VALUE ORCHESTRATION PLATFORM FOR ICT SECURITY SERVICES

Takafumi Nakamura[1]*, Kyoich Kijima[2]

[1]Fujitsu FSAS Inc., Support Administration Group, Hamamatsu-Cho Support Center, 5-1, Hamamatsu-Cho 1-Chome, Minato-ku, Tokyo, 105-0013, JAPAN, nakamura.takafu@jp.fujitsu.com

[2]Tokyo Institute of Technology, Graduate School of Decision Science and Technology,2-12-1 Ookayama, Meguro-ku, Tokyo, 152-8550, JAPAN, kijima@valdes.titech.ac.jp

*Correspondence to: Takafumi Nakamura

ABSTRACT

This paper explains the service science approach to ICT security. The first half of 2011 should prove to be the "year of the breaches." We saw numerous security breaches targeting high-profile organizations such as, Sony PlayStation, Lockheed Martin, and a dozen of other companies and government organizations. Mitsubishi heavy industries have suffered security attack from anonymous group. The attack, which involved several types of data-stealing malware on Mitsubishi computers, occurred in August 2011. The impacts of the security breach are quite sever for enormous number of people's private information and top secret information in corporations (or governments) were disclosed in those cases. The damage of the corporate in terms of reliability and economy are enormous. However the security is a non-functional requirement therefore it tends to be ignored at ICT design phase to implement security requirement. The service science approach to ICT security shed a light to the ICT security area to maximize ICT security measures and investments. This paper provides the concept of value orchestration platform for ICT security services. Firstly we survey the current ICT security market, and we conceptualized this situation as two parties' model between customers and providers. Then we use ICT security standard as security service platform. This enables us to visualize current ICT security venerability or inappropriate investments. Lastly we conceptualize this solution as three parties' model (i.e. value orchestration platform) between customers, providers and security service platform providers. We conclude that the three parties' model contribute maximizing ICT security measures and investments as value orchestration platform.

Key words: Service System Modeling; Value Co-Creation Process; Value Orchestration Platform; Curation; Risk Management; Information and Communication Technology (ICT)

INTRODUCTION

ICT security market for products, tools, integration and services is divided into small segments and ICT vendors are concentrated in their own special technical area. Figure 1 explains the complicated situation of ICT security products, tools, integration services and operation services. The vertical dimension in figure 1 is the ICT life cycle when those services should be applied at design, development and operation phase. The customers have to integrate their ICT security system in piecemeal fashion. These environments lead to hinder an efficacy and profitability of ICT security. On the other hand the security incidents are increasing and the subjects and purposes of security attacker are increasing diversity. Figure 2 is the classification of targeted attackers and its subjects and purpose. Hacktivism (a portmanteau of *hack* and *activism*) is the use of computers and computer networks as a means of protest to promote political ends. IPA Japan (2011) issued 10 major security threat explain security incidents trend. For the year 2011, 5 new threats that were not in top 10 in past years ranked in, such as attacks targeting smart phones and the SNS users. Information leakage and targeted attacks are making regular appearance on the top 10 list (table 1). In summary ICT security market features are 1. Many vendors are concentrating on relatively small segment of technical expertise, 2. ICT systems owner have to integrate security feature with piecemeal fashions, 3. ICT systems owner is hard to maximize ICT security investments based upon the security vendors' situation as explained in number 1, 4. The Attackers or hackers are becoming diverse in terms of their purposes and scale. Under these circumstances, we need novel approach to maximize ICT security effectiveness and investments for both security vendors and ICT systems owners. This is the reason why the service science approach is applied to ICT security in order to maximize ICT security measure. In this paper we propose Value orchestration platform for ICT security services to manage this situation.

