サイバーリスク保険を利用したセキュリティマネジメントの一考察

石川 朝久 †　　櫻井　幸一 †

† 九州大学
819-0395 福岡市西区元岡 744
ishikawa@inf.kyushu-u.ac.jp
sakurai@inf.kyushu-u.ac.jp

あらまし 昨今の情報漏洩から、セキュリティマネジメントの必要性はより重要視されており、専門家によるベストプラクティスを示す資料は充実してきている。しかしながら、推奨されるすべての対策を実装することはコスト面でも難しく、実用的なセキュリティ投資・リスク検討手法も整理されていないため、費用対効果が分かりづらいと指摘されている。今回の論文では、セキュリティマネジメントの手法として比較的新しいサイバーリスク保険について、最近の動向を整理するとともに、サイバーリスク保険の有用性を検証するため、モンテカルロ・シミュレーションアプローチによる分析・考察を行った。

A Study of Security Management with Cyber Risk Insurance

Tomohisa Ishikawa†　　Kouichi Sakurai†

†Kyushu University
744 Motooka Nishi-ku, Fukuoka 319-0395, JAPAN
ishikawa@inf.kyushu-u.ac.jp
sakurai@inf.kyushu-u.ac.jp

Abstract Since the recent security breach requires the intensification of security management, the documents, describing the best practice of security management, are published by experts. However, the implementations of all best practice are very difficult because of cost and the difficulty of cost-effective security investment. This paper discuss the security management theory with cyber risk insurance, especially the effectiveness of cyber risk insurance by Monte Carlo simulation approach.

1　はじめに

2014 年度以降、米大手保険会社 [1][2][3]、映画配給会社 [4]、政府機関 [5][6][7] などへの大規模な不正アクセスが継続的に報道されており、情報漏洩事故は後を絶たない。RSA President の Amit Yoran 氏は、RSA Conference USA 2015 の基調講演にて、情報漏洩が連続して発生している現状を「暗黒時代」と評している [8]。この現状を受けて、セキュリティマネジメントの必要性はより重要視されており、その要請に答える形で NIST CyberSecurity Framework[9]、SANS Critical Security Control[10] などセキュリティマネジメントのベストプラクティスを示した資料が充実してきている。実際、警察庁の調査 [11] によれば、98.5%の組織が「情報セキュリティ対策の必要性を感じている」と回答して

おり、61.7%の組織が「情報セキュリティに対して積極的に投資すべき」という考え方を持っている。

その一方、上記ベストプラクティスをすべて実施することは、業務設計やコストの観点から難しく、実用的なセキュリティ投資指針も整理されていない。上記調査 [11] においても、セキュリティ対策上の問題として、「費用対効果が見えない」と回答した組織が 59.6%、「どこまで行えばよいかの基準が示されていない」と回答した組織は 46.3%に上る。また、35.4%の企業が「セキュリティサービスを利用していない」と回答しており、43.7%の組織が「予算がない」、32.9%が「価格が見合わない」と述べている。

本論文では、これらの課題を克服するため、セキュリティマネジメントにおける費用対効果について検討を行う。特に、IPA が 2015 年 6 月 [12] 最近レポートして取り上げたサイバーリスク保険を踏まえたセキュリティマネジメントについて考察を試みる。

2 先行研究

セキュリティマネジメントにおける被害額推定手法や費用対効果については、いくつかの分野において先行研究があるため、アプローチの観点から整理する。

2.1 数理モデルアプローチ

第一に、数理モデルによるアプローチが挙げられる。このアプローチの代表的研究として、Gorden&Loeb の最適投資理論 (Gorden&Loeb Model)[13] が知られている。本モデルでは、脆弱性 v、セキュリティ投資 z によって定まる情報漏洩確率関数 $S(v,z)$ が特定の数学関数に従うとき、セキュリティ投資は $1/e(\approx 36.79\%)$ 以下にとどめるべきと示した。この論文から、様々なモデルの拡張が試みられている [14][15][16][17][18]。数理モデルにより明確な結論が得られる一方、モデル内で定義される関数が抽象的で、現実への応用が難しいと考えられる。

