07-シス販-01

中堅・中小企業のITサービスメニューに関する調査研究

KEIRIN
この事業は、競輪の補助金を受けて
実施したものです。
http://ringring-keirin.jp

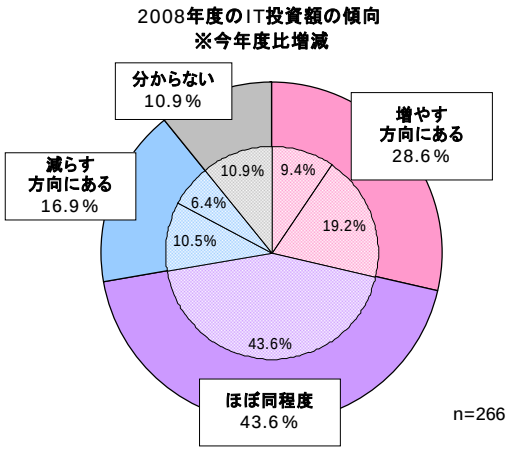
平成 20 年 3 月

社団法人　日本コンピュータシステム販売店協会
http://www.jcssa.or.jp/

はじめに

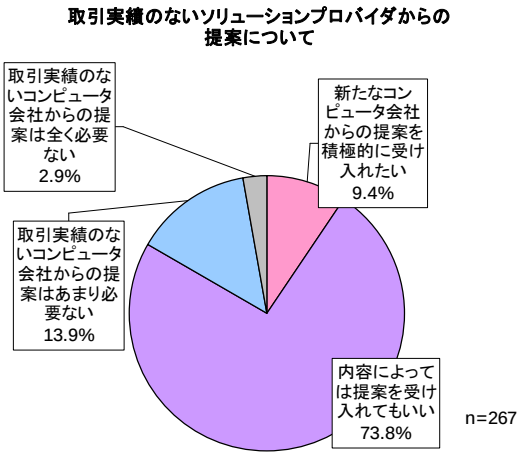
2008 年の経済産業省の重点施策のひとつに「地域・中小企業、国民一人ひとりの潜在力発揮による成長の底上げ」がある。これは同省の【緊急に取り組むべき最重点 3 本柱】のひとつであり
持続的な経済成長の実現のための重要項目となっている。
大企業の IT 予算の見込みは 3%減との予測[1]　がある一方、中堅・中小企業の IT 投資は 3 割の企業が増やす方向にあると回答しており（図表 A)、産業全体を活気づけるために国の政策も中堅・中小企業にシフトしてきていると考えられる。しかしながらこれまでの当協会の調査では、中小企業においては IT システム担当者はなかなか専任化できず、担当者がいても社内における全 IT システムの面倒を 1 人で見ざるを得ないという実態にある企業が多いことがわかっており、自社の業務改革に対する提案を待っているというデータ（図表 B）も頷けるところである。

図表 A



出典：日経ソリューションビジネス　2007.10.30 日号「緊急調査 SMB 市場に臨む SIer と顧客の本音」から転載
p37 図 D-1
「2008 年度の IT 投資額の傾向」

図表 B



p35 図 A-1
「取引実績のないソリューションプロバイダからの提案について」

また、日経ソリューションプロバイダによる調査で、2008 年度における中堅・中小企業の IT 投資の主な目的は「業務コストの削減」「セキュリティ対策の強化」「業務改革の推進」がトップ 3 に、4 位に「内部統制などへの対応」が挙げられており、IT が中堅・中小企業の企業体質の強化にとって益々重要な位置を占めつつあることがうかがわれる。

中堅・中小企業のIT化を促進することは、タイムリーな情報入手による経営判断の迅速化などで経営の効率化・競争力強化を実現し、結果的に中小企業の業績回復につながることは、いくつかの成功企業の事例を見ても明らかである。このIT導入を成功させるために、運用、情報セキュリティ、ネットワーク環境の整備などに関係するITサービスがますます重要になってきている。
大企業ではITサービスが理解され浸透してきていることがうかがわれるが、一方、中堅・中小企業では、上記を実現するITを支え、安全・安心・安定的に活用することができるようにするためのITサービスに関する認知と理解がまだ進んでおらず、これらのITサービスが本当に必要とされる商品として、十分に受け入れられている状況にはまだ到達していない。

[1]：日経コンピュータ　2007.11.26 日号　『第 2 回「企業の IT 力調査」』p16 から転載

さらに昨今では、人権尊重の観点からの「個人情報保護法[2]」が施行され、IT の幅広い活用の中で、個人情報の漏洩対策が義務付けられ、さらに健全な企業のあり方を規定した「新会社法[3]」の施行、不正の撲滅を強制し健全なる財務会計遂行を義務付けた「日本版 SOX 法[4]」の制定、これらの企業の不正全般を取り締る内部統制体制の確立なども義務付けられる状況にあり、これらへの対策の仕掛け・仕組みの早急な確立が要求されている。

この状況を鑑みると、企業において競争力強化を狙いとした IT 活用の拡大に対し、企業の生命保険とも言うべきリスク対策の強化が求められることになる。このリスク対策はネットワーク社会が拡充されることに伴い、リスク対策を推進するお客様や取引先からも強く要求されることになり、ひいては、競争力強化の仕掛け・仕組み作りと、安全・安心の確立が、企業の勝ち残りに不可欠の要素となって来ることは必然である。

本報告書は、ベンダとユーザ双方の調査を行い、ユーザの求める IT サービスを調査研究することを目的として、上記の状況や過去 3 年間の調査による実態を踏まえ、特に運用・セキュリティに的を絞り、この領域に対するベンダの IT サービスメニューの調査と、ユーザに対するアンケート調査および面接調査により得ることができた中堅・中小企業の現状を調査・分析し作成したものである。下記のような場面で参考資料として、合わせて当協会にて独自に作成した「必要なセキュリティ対策がわかる本[5]」と共に使用されることを期待している。

① 国の各種政策に呼応してベンダ・販売店から提示されている新しいメニューを、わかりやすい要素別のメニューに分解することによって、元のメニューへの理解を深める（アンケートおよび「必要なセキュリティ対策がわかる本」による）
② アンケートによる IT サービス導入実体の把握と結果分析、およびその結果のまとめを提示することで、自社の位置づけを認識する
③ これらを踏まえて、新たな IT 投資への方向性を判断する

また、経営者の方々に IT の運用やセキュリティについてご理解いただくため、企業の現状を「企業経営者の方々にご配慮いただきたい課題」として付録にまとめたので参考にして頂きたい。

本報告書が今後の IT システムの導入・強化・運用を検討する際の参考になれば幸いである。

サポートサービス委員会
委員長　　前川　和彦
副委員長　浦川　龍男

[2]：個人情報の保護に関する法律（平成一五年五月三十日法律第五十七号）
[3]：商法第 2 編、有限会社法、株式会社の監査などに関する商法の特例に関する法律などの各規定を現代的な表記に改めた上で分かりやすく再編成した新たな法典（会社法）
[4]：金融商品取引法
[5]：「必要なセキュリティ対策がわかる本」については 3.4 節参照

● 市場部会・サポートサービス委員会・委員一覧

	名　　前	会　社　名	役　　職
部会長	大塚　裕司	株式会社大塚商会	代表取締役社長
【委員会】			
委員長	前川　和彦	NEC フィールディング株式会社	執行役員
副委員長	浦川　龍男	株式会社富士通エフサス	顧問
委員	加藤　誠	NEC フィールディング株式会社	シニアエキスパート
委員	遠渡　明久	株式会社大塚商会	執行役員
委員	太田　和宏	日本事務器株式会社	部長
委員	和田　孝司	東芝情報機器株式会社	部長
委員	海老沢　久行	リコーテクノシステムズ株式会社	リーダー
委員	東谷　滋	日興通信株式会社	部長
委員	横山　一郎	日興通信株式会社	シニアマネージャー
委員	島村　宗一	株式会社ブロードリーフ	部長
委員	鈴木　規純	株式会社ブロードリーフ	課長
委員	吉村　秀樹	株式会社シー・シー・ダブル	マネージャー
委員	清水　祐昭	キューアンドエー株式会社	部長
委員	板見谷　剛史	CompTIA 日本支局	部長
委員	奥田　和男	元社団法人 日本情報システム・ユーザー協会	
委員	福永　信義	元富士通株式会社	
委員	斎藤　久雄	NEC フィールディング株式会社	
委員	三浦　一洋	全国中小企業団体中央会	部長

	名　　前	会　社　名	役　　職
【運用 WT】			
リーダー	浦川　龍男	株式会社富士通エフサス	顧問
サブリーダー	佐藤　昭博	株式会社富士通エフサス	専任部長
	篠原　英明	NEC フィールディング株式会社	マネージャー
	芳賀　明夫	株式会社大塚商会	課長
	堀　　博	日本事務器株式会社	グループリーダー
	和田　孝司	東芝情報機器株式会社	参与
	島村　宗一	株式会社ブロードリーフ	部長
	鈴木　規純	株式会社ブロードリーフ	課長
	南部　有一郎	株式会社ブロードリーフ	リーダー
	吉村　秀樹	株式会社シー・シー・ダブル	マネージャー
	清水　祐昭	キューアンドエー株式会社	部長
	海老原　隆	キューアンドエー株式会社	マネージャー
【セキュリティ WT】			
リーダー	加藤　誠	NEC フィールディング株式会社	シニアエキスパート
	内藤　剛	NEC フィールディング株式会社	マネージャー
	山本　幸司	NEC フィールディング株式会社	マネージャー
	亀田　匡司	株式会社富士通エフサス	
	渡辺　裕二	株式会社大塚商会	課長
	西浪　一雄	日本事務器株式会社	グループリーダー
	和田　孝司	東芝情報機器株式会社	参与
	海老沢　久行	リコーテクノシステムズ株式会社	リーダー
	島村　宗一	株式会社ブロードリーフ	部長
	手島　啓補	株式会社ブロードリーフ	課長
	中田　英之	株式会社ブロードリーフ	
	吉村　秀樹	株式会社シー・シー・ダブル	マネージャー
	藤本　昌宏	株式会社シー・シー・ダブル	
	板見谷　剛史	CompTIA 日本支局	部長
【事務局】			
	松波　道廣	日本コンピュータシステム販売店協会	専務理事
	山田　勝正	日本コンピュータシステム販売店協会	事務局長
	古田　正武	日本コンピュータシステム販売店協会	参与
	岩本　将典	ジーエフケーマーケティングサービスジャパン株式会社	

目次

1　調査概要

1 調査概要

1.1 調査の目的

昨年度の調査から、中堅・中小企業の IT 活用は大企業と比べて、体制や投入コスト面などの諸事情で、遅れている状況であることがわかっている。

しかしながら、ネットワークインフラやＩＴの目覚しい変革は、ビジネススタイルや業務の進め方を大きく変貌させており、IT 活用の拡大を図らない限り、事業継続が難しくなってきているのが実態である。

今回は、昨年の地域間での活用ギャップや、企業内での意識ギャップの調査を踏まえ、IT 活用の広範化において、特に今後ますます重要となる、運用とセキュリティの取り組みについて調査し、これを踏まえて中堅・中小企業の安全・安心の IT 化対策の実態を、さまざまな角度から定量的に把握することで、広範な IT 化を支援し企業の成長に寄与することを目的としている。

1.2 調査対象企業の選定

本調査の対象企業は以下の 2 つの方法で選定した。

- 当協会の会員企業の、自社顧客の紹介
- ウェブサイトからの企業情報の収集

1.3 調査の実施方法

郵送調査と面接調査の 2 種類の調査を実施した。郵送調査で全体像を把握し、面接調査によって、全体像の補完と実態の掌握を行った。

郵送調査

調査選定企業にアンケート調査票を郵送し、経営者並びに情報システム管理者の方の記入のもと、返信用封筒での返送を依頼した。

面接調査

郵送調査に回答のあった企業の中から、中堅・中小企業の今後の IT 化の参考とすべく、対策の進んでいる企業を選定し、面接調査のもと対策のきっかけや、工夫・苦労談などの実態を把握し、補完情報とした。

1.4 「郵送調査」調査方法の詳細

1.4.1 調査対象企業

企業規模

主として 350 人以下の中堅・中小企業を中心に選定した。

対象者

調査選定企業の経営者、および情報システム管理者とした。

1.4.2 調査実施時期

平成 19 年 10 月 5 日～平成 19 年 12 月 14 日

1.5 「面接調査」調査方法の詳細

1.5.1 調査対象企業

対象企業

対策の進んだ企業 9 社を選定し面接調査を行った。

面接対象者

面接企業の情報システム管理者とした。

1.5.2 調査方法

面接対象として選定した企業へ面接調査の要請を行い、承諾のあった企業に対して訪問調査を行った。面接は当協会の委員会委員 2 人一組で行った。

1.5.3 調査実施時期

平成 19 年 11 月 29 日～平成 19 年 12 月 14 日

1.6 調査項目

〈郵送調査〉

経営者向けの質問

- 情報システム全般について
- 情報セキュリティについて

情報システム管理者向けの質問

- コンピュータの運用について
- セキュリティについて
- 調査対象企業のプロフィール

〈面接調査〉

- 安全・安心の情報システム化のための、運用強化・セキュリティ対策に取り組んだきっかけ（動機）
- 運用強化・セキュリティ対策に取り組んだ主目的
- 目的の達成度合いや効果・成果・満足度など
- 苦労した点・工夫した点
- 経営者の反応・社員の反応
- 現状の課題・問題点
- JCSSA[6]への期待
- 業者・業界への期待

1.7 〈郵送調査〉回収結果

1.7.1 回収数

調査票発送数	728 件
回収数	165 件
有効回答数	160 件
回収率	22%

[6]社団法人日本コンピュータシステム販売店協会

1.7.2 都道府県

	全体	首都圏	中京圏	京阪神 大都市圏	政令指定都市	市町村
件数 (件)	160	62	6	17	40	35
構成比 (%)	100	39	4	11	25	22

本調査における地域の定義は以下の通り：

首都圏：東京都、神奈川県、千葉県、埼玉県

中京圏： 愛知県、三重県、岐阜県

京阪神大都市圏：大阪府、京都府、兵庫県、滋賀県、和歌山県、奈良県

政令指定都市：上記を除く政令指定都市

(札幌市、仙台市、新潟市、静岡市、浜松市、広島市、北九州市、福岡市)

市町村：上記以外の地域

1.7.3 業種

	全体	製造業	サービス業	建設業	その他	情報･通信業	商業
件数 (件)	160	39	33	22	6	23	37
構成比 (%)	100	24	21	14	4	14	23

業種については、集まった回答に対して以下の変更を加えた：

・「サービス業」から「情報・通信業」を分離させて新しく項目として立てた。

・「卸・小売業」の名称を「商業」に変更した。

1.7.4 企業規模

	全体	1-30人	31-60人	61-100人	101-350人	351人以上	不 明
件数 (件)	160	31	44	25	38	18	4
構成比 (%)	100	19	28	16	24	11	3

※ 調査対象企業の詳細な情報については、「4. 調査内容」の章を参照されたい。

1.8 <面接調査>実施結果

1.8.1 実施数

面接調査企業

合計	9 社
東京都	3 社
大阪府	3 社
福岡県	2 社
北海道	1 社

1.9 調査データの取り扱いについて

1.9.1 未回答の取り扱い

未回答の部分がある企業については、その企業の回答を全て削除せずに、未回答部分のみを集計対象から外した。

ただし、企業属性の部分(F1～F8)については未回答の場合は「不明」としてカウントし、集計を行った。

1.9.2 企業規模の推定

従業員数についての記入がなかった場合は、会員企業から事前に入手していた「推定従業員数」を代入して集計を行った。

1.9.3 地域の決定

住所についての記入がなかった場合は、アンケート郵送先の住所をその企業の住所として集計を行った。

2　全体のまとめ

2. 全体のまとめ

今回の調査では、過去 3 年間に亘って行った調査研究から、幅広い業務での IT 活用が進む中で、安全・安心そして安定化に不可欠なサポートサービスメニューのうち、特に重要な、運用・セキュリティに絞った。
この調査は、特に下記のことを意識して実施した。

①. 従来の調査において要望の多かった、中堅・中小企業が意識する同一業界・同規模企業・同一地域・IT 投資額などに対する自社の実態が比較できるデータの収集
②. 調査企業独自の状況と、上記比較における位置付け、診断結果に基づく今後のアドバイス書の提示
③. 運用・セキュリティの対策の実施に当っての、動機や工夫・苦労談等、中堅・中小企業のヒントとなる情報を、面接調査により収集する。
この情報を、報告書の補完に活用すると共に、報告書に掲載し提供
④. わかりにくく、投資効果面で躊躇するセキュリティに関する理解度や、ベンダが提供しているメニューの理解度を助けるための、小冊子「必要なセキュリティ対策がわかる本」を、当協会にて独自作成し配布
（「必要なセキュリティ対策がわかる本」については「3.4 セキュリティについて」を参照）
⑤. これらを通し、企業への安全・安心の IT を支援

アンケートについては、難しい表現や専門用語は極力避けた。そして意図を理解しやすくすることを意識し質問項目を作成した。その結果アンケートに答えることで、運用・セキュリティに関する理解度がチェックできることや、新たな知識が吸収できる点で、大変良い勉強材料になるとの評価を得た。回答については記述式を避け、5 者択一の選択式を採用。また比較情報として、IT 投資額や活用パソコン台数他の、一歩踏み込んだ企業プロフィールを収集したことで、内容の充実化に大いに役立った。

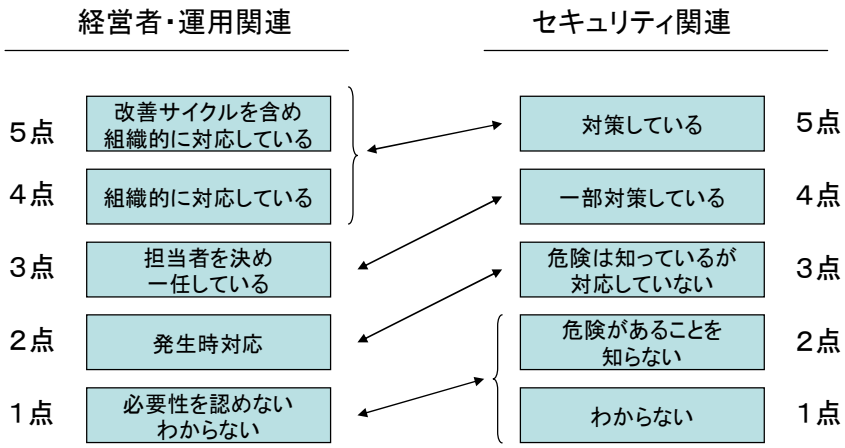
面接調査については、アンケートの結果を補完するために行ったが、得点が平均値よりも良い企業を中心に行うことによって、これから対策を始めようとしている企業の参考になるような情報を提供することを意識した。対策の実施状況が平均点以上の企業には以下の特徴が見られることがわかった。

①. 経営者の IT への関心が高く、担当者も積極的に自らの工夫を経営者に提言して、経営者がその提言を取り上げているため、全社的・組織的な対応ができている。
②. それらの対応は、「運用強化」「セキュリティ対策」においてだけではなく、IT の「戦略的活用」や「経営上の効果の向上」においても発揮されている。

詳細については、「3.5 面接調査まとめ」を参照されたい。

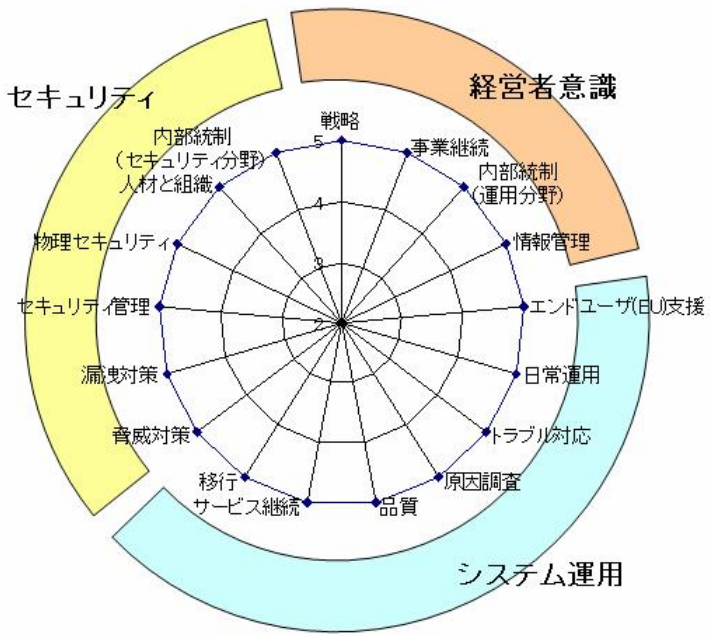
また、アンケートに回答し分析結果を希望する企業には、分析結果と共にこの情報を提供した。今回のアンケートについては 5 者択一方式となっているが、結果を見るにあたってはほぼ図表 2.0.0.1 のような対応レベルの差があるので、若干運用関連の点数が低めになることを考慮されたい。

図表 2.0.0.1



今回のアンケートでは、92 の質問を行っている。その質問を 17 個の大分類にまとめ、レーダーチャートで傾向を見やすくしている。図表 2.0.0.2 にこのレーダーチャートの凡例を示す。17 個の大分類は大きく、経営者意識・システム運用・セキュリティの 3 つのカテゴリに分類されている。

図表 2.0.0.2

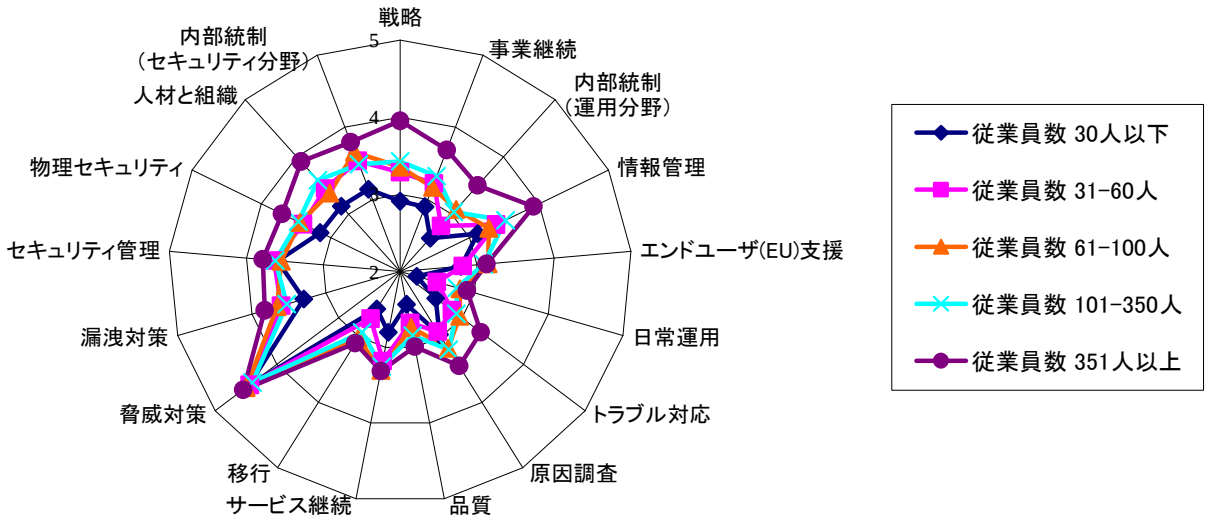


今回のアンケートによる大項目のポイントを比較してみると、次のような傾向が見えてくる。

(1)従業員数の大小による対策の傾向

全体の傾向として、351 人以上の企業ではそれ以下の従業員数の企業に比べて、より多くの対策を実施している。また従業員 30 人以下の企業では相対的に対策が遅れている傾向にあることがわかる。結果として、30 人以下の企業への対策を急ぐと共に 31 人から 350 人の従業員規模および、それ以上の従業員数の規模の企業への、対策レベルを上げるための啓蒙や提案活動を急ぎ実施していく必要があることがわかる。

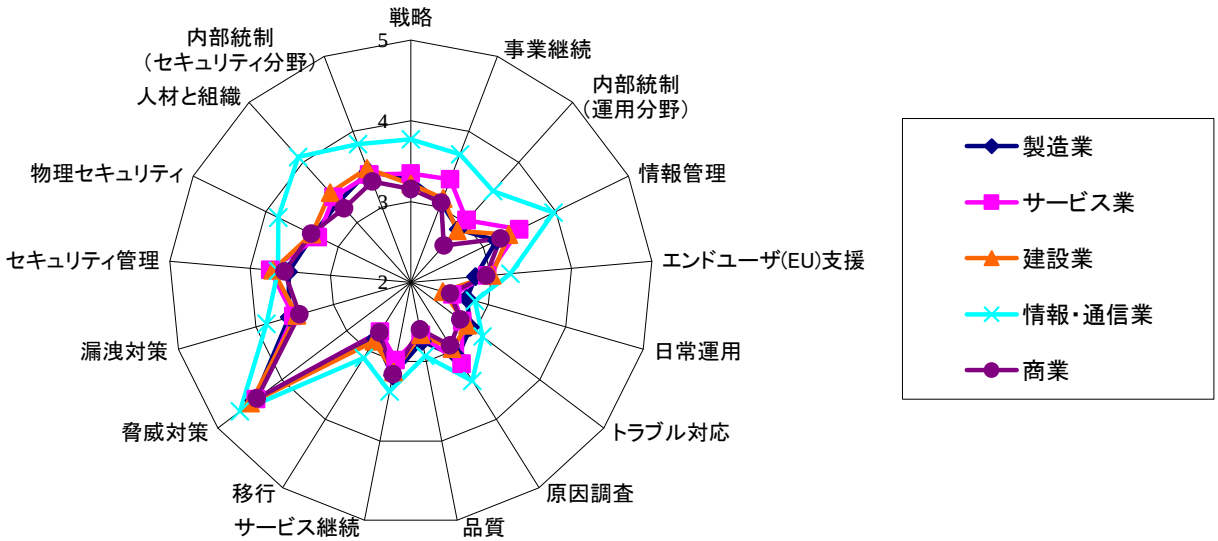
図表 2.0.0.3



(2)業種による対策の傾向

図表から明らかなように、業種の中でも情報・通信業の各種対策への対応が進んでいることがわかる。情報・通信業は顧客に安心、安全、信頼性を真っ先に提供すべき立場にあることから、この傾向は当然と考えられるが、一方その他の業種は概ね同じ傾向を示しており、業種に関わらず各種対策のレベルアップが必要であることを示している。

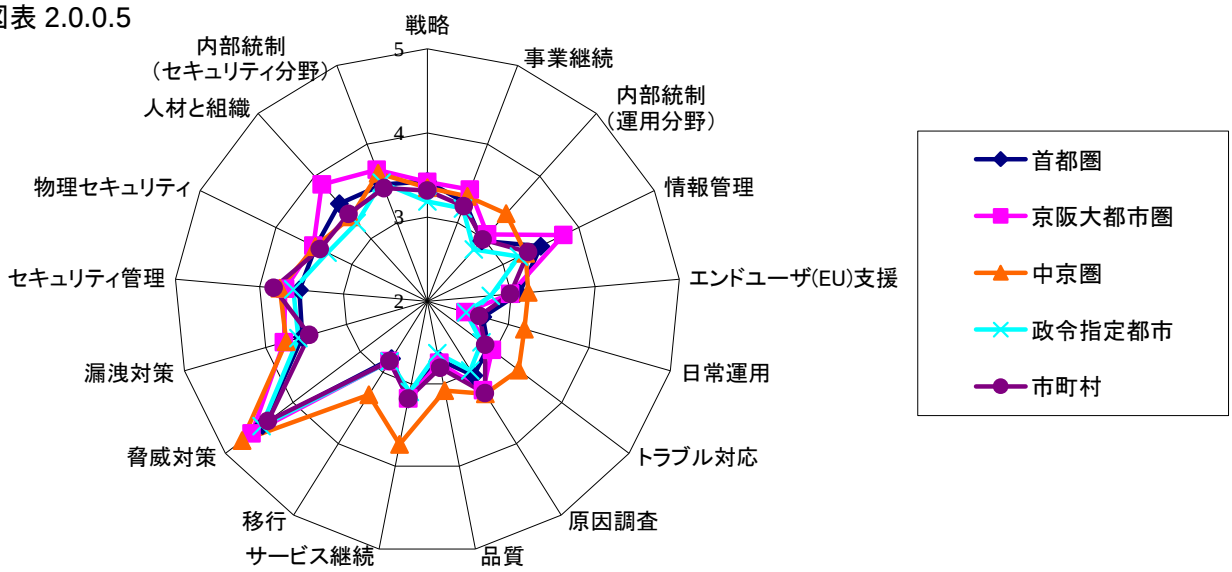
図表 2.0.0.4



(3)地域による対策の傾向

地域による違いはほとんどないが、ひとつの傾向として中京圏においては運用関連の対策が進んでおり、京阪大都市圏ではセキュリティ関連の対策が若干他の地域よりもポイントが高いようにも見える。

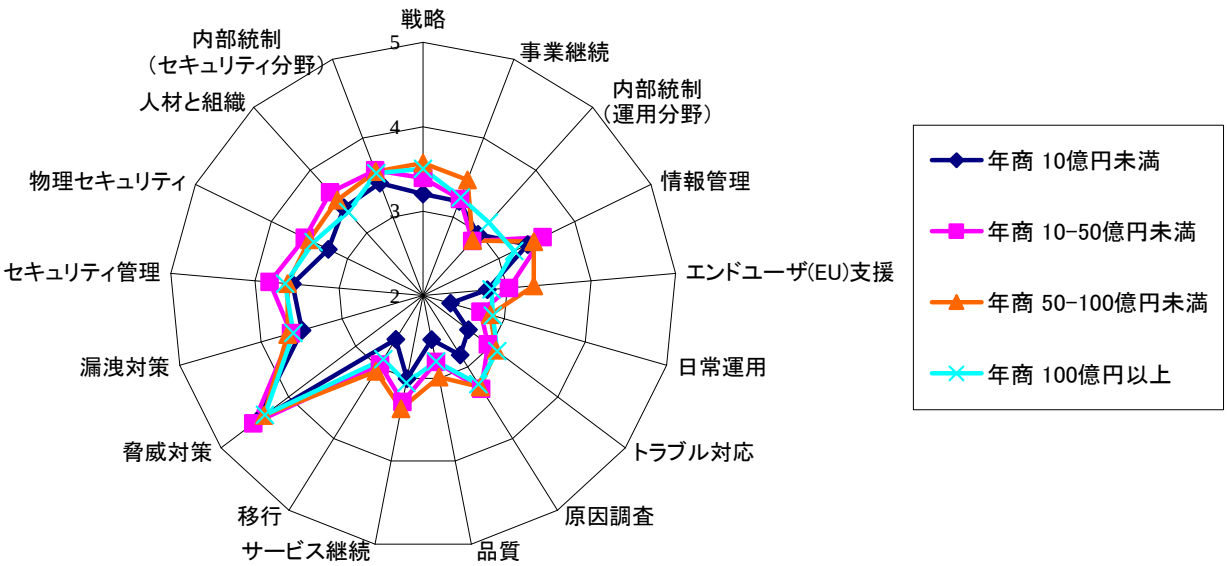
図表 2.0.0.5



(4)年商による対策の傾向

年商による対策のレベル差はほとんどないといっていい。但し年商 10 億円以下の企業では、対策が遅れる傾向にあるようである。

図表 2.0.0.6



(5)全体傾向

全体を通して 30 人以下、年商 10 億円以下の企業については、対策が進んでいない傾向にあり、専任の担当者が設けられない、費用の捻出が大変、などの課題を抱えていると推測される。また本来の得点は 4～5 の間にあることが望ましいが、全体的に運用では 3（担当者を決め任せてある）の前後、セキュリティでは 3（危険は知っているが対応していない）と 4（一部対応している）の間にあり、組織的な対応になっていないことが、今後の対策への大きな課題である。

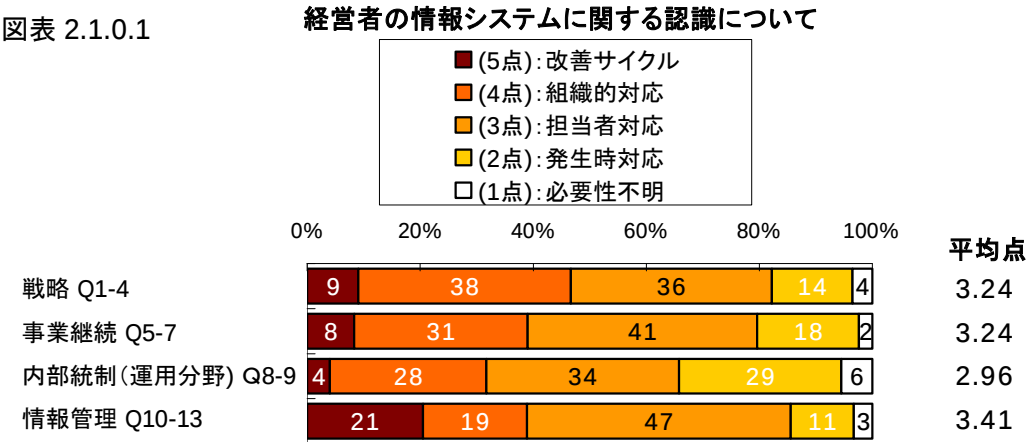
2.1 経営者の情報システムに関する認識について

アンケートの「経営者の情報システムに関する認識」では戦略に関して 4 質問、事業継続に関して 3 質問、内部統制に関して 2 質問、情報管理に関して 4 質問、合計 13 の質問について回答を得ている。なお、図表の簡易的表現は次のような内容を意味している。

改善サイクル：改善サイクルを決め、組織的に対応している
組織的対応　：組織的に対応している
担当者対応　：担当者を決め一任している
発生時対応　：把握・説明・評価・指導・対策・対応をしていない
必要性不明　：必要性を認めない／わからない

それぞれの質問グループの対策の分布は以下のようになっており、「改善サイクル」～「組織的対応」までの割合が 40%前後と全体的に低い。何らかの対応を取っていると思われる「担当者対応」まで含めると 80%程度になるが、内部統制への対応については、やはり進んでいないことがわかる。規模別・業種別・地域別に整理したデータとその分析は「3.2　経営者の情報システムに関する認識」に記載されているが、企業規模が大きくなるほど平均点は高くなり、地域別では大差はないが大都市圏は平均点が高い傾向にある。また当然といえるが情報・通信業の平均点が高くなっている。

図表 2.1.0.1



経営者の中には意識が高く、組織的な対応をしている企業も多く見られるが、平均的に見るとまだまだ組織的な対応をとっている企業は少なく、IT を利用して業績の向上に繋げるという意識を醸成するための努力が、当該企業はもちろん、国・政府・当協会のような関係団体に求められている。

2.2 運用について

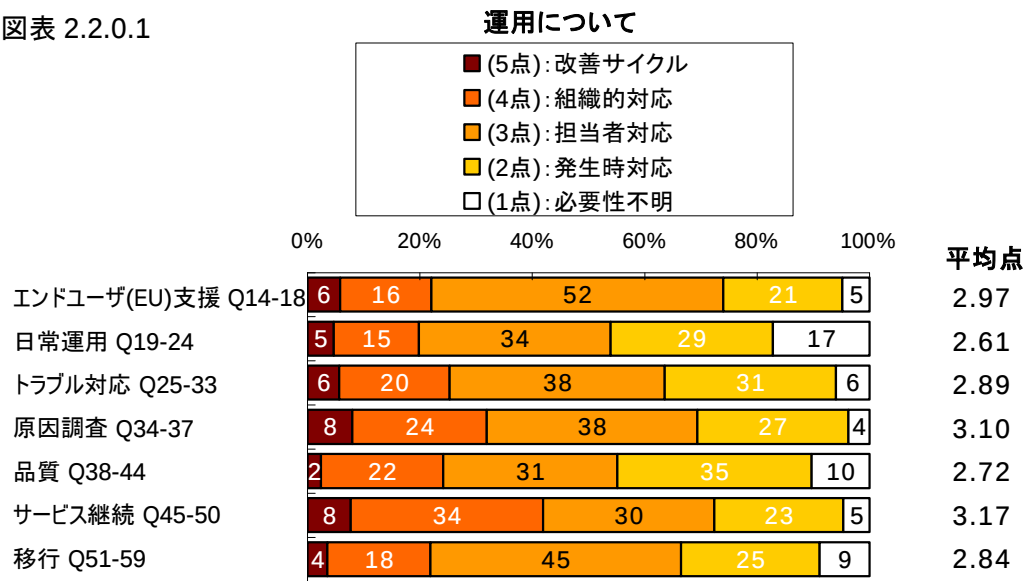
「コンピュータの運用について」では ITIL®[7]の考え方をベースに、
エンドユーザ支援で 5 問、
日常運用で 6 問、
トラブル対応で 9 問、
原因調査で 4 問、
品質で 7 問、
サービス継続で 6 問、
移行で 9 問
の合計 46 問の質問への回答を得ている。質問については ITIL®の項目をより理解しやすい表現に変え、内容も中堅・中小企業に合ったものに見直しを行ったため、全体的には、わかりやすいものになっている。図表中の簡易表現は前節に準じる。→セキュリティと同様の書き方に変更

全体の傾向をみると組織的対応を行っている企業は 20%～40%に過ぎず、非常に低い割合となっている。一方、担当者対応を合わせると 60%前後となり、運用は担当にまかせっきりで、運用担当が苦労している姿が見て取れる。

サービス継続への組織的対応までの比率が中でも高くなっているが、その中身を見てみると、災害への対応（Q45）とバックアップに対する対応（Q48）であり、自然災害・停電などシステム全体に与える影響の大きいものに対しての備えについては、比較的にしっかりとした対策を採っていることがわかる。

運用についてはこれまで、きっちりとしたルールの無い中で、運用担当者が 1 人ないし数人で全社の IT システムの多種多様な要求に対応してきたのが現状であろう。今後は「日本版 SOX 法」などによる法規制が強まる中で内部統制への対応など、ルールを明確化し運用していくことが、企業の信頼度を高め、関連企業との取引を継続していくためのキーとなってくると考えられる。

図表 2.2.0.1



[7] : ITIL®(IT Infurastructure Library)は、英国、欧州連合各国、および米国における英国政府 OGC(Office of Government Commerce)の登録商標であり、共同体商標である。ITIL®は 1980 年後半に OGC が作成した書籍集であり、実際の IT 運用において既に成果をあげた実例、知識が集約されている。昨年発行された Version 3 が最新版である。

2.3 セキュリティについて

セキュリティに関しては、まず大きくインターネットに接続している企業と、接続していない企業について、質問を行っている。結果的にはインターネットに接続していない企業は 160 社中 2 社となっており、中堅・中小の 98%強の企業がインターネットに接続していることがわかる。セキュリティの観点ではインターネットに接続していない場合もそれなりのリスクがあり、対応を行う必要があるのは言うまでもない。

インターネットに接続している企業への質問は、

インターネットからの脅威に関するものが 8 問
セキュリティ管理に関するものが 14 問
物理対策に関わるものが 5 問
人材と組織に関するものが 4 問
全体の質問のうち内部統制に係わるセキュリティ対策の質問が内数として 7 問

となっている。(以降の分析では、インターネット接続無の場合の分析は省略している。)
なお、図表の簡易的表現は次のような内容を意味している。

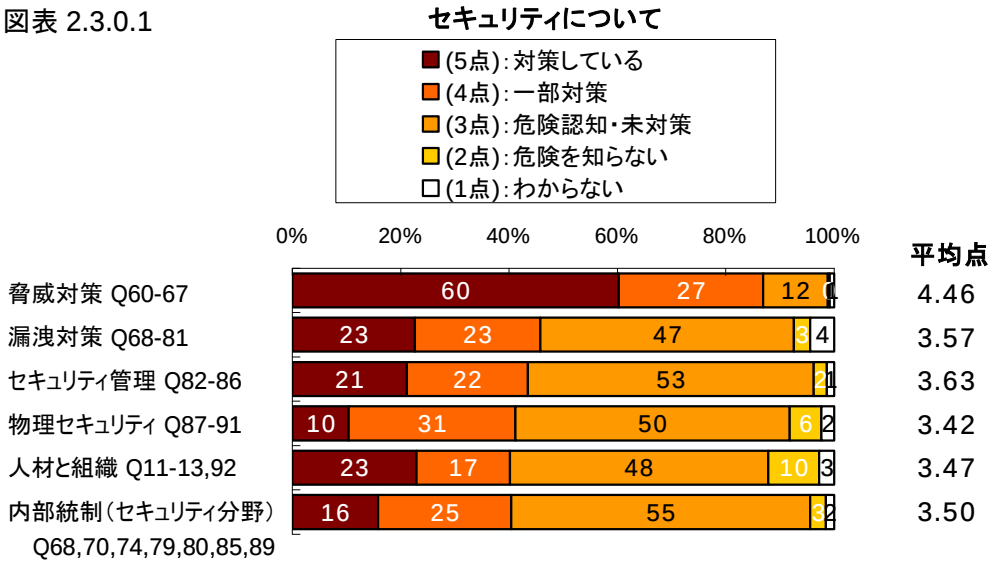
対策している	：対策を実施している
一部対策	：部分的ではあるが、対策を実施している
危険認知・未対策	：危険は知っているが対応していない
危険を知らない	：危険・必要性・サービスなどがあることを知らない
わからない	：実施しているかどうか、または質問の内容がわからない

全体の傾向を見ると、脅威への対策が他に比べ突出して割合が高い。これはウィルスやスパイウェアの脅威がマスコミでも取り上げられ一般に浸透している現れと考えられる。一方、他の対策については一部対応している企業も含めて 40%程度であり、危険はわかっているものの対応していない企業が大半を占めている。

今後はよりバランスのとれた対策を早めに打つ必要があるのは明らかであり、阻害要因を取り除き対策の採れる環境を早急に作っていく必要がある。阻害要因としては昨年までの調査でも明らかになってきているが、ひとつには投資対効果の測定方法が不明確であること、もうひとつはメニューの分かり難さであり、前者は多少保険的な要素も加わることを経営側が理解して対策を進められるか、後者は情報システム管理者が、経営者に対して説明しやすい資料を作れるかに依存していると思われる。

いずれにしても経営者・情報システム管理者双方が理解しやすい説明書が必要であり、今回リリースした当協会作成の「必要なセキュリティ対策がわかる本」は、この点を埋めるひとつの道具として使えると考えている。

図表 2.3.0.1



セキュリティ対策で内部統制に係わるものは主としてアクセス管理である。インターネット経由の企業内外からのアクセスの履歴管理、企業内の PC やプリンタから漏洩する可能性のあるデータの管理、重要なデータを保管するサーバ室への物理的アクセスの管理などがそれにあたる。セキュリティ関連のアクセス管理は、内部統制のなかの IT 全般統制の一部分として位置づけられており、内部統制への対応を行うためには、アクセス管理のみならず、より広い範囲の対策を行う必要がある。

本報告書の中では、その部分について「内部統制（セキュリティ分野)」という表現で表現されているが、その傾向は脅威対策を除く他のセキュリティ対策と同様の傾向を示している。これは、内部統制面からみたセキュリティについても、その対策は不十分であり今後、この面からも強化を必要としていることがうかがわれる。

3　調査と分析

3 調査と分析

情報通信を巡る状況は、インターネットの急速な普及、光ファイバなどによるブロードバンド化、携帯電話に代表されるモバイル化、放送のデジタル化と劇的に進展してきた。現在、ブロードバンドネットワークなど、IT を利用するためのインフラ整備が進み個人、企業内、企業間と活用の幅が広がりを見せている。今回の調査でも、インターネットには接続していない企業は、調査 160 社中 2 社であり、インターネットは、中堅・中小企業での共通のインフラとして、定着しているようである。

一方、この進展の阻害要因として、ウィルス感染、情報漏洩、外部からの不正アクセス、情報書き換えと各種リスクも増大している。法的な側面からも、個人情報保護法、新会社法、日本版 SOX 法など、健全な企業のあり方、健全な財務会計の義務づけ、人権尊重と守るべき課題は多い。

今回、システム開発、導入後の情報システムの運用とセキュリティに関して、アンケートを実施した。経営者の観点から情報システム全般、セキュリティの考え方、投資も含めた推進方法について、また情報システム管理者に、具体的な日常管理について回答を得た。アンケートの参考資料として、「企業経営者の方々にご配慮いただきたい課題」「経営者が理解できる運用やセキュリティの世の中の標準化状況」（付録　参照）を現状認識用として添付した。

サポートサービス委員会では、アンケートの分析・診断ツールを作成し、各種分析を行なうと共に、必要な企業には、「情報システム　運用・セキュリティ　状況分析診断結果」を提供した。

3.1 回答企業のプロフィール

この節では、「IT 業界のサポートサービスに関するアンケートのお願い」で企業から付加情報として以下の 9 つの項目について、回答を得た。

F1. 企業名（任意）
F2. 所在地（任意）
F3. 業種
F4. 資本金と年商
F5. 従業員数（パート・アルバイト含む）
F6. 従業員の年齢構成
F7. 情報システムの担当者数（専任、兼任）と PC 台数
F8. 情報システム投資額（対売上高比）
F9. 状況分析結果の提供の可否

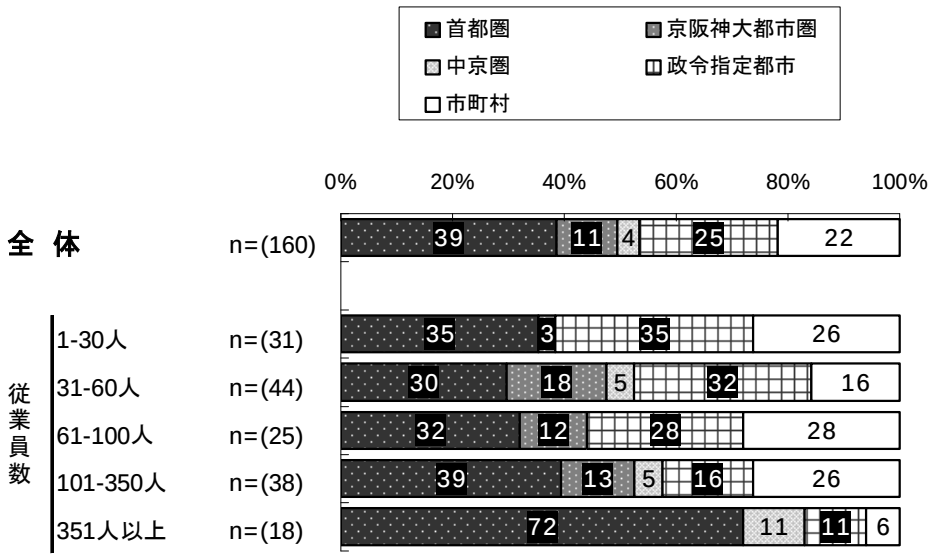
今回の調査の全体イメージ理解のために、回答企業の概要と、中堅・中小企業の IT 投資という観点から、情報システムに対する投資額（売上高比）と IT 投資の主要構成要素である、情報システム担当者数とパソコンの台数の状況について述べる。

3.1.1 従業員規模

(1) 地域別分布

「全体」の 39%、従業員数「351 人以上」では 72%が『首都圏』である。

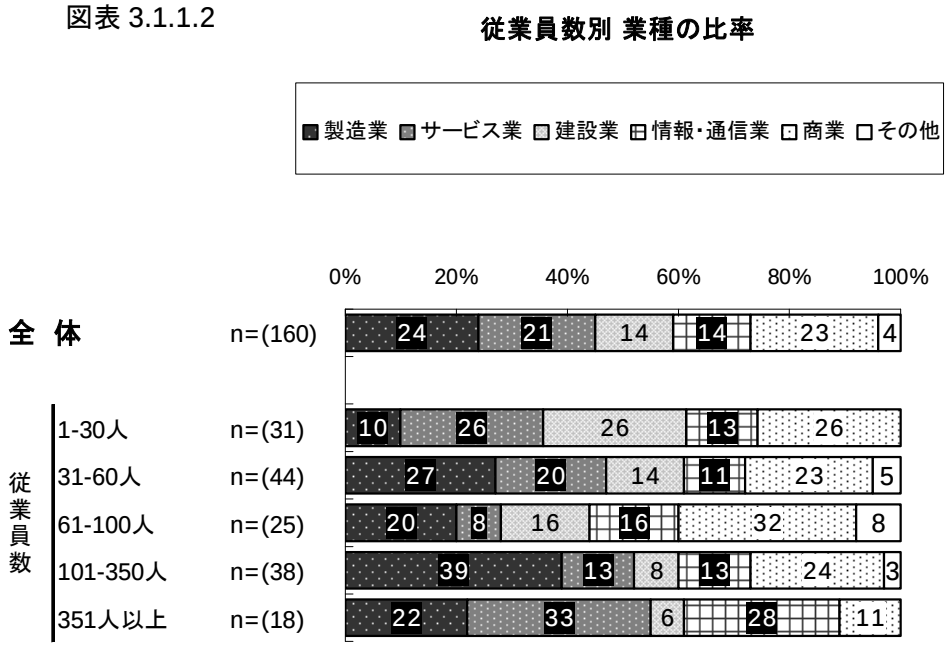
図表 3.1.1.1 **従業員数別 地域の比率**



(2) 業種別分布

各業種に平均的にばらついている、今回の調査では、特に従業員数「1-30 人」は『製造業』の割合が低い。

図表 3.1.1.2

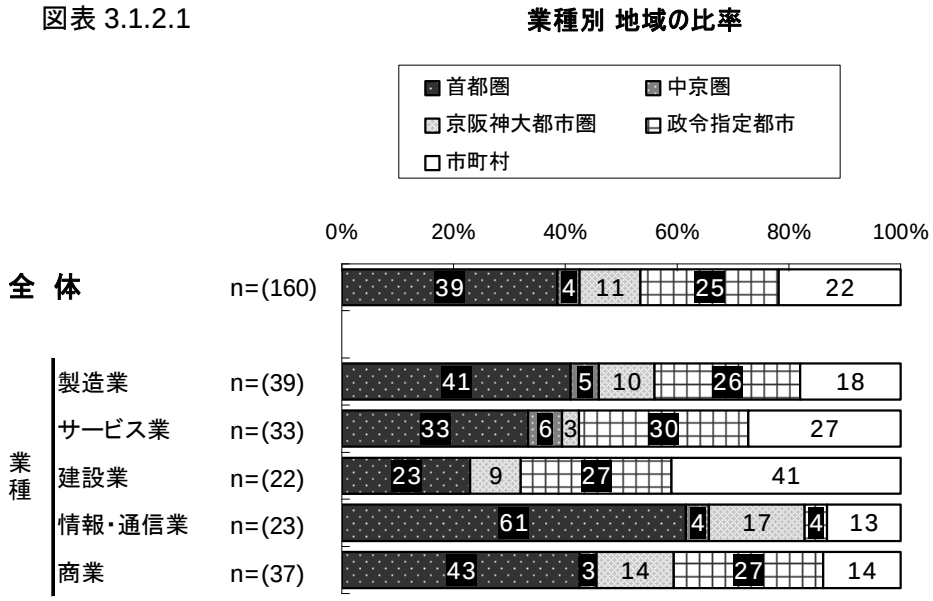


3.1.2 業種

(1) 地域別分布

「情報・通信業」の 61%が『首都圏』、「建設業」は『市町村』が 41%と割合が高い。

図表 3.1.2.1

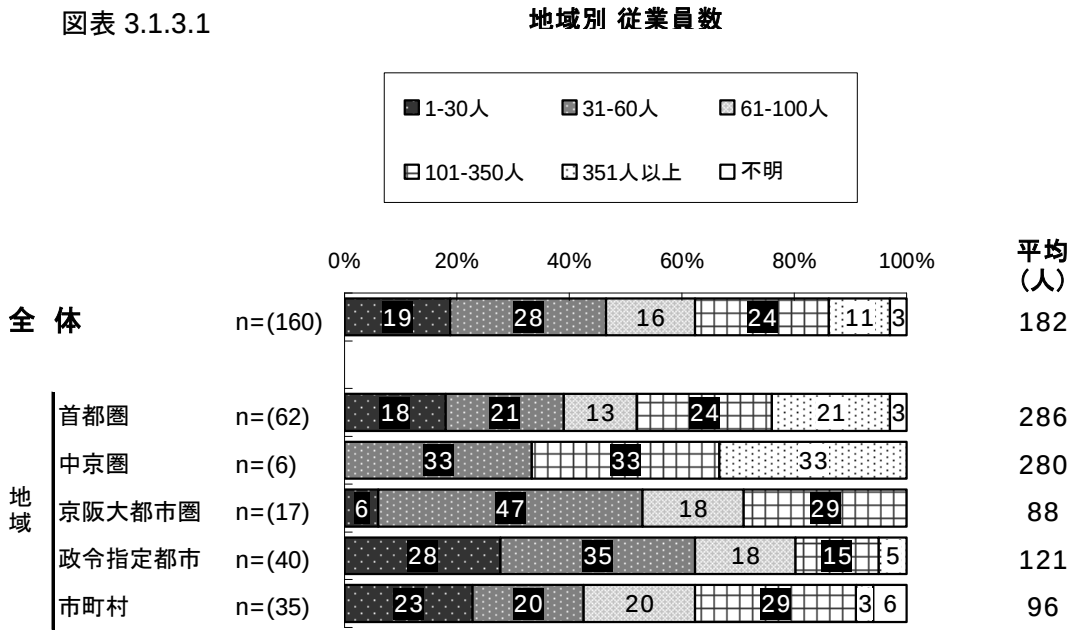


3.1.3 地域

(1) 従業員規模別分布

従業員数「60 人未満」は、「政令指定都市」が 63% 「中京圏」が 53%と割合が高い。

図表 3.1.3.1

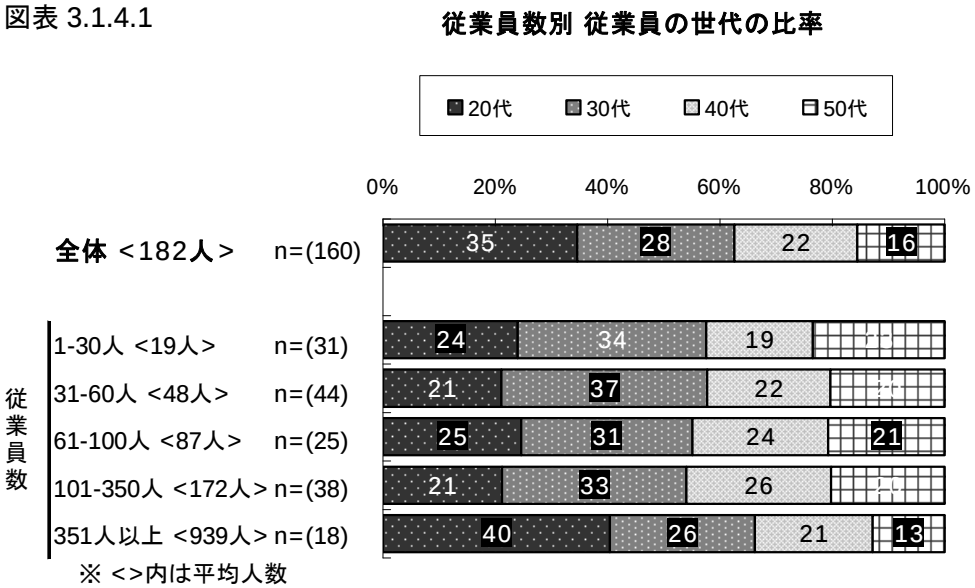


3.1.4 世代ごとの比率

(1) 従業員規模別分布

全体の 63%が『30 代』以下、従業員数「351 人以上」は 66%が 30 代以下、『50 代』は全体の 16%占めている、従業員数「1～30 人」は 23%と高めである。

図表 3.1.4.1

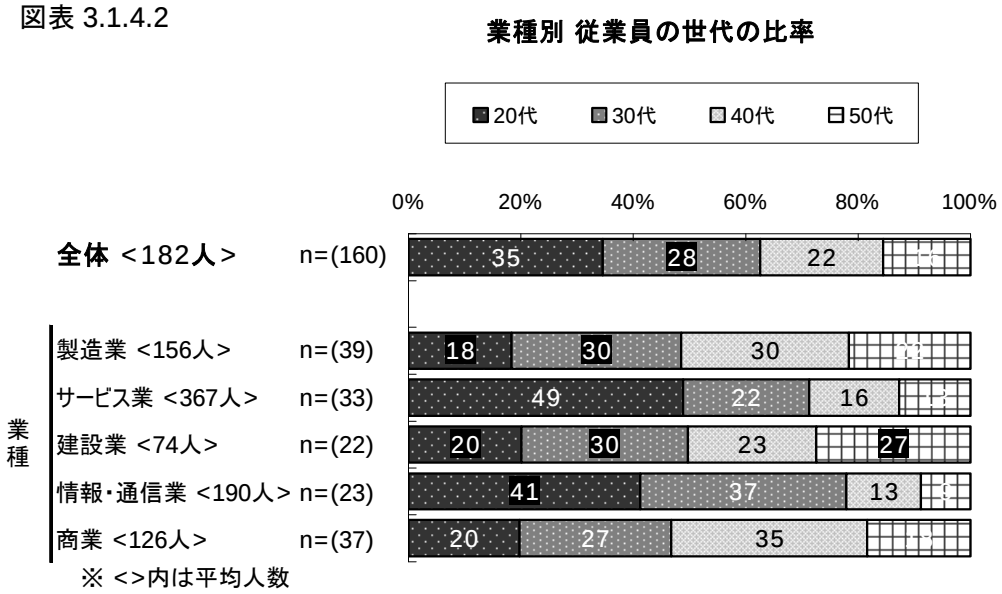


※ <>内は平均人数

(2) 業種別分布

「サービス業」、「情報・通信業」が 70%～78%が『30 代』以下であり逆に、「製造業」、「商業は」、30 代以下は 50%以下である。

図表 3.1.4.2



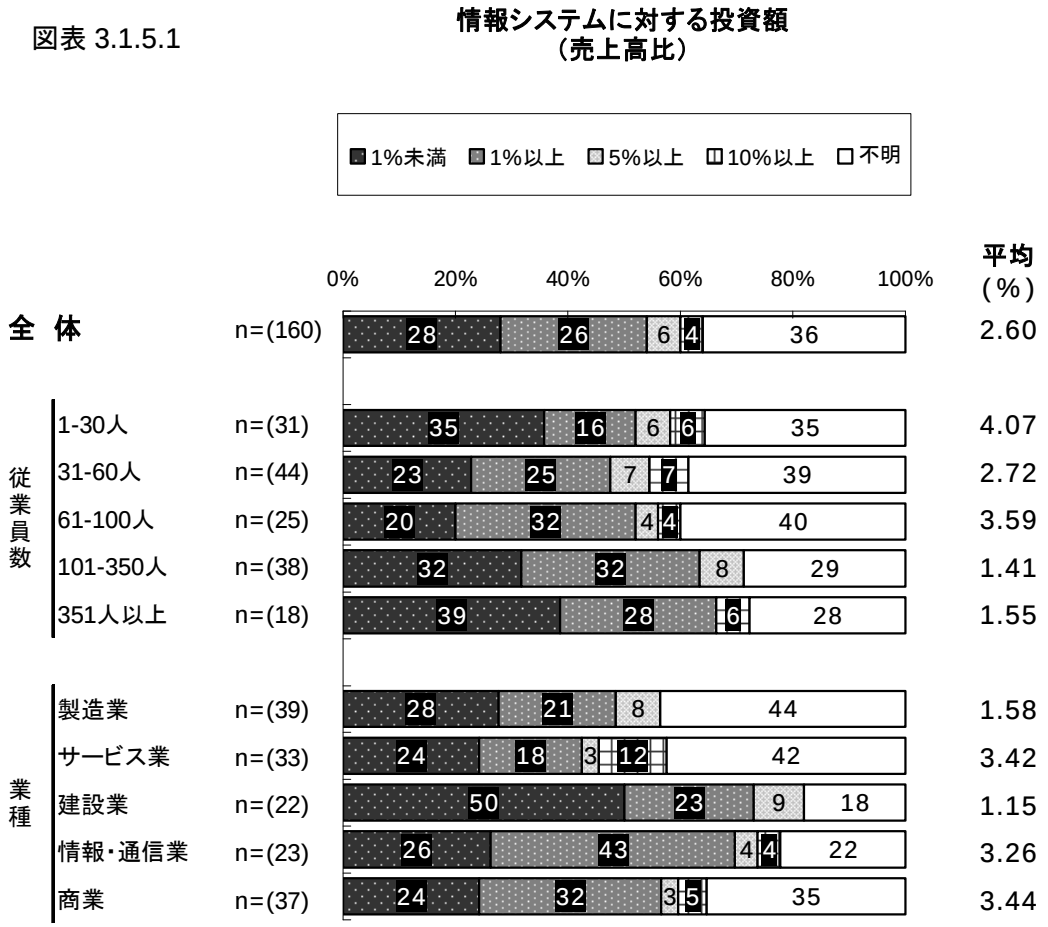
※ <>内は平均人数

3.1.5 情報システムに対する投資額

今回の調査 160 社は、従業員数にかかわらず、約 50%の企業が「5%未満」、一方、「5%以上」の投資を行なっている企業が、全体の 10%程度存在している。

業種別に見ると、全業種とも過半数が「5%未満」、「建設業」の約 50%が「1%未満」で他業種に比して若干低い、また、「サービス業」の約 10%の企業が「10%以上」投資している。単年度の特異な事情と考えられるが、継続した調査が必要であろう。

図表 3.1.5.1



3.1.6 情報システムの担当者数

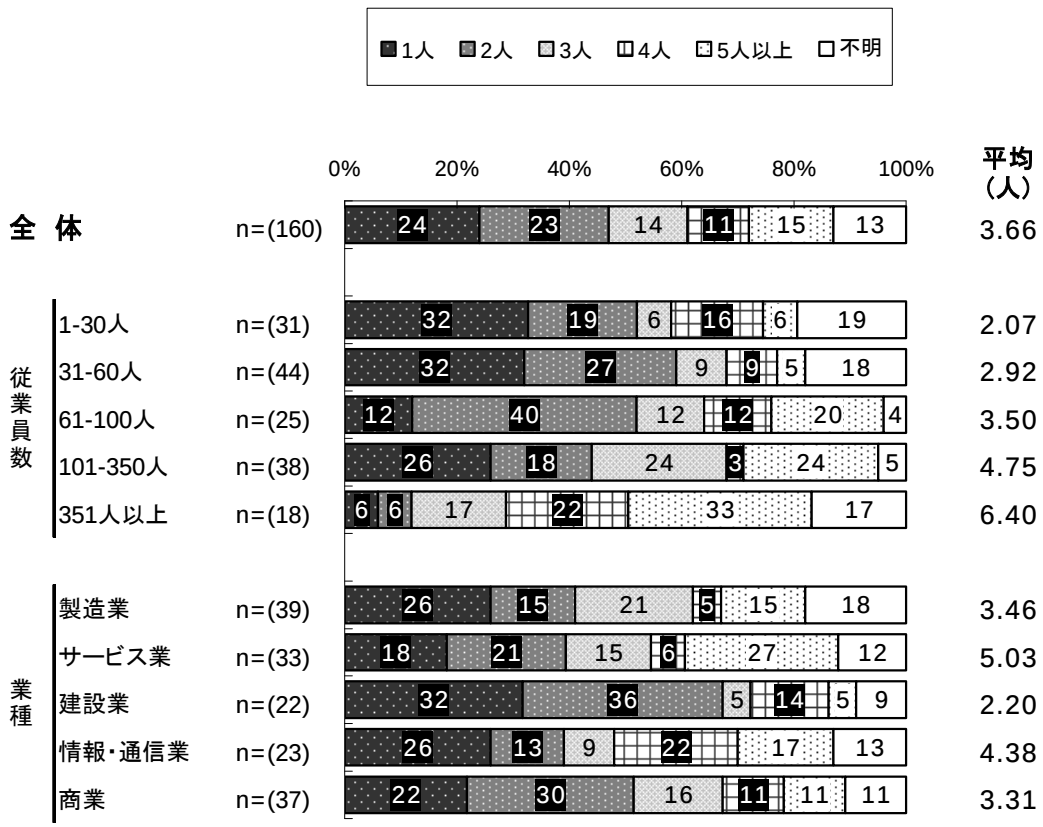
(1) 情報システム担当者（専任・兼任）

担当者は、全体平均は，約 3.7 名、従業員数「60 名以下」の企業の過半数が、兼務者を含めると規模・業種にかかわらず、2～3 名程度の担当を設置、規模の増加に比例して担当者数も増加している。

業種では、「建設業」が若干低く、従業員も少ないため約 2 名である、これをを除くと大きな差異ない。

規模にかかわらず、IT 化～運用維持のための担当者は、必須と考えられる。

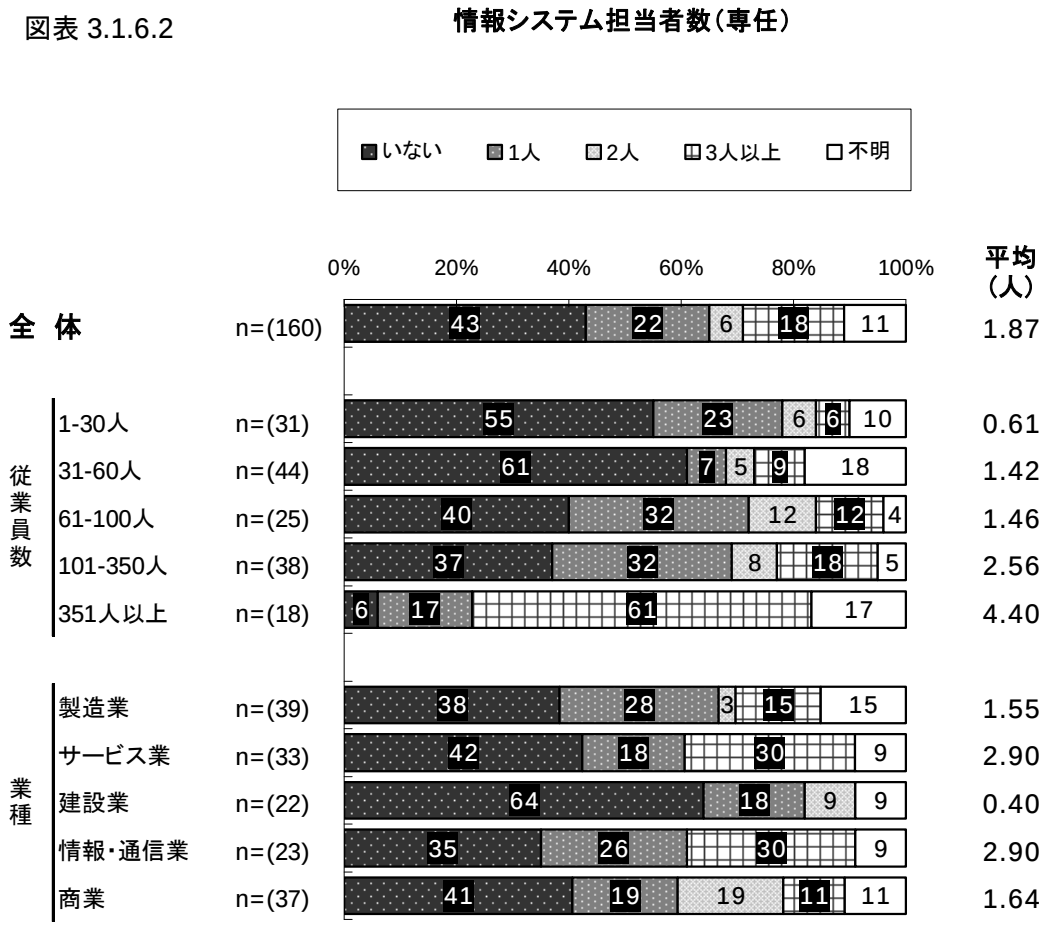
図表 3.1.6.1　　情報システム担当者数（専任・兼任）



(2)情報システムの担当者数（専任）

専任者を置いているか、どうかで見ると全体の 43%が 0 人、従業員数「60 人以下」の 60%が「建設業」の 60%が専任担当者を置いていない。

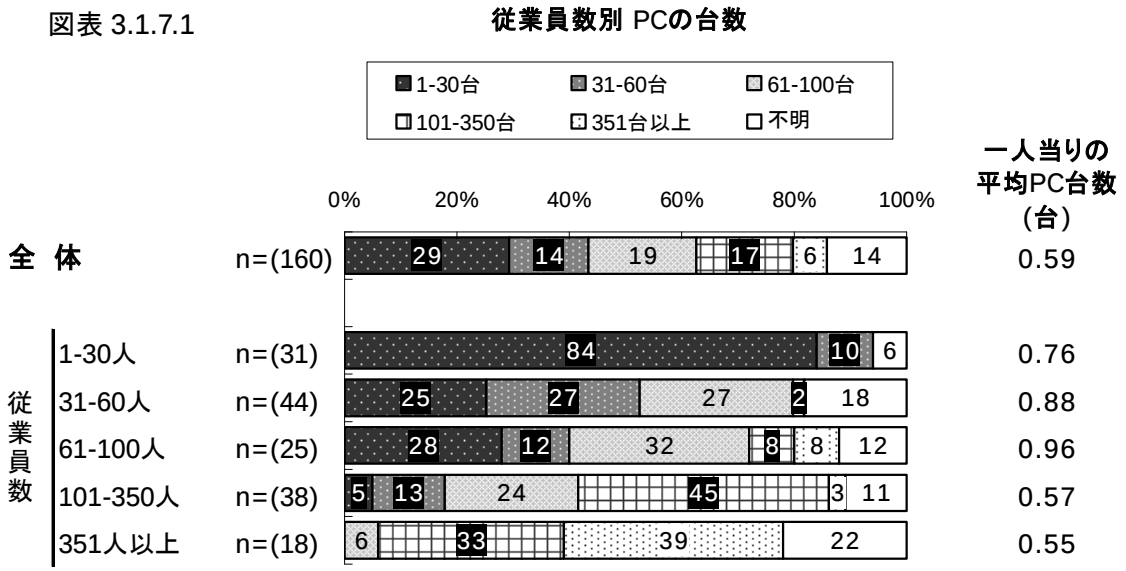
図表 3.1.6.2



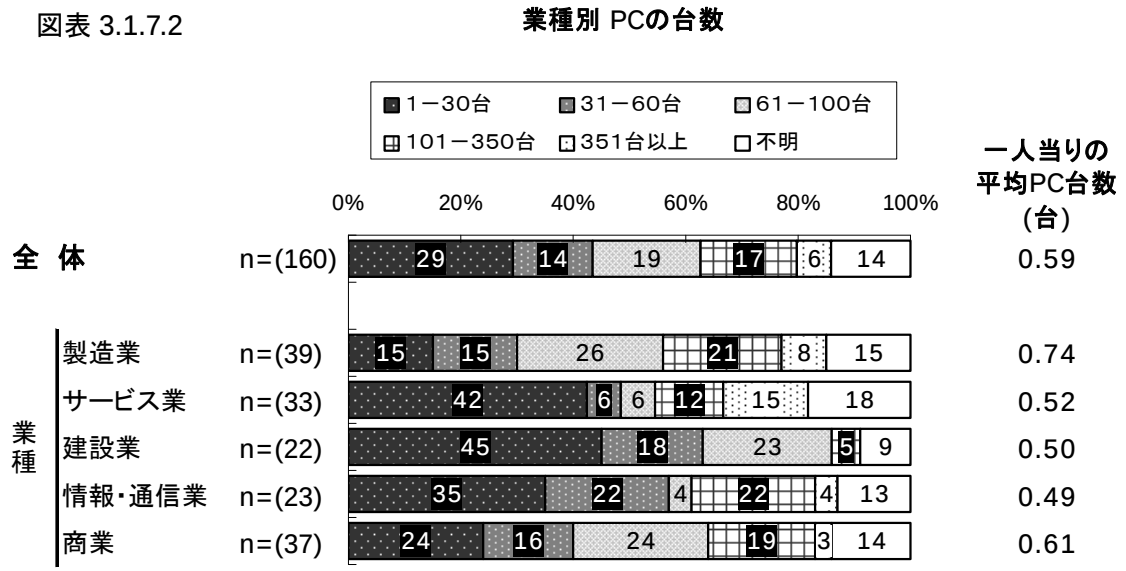
3.1.7 PC の台数

従業員数に PC 台数は比例している。平均的に 1～2 名に 1 台の配備を行なっている、IT 化のツールとして PC は定着していると考えられる。

図表 3.1.7.1



図表 3.1.7.2



3.2 経営者の情報システムに関する認識（4.3 節～4.6 節　参照）

この節では、戦略に関する質問を 4 個、事業継続に関する質問を 3 個、内部統制に関する質問を 2 個、情報管理に関する質問を 4 個の全部で 13 個の質問に対する回答を報告、分析している。

① 戦略（Q1～4）
情報システムの経営への効果をどの程度重要視しているかを知るための質問である。

② 事業継続 (Q5～7)
情報システムの安定稼動をどの程度重要視しているかを知るための質問である。

③ 内部統制 (Q8～9)
内部統制（運用分野）に関する質問は、内部統制の対象として、情報システムをどの程度重要視しているかを知るための質問である。

④ 情報管理 (Q10～13)
情報管理に関する質問は、情報システムが抱える企業に対する脅威をどの程度重要視しているかを知るための質問である。

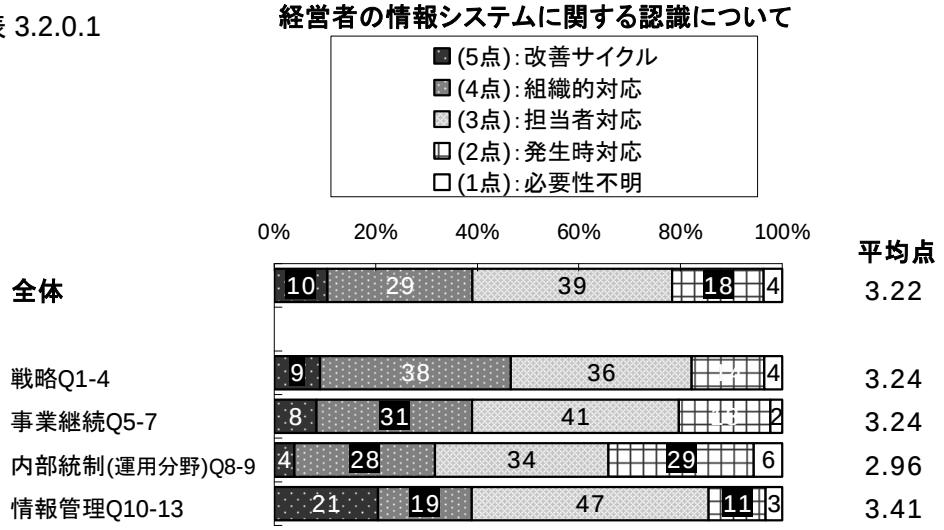
これらの質問に対する回答の選択肢の概略は、下記のとおりである。

5 点：改善サイクルを含め、組織的に対応している（便宜的に『改善サイクル』と表記）
4 点：組織的に対応している（『組織的対応』と表記）
3 点：担当者を決め、一任している（『担当者対応』と表記）
2 点：発生時対応（把握／検討／対策／指示していないなど）（『発生時対応』と表記）
1 点：必要性を認めない／わからない（『必要性不明』と表記）

これらの選択肢から容易に推測されるように、重要視の程度は全社的・組織的に取組む姿勢に現れるという考え方に立脚して、選択肢を設定している。
すなわち、「5 点・4 点であれば重要視している」、「2 点・1 点であれば重要性を認識していない」、「3 点であれば重要性を認識してはいるが本格的な対応の域に至っていない」という意味である。

各質問に対する回答の分布とその特徴については後述するが、戦略、事業継続、内部統制および情報管理の 4 領域の回答分布と平均点（上記の選択肢を点数として平均値を算出）は、下記のとおりであった。

図表 3.2.0.1



この結果から、一般論としては、次のように考えられる。

＊ 約 80%の経営者は、事業遂行の中での情報システムの重要性を相当程度（3 点以上）に認識している。

＊ しかし、領域別に見ると、戦略と事業継続の領域に関しては約 20%、内部統制の領域に関しては約 35%、情報管理の領域に関しては約 15%の経営者が、事業遂行の中での情報システムの重要性を認識していない（2 点以下）。

＊ また、認識している経営者でも、その認識に立って率先垂範し、社内を組織的に指導するまでに至っている割合は 1/2 程度である。

＊ とくに、経営者の認識は、情報管理のような目先の現実的な課題に対するよりも、内部統制のような将来を展望しての課題に対する重要性の認識が低い。

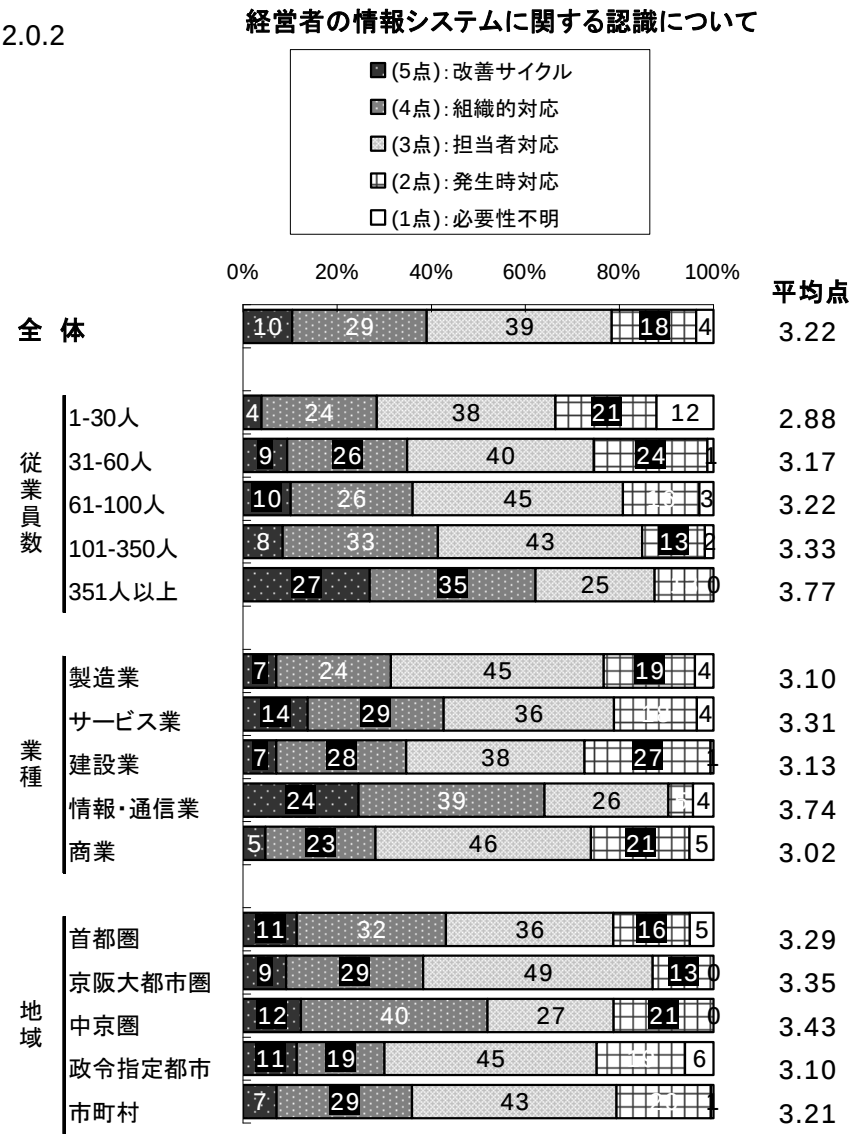
「企業経営者の方々にご配慮いただきたい課題」（本書付録参照）の中で、「IT システムの経営上の効果を高めるために、経営者は IT システムの運用に強い関心を持っていただく必要がある」と訴えているが、これらのデータによれば、この訴えはところを得ているといえよう。

それでは経営者はどうすればよいのか。ここで強調したいのは、担当者を決め一任するだけではなく担当者に一歩近づいて、担当者が抱えている苦労している課題の解決を支援することが、組織的な対応にまで状況を好転することになり、情報システムの経営上の効果を高めることになる。

一方、担当者はどうすればよいのか。一任されて、その範囲に甘んずることなく、経営者に対して組織的な対応への提案を積極的に行うべきである。そのためには、いろいろな機会を捉えて、同業者をはじめとする一般市場の有用な情報を収集しておく必要がある。

このデータを従業員数別、業種別、地域別に整理したものが下表である。

図表 3.2.0.2



＊　従業員数別に見ると、「1～30 人」と「351 人以上」を除くと平均点には大差がない。強いていえば、企業規模が大きくなるほど、情報システムを重要視している。

＊　業種別に見ると、「情報・通信業」の平均点が高い。60%以上が『組織的対応』(『改善サイクル』を含む）をしているが、これは当然といえば当然と考えられる。

＊　地域別に見ると、大差があるとはいえないが、大都市圏は平均点が高い。

事業遂行の中で情報システムが果たしている役割を経営者がどの程度重要視し、どのような対応をしているかについて、一般的な傾向を知ることができる。

以下に領域ごとに回答の集計結果を分析しているので、参考にされたい。

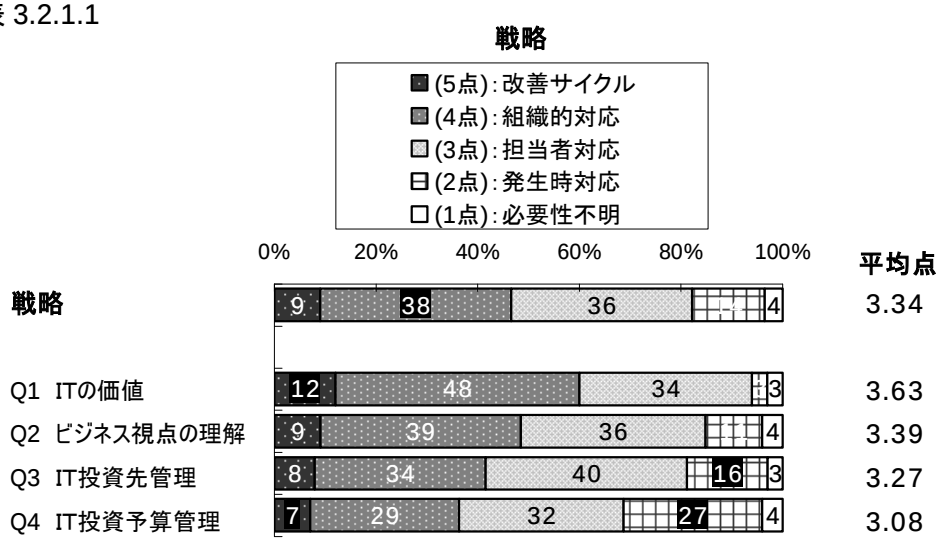
3.2.1 戦略の領域に関する認識(4.3 節　参照)

戦略の領域については、情報システムの経営への効果をどの程度重要視しているか、下記の 4 個の質問をしている。

Q1：情報システムが貴社のビジネスにもたらす価値を把握していますか。　　（IT の価値）
Q2：IT 部門にビジネス戦略や戦術について説明し、情報システムに反映させていますか。
（ビジネス視点の理解）
Q3：自社の IT 投資額とその振り向け先（新規設備、新規アプリ開発、保守・運用費用など）を明確にし、その経営効果を把握されていますか。　　(IT 投資先管理)
Q4：予算決定時に IT 設備／アプリケーションなどの新規投資以外に保守・運用に対する投資評価を行っていますか。　　(IT 投資予算管理)

質問ごとの回答の分布は下表のとおりである。

図表 3.2.1.1



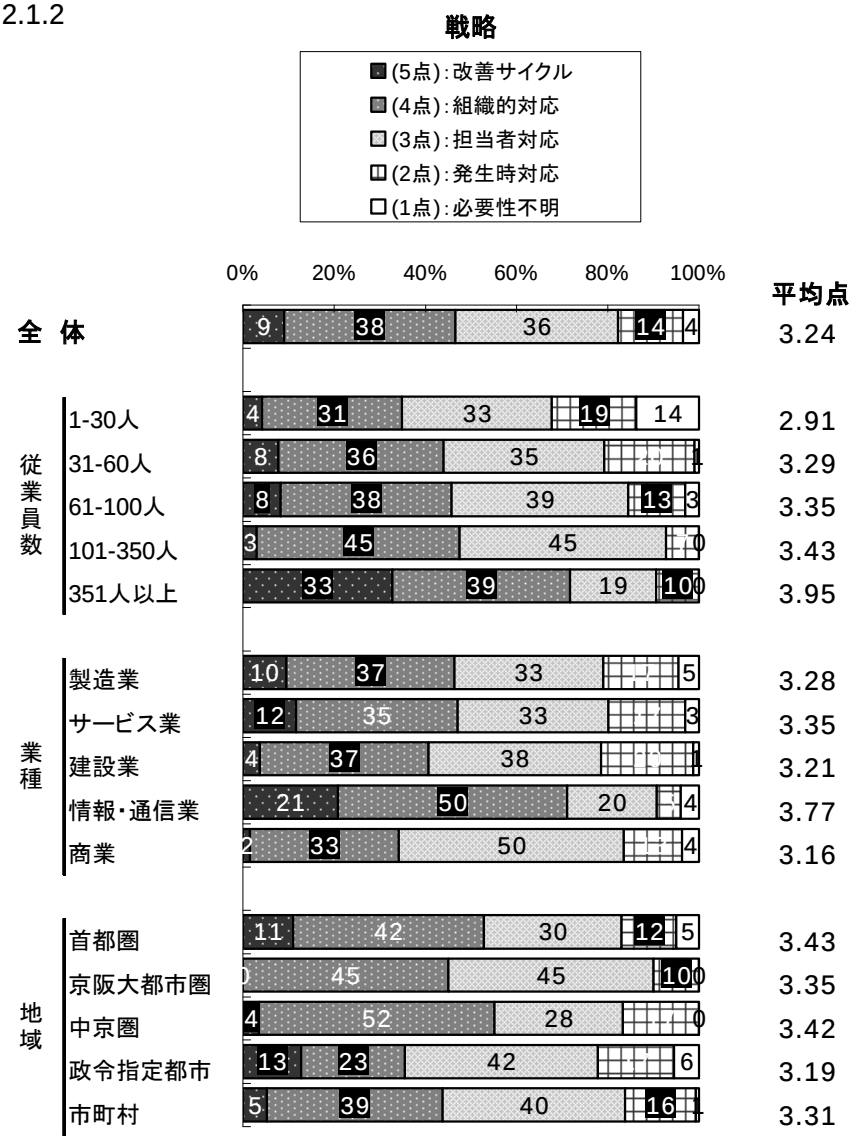
＊　情報システムの経営への効果についての経営者の認識は、IT 投資のような目先の現実的な課題に対する認識よりも、地味な保守・運用の課題に対する認識の方が低いことがうかがわれる。

＊　情報システムの保守・運用への対応は、課題に関係する者の拡がりと課題の時間的な永続性の点から対応に極めて根気が必要であるので、それを担保する組織的対応が求められる。

＊　今回のアンケート調査の目的である保守・運用に対する経営者の認識の程度を上げていきたいという意図は、この質問への回答を見れば、間違っていなかったと考えられる。

戦略の領域についての 4 個の質問に対する回答を合計したものを従業員数別、業種別、地域別に整理したものが下表である。

図表 3.2.1.2



＊ 80%以上の経営者は、情報システムの経営への効果を重要視している。しかし、重要視している経営者のうちの 1/2 程度は、社内を組織的に指導するまでには至っていない。

＊ 従業員数別に見ると、「1～30 人」と「351 人以上」を除くと、平均点には大差がない。強いていえば、企業規模が大きくなるほど、情報システムの経営への効果を重要視している。

＊ 業種別に見ると、「情報・通信業」の平均点が高いが、その他の業種の平均点に大差はない。

＊ 地域別に見ると、大差があるとはいえないが、大都市圏の平均点が高い。

4 章で、すべてのアンケート質問ごとに、企業規模別、業種別、地域別、年商別の視点で、回答の集計結果を分析しているので、参考にしていただきたい。

3.2.2 事業継続の領域に関する認識(4.4 節　参照)

事業継続の領域については、情報システムの安定稼動をどの程度重要視しているか、下記の 3 個の質問をしている。

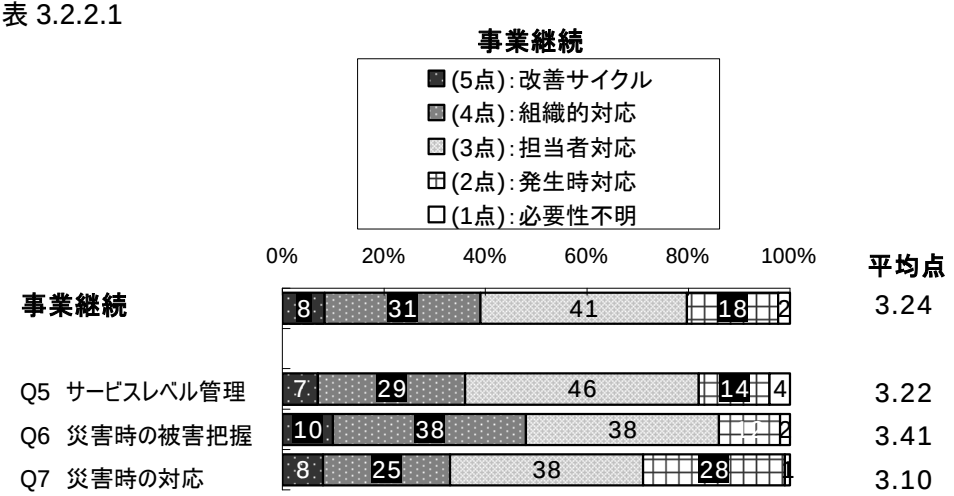
Q5:自社システムの運用に当たって自社内､サービスベンダー委託に関わらず明確な目標を設定し、システムの安定稼動を図るべく指導していますか。　　(サービスレベル管理)

Q6:重大な故障などで情報システムが利用できなくなった場合､御社のビジネスにどれほどの被害が生ずるか理解し対応していますか。　　(災害時の被害把握)

Q7:災害時など情報システムが利用できない場合に備えた対策を検討していますか。　　(災害時の対応)

質問ごとの回答の分布は下表のとおりである。

図表 3.2.2.1

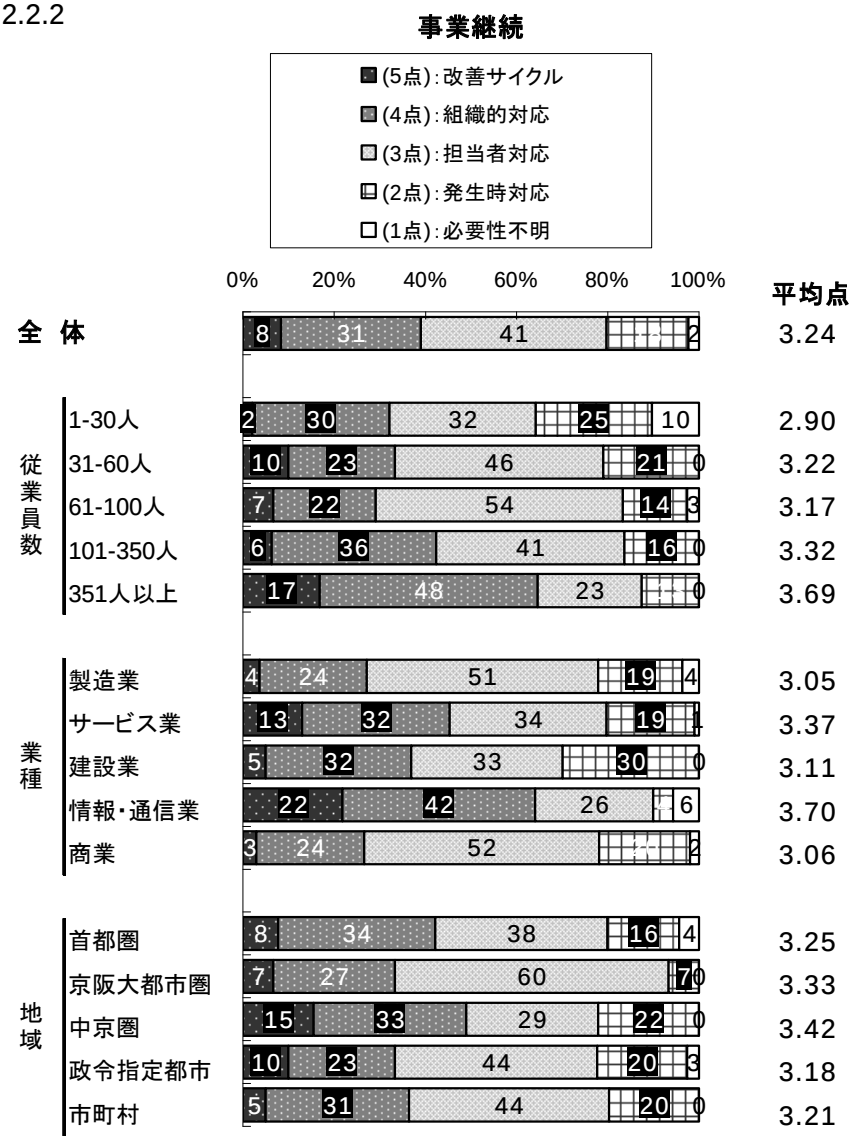


＊　情報システムの安定稼動についての経営者の認識は、ビジネス上の被害のような現実的な課題に対する認識よりも、目標設定や対策検討のような地味な具体的対応に対する認識の方が低いことがうかがわれる。

情報システムの安定稼動は、社内外を問わず関係者が共通認識を持って対応することが必要であるので、経営者の積極的な関与が求められていることを強調しておきたい。

事業継続の領域についての 3 個の質問に対する回答を合計したものを従業員数別、業種別、地域別に整理したものが下表である。

図表 3.2.2.2



＊ 約 80%の経営者は、情報システムの安定稼動を重要視している。しかし、重要視している経営者の約 1/2 は、社内を組織的に指導するまでには至っていない。

＊ 従業員数別に見ると、「1～30 人」と「351 人以上」を除くと平均点には大差がない。強いていえば、企業規模が大きくなるほど、情報システムの安定稼動を重要視している。

＊ 業種別に見ると、「情報・通信業」の平均点が高いが、その他の業種の平均点には大差がない。

＊ 地域別に見ると、大差があるとはいえないが、大都市圏の平均点が高い。

3.2.3 内部統制の領域に関する認識(4.5 節　参照)

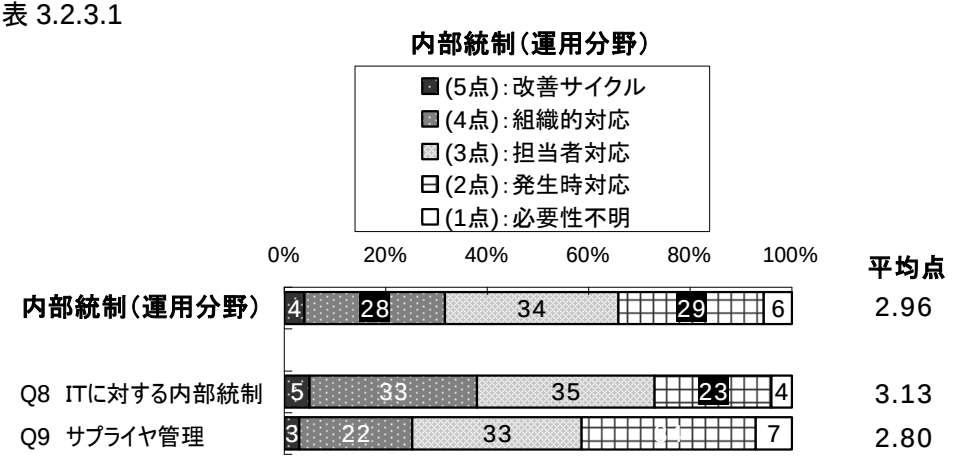
内部統制（運用分野）の領域については、内部統制の対象として情報システムをどの程度重要視しているか、下記の 2 個の質問をしている。

Q8：内部統制の基本的要素に「IT への対応」が含まれていますが、それについて対応を行っていますか。（IT に対する内部統制）

Q9：内部統制を実施している企業の業務委託先にも、内部統制の実施、管理が必要ですが、それについて対策を行っていますか。（サプライヤ管理）

質問ごとの回答の分布は下表のとおりである。

図表 3.2.3.1

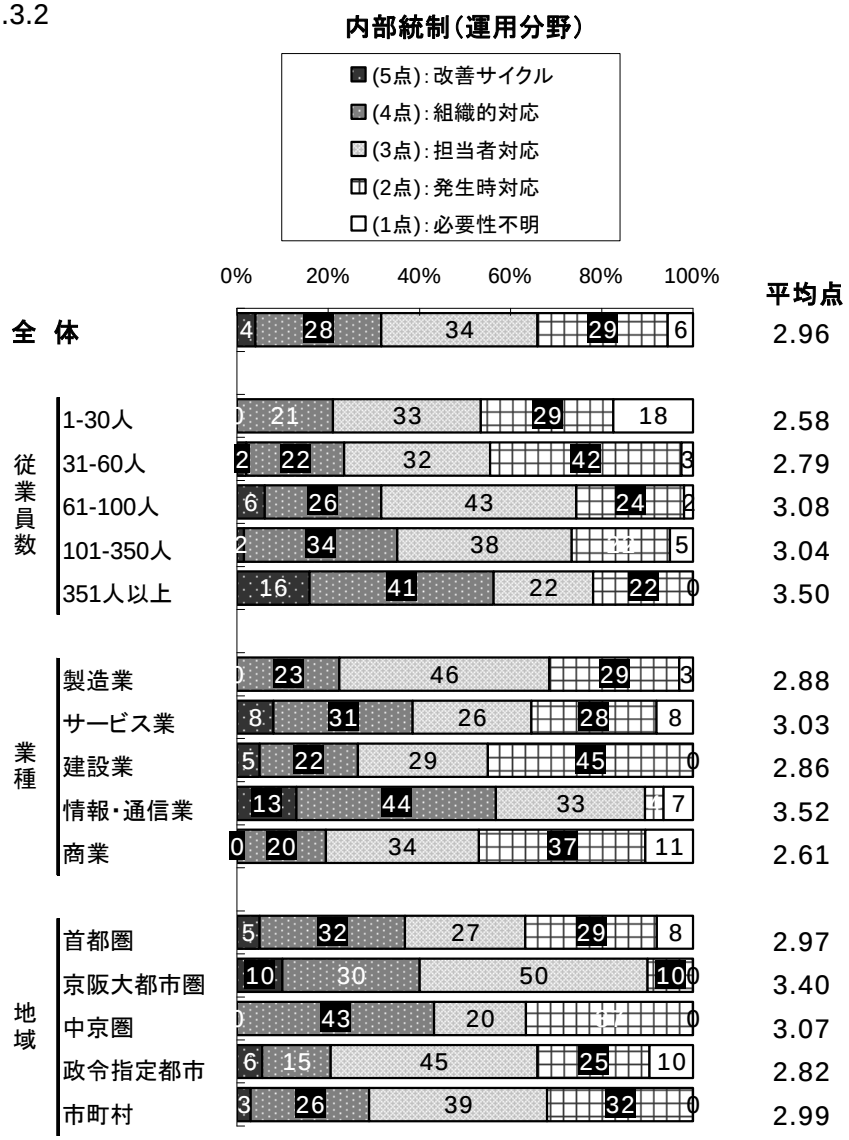


＊　内部統制の対象として情報システムについての経営者の認識は、自社に対するよりも業務委託先に対する認識の方が低いことがうかがわれる。

経営の中で IT が重要な要素となってきている状況において、IT を企業の内部統制の対象として重要視する必要性は高くなってきていることを強調しておきたい。

内部統制の領域についての 2 個の質問に対する回答を合計したものを従業員数別、業種別、地域別に整理したものが下表である。

図表 3.2.3.2



＊ 60～70%の経営者は、内部統制の対象として、情報システムを重要視している。しかし、重要視している経営者の約半分は、社内を組織的に指導するまでには至っていない。

＊ 従業員数別に見ると、「1～30 人」と「351 人以上」を除くと平均点は大差がない。強いていえば、企業規模が大きくなるほど、内部統制の対象としての情報システムを重要視している。

＊ 業種別に見ると、「情報・通信業」の平均点が高いが、その他の業種の平均点に大差はない。また、「建設業」では、約 1/2 が重要視していない。

＊ 地域別に見ると、「京阪神大都市圏」では 90%が重要視しており、平均点が他の地域と比べて際立って高い。

3.2.4 情報管理の領域に関する認識(4.6 節 参照)

情報管理の領域について、情報システムが抱える企業に対する脅威をどの程度重要視しているか、下記の 4 個の質問をしている。

Q10：情報漏洩が企業経営及び経営者に対して重大な問題を引き起こすことを意識して、しかるべき組織・技術対応をしていますか。 (セキュリティ管理)

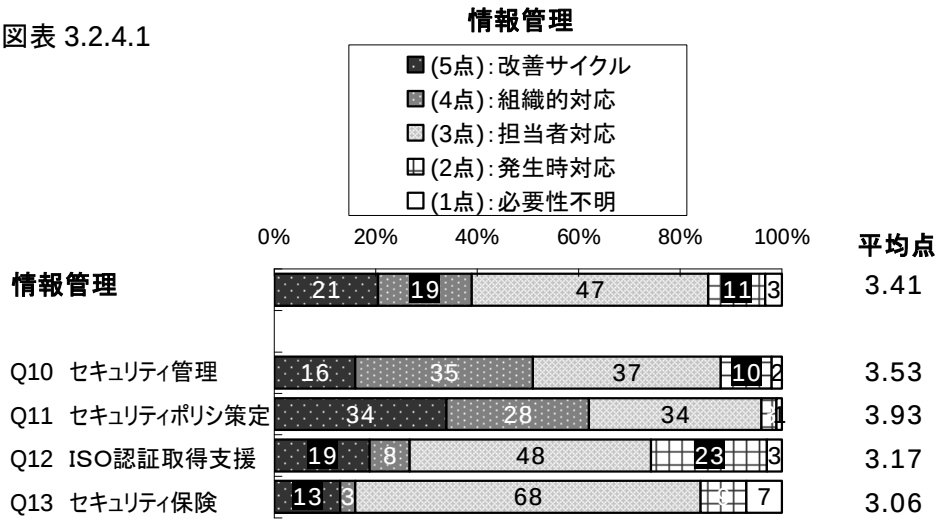
Q11：会社としてのセキュリティ方針を示すことは、従業員の意識向上に大きく役に立ちます。従業員へ徹底すべき、会社としてのセキュリティ方針を持っていますか。 (セキュリティポリシ策定)

Q12：情報セキュリティの基準として ISMS 認証があり、認証を取得することが企業の信用をより確実にする場合があります。認証の取得が必要ですか。 (ISO 認証取得支援)

Q13：万が一のセキュリティ事故に備え、何かしらの対策を施していますか。セキュリティに関する保険があることを知っていますか。 (セキュリティ保険)

質問ごとの回答の分布は下表のとおりである。

図表 3.2.4.1



＊ 情報漏洩など情報システムが抱える企業に対する脅威については、約 90%の企業で経営者に認識されている。

＊ セキュリティ方針に関しては、ほぼすべての企業で認識されているが、約 1/3 が『担当者対応』であり、『組織的対応』に至っていない。

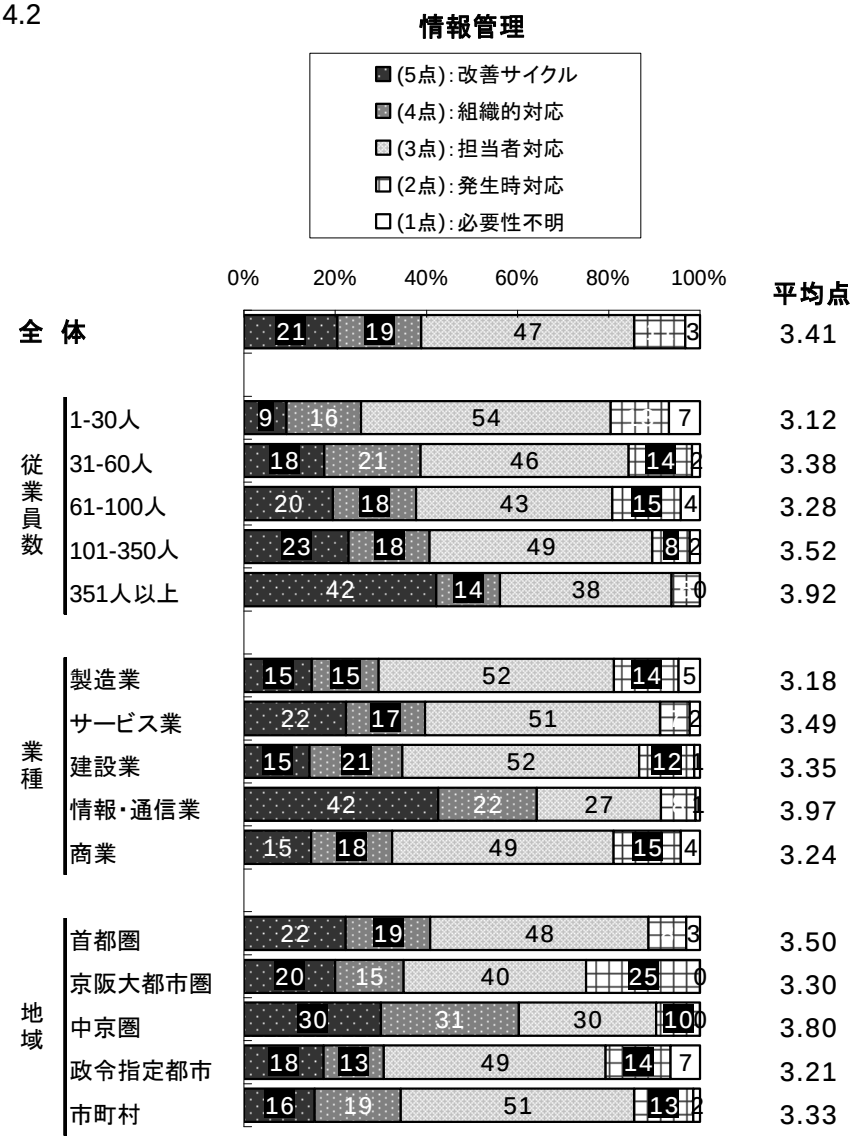
＊ 『組織的対応』が必要な ISO 認証取得に対しては、約 1/4 が認識しておらず、約 1/2 が『担当者対応』である。

＊ また、セキュリティ保険に関しては、80%以上で『組織的対応』がなされていない。

情報管理を消極的な対策とせずに、経営にとって積極的な効果をもたらす対策として考える必要があることを強調しておきたい。

情報管理の領域についての 4 個の質問に対する回答を合計したものを従業員数別、業種別、地域別に整理したものが下表である。

図表 3.2.4.2



＊ 90%以上の経営者は、情報システムが抱える企業に対する脅威を重要視している。しかし、重要視している経営者の約 1/2 は、社内を組織的に指導するまでには至っていない。

＊ 従業員数別に見ると、「1～30 人」と「351 人以上」を除くと平均点には大差がない。強いていえば、企業規模が大きくなるほど、情報システムが抱える企業に対する脅威を重要視している。

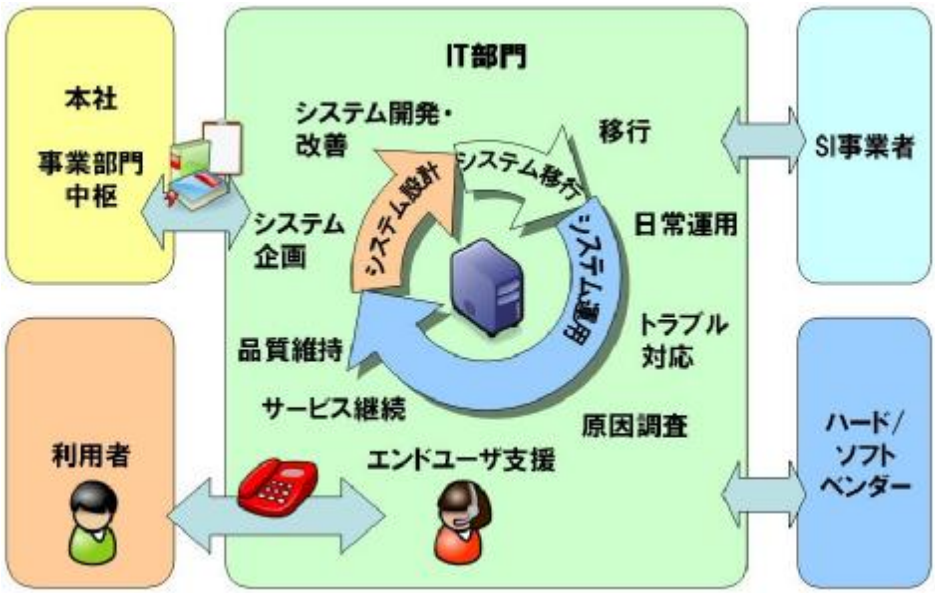
＊ 業種別に見ると、「情報・通信業」の平均点が高い。その他の業種の平均点に大差はない。

