Master Thesis
修 士 論 文

Empirical and Theoretical Analyses on the Security of Japanese Loyalty Programs

日本のロイヤルティプログラムのセキュリティに関する実証分析および理論分析

Submitted by

SHINODA, Shiori

篠田 詩織

Acknowledgement

Firstly, I would like to express sincerely appreciation to my supervisor, Professor Kanta Matsuura, for his guidance during my graduated school days. I have learned a lot from him about how to conduct research, how to think and view on security issues, what we should treat as important things regarding security, and many other things.

I would also like to appreciate to the other professors for fruitful discussion in the colloquium and the defense.

I thank Takahito Kikuchi, the owner of Poitan.net, who kindly provided the data and useful information for this study.

I would like to thank the all Matsuura-lab members including OBs and OGs, the secretaries, and visitors of the meeting.

I am supported by all of my friends, from those of the kindergarten to the university.

My favorite foods, Natto rice with Osawarouho's seaweed, and miso soup with Kayanoya's dashi, also helped me to survive my graduate school days.

Finally, I would like to thank my family and relatives — in particular my mother, father, brother, grand-mother, grand-father, and the hamsters — for supporting me a lot in many ways.

Abstract

Since much personal information or confidential information are now digitally stored and those storage are connected to the network, attackers have chances to thieve them remotely. However, while business firms or government institutions with such important information assets have to protect them from malicious people as much as possible, it is still an open question how much they should invest on information security.

Gordon and Loeb first developed the economic model of cybersecurity investment in which vulnerability and threat are first separately considered and explicitly defined, and showed some interesting implications. Their findings can be helpful to the investment decision making, but there is no established ways to measure threat while we can measure vulnerability by counting the system's vulnerability checklist.

In order to investigate what can be threat metrics, we focus on loyalty programs security issues, which are becoming big problems but have not been well studied until now.

Loyalty program (LP) is a popular marketing activity of enterprises. As a result of firms' effort to increase customers' loyalty, point exchange or redemption services are now available worldwide. In particular, Japanese LPs are taking partnership each other and therefore point exchange network has widely expanded, which enables customers to redeem points from one LP to another LP. However, these services have attract not only customers but also attackers whose purpose is to obtain monetary benefits and LPs are suffering from a large number of incidents in which LP points are stolen.

In a previous pioneering research which first focused on this LP security problem, an empirical analysis based on Japanese data is shown to see the effects of LP-point liquidity on damages caused by security incidents. They constructed an empirical model based on Gordon-Loeb's formulation of security investment and treated point liquidity as threat. However, the point liquidity definition is still not well studied.

In this thesis, we reconsider the liquidity definition based on a further observation of LP security incidents. By using newly defined proxies corresponding to the threat as well as other refined proxies, we test hypotheses to derive more implications which help LP operators to manage partnerships; the implications are consistent with recent changes in the LP network. Moreover, we construct a simple economic model of the LP operator's profit, and examine the trade-off problem regarding profit, point liquidity, and security investment.

The findings from our work can help LP operators to manage partnership and decide security investment. Our work may also inspire further work on the security of virtual currencies or electric payment beyond LPs.

Contents

Chapter 1

Introduction

1.1 Background and Motivation

Many entities are now connecting to the network. If personal information or confidential information are digitally stored and the storage are connected to the network, attackers have chances to thieve them remotely. When a business firm lets attackers thieve their customers' personal information, customers may feel anger, and the firm may lose trust in addition to the enormous damage for the compensation. Or, when government institutions let attackers thieve their confidential information, it may cause the damages which affect the whole domestic country or even the whole world.

So, business firms or government institutions with information assets have to protect their information from attackers as much as possible. However, as the same as the other all security problems, there is a trade-off, which is, in this case, between security and profit. While much investment may lead to deficit balance, no investment may lead to trust loss and profit decreasing. In consequence, they are facing decision problems how much they have to invest on information security for the information protections.

What first shed light on the ways to the security investment problems was a simple model which Gordon and Loeb introduced [7]. They first separately considered and explicitly defined *vulnerability* and *threat* in an attacking situation. *Threat* is the probability that an attacks occurs, and *vulnerability* is the conditional probability that the attacks successes on the condition that an attacks occurs.

The implications from the Gordon-Loeb's model can help organizations to decide security investment, but there is no established ways to measure *threat* while we can measure *vulnerability* to some extent by counting system's vulnerability checklist.

In this context, we focus on the loyalty program's security issues in order to try to derive some implications which will help to make the *threat* metrics.

Loyalty programs (LPs) are structured marketing efforts which reward, and therefore encourage, loyal behavior of customers [1].LPs have proliferated in recent years as companies seek to acquire and retain customers, increase customer spending, influence customer spending habits, and encourage the purchase of additional products [2].

However, some studies such as [3] argued that since most firms now utilize LPs, they are no longer effective in contributing to competitive advantage. Consequently, many firms are attempting to redesign LPs to enhance their effectiveness. In particular, in

order to increase customers' loyalty, point exchange or redemption services have matured worldwide. For example, Points.com[1] is a major point exchange or redemption service in the U.S. In Japan, point exchange network is expanding, which enables customers to redeem points from one LP to another LP [4]. However, these services attract not only customers but also attackers whose aim is to obtain monetary benefits. In fact, there are an increasing number of LP incidents worldwide, as described in Chapter 2.

There is a pioneering research on these LPs incidents by Jenjarrussakul and Matsuura [6]. They studied the features of LP network, and conducted an empirical analysis with a linear regression model with four fundamental factors, damage, expense (or security investment), threat, and vulnerability, as in Gordon-Loeb model. Then they provided security-liquidity implications by using the *liquidity* of an LP as a metric of threat.

Although they found out that liquidity can be a threat metric, the definition of the liquidity itself is not deeply studied. The possibility of using other metrics is not well considered, either. In this paper, we investigate this threat metric more deeply by considering different metrics based on an observation of actual security incidents on LP systems. Moreover, we also try to see the trade-off between profit and security risk regarding LP liquidity and security investment.

Our empirical study contribute to this context in the following points. First, the liquidity definition is reconsidered, and more intuitively convincing one is introduced. Second, we observe actual security incidents more deeply and give more implications which help LP operators to manage partnerships; the implications are consistent with recent changes in the LP network. Minor changes over the model proxies used to test hypotheses also help our empirical study.

Moreover, in order to examine the trade-off between profit and security, we construct a simple economic model based on Matsuura's revised Gordon-Loeb model [9]. The numerical examples are shown to see the profit optimization problems regarding liquidity and security investment.

Our work may also inspire to other virtual currencies or electric payment research. Virtual currencies such as Bitcoin or game currencies are also frequently theft. Online banking is quite well abused and legitimate users' assets are stolen every day. Because of the convenient financial network, the liquidity is raised but the systems are exposed to threats. The liquidity of these services reduces costs, provides great usability with not only the customers but also the operators, and improves efficiency of the whole economy. However, the security risk is also raised as the liquidity is raised. We may derive some interesting implications if we focus on the threats on them like the way we explain the LP cases in this thesis.

1.2 Outline and Summary of This Thesis

In this thesis, we show empirical and theoretical analyses on LPs security issues. We investigate liquidity definition , which leads to some implications on what can be a threat metric in LP security problems. Moreover, we also considered the profit optimization problems with regard to the security risk on LP.

[1] `https://www.points.com`

- In Chapter 2, we see major incidents on LPs which occurred worldwide and their characteristics as well as the trend of LPs.
- In Chapter 3, we describe the related and previous works.
- In Chapter 4, we show the methods and results of empirical analyses on Japanese LPs, using linear regressions considering Gordon-Loeb's model of security investment. We reconsider liquidity definition over the pioneering previous research, and showed some implications: if an LP has more outgoing partnerships, the damage from the incidents get bigger; number of outgoing partners with short time redemption affect more on damage than those with long time redemption; if an LP has outgoing partnership with Amazon Gift Card or iTunes Gift Code, the damage from the incidents get bigger.
- In Chapter 5, we introduce logistic regression using the real data of LP incidents. Also, we utilize the social network analysis metrics for measuring the threat and derive some implications.
- In Chapter 6, we construct a simple model regarding a firm's profit and security risk with LP. Liquidity is considered on a threat proxy based on the current empirical findings. Then the profit optimization problems are solved with respect to the LP points liquidity and security investment.
- Lastly, Chapter 7 concludes this thesis and see the future prospects.

Chapter 2

Incidents on Loyalty Programs

2.1 Trend of Loyalty Program

Loyalty program's marketing value is large in developed countries. The most popular LP is the mileage programs operated by airline companies. It is reported that the annual amount of issued mileage is more than seven billion dollars [54], and the amount of all issued mileage is more than 10 trillion dollars [58]. In Japan, the annual issued points in 2013 is estimated to amount 868.4 million (0.17% of GDP) [59]. The number of LP members in the U.S. amounted to 2.6 billion people which increased by 26.7 % from 2010 to 2012 [55]. People who use at least one LP is over 90% in Canada [56], and over 90% in Japan [57].

Let us introduce the recent trend of the LP structure. In many countries, such as Germany, U.S., Japan and Korea, the coalition loyalty program has become popular [58]. The redemption and exchange services are also introduced. In Japan, the redemption partnership network has matured, which enables one to redeem his/her points from one LP to another LP. In the U.S., some services such as Points.com provide a points redemption/exchange platform.

2.2 Security Incidents on Loyalty Programs

If one can exchange LPs points with other valuable goods or currencies, the point itself has value. LP operators are trying to add more ways users expense LP points out, which leads to rises of the users' loyalty. However, not only customers but also malicious people find attractiveness of LP points' value and indiscriminate attackers have become to target LP points which can be eventually transformed to real currency.

We will show some examples of the actual worldwide occurring incidents. In the U.K., users' miles in British Airways loyalty program were stolen by using credentials stolen in third party in March 2015, as Dark Readinig.com reported [10].

In the U.S., rewards points of Hilton Hotel loyalty program were stolen in November 2014, as KrebsOnSecurity reported [11].This case happened because the login process is weak, such that it required only 4 digit PIN code and allowed hackers to success attack attempts easily with a brute force method. It says that hackers can not only sell the stolen accounts or redeem the points into other gift cards at Points.com and other locations that

Table 2.1: Major LP security incidents in Japan.

Date	LP	# of attempts	Redemption destination	# of login attempts	# of redemption fraud	Damage (USD)	Source
2012.4.14-16	G Point	-	Amazon Gift Card	59044	442	13258	[15]
2013.3.26	T Point	-	other account	299			[16]
2013.12	Rakuten Super Point	-	electric money	about 250		24590	[17]
2014.1.19 13:00	Potora	-		323			[18]
2014.1.31-2.2	JAL Mileage Bank	-	Amazon Gift Card	-	65	>10000	[19]
2014.3	Suica Point Club	920000		-			[20]
2014.2	Hatena	-	Amazon Gift Card	-			[21]
2014.3.7-9	ANA Mileage Club	-	iTunes Gift Code	9		5328	[22]
2014.3	Oki Doki Point Program	-	T point	100-500	Some		[23]
2014.4.19-29	Sony Point	-	Playstation store ticket, mora music card	-	273	6172	[24]
2014.5.27-6.4	niconico point	-		219926	19	1423	[25]
2014.6.16-19	Hatena	1600000	Amazon Gift Card	2398	0 (of 3 attempts)		[26]
2014.6.23	CAPAT	-		-	203		[27]
2014.7.4	anpara	3420000		15092	60		[28]
2014.7.11-28	Poin-talk	-	prize, other point programs	1,265	568	4918	[29]
2014.8	Suica Point Club	300000		756			[30]
2014.1	D STYLE WEB	-		108185	47		[31]
2014.11	hearcon	3160000		1320	291		[32]
2014.12.23	morappo (mixi)	19600000		4536	332	3,566	[33]
2015.5.17-6.29	AIP	-		≤18935	33	1228	[34]
2015.7.4-6	Life Media	-	Amazon Gift Card, iTunes Gift Code	30001	0 (of 25 attempts)	0	[35]
2015.7	Orico Point	-	T Point	-	156		[36]
2015.7.11 PM	Prize Prize	-	Point-on PON	-	Some		[37]
2015.8.4 14:00	Lodging Net Point	-	Amazon Gift Code	-	123	2418	[38]

convert points to currency, but also buy expensive items at Hilton shopping mall.[1]

It is reported by The Dallas Morning News that about 10,000 accounts' miles of American and United Airlines loyalty programs were stolen in late December 2014 [12].It says Delta Airlines detected similar attempts to crack into customers' accounts in late 2014 but isn't aware that any were successful.

