情報処理学会論文誌 Vol.61 No.12 1781–1791 (Dec. 2020)

セキュリティマネジメントによるサイバーインシデントリスク削減の評価

山田 道洋[1] 池上 和輝[1] 菊池 浩明[2,a)] 乾 孝治[3]

受付日 2020年3月11日, 採録日 2020年9月10日

概要：近年，企業における内部不正や外部からの攻撃による個人情報漏洩事件などが増加している．これらに対して，情報セキュリティマネージメントや最高情報責任者（CIO）の設置，セキュリティ監査の実施などにより企業の社会的責任を高めることが求められているが，東洋経済新報社が調査した5年間のCSRデータを解析したところ，経営マネジメント方策の実施によってインシデント件数がむしろ増加していることが明らかになった．そこで，本稿では，企業の業種や規模などの交絡因子の影響を考慮して，マネジメント方策の実施によるサイバーインシデントの削減効果を評価する．

キーワード：セキュリティマネジメント，情報漏洩，ISMS，CIO

Evaluation on Cyber Incident Risk Reduced by Security Management

Michihiro Yamada[1] Kazuki Ikegami[1] Hiroaki Kikuchi[2,a)] Koji Inui[3]

Received: March 11, 2020, Accepted: September 10, 2020

Abstract: With increasing risk of cyber incident and privacy breaches, enterprises are required to introduce information security managements such as the certification of an information security management system, periodic security auditing, and creating dedicated positions such as a Chief Information Officer (CIO). However, our analysis of five-year Toyo Keizai Corporate Social Responsibility (CSR) survey reveals a negative effect for most security practices. In this paper, by regarding confounding factors such as business style and corporate scale, we evaluate the adjusted effect of security practices in reduction of cyber incident risk.

Keywords: security management, data breach, ISMS, CIO

1. はじめに

近年，企業におけるIT技術や個人情報などの利活用が広がっている．それにともない，不正アクセスや内部犯行などによる個人情報の流出事件が増加している．2014年にはベネッセコーポレーション社の業務委託先の元社員が与えられていた権限を利用し，約3,504万件の個人情報を不正に持ち出し名簿業者3社へ売却していた[1]．また，幻冬舎は運営するウェブサイトへの不正アクセスにより，最大で93,014名のメールアドレスやユーザIDが流出した可能性を2018年に報告している[2]．

これらのセキュリティ上の脅威に対して，企業は情報セキュリティマネージメントISMS認証や最高情報責任者（CIO）の設置，セキュリティ監査の実施などの各種経営マネジメント方策を実施し，個人情報取扱事業者としての社会的責任を果たすことが求められている．

そこで我々は，2018年の株式会社東洋経済新報社の社会

[1] 明治大学大学院先端数理科学研究科
Graduate School of Advanced Mathematical Sciences, Meiji University, Nakano, Tokyo 164–8525, Japan
[2] 明治大学総合数理学部先端メディアサイエンス学科
Department of Frontier Media Science, School of Interdisciplinary Mathematical Sciences, Meiji University, Nakano, Tokyo 164–8525, Japan
[3] 明治大学総合数理学部現象数理学科
Department of Mathematical Sciences Based on Modeling and Analysis, School of Interdisciplinary Mathematical Sciences, Meiji University, Nakano, Tokyo 164–8525, Japan
[a)] kikn@meiji.ac.jp

本研究の初期稿はコンピュータセキュリティシンポジウムCSS 2018にて発表している．

的責任投資 Corporate Social Responsibility（CSR）データベース [3] に注目する．本データベースは，CIO 設置の有無や ISMS の取得などの全 840 項目についての国内企業 1,413 社の 5 年間の情報を格納している．本データベースを，国内の情報漏洩インシデントをカバーしている JNSA データセット [8] と Security Next のインシデント情報と照合することで，これらの経営マネジメント方策がインシデントを削減する効果を分析する．1,413 の企業群に内在する種々の違い，業種，規模，観測年（景気などの影響）などを交絡因子（confounding factor）と見なし，それらがリスクに見かけ上の誤った差をもたらしたという仮説を立てる．こうして，企業の業種などについてデータを分析することで，マネジメント方策の実施によるインシデントの件数の統計量を明らかにし，マネジメント方策の効果を検討する．

マネジメント方策などの条件により，サイバーインシデントのリスクがどのように影響するかを明らかにすることには，サイバー保険や経営などの観点から大きな需要がある [6], [11], [12]．たとえば，江口らは ISO 27001 認証の有無によるインシデント事例の比較分析を行っている [19]．小梶らは，金融機関におけるリスクアセスメントの動向について調査をしている [13]．これらに対して，近年，従来疫学分野で用いられていた相対リスク [17] などの概念を導入して，サイバーインシデントの発生リスクに対する効果を評価する試みがさかんになってきている．Romanosky は，Advisen [10] の全米のインシデントデータを用いたロジスティック回帰によるコスト予測を行っている [7]．Eling らは，一般化パレート分布（generalized Pareto distribution）による新たなモデルを提案している [21]．Sen らは，インシデント間隔が負の二項分布に従うことを利用して，業種ごとのリスクの大きさを定量化している [20]．各種の疫学的な概念や確率分布を導入する研究が多く試みられている [14], [15], [23]．このような潮流の中で，本研究では，マネジメント方策を説明変数としてインシデント発生リスクを説明する点が新規的であり，多重ロジスティックモデルを適用してインシデント発生を定量化する．

2. データ

2.1 インシデントデータセット

本研究では，後述する JNSA データセットと Security Next データセットの 2 つをインシデントデータセットとして用いる．インシデントデータセットの統計量を**表 1** に示す．

2.1.1 JNSA データセット

日本ネットワークセキュリティ協会（Japan Network Security Assosiation, JNSA）セキュリティ被害調査ワーキンググループは，2002 年より新聞やインターネットニュースなどで報道されたインシデントの記事，組織からリリースされたインシデントに関連した文書の情報を集計し，漏洩した組織の業種，漏洩人数，漏洩経路などの分類・評価を行っている．インシデントデータベース [8] には，日付，情報管理・保有責任者（企業名），業種名，社会的貢献度，被害人数，漏洩情報区分，漏洩原因，漏洩経路，事後対応姿勢，漏洩情報（氏名，住所，電話番号，生年月日など）といった事件の特性を記録している．

表 1 インシデントデータセットの統計量
Table 1 Statistics of incident datasets.

データセット	期間	インシデント数	インシデントを起こした企業数
JNSA	2005–2017	15,569	8,853
SecurityNext	2013–2018	174	121

表 2 CSR データセットの統計量
Table 2 Statistics of CSR dataset.

