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

2015年情報セキュリティアンケート調査結果

2015年12月19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

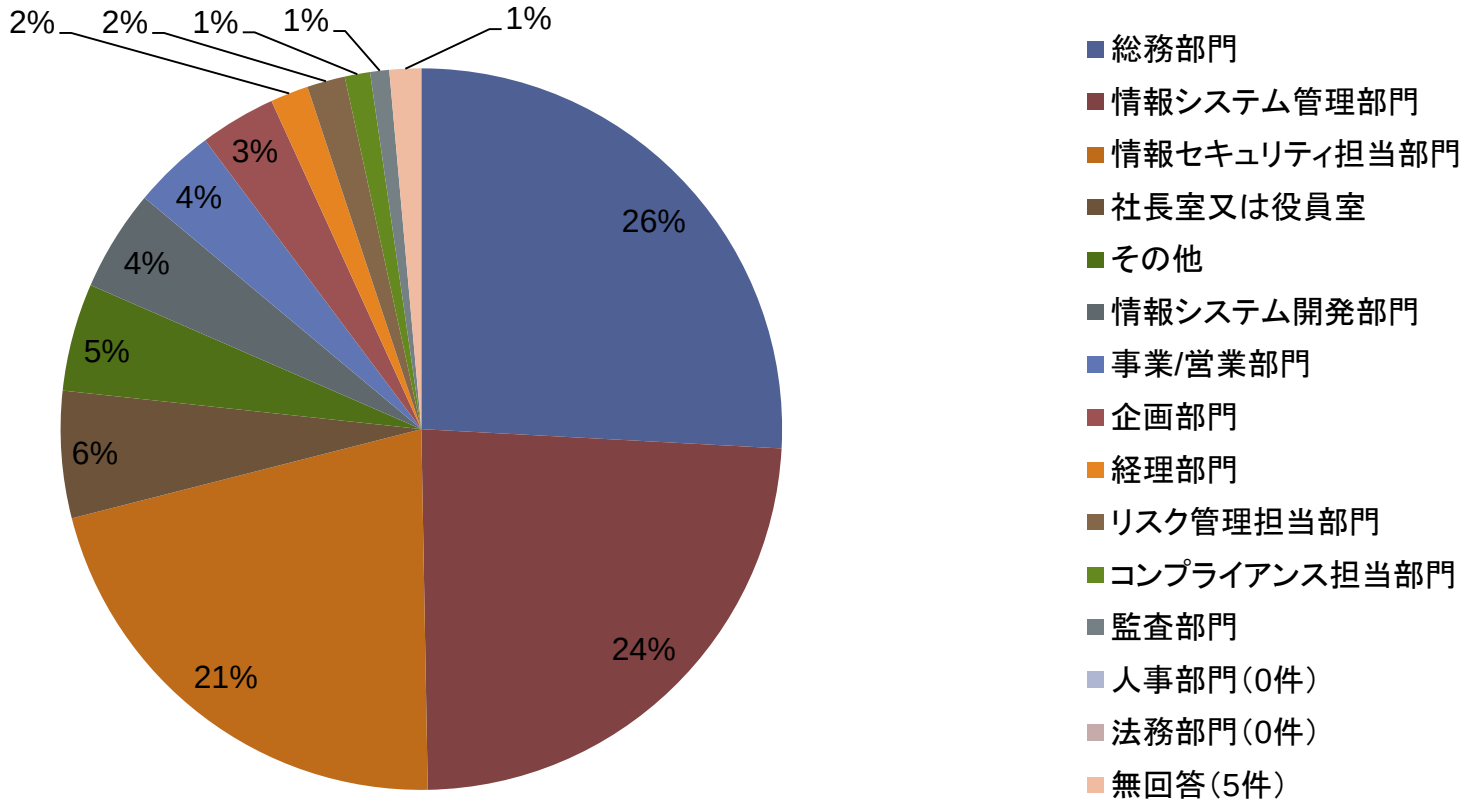
- アンケート実施期間
  2015年7月30日～8月31日
- アンケート対象
  Pマーク取得企業、ISMS認証取得企業、BCMS認証取得企業、官公庁、教育機関(以下「組織」という。)など4,500組織の情報セキュリティ関係者
- アンケート内容
  情報セキュリティマネジメントの取組状況、(例外措置や運用、管理者権限等)、リスクの認識と支出の動向、事業継続に関わる実施状況、組織内の電子データ管理、大規模情報漏えい事故に関する個人情報管理、過去の事例・事故や用語の認知度について
- 調査方法
  郵送による
- 回答状況
  352件(送達確認できた4,373組織に対して8.0%)

第1章
概要（回答者の基本データ等）

第1章　概要（回答者の基本データ等）

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

設問1. 回答者の所属(N=352)

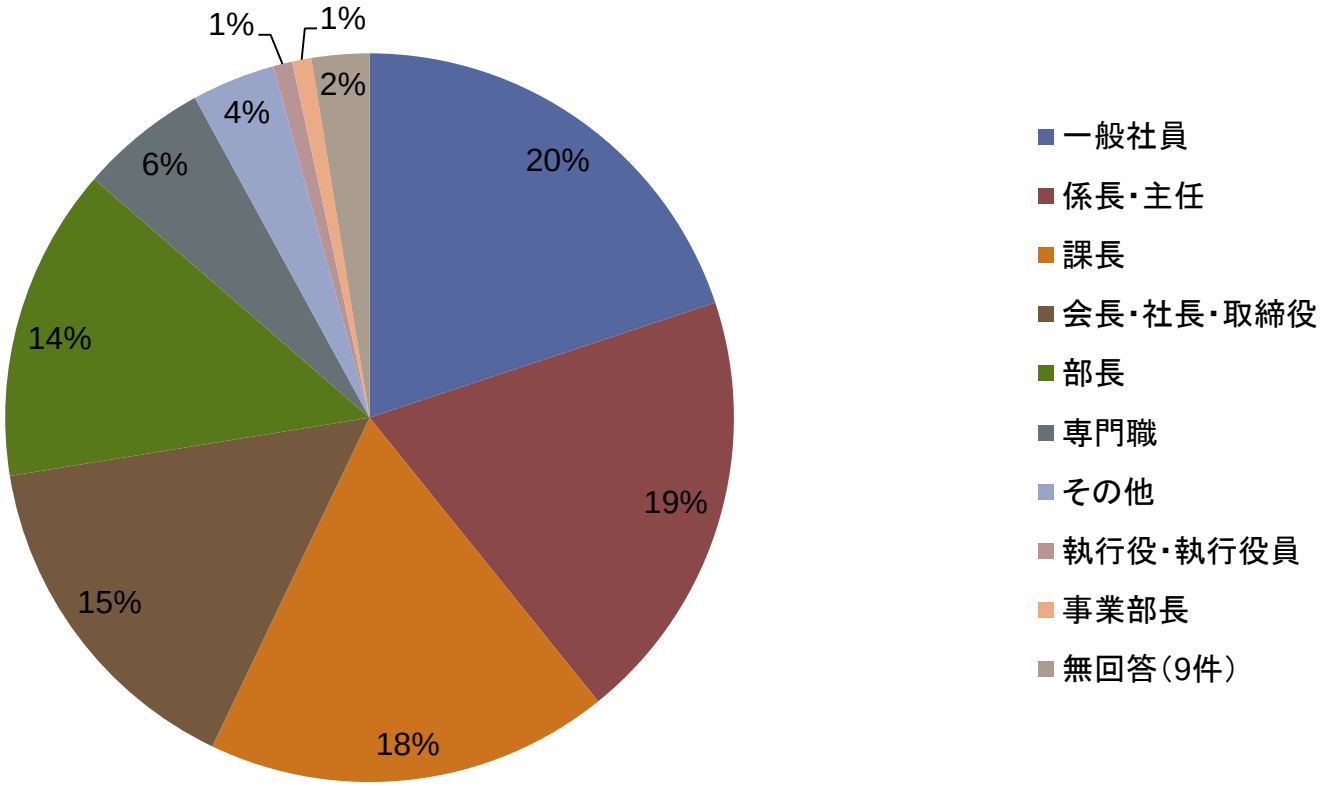


所属部門は、総務部門、情報システム管理部門、
情報セキュリティ担当部門の順に多かった。

第1章　概要（回答者の基本データ等）

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

設問2. 回答者の役職(N=352)

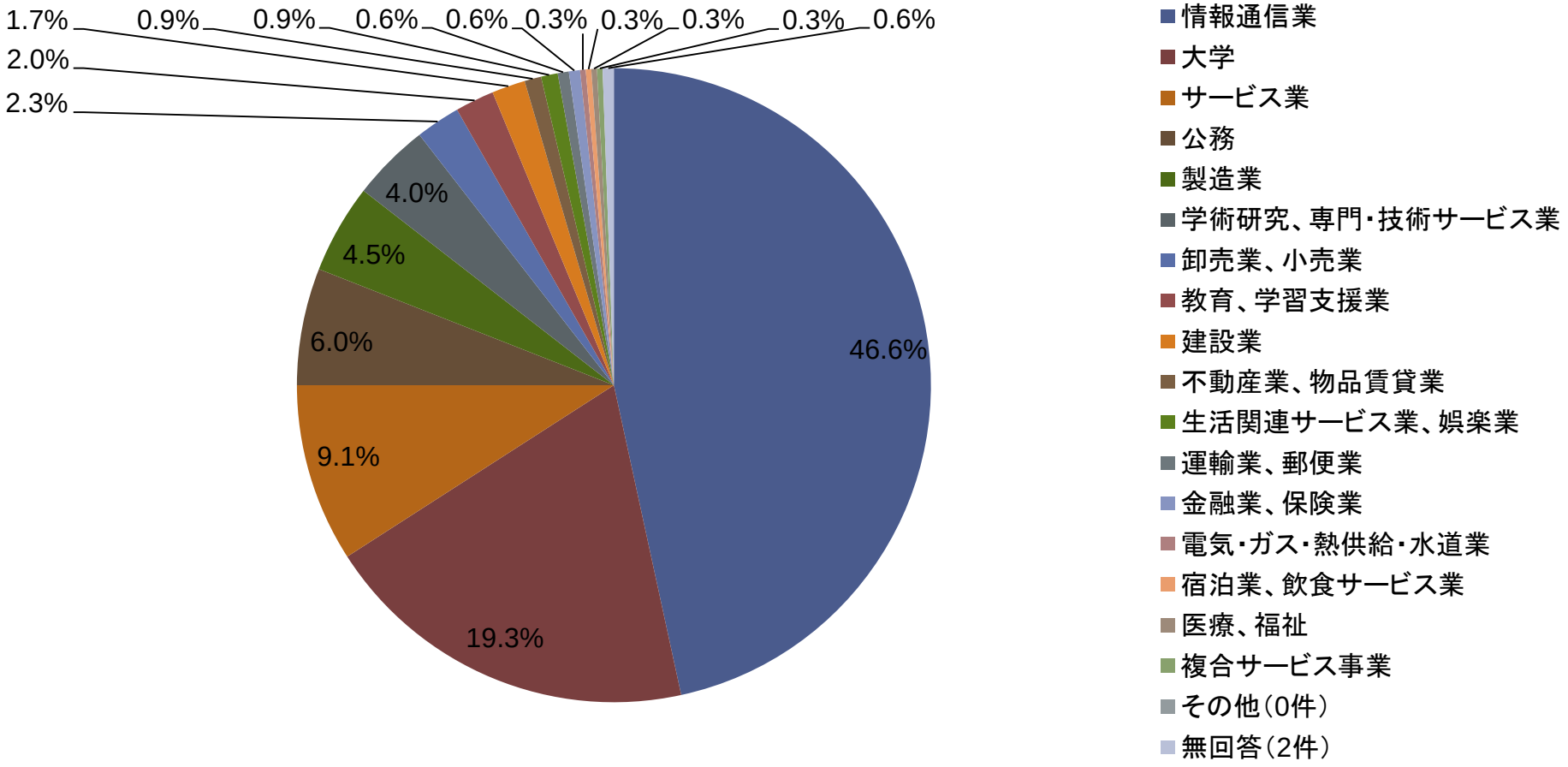


回答者は、一般社員が一番多く、
係長・主任、課長、会長・社長・取締役と続く。

第1章　概要（回答者の基本データ等）

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

設問3. 回答組織の業種(N=352)



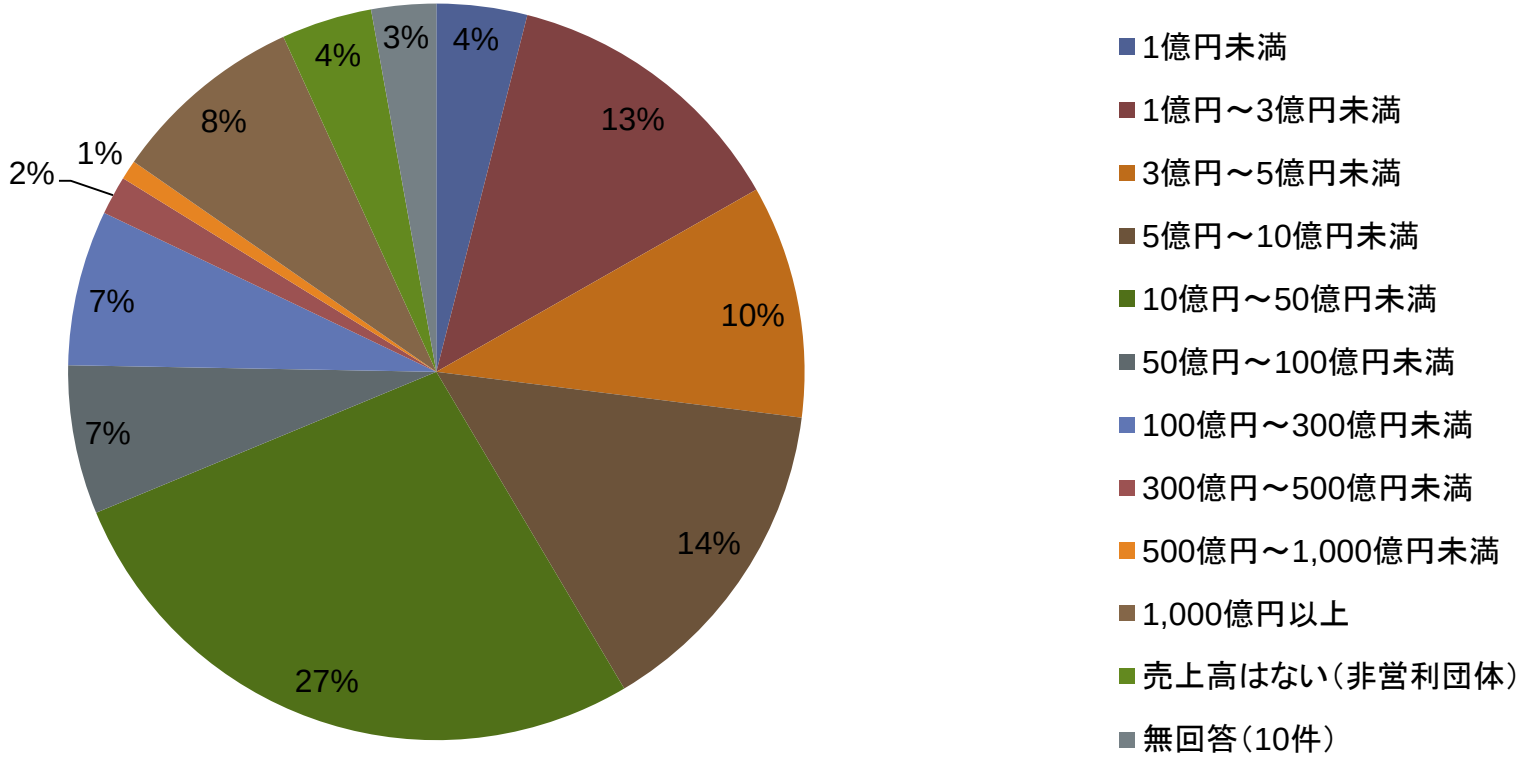
情報通信業が47%と半数近い割合となっている。

第1章　概要（回答者の基本データ等）

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

設問4. 年間売上高（単独）（N=352）

※大学・官公庁等は予算額、銀行は経常収益高、保険は収入保険料または正味保険料、証券は営業収入高で算出

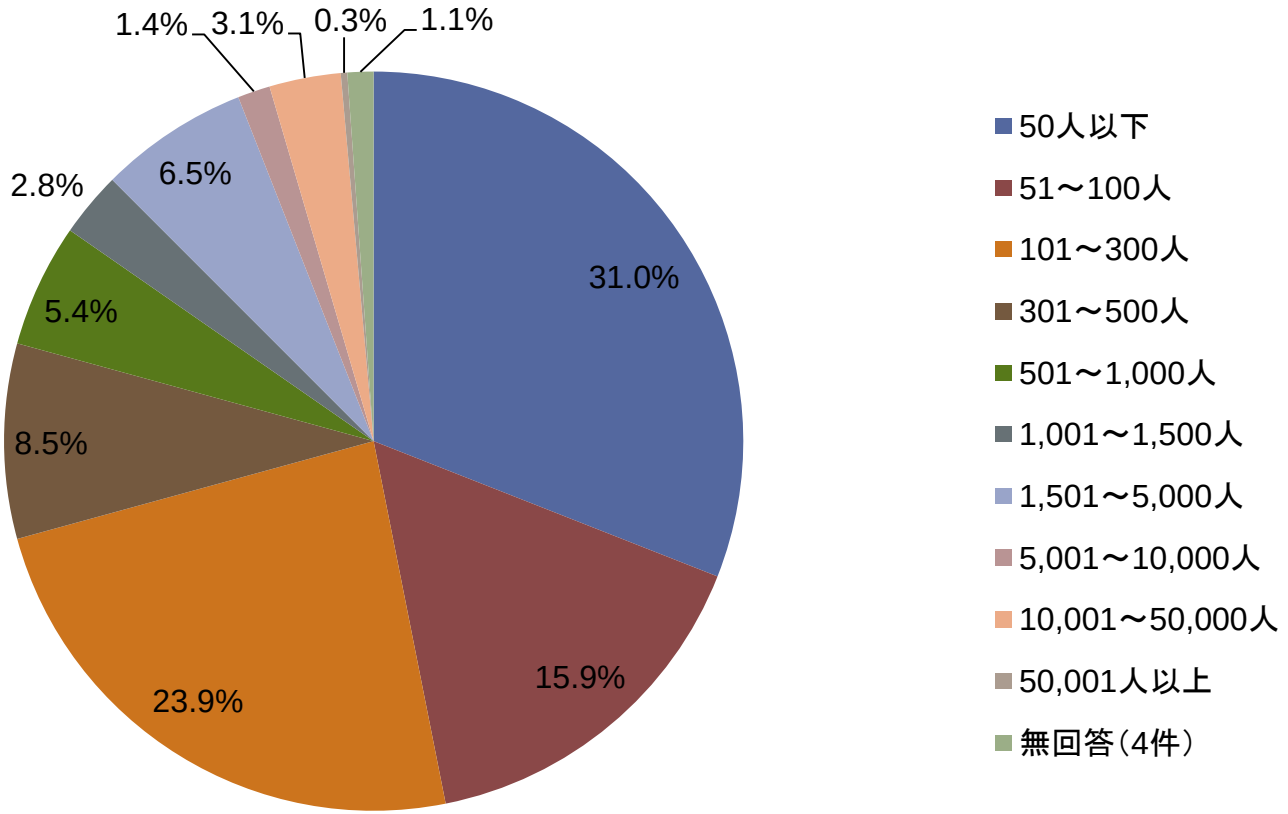


売上高10億円から50億円未満の組織が一番多い。

第1章　概要（回答者の基本データ等）

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

設問5. 全従業員数(N=352)

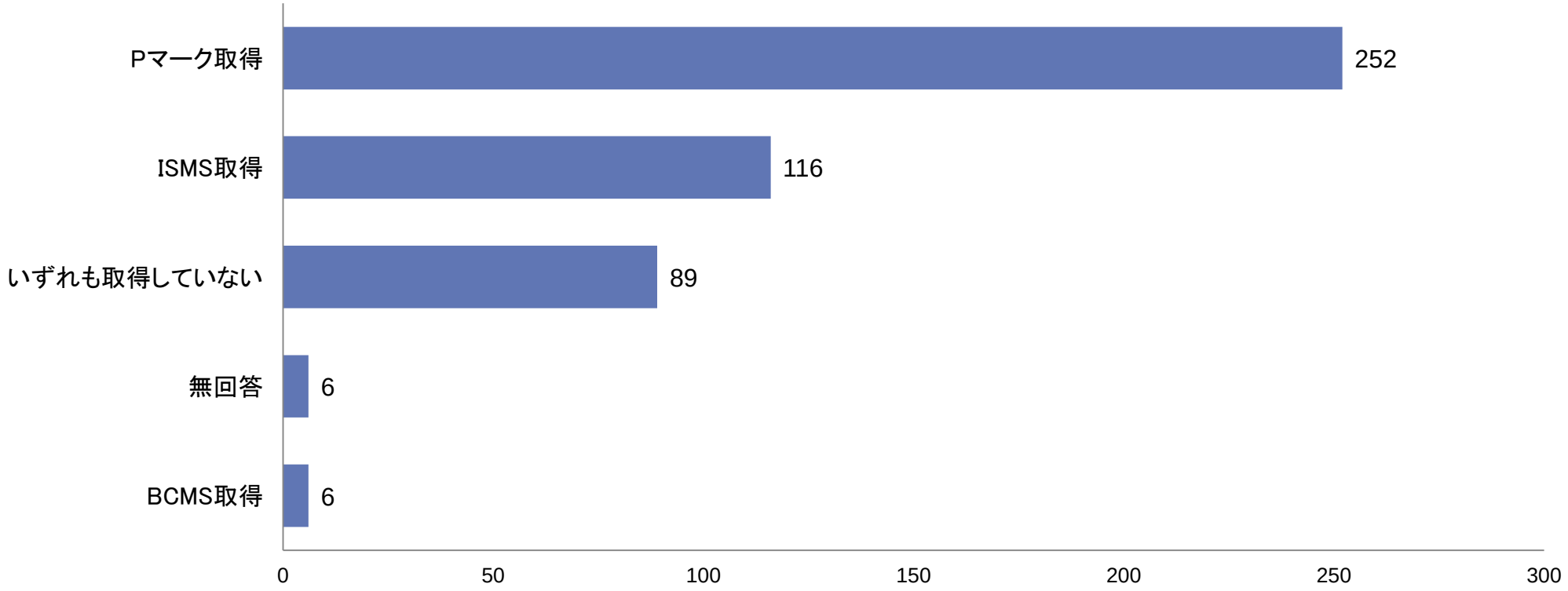


従業員数50人以下の組織が最も多い。
101～300人の組織が2番目に多く、51～100人の組織が3番目に多い。

第1章　概要（回答者の基本データ等）

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

設問6. プライバシーマーク、ISMS、BCMSの取得状況（複数回答）（N=352）



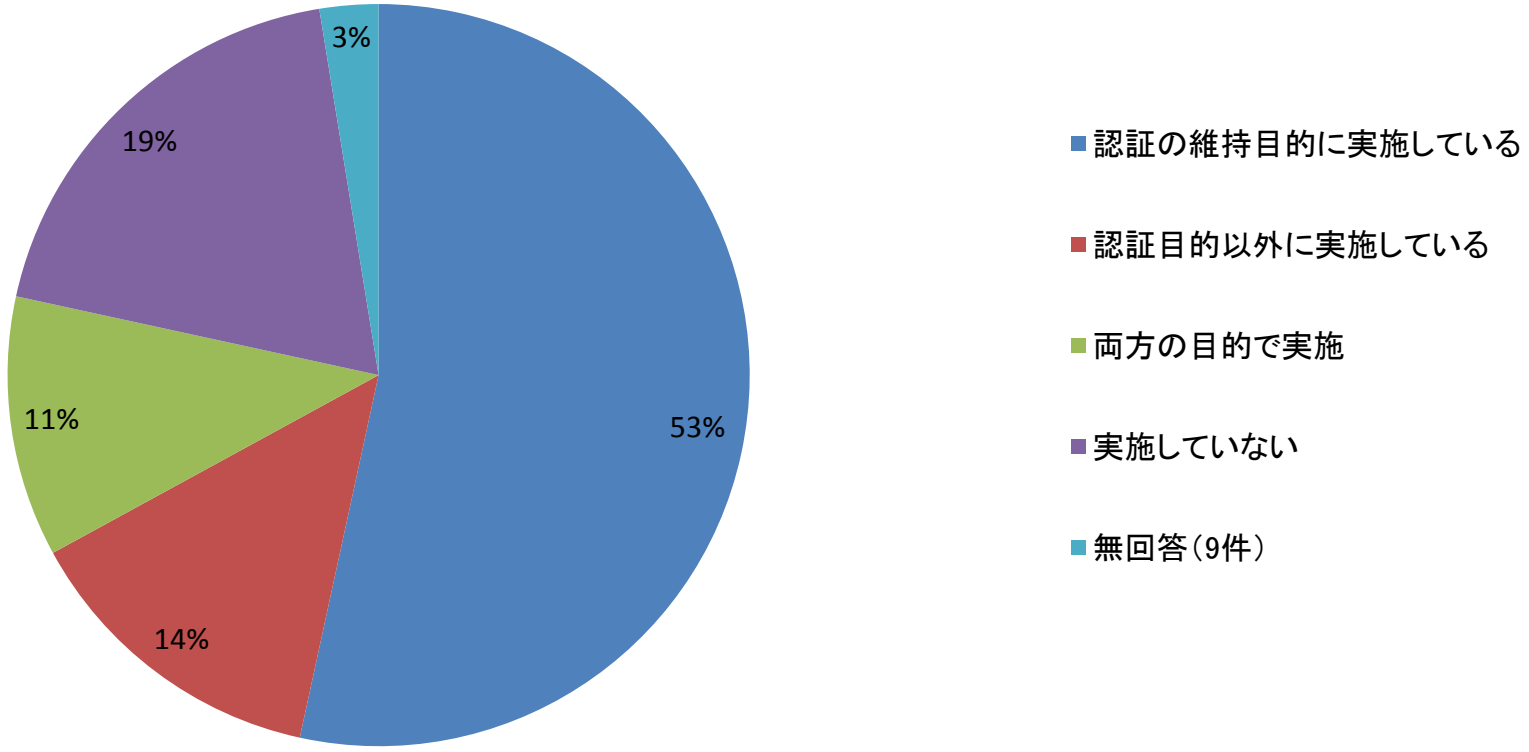
252組織がPマークを取得している。116組織がISMSを取得している。
6組織がBCMSを取得している。

※　アンケートに回答頂いた組織のうち、すべての企業はPマーク、もしくは、PマークとISMSの両方を取得している。

第1章　概要（回答者の基本データ等）

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

設問7. 情報セキュリティ監査の実施状況(N=352)



53%が認証の維持目的、14%が認証目的以外、11%が両方の目的で情報セキュリティ監査を実施している。

考察(第1章　概要(回答者の基本データ等))

- 情報通信業が半数に近い割合を占めている。

- 売上高10億円から50億円未満の組織が全体の27%と一番多い。売上高50億円未満の組織は68%であった。

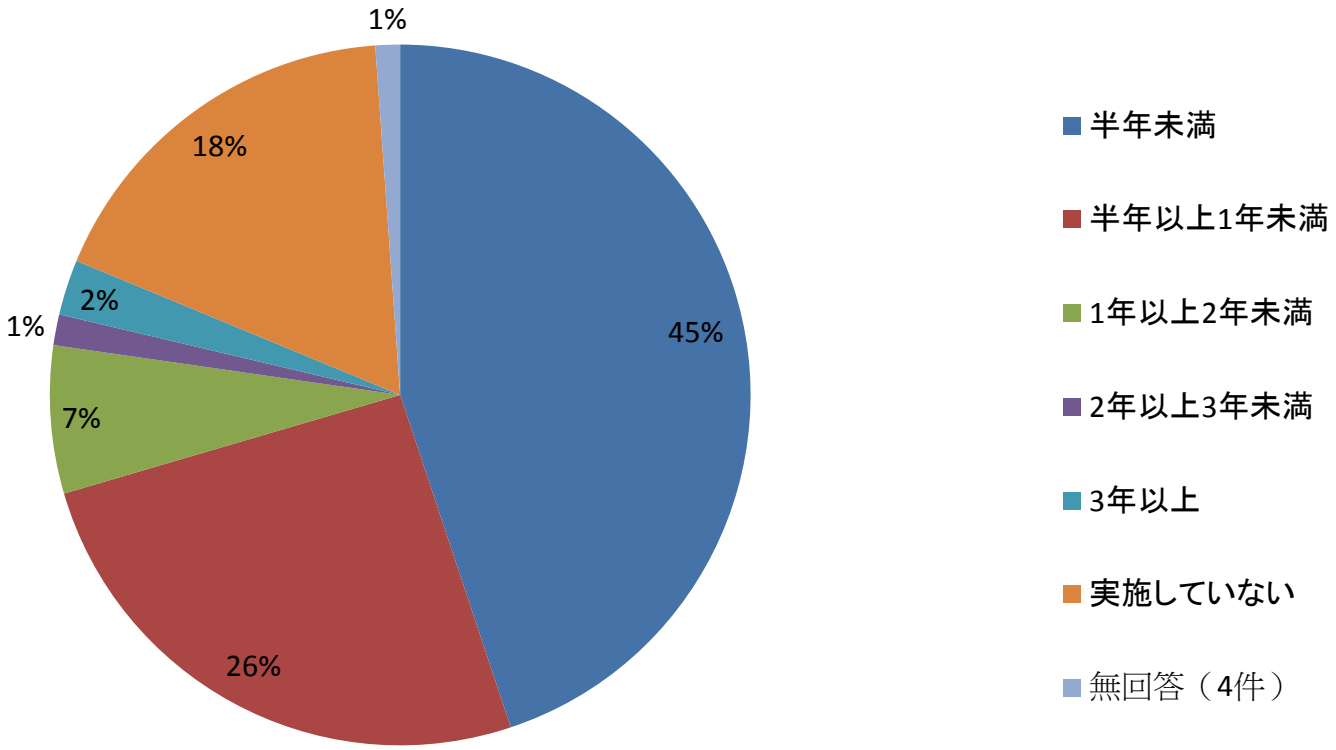
- アンケートに回答いただいた組織の傾向としては、従業員数50人以下の組織が最も多い。101～300人の組織が2番目に多く、51～100人の組織が3番目に多い。

