一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
ICSS2020-30(2021-03)

組織の属性に基づくインシデント規模と頻度モデルの提案

池上　和輝†　　菊池　浩明††

† 明治大学大学院　先端数理科学研究科
†† 明治大学　総合数理学部　先端メディアサイエンス学科
E-mail: †{cs192021,kikn}@meiji.ac.jp

あらまし　今日企業は多くのサイバー攻撃を受けている．例えば，2018 年には 443 件の個人情報漏洩インシデントが発生し，約 561 万件の個人情報が漏洩した．従って組織は，自社の業種などの各種属性を把握して起こり得る全ての脅威を予測し，被害規模を最小化するように務める必要がある．我々は 2005 年から 2018 年に起きた 15,604 件のインシデントを分析し，その被害規模と発生頻度の間に相関があることを発見した．本稿では，この知見を用いて，インシデントを 3 つの漏洩原因に分類し，16 業種と組み合わせて，インシデント発生履歴から将来起きるであろうインシデントの被害規模とその頻度を算出するモデルを提案する．

キーワード　個人情報漏洩，インシデント

A proposal of model for scale and frequency of cyber incidents based on organizational attributes

Kazuki IKEGAMI† and Hiroaki KIKUCHI††

† Graduate School of Advanced Mathematical Sciences，Meiji University
†† Department of Frontier Media Science, School of Interdisciplinary Mathematical Sciences，Meiji University
E-mail: †{cs192021,kikn}@meiji.ac.jp

1. はじめに

2020 年 12 月 1 日，paypay 株式会社は不正アクセスを受け，第三者に最大約 2,000 万件の情報が漏洩した[1]．日本ネットワークセキュリティ協会（JNSA）の調査によると，2018 年の 1 年間で 443 件のインシデントが発生し，561 万件の個人情報が漏洩した [1]．インシデント 1 件あたりの平均想定損害賠償額は 6 億 3,767 万円に上り，前年と比較しても 9,000 万円の増加であった．このように近年，不正アクセスや内部犯行といった悪意のある攻撃による個人情報漏洩が増加している．

これらの脅威に対して，組織は，自社の業種などの各種属性を把握して起こり得る全ての脅威を予測し，被害規模を最小化するように務める必要がある．対策の一つとして，セキュリティ保険が日本でも 2015 年から大手保険会社で取り扱われ始めた．しかし，保険加入率 50% のアメリカ [2] などの諸外国に比べてセキュリティ保険の加入率が 17.2 %（2017 年，ICDJapan 社調査）と低い．[3] では，その理由として「情報漏洩の可能性を感じていない」，「費用対効果が見えない」が挙げられていた．多くの組織では，サイバーインシデントを受ける確率を過小に見積もり，ISMS などの認証を取るのにかかるコストに対して，それに見合う必要性を認識していない現状がある．従って，各組織のインシデントリスクを簡易的に定量化できれば，セキュリティ意識の向上やセキュリティ対策への投資などの経営戦略に利活用する有益な情報を提供できる．

このような背景から，本研究はある組織で将来起きるであろうインシデントの被害規模とその頻度を算出することを目的とする．そこで，我々は 2005 年から 2018 年に起きた 15,604 件のインシデントを分析したところ，その被害規模と発生頻度の間に興味深いある相関があることを発見した．本稿では，この知見を用いて，インシデントを 3 つの漏洩原因に分類し，16 業種と組み合わせて，インシデント発生履歴から将来起きるであろうインシデントの被害規模とその頻度を算出するモデルを提案する．

（注1）：PayPay 株式会社 HP https://paypay.ne.jp/notice/20201207/02/

2. 関 連 研 究

2.1 インシデントリスク

リスク評価の先行研究として，Edwards らは 2005−2015 年の PRC(Privacy Right Clearinghouse) 公開データセットの 2,234 件のインシデントを使用して，アメリカの個人情報漏洩の傾向を調査した [4]．彼らは，インシデントによる被害人数と発生頻度をモデル化した．ベイズ一般化線形モデル (Bayesian Generalized Linear Models) を用いて，悪意のある攻撃により発生した 1 インシデントの被害人数に対数正規分布，人的ミス等による被害人数に対数歪曲正規分布 (Log SkewNormal)，インシデントの発生頻度に負の二項分布が適切であることを突き止め，インシデントの被害人数と頻度が 2005−2015 年の間に変化していないことを示した．提案モデルにより，全米で単年度に生じるインシデント発生総数を予測した．

