Vol.2021-DPS-186 No.2
Vol.2021-CSEC-92 No.2
2021/3/15

グループ会社の情報セキュリティ対策実施を左右する要因の分析

古殿瑶子[1]　稲葉緑[1]

概要：企業グループのセキュリティ強化は喫緊の課題である.このためには，個々のグループ会社のセキュリティ対策が欠かせないが，実施できていない会社が多くあるという問題がある.本研究では企業グループに属するグループ会社の情報セキュリティ対策の実施を左右する要因について明らかにすることを目的とした.ある企業グループを対象に，グループ会社にアンケート調査を実施し，情報セキュリティ対策の実施を左右する要因分析を行ったところ自立因子，社内因子，他社参考因子の３つの心理要因を特定した.

キーワード：グループ会社，企業グループ，セキュリティ

Analysis of factors that affect the implementation of information security measures in group companies

YOKO FURUTONO[†1]　MIDORI INABA[†1]

Abstract: Strengthening the security of corporate groups is an urgent issue. For this purpose, it is essential to take security measures for each group company, but there is a problem that many companies are not able to implement such measures. The purpose of this study is to clarify the factors that affect the implementation of the information security measures of the group companies belonging to a corporate group. We conducted a questionnaire survey on the group companies in a certain corporate group and analyzed the factors that influence the implementation of information security measures, and identified three psychological factors: self-reliance factor, internal factor, and reference factor of other companies.

Keywords: corporate groups, the group companies, security

1. はじめに

複数の企業から構成される企業グループのセキュリティ強化は喫緊の課題である.大企業や政府機関ではサイバー攻撃の増加に対し，高度なセキュリティ対策を実施しているため，その取引先やグループ会社で情報セキュリティ対策が十分でない組織を狙い，そこからターゲットである組織に攻撃を行う手法の攻撃も行われている.株式会社セキュアオンラインが運営するウェブサイト CyberSecurity.com はセキュリティニュースを掲載している[1].2019 年 1 月から 2020 年 10 月までの個人情報漏洩事件・被害事例一覧には 129 件の事例がある.その中から企業グループに属している企業が被害にあった事例を著者がカウントしたところ 31 件であり，多くの企業グループがサイバーインシデントの危険にさらされていることがわかる.グループ会社の情報セキュリティインシデントは企業イメージのダウンや株価低下，事業ができないことによる損失など，グループ経営に大きな損失をもたらす可能性がある.そのため企業グループを統括する親会社は情報セキュリティインシデントによる被害を最小限にする，情報セキュリティインシデント自体を減らすといった情報セキュリティマネジメントに取り組む必要がある.多くの企業が属する企業グループでは，特にセキュリティ対策が弱い企業を減らすためのセキュリティマネジメントが重要になるが，企業グループ全体の総合的な対策は近年難しくなっている.

本研究では多業種から形成される企業グループに所属するグループ会社の情報セキュリティ対策の実施を左右する要因の解明をめざす.そして，親会社などが情報セキュリティ対策を促すときに，解明した要因を考慮したうえで，どのような働きかけができるのか検討する.

2. 企業グループの情報セキュリティに関する現状

(1) 企業グループの大型化と課題

企業の多角化，グローバル化に伴い，事業部門別の戦略推進による企業買収や，分離子会社化などにより企業グループの大型化が進んでいる [2].1997 年 12 月に独占禁止法の改正により持ち株会社が解禁となり持ち株会社が増え（図１），コングロマリットとよばれる多種の企業を統合し，多角経営を行う巨大な複合企業体が増えている [3]. 事業部を分社化し，企業グループを形成することは経営面のメリットが多くある [4] [5]. 事業ごとに責任が明確になることで，他社への事業譲渡や事業の再編，M&A がしやすい体制になる.企業のグローバル化を見据え，海外展開時に権限委譲を進めながら分社化することで現地対応がスムーズになるというメリットもある.分社化したグループ会社

1 情報セキュリティ大学院大学
Institute of Information Security.

