Vol.2019-CSEC-86 No.64
Vol.2019-SPT-34 No.64
2019/7/24

新聞報道される情報漏えい事故の属性分析

新原 功一[1]　池上 和輝[2]　菊池 浩明[3]

概要：毎年，数多くの組織で情報漏えい事故が発生している．情報を漏えいしたことが公になると，組織はレピュテーションが低下し，取引停止等に陥るなどの悪影響を受ける恐れがある．さらに重大な事故であった場合，テレビ，新聞，インターネット等で報じられ，SNS やブログ等で拡散し，組織は信頼の失墜につながる大きなダメージを受ける．しかし，今までどのような事故が重大な事故だと扱われる傾向にあるかは，明らかではなかった．そこで，本研究は新聞で報道された情報漏えい事故の属性（漏えい経路，被害人数など）に着目する．本研究では朝日新聞社で報道された情報漏えい事故の記事データと日本ネットワークセキュリティ協会が収集した情報漏えい事故データをもとに，新聞報道の有無と属性に関係があるかを調べるため，フィッシャーの直接確率検定，ロジスティック回帰分析を行った．分析結果から，漏えい経路が第三者，被害人数が 5,000 名以上の情報漏えい事故は，新聞で報道される確率が上がることが分かった．

キーワード：情報漏えい，インシデント，新聞報道

Koichi Niihara[1]　kazuki ikegami[2]　Hiroaki Kikuchi[3]

1. はじめに

昨今，インターネット上では様々なサービスが提供されている．サービス提供組織は個人情報を取り扱うことがある．これらの情報は，スマートフォンの爆発的な普及や IoT サービスの進化などによって，日々増加している．個人情報が悪意のある第三者に流出してしまうと，なりすましによる不正ログインやソーシャルエンジニアリングなどに悪用されてしまう恐れがある．このように組織は，適切に個人情報を取り扱うことが求められている．

一方，個人情報が漏えいする事故（以下，情報漏えい事故）は毎年数百件が公表されている [1]．しかし，一般の利用者はどこまでの情報漏えい事故ならば認知しているだろうか．マカフィー社が国内の企業経営者や一般従業員などに行った「セキュリティ事件に関する意識調査」によれば，情報漏えい事故に対する認知度は日本年金機構への標的型攻撃で 125 万件の個人情報が漏えいした事件，県立学校が不正アクセスを受け、個人情報を含むファイル約 15 万 3000 件が漏えいした事件でそれぞれ 60.1 %，21.6 %であった [2][3]．このように認知度は事故の内容により差がある．もし，情報漏えい事故が新聞などのマスコミで重大ニュースとして報じられ，SNS やブログなどで拡散されると認知度は高まるだろう．しかし，今までどのような情報漏えい事故が，重大事故として広く報道されるかは明らかになっていなかった．

そこで，本研究は新聞の全国版で報道された情報漏えい事故が，どのような特徴を有しているか明らかにする．新聞を対象とした理由は，ニュースが大勢の人に伝わりやすく，他のマスメディア（テレビ，ラジオなど）と比べて報じられた内容を事後に確認しやすいためである．

まず，2015 年〜2016 年に朝日新聞の全国版で報道された情報漏えい事故の記事を調査した．次に，日本ネットワークセキュリティ協会（JNSA）が収集した 2015 年〜2016 年に公表された情報漏えい事故が，新聞で報道されているかを確認した．そして，情報漏えい事故における漏えい原因，漏えい経路，被害人数，業種などの属性が，新聞報道の有無に与える影響を分析した．属性と新聞報道の独立性を検定するために，フィッシャーによる直接確率検定を行った．また，影響の大きさを明らかにするため，ロジスティック回帰分析を行った．

[1] 明治大学先端数理科学インスティテュート
Meiji Institute for Advanced Study of Mathematical Sciences
[2] 明治大学大学院先端数理科学研究科
Meiji University Graduate School of Advanced Mathematical Sciences
[3] 明治大学総合数理学部
Meiji University Undergraduate School of Interdisciplinary Mathematical Sciences

フィッシャーの直接確率検定の結果，漏えい原因，漏えい経路，被害人数，業種がともに新聞報道の有無と関係があることが分かった．また，ロジスティック回帰分析の結果，被害人数が 5000 名以上，漏えい原因が第三者や故意などの場合に新聞報道の有無に著しい影響を与えていた．

