1ZA-03

北陸地域の企業・団体等における情報セキュリティ管理

高正　智†　　岡田政則‡
金沢学院大学経営情報学研究科†　　金沢学院大学基礎教育機構‡

1. はじめに

昨今、サイバー・セキュリティをめぐる状況は2017 年 5 月のワナクライ被害にみられるように、大規模なサイバー攻撃が世界的に増加するなど悪化している。FBI の報告では 2017 年 1 年間の被害報告件数は全世界で 30 万件以上ある[1]。また日本国内の被害報告は約 2 万件弱報告されている[2]。2020 年の東京オリンピック開催に向け、サイバー・セキュリティの強化は喫緊の課題となっている。

2. 北陸地域での中小企業対象の調査の目的

サイバー・セキュリティに関する実態調査については、これまで情報処理推進機構（以下 IPA）が全国調査[3]、[5]を行っているが、被害など企業が秘匿する内容を含むことから大学による調査は困難であった。大阪商工会議所[4]（以下大商）による調査での回収率の低さにも表れている。中立な立場である大学が地元の商工会議所の後援を得る事で、主に中小企業対象に同様の調査をより確実に行うことが可能と考えた。企業数の99%を占める中小企業の対応が遅れているとされる中、製造業におけるサプライチェーンの重要性から中小企業の調査が必要と考えた。例えばボット対策においては企業の規模は問われない。本研究では北陸地域の商工会議所を経由し調査を行い、会員に結果を報告し、サイバー・セキュリティの現状を理解してもらう事を目的とする。

3. サイバー攻撃対策に関する調査

石川県、富山県、福井県の中規模市の商工会議所と連携し、主に中小企業や団体のうちインターネット等を活用している先を抽出して無記名手書きアンケートを郵送する調査を実施した。
大商や IPA の調査結果[4]、[5]を踏まえ、以下の仮説を置いた。サイバー空間であることから「被害率がほぼ同じ」、大都市圏と異なりノウハウの蓄積が薄いため「情報セキュリティ対策に対する担当者の配置や対策実施の比率は低い」、知的財産の規模が誘因となり「企業規模に比例して被害率が高い」、「対策や管理状況等の要因が被害状況と一定の関連がある」。上記仮説を検証するための質問項目を以下のとおりとした。

- IT 活用状況　（12 項目）
- サイバー攻撃への対策状況　（18 項目）
- 被害および被害未遂の経験　（17 項目）
- 情報セキュリティ管理状況　（14 項目）
- ベンダー利用状況　（6 項目）

先行調査と質問内容をそろえた上で、有効回答数のうちの該当比率の水準を比較する。
その上で企業・団体における以下の要素などとの因果関係を探るため、上記の要素を説明変数とし、被害を被説明変数として重回帰分析やロジスティック回帰分析等を行った。

4. サイバー攻撃対策に関する調査結果

平成 30 年 3～5 月に企業・団体 738 先へ無記名手書きアンケートを郵送し、241 先から有効回答（32%）を得た。この定量的調査を踏まえて定性的調査を追加実施した。

4.1 定量的結果の概要

(1)サイバー攻撃の対策の導入

導入項目	大企業 IPA	中小企業 IPA	関西大商	北陸 本研究
アンチウイルス	91%	80%	78%	92%
ファイアウォール	68%	34%	56%	46%
クラウド	ー	13%	ー	19%
ソフトウェア導入権限の制限	39%	8%	ー	15%
セキュリティパッチの更新	ー	47%	ー	32%

北陸地域はサイバー攻撃対策を全国並に導入しているが、小売業に改善の余地がある。

Information Security Management in corporates and groups of the Hokuriku area
Satoshi Takamasa† Masanori Okada‡
Graduate Schol of Business Administration and Information Science, Kanazawa Gakuin University†
Kanazawa Gakuin University‡

(2)ウイルス感染による被害

	大企業 IPA	中小企業 IPA	北陸本研究
被害	11%	5%	17%
未遂	24%	27%	14%
なし※	65%	68%	69%

※：回答がないケースを含む

被害と未遂の合計は 3 割強になり、全国水準とほぼ変わらない。実害に関してはサービス業、小売業で北陸はやや多い。

(3)標的型サイバー攻撃による被害

	大企業 IPA	中小企業 IPA	北陸本研究
被害	9%	1%	7%
未遂	9%	5%	8%
なし※	82%	94%	85%

※：回答がないケースを含む

被害と未遂の合計は 15%になり、全国水準の中小企業に比べやや多い。業種別には製造業で北陸のサイバー攻撃がやや多い。

(4)社内の情報セキュリティ研修・担当体制

	中小企業 IPA	北陸本研究
社内研修	17%	8%
担当者有	38%	51%

北陸の情報セキュリティ担当者の設置比率は全国対比で高いが、社内研修実施率については全国対比で低い。全国比での低い社内研修実施率は北陸の多くの業種での共通の課題である。

(5) 各対策と被害状況の回帰分析

各対策状況と被害状況との相関については決定係数が 0.26 と弱めであるが、クラウド導入や一般社員のソフトウェア導入権限の制限は被害状況に対し負の係数となったので、防止効果を示唆する。全般に負よりもむしろ正の相関が多くみられ、サイバー攻撃を受けたため、その対策をしている状況もあることがうかがえた。対策状況について現在と予定について調査したが、被害前と被害後としてする事が必要である。

4.2 地元企業に対するインタビュー

上記の定量的データを地元大企業に提示した後で、以下のコメントが得られた：

(1)設備関連 A 社（従業員数 300 以上）

ウイルス・メールの受信による障害経験あり。実際にはウイルス・メールによる未遂の比率はもっと高いのではないか。定期社内研修はしていない。

(2)機械関連 B 社（従業員数 900 以上）

パターン認識ではなく、振舞で検知するエンドポイントでの AI セキュリティを、経営の理解を得て数年前に導入した。サイバー・セキュリティ事件報道から情報漏洩に関する経営の意識が高まり、コストの課題を乗り越えられた。社内研修は E ラーニング形式で年 1 回実施しているが集合研修はしていない。

4.3 考察と提案

北陸のような非中核地域の中小企業・団体等の被害も全国水準と同程度か一部上回る。未遂を含めるとサイバー被害は 10%を、ウイルス被害は 30%を上回る。規模別には小規模よりも中規模企業の方が被害は多い。北陸地域では担当者設置の比率は高いものの、社内研修体制に課題が見られるので、組織の意識の底上げを提案する。今後の調査手法については、対策状況等の質問は被害後と前に分離する事を提言したい。

5. まとめ

地元の商工会議所や企業の理解を得て、大学主導でサイバー被害などの機微情報に迫ることは、地域密着型の大学にとって適した研究領域といえる。商工会議所や企業にアンケート結果を還元し、中小企業・団体等の参考に供した。

参考文献

[1]IC3、「2017 Internet Crime Report」、2018、P4、P18
[2]JPCERT、「インシデント報告対応レポート」、2017/4～2018/1
[3]独立法人情報処理推進機構、「2016年度 中小企業における情報セキュリティ対策に関する実態調査」、2017/8/8
[4]大阪商工会議所、「中小企業におけるサイバー攻撃対策に関するアンケート調査について」、2017/6/30
[5] 独立法人情報処理推進機構、「企業のCISOやCSIRTに関する実態調査2017」、2017/4/13