ISSN 1346-9029

研究レポート

No.373 May 2011

日本企業における情報セキュリティ逸脱行為と組織文化・風土との関係

主任研究員 浜屋 敏
情報セキュリティ大学院大学 山本 哲寛

富士通総研(FRI) 経済研究所

要　旨

わが国では、情報セキュリティポリシーの策定やセキュリティ教育の実施など組織的に情報セキュリティ対策を行っている企業が多いが、それにもかかわらず情報セキュリティの事故は後を絶たない。これは、情報セキュリティ対策の実効性を高めるためには、ルールの策定や教育の実施など形式的な対応を行うだけでは不十分なことを示唆している。形式的な対策だけでなく、ルールが守りやすいような運営を行うと同時に、形式化できない組織風土や組織文化を考慮し、それに合った対策を実施する必要があるのではないだろうか。一般的には、情報セキュリティ対策は組織文化・組織風土による違いを考慮することなく、どのような組織でも同じような形式的なルールを遵守するべきものと考えられているが、そのような認識は間違っているかもしれない。

そこで、本調査研究では、集団主義などの組織文化・組織風土に注目し、情報セキュリティのルールからの逸脱行為について、以下の３つの仮説を設定した。

① 情報セキュリティのルールを破る行為（逸脱行為）の程度は、情報セキュリティに関する形式的な対策が実施されているかということに影響を受ける。

② 情報セキュリティに関する逸脱行為の程度は、形式的な情報セキュリティ対策だけでなく、上司の態度や職場の雰囲気といった形式化できない組織的な要因に影響を受ける。

③ さらに、そういった形式化できない組織的な要因は、「集団主義」に代表される組織文化・組織風土に影響を受ける。

アンケート調査で収集したデータを分析して、セキュリティ・ルールからの逸脱行為や形式的対策の実施状況などについて国内の企業の実態を分析した。そして、上記３つの仮説を検証するために共分散構造分析を行った結果、これらの仮説はすべて成り立っていることが検証された。つまり、わが国の企業において情報セキュリティ対策の実効性を高めるためには、形式的なルールを定めるだけでなく、組織文化・組織風土に合った対策を行うことが必要である。

キーワード：情報セキュリティ、逸脱行為、組織文化、組織風土

目　次

1. はじめに

1.1. 問題意識

現在の日本社会は、プライバシーや個人情報の保護に関する認識の高まりとともに、情報セキュリティに対して非常に敏感になっており、企業などでも多額のコストと時間をかけて情報セキュリティ対策が行われてきた。それにもかかわらず、さまざまなセキュリティ事故が発生している。

事故を起こした企業が情報セキュリティに対して何の対策も講じていないとは考えられず、たとえばファイアウォールに始まるネットワークセキュリティ機器等のコンピュータシステムにおける対策を実施し、ISMS 認証やプライバシーマークの取得といった情報セキュリティマネジメントシステムも構築していることが多いはずである。しかしながら実際には事件や事故は絶えず発生しており、それはコンピュータシステムやセキュリティマネジメントシステムといった形式的な対策がいかに実施されようとも、ルールやシステムの軽視・逸脱が黙認されるような風土（文化）があることが一因ではないかと考えられる。

情報セキュリティ関連の事故や事件の実態については、財団法人日本情報処理開発協会（以下JIPDEC）が、「(平成 21 年度）個人情報の取扱いにおける事故報告にみる傾向と注意点」として、平成 21 年度のプライバシーマーク認定事業者等からの個人情報の取扱いにおける事故等についての概要を報告している。これによると、平成 21 年度は認定取得事業者 11,379 社のうち、624 事業者が何らかの事故報告を行っている。(図表 1、図表 2参照)

図表 1. 認定事業者の事故報告件数（平成 20～21 年度）

	年度	20 年度	21 年度
JIPDEC	付与事業者数	339	340
	事故件数	742	852
指定機関	付与事業者数	226	284
	事故件数	320	417
合 計	付与事業者数	565	624
	事故件数	1,062	1,269

（出所：財団法人日本情報処理協会（2010）

図表 2. 年度別認定事業者数（平成 10～21 年度）

年 度	10 年度	11 年度	12 年度	13 年度	14 年度	15 年度
事業者数	58	129	219	321	485	762
年 度	16 年度	17 年度	18 年度	19 年度	20 年度	21 年度
事業者数	1,294	3,508	7,348	9,332	10,276	11,379

（出所：財団法人日本情報処理協会（2010）

事故原因については、報告があった 1,269 件のうち、漏えいが 823 件で紛失が 336 件であり、これらは注意すれば防ぐことのできたものである。紛失・漏えいを原因別に分類すると、宛名間違いや封入ミス、FAX送信ミス、メールの誤送信による「誤送付」647 件と最も多く、全体の 51.0%を占めている。次いで、「紛失」が全体の 26.5%、誤交付、データ管理ミス等による「その他漏えい」が 167 件（同 13.1%）である。また、ファイル交換ソフト（Winny、Share等）のウィルス感染による漏えい（流出）は 9 件（同 0.7%）であり、空巣・置き引き、車上荒らし等による「盗難」は 57 件（同 4.5%）である。（図表 3参照）

図表 3. 付与事業者から報告のあった原因別事故報告件数（平成 21 年度）

報告先	漏えい						盗難・紛失			その他	合計
	誤送付				ウィルス感染	その他漏えい	盗難		紛失		
	宛名間違い等	封入ミス	FAX	メール			車上荒し	置き引き等			
JIPDEC	215	22	74	142	3	128	14	17	204	33	852
指定機関	83	11	31	69	6	39	15	11	132	20	417
計（割合）	298	33	105	211	9	167	29	28	336	53	1,269
	23.5%	2.6%	8.3%	16.6%	0.7%	13.1%	2.3%	2.2%	26.5%	4.2%	100.0%

（出所：財団法人日本情報処理協会（2010）

この報告はプライバシーマーク取得事業者の統計であるため、一定のレベルで形式的な情報セキュリティ対策を組織的に行っている事業者を対象としたものであるが、この「一定レベル」に到達した事業者でも 5%以上の事業者が事故を起こしていることがわかる。また注目すべき点はそのうち、誤送付や紛失といった人間系のミスの多さである。これらは、情報セキュリティのルールやマネジメントシステムを守っていれば防ぐことのできたものが多い。つまり、これらの事故は、ルールは定められているものの、日ごろから小さなことであればルールを守らない個人の行動によって引き起こされていると想定することができる。このことから、情報の漏えいの件数に対しては、コンピュータシステムそのものによる脆弱性よりも「人」が介在する業務の方が影響が大きいことが分かる。そして、そこには組織文化・風土が大きく関係していると考えられる。一般的には、情報セキュリティ対策は組織文化・組織風土による違いを考慮することなく、どのような組織でも同じような形式的なルールを遵守するべきものと考えられているが、そのような認識は間違っているかもしれないのである。

1.2. 研究仮説

以上のような問題意識に基づいて、本調査研究では以下のような仮説を設定し、アンケート調査で回収したデータを用いて、調査項目の現状を集計するとともに、これらの仮説

の検証を行った。

① 情報セキュリティのルールを破る行為（逸脱行為）の程度は、情報セキュリティに関する形式的な対策が実施されているかということに影響を受ける。

② 情報セキュリティに関する逸脱行為の程度は、形式的な情報セキュリティ対策だけでなく、上司の態度や職場の雰囲気といった形式化できない組織的な要因に影響を受ける。

③ さらに、そういった形式化できない組織的な要因は、「集団主義」に代表される組織文化・組織風土に影響を受ける。

2. 調査の概要とデータ

2.1. 調査の概要

本調査研究では、インターネットのホームページを利用してアンケート調査を行った。調査実施時期は 2010 年 12 月である。調査対象として、調査会社㈱ネットマイルのモニターの中から、以下の条件に合う対象者を 3,000 人抽出した。外資系企業（外資の比率 33%以上）の勤務者を 1,000 サンプル集めたのは、組織文化・風土は企業の資本構成にも影響を受けると考えたからである。

- 年齢 18 才～70 才
- 民間企業の正社員
- 従業員数 100 名以上の会社で仕事をしている人
- 店頭での販売、工場のライン、物流の現場で働いている人を除く
- 業務で、個人情報や機密情報にアクセスできる人
- 国内企業 2,000 人、外資系企業 1,000 人、合計 3,000 人

主な調査項目は、下記のとおりである。

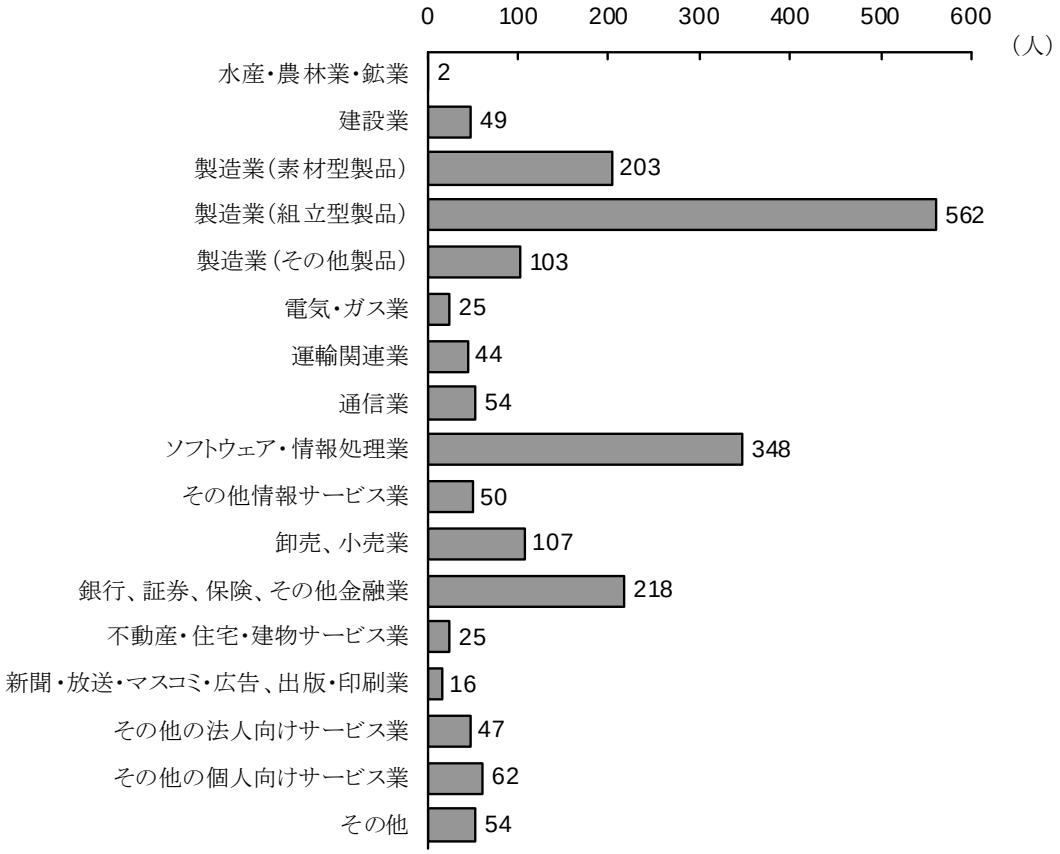
- 回答者が所属する企業の属性（業種、従業員数）、回答者の属性（役職、職種）
- 情報セキュリティに関する形式的な対策の実施状況
- 情報セキュリティに関するルールからの逸脱行為の有無とその程度
- 職場におけるコミュニケーションの程度
- 回答者自身の仕事に対する意識、取り組み
- 職場における倫理観、社会規範との整合性など
- 職場における組織文化・組織風土（集団主義の程度）

