A Study on Evaluation Methodology of Cybersecurity Investment

石川, 朝久

https://doi.org/10.15017/1928635

出版情報：九州大学, 2017, 博士（工学）, 課程博士
バージョン：
権利関係：

Doctoral Dissertation

A Study on Evaluation Methodology of Cybersecurity Investment

Tomohisa Ishikawa

Department of Informatics
Graduate School of Information Science and
Electrical Engineering
Kyushu University

October 2017

Contents

Contents i

List of Figures v

List of Tables vii

Abstract viii

Abstract (Japanese) xii

Acknowledgments xv

1 Introduction 1
- 1.1 Backgrounds . . . 1
- 1.2 Motivation . . . 2
- 1.3 Related Works . . . 3
- 1.4 Challange and Contribution . . . 4
  - 1.4.1 Price of Personally Identifiable Information . . . 5
  - 1.4.2 Corporate Value Evaluation as an Intangible Costs . . . 6
  - 1.4.3 Effectiveness of Cyber Risk Insurance . . . 7

2 Overview of Security Strategy and Security Investment 9
- 2.1 Introduction . . . 9
- 2.2 Building Security Strategy . . . 9
  - 2.2.1 Step 1 : Building Security Standards . . . 9
  - 2.2.2 Step 2 : Analysis of the Status Quo . . . 10
  - 2.2.3 Step 3 : Risk Visualization . . . 10
  - 2.2.4 Step 4 : Building Roadmap . . . 11
- 2.3 Security Investment Effectiveness Evaluation . . . 11
  - 2.3.1 ROSI (Return On Security Investment) . . . 12
  - 2.3.2 TCO Minimization . . . 13
  - 2.3.3 Mathematical Approach . . . 14
- 2.4 Expected Damage Estimation . . . 14
  - 2.4.1 Tangible Cost Estimation . . . 14
  - 2.4.2 Intangible Cost Estimation . . . 17
- 2.5 Case Study . . . 20
  - 2.5.1 Case Study 1 : Target . . . 20

2.5.2 Case Study 2 : Home Depot 22

3 The Price of Personally Identifiable Information in Data Breach 24
3.1 Introduction 24
3.1.1 Attack Vector 24
3.1.2 Challange 25
3.1.3 Contribution 26
3.2 Compensation After PII Breach 27
3.2.1 The United States of America 27
3.2.2 Global Trends in Legislation and Regulations 28
3.2.3 Japan 29
3.3 JO Model 29
3.3.1 Value of Information Leaked 30
3.3.2 Degree of Social Responsibility of the Organization 31
3.3.3 Appraisal of Post-Incident Response 32
3.3.4 The Application of JO Model 32
3.4 Survey Research 34
3.4.1 Actual Trends in Compensation of PII Leakage 34
3.4.2 Gap Analysis between JO Model and Reality 37
3.4.3 Japanese Lawsuit Trends 39
3.4.4 The Comparison Between U.S. and Japan 40
3.5 The Challenge in PII Value and Concept 41
3.5.1 Searchability 41
3.5.2 Cancellability 42
3.5.3 Retrievability 42
3.6 Conclusion 43

4 Intangible Cost Estimation by Twitter Sentiment Event Study 44
4.1 Introduction 44
4.1.1 Motivation 44
4.1.2 Challange 45
4.1.3 Contribution 45
4.2 General Dataset Analysis 46
4.2.1 Stock Price Data Overview 46
4.2.2 Tweet Reputation Index Overview 46
4.2.3 Data Simlirality 47
4.2.4 Data Difference 48
4.2.5 Dataset Sumamry 50
4.3 Event Study Methodology 50
4.3.1 Terminology 50
4.3.2 Step 1: The Estimation of Theoretical Stock Price 51
4.3.3 Step 2: The Calculation of AR 52
4.3.4 Step 3: The Calculation of CAR 53
4.3.5 Step 4: The Statistical Test 53
4.4 Sentimental Analysis 54
4.4.1 Technology 54

4.4.2 Research Trends . . . 55
4.5 Proposed Model . . . 55
4.5.1 Terminology . . . 55
4.5.2 Module 1 : Tweet Gathering Module . . . 56
4.5.3 Module 2 : Sentimental Analysis Module . . . 57
4.5.4 Module 3 : TRI Calculation Module . . . 57
4.5.5 Event Study Analysis Module . . . 58
4.6 Experiment . . . 60
4.6.1 Case 1 : GMO Payment Gateway . . . 60
4.6.2 Case 2 : Correlation Analysis with Stock Price . . . 64
4.6.3 Case 3 : Applicability . . . 66
4.7 Conclusion . . . 68

5 The Effectiveness of Cyber Risk Insurance 70
5.1 Introduction . . . 70
5.1.1 Cyber Risk Insurance Market . . . 70
5.1.2 Challange . . . 72
5.1.3 Contribution . . . 72
5.2 Basics and Challenge of Insurance . . . 73
5.2.1 Insurance Mechanism . . . 73
5.2.2 The Challenge of Cyber Risk Insurance . . . 74
5.3 The Status Quo of Cyber Risk Insurance . . . 77
5.3.1 Coverage . . . 78
5.3.2 Premium . . . 80
5.3.3 Payment Claims . . . 80
5.4 Cyber Risk Insurance vs. Outsourcing . . . 81
5.5 Theoritical Assumption of Insurance Design . . . 83
5.6 Qualitative Analysis . . . 84
5.7 Quantitative Analysis . . . 85
5.7.1 Simulation Overview . . . 85
5.7.2 Model Building . . . 87
5.7.3 Simulation . . . 91
5.8 Results and Analysis . . . 91
5.8.1 Investment Constraint . . . 93
5.8.2 Average Relative Cost . . . 93
5.8.3 ROSI : Return On Security Investment . . . 93
5.8.4 Effectiveness Evaluation of Cyber Risk Insurance . . . 94
5.8.5 The Comparison with Actual Example . . . 95
5.8.6 Analysis from Insurance Company Sides . . . 96
5.9 Conclusion . . . 96

6 Conclusions 98
6.1 Concluding Remarks . . . 98
6.2 Future Issues . . . 99

Appendix 100

A Experimental Data of Proposed Event Study Methodology **101**
A.1 Introduction 101
A.2 Public Sectors Example 101
A.3 Side Effect Elimination 102
A.4 Standardized Cumulative Abnormal Return 104

Publications **106**

References **108**

Index **142**

List of Figures

2.1 Target Stock Price (from Yahoo Finance) 20

3.1 Economic Privacy Map 31
3.2 Simple EP Map 32
3.3 Compensation Cost Mapping 36
3.4 Total Compensation Cost Map 38
3.5 Gap Analysis Between Reality and JO Model Results 38

4.1 Timeline in Event Study 51
4.2 Abnormal Return / Cumulative Abnormal Return 61
4.3 The Comparison between Stock Price Data and Twitter Data . . . 62
4.4 The Comparison of Apache Struts2 Vulnerability Impact 64
4.5 The Comparison of Stock Price and Tweet Reputation Index 65
4.6 The Application of Non-Public Organizations (JTB) 67

5.1 Simulation Algorithm 92

A.1 Example : TRI-CAR of Saga Prefecture 102
A.2 Example : Side Effect Elimination 103
A.3 Standardized Cumulative Abnormal Return 105

List of Tables

2.1 Security Framework, Maturity Model, Best Practice, and Regulation 10
2.2 TCO Minimization Example - Security Investment Options 13
2.3 TCO Minimization Example - Approach 13
2.4 Security Damage Estimation Framework 15
2.5 Event Study Research Papers of Security Incident 18
2.6 Target Settlement in Class Action 21

3.1 Degree of Ease in Identifying the Individual 31
3.2 Degree of Social Responsibility of the Organization 32
3.3 Appraisal of Post-Incident Response 33
3.4 Configured Parameter in Benesse Corporation Incident 33
3.5 Configured Parameter in JINS Corporation Incident 34
3.6 Spontaneous Compensation 35
3.7 Average Price of Compensation (N=45) 37
3.8 Compensation Decided by Lawsuit 39
3.9 Average Price of Compensation (N=6) 39

4.1 Experimental Condition (GMO Payment Gateway) 61
4.2 The Comparison between Stock Price and Twitter Data 62
4.3 Correlation Analysis 1 : GMO (same as Table 4.2) 66
4.4 Correlation Analysis 2 : Nippon TV 66
4.5 Correlation Analysis 3 : Piped Bits 66
4.6 Correlation Analysis 4 : JINS 66
4.7 Experimental Condition (JTB) 67

5.1 Disclosed Damage Cost 86
5.2 Initial Parameter : Model Company 87
5.3 Initial Parameter : The existence probability of the vulnerability . . 88
5.4 Initial Parameter : Data Breach Decision Algorithm 88
5.5 Security Investment 1 : Security Assessment 89
5.6 Security Investment 2 : Cyber Risk Insurance 89
5.7 Breach Cost : Total Costs 90
5.8 Breach Cost : Incident Response Cost 90
5.9 Initial Parameter : Customer Liability (Compensation) 91
5.10 Initial Parameter : Customer Liability (Q&A) 91
5.11 Simulation Scenarios 92
5.12 Experiment Results (Unit : cases, 1 million JPY) 93

5.13 Experiment Results (Unit : cases, 1 million JPY) 94
5.14 Insurance Coverage Ratio & Insurance ROSI 95

A.1 Experiment Condition 103
A.2 Experiment Target 104

Abstract

Since cybersecurity incidents happened every day, the senior management team has recognized that cybersecurity issue is not IT issue, but a management issue. Also, they have recognized that the implementation of countermeasures is critical. As long as each organization implements appropriate security controls by following the guidelines or regulations, many security incidents are preventable. However, we do not have any reasonable standards to decide the amount of security investment, and it is one of the challenges in cybersecurity strategy.

To validate the appropriateness of cybersecurity countermeasures, we need to estimate expected damage cost by using the model or past examples. We need to consider not only "Tangible Cost" such as an investigation or customer follow-up cost, but also "Intangible Cost" such as the decline of corporate value, customer loyalty, and corporate branding. From research fields of the evaluation methodology in cybersecurity investment, we pick up three critical challenges as follows.

The first challenge is the gap between real compensation value and theoretical value. In 2003, "JO model" was formulated, and it has been a benchmark for calculating the compensation cost of the personally identifiable information breach. The background of this model had three reasons. Firstly, the Supreme Court decided the compensation price in a lawsuit case in 2002. Secondly, "Act on the Protection of Personal Information" was published in 2003. Thirdly, many victimized companies hesitated to disclose detailed information about security incidents. On the contrary, a security breach in 2003 became the defacto-standard to pay 500 JPY coupons for the data breach, and this has led to making the disparity between model and the reality.

The second challenge is that we do not have an approach to evaluate corporate value impact in security incidents for the companies not having stock price data, although event study methodology by using stock price data is a well-known approach. This known method assumes that stock price means corporate value, and calculates Cumulative Abnormal Return (CAR) for understanding short-term impact by the security incident. It is powerful, but we need a new method since we cannot apply the traditional method to the organizations not having stock price data such as private companies, government agencies, and non-profit organizations.

The third challenge is that we do not have enough analysis about the effectiveness of cyber risk insurance. Cyber risk insurance is a typical risk transfer approach, but the mechanism, risk assessment, and deployment of cyber risk insurance are in dawning age. Also, we cannot use traditional actuarial science approach. Because of this situation, the effectiveness of cyber risk insurance is controversial. However, cyber risk insurance is powerful since it makes volatile incident cost to fixed cost, and it will become a more valuable solution. Therefore, we need to analyze the effectiveness of cyber risk insurance by using simulative approach.

This doctoral dissertation is organized as follows.

Chapter 1 shows the background and motivation of evaluation methodology of cybersecurity incidents. In addition to this, we discuss the academic challenges and our contributions to this area.

Chapter 2 presents the background knowledge and related works about investment evaluation methodology in cybersecurity and cost estimation methods. By analyzing the previous works, we identify the academic challenge and their backgrounds.

In Chapter 3, by case study analysis about the compensation of personally identifiable information, we have three major contributions in this area. Firstly, we analyze 45 cases of Japanese personally identifiable information leakage, and we find that the value of average spontaneous compensation is 543 JPY, and

the theoretical value by JO model is 60 times higher than this average price. Secondly, we did case study analysis about lawsuits in Japan and U.S. In Japan, the compensation is more than 5,000 JPY in Japan, although one in U.S. is averagely less than one dollar. We think Japanese compensation value is averagely higher than U.S., and we find that it is caused by the difference of compensation style. Thirdly, we analyze how to handle personally identifiable information in the current situation, and we point out three data characteristics model should include.

In Chapter 4, we propose new corporate valuation method by defining the value named Tweet Reputation Index (TRI), to evaluate targeted organizations instead of stock price in security incidents. Tweet Reputation Index is a cumulative emotion value against the targeted entities by unit time after performing sentiment analysis against Tweets related to them. As same as stock price data, we calculate Cumulative Abnormal Return(TRI-CAR: Tweet Reputation Index Cumulative Abnormal Return) from this Tweet Reputation Index, and we can estimate the event impact on corporate value. As case studies by applying this method, we have two contributions. Firstly, with the analysis of public enterprises, we demonstrate our approach, and we confirm high correlations (Correlation Coefficient: +0.8) between stock price data and Tweet Reputation Index in short-term (3 days before and after the Event Day) by analyzing both data. Secondly, we apply this method to the non-public organization not having stock price data, in order to prove the applicability of our proposed approach.

In Chapter 5, firstly, we analyze the mechanism, current service, and challenge of cyber risk insurance from the technical and economic perspective. Secondly, we have cost-benefit analysis from the quantitative perspective. Since the result of simulation will be changed based on the risk scenario such as the occurrence of information leakage or the number of leaked data, we performed analysis by using Monte-Carlo simulation. In the case study by using virtual companies, we acquire the result that ROSI（Return on Security Investment） is approximately 200 times, and the coverage of cyber risk insurance is approximately 65%. We

conclude that cyber risk insurance is beneficial for security management and risk management perspective.

Chapter 6 shows our conclusion and further research issues.

Abstract (Japanese)

サイバーセキュリティ事故は毎日のように発生しており、サイバーセキュリティはIT の問題ではなく、経営マネジメントの問題と認識され、対策の推進が重要とされる。セキュリティ対策は、ガイドライン・規制を参考に適切に実装すれば、その多くを予防可能である。しかし、セキュリティ対策をどこまで実施すればよいか投資基準は明らかでなく、セキュリティ戦略上の課題である。

セキュリティ投資の妥当性を検証するため、モデル・過去事例を通して妥当な想定被害額の算出が重要となる。調査費用や顧客対応費用など「有形コスト」（Tangible Cost）のみならず、企業価値・ブランディング低下など「無形コスト」（Intangible Cost）についても検討が必要である。本論文では、セキュリティ投資評価手法に関して次の重要な 3 つの課題を研究した。

第一に、個人情報漏洩時の賠償価格について、理論モデルの算出価格と実際に訴訟・自主的な「お詫び」を通じて支払われる金額に乖離がある。2003 年に「JO モデル」が定式化され、個人情報漏洩時の賠償価格を算出するベンチマークが提案された。この背景には、2002 年に関する個人情報漏洩の賠償金の判例が出たこと、2003 年に個人情報保護法が制定されたこと、事故情報の開示件数が非常に少ないことが挙げられ、現在でも利用されている。一方、2003 年の情報セキュリティ事故を前例に、事故発生時には 500 円の金券を送付することが慣習化された。

第二に、セキュリティ事故発生時における企業価値への影響を評価する手法として、株価の時系列情報を利用したイベント・スタディ手法が知られているが、株価を持たない企業には応用ができないという課題が存在する。この既存手法は、「株価が企業価値を示す指標である」という前提の下、イベント前後の株価の変動に注目して「累積異常変化率」を算出し、イベントが株価にもたらす短期的影響を分析する方法である。しかし、非上場企業などに応用できないため、既存手法

の応用範囲の観点から改善が必要となる。

第三に、「サイバー保険」について、投資の有効性分析が十分に行われていない。保険は代表的なリスク転移手法であるが、サイバー保険の制度設計・導入の黎明期であるため、伝統的な保険数理手法が使えず、有効性・費用対効果について様々な意見・議論がある。しかし、変動性の高い費用を固定化する「サイバー保険」は、今後より重要になると推測される。様々な条件を入力して評価を実施できる手法を採用し、現時点での有効性を示す必要がある。

本学位論文は以下のように構成される。

第 1 章では、本研究の背景と目的を述べる。また、本研究の主要な課題と貢献についても論じる。

第 2 章では、セキュリティ投資評価手法と被害額推定手法に関する背景知識と既存手法について説明する。既存研究を体系的に整理することで、上記で挙げた研究課題を抽出した。

第 3 章では、第一に日本における個人情報漏洩事件 45 件の事例分析を行い、企業が金券・商品券を送付した平均金額が 543 円であり、JO モデルの理論値と 60 倍以上の差異があることを示した。第二に、米国と日本における訴訟について事例分析を行った。日本では賠償金額が 1 名当たり平均 5,000 円以上である一方、米国では平均 1 ドル以下であることを突き止め、日本の賠償金額が平均的に高いこと、および賠償に対する考え方の違いを論じた。第三に、個人情報の取り扱われ方の変化について検討を行い、モデルが改善すべき点について「検索容易性」、「変更容易性」、「回収容易性」という 3 つの特徴を指摘した。

第 4 章では、株価の代替として、「ツイート感情指数」を定義し、インシデントによる企業価値への影響を測定する手法を提案した。「ツイート感情指数」とは、調査対象企業のツイートに対して感情分析を行い、数値化されたデータを単位時間毎に累積した値である。この「ツイート感情指数」の時系列情報に対して、イベント・スタディ手法を適用し「累積異常変化率」を算出することにより、インシデントの影響を分析する。事例分析では以下の結果を得た。第一に、上場企業の株価・「ツイート感情指数」の両時系列情報に対してイベント・スタディを実施し、短期間（イベント日前後 1 日を含む計 3 日間）の範囲で、両時系列情報に相

関係数 0.8 以上の強い相関性があり、「ツイート感情指数」が株価の代替として利用可能であることを示した。第二に、非上場企業の事例について考察を行い、企業価値の影響を測定できることを示した。

第 5 章では、第一にサイバー保険の仕組み・現状・課題について、技術的・経済学的の観点から分析を実施した。その後、具体的な想定事例を元に、定量的な費用便益分析を実施した。情報漏洩の発生確率や漏洩件数など想定シナリオにより結果が変化するため、モンテカルロ・シミュレーションを利用して考察を行った。被害コストの公開事例に基づく仮想企業の事例では、投資対効果は約 200 倍、保険の被害額カバー率は約 65%という結果となり、サイバー保険が被害額を抑え、有効性があるという結論を得た。

第 6 章では本研究の結論を述べ、今後の研究課題について論じる。

Acknowledgement

I would like to thank all the researchers and colleagues who helped me in this thesis. Especially, I would like to thank my supervisor, Professor Kouichi Sakurai, who has supervised me for years and provided me valuable discussions, critics, and advice at any time. Also, I would like to express my gratitude to Associate Professor Daisuke Ikeda and Associate Professor Shingo Saito because they provide valuable comments and advice to my doctoral dissertation. In addition to this, I thank my external advisor Dr. Naohiko Uramoto and Professor Masakatsu Nishigaki, who gave me helpful suggestions to my research paper, and Professor Reiko Aoki had insightful comments. Lastly, I would like to thank Dr. Mike David and Mr. Kurt Sauer for helping my doctoral dissertation in English perspective.

I would like to thank my all supervisors and colleagues in my workplace, who provided tremendous knowledge and skills of cybersecurity, much valuable support, and a lot of challenges. In addition to this, I would like to offer my special thanks to all friends in infosec community since I have always acquired cutting-edge knowledge from practical and academic perspective.

Lastly and most importantly, I wish to thank my loving and supportive my wife, Nagisa, and my wonderful daughter, Rin, who provide tremendous support and unending inspiration.

Chapter 1

Introduction

1.1 Backgrounds

Information breach and unauthorized attack are continuously happened, such as the serial security attack to SONY group by Anonymous and LulzSec in 2011 [1], serial APT attack to Blue Cross in 2014 [2–5], breach from governmental office [6–8], private company [9], SNS [10], and cybersecurity is one of the serious risks for each organization. In Keynote of RSA Conference USA 2015 [11], RSA President, Mr. Amit Yoran named these situations as "Dark Age".

Because of these situations, security management has been considered to be important. In order to response these requests, there are many documents, framework and maturity model, describing the best practice of security management, have been released by authorized organizations. On top of that, industry group or public administration office tends to provide standards and regulations, such as PCI-DSS [12], NYDFS Cybersecurity Regulation [13], or MAS Technology Risk Management [14], to maintain appropriate security maturity. According to research by National Policy Agency (hereinafter NPA) [15], 98.5% of organizations answered "implementation of security control is necessary", and 61.7% of organizations responded "Our organization should have an investment actively to information security".

Originally, cybersecurity was an IT problems, but currently, cybersecurity is acknowledged as one of management risks. According to "Global Risk Report

2015" of World Economic Forum [16], cyber attack, and data leakage is a high-risk issue from possibility and impact. Also, leading credit rating agency, Standard & Poor's, announced that the companies that do not have appropriate security countermeasure might be downgraded although they do not have security incidents [17]. In addition to this, METI (Ministry of Economy, Trade, and Industry) and IPA (Information Processing Agency) released the security guideline, "Cybersecurity Management Guidelines" [18] for senior management, and it clearly mentioned the necessity of security investment as a management strategy and the responsibility of senior management team. From this tendency, security management has been one of the business challenges offered by markets.

1.2 Motivation

The majority of security incidents can be avoidable when each organization implements necessary security controls in best practice and appropriate operation process, that will be mention in Table 2.1. However, from business process and cost perspectives, it is difficult to implement and manage all security control, and also, it requires huge budgets. In addition to this, the effective security investment concept has not been released or authorized yet. According to NPA survey [19], 51.3% answered "it is difficult to identify minimum standards of security control", 47.3% answered that "it is difficult to know cost-effectiveness of each security control", and 42.5% answered that "security control takes too many costs". Also, 35.4% of companies answered "not using security services" and 43.7% of them answered "only limited budget for IT security", 32.9% answered "security control cost is inappropriate".

It is a common problem around the world. For example, PwC report [20] mentioned that many organizations struggled to understand how much cost each organization needs to spend on security and how to determine the return on investments of their security outlay. Also, British Government research report [21]

revealed that 24% of small and midium-sized enterprise (hereinafter SME) mentioned that security was too expensive and 22% answered that they "don't know where to start". Therefore, we think it is a challenging topic to propose the methodology to judge and evaluate security investment from a realistic and practical perspective as the security strategy.

On top of that, in the white paper "The Second National Strategy on Information Security" [22] published in 2009 by NISC (National Information Security Policy Council), this document proposed a keyword "Accident Assumed Society", and the direction of security control measure has been changed. According to NIST security framework [23], security countermeasures are categorized into five categories including, Identification, Prevention, Detection, Response, and Recovery. Before 2009, typical Japanese companies focused on identification and prevention, but recently, from a security perspective, these companies tended to shift the focus of security investment to post-countermeasure including detection, response, and recovery. Based on this, these companies started to calculate the cost of security incidents seriously and the framework about security investments as if security incidents is necessary.

1.3 Related Works

Security investment is a critical phase for building security strategy. In chapter 2, we will show three critical issues to understand the current view of this area.

Risk Visualization and Quantification Methodology

Building corporate security strategy is a critical part of security improvement, but risk visualization and quantification is the pre-requisite to consider security investment. In Chapter 2, we will show general steps of creating security strategy in business fields and risk visualization and quantification methodology.

Security Investment Effectiveness Evaluation

CISO and security team need to show the effectiveness of security investment against visualized risks and gain the approval by senior management team. Especially, the research related to IT security investment evaluation methodology is theorized based on the knowledge of other areas such as IT investment evaluation theory and corporate valuation methodology. In Chapter 2, we can show the current research methodology. The basic idea is the comparison of expected damage between having security investment and not having security investment, and verify the effectiveness of investments.

Expected Damage Estimation

In the effectiveness evaluation process of security investment, the most important issue is how to estimate the expected loss. Since effectiveness evaluation is entirely dependent on this assessed value, we need to pursue the accuracy as soon as practical. In Chapter 2, we will show current research and challenge.

1.4 Challange and Contribution

One of the general challenges of this area is how to estimate expected damage cost and the possibility of occurrence. Generally speaking, the companies having the experience of security incident do not tend to disclose the detailed costs of security incidents, and this tendency prevents the researchers from improving the algorithm of expected damage cost. From public information, the only way to know the cost is seeing an extraordinary loss in a financial report. Therefore, since we have only limited data, it is difficult to have analytical and mathematical decision-making from these data.

Based on this situation, we can see following specific issues for considering security investment.

1.4.1 Price of Personally Identifiable Information

The first challenge is the gap between real compensation value and theoretical value. In 2003, NPO Japan Network Security Association (hereinafter JNSA) formulated JO model (JNSA Damage Operation Model for Individual Information Leak), and it has been a benchmark for calculating the compensation cost of personally identifiable information. The background of formulating this model was three reasons. Firstly, on July 11, 2002, the Supreme Court judged that Uji City had to pay 15,000 JPY as compensation [24] (Technically, 10,000 JPY is for solatium, and 5,000 JPY is for the compensation coverage of legal cost.) Secondly, in 2003, "Act on the Protection of Personal Information" [25] was published, and it was likely to increase the awareness of protecting personally identifiable information. Thirdly, the detailed information related to cybersecurity incidents had not released during this period. From these reasons, JNSA tried to create calculation model of personally identifiable information, and it has been a great resource to consider the leakage. On the contrary, in 2003, Lawson, leading retail chain, leaked 560,000 records of personally identifiable information, and they proactively decided to send 500 JPY gift certificate to all 1.15 million exclusive customers including the customers who were not victims of this breach. Based on this example, many companies those leaked customer information referred this case, and 500 JPY coupons became a defacto-standard price of data breach cases in Japan. We think this current situation has the difference from theoretical JO model.

In Chapter 3, by case study analysis about the compensation of personally identifiable information, we have three major contributions in this area. Firstly, we analyze 45 cases of Japanese personally identifiable information leakage, and we find that the value of average spontaneous compensation is 543 JPY, and theoretical value by JO model has more than 60 times gap from this average price. Secondly, we have case study analysis about lawsuit case in Japan and U.S. In Japan, the compensation is more than 5,000 JPY in Japan, although one in U.S. is

averagely less than one dollar. We think Japanese compensation value is averagely higher than U.S., and we find that it is caused by the difference of compensation style. Thirdly, we analyze how to handle personally identifiable information in the current situation, and we point out three data characteristics that model should include. The first factor is "Searchability". Many people recently tend to open the primitive personally identifiable information to SNS platform and attackers can gain them without any security breach. The problem is, by the information leakage, attackers or the meddling third party can link the breached data (the data users do not want to disclose such as porn history data or purchase history) to disclosed data in SNS. We think this undesirable linkage is one of the keywords for improving the model. The second factor is "cancellability", and it means that some data such as password can be changeable after information breach although some information such as date of birth can not be. We consider the lifecycle of data is one of the important factors. The last element is "Retrievability, " and it means the possibility of the prevention of leaked information proliferation. In the case of internal fraud, it is easy to prevent the spread of leaked data because police or investigation organization can take over the data. However, it is difficult to remove the information online as we learned in Winny case.

1.4.2 Corporate Value Evaluation as an Intangible Costs

The second challenge is that we have the limited approaches to evaluate the impact of corporate value in security incidents for the companies that do not have stock price data. As the evaluation method of corporate value impact by security incidents, the application of event study methodology by using stock price data is a modern approach. Event study methodology is analyzing the short-term impact to corporate value by an event, such as M&A announcement or new product release, by examining the volatility of stock price before and after the event and calculating the Cumulative Abnormal Return (hereinafter CAR). CAR allows us to have the quantitative analysis of corporate value impact. The assumption of

this approach is that market capitalization calculated by stock price means the corporate value. In related works, many researchers apply this methodology to analyze information security incidents and to examine the short-term impact on corporate value. However, this method is entirely dependent on the stock price data, and we think it is a challenge that we cannot analyze the various cases. For example, we can not examine the organizations, which do not have stock price data such as private companies and governmental agency.

In Chapter 4, we propose new corporate valuation method by defining the value named Tweet Reputation Index (hereinafter TRI), to evaluate targeted organizations instead of stock price in security incidents. Tweet Reputation Index is a cumulative emotion value against the targeted entities by unit time after performing sentiment analysis against Tweets related to them. As same as stock price data, we calculate Cumulative Abnormal Return (hereinafter TRI-CAR: Tweet Reputation Index Cumulative Abnormal Return) from this Tweet Reputation Index, and we can estimate the event impact on corporate value. As a case study by applying this method, we have two contributions. Firstly, with the analysis of public enterprises, we demonstrate our approach, and we confirm high correlations (Correlation Coefficient: +0.8) between stock price data and Tweet sentiment data in short-term (3 days before and after the Event Day) by analyzing both data. Secondly, we apply this method to the non-public organization not having stock price data, in order to prove the applicability of our proposed approach.

1.4.3 Effectiveness of Cyber Risk Insurance

The third challenge is that we do not have enough quantitative analysis about the effectiveness of cyber risk insurance that is a new risk finance method. Cyber risk insurance is a typical risk transfer approach, but the mechanism and deployment of cyber risk insurance are in dawning age. In addition to this, the occurrence of cyber risk is different from other hazards. We can not use traditional actual science approach, and insurance companies are now considering the cyber risk

assessment method. However, since the awareness of cyber attack is increasing, the cost for incident response will be large in the future. Therefore, the cyber risk insurance will be a more valuable solution since cyber risk insurance makes the volatile incident cost to fixed cost. Therefore, we think we need to analyze the effectiveness of cyber risk insurance by using simulative approach.