第２章
情報セキュリティマネジメントの
取組み状況について

第2章　情報セキュリティマネジメントの取組み状況

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

設問8. 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？(N=352)

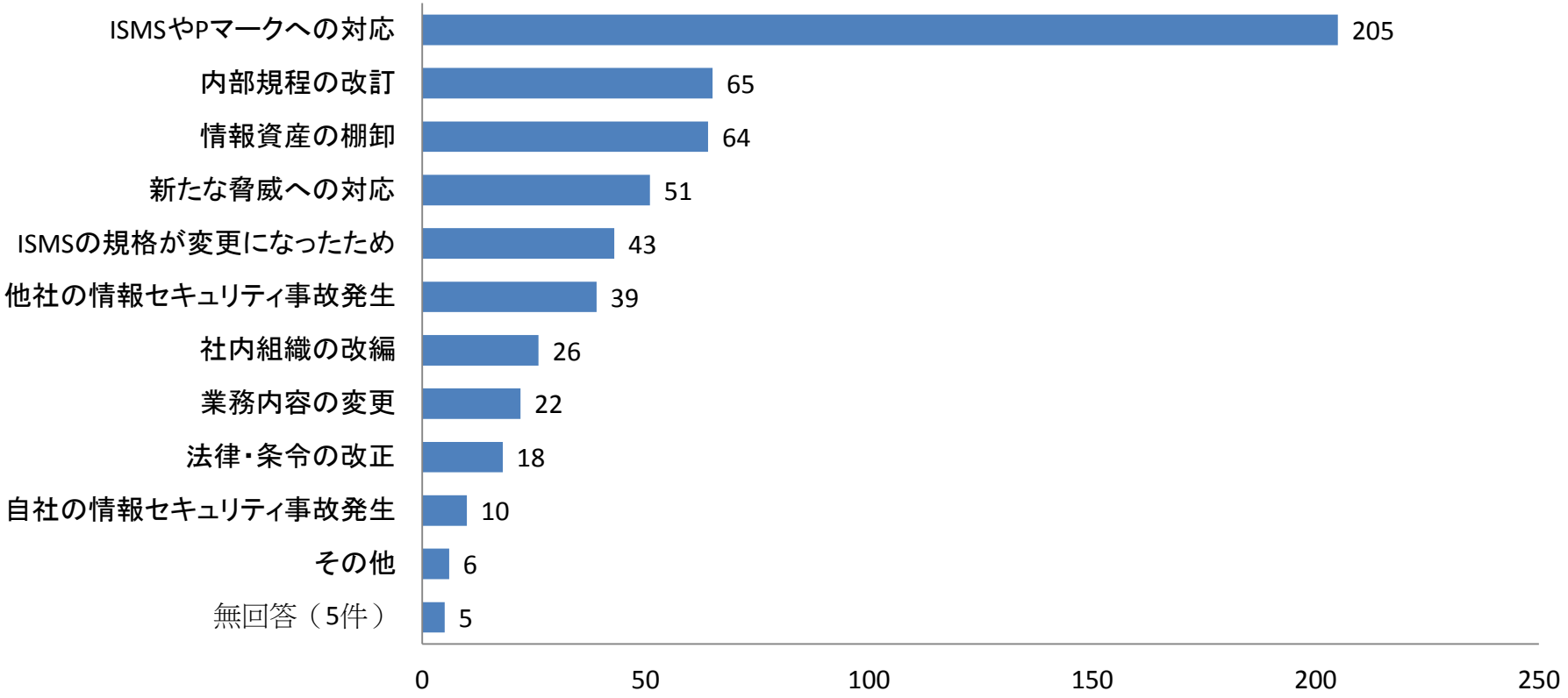


1年未満に実施している組織が71%を占める。
一方、実施していない組織は18%ある。

第2章　情報セキュリティマネジメントの取組み状況

※設問 8 で「(**リスク分析を**)**実施していない**」と回答した組織を除く

設問9. リスク分析を実施した理由(複数回答可　N=290)

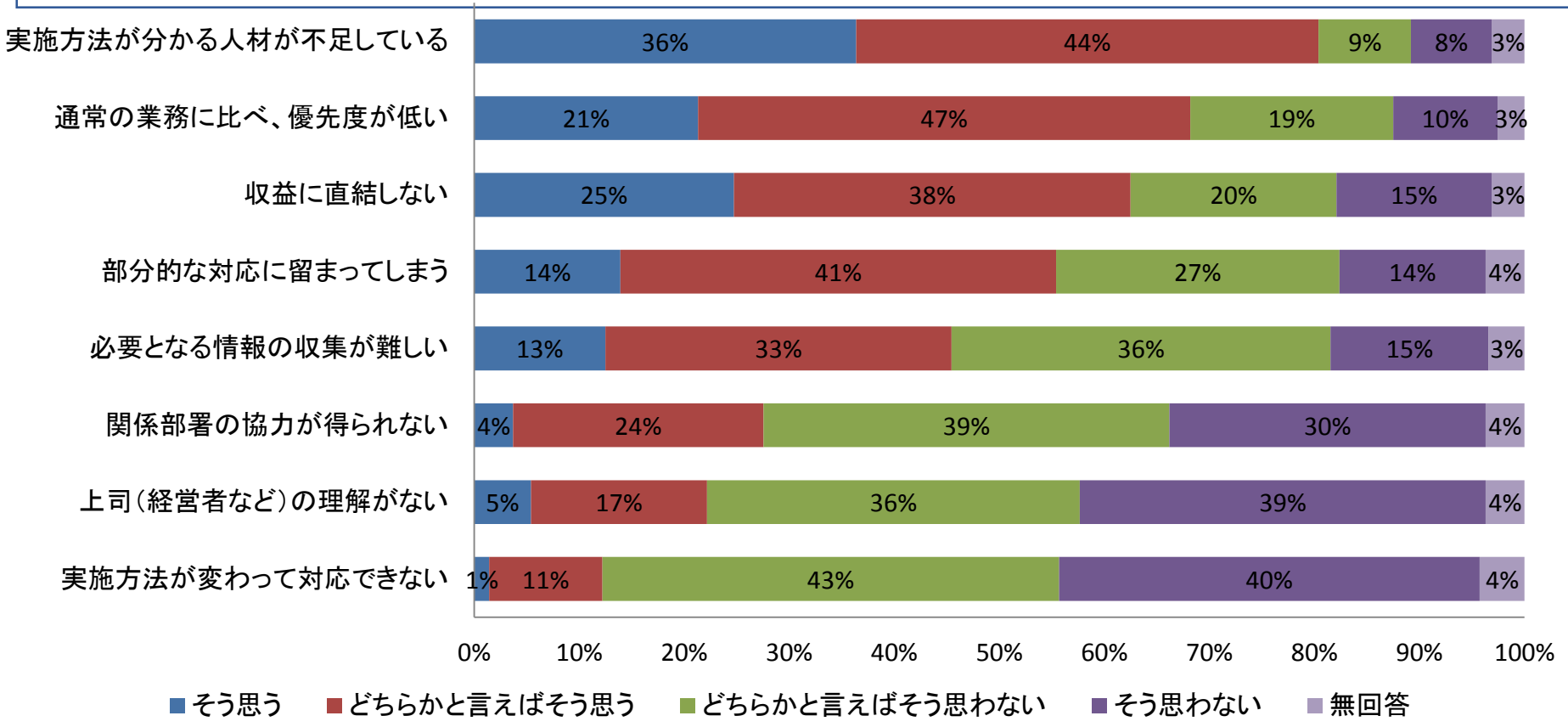


多くの組織が「ISMSやPマークへの対応」を実施理由として挙げている。
「内部規程の改訂」、「情報資産の棚卸」が続いている。

第2章　情報セキュリティマネジメントの取組み状況

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

設問10. リスク分析を行う際の問題点(N=352)
（そう思う、どちらかと言えばそう思うが多い順）

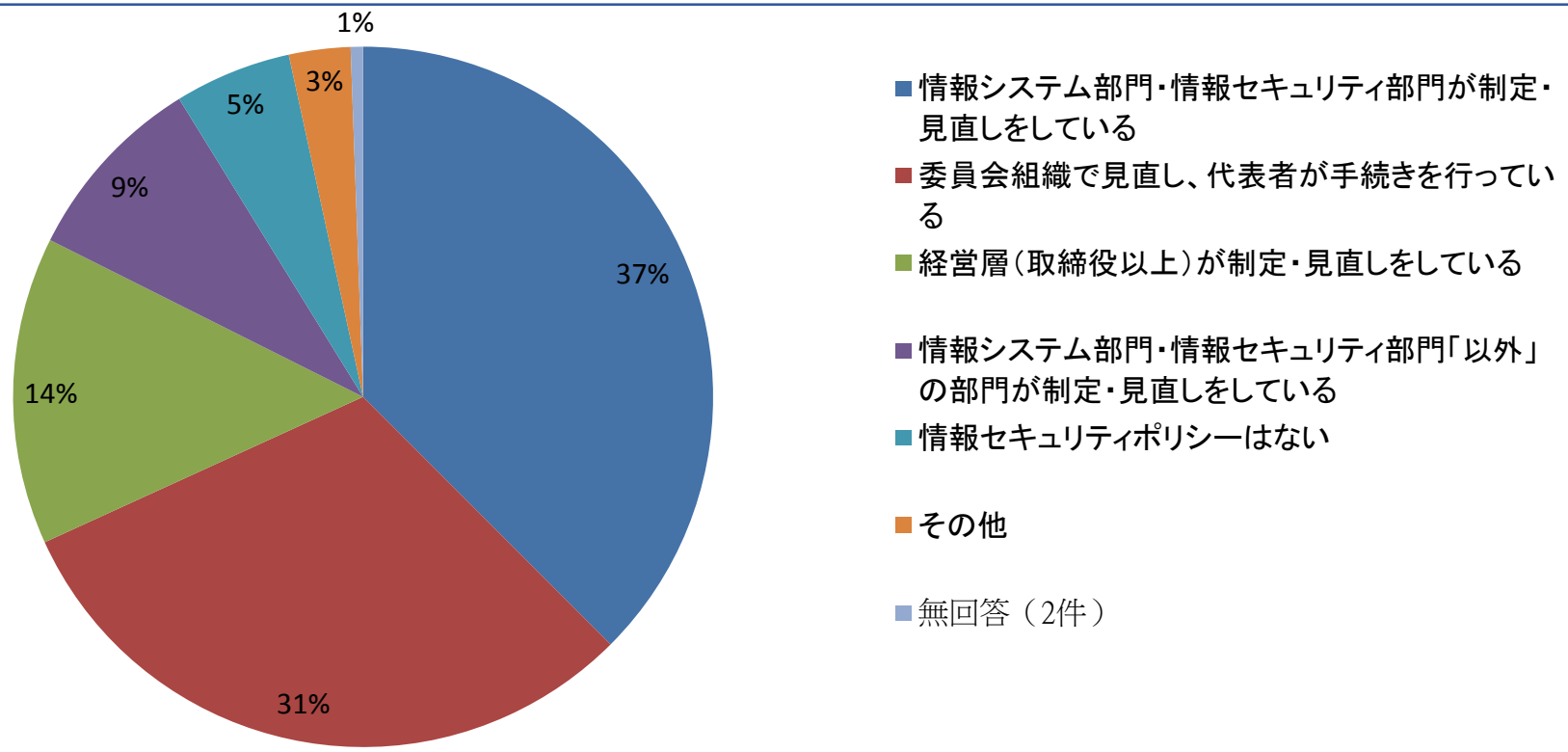


「実施方法が分かる人材が不足している」と答えた組織が多かった。

第2章　情報セキュリティマネジメントの取組み状況

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

設問11. 情報セキュリティポリシー(全体)の制定・見直しの手続きを行っている部門はどこか (N=352)

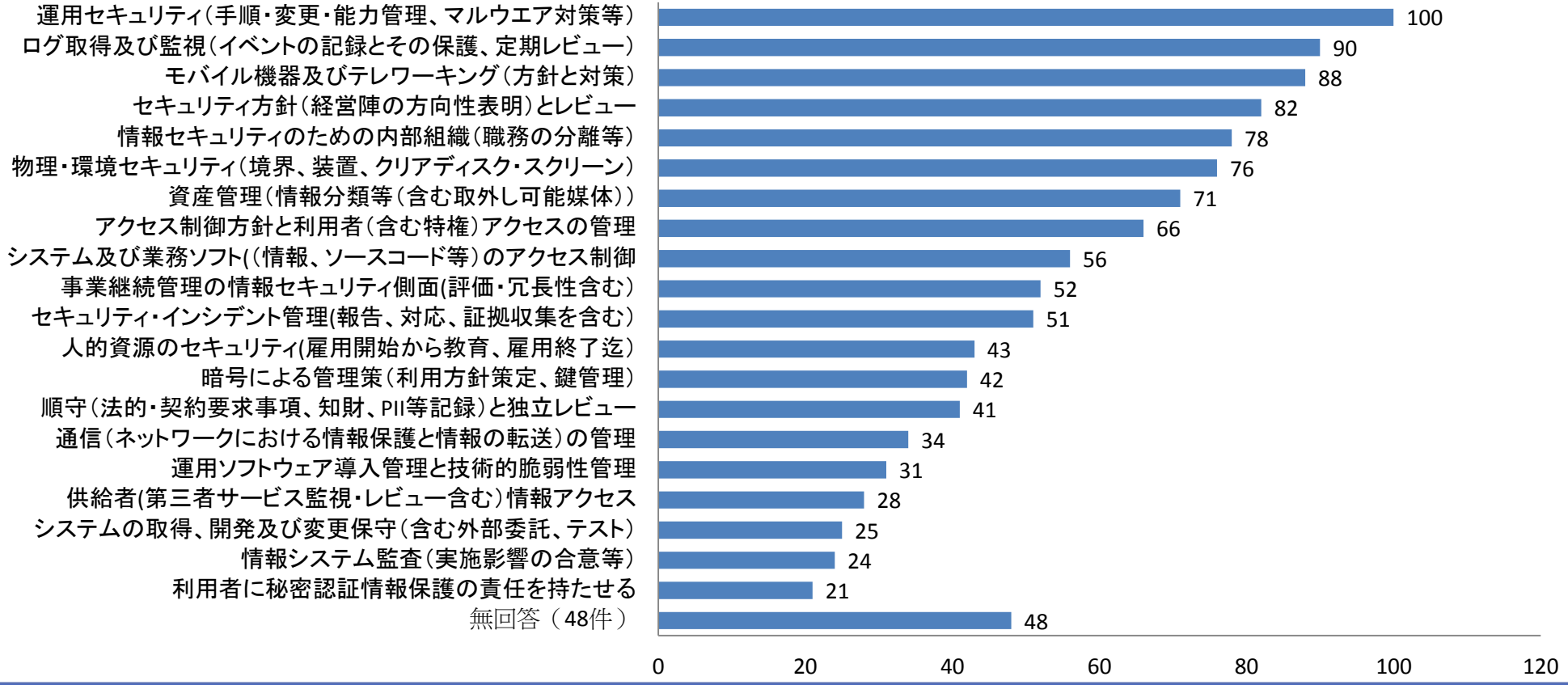


「情報システム部門・情報セキュリティ部門」で制定・見直ししている組織が37%と多い。
「委員会組織で見直し、代表者が手続きを行っている」組織が31%と続く。

第2章　情報セキュリティマネジメントの取組み状況

※設問 11で「**情報セキュリティポリシーはない**」と回答した組織を除く

設問12. 2013年10月以降で新規導入・見直しした管理策(複数回答可　N=333)

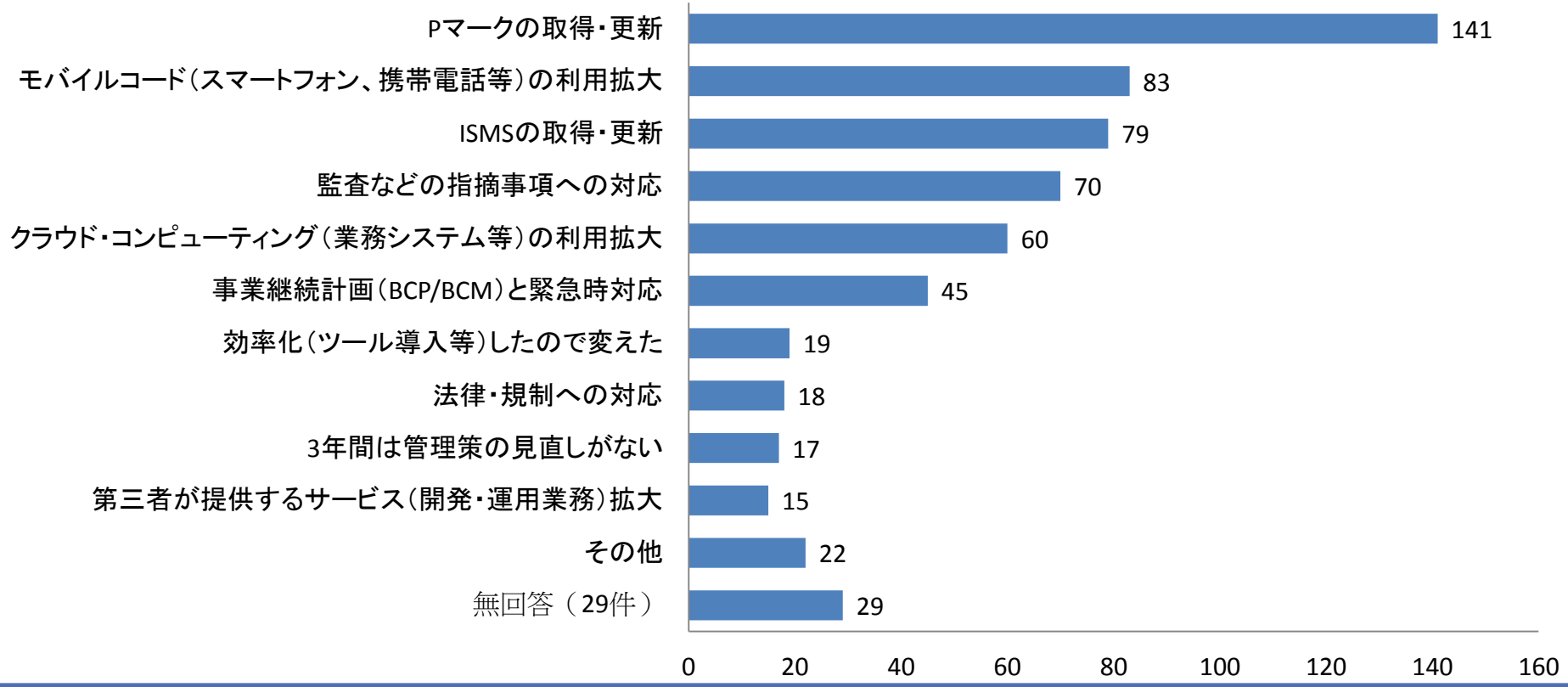


「運用セキュリティ」、「ログ取得及び監視」、「モバイル機器及びテレワーキング」に関する管理策項目の見直しを行っている組織が多い。

第2章　情報セキュリティマネジメントの取組み状況

※設問 11で「**情報セキュリティポリシーはない**」と回答した組織を除く

設問13. 管理策を新規導入・見直しした理由(複数回答可　N=333)



情報セキュリティポリシー（管理策）を新規導入・見直した理由は、「Pマーク取得・更新」、「モバイルコード（スマートフォン等）の利用拡大」、「ISMSの取得・更新」の順である。3年間は管理策見直しがない組織は17件であった。

考察 （第2章　情報セキュリティマネジメントの取組み状況）

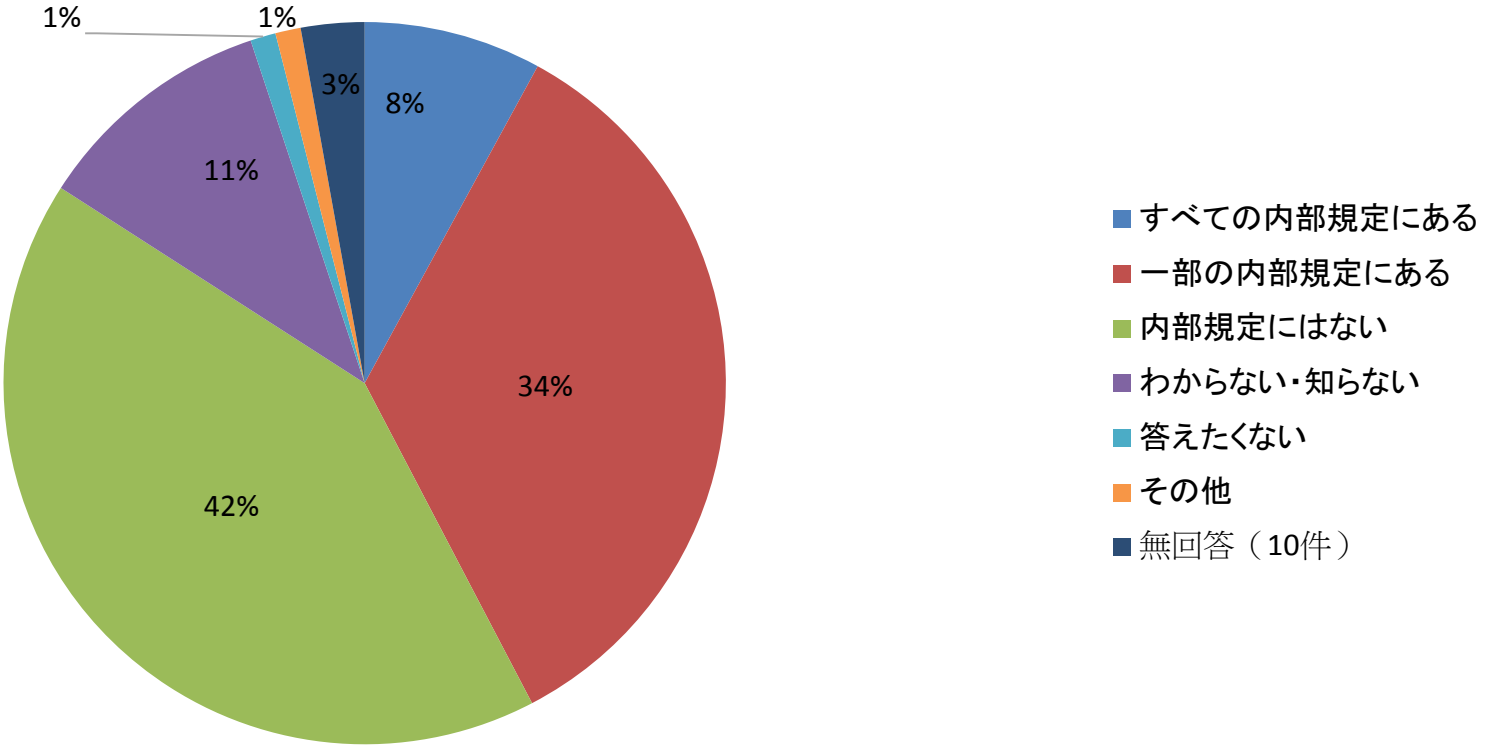
- 情報セキュリティリスク分析を71%の組織が1年以内に実施している。昨年は66%であったので、5%増えており、ISMS基準改定対応（2年以内に切り替え）の影響が多いものと考えられる。リスク分析の実施理由で、ISMSやPマークへの対応（71%）が最も多いことからも言える。
  リスク分析を行う際の問題点は、「実施方法が分かる人材が不足している」とした組織が80%で一番多く、人材育成が課題である。
- 情報セキュリティポリシーの策定・見直し手続きを行っている部門は、新規に加えた「委員会組織で見直し代表者が手続きを行っている」が31%になり、「情報システム部門・情報セキュリティ部門」と並んだ。
  管理策項目は、2013年10月に改訂されたISO/IEC27001及び27002に対応して20項目に変更・細分化した。「運用セキュリティ（マルウエア対策等）」が30%で多く、「ログ取得及び監視」が27%「モバイル機器及びテレワーキング」が26%と続き、「技術的な管理策」に重点が置かる傾向が見える。見直し理由では、昨年は21%あった「3年間は管理策の見直しがない」組織が 5%に減じたことでも、ISMS基準の改訂効果が大きいと言える。

第3章
情報セキュリティマネジメントの
「例外措置」への取組み

第3章　情報セキュリティマネジメントの「例外措置」への取組み

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

設問14. 情報セキュリティに関わる内部規定全般においての「例外規定」の有無
(N=352)

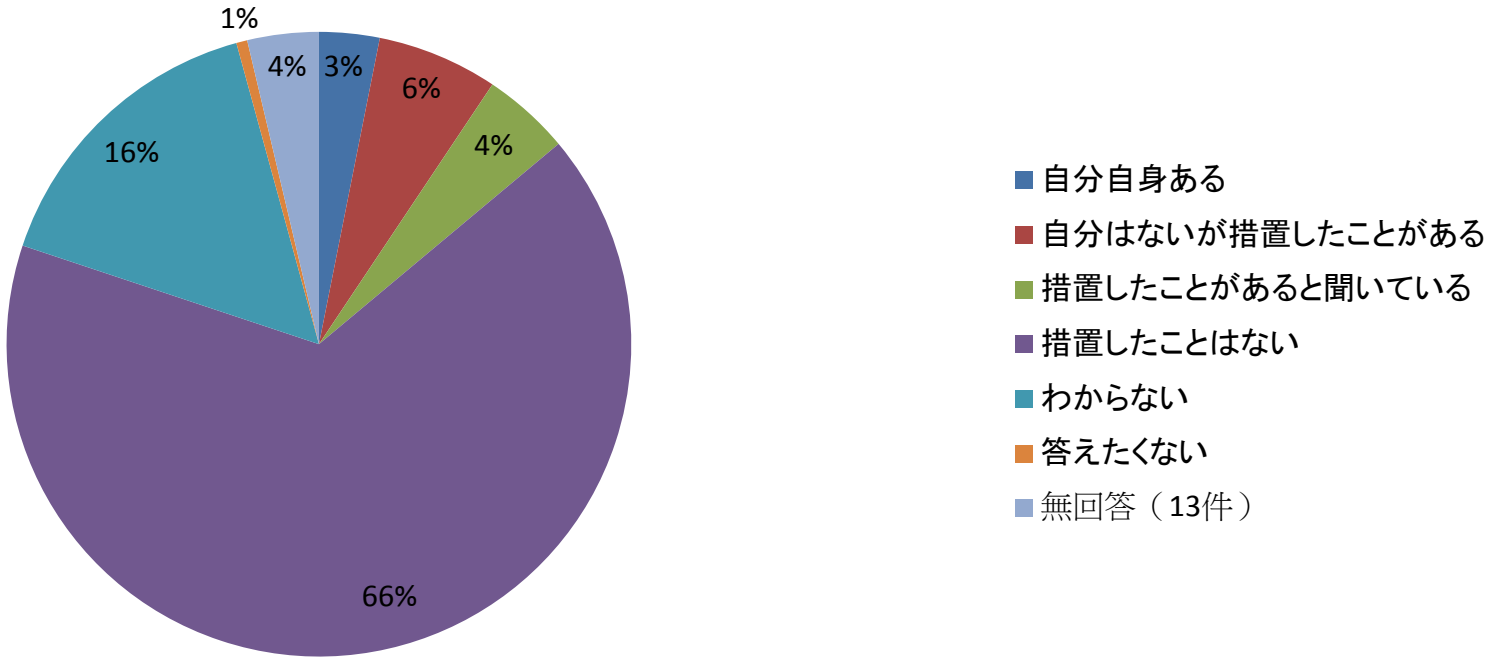


例外規定が内部規定に記載されている／いないの
割合はほぼ同程度である。

第3章　情報セキュリティマネジメントの「例外措置」への取組み

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

設問15. 例外規定が明記されていない事象（障害、事故・事件、災害等）に対する一時的な例外措置の経験の有無(N=352)

