情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

2011年情報セキュリティ
アンケート調査結果

2011年12月1日

情報セキュリティ大学院大学
原田研究室

アンケート調査概要

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

情報セキュリティ調査について

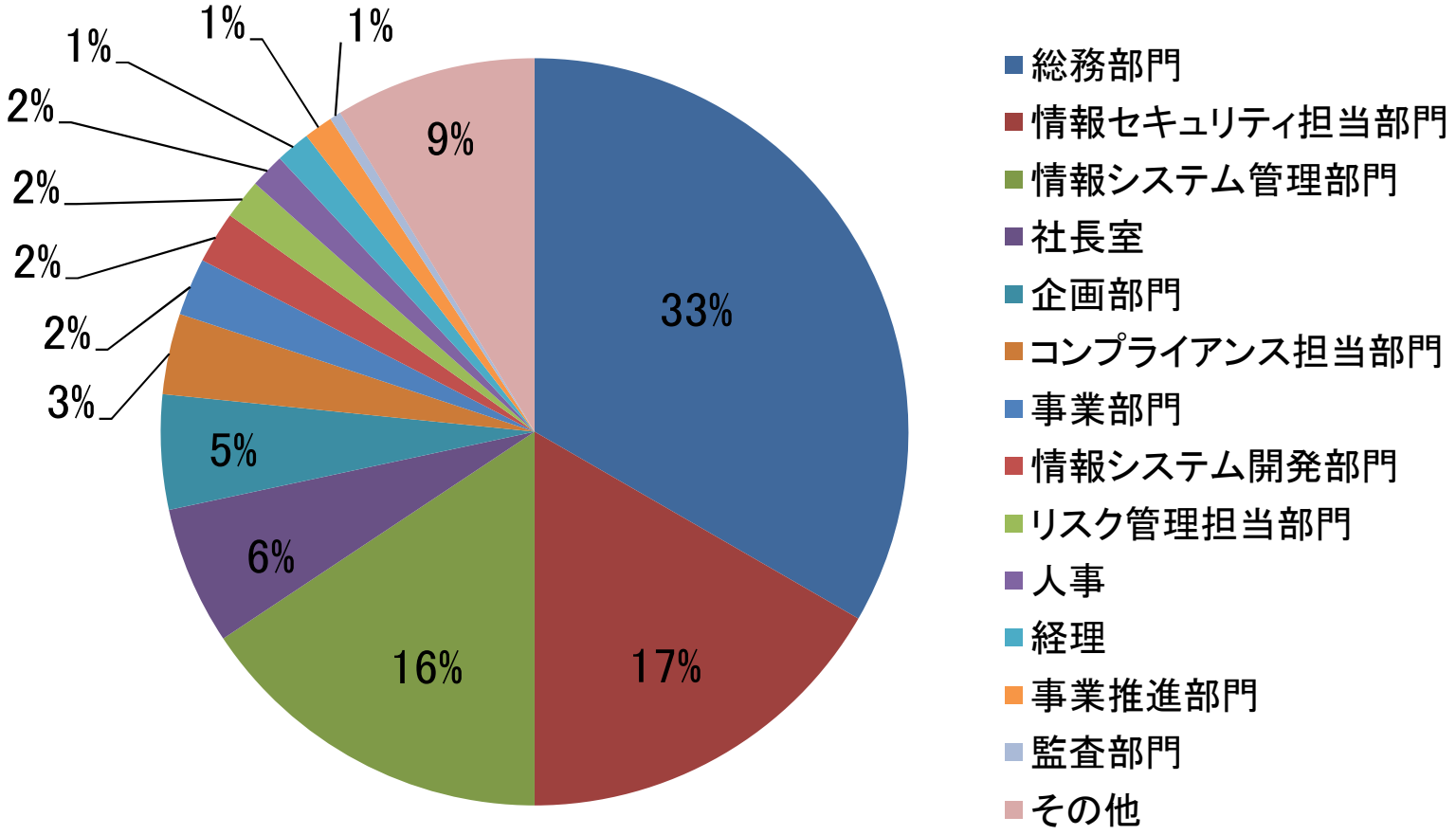
- アンケート実施期間
  2011年7月24日～8月26日
- アンケート対象
  プライバシーマーク取得企業、ISMS認証取得企業、官公庁、教育機関など4,500組織の情報セキュリティ・システム担当者
- アンケート内容
  プライバシーマーク取得状況、セキュリティマネジメントの運用状況、デジタルフォレンジックの実態、番号制度に関する意識調査
- 調査方法
  郵送による
- 回答状況
  407件（9.0%）

第1章

概要・IT環境について

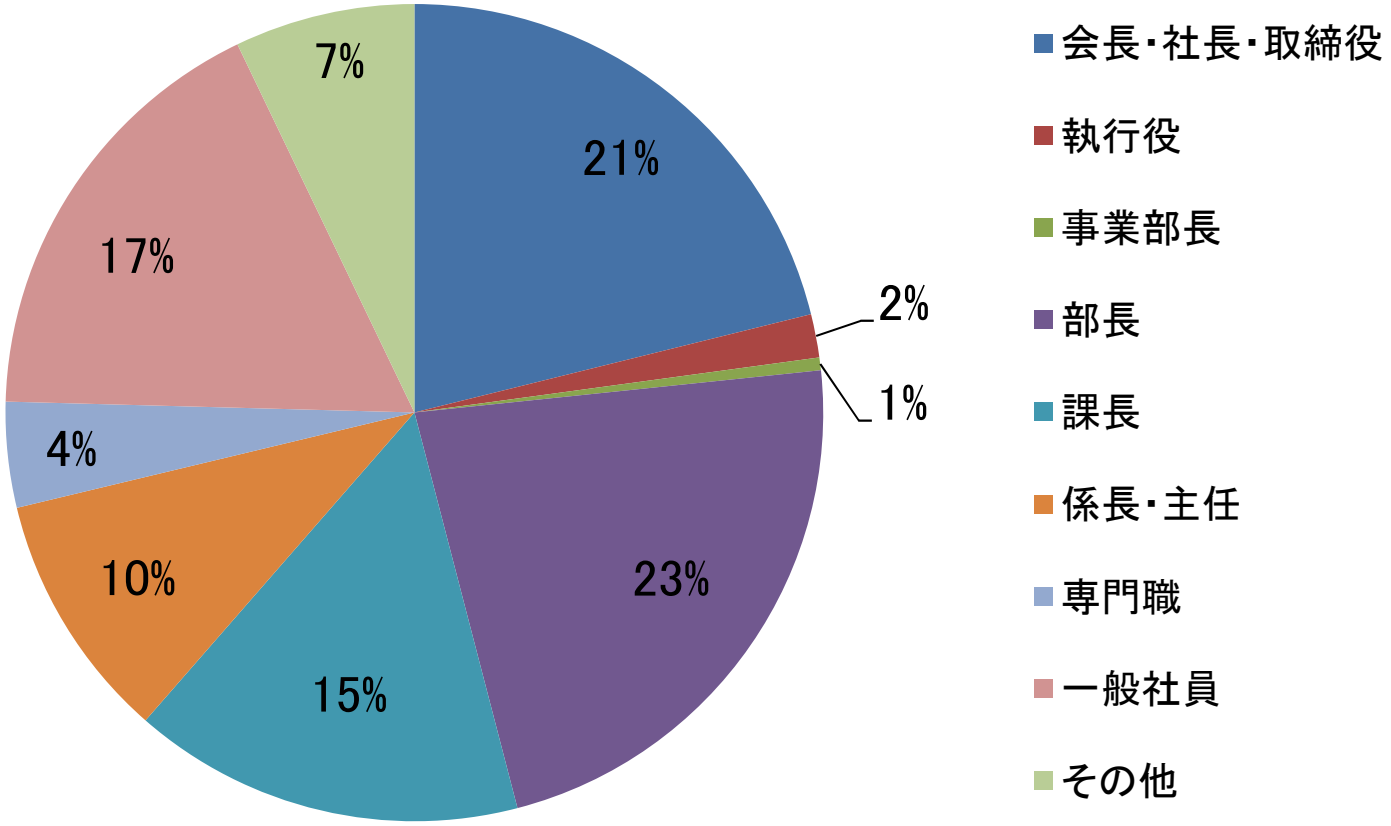
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

設問1.記入者の所属　（N=402）



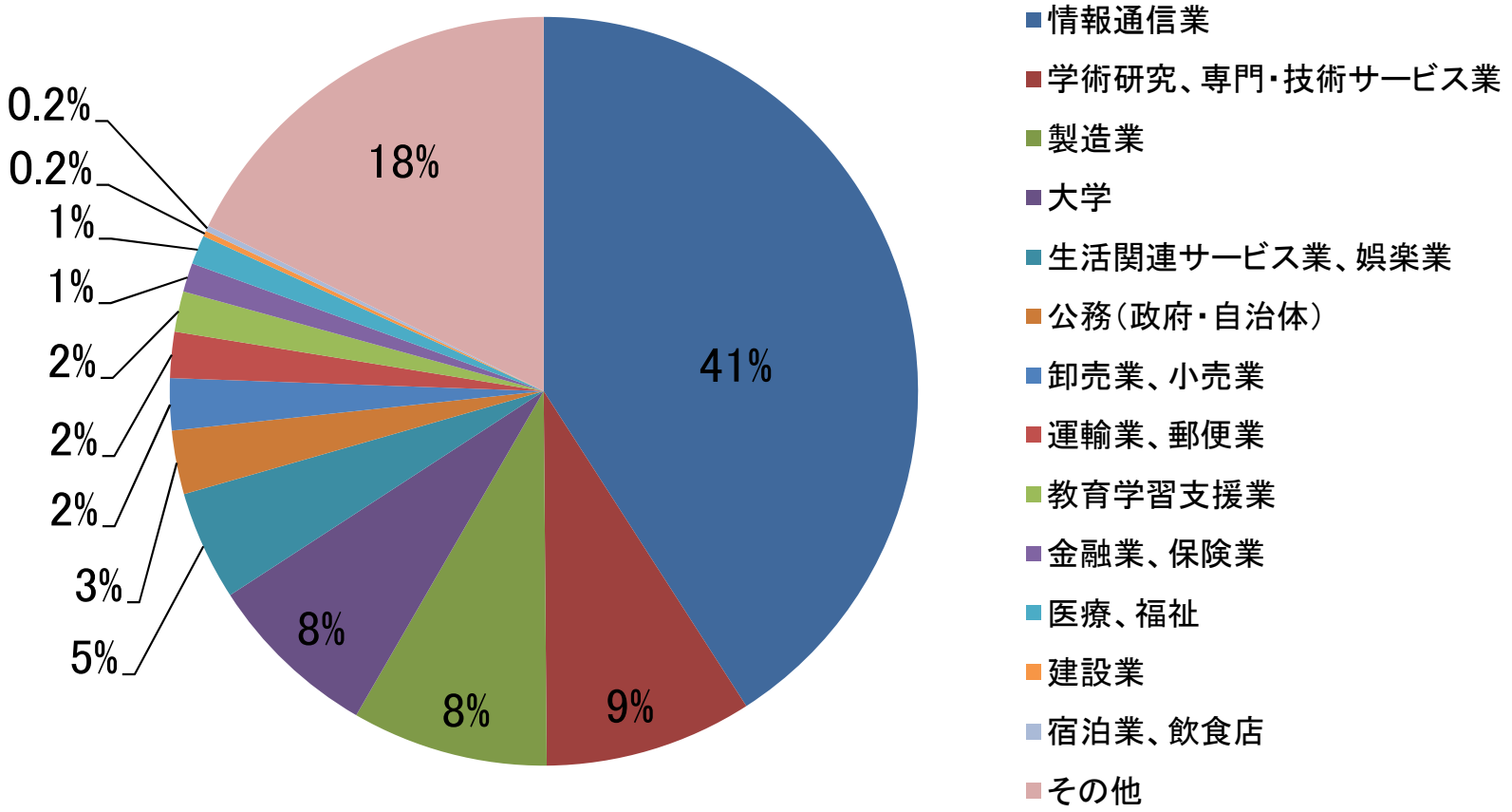
第1章　概要・IT環境について

設問2.記入者の役職　（N=407）



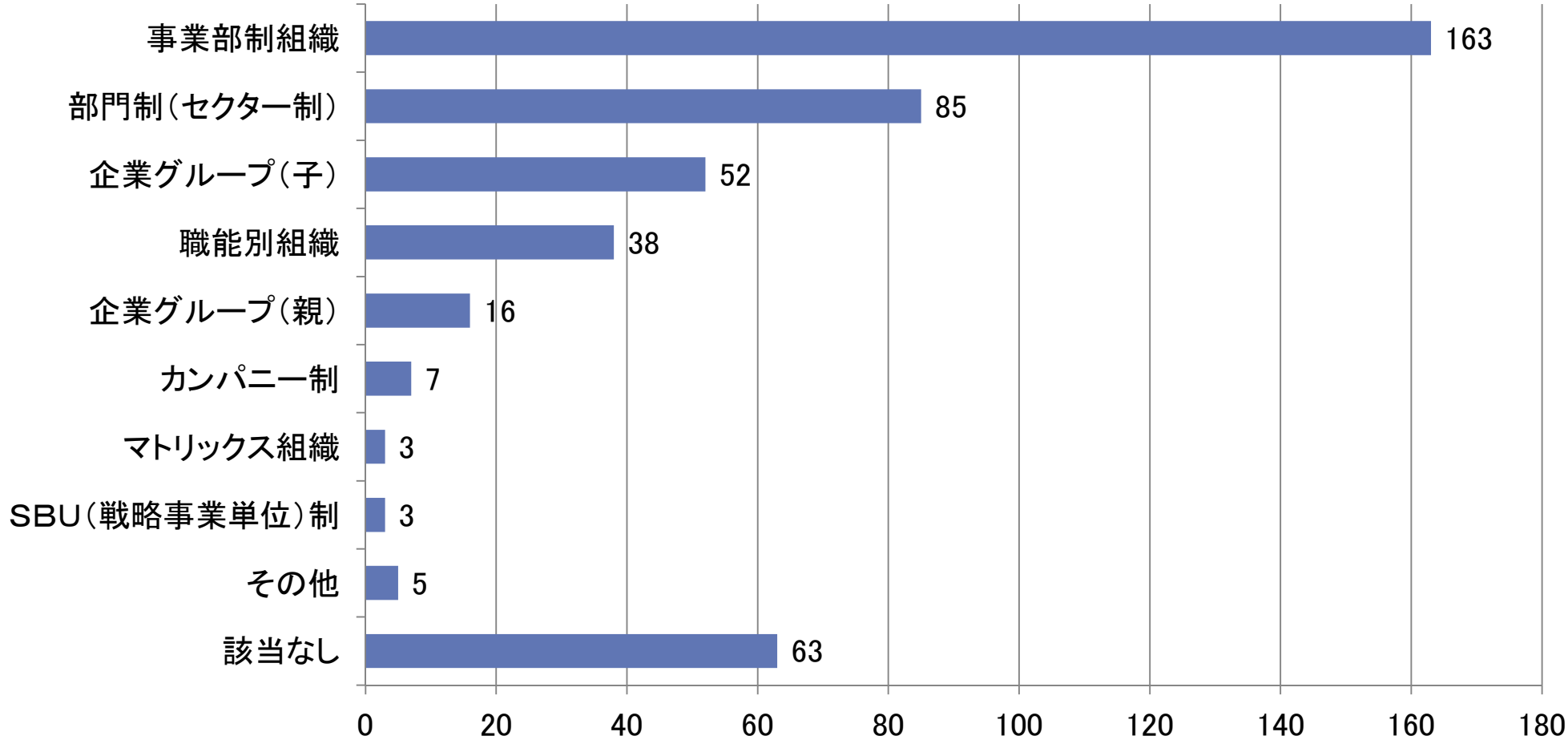
第1章　概要・IT環境について

設問3.業種（複数業種に該当する場合、売上高が最も高い業種（日本産業分類をベースとして使用）を選択）（N=401）



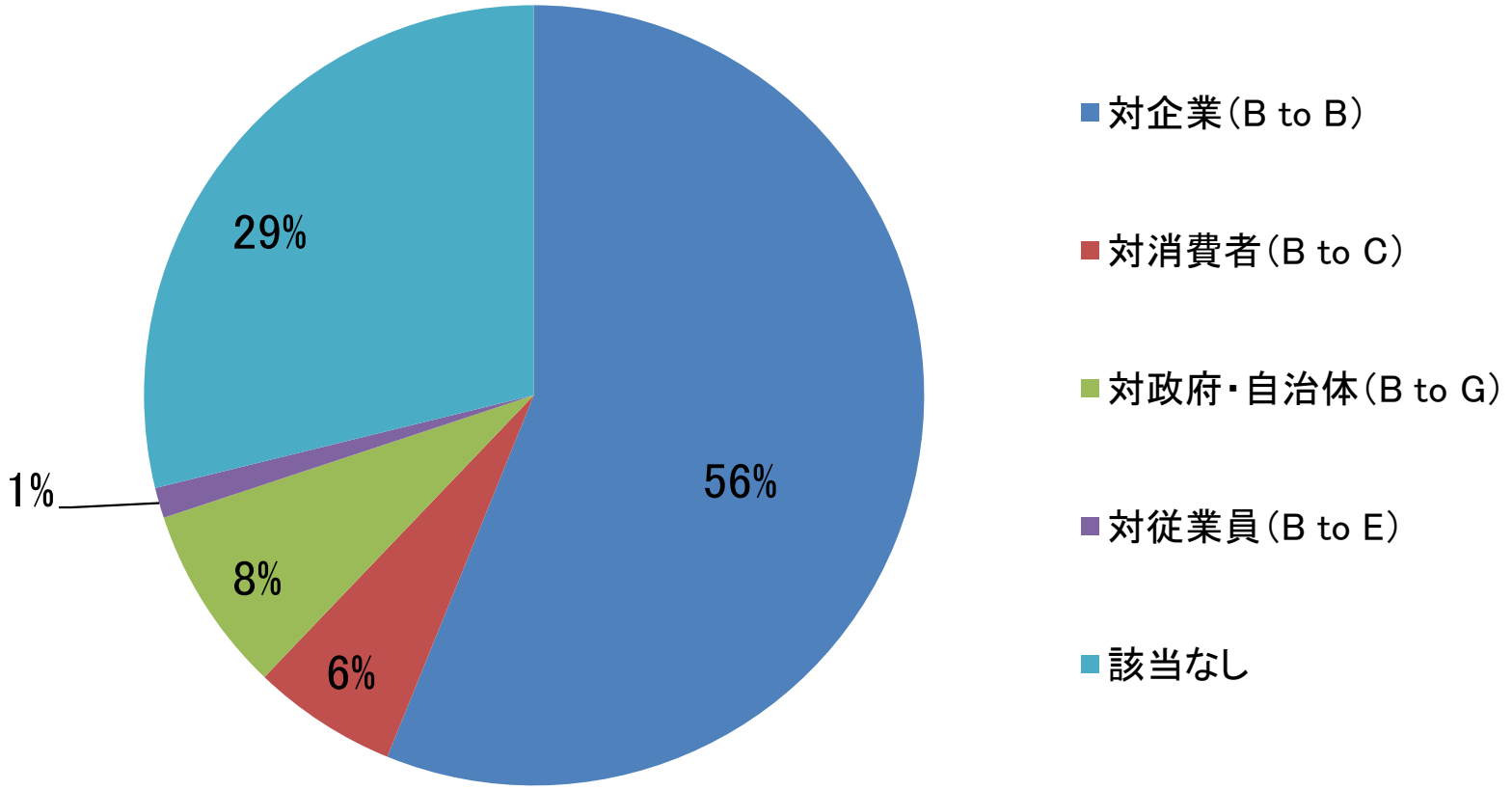
第1章　概要・IT環境について

設問4.組織構造（複数回答）（N=400）



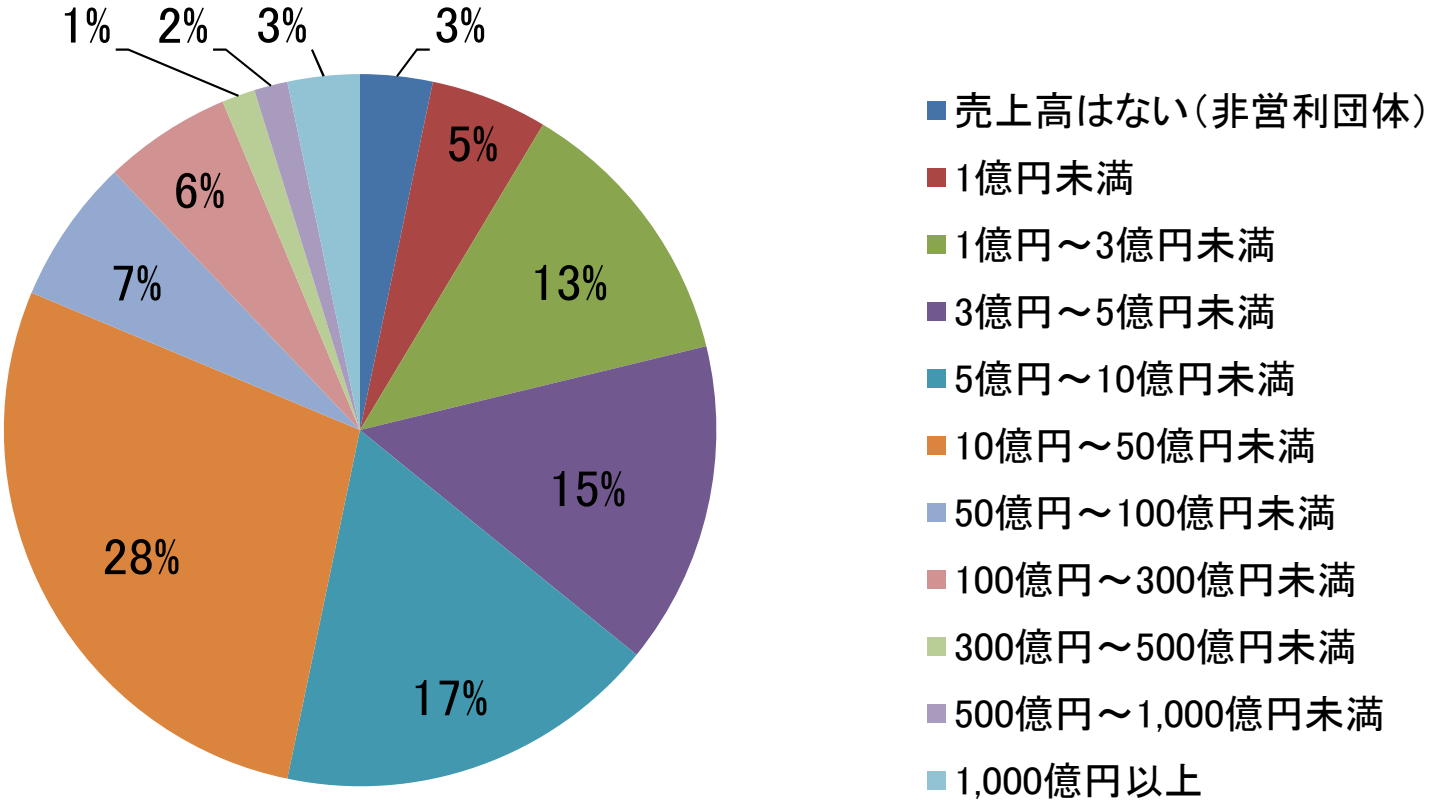
第1章　概要・IT環境について

設問5.主な電子商取引形態　（N=399）

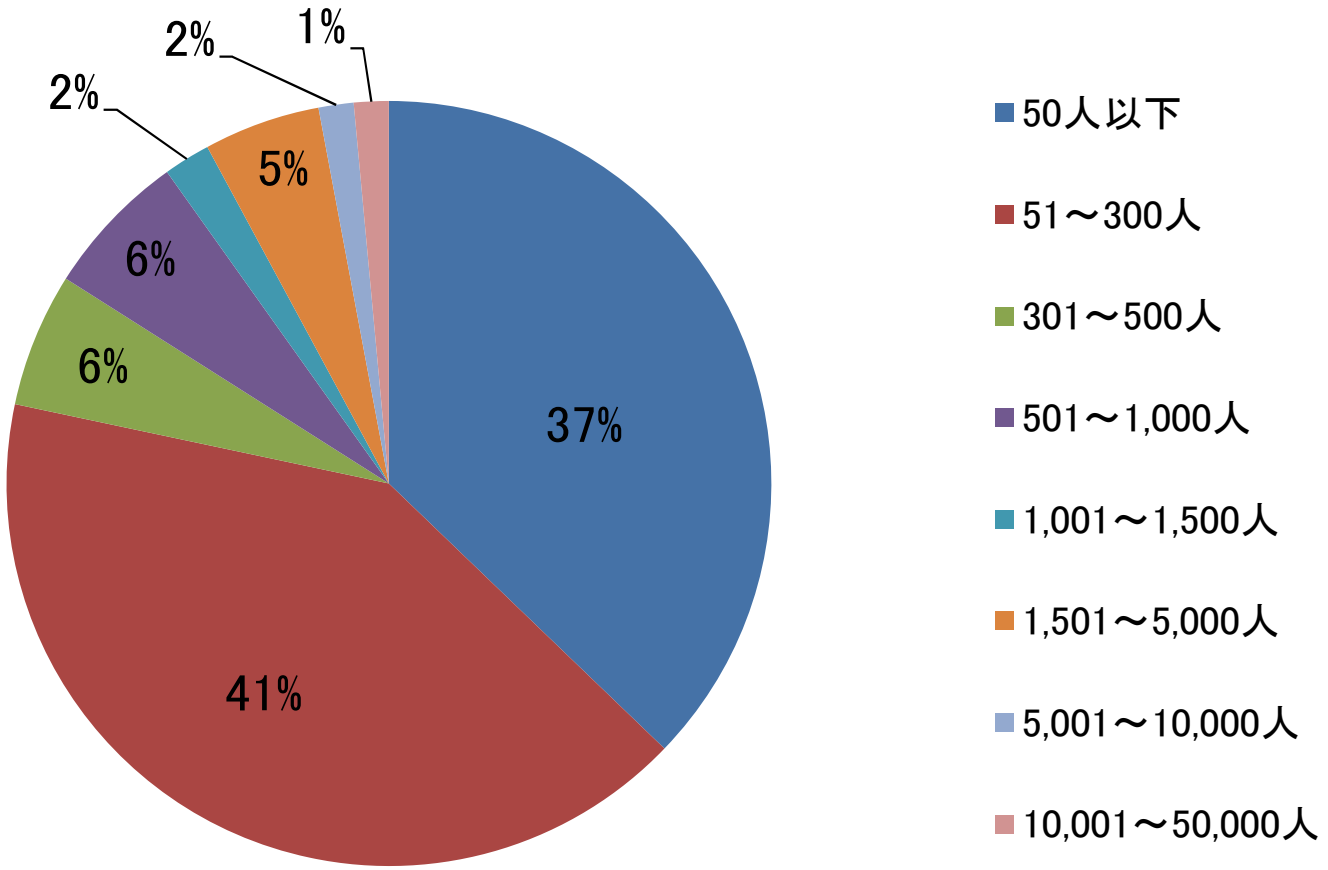


情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

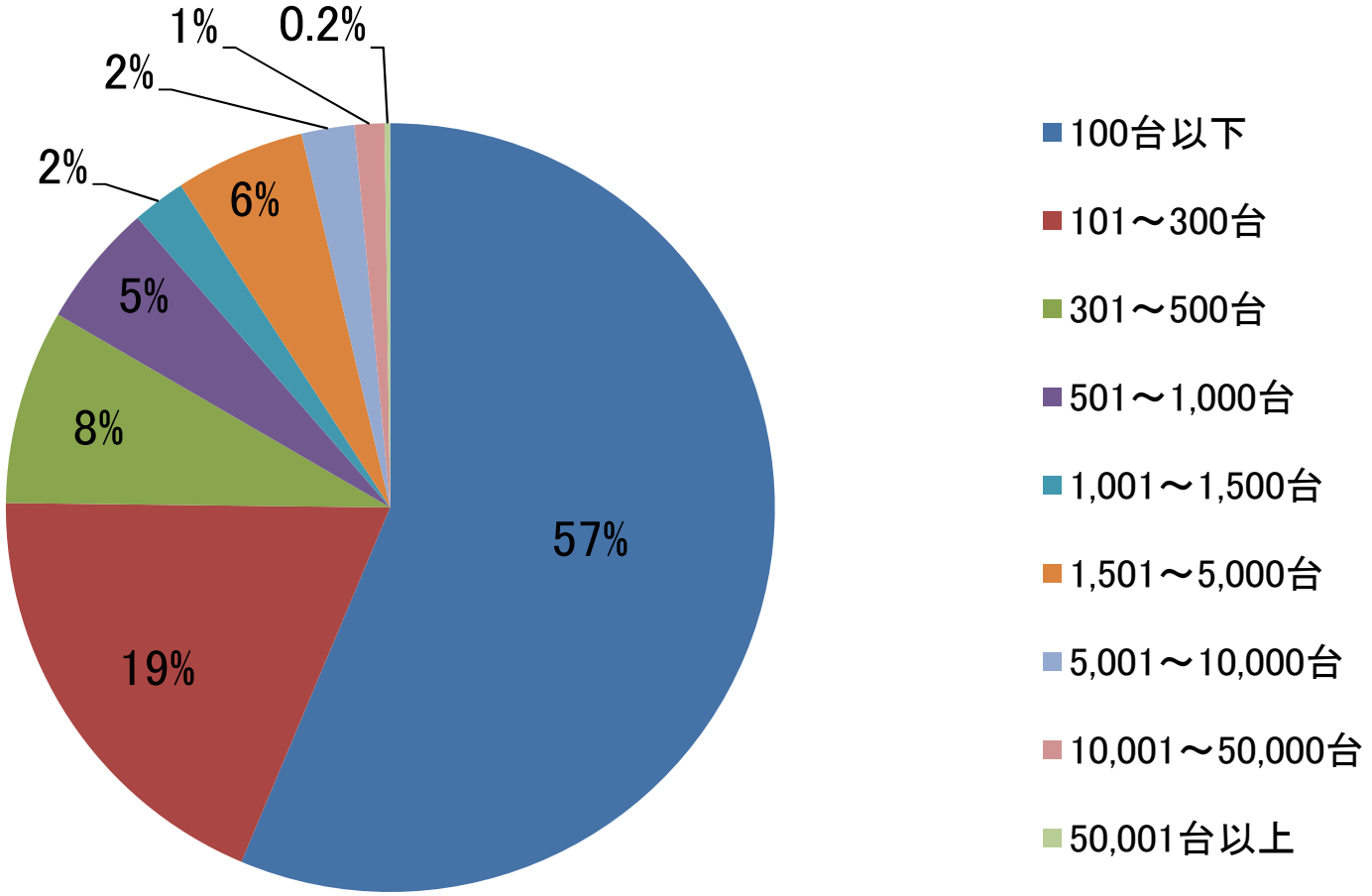
設問6.年間売上高（単独）（対象期間:2010 年4 月1 日から2011 年3 月31 日、大学・公務等は予算額、銀行は経常収益高、保険は収入保険料または正味保険料、証券は営業収入高。）（N=399）



