個人情報漏洩の損害額の新しい数理モデルの提案

山田　道洋[1]　菊池　浩明[1]　松山　直樹[2]　乾　孝治[2]

1:明治大学大学院先端数理科学研究科FMS専攻

2:明治大学大学院先端数理科学研究科現象数理学専攻

はじめに：サイバーセキュリティリスク

- 近年，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（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
- このような個人情報漏洩による被害額の算出にはセキュリティ保険の観点から大きな需要がある

ＭＳ＆ＡＤ、１月のサイバー保険契約13倍に　中小の意識高まる

ツイート　シェア 7　LINEで送る　(2018/2/28 05:00)

ＭＳ＆ＡＤインシュアランスグループホールディングの１月のサイバー保険契約件数が前年同月比１３・５倍となった。２０１７年の「ランサムウェア騒動」などを受けて企業のサイバー攻撃への意識が高まり、大企業だけでなく中小企業の契約も伸びた。

同社は１月にサイバー保険を刷新、三井住友海上火災保険の「サイバープロテクター」、あいおいニッセイ同和損害保険の「サイバーセキュリティ保険」として発売。中堅・中小企業でも加入しやすいよう三つのプランから補償を選択する分かりやすい商品設計とした。従来に比べ調査費用や対策費用の補償を充実させたことも好評だ。

日刊工業新聞（2018年2月28日）

被害額の評価1：JOモデル[2002]

- 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は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を集計し，分類・評価
- これらの情報から各企業の想定損害賠償額を算出する JNSA Damage Operation Model for Individual Information Leak（JOモデル）を2002年に提案

損害賠償額＝漏洩情報価値 × 社会的責任度 × 事後対応度
＝（基礎情報価値 × 機微情報度 × 本人特定容易度）× 社会的責任度 × 事後対応度

被害額の評価2：Romanosky[2016]

- Advicen社より入手した 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モデルを提案

$$\log(cost_{i,t}) = \beta_0 + \beta_1 \times \log(revenue_{i,t}) + \beta_2 \times \log(records_{i,t}) + \beta_3 \times repeat_{i,t} + malicious_{i,t} + \alpha \times Firmtype_{i,t} + \lambda_t + \rho_{ind} + \mu_{it'}$$

cost: 損害額，revenue:売上高，records:被害人数，
repeat：過去にインシデントが発生しているかどうか，malicious：故意か否か，
lawsuit：訴訟されたかどうか，FirmType：政府機関か一般企業かなど

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

先行研究の問題点

- JOモデル

損害賠償額＝基礎情報価値[500]

$\times$ 機微情報度$[\max\left(10^{\max(x)-1}+5^{\max(y)-1}\right)]$

$\times$ 本人特定容易度[6,3,1] $\times$ 社会的責任度[2,1] $\times$ 事後対応度[2,1]

1. 500円，3倍などの定数は専門家の主観で定められたものであり，その根拠がない
2. 16年前に設計された古いモデルであり，最近の法改正などの事情が考慮されていない
3. 予測された損害額の信頼性が不明

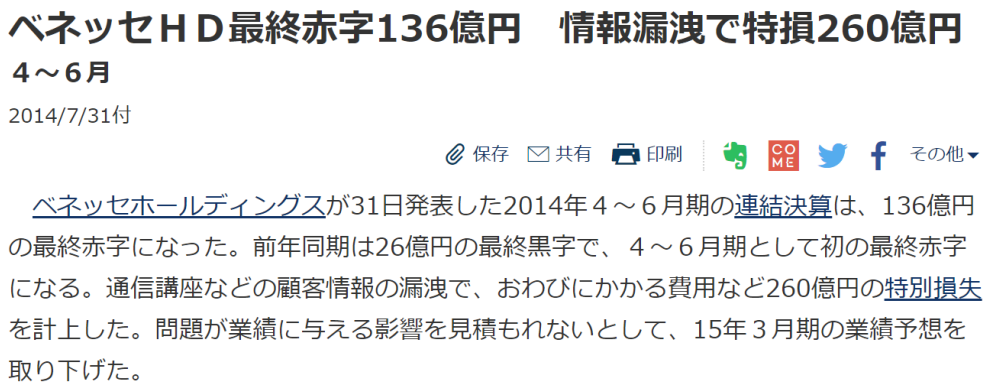
» ベネッセHD：1人当たりの賠償額33000円

提案手法

1. 専門家の主観
   - 漏洩した情報や企業規模などを説明変数として重回帰を適用
2. 古いモデル
   - 2010年から2016年のインシデント情報を使用
3. 信頼性
   - 重回帰の目的変数を特別損失額を利用