Additionally in March 2015, "with Starbucks, hackers were somehow (still unclear) able to obtain customer usernames and passwords that opened up access to payment methods, which were used to refill gift card balances and transfer out gift card funds. Hackers can then sell these gift card balances to other people," MyBankTracker reported [13].In these cases, hackers are said to have used ID-password lists for cracking.

There are an increasing number of LP security incidents in Japan as well [14]. Table 2.1 shows a list of major security incidents of LPs in Japan collected from web news articles.

[1] `https://www.hiltonhhonorsshopping.com/`

For the following empirical analyses using Japanese data, we would like to closely look at these Japanese incidents survey in Table 2.1. According to it, we can find some characteristics of the attackers' behavior: they often (1) attempt to break the web login authentication to compromise as many accounts as possible, (2) act malicious attempts in one or two days at once, and (3) attempt to steal the compromised accounts' points by redeeming into certain LPs.

The first characteristic is shown by the following observations. In the incidents on the airline mileage programs, since they had provided a very weak authentication system with only 4-digit PIN, brute force attack is used for the unauthorized logins. The other incidents are said to be identity frauds; attackers used an ID-password list they obtained from some other third parties in advance.

The second one is clear if we see the first column of Table 2.1. Attackers often take actions in one or two days, so almost all the attacks are recognized after attackers finish actions and operators are informed by some customers whose points have been already stolen. Because of the difficulties of real-time detection, some LPs with automatic redemption processing systems tend to be damaged and others which take time to redeem tend to avoid damages.

The third one is suggested by the following observations and speculations. We also find that Amazon Gift Card [2] and iTunes Gift Code[3] are often chosen as the redemption destinations by attackers. We can show several reasons that Amazon and iTunes Gift are often chosen by attackers. Firstly, it is because it is easy to exchange them with real money by selling the codes. When we redeem LP points into Amazon Gift Voucher or iTunes Gift Code, we get an alphabet code of them via e-mail, which becomes a coupon when we enter the codes in the website. Amazon and iTunes Gift may be attractive for attackers because the codes can be sold and eventually converted into real money. Secondly, it is because attackers live abroad Japan. It is said that all these attacks are from abroad. Amazon and iTunes are both the services provided internationally and the head office is in America (abroad Japan), so attackers can avoid pursuit from Japanese polices because domestic polices cannot investigate abroad offices. Thirdly, it is because Amazon and iTunes are not willing to publish the redemption algorithm that is used for the exchanges from specific alphabet codes to a discount coupon. Without their disclosure of this algorithm, we cannot pursuit and find who got the stolen points.

Thus we can see that criminals usually attack authentication mechanisms of LP systems.

[2] `http://www.amazon.com/gift-cards/`

[3] `https://www.apple.com/support/itunes/cards-codes/`

Chapter 3

Related Works

3.1 Partnership Network of Japanese Loyalty Programs

For LP, the effectiveness of the program system is well investigated in the management area [3]. Also, there are some researches which focus on the Japanese point exchange network from the management or economic point of view, which try to derive some helpful implications to operate LP using social network analyses. For example, the researches on the characteristics of Japanese LP exchange network [39], the factor which leads LP partnership [40], LP network's economic reliability [41] and the network's impact on marketing performances [4] were conducted. It is tried to visualize the network of airline's frequent flier program and other LPs Mileage program using network centrality metrics [60].

However, these works do not consider security issues on LP systems.

3.2 Virtual Currency and Security

ECB defined virtual currency as "a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community" and pointed out that LP points or miles satisfy the definition if they are provided via web [5].

Other representative virtual currencies include cryptocurrency and game currency. Since these currencies have relatively new schemes than traditional currencies, they receive many attention by researchers of wide range, from the central banks, who have interests on whether the new currency will give a blow on traditional one, to the computer scientists, who have interests on how the currency can be designed more effective way. In this literature, the studies on these virtual currencies' security are also being conducted both in theoretical and empirical ways because the scam methods attackers take are the problems in order to make the system sufficiently secure.

For cryptocurrency, Bitcoin, the most popular one, is the main research target. Moore and Christin conducted empirical analysis of Bitcoin-exchange risk, inspired by the fact that many bitcoin exchanges suffer breaches or are driven to closure and its users suffer loss. They showed that a less popular exchange are more likely to be shut down than popular ones but popular ones are more likely to suffer a security breach [42]. Vasek et al. empirically analyzed denial-of-service attacks on exchanges, mining pools, gambling

operators and so on [43]. Johnson et al. explored the trade-off between mining pool's strategies, invest computing resources to win the next mining race or take DDoS attacks on a competing mining pool, with a series of game-theoreical models of competition between two pools [44]. Kroll et al. analyzed whether Bitcoin protocol can survive attacks game-theoretically [45]. Because of the Bitcoin's novel system architecture and its popularity, many researches are being conducted considering security issue.

Massively multiplayer online games (MMOGs) currencies are also one of the virtual currencies and its security issues have also been researched. Hu and Zambetta investigated MMOGs' security issues and proposed a taxonomy framework for online cheating [46]. Ku et al. studied MMOGs crime characteristics empirically using Taiwan's crime reports between 2002 to 2004 [47]. Bardzell et al. classified the MMOGs fraud [48]. Kiond et al. explored some security risks in virtual economies with Second Life[1] [49]. Irwin and Slay indicated that money laundering and terrorism financing may be within MMOGs [50].

Although these works handle security problems, they do not consider relation between Bitcoin/MMORPGs coins and LP systems.

3.3 Loyalty Program and Security

Enzmann and Schneider proposed privacy-friendly LP systems using a signature protocol in order to keep customer retention [61].

Real LP security incidents were first economically researched by Jenjarrussakul and Matsuura, which was presented at workshop on economics of security in 2014 [6]. They showed two implications: the impact of LP security incidents gets lower if stronger security requirements in web authentication process are satisfied, and gets higher if the liquidity of the LP points gets higher.

Our work is inspired by this primary study by Jenjarrussakul and Matsuura.

3.4 Attackers' Target Firms

We investigate mainly the threat on the LP systems which business firms are operating. Some researches exist which focus on the attackers' behavior or profiles of the targeted firms. The reports from the many security vendors, such as Symantec [64], provides the brief statistics regarding business sectors or organization sizes. Thonnard et al. [62] empirically studied the profiles of the targeted organizations and showed that certain industry sectors and larger organizations are statistically at elevated risk compared with others. Sarabi et al. [63] empirically showed that the incidents types are likely to be different between each business profiles. These analyses can be helpful to estimate risks of security incidents for business firms, but they did not consider threat itself.

3.5 Investment Model of Cybersecurity

We construct a economic model for LP security analysis based on the previous research on the investment model of cybersecurity.

[1] `http://secondlife.com/`

Among many proposed models, Gordon and Loeb's security investment model is the most famous one [7]. There are some inspired work on this model such as [8], [9], [53], [66].

Chapter 4

Empirical Analyses on Loyalty Programs considering Investment Models

4.1 Introduction

When we consider security investment to reduce the damages by such incidents, we need to ask the features of LP network from the viewpoint of the effects of security investment. In order to answer to the above question, Jenjarrussakul and Matsuura [6] conducted an empirical study of LPs. Their study was performed inspired by the Gordon-Loeb model [7] of security investment; they considered damage, expense (or security investment), threat, and vulnerability as four fundamental factors when they developed their empirical analysis model. In particular, they provided security-liquidity implications by using the *liquidity* of an LP as a metric of threat. This analysis is possible because threat (defined as the probability of a threat occurring) and vulnerability (defined as the conditional probability that a threat once realized would be successful) are handled separately.

However, the definition of the liquidity itself is not deeply studied. The possibility of using other metrics is not well considered, either. In this chapter, we investigate this threat metric more deeply by considering different metrics based on an observation of actual security incidents on LP systems.

Our work to be reported in the rest of this chapter is inspired by the primary study [6] but there are important differences as follows. First, the liquidity definition is reconsidered, and more intuitively convincing one is introduced. Second, we observe actual security incidents more deeply and give more implications which help LP operators to manage partnerships; the implications are consistent with recent changes in the LP network. Minor changes over the model proxies used to test hypotheses also help our empirical study.

4.1.1 Chapter Organization

The rest of this chapter is organized as follows. In Section 4.2, the data used in our empirical analyses are shown. In Sections 4.3, 4.4 and 4.5, different threat metrics and liquidity definition are investigated. Lastly, Section 4.6 concludes this chapter.

Table 4.1: Data used in our study.

Data	Details
LPs	82 Japanese LPs which were selected by Jenjarrussakul and Matsuura [6] among 207 Japanese LPs registered at Poitan.net in Feb. 2014. For details, see Appendix B.1.
Security investment and damage amount of security incident	Retrieved from Information Processing Census (2012), the statistical data by METI (Ministry of Economics, Technology and Industries) of Japan [51].
Exchange network	Retrieved at Poitan.net in Dec. 2014.
Security requirement	Retrieved by Jenjarrussakul and Matsuura [6] in Apr. 2014; they investigated security requirements in each process of registration, login authentication and back-up authentication. For more details, see Appendix B.3.3.
Capital size	Retrieved from every LP operator's web page,in Feb. 2015. Each capital size is shown in Appendix B.1.

Table 4.2: Representative metrics of LPs partnership network in September 2014.

# of nodes	# of edges	Density	Average path length	Clustering coefficient
239	1265	0.0222	3.39	0.0985

4.2 Data Collection

For empirical analyses, we collected data from some sources. We retrieved the LP network structure from Poitan.net[1], a portal site of Japanese LP network where users can search possible routes of point redemption, find the market value of each LP point, and so on (see Appendix A.1.). Each LP operator's capital size was retrieved from each LP operator's website. The data of the security investment, damage amount and security investments are the same as those in [6]. Table 4.1 summarizes the data used in our study.

Figure 4.1 shows partnership network between LPs in Japan. Each node represents each LP, and each edge represents each exchange route. LPs with no partner are omitted in this figure. Table 4.2 shows representative metrics of this network. In September 2014, the number of LPs which has at least one partnership is 239 out of all 274 LPs registered in Poitan.net.

4.3 Point Liquidity and Number of Partners

4.3.1 Hypothesis Development

In the previous work by Jenjarrussakul and Matsuura [6], it was showed that an LP with higher liquidity points suffers a bigger impact from incidents. *Liquidity* means the degree to which an asset or security can be quickly bought or sold in the market without affecting the asset's price. This implication is the very important one to LP operators in

[1] `http://www.poitan.net`

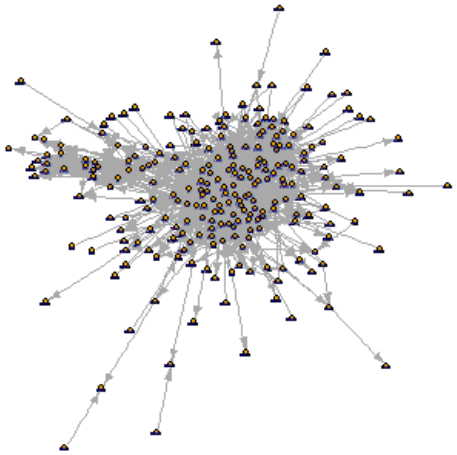


Figure 4.1: Partnership network between LPs in Japan in September 2014.

taking partnerships with other LPs because the *liquidity* was defined by the number of partnerships.

However, the definition of the liquidity in [6] was not intuitively convincing one. As described in detail in Appendix C, it was defined as

$$liquidity_i = x_i * y_i \tag{4.1}$$

where i is an index which indicates each LP, x_i is the number of edge types and y_i is the number of partners. Figure 4.2(a) and (b) show this definition graphically. Against this definition, you would wonder if it is necessary to multiply the edge type x_i and if the coming partner really affect on the liquidity of LP$_i$'s points. For example in Figure 4.2(b.2) and (b.3), number of partners is tha same but the number of edge types is different. It is intuitive when $liquidity_k > liquidity_j$ is consisted, but this definition establishes $liquidity_k < liquidity_j$.[2]

It may be more intuitive and release us from these worries if *liquidity* is defined more simply as:

$$liquidity_i = GoPartner_i \tag{4.2}$$

where $GoPartner_i$ is the number of partners into which one can redeem points from LP$_i$. Figure 4.2(b) shows this calculation graphically.