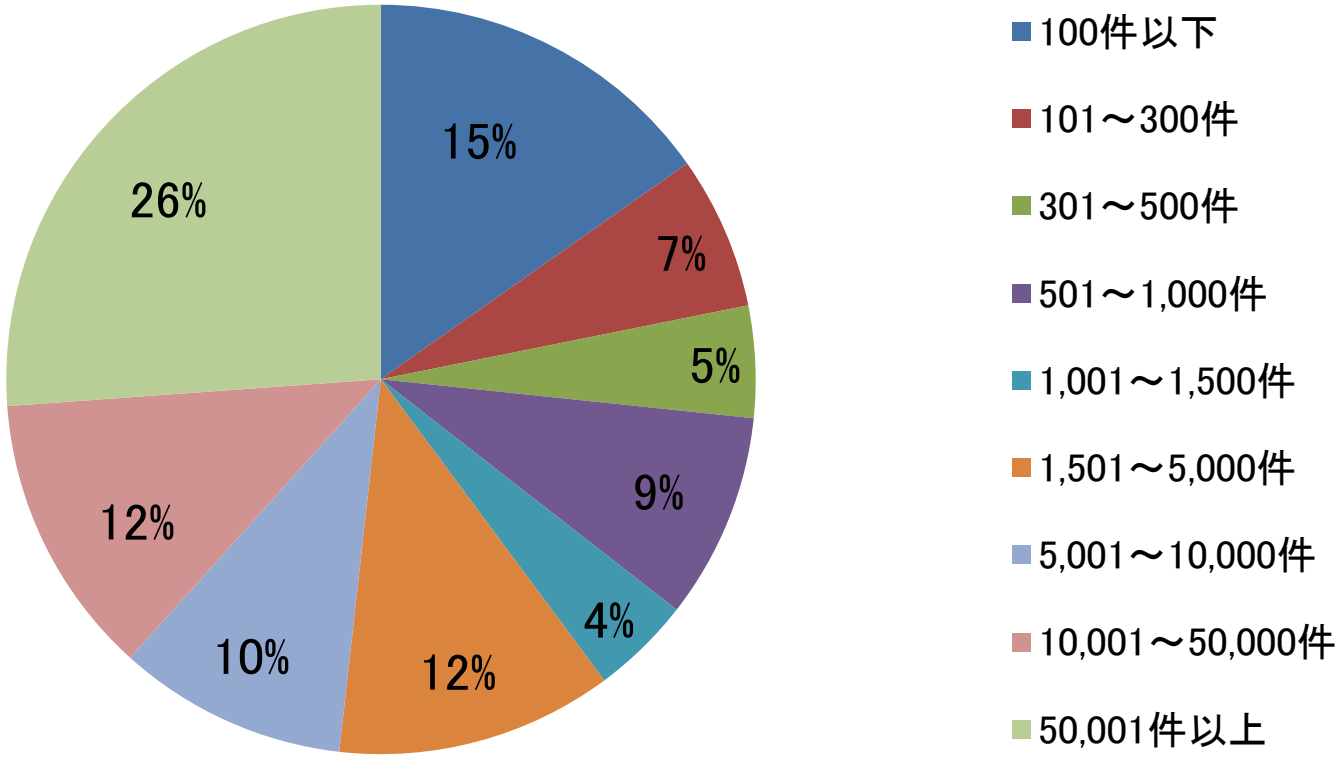
設問7.全従業員数　（単独）（N=406）



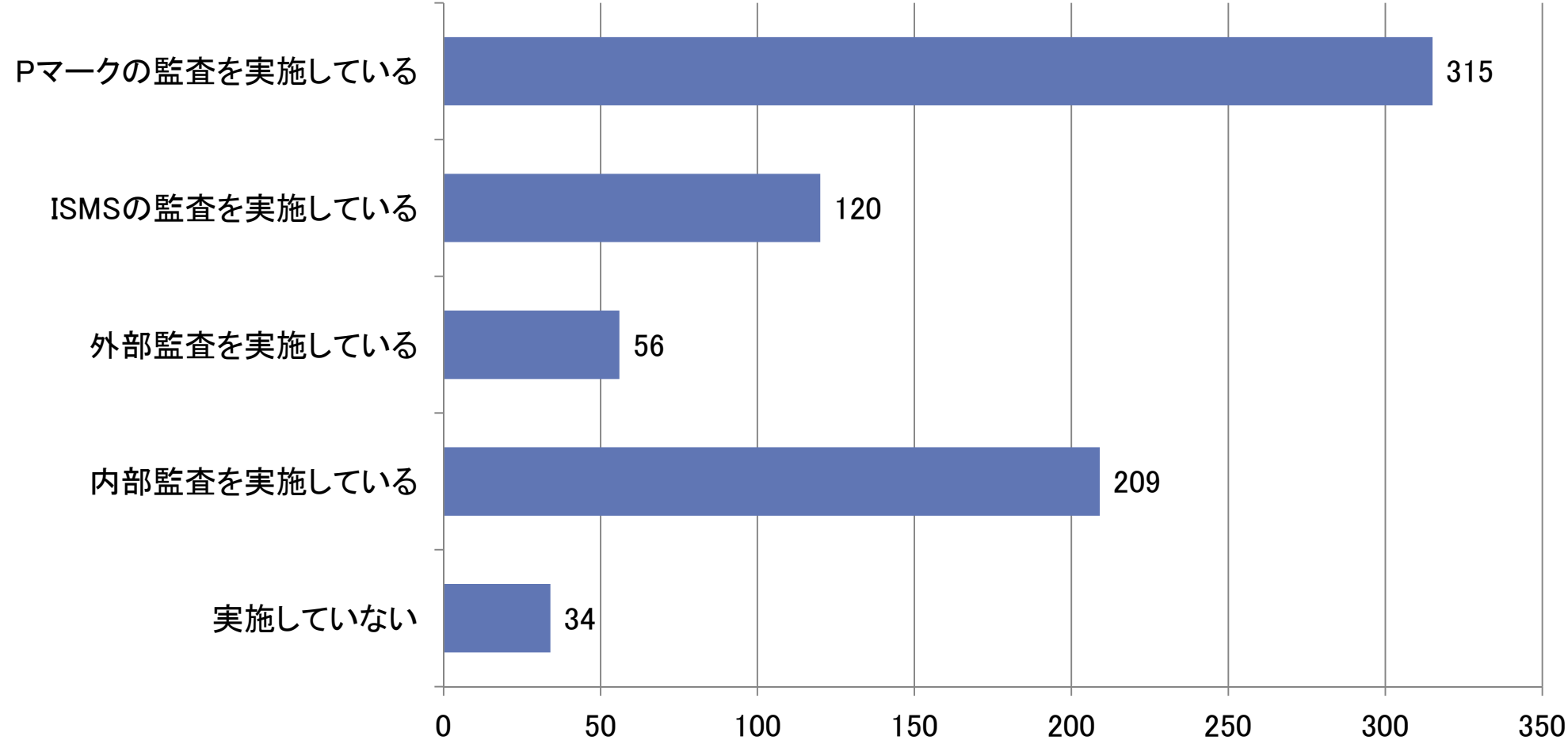
設問8.PC数（全社のおおまかな台数）（単独）（N=403）



設問9.個人情報の保護に関する法律で定義されている「保有個人データ」の件数（単独）（N=394）

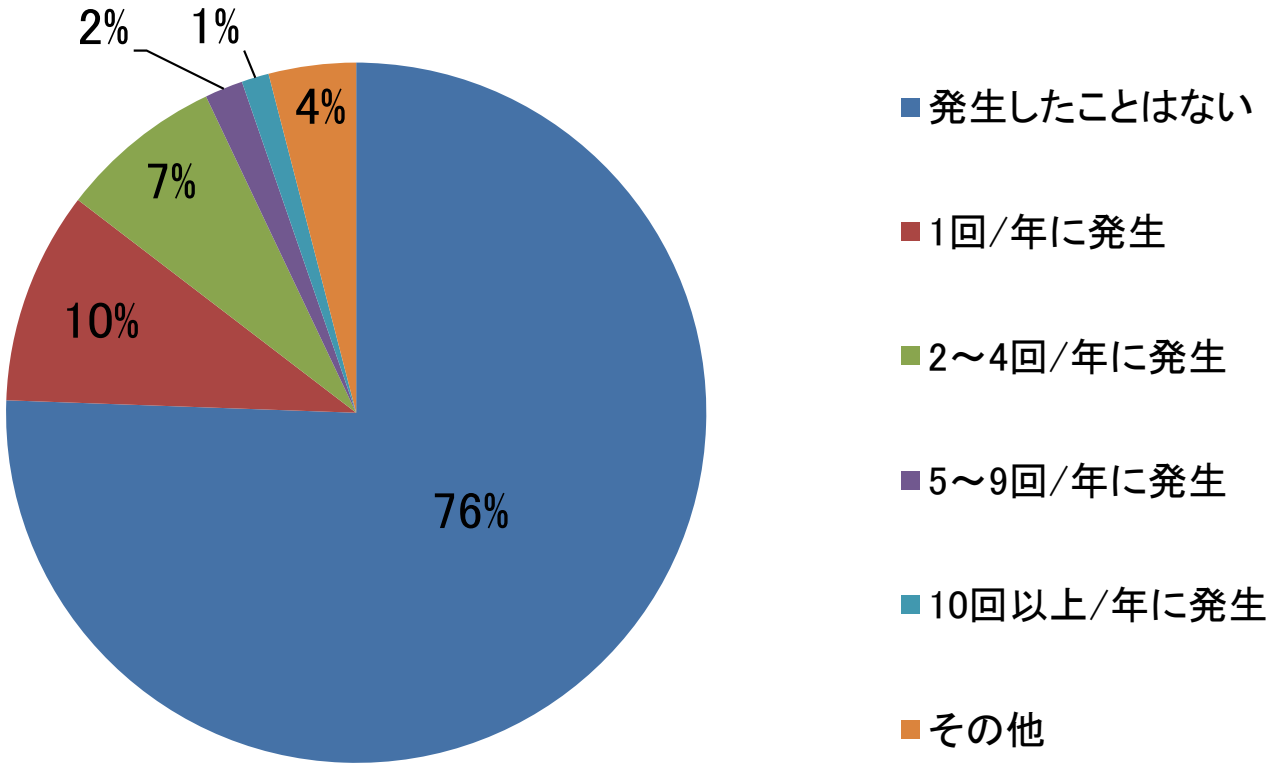


設問10.情報セキュリティ監査の実施有無　（複数回答）（N=404）



第1章　概要・IT環境について

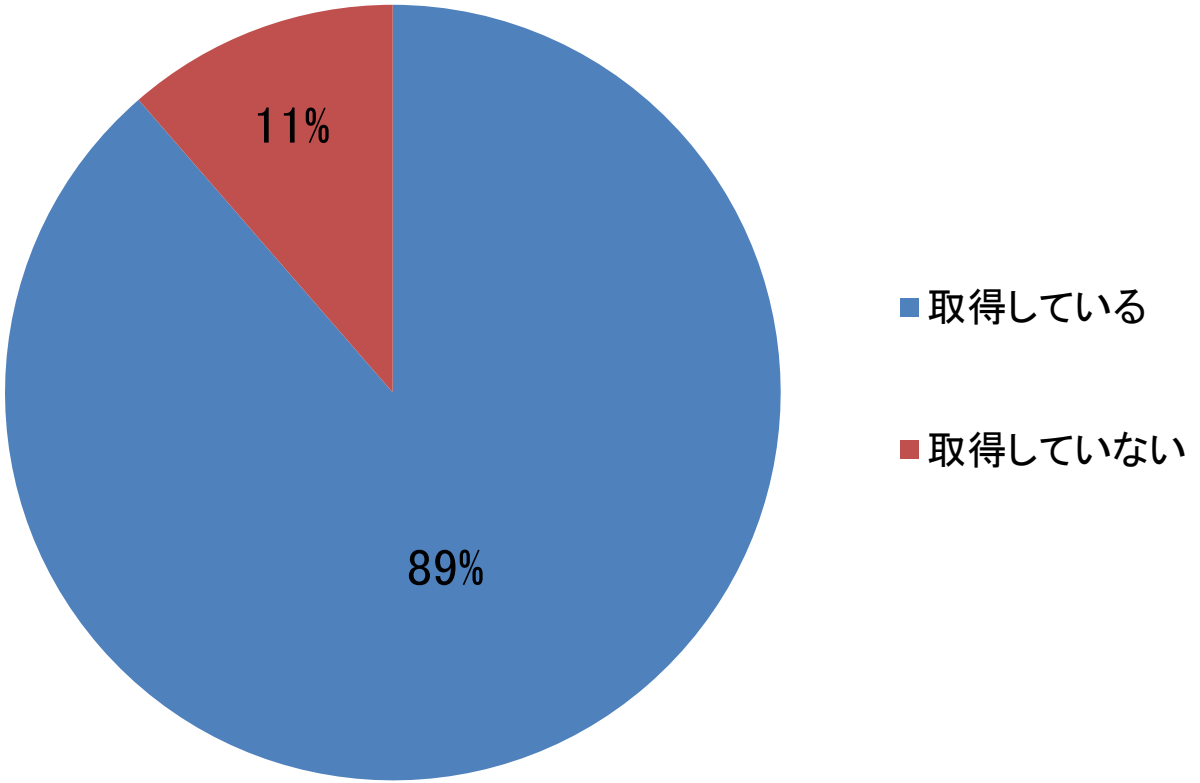
設問11.機密情報の誤送信（メール/FAX）や紛失、盗難、ファイル交換ソフト（P2Pソフト）による情報流出などの情報セキュリティ事故/事件が発生したことがありますか。（N=397）



第2章
プライバシーマーク取得状況について

第2章　プライバシーマーク取得状況について

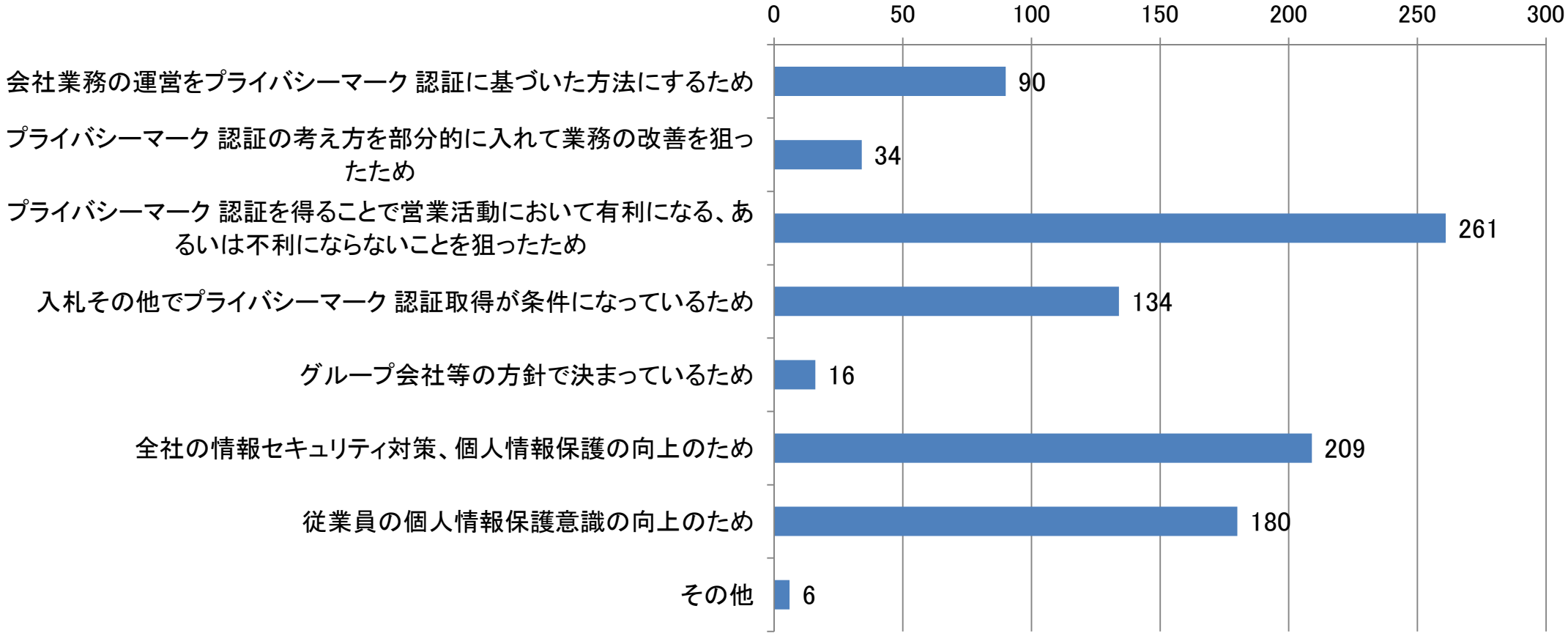
設問12.貴社はプライバシーマークを取得していますか。（N=404）



アンケート回答事業者の内、
約9割の事業者が、プライバシーマークを取得していた。

第2章　プライバシーマーク取得状況について

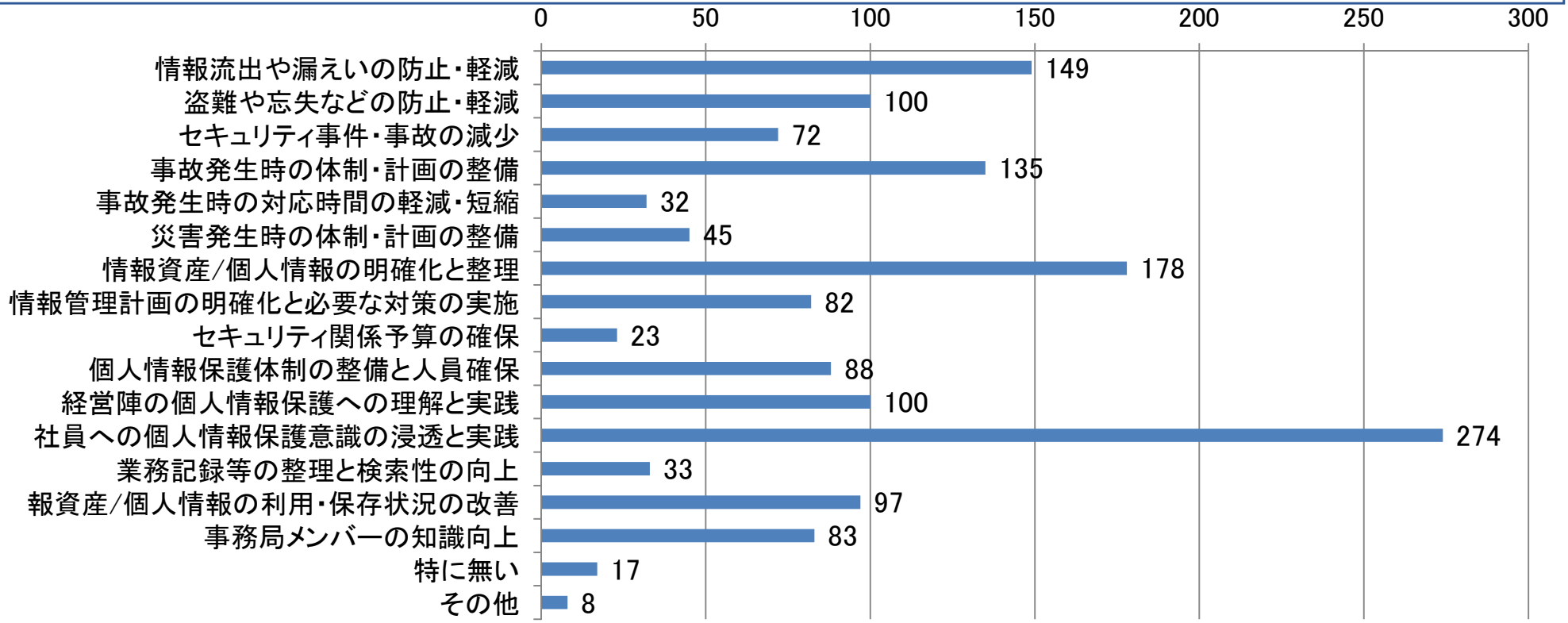
設問13.認証取得の主な目的をお答えください。（複数回答）（N=361）



営業活動の向上や入札目的の他に、
社内の個人情報保護の取り組み向上を目的としている事業者が多い。

第2章　プライバシーマーク取得状況について

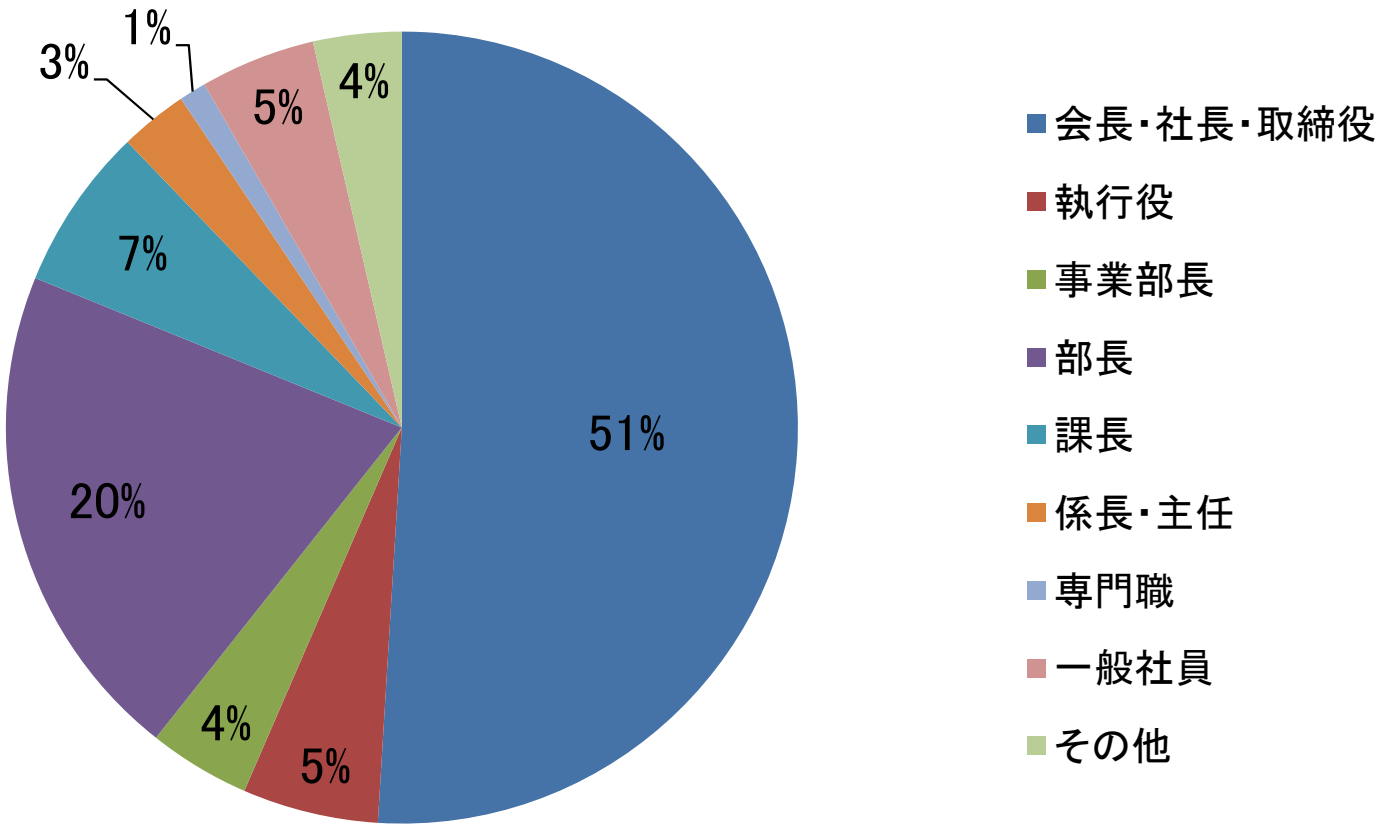
設問14.認証を取得して得られた効果をお答えください。（複数回答）
（N=358）



プライバシーマークの取得は、
社内の個人情報保護意識の浸透と実践に繋がっている。

第2章　プライバシーマーク取得状況について

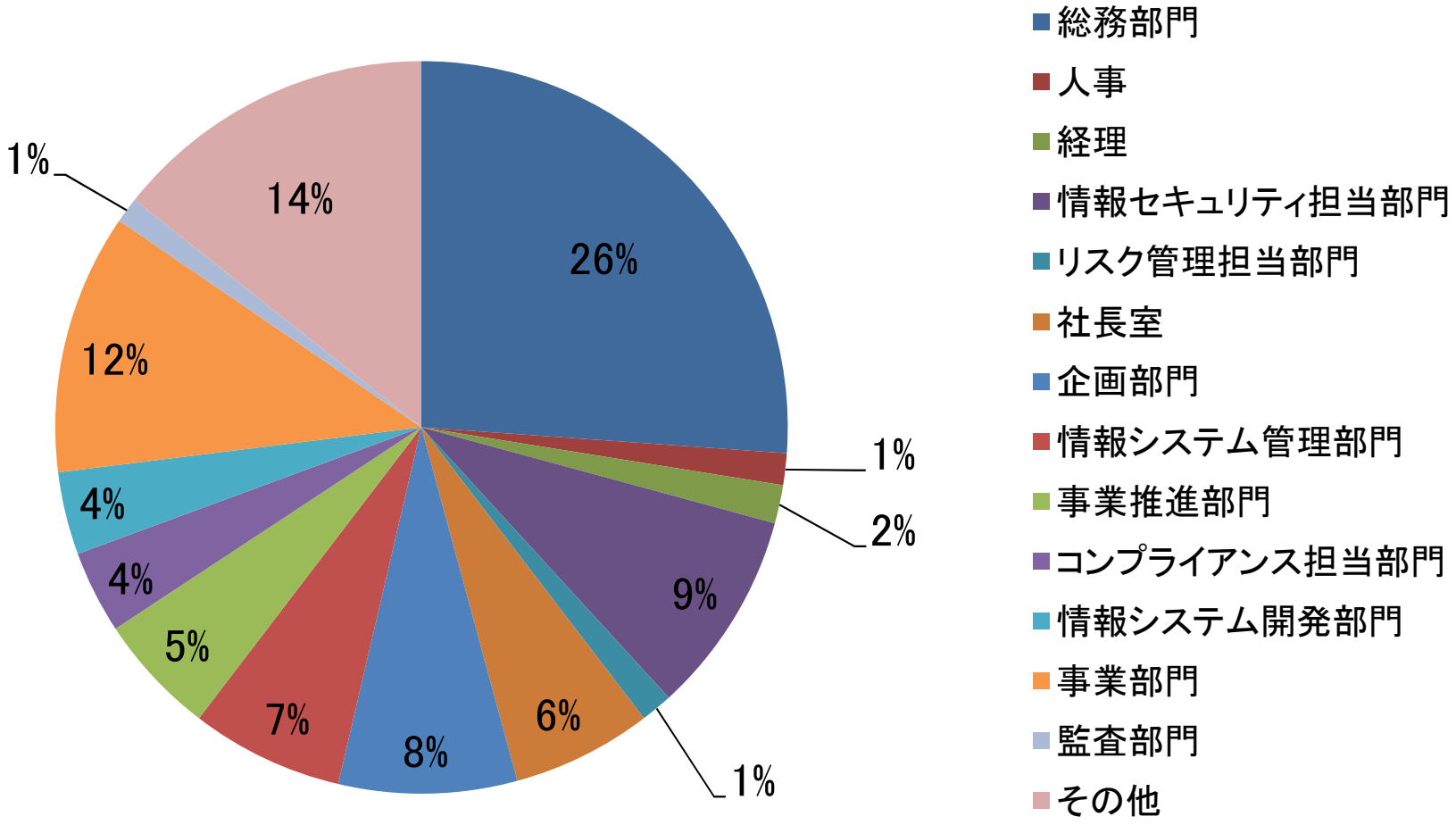
設問15.貴社の個人情報保護管理者の役職（N=361）



個人情報保護管理者は、会長・社長・取締役が多い。

第2章　プライバシーマーク取得状況について

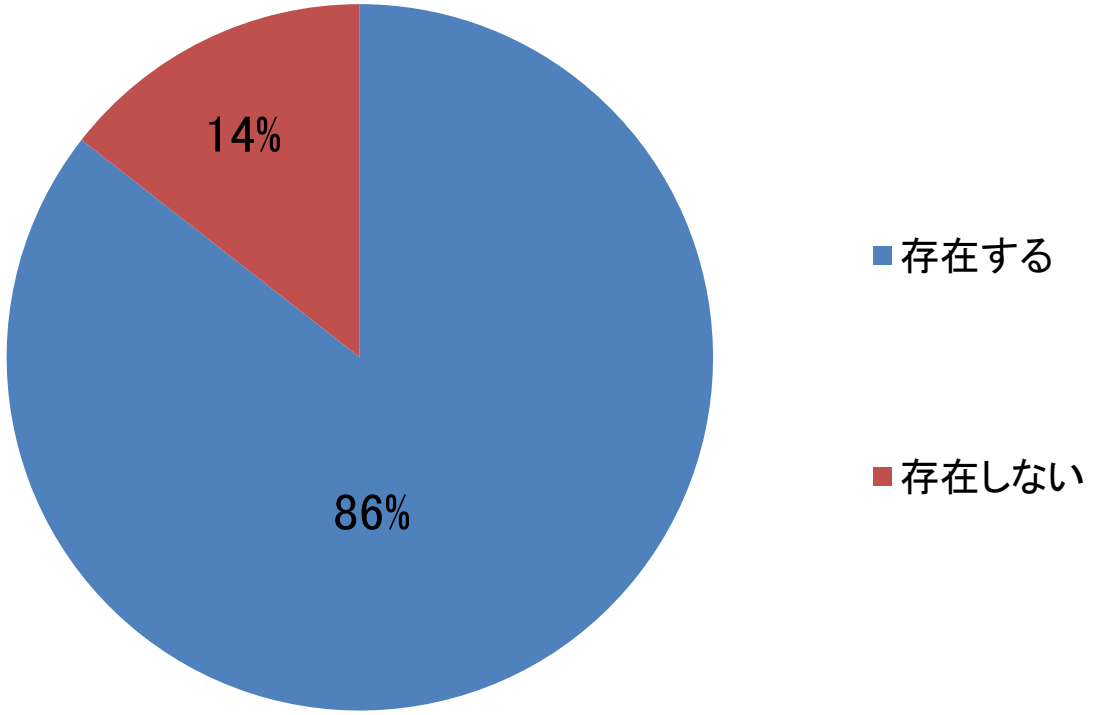
設問16.個人情報保護管理者の所属組織（N=355）



個人情報保護管理者の所属組織は、総務部門が最も多い。

第2章　プライバシーマーク取得状況について

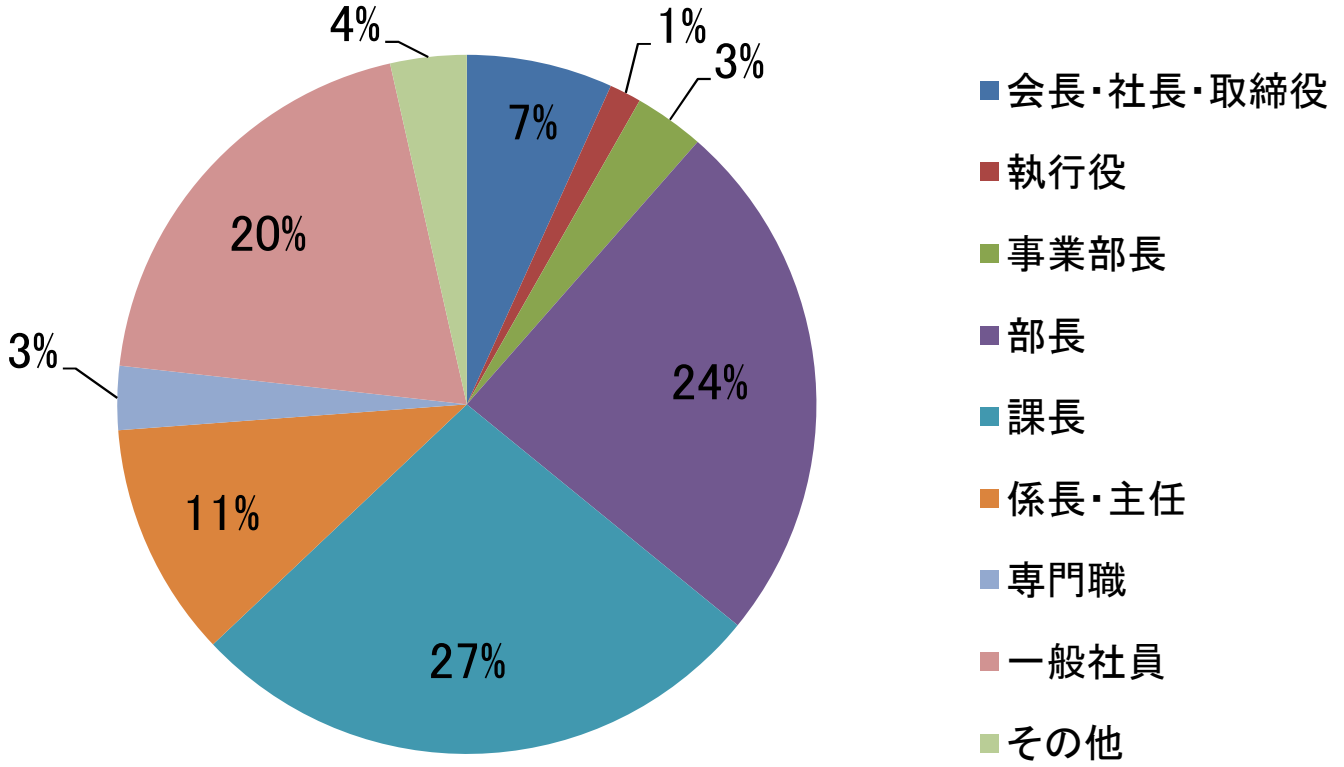
設問17.貴社には、現場で個人情報保護活動を推進する「個人情報保護担当者」が存在しますか。（N=353）



「個人情報保護担当者」が、現場の活動を推進している。

第2章　プライバシーマーク取得状況について

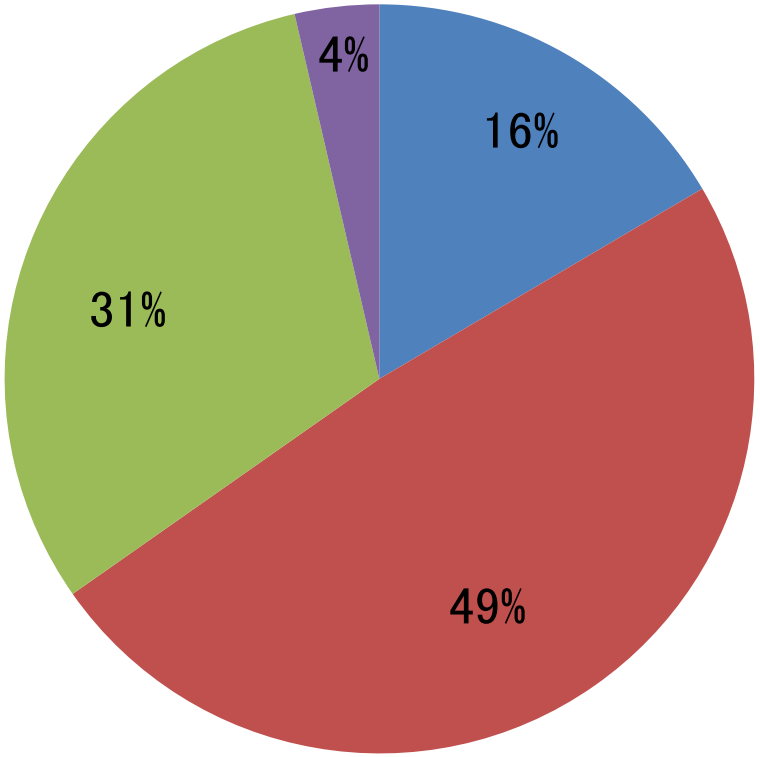
設問18.貴社の個人情報保護担当者の役職（多数存在する場合は、最も多い役職）（N=340）



個人情報保護担当者は、管理職（部長、課長）が担当している割合が高い。

第2章　プライバシーマーク取得状況について

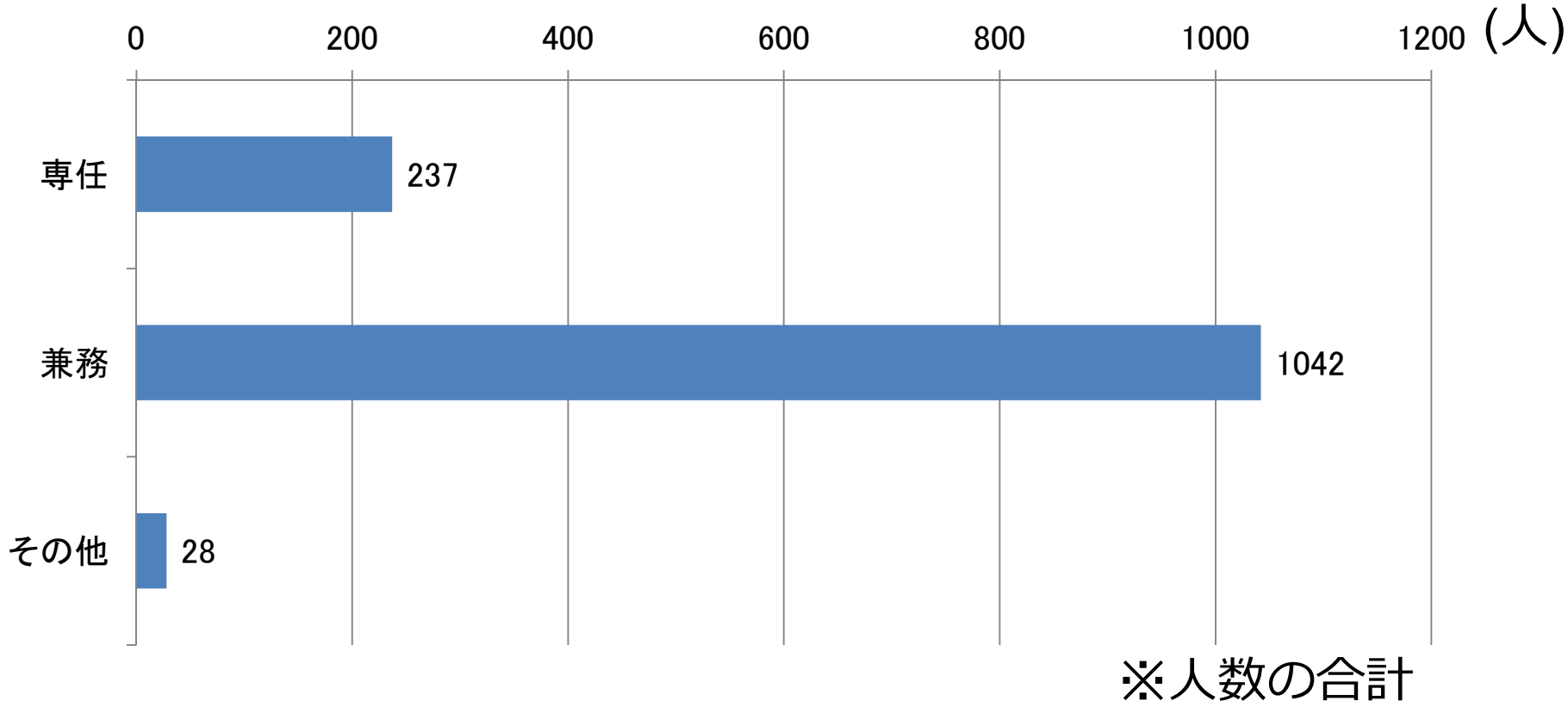
設問19.貴社ではプライバシーマーク事務局（以下「事務局」という。）メンバーをどの様に編成しましたか。（N=357）



既存組織の中で事務局メンバーを編成する事業者が、最も多い。

第2章　プライバシーマーク取得状況について

設問20.前回審査時の事務局のメンバーは何人ですか。(複数回答)
(N=337)

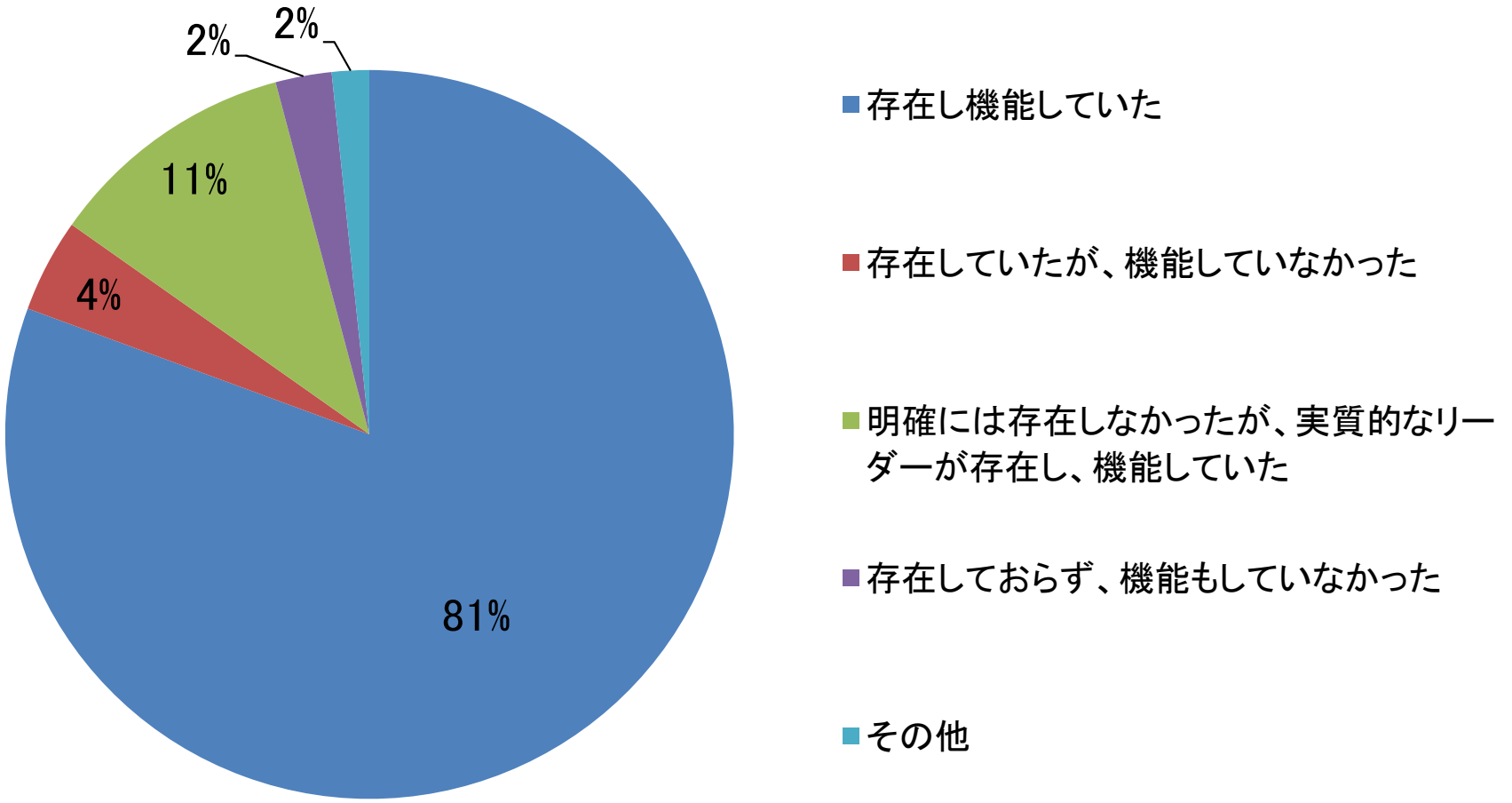


※人数の合計

事務局は、主に兼務のメンバーによって編成されている。

第2章　プライバシーマーク取得状況について

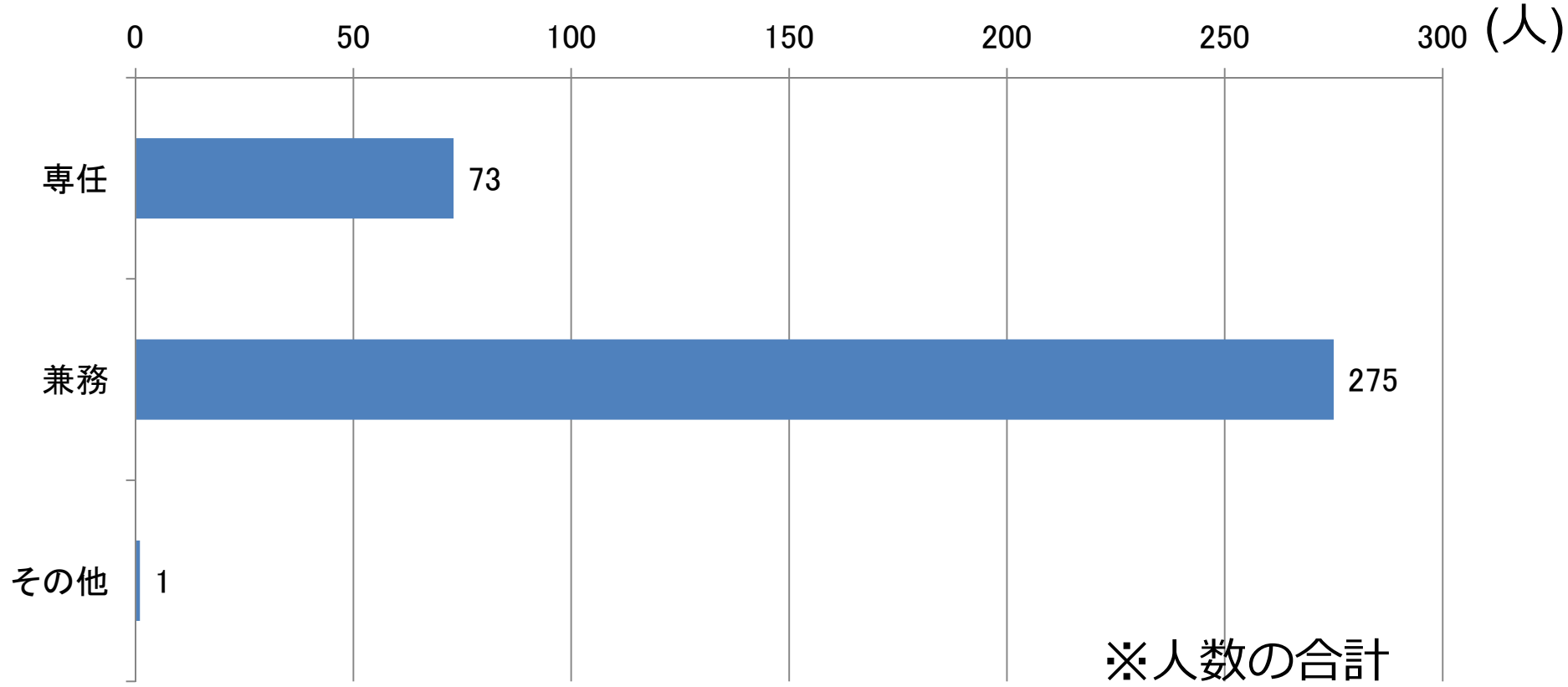
設問21.「事務局リーダー」が存在し、機能していましたか。（N=361）



事務局のリーダーを明示的に決め、機能させている事業者が多い。

第2章　プライバシーマーク取得状況について

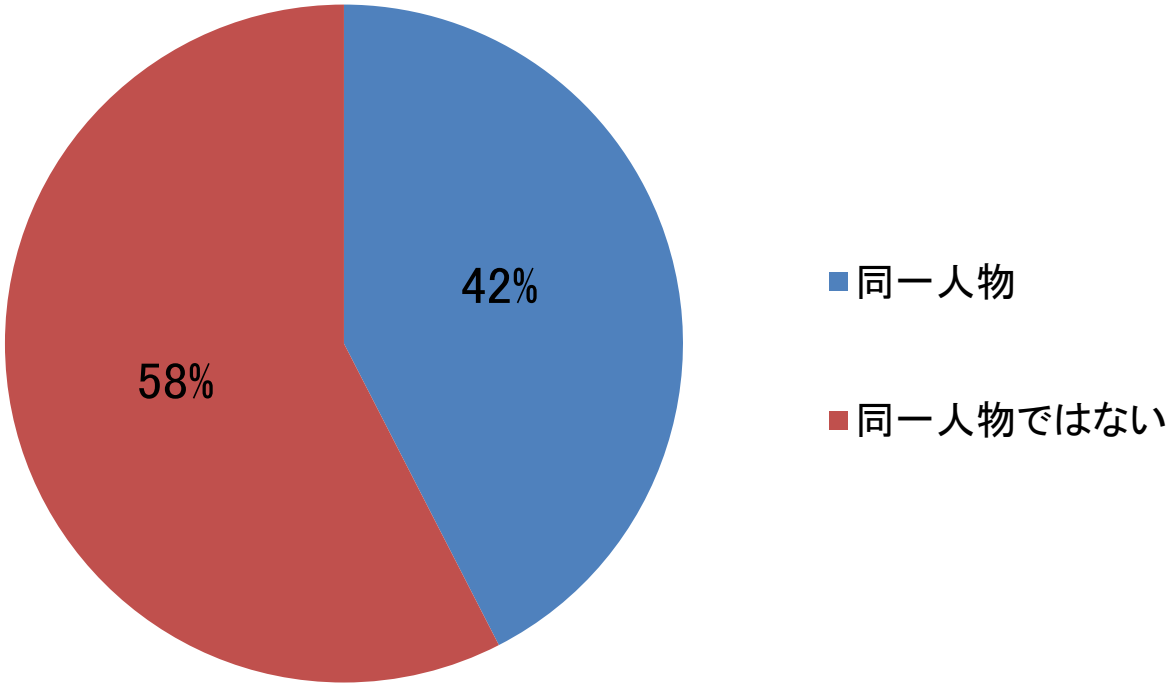
設問22.前回審査時、事務局リーダーはどの様に配置されていましたか。（N=361）