3,000 サンプルのうち、「わからない」という回答を除外し、回答時間が極端に短い回答者は除外するなどデータのスクリーニングを行い、最終的に分析に使用した有効回答数は 1,866 であった。

2.2. 回答者の所属企業の特徴

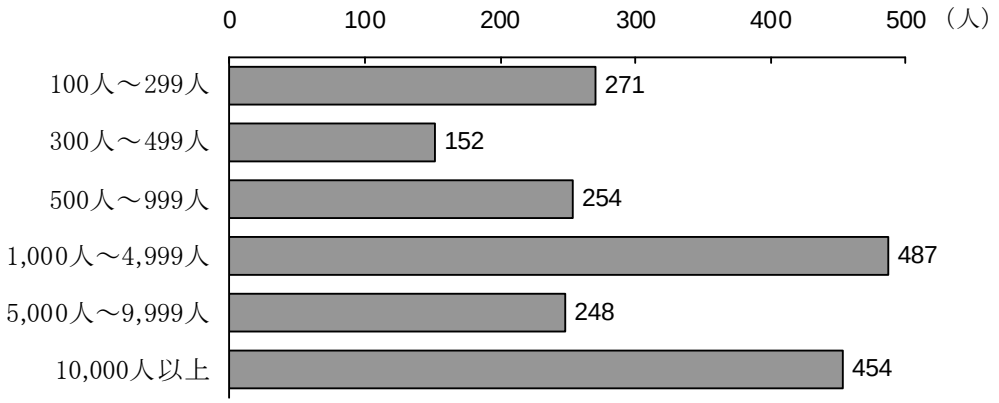
図表 4は、有効回答者が所属する企業の業種別の構成を示したものである。

図表 4. 所属企業の業種



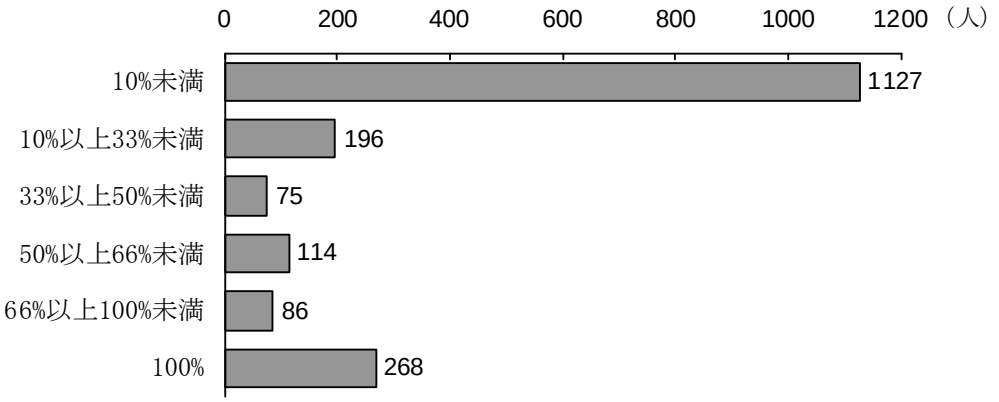
図表 5は、回答者の所属企業の従業員数を示している。

図表 5. 所属企業の従業員数



図表 6は、回答者の所属企業の外資比率を示している。上述したとおり、企業の資本構成は組織風土・文化にも影響を与えると考えられるため、以下では、主な質問項目について、従業員数別とともに外資比率別に回答をクロス集計して示すことにする。

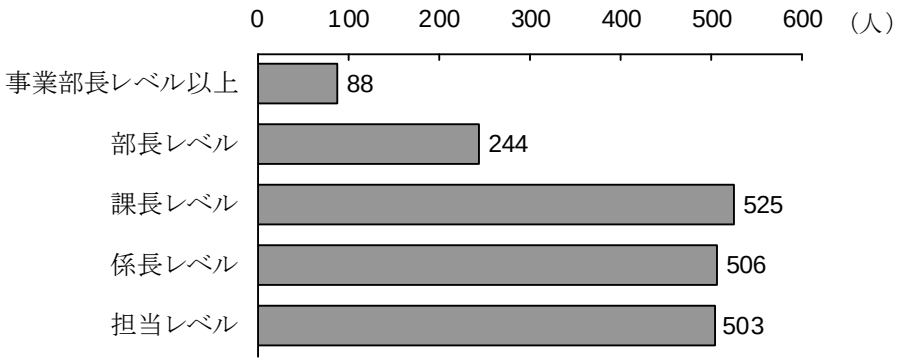
図表 6. 所属企業の外資比率



2.3. 回答者の特性

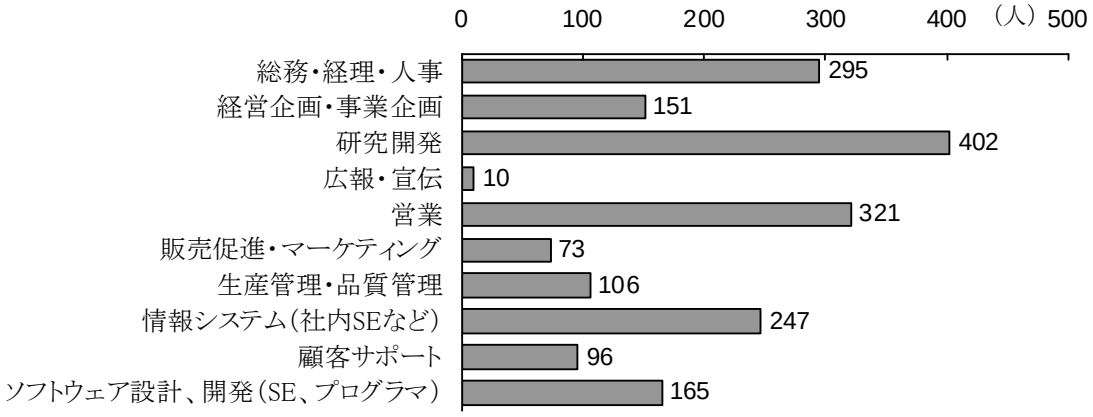
図表 7は、回答者の役職を示している。課長以下で全体の 82%を占める。

図表 7. 回答者の役職



図表 8は回答者の所属部署を表している。もっとも多いのは研究開発部門で、次いで、営業、総務・経理・人事、情報システム（社内SEなど）の順になっている。

図表 8. 回答者の所属部署

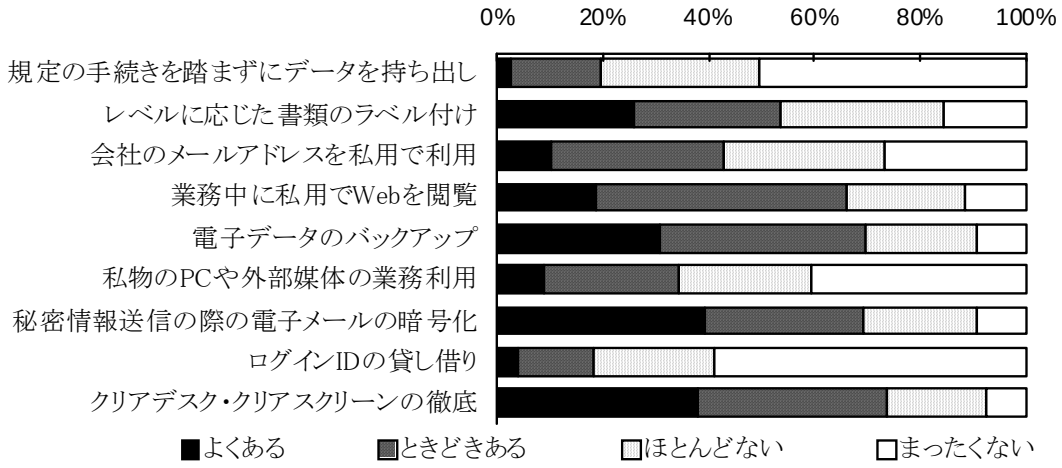


3. 情報セキュリティに関する逸脱の状況

3.1. 全体的な傾向

図表 9は、情報セキュリティに関するルールを回答者自身が破った経験について調べた結果を示している。ここでは、「規定の手続きを踏まずにデータを持ち出す」というかなり重大な逸脱から、「クリアデスク・クリアスクリーンの徹底」という軽微なものまで各種の逸脱行為を列挙した。当然ながら、重大な逸脱行為の頻度は少ないが、軽微なものは過半数が「ときどきある」と回答している。

図表 9. 情報セキュリティに関する逸脱の状況



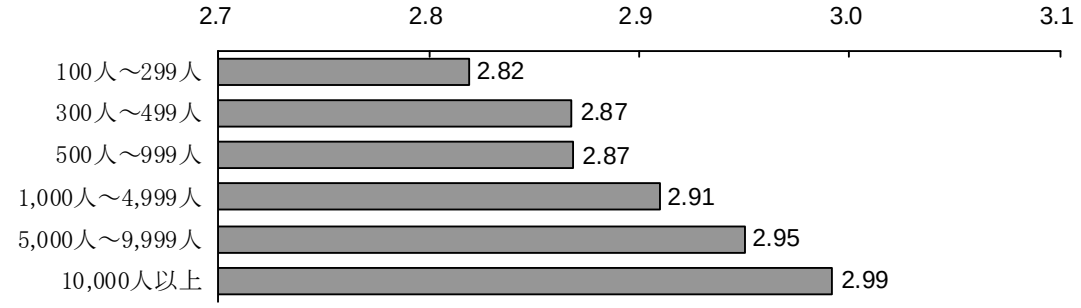
3.2. 企業特性別の傾向

図表 10は、逸脱の程度を数値化し、そのスコアを回答者の所属企業別に集計した結果を示している。逸脱の程度を表すスコアは、図表 9の各項目について、「よくある＝１」「ときどきある＝２」「ほとんどない＝３」「まったくない＝４」として、平均値を計算した（た

だし、「電子データのバックアップ」「秘密情報送信の際の電子メールの暗号化」「クリアデスク・クリアスクリーンの徹底」についてはスコアを逆転した)。したがって、スコアの値が大きいほど、逸脱行為は少ないことになる。