Vol.2021-DPS-186 No.2
Vol.2021-CSEC-92 No.2
2021/3/15

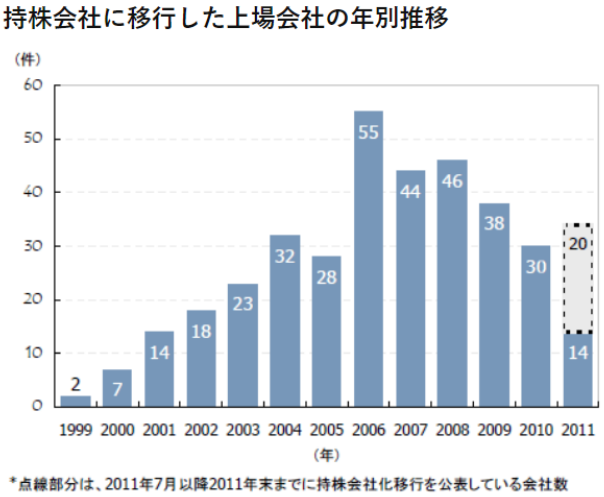

図 1　株会社化の年別推移[3]

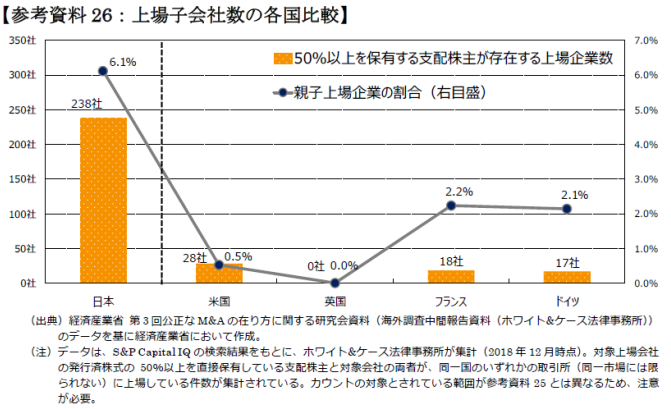

図 2　上場子会社数の各国比較 [6]

の自立性を確保することで，権限委譲による意思決定の迅速化やグループ会社が機動的な経営が実現する.その一方で各事業の独立性が高いため，本体からグループ会社内の意思決定が見えにくいなどのデメリットがあり，コーポレートガバナンスの低下が懸念されている.

このような近年の経営形態の急激な変化に伴い，企業グループに所属するグループ会社数の増加という量の観点と，組織文化や商習慣の違うグループ会社が一つの企業グループを形成することからくる質の観点からも，現状のグループ経営の限界が示唆されている [2].

コーポレートガバナンスについて経済産業省もグループ・ガバナンス・システムに関する実務指針（ガイドライン）の中で，グループとしての基本的な方向性と実際の取り組みが整合していないと指摘している [6].また自立分権を掲げながらも実際には結果管理すらせず放任に陥っている事例もみられるとの指摘があるとし，日本企業のグループ設計や実効的なガバナンスの在り方に課題があると述べている．青木ら [7]も事業ガバナンスを実態とモニタリングの観点から分析を行った結果，子会社の分権度が高いのに対し，モニタリング制度が十分に整備されていないことがわかったと記しており，子会社のモラル・ハザード等の潜在的な問題の深刻化が懸念されると指摘している.また，経済産業省の実務指針（ガイドライン）の中では，日本独特ともいえる課題として上場子会社と親会社の関係というものも指摘されている.図 2 に示すよう，日本は上場子会社数が他の国に比べ多い.上場子会社の独立性を配慮するとリスク管理を親会社で一元的に実施できないというアンケート結果もあげられており，情報セキュリティに限らずグループ会社のガバナンスに様々な問題がはらんでいることがわかる．このガイドラインの中でサイバーセキュリティ対策についても，内部統制システム上の重要なリスク項目と認識し，グループ全体やサプライチェーンも考慮に入れた対策の在り方が検討されるべきであると指摘されている.