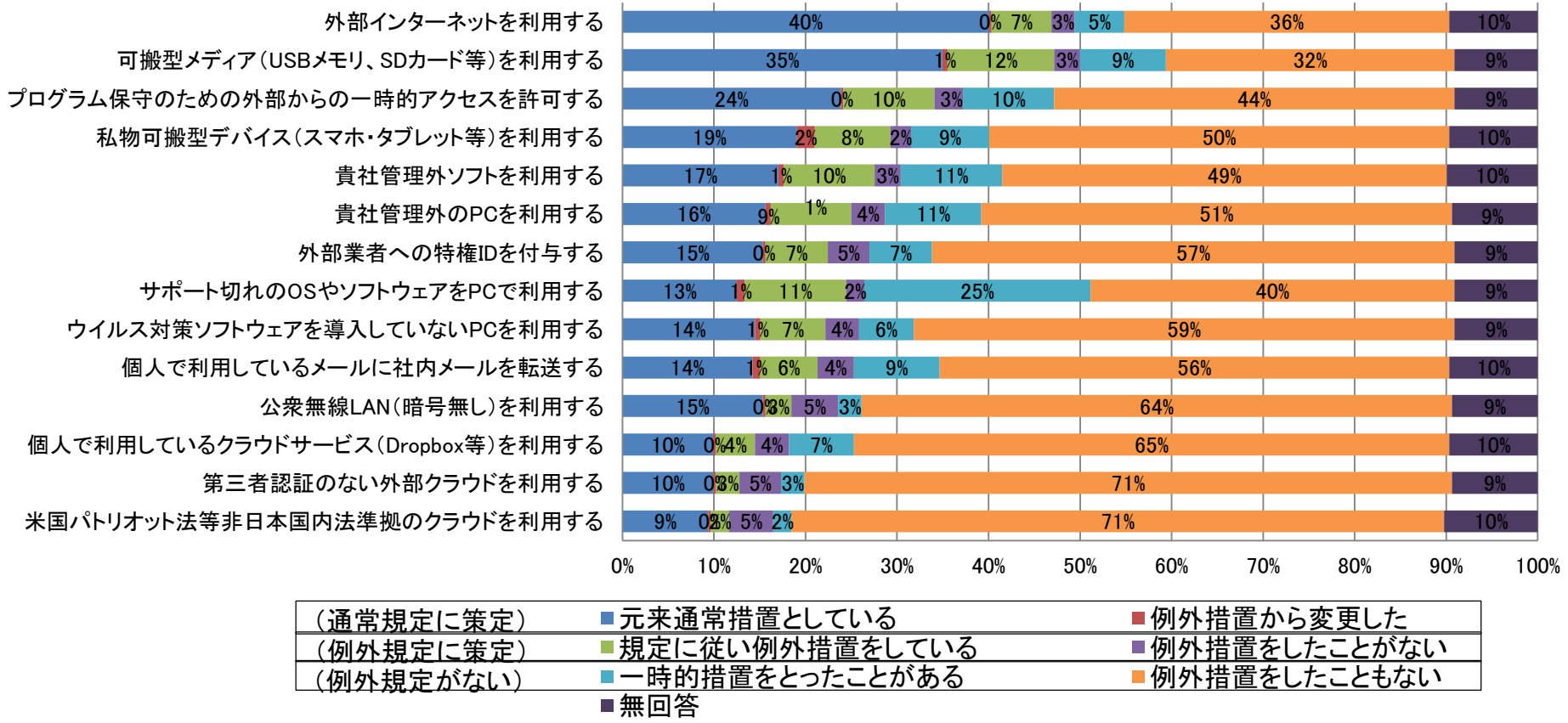


例外措置を実際に実施した総数は13%にとどまり、
7割近くは措置をしたことがない。

第3章　情報セキュリティマネジメントの「例外措置」への取組み

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

設問16. 具体的な業務上の事象における例外規定の有無(N=352)

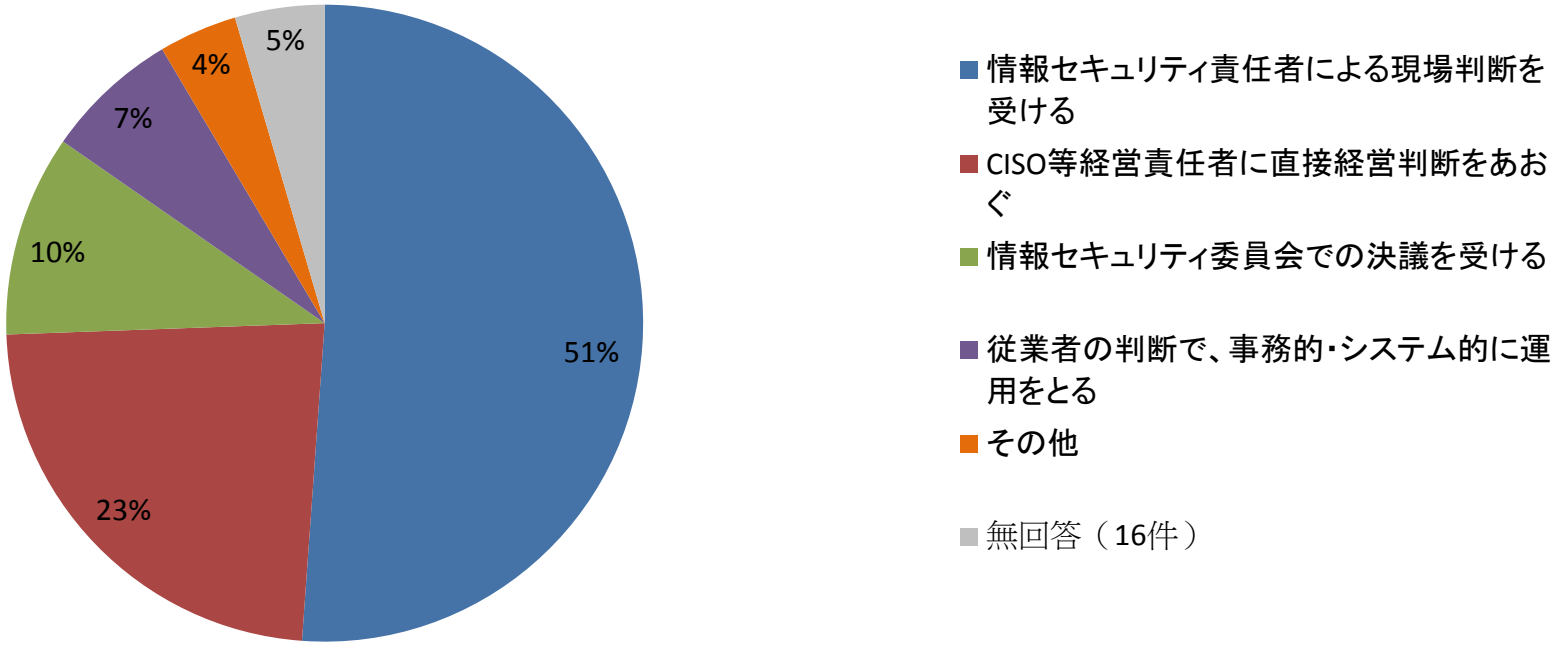


通常規定も含め例外規定を策定して措置している項目には「外部インターネットの利用」「可搬型メディア（USBメモリ、SDカード等）の利用」に関して目立っている。

第3章　情報セキュリティマネジメントの「例外措置」への取組み

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

設問17. 内部規定に例外規定がない事象で緊急を要する事態において一時的措置をとる場合の「最初」にとる手段(N=352)

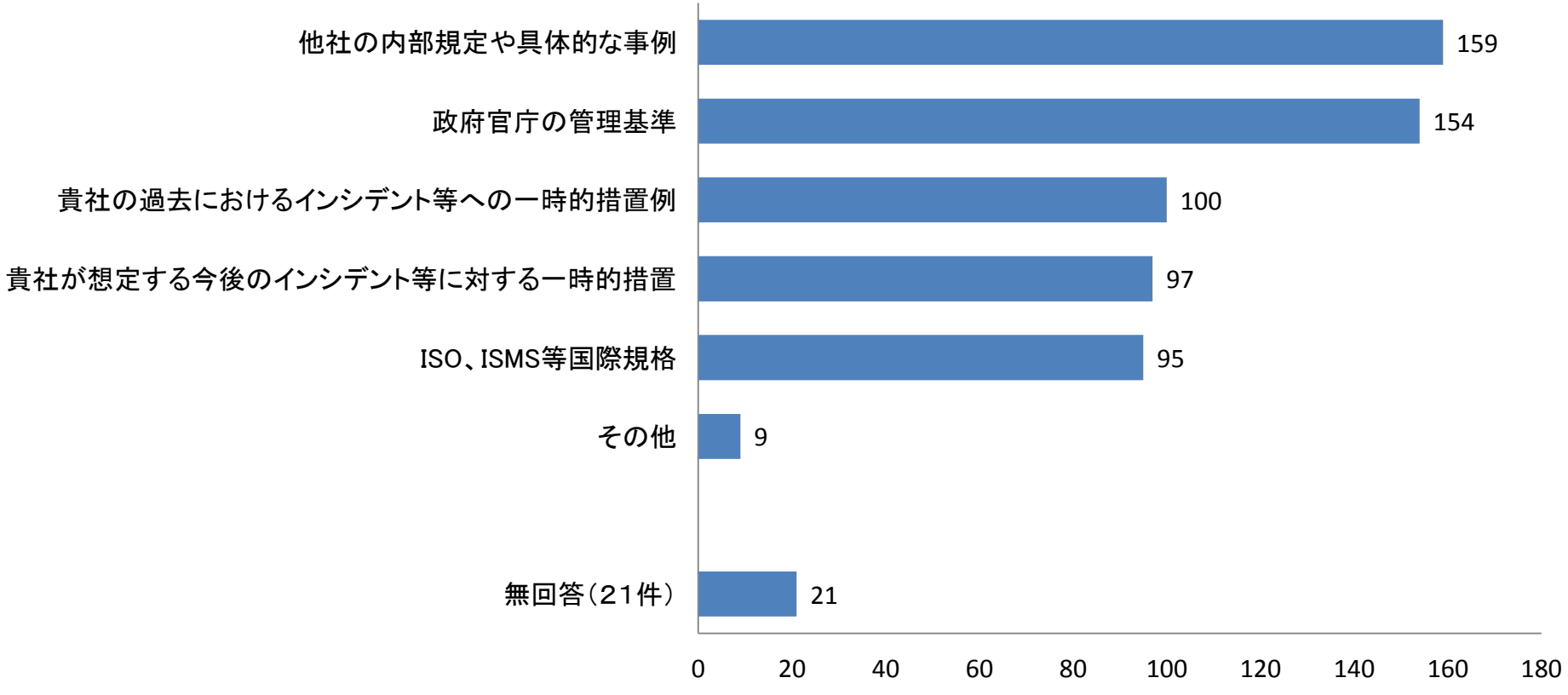


最初の措置判断は、現場の情報セキュリティ責任者であることが半数を占める。

第3章　情報セキュリティマネジメントの「例外措置」への取組み

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

設問18. 内部規定に新規の例外規定を策定する場合に参考にするもの(N=352)

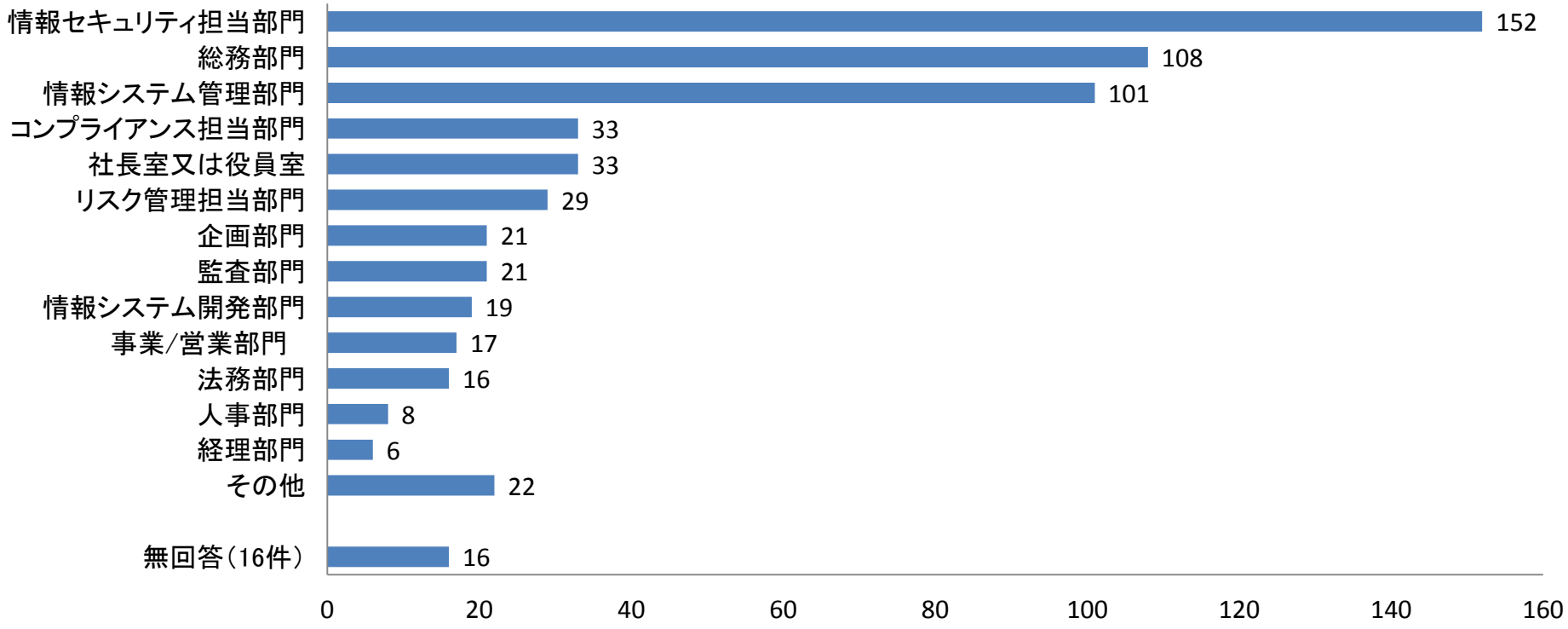


例外規定は、他社事例や政府官庁の管理基準をもとに策定されることが多い。

第3章　情報セキュリティマネジメントの「例外措置」への取組み

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

設問19. 例外規定を策定するにあたり、規程の策定と管理の事務処理をする主体部門（複数回答可）(N=352)

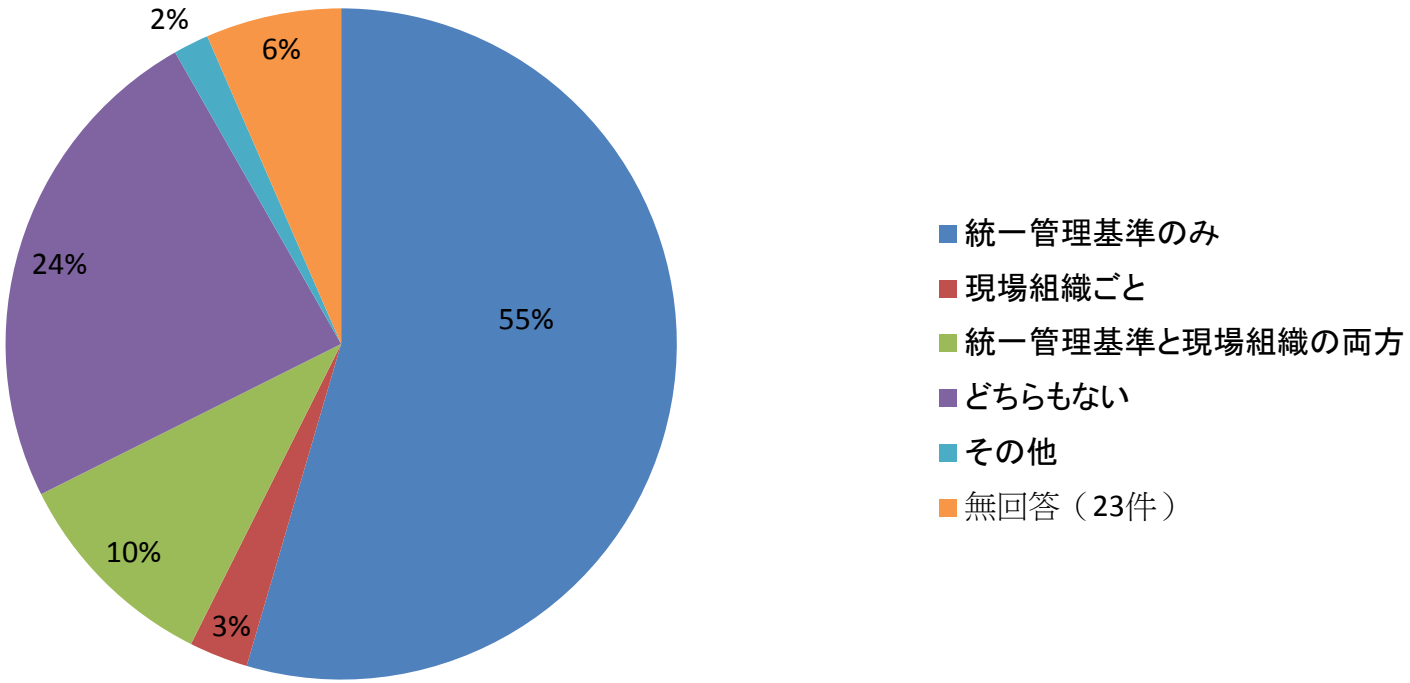


策定する組織は情報セキュリティ担当部門、
総務部門、情報システム管理部門が多い。

第3章　情報セキュリティマネジメントの「例外措置」への取組み

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

設問20. 例外規定は、全体で統一された内部規定のみか、現場組織ごとにも規定されているか(N=352)

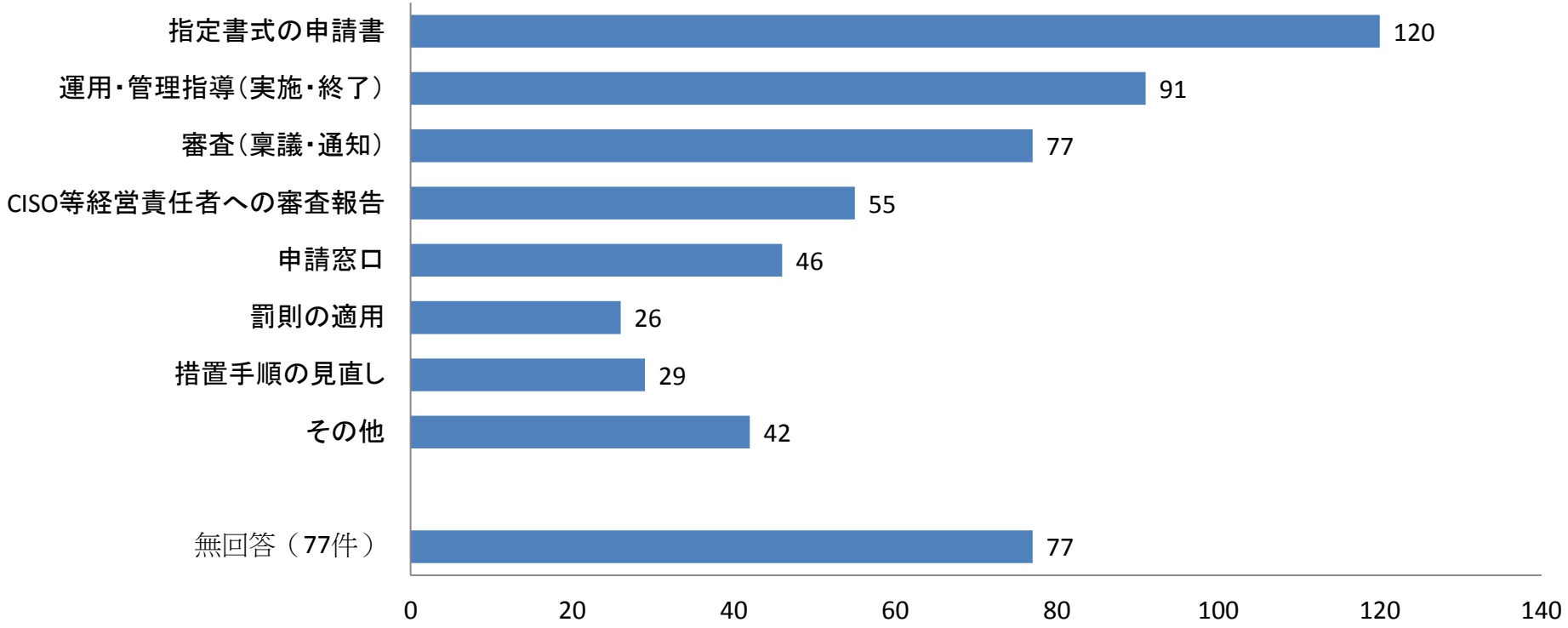


例外規定は統一管理基準のみ規定されている組織が5割を超える。

第3章　情報セキュリティマネジメントの「例外措置」への取組み

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

設問21. 例外規定における例外措置の業務にはどのような手続きを盛り込んでいるか（複数回答可）(N=352)

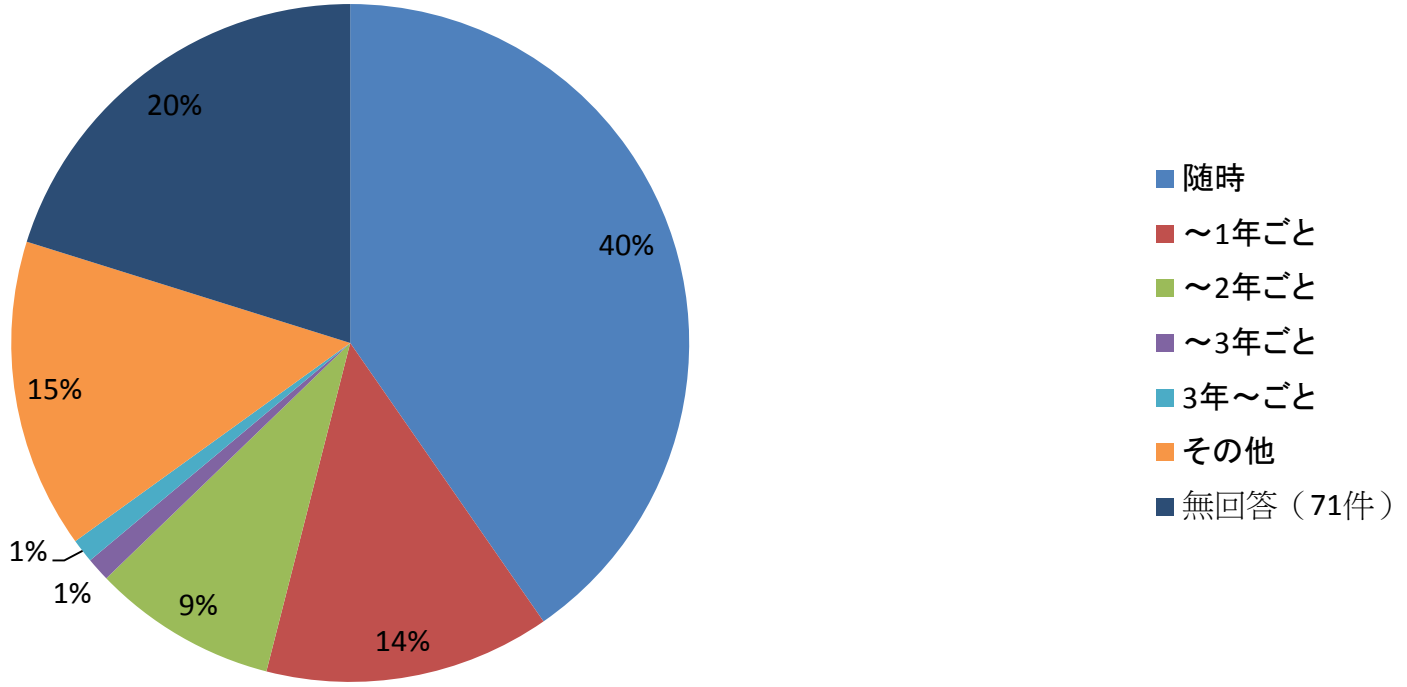


「指定書式の申請書」、「運用・管理指導（実施・終了）」、「審査（稟議・通知）」が手続きとして盛り込まれている一方、「罰則の適用」は少ない。

第3章　情報セキュリティマネジメントの「例外措置」への取組み

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

設問22. 例外規定の見直し頻度(N=352)

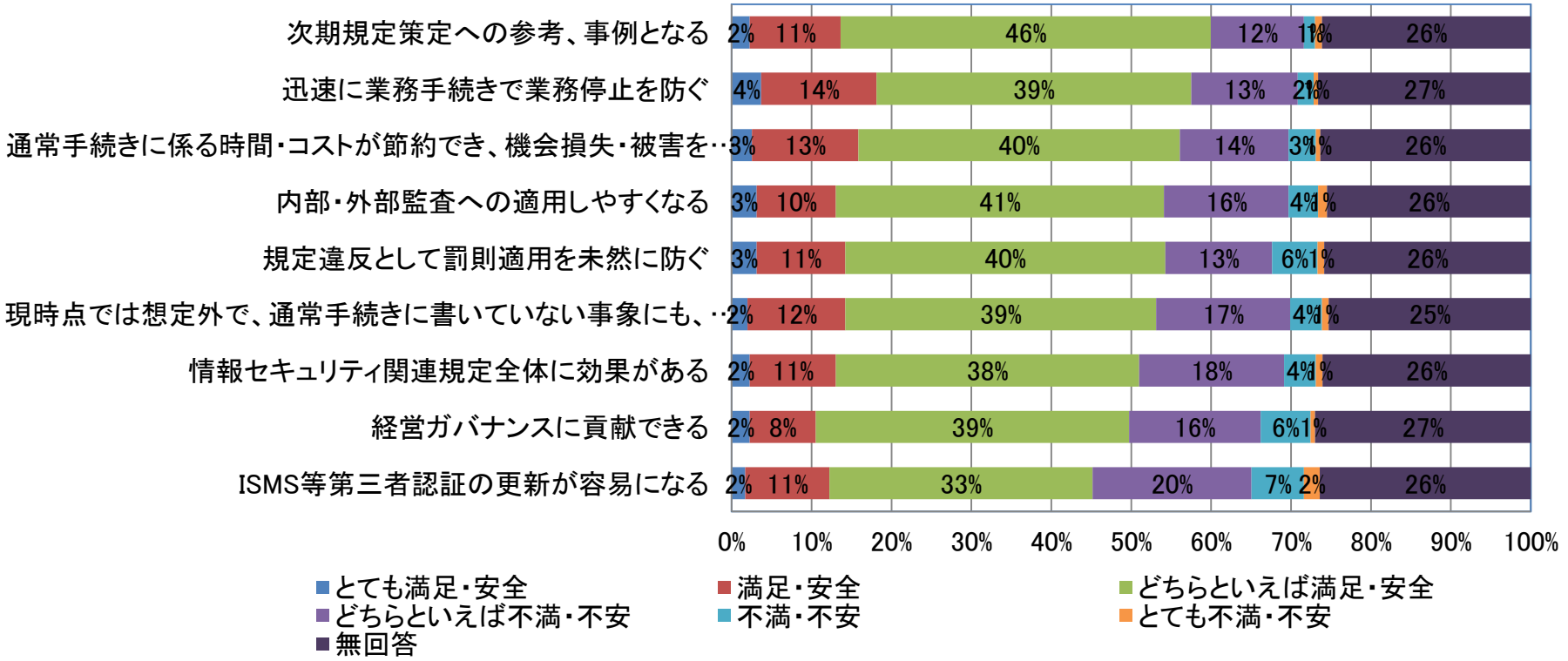


例外規定の見直し頻度は、随時見直ししている組織が多い。

第3章　情報セキュリティマネジメントの「例外措置」への取組み

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

設問23. 具体的な目的や効果に対してどのような効果があると、主観的に感じているか(N=352)



