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（2）

山田　道洋[1,a)]　池上　和輝[2]　菊池　浩明[2]　乾　孝治[3]

概要：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．それに伴い，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，東洋経済新報社が国内 1413 社を調査した 5 年間の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，マネジメント方策の実施によってインシデントの件数が増加した原因を明らかにするため，企業の業種や漏洩原因によってデータを分類し，業種などの交絡因子の影響を考慮してリスクの大きさを分析する．

キーワード：セキュリティマネジメント，情報漏洩，ISMS，CIO

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

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．それに伴い，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 3504 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 1413 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したところ，**ISMS 認証の取得や，CIO の設置によってインシデント件数が増加していること**が明らかになった [4]．ISMS 認証と CIO 設置による相対危険度 (Relative Risk) は各々 1.302 と 1.095 であり，両者とも 1.0 を超えており，方策によってインシデントの発生確率が増加したことを示した．中でも，内部告発窓口の設置，内部監査部門の設置，リスクマネジメント体制の構築の RR は，各々 1.36，1.166，1.354 であり，5%の水準で統計的に有意であった．[4] では，この原因として，

(1) 業種等による影響，
(2) 実施予定を誤分類している，
(3) 同一年に，インシデントと方策が導入され，因果関係

[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
[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
[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
[a)] cs172001@meiji.ac.jp

表 1　インシデントデータセットの統計量

データセット	期間	レコード数	企業数
JNSA	2005-2016	15569	8853
SecurityNext	2013-2018	174	121

が逆になっている，

(4) マネジメントの何らかの副作用で，インシデントが増えている

を上げたが，その真偽は不明であった．

そこで，本稿では，[4] の続きとして，上記原因の (1) に着目する．すなわち，1413 の企業群に内在する種々の違い，

a. 業種，
b. 規模，
c. 漏洩原因，
d. 観測年 (景気などの影響)

を交絡因子 (confounding factor) とみなし，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，企業の業種や漏洩原因によってデータを分類することで，マネジメント方策の実施によってインシデントの件数が増加した原因を明らかにする．

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 SecurityNext 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 [5] 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．

2.1.2 SecurityNext 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 SecurityNext[*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には偏りがあり，CSR データセットと共通の企業数は非常に少ない．2017 年のインシデント情報も存在しないため，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 SecurityNext 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．本サイトにて，情報漏洩事件・事故に分類された記事の内，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．

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

表 2　CSR データセットの統計量

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	1210(1157)	2672	753	185
2014	1305(1259)	2582	764	186
2015	1325(1284)	2646	811	193
2016	1408(1364)	2579	832	197
2017	1413(1370)	2627	840	207

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 つから成る．

質問項目は多様な形式を含んでいる．例えば，「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 Yes，No に分類し直し調査を行った．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 2，3，4 に示す．本稿では，約 800 の質問項目の内，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．

本研究では，CSR データセットとインシデントデータセットを照合する．[*2]

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．[4] ではマネジメントの実施によって，インシデント件数が増加していることを報告したが，この原因を調査するために，データを以下の 3 種類で分類する．

- 企業の業種
- 企業の規模
- インシデントの漏洩原因

[*2] 本研究では，CSR データセットの回答の集計方法の精査や，インシデント内容の精査をし直したデータを利用しているため，先行研究 [4] のデータとはインシデント発生企業数や，マネジメント実施企業数が一部異なっている．

表 3　CSR データセットの回答内容の集計例

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

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

表 5　マネジメント方策 M とインシデントの分割表

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

3.2　分析手法：相対危険度

本研究では，あるマネジメントを実施していた場合のインシデント発生への影響を計る指標として相対危険度 Relative Risk(RR) を用いる．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は表 5 の様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 を実施した時のインシデント発生の条件付確率と一般のインシデント発生確率の比，すなわち，

$$RR(M) = \frac{Pr(\text{インシデント}\,|M)}{Pr(\text{インシデント発生})} = \frac{a/m_1}{n_1/N} \qquad (1)$$