特別損失額

- 企業の通常の経営活動では発生しない，特別な要因によって一時的に発生した損失



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。

日本経済新聞（2014/7/31）

- 他の企業においてもインシデントによる損失額は特別損失として計上されると考えられる
- 目的変数として重回帰を適用することで現実の事例に近い損失額を予想できる

データの精査

- 年度ごとのデータの集約
  - 同一企業にて同年度中に複数回インシデントが発生した場合，「被害人数」などのデータを集約
    - » サイバーエージェント社：2016年度　640,368件
    - » 2016年5月11日（50,905件），2016年11月29日（589,463件）
- 2009年以前のデータの除外
  - 特別損失額は災害や社会情勢などの影響によっても増加する
  - リーマンショックの影響を排除するため，本研究では2010年以降のデータを使用

企業名	2008	2009	2010	2011	2012	2013	2014
日産自動車	86580	108187	86679	85662	61752	32357	24939
東京電力HD	269288	68811	-	1077685	2867864	1248811	1462243

アニュアルレポートの調査

- 特別損失額は全額がインシデントに関与しているわけではない
  - ex システム開発中止に伴う損失，事業構造改善費用
- 被害人数上位105件のインシデントについてアニュアルレポートなどを調査
- 5件のレポートに「情報セキュリティ対策費」と記載あり
  - 「昨年 9 月 15 日付で「当社お客様情報の流出に関するお詫びとお知らせ」を公表しました．その後の二次的な被害に関しましては，現在のところ報告されておりません．外部からの不正アクセスにより個人情報が外部に流出した懸念があり，それらに関わる対応費用を情報セキュリティ対策費として計上しております．」（セキ株式会社）

漏洩損害額の仮定

- セキュリティ対策費を真の損失額とし，特別損失額による単回帰を行った
- その結果から　漏洩損害額y=0.849・特別損失額　と仮定

企業名	年度	セキュリティ対策費 [百万円]	特別損失額 [百万円]	0.849×特別損失額 [百万円]	誤差[%]
ベネッセHD	2015	26039	30642	26045.7	0.025
セキ	2016	210.67	234	198.9	5.917
ストリーム	2014	5.56	66	56.1	908.992
ミサワ	2012	27.24	42	35.7	31.057
アークン	2016	8.92	11	9.35	4.820
平均		5256.69	6199.4	5269.15	190.162

損失モデルの算出

データ	期間	件数	出典
インシデントデータ（年度別データ）	2010－2016	180件（144件）	JNSAデータセット
会計データ	2010－2016	144件	決算短信
情報セキュリティ対策費	2012－2016	5件	決算短信