Romanosky らは，Advicen 社が収集した 2005 年から 2015 年のアメリカ企業の 11,705 件のインシデントを用いて各年に企業が被った損害額を企業の収益や漏洩情報の件数，企業の種類などから算出するモデルを提案した [6]．

Ravi らは．犯罪の機会理論，institutional anomie theory, institutional theory を個人情報漏洩に影響する因子を明らかにするために応用した [7]．彼らは，IT セキュリティへの投資とインシデントインシデントの高いリスクに強い相関があることを示した．Martin らは．多次元尺度構成法と適合度テストを使用してインシデントの分布を分析し，モデルを保険数理領域での適合度，価格設定，およびリスク測定に関する現在の議論に繋げた [8]． Maochao らは 2005-2017 年のサイバーハッキングインシデントの到着間隔と被害の大きさを確率過程によりモデル化した [9]．提案モデルにより到着間隔と被害規模を予測できることを示した．

2.2 インシデントの交絡因子

山田らは，200 項目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抑制効果を分析した．彼らは，その過程で，業種や企業規模，観測年などの属性によってインシデント発生の偏りがあり，マネジメント効果の交絡因子として働いていたことを明らかにした．例えば，電気・ガス業界では他の業界と比べて約 11 倍インシデントが発生しやすく，企業規模が大きくなるほどインシデントリスクが増加することを示した．彼らは，その原因として重要インフラであり多くの顧客情報を持つことや従業員が増えることでの人的ミス増加を指摘している．

従って，被害規模と頻度を目的とする本分析のために，先行研究で交絡因子と指摘されていた業種に漏洩原因も加えて，インシデント発生を予測するモデルを構築する．

Edwards らの研究では，被害規模や頻度を各々別々のモデルで定式化している．しかし，後述するように被害規模と頻度は独立ではなく，これらは本来互いに影響する因子として合わせて分析するべき量である．表 1 に，本提案と主要な関連研究との比較を示す．Edwards らが，独立に算出した被害規模と頻度の間の相関を考慮して，被害規模を説明変数として頻度を見積もるモデルとしたところに，本研究の特徴がある．

表 1　本研究の位置づけ

	本分析	Edwards [4]	山田ら [5]
目的変数	頻度	**被害規模**，頻度	生起確率（頻度）
説明変数	**被害規模**，業種，漏洩原因	時間（日）	マネジメント方策，業種，企業規模
データ	JNSA(2005-2018)	PRC(2005-2016)	JNSA(2012-2016) Security Next
対象	（単一）企業	国内全企業	（単一）企業

3. 提案モデル

3.1 JNSA データセット

JNSA セキュリティ被害調査ワーキンググループは，企業のプレスリリースやニュースサイトなどでの報道から個人情報漏洩インシデントを 2005 年から毎年収集している [1]．企業経営者がセキュリティ対策投資を行う際の参考情報として，インシデント情報を被害人数，漏洩原因 (紛失 ・置忘れ，不正アクセス，誤操作等)，漏洩経路（紙媒体，インターネット等）に分類し，評価を行っている．

JNSA データセットには，2005-2018 年の 16,392 インシデント，計 9,358 組織のデータが含まれる．本稿では，被害人数と業種名が欠損していない 15,604 インシデント，9,007 組織を使用する．

3.2 インシデント生起モデル

図 1 に，ある組織に生起したインシデントのモデルを図示する．観測期間に業種 k 組織 j で，i 番目に起きたインシデントの日付を t_i，被害規模を S_i(人)，t_{i-1} から t_i までの日数を発生間隔 d_i(日)，期間内に起きたインシデント合計件数を C とする．

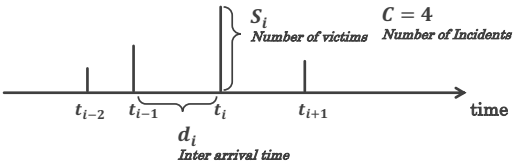

図 1　インシデント生起モデル

3.3 被害規模と発生間隔

図 2 に JNSA の 9,007 組織の平均被害人数 S とインシデント数 C の分布を示す．インシデント数 C が多い企業ほど，平均被害人数 S は小さくなる傾向がある．例えば，図 2 の x_4 と x_5 は地方銀行，x_6 と x_7 は自治体（大都市）であり，インシデント数 C が多いが 1 インシデントあたりの被害規模 S は小さい．一方で，x_1（教育業界大手）や x_2（総合印刷業），x_3（大手クレジットカード会社）は，いずれも一部上場の大企業であり，インシデント数 C は少ないが一度の被害規模 S が大きくなる．そこで，被害規模 S は企業によって決まる固有の値になるという仮説が立つ．

