2019年2月1日

修士論文発表会

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

山田　道洋

菊池研究室

本稿の構成

1. 序論
2. 基礎定義
3. 個人情報漏洩の損害額の数理モデルの提案
4. 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
5. まとめ

はじめに

ベネッセＨＤ最終赤字136億円　情報漏洩で特損260億円
４～６月

2014/7/31付

保存　共有　印刷　その他

ベネッセホールディングスが31日発表した2014年４～６月期の連結決算は、136億円の最終赤字になった。前年同期は26億円の最終黒字で、４～６月期として初の最終赤字になる。通信講座などの顧客情報の漏洩で、おわびにかかる費用など260億円の特別損失を計上した。問題が業績に与える影響を見積もれないとして、15年３月期の業績予想を取り下げた。

- 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発生している（2016年には468件）
  - ベネッセコーポレーション社（2014 年）：業務委託先の元社員が約3504万件の個人情報を名簿業者3社へ売却
    - » 約260億円の損失
- セキュリティ保険の登場

- セキュリティ上の脅威に対して，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

研究目的

- 企業で個人情報漏洩インシデントが発生した場合の損失額の算出
- 企業が行っているマネジメントと，その実施によるインシデント発生の関係を明らかにする
  - 企業がマネジメント方策を実施することによってインシデントは減少するか？
    - » CIOの設置
    - » ISMS認証の取得
    - » 内部告発窓口の設置
    - » etc…

本研究のアプローチ

- データセット取得

A インシデント データセット
- JNSA
- SecurityNext

×

B マネジメント状況 データセット
- 東洋経済CSR

- マネジメント方策とインシデント発生の関係
  - ❑相対危険度と確率検定
  - ❑ロジスティック回帰分析

A. インシデントデータ

- JNSAインシデントデータセット
  - 日本ネットワークセキュリティ協会（JNSA）の セキュリティ被害調査ワーキンググループ
  - 新聞やインターネット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文書の情報
- Security Nextデータセット
  - 脆弱性やインシデントのニュースを掲載しているサイトSecurityNext*
  - サイトにて，情報漏洩事件・事故に分類された記事を精査

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

* http://www.security-next.com/

東洋経済CSRデータ

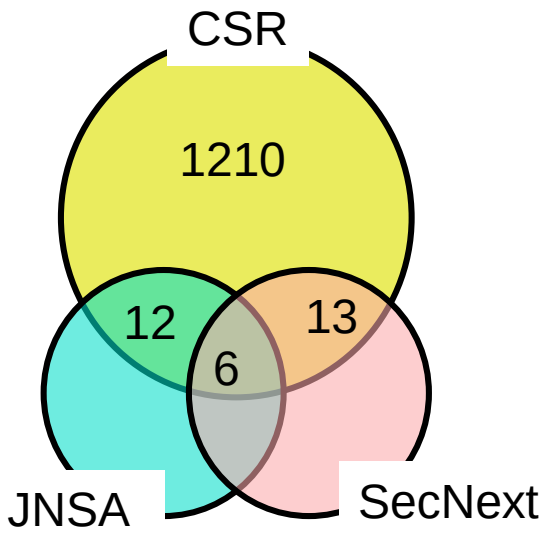
- 株式会社東洋経済新報社は，上場,主要未上場企業1400社に800項目の調査票を送付

雇用編		CSR全般		環境	
Q1	従業員数、年齢、勤続年、給与	Q1	CSR全般を統括する部署	Q1	環境対策を統括する部署
Q2	離職者	Q2	CSR担当役員	Q2	環境担当役員
Q3	従業員の世代分布	Q3	CSR活動の基本的方針姿勢	Q3	環境報告書
Q4	30歳賃金	Q4	IR、消費者対応等の各専任部署	Q4	環境会計
Q5	残業時間、手当て	Q5	社会貢献活動支出、政治献金等	Q5	環境会計の主要なコスト
Q6	役職登用状況	Q6	各種制度	Q6	環境監査
Q7	多様な人材の能力活用	Q7	NPO、NGOとの連携	Q7	環境マネジメントシステム
Q8	障害者雇用	Q8	ESGの情報開示、ファンド等組入	Q8	ISO14001認証取得事業割合
Q9	有給休暇	Q9	CSR関連行動基準への参加状況等	Q9	CO2排出量の削減中期計画
Q10	労働安全衛生の取り組み	Q10	CSR調達	Q10	環境対策
Q11	入社3年後在籍状況	Q11	内部告発	Q11-13	グリーン購入
Q12-13	社内制度	Q12	対応マニュアル	Q14	環境ラベリングの取り組み
Q14	産休、育休、介護休業等	Q13	ISO9000S	Q15	環境リスクマネジメント
Q15	両立支援	Q14	内部統制	Q16	環境関連法令の有無
Q16-17	採用	Q15	リスクマネジメント	Q17	表彰事例
Q18	人権・労働問題	Q16	企業倫理方針と倫理行動規定・規範マニュアル	Q18	気候変動や生物多様性など環境への影響