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 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．この時，カイ 2 乗値 χ^2 は，

表 6　2014 年に内部統制委員会を設置している企業数

内部統制委員会	インシデント・Yes	No	計
Yes	17	1012	1029
No	2	179	181
計	19	1191	1210

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

で与えられる．例えば，2014 年に内部統制委員会の設置をしていた企業数が表 6 で与えられた時，RR（$M_{\text{内統}}$）は，

$$RR(M_{\text{内統}}) = \frac{17/1029}{19/1210} = 0.513 \qquad (3)$$

となる．また，カイ 2 乗検定による p 値は 0.049 となり，5%の有意水準を満たしている．それゆえ，2014 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結論付ける．

3.3　分析手法：ロジスティック回帰

企業の業種毎，企業規模毎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排除して，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ためにロジスティック回帰を行う．

ある企業 i の y 年のインシデント発生確率 p_{iy} を

$$p_{iy} = \frac{1}{1+e^{-z_i}} \qquad (4)$$

で表す．ここで，

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

を仮定する．b_i，c_y および d_i は業種，CSR データ調査年の社会情勢や，企業規模毎に異なるインシデント発生率を吸収するためのダミー変数である．x_m は説明変数であり，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．

ここで，ある x_1 について，他の変数 α，b，c，d，x_2，…，x_m の交絡因子の影響を調整したオッズ比 (adjusted Odds Ratio) は，

$$OR = e^{\beta_1} \qquad (6)$$

で与えられる．表 5 では，M マネジメントなしを基準とすると，M によるインシデント発生確率 p を用いて，

$$OR = \frac{a/b}{c/d} = \frac{p}{1-p} \qquad (7)$$

である．$a << b$ で $a+b \approx b$ が言えるとき，M なしの群

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

	2013	2014	2015	2016	2017	計
CSR	1210	1305	1325	1408	1413	6661
JNSA	12	19	21	25	12	89
SecurityNext	13	17	22	29	24	105
JNSA・SecurityNext の被り	6	9	16	24	12	67
使用インシデント件数	19	27	27	30	24	127

に対する M の相対危険度 RR は，

$$\frac{a/(a+b)}{c/(c+d)} \approx \frac{a/b}{c/d} = OR \qquad (8)$$

となり，OR に近づく．

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 6095 件の企業のデータを用いて分析を行う．回帰には R の glm 関数を用いる．

3.4　分析結果

3.4.1　全体でのインシデント発生企業 [4]

表 7 に年毎の 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．

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．例えば，PP，RM・CM，RM・CMP，労働 M については，全て有意確率 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．ただし，2.3 節で述べた通り，2014 年のみのデータでは RR が 1 を下回りかつ，カイ 2 乗検定で有意差が見られたが，総計ではカイ 2 乗検定による有意差は見られなかった．

3.4.2　業種毎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 シリーズを利用し，17 業種に区分した [6]．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．

総計の業種毎での RR とカイ 2 乗検定の結果を表 10 に示す．[*3]銀行，金融（除く銀行）の RR が全体的に低く，1 を下回った項目が多数存在する．**一方，小売，電機・精密，素材・化学などの業種では RR が 1 を上回る**項目が多くなっており，特に，小売，素材・化学では今回注目した項目の中ではいずれの項目でも RR が 1 を上回った．

表 8　総計での RR

方策	実施企業数	インシデント発生企業数	RR	p 値	
告発保護	4975	106	1.118	0.028	**
内統委員	2997	50	0.875	0.232	
CIO	1901	38	1.048	0.803	
CFO	2248	56	1.307	0.017	**
PP	4424	106	1.257	0.000	***
SP	4934	104	1.106	0.054	
内部監査	4346	93	1.122	0.070	
外部監査	3238	68	1.101	0.302	
ISMS	999	25	1.313	0.171	
内部窓口	5086	108	1.114	0.026	**
外部窓口	3543	76	1.125	0.154	
独立監査	4687	102	1.141	0.017	**
RM・CM	3920	101	1.351	0.000	***
RM・CMP	3650	97	1.394	0.000	***
環境監査	3541	70	1.037	0.721	
環境 M	3722	71	1.001	0.933	
労働 M	2656	66	1.303	0.007	***