本論文の構成は次のとおりである．2 章では，関連研究の調査について述べる．3 章では実験方法，4 章で実験結果，評価を記す．5 章で考察を与え，最後に 6 章でまとめる．

2. 関連研究

本章は，情報漏えい事故の特徴を分析した関連研究を述べる．JNSA は，個人情報漏えいの被害額の算出する手法として，想定損害賠償額算定式（JO モデル）を提案した [4]．山田らは JO モデルを改良し，より実際の損害額に近い金額を算出できるモデルを提案した [5]．これらのモデルは，情報漏えい事故によって企業がどれだけの損失を被ったかを把握することができる．Ponemon は，個人情報漏えいの発生に関する 1 件当たりの平均コストを毎年算出している [6]．Jocobs は，Ponemon が収集したデータを分析し，線形回帰モデルを提案した [7]．Romanosky は，米国 Advicen 社のインシデント情報から定式化したコスト算出モデルを提案した [8]．また，米国のサイバー保険は，業種毎にリスクの重みづけを変えているものも存在する [9]．しかし，情報漏えい事故の漏えい原因，漏えい経路などの属性によって，どれくらいの注目を集める度合いが変わるかについては考慮されていない．

山田らは，ISMS 認証の取得や CIO の設置などのマネジメント方策が，情報漏えい事故の発生に及ぼす影響の大きさを分析し，CIO 設置企業ではインシデントの発生確率が約 0.3 倍に抑えられることを示した [10][11]．ただ，情報漏えい事故の大きさ自体を分析しているものではない．

3. 方法

3.1 仮説

漏えい情報，漏えい原因，業種は，JNSA は，情報漏えい事故の傾向を分析する際の属性として挙げている．被害人数は，情報漏えい事故の大きさを示す基礎的な指標であると筆者らは想定した．

そこで，本研究では次の 4 つの仮説を立てる．

$H_{原因}$：情報漏えい事故における漏えい原因は，新聞報道の有無と関係がある．

$H_{経路}$：情報漏えい事故における漏えい経路は，新聞報道の有無と関係がある．

$H_{被害人数}$：情報漏えい事故における被害人数は，新聞報道の有無と関係がある．

$H_{業種}$：情報漏えい事故を発生させた組織の業種は，新聞報道の有無と関係がある．

これらを確かめるため，次節以降で示す実験を行う．

3.2 困難性

仮説を検証するには以下の困難性が存在する．

困難性 1 ：新聞報道から情報漏えい事故を抽出することが難しい．情報漏えい事故を示す単語が「漏えい」「漏洩」「流出」「紛失」など多様である．さらに，個人情報とは関係がない情報漏えい（警察による捜査情報の漏えい，インサイダー取引など）が数多く含まれる．

困難性 2 ：新聞で報道された情報漏えい事故が少なく，特徴を把握することが難しい．

3.3 着想

これらの課題に対して，本研究では以下の着想により困難性を解決した．

着想 1 ：新聞報道された記事から，情報漏えい事故に関連がある記事を選定するため，JNSA の情報漏えい事故のうち，いくつかの事故をサンプルで抽出し，該当する新聞記事にある文章から情報漏えい事故であることを表しているキーワードを収集した [*1]．このキーワードに合致した新聞記事を選定して，新聞報道データとした．そして，新聞報道データにおける記事に対して，実際に発生した情報漏えい事故の組織名や被害人数などが含まれるかを検索することで，個人情報とは関係がない情報漏えい事故と区別することを可能とした．

着想 2 ：属性を特徴毎にまとめてグループ化することで，グループ毎における新聞で報道された情報漏えい事故の件数が多くなり．特徴を把握しやすくした．

本研究は，これらの着想によって新聞で報道される情報漏えい事故の特徴を明らかにする．

3.4 データ

3.4.1 情報漏えい事故データ

JNSA は毎年インターネット等で公表された情報漏えい事故を調査している．本研究はこの調査データを情報漏えい事故データとして用いた．

情報漏えい事故データで定められた属性は，項目数が多い．一方，新聞報道の件数が限られているため，既存の属性の項目で分析すると項目毎の新聞報道数が極めて少なくなり，十分な差を確認できない恐れがあった．そこで，本研究では漏えい原因，漏えい経路の属性を特徴毎にまとめてグループを作成した．例えば，漏えい原因であれば「管理ミス」「誤操作」「過失」「紛失・置忘れ」を「過失」グループとした．また，被害人数は 10 件未満を「小規模」，10 件以上 5000 件以下を「中規模」，5001 件以上を「大規模」とした．

