情報処理学会論文誌 Vol.57 No.9 2088–2098 (Sep. 2016)

セキュリティ管理におけるサイバーリスク保険の有効性評価

石川 朝久[1,a)] 櫻井 幸一[1,b)]

受付日 2015年12月3日, 採録日 2016年6月2日

概要：昨今報道されている情報セキュリティ事故により，セキュリティ管理への関心は高まり，その必要性はより重要視されている．また，その動向を受け，多くの専門家や研究機関によりベストプラクティスが示されつつある．その一方，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．そのため，セキュリティ対策担当者からは投資基準・費用対効果が分かりにくいと指摘されている．その批判は，新しいセキュリティ管理手法として最近注目されているサイバーリスク保険にもあてはまる．本論文では，実用的な費用便益分析ができる手法を利用して，サイバーリスク保険の有効性を示すことに成功した．

キーワード：セキュリティ管理，サイバーリスク保険，モンテカルロ・シミュレーション

An Effectiveness Evaluation of Cyber Risk Insurance as a Security Control Method

Tomohisa Ishikawa[1,a)] Kouichi Sakurai[1,b)]

Received: December 3, 2015, Accepted: June 2, 2016

Abstract: Since the recent security breach requires the intensification of security control, the documents, describing the best practice of security control, 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 analyzes related works of security control method based on cost-benefit analysis and current cyber risk insurance. Then, this paper evaluates the effectiveness of cyber risk insurance as the security control method.

Keywords: security management, cyber insurance, Monte Carlo simulations

1. はじめに

1.1 背景

2014 年度以降，米大手保険会社 [1], [2], [3], [4]，映画配給会社 [5]，政府機関 [6], [7], [8]，SNS [9] 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．この現状を受けて，セキュリティ管理の必要性はより重要視されており，その要請に応える形で NIST CyberSecurity Framework [10]，SANS Critical Security Control [11] などセキュリティ管理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 [12] 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．

サイバーセキュリティの問題は従来 IT の問題ととらえられていたが，現在では経営リスクの 1 つとして認識されつつある．世界経済フォーラムの「グローバルリスク報告書 2015 年版」[13] によれば，サイバー攻撃・データ漏洩は，発生可能性・影響度のいずれの観点からも高いリスクと位置づけられている．また，信用格付会社として知られている Standard & Poor's 社は，情報漏洩などのインシデントが発生していない企業でも，サイバーセキュリティ対

[1] 九州大学大学院システム情報科学研究院
Graduate School and Faculty of Information Science and Electrical Engineering, Kyushu University, Fukuoka 819–0395, Japan
[a)] tomohisa.ishikawa@inf.kyushu-u.ac.jp
[b)] sakurai@inf.kyushu-u.ac.jp

策を適切に行っていない場合には格付けを下げる可能性があると発表した [14]．このことから，市場からも経営課題の 1 つとしてセキュリティ管理に取り組むことが求められている．

1.2 動機

前述した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．上記の警察庁の調査においても，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%にのぼる．そのため，実用的なセキュリティ投資判断ができる方法を提示する必要がある．

また，昨今の攻撃は巧妙化しており，インシデントを未然に防止することが困難になりつつある．そのため，セキュリティ事故を前提とした対策も検討する必要があり，その 1 つであるサイバーリスク保険も，セキュリティ施策としての有効性を評価する必要がある．

1.3 先行研究

1.3.1 研究テーマ 1：セキュリティ投資の費用便益分析

セキュリティ投資の費用便益分析には，様々なアプローチが提唱されている．

第 1 に，セキュリティ投資を解析的に解ける数学問題へ定式化するアプローチがあげられる．例として，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 Gorden & Loeb の最適投資理論（Gorden & Loeb Model）[15] や，セキュリティ施策を離散最適化問題として定式化した研究などがある [16], [17]．

第 2 に，被害額算出の観点・項目の整理に重点を置いたアプローチがあり，その研究例を**表 1** に示す．

韓国ではこれらの研究が多数行われており，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 [28]．その一方，「お詫び金」に着目した筆者らの研究 [29] では，推計値と実際の企業が支払う金額に差異があることを示し，モデル化の難しさを指摘した．

表 1 被害額算出の観点・項目の整理によるアプローチ
Table 1 Damage calculation model approach.

モデル名	参考
IPA 被害額算出モデル	[18], [19]
JNSA セキュリティインシデント被害額算出モデル	[20]
JNSA JO モデル	[21]
ALE（Annual Loss Expectancy）モデル	[22]
CyberTab モデル	[23]
KISA モデル	[24], [25]
インターネット侵害事故被害額算出モデル	[26], [27]

第 3 に，各業界団体・サービス提供企業により，アンケート調査・自社サービスデータを利用したデータ分析があげられる．Incapsula 社のレポート [30] では DDoS 攻撃を受けた場合の 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 [31] では 1 レコードあたりの情報漏洩コストは$154 であることを示した．

第 4 に，モンテカルロ・シミュレーションを利用したアプローチがあげられる．昨今の被害額推定では，情報漏洩件数が被害額に大きな影響を与えるため，その分析などに適している．Conrad [32] は，前述の ALE（Annual Loss Expectancy）モデルをベースにモンテカルロ・シミュレーションを利用した分析を行い，その有効性を提案している．Burtescu の研究 [33] では，ALE モデルに加えてリスクレベルを加味したモデルを構築して，リスク管理にモンテカルロ・シミュレーションが有効であることを示している．Lyon の研究 [34] では，SANS Critical Security Control の有効性を評価するためにモンテカルロ・シミュレーションを利用して，その有効性を評価している．

本論文では，サイバーリスク保険の有効性を定量的に評価するため，本アプローチを採用する．

1.3.2 研究テーマ 2：サイバーリスク保険

サイバーリスク保険の研究は，経済学・数理モデルの観点から保険モデルの学術的研究が行われている [35], [36]．その一方，実務（保険数理）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，保険料の料率・リスク評価方法について検討段階にあるといわれている [37]．また，2015 年頃から各組織が保険に関するレポートの公開を始めており，NetDiligence 社 [38]，Marsh 社 [39]，米損保情報調査研究所 [40] などの報告書が知られている．特に，Marsh 社は Cyber IDEAL（Identify Damages, Evaluate, and. Assess Limits）という独自の分析手法を確立し，自社の保険料やリスク分析評価サービスなどを開始している．

