明治大学大学院　先端数理科学研究科

2018 年度

修士学位請求論文

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

学位請求者　先端メディアサイエンス専攻

山田　道洋

目 次

第1章　序論

1.1　本研究の背景

近年，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，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て企業の社会的責任を高めることが求められている．しかし，経済産業省によって行われた平成 26 年度情報処理実態調査の結果によると，平成 25 年度の国内企業における CIO の平均設置率はわずか 29.5%であった [19]．情報セキュリティを高める方策の普及が滞っている背景には，これらの経営マネジメント方策が漏洩インシデントを本当に削減しているのか否か，その効果が不明なことが一因であった．

また，個人情報漏洩インシデントを完全に防ぐことは困難であることから，サイバー保険という商品も登場している．このような個人情報漏洩による被害額の算出にはサイバー保険の観点から大きな需要がある．Gartner 社のような IT 戦略コンサルタントは，サイバー保険を効果的に使用するためのガイドラインを提供している [16]．保険業界の予測では，2015 年の約 20 億ドルから 2025 年には約 200 億ドルまでになると予測されている [15]．英国などの各国政府は，サイバーセキュリティリスク管理の改善のためにサイバー保険市場の成長を支援している [9]．Franke は，インタビューの結果からスウェーデンのサイバー保険市場の特徴を報告している [10]．

1.2　本研究の目的

日本ネットワークセキュリティ協会（JNSA) は，2002 年に，本人の特定容易度や企業の社会的責任度から各組織が所有する個人情報の潜在的リスクを把握するためのひとつの推定手法として，想定損害賠償額算定式（JNSA Damage Operation Model for Individual Information Leak： JO モデル）を提案している [3]．JO モデルは 1 人当たりの基本情報価値を 500 円とし，氏名と住所が同時に漏れた時はその 3 倍とするなどのシンプルなルールから構成されたもので，広く知られている．しかしながら，我々は，JO モデルには次の問題点があることを指摘する．

1. 500 円，3 倍などの定数は専門家の主観で定められたものであり，その根拠が不足しており，信頼性が低い．

2. 16 年前に設計された古いモデルであり，最近の法改正などの事情が考慮されていない．

3. 予測された損害額の信頼性が不明である．

これらに対し，本研究では，2005 年からの 12 年分の 1 万 5 千件の情報漏洩事件のビッグデータを解析し，より精度の高い最新の損失額の数理モデルを定式化することを試みる．同様の先行研究に，米国の 1 万件のインシデント情報から定式化した Romanosky のモデル [5] がある．しかし，このモデルは，Advicen 社の米国のインシデントデータセットに基づいたモデルであり，日本国内のインシデントについては同様のデータセットが存在しないため，国内のケースには適用が困難と考える．

そこで，我々は，企業が公開している会計情報 [6] に注目した．大規模な漏洩インシデントが生じた時，その対応にかかるコストを特別損失に計上しているためである．こうして，漏洩した個人情報や企業規模などの情報を説明変数とし，その企業の特別損失額を目的変数として重回帰を適用し，新しい数理モデルを提案する．1 万 5 千件のインシデントに損害モデルを適用し，損失額と先行する JO モデルとの比較を示し，両者の関係を考察する．

また，個人情報漏洩などに対して，情報セキュリティマネ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が求められている．企業の情報セキュリティマネジメントシステムを審査し，国際基準と同等の基準に準拠していれば与えられる，ISMS(Information Security Management System) 認証については，佐野ら [20] による導入による効果の検証や，ISMS において必要な「情報セキュリティインシデントからの学習」の手順化を提案する先行研究 [21] が存在するが，その他のマネジメント方策の実施によって，どの程度個人情報漏洩のリスクが削減されるかの定量的な評価は行われていない．

そこで我々は，過去のインシデント発生企業の情報を元にした，個人情報漏洩の損害額の数理モデルの提案，株式会社東洋経済新報社の社会的責任投資 CSR データベースを用いた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を行う．CSR データベースより各企業のマネジメント方策の実施状況を取得し，マネジメント方策の実施によるインシデント発生リスクの削減効果を，業種別，企業規模別による相対危険度の計算，ロジスティック回帰の適用の 2 つの手法から評価する．

このように，個人情報漏洩によるリスクと，方策の効果を定量的に示すことで，企業における情報セキュリティ対策が推進されることが期待できる．

1.3 本研究の構成

本論文は 5 章により構成されている．

第 1 章においては，まず本研究の背景と目的を述べる．個人情報漏洩インシデントの例や傾向，推奨されている対策などを示す．次に，問題点を整理することで，本研究の目的を定める．現在広く知られている JO モデルで定められている定数は信頼性が不明であり，また，各種マネジメント方策の実施によるインシデント削減効果の定量的な評価が行われていない．これらを解決する本研究の着想を示す．そして，本研究の貢献について明らかにする．

第 2 章では，本論文を通して使用する基本定義を示すとともに，先行研究を整理する．第 3 章では，国内で発生した個人情報漏洩インシデントの発生情報と各企業の決算短信を用いることで，個人情報漏洩の損害額の数理モデルの提案を行う．個人情報漏洩インシデントの発生情報は，JNSA セキュリティ被害調査ワーキンググループが 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，漏えいした組織の業種，漏えい人数，漏えい経路などの分類・評価をした結果が記録されているデータセットを使用する．また，インシデントによる損失が計上されている特別損失額を各企業の決算短信から取得し，特別損失額を目的変数，重回帰を適用することで，企業で個人情報漏洩インシデントが発生した場合の損害額を見積もることができるモデルを提案する．第 4 章では，株式会社東洋経済新報社の社会的責任投資 CSR データベースを用いた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を行う．CSR データベースは株式会社東洋経済新報社が毎年，国内の上場企業及び，主要な未上場企業にアンケート調査を行い，各企業の従業員数などの基本情報や，CIO の設置をしているかどうかなどのマネジメント方策の実施状況を記録しているものである．インシデント発生の有無を目的変数，マネジメント方策の実施状況などの企業の情報を説明変数としロジスティック回帰を適用することで，マネジメント方策の実施状況の違いにより，インシデント発生の生起確率に影響があるかを明らかにする．

第 5 章では，本論文のまとめを述べ，本研究について結論づける．本研究主要な結論は次の通りである．個人情報漏洩インシデントによる損害額，インシデント発生の生起確率は企業の規模（売上高，従業員数），に強く依存して高くなる．ここで，従業員数が 10 倍になるごとに，インシデント発生の生起確率はオッズ比で 2.58 倍になる．また，CIO の設置によりインシデント発生の生起確率はオッズ比で 0.33 倍に抑えられることを明らかにした．

第2章　基本定義と従来研究

2.1　基礎定義

2.1.1　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 2.1 に示す．

2.1.1.1　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 [4] 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．

2.1.1.2　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．

表 2.1: 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

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

表 2.2: 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

表 2.3: 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

2.1.2 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 [22] 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 2.2，2.3，2.4 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 2.4 に示した 17 に絞り，調査結果を報告する．

2.2 従来研究

2.2.1 JO モデル

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，漏えいした組織の業種，漏えい人数，漏えい経路などの分類・評価を行っており,「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 [4]．2005 年から 2016 年のインシデントの統計量を表 2.5 に示す．

また，これらの情報から各企業の顧客 1 人当たりへの想定損害賠償額を算出する JNSA Damage Operation Model for Individual Information Leak（JO モデル）を提案している [3]．算出式を次に

表 2.4: 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 2.5: JNSA のデータセットの統計量

期間	レコード数	企業数	属性数	平均被害人数	平均インシデント数/年	平均想定損害賠償額（円/人）	平均想定損失額（百万円）
12 年間	15,569	8,853	25	11,764.32	1,297.42	42,361.73	460.27

示す.

$$
\begin{aligned}
\text{損害賠償額} &= \text{漏洩情報価値} \times \text{社会的責任度} \times \text{事後対応評価} \\
&= (\text{基礎情報価値} \times \text{機微情報度} \times \text{本人特定容易度}) \\
&\quad \times \text{社会的責任度} \times \text{事後対応評価} \\
&= \text{基礎情報価値}\ [500] \\
&\quad \times \text{機微情報度}\ [\max(10^{\max(x)-1} + 5^{\max(y)-1})] \\
&\quad \times \text{本人特定容易度}\ [6, 3, 1] \\
&\quad \times \text{社会的責任度}\ [2, 1] \\
&\quad \times \text{事後対応度}\ [2, 1]
\end{aligned}
\tag{2.1}
$$