漏えい原因，漏えい経路，被害人数のグループと既存の属性の関係をそれぞれ表 1，表 2 表 3 に示す．

[*1] 詳細は 3.4.2 章参照

表 1　漏えい原因グループの分類

グループ	既存の項目
第三者	設定ミス，盗難，不正アクセス
	バグ・セキュリティホール，ワーム・ウィルス
過失	管理ミス，誤操作，過失，紛失・置忘れ
故意	内部犯罪・内部不正行為，不正な情報持ち出し
	目的外使用
その他	その他，不明

表 2　漏えい経路グループの分類

グループ	既存の項目
電子	USB 等可搬記録媒体，携帯電話スマートフォン
	電子メール，PC 本体，インターネット，FTP
紙	紙媒体
その他	その他，不明

表 3　被害人数グループの分類

グループ	件数
ヒヤリハット	10 件未満
軽微	10 件以上 5000 件以下
重大	5001 件以上

3.4.2　新聞報道データ

本研究は，新聞で報道された情報漏えい事故の記事を収集した．収集には，朝日新聞社「聞蔵 2 ビジュアル」サービス（以下，聞蔵）」[*2] を用いた．対象期間は 2015 年 1 月 1 日〜2016 年 12 月 31 日である．

新聞の紙面には全国版，地方版などがあるが，対象する記事は全国版に掲載されたものに限定した．全国版に限定した理由は，地方版には紙面数に限りがあり，地域毎に掲載される事故の水準に差が大きいと想定したためである．

また，対象記事は，記事の見出しに個人情報や漏えいなどのキーワードを含む記事を対象とした．キーワードは「漏えい」「流出」「紛失」「個人情報」「漏えい」「盗難」「不正アクセス」「誤送信」である．いずれかのキーワードを含む記事を「新聞報道データ」とした．

3.4.3　新聞報道の有無の調査

情報漏えい事故データの各事故が，新聞報道データで報道されているかを確認した．具体的には，情報漏えいデータの事故毎における組織名や被害人数を元に，新聞報道データに該当するものがないかを確認した．該当した事故については，情報漏えい事故データの新聞報道の有無を「報道あり」とし，該当しなかったものは「報道なし」とした．なお，1 つの事故が複数回報道されるケースについても，報道回数のカウントはせずに「報道あり」とした．

3.5　分析

3.5.1　独立性の検定

情報漏えい事故の属性と新聞報道の有無に有意な差があるかを検定する．3.1 節で立てた仮説について，有意な差があるかを統計的に検定するため，H_0 と H_1 について，フィッシャーの直接確率検定を行う．

帰無仮説（H_0）: 属性と新聞報道の有無は独立である．

対立仮説（H_1）: 属性と新聞報道の有無は独立ではない．

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，属性は新聞報道の有無に関連があると判断する．

3.5.2　ロジスティック回帰

情報漏えい事故が新聞で報道される確率は，漏えい原因や漏えい経路などの属性が複合的に関与していると考える．これらの交絡因子の影響を排除して，それぞれの属性が情報漏えい事故の発生に与える影響の大きさを明らかにするため，多重ロジスティック回帰分析を行う，

情報漏えい事故が新聞で報道される確率 $p(x)$ を

$$p(x) = \frac{1}{1 + \mathrm{e}^{-z}}$$

とする．また，

$$z = \alpha + \beta_{x_1} x_1 + \beta_{x_2} x_2 + \beta_{x_3} x_3 + \ldots + \beta_{x_m} x_m$$

を仮定する．x_m は属性（漏えい原因グループ，漏えい経路グループ，被害人数グループ，業種）の説明係数である．α は定数，β は各変数の係数である．

x_1 について，他の変数 α，x_2，x_3，...，x_m の影響を調整したオッズ比 (adjusted Odds Ratio) は，

$$OR = \mathrm{e}^{\beta_{x_1}}$$

である．すべての統計解析には R を使用した．

4.　実験結果

4.1　情報漏えい事故の公表件数

情報漏えい事故データの件数は 1,256 件である．そのうち，新聞の全国版で報道された事故の件数は 38 件である．情報漏えい事故と新聞報道の有無の件数を集計した結果を表 4 に示す．