In Chapter 5, we evaluate the effectiveness of cyber risk insurance from the quantitative perspective. Firstly, we analyze the mechanism, current service, and challenge of cyber risk insurance from the technical and economic perspective. Secondly, we have cost-benefit analysis from the quantitative perspective. Since the results of simulation will be changed based on the risk scenario such as the occurrence of information leakage or the number of leaked data, we have the analysis by using Monte-Carlo simulation. The benefit of this model is we can add and modify the initial parameters based on the risk preference and risk scenario. In the case study by using a virtual company, we acquire the result that ROSI （Return on Security Investment） is approximately 200 times, and the coverage of cyber risk insurance is approximately 65%. We conclude that cyber risk insurance is beneficial for security management and risk management perspective.

Chapter 2

Overview of Security Strategy and Security Investment

2.1 Introduction

As we mentioned in Chapter 1, security investment is a very critical phase of building cybersecurity strategy, and it is not an IT issue but a corporate management problem. Since security countermeasure cannot contribute the profitability of organizations, CISO and security team have to prepare a comprehensive security strategy in order to justify the investment. In this chapter, we show current methodology and research of building security strategy, security investment effectiveness evaluation, and expected cost estimation.

2.2 Building Security Strategy

According to the research paper by NRI [26], a leading IT consulting firm in Japan, when we consider the security strategy in the business field, we have following steps.

2.2.1 Step 1 : Building Security Standards

As Step 1, we prepare the goal and security standards by using various documents as we show in Table 2.1. It is a critical phase because we need to define the goal and objectives. One of the important things at this stage is understanding the characteristics of each best practice document because each document has different scope, granularity, and depth of descriptions.

Table 2.1: Security Framework, Maturity Model, Best Practice, and Regulation

No.	Security Framework	Reference
1	ISO 27001/27002	[27]
2	CIS Critical Security Controls	[28]
3	NIST Cyber Security Framework	[23]
4	ISF Standards of Good Practice for Information Security	[29]
5	Payment Card Industry Data Security Standard (PCI DSS)	[12]
6	NYDFS Cyber Security Regulation	[13]
7	NIST SP800 Series	[30]
8	Australian Government - The Protective Security Policy Framework	[31]
9	ASD Australian Government Information Security Manual	[32]
10	ASD Strategies to Mitigate Cyber Security Incidents	[33]
11	MAS Technology Risk Management	[14]
12	FFIEC Cybersecurity Assessment Tool	[34]
13	Cybersecurity Capability Maturity Model (C2M2)	[35]
14	HITRUST Cyber Security Framework	[36–38]
15	FISC Security Guideline	[39]

2.2.2 Step 2 : Analysis of the Status Quo

Secondly, we analyze the status quo from various perspectives such as 4P (Policy, Product, Process, People) or management resource (Human Resource, Goods, Budgets, Time, Information). Regarding analysis technique, there is a different method such as questionnaire, documents evaluation, interview, onsite review, and cyber fire drill, but we need to have a balance between cost and analysis accuracy.

2.2.3 Step 3 : Risk Visualization

After collecting the various information of current environment, we can visualize risk. One of the usual approaches is known as baseline approach. It is the gap analysis by comparing between defined standards (baseline) and current status. In many cases, we typically use metrics technique (risk quantification) approach or risk scenario approach. Especially, risk scenario approach is very powerful since it visualizes how current security control mechanism can stop the threat from

Defense-In-Depth perspective.

2.2.4 Step 4 : Building Roadmap

Finally, we build a roadmap and the plan of security investment. Based on visualized risks, we consider the options for security investment and the effectiveness. In building roadmap phase, one of the critical concepts is risk treatment strategy. Risk treatment strategy is how to treat the risk based on the risk impact and risk preference. There are four strategies including **Risk Avoidance**, **Risk Mitigation**, **Risk Transfer**, and **Risk Acceptance**. We need to classify the identified risks based on these categories.

In addition to this, from a financial perspective, **Risk Finance** is also important and ISO 31000 [40] defines this keyword and shows two options named **Risk Acceptance** and **Risk Transfer**. Risk Acceptance means accepting the risks and preparing the retained earnings for the future security incidents. On the contrary, Risk Transfer implies transferring the risk to the third party by using insurance. Cyber risk insurance, which is recently notable, is one of the practical options in risk finance context.

2.3 Security Investment Effectiveness Evaluation

The methodology of security investment effectiveness evaluation is one of the critical activity since CISO and security team need to explain the effectiveness and gain the approval of security investment. The basic idea is the comparison of expected damage between having security investment and not having security investment, and verify the effectiveness of investments. Many research papers apply the knowledge of other areas such as IT investment evaluation theory and corporate valuation methodology. In following parts, we show various methods proposed by related research papers.

2.3.1 ROSI (Return On Security Investment)

One of the popular frameworks is ROSI (Return On Security Investment). Originally, this ROSI idea is from CBA (Cost-Benefit Analysis) approach in accounting domain. This idea is a simple, but a very powerful concept. According to ENISA reports [41], ROSI is defined as follows.

$$ROSI = \frac{Loss\ Reduction - Security\ Investment}{Security\ Investment} \tag{2.1}$$

"Loss Reduction" means that expected loss reduction by security investment. "Security Investment" means the monetary cost of security investment including initial cost, operation cost, learning cost, and process reforming cost. According to this definition, as long as ROSI is larger than 1, we can determine that these options are cost-effective.

On top of that, "Loss Reduction" is defined as follows when we apply ALE (Annual Loss Expectancy) theory. ALE approach is estimating risks based on an annual basis. It was proposed in 1975 by the National Bureau of Standards in Federal Information Processing Standard 65, "Automatic Data Process Risk Analysis" [42].

$$Loss\ Reduction = ALE - mALE \tag{2.2}$$

Annual Loss Expectancy (ALE) is a monetary loss that can be expected from a particular risk on a specific asset in one year. **mALE** means "modified ALE" by security investment. The definition is as follows.

$$ALE = ARO * SLE \tag{2.3}$$

Annual Rate of Occurrence (ARO) is a measure of the probability that a risk occurs in a year. **Single Loss Expectancy** (SLE) means the total cost of an incident assuming its single occurrence.

2.3.2 TCO Minimization

Lawrence Gordon and Martin Loeb, who are economists at the University of Maryland, proposed TCO (Total Cost of Ownership) minimization theory in a famous book named "Managing Cybersecurity Resource: A Cost-Benefit Analysis" [43]. It is also a simple but powerful concept to evaluate the security investment since this idea can answer a question like "what is the necessary baseline of security investment?". For example, when we have following security investment as Table 2.2, TCO theory can be helpful to decide optimal security investment.

Table 2.2: TCO Minimization Example - Security Investment Options

No.	Investment Name	Poential Loss	Investment	Probability of Loss
1	No Investment	10,000,000	0	0.75
2	Solution : A	10,000,000	650,000	0.50
3	Solution : A + B	10,000,000	1,300,000	0.40
4	Solution : A + B + C	10,000,000	1,950,000	0.33
5	Solution : A + B + C + D	10,000,000	2,600,000	0.29

After calculating expected loss and TCO (Expected Loss + Investment), we can understand that No.4 minimizes TCO as Table 2.3 shows, and we can assume this is the optimal investment.

Table 2.3: TCO Minimization Example - Approach

No.	Investment Name	Investment	Expected Loss	TCO
1	No Investment	0	7,500,000	7,500,000
2	Solution : A	650,000	5,000,000	5,650,000
3	Solution : A + B	1,300,000	4,000,000	5,300,000
4	Solution : A + B + C	1,950,000	3,300,000	5,250,000
5	Solution : A + B + C + D	2,600,000	2,900,000	5,500,000

This approach is similar to introductory economics such as maximizing profit by considering marginal costs. Gordon and Loeb generalized this concept by applying economic approach and modeling. They constructed optimal investment theory [44] named "Gorden & Loeb Model" (GLEIS Model). This study provided that

security investment should not exceed $1/e(\approx 36.79\%)$ of the expected loss of a security breach. Many researchers improved and verified this study [45–48].

2.3.3 Mathematical Approach

Another approach is applying combinational optimization theory in mathematics for security investment evaluation. For example, Sasaki et al. proposed to use combinational optimization method to Fault Tree describing the causal relationship between threat and countermeasure [49, 50]. Also, Nakamura et al. proposed generalized modeling methods [51, 52]. In addition to this, as a similar approach, some research applied game theory to risk assessment. For example, Carin et al. proposed the QuERIES model (Quantitative Evaluation of Risk for Investment Efficient Strategies) as risk assessment approach by using game theory [53, 54] and other researchers proposed similar approach [55–60].

2.4 Expected Damage Estimation

One of the most difficult things in security investment effectiveness evaluation is estimating expected damage and cost. It is because effective evaluation is totally dependent on this estimation. Before consideration of damage estimation, we describe the type of costs.

Tangible Cost

It is the cost of direct losses, including website downtime, forensic investigation cost, customer follow-up cost, and legal cost.

Intangible Cost

It is the indirect losses, including the loss of customer loyalty, reputation damage, and corporate branding damage.

2.4.1 Tangible Cost Estimation

For the tangible cost estimation, there are several approaches to estimate the costs.

Approach 1 : Analytical Framework Approach

The first approach is analytical framework approach. This approach provides the items and perspectives affecting the amount of damage and estimating the damage cost based on the framework. Table 2.4 shows the related works.

Table 2.4: Security Damage Estimation Framework

No.	Framework Name	Reference
1	IPA Damage Estimation Model (2001)	[61, 62]
2	JNSA Security Incident Damage Estimation Model (2002)	[63]
3	JNSA JO Model (2002)	[64]
4	KISA Model (2006)	[65]
5	Internet Incident Damage Evaluation Model (2008)	[66]
6	CyberTab Model (2014)	[67]
7	FAIR-Based Loss Measurement Model (2015)	[68]

For example, CyberTab proposed by The Economist Intelligence Unit is remarkable calculation framework to consider the incident cost of specific incidents because it includes many perspectives including legal expenses and corporate communication costs that are easily missed.

Also, In South Korea, research on loss estimation has been done actively. In 2013, several Korean organization got the cyber attacks (known as 3.20 cyber attack), and research group in KAIST (Korean Advanced Institute of Science and Technology) estimated damage with Internet Incident Damage Evaluation Model, and it concluded 867.2 billion won [69].

Approach 2 : Statistical Data Approach

The second approach is called as statistical data approach. Many security service vendors and security consulting firms publish the statistical data based on the survey and the log data generated by their services. As a cost evaluation perspective, we can utilize these data to estimate the impact of the security incident.

For example, Incapsula Inc., that is a leading DDoS solution vendor, revealed that the average per-hour costs by DDoS attacks were 40,000 USD [70]. Also,

Ponemon Institutes report [71] taught us that information leakage cost per records was 158 USD in 2016. As another example, PwC [20] mentioned that large companies had a more significant financial loss than SME(small and medium-sized enterprise), and the average financial loss of large companies having more than 1 billion USD revenue was 5.9 million USD, although companies having less than 100 million USD was 0.41 million USD. In addition to this, British Government report [72] had a similar conclusion that the breach cost of the large organization was between 600,000 GBP and 1.15 million GBP although the one of SME was between 65,000 GBP and 115,000 GBP.

In different perspective, indirect data is also helpful. For example, "Cisco 2017 Annual Cybersecurity Report" [73] revealed that following facts.

- 24% of breached organizations lost customers, and 40% of them lost more than 20 percent of their customer)
- 29% of breached organizations lost revenue, and 38% of them lost more than 20% of revenue.
- 23% of breached organizations lost business opportunities, and 42% of them lost more than 20% of them.

Another example is "Flipping the Economics of Attacks" [74] by Ponemon Institute. They concluded interesting data.

- An increase of approximately two days (40 hours) in the time required to conduct successful cyber attacks can eliminate as much as 60 percent of all attacks.
- On average, a technically proficient attacker will quit an attack and move on to another target after spending approximately a week (209 hours) without success.

Approach 3 : Simulation Approach

The third approach is simulation approach. This method estimated a reasonable cost with Monte-Carlo Simulation. Conrad [75] applied Monte-Carlo Simulation to security incident cost estimation based on ALE modeling and he concluded that Monte-Carlo Simulation was an effective method. After this report, Burtescu [76] created a model with ALE model and risk level analysis, and he found that these methods was efficient for risk management by considering risk level classification. Lyon [77] analyzed the effectiveness of SANS Critical Security Control by using Monte-Carlo Simulation.

2.4.2 Intangible Cost Estimation

For intangible cost estimation, it is wise to search for alternative indicators instead of calculating direct costs because it is tough to estimate the actual intangible cost of security breaches. Many researchers tried to evaluate corporate value loss as "intangible cost" by security incidents because we assumed that the decrease of corporate value was one of the typical examples of indirect losses. They applied corporate valuation methodology in corporate finance theory because the evaluation of corporate value loss was typical research area in the corporate finance field. We introduce two standard approaches, that is also applied to information security.

Accounting Approach with "Matched Sample Comparison"

"Matched Sample Comparison" is a scientific approach to reveal the impact of one condition difference by preparing two groups called "Control Group" and "Treatment Group". This scientific technique is applicable for the evaluation of corporate valuation impact by security incident from an accounting perspective. This accounting approach revealed that long term impact of security incidents since it analyzes the annual report of victimized companies.

For example, Gorden, Loeb, and Sohail [78] had an accounting analysis of

the market value impact by using Ohlson Model. Ohlson model was one of the corporate valuation methods by using net asset value on the balance sheet and net income in profit and loss sheet. This study added the other elements of voluntary disclosure of security incident.

Ko and Dorantes [79] applied this technique for the analysis of security breach. They picked up the samples called "Treatment Group" that have experienced information security breaches, and "Control Group" samples that represent the firms that were selected to match the treatment samples by size and industry. Then, they have deeper accounting analysis to evaluate the impact of corporate valuation by security breaches.

Event Study Methodology

Another approach for calculating corporate value is the using "Event Study Methodology". It analyzes the change of stock price before and after the event from the statistical perspective, and evaluate the impact of corporate value by calculating CAR (Cumulative Abnormal Return). The assumption of this methodology is stock price means the corporate value. This method was developed in 1969 by a study [80], and a study [81] formulated this methodology. After this paper, many researchers started the empirical research and applied this method to many cases such as the analysis of M&A or new product announcement. Since this approach allows to analyze the direct impact of corporate value after the incident, it is appropriate to security breach analysis, and many remarkable research papers have been available. Table 2.5 shows the empirical research against security breach cases by event study.

Table 2.5: Event Study Research Papers of Security Incident

No.	Researh Group	Ref.	Keywords
1	Campbell et al. (2003)	[82]	data breach (sensitive, non-sensitive)
2	Hovav et al. (2003)	[83]	attack vector (DoS attack)
3	Ettredge et al. (2003)	[84]	attack vector (DoS attack)

Continued on next page

No.	Researh Group	Ref.	Keywords
4	Garg et al. (2003)	[85]	attack vector (DoS, data breach, web tamparing)
5	Hovav et al. (2004)	[86]	attack vector (malware infection)
6	Cavusoglu et al. (2004)	[87]	corporate profile (size, industry), attack vector
7	Acquisti et al. (2006)	[88]	damage size, media type
8	Kawaji (2006)	[89]	Japanese company, attack vector
9	Ishiguro et al. (2006)	[90]	comparison (Japan, U.S., Europe)
10	Telang et al. (2007)	[91]	vulnerability disclosure
11	Kanna et al. (2007)	[92]	analysis window (short, long)
12	Andoh-Baidoo et al. (2007)	[93]	decision tree analysis
13	Goel et al. (2009)	[94]	impact on stock price
14	Muntermann et al. (2009)	[95]	notification of PII breach
15	Roztocki et al. (2009)	[96]	survey paper
16	Gatzlaff et al. (2010)	[97]	data breach impacting stakeholders' asset
17	Takayabu et al. (2011)	[98]	data breach (payment card)
18	Chai et al. (2011)	[99]	security investment
19	Gordon et al. (2011)	[100]	damage type (Information CIA)
20	Bose et al. (2011)	[101]	RFID impementation
21	Malhotra et al. (2011)	[102]	analysis window (short, long)
22	Morse et al. (2011)	[103]	long term impact
23	Konchitchki et al. (2011)	[104]	survey paper
24	Yayla et al. (2011)	[105]	integrated analysis
25	Hiromatsu (2011)	[106]	corporate profile (size, industry)
26	Hiromatsu (2012)	[107]	PII protection law
27	Parameswaran, et al. (2012)	[108]	cloud Service Use
28	Das et al. (2012)	[109]	comparison (India, U.S.) , attack vector
29	Andoh-Baidoo et al. (2013)	[110]	decision tree analysis
30	Brock et al. (2013)	[111]	security investment on onlin banking
31	Tanaka (2013)	[112]	corporate profile (indsutry, ISMS, disclosure)
32	Bose et al. (2013)	[113]	security investment
33	Oxford Economics (2014)	[114]	British company
34	Yoshimi (2015)	[115]	SNS flaming
35	Tanaka et al. (2015)	[116]	Japanese comapny
36	Spanos et al. (2016)	[117]	survey paper
37	Miyayuchi et al. (2016)	[118]	integrated paper
38	Nakamura (2016)	[119]	Impact difference by risk disclosure

2.5 Case Study

In order to discuss and verify the effectiveness of new proposed methodology of cybersecurity investment and cost estimation, we need to know real security incident examples. We picked up two famous example to know the reality.

2.5.1 Case Study 1 : Target

Target, which is a famous retailer, had significant security information breach in November and December of 2013, and they leaked 40 million records of credit card information and 70 million records of PII data by POS malware. It was very famous security incidents because of three reasons. Firstly, primary cause of this security incidents was POS malware. Secondly, they leaked approximately 110 million records, and it was the catastrophic breach [120] in cybersecurity history. Thirdly, this incident had huge negative impact on profit and stock price. According to Forbes [121], profit fell 46% in its fourth fiscal quarter of 2013 and declined by more than a third for all of 2013. In addition to this, Figure 2.1 revealed that more than 5 USD was declined in stock price perspective [122].

Figure 2.1: Target Stock Price (from Yahoo Finance)

Total Expenses and Insurance Coverage

According to 2016 annual report and Form 10-K of Target [123], it stated that they spent 292 million USD as cumulative expenses of countermeasures including

settlements through the end of 2016. However, insurance covered 90 million USD and net cumulative expenses of 202 million USD. In another word, we assumed insurance covered approximately 30.82% of total countermeasure cost. In addition to this, according to DXC Technology [124], new branding company of leading IT consulting firm CSC (Computer Sciences Corporation) and HPE (Hewlett Packard Enterprise Services), they assumed that the cost of annual premiums of Target was probably between 200,000 USD and 400,000 USD in the case of the coverage beyond 100 million USD. Also, they mentioned that this comprehensive coverage could be realized by combining multiple underwriters. When we assume the annual premium of Target is between 200,000 USD and 400,000 USD, ROSI of this cyber risk insurance is approximately between 224 times to 449 times.

Class Action

From class action perspective, according to this news [125, 126], They had over 100 lawsuits, but they were consolidated into three groups including victimized customers, financial institutions, and Target stakeholder. After several years later, Target agreed to pay tremendous money to several stakeholders as Table 2.6 shows. Especially, Target decided to pay 10 million USD as the maximum to victimized people, and each victimized individual, whose information records has been leaked, can acquire compensation up to 10,000 USD.

Table 2.6: Target Settlement in Class Action

No.	Stakeholders	Settlement Amount	Settlement Day
1	Customers	$10 million	March 2015
2	MasterCard	$19 million	April 2015
3	Visa	$67 million	August 2015
4	Banks & Credit Union	$39.4 million	December 2015
5	47 State Governments	$18.5 million	May 2015
	Total	$153.9 million	

Compensation of Personally Identifiable Information

One of the arguments about this settlement to clients is 10 million USD is too small for 40 million victimized people. However, this settlement works correctly. As news articles [127, 128] quoted the comments by Sasha Romanosky, who is a researcher of the economics of information security at Carnegie Mellon University, "Many customers will likely not be able to prove that they lost money due to hacker activities". From this perspective, technically, people can only gain 25 cents averagely as compensation.

2.5.2 Case Study 2 : Home Depot

Home Depot, which is famous home improvement retailer, also had significant security information leakage in 40 million records of payment card and 56 million records of personally identifiable information in September 2014.

Total Expenses and Insurance Coverage

According to 2016 annual report [129], it stated that they spent 298 million USD as accumulated countermeasures cost including settlement. However, insurance covered 100 million USD, and cumulative net expenses are 198 million dollars. In another word, we assumed insurance covered approximately 34.56% of total countermeasure cost.

Class Action

From the class action perspective, Home Depots decided to pay 179 million USD for settlement. According to the news article [130], Home Depots had 57 class actions in U.S. and Canada with victimized individual and agreed to pay 19.5 million USD to them. 13 million USD is for reimbursing impacted customers for out-of-pocket losses, and 6.5 million USD is for covering 18 months of cardholder identity protection services. Also, for the financial institutions, Fortune [131] mentioned that Home Depot paid 134.5 million USD to Visa, MasterCard, and various banks,

and they agreed to pay 25 million USD in March 2017 to dozens of banks.

PII Compensation

From PII compensation perspective, 56 million people struggled with the 13 million USD budgets as the compensation. In another word, averagely, people can only gain 23.2 cents as compensation.

Chapter 3

The Price of Personally Identifiable Information in Data Breach

3.1 Introduction

Personally identifiable information (hereinafter PII) is a critical competitive resource for the service providers, and it is necessary for service development, continuous improvement of service, and marketing. On the contrary, the security incidents of PII breach is increasing, and it will be catastrophic damage to corporate branding and business continuity. Especially for B2C companies, PII breach is influential and senior management team also seriously considers the prevention of PII breach.

3.1.1 Attack Vector

Generally speaking, the attack vector of PII breach has two types.

Traditional Hacking

The first vector is abusing the vulnerability of web application or infrastructure for leaking the information. According to an article [132], The attacks against e-commerce sites and CMS (Contents Management System) have been notable, and there are many cases, such as the information breach of Nippon Television Network Corporation by abusing the vulnerability of OS command injection [133],

or the leakage from Spiral EC, cloud environment managed by PIPED BITS [134]. According to white paper by NRI SecureTechnologies, "Cyber Security Trend Annual Report 2016" [135], 32.1% websites have serious access control vulnerabilities that allow unauthorized users to access sensitive information, and this is still a dangerous attack vector for corporate management.

Advanced Persistent Threat

The second vector is a breach by spear phishing or APT (Advanced Persistent Threat). In recent examples, medical insurance companies [2–5], JPS (Japan Pension Service) [8], JTB [9] are notable cases. In this vector, the attackers exploit the human psychology by using social engineering technique and steal PII data silently after deployment of the sophisticated malware into corporate environments. Since the malware has been sophisticated and it is hard to catch the malware with current detective control mechanism, the corporate network needs to consider not only usual prevention and detection in inbound but also the countermeasure in outbound.

3.1.2 Challange

The emerging challenge is the gap between real compensation value and theoretical value. In 2003, JNSA (Japan Network Security Association) formulated JO model (JNSA Damage Operation Model for Individual Information Leak), and it has been a benchmark for calculating the compensation cost of personally identifiable information. The background of formulating this model was three reasons. Firstly, on July 11, 2002, the Supreme Court judged that Uji City had to pay 15,000 JPY as compensation [24] (Technically, 10,000 JPY is for solatium, and 5,000 JPY is for the compensation coverage of legal cost.) Secondly, in 2003, "Act on the Protection of Personal Information" [25] was published, and it was likely to increase the awareness of protecting personally identifiable information. Thirdly, the detailed information related to cybersecurity incidents had not released during

this period. From these reasons, JNSA tried to create calculation model of personally identifiable information, and it has been a great resource to consider the leakage.

On the contrary, in 2003, Lawson, leading retail chain, leaked 560,000 records of personally identifiable information, and they proactively decided to send 500 JPY gift certificate to all 1.15 million exclusive customers including the customers who were not victims of this breach. Based on this example, many companies those leaked customer information referred this case, and 500 JPY coupons became a defacto-standard price of data breach cases in Japan. We think this current situation has the difference from theoretical JO model.

3.1.3 Contribution

By case study analysis about the compensation of personally identifiable information, we have three major contributions in this area. Firstly, we analyze 45 cases of Japanese personally identifiable information leakage, and we find that the value of average spontaneous compensation is 543 JPY, and theoretical value by JO model has more than 60 times gap from this average price. Secondly, we have case study analysis about lawsuit case in Japan and U.S. In Japan, the compensation is more than 5,000 JPY in Japan, although one in U.S. is averagely less than one dollar. We think Japanese compensation value is averagely higher than U.S., and we find that it is caused by the difference of compensation style. Thirdly, we analyze how to handle personally identifiable information in the current situation, and we point out three data characteristics that model should include. The first factor is “Searchability”. Many people recently tend to open the primitive personally identifiable information to SNS platform and attackers can gain them without any security breach. The problem is, by the information leakage, attackers or the meddling third party can link the breached data (the data users do not want to disclose such as porn history data or purchase history) to disclosed data in SNS. We think this undesirable linkage is one of the keywords for improving the model.

The second factor is “cancellability”, and it means that some data such as password can be changeable after information breach although some information such as date of birth can not be. We consider the lifecycle of data is one of the important factors. The last element is “Retrievability, ” and it means the possibility of the prevention of leaked information proliferation. In the case of internal fraud, it is easy to prevent the spread of leaked data because police or investigation organization can take over the data. However, it is difficult to remove the information online as we learned in Winny case.

3.2 Compensation After PII Breach

In this section, we show the difference between the U.S. and Japan from PII compensation.

3.2.1 The United States of America

In the U.S., the right of protecting PII is very strong, and many people require the compensation by collective sue (class action) when the organizations have PII breach. Therefore, the compensation has been decided by the court of justice, and these societies accumulate the logic, methodology and judicial precedent. In each incident, many customers have the class action against the victimized enterprise, but as we discussed in Section 2.5, class actions by customers pull out tremendous compensation as the total, but averagely, then can gain less than one USD.

Legislation and Regulations

In the United States, various legislation and regulations of protecting PII had been created such as California State Security Breach Information Act [136], HIPAA (Health Insurance Portability and Accountability Act) [137], and NYDFS Cybersecurity Requirement [13]. These regulations defined the procedure of information disclosure or penalties when organizations do not comply with the regulations. Especially, HIPAA is very remarkable since HHS (U.S. Department of Health and

Human Services) imposed severe fines and penalties to the organizations that violate HIPAA. HHS websites [138] show the list of penalties and an article [139] has the list of largest HIPAA settlement fine. For example, Advocate Health Care Network, which operates 12 hospitals and more than 200 other treatment locations in Illinois, paid $5.55 million to the HHS, since Advocate Health leaked 4 million records of patients [140]. Also, WellPoints, currently known as Anthem that had another serious information breach, paid $ 1.7 million as a settlement [141].

3.2.2 Global Trends in Legislation and Regulations

As global trends, since PII data are transferred globally, the improvement of legislation and regulations to protect PII are sophisticated, such as EU GDPR (General Data Protection Regulation) [142], Privacy Management Framework in Canada [143], various PII data protection activity in Japanese government [144].

One of the remarkable issues in these regulations is they define the penalties when organizations do not comply with the regulations. For example, in GDPR, when an organization has a severe violation to GDPR, it has to pay 20 million EUR or 4% of the total annual worldwide turnover of the preceding year. According to white paper [145], South Korea has Personal Information and Protection Act, it defines the penalties up to KRW 100 million (approximately $87,994 USD) and/or as much as ten years in prison. In Hong Kong, Personal Data Ordinance is defined including the fines up to HKD 1 million (approximately $128,900 USD) and prison sentences of up to 5 years when violating data transfer rules. Singapore defines Personal Data Protection Act, and it states the penalties of SGD 1 million (approximately $735,862 USD) and imprisonment of up to 4 years in the case of data regulation violation.

Therefore, these global trends have created the incentive to invest security control.

3.2.3 Japan

In modest Japanese culture, only a few people argue the right of victims in collective sue, and they have only few lawsuit cases to ask the compensation of PII. Therefore, the logic, methodology and judicial precedent are not enough to decide the compensation. On top of that, because of "apology culture" of Japanese characteristics, it is a unique but common activity that the companies leaked PII distribute the 500 JPY vouchers as the compensation. According to newspaper The Nikkei [146, 147], this was started because Lawson leaked 560,000 records and they distributed 500 JPY voucher to all victimized customers. After this case, it became a defacto-standard, and a recent case such as Benesse breach in 2015 still paid 500 JPY voucher to customers.

While we think this unique trend will be continued in the future, some people have argued this 500 JPY compensation is not appropriate because recently, the awareness of the right to protect PII is improved. Based on this background, gradually, the number of legal debates, asking the legal court to decide the compensation price, is increasing.

On the contrary, JNSA has started to consider the problem of compensation price from 2002. Also, this organization proposed JO model that can estimate the expected compensation value per person in the PII leakage and published the assessed value every year. However, some professionals have pointed out the gap between JO model and reality.

3.3 JO Model

In this section, we describe the overview of JO model with report [148] According to JO model, the assumed compensation cost should be decided by the multiplication of three factors.

1. Value of Information Leaked

2. Degree of Social Responsibility of the Organization

3. Appraisal of Post-Incident Response

3.3.1 Value of Information Leaked

The first factor is "Value of Information Leaked". To evaluate the value accurately, the multiplication of following three parameters define this value.

Value of Basic Information

The first parameter is "Value of Basic Information," and it is the basis of personal information. In JO model, the default value is 500 yen, and the working group referred the case of Lawson Card leakage, as we mentioned.