1.4 研究課題と貢献

研究課題としては，実用的な費用便益分析手法により，サイバーリスク保険の有効性を示すことである．これにより，各組織のセキュリティ担当者の投資判断をやりやすくし，サイバーリスク保険の普及を後押しできると考えている．本論文は CSS2015 の発表論文 [41] を大幅に発展させることにより作成した．本論文の学術的貢献は以下のとおりである．

- サイバーリスク保険の現状を分析するとともに，定性的・定量的な観点から有効性評価を行い，その有効性を示した．
- モンテカルロ・シミュレーションを利用した想定被害額分析を行うことで，実践的なセキュリティの投資判

断ができることを示した．

2. サイバーリスク保険

サイバーリスク保険とは，セキュリティ事故発生にともなう損害を包括的にカバーする保険であり，リスク対応戦略（回避・軽減・転移・受容）における「リスク転移」の具体的手法として知られている．サイバーリスク保険を利用することで，変動の激しい対応費用の全額または一部を，保険料という形で固定化することが可能となる．Latham & Watkins 社は，「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 [42]．

米国では，規制による罰金や集団訴訟も多いため，一般的なリスク対応戦略として知られている．PwC 社のレポートによれば，証券取引委員会（SEC）のコンプライアンス検査局（OCIE）の指針で，金融サービス企業の加入が推奨されており，調査対象企業の 44%は保険に加入していると報告している [43]．また，Marsh 社の調査によれば，2014 年度における正味収入保険料で 20 億ドルの市場規模であると報じられている [44]．

一方，国内でのサイバーリスク保険の認知度は低く，2015 年 6 月に IPA が発表した調査 [45] によれば，28%程度である．また，JNSA の『情報セキュリティ市場調査報告書』[46] によれば，サイバーリスク保険の市場規模は，2015 年度に 106 億円程度になると予測される一方，保険の売り行きも伸び悩んでいると報告もある [47]．

2.1 提供されている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 [48], [49], [50], [51] で提供が行われており，補償範囲はほぼ同じである．たとえば，AIU 保険の CyberEdge [51] 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 [52] によれば，海外の動向も同様である．ただし，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．

また，米国では補償範囲をより拡大した保険も登場してきている．米大手保険会社 AIG は，2014 年 4 月にサイバーリスク保険の補償範囲を物損や人体への被害まで拡張することを発表した [53]．IoT（モノのインターネット化）や SCADA へのセキュリティを意識した保険だと考えられる．

2.2 サイバーリスク保険の保険料・支払額

サイバーリスク保険の保険料については，Cyber Data Risk Managers 社のモデルケース [54] が詳しく記載され，100 万ドルを限度額とする補償の場合，収益・業種により 1200 ドル～3.7 万ドルと幅があることが分かる．また，ロイター通信 [55] によれば，サイバー攻撃が多数行われていることから，保険会社は最近保険料を大幅に引き上げたり，補償範囲を限定したりしている傾向にあるとも報道されている．

また，保険の支払額については，NetDiligence 社のレポート “Cyber Liability & Data Breach Insurance Claims” が詳しく分析しており，典型的な保険金支払額は 3 万ドル～26.3 万ドルになると発表している [38]．

2.3 リスク転移手法：「アウトソーシング」との比較

「リスク転移」の他の手法として，ASP・クラウドサービスを利用する「アウトソーシング」があげられる．「アウトソーシング」の一般的メリットとしては，「専門性を有する企業に業務を委託することにより業務やリスク管理の高度化・効率化が期待できる」，「業務運営コストが安価な企業に委託することにより経費を削減できる」などがあげられる [57]．この 1 つとして，セキュリティ対策もあわせて委託できるという考え方である．ただし，アウトソーシングを利用する際には以下の点を考慮する必要がある．

第 1 に，「アウトソーシング」がもたらす利点がサイバーリスク保険とは異なる点があげられる．一般に，セキュリティ投資がもたらす効果として，「攻撃が成功する確率を下げる効果」と「攻撃成功時に被害を最小化・局所化する効果」の 2 つに分類される．サイバーリスク保険は「攻撃成功時の被害を最小化・局所化する効果」を持つ一方，「アウトソーシング」は委託先企業が適切にセキュリティ対策を行っていれば，両方の効果をもたらすと期待される．しかしながら，次の論点で議論するとおり，委託先のセキュリティ対策・情報管理体制がどこまで適切に整備されているか確認する必要がある．また，攻撃者の観点から見れば委託先の「アウトソーシング」企業は様々な企業の情報を保有していることから，非常に効率の良い攻撃対象ともなりうる．そのため，逆に攻撃されるリスクが高まる可能性も想定される．

第 2 に，個人情報・重要情報の管理，セキュリティ対策が委託先で適切になされているか確認する必要がある．NRI セキュアテクノロジーズ社の調査では，「クラウドサービスの選定観点」として 61.8%が「情報管理体制が整備されていること」と回答しており [58]，経済産業省によりセキュリティ対策に関するガイドラインも公開されている [59], [60]．このことから，セキュリティ対策を含めて「アウトソーシング」を行う際には，委託先が適切な専門性・情報管理体制を持っているか見極める必要があり，また継続的に確認を行う必要もある．

第 3 に，委託先で情報漏洩が発生した場合，委託元の情報管理責任が問われる点があげられる．2014 年度に発生し

た教育系企業の事例をあげれば，委託先の内部不正問題ではあるが，委託元の管理責任も問われている事例となる．

以上をふまえると，「アウトソーシング」を行う場合は，上記の 3 点を考慮して利用するか否か判断することが重要になる．なお，最近では「アウトソーシング」先に対する保険 [61] も登場し始めているため，両者を平行するようなケースも今後登場するのではないかと考えられる．

2.4 サイバーリスク保険の前提条件

保険会社がサイバーリスク保険を提供できる前提として，2 つの前提条件が考慮されていると考えられる．

(1) セキュリティ対策が行われていること
(2) 利用される脆弱性は，既知であること

2.4.1 前提 1：セキュリティ対策が行われていること

第 1 の前提として，一定のセキュリティ対策が行われている点があげられる．サイバーリスク保険の性質上，セキュリティ侵害を受けた場合に約束された保険金を支払うことになる．そのため，加入企業が一定以上の割合でセキュリティ侵害を受けると，侵害を受けた全企業が保険金を請求し，保険制度の仕組みが破綻してしまう．