例外措置への効果は、「次期規定の見直し」「手続きの迅速化」「時間・コスト削減への効果」の満足度・安全度が高い。

考察 （第3章　情報セキュリティマネジメントの「例外措置」への取組み）

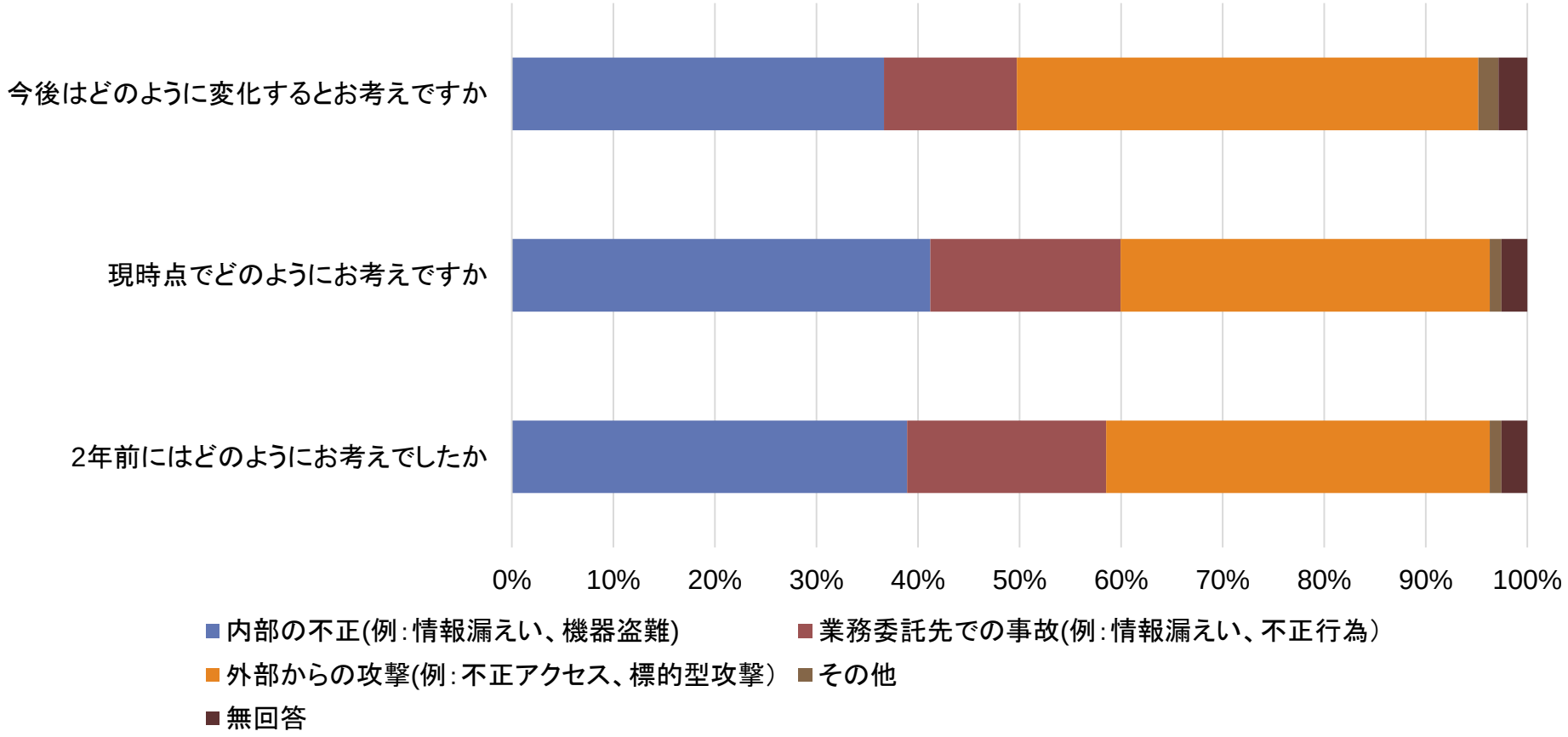
- 情報セキュリティに関する内部規定への例外措置の規定については策定している組織とそうでない組織とで2分化されている。
- 部署ごとにカスタマイズして策定しているものは少なく、多くは統一基準で策定・措置されている。また策定・管理は情報セキュリティに関わる部署が多く、現場からの策定は少ない。
- 「実際に措置をすることが少ない」「見直し頻度もその都度」「例外規定がないものの、一時的に例外措置を実施した」回答が多いことから、例外措置は事象が起きたその都度対応し、その後規定として策定・見直ししていると考えられる。
- 一方で、例外規定を策定している組織では、「申請者書式」「受領後の審査」「実施・終了時への指導」など措置への業務フローが整備されていると思われる。

第４章
情報セキュリティリスクの認識と支出の動向

第4章　情報セキュリティリスクの認識と支出の動向

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

設問24. 情報セキュリティリスクにおける重要な脅威（N=352）

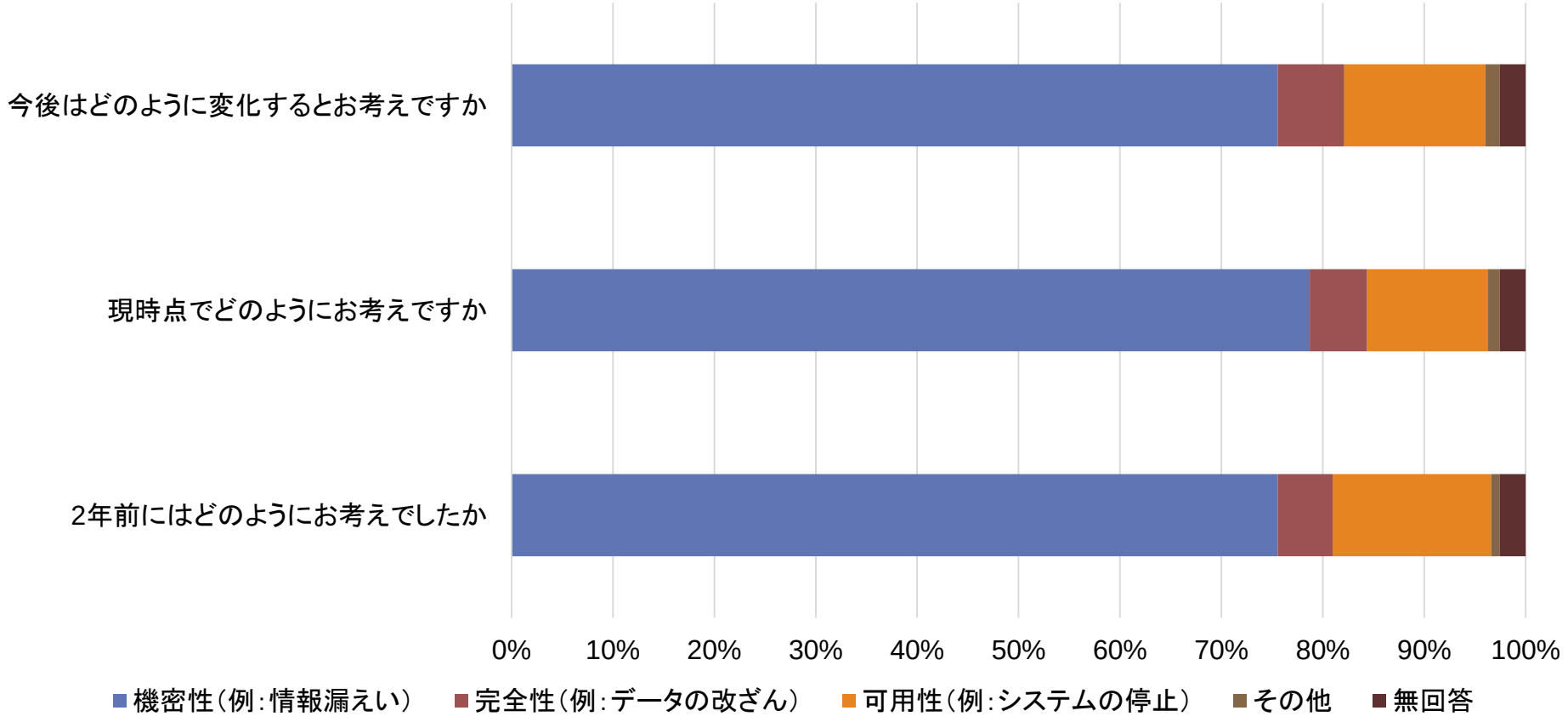


脅威に関する認識は、内部不正から外部からの攻撃に移りつつある。

第4章　情報セキュリティリスクの認識と支出の動向

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

設問25. 情報セキュリティに対する重視項目 （N=352）

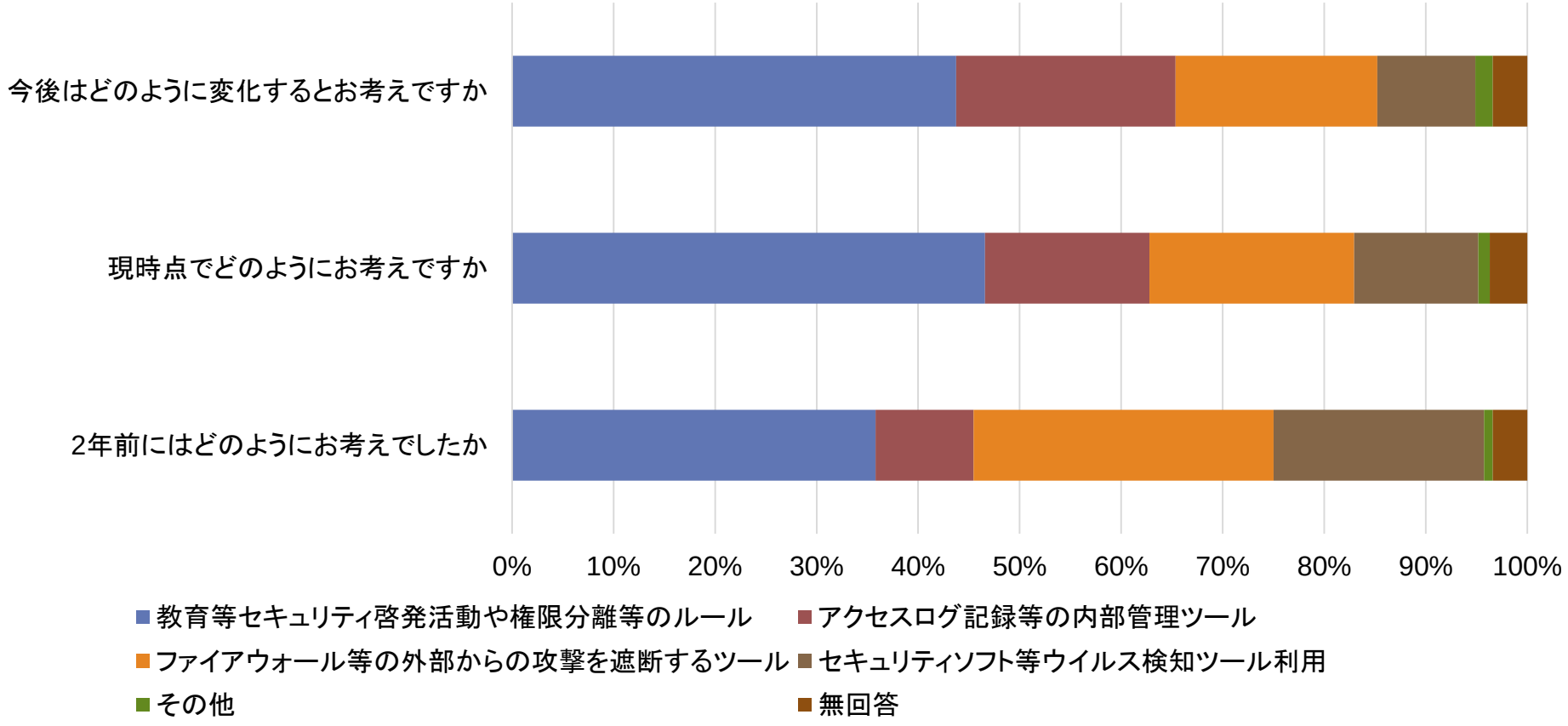


機密性が情報セキュリティで最も重視される項目とする回答が多い。

第4章　情報セキュリティリスクの認識と支出の動向

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

設問26. 情報セキュリティに対する重点対策（N=352）

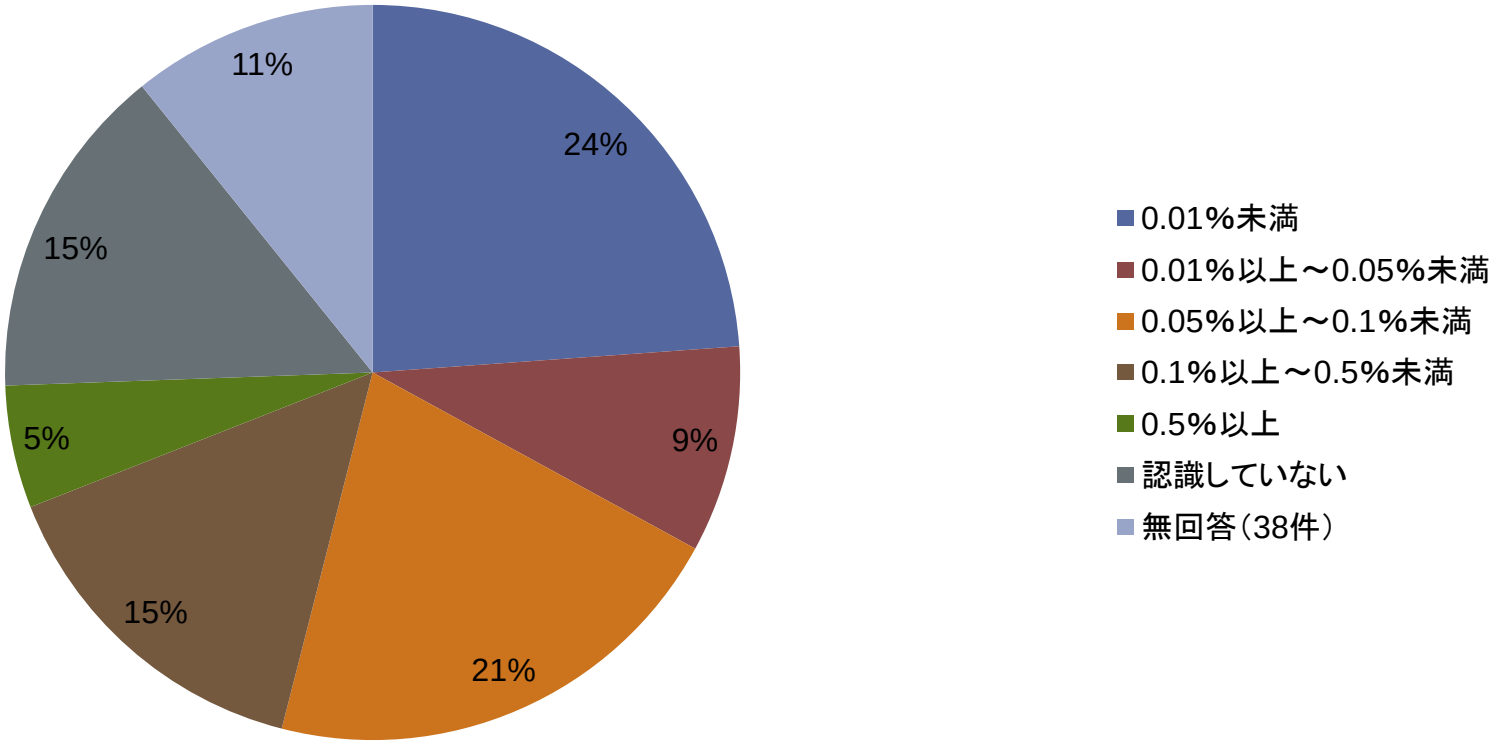


今後の動向として、アクセスログ記録等の内部管理ツールを重視する組織が多い。

第4章　情報セキュリティリスクの認識と支出の動向

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

設問27-1. 情報セキュリティに関する支出実績（前期） 対売上/予算比 （N=352）

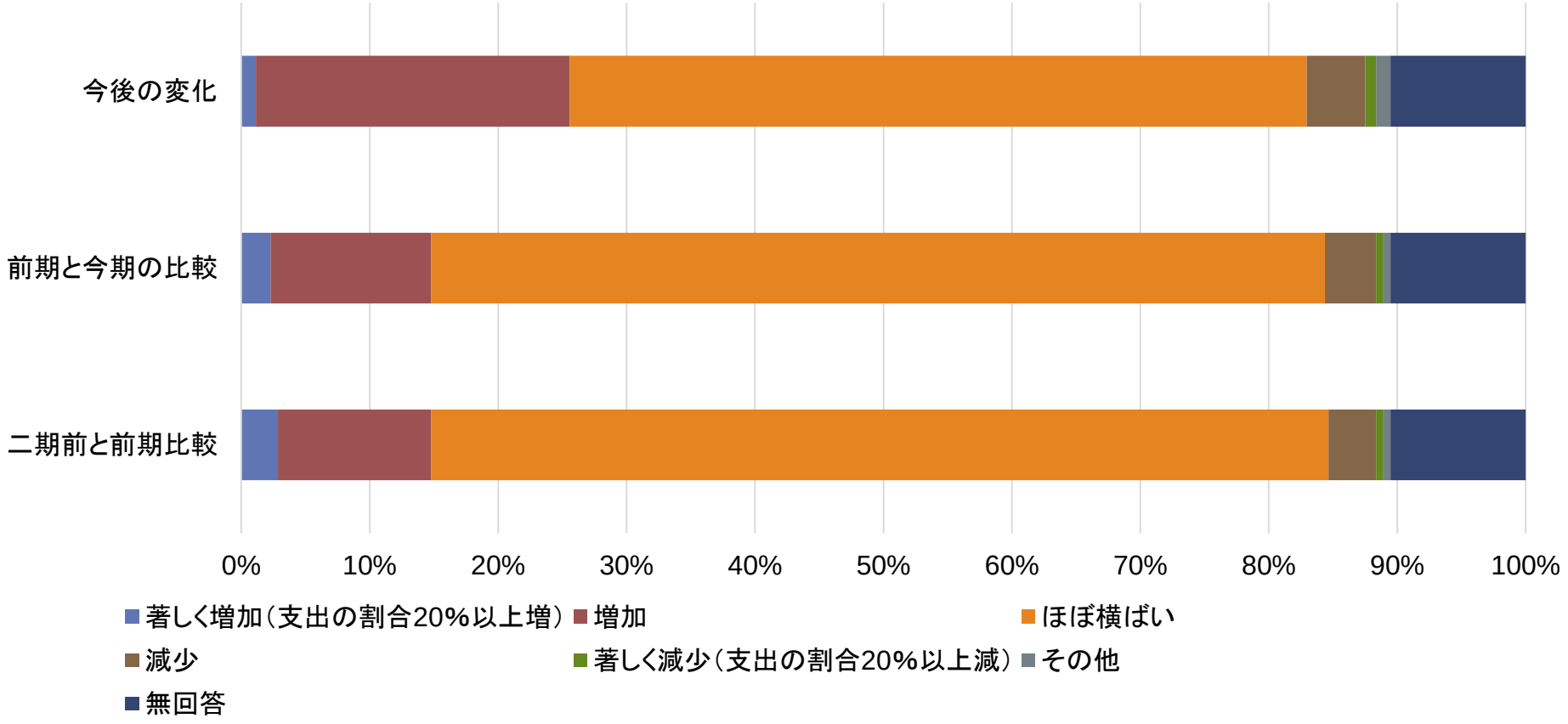


半数以上の組織は情報セキュリティについて、
売上や予算の0.1%未満の支出である。

第4章　情報セキュリティリスクの認識と支出の動向

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

設問27-2. 情報セキュリティに関する支出の傾向（N=352）



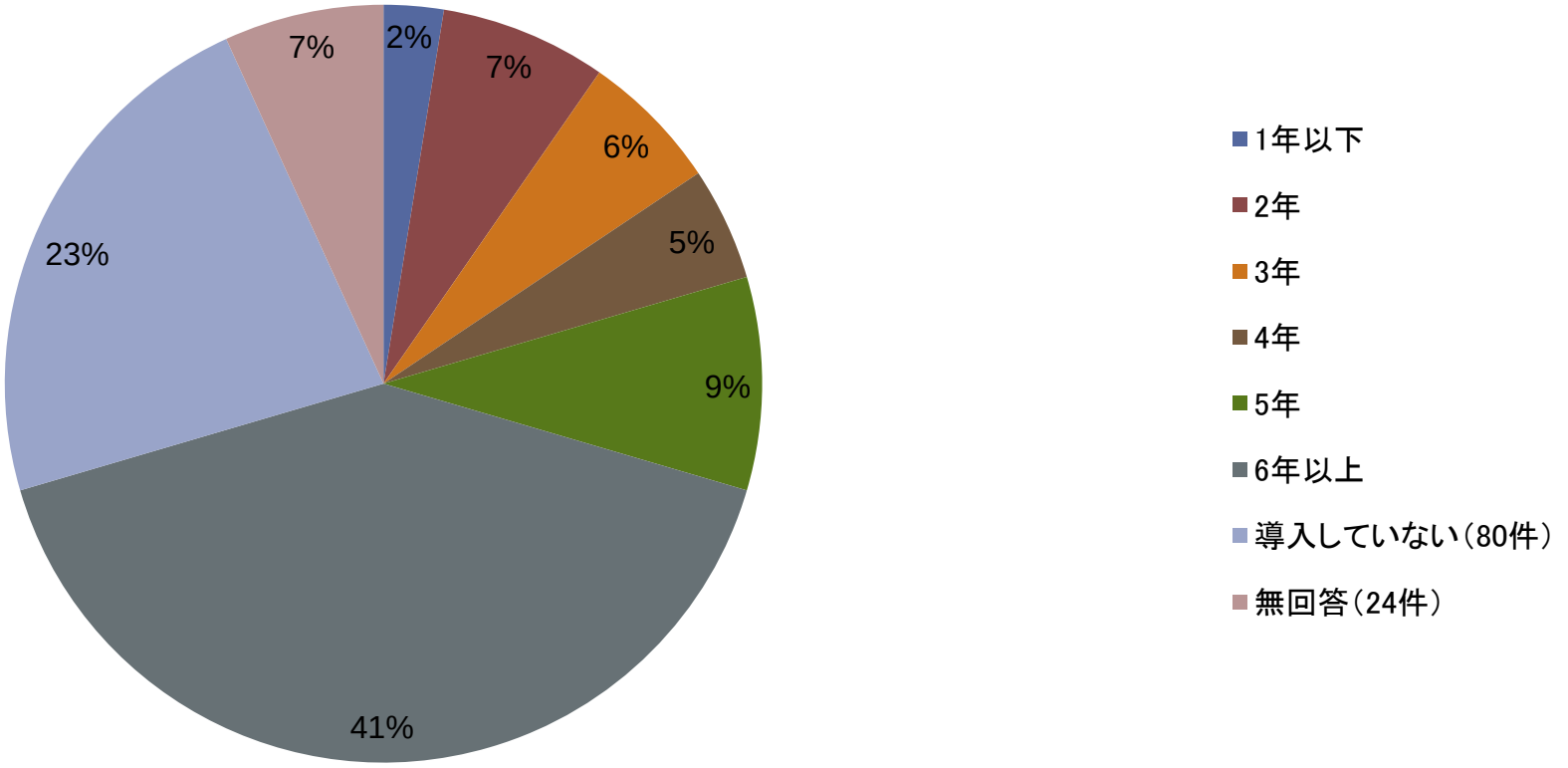
情報セキュリティ支出はこれまで横ばいだが、増加させる方向の組織は増えている。

考察（第4章　情報セキュリティリスクの認識と支出の動向）

- 脅威の認識は内部不正から外部からの攻撃に移りつつある。
- 重視するのは機密性である。
- 対策の重点は外部からの攻撃から内部不正に移りつつある。
- 半数以上の組織は売上や予算の0.1%未満しか、セキュリティに支出していない。
- セキュリティに対する支出は横ばいと回答する組織は多い。これから増加させると回答した組織は増えている。
- 脅威の認識と対策の重点のトレンドが異なる点が興味深い。また、セキュリティ支出が少ないことを考えると、情報セキュリティに関するリスク分析やPDCAのサイクルが、どのように運用されているのか、さらに検討が必要だと思われる。

第５章
情報セキュリティマネジメント
の運用状況

設問28. 情報セキュリティマネジメントシステムの運用期間(N=352)

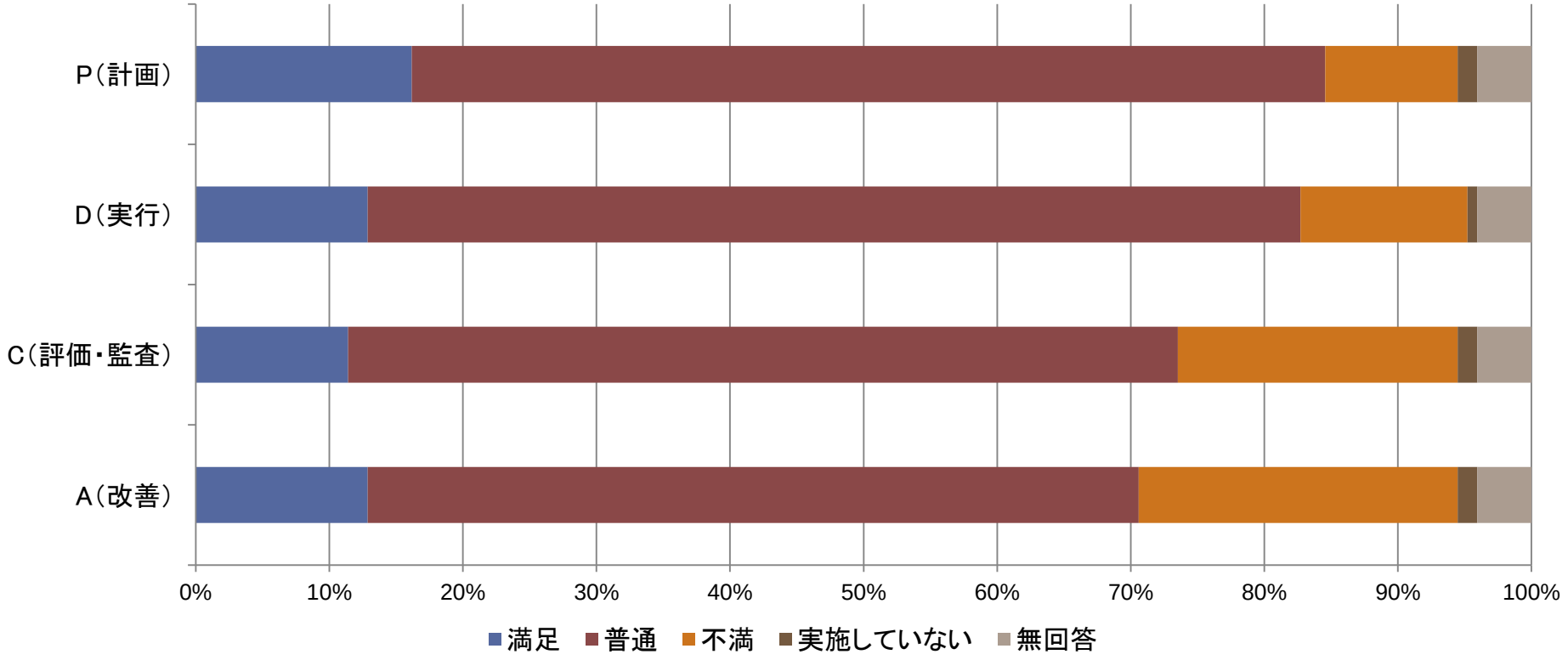


情報セキュリティマネジメントシステムの運用期間が
5年以上である企業が半数(9%+41%)を占める。

第5章　情報セキュリティマネジメントの運用状況

※設問28.で「**導入していない**」と回答した組織を除く

設問29. 情報セキュリティマネジメント運用におけるPDCA別の満足度(N=272)

