Analysis of Japanese Loyalty Programs Considering Liquidity, Security Efforts, and Actual Security Levels

Bongkot Jenjarrussakul and Kanta Matsuura

Institute of Industrial Science, The University of Tokyo, Japan.

Abstract

Virtual currency is an important medium of exchange in cyber space, and loyalty program (LP) can be considered as a type of virtual currency. In the U.S., according to a report in COLLOQUY talk[5], the total number of LP memberships is more than 2.6 billion in 2012 after 26.7% growth from 2010. In addition, the number of LPs is also reported to show a clear increasing trend. LPs are very popular in Japan, too; there are more than 200 LPs in Japan and the use of them is widespread among Japanese people. People collect their LP points and redeem them to obtain goods and enjoy services. In addition, many LP points can be converted into points of different LPs. LPs in Japan are thus increasing redemption options, and getting more and more popular and liquid virtual currencies. This situation can motivate malicious people to abuse such increasingly useful LPs for crimes, and in fact, there are some reports of such crimes. However, the security issues of LPs have not been well studied. In this paper, we investigate Japanese LPs with focuses on their liquidity, their operating firms' security efforts, and the LP systems' actual security levels.

Keywords: Loyalty program, virtual currency, security effort, liquidity.

1 Introduction

Virtual currency is an important medium of exchange for both virtual and physical goods and services. According to the classification of virtual currency by Accountability Office of the U. S. Government in [64], virtual currency is classified into 3 types: closed-flow, hybrid-flow, and opened-flow. In the case of closed-flow, there is no interaction between the virtual currency and real currencies or goods, and hence virtual environment is the only space where users can use their virtual currency. In the case of hybrid-flow, the virtual currency can be used to purchase both virtual and physical goods or services. However, virtual currencies in this type cannot be directly converted into real currencies. In the case of opened-flow, users can spend their virtual currency to buy both virtual and physical goods or services, too. In addition, they can directly convert their virtual currencies into real currencies.

There are many studies about security risks in virtual economics. Several studies considered massively multiplayer online games (MMOGS) in their works. Bardzell et al. surveyed some security vulnerabilities in MMOGS in general[4]. In their work, they also discussed how attacker cheats the system by using online frauds such as phishing and click-fraud. Some studies considered massively multiplayer online role-playing games (MMORPGS), where players use Avatar such as Second Life (SL) and World of Warcraft (WW)[11], [28], [29].

Irwin and Slay pointed out that MMORPGS can be used for some economic crimes[25]; they study money laundering and terrorism financing detection. Kiondo et al. explored some security risks in virtual economies with SL[30].

Beside MMOGS and MMORPGS, Bitcoin is another well-known actively studied virtual currency. Christin conducted a comprehensive measurement analysis of Silk Road, an online marketplace where Bitcoin can be used for payment[10]. He analyzed description of goods sold there, pictures, item categories, and so on to show characteristic of this online marketplace. Plohmann and Gerhards-Padilla focused on the concepts of botnet-related money-making where Bitcoin plays an important role[49]. Tyler and Christin studied the risk of exchanges between Bitcoin and real currency[39]. Compared to valuables (e.g. precious items) in online games, Bitcoin is closer to real currency in terms of its liquidity.

Loyalty program (LP) is another type of virtual currency located between online games and Bitcoin. Retail stores, credit card companies, airline companies, hotel chains and so on use LPs to increase motivation of their customers. Since the main objective of LP is to increase customers' repeat-purchase behavior, there are studies on LP in the economic aspect mostly focused on customer behavior and effective LP management[7], [14], [32], [56], [63]. There are also empirical studies on this topic. For example, in [31], it is shown that customer-oriented firms most likely adopt LPs. Security aspects of LPs are not really well studied.

In Japan, LPs are very popular and their liquidity is high; there is even an LP information website called *Poitan* (Point Exploration Club)[1]. At Poitan, information of more than 200 LPs in Japan is provided. The LPs supported there are widespread in terms of their parent businesses: airline companies, electronics discount shops, convenience stores, and so on. Poitan shows information such as estimated real-currency values of LP points, exchange/conversion rates between different LPs, and how long the conversion would take. Suppose that a consumer would like to convert a certain amount of ANA (All Nippon Airways, a star alliance member) miles, say, 20,000 miles, into JAL (Japan Airlines, a one-world alliance member) miles. In response to this query, Poitan shows all the possible conversion routes. For example, on February 21, 2014, Poitan showed that the following was only one possible route for this conversion:

- By redeeming at ANA's website, one can convert 20,000 ANA miles (estimated value is 30,000JPY (Japanese Yen)) into 20,000 Matsumoto-Kiyoshi[2] points (estimated value is 20,000JPY). This would take about 30 days.
- Likewise, at Matsumoto-Kiyoshi, one can convert 20,000 points into 14,000 G-Points[3] (estimated value is 14,000JPY). This would take about 21 days.
- 14,000 G-points can be converted into 14,000 Nimoca points[4] (estimated value is 14,000JPY). This would take about one day.
- By redeeming at Nimoca's website, 14,000 Nimoca points can be converted into 7,000 JAL miles (estimated value is 10,500JPY). This would take about 7 days.

