	is the index of the origin LP (1,...,82).
j	is the index of the destination LP (1,...,82).
$impact\_org_i$	is the impact from security incidents at origin LP$_i$.
$impact\_dest_j$	is the impact from security incidents at destination LP$_j$.
$expense_i$	is the average size of expense on countermeasures in the industry which LP$_i$ belongs to.

The values of *liquidity* and *secscore* used in both models are the values of *liquidity* and *secscore* of the origin LP.

The model 4.8 is used to find the impact from security incidents at the destination LP on the origin LP. Likewise, the model 4.9 is used to find the impact from security incidents at the origin LP on the destination LP.

4.7.2 Verifying the Data

Similarly to Section 4.6, we firstly verify the independence of explanatory variables which are used in model 4.8 and 4.9.

For the model 4.8, the correlation coefficients between explanatory variables are shown in Table 4.13. For the model 4.9, the correlation coefficients between explanatory variables are shown in Table 4.14.

Table 4.13: Correlation coefficients between explanatory variables in the model 4.8.

Variables	*impact_org*	*expense*	*impact_dest*	*liquidity*	*secscore*
impact_org	1	0.2368	0.8903	0.5609	−0.1811
expense		1	0.2370	0.0059	0.2721
impact_dest			1	0.4550	−0.1020
liquidity				1	−0.0264
secscore					1

Table 4.14: Correlation coefficients between explanatory variables in the model 4.9.

Variables	*impact_dest*	*expense*	*impact_org*	*liquidity*	*secscore*
impact_dest	1	0.2370	0.8903	0.4550	−0.1020
expense		1	0.2368	0.0059	0.2721
impact_org			1	0.5609	−0.1811
liquidity				1	−0.0264
secscore					1

From Table 4.13 and Table 4.14, we found that the correlation coefficient between *impact_dest* and *liquidity* in the model 4.8 and the correlation coefficient between *impact_org* and *liquidity* in the model 4.9 are slightly high compared to the correlation coefficients when we tested other pairs of explanatory variables.

In terms of statistics, the value of correlation coefficient is bounded between −1 and 1. The value of Corr(X,Y) = 0 (i.e. correlation coefficient between variables X and Y equals 0) means that there is no linear relationship between X and Y. In other word, they are independent. The value of correlation coefficient towards −1 or 1 means that they are somehow correlated between each other. Such correlation could lead to some problems such as autocorrelation in the statistical analysis. As in the least-squared regression which is a common type of linear regression, the correlation coefficients at 0.4550 in the model 4.8 and 0.5609 in the model 4.9 are said to have low and moderate correlations, respectively[161].

The autocorrelation is a correlation between the errors in different time periods[160]. This problem occurs when we test the time series or panel data model. However, data which we used in our model is a cross-sectional data set[22]. Therefore, the problem of autocorrelation does not likely occur. As a result, the explanatory variables in both models are still acceptable for our study.

[22] Cross-sectional data set is a set of data collected by sampling a population at a given point in time[160].

4.7.3 Results of the Regression Analyses

The results of the linear regression analyses of our model 4.8 and 4.9 are shown in Tables 4.15 and 4.16, respectively.

Table 4.15: The results of the linear regression analysis of the model 4.8.

Variables	Coefficient	p-value
Intercept	2315.09	0.6408
impact_dest	0.79	$4.27e^{-22***}$
expense	0.06	0.0867^{*}
liquidity	18.99	0.0002^{***}
secscore	−15921.73	0.0158^{**}
R^2	0.838842	
DW-Stat	2.024001	

* indicates significance at 10% level.
** indicates significance at 5% level.
*** indicates significance at 1% level.

Table 4.16: The results of the linear regression analysis of the model 4.9.

Variables	Coefficient	p-value
Intercept	402.87	0.9394
impact_org	0.91	$4.27e^{-22***}$
expense	−0.003	0.9317
liquidity	−6.31	0.2597
secscore	8578.150	0.2301
R^2	0.799882	
DW-Stat	2.051867	

*** indicates significance at 1% level.

1. The impact from security incidents at the destination LP on the origin LP
   First of all, let's consider the statistical result from the linear regression model 4.8.

   From the result, we can see that p-value of *liquidity* is very low. Three asterisks after the p-value of *impact_dest* and *liquidity* of the origin LP show the significance of this variable at 1% level. This means that the impact from security incidents at the destination LP and liquidity of the origin LP show strong significance to the impact at the origin LP. Once there happens a security incident at the destination LP, the origin LP, which is connected to that breached destination LP, would also be affected. Hence, Hypothesis 3 is supported.

   Although p-value of *secscore* of the origin LP shows lower significance to the impact on origin LP, this variable is still significant in the model. In addition, the high value of

R^2 implies that the model is appropriate[23].

Beside the importance of *impact_dest*, the coefficients of *liquidity* and *secscore* from the model 4.8 also support our Hypotheses 1 and 2 in Section 4.6. That is, the coefficient of *secscore* is a negative sign which implies that satisfying more security requirement would reduce the impact from security incidents. On the other hand, the positive sign of the coefficient of *liquidity* implies that higher liquidity would increase the impact from security incidents.

With the same reason as in Section 4.6 regarding data of *expense*, we do not give any implication regarding this variable for this analysis.

2. The impact from security incident at the origin LP on the destination LP
According to the result from the linear regression model 4.9, we can see that the p-value of *impact_org* is very low. That is, the impact from security incidents at the origin LP has high effects on the impact at the destination LP. Hence, Hypothesis 4 is supported. In addition, let consider the values of coefficients between *impact_org* and *impact_dest* from the test of impact from destination LP on origin LP in Table 4.15 and the test of impact from origin LP on destination LP in Table 4.16. According to the results in both tables, we found that the impact from security incidents at the systems of origin LP on destination LP show larger size of impact due to larger value of coefficient at the same level of significance. Therefore, LP operators should also pay attention to the security at the transaction process.

   Next, let's consider p-values of *liquidity* and *secscore*. According to the result in Table 4.9, p-values of both variables are higher than 0.1. In statistics, the value of p-value which is higher than 0.1 implies that an explanation variable is *insignificant* to the explained variable. In our case, such result implied that the liquidity and security of the origin LP do not have direct influence on the impact on the destination LP.

   However, since the Hypothesis 4 is supported, the size of impact at the destination LP would depend on the size of impact from security incidents at the origin LP where liquidity and security level of its own system are significant. This is an indirect effect of the liquidity and security level of the origin LP on the destination LP. Hence, Hypothesis 5 is also supported.

   From such results, we could point out that if the operators of each system concern security of their systems and implement stronger security-related requirements, the security of the whole LP network would be increased. Then the impact from security incidents would be lower.

4.8 Conclusion

In this chapter, we first showed the worldwide trend of loyalty programs and security incidents related to the loyalty programs. We also showed that the LP network in Japan is really large and that associated virtual currencies are very liquid. We then identified four industries with high/medium-high liquidity: *Video picture, sound information, broadcasting and communications*, *Information services*, *Transportation and postal activities*, and *Finance and insurance.*

[23] Value of R^2 is bounded between 0 and 1. The value towards 1 implies that independent variables explain much of the variation in the dependent variable in the sample[160].

It should be noted that major incidents [6], [50], [107], [78], [137] actually happened in these four industries. We should be careful because more attackers would choose such highly liquid LPs.

One may expect that higher liquidity would imply larger security efforts and stronger countermeasures because such LPs would need higher security. However, we found no definite relationship among liquidity, operating firms' security efforts, and LP systems' actual security levels.

After investigating the network of Japanese LPs, we conducted a linear regression analysis and supported two hypotheses: the impact of LP security incidents gets lower if stronger security requirements are satisfied, and gets higher if the liquidity of the LP gets higher.

Further analyses of the linear regression models regarding the impact from security incidents and the partnership between Japanese LPs are also conducted. The results from our analyses supported our first two hypotheses, as well as, three new hypotheses which are used to imply more about the issues of network externalities in the field of economics of information security.

In conclusion, we recommend LP operators more security efforts particularly to satisfy strong security-related requirements in their systems. Once stronger security-related requirements in the systems are satisfied, one could expect lower impacts from the security incidents at the systems that have more security efforts, as well as, their partner LPs. Furthermore, we also suggest LPs to carefully consider the issue related to security of their future partner since impacts from security incidents can be transferred between systems through their interconnectivity.

There are two main limitations in our work. According to the lack of data regarding types of countermeasures which are implemented by each operator, we could not include items such as implementation of anti-virus softwares, etc. in our consideration when we consider security score. Therefore, only observable items are included in our checklist. Beside the limitation regarding the observable data, consideration on other factors which could enhance an evaluation of liquidity score would also lead us to other interesting implications.

Chapter 5

Multi-Level Discussion

In the past, when most of the personal computers were used as a *standalone* workstation at home or workplaces, users did not worry much about security threat and vulnerability. Actually, it might be because users were not aware or did not understand much about importance of information security. The introduction of computer network allows users to connect to each other in different places easily. Businesses take huge advantages from the use of computer network to manage their branch offices, connect to their suppliers, sell their products, and so on. By contrast, computer network also allows malicious parties to intrude the system easier and faster. By launching a computer virus from one of the terminals in the network, the virus spreads and terminal systems with no or weak protection are infected. In addition, plenty of new techniques are introduced to steal information which is considered as a valuable asset to the owners of that information from every level. Loss from such crimes is not limited to the owners of the information but also some related parties. For example, when a cyber incident due to information leakage occurs, not only the owner of the information (such as the owner of a personal information) the firms which store that piece of information also lose their trust to the customers. These are remarkable examples of modern crimes or cybercrimes.

Approaches aimed at reducing the security threat and vulnerability are different due to what practitioners have to consider. That is because the introduced approaches must show their results in different ways as mentioned by Matsuura in [98][1]. Therefore, consideration of security threat and vulnerability cannot be separated if the owner of the system wants to introduce a secure system.