2.2 分析フレームワークアプローチ

第二に、分析フレームワークによるアプローチが挙げられる。これは、被害額に影響する観点・項目をフレームワークとして整理を行い、被害額の算出をするアプローチである。

国内では、2001 年に IPA が提唱した「被害額算出モデル」[19][20]、JNSA が提唱している「セキュリティインシデント被害額算出モデル」[21] や「JO モデル」[22] などが有名である。そのほかにも、「情報セキュリティ会計」[23] や、株価への影響分析 [24] などいくつかの方法論も検討されているが、あまり根付いていない。また、2013 年度以降のセキュリティインシデントが報道されるようになってから、IPA を中心にモデル拡張に関する議論 [25] や、サイバーリスク保険に関する認識調査 [12] などを始めており、再度注目されている。

国外では、ROSI(Return On Investment)[26] や、米エコノミスト社が提唱する CyberTab[27] などが挙げられる。また、韓国では被害額推定手法の研究が活発に行われており、KISA モデル [28] や Gorden&Loeb の考え方をもとにした「インターネット侵害事故被害額算出モデル」[29] などが提唱されており、様々な応用が行われている [30][31]。実際に、韓国科学技術院 (KAIST) の研究グループは、2013 年 3 月 20 日に発生した韓国の同時多発サイバー攻撃の被害額を 8,672 億ウォンと推定した [32]。

この手法は、多くの活用で利用されている一方、各要素のデータを収集が難しいこと、各組織の個別要素に大きく依存すること、将来的な推計がしづらい点が挙げられる。

2.3 統計データアプローチ

第三に、統計データアプローチが挙げられる。各セキュリティ企業が独自アンケート調査・自社サービスのデータを利用して分析を行うアプローチである。Incapsula 社のレポート [33] では DDoS 攻撃を受けたときの 1 時間あたりにかかるコストが$40,000 であることを明らかにし、Ponemon 社のレポート [34] では 1 レコード当たりの情報漏洩コストは$157 であることを示し

た。これらのデータはセキュリティマネジメントにおけるベンチマークとしてよく活用される一方、個別の組織に活用する点が難しいという点が挙げられる。

2.4　シミュレーションアプローチ

第四に、シミュレーションアプローチが挙げられる。これは、統計データアプローチの取得データとモンテカルロシミュレーションを組み合わせて、より現実に近いデータを算出するアプローチである。この分野の論文は数少ないが実施されており、Conrad[35] や Lyon[36] の研究が挙げられる。本研究では、このアプローチを採用し、サイバーリスク保険の効用について測定する。

3　サイバーリスク保険

サイバーリスク保険は、リスク対応戦略（回避・軽減・転移・受容）の「リスク転移」の具体的手法として知られている。米国では、規制による罰金や集団訴訟も多いため、非常に一般的なリスク対応戦略として知られており、その市場規模も大きい。Latham & Watkins 社のホワイトペーパー [37] では、サイバー攻撃の最終防衛ラインとして保険が有効であると指摘し、統合的なリスク管理として保険は有益なツールであると述べている。また、Marsh 社の調査によれば、2013 年度における正味収入保険料で 10 億ドルの市場規模であると報じられている [38]。実際に、POS マルウェアで 4000 万件のカード情報、7000 万件の個人情報漏洩に見舞われたターゲット社 [39] は、累積 2.52 億ドル（2014 年度 4 半期時点）の対策コストを計上し、2015 年 3 月には集団訴訟により 12.2 億ドルの賠償金を支払うことで和解しているが、うち 0.9 億ドルは保険により賄われていると報じられている。[40]

一方、国内でのサイバーリスク保険の知名度は低く、2015 年 6 月に IPA が発表した調査 [12] によれば、28%にとどまり、保険の売り行きも伸び悩んでいると報告されている [41]。但し、生命保険分野などでは日本は米国に次ぐ保険大国 [42] だと知られているため、サイバーリスク保険の認知度が上がれば、市場も拡大すると考えられる。

3.1　サイバーリスク保険の特徴

サイバーリスク保険は、現在数社で提供が行われており [43][44][45][46]、補償範囲はほぼ同じである。たとえば、AIU 保険の CyberEdge においては、保障分野は「賠償責任に対する補償」、「行政手続きに対する補償」「危機管理対応費用に対する補償」の 3 種類を規定し、実際のインシデントにかかる費用をほぼすべてカバーしている。金融庁の委託研究 [47] によれば、海外の動向も同様である。但し、海外の方が訴訟・罰金による金銭的コストが膨らむ傾向にあるため、罰金への補償など保険の種類も幅広く見受けられる。