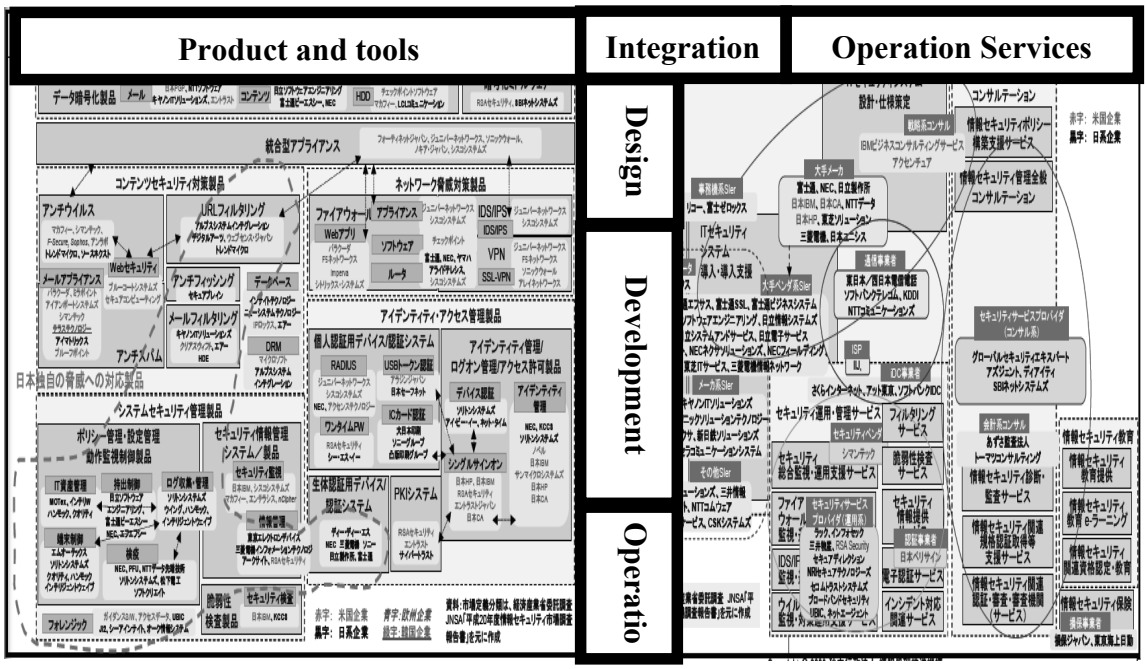

Figure 1 the structure of Japanese ICT security market

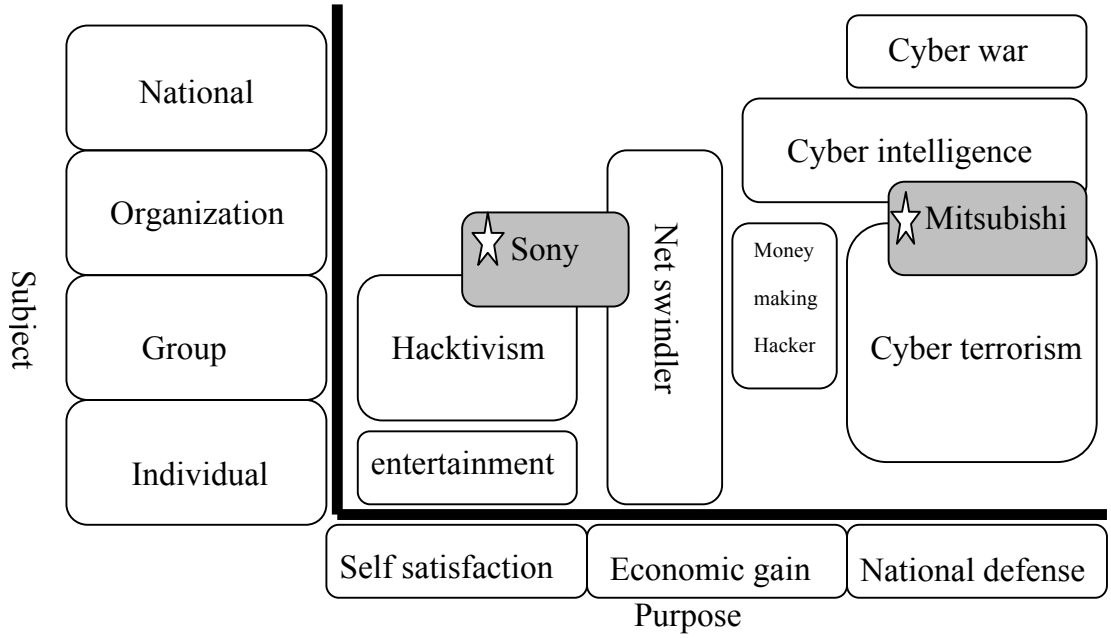

Figure 2. Classification of targeted attacks and its subject and purpose

Table 1. Trend of 10 Major Security Threats

10 Major Security Threats in 2010		Ranking in 2009	Ranking in 2008	Ranking in 2007	Ranking in 2006
1st	Information leakage caused by "people"	5	5	3	7
2nd	Unstoppable! Attacks via websites	1	2	5	9
3rd	Attacks exploiting vulnerability in standard softwares	2	—	8	—
4th*	Attacks targeting smartphones on the rise	—	—	—	—
5th*	Advanced Persistent Threats (APT) that combines multiple attacking methods	—	—	—	—
6th*	Troubles caused by inadequate security measures	—	—	—	—
7th*	Security issues in mobile phone websites	—	—	—	—
8th	Hard-to-detect targeted attacks	6	3	4	2
9th	Security issues in cloud computing	9	—	—	—
10th*	Attacks targeting users of microblogging service and SNS	—	—	—	—

* Threats that are newly ranked in IPA's 10 Major Security Threats

1. SERVICE DOMINANT LOGIC

Service science is an emerging area of study that draws on decades of pioneering work in the research area of service marketing, service operations, service management, service engineering, service economics, and service computing (Spohrer, J., Maglio, P., 2008; Maglio, P., Spohrer, J. ,2008; Cambridge, 2008; Barile, S., Spohrer, J.,2010) . Service science tries to define service as a phenomenon observable in the world in terms of a service system with value co-creation interactions among entities (Spohrer, J., Maglio, P., 2008) by taking a bird' s eye view of various perspectives in which service system entities can be people, businesses, non-profits, government agencies, and even cities. Service system is a dynamic interaction between providers, customers, ICT, and shared information that creates value between the provider and customer (University of Cambridge and IBM, 2008). Value and value creation are at the heart of service and are critical to understanding the dynamics of service systems and furthering service science (Vargo, SL, Maglio, P, 2008). If we see the ICT security through the eyes of service science, the new approach to enhance security and service for both user and ICT security provider would be introduced. The current model of ICT security is consisting of a provider and a user relationship. The user should integrate ICT security with

piecemeal fashion or buy the products and services through ICT integrators. In this model the user have difficulty to decide the current ICT security is effective compared to the investments. Table 2 shows some perspective to services (i.e. good dominant (G-D) logic, service dominant (S-D) logic and Nordic School Approach and New Service Development (NSD)). The service dominant logic has emphasis on dynamic and co-creation between stakeholders over the good dominant logic as static exchange values. NSD understand service as a process. Value co-creation is an active, creative, and social process based on collaboration between the provider and customer that is initiated by the provider to generate value for customers. These perspectives about service are not exclusive and are used to provide different, rich, and complementary angles to understanding service.

Table 2. Some perspective to service

Perspective/ Paradigm/ Logic	Good Dominant Logic	Service Dominant Logic Interpretative Consumer Research Consumer Cultural Theory	Nordic School Approach New Service Development (NSD)
What is service?	Service as an outcome (New kinds of service products or attributes)	Service as an experience (Valuable, subjective experiences in different events)	Service as a process (A new, well-functioning process)
Emphasis	Service is measured by attributes and variables in a functional domain.	Value is always co-created, jointly and reciprocally, in interactions among providers and beneficiaries	Value co-creation is an active, creative and social process based on collaboration between provider and customer
In what is value created?	Value-in-exchange	Value-in-context Value-in-experience	Value-in -use

As we explained the shortcomings of the current ICT security service, current mainstream of ICT security services is provided under the good dominant logic. If we approach ICT security services through service dominant logic, the difficulties of the current ICT security service could be examined through different angle. In order to change good dominant logic to service dominant logic in ICT security, we need a concept to invite security providers and its users onto a service platform. We call the concept as value orchestration platform (Kijima, K., 2012). The next section explains value orchestration management strategy.

