内部不正による
情報セキュリティインシデント実態調査

－調査報告書－

2016年3月3日

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

目 次

1. はじめに

1.1 背景・目的

独立行政法人情報処理推進機構（以下、IPA）では、情報システムに係る組織の内部者の不正行為（以下、内部不正とする）について、2012 年度に「組織内部者の不正行為によるインシデント調査 [1]」（以下、前回の調査）を実施し、「組織における内部不正防止ガイドライン [2]（以下、内部不正防止ガイドライン）」を発行、2014 年度に改版する等、内部不正の防止に向けた取り組みを推進している。

近年、内部不正を原因とする情報漏えい事件の報道が相次いでおり、被害も深刻化している。組織は内部不正を未然に防ぐ必要に迫られているが、内部不正は、職務上与えられた権限を使い行われるため、その対策は容易ではない。このような背景を受け、組織が内部不正から重要情報を守るため、近年の内部不正の事例や情報セキュリティに関連する政府の指針等を基に、内部不正の防止に向けた環境整備を促す必要がある。

本調査は、内部不正の発生及び対策の実施状況等の実態を調査・分析し、内部不正の予防や抑止、事後対応に役立つ効果的な対策を広範に情報提供することを目的として実施した。

1.2 調査概要

内部不正による情報セキュリティインシデントの実態調査として、国内外の文献調査および Web アンケートにより内部不正の発生や対策状況を調査した。また、企業へのインタビュー及び法律・労務の有識者へのインタビューにより、企業が実施すべき対策について法的な観点も含めて調査した。

前回の調査では、内部不正の動機や抑止・防止策について、組織に所属する幅広い人々を対象とした意識調査を行い、その中で主にどのような要因が不正行為に至るのか、どのような抑止・防止策が不正行為への気持ちをどの程度低下させるかを示した。

今回の調査では、組織の従業員等に加え、内部不正の経験者を対象としたウェブアンケートを実施し、内部不正の実態をより掘り下げるとともに、前回の調査を基に作成した内部不正防止ガイドラインに沿った対策の実施状況や発生時の対応を把握することを目指した。

本調査報告書では、第 2 章に内部不正に係わる文献調査の結果、第 3 章に内部不正に関するアンケート調査の結果、第 4 章に企業及び法律・労務の有識者に対するインタビュー調査の結果、第 5 章に判例調査の結果を報告する。最後に、第 6 章で、これらの調査結果から得られた内部不正の実態及び内部不正の予防、抑止、事後対応に役立つ対策等について報告する。

[1] https://www.ipa.go.jp/security/fy23/reports/insider/

[2] https://www.ipa.go.jp/security/fy24/reports/insider/

2. 文献調査

2.1 内部不正による情報セキュリティインシデントに関する概況

本章では、内部不正に関連する国内外の論文及び調査報告書により、内部不正に関するセキュリティインシデントの発生状況、及び不正行為者の傾向、不正行為の動機、セキュリティ対策の最新動向について述べる。

2.1.1 内部不正の発生状況

世界における内部不正の発生状況をセキュリティベンダ等の報告者や報道とから概観する。シマンテック社の調査[3]によると、2014 年に世界で発生したデータ侵害の原因は、外部の攻撃者によるものが 49%と最も多く、内部犯行の割合は 8%であった。Verizon Communications Inc.の調査[4]でも、データ漏えい/侵害の攻撃実行者を外部者、内部者、パートナーに分けると、外部者によるものが 8 割以上を占め、内部者の割合は、十数パーセントと外部者に比べ低い割合であった。また、地域は限定されるが、北米及び欧州、アフリカを対象に ISACA (Information Systems Audit and Control Association[5]) が RSA Conference[6]と共同で実施した調査[7]では、2014 年に経験した脅威の行為者は、サイバー犯罪者が 45.6%で最も多く、次に悪意のない内部者が 40.7%であり、悪意のある内部者は 28.6%であった。

日本国内では、近年、退職者による海外への技術流出や従業員による不正な情報の窃取など、内部者の不正行為による事件が報道されている。2014 年から 2015 年にかけて報道された内部不正事件を表 1 に示す。中でも、2014 年 7 月に教育事業者で発生した委託先社員による個人情報漏えい事件は、漏えい件数が 3500 万件超と大規模であり、関連する法改正やガイドラインの改訂等にも影響を及ぼし、企業や組織において内部不正対策を見直す契機にもなった。

経済的な側面では、Ponemon Institute, LLC が日本を含む 7 カ国で実施した調査[8]によると、9 種のサイバー犯罪について、企業が経験した割合は、内部不正が 35%で最も低いが、年間の平均被害額は、約 14.4 万ドルと最も高かった。このうち、日本企業の 32 社を見ても、企業が経験した割合は、内部不正が 22%と最も低いが、サイバー犯罪の年間平均被害額は最も高い結果となり、発生頻度は比較的低いが経済的影響が大きいといえる。

---

[3] シマンテック：2015 年インターネットセキュリティ脅威レポート第 20 号
http://www.symantec.com/ja/jp/security_response/publications/threatreport.jsp

[4] ベライゾン：2015 年度データ漏洩/侵害調査報告書　https://www.verizonenterprise.com/jp/DBIR/2015/

[5] 情報システム監査や IT ガバナンス、リスク管理等の情報通信技術専門家の国際的な NPO 団体。
https://www.isaca.org/

[6] 暗号化や情報セキュリティを扱う世界最大級のカンファレンス。 https://www.rsaconference.com/

[7] ISACA and RSA Conference：State of Cybersecurity:Implications for 2015
http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf

[8] Ponemon：2015 Cost of Cyber Crime Study:Global（提供：HP Enterprise）
http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/

表１　2014 年～2015 年に報道された内部不正事件

報道時期	不正行為者	動機	結果	概要
2015年10月	職員	仕事や勉強に利用	停職6ヶ月	市民の個人情報を含む行政情報等のファイル約220万件を、職場に貸与されたUSBメモリを使い不正に持ち出し、自宅に保管していた。
9月	職員	私的な開発に利用	懲戒免職	市職員が、約68万件の有権者情報を無断で自宅に持ち帰り、外部に流出させた。
4月	退職者	転職先での利益取得	逮捕※	元社員が、競合会社に転職する際、営業秘密である機械の図面データを不正に持ち出した。
2月	退職者	転職先での利益取得	逮捕※	元社員が、営業秘密である情報を不正に取得し、自分のハードディスクに複製した。退職後は海外企業に転職していた。第三者提供は確認されていない。
1月	退職者	転職先で役立てるため	逮捕※	元社員が、販売戦略に関する営業秘密を不正に取得した。
2014年7月	委託先社員	金銭取得	逮捕※	顧客データベースを保守管理するグループ会社の業務委託先の社員が、約3,504万件の個人情報を不正に持ち出し転売した。
5月	委託先社員	自社の利益享受	懲戒解雇	ネットワークシステムを保守管理する委託先の社員が、権限を悪用し委託先の情報を不正に入手、自社の入札活動に利用した。
3月	業務提携先退職者	処遇の不満、金銭取得	逮捕※	業務提携先の社員が、機密情報を不正に持ち出し、転職先の海外企業に提供した。

※不正競争防止法違反による　　（報道により公表された事例を IPA がまとめたもの）

報道等により公表された事件以外にも、組織では、うっかりミスや不注意による情報漏えいが後を絶たない。一般財団法人日本情報経済社会推進協会（JIPDEC）が IT 調査・コンサルティング会社と共同で 2015 年 1 月に実施した調査 [9]によると、過去1年間で経験したセキュリティインシデントについて、「個人情報の漏えい・逸失」では、人為ミスが 12.6%、内部不正が 5.2%であった。NPO 日本ネットワークセキュリティ協会(JNSA)が実施した個人情報漏えいに関する調査 [10]では、2013 年に発生した個人情報漏えいインシデントのうち、従業員のうっかりミスと考えられる「誤操作」及び「紛失・置き忘れ」は合わせて 49.2%と約半数を占める結果であった。

2.1.2　内部不正行為に至る動機、行動

米国 CERT 及びプライスウォーターハウスクーパース社（以下、PwC 社）、米国シークレットサービス等が共同で実施した調査 [11]によると、2014 年に米国内で発生した内部犯行の動機について、金銭目的が最も多く 16%、続いて、興味本位が 12%、復讐が 10%であった。

日本国内の内部不正の事例について同様の調査はないが、表 1 から、転職先での利益取得、及び金銭目的、個人的な利益取得等が動機となっていることがわかる。

不正行為者の振る舞いについて、PwC 社が内部関係者によるサイバー犯罪についてまとめたレポー

[9] JIPDEC、アイ・ティ・アール株式会社：企業 IT 利活用動向調査 2015
http://www.jipdec.or.jp/library/itreport/u71kba0000002110-att/itreport2015_spring_chapter1.pdf

[10] JNSA：2013 年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～
http://www.jnsa.org/result/incident/data/2013incident_survey_ver1.2.pdf

[11] PwC 社：激増するリスク追いつかない対策-米国サイバー犯罪調査 2014 における主要な発見事項
http://www.pwc.com/jp/ja/japan-knowledge/archive/assets/pdf/2014-us-state-of-cybercrime1503.pdf

ト[12]によると、システム的な面では、「物理的な接近ではなく正規のアクセス権でシステムやデータにアクセスする」、「ネットワーク共有や外部メディアを利用」、「不正ソフトをインストール」等、システム的な面以外として、業績の低下や欠勤の増加、同僚の言動の変化等を挙げている。

このような内部不正の動機及び不正の兆候に繋がる振る舞いを把握することは、早期発見や予防対策を検討する上で役立つ。

2.1.3 内部不正対策

CERT Insider Threat Center[13]は、2013 年に公開した内部者による知的財産窃盗に関する調査報告書[14]において、知的財産を流出から守るための 5 つの対策法（表 2）を提言している。これらは CERT が米国において収集した 700 件以上の事例から得た知見であり、参考にすべき対策といえる。

表 2　知的財産を流出から守るための 5 つの対策法

1. 退職手続きの中で、知的財産保護契約の内容を確認し、退職者に会社の資産の返却を求めること。
2. 退職者からの情報漏えいは退職の前後 1 ヶ月に集中するため、この期間のサーバへのアクセスログや、電子メールのログを保存すること。
3. 印刷物を監視し、紙媒体での情報流出を防ぐこと。
4. 情報へのアクセス権を制限し、従業員のアクセスできる知的財産情報を必要最小限にすること。
5. 競合他社との電子メールのやりとりを監視すること。

また、組織がどのような対策に重点を置いているかについて、トレンドマイクロ社の調査[15]によると、2015 年のセキュリティ対策の実施率を前年と比較し、最も高い伸びを見せたのは「社員教育の定期的あるいは随時実施」で、7.3 ポイント増であった。続いて「監査の定期的実施」（6.0 ポイント増）、「注意喚起の定期的あるいは随時実施」（4.6 ポイント増）の順であった。従業員への注意喚起及び抑止力、及びチェック体制の強化に重点を置き対策を強化していることがわかる。

2.1.4 内部不正発生時の対応

サイバー攻撃による被害が後を絶たない中、インシデント対応チーム CSIRT(シーサート: Computer Security Incident Response Team)による活動への期待が高まっており、内部不正が発生した場合のインシデント対応の施策としても期待できる。

JPCERT コーディネーションセンターがまとめた報告書[16]によると、CSIRT は「発生した事象を検知及びその報告を受け、組織におけるインシデントと判断でき、解決に向けた対応及び調整ができる機能或いはチームであり、特にインシデントの発生抑止あるいは解決のため、外部との技術的な連携ができる機

---

[12] PwC 社：内部関係者によるサイバー犯罪
http://www.pwc.com/jp/ja/japan-knowledge/archive/assets/pdf/managing-insider-threats1509.pdf

[13] http://www.cert.org/insider-threat/

[14] CERT® Insider Threat Center: Spotlight On: Insider Theft of Intellectual Property Inside the United States Involving Foreign Governments or Organizations (May 2013)
http://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_48680.pdf

[15] トレンドマイクロ：組織におけるセキュリティ対策実態調査 2015 年版
http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20150520054603.html

[16] JPCERT コーディネーションセンター：経営リスクと情報セキュリティ～CSIRT：緊急対応体制が必要な理由～
https://www.jpcert.or.jp/csirt_material/files/csirt_for_management_layer_20151126.pdf

能或いはチームでもある」と定義されている。また、CSIRT は、「緊急対応（インシデントハンドリング）」を構成する 4 つの機能「モニタリング（事象の検知、報告受付）」「トリアージ（事実確認、対応の判断）」「インシデントレスポンス（分析、対処、エスカレーション [17]、連携）」「リスクコミュニケーション（報告・情報公開）」の一部もしくはすべてを有するとしている。さらに、組織の状況や方針に沿って、CSIRT がセキュリティ監視、教育／トレーニング等のサービスもカバーしているケースがあることも紹介されている。内部不正特有の対応が必要であればそれを明らかにし、組織における体制を整備する必要があると考えられる。

また、インシデント対応時の重要な技術として、情報収集及び証拠保全を行うデジタルフォレンジック技術がある。デジタルフォレンジックにより、インシデントの事後に、具体的な状況を把握し、影響範囲を調査するために検証可能な証拠を保全するほか、従業員の無実を証明することも可能となる。また、フォレンジックのためのデータ収集を実装している事実を従業員に明示することにより、不正行為を抑止する上で効果的と考えられる。CSIRT の活動においても、インシデントの対応や法的な問題の解決等にフォレンジック機能は不可欠である。

2.2 環境犯罪学に関連する理論の整理

「不正のトライアングル理論」、「状況的犯罪予防 [18]」のほか、「環境設計による犯罪予防（Crime Prevention Through Environmental Design:CPTED／以下、CPTED）」という環境犯罪学に関連する理論の援用が内部不正防止に有効ではないかと考えられてきた。

CPTED は、犯罪学者の C. Ray Jeffery が 1970 年代初頭に提唱した理論 [19]で、「接近の制御」「監視性の確保」「被害対象の強化・回避」「領域性の強化」を主軸に、「人間による環境の適切なデザインと効果的な利用により、犯罪と犯罪不安を減少させ、生活の質の向上をもたらすことができる」[20]という考え方である [21]。1970 年代以降、主に都市デザインの有識者や犯罪学者により改変が加えられている。

さらに心理学のアプローチも取り入れられ、1990 年代後半には、第二世代の CPTED[22]として、「組織内の社会的凝縮性」「組織内外のグループとの連携・協調」「組織の文化や場所性」「多様性・密度の閾値」を加え、主に防犯や街づくりの場面で参照されている。表 3 はその具体例である。

---

[17] 業務に関連する事項について、より上の階層に報告し、対応すること。

[18] 犯罪学者の Cornish & Clarke（2003）が提唱した都市空間における犯罪予防の理論。犯罪予防対策を実施すべき 5 つに分類し、さらに 25 の犯罪予防技術に細分化している。監視者の設置などによって外部からのコントロールが可能な「環境」を適切に定めることを主眼として、犯罪機会・動機を低減し予防するという犯罪予防策であり、直接的に犯罪を防止する対策及び間接的に犯罪を防止及び抑止する対策を含んでいる。

[19] Crime Prevention Through Environmental Design:Aplicaions of architectural design and space management concepts.Oxfprd, MS:Butterworth-Heinemann,Crowe,T.D.2000.

[20] 財団法人社会安全研究財団「環境犯罪学と犯罪分析」より。

[21] JNSA（組織で働く人間が引き起こす不正・事故対応ワーキンググループ）「内部不正対策 14 の論点」より。

[22] ”Crime prevention through environmental design (CPTED): a review and modern bibliography”, 1)Paul Michael Cozens; 2)Greg Saville; 3)David Hillier,1)Department of the Premier and Cabinet, Perth, Australia;2)University of New Haven, New Haven, Connecticut, USA;3)University of Glamorgan, Pontypridd, UK,2005.

表 3　CPTED の概要（防犯環境設計の考え方）

分類	内容
(1)被害対象の強化・回避	部材や設備等を破壊されにくいものとする。 住戸の玄関扉、窓等は侵入盗等の被害に遭いにくいように、破壊等が行われにくい構造とするとともに、必要に応じて補助錠や面格子の設置等の措置を講じたものとする。
(2)接近の制御	犯罪企図者の動機を限定し、接近を妨げる。 住戸の玄関扉、窓、バルコニー等は犯罪企図者が接近しにくいように、敷地内の配置計画、動線計画、住棟計画、各部位の設計等を工夫したものとするとともに、必要に応じてオートロックシステム等の措置を講じたものとする。
(3)監視性の確保	周囲からの見通しを確保する。 敷地内の屋外各部及び住棟内の共用部分は、周囲からの見通しが確保されるように、敷地内の配置計画、動線計画、住棟計画、各部位の設計等を工夫したものとするとともに、必要に応じて防犯カメラの設置等の措置を講じたものとする。
(4)領域性の強化	帰属意識の向上、コミュニティ形成の促進を図る。 共同住宅に対する居住者の帰属意識が高まるように住棟の形態や意匠、共用部分の利用機会が増え、コミュニティ形成が促進されるように、敷地内の配置計画、動線計画、住棟計画、共用部分の維持管理計画及び利用計画等を工夫する。

（出典）国土交通省在宅局「防犯に配慮した共同住宅に係る設計指針」[23]

CPTED の「被害対象の強化・回避」、「接近の制御」、「監視性の確保」、「領域性の強化」等は、これまでに検討してきた企業における内部不正の対策と重なる視点も多い。例えば、「被害対象の強化・回避」とは、犯罪の誘発要因を除去し、対象物を強化、犯罪の被害対象となることを回避することである。「接近の制御」とは、出入口を管理するなどして、被害対象者に近づきにくくすることである。「監視性の確保」とは、多くの人の目を確保することである。「領域性の確保」とは、職場環境を整備し従業員の意識を高め、管理が及んでいることを示すことである。また、第二世代の CPTED については、職場環境や従業員の意識として整理することができる。

本調査では、これまでに都市設計の分野で活用されていた CPTED の理論の観点から内部不正や職場環境について分析を行い、環境犯罪学の視点から内部不正対策のあり方について検討を行う。

[23] 国土交通省在宅局：防犯に配慮した共同住宅に係る設計指針
http://www.mlit.go.jp/jutakukentiku/house/press/h12/130323-3.htm

2.3 本調査における定義と分類

本調査は、組織内で発生した情報セキュリティインシデントのうち、内部不正を対象としている。本調査における内部不正経験者の定義及び内部不正の分類を以下に示す。

2.3.1 内部不正経験者

本調査の対象は、表4で示す内部者であり、役員や従業員のほか退職者及び委託先社員等を含む。次項で示す不正行為を行ったこれらの内部者を内部不正経験者とする。

表 4 内部不正防止ガイドラインによる内部者の定義

役員、従業員（契約社員を含む）及び派遣社員等の従業員に準ずる者（以下、総称して「役職員」という）又は、元役職員であった者のうち、以下の 2 つのどちらかでも満たした者 ・ 組織の情報システムや情報（ネットワーク、システム、データ）に対して直接又はネットワークを介したアクセス権限を有する者 ・ 物理的にアクセスしうる職務についている者（清掃員や警備員等を除く）

2.3.2 内部不正の分類

本調査では、内部者による違法行為だけでなく、情報セキュリティに関する内部規程違反等の違法とまではいえない不正行為も内部不正に含めている。また、国内で発生している情報漏えい事件等をみると、うっかりミスや不注意によるものも多く発生していることから、これらも調査の対象とした。

内部不正の種類について、本調査では、CERT の研究[24]及び前回の調査を参考に、表 5 の 5 つに分類し、どのような種類の不正行為が発生したかを尋ねた。

表 5 内部不正の分類

	分類	概要	本調査における不正行為の例
1	システム破壊 (IT Sabotage)	特定個人、組織（組織のデータ、システム、日常業務を含む）に損失を与えるという意志に基づいた悪意ある行動	システムの破壊・改ざん
2	知的財産の窃盗 (theft of IP[25])	機密や知財に関連する情報などを組織から盗み出す	顧客情報等の職務で知りえた情報の持ち出し
3	システム悪用 (fraud)	組織の財やサービスをごまかし(deception)やペテン(trickery)で手に入れる	個人情報を売買するなど職務で知りえた情報の目的外利用
4	意図しない内部不正 (Unintentional Insider Threat)	悪意のない内部者が、誤った相手に電子メール・FAX を送信する、誤ってインターネット上に公開する、紙媒体や可搬記録媒体を紛失・廃棄・盗難される	うっかりミスや不注意によるルールや規則の違反
5	その他 (miscellaneous)	上記にあてはまらないケース	上記以外のなんらかのルールや規則の違反

[24] CERT® Insider Threat Center: Unintentional Insider Threats: A Foundational Study (August 2013) http://www.sei.cmu.edu/reports/13tn022.pdf

[25] IP(Intellectual Property):特許、著作権、商標、意匠、科学的公式、ソースコードの一部であり、顧客に関する機密情報を含む独自の創造的な発想などをさす。知的財産。

3. アンケート調査

本章では、内部不正に関するアンケート調査の概要及び調査結果を述べる。

3.1 アンケート調査概要

本調査では、組織における内部不正の発生状況及び発生時の対応、対策の実施状況等について、アンケートの内容を設計し、企業の実態を調査した。

本調査の実施にあたっては、有識者によるレビューを実施し、設問の設計、調査方法について検討した。本調査では、業種、従業員数、職種（経営者、システム管理者、従業員）を基に割付を行った調査（調査①）と、内部不正を働いた経験のある従業員を対象とした調査（調査②）を実施している。調査①、②のアンケート調査票は共通である（アンケート調査票については、付録2：アンケート調査票を参照）。調査概要を表 6、調査項目を表 7 に示す。

表 6　アンケート調査の概要

項目	概要
対象	【調査①】 民間企業における従業員等（経営者・システム管理者と従業員）を対象とする。 業種・従業員規模（従業員が 300 名未満と 300 名以上）については、統計上の妥当性を確保するため総務省「経済センサス」の日本標準産業分類に基づく従業員規模毎・業種毎の企業数分布に則り、層別抽出（比例割当法）する。 【調査②】 内部不正（規程違反を含む）の経験がある従業員等を対象とする。
標本抽出方法	インターネットアンケート調査会社が保有するモニターから、回答者の内部不正行為の業務との関わり、内部不正の経験に基づき、割付・抽出を行った。 プレ調査を実施して対象者のスクリーニングを行い、その後本調査を実施した。
回収数	3,852 件 (調査①：3,652 件、調査②：200 件)
期間	2015 年 11 月 25 日～11 月 30 日
実施方法	ウェブアンケート調査による実施。

表 7　アンケート調査項目

調査項目	調査のポイント
1.回答者の企業属性・個人属性及び企業状況	属性や所属組織、企業の概況を把握する。過去の類似調査で実施した内部不正に係るアンケート調査の属性設問と整合性を取る。
2.情報セキュリティインシデントの発生状況	外部攻撃及び内部不正の発生状況を把握する。内部不正については、情報の窃取、持ち出し、破壊といった事件性のあるものだけでなく、軽微な内部規程違反も含めた状況を把握する。
3.内部不正対策の実施状況	IPA「組織における内部不正防止ガイドライン」を基に、組織における内部不正対策の詳細な実施状況を把握する。
4.内部不正発生時の対応	内部不正事件が発生した場合に想定されるリスク、対応について調査する。
5.経営者・システム管理者と従業員の意識	2012 年に実施した「組織内部者の不正行為によるインシデント調査」の中で、経営者・情報システム管理者と従業員で認識にギャップが見られた選択肢を取り上げて調査する。
6.職場文化、企業風土等	内部不正版の CPTED の検証に資する指標を作成するための試行を行う。なお、第一世代の CPTED に加え、「組織内の社会的凝縮性」「組織内外のグループとの連携・協調」「組織の文化や場所性」「多様性・密度の閾値」といった第二世代と呼ばれるものも含めた形で検討を行う。

本調査における回収結果を表 8、表 9 に示す。調査①は、対象に一定程度のシステム管理者、経営者を含めたものとするため、プレ調査を実施し、経営者 600 サンプル、システム管理者 900 サンプルを収集した。また、調査①では、総務省「経済センサス」を基に業種別割付も行い、システム管理者、経営者を必要数確保したうえで、業種別の割付数に必要な数は従業員数で補填した。

調査②では、「2.3.2　内部不正行為の分類」で定義した「顧客情報等の職務で知りえた情報の持ち出し」「システム破壊・改ざん」「個人情報を売買するなど職務で知りえた情報の目的外利用」「うっかりミスや不注意によるルールや規則の違反」「前記以外の何らかのルールや規則の違反」のいずれか 1 つ以上の経験があると回答したものを対象者とした。職種、業務、企業規模は考慮していない。

表８　調査①の回収結果

企業規模（従業員数）	業種	職種		
		従業員	システム管理者	経営者
300名以上	A～B 農林漁業		3	1
	C 鉱業，採石業，砂利採取業	1		1
	D 建設業	23	19	7
	E 製造業	157	119	28
	F 電気・ガス・熱供給・水道業	2	5	
	G 情報通信業	16	105	9
	H 運輸業，郵便業	52	18	5
	I 卸売業，小売業	157	26	8
	J 金融業，保険業	18	28	5
	K 不動産業，物品賃貸業	13	2	5
	L 学術研究，専門・技術サービス業	21	4	
	M 宿泊業，飲食サービス業	57	2	
	N 生活関連サービス業，娯楽業	33	1	2
	O 教育，学習支援業	25	19	8
	P 医療，福祉	117	13	5
	Q 複合サービス事業	16	5	1
	R サービス業(他に分類されないもの)	70	31	15
300名未満	A～B 農林漁業	5	9	9
	C 鉱業，採石業，砂利採取業	1	2	1
	D 建設業	166	31	36
	E 製造業	154	65	29
	F 電気・ガス・熱供給・水道業	1	4	1
	G 情報通信業	3	160	12
	H 運輸業，郵便業	26	9	11
	I 卸売業，小売業	312	66	96
	J 金融業，保険業	9	4	11
	K 不動産業，物品賃貸業	85	27	63
	L 学術研究，専門・技術サービス業	59	6	31
	M 宿泊業，飲食サービス業	209	7	54
	N 生活関連サービス業，娯楽業	131	10	51
	O 教育，学習支援業	41	15	13
	P 医療，福祉	102	15	23
	Q 複合サービス事業		6	5
	R サービス業(他に分類されないもの)	70	64	54
計		2152	900	600

表９　調査②の回収結果

企業規模（従業員数）	業種	職種		
		従業員	システム管理者	経営者
300名以上	A～B 農林漁業		1	2
	C 鉱業，採石業，砂利採取業	1	2	
	D 建設業	1	7	1
	E 製造業	18	16	1
	F 電気・ガス・熱供給・水道業	1	1	
	G 情報通信業	2	8	
	H 運輸業，郵便業	4	1	
	I 卸売業，小売業	4	2	
	J 金融業，保険業	5	14	
	K 不動産業，物品賃貸業	1	1	
	L 学術研究，専門・技術サービス業	2		
	M 宿泊業，飲食サービス業	3		
	N 生活関連サービス業，娯楽業	2	3	
	O 教育，学習支援業	6	2	
	P 医療，福祉	2	4	
	Q 複合サービス事業	3	10	
	R サービス業(他に分類されないもの)			
300名未満	A～B 農林漁業	2	1	
	C 鉱業，採石業，砂利採取業			
	D 建設業	1	1	1
	E 製造業	10	4	1
	F 電気・ガス・熱供給・水道業			
	G 情報通信業	1	7	
	H 運輸業，郵便業	2		
	I 卸売業，小売業	3	5	
	J 金融業，保険業	2		
	K 不動産業，物品賃貸業	2		1
	L 学術研究，専門・技術サービス業			
	M 宿泊業，飲食サービス業	1		
	N 生活関連サービス業，娯楽業		1	
	O 教育，学習支援業	3	4	1
	P 医療，福祉	2	2	
	Q 複合サービス事業			
	R サービス業(他に分類されないもの)	5	5	1
計		89	102	9

3.2　アンケート調査結果

本節では、アンケート調査の集計と分析結果を述べる。

3.2.1　情報セキュリティインシデントの発生状況

① 企業規模別

所属する企業・組織で外部攻撃や内部不正が発生しているかどうか尋ねた結果を図 1 に示す。従業員数 300 名以上の企業では、18.5%が外部攻撃を、8.6%が内部不正を経験している。従業員数 300 名未満の企業では、5.4%が外部攻撃、1.6%の企業が内部不正を経験している。

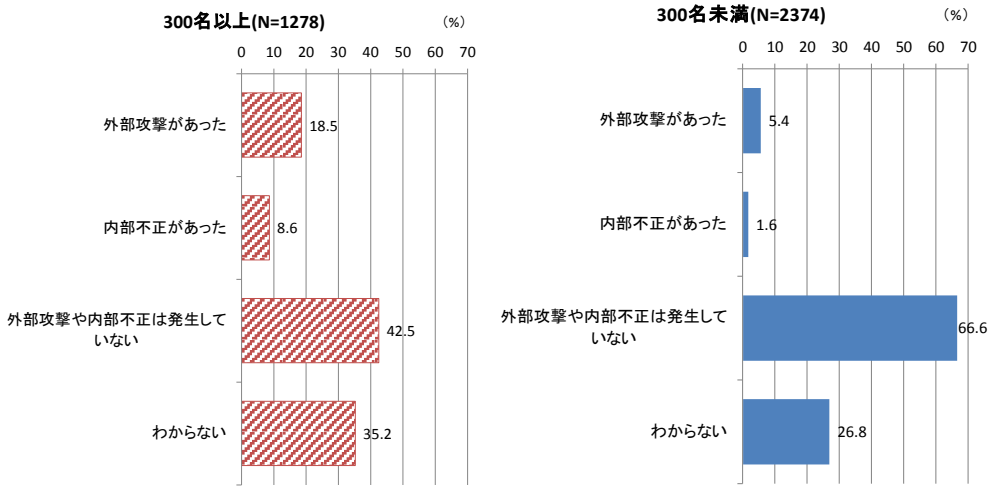

図 1　内部不正、外部攻撃の経験（企業規模別）≪SC6≫

内部不正が組織内で起こったことを「聞いたことがある」、「経験がある」という回答者にその詳細を尋ねた結果を図 2 に示す。企業規模に関わらず、「うっかりミスや不注意によるルール違反や規則の違反」が最も多く 75%以上であった。次いで「顧客情報等の業務で知りえた情報の持ち出し」が多く、70%以上であった。