ここで，[ ] 内の値は，それぞれの項目の値域である．機微情報度，本人特定容易度は漏洩した情報によって定められている，機微情報度は，3 値を取る精神的レベル x と経済的レベル y の 2 変数で与

えられる．例えば，氏名の場合，x=y=1 であるが，病名は x=1，y=2 である．本人特定容易度は

$$\text{本人特定容易度} = \begin{cases} 6 & \text{氏名 } and \text{ 住所} \\ 3 & \text{氏名 } or(\text{住所 } and \text{ 電話番号}) \\ 1 & \text{その他} \end{cases}$$

と定められている．JO モデルを用いて，2014 年に発生したベネッセコーポレーション社のインシデントによる損害額を算出すると，パラメータはそれぞれ 精神的レベル $x = 2$，経済的レベル $y = 1$，本人特定容易度 = 6，社会的責任度 = 1，事後対応度 = 1 となり，1 人当たりの損害賠償額は 33,000 円となる．同インシデントの被害人数は 4,858 万人とされており，損害賠償額は全体で 1 兆 6 千 31 億 4 千万円となる．

2.2.2 Romanosky モデル

Romanosky は Advicen 社[2]より入手した 2005 年から 2014 年のアメリカの企業の 11,705 件のインシデント情報を元に，各年に企業が被った総コストを算出するモデルを次のように提案している [5]．なお，単位は百万ドルである．

$$\begin{aligned} \log(cost_{i,t}) = \beta_0 &+ \beta_1 \cdot \log(revenue_{i,t}) + \beta_2 \cdot \log(records_{i,t}) \\ &+ \beta_3 \cdot repeat_{i,t} + \beta_4 \cdot malicious_{i,t} \\ &+ \beta_5 \cdot lawsuit_{i,t} + \alpha \cdot FirmType_{i,t} \\ &+ \lambda_t + \rho_{ind} + \mu_{i,t} \end{aligned} \tag{2.2}$$

ここで，各係数の値を表 2.6 に示す．i,t は t 年の企業 i のデータを参照すること示し，$revenue$ は収益[3]，$records$ は漏洩情報の件数を示している．$rpeat$，$lawsuit$ はブール値，$FirmType$ はダミー変数として，過去に事件を起こしているか，事件について提訴されたかどうか，政府機関か一般企業かなど，それぞれ当てはまる場合に 1，それ以外は 0 を取る．

しかし，このモデルはアメリカの企業の情報を元にした回帰式であり，日本の企業についても同じモデルが適用できるかは疑問である．

2.2.3 その他関連研究

アメリカでは，個人情報の盗難による企業および個人の損失が 2005 年には 560 億ドルとなり，35 %は企業において発生した個人情報漏洩事件によるものであった．Romanosky らは，2002 年から 2009 年の間の個人情報漏洩事件に関する法律 (data breach disclosure laws) の影響を推定した [14]。彼らは，同法の採用により，個人情報の漏えいが平均で 6.1 %減少することを報告している．[13] によると，個人が金銭的損害を被ると企業が訴訟を起こされる確率は，オッズ比で 3.5 倍高くなる．さらに，原告が金銭的損失を被った場合や，認定された集団訴訟に直面したときには訴訟が和解する割合は 30%増になることが示されている．

[2]https://www.advisenltd.com/

[3]$revenue$ には「純利益」,「歳入」などの意味があるが，本稿ではこれを「売上額」と解釈して算出する

表 2.6: Romanosky の提案モデルの各係数（一部）[5]

係数			Estimate	
定数	β_0		-3.858	*
$\log(revenue_{i,t})$	β_1		0.133	**
$\log(record_{i,t})$	β_2		0.294	***
$repeat$	β_3		-0.352	
$malicious$	β_4		-0.029	
$lawsuit$	β_5		0.444	
		Government	-1.339	
$FirmType_{i,t}$	β_6	Private	-1.032	
		Public	-0.065	

Gordon らは与えられた情報を保護するために投資する最適な金額を決定するモデルを提案している [11][12]．ここでは，企業における情報セキュリティに対する投資が，情報漏洩やサイバー攻撃から生じると予想される損失の 37 %を超えてはならないことを推奨している．

Edward らは一般的な公開データセットを研究し，ベイズの一般化線形モデルを開発してデータ侵害の傾向を調査した [17]．

佐野らは，徳島大学における ISMS 認証の導入および運用の効果について検証を行っている [20]．ISMS の導入によって，運用業務の可視化が行われ，BCP における人的リスクを抑える効果や，情報共有度の向上によるセキュリティ事象の早期把握など，インシデントを未然に防ぐ可能性を報告している．

堀川らは，ISMS において必要な「情報セキュリティインシデントからの学習」の手順化を提案している [21]．ISMS では，インシデントが発生した際に「発見された不具合の対処」と「不適合の原因を除去するための処置」を行い，処置の結果を学習することを求めている．しかし，学習の具体的な手引きは与えられていない．このため，ISMS 認証を取得してもインシデントが減らず，PCDA サイクルの改善が効果的に働いていない組織が存在する．これに対し，堀川らはインシデントデータベースを「組織全体のセキュリティ対策の改善」のために活用していくための具体的な方法・手順を「デルタ ISMS」モデルとして提案している．デルタ ISMS では，組織で実際に発生した事故データに基づきインシデントによる予想損失額，対策のコスト，対策により低下する予想損害額の割合をまとめたデルタ ISMS 表を作成し，リスクアセスメントにおいて最も投資効果の高い選択を推奨する．提案手法により提供される情報が，最高情報セキュリティ責任者（CISO）等と経営陣の間で共有すべき情報として余分がないことが報告されている．

第3章　個人情報漏洩の損害額の数理モデルの提案

3.1　提案手法

本研究では，QICK Astra Manager[6] より購入した本決算（連結優先）データの個人情報流出インシデントが発生した年の会計情報，及び，2005 年から 2016 年までの JNSA データセット [3][4] に記載されている情報漏洩インシデントのデータを使用する．日本には Advicen 社に該当する企業がない．そこで，公開されている会計情報に注目した．

JO モデルでは，インシデント 1 件ごとに想定損害賠償額を算出していたが，本研究ではインシデントが発生した年の特別損失額を目的変数として重回帰を適用する．関連研究との違いを表 3.1 に整理する．式 (2.1) と (2.2) は形式が積と和で大きく異なるように見えるが，等価な形に変形できることを 4.1 節で示す．

3.1.1　特別損失額

企業の通常の経営活動では発生しない，特別な要因によって一時的に発生した損失を特別損失という．ベネッセホールディングスは 2014 年に発生した個人情報流出事件のおわびにかかる費用などとして約 260 億円を特別損失として計上しており [7]，他の企業においてもインシデントによる損害額は特別損失として計上されると考えられる．そこで本研究では，各企業の特別損失額がそのインシデントにかかったコストを代表していると考える．

3.1.2　データのクレンジング

特別損失額には，インシデントによる損害額が計上されると考えられるが，特別損失額には「システム開発中止に伴う損失」や「事業構造改善費用」なども含まれており，特別損失額の全額がインシデントに関与しているわけではない．そこで，特別損失額，JNSA データセットに対して，重回帰を適用するための次の様にデータの加工，精査を行う．

表 3.1: 関連研究との違い

	JO モデル	Romanosky	提案モデル
y	想定損害賠償額	*cost*	漏洩損害額
被害の見積もり	専門家の経験	Advisen 社	決算短信
モデル	定数の積形式	線形式	線形式

表 3.2: アニュアルレポートの調査対象

対象年数	対象件数	対象企業数
2005-2016	105	90

3.1.2.1 年度毎のデータの集約

サイバーエージェント社では 2016 年 5 月 11 日に不正ログインが発生した後，同年 11 月 29 日に再び不正ログインが発生している．このように，同一企業にて同年度中に複数回インシデントが発生していた 21 社の,「被害人数」「漏洩原因」「漏洩情報」「事後対応度」「経済的ランク」「精神的ランク」「本人特定容易度」の項目についてデータの集約を行う．各項目の集約方法を以下に示す.