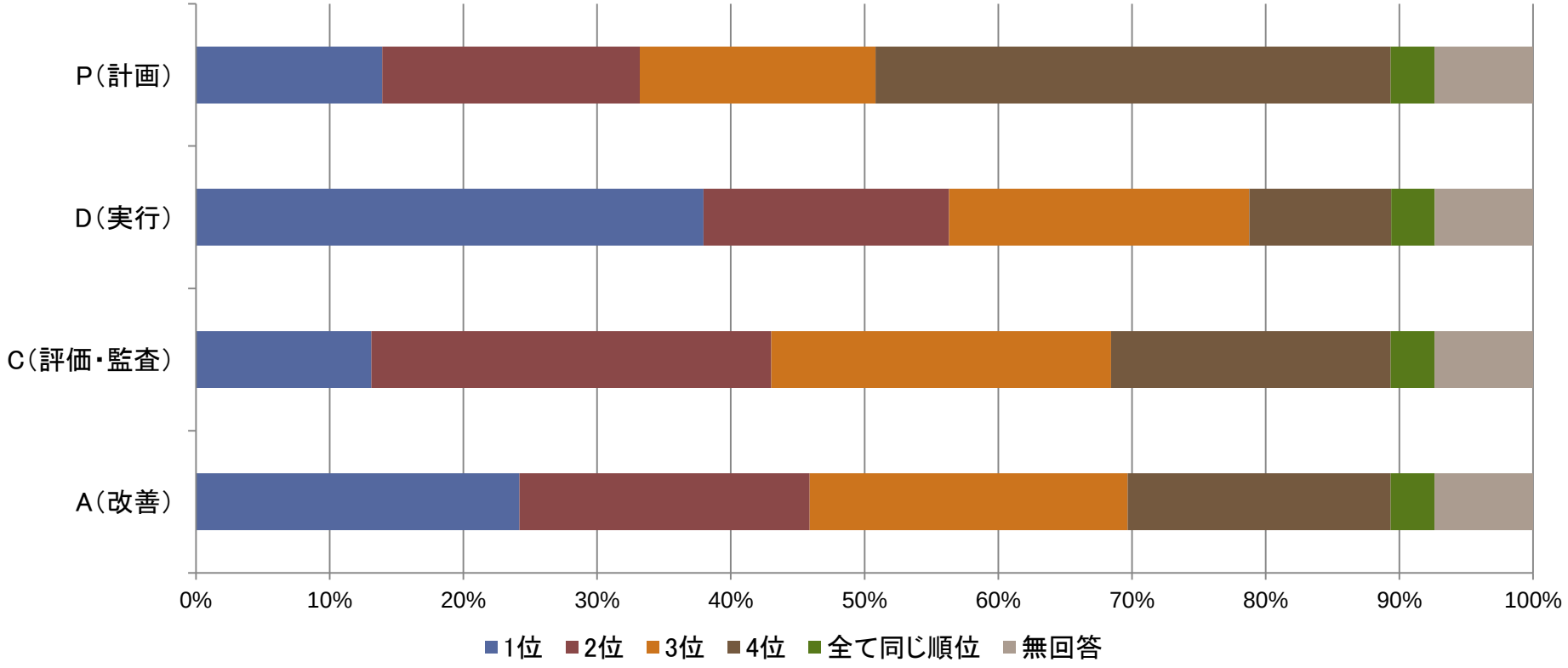


PDCA別の満足度は、P・D・C・Aの順で不満を持つ組織が増加している。

第5章　情報セキュリティマネジメントの運用状況

※設問28.で「**導入していない**」と回答した組織及び無効回答を除く

設問30. 情報セキュリティマネジメント運用におけるPDCA別の重視順位(N=244)

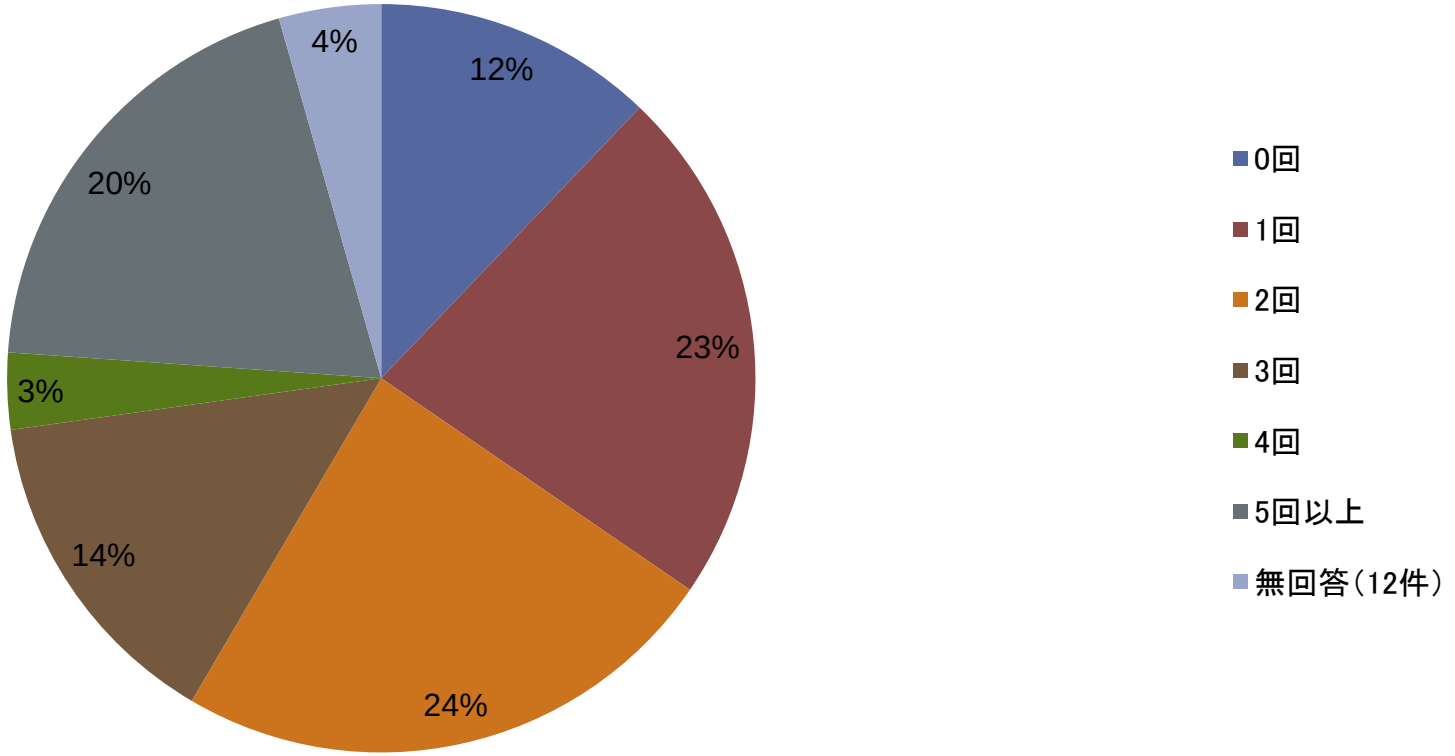


PDCAの中で重視しているプロセスについて、
1位が最も多いのがD(実行)で、4位が最も多いのはP(計画)。

第5章　情報セキュリティマネジメントの運用状況

※設問28.で「**導入していない**」と回答した組織を除く

設問31. 過去3年間で情報セキュリティマネジメントシステムの規程を改定した回数 (N=272)

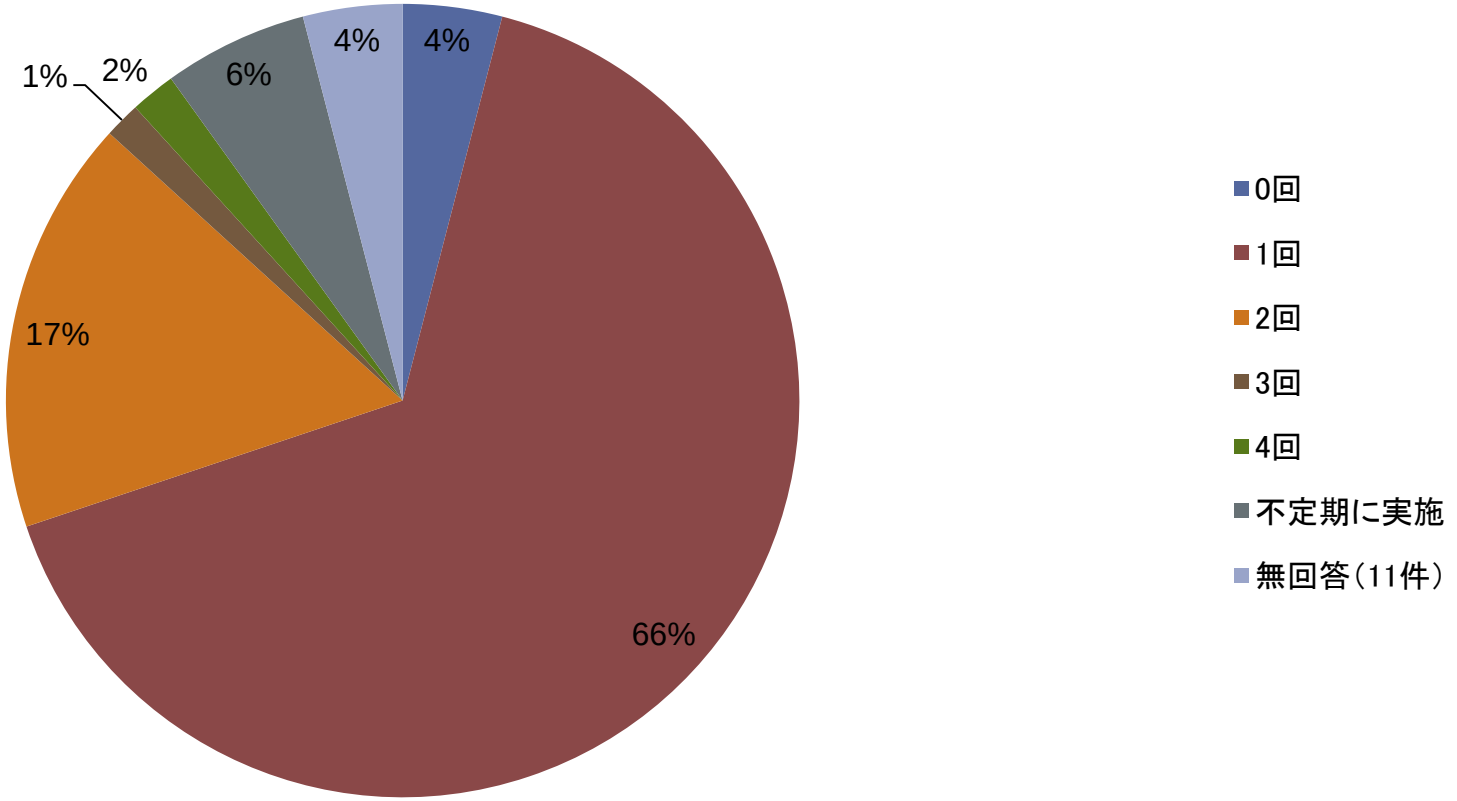


過去3年間で、84%の組織が1回以上の改定を行っており、
改定がなかったのは12%である。

第5章　情報セキュリティマネジメントの運用状況

※設問28.で「**導入していない**」と回答した組織を除く

設問32. 情報セキュリティマネジメントシステムの年間監査回数(N=272)

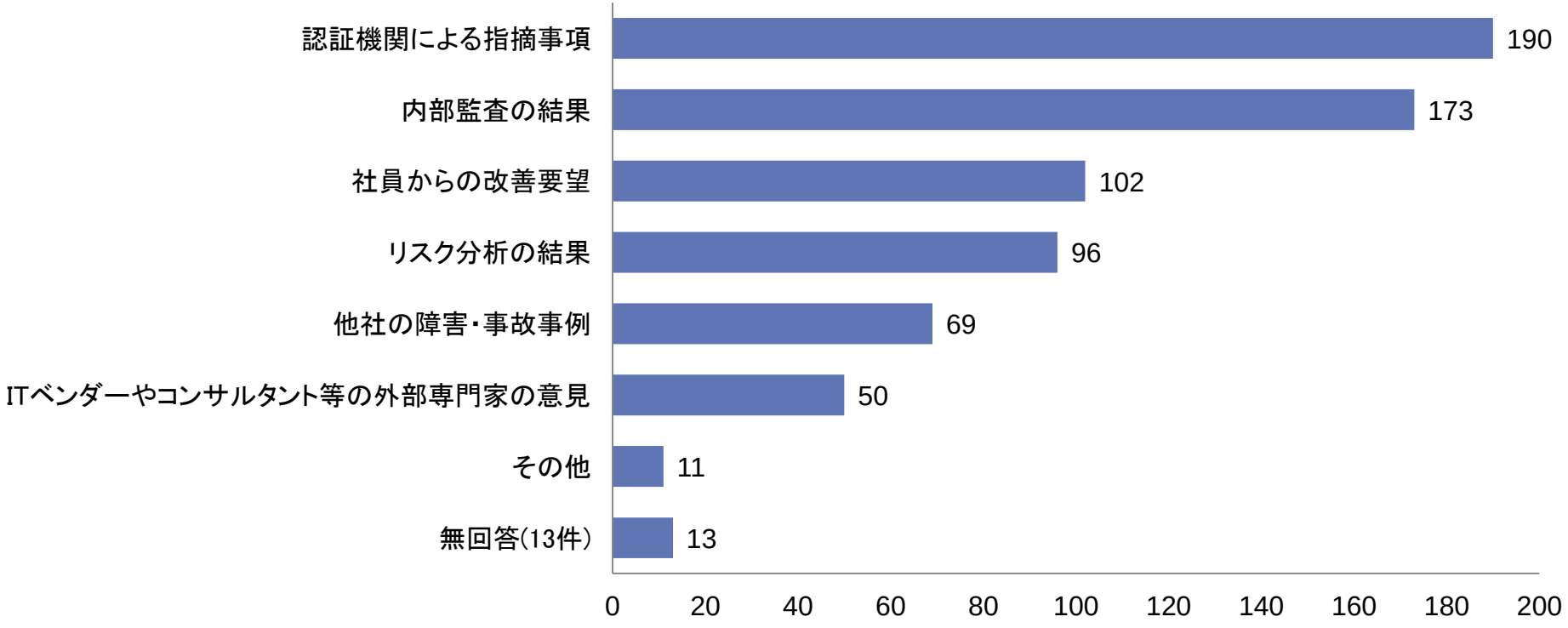


（内部）評価・監査を実施している組織が92%であり定着している。
年間1回の実施が66%で一番多い。

第5章　情報セキュリティマネジメントの運用状況

※設問28.で「**導入していない**」と回答した組織を除く

設問33. 情報セキュリティマネジメントシステムの規定改定時の参考とする事柄（複数選択可）(N=272)

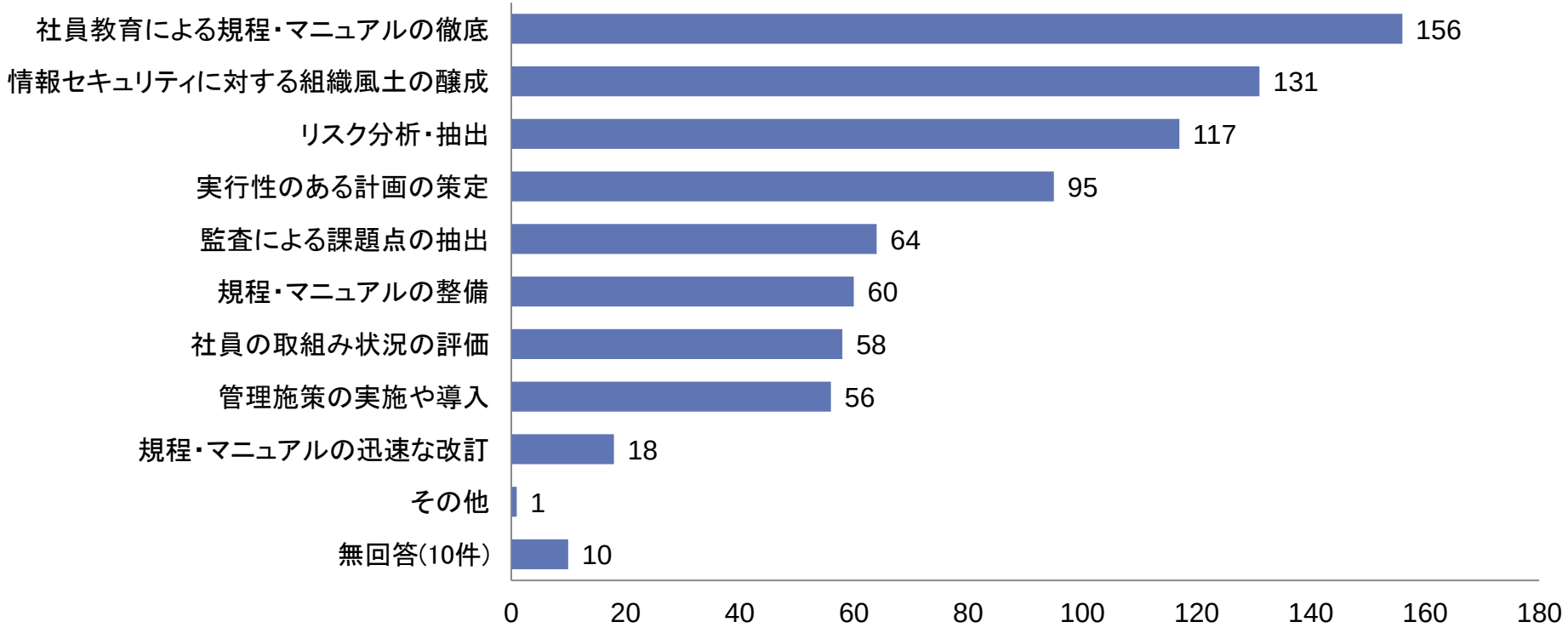


改定時の参考とする事柄は「認証機関の指摘事項」及び「内部監査」の結果が多い。

第5章　情報セキュリティマネジメントの運用状況

※設問28.で「**導入していない**」と回答した組織を除く

設問34. 情報セキュリティマネジメントシステムの運用時に重要と考える事柄の意識調査（3つまで選択可）(N=272)



運用に重要と考える事柄は、「社員教育」、
「組織風土の醸成」及び「リスク分析・抽出」が多い。

考察（第5章　情報セキュリティマネジメントの運用状況）

- 情報セキュリティマネジメントを5年以上運用している組織が半数にのぼり、監査の実施回数も1年間に1回以上行っている組織が9割を超えることから、情報セキュリティマネジメントが組織の中で定着しつつあることが分かる。

- 一方で、組織によってPDCA別の満足度や重点取組みする箇所の違いが見られ、P・D・C・Aの順で満足度が低くなる傾向がある。

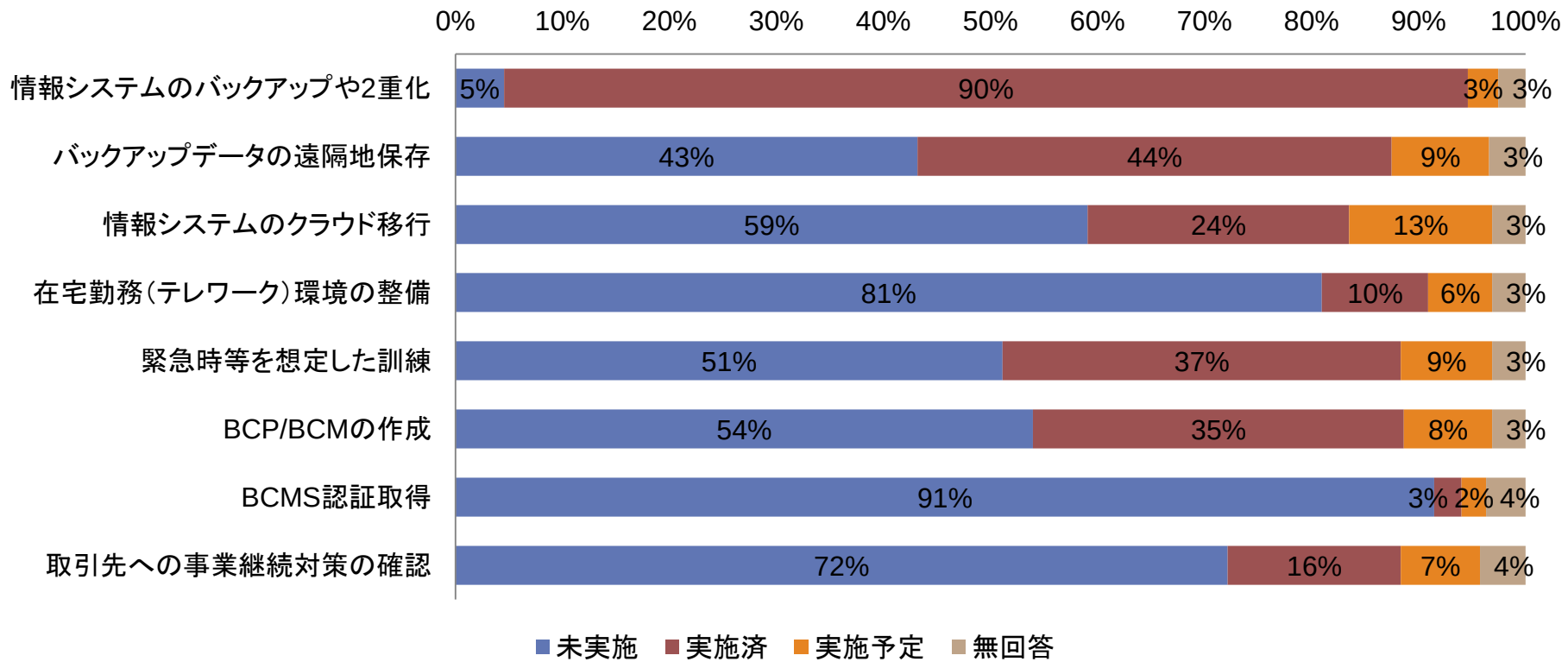
- 情報セキュリティマネジメント運用にあたり、「社員教育」及び「組織風土の醸成」といったシステム面以外の事柄を重要と考えている組織が多い。

第６章
事業継続に関わる取組み
の実施状況

第6章　事業継続に関わる取組みの実施状況

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

設問35. 事業継続に関わる取組みの実施状況(N=352)

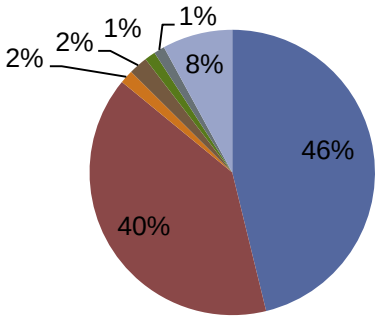


「情報システムのバックアップや2重化」は多くの組織で実施済であり、
「在宅勤務環境の整備」と「BCMS認証取得」は未実施組織の割合が高い。

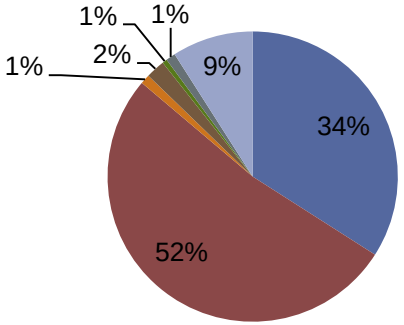
第6章　事業継続に関わる取組みの実施状況

※N数：設問35で「**未実施**」及び無効回答を除く

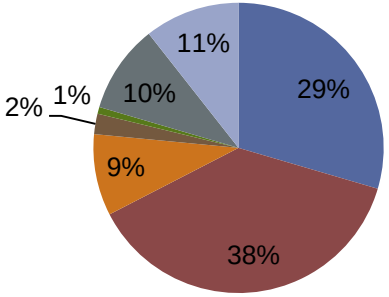
設問35-1. 事業継続に関わる取組みの実施を検討したきっかけ（全体）



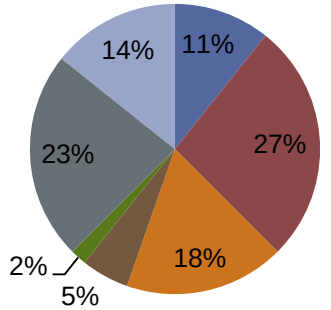
情報システムのバックアップや2重化(N=327)



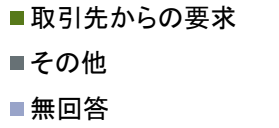
バックアップデータの遠隔地保存(N=188)

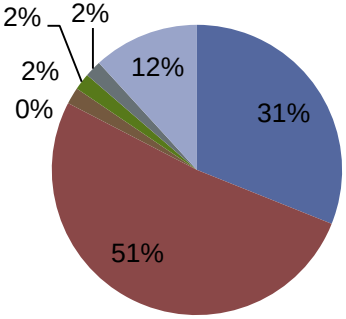


情報システムのクラウド移行(N=132)

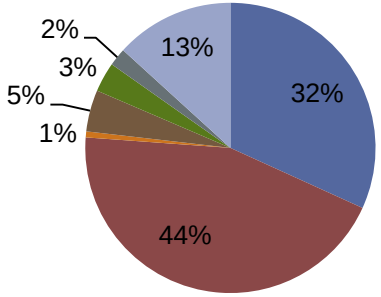


在宅勤務（テレワーク）環境の整備(N=56)

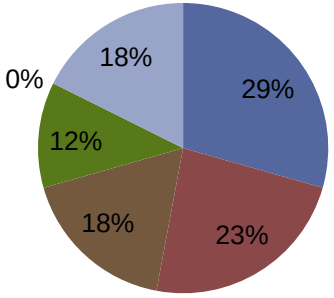




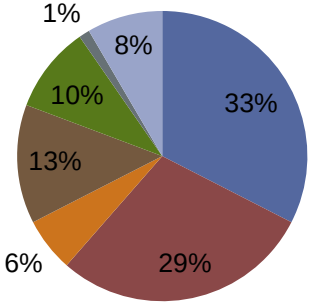
緊急時等を想定した訓練(N=161)



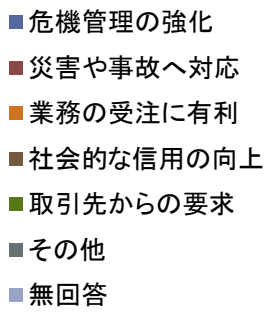
BCP/BCMの作成(N=151)



0%
BCMS認証取得(N=17)



取引先への事業継続対策の確認(N=83)



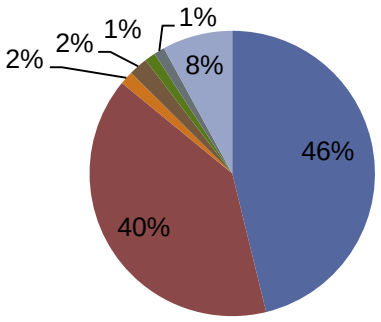
概ね「危機管理の強化」や「災害や事故への対応」をきっかけとして実施している組織の割合が高い。

第6章　事業継続に関わる取組みの実施状況

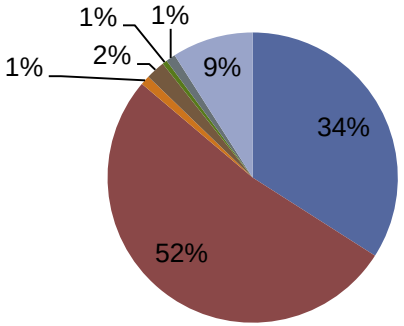
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

※N数：設問35で「**未実施**」及び無効回答を除く

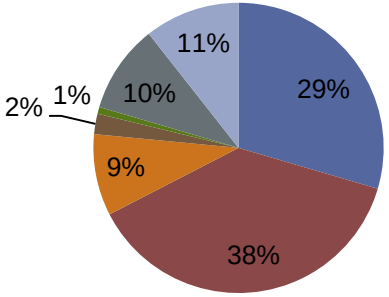
設問35-2. 事業継続に関わる取組みの実施を検討したきっかけ（特徴1）



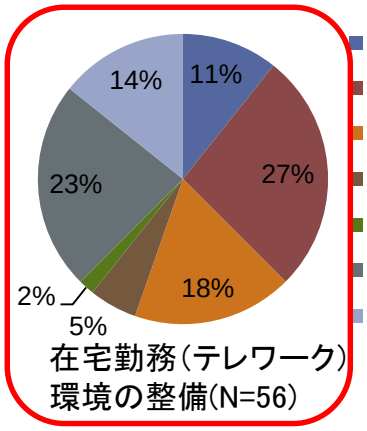
情報システムのバックアップや2重化(N=327)



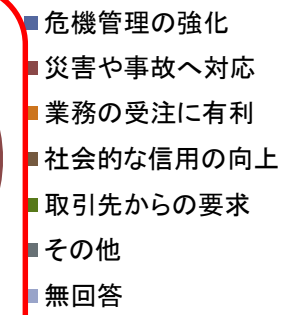
バックアップデータの遠隔地保存(N=188)

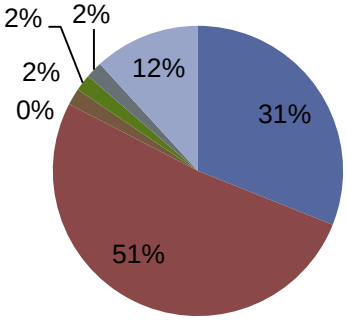


情報システムのクラウド移行(N=132)

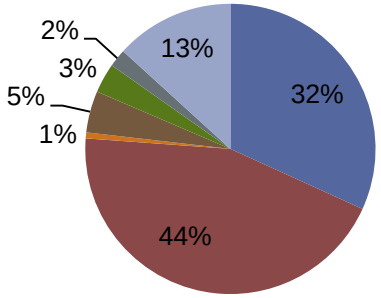


在宅勤務（テレワーク）環境の整備(N=56)