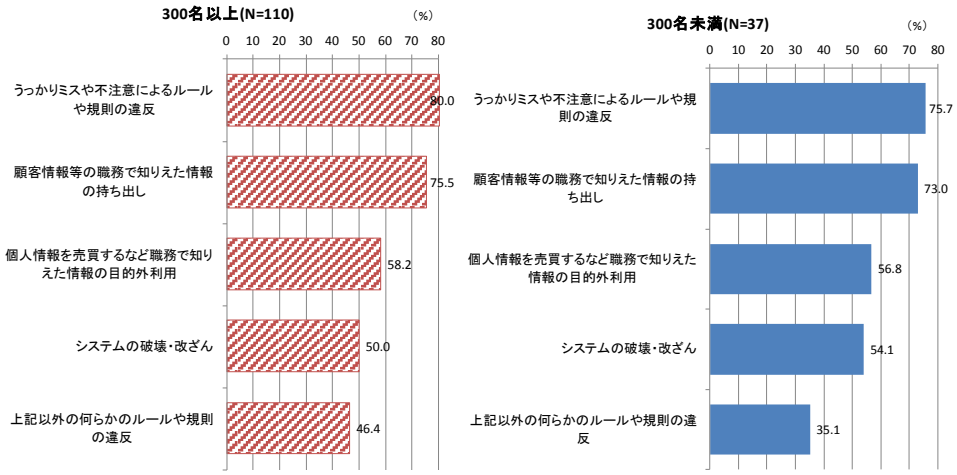

図 2　内部不正の詳細（聞いたことがある）（企業規模別）≪SC7-1≫

内部不正を起こした人の属性を尋ねた結果を図 3 に示す。300 名以上の企業では、多い方から順に、システム管理者（37.3%）、技術者・開発者（35.5%）、派遣社員（19.1%）となった。300 名未満の企業では、技術者・開発者（37.8%）、システム管理者（29.7%）、退職者（24.3%）の順となり、300 名以上の企業と比べると退職者が多い。

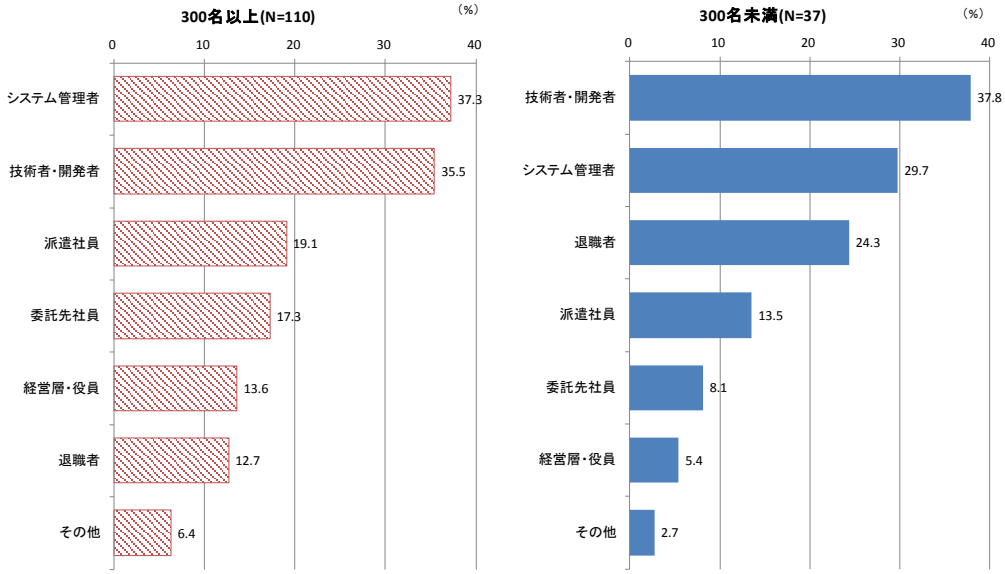

図 3　内部不正を起こした人の属性（聞いたことがある）（企業規模別）≪Q7≫

所属する企業・組織で「今後内部不正が起こると思うか」尋ねた結果を図 4 に示す。300 名以上の企業では、「対策をしているが、軽微なルール違反が発生する恐れがある」が 31.8%で最も高い。300 名未満の企業では、「これまで発生していないので、今後も発生しない」が 42.3%で最も高い。「対策をしても内部不正を防ぐことはできない」という回答は、300 名以上の企業では 24.8%、300 名未満の企業では 20.3%であった。

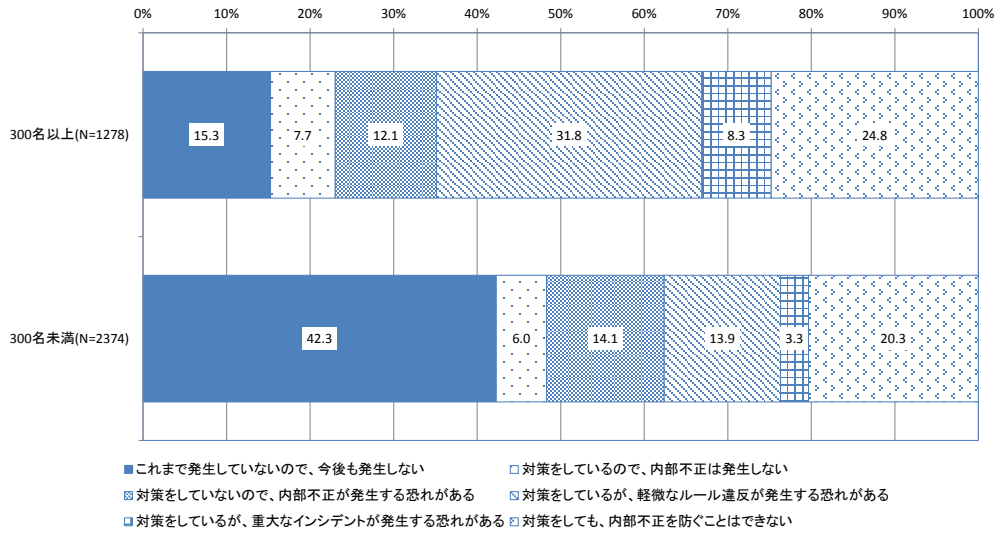

図 4　今後内部不正が起こると思うか（企業規模別）≪Q8≫

② 内部不正経験者

調査②の対象である、内部不正の経験がある者（以下、内部不正経験者）200 名の企業規模、職種、世代、勤続年数の内訳を図 5～図 8 に示す。システム管理者（兼務も含む）が半数を超えている。

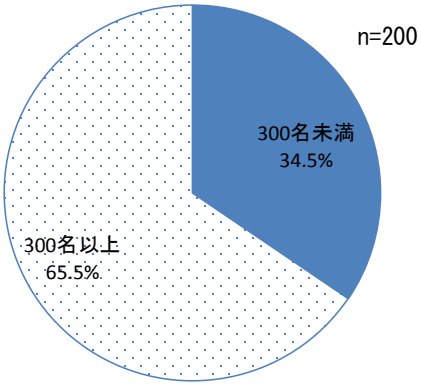

図 5　内部不正経験者の内訳（企業規模）≪SC2≫

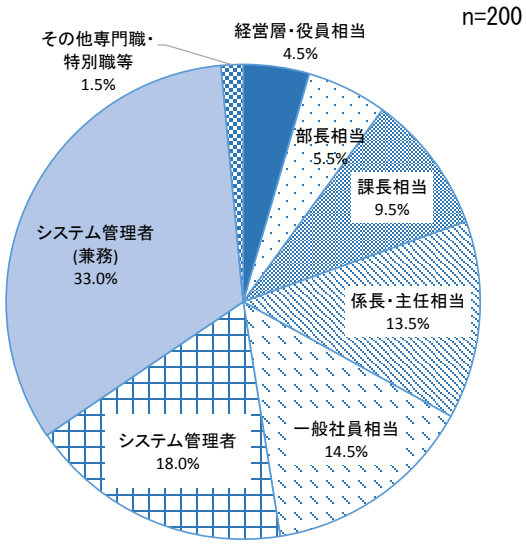

図 6　内部不正経験者の内訳（職務）≪SC5≫

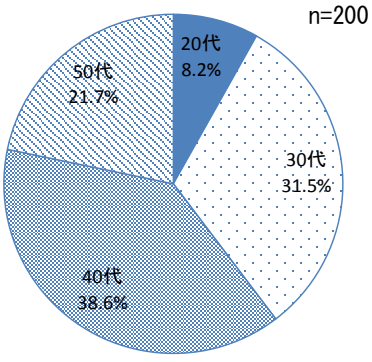

図 7　内部不正経験者の内訳（世代）≪問 2≫

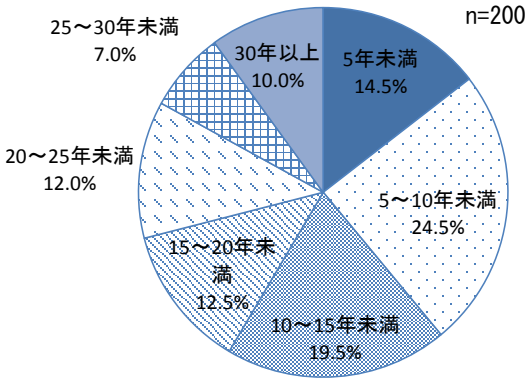

図８　内部不正経験者の内訳（勤続年数）≪Q1≫

内部不正経験者が起こした内部不正の詳細を図９に示す。「うっかりミスや不注意によるルール違反や規定違反」(66.5%)が最も多い。内部不正の分類としては、「顧客情報等の職務で知りえた情報の持ち出し」(58.5%)、「個人情報を売買するなど職務で知りえた情報の目的外利用」（40.5%）、「システムの破壊・改ざん」（36.5%）であった。

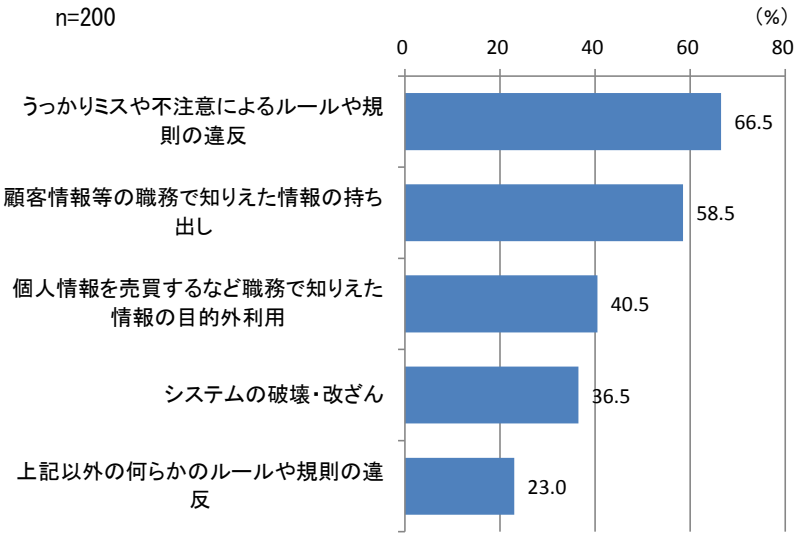

図９　内部不正の詳細（内部不正経験者）≪SC7-2≫

内部不正経験者に、内部不正を行った理由を尋ねた結果を図 10 に示す。図中の赤枠で囲ったものを「故意による」内部不正、それ以外は「故意が認められない」内部不正であるとすると、故意による内部不正が 42.0%、故意が認められない内部不正が 58.0%である。

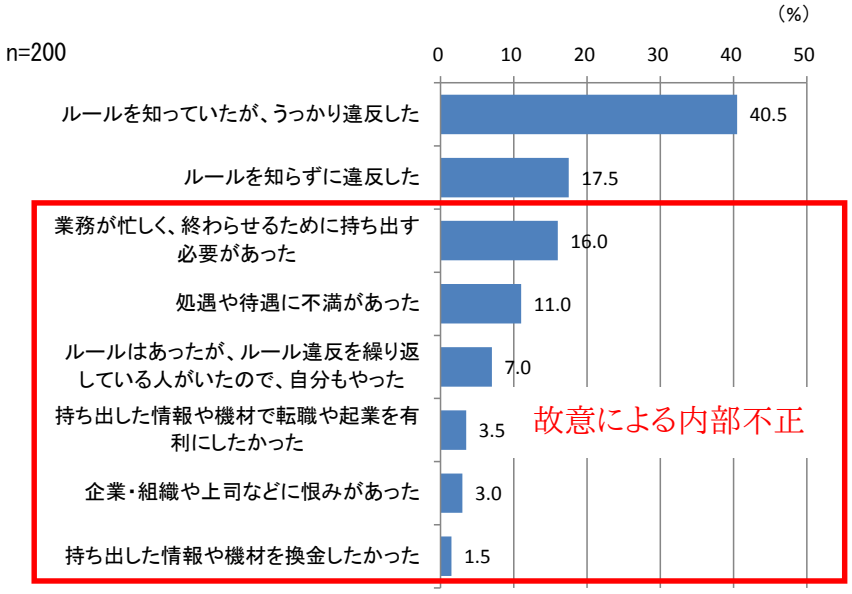

図 10　内部不正を行った理由（内部不正経験者）≪SC8≫

また、内部不正経験者に、所属する企業・組織で起きた故意による内部不正の詳細について尋ね、顧客情報、技術情報、営業計画、製造計画、開発物品がどのような経路・媒体で流出したのかを図 11 にまとめた。内部不正行為の対象となった情報等の種類に関わらず、USB メモリからの流出が最も多い。

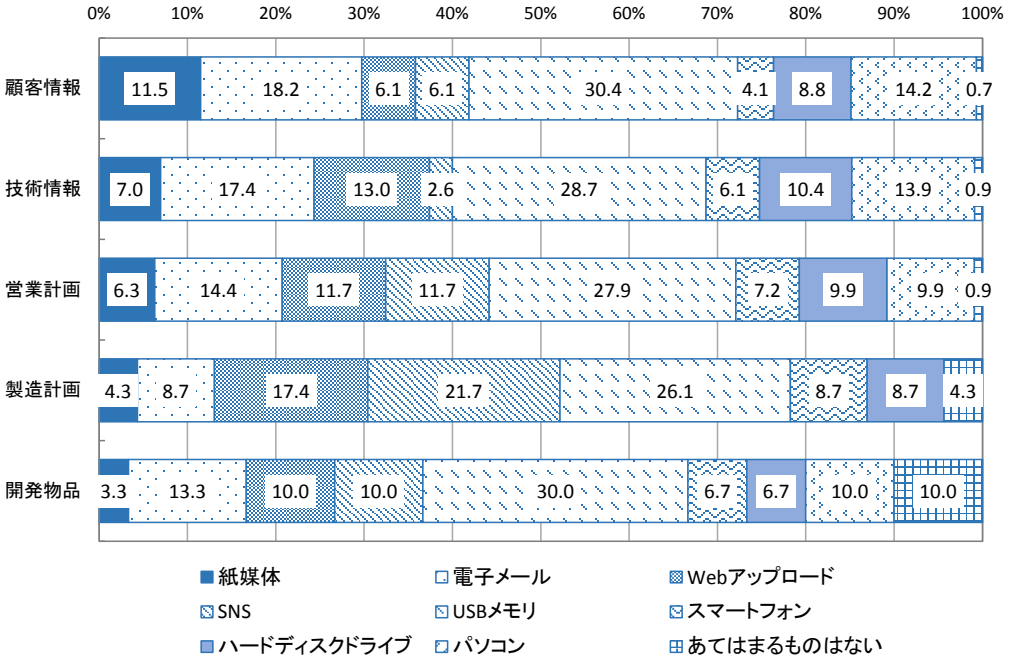

図 11　故意による内部不正の対象となった情報等の流出経路・媒体（内部不正経験者）≪Q7-1-2／7-1-3≫

内部不正経験者に、所属する企業・組織で「今後内部不正が起こると思うか」尋ねた結果を図12に示す[26]。「対策をしているが軽微なルール違反が発生する恐れがある」が最も多く38.2%であった。

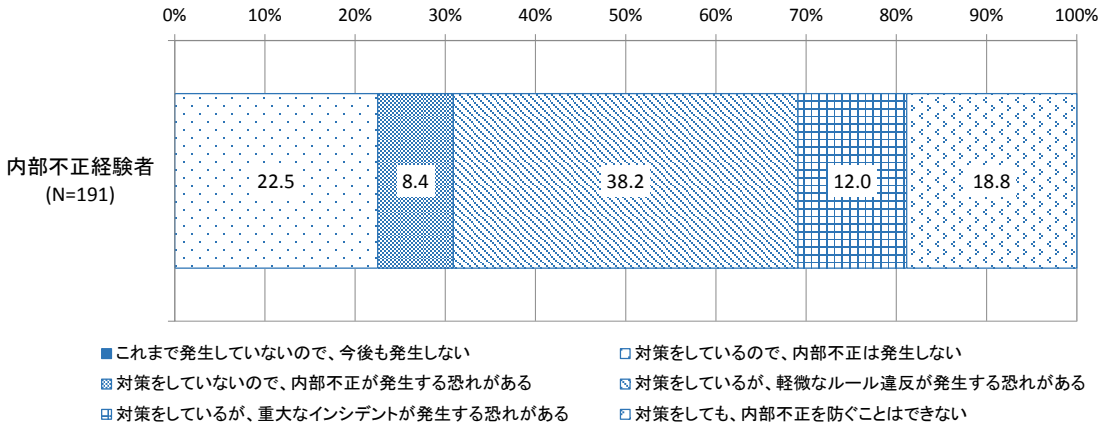

図12　今後内部不正が起こると思うか（内部不正経験者）≪Q8≫

[26] Q8の回答内容をQ8以外の回答内容とも照らし合わせ、矛盾する回答は除外した。

3.2.2　内部不正対策の実施状況

①　内部不正対策に関するルールや管理の状況

図 13 に、所属する企業・組織の方針やルールを尋ねた結果を企業規模別に示す。尋ねた項目全般について、300 名以上の企業に比べ 300 名未満の企業では方針やルールがあると回答した割合が低い。内部不正対策に関する方針・ルールに着目すると、「内部不正対策の担当責任者や管理体制、実施方針がある」「内部不正の対策は経営者の責任であることを示す基本方針がある」について、300 名以上の企業の 25%以上があてはまるのに対し、300 名未満では 10%未満である。

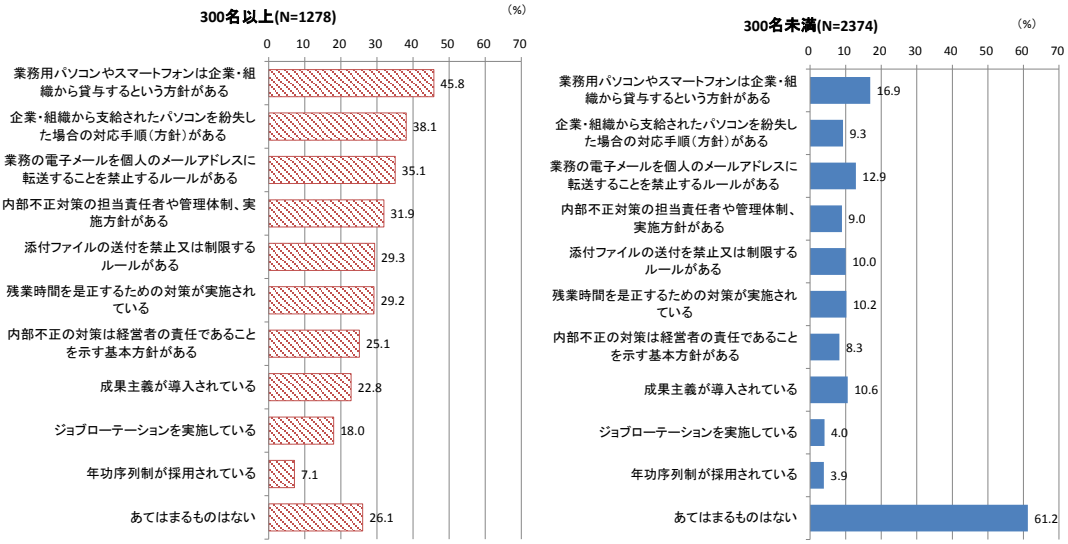

図 13　所属する企業・組織の方針やルール≪Q5≫

図 14 に、内部不正経験者に、所属する企業・組織の方針やルールを尋ねた結果を示す。図 13 と同様に、「業務用パソコンやスマートフォンは企業・組織から貸与するという方針がある」(58.5%)が最も多い。内部不正対策に関する方針・ルールに着目すると、「内部不正対策の担当責任者や管理体制、実施方針がある」「内部不正の対策は経営者の責任であることを示す基本方針がある」について、ともに 41.5%と図 13 の結果を上回った。

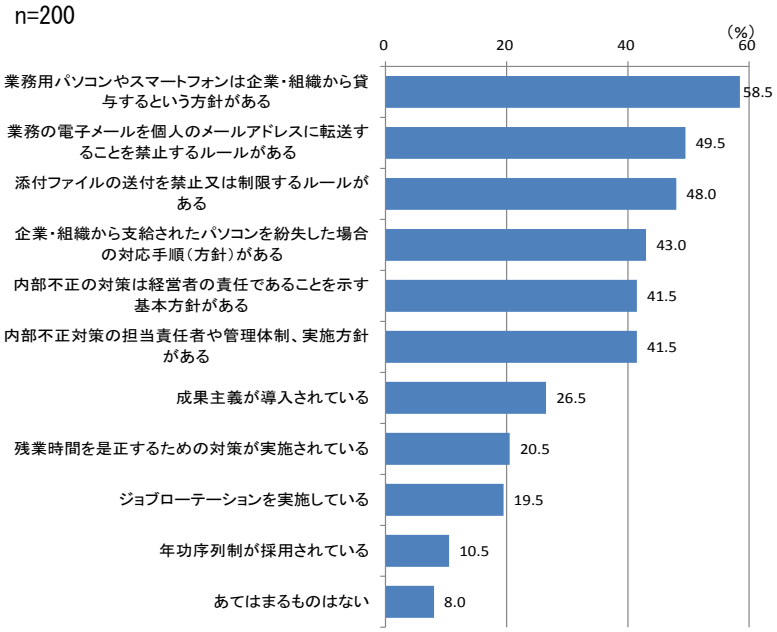

図 14　所属組織のルール（内部不正経験者）≪Q5≫

表 10 に、内部不正による情報持ち出しについて、内部不正経験者すべてと、故意の不正行為経験者のみの順位の比較を示す。情報の持ち出し手段は「USB メモリ」(内部不正経験者すべて:43.6%、故意の内部不正経験者:53.0%)の利用が最も多い。

表 10　情報持ち出しに関する順位の比較

上段:内部不正経験者すべて(n=200)、下段:故意の内部不正経験者のみ(n=98、「不正行為の動機」は n=84)[27]

(単位:%)

項目	1位		2位		3位	
発生部門	販売・営業部門	31.5	企画・広報部門	23.7	情報システム部門	20.9
	販売・営業部門	36.2	情報システム部門	21.5	企画・広報部門	19.5
行為者	技術者・開発者	39.0	システム管理者	37.0	派遣社員	27.0
	システム管理者	23.5	技術者・開発者	22.1	経営層・役員	17.4
不正行為の動機	ルールを知っていたが、うっかり違反した	40.5	ルールを知らずに違反した	17.5	業務が忙しく終わらせるため持ち出した	16.0
	業務が忙しく終わらせるため持ち出した	38.1	処遇や待遇に不満があった	26.1	持ち出した情報や機材で転職を有利にしたかった	16.7
対象情報	顧客情報	52.3	技術情報	35.8	営業計画	26.2
	顧客情報	48.3	技術情報	36.9	営業計画	32.9
持ち出し手段	USBメモリ	43.6	電子メール	34.3	パソコン	25.5
	USBメモリ	53.0	電子メール	28.9	紙媒体	18.8

(「不正行為の動機」以外は複数回答)

[27] 「不正行為の動機」は、不正行為の経験者自身が行った内部不正についての回答。その他の項目は、所属する企業・組織で発生した、経験者以外によるものを含む。

② 内部不正防止ガイドラインに基づいた対策の実施状況

内部不正防止ガイドラインに基づく対策が、所属する企業・組織においてどの程度実施されているか、経営者・システム管理者に尋ねた。ガイドラインから 32 の対策を抽出し、それぞれについて、所属する企業・組織での実施状況を表 11 の 5 段階で回答を得た。

表 11 対策の実施状況(段階)

①	②	③	④	⑤
方針やルールはない	方針やルールがある(実施無し)	②に加えて実施あり(確認無し)	③に加えて定期的に確認している(監査を含む)	わからない

ここでは、表 11 の②、③、④の段階であるものを、その対策を「実施している」と定義した。

調査①において、所属する企業・組織で「実施している」対策の数(対策実施数)を求め、全体に占める割合を企業規模別に図 15 にまとめた。300 名以上の企業の 39.6%で 32 個の対策が何らかの形で実施されている。一方、300 名未満の企業の 45.9%で何も対策が実施されていない(0 個)状況にあることがわかる。

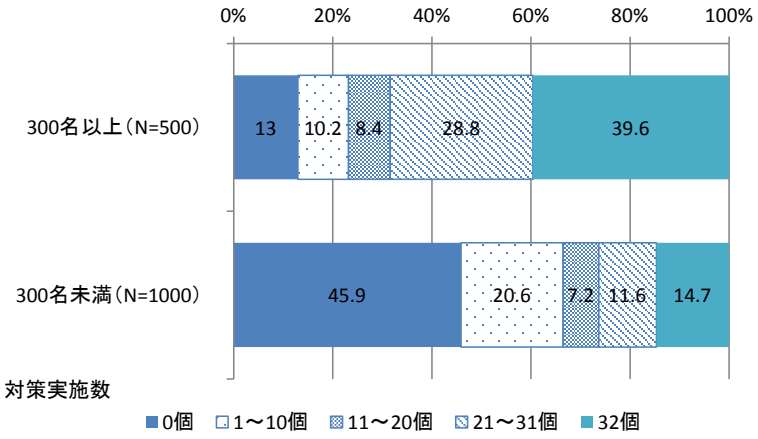

図 15 対策の実施状況(経営者、システム管理者のみ)≪Q9≫

図 16 に、対策実施数別に「今後内部不正が起こると思うか」尋ねた結果をまとめた。この結果によると、対策を実施していない企業（対策実施数：0 個）の 6 割で「これまで発生していないので、今後も発生しない」と回答している。また、対策実施数 11 個以上の企業では、10 個以下の企業と比較して「対策をしているので内部不正が発生しない」の割合が増える。さらに、対策実施数が増えるほど「対策をしているが軽微なルール違反が発生する恐れがある」という回答の割合も増える。

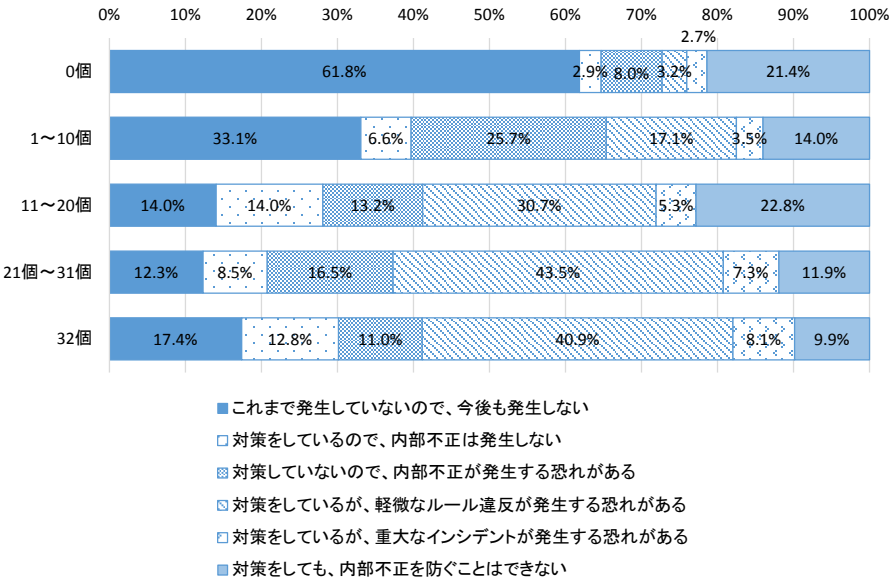

図 16　対策の実施状況と内部不正への意識（経営者、システム管理者のみ）≪Q9≫

図 17 に、300 名以上の企業での対策の実施状況を示す。各項目において平均して 6 割程度は何らかの対策を講じているという結果となった。「情報システムの利用者に対し、利用者 ID およびアクセス権を設定している」(79.2%)や「役職員の異動や退職(雇用終了)により不要となった利用者 ID およびアクセス権を速やかに削除している」(77.0%)は「方針やルールがない」という回答が少ない。一方、「重要情報に対し、時間やアクセス数・量等の条件でアクセスを制限している（夜間はアクセス不可等）」(61.2%)の対策実施率は低い。

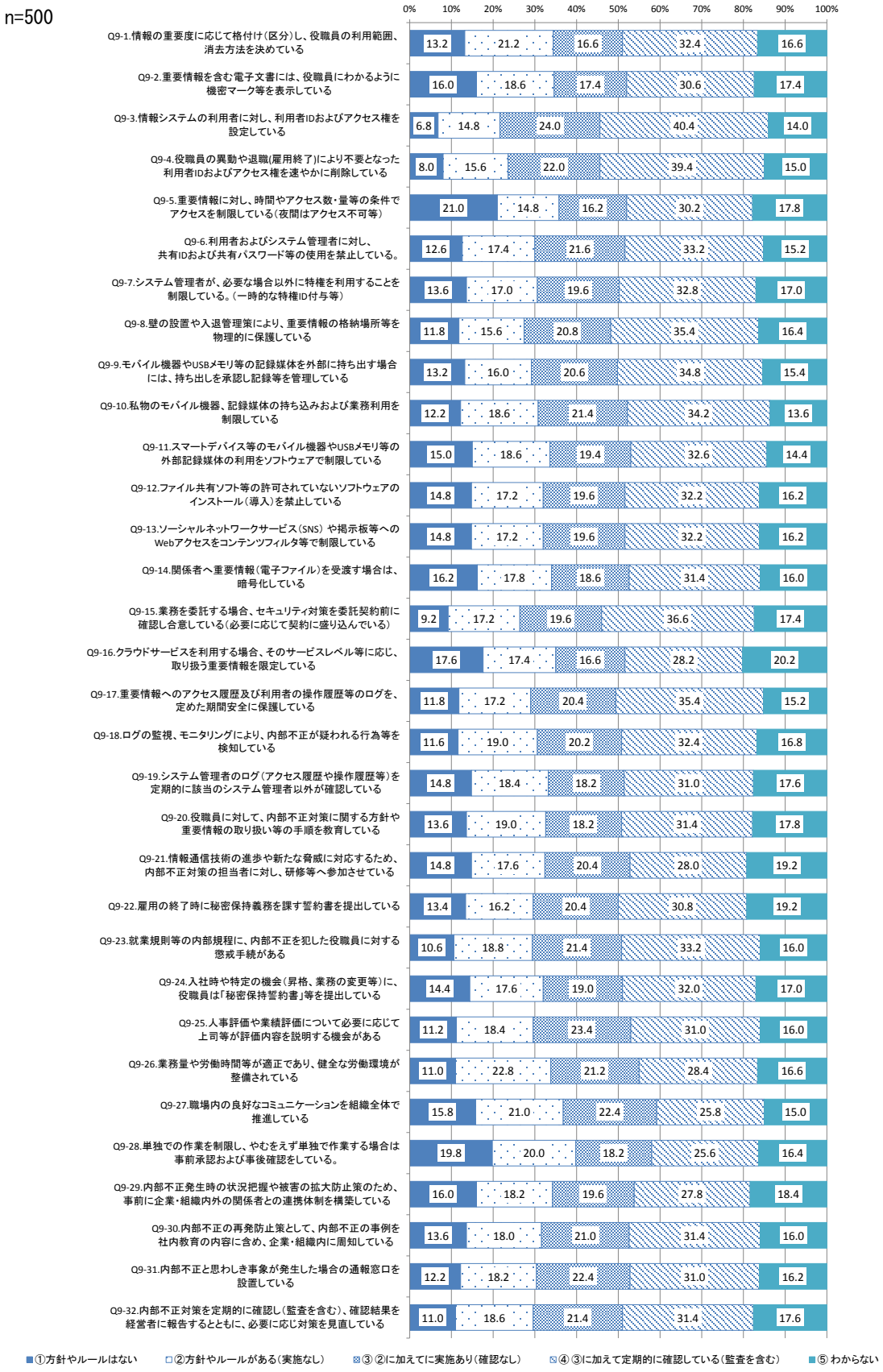

図 17　対策の実施状況（300 名以上／経営者、システム管理者のみ）≪Q9≫

図 18 に、300 名未満の企業での対策の実施状況を示す。図 17 の 300 名以上の企業の対策の実施状況と比較して、「方針やルールは無い」という結果の割合が高く、全項目で 4 割を超える。「情報システムの利用者に対し、利用者 ID およびアクセス権を設定している」、「役職員の異動や退職(雇用終了)により不要となった利用者 ID およびアクセス権を速やかに削除している」、「ファイル共有ソフト等の許可されていないソフトウェアのインストール（導入）を禁止している」は他の項目と比較すると対策実施率が高い。