この仮説検証の真偽を明らかにするために，図 3 に代表的な組織ごとの被害規模の分布を示す．組織 1 は，S が正規分布に従い，組織 2 は小規模の偏りがある．組織 3 は大規模に偏っているが，小規模のインシデントも生じている．いずれも，発生分布に違いがあるが，企業ごとに固有の被害規模があるという仮説は成立していない．全 9,007 組織の S の分散を精査した上

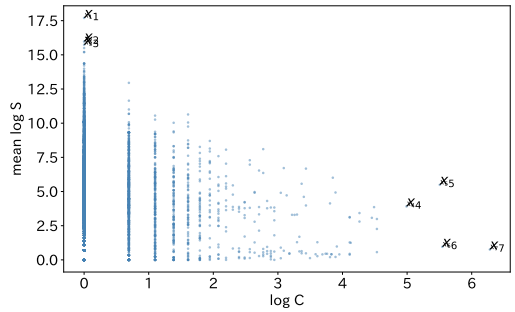

図 2　平均被害規模 S とインシデント数 C の分布

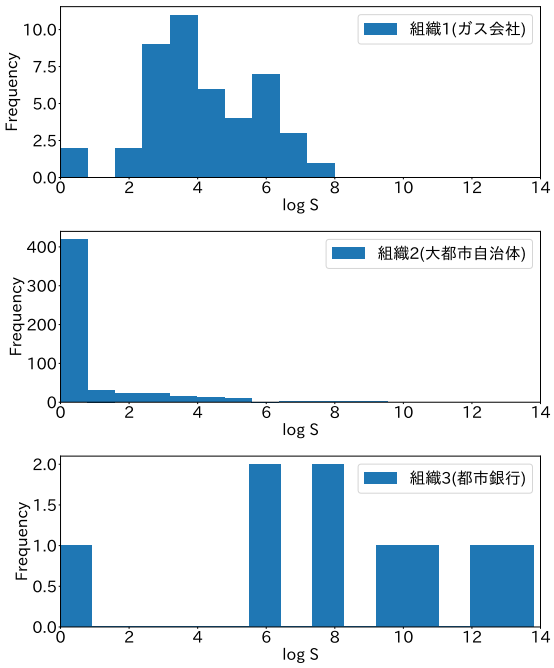

図 3　代表組織の被害規模 S の分布

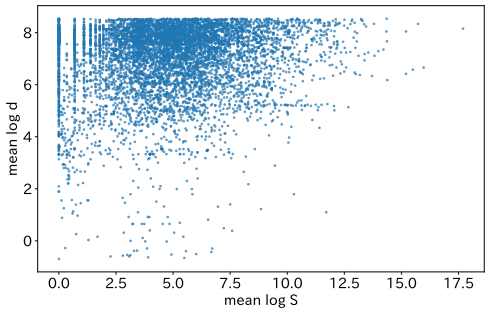

図 4　被害規模 S と発生間隔 d の分布

で，いかなる組織も小規模から大規模までインシデントが発生していたことを確認した．従って，組織と被害人数は独立であり，S に応じた C のモデルを考える必要がある．

3.4　提案モデル

我々は，3.3 節の観測に基づきインシデントの頻度 C とその規模 S の間に負の相関があると仮定する．すなわち，被害人数の多い大規模インシデントはまれにしか発生せず，被害人数の少ないインシデントは頻度が高い．そこで，次のモデルを提案する．