その対策として，一定のセキュリティ対策が行われていること，いい換えればリスクが一定以下の企業のみがサイバーリスク保険に加入できる前提があると考えられる．実際，英エネルギー会社がサイバーリスク保険の加入を希望したにもかかわらず脆弱であることを理由に断られた事例 [56] が報告されている．対策状況や取り扱っている情報を総合的に加味した場合，拒否される事例も存在する．また，セキュリティ対策を支援するため，サイバーリスク保険を提供している東京海上日動火災保険は，2015 年 10 月から「サイバーリスク統合支援サービス」というセキュリティ対策を支援するサービスを始めている [62]．

2.4.2 前提 2：利用される脆弱性は，既知であること

第 2 の前提として，侵害に利用される脆弱性の多くは既知の内容であり，適切な処置が行われていれば情報漏洩の大半は防げることを前提としている．Verizon の調査報告書である「2015 年度データ漏洩/侵害調査報告書」によれば，悪用された脆弱性の 99.9%は，公表されてから 1 年以上経過していることが報告されている [63]．

攻撃者が既知の脆弱性を利用する理由は，経済学的な観点で説明できる．一般に，新しい脆弱性を自分で発見して利用することは非常にコストがかかるため，研究者・攻撃者が発見した脆弱性をパッケージ化した Exploit Kit を購入して利用することが多い．しかしながら，新しい脆弱性を含んでいる Exploit Kit は高額である．その一方，時間が経過するについて脆弱性も対策が進んでいくことから，Exploit Kit の価格も下落してくるため，利用を試みる攻撃者も増えてくると考えられる．Trend Micro の報告書 [64] によれば，有名な Phoenix Expoit Kit の価格は 2011 年には$600 で販売されていたが，2012 年には$250 にまで下落し，2013 年には無償で公開されていることを指摘している．

このことから，保険会社は未知の攻撃が起こることをそこまで懸念しておらず，通常であれば対応可能な脆弱性が，対策されていない場合のみを想定し，商品設計を行っていると考えられる．

3. 有効性評価：定性的観点から

サイバーリスク保険の有効性は，定性的な観点からは 2 つあると考えられる．

(1) セキュリティ対策の推進
(2) インシデント対応の体制強化

3.1 観点 1：セキュリティ対策の推進

第 1 に，サイバーリスク保険に加入することでセキュリティ対策が推進される．前章で示したとおり，保険加入の前提条件として，セキュリティ対策が行われていることがあげられる．実際に海外保険会社の中には，セキュリティ対策のコンサルティングサービスを提供する企業も存在する．また，セキュリティ対策をとることで保険料減額，支払い保険金の上限拡大などのインセンティブを与えるケースも存在する．以上のことから，セキュリティ対策を推進させる強制力を持つと考えられる．和泉ら [65] は，アンケート調査を利用して「サイバーリスク保険」に加入している企業の特徴を分析しており，「リスク分析の実施」，「高度セキュリティ対策の実施傾向」，「人為的リスクの影響度の大きさ」，「従業員数」などの 4 つの組織特徴がサイバーリスク保険の加入に大きく影響を与えると結論付けている．このことからも，高度セキュリティ対策の推進とサイバーリスク保険への加入は相関性があり，有効性があると考えられる．

3.2 観点 2：インシデント対応の体制強化

第 2 に，サイバーリスク保険への加入はインシデント対応の体制強化を推進できると考えられる．サイバーリスク保険へ加入することでセキュリティ事故発生にともなう損害に目を向け，セキュリティ事故発生時に備えどのようなことを準備しなければならないか，検討を進めることができる．その意味で，インシデント対応の体制強化の一役を担っていると推測される．

4. 有効性評価：定量的観点から

本章では，モンテカルロ・シミュレーションを利用して，各組織の状況に合わせた想定被害額と投資の有効性評価を行う．そのため，各組織固有の情報を利用しつつ，推計が難しい部分については統計データを利用して，定量的な有効性評価を試みる．

4.1 定量的評価に必要なデータについて

一般にインシデントに見舞われた企業は，費用の詳細情報を公開することはほとんどない．そのためデータが不足しており，各組織に最適なデータを適用して，分析・数量的な意思決定を行うことが非常に難しいという課題が存在する．公開情報から情報を得る場合は，教育サービス会社の事例 [66] のように有価証券報告書に記載された特別損失計上を読み解く方法しか現時点では方法が存在しない．

米国では情報公開が進んでおり，米証券取引委員会により，上場企業がサイバー攻撃に遭遇した場合の情報公開を求めるガイドラインを公開している [67], [68].

日本の金融庁も，米国の方針を参考にして，有価証券報告書へのサイバーリスク提示義務について検討が始まっている [69]．これにより，投資家に対して透明性のある情報開示とともに，経営者の情報セキュリティリスクへの意識向上が期待される．

4.2 シミュレーション概要

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にくいことから，本提案手法を実施する際には，仮想的なモデル企業を想定して実施する．今回の実験では，2008 年に情報漏洩事故に遭遇した「サウンドハウス社」をモデルとして各種パラメータを決定した．

サウンドハウス社は，音響機器・楽器などを専門に取り扱う専門通信販売会社であり，2008 年に SQL インジェクション攻撃によって，過去に商品購入を行った顧客情報 97,500 人分が流出したことで有名な会社である．顧客情報（氏名・生年月日・メールアドレス・パスワード）だけでなく，一部顧客のクレジットカード情報の漏洩も確認された．この事件の特徴的な点として，インシデントの仔細を公開しており，時系列情報などふだん知ることができない内情も公開していることがあげられる [70], [71]．本実験でも，この情報を活用する．

4.3 前提条件

簡単のため，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」のみを保有すると仮定する．

当該サイトは EC サイトを運営しており，SQL インジェクションを脆弱性として想定する．モデル企業は，自社サイトの脆弱性の存在を把握できていないとし，確率分布に従い脆弱性の存在有無を確定する．脆弱性が存在する場合は，漏洩データ数の決定ロジックにより情報漏洩件数が決定し，被害額を算出する．また，脆弱性が存在しない場合は情報は漏洩しないとする．

4.3.1 初期パラメータ：モデル企業

モデル企業は，「サウンドハウス社」の当時の収益をもとに，**表 2** のとおりに設定する．

表 2 初期パラメータ：モデル企業
Table 2 Initial parameter: Model company.

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

表 3 SQL インジェクション脆弱性が存在する確率
Table 3 The existing probability of SQL injection.