(2) 情報セキュリティの一元管理の難しさ

情報セキュリティ対策の検討に際しても同じく経済産業省のサイバーセキュリティ経営ガイドラインが策定されており，セキュリティ対策の企業グループ全体での一元管理の難しさが課題となっている [8].グループ傘下のグループ会社で情報セキュリティインシデントが発生すると企業グループ全体の経営に影響を及ぼす可能性がある.事業内容や組織体制，グループ各社の規模，セキュリティ対策に掛けられる投資コストが違うなどの理由があるため，統一的・画一的な管理が難しいものになっている [9].

この難しさや限界を示したグループ会社を対象としたサイバー攻撃の例がある.2020 年 1 月に報告された三菱電機株式会社（以下，三菱電機㈱）の不正アクセスなどである [10].三菱電機㈱はこの事象以前より CSIRT を構築しており，米国国立標準技術研究所（NIST）の「サイバーセキュリティフレームワーク」に則した対策を講じていた [11].しかし，三菱電機㈱の報告書によると，2019 年 6 月 28 日に日本国内拠点の端末でウイルス対策ソフトの挙動検知をきっかけに調査を行ったところ，2018 年 3 月 18 日に中国拠点内のウイルス対策管理サーバーがゼロデイ攻撃を受け，それ以降外部からの不正アクセスにより感染が拡大，さらに日本国内のウイルス対策管理サーバーへ感染拡大した.

経済産業省の情報セキュリティガバナンス導入ガイダンスには，企業グループのセキュリティについて，業種や企業規模，予算など置かれている環境が様々なグループ各社において同じ対策を一律に適用することは現実的でないとする [12].また，各社の判断によってしまうため，グループ全体としての統制がとれていないケースが多いとみられるとする.このガイドの中には，各社に応じた情報セキュリティガバナンスの確立に関するアプローチ例がいくつか示されている.また情報セキュリティの取り組みを公開している企業グループは他にも見られる.例えば日本ユニシスでは IT サービス提供企業として全社的に情報セキュリティ文化を浸透させる取り組みを 1990 年から行っており，ISMS 認証やプライバシーマーク取得を企業グループ全体

で取り組んできている [13].また，住友化学グループではグローバル展開に向けて海外のグループ会社を含めた情報セキュリティの取り組みを公開しており，地域ごとの管理だけではなく言語や国などの違いから対応が遅延しないようローカルベンダも利用していくなどの取り組みが紹介されている [14].

このように，企業グループ全体の情報セキュリティ対策を強化するためには，グループとしての方針を打ち出しつつ，グループ会社の実情に合わせた対策の実施が重要であると考えられる．経済産業省のグループ・ガバナンス・システムに関する実務指針（ガイドライン）の中でも、事業構造の多様性・複雑性が高まると、グループ経営人と各事業部門との間の情報の非対称性の程度も大きくなるため，分権化を進め，各事業部門の自律性・独立性を高めるグループ設計を考えることが合理的となる場合が多いと記載されている.情報セキュリティの意識を根付かせるためには，グループ全体の統制をとる親会社が対策を実施するだけでなく，企業グループに属する各グループ会社が自律的に対策を進めることが求められていると思われる.しかし，情報セキュリティガバナンス導入ガイダンスの“多くの企業において「(企業の利益に直結しない）コスト」の位置づけであり対策を実施することの重要性が理解されていない”との記載から，適切に対策の実施について判断することができていないグループ会社があると推測した.

3. 先行研究調査

本章ではこの研究を進めるにあたって有用と思われた先行研究調査の結果を報告する.

グループ会社の中には中小規模，業種の異なる会社が含まれていることからこれらの企業特性と情報セキュリティ対策の実施殿関連を調べた研究を取り上げる.最後に情報セキュリティ対策の実施を左右するモチベーションに関する研究を紹介する.