＊ 地域別に見ると、「中京圏」の平均点が他の地域と比べて際立って高いが、他の地域の平均点に大差がない。

3.3 運用について

IT システムの導入においては、ビジネス要件を IT システム化し、IT サービスを開始するまでの「システム設計」に目が行きがちである。しかし、「構築半年、運用 10 年」、「IT 投資に占める運用費用の割合は 60%以上」などと言われるように、IT サービスの有効性は、その後のシステム運用に移るまでの「システム移行」、サービス開始後の「システム運用」を旨く運営しなければ得ることができない。(図表 3.3.0.1 参照）例えば、開発したシステムの品質が悪く、しばしば停止したり、多くの手作業を要求したりした場合、誰も使わなくなってしまうこともある。

図表 3.3.0.1　　IT システムのライフサイクル



また、IT サービスが企業の基幹システムとして使われるようになったことから、ハードウェアの故障やソフトウェアの障害、ウイルスの感染や、停電、災害でサービスが停止したり、データが失われたりしてしまった場合、企業活動への影響は甚大になる。

従って、今回は、普段見落としがちである「システム移行」、「システム運用」に企業がどう備えているかを中心にアンケートを実施した。特に、日常のサービスを安定して提供するために必要な、サービス運用については、必要な作業内容を下記に細分化し、その実施体制や、品質管理の程度を調査することにした。

①. エンドユーザ支援（Q14～18）

IT サービスの利用者にとって、PC や IT サービスの利用に関する疑問への回答や、PC 故障時の対処が迅速に行われないと、業務の停滞につながる恐れがあり、適切な支援が必要となる。

②. 日常運用（Q19～24）

コンピュータ（サーバ）は故障したり、ソフトウェア障害が顕在化したりして、重要なデータが失われたりする可能性があり、定期的なバックアップ作業が必要になる。また、記憶装置内にごみが累積（財布の中に小銭があふれるような状況）するため、定期的に記憶装置の整理を行っ

たりする必要がある。昨今では、セキュリティ対策の修正もしばしば発生し、適用する必要がある。

③. トラブル対応（Q25～33）

コンピュータの故障時や、障害発生時は、状況を見極め、ハードウェアの交換や、データのリストアなどを素早く対処を行い、サービスを迅速に復旧させる必要がある。故障の予兆を掴み、予防措置をとることも重要になる。

④. 原因調査（Q34～37）

トラブルからの復旧は迅速で無ければならないが、同時にその原因を正確に把握し、同じ問題が再発しないように、業務ソフト開発者や、ハード・ソフトのベンダと連携した調査と対処を行う必要がある。

⑤. 品質（Q38～44）

IT サービスの品質にはいろいろな側面があるが、基本的にはサービスの中断をビジネス上許される範囲に収めることが重要になる。システムの設計如何で中断時間を最小限にとどめることはできるが、過剰品質にすると投資が莫大になるため、ビジネス部門と適切な目標を決め、そこへ向かって行く姿勢が求められる。

⑥. サービス継続（Q45～50）

如何に旨く設計されたシステムでも、大規模停電や災害時にはサービスを継続できない。しかし、ビジネスによっては、このような状況でも一定期間の内に IT サービスの再開を必要とする場合がある。災害が発生してから、あわてて泥縄式に対処するのではなく、事前に対処を検討しておくことが重要になる。

⑦. 移行（Q51～59）

新しいシステムやサービスの組込時には当然、（サービス）移行が発生するが、これ以外にも、業務ソフトの修正、改善、ベンダ・ソフトの修正時にも、本番システムへの移行作業が発生する。この作業では、システムの安定性が損なわれたり、悪意を持った処理が組み込まれたりする可能性がある。内部統制面からも、この移行作業の厳格さが求められている。

これらの内容については、ITIL®、COBIT[8]などのベストプラクティスや標準化案、ISO20000[9]と言う管理標準が存在し、普及し始めており、今回のアンケート項目もこれらを参照して作成し、専門用語はできるだけ平易に置き換えるようにした。

[8] Control Objectives for Information and related Technology： 企業・自治体といった組織の IT ガバナンスの指針として、米国の情報システムコントロール協会（ISACA）などが提唱する IT ガバナンスの実践規範のこと。昨年発行された Version 4.1 が最新版である。
[9] IT サービスマネジメントの国際規格。IT サービスを提供するすべての組織に適用されるマネジメントシステム規格。ITIL®をもとに作成した英国の国家規格 BS15000 を国際標準化。日本では日本工業規格として制定され、JIS Q 20000：2007 として発行された。

3.3.1 エンドユーザ(EU)支援(4.7 節　参照)

この項では、社内利用者に対する支援についての下記の 5 個の質問への回答を分析している。

Q14： トラブルの問い合せ窓口を設置し、社内に公開していますか。(社員の生産性を向上するには、専門の社員支援体制が必要です)　(窓口明確化)

Q15： 質問対応要員のスキルを維持していますか。(スキル低下は社員から「応対が悪い」とのクレームが多くなります)　(スキル維持)

Q16： 質問対応要員、電話の数は充分ですか。(不十分ですと社員から「電話がつながりにくい」とのクレームが多くなります)　(窓口要員数)

Q17： PC の使い方や業務処理に関する問い合せに対応していますか。(社員の生産性向上のために必要になります)　(サービス内容)

Q18： 質問内容を記録し、改善に役立てていますか。(質問を低減し、満足度を向上するために必要になります)　(記録・改善)

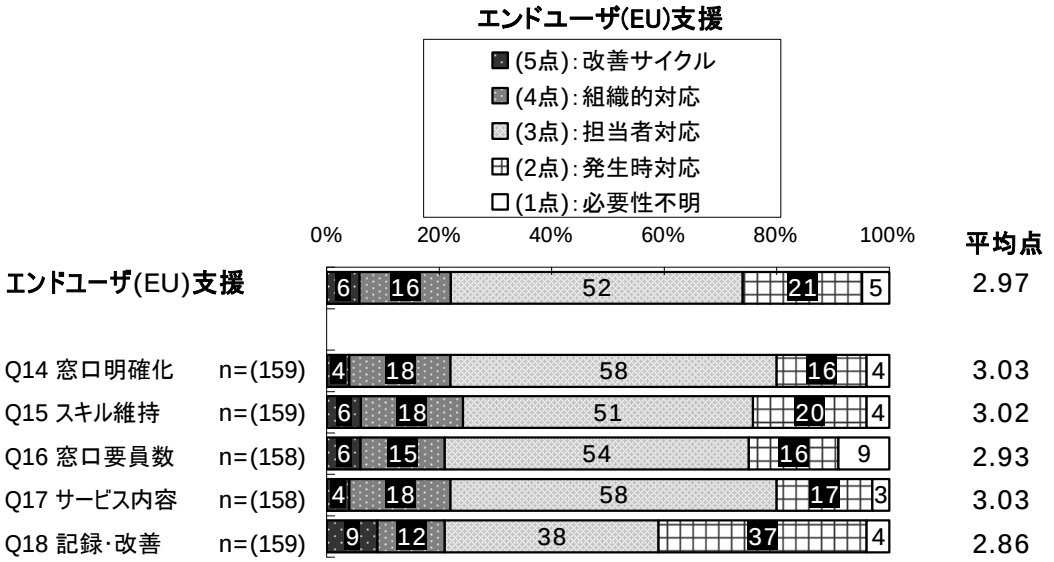
各質問に対する回答の選択肢は微妙に異なるので、それらを表示すると以下のとおりである。

図表 3.3.1.1

エンドユーザ (EU)支援	(5点): 改善サイクル	(4点): 組織的対応	(3点): 担当者対応	(2点): 発生時対応	(1点): 必要性不明
Q14 窓口明確化	負荷を評価し 改善している	専門組織化している	担当者を決め、 一任している	特定者はいない	必要性を認めない ／分からない
Q15 スキル維持	対応のミスを分析、 改善している	教育を実施している	担当者を決め、 一任している	対応していない	必要性を認めない ／分からない
Q16 窓口要員数	負荷を評価、 改善している	専門組織化している	担当者を決め、 一任している	特定者はいない	必要性を認めない ／分からない
Q17 サービス内容	負荷を評価、 改善している	専門組織化している	担当者を決め、 一任している	特定者はいない	必要性を認めない ／分からない
Q18 記録･改善	記録を分析、 改善している	対応を記録している	担当者を決め、 一任している	記録していない	必要性を認めない ／分からない

各質問に対する回答の分布と平均点（上記の選択肢を点数として平均値を算出）は、下記のとおりであった。

図表 3.3.1.2



＊ エンドユーザ支援に関する 5 個の質問への回答の平均点は、すべてがほぼ 3.0 点であり、想定した点数よりも低い。

＊ その理由を類推すると、エンドユーザ支援に関しては、担当者に一任しておれば、担当者の尽力で、社員はある程度満足し、致命的な問題が起きていないということではないかと思われる。

＊ しかし、担当者に一任するだけでは状況の好転は期待できないので、組織的対応が求められている状況は変わっていないと考えられる。

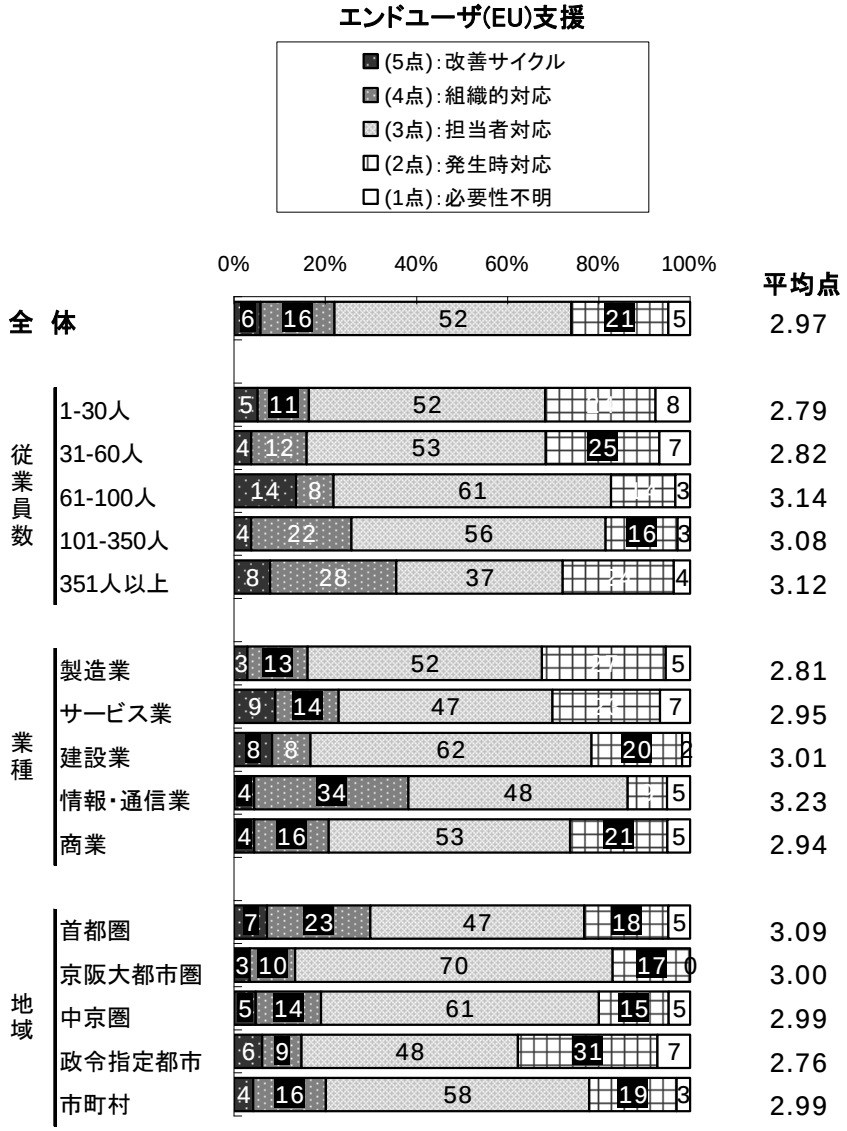
＊ 質問ごとの回答分布の傾向と平均点は、記録・改善についての質問への回答を除いてほとんど同じであり、約 75～80%が対応している。

＊ しかし、そのうち 50%以上が『担当者対応（3 点)』であり、『組織的対応（4 点)』して対応していないし、『改善サイクル（5 点)』には至っているのは 5%程度である。

＊ 記録・改善についての質問への回答では、約 50%が『記録していない』なので、平均点も他の質問への回答と比べて低い。

このデータを従業員数別、業種別、地域別に整理したものが下表である。

図表 3.3.1.3



＊ 従業員数別に見ると、「351 人以上」を含めて平均点には大差がない。

＊ 業種別に見ると、「情報・通信業」はその他の業種と比べて、『発生時対応（2 点)』の割合が低く、平均点が高い。その他の業種の平均点には大差がない。

＊ 地域別に見ると、平均点に大差があるとは考えられない。

3.3.2 日常運用(4.8 節 参照)

この項では、日常運用についての下記の 6 個の質問への回答を分析している。

Q19： アプリケーション維持の要・不要の観点から棚卸し評価を行っていますか。(不要なアプリケーションを維持するコストを低減できます) (アプリ資産管理)
Q20： アプリケーション関連の 2007 年問題に対して対策を行っていますか。(団塊世代の退職に伴い、障害修正や機能追加ができなくなる恐れがあります) (レガシー対策)
Q21： 休日・夜間を含め、オペレーション業務において要員数は十分ですか。(不十分ですと作業ミスなどの修復での就業が増え、退職者が増える恐れがあります) (運転要員数)
Q22： オペレーション要員のスキルを維持していますか。(作業ミスが増えたり、効率が下がる恐れがあります) (スキル維持)
Q23： 定常操作や非定常操作に対するオペレーション手順書を整備していますか。(作業ミスが増えたり、効率が下がる恐れがあります) (手順標準化)
Q24： オペレーションの自動化を進めていますか。(手動オペレーションはミスを招いたり、コスト高につながります) (運転自動化)

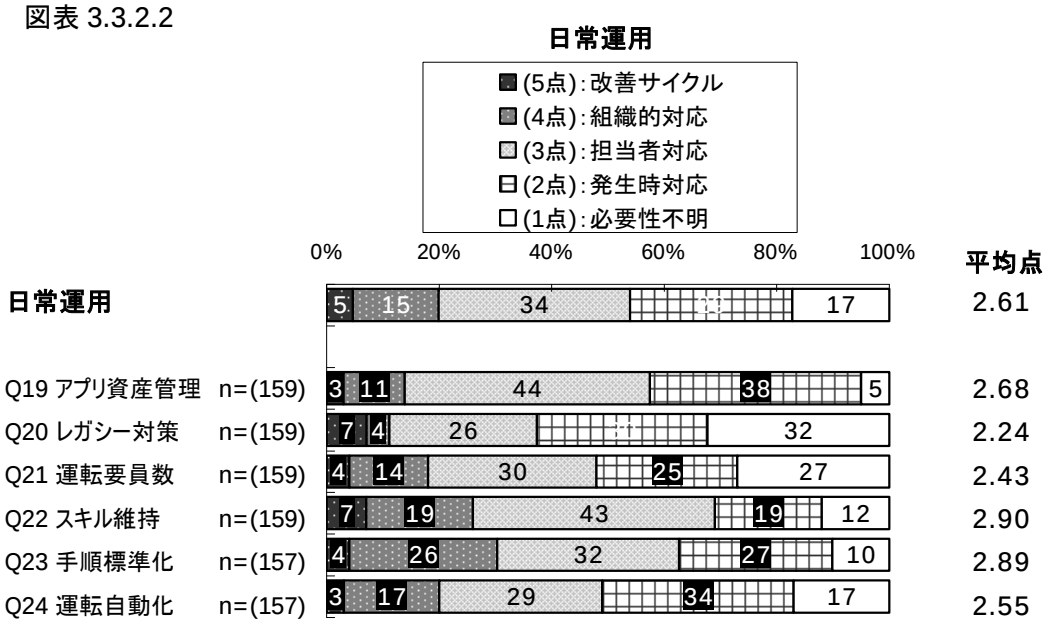
各質問に対する回答の選択肢は微妙に異なるので、それらを表示すると以下のとおりである。

図表 3.3.2.1

日常運用	(5点): 改善サイクル	(4点): 組織的対応	(3点): 担当者対応	(2点): 発生時対応	(1点): 必要性不明
Q19 アプリ資産管理	指標で管理している	評価会議をしている	担当者を決め、一任している	評価していない	必要性を認めない／分からない
Q20 レガシー対策	移行を完了している	移行中である	担当者を決め、一任している	移行する予定はない	必要性を認めない／分からない
Q21 運転要員数	負荷を評価、改善している	専門組織化している	担当者を決め、一任している	特定者はいない	必要性を認めない／分からない
Q22 スキル維持	作業ミスを分析、改善している	教育を実施している	担当者を決め、一任している	対応していない	必要性を認めない／分からない
Q23 手順標準化	作業ミスを分析、手順書を改版している	手順書を整備している	担当者を決め、一任している	整備していない	必要性を認めない／分からない
Q24 運転自動化	負荷を評価、自動化を推進している	自動化を導入している	担当者を決め、一任している	手作業で行っている状況	必要性を認めない／分からない

各質問に対する回答の分布と平均点（上記の選択肢を点数として平均値を算出）は、下記のとおりであった。

図表 3.3.2.2



＊ 日常運用に関する 6 個の質問への回答の平均点は、すべて 3.0 点以下であり、想定した点数よりも低い。

＊ その理由を類推すると、日常運用に関しては、専任の担当者を決めるレベルまでの認識に至っていないということではないかと思われる。

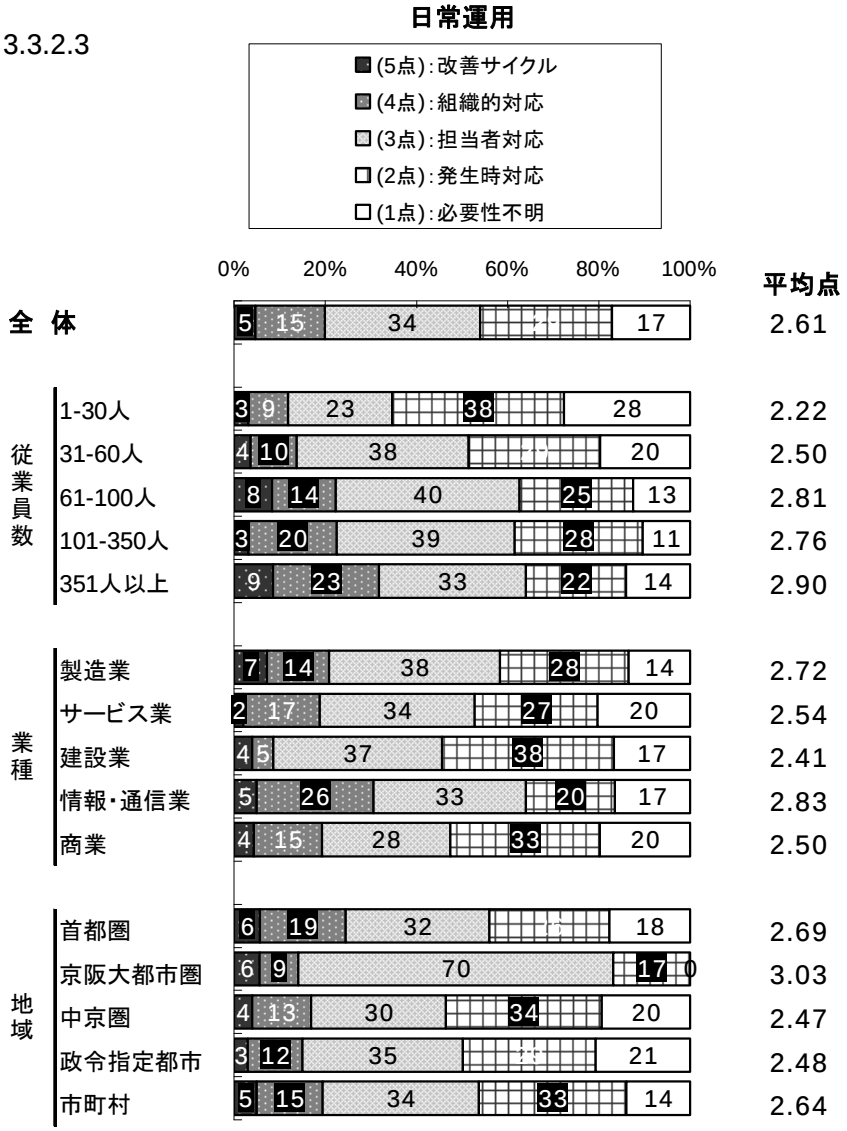
＊ レガシー対策および運転要員数の 2 個の質問に対する回答の平均点が低い。その原因は『必要性不明（1 点)』の割合が極端に高いことによる。

＊ これは、「質問の中にある 2007 年問題は無関係」、「専任要員は配置していない」などの理由も推測され、回答企業の個別事情によって、回答の選択が『1 点』と『2 点』とに分かれたことが考えられる。（今後同種の調査に際しての検討課題である）

＊ そのように考えたとしても、どの質問に対する回答においても『担当者対応（3 点)』の域を越えている割合が 10～30%であるのは、日常運用に対しての切実感が一般的に薄いことがうかがわれる。

このデータを従業員数別、業種別、地域別に整理したものが下表である。

図表 3.3.2.3



＊　従業員数別に見ると、「1～30 人」を除くと平均点には大差がない。強いていえば、企業規模が大きくなるほど、日常運用を重要視している。

＊　業種別に見ると、「情報・通信業」と「製造業」の平均点が高いが、大差ではない。

＊　地域別に見ると、「京阪神大都市圏」の平均点が高い。他の地域の間に大差はない。

3.3.3 トラブル対応（4.9 節　参照）

この項では、トラブル対応についての下記の 9 個の質問への回答を分析している。

Q25： 重要なシステムの稼働状況の監視を行っていますか。（社員からのクレームを待たず、より迅速に解決を図る必要があります）　（稼働監視）

Q26： ハードやソフトのトラブルの兆候が検出できていますか。（ハード品質劣化や、システム負荷を検出することでトラブルを未然に防止できる割合が増えます）　（兆候監視）

Q27： 重要システム周辺の電源・空調に異常が発生した場合の監視・通報の仕組みはありますか。（放置すると稼働条件面からシステム停止となり、重要なデータを消失したり、作業のやり直しが必要になります）　（周辺監視）

Q28： トラブル対応の内容や処理時間など記録をつけていますか。（記録をつけることで、再発時の対応を円滑にできます）　（記録・改善）

Q29： トラブル対応を実施する場合、トラブル対応手順書の整備は行っていますか。（トラブル解決を効率的に行い、特定の担当者に依存しない均一的な処置が可能です）　（手順標準化）

Q30： トラブルが発生した場合、重大度や緊急度を適切に判断し、優先順位を意識した対応をしていますか。（企業活動への影響を最小限にするために必要です）　（優先度付け）

Q31： PC 故障時の対策を考慮していますか。（社員の業務への影響を最小限にとどめるために必要です）　（PC 故障対策）

Q32： トラブル対応要員のスキルを維持していますか。（対応要員が適切に教育されていないと積み残しが増え、企業活動に影響する恐れがあります）　（スキル維持）

Q33： 障害が起ったときの影響範囲はある程度推測できる対策をとっていますか。（トラブル発生、あるいは兆候検出時点で、その影響度合いを見極め、対策を取ることが重要です）　（構成管理）

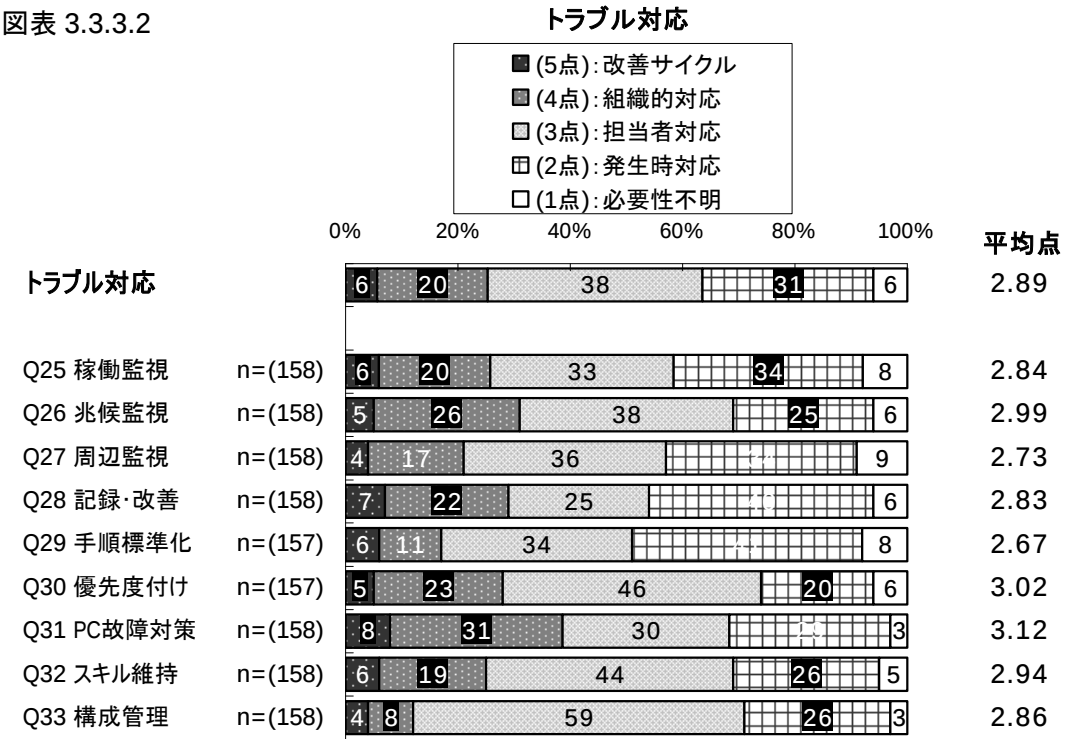
各質問に対する回答の選択肢は微妙に異なるので、それらを表示すると以下のとおりである。

図表 3.3.3.1

トラブル対応	(5点): 改善サイクル	(4点): 組織的対応	(3点): 担当者対応	(2点): 発生時対応	(1点): 必要性不明
Q25 稼働監視	障害を分析、 稼動改善している	監視システムを 導入している	担当者を決め、 一任している	社員からの申告で 対応している	必要性を認めない ／分からない
Q26 兆候監視	監視の上、障害を分析し、改善している	監視し、 兆候を検出している	担当者を決め、 一任している	検出できていない	必要性を認めない ／分からない
Q27 周辺監視	障害を分析、兆候検出し改善している	監視システムを 導入している	担当者を決め、 一任している	監視していない	必要性を認めない ／分からない
Q28 記録･改善	記録を分析、 改善している	対応を記録している	担当者を決め、 一任している	記録していない	必要性を認めない ／分からない
Q29 手順標準化	トラブルを分析し、 改善している	手順書を 整備している	担当者を決め、 一任している	整備していない	必要性を認めない ／分からない
Q30 優先度付け	重要度と緊急度定義し、判断ミスの分析も行い改善している	重要度と緊急度を定義し対応している	担当者を決め、 一任している	対応していない	必要性を認めない ／分からない
Q31 PC故障対策	すぐに使える代替機（カストマイズ後）を用意している	予備機を 用意している	担当者を決め、 一任している	修理を手配している	必要性を認めない ／分からない
Q32 スキル維持	対応内容を分析、 改善している	教育を 実施している	担当者を決め、 一任している	対応していない	必要性を認めない ／分からない
Q33 構成管理	解決遅延を分析し、 改善している	影響予測の管理表を整備している	担当者を決め、 一任している	対策していない	必要性を認めない ／分からない

各質問に対する回答の分布と平均点数（上記の選択肢を点数として平均値を算出）は、下記のとおりであった。

図表 3.3.3.2



本項の平均点は、2.89 と低い。特に、周辺監視、記録・改善、手順標準化、構成管理の 4 個の質問に対しての低さが目立つ。

＊ 記録・改善と手順標準化の 2 個の質問に対して、『記録していない』、『整備していない』との回答が最多回答である点は、着目すべきである。
一方、これらの問いに『記録を分析、改善している』、『トラブルを分析し、改善している』との高点回答も、7%、6%と少なくない。

トラブル対応の内容や時間を記録し、対応のしかたを改善して、これを関係者間で情報共有しなければならない。これにより、運用の組織的対処へ一歩近づくことができる。この認識を持つか持たないかの差が出ている。

他の具体的な 7 個の質問についても見ていく。

＊ 稼働監視の質問については、約 90%の回答が何らかの対応をしていると答えている。
さらに、『監視システムを導入している』というレベルは 20%であり、その上のレベルである『障害を分析、稼働改善を行っている』と回答も 6%ある。
稼働を注視することが運用の基本である点の認識は、十分できているとみる。
＊ 兆候監視の質問については、『担当者対応』の回答が多く、『改善サイクル』の回答は少ない。
＊ 周辺監視の質問については『監視していない』との回答も多いが、『監視システムを導入している』との回答も 17%あり、さらに『改善サイクル』レベルの回答も 5%あって、広がりのある回答分布を示している。
監視システムに対する見解の差が出ているからであろう。
＊ 優先度付けの質問については、『担当者対応』が 46%をしめる最多回答となっている。
＊ PC 故障対策の質問は、単に『修理を手配』というレベルも多いが、『予備機を用意』というレベルもほぼ同数の回答を得ている。広がりのある回答分布である。
＊ スキル維持の質問については、『対策していない』という回答が 26%あるものの、『改善サイクル』レベルも 6%しめており、多様な回答分布である。

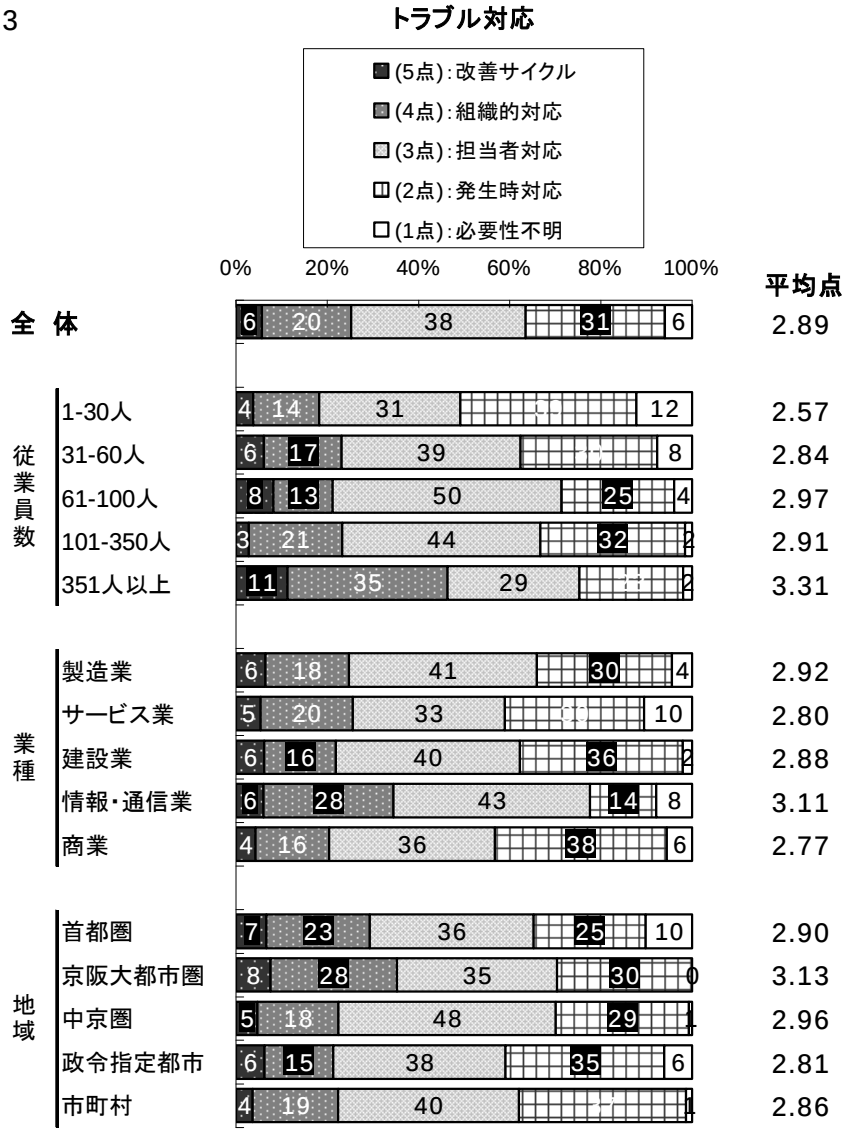
面接調査において、要員教育の徹底によってトラブル件数を減少させたという以下の話が聞けた。『障害減少は、要員に対する教育を徹底したことが貢献していると考えている。特に、関係するハード・ソフト全体をとらえた上で、諸状況を見るということを、一件一件、部長自ら、ポンチ絵をかくことによって理解させた。しかし、画面上の情報だけにとらわれた問題の把握で済ませてしまう担当者の姿勢は改めきれていない。

トラブル対応を通じても要員教育を行おうとしている点、全体システムをとらえるという考え方を繰り返し徹底している点、参考とすべきである。

＊ 構成管理の質問については、『対策していない』という回答が 26%あるものの『影響予測の管理票を整備している』との回答も 8%ある。『改善サイクル』レベルの回答は少ない。

このデータを従業員数別、業種別、地域別に整理したものが下図表である。

図表 3.3.3.3



＊ 従業員数別に見ると、規模の大きいところがより高得点を得ているが、境界となるところは、「351 人以上」のところである。
「351 人以上」の企業は、高得点 3.31 をとっているだけでなく、『改善サイクル』レベルの回答が 11%あり、『組織的対応』レベルが 35%ある。
一方、「1～50 人」企業の最多回答は、『把握していない』レベルであり、39%を占めている。

＊ 業種別に見ると、「情報・通信業」が、やや高得点の 3.11 を得ている。
一方、「商業」の平均点が、2.77 と低い。また、「商業」の最多回答は『発生時対応』レベルである。

＊ 地域で見た場合、「京阪神大都市圏」が 3.13 とやや高得点をえているものの、大きな差異はない。

3 個の個別の質問について触れる。個々の関連図表は、4.9 節に載せている。

＊ 記録・改善の質問について、従業員数別に見ると、「351 人以上」のところでは、高得点 3.50 をとり、『記録していない』ところも、22%と少ない。
一方、それ以外のところでは、最多回答を『記録していない』としている。特に、「1～30 人」のところでは、これが 50%も占めている。
また、業種別で見ても、すべての業種での最多回答が『記録していない』である。
地域で見ると、「京阪神大都市圏」では、50%が『対応を記録』と回答しており、比較的よい傾向を示している。

＊ 手順標準化の質問について、従業員別に見ると記録・改善の質問と同様の傾向である。
しかし、「351 人以上」のところでも、平均点が 3.17 にとどまっている。
業種別では、「情報・通信業」だけが、『整備していない』との回答は少ない。しかし、『担当者対応』レベルにとどまっており、その上のレベルは少ない。
製造業は、『整備していない』との回答が最多回答であるが、『手順書を整備している』、さらに『トラブルを分析し改善している』という回答もそれぞれ 16%、11%あり、多様な回答分布となっている。

＊ スキル維持の質問について、従業員数別の差異は少ない。
地域で見ると、明確な差異が示される。「首都圏」、「京阪神大都市圏」、「中京圏」では、『改善サイクル』のレベルを含めて、幅広い分布をしている。
「政令指定都市」は、『担当者対応』レベルが最多回答であるが、『改善サイクル』レベルはない。
市町村では、『対応していない』が最多回答となっている。

3.3.4 原因調査（4.10 節　参照）

この項では、トラブル原因調査についての下記の 4 個の質問への回答を分析している。

Q34： トラブル発生状況を把握し、対策を検討していますか。（トラブルの発生増大を放っておくと、更にトラブルが増え、企業活動に深刻な影響を与える場合もあります）
（傾向分析）

Q35： 原因調査の内容や処理時間など、記録をつけていますか。（記録をつけないと、改善の糸口がつかめなくなります）（記録・改善）

Q36： イベントログやシステムログを収集していますか。（問題の根本原因を調査するために必要になります）（ロギング）

Q37： ソフトウェアの最新修正版を常に適用していますか。（修正を適用することで、トラブルの発生を未然に防止することができます）（予防保守）

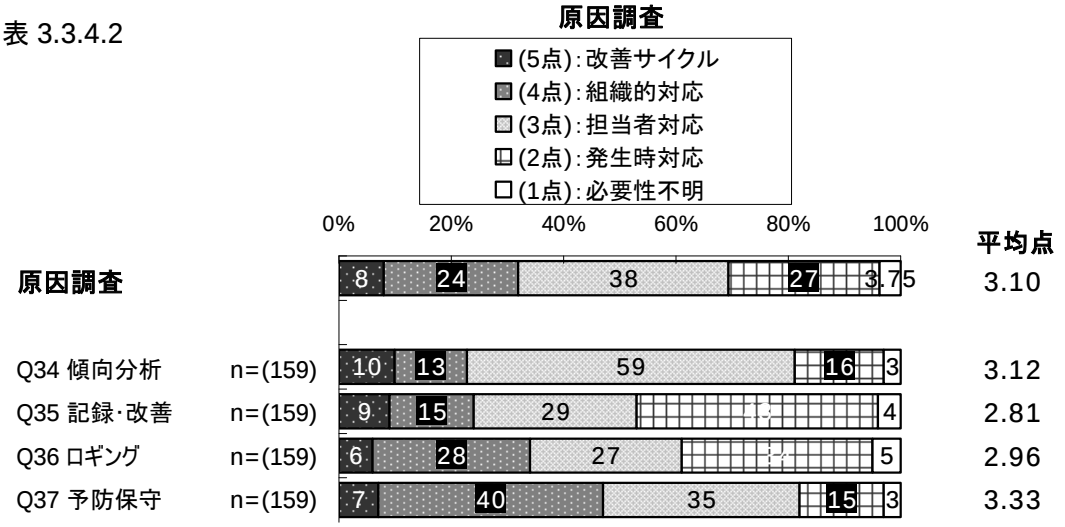
各質問に対する回答の選択肢は微妙に異なるので、それらを表示すると以下のとおりである。

図表 3.3.4.1

原因調査	(5点): 改善サイクル	(4点): 組織的対応	(3点): 担当者対応	(2点): 発生時対応	(1点): 必要性不明
Q34 傾向分析	対応状況を分析し、改善している	専門組織化している	担当者を決め、一任している	把握していない	必要性を認めない／分からない
Q35 記録･改善	記録を分析し、改善している	調査を記録している	担当者を決め、一任している	記録していない	必要性を認めない／分からない
Q36 ロギング	自動化を導入しつねに内容を分析し、改善している	ログ収集の自動化を導入している	担当者を決め、一任している	収集していない	必要性を認めない／分からない
Q37 予防保守	修正の影響を分析し適応している	修正を適用している	担当者を決め、一任している	適用していない	必要性を認めない／分からない

各質問に対する回答の分布と平均点（上記の選択肢を点数として平均値を算出）は、下記のとおりであった。

図表 3.3.4.2



＊ 本項に対する平均点は、3.10 であり、運用関係の他の項に比べてやや高い。これは、5 点レベルへの回答が比較的多いことによる。
＊ 対応をとっているとの回答は、70%であるが、このうちの約 60%近くは、『担当者対応』である。
『組織的対応』『改善サイクル』というレベルの回答も、それぞれ 24%、8%あって多様な回答となっている。
＊ ４個の質問に対しての回答分布については、一様ではない。
＊ 記録・改善の質問については、約 40%が『記録していない』と回答していて、これが一番多い回答である。
しかしながら、『改善サイクル』レベルの回答が 9%、『組織的対応』が 15%となっており、多様性も示している。

『記録していない』というということは、情報共有が行われず、組織的対応に結び付かない。部門マネージャーの課題としてまず「記録させる」べきであろう。

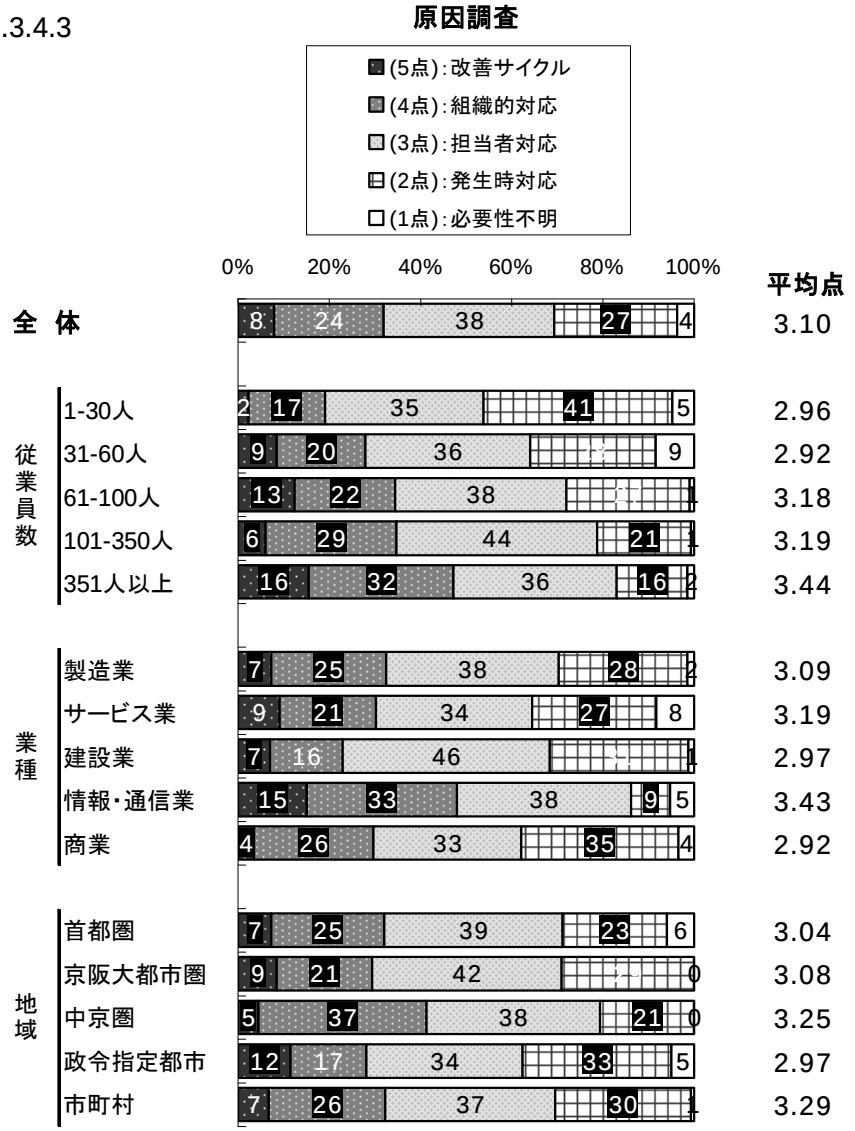
＊ ロギングの質問についても、同じような傾向を示している。
34%が、『収集していない』と回答していて、最多回答である。
また、『自動化して分析』レベル、『収集の自動化』レベルの回答も少なくない。

ロギングは、問題未解決状況の長期化を避けるための、あるいは、ペンディング項目を減少させるための有力なツールである。特に、マルチベンダ状況下では、必須のツールと考えられる。
ロギング情報はかならずしも原因究明の絶対的情報ではないが、ロギング情報をとることによって明らかとなる事象を、まず理解すべきである。また、ベンダはこのことを明確に伝えなければならない。

他の 2 個の質問についても見ていく。
＊ 傾向分析の質問については、約 80%が『把握している』と回答していて、得点も比較的良い。しかし、『担当者対応』がその 80%をしめている。
＊ 予防保守の質問については、約 80%が『担当者対応』を含むものの、対応していると回答している。『改善サイクル』、『組織的対応』レベルも合わせて 40%と多い。
従って、平均点も 3.33 と高い。

このデータを従業員数別、業種別、地域別に整理したものが下図表である。

図表 3.3.4.3



＊　従業員数別に見ると、顕著に差が表れている。
「1～30 人」では、『発生時対応』との回答が約 40%で、最多回答である。
「351 人以上」では、『改善サイクル』レベルおよび『組織的対応』レベルの回答が合わせて 50%近くとなっている。

＊　業種別に見ると、「情報・通信業」の平均点が 3.43 と高い。また、『改善サイクル』レベルおよび『組織的対応』レベルの回答が合わせて 50%近くとなっている。
「商業」は低く、2.92 であり、最多回答も『発生時対応』となっている。

＊　地域別に見た場合には、大きな差異はない。

2 個の個別質問について、見ていく。図表は 4.10 節を参照されたい。

＊ 記録・改善の質問については、人数規模が大きいところほどよくなっているが、ほとんどの規模で『発生時対応（記録していない)』との回答が最多回答となっている。
「351 人以上」だけは例外であり、幅広い回答分布を示している。『改善サイクル（記録を分析し、改善している)』という 5 点レベルの回答も 17%ある。
業種別にみると、「情報・通信業」を除いて『発生時対応（記録していない)』が最多回答となっている。
「情報・通信業」では、対応をとっているところが多い。
ただ、この「情報・通信業」で、9%が，1 点レベルの『必要性不明』と回答している。この 9%は、他の業種より多い。
地域別に見た場合には、大きな差異はない。

＊ ロギングの質問についても、記録・改善の質問と同様に、人数規模が大きいところほどよくなっている。
業種別に見ると、『収集していない』が最多回答でないのは、「建設業」と「情報・通信業」である。他の業種では、『収集していない』が最多回答である。
「情報・通信業」では、『ログ収集の自動化を導入している』が最多回答である。
「サービス業」では、12%が『必要性不明』と回答している。
地域別に見ると、「中京圏」が、『収集の自動化』を 41%で行っており、平均点も 3.35 と高い。
「市町村」では、『収集の自動化』を 31%で行っているが、一方、『収集していない』ところが、37%である。

3.3.5 品質(4.11 節 参照)

この項では、品質についての下記の 7 個の質問への回答を分析している。

Q38： 社内に約束するシステムの稼働率を設定していますか。(100%の稼働率を求めることは難しく、コスト効果を考え適切なバランスで折り合いをつける必要があります) (稼働率)

Q39： 使用者の満足度を考慮した運用改善目標を設定し、達成したかを把握していますか。(サービス提供は使用者の満足度の向上につながるようにする必要があります)
(ユーザ満足度)

Q40： 将来的にシステムに必要な処理量を把握していますか。(処理能力増強のシステム変更には充分な準備期間が必要なため、将来的な処理量の把握が必要です) (処理量予測)

Q41： 導入以降のシステム処理量の変動を把握していますか。(システムの負荷増大は、システムのレスポンス速度や故障率に大きく影響します) (負荷解析)

Q42： システム導入にあたって必要な運用コストを把握していますか。(一般にシステム費用のうち 60%が運用コストと言われています) (コスト管理)

Q43： 外部委託した作業の進捗状況や作業結果をレビューし、必要な指示を行っていますか。(レビューの実施は自らのサービス品質を確保するために必要です) (委託業務レビュー)

Q44： 外部委託にあたって、作業責任を明確化し、期待するサービス品質を提示していますか。(サービス品質の提示は、自らのサービス品質目標を定めるために必要です)
(委託業務品質)

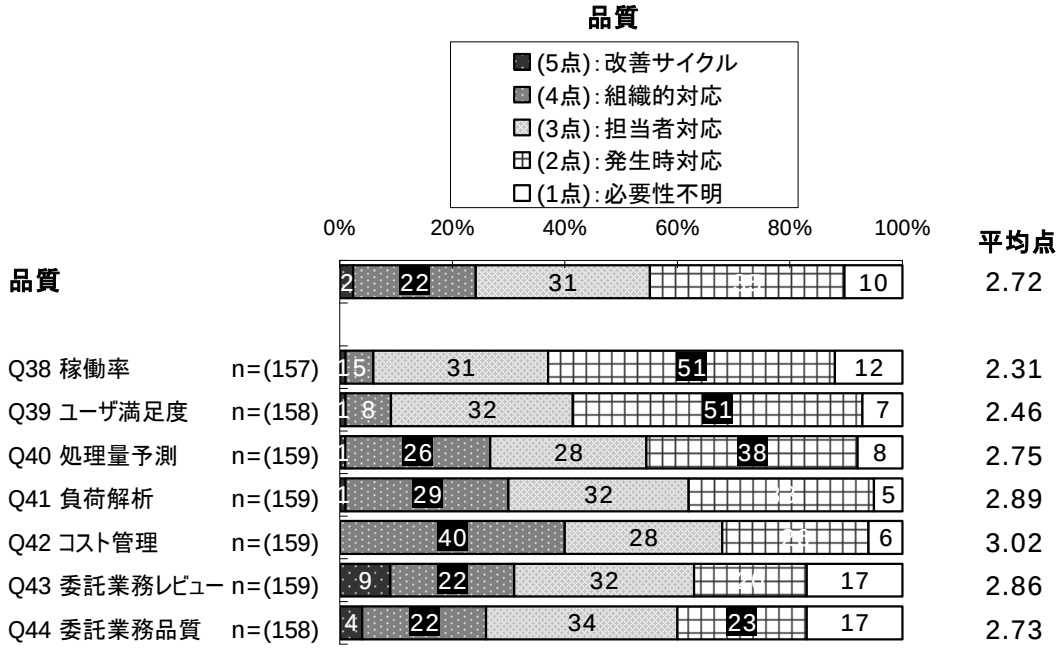
各質問に対する回答の選択肢は微妙に異なるので、それらを表示すると以下のとおりである。

図表 3.3.5.1

品質	(5点): 改善サイクル	(4点): 組織的対応	(3点): 担当者対応	(2点): 発生時対応	(1点): 必要性不明
Q38 稼働率	指標で管理している	目標を設定している	担当者を決め、一任している	設定していない	必要性を認めない／分からない
Q39 ユーザー満足度	指標で管理している	達成度を把握している	担当者を決め、一任している	把握していない	必要性を認めない／分からない
Q40 処理量予測	指標で管理している	処理量を把握している	担当者を決め、一任している	把握していない	必要性を認めない／分からない
Q41 負荷解析	指標で管理している	処理量を把握している	担当者を決め、一任している	把握していない	必要性を認めない／分からない
Q42 コスト管理	指標で管理している	運用コストを把握している	担当者を決め、一任している	把握していない	必要性を認めない／分からない
Q43 委託業務レビュー	進捗レビューし、管理している	進捗報告を受領している	担当者を決め、一任している	管理していない	必要性を認めない／分からない
Q44 委託業務品質	作業仕様を締結し指標で管理している	作業仕様を締結している	担当者を決め、一任している	管理していない	必要性を認めない／分からない

各質問に対する回答の分布と平均点（上記の選択肢を点数として平均値を算出）は、下記のとおりであった。

図表 3.3.5.2



＊ 品質に関する 7 個の質問への回答の平均点は、コスト管理に関する質問への回答を除いてすべて 3.0 点以下であり、想定した点数よりも低い。

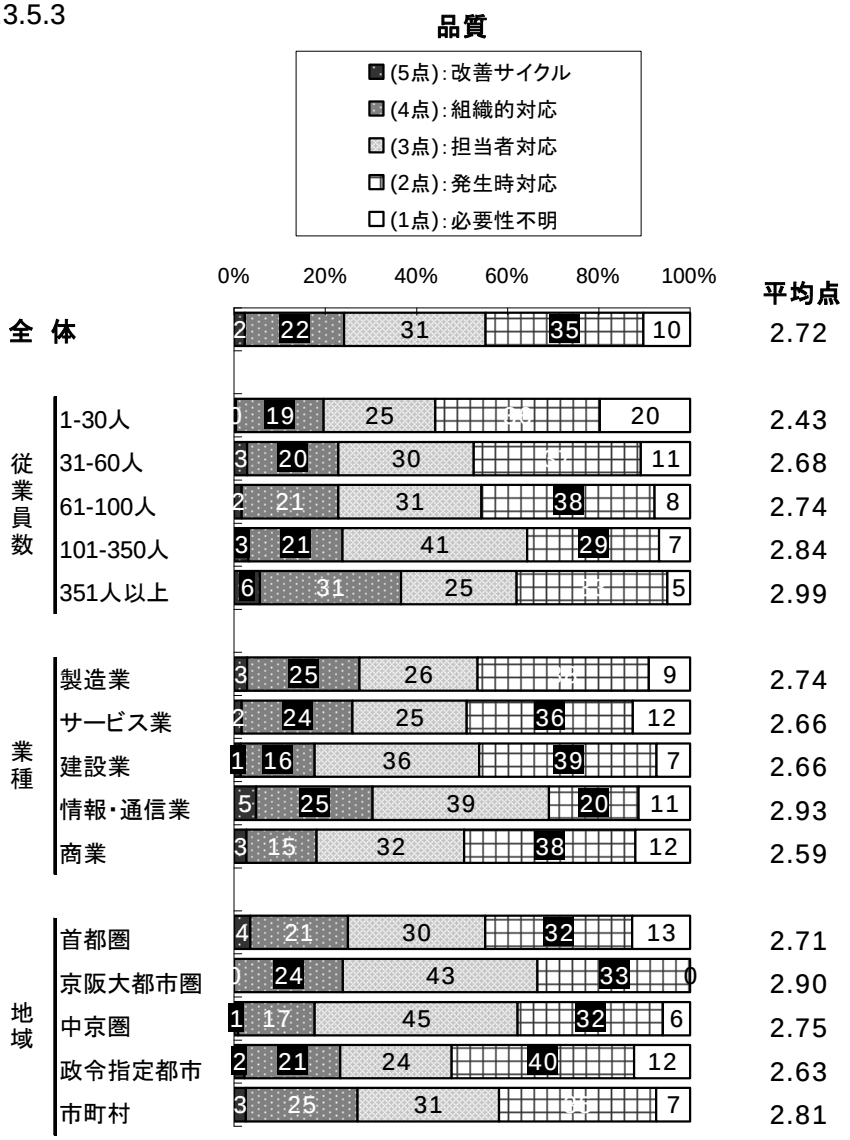
＊ 稼働率目標とユーザ満足度（運用改善目標）の 2 個の質問に対する回答では、『目標設定や達成度把握（4 点)』の割合が 10%以下であり、また、『設定・把握していない（2 点)』の割合が 50%以上であり、結果的に平均点が 2.5 点以下である。この 2 個の質問は、品質に関しての質問の中で最も重要なものであるので、この結果は憂慮される。

＊ コスト管理に関する質問に対する回答のうち、『運用コストを把握している（4 点)』の割合が 40%であり、平均点は 3.0 点を超している。システム関連コストのうちで、運用コストの比重が高いこともあり、経営者の関心も高いことが想定され、その結果が現れたと思われる。この項で取り上げている品質に関する事柄に対して、コストに対すると同様の関心を経営者が示せば、状況は進展するのではないかということをうかがわせる。

＊ そのように考えたとしても、どの質問に対する回答においても『担当者対応（3 点)』の域を越えている割合が 10～30%であるのは、品質に対しての切実感が一般的に薄いことがうかがわれる。

このデータを従業員数別、業種別、地域別に整理したものが下表である。

図表 3.3.5.3



＊ 従業員数別に見ると、「1~30 人」と「351 人以上」を除いて、平均点には大差がない。強いていえば、企業規模が大きくなるほど、平均点が高い。

＊ 業種別に見ると、「情報・通信業」はその他の業種と比べて、対応していない割合が低く、平均点が高い。その他の業種の間には大差がない。

＊ 地域別に見ると、「京阪神大都市圏」の平均点が高い。他の地域の間に大差はない。

3.3.6 サービス継続(4.12 節 参照)

この項では、サービス継続についての下記の 6 個の質問への回答を分析している。

Q45： 企業の業務継続の面から欠くことのできないシステムの災害、事故、停電対策を行っていますか。(企業活動を継続させるために必要です) (災害対策)

Q46： システムのレスポンスを把握していますか。(システムのレスポンス速度は、社員の生産性や満足度におおきな影響を与えます) (システム性能)

Q47： システムの負荷状況を把握していますか。(システムの負荷は、システムのレスポンスや害発生率に大きな影響を与えます) (システム負荷)

Q48： バックアップの取得は確実にできていますか。(システムの障害により重要なデータが失われたり、システムの再構成が必要になったりする場合があります) (バックアップ)

Q49： バックアップからのリストアが確実にできていますか。(データやシステムのバックアップが、いざというとき読み出せなかったり、作業ミスで役立たないことがありがちです) (リストア)

Q50： システムの稼働率の目標を定め、実態を把握していますか。(システムの稼働率は、障害の頻度だけでなく、システムの冗長性やトラブルからの復旧速度にも影響されます) (稼働率管理)

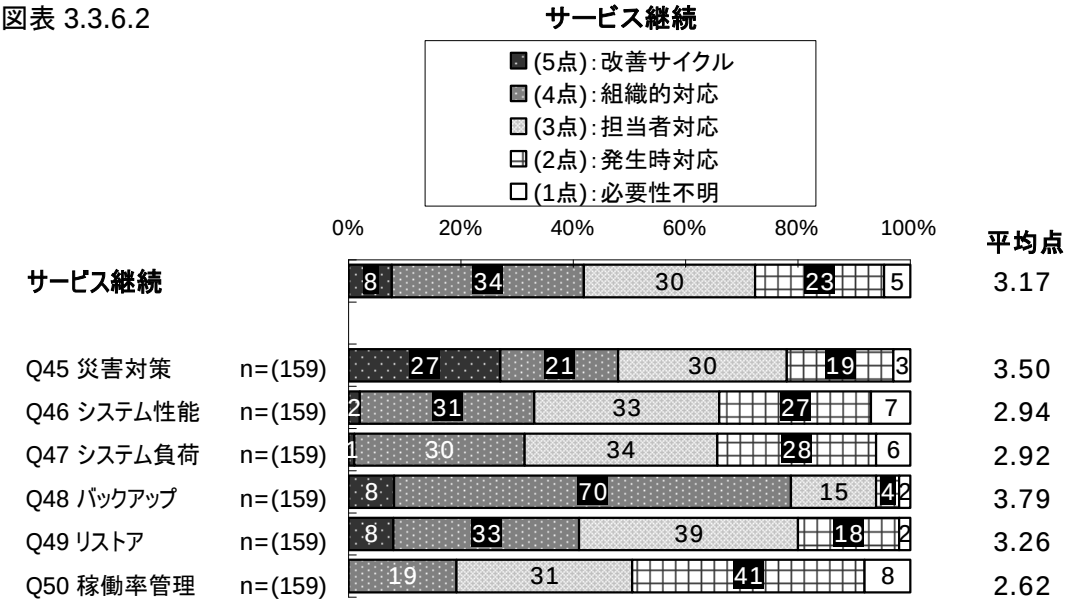
各質問に対する回答の選択肢は微妙に異なるので、それらを表示すると以下のとおりである。

図表 3.3.6.1

サービス継続	(5点): 改善サイクル	(4点): 組織的対応	(3点): 担当者対応	(2点): 発生時対応	(1点): 必要性不明
Q45 災害対策	対策を導入している	対策を 検討済である	担当者を決め、 一任している	対策していない	必要性を認めない ／分からない
Q46システム性能	指標で管理している	レスポンスを 把握している	担当者を決め、 一任している	把握していない	必要性を認めない ／分からない
Q47 システム負荷	指標で管理している	負荷を 把握している	担当者を決め、 一任している	把握していない	必要性を認めない ／分からない
Q48 バックアップ	基準を定め指標で 管理している	バックアップを 実施している	担当者を決め、 一任している	取得していない	必要性を認めない ／分からない
Q49 リストア	リストア訓練を 実施している	読み出し確認を している	担当者を決め、 一任している	実施していない	必要性を認めない ／分からない
Q50 稼働率管理	指標で 管理している	稼働率を 把握している	担当者を決め、 一任している	把握していない	必要性を認めない ／分からない

各質問に対する回答の分布と平均点数（上記の選択肢を点数として平均値を算出）は、下記のとおりであった。

図表 3.3.6.2



＊ 本項について平均点は、3.17 と比較的高い。
災害対策、バックアップ、リストアの 3 個の質問に、高い点を出している。
これらの質問に対しては、『対策を導入』、『基準を定め指標で管理』、『訓練を実施』という 5 点レベルでの回答が比較的多い。特に、災害対策の質問に対しては、27%が『対策を導入』と答えている。

＊ 回答のパターンは、上述の 3 個の質問に対するパターンと、これ以外のシステム性能、システム負荷、稼働率管理の 3 個の質問に対するパターンに二分される。

＊ 後者のパターンは、低い平均点である。後者 3 個の質問については、『指標で管理している』を最高レベルの回答としている。システム性能、システム負荷、稼働率管理の質問についての最高レベルの回答は、それぞれ 2%、1%、0%と極めて少ない。

IT サービスにおける運用を評価する上で、指標を持つことは極めて重要である。今どこにいるのか、どこへ行きたいのか、どうやって到達点をチェックするかという問いに、明確な答えを出すとしたら指標なしには考えられない。

定性的な見解は、恣意的見解ととられがちであり、指標による管理へ向かうことが望ましい。

＊ 稼働率管理の質問については、平均点が 2.62 と低い。
41%が『把握していない』と答え、最高レベル回答の『指数で管理している』ところはない。

高機能なシステムを持ったとしても、稼働率が低ければそのシステム効果は現れたことにはならない。また、良いシステムを持ったことにもならない。

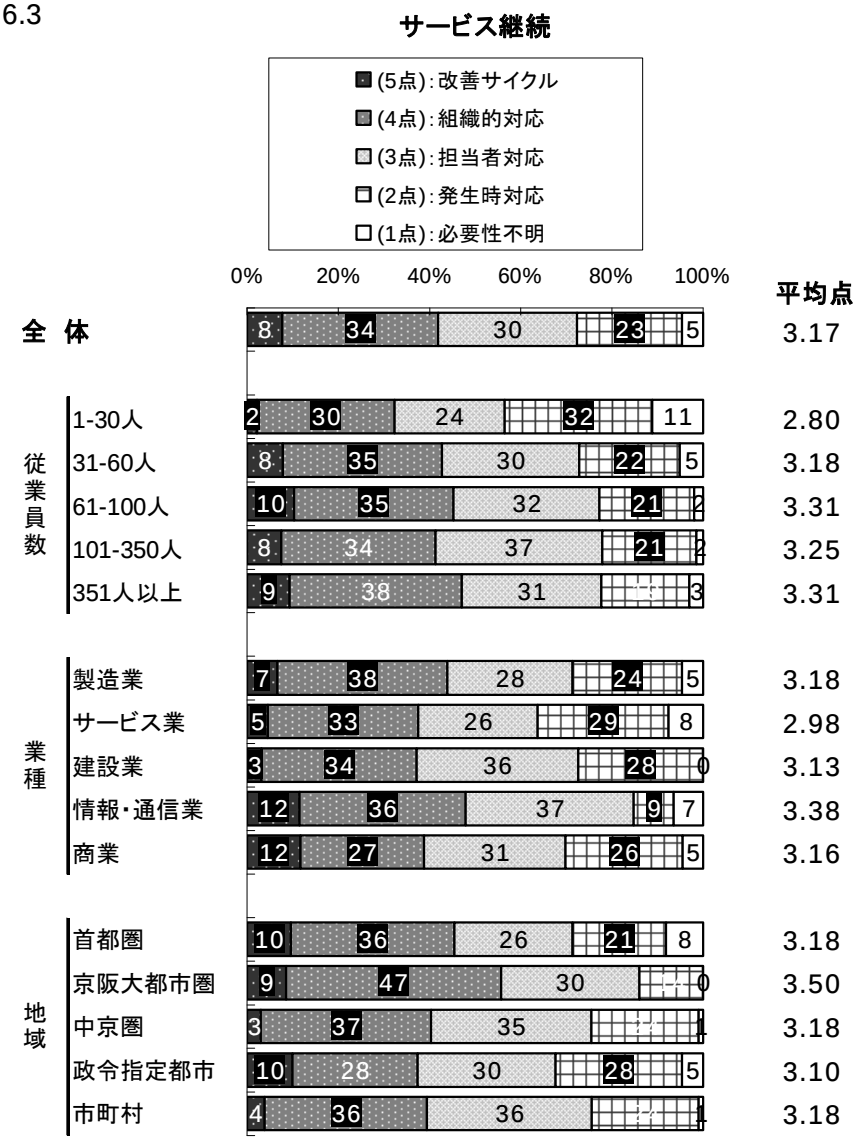
例えば、月度の締め処理が複雑なため月末、月初に運用トラブルが頻発することがある。これにより、稼働率を下げることとなる。この時、十分な運用訓練、運用要員教育などによりこれを克服することが、運用に求められるわけである。

運用がうまく行っているか否かの、第一のポイントが、稼働率であると考える。

まず、稼働率についての定義をした上でこれを『把握』し、データを蓄積する。次のステップとして、改善目標値を定めて運用していくことが望ましい。

このデータを従業員数別、地域別、業種別に整理したものが下図表である。

図表 3.3.6.3



＊ 従業員数別に見ると、「1～30 人」が低い平均点であり、『把握していない』が最多回答となっている。さらに、『必要性を認めない／わからない』との回答が 11%ある。
他のところでは大差がない。

＊ 業種で見た場合には、「サービス業」がやや低い平均点であり、『把握していない』が最多回答となっている。また、『必要性を認めない／わからない』との回答が 8%ある。

＊ 地域別には、京阪神大都市圏が高い平均点を得ている。4 点レベルの回答が、47%ある。

4 個の個別質問について見る。個々の図表については、4.12 節にある。

＊ 災害対策の質問については、「1～30 人」のところで『対策していない』との回答が 39%あり、目立つ。
一方、「61～100 人」のところで、『対策を検討済である』との回答が、42%と多い。
業種的には、「商業」で、『対策を導入している』との最高レベル回答が最多回答である。「商業」は 43%がそのように回答している。
「製造業」と「情報・通信業」は、『対策を導入している』も多いが、『対策していない』との回答も多く、広い分布となっている。
地域的には、政令指定都市で高レベル回答が得られている。

＊ システム性能の質問については、「1～30 人」、「31～60 人」が、『把握していない』を最多回答としている。また、「1～30 人」のところでは、16%が、『必要性を認めない／わらない』と回答している。
業種的には、「サービス業」の平均点が比較的低く、「情報・通信業」が比較的高い。
少ないながらも『指標で管理している』との答えがあるのは、「製造業」と「商業」のみである。
なお、システム負荷の質問でも「製造業」と「商業」だけに、『指標で管理』との回答がある。
地域的には、「京阪神大都市圏」の平均点が高く、『レスポンスを把握している』という 4 点レベルの回答を 50%がしている。

＊ バックアップの質問について見る。平均点としては、3.79 と高く、『取得していない』、『必要性を認めない／わらない』との回答は、6%にすぎない。
データ喪失時、紙ベースのデータからデータを入れ直したり、特殊なプログラムを組んでデータを復元したという苦い経験を一度はしているのであろう。
「1～30 人」のところでは、それでも、上記の回答が 16%をしめている。
業種的には、「情報・通信業」で、5 点レベルの回答である『基準を定め指標で管理している』と答えているところが、26%もある。
地域的には、「首都圏」「京阪神大都市圏」「政令指定都市」で、上記 5 点レベルの回答をそれぞれ、11%、17%、13%得ている。

＊ リストアの質問については、平均点としては 3.26 と悪いこともないが、『実施していない』、『必要性を認めない/分らない』との回答が、20%もある。
「1～30 人」のところで、上記の回答が 32%あり、「31～60 人」のところで、16%ある。
業種的には、「商業」での回答の 35%が、これにあたっている点が目立つ。
地域的には、「京阪神大都市圏」が、上記回答 0%である。

3.3.7 移行(4.13 節 参照)

この項では、移行についての下記の 9 個の質問への回答を分析している。

Q51： システムの導入・展開のスケジュール管理を実施していますか。(システム展開のスケジュールが狂うと、事態を収めるために思わぬ費用や作業が発生します)
(展開スケジュール)

Q52： PC の導入・展開の作業工数を管理していますか。(PC の導入にはソフトウェア・インストールやネットワーク情報設定などカスタマイズ作業が必要になります)
(展開計画立案)

Q53： 運用への移行を判定するため、移行試験における品質目標を定めていますか。(高品質のシステムを実現するには、運用に移行する前に品質評価が必要です) (品質目標)

Q54： システム開発から運用に移行する過程でシステム開発担当者以外による検査を実施していますか。(誤謬や悪意を持った処理が紛れ込む可能性があります) (悪意・誤謬防止)

Q55： ライセンス契約違反や無駄なライセンス購入はありませんか。(著作権保護法で守られており、違反すると懲罰的罰金が課せられたり、企業名が公表されたりします)
(ライセンス管理)

Q56： 最新のシステム構成情報(ハード/ソフト)の管理を行っていますか。(最新の情報になっていないと、トラブルを悪化させたり、回復が遅くなり場合があります) (構成管理)

Q57： 発生したトラブル解決のための変更内容と、変更後の検査を第三者が検査していますか。(品質が劣化したり、悪意を持った処理が混入することを防ぐために必要です)
(変更検査)

Q58： 変更の必要性を事前に確認していますか(不適切な計画に基づく構成変更・修正適用は、業務運用のスケジュールに支障をきたします) (変更承認)

Q59： 追加または改善した機能で、使われていないものが多くありませんか。(社員が希望したとしても、投資効果やシステム品質の面から必要性を吟味する必要があります)
(効果測定)

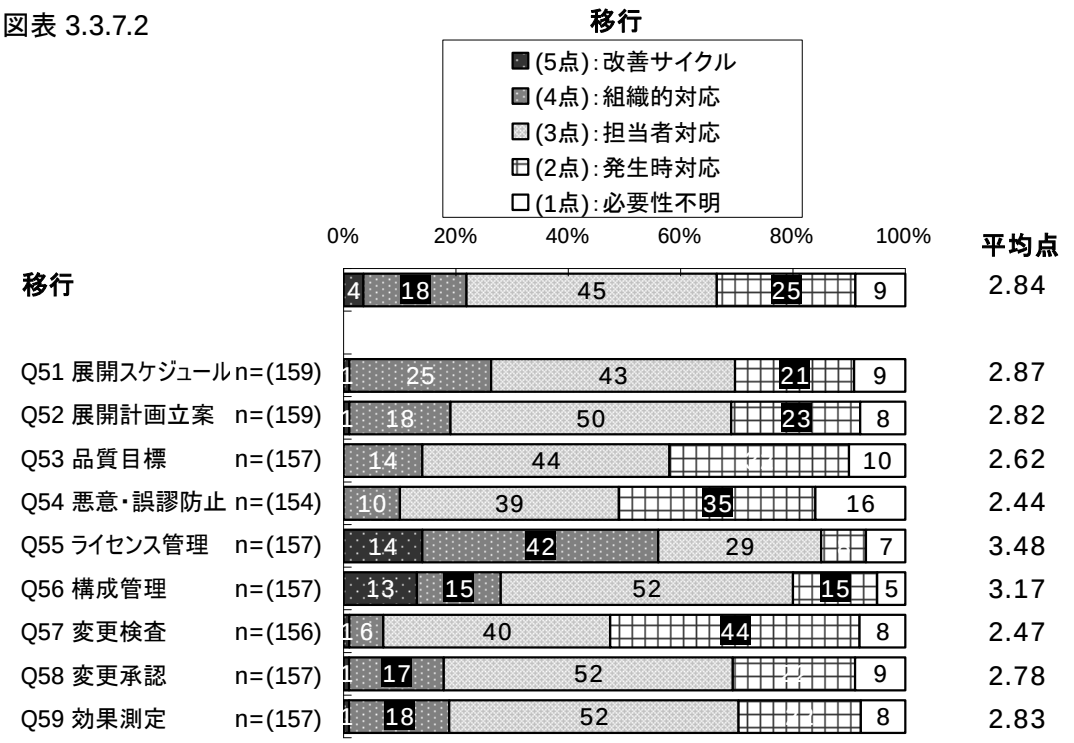
各質問に対する回答の選択肢は微妙に異なるので、それらを表示すると以下のとおりである。

図表 3.3.7.1

移行	(5点): 改善サイクル	(4点): 組織的対応	(3点): 担当者対応	(2点): 発生時対応	(1点): 必要性不明
Q51 展開スケジュール	専門体制を整備し進捗指標で管理している	専門体制を整備している	担当者を決め、一任している	管理していない	必要性を認めない／分からない
Q52 展開計画立案	専門体制を整備し進捗指標で管理している	専門体制を整備している	担当者を決め、一任している	管理していない	必要性を認めない／分からない
Q53 品質目標	指標で管理している	移行規準を定義している	担当者を決め、一任している	設定していない	必要性を認めない／分からない
Q54 悪意・誤謬防止	指標で管理している	第三者検査をしている	担当者を決め、一任している	検査していない	必要性を認めない／分からない
Q55 ライセンス管理	定期的に棚卸し、管理している	利用数を把握している	担当者を決め、一任している	把握していない	必要性を認めない／分からない
Q56 構成管理	一括集中管理している	管理を義務化している	担当者を決め、一任している	管理していない	必要性を認めない／分からない
Q57 変更検査	第三者検査をし指標で管理している	第三者検査をしている	担当者を決め、一任している	検査していない	必要性を認めない／分からない
Q58 変更承認	要否判定会議をし、指標で管理している	要否判定会議をしている	担当者を決め、一任している	確認していない	必要性を認めない／分からない
Q59 効果測定	要否判定会議をし、指標で管理している	要否判定会議をしている	担当者を決め、一任している	確認していない	必要性を認めない／分からない

各質問に対する回答の分布と平均点数（上記の選択肢を点数として平均値を算出）は、下記のとおりであった。

図表 3.3.7.2



＊ 本項についての平均点は、2.84 とやや悪い。
＊ 各質問についての回答パターンは、大きく「おおむね管理している」、「その場しのぎにとどまっている」、「比較的良く管理されている」の 3 パターンに分かれる。各質問について、パターンを意識しながらふれていく。
＊ 展開スケジュールの質問については、『進捗指標で管理している』ところは、少ないものの、『専任体制』あるいは『担当者対応』で約 70%が管理している。しかし、『管理していない』ところが 21%あり、得点を下げている。「おおむね管理している」パターンでである。
＊ 展開計画立案の質問についても、上記と似た分布を示している。「おおむね管理している」パターンでである。
＊ 品質目標の質問については、『設定していない』との回答が、30%以上あり、低い平均点しか上げていない。また、『移行基準を定義している』ところもあるが、『指標管理』まで行っていない。「その場しのぎ」のパターンである。

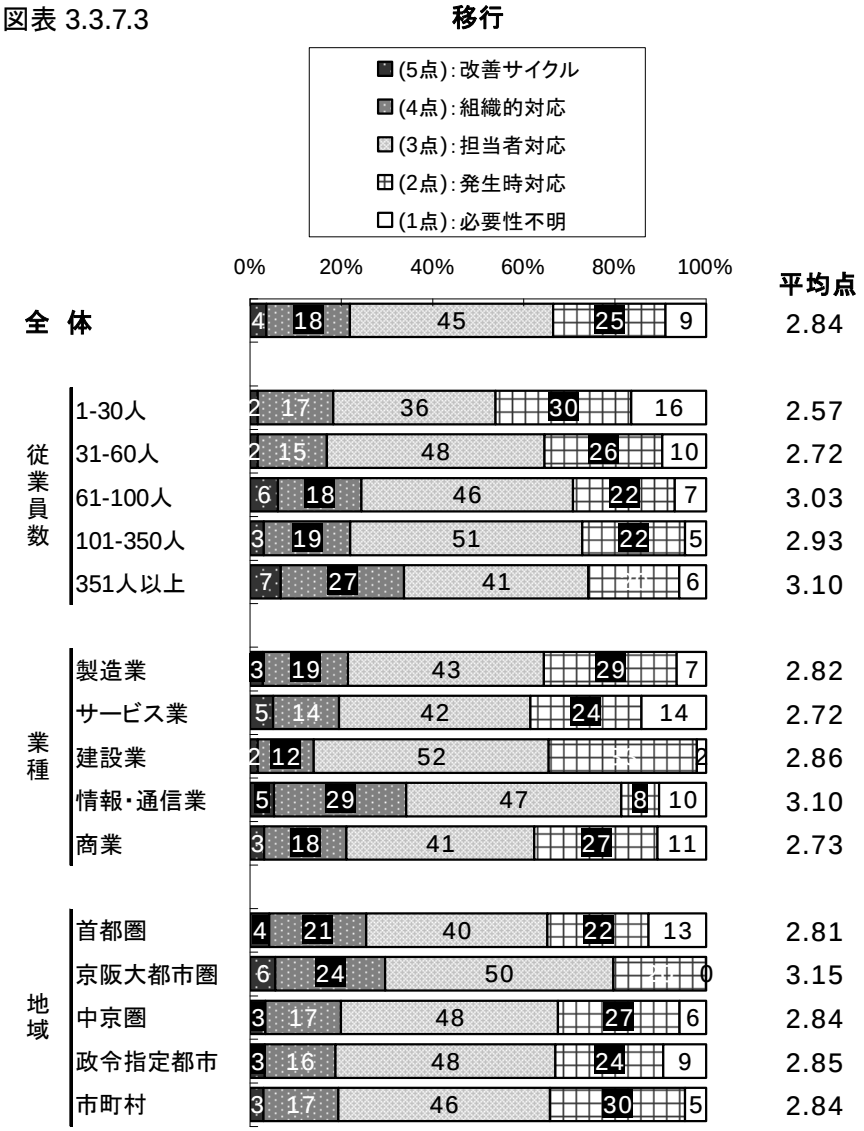
システム開発者は、ある程度の初期障害は当然との考えを持ちがちでる。一方、利用者は、新しい運用に慣れていないため、新システムを敬遠しがちである。従って、新システムの品質が合格かどうかの『移行基準を定義』しておく必要がある。これが、定性的なものでなく、指標で示される形であることが望ましい。

また、移行直後では、新しい運用に慣れていないため、二重障害を招いて、重大障害となることもある。

＊ 悪意・誤謬防止の質問については、『検査していない』が 35%、『必要性を認めない／わらない』が 16%であり、本項のなかで最も低い平均点である。関係担当者だけに任せるのではなく、まちがいが起らない仕組みも必要である。「その場しのぎ」のパターンである。
＊ ライセンス管理、構成管理の 2 個の質問については、比較的よい点を取っている。ハードとしてはクライアント・サーバ、ソフトとしては多種コンポーネント使用という環境で、これらは重要な課題であり、この環境に対応できつつあると言ってよい。「比較的良く管理されている」パターンである。
＊ 変更検査の質問については、移行時の品質目標の質問と同様に考えなければならないが、最多回答が、『検査していない』である。安易なシステム変更により重大トラブルが発生することがある。「その場しのぎ」のパターンである。
＊ 変更承認の質問については、70%が確認している。「おおむね管理している」のパターンである。
＊ 効果測定の質問についても同様である。

このデータを従業員数別（企業規模別）、業種別、地域別に整理したものが下表である。

図表 3.3.7.3



＊ 従業員数別に見たとき、対応の差がはっきり出ている。
「1～30 人」のところでは、50%近くが、『把握していない』、『必要性を認めない／わからない』と回答しているところが目立つ。
「61～100 人」のところから、これが 30%を切るようになる。
「351 人以上」のところでは、『組織的に対応』するという回答が 30%以上を占めている。

＊ 業種別に見ると、「サービス業」、「商業」、「製造業」で、『把握していない』、『必要性を認めない/分らない』と 40%近くが回答している。
「情報・通信業」では、この数値が 20%以下である。

＊ 地域別には、「京阪神大都市圏」の平均点が良い。

3 個の個別質問について見る。図表については、4.13 節にある。

＊ 展開スケジュールの質問については、従業員数別に見たときの対応の差が顕著であるが、『専門体制を整備し進捗指標で管理している』との最高レベルの回答をしているのは、「31～60 人」のところと、「61～100 人」のところである。
この 2 社は、政令指定都市の「サービス業」と「建設業」である。
また、「京阪神大都市圏」では、『管理していない』および、『必要性を認めない／わからない』という 2 点、1 点レベルの回答はなく、高い平均点をあげている。

＊ 品質目標の質問については、従業員数別に見たとき、対応の差が顕著である。
「1～30 人」のところでの 1 点レベル回答が 16%と多いこと、および「351 人以上」のところでの 5 点レベル回答が 28 点と多いことが目立つ。
業種別にみると、「サービス業」と「情報・通信業」で、『必要性を認めない／わからない』との回答が、20%近くを占めている。

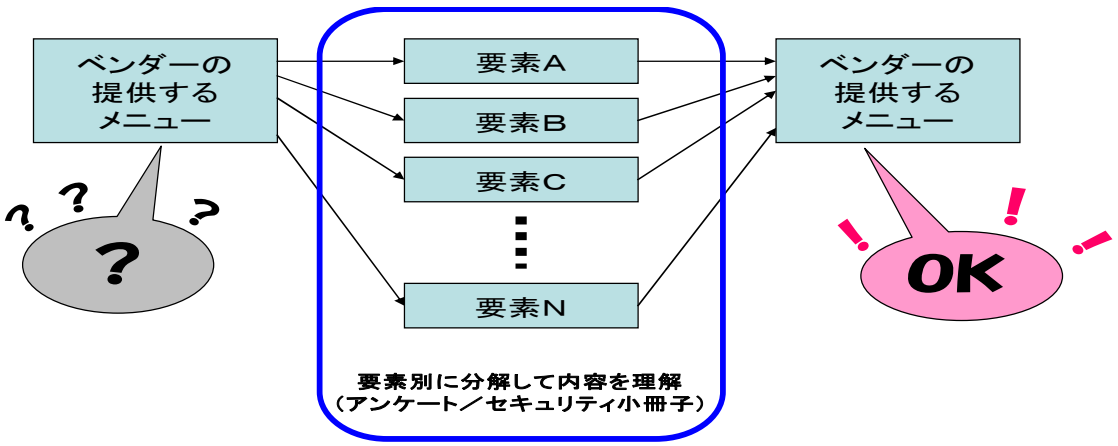
＊ ライセンス管理の質問については、従業員別に見ると、同様に、規模の大きなところほどよい状況を示している。
業種としては、「情報・通信業」の 30%が『定期的に棚卸し、管理している』という完璧回答をしている。
一方、「建設業」の 30%が、『把握していない』と答えている。
地域的には大差はない。

3.4 セキュリティについて

昨年までの調査研究で、ベンダの提供するメニューはその内容がわかりにくく、何をどう選択して良いのかわからないという意見が多い事がわかっていた。ベンダの提供するメニューは SI（システム・インテグレーション：システム全体を取りまとめ、構築する作業）を含むものがほとんどであり、これはそれぞれのベンダの戦略とも絡み単純に統一することは難しい。今回のアンケートおよび当協会独自作成の「必要なセキュリティ対策がわかる本」は、このメニューをできるだけ要素化して単純にしていくことを考慮して作成した。

アンケートについては要素別に問題点と対策とをセットにしてひとつの質問項目を構成することで、質問を読むだけでこの問題にはそこにどんな問題が内在しているのかを理解できるようにしている。ベンダの提供しているメニューはこれらの要素の組み合わせと、それらをまとめるための作業で構成されているため、それぞれの要素が理解できれば組み合わせも理解できることになる。この構成に対応して作成したのが「必要なセキュリティ対策がわかる本[10]」である。この小冊子は、図表 3.4.0.1 のように、要素別の問題に対する対策を記述しており、アンケートに回答した企業はアンケートに対応した解決策を、その中から見つけ出すことができるようになっている。

図表 3.4.0.1



アンケートは 5 者択一の構成になっており、質問事項は多いが、それほど時間をかけなくても答えられるようなものになっている。5 段階の 3 は「危険はわかっているが対応していない」の項目になっており、1～3 の段階は対策を取っていない項目となるため、アンケート回答に対する診断結果では、対策に関するアドバイスを記述している。

セキュリティに関する質問は、経営者への質問の Q10～13 までの 4 問から始まり、インターネットへの接続の有無により Q60～92 と Q93～111 までの質問に大きく分類している。インターネットへの接続の有無による質問の違いは、インターネット接続に起因する脅威に関するもののみであり、インタ

10：「必要なセキュリティ対策がわかる本」は、主として中堅・中小企業の企業のセキュリティに対する理解を助けるために作成した。そのために構成は
①ここから始めよう、セキュリティ対策の第一歩（ステップ 1）
②早めにやった方がいい次の段階のセキュリティ対策（ステップ 2）
③状況により実施しておく必要のあるセキュリティ対策（ステップ 3）
④より強固なシステムを構築するためのセキュリティ対策（ステップ 4）
とし、さらに要素別メニューの説明、導入事例と費用例を加えわかりやすく構成している

ーネット接続をしていなくてもその他については、その持っているリスクは基本的に同じと考えられる。従って、質問の内容は脅威の部分を除いてほとんど同じ項目となっている。今回のアンケートではインターネット接続無しの企業が 2 社あった。うち 1 社は個人情報を大量に取り扱っていることから、リスク回避のための手段としての施策との事であった。この 2 社については今後のデータとして活用する。

① 脅威対策（Q60～67）

インターネットに接続することは、外部からの攻撃や内部からの情報漏洩のリスクを背負い込むことになるが、それらへの対策を行っていれば、リスク以上のメリットを享受することが可能となる。現在ではビジネスを進める上でインターネットの利用は必須の条件となっており、従ってこの脅威への対策をしっかり行うことも必須の条件となっている。

② 漏洩対策（Q68～81）

情報漏洩には、インターネット接続を行ったことにより、スパイウェアの侵入を許し、結果として内部情報がインターネットを通じて漏洩する場合もあるが、むしろ内部犯行によりインターネット以外の各種媒体（紙、CD-R、DVD、USB メモリなど）を通じて漏洩するケースの方が、情報漏洩の約 7 割を占めるというほど多い。インターネットに接続する／しないに関わらず情報漏洩への対策は重要である。

③ セキュリティ管理（Q82～86）

重要情報の管理には二つの側面がある。ひとつはビジネス継続のための、経理情報などのデータベースのバックアップ、二重化など、もうひとつは重要情報をみだりに社外に持ち出すことを禁止・抑制するための管理である。後者は今後益々重要になる内部統制にも大いに関係しているので充分な対策をとっておく必要がある。

④ 物理セキュリティ（Q87～91）

情報漏洩や破壊に対する物理的な対策としては、人的要因への対策と自然災害などの外部要因への対策がある。人的要因に対しては IC カードなどによるアクセス制御が有効であるが、外部要因に対しては別の場所へのシステムの二重化やデータセンタ利用のアウトソーシングを検討する必要があるが、全社に対してはテナントビルの場合の対処方法や、ビルの老朽化による対策不可のケースもあり課題も多い。

⑤ 人材と組織（Q10～13、92）

主として組織や会社の経営方針に依存する項目についての質問。経営者の考え方がセキュリティ対策への取り組み方に大きく影響するのは当然であるが、それが全社的に組織として実施されているかが、従業員のモチベーションの向上と客先からの信頼に繋がり、ひいては業績向上のポイントとなる。

3.4.1 脅威対策(4.14 節 参照)

この項では、インターネット脅威対策についての下記の 8 個の質問への回答を分析している。

Q60： インターネットに接続していると、外部から侵入される危険があります。不正アクセスへの対応策をとっていますか。 (ファイアウォール対策)

Q61： コンピュータウィルスに感染すると、PC のファイルが改ざんされたりコンピュータが破壊される危険があります。対応策をとっていますか。 (ウィルス対策)

Q62： 次々と送られてくる広告や迷惑メールを制限する方法やサービスがあります。対応策をとっていますか。 (スパムメール対策)

Q63： コンピュータウィルスに感染すると、知らないうちにインターネットに情報を漏洩したり他のコンピュータに迷惑行ためを行う可能性があります。対応策をとっていますか。 (スパイウェア対策)

Q64： 外部からの攻撃を監視したり、防御したりする仕組みがあります。またそれらの攻撃を監視したり通報する仕組みがあります。これらの対策を採用していますか。 (IDS/IPS[11])

Q65： 外部からの浸入で PC 内の重要なファイルが壊れたり、無くなったりする場合があります。それに備えてデータバックアップ対策をしていますか。 (データバックアップ対策)

Q66： Windows の不具合を利用して、悪意のある人がＰＣを攻撃することができます。定期的なパッチ適用などの対応策をとっていますか。 (パッチ配信サービス)

Q67： ウィルスなどの侵入を防ぐため、社内 LAN に、許可したＰＣ以外を接続できないように制限することができます。対応策をとっていますか。 (不正 PC 接続対策)

[11]不正侵入検知／不正侵入防御システム

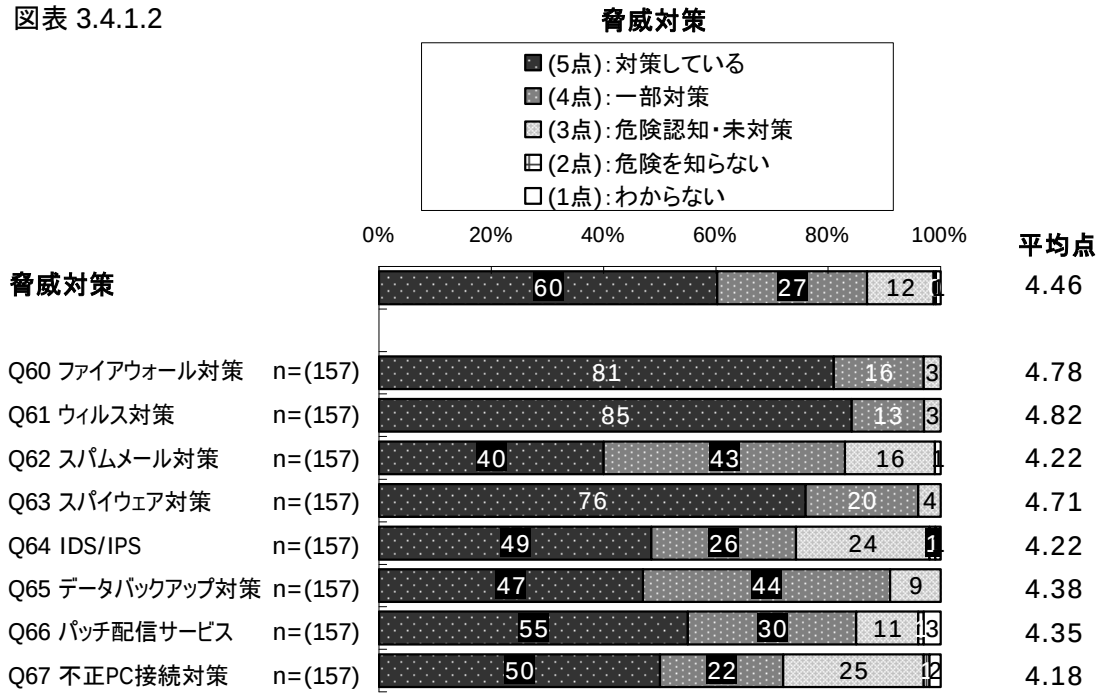
各質問に対する回答の選択肢は微妙に異なるので、それらを表示すると以下のとおりである。

図表 3.4.1.1

脅威対策	(5点): 対策している	(4点): 一部対策	(3点): 危険認知・未対策	(2点): 危険を知らない	(1点): わからない
Q60 ファイアウォール対策	対応している	一部対応している	危険は知っているが対応していない	危険があることを知らない	わからない
Q61 ウィルス対策	対応している	一部対応している	危険は知っているが対応していない	危険があることを知らない	わからない
Q62 スパムメール対策	対応している	一部対応している	危険は知っているが対応していない	危険があることを知らない	わからない
Q63 スパイウェア対策	対応している	一部対応している	危険は知っているが対応していない	危険があることを知らない	わからない
Q64 IDS/IPS	採用している	一部採用している	仕組みは知っているが採用していない	仕組みがあることを知らない	わからない
Q65 データバックアップ対策	対策している	一部対策している	危険は知っているが対応していない	危険があることを知らない	わからない
Q66 パッチ配信サービス	対策している	一部対策している	危険は知っているが対応していない	危険があることを知らない	わからない
Q67 不正PC接続対策	対策している	一部対策している	危険は知っているが対応していない	危険があることを知らない	わからない

各質問に対する回答の分布と平均点（上記の選択肢を点数として平均値を算出）は、下記のとおりであった。

図表 3.4.1.2



＊ 図表 3.4.1.2 より、脅威対策に関する 8 個の質問への回答の全体平均点（選択肢を得点として平均値を算出）は、4.45 点と高い結果であった。
質問した 8 項目全てにおいて平均点が 4 点を超えており、インターネットに接続した時の危険性の理解度が高く、予防策を講じている企業の多いことがうかがえる。

＊ ファイアウォール対策、ウィルス対策、スパイウェア対策の 3 個の質問では、『対策している（5 点）』が 76%～85%、『一部対策（4 点）』を含めると対策している割合が 91%～98%と非常に高い。
これは、世間で被害が多発している情報が浸透しており、危険に対する理解度が高いことから、優先的に対策を行っているものと推測される。

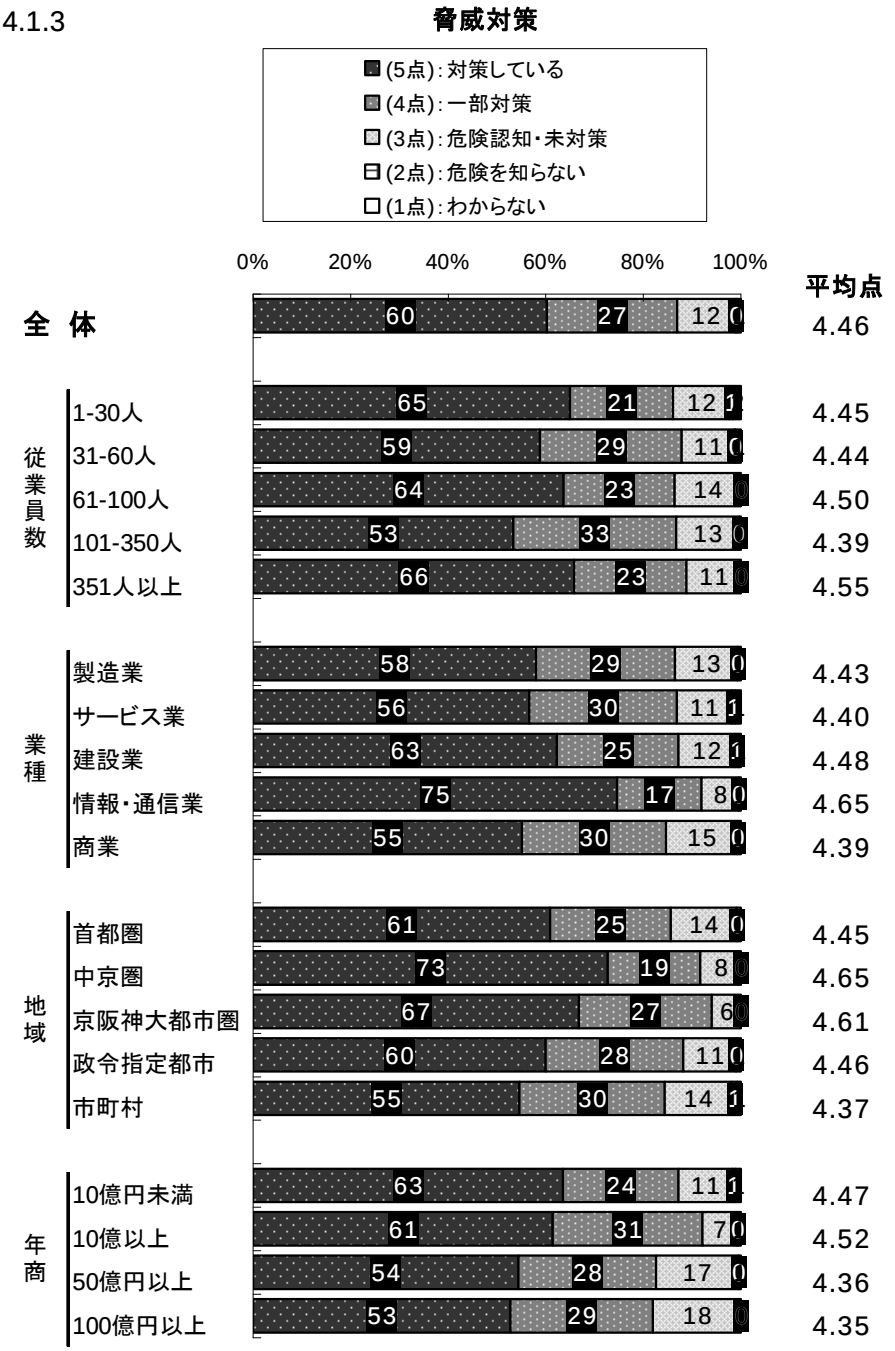
＊ スパムメール対策、パッチ配信サービスの 2 個の質問では、『対策している』の割合は 40%～55%であるが、『一部対策』を含めた割合では 83%～85%と高い。
また、IDS/IPS や不正 PC 接続対策についても『一部対策』を含めた割合は 72%～75%と比較的に高い。

＊ データバックアップ対策の質問では、『対策している』の割合は 47%であるが、『一部対策』を含めた割合では 91%と高い。
これは、データのバックアップは一般的にシステム運用作業に組み込まれる場合が多いことから、実施率が高い結果になっているものと推測される。

インターネットからの脅威対策の各項目については、セキュリティ対策の基本ステップに位置する内容が多いことから、その必要性の理解度が高く対策の実施率も高い。
企業にとって必要不可欠なセキュリティ対策であり、今後も一層の対策実施が期待できるものと考える。

このデータを従業員数別、業種別、地域別に整理したものが下表である。

図表 3.4.1.3



＊ 従業員数から見ると、『対策している』割合では若干バラツキがあるものの、『一部対策している』を含んだ割合ではほとんど差が無い。

＊ 業種別では、「情報・通信業」が『対策している』割合で 75%、『一部対策』を含めた割合でも 92%と他業種より対策が進んでいることがうかがえる。予想どおり IT 関連業種である「情報・通信業」の対策が先行している。

＊ 地域別では、全体の対策実施率が高い中でも、京阪神大都市圏、中京圏の対策が進んでおり、首都圏と市町村がやや遅れている傾向にある。

3.4.2 漏洩対策(4.15 節 参照)

この項では、情報の漏洩対策についての下記の 14 個の質問への回答を分析している。

Q68： 従業員の PC に重要な個人情報や、どのようなソフトウェアやフリープログラムが入っているか把握していますか。（不正ソフトウェア検出）

Q69： Winny などのファイル交換ソフトが PC に入っていると内部情報が外部に公開される危険が大きくなります。PC の監視などの対策をしていますか。（ファイル交換ソフト対策）

Q70： 内部からのメールにより、重要な情報が漏洩することがあります。メールの情報を保存したり、内容によっては送信を抑止できる対策をしていますか。（メールフィルタリング）

Q71： 盗難・紛失による情報漏洩対策として、PC 内の全データを暗号化して、データを読み取ることができなくする方法があります。対応策をとっていますか。（データ暗号化）

Q72： 無線 LAN を使用していて、PC でファイル共有の設定をしていると、外部の人間からファイルが見られてしまうことがあります。これを避けるために暗号化することがます。対応策をとっていますか。（無線 LAN 暗号化）

Q73： 情報漏洩対策として、PC を複数人で使用する場合、各自の ID を利用しファイルアクセスなどの制限をすることができます。対応策をとっていますか。（ID 管理）

Q74： 情報漏洩対策として、PC から外部媒体（USB メモリや CD-R、フロッピーディスクなど）への出力を禁止、管理、制限することができます。対応策をとっていますか。（PC 操作制限）

Q75： 情報漏洩対策として、クライアント PC を最小限の機能のみにし（シンクライアント）、サーバでほとんどの処理を行うようにすることができます。このような対応策をとっていますか。（シンクライアント）

Q76： セキュリティ全体の有効性を評価するサービスがあります。実施していますか。（セキュリティ評価・診断）

Q77： Windows ログイン ID がわからなくても、ハードディスクだけ取り出すと内容を読取ることができるため、盗まれると中味のデータを読み取られることがあります。この情報漏への対応策をとっていますか。（ノート PC 暗号化）

Q78： 機器・媒体廃棄前に残存データを完全に消去しないと、情報漏洩に繋がる恐れがあります。対応策を実施していますか。（データ消去）

Q79：業務外の Web アクセスやメールにこそ、ウィルス感染や情報漏洩の機器が潜んでいます。従業員の作業履歴を収集・解析することが漏洩防止に繋がります。対応策をとっていますか。（ログ収集・解析）

Q80： 情報漏洩抑止のために、従業員のファイルアクセスを管理し監視する仕組みがあります。対応策をとっていますか。（ファイルアクセス管理）

Q81： コピー機で印刷したはずの用紙が紛失し、情報漏洩に繋がることがあります。印刷物についても出力の管理をすることができます。対応策をとっていますか。（ドキュメントセキュリティ）

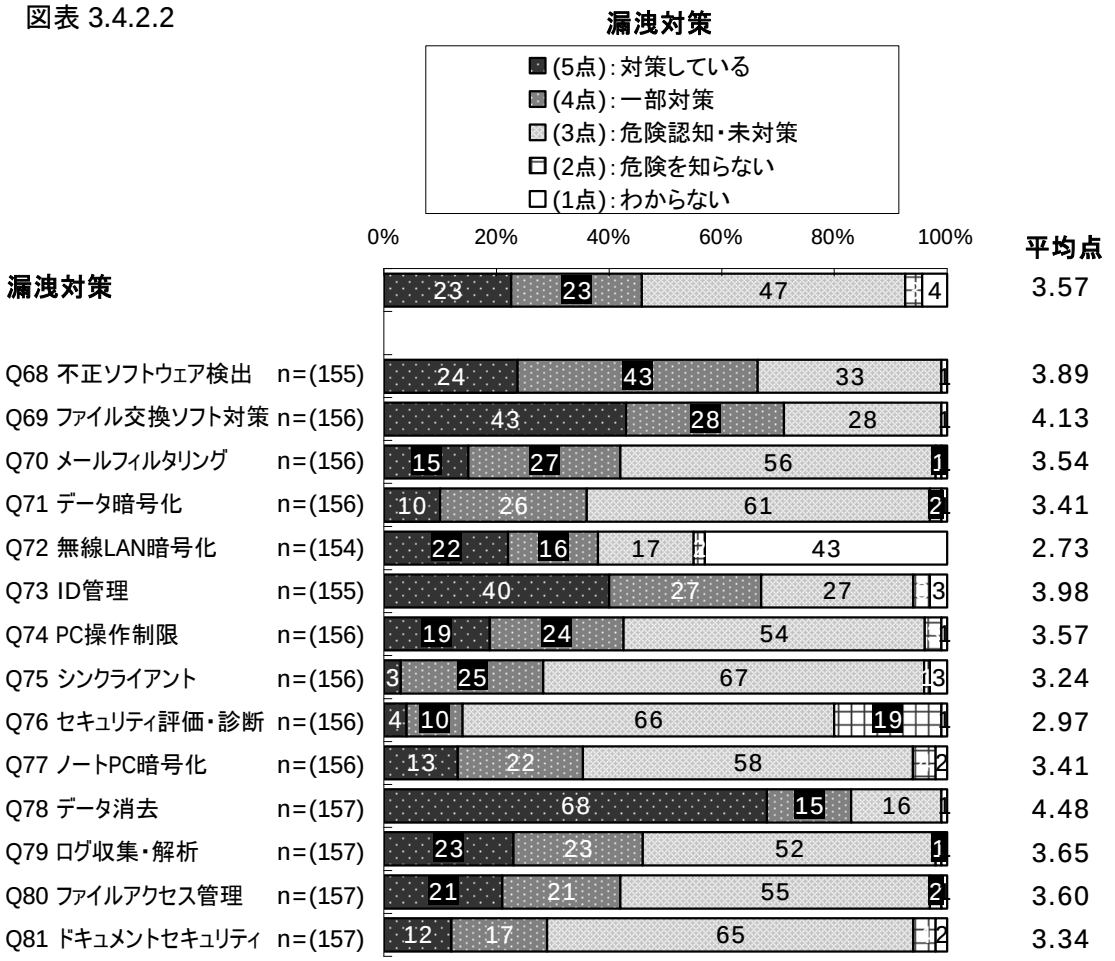
各質問に対する回答の選択肢は微妙に異なるので、それらを表示すると以下のとおりである。

図表 3.4.2.1

漏洩対策	(5点): 対策している	(4点): 一部対策	(3点): 危険認知・未対策	(2点): 危険を知らない	(1点): わからない
Q68 不正ソフトウェア検出	全て把握している	一部把握している	必要性はわかるが把握していない	必要性があることを知らない	わからない
Q69 ファイル交換ソフト対策	対策している	一部対策している	必要性はわかるが対応していない	必要性があることを知らない	わからない
Q70 メールフィルタリング	対策している	一部対策している	必要性はわかるが対応していない	必要性があることを知らない	わからない
Q71 データ暗号化	対策している	一部対策している	危険は知っているが対応していない	危険があることを知らない	わからない
Q72 無線LAN暗号化	対策している	一部対策している	危険は知っているが対応していない	危険があることを知らない	該当しない
Q73 ID管理	対策している	一部対策している	危険は知っているが対応していない	危険があることを知らない	わからない
Q74 PC操作制限	対策している	一部対策している	危険は知っているが対応していない	危険があることを知らない	わからない
Q75 シンクライアント	対策している	一部対策している	危険は知っているが対応していない	危険があることを知らない	わからない
Q76 セキュリティ評価・診断	定期的に実施している	実施したことがある	サービスがあることは知っているが対応していない	サービスがあることを知らない	わからない
Q77 ノートPC暗号化	対策している	一部対策している	危険は知っているが対応していない	危険があることを知らない	わからない
Q78 データ消去	対策している	時々対策している	危険は知っているが対応していない	必要性を感じない	わからない
Q79 ログ収集・解析	対策している	一部対策している	危険は知っているが対応していない	必要性があることを知らない	わからない
Q80 ファイルアクセス管理	対策している	一部対策している	危険は知っているが対応していない	必要性があることを知らない	わからない
Q81 ドキュメントセキュリティ	対策している	一部対策している	危険は知っているが対応していない	必要性があることを知らない	わからない

各質問に対する回答の分布と平均点（上記の選択肢を点数として平均値を算出）は、下記のとおりであった。

図表 3.4.2.2



＊ 図表 3.4.2.2 より、情報の漏洩対策に関する 14 個の質問への回答の全体平均点（選択肢を得点として平均値を算出）は、3.57 点と予想より低い結果であった。
これは、データ消去やファイル交換ソフト対策の平均点が 4.48 点、4.13 点と 4 点を超えているものの、他 12 個の質問のうち 10 個の平均点が 3 点台、2 個（セキュリティ評価・診断、無線 LAN 暗号化）の平均点が 2 点台と低いために、全体の平均点が引き下げられている。

＊ データ消去の質問では、『対策している（5 点）』が 68%、『一部対策（4 点）』と合わせると 83%と実施割合が高い。
これは、機器・媒体廃棄時に残っているデータから情報が漏洩する危険性の認知度が高いことから、対策の実施率が高くなっているものと推測される。

＊ ファイル交換ソフト対策、不正ソフトウェア対策の 2 個の質問では、『一部対策』を含めた実施割合が 67%～71%であり、他の対策に比べると高い。
これは、Winny などの不正なソフトウェアによる情報漏洩被害に対する理解度が高く、優先的に対策を進めているものと推測される。

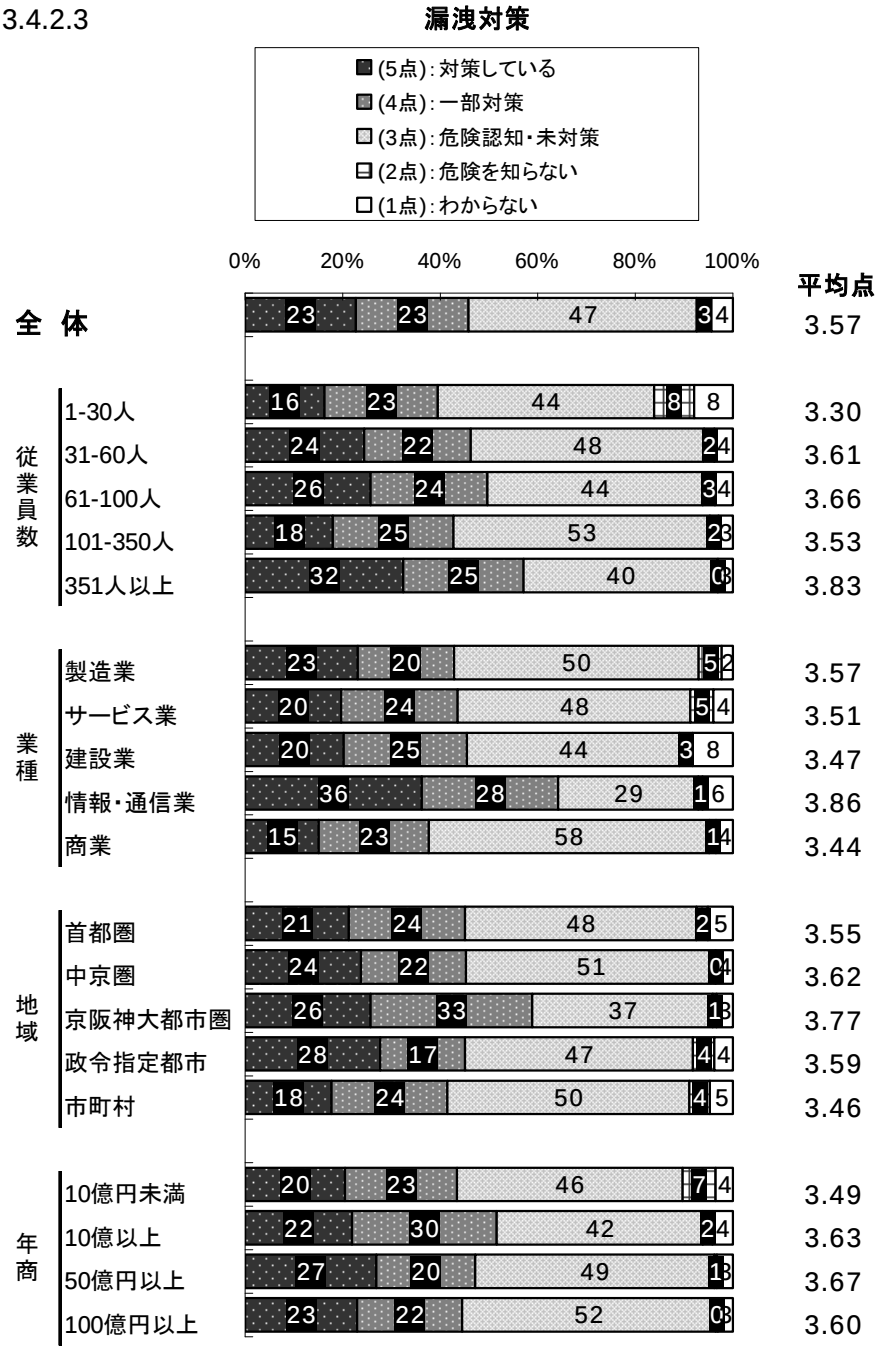
＊ データの暗号化、ノート PC 暗号化、メールフィルタリング、PC 操作制限、ファイルアクセス管理、ドキュメントセキュリティの 6 個の質問では、対策の実施率が低い。
これらについては、『危険認知・未対策（3 点)』との回答が 54%～65%と多いことから、必要性や危険性を理解してはいるが、対策の実施までには至っていないことがうかがえる。
危険性の高い対策を優先して進めているものと推測する。