表 4　情報漏えい事故の件数と新聞報道の有無

年	なし	あり	Tolal
2015	764	24	788
2016	454	14	468
N	1218	38	1256

表 5 は，漏えい原因，漏えい経路，被害人数の各グループ毎の新聞報道数である．漏えい原因では「第三者」，漏えい経路では「電子」，被害人数では「大規模」において，新聞報道される事故が多い．

表 6 は，業種毎の新聞報道数である [*3]．電気・ガス・熱

[*2] https://database.asahi.com/index.shtml

[*3] 農業，林業，分類不能の産業は情報漏えい事故が 0 件であったため，除外した．

表 5　グループ毎の新聞報道数

グループ	項目	なし	あり
漏えい原因	第三者	2248	25
	過失	868	8
	故意	89	5
	その他	13	0
漏えい経路	電子	563	33
	紙	625	4
	その他	30	1
被害人数	ヒヤリハット	275	1
	軽微	842	14
	重大	101	23
N		1218	38

供給・水道業は，48 件中 3 件の事故が報道されており，他の業種と比べて，報道される割合が高かった．

表 6　業種名の新聞報道数

	なし	あり
サービス業 (他に分類されないもの)	79	6
医療，福祉	77	0
運輸業，郵便業	29	1
卸売業，小売業	73	5
学術研究，専門・技術サービス業	12	0
教育，学習支援業	239	8
金融業，保険業	204	3
建設業	5	0
公務 (他に分類されるものを除く)	285	4
宿泊業，飲食サービス業	11	0
情報通信業	85	4
生活関連サービス業，娯楽業	15	3
製造業	38	1
電気・ガス・熱供給・水道業	45	3
不動産業，物品賃貸業	13	0
複合サービス事業	8	0
N	1218	38

表 7 は，漏えい原因グループ，漏えい経路グループ，被害人数グループ別における新聞報道数である．被害人数グループがヒヤリハットの場合，新聞報道がありの件数が 1 件のみである．新聞報道がない場合，被害人数グループは軽微の方が件数が多いが，ありの場合は重大の方が多かった．

図 1 は新聞報道の有無別の情報漏えい事故の被害人数における箱ひげ図である．被害人数の中央値は，「報道なし」では約 100 件だが，「報道あり」は約 10,000 件であった．ある．

図 2 は漏えい原因グループ毎の被害人数の確率密度関数である．過失，故意と比べて，第三者における被害人数がやや多い傾向にある．

4.2　独立性の検定

検定対象の属性は，漏えい原因グループ，漏えい経路グループ，被害人数グループおよび業種である．検定対象を新聞報道の有無で集計したものが表 5，および表 6 である．検定結果を表 8 に示す．表で有意確率 5%，1%を超えた p 値にそれぞれ*，**を付す．

表 7　漏えい原因グループ，漏えい経路グループ，被害人数グループ別における新聞報道有無

新聞報道	被害人数グループ	漏えい原因グループ	漏えい経路グループ 紙	電子	その他
なし	ヒヤリハット	過失	163	43	8
		第三者	3	29	2
		故意	8	5	6
		不明	5	2	1
	軽微	過失	366	243	3
		第三者	34	128	2
		故意	20	36	6
		不明	2	2	0
	重大	過失	22	20	0
		第三者	1	49	0
		故意	1	6	1
		不明	0	0	1
あり	ヒヤリハット	過失	0	0	0
		第三者	0	0	0
		故意	0	1	0
		不明	0	0	0
	軽微	過失	2	4	0
		第三者	1	6	0
		故意	0	1	0
		不明	0	0	0
	重大	過失	0	2	0
		第三者	1	17	0
		故意	0	2	1
		不明	0	0	0
N			629	596	31