Degree of Information Sensitivity

The second parameter is "Degree of Information Sensitivity," and it decides the importance of personal information.

$$Information\_Sensitivity = [max(10^{x-1} + 5^{y-1})] \tag{3.1}$$

x is the maximum of the emotional distress level, and y is the maximum of the economic distress level. JO Model working group had theoretical analysis, and they classified personally identifiable information into two categories; "Economic Loss" and "Emotional Loss." Then they make an ER Map (Economic Privacy Map) in Figure 3.1.

After creating ER map, the working group attempted to map each personally identifiable information into ER map, and they simplified the map called Simple EP Map. We tried to pick up the important personally identifiable information from original one in Figure 3.2. (Please refer [148] if the original one is needed.)

In JO model calculation, based on the above classification, the security manager can decide the economic distress level and the emotional distress level of leaked information and calculate the value based on the above formula.

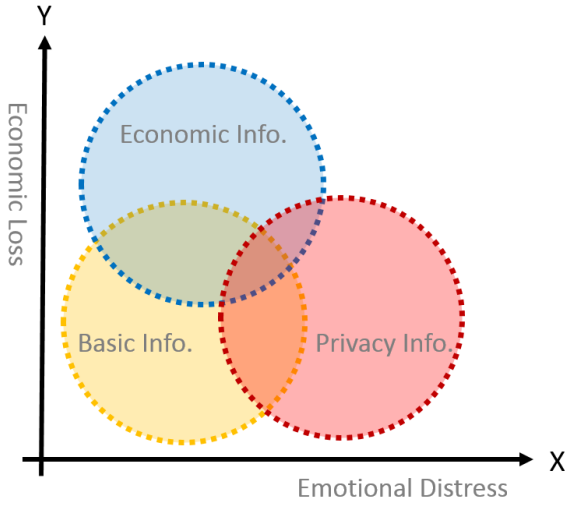

Figure 3.1: Economic Privacy Map

Degree of Ease in Identifying the Individual

The third parameter is "Degree of Ease in Identifying the Individual." According to the model, it affects the compensation value based on the identifiability of individual and the criterion of this is defined in Table 3.1.

Table 3.1: Degree of Ease in Identifying the Individual

Identifiability	PII Element	Degree
Easy	Name AND Address	6
Middle	Name OR (Address + Telephone Number)	3
Difficult	Other Informaton	1

3.3.2 Degree of Social Responsibility of the Organization

The second factor is "Degree of Social Responsibility of the Organization," and it evaluates the responsibility level of organization. The criterion is defined in Table 3.2. The organizations classified into "high" include large companies having high public recognition, governmental institutions, industries defined in "Basic Policy related to the Protection of Personal Information (Cabinet decision April 2, 2004)", such as medical, financial, and payment card industry.

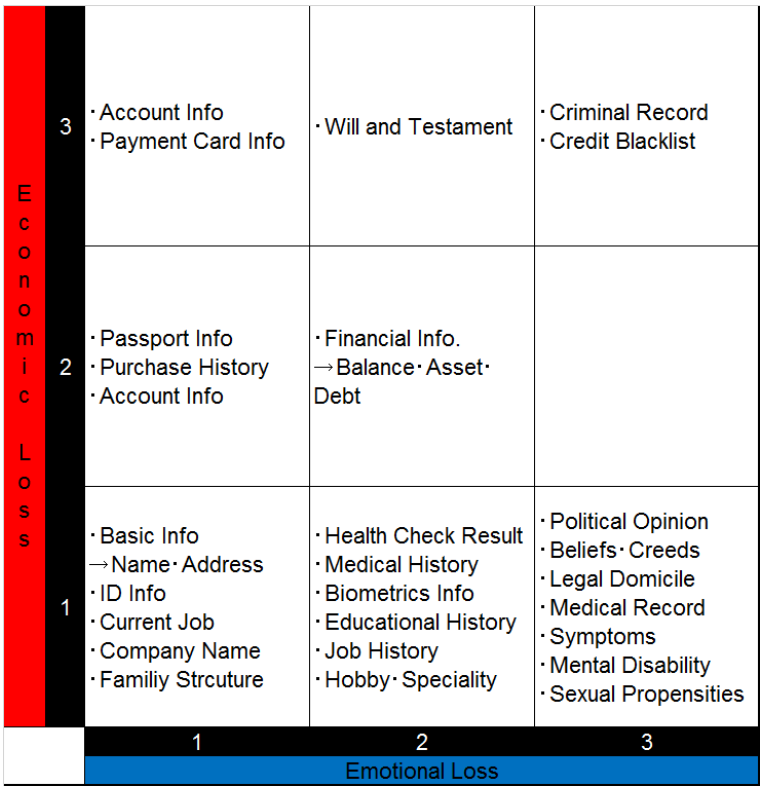

Figure 3.2: Simple EP Map

Table 3.2: Degree of Social Responsibility of the Organization

Level	Description	Degree
High	Large organizatios OR public sector OR specific industries	2
Normal	Others	1

3.3.3 Appraisal of Post-Incident Response

"Appraisal of post-incident response" is a final factor in JO model, and it means that the evaluation of attitude after disclosing the leakage. In order to simplify the judgment, JO model has qualitative standards of appraisal as Table 3.3 shows, such as response speed and the existence of inquiry point of contact.

3.3.4 The Application of JO Model

In this section, we demonstrate JO model in actual incident case.

Table 3.3: Appraisal of Post-Incident Response

Description	Degree
Appropriate	1
Inppropriate	2
Unknown	1

Benesse Corporation

The first case study is the internal fraud in Benesse Corporation, which is a very famous Japanese company as educational service providers. In July 2014, 35.04 million records of personally identifiable information were leaked [149] because a former employee of the outsourcing contractors acquired PII data without authorization, and he sold the information to mailing list brokers. The leaked information included name, gender, address, date of birth, and family structure. Benesse Corporation officially announced that they prepared 20 billion JPY as countermeasure budget [150] and sent 500 JPY vouchers to all victims. By using JO model, estimated compensation is 24,000 JPY for each person, and there is an enormous gap between actual compensation.

Table 3.4: Configured Parameter in Benesse Corporation Incident

Factors	Detailed Value	Value	Comments
Leaked Personal Information	Basic Information Value	500	-
	Information Sensitivity	2	X=1 and Y=1
	Personal Identifiability	6	Name + Address
Social Responsibility Degree	-	2	Large Company , Privacy Mark
Post-Incident Response Appraisal	-	2	Criticism on the Compensation

JINS Corporation

Another case study is payment cards leakage in March 2013 by JINS Corporation. JINS Corporation is eyewear retails to sell the product at low price. The leaked information included cardholder's name, PAN (Prime Account Number), expiration date, security code (CVV2) [151]. Although 12,036 records were possibly leaked in the first report, final report said that only 2,059 records are leaked [152]. JINS

sent the 1,000 JPY gift card for 12,036 people as the compensation. Also, JINS defrayed the cost of reissuing payment card. Usually, in Japan, reissuing cost was approximately between 500 JPY and 1,000 JPY. Therefore, the average compensation cost for each person was between 1,500 JPY and 2,000 JPY, and total cost of compensation was more than 18 million JPY. Also, the cost of postage cost and investigation cost were significant. Especially, in the payment card information leakage, the investigation by a PFI (PCI Forensic Investigator) certified forensic investigator registered by PCI SSC (Payment Card Industry Security Standard Council) is necessary. Therefore, the additional cost was also required. We are going to calculate assumed compensation cost by using JO model. The result is 39,000 JPY for each person.

Table 3.5: Configured Parameter in JINS Corporation Incident

Factors	Detailed Value	Value	Comments
Leaked Personal Information	Basic Information Value	500	-
	Information Sensitivity	26	X=1 and Y=3
	Personal Identifiability	3	Name
Social Responsibility Degree	-	1	-
Post-Incident Response Appraisal	-	1	-

This calculated value is useful as a normative example, but there is an enormous gap between actual compensation 1,000 JPY and improvement is necessary.

3.4 Survey Research

As we mentioned, in Japan, there is no clear policy and direction about personally identifiable information leakage compensation. A research paper [153] had a questionnaire research and, according to their research, basic PII data such as phone number and purchase history deserve to less than 1,000 JPY.

3.4.1 Actual Trends in Compensation of PII Leakage

We investigate disclosed 45 PII security incident cases, from 2002 to 2017, and all cases have spontaneously paid compensation. Table 3.6 shows the detailed data of

actual compensation, and the majority of spontaneous compensation is between 500 JPY to 1,000 JPY, as Figure 3.3 shows.

Table 3.6: Spontaneous Compensation

Year	Organization	Leaked Records	Compensation (JPY)	JO Model Value (JPY)
2002	Yamayoshi Seika	1,200	1,300	6,000
2002	Kinjirushi	1,200	2,000	3,000
2003	Lawson	560,000	500	6,000
2003	JCB	79,110	1,000	210,000
2003	Aplus	6,923	1,000	45,000
2003	Family Mart	182,780	1,000	6,000
2003	Tobu Railways	131,742	5,000	6,000
2004	Yahoo! BB	4,517,039	500	12,000
2004	Tsunoda	75,000	500	3,000
2004	suntory	16,000	500	6,000
2004	Cosmo Oil	923,239	500	6,000
2004	Mitsubishi UFJ NICOS	478,000	500	156,000
2005	Oriental Land	121,607	500	33,000
2005	Odakyu Electric Railway	6,203	500	6,000
2006	NHN Japan	295,775	500	7,500
2007	Dai Nippon Printing	8,640,000	500	78,000
2007	NTT Docomo Kansai	339	1,000	6,000
2008	SoundHouse	122,884	1,000	39,000
2008	SOTETSU INN	1,760	1,000	6,000
2008	IRIS Plaza	28,105	1,000	13,000
2009	NHN Japan	399	500	33,000
2009	Mitsubishi UFJ Securities	49,159	10,000	180,000
2009	Amuse	18,184	500	78,000
2009	MetLife Inc. (Alico Japan)	148,680	10,000	26,000
2010	Messe Sanoh	5,346	5,000	315,000
2010	Higashimura Japan	722	1,000	1,000
2012	JAM TV	169	500	5,500
2013	JINS	12,036	1,000	39,000
2013	XCom Global	109,112	3,000	26,000
2014	Benesse	35,040,000	500	24,000

Continued on next page

Year	Organization	Leaked Records	Compensation (JPY)	JO Model Value (JPY)
2015	JAL	4,131	500	12,000
2015	Hotel Ryumeikan Tokyo	1,954	500	1,000
2016	Ahkun	3,859	500	24,000
2016	Alba	83,194	500	3,000
2016	Glico	1,000	500	156,000
2016	Nippon TV	428,138	1,000	12,000
2016	Rohto Pharmaceutical	6,249	500	12,000
2016	ARDEPRO	329	500	12,000
2016	Golf Digest Online	1,949	3,000	12,000
2016	Sanrio	2,724	1,000	12,000
2016	Graphic	192,594	500	312,000
2016	RD Support	1,221	500	3,000
2016	Kagoya Japan	48,685	500	156,000
2016	IPSA (Shiseido Group)	421,313	1,000	156,000
2017	PIA Corporation[a]	155,000	500	6,000

[a] PIA corporateion totally leaked 155,000 records, but 32,000 records included not only PII but also payment card information. Although basic compensation is 500 JPY, PIA corporation decided to pay 3,000 JPY for the 32,000 victims, and we consider this condition when calculating total damange or average.

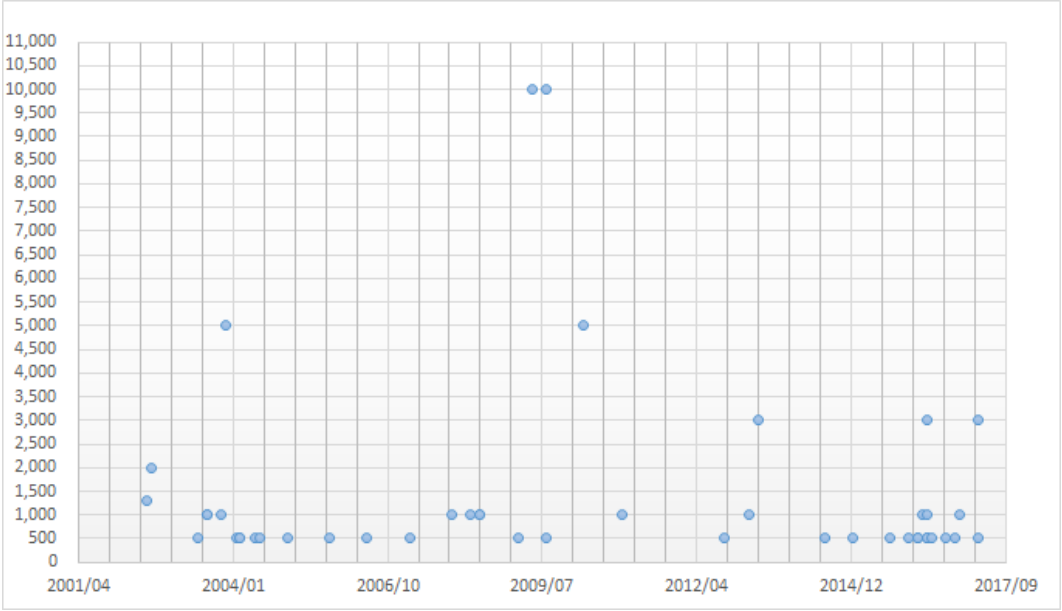

Figure 3.3: Compensation Cost Mapping

In order to analyze this results correctly, we define two indicators named **Arith-**

metic Mean and **Weighted Mean**. When we set each compensation price of each victimized organizations i as CP_i and Breach Records Number of the organizations i as BRN_i, we can define these two indicators as follows.

$$Arithmetic\,Mean = R_{it} = \frac{1}{N}\sum_{i=1}^{i=N} CP_i \tag{3.2}$$

$$Weighted\,Mean = \frac{1}{\sum_{i=1}^{i=N} BRN_i}\sum_{i=1}^{i=N}(CP_i * BRN_i) \tag{3.3}$$

As Table 3.7 shows, arithmetic mean of actual compensation is 1,453 JPY, and weighted means is 543 JPY. From this result, the companies considered that this value is appropriate when the companies spontaneously paid the compensation. The total cost will be larger when we consider the postage and reissue fee of credit cards.

Table 3.7: Average Price of Compensation (N=45)

Mean Type	Average (Real)	Average (JO Model)	Gap (JO Model / Real)
Arithmetic Mean	1,453 JPY	51,043 JPY	35.13
Weighted Mean	543 JPY	35,000 JPY	64.46

Also, Figure 3.4 shows that estimated total amount of payment by victimized companies, and it is calculated the multiplication of compensation cost per person and the number of breached data. Since the number of leaked data is different, total amount covered by victimized companies is deviated, and the arithmetic mean of them is approximately 638 million JPY.

3.4.2 Gap Analysis between JO Model and Reality

We applied JO model to these 45 cases and conducted a gap analysis. Figure 3.5 depicts the gap between real compensation value and expected compensation value by JO model. (The bottom of each blue box means the actual price and top of each box is expected value by JO model. Also, we use logarithmic scale to

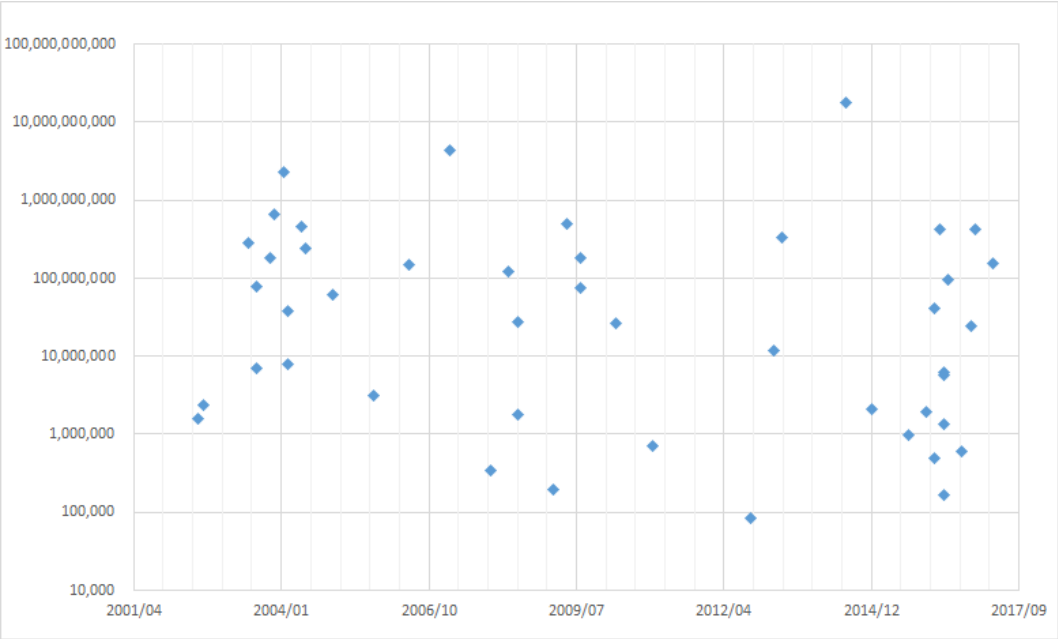

Figure 3.4: Total Compensation Cost Map

depict the data). This large gap is an obvious example that JO model needs to be improved.

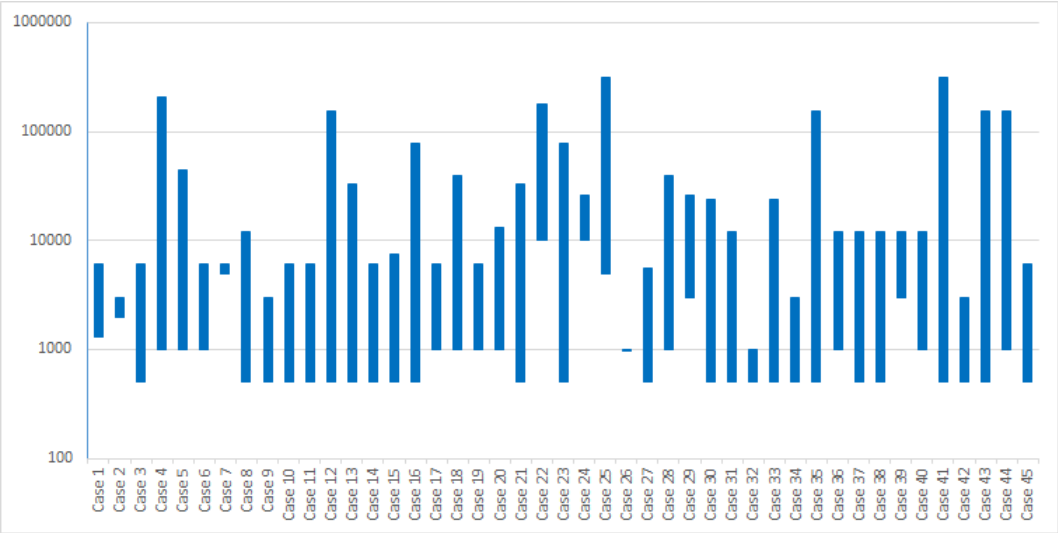

Figure 3.5: Gap Analysis Between Reality and JO Model Results

In addition to this, Table 3.6 shows estimated value of each case and Table 3.7 shows an average value. According to this table, arithmetic mean of JO model value is 51,043 JPY, and weighted means of this is 35,000 JPY. From this result, we assume theoretical value by JO model 64.46 times larger than real weighted

means, and the gap between theoretical value and reality is tremendous.

3.4.3 Japanese Lawsuit Trends

When customers do not accept compensation, an available option is lawsuits from privacy violation perspective. There are several trial cases as Table 3.8 shows and many legal cases require more than 5,000 JPY compensation. Also, in 2013, the class action in Benesse expects 55,000 JPY per person, and it is a remarkable example.

Table 3.8: Compensation Decided by Lawsuit

Year	Organization	Leaked Records	Qualified Plaintiff	Compensation	JO Model Value
2002	Uji City	217,617	3	10,000 JPY[1]	12,000 JPY
2003	Waseda University	1,400	6	5,000 JPY[2]	606,000 JPY
2003	Ozu City	180	186	50,000 JPY	606,000 JPY
2007	TBC	50,000	14[3]	30,000 JPY	33,000 JPY
2007	Yahoo BB!	6,500,000	4	5,000 JPY[4]	6,000 JPY
2010	JAL Labor Union	9,862	193	230,000 JPY	303,000 JPY

[1] Actual payout is 15,000 JPY and 5,000 JPY is for legal cost of this lawsuit.
[2] Actual payout is 10,000 JPY and 5,000 JPY is for legal cost of this lawsuit.
[3] Majority of plaintiff, 13 people, got 35,000 JPY (5,000 JPY is for legal cost), and 1 plaintiff got 22,000 JPY including 5,000 JPY legal cost.
[4] Actual payout is 6,000 JPY and 1,000 JPY is for legal cost of this lawsuit.

Also, we calculate the expected compensation value by JO model in Table 3.8. According to the average value as Table 3.9 shows, we think there is still a gap between the real value and the value of the lawsuit, although it is smaller gap than spontaneous compensation.

Table 3.9: Average Price of Compensation (N=6)

Mean Type	Average (Real)	Average (JO Model)	Gap (JO Model / Real)
Arithmetic Mean	55,000 JPY	261,000 JPY	4.75
Weighted Mean	133,441 JPY	431,904 JPY	3.25

3.4.4 The Comparison Between U.S. and Japan

We think Japanese companies usually paid more compared with U.S. enterprises in PII compensation perspective. As we mentioned, U.S. cases had a lot of lawsuits and victimized companies spent the tremendous amount of money. However, as PII leakage compensation, victims in U.S. could gain less than one dollar, although Japanese victims could receive more than 500 JPY. It was because enterprises in U.S. had to consider not only victimized customers, but also the penalty and fine by regulators and governmental agency, and invoice by credit card issuer in the case of payment card breaches.

The major difference is the different idea about collective sue. In Japan, when people would like to have collective sue, the stakeholders need to agree on the details of appeal and to create plaintiff group. Therefore, usually, plaintiff group is small, and the judgment by the court is usually like "Company needs to pay 10,000 JPY to each person in plaintiff". On the contrary, in the U.S., "class action" is a very typical approach, and the part of victims can sue the organizations on behalf of all victims. Rule 23 of "TITLE IV. PARTIES" in Federal Rules of Civil Procedure [154] states the actual procedure and specific condition of class action. Basically, in the class action, court decides the condition of "class" before starting judge, and the victims classified into the "class" automatically join the plaintiff group. Also, all judgments by the court will be applied to all victims in this class. If he/she do not prefer to join the classified class, he/she needs to have a request of "opt-out" before starting the legal debate. Therefore, the judgment of the court usually states that "Prepare the 70 million USD for the compensation of victims, and acknowledged victims who can prove the financial damage can request 10,000 USD as a maximum."

3.5 The Challenge in PII Value and Concept

One of the considerations is that the gap between actual compensation and estimated JO model value, even though JO model provides a normative example of compensation. We think it is dependent on the history of JO model as we mentioned. JO model was originally formulated in 2003 based on various research, interview by professional, and the consideration by the working group. The external environment in 2003, such as technology, available information in cyberspace, and awareness of PII was different, and we think one decade has brought a substantial change in the external environment. Especially, under the status quo, SNS (Social Network Service) has become our necessary platforms, and many users put the basic personally identifiable information on this platform. Because of this situation, by using OSINT (Open Source Intelligence) technique or the diversification of the attack method, attackers or the meddling third party can collect various PII data from cyberspace. From this situation, we need to improve JO model, the idea of personally identifiable information value.

3.5.1 Searchability

The first point is "Searchability." In the current situation, as we mentioned, it is possible to extract PII from SNS platform because many people upload PII information in SNS platform. Although many SNS users stored personally identifiable information based on the free choice of an individual, people do not expect to link these data with breached privacy information. Especially, if privacy information is leaked with PII, it is easy to connect another information. For example, In the case of high privacy data leakage case (such as online pornography service usage history, or the fact of using online porn service), users do not want to link the leaked privacy data with publically available data in SNS data, although users decided to disclose the personal emails to SNS. However, since the basic idea behind OSINT technique is connecting data dots in cyberspace, the attackers and the

meddling third party can easily link these data. We think the undesirable linkage between published data and privacy data will be a next generation keyword for considering information leakage and PII value.

3.5.2 Cancellability

The second point is “cancellability”. It means that non-changeable leaked data is more valuable than changeable data. For example, although the leakage of password information is very attractive for the public, SYK (Something You Know) type authentication information is changeable in the online system. On the contrary, date of birth(DoB) or the address is not changeable even if users would like to change. Also, we think the data lifecycle is also an important factor in “cancellability” perspective. We assume that DoB information of children is more valuable than one of the seniors because children have to handle information leakage risk in a long time, and they have more opportunity to jeopardize their information by this leakage. We think one of the reasons that Benesse leakage had a lot of backlash by victims was Benesse leaked the children’s information.

3.5.3 Retrievability

The third issue is ”Retrievability.” In the case that leaked information is posted on online such as PasteBin [155], many people can download the data, and it is tough to retrieve the data. Also, as a lesson from Winny information leakage, it is very difficult to delete the leaked data in cyberspace [156]. On the contrary, in the case of internal fraud by removable media, the majority of motivation is a financial motivation, and the leakage is limited such as a mailing list broker. In this case, public investigation sectors can eliminate the leaked information by arresting agents. Because of these cases, data leakage path is one of the important factors to decide the value of PII.

3.6 Conclusion

In this chapter, We have various case study analysis about the compensation of personally identifiable information. Firstly, we analyze 45 cases of Japanese personally identifiable information leakage, and we find that the value of average spontaneous compensation is 543 JPY. In addition to this, average theoretical value by JO model is 60 times higher than the average real price. Secondly, we have the case study analysis about lawsuit case in U.S. and Japan. In Japan, the compensation was more than 5,000 JPY, although U.S. was averagely less than 1 dollars. We think Japanese compensation value is averagely higher than U.S. because of difference of compensation style. Thirdly, we analyze how to handle personally identifiable information in the current situation, and we point out three data characteristics that model should include.

As future work, we will have the quantitative analysis of the linkage between compensation and other factors such as payment, the speed of information disclosure, calculation concept, stock price, and Twitter response. In addition to this, we would like to contribute a sophistication of JO model since there are various changes in external environments.

Chapter 4

Intangible Cost Estimation by Twitter Sentiment Event Study

4.1 Introduction

As we mentioned previously, once organizations have the information security incidents and data breaches, victim organizations have to pay tremendous costs. From risk management perspective, the accurate estimation of security incident impact is critical. Tangible cost, such as investigation cost, customer follow-up cost, and legal cost are predictable and calculable, and many theoretical frameworks are proposed as we mentioned in Section 2.4.1. However, it is tough to estimate the intangible damage, such as loss of customer loyalty, reputation impact, and the damage of branding although several methods have been proposed as we mentioned in Section 2.4.2. This chapter introduces a new approach called "Event Study Methodology with Twitter Sentimental Analysis" to evaluate these intangible costs, and this proposed method can solve the constraint of previous works, as we will discuss in Section 4.2.

4.1.1 Motivation

As we mentioned in Chapter 1, NISC introduced the concept of "Accident Assumed Society", and many private organizations started to prepare the incident management plan and the cost when security incidents happened. However, "intangible cost" evaluation is one of the concerns because it is difficult to evaluate

them as we mentioned in Chapter 2.

4.1.2 Challange

The emerging challenge is that we have limited approaches to evaluate the impact of corporate value in security incidents for the companies that do not have stock price data. As the evaluation method of corporate value impact, the application of event study methodology by using stock price data is a modern approach. Event study methodology is analyzing the short-term impact to corporate value by an event, such as M&A announcement or new product release, by examining the volatility of stock price before and after the event and calculating the CAR (Cumulative Abnormal Return). CAR allows us to have the quantitative analysis of corporate value impact. The assumption of this approach is that market capitalization calculated by stock price means the corporate value. In related works, many researchers apply this methodology to analyze information security incidents and to examine the short-term impact on corporate value. However, this method is entirely dependent on the stock price data, and we think it is a challenge that we cannot analyze the various cases. For example, we can not examine the organizations, which do not have stock price data such as private companies and governmental agency.

4.1.3 Contribution

In this chapter, we propose new corporate valuation method by defining the value named Tweet Reputation Index (TRI), to evaluate targeted organizations instead of stock price in security incidents. Tweet Reputation Index is a cumulative emotion value against the targeted entities by unit time after performing sentiment analysis against Tweets related to them. As same as stock price data, we calculate Cumulative Abnormal Return (TRI-CAR: Tweet Reputation Index Cumulative Abnormal Return) from this Tweet Reputation Index, and we can estimate the event impact on corporate value. As a case study by applying this method, we have

two contributions. Firstly, with the analysis of public enterprises, we demonstrate our approach, and we confirm high correlations (Correlation Coefficient: +0.8) between stock price data and Tweet sentiment data in short-term (3 days before and after the Event Day) by analyzing both data. Secondly, we apply this method to the non-public organization not having stock price data, in order to prove the applicability of our proposed approach.

4.2 General Dataset Analysis

In the context of information security incidents, stock price data has a challenging issue and limited capacity to reveal corporate value. In this proposed approach, we focus on the new dataset Tweet Reputation Index (TRI), and this is time-series data of Tweet sentiment. In this section, we describe the overview of both data and discuss and compare the strength and weakness of them.

4.2.1 Stock Price Data Overview

The inventor of traditional event study methodology decided to use stock price data. It is because, as Benjamin Graham, a famous professor called "father of value investing", mentioned, the stock price is reflecting the popularity and corporate value of the public company. From this perspective, the event study, which analyzes the change of stock price before and after the event from the statistical perspective in the short term, use a suitable dataset. Also, as we mentioned, the negative impact on corporate value and popularity is a common loss of intangible cost.