データの照合

- CSR データセットとJNSA とSecurityNextのインシデント情報を照合する
  - JNSAデータセット内でCSR記載企業のインシデント情報
  - JNSAデータセットとSecurityNextデータセットのインシデントの被り

	2013	2014	2015	2016	2017
CSR記載企業数	1210	1305	1325	1408	1413
JNSA	12	19	21	25	-
SecurityNext	13	17	23	28	24
JNSA SecurityNextの被り	6	9	16	23	0
使用インシデント件数	19	27	28	30	24



分析手法(1):相対危険度

	インシデント発生	なし	計	発生率
ISMS認証	25	974	999	0.025
なし	99	5563	5662	0.017
計(5年間)	124	6537	6661	0.018

発生率増加

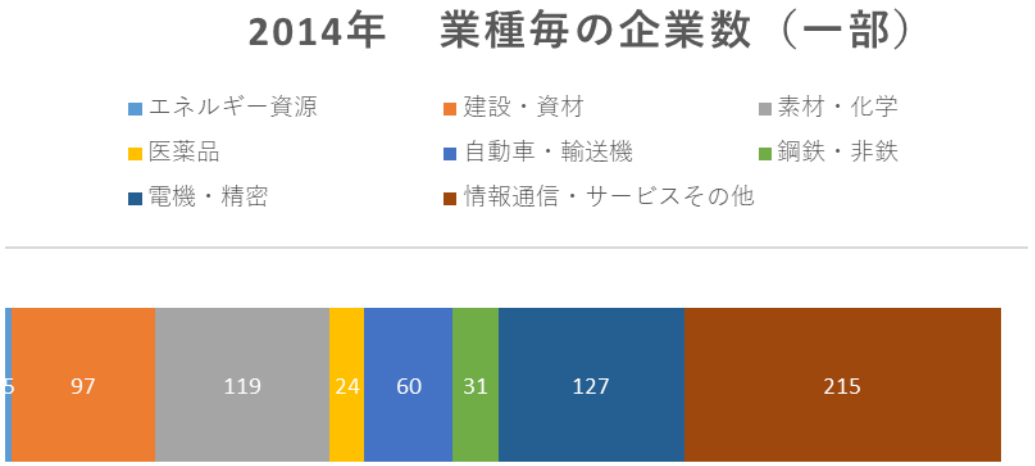
$$\text{相対危険度 Relative Risk (RR)} = \frac{\text{ISMS認証の時のインシデント発生率}}{\text{全体のインシデント発生率}} = \frac{0.025}{0.018} = 1.30$$

分析結果（1）：相対危険度

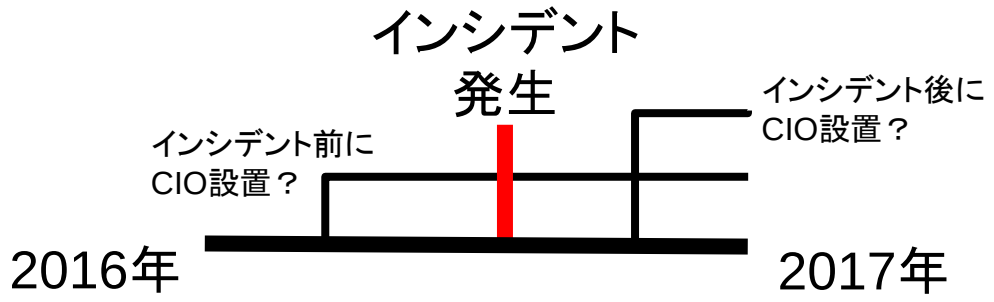
全企業数	6661	124			
質問項目	全体	インシデント発生	RR	p値	
環境監査	3541	71	1.043	0.597	
環境マネジメントシステム	3495	62	0.923	0.356	
内部告発窓口（社内）	5086	111	1.136	0.005	***
内部告発窓口（社外）	3543	73	1.072	0.379	
内部統制委員会	2997	53	0.920	0.410	
内部監査部門	4687	105	1.166	0.004	***
CIO	1901	40	1.095	0.493	
情報システムに関するセキュリティポリシー	4934	107	1.129	0.013	**
ISMS認証	999	25	1.302	0.147	