＊ 無線 LAN の暗号化対策の質問では、43%が『該当しない（1 点)』と回答していることから平均点が 2.73 点と極端に低い結果となっている。
これは、『該当しない』と回答したものは無線 LAN を使用していないと推測されるため、それらを除いて分析すると、『一部対策』を含めた対策の実施割合は約 7 割で、平均点も 4 点に近い値となり対策が遅れているとは言いにくい状況である。

この項目では、一般的に良く知られている機器廃棄時のデータの消去や Winny などの不正なソフトウェアに対する対応は進んでいるが、暗号化などの項目では対策の遅れが目立つ結果となっている。
投資対効果やコストなどの難しい面もあるが、もう一歩進めた対策を推進されることを期待したい。

このデータを従業員数別、業種別、地域別に整理したものが下表である。

図表 3.4.2.3



＊ 従業員数から見ると、従業員が多くなるほど対策が進んでいる傾向にあるが、「101～350 人」の企業においてはその傾向から外れ、若干対策が遅れている。
また、「1～30 人」の企業では、『危険を知らない（2 点)』『わからない（1 点)』と回答している割合が 16%もあるので、このあたりも今後の課題の 1 つになると思われる。

＊ 業種別では、「情報・通信業」の対策が他業種に比べ進んでいるが、『対策している』と『一部対策』を含めた割合でも 64%しかなく、IT 関連業種として見た時には進んでいるとは言いにくい状況である。

他業種も全体的に対策実施率は低い。

＊　地域別では、京阪神大都市圏の対策実施率が高く、中京圏、政令都市、首都圏、市町村ではほとんど差が無い状況である。

首都圏はもっと対策が進んでいることを予想したが、あまり進んでいない結果である。

3.4.3 セキュリティ管理（4.16 節　参照）

この項では、セキュリティ管理についての下記の 5 個の質問への回答を分析している。

Q82： 電源や装置の故障で、PC 内の重要なファイルが壊れたり、なくなったりする場合があります。それに備えてデータバックアップなどの対策をしていますか。
（データバックアップ対策）

Q83： アダルトサイトなど、インターネットで開くことができるページを制限できますが、対応をしていますか。（URL フィルタリング）

Q84： ファイルが改ざんされていないことを保証するひとつの方法として、ファイルに署名ができることが一般化されつつありますが、電子署名を採用していますか。（電子署名）

Q85： 通常のパスワードだけでなく、指紋などの生体認証によりユーザ認証をより強固にする方法があります。対応策をとっていますか。（ユーザ認証強化）

Q86： 災害時のデータ紛失に備えて、重要なデータを別の場所に定期的にバックアップしていますか。（災害対策）

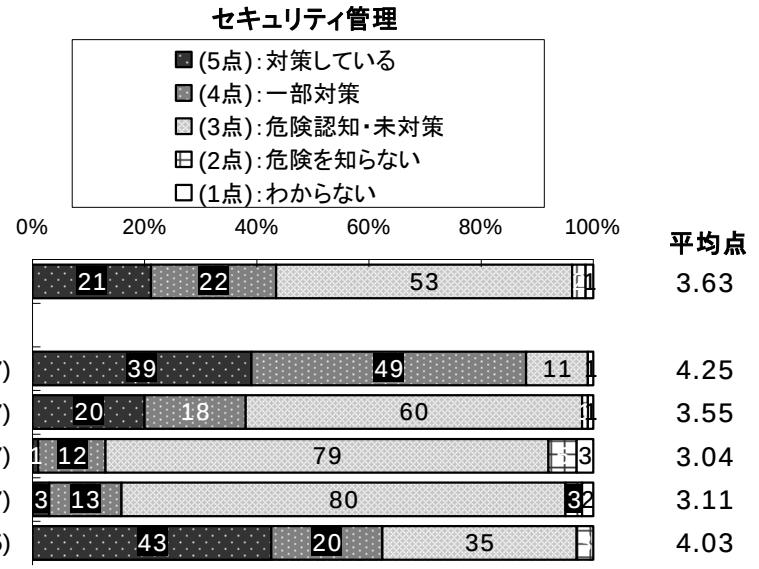
各質問に対する回答の選択肢は微妙に異なるので、それらを表示すると以下のとおりである。

図表 3.4.3.1

セキュリティ管理	(5点): 対策している	(4点): 一部対策	(3点): 危険認知・未対策	(2点): 危険を知らない	(1点): わからない
Q82 データバックアップ対策	対策している	一部対策している	危険は 知っているが 対応していない	危険があることを 知らない	わからない
Q83 URLフィルタリング	対策している	一部対策している	必要性はわかるが 対応していない	必要性が あることを 知らない	わからない
Q84 電子署名	採用している	一部採用している	必要性はわかるが 採用していない	必要性が あることを 知らない	わからない
Q85 ユーザ認証強化	対策している	一部対策している	危険は 知っているが 対応していない	危険があることを 知らない	わからない
Q86 災害対策	定期的に実施・ 保管している	時々実施・ 保管している	必要性はわかるが 実施していない	必要性を感じない	わからない

各質問に対する回答の分布と平均点（上記の選択肢を点数として平均値を算出）は、下記のとおりであった。

図表 3.4.3.2



＊ 図表 3.4.3.2 より、セキュリティの管理に関する 5 個の質問への回答の全体平均点（選択肢を得点として平均値を算出）は、3.63 点と予想より低い結果であった。
これは、データバックアップ対策や災害対策の平均点が 4.25 点、4.03 点と 4 点を超えているものの、URL フィルタリング、電子署名、ユーザ認証強化などの対策実施率が低く、全体平均が引き下げられている。

＊ データバックアップ対策の質問では、『対策している（5 点)』と『一部対策（4 点)』を合わせた割合が 88%と高い。
これは、一般的にシステム運用上データのバックアップは、業務の一環として運用作業に組み込まれていることが多いことから、実施率が高い結果になっているものと推測される。

＊ URL フィルタリング、電子署名、ユーザ認証強化の 3 個の質問では、『危険認知・未対策（3 点)』の割合が 60%～80%と多いことから、対策の実施率が低い結果となっている。
これは、危険性は認知しているが、投資効果やコスト面などからもう一歩踏み込んだ対策までには至っていないものと推測される。

＊ 災害対策の質問では、『対策している』と『一部対策』を合わせた割合が、63%と他対策よりは高い。
このデータの保管については、データバックアップ対策と関連性が高いことから、比較的に対策実施率が高くなっていると推測する。

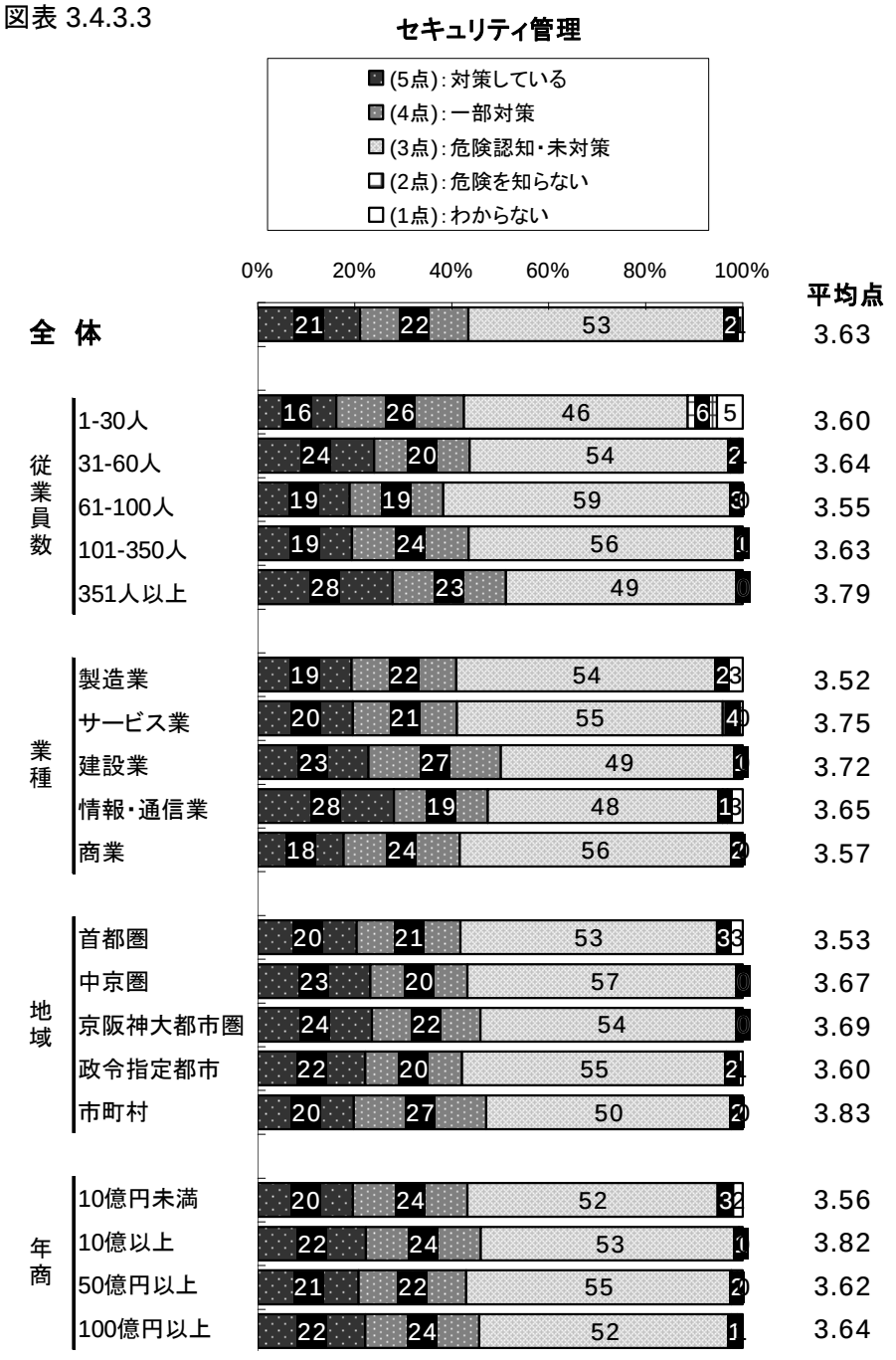
この項目では、セキュリティ対策の基本ステップに位置するデータの保護については対策実施率が高い。しかし、もう一歩進めた対策に位置付けられる URL フィルタリング、電子署名、ユーザ認証強化については、対策の遅れが目立っている。

情報管理は個人情報保護や企業機密情報保護という情報漏洩防止の観点から、企業にとって必要不可欠なセキュリティ対策であり、今後の積極的取り組みを期待する。

また、各ベンダにおいても防止策につながるサービスメニューを含めたコンサルタントをさらに強化し、企業のセキュリティ対策に貢献されることを望みたい。

このデータを従業員数別、業種別、地域別に整理したものが下表である。

図表 3.4.3.3



＊　従業員数から見ると、バラツキがあるものの従業員が多くなるほど対策の実施割合が高くなる傾向にある。

＊　業種別では、『対策している』割合だけで見ると「情報・通信業」の対策が進んでいるが、『一部対策』を含めた割合では「建設業」の方が進んでいる。
予想したIT関連業種である「情報･通信業」の対策が先行しているとはいいにくい結果である。

＊　地域別では、地域による情報の浸透度や対策の実施割合を捉えるために、5つの地域に分けて分析を行ったが差は少なく、全国同じような傾向である。

3.4.4 物理的セキュリティ（4.17 節　参照）

この項では、物理的セキュリティについての下記の 5 個の質問への回答を分析している。

Q87： 外部からの不審者の侵入に備え、監視カメラや警備員の常駐、また入館者をチェック・記録していますか。（入退館管理）

Q88： 部外者が重要なシステムを設置した部屋へ入室するのを制限したり、記録したりする仕組みはありますか。（入退室管理）

Q89： IC カードなどで、建物・サーバ室・システムへのアクセスを一元的に管理するシステムがあります。導入していますか。（アクセス管理）

Q90： 大規模災害時に重要システムの稼動を確保するため、別拠点に予備のシステムを設置し、業務を続ける対策があります。この対策をとっていますか。（システム冗長化）

Q91： システム障害時にシステムを短時間で復旧し、業務を継続するための二重化などの対策・手順は確立していますか。（業務継続対策）

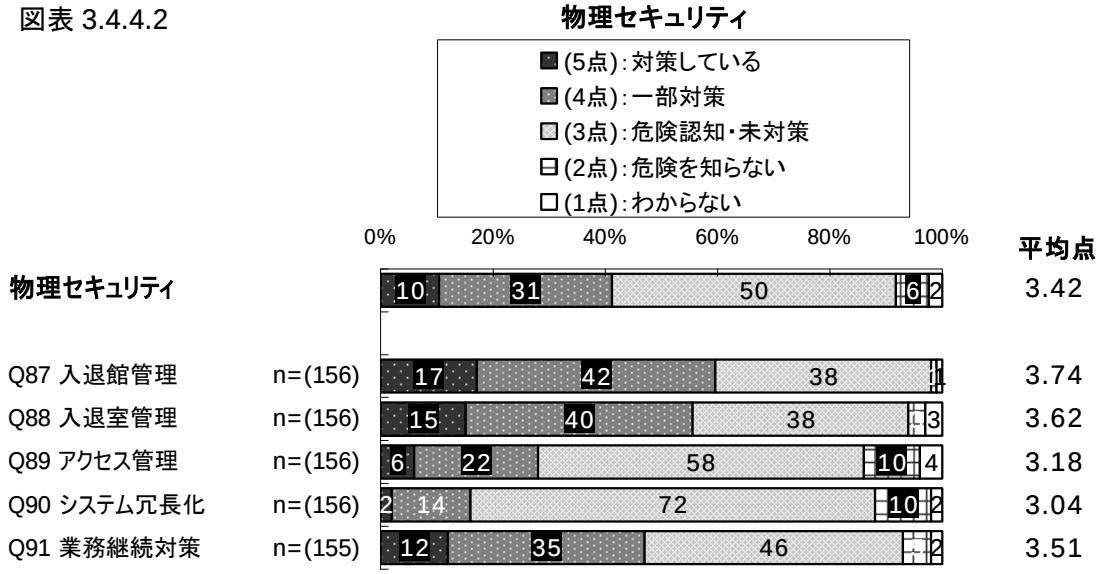
各質問に対する回答の選択肢は微妙に異なるので、それらを表示すると以下のとおりである。

図表 3.4.4.1

物理セキュリティ	(5点): 対策している	(4点): 一部対策	(3点): 危険認知・未対策	(2点): 危険を知らない	(1点): わからない
Q87 入退館管理	365日・24時間 対応している	全てではないが 対応している	必要性があることを 知っているが 対応していない	必要性があることを 知らない	わからない
Q88 入退室管理	365日・24時間 対応している	全てではないが 対応している	必要性があることを 知っているが 対応していない	必要性があることを 知らない	わからない
Q89 アクセス管理	全面的に 導入している	一部導入している	必要だと思うが 導入していない	必要性を感じない	わからない
Q90 システム冗長化	対策している	一部対策している	危険は知っているが 対応していない	必要性を感じない	わからない
Q91 業務継続対策	対策している	ハードディスク のみ対応している	危険は知っているが 対応していない	必要性を感じない	わからない

各質問に対する回答の分布と平均点（上記の選択肢を点数として平均値を算出）は、下記のとおりであった。

図表 3.4.4.2



＊ 図表 3.4.4.2 より、物理的なセキュリティ対策に関する 5 個の質問への回答の全体平均点（選択肢を得点として平均値を算出）は、3.42 点と予想より低い結果であった。
これは、5 個全ての質問の平均点が 3 点台で、その中でもアクセス管理とシステムの冗長化の平均点が 3.18 点、3.04 点と極端に低いことから、全体平均が引き下げられている。

＊ 入退館管理、入退室管理の 2 個の質問では、外部からと内部からの情報流出を防止するために必要な基本的対策であるが、平均点は 3.74 点、3.62 点と予想より低い結果であった。
これは、『危険認知・未対策（3 点)』の回答割合が 38%と多いことから、危険性は理解されているものの、まだ、対策までには至っていない企業が多いことがうかがえる。

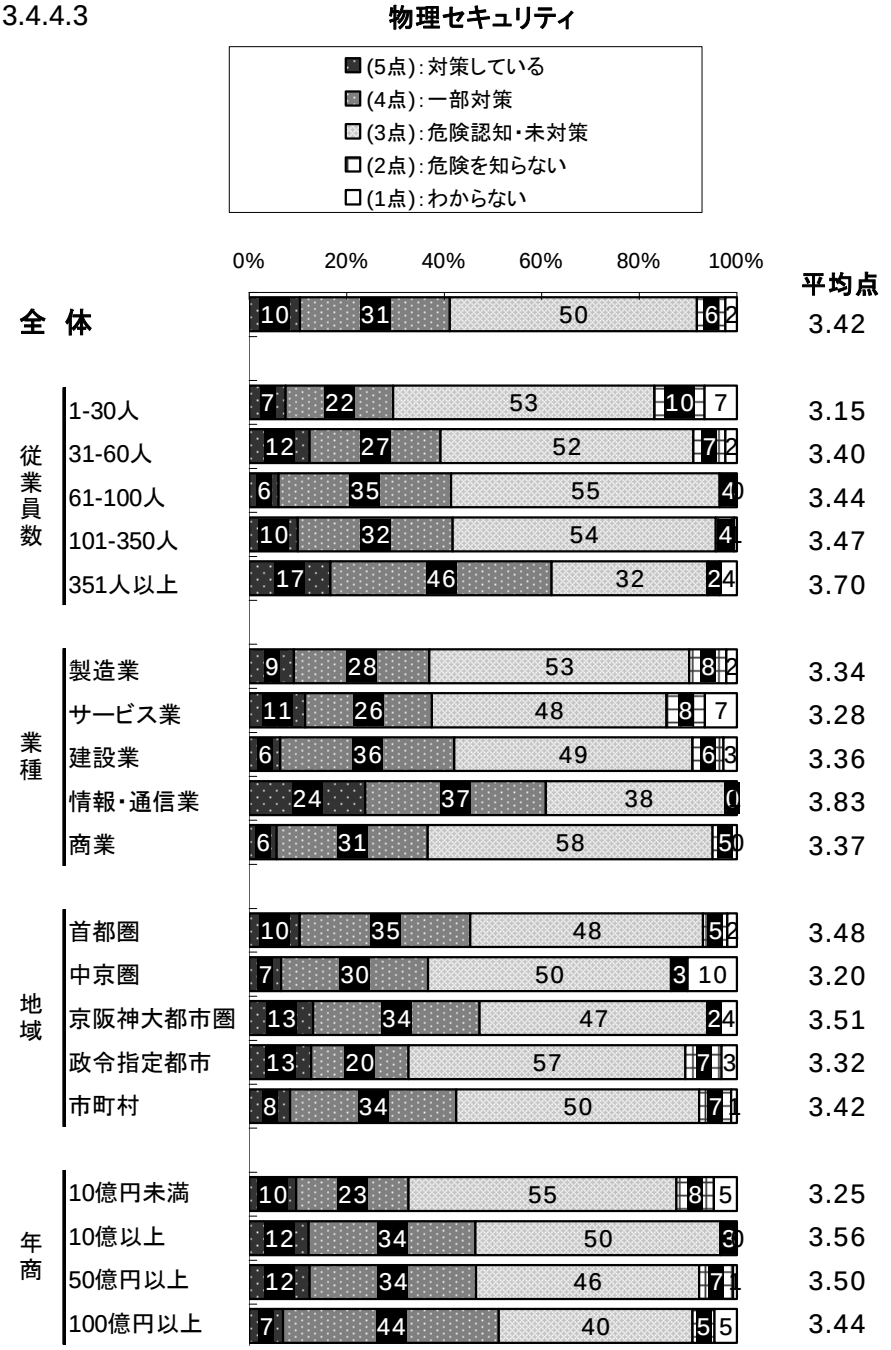
＊ アクセス管理、システム冗長化の 2 個の質問では、『対策している（5 点)』と『一部対策（4 点)』をあわせてもアクセス管理 28%、システム冗長化 16%と実施割合が低いことから、平均点が極端に低くなっている。
これは、『危険認知・未対策』の回答がアクセス管理 58%、システム冗長化 72%となっていることから、危険に対する認知度は高いものの予備システム設置などへの対策は、投資対効果やコスト面でなどの要因で遅れているのではないかと推測される。

＊ 業務継続対策の質問では、『対策している』と『一部対策』をあわせた割合が 47%あるものの、『危険認知・未対策』と回答したものも 46%あり、約半分の実施率である。
また、対策していると回答した中でもハードディスクのみでの対応割合が 35%と高く、より安全なシステムの二重化などで対策を行っているのは 12%にすぎない。ここでも投資対効果の面が大きく係わっているものと推測される。

物理的なセキュリティ対策についても、セキュリティ管理と同様に認知度が高いものの全体的にあまり対策が進んでいない。投資効果が曖昧かつコストがかかりすぎるという問題もあるが、被害の局限化や法令遵守の観点からもセキュリティ対策に積極的に取り組まれることを期待したい。

このデータを従業員数別、業種別、地域別に整理したものが下表である。

図表 3.4.4.3



＊ 従業員数から見ると、従業員が多くなるほど対策の実施割合が高くなる傾向にある。
「351 人以上」の企業においては、『一部対策』を含めた実施割合が 63%と高い。

＊ 業種から見ると、「情報・通信業」の対策実施割合が他業種に比べ全項目で進んでいる。これは IT 関連業種であることから予想された結果である。
また、業務継続対策においては「製造業」の対策が進んでいる。IT が製造事業に組み込まれるなどで、製造ラインの停止が企業の大きなリスクとなることから、他業種よりも対策が進んでいるものと推測される。

＊ 地域別で見ると、「京阪神大都市圏」「首都圏」の順で対策実施率が高く、他地区においてはほとんど差が無い。

3.4.5 人材と組織（4.18 節 参照）

この項では、情報セキュリティ対策を支える人材と組織についての下記の 4 個の質問への回答を分析している。

Q11： 会社としてのセキュリティ方針を示すことは、従業員の意識向上に大きく役に立ちます。従業員へ徹底すべき、会社としてのセキュリティ方針を持っていますか。
（セキュリティポリシ）

Q12： 情報セキュリティの基準として ISO があり、認証を取得することが企業の信用を、より確実にする場合があります。認証の取得が必要ですか。 （ISO 認証取得支援）

Q13： 万が一のセキュリティ事故に備え、何かしらの対策を施していますか。セキュリティに関する保険があることを知っていますか。 （セキュリティ保険）

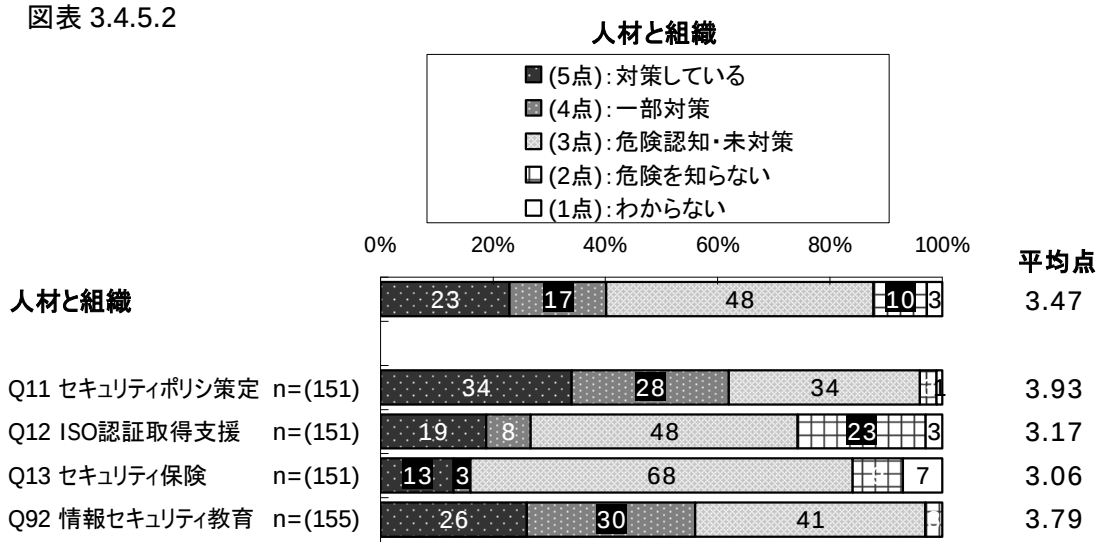
Q92： 情報セキュリティについては、定期的に注意喚起を行うことが、意識向上に繋がります。定期的に従業員に情報セキュリティ教育を行っていますか。 （情報セキュリティ教育）

図表 3.4.5.1

人材と組織	(5点): 対策している	(4点): 一部対策	(3点): 危険認知・未対策	(2点): 危険を知らない	(1点): わからない
Q11 セキュリティポリシ策定	方針を定め定期的に見直しをしている	方針を定め示したが見直しをしていない	必要とは思うが決めていない	必要性を感じない	わからない
Q12 ISO認証取得支援	既に認証を取得している	取得の準備を進めている	必要とは思うが意思決定をしていない	必要性を感じない	わからない
Q13 セキュリティ保険	既に保険に入っている	保険に入る準備を進めている	必要とは思うが決めていない	必要性を感じない	わからない
Q92 情報セキュリティ教育	定期的に教育を行っている	教育を行ったことがある	教育は必要だが行っていない	教育が必要だと思わない	わからない

質問に対する回答の割合と平均点（選択肢を得点として平均値を算出）は以下のとおりであった。

図表 3.4.5.2



＊ 図表 3.4.5.2 より、人材と組織に関する 4 個の質問への回答の全体平均点（選択肢を得点として平均値を算出）は、3.47 点と予想よりも低い。
これは、4 個の質問全ての平均点が 3 点台と低く、また、ISO 認証取得支援は 3.06 点、セキュリティ保険は 3.17 点と極端に低いことから、全体平均点が大きく引き下げられている。

＊ セキュリティポリシの質問では、セキュリティ方針を定めていると回答した割合が 62%とあるものの、必要性を知っているが対策していないとの回答も 34%あり、大半が必要との認識にあることがうかがえる結果となった。

＊ 情報セキュリティ教育の質問では、教育を行っていると回答した割合が 56%あるものの、行っていないと回答した割合も 44％と半数近くある。
また、教育を行っていないと回答した中でも大半は必要性を認識しているので、さらに教育が推進されることを期待したい。

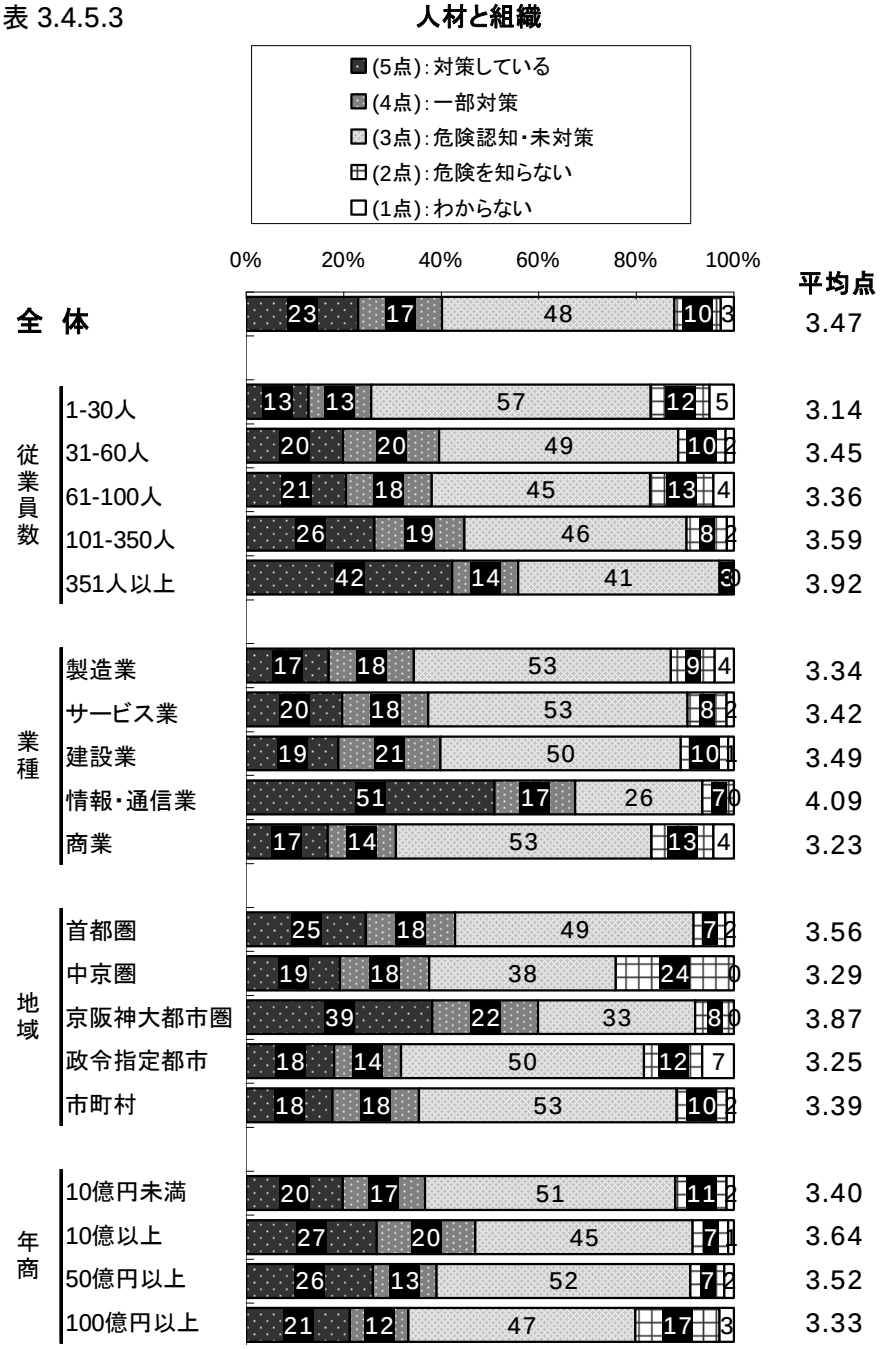
＊ ISO 認証取得支援、セキュリティ保険の 2 個の質問では、ISO 認証取得は取得済みと取得の準備を進めていると回答した割合は 27%、セキュリティ保険は加入済みと準備を進めていると回答した割合が 16%しかなく、あまり進んでいない状況である。
しかし、必要と思うと回答した割合も、それぞれ 48%、68%と多く認識は高いことがうかがえる。

企業のセキュリティ対策を支えるのは従業員であり、企業が定めたセキュリティ方針に基づき従業員が高い意識を持って活動することが重要である。組織として従業員に教育を行う仕組みの構築と教育の実施を推進されることを期待したい。

また、企業の信頼度を高める ISO 認証取得、不測の事態への対策としての保険加入も選択肢のひとつである。

このデータを従業員数別、業種別、地域別に整理したものが下表である。

図表 3.4.5.3　　人材と組織



＊　従業員数から見ると、従業員が多くなるほど対策の実施率が高くなる傾向にある。
「351 人以上」の企業においては、他企業に比べて対策が進んでいることがうかがえる。

＊　業種から見ると、IT 関連企業である「情報・通信業」は予想通り対策実施率が高い。
他業種においては若干のバラツキはあるものの、ほとんど差がない状況である。

＊　地域から見ると、「京阪大都市圏」が抜き出て対策割合が高い。他地域においてはほとんど差が見られない。

3.5 面接調査のまとめ

3.5.1 面接調査について

前述したとおり、今年度もアンケートの結果を補強する目的で対象企業を選定して面接調査を実施した。補強のポイントは、下記の 3 点である。

＊ 運用強化・セキュリティ対策に取組んだ動機について
＊ 対策の目的の達成度合いや効果・成果・満足度について
＊ 対策実施に際して、苦労した点や工夫した点について

面接調査の対象企業のアンケートへの回答結果を今年度作成の診断ツールによりグラフ表示すると下図のとおりである。小さな点とそれを繋ぐ破線がアンケートへの全回答の平均点数であり、大きな点とそれを繋ぐ実線が当該社の回答の点数である。

企業番号 74 を除いては、各社共に平均点数を上回る点数であるが、これは、各社が運用強化・セキュリティ対策にあたって、実施している工夫のヒントを確かめるためのインタビューであることによる。

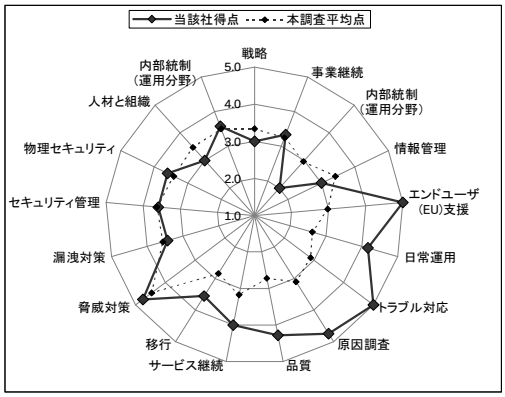
企業番号 74 は、戦略から情報管理までの 4 項目について無回答であり、その他の項目についてはそのほとんどが 3 点である背景を確かめるために対象に選んだものである。

面接調査にあたっては、当該社のグラフを持参し、上記の補強ポイントを中心とするインタビューを行った。その結果を一言でいえば、次のとおりである。

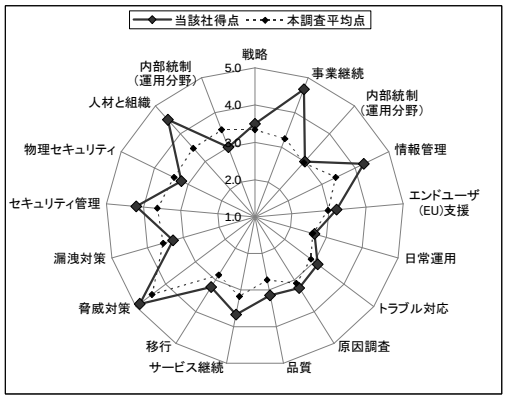
＊ 平均点数を上回る得点を挙げている企業へのインタビュー結果の特徴は、経営者の IT への関心が高い点と、担当者も積極的に自らの工夫を経営者に提言して、経営者が担当者の提言を取り上げている点で、全社的、組織的な対応ができている。
＊ それらの対応は、「運用強化・セキュリティ対策」においてだけではなく、IT の「戦略的活用」や「経営上の効果の向上」においても発揮されている。
＊ 一方、得点のほとんどが 3 点である（担当者任せである）企業の背景は、経営者、情報システム管理者、担当者等との提言や情報収集に対する運営体制が整えられていないので、担当者の提案は全社的、組織的な対応には至らず、任された担当者だけがあらゆる場面で苦心惨憺している。

概要は以下に項を改めて、ポイントごとにインタビューの結果をまとめてある。

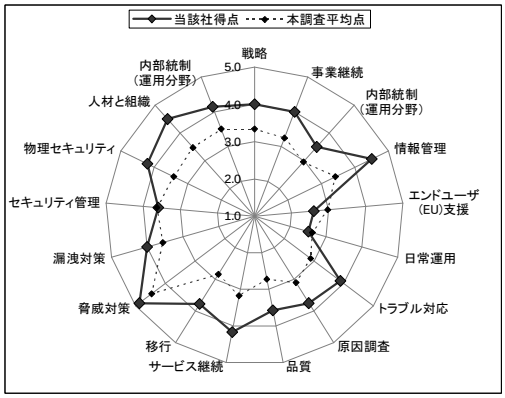
企業番号 22



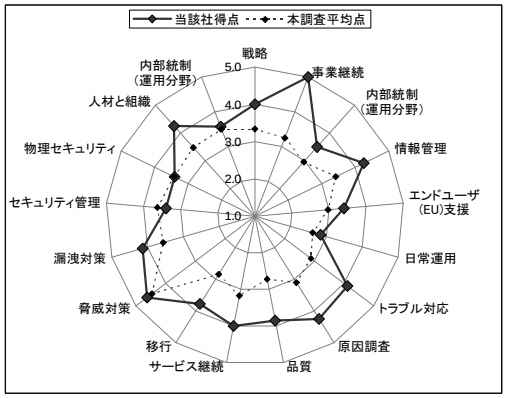
企業番号 34



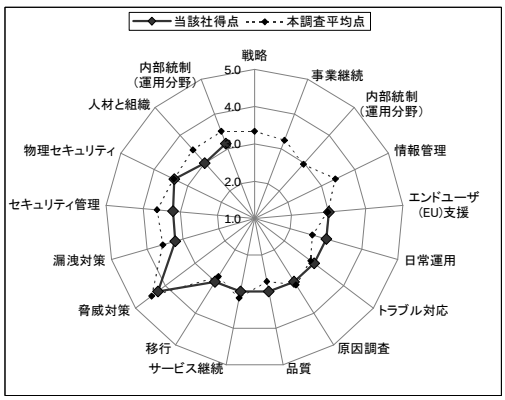
企業番号 47



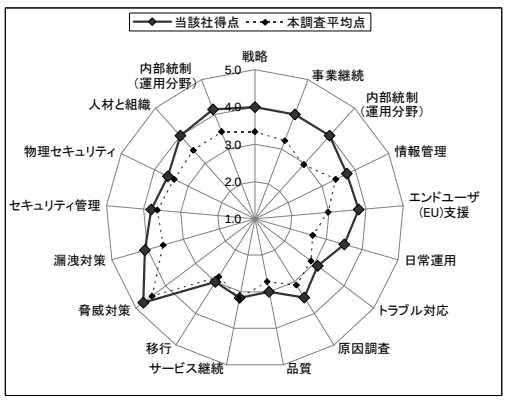
企業番号 72



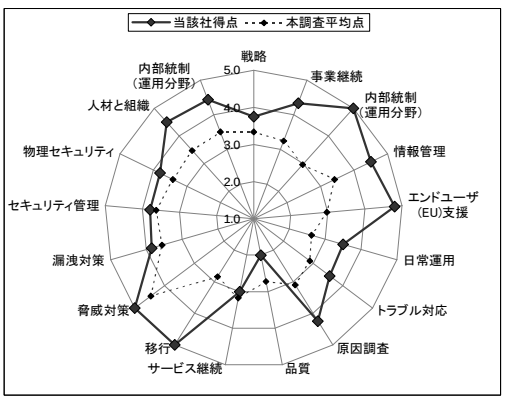
企業番号 74



企業番号 89



企業番号 98



3.5.2 運用強化・セキュリティ対策に取組んだ動機について

「得意先・取引先から経営者が指導され、取引の継続や拡大のために対策に踏み切った」との回答が最も多く、中には得意先・取引先から審査を受けている企業もあり、「期限付きで改善指示ポイントを上回らないと取引に大きな支障をきたす」という企業もあった。

この回答も、経営者が得意先・取引先の指導を理解して、「企業姿勢の強化も含め積極的に進めて来た企業」と、必ずしも理解していないけれども、「やむなく、進めて来た企業」とに大別される。しかし、双方とも「結果的には取組んで良かった」という点では共通している。

個人情報保護法、新会社法の施行と間もなく始まる日本版 SOX 法などのコンプライアンス強化や内部統制などに対する義務化が、中堅・中小企業まで着実に影響し始めていることがうかがえる。なお、同様に外部監査人の指導で取組んだという企業もあった。

また、対策を進めてきたが、コスト面の問題もあるので、「どこまでやるべきかの基準を知りたい」という指摘もある。

「運用」、「セキュリティ」ともに社員全般が関わることであるので、対策の一貫として、「社員教育が重要な課題」になっている。

これへの取組みについては、「当初は自前の研修計画を策定し取組んだ。しかし、外部のメジャーな教育機関で受講させる方が信用度も上がるので、昨今は教育機関を利用している」との回答もあった。

しかし、「地方都市ではメジャーな教育機関はあるのかとの疑問や教育機関の明示を求める声もある。また今後は段階的な定例教育やタイムリーな受講のためのｅラーニングも視野に入れていく」との声もあった。

社内の情報システムや IT 業務が広範化してきているので、IT の安全・安心の重要性とそのための「運用強化・セキュリティ対策の必要性を情報システム部門が経営者に対して提案し、説得した」という回答も多くあった。

一方では未対策企業は経営者の理解が得られなかった企業もあるが、それらの企業においても「情報システム部門の大半は重要性を理解している」ことが把握できた。

経営者が自ら IT を使う企業は、情報システムや安全・安心の運用強化・セキュリティ対策の重要性を得心していると共に、安定稼動やレスポンスの速さなどにも高い関心を持っていることが把握できた。経営者のパソコン活用促進が理解への最大の近道だと思われる。

アンケートのあらゆる項目で平均点数を上回る企業へのヒアリングのひとつに、得意先の指導で ISMS 認証を取得した所もあった。年商 20 億・従業員 100 名弱の企業であるが、社員啓蒙やコンサルタントによる教育の徹底から始め、入念な社員との話し合いを進めながら、取得し運営してきており、取得後各部署より 1 名選出の委員会を設置し、一層の意識改革を図りながら現在に至り、ほぼ完璧な対策が確立されていた。今でも話し合いは実施中で、「週 1 回の朝礼に抜き打ちで、選出された委員から安全・安心の話をさせている」とのことで、その徹底ぶりに驚かされた。今後は委員を一定の周期で交代させ、全員が一枚岩となるように更なる強化を進めるとのことであった。

安全・安心の IT 化を進めて来た結果として、さらに安全・安心を進めるべく別会社を設立し、アウトソーシングに踏み切った企業もあった。この別会社は今後教育の徹底を図るうえで、ｅラーニングも準備中とのこと。情報システムも大変高度で、極力紙を出さな構造で、データでのやり取りが主体のシステムとしていた。つまりパソコンが操作できないと仕事ができない仕組みを構築しており、この仕組みが従来のオフコンシステムをオープンシステムに移行する時に大いに役立ったとのことであった。

3.5.3 対策の目的の達成度合いや効果・成果・満足度について

運用強化に取組んだ企業の多くは、「障害が減り、障害時の復旧時間も短縮した」という効果を上げており、目に見える効果として満足度も高い。一方、セキュリティ対策を進めた企業では、「効果が良く見えない」ことから満足度も若干低い状況であった。

しかしながら社員のコンピュータ利用状況の監視をすることで、「ウィルス侵入や情報漏洩がなくなった」という意見が多かった。反面、社員との信頼関係の問題から、監視することへのためらいも併せ持っている。

取引先の要請で改善に踏み切った企業については、取引が減ることもなく順調に取引が進んでいる点から判断して、効果があったと考えているとの回答も多かった。

運用強化・セキュリティ対策への取組みについて、企業の満足度を 100 点満点で答えてもらったところ、上述の通り、「運用強化は効果が見える」ことから 70 点以上が大半で、中には 100 点を出す企業もあった。ただし、「セキュリティ対策においては、効果がみえにくい」という点と「コストが掛かる」という点で 50～60 点の評価を出す企業が多かった。

また、テナントビルに入居している企業では、入退室管理の面で物理的対策が思うように進められないという点でセキュリティに対する評価は更に低かった。

3.5.4 対策実施に際して、苦労した点や工夫した点について

「社員の不満を和らげることに苦労した」との回答が一番多く、教育や話し合い、そして親切で迅速な対応など工夫を凝らし、不満を緩和させているとのことであった。「新しいことをする時は常に不満はつきもので、時が解決をする」との回答もあった。逆に、「話を訊き過ぎるのも足並みなどが揃わなくなる原因となることもあるので、バランスが重要」との声もあった。

新しいことを進めた場合の結果としては総じて「当初は不満が高かったが、今では感謝されている」とのことであり、社員がほとんどは、「元には戻れない、元に戻すと困る」というように、便利さを理解しているとのことであった。

また、「対策をどこまでやったら認められるのか」、「投資対効果の観点で経営者にどのように理解してもらうか」などに苦労・工夫している情報システム部門の姿もあった。このために色々な情報を集めている企業も多く、情報提供を強く要望していた。

3.5.5 今後の課題

「運用強化・セキュリティ対策」を中心とする今後の課題・問題点について聞いた中で、平均点数が高い企業であってもたくさんの課題や問題意識があることがわかる。それらを以下に列挙しておく。

- ＊ 「対策予算」の確保
- ＊ 運用強化・セキュリティ対策の「投資対効果」の視点
- ＊ 運用強化・セキュリティ対策の「社員教育」
- ＊ 「コンプライアンス」関連の社員教育
- ＊ 取引先との関連も含めて、「国際標準」への対応
- ＊ 社員教育への「e ラーニング」の適用
- ＊ 運用強化・セキュリティ対策の「人材」の育成・確保

ユーザ企業のこれらの課題解決に際して、IT 事業者が保有・具備している情報やサービスを提供することによって、産業競争力強化の視点で、しかるべき貢献をすることを期待したい。

4 調査内容

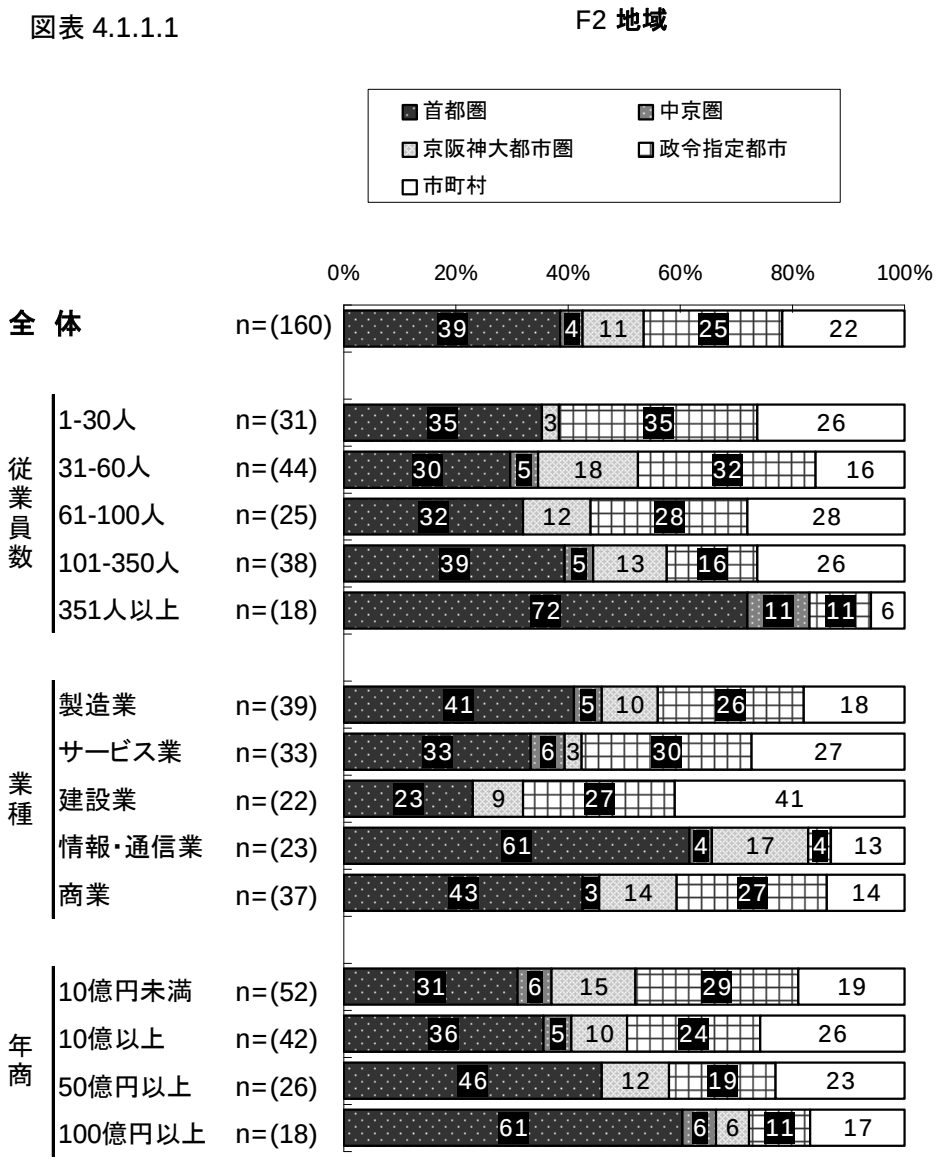
4 調査内容

4.1 回答企業の属性

4.1.1 地域

- 全体で見ると、『首都圏』が 39%と最も多い。
- 従業員規模別で見ると、「351 人以上」で『首都圏』が 72%と非常に多くなっている。
- 業種別に見ると、特徴的な部分は「建設業」では『市町村』が最も多く 41%、「情報・通信業」では『首都圏』が最も多く 61%となっている。

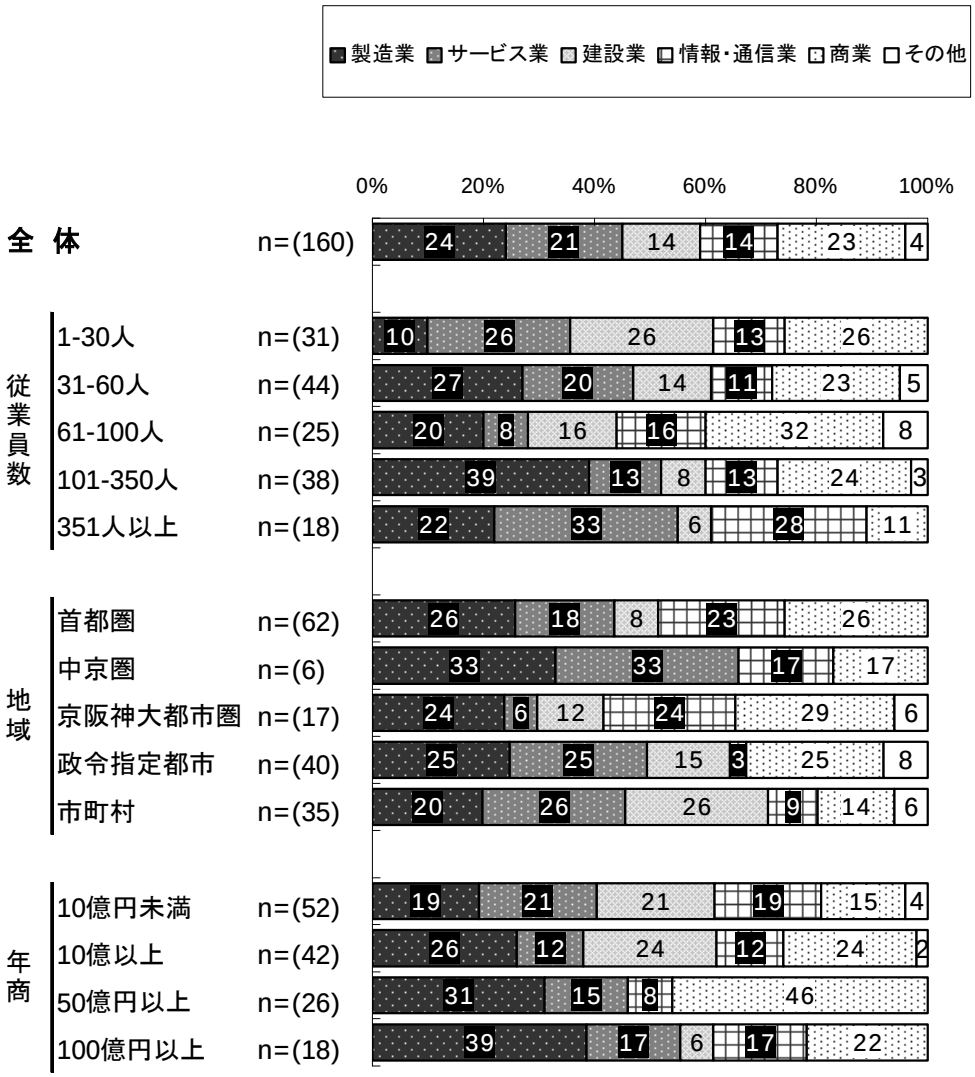
図表 4.1.1.1



4.1.2 業種

- 全体で見ると、『製造業』が 24%と最も多く、ついで『情報・通信業』が 23%、『サービス業』が 21%となっている。
- 従業員規模別に見ると、「1～30 人」では『建設業』が多く、「61～100 人」では『商業』が多く、「101～350 人」では製造業が多いなどの特徴が見られる。

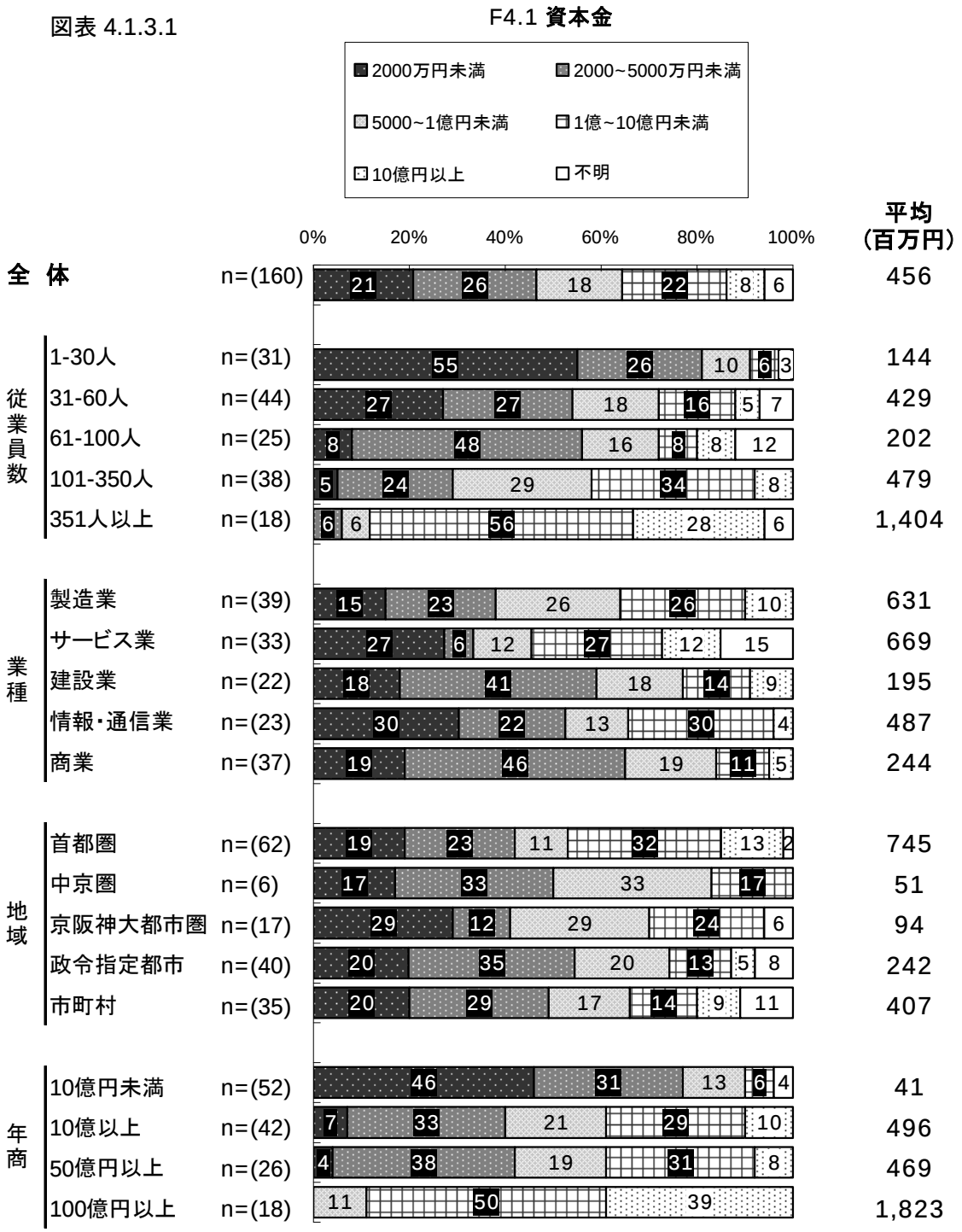
図表 4.1.2.1 F3 業種



4.1.3 資本金

- 全体で見ると、資本金の平均値は 456 百万円となっている。
- 従業員規別で見ると、規模が大きくなるにつれて、資本金は大きくなっている。
- 業種別に見ると、「建設業」で 195 百万円、「商業」で 244 百万円と他の業種と比べて低くなっている。

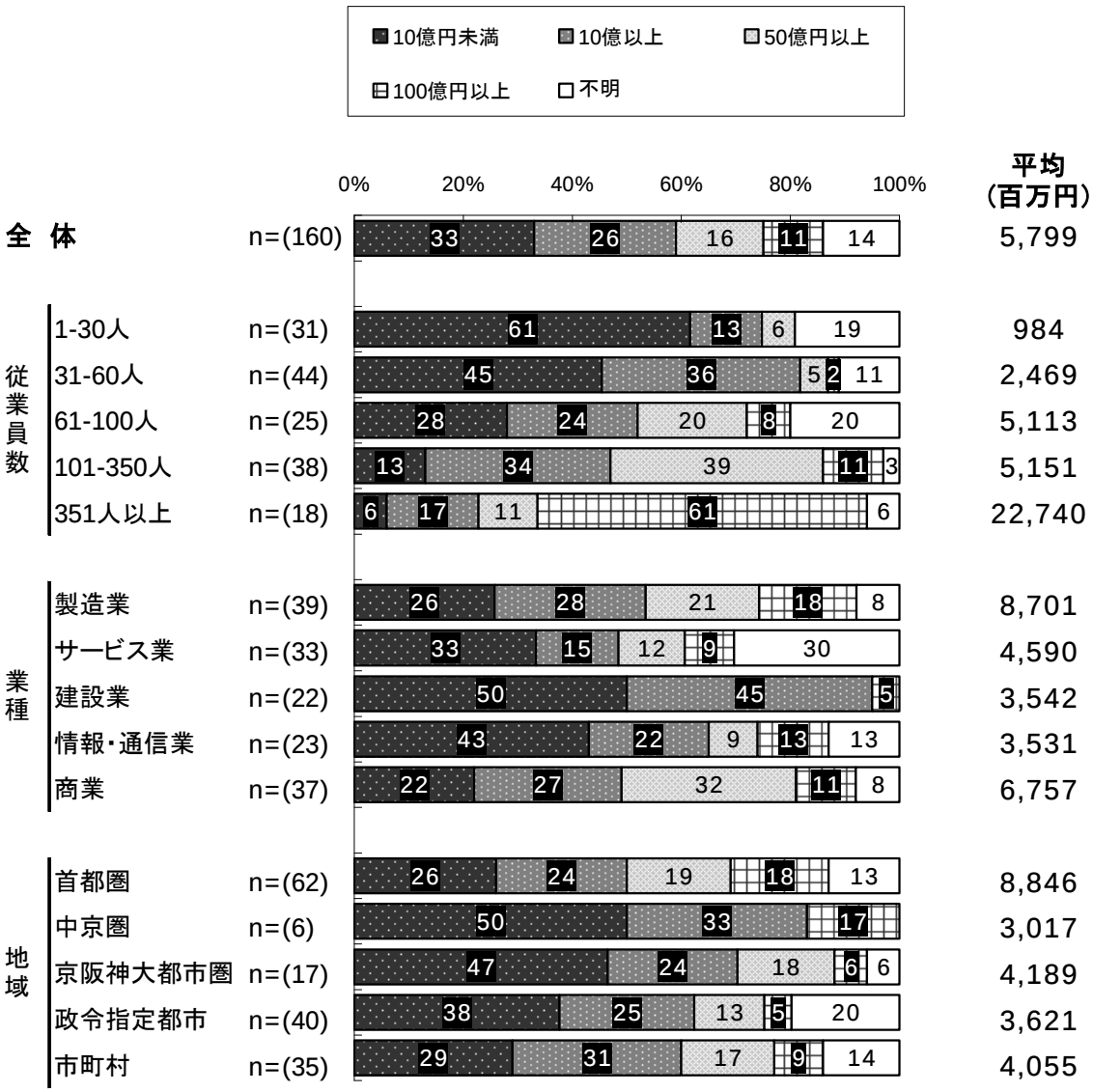
図表 4.1.3.1



4.1.4 年商

- 全体で見ると、年商の平均値は 5,799 百万円となっている。
- 従業員規模別に見ると、規模が大きくなるにつれて年商は高くなっている。
- 業種別に見ると、「製造業」で平均値が 8,701 百万円と他の業種とひかくして高くなっており、「建設業」と「情報・通信業」で他の業種と比較して低くなっている。

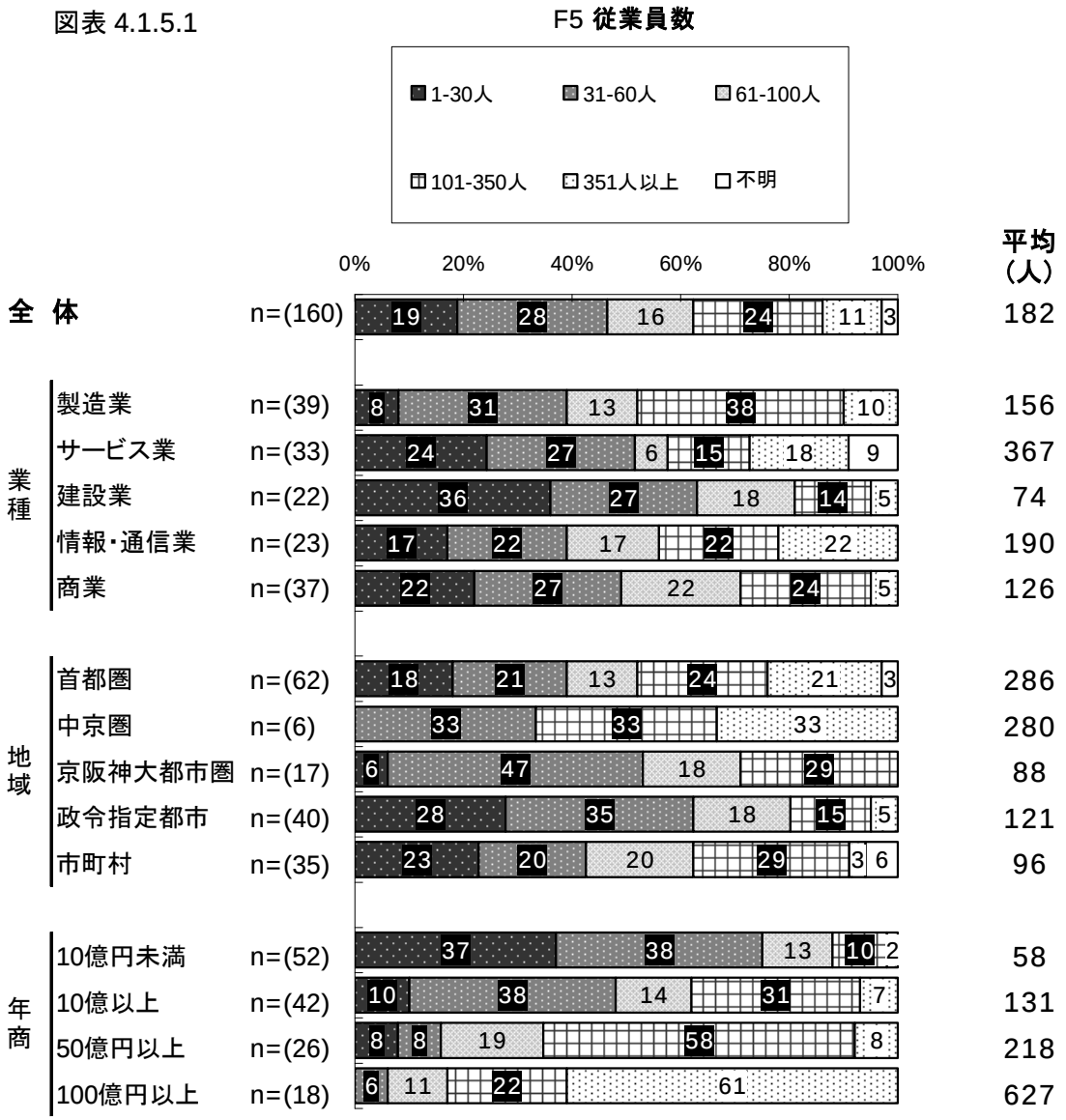
図表 4.1.4.1　F4.2 年商



4.1.5 従業員数

- 全体を見ると、従業員数の平均は 182 人となっている。
- 業種別に見ると、「サービス業」で 367 人と他の業種と比較して高くなっている。

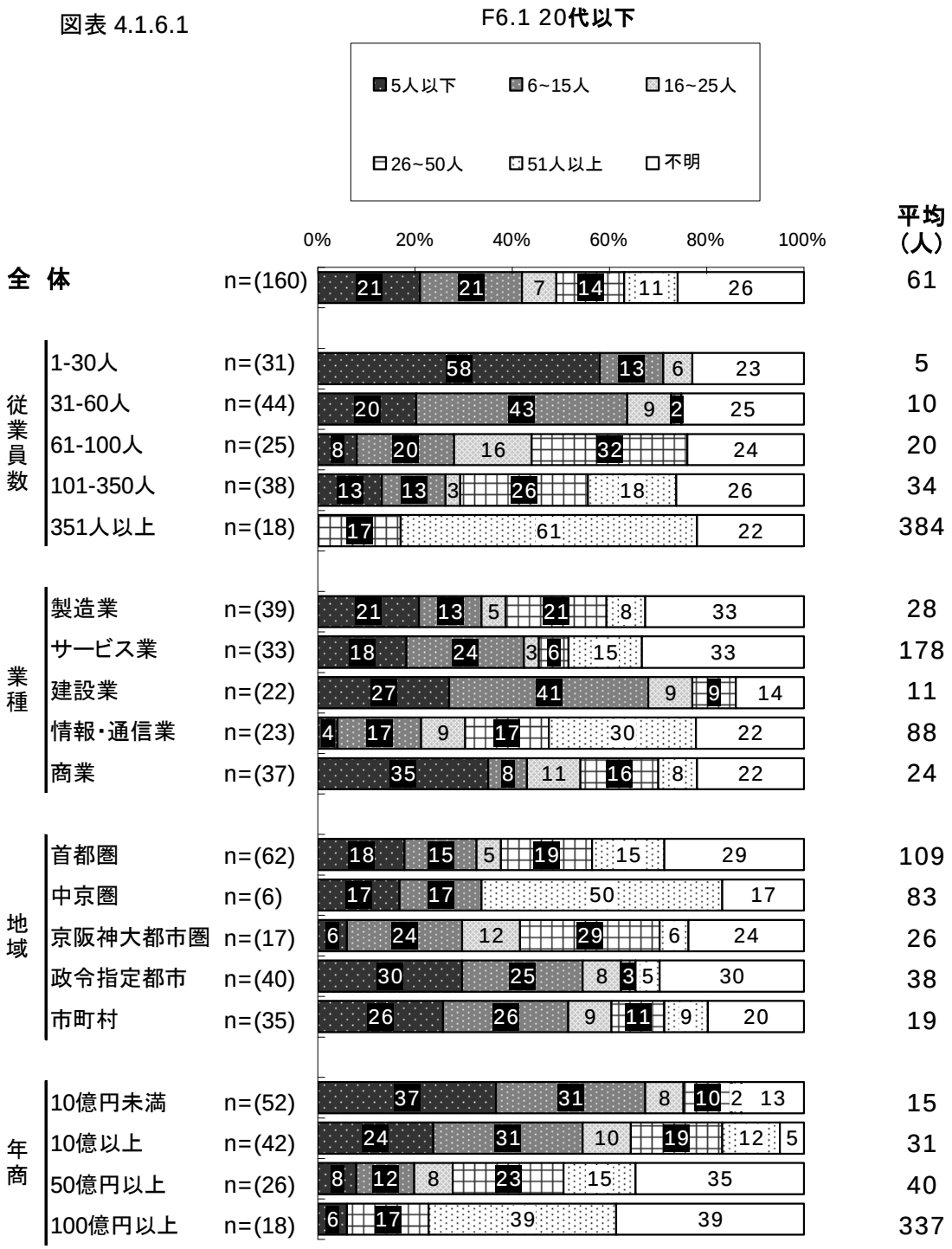
図表 4.1.5.1



4.1.6 従業員数 20 代以下

- 全体で見ると、20 代以下の従業員数は平均で 61 人となっている。
- 業種別に見ると、「サービス業」で最も高く平均で 178 人、「建設業」で最も低く 11 人となっている。

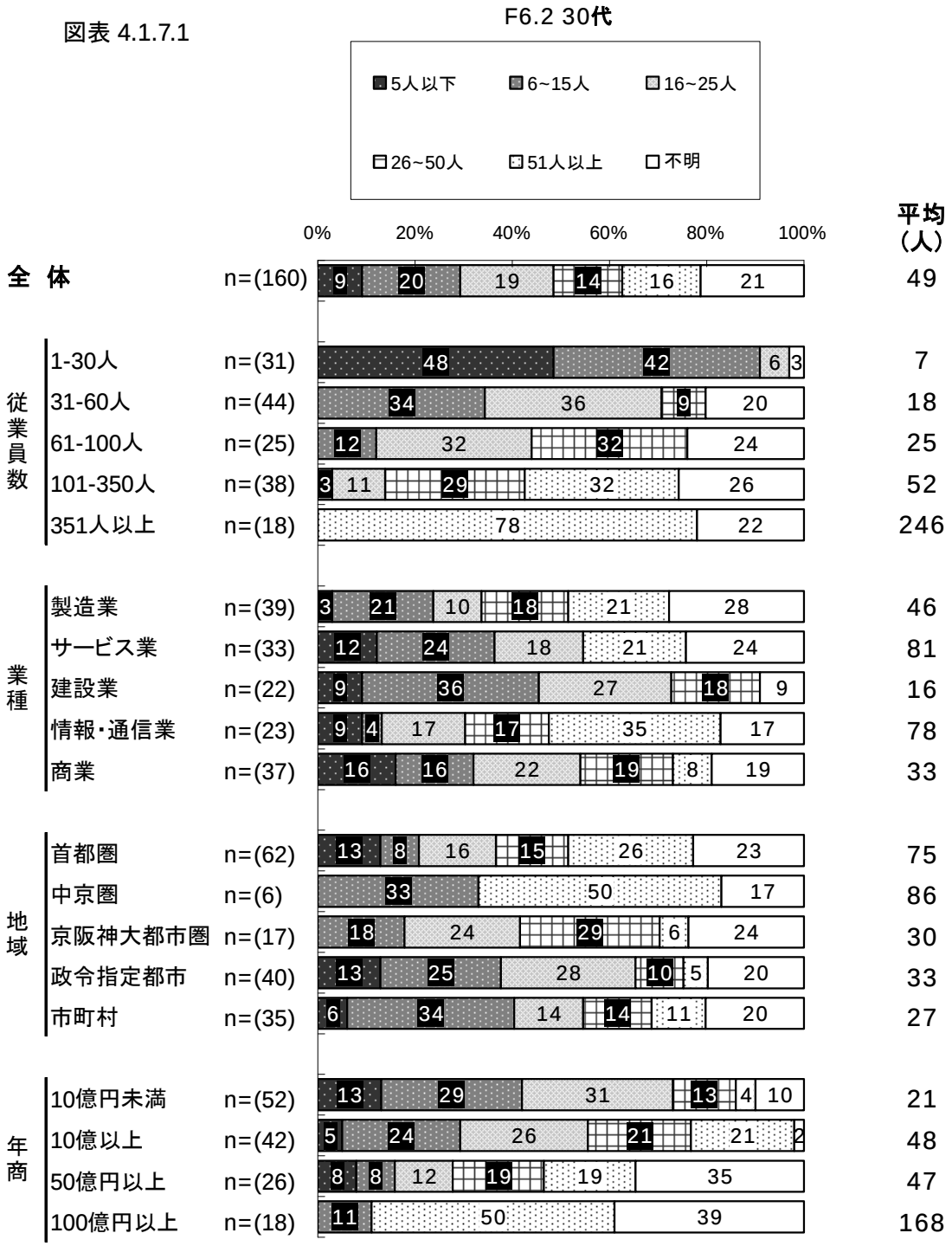
図表 4.1.6.1



4.1.7 従業員数 30 代

- 全体で見ると、30 代の従業員数は平均で 49 人となっている。
- 業種別に見ると、「サービス業」で 81 人「情報・通信業」で 78 人と高くなっており、「建設業」で最も低く 11 人となっている。

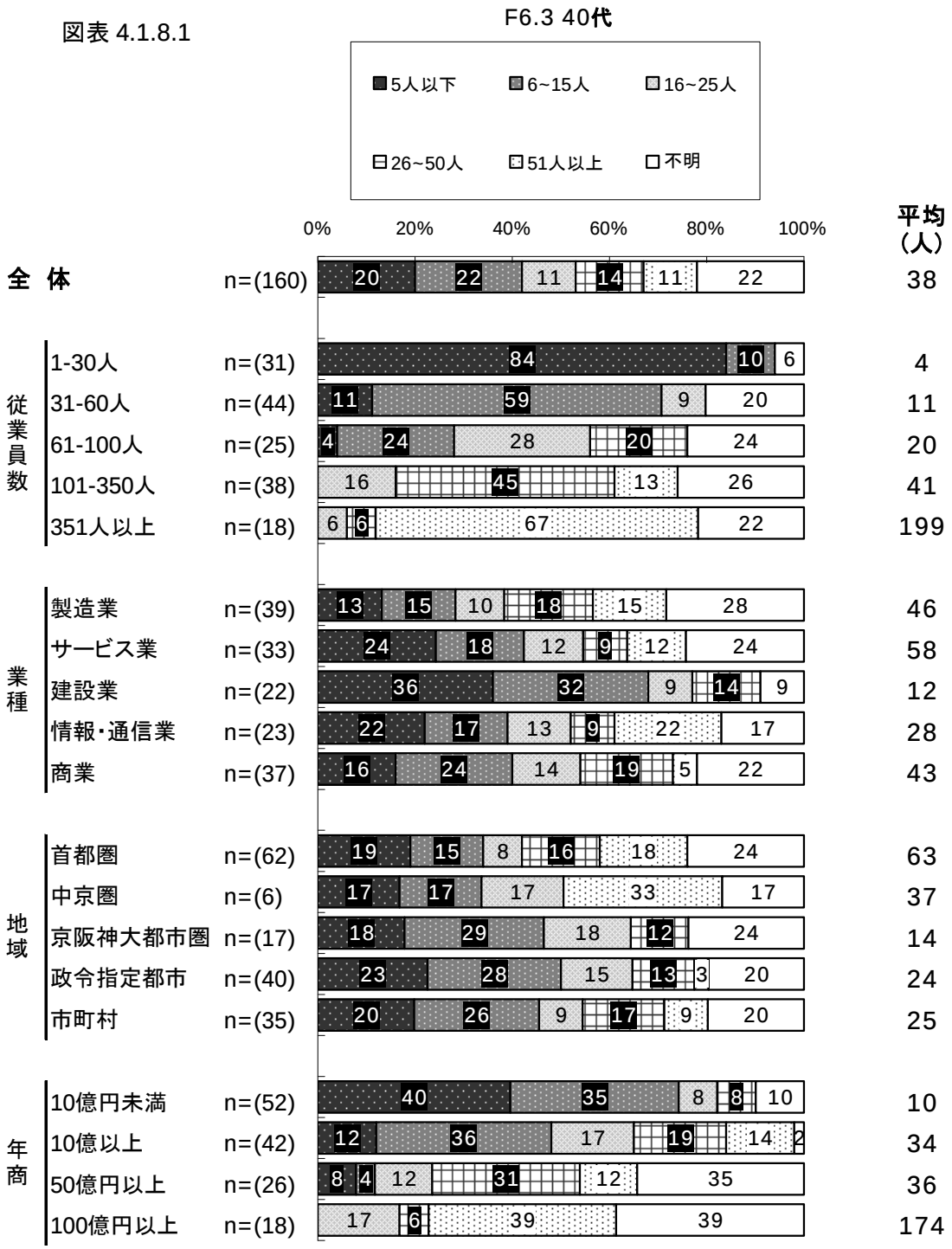
図表 4.1.7.1



4.1.8 従業員数 40 代

- 全体で見ると、40 代の従業員数は平均で 38 人となっている。
- 業種別に見ると、「サービス業」で 58 人「製造業」で 46 人、「商業」で 43 人の順に高くなっている。

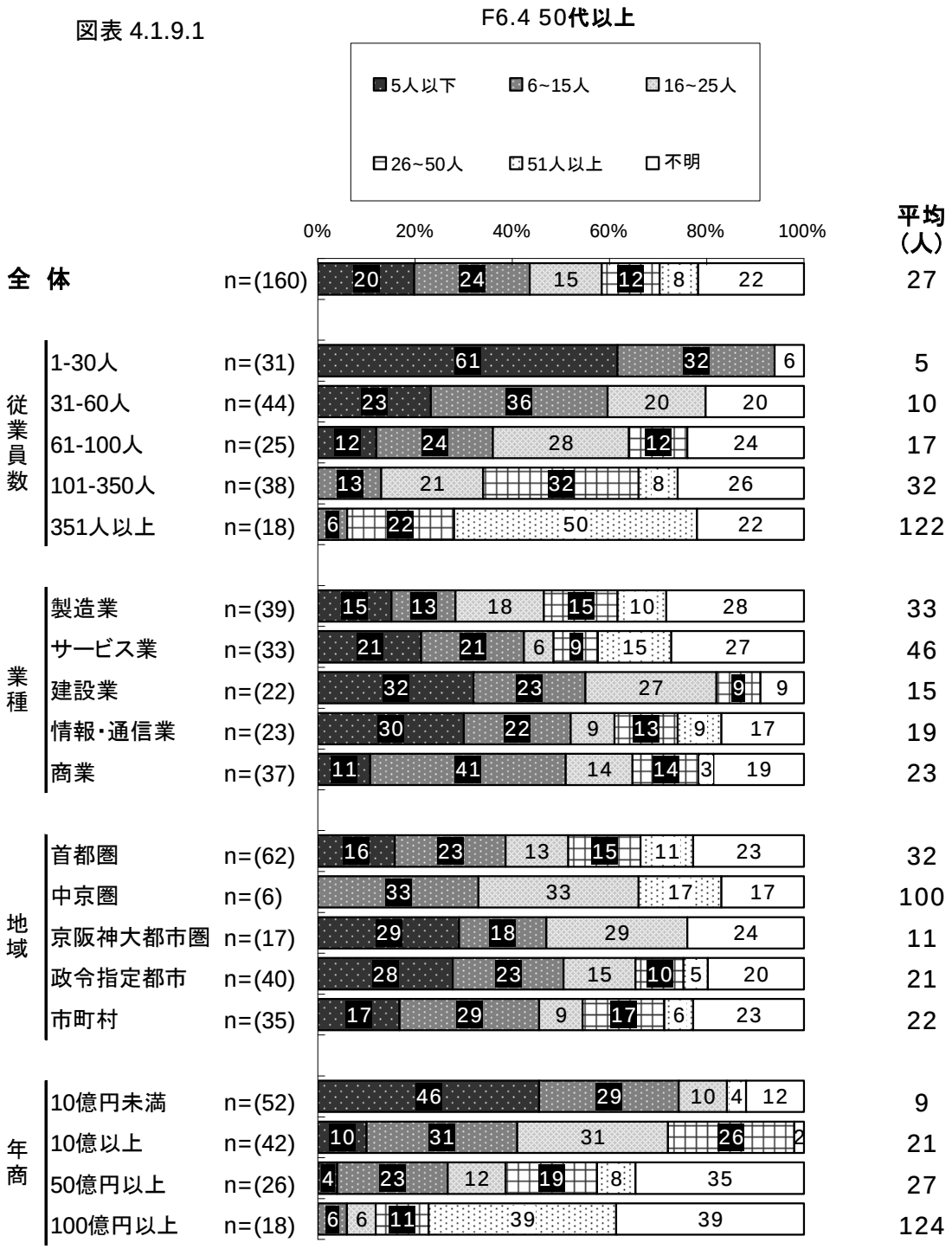
図表 4.1.8.1



4.1.9 従業員数 50 代以上

- 全体で見ると、40 代の従業員数は平均で 38 人となっている。
- 業種別に見ると、「サービス業」で 58 人「製造業」で 46 人、「商業」で 43 人の順に高くなっている。

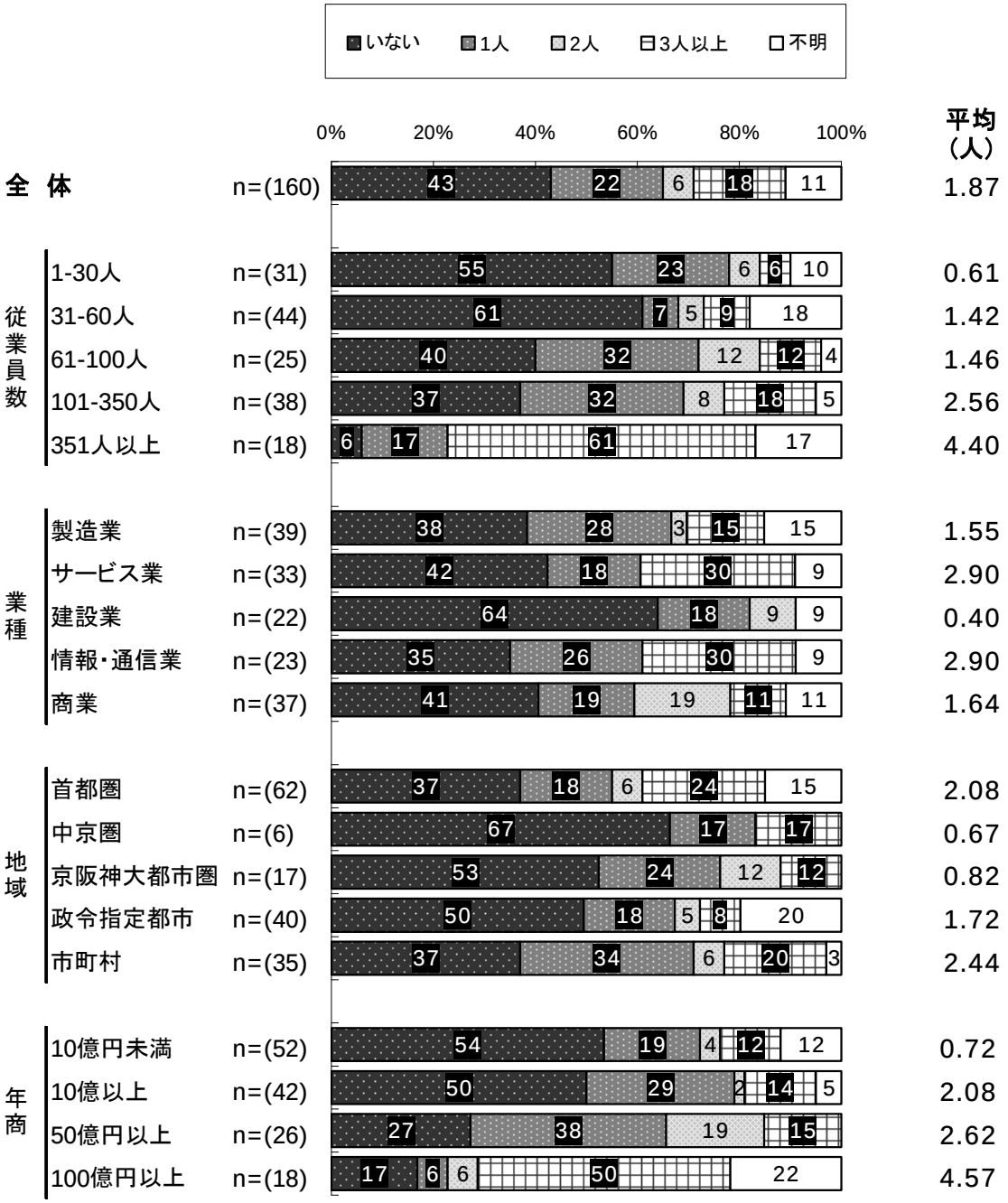
図表 4.1.9.1



4.1.10 情報システム専任担当者

- 全体で見ると、『いない』の比率が 43%と最も高くなっている。平均では 1.87 人となっている。
- 従業員規模別に見ると、『いない』の割合が高いのは「1～30 人」と「31～60 人」となっている。逆に「351 人以上」では『いない』の比率が 6%と非常に低く、平均は 4.40 人と高くなっている。

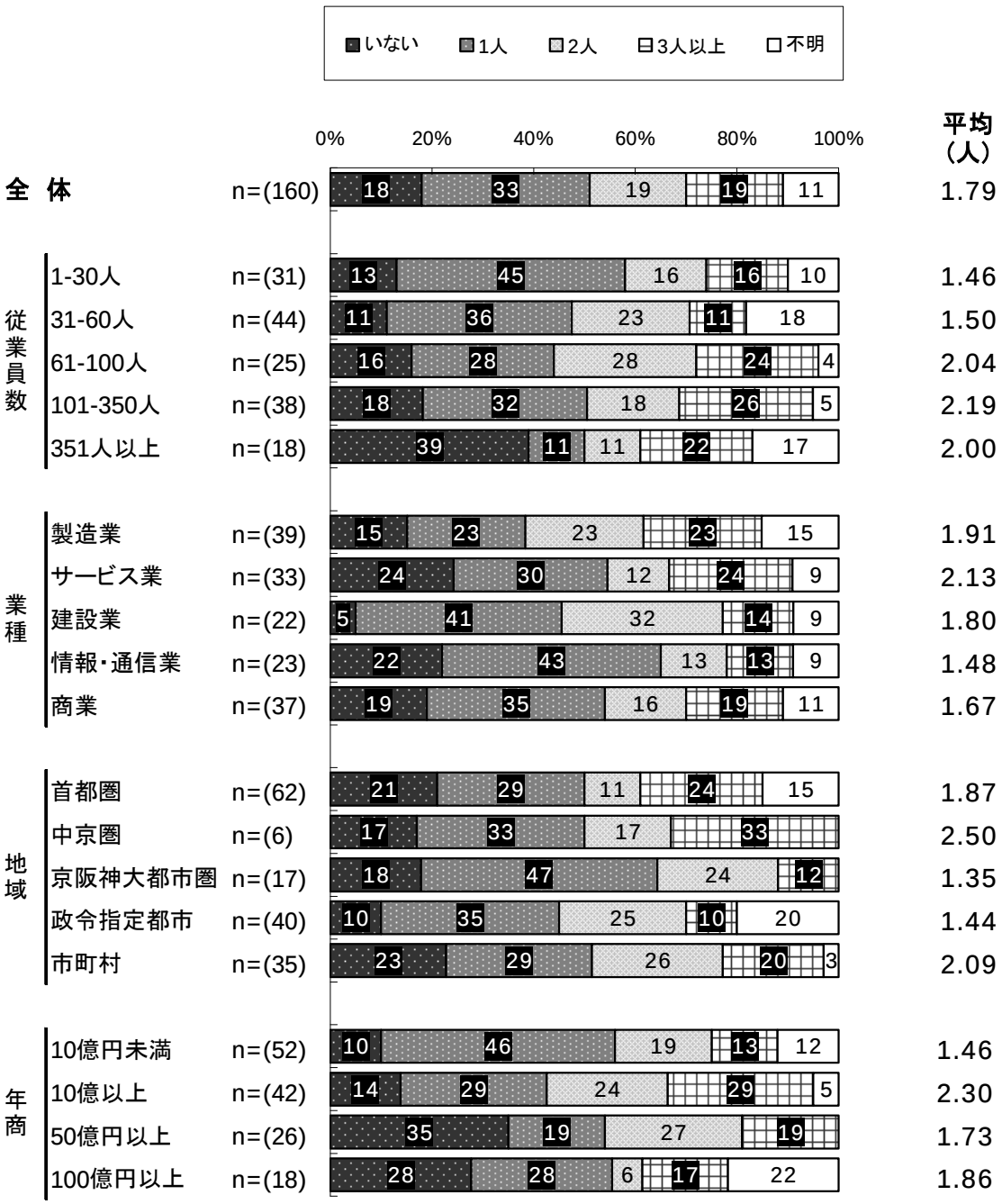
図表 4.1.10.1　　F7.1 **情報システム専任担当者**



4.1.11 情報システム兼任担当者

- 全体で見ると、『1 人』の比率が 33%と最も高くなっている。平均では 1.79 人となっている。
- 従業員規模別に見ると、350 人以下の企業では『1 人』の割合が最も高くなっている。「351 人以上」の企業では、『いない』の割合が 39%と最も高くなっている。

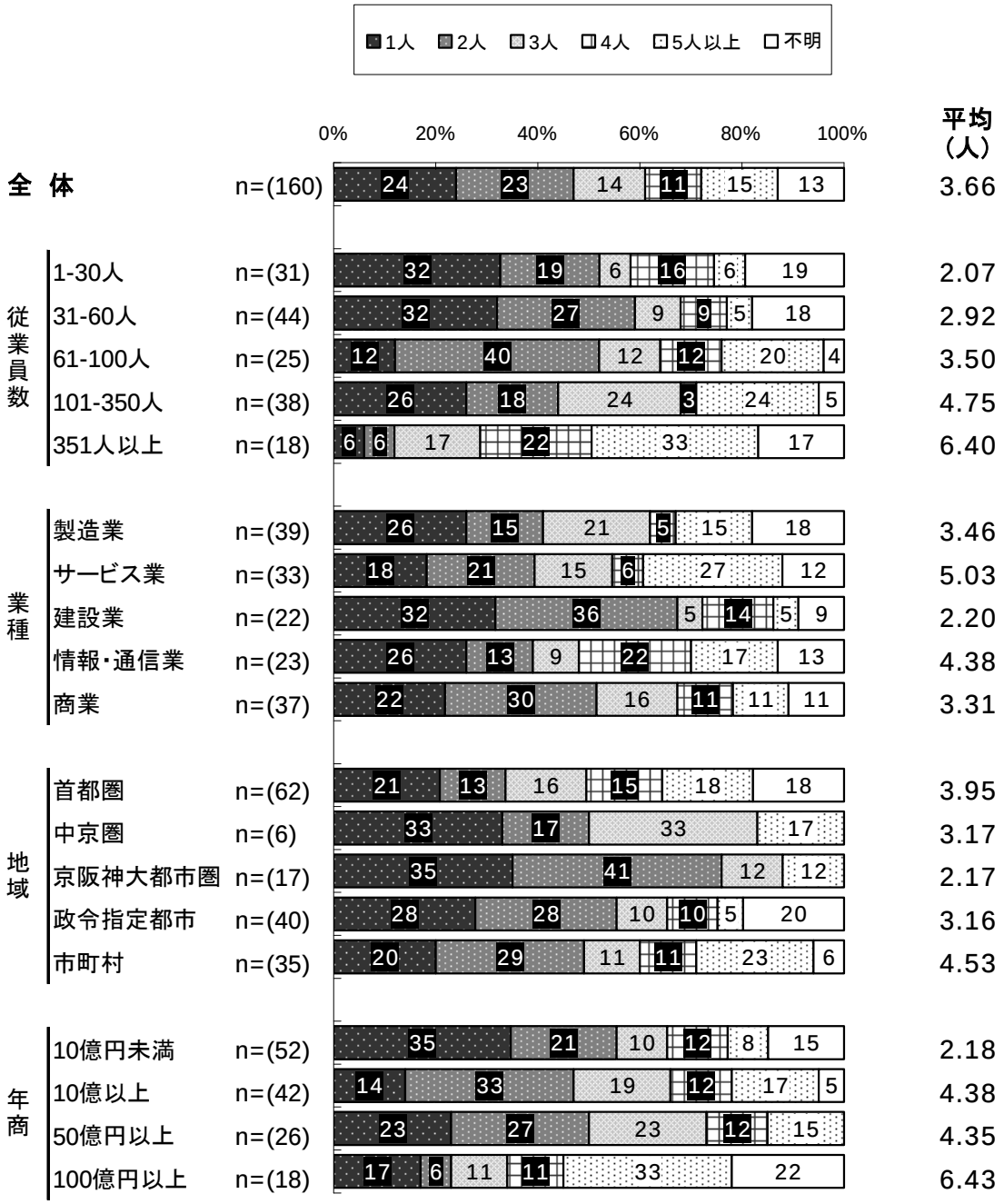
図表 4.1.11.1　　F7.2 情報システム兼任担当者



4.1.12 情報システム担当者合計

- 全体で見ると、『1 人』の比率が 24%と最も高くなっている。平均では 3.66 人となっている。
- 従業員規模別に見ると、規模が大きくなるにつれて平均の人数は多くなっている。

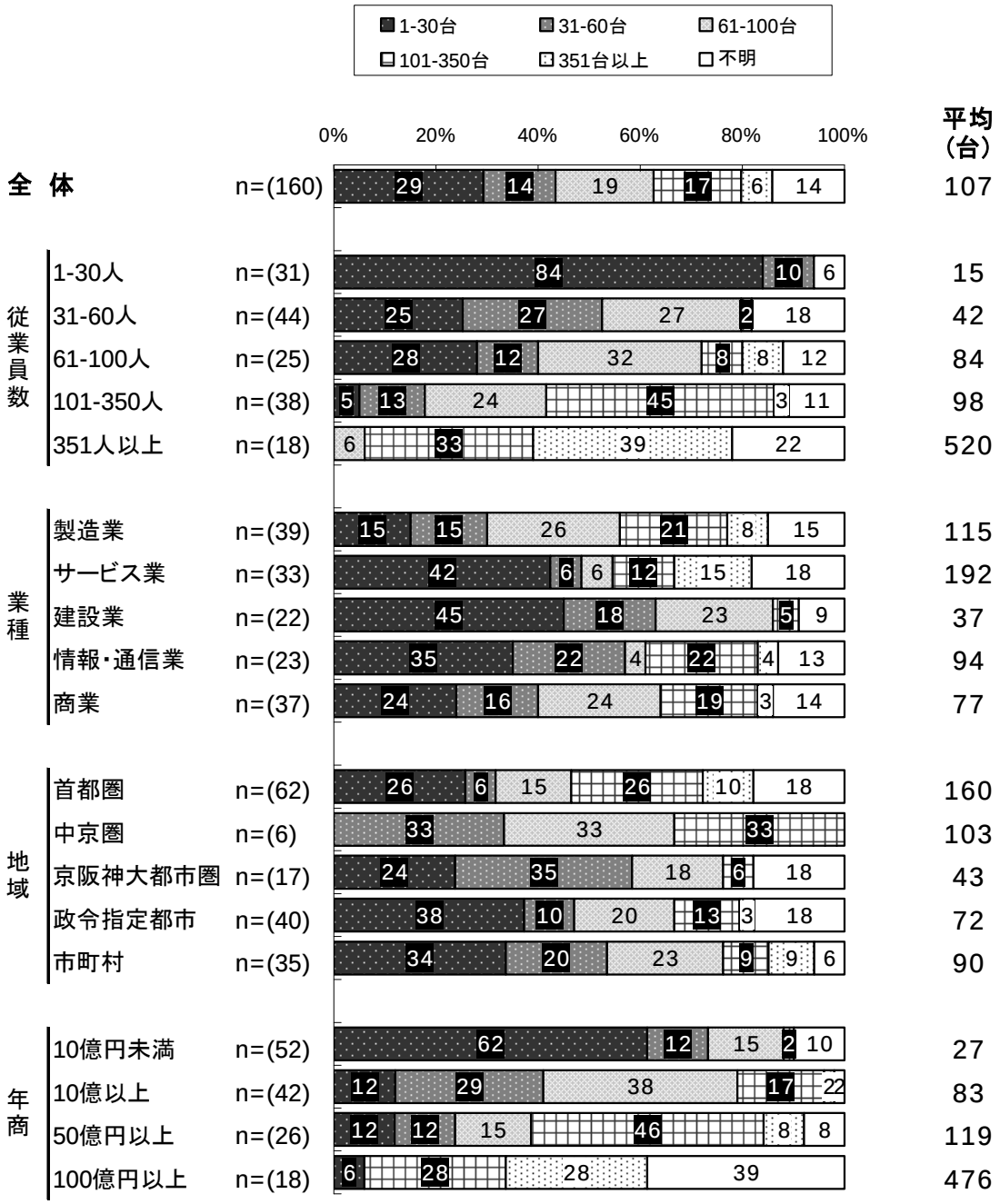
図表 4.1.12.1 F7 情報システム担当者合計



4.1.13 PC の台数

- 全体で見ると、平均の PC 台数は 107 台となっている。
- 従業員規模別に見ると、規模が大きくなるにつれて平均の人数は多くなっている。
- 業種別に見ると、「サービス業」で平均の PC 台数が 192 台と最も多くなっている。

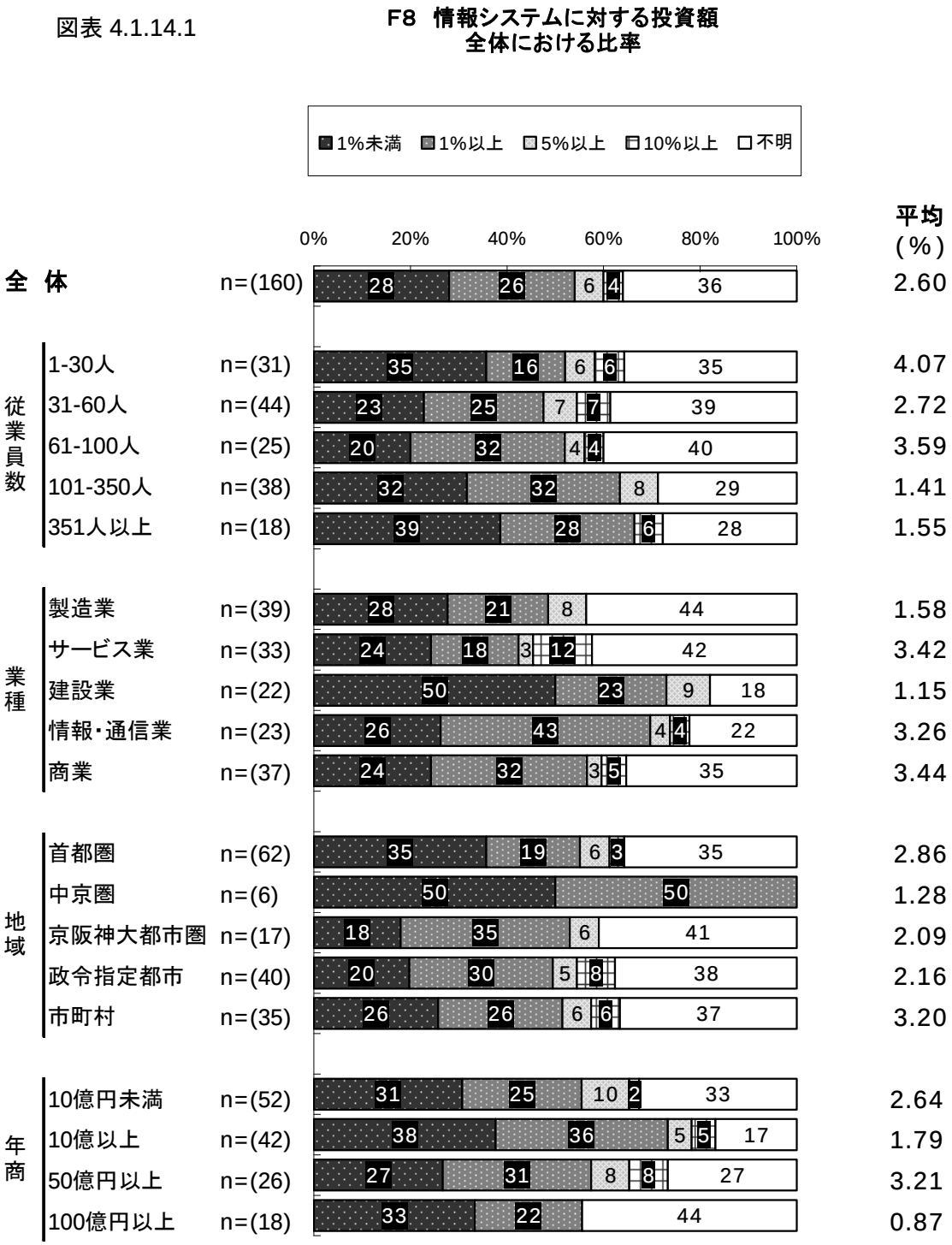
図表 4.1.13.1 F7.3 PCの台数



4.1.14 情報システムに対する投資額　全体における比率

- 全体で見ると、『1%未満』が 28%と最も高くなっている。
- 業種別に見ると、『建設業』で『1%未満』が 50%と最も高くなっている。

図表 4.1.14.1



4.2 大分類の得点　全体

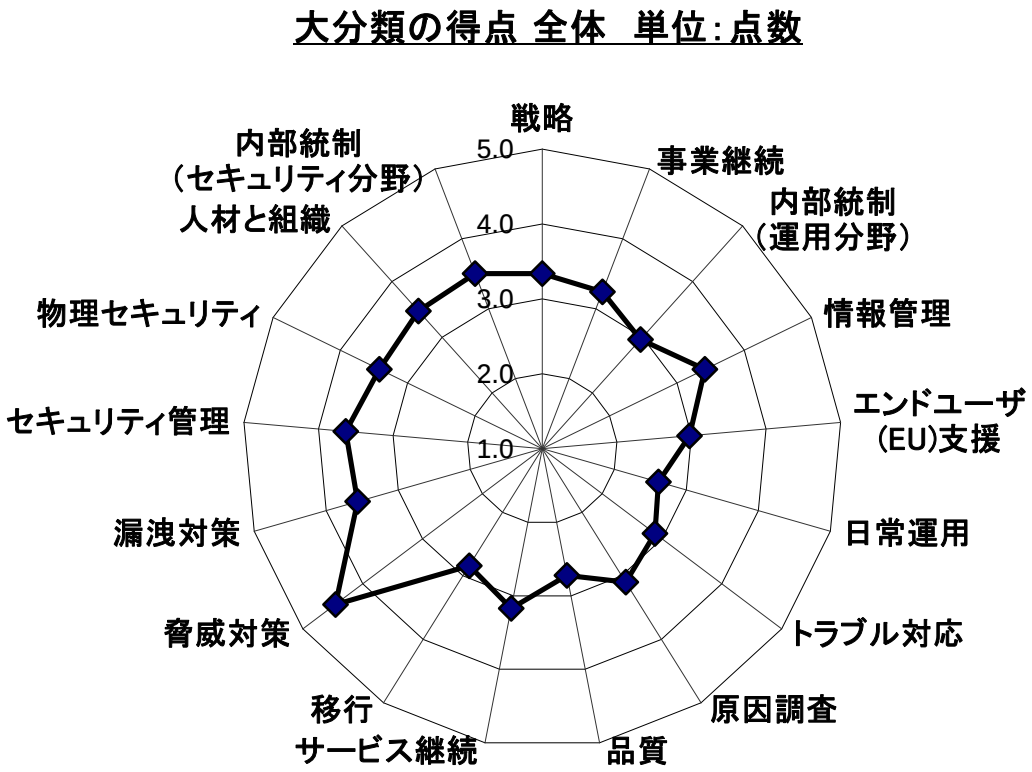
得点の計算方法

下記の図表では、質問紙の設問をいくつかのカテゴリにまとめて大分類を作成し、その得点を算出している。
得点は各設問ごとに算出されて、大分類の得点はそこに含まれる設問の平均点を使用している。

各設問では、情報システム対策に対する取り組みの度合いを5段階の尺度を用いて質問しており、
最も取り組みに力を入れている場合を5点、最も力を入れていない場合は1点として点数化を行った。

※ Q93-Q111 のインターネットに接続していない場合の設問については、該当企業数が 2 社と非常に少なく分析不可能であったため、結果は省略しております。

図表 4.2.0.1



図表 4.2.0.2

設問	大分類	得点
Q1-Q4	戦略	3.34
Q5-Q7	事業継続	3.24
Q8-Q9	内部統制（運用分野）	2.96
Q10-Q13	情報管理	3.41
Q14-Q18	エンドユーザ(EU)支援	2.97
Q19-Q24	日常運用	2.61
Q25-Q33	トラブル対応	2.89
Q34-Q37	原因調査	3.10
Q38-Q44	品質	2.72

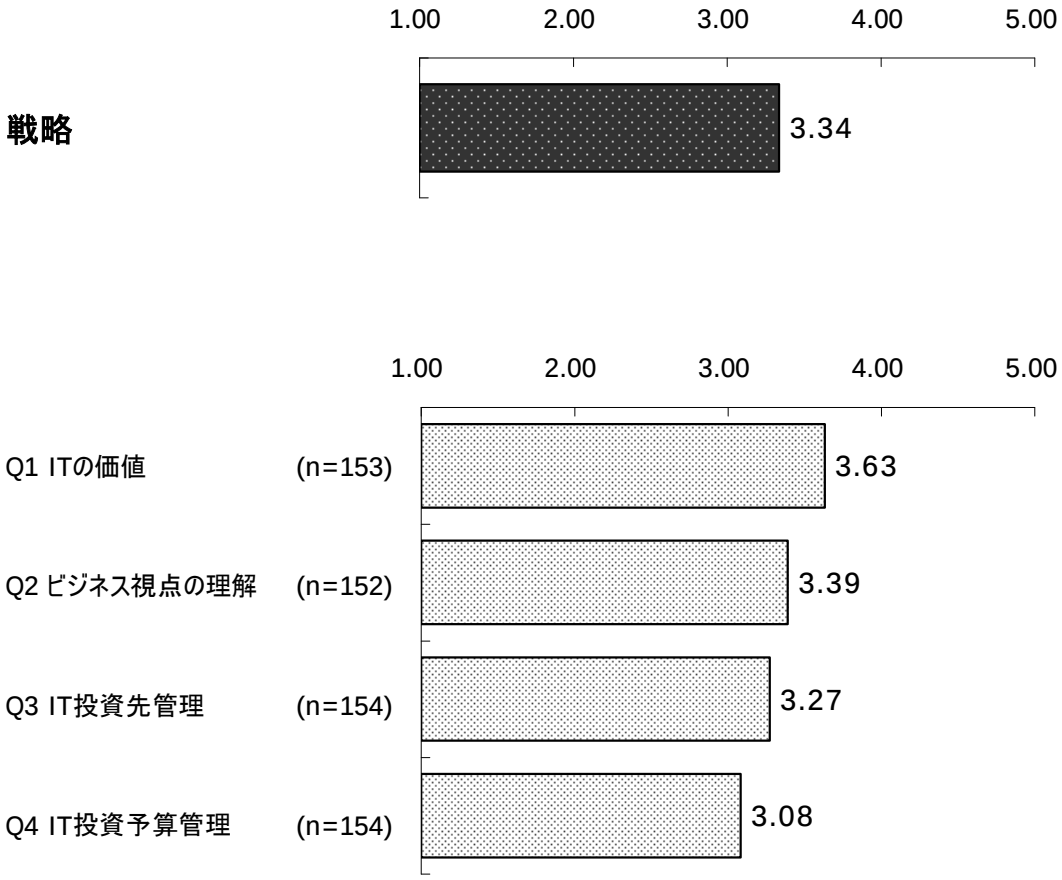
設問	大分類	得点
Q45-Q50	サービス継続	3.17
Q51-Q59	移行	2.84
Q60-Q67	脅威対策	4.46
Q68-Q81	漏洩対策	3.57
Q82-Q86	セキュリティ管理	3.63
Q87-Q91	物理セキュリティ	3.42
Q11-13,Q92	人材と組織	3.47
Q68,70,74,79,80,85,89	内部統制（セキュリティ分野）	3.50

4.3 戦略

4.3.1 戦略

- 戦略については、全体で 3.34 点となり、戦略に含まれる項目の得点を見ると、『IT の価値』が最も高く 3.63 点となっている。
- 逆に最も低くなっているのが『IT 投資予算管理』で 3.08 点である。