4.2.2 Tweet Reputation Index Overview

The technical-detailed definition will be introduced in Section 4.5, and Tweet Reputation Index (TRI) is time-series data describing the change of accumulated Tweet sentiment value. We decide to use Twitter data as a dataset because of two reasons. Firstly, Twitter has significant characteristics of reflecting positive and

negative opinions and evaluating existing image and impacts on the targeted entity. Recently, social media marketing and communication have been a critical domain of marketing department. Secondly, Twitter allows to use only 140-character words, and it realizes "readily usable" and "real-time update" features. We think these features reflect the response against victims' organization quickly.

4.2.3 Data Simlirality

Both data have pros and cons, but, we would like to show the similarity of both data.

Firstly, as we mentioned, a common characteristic of them is elaborating the popularity and corporate value of public companies.

Secondly, both data has a close relationship. Paper [157] reported that they could predict the stock price by using Twitter sentiment analysis and the success ratio was 87.6% because of a strong correlation between both data. According to the article [158], European hedge fund developed algorithm trading system based on this research, and they achieved remarkable investment performance. In addition to this, the market also considers that negative impact on Twitter is one of the very critical factors to estimate stock price because recent flash trade (HFT: High-Frequency Trade) algorithm referred the contents of Twitter. For example, when the Twitter account of Associated Press was hacked, and hacker released fake news on this compromised Twitter, it had substantial negative impact on NASDAQ or Dow Jones Industrial Average [159].

Since Twitter sentiment has been a significant factor of stock price, several Japanese companies started to apply the sentiment value for the stock price estimation. For example, NTT Data launched the service called "Twitter Sentiment Index" by using Twitter sentiment data for financial market in 2014 [160]. In addition to this, NRI had an empirical study of natural language analysis to investment judgment in 2017 [161].

4.2.4 Data Difference

In this section, we will compare both data from five perspectives.

Comparison 1 : Applicability

Firstly, Twitter data has more applicable to more organization. Since only public companies have the stock price data, and the traditional event study method can evaluate only public companies. However, in the proposed method, all entities, including not only public companies but also organizations not having stock data such as private companies, government agencies, and non-profit organizations, will be evaluated, as long as Twitter data are available for them. Therefore, from the applicability perspective, the Twitter dataset is more applicable to many situations.

Comparison 2 : Users Amount

From user amount perspective, we believe that larger population reflects more diversified opinions and the population of Twitter users is greater than one of stock traders. According to statistical data in Japan, although there are 14 million individual stock traders [162, 163], Twitter has 40 million active users [164]. In addition to this, the people who reflect opinions via stock are only stockholders, and actual influential stakeholders are limited. It means that Tweet data can reflect broader views for the security incident.

Comparison 3 : Incentive of Stakeholders

We think Twitter data has more honest opinions against information breach because the incentive of stakeholders is different.

The primary purpose of stock trading is not an evaluation of corporate value or a reflection of opinions, but gaining margin or capital gains by trading. It means that the stock price does not always reflect the actual opinion of the security incident. For example, some strategic traders may purchase stocks after security

breach disclosure because they get them with a small price to sell them at a higher price in the future. In another case, some traders may keep stocks because security breach is temporary events and it is not so impressive from long-term perspectives. Therefore, the stock price may not reflect the impact of valuation.

On the contrary, the primary purpose of Twitter is communication, and Twitter users use these services to publish, spread and gather the news, valuable information, and individual opinion. In another word, active Twitter users do not tweet their opinions by monetary incentives, and all tweets related to incident response is honest opinions against the organization and incidents.

Comparison 4 : Side Effect Elimination

We consider that our proposed methods can eliminate unrelated data or another event effects from Twitter data if several incidents or events related to reputation risks are handled simultaneously, and the analysts can focus on the analysis of the particular event deeply. In a multi-incident situation, it is difficult to distinguish one incident impact from the others in stock price data. However, in Twitter dataset, analysts can pick up relevant data with keyword search and filter out irrelevant data from the dataset. This side effect elimination is one of the unique capabilities our proposed methods, and Twitter dataset has.

Comparison 5 : Real-Time Evaluation

As a final point, we consider that Twitter data has real-time evaluation capability rather than stock data. Stock data tends to be usually delayed to reflect the market opinions to actual price because stock price will be decided by matching of sell order and buy order. In addition to this, real-time evaluation by stock data is only available when stock exchange markets open. In another word, the stock price is not useful to evaluate the reputation on the weekend or after closing markets, although negative reputation spread in anytime. On the contrary, Twitter data can reflect opinions in real-time because publishing tweets requires no prerequisite

process and the analysts can use these data as long as Twitter users comment on them actively.

Also, Twitter data is also effective from risk communication and social media communications domain, because modern corporate communication utilizes social media and many important announcements also tends to be published on Twitter. By using the proposed method, we consider that PR (Public Relations) or Marketing department in each victimized organizations can utilize this approach to analyze the impact of each announcement.

4.2.5 Dataset Sumamry

In this section, we discussed the similarity and difference of both data. In Section 4.6, based on the similarity assumption, we have several case studies by applying the proposed approach. We would like to notice that we will only verify the similarity of both data, and also the effectiveness of "Applicability". We note that the impact analysis caused by the other data differences will be discussed as a future work.

4.3 Event Study Methodology

As we mentioned in Section 2.4.2, event study methodology is very popular methods to analyze intangible costs. The original concept of event study methodology is, by using stock price, the evaluation of the impact of public announcement or an event.

4.3.1 Terminology

As the terminology, we define following keywords; *Event Day*, *Estimation Window*, and *Event Window*. Also, we depict the relationship between them by using a timeline in Figure 4.1. (Also, we use capital letter T for time variable of traditional event study methodology because the unit time of traditional event study is a day.)

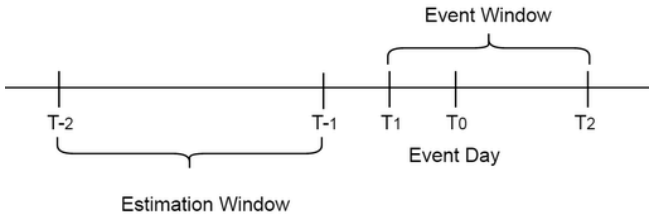

Figure 4.1: Timeline in Event Study

Event Day ($T_0 = 0$)

The day of event occurrence or public announcement day. (Event Day is defined based on the purpose)

Estimation Window

It is a particular period before Event Day (such as $T_{-2} = -200$ and $T_{-1} = -5$), and we use this window to estimate the stock price of Event Window as if the event does not happen.

Event Window

It is the period around the Event Day before and after (such as $T_1 = -1$ and $T_2 = 10$), and we use this window to analyze the impact of events.

In event study method, by using the change of stock price in estimation window, we estimate the stock price in Event Window as if the event (or public announcement) does not happen. It is called *Theoretical Stock Price without Event*. After the estimation of expected normal stock price, we analyze the difference between actual stock price and theoretical stock price and examine the impact of the event. In event study methodology, we usually look at the daily return ratio to normalize the value for future comparison since the absolute gap value between theoretical stock price, and the actual stock price is entirely different in each stock.

4.3.2 Step 1: The Estimation of Theoretical Stock Price

The first step is the estimation of "Theoretical Stock Price without Event" in event window, by using estimation window information. Usually, the estimation

considers the market trends, and we will create the market model with equally-weighted index (such as NYSE, NASDAQ or TOPIX).

$$R_{iT} = \alpha_i + \beta_i R_{mT} + \epsilon_{iT} \tag{4.1}$$

In above equasion, we define R_{iT} and R_{mT} as follows.

$$R_{iT} = \frac{P_{iT} - P_{i(T-1)}}{P_{i(T-1)}} \tag{4.2}$$

$$R_{mT} = \frac{P_{mT} - P_{m(T-1)}}{P_{m(T-1)}} \tag{4.3}$$

R_{iT} is a daily stock return ratio of firm i in day T, and R_{mT} is a daily stock return ratio of market in day T. P_{iT} means the stock price of firm i in day T and P_{mT} means the stock price of market in day T. α_i and β_i is the intercept and the slope of the market model for a firm i determined by the least-square method. ϵ_{iT} is disturbance term. In the calculation of α_i and β_i, we usually use the equally-weighted index with sufficient estimation window because it is a typical index to reflect the market and economy.

After creating a market model, we can estimate "Theoretical Stock Price without Event" in event window by calculating the theoretical stock price.

4.3.3 Step 2: The Calculation of AR

In next step, we calculate *Abnormal Returns* (AR) of firm i in day T in event window by using following formula (4.4) when we abbreviate theoretical stock price in Event Window as $Model\text{-}R_{iT}$. $Model\text{-}R_{iT}$ is defined as formula (4.5). AR means that the difference between the actual stock return ratio and the return ratio of theoretical stock price in event period, and AR will be an indicator to describe the impact of the event in one day.

$$AR_{iT} = R_{iT} - Model\text{-}R_{iT} \tag{4.4}$$

$$Model\text{-}R_{iT} = \alpha_i + \beta_i R_{mT} \tag{4.5}$$

4.3.4 Step 3: The Calculation of CAR

In the third step, we calculate *Cumulative Abnormal Returns* (CAR) of firm i for event window. We sum up all of AR values in event window. CAR will be an indicator to describe the impact of the event in event window and to quantify the magnitude of event impact. Therefore, we can know the size of intangible cost by comparing this value. Many previous works analyze the size of intangible costs by comparing the CAR of each analysis group.

$$CAR_i = \sum_{T_1}^{T_2} AR_{iT} \tag{4.6}$$

4.3.5 Step 4: The Statistical Test

As a final step, we confirm whether or not an event is influential to stock price by the statistical test. We define null hypothesis like following, and we verify whether or not the equations are following to the normal distribution. In this following formula, σ is the standard deviation of Abnormal Return (AR) in estimation window, and T is the window of calculating Cumulative Abnormal Returns.

- H_0 : Event does not affect to stock price, and AR is 0
- H_0 : Event does not affect to stock price, and CAR is 0

$$\frac{AR_{it}}{\sigma} \approx N(0,1) \tag{4.7}$$

$$\frac{CAR_{it}}{\sqrt{T * \sigma^2}} \approx N(0,1) \tag{4.8}$$

4.4 Sentimental Analysis

Before discussing our proposed method, we would like to describe a basic overview of sentimental analysis. The sentimental analysis is one of the computational linguistics approaches to estimate the sentiment and emotion of writer by analyzing text. As a simple method, by using Sentiment Polarity Dictionary (the mapping between vocabulary and the emotion quantified value), we count vocabularies expressing emotion and quantify the emotion of sentences. Since this simple method has a lot of challengings, many researchers have proposed sophisticated methods.

4.4.1 Technology

Morphological Analysis

One of the fundamental technology of sentiment analysis is morphological analysis. This technology divides natural language into morpheme (minimum unit of language). Especially, in Japanese language, sentences do not have the separator, and sentence analysis is very complicated. As a Japanese morphological analysis library, ChaSen [165] and MeCab [166] are very famous libraries.

Sentiment Polarity Dictionary

As a second fundamental technology, sentiment polarity dictionary is the mapping between vocabulary quantified polarity value each vocaburary has. By using this dataset, we can estimate the magnitude of emotion of each sentense. There are various approach to quantify emotions each vocaburary has, but as sentiment polarity dictionary, "Sentimental Word Dictionary" by Takamura [167, 168], "Polar Phrase Dictionary" by Kaji and Kitsuregawa [169, 170], "Japanese Sentiment Polarity Dictionary" by Inui and Okazaki [171–173] are very famous dictionaries.

4.4.2 Research Trends

Sophistication of Sentiment Analysis Algorithm

One of the latest research trends is the sophistication of sentiment analysis algorithm. In natural language processing, the meaning is entirely dependent on the context, and the simple approach may not evaluate actual emotion such as ironic expression. Paper [174] proposed the sentiment analysis algorithm for ironic expression by using machine learning. Especially, machine learning improves the analysis accuracy, and some cloud-based APIs with machine learning approach are available [175, 176].

The Application of Sentiment Analysis Technology

Another research trend is the application of sentiment analysis technology usage, as we mentioned in Section 4.2.3. As another example, paper [177] applied Twitter sentiment analysis to the estimatoin of election results and political trends, and there are various research papers from computational politics area.

4.5 Proposed Model

In order to evaluate the impact of information leakage and unauthorized access, our research proposes the application of event study methodology with TRI (Tweet Reputation Index). Our proposed model is novel in the process of calculating TRI dataset and applying the event study methodology to this data although event study methodology is same. Our proposed model consists of four core modules.

4.5.1 Terminology

Although the fundamental idea is as same as the event study with stock price data, we define following keywords. (Also, we use small letter t for time variable of proposed methodology because the unit time is user-definable based on purpose. In this paper, we define unit time is one-hour.)

Tweet Sentiment Value (TSV)

The value quantifying the sentence by analyzing one Tweet.

Cumulative Tweet Sentiment Value (CTSV)

The accumulated value of TSV (Tweet Sentiment Value) by unit time

Tweet Reputation Index (TRI)

Time-Series Accumulated data of CTSV (Cumulative Tweet Sentiment Value) and it shows the time-series change of cumulative emotions against the targeted entities. As same as the stock price, this data is used for the analysis of event study methodology.

Event Time ($t_0 = 0$)

Time of event occurrence or public announcement. (Event Time is defined based on the purpose.)

Estimation Window

It is a particular period before Event Time (such as $t_{-2} = -200$ and $t_{-1} = -5$), and we use this window to estimate the TRI in Event Window as if the event does not happen.

Event Window

It is the period around the Event Time before and after (such as $t_1 = -1$ and $t_2 = 144$), and we use this window to analyze the impact of events.

4.5.2 Module 1 : Tweet Gathering Module

This module gathers tweets based on the keywords. We develop this module with Google Apps Script and Twitter API. One of the differences between stock price data and Twitter is that Twitter API only allows to access last seven days. Since this module will be executed after knowing the incident, the data for estimating the expected normal returns is limited to only last seven days in maximum. In our empirical experiment, we use the keywords of organization's name or service

name for gathering tweets. In the case that collected data have many irrelevant data, as we discussed Section 4.2.4, we can narrow down data by using the specific keywords.

4.5.3 Module 2 : Sentimental Analysis Module

This module evaluates the gathered tweets by using sentiment polarity dictionary and calculates TSV (Tweet Sentiment Value). We implement this module with Python with MeCab (a Japanese morphological analysis library) and "Semantic Orientations of Words" by Takamura as Sentiment Polarity Dictionary. In details, this module matches the separated words with a sentiment polarity dictionary after morphological analysis. Then, when the module finds out the corresponded vocabulary, this module determines the value of sentiment polarity in the dictionary and calculates the total value as TSV. Generally speaking, the long sentence has significant TSV value, and general sentiment research uses the average value to normalize the effects of sentence length. However, since Twitter has 140 words limitation, we used total value for this analysis.

4.5.4 Module 3 : TRI Calculation Module

This module creates TRI (Tweet Reputation Index), and it is implemented with statistical analysis language R.

Step 1 : The calculation of CTSV

As a first step, we calculate the accumulated value of TSV(Tweet Sentiment Value) by unit time to output CTSV (Cumulative Tweet Sentiment Value). In this paper, we define the unit time as one hour.

Step 2 : The calculation of TRI

Based on CTSV (Cumulative Tweet Sentiment Value), we calculate TRI (Tweet Reputation index). When we define CTSV of firm i in time t as $CTSV_{it}$, the TRI_{it} is defined as follows.

$$TRI_{it} = TRI_{i(t-1)} + CTSV_{it} \tag{4.9}$$

4.5.5 Event Study Analysis Module

This module executes event study analysis to TRI, and it is implemented with statistical analysis language R.

Step 1: The Estimation of Theoretical Tweet Reputation Index

We define Event Time as $t_0 = 0$ and estimate the "Theoretical Tweet Reputation Index without Event" of firm i by using Estimation Window. In the estimation, we create the estimation model of Theoretical TRI based on only time-series change, because Twitter data do not have reliable trends information like market stock prices such as NYSE, NASDAQ, or TOPIX. In traditional event study with stock price data, although we have the estimation of theoretical stock price value by using normalized daily stock return ratio, we change the detailed process in TRI case. We estimate the theoretical TRI with absolute value by model, and then, normalize them by calculating return ratio. It is because TRI usually has positive and negative value and calculation will be complicated.

$$Model\text{-}TRI_{it} = \alpha_i + \beta_i t + \epsilon_{it} \tag{4.10}$$

$Model\text{-}TRI_{it}$ is a Theoretical TRI of firm i in time t, and α_i and β_i is the intercept and the slope of the model for a firm i determined by the least-square method by time t and estimation window. ϵ_{it} is disturbance term. After the calculation of Theoretical TRI of Event Window by using Estimation Window, we normalize the value by calculation of return ratio of TRI R_{it}, and return ratio of Theoretical TRI $Model\text{-}R_{it}$.

$$R_{it} = \frac{TRI_{it} - TRI_{i(t-1)}}{TRI_{i(t-1)}} \tag{4.11}$$

$$Model\text{-}R_{it} = \frac{Model\text{-}TRI_{it} - Model\text{-}TRI_{i(t-1)}}{Model\text{-}TRI_{i(t-1)}} \tag{4.12}$$

Step 2: The Calculation of Abnormal Return (TRI-AR)

In Event Window, we calculate $TRI\text{-}AR_{it}$ (Tweet Reputation Index Abnormal Return) of firm i in time t. $TRI\text{-}AR_{it}$ means the difference between TRI and Theoretical TRI and equation is following.

$$TRI\text{-}AR_{it} = R_{it} - Model\text{-}R_{it} \tag{4.13}$$

As same as AR (Abnormal Return) in stock price data, $TRI\text{-}AR_{it}$ elaborates the impact of events in Twitter in unit time.

Step 3: The Calculation of TRI-CAR

As next step, we calculate $TRI\text{-}CAR_i$ (Tweet Reputation Index Cumulative Abnormal Return) in Event Window.

$$TRI\text{-}CAR_i = \sum_{t_1}^{t_2} TRI\text{-}AR_{it} \tag{4.14}$$

As same as CAR (Cumulative Abnormal Return) in stock price data, $TRI\text{-}CAR_i$ elaborates the impact of events on Twitter, and tell us the size of intangible cost.

Step 4: The Statistical Test

As a final step, we confirm whether or not an event is influential to TRI by the statistical test. We define null hypothesis like following, and we verify whether or not the equations are following to the normal distribution. In this following formula, σ is the standard deviation of Abnormal Return (TRI-AR) in Estimation Window, and T is the window of calculating Cumulative Abnormal Returns (TRI-CAR).

- H_0 : Event does not affect to stock price, and TRI-AR is 0

- H_0 : Event does not affect to stock price, and TRI-CAR is 0

$$\frac{TRI\text{-}AR_{it}}{\sigma} \approx N(0,1) \tag{4.15}$$

$$\frac{TRI\text{-}CAR_{it}}{\sqrt{T * \sigma^2}} \approx N(0,1) \tag{4.16}$$

4.6 Experiment

In order to apply the proposed method to actual examples, we collect Twitter data related to security incidents. By using examples, we discuss the effectiveness of event study with Twitter sentiment data.

4.6.1 Case 1 : GMO Payment Gateway

In 2017 March, GMO Payment Gateway, leading credit card settlement service provider, experienced significant security breach from settlement service infrastructure, and they leaked 0.72 million records including payment card and personally identifiable information. The primary cause of this incident was abusing Apache Struts2 Vulnerability (CVE-2017-5638) released March 6, but they detected the unauthorized access on March 9. One of the substantial criticism on GMO Payment Gateway was they leaked security code (CVV) that PCI DSS prohibited to store them. This hacking brought the impact on the settlement mechanism of metropolitan tax by Tokyo Government Office and life insurance by Japan House Finance Agency.

Figure 4.2 shows that the results of TRI-AR (Blue) and TRI-CAR (Orange), and Table 4.1 shows the experimental conditions. Also, we confirm that all CAR in event window is 1% significance.

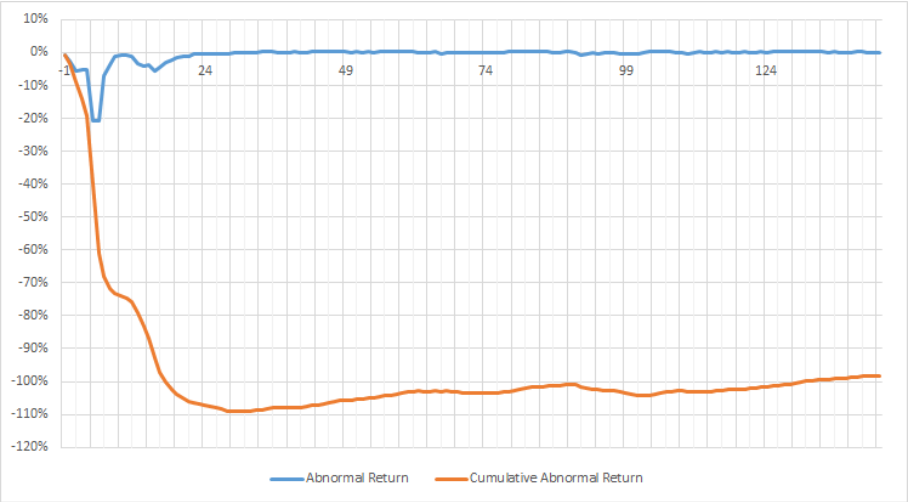

Figure 4.2: Abnormal Return / Cumulative Abnormal Return

Table 4.1: Experimental Condition (GMO Payment Gateway)

No.	Experiment Condition	Experiment Value
#1	Search Keyword	"GMO"
#2	Tweet Gathering Window	2017/03/03 03:51 ∼ 2017/04/13 19:07
#3-1	Total Tweet Amount[1]	114,623 Tweets
#3-2	Total Tweet Amount (Modified)[2]	24,667 Tweets
#4	Event Time ($t = 0$)	2017/03/10 19:00
#5	Estimation Window ($t = -65 \sim t = -5$)	2017/03/08 02:00 ∼ 2017/03/10 14:00
#6	Event Window ($t = -1 \sim t = 144$)	2017/03/10 18:00 ∼ 2017/03/16 19:00
#7	Tweet Amount (Estimation Window)[3]	9,137 Tweets
#8	Tweet Amount (Event Window)[3]	20,079 Tweets

[1] The sentiment analysis is focusing on the tweets with Japanese language.
[2] The keyword "GMO" is also the abbreviation of "Genetically Modified Food". We put a flag to eliminate the tweets mentioning "genetically modified food".
[3] Amount of Tweets Data is calculated without the elimination of "Genetically Modified Food" tweets.

TRI-CAR of GMO Payment Gateway shows substantial negative impact by security incidents. However, we assume that TRI-CAR will be back to zero or positive when victimized organizations have a great response to security incidents including PR, compensation, customer follow-up, and timely information disclosure. However, when the response is not remarkable, CAR is staying after having negative value. Therefore, from an incident response perspective, we think the

shape of TRI-CAR graph needs to be "V" shape for minimizing the damage of intangible cost.

Supplementary Analysis 1: Correlation with Stock Price Data

We analyze the linkage between stock price data (Closing Price) and the value of TRI-CAR. We re-calculate TRI-CAR with per weekday unit time because unit time in stock price data is per weekday, but unit time in Twitter data is per hour. Table 4.2 and Figure 4.3 visualizes the data, and statistical analysis shows the strong correlation between them.

Table 4.2: The Comparison between Stock Price and Twitter Data

Analyzed Window	CAR	TRI-CAR	Correlation Coefficient
$T[-1, 1]$	-19.92%	-105.06%	0.9986
$T[-1, 3]$	-16.00%	-105.17%	0.9584
$T[-1, 5]$	-18.55%	-97.92%	0.9521
$T[-1, 10]$	-19.32%	-84.06%	0.9203

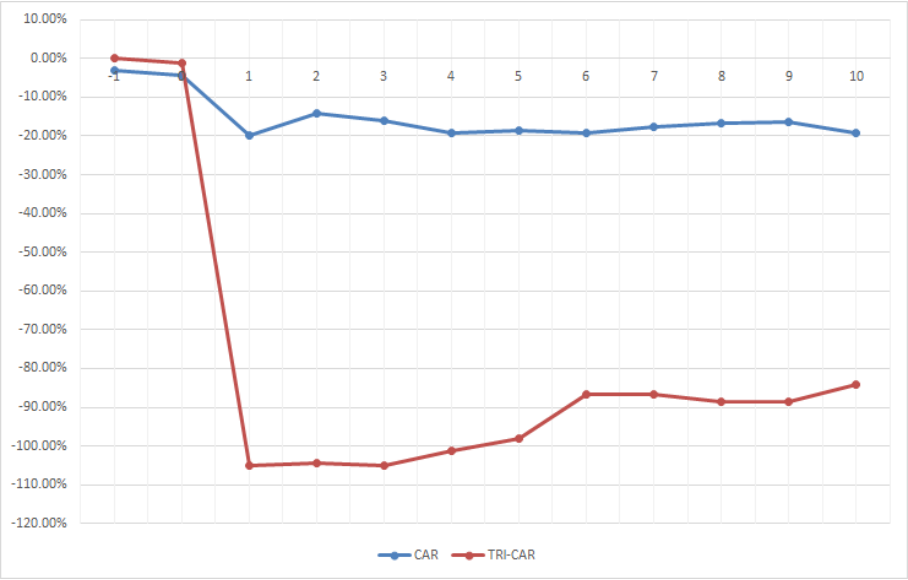

Figure 4.3: The Comparison between Stock Price Data and Twitter Data

Supplementary Analysis 2: Impact of Apache Struts2 Vulnerability

Apache Struts2 vulnerability (CVE-2017-5638) was significant impacts because many websites were affected by this vulnerability and damaged. Since we collected the Twitter data of five organizations including GMO Payment Gateway case, Figure 4.4 shows the results of CAR, and we have additional comments for each organization.

Case 1-0 : GMO Payment Gateway

They used vulnerable Apache Struts2 in their credit card settlement service platform, and it affected many customers.

Case 1-1 : Metropolitan Tax Payment Website

They used the platform of GMO Payment Gateway, and approximately 670,000 records were leaked. The volatility of TRI-CAR is very similar to TRI-CAR of GMO Payment Gateway.

Case 1-2 : Life Insurance request form by JHFA

They used the platform of GMO Payment Gateway, and they leaked 43,540 records. JHFA (Japan House Finance Agency) has high negative value in TRI-CAR because JHFA stored security code (CVV) of credit card and it is prohibited by PCI DSS.

Case 1-3 : JINS

Their platform of online shop has been attacked, and more than 1.2 million records of personally identifiable information because of Apache Struts2 vulnerability. It has more negative value than GMO Payment Gateway in TRI-CAR. We assume it is because a large number of data has been leaked, and JINS had data breach by abusing Apache Struts2 vulnerability in 2013. Therefore, they have more reflection rather than GMO example.

Case 1-4 : JETRO

JETRO leaked approximately 20,000 records of e-mail addresses. TRI-CAR

is smaller than others because it had the more low impact rather than other incidents.

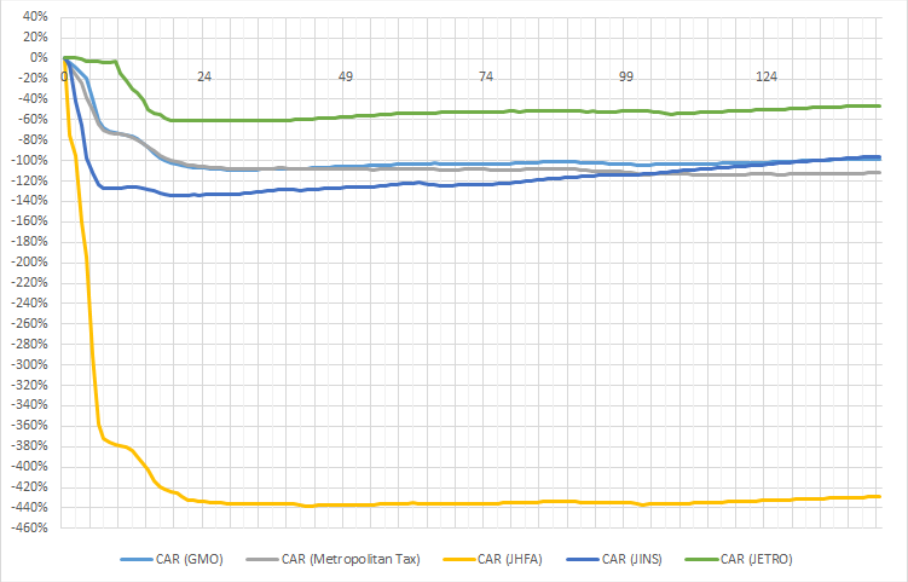

Figure 4.4: The Comparison of Apache Struts2 Vulnerability Impact

4.6.2 Case 2 : Correlation Analysis with Stock Price

By picking up four victimized organizations having stock price data, we confirm the correlation between stock price data and Twitter data. Since we collected the Twitter data of four organizations including previous cases, Figure 4.5 shows the visualized change of them, and Table 4.3 - Table 4.6 shows the linkage between them.

Case 2-1 : GMO Payment Gateway

They used vulnerable Apache Struts2 (CVE-2017-5638) in their credit card settlement service platform, and it affected many customers in March 2017.

Case 2-2 : JINS

Their platform of online shop has been attacked in March 2017, and more than 1.2 million records of personally identifiable information because of Apache Struts2 vulnerability (CVE-2017-5638).

Case 2-3 : Nipon TV

In July 2016, Nippon TV leaked approximately 430,000 records by abusing OS command injection in the web application.