In order to examine this definition, we set the following hypothesis:

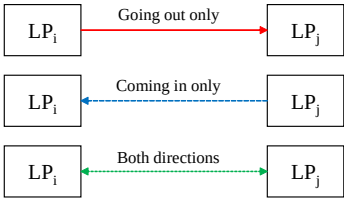
H1. An LP with more outgoing partners suffers bigger damage.

4.3.2 Model

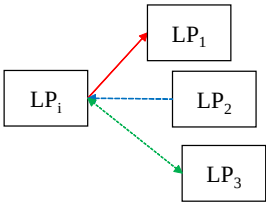
In order to test *H1*, the following linear regression model is set:

$$\frac{\log(damage_i)}{\log(capital_i)} = \beta_0 + \beta_1 \frac{\log(expense_i)}{\log(capital_i)} + \beta_2 GoPartner_i + \beta_3 sec\_score_i + u_i \tag{4.3}$$

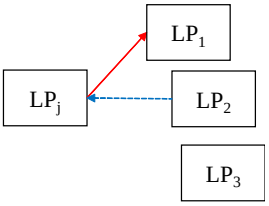
[2] Appendix **??** shows why they defined *liquidity* as this. Since they first tried to deal with LP security issues not LP-wise but industry-wise and they apply it to LP-wise situations without any changes, these kind of mismatch has happened.



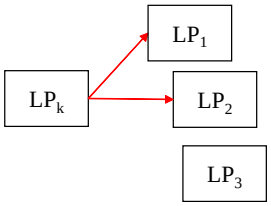
(a) Three edge types.



(b.1) $x_i = 3, y_i = 3$, $liquidity_i = 9$ by (4.1) $liquidity_i = 2$ by (4.2).



(b.2) $x_j = 2, y_j = 2$, $liquidity_j = 4$ by (4.1) $liquidity_j = 1$ by (4.2).



(b.3) $x_k = 1, y_k = 2$, $liquidity_k = 2$ by (4.1) $liquidity_k = 2$ by (4.2).

(b) Examples of liquidity calculation using two definitions, (4.1) and (4.2). It is intuitive when $liquidity_k > liquidity_j$ is consisted, but this definition establishes $liquidity_k < liquidity_j$.

Figure 4.2: LP point liquidity definition by Jenjarrussakul and Matsuura [6] and ours.

where i is an index which indicates each LP, $damage_i$ is the annual damage amount of the overall IT security incidents of LP$_i$'s operator, $capital_i$ is the capital size of LP$_i$'s operator, $expense_i$ is the annual IT security expense of LP$_i$'s operator, $GoPartner_i$ is the number of the partners into which one can redeem points from LP$_i$, sec_score_i is the security requirement level of the LP$_i$'s authentications, and u_i is the model's error term, assumed to be independent of the observed covariates. For more calculation details of these proxies, see Appendix B.3.

Correlations between variables are shown in Table 4.3.

Table 4.3: Correlations between the variables in Equation (4.3). To save space, the following notations are used: ldam is log($damage_i$), lcap is log($capital_i$), lex is log($expense_i$), GoPartner is $GoPartner_i$ and SecScore is sec_score_i.

	log(damage)/ log(capital)	log(expense)/ log(capital)	GoPartner	SecScore
log(damage)/ log(capital)	1.000	-	-	-
log(expense)/ log(capital)	0.790	1.000	-	-
GoPartner	0.204	0.090	1.000	-
SecScore	-0.491	-0.417	0.025	1.000

Table 4.4: Results of the linear regression by Equation (4.3). The notations are the same as in Table 4.3

Variable	Coef.	Std. Err	Prob.
C	-0.218	0.091	0.020**
Expense	1.107	0.117	0.000***
GoPartner	0.002	0.001	0.029**
Secscore	-0.054	0.019	0.006***
Adj. R2	0.677		

p-value tells significance of the data.
** indicates significance at 5% level.
*** indicates significance at 1% level.

4.3.3 Results and Discussion

To test *H1*, let a null hypothesis be $\beta_2 = 0$ in Equation (4.3). *H1* is accepted if this null hypothesis rejected. The estimated result is shown in Table 4.4. The coefficient of $GoPartner_i$ is significantly positive, so null hypothesis $\beta_2 = 0$ is rejected and *H1* is accepted. Additionally, the coefficient of *sec_score* is significantly negative. This result is consistent with the results of [6].

4.4 Does Time Required for Redemption Affect the Damage?

4.4.1 Hypotheses Development

When you redeem points from one LP to another LP, you apply the redemption request but it is not always approved soon; it may take one week, or even longer. For example, if you apply redemption from your ANA (All Nippon Airways) miles to iTunes Gift Code, your iTunes Gift Code is issued 7 days after the application.

If the LP operators have longer time to give approval, they may notice suspicious redemption applications and reject them with higher chances. Thus attackers may prefer quicker redemption to avoid the risk of being detected. In fact, the incidents surveyed in Chapter 2 suggest this preference. LPs always didn't notice the attacks until victims, who received confirmation emails or found their points lost, contacted the corresponding LP, or until they saw many suspicious requests at the step of the approvals. If LPs approve redemptions soon automatically after the requests, attackers can easily get issued points of their purposes.

So let us consider the following null hypothesis.

H2. If an LP has more number of outgoing partners with short redemption time, the damage from incidents gets bigger.

4.4.2 Data and Descriptive Statistics

Figure 4.3 shows the histogram of the time required for redemptions of all the exchange routes of 274 LPs and Table 4.5 shows the descriptive statistics. Table 4.6 shows the descriptive statistics regarding the 82 selected LPs.

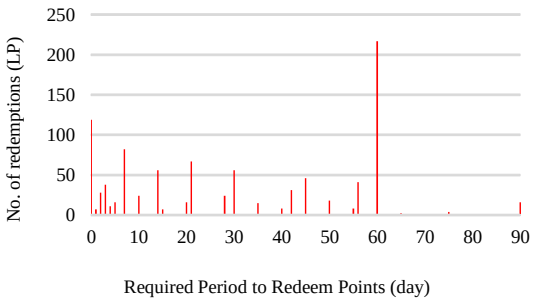


Figure 4.3: Histogram of the time required for redemption in December 2014.

Table 4.5: Descriptive statistics of the time required for redemption.

No. of edges	Min	Max	1st Quartile	3rd Quartile	Mean	Median
1265	0	90	7	56	30	28

Table 4.6: Descriptive statistics of the number of outgoing partners regarding the 82 selected LPs. Go_N represents the number of partners into which one can redeem points from each LP within N days.

	Min	Max	1st Quar.	Median	3rd Quar.	Average	Std. Dev.
Go_0	0	9	0	0	1	0.890	1.61
Go_5	0	16	0	1	2	1.77	2.79
Go_{10}	0	19	0	1	3	2.44	3.72
Go_{20}	0	19	0	1	3	2.44	3.72
Go_{30}	0	26	0	2	4	3.15	4.54
Go_{45}	0	37	0	2	7	4.55	6.41
Go_{60}	0	39	1	3	9	6.33	7.85
Go_{90}	0	40	1	3	9	6.50	7.94

Table 4.7: Correlations between the variables in Equation (4.4) for different values of N. Go_N represents $GoPartner_{i,N}$ and the other notations are the same as in Table 4.3.

(a) $N = 0$

	ldam/lcap	lex/lcap	Go_0	Go_{90}-Go_0	SecScore
ldam/lcap	1.000	-	-	-	-
lex/lcap	0.790	1.000	-	-	-
Go_0	0.273	0.247	1.000	-	-
Go_{90}-Go_0	0.164	0.044	0.380	1.000	-
SecScore	-0.491	-0.417	-0.134	0.058	1.000

(b) $N = 5$

	ldam/lcap	lex/lcap	Go_5	Go_{90}-Go_5	SecScore
ldam/lcap	1.000	-	-	-	-
lex/lcap	0.790	1.000	-	-	-
Go_5	0.223	0.255	1.000	-	-
Go_{90}-Go_5	0.152	0.000	0.333	1.000	-
SecScore	-0.491	-0.417	-0.192	0.112	1.000

(b) $N = 10$

	ldam/lcap	lex/lcap	Go_{10}	Go_{90}-Go_{10}	SecScore
ldam/lcap	1.000	-	-	-	-
lex/lcap	0.790	1.000	-	-	-
Go_{10}	0.320	0.265	1.000	-	-
Go_{90}-Go_{10}	0.075	-0.047	0.278	1.000	-
SecScore	-0.491	-0.417	-0.184	0.234	1.000

(c) $N = 30$

	ldam/lcap	lex/lcap	Go_{30}	Go_{90}-Go_{30}	SecScore
ldam/lcap	1.000	-	-	-	-
lex/lcap	0.790	1.000	-	-	-
Go_{30}	0.289	0.210	1.000	-	-
Go_{90}-Go_{30}	-0.001	-0.121	0.379	1.000	-
SecScore	-0.491	-0.417	-0.100	0.196	1.000

(d) $N = 45$

	ldam/lcap	lex/lcap	Go_{45}	Go_{90}-Go_{45}	SecScore
ldam/lcap	1.000	-	-	-	-
lex/lcap	0.790	1.000	-	-	-
Go_{45}	0.294	0.171	1.000	-	-
Go_{90}-Go_{45}	-0.081	-0.117	0.278	1.000	-
SecScore	-0.491	-0.417	-0.088	0.234	1.000

(e) $N = 60$

	ldam/lcap	lex/lcap	Go_{60}	Go_{90}-Go_{60}	SecScore
ldam/lcap	1.000	-	-	-	-
lex/lcap	0.790	1.000	-	-	-
Go_{60}	0.204	0.090	1.000	-	-
Go_{90}-Go_{60}	0.034	0.006	0.123	1.000	-
SecScore	-0.491	-0.417	0.021	0.063	1.000

4.4.3 Model

To test *H2*, we set the linear regression model as follows:

$$\begin{aligned}\frac{\log(damage_i)}{\log(capital_i)} &= \beta_0 + \beta_1 \frac{\log(expense_i)}{\log(capital_i)} + \beta_2 GoPartner_{i,N} \\ &\quad + \beta_3 (GoPartner_{i,90} - GoPartner_{i,N}) + \beta_4 sec\_score_i + u_i \quad (4.4)\end{aligned}$$

where $GoPartner_{i,N}$ is the number of the partners into which one can redeem points from LP_i within N days and the other variables are the same those in Equation (4.3). Correlations between variables are shown in Table 4.7.

4.4.4 Results and Discussion

The estimated results of Equation (4.4) for $N = 0, 5, 10, 30, 45, 60$ are shown in Table 4.8. When N is 0 or 5, β_3 is significantly positive but β_2 does not show any significances, which means if an LP has larger number of partners into which one can redeem over the threshold time of 0 or 5 days, the LP suffers larger damage. On the other hand, when N is 45 or 60, β_3 shows no significance but is significantly positive, which means if an LP has larger number of partners into which one can redeem under the threshold time of 45 or 60 days, the LP suffers larger damage. When N is 10 or 30, no significances were provided.

These results suggest that the number of outgoing partners which require about 45 days or longer for redemption does not affect the liquidity. That is, although it is not supported if the threshold time is 5 days, *H2* is supported if the threshold time is 45 days. This might be different from the intuition, but as a whole, it is shown that the damage gets bigger if the LP takes more partnerships with shorter redemption time. Thus we find that redemption time has some effects on liquidity, and hence, on the threats to LPs.

Table 4.8: Results of linear regression (4.4) for each $p = 0, 5, 10, 30, 45, 60$.

