

企業における情報セキュリティガバナンスの
あり方に関する研究会 報告書
参考資料

情報セキュリティ対策の取組状況に関する
アンケート調査結果

1. 調査概要

情報セキュリティ現在の対策の相場観を明らかにしてベンチマークを設定するため、経済産業省は企業を対象とする情報セキュリティ対策の取組み状況についてアンケートを行った。

(1) 発送・回収件数

< 発送 >

大手企業(300人以上)	3,024社(上場企業を中心に抽出)
中小企業(300人未満)	3,000社(非上場企業を中心に抽出)
合計	6,024社

< 回収 >

大手企業(300人以上)	953社(回収率 31.5%)
中小企業(300人未満)	680社(回収率 22.7%)
合計	1,633社(回収率 27.1%)

(2) 調査時期

2005年1月

(3) 調査方法

郵送方式

1. 調査概要

情報セキュリティ対策の相場観を明らかにして、対策ベンチマークの「望まれる水準」を導出するため、企業を対象とする情報セキュリティ対策の取組み状況に関するアンケートを実施した。

(1) 発送・回収件数

< 発送 >

大手企業(300人以上) 3,024社(上場企業を中心に抽出)
中小企業(300人未満) 3,000社(非上場企業を中心に抽出)
合 計 6,024社

< 回収 >

大手企業(300人以上) 953社(回収率 31.5%)
中小企業(300人未満) 680社(回収率 22.7%)
合 計 1,633社(回収率 27.1%)

(2) 調査時期

2005年1月

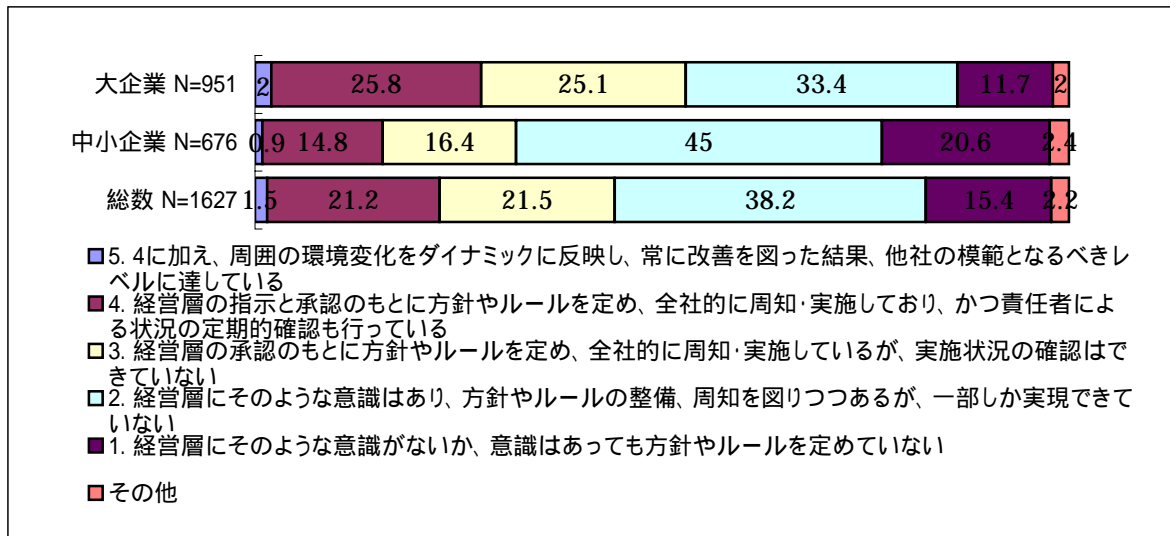
(3) 調査方法

郵送方式

問1 貴社における情報セキュリティに対する組織的な取り組み状況についてうかがいます。

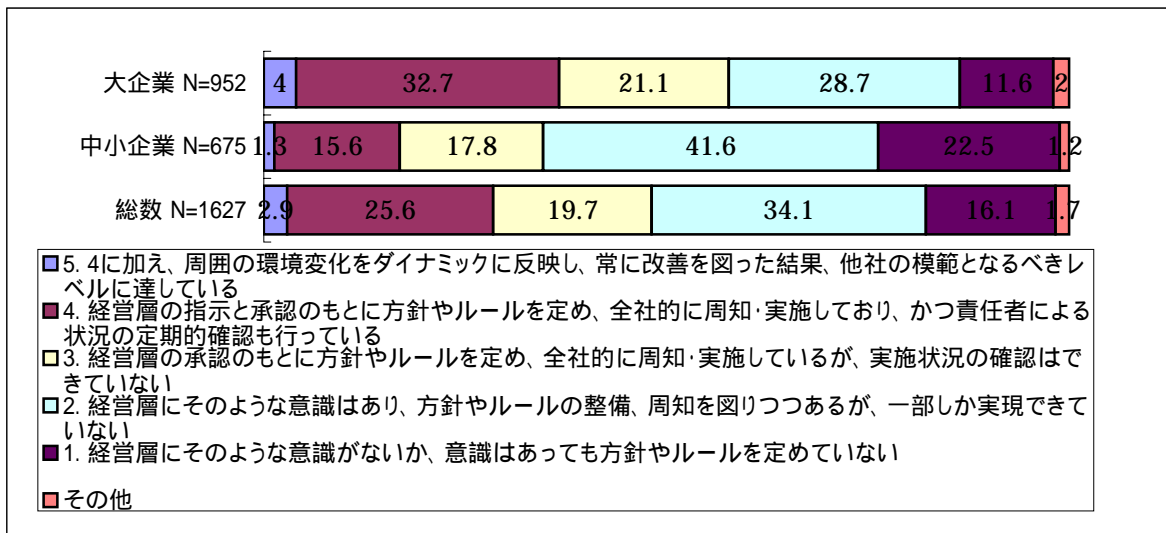
以下の ~ のそれぞれの設問について、選択肢の中からもっともあてはまる回答欄の番号に をつけてください。

貴社では、情報セキュリティポリシーや情報セキュリティ管理に関する規程を定め、それを実践していますか。自社の状況に見合った規程とするためには、サンプルのコピーではなく、自社の事業やリスクを鑑みたものであることが重要です。



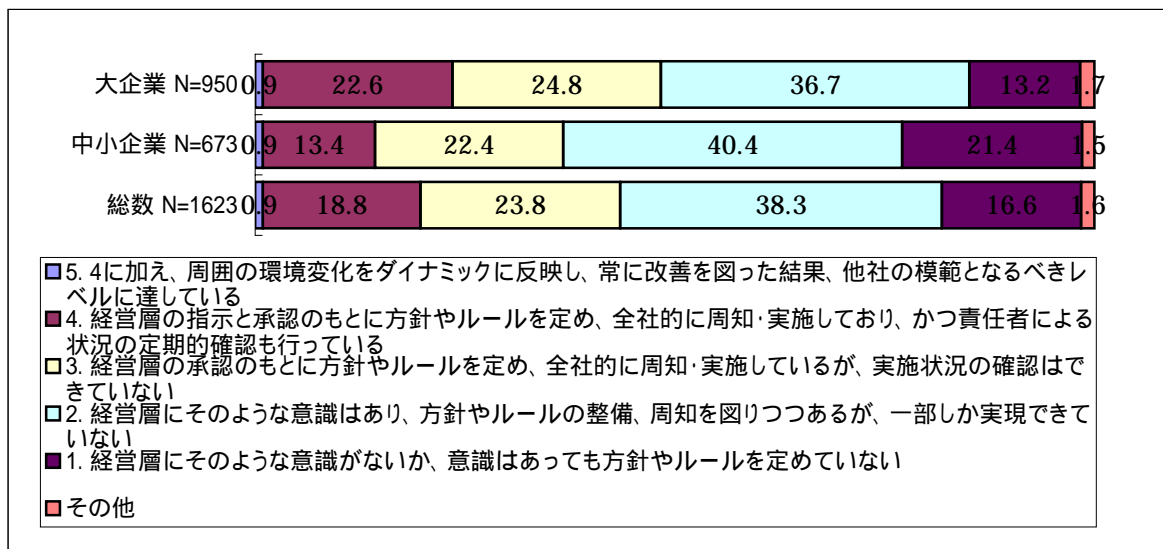
問1

貴社では、経営層を含めた情報セキュリティの推進体制やコンプライアンス(法令遵守)の推進体制を整備していますか。推進体制の整備のためには、監査を含めた各担当者の責任が明文化されることが重要です。



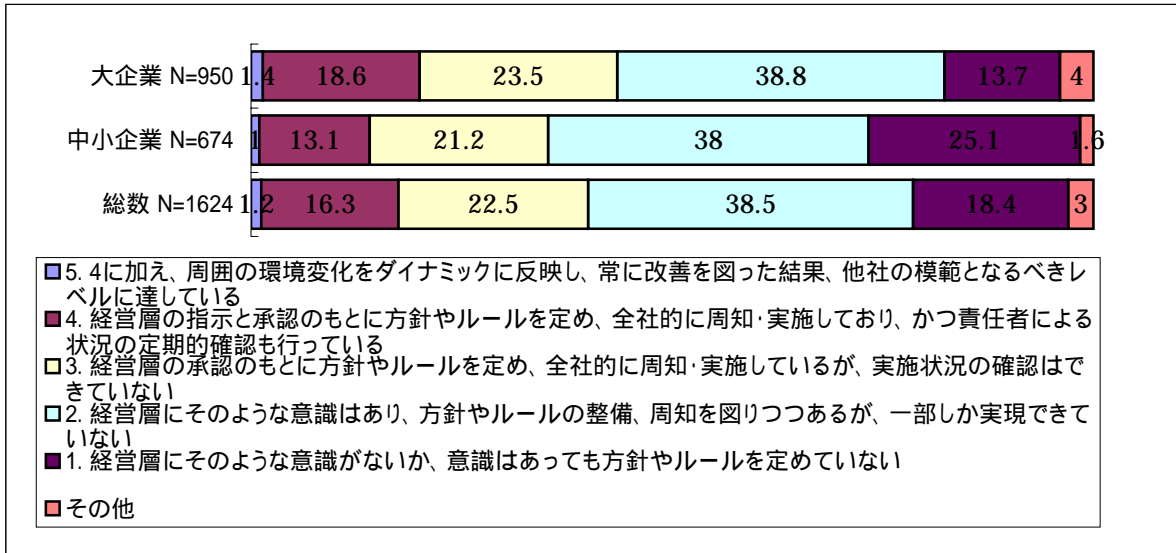
問1

貴社では、重要な情報資産(情報および情報システム)については、重要性のレベルごとに分け、そのレベルに応じて管理していますか。



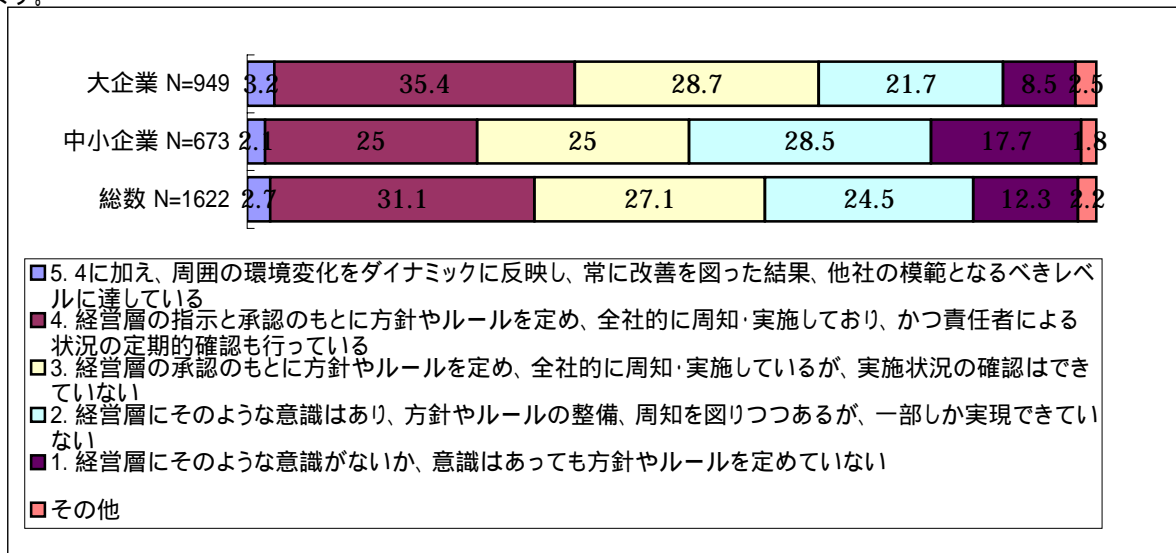
問1

貴社では、個人データなど重要な情報については、取得、利用、保管、開示、消去などの一連の業務工程ごとにきめ細かく適切な措置を講じていますか。適切な措置とは、作業責任者や手順の明確化、取扱者の限定や処理の記録、確認などを指します。