In Chapter 3, the interdependency of information security is studied as one of our empirical studies to show the issue of network externalities in information security. This empirical study shows that the issue of network externalities should be considered at the national level. On the other hand, in Chapter 4, the security of Japanese loyalty network is raised as our main topic to conduct empirical studies which consider the problem of network externalities in the firm or organization level. The studies at both national level and firm/operator level show that the impact of security incidents is expanded to its partners whether it is a region, an industrial sector, or firm. The expansion of the impact occurs via inter-connectivity among nodes in the network. Therefore, vulnerability of the system would be one of the very important issues. That is because, once the system is breached, partners of the breached system could have

[1] To recall, definitions regarding vulnerability reduction and threat reduction are as follows: "vulnerability reduction is called when countermeasure of information security is introduced so that the *attack will fail.* On the other hand, "threat reduction" is called when countermeasures of information security is introduced so that the *attack will not occur*"[98].

a high possibility to be attacked. From these two chapters, we can see that security issues under the problem of network externalities can occur at any level of information systems.

In this chapter, more discussions on network externalities are given with a consideration on both levels. In our discussion, we give examples of what policy makers, operators, or IT practitioners could earn when they understand the characteristic of the information security in each level, as well as, the overall image. We raise an application or how to use the knowledge of the multi-level of network externalities to guide operators of the loyalty programs.

According to our findings in Chapter 4, one of our implications shows that liquidity is one of the important factors since higher liquidity could increase the impact from the security incidents. Such evidence becomes an incentive to attack the system. In other words, such incentive could increase the security threat to the system. Higher liquidity might lead to a larger number of attacks. That is, the threat probability of the loyalty program with high liquidity could be high. Security protection, which each operator introduces to its system, would help reducing such treats. This is similar to our findings on the benefit of requesting stronger security requirements[2] and what Matsuura stated in [98].

Beside our discussions and suggestions to the operators of the loyalty programs in Chapter 4, let us consider deeper on the four industries mentioned above by using the findings and knowledge from Chapter 3 in this chapter. In our study, the four industries are suggested to pay more attention to security issues since they have high or medium-high liquidity. The four industries mentioned in Chapter 4 are *Video picture, sound information, broadcasting and communications* (industry 17), *Information services* (industry 19), *Transportation and postal activities* (industry 20), and *Finance and insurance* (industry 23). In addition, these are industries where major security incidents occur. Example LPs which belong to these four industries are as follows:

Industry 17	Softbank Point, Docomo Point, Pointalk, au Point, Chocom Point
Industry 19	T Point, Web Money, NetMile, PeX, G-Point, Rakuten Super Point
Industry 20	ANA Mileage Club, JAL Mileage Bank, Metro Point, Suica Point
Industry 23	World Present (by Mitsui Sumitomo Bank), Citi Rewards, Nanaco

5.1 Discussion from the Level of Security Expense and Activities

First of all, let's take a look at how all the nine industries that provide LPs spend on information security and how much they focus on the implementation of security measures. Fig. 5.1 shows the trend of an average size of the expense on security countermeasures of all the 26 industries. According to the data, the average value of the average size of the expense on security countermeasures by 26 industries in 2012 is 86,284 US$ per firm and the median is 70,562 US$.

We also recall Fig. 3.7 in Chapter 3 and show Fig. 5.2 for the ease of consideration. This figure shows the level of IS measure and the IS multipliers of 26 industrial sectors [3]. According to the data, the average value of IS measure in this table is 8.7569 and the median is 7.7254.

According to Fig. 5.1 and Fig. 5.2, the level of IS measure of the nine industries that operate LPs varies from low to high. More than half of the industries that operate LPs

[2] Supportive findings to Hypothesis 1 in Chapter 4 that the stronger security requirements in registration, authentication, back-up authentication would reduce the impact from security incident.

[3] Data of the year 2012.

deploy IS measures above average, only three of them invest in security countermeasures above average. Five out of the nine industries which deploy IS measures above average are industries 19, 23, 16, 09, and 17, respectively[4]. And the three industries which invest in security countermeasures above average are industries 23, 19, and 16, respectively[5].

Next, let's focus on the four industries where major incidents occurred at their LP systems. The summary of the levels of average size of the expense on security countermeasures and IS measures of the four industries is shown in Table 5.1.

From Table 5.1, we can see that the level of expense on security countermeasure and the value of IS measure of industry 20 (Transportation and postal activities) are below average. Therefore, the LP systems from this industry could be the weakest link in the system when we consider their investment on and deployment of information security.

Table 5.1: Conclusion of the levels of average size of expense on security countermeasures and IS measures of four industries with LPs where major security incidents occurred.

Industry ID	Industry Name	Level of the Average Size of Expense	Level of IS Measure
17	Video picture, sound information, broadcasting and communications	below average	above average
19	Information services	above average	above average
20	Transportation and postal activities	below average	below average
23	Finance and insurance	above average	above average

Unsurprisingly, according to our survey on security incidents that happened to LPs in Chapter 4 , airlines, the member of industry 20, is one of the industries attractive to malicious parties; for example, [6], [70], [78], [92], and [153]. Therefore, LPs from this industry are recommended to consider more efforts on security investment and activities.

Additional consideration of the investment in information security is also suggested to the operators of LPs from industry 17. For this case, not only the level of average size of expense on security countermeasure is lower than average, but also the activities of this industry highly depend on information systems according to the result shown in Fig. 3.4 in Chapter 3[6].

Although the results of industries 19 and 23 in Table. 5.1 are above average, they still have to be careful about issues regarding information security. That is because many LPs in these two industries act as an origin LP that connects with several partners among the network [7]. Furthermore, as mentioned above, these two industries include LP operators where major incidents related to information security occurred.

[4] Ordered from high level of IS measure to low level of IS measure.

[5] Ordered from large average size of security expense to small average size of security expense.

[6] Industry 17 is the industry of *Video picture, sound information, broadcasting and communications* which is included in the sector of ICT in Fig. 3.4.

[7] Refer to Fig. 4.5 in Chapter 4 for the image of the network of the Japanese loyalty program.

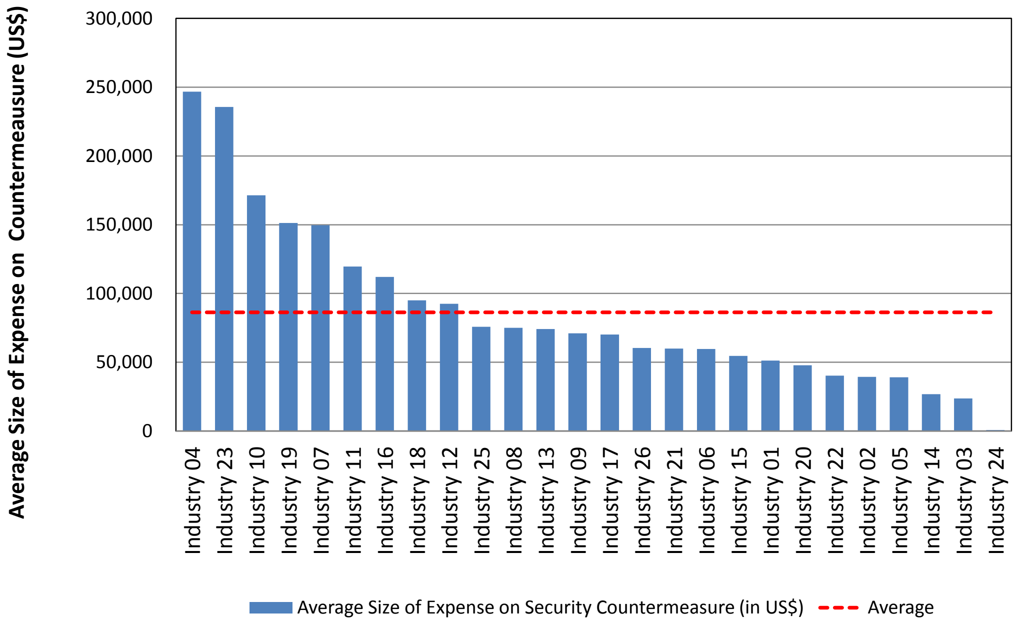


Figure 5.1: Average size of expense on security countermeasure of 26 industries in 2012 (in US$). Refer to Table 4.2 for the name of industries.

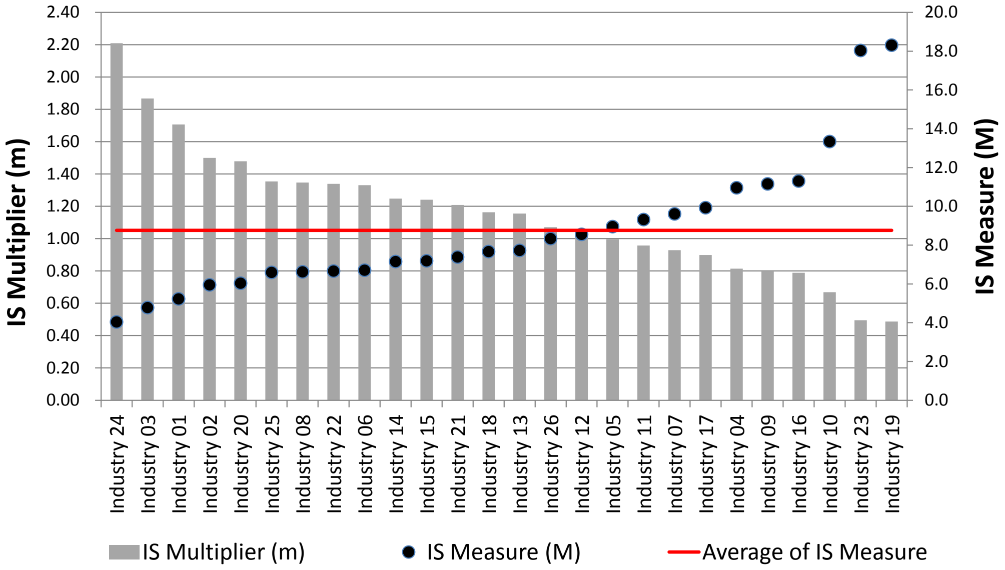


Figure 5.2: [Recall] The level of IS measure and the IS multipliers of 26 industrial sectors. Calculated from Data of the year 2012 in [104] Refer to Table 4.2 for the name of industries.