組織 j における，観測期間 T の平均被害規模 $\bar{S}_j$ とインシデント数 C_j の対数は，次の式に従う．

$$\ln C_i = \frac{1}{\alpha \ln \bar{S}_j} \tag{1}$$

ここで，α は，業種 k と漏洩原因 ℓ から決まる定数である．C と S がこのモデルに従うならば，任意の被害人数 S_j における推定インシデント数は

$$\hat{C}_j = \mathrm{e}^{\frac{1}{\alpha \ln S_j}}$$

で求まり，$\hat{C}$ についてインシデント発生確率 P_j と発生間隔 d_j は，インシデントの観測期間を T とすると

$$\hat{P}_j = \frac{\hat{C}_j}{T}, \qquad \hat{d}_j = \frac{T}{\hat{C}_j}$$

に従う．

図 4 に，組織ごとの平均被害人数 S と平均発生間隔 d の分布を示す．S が大きいほど d が大きくなり，S が小さいほど d が小さい組織が多くなっている．(1) 式が成り立つ時，d は

$$d = T\mathrm{e}^{\frac{1}{\alpha \ln S_j}}$$

で得られる．従って，S が大きいほど d が大きくなる傾向は提案モデルにも当てはまっている．

4.　分　　析

4.1　漏 洩 原 因

JNSA ではインシデントを 13 種類の漏洩原因に分類している．被害人数の分布は 13 種類あるわけではなく，いくつかの原因は同じ振る舞いをしている．従って，いくつかの漏洩原因を表 2 に従って分類して分析を行う．Negligent は人的ミス，Malicious は外部の第三者による悪意のある攻撃，Insider は内部犯を示す．本稿では，Other を除いた 3 分類を使用する．

表 3 に，漏洩原因の統計量を示す．Negligent は Malicious に比べてインシデント数が 4 倍であるが，平均被害人数は 3 分の 1 である．それ故に，明らかに統計量だけでなく，被害人数 S の分布も漏洩原因に依存する．図 5 に示すように，Negligent のみ，$\log S < 1.0$ の小さなインシデントが多く発生しており，二つのピークがある．一方 malicious には，この小規模インシデントが観測できない．

表 2　漏洩原因の分類

本分類	JNSA の漏洩原因
Negligent	紛失・置忘れ，誤操作，管理ミス
Malicious	不正アクセス，設定ミス，盗難， ワーム・ウイルス，バグ・セキュリティホール
Insider	内部犯罪・内部不正行為，不正な情報持ち出し， 目的外使用
Other	不明，その他

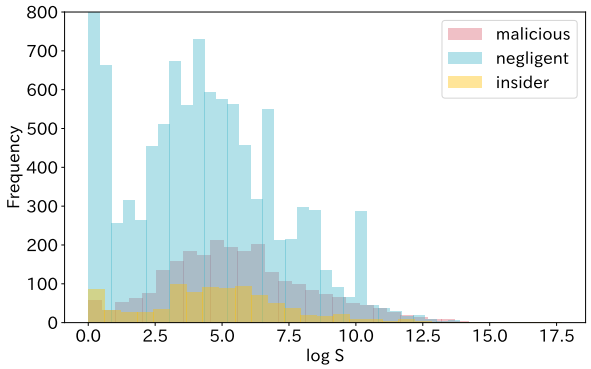

図 5　漏洩原因別被害人数の分布

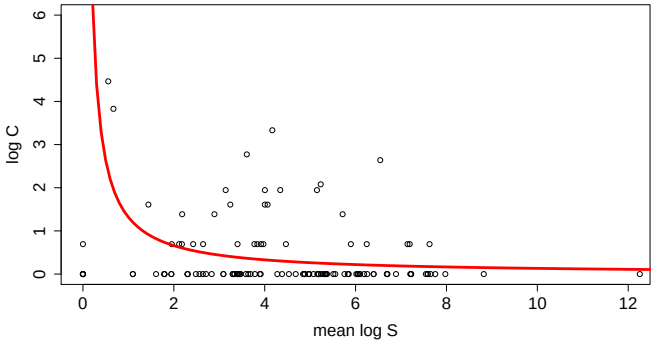

図 6　電気・ガス業の negligent のインシデント分布

表 3　漏洩原因別の被害人数 S の統計量

	Malicious	Negligent	Insider
C	2,154	8,194	692
mean(S)	19,022	6,445	105,583
std(S)	189,436	164,376	1,888,877
min(S)	1	1	1
max(S)	6,788,443	14,430,000	48,580,000

4.2　モデルのパラメータ推定

4.1 節で分類した 3 種類の漏洩原因 ℓ，JNSA が分類した 16 種の業種 k 別とした計 48 種類ごとに 3.4 節で提案したモデルのパラメータ $\alpha_{k\ell}$ を推定する．パラメータは R の glm 関数を使用し推定する．また，パラメータ推定を収束させるために，$\log C$, $\log S$ が 0 の値をそれぞれ $1e-10$ に置換した．