項目	記号	値
存在確率（投資なし）	P_0	16.40%
存在確率（投資あり）	P_1	5.00%

表 4 漏洩データ決定ロジック
Table 4 The decision logic of information leakage.

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 ($= R_{max}$)
平均値	N_{ave}	29,087

4.3.2 初期パラメータ：情報漏洩条件（脆弱性の存在）

情報漏洩条件に関連する初期パラメータとして，**表 3** のようにパラメータを想定した．

前提条件に記載したとおり，企業は自分の Web サイトに SQL インジェクション脆弱性が存在しているか否か把握できていないとする．そのため，Web アプリケーション上に SQL インジェクション脆弱性が存在するか否かについては，確率に従い決定するモデルを定義した．SQL インジェクション脆弱性が存在する確率は，『サイバーセキュリティ傾向分析レポート 2014』[72] 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，SQL インジェクション脆弱性が存在する確率が下がるというモデルを作成した．

4.3.3 初期パラメータ：情報漏洩条件（漏洩件数）

漏洩データ数については，Ponemon Institute 公表データ・モデル企業が保有するデータ件数（表 2）をもとにして，**表 4** のように確率分布（三角分布）に基づいて漏洩データ数を決定するモデルを作成した．

4.3.4 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．2.3 節でも示したとおり，セキュリティ投資の効果には，「攻撃が成功する確率を下げる効果」と「攻撃成功時に被害を最小化・局所化する効果」の 2 つに分類される．

セキュリティ投資 1 は，「セキュリティ診断」である．「セキュリティ診断」とは，セキュリティサービス・プロバイダや脆弱性スキャナと呼ばれるツールを利用し，Web アプリケーションに疑似攻撃を仕掛け，脆弱性を発見する．そのため，「攻撃が成功する確率を下げる効果」を持つと

表 5 投資 1：セキュリティ診断
Table 5 Investment 1: Security assessment.

項目	記号	値
コスト	C_1	4,200,000
効用	P_1	存在確率を 5.0%に低下

表 6 投資 2：サイバーリスク保険
Table 6 Investment 2: Cyber risk insurance.

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

表 7 漏洩被害額：総コスト
Table 7 Total cost.

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）	$C_{qa-total}$

考えられる．ただし，品質・実施スコープにより，脆弱性の見逃しが発生することも考慮する必要がある．今回のシミュレーションでは，**表 5** にあるとおり，投資コスト 420 万円に対し，「SQL インジェクション脆弱性が存在する確率」を 5.0%まで低下させると仮定した（発見された脆弱性は修正することを前提としている）．金額についてはサウンドハウス社の事例を参考にし，また「セキュリティ診断」の投資効果については Web アプリケーション用スキャナにおける SQL インジェクション脆弱性の検知率が 95%前後であることを根拠 [73] に，診断実施後も脆弱性が存在すると想定した．

セキュリティ投資 2 は，「サイバーリスク保険」である．「サイバーリスク保険」とは，保険料として一定額を支払う代わりに，情報漏洩時に対応コスト・被害コストを保険金として受け取ることができるサービスで，「攻撃成功時に被害を最小化・局所化する効果」を持つと考えられる．前述のとおり，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分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」[48] のサンプル例を採用した．保険の仔細を**表 6** に示す．

4.3.5 初期パラメータ：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 4 つの値の合計で構成される（**表 7** 参照のこと）．

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

今回のモデルでは，情報漏洩事故で新たに発生するコストは「事故対応コスト」，「顧客対応コスト（お詫び）」，「顧客対応コスト（QA 対応）」に分類される．

表 8 漏洩被害額：事故対応コスト
Table 8 Incident response cost.

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
サーバ交換費用	34,000,000
合計 ($C_{ir-total}$)	62,800,000

表 9 漏洩被害額：顧客対応コスト（お詫び）
Table 9 The cost for compensation.

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	表 4 に記載済み
お詫び金単価	C_{cp}	750 円/人

4.3.6 初期パラメータ：漏洩被害額（事故対応コスト）

「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をもとに**表 8** のように算出し，固定値とした．

4.3.7 初期パラメータ：漏洩被害額（顧客対応コスト）

「顧客対応コスト」とは，お詫び金やそれにともなう事務費用，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（お詫び金）」と，顧客問合せによる「顧客対応コスト（QA 対応）」を想定して，**表 9** のように定義した．

「お詫び金」については，事例に従い 1 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．

問合せによる「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%の人から問合せが行われているため，その値を参考とした．また，1 人あたりの対応コストについては，平均 1 時間かかると仮定し，コールセンタの自給をもとに平均 1000 円程度かかると想定し，以下の式（**表 10**）を想定した．

4.4 シミュレーション 実施内容

上記の前提をもとにした，フローチャートを**図 1** に示す．

まず，表 3 で提示した確率に従い，SQL インジェクションの有無を決定する．もし，SQL インジェクションが存在した場合，攻撃を受けたとして表 4 で提示したロジックに従いデータ漏洩件数を決定する．最後のステップとして，

表 10 漏洩被害額：顧客対応コスト（QA 対応）
Table 10 The cost for inquiry.

項目	記号	値
合計	$C_{qa-total}$	$N_i * P_{qa} * C_{qa}$
漏洩データ数	N_i	表 4 に記載済み
問合せ率	P_{qa}	5.0%
QA 対応単価	C_{qa}	1,000 円/人

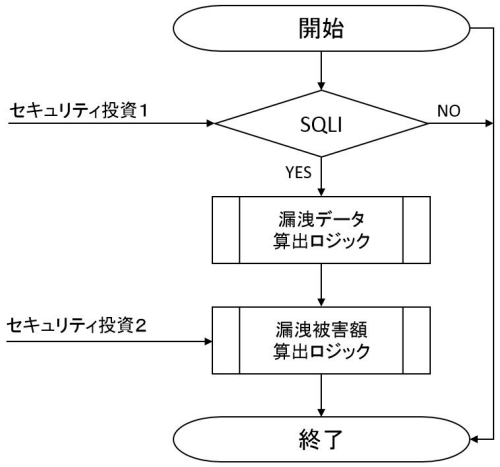

図 1 シミュレーションフロー
Fig. 1 The simulation flow.

表 11 シミュレーション・シナリオ
Table 11 The simulation scenarios.