	N = 0			N = 5			N = 10		
Variable	Coef.	Std.Err	Prob.	Coef.	Std. Err	Prob.	Coef.	Std. Err	Prob.
C	-0.219	0.0930	0.0212**	-0.238	0.0908	0.0106**	-0.221	0.0931	0.0202**
Expense	1.11	0.119	0***	1.14	0.116	0***	1.11	0.120	0.000***
Go_p	0.00148	0.00475	0.763	-0.00259	0.00268	0.337	0.00147	0.00212	0.489
Go_{90}-Go_N	0.00197	0.00103	0.0607*	0.00316	0.0011	0.0054***	0.00214	0.0133	0.110
Secscore	-0.0543	0.0192	0.0061***	-0.0602	0.0191	0.0023***	-0.0550	0.0195	0.0063***
Adj. R2	0.677			0.690			0.677		
	N = 30			N = 45			N = 60		
Variable	Coef.	Std. Err	Prob.	Coef.	Std. Err	Prob.	Coef.	Std. Err	Prob.
C	-0.222	0.0934	0.0199**	-0.209	0.0919	0.0261**	-0.217	0.0919	0.0206**
Expense	1.11	0.120	0***	1.09	0.118	0***	1.11	0.117	0***
Go_N	0.00162	0.00137	0.242	0.00259	0.00113	0.0253**	0.00187	0.000881	0.0367**
Go_{90}-Go_N	0.00241	0.00199	0.230	-9.68E-06	0.00227	0.997	0.00467	0.0122	0.704
Secscore	-0.0550	0.0194	0.006***	-0.0503	0.0195	0.0118**	-0.0544	0.0192	0.0059***
Adj. R2	0.677			0.680			0.677		

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

Table 4.9: Number of LPs (out of the 82 selected LPs) from which one can redeem points into Amazon and iTunes in each redemption period (days), $p = 0, 5, 10, 30, 45, 60, 90$.

	N=0	N=5	N=10	N=30	N=45	N=60	N=90
Amazon	4	6	10	14	15	16	17
iTunes	3	5	9	14	14	15	16
Amazon or iTunes	5	7	11	16	17	19	20
Amazon and iTunes	2	4	8	12	12	12	13

4.5 Do the Specific Partners Affect the Damage?

4.5.1 Hypotheses Development

As we mentioned in Chapter 2, attackers seem to prefer Amazon Gift Card and iTunes Gift Code as their destinations of malicious redemptions. Taking alliances with the specific partners might expose an LP to bigger threats.

So we set the following hypothesis.

H3. An LP which takes partnership with Amazon or iTunes suffers bigger damage.

4.5.2 Data and Descriptive Statistics

Table 4.9 shows the number of LPs (out of the 82 LPs) from which one can redeem into Amazon and iTunes for each redemption period. Figure 4.4 shows the histogram of the number of LPs (from 82 selected LPs) from which one can redeem into Amazon Gift Card and iTunes Gift Code, and how it depends on the time required for redemption

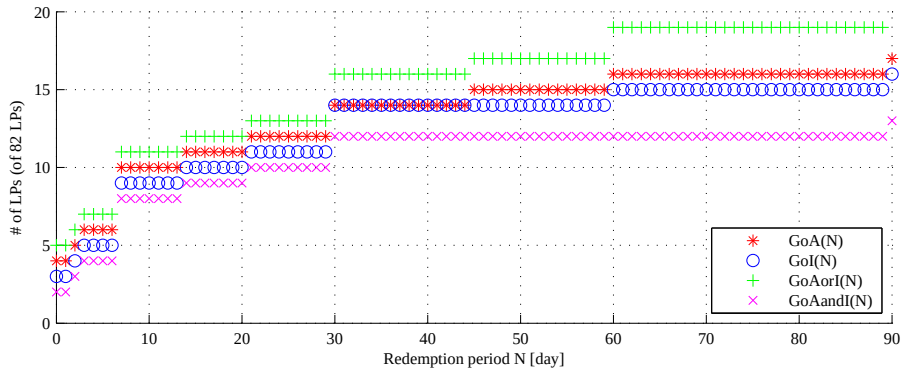


Figure 4.4: Number of LPs (of the 82 selected LPs) from which one can redeem into Amazon Gift Card or iTunes Gift Code within N days. The notations are as follows: GoA(N) is considering only Amazon, GoI(N) only iTunes, GoAorI(N) Amazon *OR* iTunes, and GoAandI(N) Amazon *AND* iTunes.

4.5.3 Model

To test *H3*, we set the linear regression model as follows:

$$\frac{\log(damage_i)}{\log(capital_i)} = \beta_0 + \beta_1 \frac{\log(expense_i)}{\log(capital_i)} + \beta_2 GoToAorI_{i,N} + \beta_3 (GoToAorI_{i,90} - GoToAorI_{i,N}) + \beta_4 sec\_score_i + u_i \quad (4.5)$$

or when N is 90,

$$\frac{\log(damage_i)}{\log(capital_i)} = \beta_0 + \beta_1 \frac{\log(expense_i)}{\log(capital_i)} + \beta_2 GoToAorI_{i,90} + \beta_3 sec\_score_i + u_i \quad (4.6)$$

where $GoToAorI_{i,p}$ is the binary value representing whether one can redeem points from LP_i to Amazon Gift Card or iTunes Gift Code within N days (1 if one can, 0 otherwise), and the other variables are the same those in Equation (4.3).

Correlations between the variables in Equation (4.5) and Equation (4.6) are shown in Table 4.10.

4.5.4 Results and Discussion

The estimated results for $N = 0, 5, 10, 30, 45, 60, 90$ are shown in Table 4.11. When N is 10, 45 and 90, β_2 is significantly positive weakly at 10% level. When N is 10 or 45, β_3 does not show any significances. This means that *H3* is weakly supported for the redemption time, 10, 45 and 90 days, and suggests that availability of redemptions into Amazon or iTunes does not affect on the damage if one has to wait more than 45 days to complete it. When N is 30 or 60, the p-values of β_2 are rather small although it is insufficient for the 10%-level weak support. On the other hand, when N is 10 or 5, β_3 is significantly positive and β_2 does not show any significances. This means if an LP takes outgoing partnership with Amazon or iTunes and the redemption takes more than 0 or 5 days, it suffers a bigger damage, while we cannot see any relations between the damage and the availability of 0 or 5-day redemption. It is also different from the intuition but almost the same discussion as in Section 4.4.4 can be applied

Table 4.10: Correlations between variables in Equations (4.5) and (4.6) for different values of N. GoAI_N represents $GoToAorI_{i,N}$ and other notations are the same as in Table 4.3

(a) $N = 0$

	ldam/lcap	lex/lcap	GoAI_0	GoAI_{90}-GoAI_0	SecScore
ldam/lcap	1.000	-	-	-	-
lex/lcap	0.790	1.000	-	-	-
GoAI_0	-0.054	-0.019	1.000	-	-
GoAI_{90}-GoAI_0	0.488	0.385	-0.126	1.000	-
SecScore	-0.491	-0.417	-0.055	-0.361	1.000

(b) $N = 5$

	ldam/lcap	lex/lcap	GoAI_5	GoAI_{90}-GoAI_5	SecScore
ldam/lcap	1.000	-	-	-	-
lex/lcap	0.790	1.000	-	-	-
GoAI_5	0.007	0.073	1.000	-	-
GoAI_{90}-GoAI_5	0.476	0.339	-0.138	1.000	-
SecScore	-0.491	-0.417	-0.149	-0.304	1.000

(c) $N = 10$

	ldam/lcap	lex/lcap	GoAI_{10}	GoAI_{90}-GoAI_{10}	SecScore
ldam/lcap	1.000	-	-	-	-
lex/lcap	0.790	1.000	-	-	-
GoAI_{10}	0.320	0.234	1.000	-	-
GoAI_{90}-GoAI_{10}	0.212	0.205	-0.144	1.000	-
SecScore	-0.491	-0.417	-0.243	-0.224	1.000

(d) $N = 30$

	ldam/lcap	lex/lcap	GoAI_{30}	GoAI_{90}-GoAI_{30}	SecScore
ldam/lcap	1.000	-	-	-	-
lex/lcap	0.790	1.000	-	-	-
GoAI_{30}	0.296	0.259	1.000	-	-
GoAI_{90}-GoAI_{30}	0.271	0.193	-0.116	1.000	-
SecScore	-0.491	-0.417	-0.243	-0.263	1.000

(e) $N = 45$

	ldam/lcap	lex/lcap	GoAI_{45}	GoAI_{90}-GoAI_{45}	SecScore
ldam/lcap	1.000	-	-	-	-
lex/lcap	0.790	1.000	-	-	-
GoAI_{45}	0.377	0.296	1.000	-	-
GoAI_{90}-GoAI_{45}	0.123	0.129	-0.104	1.000	-
SecScore	-0.491	-0.417	-0.272	-0.226	1.000

(f) $N = 60$

	ldam/lcap	lex/lcap	GoAI_{60}	GoAI_{90}-GoAI_{60}	SecScore
ldam/lcap	1.000	-	-	-	-
lex/lcap	0.790	1.000	-	-	-
GoAI_{60}	0.391	0.321	1.000	-	-
GoAI_{90}-GoAI_{60}	0.100	0.083	-0.064	1.000	-
SecScore	-0.491	-0.417	-0.329	-0.129	1.000

(g) $N = 90$

	ldam/lcap	lex/lcap	GoAI_{90}	SecScore
ldam/lcap	1.000	-	-	-
lex/lcap	0.790	1.000	-	-
GoAI_{90}	0.410	0.336	1.000	-
SecScore	-0.491	-0.417	-0.357	1.000

Thus it is suggested that if an LP has outgoing partnership with Amazon or iTunes, it suffers a bigger damage, and shorter redemption time shows some effect on the damage.

In Japan, some of the LP operators who experienced damages by malicious redemption into Amazon Gift Card or iTunes Gift Code introduced countermeasures; they either temporarily stopped alliance with Amazon and iTunes vouchers or introduced phone authentications on the redemption into Amazon, iTunes and other gift cards.[3] These recent trend is supported by the above result of our empirical analysis.

4.6 Conclusion

We revisit the empirical models used in a former study [6] regarding the security of loyalty programs. In the models, the choices of variables are inspired by the Gordon-Loeb's formulation of security investment: damage, investment, vulnerability, and threat. The liquidity of LP points corresponds to the threat in the formulation, and plays an important role in the empirical study because it particularly captures the feature of LP networks. However, the actual proxy used in the former study is artificial due to the fact that its original definition is not LP-wise but industry-wise. In this chapter, we reconsidered the

[3] ANA temporarily stopped alliance with iTunes from Mar. 10th, 2014 to Dec. 10th, 2014 (`https://www.ana.co.jp/topics/itunes140818/index.html`). JAL has stopped alliance with Amazon till Oct. 2015) (`http://www.jal.co.jp/info/jmb/140924.html`). G-point added phone authentications regarding the redemption into Amazon, iTunes and some other gift cards.(`http://www.gpoint.co.jp/aboutg/authentication/`.)

Table 4.11: Results of linear regression by Equations (4.5) and (4.6) for $N = 0, 5, 10, 30, 45, 60, 90$. The notations are the same as in Table 4.10.

	N = 0			N = 5			N = 10		
Variable	Coef.	Std.Err	Prob.	Coef.	Std. Err	Prob.	Coef.	Std. Err	Prob.
C	-0.179	0.0930	0.0585*	-0.179	0.0910	0.053*	-0.205	0.0936	0.0318**
Expense	1.05	0.120	0***	1.05	0.117	0***	1.09	0.121	0***
$GoAI_N$	-0.0120	0.0284	0.674	-0.0137	0.0244	0.575	0.0389	0.0215	0.0749*
$GoAI_{90}$-$GoAI_N$	0.0468	0.0196	0.0197**	0.0557	0.0200	0.0067***	0.018	0.0233	0.441
Secscore	-0.0405	0.0196	0.0425**	-0.0423	0.0192	0.0311**	-0.0428	0.0199	0.0351**
Adj. R2	0.682			0.693			0.670		

	N = 30			N = 45			N = 60		
Variable	Coef.	Std.Err	Prob.	Coef.	Std. Err	Prob.	Coef.	Std. Err	Prob.
C	-0.20475	0.093583	0.0318**	-0.20268	0.093735	0.0338**	-0.20522	0.093981	0.0322**
Expense	1.088361	0.120664	0***	1.088246	0.120784	0***	1.090464	0.121144	0***
$GoAI_N$	0.024727	0.018525	0.186	0.033147	0.018296	0.0741*	0.029541	0.017817	0.1016
$GoAI_{90}$-$GoAI_N$	0.052302	0.033744	0.1254	0.005776	0.038032	0.8797	0.028243	0.063396	0.6573
Secscore	-0.0407	0.020094	0.0465**	-0.04441	0.020098	0.0302**	-0.04273	0.020056	0.0365**
Adj. R2	0.671			0.670			0.668		

	N = 90		
Variable	Coef.	Std.Err	Prob.
C	-0.205	0.0933	0.031**
Expense	1.09	0.120	0***
$GoAI_N$	0.0295	0.0175	0.0958*
Secscore	-0.0427	0.0199	0.035**
Adj. R2	0.668		

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

liquidity definition based on a further observation of LP security incidents. By using newly defined proxies corresponding to the threat as well as other refined proxies, we conducted hypotheses testing to derive more implications. We show the damage from LP incidents gets bigger if outgoing partnerships with rather short redemption time are taken, and if partnerships with Amazon or iTunes are taken.