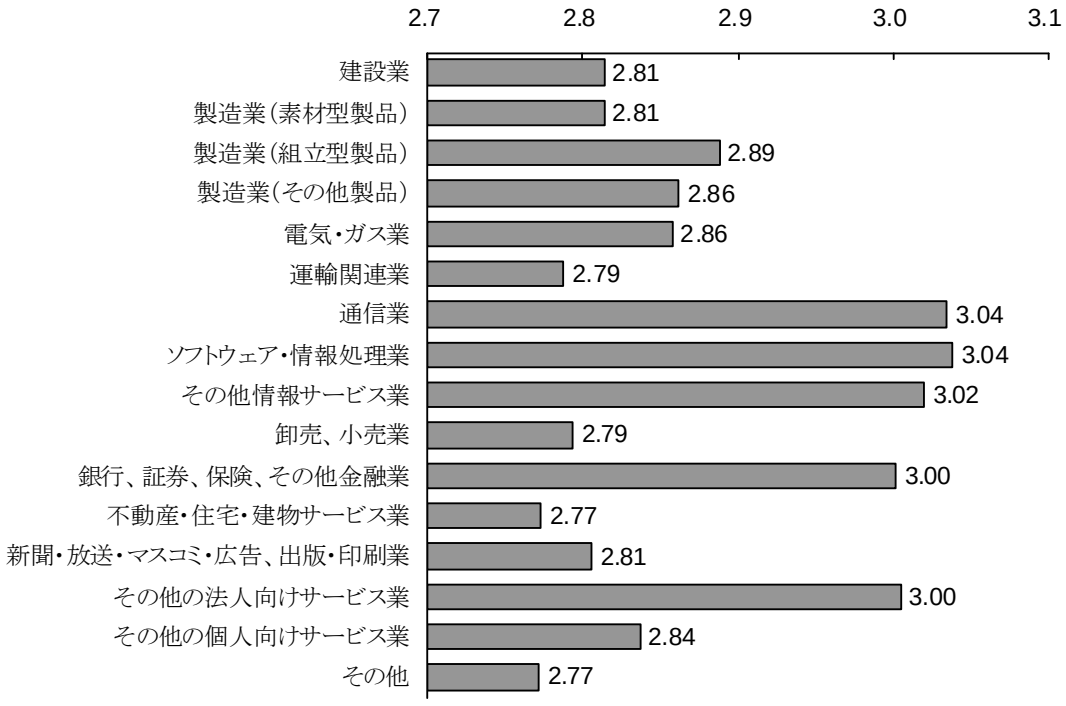
このグラフからは、明らかに、従業員数の多い大企業ほど回答者の逸脱行為が少ないという傾向を見て取ることができる。

図表 10. 逸脱に関するスコアの平均値（従業員数別）



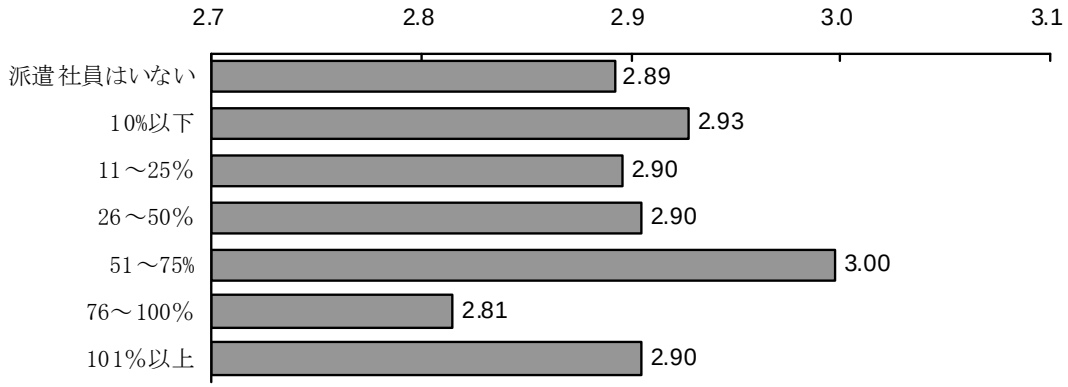
図表 11は、この逸脱スコアを業種別に集計したものである。逸脱が少ない（スコアが高い）のは、通信業、ソフトウェア・情報処理業、その他情報サービス業、銀行など金融業、その他の法人向けサービス業である。一方、運輸関連業や不動産関連業では相対的に逸脱傾向が高い。

図表 11. 逸脱に関するスコアの平均値（業種別）



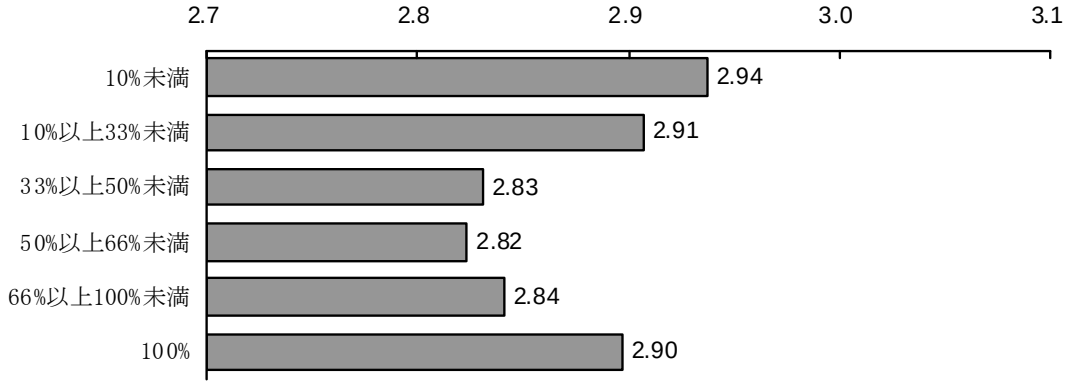
図表 12は、回答者の職場における派遣社員の比率別に回答者自身の逸脱傾向を集計したものである。このグラフからは、職場における派遣社員の比率と逸脱行為の頻度については、それほど明確な傾向はないように見える。

図表 12. 逸脱に関するスコアの平均値（派遣社員比率別）



図表 13は、回答者の逸脱スコアを所属企業の外資比率別に示したものである。外資の比率の高さと逸脱傾向には明確な比例的な傾向はなく、外資が少ない企業（33%未満）は逸脱傾向が低いが、外資100%の企業でも逸脱傾向は低くなっている。

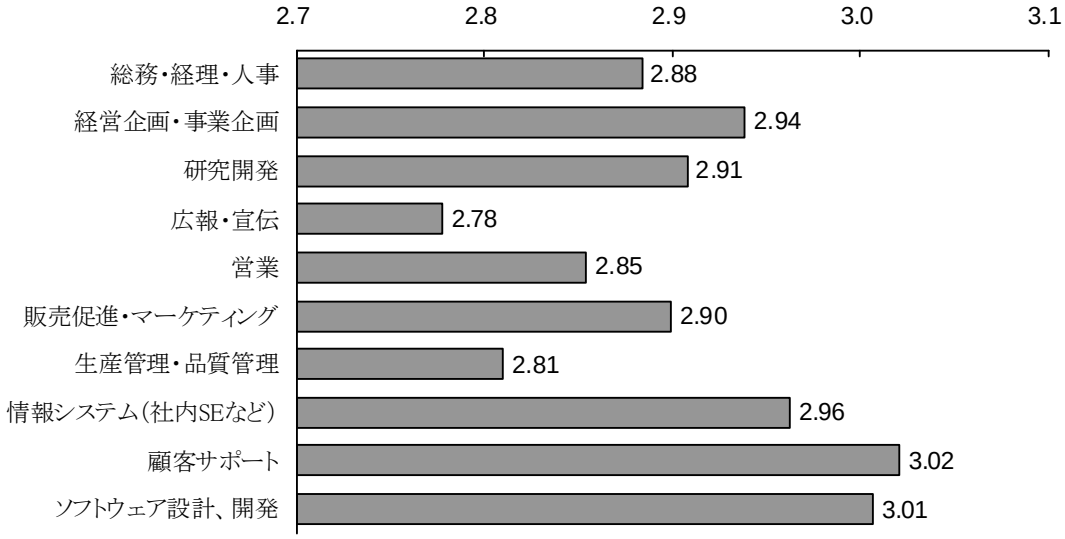
図表 13. 逸脱に関するスコアの平均値（外資比率別）



3.3. 回答者特性別の傾向

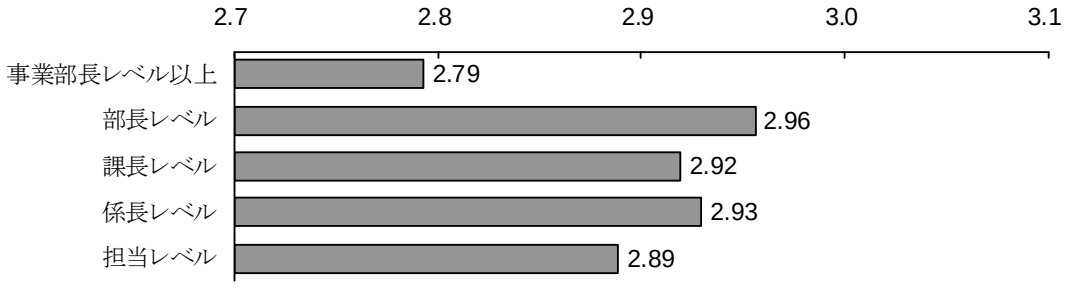
つぎに、回答者自身の属性と逸脱傾向の関係を見てみよう。まず、図表 14は回答者の所属部署別に逸脱スコアを示したもので、広報・宣伝や生産管理・品質管理では相対的に逸脱傾向が高い。逸脱が少ないのは、顧客サポート、ソフトウェア設計・開発といった部署に所属する回答者である。これらの部署では、相対的にルールが厳密に守られている場合が多いようである。