年	企業数（上場）	平均社員数	総質問項目数	方策についての質問数
2013	1,210（1,157）	2,672	753	185
2014	1,305（1,259）	2,582	764	186
2015	1,325（1,284）	2,646	811	193
2016	1,408（1,364）	2,579	832	197
2017	1,413（1,370）	2,627	840	207

2.1.2 Security Next データセット

ニュースガイア株式会社が運営するウェブサイト Security Next [*1] は，脆弱性やインシデントについてのニュースを掲載している．

JNSA のインシデントデータベースでカバーされている企業はニュースになりやすい大企業や大都市の自治体に偏っており，CSR データセットと共通の企業数は非常に少ない．また，外部に公開されない限定的なインシデントも含まれていない．CSR データセットと照合するインシデントデータセットとしては不十分であった．そこで本研究では，2013 年から 2017 年に Security Next ウェブサイトで公開されているインシデントのデータで補完することとした．補完の十分性については，3.4.1 項で述べる．本サイトで，情報漏洩事件・事故に分類された記事のうち，後述する CSR データベースに記載されている企業についての記事の内容を精査し，企業名や流出経路などの情報を収集した．

2.2 東洋経済 CSR データ

株式会社東洋経済新報社は，上場企業全社および主要未上場企業に調査票を送付し，その回答から社会的責任投資 CSR データベース [3] を作成している．データセットは従業員数や平均年間給与，管理職の男女比率などの雇用人材活用編，環境担当役員の有無や温室効果ガス排出量などの

[*1] http://www.security-next.com/

表 3 CSR データセットの回答内容の集計例
Table 3 Example classification of answers into Yes or No in CSR dataset.

質問項目	Yes	No
CSR 専任部署の有無	1. 専任部署あり，2. 兼任部署で担当	3. なし，4. その他
情報システムのセキュリティに関する内部監査	1. 定期的に実施，2. 不定期に実施	3. なし，4. その他

表 4 CSR データセットの質問項目の一部
Table 4 List of questions in CSR dataset.

項目 ID	質問項目	略称
C122	内部告発者の権利保護に関する規定制定	告発保護
C139	内部統制委員会の設置	内統委員
C147	CIO（最高情報責任者）の有無	CIO
C150	CFO（最高財務責任者）の有無	CFO
C161	プライバシー・ポリシーの制定	PP
C153	情報システムに関するセキュリティポリシー	SP
C155	情報システムのセキュリティに関する内部監査	内部監査
C157	情報システムのセキュリティに関する外部監査	外部監査
C159	ISMS（情報セキュリティマネジメントシステム）認証	ISMS
C120	内部告発窓口（社内）の設置	内部窓口
C202	内部告発窓口（社外）の設置	外部窓口
C207	業務部門から独立した内部監査部門の有無	独立監査
C227	リスクマネジメント・クライシスマネジメントの体制の構築	RM・CM
C229	リスクマネジメント・クライシスマネジメントの基本方針の有無	RM・CMP
E082	環境監査の実施状況	環境監査
E087	環境マネジメントシステムの構築	環境 M
K136	労働安全衛生マネジメントシステムの構築の有無	労働 M

環境編，CIO 設置の有無や ISMS の取得状況，内部監査の有無などの CSR 全般編の 3 つからなる．

CSR データセットの統計量，回答内容の集計例，質問項目の一部と略称をそれぞれ**表 2**，**表 3**，**表 4** に示す．質問項目は多様な形式を含んでいる．たとえば，「内部監査を行っているか」という質問に対し「1. 定期的に行っている 2. 不定期で行っている...」など複数の選択肢がある．本研究では，それらの質問の回答を表 3 に従って Yes，No に分類し直し調査を行った．2 値に分類した大きな理由は，対応する項目とインシデント数の関係を明らかにするためである．「その他」を No に分類したのは，「検討中」や「今後実施の予定」などの回答例があり，ほとんどはその方策を調査時点では行っていないと判断されたためである．本稿では，約 800 の質問項目のうち，情報セキュリティに深く関係する表 4 に示した 17 に絞り，調査結果を報告する．ここで，C122 などの項目 ID は，CSR データセット [22] の付番に従っている．K，E，C はアンケート項目の種類を表しており，それぞれ，雇用・人材活用，環境，CSR 全般の 3 つを表している．E や K の項目はセキュリティとは直接関係ない可能性はあるが，潜在的な影響を完全には否定できないため，幅広く調査項目に加えている．

3. 分析

3.1 分析目的

本研究は，CSR が扱う約 200 のマネジメント方策とその実施によるインシデント発生の相互作用を明らかにすることを目的とする．データを以下の観点で分析する．

- 企業の業種
- 企業の規模
- インシデント観測年
- セキュリティマネジメント方策

分析の全体的な流れは次のとおりである．

まず，企業の業種や規模，実施しているセキュリティ方策などについてインシデント数を集計し，各マネジメント方策に対する相対危険度 Relative Risk（RR）を評価する．次に，業種や観測年などがインシデントに対して影響を与える交絡因子となっていないかを調べるために，業種別や企業規模別でのインシデント数について仮説検定を行う．交絡因子となっている可能性が見られれば，調査計画時点で無作為化することが困難なため，交絡因子の調整が可能な分析手法として知られている多重ロジスティック回帰を適用する．RR を用いる意義は，単純なクロス集計により要因の帰着であるインシデントの有無における効果を定量化することができるためである．加えて，RR の仮説検定が確立しており，疫学分野をはじめとするリスク評価に広く用いられている．

これらの分析で用いられる相対危険度 RR と調整済みオッズ比 adjusted Odds Ratio（OR）について次節で述べる．

3.2 分析手法：相対危険度

相対危険度 Relative Risk は，マネジメント方策 M を実施しているか否かについて，インシデントが発生した企業数が**表 5** のように与えられているとき，M によるインシデント発生の RR (M) は，M を実施したときのインシデント発生の条件付き確率と M がないときのインシデント発生確率の比，すなわち，

$$\mathrm{RR}(M) = \frac{Pr(\mathsf{incident}|M)}{Pr(\mathsf{incident}|\overline{M})} = \frac{a/m_1}{c/m_2} \quad (1)$$

と定義される．相対危険度が 1 以下の場合，実施しているマネジメントによってインシデント発生のリスクが抑えられていると考える．

RR が統計的に有意かどうかを確認するために，カイ 2

表 5 マネジメント方策 M とインシデントの分割表
Table 5 Contingency between security practice M and cyber incidents.

マネジメント	インシデント・Yes	No	計
M・Yes	a	b	m_1
M・No	c	d	m_2
計	n_1	n_2	N

表 6 2013 年に内部統制委員会を設置している企業数
Table 6 The incident frequencies for companies that established internal control in 2013.