[1] "Poi" is from "point" and "tan" is from "tanken", a Japanese word which means exploration.
[2] Matsumoto-Kiyoshi is a popular pharmacy chain.
[3] G-Point is an LP point exchange service with a comprehensive e-commerce portal service.
[4] Nimoca is an LP operated jointly by local bus and railway companies in the western part of Japan.

LPs in Japan are still increasing such redeeming options, and thus getting more and more popular and liquid virtual currencies. However, their security issues have not been well studied. In this paper, we investigate Japanese LP systems with focuses on their liquidity, their operating firms' security efforts, and the LP systems' actual security levels. The rest of this paper is structured as follows. In the next section, we talk about LP in general, and show some recently reported security incidents of LPs. In Section 3, we analyze the Japanese LP network, and evaluate liquidity of LP points in different industries. Next, based on the statistics published by the Japanese government, we show security-related data of the industries which have LP operating firms in Section 4. We then proceed to a detailed network analysis and a security analysis of selected LP systems in Section 5. The security analysis considers registration, authentication, and back-up authentication systems (e.g. password recovery protocols) of LPs to observe their actual security levels. Based on our intuition that attackers would be more interested in more liquid LPs, we consider a model to derive security-liquidity implications and conduct a linear regression analysis in Section 6. Section 7 shows a summary of the results.

2 Loyalty Programs and Security Incidents

Loyalty program is a marketing activity whose main objective is to encourage customers' *loyalty behaviors* by rewarding them[59]. The rewards usually take the form of *reward currency* or *point*. Firms which operate LPs can gain more information about their customers' behaviors[13]. These data would give more opportunities to the vendor to understand more about their customers [42]. Many LP operators also cooperate with their business partners so that rewards can be exchanged between different LPs. Liquidity of reward currencies is thus increased. However, this is not the only strategy that operators use. For example, some LPs allow their customers to earn and spend their points at variety of participating shops [42]. Such strategy is said to be popular outside the U.S. In addition, some reward points can be redeemed to obtain both virtual and physical goods or services.

Despite the cooperative strategy, the world trend of the number of LP memberships is also interesting. In the U.S., according to a report in COLLOQUY talk[5], the total number of LP memberships is more than 2.6 billion in 2012 after 26.7% growth from 2010. This increasing number of LP memberships also brought the average number of LPs per U.S. household to 21.9 from 18.4 in 2010. This growth is said to be a result from the gradual recovery rate from the recession during 2007-2009 and introduction of new programs, especially those that operated by companies which had never operated LPs before.

According to another report in COLLOQUY talk in the same year[6], 90% of Canadian customers belong to at least one LP. This number is very high comparing to 74% in the U.S. However, due to the report, the average number of LPs per Canadian household has dropped 7.5% from 2010. The report claims that the main part of this declination rate comes from demographic factors; 1.) The 7% increment of the number of households with steady figure of membership. 2.) An immigration-driven growth of population. Other factors are such as privacy concern, and similarity of the benefits from different LPs. Thus LPs are still popular among Canadian customers in spite of the slightly decreasing trend.

What about LPs in Europe? Although loyalty program marketing is quite new in Europe, it is estimated that roughly 80% of shoppers in Europe belong to at least one LP[34]. In addition, one-third of those European shoppers use two or more LPs.

In UK, according to the information by SAS[5], almost 95% of UK consumers possess at least one loyalty card[57]. Sixty-Five percent of UK customers join 3 or more LPs. Interestingly, the active customers, who regularly use their LPs, are as high as 88%. And 40% of UK customers say they are less likely to visit retailers with no LP.

LPs are also very popular in Japan. There are more than 200 LPs in Japan. In 2012, Japanese Statistics Bureau survey did a survey about household expenditure which includes the use of e-money and point cards[6][62][7]. This report shows an increasing trend of the use of both e-money and point cards. 74.6% of 30,000 Japanese households possess point cards in 2012 (increased from 72.1% in 2011). And 38.7% of the same group of Japanese households possess e-money cards in 2012 (increased from 35.6% in 2011).

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

In fact, there are many reports and articles about security incidents related to LPs. Loyalty-card fraud (sometimes called Affinity-card fraud) is different from credit-card fraud[43]. The main difference is the retrieved information from Loyalty-card fraud could be used for identity theft. Identity theft lets an attacker easily impersonate the cardholder and break into the corresponding online systems. In addition, it could also let attacker trace the victim's routine and/or behavior which lead to other types of crime.