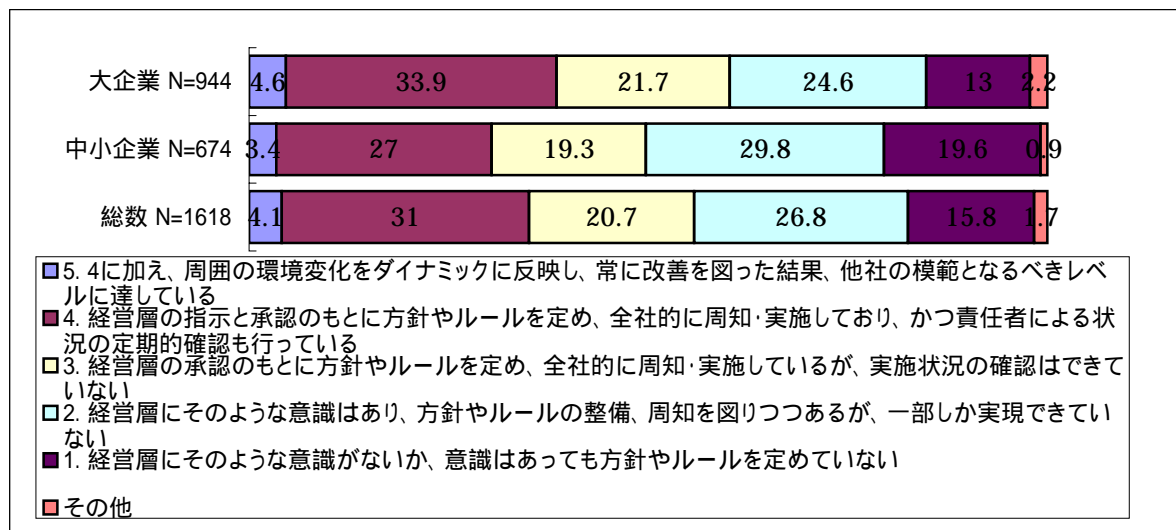
問1

貴社では、社外の組織に業務を委託する際の契約書に、セキュリティ上の理由から相手方に求めるべき事項を記載していますか。セキュリティ上の理由とは、データの漏洩や消失、情報あるいは情報システムの誤用などをさします。



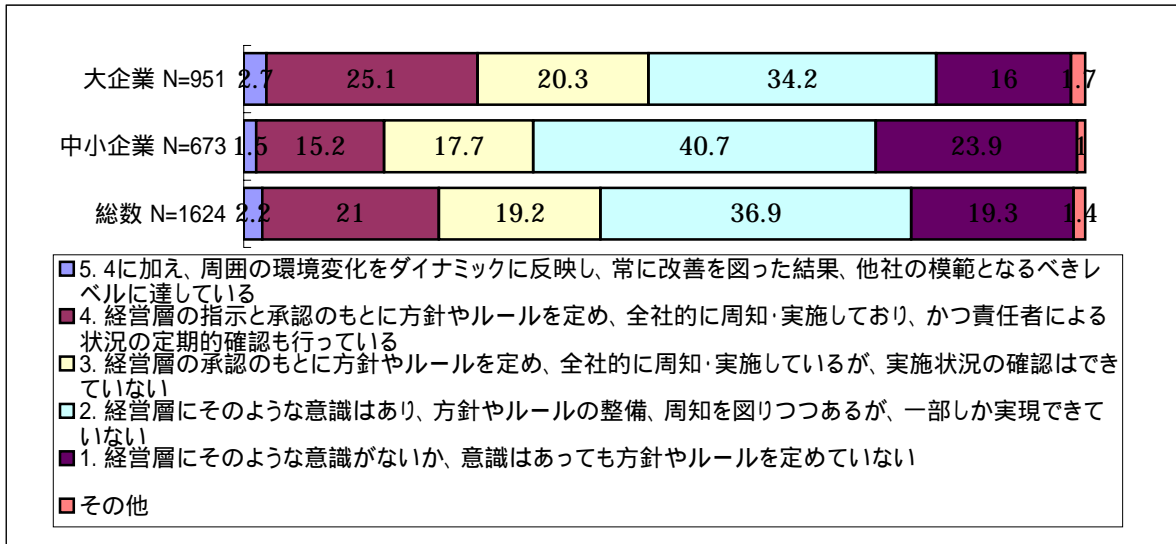
問1

貴社では、従業者(派遣を含む)に対し、入社、退職の際に機密保持に関する書面を取り交わすなどして就業上のセキュリティに関する義務を明確にしていますか。

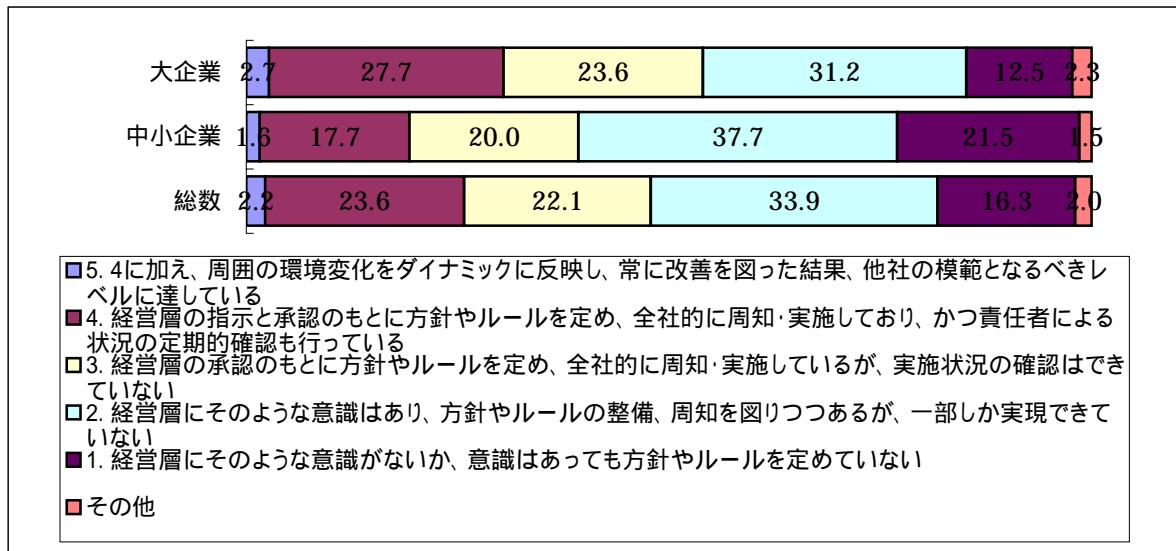


問1

貴社では、従業者(派遣を含む)に対し、情報セキュリティに関する貴社の取り組みや関連ルールについての計画的な教育や指導を実施していますか。

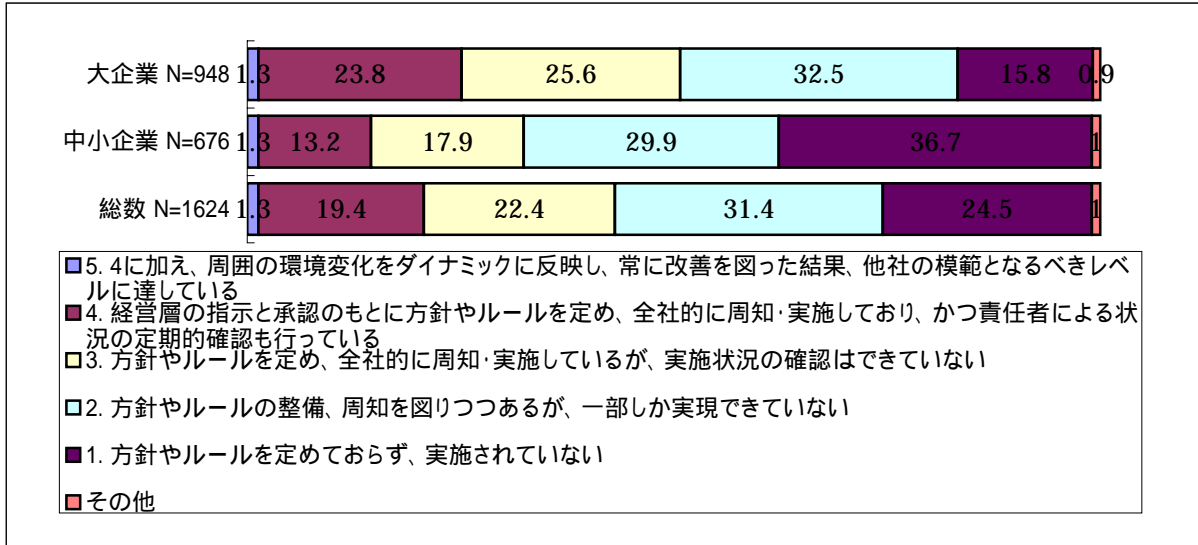


問1 ~ の平均



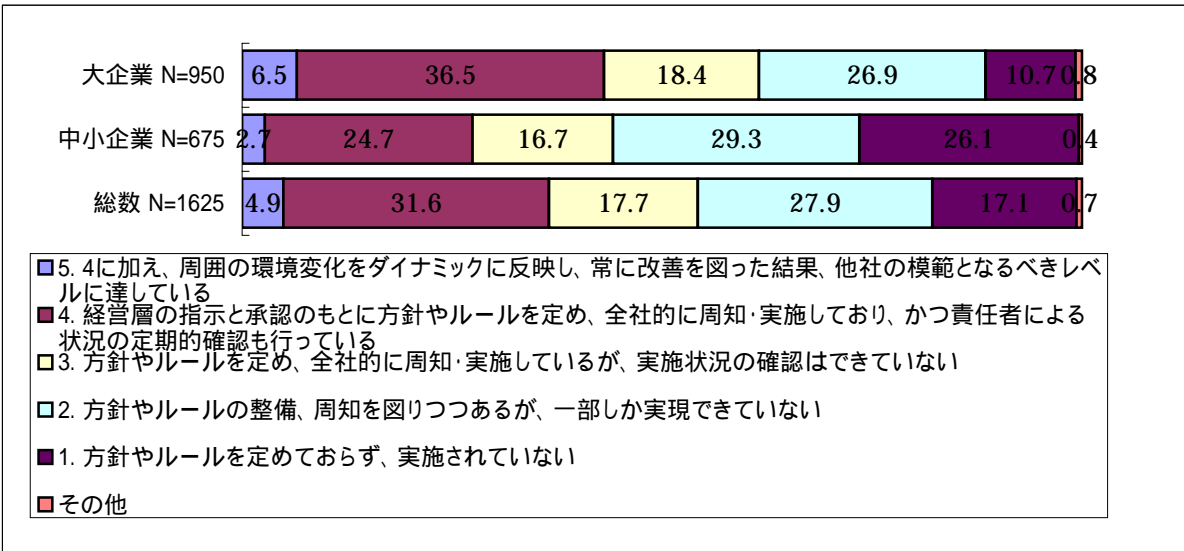
問2 貴社における物理的(環境的)セキュリティ上の施策についてうかがいます。以下の ~ のそれぞれの設問について、選択肢の中からもっともあてはまる回答欄の番号に をつけてください。

貴社では、ベンダーや清掃業者など貴社に出入りする様々な人々に対するセキュリティ上のルールを定め、それを実践していますか。



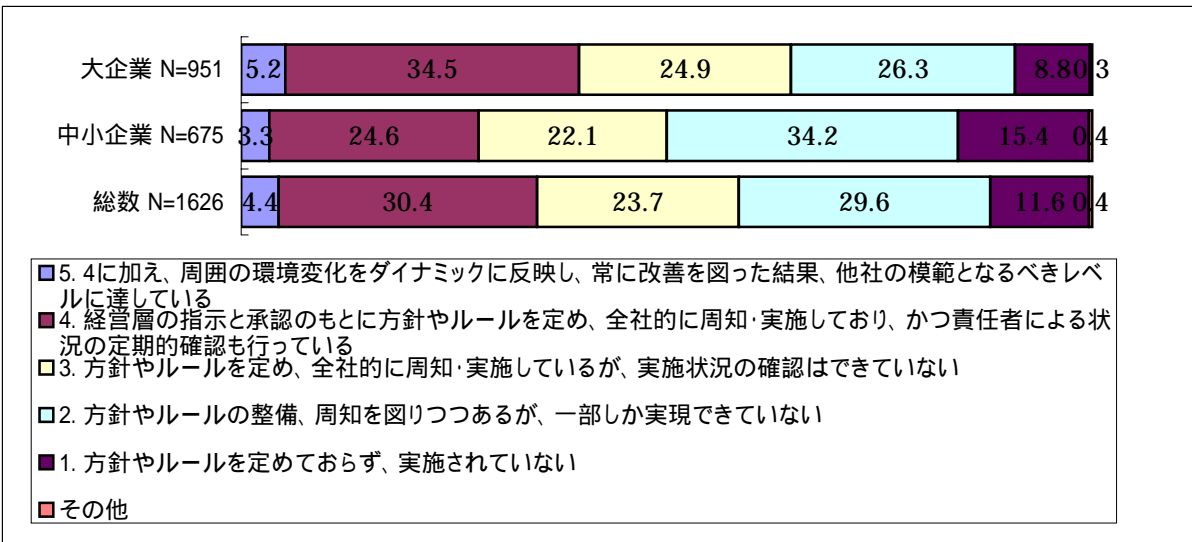
問2

貴社では、特にセキュリティを強化したい建物や区画について、必要に応じたセキュリティ対策を実施していますか。対策には、外部とのセキュリティ上の境界を明確に意識した入退館・入退室管理や警報装置の設置などがあります。