5.2 Discussion from the Characteristics of Interdependency

Next, we consider the characteristics of interdependency under information security risks in the nine industries which operate LPs. We also focus on four industries where major security incidents such as [6], [50], [107], [78], [137], [153] occurred. These are the four industries which we suggest the operators to be careful because they might have greater threat probability due to high liquidity.

In order to refer back to our findings of five-classes of sectoral interdependency in Section 3.6.1, let us introduce the industry mapping table between industries in the data of year 2006 and the data of year 2012 so that the readers will be able to follow. The detail of mapped industries between 12 industries in the data of year 2006 and 26 industries in the data of year 2012 is shown in Table 5.2.

According to the characteristics of sectoral interdependency in Section 3.6.1, the nine industries which operate LPs have characteristics of sectional interdependency as of class 1, 2, and 3:
class 1 contains industry 16
class 2 contains industry 09, 17, 19, 20, 22, and 26
class 3 contains industry 13 and 23 [8].
The main features of these classes of characteristics of sectoral interdependency are that they have high self-dependency (all of the three classes) and high interdependency when tested with critical sectors (only class 2 and 3). Furthermore, industries 13, 20, 23, and 26 are considered as critical sectors.

The above characteristics emphasize that the interdependency is one of the important factors in the network of loyalty programs in Japan. Since the security breach at systems from industry such as industry 20 (i.e. LPs provided by airline) would highly affect their partner LPs. That is not only because of the fact that LPs from this industry are highly liquid and being attractive to attackers, but also because it acts as one of the critical sectors as well. Thus a consideration on national-level of network externalities emphasizes our suggestions, especially to industry 20, to pay more attention to the investment in security countermeasures and deployment of security activities. It also shows a similar trend of the security characteristics that exist in both levels.

[8] Although the sector of Financial, insurance and real estate (IND 10) in data of the year 2006 is considered as having the characteristic of class 4 in Section 3.6.1, its sub-sector of Financial and insurance has the characteristic of class 3. Thus we classify industry 23 (data of the year 2012), which has no sub-sector of real estate, as class 3 here.

Table 5.2: Mapping table of industrial sectors between data from years 2006 and 2012.

12 Industrial Sectors for data in year 2006		26 Industrial Sectors for data in year 2012	
Sector ID	Sector Name	Sector ID	Sector Name
01 02	Agriculture Mining	14	Agriculture, forestry, fisheries, cooperative association and mining
03	Manufacturing - Food & Beverage	01	Manufacture of food, beverages, tobacco and feed
04	Manufacturing - Metal	07 08	Manufacture of iron and steel Manufacture of non-ferrous metals and fabricated metal products
05	Manufacturing - Machinery	09 10 11 12	Manufacture of electrical machinery, equipment and supplies Manufacture of information and communication electronics equipment transportation equipment Miscellaneous machinery, equipment and supplies
06	Manufacturing - Other	02 03 04 05 06 13	Manufacture of textile mill products Manufacture of pulp, paper and paper product Manufacture of chemical and allied products Manufacture of petroleum, coal and plastic products Manufacture of ceramic, stone and clay products Miscellaneous manufacturing industries
07	Construction	15	Construction
08	Utilities	16	Electricity, gas, heat supply and water
09	Commerce & Logistic	20 21 22	Transportation and postal activities Wholesale trade Retail trade
10	Financial, Insurance, and Real Estate	23	Finance and insurance
11	ICT	17 19	Video picture, sound information, broadcasting and communications Information services

Table 5.2: Mapping table of industrial sectors between data from years 2006 and 2012(Cont'd).

12 Industrial Sectors for data in year 2006		26 Industrial Sectors for data in year 2012	
Sector ID	Sector Name	Sector ID	Sector Name
12	Services	18 24 25 26	Newspaper and publishing Medical and other health services (exclude national services) Education (exclude national services) and learning support Miscellaneous non-manufacturing industries

Note: Table 3.1 is referred for the mapping.

5.3 Discussion with Consideration on Network Externalities, Threat, and Vulnerability in a General Aspect

As we mentioned at the beginning of this chapter, introduction of computer network raises the importance of the problem of network externalities to the field of information security. Since a computer network links numbers of computers together, an attacker has plenty of choices to attack at the same time. In this section, we would like to discuss network externalities, security threat, and vulnerability of the system in general.

In a general aspect, an economic problem (e.g. recession, etc.) could be one of incentives that motivate malicious parties to attack systems for economic benefits. An example is the case of breaking into LP systems where attackers steal some amounts of points from victims' accounts. Or the case of stealing personal information which is now considered as a valuable assets. Besides that, the cause of cybercrimes might come from *personal motivation*. In this case, a person might decide to attack his friends or company where he works just because the person gets angry with them[100]. *Ideologically motivation* or *moral motivated cause* is another cause to cybercrimes. Attackers might initiate some attacks due to their moral reasons. Mercer gives an example of bot attacks on the servers of financial companies (e.g. Visa, Master) as a reaction to their decision of not allowing their cardholders to donate to the WikiLeaks. In a cyber security aspect, vulnerability might be the first incentive for attackers to intrude systems (i.e. threat introduction). That is because the system with weakness requires less time, easier techniques, and less cost to complete the attempt.

Let us compare two different systems, one of which includes a firewall as one of its security protections while the other does not have a firewall. We assume that both systems have information which the attacker wants. Once the attacker found the difference, the system with no firewall then likely becomes the target. In such a case, the firewall acts as an element which helps reducing security threat to the first system with the implementation of firewall. We might also be able to imply from the implementation of a firewall at the first system that the first system would be stronger in the sense of security (i.e. lower vulnerability). This is quite similar to our findings in Chapter 4 that implementing stronger security-related requirements or adding some kinds of techniques (e.g. CAPTCHA) could help reducing the impact from security incidents. Such situation can be considered as a context of threat reduction. That is, the implementation of protection techniques helps screening the access so that malicious accesses are blocked.

Possibility of the security breach at the targeted systems also depends on other security techniques used in each system. For example, implementation of some protections with updated security patches (e.g. anti-virus software, etc.) would help reducing the chance that the attack will be successful. These implemented techniques also help reducing security vulnerability at a specific system in the network. Up-to-date and stronger protection help a system become more robust. By removing the weak point in the network, one can expect better security of the overall network. In contrast, in this situation, a good protection at one of the systems in the network could increase the security threat to another system in the same network. These are results from the existence of network externalities. Therefore, we could see that the issue regarding network externalities has both advantage and disadvantage either direct or indirect.

In addition, how to manage existing security resources is also important to reduce the possibility of the security breach. By this, an organization might provide its staffs basic education on information security. The rule or policy about information security is also important to keep the security in track. In addition, security assurance systems should also be included in a basic policy.

Since our studies focus on the Japanese information security, we use Japan as our example in this discussion. Information security is one of the topics which the Japanese government concerns. In 2006[9], the *First National Strategy on Information Security – Toward the realization of a trustworthy society* was launched[73]. Three years later, National Information Security Policy Council launched the *Second National Strategy on Information Security – Aiming for Strong "Individual" and "Society" in IT Age*[109]. According to the two governmental documents mentioned above (i.e. [73] and [109]), as well as, a recent document of *the Basic Policy of Critical Information Infrastructure Protection (3rd Edition)* which was launched in 2014[74], we could see that information security in sectoral perspective is considered in their discussion; i.e. consideration on critical information infrastructures[109]. Network externalities of information security also shows its importance to the overall network. We could see that the topic of *interdependency* is also mentioned in [74]. Consideration on adding one of the industries as critical information infrastructure in [74] due to the *interdependency with the current critical information infrastructures* could be one of the supportive examples. However, information security in regional perspective is slightly lacking in their consideration. In national level, more attention is paid to the governmental elements; i.e. security sharing between local government offices[109]. To employ suitable security at the system, policies or framework regarding information security management at national level would guide firms and organizations from a large viewpoint. Combinations of characteristics of interdependency of information from sectoral and regional perspectives would enrich detail in the guideline. That is because interdependency of information security on some industries shows high self-dependency. In fact, more than half of 12 industrial sectors in Chapter 3 have this property. Hence, consideration from the sectoral perspective only might not be enough. This combination would show a big image of information security. Furthermore, it would also be very important to the high-level network.

General instructions and encouragement are also important to normalize the information

[9] The mentioned year refers to what is said on the first page of the translated version of the document.

security activities among firms. That is because the use of IT systems and information management at each firm are different according to the firms' policy [74]. In addition, information security breaches can also occur in any systems from any industries in the network. For example, in our study on loyalty programs, we consider security of the firms which operate LPs. Therefore, information security of only the nine industries is mainly considered when LPs are focused.

Although information management is different due to firms' policy, the general guideline would be useful to operators to manage, implement, and invest in proper security techniques or policy. For example, in the case of the Japanese LPs, security-related requirements at each system have no common rule. That is, each system introduces its own pattern to ask their customers at registration, authentication, and back-up authentication processes. By this, their requirements might relate to what they want to know, as well as, what they think it would make their systems secure. However, what they require might not be enough in terms of information security. Allowing customers to use free mails or information which cannot be certified to become a member could lead to further serious crimes both in physical and cyber environments. In such cases, the general guideline which provides a list of basic requirements would help operators of the LPs implement more proper systems. With the standard, LP operators might concern more on topics which they have never concerned before.

Let us use LP systems as our example to show an importance of consideration of multi-level findings and how a group of businesses should consider in general. According to our studies in Chapter 4, we found that the security level of the origin LP shows indirect influence on the destination LP through the size of the impacts from security incidents. This finding emphasizes the influence of interconnectivity between systems in the network. Better security management at the origin LP would also increase the security of the destination LP. With better security management at the origin LP, the vulnerability of the overall network is then expected to be reduced.