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

表 7〜表 10 に従い被害額を決定する．ただし，セキュリティ投資 2（サイバーリスク保険）を導入している場合は，表 6 に従い，被害額に対して保険の支払い限度額まで補填するモデルを採用する．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漏洩被害額（総コスト）が変わるのか分析するため，**表 11** にあるとおりの 4 種類のシナリオを想定して分析を行った．

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実施した．**表 12** に結果を示す．

コスト（最大値）・コスト（最小値）は各シナリオごとに実施した 100 万回の試行の中の最大値・最小値を記載している．そのため，コスト（最小値）は，脆弱性が存在せずにセキュリティ投資コストの合計値となる．また，コスト（最大値）は当該シナリオの中で最もコストがかかったケースを意味する．コスト（中央値）・コスト（平均値）は 100 万回の試行時の中央値・平均値を意味する．なお，CASE1

表 12 結果一覧（単位：件，百万円）
Table 12 The analysis result (Unit: Case, million yen).

	CASE1	CASE 2	CASE 3	CASE 4
SQLI 存在確率	16.40%	5.00%	16.40%	5.00%
サイバー保険	なし	なし	あり	あり
攻撃成功件数	163,909	50,282	165,068	50,157
コスト（最小値）	0.000	4.200	0.500	4.700
コスト（最大値）	302.244	305.796	172.643	176.822
コスト（平均値）	24.831	11.808	8.856	7.232
コスト（中央値）	0.000	4.200	0.500	4.700
平均相対コスト	1	0.476	0.357	0.291
ROSI	-	3.101	31.950	3.744

と CASE2，CASE3 と CASE4 のコスト（最大値）が類似している理由は，比較ケースの差分であるセキュリティ投資 1（セキュリティ診断）が「攻撃が成功する確率を下げる効果」を持つが，攻撃成功後の情報漏洩件数に影響を及ぼさないためである．

セキュリティ対策を行わずにサイバーリスク保険に加入することは考えにくいため，CASE1（セキュリティ投資をしていない場合），CASE2（セキュリティ診断を実施した場合），CASE4（セキュリティ診断を実施し，かつサイバーリスク保険に加入している場合）の 3 種類が重要と考えられる．

5.1 投資制約条件

CASE1（投資なし）の平均被害コスト（2483 万円）は，その定義より本モデルの期待値（期待損害額）と見なすことができ，投資の制約条件と考えることができる．本モデルで想定している状況では，約 2500 万円以下の投資が妥当だと考えられ，それ以上に投資をすることは過剰投資になってしまうと判断できる．

5.2 平均相対コスト

平均相対コストとは，CASE1（投資なし）の平均コストを 1 とした場合の相対値である．セキュリティ診断のみ実施した CASE2 が 52.4%のコスト削減，2 つの投資戦略を同時にとった CASE4 が 70.9%のコスト削減に寄与していることが分かる．

5.3 ROSI：Return On Security Investment

ROSI（Return On Security Investment）とは，セキュリティ投資がコストの平均値減少にどれぐらい寄与しているかを示す比率である．実際には，セキュリティ診断サービスを受けたうえで保険に入ることが一般的だと想定すると，2 つの投資戦略を同時にとった CASE4 が約 4 倍の効用をもたらすことが分かる．セキュリティ診断の内容や保険の条件にも大きく依存するが，ROSI として高い効用をもたらすセキュリティ管理施策であると判断できる．

表 13 結果一覧（単位：件，百万円）
Table 13 The analysis result (Unit: Case, million yen).

	CASE1	CASE 2	CASE 3	CASE 4
SQLI 存在確率	16.40%	5.00%	16.40%	5.00%
サイバー保険	なし	なし	あり	あり
攻撃成功件数	163,909	50,282	165,068	50,157
コスト（最小値）	64.771	69.202	33.300	37.500
コスト（最大値）	302.244	305.796	172.643	176.822
コスト（平均値）	151.492	155.512	51.121	55.182
コスト（中央値）	142.388	146.409	33.300	37.500

表 14 保険カバー率・ROSI
Table 14 Insurance coverage ratio · ROSI.

保険カバー率	$(CASE2 - CASE4)/CASE2$	64.50%
保険 ROSI	$(CASE2 - CASE4)/C_{inv}$	200.659

5.4 サイバーリスク保険の有効性評価

サイバーリスク保険の有効性は，攻撃が成功したケースだけを抽出して，セキュリティ投資 2（サイバーリスク保険）の有無を比較することで評価可能である．**表 13** に攻撃に成功した事例を抽出した結果を示す．

サイバーリスク保険有無による，比較結果を**表 14** に示す．

保険カバー率とは，本来の被害額に対して保険がカバーしたコストの割合と定義する．今回の事例では，CASE2（セキュリティ診断あり・サイバーリスク保険なし）と CASE4（セキュリティ診断あり・サイバーリスク保険あり）の差分が「保険で支払われる平均金額」であると考えられる．また CASE2 は，「サイバーリスク保険がない場合の実質的被害額」と考えられる．そのため，$(CASE2 - CASE4)/CASE2$ という算出式が成立する．

今回のシミュレーションでは，1 年間の保険の投資と限定すれば，攻撃が必ず成功する場合は約 65%の保険カバー率となり ROSI は約 200 倍であることが分かる．各種パラメータの条件には依存するが，非常に効果の高いセキュリティ投資と考えられる．

5.5 現実の事例との比較

シミュレーションで得られたサイバーリスク保険の有効性評価の妥当性を検証するため，サイバーリスク保険の導入が進んでいる米国の事例を示す．

5.5.1 事例 1：ターゲット社

ターゲット社は，2013 年 12 月に情報漏洩に見舞われ，POS マルウェアで 4000 万件のカード情報，7000 万件の個人情報が漏洩した．2014 年年度第四半期の報告によると，累積 2.52 億ドルの対策コストを計上しており，また 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．そのため，今後も他の集団訴訟について，支払いをしていくことになると思われるが，2014 年年度第四半期時点において，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 [74]．これより，対策コストの約 35.7%が保険によりカバーされていると算出できる．

5.5.2 事例 2：ホーム・デポ社

ホーム・デポ社は，2014 年 9 月に 5600 万枚のカード情報が流出したことで有名になった会社である．Bloomberg Business の報道 [75] によれば，対策費は 6200 万ドルになり，2700 万ドルは保険で払い戻される見通しとされ，対策コストの 43.5%が保険でカバーされていると知られている．