Airline industry is one of the well-known participating industry in loyalty marketing. There are plenty of alerts from several airlines which are related to security incidents that occurred with frequent flyer's accounts. With frequent flyer programs, generally, attackers attack the system by taking advantages of system's weakness such as weak login credentials, and phishing campaigns[33]. Attackers could, then, utilize the account owner's collected points in various redemption ways. Many airlines also put on alert and advisory on their website regarding this topic. For example, there are such announcements by U.S. airways [8], Delta airlines [9], and British airways [10].

Security of LP is also one of the concerns in hotel industry. During the panel discussion in a conference for hotel industry at the beginning of 2014[3], gift-card and LP frauds are picked up in the discussion. They mentioned that "*as the points have been paid for before reaching the hotel, it's easy for partners (i.e. hotels) to cover their eyes to potential fraud.*".

In Britain, Tesco, a well-known supermarket chain, also experienced irregular activities in 2013[27]. At that time, some amounts of gift vouchers from accounts of Tesco's Clubcard members were spent by malicious parties. Some members also reported that some parts of their account information are slightly changed. Since they did not respond to any phishing e-mails, some members believed that their accounts have been compromised through the vulnerability of the LP system.

In addition, according to many news, LP's security incidents are usually related to identity thefts. In March 2014, Canadian police investigated a scamming case in which the suspects used fraudulent credit cards[9]. Their revealed investigation result shows that this scam included illegal redemption of the credit card points for gift cards.

[5]SAS Institute for advanced analytics, business intelligence, data management, and predictive analytics.
[6]Definition of *point card* in this report excludes paper-based stamp cards.
[7]In our study, Japanese LPs come in both types of e-money and point card.
[8]http://www.usairways.com/en-US/contact/scamalert.html
[9]http://www.delta.com/content/www/en_US/traveling-with-us/advisories/phishing-email-alert.html
[10]http://www.britishairways.com/travel/flightops/public/en_gb?p_faqid=4290

Recently, in Japan, there are several reports about security incidents related to LPs too. For example, in 2012, there was a report from G-Point about unauthorized access[19]. In this incident, 59,044 IDs were compromised and points from 447 accounts were illegally used to obtain Amazon gift vouchers. The damages of this incident cost 1,617,525 JPY (or 15,808 USD[11]). In April 2013, there was a news about T-Point[58][12] when it was attacked by unauthorized accesses from both domestic and oversea origins. In this incident, points from at least 299 member accounts were illegally transferred to several different accounts. In December 2013, two Chinese college students were arrested due to the Rakuten point exchange fraud[40][13]. They bought an ID-Password list from someone through the Internet, accessed some accounts by using the list, and converted Rakuten points into e-money. As a very recent case, in February 2014, JAL experienced malicious redemption. Some of the FFP (frequent flyer program) accounts were compromised and their JAL miles were used to obtain Amazon gift vouchers[26].

From the above examples, we can see security of LP systems is becoming an important issue.

3 Japanese Loyalty Programs and Their Network

3.1 Loyalty programs in Japan

Firstly, by using Poitan[44], we overview LPs in Japan. LPs supported at Poitan are categorized into 16 groups based on the types of shops or services: airlines, banks, books/CD/DVD, petroleum stations, shared point (common point system), credit card, e-money (digital cash implemented by using rechargeable IC cards), electronics discount retail stores, hotel chains, online shopping, online point exchange system, telecommunication (telephone companies and Internet service providers), supermarkets, railway companies, travel agencies, and others[14]. In our study, we re-categorize LPs as shown in Table 1 so that we can use the governmental statistics[37] in our subsequent analysis on the security and liquidity of LPs.

At Poitan, we collected the information of 247 LPs. Among them, 207 LPs (84% of the 247 LPs) are operated by Japanese firms and are still active. We then classify these 207 LPs according to the re-categorized list of industries. As a result, these LPs are operated by firms in nine industries: Manufacture of electrical machinery, equipment and supplied (industry ID 09), Miscellaneous manufacturing industries (industry ID 13), Electricity, gas, heat supply and water (industry ID 16), Video picture, sound information, broadcasting and communication (industry ID 17), Information services (industry ID 19), Transportation and postal activities (industry ID 20), Retail trade (industry ID 22), Finance and insurance (industry ID 23), and Miscellaneous non-manufacturing industries (industry ID 26). Unsurprisingly, these nine industries are those that have high interaction with customers or so-called *customer-oriented* industries[20], [61].

Next, in Fig. 1, we draw a graph of the Japanese LP network as follows.

[11]Exchange rate on Feb 1, 2014. 100 JPY = 0.98 USD. We use this rate throughout the paper.

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

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

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

Table 1: List of industries* conforming to the governmental statistics[37].

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

*We use the Japanese-English contrast table in [50] when we translate the names of the industries.

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

  Group 1: Between the two nodes connected by the edge, there are all the three types of flows. In Fig. 1, we use 3 parallel lines (blue, red, and green) to represent such edges.

  Group 2: Between the two nodes connected by the edge, there are two types of flows. The possibilities are "one-directional flow and the opposite one-directional flow" and "one-directional flow and bidirectional flow". In Fig. 1, we use two arrows to represent such edges; one-directional flows are blue or red, and bidirectional flows are green.