However, due to our survey, most Japanese LP can act as both origin LP and destination LP. That is, to reduce the impact from the security incident, one consideration which the operators should also keep in their mind is to introduce secure transaction mechanisms. This is what operators should consider besides implementing strong security requirements for registration, authentication, and back-up authentication processes.

With the above consideration, vulnerability at each process should be reduced. The stronger protection will then becoming a sign for attackers that they might have to spend more efforts to break into the system. On the other hand, in the case that the system is breached, proper requirements for all processes would help increasing traceability of attackers. Thus, the digital forensic after the incidents would become more efficient. Such advice could be included in the security management policy especially for LP operators, in general.

If we consider other types of businesses, information security of the considered group of industries would be changed according to a specific type of business. However, general consideration of information security at national level still be necessary since all types of businesses share some characteristics in common. For example, recall our five classes of sectoral characteristics of interdependency of information security in Chapter 3. In this case, different industries share some common characteristics according to the class that each industry belongs to. Lack of consideration on interconnectivity among nodes in multi-level perspectives could make IT practitioners improperly invest in information security. Problems such as over- or under- investment might occur. Thus, vulnerability, threat, and security risk of a specific system might not efficiently reduce by the improperly invested amount.

5.4 Network Externalities and Results from Multi-level Analyses

Under the consideration of network externalities, we can see a similar pattern of relationship between impact from security incident and the concept of liquidity in both levels. In the case of national level, the expansion of the impact from security incidents likely concentrates on the groups of sectors which have high self-dependency and high interdependency when tested with critical sectors according to the results (i.e. sectors in classes 1, 2, and 3 of sectoral characteristics). Furthermore, sectors in the class where the feature of high self-dependency exists might suffer more from security incidents. The main supportive reason comes from our result which shows a positive relationship between the level of IT dependency[10] and the characteristic of security interdependency. For example, ICT, Machinery, and Services are sectors with a high level of IT dependency[11]. Their characteristic of interdependency of information security falls into class 2 which has high self-dependency and high interdependency when tested with all critical sectors. Industries which have high interdependency with more features would gain higher loss or impact from the security incidents because security at their systems relies on security of others more than those with fewer features.

For the case of sectors in class 2 and 3 where high self-dependency is also feature of their characteristic, besides impact from security incident at the critical sectors, sectors in these two classes would also receive impact from firms in the same industry. In the latter type of impact, although the impact would likely be limited inside the sector, we could expect the expansion through regional connections. Therefore, sectors in these classes where feature of high self-dependency exists could suffer more.

From the above discussion and results, higher interdependency would mean higher interconnectivity between systems. It can also imply higher usage among connected edges. Finally, these available interconnections could refer to higher liquidity of the system. Then more available channels or services are expected to nodes with high interdependency. Therefore, it corresponds to the concept of liquidity in cyberspace. Such scenario let us be able to consider in the same way as in the scenario of Hypothesis 2 in the firm/organization level. That is, the impact from security incidents relates to the liquidity of the LP; the higher liquidity, the higher expected impact from the security incident.

5.5 Conclusion

According to our discussion, we could see that the knowledge of multi-level network externalities helps us understand more about information security. Such understanding could be used for setting the future direction of information security by policy makers and practitioners to raise the level of security of their systems, as well as, the security of the overall network. By properly investing an adequate amount on security countermeasures, and properly implementing security-related activities, vulnerability and threat are expected to be reduced.

[10] Level of IT dependency lets us know how each sector rely on IT systems. The higher value also implies that the sector uses/spends more on IT systems.

[11] Refer to Fig 3.4 for the trend.

Chapter 6

Conclusion

In this thesis, empirical analyses on the topic regarding network externalities of information security are conducted. We consider multi-level of network externalities since this problem could occur at any level in the information network. Findings and implications in the studies also show importance of study on economics of information security. Understanding characteristics of information security in both levels would provide policy makers, operators, IT practitioners more ideas on how to properly manage and invest in information security.

In the following, we summarize the contributions of this thesis. Furthermore, we also provide future directions regarding our studies at the end of this chapter.

6.1 Summary of Contributions

6.1.1 National-level Network Externalities

In the study regarding national-level of network externalities, there are two main contributions. Firstly, we conducted the empirical study to find sectoral and regional interdependencies under the influence of information security risks. In order to analyze the interdependency in both perspectives, we extended the basic economic methodology introduced by Dietzenbacher and Van der Linder in [34] and the information security-related methodology introduced by Tanaka in [150]. After that, the result collection process was introduced to classify the characteristics of interdependency for Japanese industries and regions. We also found some empirical findings which are useful for the understanding in the national-level.

The second contribution is related to the change of interdependency according to the impact from the Great East Japan Earthquake in 2011. Beside the basic model, we introduced the methodology to find the impact from the Great East Japan Earthquake. Additional consideration on the damage from the quake was added to find the impact from the disaster. Then, we compared the interdependency before and after the disaster. The findings showed that the impact from such disaster would be limited in some industries, as well as, regions.

6.1.2 Firm/Operator-level Network Externalities

In the study in firm/operator-level, we focused on the network of the Japanese loyalty program. Due to our knowledge, researches on the loyalty programs are mostly conducted in the field of marketing and economics. However, the security of the loyalty programs is not well-studied.

Firstly, we introduced the concept and definition of liquidity of loyalty programs. According to our concept of liquidity, we investigated the network of Japanese loyalty programs.

After that, the linear regression analyses were conducted to find security-liquidity implications. The actual security level was introduced to indicate the security in each LP system.

Finally, several implications and suggestions were introduced to the operators of loyalty programs.

6.1.3 Discussion on the Multi-level Network Externalities

To show the usefulness of findings from our studies in both levels, we gave an example of how to use those knowledges to suggest firms or policy makers on the issues of information security. Besides that, we also discussed network externalities, security threat, and vulnerability of systems in general. Discussion in this part will help readers understand more about the reason why multi-level externalities are important in the field of economics of information security.

The case of the Japanese loyalty program is used as our example. In the discussion, we referred to the level of security activities (the value of IS measure), characteristics of sectoral interdependency, the average size of expenditure on security countermeasure, and the level of liquidity.

Our results showed that knowledge of network externalities from the national-level can be used to emphasize our suggestions at the firm level, and vice versa.

6.2 Future Work

There are still challenges which are interesting related to our work. Especially, we can find important challenges related to the network externalities of loyalty programs. That is because points from a loyalty program is considered as one of virtual currencies. With high competition in marketing, shops and service providers introduce their own loyalty programs to motivate more customers. By this, many operators also allow their customers to manage or use their possessed points online. Thus, the network of the loyalty programs is expected to become larger and larger. This expansion then becomes an incentive to cybercrimes. Another reason is that LP systems are used by general customers who might not be familiar with how to deal with password security well. Although there's a sign from the side of Canada that more customers concern more about their privacy[18], many of them are more interested in joining the LP for financial benefits. Therefore, LP systems might be another targeted system in cybercrimes.

However, the analysis of network externalities and security issues of LP systems from the view of economics of information security are quite new and limited. Even in a recent article about security incidents on loyalty programs gives its title as *Loyalty Rewards Programs: A New Cybercrime?* [32].

In Chapter 4, we introduced the definition of the liquidity of LP by considering elements in the network of loyalty programs. That is, we considered the type of edges between nodes (i.e. a specific LP and industries), and the number of partners linked to a specific LP (or industry). However, there are still other factors related to the liquidity: for example, duration that the customer has to spend to exchange their points from a particular system to another, or loss of value according to the exchange rate between LPs, etc.

Other concerns on security of LPs such as the probability of money laundering and an impact from the data breach where an LP is one of the main players are also interesting. In fact, for the case of money laundering, there are several evidences that the stolen points from loyalty programs are sold in the dark online market. Clear examples can be seen from the recent case of the security breach at Hilton HHonors. According to [117], 833,000 stolen points was sold for $20 worth of Bitcoins, in this case. This is just one of several evidences that the loyalty points can be used for money laundering. Another concern which we mentioned above is the impact from the data breach where LP becomes one of the players. In this case, data breach at the LP could lead to several security concerns, especially issues on risk management and privacy from the trading of breached information.

These are only a few examples of our future directions.

Bibliography

[1] Abel, J., Hackers steal Hilton Hotels' loyalty program reward points – Check your Hilton HHonors account and any credit cards attached to it, Nov. 3, 2014. Last accessed on Jan. 28, 2015. http://www.consumeraffairs.com/news/hackers-steal-hilton-hotels-loyalty-program-reward-points-110314.html

[2] Acquisti, A., The Economics of Privacy (Talk), Carnegie Mellon University, Software Engineering Institute, Feb. 2004. Last accessed on Jan. 28, 2015. http://www.heinz.cmu.edu/ acquisti/papers/acquisti_privacy_economics.ppt

[3] Acquisti, A., The Economics of Privacy, Last accessed on Jan. 28, 2015. http://www.heinz.cmu.edu/ acquisti/economics-privacy.htm

[4] Adrian, T., and Shin, H.S., Liquidity, Monetary Policy, and Financial Cycles, In *Current Issues in Economics and Finance*, Vol. 14, No. 1, 2008, pp.1–7.

[5] Ahn, L., Blum, M., Hopper, N., and Langford, J., CAPTCHA: Using Hard AI Problems for Security, In *Advances in Cryptology — EUROCRYPT 2003*, LNCS 2656, Springer, 2003, pp.294–311.

[6] All Nippon Airways, ANA マイレージクラブ特典「iTunes ギフトコードへの交換サービス」一時停止と会員パスワード変更のお願い, 2014. Last accessed on Jan. 28, 2015. http://www.ana.co.jp/topics/notice140311/

[7] Anderson, R., Why Cryptosystems Fail. In *Communications of the ACM*, Vol. 37, No. 11, 1994, pp.32–40.