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元に，企業を中小企業（従業員数 <300），大企業 1（従業員数 <1500），大企業 2（1500≤ 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 11 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わかる．

ISMS 取得企業の散布図を図 1 に示す．x 軸は LOG(従業員数)，y 軸はインシデントによる被害者人数を同じく LOG をとったものである．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わかる．**

企業規模別での RR と，カイ 2 乗検定の結果を表 12 に示す．**全体での RR は，中小企業，大企業 1 で 1 を下回り，中小企業では有意差も見られた．一方，大企業 2 では RR が 1 を上回り有意差が見られた．**

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

[*3] RR はインシデントが発生していない群については計算できないため，エネルギー資源，医薬品，不動産の業種は除外した．また，業種が不明であった企業群についても省略した．

表 9　各業種の企業数とインシデント発生企業数

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	6	1227	26
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	4	59	11
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	2	215	7
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	0	235	2
総計	1210	19	1305	27	1325	27	1408	30	1413	24	6661	127

表 10　業種別の RR

方策	情報通信・サービスその他 RR	小売 RR	銀行 RR	電気・ガス RR	電機・精密 RR	建設・資材 RR	素材・化学 RR	運輸・物流 RR	商社・卸売 RR	金融（除く銀行） RR	食品 RR	自動車・輸送機 RR	機械 RR	鋼鉄・非鉄 RR
告発保護	1.167	1.21	0.945	1.093	1.211	0.932	1.259	1.236	1.113	0.850	1.269	1.136	0.923	1.311
内統委員	0.621	1.469	0.319	0	1.178	1.026	1.071	0.830	1.500	0.973	1.371	1.499	1.627	0
CIO	0.784	2.475**	0.514	1.192	0.487	0.752	1.496	1.638	1.738	0	1.882	1.842	1.284	0
CFO	1.530	1.942	0	1.877	1.164	0.924	1.095	2.133	3.221***	0	1.641	1.659	1.272	0
PP	1.279	1.349	0.915	1.135	1.341	1.196	1.442	1.387	1.676	0.900	1.303	1.336	1.154	0
SP	1.066	1.218	0.964	1.093	1.222	0.934	1.129	1.303	1.352	0.837	1.274	1.090	0.953	1.258
内部監査	1.183	1.377	0.915	1.022	1.214	1.100	1.192	1.066	1.393	0.878	0.965	0.768	1.069	1.576
外部監査	1.096	1.469	1.329	0.670	1.172	1.251	1.426	1.146	0.939	0.837	0.571	0.578	0.679	1.714
ISMS	0.621	3.699**	0	2.011	2.774***	0.879	1.892	1.463	0	0	0**	0	0	0
内部窓口	1.356	2.576	0	0.692	2.006***	1.446	2.579***	2.792**	4.380***	1.333	2.526	1.459	0	0
外部窓口	1.055	1.822**	0.477**	1.135	1.603**	0.419	1.054	1.269	1.813	0.649	1.016	1.309	1.272	0
独立監査	1.180	1.167	1.005	1.093	1.281	0.983	1.184	1.361	1.239	0.908	0.869	1.144	0.939	1.431
RM・CM	1.557**	1.682	1.042	1.204	1.409	1.241	1.175	1.558	1.596	0.915	1.309	1.405	1.129	1.529
RM・CMP	1.488**	1.944**	1.042	1.204	1.45**	1.191	1.246	1.617	1.807	0.956	0.941	1.575	1.144	1.814
環境監査	0.791	1.568	0.716	1.135	1.236	1.046	1.253	1.280	1.364	1.108	1	1.105	1.083	1.368
環境 M	0.830	1.596	0.882	1.204	1.202	0.988	1.240	0.743	1.307	0.986	0.897	1.083	1.040	1.368
労働 M	1.377	1.233	0.633	1.632	2.000***	0.860	1.435	1.706	2.790**	1.636	2.102	1.214	1.303	0