内部統制委員会	インシデント・Yes	No	計
Yes	17	1,012	1,029
No	2	179	181
計	19	1,191	1,210

乗検定を行う．カイ 2 乗検定では，帰無仮説 H_0：（マネジメント M の実施の有無とインシデントの発生の有無は関連がなく，2 つのインシデント発生率は等しい）を立て，帰無仮説の生起確率 p 値が有意水準（$p < 0.05$）の場合，帰無仮説が棄却されマネジメント M の実施とインシデントの発生に関連があると判断する．このとき，カイ 2 乗値 χ^2 は，

$$\chi^2 = \frac{N(|ad - bc| - \frac{N}{2})}{n_1 n_2 m_1 m_2} \tag{2}$$

で与えられる．たとえば，2013 年に内部統制委員会の設置をしていた企業数が**表 6** で与えられたとき，RR（$M_{\text{内統}}$）は，

$$RR(M_{\text{内統}}) = \frac{17/1029}{2/181} = 1.495 \tag{3}$$

となる．また，カイ 2 乗検定による p 値は 0.5852 となり，5%の有意水準を満たしていない．それゆえ，2013 年において内部統制委員会を設置することは，インシデント発生のリスクを低下させているとはいえない．

3.3 分析手法：多重ロジスティック回帰

企業の業種，規模，観測年によってインシデント発生率が異なることが考えられる．これら交絡因子の影響を調整して，マネジメント方策によるインシデント抑制効果を明らかにする手法として知られている多重ロジスティック回帰 [17] について述べる．

ある企業 i の y 年のインシデント発生確率 p_{iy} を

$$p_{iy} = \frac{1}{1 + e^{-z_i}} \tag{4}$$

で表す．ここで，z_i は，線形式

$$z_i = \alpha + \beta_i b_i + \beta_y c_y + \beta_d d_i + \beta_{x_1} x_1 + \cdots + \beta_{x_m} x_m \tag{5}$$

で定められ，b_i，c_y および d_i は i の業種，CSR データ調査年 y の社会情勢，i の企業規模である．m 個の説明変数

表 7 CSR データセットの記載企業数と，インシデント発生企業数
Table 7 Number of companies compromised by cyber incidents.

	2013	2014	2015	2016	2017	計
CSR	1,210	1,305	1,325	1,408	1,413	6,661
JNSA	12	19	21	25	23	100
SecurityNext	13	17	22	29	24	105
JNSA・SecurityNext の被り	6	9	16	24	18	67
使用インシデント件数	19	27	27	30	29	132

x_m は，m 種類のマネジメント方策実施の有無を Bool 値で表す．α は定数，β は各変数の係数である．

マネージメント方策 M とインシデントの間に，表 5 の関係があるとき，a/b や c/d をオッズ，その比 $\frac{a/b}{c/d}$ をオッズ比 Odds Ratio（OR）という．$a \ll b$ で $a + b \approx b$ がいえるとき，

$$RR = \frac{a/(a+b)}{c/(c+d)} \approx \frac{a/b}{c/d} = OR \tag{6}$$

となり，OR と RR とほぼ等しい．したがって，マネージメント方策の有無という説明変数のインシデント削減の効果を見るためには，OR と RR のどちらを使ってもよいが，OR には次のようにして，交絡因子の影響を調整することができる性質があることに着目する．

ある説明変数 x_1 によるインシデント発生の条件付き確率を $p_1 = Pr(\mathsf{incident}|x_1 = 1)$ と $p_0 = Pr(\mathsf{incident}|x_1 = 0)$ と表す．しかし，他の説明変数 α，b，c，d，$x_2, \ldots, x_m$ に偏りがあり，交絡因子となっている可能性がある．そこで，x_1 以外の説明変数の値を同一に揃えたときの 2 つオッズが，

$$\frac{p_1}{1 - p_1} = e^{\alpha + \beta_i b_i + \beta_y c_y + \beta_d d_i + \beta_{x_1} 1 + \cdots + \beta_{x_m} x_m} \tag{7}$$

$$\frac{p_0}{1 - p_0} = e^{\alpha + \beta_i b_i + \beta_y c_y + \beta_d d_i + \beta_{x_1} 0 + \cdots + \beta_{x_m} x_m} \tag{8}$$

と表されることを利用すると，その比は

$$\widehat{OR} = \frac{p_1}{1 - p_1} / \frac{p_0}{1 - p_0} = e^{\beta_1} \tag{9}$$

で与えられる．これを，調整したオッズ比（adjusted Odds Ratio）と呼ぶ．

本稿では，x は $m = 119$ のマネジメント項目 b_i はインシデントの発生した 14 業種について，d_i は従業員数の対数，i は CSR データセットの 6,661 件の企業のデータを用いて分析を行う．119 件は，CSR データベースの質問項目 800 件のうち男女比，件数などの数値の項目を除き，分析可能なできるだけ多くの項目を入れた件数である．なお，従業員数や時価総額などは，特異な少数の企業が混在してしばしば分布の右側の裾野が広くなり，バイアスを生じる可能性がある．そこで，ここでは従業員数の対数をとっている．回帰には R の glm 関数を用いる．

表 8 セキュリティ方策についてのインシデントの相対リスク
Table 8 Relative risks (RRs) of incidents given security practices.

方策	実施企業数	インシデント発生企業数	数	*RR*	p 値
告発保護	4,975	106	118	1.118	0.028 **
内統委員	2,997	50	55	0.875	0.232
CIO	1,901	38	43	1.048	0.803
CFO	2,248	56	65	1.307	0.017 **
PP	4,424	106	118	1.257	0.000 ***
SP	4,934	104	116	1.106	0.054
内部監査	4,346	93	103	1.122	0.070
外部監査	3,238	68	75	1.101	0.302
ISMS	999	25	29	1.313	0.171
内部窓口	5,086	108	120	1.114	0.026 **
外部窓口	3,543	76	86	1.125	0.154
独立監査	4,687	102	114	1.141	0.017 **
RM・CM	3,920	101	111	1.351	0.000 ***
RM・CMP	3,650	97	107	1.394	0.000 ***
環境監査	3,541	70	75	1.037	0.721
環境 M	3,722	71	77	1.001	0.933
労働 M	2,656	66	71	1.303	0.007 ***

3.4 分析結果

3.4.1 全体でのインシデント発生企業

表 7 に年ごとの CSR データベースの記載企業数と，インシデント件数を示す．JNSA と SecurityNext の 2 つのデータセットの重複が 5 年間で 67 件であり，これはそれぞれの 75%と 63%を占めている．SecurityNext にのみ記載されている大きな事例には，良品計画（2014 年，ハードディスク紛失），東洋証券（2015 年，取引残高報告書紛失），東京ガス（2016 年，ウェブサイト設定ミス）などがある．以上より，2 つのデータセットを統合することで，2.1.2 項で指摘したデータの偏りを補正し，十分に調査対象を広げることができたと判断できる．ここで網羅されていない非公開の小規模なインシデントが隠れている可能性はあるが，本研究の目的であるセキュリティ方策の効果には大きく影響しないと考える．

CSR の社会的責任編の 14 件と，環境編の 2 件，雇用編の 1 件の計 17 件のマネージメント方策について，各年のマネジメント実施企業数，インシデント発生数を合計し，計算した RR と，カイ 2 乗検定の結果を**表 8** に示す．表で，有意確率 5%，1%を超えた p 値に，各々，**，***を付す．たとえば，PP，RM・CM，RM・CMP，労働 M については，すべて有意確率 1%を超えており，各方策インシデント発生比率に対する負の効果が統計的に有意なレベルで生じている．CIO や ISMS 認証などによって，インシデント発生のリスクが抑えられると考えたが，1.048，1.313 と，RR は 1 を上回った．内部統制委員会の設置の RR は 0.875 であり，1 を下回る．