- 被害人数： 1 年間の被害人数の合計
- 漏洩原因： 「内部犯行」「不正な情報持ち出し」などの故意による漏洩が 1 件でもあったかどうか
- 漏洩情報： 1 年間で漏洩したすべての項目の和集合
- 事後対応度： 1 年間の最大値
- 経済的ランク： 1 年間の最大値
- 精神的ランク： 1 年間の最大値
- 本人特定容易度： 1 年間の最大値

3.1.2.2 アニュアルレポートの調査

インシデント 105 件の企業の決算短信，アニュアルレポートなどを被害人数の多い順の 90 社を調査した．調査対象の統計を表 3.2 に示す.

調査の結果，表 3.3 の 5 件のレポートに特別損失の内訳として「情報セキュリティー対策」と記載されていた[1]．情報セキュリティー対策と記載されていた企業名とその金額を表 3.3 に整理する．このセキュリティ対策費を真の損失額とし，特別損失額による単回帰を行ったところ，予測損害額 $= 0.849\cdot$ 特別損失額が得られた．そこで，

$$\text{漏洩損害額 } y = 0.849 \cdot \text{特別損失額}$$

と定義する．表 3.3 に示す通り，セキュリティ対策費（真値）と漏洩損害額の誤差は平均で 10.87 百万円であり，95%信頼区間は [−18.37 百万円，+40.11 百万円] である．

[1]セキ株式会社のレポートには,「昨年 9 月 15 日付で「当社お客様情報の流出に関するお詫びとお知らせ」を公表しました．その後の二次的な被害に関しましては，現在のところ報告されておりません．外部からの不正アクセスにより個人情報が外部に流出した懸念があり，それらに関わる対応費用を情報セキュリティ対策費として計上しております.」[8] というように情報流出インシデントへの補償によるものであると明記されている

表 3.3: 情報セキュリティー対策費 [百万円]

企業名	年度	セキュリティ対策費	特別損失額	0.849· 特別損失額	誤差
ベネッセホールディングス	2015	26,039	30,642	26,045.7	+6.7
セキ	2016	210.67	234	198.9	−11.77
ストリーム	2014	5.56	66	56.1	+50.54
ミサワ	2012	27.24	42	35.7	+8.46
アークン	2016	8.92	11	9.35	+0.43
平均		5,256.69	6,199.4	5,269.15	+10.87
信頼区間 (95%)					10.87 ± 29.24

表 3.4: 重回帰対象のデータセット

期間	レコード数	企業数	平均被害人数	平均売上高（百万円）	平均特別損失額（百万円）
2010-2016	144	115	356,630.2	407,317.46	5,812.27

3.1.2.3 特異なデータの除外

特別損失額は災害や社会情勢などの影響によっても増加する．2008 年に起こったリーマンショックにより多くの企業が影響を受け，2008 年前後の特別損失額が大きく増加している企業が存在していた．このようなリーマンショックによる影響を排除するため，本研究では 2010 年以降のデータを使用する．

銀行では，貸付債権と有価証券の損失を数年に渡って特別損失に乗せて計上し，ある閾値を超えた時点で急激に増額する．つまり一般の企業における特別損失額と計上年とは意味が大きく異なる．そのため，本研究では銀行のインシデントデータは除外する．

3.1.2.4 決算データを取得できないデータの除外

売上高や特別損失額は証券コードを元に取得しているため，日本年金機構や日本郵政といった証券コードのない企業や団体のインシデントデータを除外する．

3.1.3 線形重回帰モデル

以上のデータの加工，精査を行った結果データは 144 件となった．対象としたデータセットの統計を表 3.4 に示す．144 件のデータに対して，漏洩損害額 y を目的変数として重回帰を適用して得た次の線形モデルを提案する．重回帰には R の lm 関数を用いた．

$$\begin{aligned} \log(y) &= f(x_1, x_2, \cdots, x_{16}) \\ &= \beta_0 + \beta_1 \cdot \log(x_1) + \beta_2 \cdot \log(x_2) \\ &\quad + \beta_3 \cdot x_3 + \cdots + \beta_{16} \cdot x_{16} \end{aligned} \tag{3.1}$$

3.1 式の各係数と，説明変数の閾値を表 3.5 に示す．*を $p < 0.1$(有意水準 10%) とし，**を $p < 0.05$(有意水準 5%)，***を $p < 0.01$(有意水準 1%) とする．提案モデルでは売上高に高い有意差 (***) がみ

表 3.5: 提案モデルにおける係数

係数				*Estimate*	*p.value*		定義域	平均値
	β_0			-3.9632	0.0093	$***$		
	log(被害人数)	$\log(x_1)$	β_1	0.0379	0.4612			6.15
	log(売上高)	$\log(x_2)$	β_2	0.9904	$2.18E-23$	$***$		11.40
	故意	x_3	β_3	0.6261	0.6808		0,1	0.15
	事後対応度	x_4	β_4	N/A	N/A		0,1	0
	経済的ランク	x_5	β_5	0.1590	0.5025		1,2,3	1.31
	精神的ランク	x_6	β_6	0.0128	0.9772		1,2,3	1.11
	本人特定容易度	x_7	β_7	0.2079	0.6930		1,3,6	4.26
業種	不動産業	x_8	β_8	-0.0773	0.9071		0,1	0.08
	建設業			-1.4450	0.0258	$*$		0.10
	情報通信業			-0.1350	0.8014			0.19
	林業			-0.4030	0.7309			0.01
	電気・ガス			-0.9330	0.3081	$*$		0.03
	生活関連サービス業，娯楽業			-1.004	0.3771			0.01
	卸売業，小売業			-0.4550	0.4203			0.17
	医療，福祉			-0.6319	0.5045			0.03
	宿泊業，飲食サービス業			-0.4607	0.53801			0.04
	製造業			-0.7577	0.1728			0.17
	教育，学習支援業			-0.0654	0.9531			0.02
	学術研究，専門・技術サービス業			-0.1173	0.9219			0.01
	金融業，保険業			-1.7570	0.0572	$*$		0.03
	運輸業，郵便業			-0.8893	0.7994			0.03
	氏名	x_9	β_9	-0.6231	0.6007		0,1	0.82
	住所	x_{10}	β_{10}	-0.5169	0.7406		0,1	0.55
	電話番号	x_{11}	β_{11}	-0.5337	0.7562		0,1	0.51
	生年月日	x_{12}	β_{12}	-0.2348	0.5105		0,1	0.26
	性別	x_{13}	β_{13}	0.2624	0.5296		0,1	0.17
	職業	x_{14}	β_{14}	0.1453	0.7767		0,1	0.07
	メールアドレス	x_{15}	β_{15}	-0.3845	0.2318		0,1	0.46
	ID/PASS	x_{16}	β_{16}	-0.2810	0.5025		0,1	0.12

られ，漏洩損害額は売上高に強く依存している．また，建設業などの業種の一部にも有意差が見えるが，これらは対象インシデントの数が少ないことが原因である．

3.2 評価

売上高についての漏洩損害額の散布図と提案損失コストモデルの回帰直線を図 3.1 に示す．なお売上高 x_2 と漏洩損害額 y 以外の項目 $x_1, x_3, \cdots x_{16}$ には各値の平均値を入力している．

被害人数 x_1 についての漏洩損害額 y の散布図と提案損失モデルの回帰直線を図 3.2 に示す．なお被害人数と漏洩損害額以外の項目 $x_2, x_3, \cdots$ には各値の平均値を入力している．図 3.1 と比較して，被害人数 x_1 は損害額への相関が高くない．