[8] Anderson, R., Open and Closed Systems are Equivalent (that is, in an ideal world), In *Perspectives on Free and Open Source Software, MIT Press, Cambridge*, 2005, pp.127–142.

[9] Anderson, R. and Moore, T., The Economics of Information Security, In *Science*, Vol. 314, No. 5799, 2006, pp.610–613.

[10] Anderson, R. and Moore, T., Information Security: Where Computer Science, Economics and Psychology Meet In *Philosophical Transactions of the Royal Society A*, Vol. 367, 2009, pp.2717–2727.

[11] Anderson, R., Moore, T., Nagaraja, S., and Ozment, A., Incentives and information security, In *Algorithmic Game Theory*, 2007, pp.633–650.

[12] Aoyama, Y., and Ratick, S.J., Trust, Transactions, and Information Technologies in the U.S. Logistics Industry. In *Economic Geography*, Vol. 83, Issue 2, 2007, pp.159–180.

[13] Baker, T. Panelists: Management risk to protect growth, In *The 2014 Master Innholders Conference*, Jan. 2014. Last accessed on Jan. 28, 2015. https://www.hotelnewsnow.com/Article/12996/Panelists-Manage-risk-to-protect-growth

[14] Bandyopadhyay, T. Jacob V., and Raghunathan, S., Information security in networked supply chains: impact of network vulnerability and supply chain integration on incentives to invest. In *Information Technology and Management*, Vol. 11, No. 1, 2010, pp.7–23.

[15] Bardzell, J., Jakobsson, M., Bardzell, S., Pace, T., Odom, W., and Houssan, A., Virtual Worlds and Fraud: Approaching Cybersecurity in Massively Multiplayer Online Games, In *Proceedings of Digital Games Research Association (DiGRA)'s Third International Conference*, 2007, pp.742–751.

[16] Baryshnikov, Y., IT Security Investment and Gordon-Loeb's $1/e$ Rule, In 11th Annual Workshop on the Economics of Information Security (WEIS) 2012, Jun. 2012. Last accessed on Jan. 28, 2015. http://weis2012.econinfosec.org/papers/Baryshnikov_WEIS2012.pdf

[17] Berry, J., Bulking Up: The 2013 COLLOQUY Loyalty Census. Growth and Trends in U.S. Loyalty Program Activity, In *COLLOQUY talk*, Jun. 2013, pp.1–13.

[18] Berry, J., Bulking Up: The 2013 COLLOQUY Loyalty Census. Growth and Trends in Canadian Loyalty Program Activity, In *COLLOQUY talk*, Jun. 2013, pp.1–8.

[19] Bijmolt, T.H.A., Dorotic, M., and Verhoef, P.C. Loyalty Programs: Generalizations on Their Adoption, Effectiveness and Design, In *Foundations and Trends in Marketing*, Vol. 5, No. 4, 2010, pp.197–258.

[20] Billock, J., Hilton HHonors Hit by Hackers, Points Stolen & Credit Cards Charged, Nov. 5, 2014. Last accessed on Jan. 28, 2015. http://www.flyertalk.com/story/hilton-hhonors-hit-by-hackers-points-stolen-credit-cards-charged.html

[21] Boot, A.W.A., and Marinc M. The evolving landscape of banking. In *Industrial and Corporate Change*, Vol. 17, Issue 6, 2008, pp.1173–1203.

[22] Bronk, C., Monk, C., and Villasenor, J., The Dark Side of Cyber Finance, In *Survival: Global Politics and Strategy*, Vol. 54, No. 2, 2012, pp.129–142.

[23] Cabineet office, Government of Japan, Gross Capital Stock by Industry, 2009. Last accessed on Nov. 2010. http://www.esri.cao.go.jp/jp/sna/sonota/minkan/kekka/20110107/h21y_stock_all.xls

[24] Cabinet office, Government of Japan, Special cabinet meeting material on monthly economic report due to the earthquake, 2011. Last accessed on Jan. 28, 2015. http://www5.cao.go.jp/keizai/bousai/pdf/keizaitekieikyou.pdf

[25] Carr, N.G., IT Doesn't Matter In *Harvard Business Review*, 2003, pp.41–49.

[26] CBC News, Major new credit card scam uncovered in B.C. – 'Web of criminal activity' involves hundreds of credit cards and thousands of dollars in reward points, Mar. 19, 2014. Last accessed on Jan. 28, 2015. http://www.cbc.ca/news/canada/british-columbia/major-new-credit-card-scam-uncovered-in-b-c-1.2579214

[27] Chen, Y.C., Chen, P., Song, R., and Korba, L., Online gaming crime and security issue: Cases and countermeasures from Taiwan, In *The Second Annual Conference on Privacy, Security and Trust*, Oct. 2004.

[28] Christin, N., Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace, In *Proceddings of the 22nd International Conference on World Wide Web (WWW'13)*, 2013, pp.213–224.

[29] Clark, T.H., Croson, D.C., and Schiano, W.T., A Hierarchical Model of Supply-Chain Integration: Information Sharing and Operational Interdependence in the US Grocery Channel In *Information Technolgy and Management*, Vol. 2, 2001, pp.261–288.

[30] Cranor, L.F., 'I didn't buy it for myself' privacy and ecommerce personalization. In *WPES '03 Proceedings of the 2003 ACM Workshop on Privacy in the Electronic Society*, 2003, pp.111-117.

[31] Crypto-currency market capitalizations, Last accessed on Jan. 28, 2015. http://coinmarketcap.com/currencies/views/all/

[32] CSID (website), Loyalty Rewards Programs: A New Cybercrime?, Nov. 2014. Last accessed on Jan. 28, 2015. http://www.csid.com/2014/11/loyalty-rewards-programs-new-cybercrime/

[33] Dedrick, J. and Kraemer, K.L., The impacts of IT on Firm and Industry Structure: The Personal Computer Industry, In *California Management Review*, Vol. 47, Issue 3, 2005, pp.122–142

[34] Dietzenbacher, E., and Van der Linder, J.A., Sectoral and Spatial linkages in the EC production structure. In *Journal of Regional Science*, Vol. 37, No. 2, 1997, pp.235–257.

[35] Dimsdrive, Survey on Point Card (in Japanese), Timely research, 2006. Last accessed on Jan. 28, 2015. http://www.dims.ne.jp/timelyresearch/2006/060516/index.html

[36] Dimsdrive, The 22th Survey Result on Electronics Retail Store's Point Card (in Japanese), Ranking research, 2007. Last accessed on Jan. 28, 2015. http://www.dims.ne.jp/rankingresearch/101_150/122/004.html

[37] Dimsdrive, Survey on Department Store (in Japanese), Timely research, 2007. Last accessed on Jan. 28, 2015. http://www.dims.ne.jp/timelyresearch/2007/071002

[38] Dimsdrive, Survey on the Use of Convenience Store (in Japanese), Timely research, 2010. Last accessed on Jan. 28, 2015. http://www.dims.ne.jp/timelyresearch/2010/100204

[39] Dion, D.A., I'll Gladly Trade You Two Bits on Tuesday for a Byte Today: Bitcoin, Regulating Fraud in the E-Conomy of Hacker-cash, In *Journal of Law, Technology, and Policy*, Vol. 165, 2013, pp.165–202.

[40] Dorotic, M., Bijmolt, T.H.A. and Verhoef, P.C., Loyalty Programmes: Current Knowledge and Research Directions, In *International Journal of Management Reviews*, Vol. 14, 2012, pp.217–237.

[41] Dowling, G.R., and Uncles, M., Do Customer Loyalty Programs Really Work?, In *MITSlone Management Review*, 1997. Last accessed on Jan. 28, 2015. http://sloanreview.mit.edu/article/do-customer-loyalty-programs-really-work/

[42] Eeten, M.J.G., and Bauer, J.M., Economics of Malware: Security Decisions, Incentives and Externalities, OECD Science, Technology and Industry Working Papers 2008/1, OECD Directorate for Science, Technology and Industry, May 2008.

[43] ENISA, and RAND Europe, Incentives and Challenges for Information Sharing in the Context of Network and Information Security, 2010. Last accessed on Jan. 28, 2015. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/incentives-and-barriers-to-information-sharing

[44] Enzmann, M., and Schneider, M., Improving Customer Retention in E-Commerce Through a Secure and Privacy-Enhanced Loyalty System In *Information Systems Frontiers*, Vol. 7, Issue 4–5, Dec. 2005, pp.359–370.

[45] eTN Global Travel Industry News (website), Hilton boosts reward program security after hacker attack, Nov. 13, 2014. Last accessed on Jan. 28, 2015. http://www.eturbonews.com/52529/hilton-boosts-reward-program-security-after-hacker-attack

Last accessed on Jan. 28, 2015.

[46] Fearon, C, and Philip, G., An empirical study of the use of EDI in supermarket chains using a new conceptual framework, In *Journal of Information Technology*, Vol. 14, Issue 1, 1999, pp.3–21.

[47] Fearon, C, and Philip, G., Measuring success of electronic trading in the insurance industry: operationalising the disconfirmation of expectations paradigm. In *Behaviour & Information Technology*, Vol. 27, Issue 6, 2008, pp.483–493.

[48] Finley, K., Bitcoin Exchange Mt. Gox Files for U.S. Bankruptcy as Death Spiral Continues, Mar. 10, 2014. Last accessed on Jan. 28, 2015. http://www.wired.com/2014/03/gox-texas/

[49] Frequent Flyer Services, Web Flyer (website), Last accessed on Jan. 28, 2015. http://webflyer.com/

[50] G-Point, Report on unauthorized access to G-Point (in Japanese), Apr. 24, 2012. Last accessed on Jan. 28, 2015. http://info.gpoint.co.jp/blog/2012/04/g424-1915-93b6.html

[51] Gable, M., Fiorito, S.S., and Topol, M.T., An empirical analysis of the components of retailer customer loyalty programs, In *International Journal of Retail & Distribution Management*, Vol. 36 Issue 1, 2008, pp.32–49.