2.1 Value orchestration Management Strategy and Business Model Canvas

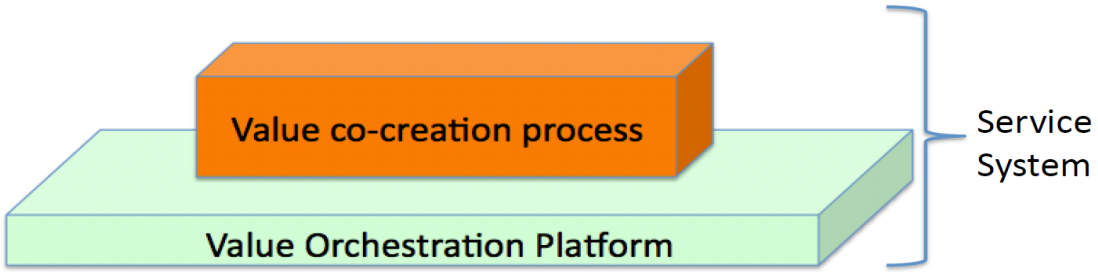

Figure 3 Value co-creation and Value orchestration

As shown in the figure 3, in the value co-creation process, customers and providers interact with each other and co-cerate new values. The other layers invite customers and providers to “get on board.” It facilitates and orchestrates new value co-creation by customers and providers, but leaves the control of the process entirely in the hands of providers and sometimes of customers as well. We call this layer the value orchestration platform. One of a practical ways to build value orchestration platform is to use the business model canvas (Osterwalder, A., 2004). Formal descriptions of the business become the building blocks for its activities. Many different business conceptualizations exist; Osterwalder's work and thesis (2004, 2010) propose a single reference model based on the similarities of a wide range of business model conceptualizations. With this business model design template, an enterprise can easily describe their business model. Figure 4 shows the business canvas. This simple canvas uses 9 building blocks to understand the way in which our chosen business actually works. The idea is to stick a giant copy of this on the wall and have people cover it in post its. Key offering within 9 blocks is Value Proposition : the collection of products and services a business offers to meet the needs of its customers. According to Osterwalder (2004), a company's value proposition is what distinguishes itself from its competitors. The value proposition provides value through various elements such as newness, performance, customization, "getting the job done", design, brand/status, price, cost reduction, risk reduction, accessibility, and convenience/usability. The value propositions (i.e. appropriate price and efficiency with overall customer experience and outcome) could be delivered through value orchestration platform.

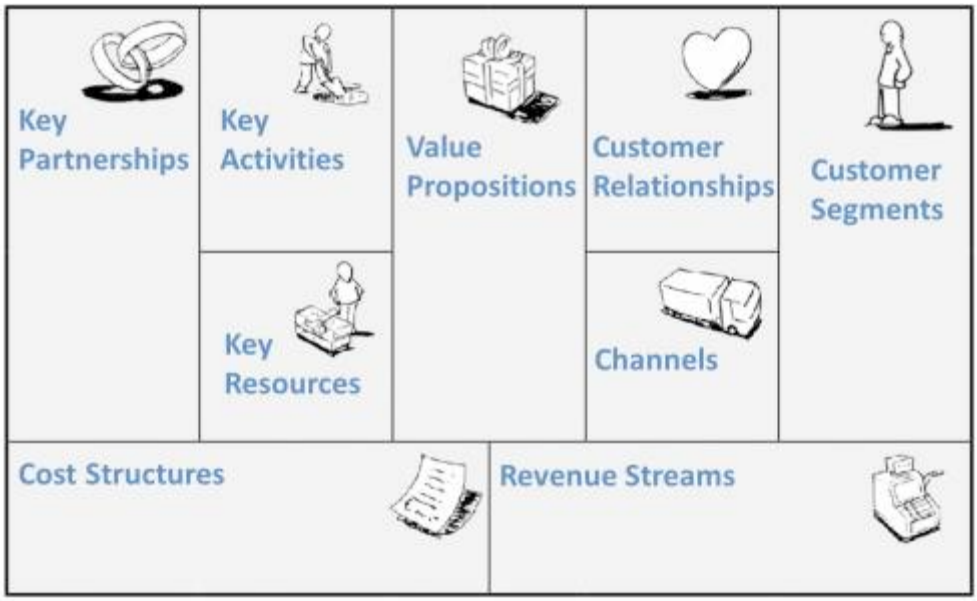

Figure 4 The business model canvas

While strategy for involvement of customers and provides focuses on how to attract customers and provides on the platform, value creation is essential for the platform to encourage customers and providers. In order to create value, data is a fantastic resource, volumes of data are exploding and with it, there is huge potential for tapping into the valuable insights it contains. Data curation is "gaining commercial and competitive advantage through the application of data." It's exploiting corporate data where ever it is held, fusing it with on-line, in-house and external data, to build a deep understanding of business and the opportunities it presents. By unlocking the potential of business data, organizations can make more informed decisions, drive marketing and sell more. Review each source, auditing its content to establish its currency and value. Understand what it the data means, not just individual fields of data, but in its entirety. Figure 5 explains where seeds from providers and needs from customers meet at very high level yields data curation which then evolve co-elevation and co-development. On the other hands, the traditional goods dominant logic area is the place where only data utilization is necessary.