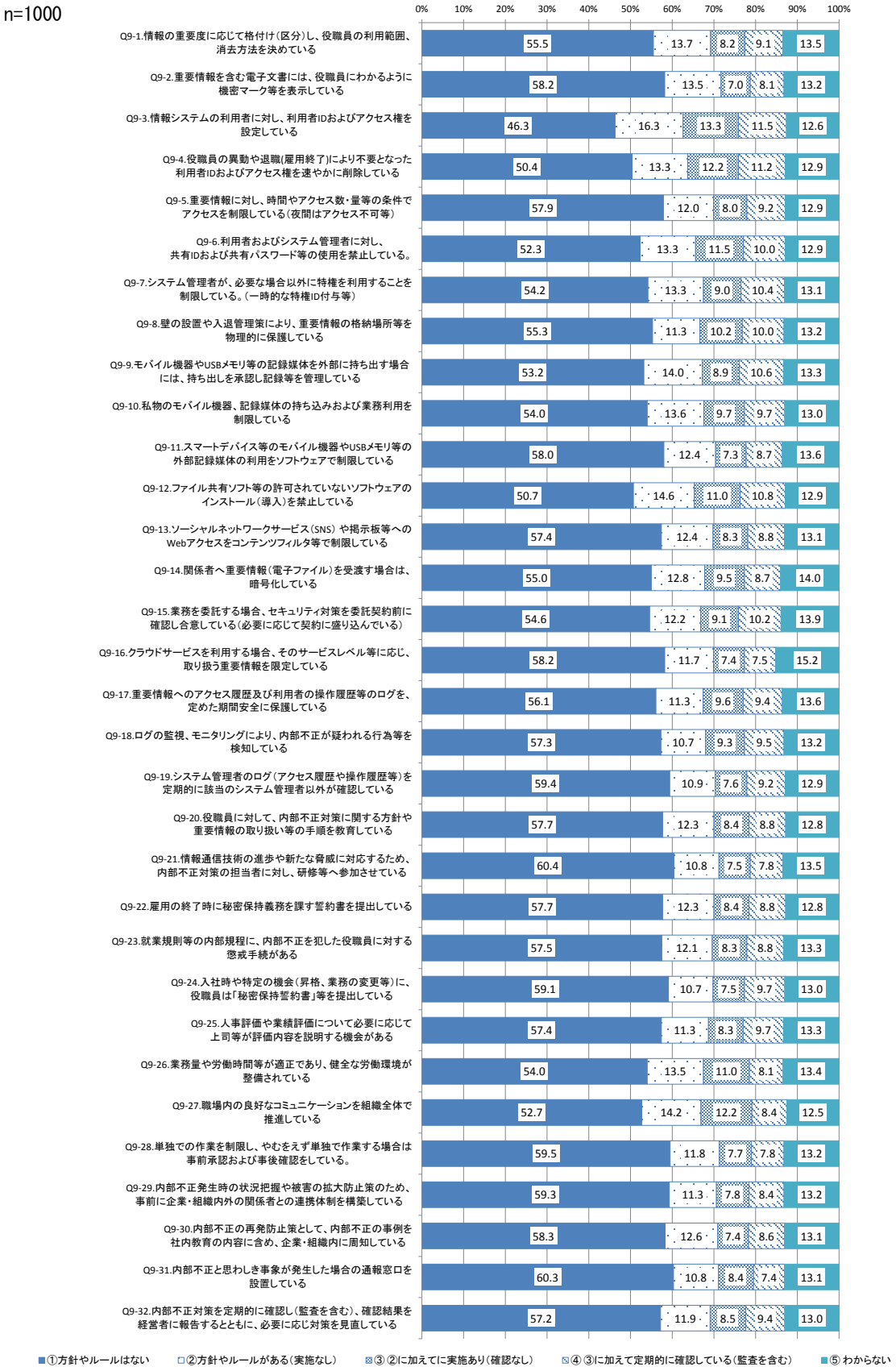

図 18　対策の実施状況（300 名未満／経営者・システム管理者のみ）≪Q9≫

図 19 に、内部不正経験者が所属する企業の対策実施状況の結果を示す。企業規模別の対策の実施状況(図 17、図 18)と比較して、内部不正経験者は「業務量や労働時間等が適正であり、健全な労働環境が整備されている」を除き、方針やルールがある、または方針やルールに従い実施しているとした割合が高い。

n=200

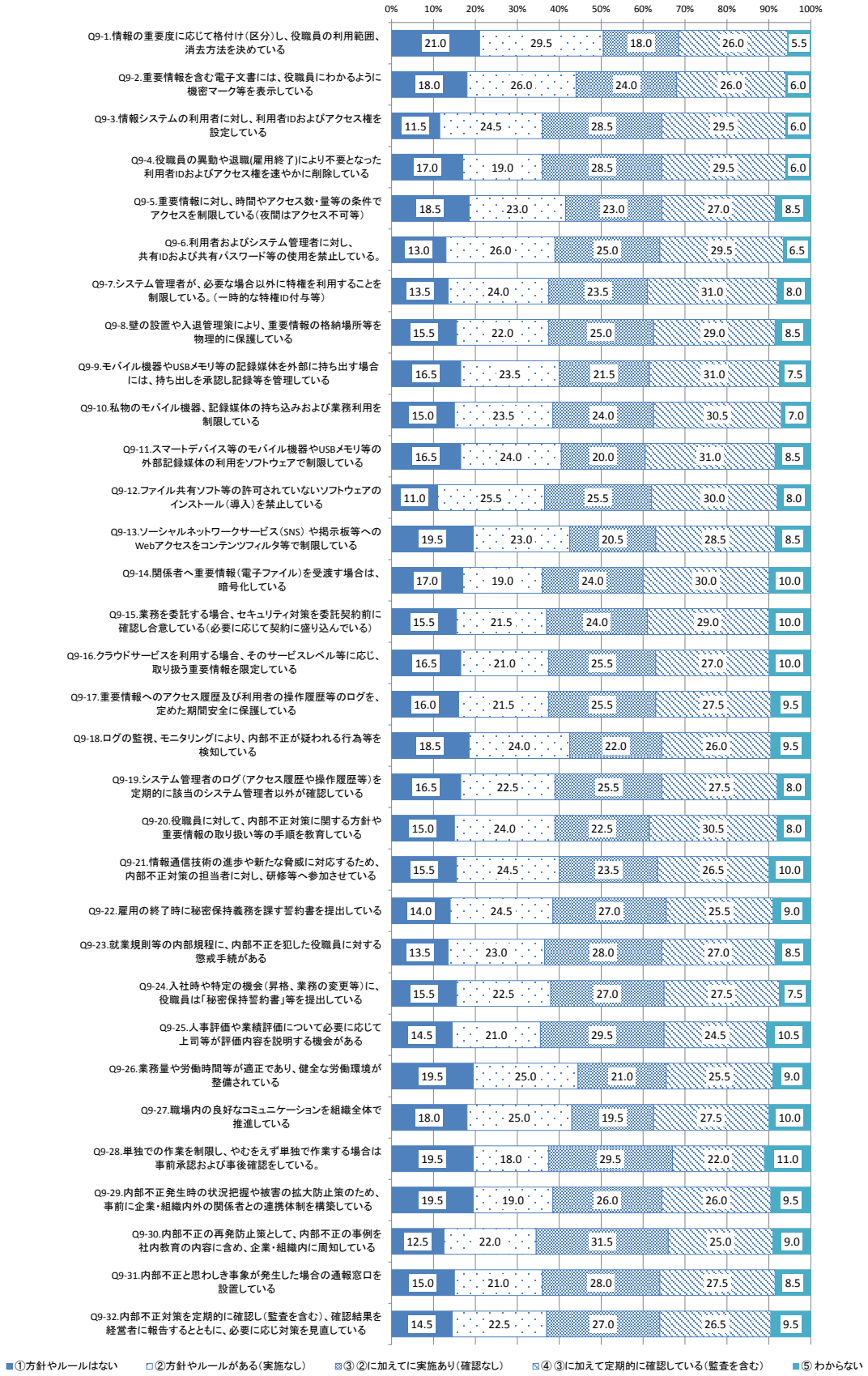

図 19　対策の実施状況（内部不正経験者）≪Q9≫

内部不正防止ガイドラインでは、基本方針、資産管理、物理的管理、技術・運用管理、証拠確保、人的管理、コンプライアンス、職場環境、事後対策、組織の管理の 10 の観点から各種対策を示している。このうち、基本方針を除く 9 の観点にあてはまる対策の実施状況を図 20、図 21、図 22 に示す。観点別実施状況は、上述の内部不正にかかわる対策の実施状況から、該当する観点別に平均値を算出したものである。なお、基本方針については、別の設問としている(図 13、図 14 を参照)。

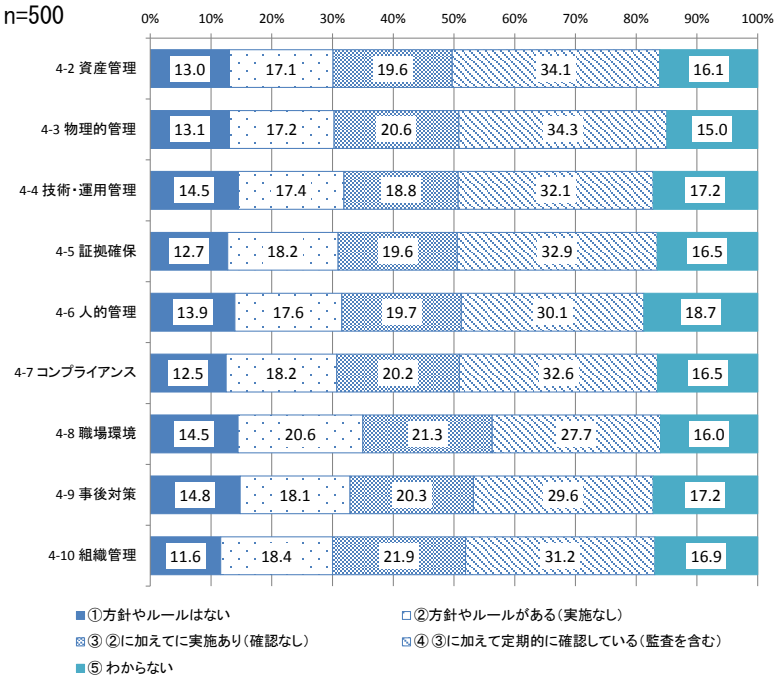

図 20　観点別実施状況(300 名以上／経営者・システム管理者のみ)≪Q9≫

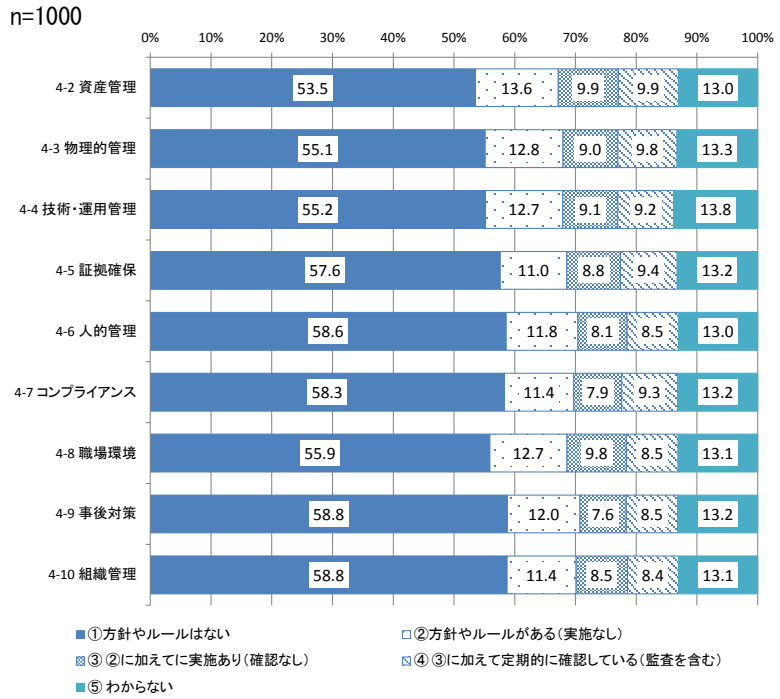

図 21　観点別実施状況(300 名未満／経営者・システム管理者のみ)≪Q9≫

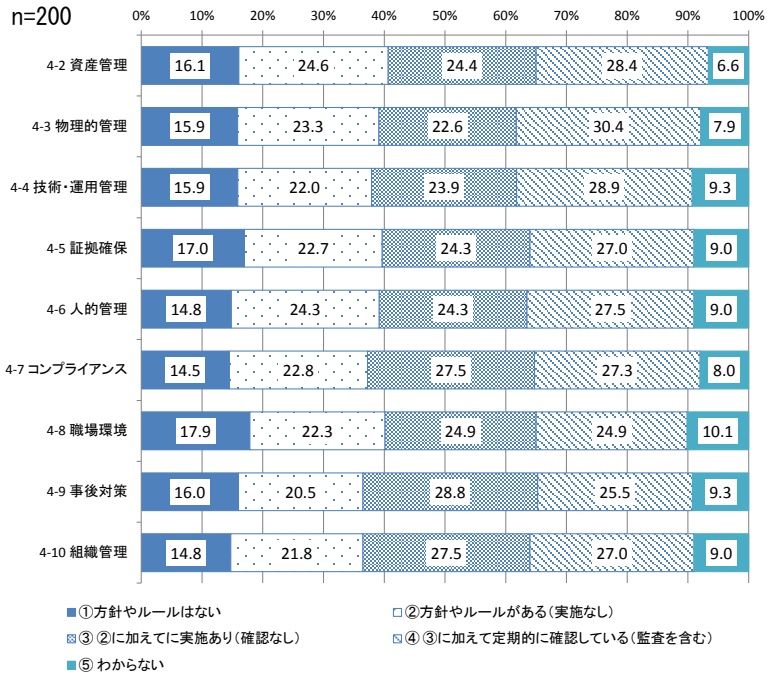

図 22　観点別実施状況（内部不正経験者）≪Q9≫

③　委託先の管理状況

所属する企業・組織が他社に業務委託[28]をしているか尋ねた結果を図 23 に示す。委託先の管理項目として、特定非営利活動法人 日本セキュリティ監査協会が公表している「サプライチェーン情報セキュリティ管理基準」[29]を参考に、「サプライチェーンにおいて重要な基準」を中心とした 14 項目を設定した。

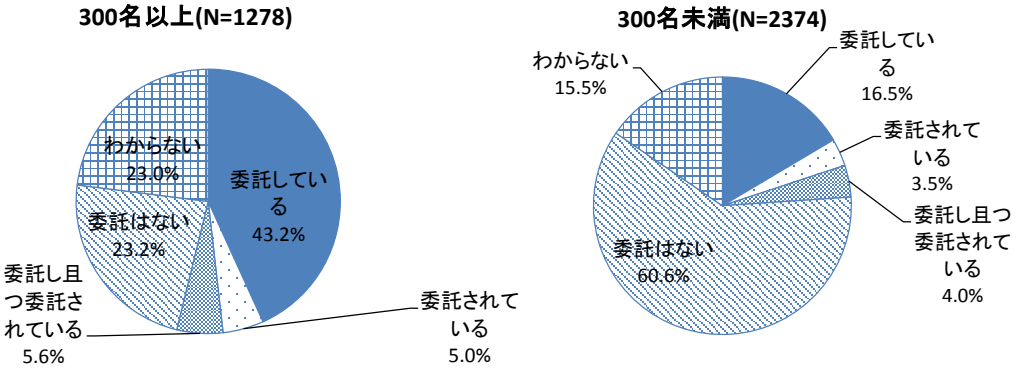

図 23　業務委託の有無≪Q10≫

ここで、他社に業務を「委託している」「委託し且つ委託されている」と回答した経営者・システム管理者に、委託先の管理状況を尋ねた。300 名以上の企業の結果を図 24、300 名未満の企業の結果を図 25 に示す。

[28] 業務の一部を、業務委託契約（準委任契約、または請負契約）を結び委託すること。ここでは、契約社員及び労働者派遣業法で定義する労働者派遣は含まない。

[29] 特定非営利活動法人日本セキュリティ監査協会：サプライチェーン情報セキュリティ管理基準
http://artemis.jasa.jp/include/result/pdf2011/2011_supplychain_doc03.pdf

図 24 より、「ISMS やプライバシーマークを取得、更新すること」を除いたすべての項目において 300 名以上の企業の 6 割程度が何らかの管理を行っていることがわかる。委託先に書面で要求している割合が最も高かった項目は、「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て実践すること」であり、300 名以上の企業で 43.7%、300 名未満の企業で 29.1%であった。

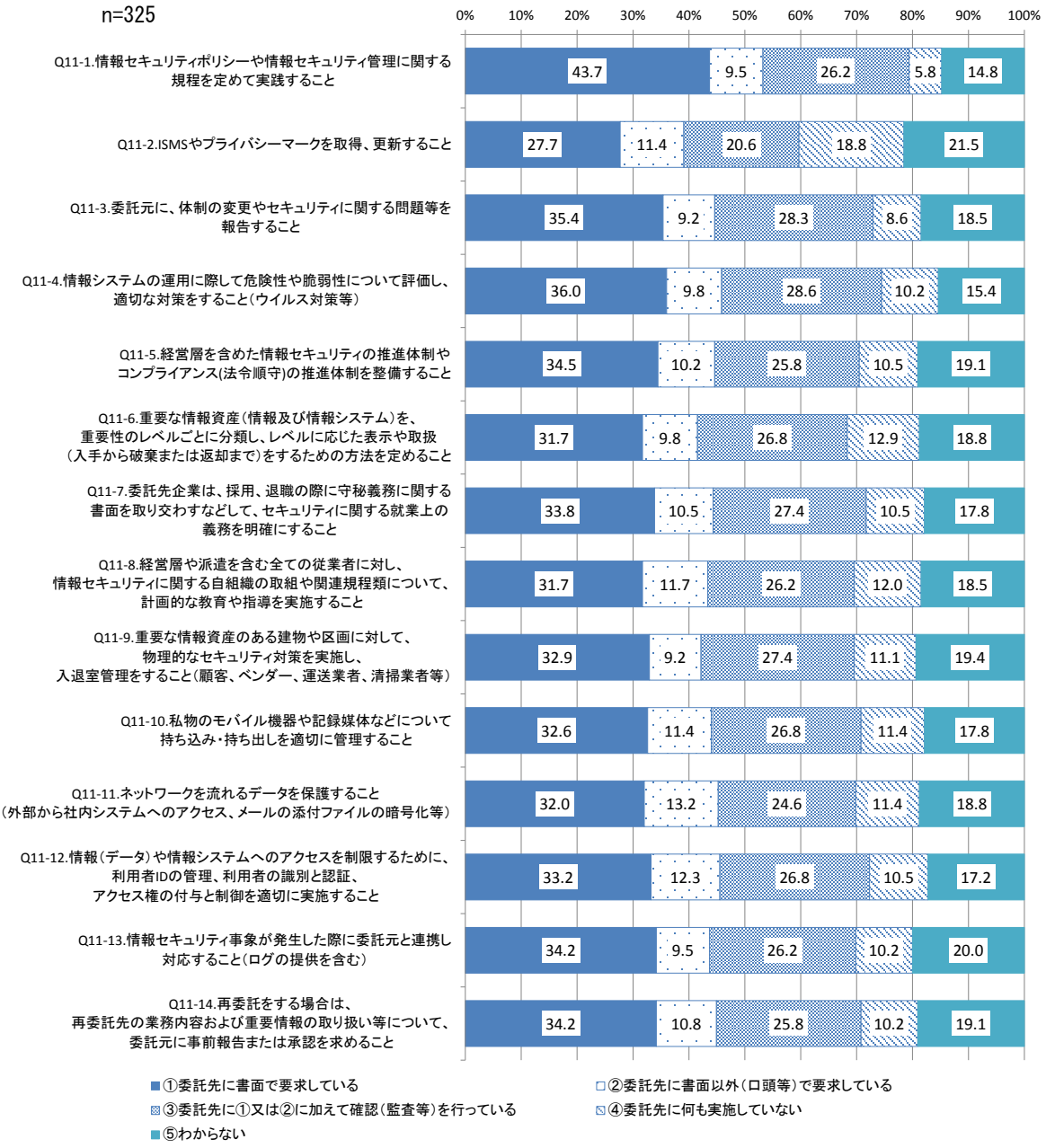

図 24　委託先管理の状況(300 名以上／経営者、システム管理者のみ)≪Q11≫

一方、図 25 より、300 名未満の企業では、300 名以上の企業と比較して、総じて管理している割合が低く、4 割を下回る項目も見られる。

図 25　委託先管理の状況(300 名未満／経営者、システム管理者のみ)≪Q11≫

図 23 で、他社に業務を「委託されている」「委託し且つ委託されている」と回答した者に、所属する企業・組織の内部不正対策の実施状況を尋ねた結果を図 26 に示す。「方針やルールはない」と答えた割合が最も低かったのは、「情報システムの利用者に対し、利用者 ID およびアクセス権を設定している」（13.7%）であり、他の項目と比べ対策が対策がとられていると考えられる。

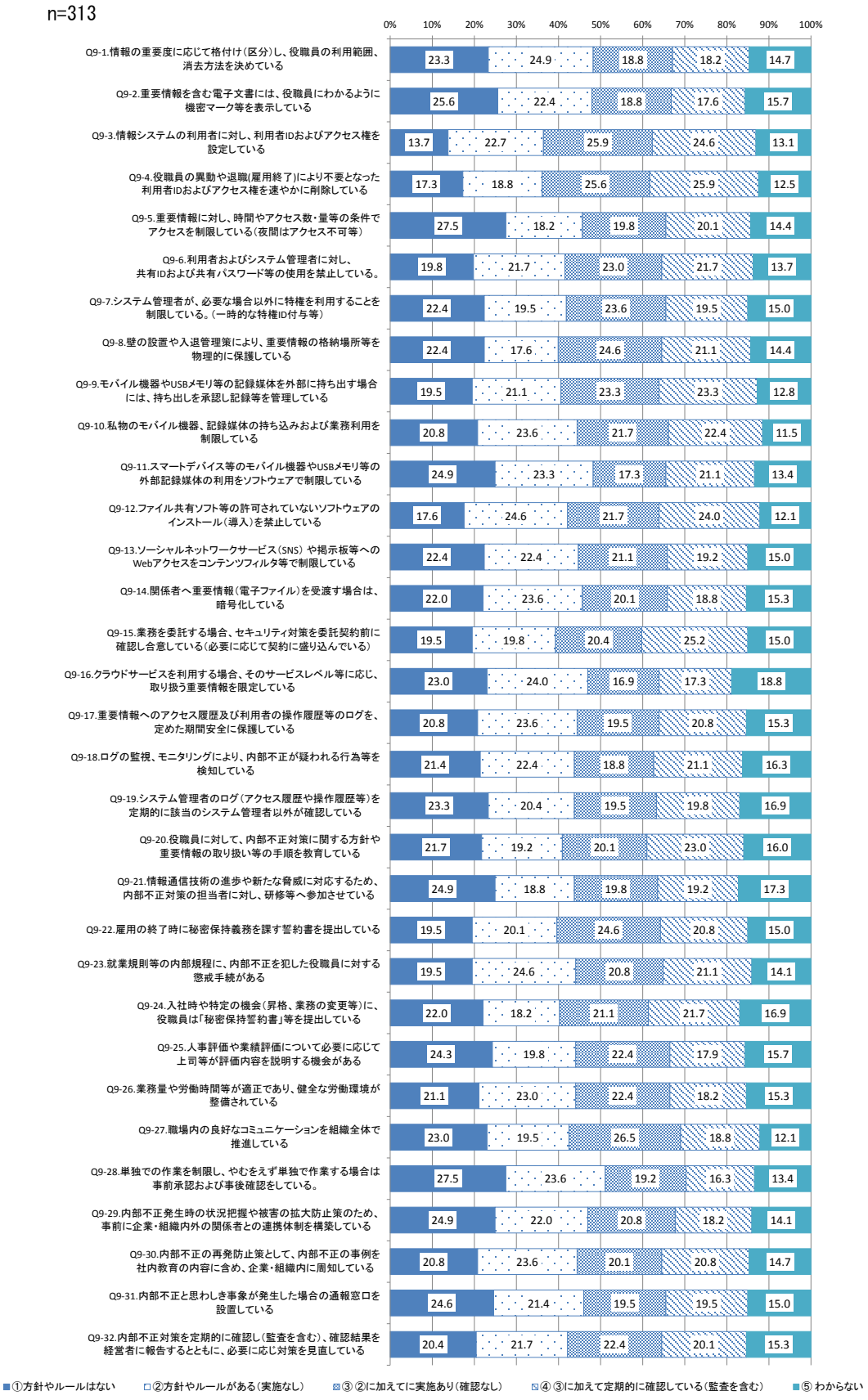

図 26　対策の実施状況（委託を受けている企業のみ）≪Q9≫

④　その他対策に関わる事項

図 27 に、所属する企業・組織の内部不正対策を検討している部署(複数回答可)を尋ねた結果を企業規模別に示す。300 名以上の企業では「情報システム部門」(63.6%)が最も多く、「総務部門」(37.0%)、「経営層」(25.0%)が続く。300 名未満の企業では「経営層」(35.9%)が最も多いが、「なし」という回答も 35.4%ある。

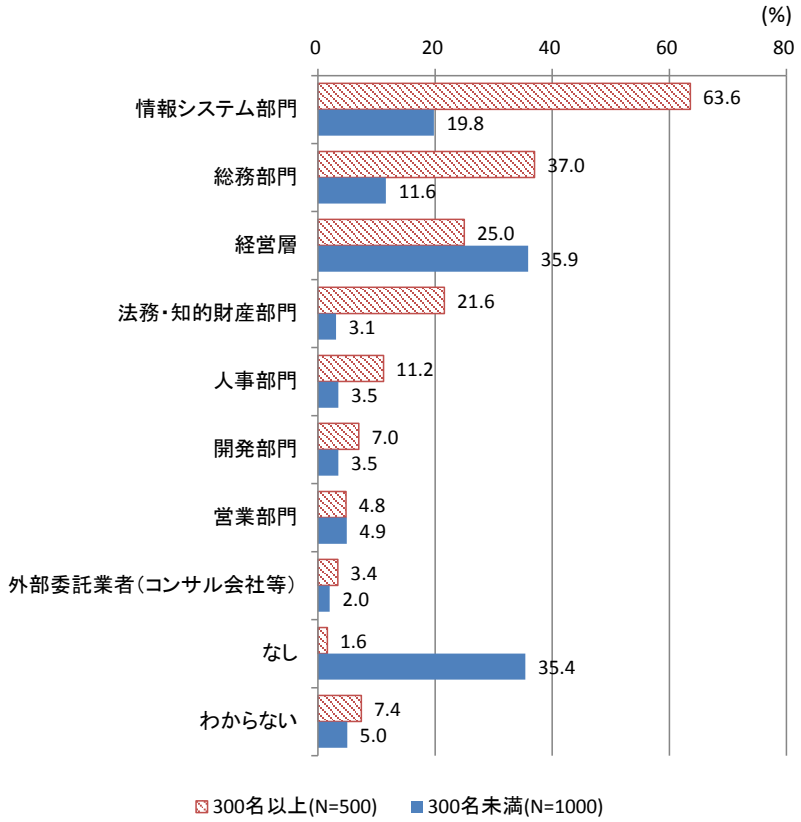

図 27　内部不正対策の検討部署（企業規模別／経営者・システム管理者のみ）≪Q12≫

また、内部不正対策の検討部署数を図 28 に示す。ここでは検討部署として、90 種類を超える部署の組み合わせ（単独部門の実施も含む）の回答があった。2部署以上で実施しているケースが約3割ある。組み合わせの上位 10 種類を表 12 に示す。最も多いケースは、情報システム部門単独と経営層単独で2割ずつである。2部署以上が連携しているケースでは、総務部門と情報システム部門の連携が最も多いが 5%程度である。なお、表 12 に示したケースのみで全体の約 8 割を占める。

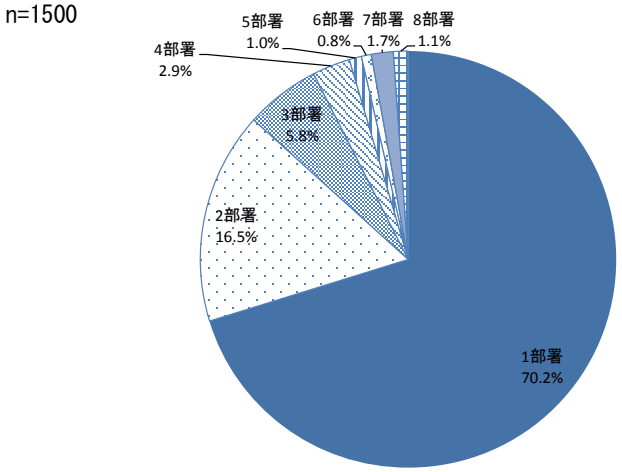

図 28　内部不正対策の検討部署数（経営者・システム管理者のみ）≪Q12≫

表 12　内部不正対策の検討部署の組み合わせ（上位 10 種類）

順位	担当部門	割合(%)
1	情報システム部門	21.9
2	経営層	20.8
3	総務部門	15.5
4	営業部門	4.9
5	総務部門、情報システム部門	4.8
6	法務・知的財産部門	2.8
7	経営層、総務部門	2.7
8	人事部門	2.7
9	経営層、総務部門、情報システム部門	2.4
10	開発部門	2.1