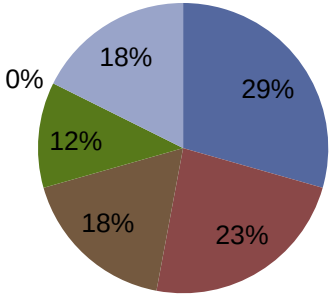




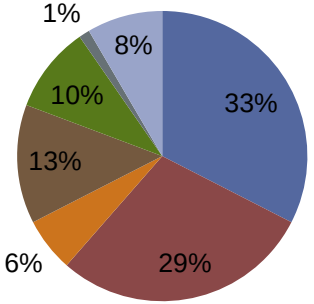
緊急時等を想定した訓練(N=161)



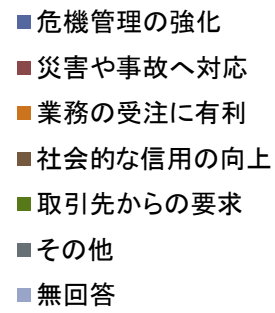
BCP/BCMの作成(N=151)



0%
BCMS認証取得(N=17)



取引先への事業継続対策の確認(N=83)

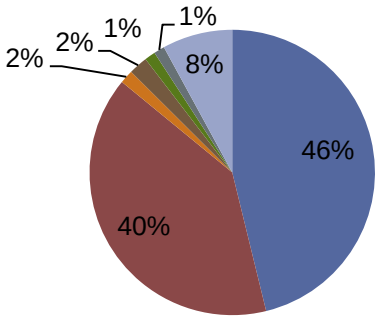


「在宅勤務環境の整備」は、他の取組みと比較して「危機管理の強化」の割合が低く、「業務の受注に有利」と「その他」の割合が高い。

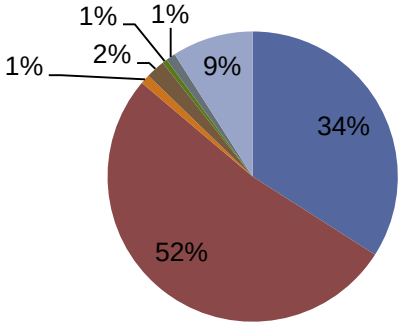
第6章　事業継続に関わる取組みの実施状況

※N数：設問35で「**未実施**」及び無効回答を除く

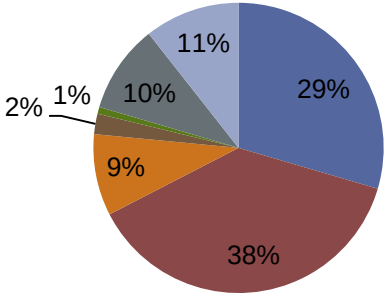
設問35-3. 事業継続に関わる取組みの実施を検討したきっかけ（特徴2）



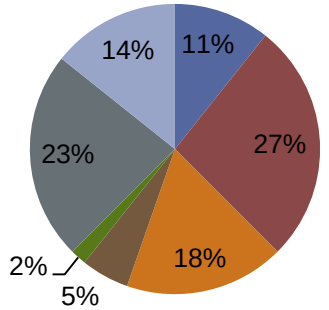
情報システムのバックアップや2重化(N=327)



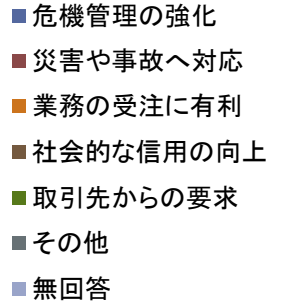
バックアップデータの遠隔地保存(N=188)

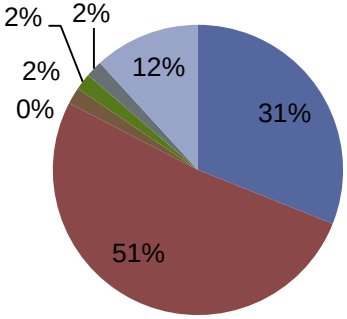


情報システムのクラウド移行(N=132)

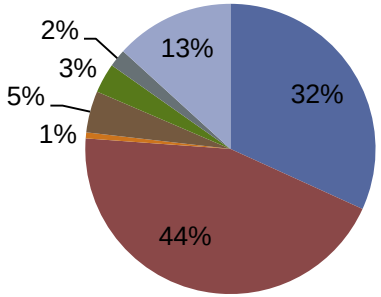


在宅勤務（テレワーク）環境の整備(N=56)

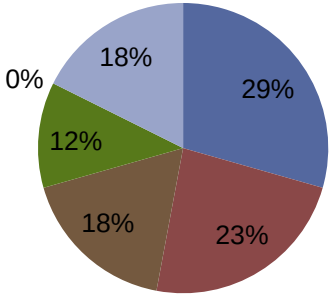




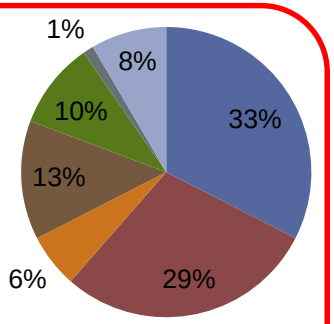
緊急時等を想定した訓練(N=161)



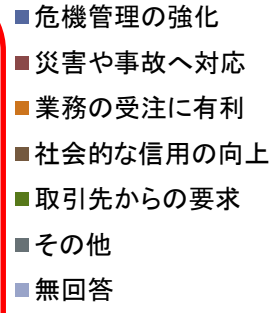
BCP/BCMの作成(N=151)



0%
BCMS認証取得(N=17)



取引先への事業継続対策の確認(N=83)



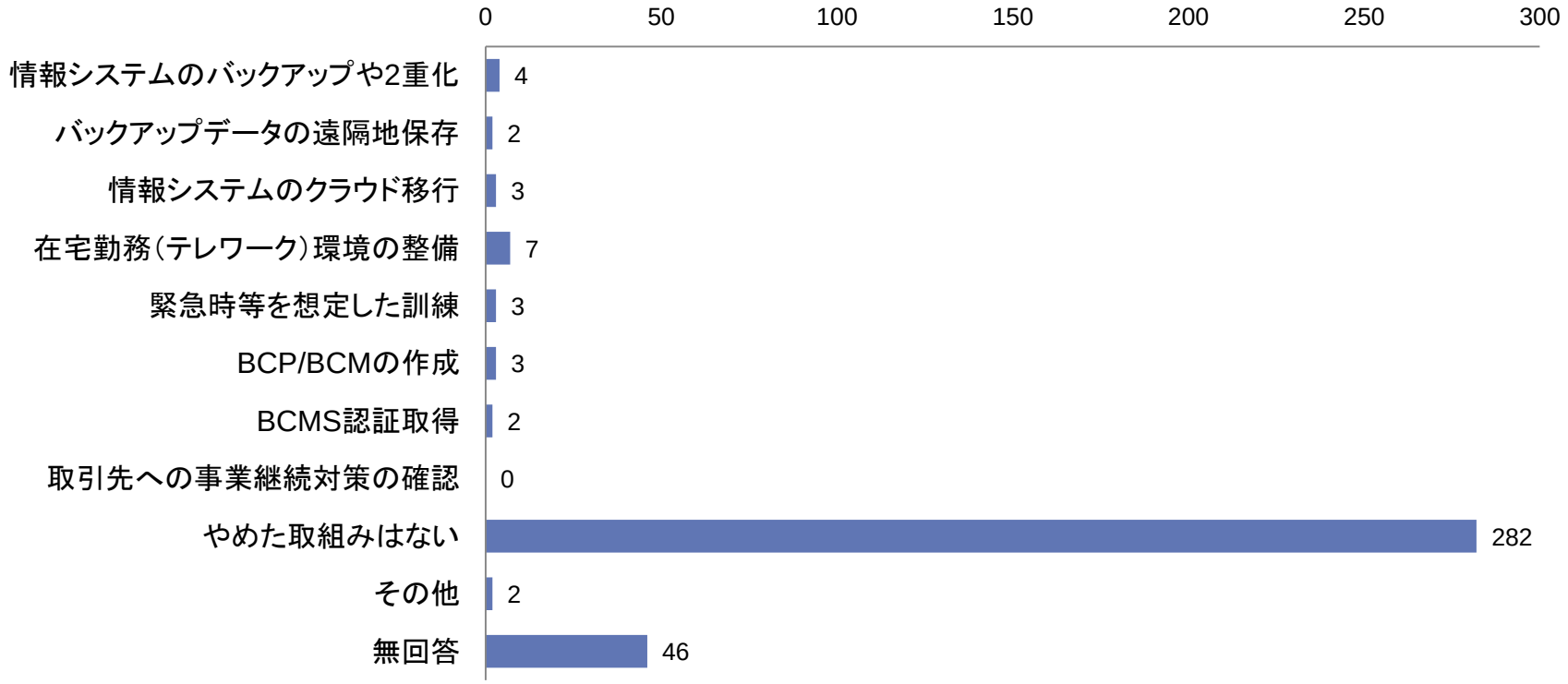
「BCMS認証取得」と「取引先への事業継続の確認」は「社会的な信用向上」と「取引先からの要求」の割合が他の取組みよりも高い。

第6章　事業継続に関わる取組みの実施状況

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

※N数：無効回答を除く

設問36.「過去に実施していたがやめた事」（複数回答可）(N=351)

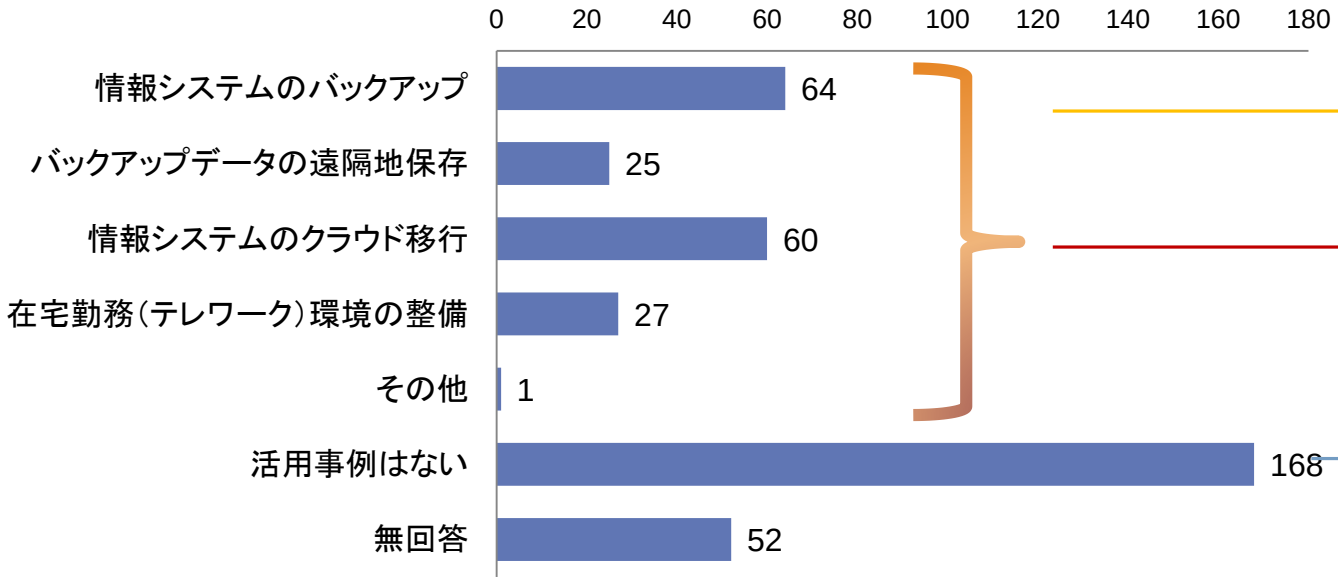


事業継続に関わる取組みは、多くの組織で継続されている。

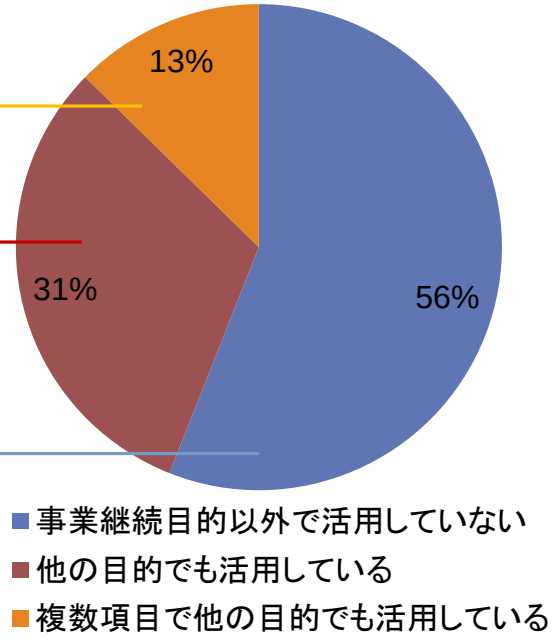
第6章　事業継続に関わる取組みの実施状況

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

設問37.「事業継続以外の目的」でも活用している事（複数回答可）(N=352)



事業継続以外の目的でも活用している取り組み
（複数回答）



事業継続以外の目的で活用しているか
（組織数N=300）

無回答を除く300組織の内、44%の組織が事業継続以外の目的でも活用し、56%の組織が事業継続以外の目的で活用していない。

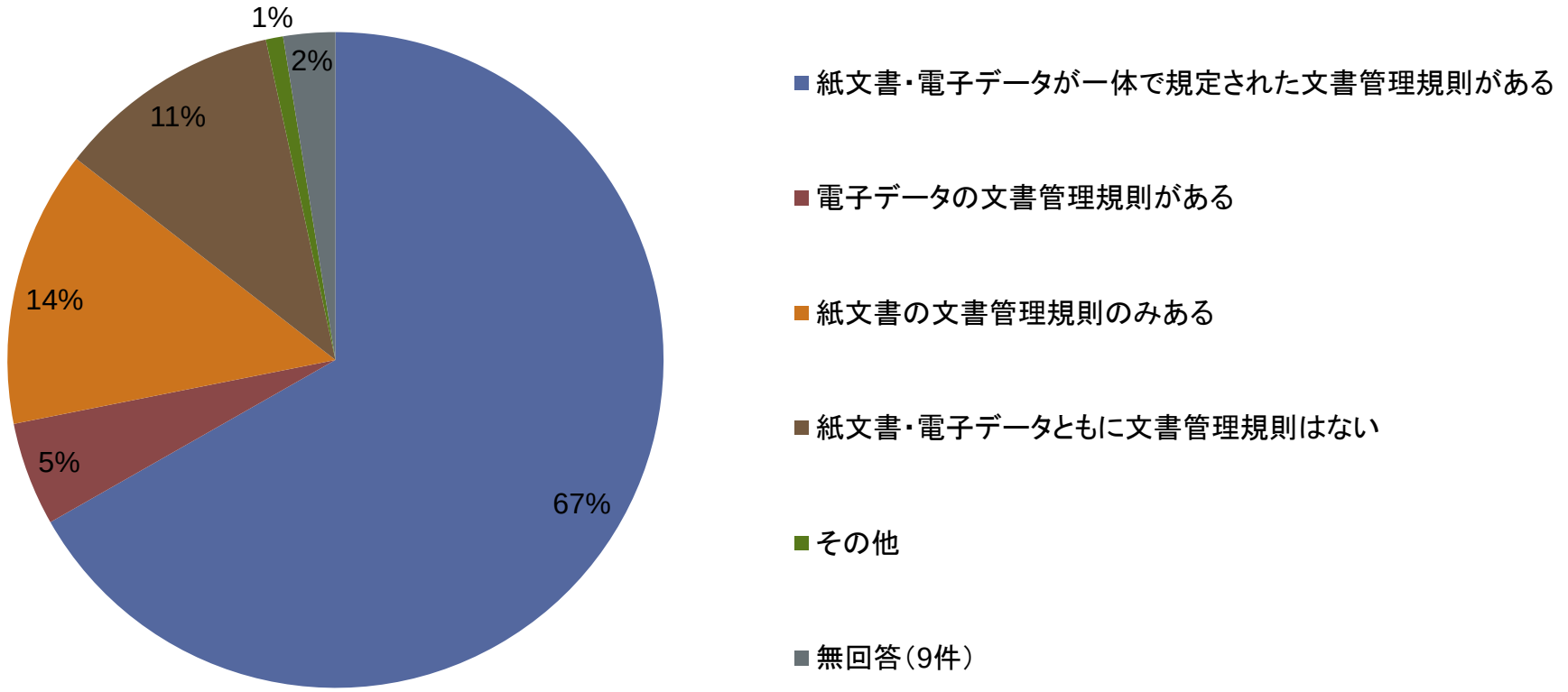
考察（第6章　事業継続に関わる取組みの実施状況）

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

- 「情報システムのバックアップや2重化」は多くの組織で実施済であり、「在宅勤務（テレワーク）環境の整備」と「BCMS認証取得」は未実施組織の割合が高い。
- 各取組みの実施を検討したきっかけは、概ね「危機管理の強化」や「災害や事故への対応」をきっかけとして実施している組織の割合が高い。
- 「在宅勤務環境の整備」は、他の取組みと比較して「危機管理の強化」の割合が低く、「業務の受注に有利」と「その他」の割合が高い。
- 「BCMS認証取得」と「取引先への事業継続の確認」は「社会的な信用向上」と「取引先からの要求」の割合が他の取組みよりも高い。
- 事業継続に関わる取組みは、多くの組織で継続されている。
- 無回答を除く300組織の内、44%（132）の組織が事業継続以外の目的でも活用し、56%（168）の組織が事業継続以外の目的で活用していない。

第7章
電子データの管理実態

設問38. 電子データの文書管理規則策定状況(N=352)

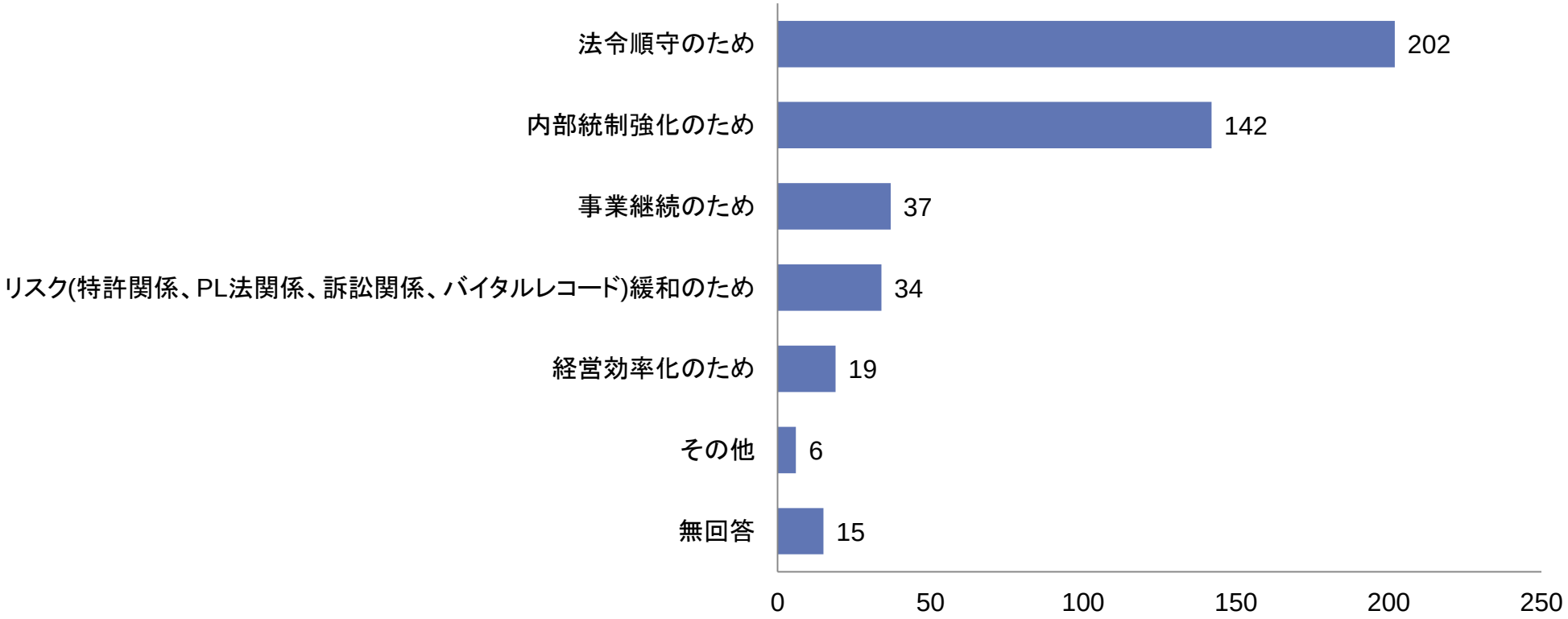


72%の組織が電子データの文書管理規則を策定済であり、
25%の組織が電子データの文書管理規則を未策定である。

第7章　電子データの管理実態

※設問38.で「**紙文書・電子データともに文書管理規則はない**」と回答した組織を除く

設問39. 文書管理規則の策定・運用の目的（2つまで回答可）（N=313）

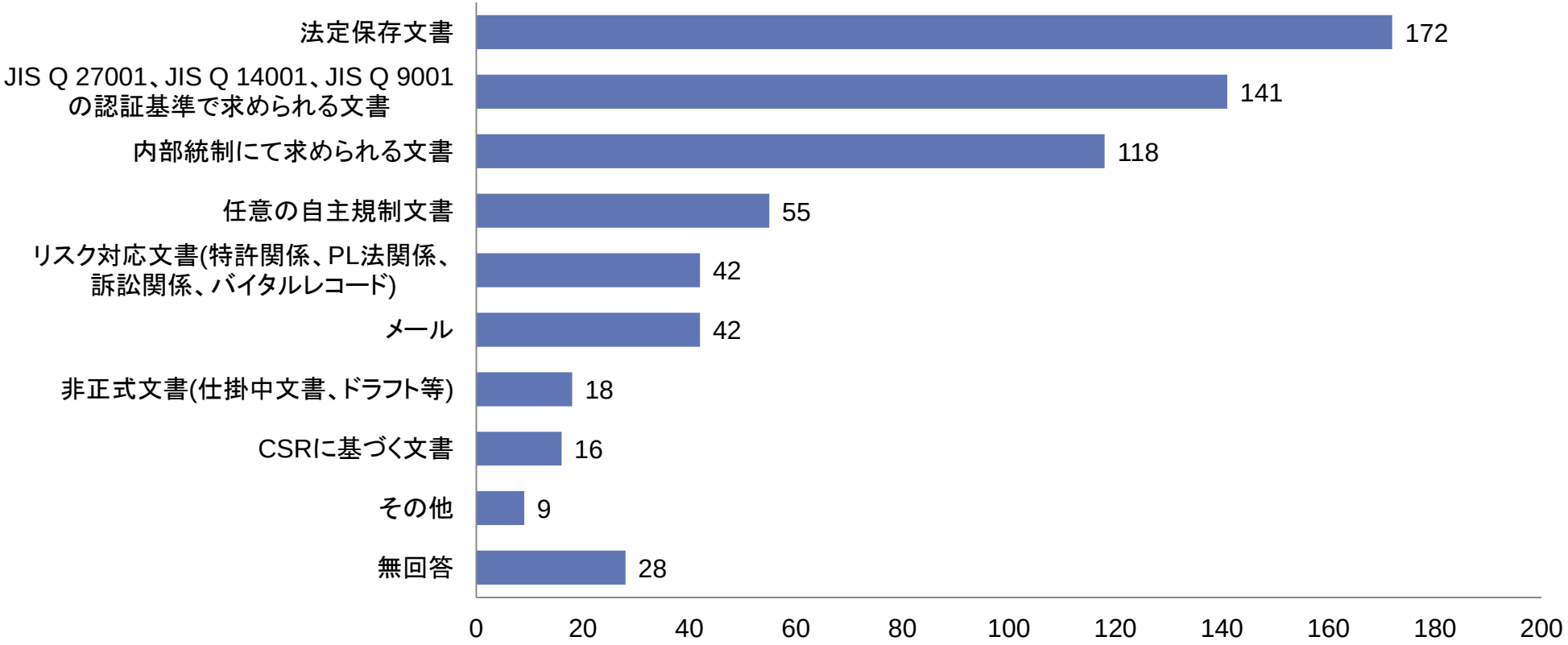


多くの組織が「法令順守」、「内部統制強化」の目的で文書管理規則を策定・運用している。

第7章　電子データの管理実態

※設問38.で「**紙文書・電子データともに文書管理規則はない**」と回答した組織を除く

設問40. 文書管理規則の対象（複数回答可）(N=313)

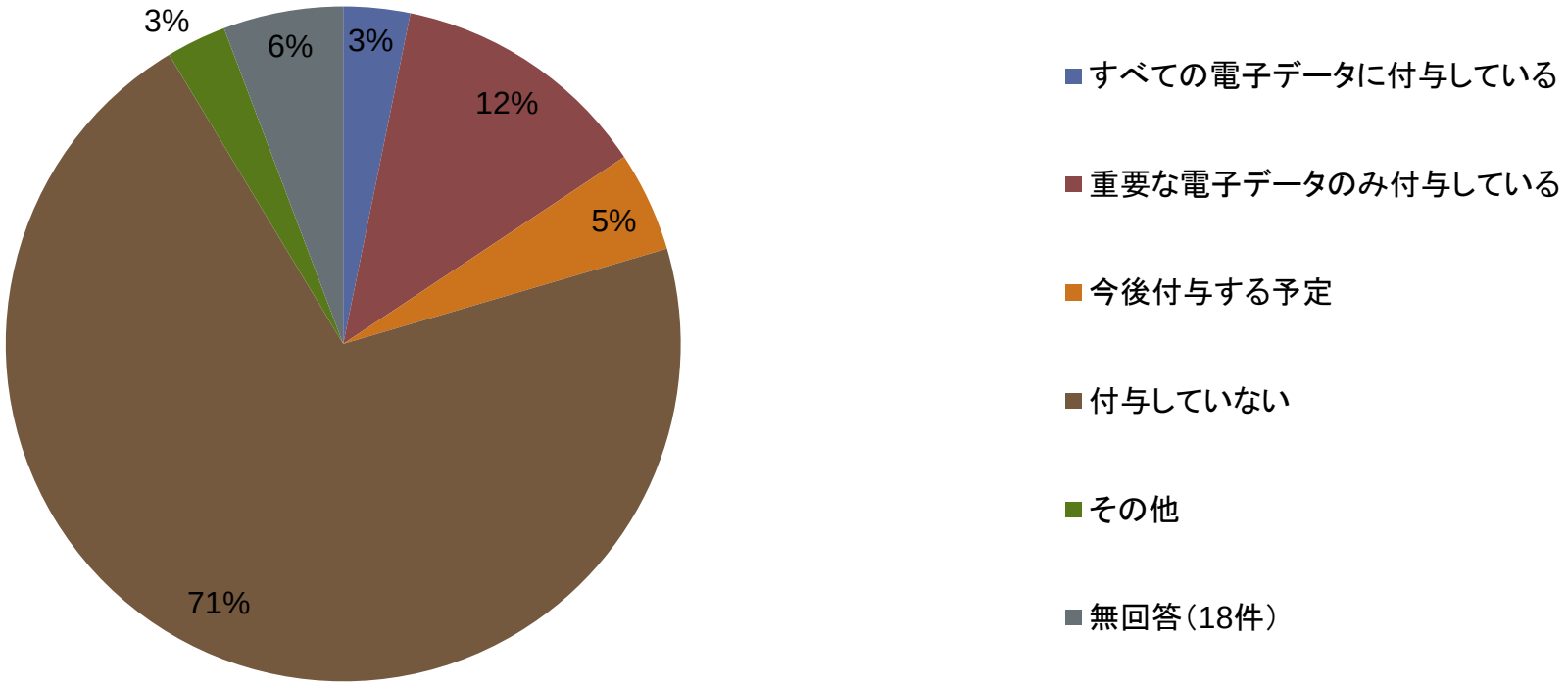


「法定保存」、「認証基準」及び「内部統制」で求められる文書を対象とする組織が多く、「メール」、「非正式文書」を対象とする組織は少ない。

第7章　電子データの管理実態

※設問38.で「**紙文書・電子データともに文書管理規則はない**」と回答した組織を除く

設問41. 電子署名・タイムスタンプの付与状況(N=313)