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 13 に示す．本稿では，これら 12 種類の漏洩原因を，人的ミス，悪意のある攻撃等の 6 種類に再分類する．

漏洩原因別の各年のインシデント発生数を表 14 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，66 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 2 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．

表 15 に漏洩原因別の RR，カイ 2 乗検定の結果を示す．ISMS によって，内部犯行や設定ミス・バグの RR は 1 を下回ったが，人的ミス，悪意のある攻撃の RR は 1 を上回った．また，盗難では今回注目した 17 項目中 14 項目で RR が 1 を下回っていた．

3.5　ロジスティック回帰

ロジスティック回帰による各係数を表 16 に示す．Estimate が係数であり，これが正の場合，業種に当てはまる時，該当年の時，マネジメントを実施している時にインシデントの生起確率が上昇することになる．逆に Estimate が負の場合，インシデントの生起確率は下がる．例えば，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：2.436），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：−1.097）．今回の結果からは，**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**，個人情報漏洩インシデント発生に関わる交絡因子は，業種と従業員数であった．マネジメント方策については CFO 設置の有無について，正の係数

表 11　企業規模別インシデント発生企業数

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	3	1825	9
大企業 1	478	9	516	7	523	9	561	8	571	9	2649	42
大企業 2	407	9	426	18	435	18	447	19	461	12	2176	76
計	1210	19	1305	27	1325	27	1408	30	1413	24	6661	127

表 12　企業規模別の RR

方策	中小企業				大企業 1				大企業 2			
	実施企業数	インシデント発生企業数	RR		実施企業数	インシデント発生企業数	RR		実施企業数	インシデント発生企業数	RR	
告発保護	1044	6	1.165		2739	48	0.947		1185	52	1.062	
内統委員	669	3	0.909		1667	22	0.713	**	657	25	0.921	
CIO	242	1	0.838		1003	12	0.646		654	25	0.926	
CFO	359	4	2.259		1133	16	0.763		754	36	1.156	
PP	815	6	1.493		2437	48	1.064		1165	52	1.081	
SP	1054	5	0.962		2689	47	0.944		1184	52	1.063	
内部監査	888	4	0.913		2349	42	0.966		1102	47	1.033	
外部監査	659	2	0.615		1809	31	0.926		763	35	1.111	
ISMS	130	0	0		464	2	0.233	**	400	23	1.392	
内部窓口	1116	6	1.090		2773	50	0.974		1190	52	1.058	
外部窓口	571	4	1.421		1937	29	0.809		1034	43	1.007	
独立監査	942	4	0.861		2564	46	0.969		1177	52	1.070	
RM・CM	595	4	1.363		2176	45	1.117		1146	52	1.099	**
RM・CMP	505	4	1.606		2022	43	1.149		1120	50	1.081	
環境監査	404	0	0		2056	27	0.710	***	1078	43	0.966	
環境 M	429	0	0		2178	28	0.695	***	1112	43	0.936	
労働 M	325	3	1.872		1369	23	0.908		957	40	1.012	
全体	1825	9	0.259	***	2649	42	0.832		2176	76	1.831	***

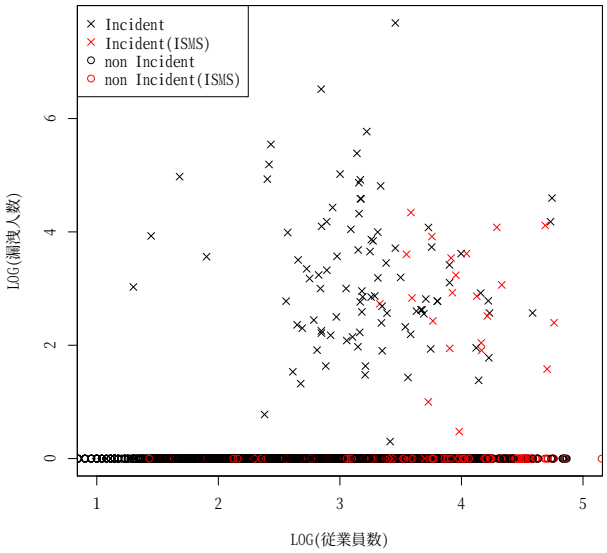

図 1　ISMS 取得企業の散布図

での有意差が見られ，CIO，外部での内部告発窓口設置などについて，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 11.4 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，約 0.3 倍に抑えられる．