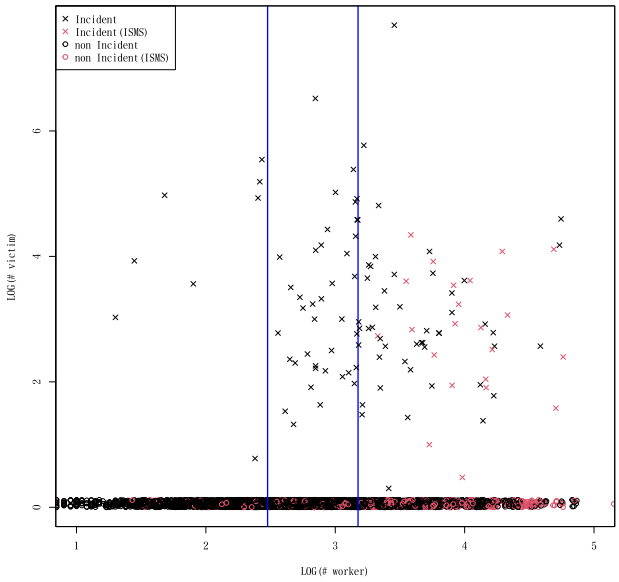

図 1 ISMS 取得企業の散布図
Fig. 1 ISMS-certified companies plotted by number of employees and number of victims.

3.4.2 業種ごとのインシデント発生率

表 9 に CSR データベース内の企業の業種の分布とインシデント発生企業数を示す．業種区分は，東京証券取引所が日本株の分類として利用してきた 33 業種分類を 17 業種に再編した TOPIX-17 シリーズ [9] を利用し，17 業種に区分した．表 9 より，最頻の業種は情報通信・サービスに関する約 230 の企業群である．次いで，商社，小売，素材・科学と続く．インシデント発生企業数も，情報通信・サービスに関する企業群が 5 年間で 26 と最も多くなっており，銀行，小売，電機・精密と続く．

3.4.3 企業規模別

CSR データベースは，企業の従業員数が記載されている．本稿では，各企業の従業員数をもとに，企業を中小企業（従業員数 <300），大企業 1（従業員数 $<1{,}500$），大企業 2（$1{,}500 \leq$ 従業員数）の 3 種類に分類した．企業規模別での各年のインシデント発生企業数を**表 10** に示す．企業規模が大きくなるにつれてインシデント数も増加していることが分かる．

ISMS 取得企業の散布図を**図 1** に示す．X 軸は Log(従業員数)，Y 軸は Log(インシデントによる被害者人数) である．中小企業，大企業 1，大企業 2 の境界に垂直線を入れている．丸で示したのは，インシデントが発生していない企業であり，y 座標は 0 になっているが，インシデントの被害者はいない．赤く色をつけている企業が，ISMS 認証を取得している企業である．ISMS 認証を取得している企業の多くは，企業規模が大きい企業であることが分かる．また，インシデントの分布が X 軸の従業員数に対しては右の大企業に偏っているのに対して，Y 軸の漏洩人数にはあまり影響せず，幅広く分布している．

表 9 各業種の企業数とインシデント発生企業数
Table 9 Numbers of companies and incidents per industry.

業種	2013		2014		2015		2016		2017		計	
	企業数	インシデント発生企業数	企業数	インシデント発生企業数	企業数	インシデント発生企業数	企業数	インシデント発生企業数	企業数	インシデント発生企業数	企業数	インシデント発生企業数
情報通信・サービスその他	215	4	233	6	237	4	269	6	273	8	1,227	28
銀行	31	4	37	2	37	4	42	2	42	4	189	16
小売	102	1	106	3	106	4	108	5	119	2	541	15
電機・精密	127	3	129	4	129	2	140	0	136	3	661	12
電気・ガス	12	0	12	2	11	2	12	3	12	5	59	12
建設・資材	97	3	105	2	107	2	114	2	115	0	538	9
素材・化学	119	2	131	1	139	0	136	3	141	2	666	8
運輸・物流	40	0	44	2	44	2	42	1	45	3	215	8
商社・卸売	121	0	129	2	131	3	142	1	134	0	657	6
金融（除く銀行）	28	0	36	2	36	3	41	0	39	0	180	5
食品	52	0	54	0	59	1	64	2	59	0	288	3
自動車・輸送機	60	1	66	0	68	0	66	0	66	0	326	3
機械	65	0	77	0	77	0	88	3	86	0	393	3
鋼鉄・非鉄	31	0	33	0	32	0	30	0	30	0	156	1
エネルギー資源	5	0	6	0	6	0	6	0	6	0	29	0
医薬品	24	0	26	0	30	0	32	0	33	0	145	0
不動産	28	0	32	0	33	0	31	0	32	0	156	0
不明	53	1	49	1	43	0	45	0	45	1	235	3
総計	1,210	19	1,305	27	1,325	27	1,408	30	1,413	29	6,661	132

表 10 企業規模別インシデント発生企業数
Table 10 Number of compromised companies for company scales.

企業規模	2013		2014		2015		2016		2017		計	
	企業数	インシデント発生企業数	企業数	インシデント発生企業数	企業数	インシデント発生企業数	企業数	インシデント発生企業数	企業数	インシデント発生企業数	企業数	インシデント発生企業数
中小企業	320	1	359	2	366	0	400	3	380	4	1,825	9
大企業 1	478	9	516	7	523	9	561	8	571	9	2,649	42
大企業 2	407	9	426	18	435	18	447	19	461	16	2,176	76
計	1,210	19	1,305	27	1,325	27	1,408	30	1,413	29	6,661	132

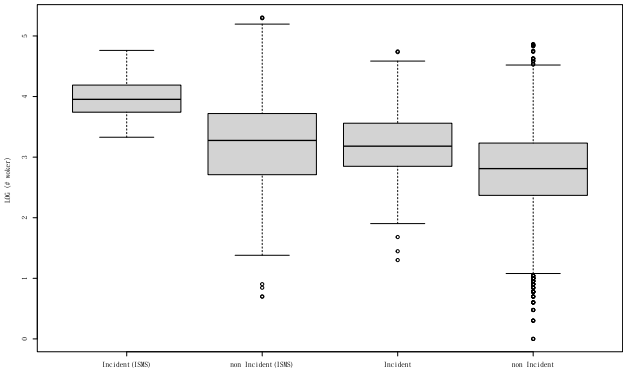

図 2 インシデント有無による従業員数の分布
Fig. 2 Box-plot of number of employees in company that have (not) incidents.