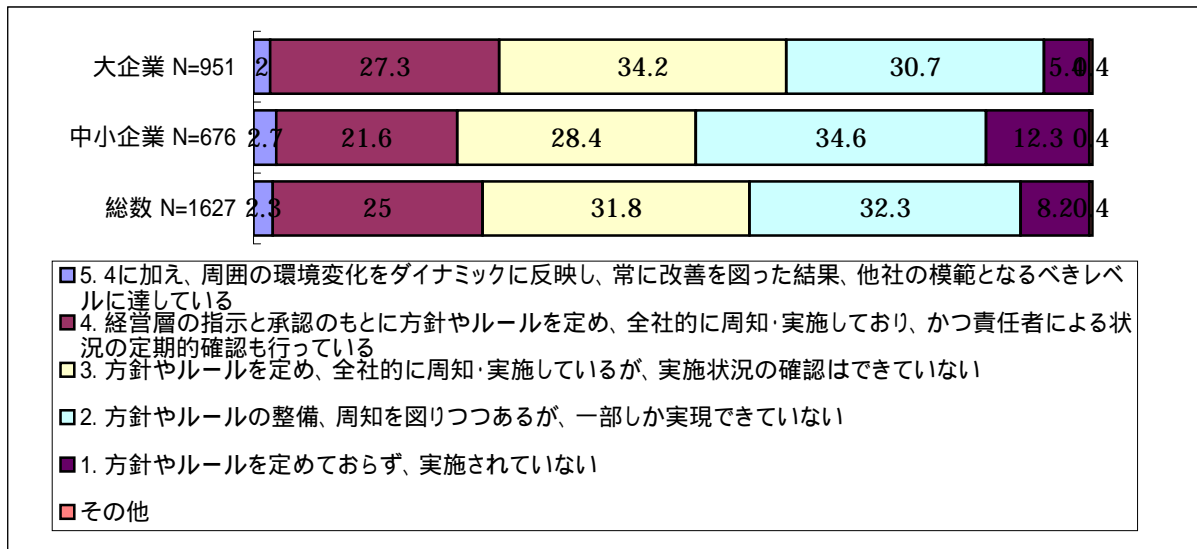
問2

貴社では、重要な情報機器や配線等は、安全性に配慮して配置・設置していますか。安全性に配慮した配置・設置とは例えば、人目につかない場所への設置、配線類の地下や床下への配置、浸水等を考慮した配置などを言います。



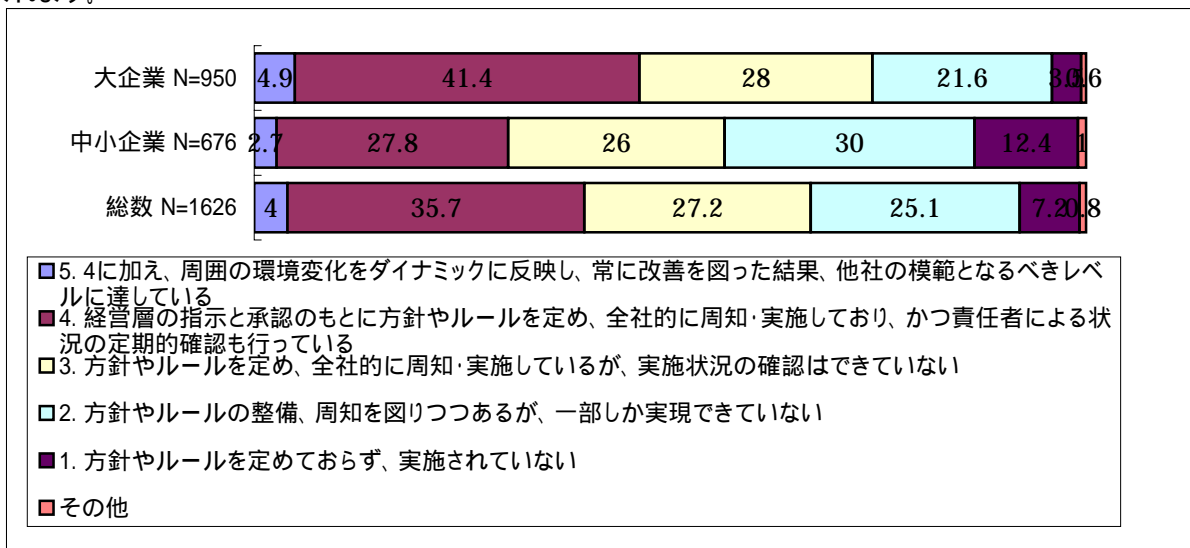
問2

貴社では、重要な書類や記憶媒体の適切な管理を行っていますか。
適切な管理とは例えば、キャビネットの施錠やプリント出力の放置禁止、記憶媒体の粉碎廃棄などを言います。

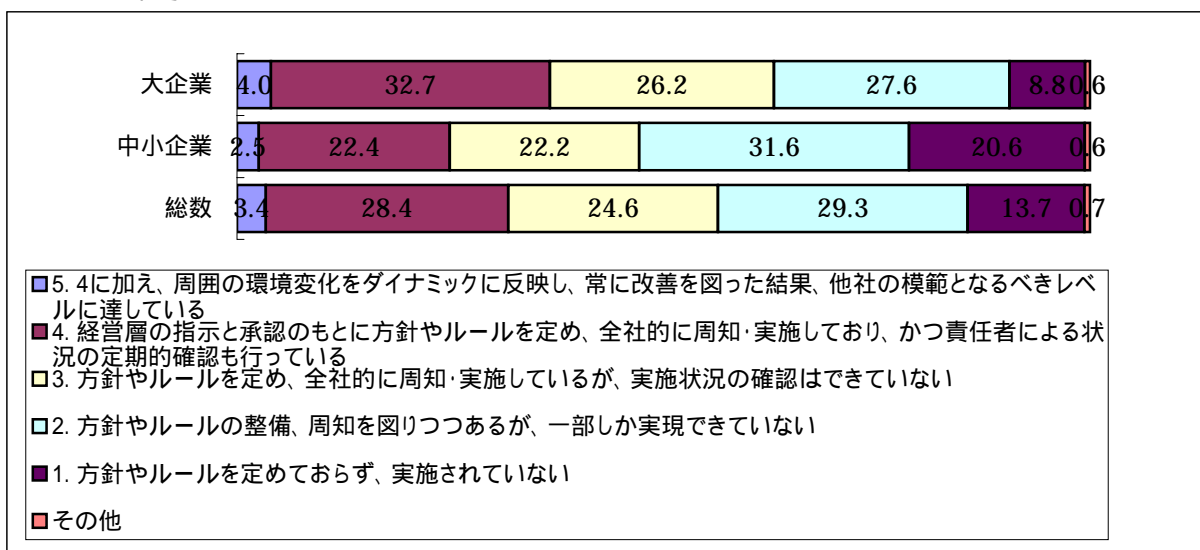


問2

貴社では、実稼働環境の情報システム（本番環境）やデータ（本番データ）を適切に保護していますか。
適切な保護には、実稼働環境と開発環境の分離、変更管理手順の策定、開発での本番データの使用制限などが含まれます。

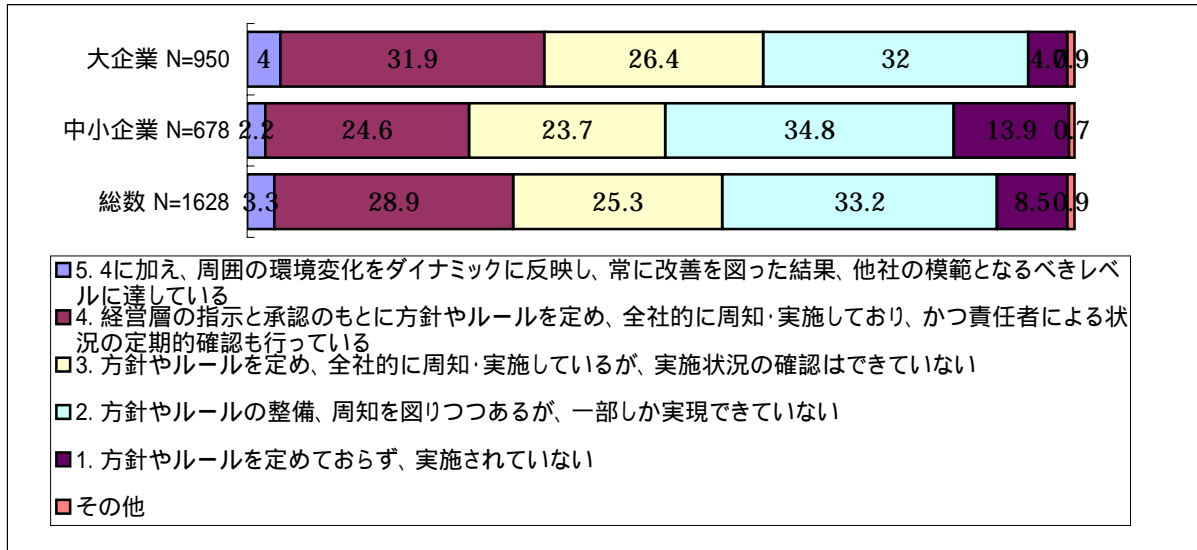


問2 ~ の平均



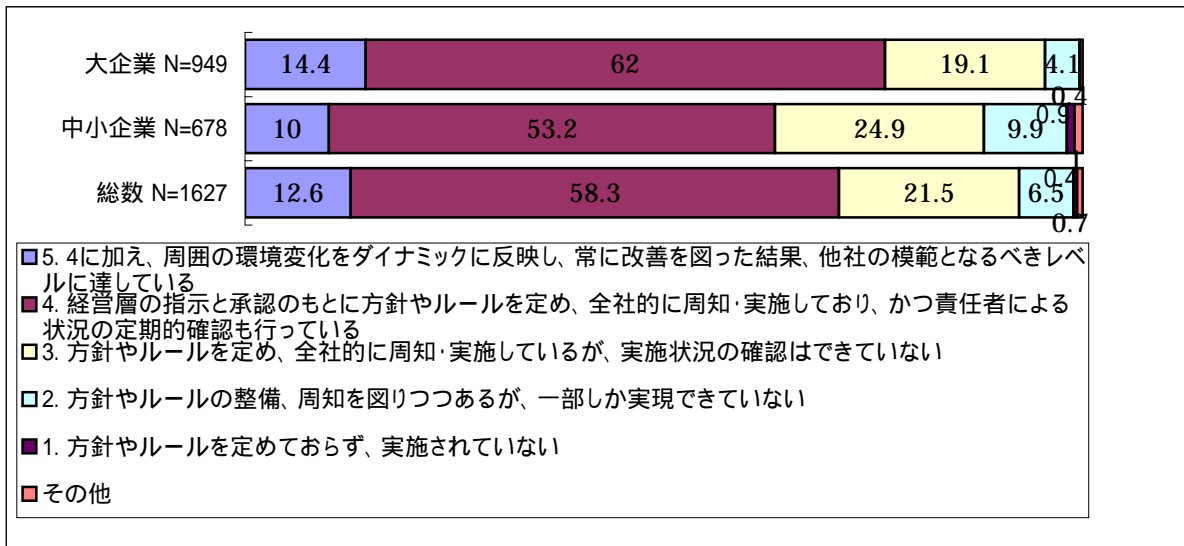
問3 貴社における通信ネットワークおよび情報システムの運用管理に関するセキュリティ対策についてうかがいます。
以下の ~ のそれぞれの設問について、選択肢の中からもっともあてはまる回答欄の番号に をつけてください。

貴社では、情報システムの運用に必要なセキュリティ対策を実施していますか。必要とされるセキュリティ対策には、セキュリティ要件の明確化、各種手順書の策定、セキュリティログの記録とチェックなどがあります。