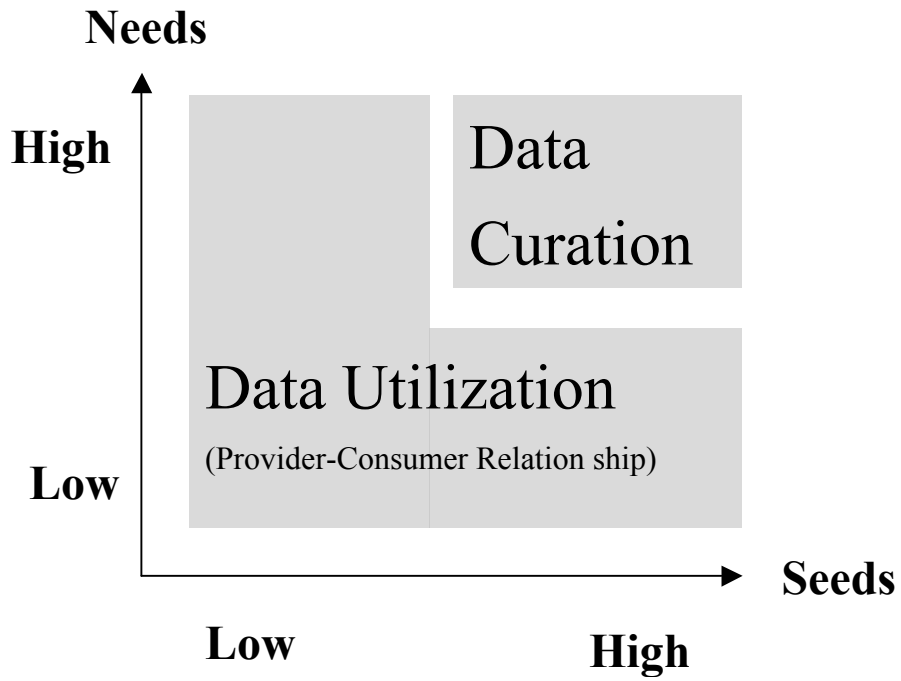

Figure 5 data curation and data utilization

In order to derive useful strategies to introduce value orchestration platform, we conduct a formal analysis based on simple mathematical model. We illustrate the model in terms of a shopping mall. Let us assume that the numbers of customers and merchants (providers) are m and n, respectively. In some cases m and n may be interpreted as an indicator of the variety of customers and providers, respectively. In case of e-commerce, we may assume that m and n substantially acquire any integers, thanks to current computation and database capabilities. Then, the benefit U that a customer gained by participation can be expressed by

$U = \alpha n - f$

where α is the utility for the customer obtained by using each tenant and f denotes the participation fee (e.g., registration fee). Symmetrically, we can represent the benefit V of a tenant by participation in the shopping mall by

$V = \beta m - g$

where β is the utility for the tenant by serving each customer and g expresses the participation fee (e.g., tenant fee). However, since m is determined by the benefit of the customers, we may assume

$m = F(U)$;

where F is an increasing function of U. This means that the higher the benefit to the customer is expected, the more customers will want to visit the shopping mall. By entirely symmetric arguments, we have

$n = G(V)$;

where G is an increasing function of V. Now, the platform's utility can be represented by

$P = m(f - c) + n(g - d)$;

where c and d are management/maintenance costs for taking care of customers and tenants, respectively. Our key question here is how the platform can maximize the utility P by assuming that their decision variables are f and g. By a simple calculation (refer to the Appendix), we are able to claim that the optimal f* and g* should satisfy these symmetric equations.

$f^* = c - \beta n + F/F'$ and $g^* = d - \alpha m + G/G'$

By observing them, we can derive the following propositions.

Proposition 1 (a below-cost strategy)

If βn is sufficiently large, then f* may be less than c. A symmetric statement also holds. The proposition suggests a below-cost strategy. Indeed, it implies that sometimes it is reasonable that the optimal f* is below the marginal cost c or that g* is below d to encourage customers or providers to join.

Proposition 2 (an asymmetric charging strategy)

If F' is large, then customers should be charged by a small fee. A symmetric statement also holds. A large F' implies that, even if the customer's benefit increases slightly, the number of customers can increase greatly. According to the proposition, if customers are much more valuable compared to tenants, it is reasonable for the platform to charge the tenants more than the customers. This suggests an asymmetric charging strategy, in that it encourages not balancing the sides of customers and providers to make the ICT security service system more attractive.

If we see the interaction between user and provider thorough the eyes of good dominant logic, the users approach is to seek products or services suitable for users' purposes with appropriate price. And the providers approach is to find out valuable customers and provide them with low cost manners. Figure 6 explains in this situation. In this two parties' model, the key activities in the business model canvas are to find out proper partner relationship with try and error basis. Therefore value proposition are limited in terms of a provider's specific services' scope itself without exploring other providers relations. On the other hand, if we see the interaction between user and provider thorough the eyes of service dominant logic, we introduce value orchestration platform as shown in figure 7. In the three parties' model, the key activities of the value orchestration platform in the business model canvas are to invite users and providers as many as possible on the platform. Using the value orchestration platform, two value propositions are derived as we explained using simple mathematical model in this section (i.e. a below-cost strategy and an asymmetric charging strategy). And moreover under this platform, a synergy between providers and users can be explored, users can maximize their ICT security system's performance with justified cost and providers can expand their business using the holistic view of total performance.

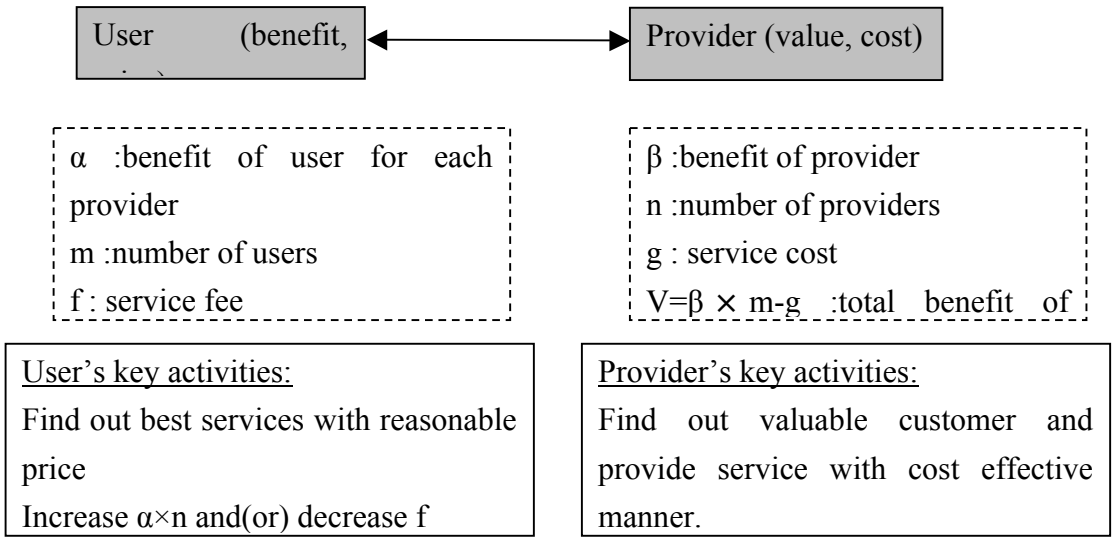

Figure 6 Two parties model

The benefit in this three parties' model (i.e. User, Provider and Platform) users and providers can perform better (i.e. f* and g* is lower than f and g respectively) than two parties' model in figure 7.