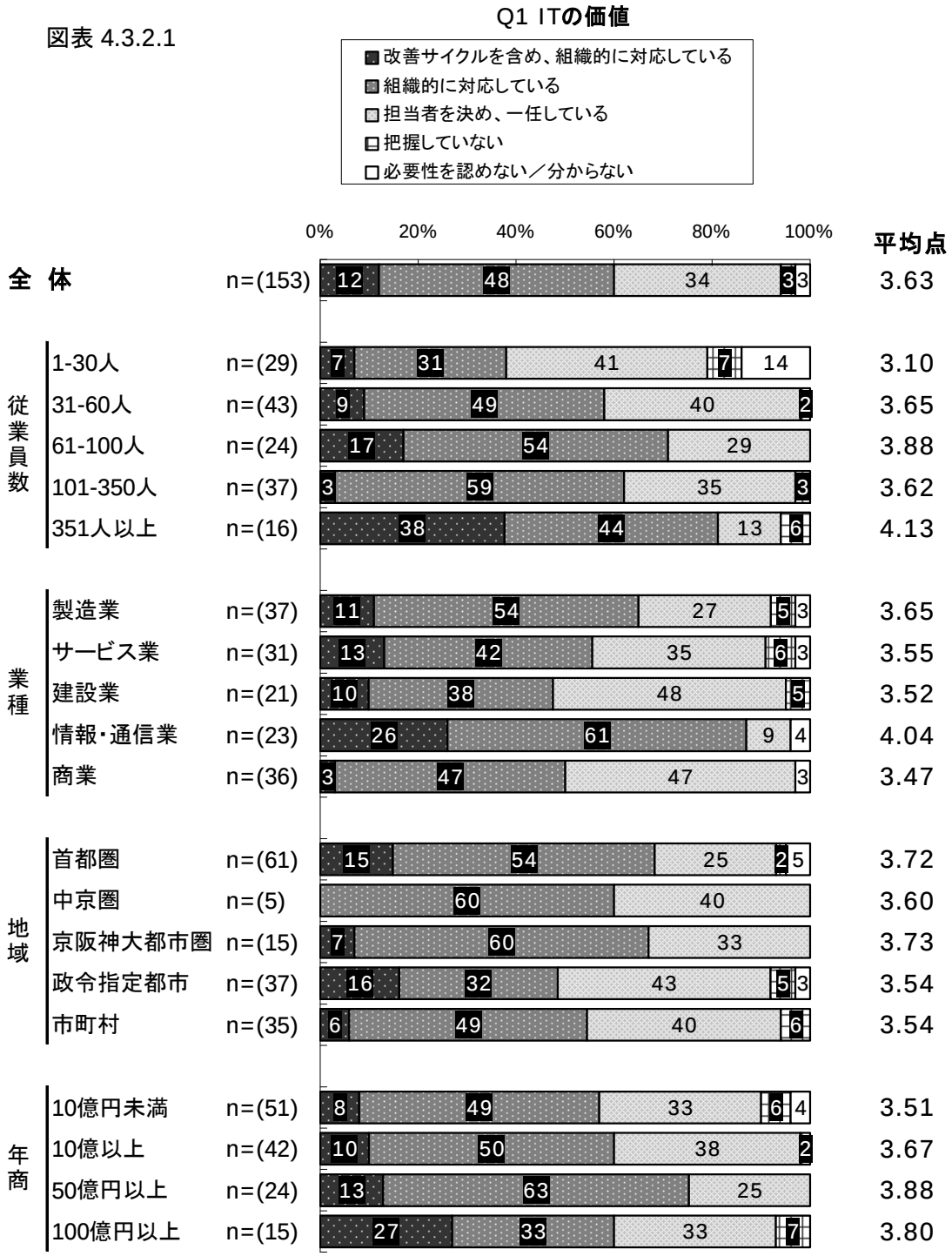
図表 4.3.1.1



4.3.2 戦略 -Q1 IT の価値

- 全体では 3.63 点となり、『改善サイクルを含め、組織的に対応している』は 12%となっている。
- 従業員規模別に見ると、基本的には規模が大きくなるにつれて点数も高くなるが、「101～350 人」では、「31～60 人」「61～100 人」の規模に比べて点数が低くなっている。また、「351 人以上」の規模になると、点数は 4.13 点と大幅に高くなり、『改善サイクルを含め、組織的に対応している』の割合は 38%と、他の規模と比較して大きく上昇する。
- 業種別に見ると、「情報・通信業」が他の業種と比較して高く 4.04 点であり、「製造業」「サービス業」「建設業」については 3.6 点前後でほとんど変わらない。「商業」だけが他の業種と比較して若干低くなっている。

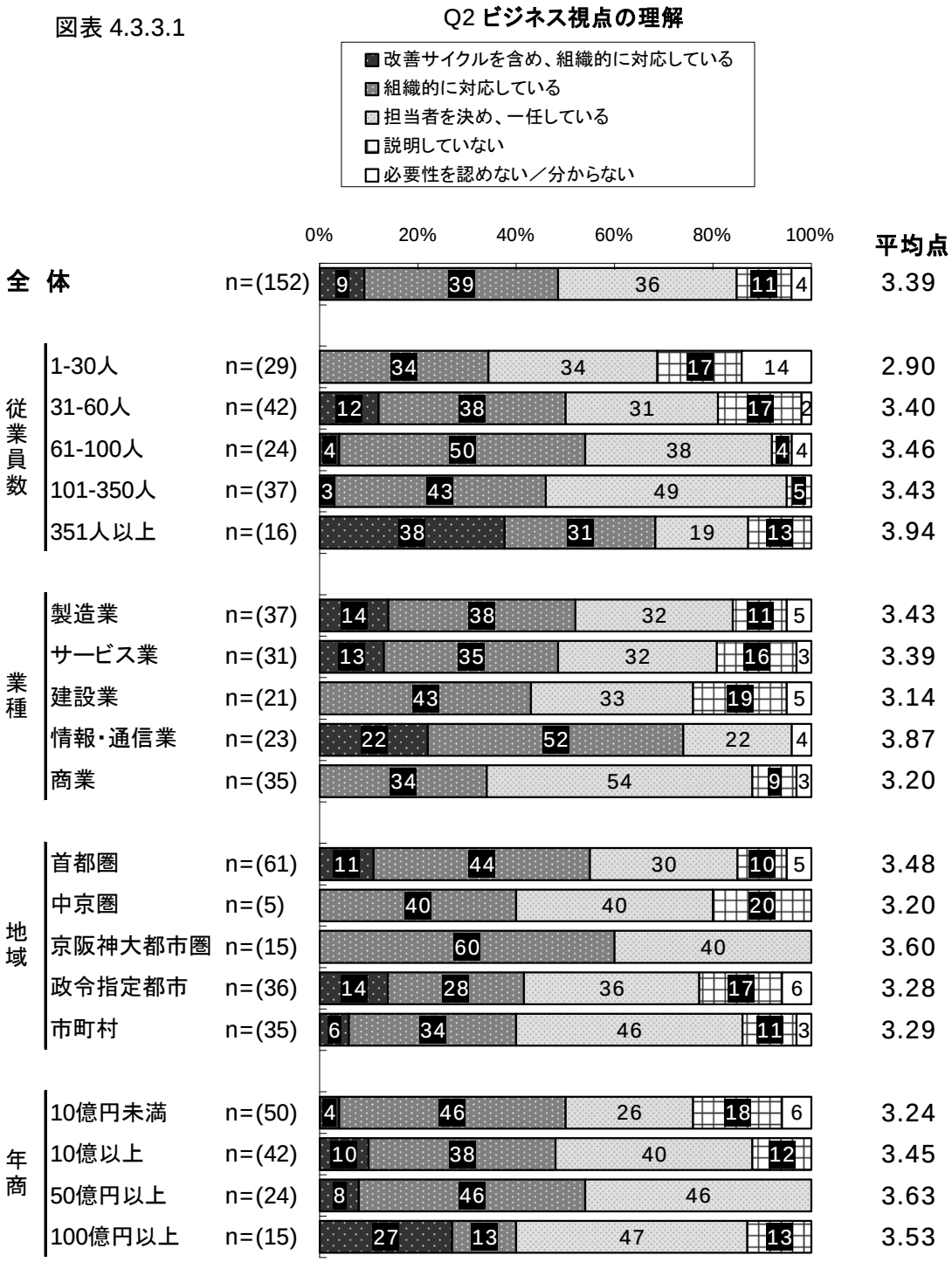
図表 4.3.2.1



4.3.3 戦略 –Q2 ビジネス視点の理解

- 全体では 3.39 点となり、『改善サイクルを含め、組織的に対応している』は 9%となっている。
- 従業員規模別に見ると、「1～30 人」で 2.90 点と非常に低く、逆に「351 人以上」で 3.94 点と高くなっているが、31～350 人の規模ではほとんど値が変わらず 3.4 点程度となっている。
- 業種別に見ると、「建設業」と「商業」で『改善サイクルを含め、組織的に対応している』の割合が 0%と非常に低く、点数も「建設業」で 3.14 点、「商業」で 3.20 点と他の業種と比較して低くなっている。

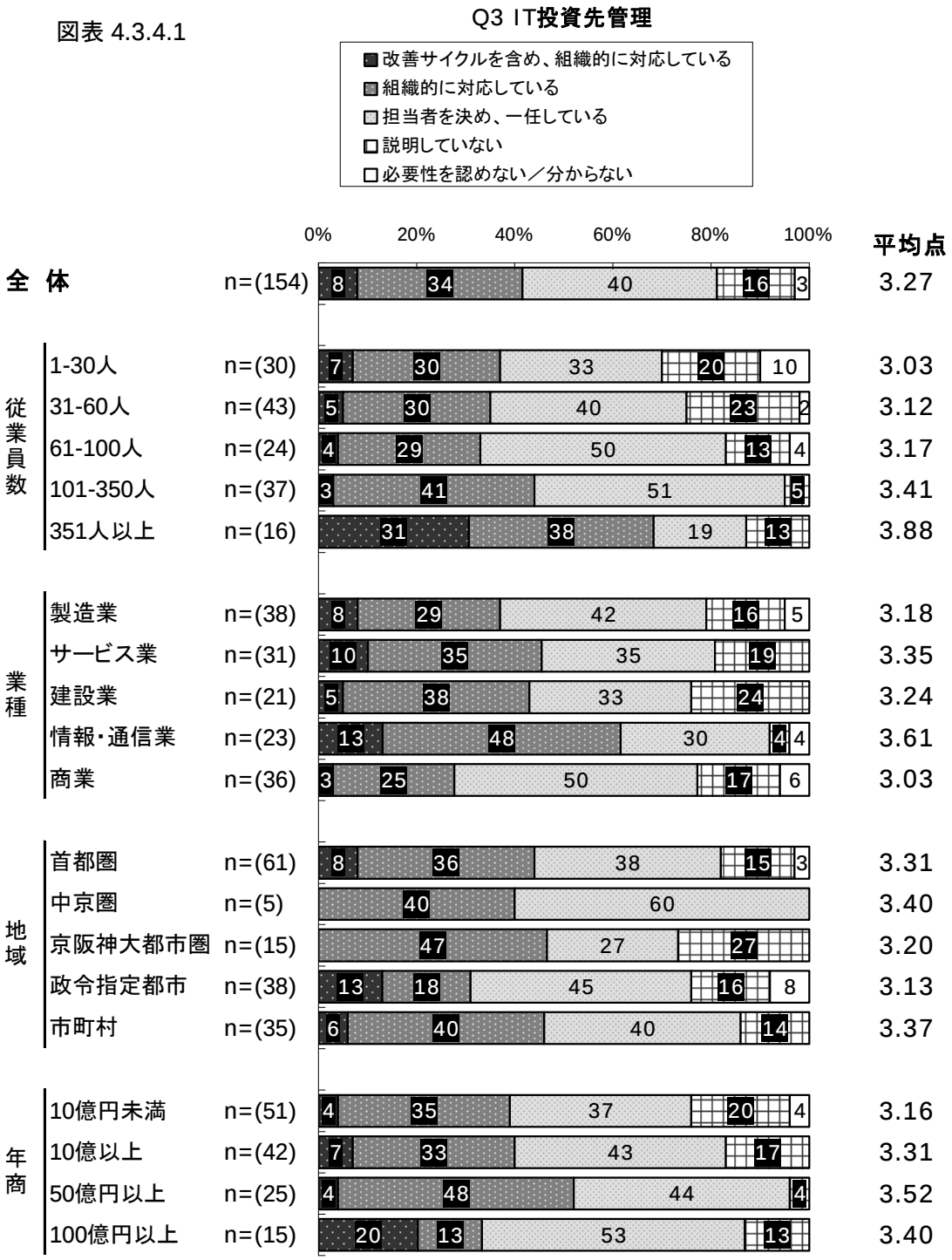
図表 4.3.3.1



4.3.4 戦略 –Q3 IT 投資先管理

- 全体では 3.27 点となり、『改善サイクルを含め、組織的に対応している』は 8%となっている。
- 従業員規模別に見ると、100 人までの企業では、点数が 3.1 点前後とほとんど変わらないが、『説明をしていない』『必要性を認めない/分からない』というネガティブな回答が、規模が大きくなるにつれて減っている。また、「351 人以上」では他の規模とは傾向が異なり、『改善サイクルを含め、組織的に対応している』の割合が 31%と非常に高い。

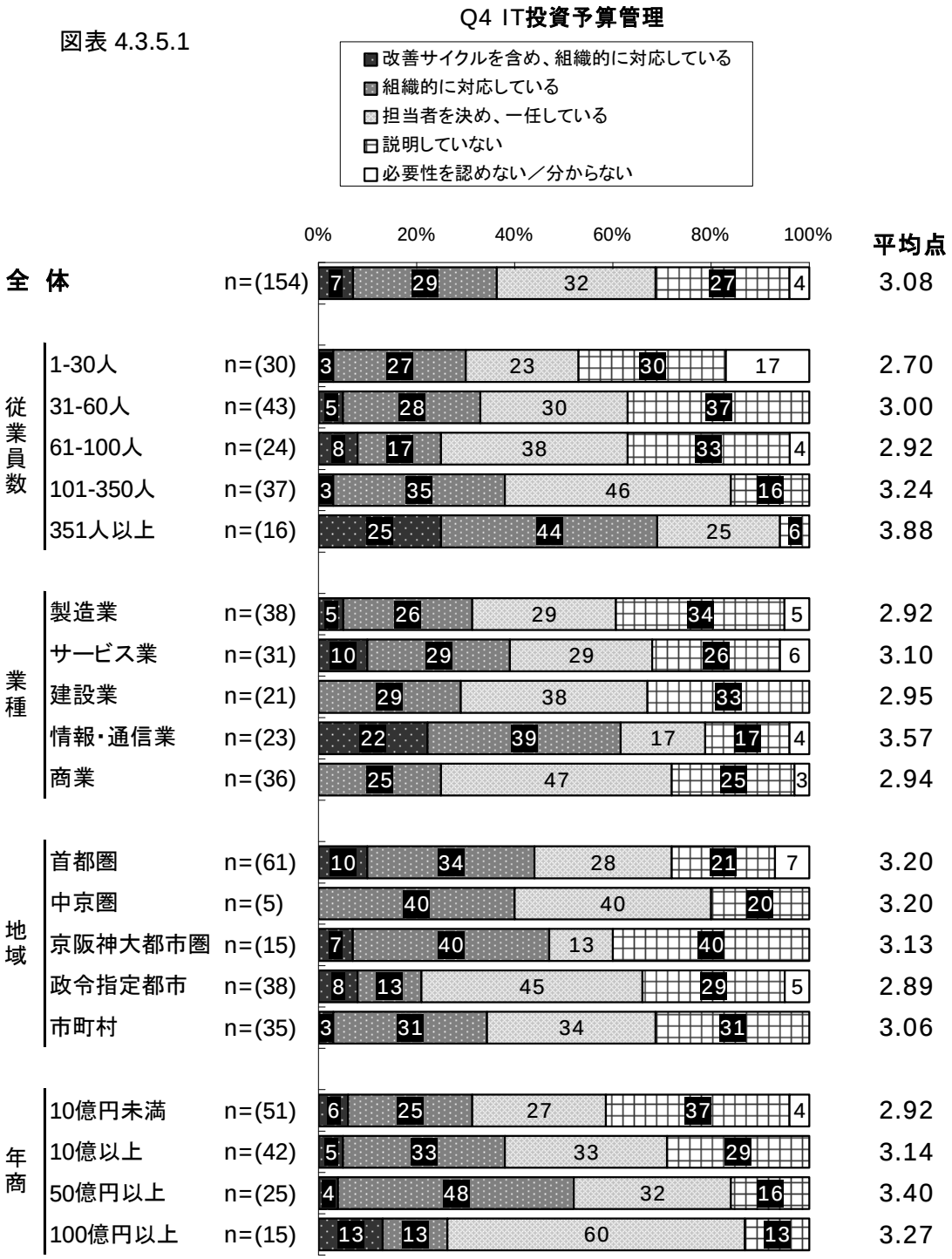
図表 4.3.4.1



4.3.5 戦略 −Q4 IT 投資予算管理

- 全体では 3.08 点となり、『改善サイクルを含め、組織的に対応している』は 7%となっている。
- 従業員規模別に見ると、「351 人以上」で 3.88 点と非常に高い。規模が大きくなるにつれて、『説明していない』『必要性を認めない/分からない』というネガティブな回答が減り、「351 人以上」では他の規模の企業と比べ『改善サイクルを含め、組織的に対応している』が大幅に上昇している。
- 業種別に見ると、「建設業」と「商業」で『改善サイクルを含め、組織的に対応している』の割合が 0%と非常に低い。

図表 4.3.5.1

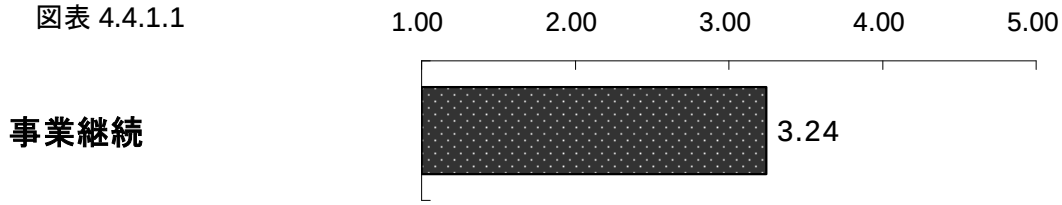


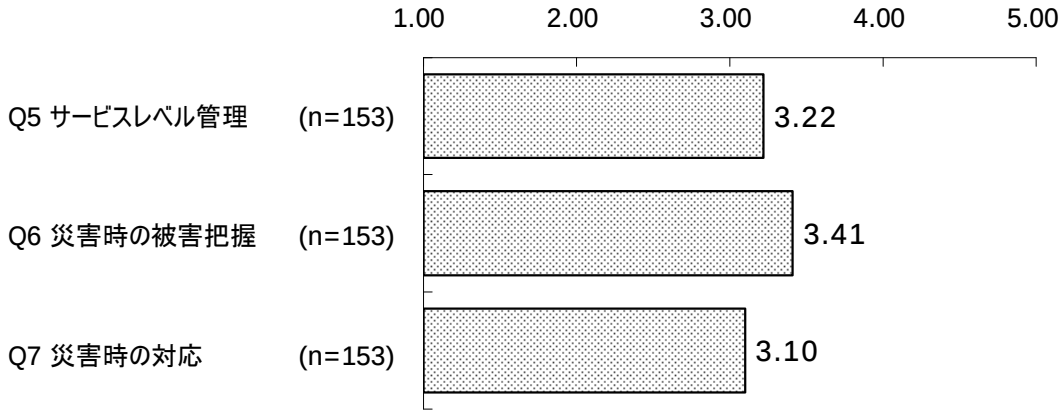
4.4 事業継続

4.4.1 事業継続

- 事業継続については、全体で 3.24 点となり、事業継続に含まれる項目の得点を見ると、『災害時の被害把握』が最も高く 3.41 点となっている。
- 逆に最も低くなっているのが『災害時の対応』で 3.10 点であるが、いずれも項目間に大きな差は見られない。

図表 4.4.1.1

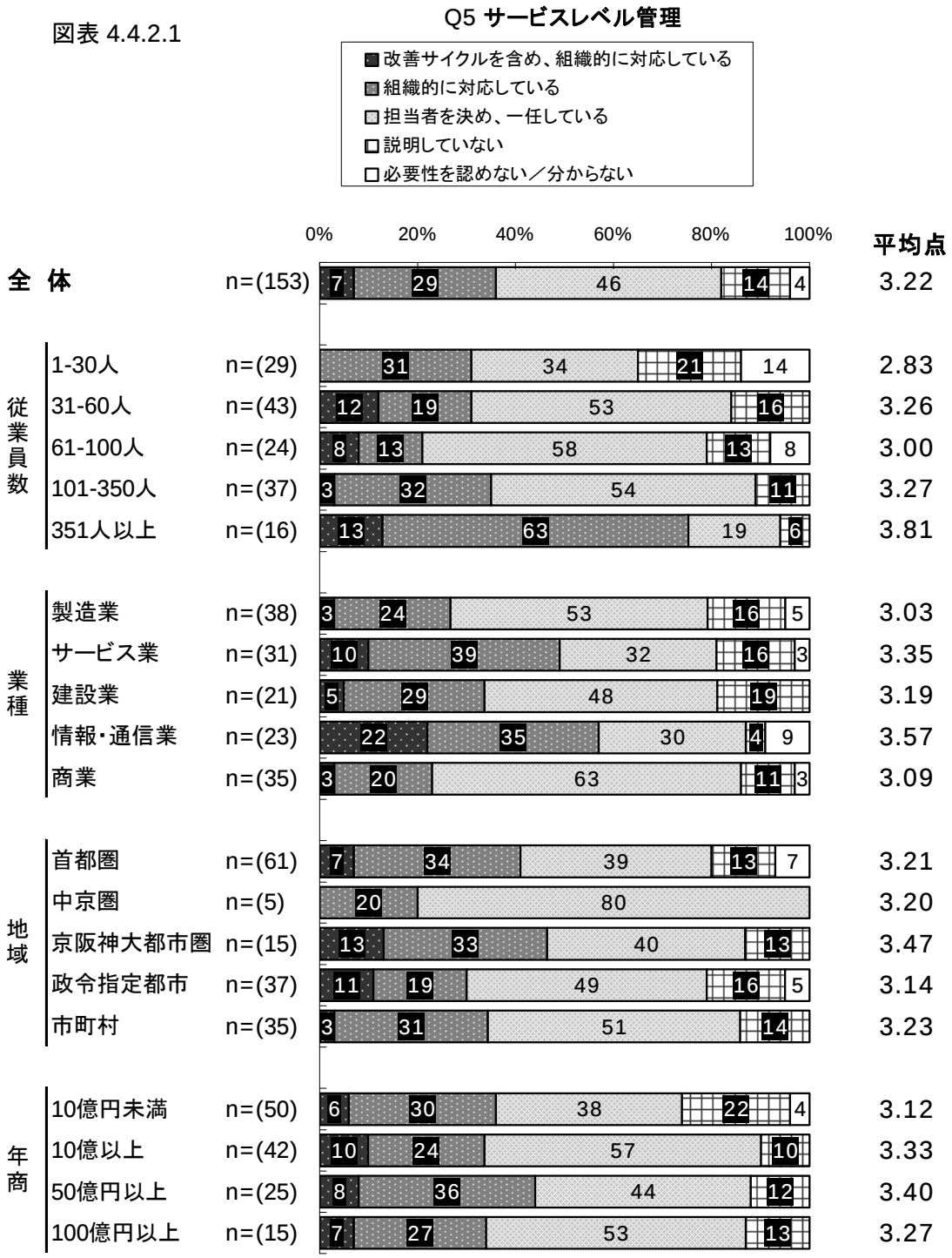




4.4.2 事業継続 –Q5 サービスレベル管理

- 全体では 3.22 点となり、『改善サイクルを含め、組織的に対応している』は 7%となっている。
- 従業員規模別に見ると、「351 人以上」で 3.81 点と点数が最も高い。また、1～350 人では構成比に大きな差は見られないが、「351 人以上」になると『組織的に対応している』の割合が飛躍的に上昇し、『担当者を決め、一任している』の割合が下がっている。
- 業種別に見ると「情報・通信業」で得点が最も高く 3.57 点となっており、他の業種と比較して『改善サイクルを含め、組織的に対応している』の割合も高い。

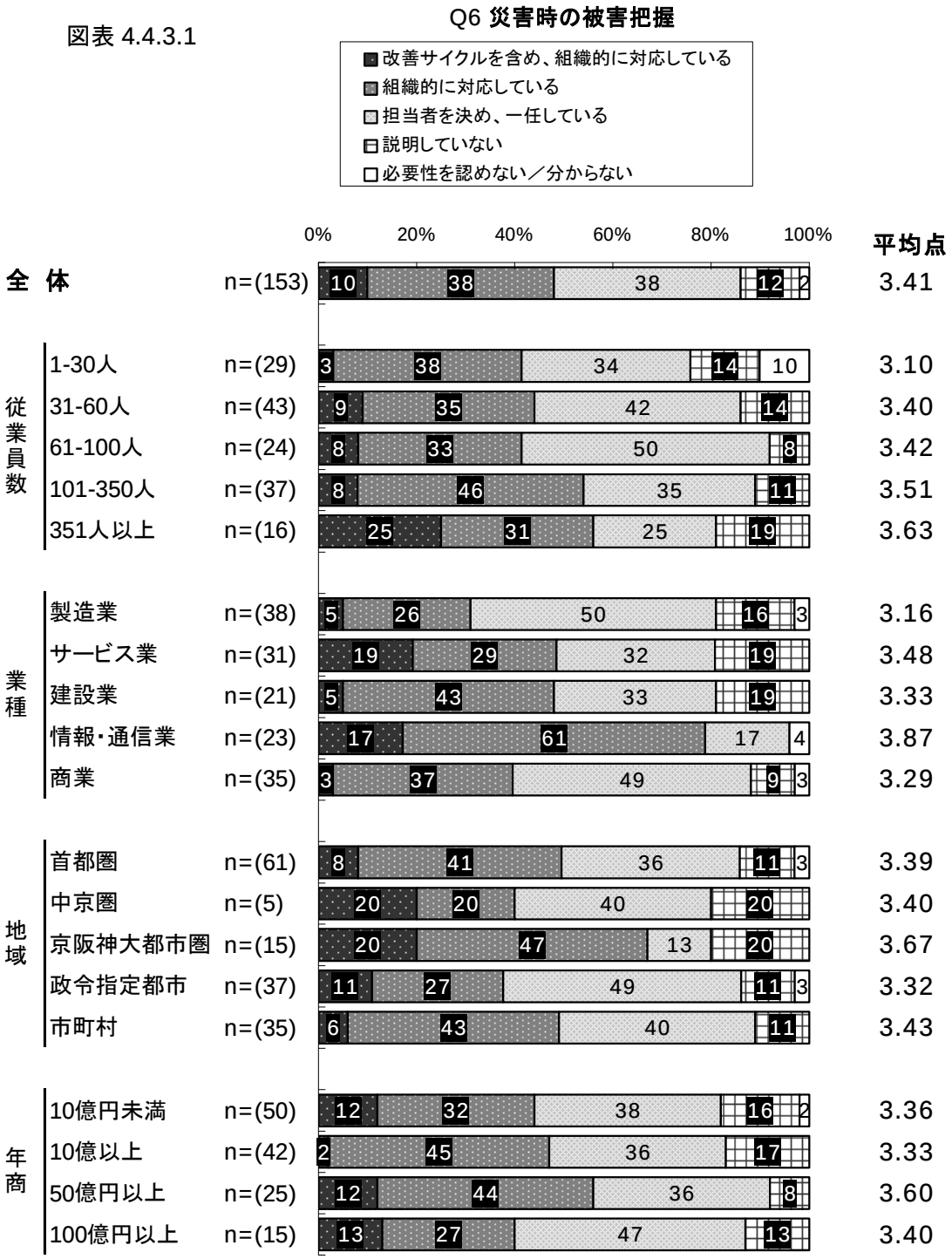
図表 4.4.2.1



4.4.3 事業継続 –Q6 災害時の被害把握

- 全体では 3.41 点となり、『改善サイクルを含め、組織的に対応している』は 10%となっている。
- 従業員規模別に見ると規模が大きくなるにつれて点数が高くなり、「1～30 人」では 3.10 点だが「351 人以上」では 3.63 点になっている。「351 人以上」では『改善サイクルを含め、組織的に対応している』が 25%と他の規模と比較して最も高い一方で、『説明していない』の割合も 19%と、他の規模より高くなっている。

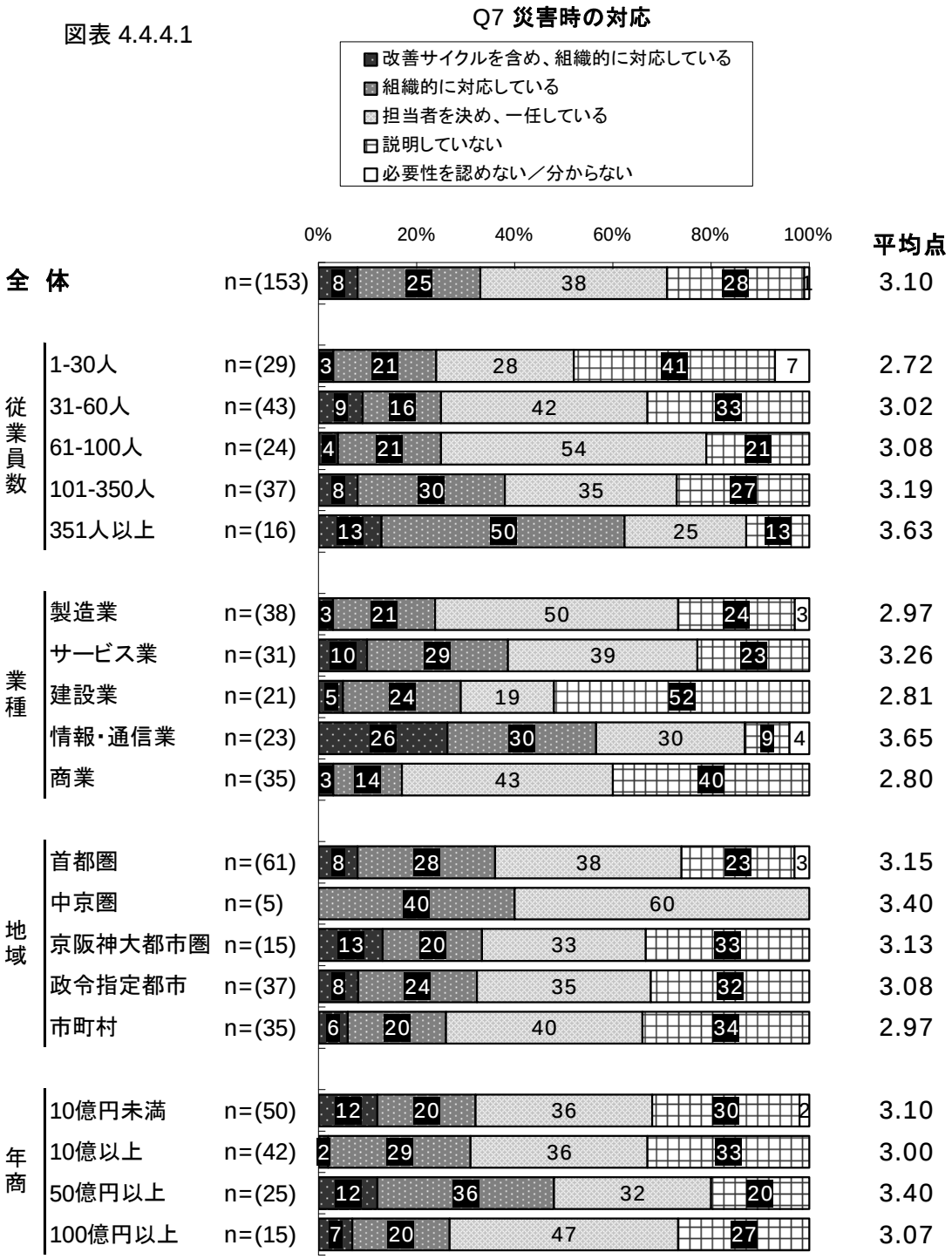
図表 4.4.3.1



4.4.4 事業継続 –Q7 災害時の対応

- 全体では 3.10 点となり、『改善サイクルを含め、組織的に対応している』は 8%となっている。
- 従業員規模別に見ると、規模が大きくなるにつれて点数も高くなる。また、1 ～100 人の規模では、『改善サイクルを含め、組織的に対応している』『組織的に対応している』というポジティブな回答の割合に差は見られないが、「101～350 人」「351 人以上」の規模で、割合が上昇する。
- 業種別に見ると、「情報・通信業」で最も点数が高く 3.65 点となっている。また、「建設業」では『説明していない』の割合が 52%とネガティブな回答が過半数を占めていた。

図表 4.4.4.1

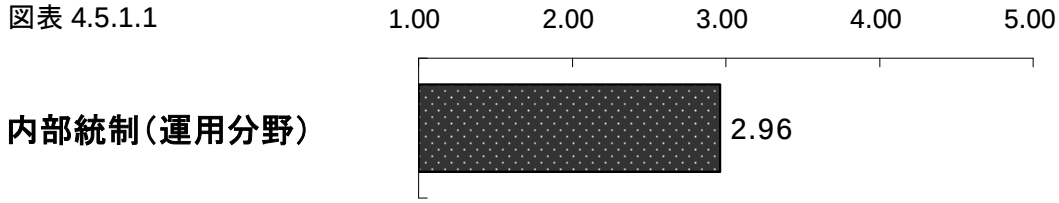


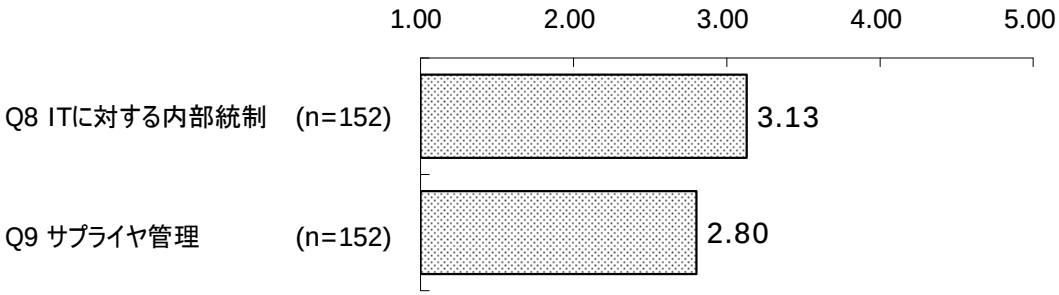
4.5 内部統制（運用分野）

4.5.1 内部統制（運用分野）

・ 内部統制については、全体で 2.96 点となっており、『IT に対する内部統制』の点数が『サプライヤ管理』より高い。

図表 4.5.1.1

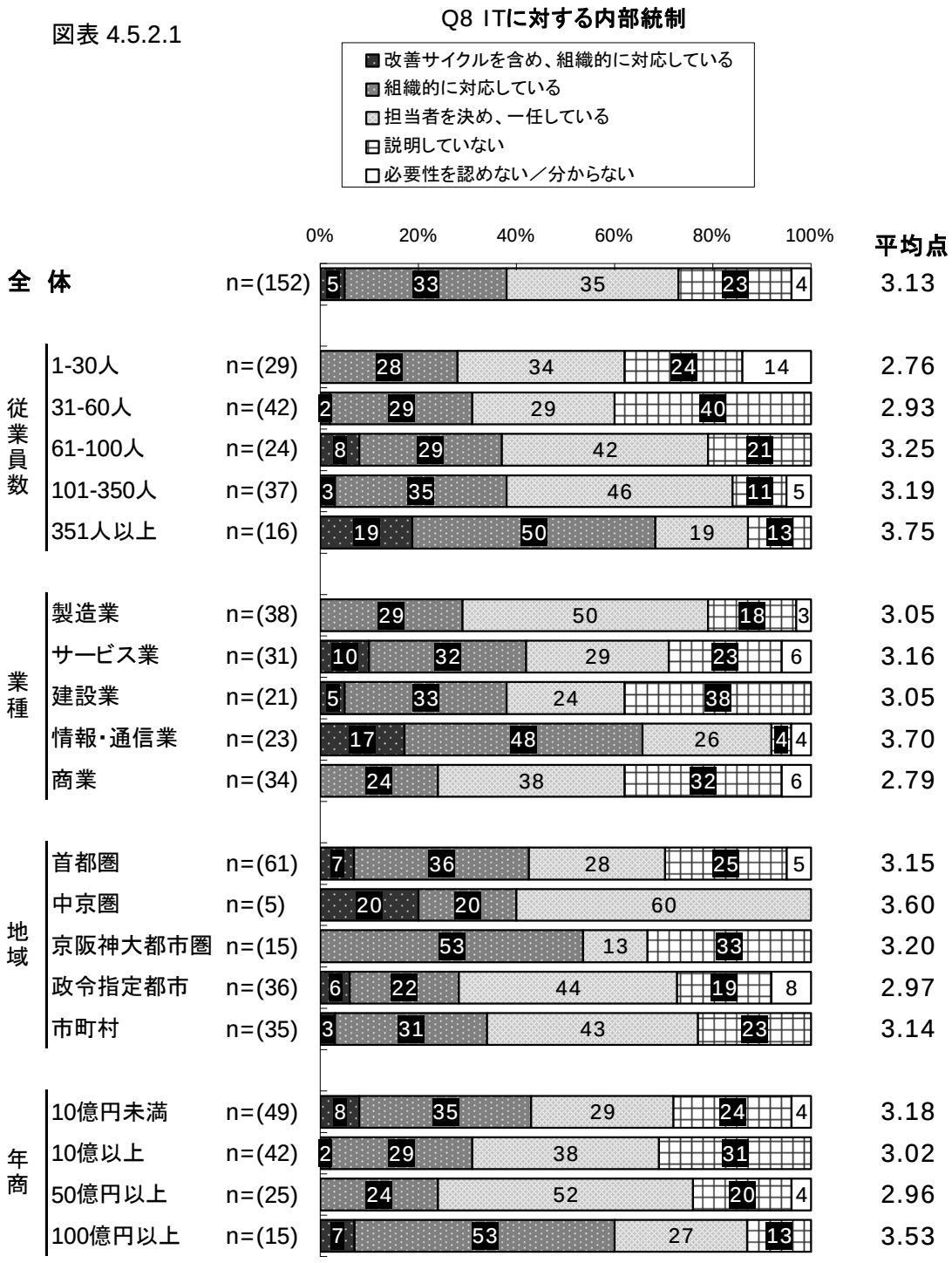




4.5.2 内部統制（運用分野）-Q8 IT に対する内部統制

- 全体では 3.13 点となり、『改善サイクルを含め、組織的に対応している』は 5%となっている。
- 従業員規模別に見ると、「351 人以上」の点数が最も高く 3.75 点となっている。また、「1～30 人」で『改善サイクルを含め、組織的に対応している』が 0%となっている。。
- 業種別に見ると、「情報・通信事業」で最も点数が高く 3.70 点となっている。また、「製造業」と「商業」で改善サイクルを含め、組織的に対応している』が 0%となっている。

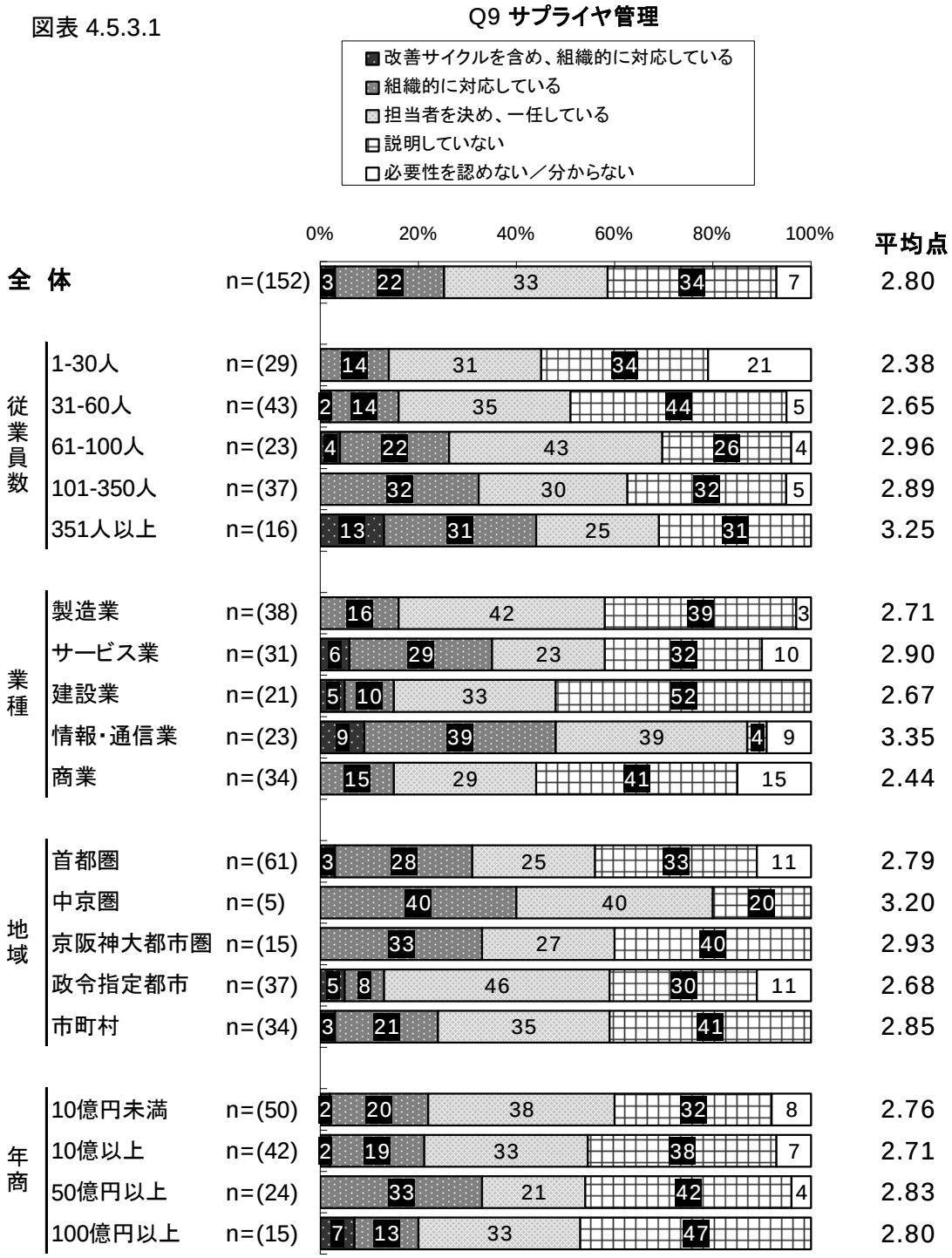
図表 4.5.2.1



4.5.3 内部統制（運用分野）-Q9 サプライヤ管理

- 全体では 2.80 点となり、『改善サイクルを含め、組織的に対応している』は 3%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 3.25 点となっている。また、「1～30 人」と「101～350 人」で『改善サイクルを含め、組織的に対応している』が 0%となっている。
- 業種別に見ると、「情報・通信業」で最も点数が高く 3.35 点となっている。「製造業」と「商業」で『改善サイクルを含め、組織的に対応している』が 0%となっており、他の業種と比較して対策が進んでいない。

図表 4.5.3.1

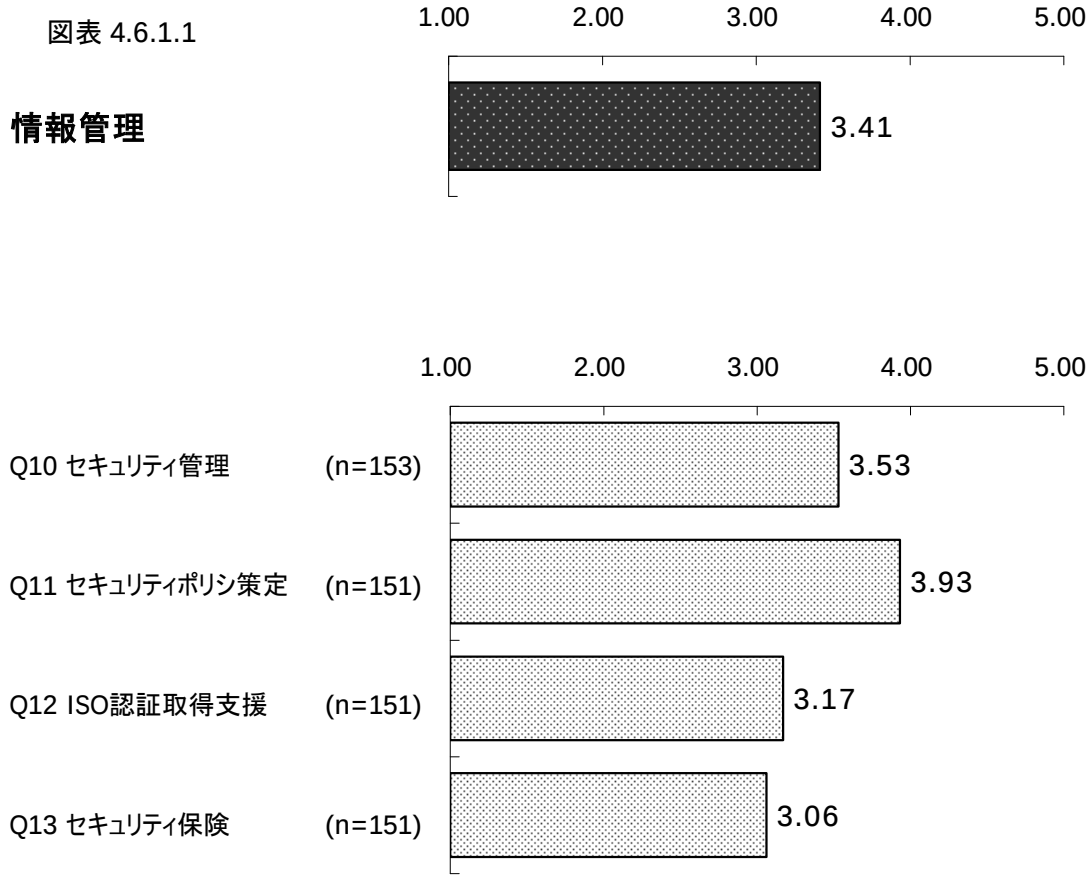


4.6 情報管理

4.6.1 情報管理

・ 情報管理については、全体で 3.41 点となり、情報管理に含まれる項目の得点を見ると、『セキュリティポリシ策定』が最も高く 3.93 点となっている。
・ 逆に最も低くなっているのが『セキュリティ保険』で 3.06 点である。

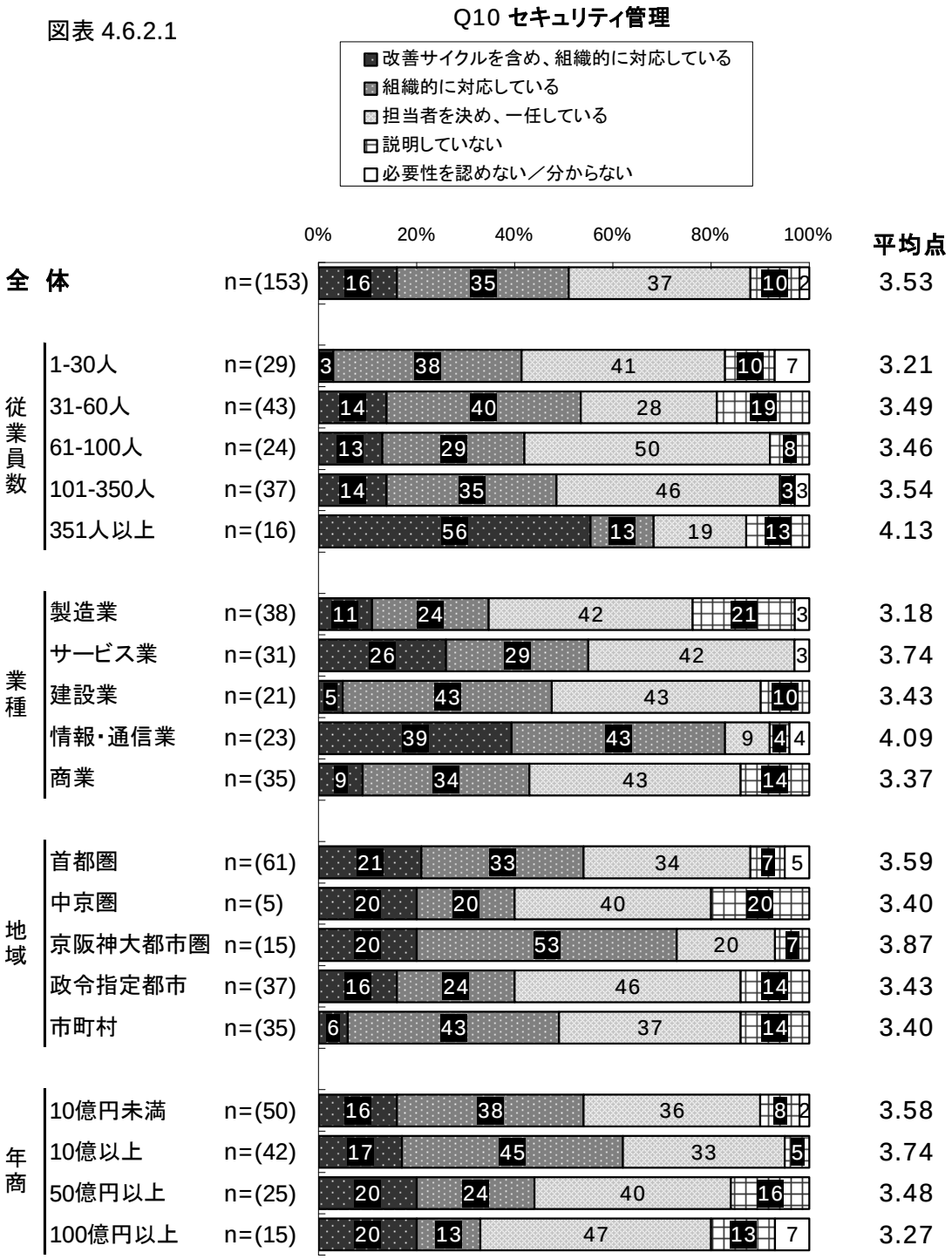
図表 4.6.1.1



4.6.2 情報管理 –Q10 セキュリティ管理

- 全体では 3.53 点となり、『改善サイクルを含め、組織的に対応している』は 16%となっている。
- 従業員規模別に見ると、規模が大きくなるにつれて点数が高くなっている。また、「351 人以上」で『改善サイクルを含め、組織的に対応している』の割合が大幅に上昇しており、5 割以上の企業が同項目に回答している。
- 業種別に見ると「情報・通信事業」で最も点数が高く 4.09 点となっており、『改善サイクルを含め、組織的に対応している』と『組織的に対応している』というポジティブな回答が 8 割を越えている。

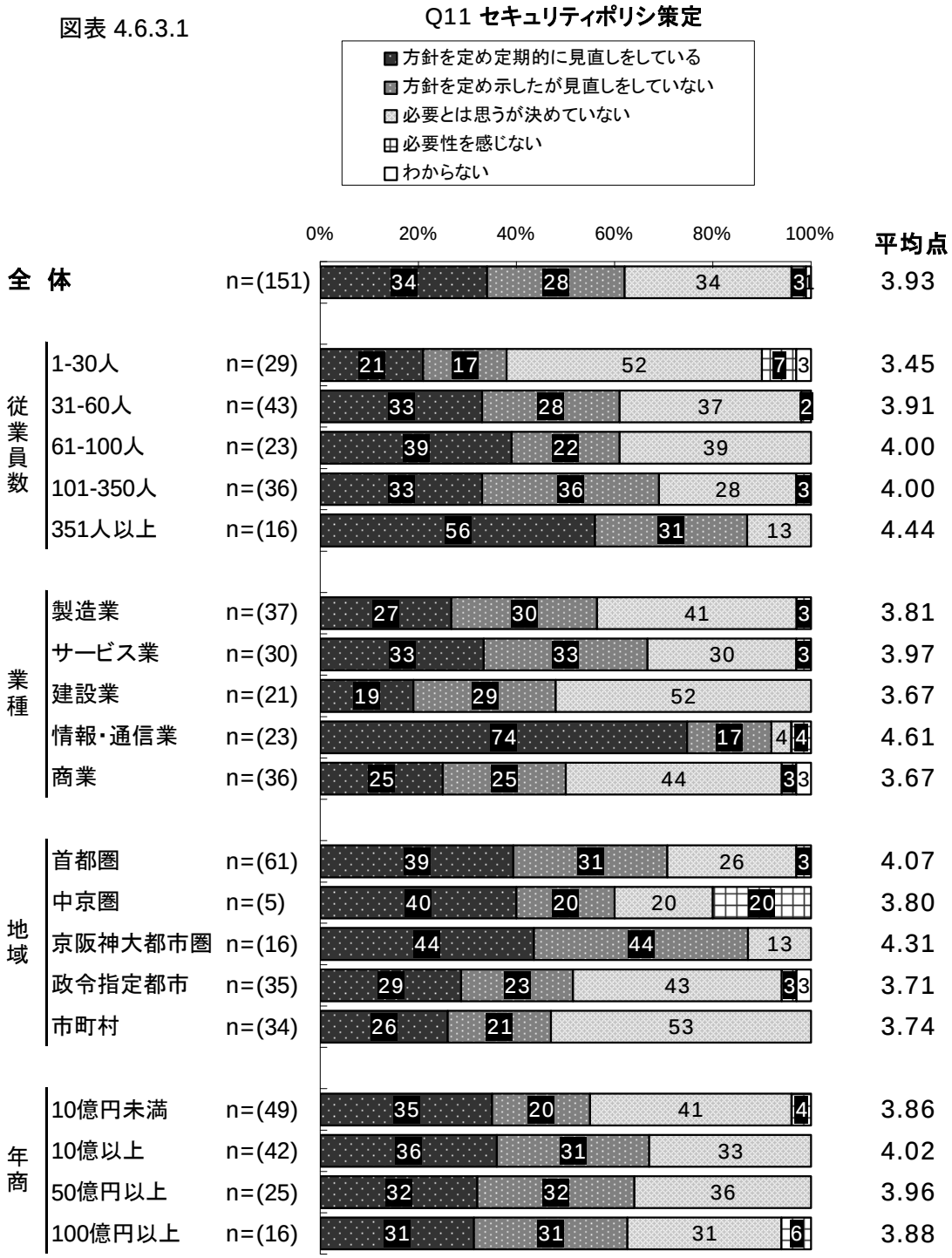
図表 4.6.2.1



4.6.3 情報管理 –Q11 セキュリティポリシ策定

- 全体では 3.93 点となり、『方針を定め定期的に見直しをしている』は 34%となっている。
- 従業員規模別に見ると「1～30 人」で 3.45 点と非常に低く、「351 人以上」で 4.44 点と高くなっているが、31～350 人の規模ではほとんど値が変わらず 4 点程度となっている。
- 業種別に見ると、「情報・通信業」で最も点数が高く 4.61 点となっており、他の規模と比較して『方針を定め定期的に見直しをしている』の割合が非常に高い。

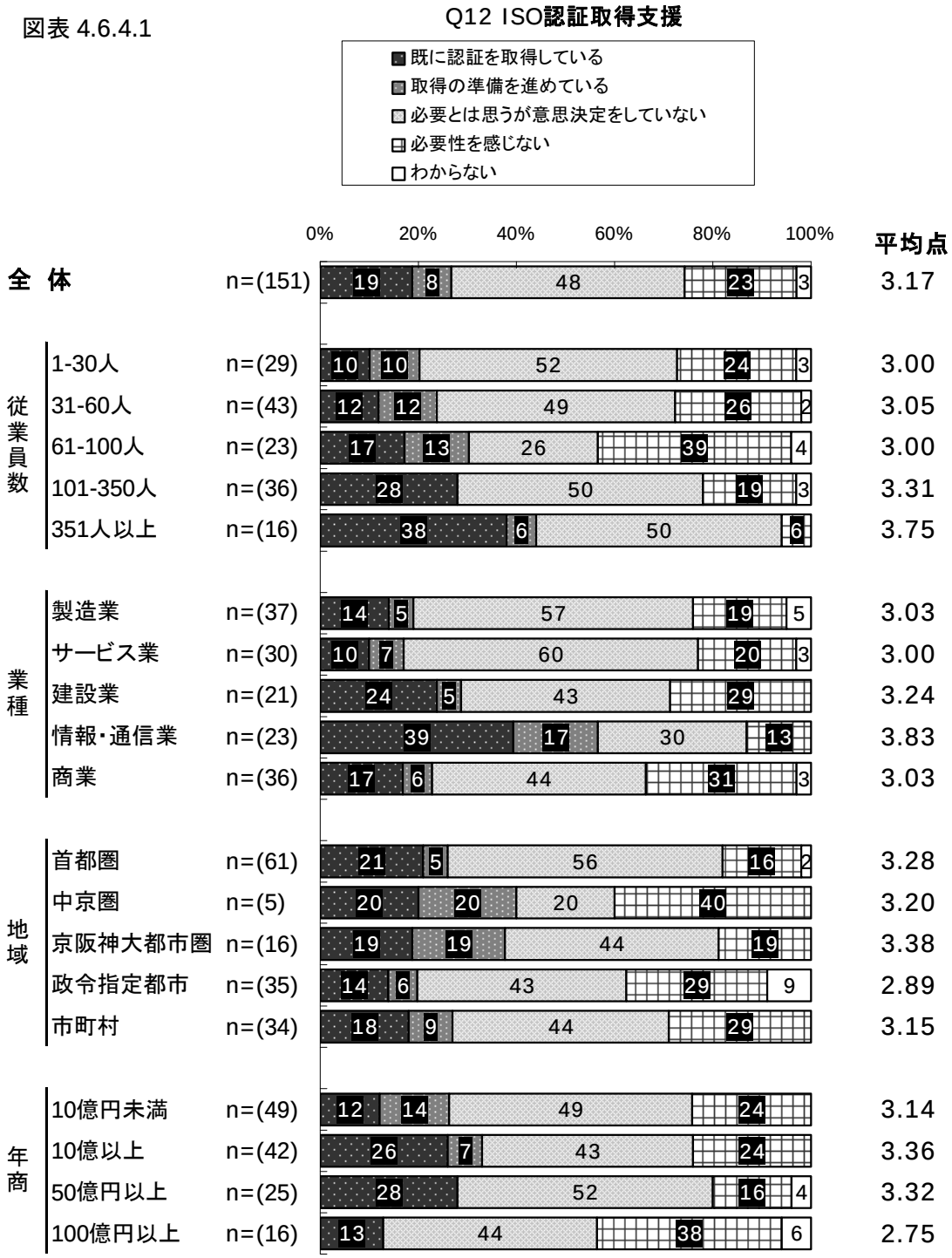
図表 4.6.3.1



4.6.4 情報管理 −Q12　ISO 認証取得支援

- 全体では 3.17 点となり、『既に認証を取得している』は 19%となっている。
- 従業員規模別に見ると「351 人以上」で 3.75 点と非常に高いが、1～100 人規模では値が変わらず 3 点程度となっている。
- 業種別に見ると、「情報・通信業」で最も点数が高く 3.83 点となっている。

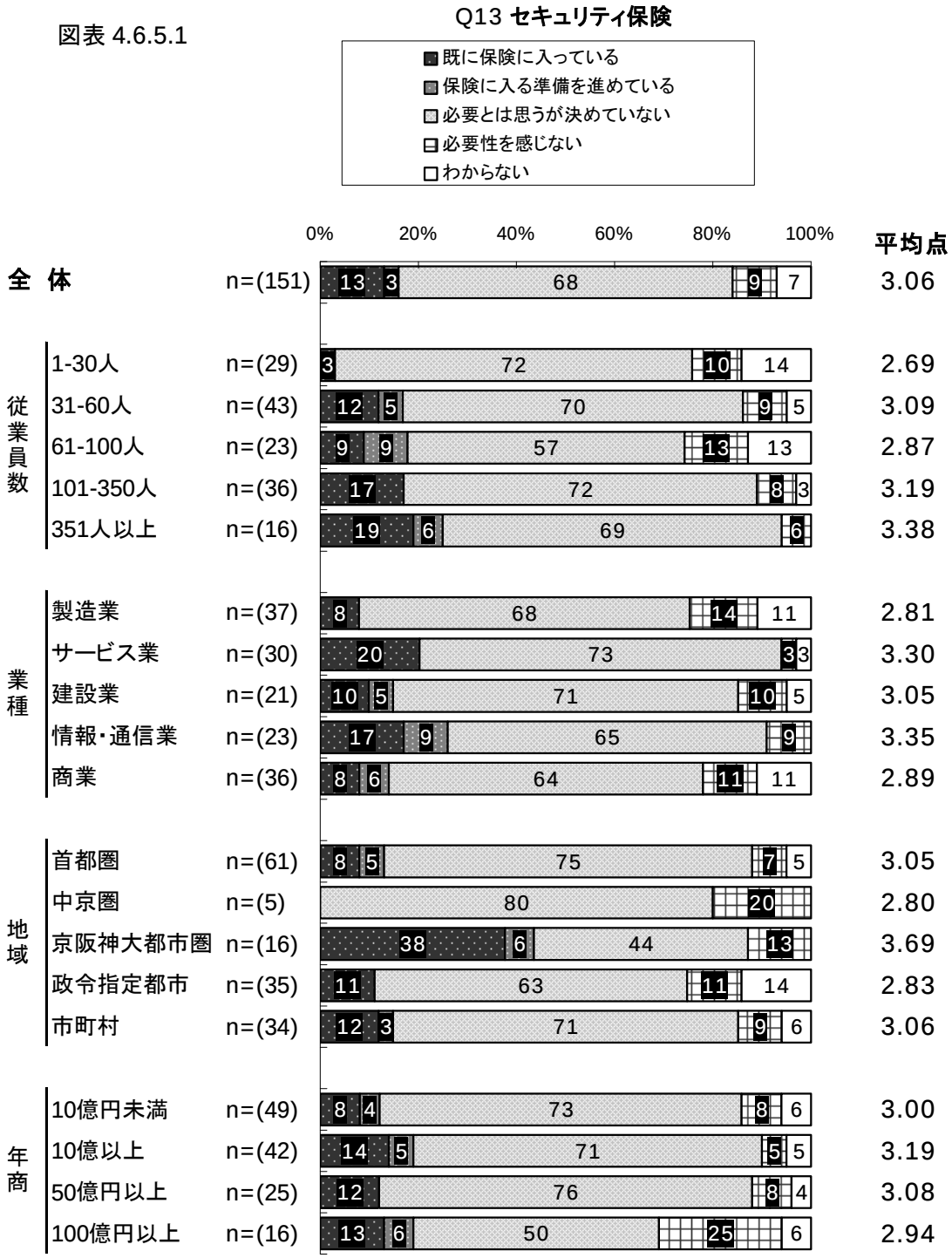
図表 4.6.4.1



4.6.5 情報管理 –Q13 セキュリティ保険

- 全体では 3.06 点となり、『既に保険に入っている』は 13%となっている。
- 従業員規模別に見ると、「351 人以上」でも最も点数が高く 3.83 点となっている。また、いずれの規模でも『必要とは思うが決めていない』の割合が高く、「61～100 人」を除く全ての規模で約 7 割が同回答を選んでいる。
- 業種別に見ると、『既に保険に入っている』と回答した割合は「サービス業」で最も高く 20%であった。

図表 4.6.5.1

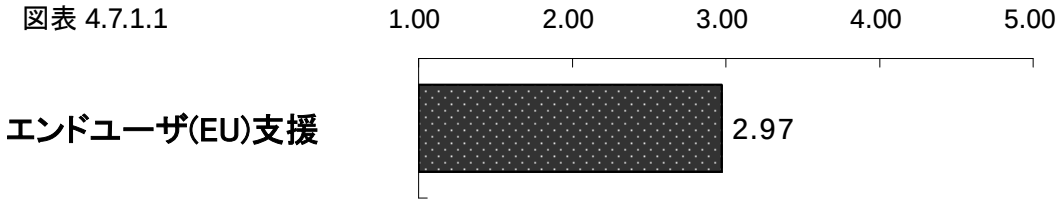


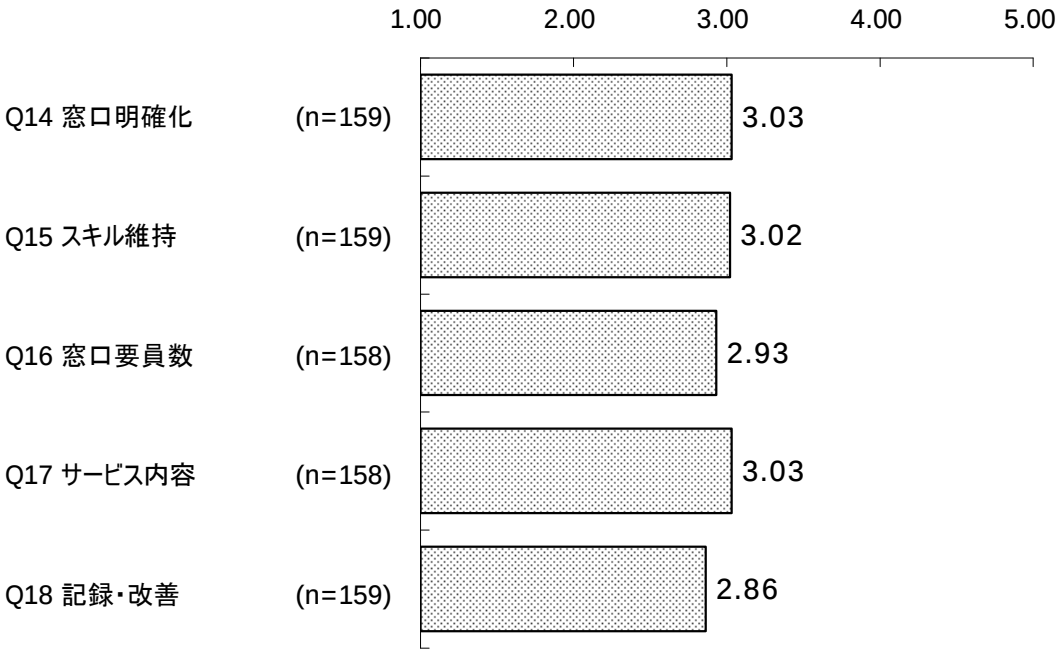
4.7 エンドユーザ(EU)支援

4.7.1 エンドユーザ(EU)支援

・ エンドユーザ(EU)支援については、全体で 2.97 点となり、いずれの設問でも 3 点程度と値に大きな違いは見られない。

図表 4.7.1.1

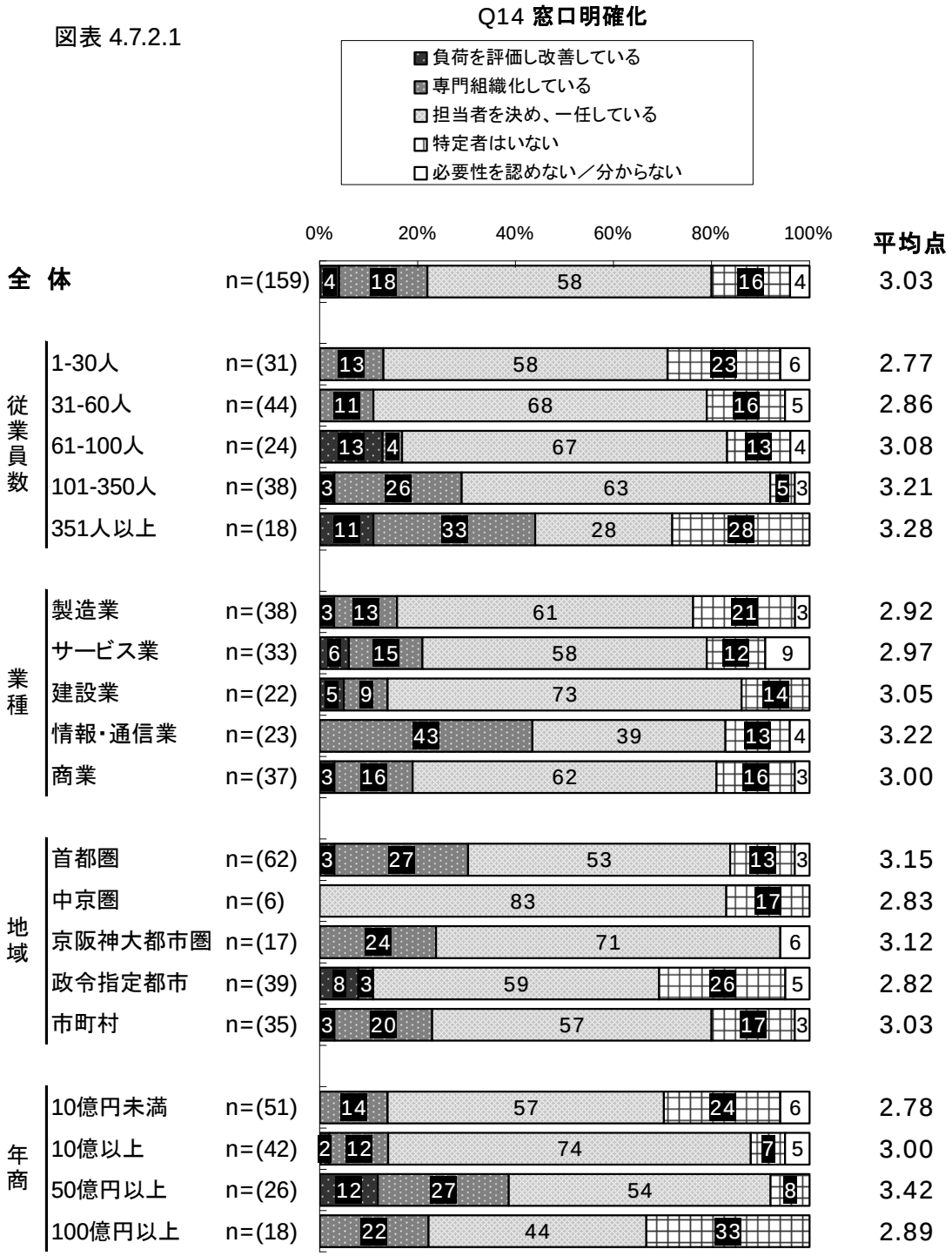




4.7.2 エンドユーザ(EU)支援 –Q14 窓口明確化

- 全体では 3.03 点となり、『負荷を評価し改善している』は 4%となっている。
- 従業員規模別に見ると、規模が大きくなるにつれて点数が高くなっている。また、『特定者はいない』と『必要性を認めない/分からない』というネガティブな回答の割合は 1～350 人では規模が大きくなるにつれて割合が低くなるが、「351 人以上」でまた高くなる。
- 業種別に見ると、「情報・通信業」で最も点数が高く 3.22 点となっているが、『負荷を評価し改善している』の割合が 0%と最も低い。

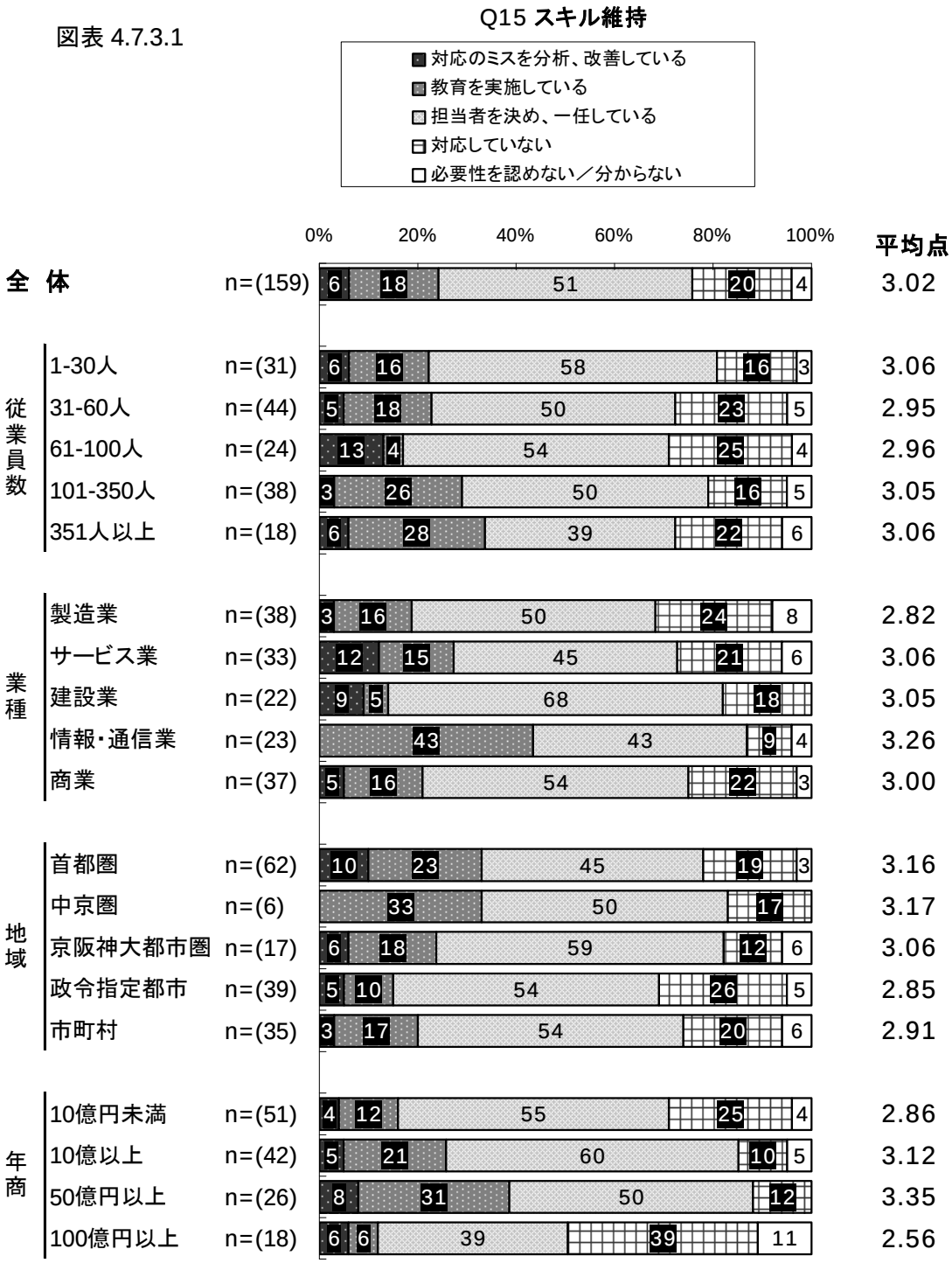
図表 4.7.2.1



4.7.3 エンドユーザ(EU)支援 –Q15 スキル維持

- 全体では 3.02 点となり、『対応のミスを分析、改善している』は 6%となっている。
- 従業員規模別に見ると、いずれの規模でも点数が 3 点程度となっている。また、他の規模と比較して「61～100 人」で『対応のミスを分析、改善している』の割合が高い。
- 業種別に見ると、「情報・通信業」で 3.26 点と他の業種と比較して点数が高いが、『対応のミスを分析、改善している』と回答する割合は 0%である。

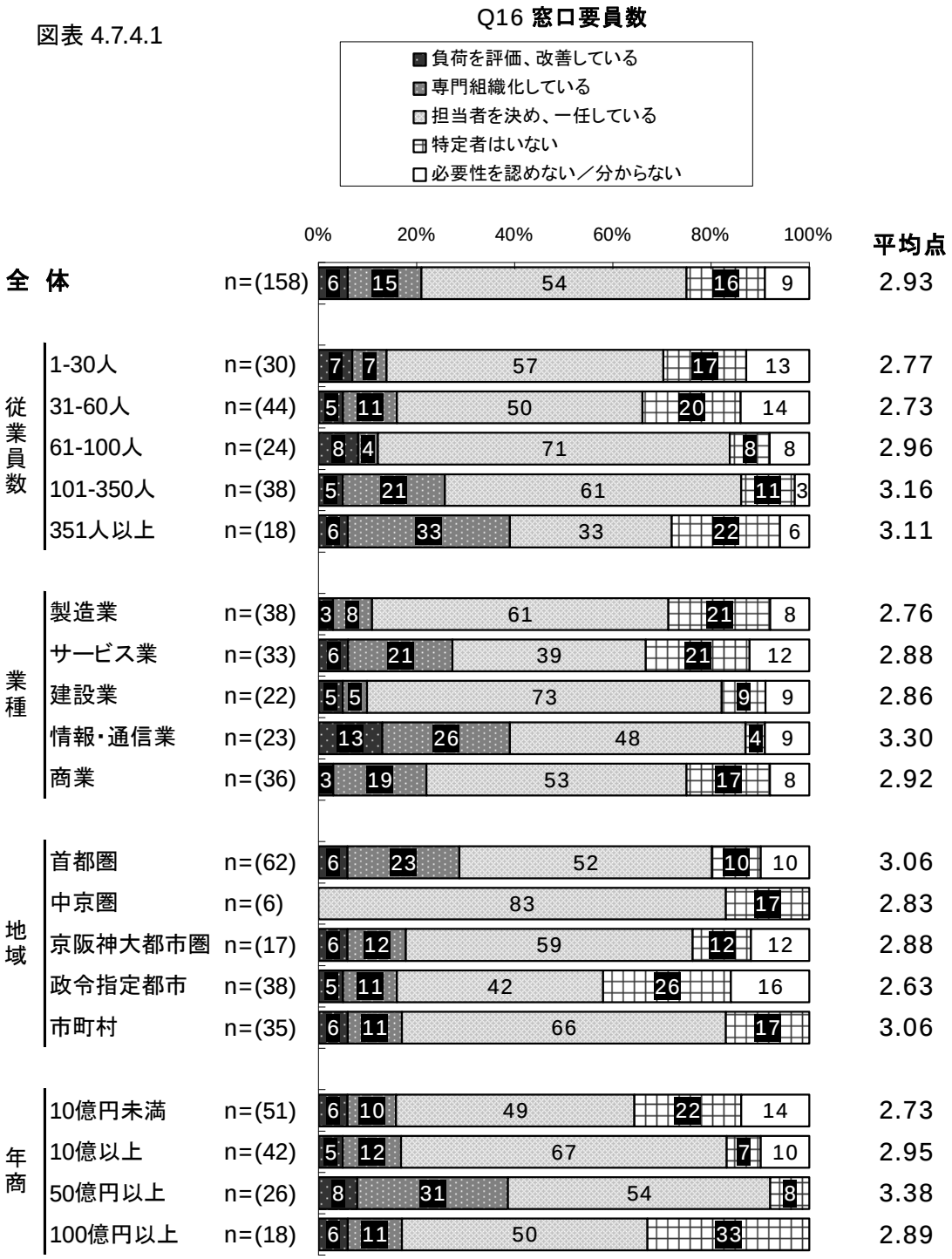
図表 4.7.3.1



4.7.4 エンドユーザ(EU)支援 −Q16 窓口要員数

- 全体では 2.93 点となっており、『負荷を評価、改善している』は 6%となっている。。
- 従業員規模別に見ると、「101～350 人」で最も点数が高く 3.16 点となっている。また、他の規模と比較して「351 人以上」では『負荷を評価、改善している』『専門組織化している』というポジティブな回答の割合が高い一方で、『特定者はいない』と『必要性を認めない/分からない』の割合も高い。

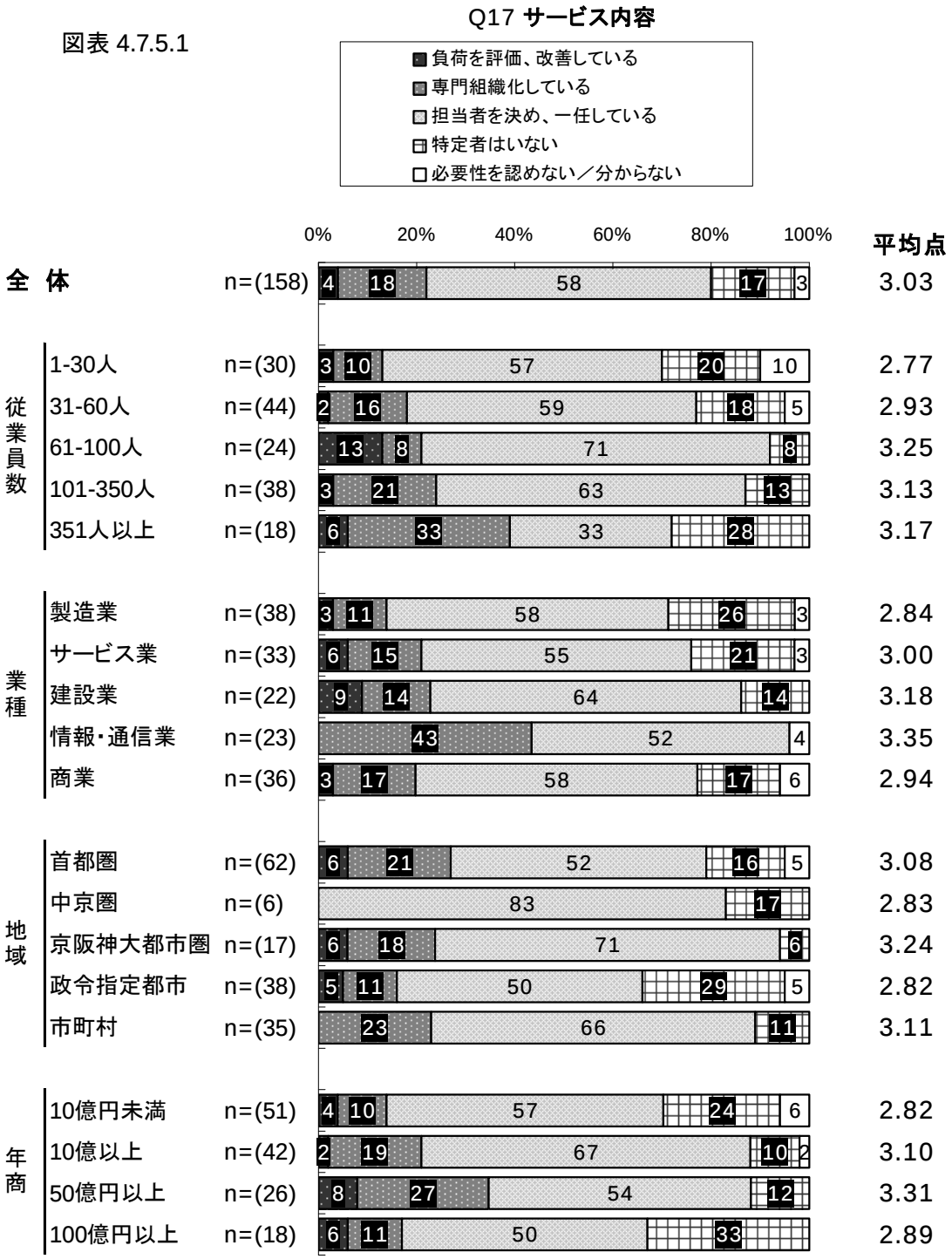
図表 4.7.4.1



4.7.5 エンドユーザ(EU)支援 –Q17 サービス内容

- 全体では 3.03 点となり、『負荷を評価、改善している』は 4%となっている。
- 従業員規模別に見ると、「61～100 人」において最も点数が高く 3.25 点となっている。また、規模が大きくなるについれて『負荷を評価、改善している』と『専門組織化している』というポジティブな回答の割合が増える一方で、『特定者はない』と『必要性を認めない/分からない』というネガティブな回答は１～100 人の間では規模が大きくなるにつれ減少するが、101 人以上の規模でまた増加する。

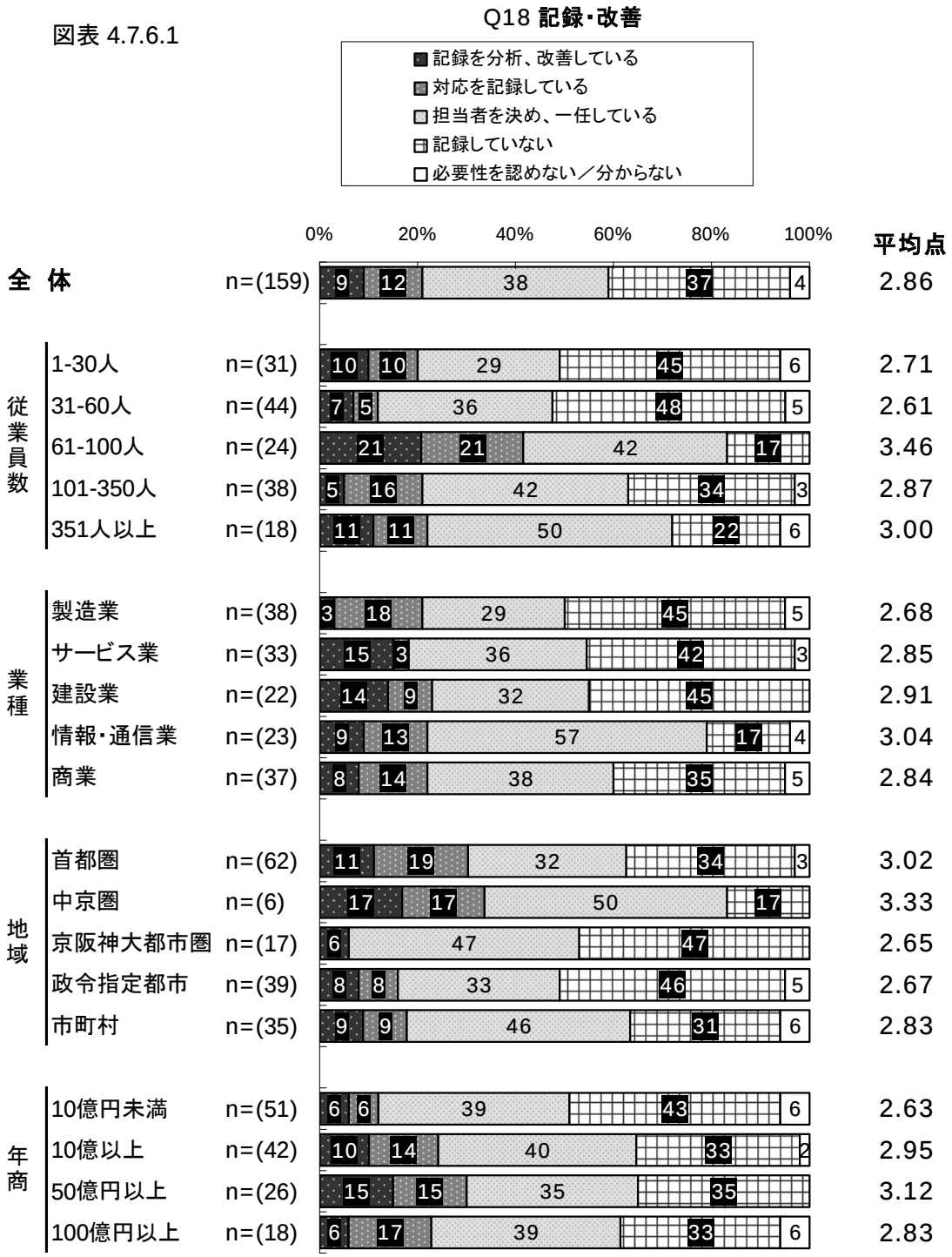
図表 4.7.5.1



4.7.6 エンドユーザ(EU)支援 −Q18 記録・改善

- 全体では 2.86 点となり、『記録を分析、改善している』は 9%となっている。
- 従業員規模別に見ると、「61～100 人」において最も点数が高く 3.46 点となっている。また、「61～100 人」で『記録を分析、改善している』の割合が最も高い。また、『記録していない』『必要性を認めない/分からない』というネガティブな回答の割合を見ると、「61～100 人」で最も少なく 2 割弱となっている。

図表 4.7.6.1

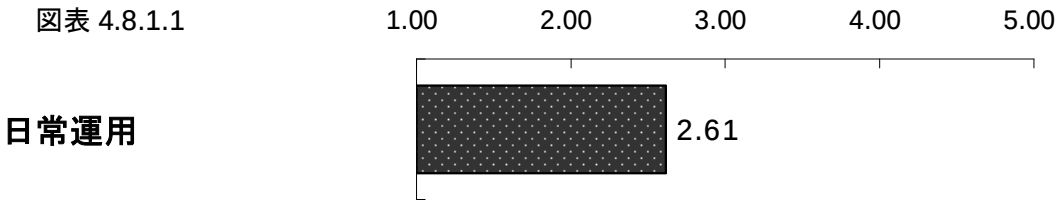


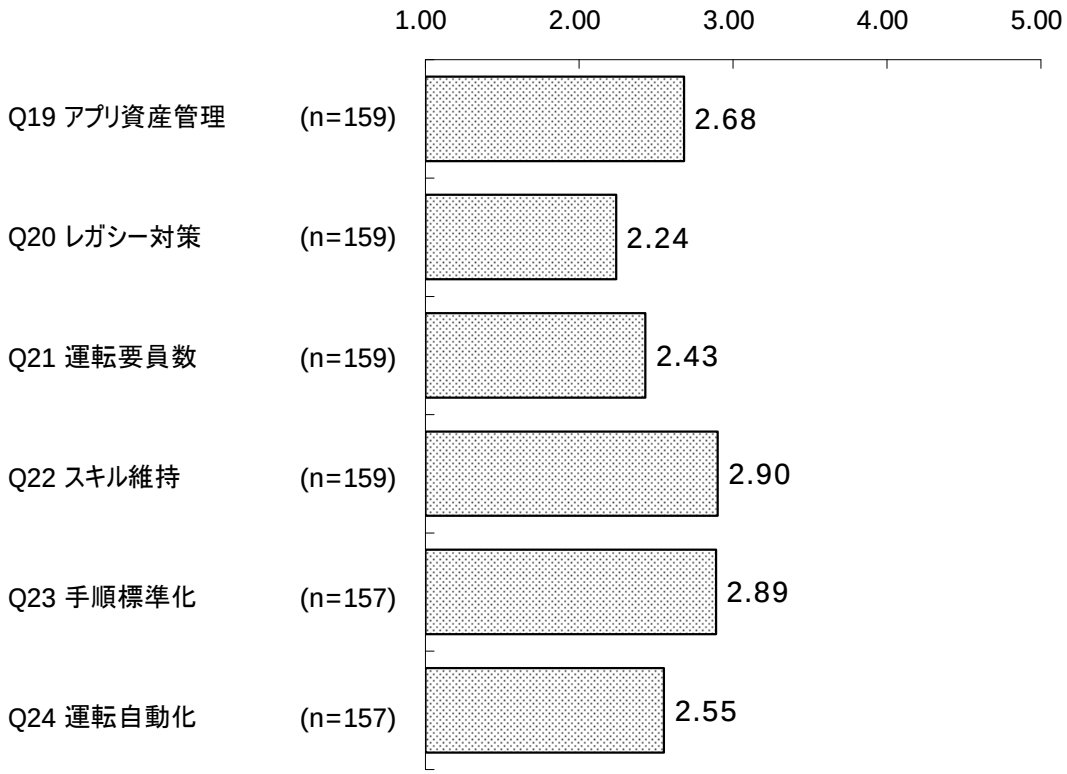
4.8 日常運用

4.8.1 日常運用

・ 日常運用については、全体で 2.61 点となり、日常運用に含まれる項目の得点を見ると、『スキル維持』が最も高く 2.90 点となっている。
・ 逆に最も低くなっているのが『レガシー対策』で 2.24 点である。

図表 4.8.1.1

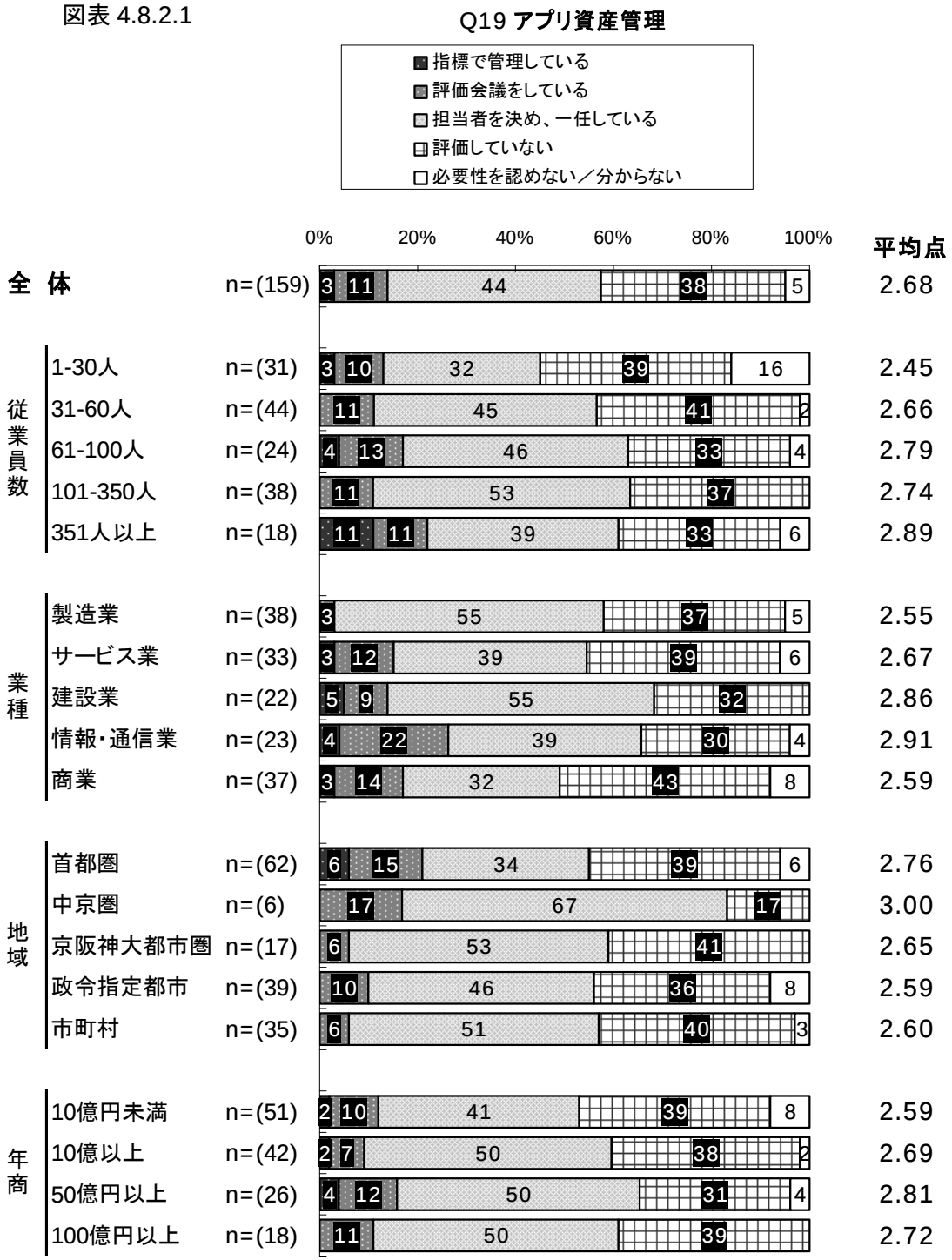




4.8.2 日常運用 –Q19 アプリ資産管理

- 全体では 2.68 点となり、『指標で管理している』は 3%となっている。
- 従業員規模別に見ると、「351 人以上」において最も点数が高く 3.89 点となっている。また、「31～60 人」と「101～350 人」で『指標で管理している』の割合が 0%となっており、「351 人以上」で同回答の割合が最も高い。
- 業種別に見ると、「情報・通信業」で最も点数が高く 2.91 点となっている。「製造業」で『指標で管理している』の割合が 0%となっているが、いずれの業種を見ても 4%前後と、あまり差は見られない。

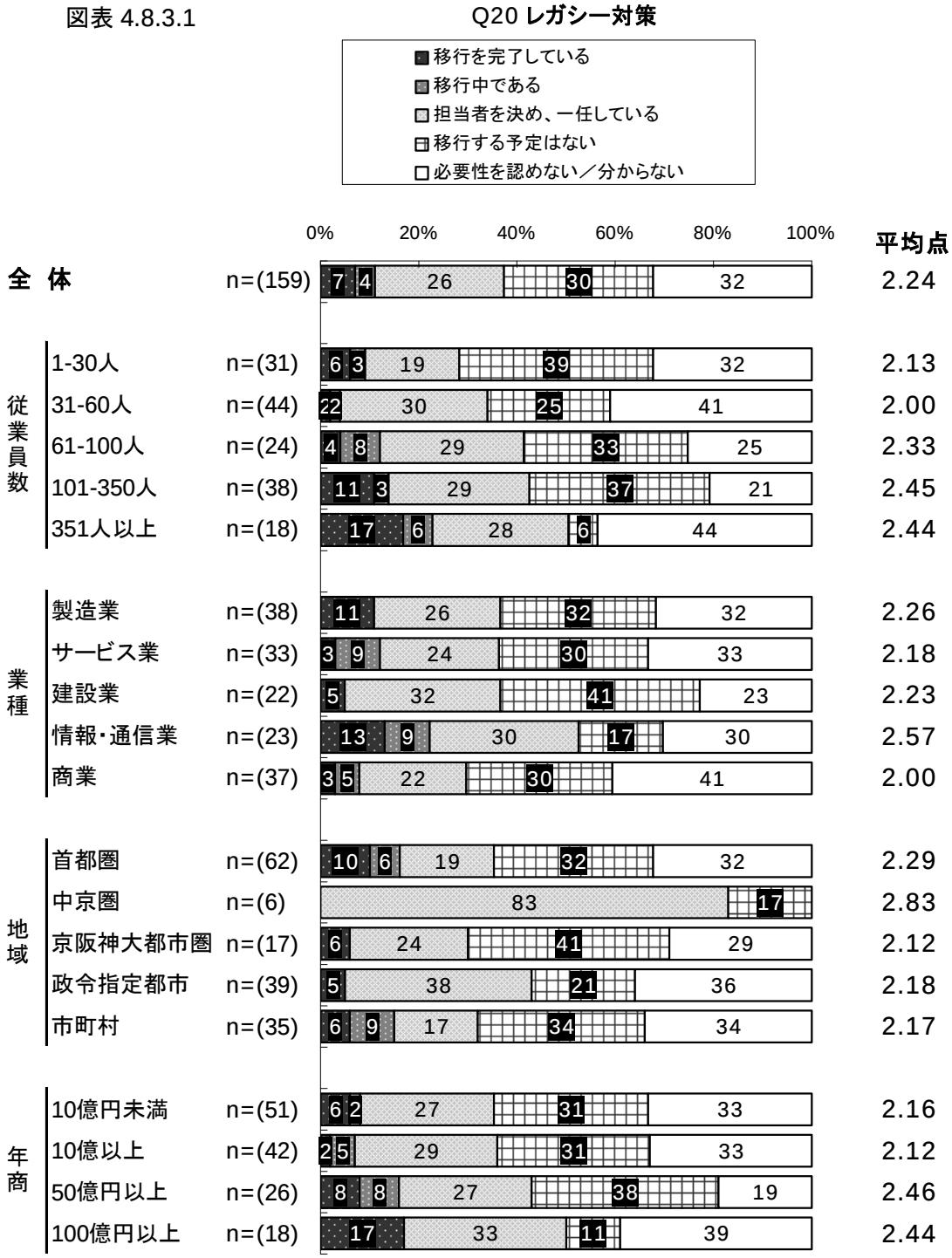
図表 4.8.2.1



4.8.3 日常運用 –Q20 レガシー対策

- 全体では 2.24 点となり、『移行を完了している』は 7%となっている。
- 従業員規模別に見ると、「351 人以上」において『移行を完了している』の割合が最も高く 17%となっているが一方で、『必要性を認めない/分からない』の割合も最も高く 44%である。
- 業種別に見ると、「情報・通信業」で最も点数が高く 2.57 点となっており、他の業種と比較して『移行を完了している』『移行中である』というポジティブな回答がやや多い。

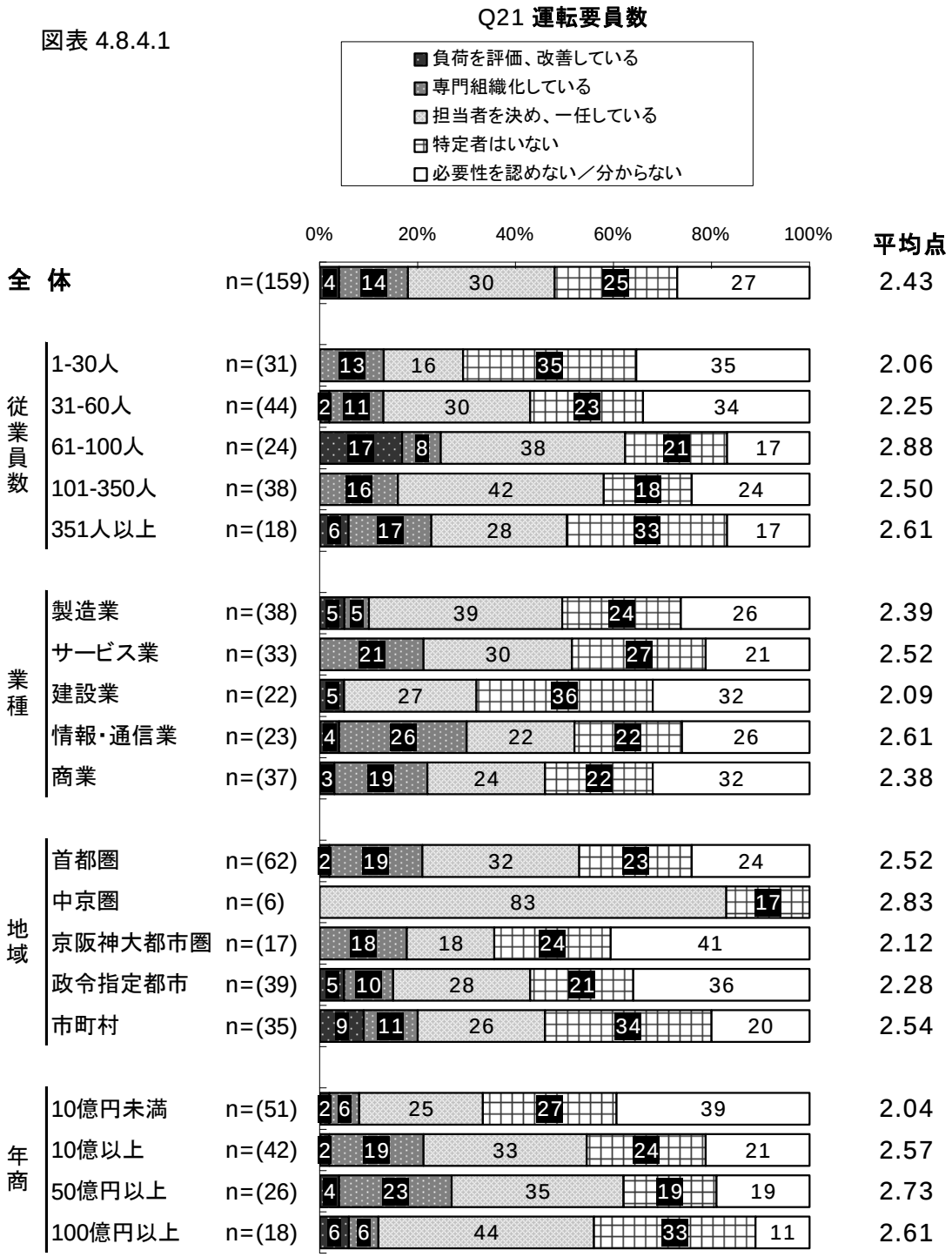
図表 4.8.3.1 Q20 レガシー対策



4.8.4 日常運用 –Q21 運転要員数

- 全体では 2.43 点となり、『負荷を評価、改善している』は 4%となっている。
- 従業員規模別に見ると、「61～100 人」で最も点数が高く 2.88 点となっている。また、「1～30 人」と「101～350 人」で『負荷を評価、改善している』の割合が 0%となり、「61～100 人」で 17%と最も高い。
- 業種別に見ると、「情報・通信業」が最も高く 2.61 点となっている。また、『負荷を評価、改善している』の割合が「サービス業」で 0%となっているが、他の業種間で比較するといずれも 4%前後と値に大きな差は見られない。

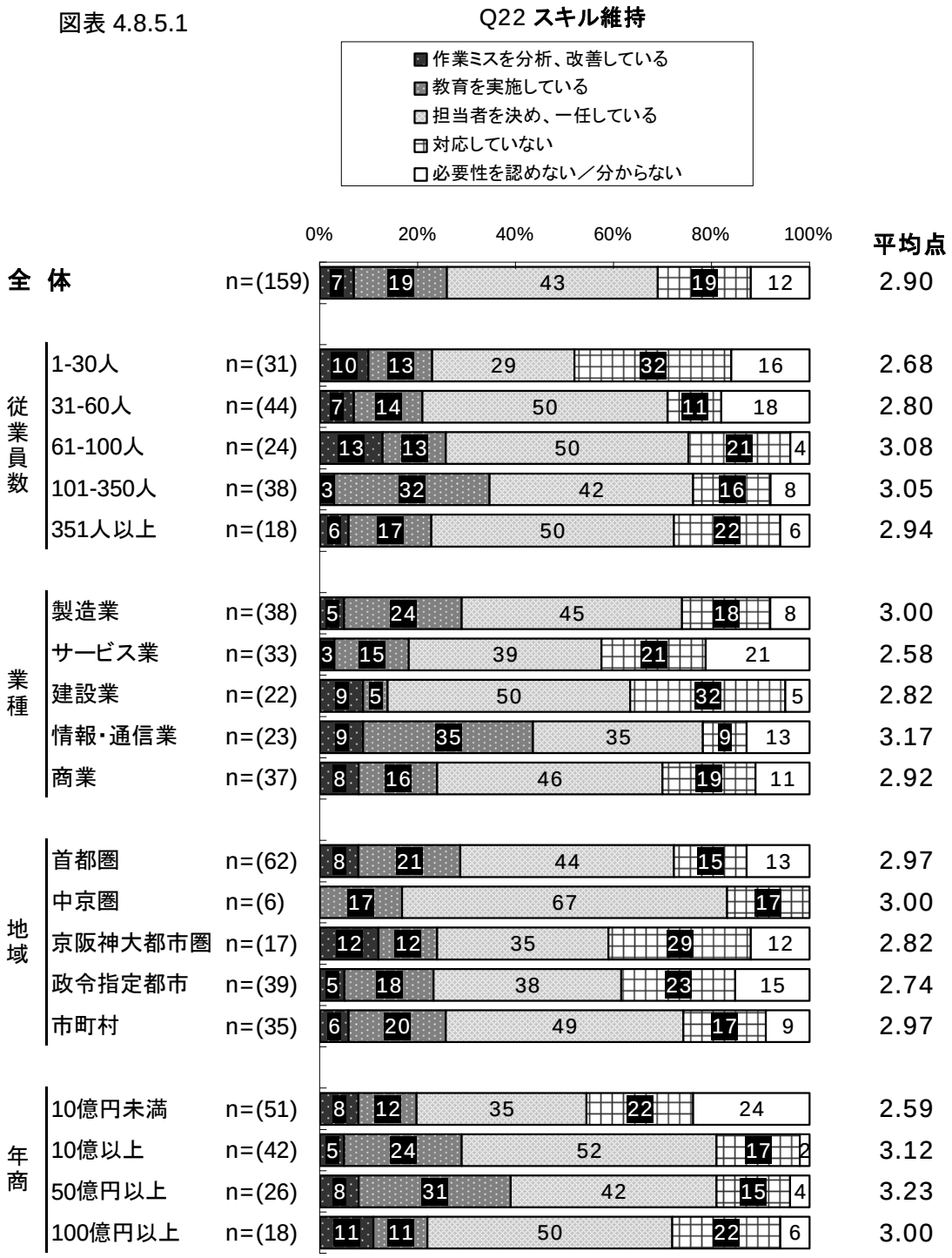
図表 4.8.4.1



4.8.5 日常運用 –Q22 スキル維持

- 全体では 2.90 点となり、『作業ミスを分析、改善している』は 7%となっている。
- 従業員規模別に見ると、61 人以上の規模では、点数が 3 点程度と値に大きな差は見られない。また、「1～30 人」で『対応しいてない』『必要性を認めない/分からない』というネガティブな回答の割合が最も高く 5 割弱である。