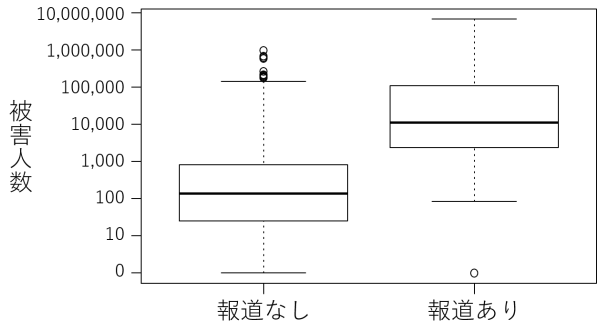

図 1　新聞報道の有無における被害人数の箱ひげ図

表 8　フィッシャーの直接確率検定の結果（仮説ごと）（片側検定）

仮説	P 値	
$H_{原因}$	0.000	**
$H_{経路}$	0.000	**
$H_{被害人数}$	0.000	**
$H_{業種}$	0.020	*

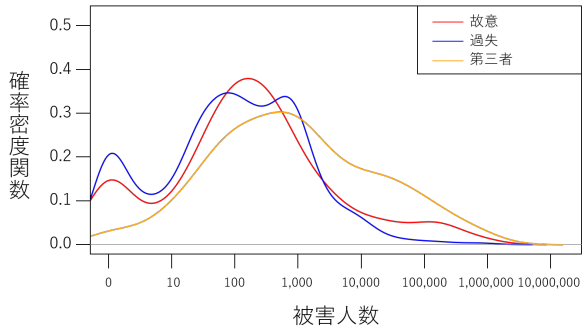

図 2 漏えい原因グループ毎の被害人数の確率密度関数

検定対象のうち，漏えい原因グループ，漏えい経路グループ，被害人数グループの p 値はいずれも 0.01 を下回っており，1%の有意水準で帰無仮説は棄却された．また業種の p 値はいずれも 0.05 を下回っており，5%の有意水準で帰無仮説は棄却された．これらの属性と新聞報道には関係性があることが明らかになった．

4.3 ロジスティック回帰分析

ロジスティック回帰分析の分析結果を表 9 に示す．Estimate が係数 β であり，これが正の値の場合，該当する属性で，新聞報道の発生確率が高まる．逆に負の値であれば，新聞報道の発生確率は低くなる．例えば，被害人数グループ（重大）の発生確率は高くなる（$\beta_2 = 3.31736$）．今回の結果からは，「重大：被害人数グループ」，「第三者」，「故意」，「電子」，「電気・ガス・熱供給・水道業」，正の係数での有意差が見られた．

ロジスティック回帰分析の分析結果における調整オッズ比を表 10 に示す．オッズ比より，被害人数グループ（重大）に対する新聞報道の確率は $exp(3.37559) = 29.242$ である．すなわち被害人数が 5000 名を超えると，超えないときに対して約 29.2 倍報道がされやすくなる．また，漏えい原因グループが「第三者」，「故意」，漏えい経路グループが「電子」，業種が「電気・ガス・熱供給・水道業」の情報漏えい事故では，新聞で報道がされる確率がそれぞれ約 4.2 倍，4.1 倍，3.8 倍，5.8 倍となる．

5. 考察

5.1 新聞報道される情報漏えい事故の傾向

ロジスティック回帰分析の結果により，被害人数については，5001 人以上（重大）の情報漏えい事故では，10 件未満（ヒヤリハット）と比べて新聞で報道される確率が約 29 倍に高まることが分かった．情報漏えい事故により影響を及ぼした人が多い方が，報道される確率が高まることは当然であると考える．いままでその確率がどれくらいになるかは明らかではなかったが，本研究では定量的に示すことができた．組織は，大量の個人情報を取り扱う場合，より慎重かつ適切な管理が施すことが望ましいだろう．

漏えい原因については，過失と比べて第三者や故意の情報漏えい事故の場合，報道される確率は約 4 倍であった．第三者であればサイバー攻撃や盗難，故意であれば内部不正が原因となった場合，世間の関心が高くなることが想定される．

漏えい経路については，紙媒体に比べて電子媒体の方が，報道される確率が約 4 倍であった．紙媒体は物理的な制約があり，電子媒体と比べて多くの情報を記録することが難しい．また，電子媒体は大量の情報をインターネットや USB 等可搬記録媒体で，比較的容易に持出可能でありも要因の一つと考える．