表 13　漏洩原因区分

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		

表 14　漏洩原因別インシデント発生数

漏洩原因	2014	2015	2016	2017	2018	計
人的ミス	8	18	12	12	16	66
悪意のある攻撃	6	7	5	8	5	31
設定ミス・バグ	2	2	4	4	2	14
盗難	1	0	4	5	1	11
内部犯行	1	1	2	2	2	8
その他	1	0	0	0	0	1
不明	0	0	1	0	1	2
計	19	28	28	31	27	133

4. 考察

業種毎，企業規模毎で，それぞれ漏洩原因別にインシデント発生件数を集計したものを表 17，表 18 に示す．業種

表 15 漏洩原因別の RR

方策	実施企業数	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	
		インシデント発生企業数	RR	インシデント発生企業数	RR	インシデント発生企業数	RR	インシデント発生企業数	RR	インシデント発生企業数	RR	インシデント発生企業数	RR
告発保護	4975	52	1.055	27	1.166	14	1.339	8	0.974	7	1.172	1	1.339
内統委員	2997	26	0.876	13	0.932	7	1.111	3	0.606	3	0.833	0	0
CIO	1901	17	0.903	12	1.356	6	1.502	2	0.637	2	0.876	0	0
CFO	2248	22	0.988	18	1.720 ***	11	2.328 ***	3	0.808	5	1.852	0	0
PP	4424	52	1.186 **	27	1.311 **	14	1.506 **	8	1.095	7	1.317	1	1.506
SP	4934	53	1.084	26	1.132	14	1.350	6	0.736	7	1.181	1	1.350
内部監査	4346	49	1.138	21	1.038	11	1.204	6	0.836	6	1.150	1	1.533
外部監査	3238	40	1.247	13	0.863	6	0.882	4	0.748	5	1.286	1	2.057
ISMS	999	16	1.616	6	1.291	2	0.953	1	0.606	1	0.833	0	0
内部窓口	5086	55	1.091	27	1.141	14	1.310	7	0.833	7	1.146	1	1.310
外部窓口	3543	38	1.082	21	1.274	10	1.343	6	1.025	4	0.940	1	1.880
独立監査	4687	52	1.120	26	1.192	13	1.320	6	0.775	7	1.244	1	1.421
RM・CM	3920	51	1.313 ***	24	1.316	14	1.699 ***	6	0.927	7	1.487	1	1.699
RM・CMP	3650	50	1.383 ***	21	1.236	14	1.825 ***	6	0.995	7	1.597	1	1.825
環境監査	3541	38	1.083	13	0.789	12	1.612 **	5	0.855	5	1.176	0	0
環境 M	3722	38	1.030	14	0.808	12	1.534 **	5	0.813	5	1.119	0	0
労働 M	2656	33	1.254	16	1.294	10	1.791 **	5	1.140	2	0.627	0	0