(1) 中小企業の情報セキュリティ対策実現に向けた研究

Spruit & Roeling は中小企業規模の組織では情報セキュリティが専門の担当者ではなく，情報技術部門が取り仕切っていることが多く，情報セキュリティ対策の現状の評価やどのように改善していくか決めることが難しいと考え，中小企業には中小企業向けのガイドラインが必要だと考えISFAM（The Information Security Focus Area Maturity Model）を提唱した [15].Spruit & Roeling によると，CISSP や ISO 27000 シリーズ，ISO-light，ISF,IBM などは中小企業に適応しにくい分野がある.そこで先述の 5 個のガイドラインから，リスクマネジメントやポリシー・規則標準類，組織などほぼすべてに共通する①リスクマネジメント②制作，法制，規格③組織④人的セキュリティ⑤コンプライアンス⑥アイデンティティ/アクセスマネジメント⑦ソフトウェア開発⑧インシデントマネジメント⑨事業継続性⑩変革管理⑪物理的環境⑫資産運用管理⑬アーキテクチャの 13 の分野を抽出し，各分野で専門家のインタビューを実施，1 個の分野につき 5 段階の達成レベルを評価できるよう，yes/no の質問を考案した.それにより全 13 分野で合計 161 個の yes/no の質問に中小企業の担当者が答えることで，現在の自社の情報セキュリティ対策状態がわかり，次にどこを改善すれば達成レベルを上げることができるのか明確にできるモデルを作成した.このモデルを従業員 65 人の中小

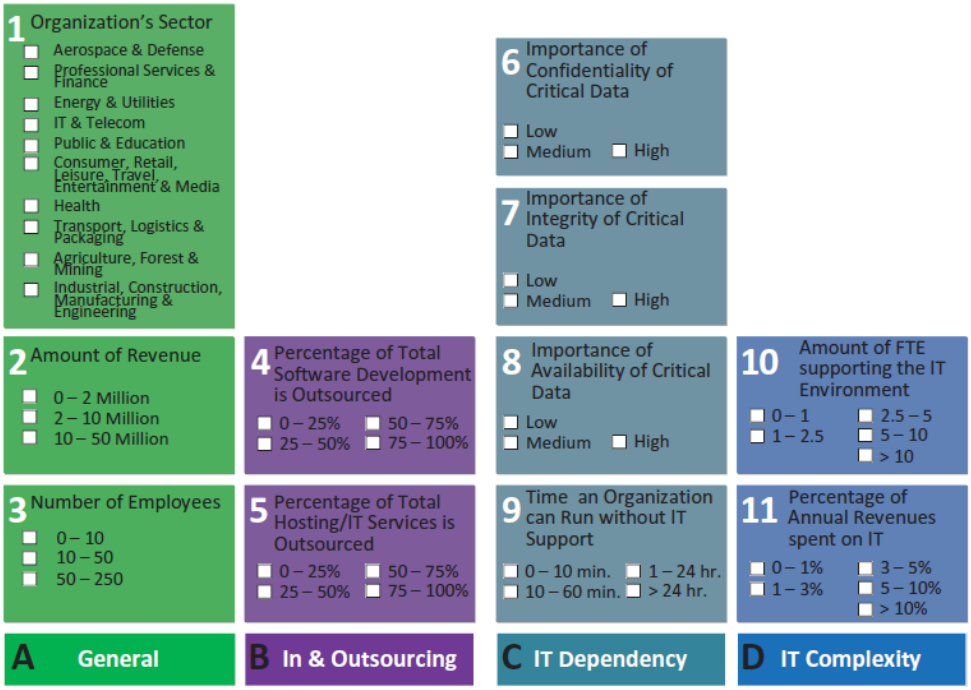

図 3 情報セキュリティの実装と関係のある企業特性 [16]

規模の通信会社の情報セキュリティ担当者に使ってもらった結果，３時間程度の作業で現状把握と今後の改善計画を提案でき，具体的なアドバイスを提供できることを明らかにした.