Group 3: Between the two nodes connected by the edge, there is only one type of flow. In Fig. 1, we use a single black arrow to represent such edges.

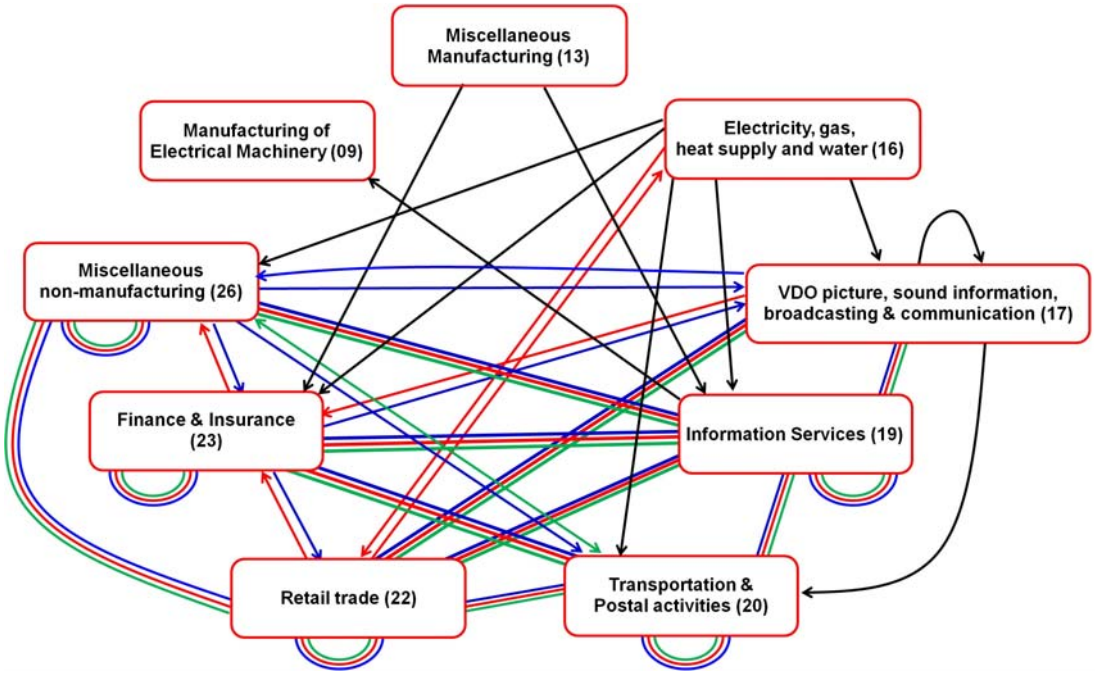

Figure 1: Japanese loyalty-program (LP) network focused on the nine industries and convertibility of the LP points.

3.2 Liquidity of LPs

In economics, liquidity is a characteristic possessed only by perfectly marketable assets[23]. A study by Adrian and Shin introduces a new definition of liquidity: the rate of growth of aggregate balance sheets[1]. They explained the effects of monetary policy on overall liquidity conditions. European central bank mentions that liquidity is a flow concept in financial systems[41]. It also has the ability of realizing the flow. Liquidity is also important in the area of foreign exchange market[35]; in their study, liquidity of foreign exchange could also affect issues such as insurance premium, appreciation of the low or high interest rate currencies, etc. Liquidity is thus becoming a topic discussed in a wider spectrum.

In the cyber world, online services such as online auction, exchanges, and e-marketplace increase liquidity, and there is a view that more secure systems provide higher liquidity[60]. Liquidity is also becoming important in cyber finance[8]. With increasing number of channels for online transaction, liquidity is getting higher and vulnerability of the organization is increased[21]. Security, trust, and risk management are fundamental research items there.

Bitcoin is a particular implementation of crypto-currency, and there are several different views about its liquidity. In a country where the liquidity of real currency is problematic (e.g. Iran), Bitcoin is becoming an important way of making transactions especially with business partners abroad[51]. In such cases, Bitcoin is considered highly liquid. However, in general, disadvantages of Bitcoin are discussed from the viewpoint of its limited liquidity[12]. Online

currency exchange sites like Mt.Got and Tradehill also consider this point. In the case of Tradehill, it even paused the exchange services for Bitcoin[22]. By observing the discussions on the liquidity of Bitcoin, it is easy to notice that liquidity is an important research topic in LPs.

We evaluate the liquidity of LPs based on the classification of the edges in Fig. 1 and the number of their partner programs. We introduce four liquidity levels: Low (L), Medium-Low (ML), Medium-High (MH), and High (H). The evaluation process is as follows.

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

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

3. Define *liquidity score* as xy.

4. If $0 \leq xy \leq 15$, we say the liquidity is low. If $15 < xy \leq 23$, we say the liquidity is medium-low. If $23 < xy \leq 30$, we say the liquidity is medium-high. Finally, if $30 < xy$, we say the liquidity is high. The final column of Table 2 shows the results.