3.2　サイバーリスク保険の研究

サイバーリスク保険の研究については、経済学・数理モデルの観点から学術的研究が行われている [48][49]。その一方、実務の観点からは、重要な保険数理上のデータが手に入らないため、伝統的な手法でリスク評価をすることが難しく、保険の料率、リスク評価方法について検討段階にあると言われている [38]。その中で、Marsh 社がこの分野において積極的なレポート公開をしており、Cyber IDEAL(Identify Damages, Evaluate, and Assess Limits) という分析手法を公表している [50][51]。

4　シミュレーション概要

本研究では、セキュリティマネジメントの費用対効果を分析するため、シミュレーションによる分析を行った。セキュリティ投資・被害総額の詳細情報は公開情報となりづらいことから、仮想的なモデル企業を想定し、各種レポートから取得した統計情報をもとにモンテカルロシュミレーションを実施した。

4.1 モデル構築

仮想的なモデル企業として、通信販売会社を想定し、当該モデル企業のみ存在する社会を想定する。今回の実験では、2008 年に SQL インジェクション攻撃により情報漏洩事故に遭遇した「サウンドハウス社」をモデルとしてパラメータを決定した。理由は、被害額や対応の詳細を公表 [52][53] しており、現実に即したシミュレーションが可能となるためである。

4.1.1 攻撃対象データ

当該モデル企業は、金銭的価値を持つデータとして「顧客情報レコード」のみを保有する。

4.1.2 存在する脆弱性

当該サイトはEC サイトを運営しており、SQL Injection 脆弱性のみ脆弱性として存在する。但し、自社サイトに SQL Injection 脆弱性の存在を把握できていないと仮定し、ある確率モデルに従い脆弱性の存在を確定する。脆弱性が存在しないケースでは、情報は漏洩しないとする。以上の条件から、「顧客情報レコード」を SQL Injection 脆弱性にて取得するということを想定する。以下に簡単なフローチャートを示す。

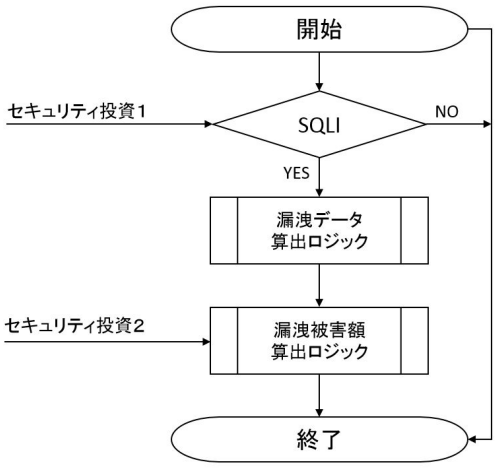

図 1: シミュレーションフロー

4.1.3 初期パラメータ：モデル企業

モデル企業を、以下の通りに設定する。

表 1: 初期パラメータ：モデル企業

項目	記号	値
売上 (円)	R_{ev}	7,000,000,000
利益率	P_{ro}	15%
顧客レコード数	R_{max}	300,000

4.1.4 初期パラメータ：情報漏洩条件

情報漏洩条件に関連する初期パラメータとして、以下のパラメータを想定した。

表 2: SQL インジェクションの存在確率

項目	記号	値
存在確率（投資なし）	P_0	16.72%
存在確率（投資あり）	P_1	05.00%

脆弱性の存在確率は、『サイバーセキュリティ傾向分析レポート 2014』[54] をもとに、5 年間の統計データの平均値を採用した。また後述するセキュリティ投資を行った場合は、存在確率を下げるモデルとした。

表 3: 漏洩データ決定ロジック

項目	記号	値
漏洩データ数	N_i	三角分布にて決定
最小値	N_{min}	2415
最大値	N_{max}	300,000
平均値	N_{ave}	29,087