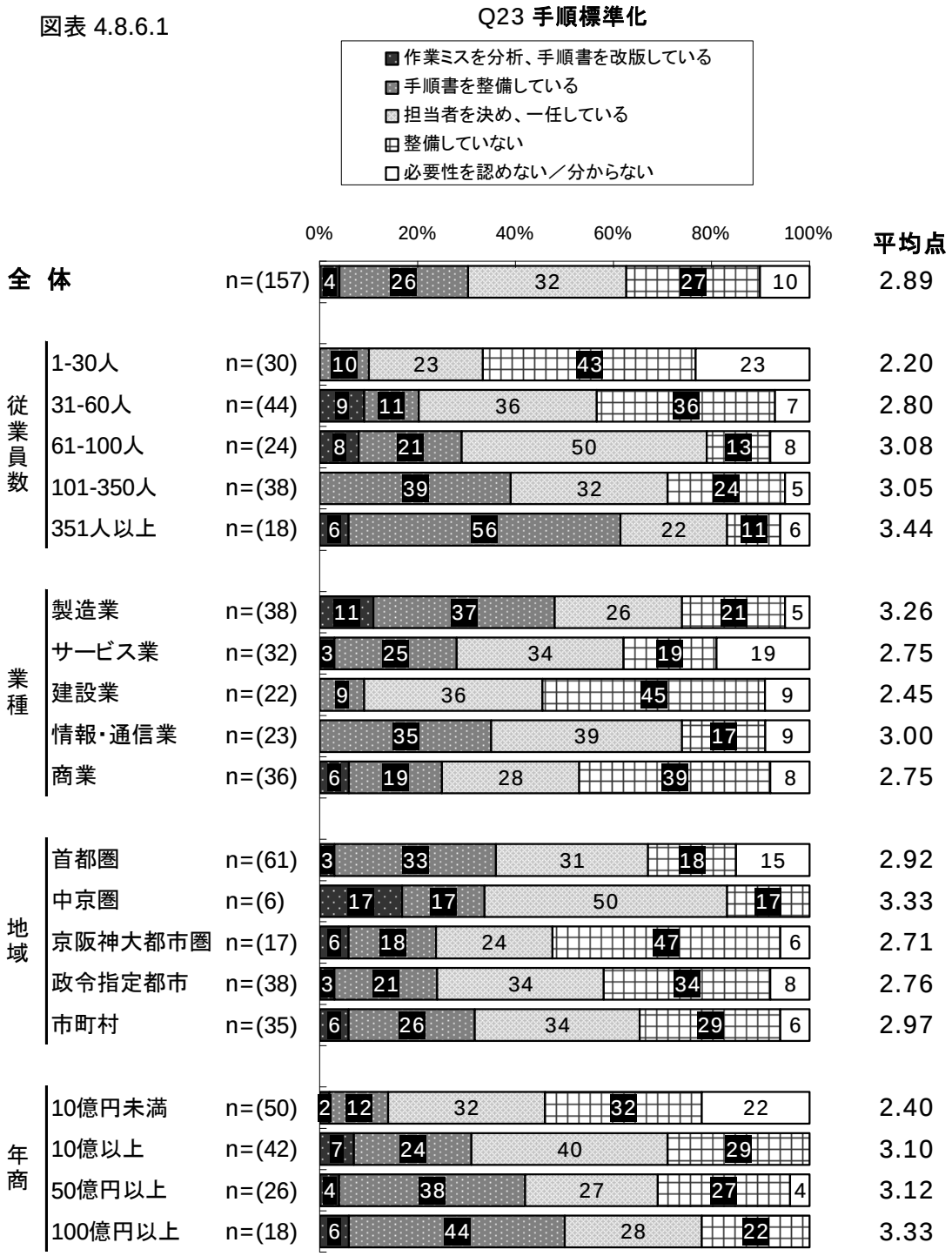
図表 4.8.5.1



4.8.6 日常運用 –Q23 手順標準化

- 全体では 2.89 点となり、『作業ミスを分析、手順書を改版している』は 4%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 3.44 点であった。『作業ミスを分析、手順書を改版している』と回答する割合に大きな値の違いは見られないが、規模が大きくなるにつれ『手順書を整備している』と回答する割合が高くなる。
- 業種別に見ると、「情報・通信業」で最も点数が高く 3.00 点であった。また、「建設業」と「情報・通信業」で『作業ミスを分析、手順を改版している』と回答する割合が 0%であった。

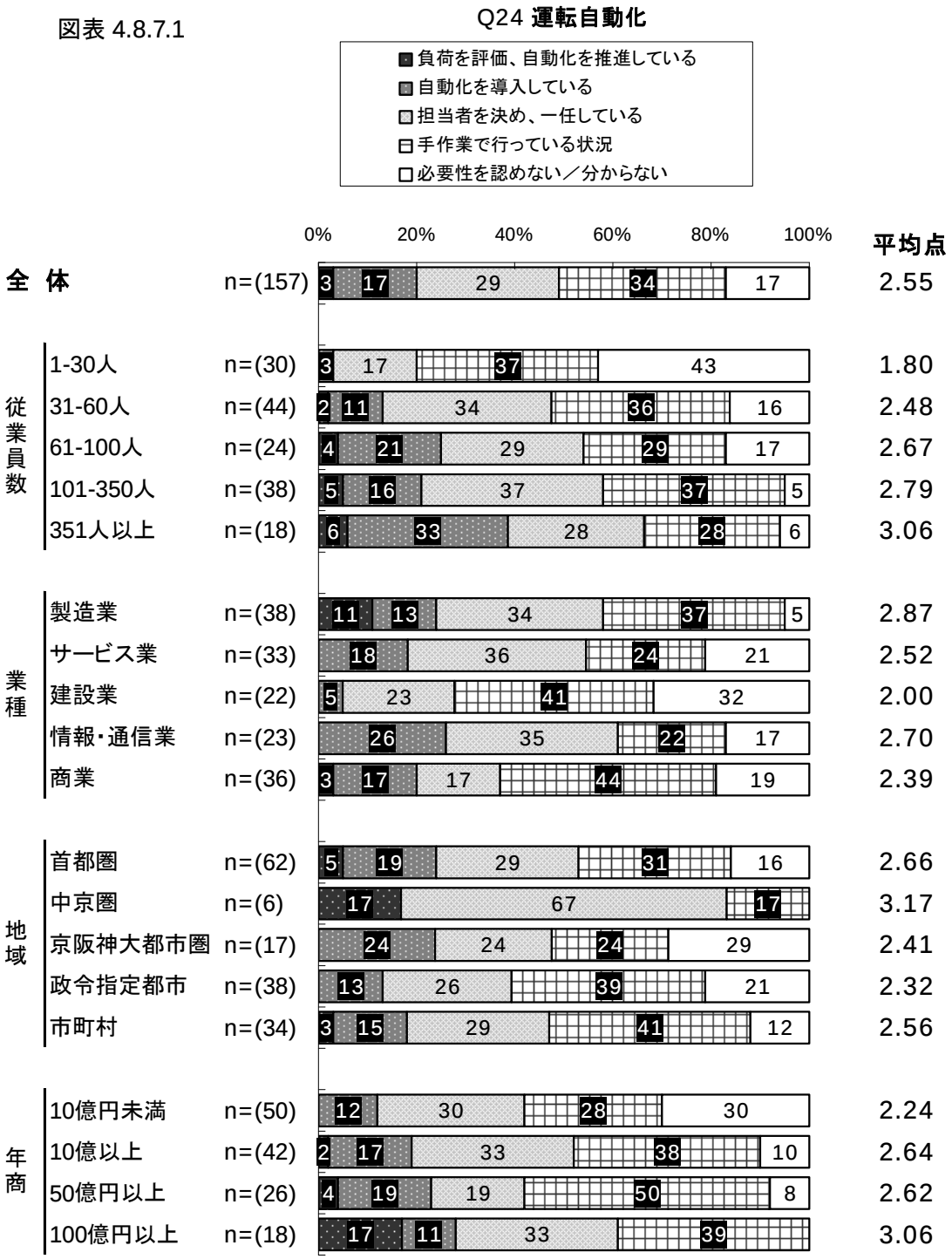
図表 4.8.6.1



4.8.7 日常運用 –Q24 運転自動化

- 全体では 2.55 点となり、『負荷を評価、自動化を推進している』は 3%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 3.06 点で、「1～30 人」では非常に点数が低く 1.80 点となっている。「1～30 人」では『負荷を評価、自動化を推進している』の割合が 0%で、『必要性を認めない/分からない』の割合が最も高く 43%である。

図表 4.8.7.1

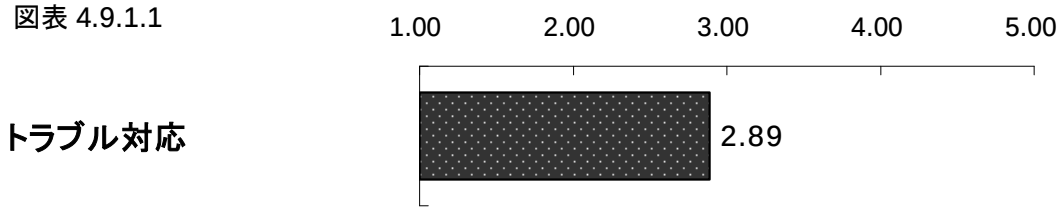


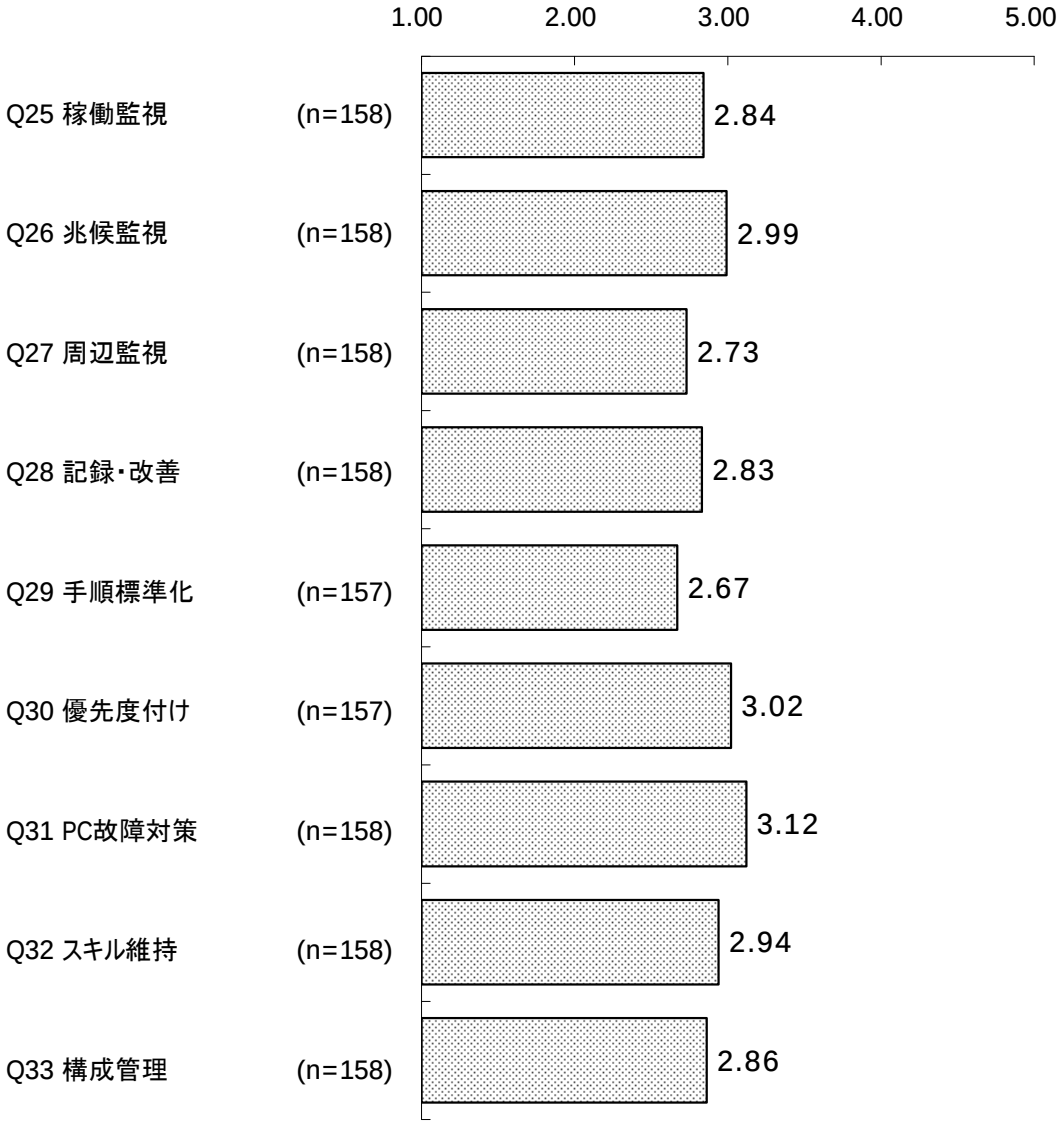
4.9 トラブル対応

4.9.1 トラブル対応

・ トラブル対応については、全体で 2.89 点となり、トラブル対応に含まれる項目の得点を見ると、『PC 故障対策』が最も高く 3.12 点となっている。

図表 4.9.1.1

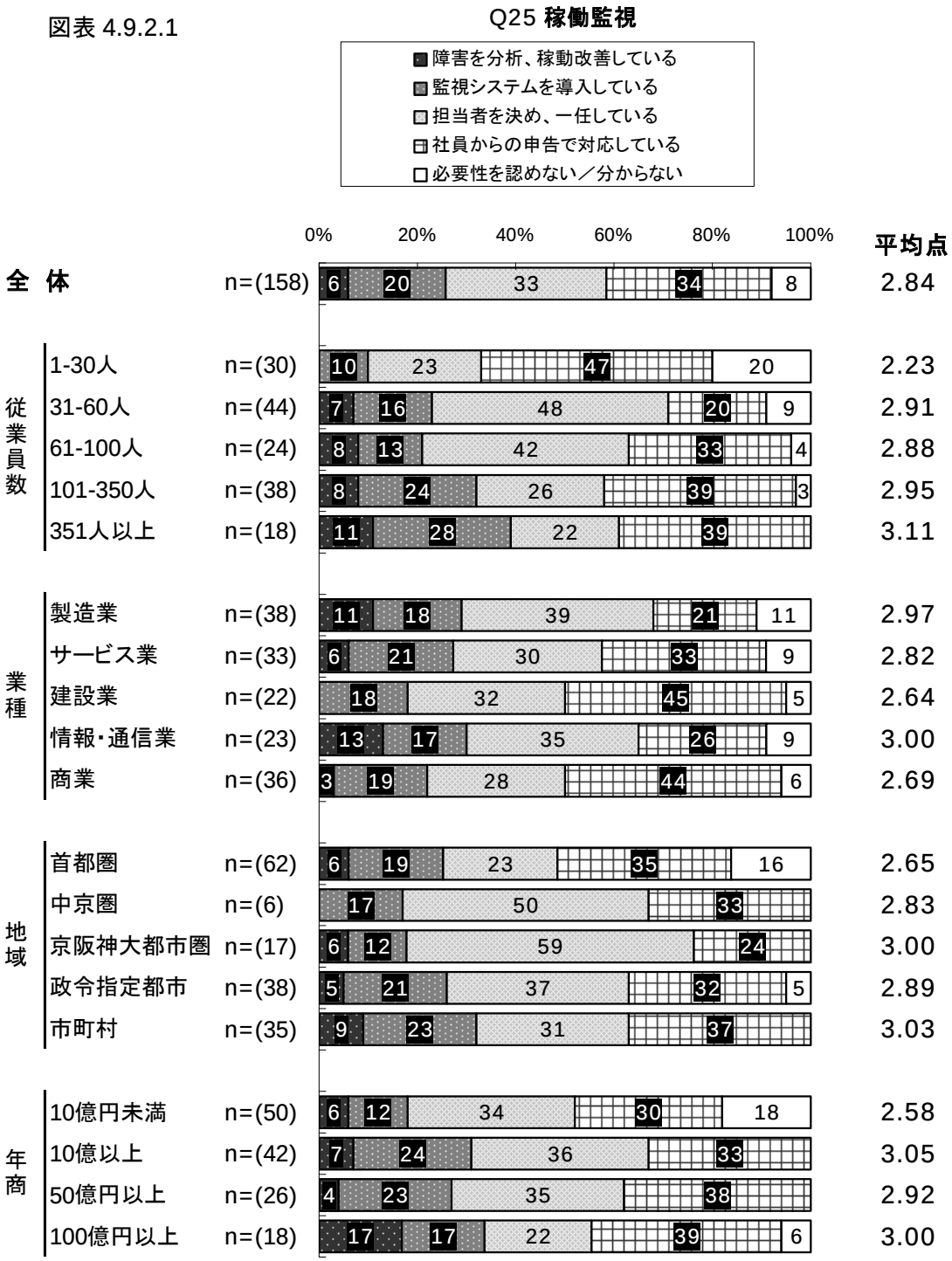




4.9.2 トラブル対応 −Q25 稼動監視

- 全体では 2.84 点となり、『障害を分析、稼動改善している』は 6%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 3.11 点であった。「1～30 人」で『障害を分析、稼動改善している』の割合が 0%となっている。また、規模が大きくなるにつれて『必要性を認めない/分からない』の割合は小さくなっている。

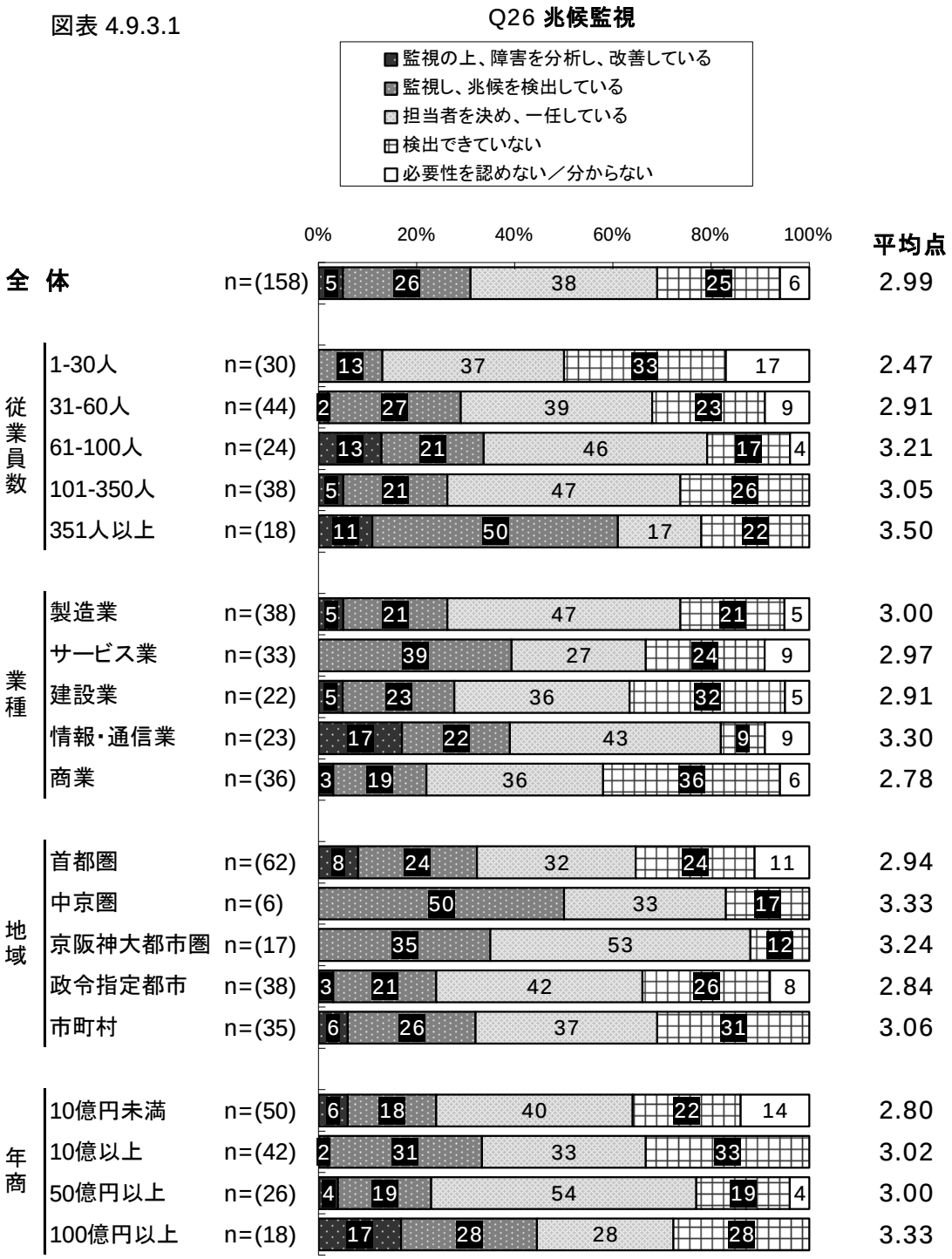
図表 4.9.2.1



4.9.3 トラブル対応 −Q26 兆候監視

- 全体では 2.99 点となり、『監視の上、障害を分析し、改善している』は 5%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 3.50 点であった。『監視の上、障害を分析し、改善している』『監視し、兆候を検出している』というポジティブな回答の割合は「351 人以上」において高くなる。
- 業種別に見ると、いずれの業種でも『必要性を認めない/分からない』が数%ずつ出現している。

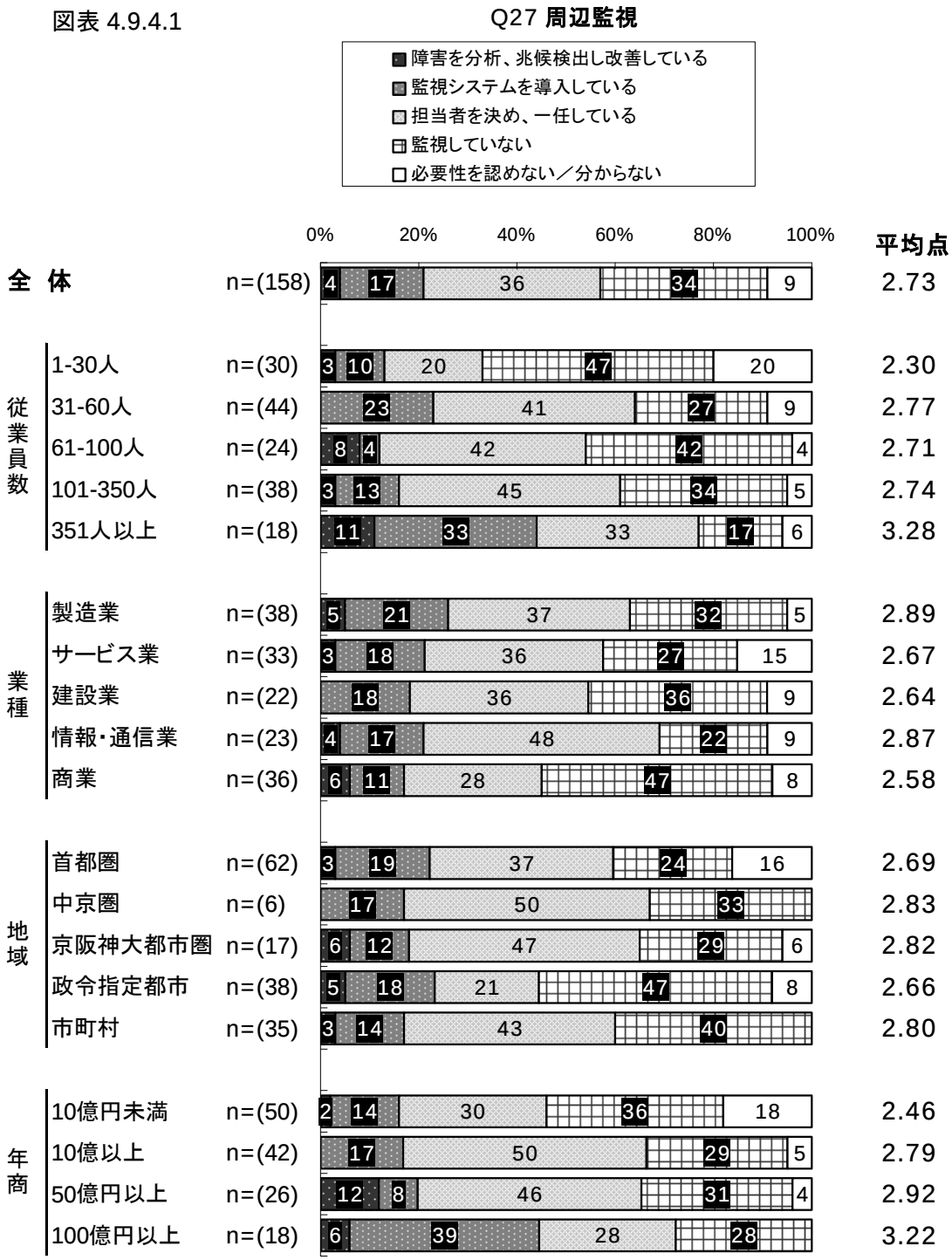
図表 4.9.3.1



4.9.4 トラブル対応 −Q27 周辺監視

- 全体では 2.73 点となり、『障害を分析、兆候検出し改善している』は 4%となっている。
- 従業員規模別に見ると、「351 人以上」で点数が 3.28 点と最も高くなっている。また、他の規模と比較して「1～30 人」で『監視していない』『必要性を認めない/分からない』というネガティブな回答の割合が高く 7 割弱となっている。

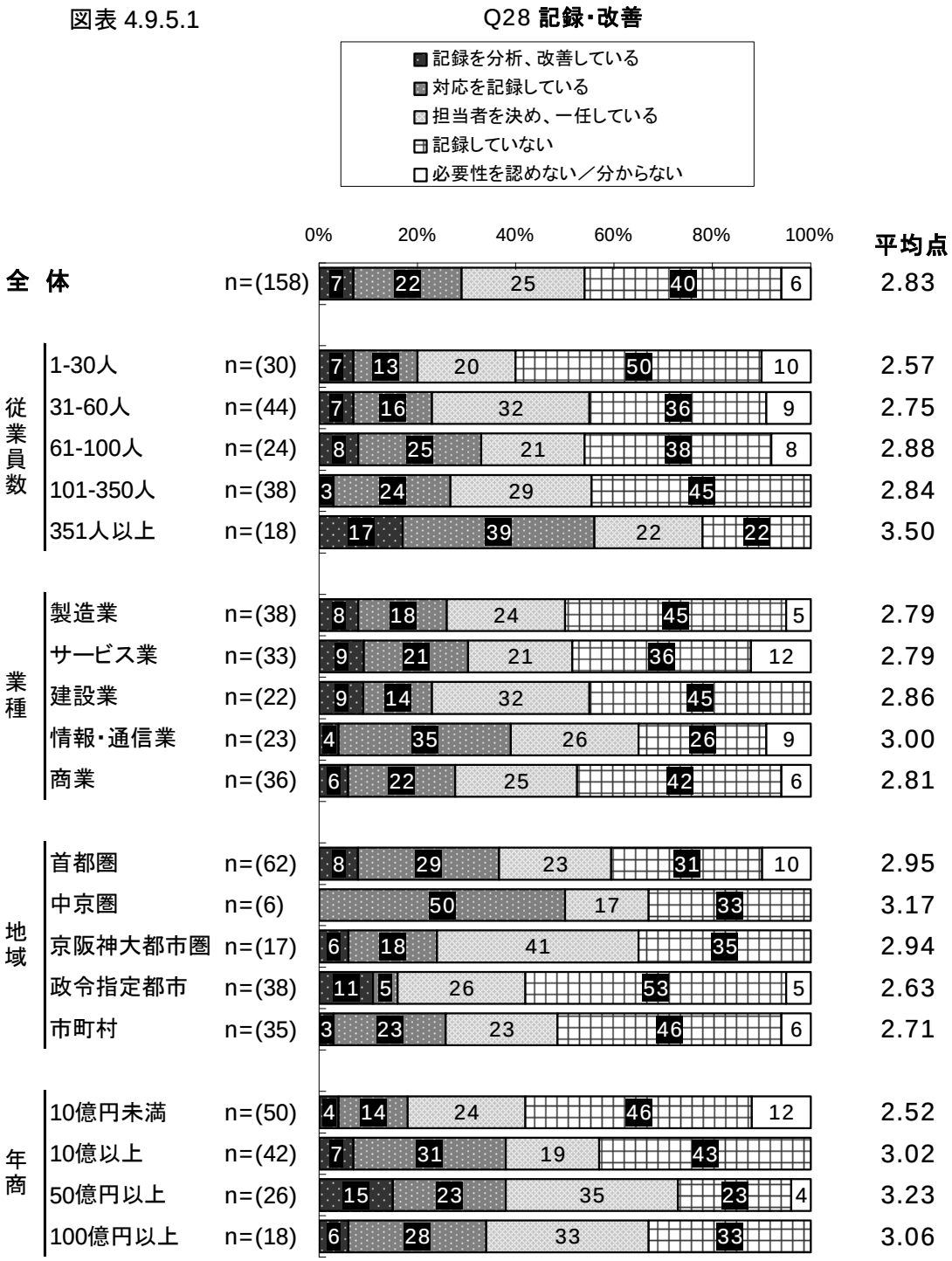
図表 4.9.4.1



4.9.5 トラブル対応 −Q28 記録・改善

- 全体では 2.83 点となり、『記録を分析、改善している』は 7%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 3.50 点となっている。また、101 人以上の規模では、『必要性を認めない/分からない』の割合が 0%となっている。
- 業種別に見ると、「建設業」においてのみ『必要性を認めない/分からない』の割合が 0%となっている。

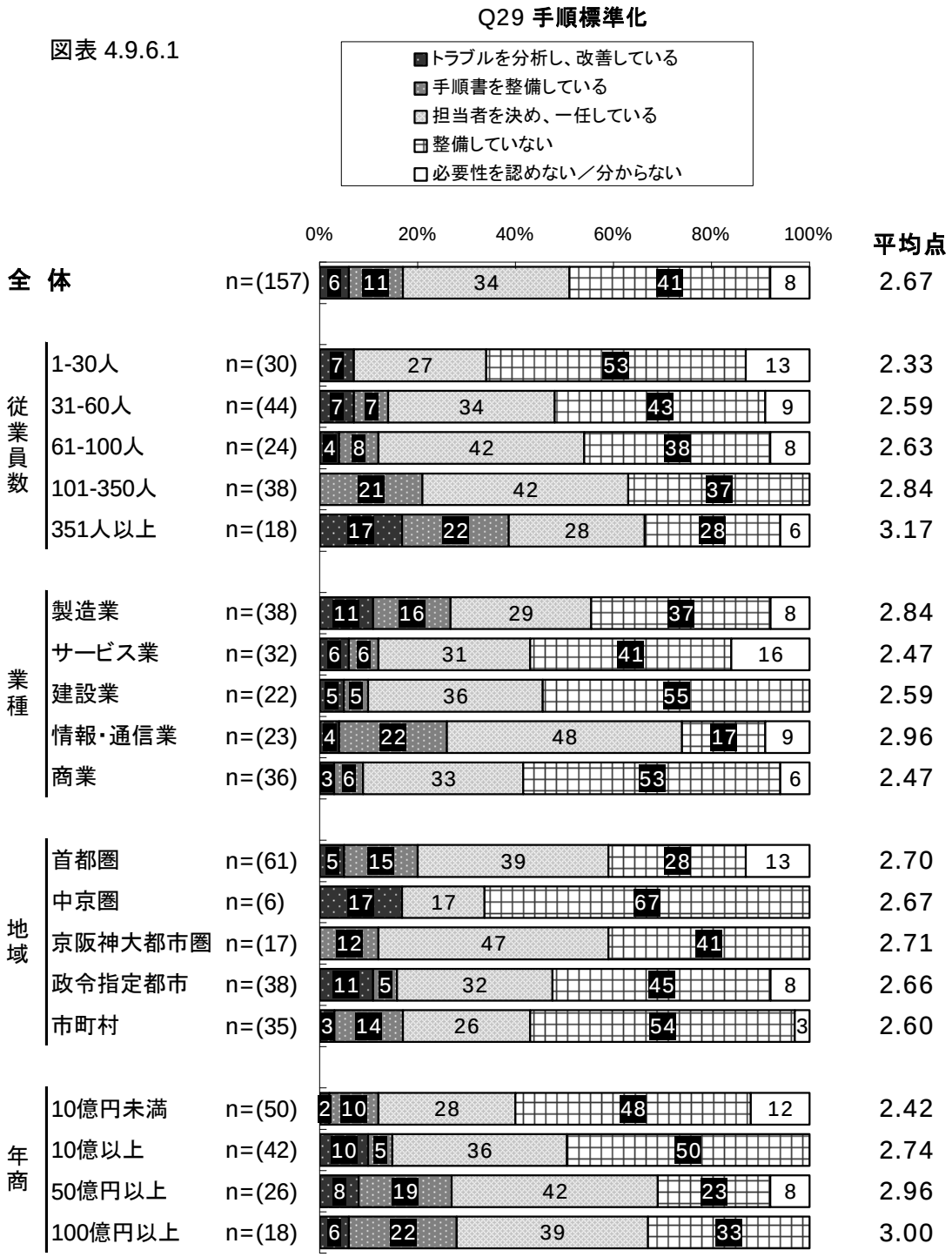
図表 4.9.5.1



4.9.6 トラブル対応 −Q29 手順標準化

- 全体では 2.67 点となり、『トラブルを分析し、改善している』は 6%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 3.17 点となっている。また、『整備していない』『必要性を認めない/分からない』というネガティブな回答の割合は、規模が大きくなるにつれて低くなっている。
- 業種別に見ると、「製造業」と「情報・通信業」において『トラブルを分析し、改善している』『手順書を整備している』の割合が高い。

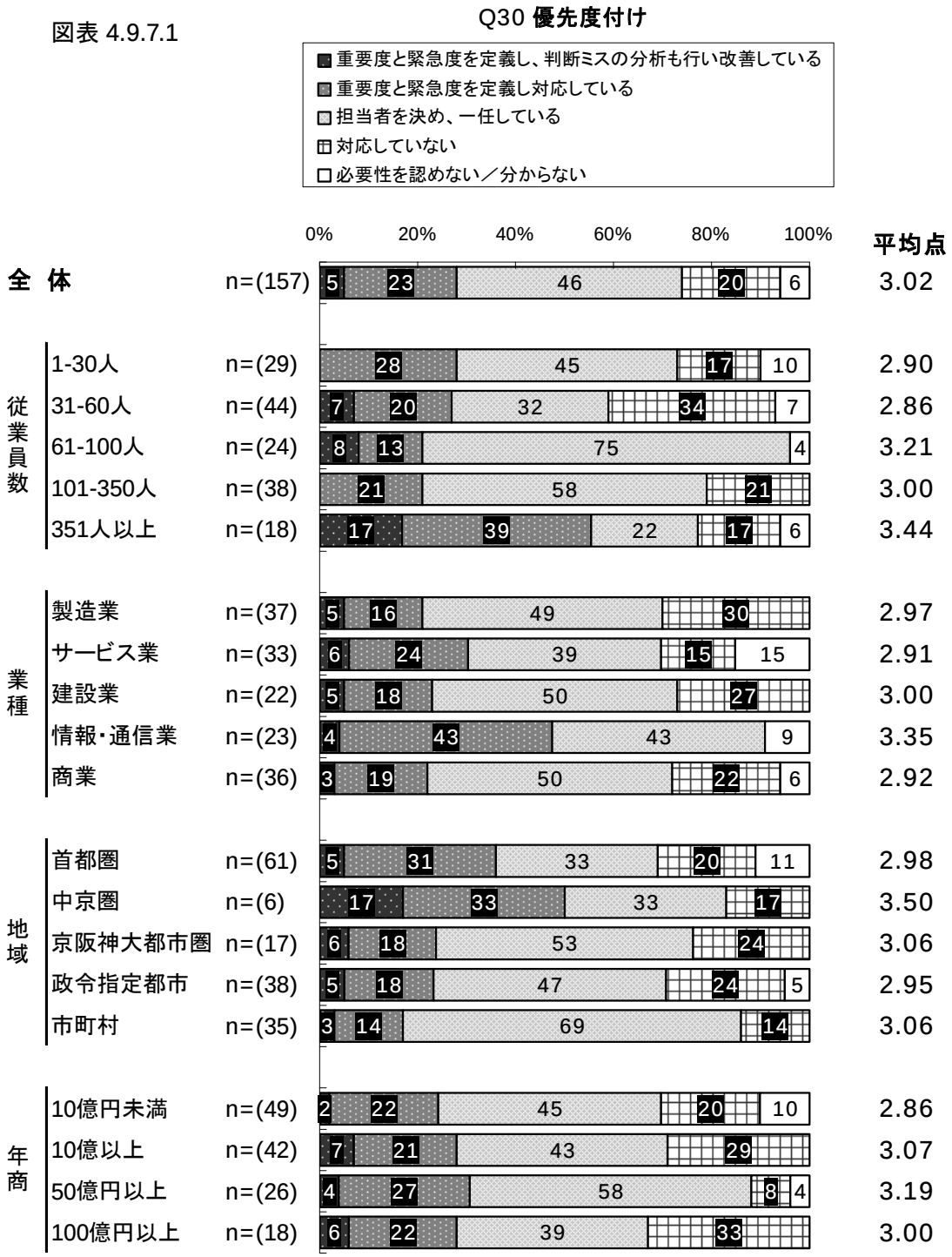
図表 4.9.6.1



4.9.7 トラブル対応 −Q30 優先度付け

- 全体では 3.02 点となり、『重要度と緊急度を定義し、判断ミスの分析も行い改善している』は 5%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 3.44 点であった。他の規模と比較して「351 人以上」で『重要度と緊急度を定義し、判断ミスの分析も行い改善している』『重要度と緊急度を定義し対応している』というポジティブな回答の割合が高く 5 割以上である。また、「61～100 人」規模では『担当者を決め、一任している』の割合が 75%と非常に高い。

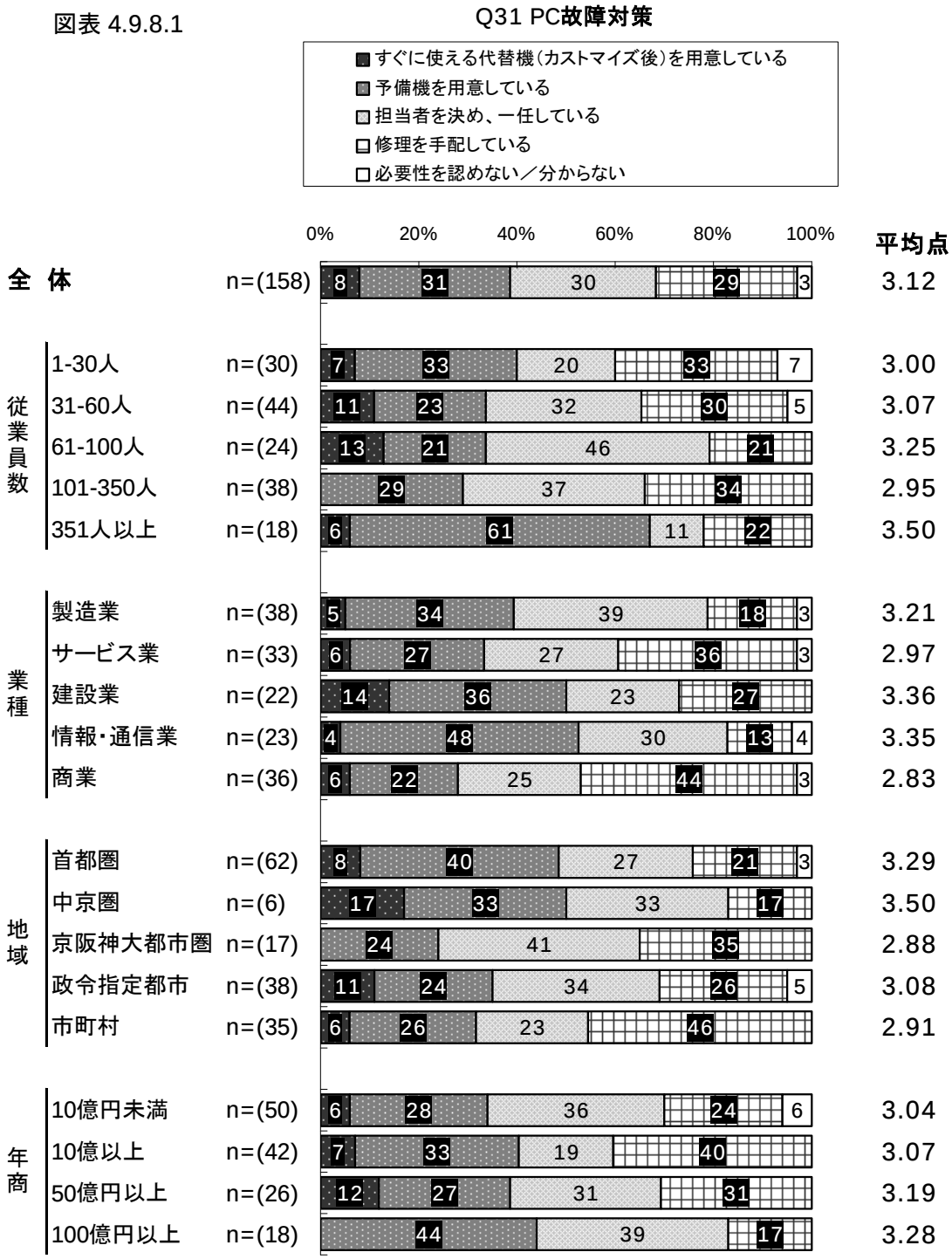
図表 4.9.7.1



4.9.8 トラブル対応 −Q31 PC 故障対策

- 全体では 3.12 点となり、『すぐに使える代替機（カストマイズ後）を用意している』は 8%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 3.50 点で、『予備機を用意している』の割合が非常に高い。
- 業種別に見ると、他の業種と比較して「建設業」において『すぐに使える代替機（カストマイズ後）を用意している』の割合が最も高く 14%であった。

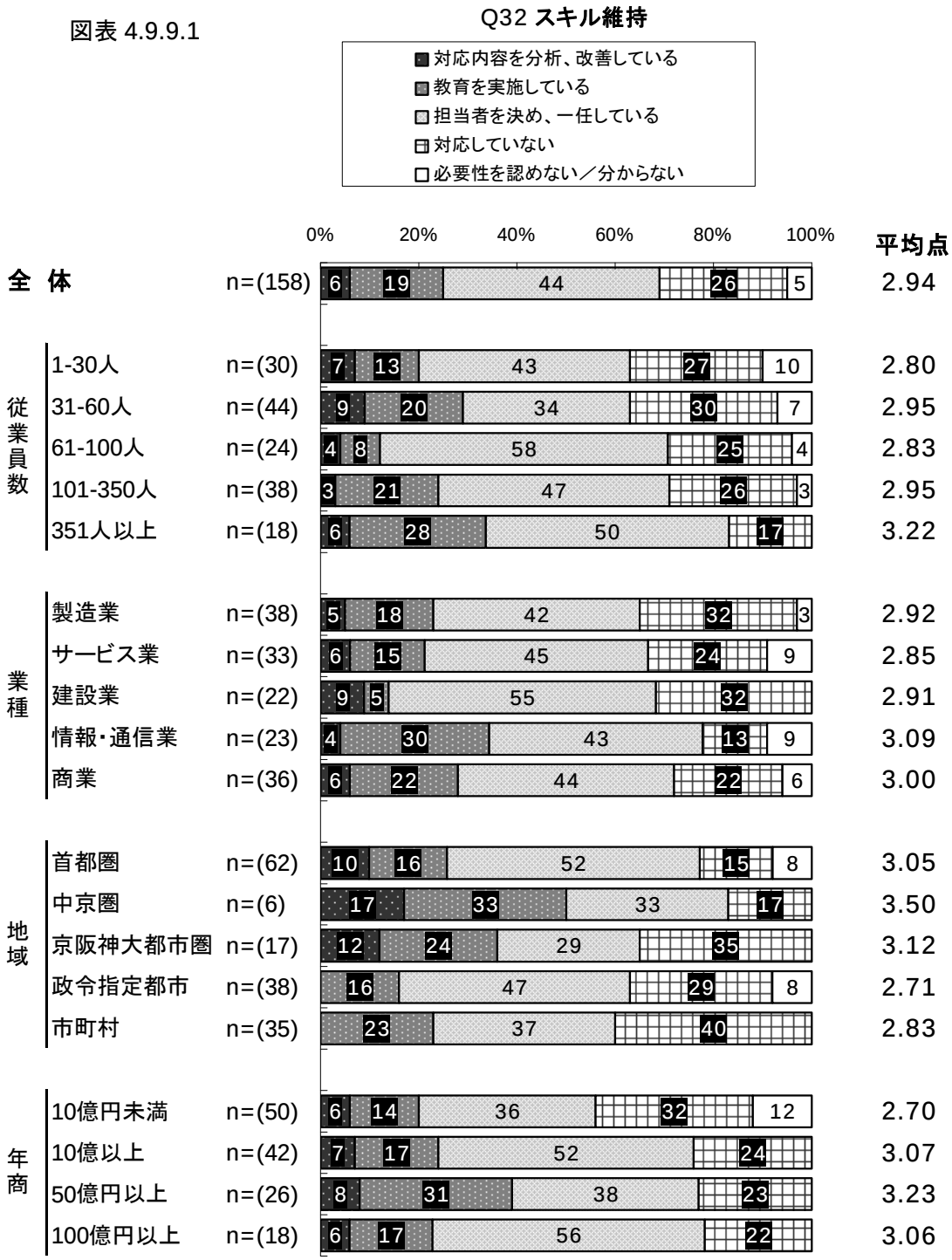
図表 4.9.8.1



4.9.9 トラブル対応 −Q32 スキル維持

- 全体では 2.94 点となり、『対応内容を分析、改善している』は 6%となっている。
- 従業員規模別に見ると、「351 人以上」において最も点数が高く 3.22 点となっている。また、『対応していない』『必要性を認めない/分からない』というネガティブな回答は、規模が大きくなるにつれて減少する傾向にある。
- 業種別に見ると、いずれの業種でも『担当者を決め、一任している』と回答する割合が高い。

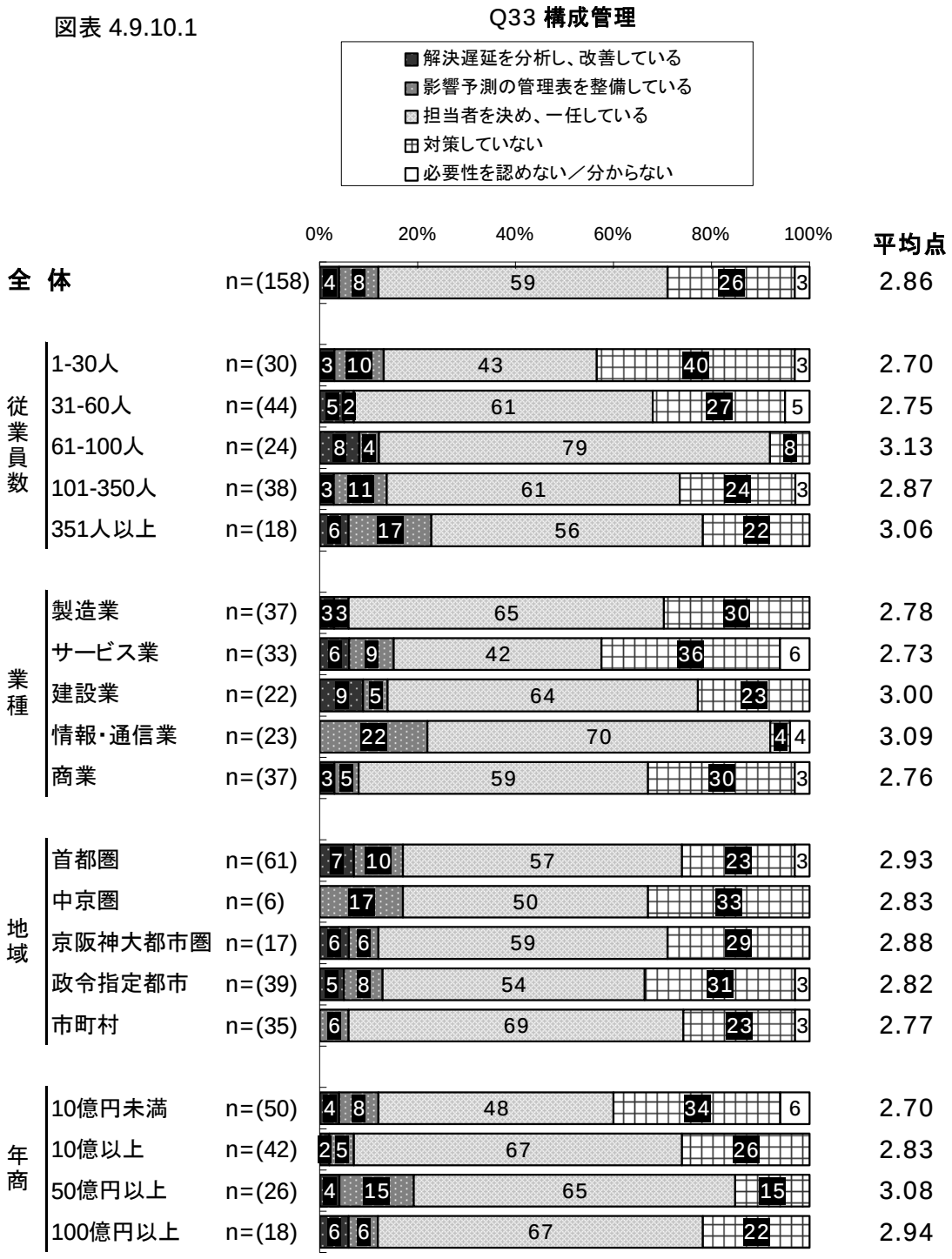
図表 4.9.9.1



4.9.10 トラブル対応 –Q33 構成管理

- 全体では 2.86 点となっており、『解決遅延を分析し、改善している』は 4%となっている。
- 従業員規模別に見ると、「61～100 人」で最も点数が高く 3.13 点となり、「61～100 人」において『担当者を決め、一任している』と回答する割合が非常に高く 8 割程度を占めている。
- 業種別に見ると、「情報・通信業」で点数が最も高く 3.09 点であるが、一方で「情報・通信業」は『解決遅延を分析し、改善している』の割合は 0%と最も少ない。

図表 4.9.10.1

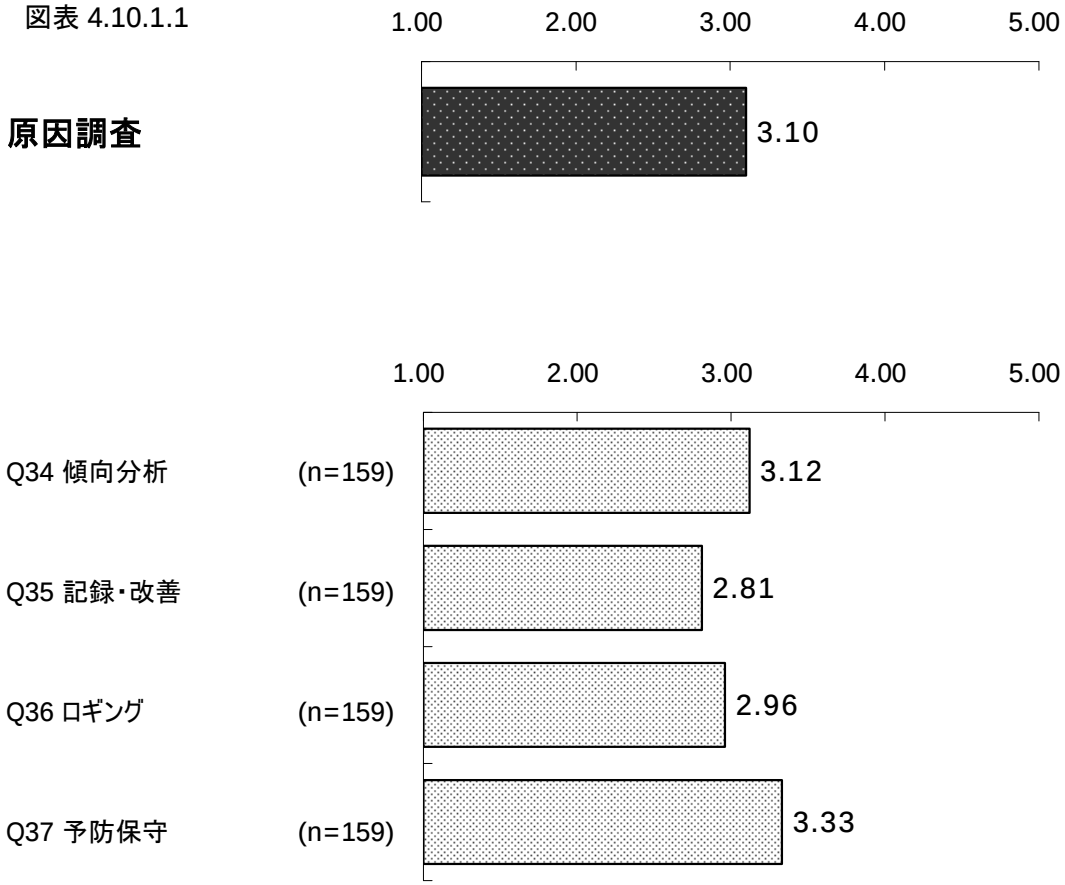


4.10 原因調査

4.10.1 原因調査

・ 原因調査については、全体で 3.10 点となり、原因調査に含まれる項目の得点を見ると、『予防保守』が最も高く 3.33 点となっている。
・ 逆に最も低くなっているのが『記録・改善』で 2.81 点である。

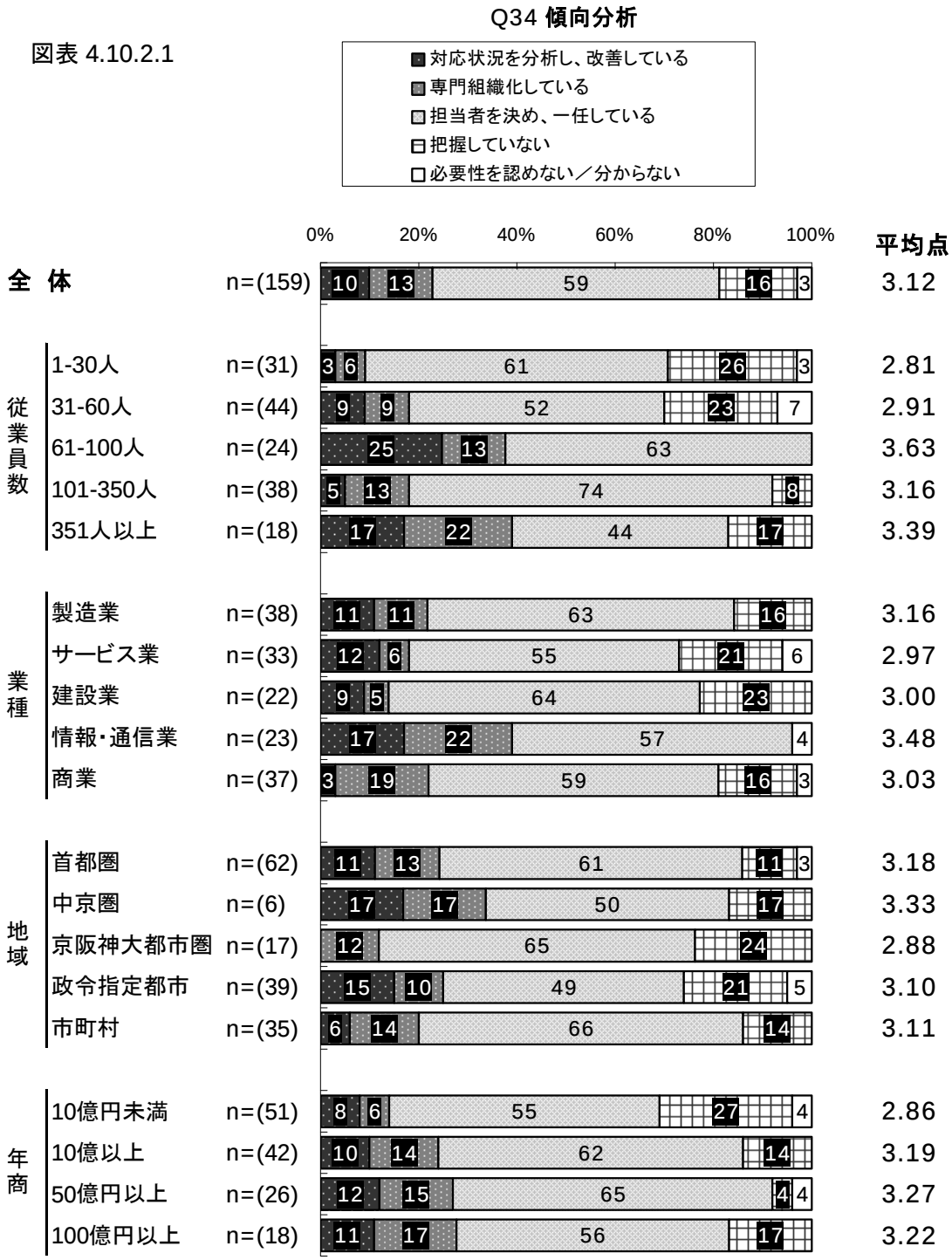
図表 4.10.1.1



4.10.2 原因調査 -Q34 傾向分析

- 全体では 3.12 点となり、『対応状況を分析し、改善している』は 10%となっている。
- 従業員規模別に見ると、「61～100 人」で最も点数が高く 3.63 点となっている。「61～100 人」と「351 人以上」で『対応状況を分析し、改善している』『専門組織化している』というポジティブな回答の割合が高い。また、「61～100 人」では『把握していない』『必要性を認めない/分からない』というネガティブな回答が見られない。
- 業種別に見ると、他の業種と比較して「情報・通信業」において『対応状況を分析し、改善している』『専門組織化している』というポジティブな回答の割合が高い。

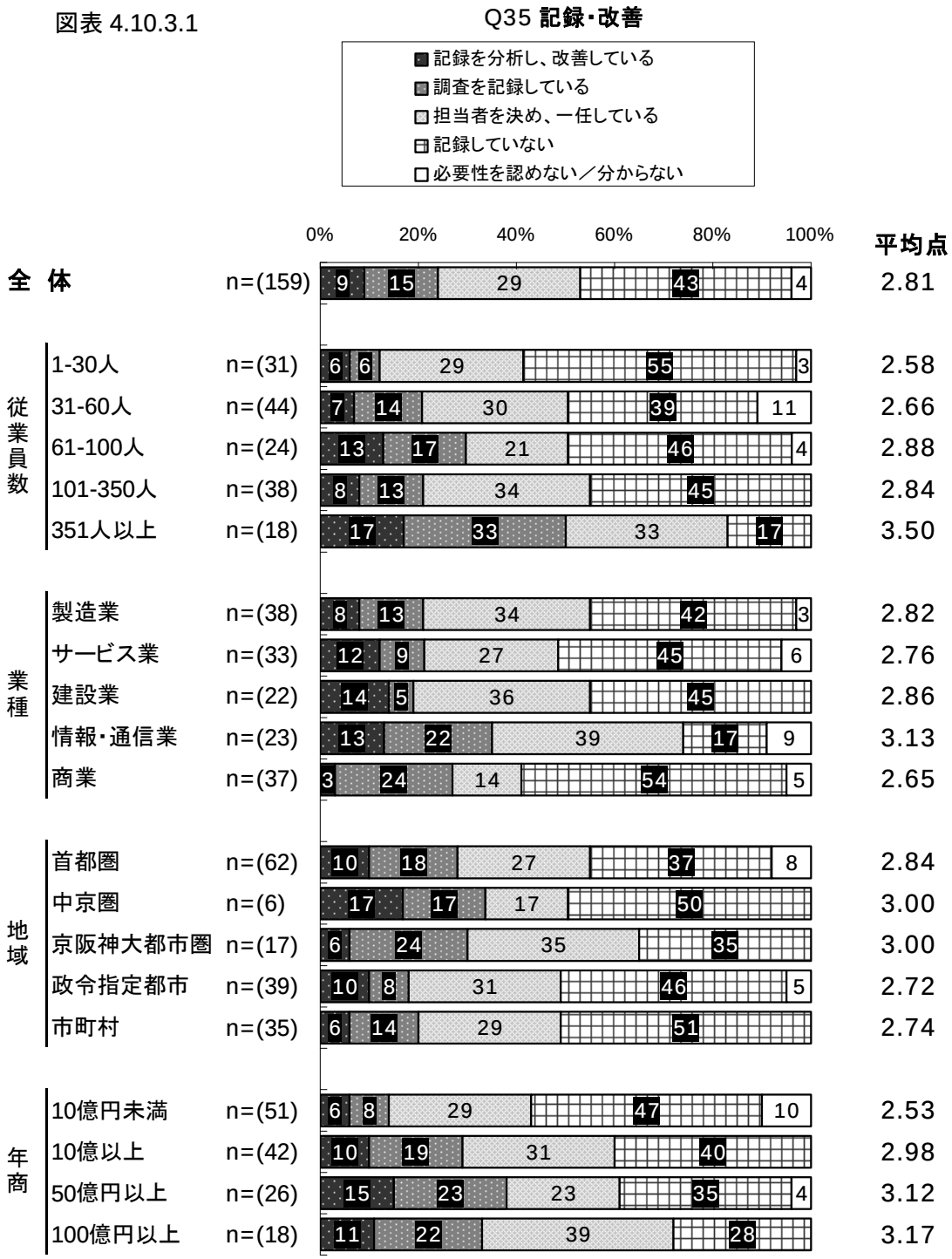
図表 4.10.2.1



4.10.3 原因調査 –Q35 記録・改善

- 全体では 2.81 点となり、『記録を分析し、改善している』は 9%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 3.50 点となっており、他の規模と比較して『記録を分析し、改善している』『調査を記録している』というポジティブな回答の割合が高い。また、350 人以下の規模では『記録していない』『必要性を認めない/分からない』というネガティブな回答の割合が 5 割程度を占めている。

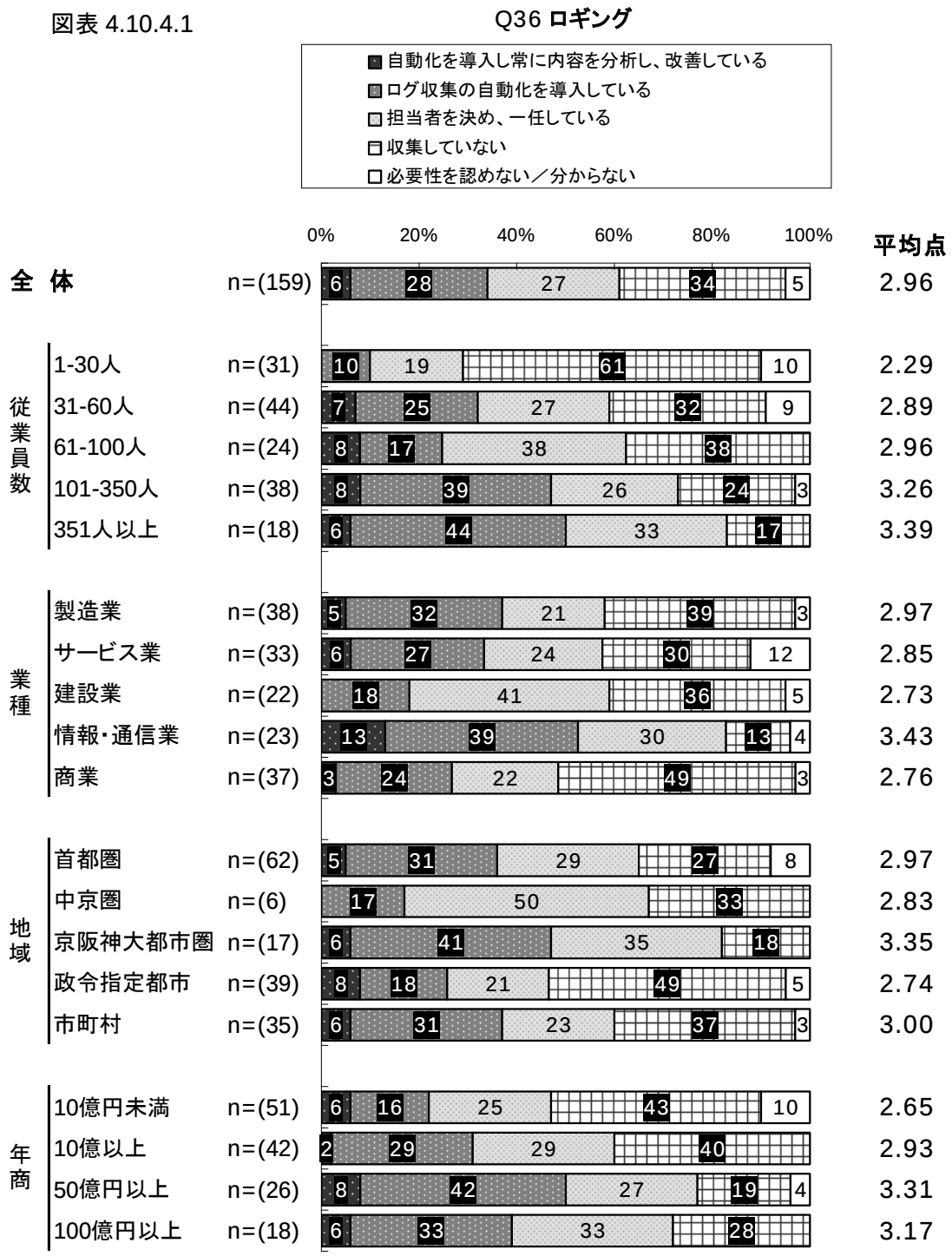
図表 4.10.3.1



4.10.4 原因調査 –Q36 ロギング

- 全体では 2.96 点となり、『自動化を導入し常に内容を分析し、改善している』は 6%である。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 3.39 点となっている。また、規模が大きくなるにつれて『収集していない』『必要性を認めない/分からない』というネガティブな回答の割合は低くなる。

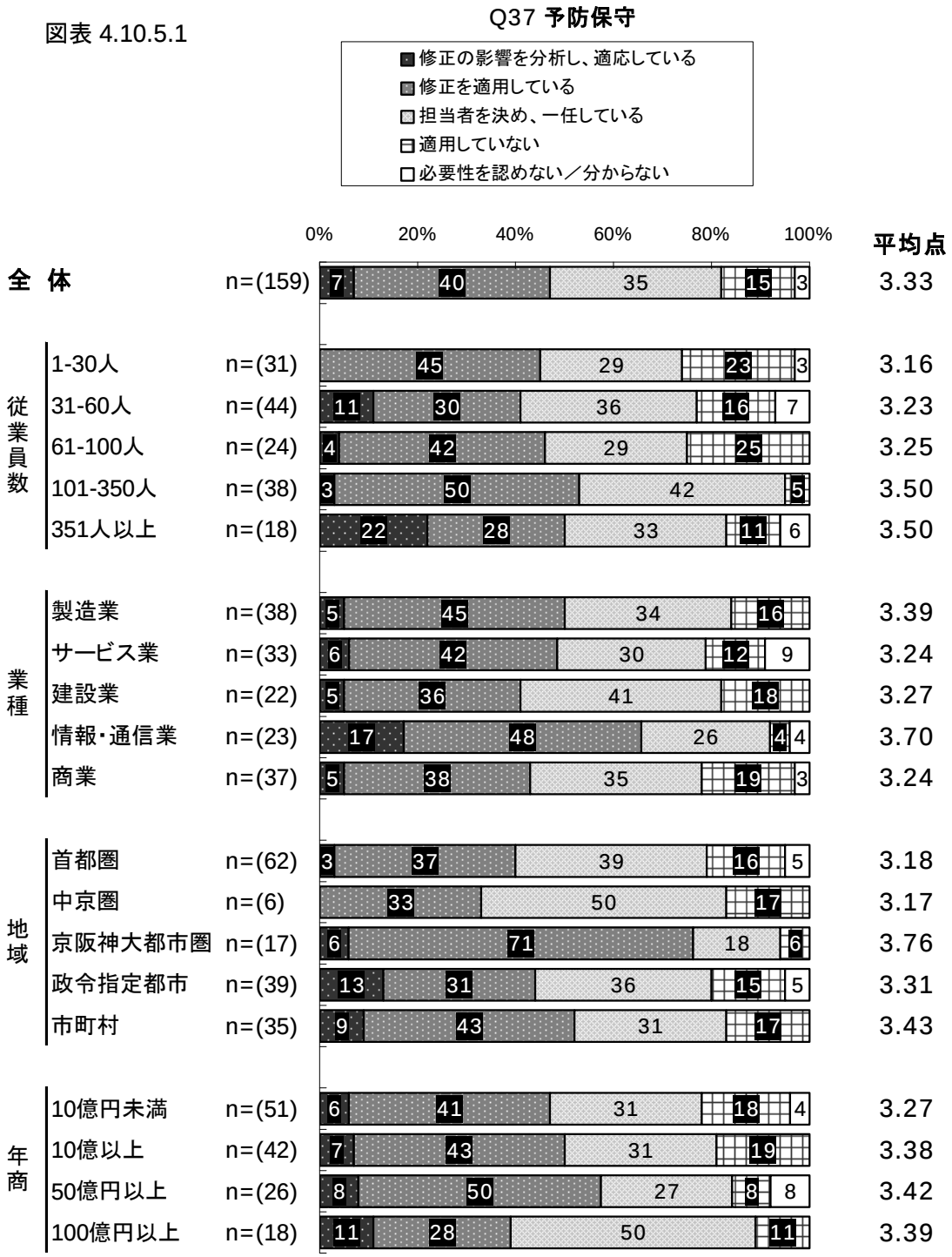
図表 4.10.4.1



4.10.5 原因調査 –Q37 予防保守

- 全体では 3.33 点となり、『修正の影響を分析し、適応している』は 7%となっている。
- 従業員規模別に見ると、『修正の影響を分析し、適応している』割合が「1～30 人」では 0%と低く、「351 人以上」で 22%と最も高い。
- 業種別に見ると、「情報・通信業」で最も点数が高く 3.70 点となっており、他の業種と比較して『修正の影響を分析し、適応している』『修正を適用している』というポジティブな回答の割合が高くなっているが、他の業種間ではいずれの項目においても大きな差は見られない。

図表 4.10.5.1

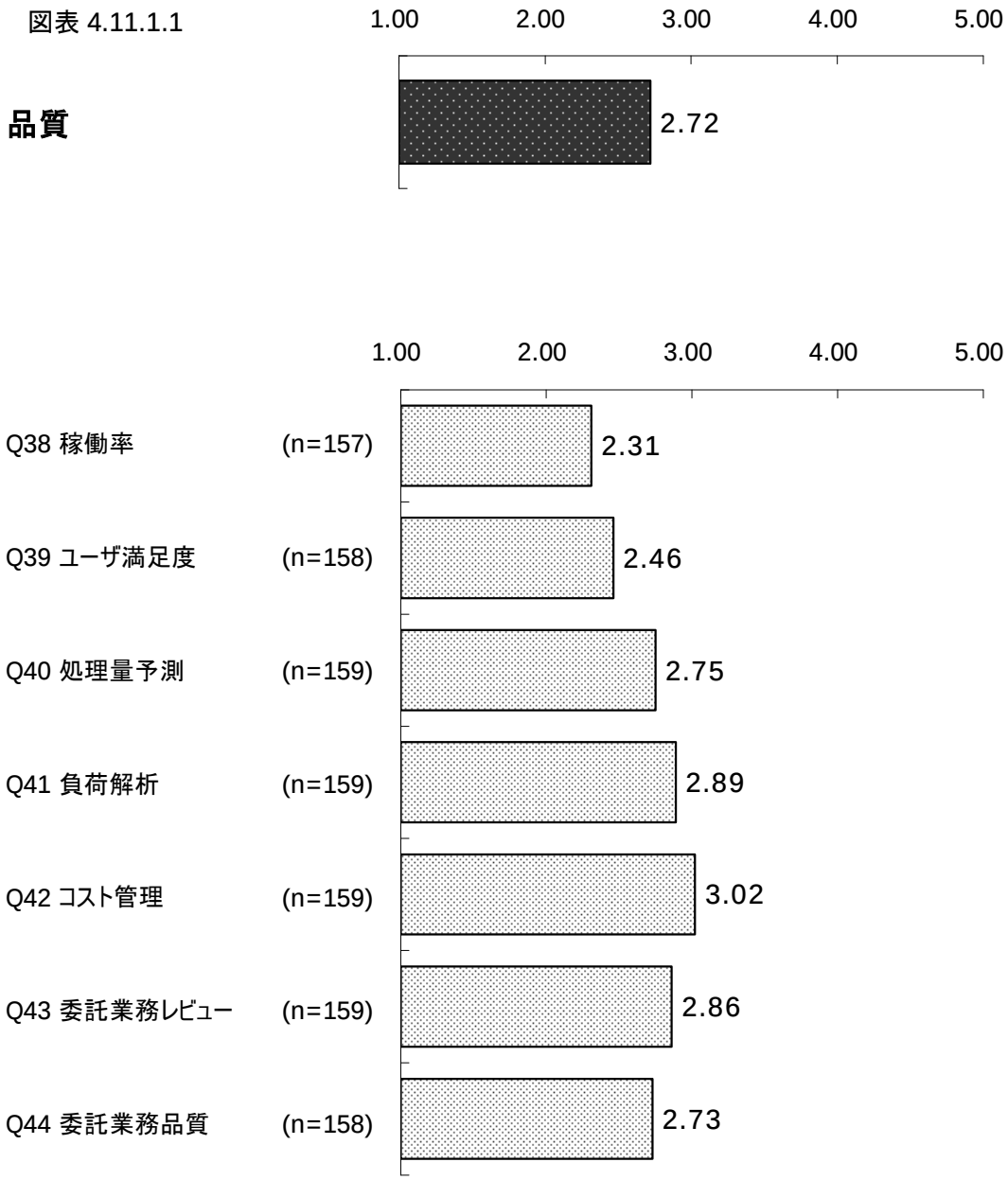


4.11 品質

4.11.1 品質

・ 品質については、全体で 2.72 点となり、品質に含まれる項目の得点を見ると、『コスト管理』が最も高く 3.02 点となっている。
・ 逆に最も低くなっているのが『稼働率』で 2.31 点である。

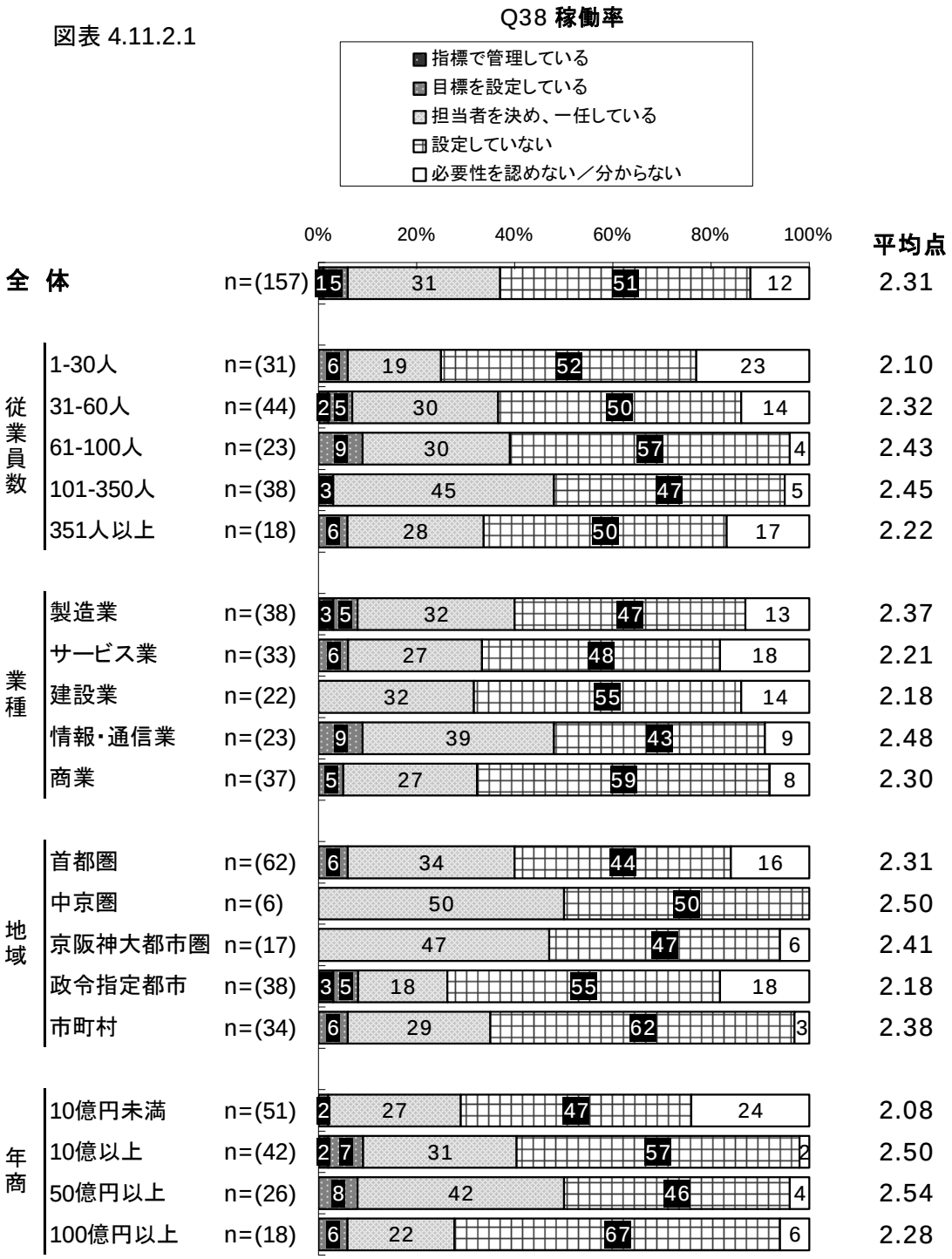
図表 4.11.1.1



4.11.2 品質 -Q38 稼働率

- 全体では 2.31 点となり、『指標で管理している』は 1%となっている。
- 従業員規模別に見ると、いずれの規模においても『指標で管理している』『目標を設定している』というポジティブな回答の割合は少なく 1 割に満たない。
- 業種別に見ると、「情報・通信業」で最も点数が高く 2.48 点となっている。また、「建設業」では『指標で管理している』『目標を設定している』というポジティブな項目の割合が 0%である。

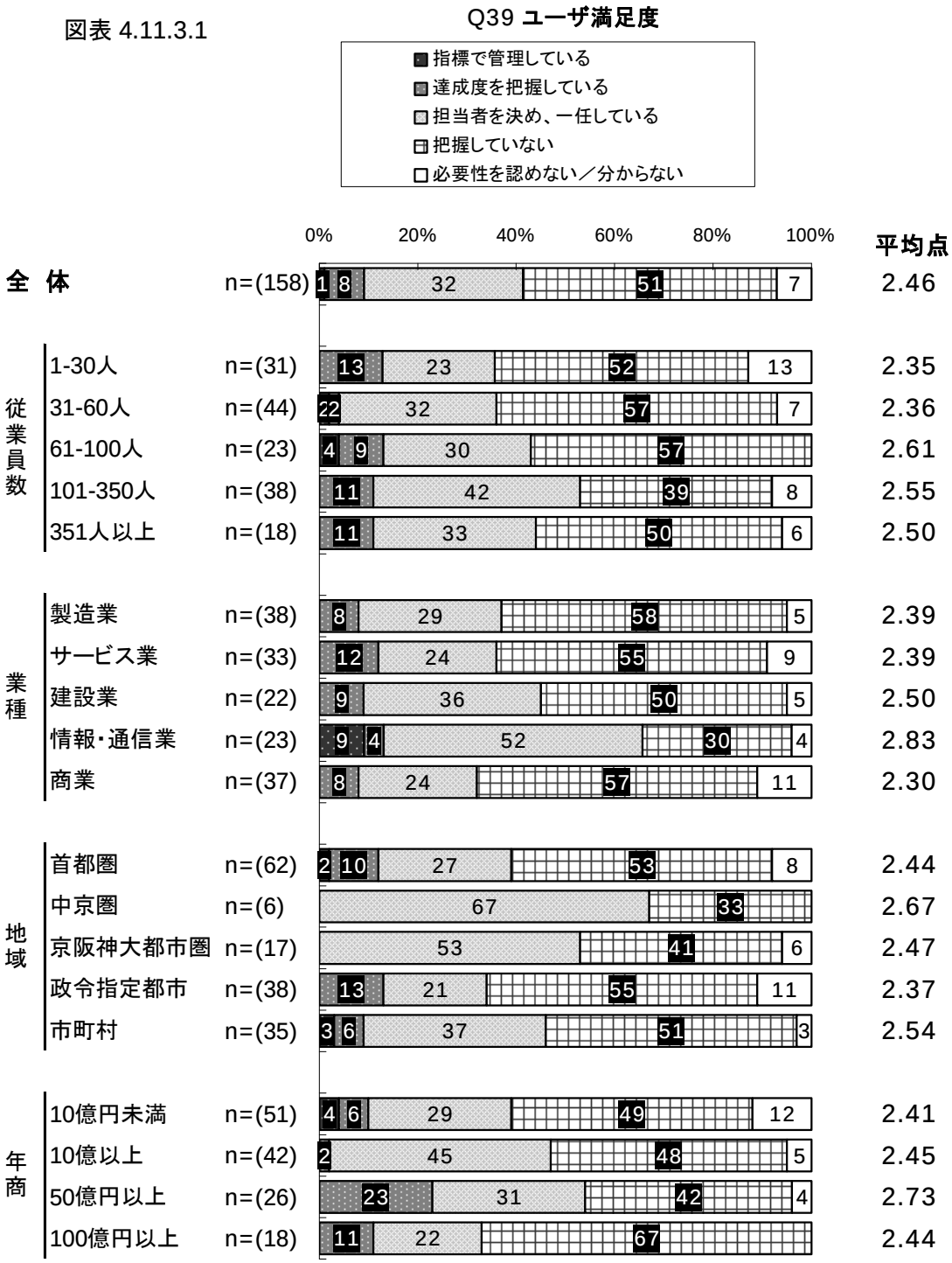
図表 4.11.2.1



4.11.3 品質 -Q39 ユーザ満足度

- 全体では 2.46 点となり、「指標で管理している」は 1%となっている。
- 従業員規模別に見ると、いずれの規模でも『指標で管理している』の割合はわずかで、「1～30 人」「101～350 人」「351 人以上」では 0%であった。
- 業種別に見ると、「情報・通信業」が他の業種と比較して高く、2.83 点であった。

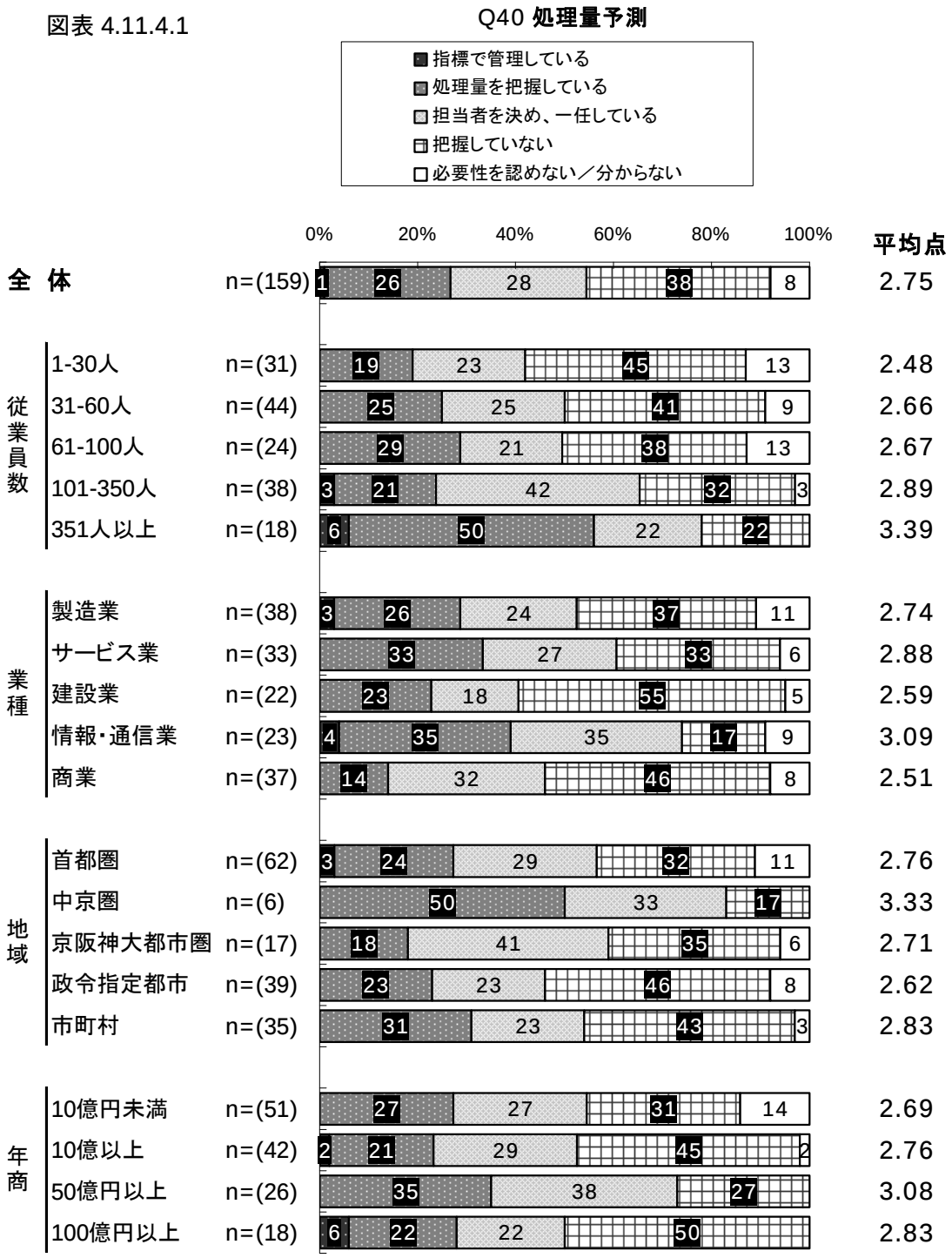
図表 4.11.3.1



4.11.4 品質 −Q40 稼働率

- 全体では 2.75 点で、『指標で管理している』は 1%となっている。
- 従業員規模別に見ると、規模が大きくなるにつれて点数が高くなっており、「351 人以上」では 3.39 点と大幅に高くなる。また、『把握していない』『必要性を認めない/分からない』というネガティブな回答の割合は規模が大きくなるにつれて少なくなる。

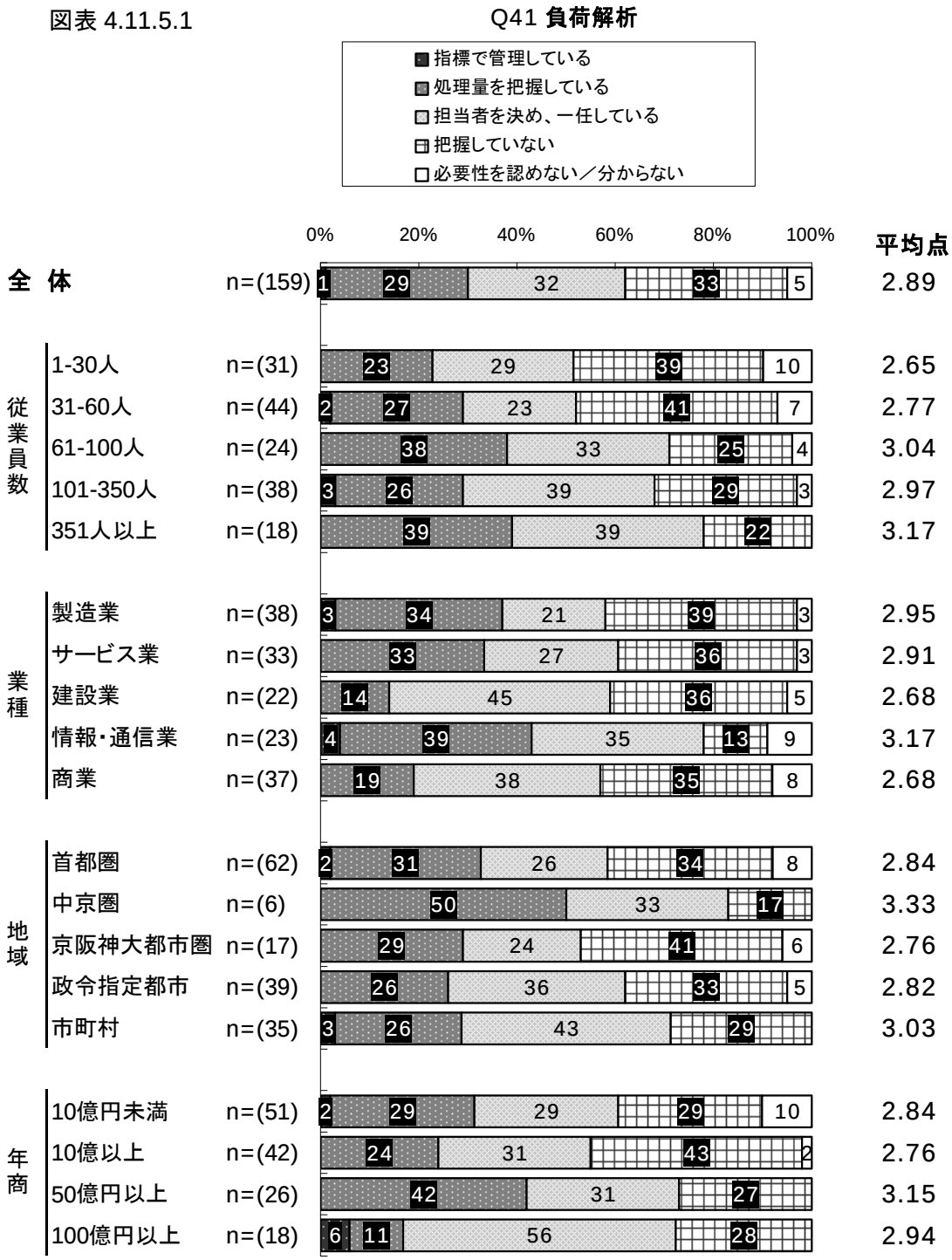
図表 4.11.4.1



4.11.5 品質 -Q41 負荷解析

- 全体では 2.89 点となり、『指標で管理している』は 1%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高くなる。
- 業種別に見ると、「情報・通信業」において最も点数が高くなり、『把握していない』『必要性を認めない/分からない』というネガティブな回答の割合が他の業種と比較して非常に少ない。

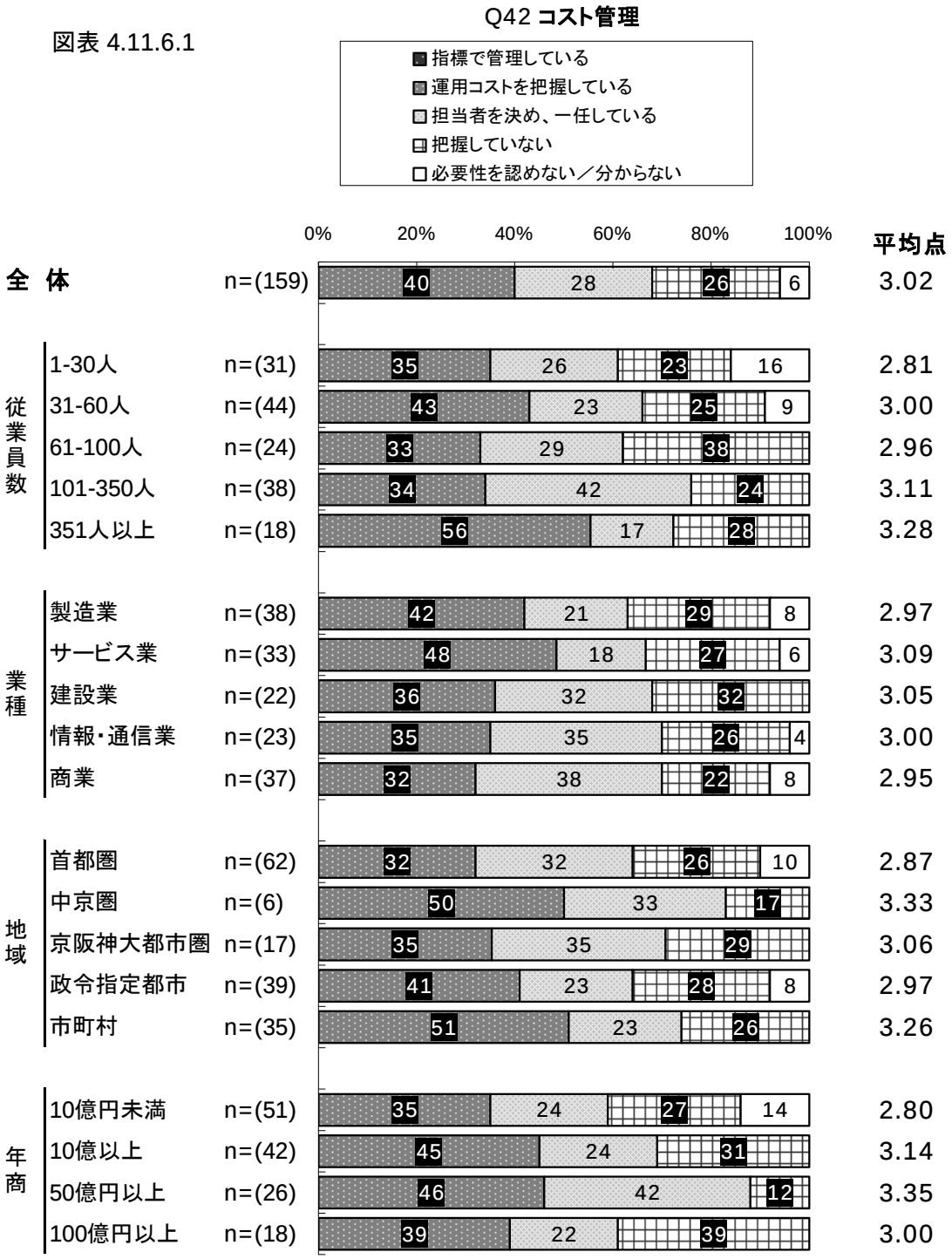
図表 4.11.5.1



4.11.6 品質 -Q42 コスト管理

- 全体では 3.02 点となり、『指標で管理している』は 0%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く、3.28 点となっている。また、他の規模と比較して『運用コストを把握している』の割合が高い。
- 業種別に見ると、いずれの業種においても点数が 3 点程度となっており、数字に大きな差は見られない。

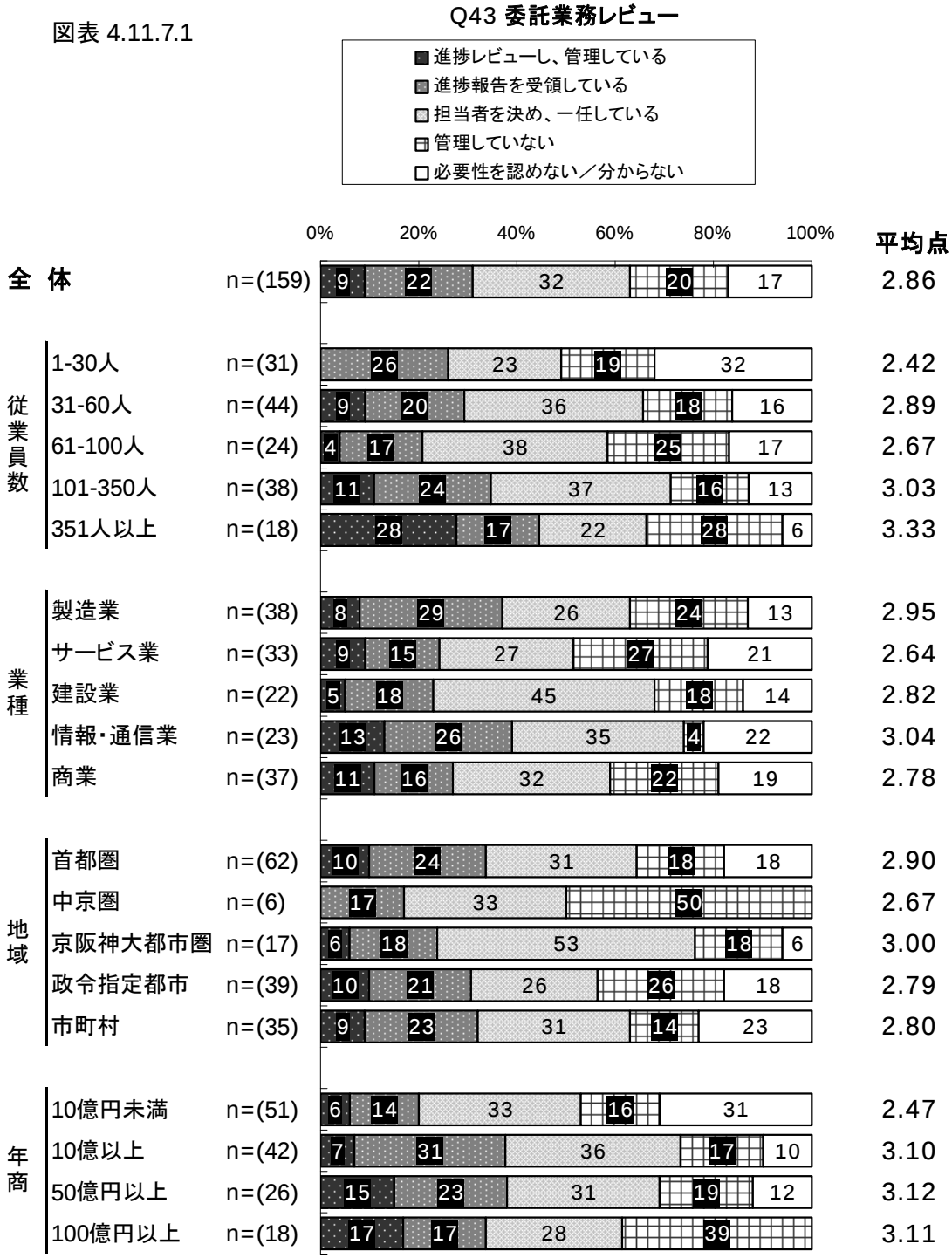
図表 4.11.6.1



4.11.7 品質 -Q43 委託業務レビュー

- 全体では 2.86 点となり、『進捗レビューし、管理している』は 9%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数がもっとも高く、他の規模と比較して「351 人以上」は『進捗レビューし、管理している』の割合が高い。
- 業種別に見ると、「製造業」と「情報・通信業」で『進捗レビューし、管理している』『進捗報告を受領している』というポジティブな回答の割合が高い。

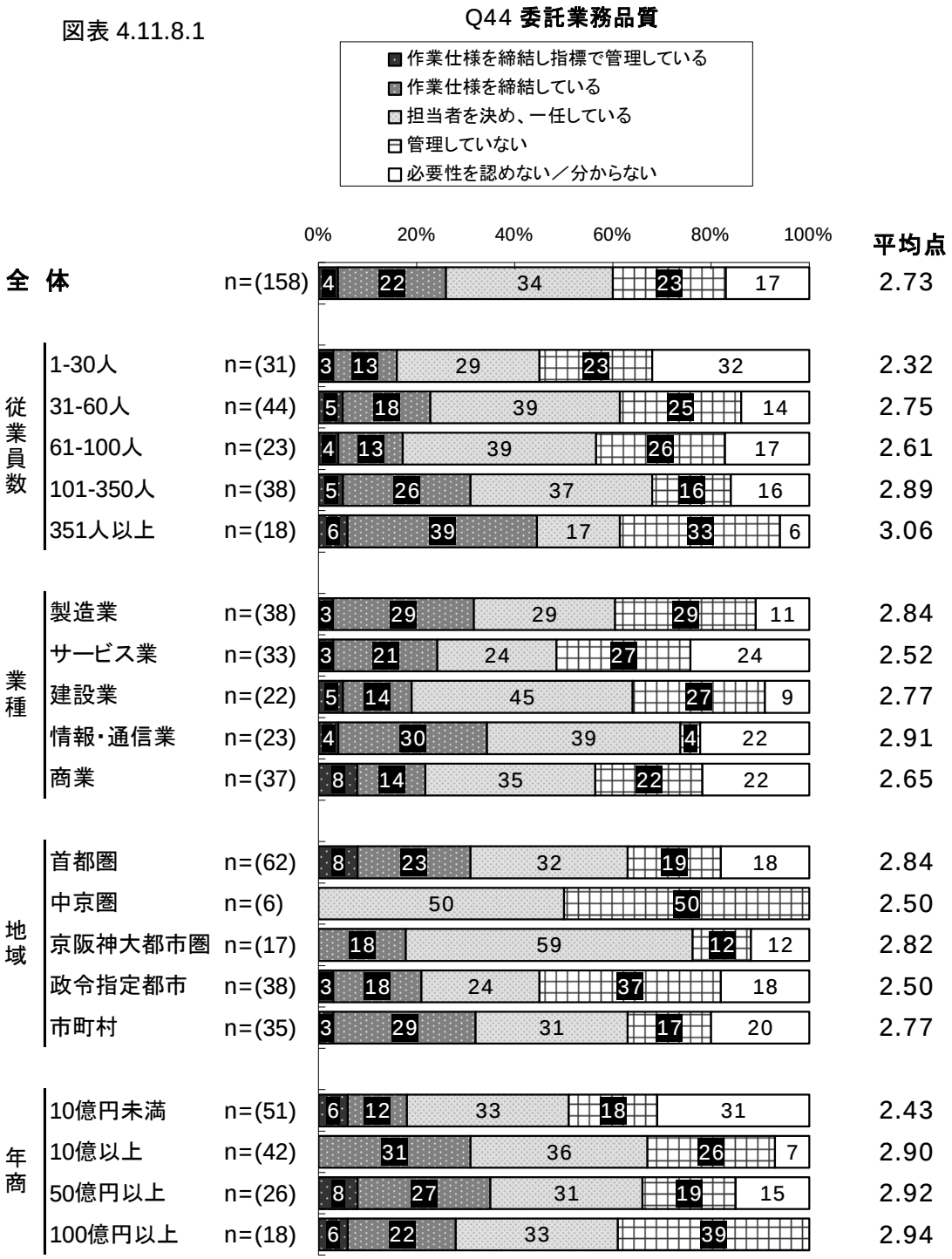
図表 4.11.7.1



4.11.8 品質 -Q44 委託業務品質

- 全体では 2.73 点となり、『作業仕様を締結し指標で管理している』は 4%となっている。
- 従業員規模別に見ると、「351 人以上」で点数が最も高く 3.06 点となっており、他の規模と比較して『作業仕様を締結し指標で管理している』『作業仕様を締結している』というポジティブな回答の割合が高い。
- 業種別に見ると、「情報・通信業」の得点が最も高く 2.91 点となっている。

図表 4.11.8.1

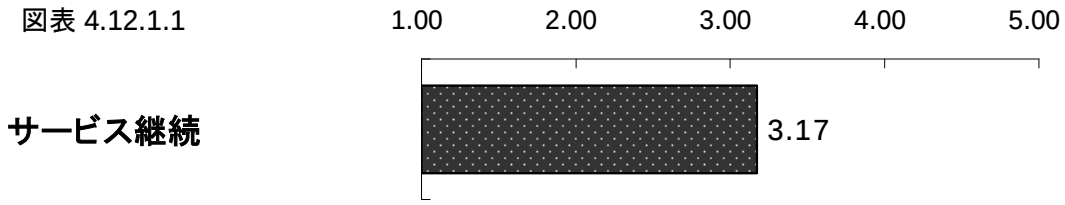


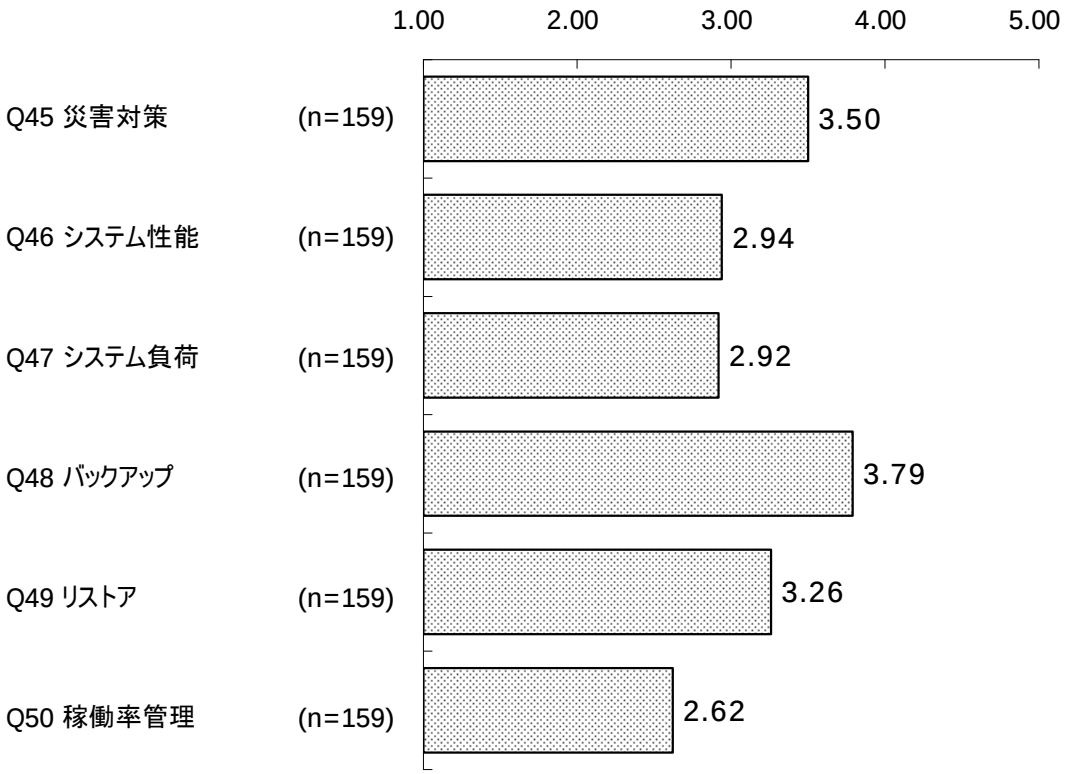
4.12 サービス継続

4.12.1 サービス継続

・ サービス継続については、全体で 3.17 点となり、サービス継続に含まれる項目の得点を見ると、『バックアップ』が最も高く 3.79 点となっている。
・ 逆に最も低くなっているのが『稼働率管理』で 3.62 点である。

図表 4.12.1.1

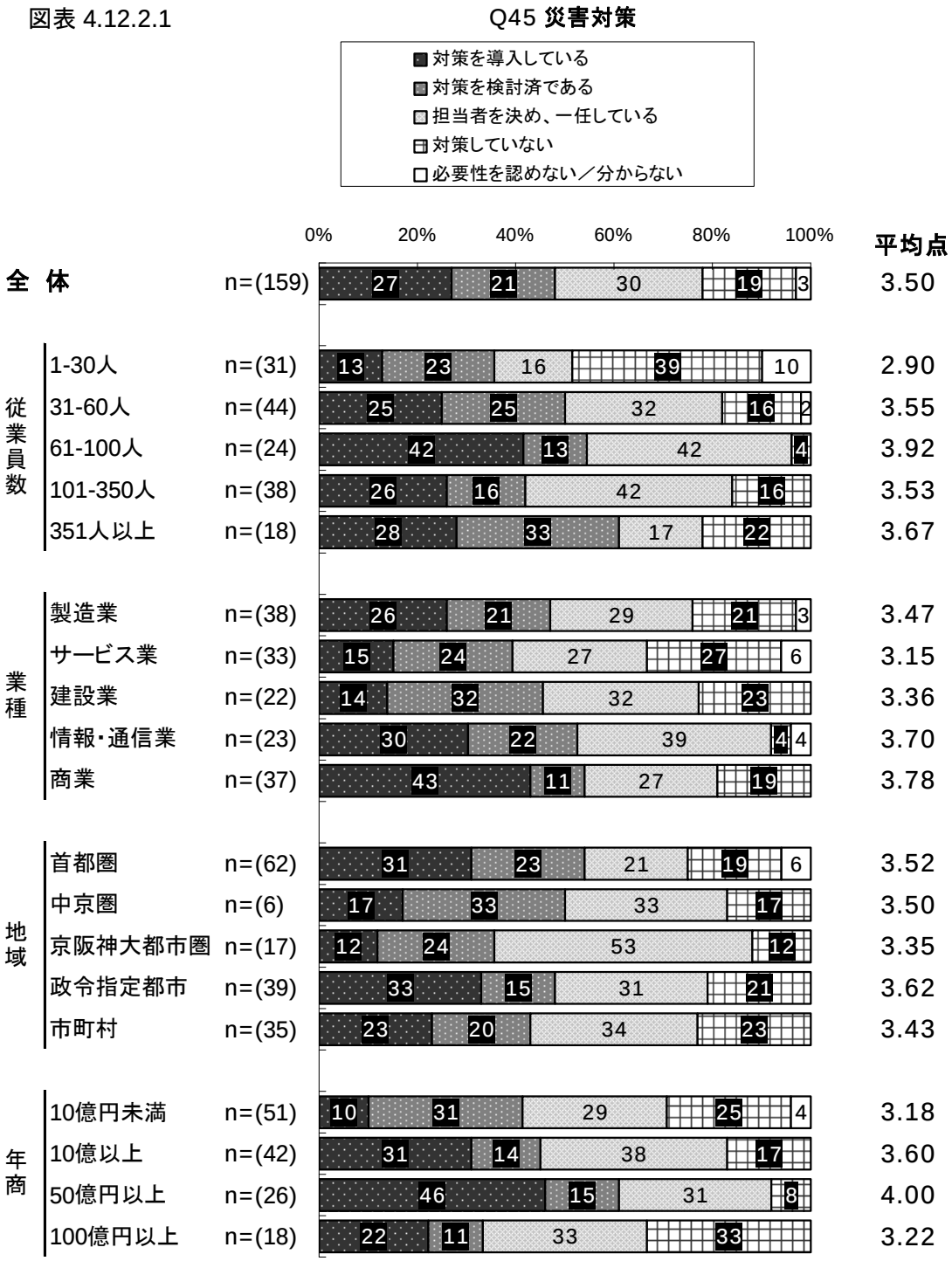




4.12.2 サービス継続 –Q45 災害対策

- 全体では 3.50 点となり、『対策を導入している』は 27%となっている。
- 従業員規模別に見ると、「61～100 人」において最も点数が高く 3.92 点となっており、他の規模と比較して『対策を導入している』の割合が高い。
- 業種別に見ると、「商業」において最も点数が高く 3.78 点となっており、他の業種と比較して『対策を導入している』の割合が高い。