推定結果の例として，図 6, 7 に電気ガス業種の negligent と公務の malicious，表 4 に全業種の全原因のパラメータの推定結果を示す．ここで，推定に用いたデータは 2005 年から 2018 年である．

α は，発生頻度の逆数の係数であり，α が小さいほど同じ被害規模 S でモデルを比較したときにインシデント数 C が多くなることを意味する．malicious と negligent では，電気・ガス・熱供給・水道業，insider では情報通信業の α が最小であった．一方で，insider では他に比べて α が著しく高い業種が多く，7 業種 (16 業種中) で $\alpha > 1.0E+09$ だった．また，農業，林業はサンプル数が小さくパラメーター計算が収束しなかったため除いた．これらの原因については， 5.3 節で述べる．

5.　評価・考察

5.1　提案モデルの誤差

提案モデルを用いて過去 5 年のインシデントから翌年のインシデント発生数を次の手順で推定する．インシデント発生数は表 5 に示す被害規模別 S_S, S_L に推定する．

（1） y 年から T 年間を α 推定の学習データ，$y+T+1$ 年をテストデータとする．

（2） 学習データ内で業種 k，漏洩原因 ℓ についてモデルを作成

（3） 作成したモデルから大規模 ($S_L = 1,000$)，小規模 ($S_S = 1.5$) インシデントの発生数をそれぞれ $\hat{C}_{k\ell}(S_L)$ と $\hat{C}_{k\ell}(S_S)$ と推定する．

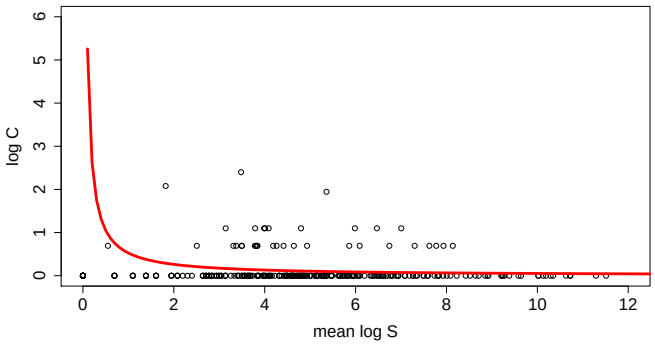

図 7　公務の malicious のインシデント分布

表 4　業種，漏洩原因別の推定パラメータ $\alpha_{k\ell}$

業種 k	漏洩原因 ℓ		
	mailcious	negligent	insider
サービス業 (他に分類されないもの)	5.38	5.80	9.64
医療，福祉	6.01	3.96	2.66
運輸業，郵便業	1.69	2.09	1.75.E+09
卸売業，小売業	3.26	2.62	1.78.E+09
学術研究，専門・技術サービス業	1.70.E+09	8.09	–
教育，学習支援業	2.25	2.67	7.26
金融業，保険業	3.00	1.24	2.79
建設業	2.08	1.43	1.67
公務 (他に分類されるものを除く)	1.90	1.55	3.54
宿泊業，飲食サービス業	2.74	4.89	1.40.E+09
情報通信業	1.79	1.73	0.98
生活関連サービス業，娯楽業	6.93	3.23	1.86.E+09
製造業	4.33	2.84	1.47.E+09
電気・ガス・熱供給・水道業	**1.01**	**0.76**	**5.81**
不動産業，物品賃貸業	2.02	1.62	2.41.E+09
複合サービス事業	1.89.E+09	2.20	1.27.E+09