漏洩データ数については、Ponemon Institute のデータ [34] を採用し、確率分布（三角分布）に基づいて漏洩データ数を決定するモデルを想定した。

4.1.5 初期パラメータ：セキュリティ投資

情報漏洩への対策を考慮するため、以下の 2 つのセキュリティ投資 (投資コスト：C_{inv}) をモデル化した。

表 4: 投資 1 ：セキュリティ診断

項目	記号	値
コスト	C_1	4,000,000
効用	P_1	存在確率：5.0%に低下

表 5: 投資 2 ：サイバーリスク保険

項目	記号	値
コスト	C_2	500,000
効用	I_{cmp}	以下のコストをカバーする 顧客への賠償責任　1 億円 費用損害 3,000 万円

投資 1 は、「セキュリティ診断」である。投資コスト 400 万円に対し、SQL Injection の存在確率を 5.0%まで低下させると仮定した。金額についてはサウンドハウス社の事例から、SQL インジェクション攻撃の存在確率については、一般的な Web アプリケーション用スキャナの SQLI 検知率が 95%前後であることを根拠 [55] に、診断実施後も脆弱性が存在すると想定している。

投資 2 は、「サイバーリスク保険」である。前述の通り、サイバーリスク保険については実際の商品が公開されている一方、その仔細についてはわからないことも多い。モデル企業の想定売上をベースに、東京海上日動が出している「情報漏えい保険」のサンプル例 [43] を採用した。

4.1.6　漏洩被害額（総コスト）

情報漏洩事故が発生した場合に発生する被害額（総コスト：C_{total}）は、以下の 3 つの値の合計で構成される。

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

表 6: 漏洩被害額：総コスト

項目	記号
セキュリティ投資コスト	C_{inv}
事故対応コスト	$C_{ir-total}$
顧客対応コスト (お詫び)	$C_{cp-total}$
顧客対応コスト (QA 対応)	$C_{qa-total}$

但し、SQL Injection 脆弱性が存在しない場合、セキュリティ投資コストのみコストとして計上される。

今回のモデルでは、情報漏洩事故で発生するコストを「事故対応コスト」、「顧客対応コスト」に分類される。

「事故対応コスト」とは、フォレンジック調査費用、復旧コスト、セキュリティ対策費用などを含む。今回、仮想モデル企業にかかるコストについては、サウンドハウス社が公表したコスト [52] をもとに算出し、固定値とした。

「顧客対応コスト」とは、お詫び金やそれに伴う事務費用、QA 対応など対顧客への対応コストなどを意味する。今回は、企業が直接支払う「顧客対応コスト (お詫び)」と、顧客問い合わせによる「顧客対応コスト (QA 対応)」を想定して、以下の値を検討した。

表 7: 漏洩被害額：事故対応コスト

項目	値
インシデント調査費用	4,000,000
サーバ改竄検知ツール	1,100,000
FW 監視サービス	4,200,000
IPS 監視サービス	15,000,000
セキュリティ診断サービス	4,200,000
サーバールーム諸工事	300,000
合計 ($C_{ir-total}$)	28,800,000

表 8: 漏洩被害額：顧客対応コスト (お詫び)

項目	記号	値
お詫び金合計	$C_{cp-total}$	$N_i * C_{cp}$
漏洩データ数	N_i	既に記載済み
お詫び金単価	C_{person}	750 円/人

表 9: 漏洩被害額：顧客対応コスト (QA 対応)

項目	記号	値
合計	$C_{qa-total}$	$N_i * P_{qa} * C_{qa}$
漏洩データ数	N_i	既に記載済み
問い合わせ率	P_{qa}	5.0%
QA 対応単価	C_{qa}	1,000

「お詫び金」については、事例に従い一人あたり 500 円を想定した。なお、事務処理コスト（おわび状、郵送費用）もかかるため、モデルでは 750 円で計算した。

問い合わせによる「QA 対応」コストは、漏洩データ数 N に比例して決定すると仮定する。サウンドハウス社の場合、漏洩データ件数に対して、約 5.0%の人から問い合わせが行われているため、その値を参考とした。また、一人当たりの対応に平均 1000 円程度かかると想定し、上記式を想定した。

4.1.7　モデルによるシミュレーション

上記モデルを Python と R 言語を用いて実装して、シミュレーションを実施した。その際、セキュリティ投資状況によりどのように総コストが変わるのか分析するため、以下の 4 種類のシナリオを想定して分析を行った。