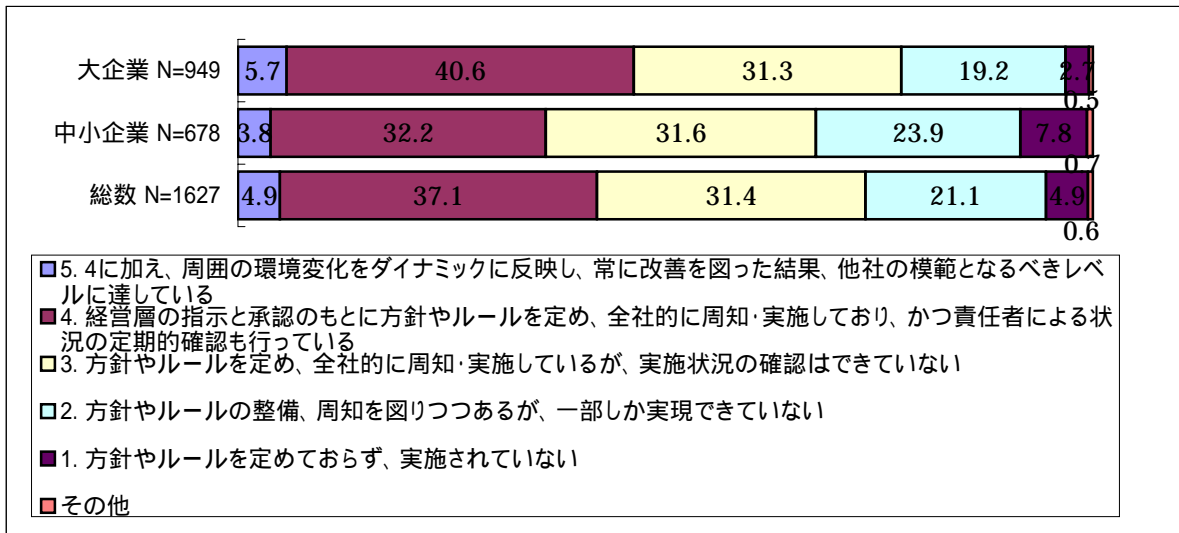
問3

貴社では、不正ソフトウェア(ウイルス、ワーム等)に対する対策を実施していますか。不正ソフトウェア対策にはコンピュータウイルス対策ソフトを導入し、パターンファイルのアップデートを適時行うことなどが含まれます。



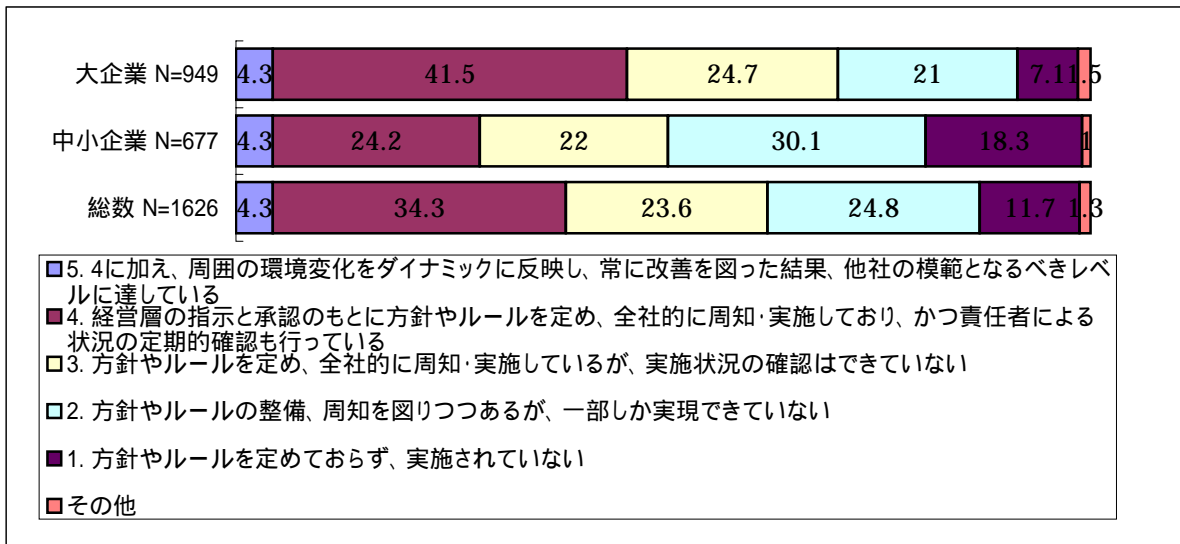
問3

貴社では、貴社で導入しているソフトウェアに対して適切な脆弱性対策を実施していますか。適切な脆弱性対策とは、セキュリティを考慮した設定や、パッチ(脆弱性修正プログラム)の適用、定期的な脆弱性検査などを言います。



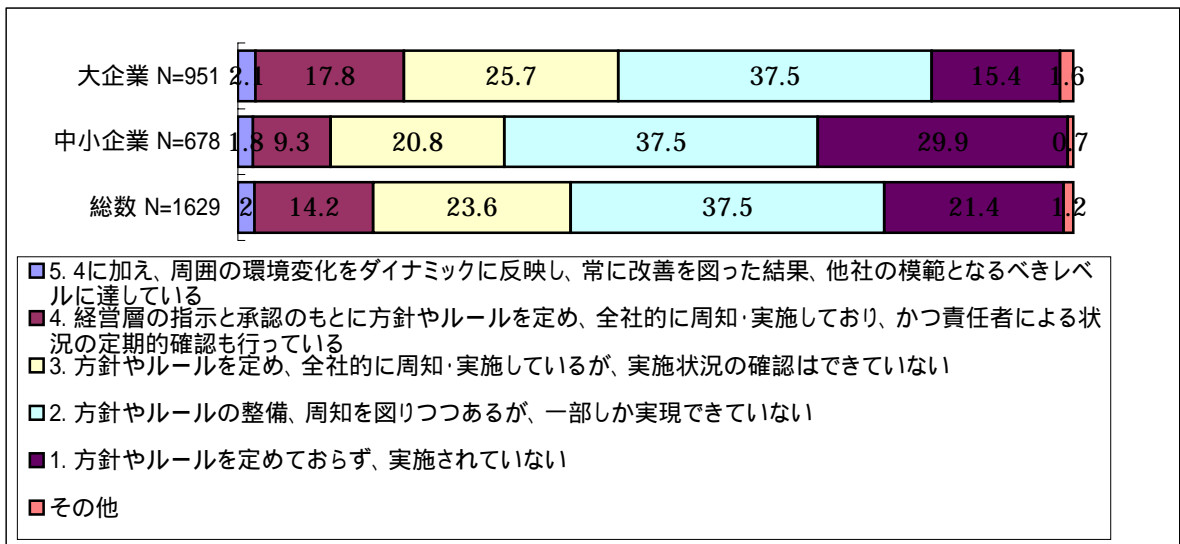
問3

貴社では、通信ネットワークに流れるデータに関して、暗号化などの適切な保護策を実施していますか。適切な保護策にはVPNの使用や、重要な情報のSSL等での暗号化が含まれます。

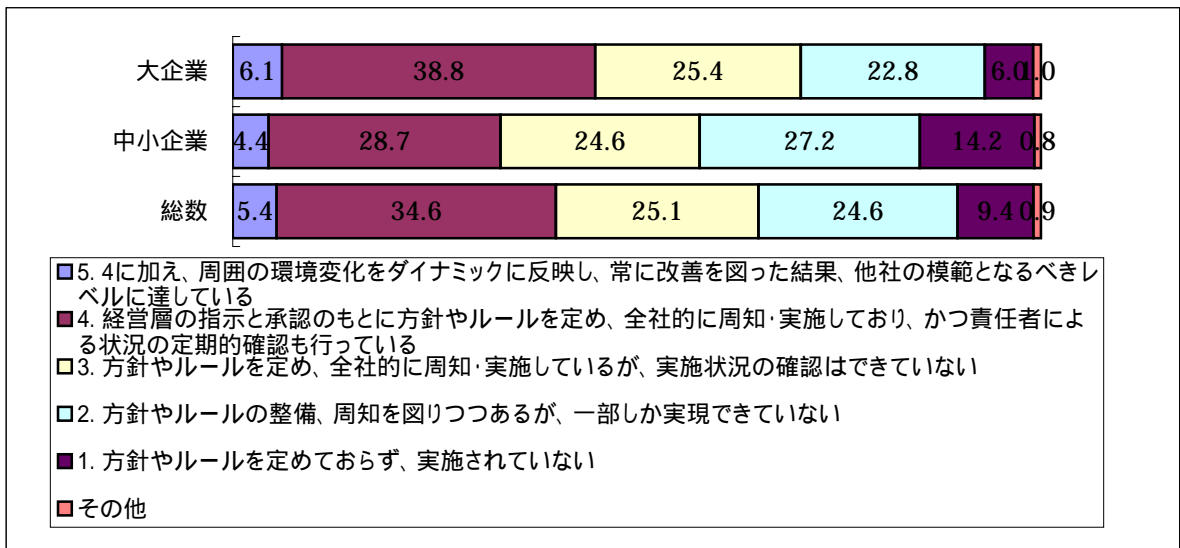


問3

貴社では、携帯PCやフロッピーディスク等の記憶媒体に対して、盗難、紛失等を想定した適切なセキュリティ対策を実施していますか。携帯PCやフロッピーディスク等の記憶媒体の使用場所には、社外のパブリックスペースやリモートオフィス、自宅などを含みます。

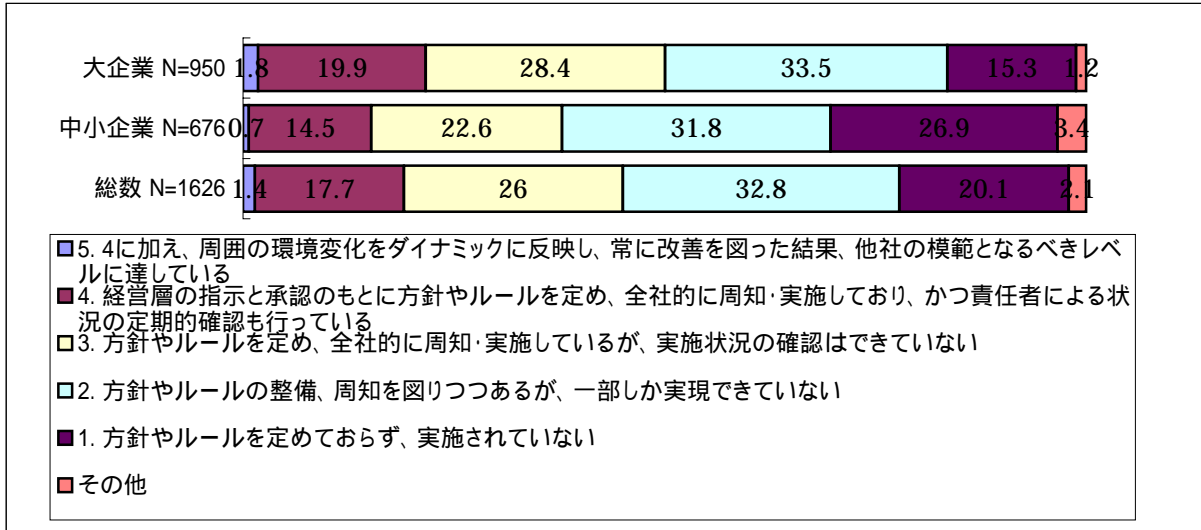


問3 ~ の平均



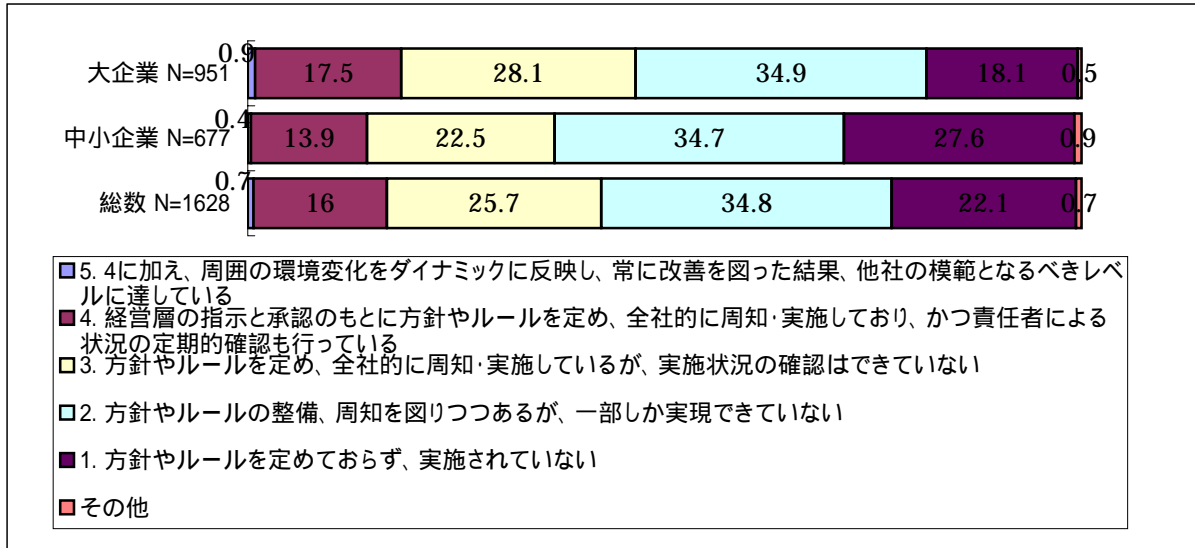
問4 貴社における情報システムの開発、保守におけるセキュリティ対策及び情報や情報システムへのアクセス制御の状況についてうかがいます。以下の ~ のそれぞれの設問について、選択肢の中からもっともあてはまる回答欄の番号に つけてください。