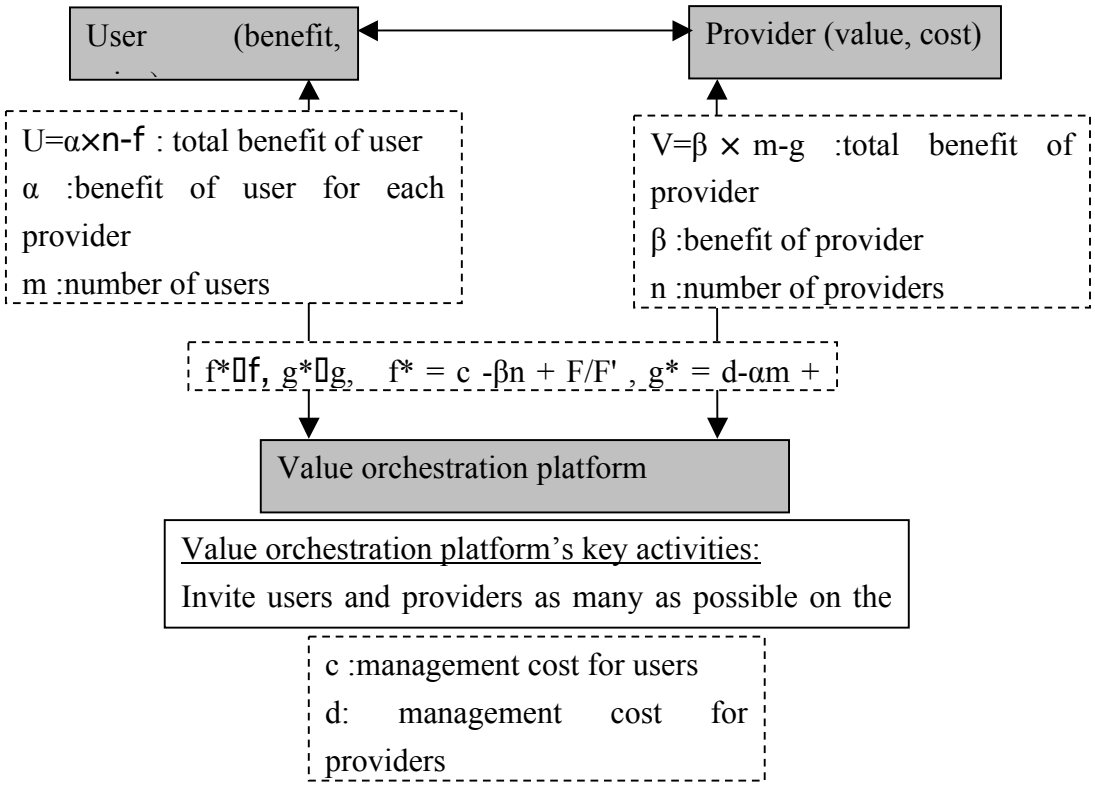

Figure 7 Three parties model

ICT SECURITY SERVICES AND VALUE ORCHESTRATION PLATFORM

ICT security and risk

The purpose and subject of attacker are expanding rapidly according to the recent security incidents as explained in the introduction (fig.2.). Sony and Mitsubishi heavy industries are the examples. Also the system boundary of ICT security is expanding in terms of the cause of security incidents and the measurement of the security. Traditionally the security measurement have been targeting to illegal conduct of security breach (i.e. narrow sense in figure 8), recently natural disaster, malfunction of ICT and human error are also taking into consideration (i.e. wide sense in figure 8). The increase of social dependence on ICT would have same impact whether those cause are intentional or non intentional (Sasaki, R, 2008). The situation requires holistic measures to manage security incidents. The other area is the movement to include reliability and safety on top of security in narrow sense. The concept of 'trust', which include security, reliability, privacy, availability, safety and usability, is proposed by Hoffmann, L.J. (2006). Figure 8 shows the situation.