図 29 に、企業規模別に見た内部不正対策の検討方針を示す。300 名以上の企業では、「情報セキュリティ対策の一環として内部不正対策を検討している」(42.4%)、「ガバナンス（内部統制）の一環として内部不正対策を検討している」(41.2%)が多く、「内部不正対策は他の取組とは分けて個別に検討している」(13.6%)の約 3 倍である。一方、300 名未満の企業では 58.1%が「内部不正対策について検討していない」という結果となった。

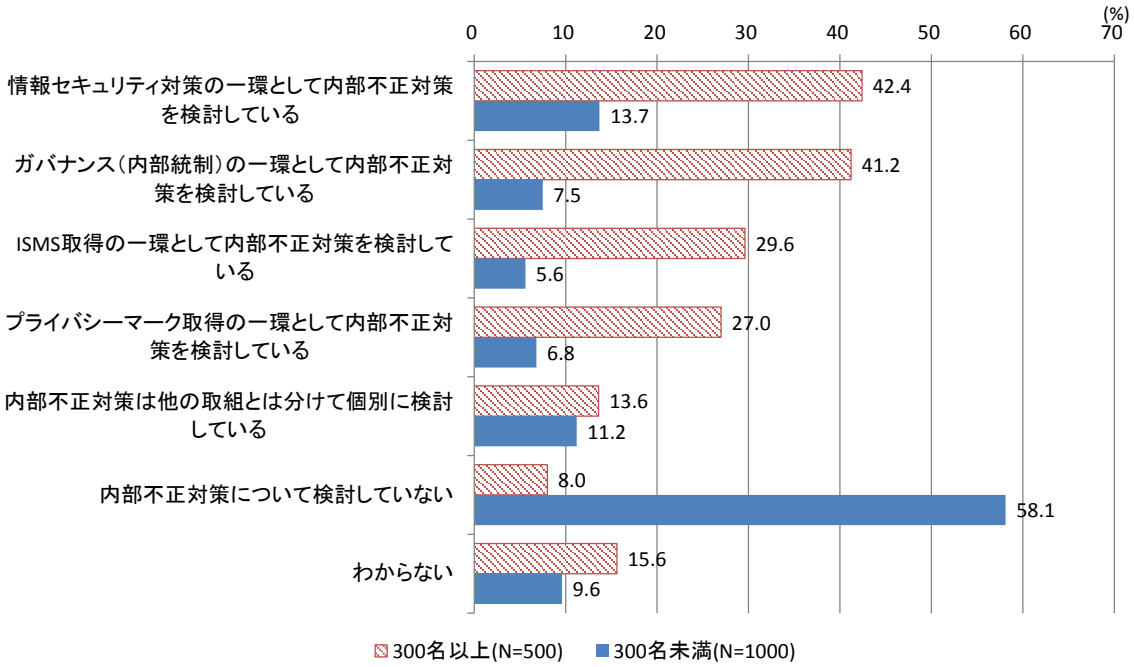

図 29　内部不正対策の検討方針（企業規模別／経営者・システム管理者のみ）≪Q13≫

図 30 に、所属する企業・組織の「内部不正対策に関わる課題」を尋ねた結果を企業規模別に示す。300 名以上の企業では、「各種対策を講じる際、部署ごとに意識のばらつきがある」(21.4%)、「現場の意識が低く各種対策が徹底されていない」(20.8%)が比較的高い。300 名未満の企業では、「内部不正対策に関わる課題は無い」が 6 割を超えた。これを除くと、「経営層による内部不正対策への意識が低い」(14.2%)が最も高い。

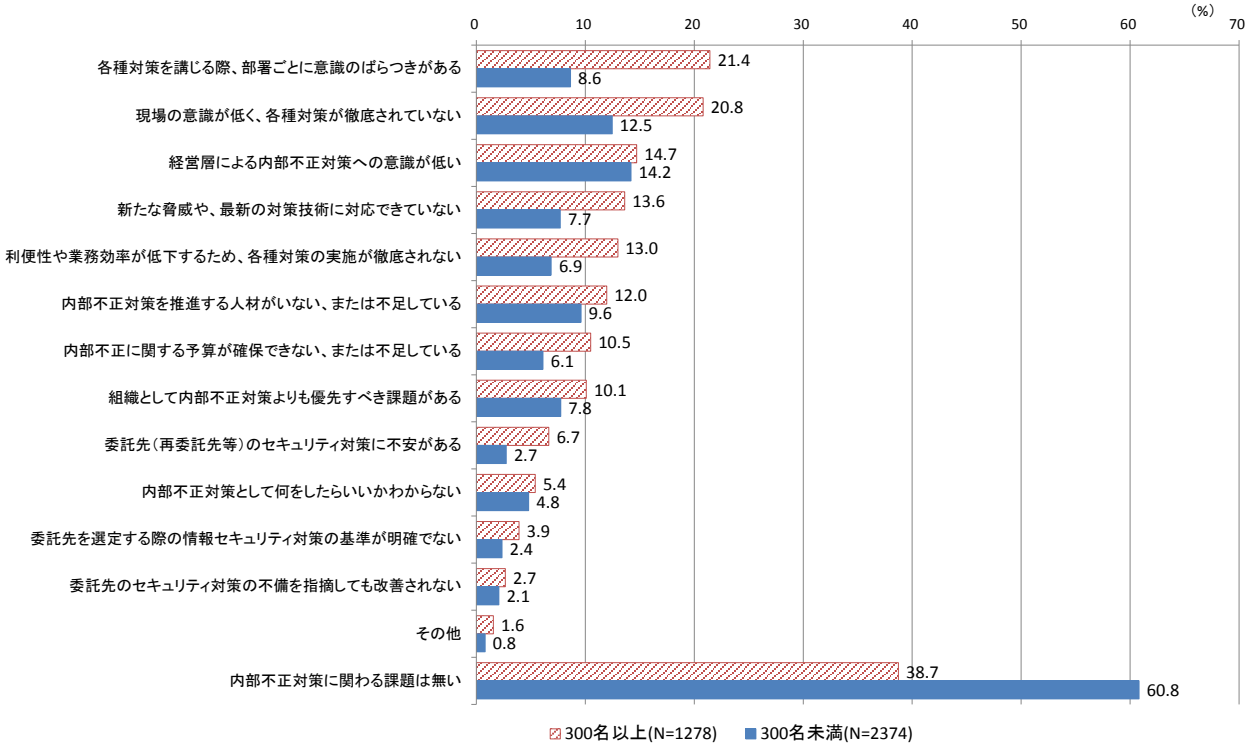

図 30　内部不正対策に関わる課題（企業規模別）≪Q14≫

図 31 に、昨年度と比較して「内部不正対策にかける予算に変化があったか」尋ねた結果を企業規模別に示す。300 名以上の企業では、予算が「減った」(5.4%)割合に対し、「増えた」(13.2%)が 2 倍以上となった。予算の変化がない企業が約 6 割を占めるが、その約半数で「対策は変わった」(27.2%)と回答している。一方、300 名未満の企業では、予算が「減った」(3.8%)と「増えた」(3.4%)の割合がほぼ同じである。予算の変化がない企業が約 7 割を占め、51.0%が予算も対策内容にも変化は無いと回答している。

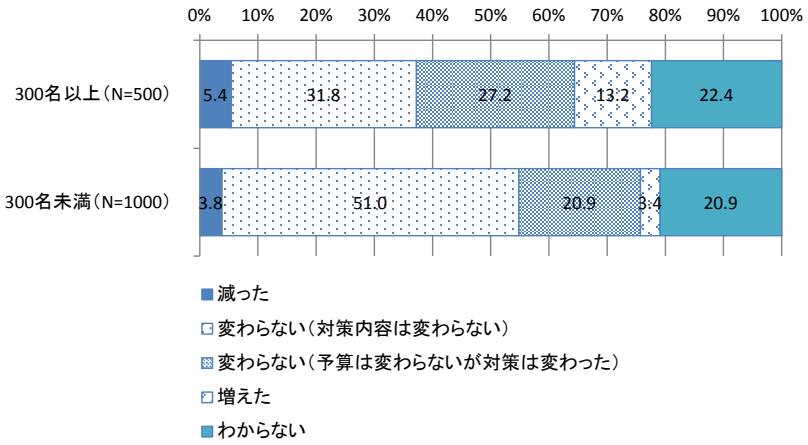

図 31　内部不正対策にかける予算の変化（企業規模別／経営者・システム管理者のみ）≪Q16≫

図 32 に、「内部不正対策を見直すきっかけとなった出来事」を尋ねた結果を企業規模別に示す。300 名以上の企業の 22.1%が 2016 年 1 月のマイナンバー導入を契機に対策の見直しを行っている。教育事業者による個人情報の漏洩や、公的機関のサーバへの不正アクセスによる個人情報の漏洩といった事件をきっかけに見直した企業は 1 割を超える。300 名未満の企業では、割合はより低くなるが同じ傾向がみられる。

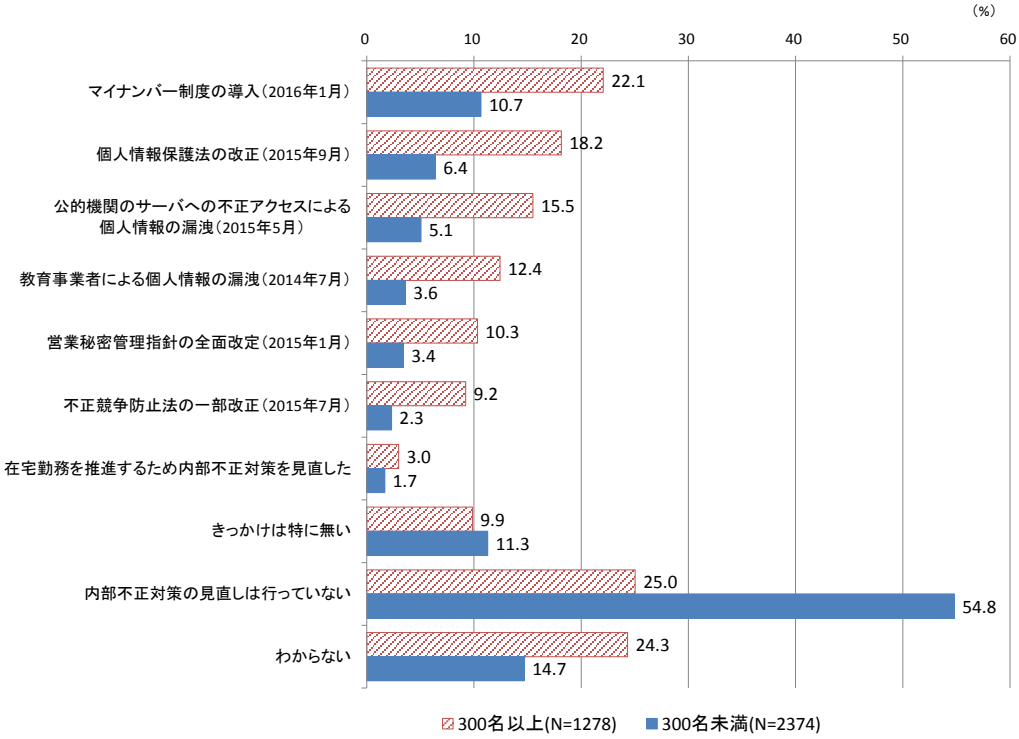

図 32　内部不正対策を見直すきっかけ（企業規模別）≪Q15≫

3.2.3　内部不正発生時の対応

内部不正経験者に、故意の内部不正に対する処分を尋ねた結果を図 33 に示す。「懲戒処分や起訴はしなかった」が 30.9%、「社内規定に従い懲戒処分とした」が 51.7%である。

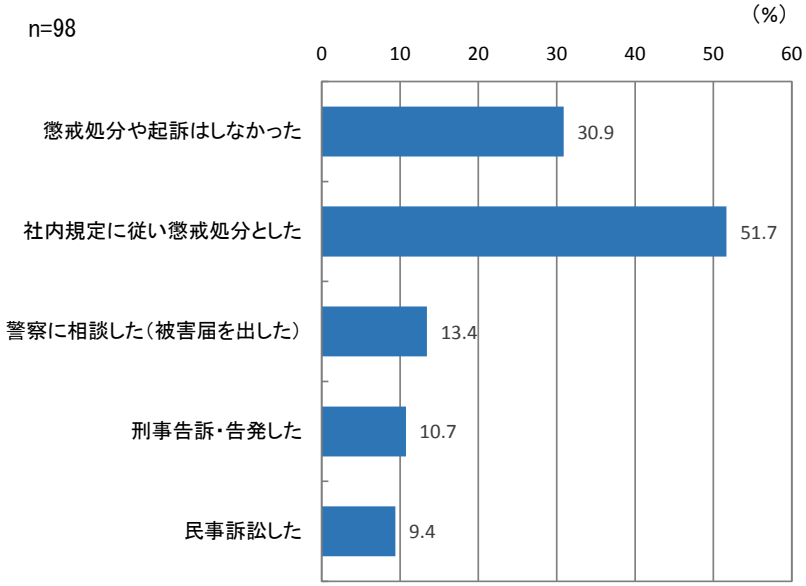

図 33　故意に内部不正を行った者への処分の状況（内部不正経験者）≪Q7-1-6≫

さらに、上記設問で「懲戒処分や起訴はしなかった」と回答した者に、その理由を尋ねた結果を図 34 に示す。「懲戒処分や起訴ほどの被害が出なかった」(41.3%)が最も多い。次に多いのは、「証拠がない、情報が不足している」(32.6%)であり、「不正行為を行った個人を特定できなかった」(23.9%)も含め、十分な証跡が取れていなかったために処分ができなかった可能性がある。

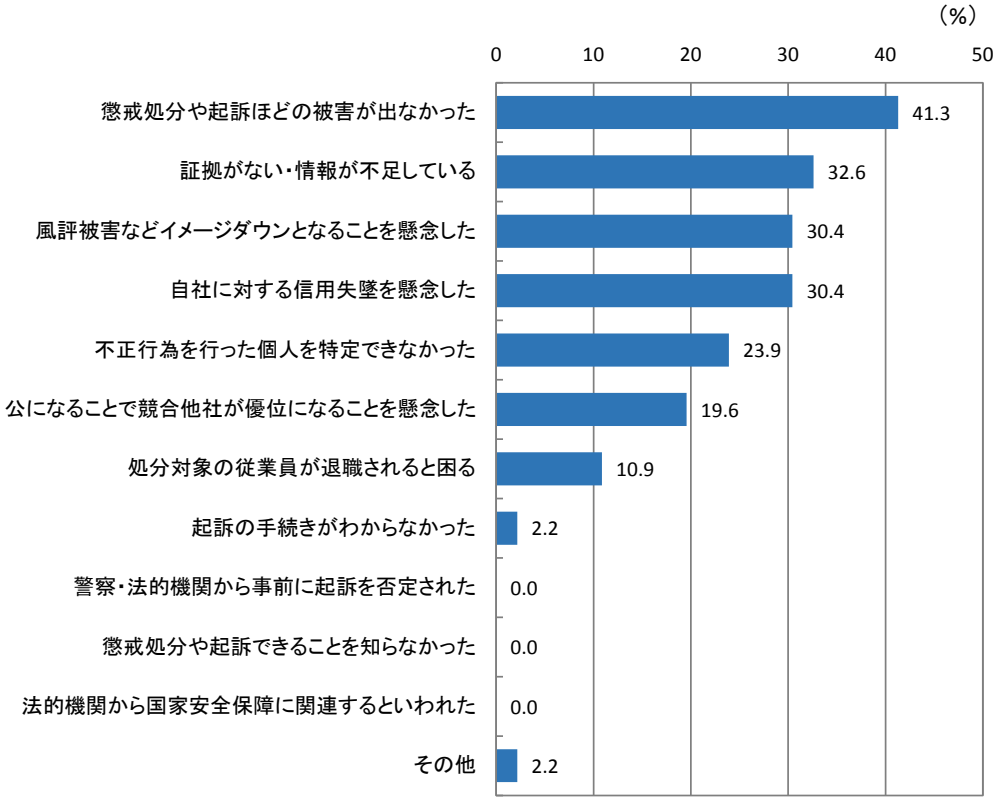

図 34　懲戒処分や起訴を行わなかった理由（故意／内部不正経験者）≪Q7-2≫

図 35 に、「内部不正が発生し、企業・組織内で解決できた場合に、その詳細を外部に公開するか」経営者・システム管理者に尋ねた結果を企業規模別に示す。300 名以上の企業では、「公開する」、「場合によっては公開する」が合わせて 6 割を超えており、公開に積極的である。300 名未満の企業では、「場合によっては公開しない」「公開しない」が合わせて 4 割程度だが、「公開する」、「場合によっては公開する」も 3 割程度あり、どちらかといえば非公開の傾向にある。

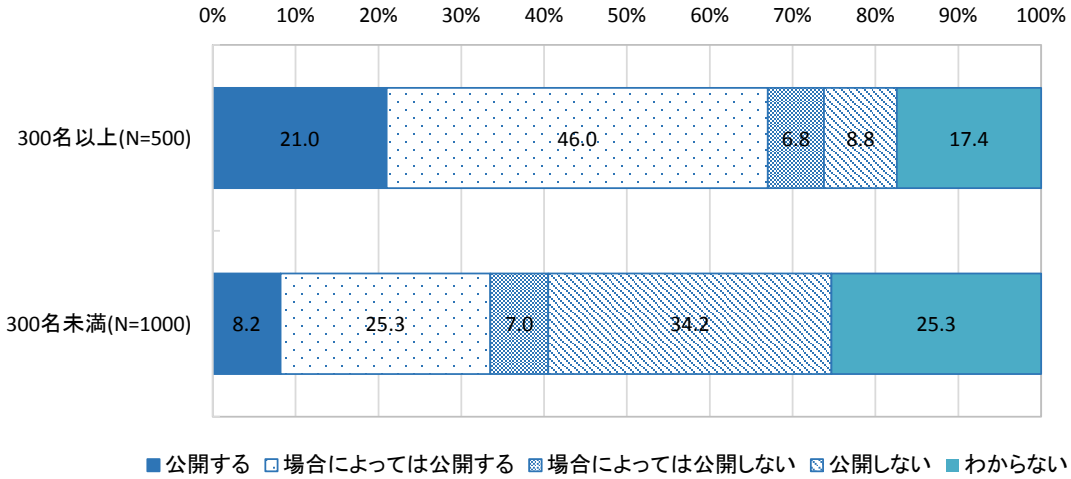

図 35　調査①：内部不正発生時の公開の有無（企業規模別／経営者・システム管理者のみ）≪Q18≫

上記設問で、外部に「公開しない」、「場合によっては公開しない」という回答者に、その理由を尋ねた結果を図 36 に示す。前回の調査では、今回の調査と選択肢が異なるが、内部不正が発生した場合に公開しない理由として、「風評被害などの企業のイメージダウンとなる可能性がある」(25.0%)、「関係者との調整が困難」(20.0%)が挙げられた。今回の調査では、300 名以上の企業では、「重要情報の漏えいが拡大する可能性があるから」(30.5%)が最も多い。300 名未満の企業では、「関係者との調整が困難だから」が最も多く、34.9%となった。次点はどちらも「自組織に対する否定的な評判が広まる可能性があるから」である。規模の大きな企業では、二次被害を防ぐために公表しないという判断につながっている可能性が示唆される。

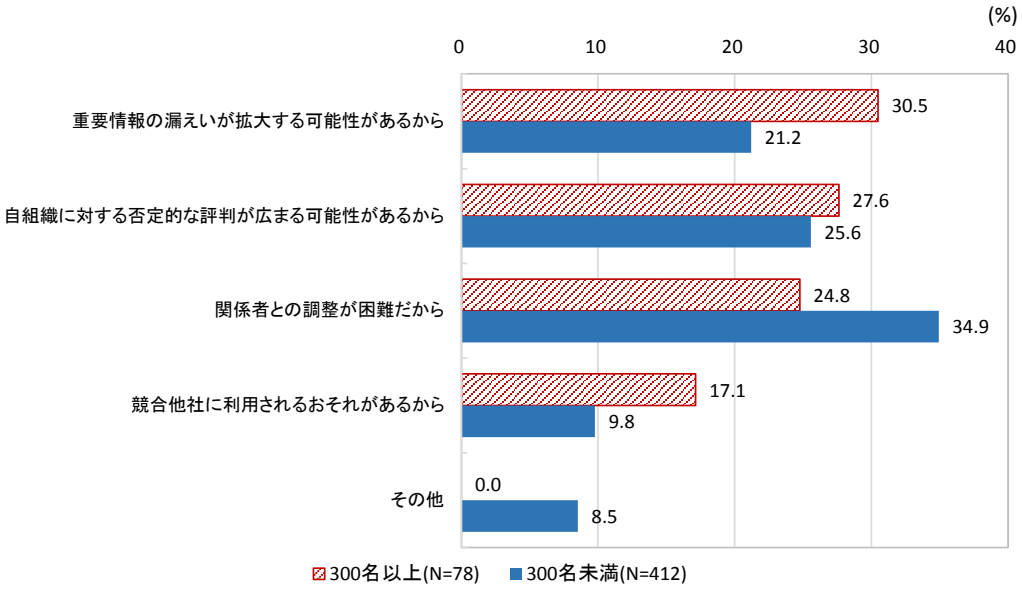

図 36　公開しない理由（企業規模別／経営者・システム管理者のみ）≪Q19≫

図 37 に、内部不正が発生した場合に想定されるリスクについて、経営者・システム管理者に尋ねた結果を企業規模別に示す。300 名以上の企業では「社会的信用失墜」(51.4%)、「損害賠償等の費用の発生」(42.4%)、「イメージダウン」(30.4%)が高い結果となった。300 名未満の企業でも、「社会的信用失墜」(35.1%)、「イメージダウン」(29.9%)、「損害賠償等の費用の発生」(26.4%)が高い。300 名未満の企業では、「従業員の退職による事業の継続困難」(15.0%)が 300 名以上の企業の割合を上回った。

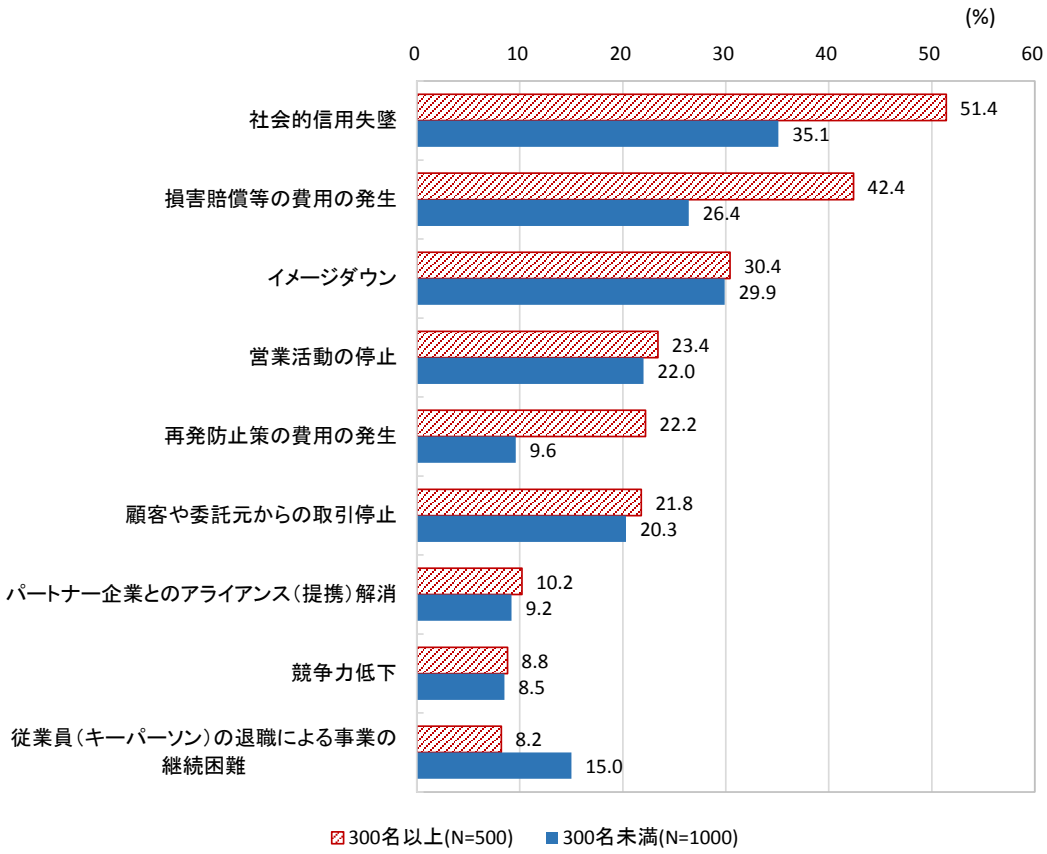

図 37　内部不正が発生した場合に想定されるリスク（企業規模別／経営者・システム管理者のみ）≪Q21≫

3.2.4　経営者・システム管理者と従業員の意識

① 効果的な対策に関する意識

内部不正に効果的だと思われる対策を尋ねた。300 名以上の企業について、職種別に見た結果を図 38 に示す。経営者、システム管理者が効果的だと考える対策の上位 3 つは、「技術情報や顧客情報などの重要情報は特定の職員のみがアクセスできる」、「ネットワークの利用制限がある」、「技術情報や顧客情報などの重要情報にアクセスした人が監視される」である。従業員が不正を行いたいと思う気持ちが低下する対策は、「情報システムの管理者以外がアクセス管理を操作することを制限している」、「技術情報や顧客情報などの重要情報は特定の職員のみがアクセスできる」、「技術情報や顧客情報などの重要情報にアクセスした人が監視される」である。

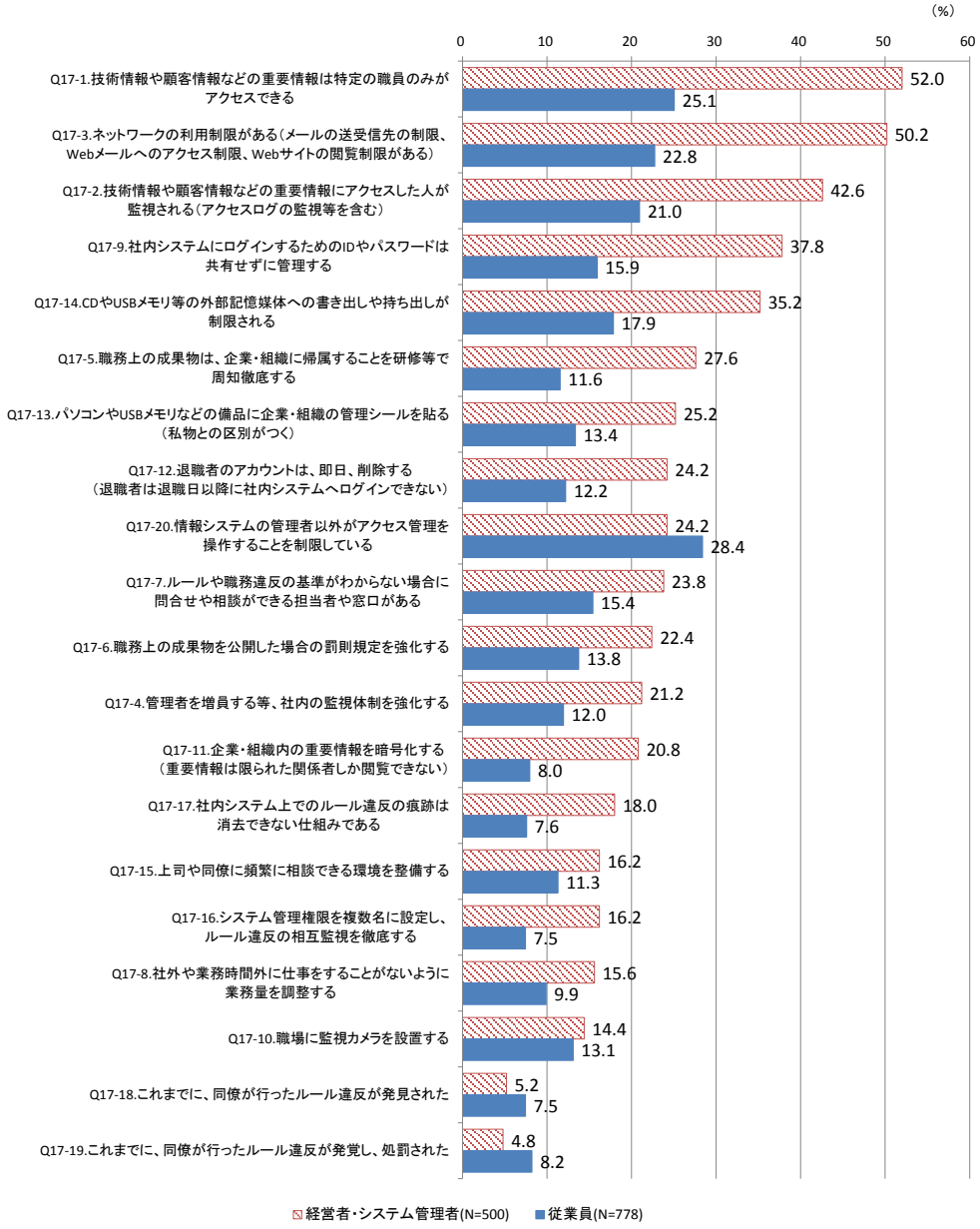

図 38　内部不正に効果的だと思われる対策（300 名以上／職種別）≪Q17≫

また、300 名未満の企業について、職種別に見た結果を図 39 に示す。経営者、システム管理者が効果的だと考える対策の上位 3 つは、「技術情報や顧客情報などの重要情報は特定の職員のみがアクセスできる」、「情報システムの管理者以外がアクセス管理を操作することを制限している」、「ネットワークの利用制限がある」である。従業員も順序は異なるものの、これらを上位 3 つの対策に挙げている。