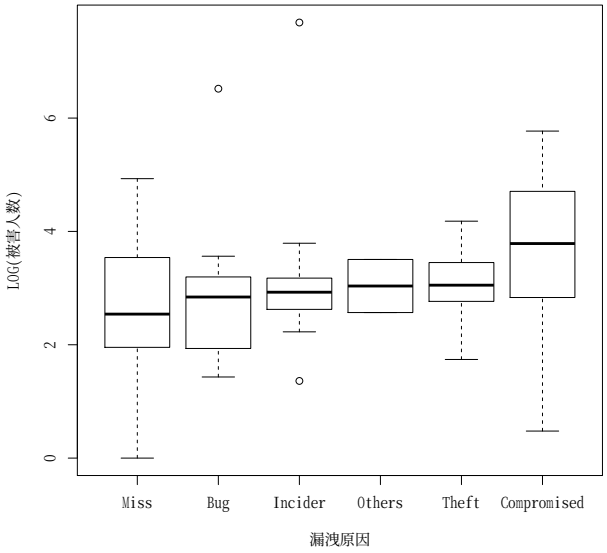

図 2 漏洩原因別被害人数の箱ひげ図

毎の企業規模別企業数を表 20 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 件の内 40 件，設定ミス・バグによるインシデントが，全体の 14 件の内 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 20 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．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．

ロジスティック回帰の結果より，今回注目した 17 のマネジメント方策のうち 11 方策で Estimate が負となり，インシデントを抑制しているという結果となった．これは，

表 16 ロジスティック回帰の結果（一部）

		Estimate	Std.ERRor	Pr(>|z|)	Odds
a	(Intercept)	−8.300	1.072	0.000 ***	0.000
b	建設・資材	0.223	0.800	0.780	1.250
	素材・化学	−0.046	0.775	0.952	0.955
	自動車. 輸送機	−0.334	0.981	0.734	0.716
	鋼鉄・非鉄	−0.838	1.325	0.527	0.432
	電機・精密	0.091	0.805	0.910	1.095
	情報通信・サービスその他	0.561	0.738	0.448	1.752
	電気・ガス	2.436	0.916	0.008 ***	11.422
	運輸・物流	0.829	0.854	0.332	2.291
	商社・卸売	0.066	0.849	0.938	1.068
	小売	0.904	0.756	0.231	2.471
	銀行	1.467	0.833	0.078	4.335
	金融（除く銀行）	0.209	0.913	0.819	1.232
	機械	−0.219	0.921	0.812	0.803
c	2014	0.221	0.333	0.507	1.247
	2015	0.185	0.343	0.590	1.203
	2016	0.185	0.350	0.597	1.203
	2017	−0.193	0.374	0.607	0.825
d	LOG(従業員数)	0.948	0.255	0.000 ***	2.580
x	告発保護	0.520	0.708	0.462	1.683
	内統委員	−0.025	0.260	0.922	0.975
	CIO	−1.097	0.330	0.001 ***	0.334
	CFO	0.655	0.320	0.040 **	1.925
	PP	0.608	0.589	0.302	1.837
	SP	−0.668	0.607	0.271	0.512
	内部監査	−0.207	0.374	0.580	0.813
	外部監査	0.117	0.277	0.674	1.124
	ISMS	−0.217	0.331	0.513	0.805
	内部窓口	−0.050	0.761	0.947	0.951
	外部窓口	−0.685	0.296	0.021 **	0.504
	独立監査	−0.557	0.481	0.247	0.573
	RM・CM	1.181	0.710	0.096	3.259
	RM・CMP	−0.279	0.626	0.656	0.756
	環境監査	−0.844	0.522	0.106	0.430
	環境 M	−1.619	0.528	0.002 ***	0.198
	労働 M	0.044	0.300	0.882	1.046