貴社では、業務システムの開発に際し、開発したシステムに脆弱性が残らないようにする施策を実施していますか。施策としては、仕様書にセキュリティ上の要求事項を盛り込むことなどがあります。



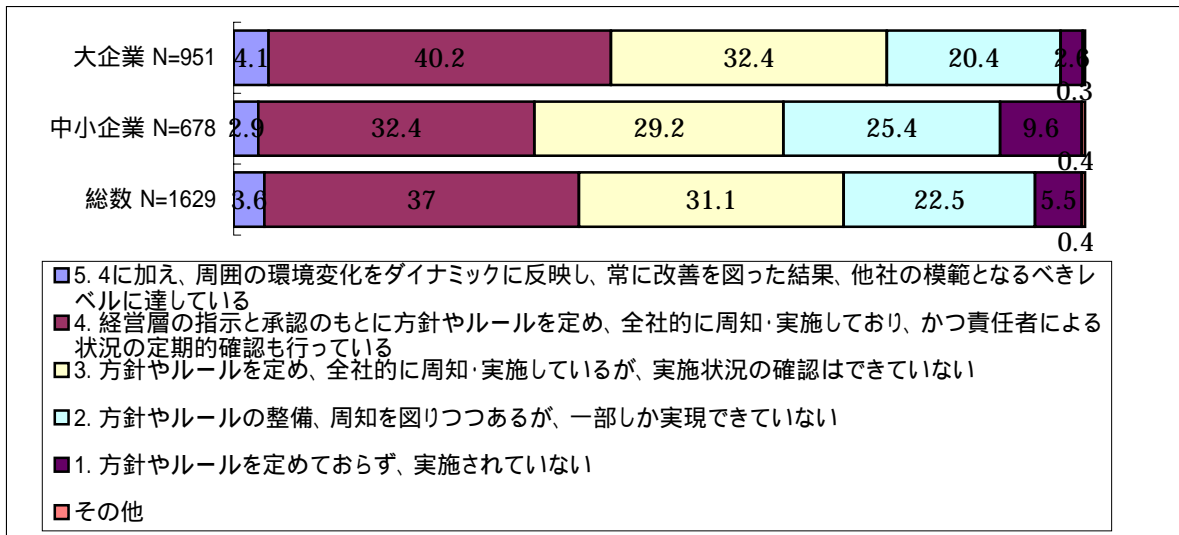
問4

貴社では、ソフトウェアの選定・購入、システムの開発・保守に際して、工程ごとにセキュリティの観点からチェックを行うなど、セキュリティ管理が実施されていますか。



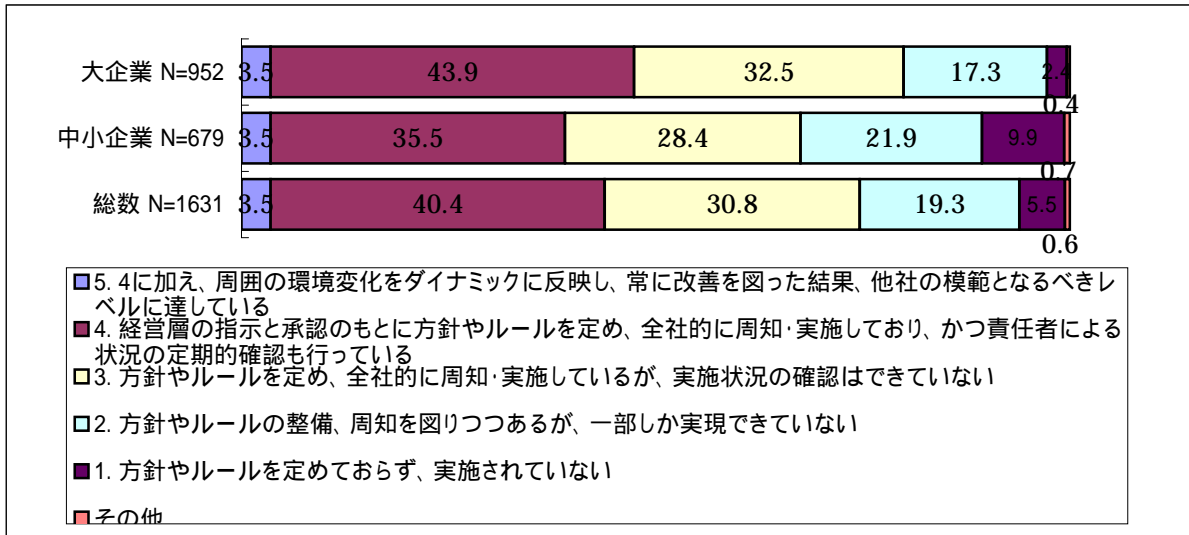
問4

貴社では、情報(データ)へのアクセスを制限するためのユーザ管理や認証を適切に実施していますか。適切なユーザ管理には、不要なユーザIDの定期的な見直しや共用IDの制限、単純なパスワードの設定禁止などがあります。



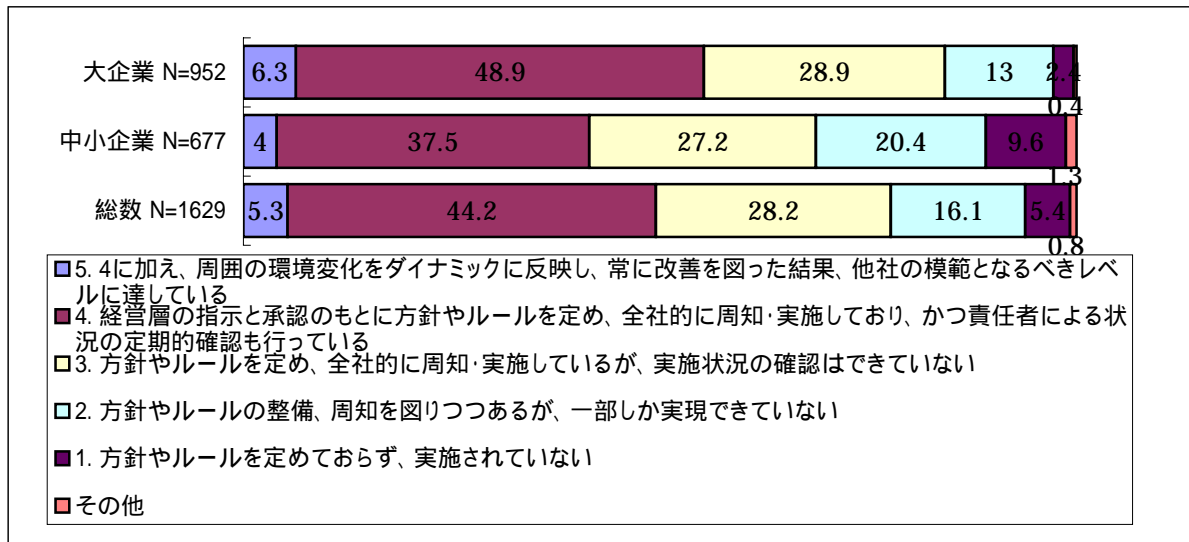
問4

貴社では、業務アプリケーションに対するアクセス制御を適切に実施していますか。
適切な業務アプリケーションに対するアクセス制御には、例えば利用者ごとに利用できる機能の制限などがあります。

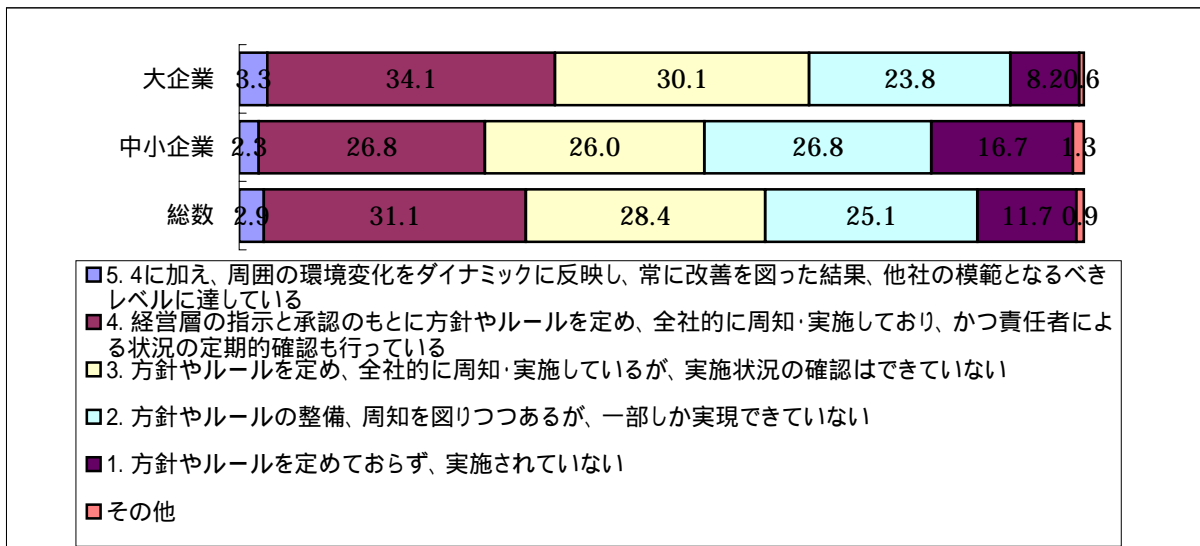


問4

貴社では、ネットワークのアクセス制御を適切に実施していますか。
適切なネットワークのアクセス制御には、例えばネットワークの分離や社外からの接続時の認証などがあります。