また, Mijnhardt らは，前述した ISFAM に基づき，中小企業の情報セキュリティ対策の実装と関連のある Mijnhardt ら組織特性の抽出を行った [16]. 中小企業の組織特性を過去の７１本の論文から７５個の企業特性をキーワードから選び出し，それをISFAMの評価のどれと関係あるかに当てはめ，重複するものは削除，マージすることで２６個の固有特性を抽出した.この２６の固有特性について５人の IS の専門家に議論してもらうことで，情報セキュリティ対策に関連のある 11 の組織特徴（①事業範囲②収益③従業員数外部のホスティング IT サービスを利用しているかの比率[%]④どのくらいソフトウェアの開発を外注しているかの比率[%]⑤外部のホスティング IT サービスを利用しているかの比率[%]⑥重大なデータの完全性のレベル[高 or 中 or 低]⑦気密性の完全性のレベル[高 or 中 or 低]⑧可用性の完全性のレベル [高 or 中 or 低]⑨IT サポートなしにはできない時間⑩IT 環境をサポートするための人数⑪年間経費に対数 IT コストの割合[%]）を抽出した(図 3).

(2) 情報セキュリティ対策におけるモチベーションについての研究

企業が情報セキュリティ対策を実施しない問題について，菅野ら [17]は，情報セキュリティ対策を実施する主体の意識や行動に関しての解明がすすんでいないと述べている.企業は社会の中でその存在価値を追求するため，企業の社会的存在価値を結びつけて情報セキュリティ対策の動機や目的を考える必要があると考え，菅野らは情報セキュリティ対策への企業のモチベーションを明らかにすることを目指した.まず文献調査とインタビューによりモチベーションに関わる諸要因を探索しアンケートを作成した.このアンケート用紙を用いて 516 名へアンケートを実施しその調査結果から，「経営者」と「情報セキュリティ責任者・担当者」の情報セキュリティ対策におけるモチベーションを構成する諸要因 10 個を解明し，共分散構造分析（ＳＥＭ）により各因子間の因果モデルの妥当性を検証した.これによると「経営者」と「情報セキュリティ責任者・担当者」の情報セキュリティ対策の動機に影響する因子が，組織内要求として①リスク管理②改善③内部統制，社会的要求として④競争優位⑤取引先の要求⑥事業継続がある.一方，対策の実施を阻む阻害因子としては⑦技術ノウハウ⑧手間・効率⑨組織運営⑩理解・協力因子の４因子あることがわかった.４因子の中でも，理解・協力因子が最も阻害要因との因果関係が強くでている.この結果，菅野らはこれまでは組織の情報セキュリティ対策を推進するためには，情報セキュリティ上のリスクとそのマネジメントを説くという，リスク管理因子を中心としたアプローチであったが，情報セキュリティ対策の動機に影響する因子として企業価値の向上に関わる社会的要求である，競争優位や取引先の要求因子，事業継続因子が含まれていることから，セキュリティ対策のモチベーションを高めるためには社会的要求を考慮したアプローチが必要なことが示唆されたと述べている.また阻害要因を低減させるために，情報セキュリティに対する意識向上と対策手段を普及するための教育に課題がありこの課題解決が阻害要因を低減させることにつながると述べている.

4. 研究目的

大企業グループ内での情報セキュリティ対策の進捗にはグループ会社間で差があること，対策の実施状況に問題がある企業の抽出方法などについて検討されていることがわかった.しかし，情報セキュリティ対策の実施に遅れがみられる企業に対し，対策を実施するよう親会社などが働きかけたとしても，これらの企業がすぐに同意し，対策を進めるとは考えにくい.前章の先行研究から，大企業グループ内の会社についても情報セキュリティ対策の実施には心理的な阻害要因や企業特性が影響を与えると考えられるからである.また，グループ会社ならではの企業グループに属するからこそ生じる阻害要因があることも考えられる.例えば，独立した企業とは異なり，大企業グループに所属する会社の中には，情報セキュリティ対策について，自社がサイバー攻撃にあったとしても何か対策がされているだろうと考え，自社では対策を実施する必要がないと認識している可能性もある.このような様々な特性や要因を考慮することが，情報セキュリティ対策の実施への働きかけの効果を左右すると考えられる．以上から，本研究では，グループ会社の情報セキュリティ対策の実施を左右する要因を明らかにすることを目的とする.