These derived implications will help LP operators to manage partnerships. In fact, these findings are consistent with recent changes in the LP network. Thus we can see the impacts of security investment models include a wider range of empirical studies in the economics of information security.

Chapter 5

Threat Investigation using Logistic Regression and Network Analysis

5.1 Introduction

Chapter 4 uses the linear regression models which are constructed inspired by Gordon-Loeb's security investment model. In order to conduct quantitative empirical analyses with those models, we use the data on each business sector as the proxies of *damage* and *security investment*. However, this point somewhat leaves suspicions on the robustness of the derived implications because the real data which reflect the actual damage from LP security incidents are not used.

While there is no efficient data about the stolen amount of points, we can get web news data which reported LP incidents, which are shown in Chapter 2. Since the data sources are only the web news articles, the data may be incomplete or biased. There is a trade-off in the empirical data, where the reliable data from the large scale statistics don't include the LP specific data, but the non-reliable biased data include the LP specific one.

However, the binary value which indicates whether the LP is reported to be attacked can represents the magnitude of threat on the LP. So, in this chapter, we try to conduct quantitative analysis using this binary data on logistic regression model. This will lead to deeper understandings about the threat on LP.

5.1.1 Chapter Organization

The rest of this chapter is organized as follows. In Section 5.2, we show the hypothesis development, methods, and results of the logistic regression analysis using the LP incidents data and each network centrality value, and consequently get centrality-threat implications. In Section 5.3, we conclude this chapter.

5.2 Network Centrality and Threat

5.2.1 Hypothesis Development

Social network analyses on Japanese LPs have been conducted from the management area as described in Section 3.1. This method can be applied when we consider security issues.

It may derive more general understanding on the relationship between LP network and security.

Among some metrics of network analyses, *network centrality* represents the importance of a node. The most popular centrality metrics are *Degree centrality*, *Betweenness centrality* and *Closeness centrality*.

Degree centrality is defined as the number of links incident upon a node (i.e., the number of ties that a node has). The degree can be interpreted in terms of the immediate risk of a node for catching whatever is flowing through the network. The degree centrality of vertex v, for a given graph $G \equiv (V, E)$ with $|V|$ vertices and $|E|$ edges, is defined as

$$C_D(v) = \deg(v).$$

In the case of a directed network, we usually define two separate measures of degree centrality, namely indegree and outdegree. Indegree is a count of the number of ties directed to the node and outdegree is the number of ties directed to others.

Closeness centrality is calculated to be higher if the distances to other vertices are shorter. In connected graphs there is a natural distance metric between all pairs of nodes, defined by the length of their shortest paths. The farness of a node x is defines as the sum of its distances from all other nodes, and its closeness is defined as the reciprocal of the farness, that is:

$$C_C(v) = \frac{1}{\sum_{u \neq v \in V} d(u, v)}.$$

Betweenness centrality is a centrality measure of a vertex within a graph. Betweenness centrality quantifies the number of times a node acts as a bridge along the shortest path between two other nodes. This is calculated as:

$$C_B(v) = \sum_{s \neq v \neq t \in V} \frac{\sigma_{st}(v)}{\sigma_{st}}$$

where σ_{st} is total number of shortest paths from node s to node t and $\sigma_{st}(v)$ is the number of those paths that pass through v.

We put an assumption of the attackers behavior as shown in Figure 5.1. First, an LP with high centrality will have high chances to scale the profit, that is, it will get more members and points. Second, since attackers will be more likely to attack an LP if the expected value from the attack gets bigger, an LP with more members or points has higher probability to be chosen as a target by them. From these assumption, it is inferred that if malicious people attack an LP with higher centrality, the expected value will get bigger, which leads to the bigger threat.

From the above discussion, we set the following hypothesis:

H4. An LP with higher centrality in point exchange network are exposed to bigger threat.

5.2.2 Data and Descriptive Statistics

The data used for the analysis were as follows:

- Point exchange network retrieved from Poitan on September 2014.
- Survey of Japanese LP incidents from web news, which is shown in Chapter 2.

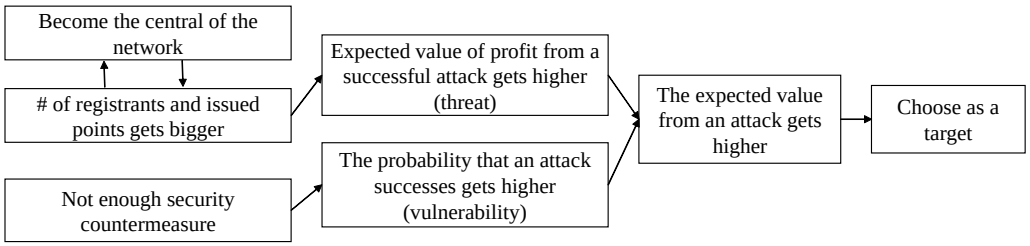


Figure 5.1: Process of how attackers choose an LP as the target.

5.2.3 Model

To test *H3*, the following logistic regression model is set:

$$attacked_i = \frac{1}{1 + e^{-(\beta_0 + \beta_1 centrality_i + \epsilon)}} \tag{5.1}$$

where $i = 1, 2, ..., 239$ denotes the index of each LP, $attacked_i$ is the probability that LP_i is attacked, and $centrality_i$ is the centrality of LP_i.

5.2.4 Results

The estimated results of Equation (5.1) for each centrality metric are as in Table 5.2. Figure 5.2 show the plots of the estimation and the real data. When the centrality is set as a *degree* or *betweeness* one, a coefficient is significantly positive and hence *H1* is supported. On the other hand, in the case of *closeness* centrality, it does not show any significances.

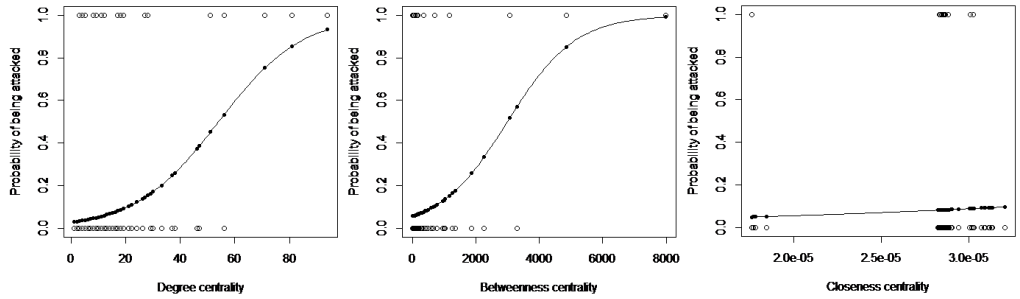


Figure 5.2: Estimated results of the logistic regression on Equation (5.1) for each centrality metric.

5.2.5 Discussion

Degree Centrality

Degree centrality indicates the number of the outgoing partner. This results are consistent with previous work [6] and Chapter 4.

Table 5.1: The estimation results of logistic regression in Equation (5.1).

	Estimate	p-value
(Intercept)	-3.53242	<2.00E-16***
degree	0.06545	1.25E-05***

	Estimate	p-value
(Intercept)	-2.8016213	<2.00E-16***
betweenness	0.000937	0.00279**

	Estimate	p-value
(Intercept)	-3.816	0.013*
closeness	49568.868	0.381

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

Centrality and Popularity

In Section 5.2.1, we set the assumptions that an LP's centrality and popularity interact each other. Let us consider the following linear regression model:

$$member_i = \beta_0 + \beta_1 centrality_i + \epsilon$$

where $member_i$ is the number of members who registered the LP_i's account at Poitan, and $centrality_i$ is the centrality of LP_i. The estimation results of this regression for *centrality* as degree and betweenness one are as in Table 5.2. In both cases, the p-values are sufficiently low and the coefficients are positive. That means that the above assumption was supported quantitatively. This suggests that the process in Figure 5.1 is reasonable one.

Table 5.2: Centrality and the number of LPs.

	Estimate	p-value
(Intercept)	-607.24	0.0139*
degree	215.47	<2e-16***
Adj. R2	0.4756	

	Estimate	p-value
(Intercept)	1131.5442	6.12E-07***
betweenness	3.2557	<2.00E-16***
Adj. R2	0.3269	

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

5.3 Conclusion

In this chapter, we use the real data about LP incidents instead of the sector data used in Chapter 4, and conduct a quantitative analysis with assumptions that this approach consequently leads to deeper understandings of the threat on LPs. We also applied social network analyses to the LP security incidents, as the methods have been used in the management and economic context for studying the characteristics of the LP network.

We considered the attackers behavior of choosing target LPs and suppose that network centrality can be a *threat* metric. Then, it is supported by logistic regression analyses that if an LP has higher degree or betweenness centrality, it is more likely to be attacked.

Our contribution is as follows: the network analysis was first applied to the LP security incidents analysis and the threat was more investigated in a more general perspectives; we first used as a damage proxy the binary variable which indicates if the LP was attacked or not (not the industry-wise variable provided by METI,) and showed more robust implications for threat using logistic regression analysis.

Chapter 6

Theoretical Analyses on the Security of Loyalty Programs

6.1 Introduction

In Chapter 4 and Chapter 5, we conduct empirical analyses. These results provide fruitful implications, but they only tell us that higher liquidity leads to bigger damage and we should lower liquidity for security. There should be a trade-off between security and profit for the operator but we cannot see any relations via the shown empirical analyses.

So, in this chapter, we will try to economically construct a model of LP security and profit, and examine if there is a trade-off between them. In order to make discussion easier, we construct a quite simple model.

6.1.1 Chapter Organization

In Section 6.2, we describe the model construction regarding the firm's profit, effects of introducing LPs, and the security of LPs. In Section 6.3, some numerical examples about the model are shown to see the optimization problem. Finally we conclude this chapter in Section 6.4.

6.2 Economic Model of LP-operating Firm's Profit

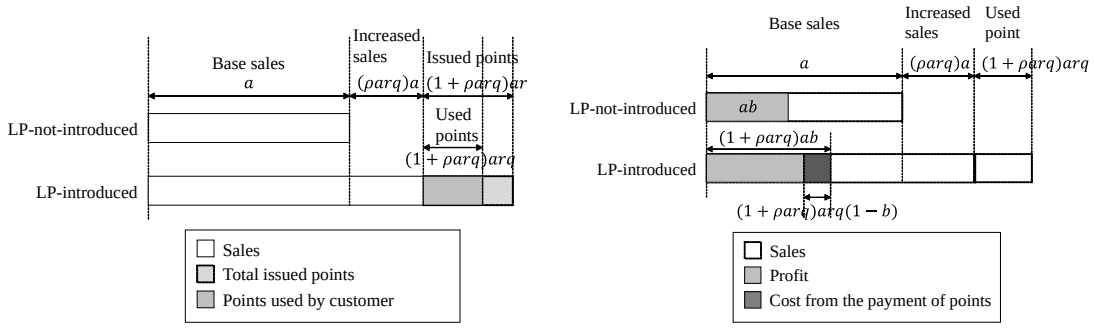
We construct one firm's profit model.

6.2.1 Sales and Loyalty Reword Rate

Let a the sales value which was got when LP is not introduced, and b the profit rate. Then we get the profit of the firm without LP,

$$Profit_{\mathrm{noLP}} = ab$$

Next, we consider LP introduction effect. Let r the point rate per sale, q the point liquidity, and ρ the productivity of LP productivity. The point rate $r(0 \leq r \leq 1)$ means how much points an operator gives to a customer when he buy 1 unit of money. The point liquidity $q(0 \leq q \leq 1)$ indicates the ratio of used points to issued points. LP productivity



(a) Sales and points issue.