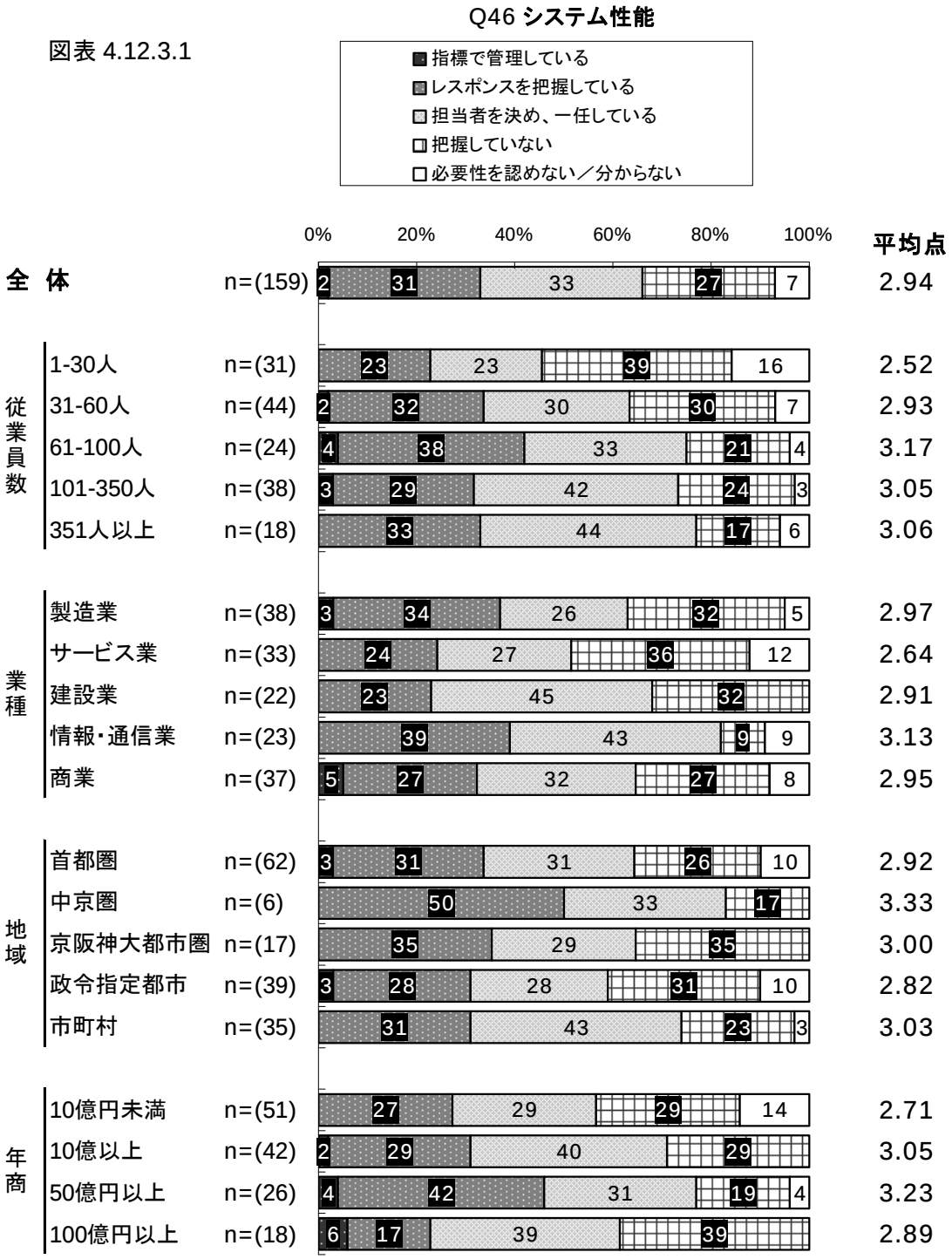
図表 4.12.2.1



4.12.3 サービス継続 –Q46 システム性能

- 全体では 2.94 点となり、『指標で管理している』は 2%となっている。
- 従業員規模別に見ると、「61～100 人」で最も点数が高く 3.17 点となっており、他の規模と比較して『指標で管理している』『レスポンスを把握している』というポジティブな回答の割合もやや高い。
- 業種別に見ると、「情報・通信業」の点数が最も高く 3.13 点となっている。

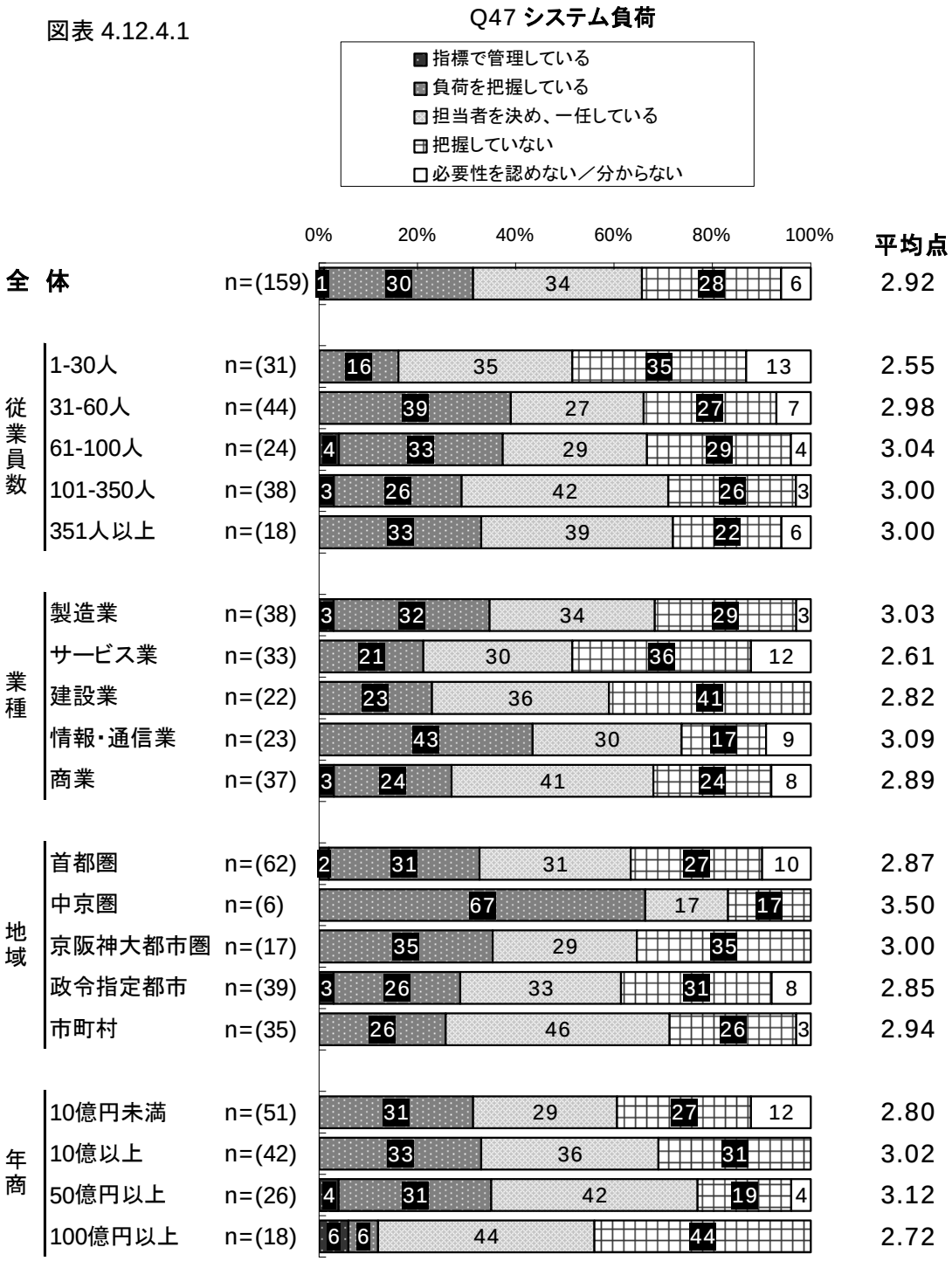
図表 4.12.3.1



4.12.4 サービス継続 –Q47 システム負荷

- 全体では 2.92 点となり、『指標で管理している』は 1%となっている。
- 従業員規模別に見ると、「61～100 人」で最も点数が高く 3.04 点となっている。また、『把握していない』『必要性を認めない/分からない』というネガティブな回答は規模が大きくなるにつれて減少している。
- 業種別に見ると、「情報・通信業」の点数が最も高く 3.09 点となっている。

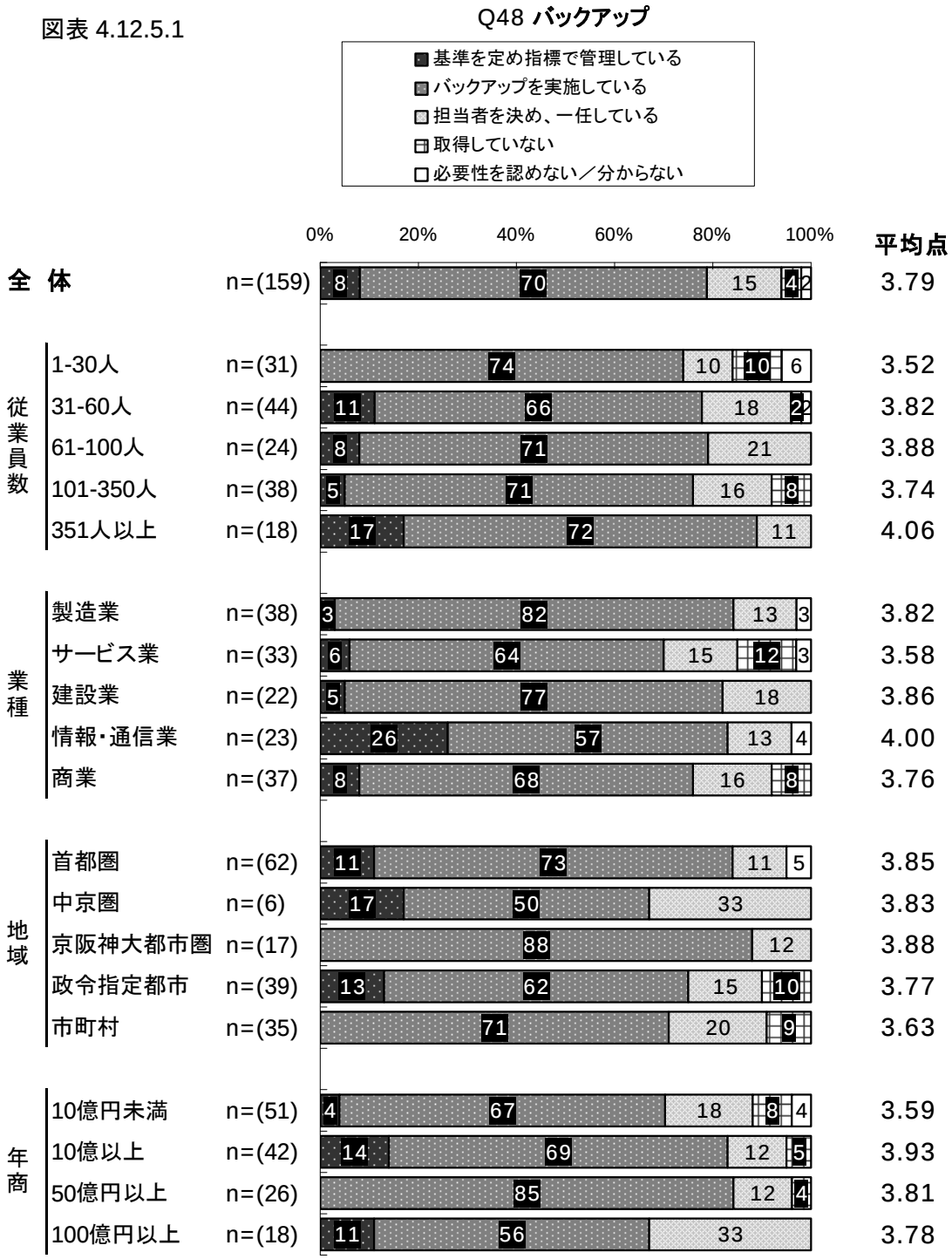
図表 4.12.4.1



4.12.5 サービス継続 –Q48 バックアップ

- 全体では 3.79 点となり、『基準を定め指標で管理している』は 8%となっている。。
- 従業員規模別に見ると、「351 人以上」の得点が最も高く 4.06 点となっている。また、いずれの規模においても『バックアップを実施している』の割合が高く 7 割程度を占めている。
- 業種別に見ると、「情報・通信業」で最も得点が高く、他の業種と比較して『基準を定め指標で管理している』の割合が高い。

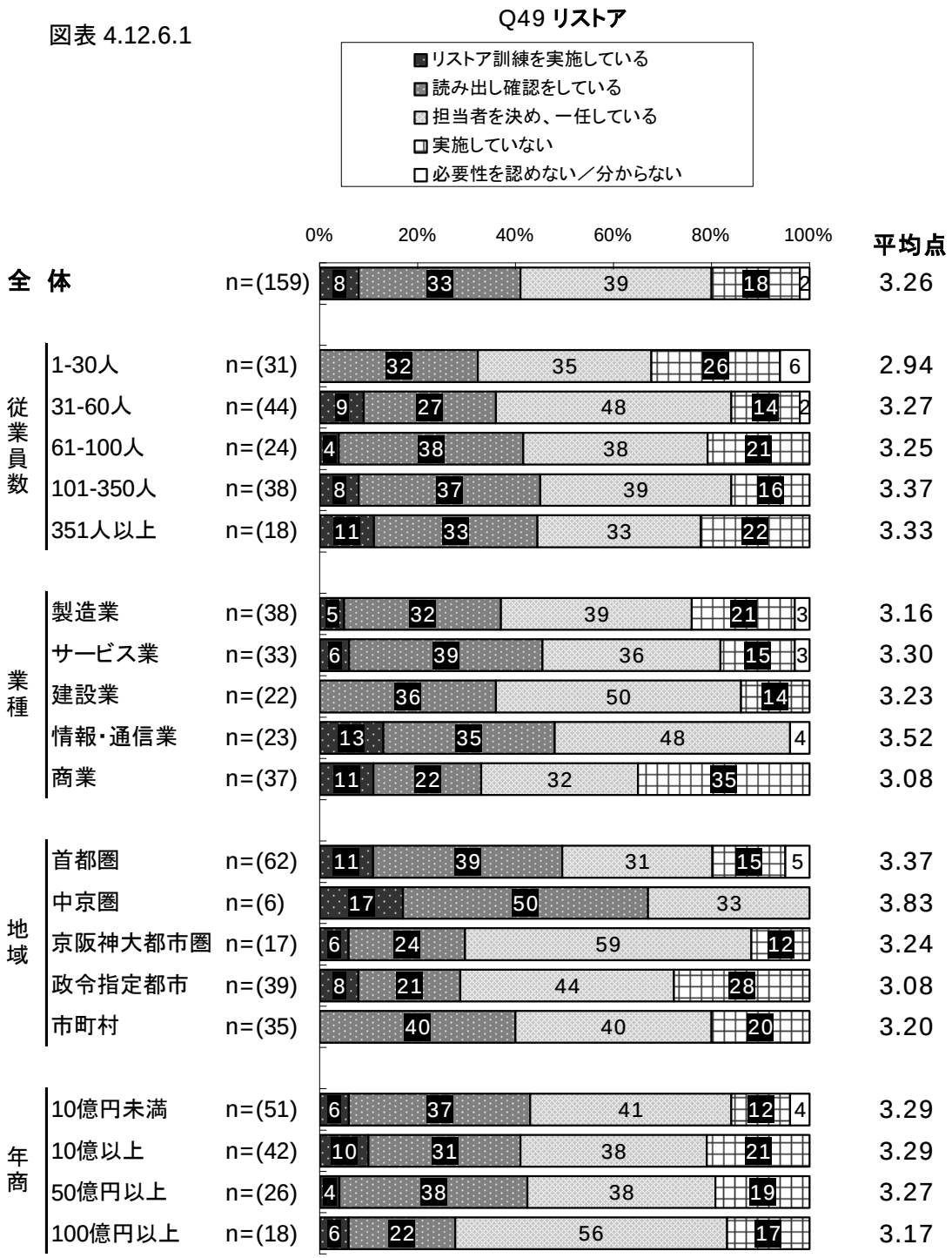
図表 4.12.5.1



4.12.6 サービス継続 −Q49 リストア

- 全体では 3.26 点となり、『リストア訓練を実施している』は 8%となっている。
- 従業員規模別に見ると、31 人以上の規模では点数が 3.3 点程度と値に大きな差は見られない。
- 業種別に見ると、「情報・通信業」で最も点数が高く 3.52 点となっている。他の業種と比較して「商業」において『実施していない』と回答する割合が高い。

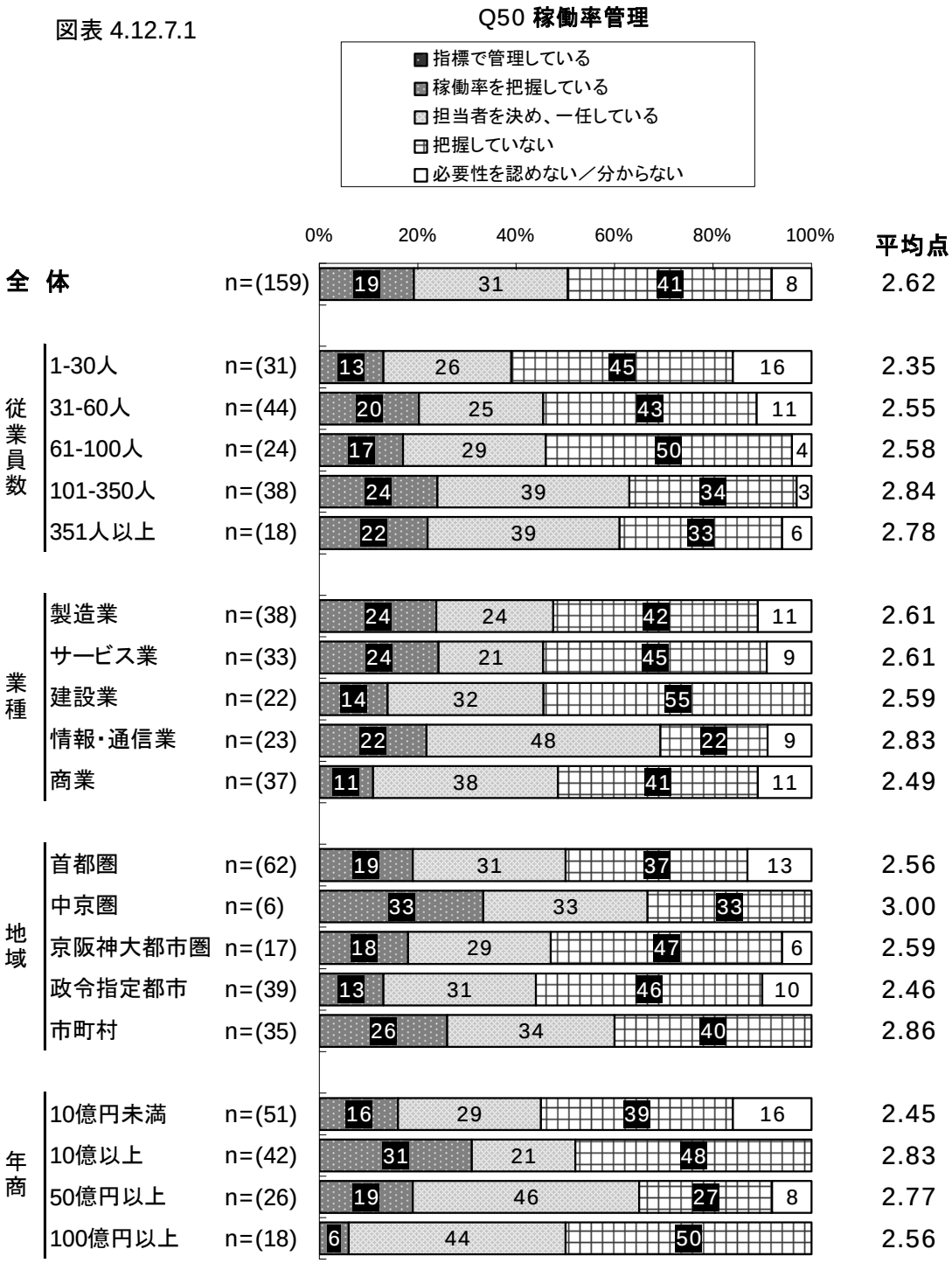
図表 4.12.6.1



4.12.7 サービス継続 –Q50 稼働率管理

- 全体では 2.62 点となり、『指標で管理している』は 0%となっている。
- 従業員規模別に見ると、規模が大きくなるにつれて『把握していない』『必要性を認めない/分からない』というネガティブな回答が減少するが、全体の割合と比較して大きな差は見られない。
- 業種別に見ると、「情報・通信業」で最も点数が高く 2.83 点となっており、『把握していない』『必要性を認めない/分からない』というネガティブな回答の割合が最も少ない。

図表 4.12.7.1

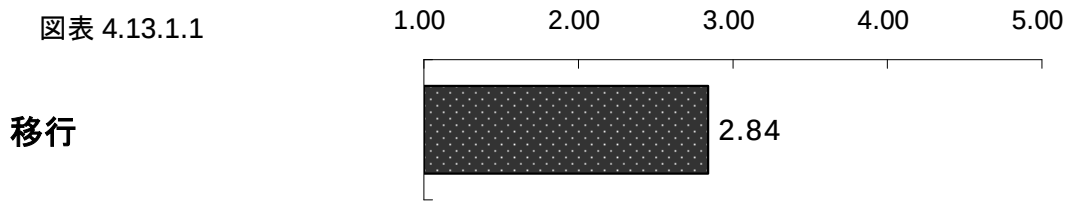


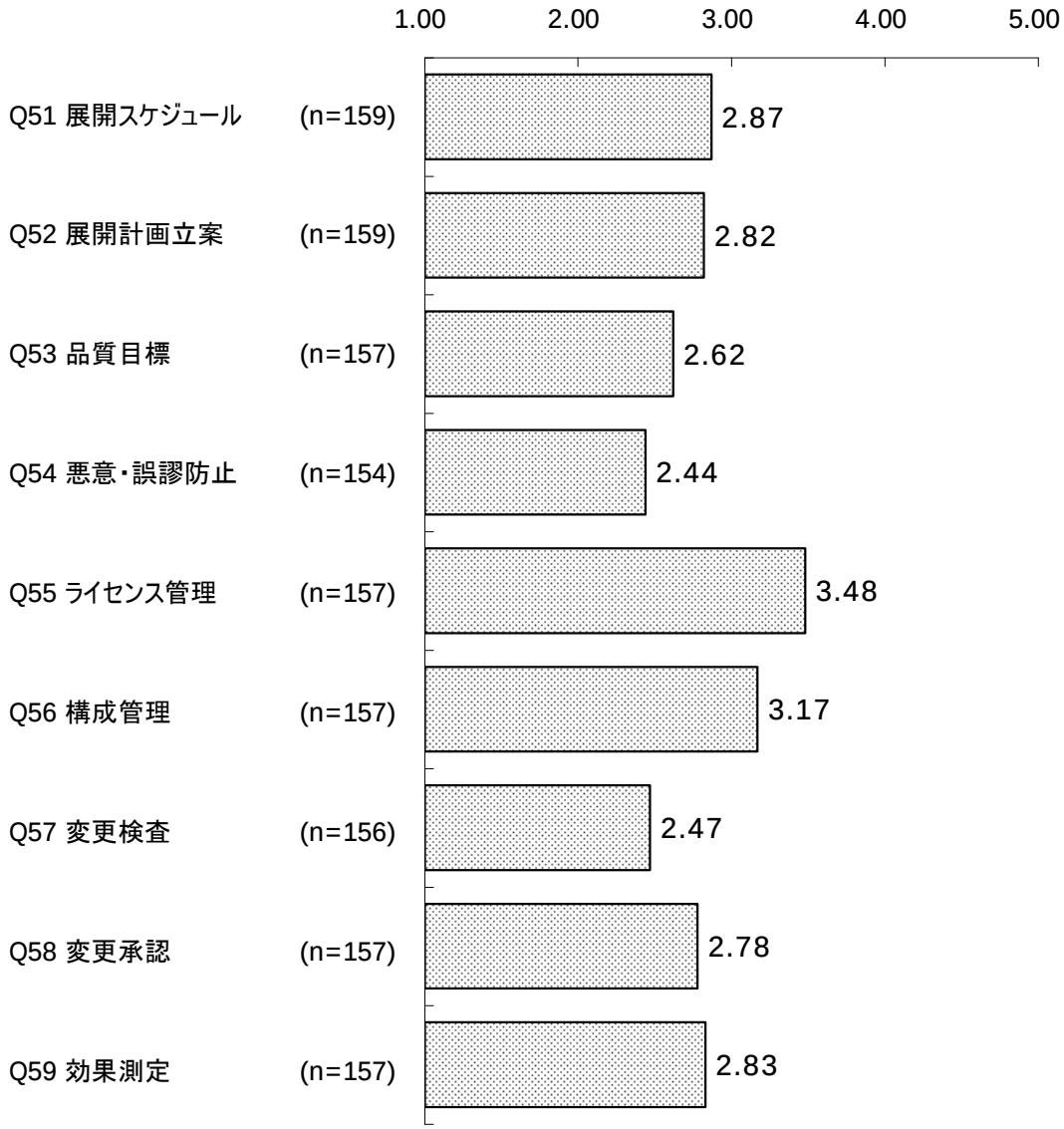
4.13 移行

4.13.1 移行

- 移行については、全体で 2.84 点となり、移行に含まれる項目の得点を見ると、『ライセンス管理』が最も高く 3.48 点となっている。
- 逆に最も低くなっているのが『悪意・誤謬防止』で 2.44 点である。

図表 4.13.1.1

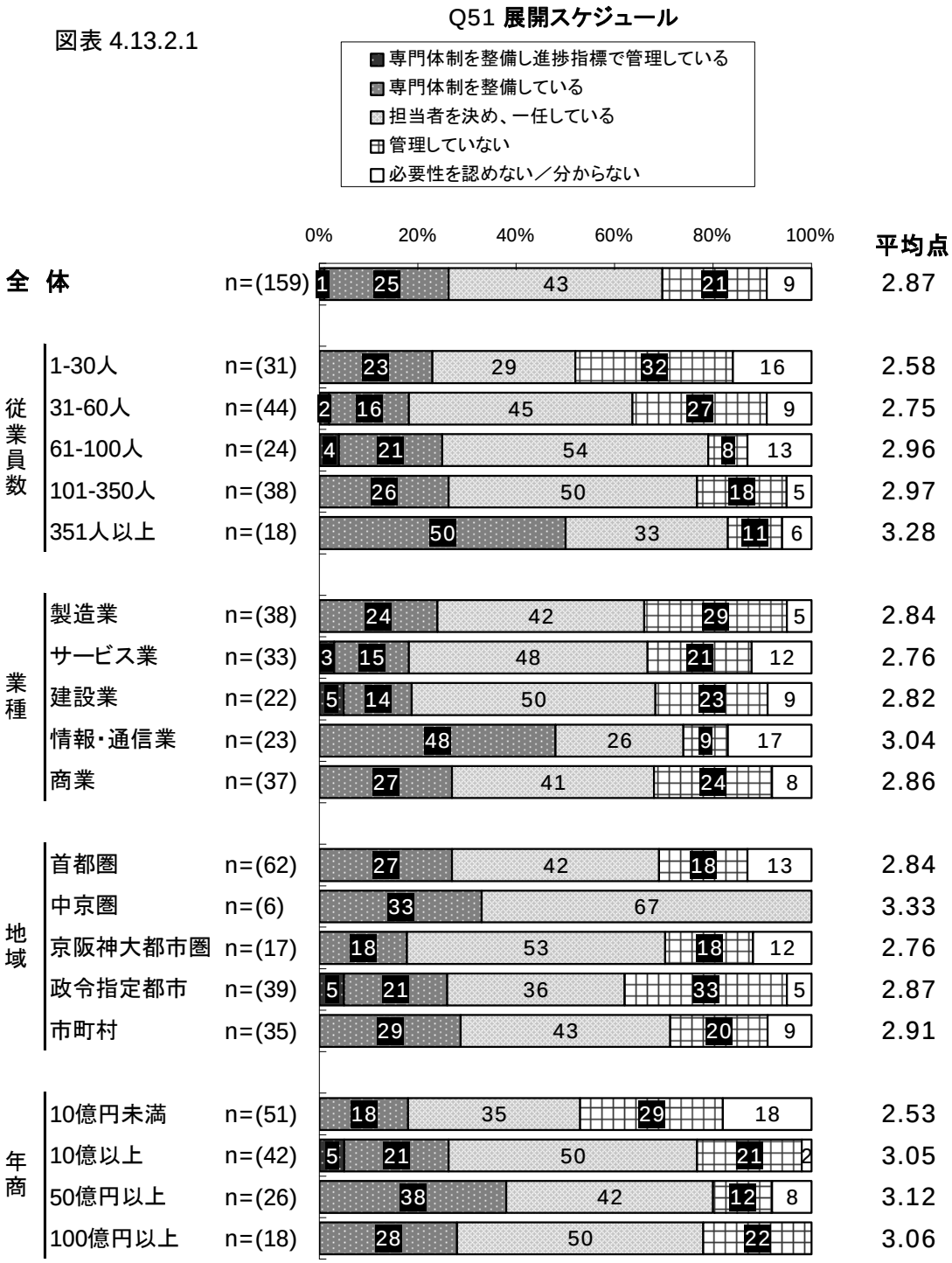




4.13.2 移行 -Q51 展開スケジュール

- 全体では 2.87 点となり、『専門体制を整備し進捗指標で管理している』は 1%となっている。。
- 従業員規模別に見ると、規模が大きくなるにつれて点数が高くなり、「351 人以上」で最も点数が高く 3.28 点となっている。
- 業種別に見ると、「情報・通信業」で点数が最も高く 3.04 点となっているが、同業種においては他の業種と比較して『必要性を認めない/分からない』の割合が最も高い。

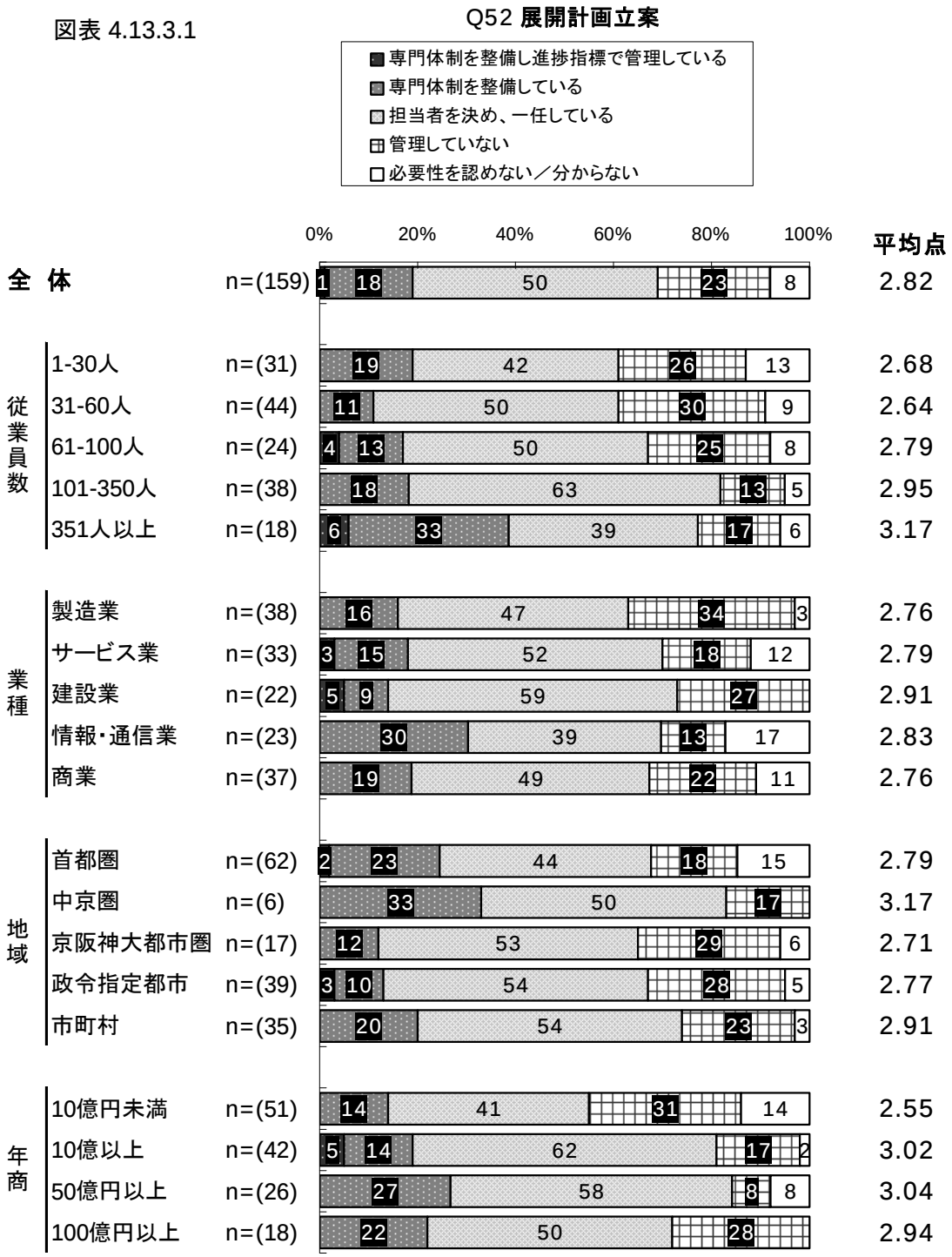
図表 4.13.2.1



4.13.3 移行 -Q52 展開計画立案

- 全体では 2.82 点となり、『専門体制を整備し進捗指標で管理している』は 1%となっている。
- 従業員規模別に見ると、規模が大きくなるにつれて点数が高くなり、「351 人以上」で最も点数が高く 3.17 点となっている。また、「351 人以上」において『専門体制を整備し進捗指標で管理している』『専門体制を整備している』というポジティブな回答の割合が最も高い。
- 業種別に見ると、「建設業」でも最も点数が高く 2.91 点となっているが、業種間で値を比較すると大きな差は見られない。

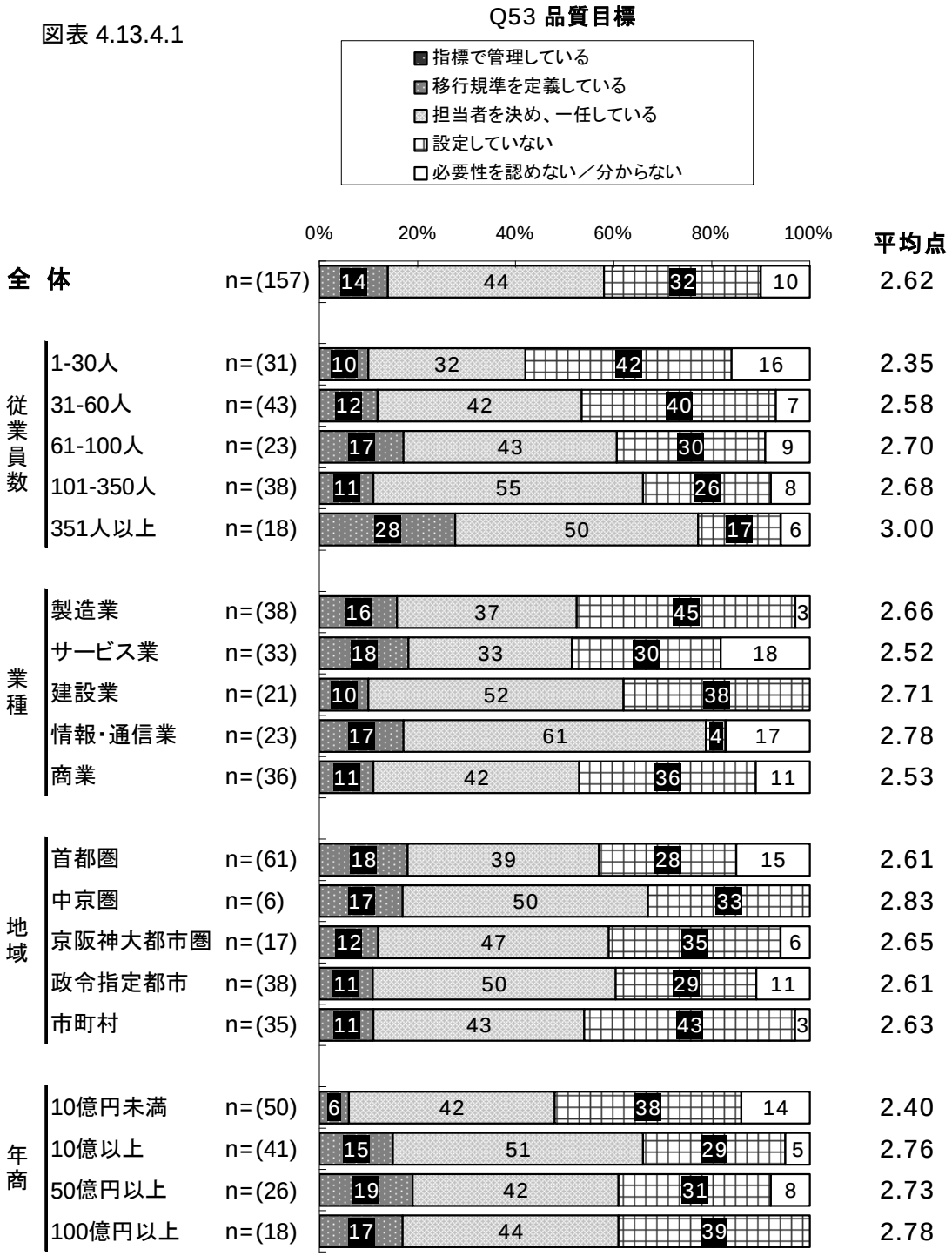
図表 4.13.3.1



4.13.4 移行 -Q53 品質目標

- 全体では 2.62 点となり、『指標で管理している』は 0%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 3.00 点となっている。また、『設定していない』『必要性を認めない/分からない』というネガティブな回答の割合は規模が大きくなるにつれて低くなっている。
- 業種別に見ると、「情報・通信業」で最も点数が高く 2.78 点であるが、業種間で値を比較すると大きな差は見られない。

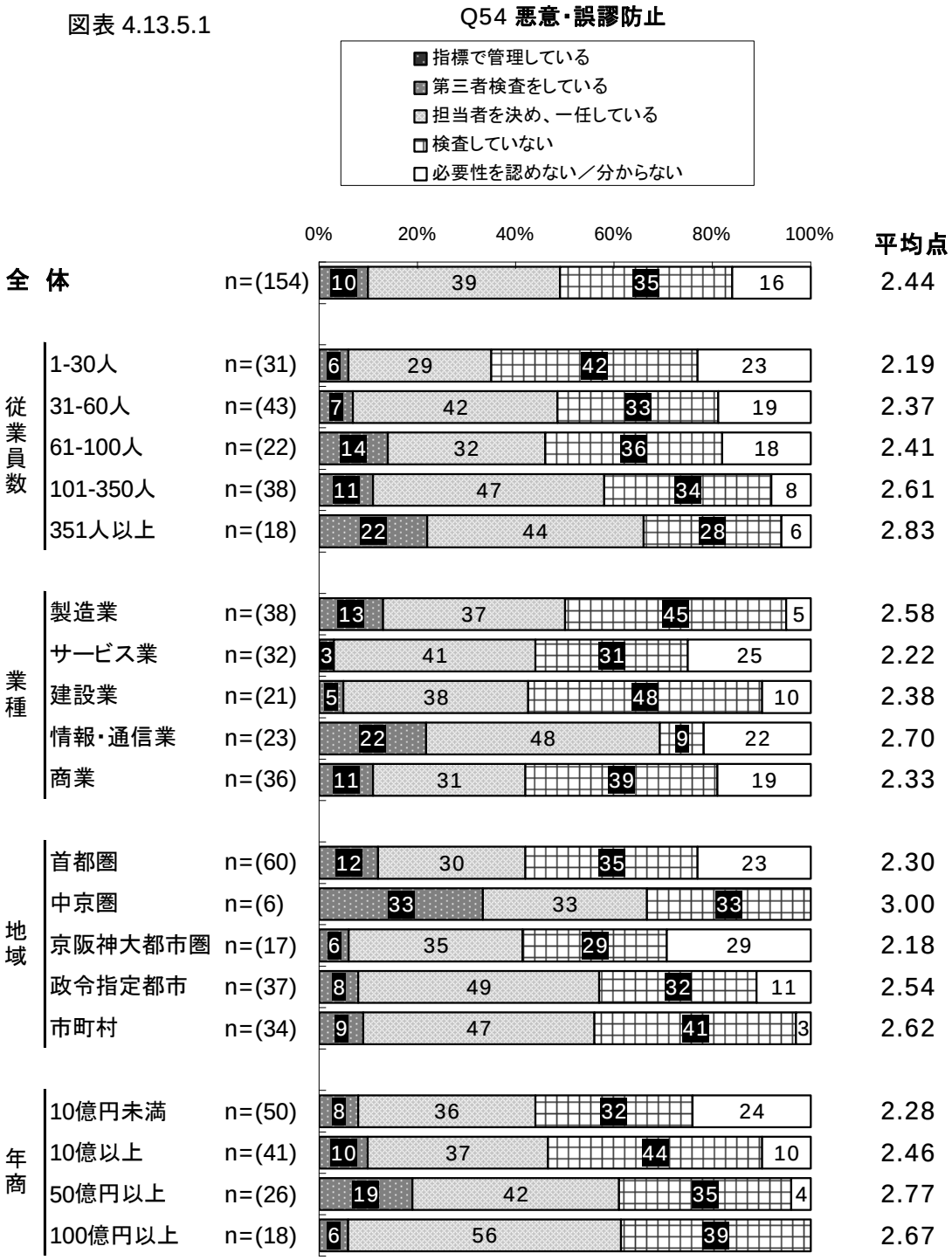
図表 4.13.4.1



4.13.5 移行 –Q54 悪意・誤謬防止

- 全体では 2.44 点となり、『指標で管理している』は 0%となっている。。
- 従業員規模別に見ると、規模が大きくなるにつれて点数が高くなり、「351 人以上」で点数が最も高く 2.83 点となっている。
- 業種別に見ると、「情報・通信業」で最も点数が高く 2.70 点となっている。

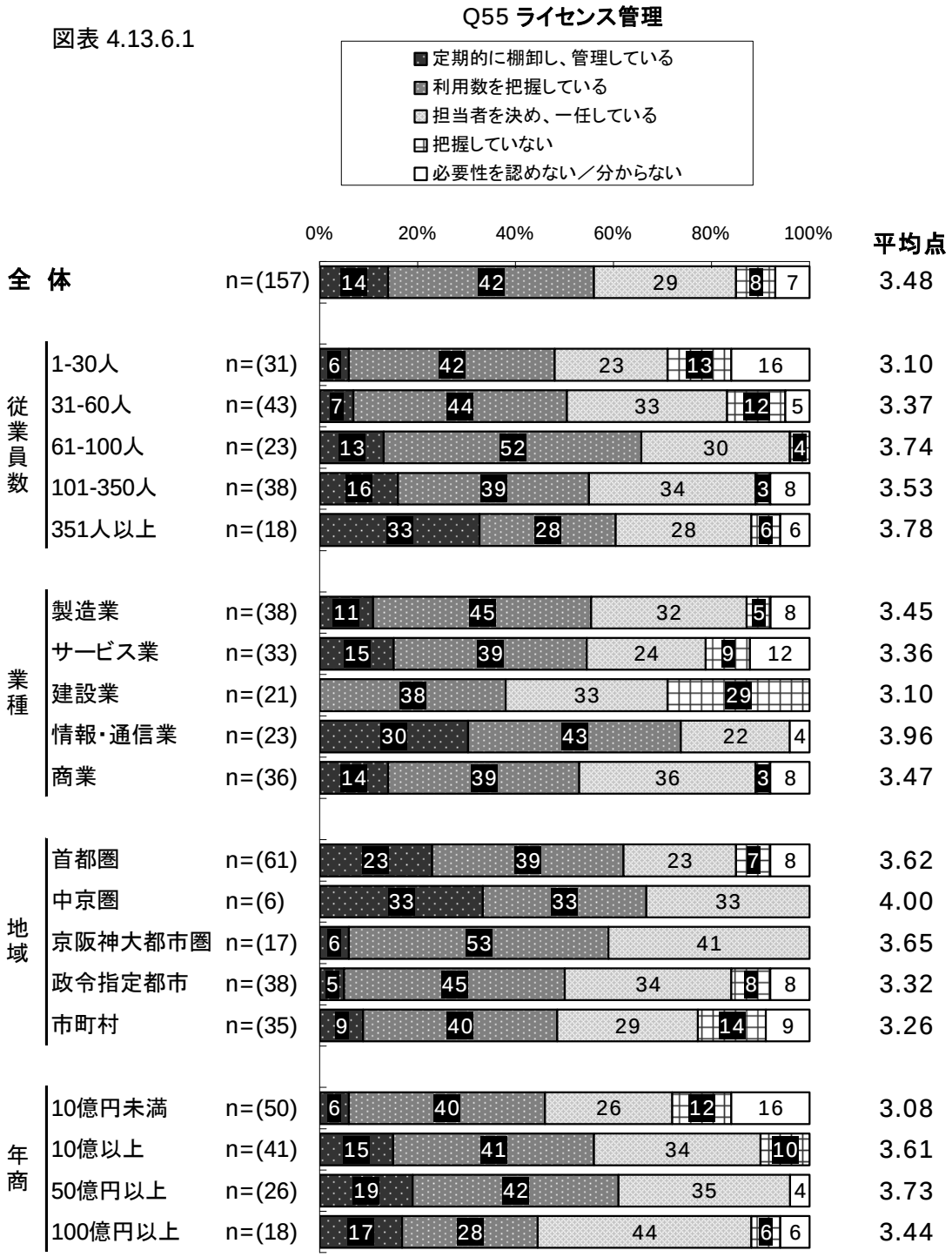
図表 4.13.5.1



4.13.6 移行 –Q55 ライセンス管理

- 全体では 3.48 点となり、『定期的に棚卸し、管理している』は 14%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 3.78 点となっている。また、『定期的に棚卸し、管理している』の割合は規模が大きくなるにつれて高くなる。
- 業種別に見ると、「情報・通信業」で最も点数が高く 3.96 点となり、他の業種と比較して点数が高い。

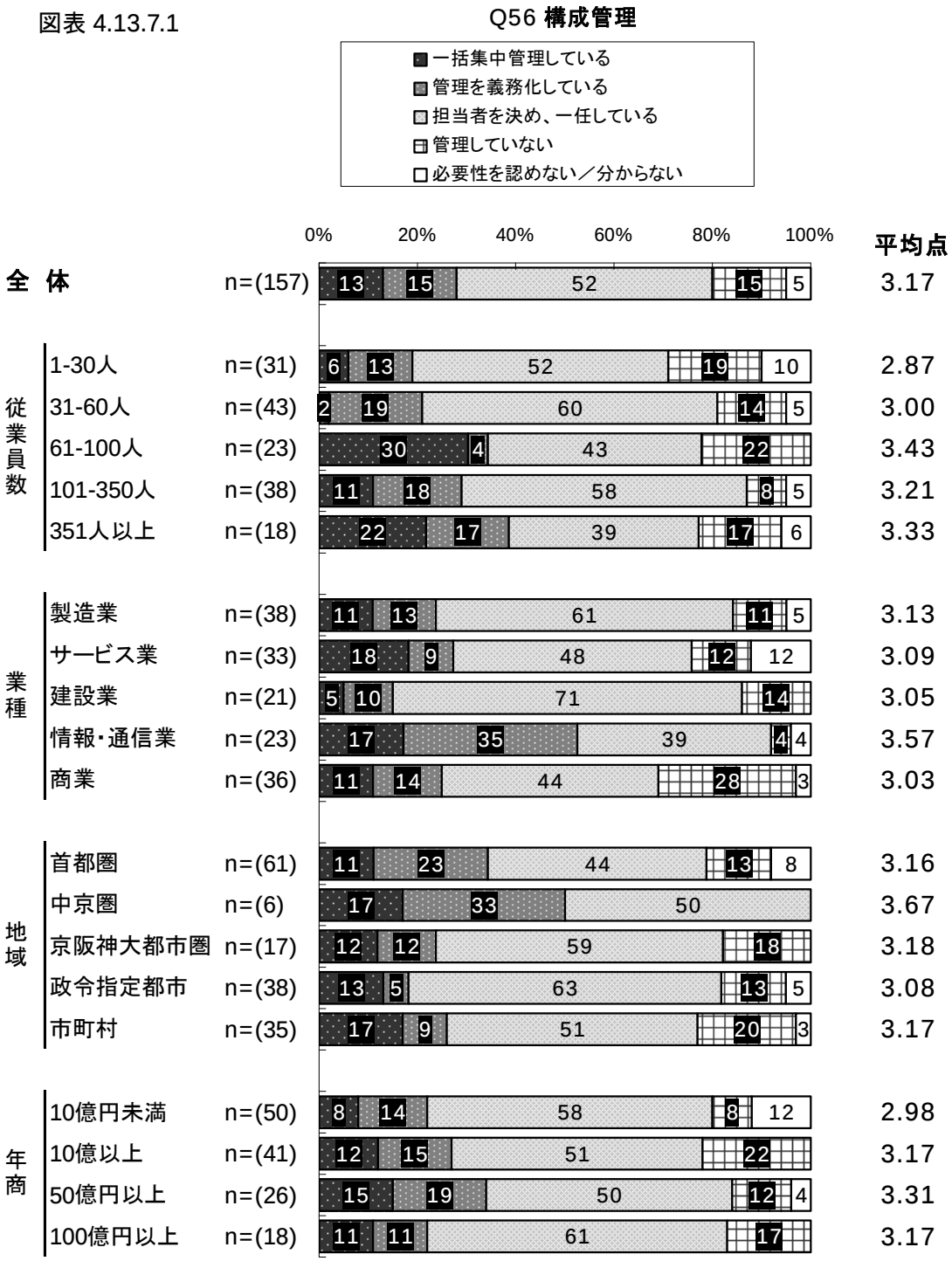
図表 4.13.6.1



4.13.7 移行 -Q56 構成管理

- 全体では 3.17 点となり、『一括集中管理している』は 13%となっている。
- 従業員規模別に見ると、「61～100 人」で最も点数が高く 3.43 点となっており、他の規模と比較して『一括集中管理している』の割合が高い。
- 業種別に見ると、「情報・通信業」で最も点数が高く 3.57 点となっており、他の業種と比較して『一括集中管理している』『管理を義務化している』というポジティブな回答の割合が高い。

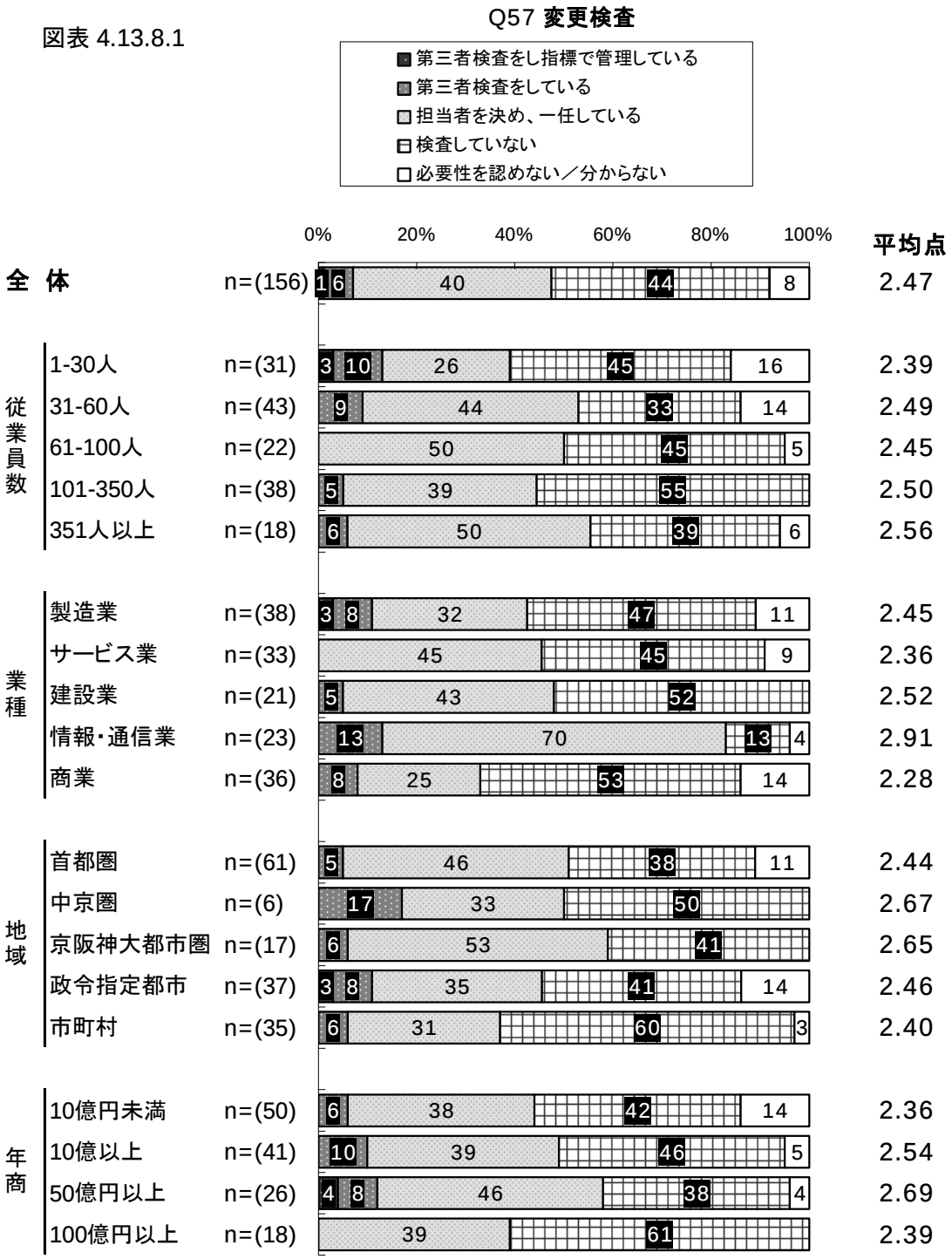
図表 4.13.7.1



4.13.8 移行 –Q57 変更検査

- 全体では 2.47 点となり、『第三者検査をし指標で管理している』は 1%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 2.56 点となっているが、規模間の値に大きな差は見られない。
- 業種別に見ると、「情報・通信業」で最も点数が高く 2.91 点となっている。また、他の業種と比較して『第三者検査をし指標で管理している』『第三者検査をしている』というポジティブな回答の割合が非常に高い。

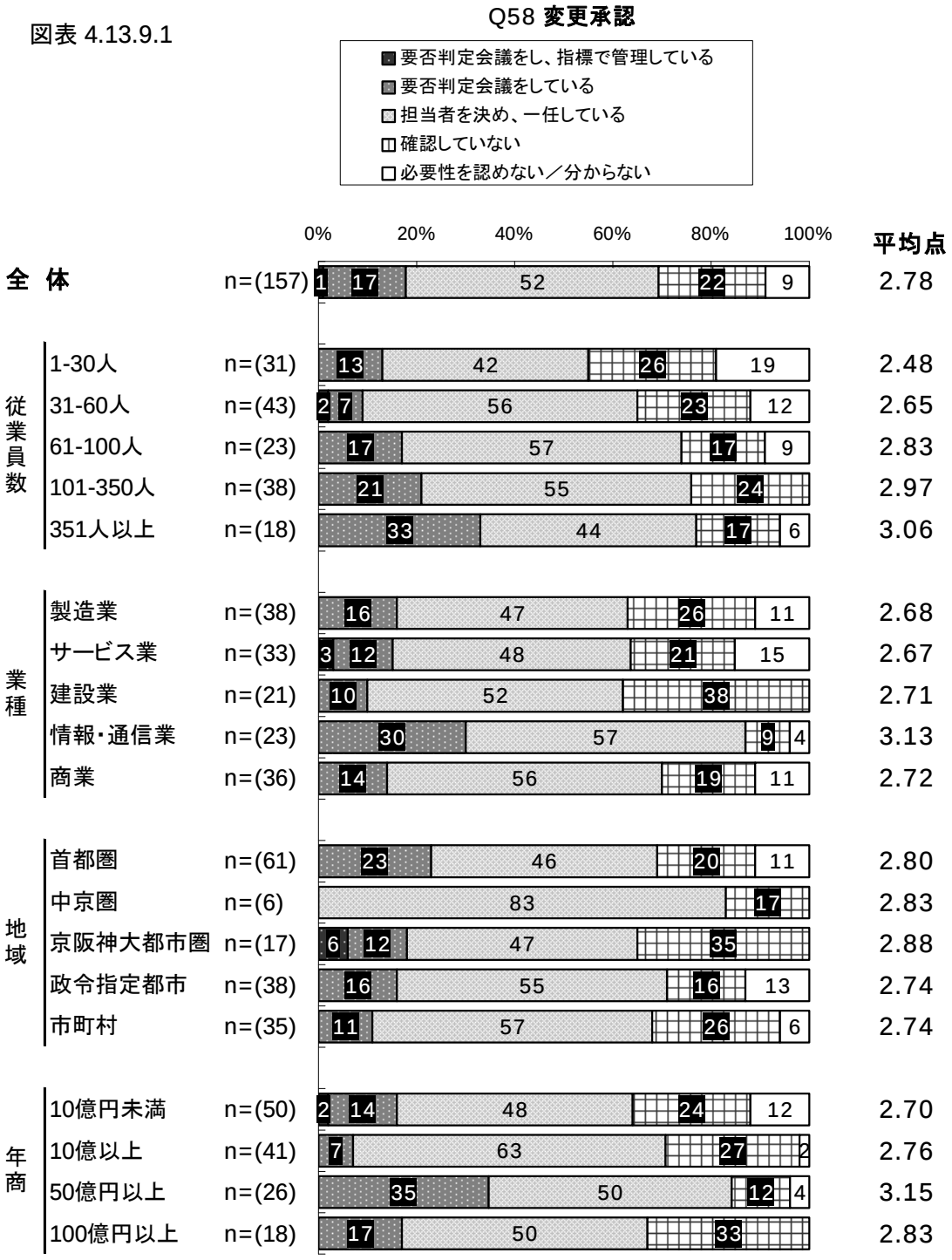
図表 4.13.8.1



4.13.9 移行 –Q58 変更承認

- 全体では 2.78 点となり、『要否判定会議をし、指標で管理している』は 1%となっている。
- 従業員規模別に見ると、規模が大きくなるにつれて点数が高くなり、「351 人以上」で最も点数が高く 3.06 点となっている。また、『確認していない』『必要性を認めない/分からない』というネガティブな回答の割合は規模が大きくなるにつれて低くなる傾向にある。
- 業種別に見ると、「情報・通信業」で最も点数が高く 3.13 点となっている。また、他の業種の点数はいずれも 2.7 点程度と値に大きな差は見られない。

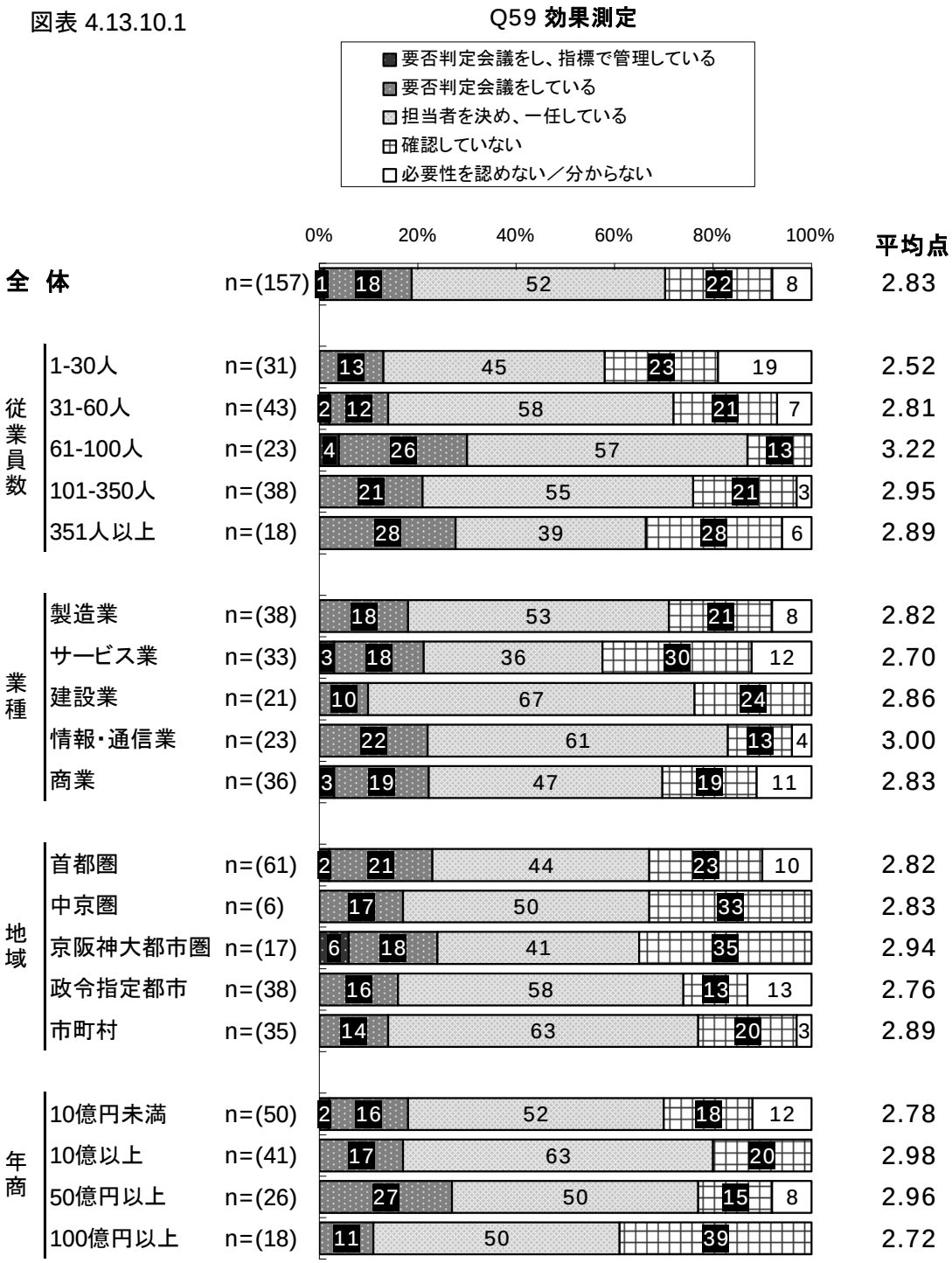
図表 4.13.9.1



4.13.10 移行 –Q59 効果測定

- 全体では 2.83 点となり、『要否判定会議をし、指標で管理している』は 1%となっている。
- 従業員規模別に見ると、「61～100 人」で最も点数が高く 3.22 点となっている。『確認していない』『必要性を認めない/分からない』というネガティブな回答の割合は「61～100 人」で最も低く、1～60 人の間では規模が大きくなるにつれ割合が低くなり、101 人以上では規模が大きくなるにつれ割合が高くなっている。
- 業種別に見ると、「情報・通信業」で最も点数が高く 3.00 点となっている。

図表 4.13.10.1

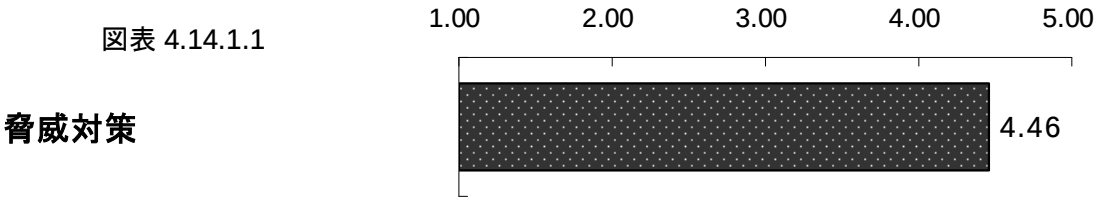


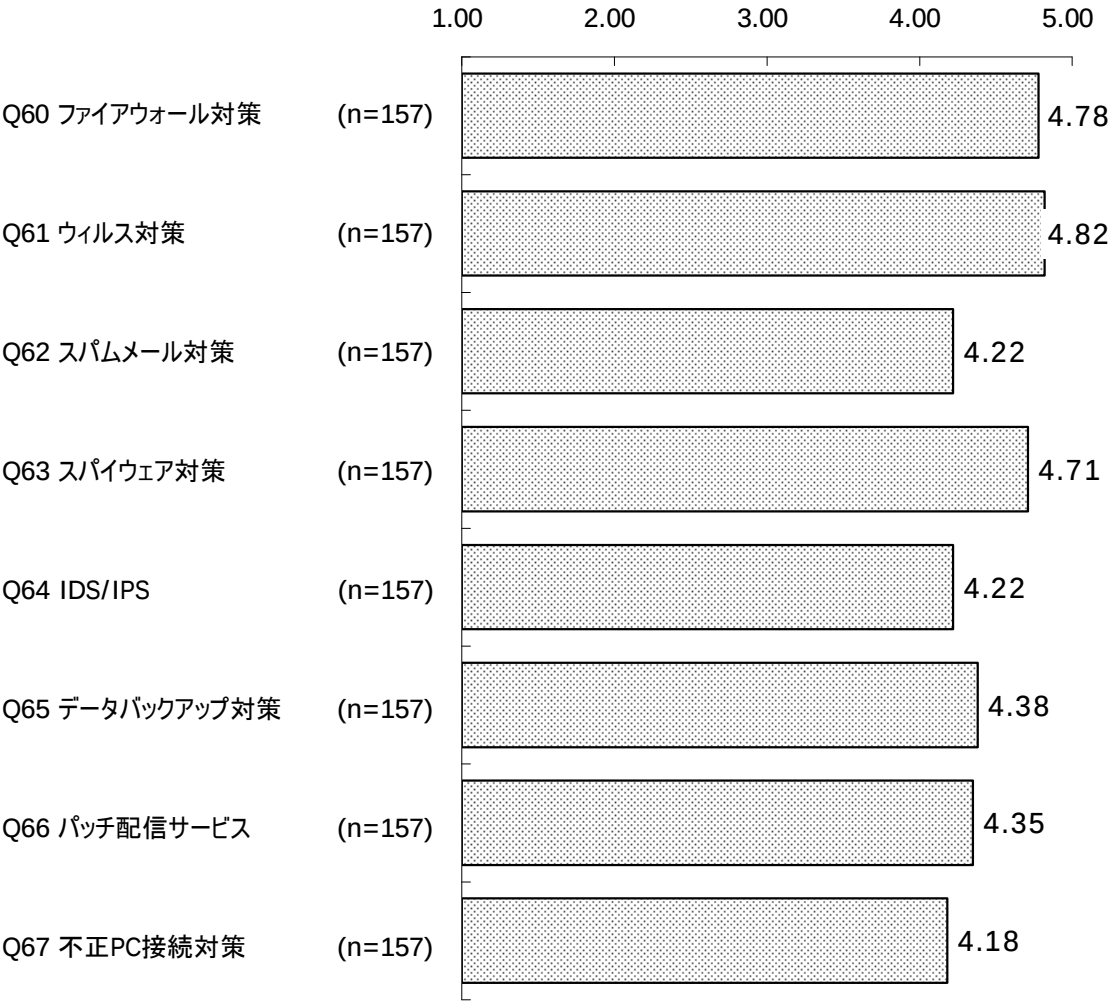
4.14 脅威対策

4.14.1 脅威対策

- 脅威対策については全体で 4.46 点となり、脅威対策に含まれる項目の得点を見ると、『ウィルス対策』が最も高く 4.82 点となっており、次いで『ファイアウォール対策』が 4.78 点、『スパイウェア対策』が 4.71 点と僅差で続く。
- 逆に最も低くなっているのが『不正 PC 接続対策』で 4.18 点である。

図表 4.14.1.1

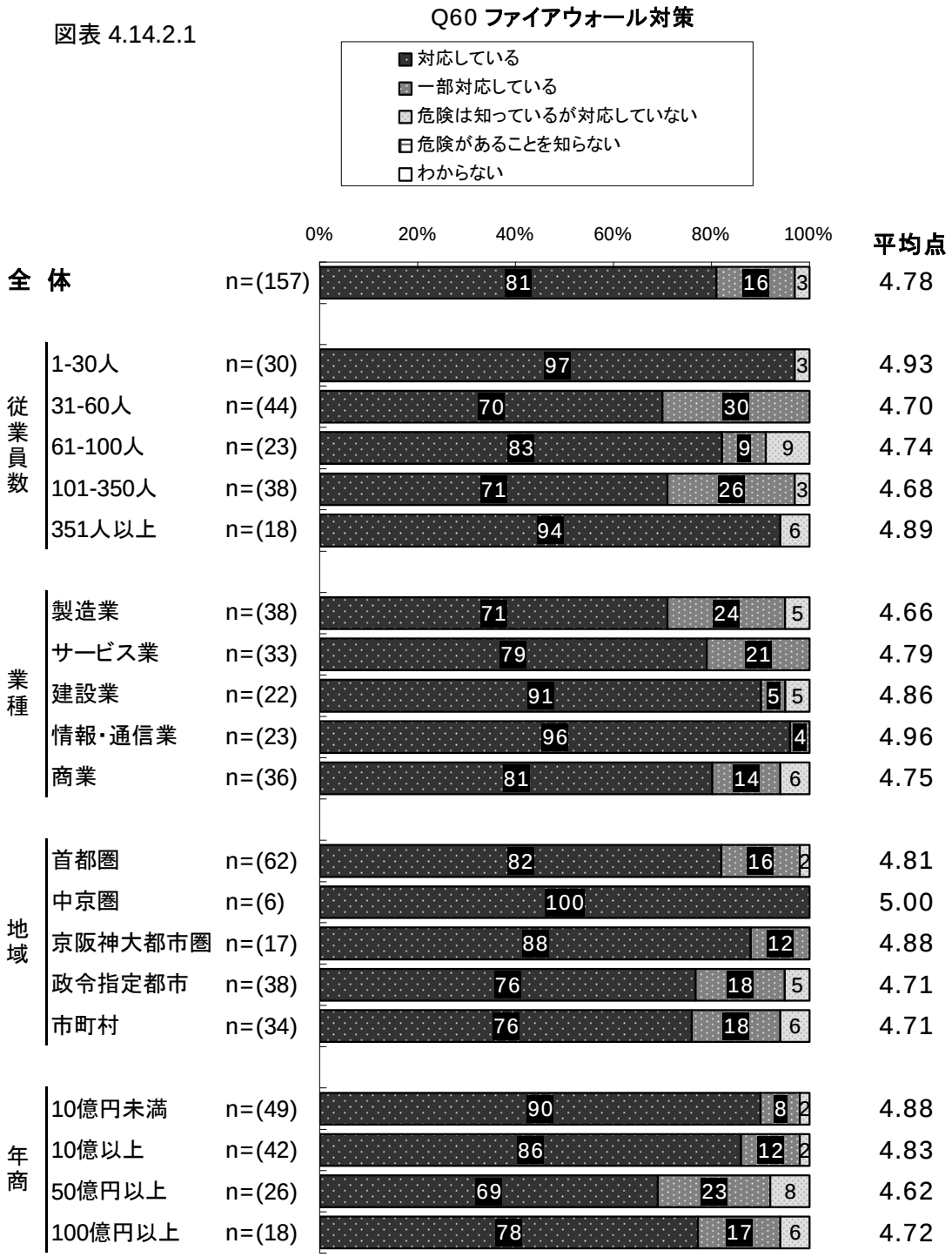




4.14.2 脅威対策 -Q60 ファイアウォール対策

- 全体では 4.78 点となり、『対応している』は 81%となっている。
- 従業員規模別に見ると、「1～30 人」で最も点数が高く 4.93 点となっている。『危険は知っているが対応していない』『危険があることを知らない』というネガティブな回答の割合は「31～60 人」で 0%となっている。
- 業種別に見ると、「情報・通信業」で 4.96 点と最も点数が高く、『危険は知っているが対応していない』『危険があることを知らない』というネガティブな回答の割合は 0%となっている。

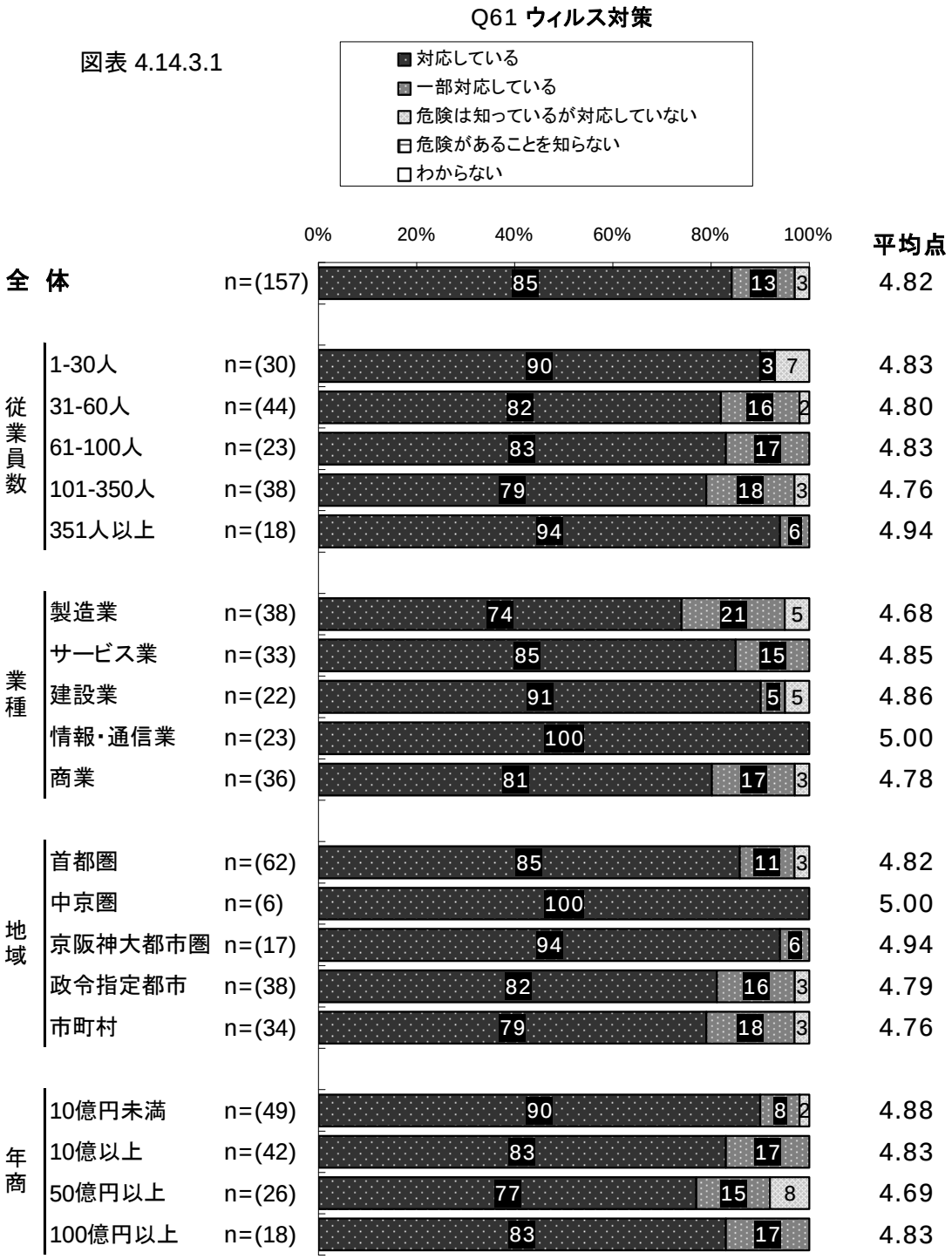
図表 4.14.2.1



4.14.3 脅威対策 -Q61 ウィルス対策

- 全体では 4.82 点となり、『対応している』は 85%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 4.94 点となっている。いずれの規模においても『対応している』『一部対応している』というポジティブな回答の割合は 9 割以上と非常に高い。
- 業種別に見ると、「情報・通信業」で 5.00 点と最も点数が高くなっている。

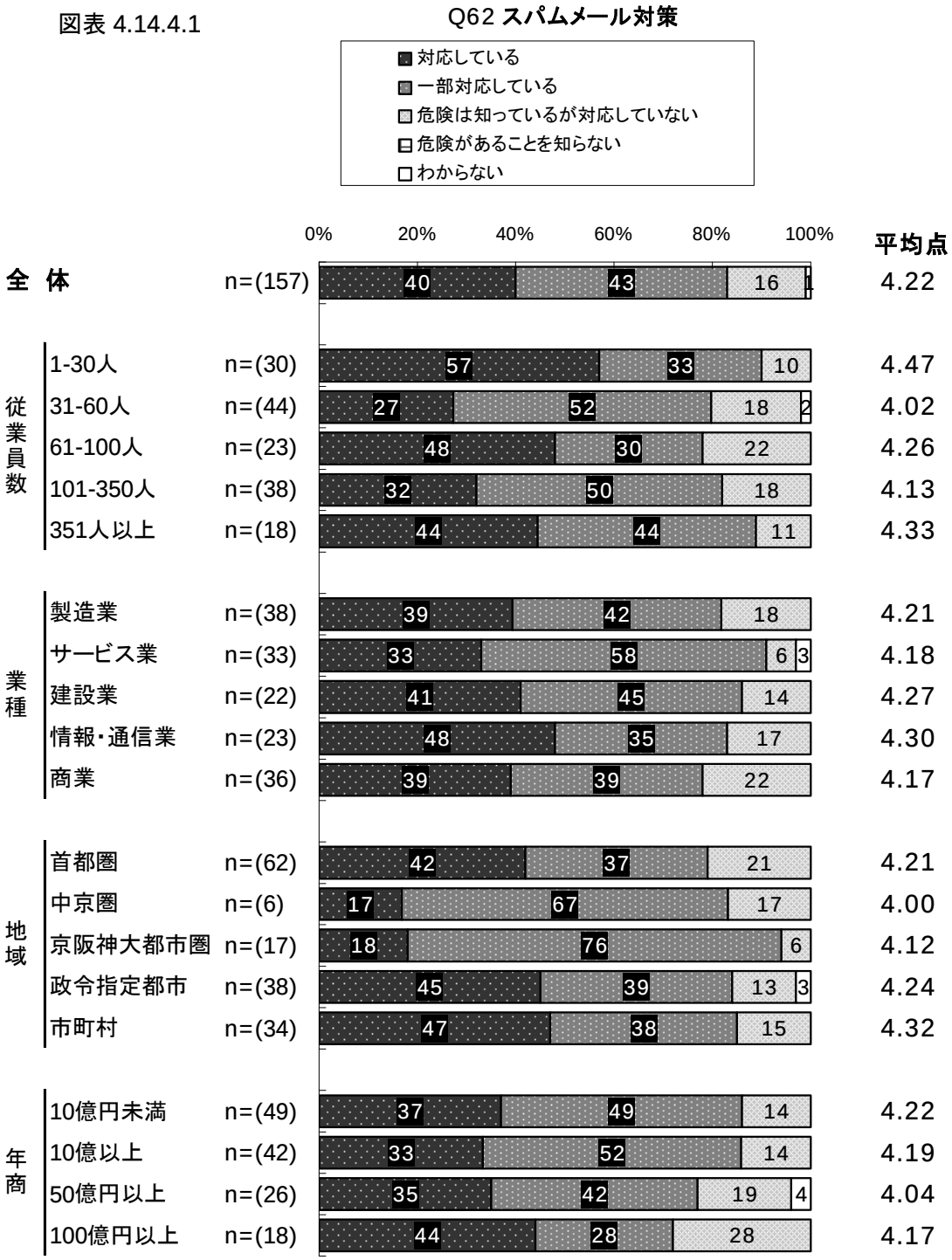
図表 4.14.3.1



4.14.4 脅威対策 -Q62 スパムメール対策

- 全体では 4.22 点となり、『対応している』は 40%となっている。
- 従業員規模別に見ると、「1～30 人」で最も点数が高く 4.47 点となっており、『対応している』割合も全体で最も高い。
- 業種別に見ると「情報・通信業」で 4.30 点と最も点数が高いが、比較的業種間の差は少ない。『対応している』『一部対応している』というポジティブな回答の割合は「サービス業」で 91%と最も高い。

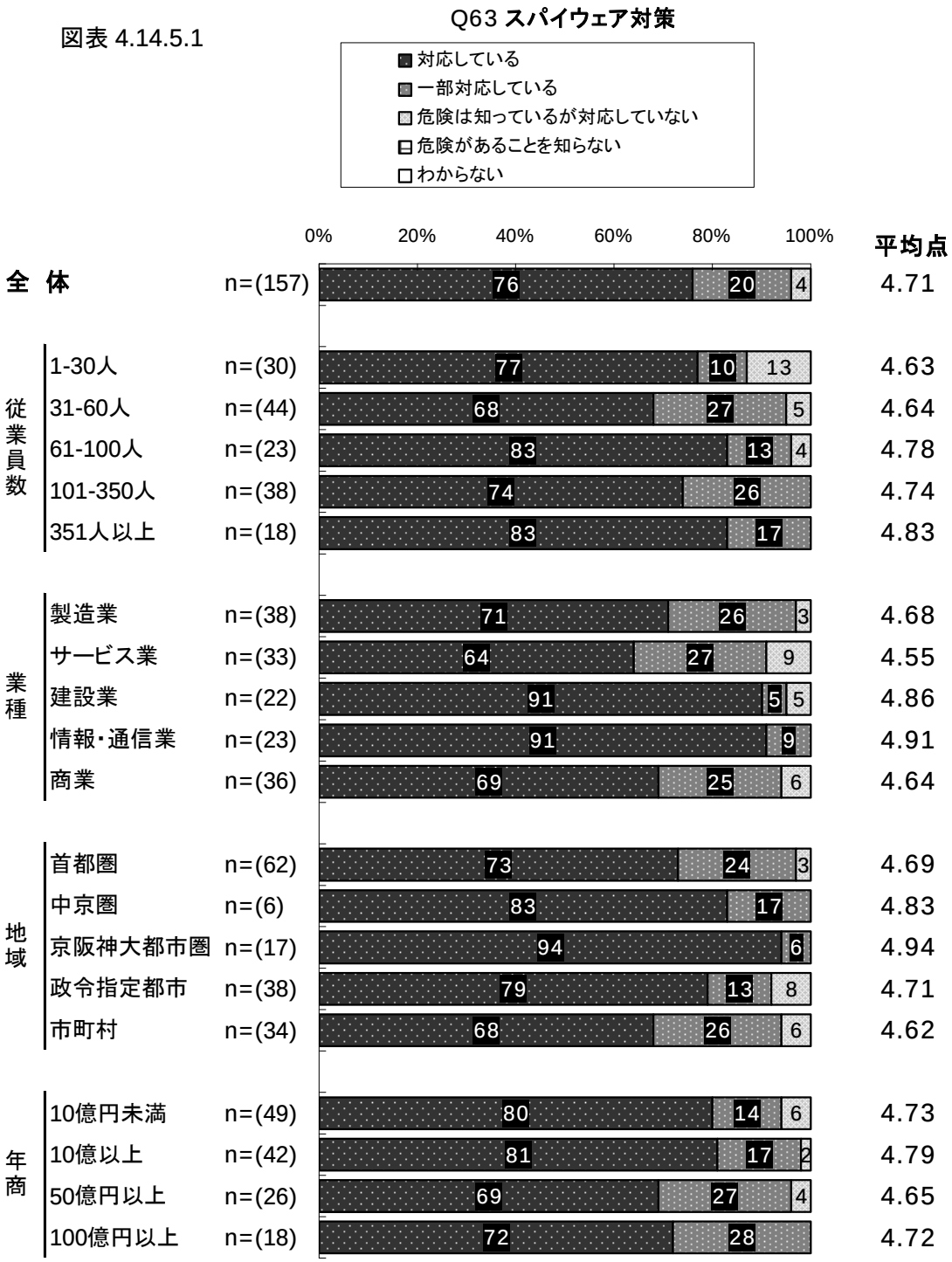
図表 4.14.4.1



4.14.5 脅威対策 -Q63 スパイウェア対策

- 全体では 4.71 点となり、『対応している』は 76%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 4.83 点となっているが、いずれの規模でも大きな差は見られない。「101～350 人」と「351 人以上」では『危険があることを知らない』『わからない』というネガティブな回答が 0%となっている。
- 業種別に見ると、「情報・通信業」で 4.91 点と最も点数が高いが、『対応している』は「情報・通信業」と「建設業」が 91%で同率である。

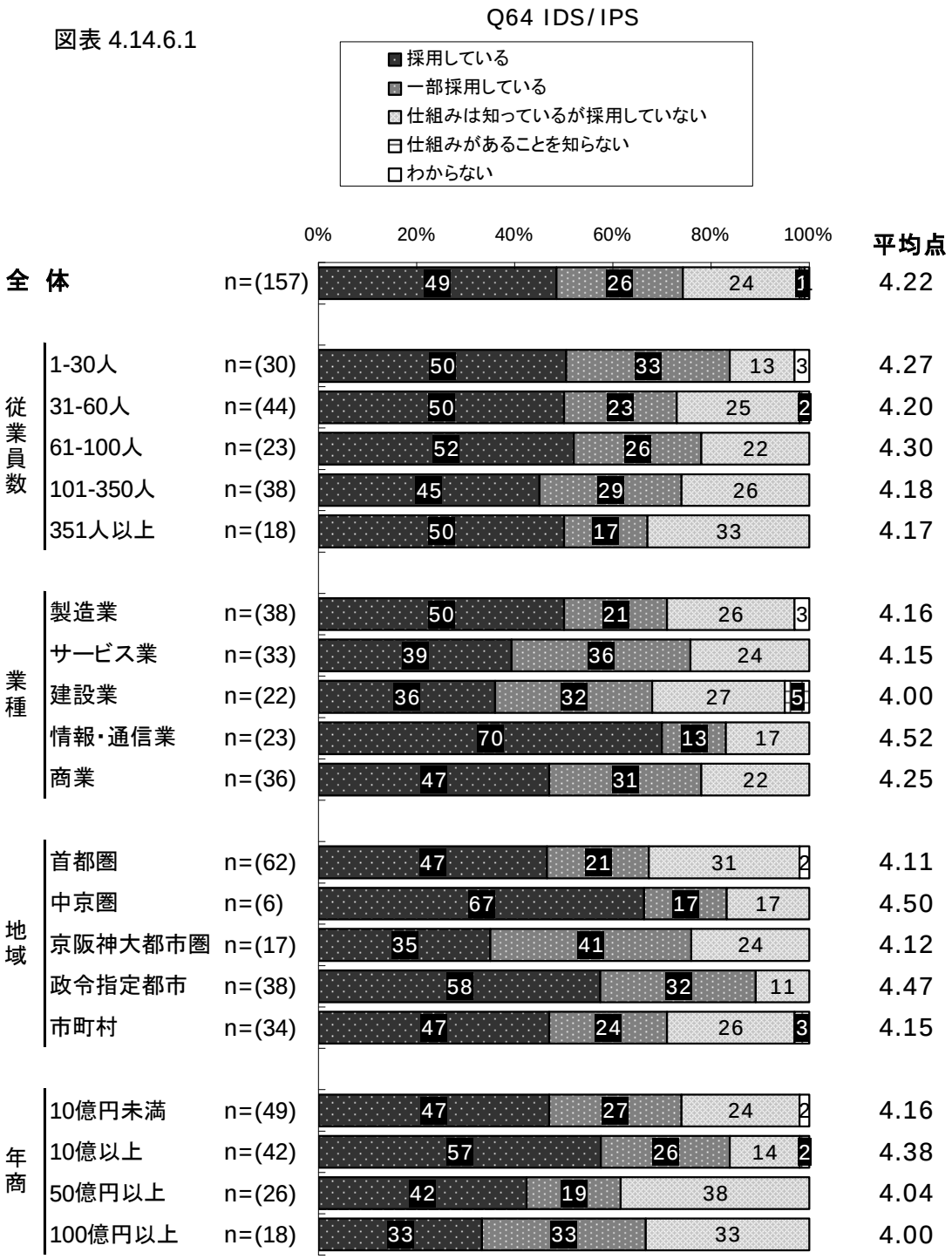
図表 4.14.5.1



4.14.6 脅威対策 −Q64 IDS/IPS

- 全体では 4.22 点となり、『採用している』は 49%となっている。
- 従業員規模別に見ると、「61～100 人」で最も点数が高く 4.30 点となっているが、いずれの規模を比較しても大きな差は見られない。
- 業種別に見ると「情報・通信業」で 4.52 点と最も点数が高い。「サービス業」「情報・通信業」「商業」では『仕組みがあることを知らない』『わからない』というネガティブな回答が見られなかった。

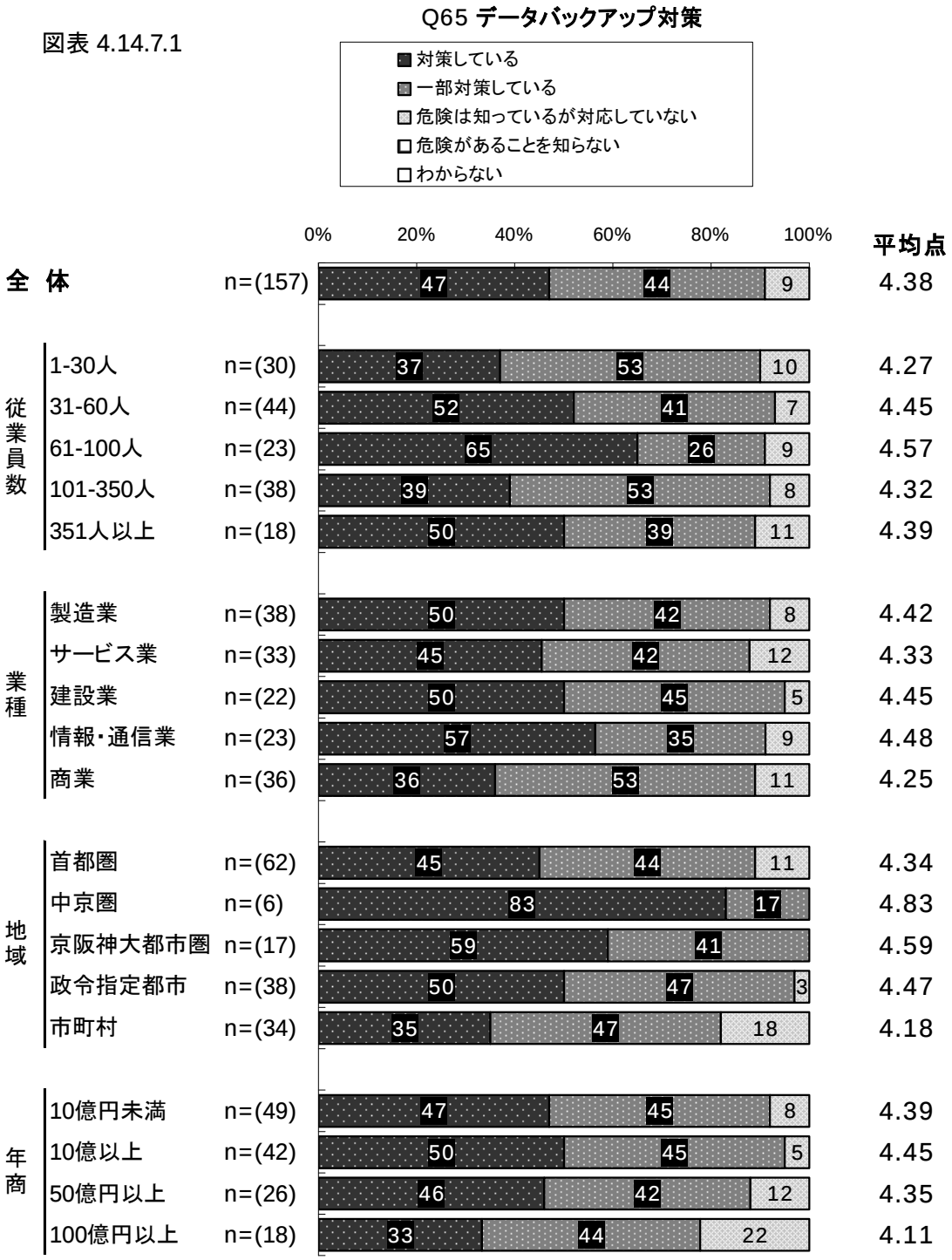
図表 4.14.6.1



4.14.7 脅威対策 -Q65 データバックアップ対策

- 全体では 4.38 点となり、『対策している』は 47%となっている。
- 従業員規模別に見ると、「61～100 人」で最も点数が高く 4.57 点となっている。いずれの規模においても『危険があることを知らない』『わからない』というネガティブな回答は見られなかった。
- 業種別に見ると、「情報・通信業」で 4.48 点と最も点数が高い。『対策している』の割合は「商業」で 36%と他の業種と比較して低い。

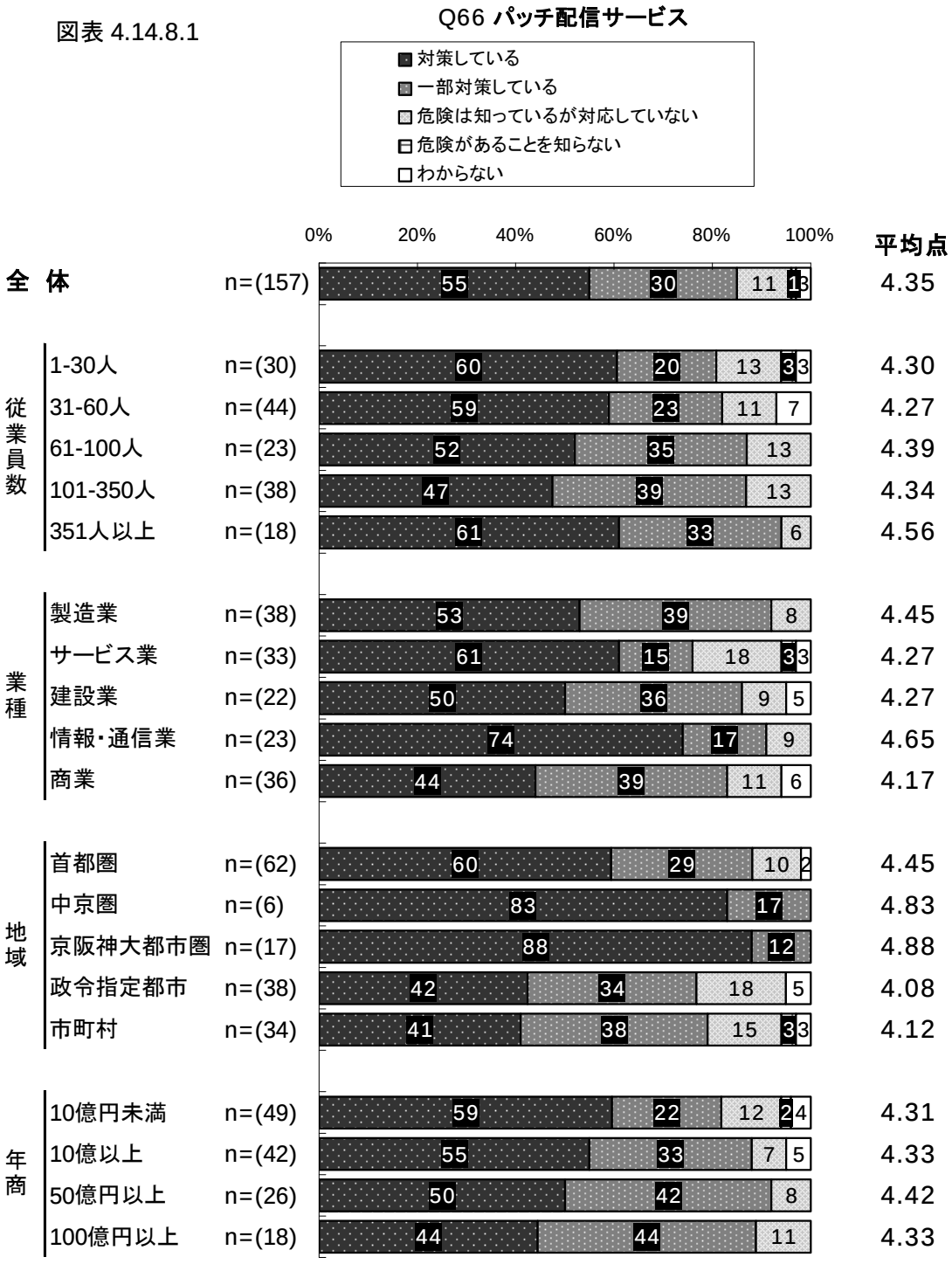
図表 4.14.7.1



4.14.8 脅威対策 -Q66 バッチ配信サービス

- 全体では 4.35 点となり、『対策している』は 55%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 4.56 点となっている。350 人以下の規模では、規模が大きくなるにつれて、『対策している』の割合が少なくなる。
- 業種別に見ると、「情報・通信業」で 4.65 点と最も点数が高い。「サービス業」においてはネガティブ回答の割合が 24%と他の業種と比較して若干高い。

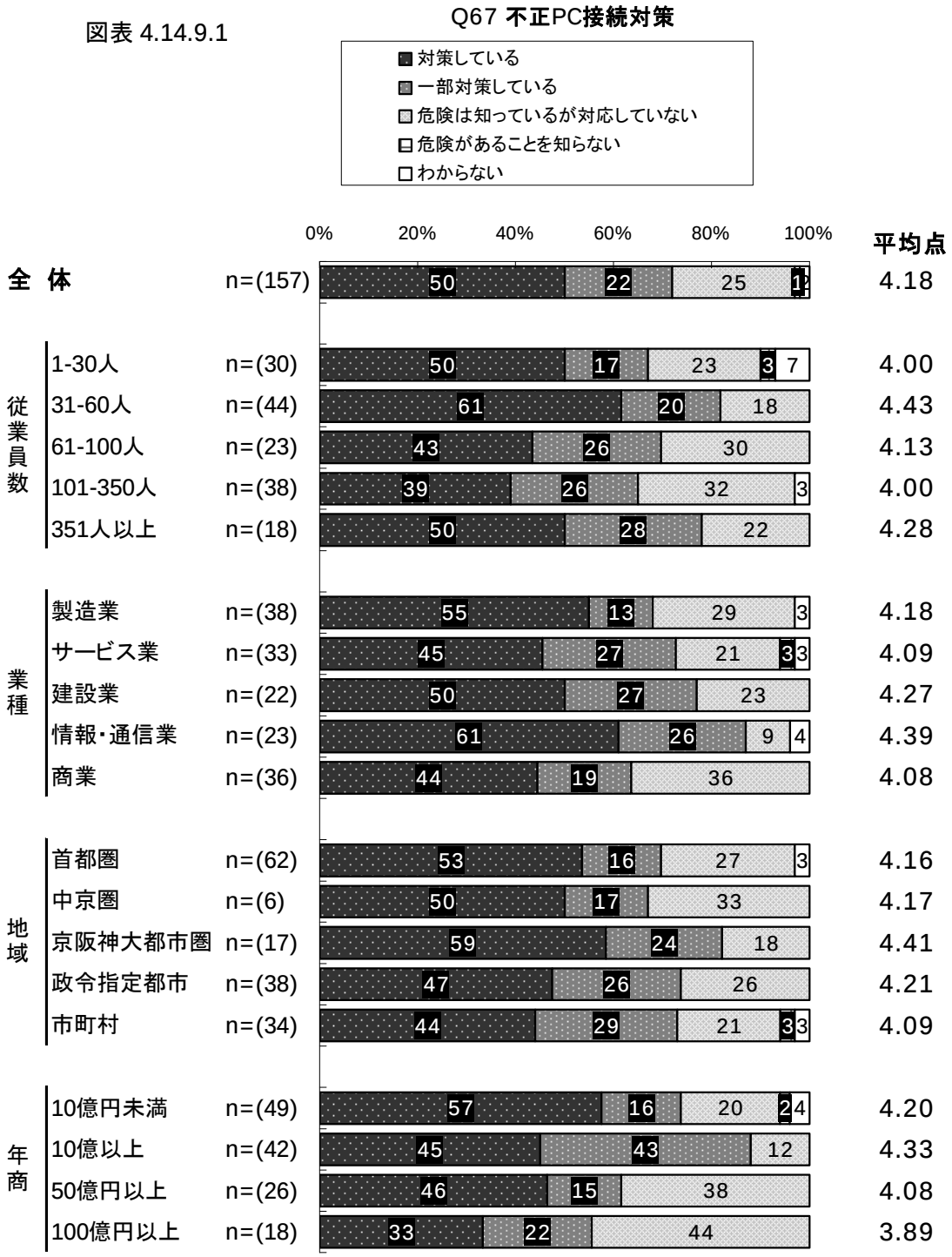
図表 4.14.8.1



4.14.9 脅威対策 -Q67 不正 PC 接続対策

- 全体では 4.18 点となり、『対策している』は 50%となっている。
- 従業員規模別に見ると、「31～60 人」で最も点数が高く 4.43 点となっている。『危険は知っているが対応していない』割合が高く、特に「101～350 人」では 32%となっている。
- 業種別に見ると、「情報・通信業」で最も点数が高く 4.39 点となっている。『危険は知っているが対応していない』割合は「情報・通信業」以外で高く、「商業」では 36%となっている。

図表 4.14.9.1

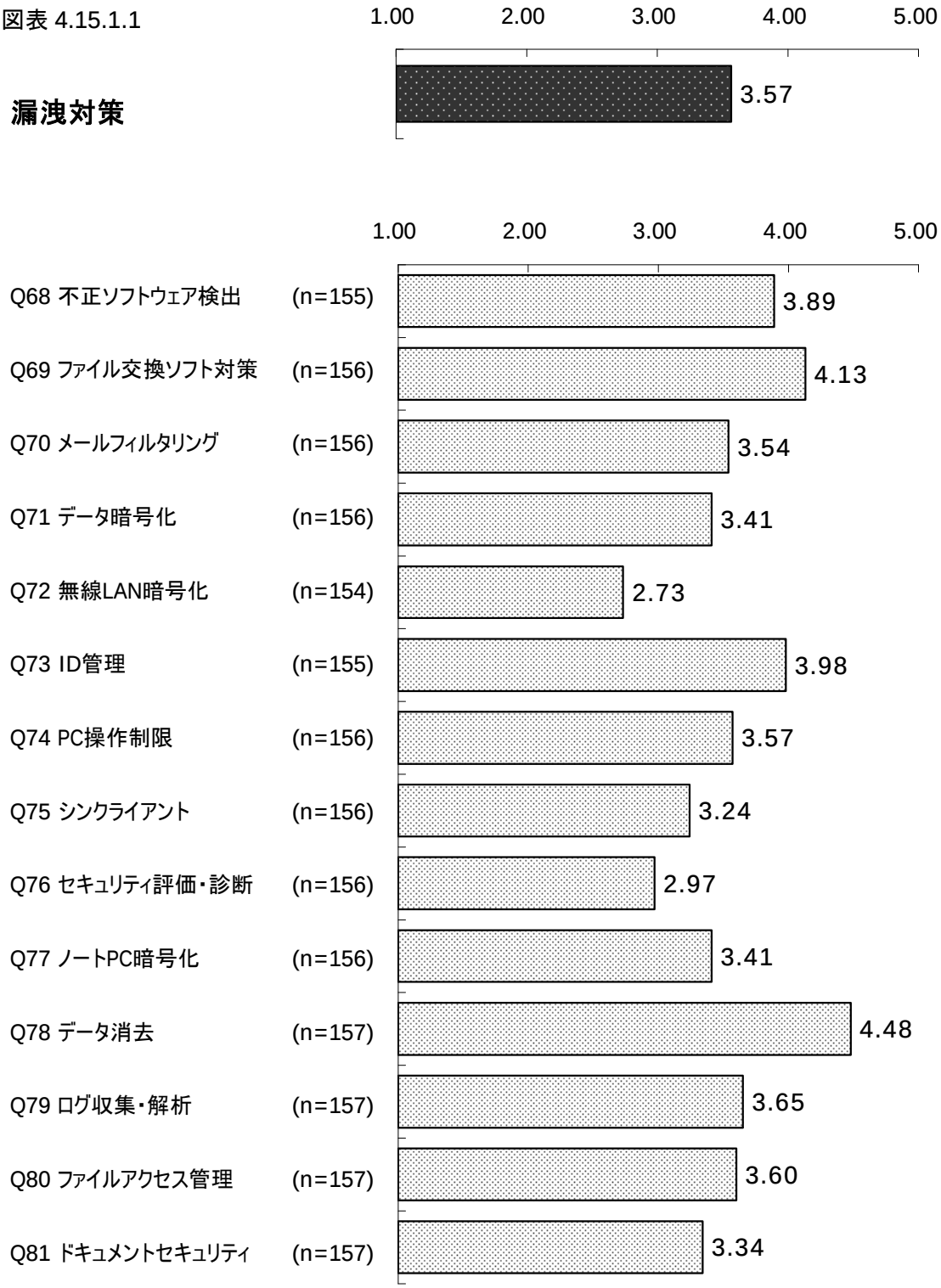


4.15 漏洩対策

4.15.1 漏洩対策

- 漏洩対策については、全体で 3.57 点となり、漏洩対策に含まれる項目の得点を見ると、『データ消去』が最も高く 4.48 点となっている。
- 逆に最も低くなっているのが『無線 LAN 暗号化』で 2.73 点である。
-

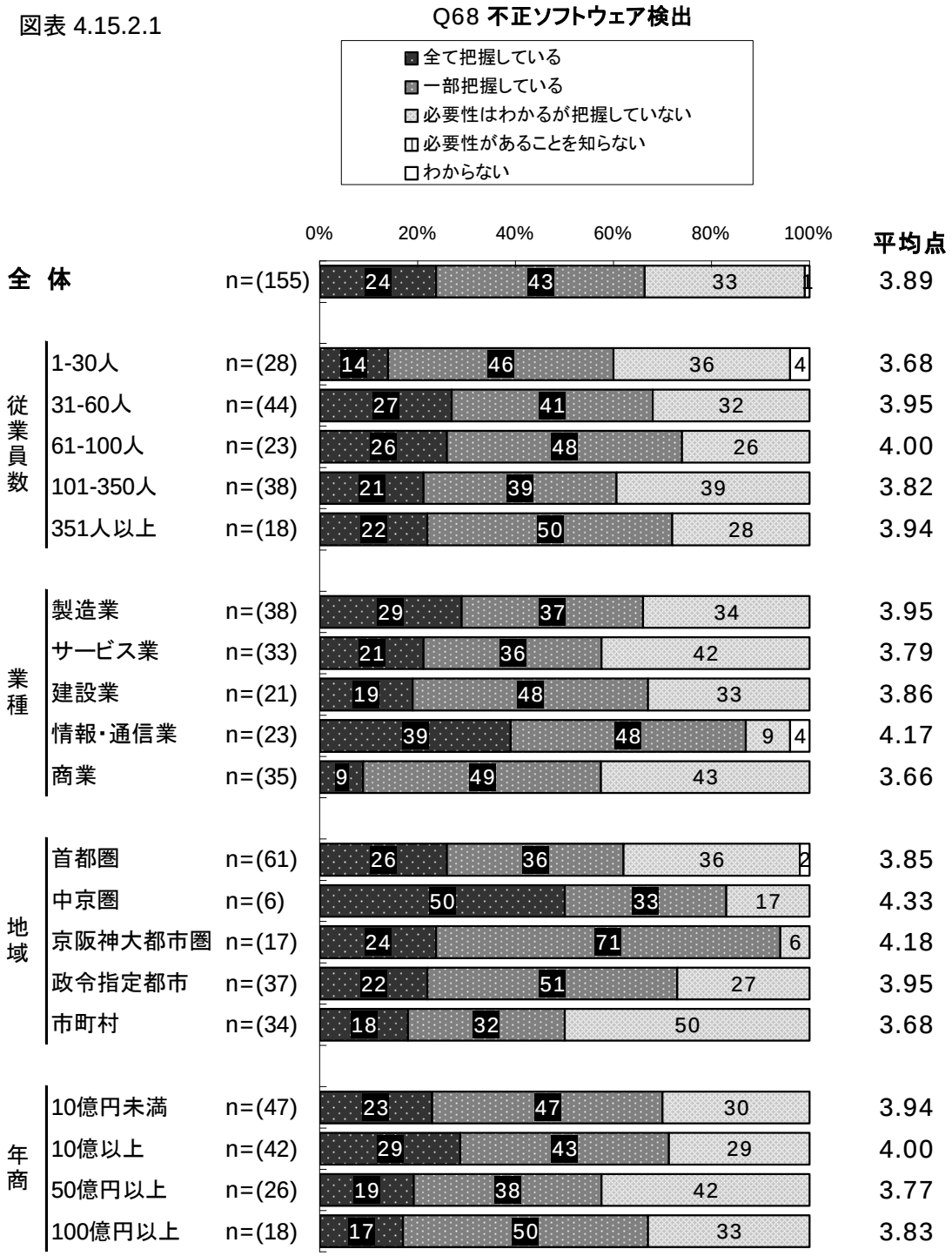
図表 4.15.1.1



4.15.2 漏洩対策 –Q68 不正ソフトウェア検出

- 全体では 3.89 点となり、『全て把握している』は 24%となっている。
- 従業員規模別に見ると、「61～100 人」で最も点数が高く 4.00 点となっている。『全て把握している』割合は「1～30 人」が最も低く 14%で、最も高い「31～60 人」の 27%の約半分となっている。
- 業種別に見ると、「情報・通信業」で最も点数が高く 4.17 点となっている。「商業」では『全て把握している』割合が 9%となっており、最も高い「情報・通信業」の 39%と比べると 4 分の 1 以下と非常に低い。