Table 2: Liquidity of LPs by industry.

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

*There is only one loyalty program.

4 Security-related Data of LP Operating Firms

The Japanese data regarding security issues can be retrieved from *Survey on information processing: result detail part 3*[38]. This data is published by Ministry of Economy, Trade

and Industry (METI) and publicly accessible. The newest data available for this work is the data of year 2012. For the nine industries, the obtained data is shown in Table 3.

One may expect that higher liquidity would imply larger security investments because such LPs would need higher security. On the other hand, one may expect that higher liquidity would imply larger damages because more attackers would choose such LPs. Table 3 supports neither of them because there is no definite tendency.

Table 3: Security-related data of industries in which Japanese firms operate LPs.

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

*Ratio of average size of damage to average capital size.

**Ratio of average size of expense on countermeasure to average capital size.

5 Selected LPs and Their Security Analysis

In this section, we consider actual security levels of LP systems. Security engineers provide some technologies so that attacks will fail. This is vulnerability reduction in the context of a security investment model[36]. In addition, they provide other technologies so that attacks will not occur. This is threat reduction in the context of the security investment model. Since both reductions are important in the evaluation of actual security levels in an empirical study, we examine the following three processes.

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

Authentication (login) plays an important role in vulnerability reduction since most LP systems accommodate general consumers whose literacy regarding password security is not really high. If an authentication process requires correct CAPTCHA inputs,[15] this process can contribute to threat reduction, too, due to the increasing cost of attack.

[15]CAPTCHA (Completely Automatic Public Turing tests to tell Computers and Humans Apart)[2] is a mechanism to avoid inputs by automated attack tools. A popular example is a text CAPTCHA which asks a user to input the texts which are displayed in a distorted manner.

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

In this paper, we firstly select representative LPs for the nine industries focused in the previous sections (i.e. the industries which have active LPs operated by Japanese firms). This selection is made based on existing surveys regarding the use of LPs and related customer behaviors in Japan[15], [16], [17], [18], [52], [53], [54], [55]. The resultant list of selected LPs are as follows:

Industry 09:	Sony point
Industry 13:	QooPo
Industry 16:	Switch! point
Industry 17:	Softbank point
Industry 19:	T Point, PeX, G-Point
Industry 20:	ANA Mileage club, JAL Mileage bank, Suica point[16]
Industry 22:	Matsumoto Kiyoshi, Yamada Denki point[17]
Industry 23:	Mitsui Sumitomo Card (credit card company)
Industry 26:	Ponta (convenience store and its partners)

In each system of the above selected LPs, we manually investigated the requirements in the three processes to see their security.[18]

Before showing the result of this investigation in the subsequent subsections, let us overview the network of the selected LPs in Fig. 2 where each node indicates each LP. We draw an arrow if point conversion in that direction is possible. Each arrow has the following two labels.

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

Actual rate of exchange: `[Yen]` is a rate of exchange in terms of the estimated real-currency values (i.e. *the estimated real-currency value of the points of the destination LP* divided by *the estimated real-currency value of the points of the original LP*). For example, 10,000 T-points can be converted into 5,000 ANA miles. At Poitan[44], the estimated real-currency value of 10,000 T-points is 10,000 JPY, and the estimated real-currency value of 5,000 ANA miles is 7,500 JPY. Therefore, the arrow from T Point to ANA Mileage Club is labeled `[Yen] 0.75`.

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

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

[18] We do not analyze the security of QooPo and Switch! point due to some operational difficulties. We use these two LPs only for drawing the LP network in Fig. 2.