表 5　被害規模 S の分類

被害規模	cassification method
S_S	$S_j \geqq 1,000$
S_L	$S_j < 1,000$

ここで，T を 5 年，最初の y を 2005 年として，テスト年 y' が 2018 年になるまでの 9 回評価を行う．

次に，インシデントの推定発生数 $\hat{C}_{k\ell}$ の評価方法を示す．

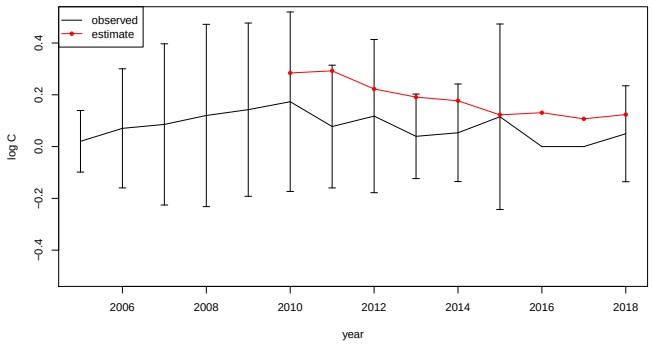

図 8　情報通信業種の観測値 $\log C$ と予測値 $\log \hat{C}$

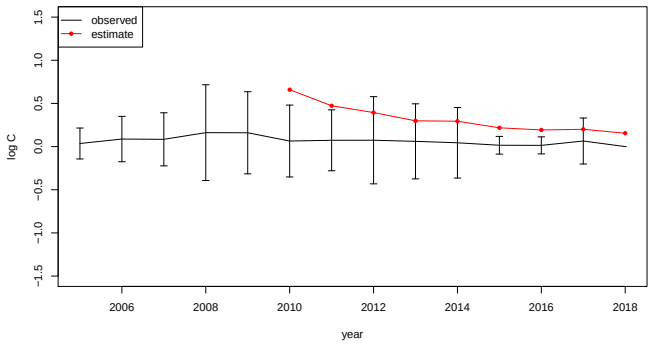

図 9　金融業の観測値 $\log C$ と予測値 $\log \hat{C}$

（1） テストデータ内で組織 j 毎に規模 S のインシデント数 $C_{jk\ell}$ を集計する (観測値).

（2） 各組織 j の被害規模 S_S, S_L ごとに予測誤差 E を計算する.

$$\log E_{jk\ell}(S_S) = |\log C_{jk\ell}(S_S) - \log \hat{C}_{k\ell}(S_S)|$$

表 6 に，漏洩原因が negligent で小規模被害 S_S，malicious で大規模被害 S_L を業種別でそれぞれ推定した時の誤差の統計量を示す．表 6 で，Nは組織数, $\bar{C}$ は 1 組織における平均インシデント発生数， $\log S$ は被害規模の対数平均を示す．

negligent で平均誤差が最小の業種は，学術研究・専門・技術サービス業で約 1 件 ($\log E = 0.053$) であり，malicious では複合サービス事業で約 1 件 ($\log E = 4.57E-11$) であった．negligent の小規模被害で，平均誤差が最大の業種は電気・ガス・熱供給・水道業であり，malicious の大規模被害で平均誤差が最大の業種は金融業，保険業である．

また，negligent の小規模被害で業種内最大誤差は公務の 121 件 ($\log E = 4.8$)，Malicious では教育，学習支援業の 1.9 件 ($\log E = 0.68$) が最大である．

表 6 内の全データ（業種，漏洩原因で分けなかった時）と各分類 $k\ell$ の平均被害規模を比較すると Neligent では 13(16 中) 業種で，Malicious では金融業・保険業を除く 15 業種で精度が向上した．また，Neligent の小規模被害では，全データモデルに比べて平均誤差が最大で 0.17 倍になる．これらの誤差が大きくなった原因については 5.3 節で考察する．

また，図 8，図 9 に，情報通信業と金融業の 2 業種の各業種内での平均インシデント発生数 C とモデルの予測結果 $\hat{C}$ を示す．$T = 5$ 年間としているため，2009 年までの最初の 5 年間は予測値がない．観測された C は 95% の信頼区間を図に示している．予測 $\hat{C}$ が十分な制度で精度で推移していることが示されている．