表 10: シミュレーション・シナリオ

		投資 2	
		未採用	採用
投資 1	未採用	CASE 1	CASE 3
	採用	CASE 2	CASE 4

5　実験結果と分析

4 種類のシナリオそれぞれに対し、100 万回のシミュレーション試行を行い、分析を行った。

表 11: 結果一覧（単位：件, 百万円）

	CASE1	CASE 2	CASE 3	CASE 4
SQLI 存在確率	16.72%	5.00%	16.72%	5.00%
サイバー保険	なし	なし	あり	あり
攻撃成功件数	167,141	50,136	167,232	50,215
コスト（最小値）	0.000	4.000	0.500	4.500
コスト（最大値）	301.083	304.739	171.834	175.726
コスト（平均値）	25.172	11.548	8.829	6.999
コスト（中央値）	0.000	4.000	0.500	4.500
平均相対コスト	1	0.459	0.351	0.278
ROSI	-	3.406	32.686	4.038

コストの平均値（期待値）をもとに相対コストを算出したところ、シミュレーション上、2 つの投資戦略を同時にとることにより 72.2%のコスト削減に寄与していることが分かる。また、サイバー保険単体で見ても 64.9%コスト削減可能であることが確認できた。

また、ROSI とは、セキュリティ投資によりコストの平均値減少にどれぐらい寄与しているか、その比率を分析したものになる。セキュリティ診断の ROSI は約 3.4 倍、サイバーリスク保険の ROSI は、32.68 倍だということがわかる。保険の条件などに依存するが、ROSI として高い効用をもたらすこと施策だと言える。

また、同様に「攻撃に成功した」事例のみで集計すると以下のようなデータを得た。

表 12: 結果一覧（単位：件, 百万円）

	CASE1	CASE 2	CASE 3	CASE 4
SQLI 存在確率	16.72%	5.00%	16.72%	5.00%
サイバー保険	なし	なし	あり	あり
攻撃成功件数	167,141	50,136	167,232	50,215
コスト（最小値）	63.986	68.094	32.500	36.500
コスト（最大値）	301.083	304.739	171.834	175.726
コスト（平均値）	150.602	154.560	50.306	54.268
コスト（中央値）	141.489	145.634	32.500	36.500

表 13: 保険効果率・ROSI

保険効果率	$CASE3/CASE1$	0.334
保険効果率	$CASE4/CASE2$	0.351
ROSI	$(CASE1 - CASE3)/C_{inv}$	200.562
ROSI	$(CASE2 - CASE4)/C_{inv}$	200.584

以下に「攻撃に成功した」事例のみを集計し、被害額の分布を示す。最初に定義した三角分布に従う形となり、また保険の有無により x 軸方向に約 42.3%移動することが分かる。このことから、保険効果によりコストが約 65%低下すること、ROSI が 200 倍程度あることを踏まえるとサイバーリスク保険が非常に効果の高い「リスク転移」戦略であることが分かる。

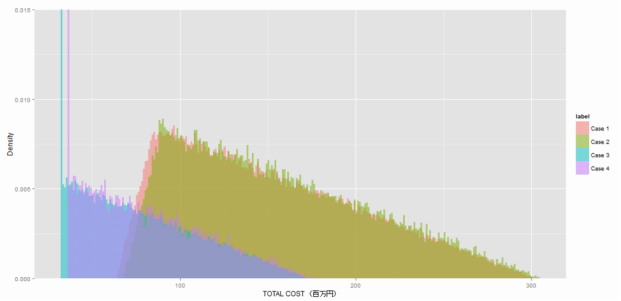

図 2: 攻撃成功時の被害額確率分布

6 まとめ

本稿では、被害額算出手法について先行研究を整理した後、サイバー保険の特徴について分析を行った。そのうえで、サイバーリスク保険の具体的な影響を確認するため、想定モデル企業を利用したモンテカルロシミュレーションを実施してサイバーリスク保険の影響について検討を行った。分析の結果、サイバーリスク保険により 65%の予算削減、および ROI としては 32 倍に上るということが分かった。これらの条件は想定しているリスク・保有データ・保険の諸条件により決まるが、かなり効果的な効果をもたらすという結果を示すことができた。今後の研究として、これらのモデルをより精緻に行えるように他のパラメータを追加する、あるいは他の数理モデルの応用を試みたいと考えている。

参考文献

[1] The Wall Street Journal, Anthem: Hacked Database Included 78.8 Million People, http://on.wsj.com/1LAiwDX

[2] The Wall Street Journal, Premera Blue Cross Says Cyberattack Could Affect 11 Million Members, http://on.wsj.com/1Eu5iau

[3] The Wall Street Journal, Health Insurer CareFirst Says It Was Hacked, http://on.wsj.com/1eg4XQI