そこで，インシデントの有無と従業員数の関係を表すボックスプロットを**図 2** に示す．ISMS 認証を取得している左の 2 群は，そうでない右よりも従業員数が多く，インシデントのある企業群（左から 1，3 番目）は生じていない企業群（2，4 番目）より多くの従業員を雇用している．

3.4.4 漏洩原因別のインシデント発生数

JNSA データセットでは，インシデントの発生原因を紛失・置忘れ，不正アクセスなどの 12 種類に分類をしている．また，SecurityNext からインシデント情報を収集した際に，記事内容を精査し，JNSA と同様にインシデント発生原因を分類した．漏洩原因区分を**表 11** に示す．本稿では，これら 12 種類の漏洩原因を，人的ミス，悪意のある攻撃などの 6 種類に再分類する．

表 11 漏洩原因区分
Table 11 Reasons of cyber incidents.

再区分した漏洩原因	元の漏洩原因		
人的ミス	紛失・置忘れ	管理ミス	誤操作
悪意のある攻撃	不正アクセス	不正ログイン	ワーム・ウイルス
内部犯行	不正な情報持ち出し	内部犯罪・内部不正行為	
設定ミス・バグ	設定ミス	バグ・セキュリティホール	
盗難	盗難		
その他	その他		

漏洩原因別の各年のインシデント発生数を**表 12** に示す．人的ミスによるインシデントが 5 年間で最も多く，70 件発生していた．漏洩原因別の被害人数についての箱ひげ図を**図 3** に示す．人的ミス（Miss）によるインシデントは発生件数は最も多かったが，被害人数は他の漏洩原因と比べ

表 12 漏洩原因別インシデント件数
Table 12 Number of cyber incidents per reason.

漏洩原因	2013	2014	2015	2016	2017	計
人的ミス	9	19	12	13	17	70
悪意のある攻撃	6	7	5	9	9	36
設定ミス・バグ	2	2	4	4	2	14
盗難	1	0	4	5	2	12
内部犯行	1	1	3	2	3	10
その他	2	0	0	0	0	2
不明	0	0	1	0	1	2
合計	21	29	29	33	34	146*

*合計数 146 が表 9，11 などの 132 件と合わないのは，1 社で複数のインシデントを起こす例があるので，インシデント発生企業数でなくインシデント件数を集計しているためである．

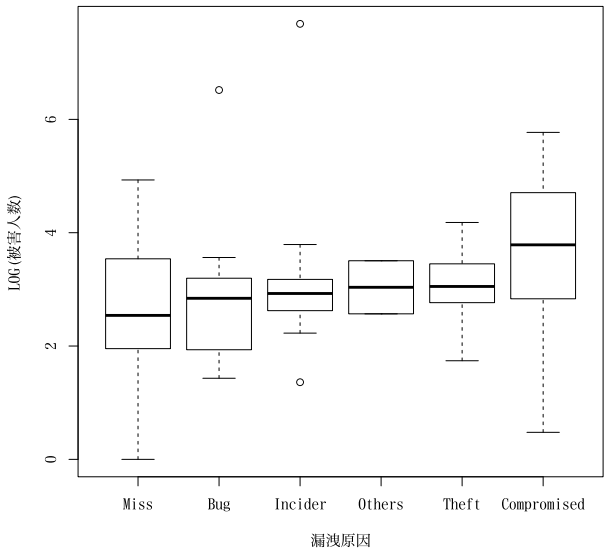

図 3 漏洩原因別被害人数の箱ひげ図
Fig. 3 Box-plot of number of victims per reason.

て少なく，内部犯行（Insider）や盗難（Theft），特に悪意のある攻撃（Compromised）による被害人数が多くなっている．

3.4.5 観測年によるインシデント発生率

表 7 は，年々インシデントが増加していることを示している．観測した 5 年間において，2013 年を基準とすると 1.52 倍に増加している．これはセキュリティの脅威が年々増加していることを表しているが，その間において CSR 対象企業も増加しているので，観測年がインシデントが発生率増加の直接的な要因であるかは自明ではない．

3.5 交絡因子の検定

企業規模や観測年などが交絡因子となり，セキュリティマネジメント方策のインシデントに対する効果を正しく評価できていない恐れがある．そこで，層別 2×2 分割表に対する Mantel-Haenszel 法 [16], [17], [18] を用いて検定をする．

Mantel-Haenszel 法は，マネジメントやインシデント発生有無のような名義尺度に対する相対危険度を調整する方法である．マネジメントとインシデントの件数についての 2×2 の分割表が，企業規模などの k 個の因子によって独立であると仮定（帰無仮説）すると，統計量

$$\chi^2 = \frac{(\sum_k n_i - \mu_i)^2}{\sum_k \sigma(n_i)}$$

は自由度 1 のカイ二乗分布に従う．ここで，n_i は i 番目の因子におけるマネジメントを導入してインシデントを生じた企業の数，μ_m はその平均，$\sigma(n_i)$ はその推定分散である．各方策 x における各因子についての Mantel-Haenszel 検定による P 値を**表 13** に示す．業種，規模，観測年の 3 つについていずれも有意水準（5%を**，1%を***で記す）を超える方策が，それぞれ 8，6，9 個検出された．したがって，帰無仮説が棄却され，これら 3 つが交絡因子であることが示された．

表 13 マネジメント方策による因子についての Mantel-Haenszel 検定による P 値
Table 13 p-values of Mantel-Haenszel test for security practices.

方策 x	p（業種）	p（規模）	p（観測年）
告発保護	0.030 **	0.770	0.019 **
内統委員	0.986	0.023 **	0.182
CIO	0.695	0.109	0.745
CFO	0.003 ***	0.707	0.012 **
PP	0.000 ***	0.041 **	0.000 ***
SP	0.053	0.908	0.042 **
内部監査	0.083	0.973	0.057
外部監査	0.286	0.889	0.376
ISMS	0.417	0.756	0.248
内部窓口	0.026 **	0.647	0.019 **
外部窓口	0.256	0.306	0.174
独立監査	0.022 **	0.800	0.016 **
RM/CM	0.000 ***	0.021 **	0.000 ***
RM/CMP	0.000 ***	0.019 **	0.000 ***
環境監査	0.206	0.003 ***	0.727
環境 M	0.342	0.000 ***	0.984
労働 M	0.000 ***	0.982	0.005 ***

交絡因子の影響を調整して，インシデント発生リスクに対する方策の効果を明らかにするために，次節で，多重ロジスティック回帰による調整されたオッズ比を求める．

3.6 多重ロジスティック回帰

業種，企業規模，年代は独立ではなく，偏差が激しく，それぞれ相関もあるためインシデントの効果を正しく評価できない．そこで，交絡因子の影響を考慮して，これらの変数をまとめて評価する多重ロジスティック回帰を適用する．

多重ロジスティック回帰による各係数を**表 14** に示す．Estimate が係数であり，これが正の場合，マネジメント

表 14 多重ロジスティック回帰の結果（一部）
Table 14 Result of multiple logistic regression.