Case 2-4 : Piped Bits

In June 2016, SPIRAL EC, EC platform service for apparel industries by Piped Bits, was compromised. As maximum, this hacking brought the impact on the users of this platform, and they leaked approximately 1 million records.

Based on this analysis, firstly we can say, in the short term ($T = -1 \sim T = 1$), both data has a strong correlation, and correlation coefficients are more than 0.8. Secondly, we can say some examples have the strong correlation in the long term ($T = -1 \sim T = 10$).

Figure 4.5: The Comparison of Stock Price and Tweet Reputation Index

Table 4.3: Correlation Analysis 1 : GMO (same as Table 4.2)

Analyzed Window	CAR	TRI-CAR	Correlation Coefficient
$T[-1,1]$	-19.92%	-105.06%	0.9986
$T[-1,3]$	-16.00%	-105.17%	0.9584
$T[-1,5]$	-18.55%	-97.92%	0.9521
$T[-1,10]$	-19.32%	-84.06%	0.9203

Table 4.4: Correlation Analysis 2 : Nippon TV

Analyzed Window	CAR	TRI-CAR	Correlation Coefficient
$T[-1,1]$	-1.97%	-15.97%	0.8020
$T[-1,3]$	-3.85%	-6.48%	-0.1909
$T[-1,5]$	-	-	-
$T[-1,10]$	-	-	-

Table 4.5: Correlation Analysis 3 : Piped Bits

Analyzed Window	CAR	TRI-CAR	Correlation Coefficient
$T[-1,1]$	-13.03%	-613.75%	0.9954
$T[-1,3]$	-12.95%	-583.05%	0.9941
$T[-1,5]$	-8.34%	-565.44%	0.9506
$T[-1,10]$	-9.54%	-531.94%	0.7843

Table 4.6: Correlation Analysis 4 : JINS

Analyzed Window	CAR	TRI-CAR	Correlation Coefficient
$T[-1,1]$	-1.45%	-112.93%	0.8633
$T[-1,3]$	-0.43%	-97.36%	-0.0862
$T[-1,5]$	-2.26%	-79.82%	0.0517
$T[-1,10]$	-5.06%	-41.67%	-0.2103

4.6.3 Case 3 : Applicability

As we discussed previously, this proposed method can evaluate the organizations that do not open the stock price or accounting information such as non-public companies. In order to have deeper analysis, we pick up the security breach by JTB in June 2016. JTB is a very famous company as a travel agency, but they leaked approximately 7.93 million records of personally identifiable information by

APT attack [181].

Based on the experimental condition in Table 4.7, we have same analysis and Figure 4.6 shows the results of TRI-CAR (Tweet Reputation Index Cumulative Abnormal Returns).

Table 4.7: Experimental Condition (JTB)

No.	Condition Item	Experiment Parameter
#1	Search Keyword	"JTB"
#2	Tweet Gathering Window	2016/06/09 04:03 ～ 2016/06/30 21:25
#3	Gathered Tweet	79,864 tweets
#4	Event Time ($t = 0$)	2016/06/14 15:00
#5	Estimation Window ($t = -65 \sim -5$)	2016/06/11 22:00 ～ 2016/06/14 10:00
#6	Event Window ($t = -1 \sim 240$)	2016/06/14 14:00 ～ 2016/06/24 15:00
#7	Tweet Amount (Estimation Window)	3,558 tweets
#8	Tweet Amount (Event Window)	61,820 tweets

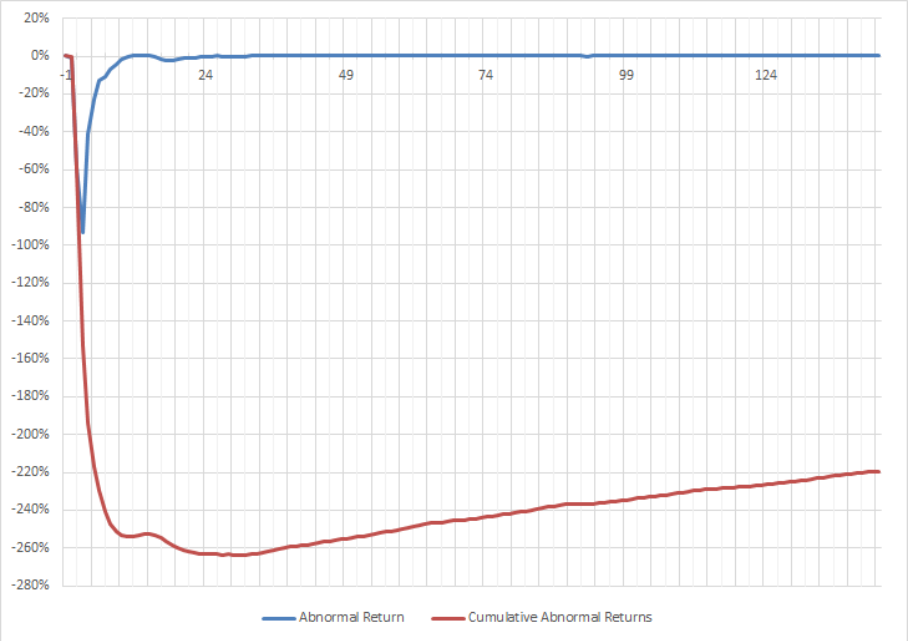

Figure 4.6: The Application of Non-Public Organizations (JTB)

Based on this results, we think this event is more influential than GMO breach cases in Figure 4.2 because TRI-CAR in JTB has double than GMO-PG example. From this standards, we can compare the impact of intangible cost even though

the organizations do not have stock price data.

4.7 Conclusion

In this chapter, we proposed event study method using Twitter sentiment analysis data for intangible cost estimation. Also, our research demonstrated the effectiveness to visualize the impact on the organizations not having stock price data or accounting information. We think this methodology has a lot of capability to support security incidents management although we also have various future works of evidence-based demonstration. Appendix A shows hypothetical examples about "side effect elimination" or "intangible cost in governmental agency". We have several future works.

The first challenge is the big data analysis by using this proposed method. The existing research about event study is analyzing trends by collecting many cases and categorizing cases based on characteristics including attack vectors, the number of leaked records, industries, and countermeasures. In order to analyze the trends with our proposed framework, we would like to continue to collect Twitter data. Especially, we would like to focus on unique analysis such as a difference between public companies and non-public companies, because only our proposal can analyze these issues.

The second challenge is the sophistication of this model. For example, about Sentimental Analysis Module, we use the most simple method in this module, but we would like to apply latest research achievement of text mining and computational linguistics on this module. On top of that, we continue to have validation to improve the accuracy. One of the consideration is, TRI data may not be accurate when we have only limited number of Twitter data such as less than 1000 tweets as the total. We would like to confirm the accuracy of TRI (Tweet Reputation Index) analysis in these cases. Finally, we will have supplemental study about the relationship between the decrease of Tweet Reputation Index and the amount of

news Internet pickup. It is because it may disclose the relationship between the how news article on the Internet affects the decrease of TRI.

The third challenge is the proposal of countermeasures based on this method. Since risk communication and incident communication is critical parts of security incidents, we would like to apply this method to these researchers.

Because of this challenge, we would like to contribute the security management against intangible cost.

Chapter 5

The Effectiveness of Cyber Risk Insurance

5.1 Introduction

Cyber risk insurance is an insurance that covers overall damage by security incidents. It is an extension of E&O (Errors and Omissions) insurance, and first insurance was available around 2005 [183]. Currently, cyber risk insurance is one of the practical options of "Risk Transfer" in Risk Treatment Strategy. As an assumption, we know that we cannot make the cybersecurity risk zero chance no matter how much we spend on cybersecurity control, and cyber risk insurance can change the volatile security incident response expense to fixed cost. A white paper [184] by Latham & Watkins pointed out that "cyber insurance policy can provide a critical last line of defense to remediate the damage and cover the losses that result from a successful cyber attack," and this insurance works as more comprehensive risk management tools. Also, the white paper [18] "Cybersecurity Management Guidelines" published by METI in 2015 mentions about cyber risk insurance, and it is a notable description.

5.1.1 Cyber Risk Insurance Market

Since security incidents are very popular around the world, cyber risk insurance has been spotlighted. According to PwC annual report in 2016 [185], 59% of enterprises purchased cyber risk insurance. In addition to this, more than 36%

of insurance purchased companies intensified the cybersecurity program, because more strong cybersecurity program can reduce the premium. Also, another PwC report "Insurance 2020 & Beyond: Future of Cyber Insurance" [186] mentioned that, although global annual revenue by cyber risk insurance was approximately 2.5 billion USD in 2015, it will be 5.0 billion USD in 2018, and it will be 7.5 billion USD in 2020.

In the United States, cyber risk insurance has been popular, and it is common risk treatment strategy since U.S. has many regulations and class action. In addition to this, the governmental agencies also have recommended to purchase cyber risk insurance. SEC DCF (Division of Corporation Finance in U.S. Securities and Exchange Commission) suggested to describe the coverage of cyber risk insurance in the guidance "CF Disclosure Guidance: Topic No. 2" published in 2011 [187]. Also, SEC OCIE (Office of Compliance Inspections and Examinations in U.S. Securities and Exchange Commission) recommended to purchase the insurance to financial services industries in 2014 guidance [188]. In addition to this, according to the report by NRI SecureTechnologies [189], they investigated the motivation of U.S. companies to purchase cyber risk insurance, and typical reasons were following.

- Starting a new business with high-security risk
- Having sensitive information because of business nature
- Preparing the cost for security incidents

On the contrary, the awareness of cyber risk insurance in Japan was very low, and only 28% knew the cyber risk insurance according to the IPA report [190] published in June 2015. On top of that, according to the report by NRI SecureTechnologies, 56.8% of U.S. companies, and 32.1% of Singapore purchased this insurance, but only 7.8% of Japanese companies bought them. This showed that the spread of cyber risk insurance in Japan has been halfway.

5.1.2 Challange

The emerging challenge is that we do not have enough quantitative analysis about the effectiveness of cyber risk insurance that is a new risk finance method. Cyber risk insurance is a typical risk transfer approach, but the mechanism and deployment of cyber risk insurance are in dawning age. In addition to this, the occurrence of cyber risk is different from other hazards. We can not use traditional actual science approach, and insurance companies are now considering the cyber risk assessment method. However, since the awareness of cyber attack is increasing, the cost for incident response will be large in the future. Therefore, the cyber risk insurance will be a more valuable solution since cyber risk insurance makes the volatile incident cost to fixed cost. Therefore, we think we need to analyze the effectiveness of cyber risk insurance by using simulative approach.

5.1.3 Contribution

As our contribution, we evaluate the effectiveness of cyber risk insurance from the quantitative perspective. Firstly, we analyze the mechanism, current service, and challenge of cyber risk insurance from the technical and economic perspective. Secondly, we have cost-benefit analysis from the quantitative perspective. Since the results of simulation will be changed based on the risk scenario such as the occurrence of information leakage or the number of leaked data, we have the analysis by using Monte-Carlo simulation. The benefit of this model is we can add and modify the initial parameters based on the risk preference and risk scenario. In the case study by using a virtual company, we acquire the result that ROSI （Return on Security Investment） is approximately 200 times, and the coverage of cyber risk insurance is approximately 65%. We conclude that cyber risk insurance is beneficial for security management and risk management perspective.

5.2 Basics and Challenge of Insurance

Cyber risk insurance handles new types of risks, and cybersecurity threats have various unique problems. In this section, we explain the primary mechanism of cyber risk insurance, and general issues that cyber risk insurance has by applying information economics.

5.2.1 Insurance Mechanism

In order to understand cyber risk insurance, it is important to comprehend the mechanism of general casualty insurance or life insurance. This mechanism is theoretically very simple. Generally speaking, casualty insurance is a risk diversification method that all insurance policyholders cover the damage on a particular person via premium. In this perspective, the design of accurate premium based on information economics and game theory is critical for sustainability.

Statistical Data and Law of Large Numbers

In order to consider appropriate insurance premium, knowing statistical data of casualty is necessary. Generally speaking, it is difficult to know the probability of damage happening to particular individuals. However, based on the concept of the law of large numbers, we can figure out the rules of probability against population when we have a particular population. In automobile insurance, it is hard to estimate the likelihood of car accident for a particular person, but we can statistically determine the car accident probability in one year when we consider many drivers. From these statistical data, the insurance companies determine the premium.

Risk Profile Identification and "Adverse Selection" Elimination

In the calculation of premium in the statistical data, the identification and classification of the risk profile of each insured entity is a general approach. It is because the probability of having damage is different by each risk profile. For example, in

the case of life insurance and medical insurance, some occupations such as Alpinist or performer cannot purchase the insurance or have some specific limitation in the acquisition of insurance policy because these occupations have more risks to have accidents or damage compared with the other categories. As another evidence, medical insurance increases the premium based on ages, or automobile insurance has the grading system based on the frequency of use or driving history. This design is for handling each risk profile correctly.

These risk profile identification and classification can eliminate the problem of "adverse selection". Adverse selection is also known as Gresham's law or Lemon Problem in the economics. It is a phenomenon that low-risk insured terminate the contract and only high-risk insured remain to purchase the insurance, when insurance companies do not have risk profile identification and classification. If insurance companies offer the same premium to all insured without knowing the detailed profile information from them, high-risk insured actively buy the insurance because the premium is comparatively cheaper for high-risk insured. After that, high-risk people claim the payment based on the policy, and usually, insurance companies decide to increase the premium to sustain the insurance. In another word, the increased premium will be comparatively expensive for low-risk insured and they will terminate the contract. As the results, only high-risk people continue to purchase the insurance, and it is not good for maintaining the insurance. To assure the quality of insurance services, the identification of risk profile of insured, and the application of appropriate statistical data to each profile is crucial to determine the appropriate premium.

5.2.2 The Challenge of Cyber Risk Insurance

Cyber risk insurance has several large challenges from above perspectives.

The Shortage of Statistical Data

The first challenge is, as we mentioned, only limited statistical data is available. Insurance companies think traditional methodology cannot be applied to cyber risk because statistically significant actuarial data is not available [191] although academic researchers have various research from economic and mathematical perspectives [192–200]. As an assumption, victimized enterprise do not tend to disclose the details of security incident actively, and it will cause the problems that insurance companies cannot accumulate the necessary data for statistical analysis.

Because of this situation, especially in Japan, we have an only limited technique to estimate total costs such as estimation of an extraordinary loss in the financial report or official investigation report published by each victimized company. On the contrary, SEC (U.S. Securities and Exchange Commission) issued a guideline to require information disclosure to public enterprises after having a cyber attack [187]. Also, Financial Service Agency in Japan started to consider the obligation of cyber risk disclosure in financial statements by referring the direction in U.S. [201]. From this, Japanese government expected to improve not only the transparency to investors but also the awareness of senior management to information security risks.

From this situation, each insurance company has started to develop unique approaches to evaluate this problem. For example, Marsh established original analysis framework, Cyber IDEAL(Identify Damages, Evaluate, and. Assess Limits) [202]. It helps to calculate the premium and to provide risk analysis and evaluation service to clients. Also, Sompo Japan Nipponkoa Insurance had a collaborative project with Risk Management Solutions and University of Cambridge, and they also created their original model for cyber risks [203]. In addition to this, several start-up companies started to release risk analysis services. For example, Cyence has been a start-up company established in 2015, and they announced that they supported to create an economic model of cyber risk, and Marine &

Nichido Fire Insurance started to have a strategic alliance with them [204–206]. As an another example, UpGuard applied "credit scoring" methodologies to cybersecurity fields, and they are providing assessment service, CSTAR (Cybersecurity Threat Assessment Rating) that visualize the cybersecurity preparation and countermeasure [207]. This company was famous because they announced the plan of 17 million USD fundraising recently [208]. As another method, since many security consulting firms provide the visualization service of security countermeasure [209, 210], the insurance companies can apply these service for risk profiling. Especially, AIG, leading insurance companies, offers a lot of collaborative services with various companies, and they support the risk quantification and cyber risk mitigation of clients [211].

Also, from 2015, each insurance company started to publish the report related to cyber risk, and there are important reports such as the report by NetDiligence [212] or the report by Insurance Information Institute [213]. These data are valuable inputs for future improvement of the model.

The Shortage of Risk Profile Information

The second problem is that it is difficult to identify the risk profile of each client. The enterprise security should be comprehensively evaluated from various perspectives including organizational, operational, technical, compliance perspective. Visualizing and understanding entire picture of enterprise security is a very time-consuming issue. Also, since companies have strong incentive to avoid the rejection of purchasing insurance or the increase of premium, the companies avoid disclosing unnecessary information. Therefore, there is clear information asymmetry between corporations and insurance companies. The biggest challenge for each insurance company is how to visualize and evaluate cybersecurity risk of each enterprise, and it is a typical lemon market problem in information economics.

From information economics perspectives, there are two fundamental strategies. First one is "Signaling". Signaling is the technique to create the incentive

that the organization having information (insured companies) actively provides the information. For example, job hunting has typical information asymmetry, but the educational background, extracurricular activity, or certification is typical signaling. In cyber risk insurance field, the insurance companies offer the discount of premium to clients when companies acquire particular certification or following a specific guideline. This methodology has been used in the real field. For example, Tokio Marine and Nichido [214] provides 55 % discount as maximum, when companies have countermeasure based on "Cybersecurity Management Guidelines" [18] published by METI. Also, Sompo Holdings [215] offer 60% discounts as the maximum when clients acquire ISMS qualification from the designated security consulting firm. Also, for the SMEs (Small or Medium-sized Enterprise), the insurance companies offer the discount when they submit self-security assessment sheet [216].

The second approach is "Screening". Screening is that the organization not having information (insurance companies) offer several options to companies, and it resolves the information asymmetry based on what the companies chose. For example, in automobile insurance, they provide various options based on the driving distance or frequency, this choice makes the drivers open the usage of vehicles. It is also applicable to cyber risk insurance, and the insurance companies provide optional plans for clients, but it is not the perfect solution to resolve information asymmetry.

5.3 The Status Quo of Cyber Risk Insurance

The problem we pointed out in the previous section has been remaining, but several insurance companies [217–220] have provided cyber risk insurance as service. However, as Thomson Reuters mentioned [221] , the insurance companies may increase the premium or limit the coverage because of emerging challenges we mentioned previously. In this section, from each perspective of insurance, we discuss the status quo, and we address the emerging problems.

5.3.1 Coverage

Many insurances have similar coverage. Generally speaking, each insurance covers three types of areas including “damage liability”, “incident response” and “business impact”, and they include the general expense in actual incidents. According to the research by Financial Service Agency [222], the trends in overseas is same. However, since there are various class actions and penalties in abroad, the insurance covers the compensation of penalties and class actions. In another case, some insurance covers the internal fraud or security breach caused by 3rd party vendors, but the coverage totally depends on the insurance.

Also, some insurance companies extend the coverage of insurance. For example, leading insurance companies in U.S., AIG expands the coverage of cyber risk insurance into the damage of human bodies, and they provide the protection considering IoT or SCADA security [223]. Also, Mitsui Sumitomo Insurance provides the insurance for Bitcoin service providers [224], and Sompo Japan Nipponkoa Insurance provides the special coverage when the smart cars got unauthorized access and cause the damage [225].

There are several challenges for compensation coverage.

Challenge 1 : Gap Between Expectation and Actual Coverage

Firstly, there is the gap between actual coverage and assumption. Actually, according to the research paper ”UK Cyber Security - The Role of Insurance in Managing and Mitigating the Risk”, published by British Government [226], 52% of CEO assumed that the currently purchased insurance covered the cybersecurity incidents, but only 10% of companies purchased the insurance that covered the event related to cybersecurity incidents. The famous example is SONY that leaked the tremendous amount of information by unauthorized access to PlayStation Network in 2011. SONY had 171 million USD damage, but the insurance companies Zurich claimed that they were not liable to indemnify SONY for these cybersecurity costs because the insurance policy stated that only covered claims

for bodily injury, property damage or personal and advertising injury [227]. SONY and Zurich discussed this issue in legal court, but finally, Zurich agreed to settle for undisclosed amount [228].

According to Thomson Reuters [229], another interesting story related to the cyber attack and insurance is that some companies request the payment of ransomware damage by using K&R coverage (Kidnap and Ransom). The possibility of payout is small, but insurers pointed out that the companies try to use K&R coverage because they do not have direct cyber coverage or cannot meet initial cyber risk insurance policy. Currently, K&R insurers have been adapting to ransomware-related claims, and some are modernizing coverage by setting up Bitcoin accounts for clients to speed up ransom payments.

Challenge 2 : Vague Payment Condition

Secondly, some professionals pointed out the condition of payment is vague. According to NRI SecureTechnologies Ltd. [189], 30.6% of U.S. companies think the vague condition is problematic. Especially, the root-cause and impact are complicated in security incidents, and some insured believe that they only get limited payment compared with expectation. David Nathans, the speaker at RSA Conference 2017, had a presentation [230] to criticize to have cyber risk insurance. He had a broader investigation of U.S. cyber risk insurance policy from an engineering perspective, and he concluded that cyber risk insurance was not beneficial and the companies needed to spend the money for countermeasures, not to insurance. He argued these arguments because he thought the payment condition is too tight to comply with the insurance policy. Especially, he noted various examples such that insurance did not cover malware infection, the requirement of cybersecurity policy is very tight, or insured have to submit full analysis report of security incidents within a particular time window. However, although this is still controversial topics, we assume that the requirement for the insurance coverage is as mostly same as cybersecurity frameworks we discussed in Chapter 2. This presentation provides

an obvious lesson learned that cyber risk insurance is not the 1st option as cybersecurity countermeasure, but the supportive solution after having appropriate security control.

5.3.2 Premium

The premium of cyber risk insurance is different from each insurance companies because they do not have quantitive risk assessment method. The model case in Cyber Data Risk Manager [231] can provide the detailed information in U.S., and we show that the actual examples by Japanese insurance companies based on open sources. [232, 233].

- A company having 500 million JPY revenue need to pay approximately between 200,000 JPY to 850,000 JPY as premium in the case that maximum coverage is 1 billion JPY.
- An IT company having 10 billion JPY revenue need to pay four million JPY as premium in the case that maximum compensation is 500 million JPY.

As the report by NRI SecureTechnologies mentioned [189], 37.7% of U.S. companies stated that premium was expensive. Actually, according to the research paper by UK government [226], the ratio of premium to maximum compensation in cyber risk insurance was three times than the one of general liability insurance, and it was very expensive. As we mentioned in Section 5.2.2, this is one of the results not to having risk analysis by using actual traditional science.

5.3.3 Payment Claims

For payment claims, the report of "Cyber Liability & Data Breach Insurance Claims" published by NetDiligence has detailed analysis [212]. It stated that average payout for a large company was 3.04 million USD while the average payout in a Financial Services Sector was 1.3 million and in Healthcare Sector was 726,000 USD. Also, this report mentioned the cost for each record, and a maximum was1.6

million USD, an average was 17,000 USD, and the median was 39.82 USD. As Section 2.5 mentioned that, Insurance Target or Home Depot had covered 30% of the total expense, and cyber risk insurance is very useful tools to minimize the financial loss.

5.4 Cyber Risk Insurance vs. Outsourcing

As we mentioned, cyber risk insurance is one of the risk transfer methods, but we have another method called "Outsourcing" by using ASP and cloud service. According to the white paper by Bank of Japan [234], The general benefits of outsourcing are tremendous as follows.

- The business process and risk management can be sophisticated and efficient by outsourcing that has the specialty.
- The company can save the cost of outsourcing having the speciality.

Security countermeasure is one of this benefits, but there are several caveats.

Caveat 1 : Transferring Different Type of Risks

Firstly, the benefit of outsourcing is different from cyber risk insurance. Generally speaking, security investment has two functionality that is "the effect of decreasing the success ratio of attack" and "the effect to minimize the attack impact". Cyber risk insurance can reduce the impact, but outsourcing can reduce "success rate of attack" if the outsourcing vendor adequately has security countermeasure. However, as we discussed in next section, the each organization need to confirm the countermeasures and information management of outsourcing service provider. On top of that, from attackers' perspective, outsourcing service provider has many organizations' information, and it is a cost-effective target for them. Therefore, it may increase the risk in some cases.

Caveat 2: The Necessity of Security Control Review

Secondly, we need to confirm the appropriateness of data management of personally identifiable information and valuable information and the implementation and operation of security control. According to NRI SecureTechnologies [235], 61.8% of organizations consider the effective data governance structure when they choose the cloud service. On top of that, various guideline documents [236–239] are published from authorized organizations such as METI (Ministry of Economy, Trade, and Industry), FISC (The Center for Financial Industry Information System) has a guideline for the security measure. From this consideration, users need to confirm that each service provider implements adequate professional security measure and data management structure, and it needs a periodical review to assure the process.

Caveat 3: Responsibility of Outsourcers

Thirdly, when outsourcing vendors have information leakage, each outsourcer also need to be accountable for data management and appropriate security management. For example, in Benesse example in 2014, it was an internal fraud in an outsourcing vendor, but Benesse needed to have accountability as an outsourcer for this incident. As another example, Investor Networks managed a cloud service for investor relations, and various Japanese famous companies, such as Rohto Pharmaceutical, Sanrio, and Transcosmos, used this service. However, in 2015 April, this service had information breach [240], and every business entity needed to have apology and compensation for customers as outsourcers.

From these reasons, technically outsourcing works as risk transfer methods, but each outsourcer needs to be responsible and accountable for their decision-making and security review process. In addition to this, since some insurance companies [241] have covered outsourcing, and utilizing both solutions may be one of best practice activities.

5.5 Theoritical Assumption of Insurance Design

Insurance companies consider two following assumptions in providing services.

Assuption 1 : Implementing Appropriate Security Controls

The first assumption is each company needs to have the implementation of appropriate security control to keep insurance system. For example, as we mentioned before, in the purchase of life insurance and medical insurance, some occupations, such as an alpinist, are rejected or required to have limitation to buy them because they are categorized in a risky group. As the characteristics of cyber risk insurance, insurance companies need to pay the compensation based on the coverage contract. If more companies rather than expected got breaches, these companies required to pay the compensation and the insurance would be bankrupted. Also, in the economic perspective, we need to avoid "moral hazard" problem. It is typical insurance problem that each policyholder tend to neglect risk avoidance and care duty since they consider the insurance covers these problems.

As the countermeasure, the implementation of appropriate security control is necessary. In other words, the companies that have less than certain risks can purchase the cyber risk insurance. Actually, according to this news article [242], although an energy company in U.K. would like to purchase cyber risk insurance, they were rejected because of weak security management. This example shows that insurance companies may decline the purchase after the comprehensive analysis of current security control and management. Also, to support continuous security countermeasure, one Tokio Marine and Nichido Fire Insurance started the service of promoting security countermeasures named "Cyber Risk Comprehensive Support Service" from October 2015 [243] and "cybersecurity Countermeasure Support Loan" in June 2016 [244].

Assuption 2 : Known Vulnerabilities are usually exploited

The second assumption is that majority of attacks is abusing known vulnerabilities, and the majority of attacks are avoidable as long as they have appropriate security control implementation and operation. According to "Verizon Data Breach Investigation Report 2015" [245], 99.9% of abused vulnerabilities are old vulnerabilities that are released more than one year before.

The reason why attackers use known vulnerability can be explained from economic perspectives. Generally speaking, since discovering and abusing new vulnerabilities (called 0-day vulnerabilities) need a lot of costs, usual attackers purchase the packaged tools called "Exploit Kit", that include a lot of known vulnerabilities discovered by researchers and attackers. However, exploit packs including latest vulnerabilities is very expensive, but the price of old exploit kits tend to be decreased over time because each organization has countermeasures. Therefore, we assume the attackers using these past exploits kits is increasing. According to TrendMicro report [246], the price of famous "Phoenix Exploit Kit" was $600 in 2011, but it decreased $250 in 2012, and it was free in 2013.

From this logical assumption, insurance companies design the insurance policy with the assumption of attacking with known vulnerabilities.

5.6 Qualitative Analysis

From a qualitative perspective, joining cyber risk insurance can promote security control. As we mentioned, each insurance company require appropriate countermeasures as the prerequisites and continuous improvement of security control. Some foreign insurance companies provide necessary consulting service of security countermeasures. Also, some insurance companies give an incentive to have security control by offering more coverage or decrease of premium. From these cases, we think cyber risk insurance can promote the security control. One research paper [247] analyzed the characteristics of companies having cyber risk insurance by

using questionnaire methods. This survey revealed that the four organizational characteristics, including "Conducting Risk analysis", "Implementing advanced security countermeasure', "the magnitude of impact by human risk", and "The number of Employes", were influential to join cyber risk insurance. Therefore, we consider the promotion of security control and cyber risk insurance has correlation and efficient.

On top of that, initial investigation in making insurance policy have risk analysis of the companies, and it makes cyber risks visible. By this visualization of risk, we can see expected the cost of the security breach, and we can consider the preparation of security incident.

5.7 Quantitative Analysis

5.7.1 Simulation Overview

Since compromised companies do not disclose the details of security investments and damage amount as we mentioned in 5.2.2, we assume a virtual company, and we try the simulation to validate the benefit of a company that considers to purchase cyber risk insurance. For this simulation, we use the security incident case of an e-commerce company "SoundHouse" in 2008 as a model of the virtual company.

In this simulation, since all expected damage is dependent on the number of breached records, we consider using Monte Carlo simulation. Monte Carlo simulation is a statistical simulation to analyze the situation, and we primarily use this case to calculate the number of breached records. In this simulation, we conducted 1 million trial in each scenario, because the increase of trials increases the accuracy of analysis based on statistical theory. By considering 1 million cases based on the pre-defined statistics, we can find the expected damage amount.