図表 14. 逸脱に関するスコアの平均値（職種別）



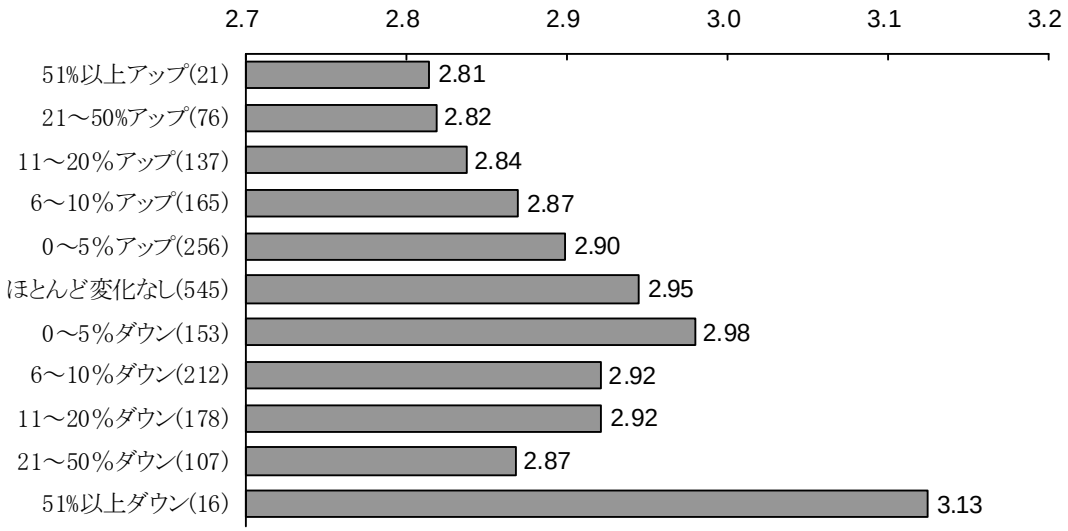
図表 15は回答者の役職別に逸脱傾向を見たものである。このグラフからは、もっとも上位の事業部長レベル以上の回答者だけ特に逸脱傾向が高くなっており、平均的に見ると部長レベルでもっとも逸脱傾向が低い。

図表 15. 逸脱に関するスコアの平均値（役職別）



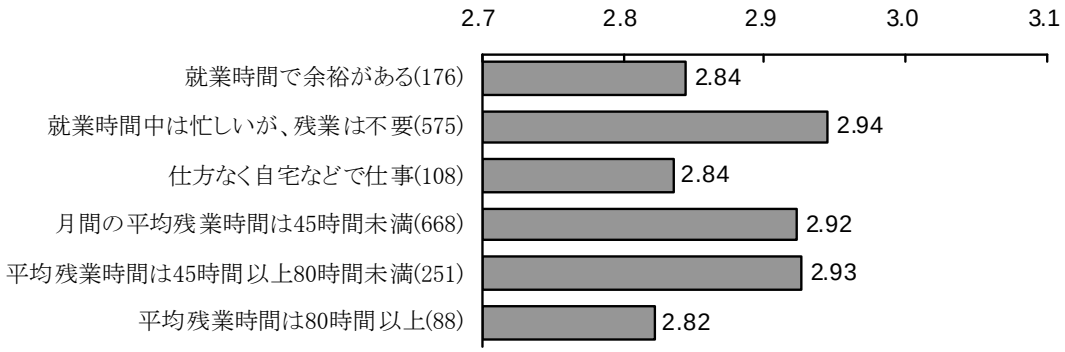
図表 16は、回答者の 3 年前からの年収の変化率別の逸脱傾向を示している。年収が 51%以上ダウンした回答者で最も逸脱傾向が低いが、このグループは対象者が 16 名と少なく、必ずしも有意な結果とはいえない。その点を考慮してこのグループを除外して見ると、年収の変化が少ないほど逸脱傾向が低く、年収が上がるにせよ下がるにせよ、変化が大きいほど逸脱傾向が高くなっていることがわかる。

図表 16. 逸脱に関するスコアの平均値（年収の変化別、（　）内はサンプル数）



図表 17は、逸脱スコアを回答者の残業時間別に集計したものだ。必ずしも残業時間に比例して逸脱が多くなっているわけではないが、残業時間がもっとも長いグループでは逸脱行為ももっとも多くなっている。また、「就業時間で仕事は終わらないが、残業は（会社の規制などで）できないので、仕方なく自宅などで仕事を行っている」というグループでも逸脱行為が多いことがわかる。

図表 17. 逸脱に関するスコアの平均値（残業時間別、（　）内はサンプル数）



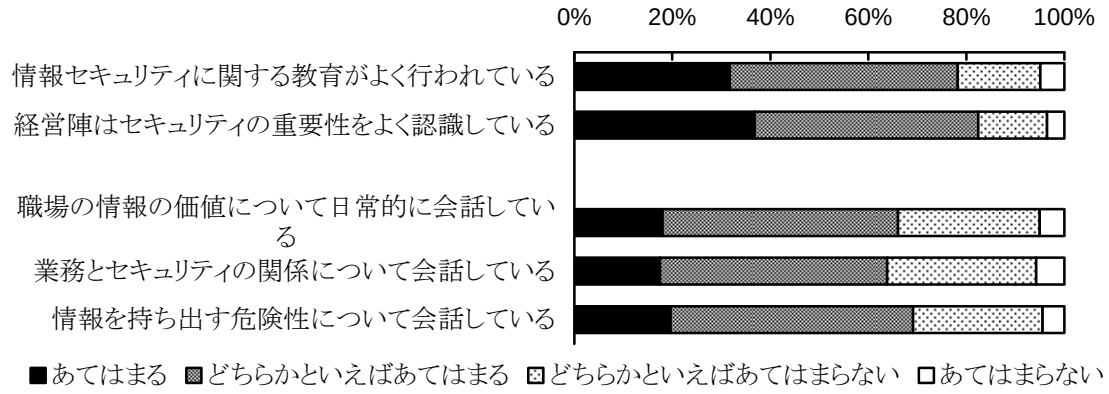
4. 情報セキュリティに関する形式的な対策の実施と運用

4.1. 組織的な情報セキュリティ対策の実施状況

本調査研究では、逸脱行為は、組織的な情報セキュリティ対策の実施状況に影響を受けるという仮説を立てている。ここでは、まず、情報セキュリティ対策の全体的な実施状況について集計結果を分析してみた、

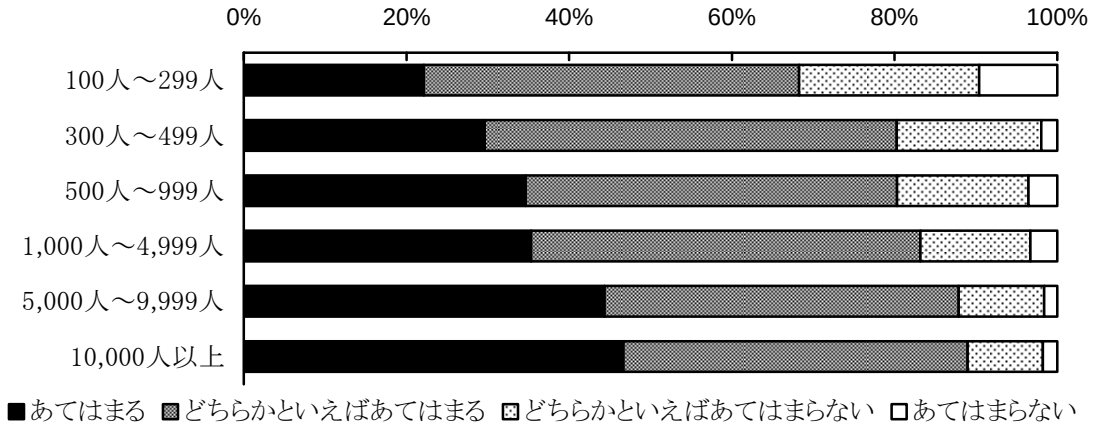
まず、図表 18からは、全体的に見れば、どのような対策についても「あてはまる」または「どちらかといえばあてはまる」という回答が 60%を超え、組織的な対策は実施されている場合が多いことがわかる。

図表 18. 組織的な情報セキュリティ対策の実施状況



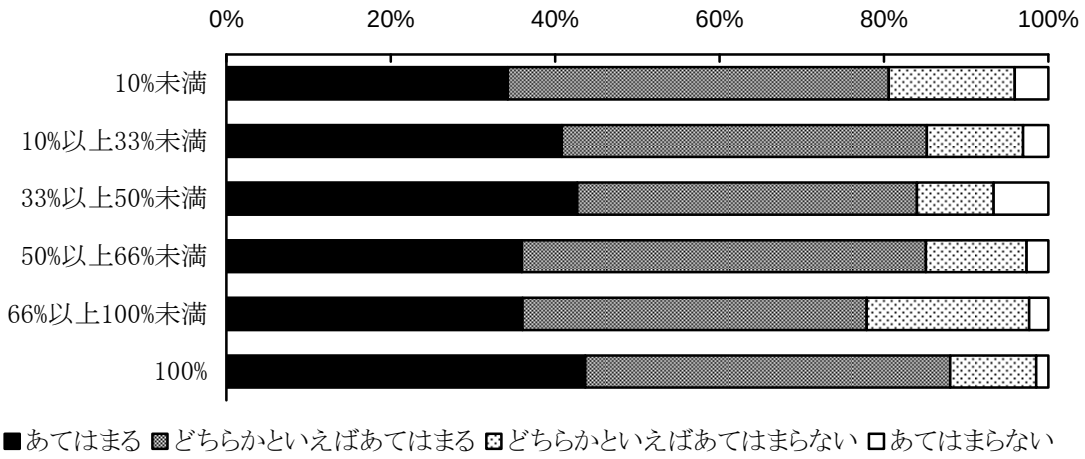
図表 19は、組織的な対策のうち、「経営陣はセキュリティの重要性をよく認識している」という質問に対する回答を、従業員数別に集計した結果である。この図から明らかなように、従業員数の多さに比例して、「経営陣はセキュリティの重要性をよく認識している」に対して「あてはまる」と答えている回答者の比率が高くなっている。大企業ほど、経営陣は情報セキュリティの重要性を認識していると考えてよいだろう。

図表 19. 経営陣はセキュリティの重要性をよく認識している（従業員数別）



つぎに、同じ質問に対する回答を外資比率別に集計したのが図表 20である。このグラフを見てもわかるように、外資比率と経営陣のセキュリティに対する意識の間には明確な関係は見られない。

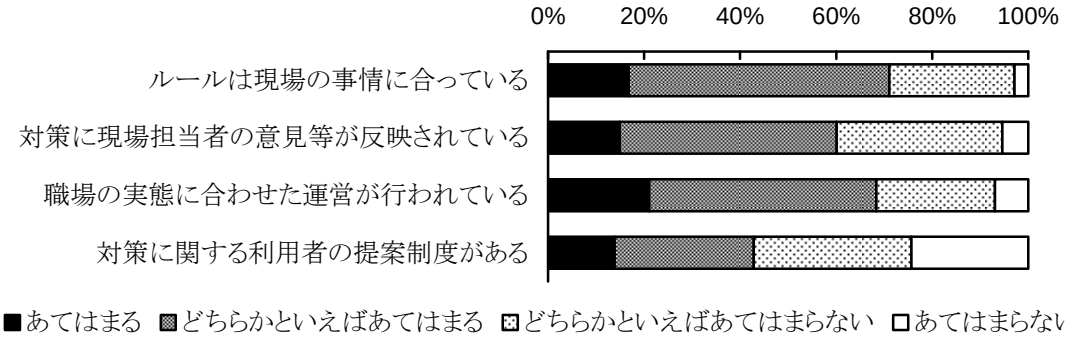
図表 20. 経営陣はセキュリティの重要性をよく認識している（外資比率別）



4.2. 情報セキュリティに関するルールの運用状況

情報セキュリティに関するルールの運用状況に関する回答を示したのが、図表 21である。先行研究によれば、情報セキュリティの実効性を高めるためには、単にルールを設定するだけでなく、現場が守りやすいルールを決めるべきであり、決定されたルールも現場の状況に応じて運営していく必要があることがわかっている[1]。図表 21からは、ルールに関する利用者からの提案制度を設けている企業は半数以下だが、ルールの運営については、「どちらかといえばあてはまる」も含めれば現場に合わせた運用を行っている企業が少なくないことがわかる。