事務局のリーダーは、兼務で配置されていることが多い。

第2章　プライバシーマーク取得状況について

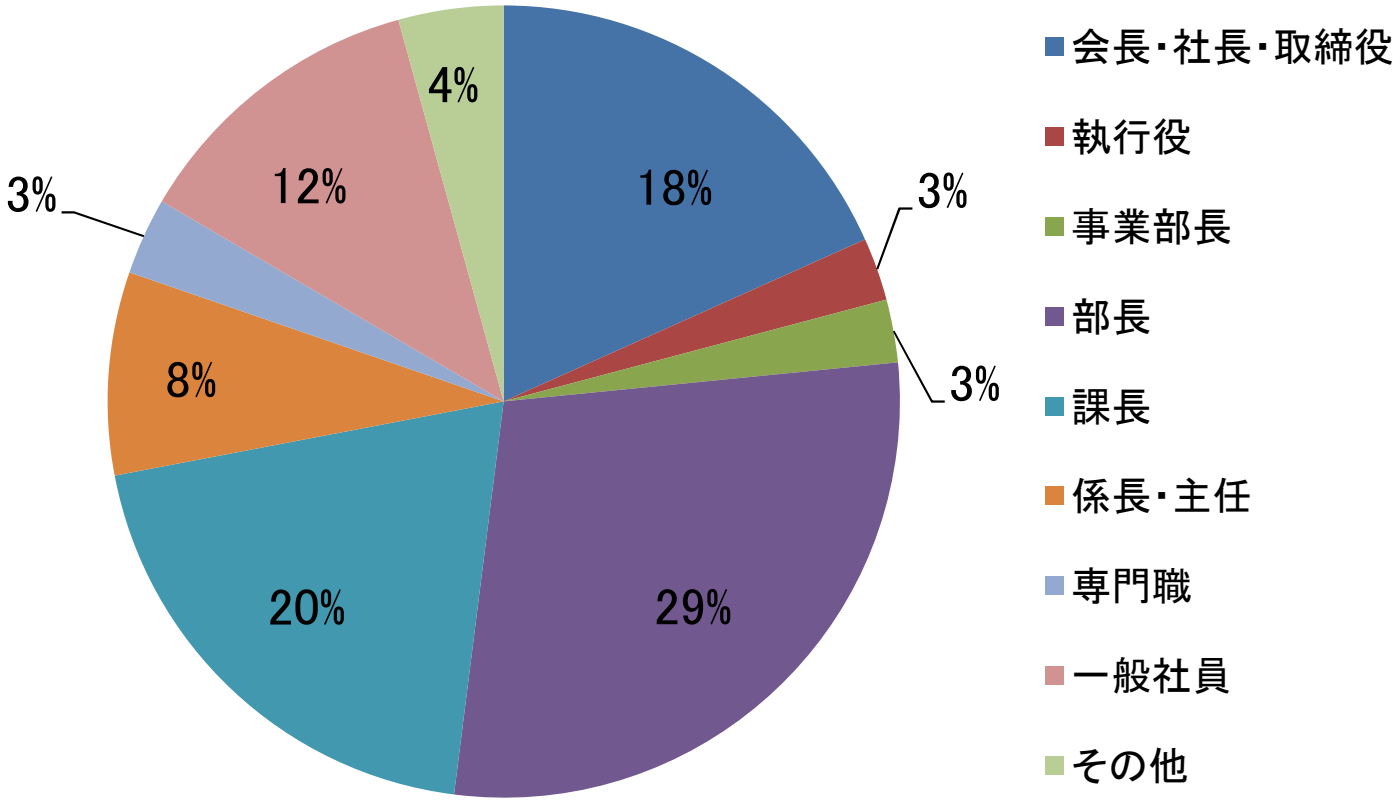
設問23.個人情報保護管理者と事務局リーダーは同一人物ですか。
（N=351）



個人情報保護管理者と事務局リーダーは、
同一では無い割合の方が若干高い。

第2章　プライバシーマーク取得状況について

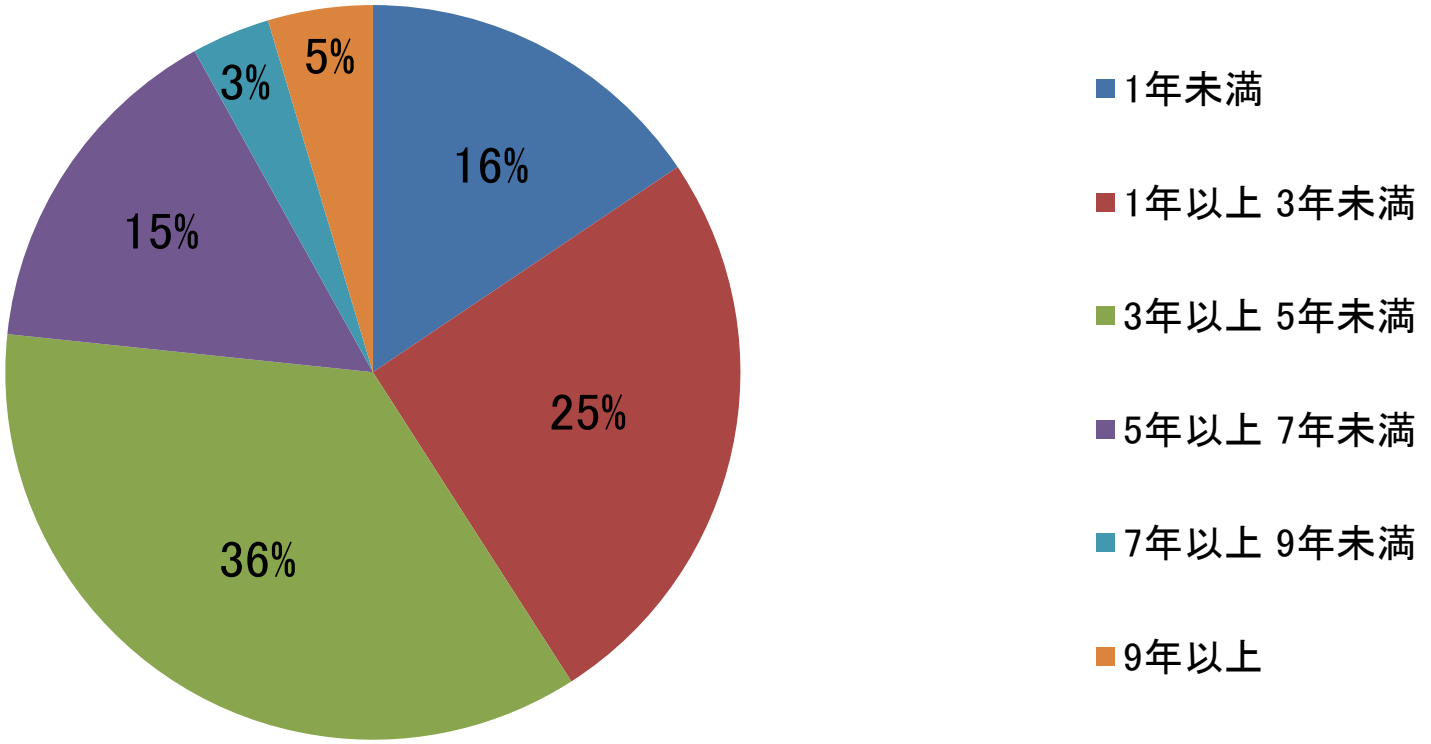
設問24.前回審査時の事務局リーダーの役職（N=350）



事務局リーダーは、管理職（部長、課長）が担当している割合が高い。

第2章　プライバシーマーク取得状況について

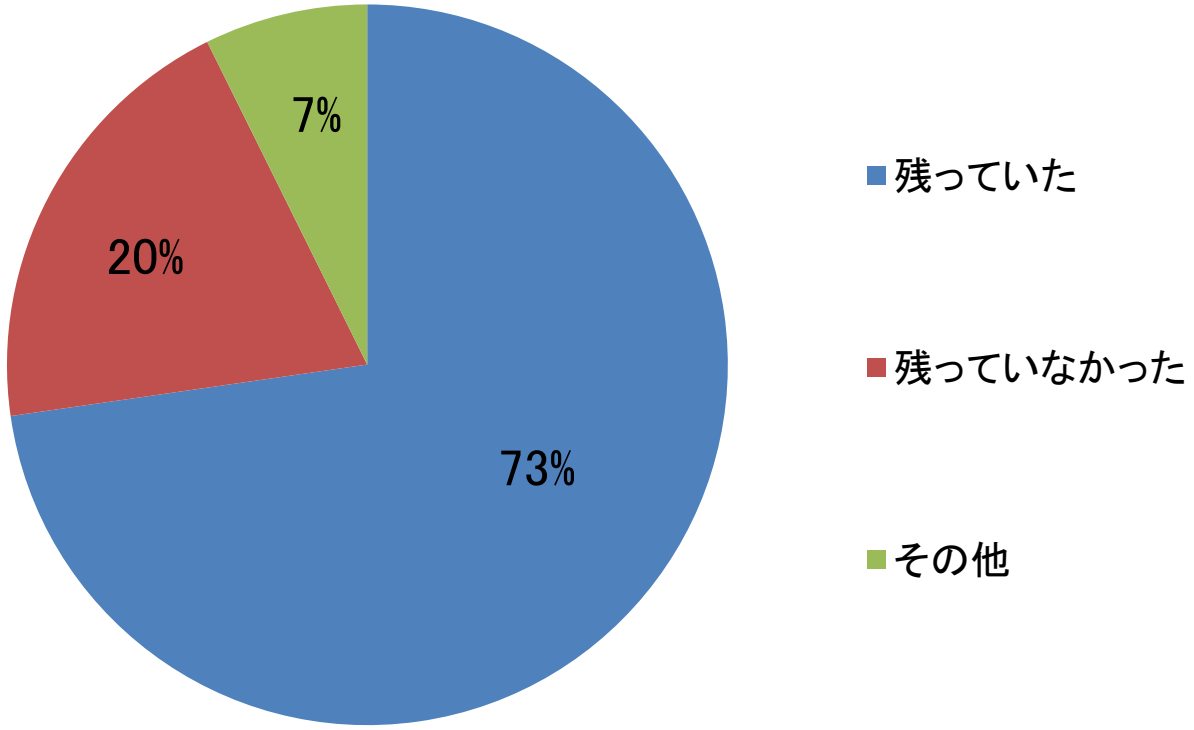
設問25.前回審査時の事務局リーダーのプライバシーマーク認証業務に関するご経験年数（N=347）



事務局リーダーが認証業務に、複数年の経験を有している事業者が、6割～8割程度を占めている。

第2章　プライバシーマーク取得状況について

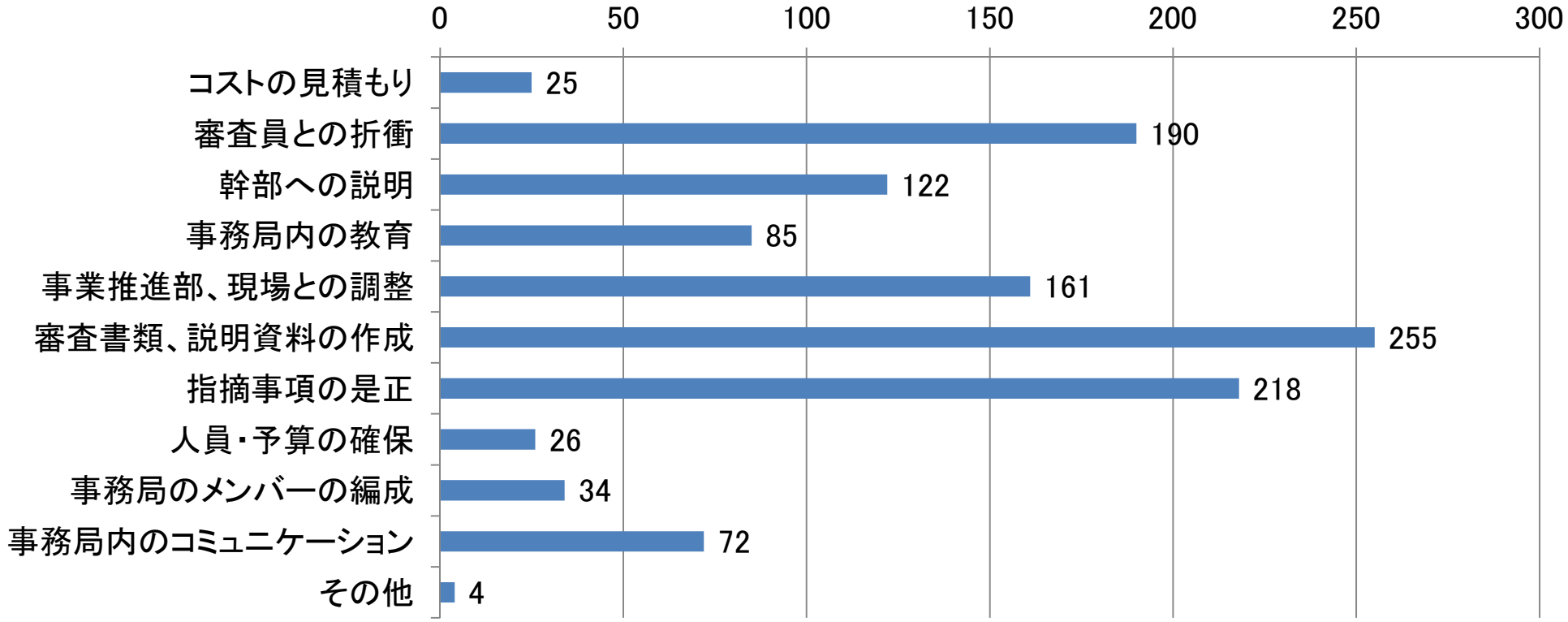
設問26.前回審査時に、初回認証取得の際の事務局リーダーが事務局に残っていましたか。（N=341）



事務局リーダーは、初回認証取得の時から継続して、
プライバシーマーク取得業務に携わっている割合が高い。

第2章　プライバシーマーク取得状況について

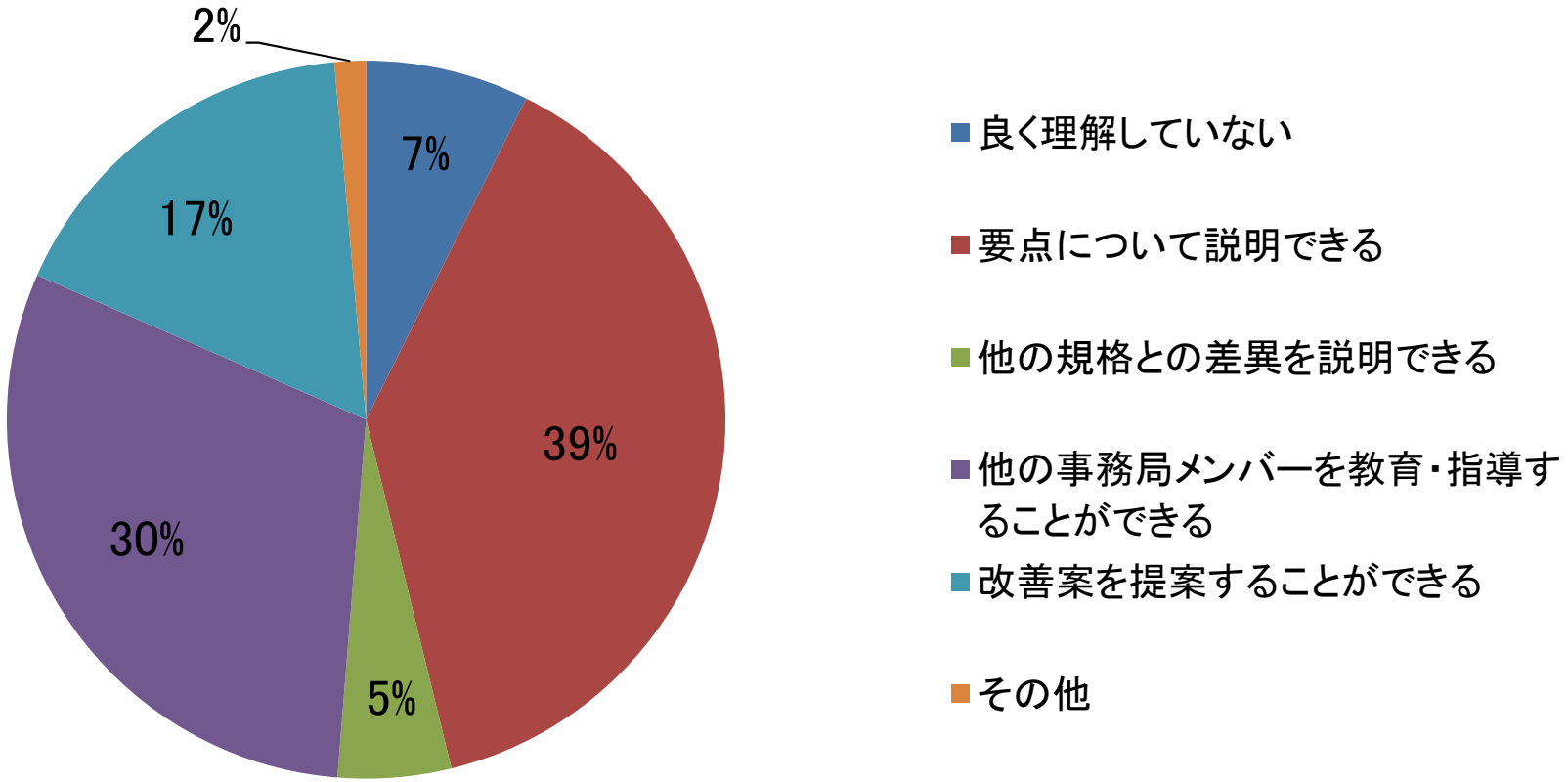
設問27.前回審査時において、事務局リーダーが主体的に取り組んだ業務は何でしたか。（複数回答）（N=349）



事務局リーダーは自らの経験を生かし、資料作成や指摘事項の是正に取り組む他、事務局外とのコミュニケーションを主体的に行なっている。

第2章　プライバシーマーク取得状況について

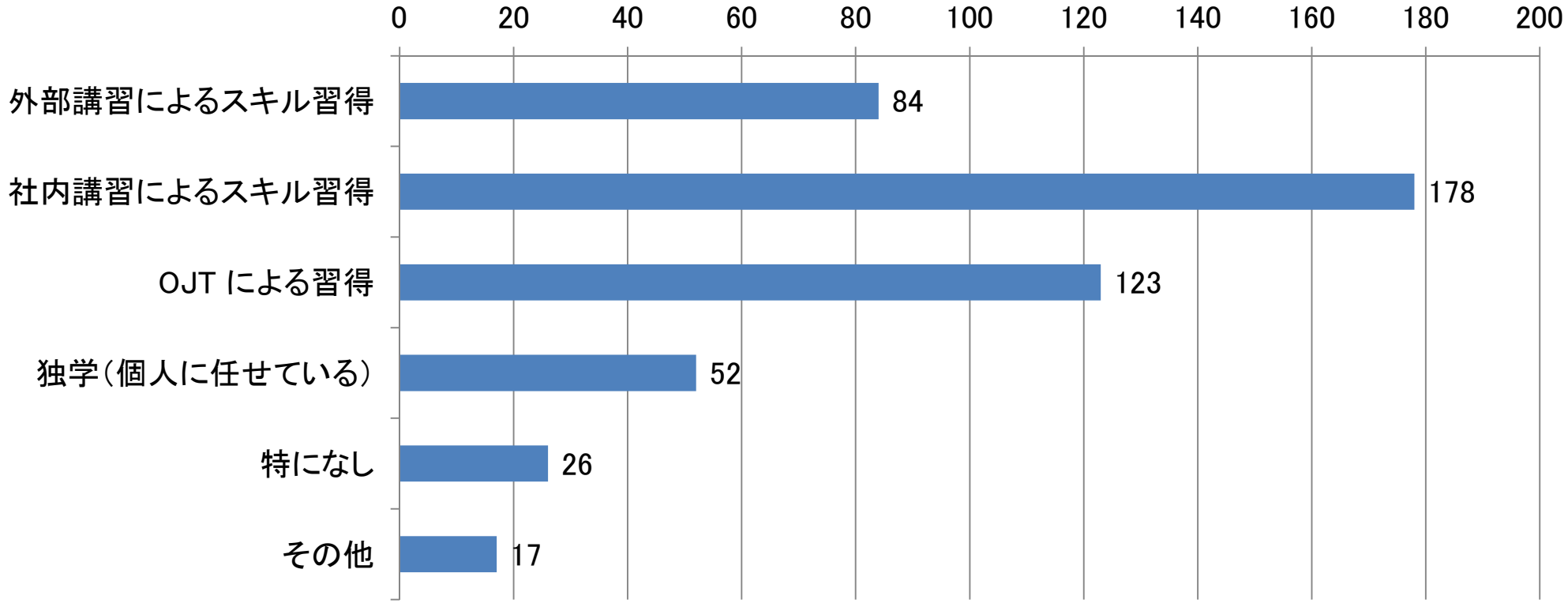
設問28.前回審査時において、事務局リーダーのJISQ15001 の理解度は如何でしたか。（N=353）



JISQ15001について、
他の事務局メンバーを教育指導できる事務局リーダーは、3割程度。

第2章　プライバシーマーク取得状況について

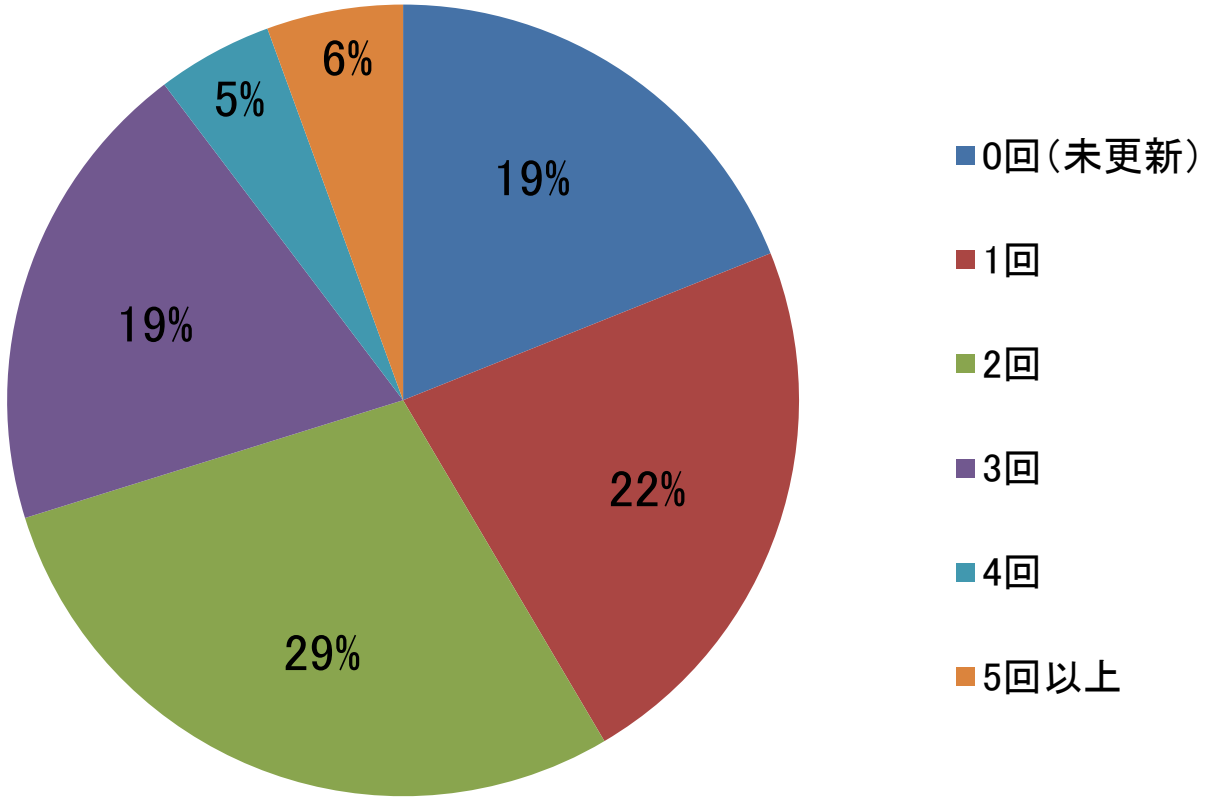
設問29.事務局の新しいメンバーに対して、どのような形でプライバシーマークに関連したスキル習得を行いましたか。（複数回答）
（N=356）



事務局メンバーへの教育は、社内講習、OJTの順に割合が高い。

第2章　プライバシーマーク取得状況について

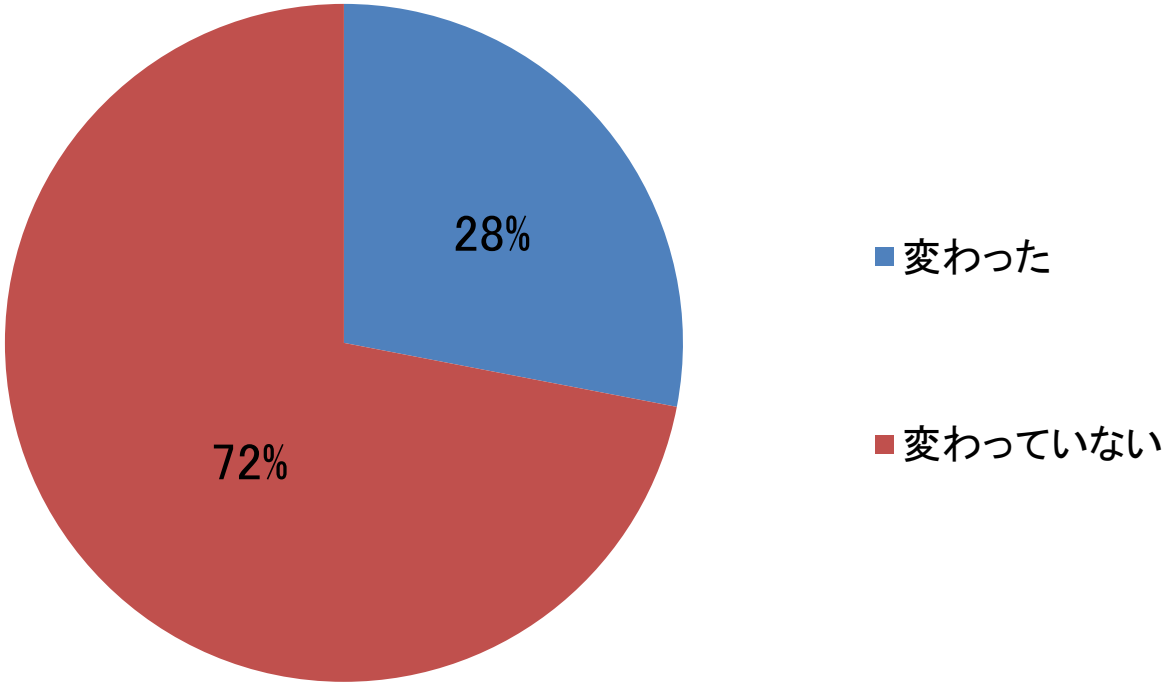
設問30.貴社はプライバシーマークを何回更新していますか。
（N=359）



1回以上更新した経験を持つ事業者が、約9割程度を占めている。

第2章　プライバシーマーク取得状況について

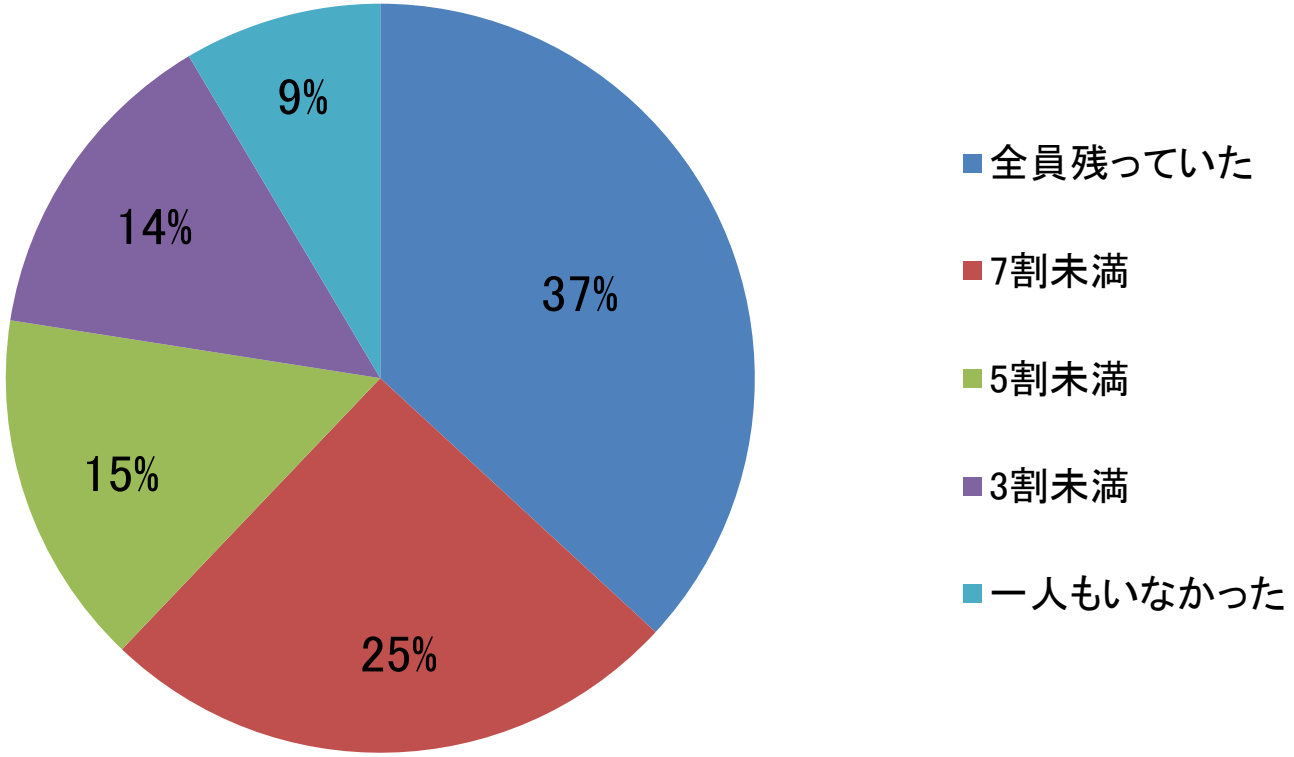
設問31.事務局リーダーは前々回更新時と前回更新時で変わりましたか。（N=289）



事務局リーダーの交代は頻繁ではなく、
更新業務に継続して取り組む傾向が見られる。

第2章　プライバシーマーク取得状況について

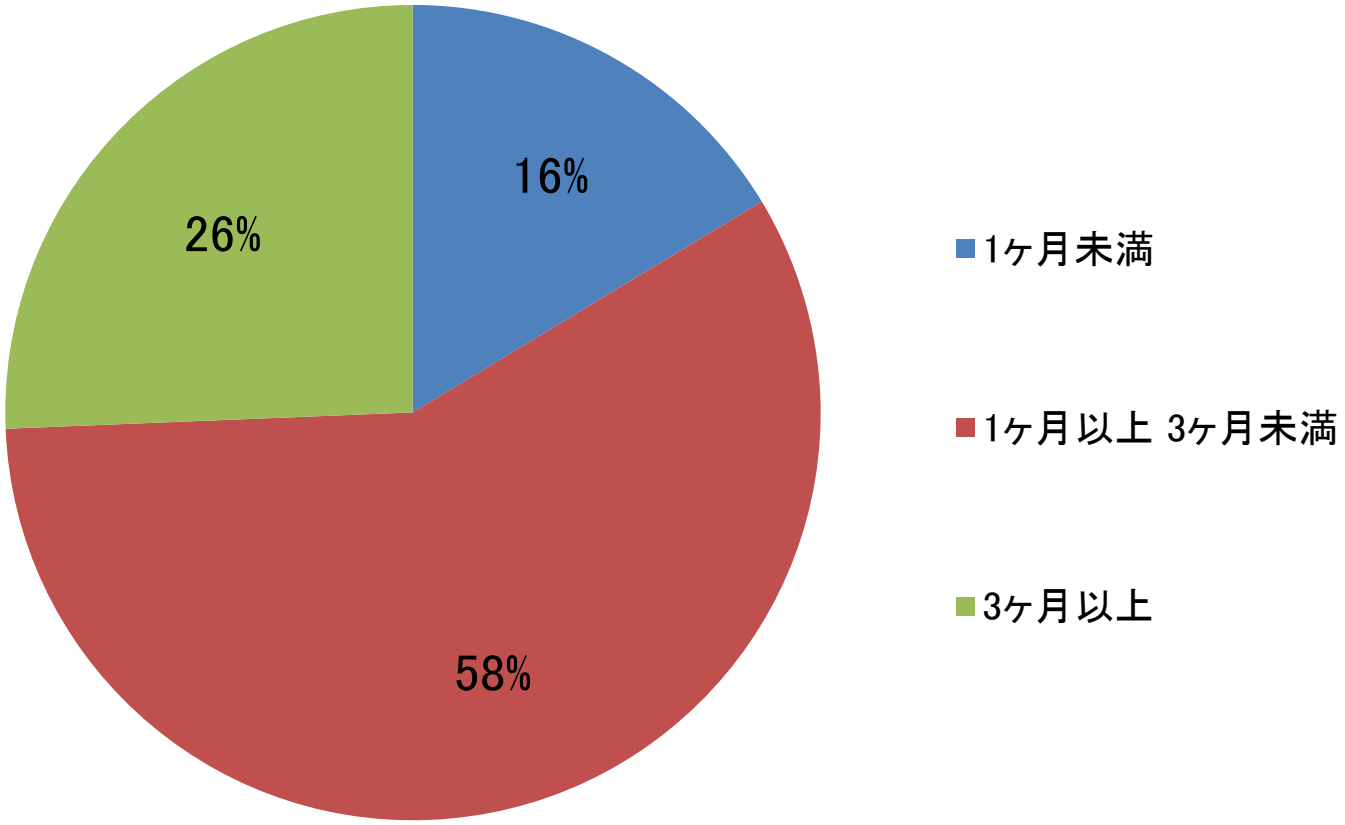
設問32.前回審査時、初回認証取得の際のメンバーが、どのくらいの割合で残っていましたか。(N=293)