被害人数 x_1 についての漏洩損害額の 3 つのモデルを図 3.3 に示す．JO モデルは被害人数によって

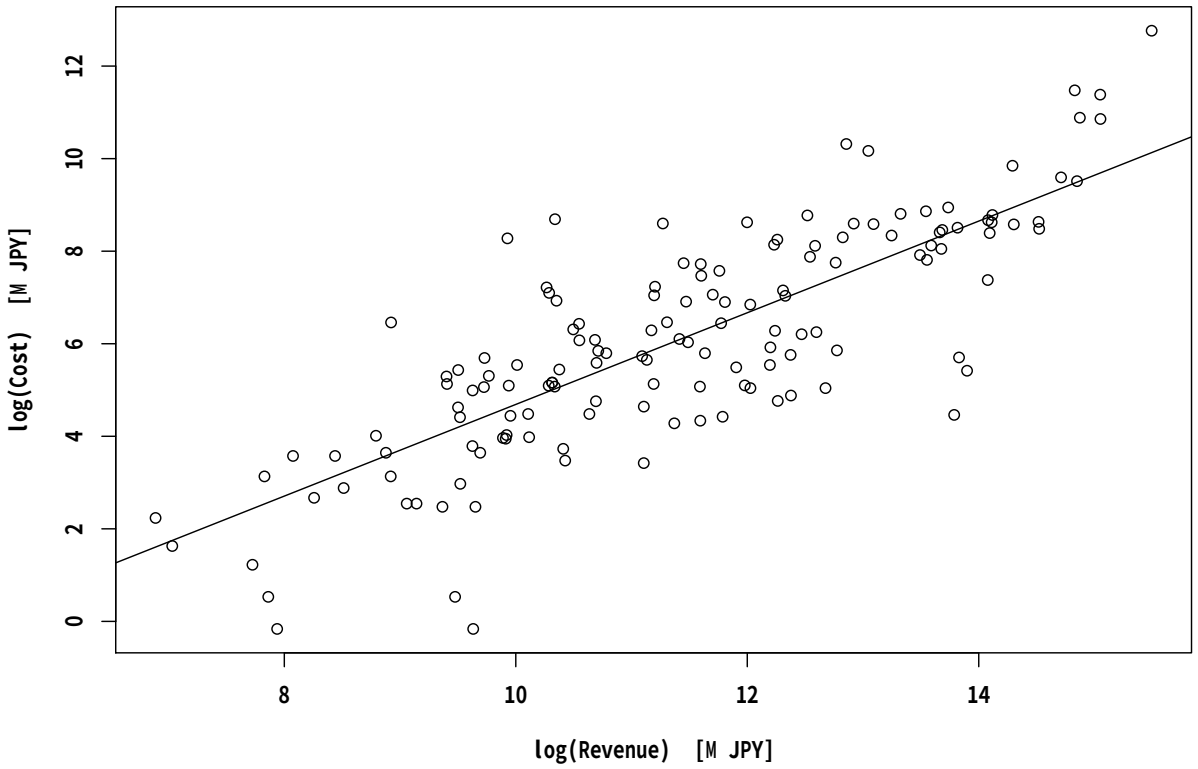

図 3.1: 売上高と漏洩損害額の散布図

損害額は比例し，影響が大きいのに比べ，提案モデルと Romanosky のモデルでは被害人数による損害額は影響が小さいことがわかる．

3.2.1 JO との比較

式（2.1）の JO モデルは，1 人当たりの賠償額が漏洩した情報によって定数倍されるモデルである．一方，提案の式（3.1）のモデルは線形式で両者は異なるように見える．しかし，提案モデルを下記のように変形することによって JO モデルと等価であることを示す．

$$\begin{aligned} y &= e^{f(x)} \\ &= e^{\beta_0+\beta_1\cdot\log(x_1)+\beta_2\cdot\log(x_2)+\beta_3\cdot x_1+\beta_4\cdot x_2+\cdots} \\ &= e^{\beta_0}\cdot e^{\beta_1\cdot\log(x_1)}\cdot e^{\beta_2\cdot\log(x_2)}\cdot e^{\beta_3\cdot x_1}\cdot\ldots \\ &= e^{\beta_0}\cdot x_1^{\beta_1}\cdot x_2^{\beta_2}\cdot e^{\beta_3\cdot x_3}\cdot\ldots \end{aligned} \tag{3.2}$$

提案モデルでの算出額と JO モデルでの想定損害賠償額の比較を表 3.6 に示す．

提案モデルと JO モデルでは算出額に大きな違いが見られ，JO モデルでは平均で約 116 億円となり，平均誤差率が 4.54 と大きな誤差が生じていた．提案モデルと漏洩損害額との平均誤差率は 1.73 となり，誤差が最小であった．

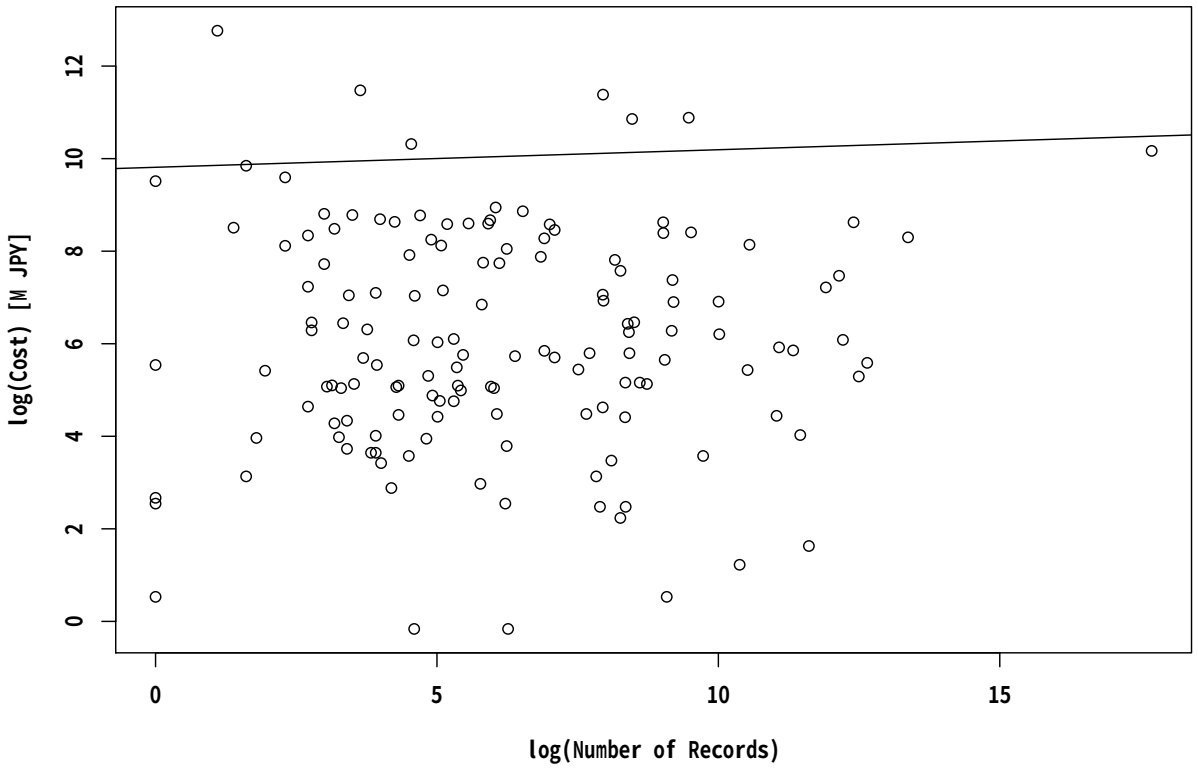

図 3.2: 被害人数と漏洩損害額の散布図

JO モデルでは経済的ランク，精神的ランク，本人特定容易度について，その段階によって 10 倍，5 倍の様に想定損害額が定数倍されていた．提案モデルで，この定数の妥当性を検討する．例えば，本人特定容易度 $x_7 = 1$ と 3 の損失額の比は

$$\begin{aligned} &\frac{f(x_1, \cdots, x_6, x_7 = 3, x_8, \cdots, x_{16})}{f(x_1, \cdots, x_6, x_7 = 1, x_8, \cdots, x_{16})} \\ &= \frac{e_0^{\beta} \cdot x_1^{\beta_1} \cdots e^{\beta_6} \cdot e^{3\beta_7} \cdot e^{\beta_8} \cdots e^{\beta_{16}}}{e_0^{\beta} \cdot x_1^{\beta_1} \cdots e^{\beta_6} \cdot e^{1\beta_7} \cdot e^{\beta_8} \cdots e^{\beta_{16}}} \\ &= \frac{e^{3\beta_7}}{e^{1\beta_7}} \\ &= e^{2\beta_7} = 1.5158 < 3 \end{aligned} \tag{3.3}$$

と算出される．すなわち，JO モデルで 3 倍としているのは，高すぎで，1.5 倍の方がより現実に近く表している．同様にして，提案モデルでの x_7 以外の経済的ランクなどが 1 段階上がった時の影響を計算することができる．それぞれの段階について提案モデルでの影響を計算した結果を表 3.7 に示す．