相対リスク増加の原因

- 仮説
  1. マネジメントによりインシデント検出精度が高まった
  2. マネジメント導入タイミング
  3. 業種の偏りの影響
  4. マネジメント疲れ



設置タイミングが不明



分析手法（2）：ロジスティック回帰

- RRに含まれる交絡因子（業種，企業規模，年）を排除し，マネジメントの効果を測る
- ある企業iのy年のインシデントの生起確率 $p_{iy} = \frac{1}{1+e^{-z_i}}$
  - $z_i = \alpha + \beta_{b_i} b_i + \beta_{c_y} c_y + \beta_{d_i} d_i + \beta_{x_1} x_1 + \cdots + \beta_{x_m} x_m$
    - » b_i：業種，c_y：年，d_i：企業規模，x_m：マネジメントmを実施しているかどうか
  - ここで，x_1について他の変数の影響を調整したオッズ比(adjusted Odds Ratio)は

$$OR = \frac{\exp(\alpha + \beta_{b_i} b_i + \beta_{c_y} c_y + \beta_{d_i} d_i + \beta_{x_1} * 1 + \cdots + \beta_{x_m} x_m)}{\exp(\alpha + \beta_{b_i} b_i + \beta_{c_y} c_y + \beta_{d_i} d_i + \beta_{x_1} * 0 + \cdots + \beta_{x_m} x_m)} = e^{\beta_{x_1}}$$

分析結果（2）：ロジスティック回帰

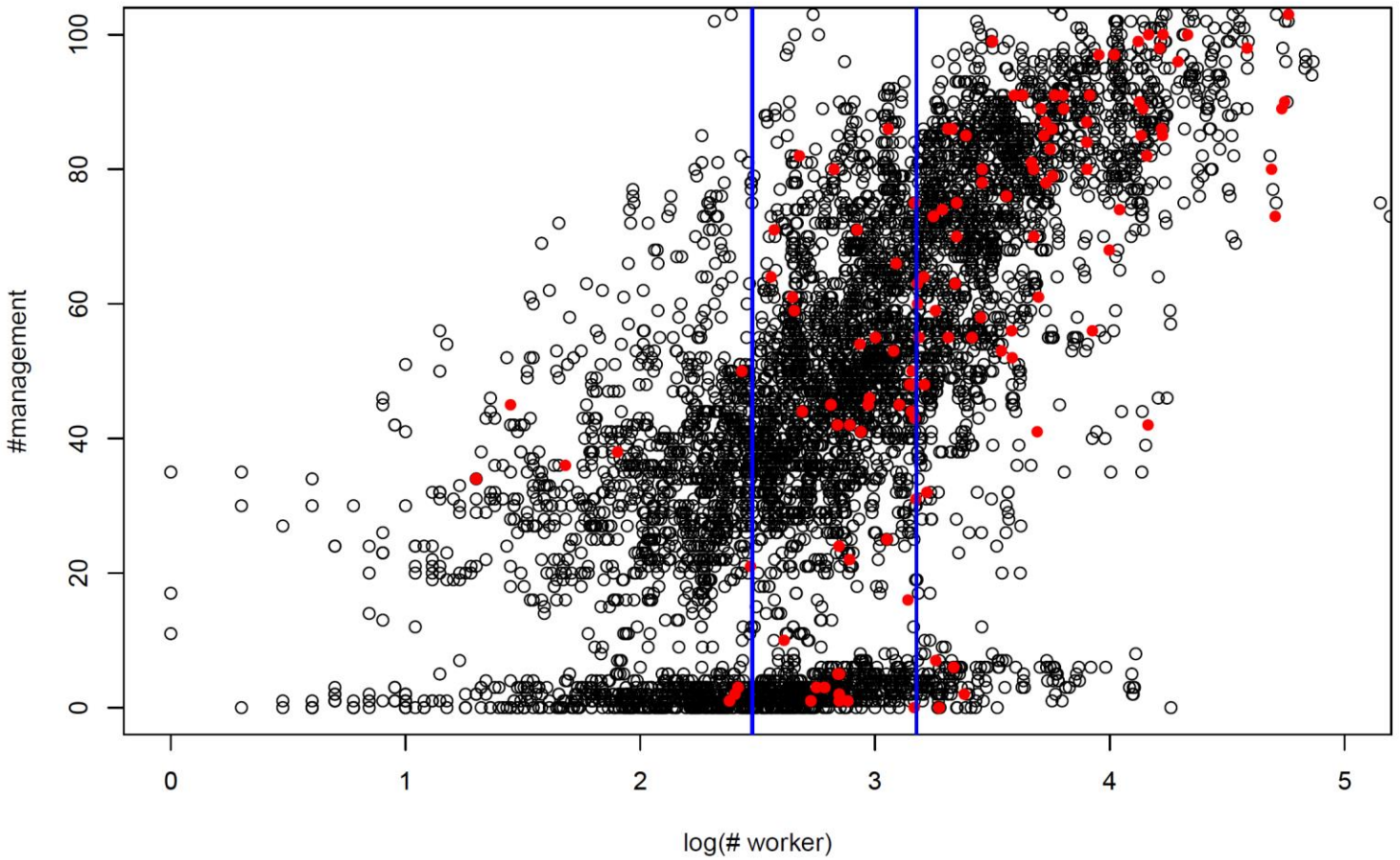
	Estimate	Pr(>|z|)	OR	
(Intercept)	-8.300	0.000	0.000	***
LOG(従業員数)	0.948	0.000	2.580	***
建設・資材	0.223	0.780	1.250	
素材・化学	-0.046	0.952	0.955	
自動車・輸送機	-0.334	0.734	0.716	
鋼鉄・非鉄	-0.838	0.527	0.432	
電機・精密	0.091	0.910	1.095	
情報通信・サービスその他	0.561	0.448	1.752	
電気・ガス	2.436	0.008	11.422	***
運輸・物流	0.829	0.332	2.291	
商社・卸売	0.066	0.938	1.068	
小売	0.904	0.231	2.471	
銀行	1.467	0.078	4.335	
金融（除く銀行）	0.209	0.819	1.232	
機械	-0.219	0.812	0.803	