プライバシーマーク事務局メンバーの入れ替わり頻度は低い。

第2章　プライバシーマーク取得状況について

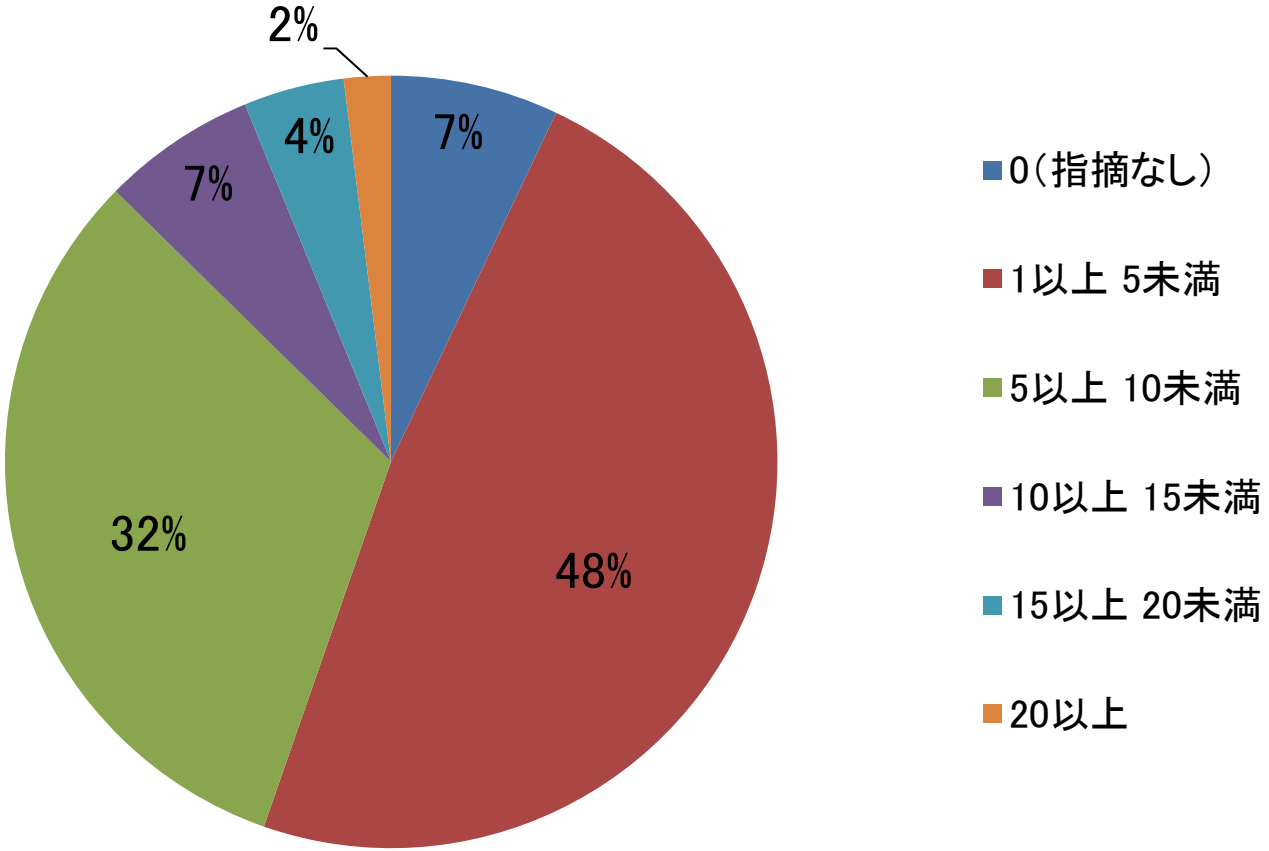
設問33.前回審査時、審査必要書類を送付するための準備期間
（N=355）



全体の3割程度が、書類の送付に3ヶ月以上かかっている。

第2章　プライバシーマーク取得状況について

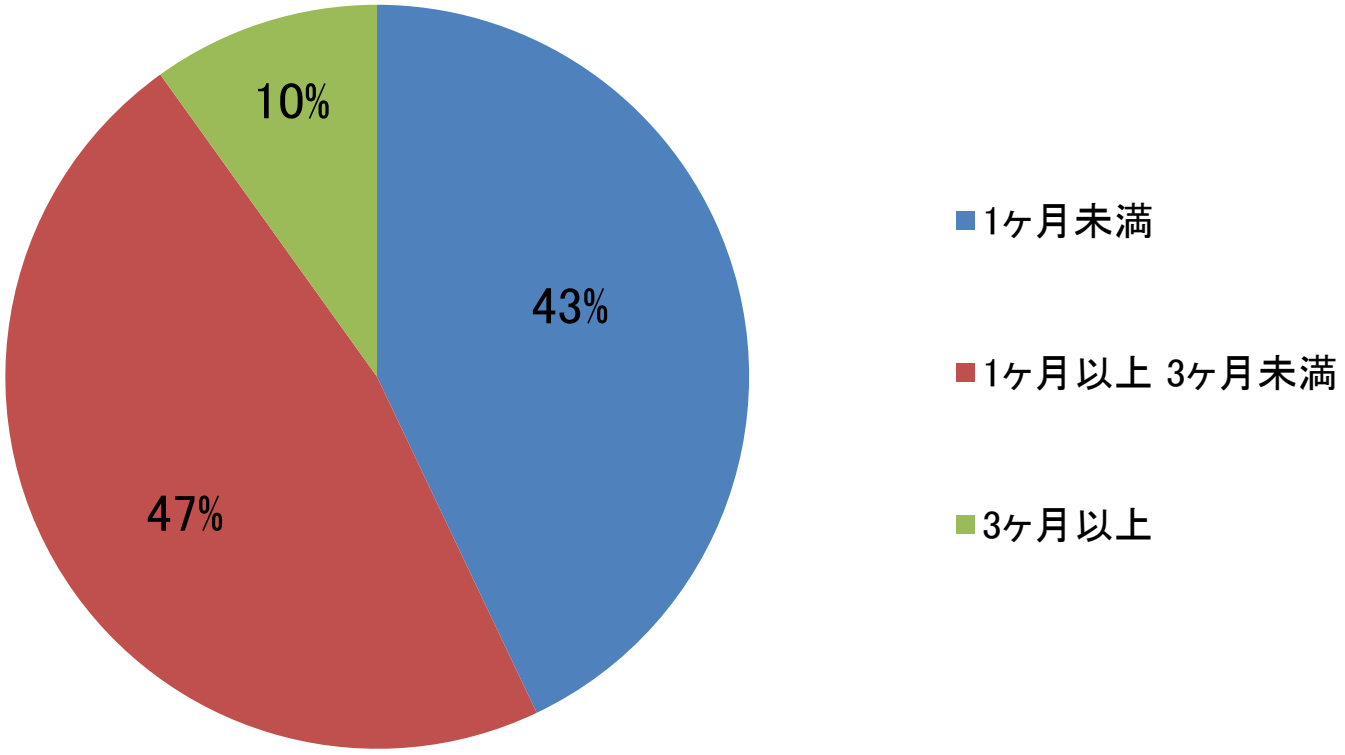
設問34.前回審査時、現地審査での指摘事項数はいくつでしたか。
（N=356）



指摘事項数が5以上の事業者が4割程度を占めている。

第2章　プライバシーマーク取得状況について

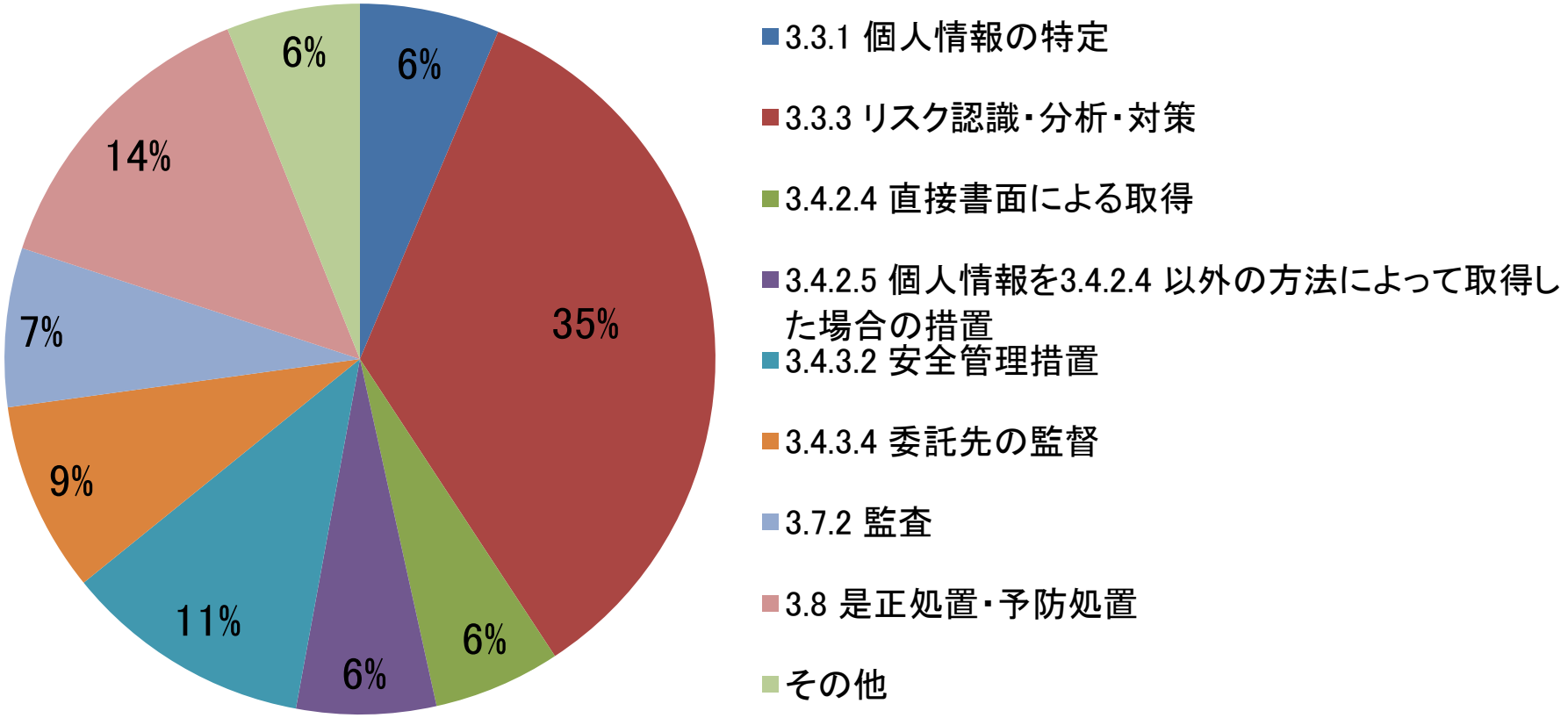
設問35.前回審査時、指摘事項を全て是正するまでにかかった期間（N=333）



全体の1割程度が、指摘事項の是正に3ヶ月程以上かかっている。

第2章　プライバシーマーク取得状況について

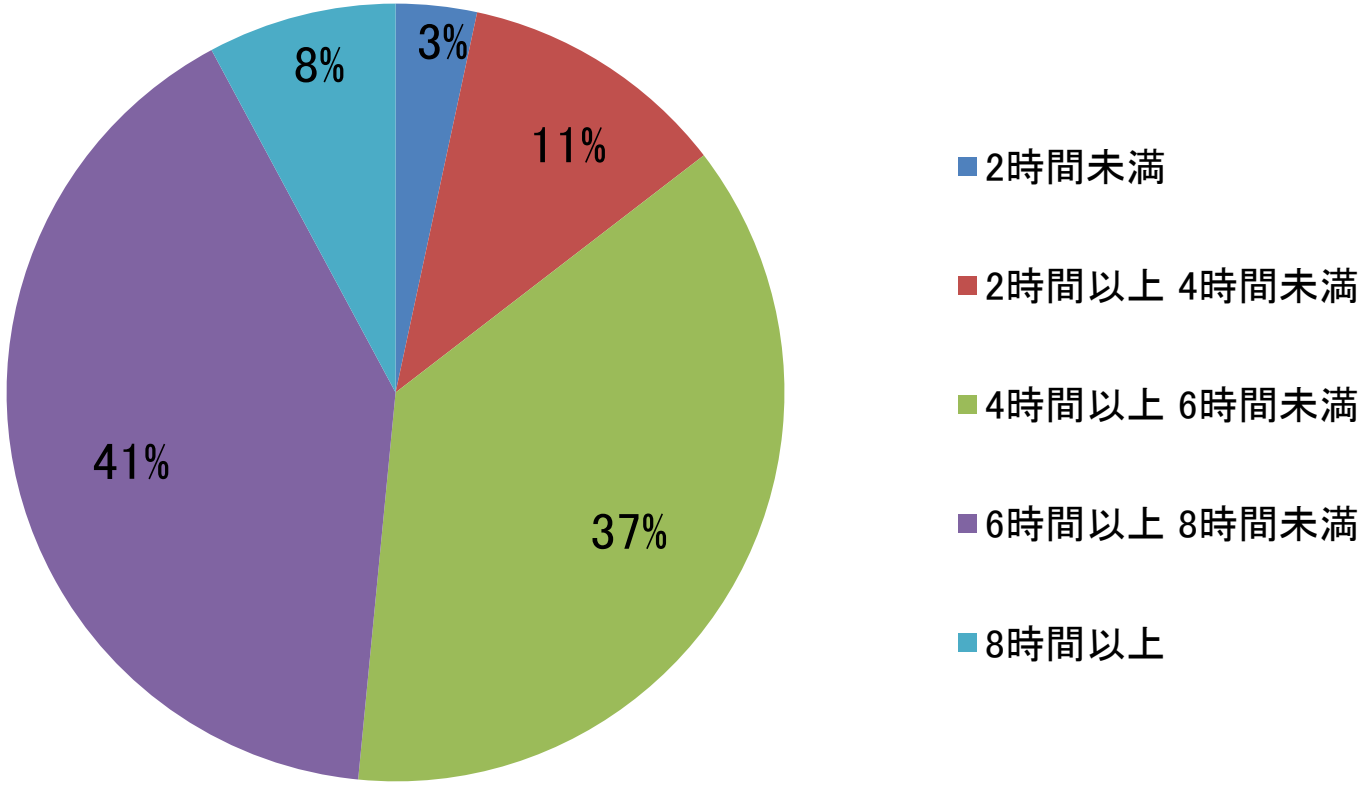
設問36.前回審査時、是正に最も時間を要した要求事項は、次の内どれですか。（N=346）



「3.3.3 リスク認識・分析・対策」の是正に時間を要する事業者が多い。

第2章　プライバシーマーク取得状況について

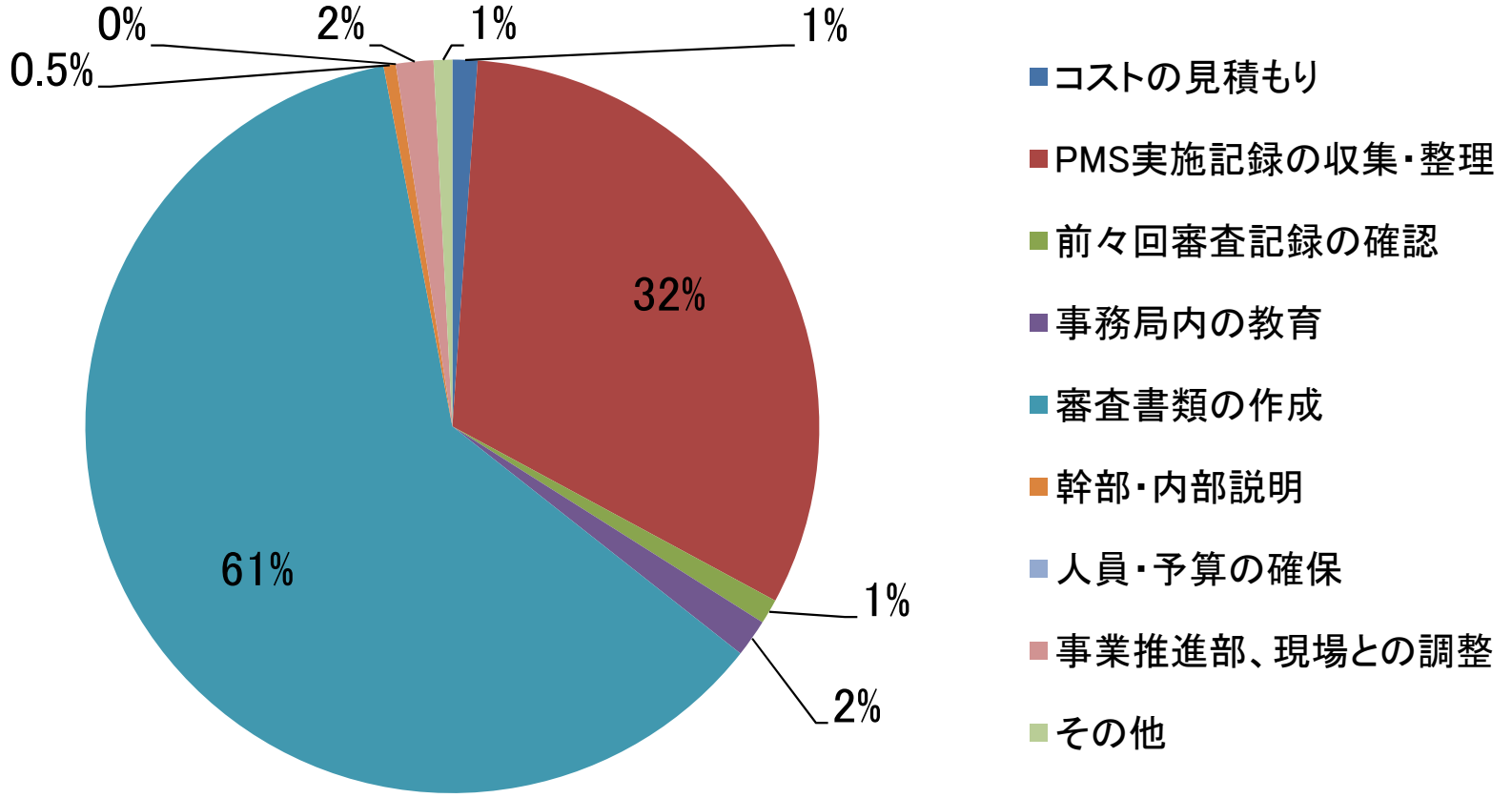
設問37.前回審査時、現地審査にかかった時間は何時間ですか。
（N=357）



全体の3割程度が、現地審査に8時間以上を要している。

第2章　プライバシーマーク取得状況について

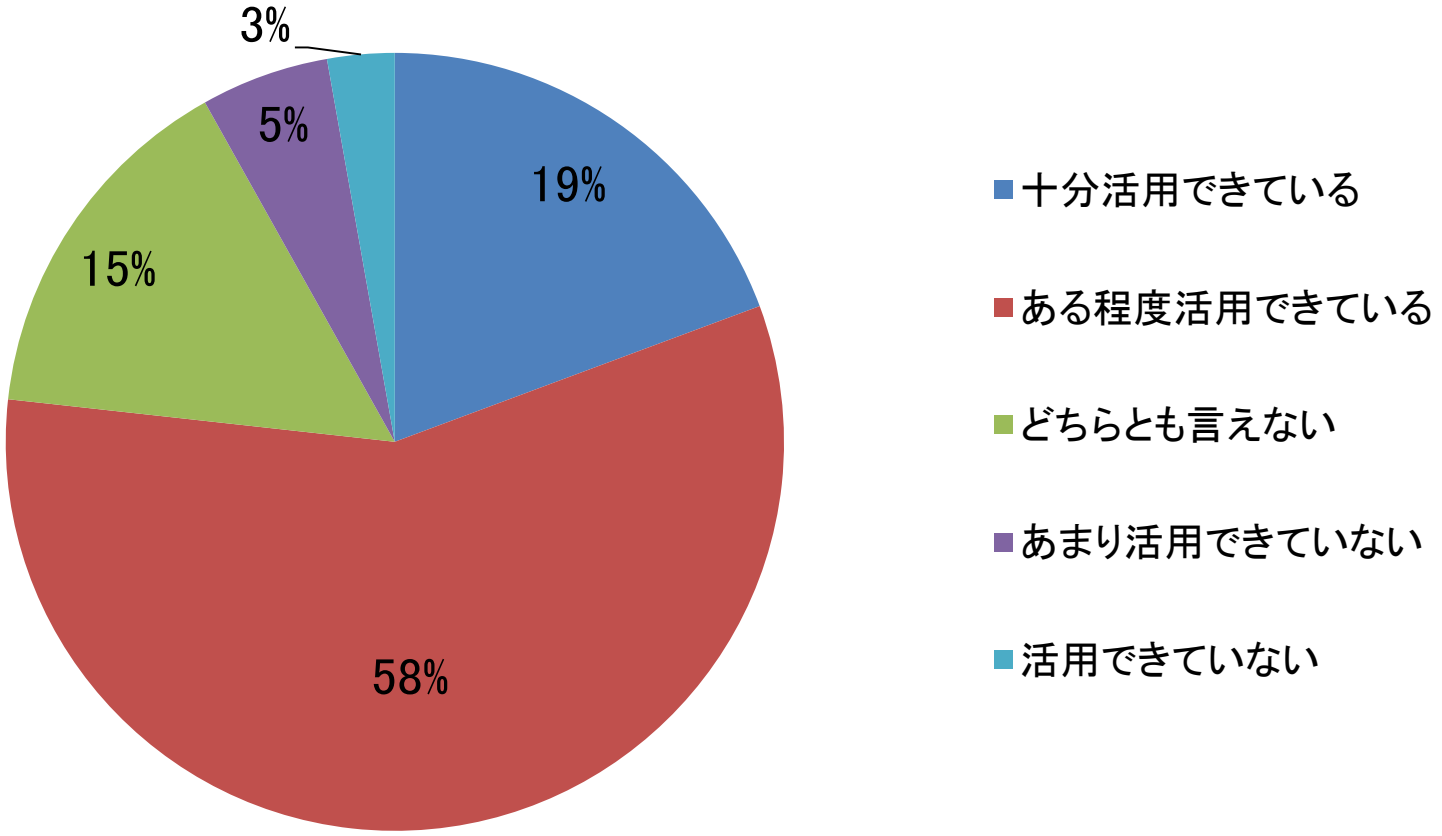
設問38.前回審査時に、審査必要書類を送付するための準備作業の中で、最も時間を要した作業。（N=365）



書類の作成と記録の収集・整理に時間を要する事業者が多い。

第2章　プライバシーマーク取得状況について

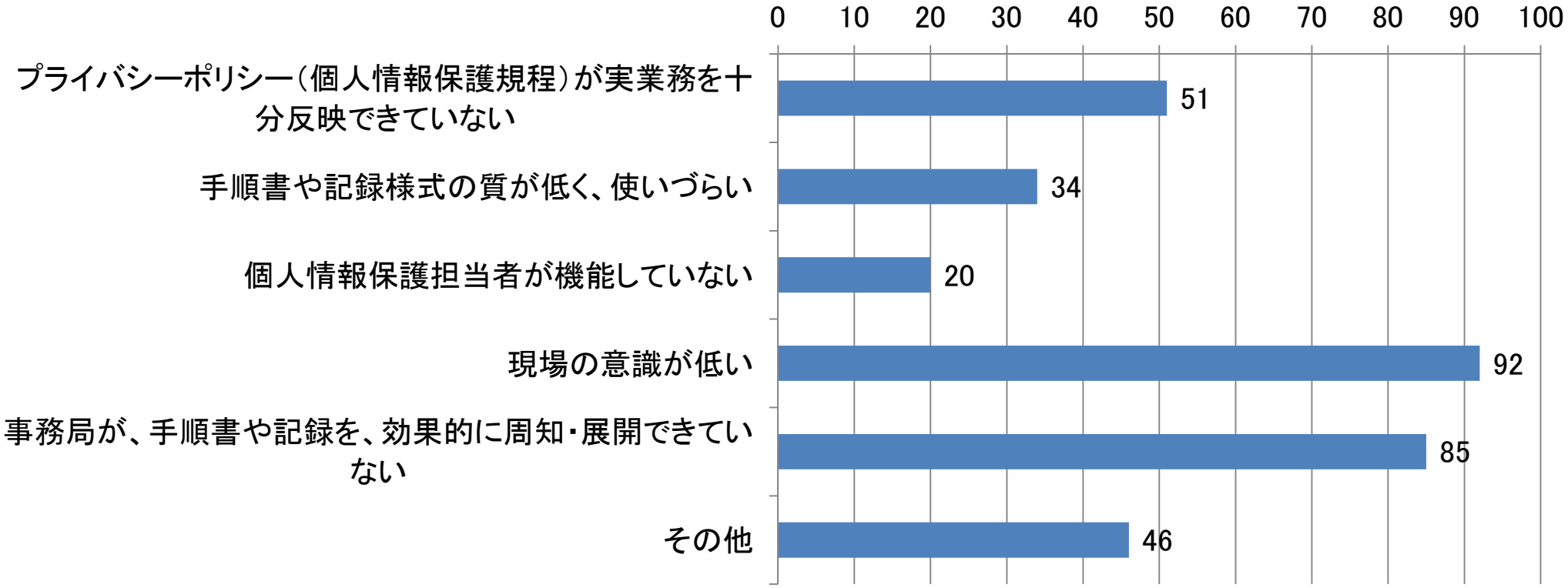
設問39.貴社において、個人情報保護関連の記録類や手順書を、現場で十分活用できていますか。(N=357)



記録類や手順書を現場で十分活用できている事業者は、
2割以下に留まった。

第2章　プライバシーマーク取得状況について

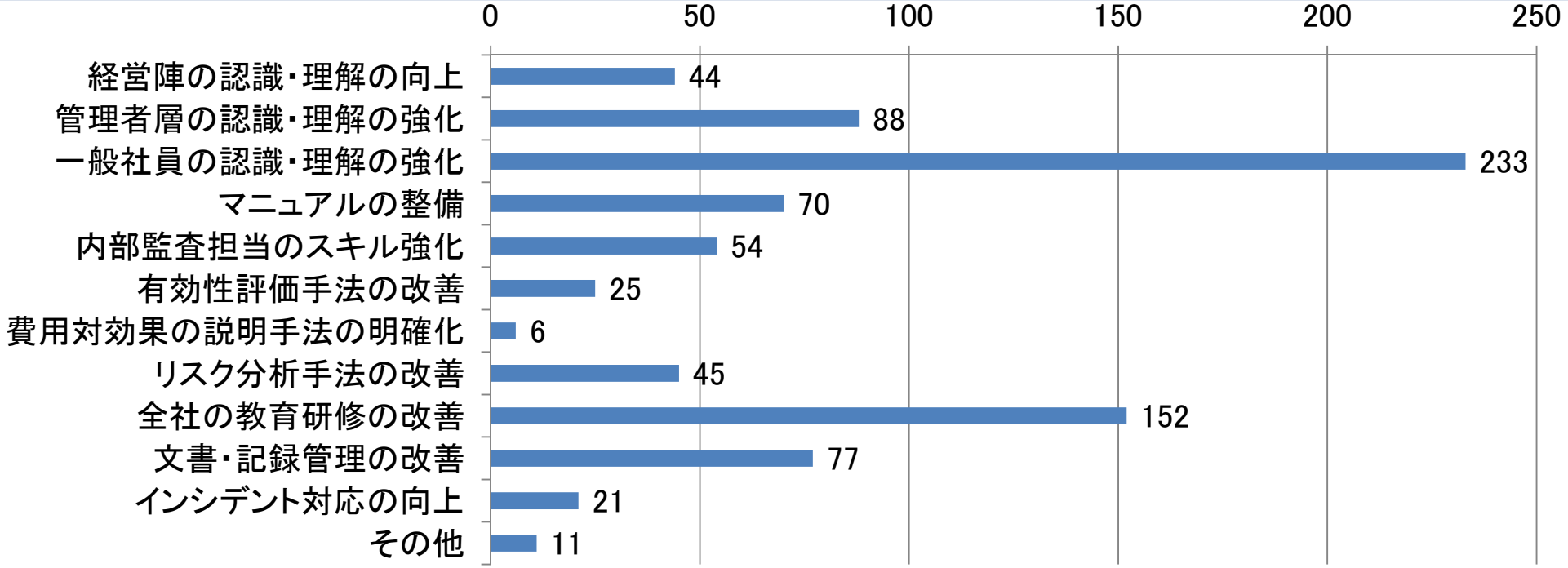
設問40.個人情報保護関連の記録類や手順書を、現場で十分活用できていない原因として何が考えられますか。（複数回答）（N=272）



記録類や手順書が現場で十分活用できない原因として、「事務局が効果的に現場へ展開できていない」「現場の意識が低い」を挙げる事業者が多い。

第2章　プライバシーマーク取得状況について

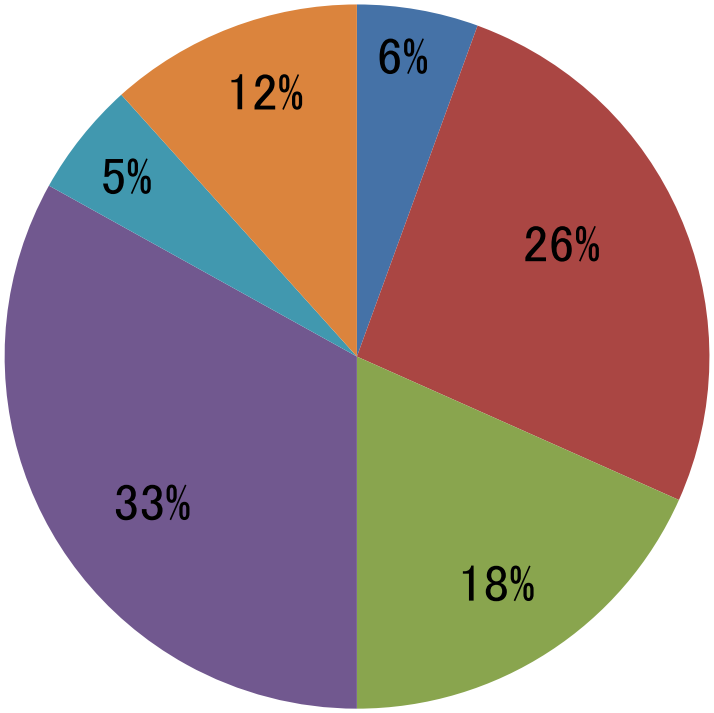
設問41.貴社において、プライバシーマークの効果を高めるために重点的に取り組んでいるもの、あるいは取り組む予定のあるものをお答えください。（複数回答）（N=354）



プライバシーマークの効果を高めるための施策として、「全社の教育研修」「一般社員の認識・理解の強化」を重要視している事業者が多い。

第2章　プライバシーマーク取得状況について

設問42.「3.3.3 個人情報のリスク認識、分析、対策」について、「個人情報の取り扱いの各局面におけるリスクを認識し、分析し、必要な対策を講じる手順の確立、維持」をするための取り組み状況は如何ですか。（N=360）

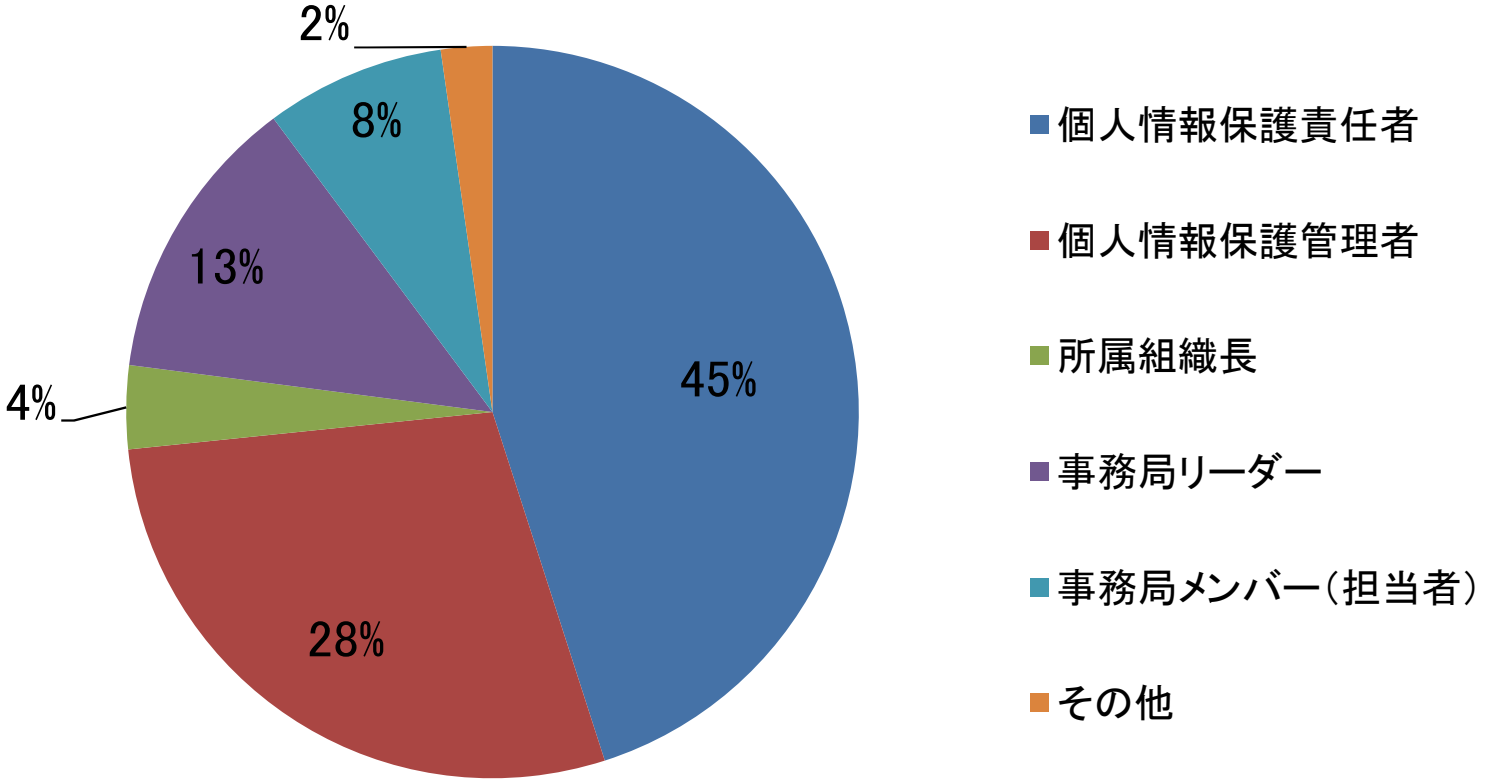


- 個人的な範囲で取り組んでいる
- 事務局内のみで取り組んでいる
- 各部署で個別に取り組んでいる
- 現場も含め、全組織で取り組んでいる
- 取り組み状況をモニタリングし、基準から逸脱しない様、全組織で取り組んでいる
- 取り組み状況をモニタリングし、基準から逸脱しない様、全組織で取り組むと共に、継続的な改善を実施している

取り組み状況のモニタリングまで実施できている事業者は、
全体の2割以下に留まった。

第2章　プライバシーマーク取得状況について

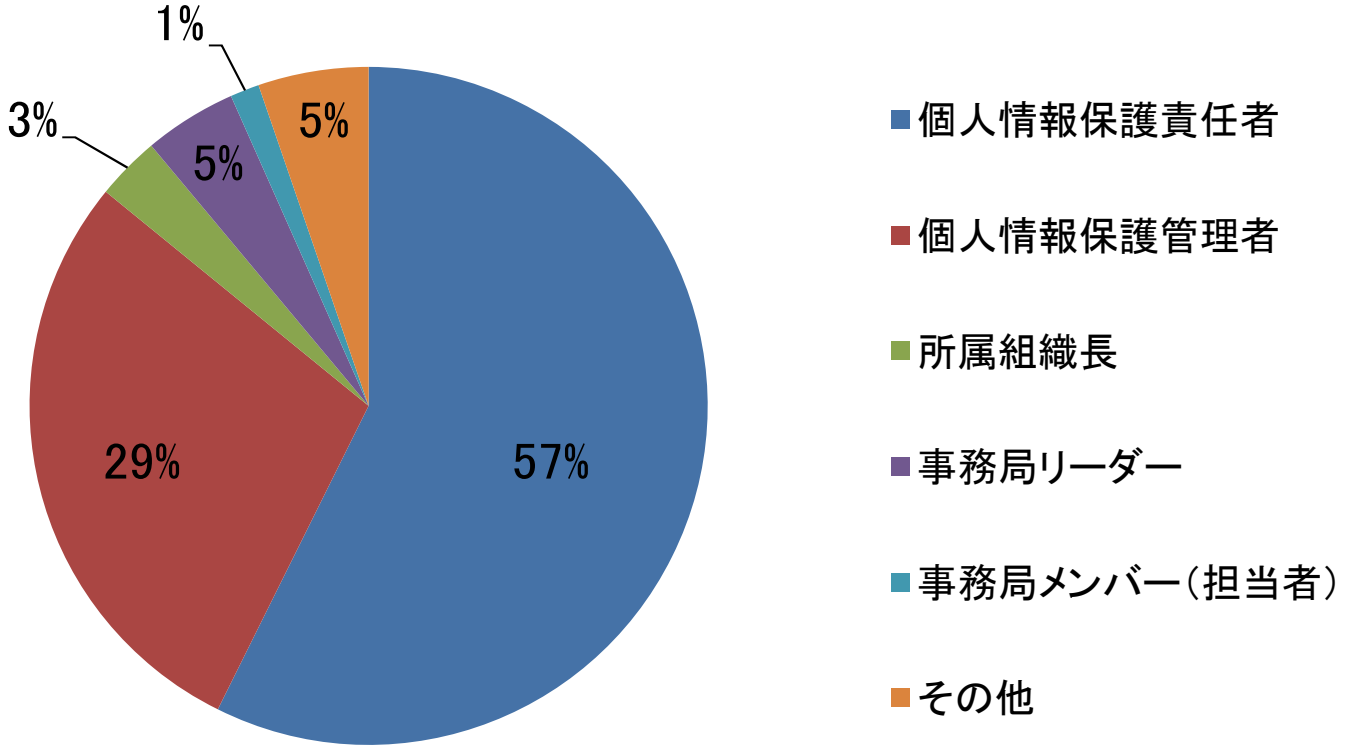
設問43.事務局が、個人情報保護関連施策を現場に展開する際、誰の名前で依頼を実施していますか。（N=353）