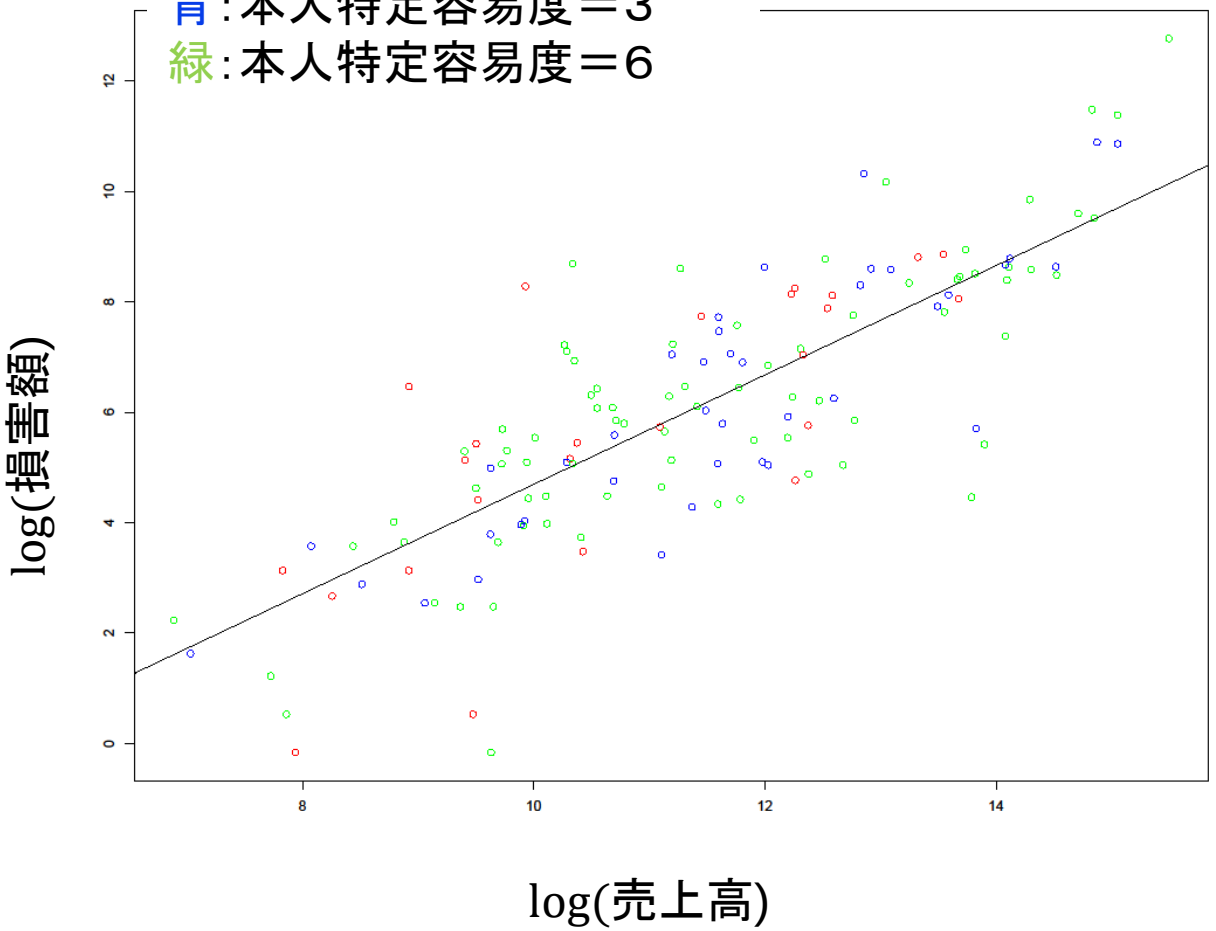
線形重回帰モデル

- 16の説明変数に対して漏洩損害額を目的変数としてRのlm関数を用いて重回帰を適用

$$\log(\text{漏洩損害額}) = \beta_0 + \beta_1 \times \log\left(x_{\text{売上高}}\right) + \beta_2 \times \log\left(x_{\text{被害人数}}\right) + \cdots$$

提案モデル

赤：本人特定容易度＝1
青：本人特定容易度＝3
緑：本人特定容易度＝6



係数			*Estimate*	*p.value*	
β_0			-3.963	0.009	***
log(被害人数)	$\log(x_1)$	β_1	0.038	0.461	
log(売上高)	$\log(x_2)$	β_2	0.990	2.18E-23	***
本人特定容易度	x_7	β_7	0.208	0.693	
業種 建設業	x_8	β_8	-2.340	0.002	***
業種 金融業	x_8	β_8	2.676	0.010	**
電話番号	x_{11}	β_{11}	-0.533	0.079	*

各モデルでの損失額

企業名	日付	被害人数	JOモデル [百万円]	Romanosky [百万円]	提案モデル [百万円]	漏洩損害額 [百万円]	情報セキュリティ対策費 [百万円]
ベネッセHD	2014	48580000	160314E+4 (33000円/人)	2367.64 (48.74円/人)	13287.36 (237円/人)	26045.7	26039
セキ	2015	267000	41652	325.19	87.43	198.9	210.68
ストリーム	2014	94359	566.15	256.64	152.89	56.1	5.56
		平均	1167345.56	57.32	2741.46		
		平均誤差	1172502.69	6398.99	4866.99		
		平均誤差率	181.82	0.99	0.75		

JOモデルとの比較：式変形

- JOモデルと提案モデルでは形式が異なるように見えるが，提案モデルを変形すると等価

損害賠償額＝基礎情報価値[500]
× 機微情報度$[\max\left(10^{\max(x)-1}+5^{\max(y)-1}\right)]$
× 本人特定容易度[6,3,1] × 社会的責任度[2,1] × 事後対応度[2,1]

漏洩損害額＝$e^{\beta_0}\times x_1^{\beta_1}\times x_2^{\beta_2}\times e^{\beta_3\cdot x_3}\ldots$
＝$0.019\times$被害人数$^{0.037}\times$売上高$^{0.99}\ldots$

JOモデルとの比較：係数

- JOモデルでは経済的ランクx_5，精神的ランクx_6，本人特定容易度x_7について，その段階によって10 倍，5 倍のように想定損害額が定数倍されている

経済的ランク	JOモデル	10^0	10^1	10^2
	提案モデル	1	1.1723	1.3743
精神的ランク	JOモデル	5^0	5^1	5^2
	提案モデル	1	1.0129	1.0261
本人特定容易度	JOモデル	1	3	6
	提案モデル	1	1.5158	2.89291

おわりに

- 個人情報漏洩の損害額の新しい数理モデルの提案を行った
  - 2010～2016年の144件（115社）の被害額を元に評価
    - » JOモデルの平均誤差率が181.82に対して，0.75の精度の高いモデルを示した
    - » ベネッセでの損害額：275円/人（JOモデルでは33000円/人）
- 今後の課題
  - インシデントだけに関連する損失額のデータの収集
  - 営利企業でない団体などへの対応
  - ガバナンスの影響