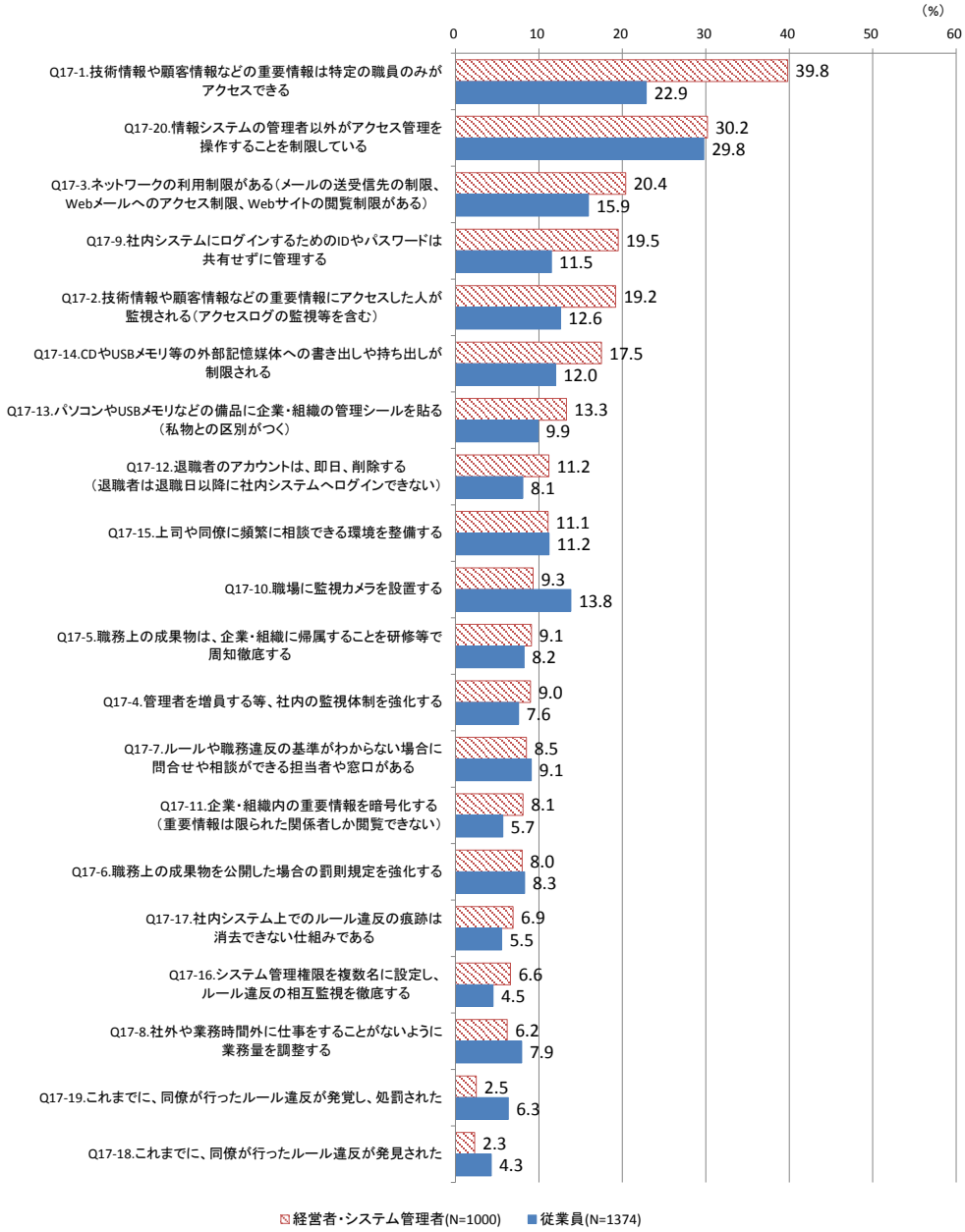

図 39　内部不正に効果的だと思われる対策（300 名未満／職種別）≪Q17≫

内部不正経験者に、内部不正に効果的だと思われる対策を尋ねた結果を図 40 に示す。内部不正経験者が効果的だと考える上位 3 つの対策は、「ネットワークの利用制限がある」、「技術情報や顧客情報などの重要情報にアクセスした人が監視される（アクセスログの監視等を含む）」、「技術情報や顧客情報などの重要情報は特定の職員のみがアクセスできる」である。

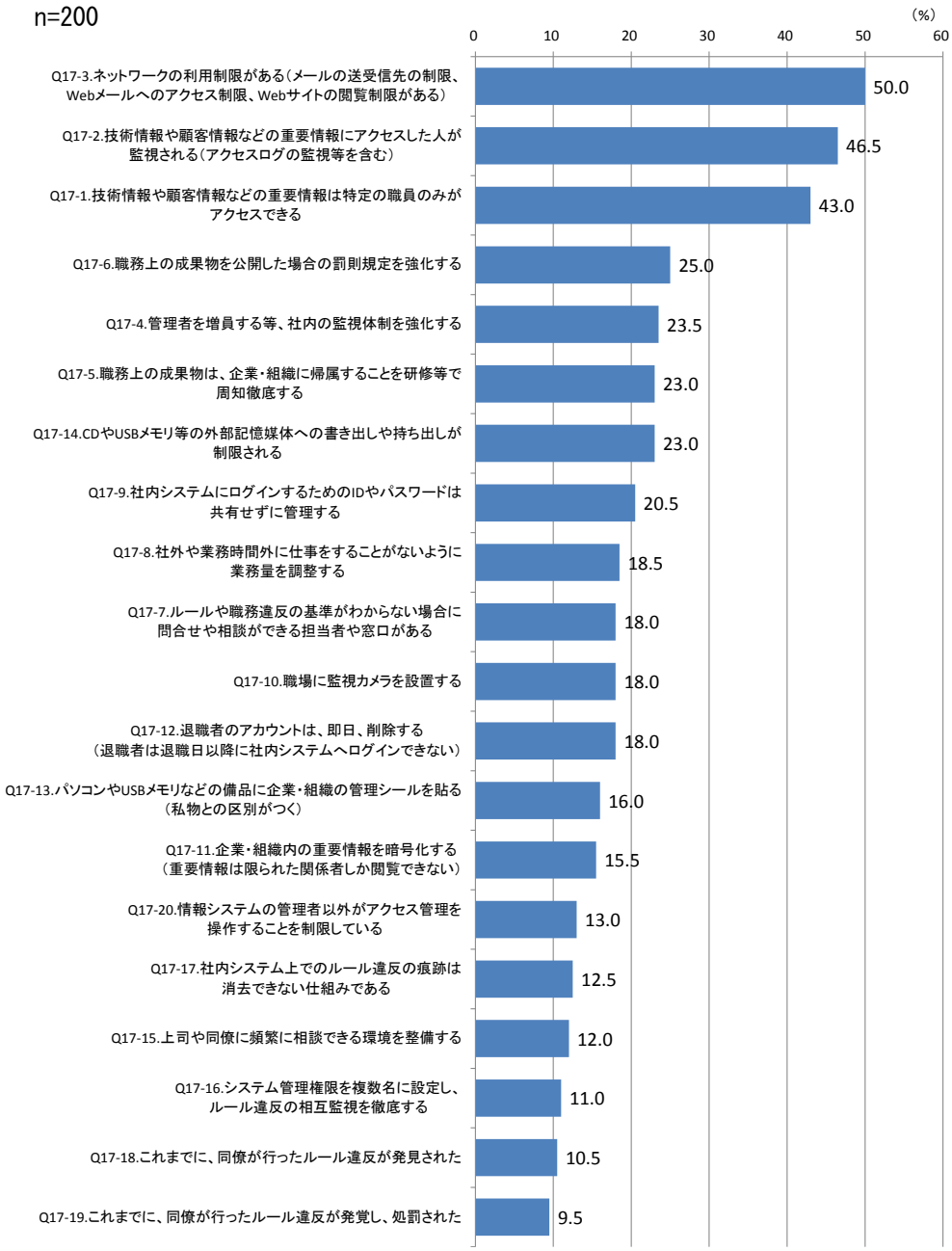

図 40　内部不正に効果的だと思われる対策（内部不正経験者）≪Q17≫

内部不正に効果的だと思われる対策について、内部不正経験者と経営者・システム管理者[30]の順位との比較を表 13 に示す。両者の違いが顕著だったのは、内部不正経験者にとって効果的と考える 4 位の「職務上の成果物を公開した場合の罰則規定を強化する」、5 位の「管理者を増員する等、社内の監視体制を強化する」であり、経営者・システム管理者でそれぞれ 12 位、11 位であった。なお、監視強化についての意識の差は前回の調査でも上位になっている。

表 13　効果的だと思う対策の比較（内部不正経験者と経営者・システム管理者）

内部不正経験者		対策	経営者・システム管理者	
順位	割合		順位	割合
1 位	50.0%	ネットワークの利用制限がある（メールの送受信先の制限、Web メールへのアクセス制限、Web サイトの閲覧制限がある）	2 位	30.3%
2 位	46.5%	技術情報や顧客情報などの重要情報にアクセスした人が監視される（アクセスログの監視等を含む）	4 位	27.0%
3 位	43.0%	技術情報や顧客情報などの重要情報は特定の職員のみがアクセスできる	1 位	43.9%
4 位	25.0%	職務上の成果物を公開した場合の罰則規定を強化する	12 位	12.8%
5 位	23.5%	管理者を増員する等、社内の監視体制を強化する	11 位	13.1%

（内部不正経験者：n=200、経営者・システム管理者：n=1500）

[30] 調査②の内部不正行為者は、企業規模等を考慮せず集計している。そのため、ここでは調査①のすべての経営者・システム管理者の割合と比較する。

② 監視、持ち出し、内部不正対策に関わる意識

監視、持ち出し、内部不正対策に関わる意識について尋ねた結果を企業規模別に図 41 に示す。300 名未満の企業が「あてはまる（非常にあてはまるとあてはまるの合計）」という回答が少ないものの、300 名以上の企業と 300 名未満の企業で回答傾向は似ている。「従業員のプライバシーよりも組織・企業のセキュリティを守るため、操作情報・取り扱っているデータが監視されることはやむをえない」については、300 名以上の企業の 74.6%、300 名未満の企業の 58.4%が「あてはまる」と回答している。

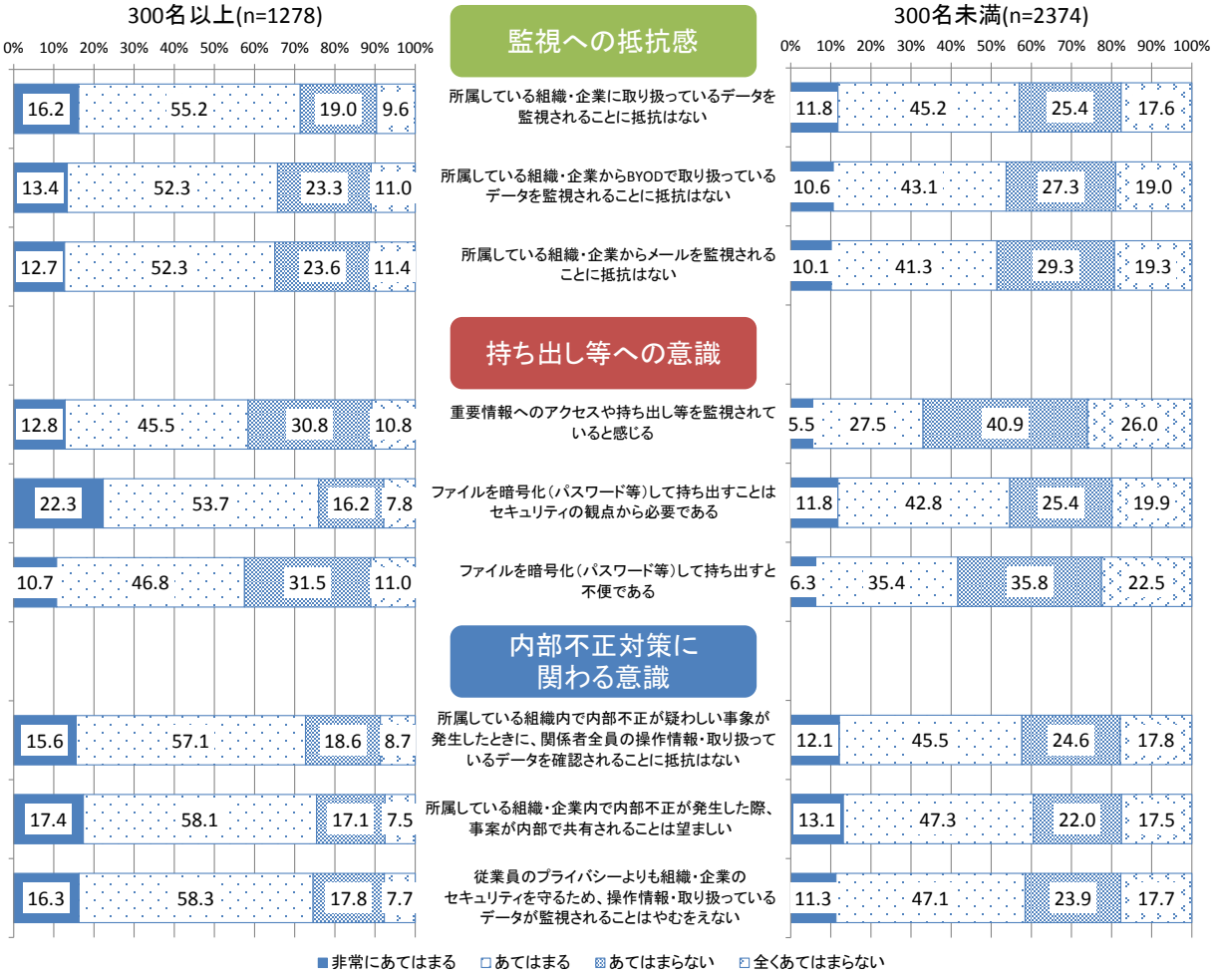

図 41　監視、持ち出し、内部不正対策に関わる意識（企業規模別）≪Q24≫

図 41 を職種別にみた結果を図 42 に示す。経営者・システム管理者と従業員では同じような回答傾向がみられるが、監視の抵抗感等は従業員の方が強い。

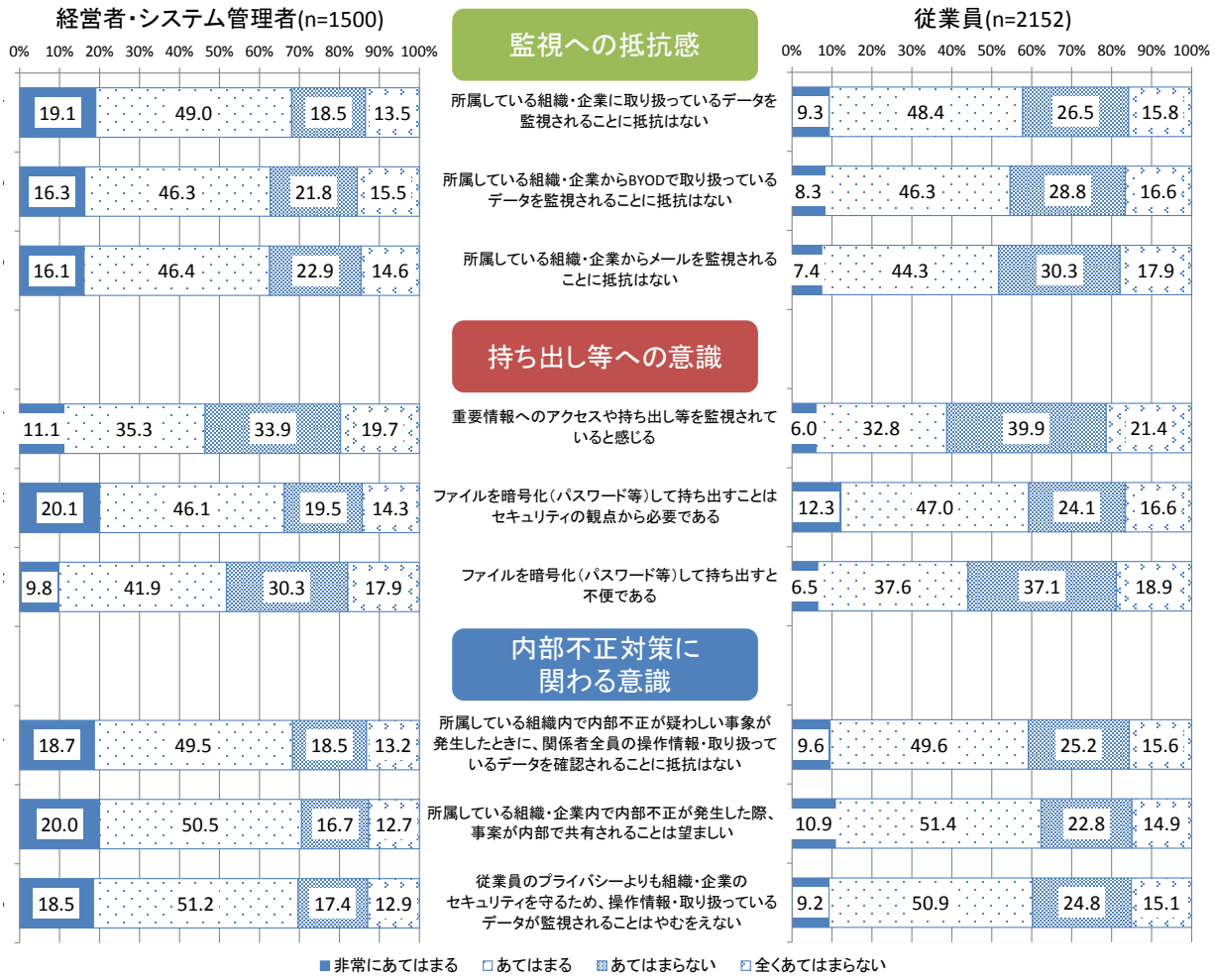

図 42　監視、持ち出し、内部不正対策に関わる意識（職種別）≪Q24≫

内部不正行為者に、監視、持ち出し、内部不正対策に関わる意識について尋ねた結果を図 43 に示す。従業員規模別、職種別の結果と比較しても内部不正経験者の監視への抵抗感は弱い。

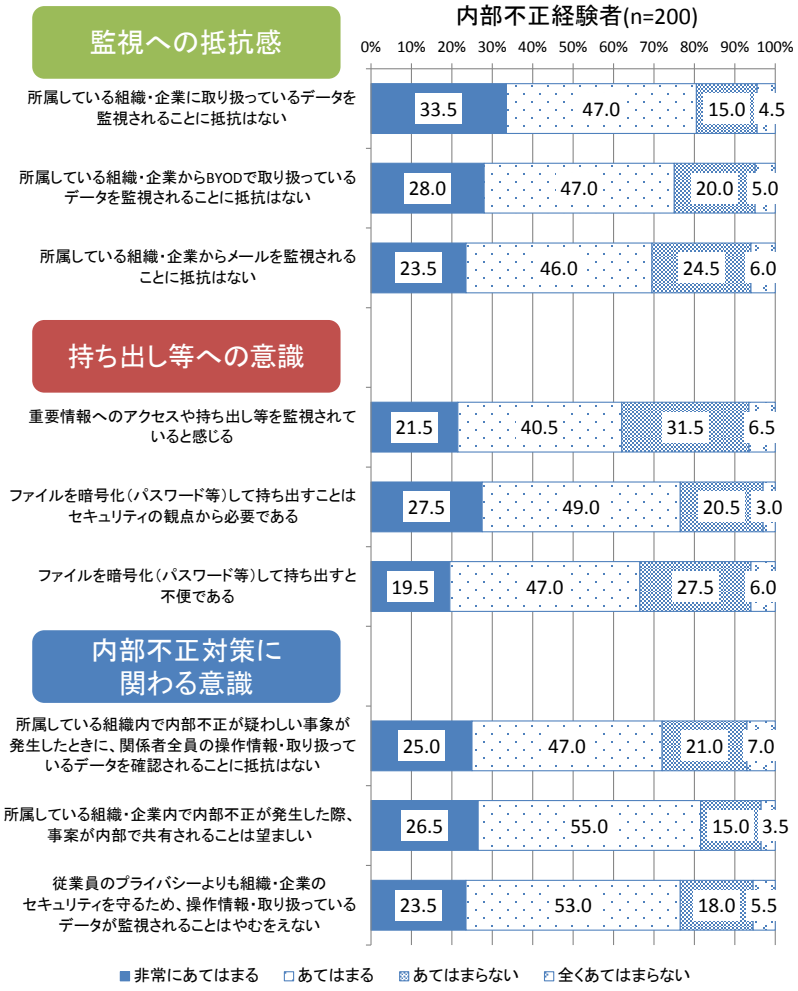

図 43　監視、持ち出し、内部不正対策に関わる意識(内部不正経験者)≪Q24≫

職場環境・企業風土等に関するアンケート調査結果は、「付録3:職場環境・企業風土等に関するアンケート調査結果」を参照されたい。

3.2.5　国内における内部不正の実態（推計の結果）

内部不正、外部攻撃の発生状況の結果から「内部不正（軽微なポリシー違反含む）があった」という回答の割合を企業規模と業種別に算出し、日本における内部不正発生数の推計を行った。業種、企業規模の推計には、「平成 24 年　経済センサス活動調査　企業等に関する集計　産業横断的集計（企業等数、従業者数）」の結果を用いた。前提として、内部不正発生割合は、今回実施したウェブアンケート調査を用いており、回答者の重複はないが、回答者が同一企業に所属している可能性は排除できない状況で推計を行っている。また、これまでに内部不正が発生したかどうか尋ねた結果を用いているため、1 年間に発生する企業の推計ではない。

上述の推計から内部不正（軽微なポリシー違反含む）が発生している企業数を推計すると、60,228 件で、日本の企業数全体の 1.4%となった。

4. インタビュー調査

本章では、内部不正に関するインタビュー調査の結果を報告する。

4.1 インタビュー調査概要

効果的な内部不正対策を検討するための被害事例収集、内部不正を防止するためにとることのできる法的な対策の 2 つについて、インタビュー調査を実施した。

被害事例収集のインタビュー調査では、実際に情報セキュリティインシデントの被害を受けた企業の担当者、インシデント対応や調査・分析を行ったフォレンジック関係者、CSIRT 関係者の協力を得て、表 14 に示した調査項目を面談形式で確認した。

表 14　被害事例収集のインタビュー調査項目

分類	項目
内部不正概要	・ 情報セキュリティインシデントの発生状況 ・ 内部不正対策の実施状況
重要情報と対策事例	・ 対象の企業が持つ重要情報（知的財産等）の分類 ・ 重要情報（知的財産等）を安全に管理する手法 ・ 重要情報（知的財産等）を活用する手法 ・ インシデントからの復旧や原因究明及び証拠保全のための対策
有効と考えられるインシデント対策事例	・ インシデントの証拠保全のために必要な対応 ・ 企業（組織）で最低限実施すべき対策 ・ 内部不正対策を考慮したインシデントレスポンスの在り方 ・ CSIRT の有効性

法的対策に関するインタビュー調査は、内部不正による情報セキュリティインシデントに対し、企業が実施している（または実施すべき）法的対策や適法の範囲等について、法律家の協力を得て、表 15 に示した調査項目を面談形式で確認した。

表 15　法的対策に関するインタビュー調査項目

分類	項目
従業員の採用について	・ 採用時の事前調査（身辺調査等）について ・ 事前調査で適法に調査可能な範囲
業務委託先との契約について	・ 委託先の体制 ・ 委託先の規程等の点検 ・ 委託先の監査（再委託先も含む） ・ システムログの提供 ・ 内部不正発生時（疑われた場合を含む）の対応

4.2　インタビュー調査で収集した事例

インタビュー調査によって収集した事例は 10 件である。これらの事例を分類した結果を図 44 に示す。

不正行為者は、従業員が最も多く、次いで派遣社員、委託先従業員の順であった。また、不正行為は、機密情報・重要情報等の「持出し」（一部メール転送も含む）が 7 割であり、社内システム内のデータや提供サービスの「破壊」が 3 割であった。

これら不正行為の手段について、前章で述べたアンケート結果（図 11）では、情報等の種類によらず USB メモリが最も多かったが、インタビューで得た事例では、電子メールや、私物の HDD[31]、自宅に設置した NAS[32]等が用いられた事例も得られた。

収集した事例の詳細については、「付録1：事例集（インタビュー調査）」を参照されたい。

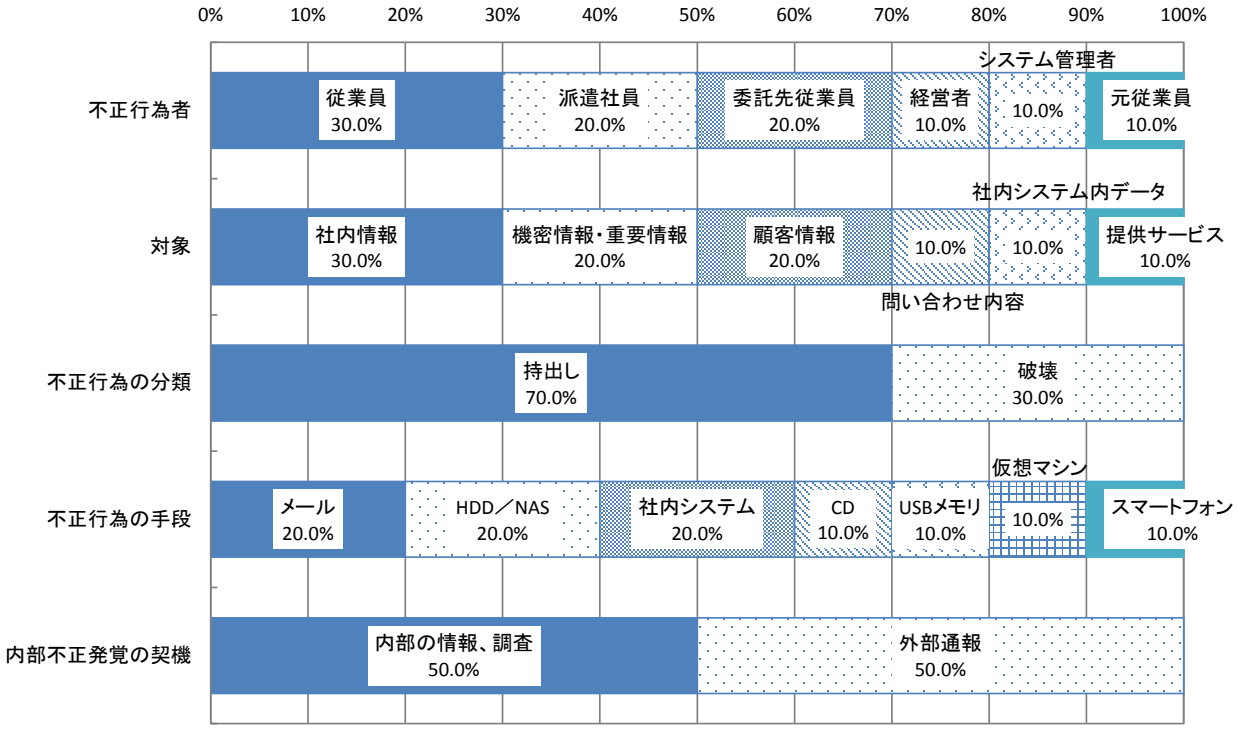

図 44　インタビュー調査結果の詳細分類 (n=10)

[31] HDD：(Hard Disk Drive)

[32] NAS：(Network Attached Storage)

4.3　インタビュー調査で得られた内部不正対策の検討状況等

効果的な内部不正対策を検討するため、実際に被害を受けた企業の担当者等にインタビューを実施した。結果を以下に報告する。

4.3.1　内部不正の概要

① 情報セキュリティインシデントの発生状況

企業の担当者に対し、内部不正による情報セキュリティインシデントが発生しているか尋ねた結果を表 16 に示す。すべての調査対象者が「内部不正が発生している」と回答した。内部規程違反等の軽微なインシデントがほとんどであるが、中には刑事事件に発展した事例を持つ企業もあった。

また、実際にインシデント対応や調査・分析を行ったフォレンジック関係者等（以下、専門家）に、最近の内部不正に関する傾向を尋ねた結果を表 17 に示す。内部不正への対応が増加傾向にあることがわかる。

表 16　内部不正による情報セキュリティインシデントの発生状況

○大企業の場合
・重大な事故には至っていないが、2014 年度は 30 件に満たないヒヤリハット事例が発生している。
メール・FAX の誤送信や郵便物の誤発送の発生頻度が高い。インシデントの記録によると、毎年、若干の減少傾向にある。
・刑事事件に発展した事例以降、インシデントをカウントしている。（PC や USB メモリの紛失、USB メモリからのウイルス感染、規程違反等の軽微なインシデントを含め）当初は月 20 件程度の報告があった。その後減少傾向にあり、現在は月 1、2 件程度の報告がある。
・発生したインシデントを報告させるようにしている。2014 年度に発生したインシデントのうち、機密性の高い情報に関わるものは約 20%であった。内部不正の発生件数は少ないが、重大な損害に結びつく可能性が高いと考えている。

○中小企業の場合
・社内の内部不正はうっかりミス、棚に施錠がされていないといった軽微なもののみと把握している。
・「認められた権限を逸脱する ID／パスワードを持っていた」、「セキュリティカードを返却しないまま退職した」、「現場で勝手にツールを導入していた」等の事例は頻繁に発生している。細かい事例が多数あるが、特に代表的な傾向や典型的な事例があるわけではない。
・例年 3、4 件ずつの軽微なインシデントが発生している。うっかりミス等による情報漏えい、パソコン本体や社員証紛失等の事例が多い。

表 17　最近の内部不正の傾向に関する専門家の意見

・内部不正を含め情報セキュリティインシデントは全体的に増えている印象である。
・内部不正事件の中では、デバイスやネットワーク経由で情報を持ち出すケースが多い。
・内部不正の調査として、スマートフォンの解析を行うことが増えた。
・経営者や上位職者の不正を調べるケースが多い。
・外部からの指摘、内部通告、会計監査から発覚するケースが多い。
・上司や権限を持つ人物が不正行為を行うことも多い。
・金銭目的での情報漏えいが多く、入手した会社の極秘情報をマスコミ等に売ってしまう事例も多い。
・被害額ベースで考えると、サイバー攻撃よりも、内部犯行による損害は大きい。
・外部からの通報により情報漏えいが発覚するケースも多い。情報と引き換えに金銭を要求される事例もある。
・不正行為者はセキュリティの一番弱い点を突いて情報を持ちだそうとする。プリンタ経由の情報漏えいもそのひとつである。中には、わからないように、重要情報のファイル名を「お花見の御連絡」等に変えているケースもあった。

② 内部不正対策の実施状況

内部不正対策の実施状況について尋ねた結果を表 18 に示す。情報の格付け、ID やアクセス権の管理、入退室管理、ログの取得と監視に関する対策が主に実施されている。また、経営層が主導して内部不正対策を実施している、内部不正対策の実施体制・実施方針がある、内部不正を働いた役職員に対する懲戒手続がある、社内教育を実施しているという企業もある。一部の中小企業からは、対策を実施していない理由、対策推進のために実施している内容が挙げられた。