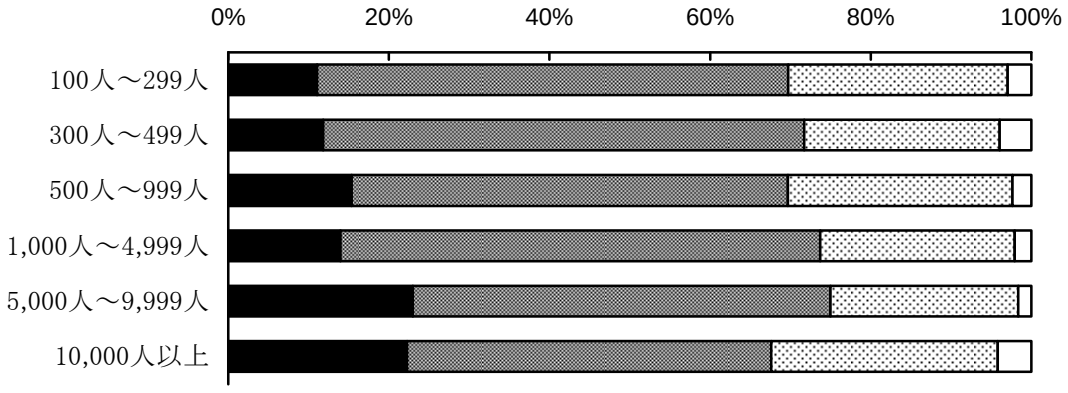
図表 21. ルールの運用状況



図表 22は、ルールの運用状況の中でも、特に「職場の実態に合わせた運営が行われている」という質問に対する回答を、従業員数別に集計したものである。このグラフでは、図表 19ほど明確な傾向はないことが見てとれる。

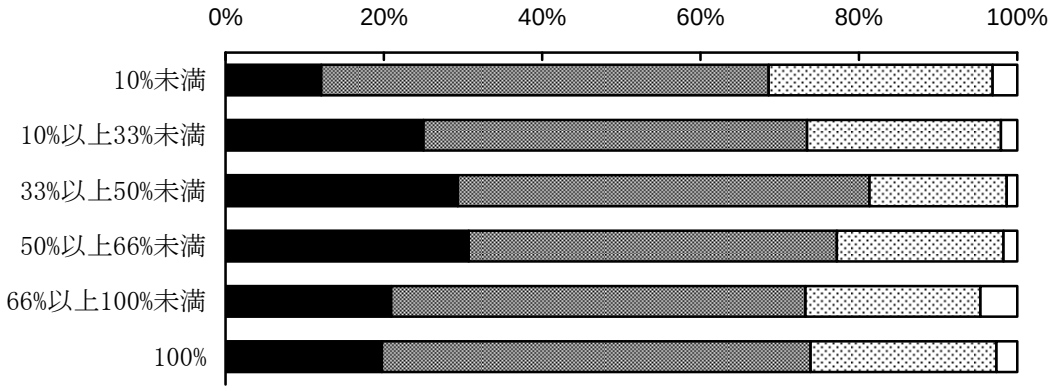
[1] たとえば、濱田・廣松・礒谷（2009）や浜屋（2009）を参照のこと。

図表 22. 職場の実態に合わせた運営が行われている（従業員数別）



図表 23は、図表 22と同じ質問について、回答者の所属企業の外資比率別に集計したものである。職場の実態に合わせたルールの運営が行われているという回答がもっとも多いのは外資比率が 33%以上 66%未満の会社だが、明確な比例的傾向があるとは言えない。

図表 23. 職場の実態に合わせた運営が行われている（外資比率別）



4.3. 対応の実施状況、ルールの運用状況と逸脱傾向との関係

つぎに、情報セキュリティの組織的な対応の状況とルールの運用状況について、上で集計した２つの質問について、回答別に逸脱スコアの平均値を計算したのが図表 24である。経営陣がセキュリティの重要性を理解しているほど、また職場の実態に合わせた運営が行われているほど、逸脱傾向は少ない（スコアが高い）という比例的な傾向があることがわかる。相関だけでは因果関係を証明することはできないが、組織的な対応や実態に合わせた運営が逸脱行為を減少させているという解釈をすることもできる。

図表 24. 組織的対応およびルールの運用状況と逸脱スコアとの関係

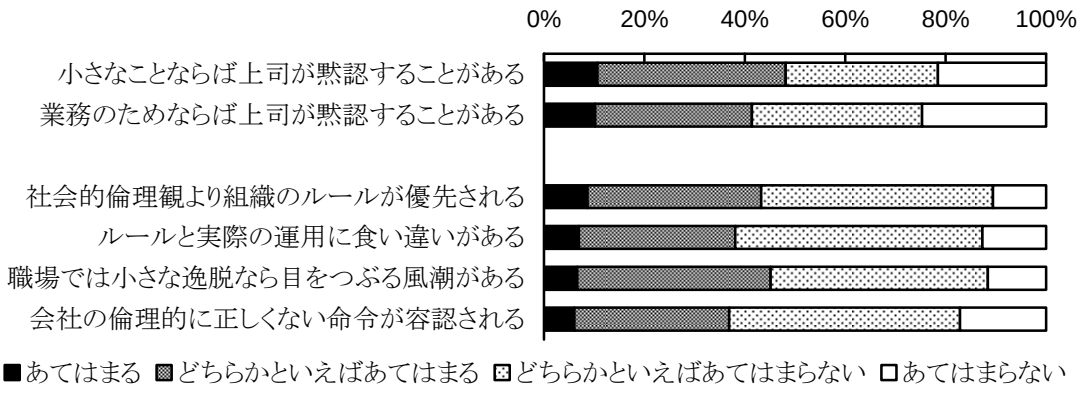
	経営陣はセキュリティの重要性をよく認識している		職場の実態に合わせた運営が行われている	
	平均値	度数	平均値	度数
あてはまる	3.128	687	3.154	393
どちらかといえばあてはまる	2.847	851	2.918	883
どちらかといえばあてはまらない	2.648	262	2.758	461
あてはまらない	2.574	66	2.697	129

5. 組織風土・文化

5.1. 上司および職場の逸脱に対する黙認傾向

個人による情報セキュリティに関するルールからの逸脱行動は、それを上司が黙認したり、職場に情報セキュリティに限定されない一般的な逸脱行為を見ないふりをしたりするような行動がある場合、増加すると考えられる。図表 25は、逸脱行為に関する上司および職場の黙認傾向に関する回答を集計したものである。

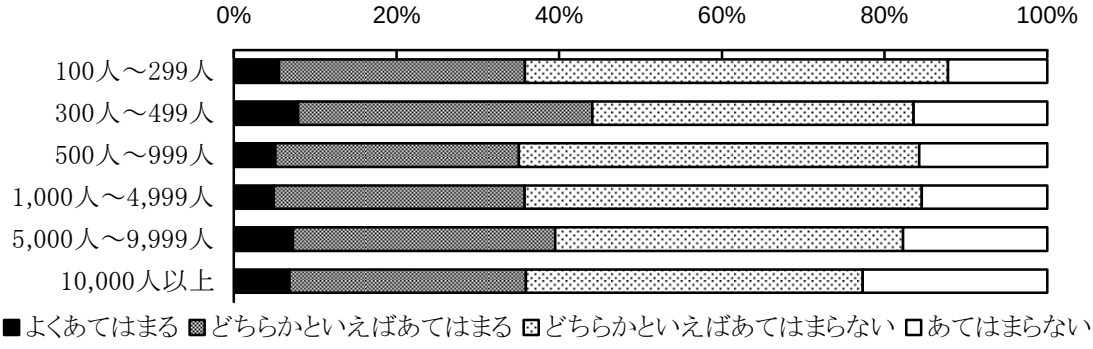
図表 25. 上司・職場の逸脱黙認傾向



上の２つは社員の情報セキュリティに関するルールからの逸脱行為を上司が黙認することに関する質問で、下の４つは情報セキュリティに限定されない一般的なルールに関する職場の雰囲気についての質問である。どの質問も、「あてはまる」という回答は 10%未満だが、「どちらかといえばあてはまる」を含めると 5 割近くが肯定的に回答している項目もある。

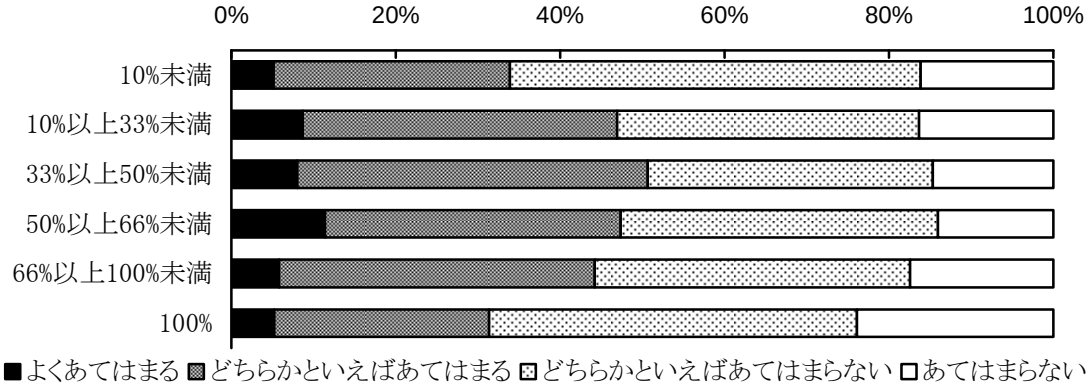
図表 26は、図表 25に示された質問のうち「会社の倫理的に正しくない命令が容認される傾向がある」という質問に対する回答を従業員数別に集計したものであるが、従業員数との間に明確な関係を見てとることはできない。

図表 26. 会社の倫理的に正しくない命令が容認される（従業員数別）



つぎに、同じ質問に対する回答を会社の外資比率別に集計したのが図表 27である。図表23と同じように、外資の比率が中程度（10%～66%）の場合に、他のグループよりも若干肯定的な回答の比率が高いものの、それほど大きな違いはない。

