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[1]　池上　和輝[2]　菊池　浩明[2]　乾　孝治[3]

1:明治大学大学院先端数理科学研究科
2:明治大学総合数理学部先端メディアサイエンス学科
3:明治大学総合数理学部現象数理学科

はじめに

- 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）
- これらの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
  - 情報セキュリティマネージメント
  - 最高情報責任者（CIO）の設置
- 経済産業省の調査結果によると，平成25 年度の国内企業におけるCIO の設置率はわずか29.5%であった

研究目的

- 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…

解決手法

- 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

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
  - 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/

B. 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

質問項目	Yes	No
CSR専任部署の有無	1. 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，不定期に実施	3. なし，4. その他

年	企業数(上場数)	平均社員数	総質問項目数	過半数が実施した質問項目数	方策についての質問数
2013	1210(1157)	2672	753	46	185
2014	1305(1259)	2582	764	46	186
2015	1325(1284)	2646	811	47	193
2016	1408(1364)	2579	832	52	197
2017	1413(1370)	2627	840	41	207
平均	1332.5(1286.8)	2621.2	800	46.4	193.6

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	26	24

分析手法：相対危険度（1）

- あるマネジメントM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

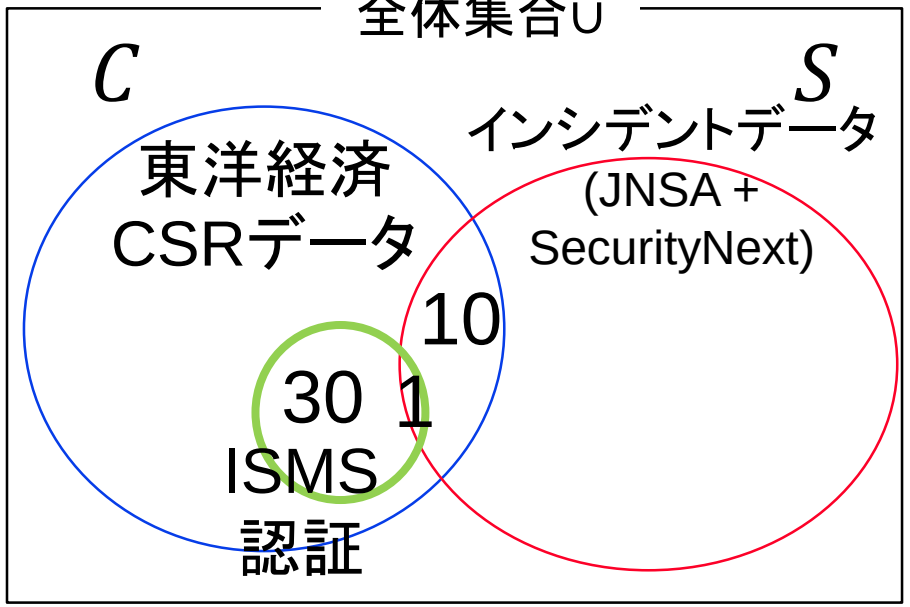
$$RR(M) = \frac{\Pr(\text{インシデント} \mid M)}{\Pr(\text{インシデント発生})} = \frac{a/n_1}{n_1/N}$$

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

分析手法：相対危険度（2）

マネジメント	インシデント・Yes	No	計
ISMS・Yes	1	29	30
ISMS・No	9	61	70
計	10	90	100

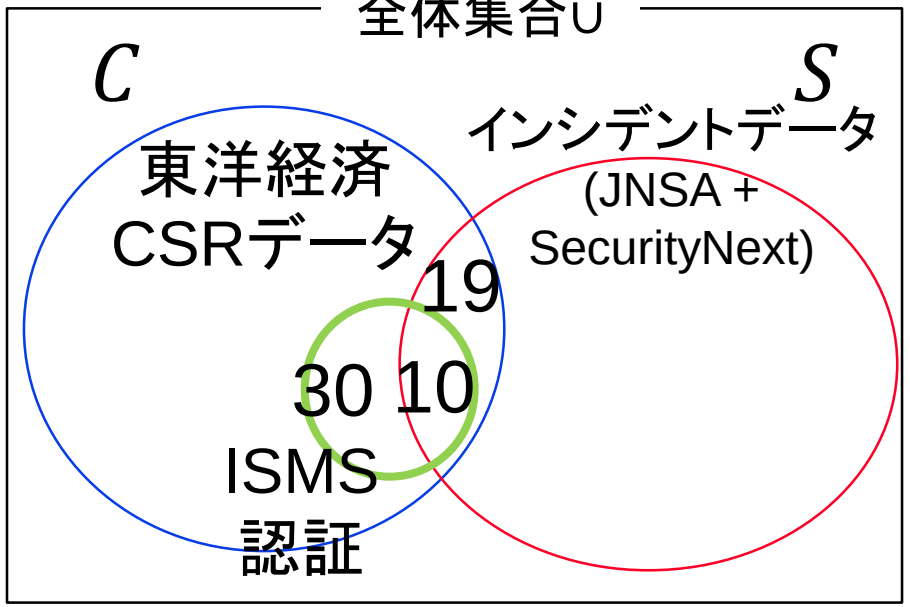
$$RR(ISMS) = \frac{\Pr(\text{インシデント} \mid ISMS)}{\Pr(\text{インシデント発生})} = \frac{1/30}{10/100} = 0.333\ldots$$