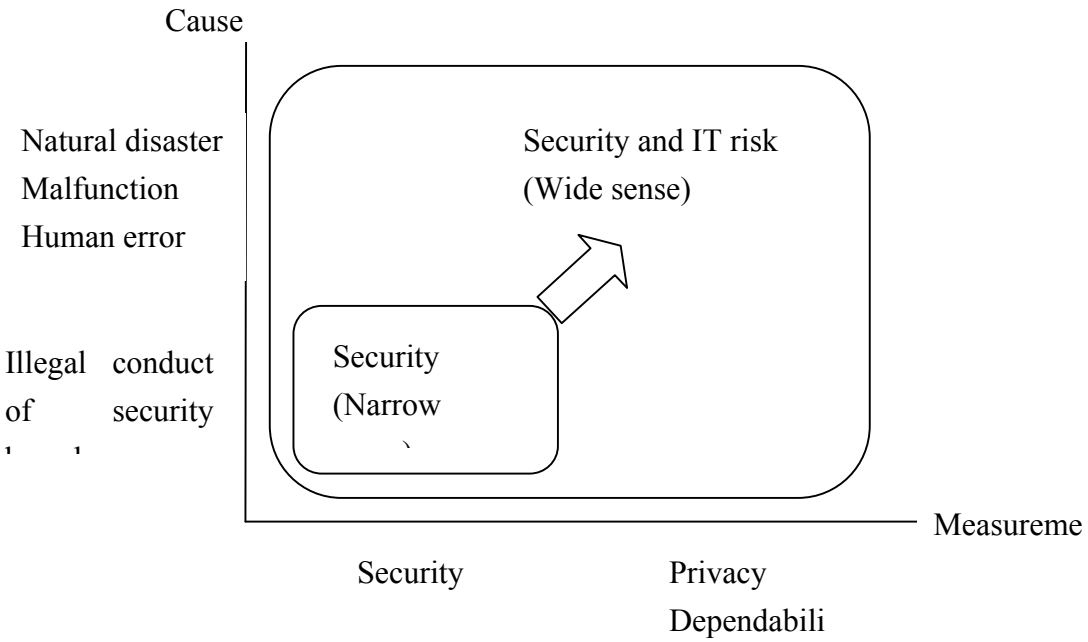

Figure 8 Expanding security scope

Value Orchestration Platform for ICT security service

As we mentioned in section 2, customers have to integrate various products, tools and services under two parties' model. This is an obstacle to maximize investments for there are no mechanisms to assess ICT security measure until customers receive security attacks. Also vendors have difficulty to customize user dependent functions on demand bases. Figure 9 shows security service as two parties' model and the trade off matrix is shown in the table 3.

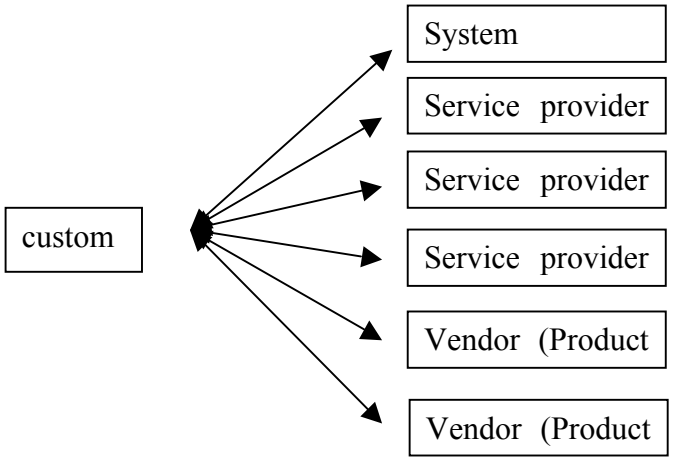

Figure 9 Two parties' model

	benefit	drawbacks
User	Self integration of ICT security system (fine tuning)	Hard to justify cost Piecemeal integration
Provider	Customize users needs	standardization

Table 3 trade off matrix of two parties' model

CSI (Computer Security Institute) conducted Computer Crime and Security Survey at 2010 and 2011, the year's survey results are based on the responses of 351 information security and information technology professionals in United States corporations, government agencies, financial institutions, educational institutions, medical institutions and other organizations. Their responses cover the security incidents they experienced and security measures they practiced from the period of July 2009 to June 2010. And one of their key findings is that the customers' requirement is something like the security service platform. When asked what security solutions ranked highest on ICT system owners wish lists, many respondents named tools that would improve their visibility—better log management, security information and event management, security data visualization, security dashboards and the like (CSI Computer Crime and

Security Survey 2010/2011). In order to satisfy those requests, we need three parities' model. We use some security standard as security service platform to invite customer and providers. We use 'Payment Card Industries Data Security Standard (PCI DSS)' as the value orchestrating platform in this paper. The PCI Security Standards Council offers robust and comprehensive standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements and support resources to help organizations ensure the safe handling of cardholder information at every step. The keystone is the PCI DSS, which provides an actionable framework for developing a robust payment card data security process including prevention, detection and appropriate reaction to security incidents.

The PCI DSS represents a common set of industry tools and measurements to help ensure the safe handling of sensitive information. Initially created by aligning Visa's Account Information Security (AIS)/Cardholder Information Security (CISP) programs with MasterCard's Site Data Protection (SDP) program, the standard provides an actionable framework for developing a robust account data security process - including preventing, detecting and reacting to security incidents. Due to a common set of industry tools and measurements, PCI DSS is widely used outside of the payment card industry.

Based upon the PCI DSS, the various products and services are mapped onto the PCI DSS. The user can easily find out their vulnerability of ICT security or excessive investments to the specific area by examining the map. Figure 10 explains the general concepts of the PCI DSS map. The PCI DSS map is not the whole platform but the mechanism to accumulate logs from various products and monitoring security attacking using overall logs information could find out vulnerability of the security system. This function enables to warn ICT administrators of potential security threat as proactive manner. These benefits could hardly be obtained from two parties' model. Using this value orchestrating mechanism, customer can maximize ICT security investments, vendors can concentrate their own expertise area and platform provider can handle security issues holistically and cost effective manners. Figure 11 is the three parties' model and table 4 is the trade off matrix.