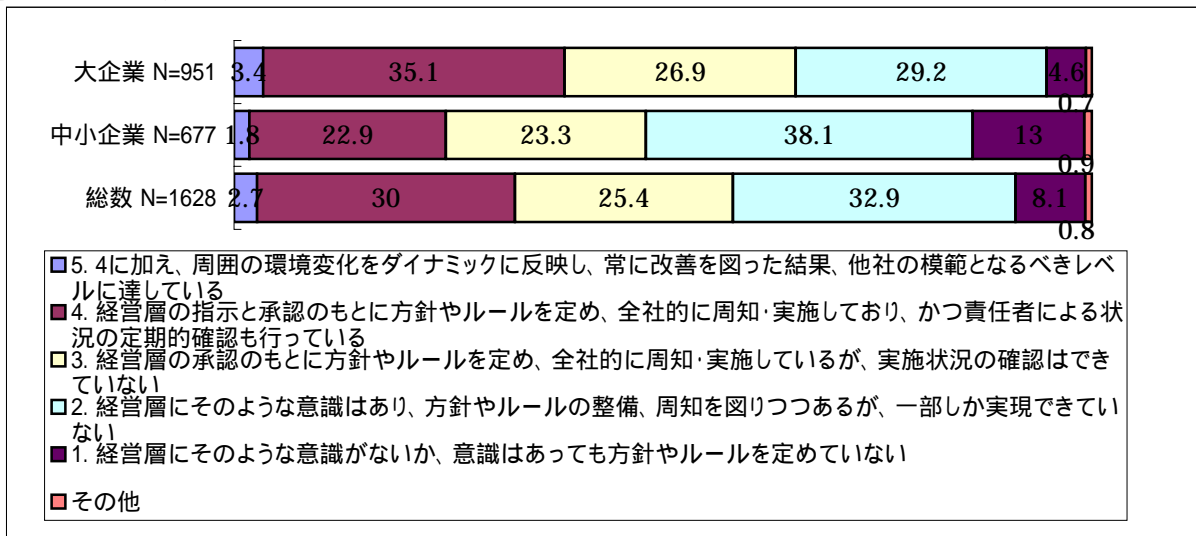


問4 ~ の平均



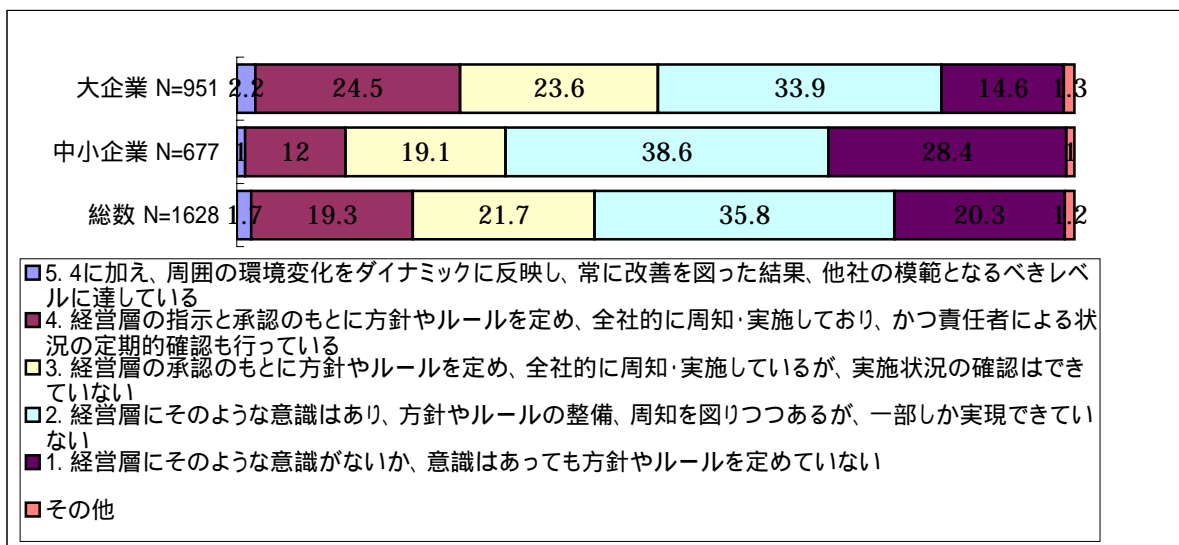
問5 貴社における情報セキュリティ上の事故対応状況についてうかがいます。以下の ~ のそれぞれの設問について、選択肢の中からもっともあてはまる回答欄の番号に をつけてください。

貴社では、情報システムの障害発生を想定した適切な対策を実施していますか。適切な対策には、例えばシステムの冗長構成やバックアップ、障害対応手順書の策定、運用記録の取得、社外委託先とのサービスレベルの合意などがあります