提案モデルではいずれの変数についても，1 段階上がった時の影響は JO モデルよりも小さい．12 年間のインシデントデータに基づき検討すると，経済的ランク，精神的ランクはいずれも損失額を 10 倍，5 倍するほど影響を及ぼしていないことがわかる．本人特定容易度については，損失に影響していると言えるがその比は JO モデルの係数の約 1/2 であった．

経済的ランク，精神的ランク，本人特定容易度がすべて 1 のインシデントのデータにより見積もっ

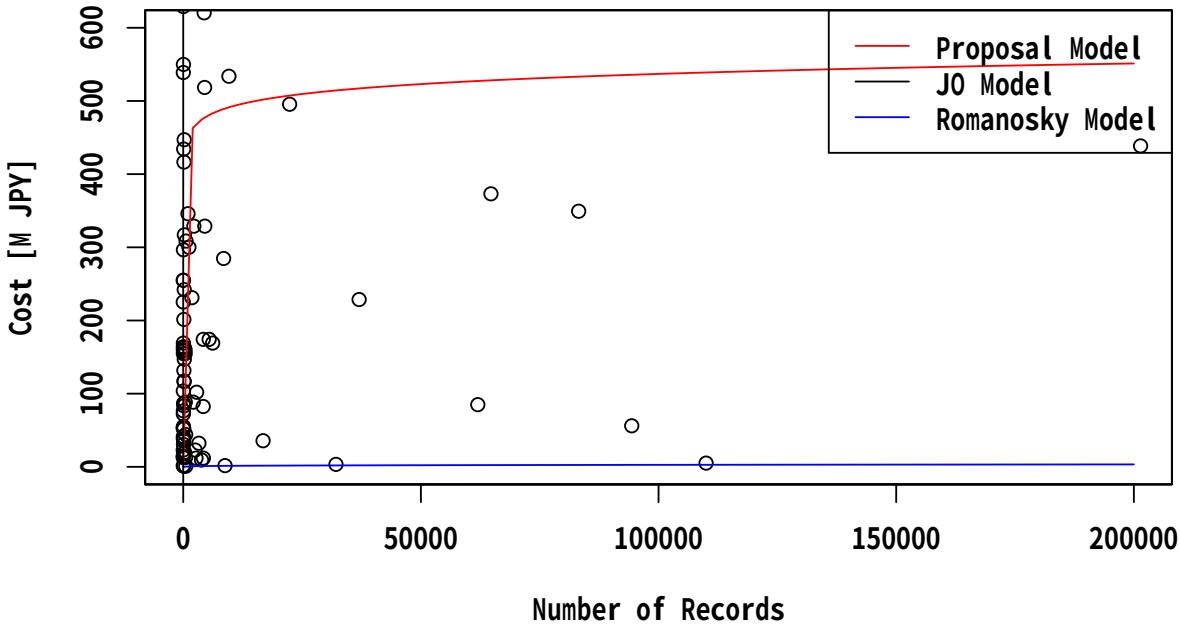

図 3.3: 被害人数と漏洩損害額の散布図：各モデルの比較

た，1 人あたりへの基礎情報価値を表 3.8 に示す．経済的ランク，精神的ランク，本人特定容易度がすべて 1 ならば，式 (2.1) より JO モデルでの 1 人あたりへの想定損失額は 500 円となるが，提案モデルでは 212,106.1 円である．この 12 年間で漏洩インシデントが企業に及ぼす影響が大きくなっていることを表している．

3.2.2 Romanosky との比較

回帰に使用したインシデントのデータに対して，Romanosky のモデルを適用した場合と提案モデルとの比較を表 3.6 に示す．また，$lawsuit_{i,t}, FirmType_{i,t}, \lambda_t, \rho_{ind}, \mu_{i,t}$ については 0 として無視している．Romanosky のモデルでは平均が 107.4 百万円と算出額が非常に小さい．Romanosky の回帰に使用したデータでは revenue の平均が 8031 百万ドルとなっている．このことから，アメリカと日本の市場規模の大きさの違いにより Romanosky のモデルが日本のインシデントに適応できていないと考えられる．

3.2.3 モデルの簡略化

3.1 式の提案線形重回帰モデルには p 値の高い変数も含められており，また，変数の数も多く複雑である．そこで，冗長な変数を削除し，損害に本質的な変数に絞りインシデント発生時の損害額をより簡単に見積もることを試みる．本研究では，モデルの簡略化の指標として，赤池情報量基準 (Akaike

表 3.6: 各モデルでの漏洩損失額（上位 20 社）

No	企業名	日付	被害人数	JO モデル	Romanosky	提案モデル	漏洩損害額	情報セキュリティ対策費
1	ベネッセホールディングス	2014/7/9	48,580,000	160,3140	2,367.6	13,287.4	26,045.7	26,039
2	セキ	2015/9/15	267,000	41,652	325.2	87.4	198.9	210.7
3	ストリーム	2014/1/30	94,359	566.2	256.6	152.9	56.1	5.6
4	ミサワ	2011/5/26	16,798	1,310.2	126.9	17.1	35.7	27.2
5	アークン	2016/1/13	3,859	23.2	66.9	4.4	9.4	8.9
6	サイバーエージェント	2016/11/29	640,368	742.2	466.4	3,532.6	4,021.4	
7	コシダカホールディングス	2014/9/17	310,000	930.0	403.7	199	266.9	
8	サイバーエージェント	2013/8/12	243,266	1,459.6	446.9	1,273.4	5,566.7	
9	パスコ	2010/3/21	201,414	9,063.6	355.0	637.1	438.6	
10	GMO インターネット	2015/2/27	188,047	1,011.3	276.5	1444.7	1752.7	
11	アミューズ	2009/8/10	148,680	11,597.0	307.1	187.9	1362.6	
12	レアジョブ	2012/5/14	110,000	330.0	182.8	7.9	5.1	
13	江崎グリコ	2016/3/7	83,194	6,489.13	361.5	1,375.6	349.4	
14	椿本チエイン	2016/11/14	64,742	194.2	311.1	612.9	373.2	
15	ホットマン	2014/7/1	61,977	1,115.6	227.8	51.9	85	
16	サイバーエージェント	2014/6/23	38,280	76.6	267.7	1,852.9	3,427.2	
17	サニーサイドアップ	2015/8/28	37,006	37	184.4	145.4	228.7	
18	リブセンス	2013/2/28	3,2132	282.8	98.2	4.6	3.4	
19	良品計画	2015/1/5	22,385	405.1	165.9	716.1	495.6	
20	学研ホールディングス	2015/7/13	22,108	132.7	205.9	509.4	1,002.2	
	平均			11,686.5	107.4	2,741.5	4,940.4	
	最大			1,603,140	2,367.6	36,953.7	349,630.7	
	最小			0.002	6.7	4.0	1.7	
	平均誤差			17,650.7	6,363.7	4,935.2		
	平均誤差率			4.54	2.50	1.73		

Information Criterion: AIC) を用いる [18]．AIC は，

$$\mathrm{AIC} = -2log(L) + 2k$$

で定められ，値が小さいほうが良いモデルとされる．ここで，L は最大尤度，k はパラメータの数をそれぞれ示す．

提案線形重回帰モデルについて，AIC を最小化する係数で定められるモデルを，

$$\hat{y} = e^{\beta_0} \cdot x_1^{\beta_1} \cdot x_2^{\beta_2} \cdot e^{\beta_8 \cdot x_8} \cdot e^{\beta_{11} \cdot x_{11}} \tag{3.4}$$

と定める．ここで，係数は表 3.9 に示す．提案モデルと，簡略化したモデルの比較を表 3.10 に示す．

表 3.7: 提案モデルとＪＯモデルの係数の比較

経済的ランク	JO モデル	10^0	10^1	10^2
	提案モデル	1	1.1723	1.3743
精神的ランク	JO モデル	5^0	5^1	5^2
	提案モデル	1	1.0129	1.0261
本人特定容易度	JO モデル	1	3	6
	提案モデル	1	1.5158	2.8291