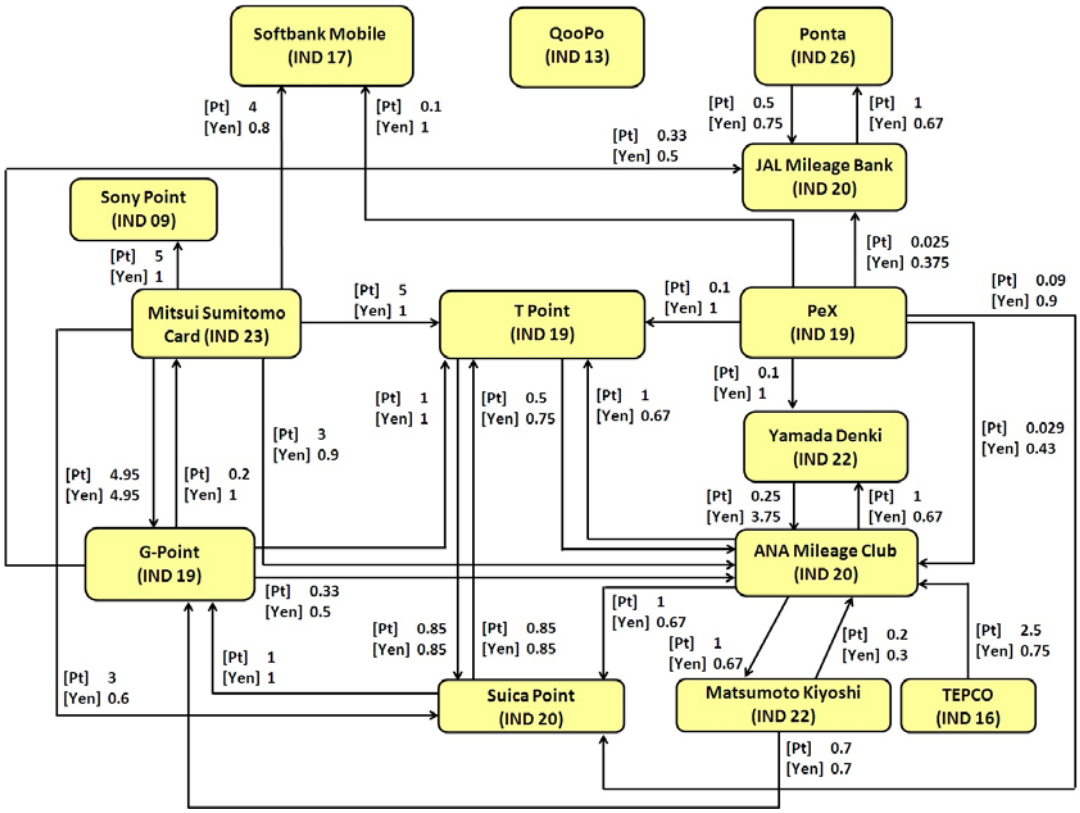

Figure 2: Network of selected loyalty programs from different industries.

5.1 Registration Requirements

Table 4 shows the result of our investigation about what are required in the registration process. "Y" indicates that the corresponding information is required in the registration process. "Y*" indicates that the corresponding information is an option (i.e. customers do not have to provide the information but they can do so optionally.). Lastly, "–" indicates that the corresponding information is not required during the registration. The column of Softbank Point in Table 4 is N/A (not applicable) because its registration process is not online; the registration for LP online access is automatically done when a person becomes a customer through an offline process.

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

An additional security mechanism, CAPTCHA, is used by the LPs in Industry 19 (medium-high liquidity) and the LP in Industry 09 (low liquidity). Another countermeasure

is *URL for further process*. If this is deployed, the LP's portal does not provide the URL for registration. Instead, the registration URL is e-mailed to the user. This countermeasure is used by LPs of various liquidity levels.

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

5.2 Authentication Requirements

All the systems use ID and password. Difference is in the types of IDs, as shown in Table 5. "Y" indicates information required during authentication. "Y†" indicates *one-out-of-the-two* requirements; that is, in the cases of Sony Point and T Point, either registered e-mail address or physical card number is required (users can make a choice by themselves). Finally, "–" indicates information that is not required during the authentication.

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

5.3 Back-up Authentication Requirements

As shown in Table 6[19], back-up authentication requirements of the LP systems are quite different system by system[20]. This suggests that heuristics of back-up authentication has not been established yet.

[19] In Table 6, symbols "Y", "Y†", and "–" are used in the same way as in Table 5.

[20] We did not analyze Suica Point due to some operational difficulties. The LP of Mitsui Sumitomo card requires users to restart from the registration without offering a back-up authentication mechanism.

Table 4: Requirements for registration.

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

Table 5: Types of required user IDs in authentication process.

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

Table 6: Requirements during back-up authentication processes.

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

6 Security-Liquidity Implications

As we can learn from the examples in Section 2, illegal exchange of LP points are often used in LP security incidents. Therefore, intuitively, an attacker would have higher incentive to compromise an LP which has higher liquidity. In this section, we investigate a relationship between security and liquidity by linear regression analysis.

6.1 Data

There are many factors that could increase an impact of an LP security incident. Financial damage is a basic factor when we consider an impact of a security incident in general. In addition, we focus on popularity because popular LPs would not only have large news values but also be preferred by attackers. At Poitan, based on the monthly statistics of queries, we can see the top 20 popular LPs or LP pairs as shown in Table 7. The "Utilized pair of exchange" column in Table 7 shows the top 20 queries made at Poitan in April 2014[46]; exchange of T Point into ANA mileage is the most frequently queried pattern. The "Origin LP" column in Table 7 shows the top 20 LPs which were used as the origins of the exchanges in queries made at Poitan in April 2014[47]; exchange of T Point into something else is the most frequently queried pattern when we focus on the origin. Likewise, "Destination LP" column in Table 7 shows the top 20 LPs which were used as the destinations of the exchanges[48]. We selected 82 Japanese LPs or 33% of Japanese LPs available at Poitan as our samples in this study so that most of the top 20 rankers are included and each of the security analyses explained in Section 5 can be done in most of the samples.

Table 7: Raking of Loyalty Program (April 2014).