[4] Forbes, Sony Pictures Hacked And Blackmailed, http://onforb.es/1uzsdJx

[5] The Wall Street Journal, OPM Breach Was Enormous, FBI Director Says, http://on.wsj.com/1eHdKev

[6] The Wall Street Journal, Breach at IRS Exposes Tax Returns, http://on.wsj.com/1J3nkUf

[7] 日本年金機構, 日本年金機構の個人情報が流出したお客様へのお詫びについて, http://www.nenkin.go.jp/n/data/service/0000028648uArRENS1eQ.pdf

[8] Yoran, A., Escaping Securitys Dark Ages, RSA Conference 2015, http://www.rsaconference.com/media/escaping-securitys-dark-ages

[9] National Institute of Standards and Technology, NIST Cybersecurity Framework, http://www.nist.gov/cyberframework/

[10] SANS Institute, SANS Critical Security Control, https://www.sans.org/critical-security-controls/

[11] 警察庁, 不正アクセス行為対策等の実態調査 調査報告書, http://www.npa.go.jp/cyber/research/h26/h26countermeasures.pdf

[12] 情報処理推進機構, 企業におけるサイバーリスク管理の実態調査 2015, https://www.ipa.go.jp/files/000045629.pdf

[13] Gordon, L.A. ,Loeb, M.P, The Economics of Information Security Investment, ACM Transactions on Information and System Security, Vol. 5, No. 4, November 2002, Pages 438-457.

[14] 松浦 幹太, 情報セキュリティと経済学, The 2003 Symposium on Cryptography and Information Security,Jaanuary 2003

[15] 倉光 君郎, 最適投資モデルに基づくセキュアシステム設計と事例研究, 情報処理学会研究報告, 2005-CSEC-30, July 2005

[16] Willemson, J, , On the Gordon&Loeb Model for Information Security Investment, WEIS 2006,June 2006

[17] Willemson, J, , Extending the Gordon and Loeb Model for Information Security Investment, ARES 2010,February 2010

[18] Varyshnikov, Y. , IT Security Investment and Gordon-Loeb's 1/e Rule, WEIS 2012,June 2012

[19] 情報処理推進機構, 情報セキュリティインシデントに関わる調査 調査報告書 (2001), http://www.ipa.go.jp/security/fy13/report/incident_survey/incident_survey.pdf

[20] 情報処理推進機構, 「被害額算出モデル」報告書 (2003), http://www.ipa.go.jp/security/fy14/reports/current/2002-calc-model.pdf

[21] NPO 日本ネットワークセキュリティ協会, 2003 年度情報セキュリティ関する調査報告書 ～第一部～ 情報セキュリティのインシデントに関する調査および被害算出モデル, http://www.jnsa.org/houkoku2003/incident_survey1.pdf

[22] NPO 日本ネットワークセキュリティ協会, 2003 年度 情報セキュリティ関する調査報告書 ～第二部～ 情報漏洩による被害想定と考察 (賠償額および株価影響額), http://www.jnsa.org/houkoku2003/incident_survey2.pdf

[23] NPO 日本ネットワークセキュリティ協会, 情報セキュリティ会計に関する検討報告書, http://www.jnsa.org/houkoku2004/kaikei_report.pdf

[24] 田中 勝行, 企業の情報セキュリティ事故による株価への影響に関する実証研究, http://www.aoyamabs.jp/programs/files/essay2011_k_tanaka.pdf

[25] 情報処理推進機構, 情報セキュリティ被害と対策に関する委員会報告 ～企業における脅威と被害の新たなモデル構築～, http://www.ipa.go.jp/security/fy14/reports/current/2002-calc-model.pdf

[26] ENISA, Introduction to Return on Security Investment, December 2012

[27] The Economist IntelligenceUnit Ltd, CyberTab, https://cybertab.boozallen.com/

[28] Korea Advanced Institute of Science and Technology,『国家サイバーセキュリティ被害額の分析と対策 - 3.20 サイバー侵害事件を中心に』(筆者邦訳), March 2013

[29] Yoo, Y. , Gee, S. , Song, H. , Chung, K., Lim, J., Estimating Economic Damages from Internet Incidents, 2008

[30] Yoo, H., 『情報保護の侵害事故発生による被害額算出モデル”』(筆者邦訳), The Korean Operations Research and Management Science Society, 2010, http://www.korms.or.kr/korms_2010_spring.htm, http://www.cimerr.net/vod/cyber2010_spring/B10-5/B10-5/B10-5.pdf