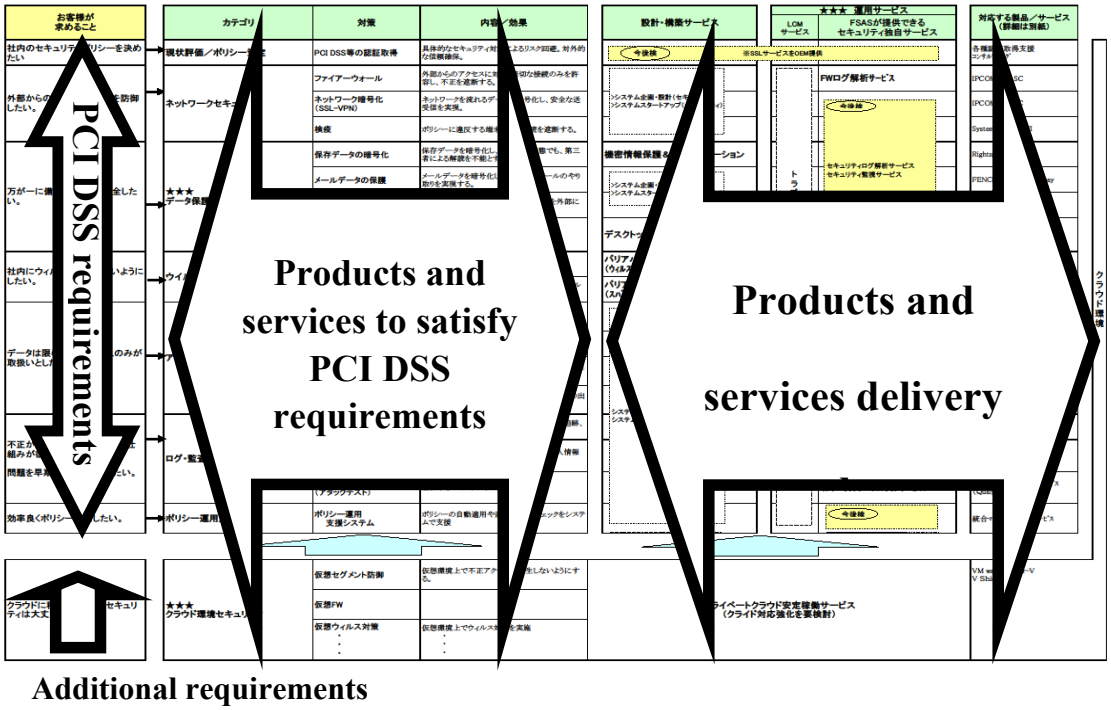

Figure 10 ICT security MAP as security platform

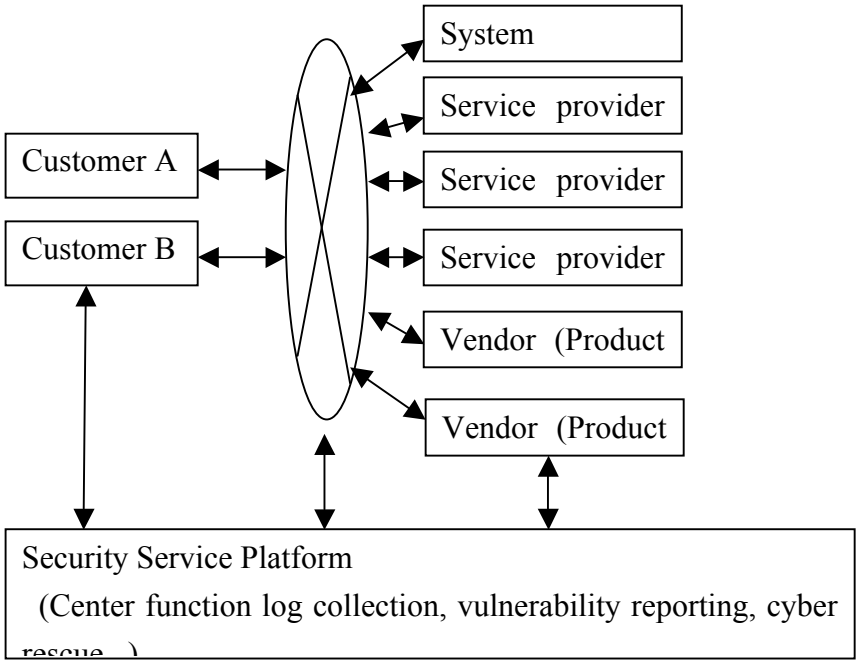

Figure 11 Three parties' model

	benefit	drawbacks
User	Maximize investments	
Provider	Concentrate on their own technical expertise area	
Platform	Bird's eye viewing security issues	Number of users and providers on the platform should exceed break even point.

Table 4 Trade off matrix of three parties' model

CONCLUSION

The concept of a value orchestration platform is general enough to explain various service systems. ICT security service is one of the applications of a value orchestration platform. The security is non- functional requirement, therefore customer tend to put a little focus on them. The traditional good dominant logic might not successful in the business scene. This paper provides the concept of the value orchestration platform for ICT security services. Figure 12 summarizes the transition from good dominant logic (G-D logic) to service dominant logic (S-D logic). Firstly, we survey the current ICT security market where products and services are interlinked complicated manner (fig. 1.). And we conceptualized this situation as two parties' model between customers and providers referring good dominant logic (fig. 9.). Then we use ICT security standard (i.e. PCI DSS in this paper) as security service platform (fig 10). This enables us to visualize current ICT security venerability or inappropriate investments. Therefore customers are easy to justify their ICT security investments and monitor ICT security vulnerability, otherwise customers have to do with piecemeal fashion. And we conceptualize this solution as three parties' model between customers, providers and security service platform providers referring service dominant logic (fig. 11.).