「個人情報保護責任者」「個人情報保護管理者」といった、JISQ15001で定義されている公式な役割名によって、施策が展開されている事業者が多い。

第2章　プライバシーマーク取得状況について

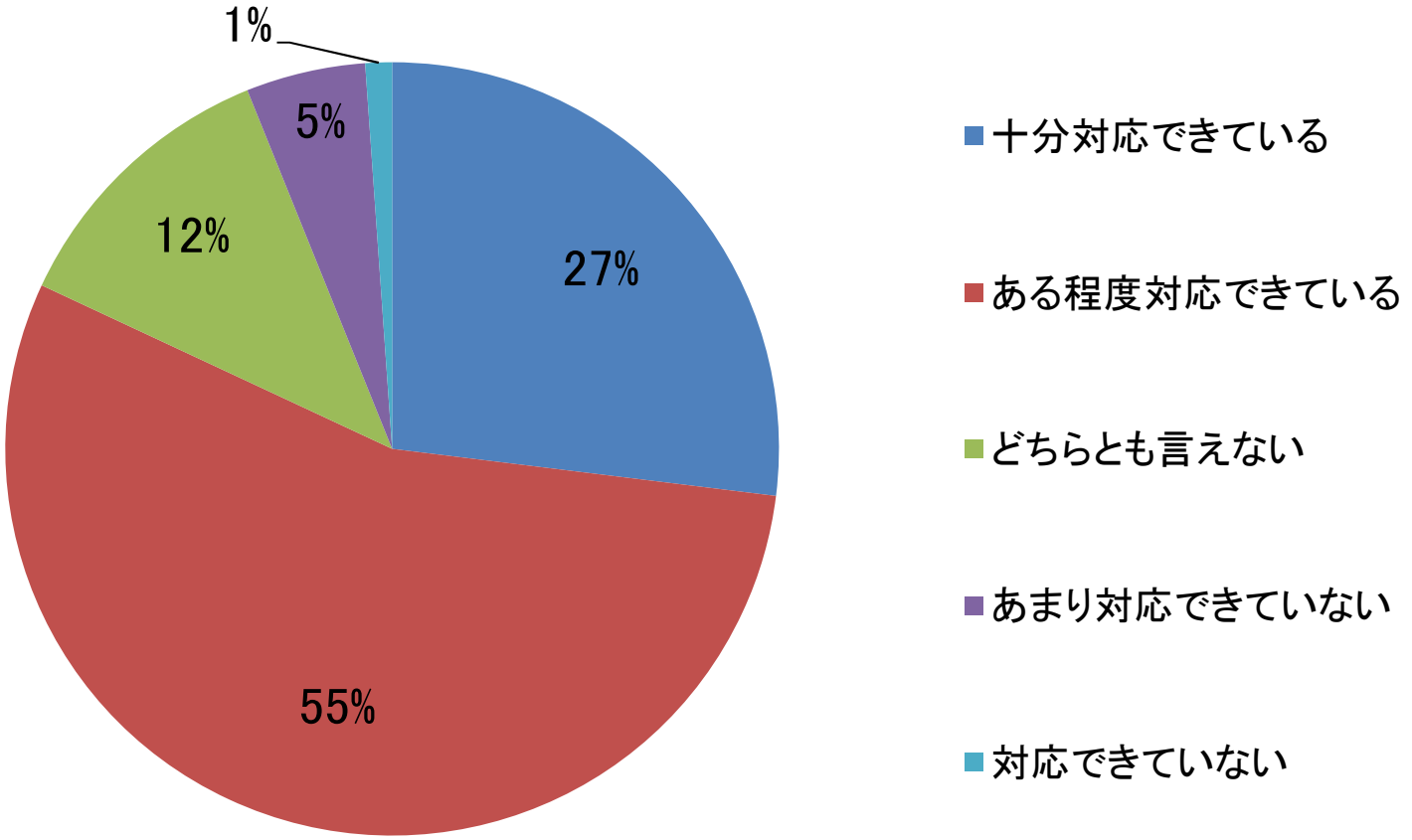
設問44.貴社では、誰が、個人情報保護施策の決定権を持っていますか。(N=361)



「個人情報保護責任者」「個人情報保護管理者」といった、JISQ15001で定義されている公式の役割を持つ人物が決定権を持っている事業者が多い。

第2章　プライバシーマーク取得状況について

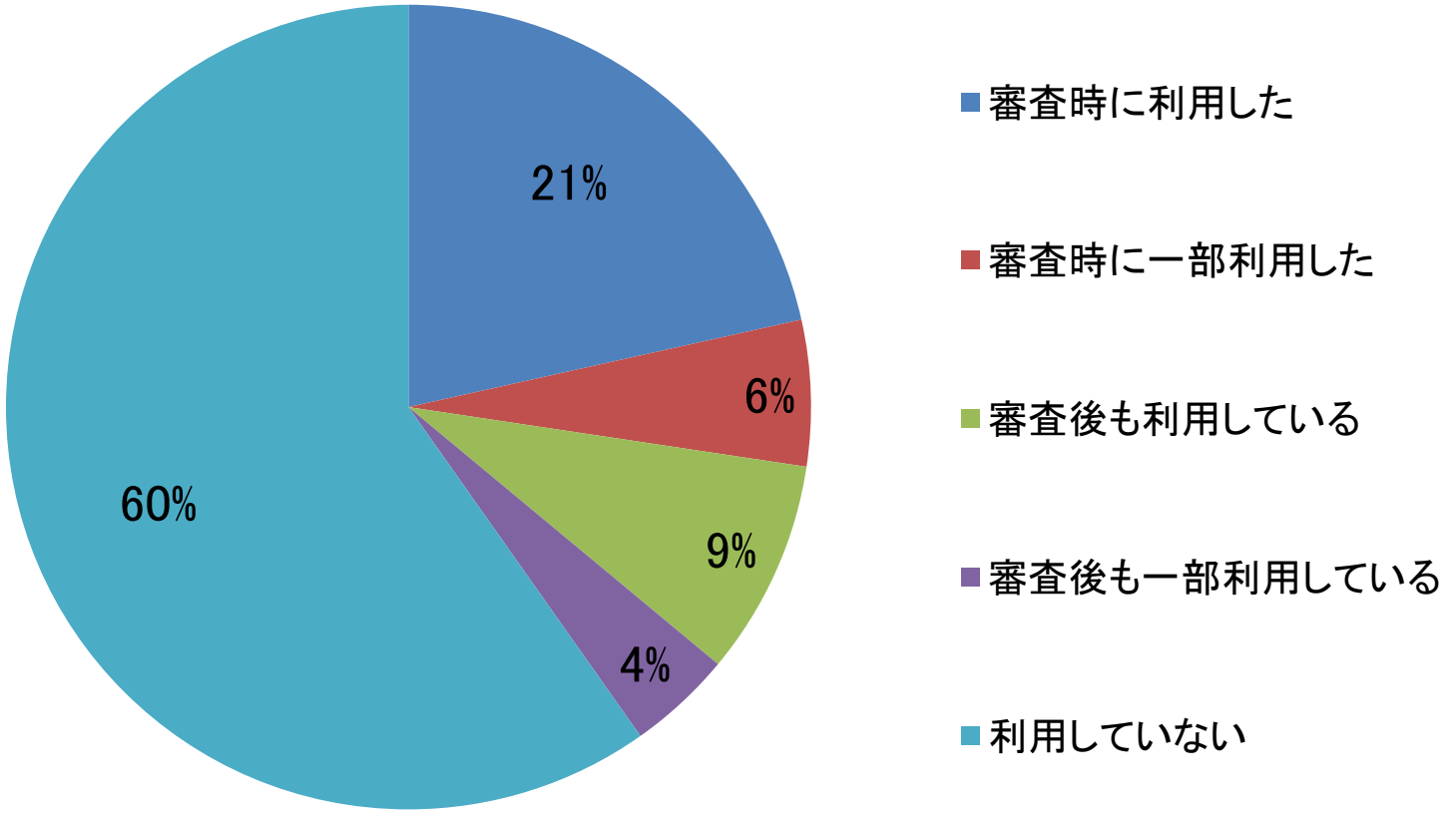
設問45.事務局は、個人情報に関わる法定、法令環境の変化に対応する事ができていますか。（N=360）



法令環境へ十分対応できている事業者は、3割程度に留まった。

第2章　プライバシーマーク取得状況について

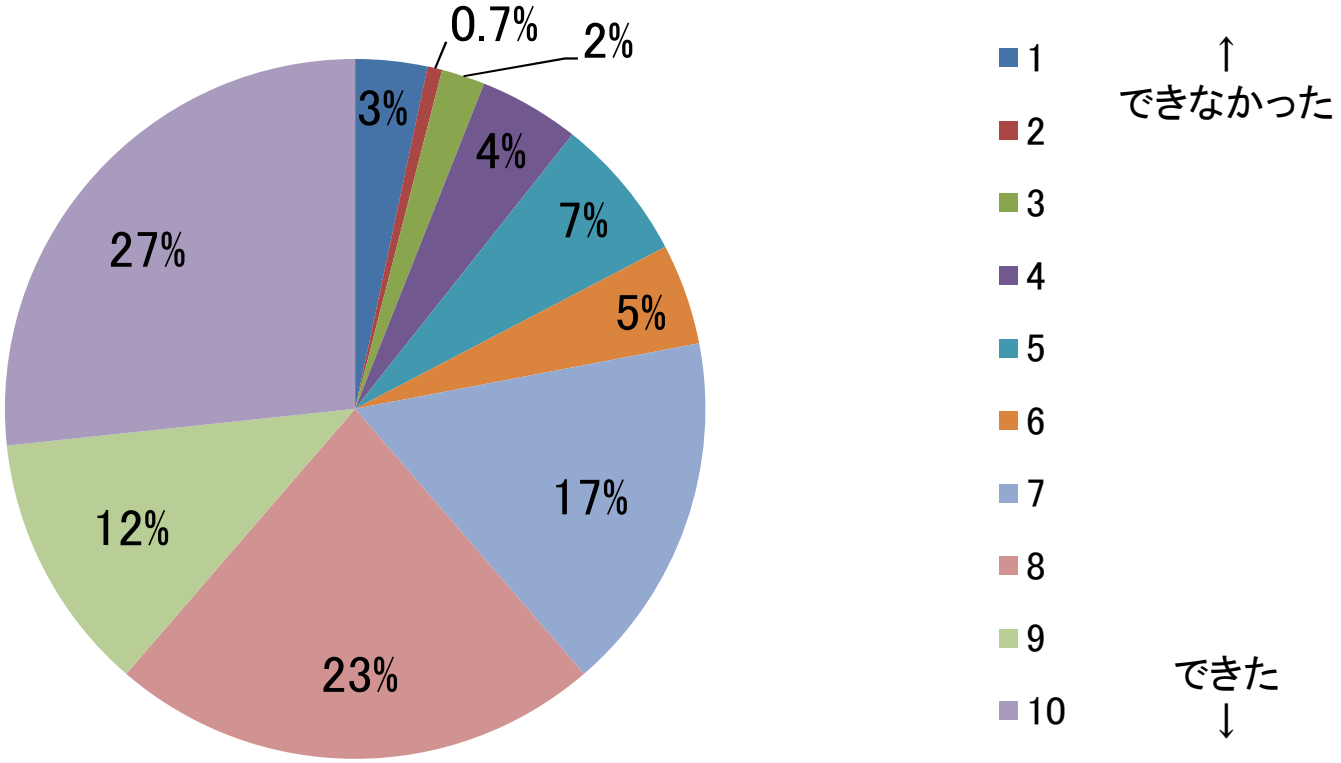
設問46.前回の更新（または新規取得）の際、コンサルタントを利用しましたか。（N=358）



コンサルタントを利用している事業者は、半数以下に留まった。

第2章　プライバシーマーク取得状況について

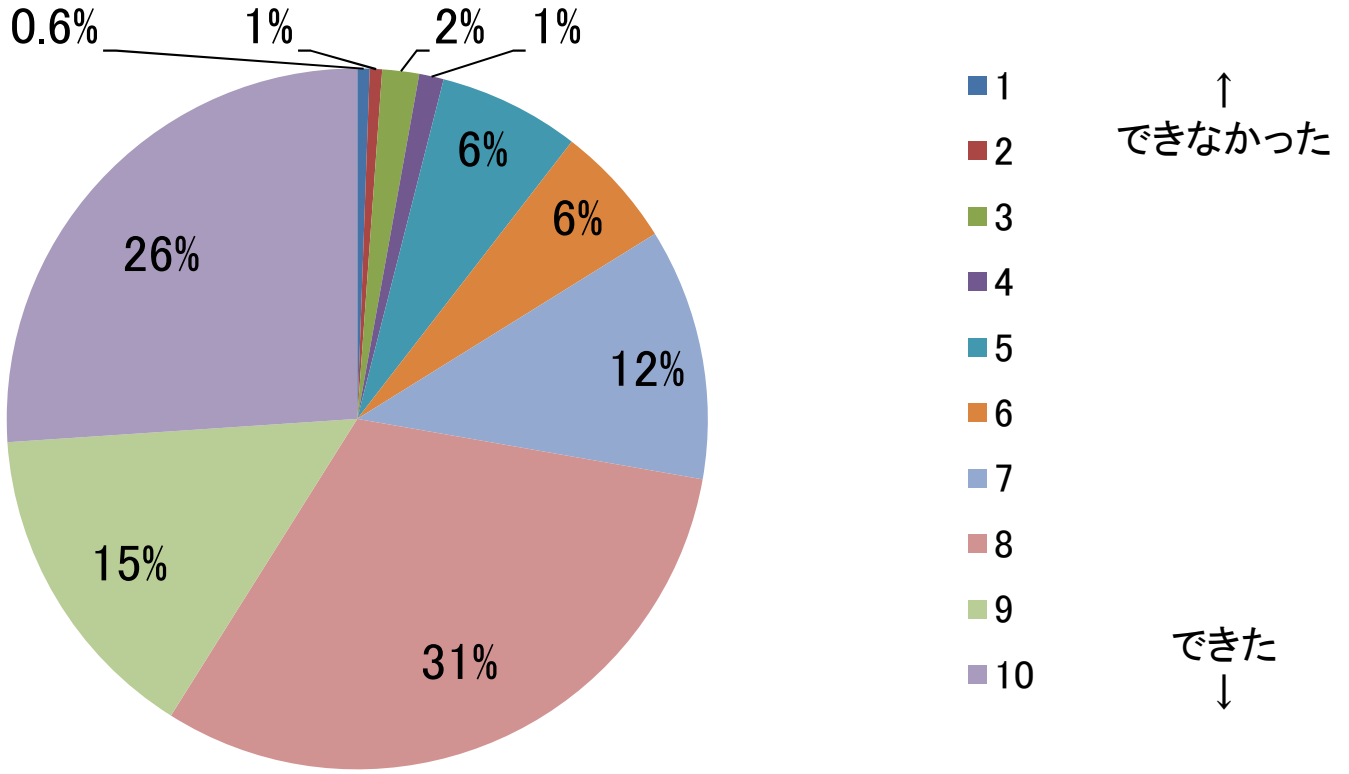
設問47.前回審査時、コンサルタントとコミュニケーションをうまく取ることができましたか。（N=150）



「8未満」と回答した事業者が4割を占め、コンサルタントとのコミュニケーションに課題がある事業者が一定数、存在する。

第2章　プライバシーマーク取得状況について

設問48.前回審査時、プライバシーマーク審査員とコミュニケーションをうまく取ることができましたか。（N=353）



「8未満」と回答した事業者が3割程度を占め、審査員とのコミュニケーションに課題がある事業者が一定数、存在する。

考察（第2章　プライバシーマーク取得状況について）

- プライバシーマークに対して、個人情報保護の取り組み向上や、従業員の意識向上といった効果を期待している事業者が、多数存在しており、プライバシーマーク取得事業者の個人情報保護への意識は比較的高い。

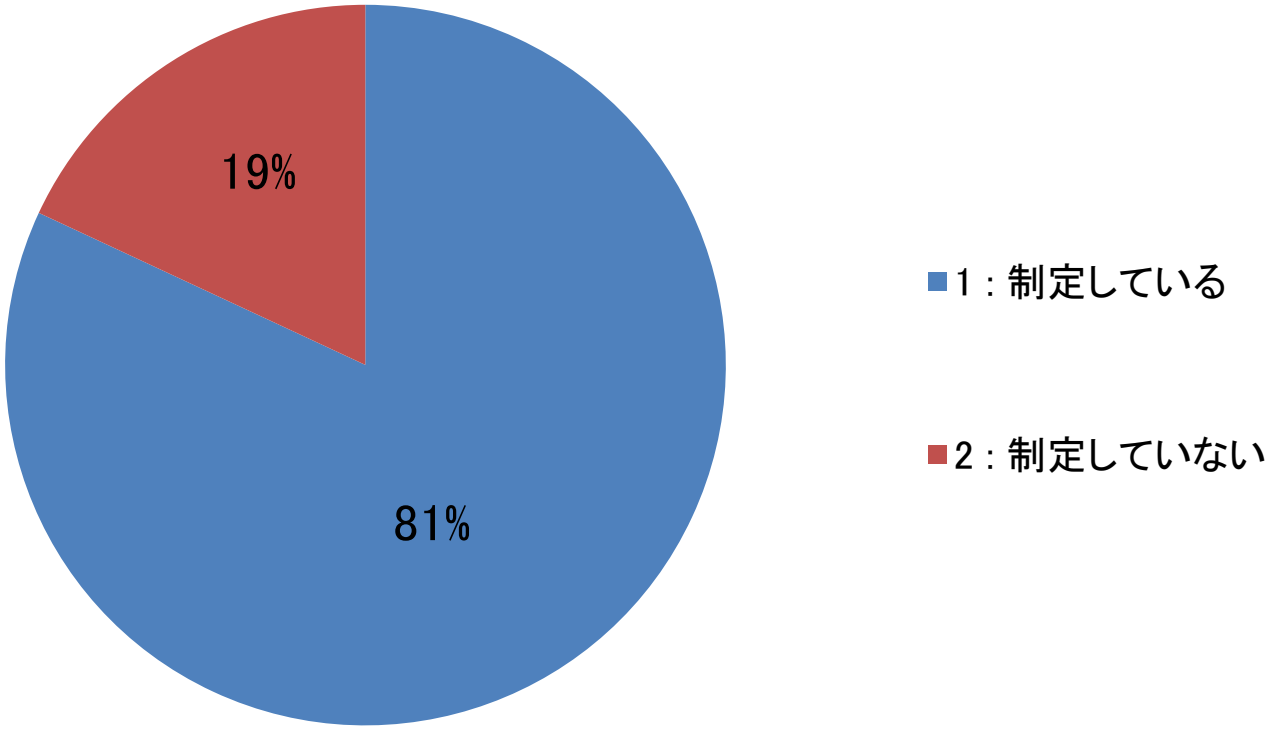
- プライバシーマークの取得が「社内の個人情報保護意識の浸透と実践」に繋がっており、期待通りの効果を上げている。

- プライバシーマーク事務局のリーダーは、プライバシーマーク取得後、PMSの運用や更新審査業務に複数年間継続して取り組んでいる傾向がみられる。

- 記録類や手順書が現場で十分活用できない原因として、「事務局が効果的に現場へ展開できていない」「現場の意識が低い」が挙げられており、PMSを改善するためには、事務局を中心とした組織全体のコミュニケーション能力の改善が必要である。

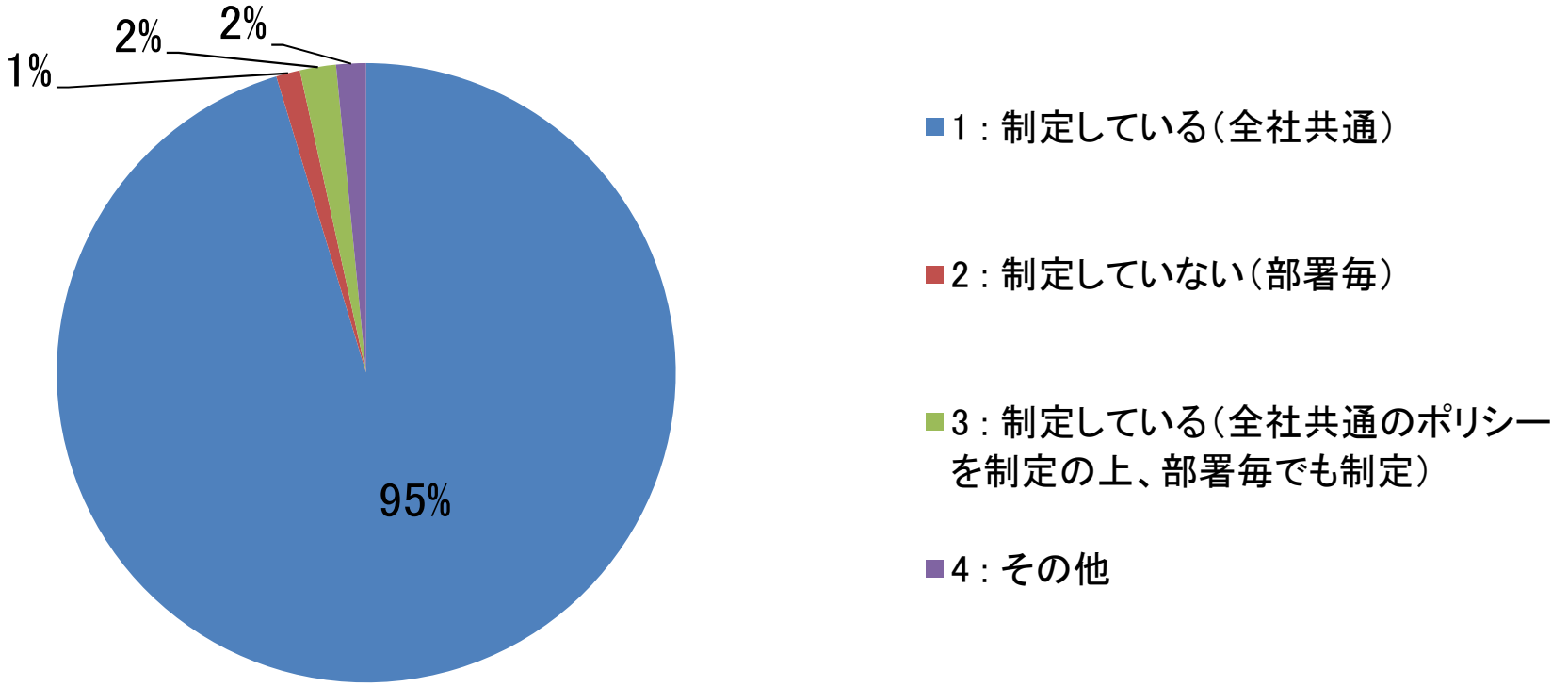
第3章
セキュリティマネジメントの運用状況

設問49. 情報セキュリティ・ポリシーを制定していますか。（N=399）



2割弱の事業者において、
情報セキュリティ・ポリシーは「制定されていない」。

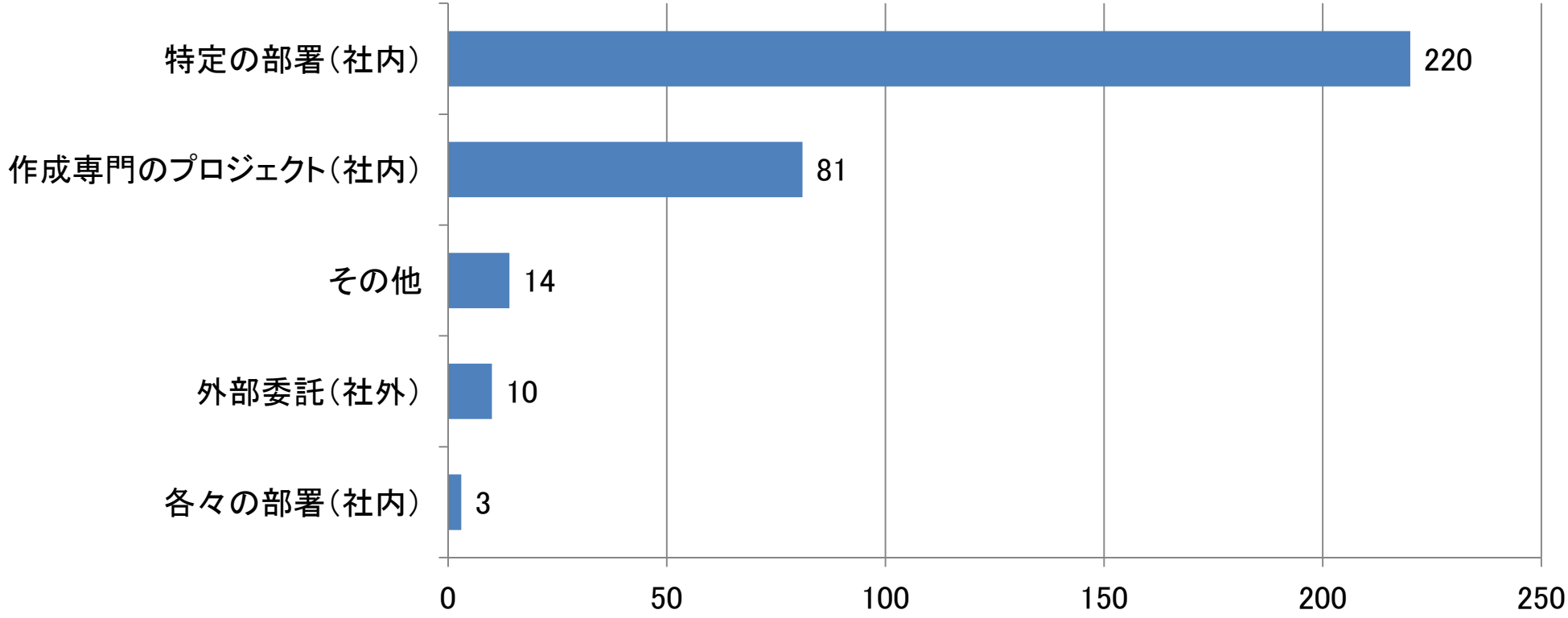
設問50. 情報セキュリティ・ポリシーは全社で共通したものを制定していますか。(N=320)



情報セキュリティ・ポリシーは、「全社共通」のものを
ほとんどの企業で制定している。

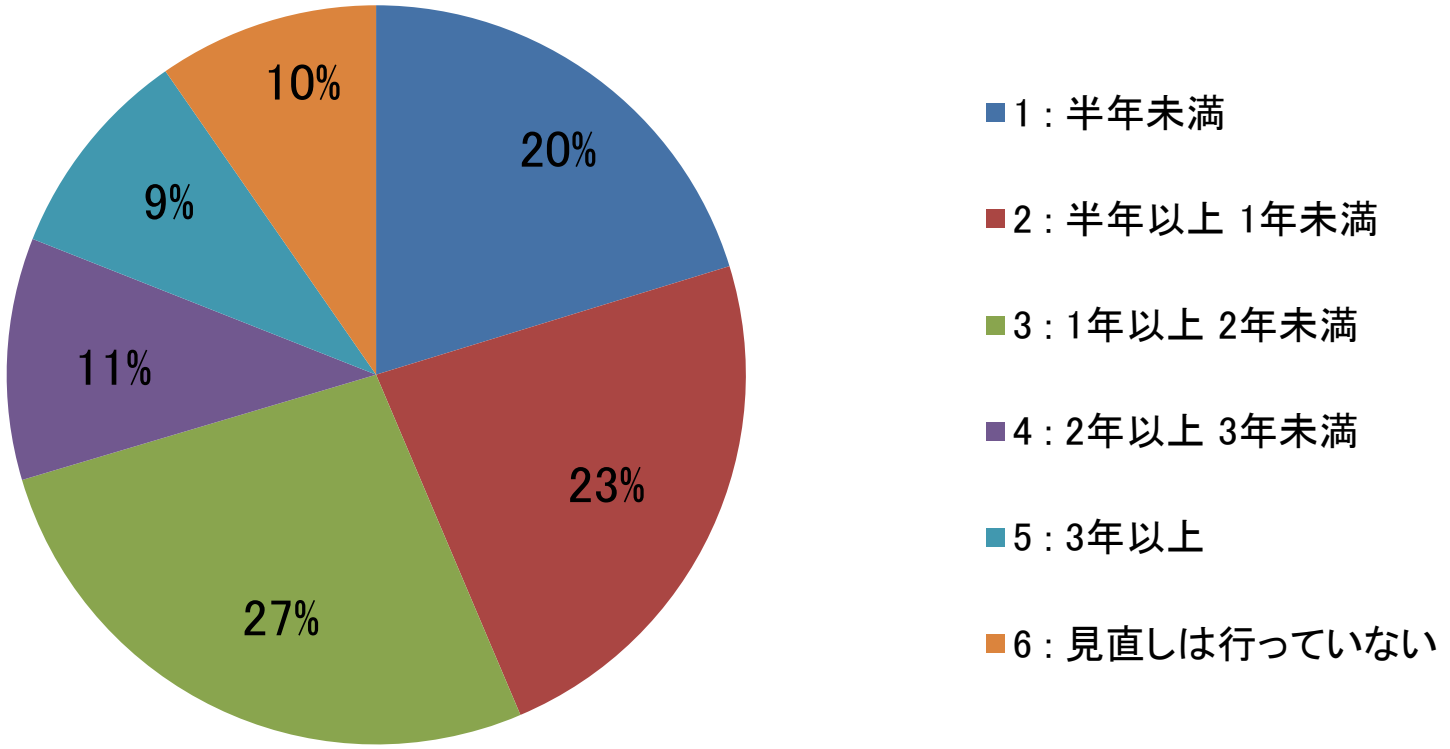
第3章　セキュリティマネジメントの運用状況

設問51.情報セキュリティ・ポリシーは、どちらの部署で作成しましたか。（複数回答）（N=319）



情報セキュリティ・ポリシーは、9割強の事業者で「社内」の「特定の組織」で作成を行なっており、「外部委託」は少ない。

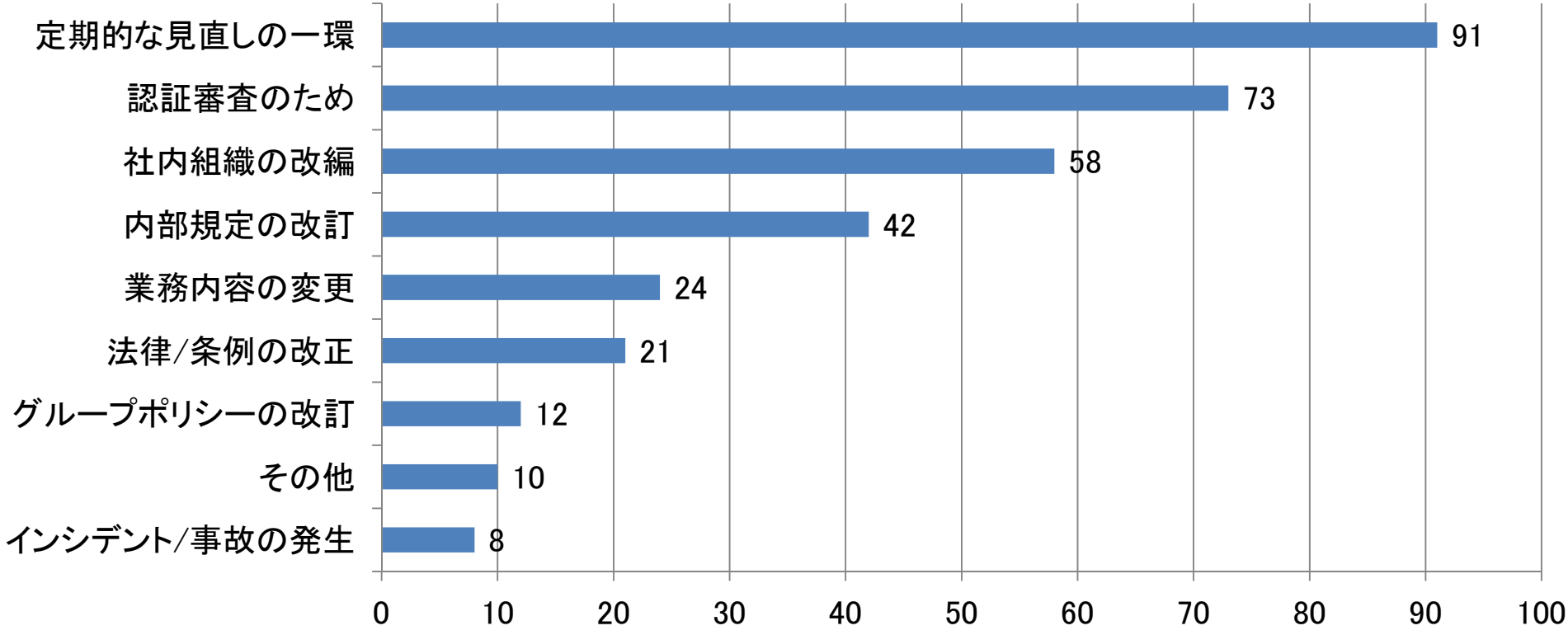
設問52. 情報セキュリティ・ポリシーの見直し（改訂）を、最後に実施したのは何年前ですか。（N=321）



7割の事業者で見直し（改訂）を「2年以内」に実施しているが、
3割の事業者では「2年以上」見直し(改訂)を実施していない。

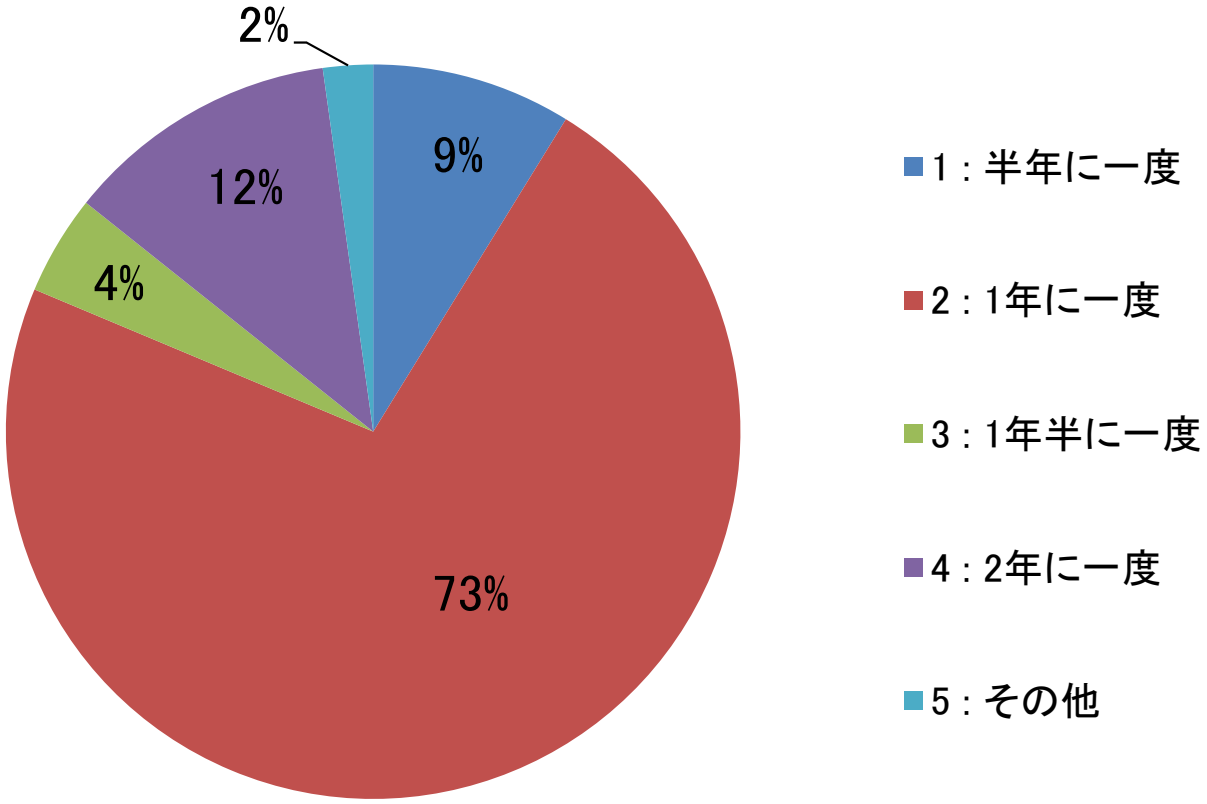
第3章　セキュリティマネジメントの運用状況

設問53.情報セキュリティ・ポリシーの見直し（改訂）を実施した理由は何ですか。（複数回答）（N=245）



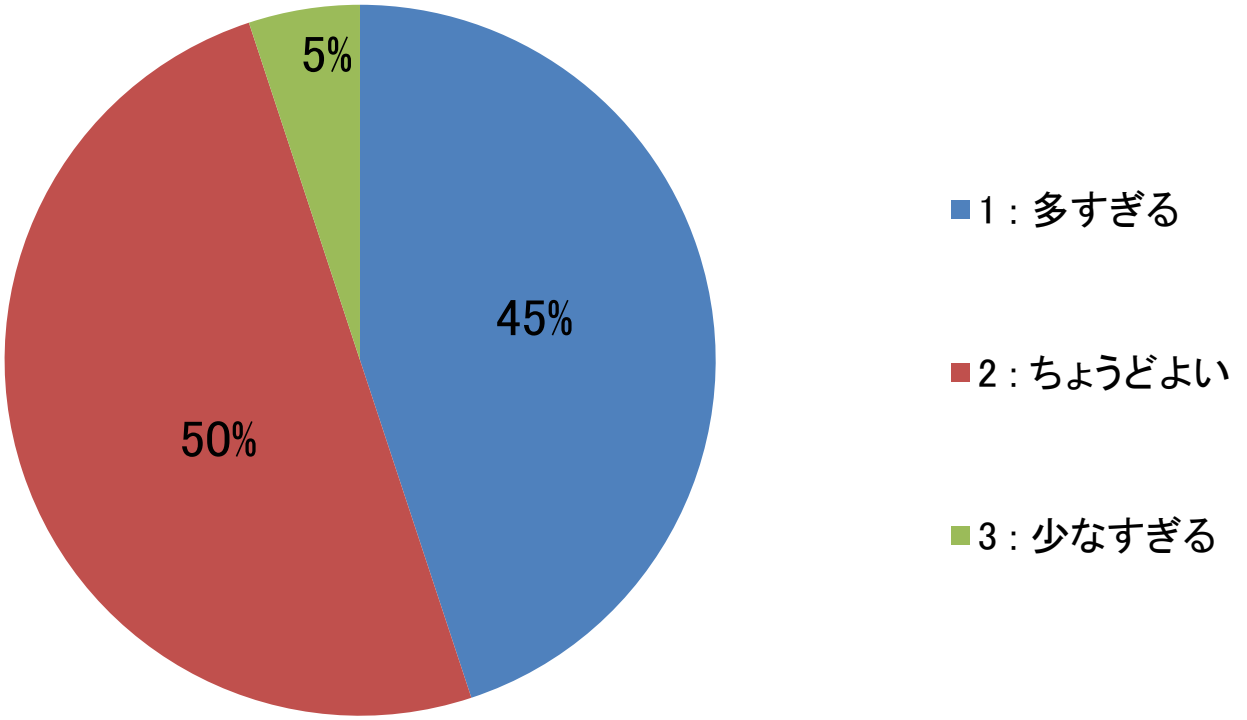
見直し（改訂）を行う理由としては、「定期的なイベント」に依ることが、最も多い。次いで多いのが、「規定類の変更」となる。