5.5.3 事例 3：ソニーピクチャーズ社

ソニーピクチャーズ社は，2014 年 11 月にハッキング攻撃を受け，未公開画像や従業員・有名ハリウッド女優の個人情報などが漏洩したと報じられている．その想定被害額は 1 億ドルにのぼるとされているが [76]，本ケースでは保険により全額カバーされていると報じられている [77]．

ただし，ソニー・グループは保険金の請求が裁判に発展するケースを過去に経験している．2011 年に発生した PlayStation Network の情報漏洩において，米保険会社チューリッヒが米裁判所に対して，「保険金の支払いが法的に不要である」ことを認めるよう，裁判を起こしている [78]．このことは，保険の補償範囲について正確に把握すべきという教訓的事例だといえる．

6. まとめと今後の課題

本論文では，セキュリティ管理の重要なテーマである費用便益分析とサイバーリスク保険の現状について様々な観点から分析を行い，サイバーリスク保険の有効性を示すことができた．今後の課題として，以下 3 点があげられる．

第 1 に，保険の支払い期間を考慮した「長期モデル」の構築があげられる．サイバーリスク保険も他の保険と同様，年 1 回の保険料の更新をしていくことが一般的となる．本論文では，1 年間での評価が行われているが，サイバーリスク保険の有効性を議論するうえでインシデントの発生確率を考慮した長期期間における投資対効果の分析が必要だと考えられる．ただし，4.1 節にも記載したとおり，「情報漏洩などのインシデントの発生確率」などの統計データについては十分なデータが存在しない，あるいは推定値にまだ議論が分かれることから，それらをふまえて「長期モデル」を確立することが今後の課題だと考える．

第 2 に，複雑なケースを分析できるように「モデルの精緻化」をすることがあげられる．今回のモデルでは，保険支払限度額までは全額払うことを想定したモデルとしているが，現実には全額支払われないケースも存在すると考えられる．それをふまえ，保険カバー率と保険の支払い額などの関係性などについて論じる必要があると考えられる．

第 3 に，企業がサイバーリスク保険への加入にともなう行動を分析し，加入を阻害する要因を分析することがあげられる．また，被害額を明確化するために，個人情報の価

値推定についても取り組む必要があると考えている．これらの研究により，各組織がより簡単にセキュリティ管理に取り組めるように貢献したいと考えている．

謝辞 原稿を注意深くお読みいただき，適切な助言をいただいたことに対して，2 人の匿名査読者および編集委員に感謝する．

参考文献

[1] USA TODAY: Massive breach at health care company Anthem Inc., available from ⟨http://usat.ly/1D0uR3l⟩ (accessed 2015-02-05).

[2] USA TODAY: Premera says data breach affects up to 11M people, available from ⟨http://usat.ly/1MHMOah⟩ (accessed 2015-03-17).

[3] USA TODAY: 1.1 million CareFirst members in D.C.-area potentially breached, available from ⟨http://usat.ly/1HhSJOp⟩ (accessed 2015-05-20).

[4] USA TODAY: Cyber breach hits 10 million Excellus healthcare customers, available from ⟨http://usat.ly/1UJWlQq⟩ (accessed 2015-09-10).

[5] Forbes: Sony Pictures Hacked And Blackmailed, available from ⟨http://onforb.es/1uzsdJx⟩ (accessed 2014-11-24).

[6] The Wall Street Journal: OPM Breach Was Enormous, FBI Director Says, available from ⟨http://on.wsj.com/1eHdKev⟩ (accessed 2015-07-08).

[7] The Wall Street Journal: Breach at IRS Exposes Tax Returns, available from ⟨http://on.wsj.com/1J3nkUf⟩ (accessed 2015-05-26).

[8] 日本経済新聞：年金機構 125 万件流出　職員，ウイルスメール開封，入手先 ⟨http://www.nikkei.com/article/DGXLASDG01HCF_R00C15A6MM8000/⟩（参照 2015-06-01）．

[9] Forbes JAPAN：不倫 SNS 流出事件　“該当者チェックサイト”も出現，入手先 ⟨http://forbesjapan.com/translation/post_7851.html⟩（参照 2015-08-26）．

[10] National Institute of Standards and Technology: NIST Cybersecurity Framework, available from ⟨http://www.nist.gov/cyberframework/⟩.

[11] SANS Institute: SANS Critical Security Control, available from ⟨https://www.sans.org/critical-security-controls/⟩.

[12] 警察庁：不正アクセス行為対策等の実態調査 調査報告書，入手先 ⟨http://www.npa.go.jp/cyber/research/h26/h26countermeasures.pdf⟩（参照 2014-02）．

[13] World Economic Forum: Global Risks 2015 10th Edition, available from ⟨http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf⟩ (accessed 2015-01).

[14] CFO: Banks With Weak Cybersecurity Could Be Downgraded: S&P, available from ⟨http://ww2.cfo.com/cyber-security-technology/2015/09/banks-weak-cybersecurity-downgraded-sp/⟩ (accessed 2015-09-29).

[15] Gordon, L.A. and Loeb, M.P.: The Economics of Information Security Investment, *ACM Trans. Information and System Security*, Vol.5, No.4, pp.438–457 (2002).

[16] 中村逸一，兵藤敏之，曽我正和，水野忠則，西垣正勝：セキュリティ対策選定の実用的な一手法の提案とその評価，情報処理学会論文誌，Vol.45, No.8, pp.2022–2033 (2004).

[17] 西垣正勝，臼井佑真，山本　匠，間形文彦，勅使河原可海，佐々木良一：賠償リスクを考慮した情報セキュリティ対策選定方式の提案と評価，情報処理学会論文誌，Vol.52, No.3, pp.1173–1184 (2011).

[18] 情報処理振興事業協会 セキュリティセンター：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，入手先 ⟨http://www.ipa.go.jp/security/fy13/report/incident_survey/incident_survey.pdf⟩（参照 2002-06）．

[19] 情報処理振興事業協会 セキュリティセンター：「被害額算出モデル」報告書，入手先 ⟨http://www.ipa.go.jp/security/fy14/reports/current/2002-calc-model.pdf⟩（参照 2003-03）．

[20] NPO 日本ネットワークセキュリティ協会：2002 年度情報セキュリティインシデントに関する調査報告書—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，入手先 ⟨http://www.jnsa.org/houkoku2002/incidentreport2002_1.pdf⟩（参照 2003-03-31）．

[21] NPO 日本ネットワークセキュリティ協会：2002 年度情報セキュリティインシデントに関する調査報告書—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），入手先 ⟨http://www.jnsa.org/houkoku2002/incidentreport2002_2.pdf⟩（参照 2003-03-31）．

[22] European Network and Information Security Agency: Introduction to Return on Security Investment (2012), available from ⟨https://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment/at_download/fullReport⟩.