5.2　その他のモデルとの比較

次のモデル候補 $f_1, \ldots, f_4$ による当てはめを検討する．

$$f_1(x) = \frac{1}{\alpha \ln \bar{S}_j} \qquad \text{(m1)}$$

$$f_2(x) = \frac{1}{\alpha + \beta \ln \bar{S}_j} \qquad \text{(m2)}$$

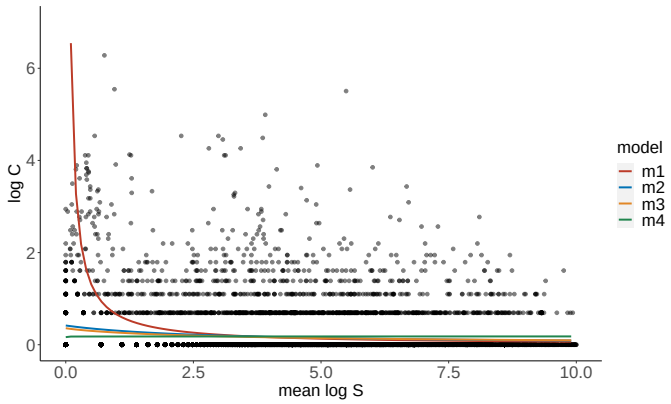

図 10　モデルの比較

$$f_3(x) = \frac{1}{\alpha + (\ln \bar{S}_j)^\beta} \qquad \text{(m3)}$$

$$f_4(x) = \frac{\alpha}{\ln \bar{S}_j^\beta} \qquad \text{(m4)}$$

図 10 に推定した各モデルと，観測値の分布を示す．モデル（m1）以外は，$\log C$ の値域が限られており，全てが 1 以下であった．実際の被害は，図 10 に示すように $C \geq e$ もありうることから，本稿では，m1 を採用した．

5.3　考　　察

図 11， 12 に，パラメータが他に比べて大きかった業種，漏洩原因の分布を示す．それぞれの分布は，ほとんどの被害規模でインシデント数が 1 回のため α が大きくなっていた．また，表 3 から他の漏洩原因に比べてインシデント数が少ない．従って，Insider では本モデルが適していないと考える．

次に，最大誤差の大きかった公務と，金融業・保険業について考察する．これらの業種で誤差が大きくなった原因には，外れ値となる組織が存在したため考える．例えば，公務の誤差が最大となった 2010 年には Y 市で 159 件，O 市で 77 件のインシデントが発生しているが，それ以外の 2010 年に公務の業種で起きた組織毎のインシデントは全て 10 以下である．また，金融業・保険業で誤差が最大となった 2012 年には，F 銀行で 246 件インシデントが発生しているが，それ以外に 2012 年で金融業で起きた 506 の組織の平均インシデント数は 1.6 件であった．従って，外れ値となる特異な組織のインシデント発生数により

表 6　誤差の統計量

industry k	N	$\bar{C}$	$\log S$	$\log E$ (negligent, S_S) μ	max	min	σ	$\log E$ (malicious, S_L) μ	max	min	σ
公務 (他に分類されるものを除く)	1,507	2.949	1.922	0.444	4.849	0.213	0.382	1.52.E-02	6.86.E-01	5.80.E-03	1.95.E-02
金融業，保険業	2,278	1.804	5.495	0.343	4.736	0.034	0.208	2.32.E-02	6.87.E-01	6.37.E-03	3.47.E-02
教育，学習支援業	1,468	1.283	4.353	0.161	4.433	0.088	0.151	1.15.E-02	6.89.E-01	3.70.E-03	1.30.E-02
情報通信業	631	1.474	4.844	0.215	1.487	0.107	0.103	1.62.E-02	6.82.E-01	1.09.E-02	1.59.E-02
医療，福祉	693	1.322	3.383	0.126	2.020	0.059	0.154	3.29.E-03	5.56.E-03	4.86.E-04	2.98.E-11
卸売業，小売業	543	1.208	5.538	0.177	0.951	0.086	0.041	4.85.E-03	1.00.E-02	1.81.E-11	4.74.E-11
サービス業 (他に分類されないもの)	533	1.118	5.435	0.244	4.849	0.034	0.173	1.87.E-03	6.27.E-03	1.77.E-11	3.96.E-11
電気・ガス・熱供給・水道業	171	2.942	3.288	0.567	2.535	0.118	0.339	1.80.E-02	2.62.E-02	4.42.E-03	2.69.E-11
製造業	292	1.168	5.948	0.120	0.546	0.077	0.012	4.65.E-03	7.73.E-03	1.77.E-11	4.24.E-11
不動産業，物品賃貸業	183	1.683	3.165	0.246	1.850	0.068	0.102	6.78.E-03	1.74.E-02	1.90.E-11	1.64.E-11
複合サービス事業	212	1.302	5.115	0.272	3.422	0.134	0.294	4.57.E-11	8.64.E-11	1.36.E-11	4.07.E-11
運輸業，郵便業	161	1.348	5.651	0.232	2.960	0.131	0.111	1.63.E-02	3.61.E-02	1.15.E-11	3.19.E-11
建設業	89	1.663	3.927	0.226	0.761	0.000	0.037	1.00.E-02	1.40.E-02	4.21.E-03	2.41.E-11
生活関連サービス業，娯楽業	88	1.102	5.597	0.130	0.601	0.000	0.054	8.51.E-04	7.66.E-03	1.92.E-11	2.28.E-11
学術研究，専門・技術サービス業	79	1.063	5.281	0.053	0.640	0.000	0.030	6.27.E-11	8.57.E-11	1.66.E-11	3.21.E-11
宿泊業，飲食サービス業	73	1.110	5.669	0.066	0.157	0.000	0.000	1.02.E-02	2.45.E-02	1.67.E-11	4.23.E-11
全データ	9,007	1.732	4.658	0.297	4.874	0.199	0.253	1.81.E-02	4.33.E+00	1.17.E-02	5.29.E-02