SoundHouse : Overview

"SoundHouse" is e-commerce company to sell audio equipment and instrument. This company was also famous because they got the cyber attack, and leaked approximately 97,500 records of clients by SQL injection in 2008 (The possible leaked data will be 122,884 records). Unfortunately, they leaked not only customers data including name, date of birth, e-mail address, password, but also records payment card information, and 27,743 records contain the PAN (Primary Account Number) and expiration code. One of the remarkable activity by this company had they disclosed the details of costs and the timeline of security incidents [248, 249]. In this experiment, we utilized this information for the simulation.

SoundHouse : Reported Cost

According to above reports, the damage cost was 62.8 million JPY.

Table 5.1: Disclosed Damage Cost

No.	Detailed Items	Cost
#1	Incident Response Cost	4.0 million JPY
#2	Security Countermaesure Cost	24.8 million JPY
#3	Server Replacement Cost	34.0 million JPY

SoundHouse : Inquiry Response Cost

One of the considerable cost that was not available in this report was Inquiry Response Cost. SoundHouse had approximately 4,000 inquiries by clients about security incidents, and they needed to intensify call center and inquiry response manual.

SoundHouse : Compensation Cost

They provided voucher points deserved to 1,000 JPY to 122,884 clients. It was totally dependent on the behaviors of customers, but it might be the massive damage from the business perspective.

SoundHouse : Opportunity Loss

In information leakage, they stopped the site in approximately 13 hours. Also, since they had payment card breach, the transaction of the credit cards was stopped, and it was restarted on September 2015. Since 30% of their revenue is credit cards, it might be an opportunity lost and lost of customer loyalty.

5.7.2 Model Building

We consider that the virtual company stored the data called "client data" that is valuable. This company runs the e-commerce site, and this site has only SQL injection as a vulnerability. In addition to this, the company does not know whether or not SQL injection is on this website, and the existence of SQL injection is determined based on the statistical distribution. If SQL Injection is on this site, the number of breached data is determined by "data leakage logic", and we estimate the damage. On the contrary, if SQL injection is not, there is no information breach.

Initial Parameter : Model Company

The revenue of Model company is following, based on "SoundHouse".

Table 5.2: Initial Parameter : Model Company

Items	Abboriviation	Value
Revenue	R_{ev}	7 Billion JPY
Profit Ratio	P_{ro}	15%
Customer Records	R_{max}	300,000

Initial Parameter : Information Breach Condition (Vulnerability)

We assume the initial parameters related to information leakage as follows.

As we mentioned, this model company do not know the existence of SQL Injection vulnerability in this websites. Therefore, the existence is defined as Table 5.3. This above data is defined as the average of 5 years by the report "Cyber

Table 5.3: Initial Parameter : The existence probability of the vulnerability

Items	Abboriviation	Value
The Existence Probability (w/o Investment)	P_0	16.40%
The Existence Probability (w/ Investment)	P_1	5.00%

Security Trend Annual Review 2014" [250] published by NRI SecureTechnologies. Also, if the virtual company invests the security countermeasure we describe later, the existing probability will be decreasing.

Initial Parameter : Information Breach Condition (Breach)

The number of leaked data will be determined with the Triangle Probability Distribution, and we use this data published by Ponemon Institute [251].

Table 5.4: Initial Parameter : Data Breach Decision Algorithm

Items	Abboriviation	Value
The Number of Breached Data	N_i	Decided by Triangle Distribution
Minimum Value	N_{min}	2415
Maximum Value	N_{max}	300,000 ($=R_{max}$)
Average Value	N_{ave}	29,087

Initial Parameter : Security Investment

To consider the countermeasures of information leakage, we assume two security investment (Investment Cost: C_{inv}) in the model. As we mentioned previously, the impact of security investments is classified into two: "the effect of decreasing the success ratio of attack" and "the effect to minimize the damage when attacks are succeeded".

Investment 1 is security assessment. A security assessment is discovering the vulnerabilities with using the simulative attack to the web application by security service provider or security scanner. This security investment is "the effect of decreasing the success ratio of attack", but it may miss the vulnerability because of service quality and assessment scope. The investment cost is 4.2 million JPY,

and it decreases the existing vulnerability of SQL injection into 5.0%. We assume security assessment cost by the examples of "Sound House." Also, since overall detection ratio of web application scanner is 95% [252], we considered the existing vulnerability is 5.0%.

Table 5.5: Security Investment 1 : Security Assessment

Items	Abboriviation	Value
Costs	C_1	4.2 million JPY
Effects		The existence vulnerability is decreased into 5.00%

Investment 2 is cyber risk insurance. Cyber risk insurance can assure the damage in security incidents instead of paying a certain amount of premium, and it has "the effect to minimize the damage" when attacks are succeeding. Majority insurance company in Japan said the cyber risk insurance is a made-to-order product. We use an example of "Information Leakage Insurance" provided by Tokio Marine & Nichido based on the size of the virtual company.

Table 5.6: Security Investment 2 : Cyber Risk Insurance

Items	Abboriviation	Value
Costs	C_2	0.5 million JPY
Effects		This cyber risk insurance covers followings.
		100 million JPY (Clients Compensation)
		30 million JPY (IR Cost Recovery)

Initial Parameter : Information Leakage Cost (Total)

The total cost (C_{total}), in information leakage accident happened, it is consist of four costs.

$$C_{total} = C_{inv} + C_{ir-total} + C_{cp-total} + C_{qa-total} \tag{5.1}$$

In this model, costs by information breach have two categories including "Incident Response Cost" and "Customer Liability".

Table 5.7: Breach Cost : Total Costs

Items	Abboriviation
Security Investment Cost	C_{inv}
Incident Response Cost	$C_{ir-total}$
Customer Liability (Compensation)	$C_{cp-total}$
Customer Liability (Q&A)	$C_{qa-total}$

Initial Parameter : Information Leakage Cost (Incident Response Cost)

"Incident Response Cost" includes computer forensics cost, recovery cost, security countermeasures cost. In this model, we use the value from "Sound House" as a fixed value.

Table 5.8: Breach Cost : Incident Response Cost

Items	Value (JPY)
Incident Reponse Cost	4,000,000
Host-Based IDS	1,100,000
Firewall Monitering	4,200,000
IPS Monitering	15,000,000
Security Assessment	4,200,000
Server Room Chanage	300,000
Server Replacement	34,000,000
Total($C_{ir-total}$)	62,800,000

Initial Parameter : Information Leakage Cost (Customer Liability)

"Customer Liability" means necessary costs for clients including compensation cost, paperwork cost, and Q&A costs. This model has two area that is "Customer Liability (Compensation)" and "Customer Liability (Q&A)".

In this example, we assume 500 JPY for each person based on past cases. Also, we add paperwork costs (including apology letter and postage), and the total cost is 750 JPY.

Also, we assume the Q&A cost is proportional to leaked data the number of victims N. In the case of "SoundHouse", the 5.0% of victims have Q&A, and

Table 5.9: Initial Parameter : Customer Liability (Compensation)

Items	Abboriviation	Value
Total	$C_{cp-total}$	$N_i * C_{cp}$
Leaked Data	N_i	Previously Defined
Unit Cost	C_{person}	750 JPY/person

we utilize the information. Also, we consider that the average cost for Q&A is 1,000 Yen with following logics since the average hourly wage is 1,000 JPY and we assume each inquiry needs averagely one hour.

Table 5.10: Initial Parameter : Customer Liability (Q&A)

Items	Abboriviation	Value
Total	$C_{qa-total}$	$N_i * P_{qa} * C_{qa}$
Leaked Data	N_i	Previously Defined
Inquiry Ratio	P_{qa}	5.0%
Unit QA Cost	C_{qa}	1,000 JPY/person

5.7.3 Simulation

By using above assumption, Figure 5.1 shows the simulation algorithm. Firstly, by following Table 5.3, this algorithm decides the existence of SQL Injection. If SQL injection exists, with the assumption of attack, the amount of data leakage is determined by Table 5.4. As a final step, we decide the total damage based on Table 5.7 - Table 5.10 However, we consider insurance covers the damage in the case of implementing Security Investment 2 (Cyber Risk Insurance). We perform this simulation model by using Python and R language.

We analyze four scenarios since total damage cost is entirely dependent on security investment as Table 5.11 shows.

5.8 Results and Analysis

We conduct simulation with 1 million times, and the results are as follows.

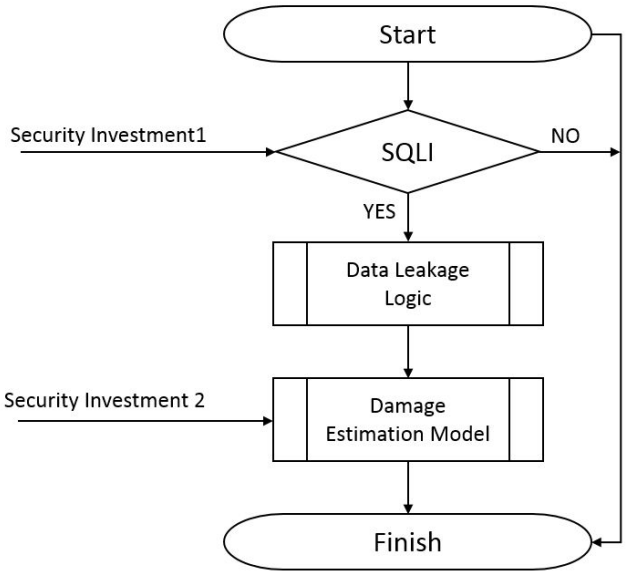

Figure 5.1: Simulation Algorithm

Table 5.11: Simulation Scenarios

		Investment 2	
		NO	YES
Investment 1	NO	CASE 1	CASE 3
	YES	CASE 2	CASE 4

Cost(maximum) and cost(minimum) shows the maximum and minimum value in 1 million attempts in each scenario, and usually, cost(minimum) means the total cost of security investment without vulnerability. Also, cost(average) and cost(median) is the average and median of 1 million attempts. As noted, cost(maximum) is similar between CASE 1 and CASE 2, or CASE 3 and CASE 4, because Security Investment 1 (Security Assessment) can decrease the possibility of attack, but it is not influential when it succeeds.

As a real situation, we assume the company that purchases cyber risk insurance also has security countermeasure. Therefore, three cases, CASE 1 (No Security Investment), CASE 2 (Having security assessment), and CASE 4 (Having both countermeasures), are critical and CASE 3 is omitted in a later discussion because it is an unrealistic case.

Table 5.12: Experiment Results (Unit : cases, 1 million JPY)

	CASE1	CASE 2	CASE 3	CASE 4
SQLI Existence Ratio	16.40%	5.00%	16.40%	5.00%
Cyber Risk Insurance	No	No	Yes	Yes
Attack Success Number	163,909	50,282	165,068	50,157
Cost (Minimum)	0.000	4.200	0.500	4.700
Cost (Maximum)	302.244	305.796	172.643	176.822
Cost (Average)	24.831	11.808	8.856	7.232
Cost (Median)	0.000	4.200	0.500	4.700
Average Relative Cost	1	0.476	0.357	0.291
ROSI	-	3.101	31.950	3.744

In the following section, we point out several useful indexes from this simulation, but all index is for the decision-making of companies that consider to join cyber risk insurance.

5.8.1 Investment Constraint

The average cost (24.83 million JPY) in CASE 1 (No Security Investment) can be expected damage value of this model by definition, and we can consider it is the investment constraint. In the situation this model finds, the security investment of less than 25 million JPY is appropriate, and the more investments can be an excessive investment.

5.8.2 Average Relative Cost

Average Relative Cost means the relative value when the average cost in CASE 1 (No Security Investment) is 1. According to this matrix, the CASE 2 having only security investment can decrease the 52.4% of costs, and CASE 4 having both two security investment strategy can contribute to decreasing 70.9% of total expenses.

5.8.3 ROSI : Return On Security Investment

ROSI (Return On Security Investment) is the ratio describing the contribution of security investment to decrease of average cost. Based on this indexes, CASE 4

can be four times effective investment strategy when we assume that each company usually buy cyber risk insurance after gaining security assessment service. It is entirely dependent on the details of security investment and cyber risk insurance condition, but cyber risk insurance is very high efficient cybersecurity control from ROSI perspective.

5.8.4 Effectiveness Evaluation of Cyber Risk Insurance

The effectiveness evaluation of cyber risk insurance is possible in the case of with-and-without comparison test after filtering attack success case. Table 5.13 shows the results of filtering attack success case.

Table 5.13: Experiment Results (Unit : cases, 1 million JPY)

	CASE1	CASE 2	CASE 3	CASE 4
SQLI Existence Ratio	16.40%	5.00%	16.40%	5.00%
Cyber Risk Insurance	No	No	Yes	Yes
Attack Success Number	163,909	50,282	165,068	50,157
Cost (Minimum)	64.771	69.202	33.300	37.500
Cost (Maximum)	302.244	305.796	172.643	176.822
Cost (Average)	151.492	155.512	51.121	55.182
Cost (Median)	142.388	146.409	33.300	37.500

Insurance Coverage Ratio is defined as the ratio of insurance coverage for an original total damage cost. In this case, the difference between CASE 2 (With Security Assessment, No Cyber Risk Insurance) and CASE 4 (With Security Assessment and Cyber Risk Insurance) is “insurance average cost”. Also, CASE 2 is considered as the actual damage cost without cyber risk insurance. Therefore, we defined the following equation as the definition of Insurance Coverage Ratio and ROSI.

$$Insurance\_Coverage\_Ratio = \frac{CASE2 - CASE4}{CASE2} \tag{5.2}$$

$$Insurance\_ROSI = \frac{CASE2 - CASE4}{C_2} \tag{5.3}$$

When we consider the insurance as 1-year insurance, Insurance Coverage Ratio is approximately 65%, and Insurance ROSI is 200 times when we consider the attack succeeds. It is entirely dependent on the parameters, but it is an adequate security investment.

Table 5.14: Insurance Coverage Ratio & Insurance ROSI

Items	Abboriviation	Value
Insurance Coverage Ratio	$(CASE2 - CASE4)/CASE2$	64.50
Insurance ROSI	$(CASE2 - CASE4)/C_2$	200.659

5.8.5 The Comparison with Actual Example

In order to verify the result of cyber risk insurance effectiveness by this simulation, we examine the U.S. cases in Chapter 2.

As we mentioned previously, Target paid 292 million USD, but insurance covered 90 million USD, and the insurance coverage is 30.82% of total countermeasure cost. Also, in the case of Home Depot, they paid 298 million USD, but insurance covered 100 million USD, and the insurance coverage is 34.56% of total countermeasure cost. From these results, approximately 30% to 35% is the coverage of insurance in significant security incidents. In addition to this, as we calculated, ROSI of Target cyber risk insurance in one year is approximately between 224 and 449. ROSI of this simulation, 200.659, is not an unrealistic indicator as simulation results.

In another case, Sony pictures got hacking in November 2014, and much personally identifiable information including unreleased movies, employees, and famous actress information were stolen. The assumed damage cost was more than 100 million dollars [253], but insurance covers all damage [254].

5.8.6 Analysis from Insurance Company Sides

All analysis above is from insured sides (the company that considers purchasing cyber risk insurance). However, as a final analysis, we reconsider this result from insurance company perspective. In this model, the premium is 0.5 million JPY, and the average payout of Case 4 (technically expected payout) should be less than 0.5 million JPY because insurance company needs to design that premium should cover all necessary payout without the deficit. In another word, the premium should be higher than the expected payout to avoid the debt and to include operational cost and profit. We calculate an average payout in Case 4, and it shows 5.046 million JPY and this value include that incident does not happen. From this results, it is ten times higher than the premium setting, and the insurance company in this model is unrealistic cases although this model is the actual model case from a real insurance company. In another word, the insurance company in this model should be set the premium more than 5 million USD to cover the necessary cost. As post-analysis, we can assume various reasons to explain this situation as follows; "the premium set by an insurance company is not appropriate since it is hard to estimate cyber risk", "since majority of simulation results is no security incidents; the average price is volatile based on the simulation results", or "model needs the improvement from algorithm perspective". However, we think we require further consideration and improvement is necessary.

5.9 Conclusion

In this paper, we had the various analysis of cyber risk insurance and cost-benefit of them, and we showed the effectiveness of cyber risk insurance. As future works, we consider following three issues.

Firstly, we believe building a more sophisticated model for a complicated situation to discuss the real-world. For example, this model only considers the one-year model with the full payout, but we need to consider the case of the long-term model

as same as other insurance. In addition to this, we also need to consider limitation and rejection of payout claims based on attack vectors, coverage, and pre-requisite conditions. By using this perspective, we would like to improve this simulative analysis. On top of that, we would like to include human factor and timeline elements in this model, although this model only considers technical elements. In actual security incidents, technology is one area, but the process, operation, violation of internal rules, and decision-making by managers based on the timeline is significant factors to evaluate total security incidents. In future works, we would like to add this improvement in my simulation model.

Secondly, we expand this analysis to large companies, or different characteristics companies. We think the corporate characteristics or size of businesses make the results different and we would like to apply this technique to these various cases.

Thirdly, we would like to analyze the behavior and incentive to purchase the cyber risk insurance. Also, in order to clarify the damage cost, the improvement of cost estimation is also necessary.

By these efforts, we would like to provide a tool to estimate the cost quickly.

Chapter 6

Conclusions

6.1 Concluding Remarks

Firstly, this thesis focused on the the compensation of personally identifiable information, and we have three major contributions in this area. Firstly, we analyzed various Japanese personally identifiable information leakage, and proved the gap between theoritical value and actual compensation. Secondly, we performed case study analysis about lawsuit case in Japan and U.S. and we think Japanese compensation value is averagely higher than U.S., and we find that it is caused by the difference of compensation style. Thirdly, we analyze how to handle personally identifiable information in the current situation, and we point out three data characteristics, named “searchability”, “cancellability”, and “retrievability”, that model should include.

Secondly, we propose new corporate valuation method by using sentiment data of Tweets related to targeted organizations instead of stock price in security incidents. We suggested the value named Tweet Reputation Index (TRI), and then, we conduct event study methodology to this value to calculate Cumulative Abnormal Return (TRI-CAR). We could estimate the event impact on corporate value. In case study, we show the effectiveness of our proposed method, including visualization of security breach impact on non-public information.

Thirdly, we evaluate the effectiveness of cyber risk insurance from qualitative and quantitative perspective. Firstly, we conducted an overview of the insurance

mechanism, current state, and the challenges of cyber risk insurance. After this, we conducted qualitative and quantitative cost-benefit analysis. However, since detailed data of security incidents was not available, the results of the quantitative analysis were dependent on the initial parameter. To consider the various possibilities, we used Monte-Carlo simulation for this effectiveness analysis, and we concluded that the cyber risk insurance is the effective solution for security management and risk management perspective.

6.2 Future Issues

We have some future issues for further improvement of security investment evaluation methodology, and we propose an overview of future work direction.

Advanced Quantitative Analysis of PII Compensation

We will have the quantitative analysis of the linkage between compensation and other factors such as payment, the speed of information disclosure, calculation concept, stock price, and Twitter response. In addition to this, we would like to contribute a sophistication of JO model since there are various changes in external environments.

Empirical Event Study Analysis with Twitter Sentiment Data

Primary works for next steps is an empirical study of security incidents or another event by using proposed methodology. The existing research about event study is analyzing trends by collecting many cases and categorizing cases based on characteristics including attack vectors, the number of leaked records, industries, and countermeasures. In order to analyze the trends with our proposed framework, we would like to continue to collect Twitter data. Especially, we would like to focus on unique analysis such as a difference between public companies and non-public companies, because only our proposal can analyze these issues.

Insurance Evaluation Modeling

As future works, we would like to create a more sophisticated model for various scenarios and long-term analysis. Especially, the model in this paper have all payout, but many cases in reality have limited payout or the rejection of payment claims based on the attack vectors. In addition to this, we have to consider the long-term benefit of having insurance because security incidents hopefully decrease with the implementation of appropriate security measures.

Appendix A

Experimental Data of Proposed Event Study Methodology

A.1 Introduction

In Chapter 4, we introduced the new method (Event Study Methodology with Twitter Sentiment Analysis), but we show several experimental examples in Appendix A for further discussion since these experimental data need to be interpreted from "intangible cost" perspective.

A.2 Public Sectors Example

In this section, we show the experimental analysis results of a local governmental agency as an another example of "Applicability". However, we think it is difficult to explain and interpret the "corporate value" of the governmental agency, and we concluded that additional research would be necessary as future works. We picked up the case of unauthorized access to SEI-NET (Saga Education Information-Network) managed by Saga Prefecture. This case was very famous because 17 years boy compromised this system in June 2016, and 210,000 files were leaked [182].

Based on Table A.1 condition, we have same analysis for this case and Figure A.1 shows TRI-CAR result.

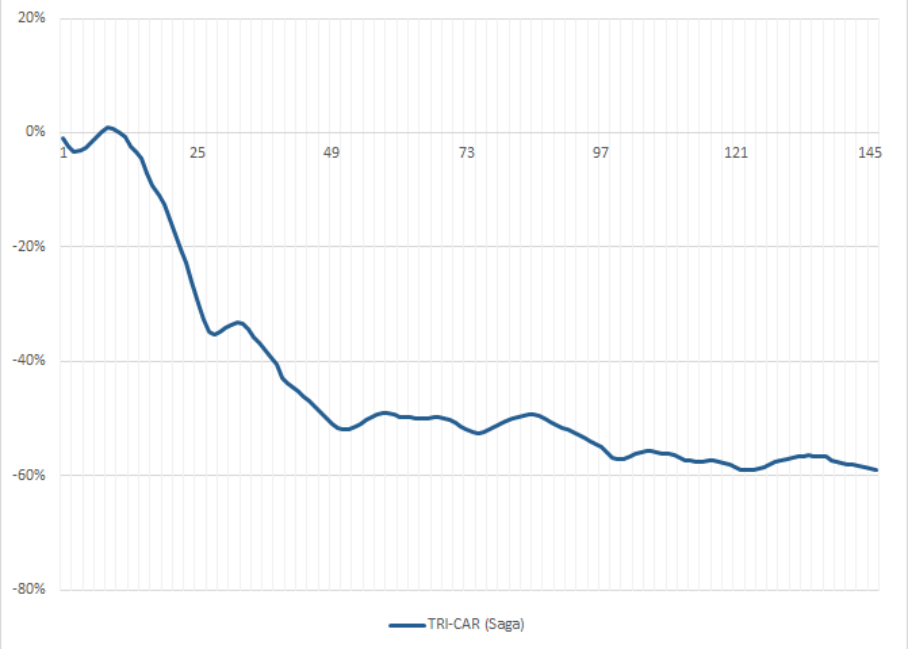

Figure A.1: Example : TRI-CAR of Saga Prefecture

A.3 Side Effect Elimination

We think the proposed method can also eliminate the impact of a specific event happening at the same time. Although the following example is not cybersecurity incidents, we demonstrate this benefit with system trouble events.

In 2016 April, Japan Airline (hereinafter JAL) had system trouble caused by system bug. In this system problem, it caused the service suspension of 2 hours, and it affected 7,000 people [178]. Figure A.2 shows the results of TRI-AR (Blue) and TRI-CAR (Red). However, this figure also revealed that TRI-CAR was increasing around April 6th ($t = 120$), and we can see another event injection happened in that time.

- Official system trouble report are published by JAL [179]
- By the disclosure of Panama Paper, some Internet media mentioned that JAL was on the list [180]

In order to eliminate the impact of Panama paper, we exclude some Tweet with the specific term (such as “Panama’, “Tax”) by keyword search, and we conduct

Table A.1: Experiment Condition

No.	Condition Item	Experiment Parameter
#1	Search Keyword	“佐賀” (Saga)
#2	Tweet Gathering Window	2016/06/23 22:44 ∼ 2016/07/07 18:46
#3	Gathered Tweet	170,750 tweets
#4	Event Time ($t = 0$)	2016/06/26 23:00
#5	Estimation Window ($t = -65 \sim -5$)	2016/06/24 06:00 ∼ 2016/06/26 18:00
#6	Event Window ($t = -1 \sim 240$)	2016/06/26 22:00 ∼ 2016/07/06 23:00
#7	Tweet Amount (Estimation Window)	24,113 tweets
#8	Tweet Amount (Event Window)	137,998 tweets

Event Study Analysis again. The results are Green graph in Figure A.2. According to this results, around $t = 120$, we can figure out the difference between original JAL TRI-CAR (Red) and JAL TRI-CAR excluding the influence of “Panama papers” (Green), and we can find out 10% difference in final. This difference is the impact by “Panama papers” influence.

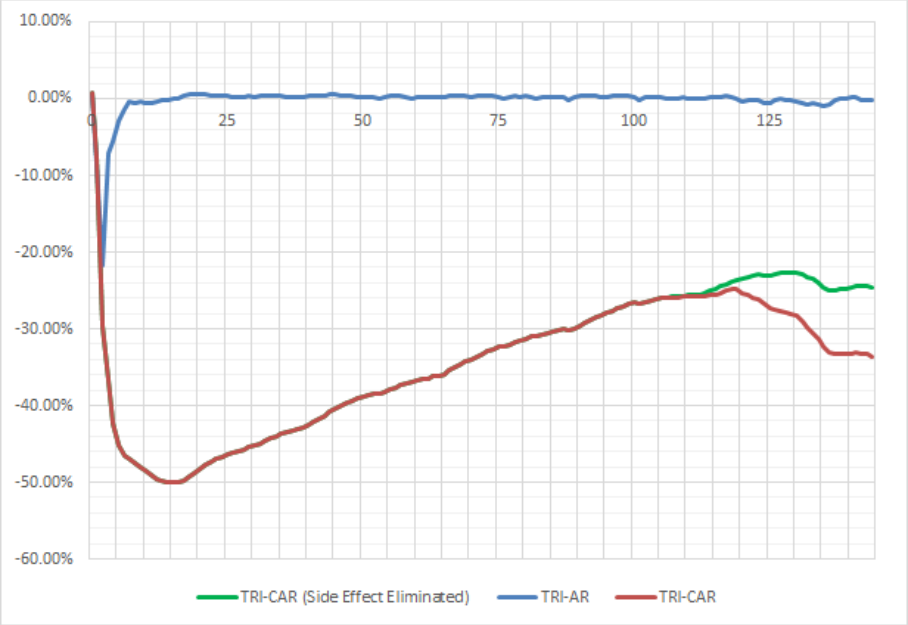

Figure A.2: Example : Side Effect Elimination

A.4 Standardized Cumulative Abnormal Return

Major analysis approach of traditional event study methodology is group comparison by considering SCAR (Standardized Cumulative Abnormal Return). Notably, many researchers related to traditional event study methodology collected many cases, categorized them based on industries, attack vectors, or existence of security controls, and then, they calculated SCAR and analyzed the linkage between corporate value impact and group categories.

SCAR was defined as follows.

$$\overline{Tweet - SCAR} = \frac{1}{N}\sum_{i=1}^{N} TRI - CAR_i \tag{A.1}$$

In our experiment, we collected 16 cases as we showed in Table A.2, and we would like to calculate SCAR value based on the condition.

Table A.2: Experiment Target

No.	Date	Organiation Name	Public	Private	Apache Struts 2
1	2016.04	Nippon TV	X	-	-
2	2016.06	JTB	-	X	-
3	2016.06	Saga	-	X	-
4	2016.06	Piped Bits (SPIRAL)	X	-	-
5	2016.06	Kodansha (Vivi)	-	X	-
6	2016.08	Nokisaki Parking	-	X	-
7	2016.10	Flat 35	-	X	-
8	2016.11	ZooNet	-	X	-
9	2017.11	Kagoya	-	X	-
10	2017.03	GMO Payment Gateway	X	-	X
11	2017.03	Metropolitan Tax	-	X	X
12	2017.03	JHFA	-	X	X
13	2017.03	JINS	X	-	X
14	2017.03	JETRO	-	X	X
15	2017.03	Yamasa	-	X	-
16	2017.04	Tosho Mart	-	X	-

In Figure A.3, it shows that average CAR (SCAR) with four categories. The

categories are as follows, and we can say that the average CAR (SCAR) can be more than 200% after 24 hours of the announcement, and SCAR gradually decreased after 24 hours.

- Case 1 : All Cases (N=16)
- Case 2 : Public Companies (N=4)
- Case 3 : Private Companies & Governmental Agencies (N=12)
- Case 4 : Apache Struts2 Victimized Group (N=5)

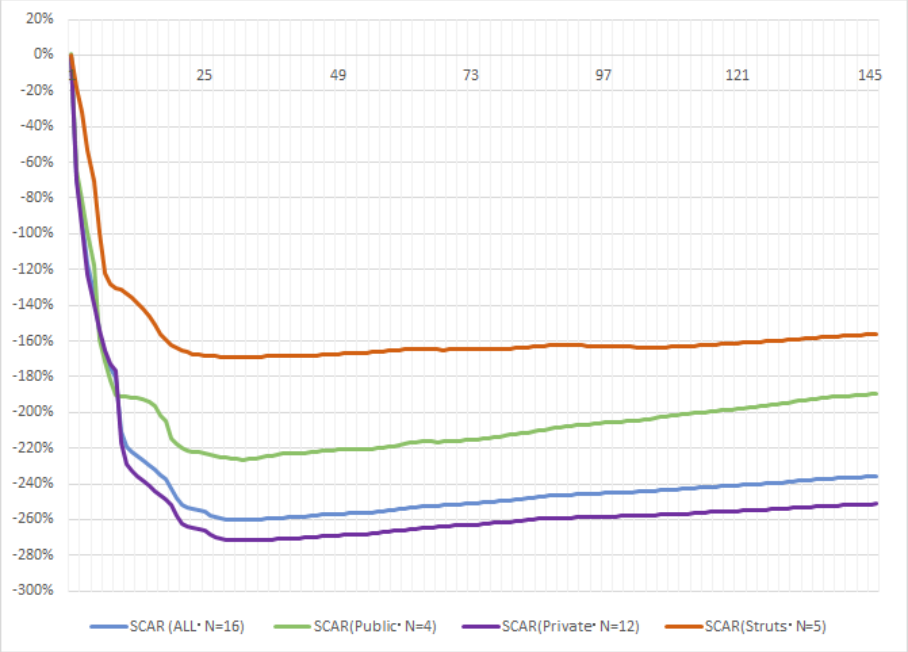

Figure A.3: Standardized Cumulative Abnormal Return

Publications

Referred Journal Papers

- Tomohisa Ishiakwa, Kouichi Sakurai, "An Effectiveness Evaluation of Cyber Risk Insurance as a Security Control Method", *IPSJ Journal*, Vol. 57, No.9, pp.2088–2098, Information Processing Society of Japan, September 2016.