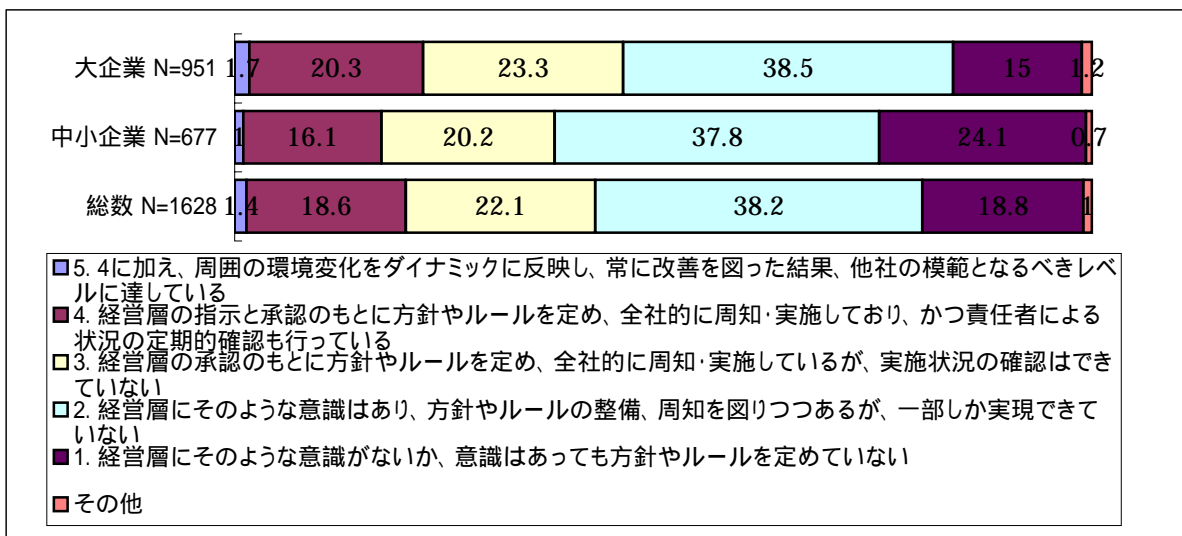
問5

貴社では、情報セキュリティに関連する事件や事故が発生した際の行動や報告、判断の基準を定めた対応手順を準備していますか。

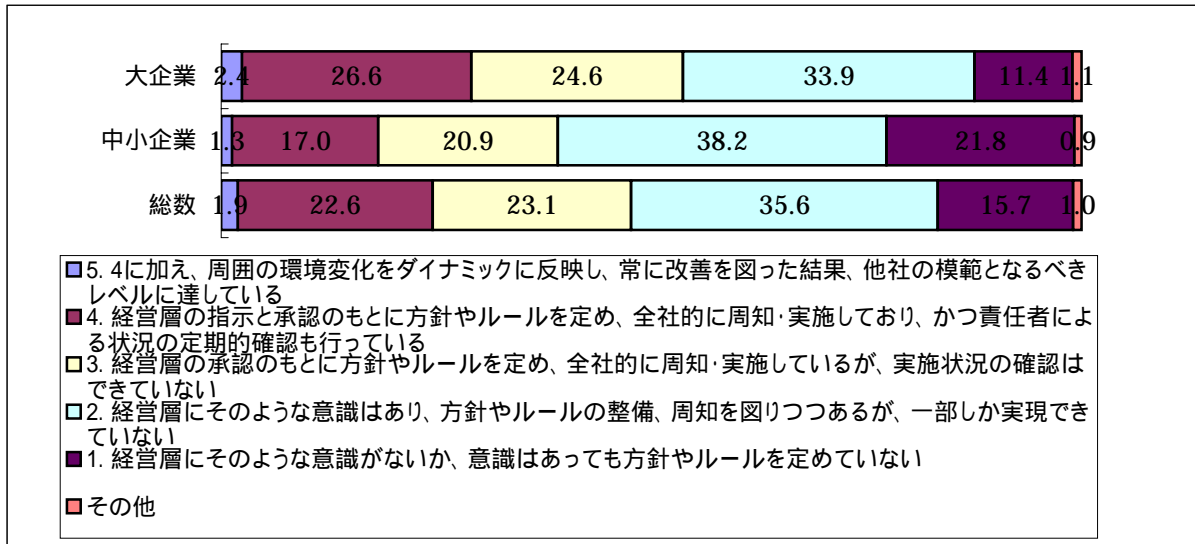


問5

貴社では、何らかの理由で情報システムが停止した場合でも事業を継続するための取り組みが、組織全体を通じて検討されていますか。

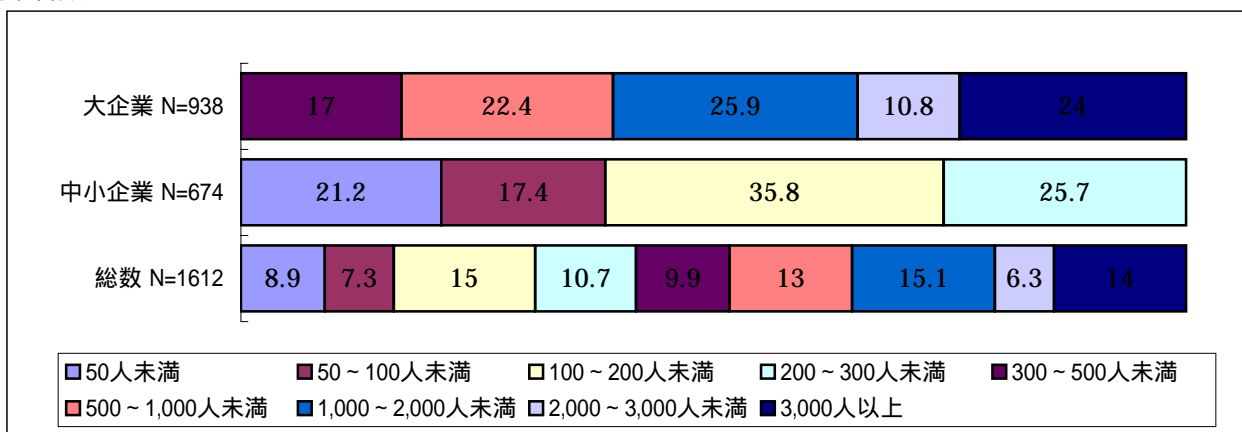


問5 ~ の平均

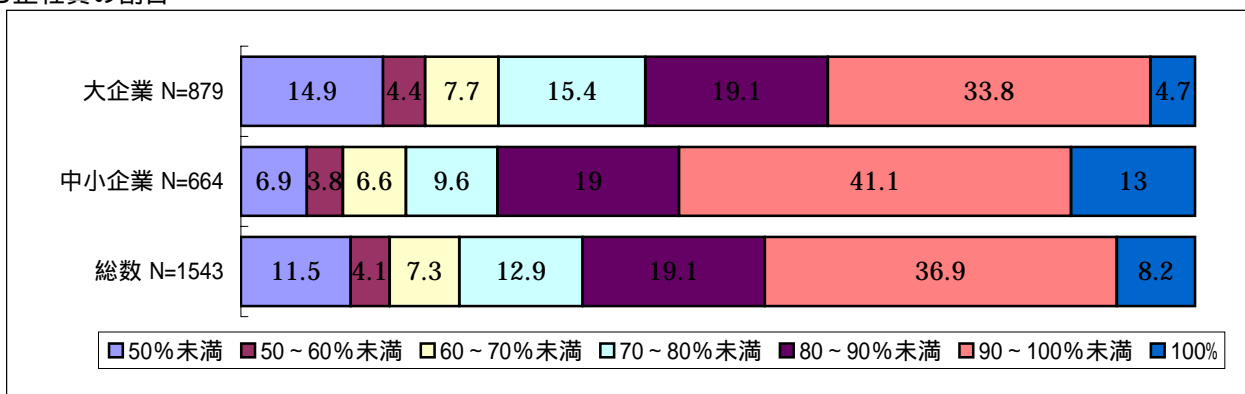


1. 貴社の従業者数(派遣、アルバイトを含む)およびそのうちの正社員の割合をお答えください。

従業者数

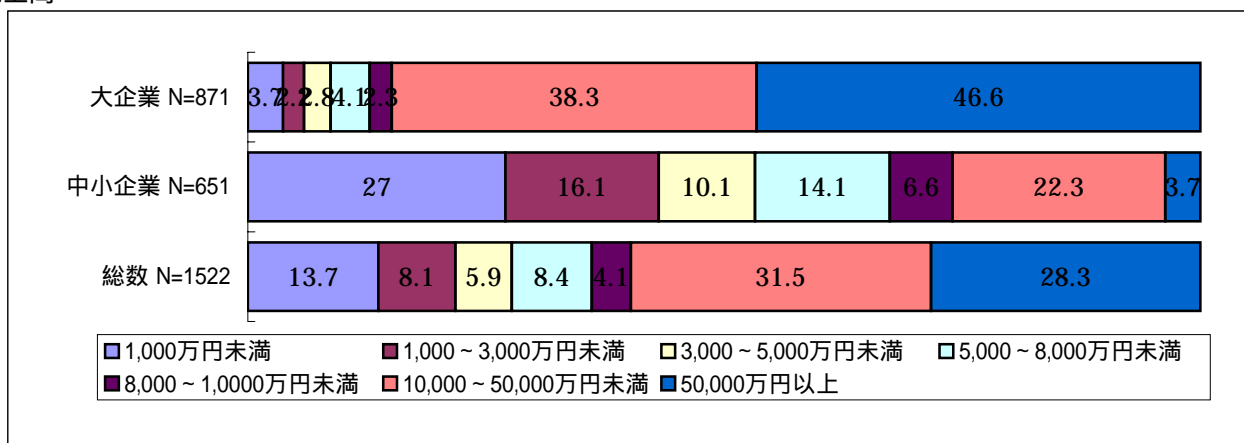


うち正社員の割合

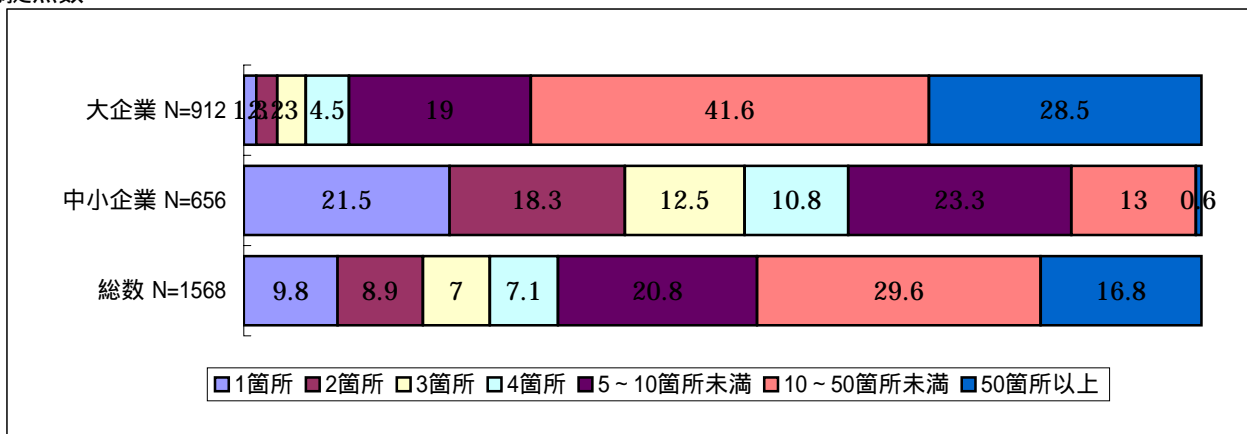


2. 貴社の売上高と国内外の拠点数(支社・支店・営業所)をお答えください。

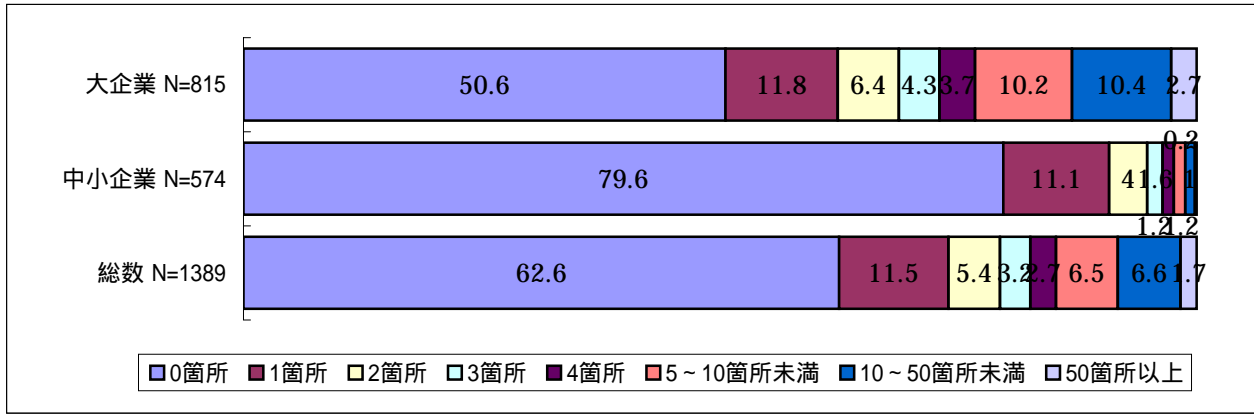
売上高



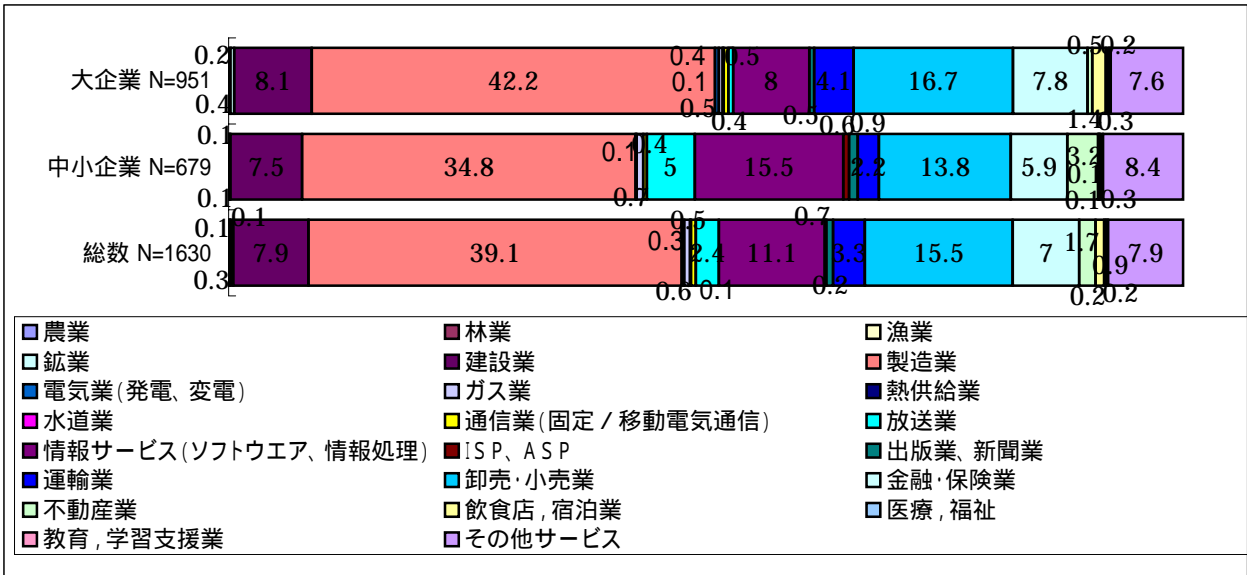
総拠点数



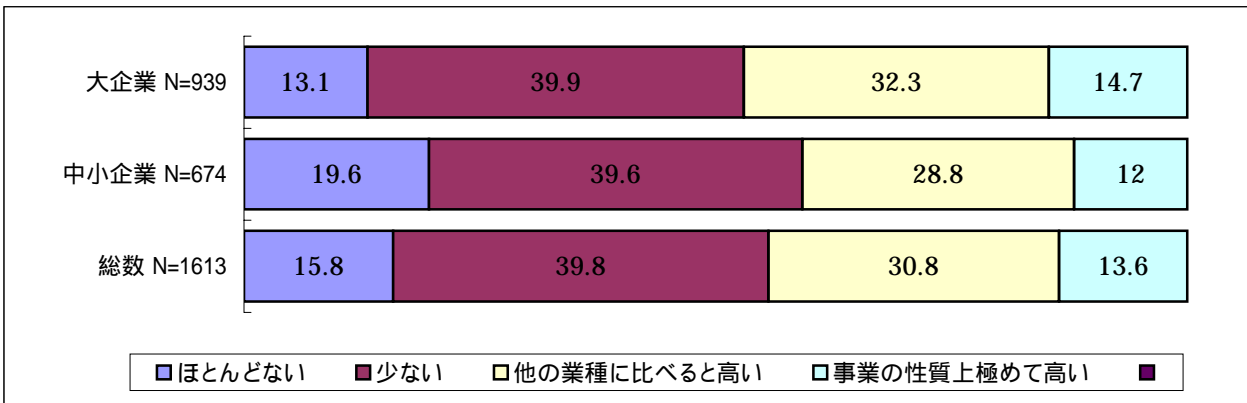
海外の拠点数



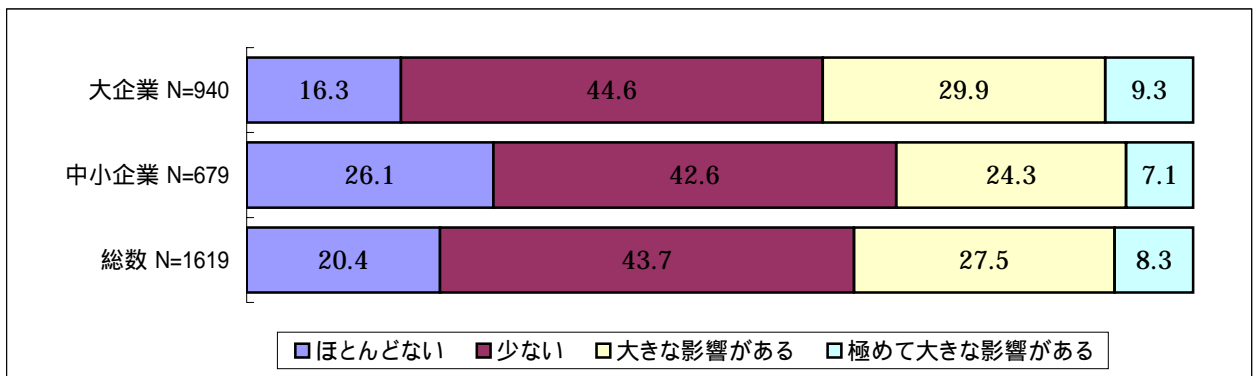
3. 貴社の業種を、以下の中からお選びください。(記号に)



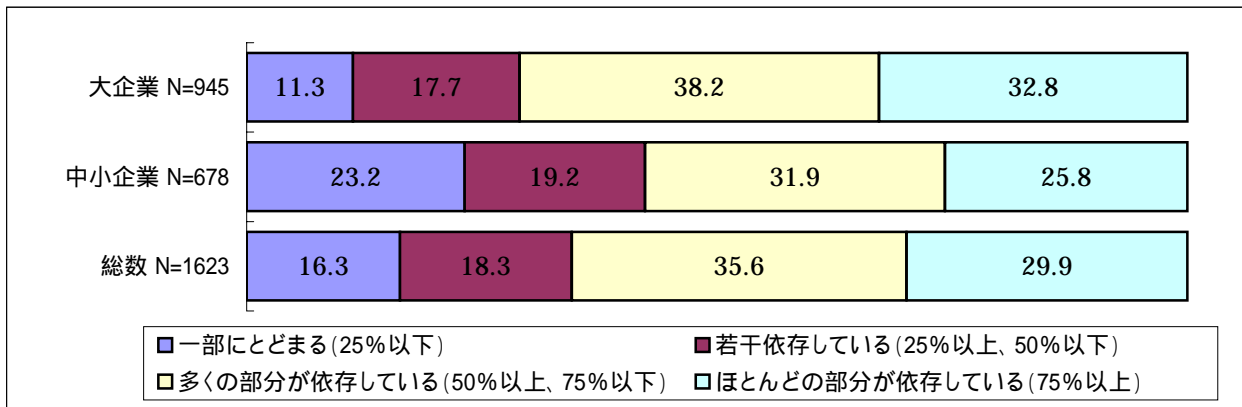
4. 貴社の事業は、国家や社会基盤、経済基盤に与える影響の観点から、どの程度の公益性がありますか。(記号に)



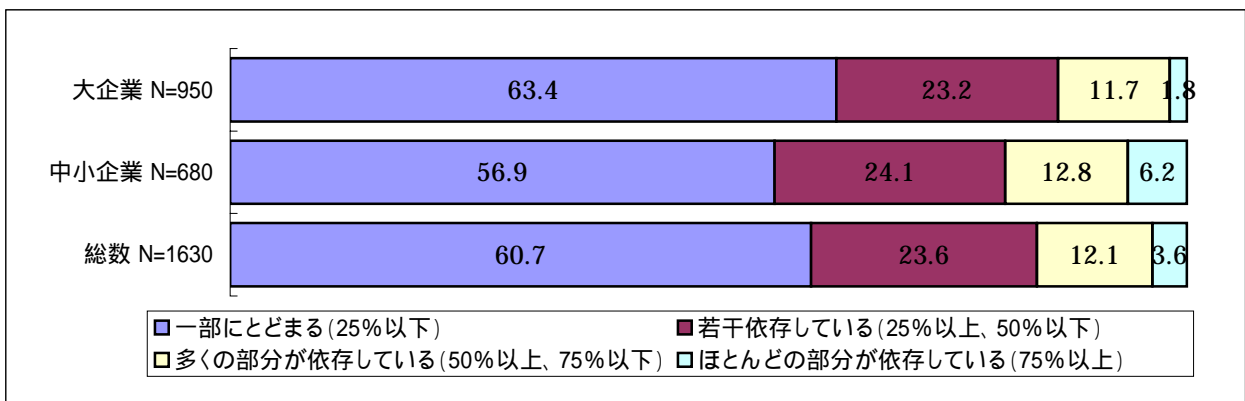
5. 貴社の事業が、顧客の生命・身体・財産・名誉等に与える影響の大きさはどの程度ありますか。(記号に)