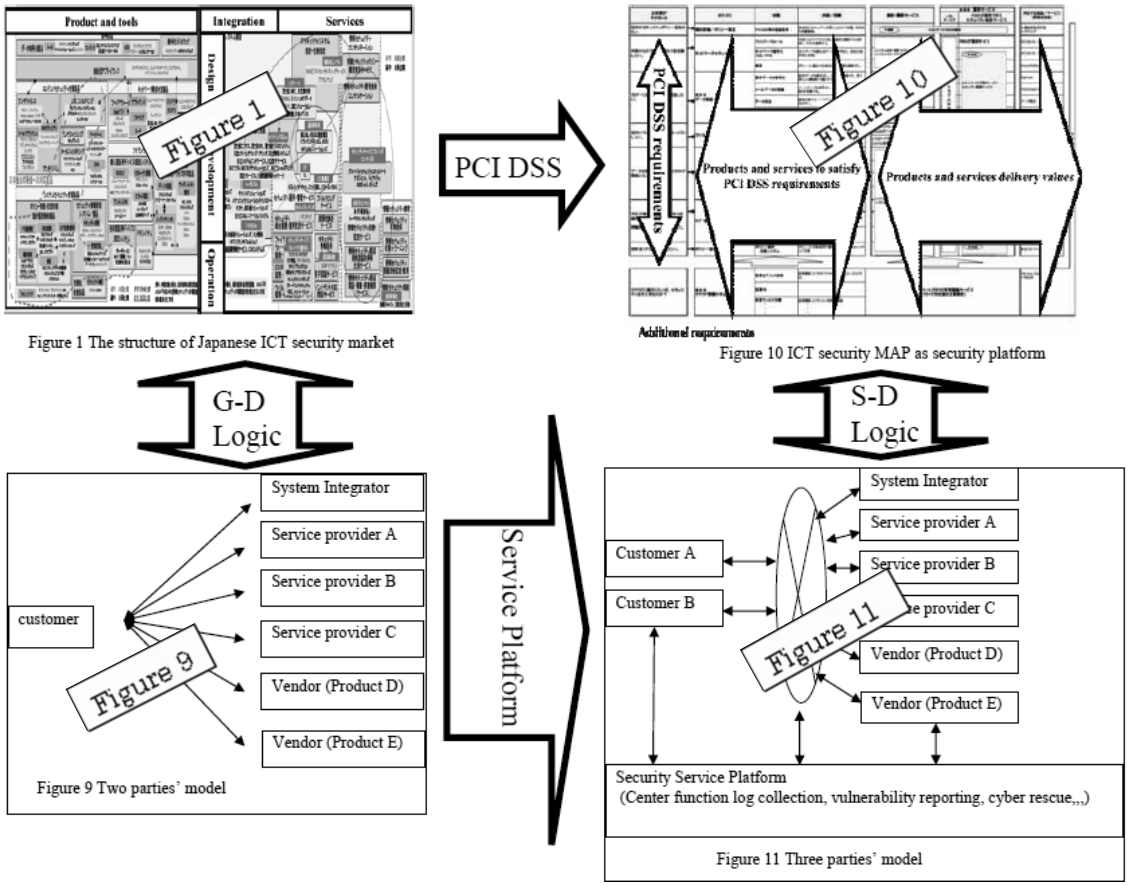

Figure 1 The structure of Japanese ICT security market

Figure 10 ICT security MAP as security platform

Figure 9 Two parties' model

Figure 11 Three parties' model

Figure 12 Summary of the transition from good dominant logic to service dominant logic

The service approach to ICT security area shows the potential benefits through enhancing security function effectively with appropriate investments. In this paper, the security service platform explained as PCI DSS map and the functions to integrate various logging information on to a server. However the scope of platform service provider (functions, methodology) should be elaborated further. Further research should be required to estimate the ICT security service model and the two proposition (i.e. a below-cost strategy and an asymmetric charging strategy) derived in section 2.1 should be confirmed in the real business scene.

REFERENCES

Barile, S., Spohrer, J. (2010) System Thinking for Service Research Advances. *Service Science.*

Cambridge. (2008). Succeeding through service innovation. *Cambridge White paper*, pages 1–33, June 2008.

Chesbrough, H., Spohrer, J (2006). A research manifesto for services science. *Communications of the ACM*, January 2006.

CSI Computer Crime and Security Survey 2010/2011, http://gocsi.com/survey, Apr. 2012.

Hoffmann, L.J., et al.(2006), Trust beyond security: an expanded trust model. Communications of the ACM, vol.49,No.7, pp.94-101.

IPA Japan (2011), 10 Major Security Threats, https://www.ipa.go.jp/security/vuln/documents/10threats2011_en.pdf, march 2011

Spohrer, J., Maglio, P.(2008). The emergence of service science: Toward systematic service innovations to accelerate co-creation of value. *Production and Operations Management*, 17(3):238–246, January 2008.

Kijima, K. (2012). Value Orchestration Platform for Value Co-creation. Frontier of service Systems Sciences, Tokyo, 2012, February

Klir, G. (2001). *Facets of Systems Science*. Plenum Press, New York, 2 edition.

Maglio, P. and Spohrer, J. (2008). Fundamentals of service science. *Journal of the Academy of Marketing Science*, January 2008.

Osterwalder, A. (2004). The Business Model Ontology - A Proposition In A Design Science Approach. PhD thesis University of Lausanne.

Osterwalder, A., Pigneur,Y., Smith, A. and 470 practitioners from 45 countries. (2010). Business Model Generation, A Wiley.

Sasaki, R. (2008). IT risk no kangaekata (in Japanese). Iwanami shinsyo.

University of Cambridge and IBM (2008). Succeeding through service innovation.

Vargo, SL, Maglio, P (2008). On value and value co-creation: A service systems and service logic perspective. *European Management Journal*, 26:145–152, January 2008.

Vargo, SL. (2009). Service-dominant logic as a foundation for service science: clarifications. *Service Science* 2009.

APPENDIX

The profit P is maximized when we have

$\partial P/\partial f=\partial P/\partial U\times\partial U/\partial f+\partial P/\partial V\times\partial V/\partial f=0$

and

$\partial P/\partial g=\partial P/\partial U\times\partial U/\partial g+\partial P/\partial V\times\partial V/\partial g=0$

where f and g are control variables for the platform owner.

It follows from

$P = F(U)(f - c) + G(V)(g - d)$

that

$$\begin{aligned}\partial P/\partial f&=\partial P/\partial U\times\partial U/\partial f+\partial P/\partial V\times\partial V/\partial f\\&=\partial P/\partial U\times(-1)+\partial P/\partial V\times 0\\&=-\partial P/\partial U\\&=0\end{aligned}\qquad(1)$$

On the other hand, since we have

$P = F(U)(f - c) + G(V)(g - d)$

$= F(U)(\alpha n - U - c) + n(\beta m - V - d)$

$= F(U)(\alpha n - U - c) + n(\beta F(U) - V - d);$

(1) implies

$$\begin{aligned}\partial P/\partial U&= F'\times(\alpha n - U - c) + F\times(-1) + n\beta F'\\&= F'\times(f - c) - F + n\beta F'\\&= 0\end{aligned}\qquad(2)$$

From (2) we have

$F'(f - c + n\beta) = F$

that is,

$F'f-F'(c-n\beta)=F$

or

$f^*= (c - n\beta) + F/F'$

A symmetric argument to

$\partial P/\partial g$

implies

$g^* = (d - m\alpha) + G/G':$