表 3.8: 基礎情報価値（$x_5 = x_6 = x_7 = 1$ の漏洩損害額）

件数	平均被害人数	平均漏洩損害額 [百万円]	平均漏洩損害額 [円/人]
20	5,031.3	1,067.17	212,106.1

表 3.9: 簡略化モデルの係数

係数				*Estimate*	*p.value*	
β_0				-4.959	$8.08E-11$	$***$
log(被害人数)		$\log(x_1)$	β_1	$5.146E-8$	0.061	$*$
log(売上高)		$\log(x_2)$	β_2	1.005	$2E-16$	$***$
業種	建設業	x_8	β_8	-1.206	0.001	$***$
	製造業			-0.529	0.076	$*$
	金融業，保険業			-1.344	0.048	$**$
	運輸業，郵便業			-1.013	0.081	$*$
電話番号		x_{11}	β_{11}	-0.467	0.037	$**$

変数の数は 30 から 8 になり，全ての変数において p 値が有意水準を満たすようになっている．

例えば，2014 年に医学生物学研究所で発生したインシデントの場合を考えよう，被害人数 $x_1 = 50$，売上高 $x_2 = 7172$[百万円]，業種 $x_8 = (0, 1, 0, 0)$(製造業)，電話番号 $x_{11} = 0$ となり，漏洩損害額 y は，

$$\begin{aligned} y &= e^{\beta_0} \cdot x_1^{\beta_1} \cdot x_2^{\beta_2} \cdot e^{\beta_8 \cdot x_8} \cdot e^{\beta_{11} \cdot x_{11}} \\ &= e^{-4.959} \cdot 50^{5.146 \times 10^{-8}} \cdot 7172^{1.005} \cdot e^{-0.529} \cdot e^{0 \times -0.467} \\ &= 31.01[\text{百万円}] \end{aligned}$$

である．同様に提案線形重回帰モデルで漏洩損害額を計算した場合，漏洩損害額は 37.97 百万円となる．実際の漏洩損害額は 38.25[百万円] であり，簡略化モデルの誤差が大きくなっている．簡略化モデルでは表 3.10 より，平均の予想損害額が小さくなり，平均誤差は提案モデルと比べて大きくなったが，平均誤差率は同等となった．

3.3 考察

JO モデルの算出額と本研究で使用したインシデントデータとの比較の結果，現実の損失額とに大きな差があることが明らかになった．表 3.6 のベネッセホールディングスの例で言うと JO モデルでは想定損害賠償額の誤差率は 60.6 であったが，提案モデルでは 0.49 となり，誤差が非常に小さい．平

表 3.10: 線形重回帰モデルと簡略化モデルの比較

	線形重回帰モデル	簡略化モデル
AIC	122.011	85.758
パラメーター数	30	8
平均予想損害額	2,741.46	2,068.35
平均誤差	4,935.22	5,247.10
平均誤差率	1.73	1.73

均誤差率を見ても，JO モデルで 4.54，提案線形重回帰モデルで 1.73 である．漏洩損害額は，企業が実際に計上した損失を基に算出しているが，JO モデルではその金額よりを大きく上回る損害額を算出してしまう．このことから，個人情報漏洩インシデント発生時の損害額は JO モデルで見積もった時代のものから大きく変わっていることが示唆される．

また，算出額を被害人数で割った 1 人当たりの損害額は JO モデルでは 33,000 円なのに対して，提案モデルでは約 273 円であった．しかし，表 3.8 から平均の 1 人当たりの漏洩損害額をみると提案モデルは非常に高額である．これは提案モデルが企業の売上高に大きく依存しているため，売上高が大きく被害人数の少ないケースに適応できていないためであると考えられる．

第4章　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

4.1　分析

4.1.1　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し，データを以下の 3 種類で分類し分析を行う．

- 企業の業種
- 企業の規模
- インシデントの漏洩原因

4.1.2　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 4.1 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，

$$RR(M) = \frac{Pr(\text{インシデント}\,|M)}{Pr(\text{インシデント発生})} = \frac{a/m_1}{n_1/N} \tag{4.1}$$

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

表 4.1: 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	$\overset{m_1}{(a+b)}$
M・No	c	d	$\overset{m_2}{(c+d)}$
計	$\overset{n_1}{(a+c)}$	$\overset{n_2}{(b+d)}$	N

表 4.2: 2014 年に CIO を設置している企業数

CIO 設置の有無	インシデント・Yes	No	計
Yes	13	357	370
No	14	921	935
計	27	1278	1305

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，

$$\chi^2 = \frac{N(|ad - bc| - \frac{N}{2})^2}{n_1 n_2 m_1 m_2} \tag{4.2}$$

で与えられる．例えば，2014 年に CIO の設置をしていた企業数が表 4.2 で与えられた時，RR（M_{CIO}）は，

$$RR(M_{\mathrm{CIO}}) = \frac{13/370}{14/935} = 4.37 \tag{4.3}$$

となる．また，カイ 2 乗検定による p 値は 0.037 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 CIO を設置することは，インシデントの件数を増加させていると結論付ける．

4.1.3 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

$$p_{iy} = \frac{1}{1 + e^{-z_i}} \tag{4.4}$$

で表す．ここで，

$$z_i = \alpha + \beta_i b_i + \beta_y c_y + \beta_d d_i + \beta_{x_1} x_1 + \cdots + \beta_{x_m} x_m \tag{4.5}$$

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，$\ldots$，x_m の交絡因子の影響を調整したオッズ比 (adjusted Odds Ratio) は，

$$OR = e^{\beta_{x_1}} \tag{4.6}$$

で与えられる．表 4.1 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，

$$OR = \frac{a/b}{c/d} = \frac{p}{1 - p} \tag{4.7}$$

である．$a << b$ で $a + b \approx b$ が言えるとき，M なしの群に対する M の相対危険度 RR は，

$$\frac{a/(a+b)}{c/(c+d)} \approx \frac{a/b}{c/d} = OR \tag{4.8}$$

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．

4.1.4 分析結果

4.1.4.1 CSR 記載のインシデント発生企業数

各年のマネジメント実施企業数とインシデント発生企業数の一部を表 4.3 に示す．ISMS(Information Security Management System) 認証とは企業の情報セキュリティマネジメントシステムを審査し，国際基準と同等の基準に準拠していれば与えられる．CSR データセット記載企業の ISMS 認定の取得率は全体で平均約 15 %，CIO の設置率は約 28 %だった．表 4.4 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．インシデント発生数は，ISMS 認定取得企業では平均約 5 件のインシデントが毎年発生しているが，CIO 設置企業では隔年でインシデント発生企業数が増減している．

表 4.3: 各年のマネジメント実施企業数とインシデント発生企業数

質問項目	2013		2014		2015		2016		2017	
	全体	インシデント発生	全体	インシデント発生	全体	インシデント発生	全体	インシデント発生	全体	インシデント発生
環境監査の実施状況	715	8	706	17	693	14	714	18	713	12
環境マネジメントシステムの構築	713	10	704	17	687	14	697	18	694	12
内部告発窓口（社内）の設置	1010	15	998	24	995	22	1040	27	1043	20
内部告発窓口（社外）の設置	568	11	644	19	700	15	791	16	840	15
内部統制委員会の設置	621	5	597	12	592	13	596	11	591	9
業務部門から独立した内部監査部門の有無	823	14	904	22	945	21	1001	26	1014	19
ＣＩＯの有無	371	4	370	13	373	5	397	11	390	5
情報システムに関するセキュリティポリシー	982	15	973	24	971	22	1000	25	1008	18
情報システムのセキュリティに関する内部監査	843	14	842	19	857	20	898	24	906	16
情報システムのセキュリティに関する外部監査	626	11	627	14	641	14	671	17	673	12
ISMS 認証	194	6	194	6	197	5	204	4	210	4

表 4.4: 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

表 4.5: 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	***

4.1.4.2　全体でのインシデント発生企業

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 4.5 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．しかし，カイ 2 乗検定による有意差は見られなかった．

4.1.4.3　業種毎のインシデント発生率

表 4.6 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 [23]．表 4.6 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．

表 4.6: 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

総計の業種毎での RR とカイ 2 乗検定の結果を表 4.7 に示す.[1]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 4.7: 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

[1] 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 4.8: 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