分析手法：相対危険度（3）

マネジメント	インシデント・Yes	No	計
ISMS・Yes	10	20	30
ISMS・No	9	61	70
計	19	81	100

$$RR(ISMS) = \frac{\Pr(\text{インシデント} \mid ISMS)}{\Pr(\text{インシデント発生})} = \frac{10/30}{19/100} = 1.754\ldots$$



分析手法:カイ2乗検定

- RRが統計的に有意かどうかを確認
  - 有意な場合($p < 0.1$)
    - » マネジメントの実施がインシデントの増減に関係がある

マネジメント	インシデント・Yes	No	計
ISMS・Yes	10	20	30
ISMS・No	9	61	70
計	19	81	100

$$RR(ISMS) = 1.754 \ldots$$

$$\chi^2 = 4.468,$$

$$p = 0.0345 < 0.05$$

- ISMS認証の取得によって，インシデント発生が増加している可能性

分析結果1：マネジメント実施企業数，インシデント発生企業数

質問項目	2013 (1210)		2014 (1305)		2015 (1325)		2016 (1408)		2017 (1413)	
	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	715	8	706	17	693	15	714	18	713	13
環境マネジメントシステム	713	8	704	14	687	12	697	18	694	10
内部告発窓口（社内）	1010	15	998	26	995	23	1040	27	1043	20
内部告発窓口（社外）	568	11	644	15	700	16	791	16	840	15
内部統制委員会	621	5	597	15	592	13	596	11	591	9
内部監査部門	823	14	904	24	945	22	1001			19
CIO	371	4	370	14	373	6	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	26	971	23	1000			18
ISMS認証	194	6	194	5	197	6	204	4	210	4

平均約28%

平均約15%

分析結果2:インシデント発生企業

- インシデント発生企業の一部

企業名	発生年	原因	CIO	ISMS
ヤフー	2013年	不正アクセス	○	○
ソニー	2014年	設定ミス	○	○
ベネッセ	2014年	内部犯行	○	×
サイバーエージェント	2016年	不正アクセス	×	×

分析結果3:相対危険度(1)

質問項目	2013	2014	2015	2016	2017
環境監査	0.713	1.164	1.024	1.183	1.073
環境マネジメント システム	0.715	0.961	0.827	1.212	0.848
内部告発窓口(社内)	0.946	1.259	1.094	1.218	1.129
内部告発窓口(社外)	1.233	1.126	1.082	0.949	1.051
内部統制委員会	0.513	1.214	1.039	0.866	0.897
内部監査部門	1.083	1.283	1.102	1.219	1.103
CIO	0.687	1.829	0.761	1.300	0.755
情報システムに関する セキュリティポリシー	0.973	1.292	1.121	1.173	1.051
ISMS認証	1.970	1.246	1.441	0.920	1.121

分析結果4：相対危険度（2）

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	

考察

- 仮説：CIOの設置や，ISMS認証の取得によってインシデントの発生リスクが抑えられる
  - 総計によるRRでは9件中7件の項目でRR＞1

- 原因
  - 業種によって必要性の低い項目が多く含まれている
  - 今回Noと分類した回答の中に検討中，実施予定が含まれる
  - インシデント発生とマネジメント方策の導入の因果関係が逆に測定されている
  - マネジメント方策がインシデントを増加させている

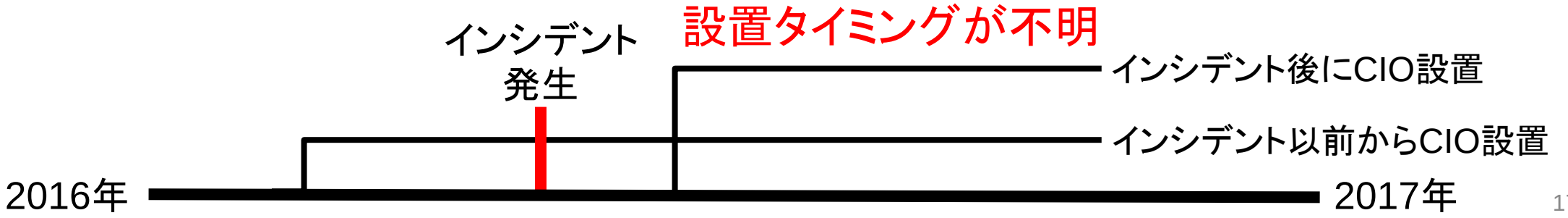
原因1：業種

業種	2013	2014	2015	2016	2017
食品	50	53	58	63	56
エネルギー資源	5	5	6	6	4
建築・資材	97	103	106	112	113
素材・科学	119	130	137	136	141
医薬品	24	26	30	32	33
自動車・輸送機	60	66	67	64	65
鉄鋼・非鉄	31	33	32	30	30
機械	65	77	78	88	86
電機・精密	126	129	127	138	135
情報通信・サービスその他	210	228	236	265	272
運輸・物流	39	43	43	42	44
商社・卸売	119	128	128	140	134
小売	101	101	102	105	119
銀行	30	37	35	42	42
金融（銀行除く）	28	35	35	42	42
不動産	28	31	33	31	32
不明	66	68	61	62	56