表 18 内部不正対策の実施状況

○大企業の場合
・経営層が主導して情報セキュリティ対策を行っている。本社及び各事業部に情報セキュリティ委員会を設置し、情報システム対策責任者を置いている。
・漏えい防止のための原則（近づけない、触らせない、取り出せない、外に持ち出させない、持ちだしても価値がない）に則り、対策を実施している。
・対策の陳腐化を防ぐため、社内の監査をし、PDCA サイクルを回すことで対策を強化している。
・社内の入退室は IC カードで管理され、3 つの格付けで社員の入れるエリアを制限している。極秘エリアには指定された社員のみ入室を許可している。
・相互監視が必要な作業を指定している。この作業を行う部屋は、入退室に 2 人の認証が必要であり、監視カメラを導入している。
・通信ログを監視し、異常を検知するシステムを導入している。
・製造現場へ私物のスマートフォンを持ち込むことを禁止している。近年のウェアラブル機器の普及により、腕時計の持ち込みも禁止している。例外として許可された区域で、会社のスマートデバイスを利用する場合（BYOD）は MDM[33]で管理している。
・インターネット上に掲載されている自社に関する情報を定期的にモニターしている。
・内部通報の体制を整備している。
・IP アドレス変更の監視や、社員のパソコンにインストールされているソフトウェアのチェックを行っている。詳細な機能が分かると対策される恐れがあるため、使用しているソフトウェアの製品名や監視システムの詳細は社員に教えていない。
・パソコンは会社から貸与されたものであり、中のデータはすべて会社が保有するものであるため、個人的な権限はないという意識付けをしている。私用メールも禁止している。
・社員 ID を用いて、社内施設の入退場管理をしている。
・IPA の内部不正防止ガイドラインを参考に、動機、機会、正当化の 3 つの視点から対策を立てている。「動機」では、ログの監視をしていることを周知している。「機会」では、社員 ID 管理、アクセス権の設定、ログの監査、USB や外部記憶媒体への書き込みの無効化等の対策を行っている。「正当化」では、教育や周知の徹底を行っている。
・インシデント管理、自己評価/監査、情報セキュリティポリシー体系、組織及び役割、情報資産の種別及び管理、教育の 6 つを柱に、海外の事業所も含めた共通の情報セキュリティポリシーを定めている。
・情報セキュリティポリシーの下に、スタンダード（標準）、プロシージャ（手続き）を定めて、セキュリティ管理をしている。
・退職時に競業避止契約はしていない（外国籍の従業員が嫌がるため）が、様々な機会（誓約書を記入する際、システム利用誓約書を記入する際、退職前の機器返却の際）で就業時に得た情報を他社で使ってはいけないことを確認している。
・退職予定者に対する対策として、退職の 1 ヶ月前から、インターネットアクセスの禁止、リモートアクセスの禁止、ウェブメールの停止の措置が取られ、これらの記録を遡って監査している。退職予定者として社内システムに登録されると、自動的に上記の制限がかかる。
・USB メモリへの書き込みを原則禁止している。やむを得ず USB メモリに書き込む場合には、専用のツールを使う必要がある。

[33] MDM：（Mobile Device Management、モバイル端末管理）モバイル端末と社内システムとの認証、アプリケーションとの同期、外部サービスとの接続等を管理するシステム。

・システム利用領域の使用状況等をリアルタイムでモニタリングしている。
・許可されたオンラインストレージ以外へのファイルのアップロードは禁止している。メールにファイルを添付して送信する場合や外部デバイスへの書き込みの際にはアラートが出る。
・年 1 回の e-learning をはじめ、セキュリティ教育に力を入れている。システムを利用するユーザーに対しては、派遣社員や協力会社の社員も含めて、全員の受講を義務付けている。
・社員にアンケートをとり、部署ごとに情報セキュリティ対策状況を評価している。
・他の企業との定期的な会合により、セキュリティに関する情報交換をしている。
・ここ 2、3 年は、従来のセキュリティ対策では業務に支障が出るようになった。セキュリティを担保しながら、IT を活用しようという意識が高まっている。セキュリティの堅牢性と仕事の生産性・スピード感のバランスをとることが大切である。

○中小企業で対策を実施していない理由
・個人情報の取り扱いについて、定期的な教育は行っていないが、入社時や退社時に情報管理についての誓約書に署名させたり、情報管理についての冊子(「SNS に書かない、情報を持ち出さない」等)を配布している。退職者は誓約書を取り交わしており、これが抑止になっていると考えている。
・セキュリティの優先度は低く、「分かっているけど対応できない」状態である。人事管理の仕組みや、社内のリソース(人材)を効率的に管理する仕組みを導入することを優先したい。

○中小企業が対策推進のために実施した内容
・体制を構築するためには、社長に対してセキュリティインシデントの事例を出し、信用を失うリスクを説明することで、理解を得た。この方法は他の中小企業でも同様に使えるだろう。
・情報漏えいの損害賠償は社員個人に及ぶこともあるという教育を行い、互いに守り合おうという職場環境を目指している。
・中小企業の社長は社員を疑うことに抵抗感がある傾向があり、内部不正に対する予算がつかないため、特化した対策は行っていない。P マーク取得や ISMS の一環として対策している。

内部不正の経験や、教育事業者の個人情報漏えい事件といった報道による影響及び意識等の変化について尋ねた結果を表 19 に示す。経験した内部不正や報道された事件を受けて対策を実施したという回答が多い。専門家からは、マイナンバー制度やサイバー攻撃等の影響を受け、経営者や従業員の内部不正への意識が高まっている、相談や問い合わせが増えたという意見が多い。ただし、対策の見直しや強化の内容等が代表的な事件に左右されているのではという指摘もある。

表 19　内部不正の経験や報道による影響、意識等の変化

○大企業の場合
・自社で起こった内部不正事例をきっかけに対策が強化された。
・教育事業者の顧客情報流出を受けて、現在実施している情報漏えい対策について、スマートフォンの最新機種にデータがダウンロードされる危険があるか点検を行った。
・他人事ではないと感じた。この事件を受けて、顧客からセキュリティ管理のチェック(教育方法、物理的管理方法等)を受けることが増えた。
・教育事業者の事件を受け、USB 機器への対策を強化した。スマートフォンの充電や、小型の扇風機の使用等、USB から電源をとることを禁じる社内ルールを作った。

○専門家の意見
・最近は、経営者の内部不正への関心が高まっており、社内の怪しい動きに対する相談が多く、相談件数は増えている。
・教育事業者の事件以降、経営者の内部不正に対する意識が高まっており、社内の調査をどのように進めるべきかの問い合わせが増えている。
・委託や派遣に対する情報管理の目が厳しくなっている。

・従来は、インシデントが起きてから履歴を確認していたが、現在は、普段からデータの持ち出しの履歴を確認し内部不正の早期発見に努めている。また、データの持ち出しを承認制にした例もある。
・企業からの問い合わせの内容から、教育事業者の顧客情報漏えいや、公的機関のサイバー攻撃による情報流出、マイナンバー制度の導入など、社会的な影響が大きく報道等でも取り上げられた事件等が、重点対策の検討に影響していると考えられる。
・システム管理部門やセキュリティ部門ではなく、現場からセキュリティレベルを上げたいと依頼を受けるケースがここ 1 年増えている。情報漏えい事件の報道等の影響もあり、現場社員のセキュリティ意識が上がっている。
・セキュリティは重要なリスクだが、保険としか考えてない経営者も多い。経営者がセキュリティ対策を指示している企業は対策が立てやすい。

内部不正を働いた従業員に対する処罰の状況について尋ねた結果を表 20 に示す。内部不正の調査に関わった専門家によると、刑事事件にまで発展するケースは少ない。中小企業では、不正行為者である従業員が業務のキーパーソンであった場合、業務の継続が困難になることもあるため処分が難しく、従業員側も処分を恐れないため抑止とならないという実態がある。

表 20　処罰の状況

○専門家の意見
・不正行為者に対しては、退職勧告を出すことが多く、懲戒解雇や損害賠償を行うケースは少ない。
・中小企業では、不正行為者である従業員が業務のキーパーソンであった場合、退職による業務継続が困難になる場合もある。従業員側も簡単に辞めさせられないことを分かっているため、処分（処罰）による抑止を期待することは難しい。
・事業に影響を与えるほどの事件は発生していないが、内部不正により、業務委託先から管理体制の不備等を問われる場合も多い。

4.3.2　重要情報と対策事例

① 対象の企業が持つ重要情報（知的財産等）の分類

知的財産等の企業が持つ重要情報について、どのような管理がなされているか尋ねた結果を表 21 に示す。情報の格付けを行い管理しているという意見が多い。

表 21　重要情報の分類

○大企業の場合
・顧客から預かった情報は部署が異なっても管理レベルが変わることはない。社内情報の秘密レベルは文書作成部門が社内基準に沿って決める。
・情報の格付けは書類ごとに行い、ラベル付けは書類毎や、情報を置く場所、フォルダ毎に決めている。
・重要情報は、3 段階の格付けで管理している。マイナンバーの情報は、特定の個人のみアクセスを許可する。重要情報には、情報の主管部署が設定されており、情報が部署をまたぐ場合でも、主管部署が設定した情報の格付けに従うように規定している。
・秘匿種別はアライアンスを結んでいる企業と共通の 4 段階で管理している。格付けはデータオーナー（情報の所有者）が設定する。

② 重要情報（知的財産等）を安全に管理する手法

重要情報を安全に管理するため、どのような手法・対策を実施しているかを尋ねた結果を表 22 に示す。ネットワークの管理を実施している例、外部サービス利用の要件を設けている例があった。

表 22　重要情報を安全に管理する手法

○大企業の場合
・社外から社内ネットワークにアクセスする場合には、ID とパスワードだけでなく、本人の所有している社員証を使った多要素認証を行うようにしている。
・社外とデータを送受信する場合には、IP アドレスによる制限や電子証明書認証、インターネットの出入口を全社で統一する、等により審査し管理している。
・サンプル製品を製造する場合等、秘密保持契約を結んだ上で、図面データを顧客から預かることがある。図面データを保存するサーバを限定し、データへのアクセスも制限している。必要がなくなったデータはすぐに削除するようにしている。
・外部サービスを利用する場合、親会社が定めている監査要件に従っている。クラウドサービスを利用する場合は、扱う情報のレベルごとに異なるセキュリティ対策の基準を満たさなければ利用は許可されない。

③　重要情報（知的財産等）を活用する手法

重要情報を活用するため、どのような手法・対策を実施しているかを尋ねた結果を表 23 に示す。情報の格付けをファイルに追加する例があった。専門家からは、重要情報の使い勝手や秘匿するための手段についての指摘があった。

表 23　重要情報を活用する手法

○大企業の場合
・秘匿種別を Microsoft office ファイルに付与するツールを自社で作成し、活用している。ファイル名を変えずにプロパティの分類に秘匿種別を埋め込むことができる。

○専門家の意見
・クローズな環境で管理しようとすると、使い勝手が悪い情報もある。マイナンバー情報もクローズな環境のみで扱うことは難しい。クローズ環境とオープン環境を行き来する情報や、オープン環境にある重要情報の管理対策に気を使うべきである。外部記憶媒体やメールや Web に持ち出された際に自動的に暗号化する仕組みを構築することで、サイバー攻撃や従業員による過失・故意による漏えいリスクを低減できる。

④　インシデントからの復旧や原因究明のための対策

インシデントからの復旧や原因究明に役に立った対策を尋ねた結果を表 24 に示す。ログやメールの保全、フォレンジック技術の利用が挙げられた。

表 24　復旧や原因究明のための対策

○大企業の場合
・社内の情報システム部が、サーバへのアクセスログや、メールの内容を保全しており、事件の際の証拠として役に立った。
・フォレンジックは外部の事業者に依頼している。内部不正事例では、PC や HDD を提供し、内容を解析した。

○専門家の意見
・アクセスログはリアルタイムで監視するだけでなく、過去の統計データをもとに異常事態を検出する仕組みがあると良い。異常を検知した場合の対応策を事前に考えておいた方が良い。
・アクセスログ、メール内容、出退勤の記録、経費精算、取引情報等をコンプライアンス部署がモニタリングし、不正行為が発覚するケースが多い。監視ツールだけなら安価で手に入れることができるので、業者に頼らずともモニタリングの環境を整備することはできる。（とはいえ、中小企業にとっては難易度が高いかもしれない。）
・不正を証明するためにも、プロキシサーバのログは取った方が良い。

・どこと通信していたか、どのようなプロセスが行われたのかを知るための仕組みを事前に仕込んでおくことが重要である。マイクロソフトのシステムモニターのように、履歴がログとして残るようにすると良い。
・フォレンジックの調査を依頼する場合は、契約前に、サンプル報告書など調査結果のイメージを確認する。「どのような結果が出てくるのか」「報告内容をインシデントレスポンスの中で活用できそうか」を確認し、不足があれば、「何を探すのか」、「どんな結果を期待するのか」を業者に伝え、適宜交渉する。
・調査方法には因果関係による分析と時間軸による分析の 2 つがある。分析を行うためには、少なくとも「重要なキーワードは何か」、「どのようなファイルを探すのか」、「いつ頃のファイルなのか」を特定し、業者に伝える必要がある。
・被害額の情報があると、顧客の経営層を納得させやすい。企業は被害額とフォレンジックにかかるコストのバランスを考える必要がある。

4.3.3 有効と考えられるインシデント対策事例

① インシデントの証拠保全のために必要な対応

インシデントの証拠保全のために必要な対応を尋ねた結果を表 25 に示す。フォレンジックを利用すること、ログを取得することが挙げられた。

表 25 証拠保全のために必要な対策

○専門家の意見
・操作ログを取ることで、どのような作業をしたのか把握することができる。ログを保管するためのサーバを切り離し、アクセス権を分離することで、システム管理者でもログの削除が行えないようにすることができる。
・Windows の標準機能にあるログ機能はイベントログであり、不具合の原因究明には使える可能性があるが、何をしたのかまでは把握することができないため、証跡にはならない。
・ドメインコントローラ、プロキシ、ファイアウォール等のログを十分な期間とれていないケースが多い。記録が少ないと、内部不正なのか外部攻撃なのかさえ判断することができない。
・多要素認証を行うことで、個人とデータを紐づけることができる。なりすましを防いだり、意図的に不正行為を行ったことが証明できたりといった効果がある。
・システム管理者とは別にセキュリティ管理者を設置し、権限分散することでシステム管理者が勝手に設定を変えたり、履歴を消せないようにしている。

② 企業で最低限実施すべき対策

企業で最低限実施すべき対策を尋ねた結果を表 26 に示す。内部不正を防止・抑止するために、技術的な対策としては、重要情報へのアクセスログ等を確認していることを組織内に告知すること、法的な対策としては、秘密保持契約の締結、競業避止義務契約の締結が重要である。

表 26 企業で最低限実施すべき対策

○大企業の場合
・入社時にセキュリティについての研修を行う他、年 1 回教育を実施している。
・システム的に制限をかけると業務上不都合が生じるため、従業員に不正行為を行わないよう意識づけ（監視されている、厳しい罰が待っている等）を行い、不正が起きない環境作りをすることが大切である。

○専門家の意見
・どのような情報が誰に狙われるのか知るためにも、過去の事例を知ることは重要である。
・自社での対応が難しい場合は、事前に専門の業者に相談し、事件が起きた場合の対応を取り決めておくと良い（ただし、最初に企業の環境を把握したり、ツールの導入が必要な場合もあり、費用が発生するケースがある）。
・ログは少なくとも 1 ヶ月分は記録しておく必要がある。本来は 1 年程度記録が残ることが望ましい。ネット

ワーク系のログはトラフィックが多く、上書きされてしまうケースが多い。
・システム変更作業中のログは取っていないが、チェックを行う担当者を決め、1 人で作業が行われないようにしている。中小企業では 1 人の人にシステム変更作業すべてを委ねてしまい、相互牽制ができないことが多い。
・インシデントが起こる前に、どのような調査会社があるのかあらかじめ把握しておいた方が良い。
・秘密保持契約や競業避止義務契約等は締結した方が良い。
・アクセスログを見張っている旨を社員に周知することは内部不正対策として有効である。コンテンツフィルタ等は画面にメッセージが出るので、見張られていることを自覚する。不正を行った事例を社内にも通知し、不正をしても必ず見つかり、割に合わないことを伝えるべきである。
・中小企業は多くのコストを負担できないため、クラウドのように管理し、セキュリティベンダが複数社まとめて管理する仕組みは考えられる。

③　内部不正対策を考慮したインシデントレスポンスの在り方

内部不正対策を考慮したインシデントレスポンスの在り方について尋ねた結果を表 27 に示す。インシデントの被害を最小化するためには、発見・報告・対処の速さが求められる。まずは、通報や報告すべき行為の定義など、インシデントに対応するための体制を整えることが重要である。

表 27　インシデントレスポンスの在り方

○大企業の場合
・セキュリティインシデント（社員証の紛失、メールの誤送信を含む）が起こった際には、60 分以内にマネージャー、部長、情報管理責任者を経由して情報管理部門へ連絡が行くようにしている。
・管理部門が事故を起こした社員に背景や原因についてヒアリングを行い、マネージャーを通してインシデントの内容を全社に展開している。また、管理部門から対策を押し付けるのではなく、現場の環境を踏まえてインシデントを起こした本人に対策を考えてもらっている。提案された対策法について当室とディスカッションを行い、採用された案は現場で実施している。
・インシデントの罰則は人事規定の中で、損害のレベル別に定められている。

○中小企業の場合
・セキュリティ対策について、中小企業の社長はどこに相談すればよいのか分からないという課題がある。安価で相談できる窓口が求められている。

○専門家の意見
・不正行為のシミュレーションを行い、発生後にどれだけ証拠が残せるのか確認した方が良い。その結果を踏まえて、対策が十分かどうかをセキュリティ会社に相談すると良い。
・不正行為の予兆を検知する場合、「どのような事象や兆候を気付いて欲しいか」、「どのような点に注意するべきか」を定義しなければならない。例えば、不正行為が疑われる等の定義を示して、該当する事象があれば社員に報告させる必要がある。
・ログから異常を検知するためには、まず正常な状態を定義する必要がある。ホワイトリストベースで使用可能なソフトウェア等を定義することで、そこから逸脱した場合を異常な動作であると判断できる。
・インシデントの被害規模の最小化については不正を早く発見できたか、早く対処できたかに依存するため、被害を最小化するにはリアルタイム監視を行うことが有効である。このためのツールとして、SIEM[34]等リアルタイムでユーザー情報を把握できるものがある。一方で、監視できるノウハウを持つ人材は不足している。
・内部の怪しい動きを察知して、内密に調査を行うケースも多い。不正行為者は周囲から見ても怪しい行動とることが多く、同僚からの通報を受け、人事が内密に履歴をチェックすることもある。

[34] SIEM：(Security Information and Event Management) セキュリティ情報及びイベント管理。

・人物が特定できれば履歴を見るのは簡単であるが、社員全体の履歴を管理しようとすると見逃してしまう点が発生する。人、ファイル等何かしら監視の手がかりになるものがあると良い。
・情報を印刷して持ち出すケースも多い。不正な印刷を防ぐことは難しいが、ログ等の履歴から誰が印刷したか調べることができる。履歴は、上司のいない時間（早朝、土日等）や勤務時間外の記録を重点的に調査する。

④ CSIRT の有効性

CSIRT が内部不正によるインシデントに対応することについて尋ねた結果を表 28 に示す。専門家の中でも意見が分かれた。企業内に CSIRT を有する場合には、内部不正に対処する部門と、インシデントレスポンスに要する技術や内部不正の兆候に関する情報交換が定期的になされるべきであろう。

表 28 CSIRT について

○大企業の場合
・情報セキュリティと個人情報保護を担当する組織と緊密に連携している。

○専門家の意見
・CSIRT は内部不正にも対応するべきである（海外の企業では内部不正にも対応している）。内部不正に対しても、サイバー攻撃と同様、全社的に取り組む必要がある。日本でも、金融関連企業、インフラ企業、知的財産をコアとする企業の CSIRT は内部不正を意識しているが、その他の事業会社は十分に内部不正対策がされているとは言えない。
・社内で、サイバー攻撃と内部不正に対応する部署が別々になっているケースは多いが、監視や分析等は共通する部分も多いため、CSIRT の中で月 1 回程度定期的に情報共有を行うと良い。
・中小企業では社内に CSIRT を置いているケースはほとんどない。内部不正に対する体制がないので、対応に困ったら外部に相談するしかない。
・CSIRT は外部攻撃と内部不正の両方に対応すべきであるが、常時内部不正に備えて監視する事はやりすぎである。
・CSIRT が内部不正対策を担当することには賛成しない。内部不正専門のセキュリティ管理者が必要である。CSIRT はインシデントに対して内部調整を行う機能もあるが、被害の最小化など技術的な内容も重要である。一方、内部不正対策はシステムが導入されていれば、ある程度は予兆が察知できることもあり、内部調整が重要である。そのため、求められる機能やスキルが異なることから同一の担当者は避けるべきである。さらに、権限を分離することで、セキュリティの設定を変えられたり、履歴を消されたりする危険性が低くなる。

4.3.4 その他

業務委託先企業や海外拠点でのセキュリティ対策・内部不正対策の実施について尋ねた結果を表 29 に示す。日本の対策をもとに、海外拠点でも同様の対策を実施させる例があった。業務委託先企業については、自社のセキュリティ方針を公開する、第三者機関の監査を受けさせる例があった。

表 29 業務委託先企業・海外拠点での対応

・近年、海外の事業所で個人情報を扱うようになってきたので、ルールを整備している。日本での安全管理措置に関するルールは国際標準を満たしているので、これを翻訳することで海外でも活用できる。海外で行う業務内容は、情報セキュリティ対策を整え実施する。
・外注先に対して当社のセキュリティ方針をアナウンスしたため、外注先も気を引き締めていると感じている。
・情報セキュリティポリシーは海外の事業所でも共通であり、セキュリティ教育コンテンツも日本から提供している。欧米諸国の事業所には、日本での対策事例やリスクを伝え、具体的な対策については現地の事業所に任せている。BRICS 諸国の事業所に対しては、日本で取られている対策をすべて強要している。
・IT 関連の業務委託先には、第三者機関の監査を受けさせ、報告書を提出させている。

○専門家の意見
・製造業の企業であっても、図面が流出して構わないと思う企業もある（製品を分解すれば分かってしまうため）。図面よりも、製品を作る際のノウハウが流出することを危惧しており、印刷やコピーができない読み取り専用ファイルで保管している。

職場環境や従業員の意識に関する意見を表 30 にまとめた。監視していることを周知することにより、内部不正行為の抑止に繋がった事例があった。また、仕事満足度を向上させる取り組みを実施している企業もあった。

表 30　職場環境・従業員の意識について

・人的アプローチとして、コミュニケーション（対話）を奨励している。
・たとえ悪意のある社員がいたとしても、監視されていることを知って、不正行為を思いとどまって欲しいと考えている。社員全体の意識レベルを上げる必要がある。
・社員のモラル向上のためには、仕事に対する満足度が不可欠であると考えている。ファミリーデーや事業参観日を設けることで、家庭内での社員の地位向上や、仕事に対するモチベーションアップにも繋がる。

○専門家の意見
・社員に内緒でログ監視ツールを導入した顧客があった。導入を周知する前と周知した後とを比較すると、不要な情報の持ち出しが減っていた。監視を周知することは不正抑止効果があると言える。

4.4　法的対策に関するインタビュー調査

内部不正による情報セキュリティインシデントに対し、企業が実施している（または実施すべき）法的対策や適法の範囲等について、インタビューを実施した。結果を以下に報告する。

4.4.1　従業員の採用について

近年、転職者による情報漏えい等で訴訟に至る事例が発生している[35]。このような情報漏えい等を未然に防ぎ、かつ、自社に他社の重要情報を持ち込むことを防ぐ対策として、従業員を採用する際の身元確認や重要情報の持ち込み等の確認が考えられる。

採用時の身辺調査については、米国 CERT の調査レポート[36]でも、「内部脅威への 19 のベストプラクティス」のひとつとして、従業員の身元調査等を含む「雇用プロセスからの監視」を挙げている。しかし、雇用プロセスや採用に関わる情報収集等は、国により関連する法律やその適法範囲が異なるため、ここでは日本で実施可能な範囲を示す。

また、退職時の重要情報の持ち出し、及び転職者による他社の重要情報の持ち込みについて、企業として実施すべき対策を示す。

〇採用時の事前調査について

・採用時の個人情報の収集について、厚生労働省の「公正な採用選考をめざして[37]」では、職業安定法第5条の4及び平成 11 年労働省告示第 141 号により「個人情報の収集は、本人から直接又は本人の同意の下で収集することが原則」としている。また、「適性・能力に関係のない事項を、応募用紙・面接・作文などによって把握すること」や「身元調査」等は就職差別につながるおそれがあるとして採用時に配慮すべき事項としていることから、収集する情報の内容についても留意が必要である。

・例えば、新卒者の学歴や転職者の職歴（自己都合退職か、懲戒解雇か等）について、面接等により本人に直接確認することは問題ない。新卒者の場合は卒業証明書、転職者の場合は履歴書等、資料提出を求める場合が多い。

・面接や資料提出等により入手したこれらの情報の確認について、前職や大学等に照会する場合、個人情報保護の観点から、本人の同意なしでは照会先から情報を得られないことが考えられるため、事前に本人の同意を得ることが必要となる。最近では、ソーシャル・ネットワーク・サービス（SNS）など、本人が公開している情報を利用するケースもある。

・企業により採用時の対応は様々であるが、中小企業では、コストが掛かる採用調査は行わないことが多い。社長の判断で従業員を解雇できる企業もあり、採用後、行動が怪しい従業員を解雇する場合もある。

・不正競争防止法の観点では、企業の規模に関わらず、一旦、情報漏えいや関連する訴訟が発生する

---

35 「2.1.2　内部不正行為に至る動機、行動」、「表 1　2014 年～2015 年に報道された内部不正事件」「図 45　判例調査結果の詳細分類」を参照のこと。

36 CERT® Insider Threat Center: Best Practices Against Insider Threats in All Nations (August 2013)
http://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_59084.pdf

37 厚生労働省 ：公正な採用選考をめざして（平成 27 年度版）
http://www.pref.okayama.jp/uploaded/life/334760_1576664_misc.pdf

と、事業の停止やイメージダウン等により経営の危機を招くことにもなりかねないことから、転職者に対し、次に述べる前職での重要情報の持ち込み等の確認が重要である。一方、新卒者の場合、同様のリスクは低いことから、入社後、適切な教育をすることで不正を未然に防止・抑止することが重要である。

○転職時の情報持ち出し／持ち込み対策について

転職に伴う情報漏えいについて、法的な観点から、退職者に対し実施すべき対策と転職者を受け入れる際に実施すべき対策を示す。これらは、転職時の情報漏えい対策として、表裏一体の関係にある。

(1)退職者に対する対策

従業員が退職する際、業務に関する秘密情報等が持ち出せないよう技術的な対策を講じる以外に、契約により秘密情報を使用しないことを求めることができる。

- 退職者に対して、「在職中に得た秘密情報は退職後使わない」「秘密情報を持ち出さない」ことを確認できる秘密保持契約等を締結する。これにより、退職者に対し、秘密情報を認識させるとともに、情報漏えいが発生し訴訟となった場合、秘密情報であること知らなかったという言い逃れができないようにする。
- 退職後、一定期間競合会社に転職しない等の競業避止義務を契約書に記載することも考えられるが、職業選択の自由を侵害しないよう注意が必要である。

(2)転職者の受け入れ時に実施すべき対策

転職者を受け入れる際、転職者が持ち込んだ情報により、他社の秘密情報を意図せず侵害してしまい訴えられることのないように、受け入れ時の対策が必要である。特に、他社の秘密情報であることを知らなかったとしても、知らなかったことに重大な過失があると、不正競争防止法による損害賠償請求や差止請求の対象になり得るため注意が必要である。

以下に、媒体に化体した情報と媒体に化体しない情報に分け、秘密情報の持ち込みへの対策を示す。

- 媒体に化体した情報の対策

「媒体に化体した情報」とは、紙、USB メモリ、CD 等の媒体にある秘密情報である。採用時、転職元秘密情報を含んだ媒体を一切持ち出していないことを転職者に表明保証[38]させ、誓約書として残しておく。これにより、転職者自身に注意喚起するとともに、不正競争防止法上の重大な過失がないことを示す根拠とすることもできる。

- 媒体に化体しない情報の対策

媒体に化体しない情報とは、従業員が体得した無形のノウハウや職務として記憶した情報等である。媒体に化体しない情報が転職者により持ち込まれ、使用されると不正競争防止法等に抵触する可能性がある。一方、転職先が、これらの情報を聞き出すことは、情報の開示を受けたことになり、違法行為とみなされる可能性があるため、転職者に対し自社情報を説明した上で、情報の転用可能性が低い旨の誓約書を取り交わす。また、必要に応じて面談記録を保存しておく。

一般的に、媒体に化体しない情報が持ち込まれたことを立証することは困難であり、刑事罰になら

[38] 表明保証は、契約当事者が契約関係に入るに際して、一定の重要な事実が存在することを相手方に言明させることにより、相手方による契約上の義務履行に対する信頼を高めることができるとともに、仮に相手方が表明保証した事実が存在しないことが判明した場合には、契約を解除して契約関係を解消したり、表明保証された事実が存在すると信じたことによって被った損害の賠償を請求したりする等の契約上の救済措置を可能とする。

ないケースも多いが、転職者を受け入れる企業としては、媒体に化体しない情報についても、媒体に化体した情報と同様に、使用しないという姿勢を示すことが重要である。

上記対策により、転職者を受け入れる側（転職先）として、少なくとも重大な過失は無いという状況を作ることが重要である。

営業秘密管理指針では、媒体に化体しない情報について、原則として紙その他の媒体に可視化することが必要としているが、これは、転職元として、退職者（転職者）が持つ情報を明らかにし、後に転職先での転用可能性を立証するという点で重要である。

なお、本指針では、従業員が体得した情報が営業秘密に該当する場合、転職後の使用・開示によって、直ちに法的措置の対象となるわけではなく、従業員が転職元の企業との関係で信義則[39]上の義務に著しく反するような形でなされた場合に限り、法的措置の対象となるのであり、その判断に当たっては、企業と従業員との間の信頼関係の程度や営業秘密の内容等を踏まえた総合的な考慮によることに留意が必要である。

4.4.2 業務委託先との契約について

○委託先への要求事項等について

委託契約において、特定の情報セキュリティ対策や、委託元による情報セキュリティ監査、疑わしい場合を含む内部不正発生時の調査協力等を要求することはできる。

調査協力義務は、「調査を要求した際に、合理的な期間・場所において調査に協力する」ことであり、強要することはできない。委託先が、調査協力の要求に対し、不当に応じない場合は、契約不履行として損害賠償請求等の対象となる。調査協力の内容について、契約に、ログの提供等を具体的に記載することは問題ないが、発生した問題により対応が変わるため、契約上はある程度抽象的な記載に留め、具体的な対応については個別に話し合うことが多い。例えば、委託先に対しログの提供を要求する場合、それが調査の合理的な範囲内かを確認する必要がある。

契約上求めたセキュリティ対策が実施されていなかった場合、軽微な違反であれば、信義則上契約の解除はできないことがある。一定の期間を定めて期間内に改善するよう求め、それでも改善されない場合には委託契約を解除する場合がある。

○再委託の管理について

内部不正対策を実施する際、委託先の階層が増えるほど、委託元による監督が間接的になり、リスクも増大することから、再委託先の管理についても委託契約の中で明確にしておく必要がある。再委託を原則禁止とし、どうしても再委託が必要な場合は、委託元の承諾を得るとともに、契約上、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、事前に合意した情報セキュリティ対策の実施を委託先に担保させることがある。

謝辞：

インタビュー調査を実施するにあたり、多くの企業のご担当者様に多大なご理解とご協力をいただきました。ここに、感謝の意を表します。

[39] 当該具体的事情のもとで相互に相手方の信頼を裏切らないよう行動すべきであるという法原則。

5. 判例調査

本章では、内部不正に関する判例調査の結果を報告する。

本調査で収集した判例は、「不正競争防止法の一部を改正する法律」の施行（2016 年 1 月 1 日）、「営業秘密管理指針」の全部改訂（2015 年 1 月 28 日）以前のものであり、これらの法律及び指針に基づく判例は含まれないことに注意いただき、参考にされたい。

