

異なる二業種間でのサイバーセキュリティの比較

氏 名† 高正 智

所 属† 株式会社富山第一銀行

1 はじめに

サイバーセキュリティには数々の側面があるが、本論文では研究対象を個人情報の漏洩リスクに絞り、かつ法人の金融業と小売業に絞る。従業員の意識するサイバーセキュリティに関し、金融業と小売業の間で、外部環境の変化、リスク対応、ガバナンス対応の3要素の連関を比較する。

2 先行研究

具体的な類似研究として、サイバーセキュリティに関する全業種の上場法人の従業員の意識や取り組みに関する先行研究としては、江口（2021）がある。セキュリティに関する外部からの要請が高まると、方針の認知度が上がるといった相関関係が質問紙調査と共分散構造分析を用いて報告されている [1]。

3.本論文のアプローチ

本論文では質問紙調査を通じて、金融業と小売業の現場の意識における以下の2つの仮説を検証する。

- ・サイバーセキュリティ全般に関し、個人情報を取り扱う業態として類似している。
- ・サイバーセキュリティに関し、個人情報保護法の令和4年改正適用という外部環境の変化について、小売業と金融業とで対応が異なる。

法人が対処する課題は大きく（1）リスク管理と（2）ガバナンス対応に分かれる。（1）リスク管理については、リスクの受容及び移転、なかでも初動対応、保険、費用対応に着目する。

（2）ガバナンス対応については、組織体制、IT ガバナンス、法人ガバナンス、委託先管理に着目する。

4.仮説モデルの構築

改正個人情報保護法の対応を説明変数とし、リスク対応やガバナンス対応が被説明変数として相関があると仮定する。順序尺度として観測し、複数の観測変数を潜在変数にまとめ、潜在変数の間の共分散構造分析上の相関係数をみる [2]。

表1 各潜在変数に紐づける観測変数

潜在変数	観測変数の質問項目
個人情報 の保護	改正個人情報保護法への対応
	サイバーセキュリティへの関心
初動対応	サイバー攻撃時の連絡先の認識
	サイバー攻撃に関する体制の認識
保険	保険の検討・実施
	損失費用の概算予想
組織体制	団体内での訓練
	団体外との演習
	サイバー攻撃に対応できる人材配置
IT ガバ ナンス	サイバー犯罪を防止する基本的対策
	ログの保存・監視・管理
	サイバー犯罪向け堅牢な仕組み
法人ガバ ナンス	経営トップの業務指示
	サイバーセキュリティに関する開示
委託先管 理	業務委託先の情報漏洩対策の認識
	クラウド業者のサイバー対策

5 調査内容と結果

5.1.調査の概要

2022年9月に小売業・金融業に勤務する方々におけるサイバーセキュリティについての意識と取り組みについて質問紙調査を実施した。

小売業と金融業を対象にしたのは、個人情報を取り扱う業態として類似しているとしたためである。質問紙調査はウェブ方式および郵送方式の併用とし、合計で277名からの有効回答を得た。（回答数/回答率 ウェブ方式269名/96%、郵送方式8名/6%）内容は主に7段階リッカート尺度の質問からなる。

Comparison of Cybersecurity between 2 different industries
Satoshi Takamasa† The First Bank of Toyama,Ltd.

表 2. 回答者の内訳 (単位: 社)

	小売業	金融業
上場企業	54	67
上場企業の 関連企業	14	26
大手未上場企業、団体	29	30
その他 (1000 人超の個 人顧客を持つ法人)	44	13
合計	141	136

5.2. 潜在変数における相関係数

共分散構造分析における検証的 2 因子モデルを適用した。各潜在変数間でモデル適合性を示す CFI (Comparative Fit Index) が 0.9 以上のモデルについて、以下の高い相関が認められた [3]。

表 3. 業種別の潜在変数間の相関係数

潜在変数 1	潜在変数 2	小売	金融
個人情報の保護	初動対応	0.83	0.86
個人情報の保護	保険	0.77	0.95
個人情報の保護	法人ガバナ ンス	0.79	0.85
個人情報の保護	組織体制	0.71	0.85
個人情報の保護	委託先管理	0.70	0.84
IT ガバナンス	保険	0.84	0.78
IT ガバナンス	初動体制	0.77	0.79
IT ガバナンス	組織体制	0.84	0.90
IT ガバナンス	委託先管理	0.99	0.91
IT ガバナンス	個人情報保 護	0.65	0.81
IT ガバナンス	法人ガバナ ンス	0.79	0.72
委託先管理	法人ガバナ ンス	0.81	0.83
委託先管理	初動体制	0.77	0.73
委託先管理	保険	0.88	0.86
委託先管理	組織体制	0.89	0.95

※ p 値はいずれも 0.1%未満。

相関係数の水準に着目すると、改正個人情報保護法に関する認識を高めることによって組織内の対応が高まることを示唆している。改正個人情報保護法についての認識と、初動対応、保険、組織体制、IT ガバナンス、法人ガバナンス、委託先管理との相関係数が 0.65~0.95 と高い。うち 4 か所で小売業よりも金融業が 0.14 以上強い相関係数となった。

なお IT ガバナンスと初動対応、保険、組織体制、委託先管理との連動が 0.77~0.91 と強く、両業種で類似した水準となった。また委託先管理と初動対応、保険、組織体制、法人ガバナンスとの連動が 0.73~0.95 と強く、両業種で類似した水準となった。

以上から、両業種は全般に水準の似た相関が観察されたが、個人情報保護に関する潜在変数の挙動だけが、小売業と金融業で異なっている。

6. 考察と今後の課題

令和 4 年適用の法改正で個人情報漏洩に関する報告が努力目標から義務になったこと、罰則が 1 億円以下と高額になったが [4]、小売業と金融業とで異なる結果につながった。

考えられる理由としては、個人情報保護委員会が金融業に対して示したガイドライン、金融情報システムセンターの活動、金融庁の監督指針が影響した可能性がある。そのプロセスについては今後の検証課題である。

謝辞 調査にあたり、金沢学院大学大学院の諸先生方にご相談させていただきました。

参考文献

- [1] 江口 彰 (2021) 「情報セキュリティインシデント抑制のための ISO/IEC27001 規格の活用に関する研究」、2021、筑波大学博士論文。
- [2] 朝野熙彦・鈴木督久・小島隆矢 (2005) 『入門 共分散構造分析の実際』、講談社、2005、28 頁。
- [3] 同上、121 頁。
- [4] 個人情報保護委員会 (2020) 「令和 2 年改正個人情報保護法について」、2020/6/12 <https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/> 2021 年 6 月閲覧。

なお、本研究は筆者自身の見解であり、筆者の所属先の意見を代表するものではありません。