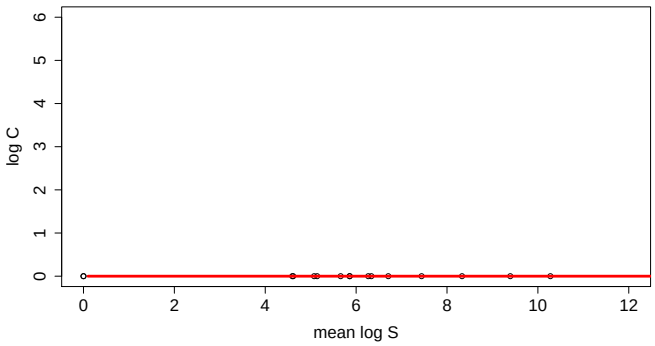

図 11　運輸業，insider のインシデント分布

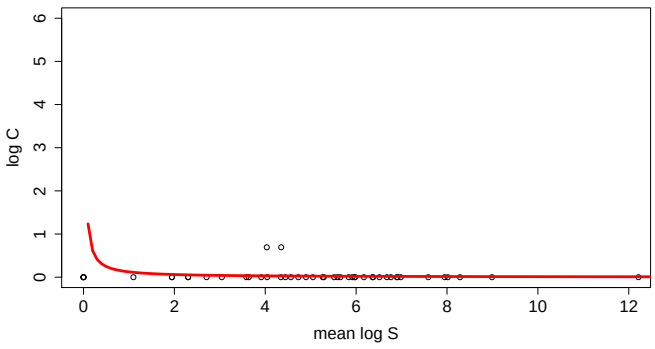

図 12　学術研究業種，negligent のインシデント分布

これらの業種では誤差が大きくなったと考える．

6. おわりに

本稿では，2005 年から 2018 年に起きた 15,604 件のインシデントを用いて，被害人数 S からインシデント数 C を推定するモデルを提案した．モデルの精度を上げるために，被害人数の分布が近い組織を 3 つの漏洩原因，16 種類の業種から作成，それら 48 分類別にモデルを作成した．48 分類別にモデルを作成することで，negligent の小規模インシデントでは全データを作成したモデルよりも 13(16 中) 業種で精度が改善し，neligent の小規模被害では，全データモデルに比べて平均誤差が最大で 0.17 倍になることを示した．また，モデルによる推定インシデント数の平均誤差の最小は，negligent の小規模被害と malicious の大規模被害のそれぞれで 1 件だった．さらに，推定モデルの誤差の原因が外れ値となる特異な組織の存在であることを指摘した．

文　献

[1] 日本ネットワークセキュリティ協会，2018 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～(速報版).

[2] NRI Secure Insight 2019 企業における情報セキュリティ実態調査，（https://www.secure-sketch.com/ebook-download/insight2019-report, 2021.1.12 参照）.

[3] 佐久間樹里，猪俣敦夫，サイバー保険の調査・分析による加入率向上への提案，研究報告インターネットと運用技術 (IOT)(IPSJ), pp. 1-8，2019

[4] B. Edwards, S. Hofmeyr, and S. Forrest, Hype and heavy tails: A closer look at data breaches, Journal of Cybersecurity, 2(1):3–14, 2016.

[5] 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(IPSJ), pp. 376-384, 2018.

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

[7] Sen R, Borle S, Estimating the Contextual Risk of Data Breach: An Empirical Approach. Journal of Management Information Systems, **32**:314–34, 2015.

[8] Eling M, Loperfido N, Data breaches: Goodness of fit, pricing, and risk measurement. Insurance:Mathematics and Economics. **75**:126–136, 2017.

[9] M Xu, K Schweitzer, R Bateman, S.Xu, Modeling and Predicting Cyber Hacking Breaches, IEEE Transactions On Information Forensics And Security, pp.2856-2871, 2018.