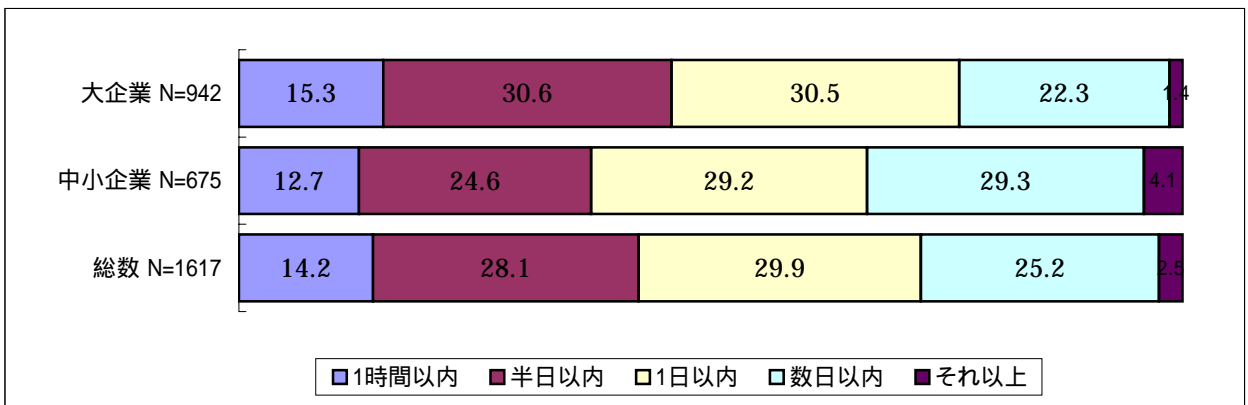
6. 貴社の主要な業務に関わる業務プロセスのうち、情報システム(社外のシステムを含む)に依存している割合はどの程度ですか。(記号に)



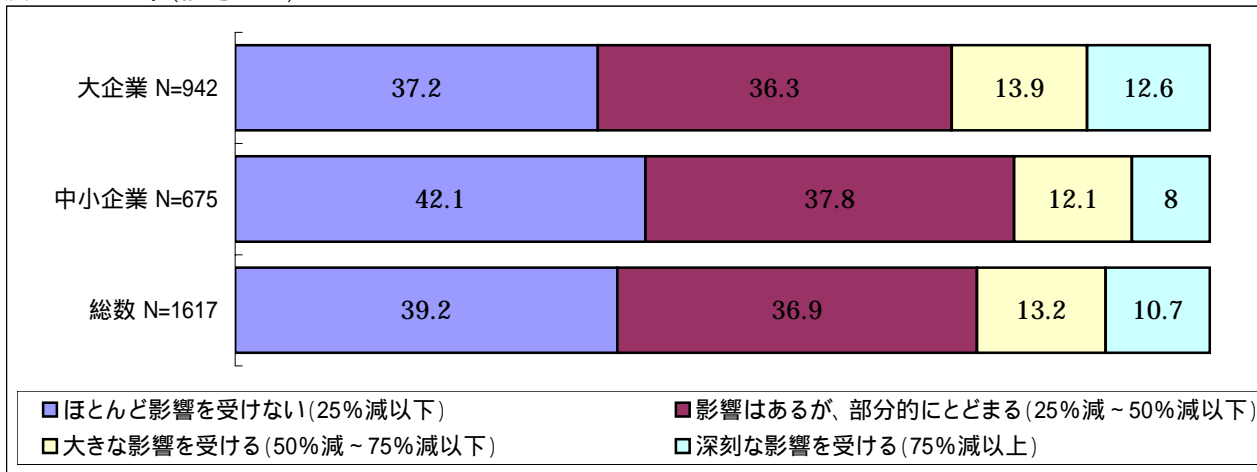
7. 貴社の主要な業務に関わる業務プロセスのうち、インターネットに依存している割合はどの程度ですか。(記号に)



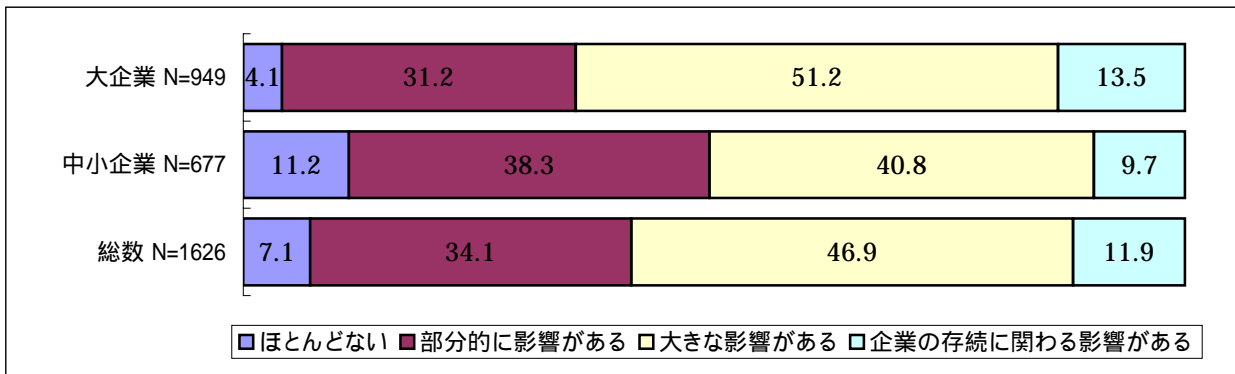
8. 貴社の主要な情報システムについて、(月間)売上高に影響を及ぼさないで済む、許容停止時間はどれぐらいですか。(記号に)



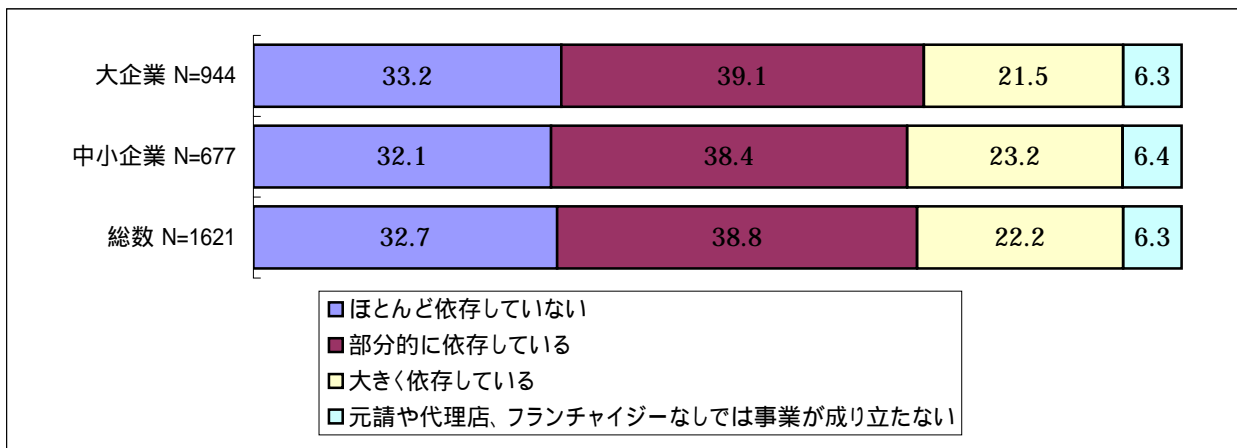
9. 貴社の主要な情報システムが営業日に「24時間」停止した場合、貴社のその日の売上高にどの程度の影響を及ぼしますか。(記号に)



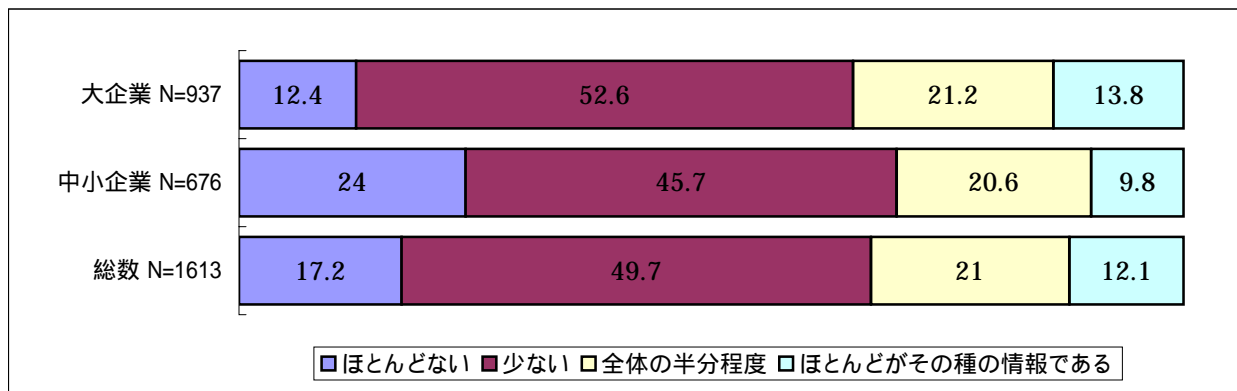
10. 個人情報漏洩等、情報セキュリティ関連の事故が発生した場合、貴社のブランド(企業イメージ)にどの程度の影響がありますか。(記号に)



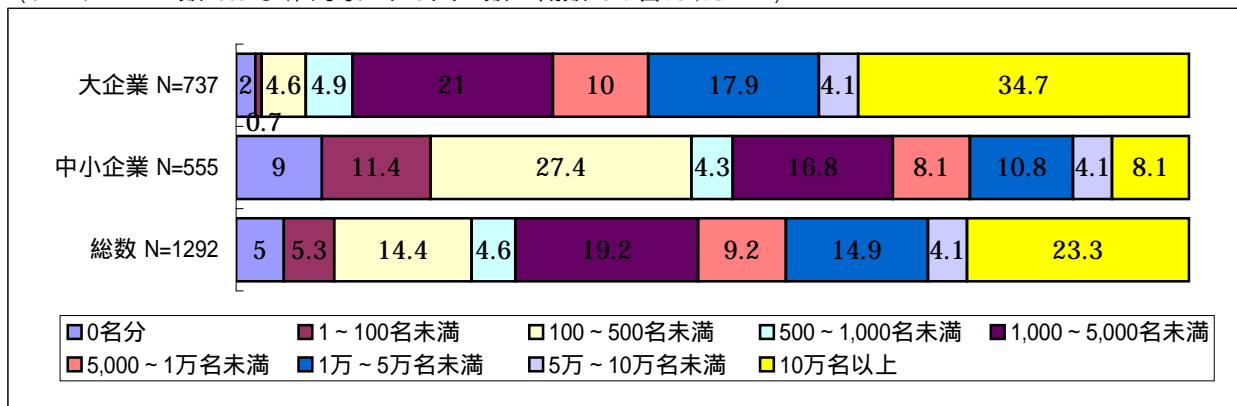
11. 貴社の業務は、元請や代理店、フランチャイジー等のビジネスパートナーにどの程度依存していますか。(記号に)



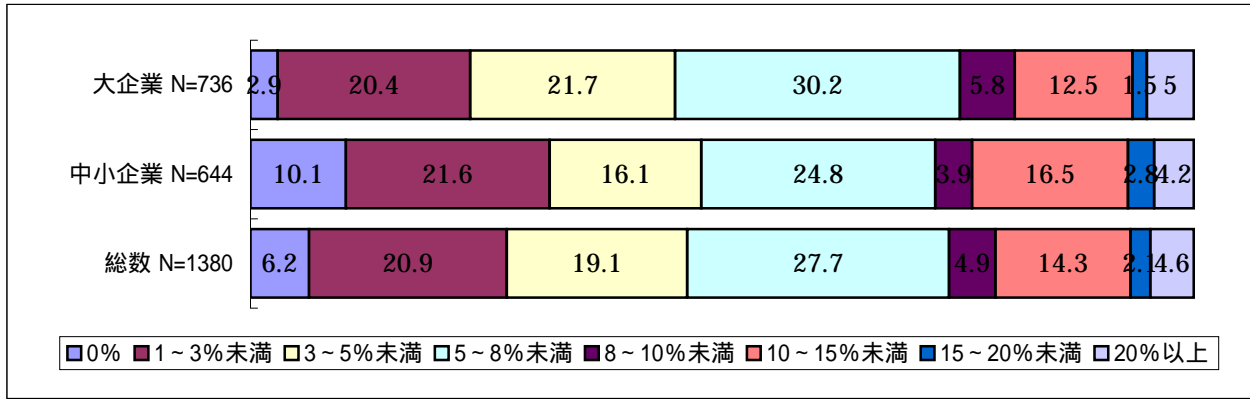
12. 貴社では、外部に漏洩すると事業に極めて深刻な影響が生じる重要情報(国家機密、営業機密、プライバシー情報等)をどの程度保有、管理または使用していますか。(記号に)



13. 貴社では、事業を実施する上で何名分程度の個人情報を取り扱っていますか。(データののべ数ではなく、対象とする人の数の概数でお答えください)



14. 貴社における離職率(直近の1年間に退職・転職された従業員の割合)はどの程度ですか。



15. 貴社において過去に、事業活動に影響を与えるようなIT事故が発生したことがありますか。
(あてはまるもの全ての記号に)