	Estimate	Pr(>|z|)	OR	
告発保護	0.520	0.462	1.683	
内部統制委員会	-0.025	0.922	0.975	***
CIO	-1.097	0.001	0.334	**
CFO	0.655	0.040	1.925	
PP	0.608	0.302	1.837	
SP	-0.668	0.271	0.512	
内部監査	-0.207	0.580	0.813	
外部監査	0.117	0.674	1.124	
ISMS	-0.217	0.513	0.805	
内部窓口	-0.050	0.947	0.951	
外部窓口	-0.685	0.021	0.504	**
独立監査	-0.557	0.247	0.573	
RM･CM	1.181	0.096	3.259	
RM･CMP	-0.279	0.656	0.756	
環境監査	-0.844	0.106	0.430	
環境M	-1.619	0.002	0.198	***
労働M	0.044	0.882	1.046	

交絡因子1:企業規模

企業規模	企業数	インシデント数	インシデント発生率[%]
中小企業	1825	9	0.5
大企業1	2649	42	1.6
大企業2	2176	76	3.5
計	6661	127	

※中小企業:従業員数< 300,
大企業1:従業員数< 1500,
大企業2:従業員数≥ 1500



- 企業規模が大きくなるにつれて，インシデント数が増加

交絡因子2：業種（電気・ガス）

業種	企業数	インシデント数	インシデント発生率[%]
情報通信・サービスその他	1227	26	2.1
銀行	189	16	8.5
小売	541	15	2.8
電機・精密	661	12	1.8
電気・ガス	59	11	18.6
建設・資材	538	9	1.7
素材・化学	666	8	1.2
運輸・物流	215	7	3.3
商社・卸売	657	6	0.9
金融（除く銀行）	180	5	2.8

業種毎の企業規模

	中小企業	大企業1	大企業2	計
情報通信・サービスその他	443	465	319	1227
銀行	2	66	121	189
小売	196	222	123	541
電機・精密	126	258	277	661
電気・ガス	5	0	54	59
建設・資材	114	208	216	538
素材・化学	153	327	186	666
運輸・物流	67	66	82	215
商社・卸売	286	321	49	657
金融（除く銀行）	71	54	55	180
食品	55	136	97	288

まとめ

- 交絡因子を考慮し，マネジメント方策実施によるインシデント抑制効果を調査した
  - 今回注目した17方策の内，11方策でインシデントが抑制されていることが明らかになった
    - » 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0.3倍に
  - 従業員数，企業の業種が交絡因子としてRRを上昇させていた