5. グループ会社の情報セキュリティ対策の阻害要因についての調査

(1) アンケート作成

先行研究 3.2 の菅野の先行研究を参照とし，菅野らが示した⑦技術ノウハウ⑧手間・効率⑨組織運営⑩理解・協力因子の４因子以外にグループ会社ならではの阻害因子があると予測した。そこで情報セキュリティに関係した立場の８名に，グループ会社が情報セキュリティ対策を実施するときの阻害要因についてインタビューし，グループ会社ならではの阻害因子を予測し，質問項目を考案した（表 1）.

企業グループに属するが故の阻害要因因子として⑪横並び⑫依存⑬権限委譲が抽出された.

本研究ではガバナンス体制について研究の対象外とするため，⑬は除外し，⑪，⑫の因子について質問を各２問作成した.さらに先行研究 2.3 の菅野のアンケート調査で明らかになっている，グループ会社への所属の有無にかかわ

依存	業種規模関係なく、統一された対策を指示されるため必要性が理解できない
	セキュリティ対策予算を親会社が負担してくれないため
	何かあった時は本社やシステム会社が対応すると考えている
	親会社が責任もってやってくれる
	親会社が方針を出してくれる
	本社との責任の所在がわからない
	問題があれば本社やシステム会社が指摘してくれる
横並び	一社だけ優れた製品等を導入すると、周りのグループ会社があわせないといけなくなってしまう
	自社だけ実施するならほかのグループ会社と足並みそろえた方が良い
	自社だけ余計なことをやって、何かあった場合のリスクを負いたくない
権限委譲	勝手にやっていいのかわからない
	自社判断でセキュリティ対策をやっていいのか不明

表 1　グループ会社の情報セキュリティ対策実施の阻害要因を調べる項目案

らない情報セキュリティ対策の阻害要因⑦技術ノウハウ⑧手間・効率⑨組織運営⑩理解・協力因子の４因子について，アンケート項目のうち，因子分析の結果 0.6 以上の負荷量のものを参考に，各因子につき２問の設問になるように質問を選定した.これは，アンケートにおける回答者の負担を減らすためであった.

以上をまとめ，グループ会社に所属するからこそ生じる阻害要因についてのアンケート４問，それ以外の阻害要因についてのアンケー８問の合計１２の質問項目のアンケート用紙を作成した.

(2) アンケートの実施

グループ会社 69 社のシステム担当者向けのセキュリティ関連の教育の後にアンケートの質問項目について Web で非常にあてはまる（６点）～全くあてはまらない（１点）のそれぞれ６段階で評価してもらった.解答期間は 2020 年 10 月 6 日～2020 年 11 月 6 日であった．グループ会社のセキュリティ教育に参加したグループ会社のシステム担当者６７名(63 社)から回答を得られた.

6. 因子分析

(1) 分析方法

分析には統計解析ソフトウェアである SPSS を利用した.因子の抽出には，最尤法を用いた.

(2) 分析結果

12 の質問項目を用いて因子分析をおこなった.ただし共通性が 0.16 に満たなかったもの，因子負荷が複数の因子に効いているものを削除し，再度，因子分析を行った.因子数はスクリープロットにより判断し３因子とし，プロマックス回転を行った結果，３因子が得られた.その因子負荷を表２に示した.