設問54. 定期的な見直しを実施する頻度はどの程度ですか。(N=91)



8割強の事業者で「1年以内に一度」の頻度で定期的な見直しを実施している。一方で、1割強の事業者では「2年に一度」の頻度で実施をしている。

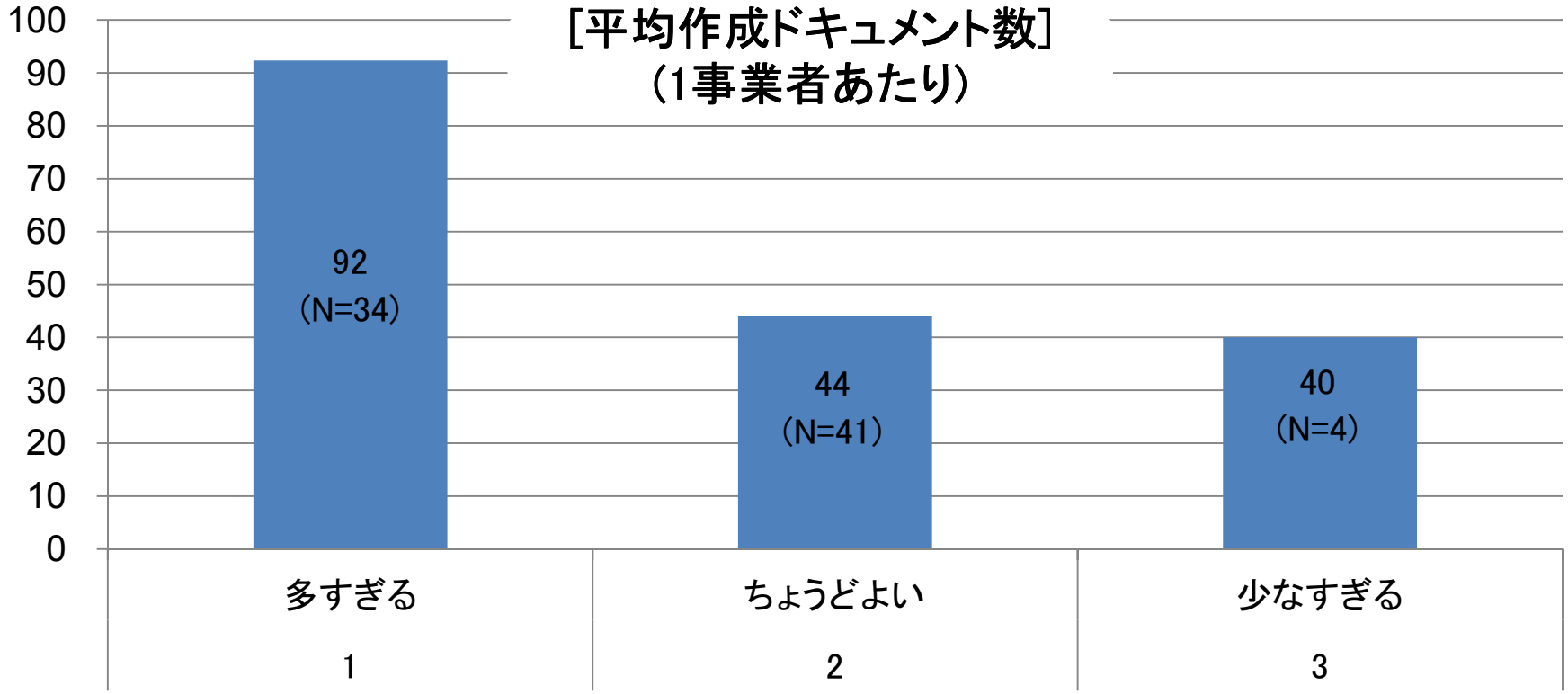
設問55. 情報セキュリティ・ポリシーに基づき作成するドキュメントの数について、どのように感じていますか。（N=296）



作成するドキュメント数については、「多すぎる」と「ちょうどよい」と感じている事業者数が拮抗している。

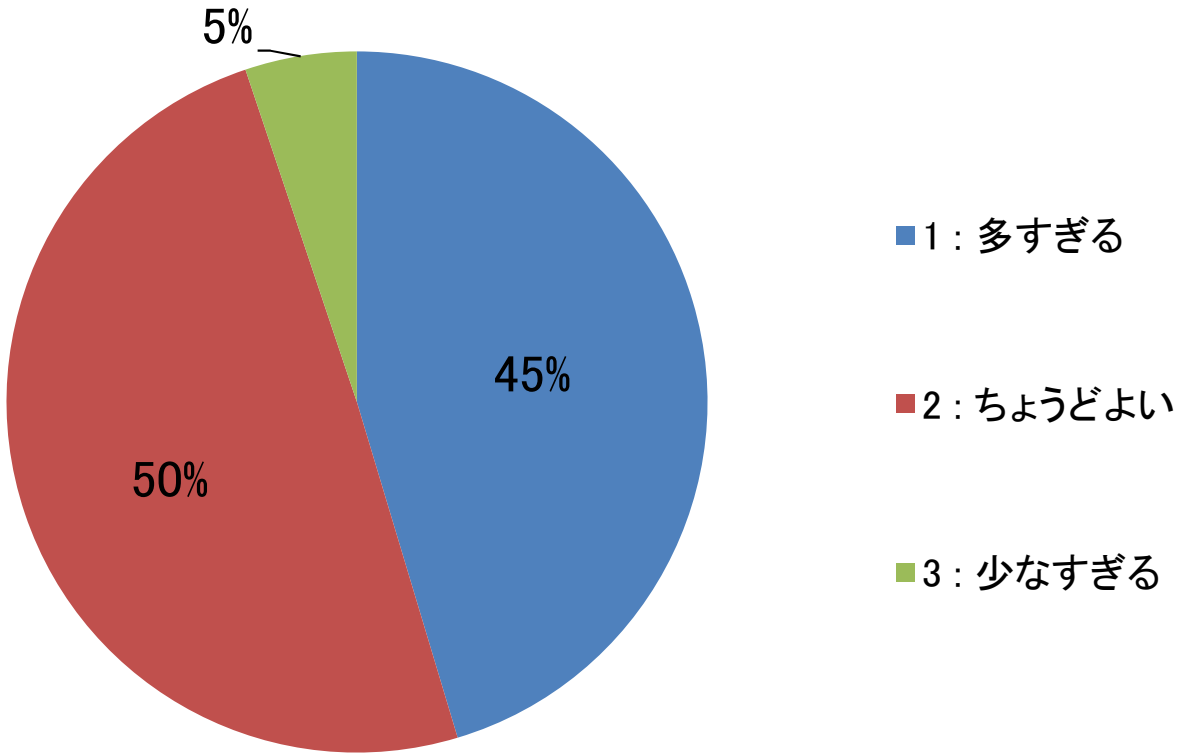
第3章　セキュリティマネジメントの運用状況

設問55. 情報セキュリティ・ポリシーに基づき作成するドキュメントの数について、どのように感じていますか。（N=79）



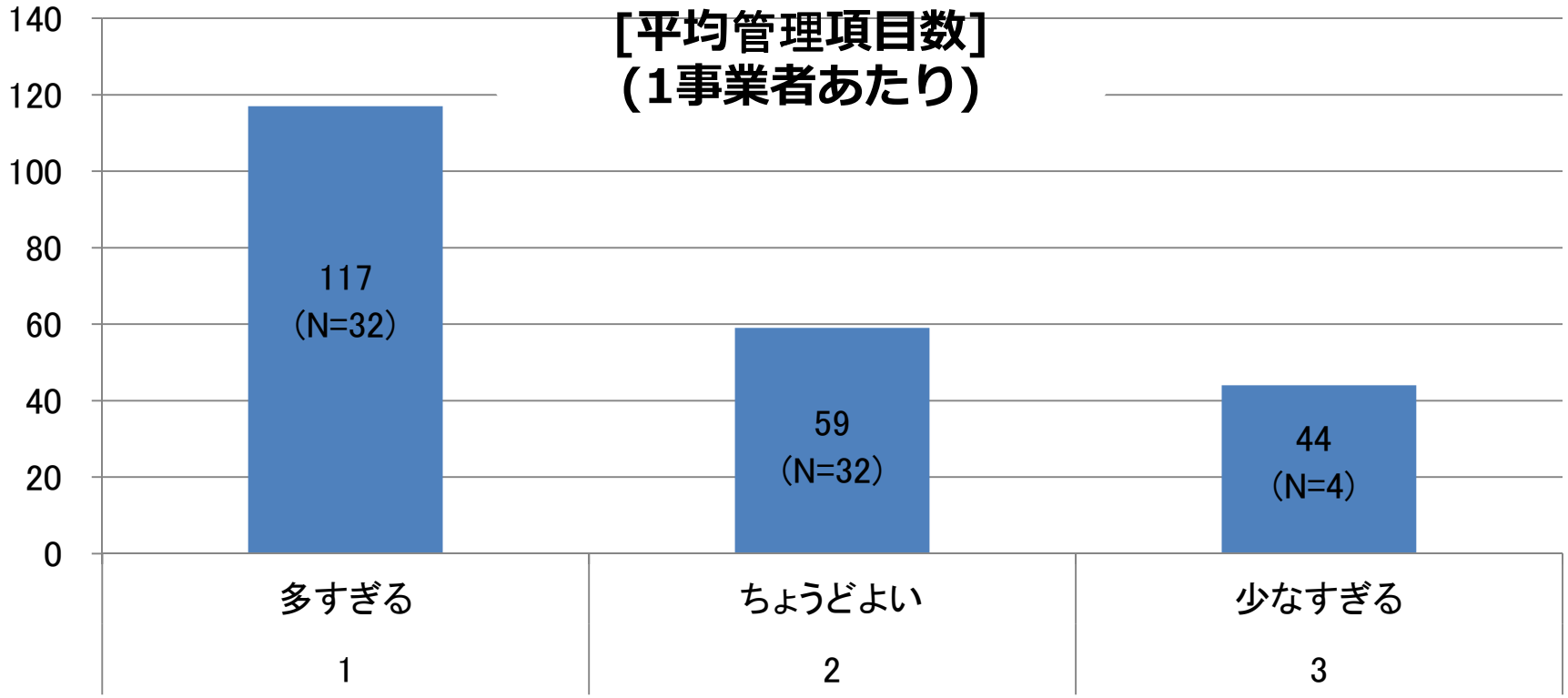
作成ドキュメント数が「多すぎる」と感じている事業者は、「ちょうどよい」と感じている事業者より、作成数の平均が2倍程度多い傾向にある。

設問56.情報セキュリティ・ポリシー関連の管理項目数について、どのように感じていますか。（N=291）



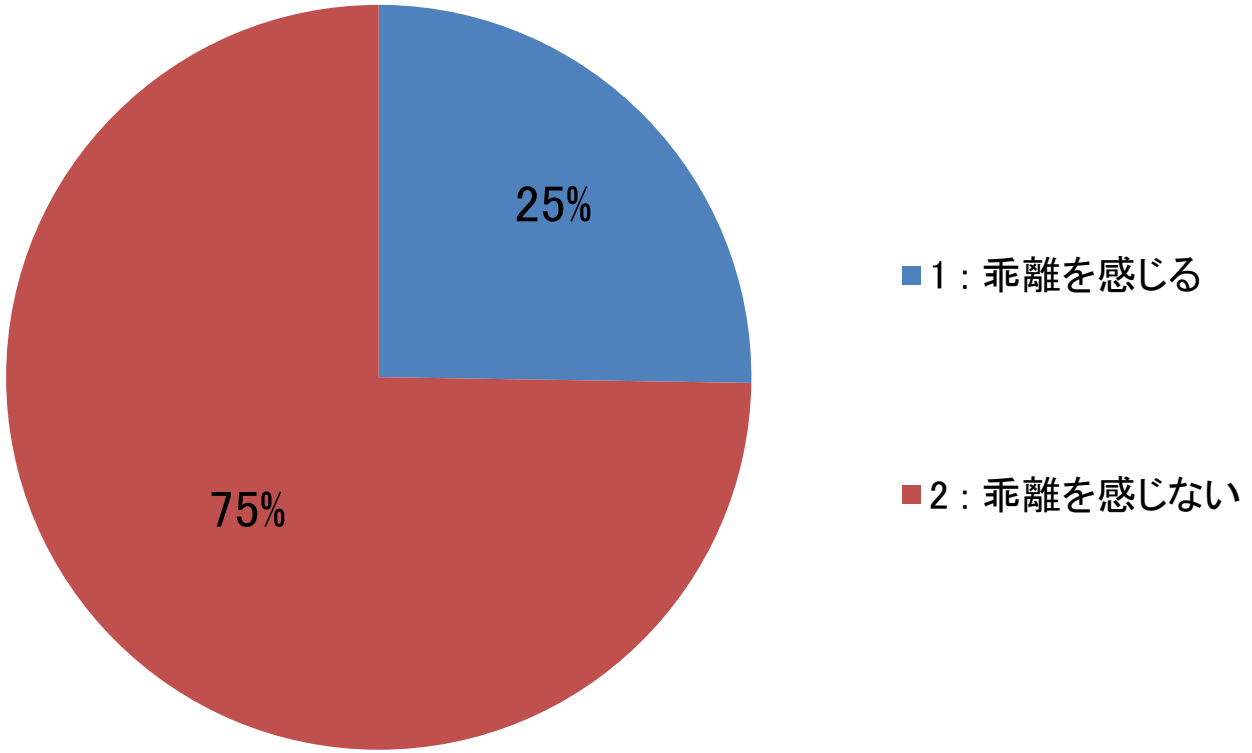
管理項目数については、「多すぎる」と「ちょうどよい」と感じている事業者数が拮抗している。

設問56.情報セキュリティ・ポリシー関連の管理項目数について、どのように感じていますか。（N=68）



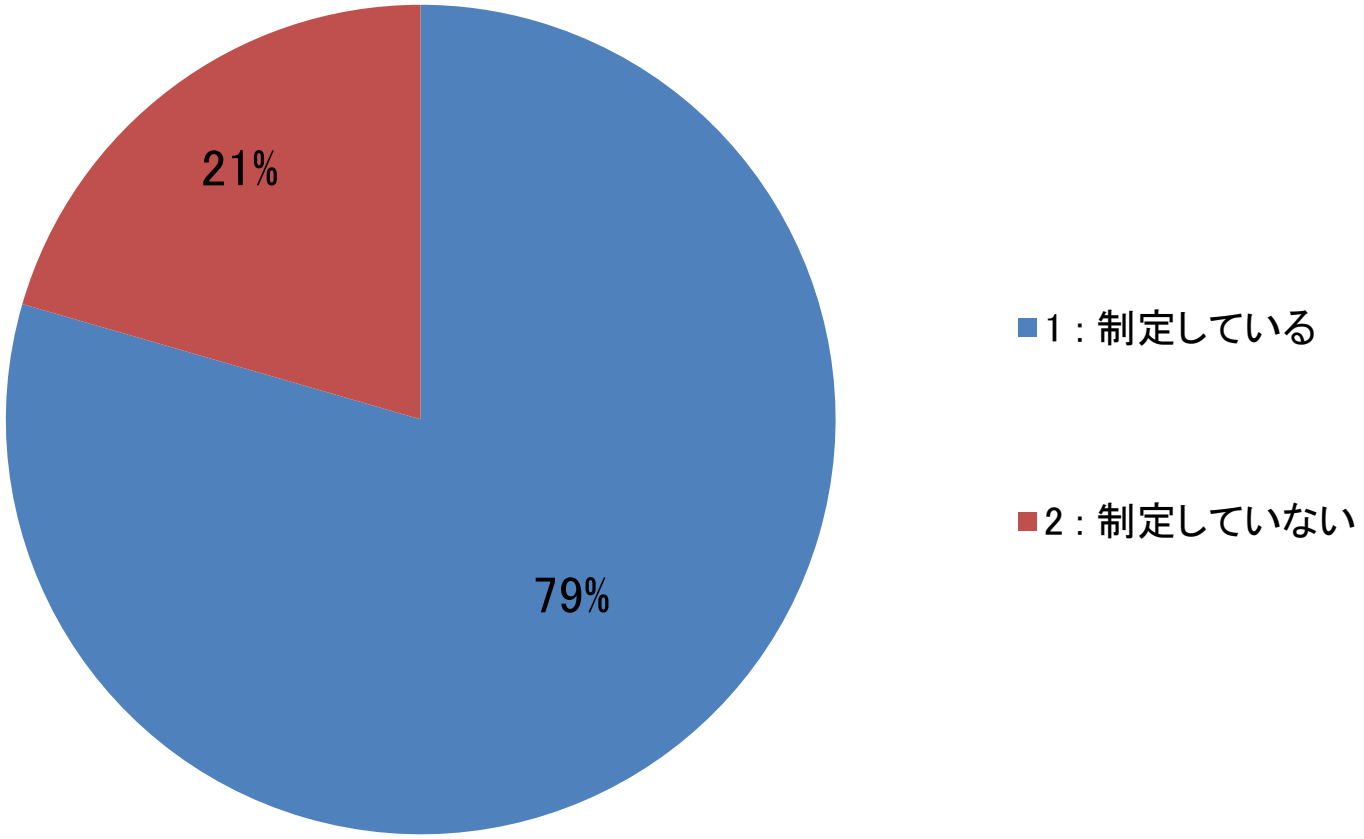
管理項目数が「多すぎる」と感じている事業者は、「ちょうどよい」と感じている事業者より、管理項目数の平均が2倍程度多い傾向にある。

設問57. 情報セキュリティ・ポリシーと情報セキュリィ・ルールとの間に乖離があると感じますか。(N=305)



75%の事業者では、ポリシーとルール間に「乖離がない」と感じている。
一方で、25%の事業者においては「乖離がある」と感じている。

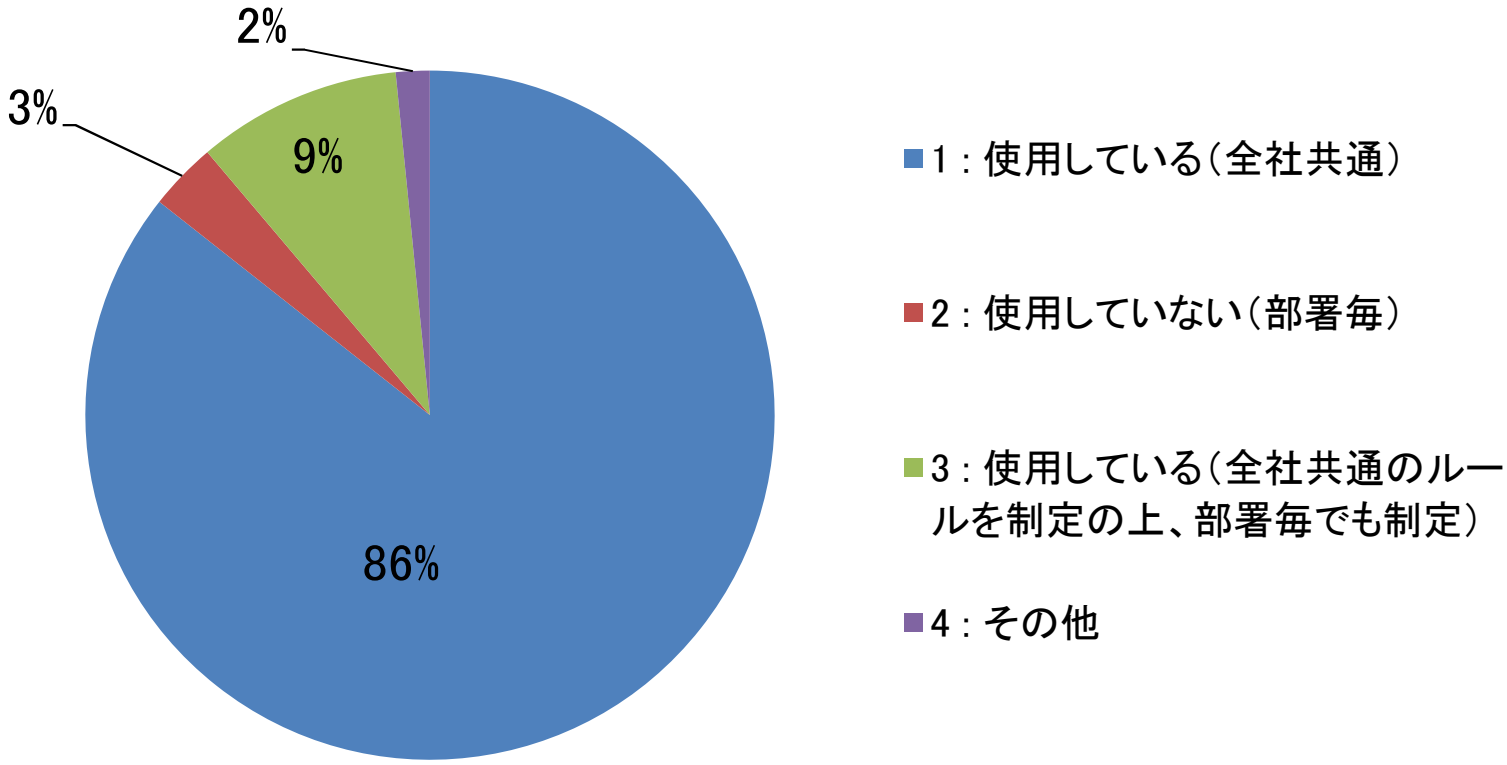
設問58.情報セキュリティ・ルールを制定していますか。（N=395）



2割強の事業者において、
情報セキュリティ・ルールは「制定されていない」。

第3章　セキュリティマネジメントの運用状況

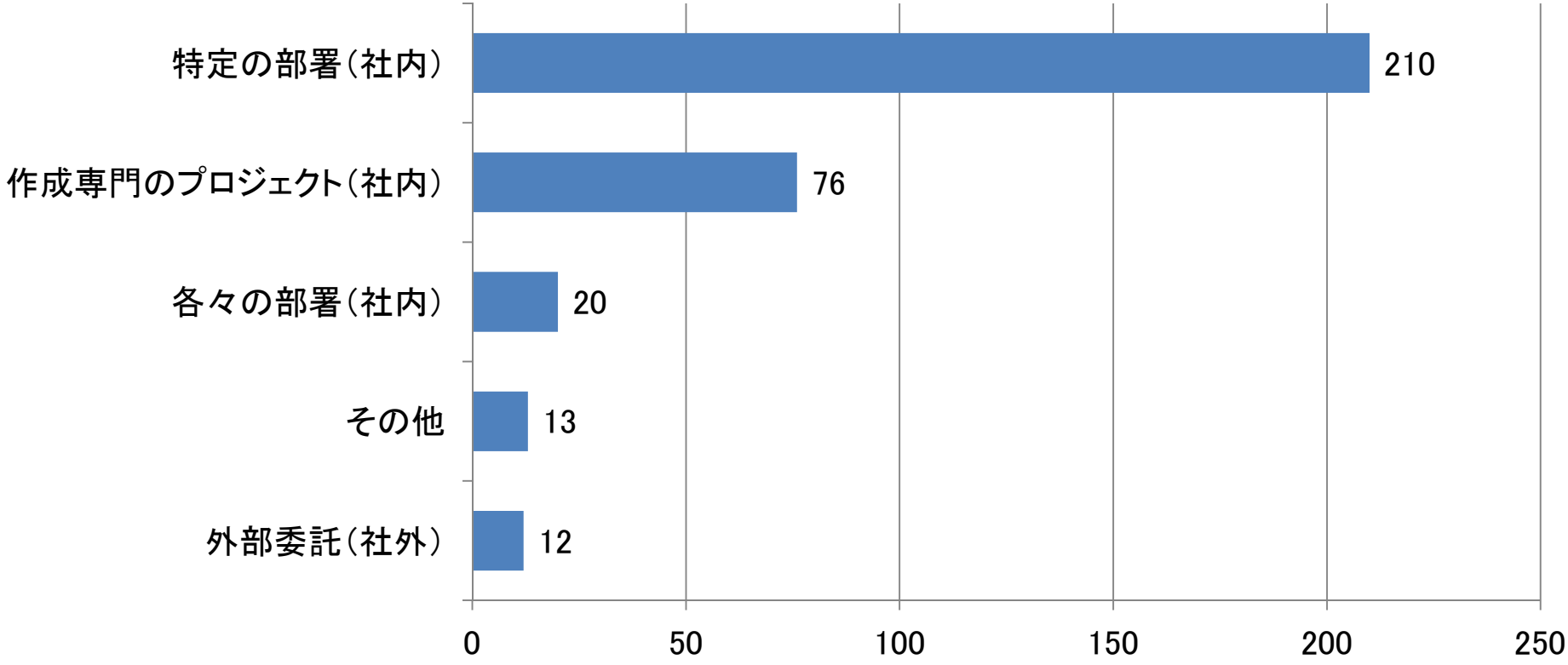
設問59. 情報セキュリティ・ルールは全社で使用したものを制定していますか。(N=313)



9割弱の事業者においては、「全社共通」のルールのみ使用している。
一方で、1割弱の事業者においては、「部署毎」でのルールも使用している。

第3章　セキュリティマネジメントの運用状況

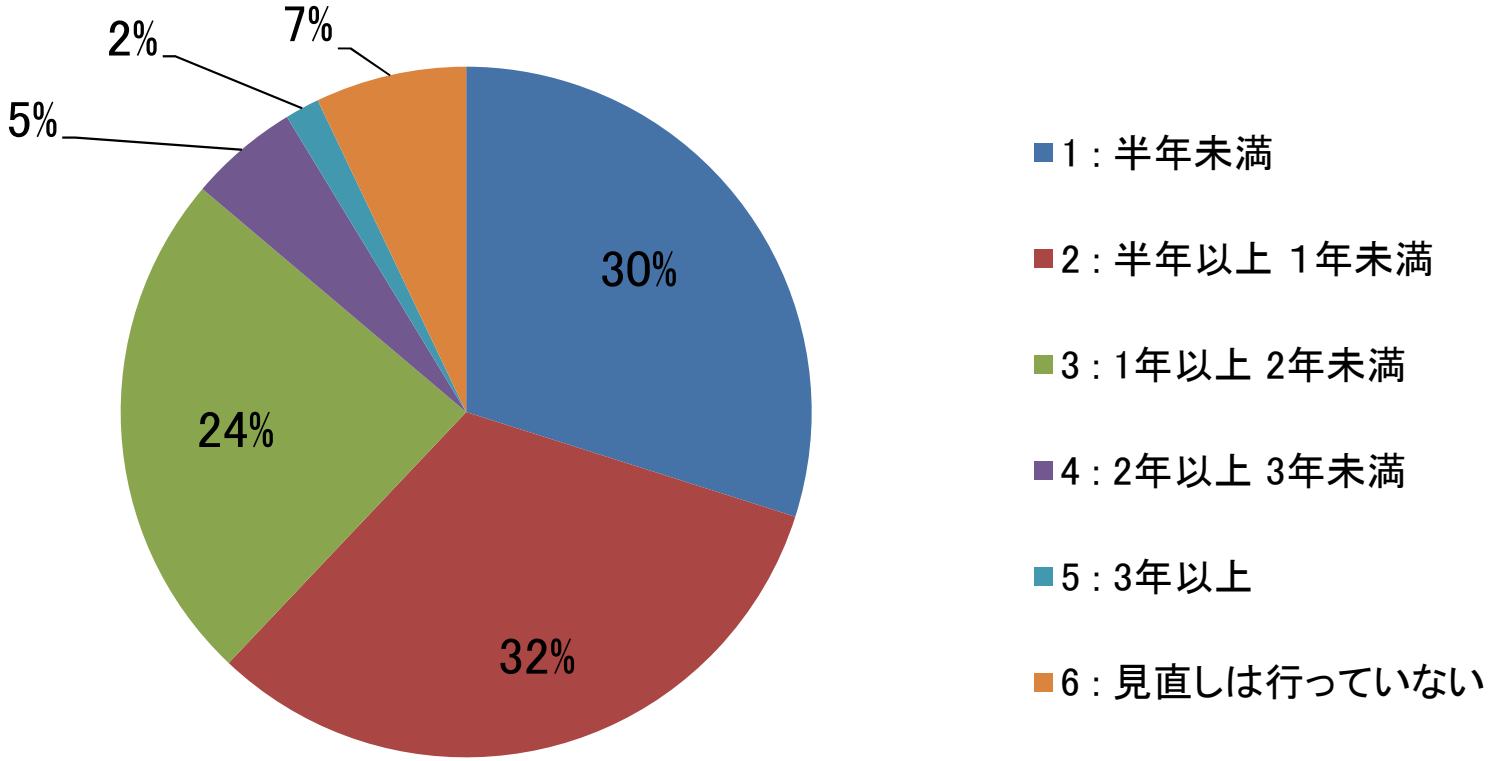
設問60.情報セキュリティ・ルールは、どちらの部署で作成しましたか。（複数回答）（N=312）



情報セキュリティ・ルールは、9割弱の事業者で「社内」の「特定の組織」で作成を行なっており、「各々の部署」や「外部委託」での作成は少ない。

第3章　セキュリティマネジメントの運用状況

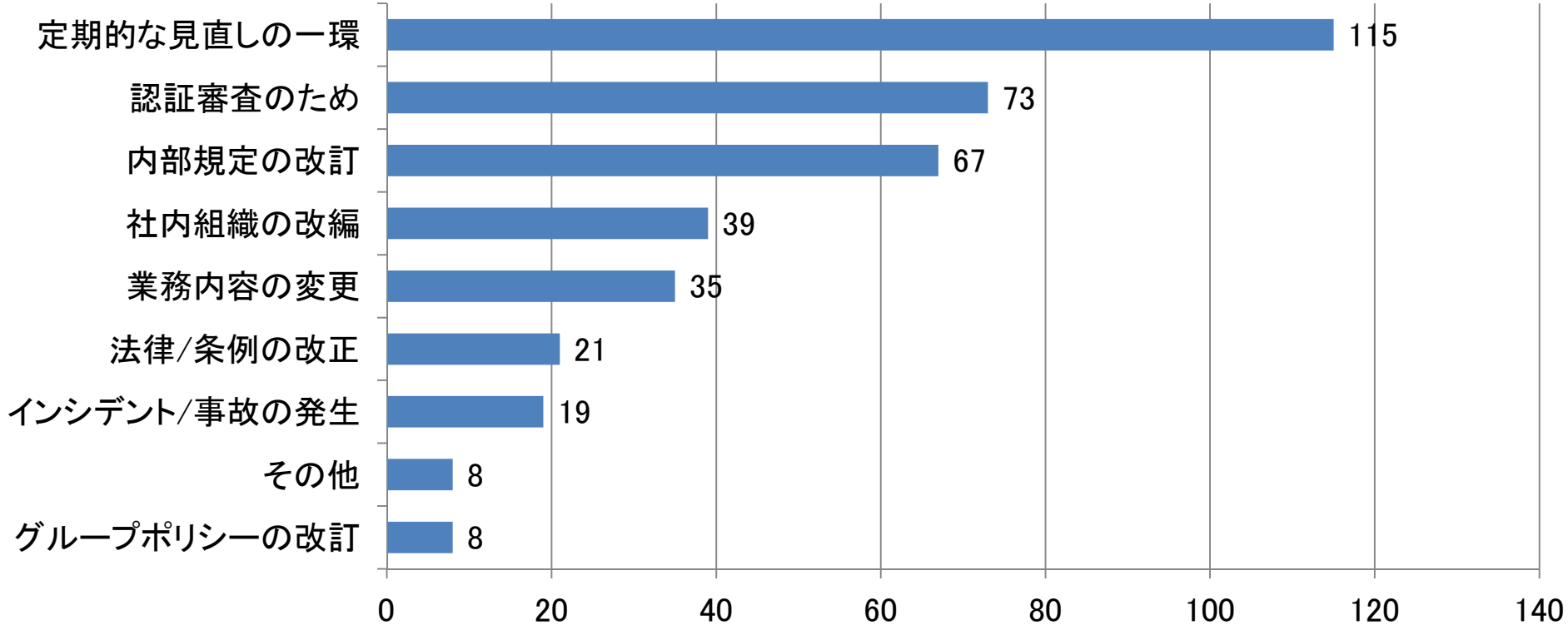
設問61. 情報セキュリティ・ルールの見直し（改訂）を、最後に実施したのは何年前ですか。（N=311）



8割強の事業者で見直し（改訂）を「2年以内」に実施しているが、
1割強の事業者では「2年以上」見直し（改訂）を実施していない。

第3章　セキュリティマネジメントの運用状況

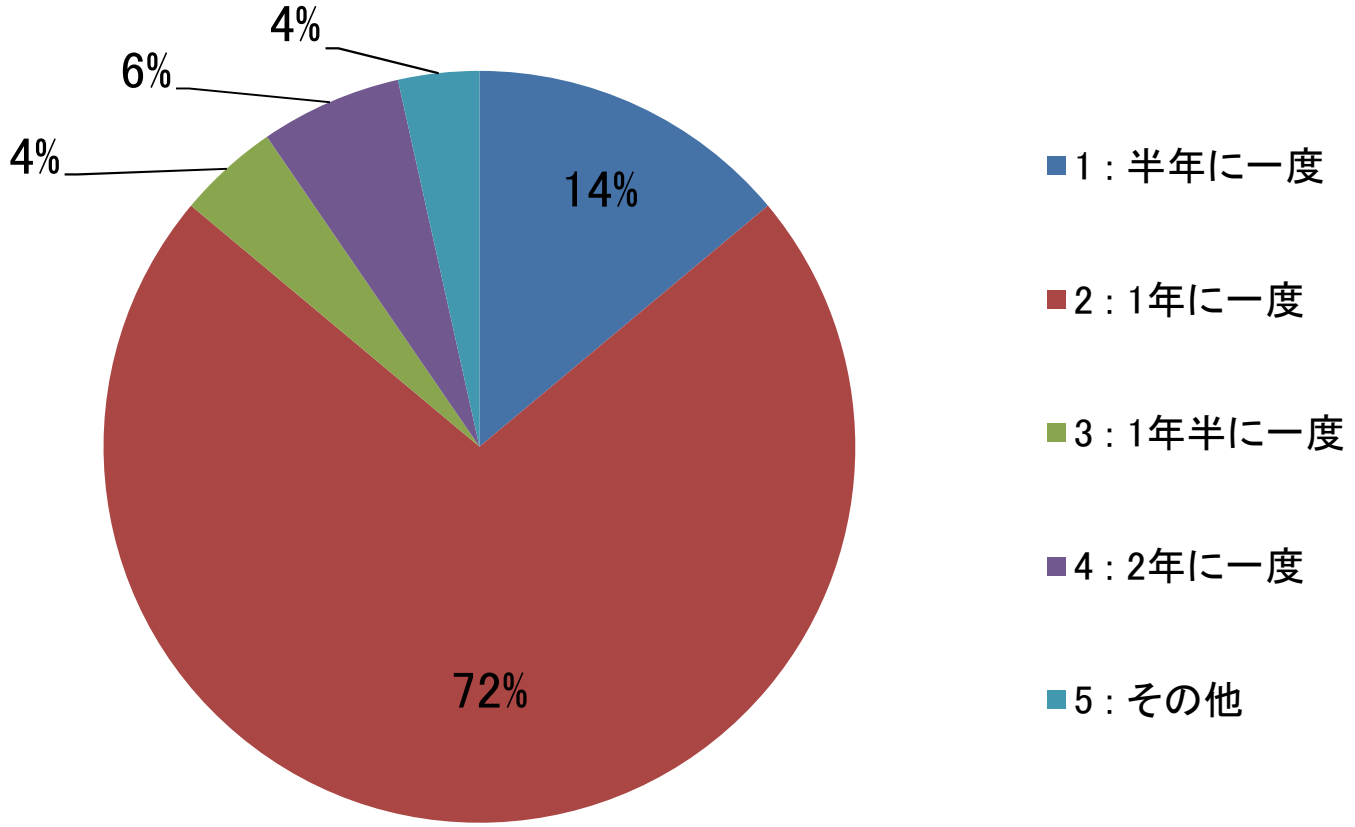
設問62.情報セキュリティ・ルールの見直し（改訂）を実施した理由は何ですか。（複数回答）（N=250）