[31] Han, C.H. , Chai, S.W. , Yoo, B.J. , Ahn, D.H., Park, D.H., A Quantitative Assessment Model of Private Information Breach, October, 2011

[32] 中央日報日本語版, 3月の韓国コンピューター網まひ、被害総額は８６７２億ウォン, http://japanese.joins.com/article/903/175903.html

[33] Incapsula, Incapsula Survey : What DDoS Attacks Really Cost Businesses, 2014, https://www.incapsula.com/blog/ddos-impact-cost-of-ddos-attack.html

[34] Ponemon Institute, 2015 Cost of Data Breach Study, 2015, http://www-03.ibm.com/security/data-breach/

[35] Conrad, J.R., Analyzing the Risks of Information Security Investments with Monte-Carlo Simulations, IEEE, March 2005

[36] Lyon,D., Modeling Security Investments With Monte Carlo Simulations, SANS Institute: Reading Room

[37] Latham & Watkins, Cyber Insurance: A Last Line of Defense When Technology Fails, http://www.lw.com/thoughtLeadership/lw-cybersecurity-insurance-policy-coverage

[38] ロイター通信, 欧米の保険会社、サイバー犯罪リスクに対応した商品の成長に期待, http://jp.reuters.com/article/2014/07/15/idJPL4N0PQ19O20140715

[39] IT Leaders, 7000 万件に及ぶ情報漏洩事件の「その後」、株価復調も CEO の辞任に発展した米 Target, http://it.impressbm.co.jp/articles/-/11538

[40] Bank Info Security, Target Breach Costs: $162 Million, http://www.bankinfosecurity.com/target-breach-costs-162-million-a-7951

[41] ITMedia, 日本でさっぱり売れない「サイバーセキュリティ保険」、普及への壁,http://itpro.nikkeibp.co.jp/atcl/column/14/346926/031600197/

[42] 日本経済新聞, 保険大国ニッポンを支える「考え抜かない加入」, http://www.nikkei.com/money/household/hokenhonto.aspx?g=DGXNASFK1201F_12072014000000

[43] 東京海上日動, 個人情報漏えい保険, http://www.tokiomarine-nichido.co.jp/hojin/baiseki/roei/

[44] 三井住友海上, 情報漏えいプロテクター, http://www.ms-ins.com/business/indemnity/pd-protector/

[45] 損保ジャパン日本興亜, 個人情報取扱事業者保険, http://www.sjnk.co.jp/hinsurance/risk/liability/information/

[46] AIU 保険, CyberEdge, http://www.aiu.co.jp/business/product/liability/cyberedge/index.htm

[47] 金融庁, 諸外国の金融分野のサイバーセキュリティ対策に関する調査研究報告書, http://www.fsa.go.jp/common/about/research/20150706-4.html

[48] Bohme, R. , Schwartz, G. , Modeling Cyber-Insurance:Towards A Unifying Framework, Workshop on the Economics of Information Security (WEIS), June 2010

[49] Naghizadeh, P. , Liu, M. , Voluntary Participation in Cyber-insurance Markets, Workshop on the Economics of Information Security (WEIS), June 2014

[50] Marsh & McLennan Companies, A Cyber Security : A Call to Action, http://chertoffgroup.com/cms-assets/documents/196659-211678.a-cybersecurity-call-to-action.pdf

[51] Marsh & McLennan Companies, Cyber Security Overview, http://www.swensonadvisors.com/assets/Cyber\%20security\%20insurance\%20coverage_RMarx.pdf

[52] INTERNET Watch, 「被害を隠すな」サウンドハウス社長が不正アクセス体験語る, http://internet.watch.impress.co.jp/cda/news/2008/06/18/19989.html

[53] 株式会社サウンドハウス, 不正アクセスに伴うお客様情報流出に関するお詫びとお知らせ, https://www.soundhouse.co.jp/company/news/pdf/20080418.pdf

[54] NRI セキュアテクノロジーズ株式会社, サイバーセキュリティ：傾向分析レポート 2014, http://www.nri-secure.co.jp/news/2014/0820_report.html

[55] Chen, S., The Web Application Vulnerability Scanners Benchmark, http://sectooladdict.blogspot.jp/2014/02/wavsep-web-application-scanner.html