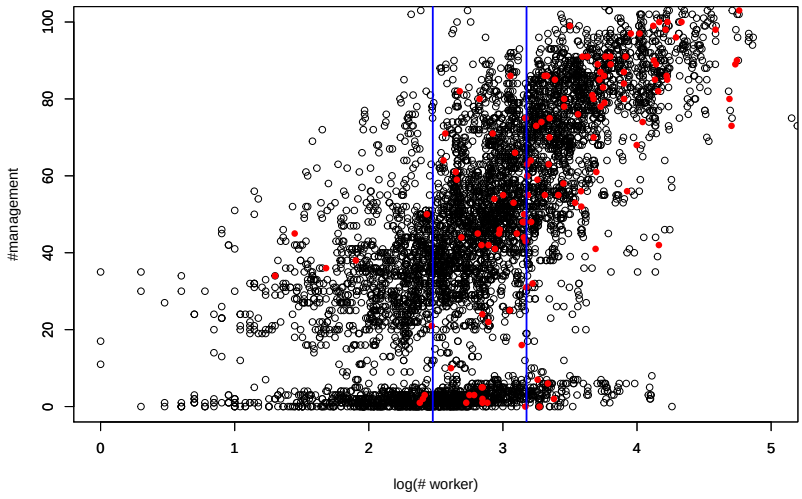

図 4.1: 従業員数とマネジメント方策実施数の散布図

4.1.4.4 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 4.8 に示す．従業員数と，実施マネジメント方策数の関係を図 4.1 に示す．黒い点はインシデント未発生の企業を，赤い点はインシデント発生企業をそれぞれ示し，青い線は，中小企業，大企業 1，大企業 2 の境界を示す．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，従業員数とマネジメント方策実施数が比例していることがわかる．

ISMS 取得企業の散布図を図 4.2 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 4.9 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．

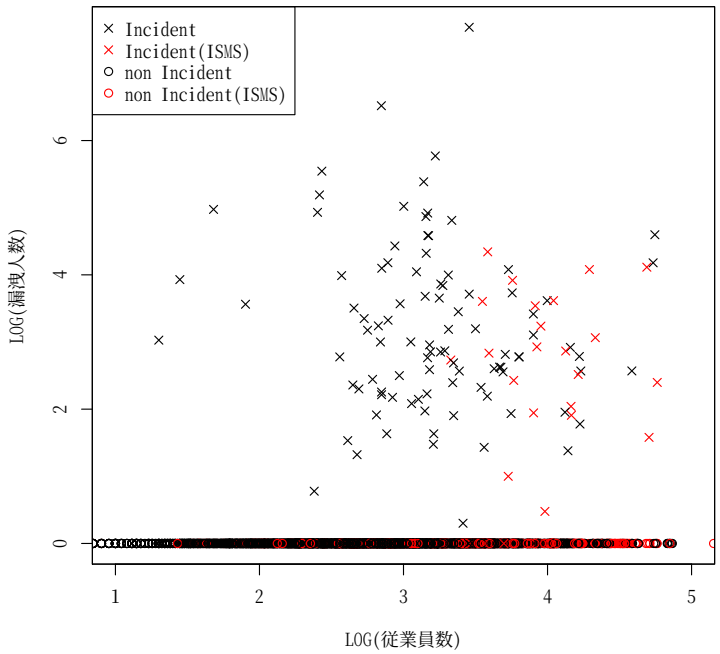

図 4.2: ISMS 取得企業の散布図

4.1.4.5　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 4.10 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 4.11 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 4.3 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 4.12 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．

4.1.5　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 4.13 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

表 4.9: 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 ***

表 4.10: 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		

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．

4.1.6 マネジメント方策導入タイミング

インシデント発生企業の内，CSR データベースの 5 年の間にマネジメント方策の実施を開始した企業数と，インシデント発生タイミングをマネジメント方策実施開始前，開始年，開始後の 3 段階で

表 4.11: 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

表 4.12: 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

分類した結果を，表 4.14 に示す．なお，複数回インシデントが発生している企業があるため，インシデント発生タイミングの合計と 5 年間でマネジメント方策を開始した企業数が合わない項目も存在する．今回集計した 4 項目中 3 項目で，マネジメント方策開始年にインシデントが発生していた．このようにインシデント発生年とマネジメント方策導入年が同年のケースが多い場合，ある時にインシデントが発生し，それを受けて方策，例えば，ISMS を導入した可能性がある．このように両者が同じ年で生じると，ISMS によってインシデントの件数が増加したと解釈してしまう．

4.2 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 4.15，表 4.16 に示す．業種毎の企業規模別企業数を表 4.18 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 4.18 より，どちらの業種も

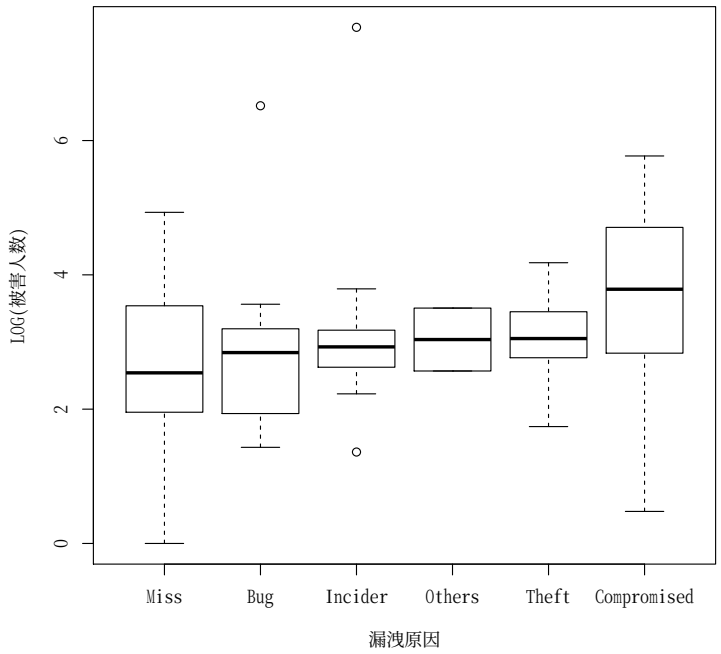

図 4.3: 漏洩原因別被害人数の箱ひげ図

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 4.5 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 4.17 に，それぞれを散布図で表したものを図 4.4 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 4.4 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

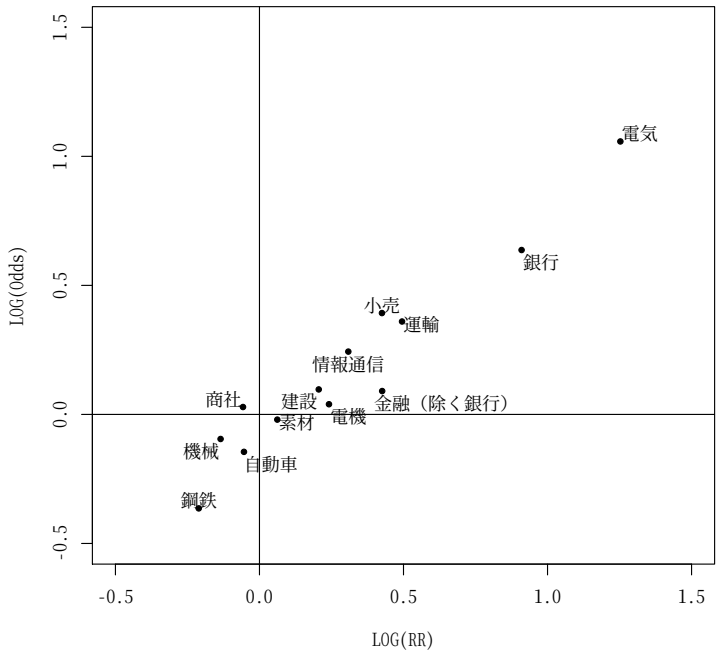

図 4.4: 食品業を基準とした RR と Odds の散布図

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．

表 4.13: ロジスティック回帰の結果（一部）

		Estimate	Std.E*RR*or	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

表 4.14: マネジメント方策導入とインシデント発生タイミング

質問項目	5 年間で開始した企業数	インシデント発生タイミング		
		開始前	開始年	開始後
CIO 設置	10	2	5	2
ISMS 認定	6	3	4	0
内部告発窓口 (社内) の設置	7	2	4	3
情報セキュリティに関する内部監査	7	3	1	3

表 4.15: 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 4.16: 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 4.17: 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 4.18: 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

第5章　まとめ

本稿では，個人情報漏洩の損害額の新しい数理モデルの提案を行い，(1) インシデント発生企業の情報を説明変数として重回帰を適用，(2)2010 年から 2016 年のインシデント情報を使用，(3) 特別損失額を目的変数として利用，を行うことで，先行研究よりも実際の損害額に近い金額を算出できるモデルを作成した．提案線形重回帰モデルの重み付き平均誤差率は 1.73 であった．ベネッセ社の 1 人当たりの損害額は 273 円であり，より現実的なモデルであることを示した．

また，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．

さらに，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り，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．

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, 2017.01.31 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, 2017.01.31 参照）.