[52] Gal-Or, E., and Ghose, A., The Economic Incentives for Sharing Security Information, In *Information Systems Research*, Vol. 16, No. 2, 2005, pp.186–208.

[53] Gil-Sauraa, I., and Ruiz-Molinaa, M.E., Logistics service quality and buyercustomer relationships: the moderating role of technology in B2B and B2C contexts, In *The Service Industries Journal*, Vol. 31, Issue 7, 2011, pp.1109–1123.

[54] Gordon, L.A., and Loeb, M.P. The Economics of Information Security Investment, In *ACM Transactions on Information and System Security*, Vol. 5, No. 4, Nov. 2002, pages 438–457.

[55] Gordon, L.A., Loeb, M.P., and Lucyshyn, W., Sharing Information on Computer Systems Security: An Economic Analysis, In *Journal of Accounting and Public Policy*, Vol. 22, 2003, pp.461–485.

[56] Gordon, L.A., Loeb, M.P., Lucyshyn, W., and Sohail, T., The Impact of the e Sarbanes-Oxley Act on the Corporate Disclosures of Information Security Activities, In *Journal of Accounting and Public Policy*, Vol. 25, 2006, pp.503–530.

[57] Gordon, L.A., Loeb, M.P., Lucyshyn, W., and Richardson, R., 2005 CSI/FBI Computer Crime and Security Survey, 2005. Last accessed on Jan. 28, 2015. http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf

[58] Gordon, L.A., Loeb, M.P., and Sohail, T., A Framework for Using Insurance for Cyber-risk Management, In *Communication of the ACM*, Vol. 46, No. 3, 2003.

[59] Garcia , M., Loyalty Programs & Fraud: What You Need to Know, Nov. 2014. Last accessed on Jan. 28, 2015. http://www.cntraveler.com/stories/2014-11-07/loyalty-programs-and-fraud-what-you-need-to-know

[60] Guerra, P., How Economics and Information Security Affects Cyber Crime and What It Means in the Context of a Global Recession. In *BlackHat USA 2009, Turbo Talk Whitepaper*, 2009. Last accessed on Jan. 28, 2015. http://www.blackhat.com/presentations/bh-usa-09/GUERRA/BHUSA09-Guerra-EconomicsCyberCrime-PAPER.pdf

[61] Haimes, Y.V., and Jiang, P., Leontief-Based Model of Risk in Complex Interconnected Infrastructures, In *International Journal of Networking and Virtual Organizations*, Vol. 4, Issue 3, 2001, pp.130–144.

[62] Haimes, Y.V., Horowitz, B.M., Lambert, J.H., Santos, J., Crowther, K., and Lian, C., Inoperability Input-Output Model for Interdependent Infrastructure Sectors. II: Case Studies. In *Journal of Infrastructure Systems*, Vol. 11, No. 2, 2005, pp.80–92.

[63] Haimes, Y.V., Barry M. Horowitz, Lambert, J.H., Santos, J., Lian, C., and Crowther, K., Inoperability Input-Output Model for Interdependent Infrastructure Sectors. I: Theory and Methodology. In *Journal of Infrastructure Systems*, Vol. 11, No. 2, 2005, pp.67–79.

[64] Han, K., Kauffman, R.J., and Nault, B.R., Information Exploitation and Interorganizational Systems Ownership, In *Journal of Management Information Systems*, Vol. 21, No. 2, 2004, pp.109–135.

[65] Harrisson, C., and Hamilton, J., Bitcoin Exchange Tradehill Pauses for Regulatory Reasons, In *Bloomberg Technology*, 2013. Last accessed on Jan. 28, 2015. http://www.bloomberg.com/news/2013-08-30/bitcoin-exchange-tradehill-pauses-trading-for-regulatory-reasons.html

[66] Hausken, K., Income, Interdependence, and Substitution Effects Affecting Incentive for Security Investment, In *Journal of Accounting and Public Policy*, Vol. 25, 2006, pp.629–665.

[67] Hausken, K., Information Sharing Among Firms and Cyber Attacks, In *Journal of Accounting and Public Policy*, Vol. 26, 2007, pp.639–688.

[68] Hicks, J.R., Liquidity, In *The Economic Journal*, Vol. 72, No. 288, 1962, pp.787–802.

[69] Hill, K., Mt. Gox CEO Says All The Bitcoin Is Gone In Bankruptcy Filing, Feb. 28, 2014. Last accessed on Jan. 28, 2015. http://www.forbes.com/sites/kashmirhill/2014/02/28/mt-gox-ceo-says-all-the-bitcoin-is-gone-in-bankruptcy-filing/

[70] Hoffman, J.M., My US Airways Account was Majorly Compromised, In *US Airways*, Aug. 2013. Last accessed on Jan. 28, 2015. http://heelsfirsttravel.boardingarea.com/2013/08/16/my-us-airways-account-was-majorly-compromised/

[71] Huang, C.D., Hu, Q., and Behara, R.S., An Economic analysis of the optimal information security investment in the case of a risk-averse firm, In *International Journal of Production Economics*, Vol. 114, Issue 2. Aug. 2008, pp. 793–804.

[72] Information-technology Promotion Agency, JAPAN (IPA), 2014年版　情報セキュリティ: 10大脅威 〜複雑化する情報セキュリティ あなたが直面しているのは？〜, 2014. Last accessed on Jan. 28, 2015. https://www.ipa.go.jp/files/000037151.pdf

[73] Information Security Policy Council, The First National Strategy on Information Security – "Toward the realization of a trustworthy society" (Translated version), Feb. 2, 2006. Last accessed on Jan. 3, 2015. http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf

[74] Information Security Policy Council, The Basic Policy of Critical Information Infrastructure Protection (3rd Edition) (Translated version), May 9, 2014. Last accessed on Jan. 3, 2015. http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf

[75] Internet Live Stats, Internet User, 2014. Last accessed on Feb. 8, 2015. http://www.internetlivestats.com/internet-users/

[76] Investopedia, Dictionary. Last accessed on Feb. 8, 2015. http://www.investopedia.com/

[77] Irwin, A.S.M., and Slay, J., Detecting Money Laundering and Terrorism Financing Activity in Second Life and World of Warcraft, In *the Proceedings of the 1st International Cyber Resilience Conference*, Aug. 2010.

[78] Japan Airlines, Temporary Suspension of the Amazon Gift Certificate Award and Request to Change JMB PINs, Feb. 3, 2014. Last accessed on Jan. 28, 2015. http://www.jal.co.jp/en/info/jmb/140203.html

[79] Johnson, C., Badger, L., and Waltermire, D., Guide to Cyber Threat Information Sharing : NIST Special Publication 800-150 (Draft), 2014. Last accessed on Jan. 28, 2015. http://csrc.nist.gov/publications/drafts/800-150/sp800_150_draft.pdf

[80] Jones, R., Tesco Clubcard fraud tale could be tip of iceberg, Nov. 30, 2013. Last accessed on Jan. 28, 2015. http://www.theguardian.com/money/2013/nov/30/tesco-clubcard-fraud-stolen-vouchers

[81] Keene, S.D., Emerging threats: Financial Crime in the Virtual World, In *Journal of Money Laundering Control*, Vol. 15, No. 1, 2012, pp.25–37.

[82] King, J.L., and Lyytinen, K., Automotive Informatics: Information Technology and Enterprise Transformation in the Automobile Industry, In *Transforming enterprise : the economic and social implications of information technology*, Cambridge, Mass. MIT Press, 2005, pp.283–312.

[83] Kiondo, C., Kowalsk, S., and Yngström, L., Exploring Security Risks in Virtual Economies, In *The First International Conference on Social Eco-Infomatics (SOTICS 2011)*, 2011.

[84] Klein, R., and Rai, A., Interfirm Strategic Information Flows in Logistics Supply Chain Relationships, In *Management Information Systems Quarterly*, Vol. 33, Issue 4, 2009, pp.735–762.

[85] Ku, Y., Chen, Y.C., Wu, K.C., and Chiu, C., An Empirical Analysis of Online Gaming Crime Characteristics from 2002 to 2004, In *PAISI, Lecture Notes in Computer Science, Springer*, Vol. 4430, 2007, pp.34–45.

[86] Kunreuther, H. and Heal, G., Interdependent Security. In *Journal of Risk and Uncertainty*, Vol. 26, Issue 2–3, 2003, pp.231–249.

[87] Last, J.V., Bitcoin Is Dead, Mar. 5, 2014. Last accessed on Jan. 28, 2015. http://www.weeklystandard.com/blogs/bitcoin-dead_784187.html

[88] Lee, T.B., Mt.Gox is Bankrupt. But Bitcoin is going to be OK., In *The Washington Post*, Feb. 28, 2014. Last accessed on Jan. 28, 2015. http://www.washingtonpost.com/blogs/the-switch/wp/2014/02/28/mt-gox-is-bankrupt-but-bitcoin-is-going-to-be-ok/

[89] Leenheer, J., and Bijmolt, T.H.A., Which retailers adopt a loyalty program? An Empirical Study, In *Journal of Retailing and Consumer Services*, Vol. 15, 2008, pp.429–442.

[90] Leenheera, J., Heerde, H.J., Bijmolt, T.H.A., and Smidts, A., Do loyalty programs really enhance behavioral loyalty? An empirical analysis accounting for self-selecting members, In *International Journal of Reserach in Marketing*, Vol. 24, Issue 1, 2007, pp.31–47.

[91] Lelarge, M., Economics of Malware: Epidemic Risks Model, Network Externalities and Incentives, In *Proceedings of the 47th Annual Allerton Conference on Communication, Control, and Computing*, 2009, pp.1353–1360.

[92] Levitte, J., Airlines face new and unexpected security threat – loyalty fraud, Nov. 29, 2012. Last accessed on Jan. 28, 2015. http://www.tnooz.com/article/airlines-face-new-and-unexpected-security-threat-loyalty-fraud/

[93] Liu, D., Ji, Y., and Mookerjee, V., Knowledge Sharinf and Investment Decisions in Information Security, In *Desision Support Systems*, Vol. 52, 2011, pp.95–107.