見直し（改訂）を行う理由としては、「定期的なイベント」に依ることが、最も多い。次いで多いのが、「規定類の変更」となる。

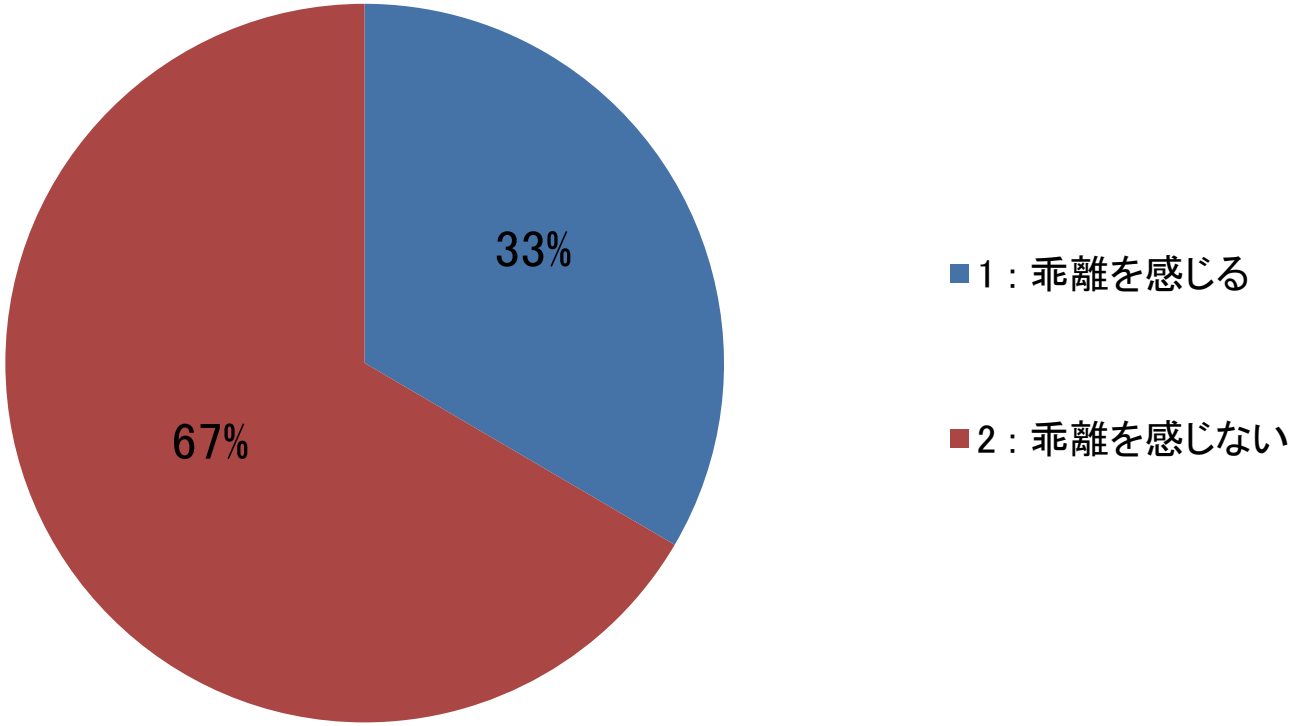
第3章　セキュリティマネジメントの運用状況

設問63. 定期的な見直しを実施する頻度はどの程度ですか。(N=115)



9割弱の事業者で「1年以内に一度」の頻度で定期的な見直しを実施している。一方で、1割強の事業者では「1年以上に一度」の頻度で実施をしている。

設問64. 情報セキュリティ・ルールと実業務との間に乖離があると感じますか。(N=302)

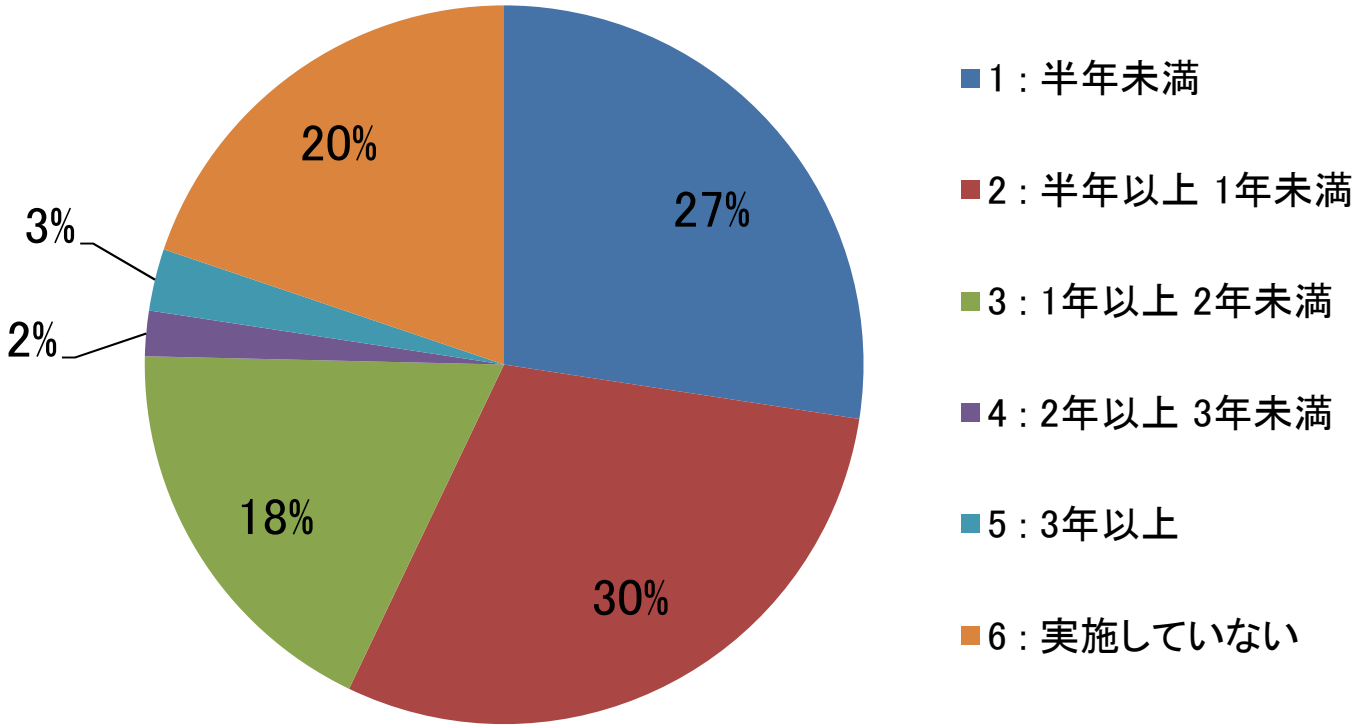


7割弱の事業者では、ルールと実業務の間に「乖離がない」と感じている。
一方で、3割強の事業者においては「乖離がある」と感じている。

第3章　セキュリティマネジメントの運用状況

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

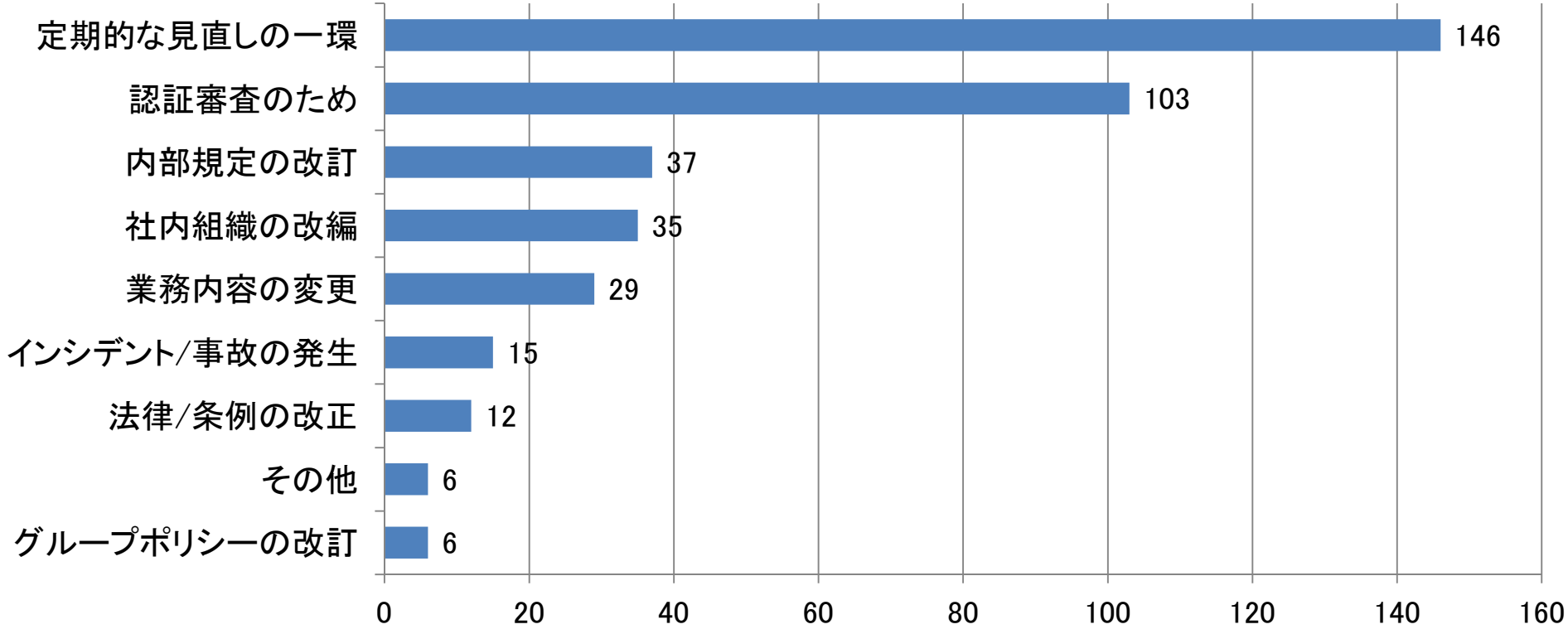
設問65. 情報セキュリティに関するリスク分析を最後に実施したのは何年前ですか。(N=264)



7割程の事業者では、「2年以内」にリスク分析を実施している。
一方で、3割程の事業者においては「2年以上」リスク分析を実施していない。

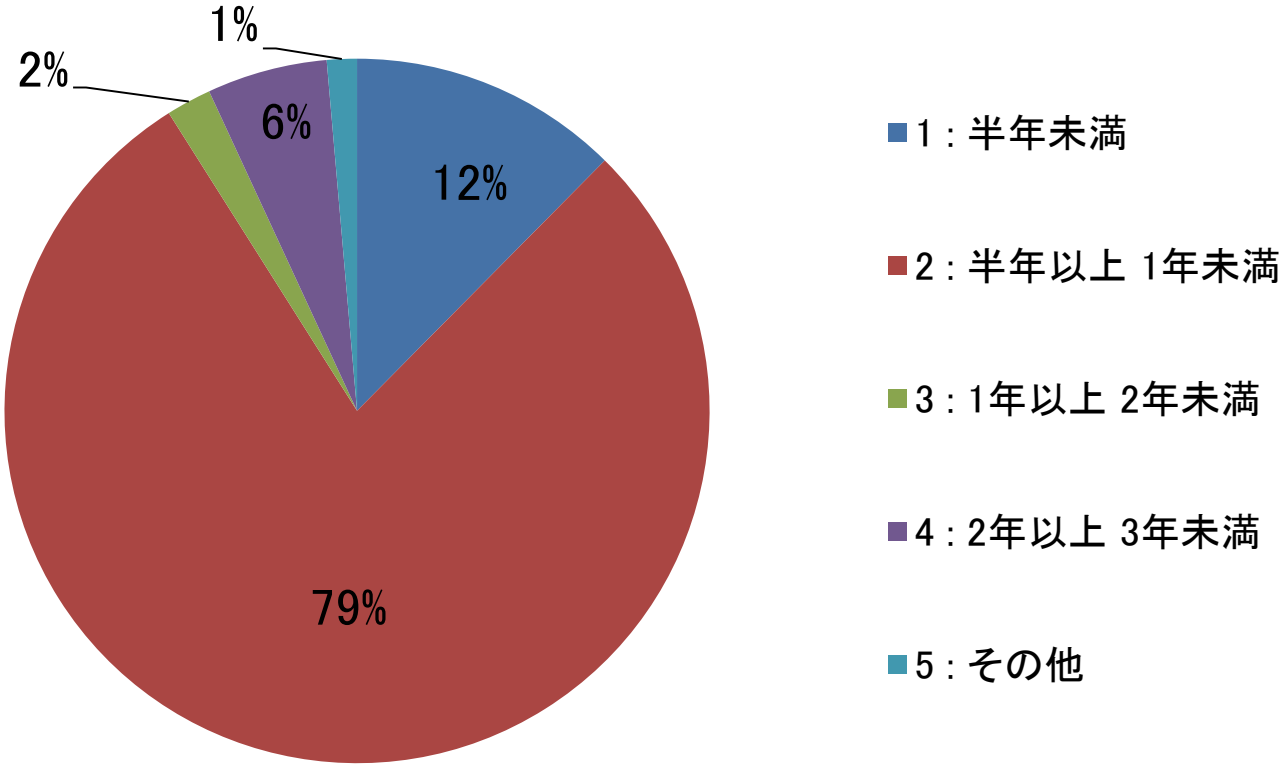
第3章　セキュリティマネジメントの運用状況

設問66.情報セキュリティに関するリスク分析を実施した理由は何ですか。（複数回答）（N=342）



見直し（改訂）を行う理由としては、「定期的なイベント」に依ることが、最も多い。次いで多いのが、「規定類の変更」となる。

設問67. 定期的な情報セキュリティに関するリスク分析を実施する頻度はどの程度ですか。(N=145)



9割の事業者で「1年以内に一度」の頻度で定期的な見直しを実施している。
一方で、1割の事業者では「1年以上に一度」の頻度で実施をしている。

考察（第3章　セキュリティマネジメントの運用状況）

- 情報セキュリティ・ポリシーと情報セキュリティ・ルールにて、ほぼ同じ回答傾向が見受けられる。（設問49～64）

- ポリシーやルールの見直し（改訂）やリスク分析を2年以上行なっていない企業が14～30%程あり、マネジメントサイクルの形骸化が潜在化している可能性が推測される。（設問52, 61, 65）。

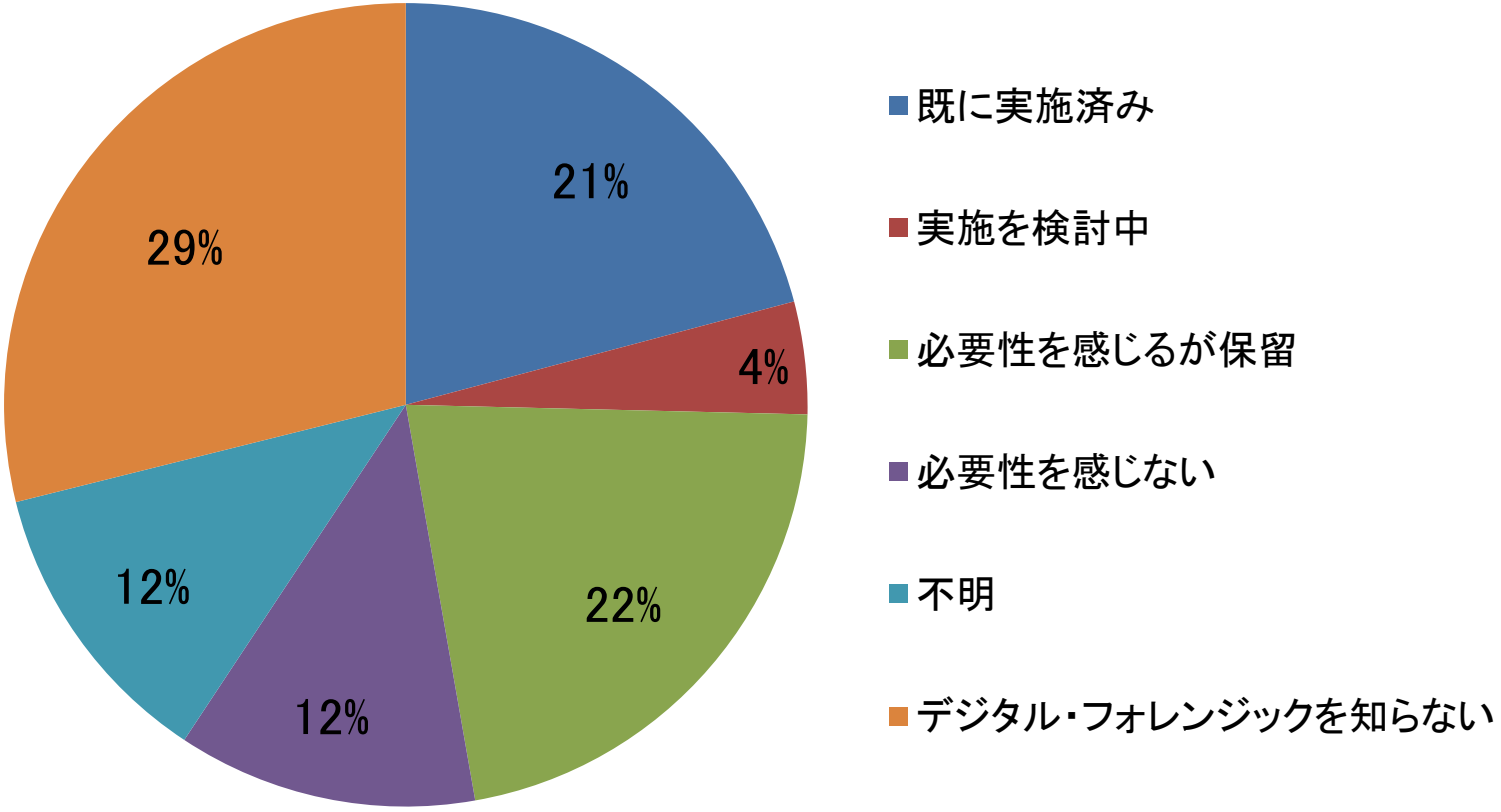
- セキュリティマネジメントの運用維持には、「定期的なイベント」によるチェックを行うことが有効であると考えられる。（設問53, 62, 66）

- ドキュメントや管理項目数が「多すぎる」と「ちょうどよい」と感じている事業者間においては、平均の作成数・管理項目数に明確な違いが見受けられる。（設問55, 56）

第4章
デジタルフォレンジックの実態について

第4章　デジタルフォレンジックの実態について

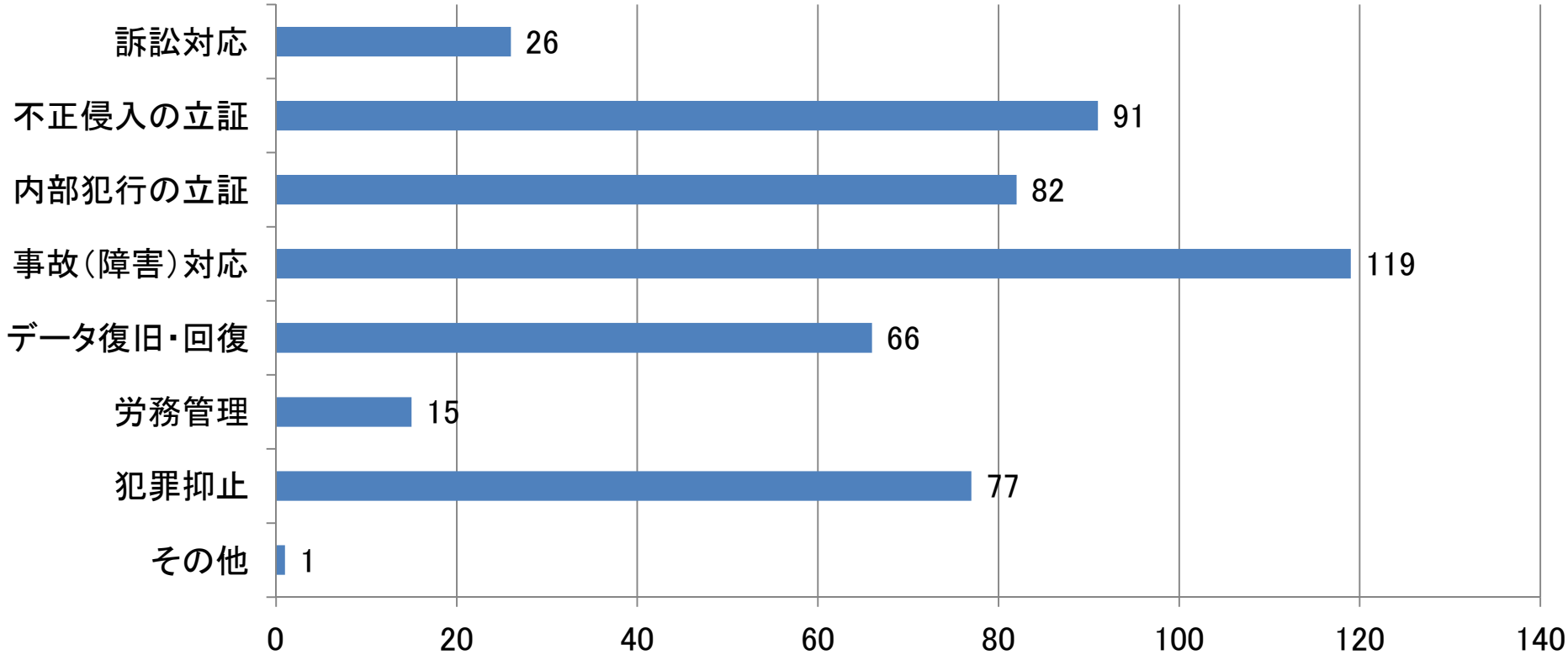
設問68.貴社はデジタル・フォレンジックを実施していますか。(N=398)



「既に実施済み」は21パーセントだが、「実施検討中」、
「必要性を感じるが保留」を合わせると、47%と約半数となる。

第4章　デジタルフォレンジックの実態について

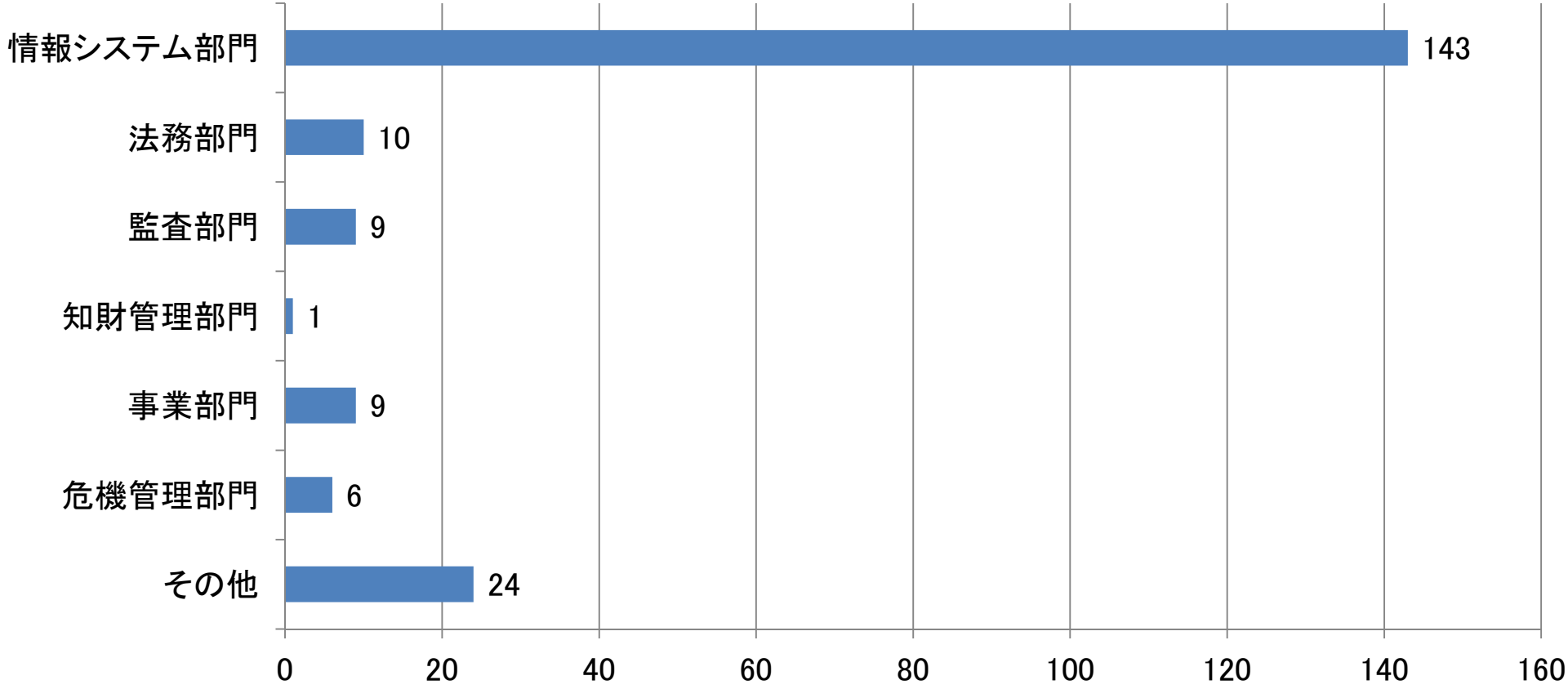
設問69.貴社でのデジタル・フォレンジックの実施理由を挙げてください。（複数回答）(N=188)



「訴訟対応」よりも「インシデント・レスポンス」や
「内部犯行の対応」へのニーズが高い。

第4章　デジタルフォレンジックの実態について

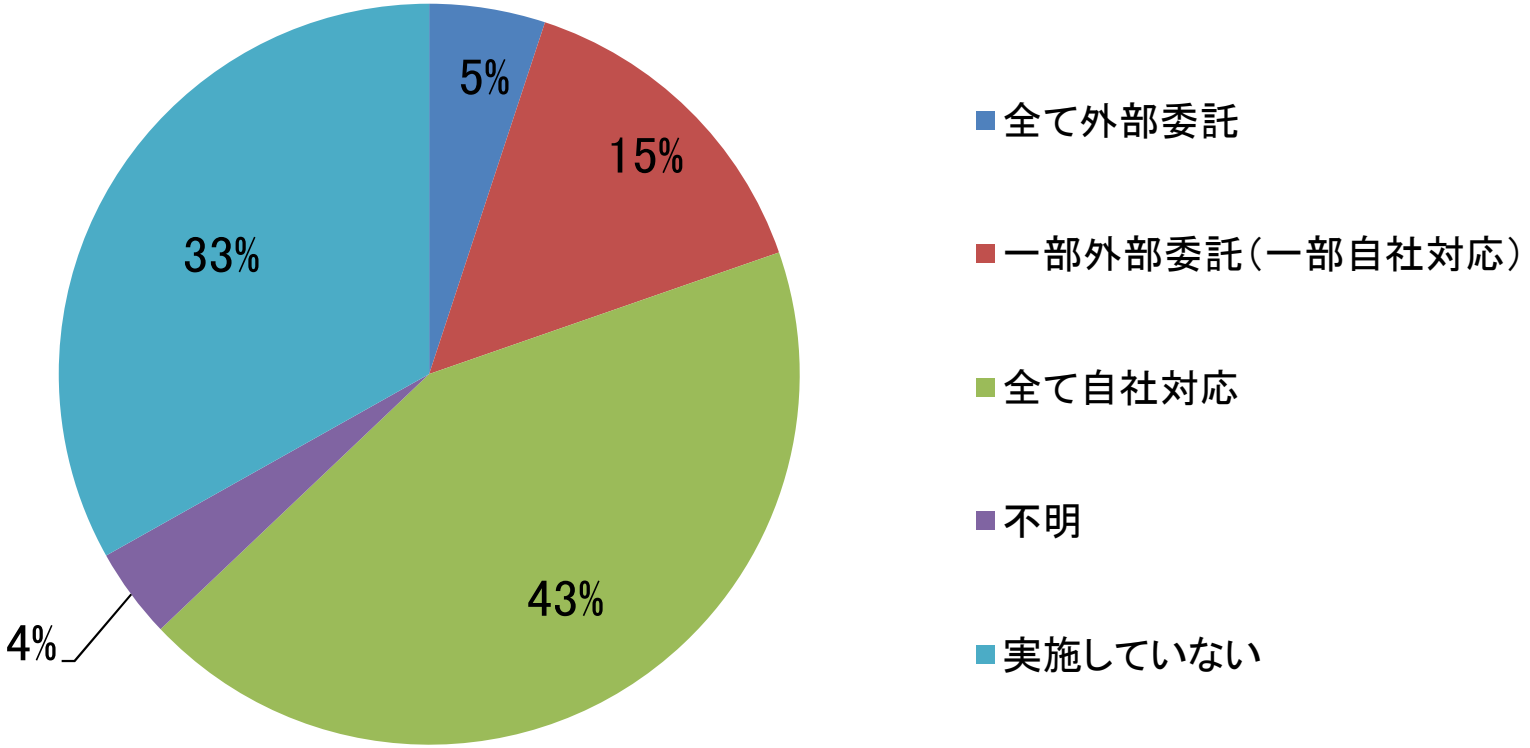
設問70.貴社でのデジタル・フォレンジック実施の主管部門をお選びください。（複数回答）(N=181)



「法務部門」より「情報システム部門」が圧倒的多数となっている。

第4章　デジタルフォレンジックの実態について

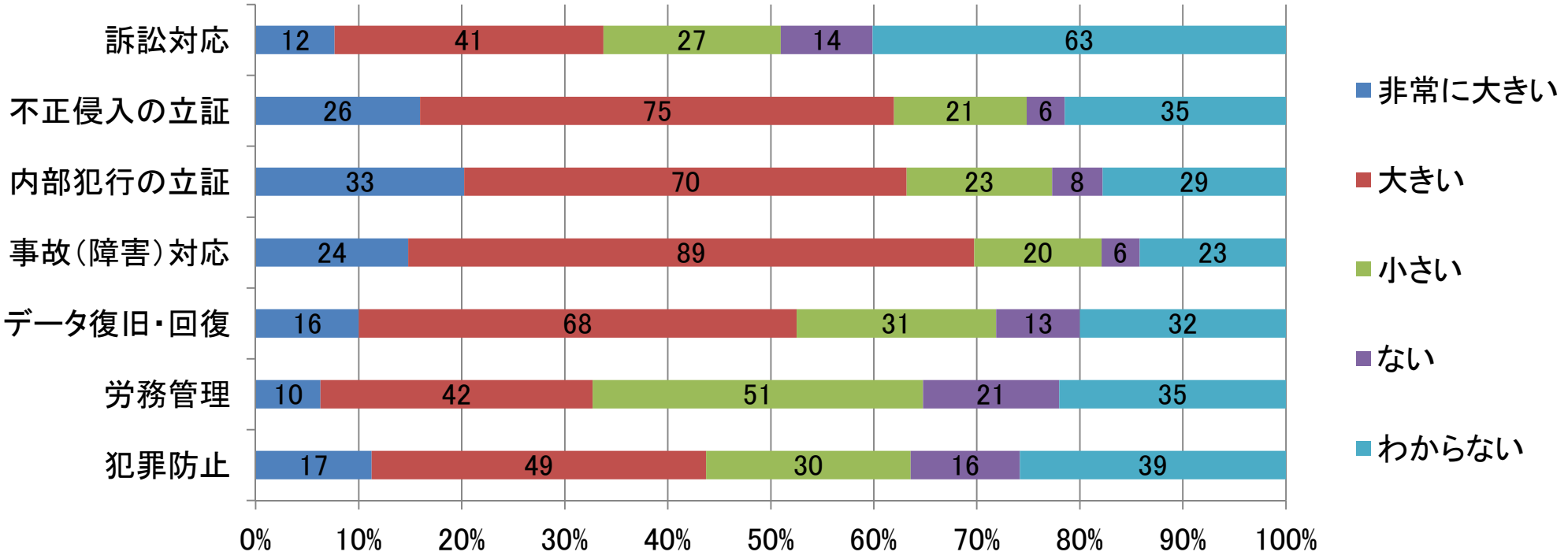
設問71.貴社でのデジタル・フォレンジックの実施方法についてお選びください。（複数回答）(N=178)



「全て自社対応」が多数を占め、「一部自社対応」と合わせると58%となり、実施企業においてはほとんどが自社対応である。

第4章　デジタルフォレンジックの実態について

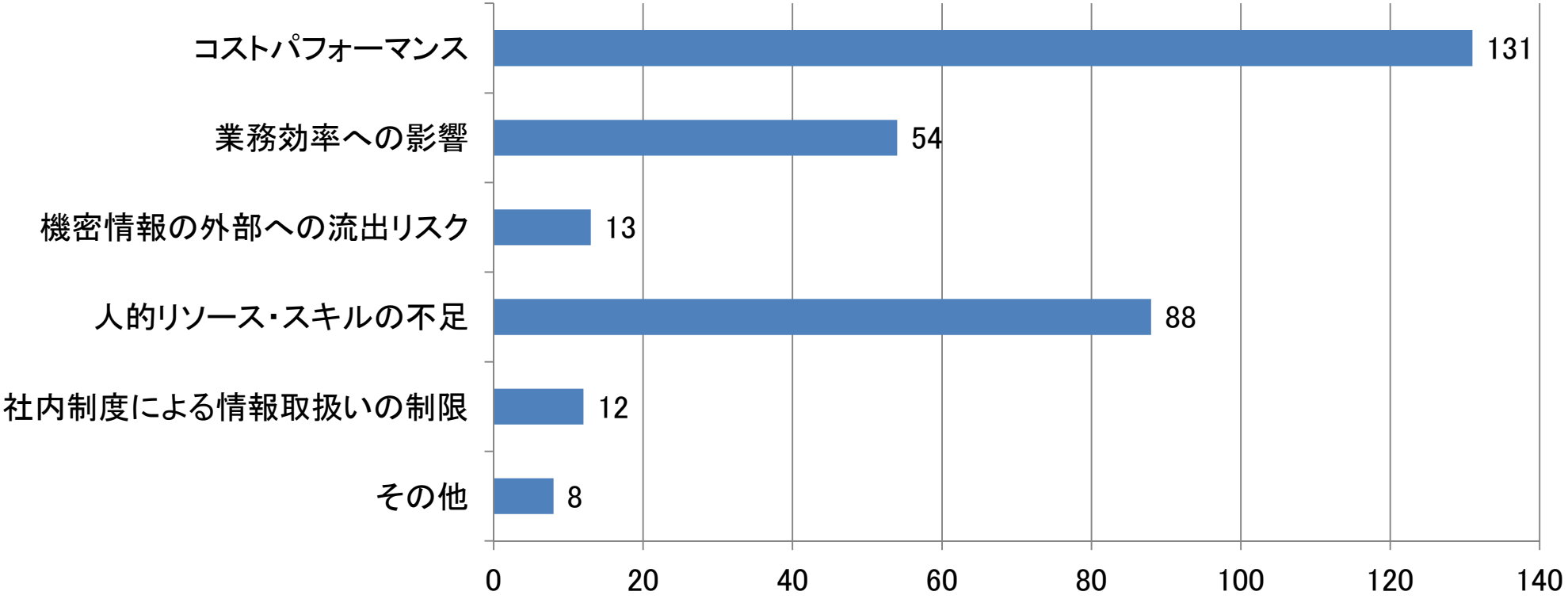
設問72.貴社のデジタル・フォレンジックの効果についてお選びください。(N=178)



実施理由同様、インシデントレスポンスや内部犯行立証に効果を見出している傾向がある。

第4章　デジタルフォレンジックの実態について

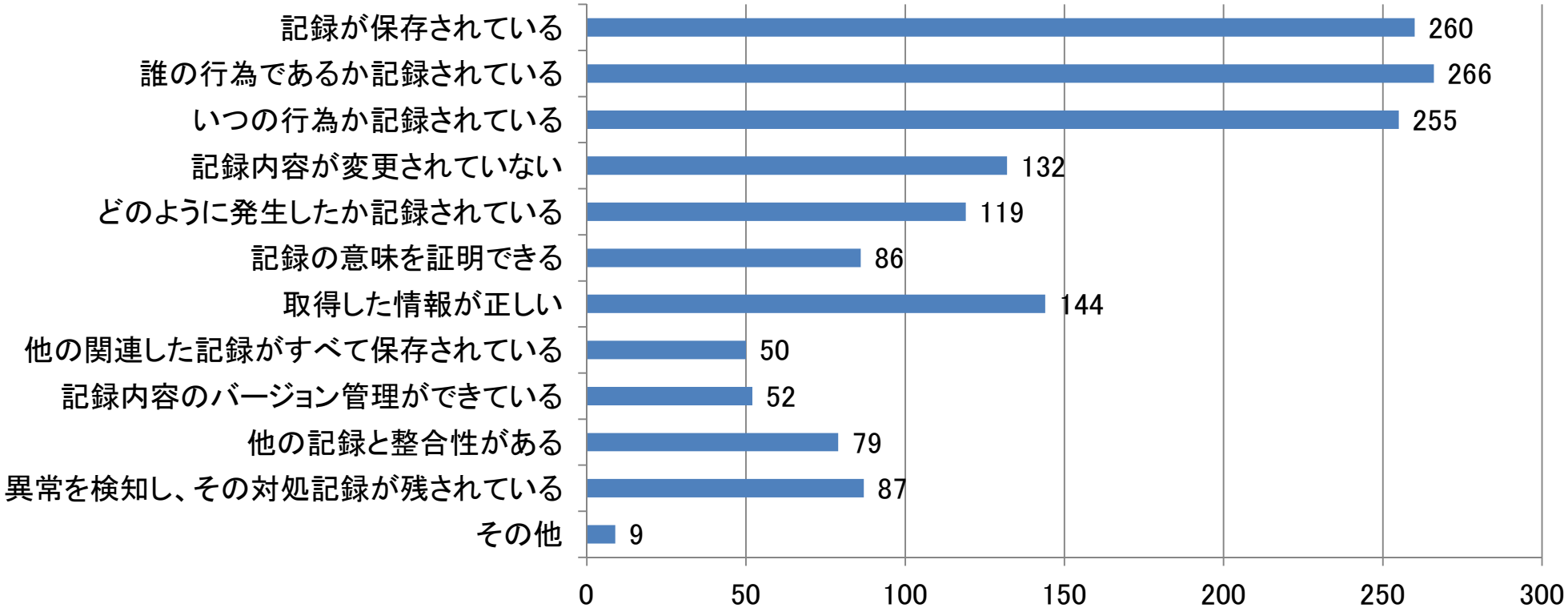
設問73.貴社でのデジタル・フォレンジックの実施における阻害要因をお選びください。（複数回答）(N=184)