		Estimate	Std.Error	Pr(>|z|)	OR
a	(Intercept)	−7.570	1.018	0.000 ***	0.001
b	建設・資材	0.384	0.786	0.625	1.469
	素材・化学	−0.002	0.767	0.998	0.998
	自動車・輸送機	−0.165	0.955	0.863	0.848
	鋼鉄・非鉄	−0.675	1.305	0.605	0.509
	電機・精密	0.160	0.791	0.840	1.173
	情報通信・サービスその他	0.603	0.725	0.406	1.828
	電気・ガス	2.424	0.943	0.010 **	11.291
	運輸・物流	0.981	0.837	0.241	2.666
	商社・卸売	0.125	0.841	0.882	1.133
	小売	1.054	0.742	0.156	2.869
	銀行	1.569	0.825	0.057	4.802
	金融（除く銀行）	−0.056	0.920	0.952	0.946
	機械	−0.184	0.910	0.840	0.832
	不動産	−15.130	779.100	0.985	0.000
	医薬品	−15.580	774.400	0.984	0.000
	エネルギー資源	−15.650	1,744.000	0.993	0.000
	不明	−2.005	1.267	0.114	0.135
c	2014	0.219	0.324	0.500	1.245
	2015	0.242	0.333	0.468	1.274
	2016	0.156	0.342	0.649	1.169
	2017	−0.257	0.367	0.483	0.773
d	LOG(従業員数)	0.276	0.100	0.006 ***	1.317
x	告発保護	0.451	0.684	0.509	1.570
	内統委員	−0.016	0.255	0.952	0.985
	CIO	−1.044	0.329	0.001 ***	0.352
	CFO	0.622	0.319	0.051	1.863
	PP	0.496	0.563	0.379	1.642
	SP	−0.593	0.592	0.317	0.553
	内部監査	−0.122	0.370	0.741	0.885
	外部監査	0.169	0.273	0.536	1.184
	ISMS	−0.171	0.318	0.592	0.843
	内部窓口	−0.121	0.751	0.872	0.886
	外部窓口	−0.726	0.289	0.012 **	0.484
	独立監査	−0.550	0.475	0.247	0.577
	RM・CM	1.292	0.682	0.059	3.640
	RM・CMP	−0.193	0.607	0.751	0.825
	環境監査	−1.109	0.515	0.031 **	0.330
	環境 M	−0.681	0.439	0.121	0.506
	労働 M	0.162	0.288	0.575	1.175

を実施しているときにインシデントの生起確率が上昇する．逆に Estimate が負の場合，インシデントの生起確率は下がる．たとえば，業種が電気・ガスの場合，インシデントの生起確率は上昇し（Estimate：2.424），CIO を設置している企業ではインシデントの生起確率は減少する（Estimate：−1.044）．業種などのカテゴリ値やマネージメント方策の実施などの名義尺度は，ダミー変数に展開している．たとえば，b = 「素材・化学」のレコードは，$(0, 1, 0, \ldots)$ というように，該当する要素のみ 1 で他を 0 とする変数で表す．この際，値域の大きさよりも 1 つ少ない数のダミー変数を用意し，ある値を基準として表す．たとえば，観測年 c は，2013 から 2017 までの 5 つの値をとるが，これを，2013 年を基準とした 4 つのダミー変数による $(0, 0, 0, 0)$，$(1, 0, 0, 0)$，$(0, 1, 0, 0)$，$(0, 0, 1, 0)$，$(0, 0, 0, 1)$ の値で表す．業種 b の基準には，インシデント率が全体の 11 位であり，中央値に近い代表的な値である，「食品業」を用いている．

本結果からは，従業員数，電気・ガス業について，正の係数での有意差が見られた，マネジメント方策については，CIO，外部での内部告発窓口設置，環境監査などについて，負の係数で有意差が見られた．また，オッズ比より，電気・ガス業界では他の業界と比べて約 11 倍インシデントが発生しやすく，CIO を設置している企業では，そうでない企業のインシデントの約 0.3 倍に抑えられる．有意水準はいずれも 0.05 である．

4. 考察

業種ごとで漏洩原因別にインシデント発生件数を集計した結果を**表 15** に示す．業種ごとの企業規模別企業数を**表 17** に示す．企業規模別では，大企業 2 では，人的ミスによるインシデントが，全体の 66 件のうち 40 件，設定ミス・バグによるインシデントが，全体の 14 件のうち 12 件と非常に多い．本稿での企業規模は従業員数から決定しているため，従業員数が増えることで人的ミスが増えることは当然であると考える．銀行，電気・ガス業界では，企業数に対してインシデント発生件数，特に人的ミスによるインシデントが多い．これは，表 17 より，どちらの業種も半数以上の企業が大企業 2 に分類されていること，個人の顧客を対象に業務を行う機会が多いことと関係がある．重要インフラ事業であるので，顧客データの数も多く，管理しなくてはならない従業員数の数も増え，サプライチェーンも大規模になるので，インシデントが生じる機会が多いと考えられる．一方で，不正アクセスなどの悪意のある攻撃については大企業 1 と大企業 2 で大きな差がなかったことから，一定以上の規模の企業は攻撃されるリスクが一律に増加している可能性がある．

多重ロジスティック回帰の結果より，注目した 17 のマネジメント方策のうち 11 方策で Estimate が負となり，ほとんどのの方策がインシデントを抑制していることを表している．ただし，5%の有意水準で満たしているものは，CIO，外部窓口，環境監査だけであり，それ以外は有意な効果は認められなかった．OR の結果は，表 8 の全体での RR による分析結果と多くの場合で逆な結果となったが，従業員数や，業種にかかる係数の多くが正であり，それが交絡因子として働き，マネジメントの効果を偽らせていたと考えられる．たとえば，CIO 設置の有無の場合全体での RR は 1.048 で，インシデント件数が増加していたが，多重

表 15 業種ごとの漏洩原因別インシデント発生件数
Table 15 Number of cyber incidents per industry and reason.

	人的ミス	悪意のある攻撃	設定ミス・バグ	盗難	内部犯行	その他	不明	計
情報通信・サービスその他	11	12	1	3	3	0	1	31
小売	11	3	1	4	1	0	0	20
銀行	13	1	0	0	2	1	0	17
電気・ガス	10	2	1	2	0	0	0	15
電機・精密	7	1	3	1	0	0	0	12
建設・資材	6	1	1	0	1	0	0	9
素材・化学	2	3	1	2	0	0	0	8
運輸・物流	2	3	1	0	2	0	0	8
商社・卸売	1	4	1	0	1	0	0	7
金融 (除く銀行)	4	0	0	0	0	0	1	5
食品	0	2	1	0	0	0	0	3
自動車・輸送機	1	0	2	0	0	0	0	3
機械	1	1	1	0	0	0	0	3
鉄鋼・非鉄	1	0	0	0	0	0	0	1
エネルギー資源	0	0	0	0	0	0	0	0
医薬品	0	0	0	0	0	0	0	0
不動産	0	0	0	0	0	0	0	0
不明	0	3	0	0	0	1	0	4
計	70	36	14	12	10	2	2	146

表 16 食品業を基準とした RR と OR
Table 16 Relative risk (RRs) and odds ratio (ORs) with food industry as reference.