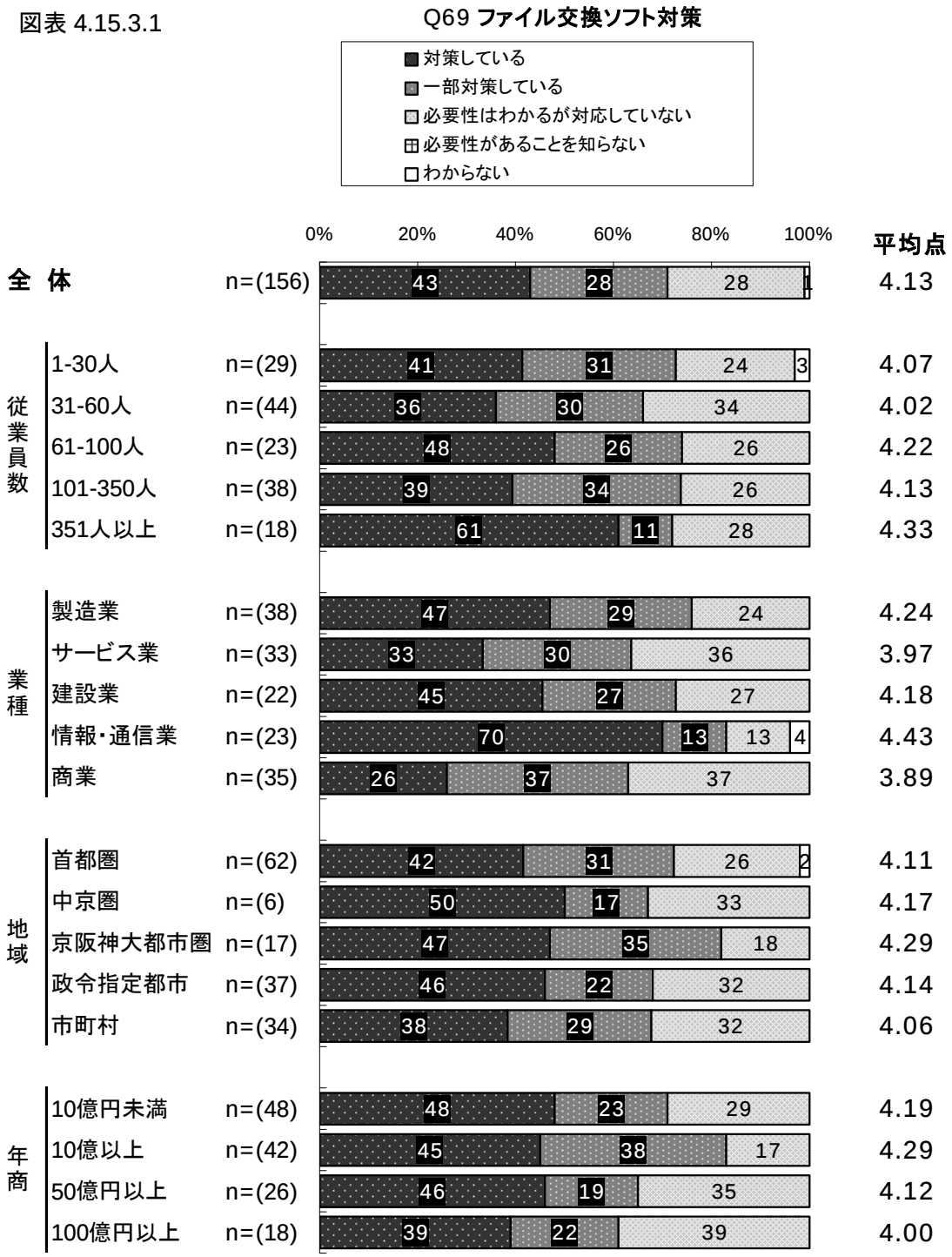
図表 4.15.2.1



4.15.3 漏洩対策 –Q69 ファイル交換ソフト対策

- 全体では 4.13 点となり、『対策している』は 43%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 4.33 点となっている。『対策している』割合も「351 人以上」で最も高く 61%だが、『対策している』『一部対策している』というポジティブな回答の割合はいずれの規模でも 7 割程度となっている。
- 業種別に見ると、「情報・通信業」で最も点数が高く 4.43 点となっている。「商業」と「サービス業」では『対応している』割合がそれぞれ 26%、33%となっており、最も高い「情報・通信業」の 70%と比較して非常に低い。

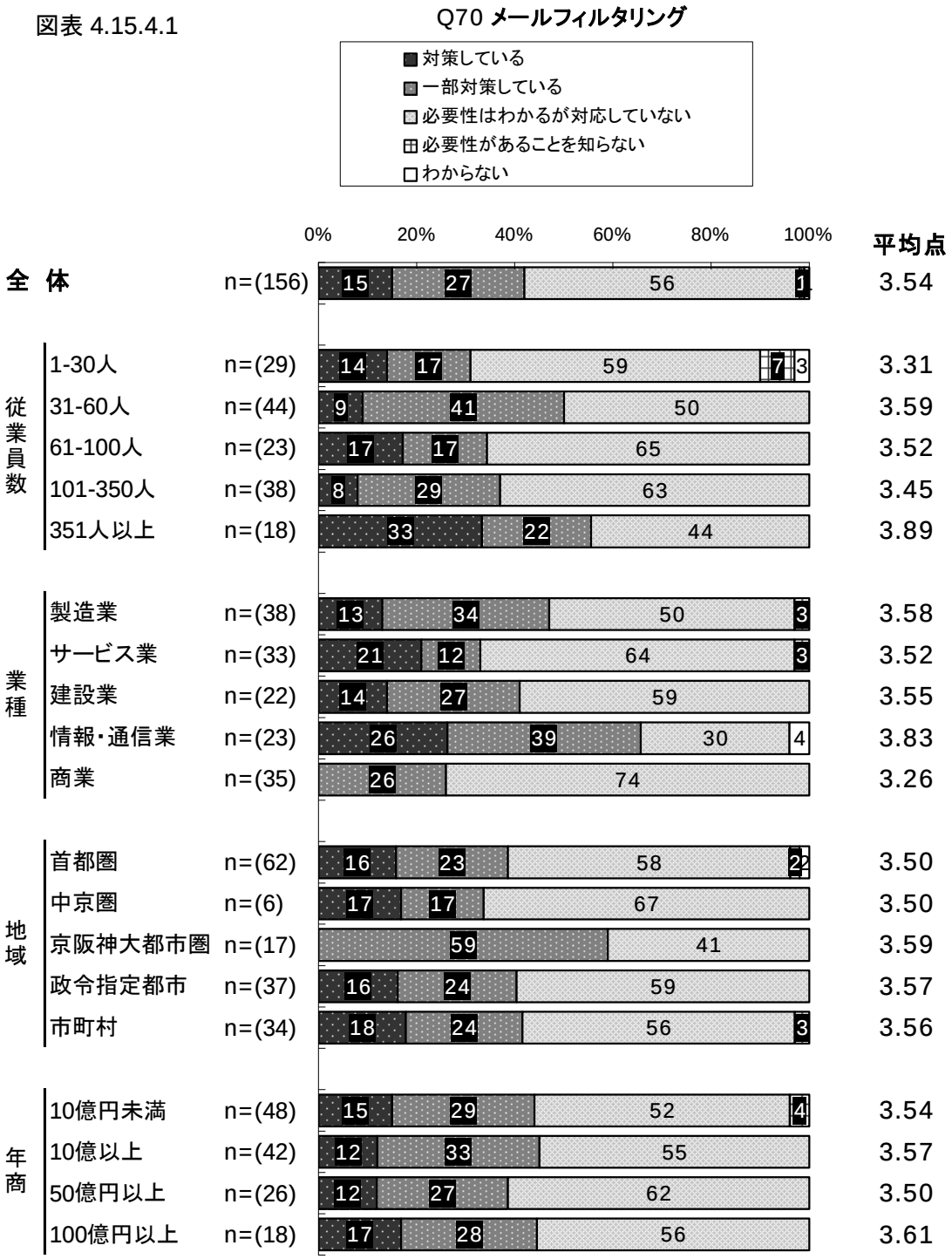
図表 4.15.3.1



4.15.4 漏洩対策 –Q70 メールフィルタリング

- 全体では 3.54 点となり、『対策している』は 15%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 3.89 点となっている。『必要性はわかるが対応していない』割合は「61～100 人」と「101-350」がそれぞれ 65%、63%と高い。
- 業種別に見ると、「情報・通信業」で最も点数が高く 3.83 点となっている。「商業」においては『対応している』割合が 0%となっており、『必要は分かるが対応してない』割合が 74%と、『情報・通信業』の 30%と比較して非常に高くなっている。

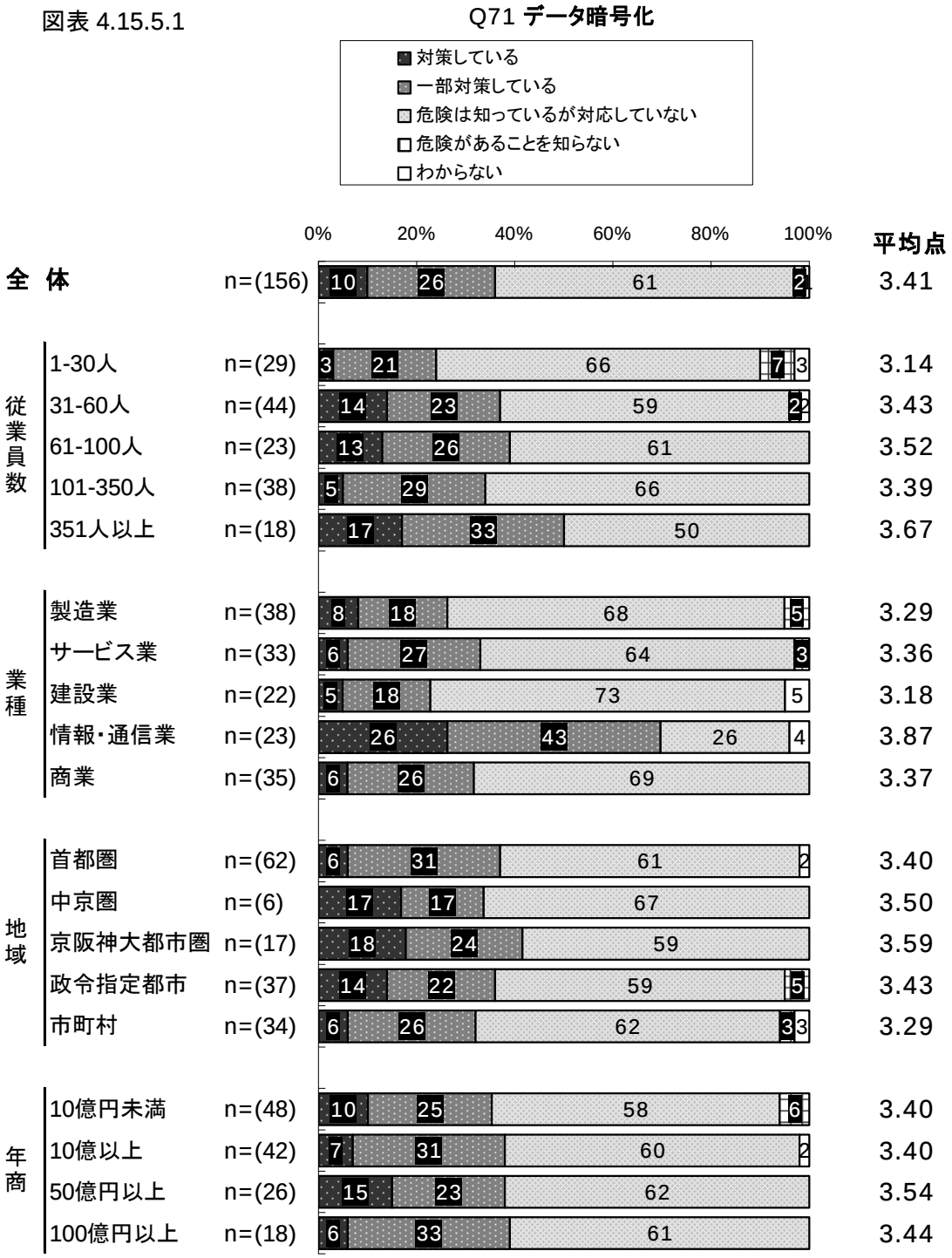
図表 4.15.4.1



4.15.5 漏洩対策 -Q71 データ暗号化

- 全体では 3.41 点となり、『対策している』は 10%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 3.67 点となっている。「1～30 人」では『対策している』割合が 3%となっている。
- 業種別に見ると、「情報・通信業」で最も点数が高く 3.87 点となっている。「情報・通信業」においては『対応している』割合も 26%と他の業種と比較して非常に高。

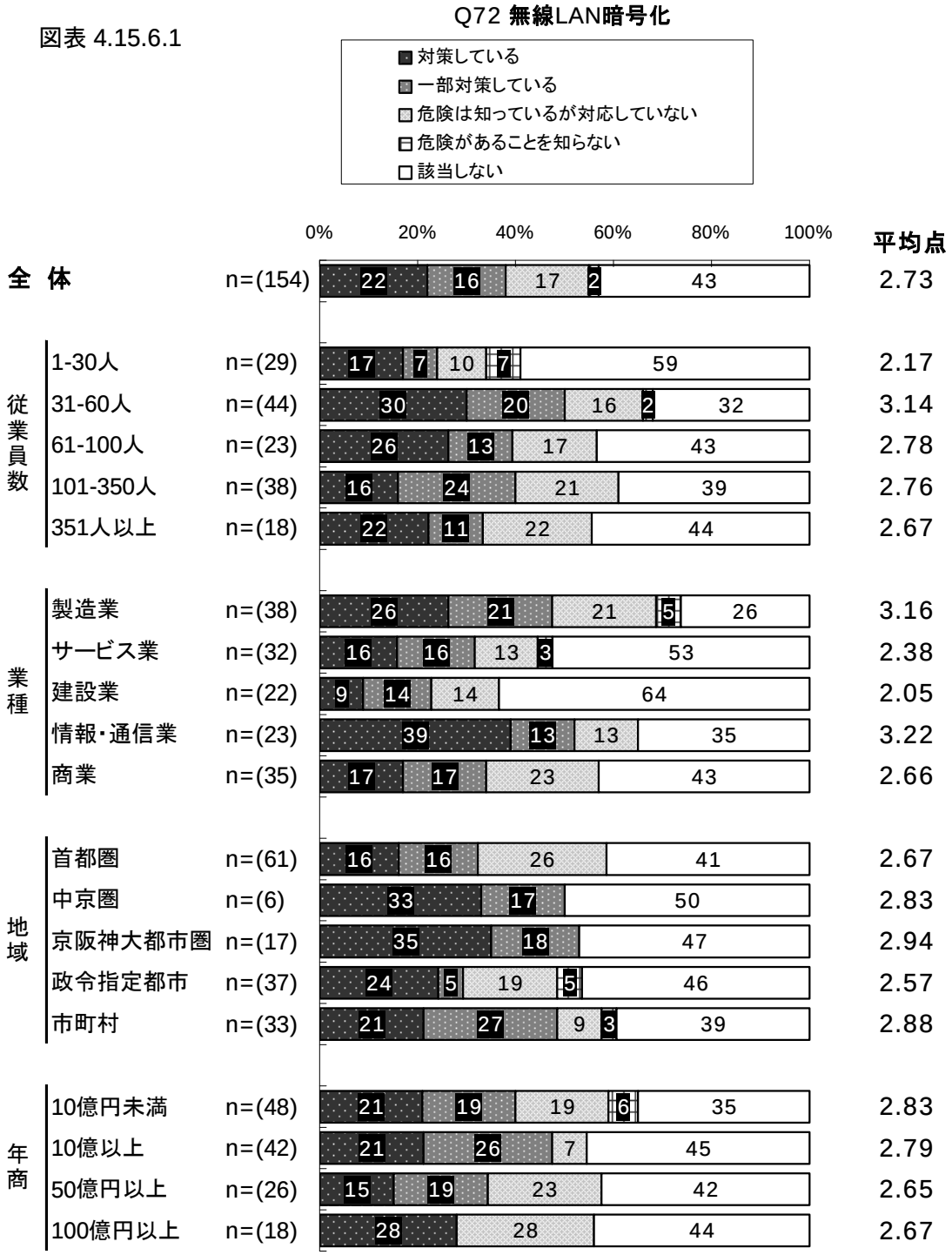
図表 4.15.5.1



4.15.6 漏洩対策 −Q72 無線 LAN 暗号化

- 全体では 2.73 点となり、『対策している』は 22%となっている。
- 従業員規模別に見ると、「31～60 人」で最も点数が高く 3.14 点となっている。「1～30 人」では『危険があることを知らない』割合が 7%あり、さらに、『該当しない』が 59%と高くなっている。
- 業種別に見ると、「情報・通信業」で最も点数が高く 3.22 点となっている。「建設業」においては『対策している』割合が 9%と低く、『該当しない』が 64%と非常に高くなっている。

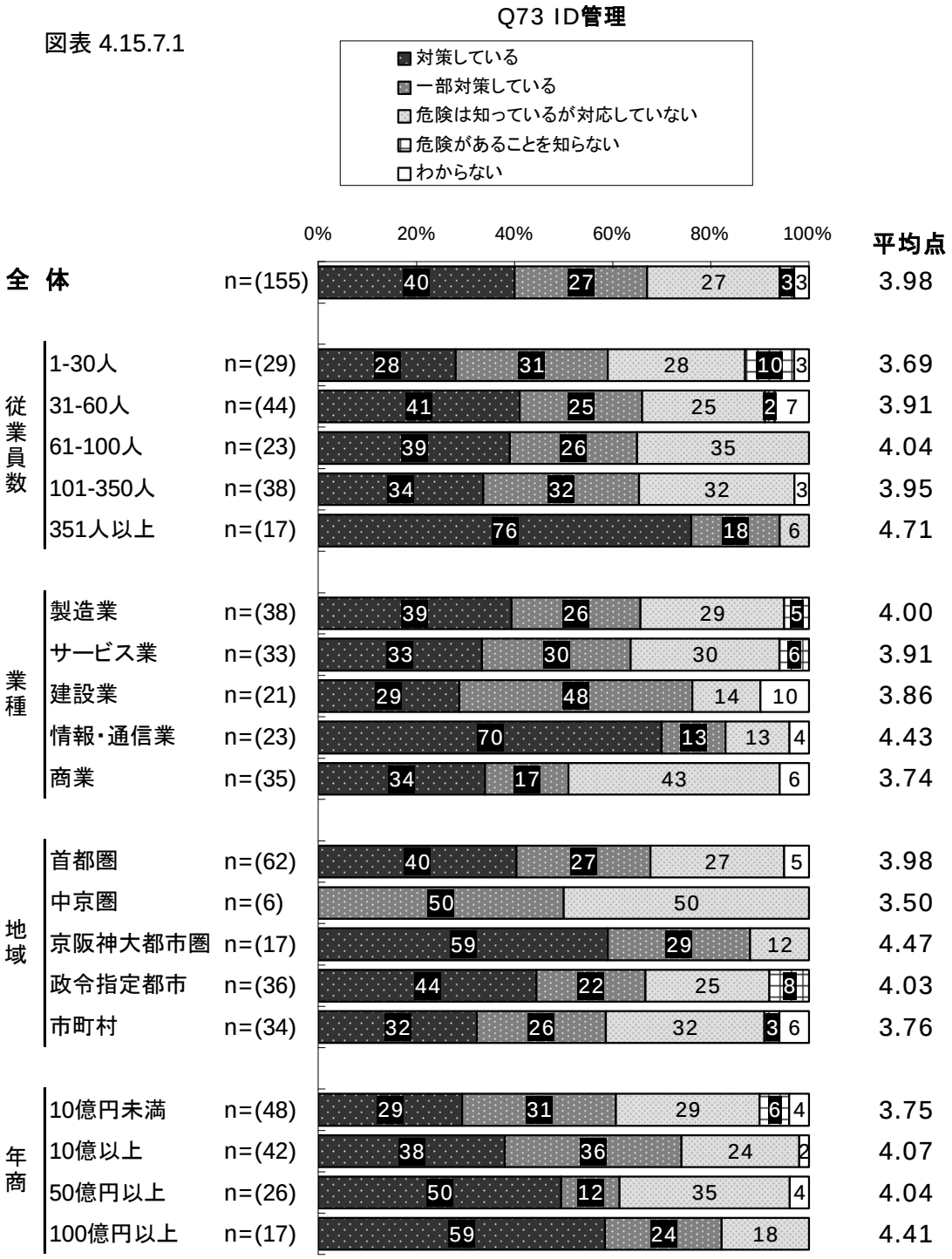
図表 4.15.6.1



4.15.7 漏洩対策 -Q73 ID 管理

- 全体では 3.98 点となり、『対策している』は 40%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 4.71 点となっている。「351 人以上」では『対策している』が 76%と、他の規模と比較して非常に高い。
- 業種別に見ると「情報・通信業」で最も点数が高く 4.43 点となっている。「商業」においては『危険は知っているが対応していない』割合が 43%と他の業種と比較して非常に高い。

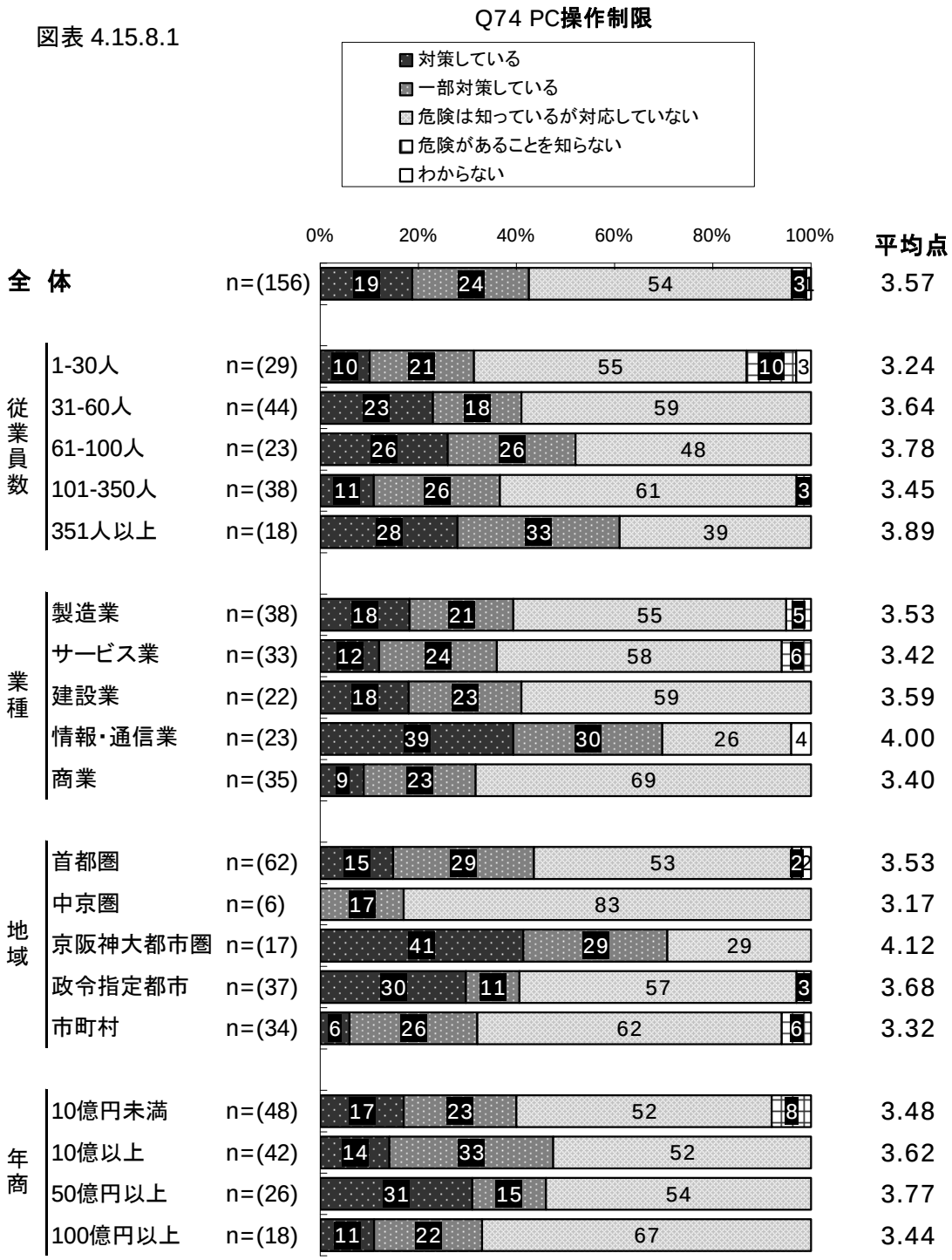
図表 4.15.7.1



4.15.8 漏洩対策 -Q74 PC 操作制限

- 全体では 3.57 点となり、『対策している』は 19%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 3.89 点となっている。「101～350 人」以外は規模が大きくなるにつれて『対策している』『一部対策している』というポジティブな回答の割合が増加する傾向にある。
- 業種別に見ると、「情報・通信業」で最も点数が高く 4.00 点となっている。「情報・通信業」以外の業種で大きな差は見られないが、「商業」において『対策している』が 9%と低い。

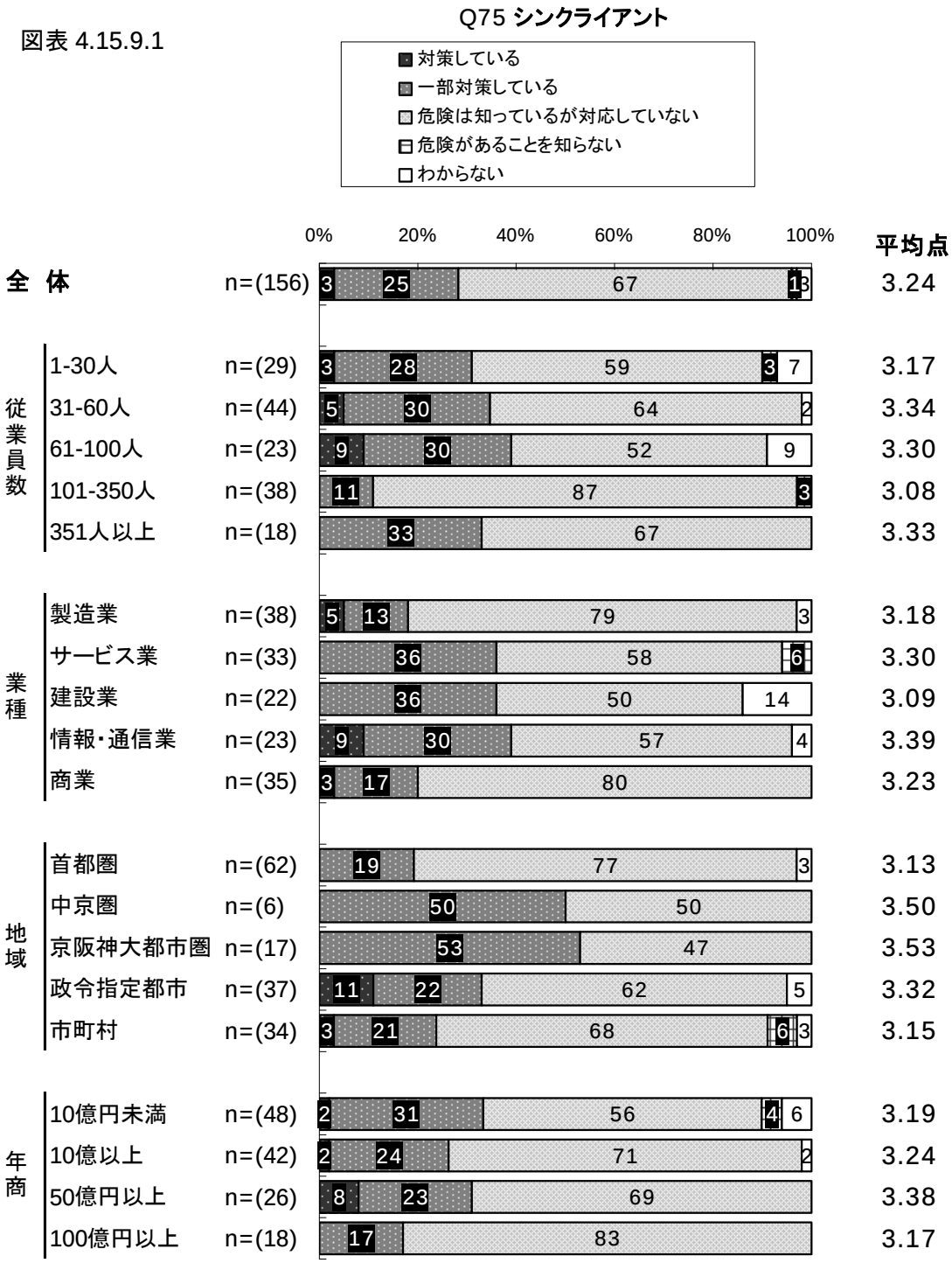
図表 4.15.8.1



4.15.9 漏洩対策 –Q75 シンクライアント

- 全体では 3.24 点となり、『対策している』は 3%となっている。
- 従業員規模別に見ると、「31～60 人」で最も点数が高く 3.34 点となっている。「101～350 人」と「351 人以上」では『対策している』割合が 0%となっている。100 人以下の規模では、規模が大きくなるにつれて『対策している』『一部対策している』というポジティブな回答の割合が増加傾向にある。
- 業種別に見ると「情報・通信業」で最も点数が高く 3.39 点となっている。「サービス業」「建設業」では『対策している』割合が 0%となっているが、「一部対策している」割合が高いため、ネガティブ回答の割合は比較的低い。「製造業」と「商業」はネガティブ回答が 8 割前後まで達している。

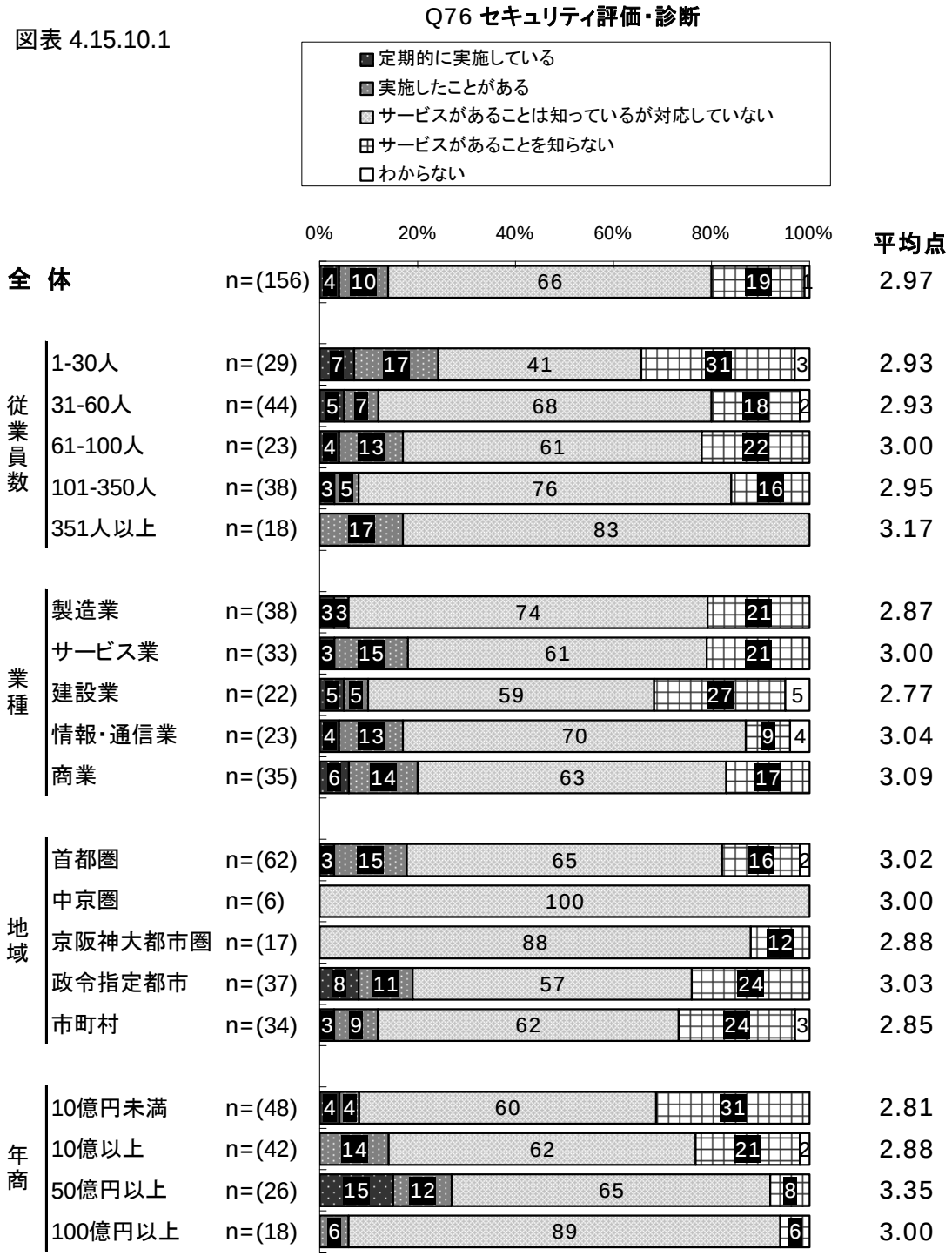
図表 4.15.9.1



4.15.10 漏洩対策 –Q76 セキュリティ評価・診断

- 全体では 2.97 点となり、『定期的に実施している』は 4%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 3.17 点となっているものの、『定期的に実施している』割合は 0%となっている。『定期的に実施している』割合は規模が小さくなるにつれて増加している。一方、『サービスがあることを知らない』割合についても規模が小さくなるにつれて高くなっている。
- 業種別に見ると「商業」で最も点数が高く 3.09 点となっている。『定期的に実施している』割合はいずれの業種でも大きな差は見られず 5%前後と低く、全体的に『サービスがあることを知らない』割合が高い。

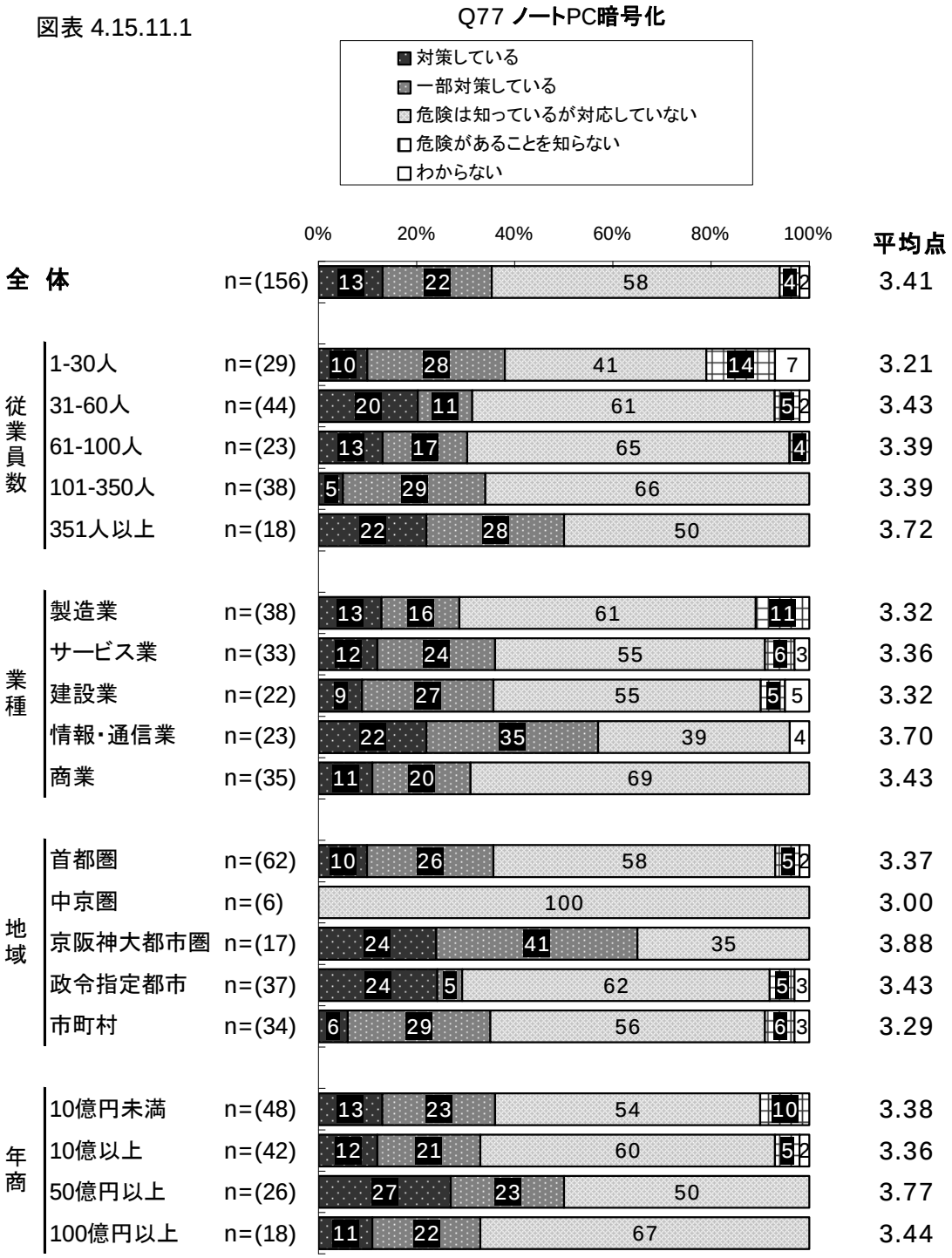
図表 4.15.10.1



4.15.11 漏洩対策 –Q77 ノート PC 暗号化

- 全体では 3.41 点となり、『対策している』は 13%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 3.72 点となっている。「101～350 人」と「351 人以上」では 0%である『危険があることを知らない』割合は規模が小さくなるにつれ高くなる傾向が見られ、「1～30 人」では 14%と比較的大きな割合を占める。
- 業種別に見ると、「情報・通信業」で最も点数が高く 3.70 点となっている。他の業種間では大きな差は見られない。

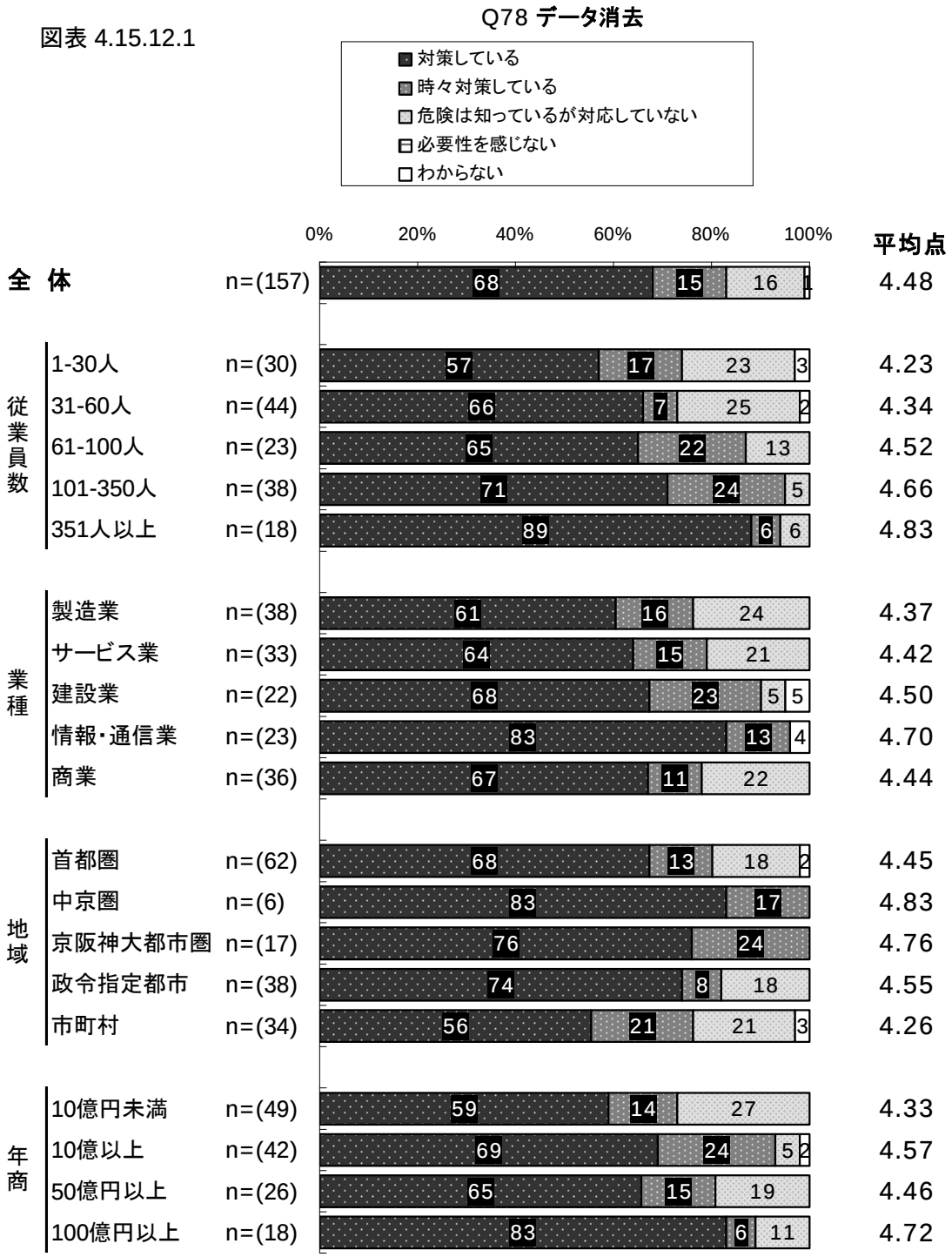
図表 4.15.11.1



4.15.12 漏洩対策 -Q78 データ消去

- 全体では 4.48 点となり、『対策している』は 68%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 4.83 点となっている。『対策している』割合は規模が大きくなるにつれて増加している。
- 業種別に見ると、「情報・通信業」で最も点数が高く 4.70 点となり、『対策している』『時々対策している』というポジティブな回答の割合は 96%と非常に高い。

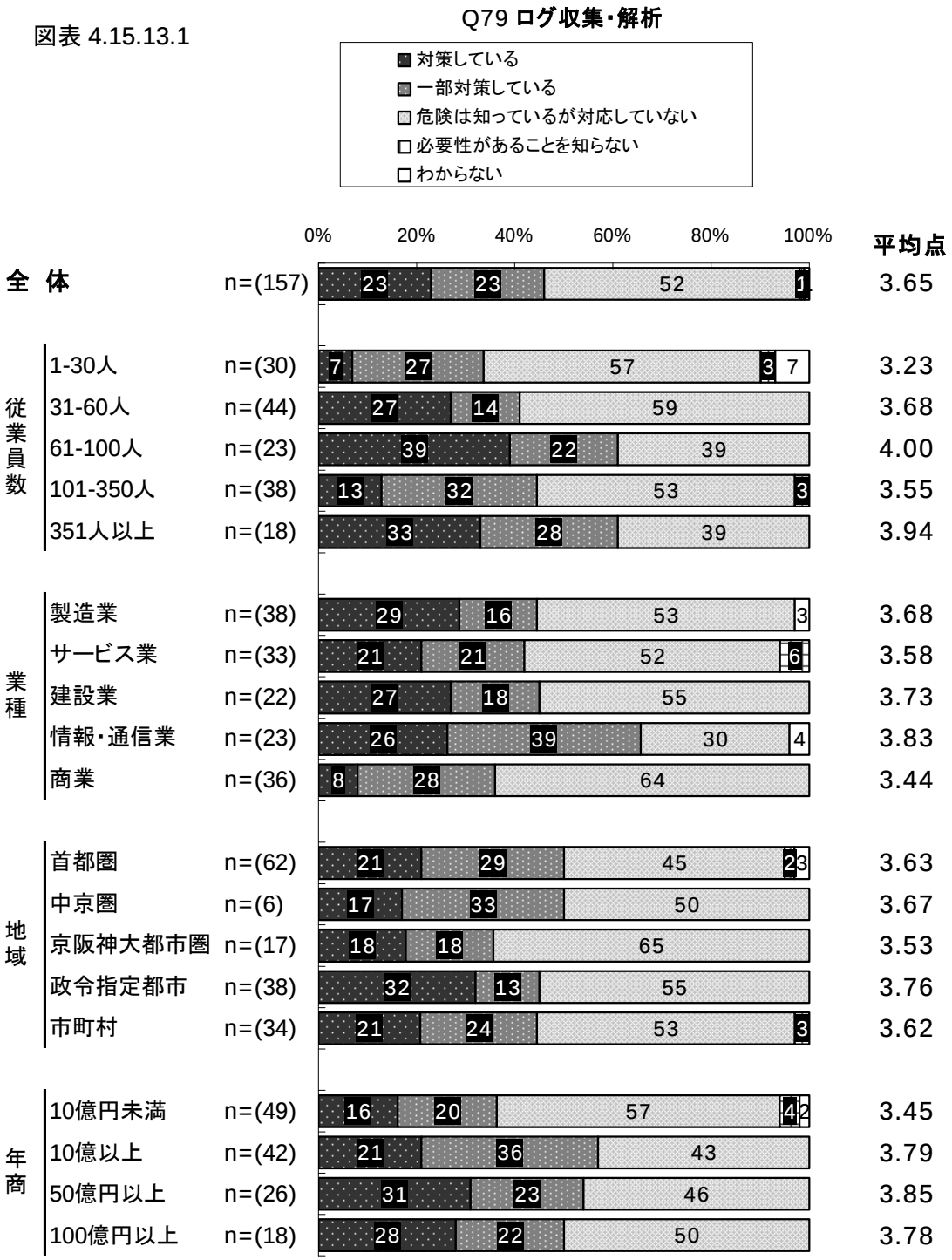
図表 4.15.12.1



4.15.13 漏洩対策 –Q79 ログ収集・解析

- 全体では 3.65 点となり、『対策している』は 23%となっている。
- 従業員規模別に見ると、「61～100 人」で最も点数が高く 4.00 点となっている。また、「61～100 人」と「351 人以上」の規模における構成比が非常に似ている。
- 業種別に見ると、「情報・通信業」で最も点数が高く 3.83 点となっている。『対策している』割合は「商業」が最も低く 8%で、他の業種と比較して非常に低い。

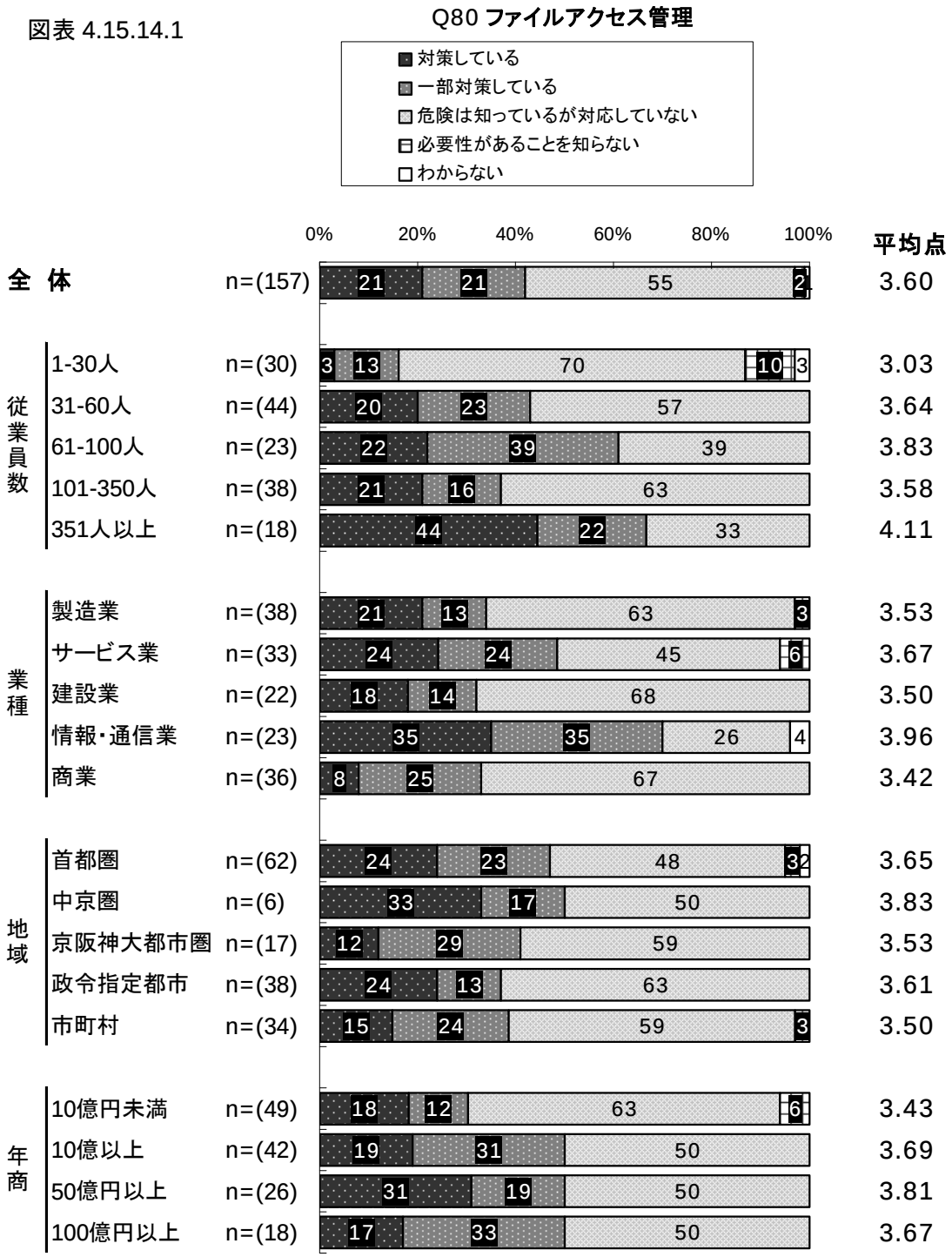
図表 4.15.13.1



4.15.14 漏洩対策 –Q80 ファイルアクセス管理

- 全体では 3.60 点となり、『対策している』は 21%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 4.11 点となっている。『対策している』割合は規模が大きくなるにつれて高くなっており、「351 人以上」では 44%と非常に高い。
- 業種別に見ると「情報・通信業」が 3.96 点と最も高い。「商業」では『対策している』が８％と他の業種と比較して非常に低いが、『一部対策している』をあわせると「製造業」「建設業」と並び 33%となる。

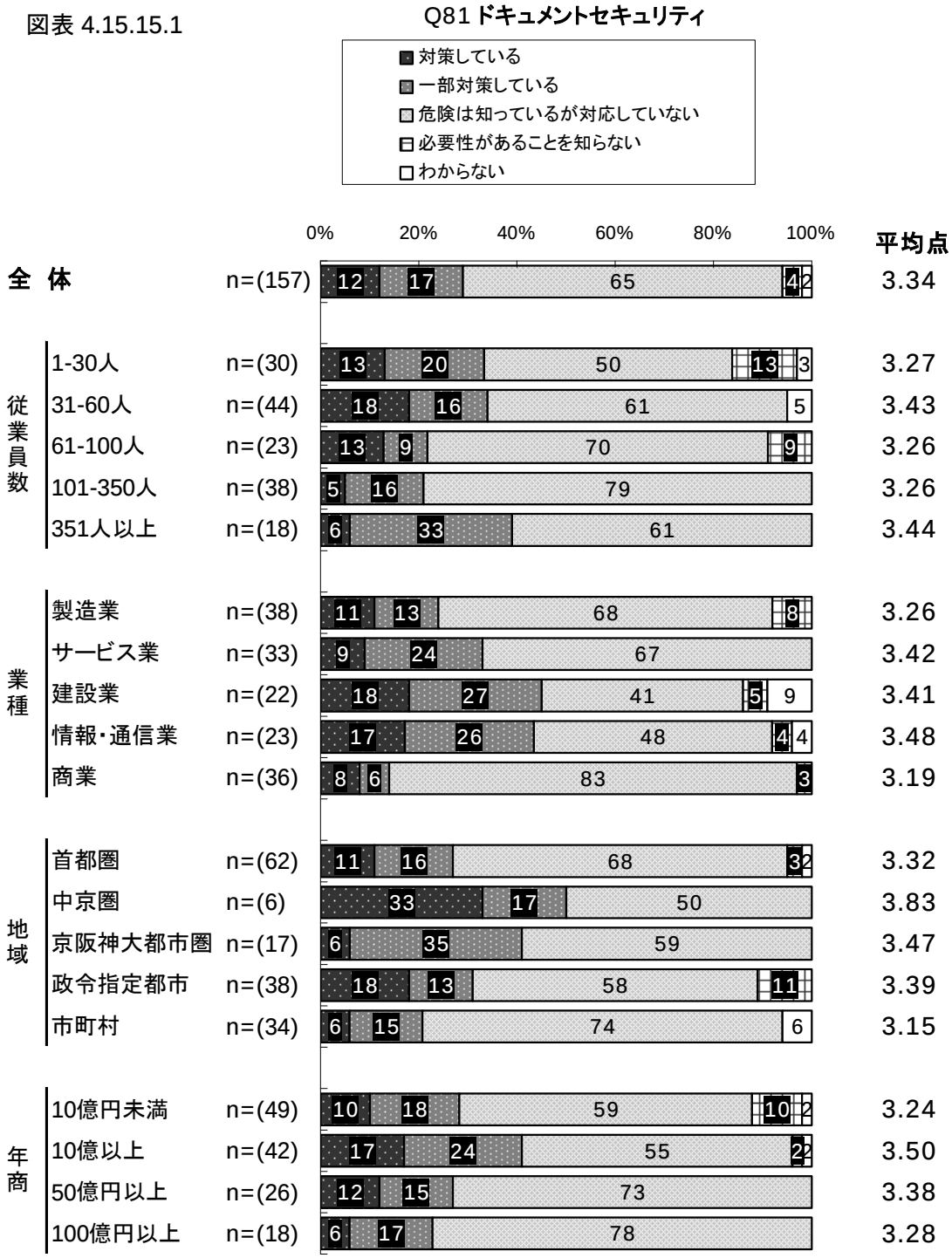
図表 4.15.14.1



4.15.15 漏洩対策 −Q81 ドキュメントセキュリティ

- 全体では 3.34 点となり、『対策している』は 12%となっている。
- 従業員規模別に見ると、「315 人以上」で最も点数が高く 3.44 点となっているが、いずれの規模においても値に大きな差は見られない。また、いずれの規模においても『危険は知っているが対応していない』の割合が最も高い。
- 業種別に見ると、「情報・通信業」で最も点数が高く 3.48 点となっている。

図表 4.15.15.1

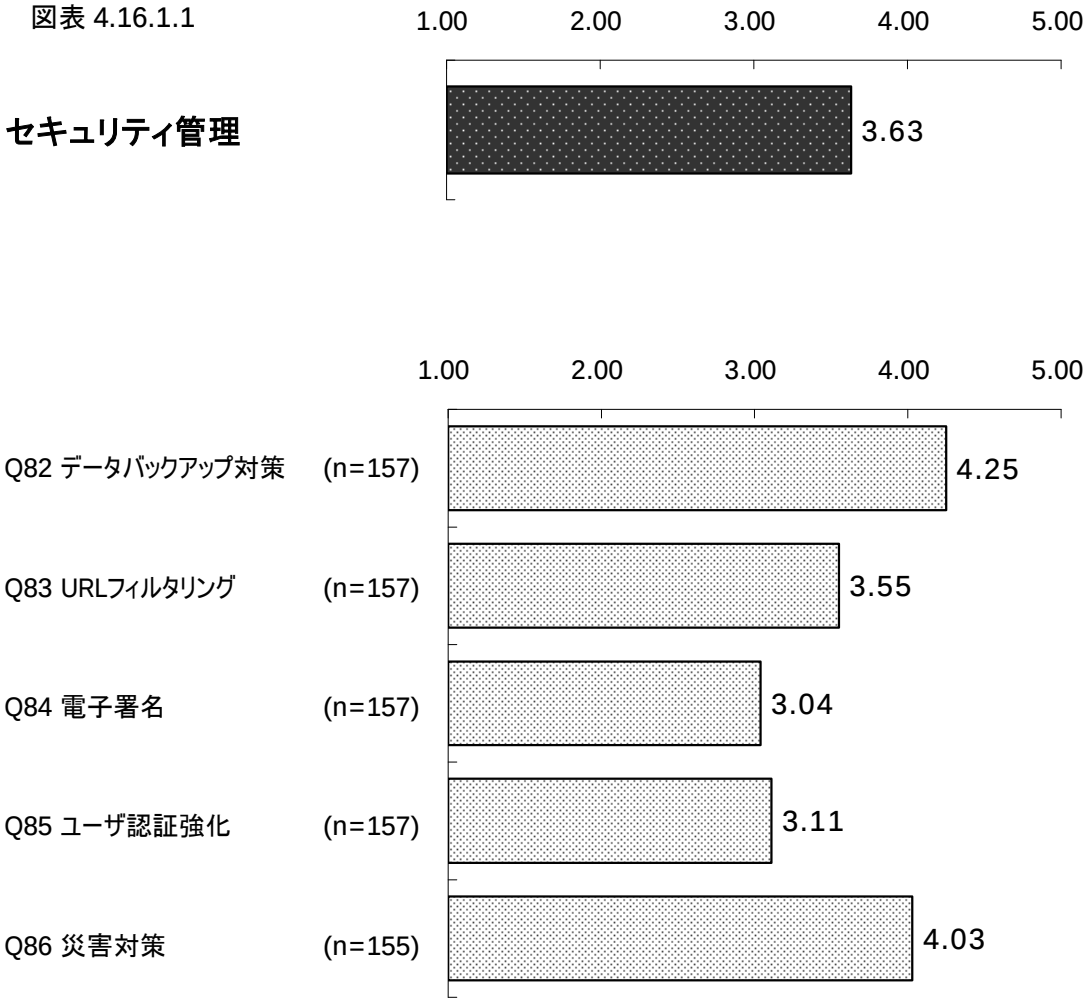


4.16 セキュリティ管理

4.16.1 セキュリティ管理

- セキュリティ管理については、全体で 3.63 点となり、セキュリティ管理に含まれる項目の得点を見ると、『データバックアップ対策』が最も高く 4.25 点となっている。
- 逆に最も低くなっているのが『電子署名』で 3.04 点である。

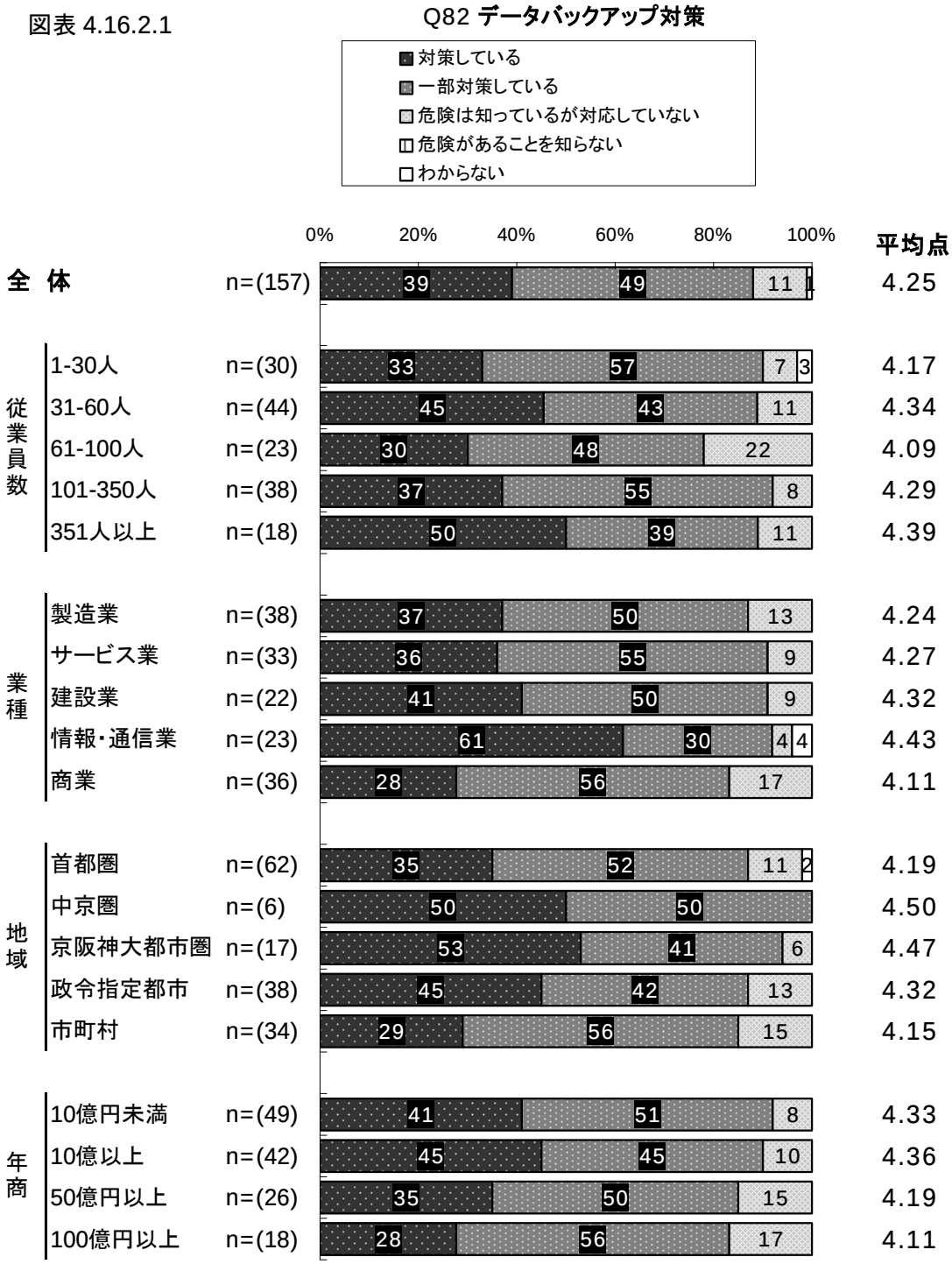
図表 4.16.1.1



4.16.2 セキュリティ管理 −Q82 データバックアップ対策

- 全体では 4.25 点となり、『対応している』は 39%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 4.39 点となっている。また、「1～30 人」以外の全ての規模において、『危険があることを知らない』『わからない』というネガティブな回答が見られない。
- 業種別に見ると、「情報・通信業」で最も点数が高く 4.43 点となり、他の業種と比較して『対策している』の割合が高く 61%となっている。

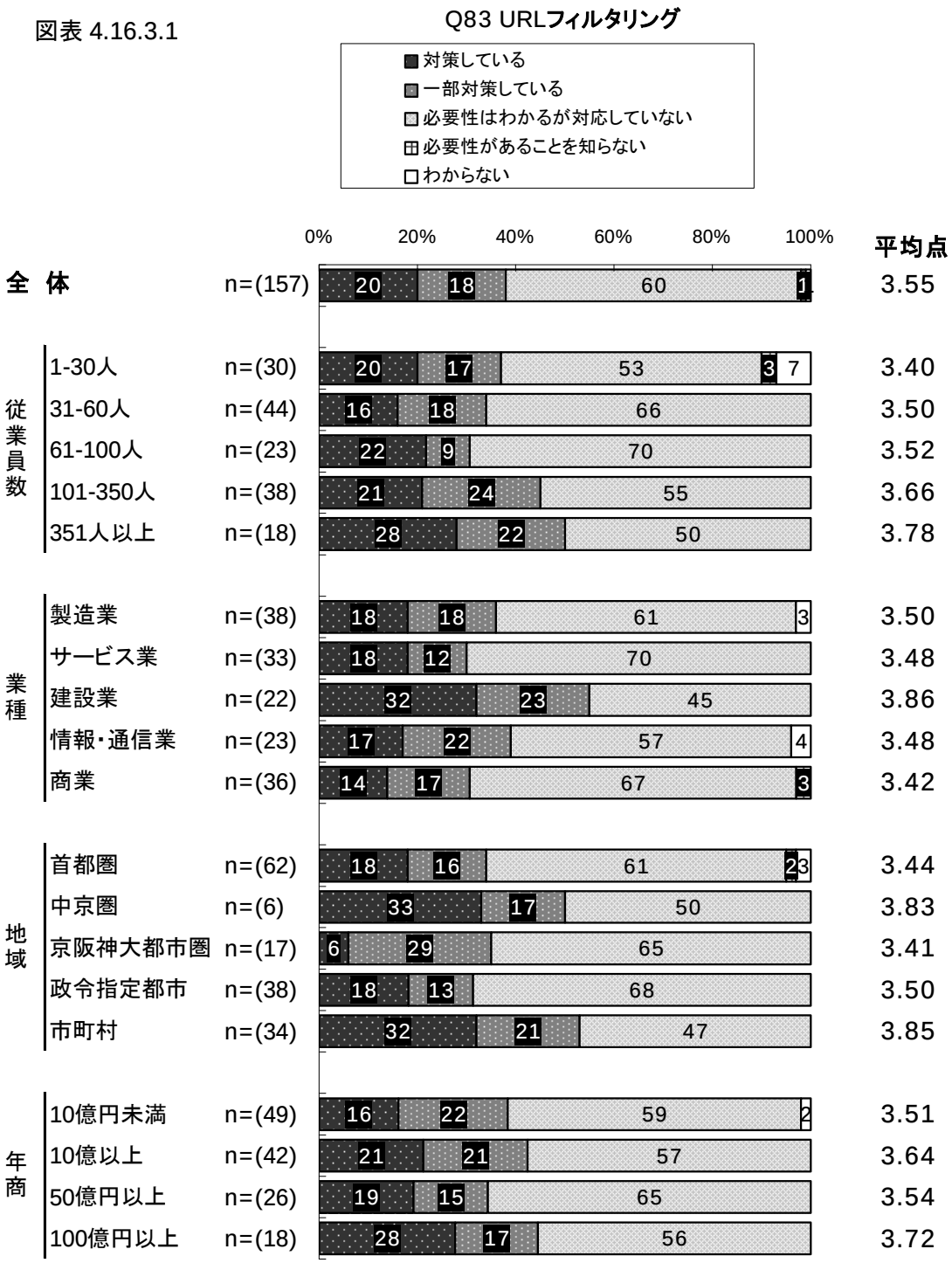
図表 4.16.2.1



4.16.3 セキュリティ管理 −Q83 URL フィルタリング

- 全体では 3.55 点となり、『対策している』は 20%となっている。
- 従業員規模別に見ると、規模が大きくなるにつれて点数が高くなり、「351 人以上」で最も点数が高く 3.78 点となっている。
- 業種別に見ると、「建設業」で最も点数が高く 3.86 点となっており、他の業種と比較して『対策している』『一部対策している』というポジティブな回答の割合も高い。

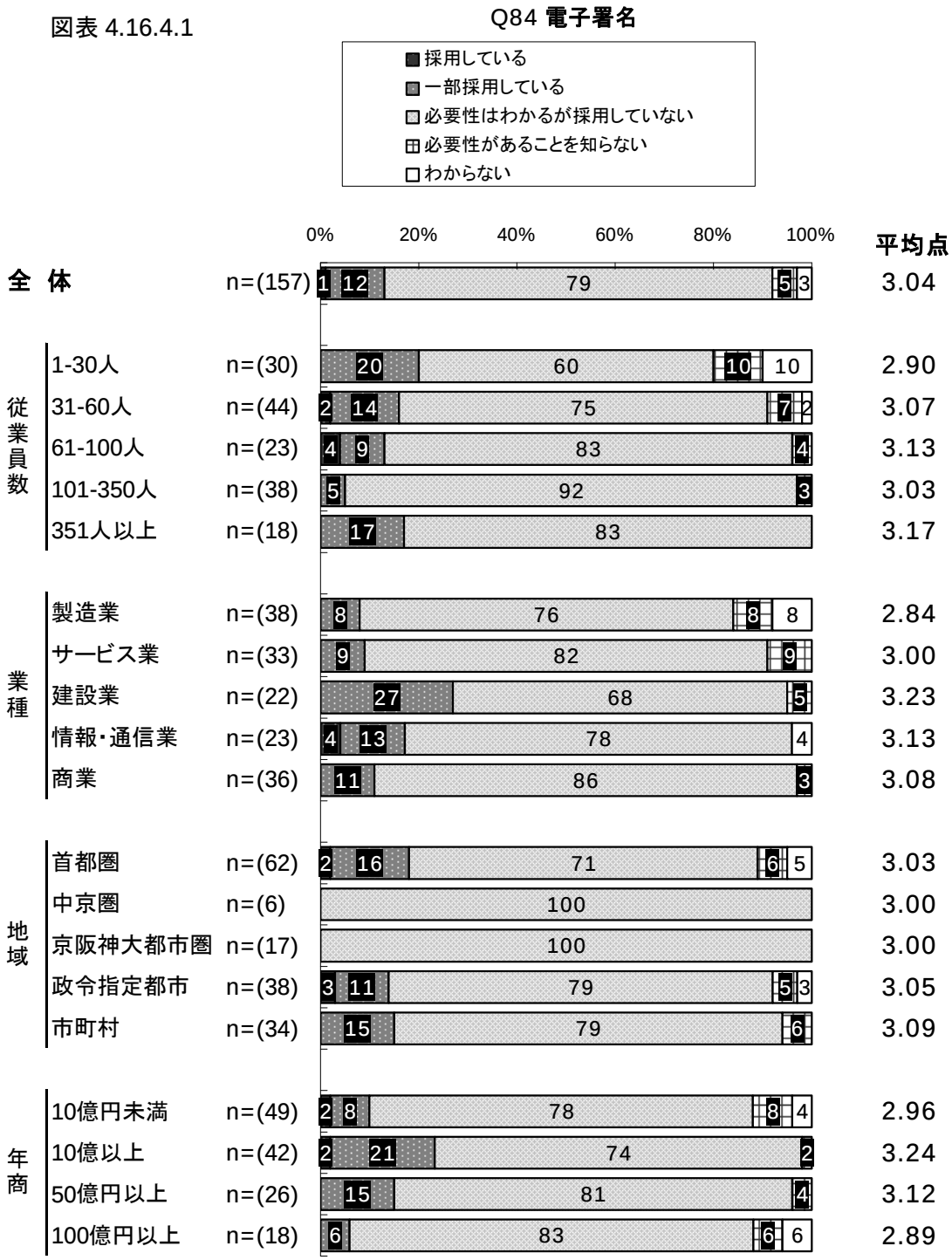
図表 4.16.3.1



4.16.4 セキュリティ管理 −Q84 電子署名

- 全体では 3.04 点となり、『採用している』は 1%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 3.17 点となっている。また、1～350 人の間では、規模が大きくなるにつれて『採用している』『一部採用している』というポジティブな回答と『必要性があることを知らない』『わからない』というネガティブな回答の両方がハの字型に減少している。
- 業種別に見ると、「建設業」で最も点数が高く 3.23 点となっている。

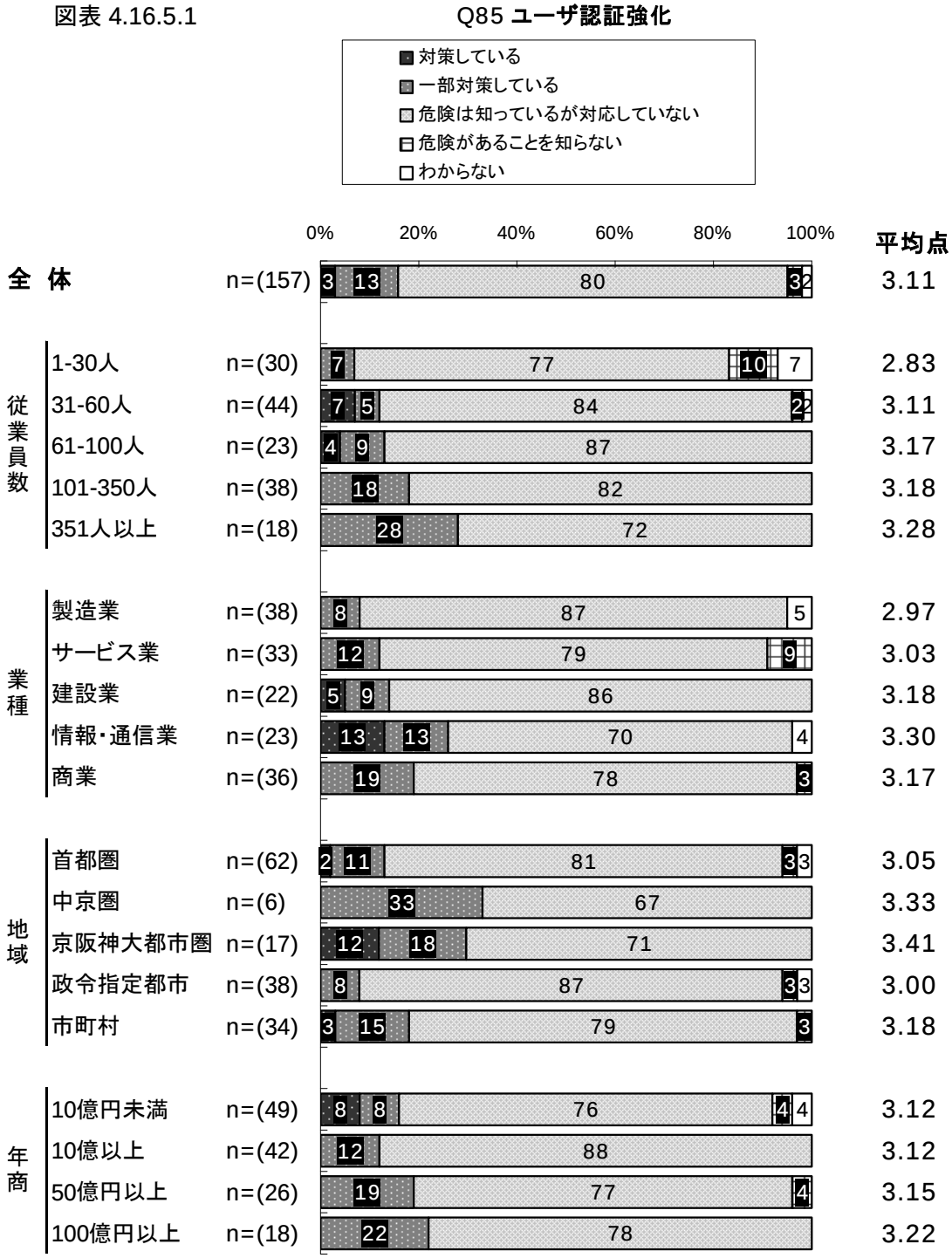
図表 4.16.4.1



4.16.5 セキュリティ管理 −Q85 ユーザ認証強化

- 全体では 3.11 点となり、『対策している』は 3%となっている。
- 従業員規模別に見ると、規模が大きくなるにつれて点数が高くなり、「351 人以上」で最も高く 3.28 点となっている。また、『対策している』『一部対策している』というポジティブな回答は、規模が大きくなるにつれて増加する。
- 業種別に見ると、「情報・通信業」で最も点数が高く 3.30 点となっている。

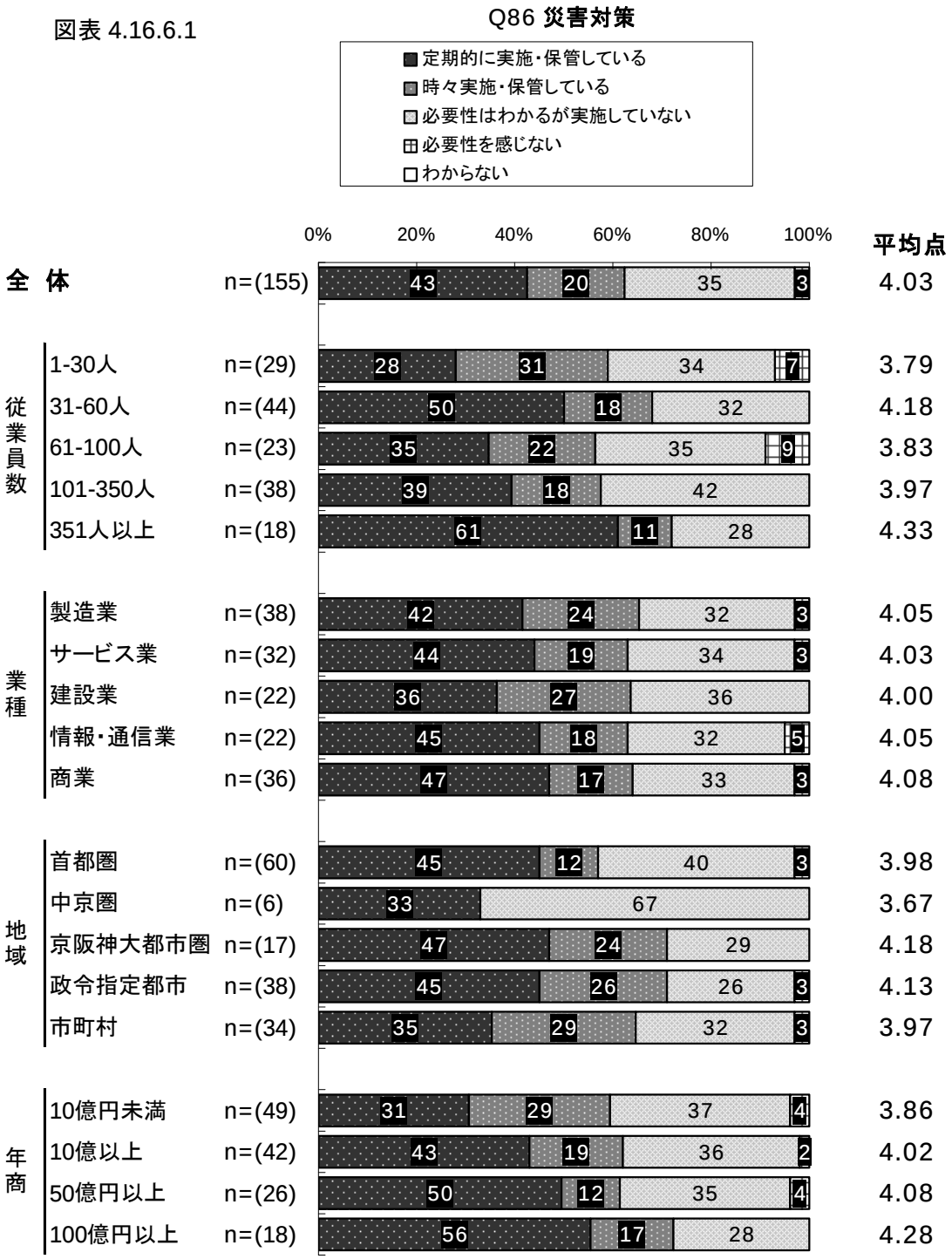
図表 4.16.5.1 Q85 ユーザ認証強化



4.16.6 セキュリティ管理 −Q86 災害対策

- 全体では 4.03 点となり、『定期的に実施・保管している』は 43%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 4.33 点となっている。
- 業種別に見ると、「商業」で最も点数が高く 4.08 点となっているが、業種間で比較すると値に大きな差は見られない。

図表 4.16.6.1

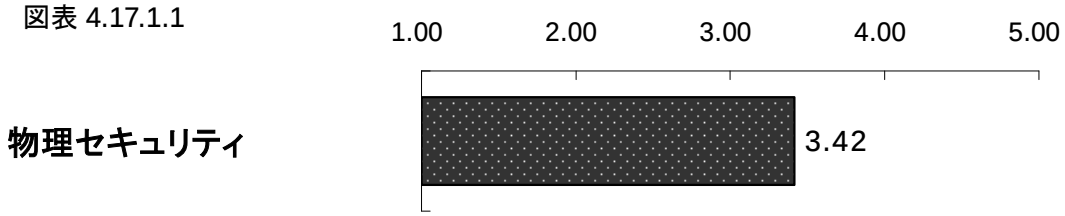


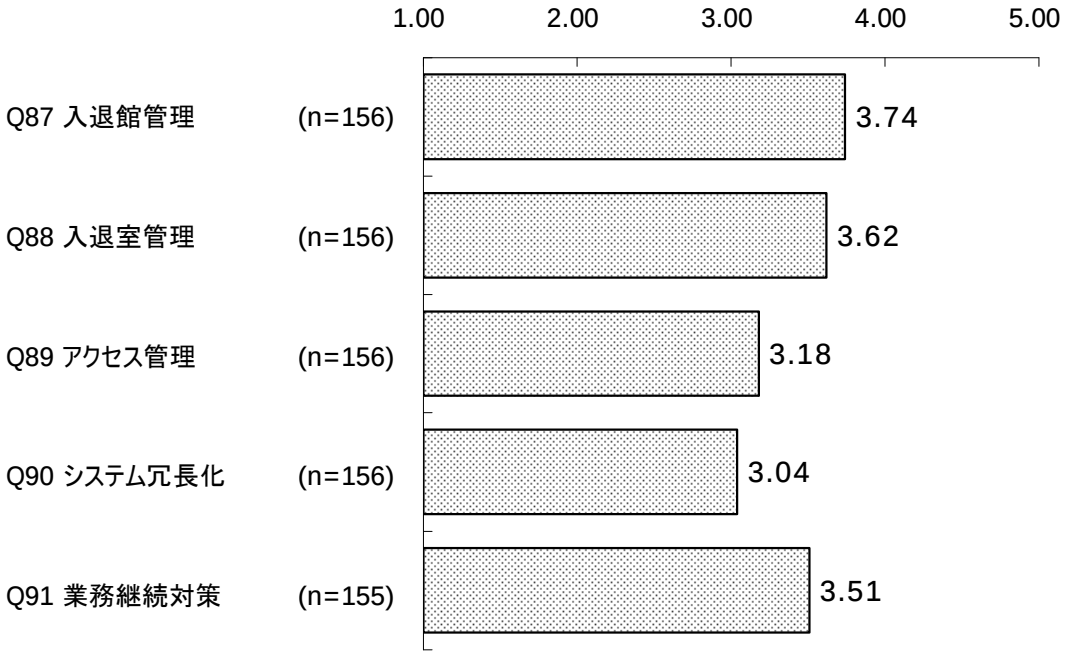
4.17 物理セキュリティ

4.17.1 物理セキュリティ

- 物理セキュリティについては、全体で 3.42 点となり、物理セキュリティに含まれる項目の得点を見ると、『入退館管理』が最も高く 3.74 点となっている。
- 逆に最も低くなっているのが『システム冗長化』で 3.04 点である。

図表 4.17.1.1

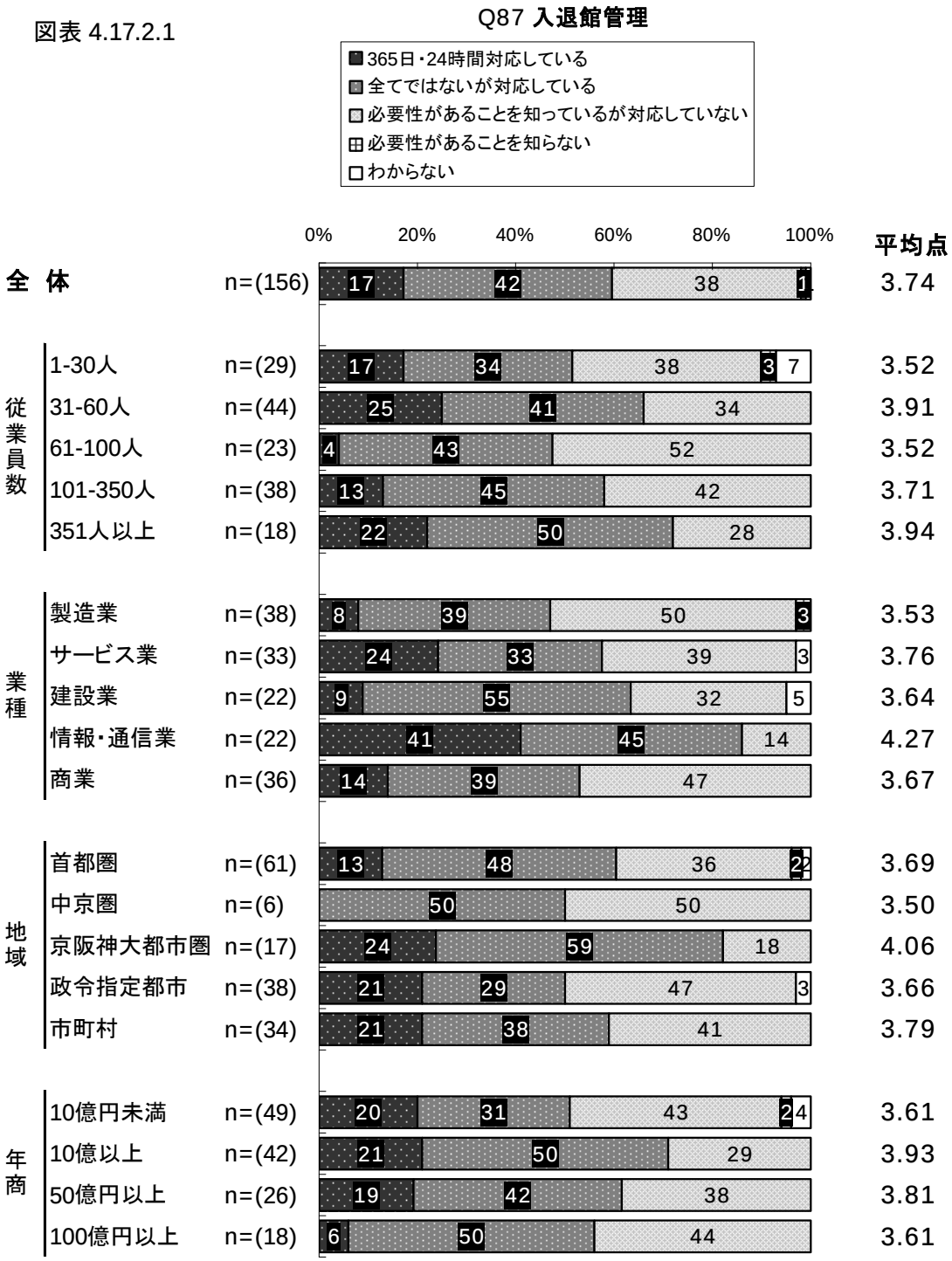




4.17.2 物理セキュリティ –Q87 入退館管理

- 全体では 3.74 点となり、『365 日・24 時間対応している』は 17%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 3.94 点となっている。「351 人以上」と「31～60 人」で点数の値に差が小さく、構成比も類似している。
- 業種別に見ると、「情報・通信業」で最も点数が高く 4.27 点となっており、他の業種と比較して点数が非常に高い。

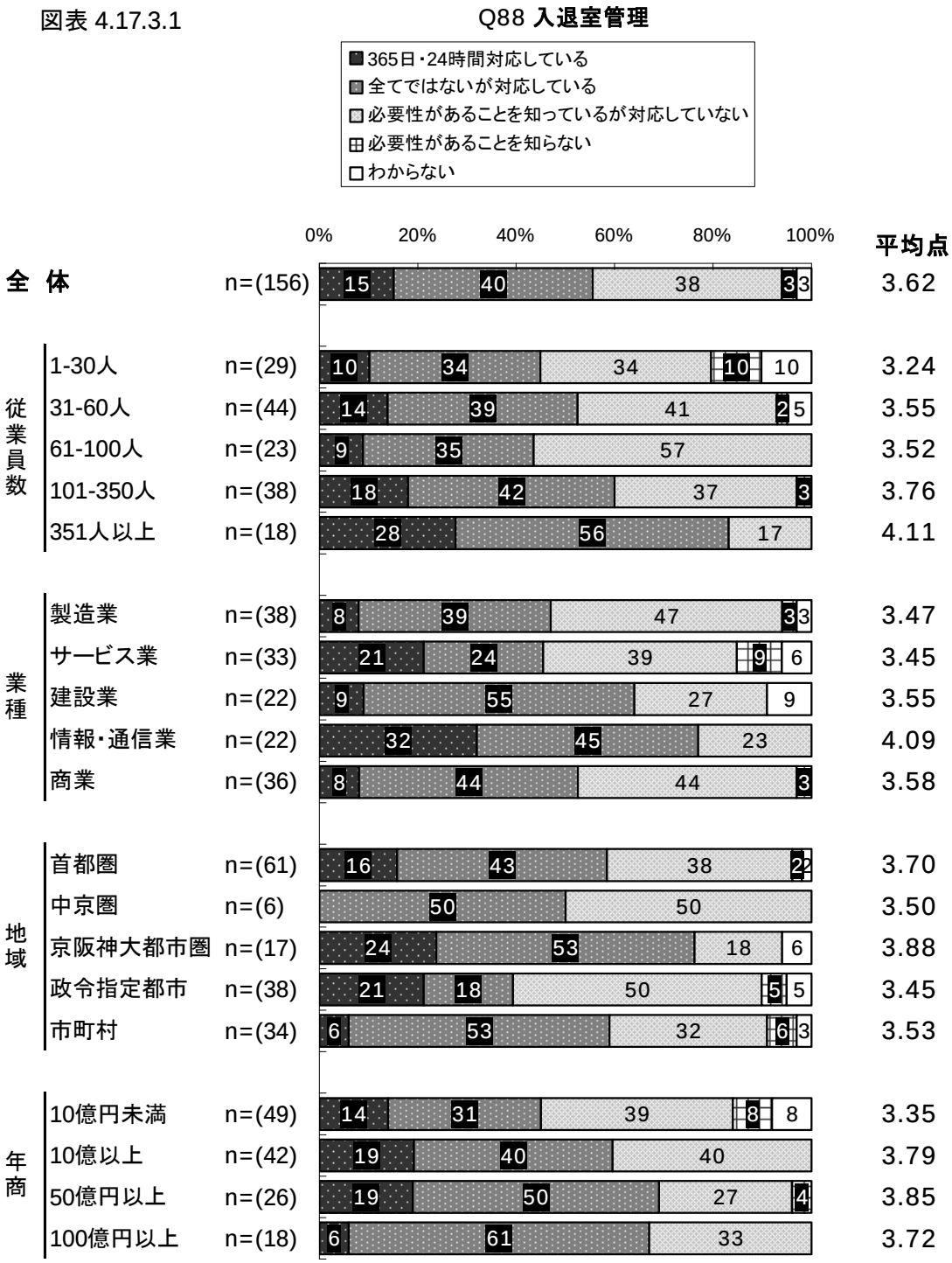
図表 4.17.2.1



4.17.3 物理セキュリティ −Q88 入退室管理

- 全体では 3.62 点となり、『365 日・24 時間対応している』は 15%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 4.11 点となっている。
- 業種別に見ると、「情報・通信業」で最も点数が高く 4.09 点となっており、他の業種と比較して非常に高い。

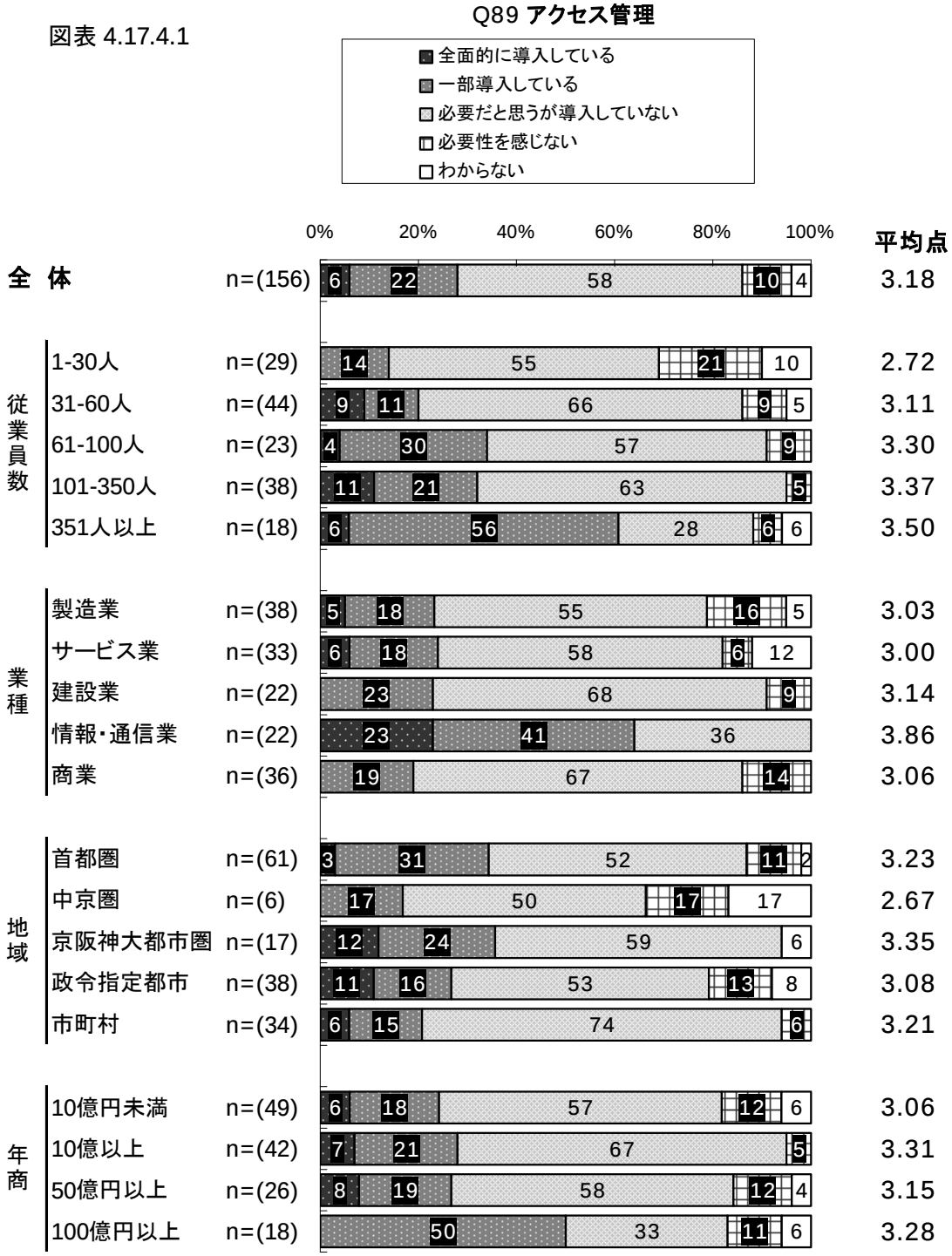
図表 4.17.3.1



4.17.4 物理セキュリティ −Q89 アクセス管理

- 全体では 3.18 点となっており、『全面的に導入している』は 6%となっている。
- 従業員規模別に見ると、規模が大きくなるにつれ点数が高くなり「351 人以上」で最も点数が高く 3.50 点となっている。また、同規模において『全面的に導入している』『一部導入している』というポジティブな回答の割合は他の規模と比較して高い。
- 業種別に見ると、「情報・通信業」において点数が最も高く 3.86 点となっており、他の業種と比較して『全面的に導入している』『一部導入している』というポジティブな回答の割合も非常に高い。

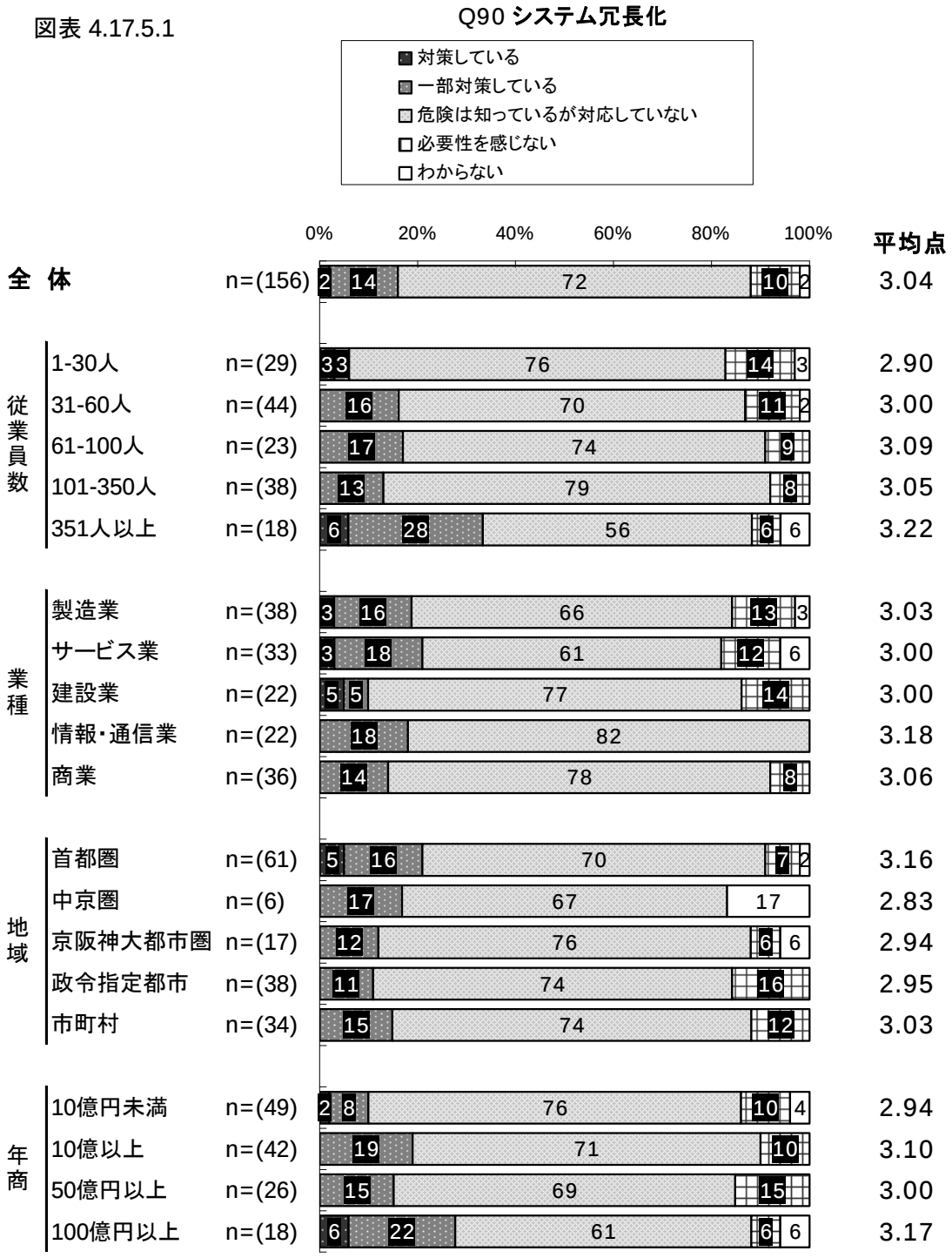
図表 4.17.4.1



4.17.5 物理セキュリティ –Q90 システム冗長化

- 全体では 3.04 点となり、『対策している』は 2%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 3.22 点となっている。また、『必要性を感じない』『わからない』というネガティブな回答の割合は 1 ～350 人規模の間では、規模が大きくなるにつれ減少するが、「351 人以上」で増加している。
- 業種別に見ると、「情報・通信業」が最も高く 3.18 点となっている。他の業種はいずれも 3 点程度と値に大きな差は見られない。

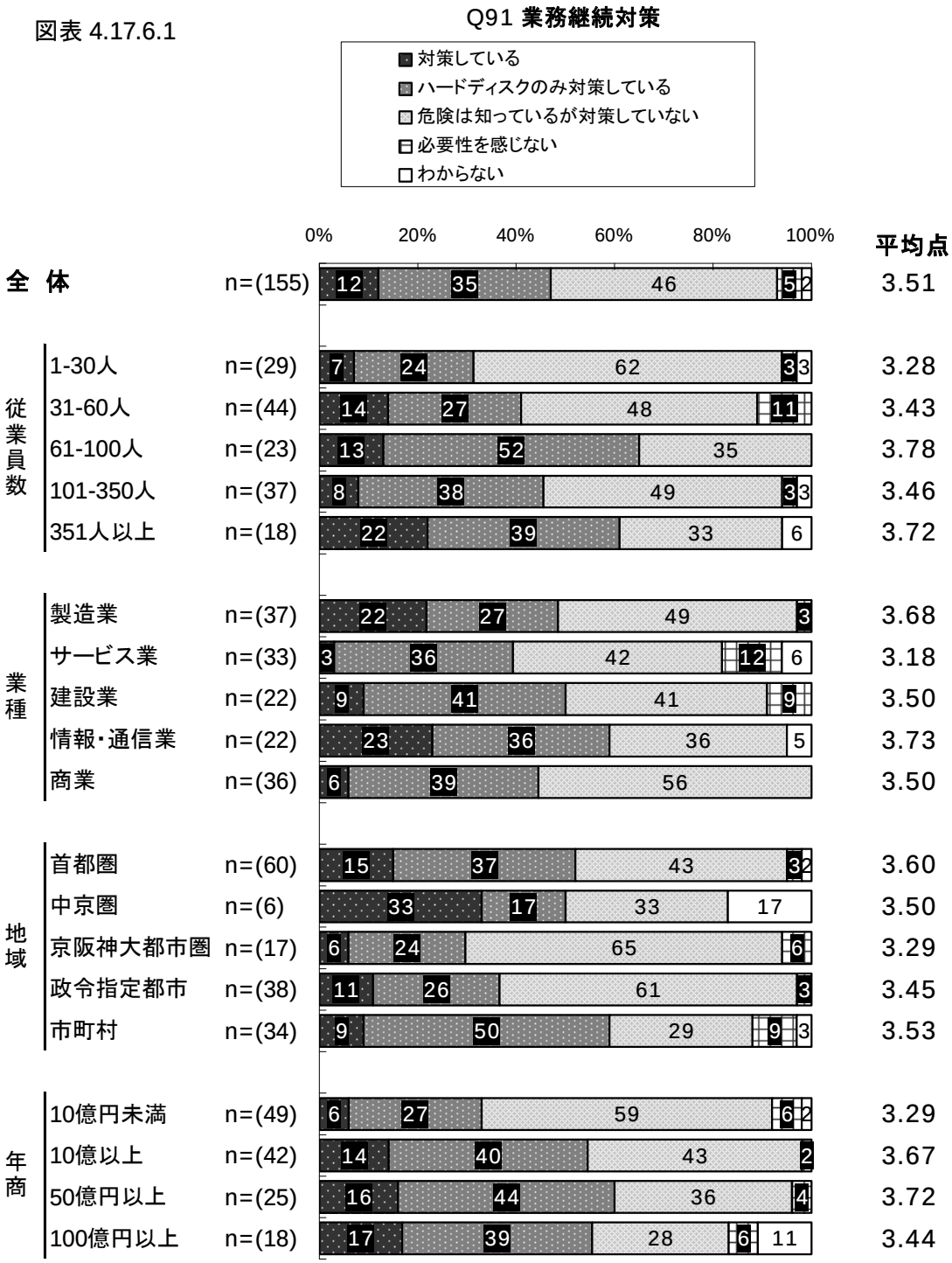
図表 4.17.5.1



4.17.6 物理セキュリティ −Q91 業務継続対策

- 全体では 3.51 点となり、『対策している』は 12%となっている。
- 従業員規模別に見ると、「61～100 人」で最も点数が高く 3.78 点となっている。また、同規模においては『対策している』『ハードディスクのみ対策している』というネガティブな回答が見られなかった。
- 業種別に見ると、「情報・通信業」で最も点数が高く 3.73 点となっている。

図表 4.17.6.1

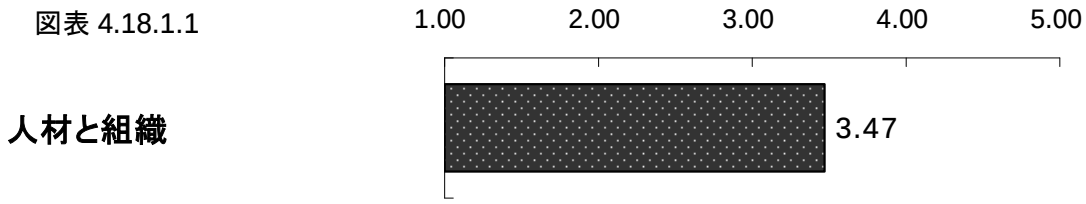


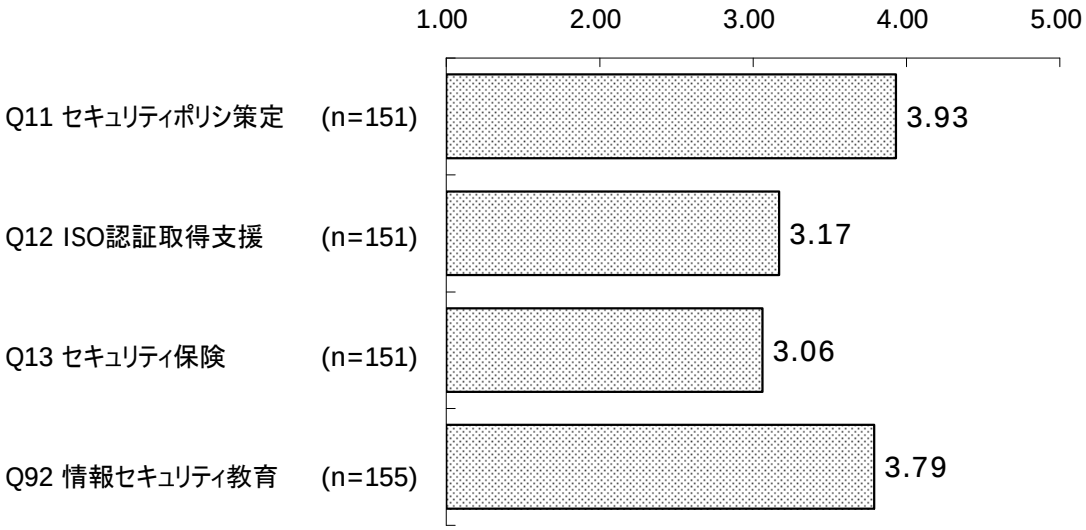
4.18 人材と組織

4.18.1 人材と組織

・ 組織については、全体で 3.47 点となり、組織に含まれる項目の得点を見ると、『セキュリティポリシ策定』が最も高く 3.93 点となっている。
・ 逆に最も低くなっているのが『セキュリティ保険』で 3.06 点である。

図表 4.18.1.1



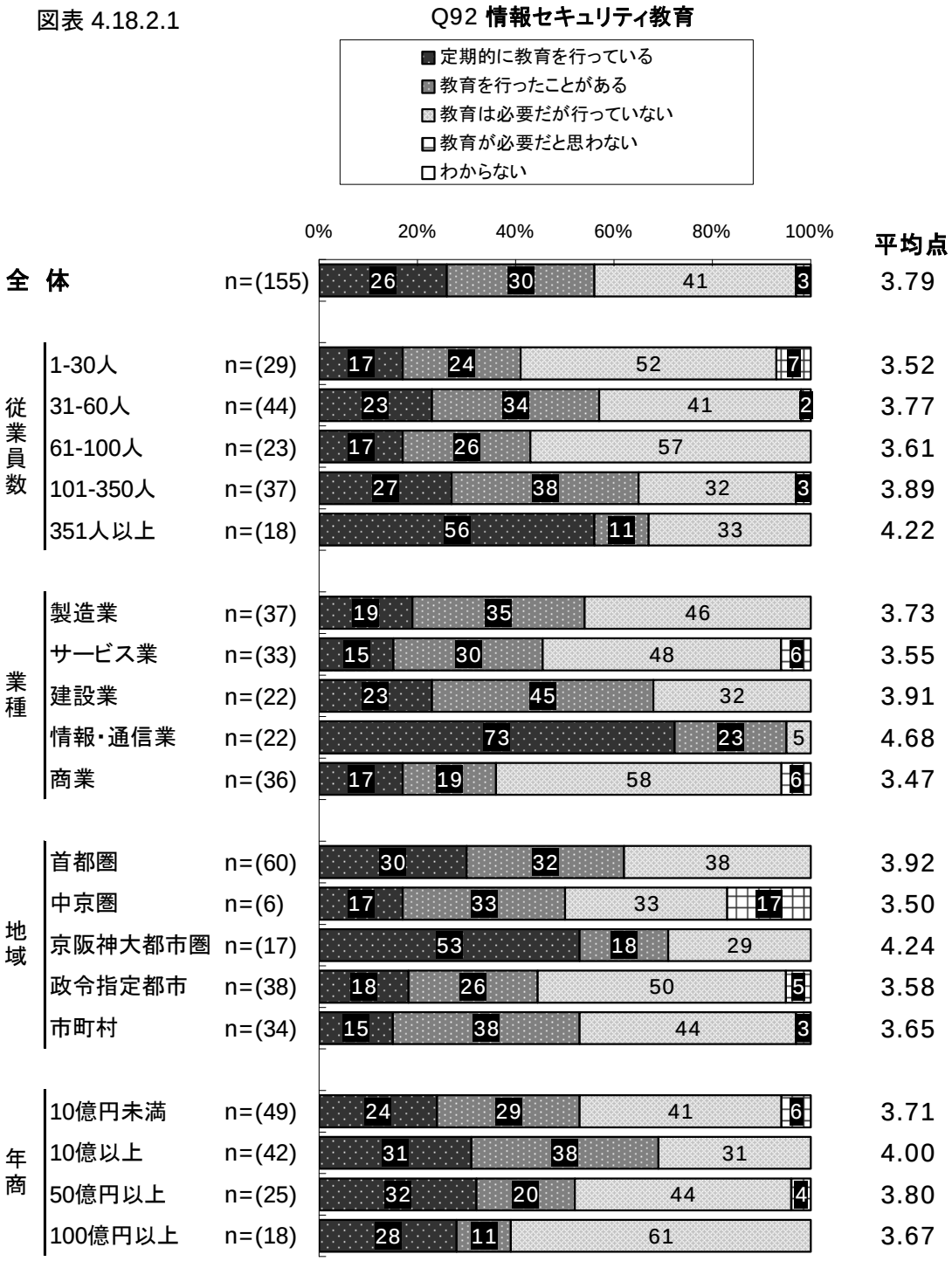


※ Q11-13 のグラフは前述のため、省略しております。

4.18.2 人材と組織 −Q92 情報セキュリティ教育

- 全体では 3.79 点となり、『定期的に教育を行っている』は 26%となっている。
- 従業員規模別に見ると、「351 人以上」で最も点数が高く 4.22 点となっており、他の規模と比較して『定期的に教育を行っている』の割合が非常に高い。
- 業種別に見ると、「情報・通信事業」で点数が最も高く 4.68 点となっており、他の業種と比較して『定期的に教育を行っている』の割合が非常に高い。

図表 4.18.2.1

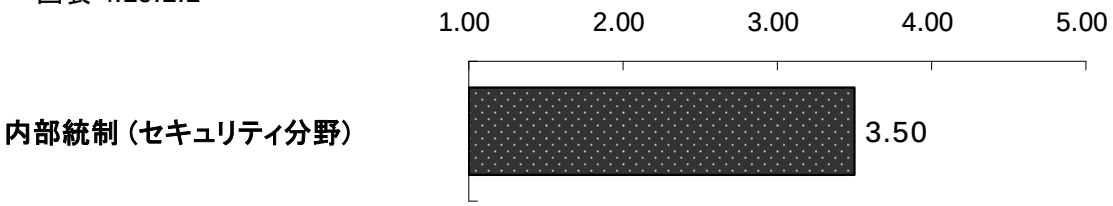


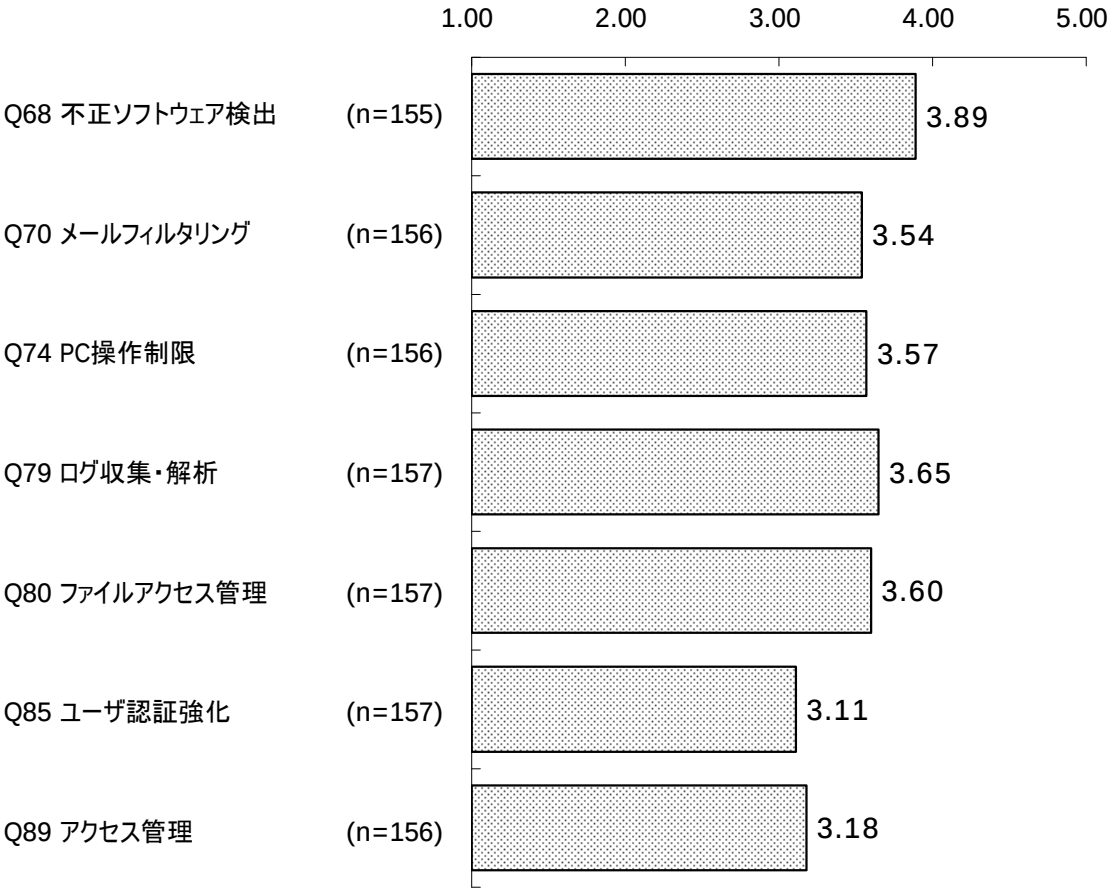
4.19 内部統制（セキュリティ分野）

4.19.1 内部統制（セキュリティ分野）

- 内部統制(セキュリティ分野)については、平均で 3.50 点となっている。内部統制に含まれる項目の得点を見ると、『不正ソフトウェア検出』が最も高く 3.89 点となっている。
- 逆に最も低くなっているのが『ユーザ認証強化』で 3.11 点である。

図表 4.19.1.1





※ 設問ごとのグラフは前述のため省略しております。

付録　−企業経営者の方々にご配慮いただきたい課題−

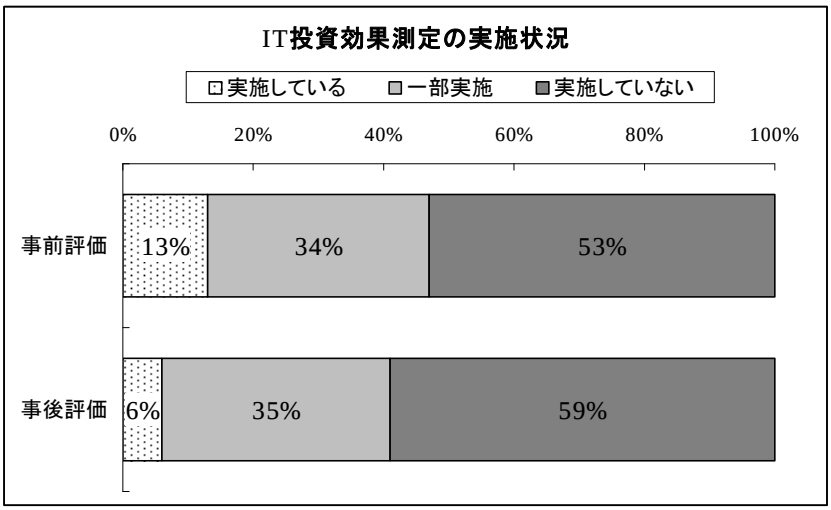
企業経営者の方々にご配慮いただきたい課題

■ IT システムの導入の成果はその後どうなっていますか?