(b) Profit regarding used points.

Figure 6.1: Sales and profit of a firm in both LP not-introduced and introduced case.

$\rho(\rho > 0)$[1] indicates how much effect an LP has on sale increase. We define ρ as the ratio of the growth rate to the amount of used points arq. The Figure 6.1 graphically shows the amount of sales and points in both LP-introduced and LP-not-introduced cases. Then, without considering any attacks, we get the profit as follows:

$$\begin{aligned} Profit_{\text{withLP,noAttack}} &= (1+\rho arq)ab - (1+\rho arq)arq(1-b) \\ &= (1+\rho arq)a(b - rq(1-b)). \end{aligned} \tag{6.1}$$

6.2.2 Thieves of Loyalty Programs Points

If a firm issues points, attackers have chances to get monetary benefit by thieving points. So let we consider the expected value of points which will be stolen. As the same as in [7] and [9], let v the vulnerability of an LP system today, t the threat on LP system today, α the productivity of security investment on vulnerability reduction, and β the productivity of security investment on threat reduction. Then let $V(v, z)$ the vulnerability after security investment, and $T(t, z, q)$ the threat after security investment and LP liquidity changes. All of the parameters are shown in Table 6.1.

We set $t = q$ as we consider the liquidity as threat.

Using Gordon and Loeb's Class-II functions, which is the only one that has a empirically support, we set V and T as follows:

$$V(v, z) = v^{1+\alpha z} \tag{6.2}$$

$$T(t, z, q) = qt^{1+\beta z} \tag{6.3}$$

This model construction is almost the same as in Matsuura's model [9] with one only difference, the multiplier q in $T(t, z, q)$.

Using these parameters, we revise $Profit_{\text{withLP,noAttack}}$ regarding the expectation loss from attacks as follows:

$$\begin{aligned} Profit_{\text{withLP,withAttack}} &= (1+\rho arq)a(b - rq(1-b)) \\ &\quad -V(v, z)T(t, z, q)(1+\rho arq)ar - z. \end{aligned} \tag{6.4}$$

[1] There are several researches which support the effectiveness of LP such as [65], so we set $\rho > 0$.

Table 6.1: Parameters used in our model.

Parameter	Scope	Unit	Definition
a	$a > 0$	JPY	sales value when LP is not introduced
b		JPY	the ratio of profit to sales
r	$0 < r < 1$		the ratio of issued points to sales
q	$0 \leq q \leq 1$		liquidity; the ratio of used points to issued points
z	$z \geq 0$	JPY	security investment
v	$0 \leq v \leq 1$		vulnerability; the probability that the attack successes on the condition an attack occurred
t	$0 \leq t \leq q$		threat; the probability that an attack occurs
α	$\alpha > 0$	/JPY	Productivity of security investment on vulnerability reduction
β	$\beta > 0$	/JPY	Productivity of security investment on threat reduction
ρ	$\rho > 0$	/JPY	Productivity of LP on sales

We want to maximize $Profit_{\text{withLP,withAttack}}$ regarding q and z.

$$\begin{aligned} Profit_{\text{withLP,withAttack}} &= (1+\rho arq)a(b - rq(1-b)) \\ &\quad -V(v,z)T(t,z,q)(1+\rho arq)ar - z. \\ &\quad \rightarrow \text{Max.} \end{aligned} \tag{6.5}$$

6.3 Numerical Examples

We show some numerical examples of this model.

Figure 6.2 shows some cases with the changes of ρ and r. We can see the following things.

- When the productivity of LP, ρ, is low, it is better if the firm doesn't introduce LP.
- When the productivity of LP, ρ, is high, optimized q and z are as the following.
  - When the ratio of issued points to sale, r, is high and there is much issued points, you have to reduce the liquidity and invest somewhat on security.
  - When the ratio of issued points to sale, r, is middle, you don't have to reduce the liquidity but invest somewhat on security.
  - When the ratio of issued points to sale, r, is sufficiently low and issued points are less, you don't have either to reduce the liquidity or to invest somewhat on security.

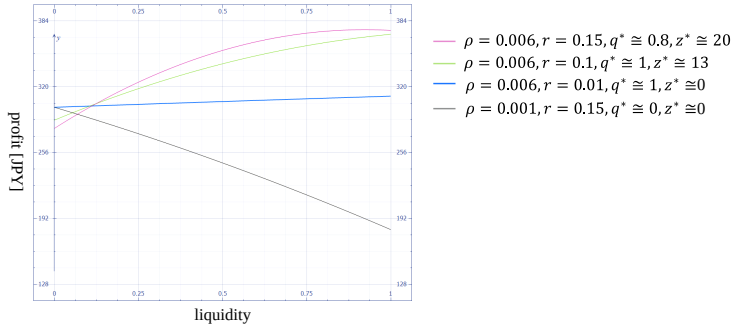


Figure 6.2: An example of profit changes with respect to point liquidity. We set each parameter as follows: $a = 1000; b = 0.3; v = 0.5; t = 0.5; \alpha = 0.01; \beta = 0.01;$

6.4 Conclusion

In this chapter, we introduced theoretical optimization model of a firm's profit regarding LP and its security. If issued points are few, it is optimal in maximum liquidity and zero security investment. If issued points are much, it is optimal in somewhat lower liquidity and some security investment. We confirm that there is a trade-off between profit and security. It is implied that it is not always the case that the operators have to reduce the points liquidity for security. Some operators with middle issued points just should invest somewhat on security.

These findings are also consistent with the real LP operators' countermeasures. While mileage programs with large issued miles had been stopped the alliance with Amazon (in another words, lower the points liquidity), the middle class point program just applied a phone authentication on the redemption.[2]

[2]See Section 4.5.4.

Chapter 7

Conclusion

In this thesis, based on a fundamental motivation to find a robust threat metric through the LP security analysis, we showed the results of empirical. Also, we confirmed that there is a trade-off between profit and threat reduction through a theoretical analysis. In the following, we summarize the contributions of this thesis, and conclude this thesis with future directions.

7.1 Summary of Contributions

Firstly, we revisit the empirical models used in a former study [6] regarding the security of LPs. In the models, the choices of variables are inspired by the Gordon-Loeb's formulation of security investment: damage, investment, vulnerability, and threat. The liquidity of LP points corresponds to the threat in the formulation, and plays an important role in the empirical study because it particularly captures the feature of LP networks. However, the actual proxy used in the former study is artificial due to the fact that its original definition is not LP-wise but industry-wise. In this thesis, we reconsidered the liquidity definition based on a further observation of LP security incidents. By using newly defined proxies corresponding to the threat as well as other refined proxies, we conducted hypotheses testing to derive more implications. It is suggested that the damage from LP incidents gets bigger if outgoing partnerships with rather short redemption time are taken, and if partnerships with Amazon or iTunes are taken.

These derived implications will help LP operators to manage partnerships. In fact, these findings are consistent with the recent changes in the LP network. Thus we can see the impacts of security investment models include a wider range of empirical studies in the economics of information security.

Secondly, we further investigate the threat with a logistic regression model using the data of .the actual incidents. We also apply social network analysis methods and get an implications from a more general perspective: if an LP has higher betweenness or degree centrality, the probability that the LP will be attacked gets higher.

Thirdly, we introduced economic model about LP security and solve the optimization problem. Although the model was quite a simple one, we can see the trade-off between profit and security.

7.2 Future Prospects

Our findings about the threat on LPs will practically be helpful when LP operators decide to how to manage the LP partnership and security investment. In addition to that, our work will also inspire to other virtual currencies or electric payment research. Virtual currencies such as Bitcoin or game currencies are also frequently theft. Online banking is quite well abused and legitimate users' assets are stolen every day. The higher liquidity of these services reduces costs, provides great utility and profit with not only the customers but also the operators, and improves efficiency of the whole economy. However, the security risk is also raised as the liquidity is raised. Likewise our study, the interesting implications may be retrieved if you conduct empirical studies considering Gordon-Loeb model focusing on the threat on them.

Bibliography

[1] B. Sharp, and A. Sharp. Loyalty Programs and their Impact on Repeat-Purchase Loyalty Patterns. *International journal of Research in Marketing*, 14(5)473–486, 1997.

[2] PricewaterhouseCoopers LLP. Loyalty Analytics Exposed: What Every Program Manager Needs to Know. `http://www.pwc.com/en_US/us/insurance/publications/assets/pwc-loyalty-analytics -exposed.pdf`, 2013.

[3] J. Zhang and E. Breugelmans. The Impact of an Item-based Loyalty Program on Consumer Purchase Behavior. *Journal of Marketing research*, 49(1):50–65, 2012.

[4] S. Katsumata and T. Wakabayashi. Loyalty Program Point Exchange Networks and their Impact on Marketing Performance. *Faculty of Economics, Nagasaki University Discussion paper series*, 2014(6):1–19, 2014.

[5] European Central Bank. Virtual Currency Schemes. `http://www.ecb.europa.eu/pub/pdf/other/virt ualcurrencyschemes201210en.pdf`, 2012.

[6] B. Jenjarrussakul and K. Matsuura. Analysis of Japanese Loyalty Programs Considering Liquidity, Security Efforts, and Actual Security Levels. *The 13th Workshop on the Economics of Information Security*, 2014.

[7] L. A. Gordon and M. P. Loeb. The Economics of Information Security Investment. *ACM Transactions on Information and System Security (TISSEC)*, 5(4):438–457, 2002.

[8] J. Willemson. On the Gordon & Loeb Model for Information Security Investment. *The 5th Workshop on the Economics of Information Security*, 2006.

[9] K. Matsuura. Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model. *The 7th Workshop on the Economics of Information Security*, 2008.

[10] DarkReading.com. British Airways The Latest Loyalty Program Breach Victim. `http://www.darkreading.com/attacks-breaches/british-airways-the-latest-loyalty-progra m-breach-victim/d/d-id/1319683`, 2015.

[11] Krebs on Security. Thieves Cash Out Rewards, Points Accounts. `http://krebsonsecurity.com/2014/11/thieves-cash-out-rewards-points-accounts/`, 2014.

[12] The Dallas Morning News. Cyberthieves Steal Miles from American, United Customers. http://www.dallasnews.com/business/airline-industry/20150112-american-united-airlines-targets-of-attempt-to-steal-customers-miles.ece, 2015.

[13] My Bank Tracker. Lesson From Starbucks: Creative Ways That Hackers Can Steal From You. http://www.mybanktracker.com/news/lesson-starbucks-creative-ways-hackers-steal, 2015.

[14] TrendMicro. TrendLabs 2Q 2014 Security Roundup in Japan (in Japanese). http://www.trendmicro.co.jp/cloud-content/jp/pdfs/security-intelligence/threat-report /pdf-2014q2-20140819.pdf?cm_sp=threat-_-sr-2014q2-_-lp-txt, 2014.

[15] G-PLAN INC. Correspondence to the Unauthorized Accesses to G-Point (in Japanese). http://www.gpoint.co.jp/company/service/gplan20120418.pdf, 2012.

[16] ITmedia Enterprise. Unauthorized Access to T-point, 299 Accounts were Compromised (in Japanese). http://www.itmedia.co.jp/enterprise/articles/1304/07/news005.html, 2013.

[17] Record China. Chinese Students were Arrested. They Exchanged 250 Accounts Rakuten Points into Electric Money (in Japanese). http://www.recordchina.co.jp/a80323.html, 2013.

[18] NTT Communications Online Marketing Solutions. The report of Unauthorized Access to Potora (in Japanese). http://www.nttcoms.com/page.jsp?id=2409, 2014.

[19] ITpro. Unauthorized Access to JAL Mileage Website, JAL Requested 27 Million People to Change their Passwords (in Japanese). http://itpro.nikkeibp.co.jp/article/NEWS/20140203/534282/, 2014.

[20] Nikkei. Enormous Unauthorized Access Attempted to JR East (in Japanese). http://itpro.nikkeibp.co.jp/atcl/news/14/081800465/, 2014.