業種	RR		OR	
情報通信・サービスその他	2.034		1.827	
小売	2.662		2.869	
銀行	8.127	***	4.802	
電気・ガス	17.898	***	11.291	***
電機・精密	1.743		1.173	
建設・資材	1.606		1.469	
素材・化学	1.153		0.998	
運輸・物流	3.126		2.666	
商社・卸売	0.877		1.133	
金融（除く銀行）	2.667		0.946	
自動車・輸送機	0.883		0.848	
機械	0.733		0.832	
鋼鉄・非鉄	0.615		0.509	

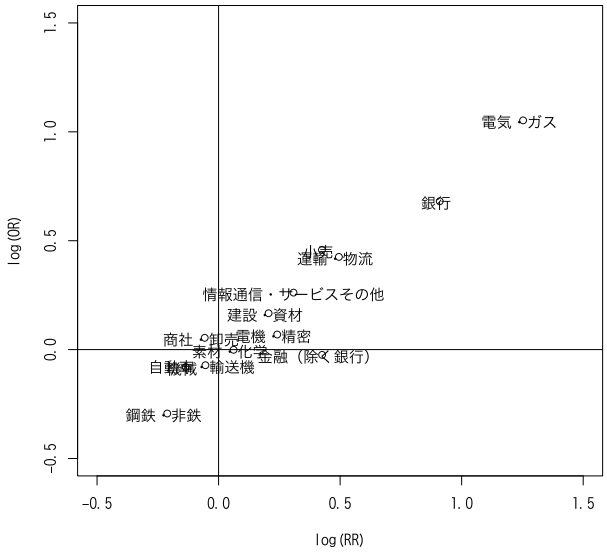

図 4 食品業を基準とした RR と調整 OR の散布図
Fig. 4 Scatter plot of industries plotted by RRs and ORs with food industry as references.

ロジスティック回帰による OR では，0.352 となっており，インシデントの生起確率を抑制していた．セキュリティ対策推進には，CIO とは異なる立場で情報セキュリティを統括する CISO（Chief Information Security Officer）が重要であるともいわれているが，CIO が CISO の役割を兼務している企業が多いことが考えられる．

企業規模については，RR では中小企業，大企業 1 が $RR < 1$，大企業 2 が $RR > 1$ となり，企業規模が大きくなるとインシデント件数が増加していた．多重ロジスティック回帰でも Estimate が正となり，企業規模（従業員数）が大きくなるとインシデントの生起確率が大きくなるため，どちらの結果も傾向としては整合している．

食品業との比較で各業種について RR を計算した結果を**表 16** に，それぞれの散布図を**図 4** に示す．ただし，エネルギー資源，医薬品，不動産の 3 業種は期間内に 1 度もインシデントがないために，RR が算出できない．そこで，不明と合わせて除外した残りの 6,095 件について比較している．多重ロジスティック回帰では食品業を基準としてその他の業種についての回帰を行っているので，この RR と OR で業種による影響を確認する．図 4 の 2 つの直線で区

表 17 業種別企業規模
Table 17 Number of companies broken up scales per industry.

	中小企業	大企業 1	大企業 2	不明	計
情報通信・サービスその他	443	465	319	0	1,227
銀行	2	66	121	0	189
小売	196	222	123	0	541
電機・精密	126	258	277	0	661
電気・ガス	5	0	54	0	59
建設・資材	114	208	216	0	538
素材・化学	153	327	186	0	666
運輸・物流	67	66	82	0	215
商社・卸売	286	321	49	1	657
金融（除く銀行）	71	54	55	0	180
食品	55	136	97	0	288
自動車・輸送機	27	120	179	0	326
機械	73	195	125	0	393
鋼鉄・非鉄	37	51	68	0	156
エネルギー資源	1	13	15	0	29
医薬品	34	31	80	0	145
不動産	110	40	6	0	156
不明	25	76	124	10	235
計	1,825	2,649	2,176	11	6,661

切られた 4 つの区分の内，右下と左上の範囲に点在するマネジメント方策は，RR と OR でマネジメント方策の効果が逆に測定されていることを示す．13 業種中，11 の業種でインシデントの増加，減少の影響が一致することを確認した．ただし，素材・化学の $RR = 1.153$，$OR = 0.998$ のように，RR と OR で業種による影響が逆に観測された業種が 2 つあった．この 2 つは，13 業種の中でもリスクが 1.0 に近い（1.0 への絶対誤差が RR で上位 1，3 位，OR で上位 1，2 位）であり，それゆえに小さな誤差で逆の効果になったと考えられる．OR と RR は厳密には一致しないので多少の違いは起こりうる．各業種の企業規模の偏りがあるときには，RR だけではなく多重ロジスティック回帰による OR を求める必要がある．逆に，交絡因子がないことが自明なときには，RR により素早く因子の影響を評価できる．このような，交絡因子の影響を調整することでマネジメント方策の効果が見えたといえる．

5. 結論

企業の業種，企業規模ごと，インシデントの漏洩原因ごとでの分類を行い，マネジメント方策の実施と，インシデント発生の関係を調査した．データの分析により，業種や企業規模によりインシデントの発生に偏りがあり，Mantel-Haenszel 検定により，(1) 業種，(2) 企業規模，(3) 観測年が交絡因子として働いていたことが示された．

また，業種や企業規模などの交絡因子による影響を調整し，マネジメント方策の実施によるインシデント抑制効果を調査するために，多重ロジスティック回帰を行った．この結果，従業員数や，業種の係数が正，今回注目した 17 のマネジメント方策のうち，11 の方策の係数が負となり，インシデントを誘発する要因，抑制する要因が明らかになった．さらに，オッズ比から CIO 設置企業では，インシデントの生起確率が約 0.3 倍に抑えられることが明らかになった．本研究により，マネジメント対策とインシデントの間にある因果関係を評価することが実現できた．ただし，インシデントの発生には多くの因子が作用するので，3.4.2 項（業種別），3.4.3 項（企業規模別），3.4.4 項（漏洩原因別）などに層別して，インシデント調査をすることが正確な評価のためには重要である．

本研究で対象とした情報漏洩は，人的ミスによって生じるケースが多く，大量の個人情報を取り扱う業種にとっては完全に防止するのは困難なインシデントである．したがって，人的ミスを削減するためにはどのようなユーザインタフェースや警告の仕組みを取り入れるべきか，ヒューマンエラーの観点からも研究を進める必要がある．また，特定の組織を対象とした標的型攻撃の脅威もますます深刻になっている．そこで今後は，個人情報漏洩以外のインシデントについても分析を検討している．

謝辞 本研究を遂行するにあたり，インシデントデータを提供いただいた日本ネットワークセキュリティ協会様に感謝する．本研究では乾が受けている JSPS 科研費 JP16K03755 で購入した CSR データセットを使用した．