業種については「電気・ガス・熱供給・水道業」では，報道される確率は約 6 倍であった．重要インフラにおける情報漏えい事故は，社会的な関心が高いことが分かる．

5.2 新聞報道データの課題

本研究で分析に使用した新聞報道データにはいくつかの課題が存在する．まず，新聞報道データについては，報道内容が新聞社毎に異なることが想定される．掲載される記事，内容や掲載面（全国版，地方版など）は各社の編集方針に従う．また，他のニュースとの関係で記事の取扱いについての有無や大小は，都度変化する．

次に，新聞報道データの中には，同一の情報漏えい事故が連日報道されるケースがあった．たとえば，ベネッセコーポレーション社や日本年金機構による情報漏えい事故が該当する．本研究では，どのような属性の記事がどれくらいの期間，回数で報道されるのかは明らかにできていない．報道回数による事故の重みづけを考慮した分析についても今後の課題である．

また，報道することに寄与した要因が，本研究で想定した属性に含まれていないと想定される記事も存在した．たとえば，漏えい後の対応に問題がある，漏えいした犯人が未成年である，漏えいした情報が極めて機微なものなどが該当する．[*4]．海外で米国のヤフー，ソニーなどの情報漏えい事故に関する記事も多かった．インターネット上では，国内から海外のサービスを利用することは容易であり，このようなサービスへの関心が高いと考える．

5.3 情報漏えい事故データの課題

情報漏えい事故データの被害人数は，必ずしも影響を受けた人数を示すものではない．1 人のユーザが複数のアカウントを保有することがあるため，漏えいしたアカウント数よりも影響した実在の人数は下回る可能性がある．情報

[*4] たとえば，スプリックス社は中高生限定のスマートフォン向けアプリ「ゴルスタ」で運営担当者とユーザが喧嘩になり，元利用者の名前などの個人情報を Twitter に書き込むなどしたことで多くの批判を浴びている．佐賀県の県立高校では 1 万 5 千人分の個人情報が漏えいしたが，原因は佐賀市内の無職少年の不正アクセスによるものであった．

表 9　ロジスティック回帰の分析結果

属性		Estimate	Std. Error	z value	Pr(>|z|)	
(Intercept)		-6.76198	1.28132	-5.277	0.00000	**
被害人数グループ	軽微	1.22142	1.05955	1.153	0.24900	
	重大	3.37559	1.07078	3.152	0.00162	**
漏えい原因グループ	第三者	1.44140	0.50844	2.835	0.00458	**
	故意	1.41602	0.66991	2.114	0.03454	*
	その他	-15.39187	2621.18198	-0.006	0.99531	
漏えい経路グループ	電子	1.33244	0.65557	2.033	0.04210	*
	その他	1.57817	1.28585	1.227	0.21970	
業種名	医療，福祉	-16.11541	1095.61557	-0.015	0.98826	
	運輸業，郵便業	-0.37104	1.20155	-0.309	0.75747	
	卸売業，小売業	-0.26973	0.69872	-0.386	0.69947	
	学術研究，専門・技術サービス業	-16.86425	2809.82999	-0.006	0.99521	
	教育，学習支援業	0.05882	0.63677	0.092	0.92640	
	金融業，保険業	0.10880	0.87530	0.124	0.90107	
	建設業	-17.21292	4178.41842	-0.004	0.99671	
	公務 (他に分類されるものを除く)	-0.56716	0.73442	-0.772	0.43996	
	宿泊業，飲食サービス業	-16.19287	3094.91322	-0.005	0.99583	
	情報通信業	-0.90223	0.72624	-1.242	0.21411	
	生活関連サービス業，娯楽業	0.99690	0.93796	1.063	0.28786	
	製造業	-1.26622	1.17171	-1.081	0.27985	
	電気・ガス・熱供給・水道業	1.75757	0.86087	2.042	0.04119	*
	不動産業，物品賃貸業	-16.54193	2646.03376	-0.006	0.99501	
	複合サービス事業	-15.38074	3454.38166	-0.004	0.99645	

表 10　ロジスティック回帰分析の分析結果における調整オッズ比

属性		調整オッズ比
(Intercept)		0.001
被害人数グループ	軽微	3.392
	重大	29.242
漏えい原因グループ	第三者	4.227
	故意	4.121
	不明	0.000
漏えい経路グループ	電子	3.790
	不明	4.846
業種名	医療，福祉	0.000
	運輸業，郵便業	0.690
	卸売業，小売業	0.764
	学術研究，専門・技術サービス業	0.000
	教育，学習支援業	1.061
	金融業，保険業	1.115
	建設業	0.000
	公務 (他に分類されるものを除く)	0.567
	宿泊業，飲食サービス業	0.000
	情報通信業	0.406
	生活関連サービス業，娯楽業	2.710
	製造業	0.282
	電気・ガス・熱供給・水道業	5.798
	不動産業，物品賃貸業	0.000
	複合サービス事業	0.000