[94] Liu, W., Tanaka, H., and Matsuura, K., Empirical-Analysis Methodology for Information-Security Investment and Its Application to Reliable Survey of Japanese Firms, In *IPSJ Digital Courier*, Vol. 3, Sept. 2007, pp.585–599.

[95] Loyalty Card (website), Loyalty Program Overview, Last accessed on Jan. 28, 2015. http://www.loyaltycard.in/content/view/33/45/

[96] Mancini, L., Ranaldo, A., and Wrampelmeyer, J., Liquidity in the Foreign Exchange Market: Measurement, Commonality, and Risk Premiums, In *The Journal of Finance*, Vol. 68, No. 5, 2013, pp.1805–1841.

[97] Marinč, M., Banks and information technology: marketability vs. relationships, In *Electronic Commerce Research*, Vol. 13, Issue 1, 2013, pp.71–101.

[98] Matsuura, K. Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model In *M.E. Johnson (ed.), Managing Information Risk and the Economics of Security*, Springer Science + Business Media, 2009, pp.99–119.

[99] McMillan, R., The Inside Story of Mt. Gox, Bitcoin ' s $460 Million Disaster, Mar. 3, 2014. Last accessed on Jan. 28, 2015. http://www.wired.com/2014/03/bitcoin-exchange/

[100] Mercer, E., Causes of Cyber Crime, Last accessed on Jan. 6, 2015. http://science.opposingviews.com/causes-cyber-crime-1846.html

[101] Miller, C., The legitimate vulnerability market: the secretive world of 0-day exploit sales In *The Sixth Workshop on the Economics of Information Security*, 2007.

[102] Ministry of Economic, Trade and Industry, Inter-Regional Input-Output Tables 2005 (in Japanese), 2005. Last accessed on Jan. 28, 2015. http://www.meti.go.jp/statistics/tyo/tiikiio/result/result_02.html

[103] Ministry of Economy, Trade and Industry, Survey on information processing: Entry outline of the survey (in Japanese), 2012. Last accessed on Jan. 28, 2015. http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/pdf/04_H24kinyuyoryo.pdf

[104] Ministry of Economy, Trade and Industry, The 2012 Survey on information processing: result detail part 3 – information security (in Japanese), 2012. Last accessed on Jan. 28, 2015. http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/h24jyojitsu.html

[105] Ministry of Economic, Trade and Industry, The 2006 Survey of Information Technology (in Japanese), 2007. Last accessed on Jan. 28, 2015. http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/h18jyojitsu.html

[106] Moore, T., and Christin, N., Beware the middleman: empirical analysis of Bitcoin-exchange risk, In *Ahmad-Reza Sadeghi, editor, Financial Cryptography*, Lecture Notes in Computer Science, Springer, Vol. 7859, 2013, pp.25–33.

[107] MSN Sankei News, Two Chinese students were arrested on Rakuten point exchange fraud suspect (in Japanese), Dec. 8, 2013. Last accessed on Dec. 2013. http://sankei.jp.msn.com/affairs/news/131208/crm13120816170005-n1.htm

[108] Nakamura, S., Bitcoin; A Peer-to-Peer Electronic Cash System, 2009. Last accessed on Jan. 28, 2015. https://bitcoin.org/bitcoin.pdf

[109] National Information Security Policy Council, The Second National Strategy on Information Security – Aiming for Strong “Individual” and “Society” in IT Age (Translated version), Feb. 3, 2009. Last accessed on Jan. 3, 2015. http://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf

[110] National Institute of Standards and Technology (NIST), Glossary of Key Information Security Terms (NISTIR 7298, Rev.2), May 2013. Last accessed on Jan. 28, 2015. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

[111] Nikolaou, K., Liquidity (Risk) Concepts: Definitions and Interactions, In *European Central Bank, Working Paper Series No.1008*, 2009. Last accessed on Jan. 28, 2015. http://ssrn.com/abstract=1333568

[112] Nomura Research Institute (NRI), ポイント・マイレージの年間最少発行額は2013年度は1兆円超へ – 国内11業界の2017年度までの年間最少発行額を予測 (New Release), May 10, 2013. Last accessed on Jan. 28, 2015. http://www.nri.com/jp/news/2013/130510_2.html

[113] Nunes, J.C., and Dreze, X., Your Loyalty Program is Betraying You, In *Harvard Business Review*, Vol. 84, Apr. 2006, pp.124–131.

[114] Odlyzko, A., Privacy, Economics, and Price Discrimination onf the Internet, In *ICEC'03 Proceedings of the 5th International Conference on Electronic Commerce*, 2003, pp.355–366.

[115] Office of the manager, National communications system, Supervisory control and data acquisition (SCADA) systems, In *Technical information bulletim 04-1, National communications system*, 2004. Last accessed on Mar. 2010. http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf

[116] Ogut, H. Menon, N., and Raghunathan, S., Cyber Insurance and IT Security Investment: Impact of Interdependent Risk. In *Workshop on the Economics of Information Security (WEIS05)*, 2005. Last accessed on Jan. 28, 2015. http://infosecon.net/workshop/schedule.php, 2005.

[117] Pauli, D., Hackers plunder Hilton 'HHonors' rewards points, go on shopping spree, Nov 2014. Last accessed on Jan. 28, 2015. http://www.theregister.co.uk/2014/11/05/hilton_honor_cards_breached/

[118] Pavlou, P.A., State of the Information Privacy Literature: Where Are We Now and Where Should We Go? In *MIS Quarterly*, Vol 35, Issue 4, Dec. 2011, pp.977–988.

[119] Pearson, B., Four differences between U.S. and Eurpean loyalty progams, Dec 2013. Last accessed on Jan. 28, 2015. http://www.loyalty.com/research-insights/blog/from-loyal-to-four-differences-between-u-s-and-european-loyalty-programs

[120] Pierre, R., and Timothy, D., Modular strategies: B2B technology and architectural knowledge, In *University of California, Berkeley, Haas School of Business*, Vol. 47, No. 4, 2005, pp.86–113.

[121] Plohmann, D., and Gerhards-Padilla, E., Case Study of the Miner Botnet, In *2012 4th International Conference on Cyber Conflict*, 2012, pp.1–16.

[122] Point Exploration Club (Poitan), Loyalty programs information (in Japanese), 2014. Last accessed on Jan. 28, 2015. http://www.poitan.net

[123] Point Exploration Club (Poitan): Statistical Information of April 2014: Rank of destination LP (in Japanese), 2104. Last accessed on Jan. 28, 2015. http://stats.poitan.net/out-201404.html

[124] Point Exploration Club (Poitan): Statistical Information of April 2014: Rank of origin LP (in Japanese). 2104. Last accessed on Jan. 28, 2015. http://stats.poitan.net/in-201404.html

[125] Point Exploration Club (Poitan): Statistical Information of April 2014: Rank of utilized pair of exchange (in Japanese). 2014. Last accessed on Jan. 28, 2015. http://stats.poitan.net/exchange-201404.html

[126] Poremba, S.M., How Shopping Loyalty Cards Help Identity Thieves, In *Tech News Daily*, Jul. 25 2012. Last accessed on Jan. 28, 2015. http://www.nbcnews.com/id/48310307/ns/technology_and_science-security/t/how-shopping-loyalty-cards-help-identity-thieves/#.VMjafmiUfOM

[127] Portal site of Official statistics of Japan: Japanese-English Contrast Table, 2012. Last accessed on Feb. 9, 2015. http://www.e-stat.go.jp/SG1/estat/GL02020101.do?method=pdfDownload&fileId=000006457491&releaseCount=1

[128] Raskin, M., Dollar-Less Iranians Discover Virtual Currency, In Bloomberg Businessweek - Global Economics, 2012. Last accessed on Jan. 28, 2015. http://www.businessweek.com/articles/2012-11-29/dollar-less-iranians-discover-virtual-currency

[129] Reinartz, W., and Kunar, V., The Mismanagement of Customer Loyalty, In *Harvard Business Review*, Jul. 2002, pp.4–12.

[130] Reposen, Attitude Survey on the Use of Point Cards (in Japanese), Jul. 2013. Last accessed on Jan. 28, 2015. https://reposen.jp/3792/2/50.html

[131] Research Bank, Survey on Women's Usage on Point Services (in Japanese), Jun. 2008. Last accessed on Jan. 28, 2015. http://research.lifemedia.jp/2008/06/080604pointservices.html

[132] Research Bank, ' Survey on Internet Shopping (in Japanese), Jan. 2013. Last accessed on Jan. 28, 2015. http://research.lifemedia.jp/2013/01/130130_netshopping.html

[133] Research Bank, Survey on the Use of Convenience Store (in Japanese), Jul. 2013. Last accessed on Jan. 28, 2015. http://research.lifemedia.jp/2013/07/130724_cvs.html

[134] Research Institute of Economy, Trade and Industry, Japan Industrial Productivity Database 2008 (in Japanese), 2008. Last accessed on Jan. 28, 2015. http://www.rieti.go.jp/jp/database/JIP2008/index.html

[135] Santos, J.R., An input-output framework for assessing disaster impacts on Nashville metropolitan region, In *The 20th International Input-Output Conference & the 2nd Edition of International Scool of Input-Output*

Analysis, Bratislava, Slovakia, Jun. 2012. Last accessed on Jan. 28, 2015. https://www.iioa.org/conferences/20th/papers/files/691_20120501071_JoostSantos-IIOABratislava.pdf

[136] SAS Institute for advanced analytics, business intelligence, data management, and predictive analytics, Are Retailers Making the Most of Loyalty Schemes, 2013. Last accessed on Jan. 28, 2015. http://www.sas.com/offices/europe/uk/downloads/loyalty/loyalty-infographic.pdf

[137] Scan Net Security, 299 IDs Compromised at the Site of T Point (in Japanese: 「Tサイト」の299IDに不正ログインが発生、Tポイントを不正利用される（CCC）), Apr.9, 2013. Last accessed on Jan. 28, 2015. http://scan.netsecurity.ne.jp/article/2013/04/09/31404.html

[138] Schneier, B., Information Security and Externalities, 2007. Last accessed on Jan. 28, 2015. https://www.schneier.com/essays/archives/2007/01/information_security_1.html

[139] Science & Technology Law Institute, Norms of Critical Infrastructire Protection in Japan, Last accessed on Jan. 3, 2015. https://stli.iii.org.tw/en/content_page.aspx?i=6150

[140] Sharp, B. and Sharp, A., Loyalty programs and their impact on repeat-purchase loyalty patterns, In *International Journal of Research in Marketing*, Vol. 14, 1997, pp.473–486.