[23] The Economist Intelligence Unit Ltd: CyberTab, available from ⟨https://cybertab.boozallen.com/⟩

[24] Yoo, Y., Gee, S., Song, H., Chung, K. and Lim, J.: Estimating Economic Damages from Internet Incidents (Korean), *Informatization policy* (2008).

[25] Kang, H., Park, K.C., Park, W.H. and Kuk, K.H.: A Study on Model for Assessment of Economic Damages Due to Cyber Terror (Korean), *Jouranl of Information and Security* (2009).

[26] Yoo, H.：情報保護の侵害事故発生による被害額算出モデル（Korean），The Korean Operations Research and Management Science Society (online) (2010)，入手先 ⟨http://www.cimerr.net/vod/cyber2010_spring/B10-5/B10-5/B10-5.pdf⟩.

[27] Han, C.H., Chai, S.W., Yoo, B.J., Ahn, D.H. and Park, D.H.: A Quantitative Assessment Model of Private Information Breach, *The Journal of Society for e-Business Studies* (2011).

[28] 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，入手先 ⟨http://japanese.joins.com/article/903/175903.html⟩（参照 2013-09-08）．

[29] 石川朝久，櫻井幸一：個人情報漏洩補償に関する一検討，*Computer Security Symposium 2014* (2014).

[30] Imperva Incapsula: Incapsula Survey: What DDoS Attacks Really Cost Businesses (2014), available from ⟨https://www.incapsula.com/blog/ddos-impact-cost-of-ddos-attack.html⟩.

[31] Ponemon Institute: 2015 Cost of Data Breach Study (2015), available from ⟨http://www-03.ibm.com/security/data-breach/⟩.

[32] Conrad, J.R.: Analyzing the Risks of Information Security Investments with Monte-Carlo Simulations, *IEEE* (2005).

[33] Burtescu, E.: Decision Assistance in Risk Assessment Monte Carlo Simulations, *Informatica Economica*, Vol.16, No.4 (2012).

[34] Lyon, D.: Modeling Security Investments With Monte Carlo Simulations, *SANS Institute: Reading Room* (2014).

[35] Bohme, R. and Schwartz, G.: Modeling Cyber-Insurance: Towards A Unifying Framework, *Workshop*

on the Economics of Information Security (2010).
[36] Naghizadeh, P. and Liu, M.: Voluntary Participation in Cyber-insurance Markets, *Workshop on the Economics of Information Security* (2014).
[37] 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，入手先 ⟨http://jp.reuters.com/article/2014/07/15/idJPL4N0PQ19O20140715⟩（参照 2014-07-15）.
[38] Net Diligence: 2015 Cyber Claims Study (2015), available from ⟨http://www.netdiligence.com/downloads/NetDiligence_2015_Cyber_Claims_Study_093015.pdf⟩.
[39] Marsh & McLennan Companies: A Cyber Security: A Call to Action, available from ⟨http://chertoffgroup.com/cms-assets/documents/196659-211678.a-cybersecurity-call-to-action.pdf⟩ (accessed 2014-11).
[40] Insurance Information Institute: Cyber Risk: Threat and opportunity, available from ⟨http://www.iii.org/sites/default/files/docs/pdf/cyber_risk_wp_final_102015.pdf⟩ (accessed 2014-10-21).
[41] 石川朝久，櫻井幸一：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，*Computer Security Symposium 2015* (2015).
[42] Latham & Watkins: Cyber Insurance: A Last Line of Defense When Technology Fails, available from ⟨http://www.lw.com/thoughtLeadership/lw-cybersecurity-insurance-policy-coverage⟩ (accessed 2014-04-15).
[43] プライスウォーターハウスクーパース社：相互につながった世界におけるサイバーリスクマネジメント グローバル情報セキュリティ調査 2015 (2015)，入手先 ⟨https://www.pwc.com/jp/ja/advisory/research-insights-report/assets/pdf/information-security-survey2015.pdf⟩.
[44] ロイター通信：Insurers struggle to get grip on burgeoning cyber risk market，入手先 ⟨http://www.reuters.com/article/2014/07/14/us-insurance-cybersecurity-idUSKBN0FJ0B820140714⟩（参照 2014-07-14）.
[45] 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，入手先 ⟨https://www.ipa.go.jp/files/000045629.pdf⟩（参照 2015-06-30）.
[46] 日本ネットワークセキュリティ協会：2014 年度 情報セキュリティ市場調査報告書，入手先 ⟨http://www.jnsa.org/result/2015/surv_mrk/index.html⟩（参照 2015-06-04）.
[47] IT Media：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，入手先 ⟨http://itpro.nikkeibp.co.jp/atcl/column/14/346926/031600197/⟩（参照 2014-03-18）.
[48] 東京海上日動：個人情報漏えい保険，入手先 ⟨http://www.tokiomarine-nichido.co.jp/hojin/baiseki/roei/⟩.
[49] 三井住友海上：情報漏えいプロテクター，入手先 ⟨http://www.ms-ins.com/business/indemnity/pd-protector/⟩.
[50] 損保ジャパン日本興亜：個人情報取扱事業者保険，入手先 ⟨http://www.sjnk.co.jp/hinsurance/risk/liability/information/⟩.
[51] AIU 保険：CyberEdge，入手先 ⟨http://www.aiu.co.jp/business/product/liability/cyberedge/index.htm⟩.
[52] 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，入手先 ⟨http://www.fsa.go.jp/common/about/research/20150706-4.html⟩.
[53] CNN Money: AIG cyber insurance covers bodily harm, available from ⟨http://money.cnn.com/2014/04/23/technology/security/aig-cybersecurity-insurance/⟩ (accessed 2014-04-23).
[54] Cyber Data Risk Managers: How much does Cyber/Data Breach Insurance Cost?, available from ⟨http://databreachinsurancequote.com/cyber-insurance/⟩ (accessed 2015-11-06).
[55] Reuters: Insight – Cyber insurance premiums rocket after high-profile attacks, available from ⟨http://uk.reuters.com/article/2015/10/12/uk-cybersecurity-insurance-insight-idUKKCN0S609S20151012⟩ (accessed 2015-10-12).
[56] BBC: Energy firm cyber-defence is 'too weak', insurers say, available from ⟨http://www.bbc.com/news/technology-26358042⟩ (accessed 2014-02-27).
[57] 日本銀行：金融機関業務のアウトソーシングに際してのリスク管理，available from ⟨https://www.boj.or.jp/research/brp/ron_2001/fsk0104b.htm/⟩ (accessed 2011-04-17).
[58] NRI セキュアテクノロジーズ株式会社：企業における情報セキュリティ実態調査 2013，入手先 ⟨http://www.nri-secure.co.jp/security/report/2013/index.html⟩（参照 2014-01-17）.
[59] 経済産業省：クラウドサービス利用のための情報セキュリティマネジメントガイドライン，入手先 ⟨http://www.meti.go.jp/press/2013/03/20140314004/20140314004-2.pdf⟩（参照 2014-03-14）.
[60] 経済産業省：アウトソーシングに関する情報セキュリティ対策ガイダンス，入手先 ⟨http://www.meti.go.jp/policy/netsecurity/docs/secgov/2009_OutsourcingJohoSecurityTaisakuGuidance.pdf⟩（参照 2009-06-01）.
[61] 東京海上日動火災保険株式会社：AWS ユーザー向け専用商品の販売開始について，入手先 ⟨http://www.tokiomarine-nichido.co.jp/company/release/pdf/151229_01.pdf⟩（参照 2015-12-29）.
[62] 東京海上日動火災保険株式会社：「サイバーリスク総合支援サービス」の提供開始について，入手先 ⟨http://www.tokiomarine-nichido.co.jp/company/release/pdf/150810_01.pdf⟩（参照 2015-08-10）.
[63] ベライゾンジャパン：2015 年度データ漏洩/侵害調査報告書，入手先 ⟨http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015_jp_xg.pdf⟩（参照 2015-07-15）.
[64] Trend Micro: Cybercriminal Underground Economy Series: Russian Underground Revisited, available from ⟨http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf⟩ (accessed 2014-04-28).
[65] 和泉あゆみ，加藤慎也，小松文子，竹村敏彦：サイバーリスクに関する実証分析，*Computer Security Symposium 2015* (2015).
[66] 株式会社ベネッセホールディングス：2015 年 3 月期 (第 61 期) 有価証券報告書，入手先 ⟨http://blog.benesse.ne.jp/bh/ja/ir_library/yuho/m/2015/06/30/uploads/pdf/yuho_61_fin.pdf⟩（参照 2015-06-21）.
[67] U.S. Securities and Exchanage Commission: CF Disclosure Guidance: Topic No. 2 CyberSecurity, available from ⟨https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm⟩ (accessed 2011-10-13).
[68] IT Media ニュース：米証券取引委員会，上場企業にサイバー攻撃の情報公開を求めるガイダンス発表，入手先 ⟨http://www.itmedia.co.jp/news/articles/1110/17/news015.html⟩（参照 2011-10-17）.
[69] 情報セキュリティ政策会議：サイバーセキュリティ 2014，入手先 ⟨http://www.nisc.go.jp/active/kihon/pdf/cs2014.pdf⟩（参照 2014-07-10）.
[70] 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，入手先 ⟨http://internet.