[3] 日本ネットワークセキュリティ協会: 2016 年 情報セキュリティインシデントに関する調査報告書 ～個人情報漏えい編～（http://www.jnsa.org/result/incident/, 2018.02.01 参照）.

[4] 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）.

[5] Sasha Romanosky, “Examining the costs and causes of cyber incidents”, Journal of Cybersecurity, 2(2), pp.121-135, 2016.

[6] 本決算（連結優先）データ, 株式会社 QUICK Astra Manager, http://biz.quick.co.jp/lp_astram/.

[7] 日経新聞: ベネッセＨＤ最終赤字 136 億円　情報漏洩で特損 260 億円（https://www.nikkei.com/article/DGXLASGD31H1G_R30C14A7EA2000/, 2018.02.05 参照）.

[8] セキ株式会社: 平成 28 年度 3 月期決算短信, pp.2 （https://www.seki.co.jp/material/dl/ir/kessan/20160506_LdfbMJKUnbPG.pdf, 2018.02.05 参照）.

[9] CabinetOffice, Cyber insurance market: joint government and industry statement. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/371036/Cyber_Insurance_Joint_Statement_5_November_2014.pdf, 2014.

[10] U. Franke, “The cyber insurance market in sweden, Computers & Security”, 68:130-144, 2017.

[11] L. A. Gordon, and M. P. Loeb, “The economics of information security investment”, ACM Trans, Inf. Syst. Secur., 5(4):438457, 2002.

[12] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and L. Zhou, “Increasing cybersecurity investments in private sector firms”, Journal of Cybersecurity, 1(1):317, 2015.

[13] S. Romanosky, D. Hoffman, and A. Acquisti, “Empirical analysis of data breach litigation”, Journal of Empirical Legal Studies, 11(1):74104.

[14] S. Romanosky, R. Telang, and A. Acquisti, “Do data breach disclosure laws reduce identity theft?”, Journal of Policy Analysis and Management, 30(2):256286, 2011.

[15] A. Wells, and S. Jones, “Growth in cyber coverage expected as underwriting evolves”, 2016.

[16] J. Wheeler, and L. Akshay, “Understanding when and how to use cyberinsurance effectively”, PE Proctor 2015 Technical report, 2015.

[17] B. Edwards, S. Hofmeyr, and S. Forrest, “Hype and heavy tails: A closer look at data breaches. Journal of Cybersecurity”, 2(1):314, 2016.

[18] 金明哲,R によるデータサイエンス, 森北出版株式会社,pp.146, 2007.

[19] 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 (http://www.meti.go.jp/)

[20] 佐野雅彦，八木香奈枝，上田哲史，徳島大学情報センターにおける ISMS の効果，学術情報処理研究，18 巻，1 号，pp. 90-98，2014.

[21] 堀川 博史，大谷 尚通，橋 雄志，加藤 岳久，間形 文彦，勅使河原 可海，佐々木 良一，西垣 正勝，デルタ ISMS モデルの提案—事故データベースに基づく全社的情報セキュリティマネジメントの強化，情報処理学会論文誌，57 巻 9 号，pp.2099-2109，2016.

[22] 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)

[23] 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)

謝辞

本論文は筆者が明治大学大学院先端数理科学研究科先端メディアサイエンス専攻博士前期課程に在学中の研究成果をまとめたものである．本研究を遂行するにあたり多くの方々から多大なる御指導と御援助を賜りました．

特に，明治大学総合数理学部先端メディアサイエンス学科の菊池浩明教授には，優柔不断で研究テーマを迷いつづけていた著者を暖かく見守り続け，本論文を完成に導いていただきました．深く感謝申し上げます．

本論文に有益なご助言を賜りました，明治大学の乾孝治教授，松山直樹教授に深く感謝申し上げます．

合同ゼミにおいて何度も有益なご討論，ご助言をいただいた静岡大学創造科学技術大学院西垣正勝教授，静岡大学情報学部情報科学科講師大木哲史先生，東京電機大学理工学部理工学科情報システムデザイン学系助教　稲村勝樹先生に心から感謝致します．

新原功一氏は，研究者として，また著者が今後目指すべき社会人としての姿勢を見せていただきました．心から感謝をしています．

明治大学池上和輝氏は，共同研究者として献身的に支援していただきました．持ち前の明るい性格のおかげで，前向きに研究を進めることができました．深く感謝申し上げます．

さらに，明治大学菊池研究室の皆様に感謝を申し上げます．

最後に，修士課程に進学する機会を与えてくださり，暖かく見守ってくれた両親，実家へ帰省するたびに大きな鳴き声と共に出迎えてくれた愛犬セサミとあずきに深く感謝します．ありがとうございました．

業績

学術論文誌

1. 新原，山田，菊池，共有アカウント利用時における不正行為の誘発要因，情報処理学会論文誌，Vol．58 No．12，pp．1875-1889，2017．
2. 滋野，山田，菊池，坂本，オノマトペ CAPTCHA の開発と評価，情報処理学会論文誌，Vol．59，No．9，1666-1677，2018．

国際会議

1. M. Yamada, K. Niihara, H. Kikuchi, “Decision Tree Analysis on Environmental Factors of Insider Threats”, HCII Posters 2017, Part II, CCIS 714, pp. 658662, 2017.
2. K. Niihara, M. Yamada, H. Kikuchi, “Sharing or Non-sharing Credentials: A Study of What Motivates People to Be Malicious Insiders”, HAS 2017, LNCS 10292, pp. 353365, 2017.
3. M. Yamada, R. Shigeno, H. Kikuchi, M. Sakamoto, Evaluation and Development of Onomatopoeia CAPTCHAs, pp.370-371, 2018.
4. M. Yamada, H. Kikuchi, N. Matsuyama, K. Inui, Mathematical Model to Estimate Loss by Cyber Incident in Japan, Information Systems Security and Privacy 2019, 2019. (採録済み)

国内研究会投稿論文

1. 新原功一，山田道洋，菊池浩明，共有アカウントは内部不正を誘発するか?，Computer Security Symposium 2016，pp．617-624，2016．
2. 新原功一，山田道洋，菊池浩明，共有アカウントは内部不正を誘発するか?(2)，2017 Symposium on Cryptography and Information Security，1F1-1，2017．
3. 山田道洋，新原功一，菊池浩明，内部犯行を誘発する環境の決定木分析，情報処理学会 第 79 回全国大会，5W-02，pp．3_599-3_600，2017．
4. 滋野莉子，山田道洋，山口通智，菊池浩明，坂本真樹，オノマトペ CAPTCHA の開発と評価，DICOMO2017，pp．1778-1785，2017．

5. 山田道洋，小池倫太郎，菊池浩明，黄緒平，RIG Exploit Kit における攻撃傾向の調査，Computer Security Symposium 2017，pp．357-363，2017.

6. 滋野莉子，山田道洋，菊池浩明，坂本真樹，オノマトペ CAPTCHA の開発と評価：日英の比較，第 22 回 曖昧な気持ちに挑むワークショップ，2017.

7. 山田道洋，菊池浩明，松山直樹，乾孝治，個人情報漏洩の損害額の新しい数理モデルの提案，情報処理学会，CSEC 研究会，CSEC80，pp．1-7，2018.

8. 山田道洋，池上和輝，菊池浩明，乾考治，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．**（CSEC 優秀研究賞受賞）**

9. 山田道洋，池上和輝，菊池浩明，乾考治，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 (2)，Computer Security Symposium 2018，pp．376-384, 2018.

10. 池上和輝，山田道洋，菊池浩明，企業プレスリリースからのサイバーインシデント情報の自動収集と分析，情報処理学会 第 81 回全国大会，1ZA-08，2019．（発表予定）