Vol.2018-CSEC-82 No.19
Vol.2018-SPT-29 No.19
2018/7/25

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,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が求められている．しかしながら，これらの方策が漏洩に対して本当に効果があるのか不明であった．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 CSR データベースを用いて調査し，これらの経営マネジメント方策と漏洩インシデント発生の関係を明らかにする．

キーワード：情報漏洩，ガバナンス，CSR

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，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 [4]．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．

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) データベースに注目する [3]．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 社の情報が格納されている．本データベースを 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明らかにすることが出来ると考えた．本稿では，この調査結果を報告する．

2. 関連研究

杉本らはシステム内の脅威がもたらすリスクからセキュリティ投資効果を算定する技術を提案している [5]．提案方式では，システムから自動収集したシステム情報と，インターネット上から収集した脆弱性公開情報を突き合わせることで，システム内の脆弱性の特定，侵入経路の抽出，攻撃容易性の算出を行う．さらに，脅威への対処によってシステムが停止する時間，侵害され得るデータの価値，損失

[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
Department of Mathematical Sciences Based on Modeling and Analysis, School of Interdisciplinary Mathematical Sciences，Meiji University
[a)] cs172001@meiji.ac.jp

ⓒ 2018 Information Processing Society of Japan

表 1　Romanosky の提案モデルの各係数（一部）[6]

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		-0.0294
$lawsuit$	β_5		0.444
		Government	-1.339
$FirmType_{i,t}$	β_6	Private	-1.032
		Public	-0.0654

機会などから，脅威に対してインシデントが発生する前に対処を行った場合にかかる投資額と，インシデントが発生した後に事後処理を行った場合にかかる想定被害額をそれぞれ算出することで，技術的なシステム把握だけでなく，経営層の経営判断に資する情報も提示している．

Romanosky は Advicen 社[*1]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次式のモデルを提案している [6]．なお，単位は百万ドルである．

$$\begin{aligned}\log(cost_{i,t}) = \beta_0 &+ \beta_1 \cdot \log(revenue_{i,t}) + \beta_2 \cdot \log(records_{i,t}) \\ &+ \beta_3 \cdot repeat_{i,t} + \beta_4 \cdot malicious_{i,t} \\ &+ \beta_5 \cdot lawsuit_{i,t} + \alpha \cdot FirmType_{i,t} \\ &+ \lambda_t + \rho_{ind} + \mu_{i,t}\end{aligned} \tag{1}$$

ここで，各係数の値を表 1 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[*2]，records は漏洩情報の件数を示している．Rpeat player，Lawsuit はブール値，Firm Type 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．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ることに注意せよ．

3. データ

3.1 JNSA

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・評価を行っている．インシデントデータベース [7] 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．

2005 年から 2016 年のデータベースの統計量を表 2 に示す．

3.2 SecurityNext

ニュースガイア株式会社が運営するウェブサイト SecurityNext[*3]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．収集したインシデント件数を表 3 に示す．

3.3 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．データベース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...」という段階的な回答や，「CIO 設置の有無」という質問に対し「1．あり　2．なし　3．その他」という選択肢などがある．その他と回答した企業には役職名が異なるが CIO と同様の業務内容の担当者がいるという質問項目なども存在する．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 データベースの統計量と質問項目の一部をそれぞれ表 5，6 に示す．ここで，質問項目は年々追加されて総数が増えていることに注意しよう．本調査では，約 800 の項目の内，マネジメント方策に関する約 200 の質問である，方策を実施したか否かの bool 値を取る質問である．200 の内，過半数の企業が実施した方策は，5 に示される約 45 項目の 20%程度である．

表 7 に CSR データベース内の企業の業種の分布を示す．業種区分は，東京証券取引所が日本株の分類として利用されてきた 33 業種分類を 17 業種に再編した TOPIX-17 シ

[*1] https://www.advisenltd.com/
[*2] revenue には「純利益」,「歳入」などの意味があるか，本稿ではこれを「売上額」とみなして算出する
[*3] http://www.security-next.com/

表 2　JNSA のデータベースの統計量

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	15569	8853	25	11764.32	1297.42	42361.73	460.27

表 3　SecurityNext から収集したインシデント件数

期間	レコード数	企業数
2013 2018	174	121

表 4　マネジメント方策 M を実施している企業数の集計例

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

リーズを利用し 17 業種に区分した [9]．表 7 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．CSR は，これらの IT 関係や小売の特徴をデータベースを有している．

本研究では，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．

4. 分析

4.1 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関係を明らかにすることを目的とする．そのため，CSR データセットと JNSA と Security Next のインシデント情報を照合する．