watch.impress.co.jp/cda/news/2008/06/18/19989.html〉（参照 2008-06-18）.
[71] 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，入手先 〈https://www.soundhouse.co.jp/company/news/pdf/20080418.pdf〉（参照 2008-04-18）.
[72] 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，入手先 〈http://www.nri-secure.co.jp/news/2014/0820_report.html〉（参照 2014-08-20）.
[73] Chen, S.: The Web Application Vulnerability Scanners Benchmark, available from 〈http://sectooladdict.blogspot.jp/2014/02/wavsep-web-application-scanner.html〉 (accessed 2014-02-05).
[74] Bank Info Security, Target Breach Costs: $162 Million, available from 〈http://www.bankinfosecurity.com/target-breach-costs-162-million-a-7951〉 (accessed 2015-02-25).
[75] Bloomberg, Home Depot Hacked After Months of Security Warnings, available from 〈http://www.bloomberg.com/bw/articles/2014-09-18/home-depot-hacked-wide-open〉 (accessed 2014-09-18).
[76] The Huffington Post Japan：ソニー・ピクチャーズへのサイバー攻撃，被害額は 120 億円にも，入手先 〈http://www.huffingtonpost.jp/2014/12/10/sony-pictures-cyber-attack_n_6305614.html〉（参照 2014-12-11）.
[77] Reuters：ソニー・ピクチャーズ，サイバー攻撃被害は保険でカバー，入手先 〈http://jp.reuters.com/article/2015/01/09/spe-insurance-idJPKBN0KI02U20150109〉（参照 2015-01-09）.
[78] Reuters：ソニー情報流出問題，保険会社が米裁判所に支払い不要の宣告求める，入手先 〈http://jp.reuters.com/article/2011/07/22/idJPJAPAN-22330520110722〉（参照 2011-07-22）.

石川 朝久 （正会員）

2009 年国際基督教大学教養学部理学科卒業．同年大手シンクタンクに入社．情報セキュリティに関する技術コンサルテーション，情報セキュリティ監査，セキュリティ研修講師等に従事．2015 年九州大学大学院システム情報科学研究院に入学．情報セキュリティの研究に従事．保有資格として，CISSP，CISA，CISM，QSA，公認不正検査士，GIAC（GPEN，GWAPT，GXPN，GWEB，GSNA，GREM，GCIH）等がある．

櫻井 幸一 （正会員）

1988 年九州大学大学院工学研究科応用物理学専攻修士課程修了．同年三菱電機（株）入社．現在，九州大学大学院システム情報科学研究院情報学部門教授．2004 年より九州システム情報技術研究所第 2 研究室（現，九州先端科学技術研究所・情報セキュリティ研究室）室長兼任．博士（工学）．2000 年情報処理学会坂井特別記念賞．2000 年，2004 年情報処理学会論文賞．2005 年第 1 回 IPA 賞受賞．2012 年第 26 回独創性を拓く先端技術大賞経済産業大臣賞（企業・産学部門最優秀賞）受賞．日本数学会，応用数理学会，電子情報通信学会，IACR，ACM，IEEE 各会員．