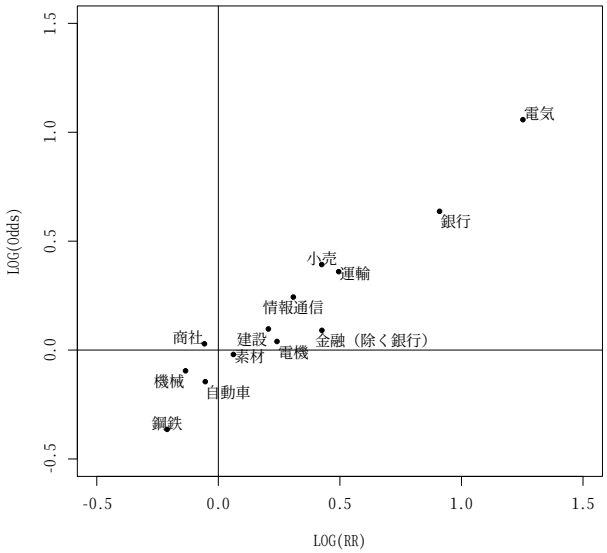

図 3 食品業を基準とした RR と Odds の散布図

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．例えば，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，ロジスティック回帰による Odds では，0.334 となっており，インシデントの生起確率を抑制していた．このように，RR が 1 を上回っていたが，Odds では 1 を下回っていた方策が 17 方策中では，10 方策あった．RR が 1 を下回っていたが，Odds では 1 を上回っていた方策はなかった．

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．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 19 に，それぞれを散布図で表したものを図 3 に示す．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 Odds で業種による影響を確認する．図 3 の 2 つの直線で区切られた 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 Odds 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．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言える．

5. まとめ

企業の業種，企業規模毎，インシデントの漏洩原因毎での分類を行い，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．データの分類により，業種や企業規模によりインシデントの発生に偏りがあることが明らかになった．しかし，この偏りにより，マネジメントによるインシデント増加の原因が判明した．(1) 業種，(2) 企業規模，が交絡因子として働いていたためであった．

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，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．

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いたします．

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ました．

参考文献

[1] ベネッセお客様本部: 事故の概要（https://www.benesse.co.jp/customer/bcinfo/01.html, 2018.01.31 参照）
[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（http://www.gentosha.co.jp/news/n446.html, 2018.01.31 参照）
[3] 東洋経済データサービス CSR データ（https://biz.toyokeizai.net/data/service/detail/id=321, 2018.06.20 参照）
[4] 山田，池上，乾，菊池，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] 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）
[6] 東証業種別株価指数・TOPIX-17 シリーズ（http://www.jpx.co.jp/markets/indices/line-up/files/fac_13_sector.pdf, 2018.06.21 参照）

表 17 業種毎の漏洩原因別インシデント発生件数（総計）

	人的ミス	悪意のある攻撃	内部犯行	設定ミス・バグ	盗難	その他	不明	計
情報通信・サービスその他	10	11	2	1	2	0	1	27
小売	8	3	1	1	4	0	0	17
銀行	13	1	2	0	0	0	0	16
電気・ガス	10	0	0	1	2	0	0	13
電機・精密	7	1	0	3	1	0	0	12
建設・資材	6	1	1	1	0	0	0	9
素材・化学	2	3	0	1	2	0	0	8
運輸・物流	2	3	1	1	0	0	0	7
商社・卸売	1	4	1	1	0	0	0	7
金融（除く銀行）	4	0	0	0	0	0	1	5
食品	0	2	0	1	0	0	0	3
自動車・輸送機	1	0	0	2	0	0	0	3
機械	1	1	0	1	0	0	0	3
鋼鉄・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	1	0	0	0	1	0	2
計	66	31	8	14	11	1	2	133

表 18 企業規模毎の漏洩原因別インシデント発生件数（総計）

	中小企業	大企業 1	大企業 2	計
人的ミス	4	22	40	66
悪意のある攻撃	4	12	15	31
内部犯行	0	3	5	8
設定ミス・バグ	1	1	12	14
盗難	1	6	4	11
その他	0	0	1	1
不明	0	0	2	2
計	10	44	79	133

表 19 食品業を基準とした RR と Odds

業種	RR		Odds	
情報通信・サービスその他	2.034		1.752	
小売	2.662		2.471	
銀行	8.127	***	4.335	
電気・ガス	17.898	***	11.422	***
電機・精密	1.743		1.095	
建設・資材	1.606		1.250	
素材・化学	1.153		0.955	
運輸・物流	3.126		2.291	
商社・卸売	0.877		1.068	
金融（除く銀行）	2.667		1.232	
自動車・輸送機	0.883		0.716	
機械	0.733		0.803	
鋼鉄・非鉄	0.615		0.432	

表 20 業種別企業規模

	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	1227
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	1825	2649	2176	11	6661