参考文献

[1] ベネッセお客様本部：事故の概要，入手先 ⟨https://www.benesse.co.jp/customer/bcinfo/01.html⟩（参照 2018-01-31）．
[2] 幻冬舎：不正アクセスによる会員情報の流出に関するご報告とお詫び，入手先 ⟨http://www.gentosha.co.jp/news/n446.html⟩（参照 2018-01-31）．
[3] 東洋経済データサービス CSR データ，入手先 ⟨https://biz.toyokeizai.net/data/service/detail/id=321⟩（参照 2018-06-20）．
[4] 山田道洋，池上和輝，菊池浩明，乾 孝治：経営マネジメント状況による情報漏洩インシデント削減効果の評価，情報処理学会 CSEC 研究会，CSEC82, pp.1–6 (2018).
[5] 平成 26 年度我が国情報経済社会における基盤整備調査報告書，入手先 ⟨http://www.meti.go.jp/statistics/zyo/zyouhou/result-2/pdf/H26_report.pdf⟩（参照 2018-06-19）．
[6] 杉本暁彦，磯部義明，仲小路博史：セキュリティ運用のための経営層向けビジネスリスク評価技術の開発，情報処理学会論文誌，Vol.58, No.12, pp.1926–1934 (2017).
[7] Romanosky, S.: Examining the costs and causes of cyber incidents, *Journal of Cybersecurity*, Vol.2, No.2, pp.121–135 (2016).
[8] 情報セキュリティインシデント調査報告書（JNSA データセット）．
[9] 東証業種別株価指数・TOPIX-17 シリーズ，入手先 ⟨http://www.jpx.co.jp/markets/indices/line-up/files/fac_13_sector.pdf⟩（参照 2018-06-21）．
[10] Advisen, available from ⟨https://www.advisenltd.com/⟩ (accessed 2018-02-05).

[11] 経済産業省：サイバーセキュリティ経営ガイドライン Ver2.0，入手先 ⟨meti.go.jp/press/2017/11/20171116003/20171116003-1.pdf⟩（参照 2019-12-12）．
[12] 佐久間樹里，猪俣敦夫：サイバー保険の調査・分析による加入率向上への提案，研究報告インターネットと運用技術（IOT）（IPSJ），pp.1–8 (2019).
[13] 小梶顯義，原田要之助，後藤厚宏：金融機関におけるサイバーセキュリティのアセスメントに関する考察，研究報告電子化知的財産・社会基盤（IPSJ），pp.1–5 (2019).
[14] Edwards, B., Hofmeyr, S. and Forrest, S.: Hype and heavy tails: A closer look at data breaches, *Journal of Cybersecurity*, Vol.2, No.1, pp.3–14 (2016).
[15] Xu, M., Schweitzer, K., Bateman, R. and Xu, S.: Modeling and Predicting Cyber Hacking Breaches, *IEEE Trans. Information Forensics and Security*, Vol.13, pp.2856–2871 (2018).
[16] Mantel, N. and Haenszel, W.: Statistical aspects of the analysis of data from retrospective studies of disease, *J. Natl. Cancer Inst.*, Vol.22, pp.719–748 (1959).
[17] 丹後俊郎：交絡因子の調整，新版 医学への統計学，13 章，pp.240–258, 朝倉書店 (1993).
[18] 奥村晴彦：タイタニック号沈没事故，(Cochran-)Mantel-Haenszel 検定，Simpson のパラドックス，入手先 ⟨https://oku.edu.mie-u.ac.jp/˜okumura/stat/titanic.html⟩（参照 2020-05）．
[19] 江口 彰，山田 秀：ISO 27001 認証の有無による情報セキュリティ インシデント事例の比較分析，日本セキュリティ・マネジメント学会誌，Vol.27, No.1, pp.3–16 (2013).
[20] Sen, R. and Borle, S.: Estimating the Contextual Risk of Data Breach: An Empirical Approach, *Journal of Management Information Systems*, Vol.32, No.2, pp.314–341 (2015).
[21] Eling, M. and Loperfido, N.: Data breaches: Goodness of fit, pricing, and risk measurement, *Insurance: Mathematics and Economics*, Vol.75, pp.126–136 (2017).
[22] 東洋経済新報社：CSR データベース テキスト版説明書 (2017).
[23] Romanosky, S., Telang, R. and Acquisti, A.: Do Data Breach Disclosure Laws Reduce Identity Theft?, *Journal of Policy Analysis and Management*, Vol.30, No.2, pp.256–286 (2011).

山田 道洋

2017 年明治大学総合数理学部先端メディアサイエンス学科卒業．2019 年明治大学大学院博士前期課程修了．現在，日本電気株式会社所属．

池上 和輝 （学生会員）

2019 年明治大学総合数理学部先端メディアサイエンス学科卒業．現在，明治大学大学院博士前期課程在学中．

菊池 浩明 （正会員）

1988 年明治大学工学部電子通信工学科卒業．1990 年同大学大学院博士前期課程修了．1994 年同博士（工学）．1990 年（株）富士通研究所入社．1994 年東海大学工学部電気工学科助手．1995 年同専任講師．1999 年同助教授，2006 年同情報理工学部情報メディア学科教授．1997 年カーネギーメロン大学計算機科学学部客員研究員．2013 年明治大学総合数理学部先端メディアサイエンス学科教授．2016 年同大学院先端数理科学研究科長．2018 年一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）代表理事．WIDE プロジェクト暗号メールシステム FJPEM の開発，認証実用化実験協議会（ICAT），IPA 独創情報技術育成事業等に従事．暗号プロトコル，ネットワークセキュリティ，ファジィ論理，プライバシ保護データマイニング等に興味を持つ．1990 年日本ファジィ学会奨励賞，1993 年情報処理学会奨励賞，1996 年 SCIS 論文賞，2010 年度，2017 年度情報処理学会 JIP Outstanding Paper Award．2013 年 IEEE AINA Best Paper Award. 2014 年 情報セキュリティ文化賞．電子情報通信学会，IEEE，ACM 各会員．日本知能情報ファジィ学会理事．本会フェロー．

乾 孝治

1987 年東京工業大学工学部化学工学科卒業．1997 年筑波大学経営・政策科学研究科経営システム科学専攻修了（経営学修士）．2000 年東京大学数理科学研究科博士後期課程数理科学専攻単位取得満期退学．2011 年明治大学博士（理学）．1987 年日本生命入社，1989 年ニッセイ基礎研究所出向，2000 年日本生命財務企画部運用リスク管理室課長，2001 年 PanAgora Asset Management Inc. 派遣を経て退職．2002 年京都大学経済学研究科寄附講座助教授．2004 年明治大学大学院グローバルビジネス研究科助教授，2010 年同教授，2013 年明治大学総合数理学部現象数理学科教授．2016 年同大学学長室専門員，2020 年同大学副学長（研究担当）．金融データサイエンス，応用ファイナンス（金融・保険リスク管理，企業価値評価，資産運用）．