Refereed International Conference Papers

- Tomohisa Ishiakwa, Kouichi Sakurai, "A Study of Compensation in personally identifiable information Leakage", In *Proceedings of 6th International Workshop on Managing Insider Security Threats (MIST 2014)*, Seoul, Republic of Korea, Vol. 1, No.7, pp.1–10, Research Briefs on Information and Communication Technology Evolution (ReBICTE), November 2014.

- Tomohisa Ishiakwa, Kouichi Sakurai, "A Study of Security Management with Cyber Insurance", In *Proceedings of the 10th International Conference on Ubiquitous Information Management and Communication (IMCOM 2016)*, Danang, Viet Nam, pp.68:1–68:6, ACM, January 2016.

- Linghuan Xiao, Shinichi Matsumoto, Tomohisa Ishikawa, Kouichi Sakurai, "SQL Injection Attack Detection Method Using Expectation Criterion", In *Proceedings of 3rd International Workshop on Information and Communication Security (WICS 2016)*, Hiroshima, Japan, IEEE, November 2016.

- Tomohisa Ishikawa, Kouichi Sakurai, "Parameter Manipulation Attack Prevention and Detection by Using Web Application Deception Proxy", In

Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication (IMCOM 2017), Beppu, Japan, pp.74:1–74:9, ACM, January 2017.

- Tomohisa Ishikawa, Kouichi Sakurai, "A Proposal of Event Study Methodology with Twitter Sentimental Analysis for Risk Management", In *Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication (IMCOM 2017)*, Beppu, Japan, pp.14:1–14:7, ACM, January 2017.

Unrefereed Domestic Conference Papers

- Tomohisa Ishiakwa, Kouichi Sakurai, "A Study of Compensation in Personal Information Leakage", In *Proceedings of Computer Security Symposium 2014 (CSS2014)*, Sapporo, Japan, Vol.2014, No.2, pp.1185–1191, Information Processing Society of Japan, October 2014.

- Tomohisa Ishiakwa, Kouichi Sakurai, "A Study of Security Management with Cyber Risk Insurance", In *Proceedings of Computer Security Symposium 2015 (CSS2015)*, Nagasaki, Japan, Vol.2015, No.3, pp.348–355, Information Processing Society of Japan, October 2015.

- Shiqian Yu, Tomohisa Ishikawa, Yaokai Feng, Danilo Vasconcellos Vargas, Kouichi Sakurai, "Privacy Leakage of Job-related Information Seeking in Online Social Networks", In *Proceedings of Hinokuni Information Symposium 2017*, Kagoshima, Japan, pp.1–6, Information Processing Society of Japan, March 2017.

References

[1] CNN Money. “Massive hack blows crater in Sony brand”. http://money.cnn.com/2011/05/10/technology/sony_hack_fallout/. Published May 10, 2011. Accessd June 2017.

[2] USA Today. “Massive breach at health care company Anthem Inc”. https://www.usatoday.com/story/tech/2015/02/04/health-care-anthem-hacked/22900925/. Published Feburary 4, 2015. Accessd June 2017.

[3] USA Today. “Premera says data breach affects up to 11M people”. https://www.usatoday.com/story/tech/2015/03/17/premera-says-cyber-attack-affects-customers/24917883/. Published March 17, 2015. Accessd June 2017.

[4] USA Today. “1.1 million CareFirst members in D.C.-area potentially breached”. https://www.usatoday.com/story/tech/2015/05/20/1-million-carefirst-blueshield-cyberattack-fireeye-mandiant/27587659/. Published March 20, 2015. Accessd June 2017.

[5] USA Today. “Cyber breach hits 10 million Excellus healthcare customers”. https://www.usatoday.com/story/tech/2015/09/10/cyber-breach-hackers-excellus-blue-cross-blue-shield/72018150/. Published September 10, 2015. Accessd June 2017.

[6] The Wall Street Journal. “OPM Breach Was Enormous, FBI Director Says”. https://www.wsj.com/articles/breach-was-enormous-fbi-director-says-1436395157. Published July 8, 2015. Accessd June 2017.

[7] USA Today. “Cyber hack got access to over 700,000 IRS accounts”. https://www.usatoday.com/story/money/2016/02/26/cyber-hack-gained-access-more-than-700000-irs-accounts/80992822/. Published Feburary 26, 2016. Accessd June 2017.

[8] The Japan Times. “Japan Pension Service hack used classic attack method”. http://www.japantimes.co.jp/news/2015/06/02/national/social-issues/japan-pension-service-hack-used-classic-attack-method/. Published June 2, 2015. Accessd June 2017.

[9] The Japan Times. “JTB hack underscores need for revamp of cybersecurity in Japan”. http://www.japantimes.co.jp/news/2016/06/16/national/jtb-hack-underscores-need-revamp-cybersecurity-japan/. Published June 16, 2016. Accessd June 2017.

[10] Bloomberg Technology. “Adultery Site Ashley Madison Fined Over Client Data Breach”. https://www.bloomberg.com/news/articles/2016-12-14/adultery-site-ashley-madison-sanctioned-over-client-data-breach. Published December 15, 2016. Accessd June 2017.

[11] Amit Yoran. “Escaping Securitys Dark Ages”. *RSA Conference USA 2015*. https://www.rsaconference.com/events/us15/agenda/sessions/1946/escaping-securitys-dark-ages. Published April 2015. Accessd June 2017.

[12] PCI Security Standards Council. “Payment Card Industry Data Security Standard - Requirements and Security Assessment Procedures”. https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf. Published April 2016. Accessd June 2017.

[13] New York State Department of Financial Service. “Cybersecurity Requirements for Financial Services Companies”. http://www.dfs.ny.gov/legal/

regulations/adoptions/dfsrf500txt.pdf. Published March 2017. Accessd June 2017.

[14] Monetary Authority of Singapore. "Technology Risk Management Guidelines". http://www.mas.gov.sg/regulations-and-financial-stability/regulatory-and-supervisory-framework/risk-management/technology-risk.aspx. Published June 2013. Accessd June 2017.

[15] National Policy Agency. "2014 Empirical Research Report of Security Countermeasure against Unauthorized Access" (published in Japanese). https://www.npa.go.jp/cyber/research/h26/h26countermeasures.pdf. Published January 2015. Accessd June 2017.

[16] World Economic Forum. "The Global Risks Report 2017 12th Edition". http://www3.weforum.org/docs/GRR17_Report_web.pdf. Published January 2017. Accessd June 2017.

[17] Bank Info Securtiy. "S&P's Cybersecurity Warning: Late to the Game". http://www.bankinfosecurity.com/standard-poor-issues-bank-cybersecurity-warning-a-8556. Published September 30, 2015. Accessd June 2017.

[18] Ministry of Economy, Trade and Industry. "Cybersecurity Management Guidelines". http://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guidelines_v1.1_en.pdf. Published December 2015. Accessd June 2017.

[19] National Policy Agency. "2016 Empirical Research Report of Security Countermeasure against Unauthorized Access" (published in Japanese). https://www.npa.go.jp/cyber/research/h28/h28countermeasures.pdf. Published November 2016. Accessd June 2017.

[20] PwC Global. “Managing cyber risks in an interconnected world - Key findings from The Global State of Information Security Survey 2015”. http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf. Published September 2014. Accessd June 2017.

[21] Government Digital Service of British Government. “Cyber security ‘myths’ putting a third of SME revenue at risk”. https://www.gov.uk/government/news/cyber-security-myths-putting-a-third-of-sme-revenue-at-risk. Published February 25, 2015. Accessd June 2017.

[22] National Information Security Policy Council. “The Second National Strategy on Information Security Aiming for Strong Individual and Society in IT Age”. https://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf. Published February 2009. Accessd June 2017.

[23] National Institute of Standards and Technology. “NIST Cybersecurity Framework”. https://www.nist.gov/cyberframework. Accessd June 2017.

[24] JPCERT/CC. “Internet Security History : Personal Identifiable Information Breach in Uji City”. https://www.jpcert.or.jp/tips/2007/wr071501.html. Published April 18, 2007. Accessd June 2017.

[25] Cabinet Secretariat, Japan. “Act on the Protection of Personal Information Act No. 57 of (2003)”. http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf. Published April, 2003. Accessd June 2017.

[26] Nomura Research Institute. “Proactive Information Security Strategy” (published in Japanese). *NRI IT Solution Frontier*. Vol. 2016.10, pp. 6–10. November 2016.

[27] International Organization for Standardization. “ISO/IEC 27000 family - Information security management systems”. https://www.iso.org/isoiec-27001-information-security.html. Accessd June 2017.

[28] Center for Internet Security. “CIS Critical Security Control”. https://www.cisecurity.org/controls/. Accessd June 2017.

[29] Information Security Forum. “ISF Standard of Good Practice for Information Security”. https://www.securityforum.org/tool/the-isf-standardrmation-security/. Accessd June 2017.

[30] National Institute of Standard and Technology - Computer Security Division. “NIST Special Publications (SP) 800s - Computer Security”. http://csrc.nist.gov/publications/PubsSPs.html. Accessd June 2017.

[31] Australian Government - Attorney-General’s Department. “The Protective Security Policy Framework (PSPF)”. https://www.protectivesecurity.gov.au/Pages/default.aspx. Accessd June 2017.

[32] Australian Government - Australian Signals Directorate. “Australian Government Information Security Manual”. https://www.asd.gov.au/infosec/ism/index.htm. Accessd June 2017.

[33] Australian Government - Australian Signals Directorate. “Strategies to Mitigate Cyber Security Incidents”. https://www.asd.gov.au/infosec/mitigationstrategies.htm. Accessd June 2017.

[34] Federal Financial Institutions Examination Council (FFIEC) . “FFIEC Cybersecurity Assessment Tool”. https://www.ffiec.gov/cyberassessmenttool.htm. Accessd June 2017.

[35] The Department of Energy. “Cybersecurity Capability Maturity Model (C2M2)”. https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf. Accessd June 2017.

[36] HITRUST Alliance - Health Information Trust Alliance. “Cybersecurity Framework”. https://hitrustalliance.net/hitrust-csf/. Accessd June 2017.

[37] HITRUST Alliance - Health Information Trust Alliance. “Healthcare Sector Cybersecurity Framework Implementation Guide”. https://hitrustalliance.net/documents/cybersecurity/HPHCyberImplementationGuide.pdf. Accessd June 2017.

[38] HITRUST Alliance - Health Information Trust Alliance. “Risk Management Framework”. https://hitrustalliance.net/documents/csf_rmf_related/HITRUST-RMF-Whitepaper-2015.pdf. Accessd June 2017.

[39] The Center for Financial Industry Infomation System (FISC). “FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions”. https://www.fisc.or.jp/english/. Accessd June 2017.

[40] International Organization for Standardization. “ISO 31000 - Risk management”. https://www.iso.org/iso-31000-risk-management.html. Accessd June 2017.

[41] European Union Agency for Network and Information Security (ENISA). “Introduction to Return on Security Investment”. https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment/at_download/fullReport. Published December 2012. Accessd June 2017.

[42] U.S. Department of Commerce - National Bureau of Standards. “Automatic Data Process Risk Analysis”. *Federal Information Processing Standardization*, 1975.

[43] Lawrence A. Gorden, Martin P. Loeb. “Managing Cybersecurity Resources: A Cost-Benefit Analysis”. McGraw-Hill Education, October 2005.

[44] Lawrence A. Gorden, Martin P. Loeb. "The Economics of Information Security Investment". *ACM Transactions on Information and System Security*, Vol. 5, No. 4, pp. 438 – 457, ACM, November 2002.

[45] Jan Willemson. "On the Gordon & Loeb Model for Information Security Investment". In *Proceedings of The 5th Workshop on the Economics of Information Security (WEIS 2006)*, Cambridge, England, June 2006.

[46] Jan Willemson. "Extending the Gordon & Loeb Model for Information Security Investment". In *Proceedings of The Fifth International Conference on Availability, Reliability and Security*, Krakow, Poland, February 2010.

[47] Yuliy Baryshnikov. "IT Security Investment and Gordon-Loeb's 1/e Rule". In *Proceedings of The 11th Workshop on the Economics of Information Security (WEIS 2012)*, Berlin, Germany, June 2012.

[48] Lawrence A. Gordon, Martin P. Loeb, Lei Zhou. "Investing in Cybersecurity: Insights from the Gordon-Loeb Model". *Journal of Information Security*, Vol.7, No.2, pp.49–59, March 2016.

[49] Masayuki Orimo, Susumu Tsuhara, Michiko Yamamoto, Ryoichi Sasaki. "Security System Planning Method for Information Systems". *IPSJ Journal*, Vol. 41, No. 1, pp. 177 – 187, Information Processing Society of Japan, January 2000.

[50] Yasuhiko Nagai, Tatsuya Fujiyama, Ryoichi Sasaki. "An Optimal Decision Method for Establishment of Security Objectives". *IPSJ Journal*, Vol. 41, No. 8, pp. 2264 – 2271, Information Processing Society of Japan, August 2000.

[51] Itsukazu Nakamura, Toshiyuki Hyodo, Masakazu Soga, Tadanori Mizuno, Masakatsu Nishigaki. "A Practical Approach for Security Measure Selection

Problem and Its Availability". *IPSJ Journal*, Vol. 45, No. 8, pp. 2022 – 2033, Information Processing Society of Japan, August 2004.

[52] Masakatsu Nishigaki, Yuma Usui, Takumi Yamamoto, Fumihiko Magata, Yoshimi Teshigawara, Ryoichi Sasaki. "A Case Study of a Security Measure Selection Scheme with Consideration of Potential Lawsuit". *IPSJ Journal*, Vol. 52, No. 3, pp. 1173 – 1184, Information Processing Society of Japan, March 2011.

[53] Lawrence Carin, George Cybenko, Jeff Hughes. "Quantitative Evaluation of Risk for Investment Efficient Strategies in Cybersecurity: The QuERIES Methodology". In *Proceedings of Metricon 3*, California., United States of America, July 2008.

[54] Lawrence Carin, George Cybenko, Jeff Hughes. "Cybersecurity Strategies: The QuERIES Methodology". *IRRC Institute*, August 2008.

[55] IRRC Institute, PwC's Investor Resource Institute. "What investors need to know about cybersecurity: How to evaluate investment risks". *Whitepaper by IRRC Institute*, June 2014.

[56] Shawn A. Butler. "Security attribute evaluation method: a cost-benefit approach". In *Proceedings of the 24rd International Conference on Software Engineering 2002 (ICSE 2002)*, Orlando, Florida, U.S.A, May 2002.

[57] Huseyin Cavusoglu, Birendra K. Mishra, Srinivasan Raghunathan. "A model for evaluating IT security investments". *Communications of the ACM*, Vol.47, No.7, July 2004.

[58] Marco Cremonini, Patrizia Martini. "Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA)". In *Proceedings of The 4th Workshop on the Economics of Information Security (WEIS 2005)*, Cambridge, Massachusetts, U.S.A, June 2005.

[59] Rok Bojanc, Borka Jerman-Blazic. "Quantitative Model for Economic Analyses of Information Security Investment in an Enterprise Information System". *Organizacija*, Vol.45, No.6, November 2012.

[60] Rainer Bohme. "Security Metrics and Security Investment Models". In *Proceedings of The 5th International Workshop on Security (IWSEC2010)*, Kobe, Japan, November 2010.

[61] Information Technology Promotion Agency (IPA). "The Research Report about Information Security Incident" (published in Japanese). `https://www.ipa.go.jp/security/fy13/report/incident_survey/incident_survey.pdf`. Published June 2002. Accessd June 2017.

[62] Information Technology Promotion Agency (IPA). "The report of "Damanage Estimation Model" (published in Japanese). `https://www.ipa.go.jp/security/fy14/reports/current/2002-calc-model.pdf`. Published March 2003. Accessd June 2017.

[63] Japan Network Security Association (JNSA). "The Research Report of Information Security Incident Part 1" (published in Japanese). `http://www.jnsa.org/houkoku2003/incident_survey1.pdf`. Published March 2004. Accessd June 2017.

[64] Japan Network Security Association (JNSA). "The Research Report of Information Security Incident Part 2" (published in Japanese). `http://www.jnsa.org/houkoku2003/incident_survey2.pdf`. Published March 2004. Accessd June 2017.

[65] Hyung Kang, Kwang Cheol Park, Won Hyung Park, Kwang Ho Kuk. "A Study on Model for Assessment of Economic Damages Due to Cyber Terror". *Journal of Information and Security*, Vol. 9, No. 3, pp.25-33, Korea Information Assurance Society, September 2009.

[66] Jinho Yoo, Sangho Gee, Hyein Song, Kyungho Chung, Jongin Lim. "Estimating Economic Damages from Internet Incidents". *Journal of Information Policy*, Vol. 15, No. 1, pp.3–18, March 2008.

[67] The Economist Intelligence Unit Ltd. "CyberTab". `https://cybertab.boozallen.com/`. Accessd June 2017.

[68] Jang Ho Yun, In Hyun Cho, Kyung Ho Lee. "FAIR-Based Loss Measurement Model for Enterprise Personal Information Breach". *Advances in Computer Science and Ubiquitous Computing*, pp. 825 – 833, McGraw-Hill Education, December 2015.

[69] Youngyung Shin, Sanghun Jeon, Chaeho Lim, Myungchul Kim. "Economic Damages Assessment for National Cyber Security Measures - Analysis of the March 20 Cyber Attack -". *Korean Association of National Information Science (KANIS) - National Information Research*, Vol. 6, No.1, pp.129 –173, September 2013.

[70] Imperva Incapsula. "Incapsula Survey : What DDoS Attacks Really Cost Businesses". `https://www.incapsula.com/blog/ddos-impact-cost-of-ddos-attack.html`. Published Nobember 2014. Accessd June 2017.

[71] Ponemon Institute. "2016 Ponemon Cost of Data Breach Study". `https://www-03.ibm.com/security/data-breach/`. Published May 2016. Accessd June 2017.

[72] Department for Business, Innovation and Skills, British Government. "Cost of business cyber security breaches almost double". `https://www.gov.uk/government/news/cost-of-business-cyber-security-breaches-almost-double`. Published April 2014. Accessd June 2017.

[73] Cisco Systems, Inc. "Cisco 2017 Annual Cybersecurity Report: Chief Security Officers Reveal True Cost of Breaches and the Actions Organizations are Taking". `https://newsroom.cisco.com/press-release-content?articleId=1818259`. Published January 2017. Accessd June 2017.

[74] Ponemon Institute. "Flipping The Economics of Attacks". `https://media.paloaltonetworks.com/lp/ponemon/report.html`. Published May 2016. Accessd June 2017.

[75] James R. Conrad. "Analyzing the Risks of Information Security Investments with Monte-Carlo Simulations". In *Proceedings of The 4th Workshop on the Economics of Information Security (WEIS 2005)*, Cambridge, Massachusetts, U.S.A, June 2005.

[76] Emil Burtescu. "Decision Assistance in Risk Assessment Monte Carlo Simulations". *Informatica Economica*, Vol. 16, No. 4, pp.86 – 92, 2012.

[77] Dan Lyon. "Modeling Security Investments With Monte Carlo Simulations". *SANS Institute InfoSec Reading Room*, September 2014.

[78] Lawrence A. Gordon, Martin P. Loeb, Tashfeen Sohail. "Market Value Of Voluntary Disclosures Concerning Information Security". *Journal - MIS Quarterly*, Vol. 34, No. 3, pp. 567-594, ACM, September 2010.

[79] Myung Ko, Carlos Dorantes. "The Impact of Information Security Breaches On Financial Performance of the Breached Firms: An Empirical Investigation". *Journal of Information Technology Management*, Vol. 17, No. 2, pp. 13-22, January 2006.

[80] Eugene F. Fama, Lawrence Fisher, Michael C. Jensen, Richard Roll. "The Adjustment of Stock Prices to New Information". *International Economic Review*, Vol. 10, No.1, pp. 1–21, Wiley, Feburary 1969.

[81] Stephen J. Brown, Jerold B. Warner. "Using Daily Stock Returns : The case of Event Studies". *Journal of Financial Economics*, Vol. 14, pp. 3–31, Elsevier Science Publishers, 1985.

[82] Katherine Campbell, Lawrence A. Gordon, Martin P. Loeb, Lei Zhou. "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market". *Journal of Computer Security*, Vol. 11, No.3, pp. 431 – 448, ACM, March, 2003.

[83] Anat Hovav, John D'Arcy. "The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms". *Risk Management and Insurance Review*, Vol.6, No.2, pp. 97–121, Wiley, September 2003.

[84] Michael L. Ettredge, Vernon J. Richardson. "Information Transfer among Internet Firms: The Case of Hacker Attacks". *Journal of Information Systems*, Vol.17, No.2, pp.71 – 82, American Accounting Association, September 2003.

[85] Ashish Garg, Jeffrey Curtis, Hilary Halper. "Quantifying the financial impact of IT security breaches". *Information Management & Computer Security*, Vol.11, No.2, pp.74 – 83, Emerald Insight, May 2003.

[86] Anat Hovav, John D'Arcy. "The Impact of Virus Attack Announcements on the Market Value of Firms". *Information Systems Security*, Vol.13, No.3, pp. 32–40, May 2004.

[87] Huseyin Cavusoglu, Birendra Mishra, Srinivasan Raghunathan. "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers", *International Journal of Electronic Commerce*, Vol.9, No.1, pp.70–104, ACM, October 2004.

[88] Alessandro Acquisti, Allan Friedman, Rahul Telang. "Is There a Cost to Privacy Breaches? - An Event Study", In *Proceedings of The 5th Workshop on*

the Economics of Information Security (WEIS 2006), Cambridge, England, June 2006.

[89] Takeshi Kawaji. "The Impact of Customer Privacy Breaches on Market Value". *The Journal of The Japanese Association of Management Accounting*, Vol.15, No.1, pp.35–56, The Japanese Association of Management Accounting, November 2006.

[90] Masaki Ishiguro, Hideyuki Tanaka, Kanta Matsuura, Ichiro Murase. "The Effect of Information Security Incidents on Corporate Values in the Japanese Stock Market". In *Proceedings The Workshop on the Economics of Securing the Information Infrastructure (WESII 2006)*, Arlington, U.S.A., October, 2006.

[91] Rahul Telang, Sunil Wattal. "An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price". *IEEE Transactions on Software Engineering*, Vol.33, No.8, pp.544–557, IEEE, August 2007.

[92] Karthik Kannan, Jackie Rees, Sanjay Sridhar. "Market Reactions to Information Security Breach Announcements: An Empirical Analysis". *International Journal of Electronic Commerce*, Vol.12, No.1, pp.69–91, Taylor & Francis, Fall 2007.

[93] Francis K. Andoh-Baidoo, Kweku-Muata Osei-Bryson. "Exploring the characteristics of Internet security breaches that impact the market value of breached firms". *Expert Systems with Applications: An International Journal*, Vol.32, No.3, pp.703–725, April 2007.

[94] Sanjay Goel, Hany A. Shawky. "Estimating the market impact of security breach announcements on firm values". *Information & Management*, Vol.46, No.7, pp.404–410, Elsevier Science Publishers, October 2009.

[95] Jan Muntermann, Heiko Robnagel. "On the Effectiveness of Privacy Breach Disclosure Legislation in Europe: Empirical Evidence from the US Stock Market". In *Proceedings of the 14th Nordic Conference on Secure IT Systems: Identity and Privacy in the Internet Age (NordSec 2009)*, Oslo, Norway, pp.1–14, Springer, October 2009.

[96] Narcyz Roztocki, Heinz Roland Weistroffer. "Event Studies in Information Systems Research : An Updated Review". In *Proceedings of the Fifteenth Americas Conference on Information Systems (AMCIS 2009)*, San Francisco, California, pp. 1–10, August 2009.

[97] Kevin M. Gatzlaff, Kathleen A. McCullough. "The Effect of Data Breaches on Shareholder Wealth". *Risk Management and Insurance Review*, Vol.13, No.1, pp.61–83, Wiley, March 2010.

[98] Satoru Takayabu, Takuro Sawatani, Haruki Murata. "Impact of "information security investment" on information industry firm values". *Annual Report of Society for the Economic Studies of Securities*, Vol.45, pp. 158–164, Society for the Economic Studies of Securities, July 2010.

[99] Sangmi Chai, Minkyun Kim, H. Raghav Rao. "Firms' information security investment decisions: Stock market evidence of investors' behavior". *Decision Support Systems*, Vol.50, No.4, pp.651–661, Elsevier , March 2011.

[100] Lawrence A. Gordon, Martin P. Loeb, Lei Zhou. "The impact of information security breaches: Has there been a downward shift in costs?". *Journal of Computer Security*, Vol.19, No.1, pp.33–56, IOS Press, January 2011.

[101] Indranil Bose, Ariel K. H. Lui, Eric W. T. Ngai. "The Impact of RFID Adoption on the Market Value of Firms: An Empirical Analysis". *Journal of Organizational Computing and Electronic Commerce*, Vol.21, No.4, pp.268–294, Taylor & Francis, October 2011.

[102] Arvind Malhotra, Claudia Kubowicz Malhotra. "Evaluating Customer Information Breaches as Service Failures: An Event Study Approach". *Journal of Service Research*, Vol.14, No.1, pp.44–59, February 2011.

[103] Edward A. Morse, Vasant Raval, John R. Wingender. "Market Price Effects of Data Security Breaches". *Information Security Journal: A Global Perspective*, Vol.20, No.6, pp.263–273, Taylor & Francis, January 2011.

[104] Yaniv Konchitchki, Daniel E. O'Leary. "Event study methodologies in information systems research". *International Journal of Accounting Information Systems*, Vol.12, No.2, pp.99–115, Elsevier, June 2011.

[105] Ali Alper Yayla, Qing Hu. "The impact of information security events on the stock value of firms: the effect of contingency factors". *Journal of Information Technology*, Vol.26, No.1, pp.60–77, Springer, March 2011.

[106] Takeshi Hiromatsu. "The Impact Analysis of Affecting Corporate Value by Information Security Incident" (published in Japanese). *The Bulletin of Synthetic Science of Information Security*, Vol.3, pp.91–106, November 2011.

[107] Takeshi Hiromatsu. "The Quantitive Analysis of Information Security Awareness Change by Personal Identifiable Information Protection Law" (published in Japanese). *The Bulletin of Synthetic Science of Information Security*, Vol.4, pp.150–170, November 2012.

[108] Srikanth Parameswaran, Srikanth Venkatesan, Manish Gupta. "Do Cloud Security Announcements Affect Firm Valuation?". In *Proceedings of Annual Symposium on Information Assurance and Secure Knowlege Management*, Vol.4, pp.23–28, New York U.S.A., June 2012.

[109] Saini Das, Arunabha Mukhopadhyay, Manoj Anand. "Stock Market Response to Information Security Breach: A Study Using Firm and Attack

Characteristics". *Journal of Information Privacy and Security*, Vol.8, No.4, pp.27–55, October 2012.

[110] Francis Kofi Andoh-Baidoo. "Explaining investors ' reaction to internet security breach using deterrence theory". *International Journal of Electronic Finance*, Vol.7, No.1, pp.1–14, January 2013.

[111] Linda Brock, Yair Levy. "The market value of information system (IS) security for e-banking". *Online Journal of Applied Knowledge Management*, Vol.1, No.1, pp.1–17, January 2013.

[112] Katsuyuki Tanaka. "Empirical Study on the Impact of Stock Price by Corporate Information Security Incidents". *ABS International Management Review*, Vol.2, pp.40–55, Aoyama Business School, March 2013.

[113] Indranil Bose, Alvin Chung Man Leung. "The impact of adoption of identity theft countermeasures on firm value". *Decision Support Systems*, Vol.55, No.3, pp.753–763, Elsevier, June 2013.

[114] Oxford Economics. "Cyber-Attacks: Effects on UK Companies". *A Report for Centre for the Protection of National Infrastructure*, Oxford Economics, July 2014.

[115] Kenji Yoshimi. "A study on inappropriate posts on social media by using event study analysis". *IPSJ SIG Technical Report*, Vol.2015-EIP-67, No.8, pp.1–6, Information Processing Society of Japan, Feburary 2015.

[116] Hideyuki Tanaka, Kunihiro Nakano. "The Impact of Cyber Security Incidents on Firm Value". *Journal of Information Studies, Interfaculty Initiative in Information Studies, The University of Tokyo*, No.91, pp.1–11, The University of Tokyo, November 2016.

[117] Georgios Spanos, Lefteris Angelis. "The impact of information security events to the stock market : A systematic literature review". *Computers and Security*, Vol.58, No.C, pp.216–229, Elsevier, May 2016.

[118] Sachiko Miyayuchi, Hiroshi Takahashi. "The relationship and impact against copporate value by information security incidents". *Master Thesis in Graduate School of Business Administration, Keio University*, pp.1–114, March 2016.