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

We use the following proxy variables in our analysis:

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

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

   And then, we calculate the impact proxy as follows:

$$impact_i = damage_{IND_i} * rank_i \tag{1}$$

   where

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

2. Liquidity
   We calculate an LP-wise liquidity score $liquidity_i = xy$ by using a similar methodology to that used in Section 3.2. In particular, we firstly consider the edge types between LP_i and 9 industries where only the 82 selected LPs are considered, and obtain the value of x. We then obtain the value of y by counting the number of the exchange partners of LP_i.

3. Security score
   In Section 5, we investigated a lot of security-related requirements in the registration process, the authentication (login) process, and the back-up authentication process of each LP. In this section, we focus on the important requirements listed below.

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

We compute the security score, $secscore_i$, of LP_i as 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, let us consider Table 8. In this case, $secscore_1 = 5/6 = 0.83$ and $secscore_2 = 2/5 = 0.40$.

Table 8: Security requirements (n/a means that data is unavailable). The value of 1 indicates that the corresponding requirement is satisfied. The value of 0 indicates that the corresponding requirement is not satisfied.

	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
⋮	⋮	⋮	⋮	⋮	⋮	⋮
LP_n	0	1	0	n/a	n/a	n/a

6.2 The model

Based on the viewpoints mentioned in the beginning of this Section 6, we examine the following two hypotheses:

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

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

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

$$impact_i = \beta_0 + \beta_1 expense_i + \beta_2 liquidity_i + \beta_3 secscore_i \tag{2}$$

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

6.2.1 Verifying the data

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

Table 9: The results of the linear regression analysis of the model.

Variable	Coefficient	p-value
Intercept	4311.912	0.6401
expense	0.193764	0.0027^{***}
liquid	643.6897	$3.49e^{-09***}$
secscore	-30138.18	0.0115^{**}

** indicates significance at 5% level.

*** indicates significance at 1% level.

6.2.2 Result of the regression analysis

The result of the linear regression analysis of our model is shown in Table 9.

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

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

Finally, the positive sign of the coefficient of *expense* suggests that larger security investment by an origin LP operator would decrease the impact of security incidents. However, since we used not LP-wise but industry-wise data for *expense*, we do not provide a corresponding hypothesis this time.

7 Summary

In this paper, we first showed that the LP network in Japan is really large and that associated virtual currencies are very liquid. We then identified four industries with high/medium-high liquidity: *Video picture, sound information, broadcasting and communications*, *Information services*, *Transportation and postal activities*, and *Finance and insurance*. It should be noted that major incidents[19], [58], [40], [26] actually happened in these four industries. We should be careful because more attackers would choose such highly liquid LPs.

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

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

In conclusion, we recommend LP operators more security efforts particularly to satisfy strong security-related requirements in their systems.

References

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

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

[3] Baker, T. "Panelists: Management risk to protect growth," In *The 2014 Master Innholders Conference*, Jan 2014. Available at https://www.hotelnewsnow.com/Article/12996/Panelists-Manage-risk-to-protect-growth

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

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

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

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

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

[9] CBC News, "Major new credit card scam uncovered in B.C. – 'Web of criminal activity' involves hundreds of credit cards and thousands of dollars in reward points," March 19, 14 Available at http://www.cbc.ca/news/canada/british-columbia/major-new-credit-card-scam-uncovered-in-b-c-1.2579214

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

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

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

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

[14] Dowling, G.R., and Uncles, M., "Do Customer Loyalty Programs Really Work?," In *MITSlone Management Review*, 1997. Available online at http://sloanreview.mit.edu/article/do-customer-loyalty-programs-really-work/

[15] Dimsdrive, "Survey on Point Card (in Japanese)," Timely research, 2006, Available at http://www.dims.ne.jp/timelyresearch/2006/060516/index.html

[16] Dimsdrive, "The 22th Survey Result on Electronics Retail Store's Point Card (in Japanese)," Ranking research, 2007, Available at http://www.dims.ne.jp/rankingresearch/101_150/122/004.html

[17] Dimsdrive, "Survey on Department Store (in Japanese)," Timely research, 2007, Available at http://www.dims.ne.jp/timelyresearch/2007/071002

[18] Dimsdrive, "Survey on the Use of Convenience Store (in Japanese)," Timely research, 2010, Available at http://www.dims.ne.jp/timelyresearch/2010/100204

[19] G-Point, "Report on unauthorized access to G-Point (in Japanese)," April 24, 2012, Available at http://info.gpoint.co.jp/blog/2012/04/g424-1915-93b6.html

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

[21] Gordon, L.A., Loeb, M.P., and Sohail, T., "A Framework for Using Insurance for Cyber-risk Management,2 In *Communication of the ACM*, Vol. 46, No. 3, 2003.