4.2 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 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率と一般の発生率の比，すなわち，

$$RR(M) = \frac{Pr(\text{インシデント}\,|M)}{Pr(\text{インシデント発生})} = \frac{a/m_1}{n_1/N} \qquad (2)$$

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（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 乗値は表 4 を例にすると，

$$\chi^2 = \frac{N(|ad-bc| - \frac{N}{2})}{n_1 n_2 m_1 m_2} \qquad (3)$$

で計算される．例えば，2014 年に情報システムのセキュリティに関する外部監査を実施していた企業数が表 8 で与えられた時，RR（$M_{\text{外監}}$）は，

$$RR(M_{\text{外監}}) = \frac{18/627}{27/1305} = 1.388 \qquad (4)$$

となる．また，カイ 2 乗検定による p 値は 0.050 となり，有意水準を満たしている．そのため，2014 年において情報システムのセキュリティに関する外部監査を実施することは，インシデント発生のリスクを増加させている可能性がある．

4.3 分析結果

4.3.1 CSR 記載のインシデント発生企業数

表 9 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．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 10 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．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．

2017 年の従業員数と実施している質問項目数の散布図を図 1 に示す．赤い丸がインシデント発生企業である．インシデント発生企業は点在しているが，その多くは 100 以上の質問項目に Yes と答えていた．

4.3.2 相対危険度

CSR の社会的責任編の 2 件と環境編の 12 件の計 14 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，RR と，カイ 2 乗検定の結果を表 11 に示す．表で，有意確率 90%，95%，99%を超えた p 値に，各々，*，**，***を付す．例えば，No.4，6，10，11 については，全て有意確率 99%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優位なレベルで生じている．CIO や ISMS 認定などによって，インシデント発生のリスクが抑えられると考えたが，1.095，1.302 と，RR は 1 を上回った．環境マネジメントシステム（EMS) の RR は 0.923 であり，1 を下回る．ただし，カイ 2 乗検定による有意差は見られなかった．

ⓒ 2018 Information Processing Society of Japan

Vol.2018-CSEC-82 No.19
Vol.2018-SPT-29 No.19
2018/7/25

表 5　CSR データベースの統計量

年	企業数 (上場)	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

表 6　CSR データベースの質問項目の一部

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 7　CSR データベースの各年の企業分布

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	40	39
不動産	28	31	33	31	32
不明	66	68	61	62	56

表 8　2014 年に情報システムのセキュリティに関する外部監査を実施している企業数

外部監査	インシデント・Yes	No	計
Yes	18	609	627
No	9	669	678
計	27	1278	1305

表 9　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
CSR	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

質問項目と RR の経年変化を表 12 に示す．RR が 1 以下のものを太字で，カイ 2 乗検定の結果有意差が見られたものに下線を引く．2013 年の CIO の設置や，2016 年の ISMS 認証によって RR が 1 を下回った年もあったが，いずれもカイ 2 乗検定による有意差は見られなかった．

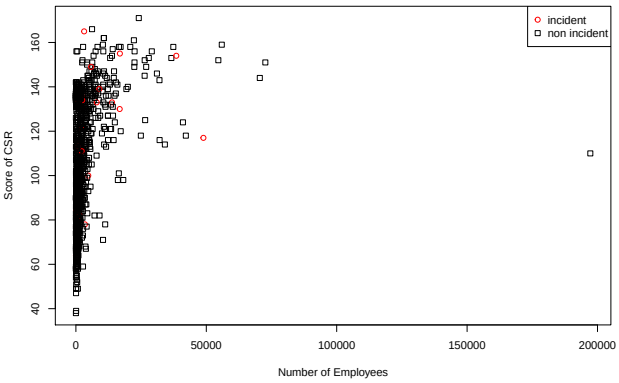

図 1　従業員数と質問項目に Yes と答えた数の散布図

4.4　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 段階で分類した結果を，表 13 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．

5.　考察

CSR データベースでの CIO 設置率は平均で約 28 %，特に 2017 年は最低の 27.6%となり，未だに国内では CIO の必要性が広まっていないことがうかがえる．また，本調査の対象である論理 1 型のマネジメント方策の実施に関する質問項目数に対して，過半数の企業が実施済と回答した質問項目数が約 2 割から 3 割にとどまっている．

CIO の設置や ISMS 認定の取得は，企業の情報セキュリティ対策が水準以上であり，インシデント発生のリスクが抑えられると考えた．しかし，表 11 より 14 件中 12 件の項目について RR は 1 以上であった．RR が 1 以下の方策もあるが，p 値には有意差は見られなかった．この原因と