[119] Masami Nakamura. "Effects of the presence or absence of risk disclosure has on the evaluation of the stock market -The event study in which the information security risks occur in the target-". *Bulletin of Graduate Studies in Strategic Management, Chuo University*, No.4, pp.1–23, April 2016.

[120] CSO Online. "The 15 worst data security breaches of the 21st Century". `http://www.csoonline.com/article/2130877/data-protection/data-protection-the-15-worst-data-security-breaches-of-the-21st-century.html`. Published June 14, 2017 Accessd June 2017.

[121] Forbes. "Target Profit Falls 46% On Credit Card Breach And The Hits Could Keep On Coming". `https://www.forbes.com/sites/maggiemcgrath/2014/02/26/target-profit-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming/`. Published Feburary 26, 2014. Accessd June 2017.

[122] Yahoo Finance. `https://finance.yahoo.com/`. Accessd June 2017.

[123] Target Corporation. "2016 Annual Report". `https://corporate.target.com/annual-reports/2016`. Published March 2017. Accessd June 2017.

[124] DXC.Technology. "Cyber insurance: State of play". `https://blogs.dxc.technology/2016/04/20/cyber-insurance-state-of-play/`. Published April 20, 2016. Accessd June 2017.

[125] Data Protection Report. “Settlement of Target Data Breach Consumer Class Action Is Derailed On Appeal”. http://www.dataprotectionreport.com/2017/02/settlement-of-target-data-breach-consumer-class-action-is-derailed-on-appeal/. Published February 7, 2017. Accessd June 2017.

[126] Hashedout. “Cost of 2013 Target Data Breach Nears $300 Million”. https://www.thesslstore.com/blog/2013-target-data-breach-settled/. Published May 26, 2017. Accessd June 2017.

[127] Fortune. “Target will pay $10 million to settle lawsuit from data breach”. http://fortune.com/2015/03/19/target-10-million-settle-data-breach/. Published May 19, 2015. Accessd June 2017.

[128] KARE TV. “Judge OKs $10 million settlement in Target data breach”. http://www.kare11.com/news/judge-oks-10-million-settlement-in-target-data-breach/105555721. Published May 19, 2015. Accessd June 2017.

[129] The Home Depot. “Annual Report 2016”. http://ir.homedepot.com/financial-reports/annual-reports/. Accessd June 2017.

[130] ThreatPost. “HOME DEPOT AGREES TO $19.5 MILLION SETTLEMENT TO END 2014 BREACH NIGHTMARE”. https://threatpost.com/home-depot-agrees-to-19-5-million-settlement-to-end-2014-breach-nightmare/116884/. Published March 18, 2016. Accessd June 2017.

[131] Fortune Tech. “Home Depot to Pay Banks $25 Million in Data Breach Settlement”. http://fortune.com/2017/03/09/home-depot-data-breach-banks/. Published March 10, 2017. Accessd June 2017.

[132] Tsuhan Shinbun. “A lot of Information Leakage : Review of Security measure is necessary” (published in Japanese). http://www.tsuhanshinbun.com/archive/2017/03/post-2785.html. Published March 2, 2017. Accessd June 2017.

[133] CNET Japan. “Information breach from Nippon TV” (published in Japanese). https://japan.cnet.com/article/35081677/. Published April 22, 2016. Accessd June 2017.

[134] Security NEXT. “e-Commerce ASP service got unauthorized access” (published in Japanese). http://www.security-next.com/071290. Published June 22, 2016. Accessd June 2017.

[135] NRI SecureTechnologies, Ltd. “Cyber Security Trend Annual Review 2016”. https://www.nri-secure.co.jp/security/report/pdf/2016/cstar_2016_en.pdf. Published August 18, 2016. Accessd June 2017.

[136] State of Calfornia Department of Justice. “DATA SECURITY BREACH REPORTING”. https://oag.ca.gov/ecrime/databreach/reporting. Accessd June 2017.

[137] U.S. Government Publishing Office. “Health Insurance Portability and Accountability Act of 1996”. https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm. Accessd June 2017.

[138] U.S. Department of Health & Human Services. “HIPAA Enforcement”. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html. Accessd June 2017.

[139] Becker’s Healthcare - IT & CIO Review. “10 largest HIPAA settlement fines”. http://www.beckershospitalreview.com/healthcare-information-technology/10-largest-hipaa-settlement-fines.html. Published August 10, 2016. Accessd June 2017.

[140] CNBC. "Huge data breach at health system leads to biggest ever settlement". http://www.cnbc.com/2016/08/04/huge-data-breach-at-health-system-leads-to-biggest-ever-settlement.html. Published August 5, 2016. Accessd June 2017.

[141] U.S. Department of Health & Human Services. "WellPoint pays HHS $1.7 million for leaving information accessible over Internet". https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/wellpoint/index.html. Accessd June 2017.

[142] European Union. "General Data Protection Regulation". http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf. Published April 27, 2016. Accessd June 2017.

[143] Australian Government Office of the Australian Information Commissioner. "Privacy management framework: enabling compliance and encouraging good practice". https://www.oaic.gov.au/agencies-and-organisations/guides/privacy-management-framework. Accessd June 2017.

[144] Ministry of Economy, Trade and Industry. "Personal Identifiable Information Protection" (published in Japanese). http://www.meti.go.jp/policy/it_policy/privacy/. Accessd June 2017.

[145] PwC. "Moving forward with cybersecurity and privacy - Key findings from The Global State of Information Security Survey 2017". http://www.pwc.com/gx/en/information-security-survey/assets/gsiss-report-cybersecurity-privacy-safeguards.pdf. Published October 2016. Accessd June 2017.

[146] Nikkei. "Customer Information Leakage, 500 JPY per person is average price" (published in Japanese). http://www.nikkei.com/article/

DGXNZO74524990Q4A720C1TJC000/. Published July 20, 2014. Accessd June 2017.

[147] Nikkei. "Benesse leaked 35 million records and paid 500 JPY as compensation" (published in Japanese). http://www.nikkei.com/article/DGXLASDZ10H6I_Q4A910C1000000/. Published September 10, 2014. Accessd June 2017.

[148] NPO Japan Network Security Association - Security Incident Investigation Working Group. "2008 Information Security Incident Survey Report". http://www.jnsa.org/result/incident/data/2008incident_survey_e_v1.0.pdf. Published March 31, 2010. Accessd June 2017.

[149] Benesse Corporation. "Report and Response Regarding Leakage of Customers' Personal Information". http://pdf.irpocket.com/C9783/o1Tt/faNa/vOGs.pdf. Published September 10, 2014. Accessd June 2017.

[150] The Japan Times. "Benesse leak suspect held; firm plans compensation". http://www.japantimes.co.jp/news/2014/07/17/national/crime-legal/arrest-warrant-looms-systems-engineer-benesse-data-leak. Published July 17, 2014. Accessd June 2017.

[151] JINS Co. Ltd. "The notification of client information leakage by illegal access" (published in Japanese). http://www.jins-jp.com/illegal-access/info20130315-1600.pdf. Published March 15, 2013. Accessd June 2017.

[152] JINS Co. Ltd. "The final investigation report of illegal access". http://www.jins-jp.com/illegal-access/info.html. Published May 2013. Accessd June 2017.

[153] Takashi Sugawara, Yonosuke Harada. "A study on the compensation by company/organization when privacy and personal information are compromised : Focusing on the money compensation". *IPSJ SIG Technical Report*,

Vol.2013-EIP-60, No.8, pp.35–41, Information Processing Society of Japan, May, 2013.

[154] Cornell Law School. “Federal Rules of Civil Procedure ¿ TITLE IV. PARTIES ¿ Rule 23. Class Actions”. https://www.law.cornell.edu/rules/frcp/rule_23. Accessd June 2017.

[155] PasteBin. https://pastebin.com/. Accessd June 2017.

[156] Information-technology Promotion Agency. “FAQ : File Sharing Software”. http://www.ipa.go.jp/security/anshin/faq/faq-file.html. Accessd June 2017.

[157] Johan Bollen, Huina Mao, Xiaojun Zeng. “Twitter mood predicts the stock market”. *Journal of Computational Science*, Vol.2, No.1, pp.1–8, Elsevier, March 2011.

[158] Public Radio International. “Twitter hedge fund beats market”. https://www.pri.org/stories/2011-08-16/twitter-hedge-fund-beats-market. Published August 16, 2011. Accessd June 2017.

[159] The Guardian. “AP Twitter hack causes panic on Wall Street and sends Dow plunging”. https://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall. Published April 23, 2013. Accessd June 2017.

[160] Nikkei Asian Review. “NTT Data mines Japanese tweets to predict stock movements”. https://asia.nikkei.com/Tech-Science/Tech/NTT-Data-mines-Japanese-tweets-to-predict-stock-movements. Published March 7, 2014. Accessd June 2017.

[161] Nikkei Asian Review. “About Emprical Study Results of Natural Language Analysis for Investment Judgement”. http://www.nri.com/Home/jp/news/2017/170626_1.aspx. Published 26, 2017. Accessd June 2017.

[162] Japan Securities Dealers Association. "2015 National Survey about Security Investments" (published in Japanese). http://www.jsda.or.jp/shiryo/chousa/data/research_h27.html. Published December 2015. Accessd June 2017.

[163] Statistics Bureau. "Population Projection" (published in Japanese). http://www.stat.go.jp/data/jinsui/2016np/index.htm. Published April 2017. Accessd June 2017.

[164] Asahi Shinbun. "Twitter hits 40 million users in Japan amid financial woes". http://www.asahi.com/ajw/articles/AJ201611040063.html. Published November 4 2016. Accessd June 2017.

[165] Nara Institute of Science and Technology. "ChaSen". http://chasen-legacy.osdn.jp/. Accessd June 2017.

[166] Nara Institute of Science and Technology. "MeCab: Yet Another Part-of-Speech and Morphological Analyzer". http://taku910.github.io/mecab/. Accessd June 2017.

[167] Advanced Information Processing Division Precision and Intelligence Laboratory. "Semantic Orientations of Words". http://www.lr.pi.titech.ac.jp/~takamura/pndic_en.html. Accessd June 2017.

[168] Hiroya Takamura, Takashi Inui, Manabu Okumura. "Extracting Semantic Orientations Using Spin Model". *IPSJ Journal*, Vol. 47, No. 2, pages 627–637, Information Processing Society of Japan, Feburary 2006.

[169] Nobuhiro Kaji. "Polar Phrase Dictionary". http://www.tkl.iis.u-tokyo.ac.jp/~kaji/polardic/. Accessd June 2017.

[170] Nobuhiro Kaji, Masaru Kitsuregawa. "Building Lexicon for Sentiment Analysis from Massive HTML Documents". In *Proceedings of the 2007 Joint Conference on Empirical Methods in Natural Language Processing and Compu-*

tational Natural Language Learning (EMNLP-CoNLL 2007), Prague, Czech Republic, pp.1075–1083. June 2007.

[171] Inui-Okazaki Laboratory, Tohoku University. "Japanese Sentiment Polarity Dictionary". `http://www.cl.ecei.tohoku.ac.jp/index.php`. Accessd June 2017.

[172] Nozomi Kobayashi, Kentaro Inui, Yuji Matsumoto, Kenji Tateishi, Toshikazu Fukushima. "Collecting Evaluative Expressions for Opinion Extraction". *Journal of Natural Language Processing*, Vol.12, No.3, pp.203-222, The Association for Natural Language Processing, 2005.

[173] Masahiko Higashiyama, Kentaro Inui, Yuji Matsumoto. "Learning Sentiment of Nouns from Selectional Preferences of Verbs and Adjectives". In *Proceedings of the 14th Annual Meeting of the Association for Natural Language Processing*, Tokyo, Japan, pp.584-587, March 2008.

[174] Piyoros Tungthamthiti. "Sentiment Analysis of Sarcasm on Microblogging". Japan Advanced Institute of Science and Technology, Doctoral Dissertation, September, 2016.

[175] Google Cloud Natural Language API. `https://cloud.google.com/natural-language/`. Accessd June 2017.

[176] IBM AlchemyLanguage. `https://www.ibm.com/watson/developercloud/alchemy-language.html`. Accessd June 2017.

[177] Alexandre Bovet, Flaviano Morone, Hernan A. Makse. "Validation of Twitter opinion trends with national polling aggregates: Hillary Clinton vs Donald Trump". `https://arxiv.org/abs/1610.01587`. Published April 26, 2017. Accessd June 2017.

[178] The Japan Times. "System trouble grounds JAL ' s domestic flights, affects travelers". `http://www.japantimes.co.jp/news/2016/04/01/`

national/system-trouble-grounds-jals-domestic-flights-affects-travelers/. Published April 1, 2016. Accessd June 2017.

[179] IT Pro. "JAL system trouble - latest remediation of exclusive control cause deadlock" (published in Japanese). http://itpro.nikkeibp.co.jp/atcl/news/16/040601011/. Published April 6, 2016. Accessd June 2017.

[180] Livedoor News. "Panama papers revealed the tax heaven" (published in Japanese). http://news.livedoor.com/article/detail/11396947/. Published April 10, 2016. Accessd June 2017.

[181] The Yomiuri Shimbun.. "Information Breach from JTB - sophisticated attack technique" (published in Japanese). http://www.yomiuri.co.jp/science/goshinjyutsu/20160615-OYT8T50004.html. Published June 15, 2016. Accessd June 2017.

[182] Nikkei Inc. "17 Years Boy Is Arrested because of CyberAttack" (published in Japanese). http://www.nikkei.com/article/DGKKASDG27H5S_X20C16A6CR0000/. Published June 28, 2016. Accessd June 2017.

[183] CIO From IDG. "What is cyber insurance and why you need it". http://www.cio.com/article/3065655/cyber-attacks-espionage/what-is-cyber-insurance-and-why-you-need-it.html. Published May 4, 2016. Accessd June 2017.

[184] Latham & Watkins. "Cyber Insurance: A Last Line of Defense When Technology Fails". https://www.lw.com/thoughtLeadership/lw-cybersecurity-insurance-policy-coverage. Published April 15, 2014. Accessd June 2017.

[185] PwC. "Turnaround and transformation in cybersecurity - Key findings from The Global State of Information Security Survey 2016". http://www.pwc.com/sg/en/publications/assets/pwc-global-state-

of-information-security-survey-2016.pdf. Published December, 2015. Accessd June 2017.

[186] PwC. "Insurance 2020 & beyond:Reaping the dividends of cyber resilience". https://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf. Published September, 2015. Accessd June 2017.

[187] U.S. Securities and Exchange Commission. "CF Disclosure Guidance: Topic No. 2 - Cybersecurity". https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm. Published October 13, 2011. Accessd June 2017.

[188] U.S. Securities and Exchange Commission. "OCIE Cybersecurity Initiative". https://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf. Published April 15, 2014. Accessd June 2017.

[189] NRI SecureTechnologies, Ltd. "NRI Secure Insight 2017 Global Edition". https://www.nri-secure.co.jp/security/report/2016/analysis_global2017.html. Published March, 2017. Accessd June 2017.

[190] Information-technology Promotion Agency. "Empirical Survey of Enterprise Cyber Risk Management " (published in Japanese). https://www.ipa.go.jp/files/000045629.pdf. Published June 30, 2015. Accessd June 2017.

[191] Thomson Reuters. "Insurers struggle to get grip on burgeoning cyber risk market". http://www.reuters.com/article/us-insurance-cybersecurity-idUSKBN0FJ0B820140714. Published July 14, 2014. Accessd June 2017.

[192] Rainer Bohme. "Cyber-Insurance Revisited". In *Proceedings of The 4th Workshop on the Economics of Information Security (WEIS 2005)*, Cambridge, Massachusetts, U.S.A, June 2005.

[193] Rainer Bohme, Gaurav Kataria. "Models and Measures for Correlation in Cyber-Insurance". In *Proceedings of The 5th Workshop on the Economics of Information Security (WEIS 2006)*, Cambridge, England, June 2006.

[194] Woohyun Shim. "Interdependent risk and cyber security : an analysis of security investment and cyber insurance". In *Doctoral Dissertation in Michigan State University*, Michigan, U.S.A., 2010.

[195] Rainer Bohme, Galina Schwartz. "Modeling Cyber-Insurance : Towards A Unifying Framework,". In *Proceedings of The 9th Workshop on the Economics of Information Security (WEIS 2010)*, Massachusetts, U.S.A., June 2010.

[196] Nikhil Shetty, Galina Schwartz, Mark Felegyhazi, Jean Walrand. "Competitive Cyber-Insurance and Internet Security". *Economics of Information Security and Privacy 2010*, pp 229-247, Springer, July 2010.

[197] Parinaz Naghizadeh, Mingyan Liu. "Voluntary Participation in Cyber-insurance Markets". In *Proceedings of The 13th Workshop on the Economics of Information Security (WEIS 2014)*, Pennsylvania, U.S.A., June 2014.

[198] Ranjan Pal. "IMPROVING NETWORK SECURITY THROUGH CYBER-INSURANCE". In *Doctoral Dissertation in University of Southern California*, Calfornia, U.S.A., December 2014.

[199] Yogesh Malhotra. "Stress Testing for Cyber Risks: Cyber Risk Insurance Modeling beyond Value-at-Risk (VaR): Risk, Uncertainty, and, Profit for the Cyber Era". In *Master Thesis in The State University of New York*, New York, U.S.A., January 2015.

[200] Stephanie K. Chak. "Managing Cybersecurity as a Business Risk for Small and Medium Enterprises". In *Master Thesis in Johns Hopkins University*, Baltimore, U.S.A., June 2015.

[201] Information Security Policy Council. "Cybersecurity 2014" (published in Japanese). `https://www.nisc.go.jp/active/kihon/pdf/cs2014.pdf`. Published July 10, 2014. Accessd June 2017.

[202] Marsh & McLennan Companies. "A Cybersecurity Call To Action". `https://www.chertoffgroup.com/files/docs/2e8e875a-78e9-4b5f-b537-7722b1826137.pdf`. Published November 2014. Accessd June 2017.

[203] The Cambridge Risk Framework. "Managing Cyber Insurance Accumulation Risk". `http://cambridgeriskframework.com/downloads`. Published Feburary 2016. Accessd June 2017.

[204] Cyence. `https://www.cyence.net/`. Accessd June 2017.

[205] MIT Technology Review. "Insurers Scramble to Put a Price on a Cyber Catastrophe". `https://www.technologyreview.com/s/603937/insurers-scramble-to-put-a-price-on-a-cyber-catastrophe/`. Published April 6, 2017. Accessd June 2017.

[206] Tokio Marine & Nichido Fire Insurance Co., Ltd. "Strategic Alliance with Cyence" (published in Japanese). `http://www.tokiomarine-nichido.co.jp/company/release/pdf/170602_01.pdf`. Published June 2, 2017. Accessd June 2017.

[207] UpGuard. `https://www.upguard.com/`. Accessd June 2017.

[208] Market Wired. "UpGuard Snags $17 Million to Accelerate Adoption of Cyber Risk Benchmark for Companies, Insurance Providers and Consumers". `http://www.marketwired.com/press-release/upguard-snags-`

17-million-accelerate-adoption-cyber-risk-benchmark-companies-insurance-2150107.htm. Published August 11, 2016. Accessd June 2017.

[209] NRI SecureTechnologies, Ltd. "Security Countermeasure Visualization Service". https://www.nri-secure.co.jp/service/consulting/security_visualization.html. Accessd June 2017.

[210] KPMG. "Cyber Maturity Assessment". https://home.kpmg.com/xx/en/home/services/advisory/risk-consulting/cyber-security-services/cyber-maturity-assessment-cma.html. Accessd June 2017.

[211] AIG. "CyberEdge - End-to-End Cyber Risk Management Solutions". https://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/aig-cyberedge0418finalsingle-brochure.pdf. Accessd June 2017.

[212] NetDiligence. "NetDiligence 2016 Cyber Claims Study". https://netdiligence.com/wp-content/uploads/2016/10/P02_NetDiligence-2016-Cyber-Claims-Study-ONLINE.pdf. Published October 2016. Accessd June 2017.

[213] Insurance Information Institute. "Cyberrisk: Threat and Opportunity". http://www.iii.org/sites/default/files/docs/pdf/cyber_risk_wp_102716-92.pdf. Published October 2016. Accessd June 2017.

[214] Tokio Marine & Nichido Fire Insurance Co., Ltd. "Cyber Risk Insurance - Risk Assessment Discount" (published in Japanese). http://www.tokiomarine-nichido.co.jp/company/release/pdf/160107_01.pdf. Published January 7, 2016. Accessd June 2017.

[215] LAC & Sompo Japan Nipponkoa Insurance Inc. "Cyber Risk Insurance" (published in Japanese). https://www.lac.co.jp/service/product/insurance.html. Accessd June 2017.

[216] Nikkei Inc. “Three Leading Insurance Company Discount the Premium of Cyber Risk Insurance for Small and Medium Sized Enterprise by Submitting Risk Assessment Sheet” (published in Japanese). http://www.nikkei.com/article/DGXLASGC07H0T_X00C17A2EE8000/. Published Feburary 7, 2017. Accessd June 2017.

[217] Tokio Marine & Nichido Fire Insurance Co., Ltd. “Cyber Risk Insurance” (published in Japanese). http://www.tokiomarine-nichido.co.jp/company/release/pdf150209_01.pdf. Published Feburary 9, 2015. Accessd June 2017.

[218] Mitsui Sumitomo Insurance Co., Ltd. “New Product - Cyber Risk Insurance” (Translated from Japanese). http://www.ms-ins.com/news/fy2015/pdf/0902_1.pdf. Published September 2, 2015. Accessd June 2017.

[219] Sompo Japan Nipponkoa Insurance Inc. “New Product - Cyber Risk Insurance” (Translated from Japanese). http://www.sjnk.co.jp/~/media/SJNK/files/news/2015/20150904_2.pdf. Published September 4, 2015. Accessd June 2017.

[220] AIG. “Cyber Insurance”. http://www.aig.com/business/insurance/cyber-insurance. Accessd June 2017.

[221] Thomson Reuters. “Cyber insurance premiums rocket after high-profile attacks”. http://www.reuters.com/article/us-cybersecurity-insurance-insight-idUSKCN0S609M20151012. Published October 12, 2015. Accessd June 2017.

[222] Financial Service Agency. “Research Paper about Cyber Security Countermeasure of Foreign Fianncial Services” (published in Japanese). http://www.fsa.go.jp/common/about/research/20150706-4/01.pdf. Published March 31, 2015. Accessd June 2017.

[223] AIG. "CyberEdge Plus". http://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyberedge-plus-070616-final-digital.pdf. Accessd June 2017.

[224] Mitsui Sumitomo Insurance Co., Ltd. "Start to Provide the insurance for Bit-Coin service providers" (published in Japanese). http://www.ms-ins.com/news/fy2016/pdf/1124_1.pdf. Published November 24, 2016. Accessd June 2017.

[225] Sompo Japan Nipponkoa Insurance Inc. "Starts to Provide the Special Insurance for Self-Driving Car" (published in Japanese). http://www.sjnk.co.jp/~/media/SJNK/files/news/2016/20170227_1.pdf. Published Feburary 27, 2017. Accessd June 2017.

[226] British Government. "UK Cyber Security - The Role of Insurance in Managing and Mitigating the Risk". https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf. Published March 2015. Accessd June 2017.

[227] IT News. "Zurich fights Sony breach pay out". https://www.itnews.com.au/news/zurich-fights-sony-breach-pay-out-264629. Published July 25, 2011. Accessd June 2017.

[228] Insurance Business. "Zurich reaches settlement with Sony over PlayStation hack". http://www.insurancebusinessmag.com/us/news/breaking-news/zurich-reaches-settlement-with-sony-over-playstation-hack-22314.aspx. Published May 1, 2015. Accessd June 2017.

[229] Thomson Reuters. "Companies use kidnap insurance to guard against ransomware attacks". http://www.reuters.com/article/us-cyber-attack-insurance-idUSKCN18F1LU. Published May 19, 2017. Accessd June 2017.

[230] David Nathans. "Cyber-Insurance: Fraud, Waste or Abuse". *RSA Conference USA 2017*. https://www.rsaconference.com/events/us17/agenda/sessions/5617-Cyber-Insurance-Fraud,-Waste-or-Abuse. Published February 17, 2017. Accessd June 2017.

[231] Cyber Data Risk Managers. "How much does Cyber/Data Breach Insurance Cost?". https://databreachinsurancequote.com/cyber-insurance/cyber-insurance-data-breach-insurance-premiums/. Published June 2, 2017. Accessd June 2017.

[232] Sankei West. "Emerging cyber attack but cyber risk insurance has not been popular in Japan". (published in Japanese). http://www.sankei.com/west/news/140917/wst1409170002-n1.html. Published September 17, 2014. Accessd June 2017.

[233] Sankei West. "The Alliance of Cyber Risk Insurance" (published in Japanese). http://www.sankei.com/west/news/170321/wst1703210008-n1.html. Published March 21, 2017. Accessd June 2017.

[234] Bank of Japan. "Risk Management about Business Process Outsourcing in Financial Services" (published in Japanese). https://www.boj.or.jp/research/brp/ron_2001/fsk0104b.htm/. Published April 17, 2017. Accessd June 2017.

[235] NRI SecureTechnologies, Ltd. "NRI Secure Information Security Trends Annual Report 2013" (published in Japanese). https://www.nri-secure.co.jp/security/report/2013/analysis.html. Published Feburary 21, 2014. Accessd June 2017.

[236] Ministry of Economy, Trade and Industry. "Information Security Management Guidelines for the Use of Cloud Computing Services". http://www.meti.go.jp/press/2013/03/20140314004/20140314004-2.pdf. Published March 14, 2014. Accessd June 2017.

[237] Ministry of Economy, Trade and Industry. "Information Security Countermeasure Guidance about Outsourcing" http://www.meti.go.jp/policy/netsecurity/docs/secgov/2009_OutsourcingJohoSecurityTaisakuGuidance.pdf. Published June, 2009. Accessd June 2017.

[238] The Center for Financial Industry Information Systems. "FISC security Guidelines on Computer Systems for Banking and Related Financial Institutions(Revised Supplement to the 8th Edition)". https://www.fisc.or.jp/publication/disp_target_detail.php?pid=316. Published June, 2015. Accessd June 2017.

[239] Information-technology Promotion Agency. "Secure Usage of Cloud Service". http://www.ipa.go.jp/security/keihatsu/pr2012/ent/02_cloud.html. Accessd June 2017.

[240] INTERNET Watch. "Personal Information Leakage of Investor Network Service was caused from Internal Corporate Environment" (published in Japanese). http://internet.watch.impress.co.jp/docs/news/704705.html. Published June 1, 2015. Accessd June 2017.

[241] Tokio Marine & Nichido Fire Insurance Co., Ltd. "Insurance for Amazon Web Services Users" (published in Japanese). http://www.tokiomarine-nichido.co.jp/company/release/pdf/151229_01.pdf. Published December 29, 2015. Accessd June 2017.

[242] BBC News. "Energy firm cyber-defence is 'too weak', insurers say". http://www.bbc.com/news/technology-26358042. Published February 27, 2014. Accessd June 2017.

[243] Tokio Marine & Nichido Fire Insurance Co., Ltd. "Cyber Risk Comprehensive Support Service" (published in Japanese). http://www.tokiomarine-

nichido.co.jp/company/release/pdf/150810_01.pdf. Published August 10, 2015. Accessd June 2017.

[244] Hiroshima Bank, Tokio Marine & Nichido Fire Insurance Co., Ltd. "Cyber Security Countermeasure Support Loan" (published in Japanese). http://www.hirogin.co.jp/ir/news/paper/news160606-1.pdf. Published June 6, 2016. Accessd June 2017.

[245] Verizon Enterprise Solutions. "2015 Verizon Data Breach Investigations Report". https://www.verizonenterprise.com/jp/DBIR/2015/. Published July 2015. Accessd June 2017.

[246] Trend Micro. "Cybercriminal Underground Economy Series - Russian Underground Revisited". http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf. Published April 2014. Accessd June 2017.

[247] Ayumi Izumi, Shinya Kato, Ayako Komatsu, Toshihiko Takemura. "An Empirical Analysis on Cyber Risk". In *Proceedings of Computer Security Symposium 2015 (CSS2015)*, Nagasaki, Japan, pp.631–638, Information Processing Society of Japan, October 2015.

[248] INTERNET Watch. ""Do not hide the security incident" SoundHouse CEO talked about the experience of unauthorized Access" (published in Japanese). http://internet.watch.impress.co.jp/cda/news/2008/06/18/19989.html. Published June 18, 2008. Accessd June 2017.

[249] INTERNET Watch. "The Aplogy and Notice about Information Leakage with Unauthorized Access" (published in Japanese). https://www.soundhouse.co.jp/company/news/pdf/20080418.pdf. Published April 18, 2008. Accessd June 2017.

[250] NRI SecureTechnologies, Ltd. "Cyber Security Trend Annual Report 2014". https://www.nri-secure.co.jp/security/report/pdf/2014/cstar_2014_en.pdf. Published August 2014. Accessd June 2017.

[251] Ponemon Institute. "2015 Ponemon Cost of Data Breach Study". https://www.ibm.com/security/data-breach/. Published May 2015. Accessd June 2017.

[252] Shay Chen. "The Web Application Vulnerability Scanners Benchmark". http://sectooladdict.blogspot.jp/2014/02/wavsep-web-application-scanner.html. Published February 5, 2014. Accessd June 2017.

[253] Thomson Reuters. "Cyber attack could cost Sony studio as much as $100 million". http://www.reuters.com/article/us-sony-cybersecurity-costs-idUSKBN0JN2L020141209. Published December 9, 2014. Accessd June 2017.

[254] Thomson Reuters. "For Sony Pictures CEO, cyberattack won't set studio back". http://www.reuters.com/article/us-northkorea-cyberattack-sony-idUSKBN0KI02420150109. Published January 8, 2015. Accessd June 2017.