[21] Hatena Co., Ltd. Please Confirm your Password and Registration Information in order to Prevent Unauthorized Access (in Japanese). http://hatena.g.hatena.ne.jp/hatena/20140224/1393211701, 2014.

[22] ITpro. 1.12 Million Miles of ANA Mileage Club were Stolen, Personal Information such as Addresses Might be Browsed (in Japanese). http://itpro.nikkeibp.co.jp/article/NEWS/20140311/542563/, 2014.

[23] Poitan News. Unauthorized Access to My JCB and Redeemed to T-point (in Japanese). http://www.poitan.jp/archives/3138, 2014.

[24] Sony Marketing (Japan) Inc. The Report of Unauthorized Access to Sony Point Service and a Request for Changing Passwords (in Japanese). https://www.sony.jp/info/pw_management2.html, 2014.

[25] Security NEXT. 0.22 Million Unauthorized Accesses to Niconico Video, 0.17 Million Yen Loss (in Japanese). http://www.security-next.com/049575, 2014.

[26] Security NEXT. Unauthorized Access to Hatena, Redemption to Amazon Gift Code was Failed in Attempts (in Japanese). http://www.security-next.com/049827, 2014.

[27] Security NEXT. 11502 Unauthorized Accesses to a Questionnaire Website and some Points were Stolen (in Japanese). http://www.security-next.com/049982, 2014.

[28] Scan Net Security. A Questionnaire Website, Anpara, was Attacked and some Points were Stolen (in Japanese). http://scan.netsecurity.ne.jp/article/2014/07/08/34495.html, 2014.

[29] NTT Communications Corporation. Unauthorized Access to Poin-talk and goo-points (in Japanese). http://www.ntt.com/release/monthNEWS/detail/20140730.html, 2014.

[30] ITpro. Enormous Number of Accesses to Suica Point Club, Unauthorized Access to Some Acounts (in Japanese). http://itpro.nikkeibp.co.jp/atcl/news/14/081800465/, 2014.

[31] D Style Web. Information of Unauthorized Access and Unauthorized Point Redemption (in Japanese). http://www.dstyleweb.com/20141028/, 2014.

[32] Security NEXT. Unauthorized Access to a Research Service of Kyushu Electric Power, which was Detected when the Operator Found the Number of Exchanges is 10 Times as Many as Usual (in Japanese). http://www.security-next.com/054803, 2014.

[33] mixi, Inc. The Report of Unauthorized Accesses to Morappo and mixi Questionnaire Using the Passwords which were Leaked at the Third Party (in Japanese). http://mixi.co.jp/press/2015/0109/15881/, 2015.

[34] AIP Corporation. Unauthorized Access, Point Redemption and Personal Information Browsing (in Japanese). http://www.aip-global.com/JP/corporate/releases/20150701.html, 2015.

[35] Lifemedia, Inc. The Report of Unauthorized Access to Lifemedia (in Japanese). http://lifemedia.jp/utilization/info_d20150713.html, 2015.

[36] Orient Corporation. Unauthorized Access to Customer Web Services (in Japanese). http://www.orico.co.jp/information/20150727.html, 2015.

[37] PrizePrize. The Report of Unauthorized Point Redemptions and our Request for Changing your Passwords (in Japanese). http://www.moneyforall.net/rss/single.php?id=121, 2015.

[38] Washington Hotel. The Report of Unauthorized Access to Lodging Net Point and our Request for Changing your Password (in Japanese). http://www.washingtonhotel.co.jp/pdf/info20150805.pdf, 2015.

[39] T. Wakabayashi. Structure and Formation of the Exchange Market of Point Programs and Electronic Moneys (in Japanese). *Organizational Science*, 42(2):47–60, 2008.

[40] T. Wakabayashi and S. Katsumata. Which Factor Matters to the Formation of Strategic Alliance Network: Industry, Firm or Network? (in Japanese). *Oganizational Science*, 47(1):69–79, 2013.

[41] H. Yuhashi and H. Gotou. The Reliability of the New Economic Platform: "Mobile Value Exchange Alliance Network." *18th Biennial ITS Conference*, 2010.

[42] T. Moore and N. Christin. Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk. In *Financial Cryptography and Data Security, Lecture Notes in Computer Science Volume 7859*, pages 25-33, 2013.

[43] M. Vasek, M. Thornton and T. Moore. Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem. In *Financial Cryptography and Data Security, Lecture Notes in Computer Science Volume 8438*, pages 57-71, 2014.

[44] B. Johnson, A. Laszka, J. Grossklags, M. Vasek and T. Moore. Game-Theoretic Analysis of DDoS Attacks against Bitcoin Mining Pools. In *Financial Cryptography and Data Security, Lecture Notes in Computer Science Volume 8438*, pages 72-86, 2014.

[45] J. A. Kroll, I. C. Davey and E. W., Felten. The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. *The 12th Workshop on the Economics of Information Security*, 2013.

[46] J. Hu and F. Zambetta. Security Issues in Massive Online Games. *Security and Communication Networks*, 1(1):83–92, 2008.

[47] Y. Ku, Y. Chen, K. Wu and C. Chiu. An Empirical Analysis of Online Gaming Crime Characteristics from 2002 to 2004. *Intelligence and Security Informatics, Lecture Notes in Computer Science Volume 4430*, pages 34-45, 2007.

[48] J. Bardzell, M. Jakobsson, S. Bardzell, T. Pace, W. Odom and A. Houssian. Virtual Worlds and Fraud: Approaching Cybersecurity in Massively Multiplayer Online Games. In *Proceedings of DiGRA 2007 Conference*, pages 451-742, 2007.

[49] C. Kiondo, S. Kowalski and L. Yngström Exploring Security Risks in Virtual Economies. *1st International Conference on Social Eco-Informatics*, 2011.

[50] A. S. M. Irwin, and J. Slay. Detecting Money Laundering and Terrorism Financing Activity in Second Life and World of Warcraft. In *Proceedings of the 1st International Cyber Resilience Conference*, pages 41-50, 2010.

[51] Ministry of Economy, Trade and Industry. Survey on Information Processing in 2012: Result Detail Part 3 - Information Security (in Japanese). `http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/h24jyojitsu.html`, 2013.

[52] Ministry of Economy, Trade and Industry. Survey on information processing in 2012: Questionnaire (in Japanese). http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/pdf/03_H24chousahyo.pd f, 2012.

[53] B. Jenjarrussakul and K. Matsuura. Another Class of Function for the Productivity Space of Information Security Investment. *The 30th Symposium on Cryptography and Information Security*, 2013.

[54] The Economist. Frequent-Flyer Miles: In terminal Decline?. *The Economist*, 2005.

[55] J. Berry. Bulking Up: The 2013 Colloqui Loyalty Census. Growth and Trends in U. S. Loyalty Program Activity. *COLLOQUI talk*, 2013.

[56] J. Berry Bulking up: The 2013 Colloqui Loyalty Census. Growth and Trends in Canadian Loyalty Program Activity. *COLLOQUI talk*, 2013.

[57] Y. Okada How to Make Successful Loyalty Reward Services (in Japanese). WAVE Press, 2010.

[58] Nomura Research Institute, Ltd. Marketing with Enterprises' Currency (in Japanese). TOYO KEIZAI INC., 2008.

[59] Nomura Research Institute, Ltd. The annual issued point and mileage will amount to 1 trillion JPY in 2020 (in Japanese). http://www.nri.com/~/media/PDF/jp/news/2015/150910_1.pdf, 2015.

[60] S. Lim. Visualization of Frequent Flier Program Network between Airline Companies and Related Services in Korea and Japan (in Japanese). In *Proceedings of the the 2012 Meeting of The Society of Socio-Informatics*, pages 131-134, 2012.

[61] M. Enzmann, M and M. Schneider. Improving customer retention in e-commerce through a secure and privacy-enhanced loyalty system. , *Information Systems Frontiers*, 7(4-5):359–370, 2005.

[62] O. Thonnard, L. Bilge, A. Kashyap and M. Lee. Are you at risk? Profiling organizations and individuals subject to targeted attacks. *Financial Cryptography and Data Security*, 2015.

[63] A. Sarabi, P. Naghizadeh, Y. Liu, and M. Liu. Prioritizing Security Spending: A Quantitative Analysis of Risk Distributions for Different Business Profiles. *The 14 th Workshop on the Economics of Information Security*, 2015.

[64] Symantec Corporation. The 2015 Internet Security Threat Report. https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf, 2015.

[65] Y. Liu. The long-term impact of loyalty programs on consumer purchase behavior and loyalty. *Journal of Marketing*, 71(4):19–35, 2007.

[66] R. B'ohme. Security metrics and security investment models. In *Advances in Information and Computer Security*, pages 10-24, 2010.

List of Publications

Refereed Papers

[1] S. Shinoda, and K. Matsuura. Empirical Investigation of Threats to Loyalty Programs by Using Models Inspired by the Gordon-Loeb's Formulation of Security Investment. *Journal of Information Security*, in Press.

Non-Refereed Papers

[2] S. Shinoda, and K. Matsuura. Investigating Liquidity Definition of Loyalty Program Points for Security Incident Impact Analysis (in Japanese). *The 32nd Symposium on Cryptography and Information Security*, 2015.

[3] S. Shinoda, and K. Matsuura. Proposal of Policy Making for Designing Loyalty Program through Empirical Analysis on Security Incidents (in Japanese). *29th Japan Society of Security Management Symposium*, 2015.

[4] S. Shinoda, and K. Matsuura. A Study on Loyalty Program Security with Network Analysis Metrics (in Japanese). *Computer Security Symposium 2015*, 2015.

Appendix A

Related Web Services to the Point Redemption

A.1 Poitan.net

As introduced in [6], Poitan.net is an LP information website (`http://www.poitan.net`). Poitan means "Point Exploration Club" in Japanese

At Poitan, information of more than 200 LPs in Japan is provided, 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 some possible conversion routes. For example, on December 25, 2015, Poitan said there were 87 possible, and showed each top 7 routes in order of output points, estimated period, and number of redemption times. One of the possible routes with the best rate was as follows:

1. By redeeming at ANA's website, one can convert 20,000 ANA miles (estimated value is 30,000JPY (Japanese Yen)) into 20,000 JQ Card Points[1] points (estimated value is 20,000JPY) This would take about 60 days.

2. Likewise, at JQ Card Point website, one can convert 20,000 points into 20,000 Epos Card Points[2] (estimated value is 20,000JPY). This would take about 3 days.

3. 20,000 Epos Card Points can be converted into 10,000 JAL miles (estimated value is 10,000JPY). This would take about 60 day.

A.2 Points.com

Although Poitan.net is a Japanese service, there is a similar service also in the U.S., Points.com (`http://www. points.com`). One can track, exchange or redeem his/her points via Points.com, unlike Poitan.net provides just exchange route search and points tracking

[1] JQ Card Point is a reward program of a credit card provided by a Japanese railway company.

[2] Epos Card Point is a reward program of a credit card provided by one of the biggest department store in Japan, Marui.

services. For example, you can redeem American Airlines' aadvantage miles to some gift cards. One possible redemption is, for example, 6,412 miles to 25 USD, 12,294 miles to 50 USD and 24,508 miles to 100 USD gift card of Toys"R"Us.

Appendix B

Data and Proxies for Empirical Analyses

In this Appendix we give the detail information of the data and proxies calculations used for our empirical analyses, showing what differs from [6].

B.1 82 Selected LPs

Table B.1 and Table B.2 show the 82 selected LPs. *LP ID* indicates the LP's ID of Poitan.net. You can access the information of an LP via `http://dir.poitan.net/(.*).html`, where (.*) is its ID number.

Table B.1: List of the 82 selected LPs (Part 1). LP ID indicates registered ID at Poitan, Industry ID indicates each industry (details are in Appendix B.1 and Appendix B.2), and Capital size is each LP operator's capital size. Security score shows a security requirement level calculated by the methods described at Appendix B.3.3. N/A means that we cannot access the corresponding information.