「コストパフォーマンス」、「人的リソース・スキル不足」の理由により
DFを実施できていない。

第4章　デジタルフォレンジックの実態について

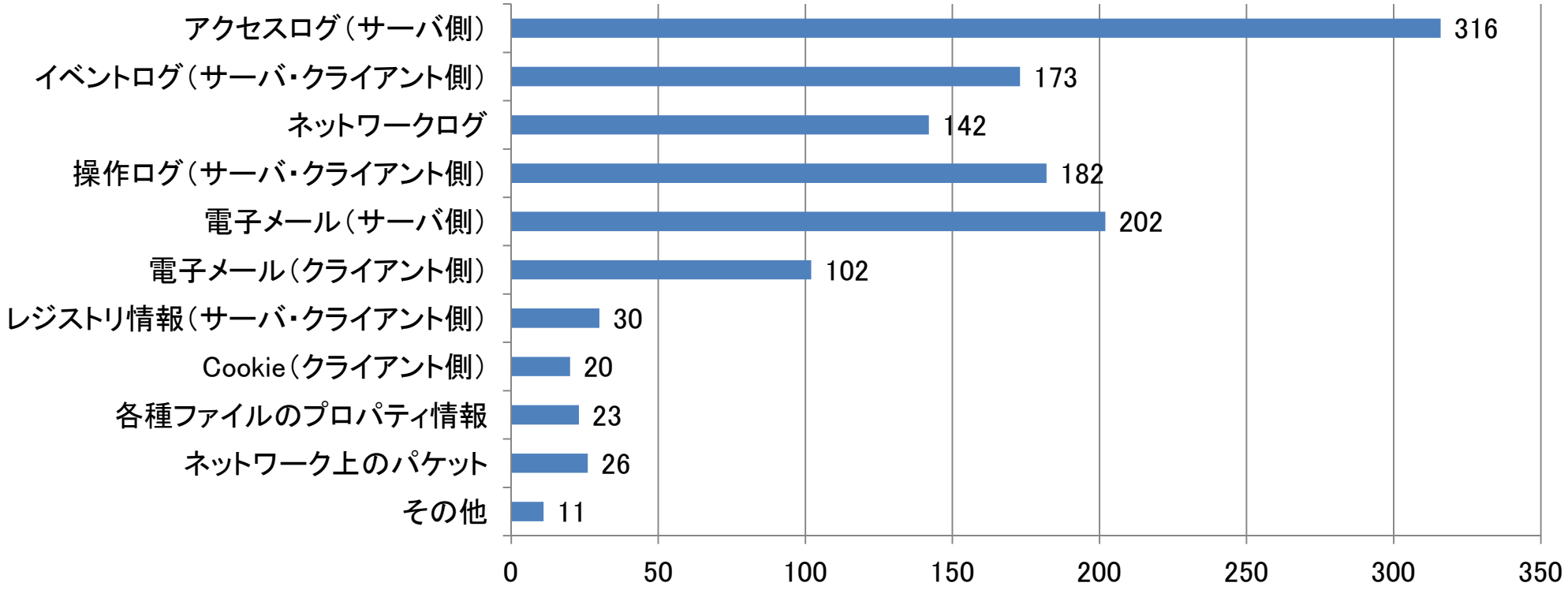
設問74.貴社においてデジタル証拠取得時に重要であると思うものをお選びください。(複数回答)(N=369)



「記録が保存されている」、「誰の行為かの記録」、
「いつの行為かの記録」が多数を占め、他は半数以下である。

第4章　デジタルフォレンジックの実態について

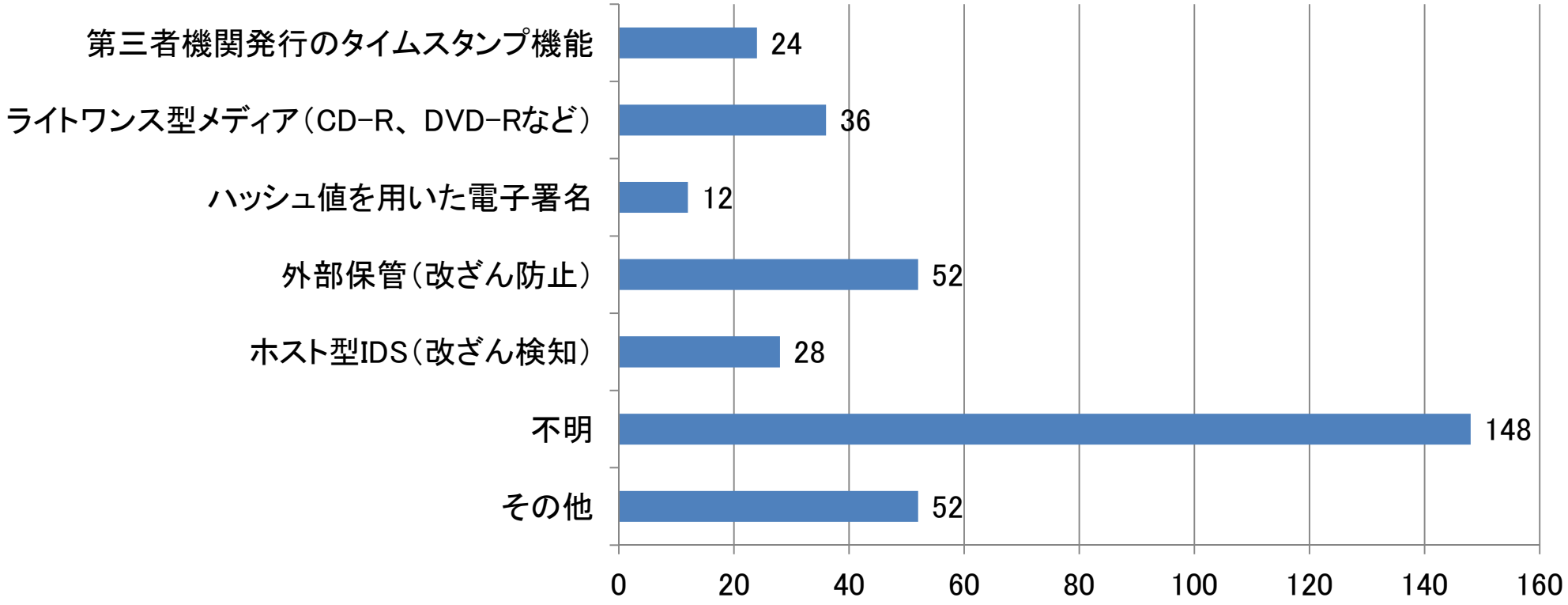
設問75.貴社においてデジタル証拠として有効なデータをお選びください。（複数回答）(N=369)



「アクセスログ」が圧倒的多数となり、次いで「電子メール」や「操作ログ」が証拠として有効なデータと見られている。

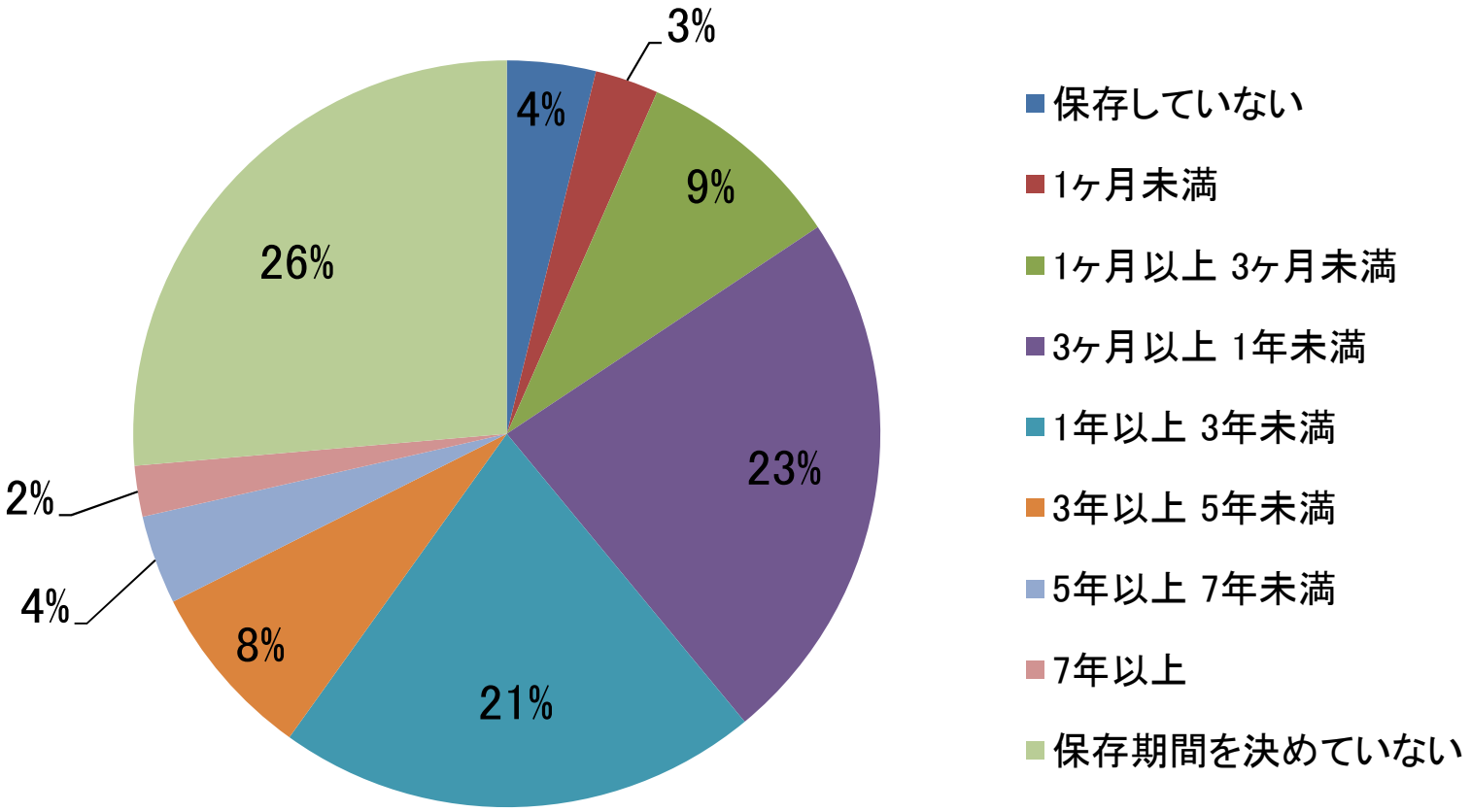
第4章　デジタルフォレンジックの実態について

設問76.貴社のログ管理に導入している機能・手法をお選びください。統合ログ管理ツールを使用している場合は、その機能をお選びください。（複数回答）(N=325)



「不明」の数値が突出している。

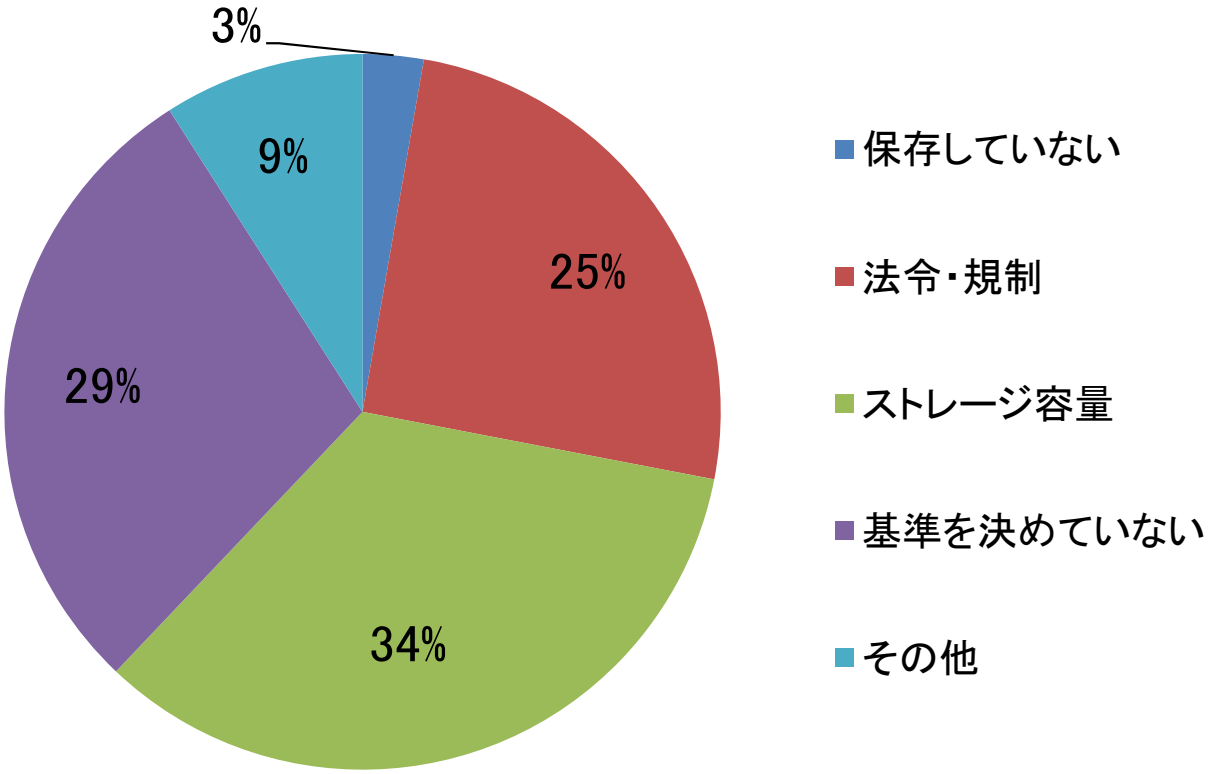
設問77.貴社のログの保存期間をお選びください。(N=364)



「3ヶ月以上1年未満」,「1年以上3年未満」が多く、
「保存期間を決めていない」組織が最多である

第4章　デジタルフォレンジックの実態について

設問78.貴社のログの保存期間を決める基準をお選びください。
(N=364)



「法令・規制」に基づいてる組織もあるが、
「ストレージ容量」,「基準を決めていない」の回答数が多い。

考察（第4章　デジタルフォレンジックの実態について）

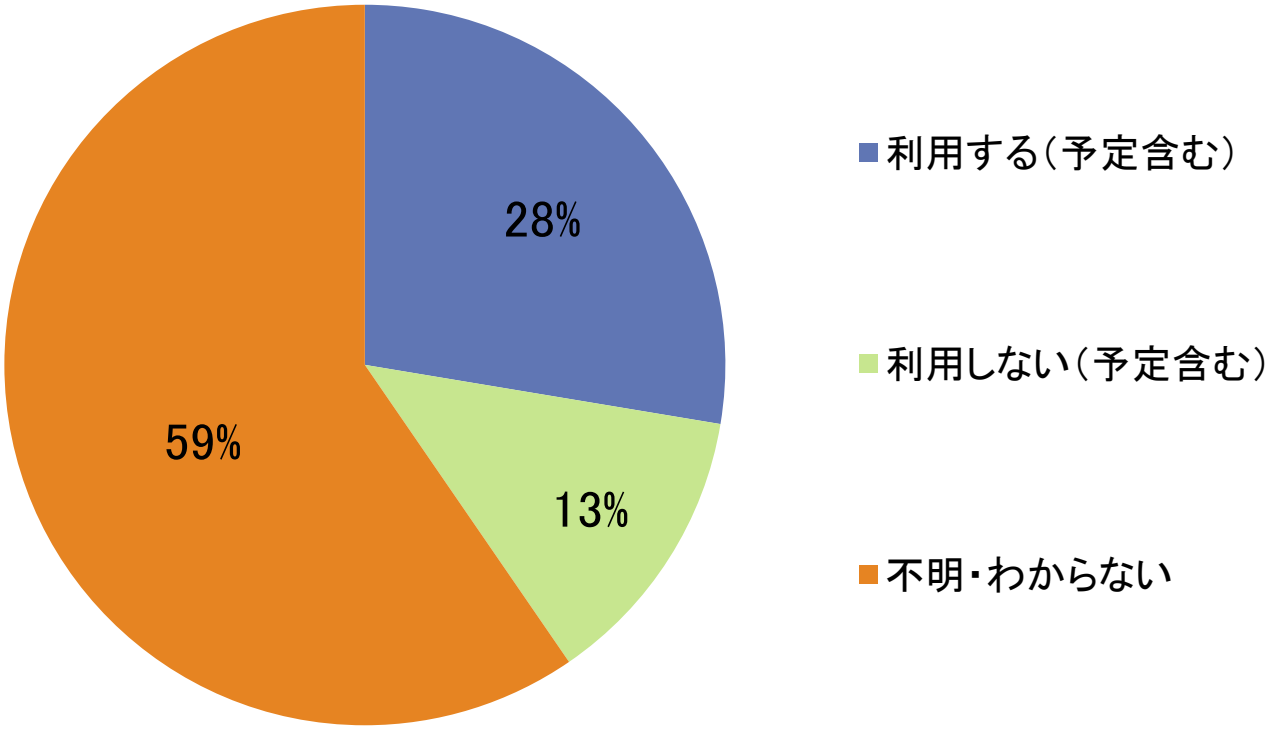
- デジタル・フォレンジックの実施組織は少数だが、検討中や保留している組織を含めると約半数に至る。
- 組織におけるデジタル・フォレンジックには、訴訟対策よりインシデント・レスポンスに効果を見出している。
- デジタル証拠としてアクセスログが有効と回答している組織が多数あるものの、導入しているログ管理・手法が不明と回答している組織が多い。
- ログの保存期間が、「3か月～3年」、「決めていない」組織が多く、その基準がストレージ容量に依る、もしくは「決めていない」組織が多数である。

第5章

共通番号制度について

第5章　共通番号制度について

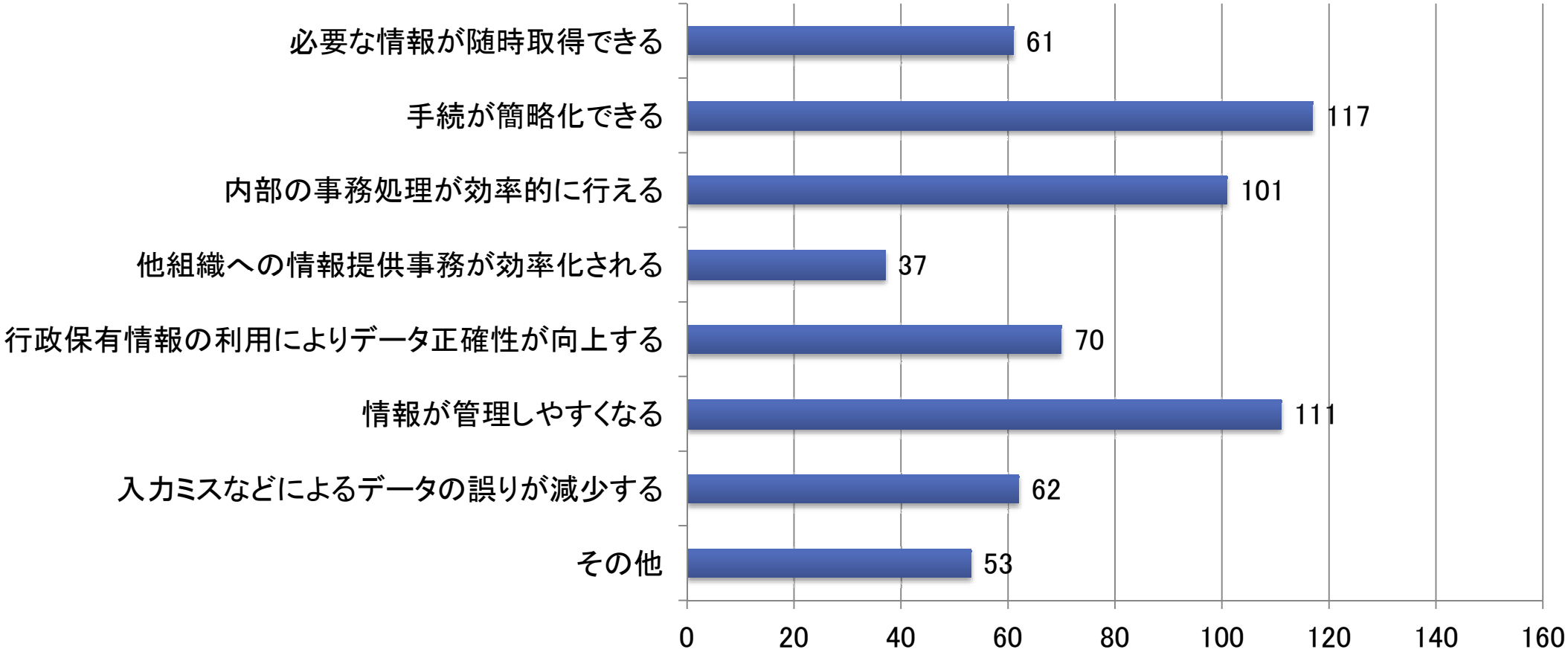
設問79.「国民ID」や「社会保障・税に関わる番号」などの共通番号が導入された場合（民間企業でも使えるようになった場合）、貴社の業務で利用しますか。（N=391）



番号制度の認知が低く、自業務への影響を想定していない組織が多い

第5章　共通番号制度について

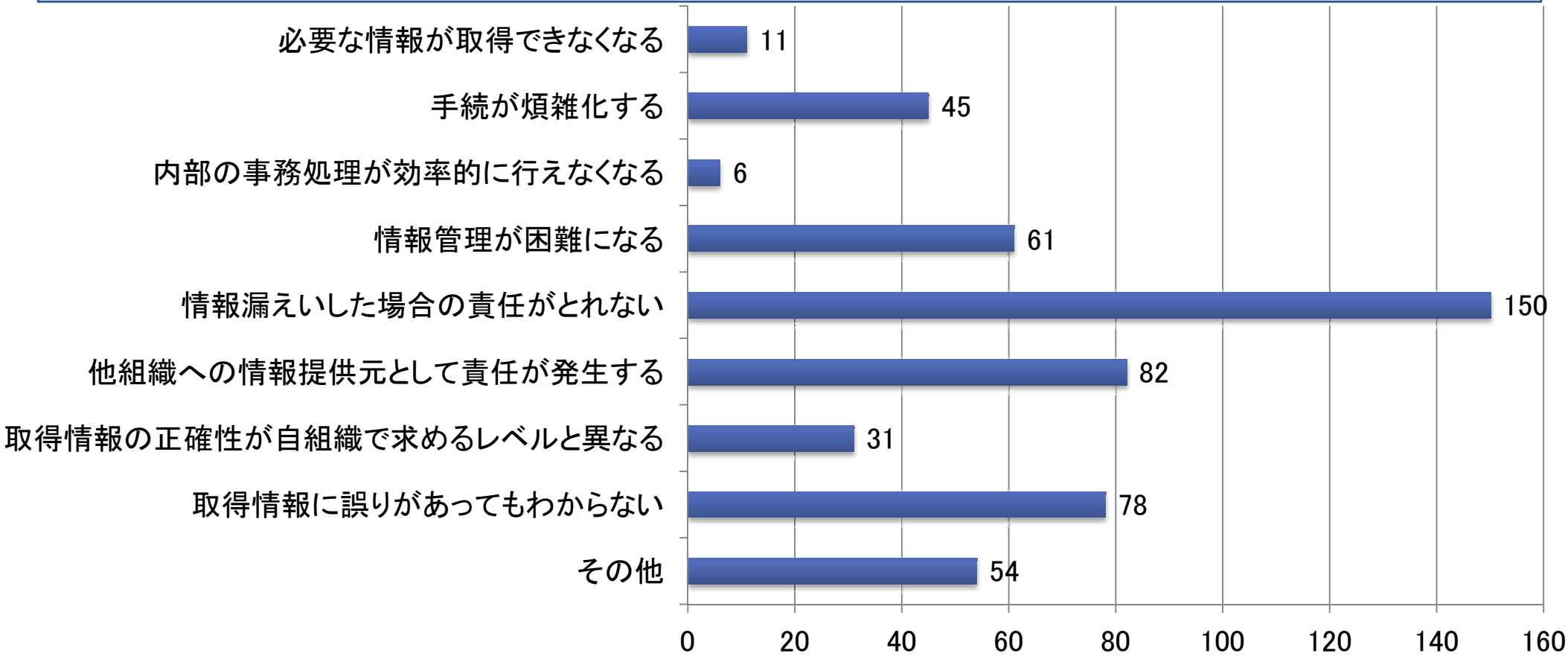
設問80.貴社の業務で共通番号を利用する場合どのようなメリットがありますか。（複数回答）（N=313）



効率化への期待が大きいが、正確化への期待はそれほど大きくない

第5章　共通番号制度について

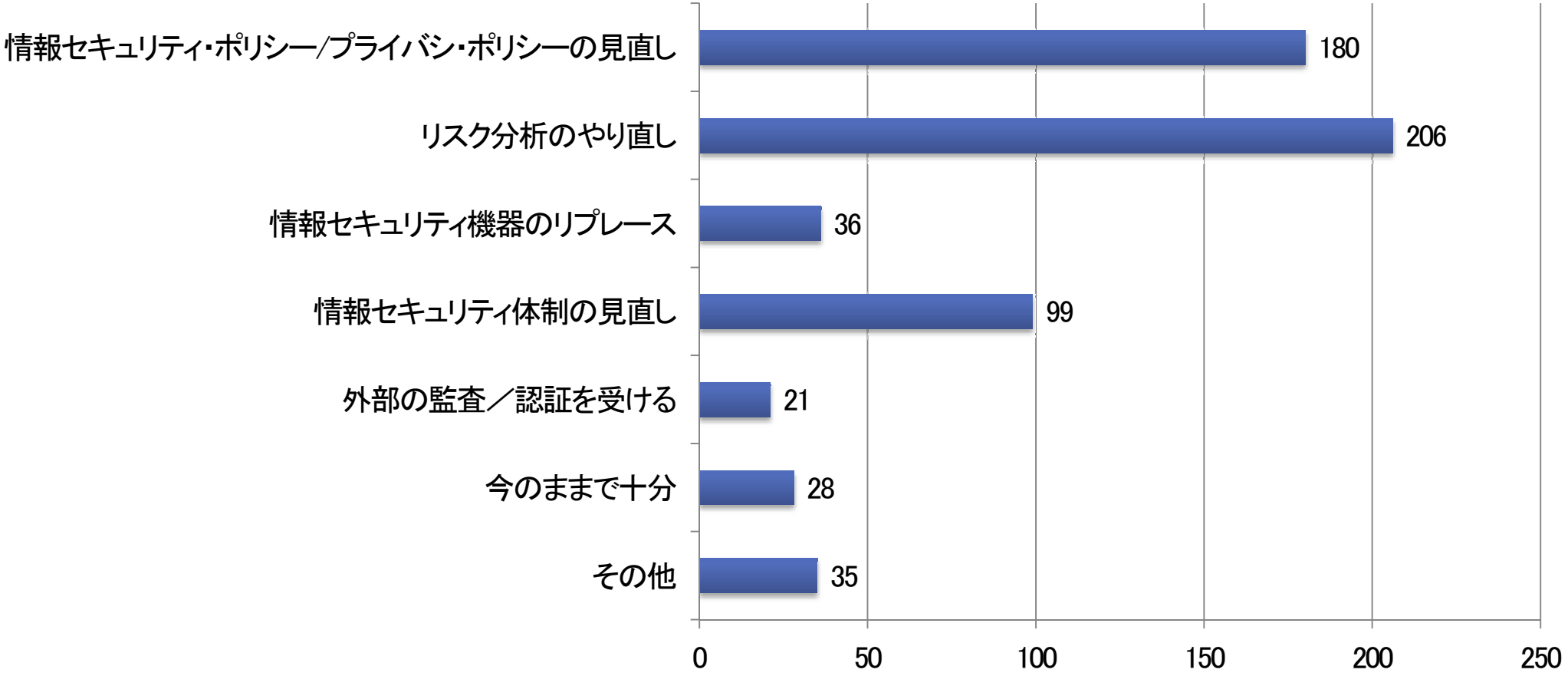
設問81.貴社の業務で共通番号を利用する場合どのような懸念がありますか。（複数回答）（N=305）



情報漏えいへの懸念がとりわけ多い

第5章　共通番号制度について

設問82.貴社の業務で共通番号を利用する場合どのような対策が必要となりますか。（複数回答）（N=332）

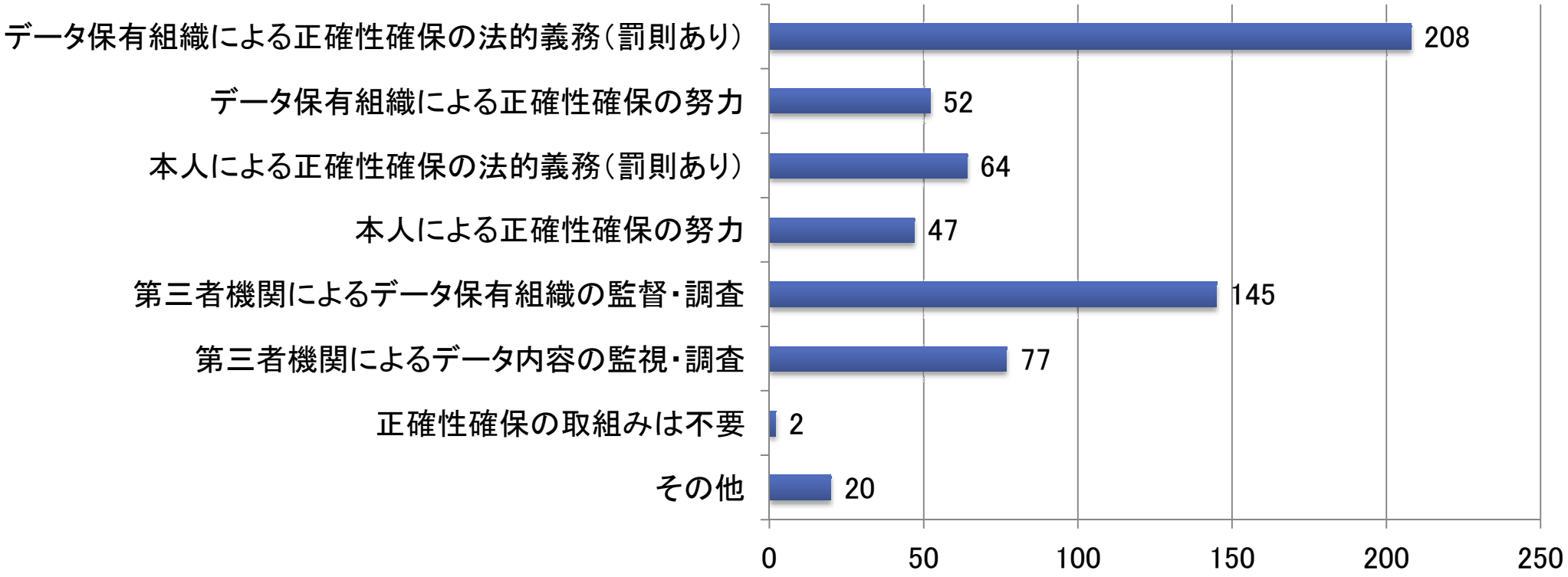


情報漏えいに対する対策が念頭にあると思われる

第5章　共通番号制度について

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

設問83.番号制度においてデータの正確性を確保するために有効と思われる取組みはどのようなものと考えますか。（2つまで選択可）（N=343）



正確性確保には強制力を持った取り組みが必要と考える組織が多い

考察（第5章　共通番号制度について）

- 番号制度の導入が自組織の業務に影響するかどうかイメージできていない組織が多い（設問79）。

- 番号制度が導入されることによる効率性向上への期待は大きいが、正確性向上への期待はそれほど高くない（設問80）。

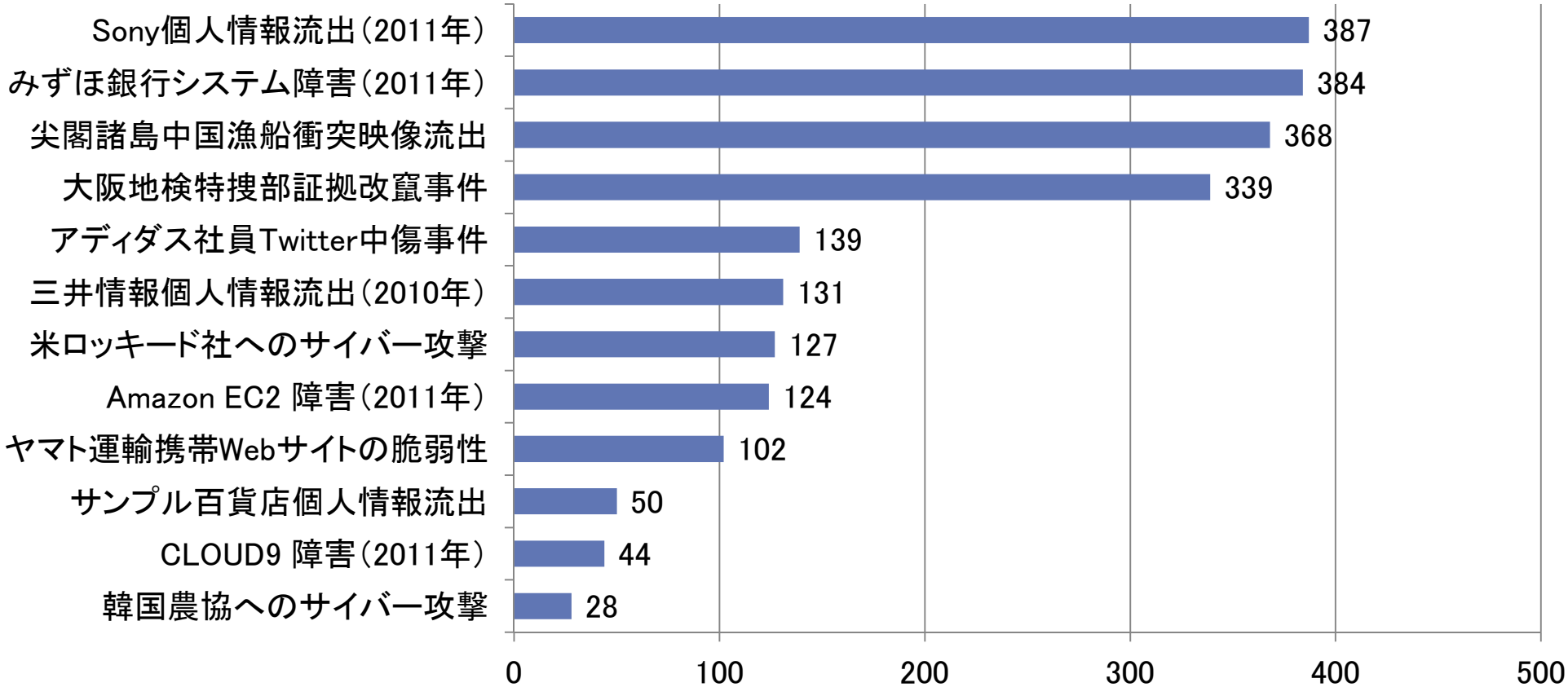
- むしろ正確なデータが取得できるか、提供できるか、についての懸念がある（設問81）。

- 正確性確保に必要な取組みとして、「データ保有組織による義務（罰則あり）」や「第三者機関による監督・調査」をあげる回答が多かったことから、何かしらの強制力を伴った取組みが必要と考えている組織が多いといえる（設問83）。

第6章

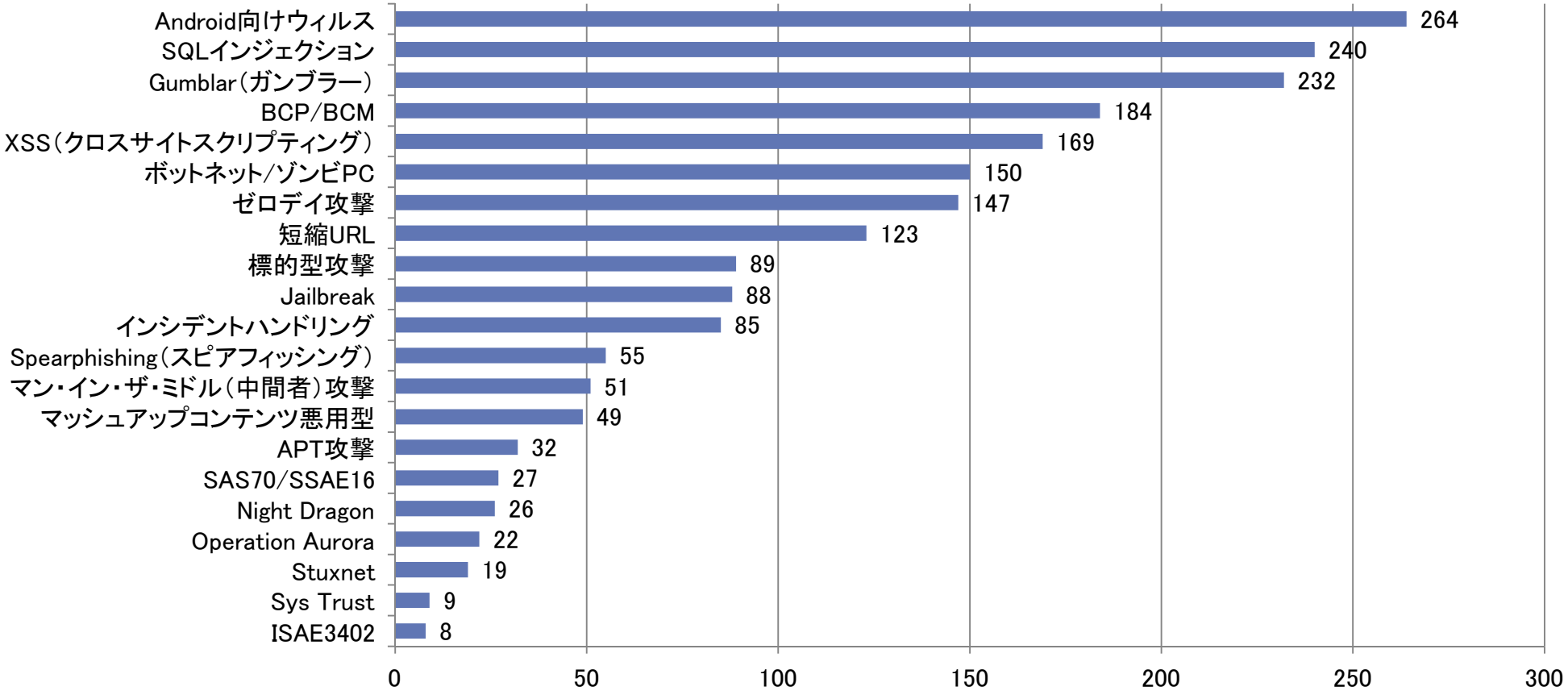
その他

設問84.次の出来事について、ご存知のものをご選択ください。
（複数回答）（N=401）



特定の分野への偏りは少なく、出来事の有名度に比例している。

設問85.次の用語について、ご存知のものをご選択ください。
（複数回答）（N=347）



標的型攻撃や監査関連の用語の知名度が低い傾向にある。