ⓒ 2018 Information Processing Society of Japan

表 10　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	15	714	18	713	13
環境マネジメントシステムの構築	713	8	704	14	687	12	697	18	694	10
内部告発窓口（社内）の設置	1010	15	998	26	995	23	1040	27	1043	20
内部告発窓口（社外）の設置	568	11	644	15	700	16	791	16	840	15
内部統制委員会の設置	621	5	597	15	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	24	945	22	1001	26	1014	19
ＣＩＯの有無	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	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	22	857	21	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	18	641	15	671	17	673	12
ISMS 認証	194	6	194	5	197	6	204	4	210	4

表 11　総計による RR

No	質問項目	RR	p 値	
1	CIO の有無	1.095	0.493	
2	ISMS 認証	1.302	0.147	
3	情報セキュリティシステムに関する内部監査	1.161	0.011	
4	内部告発窓口（社内）の設置	1.136	0.005	***
5	内部告発窓口（社外）の設置	1.072	0.379	
6	業務部門から独立した内部監査部門の有無	1.166	0.004	***
7	情報システムに関するセキュリティポリシー	1.129	0.013	**
8	情報システムのセキュリティに関する内部監査	1.161	0.011	**
9	情報システムのセキュリティに関する外部監査	1.173	0.054	*
10	リスクマネジメント体制の構築	1.354	1.3E-6	***
11	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	1.397	5.85E-07	***
12	内部統制委員会の設置	0.920	0.410	
13	環境監査の実施状況	1.043	0.597	
14	環境マネジメントシステムの構築	0.923	0.356	

して，次のことが考えられる．

(1) 業種によって必要性の低い項目が多く含まれている．
(2) 今回 No と分類した回答の中に検討中や，実施予定が含まれる．
(3) インシデントの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．
(4) マネジメント方策がインシデントを増加させている．

例えば，(1) は，表 7 からもわかるように，CSR の対象企業が情報通信に分布が偏っていることと相関があるだろう．(3) については，表 13 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リスクが増加したと解釈してしまう．また，外部監査や，内部告発窓口の設置などマネジメント方策を実施することによってこれまで見逃されていたインシデントが公表されている可能性があると我々は考える．なぜならば，図 1 より 2017 年のインシデント発生企業のほとんどは質問項目について Yes と答えた数が 100 を超えていたからである．

表 9 より，CSR 記載企業でのインシデント発生企業数は増加傾向にある．[8] より，インシデント発生件数は近年減少傾向にあるが，インターネット経由でのインシデントは増加している．業務での情報の管理媒体や使用方法，質問項目への回答も業種によって大きく異なることが予想されるため，業種ごとでの RR の計算や分析が必要である．

6. まとめ

本研究では，インシデント発生情報と CSR データセットを用いることで，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した．CIO の設置や，ISMS 認証の取得によってインシデント発生のリスクは増加し，相対危険度が 1 以上であった．

しかし，この結果から ISMS などのマネージメントがイ

ⓒ 2018 Information Processing Society of Japan

表 12　質問項目と各年の RR

No	質問項目	2013	2014	2015	2016	2017
1	環境監査の実施状況	**0.713**	1.164	1.024	1.183	1.073
2	環境マネジメントシステムの構築	**0.715**	**0.961**	**0.827**	1.212	**0.848**
3	内部告発窓口（社内）の設置	**0.946**	1.259	1.094	1.218	1.129
4	内部告発窓口（社外）の設置	1.233	1.126	1.082	**0.949**	1.051
5	内部統制委員会の設置	**0.513**	1.214	1.039	**0.866**	0.897
6	業務部門から独立した内部監査部門の有無	1.083	1.283	1.102	1.219	1.103
7	ＣＩＯ（最高情報責任者）の有無	**0.687**	1.829	**0.761**	1.300	**0.755**
8	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
9	情報システムのセキュリティに関する内部監査	1.058	1.263	1.160	1.254	1.040
10	情報システムのセキュリティに関する外部監査	1.119	1.388	1.107	1.189	1.050
11	ＩＳＭＳ（情報セキュリティマネジメントシステム）認証	1.970	1.246	1.441	**0.920**	1.121
12	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	1.296	1.433	1.360	1.311	1.338
13	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	1.427	1.546	1.325	1.343	1.351

表 13　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

ンシデントの発生リスクを増加させると結論付けるのは早急である．本研究では，業種の分類をせずに RR を計算したり，CSR データセットの質問項目のうち bool 型の質問項目のみを利用した．今後は，企業を業種や規模などで分類しての分析や機械学習を用いた分析などを検討している．

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．

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] 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/statistics/zyo/zyouhou/result-2/pdf/H26_report.pdf, 2018.06.19 参照)
[5] 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
[6] Sasha Romanosky: Examining the costs and causes of cyber incidents, Journal of Cybersecurity, 2(2), pp.121-135, 2016
[7] 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）
[8] 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）
[9] 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)

ⓒ 2018 Information Processing Society of Japan