図表 27. 会社の倫理的に正しくない命令が容認される（外資比率別）

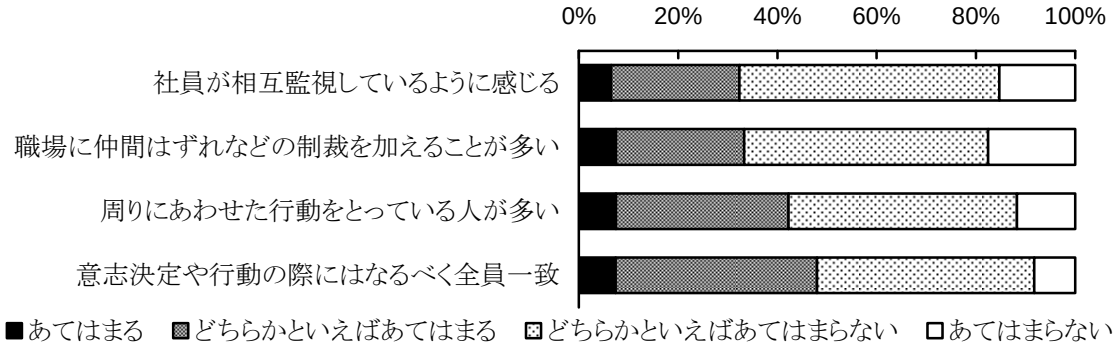


5.2. 集団主義に関する質問への回答状況

なぜ上司は部下のルールからの逸脱を黙認し、職場では社会規範から外れた命令や指示が通用するのだろうか。それは、社員一人ひとりが自己主張せず、集団に対して従属してしまうという集団主義と関係があるのではないか。実際に、本間（2007）のように、外集団意識の低下、内集団思考の強さ、集団同一化といった集団主義が組織的な逸脱行動と関係していることを明らかにした過去の研究もある。ここでは、本間（2007）の他に、「排除ゲーム」（集団から排除される可能性のあるジレンマゲーム）によって日本人の集団主義の強さを検証した高橋・山岸・橋本（2009）といった過去の研究も参考にして、集団主義に関する質問項目を作成した。なお、集団主義は、もちろんよい方向に作用すればお互いに切磋琢磨して向上するよい結果につながることもあるが、ここでは逸脱行為に注目して、逸脱行為を誰も指摘しないというマイナス面に注目している。

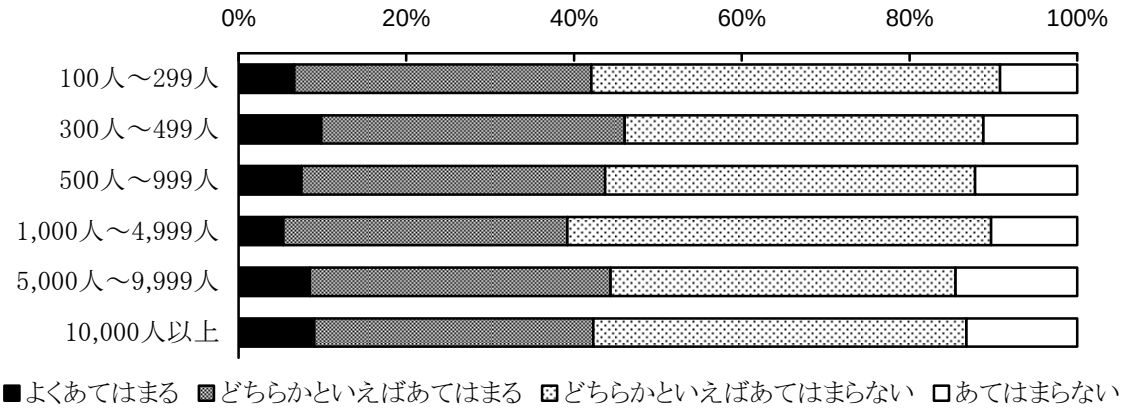
集団主義のマイナス面に関する質問に対する全体的な回答状況を集計した結果が図表28である。このグラフからは、全体的に見れば、たとえば、「周りにあわせた行動を取っている人が多い」という質問に「あてはまる」または「どちらかといえばあてはまる」と回答したのは、約40%であることがわかる。

図表 28. 集団主義のマイナス面に関する質問への回答状況

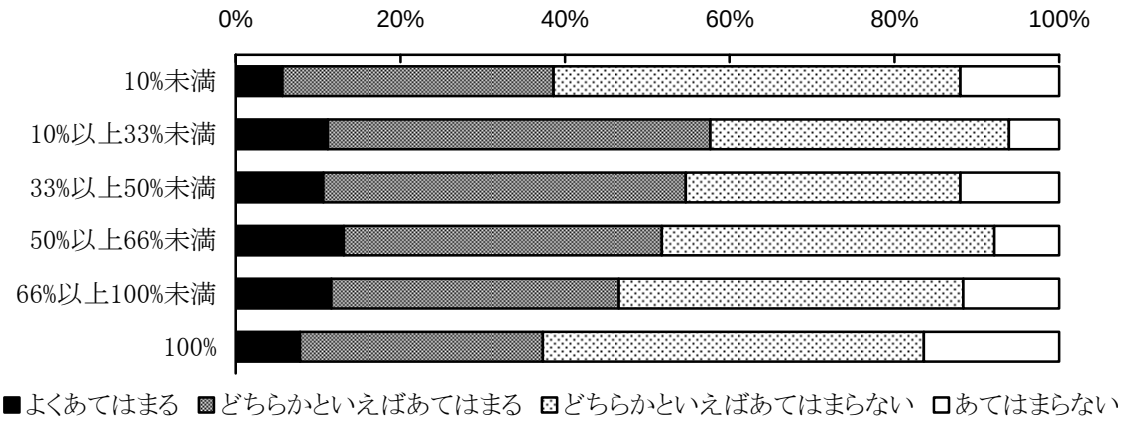


図表 29と図表 30は、「周りにあわせた行動を取っている人が多い」に対する回答を、従業員数別および外資比率別に集計したものである。まず、従業員数別については、どの規模の会社でも「あてはまる」または「どちらかといえばあてはまる」の比率は 40%程度であり、グループ別に大きな違いはないことがわかる。外資比率別に見れば、外資比率 10%未満のグループを除けば、外資比率が高いほど「あてはまる」または「どちらかといえばあてはまる」の比率は低くなる傾向にある。つまり、外資の高い企業ほど、自分が正しいと考えたことを組織の中でも主張する人が多く、いわゆる集団主義の傾向が低いということが言えるかもしれない。

図表 29. 周りにあわせた行動をとっている人が多い（従業員別）



図表 30. 周りにあわせた行動をとっている人が多い（外資比率別）



5.3. 逸脱黙認傾向および集団主義と逸脱スコアとの関係

図表 31は、上で集計した２つの質問「会社の倫理的に正しくない命令が容認される」と「周りにあわせた行動をとっている人が多い」について、回答別にグループ化して逸脱スコアの平均値を計算したものである。

図表 31. システム別のクラウドに対する関心度

	会社の倫理的に正しくない命令が容認される		周りにあわせた行動をとっている人が多い	
	平均値	度数	平均値	度数
あてはまる	2.771	113	2.779	140
どちらかといえばあてはまる	2.780	575	2.862	648
どちらかといえばあてはまらない	2.911	858	2.914	859
あてはまらない	3.207	320	3.144	219

職場の倫理に関する風土をあらわす「会社の倫理的に正しくない命令が容認される」については、明らかに、「あてはまる」グループの方が逸脱傾向が高くなっている。これは、職場で社会的な倫理よりも職場の命令や指示が優先されるようであれば情報セキュリティに対する逸脱行為も多くなるということで、ごく自然な傾向であると言える。

集団主義の強さを示す質問の一つである「周りにあわせた行動をとっている人が多い」については、「あてはまる」グループでもっとも逸脱が多く、「あてはまらない」と回答したグループでもっとも逸脱が少なくなっている。この質問についても、集団主義が強いほど逸脱が多い傾向にあることがわかる。

6. 仮説の検証：組織風土・文化と逸脱との関係

6.1. 全データを用いた検証

最後に、本調査研究で立てた３つの仮説について、共分散構造分析の手法を用いて改めて総合的に検証する。仮説は以下の３つであった。

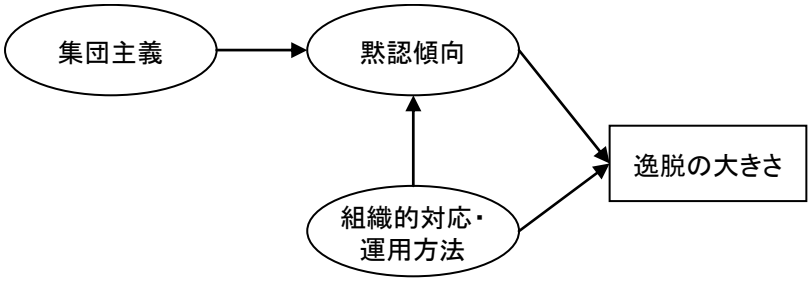
① 情報セキュリティのルールを破る行為（逸脱行為）の程度は、情報セキュリティに関する形式的な対策が実施されているかということに影響を受ける。