5.1 判例収集

判例調査では、まず、判例データベースを使用して判例を検索し、内部不正に該当する判例を抽出する作業を行った。判例収集の目的、手段等を表 31 に示す。

表 31 判例収集方法

項目	内容
目的	内部不正の判例を収集し、内部者の属性、内部不正の対象、IT システムや IT サービスとの関連性、組織の情報等が受けた被害や影響、損害賠償額及び判決の要旨を整理する。
情報源	裁判所ウェブサイトを含む日本国内の判例データベース
調査方法	1) 内部不正の公開情報を元に、判例に含まれると考えられるキーワードを幾つか決める。 2) 上記のデータベースを使い、判例のキーワード検索を行う。 （検索キーワードは表 32、収集結果は表 33 を参照） 3) 上記 2)の検索結果から判例情報をチェックし、内部不正の定義に該当する判例があるか確認する。具体的には、目的に挙げた観点を確認する。 4) 内部不正に該当する事例があると判断された判例から、IT に関連するものであって、経済的な損害が認められた判決を中心に、重要と思われる判例を選別する。
その他条件	下記条件にあてはまる判例を除く。 ・IT システムに関連しない判例 ・損害賠償請求等の具体的な被害がない判例

表 32 判例検索キーワード

検索ワード	内部、従業員、経営者、取締役、理事 不正、流出、盗、漏洩、漏えい 営業秘密、個人情報、機密情報、営業機密 営業差止、不正競争、善管注意義務、義務違反 電子計算機、コンピュータ、システム
除外ワード	人材流出、安全配慮義務 フランチャイズシステム、コンピュータ室、給食システム 営業表示、違憲

表 33 判例収集結果

判例の分類	件数
重要判例（IT に関連があり損害がある認容判例等）	26 件
上記以外で秘密管理性などに特徴のある判例	20 件
上記2種以外で本件調査に関連のある判例	54 件
本件調査に関連のない判例	128 件
合計（検索キーワードによる検索結果）	228 件

5.2　判例調査で得られた傾向

判例調査によって収集した事例は 26 件である。これらの事例を分類した結果を図 45 に示す。

不正行為者は、一般社員（元社員を含む）が 61.5%と最も多く、次いで管理職・経営者が 26.9%、委託先が 11.5%であった。また、内部不正行為の対象は、顧客情報が 57.7%と最も多く、社内情報が 34.6%、開発情報と物理装置は 3.8%であった。

動機については、転職・起業が 65.4%と最も多い。今回の調査では、一般社員の 62.5%、管理職・経営者の全員が転職・起業を目的に内部不正を働いている。

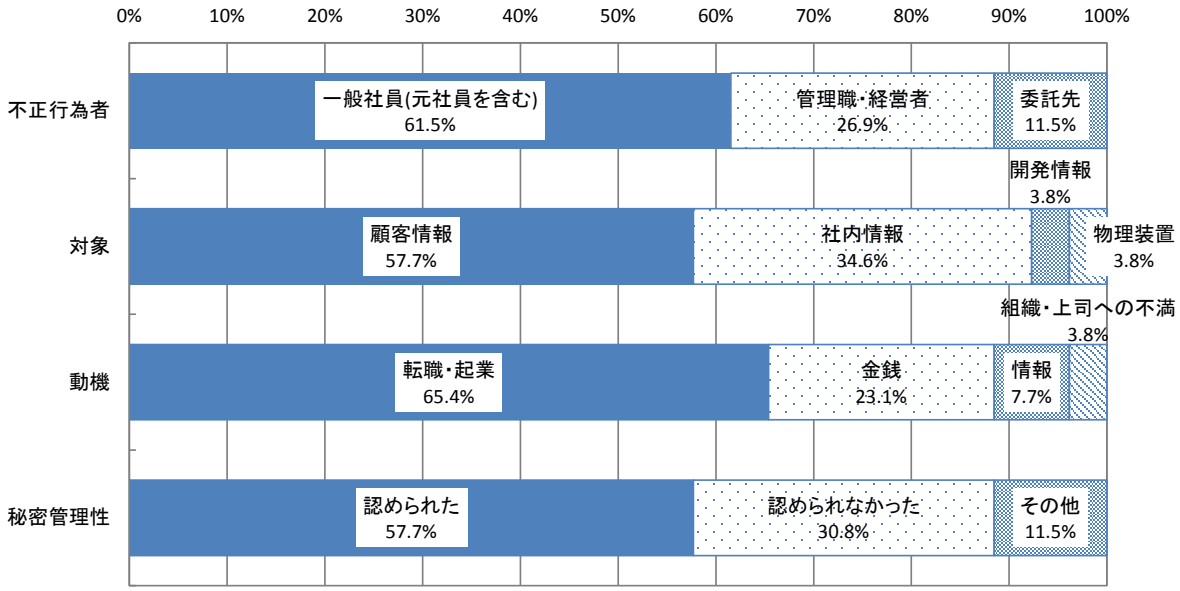

図 45　判例調査結果の詳細分類(n=26)

5.3　判例調査で得られた事例

判例調査の結果より、事例を紹介する。これらはすべて不正競争防止法違反の疑いがあった刑事・民事裁判の判例である。

不正競争防止法では、企業が重要情報の不正な持ち出し等による被害に遭った場合、営業秘密として管理しておくことで、差止請求及び損害賠償請求等の法的措置をとることができる。

不正競争防止法第 2 条第 6 項は、営業秘密を表 34 と定義しており、法的保護を受けるためにはこの三要件すべてを満たす必要がある。

表 34　不正競争防止法第 2 条第 6 項の営業秘密の定義

① 秘密として管理されている [秘密管理性] ② 生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報 [有用性] であって、 ③ 公然と知られていないもの [非公知性]

経済産業省「営業秘密管理指針」には、営業秘密として必要な「秘密管理性」を定め、具体的な管理方法等が示されているが、上記三要件のうち「① 秘密管理性」の要件については、産業界等より、判例によって秘密管理性の基準が異なる等の意見があった。

ここでは、判例の「秘密管理性」に着目し、内部不正事件において、不正行為者に対しどのような判決が下されたのかをみていく。

なお、本章の冒頭に記載したように、以下に、本調査報告書公開時点での法律及び指針に基づく判例は含まれないことに注意いただき、参考にされたい。

判例 26 件の内訳は、秘密管理性が認められたものが 15 件、認められなかったものが 8 件、秘密管理性が争点でないものが 3 件である。秘密管理性が認められた判例を表 35 に、認められなかった判例を表 36 に示す。

表 35 では、最も高額なもので約 8 億円の損害賠償命令が下されている。この判例では、被告企業（転職先企業）と被告（取締役）に各 4 億円の支払いを命じた。その他判例においても、「企業の情報を持ち出した」などの行為を発端に、企業に大きな競争力低下をもたらし、不正行為者が莫大な賠償金を求められる可能性があることを示している。一方、表 31 の判例では、情報が営業秘密として管理されていなかったとして棄却されている。

表 35　秘密管理性が認められた内部不正事件の判例

事件の概要	被告人	判決内容
従業員が自己のPCを会社のネットワークに接続し、ファイルサーバから製品の生産方法に関する情報をハードディスクに複製し不正に取得した。	従業員	懲役 2 年（執行猶予 4 年） 罰金 50 万円 ハードディスクの没収
従業員 2 名が原告会社の保有する顧客情報を不正に取得し、自身の転職先へ開示した。従業員の転職先である被告会社の売上が急増する一方、原告会社の売上が激減した。	従業員 転職先企業	不正取得した顧客情報の差止め 約 1 億 3,900 万円の損害賠償
従業員が原告会社の保有する商品の生産者情報および顧客情報を不正に持ち出した。従業員は原告会社在籍中に別会社を設立し、不正取得した情報を用いて商品の仕入れおよび顧客への販売を行った。	従業員	不正取得した生産者情報・顧客情報の差止め 1,000 万円の損害賠償
従業員が原告会社の保有する製品の設計情報を不正に取得し、転職先の被告会社へ持ち出した。被告会社は設計情報を用いて製品の製造・販売を行った。	従業員 転職先企業	不正取得した設計情報の差止め 4,100 万円の損害賠償
取締役が原告会社を退職後、被告会社の代表取締役に就任。その後、原告の従業員 82 名が退職し、そのほとんどが被告会社に就職した。取締役は退職前から従業員の移籍を働きかけた上、従業員らによって設計図の不正取得や、これを用いた製品の製造販売を行った。	取締役 転職先企業	不正取得した設計情報の差止め 約 8 億円の損害賠償

表 36　秘密管理性が認められなかった内部不正事件の判例

事件の概要	被告人	判決内容
原告会社の製品に関するソースプログラムや設計図面などを、従業員が不正取得したと主張した案件。ソースプログラムや設計図面を営業秘密として、それらを使用した製品の製造、販売等の差止めと損害賠償を求めた。	転職先企業 従業員	営業秘密としての秘密管理性は否認 原告の訴えを棄却
原告会社の業務を委託されている被告会社にて、原告の顧客に対して営業活動および原告の信用を毀損する言動を行い、顧客の契約先を原告から被告に切り替えさせた案件。顧客名簿を営業秘密として利用の差止めと損害賠償を求めた。	業務委託先	顧客名簿の秘密管理性は否定 信用毀損等による約 530 万円の損害賠償
地方自治体のシステム開発を委託されたA社がB社へ再委託し、B社はC社へ開発を再々委託した。C社の従業員がシステム開発に必要な自治体個人情報をコピーして自社へ持ち帰り、自己のPCへコピーし、名簿の販売を行う会社へ売却した。	地方自治体	原告（自治体市民）1 人あたり 1 万 5,000 円の損害賠償 （原告 3 名）

労働契約、特に従業員の採用・退職時及び業務委託先との契約に関する法的対策については、「4.4 法的対策に関するインタビュー調査」を参照されたい。

6. まとめ

本調査から把握することができた内部不正の状況等、及び調査結果を考察し得られた内部不正対策のポイントを以下に示す。

6.1 考察①（内部不正の発生状況より）

・内部不正を経験した企業は、大企業が 8.6%、中小企業が 1.6%。

これまでに内部不正（ルールや規程違反を含む）があったと回答した割合は、300 人以上の企業では 8.6%、300 人未満の企業では 1.6%であった（図 1）。内部不正の内容は、企業規模に関係なく、「うっかりミスや不注意によるルールや規則の違反」が最も高く、次いで「顧客情報の持ち出し」であった（図 2）。

・内部不正の理由の 6 割は故意が認められない“うっかり”

内部不正経験者に行為の理由を聞いたところ、“うっかり違反した”が 40.5%、“ルールを知らずに違反した”が 17.5%（合計 58.0%）と、全体の約 6 割は、故意が認められなかった。うっかりミス等を防ぐため、管理者は扱う情報に格付けする等のルールや規則を明確にし、周知徹底することが対策として有効である。一方、42.0%は故意によるもので、その理由は“業務が忙しく、終わらせるために持ち出す必要があった”が 16.0%、“処遇や待遇に不満があった”が 11.0%などであった（図 10）。

・内部不正経験者の約 5 割がシステム管理者（兼務を含む）

内部不正経験者の職務を尋ねたところ、51.0%がシステム管理者（兼務を含む）であった。システム管理者は社内システムに精通し、高いアクセス権限（特権）を有することが多いため、権限の最小化・分散、作業監視等の対策が有効といえる（図 6）。

・主たる情報の持ち出し手段は USB メモリ

情報の持ち出しには「USB メモリ」の利用が最多で、組織での対策は USB メモリ等の外部記録媒体に関する利用ルールの徹底、および利用制限が有効と考えられる（図 11）。しかし、外部記録媒体の利用制限に関するその対策状況をみると、300 名未満の企業の過半数で“方針やルールはない”と回答している（図 17、図 18 の Q9-9、Q9-10）。

6.2 考察②（内部不正対策の実施状況より）

・300 名未満の企業では、内部不正対策について「方針やルールは無い」が約 4 割

内部不正防止ガイドラインの 32 の対策について、300 名未満の企業では、300 名以上の企業と比較して、「方針やルールはない」という結果の割合が高く、すべての項目について 4 割を超える。不正行為かどうか識別するためにも、まずは、方針やルールの策定が必要といえる（図 17、図 18）。

・経営者等が重要視していない対策が内部不正行為の抑止に有効

内部不正経験者と経営者・システム管理者とで、有効と考える内部不正対策の違いが顕著だったのは「職務上の成果物を公開した場合の罰則規定を強化する」、「管理者を増員する等、社内の監視体制を強化する」であった（表 13）。不正行為抑止のためには、監視だけでなく、監視している旨を通知することが有効である。

経営者・システム管理者は、不正行為を思い留まらせるのに有効な対策を的確に把握し、実施する必要がある。

・内部不正経験者の約半数が効果的と考えるのは、「ネットワークの利用制限」

内部不正経験者が内部不正に効果的だと思う対策は、Web サイトの閲覧制限やメールの送受信先の制限等の「ネットワークの利用制限」が 50%と最も高く、続いて、「アクセスログの監視」(46.5%)「重要情報へのアクセス制限」(43%)であった(図 40)。

・適切な処分や法的措置をとるには、操作履歴等のログ取得による証拠保全が必要

故意による内部不正に対する処分について、「懲戒処分や起訴をしなかった」が 30.9%だった(図 33)。その理由を尋ねたところ、「懲戒処分や起訴ほどの被害が出なかった」が 41.3%で最も多く、次に「証拠がない、情報が不足している」の 32.6%であった(図 34)。ログ等の十分な証跡がなかったために処分ができなかったと考えられる。適切な処分や法的措置をとるためには、操作履歴等のログ取得による証拠保全が必要といえる。

6.3 考察③(判例調査・インタビュー調査より)

・事前準備の上で、インシデント調査を外部に依頼する

インシデント発生時の対応について、自社内で対応することが難しい場合は、外部の支援サービス等の利用を検討する。内部不正の調査を外部に依頼する場合、何がどのように疑わしいのか、どのような結果を期待するのかを明確に伝える必要がある。また、分析に必要な情報(時期、対象データ、分析に必要なキーワード等)を事前に準備し、提供できるようにしておくことが望ましい。

・転職にともなう情報漏えいの対策として、退職者に対して秘密保持契約を締結する

退職者に対し、「在職中に得た秘密情報は退職後使わない」「秘密情報を持ち出さない」ことを確認できる秘密保持契約を締結することで、退職者に対し注意喚起するとともに、情報漏えいが発生し訴訟となった場合、知らなかったと言い逃れができないようにする。

付録１：事例集（インタビュー調査）

No	概要
1	業務委託先の従業員が、顧客の個人情報を、会社の記録媒体（CD）に不正にコピーし持ち出した。
2	従業員が退職時、営業情報を私物のハードディスクドライブに複製し持ち出した。
3	派遣社員が、処遇への不満から外部向けサービスのシステムを破壊し、サービスを停止させた。
4	業務委託先の従業員が、顧客情報を不正に持ち出し、自宅に設置している個人所有のNAS(Network Attached Storage)に保存していた。NAS の認証機能の設定が不適切だったため、インターネット上に顧客情報が流出した。
5	従業員が、顧客から Web の問い合わせフォームに入力された内容を、個人のアドレスにも送信するよう設定し、問い合わせ内容を不正に入手していた。
6	従業員が、会社が貸与していたスマートフォンにインストールしたアプリを利用して、会社のパソコンに接続し、Wi-Fi 経由で機密情報を外部に持ちだした。
7	システム管理者が、待遇に不満があり、他の社員が社内システムにアクセスできないようシステムの設定を変更した。
8	派遣社員が、オペレーションミスでうっかりデータを消去してしまった。
9	経営者が、新たに起業する目的で、重要情報を持ち出した。
10	元従業員が、在職中に重要情報をメールに添付し、複数回に分けて自宅のアドレスに送っていたことが発覚した。

付録２：アンケート調査票

Part1．予備調査

問1　あなたの性別をお知らせください。（1つ選択）

（1）男性　　（2）女性

問2　あなたの年齢をお知らせください。（数値記入）

□ 歳

問3　あなたのお住まいの地域をお知らせください。（1つ選択）

（47 都道府県より選択）

SC1.　あなたの職業をお答えください。（1つ選択）

（1）会社役員　（2）会社員（正社員）　（3）会社員（契約社員／派遣社員）
（4）自営業／自由業　（5）公務員　（6）団体職員　（7）パート／アルバイト
（8）高校生　（9）大学生／大学院生　（10）主婦　（11）無職（求職者/退職者を含む）
（12）その他（　　）

SC2.　あなたの所属する企業・組織の従業員数を選んでください。（1つ選択）

（1）100 名未満　（2）100 名以上 300 名未満　（3）300 名以上 1,000 名未満　（4）1,000 名以上

SC3.　あなたの所属する企業・組織の業種（主な事業内容）として、もっとも近いものを1つ選んでください。（1つ選択）

（1）農林業・水産業　（2）鉱業　（3）建設・土木・工業
（4）電子部品・デバイス・電子回路製造業・情報通信機械器具製造業・電気機械器具製造業
（5）その他製造業　（6）電気・ガス・熱供給・水道業　（7）通信業　（8）情報サービス業
（9）その他の情報通信業　（10）運輸業・郵便業　（11）卸売業・小売業　（12）金融業・保険業
（13）不動産業・物品賃貸業　（14）学術研究・専門技術者（15）宿泊業・飲食サービス業
（16）生活関連サービス業・娯楽業　（17）教育・学習支援業　（18）医療・福祉
（19）複合サービス業　（20）その他サービス業　（21）その他

SC4.　あなたの現在の所属部門として、もっとも近いものを以下から選んでください。（1つ選択）

（1）企画・広報部門　（2）販売・営業部門　（3）製造・生産部門　（4）調達・購買部門
（5）生産管理・品質管理部門　（6）技術・研究開発部門　（7）総務・人事部門
（8）経理・財務部門　（9）情報システム部門

SC5.　あなたの現在の職位として、もっとも近いものを以下から選んでください。（複数選択可）
※「システム管理者(情報システム全般)」は他の職位と同時に選択することができます。

（1）経営層・役員相当　（2）部長相当　（3）課長相当　（4）係長・主任相当
（5）一般社員相当　（6）システム管理者(情報システム全般)　（7）その他専門職・特別職等

SC6. あなたが所属する企業・組織で、外部攻撃（外部者による不正アクセスや Web の改ざん、標的型攻撃等）や、内部不正（社員や退職者、委託先社員等による情報の持ち出し等の不正行為。ルールや規則違反を含む）が発生していますか。（複数選択可）

（1）外部攻撃があった　（2）内部不正があった　（3）外部攻撃や内部不正は発生していない
（4）わからない

SC7. あなたが所属する企業・組織で、ルール違反による個人情報や技術情報の漏えい等の内部不正に関する経験（聞いたことがある／ご自身でご経験がある）について お答えください。なお、ご自身がかつて所属していた企業・組織での経験もあわせてお答えください。（それぞれ複数選択可）

タテに回答 ↓		①聞いたことがある	②経験がある
（1）	顧客情報等の職務で知りえた情報の持ち出し	1	2
（2）	システムの破壊・改ざん	1	2
（3）	個人情報を売買するなど職務で知りえた情報の目的外利用	1	2
（4）	うっかりミスや不注意によるルールや規則の違反	1	2
（5）	上記以外の何らかのルールや規則の違反	1	2
（6）	聞いたことはない	1	－
（7）	経験はない	－	2

SC8. 前問でご回答いただいた内部規定違反やポリシー違反を行った理由として最もあてはまるものをお答えください。（1つ選択）

（1）ルールを知らずに違反した
（2）ルールを知っていたが、うっかり違反した
（3）ルールはあったが、ルール違反を繰り返している人がいたので、自分もやった
（4）企業・組織や上司などに恨みがあった
（5）処遇や待遇に不満があった
（6）業務が忙しく、終わらせるために持ち出す必要があった
（7）持ち出した情報や機材を換金したかった
（8）持ち出した情報や機材で転職や起業を有利にしたかった
（9）その他（　　）

文章をよく読み指示にしたがってご回答ください

SC9. 「いいえ」をご回答ください。（1つ選択）

（1）はい　（2）いいえ

予備調査のご協力ありがとうございます。
これより本調査に移ります。
引き続きご協力お願い致します。

Part2. 本調査

Q1. あなたの現在の職場の在勤年数をお答えください。(数値記入) ※半角数字でご記入ください。

□ 年

Q2. あなたが所属する企業・組織の情報管理、個人情報の管理についての取り組み状況を教えてください。あなたが所属する企業・組織では、ISMS*やプライバシーマーク**を取得していますか。(1つ選択)

*ISMS(情報セキュリティマネジメントシステム):
企業や組織で情報を適切に管理する仕組み。ここでは、企業・組織が構築した ISMS が JIS Q 27001 に適合しているかを認証する ISMS 認証取得のことを示す。

**プライバシーマーク:
日本工業規格「JIS Q 15001 個人情報保護マネジメントシステム—要求事項」に適合して、個人情報について適切な保護措置を講ずる体制を整備している事業者等を認定して、その旨を示すプライバシーマークを付与し、 事業活動に関してプライバシーマークの使用を認める制度。

(1) ISMS を取得している
(2) プライバシーマークを取得している
(3) ISMS とプライバシーマークの両方を取得している
(4) ISMS とプライバシーマークのどちらも取得していない
(5) わからない

Q3. あなたが所属する企業・組織で、「重要情報」はどの程度電子化されていますか。(1つ選択)
重要情報:漏えいすると事業に影響を及ぼす可能性がある情報。(例:顧客情報、技術情報、営業情報など)

(1) 全部 (2) 8 割程度 (3) 半分程度 (4) 3 割程度 (5) ほとんど電子化されていない
(6) わからない

Q4. あなたの所属する企業・組織では、下記の情報がどのように管理されていますか。あてはまるものをお答えください。（それぞれ複数選択可）

ヨコに回答→		①触れることのできる人をシステム的に制限している	②秘密情報であることがわかるようにしている	③施錠管理を実施している	④管理していない（管理対象外）	⑤該当情報を扱っていない	⑥わからない
（1）	経営戦略に関する情報（経営計画、目標、戦略、新規事業計画、M&A 計画など）	1	2	3	4	5	6
（2）	顧客に関する情報（顧客個人情報、顧客ニーズなど）	1	2	3	4	5	6
（3）	営業に関する情報（販売協力先情報、営業ターゲット情報、セールス・マーケティングノウハウ、仕入価格情報、仕入先情報など）	1	2	3	4	5	6
（4）	技術に関する情報（共同研究情報、研究者情報、素材情報、図面情報、製造技術情報、技術ノウハウなど）	1	2	3	4	5	6
（5）	管理に関する情報（社内システム情報（ID、パスワード）、システム構築情報、セキュリティ情報、従業者個人情報、人事評価データなど）	1	2	3	4	5	6

Q5. あなたの所属する企業・組織の方針やルールとしてあてはまるものお答えください。（複数選択可）

（1）業務の電子メールを個人のメールアドレスに転送することを禁止するルールがある
（2）添付ファイルの送付を禁止又は制限するルールがある
（3）業務用パソコンやスマートフォンは企業・組織から貸与するという方針がある
（4）企業・組織から支給されたパソコンを紛失した場合の対応手順（方針）がある
（5）内部不正の対策は経営者の責任であることを示す基本方針がある
（6）内部不正対策の担当責任者や管理体制、実施方針がある
（7）ジョブローテーションを実施している
（8）成果主義が導入されている
（9）年功序列制が採用されている
(10) 残業時間を是正するための対策が実施されている
(11) あてはまるものはない

Q6. あなたの所属する企業・組織では、クラウドサービスを利用していますか。（1つ選択）

（1）全社的に利用している　（2）一部の事業所又は部門で利用している
（3）利用していないが、今後利用する予定がある　（4）利用していないし、今後も利用する予定もない
（5）わからない

情報セキュリティインシデントの発生状況についてお伺いします。

Q7. あなたの所属する企業･組織で起きた個人情報や技術情報の漏えい等の内部不正について、誰が不正を働いたかをお答えください。（複数選択可）

（1）システム管理者　（2）技術者・開発者　（3）経営層・役員　（4）派遣社員　（5）委託先社員
（6）退職者　（7）その他（　　）

Q7-1 あなたの所属する企業･組織で起きた個人情報や技術情報の漏えい等の内部不正について、（上記 Q7 で回答した人物）が行った内部不正の詳細としてあてはまるものをお答えください。（それぞれ複数選択可）

Q7-1-1 **発生部門**
（1）企画・広報部門　（2）販売・営業部門　（3）製造・生産部門　（4）調達・購買部門
（5）生産管理・品質管理部門　（6）技術・研究開発部門　（7）総務・人事部門
（8）経理・財務部門　（9）情報システム部門

Q7-1-2 **対象となった情報・事象**
（1）顧客情報　（2）技術情報　（3）営業計画　（4）製造計画　（5）開発物品
（6）その他（　　）

Q7-1-3 **流出経路・媒体**
（1）紙媒体　（2）電子メール　（3）Web アップロード　（4）SNS　（5）USB メモリ
（6）スマートフォン　（7）ハードディスクドライブ　（8）パソコン　（9）あてはまるものはない

Q7-1-4 **不正の原因**
（1）ルールを知らずに違反した　（2）ルールを知っていたが、うっかり違反した
（3）ルールはあったがルール違反を繰り返している人がいたのでやった
（4）企業・組織や上司などに恨みがあった　（5）処遇や待遇に不満があった
（6）業務が忙しく終わらせるために持ち出す必要があった
（7）持ち出した情報や機材を換金したかった　（8）持ち出した情報や機材で転職を有利にしたかった
（9）わからない

Q7-1-5 **発生時期**
（1）2010 年以前　（2）2011 年　（3）2012 年　（4）2013 年　（5）2014 年　（6）2015 年

Q7-1-6 **不正を働いた者への対応**
（1）懲戒処分や起訴はしなかった　（2）社内規定に従い懲戒処分とした
（3）警察に相談した（被害届を出した）　（4）刑事告訴・告発した　（5）民事訴訟した

Q7-2 （上記 Q7 で回答した人物）が行った内部不正について、懲戒処分や起訴をしなかった理由をお答えください。（複数選択可）

（1）懲戒処分や起訴ほどの被害が出なかった
（2）証拠がない・情報が不足している
（3）不正行為を行った個人を特定できなかった
（4）風評被害などイメージダウンとなることを懸念した
（5）自社に対する信用失墜を懸念した
（6）処分対象の従業員が退職されると困る
（7）公になることで競合他社が優位になることを懸念した
（8）警察・法的機関から事前に起訴を否定された
（9）懲戒処分や起訴できることを知らなかった
（10）起訴の手続きがわからなかった
（11）法的機関から国家安全保障に関連するといわれた
（12）その他（　　）

Q8. あなたの所属する企業・組織で、今後内部不正が発生すると思いますか。あてはまるものをお答えください。（1つ選択）

（1）これまで発生していないので、今後も発生しない
（2）対策をしていないので、内部不正が発生する恐れがある
（3）対策をしているので、内部不正は発生しない
（4）対策をしているが、軽微なルール違反が発生する恐れがある
（5）対策をしているが、重大なインシデントが発生する恐れがある
（6）対策をしても、内部不正を防ぐことはできない

内部不正対策の実施状況についてお伺いします。

Q9. あなたの所属する組織、企業において、下記の方針やルールが定められていますか。実施や確認・監査は行われていますか。（それぞれ1つずつ選択）

ヨコに回答→		① 方針やルールはない	② 方針やルールがあり（実施なし）	③ ②に加えてに実施あり（確認なし）	④ ③に加えて定期的に確認している（監査を含む）	⑤ わからない
（1）	情報の重要度に応じて格付け（区分）し、役職員の利用範囲、消去方法を決めている	1	2	3	4	5
（2）	重要情報を含む電子文書には、役職員にわかるように機密マーク等を表示している	1	2	3	4	5
（3）	情報システムの利用者に対し、利用者 ID およびアクセス権を設定している	1	2	3	4	5
（4）	役職員の異動や退職(雇用終了)により不要となった利用者 ID およびアクセス権を速やかに削除している	1	2	3	4	5
（5）	重要情報に対し、時間やアクセス数・量等の条件でアクセスを制限している（夜間はアクセス不可等）	1	2	3	4	5

（6）	利用者およびシステム管理者に対し、共有 ID および共有パスワード等の使用を禁止している	1	2	3	4	5
（7）	システム管理者が、必要な場合以外に特権を利用することを制限している（一時的な特権 ID 付与等）	1	2	3	4	5
（8）	壁の設置や入退管理策により、重要情報の格納場所等を物理的に保護している	1	2	3	4	5
（9）	モバイル機器や USB メモリ等の記録媒体を外部に持ち出す場合には、持ち出しを承認し記録等を管理している	1	2	3	4	5
（10）	私物のモバイル機器、記録媒体の持ち込みおよび業務利用を制限している	1	2	3	4	5
（11）	スマートデバイス等のモバイル機器やUSBメモリ等の外部記録媒体の利用をソフトウェアで制限している	1	2	3	4	5
（12）	ファイル共有ソフト等の許可されていないソフトウェアのインストール（導入）を禁止している	1	2	3	4	5
（13）	ソーシャルネットワークサービス（SNS）や掲示板等への Web アクセスをコンテンツフィルタ等で制限している	1	2	3	4	5
（14）	関係者へ重要情報（電子ファイル）を受渡す場合は、暗号化している	1	2	3	4	5
（15）	業務を委託する場合、セキュリティ対策を委託契約前に確認し合意している（必要に応じて契約に盛り込んでいる）	1	2	3	4	5
（16）	クラウドサービスを利用する場合、そのサービスレベル等に応じ、取り扱う重要情報を限定している	1	2	3	4	5
（17）	重要情報へのアクセス履歴及び利用者の操作履歴（Web のアクセスログやメールの送受信履歴他）等のログを、定めた期間安全に保護している	1	2	3	4	5
（18）	ログの監視、モニタリングにより、内部不正が疑われる行為等を検知している	1	2	3	4	5
（19）	システム管理者のログ（アクセス履歴や操作履歴等）を定期的に該当のシステム管理者以外が点検している	1	2	3	4	5
（20）	役職員に対して、内部不正対策に関する方針や重要情報の取り扱い等の手順を教育している	1	2	3	4	5
（21）	情報通信技術の進歩や新たな脅威に対応するため、内部不正対策の担当者に対し、研修等へ参加させている	1	2	3	4	5
（22）	雇用の終了時に秘密保持義務を課す誓約書を提出している	1	2	3	4	5
（23）	就業規則等の内部規程に、内部不正を犯した役職員に対する懲戒手続がある	1	2	3	4	5
（24）	入社時や特定の機会（昇格、業務の変更等）に、役職員は「秘密保持誓約書」等を提出している	1	2	3	4	5
（25）	人事評価や業績評価について必要に応じて上司等が評価内容を説明する機会がある	1	2	3	4	5
（26）	業務量や労働時間等が適正であり、健全な労働環境が整備されている	1	2	3	4	5
（27）	職場内の良好なコミュニケーションを組織全体で推進している	1	2	3	4	5
（28）	単独での作業を制限し、やむをえず単独で作業する場合は事前承認および事後確認をしている	1	2	3	4	5
（29）	内部不正発生時の状況把握や被害の拡大防止策のため、事前に企業・組織内外の関係者との連携体制を構築している	1	2	3	4	5
（30）	内部不正の再発防止策として、内部不正の事例を社内教育の内容に含め、企業・組織内に周知している	1	2	3	4	5