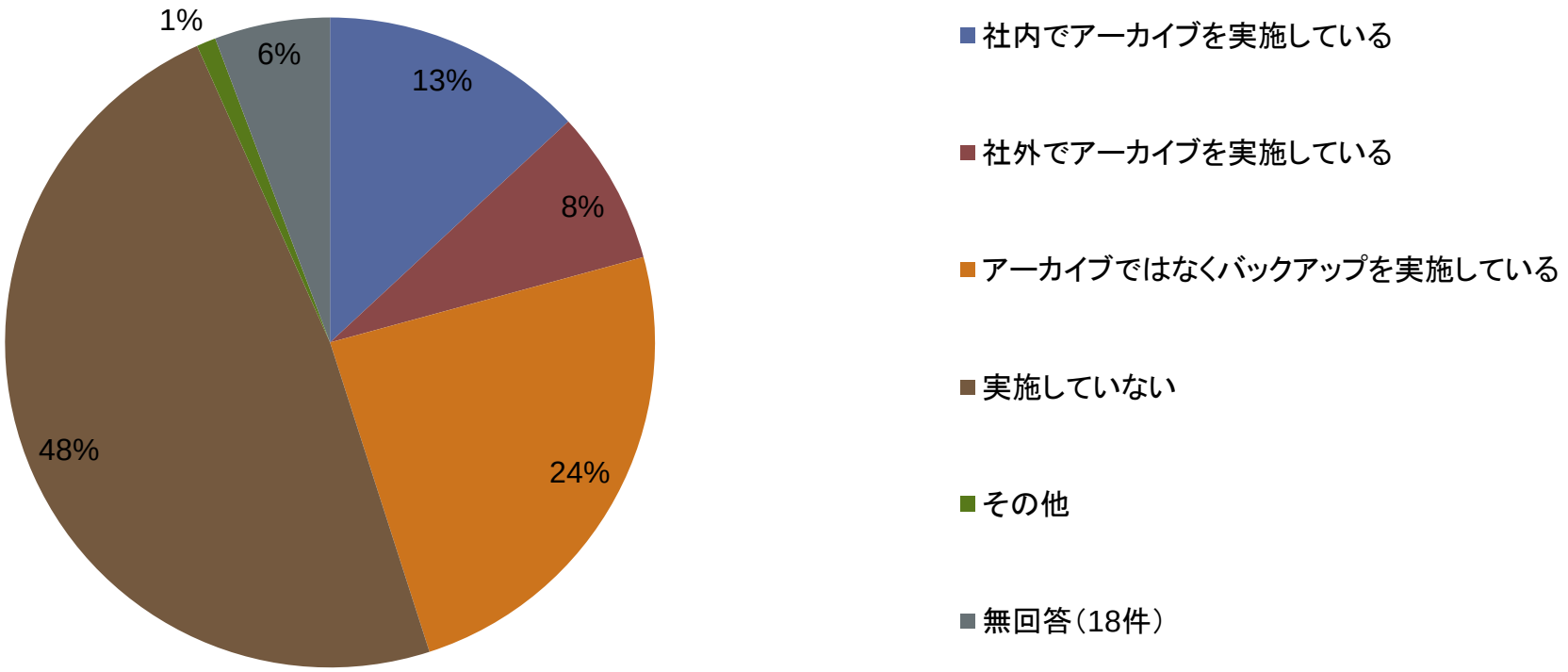


20%の組織が電子データに電子署名・タイムスタンプを付与・付与予定であり、71%の組織が付与していない。

第7章　電子データの管理実態

※設問38.で「**紙文書・電子データともに文書管理規則はない**」と回答した組織を除く

設問42. メールの保管対策(N=313)

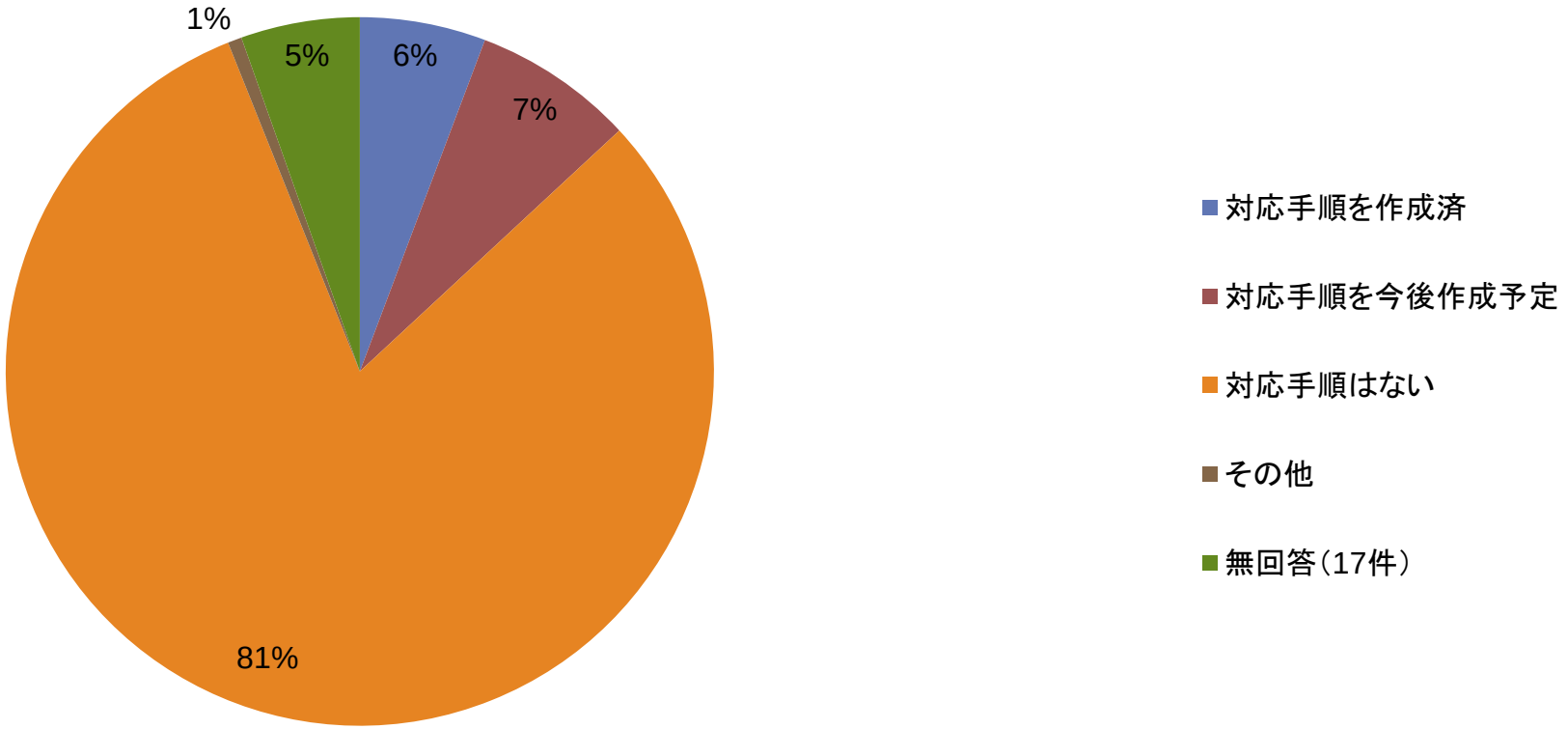


45%の組織がメール保管対策を実施済であり、
48%の組織がメール保管対策を未実施である。

第7章　電子データの管理実態

※設問38.で「**紙文書・電子データともに文書管理規則はない**」と回答した組織を除く

設問43. 訴訟ホールド対応手順の作成状況(N=313)

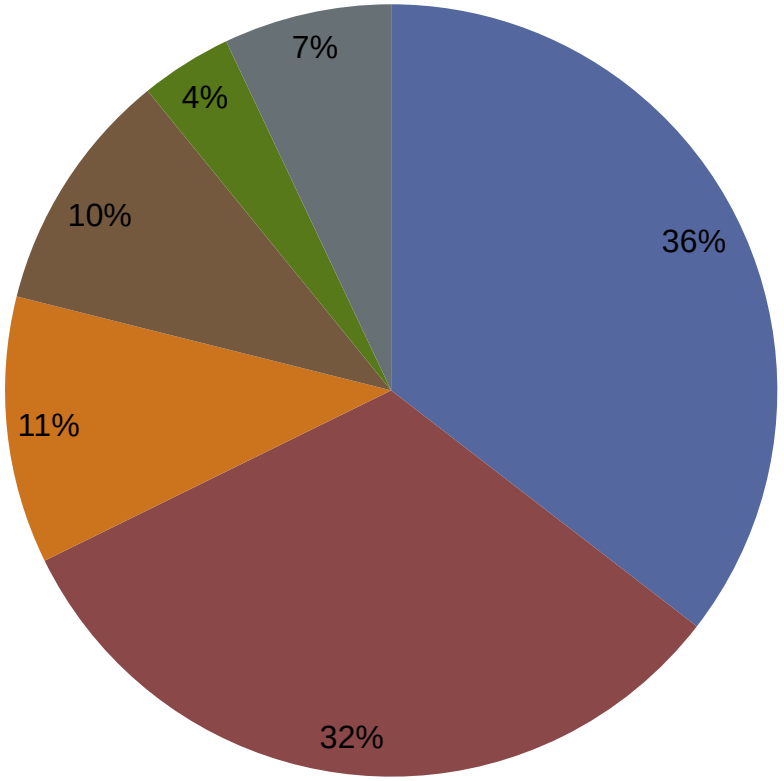


13%の組織が訴訟ホールドの対応手順を作成済・作成予定であり、81%の組織が訴訟ホールドの対応手順を未作成である。

第7章　電子データの管理実態

※設問38.で「**紙文書・電子データともに文書管理規則はない**」と回答した組織を除く

設問44. 廃棄フェーズの電子データの取扱(N=313)



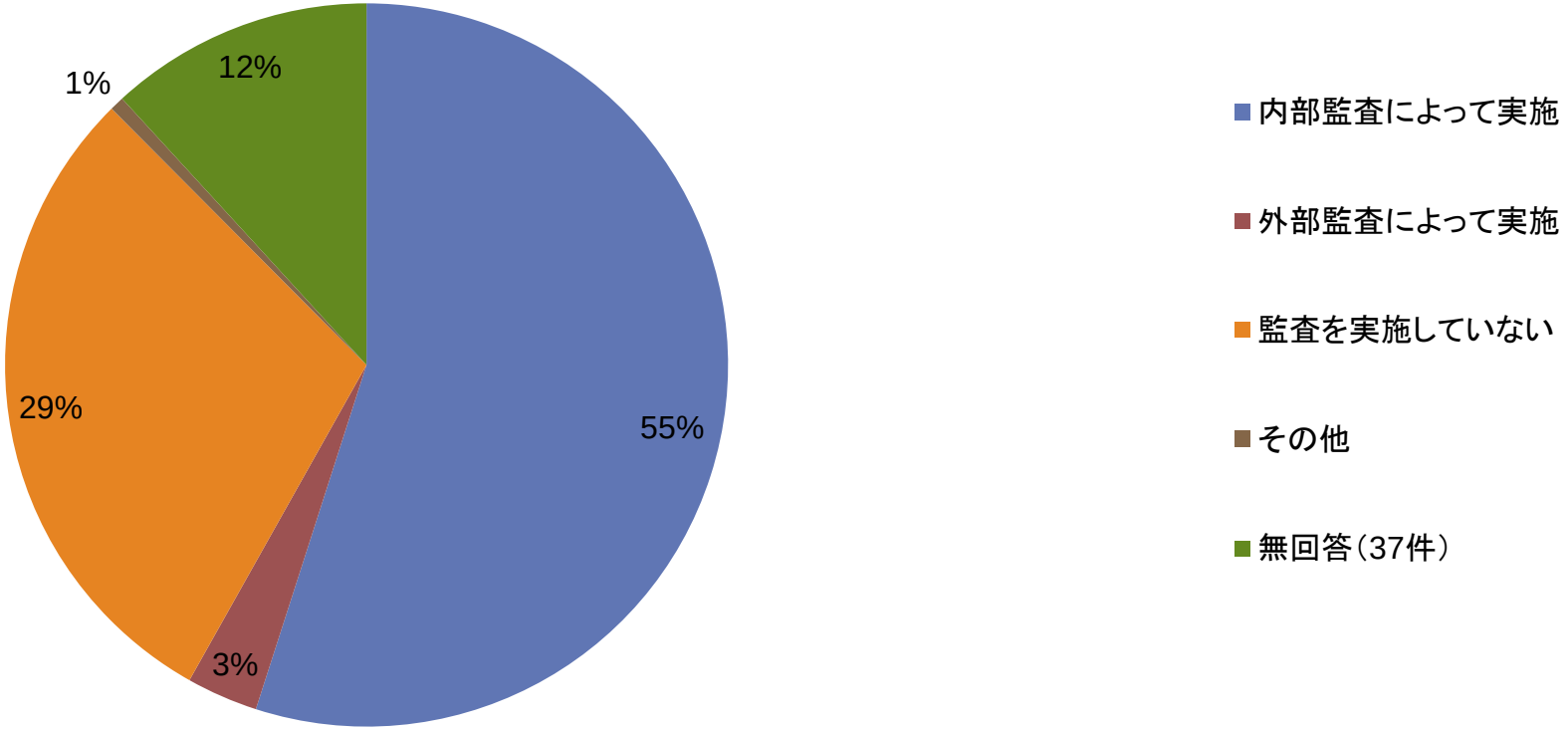
- 電子データを削除する。廃棄の作業過程(いつ、誰が、どのように)が分かる証跡を作成する
- 電子データを削除する。廃棄の作業過程(いつ、誰が、どのように)が分かる証跡を作成していない
- 電子データを削除する。別媒体にバックアップ取得する
- 電子データを削除していない
- その他
- 無回答（23件）

79%の組織が廃棄フェーズとなった電子データを削除している。

第7章　電子データの管理実態

※設問38.で「**紙文書・電子データともに文書管理規則はない**」と回答した組織を除く

設問45. 電子データのライフサイクルの監査の仕組(N=313)



58%の組織が電子データのライフサイクル（作成・編集・保管・保存・廃棄）の監査を実施している。

考察 （第7章　電子データの管理実態）

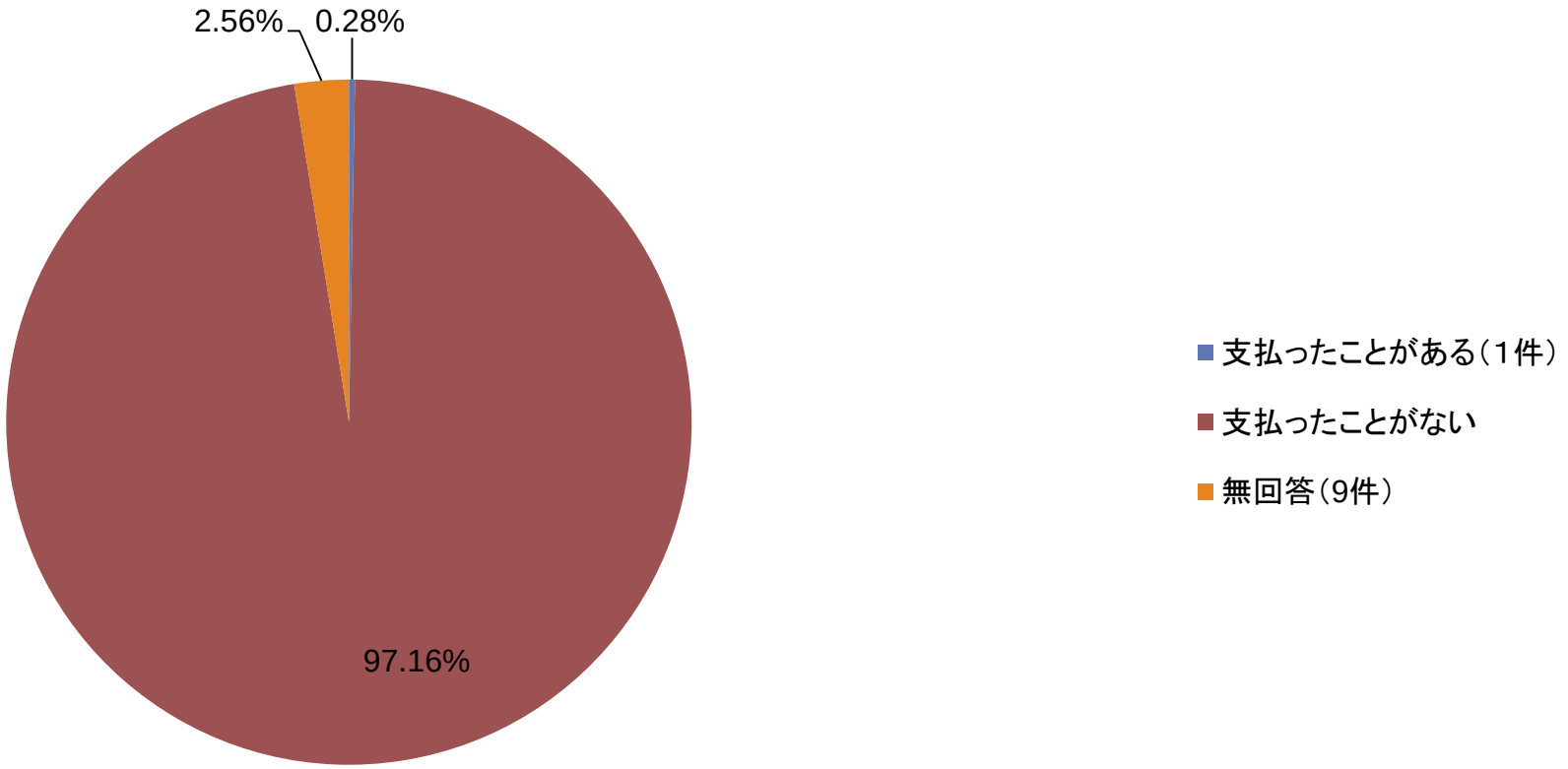
- 72%の組織が電子データの文書管理規則を策定済である。
- 文書管理規則の対象として、「法定保存文書」、「認証基準で求められる文書」及び「内部統制にて求められる文書」を対象とする組織が多く、一方、「メール」、「非正式文書」を対象とする組織は少ない。
- 電子データに電子署名・タイムスタンプを20%の組織が付与・付与予定であり、71%の組織が付与していない。
- メールの保管対策を45%の組織が実施済であり、48%の組織が未実施である。
- 訴訟ホールドの対応手順を13%の組織が作成済・作成予定であり、81%の組織が未作成である。
- 79%の組織が廃棄フェーズとなった電子データを削除している。

第8章
個人情報漏えい事故のお詫び金

第8章　個人情報漏えい事故のお詫び金

設問46. 過去にお詫び金を支払ったことがある組織(N=352)

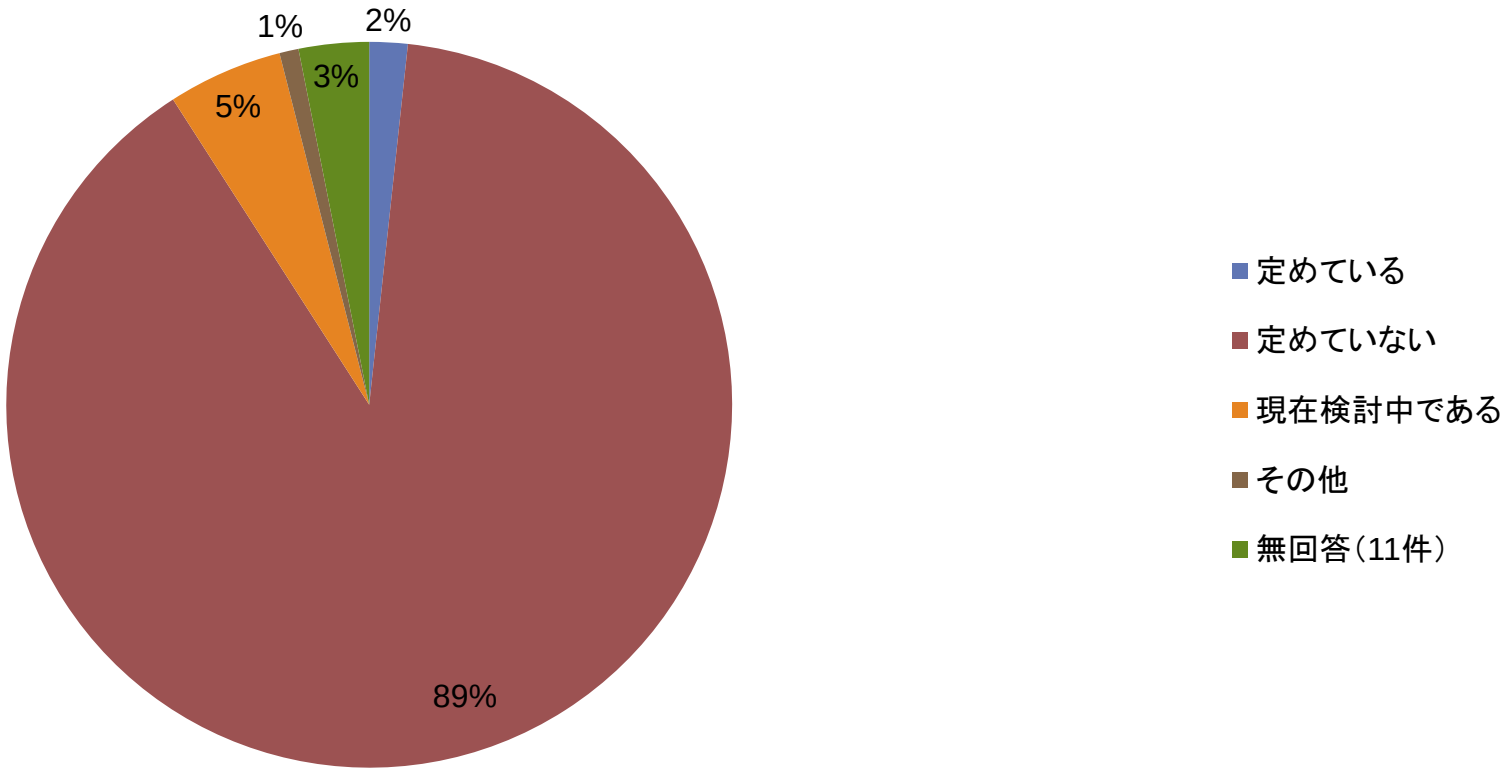
設問47. お詫び金額の決定方法



支払ったことがある組織は、回答のあった343件中1件であり、
この1件は過去の事例を参考にしてお詫び金の額を決定していた。

第8章　個人情報漏えい事故のお詫び金

設問48. お詫び金に関する基準策定状況(N=352)

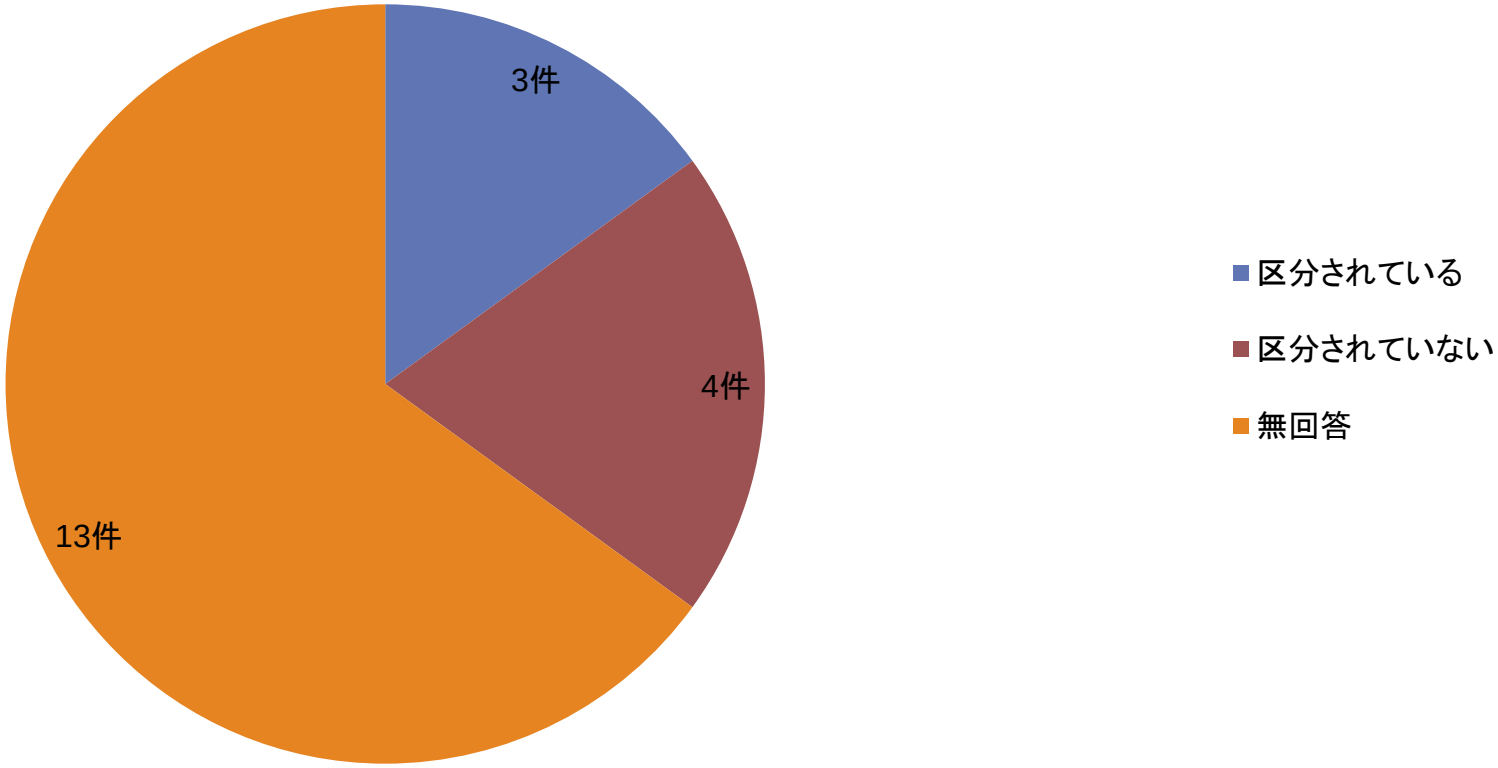


基準を定めていた組織は2%であり、検討中は5%である。
89%が基準を定めていない。

第8章　個人情報漏えい事故のお詫び金

※設問48.で「**定めていない**」と「**現在検討中**」と回答した組織を除く

設問49. 個人情報の種類によるお詫び金支払額の区分の有無(N=20)

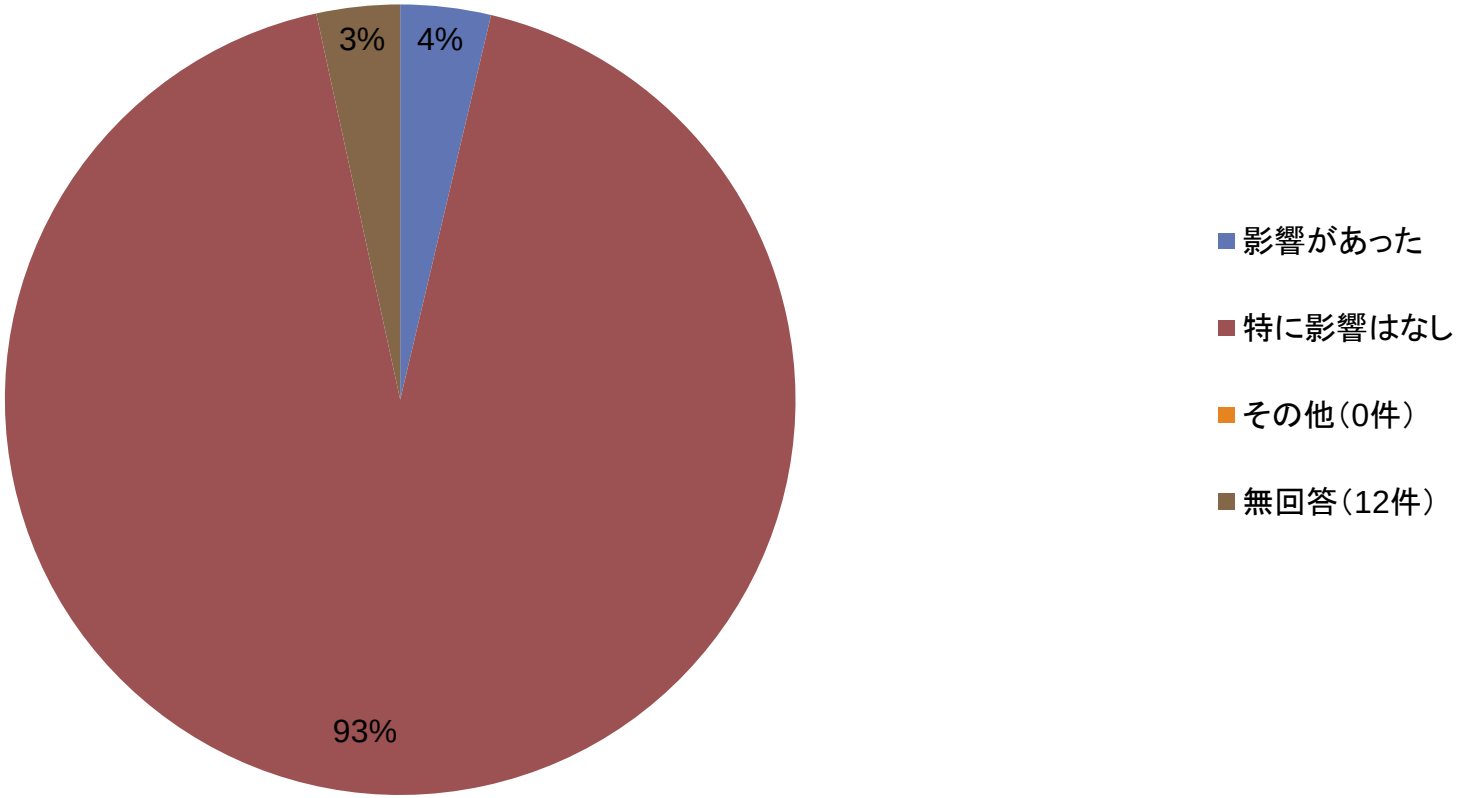


3組織では個人情報の種類によって区分している。

第8章　個人情報漏えい事故のお詫び金

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

設問50. 大規模個人情報漏えい事件の影響(N=352)