因子の解釈について第Ⅰ因子は「システム運用を委託先に任せず自社で行う」，「情報セキュリティ対策を実施するノウハウが自社にある」といった質問に対し負荷量が高く，「自立」に関する因子であるため“自立因子”と命名した.第Ⅱ因子は「経営層が情報セキュリティ対策の必要性を理解している」，「経営層から情報セキュリティに関する指示を受ける」，「情報セキュリティについて社員の理解が得られている」といった質問に対し負荷量が高く，「社内の理解」に関する因子であることから“社内因子”と命名した.第Ⅲ因子は「他社が導入しているセキュリティ製品を自社も導入しなければならないと感じる」という質問に負荷量が高く，“他社参考因子”とした.

(3) 考察

心理因子として抽出された因子より，情報セキュリティ対策を実施するときにセキュリティ担当者が感じる心理因子として３つあることがわかった.

自立因子から情報セキュリティ担当者がセキュリティ対策を実施するときに，自社で実施する必要があるのか、委託先に任せればいいのではないかと考える傾向があることがわかった.そもそも情報セキュリティ対策は専門家や委託先に任せておけばいいため，自社でやる必要がないだろうと情報セキュリティ担当者が考えることを示している。実際はシステムなど技術的なところを委託先に任せたとしても，自社でも情報セキュリティ対策に取り組む必要がある.例えば，標的型攻撃メールに対する対応など，社内の一人一人が対応を身に着け防御する必要があり，委託先任せにできないところがある.また，昨今増えているクラウド上のサービスなど，ユーザーが設定して使うシステムもあり，自社で情報セキュリティ対策を取り組む必要がある．社内因子より，情報セキュリティ担当者は情報セキュリティ対策を実施するには経営者や社内の理解が得られているかどうかが影響すると考えていることがわかった.技術的な対策を行うことで情報セキュリティインシデントの予防が見込まれるが，費用や人材などの面で実施を困難に考えるセキュリティ担当者がいることが示されていると考える.また，情報セキュリティ担当者が従業員に情報セキュリティの重要性を理解させ，ルールを守らせることを困難に感じていると考えられる.組織として情報セキュリティ意識を向上させ,1 人 1 人が不審メールに適切に対応できるようにすることは今後ますます重要になってくるため，企業グル

	Ⅰ	Ⅱ	Ⅲ
システムの運用については、委託先に任せきりとなりがちである	**-.99**	.17	.22
社内のセキュリティ担当部署には、情報セキュリティ対策を実施するノウハウが十分にある	**.61**	.15	.26
システムを新規に構築・利用する際は、ベンダーが主導権を握りがちである	**-.58**	-.09	.21
インシデントが発生した際に社内で適切に対応することができる	**.55**	.11	.28
経営層は、情報セキュリティ対策の必要性について十分に理解している	-.09	**.98**	-.15
経営層から情報セキュリティに関する指示を受けることがある	.03	**.67**	.00
情報セキュリティ上のルールを遵守することについて、社員の理解が得られている	.25	**.52**	.04
他社が優れたセキュリティ製品を導入していた場合、自社も導入しなければならないと感じる	-.05	-.11	**.62**
因子相関	Ⅰ	Ⅱ	Ⅲ
Ⅰ	-	.21	.03
Ⅱ		-	.24
Ⅲ			-

表２　阻害要因に関する項目（プロマックス回転後の因子パターン行列（N=63）と因子

ープ全体として情報セキュリティ対策の推進に取り組む必要がある.

他社参考因子より, 情報セキュリティ担当者は情報セキュリティ対策を実施するときに同業他社の情報セキュリティ対策について情報セキュリティ担当者が考えることがわかった.業種によって扱う情報が違うことをシステム担当者が理解しており, 同業他社の情報セキュリティ対策を参考に自社の対策を考えていることがわかった.業界団体が情報セキュリティ対策を推進し, どのようなセキュリティ対策が有効か指針を示すことはその業界に所属する会社のセキュリティ対策に影響をあたえるため効果が望めることがわかった.