原因2:導入タイミング

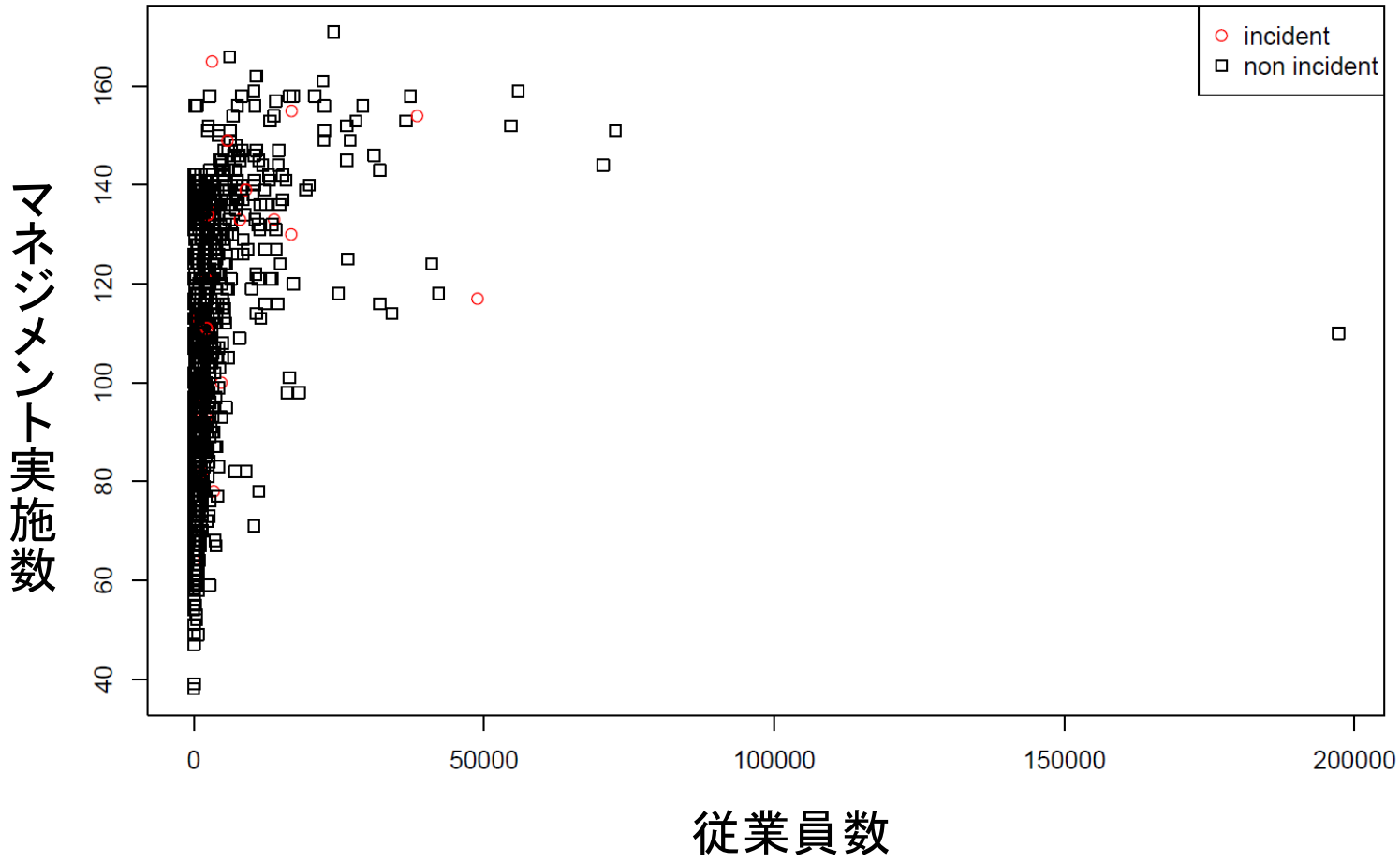
- マネジメント開始年にインシデントが発生した企業が多い
  - インシデントの発生を受けてマネジメント方策を導入した可能性がある

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



原因3：マネジメントによるインシデント増加

- 外部監査，内部告発窓口の設置による見逃されていたインシデント露見
- インシデント発生企業のほとんどが100以上の項目にYesと回答



まとめ

- 企業の経営マネジメント状況とインシデント発生の関係を調査
- CIOの設置や，ISMS認証の取得によって相対危険度が1以上に
- 今後は，業種や規模での分類をしての分析などを検討