企業経営者にとっては、投資の経営上の効果に関心を持つことは当然のことです。IT システムの導入は投資の一種です。しかも年々その規模は拡大しています。しかし、設備投資などのほかの投資と比べて、経営者のシステム投資の効果に対する関心が低いように思われます。(このことは、次に示す(資料 1)～(資料 4)にその兆候が見られます)

その理由は、投資と効果の関係が複雑なので、徹底的に追求することが困難であるということではないかと思われます。そこで、システム投資とその経営上の効果との関係を少し整理してみます

(資料 1)



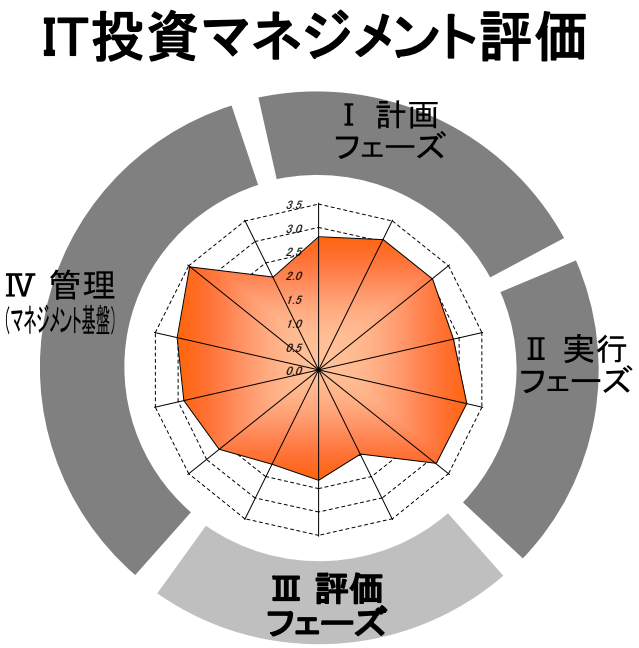
出典:ユーザ企業 IT 動向調査(社団法人日本情報システム・ユーザー協会)

実際に、投資効果測定の実施状況を見てみますと、事前評価は、「実施している」と回答した企業が 13%、一部実施が 34%で、両者をあわせて 47%と、半数に届かない状況であり、事後評価については、「実施している」企業はわずか 6%、「一部実施」とあわせても 41%である。

どちらについても不十分な状態と言わざるを得ない状況と言えます。

しかし、何から手をつけて良いか分からないということも、事実ではありますが、経営に対する貢献度を測る手法を用いることで、明確にしていくことが可能となります。

(資料 2)



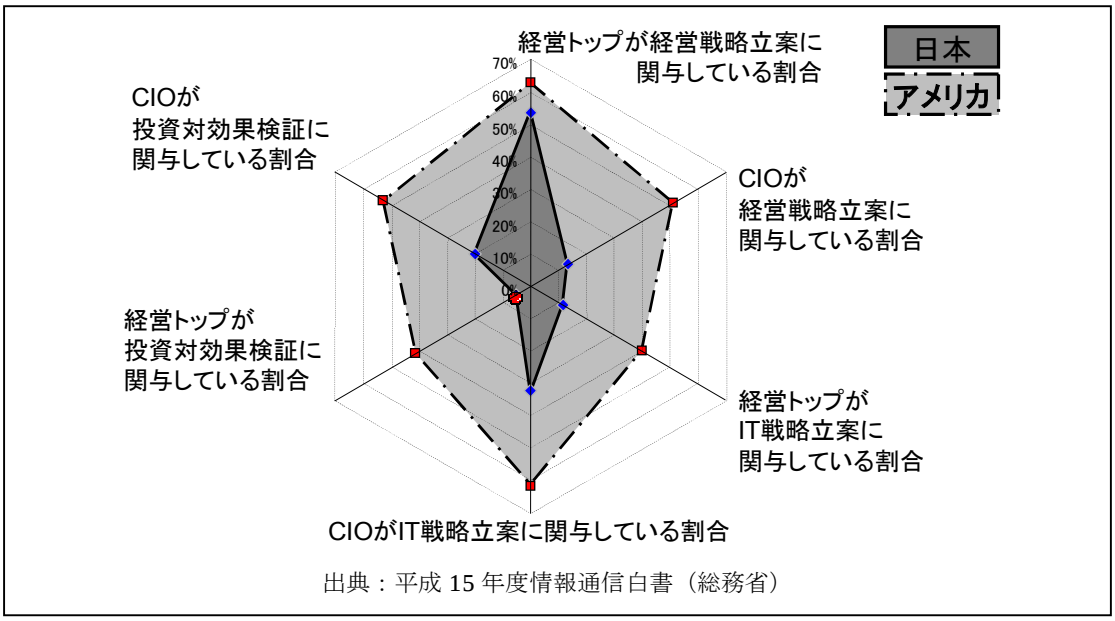
出典:富士通 LS 研資料 (161 社回答)

ここで情報化調査の一例を見てみます。調査によると計画と評価の部分でウィーク・ポイントが見られます。

経営トップ層によるビジョンの設定、情報化投資の成果評価、成果の説明責任の明確化、戦略を反映した評価の実施、こうしたフェーズに、まだまだ不十分さがあると認識されております。

また、平成 15 年度の情報通信白書を見てみますと、日米経営陣の情報戦略への関与の状況で、これだけの開きがあることがわかっております。

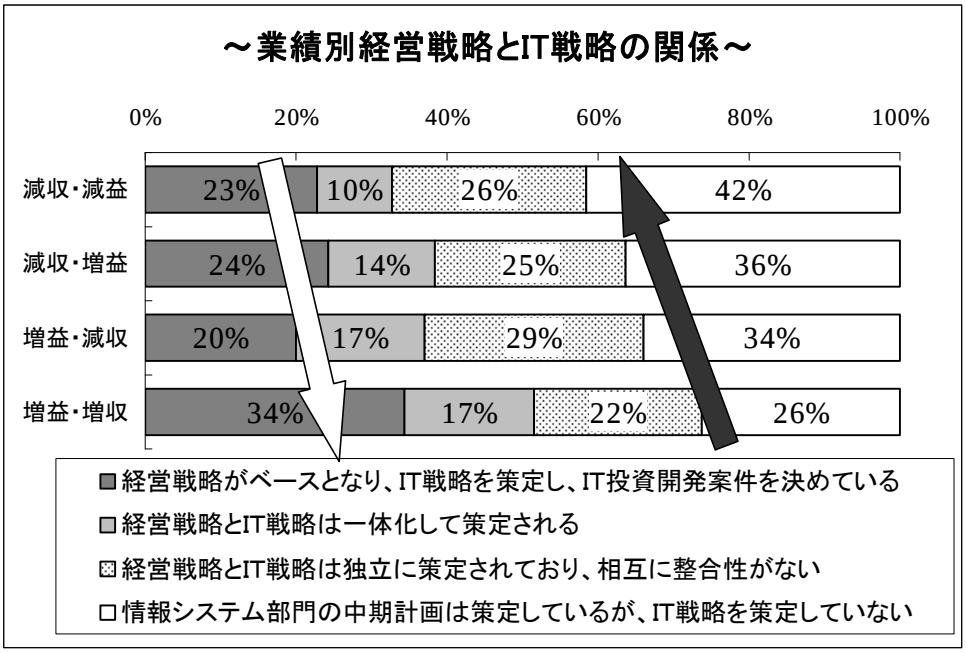
(資料 3)



出典：平成 15 年度情報通信白書（総務省）

同様に、日本情報システム・ユーザー協会のユーザ企業 IT 動向調査　2004 を見てみますと、明らかに、IT 戦略に関するガバナンスが強い企業が増収増益の、弱い企業が減収減益の、業績を示しています。

(資料 4)



出典：ユーザ企業 IT 動向調査（社団法人日本情報システム・ユーザー協会）

■ IT システムの運用が効果を生む決め手である

経営者は応分の効果を期待してシステム投資を決心しますので、その時点でどんな効果（たとえば、取引の状況や売上げの実態が速く、正確に分かり、資金や負債なども実態が把握できること）を狙うかを決めます。その後、その効果を実現できるように詳細な設計をし、その設計に基づいて効果が実現するよう具体的に構築していきますので、できあがれば当然狙った効果があがる筈ですが、現実には必ずしも狙った効果があがっているわけではありません。

〔運用費用の比率は開発費用よりも高い〕という事実

経済産業省と社団法人日本情報システム・ユーザー協会は、ユーザ企業の IT 予算実額を保守・運用費と新規投資に分けて調査している。その結果は下表の通りである。

＜1 企業当りの保守運用費と新規投資＞

	保守・運用費	新規投資
2005 年度実績	1,030 百万円	489 百万円
2006 年度計画	1,050 百万円	606 百万円
2007 年度予測	1,055 百万円	630 百万円

（企業 IT 動向調査 2007 報告書：経済産業省 社団法人日本情報システム・ユーザー協会）

＜この調査の対象企業数は、805 社であり、企業規模は、売上高 100 億円以上の企業の割合が約 80%である。＞

企業規模により状況は異なるとは思いますが、この調査結果を見れば、経営者がシステム運用に対して関心を持つべきであることは納得できるのではないかと思います。システム運用の経営上の意味合いは、システム運用を通してシステム投資で狙った経営上の効果を実現し貢献することですから、経営者が関心を持っていることを示すことで、より貢献するようになるのではないかと思われます。

設計や構築の段階は、一定の限られた期間に行われる作業ですので、経営者は関心を持続させることができますが、運用という作業（一例をあげれば、営業部署のA氏が、営業担当の上司承認の伝票メモが来た段階で、随時操作手順に基づき情報を入力し、再度入力情報の上司承認を取り売上げ計上を行ない、商品の確保を行なった後配送部署に出荷指示を行なうというような全体の流れと取り決め）はその IT システムを使っている限り継続しますので、運用への関心を継続しなければなりません。そして、運用という作業には、いわゆるユーザ部門を含めて社内外の関係者が設計や構築の段階に比べて多数であるという特質があるので、目配りの広さも要求されます。

このような事情が存在しますが、経営者は IT システムの効果を追及するのであれば、IT システムの効果は上手に使ってはじめて実現するということは事実ですから、IT システムの運用に関心を持つべきであるということも事実であります。

■ 運用段階にはたくさんの効果実現を阻害する原因がある

狙った効果があがらない原因にはどんなことがあるのでしょうか。きっと、切りがない程のたくさんのことが挙げられるのではないかと思われます。設計や構築の段階にもたくさんの原因があり、それらは運用の段階で発見され、修正や改善が要求されることになります。また保守や運用に掛かる費用は約 80%の利用者が対前年度比増加もしくは同等としており、削減がままならないのが事実です。

運用の段階にもたくさん原因があると思われます。運用の関係者はいわゆるユーザ部門も含めて多数にのぼりますし、その関係者の作業への取組そのものが何らかの形で効果の実現に関わるわけですから、関係者の理解力や集中力などの人間力に関する原因も存在することが考えられます。いずれに

せよ、効果の実現のためには運用段階に注目する必要があるといえます。

■ 運用段階の問題解決には組織的対処が必要

導入した IT システムの運用が順調でないという状況の典型的なものは、IT システム障害が多発するという状況です。

先ずは、ベンダからみれば好ましくないことですが、担当者のパソコンやサーバの故障、ネットワークやソフトウェアの不調による応答の遅延が挙げられます。更には関連 IT システムとのデータの連結の不具合等による IT システム障害があります。そしてユーザ側には、手順に基づかない使い方やエラーメッセージに対する意図しない不適切な操作、加えてオペレーションミス、入力ミス、転記や起票ミス等、人の行為に起因する IT システム障害もあります。また設置場所の環境による障害もそのひとつに挙げられます。

いわゆる何が起り得るか分からない中で障害を起こさずに、IT システムの稼働率を確保するためには、これらの現象からの速やかな回復とともに、それらの原因を除去することが必要です。

したがって、これらの現象が発生した場合の社外も含めた組織的な対処方法を日ごろから準備しておかなければ、IT システムの高稼働率を確保できません。そして経営上の効果を実現できないことになります。

またこれも運用上の問題点のひとつですが、IT システムが対象とするデータの時間・期間的な範囲の問題があります。

IT システムが狙った効果をあげる前提として、当然すべての対象データが適切に取り扱われることになっていると思われますが、往々にしてデータ入力や関連 IT システムからのデータの取り込みが遅れて対象データの一部が欠落するようなことがあります。これらのことへの対処も、部門間連携や教育訓練などの組織的な対処が必要です。

■ 組織的対処とはなにか

ここでいう組織的対処とは簡単にいえば、「社内の IT システム部門（社外のシステム・サポート・サービス・ベンダを含めて考えた方が現実的です）とユーザ部門との間の具体的な約束ごと」を明確にすることです。（当然、社外ベンダには技術料を含めて対価を支払う前提です）

より具体的にいえば、それぞれの部門が IT システムの経営上の効果に責任を負う役割と分担作業の連携方法を、組織の運営マニュアルや個々人のオペレーションマニュアルを文書化することです。ユーザ部門としても人事異動等での部署換えや、退職/新人採用等での担当替えでの処理の停滞や、オペレーションミス等の防止に対する約束の明確化も重要です。

運用段階に発生する事象が設計・構築段階へフィードバックされて、人の介在によるミスの最小限化と自動化の拡大等への IT システム改善がされるのですから、この約束ごとの範囲にはすべての段階の業務が含まれなければなりません。

これらの業務を対象として、約束ごとのモデルを含めてレベルアップのためのフレームワークが国際的な機関から示されています。それは、ITIL（IT インフラストラクチャ・ライブラリ）というものですが、ここではその詳細には触れませんが、ITIL には、「IT を活用して業務遂行を援助する方法論を体系化したもの」と記されていますが、簡潔にいうと、IT 活用での業務の進め方やレベル等を体系化し文書化したもので、レベルに基づく業務遂行能力の有無を審査する機関も存在しています。

また、前述の「社内の IT システム部門（社外のシステム・サポート・サービス・ベンダを含めて

考えた方が現実的です)とユーザ部門との間の具体的な約束ごと」を SLA（Service Level Agreement）として取り決める方法もあります。これらの約束ごとの取り決めは投資した IT システムの経営上の効果に結びついていることですので、是非とも経営者がこれらに関心を持って積極的に関与していただきたいと思います。

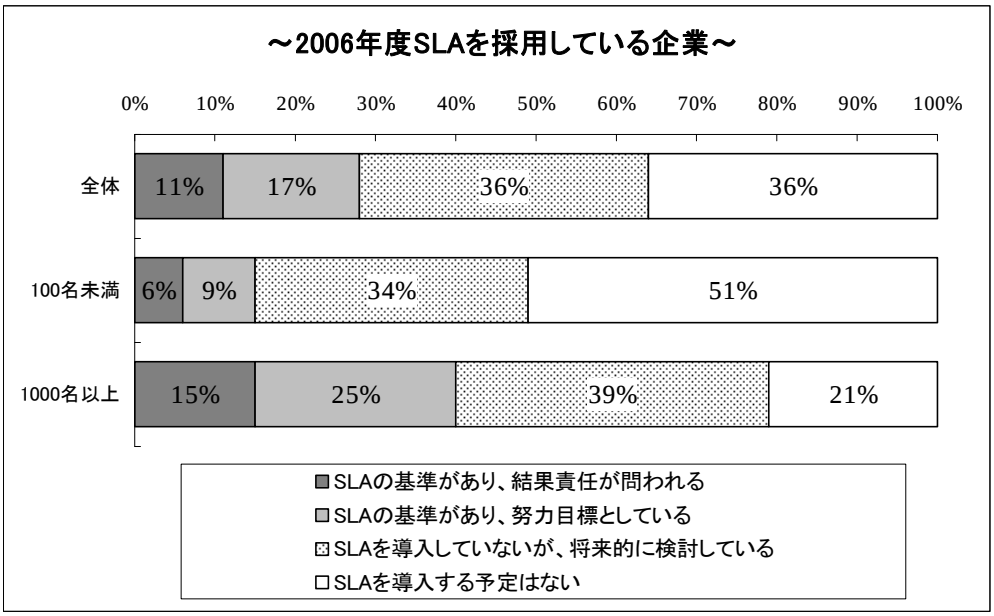
■ 運用のアウトソーシング化の進め方

保守・運用コストの削減への取組みの一つの方向としてアウトソーシングが考えられます。企業にとって IT は本業を効率化するための道具ですから何をどうしたいかを IT の専門ベンダにお願いするのも企業として人材面から効果があるでしょう。しかしアウトソーシングをする際には是非心掛けていただきたい点がいくつかあります。特に次の 3 点には意識を置いていただきたいと思います。

- お客様とサービスベンダーのなすべき行動･責任(SLA)を明確にすること
- 結果を可視化し、投資効果・経営上の評価に結びつけること
- サービスベンダーに常に IT システムの改善提案のコンサルを依頼し IT システムのライフサイクルを継続的に向上させること

企業の SLA に対する取組の状況を次の（資料 5）が示しています。

(資料 5)



出典：ユーザ企業 IT 動向調査（社団法人日本情報システム・ユーザー協会）

中小企業では SLA に対する認識がまだまだ低い状況です。

これは自ら運用をやっているがための結果ともいえるが、IT リスクを低くする策の検討は日本版 SOX 法の適用等を考慮するなどの対応をしてゆく必要がある。

■ IT システムの経営上の効果をどのように考えればよいか

IT システムに投資をする決心をする時点では、必ずその効果を見込んで、投資を評価しますが、すべての場合で、その効果を金銭的に定量表現できるとは限らないものです。その理由は、そのシステム投資目的がインフラの整備であるなど、システム投資の性格によることですので、やむをえないことであります。

しかし、その場合にも結果として経営上の効果を狙って投資するのですから、その狙いを何か具体的に表現する工夫が必要です。たとえば、販売管理の導入を一例に考えてみると「IT を導入して売上げ情報を速く正確に掴むという目的のみではなく、得意先や商品の状況や特性を管理し売上げをどれ位伸ばすか?や在庫をどれ位削減するか?等々の目標を指標化して策定し、着実な効果に結び付ける」を投資目標として、売上げの実績や実績向上の因果関係をフォローするなどです。

当然、投資時点で効果が定量的に表現されている場合には、その効果の実現をフォローしますが、その場合にも、投資と効果の因果関係を整理しておかないとフォローが困難になることがあります。その一例を挙げますと、「新しく WEB 販売のための投資をして、年間○○円の売上げ増を狙う」場合は WEB 販売の売上げをフォローすれば十分ですが、「商品カタログを掲載する WEB を新設して、年間○○円の売上げ増を狙う」場合には、売上げのフォローだけではなく、WEB 上の商品カタログへのアクセス量もフォローすることも必要でしょう。

この投資と効果の因果関係を整理してみると、効果の実現の前提条件として運用段階の事柄が大変多く含まれることが理解できると思います。その理由は、前述したとおり、運用段階というのはいろいろな人々が、いろいろな作業を通して IT システムに関わっていることによります。

「経営者が IT システムの経営上の効果に関心を持ち、そして IT システムの運用に強い関心を持っていただく必要がある」という所以はここにあります。

■ IT 化の時代変遷について

話題が変わりますが、IT の周辺では「インターネット」と「セキュリティ」とが最も重要なテーマになっています。これらのテーマに関する情報をまとめてみましたので、ご覧頂きたいと思います。

インターネットの利用は個人、企業内、企業間とますます広がりを見せています。一方で、ネットワークのブロードバンド化や IT の劇的な進展と、活用ニーズとのスパイラル化の加速は、IT 化の範囲を大きく広げて来ております。

これらの、利用が進めば進むほど、万一の障害や、情報漏洩、不正アクセストラブル等が発生すると、業務停止やビジネス停止等に発展する危険性があるばかりでなく、得意先や取引先をも巻き込む形で、多大な被害を与える事になってしまいます。

昨今の時代の変遷の中、企業にとってもユーザーにとっても、安心・安全な IT システム利用の重要性が大きくクローズアップされてきております。

ここで重要になってくるのが、企業にとっての姿勢であります。情報セキュリティに対する考え方（セキュリティポリシ）をしっかり持っている企業は、発生する問題に対して全社が終始一貫した対処を行なうことが出来ます。

◆添付資料

◎経営者が利回できる運用やセキュリティの世の中の標準化状況

・資料－6　インターネット利用状況

・資料－7　基幹業務におけるＩＣＴシステムの導入状況

1. 基幹業務

2. マーケティング・商品開発業務

3. 間接業務

4. 業務領域別ＩＣＴシステムの企業規模別導入状況

・資料－8　企業規模別ＩＣＴマネジメント体制・プロセス整備状況

・資料－9　実質情報化投資の推移

・資料－10　企業の情報セキュリティの被害状況（複数回答）

・資料－11　企業のウイルス・不正アクセス対策

◎問題発生事例

・資料－12　不具合・障害事例

・資料－13　個人情報漏洩事例

・資料－14　不正アクセス事例

付録　−郵送調査アンケート票−

IT業界のサポ―トサービスに関するアンケートのお願い

社団法人日本コンピュータシステム販売店協会　会長　　大塚 裕司
サポートサービス委員会　委員長　　前川 和彦

拝啓

拝啓秋冷の候、貴社ますますご繁栄のこととお慶び申し上げます。平素はひとかたならぬ御愛顧を賜り、厚く御礼申し上げます。

さて、当（社）日本コンピュータシステム販売店協会は、ＩＴ業界の販売店並びにメーカーの 147 社で構成される経済産業省許可の公益法人でございます。

この度は掲題の件で、一方的なお願いをさせて頂きまして誠に申し訳なく深くお詫び申し上げる次第です。

お客様の情報につきましては、お客様への一層のお役立ちを目指すための調査研究という目的で、当協会の会員より入手させて頂くか、当協会が Web 上で検索させて頂き収集いたしました。本内容は協会内部にて厳重なる管理を図り、外部への漏洩のないよう厳守致します。又、本目的以外での情報の活用は一切ないことをお約束致します。

敬具

本アンケートのお願いは以下の通りとさせて頂きました。

●協会会員企業より貴社にお持ちし、再度主旨についてご説明をさせて頂いた上でお願い申し上げます。
●会員企業よりお聞きした企業様に郵送し、同封のお願い文にてお願い申し上げます。
●当協会にて Web 上で検索させて頂いた企業様に郵送し、同封のお願い文にてお願い申し上げます。

この度お送りさせていただきました資料は下記の 3 点となります。

お送りした資料一覧

- アンケート票（本冊子）　1 部
- 返信用封筒　1 部
- 企業経営者の方にご配慮いただきたい課題（参考資料）　1 部

連絡先
社団法人
日本コンピュータシステム販売店協会
〒113-0034
東京都文京区湯島 1-9-4　鴫原ビル 2F
電話　03-5802-3198
FAX　03-5802-0743
山田 勝正
http://www.jcssa.or.jp/

JCSSA

<本件の背景>

本件の目的でございますが、ご承知の通り昨今のＩＴ化の変革は大変目覚ましく、通信のブロードバンド化（大量の情報が早く安く送受信可能）の進展との相乗効果で、大きく活用幅を広げてきております。ひとつは貴社内の業務や、貴社のお客様や取引先との大幅な仕掛け・仕組み改革であり、ひとつはインターネット網を活用したメールやホームページ等での、手軽で迅速な情報の提供・交換・収集等です。そして、これらの中に更なる利便性向上をサポートする、音声統合・画像・動画等が取扱える点や、「いつでも何処でも」で話題を集めている、携帯電話やモバイル端末等の携帯機器の機能と活用者の拡大も、活用幅を広げる要因となっております。これらのＩＴの活用が競争力強化に不可欠となり、今後の更なる急激な進展が、この傾向を助長させていくことは疑いのないところであります。

この通信とＩＴの融合化の進展を阻む天敵が、ウイルス感染、外部への情報漏洩、外部からの情報書き換えや盗難等々であります。又、昨今は人権尊重の観点からの「個人情報保護法」が施行され、ＩＴの幅広い活用の中で、個人情報の漏洩対策が義務付けられ、そして健全な企業のあり方を規定した「新会社法」の施行、更には不正の撲滅を強制し健全なる財務会計遂行を義務付けた「日本版ＳＯＸ法」の制定、これらの企業の不正全般を取り締る「内部統制」体制の確立等が義務付けられ、これらのリスク対策の仕掛け・仕組みの早急な確立が要求されております。

この状況を鑑み、企業において、競争力強化を狙いとしたＩＴ活用の拡大に対し、企業の生命保険とも言うべきリスク対策の強化が求められることになります。このリスク対策はネッワーク社会が拡充されることに伴い、リスク対策を推進するお客様や取引先からも強く要求されることになると思われます。つまり、競争力強化の仕掛け・仕組み作りと、安全・安心の確立が、企業の勝ち残りに不可欠の要素となって来ることは間違いないものと思っております。

<本件の目的>

私共の協会の会員は、以下の事業を遂行する企業で構成されております。

① 店頭での機器販売
② 販売・財務・生産他、企業の基幹業務等、トータルシステム構築のお手伝い
③ ネットワーク環境の整備・構築のお手伝い
④ 運用・保守・セキュリティ対策等の、アウトソーシングを含めたお手伝い
⑤ 人材育成の教育・研修・資格取得等のお手伝い
⑥ その他企業の「困った」を解決する多岐に亘るお手伝い　　等々

この中で、昨今特に注力しているのが④の事業であり、このアンケートはその一環であります。
お手伝いに注力している理由はネットワーク社会が広がり、企業のＩＴ活用幅が拡大する状況下において、取引の仕方や情報の享受の仕方、更には仕事の仕方等が大きく変貌しつつある中で、システムの運用・保守・セキュリティ対策等を一企業の中で万全に遂行することが極めて難しい状況にあるからであります。特にマルチベンダーと言われる、複数のメーカーのハードやソフト関係の組み合わせで構築されているシステムを、企業の方に運用して頂くのは正直なところ無理と言わざるを得ないからです。
一方で、このビジネスは企業にとって最も理解の得難いものであります。何故ならばその効果が判り難いからであります。
しかしながら、ＩＴやネットワーク活用での取引や仕事の進め方の依存率が、高まれば高まるほどこの事業は最も重要な位置付けとなるものであります。極端に考えれば仕掛け・仕組みの障害が、企業の事業継続に支障を与え大きな損失に繋がる可能性が高くなるということです。
そこで協会として、会員の的確なる事業強化を目指すために、この運用・保守・セキュリティ対策等に対し、アンケート調査をさせて頂くことと致しました。趣旨ご理解賜りましてご協力の程よろしくお願い申し上げます。

〈アンケート実施体制について〉

本内容や情報は、お願いの冒頭にも明記致しましたが、協会内部にて厳重なる管理を図り、外部への漏洩のないよう厳守致します。又、本目的以外での情報の活用は一切ないことをお約束致します。

アンケートの回収､及び集計は外部の調査期間であるジーエフケーマーケティングサービスジャパン株式会社(以下 GfK)に委託いたします。従って、ご記入頂きましたアンケートは、同封の返送用封筒にて GfK 宛てに返送賜りますようお願い申し上げます。

また、アンケートにお答えいただいた企業様には、アンケートだけでは分からないお客様のご要望などを拝聴させていただくために、サポートサービス委員会の委員が貴社に直接訪問し、お願いをさせていただく場合がございます。その際に、貴社の回答を分析した「状況分析結果」を持参し、それについてお話させていただくことも考えております。

〈ご回答頂いたお礼〉

本アンケートにご回答頂きましたお客様には、御礼として以下の資料関係をご提供させて頂きます。

- 誠に僭越ではございますが後日、サポートサービス委員会にて作成した診断ツールを使用し、サポートサービス委員会より貴社の「状況分析結果」をご提供させて頂きたいと考えております。今後の参考としてご活用頂ければ幸いです。もし内容にご興味があるようでしたら、ＩＴを導入された販売店へご相談下さい。不要な場合は、アンケート最後にあるチェック欄にチェックをつけてアンケートをご返送ください。
- 今回当協会にて総力を挙げて作成致しました「必要なセキュリティ対策が分かる本（A5 版 約 200 ページ)」をご提供させて頂きますので、理解度向上の一助としてご活用頂ければ幸いです。
- 今回の調査を調査研究報告書「中堅・中小企業のＩＴサービスメニューに関する調査研究」に纏めご提供させて頂きます。今後の参考として頂ければ幸いです。

〈アンケート回答方法について〉

本アンケートは、ご面倒ですが**経営者**の方及び**情報システム管理者**の方の両者にご回答頂きたく存じます。内容によって､どちらの方に回答いただくかが異なっております｡**経営者の方は P4-6､情報システム管理者の方は P7-30** にお答えください。

なお経営者の方が全般をご掌握されている場合は、経営者の方が全般をお答えいただいても結構でございます。

ご回答いただいたアンケートは、10/31 までに、同封の返信用封筒にて返信ください。

アンケート票の構成

【経営者向けの質問】

◆情報システム全般について（Q1-10）
◆情報セキュリティについて　（Q11-13）

【情報システム管理者向けの質問】

◆コンピュータの運用について

・エンドユーザ支援　（Q14-18）
・日常運用　（Q19-24）
・トラブル対応　（Q25-33）
・原因調査　（Q34-37）
・品質　（Q38-44）
・サービス継続　（Q45-50）
・移行　（Q51-59）

◆セキュリティについて

（インターネットに接続している場合）
・インターネットからの脅威　（Q60-67）
・情報漏洩対策　（Q68-81）
・情報の管理　（Q82-86）
・物理的な対策　（Q87-91）
・人材と組織　（Q92）

（インターネットに接続していない場合）
・情報漏洩対策　（Q93-102）
・情報の管理　（Q103-105）
・物理的な対策　（Q106-110）
・人材と組織　（Q111）

◆貴社について

【まずは、経営者・役員の方に回答をお願いいたします。】

貴社の情報システム全般について質問します。

Q1　情報システムが貴社のビジネスにもたらす意義や価値を把握していますか。あてはまるところに一つだけ○を付けて下さい。

改善サイクルを含め、組織的に対応している	組織的に対応している	担当者を決め、一任している	把握していない	必要性を認めない/分からない
5	4	3	2	1

Q2　IT 部門にビジネス戦略や戦術について説明し、情報システムに反映させていますか。あてはまるところに一つだけ○を付けて下さい。

改善サイクルを含め、組織的に対応している	組織的に対応している	担当者を決め、一任している	説明していない	必要性を認めない/分からない
5	4	3	2	1

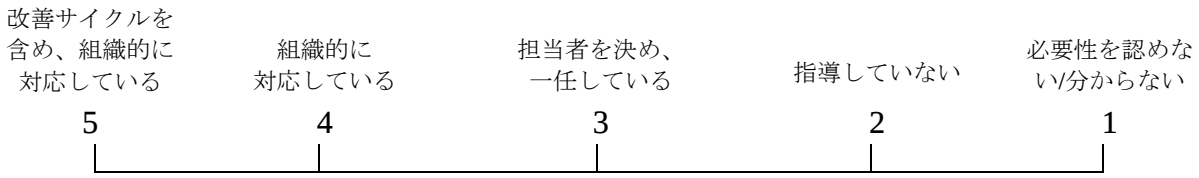
Q3　自社の IT 投資額とその振り向け先（新規設備、新規アプリ開発、保守・運用費用等）を明確にし、その経営効果を把握されていますか。あてはまるところに一つだけ○を付けて下さい。

改善サイクルを含め、組織的に対応している	組織的に対応している	担当者を決め、一任している	把握していない	必要性を認めない/分からない
5	4	3	2	1

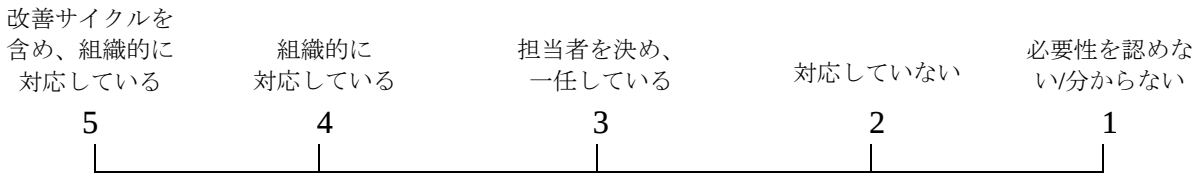
Q4　予算決定時に IT 設備/アプリケーション等の新規投資以外に保守・運用に対する経営効果の評価を行っていますか。あてはまるところに一つだけ○を付けて下さい。

改善サイクルを含め、組織的に対応している	組織的に対応している	担当者を決め、一任している	評価を行っていない	必要性を認めない/分からない
5	4	3	2	1

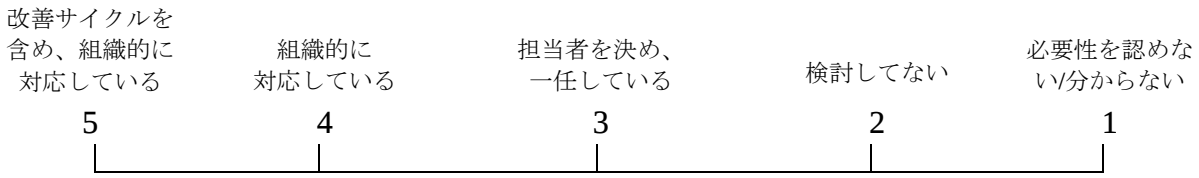
Q5　自社システムの運用に当たって自社内、サービスベンダー委託に関わらず明確な目標を設定し、システムの安定稼動を図るべく指導していますか。あてはまるところに一つだけ○を付けて下さい。



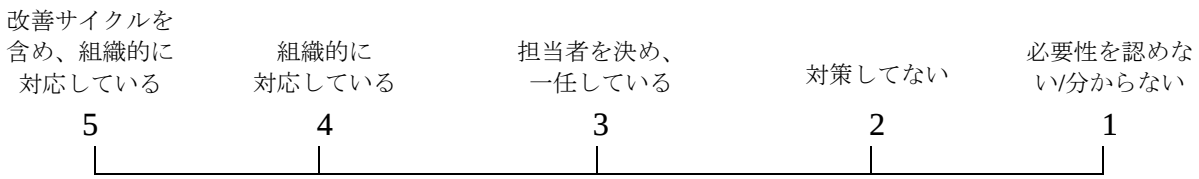
Q6　重大な故障などで情報システムが利用できなくなった場合、御社のビジネスにどれほどの被害が生ずるか理解し対応していますか。あてはまるところに一つだけ○を付けて下さい。



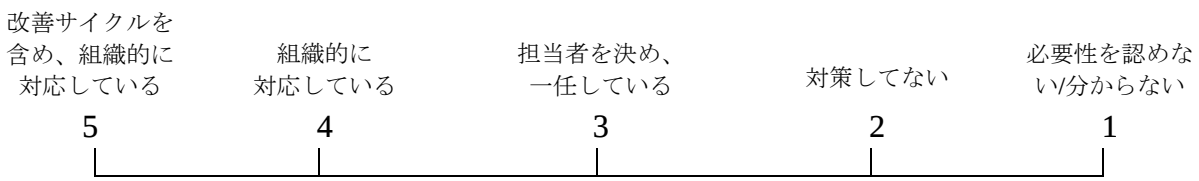
Q7　災害時など情報システムが利用できない場合に備えた対策を検討していますか。あてはまるところに一つだけ○を付けて下さい。



Q8　内部統制の基本的要素に「ＩＴへの対応」が含まれていますが、それについて対策を行っていますか。あてはまるところに一つだけ○を付けて下さい。



Q9　内部統制を実施している企業の業務委託先にも、内部統制の実施、管理が必要ですが、それについて対策を行っていますか。あてはまるところに一つだけ○を付けて下さい。



Q10　情報漏洩が企業経営及び経営者に対して重大な問題を引き起こすことを意識して、しかるべき組織・技術対応をしていますか。あてはまるところに一つだけ○を付けて下さい。

5	4	3	2	1
改善サイクルを含め、組織的に対応している	組織的に対応している	担当者を決め、一任している	対応してない	必要性を認めない/分からない

貴社の情報セキュリティについて質問します。

Q11　会社としてのセキュリティ方針を示すことは、従業員の意識向上に大きく役に立ちます。従業員へ徹底すべき、会社としてのセキュリティ方針を持っていますか。あてはまるところに一つだけ○を付けて下さい。

5	4	3	2	1
方針を定め定期的に見直しをしている	方針を定め示したが見直しをしていない	必要とは思うが決めていない	必要性を感じない	わからない

Q12　情報セキュリティの基準として ISO があり、認証を取得することが企業の信用を、より確実にする場合があります。認証の取得が必要ですか。あてはまるところに一つだけ○を付けて下さい。

5	4	3	2	1
既に認証を取得している	取得の準備を進めている	必要とは思うが意思決定をしていない	必要性を感じない	わからない

Q13　万が一のセキュリティ事故に備え、何かしらの対策を施していますか。セキュリティに関する保険があることを知っていますか。あてはまるところに一つだけ○を付けて下さい。

5	4	3	2	1
既に保険に入っている	保険に入る準備を進めている	必要とは思うが決めていない	必要性を感じない	わからない

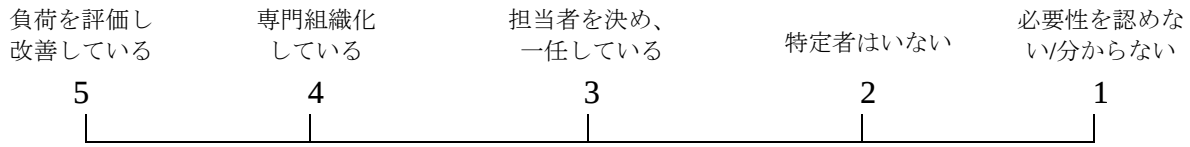
SQ1　その他、情報システムに関してや本アンケートに関する意見などについて、何かございましたらご自由にお書きください。

【続きまして、情報システム管理者の方に回答をお願いいたします。】

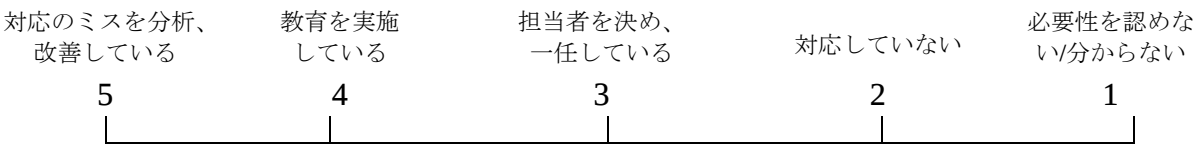
1. コンピュータの運用についての質問

社内利用者支援について質問します。

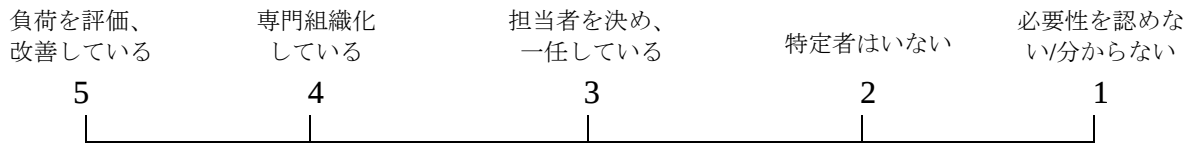
Q14　トラブルの問い合せ窓口を設置し、社内に公開していますか（社員の生産性を向上するには、専門の社員支援体制が必要です)。あてはまるところに一つだけ○を付けて下さい。



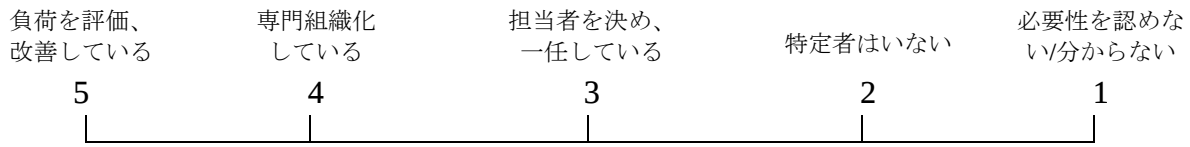
Q15　質問対応要員のスキルを維持していますか (スキル低下は社員から「応対が悪い」とのクレームが多くなります)。あてはまるところに一つだけ○を付けて下さい。



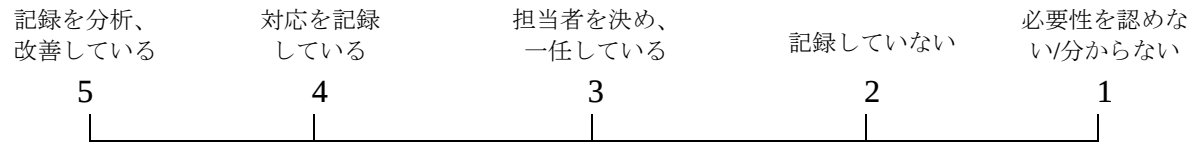
Q16　質問対応要員、電話の数は充分ですか (不十分ですと社員から「電話がつながりにくい」とのクレームが多くなります)。あてはまるところに一つだけ○を付けて下さい。



Q17　PC の使い方や業務処理に関する問い合せに対応していますか（社員の生産性向上のために必要になります)。あてはまるところに一つだけ○を付けて下さい。

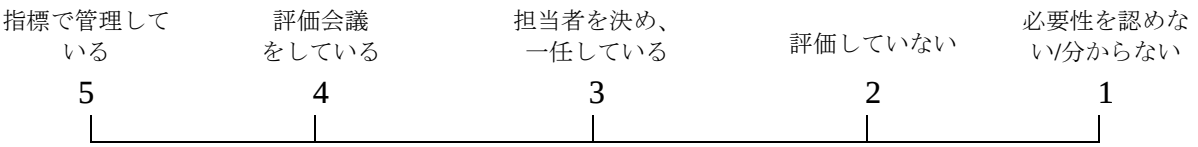


Q18　質問内容を記録し、改善に役立てていますか (質問を低減し、満足度を向上するために必要になります)。あてはまるところに一つだけ○を付けて下さい。

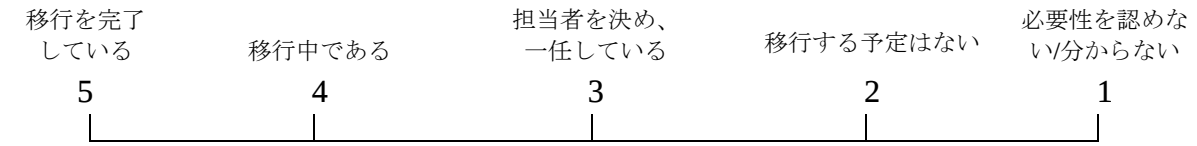


日常運用について質問します。

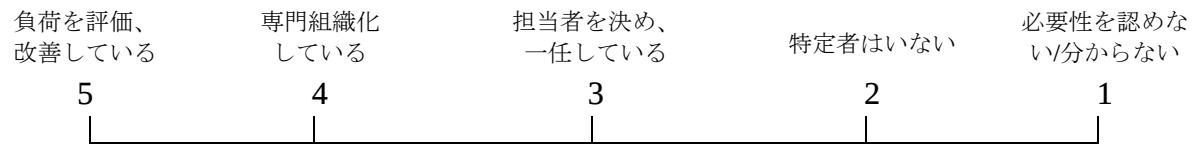
Q19　アプリケーション維持の要・不要の観点から棚卸し評価を行っていますか（不要なアプリケーションを維持するコストを低減できます)。あてはまるところに一つだけ○を付けて下さい。



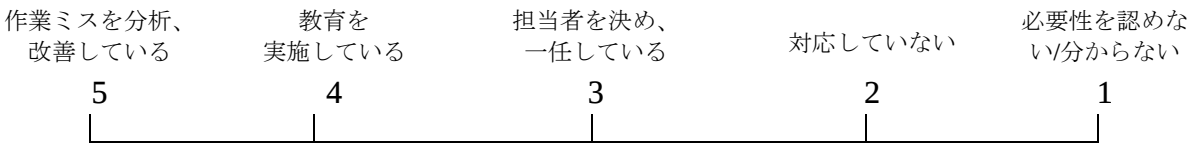
Q20　アプリケーション関連の 2007 年問題に対して対策を行っていますか（団塊世代の退職に伴い、障害修正や機能追加ができなくなる恐れがあります)。あてはまるところに一つだけ○を付けて下さい。



Q21　休日・夜間を含め、オペレーション要員数は十分ですか (不十分ですと作業ミス等の修復での就業が増え、退職者が増える恐れがあります)。あてはまるところに一つだけ○を付けて下さい。



Q22　オペレーション要員のスキルを維持していますか (作業ミスが増えたり、効率が下がる恐れがあります)。あてはまるところに一つだけ○を付けて下さい。



Q23　定常操作や非定常操作に対するオペレーション手順書を整備していますか (作業ミスが増えたり、効率が下がる恐れがあります)。あてはまるところに一つだけ○を付けて下さい。

5	4	3	2	1
作業ミスを分析、手順書を改版している	手順書を整備している	担当者を決め、一任している	整備していない	必要性を認めない/分からない

Q24　オペレーションの自動化を進めていますか (手動オペレーションはミスを招いたり、コスト高につながります)。あてはまるところに一つだけ○を付けて下さい。

5	4	3	2	1
負荷を評価、自動化を推進している	自動化を導入している	担当者を決め、一任している	手作業で行っている状況	必要性を認めない/分からない

トラブル対応について質問します。

Q25　重要なシステムの稼働状況の監視を行っていますか (社員からのクレームを待たず、より迅速に解決を図る必要があります)。あてはまるところに一つだけ○を付けて下さい。

5	4	3	2	1
障害を分析、稼動改善している	監視システムを導入している	担当者を決め、一任している	社員からの申告で対応している	必要性を認めない/分からない

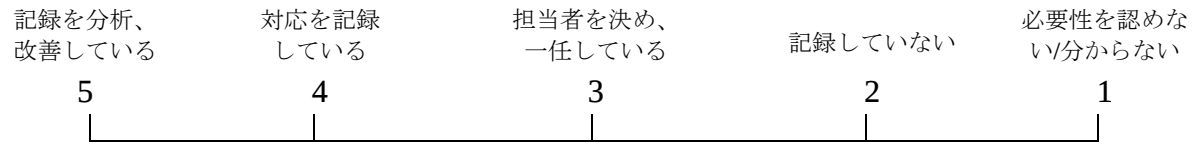
Q26　ハードやソフトのトラブルの兆候が検出できていますか (ハード品質劣化や、システム負荷傾向を検出することでトラブルを未然に防止できる割合が増えます)。あてはまるところに一つだけ○を付けて下さい。

5	4	3	2	1
監視の上、障害を分析し、改善している	監視し、兆候を検出している	担当者を決め、一任している	検出できていない	必要性を認めない/分からない

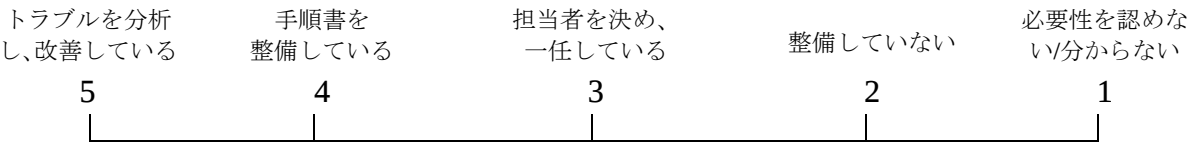
Q27　重要システム周辺の電源・空調に異常が発生した場合の監視・通報の仕組みはありますか（放置すると稼動条件面からシステム停止となり、重要なデータを消失したり、作業のやり直しが必要になります)。あてはまるところに一つだけ○を付けて下さい。

5	4	3	2	1
障害を分析、兆候検出し改善している	監視システムを導入している	担当者を決め、一任している	監視していない	必要性を認めない/分からない

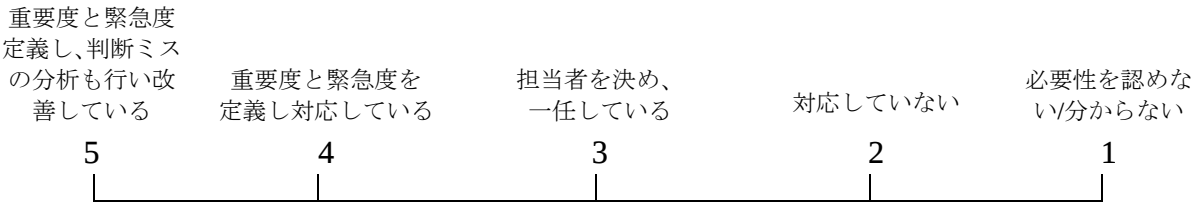
Q28 トラブル対応の内容や処理時間など記録をつけていますか（記録をつけることで、再発時の対応を円滑にできます)。あてはまるところに一つだけ○を付けて下さい。



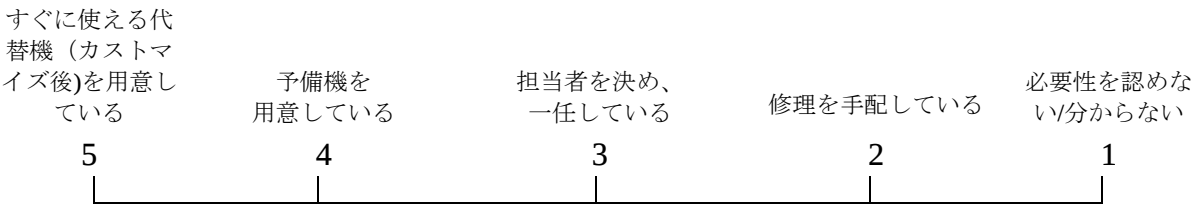
Q29 トラブル対応を実施する場合、トラブル対応手順書の整備は行っていますか (トラブル解決を効率的に行い､特定の担当者に依存しない均一的な処置が可能です)｡あてはまるところに一つだけ○を付けて下さい。



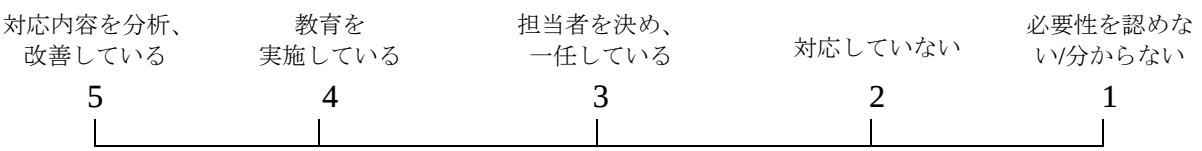
Q30 トラブルが発生した場合、重大度や緊急度を適切に判断し、優先順位を意識した対応をしていますか (企業活動への影響を最小限にするために必要です)。あてはまるところに一つだけ○を付けて下さい。



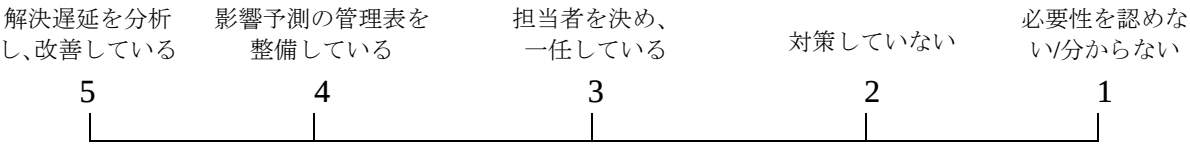
Q31 PC 故障時の対策を考慮していますか（社員の業務への影響を最小限にとどめるために必要です)。あてはまるところに一つだけ○を付けて下さい。



Q32 トラブル対応要員のスキルを維持していますか (対応要員が適切に教育されていないと積み残しが増え、企業活動に影響する恐れがあります)。あてはまるところに一つだけ○を付けて下さい。

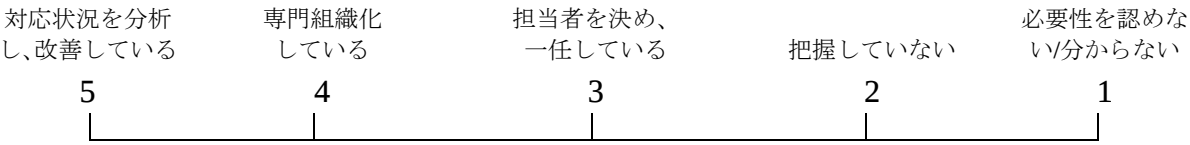


Q33　障害が起ったときの影響範囲はある程度推測できる対策をとっていますか（トラブル発生、あるいは兆候検出時点で、その影響度合いを見極め、対策を取ることが重要です)。あてはまるところに一つだけ○を付けて下さい。

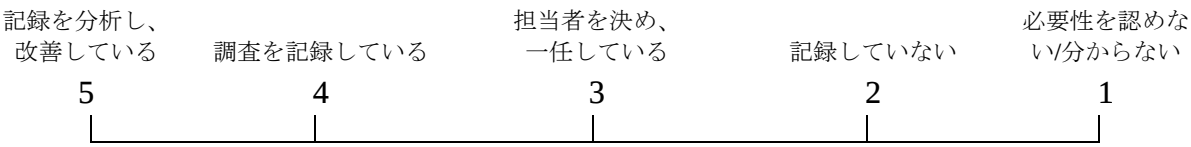


原因調査について質問します。

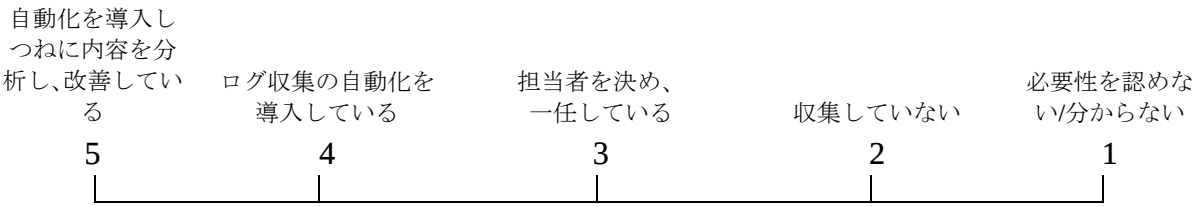
Q34　トラブル発生状況を把握し、対策を検討していますか（トラブルの発生増大を放っておくと、更にトラブルが増え、企業活動に深刻な影響を与える場合もあります)。あてはまるところに一つだけ○を付けて下さい。



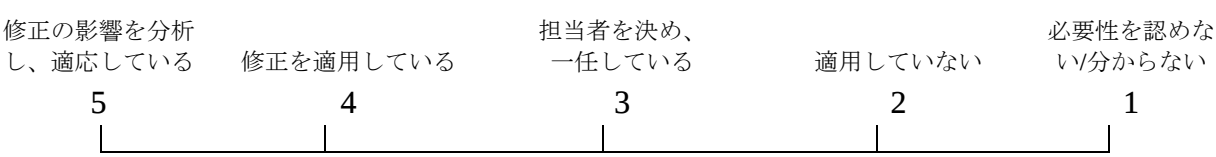
Q35　原因調査の内容や処理時間など記録をつけていますか（記録をつけないと、改善の糸口がつかめなくなります)。あてはまるところに一つだけ○を付けて下さい。



Q36　イベントログやシステムログを収集していますか　(問題の根本原因を調査するために必要になります)。あてはまるところに一つだけ○を付けて下さい。



Q37　ソフトウェアの最新修正版を常に適用していますか（修正を適用することで、トラブルの発生を未然に防止することができます)。あてはまるところに一つだけ○を付けて下さい。



品質について質問します。

Q38　社内に約束するシステムの稼働率を設定していますか。(100%の稼働率を求めることは難しく、コスト効果を考え適切なバランスで折り合いをつける必要があります)。あてはまるところに一つだけ○を付けて下さい。

指標で管理している	目標を設定している	担当者を決め、一任している	設定していない	必要性を認めない/分からない
5	4	3	2	1

Q39　使用者の満足度を考慮した運用改善目標を設定し、達成したかを把握していますか（サービス提供は使用者の満足度の向上につながるようにする必要があります)。あてはまるところに一つだけ○を付けて下さい。

指標で管理している	達成度を把握している	担当者を決め、一任している	把握していない	必要性を認めない/分からない
5	4	3	2	1

Q40　将来的にシステムに必要な処理量を把握していますか　(処理能力増強のシステム変更には充分な準備期間が必要なため、将来的な処理量の把握が必要です)。あてはまるところに一つだけ○を付けて下さい。

指標で管理している	処理量を把握している	担当者を決め、一任している	把握していない	必要性を認めない/分からない
5	4	3	2	1

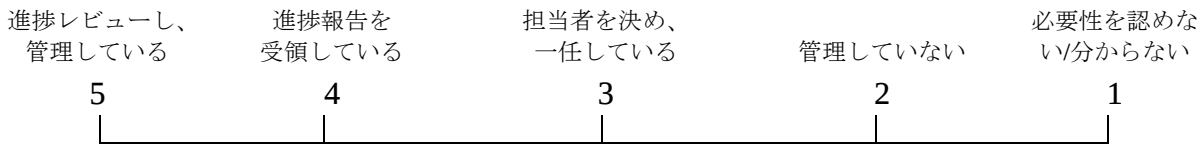
Q41　導入以降のシステム処理量の変動を把握していますか（システムの負荷増大は、システムのレスポンス速度や故障率に大きく影響します)。あてはまるところに一つだけ○を付けて下さい。

指標で管理している	処理量を把握している	担当者を決め、一任している	把握していない	必要性を認めない/分からない
5	4	3	2	1

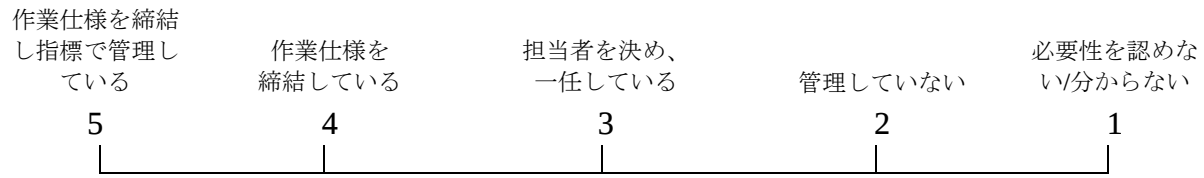
Q42　システム導入にあたって必要な運用コストを把握していますか　（一般にシステム費用のうち 60%が運用コストと言われています)。あてはまるところに一つだけ○を付けて下さい。

指標で管理している	運用コストを把握している	担当者を決め、一任している	把握していない	必要性を認めない/分からない
5	4	3	2	1

Q43　外部委託した作業の進捗状況や作業結果をレビューし、必要な指示を行っていますか（レビューの実施は自らのサービス品質を確保するために必要です)。あてはまるところに一つだけ○を付けて下さい。

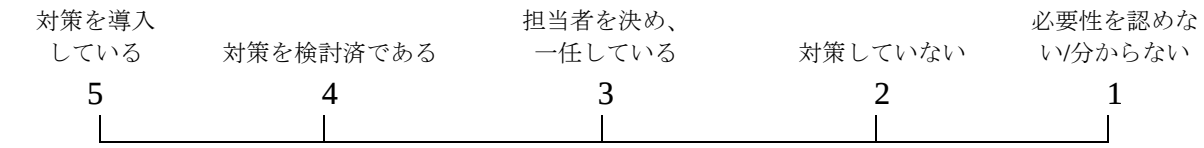


Q44　外部委託にあたって、作業責任を明確化し、期待するサービス品質を提示していますか（サービス品質の提示は、自らのサービス品質目標を定めるために必要です)。あてはまるところに一つだけ○を付けて下さい。

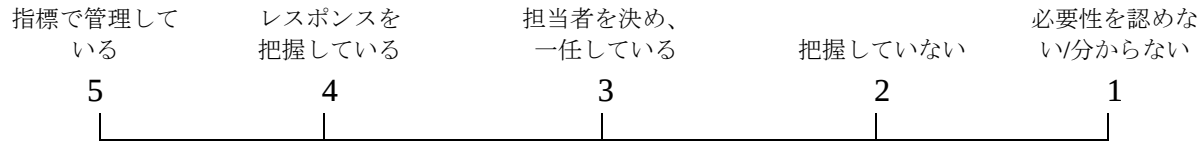


サービス継続について質問します。

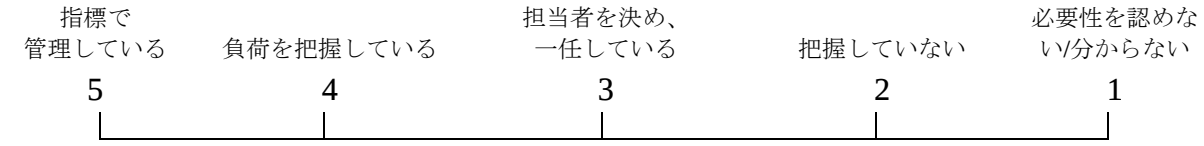
Q45　企業の業務継続の面から欠くことができないシステムの災害、事故、停電対策を行っていますか（企業活動を継続させるために必要です)。あてはまるところに一つだけ○を付けて下さい。



Q46　システムのレスポンスを把握していますか（システムのレスポンス速度は、社員の生産性や満足度に大きな影響を与えます)。あてはまるところに一つだけ○を付けて下さい。



Q47　システムの負荷状況を把握できていますか（システムの負荷は、システムのレスポンスや障害発生率に大きな影響を与えます)。あてはまるところに一つだけ○を付けて下さい。



Q48 バックアップの取得は確実にできていますか（システム障害により重要なデータが失われたり、システムの再構成が必要になったりする場合があります)。あてはまるところに一つだけ○を付けて下さい。

基準を定め指標で管理している	バックアップを実施している	担当者を決め、一任している	取得していない	必要性を認めない/分からない
5	4	3	2	1

Q49 バックアップからのリストアが確実にできていますか（データやシステムのバックアップが、いざというとき読み出せなかったり、作業ミスで役立たないことがありがちです)。あてはまるところに一つだけ○を付けて下さい。

リストア訓練を実施している	読み出し確認をしている	担当者を決め、一任している	実施していない	必要性を認めない/分からない
5	4	3	2	1

Q50 システムの稼働率の目標を定め、実態を把握していますか（システムの稼働率は、障害の頻度だけでなく、システムの冗長性やトラブルからの復旧速度にも影響されます)。あてはまるところに一つだけ○を付けて下さい。

指標で管理している	稼働率を把握している	担当者を決め、一任している	把握していない	必要性を認めない/分からない
5	4	3	2	1

移行について質問します。

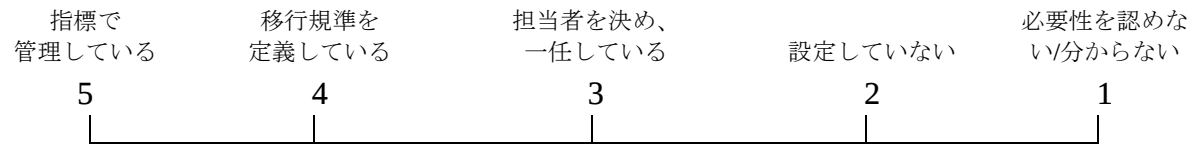
Q51 システムの導入・展開のスケジュール管理を実施していますか（システム展開のスケジュールが狂うと、事態を収めるために思わぬ費用や作業が発生します)。あてはまるところに一つだけ○を付けて下さい。

専門体制を整備し進捗指標で管理している	専門体制を整備している	担当者を決め、一任している	管理していない	必要性を認めない/分からない
5	4	3	2	1

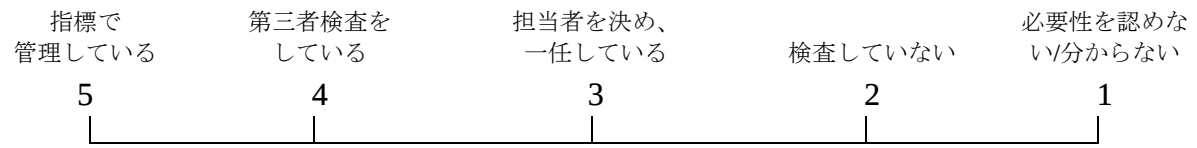
Q52 PC の導入・展開の作業工数を管理していますか（PC の導入にはソフトウェア・インストールやネットワーク情報設定などのカストマイズ作業が必要になります)。あてはまるところに一つだけ○を付けて下さい。

専門体制を整備し進捗指標で管理している	専門体制を整備している	担当者を決め、一任している	管理していない	必要性を認めない/分からない
5	4	3	2	1

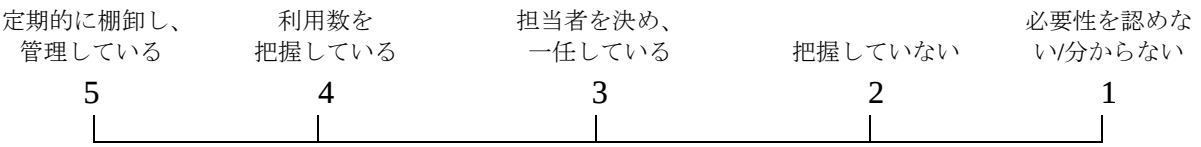
Q53　運用への移行を判定するため、移行試験における品質目標を定めていますか（高品質のシステムを実現するには、運用に移行する前に品質評価が必要です)。あてはまるところに一つだけ○を付けて下さい。



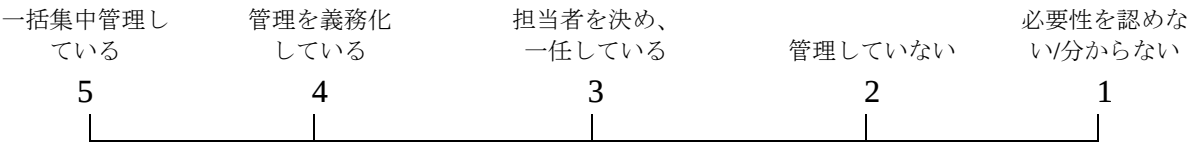
Q54　システム開発から運用に移行する過程でシステム開発担当者以外による検査を実施していますか（誤謬や悪意を持った処理が紛れ込む可能性があります)。あてはまるところに一つだけ○を付けて下さい。



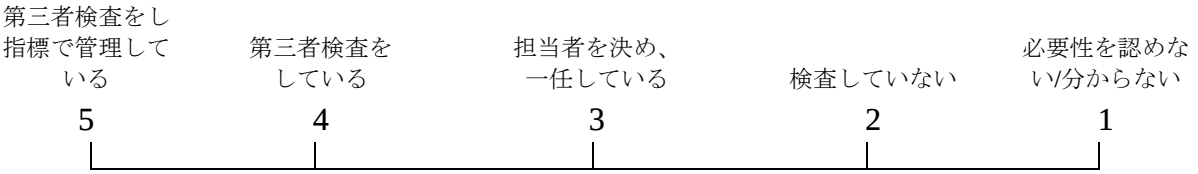
Q55　ライセンス契約数違反や無駄なライセンス購入はありませんか（著作権保護法で守られており、違反すると懲罰的罰金が課されたり、企業名が公表されたりします)。あてはまるところに一つだけ○を付けて下さい。



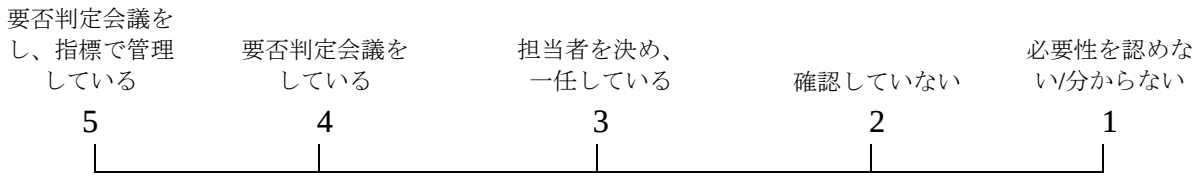
Q56　最新のシステム構成情報（ハード/ソフト）の管理を行っていますか（最新の情報になっていないと、トラブルを悪化させたり、回復が遅くなる場合があります)。あてはまるところに一つだけ○を付けて下さい。



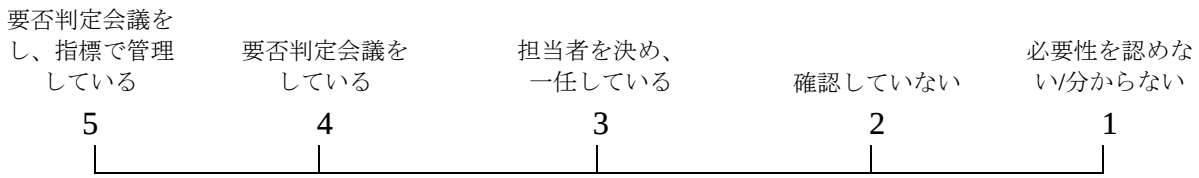
Q57　発生したトラブル解決のための変更内容と、変更後の検査を第三者が検査していますか（品質が劣化したり、悪意を持った処理が混入することを防ぐために必要です)。あてはまるところに一つだけ○を付けて下さい。



Q58　変更の必要性を事前に確認していますか（不適切な計画に基づく構成変更・修正適用は、業務運用のスケジュールに支障をきたします)。あてはまるところに一つだけ○を付けて下さい。



Q59　追加または改善した機能で、使われていないものが多くありませんか（社員が希望したとしても、投資効果やシステム品質の面から必要性を吟味する必要があります)。あてはまるところに一つだけ○を付けて下さい。



SQ2　その他、**情報システムの運用**に関してや本アンケートに関する意見などについて、何かございましたらご自由にお書きください。

2 セキュリティに関する質問

QA　貴社の情報セキュリティに対する取り組みについてお聞きします。貴社では、コンピュータをインターネットに接続して使用していますか。あてはまるところに一つだけ○を付けて下さい。

1. インターネットに接続して使用している　→Q60(下の設問)へ
2. インターネットには接続していない　→Q93(P26)へ

【ここからは、QA で「1.インターネットに接続して使用している」と回答した方にお聞きします。】

インターネットからの脅威への対策について質問します。

日々出てくる新手のウィルスや攻撃に対して常に備えておくことが、攻撃による情報の改ざんや漏洩を防ぐ手段になります。

Q60　インターネットに接続していると、外部から侵入される危険があります。不正アクセスへの対応策をとっていますか。あてはまるところに一つだけ○を付けて下さい。

対応している	一部対応している	危険は知っているが対応していない	危険があることを知らない	わからない
5	4	3	2	1

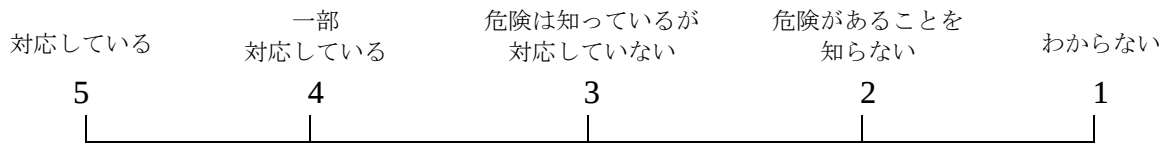
Q61　コンピュータウイルスに感染すると、PC のファイルが改ざんされたりコンピュータが破壊される危険があります。対応策をとっていますか。あてはまるところに一つだけ○を付けて下さい。

対応している	一部対応している	危険は知っているが対応していない	危険があることを知らない	わからない
5	4	3	2	1

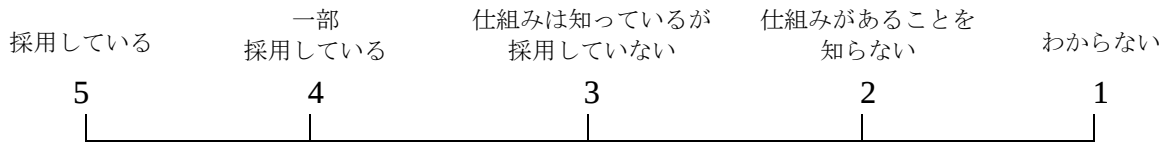
Q62　次々と送られてくる広告や迷惑メールを制限する方法やサービスがあります。対応策をとっていますか。あてはまるところに一つだけ○を付けて下さい。

対応している	一部対応している	危険は知っているが対応していない	危険があることを知らない	わからない
5	4	3	2	1

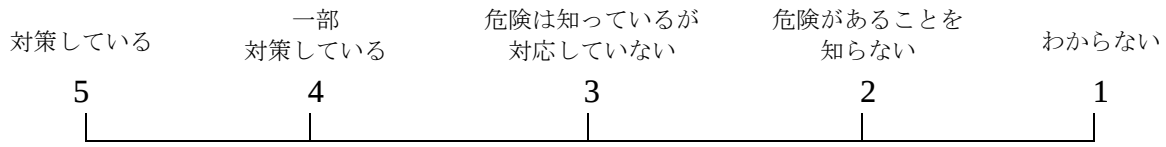
Q63　コンピュータウイルスに感染すると、知らないうちにインターネットに情報を漏えいしたり、他のコンピュータに迷惑行為を行う可能性があります。対応策をとっていますか。あてはまるところに一つだけ○を付けて下さい。



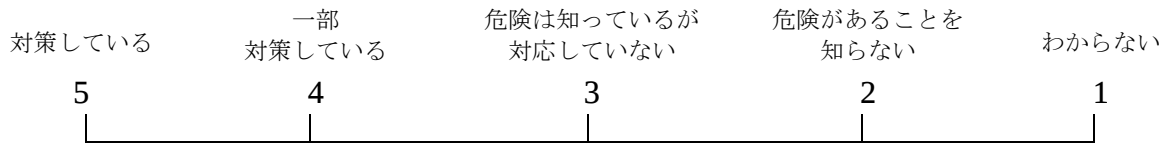
Q64　外部からの攻撃を監視したり、防御したりする仕組みがあります。またそれらの攻撃を監視し通報する仕組みがあります。これらの対策を採用していますか。あてはまるところに一つだけ○を付けて下さい。



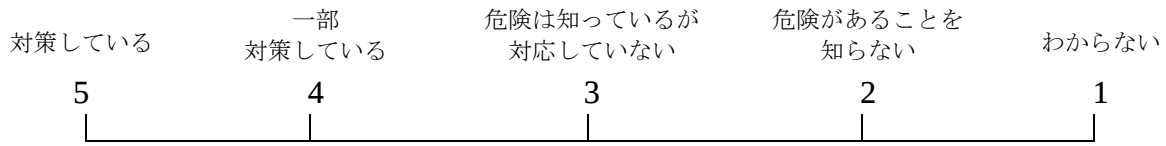
Q65　外部からの侵入で、PC 内の重要なファイルが壊れたり、なくなったりする場合があります。それに備えてデータバックアップ対策をしていますか。あてはまるところに一つだけ○を付けて下さい。



Q66　Ｗｉｎｄｏｗｓの不具合を利用して、悪意のある人が PC を攻撃することが出来ます、定期的なパッチ適用等の対応策をとっていますか。あてはまるところに一つだけ○を付けて下さい。



Q67　ウィルス等の侵入を防ぐ為、社内 LAN に、許可した PC 以外を接続できないように制限することができます。対応策を採っていますか。あてはまるところに一つだけ○を付けて下さい。



重要な情報を漏洩させない為の、各種対策について質問します。

情報そのものを漏洩させない方法や、漏洩してもそれを使うことが出来ないようにする手段等の対策について、その状況をお聞きしています

Q68　従業員の PC に重要な個人情報や、どのようなソフトウェアやフリープログラムが入っているか把握していますか。あてはまるところに一つだけ○を付けて下さい。

5	4	3	2	1
全て把握している	一部把握している	必要性はわかるが把握していない	必要性があることを知らない	わからない

Q69　Ｗｉｎｎｙ等のファイル交換ソフトがＰＣに入っていると内部情報が外部に公開される危険が大きくなります。ＰＣの監視等の対策をしていますか。あてはまるところに一つだけ○を付けて下さい。

5	4	3	2	1
対策している	一部対策している	必要性はわかるが対応していない	必要性があることを知らない	わからない

Q70　内部からのメールにより、重要な情報が漏洩することがあります。メールの履歴を保存したり、内容によっては送信を抑止できる対策を実施していますか。あてはまるところに一つだけ○を付けて下さい。

5	4	3	2	1
対策している	一部対策している	必要性はわかるが対応していない	必要性があることを知らない	わからない

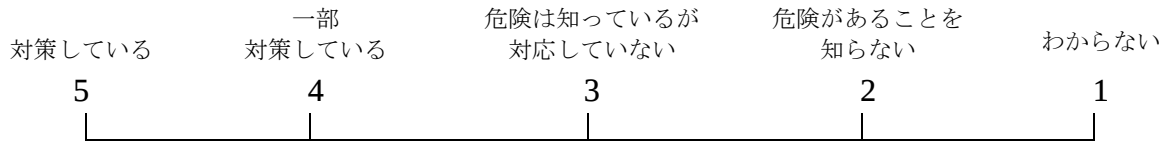
Q71　盗難・紛失による情報漏洩対策として、ＰＣ内の全データを暗号化して、データを読み取ることができなくする方法があります。対応策をとっていますか。あてはまるところに一つだけ○を付けて下さい。

5	4	3	2	1
対策している	一部対策している	危険は知っているが対応していない	危険があることを知らない	わからない

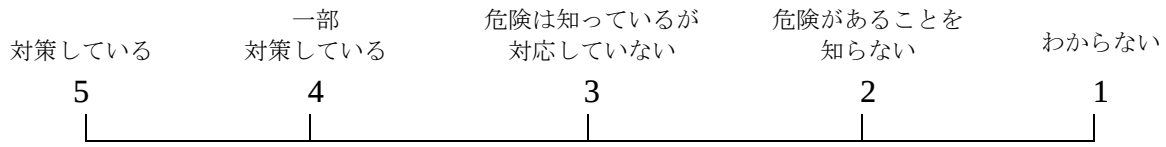
Q72　無線 LAN を使用していて、PC でファイル共有の設定をしていると、外部の人間からもファイルが見られてしまうことがあります。これを避ける為に暗号化をすることが出来ます。対応策をとっていますか。あてはまるところに一つだけ○を付けて下さい。

5	4	3	2	1
対策している	一部対策している	危険は知っているが対応していない	危険があることを知らない	該当しない

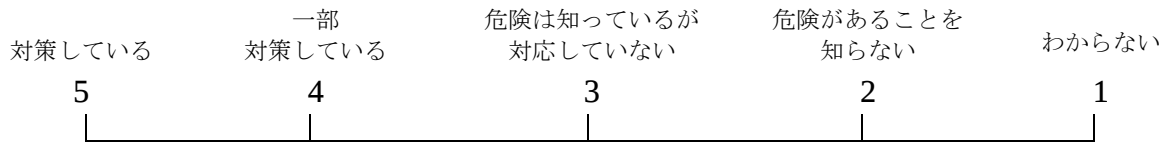
Q73　情報漏洩対策として、PC を複数人で使用する場合、各自の ID を利用しファイルアクセス等の制限をすることが出来ます。対応策をとっていますか。あてはまるところに一つだけ○を付けて下さい。



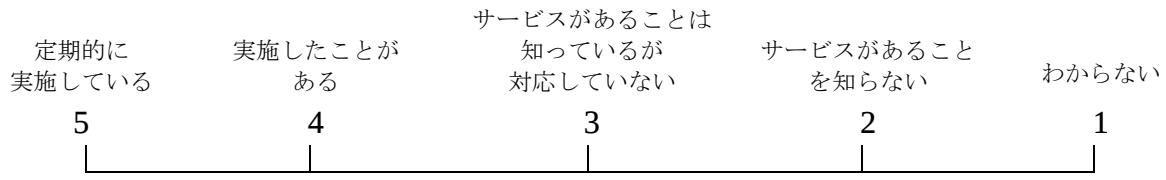
Q74　情報漏洩対策として、PC から外部媒体（USB メモリや CD-R、フロッピーディスクなど）への出力を禁止、管理、制限することができます。対応策をとっていますか。あてはまるところに一つだけ○を付けて下さい。



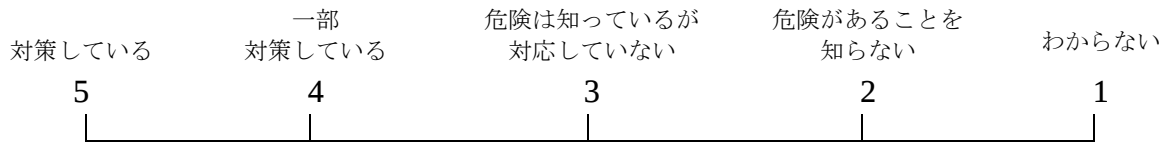
Q75　情報漏洩対策として、クライアント PC を最小限の機能のみにし(シンクライアント)、サーバでほとんどの処理を行うようにする事が出来ます。このような対応策をとっていますか。あてはまるところに一つだけ○を付けて下さい。



Q76　セキュリティ対策全体の有効性を評価するサービスがあります。実施していますか。あてはまるところに一つだけ○を付けて下さい。



Q77　Windows ログイン ID がわからなくても、ハードディスクだけ取り出すと内容を読み取ることができる為、盗まれると中身のデータを読み取られることがあります。この情報漏洩への対策をとっていますか。あてはまるところに一つだけ○を付けて下さい。



Q78　機器・媒体の廃棄前に残存データを完全に消去しないと、情報漏洩に繋がる恐れがあります。対応策を実施していますか。あてはまるところに一つだけ○を付けて下さい。

対策している	時々 対策している	危険は知っているが 対応していない	必要性を 感じない	わからない
5	4	3	2	1

Q79　業務外のＷｅｂアクセスやメールにこそ、ウィルス感染や情報漏洩の危機が潜んでいます。従業員の作業履歴を収集・解析することが漏洩防止に繋がります。対応策をとっていますか。あてはまるところに一つだけ○を付けて下さい。

対策している	一部 対策している	危険は知っているが 対応していない	必要性があることを 知らない	わからない
5	4	3	2	1

Q80　情報漏洩抑止のために、従業員のファイルアクセスを管理し監視する仕組みがあります。対応策をとっていますか。あてはまるところに一つだけ○を付けて下さい。

対策している	一部 対策している	危険は知っているが 対応していない	必要性があることを 知らない	わからない
5	4	3	2	1

Q81　コピー機で印刷したはずの用紙が紛失し、情報漏洩に繋がることがあります。印刷物についても出力の管理をすることが出来ます。対応策をとっていますか。あてはまるところに一つだけ○を付けて下さい。

対策している	一部 対策している	危険は知っているが 対応していない	必要性があることを 知らない	わからない
5	4	3	2	1

重要な情報の管理の仕方について質問します。

脅威や情報漏洩への対策はもちろん重要ですが機器、ソフト、データなどの管理をすることにより事後の復旧を最短の時間で行うことが出来ます。

Q82　電源や装置の故障で、PC 内の重要なファイルが壊れたり、なくなったりする場合があります。それに備えてデータバックアップ等の対策をしていますか。あてはまるところに一つだけ○を付けて下さい。

対策している	一部対策している	危険は知っているが対応していない	危険があることを知らない	わからない
5	4	3	2	1

Q83　アダルトサイト等、インターネットで開くことができるページを制限できますが、対策をしていますか。あてはまるところに一つだけ○を付けて下さい。

対策している	一部対策している	必要性はわかるが対応していない	必要性があることを知らない	わからない
5	4	3	2	1

Q84　ファイルが改ざんされていないことを保証するひとつの方法として、ファイルに署名ができることが一般化されつつありますが、電子署名を採用していますか。あてはまるところに一つだけ○を付けて下さい。

採用している	一部採用している	必要性はわかるが採用していない	必要性があることを知らない	わからない
5	4	3	2	1

Q85　通常のパスワードだけでなく、指紋などの生態認証によりユーザ認証をより強固にする方法があります。対応策をとっていますか。あてはまるところに一つだけ○を付けて下さい。

対策している	一部対策している	危険は知っているが対応していない	危険があることを知らない	わからない
5	4	3	2	1

Q86　災害時のデータ紛失に備えて、重要なデータを別の場所に定期的にバックアップしていますか。あてはまるところに一つだけ○を付けて下さい。

定期的に実施・保管している	時々実施・保管している	必要性はわかるが実施していない	必要性を感じない	わからない
5	4	3	2	1

物理的な対策について質問します。

情報漏洩や破壊はインターネットからだけではありません。盗難から自然災害への対応まで、物理的な対策も必要です。

Q87　外部からの不審者の侵入に備え、監視カメラや警備員の常駐、また入館者をチェック・記録していますか。あてはまるところに一つだけ○を付けて下さい。

365日・24時間対応している	全てではないが対応している	必要性があることを知っているが対応していない	必要性があることを知らない	わからない
5	4	3	2	1

Q88　部外者が重要なシステムを設置した部屋へ入室するのを制限したり、記録したりする仕組みはありますか。あてはまるところに一つだけ○を付けて下さい。

365日・24時間対応している	全てではないが対応している	必要性があることを知っているが対応していない	必要性があることを知らない	わからない
5	4	3	2	1

Q89　ＩＣカード等で、建物・サーバ室・システムへのアクセスを一元的に管理する仕組みがあります。導入していますか。あてはまるところに一つだけ○を付けて下さい。

全面的に導入している	一部導入している	必要だと思うが導入していない	必要性を感じない	わからない
5	4	3	2	1

Q90　大規模災害時に重要システムの稼動を確保するため、別拠点に予備のシステムを設置し、業務を続ける対策があります。この対策をとっていますか。あてはまるところに一つだけ○を付けて下さい。

対策している	一部対策している	危険は知っているが対応していない	必要性を感じない	わからない
5	4	3	2	1

Q91　システム障害時にシステムを短時間で復旧し、業務を継続するための二重化等の対策・手順は確立していますか。この対策をとっていますか。あてはまるところに一つだけ○を付けて下さい。

対策している	ハードディスクのみ対策している	危険は知っているが対策していない	必要性を感じない	わからない
5	4	3	2	1

情報セキュリティ対策における人材と組織について質問します。

情報セキュリティ対策を根本から支えるのは、やはり人と組織です。組織としての仕組みと従業員の意識があってこそ、セキュリティ対策が生きてきます。

Q92　情報セキュリティについては、定期的に注意喚起を行うことが、意識向上に繋がります。定期的に従業員に情報セキュリティ教育をおこなっていますか。あてはまるところに一つだけ○を付けて下さい。

定期的に教育を行っている	教育を行ったことがある	教育は必要だが行っていない	教育が必要だと思わない	わからない
5	4	3	2	1

SQ3　その他、**情報セキュリティに関して**や本アンケートに関する意見などについて、何かございましたらご自由にお書きください。

【情報セキュリティの設問はこれで終わりです。F1(P31)へお進みください。】

【ここからは、QA で「2. インターネットには接続していない」と回答した方にお聞きします。】

重要な情報を漏洩させない為の、各種対策について質問します。

情報そのものを漏洩させない方法や、漏洩しても、それを使うことが出来ないようにする手段等の対策について、その状況をお聞きしています

Q93　盗難・紛失による情報漏洩対策として、ＰＣ内の全データを暗号化して、データを読み取ることができなくする方法があります。対応策をとっていますか。あてはまるところに一つだけ○を付けて下さい。

対策している	一部対策している	危険は知っているが対応していない	危険があることを知らない	わからない
5	4	3	2	1

Q94　無線 LAN を使用していて、PC でファイル共有の設定をしていると、外部の人間からもファイルが見られてしまうことがあります。これを避ける為に暗号化をすることが出来ます。対応策をとっていますか。あてはまるところに一つだけ○を付けて下さい。

対策している	一部対策している	危険は知っているが対応していない	危険があることを知らない	該当しない
5	4	3	2	1

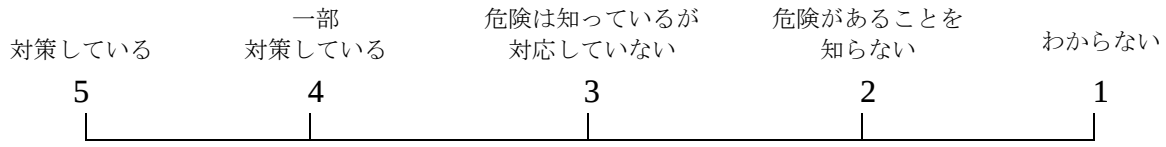
Q95　情報漏洩対策として、PC を複数人で使用する場合、各自の ID を利用しファイルアクセス等の制限をすることが出来ます。対応策をとっていますか。あてはまるところに一つだけ○を付けて下さい。

対策している	一部対策している	危険は知っているが対応していない	危険があることを知らない	わからない
5	4	3	2	1

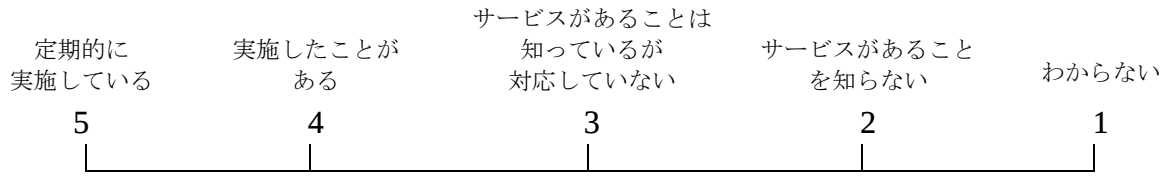
Q96　情報漏洩対策として、PC から外部媒体（USB メモリや CD-R、フロッピーディスクなど）への出力を禁止、管理、制限することができます。対応策をとっていますか。あてはまるところに一つだけ○を付けて下さい。

対策している	一部対策している	危険は知っているが対応していない	危険があることを知らない	わからない
5	4	3	2	1

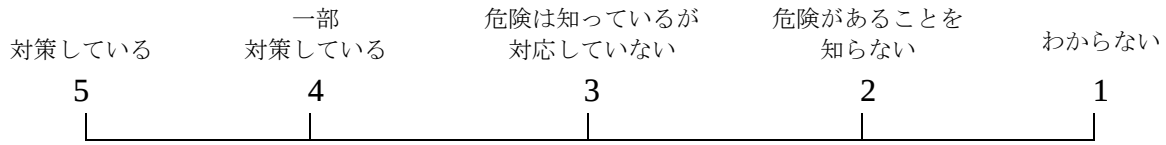
Q97　情報漏洩対策として、クライアント PC を最小限の機能のみにし(シンクライアント)、サーバでほとんどの処理を行うようにする事が出来ます。このような対応策をとっていますか。あてはまるところに一つだけ○を付けて下さい。



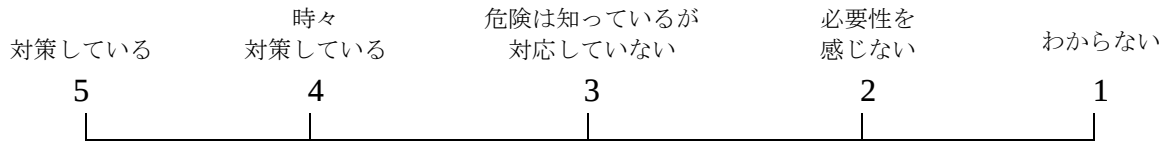
Q98　セキュリティ対策全体の有効性を評価するサービスがあります。実施していますか。あてはまるところに一つだけ○を付けて下さい。



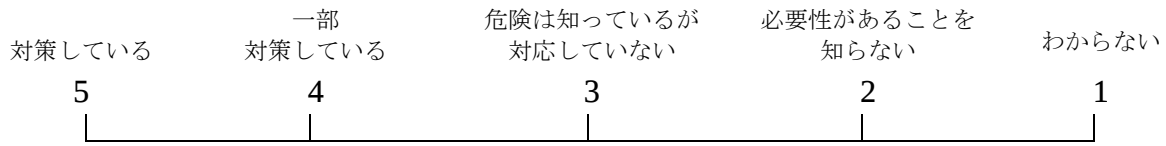
Q99　Windows ログイン ID がわからなくても､ハードディスクだけ取り出すと内容を読み取ることができる為、盗まれると中身のデータを読み取られることがあります。この情報漏洩への対策をとっていますか。あてはまるところに一つだけ○を付けて下さい。



Q100　機器・媒体の廃棄前に残存データを完全に消去しないと、情報漏洩に繋がる恐れがあります。対応策を実施していますか。あてはまるところに一つだけ○を付けて下さい。



Q101　情報漏洩抑止のために、従業員のファイルアクセスを管理し監視する仕組みがあります。対応策をとっていますか。あてはまるところに一つだけ○を付けて下さい。



Q102　コピー機で印刷したはずの用紙が紛失し、情報漏洩に繋がることがあります。印刷物についても出力の管理をすることが出来ます。対応策をとっていますか。あてはまるところに一つだけ○を付けて下さい。

対策している	一部対策している	危険は知っているが対応していない	必要性があることを知らない	わからない
5	4	3	2	1

重要な情報の管理の仕方について質問します。

脅威や情報漏洩への対策はもちろん重要ですが機器、ソフト、データなどの管理をすることにより事後の復旧を最短の時間で行うことが出来ます。

Q103　電源や装置の故障で、PC 内の重要なファイルが壊れたり、なくなったりする場合があります。それに備えてデータバックアップ等の対策をしていますか。あてはまるところに一つだけ○を付けて下さい。

対策している	一部対策している	危険は知っているが対応していない	危険があることを知らない	わからない
5	4	3	2	1

Q104　通常のパスワードだけでなく、指紋などによる生態認証によりユーザ認証をより強固にする方法があります。対応策をとっていますか。あてはまるところに一つだけ○を付けて下さい。

対策している	一部対策している	危険は知っているが対応していない	危険があることを知らない	わからない
5	4	3	2	1

Q105　災害時のデータ紛失に備えて、重要なデータを別の場所に定期的にバックアップしていますか。あてはまるところに一つだけ○を付けて下さい。

定期的に実施・保管している	時々実施・保管している	必要性はわかるが実施していない	必要性を感じない	わからない
5	4	3	2	1

物理的な対策について質問します。

情報漏洩や破壊はインターネットからだけではありません。盗難から自然災害への対応まで、物理的な対策も必要です。

Q106　外部からの不審者の侵入に備え、監視カメラや警備員の常駐、また入館者をチェック・記録していますか。あてはまるところに一つだけ○を付けて下さい。

365日・24時間対応している	全てではないが対応している	必要性があることを知っているが対応していない	必要性があることを知らない	わからない
5	4	3	2	1

Q107　部外者が重要なシステムを設置した部屋へ入室するのを制限したり、記録したりする仕組みはありますか。あてはまるところに一つだけ○を付けて下さい。

365日・24時間対応している	全てではないが対応している	必要性があることを知っているが対応していない	必要性があることを知らない	わからない
5	4	3	2	1

Q108　ＩＣカード等で、建物・サーバ室・システムへのアクセスを一元的に管理する仕組みがあります。導入していますか。あてはまるところに一つだけ○を付けて下さい。

全面的に導入している	一部導入している	必要だと思うが導入していない	必要性を感じない	わからない
5	4	3	2	1

Q109　大規模災害時に重要システムの稼動を確保するため、別拠点に予備のシステムを設置し、業務を続ける対策があります。この対策をとっていますか。あてはまるところに一つだけ○を付けて下さい。

対策している	一部対策している	危険は知っているが対応していない	必要性を感じない	わからない
5	4	3	2	1

Q110　システム障害時にシステムを短時間で復旧し、業務を継続するための二重化等の対策・手順は確立していますか。あてはまるところに一つだけ○を付けて下さい。

対策している	ハードディスクのみ対策している	危険は知っているが対策していない	必要性を感じない	わからない
5	4	3	2	1

情報セキュリティ対策における人材と組織について質問します。

情報セキュリティ対策を根本から支えるのは、やはり人と組織です。組織としての仕組みと従業員の意識があってこそ、セキュリティ対策が生きてきます。

Q111　情報セキュリティについては、定期的に注意喚起を行うことが、意識向上に繋がります。定期的に従業員に情報セキュリティ教育をおこなっていますか。あてはまるところに一つだけ○を付けて下さい。

定期的に教育を行っている	教育を行ったことがある	教育は必要だが行っていない	教育が必要だと思わない	わからない
5	4	3	2	1

SQ4　その他、**情報セキュリティに関して**や本アンケートに関する意見などについて、何かございましたらご自由にお書きください。

【情報セキュリティの設問はこれで終わりです。F1(P31)へお進みください。】

貴社について質問します。

貴社名と住所をご記入いただいた方には、後日報告書と貴社の「状況分析結果」をお送りさせていただきます。ご記入くださいますよう、よろしくお願いいたします。

F1 貴社名をご記入ください。**任意**

F2 貴社の所在地をご記入ください。**任意**

〒

F3 貴社の業種をお選びください。当てはまるものをひとつだけ選び○印をつけてください。

1. 製造業	4. 建設業
2. サービス業	5. 卸・小売業
3. 運輸業	6. その他(　　)

F4 貴社の資本金と年商をご記入ください。

資本金	百万円	**年商**	百万円

F5 貴社の従業員数（パート・アルバイト含む）をお答えください。

	人

F6 貴社の従業員の年齢構成をお答えください。分かる範囲で結構ですので大体の人数をお答えください。

20 代以下	**人**	**30 代**	**人**	**40 代**	**人**	**50 代以上**	**人**

F7 貴社の情報システムを担当している人員の人数と、社内にある PC の台数をお答えください。

専任担当者	人	**兼任担当者**	人	**PC 台数**	台

F8 貴社の情報システムに対する投資額は、貴社の売上の何%程度ですか。

売上における情報システム投資の割合	%程度

F9 アンケートにご回答いただいた方には、サポートサービス委員会にて作成した診断ツールを使用し、同委員会より貴社の「状況分析結果」をご提供させて頂きたいと考えております。不要な場合は、下記のチェック欄にチェックをつけて付けて下さい。

☐ 状況分析結果の送付を希望しない

アンケートは以上で終了です。ご協力ありがとうございました。

付録　−面接調査に関する質問−

面接調査に関する質問

	質問	回答候補
A	●安全・安心の情報システム化のための、運用強化・セキュリティ対策に取り組まれたきっかけ（動機）について教えて下さい。	①経営者の指示で ②情報システム部門や現場部門の提案で ③得意先・取引先からの指導で ④外部監査等の指摘で ⑤その他（　　） 指示・指導を受けた相手によっての成否の違いは ⇒ある　　ない ある場合の順序は？
B	●運用強化・セキュリティ対策に取り組まれた主目的について教えて下さい。	①取引や業務をスムースに進める（廻す）情報システム障害防止 ②コンプライアンス強化（個人情報保護・内部統制化） ③機密情報漏洩・情報改竄・情報盗難対策 ④顧客・取引先との取引条件 ⑤企業姿勢の強化 ⑥質問表の運用の回答選択肢にある、標準化の必要性や定着のための指標による管理の 必要性に対する考え方の重要性の認識 ⑦その他（　　）
C	●目的の達成度合いや効果・成果・満足度等について教えて下さい。	①障害が激減し、取引や業務に支障がなくなり、効果はあった ②ウイルス侵入・情報漏洩・情報盗難等がなくなった ③顧客・取引先からの信用度・信頼度が向上し売上が伸びた ④投資の割りに効果が今一歩である ⑤満足度は10点満点中（全体　点位／運用　点位／セキュリティ　点位） ⑥その他（　　）
D	●苦労した点について教えて下さい。	①詳しい・分かる人材がおらず、育成や採用に苦労した ②内部統制のための基準・規定作りに苦労した。 ③情報の取り扱いや報告等、社員への締め付けを厳しくし、コンプライアンスに対する教育・研修 の義務化も課したので、不満が続発した。 ④何処まで、どのレベルまで対策を行なえば良いのかが分からず、当社の事情を理解し、的確なアドバイスしてくれる業者見つけるのに時間を要した。 ⑤対策のプライオリティ付けや対策ステップの確立と資金調達 ⑥経営者の説得 ⑦その他（　　）
E	●工夫した点について教えて下さい	①経営者への情報システムの重要性についての啓蒙に成功 ②事件・事故等の情報を集め、障害時や情報漏洩等の損害についてのシミュレーションを実施した ③障害時やトラブル時の問い合わせ体制設置を行い、社員の不安心理を低減化した ④障害時やトラブル時の状況を記録・分析し、以降の発生時の復旧時間を短縮し効果拡大に繋げた ⑤その他（　　）
F	●経営者の反応・社員の反応について教えて下さい	①社員の反応は良い　⇔　面倒なことをさせるということで不満がある ②経営者の反応は良い　⇔　お金が掛かった割りに効果が見えず不評 ③その他（　　）
G	●現状の課題・問題点を教えて下さい	①今後の対策ステップを、投資対効果の観点でどう進めたら良いのかが課題 ②対策予算の確保が課題 ③効果が不明で、経営者層の不満が大きく今後の対策の進め方が課題 ④現場社員の不満が高く、徹底が課題 ⑤コンプライアンス対応の内部統制等組織構築の進め方が課題 ⑥ITIL等の国際基準への対応が課題 ⑦その他（　　）
H	●JCSSAへの期待について教えて下さい	①よく知らない　②中小企業経営安定化のための国への働き掛け強化 ③販売店の指導強化　④その他（　　）
I	●業者・業界への期待について教えて下さい	①技術力強化　②提案力強化 ③サポートサービス力強化　④コンサル力強化 ⑤その他（　　）

中堅・中小企業のＩＴサービスメニューに関する調査研究

発行　社団法人　日本コンピュータシステム販売店協会
東京都文京区湯島 1-9-4　鴫原ビル 2 階
電話　03-5802-3198　http://www.jcssa.or.jp
発行日　平成 20 年 3 月