② 情報セキュリティに関する逸脱行為の程度は、形式的な情報セキュリティ対策だけでなく、上司の態度や職場の雰囲気といった形式化できない組織的な要因に影響を受ける。

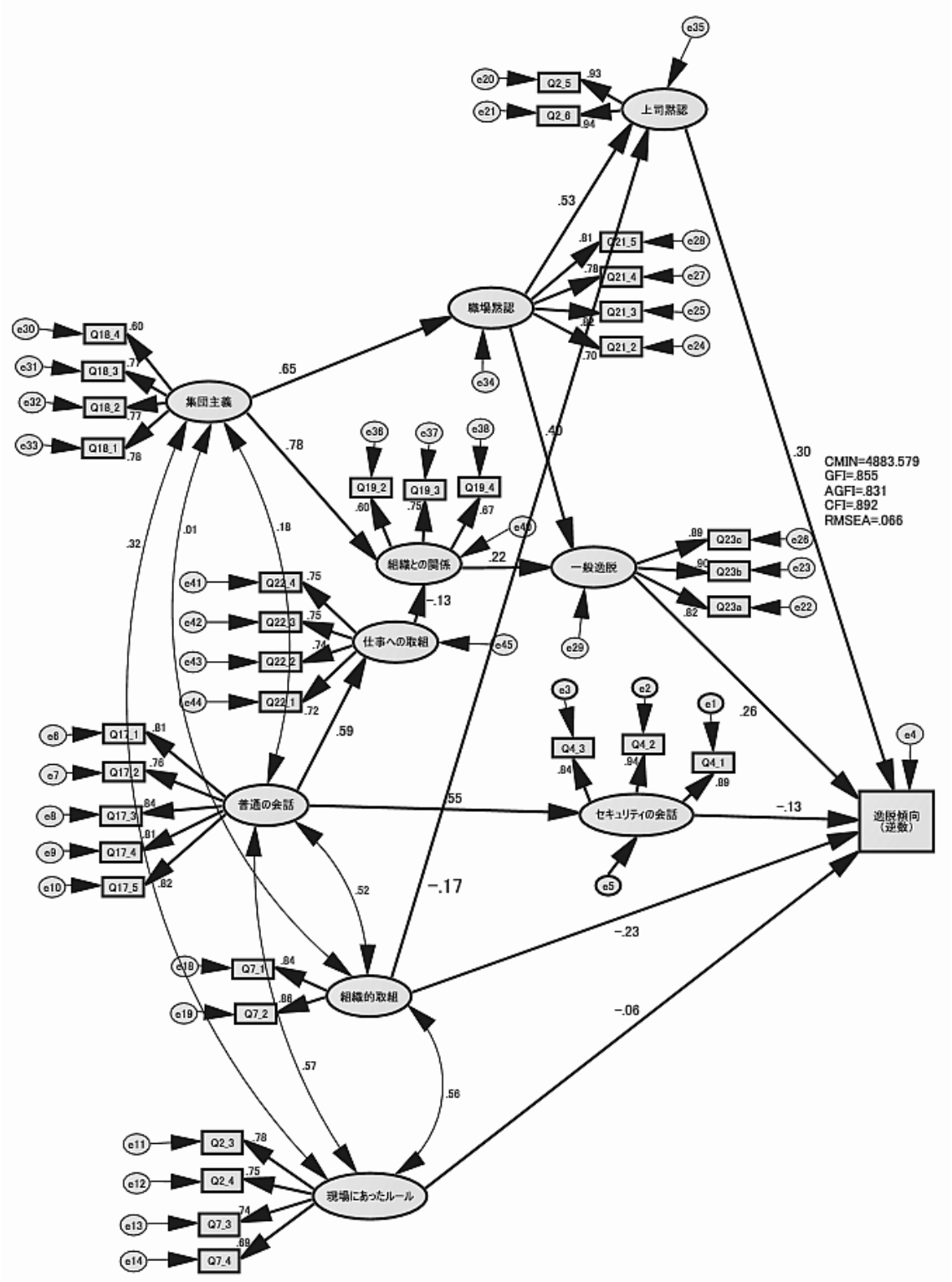
③ さらに、そういった形式化できない組織的な要因は、「集団主義」に代表される組織文化・組織風土に影響を受ける。

これらの仮説をシンプルな模式図にすると、図表 32のようになる。そして、このモデルをさらに詳細化して検証した結果が図表 33である。図表 33で、変数と変数を結ぶ片方向の矢印は因果関係を表し、数字（パス係数）は関係の強さを示しており、ここではすべて 5%水準で有意である。なお、図表 33の観測変数（長方形）のラベル（たとえばQ2_3 など）は調査票の質問番号をあらわしており、その一覧は図表 34のとおりである。

図表 32. 逸脱に関する仮説



図表 33. 仮説の詳細な検証結果（パス図）



図表 34. パス図における観測変数の一覧

潜在変数	ラベル	質問
上司黙認	Q2_5	セキュリティのルールで禁止されている事柄でも、小さなことならば上司が黙認することがある
	Q2_6	セキュリティのルールで禁止されている事柄でも、現場の業務のためならば上司が黙認することがある
職場黙認	Q21_2	職場のルールは、社会的倫理観とギャップがあっても組織のルールを優先していると感じる
	Q21_3	職場では、規定されているルールと職場内のルールに食い違いがある
	Q21_4	職場では、ルールからの小さな逸脱行動に対しては目をつぶる風潮がある
	Q21_5	上司や会社の命令が倫理的に正しくないことでも、社内ではそのような命令が容認されている
集団主義	Q18_1	職場では、社員がお互いに行動を監視しているように感じる
	Q18_2	職場では、不正を行ったり職場に不利益な行動をとったりした人物に対して、制裁（例：仲間はずれ）を加えることが多い
	Q18_3	職場では、仲間はずれにならないようにするために回りにあわせた行動をとっている人が多い
	Q18_4	職場では、なるべく全員一致で物事を決めたり、行動したりしている
組織との関係	Q19_2	職場のルールに対して疑問が発生したとしても、そのルールに従うと思う
	Q19_3	自分が周りと違う意見をもったとしても、自分でその意見を伏せてしまうことが多い
	Q19_4	自分の仕事において、組織の利益や存続のためなら社会のルールから外れてもかまわないと考えている
一般逸脱	Q23a	以下の2項目の平均値 故意に規則を曲げたり破ったりする。許可なく早退することが多い。
	Q23b	以下の2項目の平均値 勤務中に行うことべき仕事をせず個人的な仕事を行う。仕事をしないで、長い間談話する。
	Q23c	以下の 4 項目の平均値 職場の誰かについて、本人のいないところでよく悪口をいう。仕事で人を非難する。 自分の上司について、よくうわさ話をする。上司や組織について失礼なことを言う。
仕事への取組	Q22_1	自分の業務が社会的にどのような影響（関係）があるかを考慮して従事している
	Q22_2	自分の業務が会社全体の組織とどのように関わるかを理解している
	Q22_3	自分の業務から組織内全体を見渡すことができている
	Q22_4	自分と関わる他部門の業務に対し意見等を述べることができる
セキュリティの会話	Q4_1	職場内で、職場の持つ情報の価値について日常的（または定期的）に会話をしている
	Q4_2	職場内で、業務と情報セキュリティの関係について日常的（または定期的）に会話をしている
	Q4_3	職場内で、情報を持ち出す危険性について日常的（または定期的）に会話をしている
普通の会話	Q17_1	担当者と上司や上層部の人間との間で、雑談を含めて日常的な会話がよく行われている
	Q17_2	職場では、担当者同士が、雑談を含めて日常的によく会話をしている
	Q17_3	担当者は、上司や上層部の人間との間で日常業務の報告や連絡、相談を十分に行っている
	Q17_4	職場の担当者は、他部門の人間との間で、雑談を含めて日常的によく会話をしている
	Q17_5	他部門の人間との間で、日常業務の報告や連携などが必要な場合には十分に行っている
組織的取組	Q7_1	情報セキュリティに関する教育が、よく行われている
	Q7_2	経営陣は、情報セキュリティの重要性をよく認識している
現場にあったルール	Q2_3	策定されている情報セキュリティのルールは現場の事情に合っている
	Q2_4	セキュリティ対策を策定する際に現場担当者の意見や考え方が反映されていると感じている
	Q7_3	職場の実態に合わせて、情報セキュリティのルールが守りやすいような運営が行われている
	Q7_4	セキュリティ対策に関して、利用者の提案制度がある

共分散構造分析の結果を示すパス図（図表 33）からは、以下のことがわかる。

まず、情報セキュリティ教育の実施や経営者のセキュリティ重視といった組織的対策が実施されているほど、逸脱行為は少ない。職場で情報セキュリティに関する会話が日常的に行われていると、逸脱行為も少なくなる。そして、一般的なコミュニケーションが多い職場ほど、情報セキュリティに関する会話も多い。

現場に合ったルール運営がなされているかということは、「職場の実態に合わせて、情報セキュリティのルールが守りやすいような運営が行われている」や「セキュリティ対策に関して、利用者の提案制度がある」などの質問で表されるが、そのような運営がなされている場合は、そうでない場合よりも逸脱行為が少なくなる。ただし、その影響は、有意ではあるものの、組織的な対応やセキュリティに対する会話ほど大きくはない。

組織的な対策やその運営だけでなく、上司が情報セキュリティからの逸脱を黙認するかどうかも、当然ではあるが、逸脱行為の多さに大きな影響を与えている。上司がセキュリティの逸脱行為を黙認する傾向は、組織的な取組があまり実施されていない場合や、職場全体として一般的に倫理的でないことが黙認される場合に強くなる。職場が社会倫理から外れたことを黙認する傾向が強い場合は、社員の一般的な逸脱行動（怠業や他人の非難、一般的な職務ルール違反）も多くなり、結果として情報セキュリティに関する逸脱行為も多くなる。

そして、集団主義のマイナス面が強い職場では、非倫理的な命令や指示を拒否する社員も少なく、自分の仕事を組織全体の観点から把握しようとする社員も少なくなる。その結果、情報セキュリティの逸脱行為も多くなる。

つまり、本調査で設定した３つの仮説はすべて検証されたといえる。

6.2. 従業員数別の分析

全データを用いた基本分析に続いて、従業員数および外資比率別に平均構造を考慮した多母集団分析を行う。まず、図表 35および図表 36は、母集団を従業員数別に分けて、それぞれのグループのパス係数の推定値と平均構造（潜在変数の平均値）を示したものである。

図表 35. 従業員数別の分析結果：パス係数（標準化）一覧

	100～299人	300～499人	500～999人	1,000～4,999人	5,000～9,999人	10,000人以上
上司黙認→逸脱	0.238	0.353	0.371	0.295	0.329	0.279
一般逸脱→逸脱	0.338	0.268	0.278	0.246	0.255	0.260
ｾｷｭﾘﾃｨの会話→逸脱	-0.191	0.022	-0.031	-0.096	-0.223	-0.189
組織的取組→逸脱	-0.272	-0.230	-0.780	-0.332	-0.136	-0.158
現場にあったルール→逸脱	-0.026	-0.053	-0.166	-0.026	-0.064	-0.060
職場黙認→上司黙認	0.589	0.613	0.610	0.473	0.562	0.469
職場黙認→一般逸脱	0.309	0.292	0.507	0.444	0.406	0.380
組織的取組→上司黙認	-0.311	-0.109	-0.073	-0.144	-0.061	-0.211
組織との関係→一般逸脱	0.284	0.341	0.265	0.168	0.195	0.265
仕事への取組→組織との関係	-0.399	-0.008	-0.136	-0.096	-0.097	-0.094
集団主義→組織との関係	0.631	0.954	0.807	0.814	0.765	0.783
集団主義→職場黙認	0.495	0.819	0.597	0.674	0.681	0.635
普通の会話→仕事への取組	0.501	0.543	0.717	0.527	0.537	0.654
普通の会話→ｾｷｭﾘﾃｨの会話	0.562	0.505	0.589	0.435	0.538	0.614

図表 36. 従業員数別の分析結果：平均構造

	100～299人	300～499人	500～999人	1,000～4,999 人	5,000～9,999 人	10,000 人以上
集団主義	2.589	2.472	2.448	2.557	2.448	2.494
普通の会話	2.101	1.993	1.954	1.967	1.881	1.887
組織的取組	2.356	2.084	2.064	1.935	1.768	1.699
現場にあったルール	2.219	2.187	2.187	2.141	2.040	2.147
一般逸脱	3.345	3.286	3.342	3.427	3.292	3.308
仕事への取組	2.098	2.107	2.061	2.118	2.064	2.039
組織との関係	2.413	2.317	2.264	2.323	2.182	2.297
ｾｷｭﾘﾃｨの会話	2.337	2.269	2.171	2.273	2.114	2.107
上司黙認	2.472	2.491	2.587	2.730	2.602	2.700
職場黙認	2.543	2.566	2.626	2.596	2.528	2.577