7. まとめ

グループ会社のシステム担当者向けのアンケートより、セキュリティ対策を実施するときにグループ会社のシステム担当者が感じる心理因子として自立因子,社内因子,他社参考因子の３つがあることがわかった。

参考文献

[1] 株式会社セキュアオンライン, 個人情報漏洩事件・被害事例一覧“CybereSecurity.com”https://cybersecurity-jp.com/leakage-of-personal-information （2021 年 1 月 20 日確認）
[2] 山田　英司, 上杉　利次, 「共創」のグループ経営　本社と事業部門の二層化マネジメント, 中央経済社, 2016.
[3]大和総研グループ, “持株会社考察 ～上場持株会社は増加中～”
[4]奥　康平, “純粋持株会社と事業持株会社の戦略的活用-グループ経営における戦略的意図の変化と持株会社活用類型化の予備的考察-”, 阪南論集, 2019.
[5] 内閣府　経済社会総合研究所, 社団法人　経済企画協会, “第 2 章 わが国企業のM＆Aの動向とその課題” http://www.esri.go.jp/jp/prj/mer/houkoku/0405-02.pdf (2021 年 1 月 20 日確認)
[6] 経済産業省, “グループ・ガバナンス・システムに関する実務指針 （グループガイドライン）”, https://www.meti.go.jp/press/2019/06/20190628003/20190628003_01.pdf, 2019. (2021 年 1 月 20 日確認)
[7]青木 英孝, 宮島　英昭, “日本企業における事業組織のガバナンス―企業の境界と二層のエージェンシー問題の視角から―”, https://core.ac.uk/download/pdf/6722584.pdf, 独立行政法人　経済産業研究所 2010. (2021 年 1 月 20 日確認)
[8]経済産業省　独立行政法人 情報処理推進機構, “サイバーセキュリティ経営ガイドライン Ver2.0” https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide2.0.pdf, 2017. (2021 年 1 月 20 日確認)
[9]株式会社三菱総合研究所, “情報セキュリティガバナンス導入ガイダンス補足編～企業グループにおける情報セキュリティガバナンスモデル～” https://www.meti.go.jp/policy/netsecurity/docs/secgov/2010_IoformationSecurityGovernanceModel.pdf, 2011. (2021 年 1 月 20 日確認)
[10]三菱電機株式会社年 12 月 2 日 “不正アクセスによる個人情報と企業機密の流出可能性について（第３報）” https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf, 2020. (2021 年 1 月 20 日確認)
[11]三菱電機株式会社, “三菱電機グループ情報セキュリティ報告書 2019” https://www.mitsubishielectric.co.jp/corporate/csr/governance/information_security/pdf/information_security_2019.pdf, 2019. (2021 年 1 月 20 日確認)
[12]経済産業省, “情報セキュリティガバナンス導入ガイダンス” https://www.meti.go.jp/policy/netsecurity/downloadfiles/securty_gov_guidelines.pdf, 2009. (2021 年 1 月 20 日確認)
[13]住友化学システムサービス株式会社, “住友化学グループにおける情報セキュリティの確保に向けて” https://www.sumitomo-chem.co.jp/rd/report/files/docs/2014J_4.pdf, 2014. (2021 年 1 月 20 日確認)
[14]三口　充高, 大橋　幸江, “日本ユニシスグループにおける情報セキュリティ総合戦略” https://www.unisys.co.jp/tec_info/tr86/8602.pdf, UNISYS TECHNOLOGY REVIEW 第 86 号 2005. (2021 年 1 月 20 日確認)
[15]Macro Spruit & Roeling Martijn, ISFAM:The Information Security Focus Area Maturity Model” 2014.
[16]Frederik Mijnhardt, Thijs Baars & Marco Spruit, “Organizational Characteristics Influencing SME Information Security Maturity”, Journal of Computer Information System 56:2,106-115, 2016.
[17]5 菅野　泰子, 寺田　真敏, 山田　安秀, 鎌倉　稔成, 土井　範久, “企業の情報セキュリティ対策におけるモチベーションの構造に関する考察”, 情報処理学会論文誌 Vol.50 No.9 2193-2206(Sep.2009), 2009.