(31)	内部不正と思わしき事象が発生した場合の通報窓口を設置している	1	2	3	4	5
(32)	内部不正対策を定期的に確認し(監査を含む)、確認結果を経営者に報告するとともに、必要に応じ対策を見直している	1	2	3	4	5

Q10. あなたの所属する企業・組織では、他社に業務委託を実施していますか。(1つ選択)

(1) 委託している (2) 委託されている (3) 委託し且つ委託されている (4) 委託はない
(5) わからない

Q11. あなたの所属する企業・組織は委託先に対して以下のルールや規則を定めることを要求し、確認を行っていますか。(それぞれ1つずつ選択)

ヨコに回答→		① 委託先に書面で要求している	② 委託先に書面以外(口頭等)で要求している	③ 委託先に①又は②に加えて確認(監査等)を行っている	④ 委託先に何も実施していない	⑤ わからない
(1)	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て実践すること	1	2	3	4	5
(2)	ISMS やプライバシーマークを取得、更新すること	1	2	3	4	5
(3)	委託元に、体制の変更やセキュリティに関する問題等を報告すること	1	2	3	4	5
(4)	情報システムの運用に際して危険性や脆弱性について評価し、適切な対策をすること(ウイルス対策等)	1	2	3	4	5
(5)	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(法令順守)の推進体制を整備すること	1	2	3	4	5
(6)	重要な情報資産(情報及び情報システム)を、重要性のレベルごとに分類し、レベルに応じた表示や取扱(入手から破棄または返却まで)をするための方法を定めること	1	2	3	4	5
(7)	委託先企業は、採用、退職の際に守秘義務に関する書面を取り交わすなどして、セキュリティに関する就業上の義務を明確にすること	1	2	3	4	5
(8)	経営層や派遣を含む全ての従業者に対し、情報セキュリティに関する自組織の取組や関連規程類について、計画的な教育や指導を実施すること	1	2	3	4	5
(9)	重要な情報資産のある建物や区画に対して、物理的なセキュリティ対策を実施し、入退室管理をすること(顧客、ベンダー、運送業者、清掃業者等)	1	2	3	4	5
(10)	私物のモバイル機器や記録媒体などについて持ち込み・持ち出しを適切に管理すること	1	2	3	4	5
(11)	ネットワークを流れるデータを保護すること(外部から社内システムへのアクセス、メールの添付ファイルの暗号化等)	1	2	3	4	5
(12)	情報(データ)や情報システムへのアクセスを制限するために、利用者 ID の管理、利用者の識別と認証、アクセス権の付与と制御を適切に実施すること	1	2	3	4	5

（13）	情報セキュリティ事象が発生した際に委託元と連携し対応すること(ログの提供を含む)	1	2	3	4	5
（14）	再委託をする場合は、再委託先の業務内容および重要情報の取り扱い等について、委託元に事前報告または承認を求めること	1	2	3	4	5

Q12. あなたの所属する企業・組織で、内部不正対策を検討している部署、部門はどこですか。(複数選択可)
内部不正:社員や退職者、委託先社員等による情報の持ち出し等の不正行為。ルールや規則違反を含む。

（1）経営層　（2）総務部門　（3）情報システム部門　（4）人事部門
（5）法務・知的財産部門　（6）営業部門　（7）開発部門　（8）外部委託業者（コンサル会社等）
（9）なし　(10) わからない

Q13. あなたの所属する企業・組織では、内部不正の対策をどのように検討していますか。(複数選択可)
(内部不正対策には、管理策や体制の整備、予算確保や人員配置も含みます)

（1）ISMS 取得の一環として内部不正対策を検討している
（2）プライバシーマーク取得の一環として内部不正対策を検討している
（3）ガバナンス（内部統制）の一環として内部不正対策を検討している
（4）情報セキュリティ対策の一環として内部不正対策を検討している
（5）内部不正対策は他の取組とは分けて個別に検討している
（6）内部不正対策について検討していない
（7）わからない

Q14. あなたの所属する企業・組織の内部不正対策に関わる課題としてあてはまるものをお答えください。
(複数選択可)

（1）経営層による内部不正対策への意識が低い
（2）現場の意識が低く、各種対策が徹底されていない
（3）各種対策を講じる際、部署ごとに意識のばらつきがある
（4）利便性や業務効率が低下するため、各種対策の実施が徹底されない
（5）内部不正に関する予算が確保できない、または不足している
（6）内部不正対策を推進する人材がいない、または不足している
（7）新たな脅威や、最新の対策技術に対応できていない
（8）組織として内部不正対策よりも優先すべき課題がある
（9）内部不正対策として何をしたらいいかわからない
(10) 委託先（再委託先等）のセキュリティ対策に不安がある
(11) 委託先を選定する際の情報セキュリティ対策の基準が明確でない
(12) 委託先のセキュリティ対策の不備を指摘しても改善されない
(13) その他（　　）
(14) 内部不正対策に関わる課題は無い

Q15. **あなたの所属する企業・組織では、内部不正対策について見直しが行われていますか。見直すきっかけとなった出来事としてあてはまるものをお答えください。（複数選択可）**

（1）教育事業者による個人情報の漏洩（2014 年 7 月）
（2）公的機関のサーバへの不正アクセスによる個人情報の漏洩（2015 年 5 月）
（3）営業秘密管理指針の全面改定（2015 年 1 月）
（4）不正競争防止法の一部改正（2015 年 7 月）
（5）個人情報保護法の改正（2015 年 9 月）
（6）マイナンバー制度の導入（2016 年 1 月）
（7）在宅勤務を推進するため内部不正対策を見直した
（8）きっかけは特に無い
（9）わからない
（10）内部不正対策の見直しは行っていない

Q16. **あなたの所属する企業・組織の内部不正対策にかける予算について、今年度の規模と昨年度を比較して変化はありますか。（1つ選択）**

（1）減った　（2）変わらない（対策内容は変わらない）
（3）変わらない（予算は変わらないが対策は変わった）　（4）増えた　（5）わからない

Q17. **（経営者・システム管理者向け）あなたの所属する企業・組織で、役職員等の内部者による不正行為について、効果があると思われる対策をお答えください。（複数選択可）**
（従業員向け）あなたの所属する企業・組織で、どのような条件が整えば、不正を行いたいと思う気持ちが低下すると思いますか。あてはまるものをすべてお答えください。（複数選択可）

（1）技術情報や顧客情報などの重要情報は特定の職員のみがアクセスできる
（2）技術情報や顧客情報などの重要情報にアクセスした人が監視される（アクセスログの監視等を含む）
（3）ネットワークの利用制限がある（メールの送受信先の制限、Web メールへのアクセス制限、Web サイトの閲覧制限がある）
（4）管理者を増員する等、社内の監視体制を強化する
（5）職務上の成果物は、企業・組織に帰属することを研修等で周知徹底する
（6）職務上の成果物を公開した場合の罰則規定を強化する
（7）ルールや職務違反の基準がわからない場合に問合せや相談ができる担当者や窓口がある
（8）社外や業務時間外に仕事をすることがないように業務量を調整する
（9）社内システムにログインするための ID やパスワードは共有せずに管理する
（10）職場に監視カメラを設置する
（11）企業・組織内の重要情報を暗号化する（重要情報は限られた関係者しか閲覧できない）
（12）退職者のアカウントは、即日、削除する（退職者は退職日以降に社内システムへログインできない）
（13）パソコンや USB メモリなどの備品に企業・組織の管理シールを貼る（私物との区別がつく）
（14）CD や USB メモリ等の外部記憶媒体への書き出しや持ち出しが制限される
（15）上司や同僚に頻繁に相談できる環境を整備する
（16）システム管理権限を複数名に設定し、ルール違反の相互監視を徹底する
（17）社内システム上でのルール違反の痕跡は消去できない仕組みである
（18）これまでに、同僚が行ったルール違反が発見された
（19）これまでに、同僚が行ったルール違反が発覚し、処罰された
（20）情報システムの管理者以外がアクセス管理を操作することを制限している

内部不正対策時の対応についてお伺いします。

Q18. 役職員による内部不正が発生し、企業・組織内で解決できた場合を想定してください。今後、企業・組織が対策に役立てるため、その詳細について情報を公開する（関係機関への届出も含める）可能性はありますか。あてはまるものを下記の中からお答えください。（1つ選択）

（1）公開する　（2）場合によっては公開する　（3）場合によっては公開しない
（4）公開しない　（5）わからない

Q19. あなたの所属する企業・組織で『公開しない』という判断に影響を与えるものとしてあてはまるものを、下記の中からお答えください。（複数選択可）

（1）関係者との調整が困難だから　（2）競合他社に利用されるおそれがあるから
（3）重要情報の漏えいが拡大する可能性があるから
（4）自組織に対する否定的な評判が広まる可能性があるから　（5）その他（　　）

Q20. 仮に、あなたの所属する企業・組織で内部不正が発生した場合、届出・相談を行う可能性のある外部組織についてあてはまるものを下記の中からお答えください。（複数選択可）

（1）監督官庁　（2）警察　（3）JPCERT/CC（JPCERT コーディネーションセンター）
（4）IPA（独立行政法人情報処理推進機構）
（5）営業秘密・知財戦略相談窓口（INPIT/営業秘密 110 番）　（6）弁護士／弁理士
（7）監査人（内部監査員含む）　（8）不正検査士　（9）フォレンジック事業者　（10）その他

Q21. 仮にあなたの所属する企業・組織で内部不正が発生した場合、想定されるリスクとしてあてはまるものをお答えください。（3つまで選択可）

（1）営業活動の停止　（2）損害賠償等の費用の発生　（3）再発防止策の費用の発生
（4）社会的信用失墜　（5）顧客や委託元からの取引停止
（6）パートナー企業とのアライアンス（提携）解消　（7）競争力低下　（8）イメージダウン
（9）従業員（キーパーソン）の退職による事業の継続困難

職業文化、企業風土等についてお伺いします。

Q22. あなたの所属する企業・組織の職場環境や企業風土についてあてはまるものを、下記の中からお答えください。（それぞれ1つずつ選択）

ヨコに回答→	①非常にあてはまる	②あてはまる	③あてはまらない	④全くあてはまらない
■対象物の強化				
（1） 重要情報には必ずパスワード設定や暗号化をしている	1	2	3	4
（2） 重要情報はアクセスできる人が限られている	1	2	3	4
（3） 重要情報は施錠管理や施設立ち入り制限をしている	1	2	3	4
■接近の制御				
（4） 情報が保管されている部屋には決まった人しか入れない	1	2	3	4
（5） 入室記録が管理されている	1	2	3	4
（6） 執務室に一人きりになる時がある	1	2	3	4
■監視性の強化				
（7） 監視カメラが設置されている	1	2	3	4
（8） お互い同僚の目が届くところで仕事をしている	1	2	3	4
（9） 守衛がいる	1	2	3	4
■領域性の確保				
（10） 執務室と共用スペースには明確な境界がある	1	2	3	4
（11） 職場は安全で衛生的である	1	2	3	4
（12） 仕事をしていて、体に悪いと思うようなことはない（肉体的・精神的に健康を損ねることはない）	1	2	3	4
（13） 企業・組織から仕事に必要な機器（パソコン、携帯等）が十分与えられている	1	2	3	4
■企業・組織内の社会的凝集性				
（14） あなたと同僚との間には良好なチームワークがある	1	2	3	4
（15） 仕事が遅れたり困ったりしているとき、同僚はお互いに助け合っている	1	2	3	4
（16） 同僚との間では仕事上の情報交換が活発である	1	2	3	4
（17） 顔見知りの役職員が多い	1	2	3	4
■企業・組織内外のグループとの連携・協調				
（18） 役職員同士で挨拶、声掛けをする雰囲気がある	1	2	3	4
（19） 他部署とも連携できるようなネットワークがある	1	2	3	4
（20） 組織外部の人とも仲が良い	1	2	3	4
（21） 不審者に目が留まりやすい	1	2	3	4
■企業・組織の文化や場所性				
（22） 組織のかかげるビジョンや目標に、社員の多くが賛同している	1	2	3	4
（23） 企業・組織主催のイベント（運動会や慰安旅行等）が開催されている	1	2	3	4
（24） 役職員同士で食事等に出掛けることがある	1	2	3	4

■多様性・密度の閾値					
（25）	役職員同士の考え方は似ている	1	2	3	4
（26）	役職員は同じような就学環境の出身である	1	2	3	4
（27）	役職員は多様な年齢層で構成されている	1	2	3	4
（28）	組織内の役職員数は少なすぎる	1	2	3	4
■職場の信頼性、職場での助け合いの規範					
（29）	あなたの職場の人は、一般的に信頼できる	1	2	3	4
（30）	あなたの所属する企業・組織の人は、一般的に他人の役に立とうとしている	1	2	3	4

Q23. あなたが気軽に相談事ができる人は、企業・組織内に何人いますか。（1つ選択）

（1）0人　（2）1人　（3）2人　（4）3人　（5）4人　（6）5人　（7）6人以上

Q24. あなたの考え方に近いものをお答えください。（それぞれ1つずつ選択）
BYOD：Bring your own device の略で、役職員が個人保有の携帯用機器を職場に持ち込み業務利用を行うこと。

		① 非常にあてはまる	② あてはまる	③ あてはまらない	④ 全くあてはまらない
ヨコに回答→					
■監視への抵抗感					
（1）	所属している組織・企業に取り扱っているデータを監視されることに抵抗はない	1	2	3	4
（2）	所属している組織・企業から BYOD で取り扱っているデータを監視されることに抵抗はない	1	2	3	4
（3）	所属している組織・企業からメールを監視されることに抵抗はない	1	2	3	4
■持ち出し等への意識					
（4）	重要情報へのアクセスや持ち出し等を監視されていると感じる	1	2	3	4
（5）	ファイルを暗号化（パスワード等）して持ち出すことはセキュリティの観点から必要である	1	2	3	4
（6）	ファイルを暗号化（パスワード等）して持ち出すと不便である	1	2	3	4
■内部不正対策に関わる意識					
（7）	所属している組織内で内部不正が疑わしい事象が発生したときに、関係者全員の操作情報・取り扱っているデータを確認されることに抵抗はない	1	2	3	4
（8）	所属している組織・企業内で内部不正が発生した際、事案が内部で共有されることは望ましい	1	2	3	4
（9）	従業員のプライバシーよりも組織・企業のセキュリティを守るため、操作情報・取り扱っているデータが監視されることはやむをえない	1	2	3	4

付録３：職場環境・企業風土等に関するアンケート調査結果

所属する企業･組織の職場環境･企業風土等について尋ねた。300 名以上の企業の職場環境･企業風土の評価の結果を図 46 に示す。「重要情報はアクセスできる人が限られている」という回答は 8 割を超える。「対象物の強化」、「組織内の社会的凝集性」の項目は比較的「あてはまる」という回答が高い割合となった。

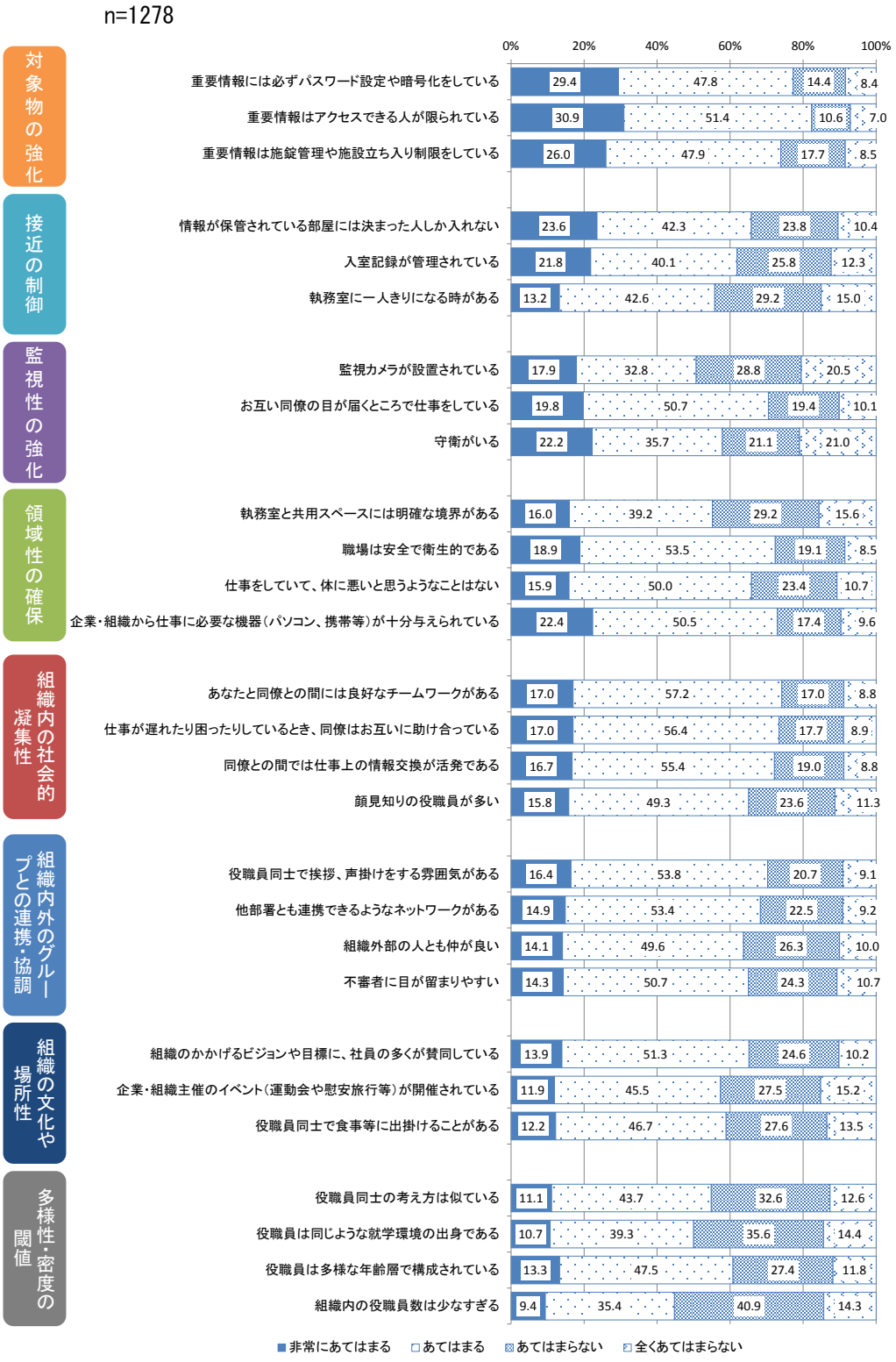

図 46　職場環境の評価（300 名以上）≪Q22≫

300 名未満の企業の職場環境・企業風土の評価の結果を図 47 に示す。全体的に 300 名以上の企業と比較して、「あてはまる（非常にあてはまるとあてはまるの合計）」の回答割合は低い。

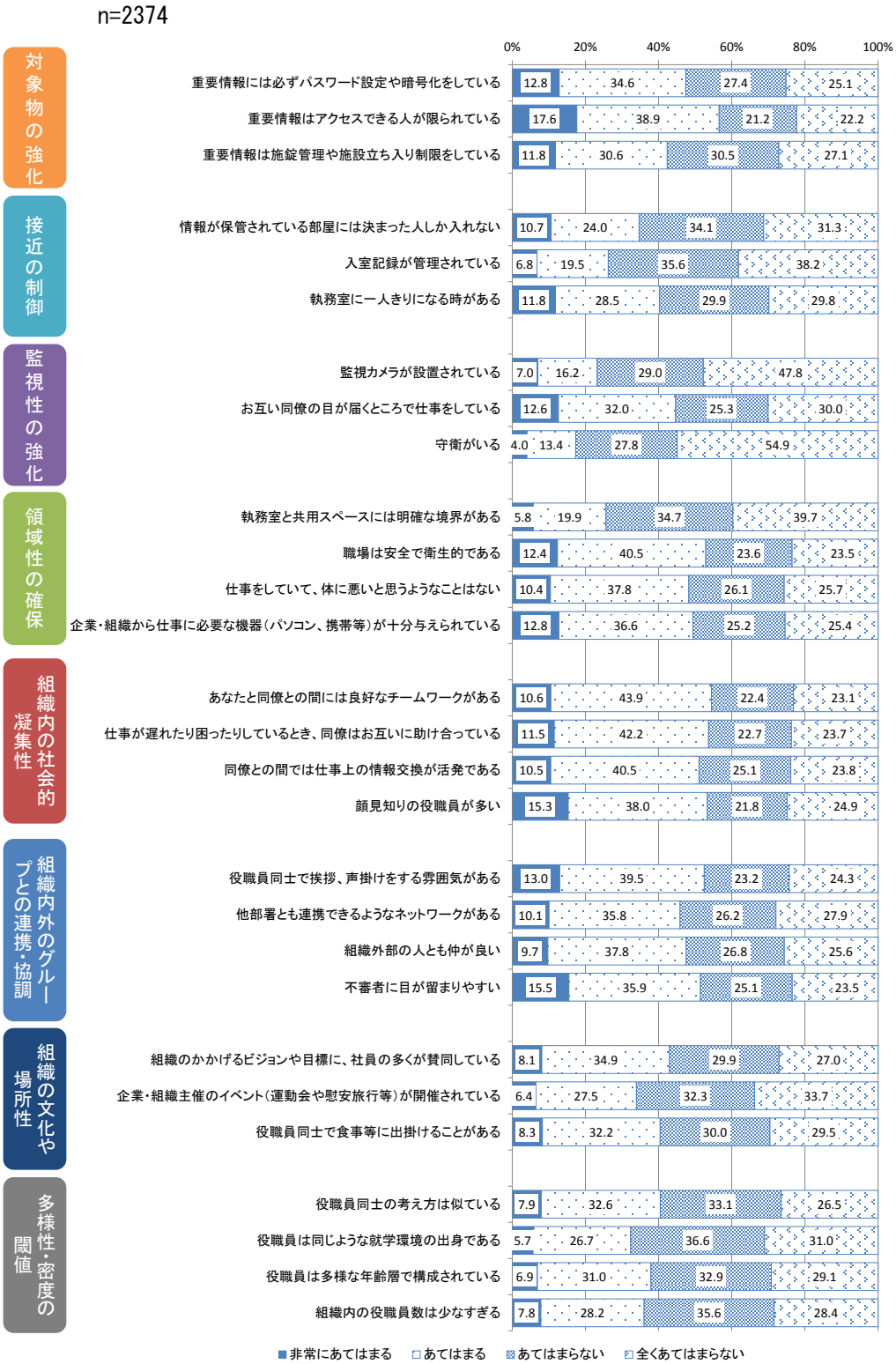

図 47　職場環境の評価（300 名未満）≪Q22≫

内部不正が発生することと職場環境・企業風土に関係があるか検証するため、内部不正が発生した企業と発生していない企業で職場環境の評価を比較する。ここでは比較のため、調査①の回答者の結果を、経済センサスの企業規模に応じてウエイトバック集計[40]した結果を用いる。

内部不正が発生した企業に所属する回答者の職場環境・企業風土の評価の結果を図 48 に示す。内部が発生した企業では、「執務室に一人きりになる時がある」という項目に「あてはまる」という回答が、企業規模別の結果（図 46、図 47）と比較して高い。

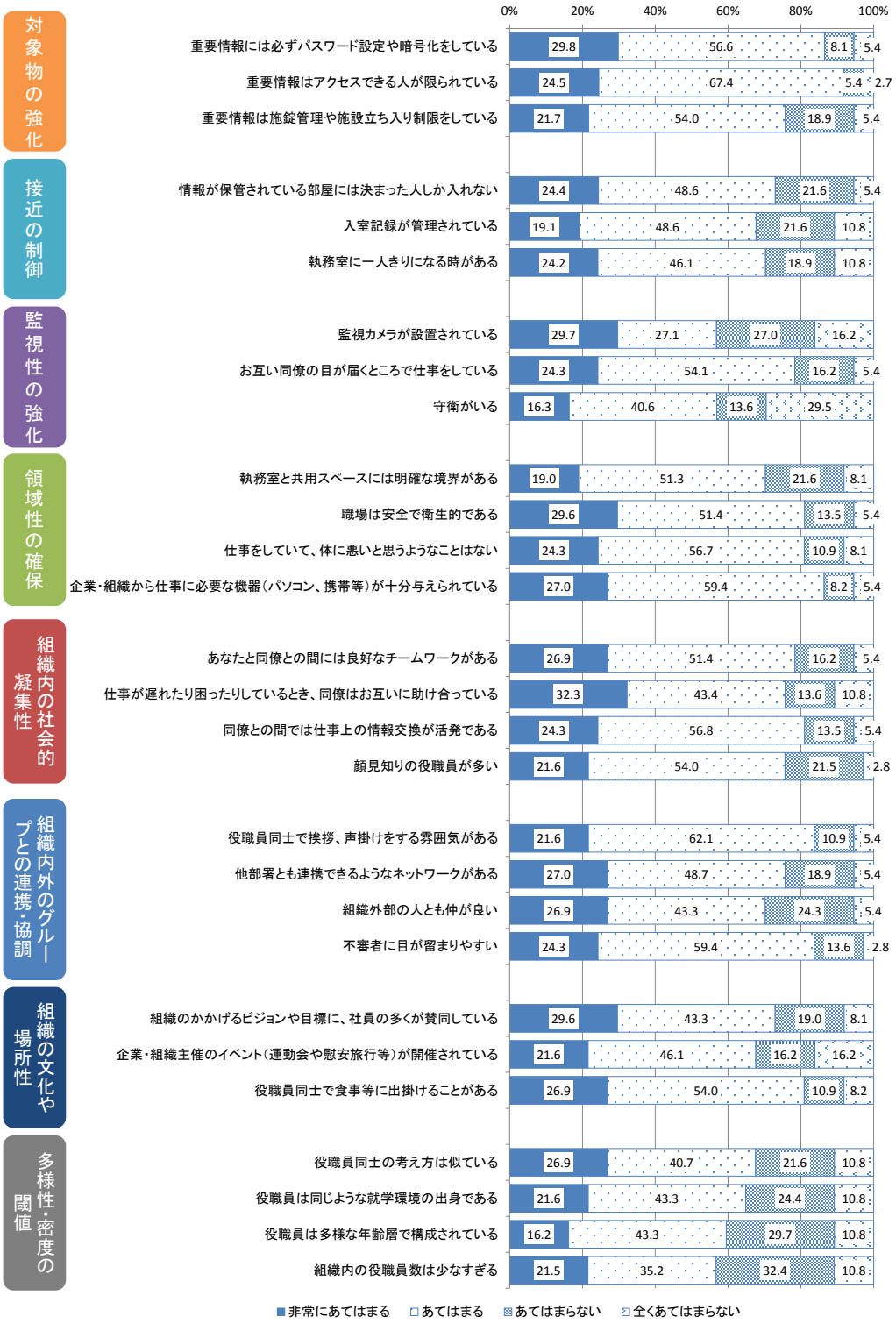

図 48　職場環境の評価（内部不正が発生した企業）≪Q22≫

[40] 調査したい母集団の構成比と、アンケートで回収したサンプルの構成比が異なる際に、その母集団の構成比に合わせるために、サンプルに重み付けをして集計する方法。

内部不正が発生していない企業に所属する回答者の職場環境・企業風土の結果を図 49 に示す。全体的に内部不正が発生した企業と比較して、職場環境が整備されていない傾向がみられる。内部不正が発生していないのではなく、内部不正が発生していても見過ごされている可能性が指摘される。

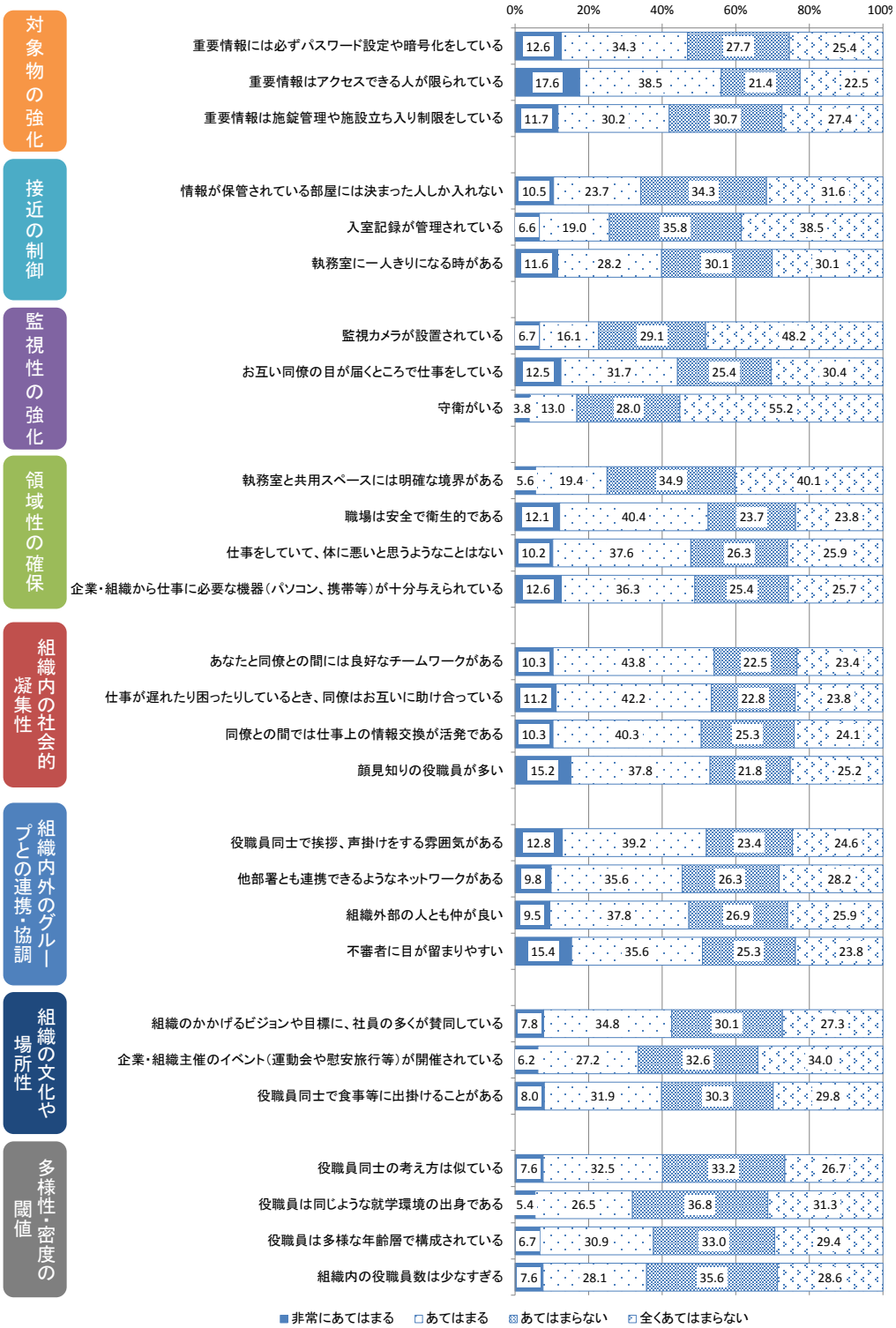

図 49　職場環境の評価（内部不正が発生していない企業）≪Q22≫