[141] Sharp, B. and Sharp, A., Loyalty Programs and Their Impact on Repeat-Purchase Loyalty Patterns: A Replication and Extension, In *28th European Marketing Academy Conference proceedings. Berlin, Germany: Institute of Marketing II, Humboldt-University*, 1999.

[142] Shinozaki, A., Yamamoto, Y., and Yamazaki, S., Technical papers on ICT related economics. No. 11-1: Estimation on the Amount of Damage on ICT-Related Capital Stock, 2011. Last accessed on Oct. 3, 2011. http://www.icr.co.jp/ICT/report/TP_201106.pdf

[143] Sloni, D.K., and Sharma, S.K., Effectively Securing Online Business from Online Threat: Minimizing the Risk Associated, In *National Conference on Management Issues: Competing through Capability Enhancement*, 2011. Last accessed on Feb. 20, 2014. http://www.bhagwantuniversity.com/research_papers/securing_online_business.pdf

[144] Smith, G., 52 Ways to Differentiate a Loyalty Program, 2014. Last accessed on Nov. 2014. http://www.colloquy.com/article_view.asp?xd=11672

[145] Smith, R., and Shao, J., Privacy and E-commerce: a Consumer-centric Perspective, In *Electronic Commerce Research*, Vol. 7, Issue 2, Jun. 2007, pp.89–116.

[146] Smith, A., Sparks, L., Hart, S., and Tzokas, N., Delivering customer loyalty schemes in retailing: exploring the employee dimension, In *International Journal of Retail & Distribution Management*, Vol. 32 Issue 4, 2004, pp.190–204.

[147] Statistics Bureau, Ministry of Internal Affairs and Communications, Household Expenditure Report – 2012 Report Summary (in Japanese), 2012. Last accessed on Jan. 28, 2015. http://www.stat.go.jp/data/joukyou/2012ar/gaikyou/pdf/gkall.pdf

[148] Symantec Corporation, Internet Security Threat Report 2014, Vol. 19, 2014. Last accessed on Jan. 28, 2015. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

[149] Tanaka, H., Geography and Information Security: Does Location Affect Information Security Effort? In *the Fourth Forum on Financial Systems and Cyber Security: A Public Policy Perspective*, 2007.

[150] Tanaka, H., Quantitative analysis of information security interdependency between industrial sectors. In *ESEM '09: Proceedings of the 2009 3rd International Symposium on Empirical Software Engineering and Measurement*, 2009, pp.574–583.

[151] Tanaka, H., Matsuura. K., and Sudoh, O., Vulnerability and information security investment: An empirical analysis of e-local government in Japan, In *Journal of Accounting and Public Policy*, Vol. 24, Issue 1, Jan.-Feb. 2005. pp.37–59.

[152] The Institute for Information Infrastructure Protection (I3P), Secutity Solution for the Oil and Gas Industry, Technology Fact Sheet. Inoperability Input-Output Model (IIM), 2007. Last accessed on Jan. 28, 2015. http://www.dartmouth.edu/ i3p/docs/publications/IIM-factsheet-Feb2007.pdf

[153] The Japan Times, Hackers steal data on JAL frequent fliers, airline says, Sept. 2014. Last accessed on Jan. 28, 2015. http://www.japantimes.co.jp/news/2014/09/25/business/corporate-business/data-750000-jal-mileage-club-members-may-leaked/#.VIZsGTGUeik

[154] tnooz (website), Points as cash: How to do a better job protecting loyalty accounts, Nov. 21, 2014. Last accessed on Jan. 28, 2015. http://www.tnooz.com/article/points-cash-better-job-protecting-loyalty-accounts/

[155] Uncles, M.D., Dowling, G.R., and Hammond, K., Customer loyalty and customer loyalty programs, In *Journal of Consumer Marketing*, Vol. 20, Issue 4, 2003, pp.294–316.

[156] United States Government Accountability Office, Virtual economies and currencies: Additional IRS guidance could reduce tax compliance risks, May 2013. Last accessed on Jan. 28, 2015. http://www.gao.gov/assets/660/654620.pdf

[157] Walter, J., Managing Supply Chain Interdependencies, In *AIAG Actionline*, 2006, pp.10–14.

[158] wiseGEEK (website), What is Demand Side Economics?, Last accessed on Jan. 28, 2015. http://www.wisegeek.org/what-is-demand-side-economics.htm

[159] Wong, J.I., Citi Chief Economist: Bitcoin is Closest Commodity to Gold, Nov. 27, 2014. Last accessed on Jan. 28, 2015. http://www.coindesk.com/citi-chief-economist-bitcoin-closest-commodity-gold/

[160] Woodldridge, J.M., Introductory Econometrics A Modern Approach, 5th edition, South-Western Cengage Learning, Canada, 2013.

[161] Zady, M.F., Z-12: Correlation and Simple Least Squares Regression, Last accessed on Dec. 2014. https://www.westgard.com/lesson42.htm

[162] ポイント探検倶楽部, 菊池　崇仁, 新かんたんポイント&カード生活, 自由国民ムック, Apr. 2012.

Appendix A

Publication List

Hard cover:

<1> Bongkot Jenjarrussakul, Kanta Matsuura. Analysis of Japanese Loyalty Programs Considering Liquidity, Security Efforts, and Actual Security Levels. (to be published as a chapter of an edited volume from Springer)

<2> Bongkot Jenjarrussakul, Hideyuki Tanaka, Kanta Matsuura. Sectoral and Regional Interdependency of Japanese Firms Under the Influence of Information Security Risks, In *The Economics of Information Security and Privacy, Böhme, R. (ed.)*, pp.115–134, 2013.

Journal:

<3> Bongkot Jenjarrussakul, Kanta Matsuura. Japanese Loyalty Programs: An Empirical Analysis on their Liquidity, Security Efforts, and Actual Security Levels, In 日本セキュリティ・マネジメント学会誌, Vol. 28, No. 3, pp.17–32, January 2015.

<4> Bongkot Jenjarrussakul, Kanta Matsuura. A Survey on Information Security Economics, In 日本セキュリティ・マネジメント学会誌, Vol. 24, No. 3, pp.53–60, January 2011. (Commentaries)

International conferences:

<5> Bongkot Jenjarrussakul, Kanta Matsuura. Analysis of Japanese Loyalty Programs Considering Liquidity, Security Efforts, and Actual Security Levels, In *The 13th Annual Workshop on the Economics of Information Security (WEIS2014)*, Pennsylvania, USA, June 2014. (Peer-reviewed)

<6> Bongkot Jenjarrussakul, Hideyuki Tanaka, Kanta Matsuura. Sectoral and Regional Interdependency of Japanese Firms under the Influence of Information Security Risks, In *The 11th Annual Workshop on the Economics of Information Security(WEIS2012)*, Berlin, Germany, June 2012. (Peer-reviewed)

<7> Bongkot Jenjarrussakul, Hideyuki Tanaka, Kanta Matsuura. Impact on Information Security from the Great East Japan Earthquake on March 11, 2011. In *Eighth Annual Forum on Financial Information Systems and Cybersecyrity: A Public Policy Perspective*, the University of Maryland, January 2012. (Oral Presentation)

<8> Bongkot Jenjarrussakul, Ryouta Hishiki, Hideyuki Tanaka, Kanta Matsuura, Hideki Imai. Interdependency of Information Security and Its Dependence on IS Multiplier of Sub-industries. In *The 6th International Workshop on Security (IWSEC2011)*, November 2011. (Poster Presentation)

<9> Bongkot Jenjarrussakul, Hideyuki Tanaka, Kanta Matsuura. Empirical Study on Interdependency of Information Security Between Industrial Sectors and Regions. In *Seventh Annual Forum on Financial Information Systems and Cybersecurity: A Public Policy Perspective*, the University of Maryland, January 2011. (Oral Presentation)

Domestic conference:

<10> Bongkot Jenjarrussakul, Kanta Matsuura. Impact from Security Incidents and Partnership in Japanese Loyalty Program, In *The 32th Symposium on Cryptography and Information Security(SCIS '15)*, IEICE, Kokura, Japan, January 2015.

<11> Bongkot Jenjarrussakul, Kanta Matsuura. Another Class of Function for the Productivity Space of Information Security Investment, In *The 30th Symposium on Cryptography and Information Security(SCIS '13)*, IEICE, Kyoto, Japan, January 2013.

<12> 飛鋪亮太, Bongkot Jenjarrussakul, 田中秀幸, 松浦幹太, 今井秀樹, 日本における情報セキュリティの相互依存性の分析, 電子情報通信学会情報セキュリティ研究会 (電子情報通信学会技術研究報告), Vol.111, No.455, pp.23–29, 2012.

<13> Bongkot Jenjarrussakul, Hideyuki Tanaka, Kanta Matsuura. Information Security and Impact from the Great East Japan Earthquake, In *The 29th Symposium on Cryptography and Information Security(SCIS '12)*, IEICE, Kanazawa, Japan, January 2012.

<14> Bongkot Jenjarrussakul, Hideyuki Tanaka, Kanta Matsuura. Empirical Study on Interdependency of Information Security Between Industrial Sectors and Regions, In *The 28th Symposium on Cryptography and Information Security(SCIS '11)*, IEICE, Kokura, Japan, January 2011.