LP ID	Name of LP	Industry ID	Capital size (JPY)	Security score
1	JAL Mileage bank	20	355,845,000,000	0.667
2	ANA Mileage club	20	25,000,000,000	0.667
15	Mitsui Sumitomo card	23	34,030,000,000	0.667
29	G-Point	19	296,000,000	0.333
30	Net Mile	19	N/A	0.000
31	J-Point (changed to "My green stamp")	19	100,000,000	0.167
32	Outlet Point	26	1,527,000,000	0.500
34	Biccamera	22	18,402,380,000	0.167
36	Rakuten	19	1,095,300,000	0.000
38	Cecile	22	2,000,000,000	0.167
39	Belle Maison	22	20,359,000,000	0.167
42	Amazon Gift Voucher	22	N/A	0.000
43	T Point	19	100,000,000	0.333
44	Jbook	22	4,340,000,000	0.000
45	Honto	22	4,340,000,000	0.000
46	NTT Docomo	17	949,679,500,000	1.000
47	au	17	141,851,000,000	1.000
48	NTT communication	17	211,700,000,000	1.000
62	Ponta	26	2,381,578,000	0.500
63	Mitsubishi Tokyo UFJ Bank	23	1,711,900,000,000	0.667
66	Manex Stock Company	23	12,200,000,000	0.833
70	Starbucks Card	22	8,548,090,000	0.333
71	Matsumoto Kiyoshi	22	21,086,000,000	0.500
74	Rakuten Edy	19	1,840,000,000	1.000
78	Risona Bank	23	50,400,000,000	1.000
81	Yamada Denki	22	71,050,000,000	0.000
92	Recruit	26	10,000,000,000	0.000
97	Sony Finance	19	N/A	1.000
98	Sony point	9	100,000,000	0.167
100	Daiwa Stock Company	23	100,000,000,000	1.000
101	Circle K Sunkus	22	8,380,400,000	0.000
103	Chobi Rich	26	65,700,000	0.167
110	ANA JCB Card	23	10,616,100,000	0.800
123	Sofmap	22	100,000,000	0.167
126	Bidders	19	10,397,000,000	0.167
127	Softbank Mobile	17	177,251,000,000	0.600
131	Web Money	19	495,784,000	1.000
133	Icoca	20	100,000,000,000	0.667
134	J-WEST Card	20	100,000,000,000	0.667
138	Times	26	8,219,000,000	0.167
146	PeX	19	198,000,000	0.167

Table B.2: Selected 82 LPs (Part 2). The explanation of each value is the same as Table B.1.

LP ID	Name of LP	Industry ID	Capital size (JPY)	Security score
148	nanaco	23	7,500,000,000	0.500
149	nanaco Point	23	7,500,000,000	0.500
152	Suica point club	20	200,000,000,000	N/A
155	Chocom e Money	17	306,578,542	0.000
158	Tepore	17	270,000,000	0.000
159	Chocom point	17	306,578,542	0.000
160	JP BANK Card	23	3,500,000,000,000	0.833
161	Point Monkey	26	80,000,000	0.167
163	Central Nippon Expressway Company	20	65,000,000,000	1.000
164	SBI Point	23	81,681,000,000	0.000
171	MUFG Card	23	N/A	0.667
200	ENEOS Card	22	139,400,000,000	1.000
206	Kaetoku card	19	N/A	1.000
208	Cue Monitor	19	N/A	0.167
209	NTT East Japan (Flet internet)	17	335,000,000,000	1.000
211	Point Exchange	19	411,162,000	0.000
212	Gendama	19	411,162,000	0.167
215	Apple World	26	200,000,000	0.000
217	nimoca	20	126,400,000	1.000
227	TEPCO	16	1,400,900,000,000	N/A
232	GetMoney!	26	211,500,000	0.000
237	Saitama Risona Bank	23	70,000,000,000	1.000
238	MyVoice	19	178,000,000	0.000
239	Chance It	19	211,500,000	0.000
240	Ikyu	19	914,000,000	0.000
241	Fastask	19	10,146,510,000	1.000
242	Ogaki Kyoritsu Bank	23	36,100,000,000	1.000
244	Juroku Bank	23	36,800,000,000	0.400
246	Ikeda Senshu Bank	23	50,700,000,000	1.000
248	Kinki Osaka Bank	23	389,071,000,000	1.000
253	For Travel	19	915,984,000	0.000
255	Tokopo	20	N/A	0.500
259	POINT-BOX	19	10,000,000	0.000
261	East Nippon Expressway Company	20	52,500,000,000	1.000
262	Apa Hotel	26	1,912,000,000	1.000
273	E Tour	26	260,500,000	0.167
284	Go to Dentist!	26	13,000,000	0.167
286	Boox Store	22	310,100,000	0.000
296	ANA Sky Coin	20	25,000,000,000	0.667
303	QooPo	13	28,534,000,000	N/A
307	My Acuvue	22	8,000,000,000	0.333

B.2 Industry

Table B.3 shows the nine industries which operate LPs in Japan. Full list of industry is in [6].

Table B.3: Nine industries which operate LPs in Japan. Each industry ID is the same as in [6].

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

B.3 Calculations of the Proxies

Our empirical studies were conducted based on the Gordon-Loeb security investment model [7], which con-siders the following four parameters as fundamental parameters: *expense* − the amount of security investment, *damage* − the amount of damage when the attack occurred, *threat* − the probability that an attack occurs, and *vulnerability* − the conditional probability that a threat once realized would be successful. When we consider the security of LP systems, one possible interpretation of the four parameters is as follows: *Expense* is the expense on IT security countermeasures by the LP-operating company; *Damage* is the amount of damage from IT incidents; *Threat* is considered to be high if the LP points' liquidity is high because higher liquidity implies more chances of achieving criminal benefits by malicious conversion of LP points or their redemption and it can be a main attractive factor; *Vulnerability* is considered to be lower if the online user authentication system of an LP is implemented in a more secure manner.

This appendix show how we set and calculate each proxy based on this interpretation, other than *threat*, with an explanation of different points from [6].

B.3.1 Damage

As is shown in Table B.4, METI's numerical data of IT damage represent only the damage ranges because METI's questionnaire answer sheet format used for this annual survey provides just the range for the damage amount [52]. So we calculated the average damage size for every capital size level by using the number of surely responded firms, and the middle value of the range (e.g. 0.75 million JPY for the range "0.5 million to 1 million") with an exception at the edge (i.e. we use 200 million JPY for the range " over 100 million. ") This method is also taken by METI itself for calculation of the damage to IT expense ratio [51].

Then, from each LP's industry and capital size,[1] we calculate its damage. We set this damage size as $damage_i$ where $i = 1, 2, ..., 82$ indicates each respective LP. For example, if LP_1's industry is "Information Service" and capital size is "under 50 million JPY," $damage_2 = 1875000$ (JPY).

This proxy calculation differs from [6] in the following three points. (1) [6] ignored firms which answered "did not suffer information security incidents," but we consider them as zero because it is more accurate. (2) In [6], they calculated the average damage considering only the industrial categorization, but we also considered the capital size for segmentation. (3) [6] used $impact = damage_{IND_i} * rank_i$ as the proxy of damage, where IND_i indicates LP i's belonging industry ID, $damage_{IND_i}$ is the average damage amount of its industry and $rank_i$ indicates the LP's ranking score at Poitan.net. However, this might be somewhat artificial.

[1] See Appendix B.1 and Appendix B.2

Table B.4: Examples of METI's data about the IT damage amount [51].

	Capital Size (JPY)	Total # of Firms	Damage from incidents																
			# of responded firms	Under 0.5 million	0.5 million to 1 million	1 million to 1.5 million	1.5 million to 2 million	2 million to 4 million	4 million to 6 million	6 million to 8 million	8 million to 10 million	10 million to 15 million	15 million to 20 million	20 million to 30 million	30 million to 50 million	50 million to 100 million	over 100 million	Not sure	did not suffer
				# of firms	# of firms	# of firms	# of firms	# of firms	# of firms	# of firms	# of firms	# of firms	# of firms	# of firms	# of firms	# of firms	# of firms	# of firms	# of firms
Information Service	under 50 million	69	10	3	1	·	·	·	·	·	·	·	·	·	·	·	·	2	4
	50 million to 100 million	132	26	9	2	·	·	1	·	·	·	·	·	·	·	·	·	2	12
	100 million to 300 million	48	10	3	1	1	·	·	·	·	·	·	·	·	·	·	1	2	2
	300 million to 500 million	26	9	4	1	·	·	·	·	·	·	·	·	·	·	·	·	3	1
	500 million to 1 billion	18	6	4	·	·	·	·	·	·	1	·	·	·	·	·	·	·	1
	1 billion to 10 billion	39	15	5	1	·	·	1	·	·	·	1	·	·	·	·	·	3	4
	over 10 billion	8	3	1	·	·	·	·	·	·	·	1	·	·	·	·	·	·	1
	unknown	1	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
	Total	341	79	29	6	1	·	2	·	·	1	2	·	·	·	·	1	12	25
Transportation and postal activities	under 50 million	65	5	3	·	·	·	·	·	·	·	·	·	·	·	·	·	·	2
	50 million to 100 million	113	10	3	1	·	·	·	·	1	·	·	·	·	·	·	·	·	5
	100 million to 300 million	30	4	3	·	·	·	·	·	·	·	·	·	·	·	·	·	·	1
	300 million to 500 million	19	1	·	·	·	·	·	·	·	·	·	·	·	·	·	·	1	·
	500 million to 1 billion	10	1	·	·	·	·	·	·	·	·	·	·	·	·	·	·	1	·
	1 billion to 10 billion	34	5	1	·	·	·	·	·	·	·	·	·	·	·	·	·	2	2
	over 10 billion	15	6	2	·	·	·	·	·	·	·	·	·	·	·	·	·	2	2
	unknown	1	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
	total	287	32	12	1	·	·	·	·	1	·	·	·	·	·	·	·	6	12

Table B.5: Security requirements in web authentications used for the calculation of sec_score [6].

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.

B.3.2 Expense

The proxy of expense is also calculated from METI's data by the same method used for the damage. Then, $expense_i$ $(i = 1, 2, ..., 82)$ is set.

B.3.3 Vulnerability

The metric of vulnerability is just the same as [6] used.

We used six requirements in the registration process, the authentication (login) process and the back-up authentication process of each LP. Table B.5 shows these six requirements.

They computed the security score, sec_score_i, of LP_i as the ratio of "the number of satisfied requirements in LP_i" to "the number of requirements about which we can obtain data regarding LP_i." For example, in Table B.6, $sec\_score_1 = 5/6 = 0.83$ and $sec\_score_2 = 2/5 = 0.40$.

sec_score_i represents how unsuccessful an attack is, so we can view sec_score_i as a metric for *anti*-vulnerability.

B.3.4 Normalization

[6] did not normalize any parameters, but we normalized *damage* and *expense* with *capital size* as follows:

$$\text{damage} : \frac{\log(damage_i)}{\log(capital\_size_i)}$$

$$\text{expense} : \frac{\log(expense_i)}{\log(capital\_size_i)}$$

Each LP-operating company has a lot of IT systems, and an LP system is just a one of them. Since the empirical data of expense and damage is for all the IT systems of the company, some normalization would be necessary when we measure the expense and expense on its LP system.

Table B.6: Security requirements example by [6]. "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.

	Requirements					
	Registration			Login	Back-up authentication	
	Trusted information	Physical card or account	Implementation of security techniques	Data which increases 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
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
LP_n	0	1	0	n/a	n/a	n/a

Appendix C

Liquidity Definition at the Previous Research

We briefly describe how Jenjarrussakul and Matsuura [6] defined *liquidity* and used this metric.

Before they conducted quantitative analysis, they had first considered the LPs security issues by industry. They listed up domestic 204 LPs and classified them into industries, eventually with 9 industries found to have LPs. They drew a graph of Japanese LP partnership network where each node indicates each industry. Since they had interests on how each industry node is connected, they checked the edge types (see Figure 4.2(a)) between industries and the average number of connecting LPs of all the LPs belonging to each industry.

In order to quantitatively examine which industry is more willing to connect with other industries via LP, they introduced a metric *liquidity* as a multiplier of the number of edge types, x, and the average number of partners regarding the LPs in a node, y:

$$liquidity = x * y$$

Then, they discussed industry with high liquidity LPs points does not always implement high security requirements.

After this industry based discussion, they entered upon a LP divided discussion and carried on quantitative empirical analysis with the same liquidity definition above. However, as described in Section 4.3.1 with Figure 4.2 (b), this definition does not seem suitable and intuitive convincing when we consider the LP-wise situation divided from the industry-wise cluster.