[22] Harrisson, C., nand Hamilton, J., "Bitcoin Exchange Tradehill Pauses for Regulatory Reasons," In *Bloomberg Technology*, 2013, Available at http://www.bloomberg.com/news/2013-08-30/bitcoin-exchange-tradehill-pauses-trading-for-regulatory-reasons.html

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

[24] Investopedia, Available at http://www.investopedia.com

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

[26] Japan Airlines, "Temporary Suspension of the Amazon Gift Certificate Award and Request to Change JMB PINs," Feb 3, 2014, Available at http://www.jal.co.jp/en/info/jmb/140203.html

[27] Jones, R., "Tesco Clubcard fraud tale could be tip of iceberg," November 30, 2013. Available at http://www.theguardian.com/money/2013/nov/30/tesco-clubcard-fraud-stolen-vouchers

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

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

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

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

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

[33] Levitte, J. "Airlines face new and unexpected security threat – loyalty fraud," Nov 29, 2012. Available at http://www.tnooz.com/article/airlines-face-new-and-unexpected-security-threat-loyalty-fraud/

[34] Loyalty Card (website), "Loyalty Program Overview," Available at http://www.loyaltycard.in/content/view/33/45/

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

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

[37] Ministry of Economy, Trade and Industry, Survey on information processing: Entry outline of the survey (in Japanese), Available at http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/pdf/04_H24kinyuyoryo.pdf

[38] Ministry of Economy, Trade and Industry, Survey on information processing: result detail part 3 - information security (in Japanese), Available at http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/h24jyojitsu.html

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

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

[41] Nikolaou, K., "Liquidity (Risk) Concepts: Definitions and Interactions," In *European Central Bank, Working Paper Series No.1008*, 2009, Available at http://ssrn.com/abstract=1333568

[42] Pearson, B., "Four differences between U.S. and Eurpean loyalty progams," Dec 2013. Available at http://www.loyalty.com/research-insights/blog/from-loyal-to-four-differences-between-u-s-and-european-loyalty-programs

[43] Poremba, S.M., "Security How Shopping Loyalty Cards Help Identity Thieves," In *Tech News Daily,* July 25 2012, Available at http://www.technewsdaily.com/4608-loyalty-card-identity-theft.html

[44] Point Exploration Club (Poitan), Loyalty programs information in Japanese, Available at http://www.poitan.net

[45] Point Exploration Club (Poitan), Statistical Information, Available at http://stats.poitan.net

[46] Point Exploration Club (Poitan), Statistical Information of April 2014: Rank of utilized pair of exchange, 2014, Available at http://stats.poitan.net/exchange-201404.html

[47] Point Exploration Club (Poitan), Statistical Information of April 2014: Rank of origin LP, 2014, Available at http://stats.poitan.net/in-201404.html

[48] Point Exploration Club (Poitan), Statistical Information of April 2014: Rank of destination LP, 2014, Available at http://stats.poitan.net/out-201404.html

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

[50] Portal site of Official statistics of Japan, Japanese-English Contrast Table, Available at http://www.e-stat.go.jp/

[51] Raskin, M., "Dollar-Less Iranians Discover Virtual Currency," In Bloomberg Businessweek - Global Economics, 2012. Available at http://www.businessweek.com/articles/2012-11-29/dollar-less-iranians-discover-virtual-currency

[52] Reposen, "Attitude Survey on the Use of Point Cards (in Japanese)," Jul, 2013, Available at https://reposen.jp/3792/2/50.html

[53] Research Bank, "Survey on Women's Usage on Point Services (in Japanese)," Jun, 2008, Available at http://research.lifemedia.jp/2008/06/080604pointservices.html

[54] Research Bank, "Survey on Internet Shopping (in Japanese)," Jan, 2013, Available at http://research.lifemedia.jp/2013/01/130130_netshopping.html

[55] Research Bank, "Survey on the Use of Convenience Store (in Japanese)," Jul, 2013, Available at http://research.lifemedia.jp/2013/07/130724_cvs.html

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

[57] SAS Institute for advanced analytics, business intelligence, data management, and predictive analytics, "Are Retailers Making the Most of Loyalty Schemes," 2013. Available at http://www.sas.com/offices/europe/uk/downloads/loyalty/loyalty-infographic.pdf

[58] Scan Net Security, "299 IDs Compromised at the Site of T Point (in Japanese)," April 9, 2013. Available at http://scan.netsecurity.ne.jp/article/2013/04/09/31404.html

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

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

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

[62] Statistics Bureau, Ministry of Internal Affairs and Communications, "Household Expenditure Report – 2012 Report Summary (in Japanese)," 2012, Available at http://www.stat.go.jp/data/joukyou/2012ar/gaikyou/pdf/gkall.pdf

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

[64] United States Government Accountability Office, "Virtual economies and currencies: Additional IRS guidance could reduce tax compliance risks," May 2013. Available at http://www.gao.gov/assets/660/654620.pdf

[65] Yomiuri Newspaper, "299 T-Point account were robbed by unauthorized login (in Japanese)," April 6, 2013. Available at http://premium.yomiuri.co.jp/pc/#!/news_20130406-118-OYT1T00509