漏えい事故を公表する際，組織が複数アカウントの名寄せをしているケースも想定されるが，公表する組織によって名寄せの実施有無は異なる可能性が高い．

情報漏えい事故データは全国で発生した情報漏えい事故を網羅的に収集したものではない．まず，組織が情報漏えい事故の発生に気付かないことがある．大谷は，事故に気付いたとしても規模が小さいものは組織が公表しないことがあると指摘する [12]．また，公表されたものに情報漏えい事故のデータの調査段階で気づかずに未収集となることもある [13]．情報漏えい事故データの精度を向上させることも今後の課題である．

6. まとめ

本研究は 2015 年と 2016 年に新聞で報道された情報漏えい事故の特徴を明らかにした．漏えい原因，漏えい経路，被害人数，業種の各属性における独立性の検定，ロジスティック回帰分析により，被害人数が 5000 人を超える情報漏えい事故では新聞報道される確率が約 29 倍になることを明らかにした．また，漏えい原因グループが「第三者」，「故意」，漏えい経路グループが「電子」の発生確率は約 4 倍，業種が「電気・ガス・熱供給・水道業」の場合，発生確率は約 6 倍であった．経年変化を調査するとともに，属性を漏えいデータの価値や事後対応などへ広げていくことは今後の課題である．

7. 謝辞

情報漏えい事故データをご提供いただきました日本ネットワークセキュリティ協会に感謝申し上げます.

参考文献

[1] 特定非営利活動法人 日本ネットワークセキュリティ協会 セキュリティ被害調査ワーキンググループ: 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〜 , 特定非営利活動法人 日本ネットワークセキュリティ協会 (2017).
[2] マカフィー株式会社 : マカフィーセキュリティニュース 2016 年セキュリティ事件ランキング, https://www.mcafee.com/japan/home/security/news/064.html, 2019.05.02 参照.
[3] ASCII : 2015 年は「標的型」の一年に 1 位はあの事件、2015 年の 10 大セキュリティ事件ランキング, https://ascii.jp/elem/000/001/078/1078170/, 2019.05.02 参照.
[4] 特定非営利活動法人 日本ネットワークセキュリティ協会: 2003 年度情報セキュリティインシデントに関する調査報告書＜第 2 部＞情報漏洩による被害想定と考察 (賠償額および株価影響額), 特定非営利活動法人 日本ネットワークセキュリティ協会 (2003).
[5] 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, 研究報告コンピュータセキュリティ（CSEC）, 2018-CSEC-80(18), pp. 1-7(2018).
[6] Larry Ponemon: Calculating the Cost of a Data Breach in 2018, the Age of AI and the IoT, https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/, 2019.05.02 参照.
[7] Jay Jacobs: Analyzing Ponemon Cost of Data Breach, https://datadrivensecurity.info/blog/posts/2014/Dec/ponemon/, 2019.05.02 参照.
[8] Sasha Romanosky: Examining the costs and causes of cyber incidents, Journal of Cybersecurity, 2(2), pp. 121-135(2016).
[9] Sasha Romanosky, Lillian Ablon, Andreas Kuehn, and Therese Jones: Content analysis of cyber insurance policies: how do carriers price cyber risk? , Journal of Cybersecurity, Volume 5, Issue 1(2019).
[10] 山田道洋, 池上和輝, 菊池浩明, 乾孝治: 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, 研究報告コンピュータセキュリティ（CSEC）, 2018-CSEC-82(19), pp. 1-6(2018).
[11] 山田道洋, 池上和輝, 菊池浩明, 乾孝治: 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(2018).
[12] 大谷尚通: 個人情報漏えいインシデントの変遷と挑戦, 日本セキュリティ・マネジメント学会学会誌, 第 30 巻, 第 1 号 (2016).
[13] 池上和輝, 山田道洋, 菊池浩明, 乾考治: 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 (2019).