これらの表からわかることは、まず、「組織的取組」という変数の平均値が従業員数が多いほど低くなっていることから（この変数は１＝「あてはまる」、４＝「あてはまらない」を数値化したものなので、値が小さいほど実施している企業の比率が高い)、大企業ほど情報セキュリティに関する組織的な対策が実施されている傾向が強い。「組織的取組」から逸脱傾向へのパス係数は、従業員数 500 人～999 人のグループでもっとも絶対値が大きく（-0.780)、大企業よりは小企業の方で値の絶対値が大きいことから、中堅・中小企業においては、大企業に比べると組織的な取組を実施している企業の比率が少なく、組織的な取組を行うことで逸脱行為を防ぐ効果も高いということがわかる。

従業員数 5,000 人以上の大企業においては、セキュリティ・ルールからの逸脱行動にもっとも大きな影響を与えるのは「上司黙認」という変数である。そして、「上司黙認」に対しては、情報セキュリティに関する「組織的取組」よりも、セキュリティに限らない一般的なルール違反や非倫理的な行動に対する「職場黙認」の方が大きな影響を与えている。そして、「集団主義」から「職場黙認」へのパス係数の値は 0.6 以上で高い。このことから、大企業においては、集団主義に流されずに個々の社員が正しいと考えていることを主張することが、セキュリティに限らず職場の逸脱行為を抑制する効果があることがわかる。逆に言えば、集団主義のマイナス面が強い職場ではルールからの逸脱行為が多いということもわかった。

6.3. 外資比率別の分析

つぎに、母集団を外資比率 33%未満と 33%以上の２つのグループに分けて、それぞれのグループのパス係数の推定値と平均構造（潜在変数の平均値）を示したのが、図表 37と図表 38である。

本調査研究では、集団主義に代表される組織文化・組織風土は企業の資本構成によって異なるのではないかという点に注目したが、平均構造を見ると外資比率の低いグループの

方が「集団主義」という変数の平均値が低く（2.509 と 2.515)、マイナス面の集団主義が強いことがわかる（上述したとおり、値が低いほど「あてはまる」という回答が多い)。また、パス係数の値を見ると、セキュリティの逸脱行為にもっとも大きな影響を与えているのは、外資比率の低いグループでは「上司黙認」であり、外資比率の高いグループは「一般逸脱」（回答者のセキュリティ以外の一般的なルールからの逸脱）である。つまり、情報セキュリティ対策の実効性を高めるためには、外資比率の低いグループでは上司による黙認を許さないようにするのがもっとも効果が高く、外資比率の高いグループでは、上司による監視よりは、個々の社員の一般的なルールからの逸脱をなくすことが効果的であると言える。

図表 37.外資比率別の分析結果：パス係数（標準化）一覧

	33%未満	33%以上
上司黙認→逸脱	0.298	0.308
一般逸脱→逸脱	0.229	0.352
ｾｷｭﾘﾃｨの会話→逸脱	-0.114	-0.145
組織的取組→逸脱	-0.278	-0.145
現場にあったルール→逸脱	-0.007	-0.213
職場黙認→上司黙認	0.487	0.594
職場黙認→一般逸脱	0.416	0.357
組織的取組→上司黙認	-0.204	-0.111
組織との関係→一般逸脱	0.208	0.304
仕事への取組→組織との関係	-0.186	-0.027
集団主義→組織との関係	0.780	0.814
集団主義→職場黙認	0.620	0.695
普通の会話→仕事への取組	0.601	0.547
普通の会話→ｾｷｭﾘﾃｨの会話	0.542	0.554

図表 38. 外資比率別の分析結果：平均構造

	33%未満	33%以上
集団主義	2.509	2.515
普通の会話	1.989	1.875
組織的取組	1.961	1.912
現場にあったルール	2.196	2.037
一般逸脱	3.374	3.273
仕事への取組	2.121	1.978
組織との関係	2.332	2.235
ｾｷｭﾘﾃｨの会話	2.233	2.140
上司黙認	2.664	2.546
職場黙認	2.603	2.511

7. まとめ

本調査研究は、わが国の企業における情報セキュリティ対策において、セキュリティポリシーの策定やセキュリティ教育といった形式的な対策だけでなく、集団主義に代表される組織文化・組織風土もルールからの逸脱行動に影響を与えているのではないかという問

題意識にもとづいて実施したものである。そして、具体的には以下の３つの仮説を、アンケート調査で得られたデータを用いて検証した。

① 情報セキュリティのルールを破る行為（逸脱行為）の程度は、情報セキュリティに関する形式的な対策が実施されているかということに影響を受ける。

② 情報セキュリティに関する逸脱行為の程度は、形式的な情報セキュリティ対策だけでなく、上司の態度や職場の雰囲気といった形式化できない組織的な要因に影響を受ける。

③ さらに、そういった形式化できない組織的な要因は、「集団主義」に代表される組織文化・組織風土に影響を受ける。

共分散構造分析による検証の結果、これら３つの仮説はすべて成立していることが明らかになった。また、企業規模別に母集団を分けて分析を行うことで、中堅・中小企業では、まずは組織的取り組みを実施することの効果が高いことや、大企業では集団主義のマイナス面が結果的に逸脱行為に結びつく傾向が強いことも検証することができた。さらに、外資比率別の分析では、外資比率の低い方が集団主義的な傾向が強く、それが情報セキュリティ・ルールからの逸脱に影響を与えている傾向も強いことがわかった。

これらのことから、情報セキュリティ対策の実効性を高めるためには、たとえばセキュリティ教育の実施といった形式的な対応だけでは不十分であり、組織文化・組織風土に合わせて、現場を巻き込んだ守りやすいルールを作ったり、そのルールを職場の実態に合わせて運営したりしていくことも必要であることが示唆される。また、過度な集団主義は、逸脱行動に対する黙認傾向につながり、セキュリティ対策の効果を抑制するというマイナスの効果を持つため、社員が集団主義に流されずに自らの考えに従ってお互いに注意しあうなど、ルールからの逸脱を黙認しないような風土・文化の改革を行うことも大切である。

参考文献

- 高橋知里・山岸俊男・橋本博文（2009）「集団からの排除と相互協調的自己呈示」、『社会心理学研究』Vol. 25, No. 2, pp. 113–120.
- 財団法人日本情報処理開発協会 プライバシーマーク推進センター（2010）「（平成 21 年度）個人情報の取扱いにおける事故報告にみる傾向と注意点」 http://privacymark.jp/reference/pdf/H21JikoHoukoku_100712.pdf
- 濱田良隆・廣松毅・礒谷洋平（2009）「情報持ち出し抑制要因に関する共分散構造分析」、経営情報学会　2009 年秋季全国研究発表大会
- 浜屋敏（2009）「情報セキュリティ対策の望ましいガバナンス構造」、経営情報学会　2009 年秋季全国研究発表大会
- 本間道子（2007）『組織性逸脱行為過程-社会心理学視点から』多賀出版

研究レポート一覧

No.373	日本企業における情報セキュリティ逸脱行為と組織文化・風土との関係	浜屋　敏 山本　哲寛	（2011年5月）
No.372	企業の社外との連携によるイノベーションの仕掛けづくりの現状－大学との連携を中心として－	西尾　好司	（2011年4月）
No.371	Linking Emissions Trading Schemes in Asian Regions	Hiroshi Hamasaki	（2011年4月）
No.370	COP17へ向けての日本の戦略 －アジア大での低炭素市場で経済と環境の両立は可能か？－	濱崎　博	（2011年4月）
No.369	成長する中国の医療市場と医療改革の現状	江藤　宗彦	（2011年4月）
No.368	住基ネットはなぜ『悪者』となったのか(共通番号[国民ID]を失敗させないために) －住基ネット報道におけるセンセーショナル・バイアスと外部世論の形成に関する研究－	榎並　利博	（2011年3月）
No.367	生物多様性視点の成長戦略	生田　孝史	（2011年2月）
No.366	北欧から考えるスマートグリッド ～再生可能エネルギーと電力市場自由化～	高橋　洋	（2011年1月）
No.365	大手ICT企業がベンチャー企業を活用するべき理由 －エコシステムからみた我が国大手ICT企業とベンチャー企業の関係構造－	湯川　抗	（2011年1月）
No.364	中印ICT戦略と産業市場の比較研究	金　堅敏	（2011年1月）
No.363	生活者の価値観変化と消費行動への影響	長島　直樹	（2010年11月）
No.362	賃金所得の企業内格差と企業間格差 －健康保険組合の月次報告データを用いた実証分析－	齊藤有希子 河野　敏鑑	（2010年10月）
No.361	健康保険組合データからみる職場・職域における環境要因と健康状態	河野　敏鑑 齊藤有希子	（2010年10月）
No.360	生物多様性視点の企業経営	生田　孝史	（2010年8月）
No.359	クラウドコンピューティングに関するユーザーニーズの調査	浜屋　敏	（2010年7月）
No.358	高齢化社会における「負担と給付」のあり方と「日本型」福祉社会	南波駿太郎	（2010年6月）
No.357	「温室効果ガス25％削減と企業競争力維持の両立は可能か？」	濱崎　博	（2010年6月）
No.356	Global Emission Trading Scheme -New International Framework beyond the Kyoto Protocol-	Hiroshi Hamasaki	（2010年6月）
No.355	中国人民元為替問題の中間的総括	柯　隆	（2010年6月）
No.354	サービス評価モデルとしての日本版顧客満足度指数	長島　直樹	（2010年5月）
No.353	健康と経済・経営を関連付ける視点	河野　敏鑑	（2010年4月）
No.352	高齢化社会における福祉サービスと「地域主権」	南波駿太郎	（2009年12月）
No.351	米国の医療保険制度改革の動向	江藤　宗彦	（2009年11月）
No.350	サービスプロセスにおける評価要素の推移 －非対面サービスを中心として－	長島　直樹	（2009年10月）
No.349	社会保障番号と税制・社会保障の一体改革	河野　敏鑑	（2009年9月）
No.348	カーボンオフセットと国内炭素市場形成の課題	生田　孝史	（2009年8月）
No.347	中国のミドル市場開拓戦略と日系企業	金　堅敏	（2009年7月）

http://jp.fujitsu.com/group/fri/report/research/

研究レポートは上記URLからも検索できます

富士通総研　経済研究所

〒105-0022　東京都港区海岸1丁目16番1号（ニューピア竹芝サウスタワー）
TEL.03-5401-8392　FAX.03-5401-8438
URL http://jp.fujitsu.com/group/fri/