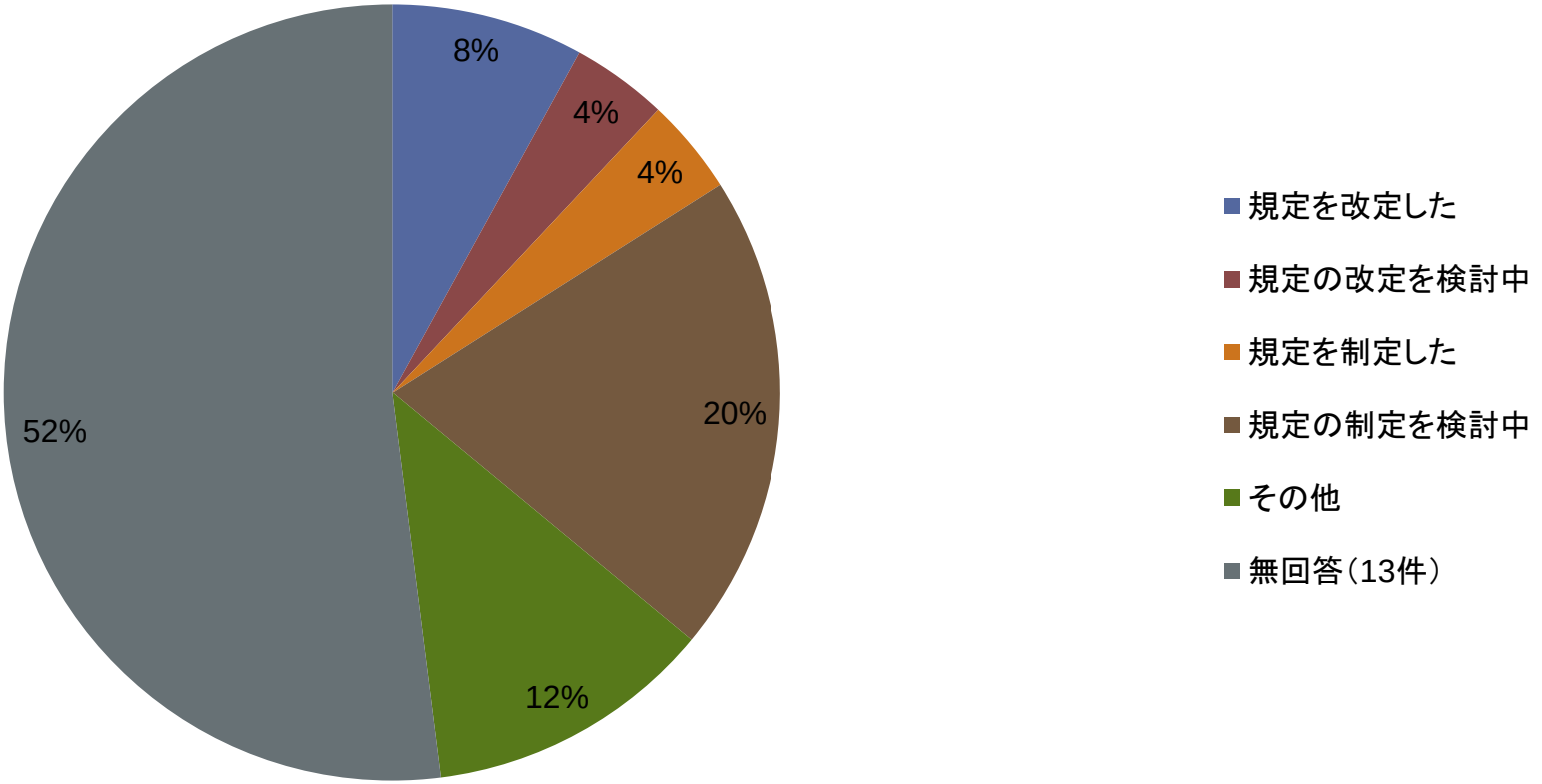


4%の組織のお詫び金規定に影響があった。

第8章　個人情報漏えい事故のお詫び金

※設問50.で「**特に影響はなし**」と回答した組織を除く

設問51. 大規模個人情報漏えい事件の影響内容(N=25)

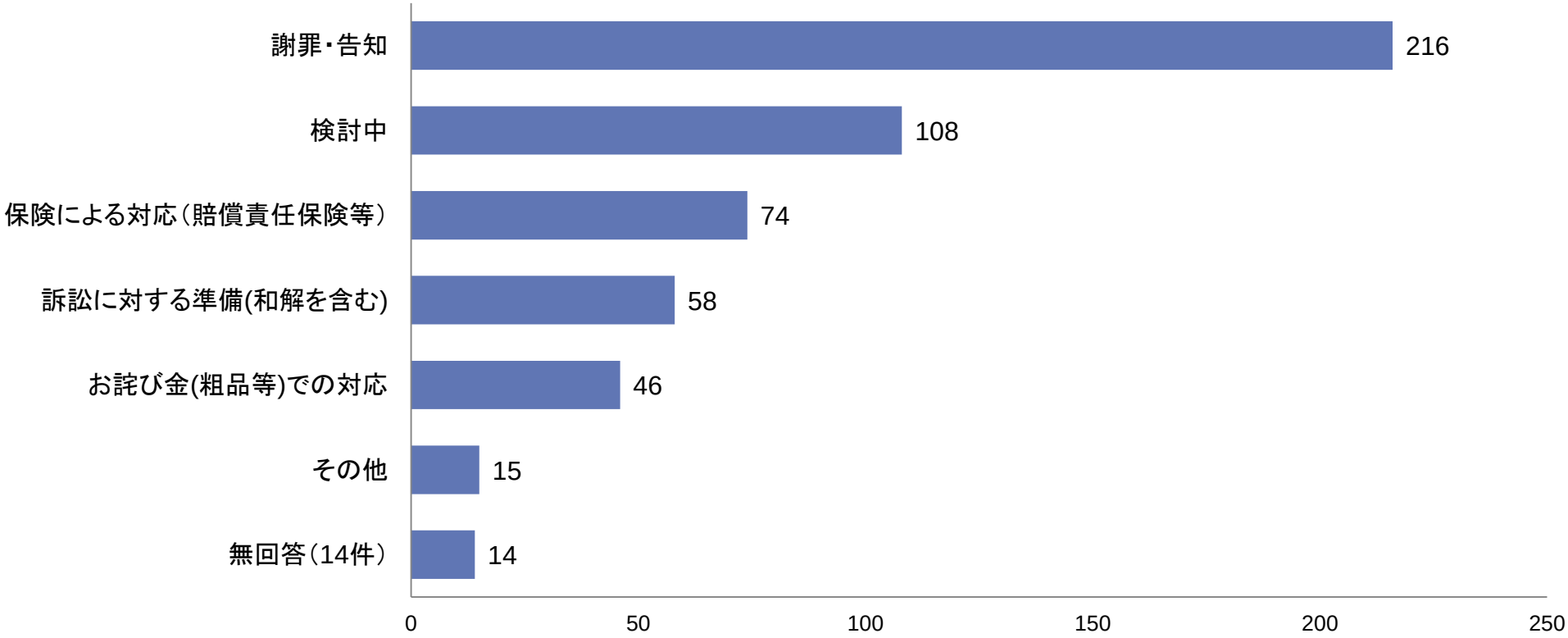


3組織（12%）が規定を改定し（検討中を含む）、
6組織（24%）が新規に制定した（検討中を含む）。

第8章　個人情報漏えい事故のお詫び金

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

設問52. 個人情報漏えい時の対応案(複数回答可)(N=352)

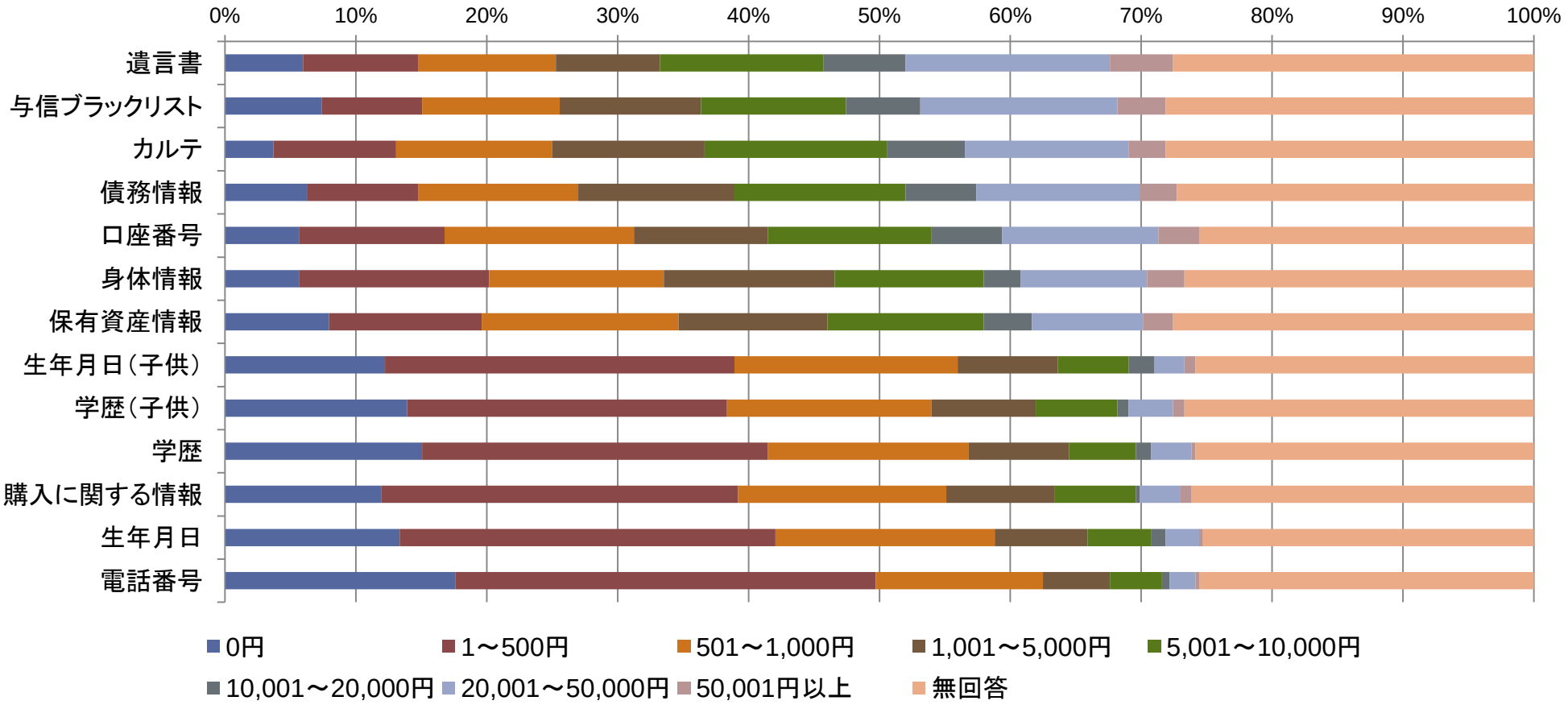


「謝罪・告知」が216件(61%)と圧倒的であった。
「お詫び金(粗品等)での対応」は46件(13%)に留まった。

第8章　個人情報漏えい事故のお詫び金

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

設問53. 情報漏えい時の想定支払額(N=352)



「遺言書」、「与信ブラックリスト」、「カルテ」、「債務情報」の金額が高かった。

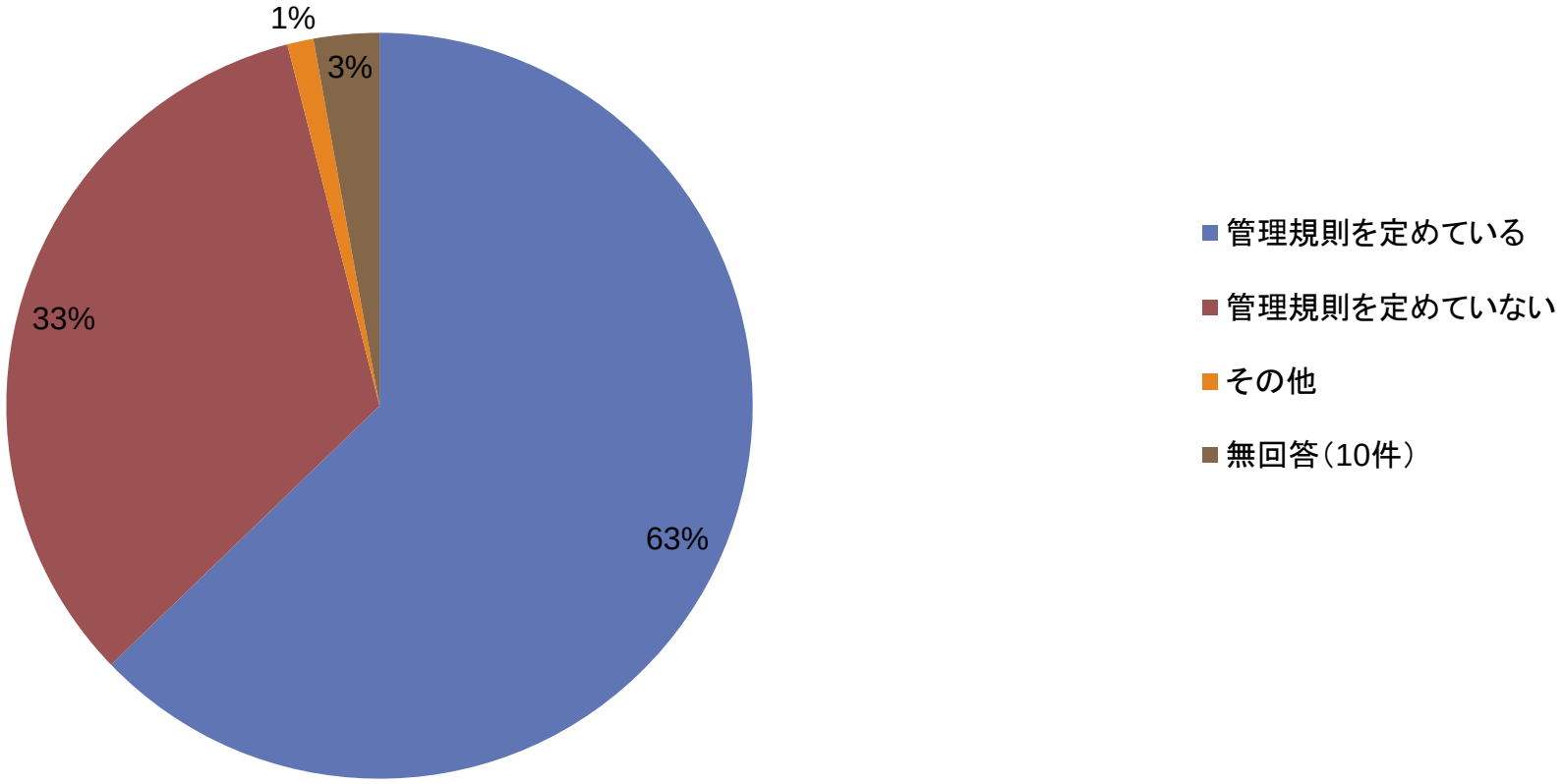
考察 （第8章　個人情報漏えい事故のお詫び金）

- お詫び金を支払ったことがある組織は、回答のあった343件中1件であり、この1件は過去の事例を参考にしてお詫び金の額を決定していた。
- お詫び金支払額の基準を定めていた組織は2%であり、検討中は5%である。89%が基準を定めていない。
- 個人情報の種類によるお詫び金支払額は、3組織で個人情報の種類によって区分している。
- 大規模個人情報漏えい事件を受けて、4%の組織のお詫び金規定に影響があった。その内、3組織が規定を改定し（検討中を含む）、6組織が新規に制定した（検討中を含む）。
- 個人情報漏えい時の対応としては、「謝罪・告知」が216件（61%）と圧倒的であり、「お詫び金（粗品等）での対応」は46件（13%）に留まった。
- 情報漏えい時の想定支払額としては、「遺言書」、「与信ブラックリスト」、「カルテ」、「債務情報」の金額が高かった。

第9章
管理者権限（特権ID）の運用状況

第9章　管理者権限（特権ID）の運用状況

設問54. 管理者権限の運用ルール制定状況 （N=352）

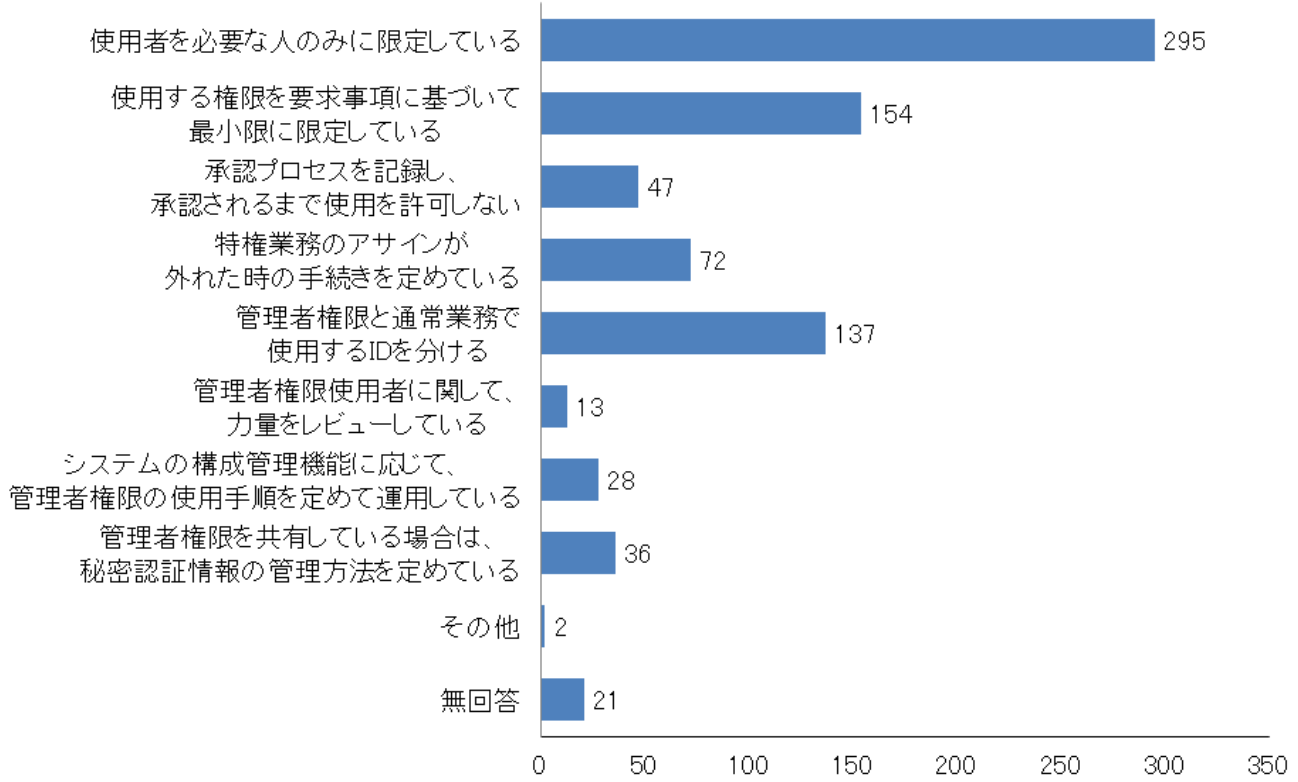


運用ルールとして「管理規則を定めている」が63%、
「管理規則を定めていない」が33%であった。

第9章　管理者権限（特権ID）の運用状況

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

設問55. 管理者権限の運用に関して重視している施策（3つまで回答可）(N=352)



※ISO/IEC 27002;2013「9.2.3特権的アクセス権」の実施の手引きより記述順に回答を求めている。

回答の多かった項目は、「使用者の限定」84%　「使用者の最小限化」44%
「IDの使い分け」39%であった。

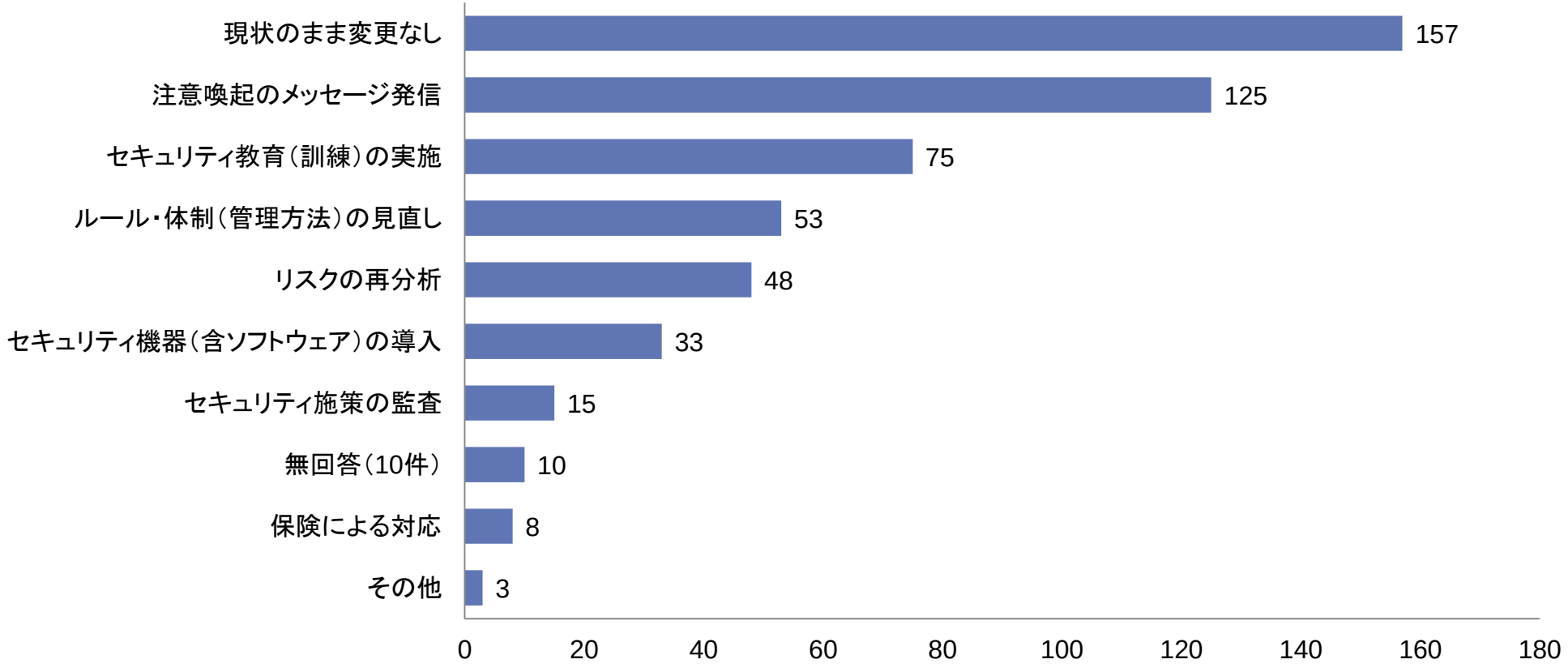
考察 （第9章　管理者権限（特権ID）の運用状況）

- 「管理規則を定めている」が63%、「管理規則を定めていない」が33%であった。管理規則の制定を行なっている組織は、全体の6割以上である。
- 管理者権限の運用に関して重視している施策は、回答の多いものから順に「使用者を必要な人のみに限定している」84%(295件)、「使用する権限を要求事項に基づいて最小限に限定している」44%(154件)、「管理者権限と通常業務で使用するIDを分ける」39%(137件)であった。
- 管理者権限の運用に関する管理策の実施には偏りがある。

第10章
日本年金機構の個人情報流出事案に関連する事項

第10章　日本年金機構の個人情報流出事案に関連する事項

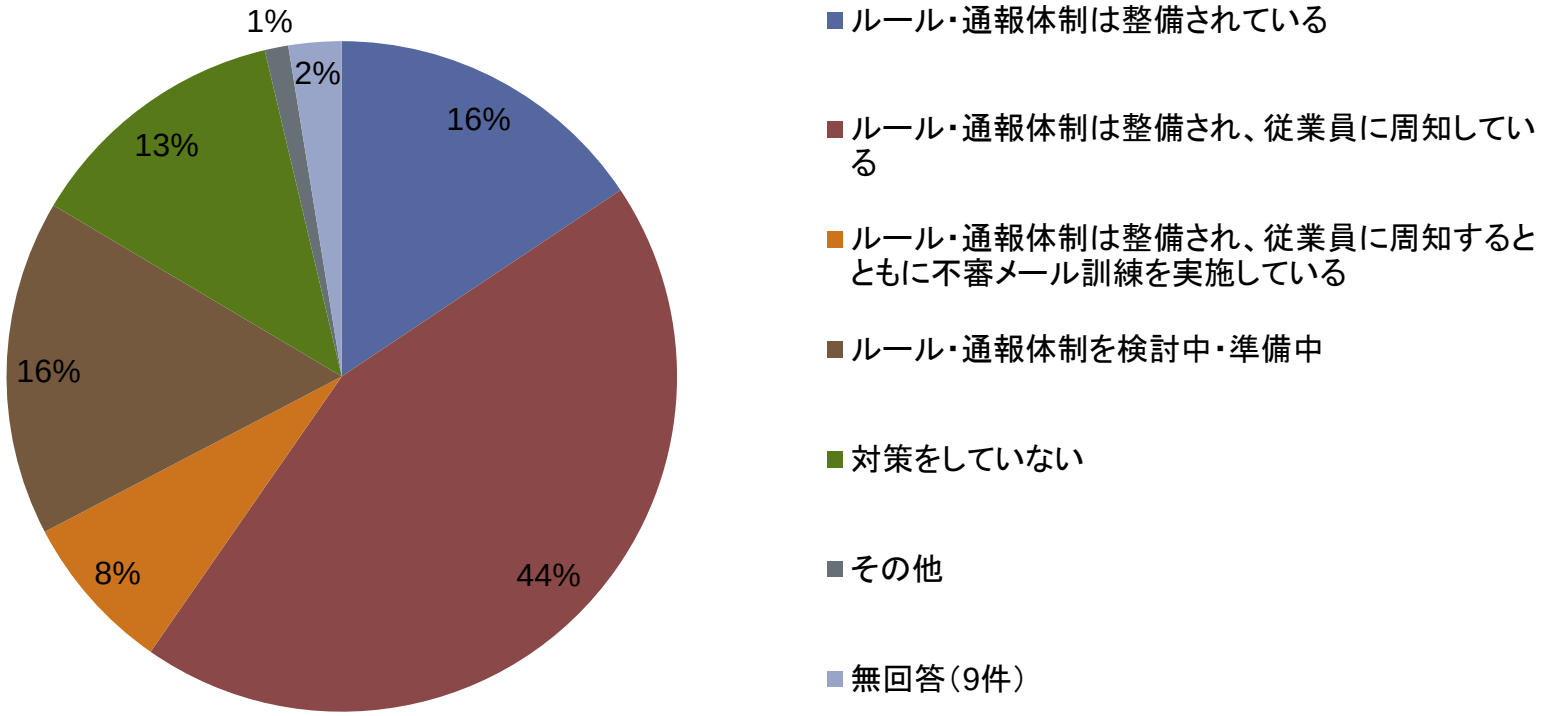
設問56. 日本年金機構の大量個人情報流出の報道を受け、組織で保有する重要データに対して実施した（予定）のセキュリティ施策（複数回答可）（N=352）



「現状のまま変更なし」が一番多い。

第10章　日本年金機構の個人情報流出事案に関連する事項

設問57. 不審なメールの受信時におけるルール・通報体制 （N=352）



68%の組織でルール・通報体制は既に整備されており、検討中・準備中も含めると84%になる。ただし13%の組織では対策をしていない。

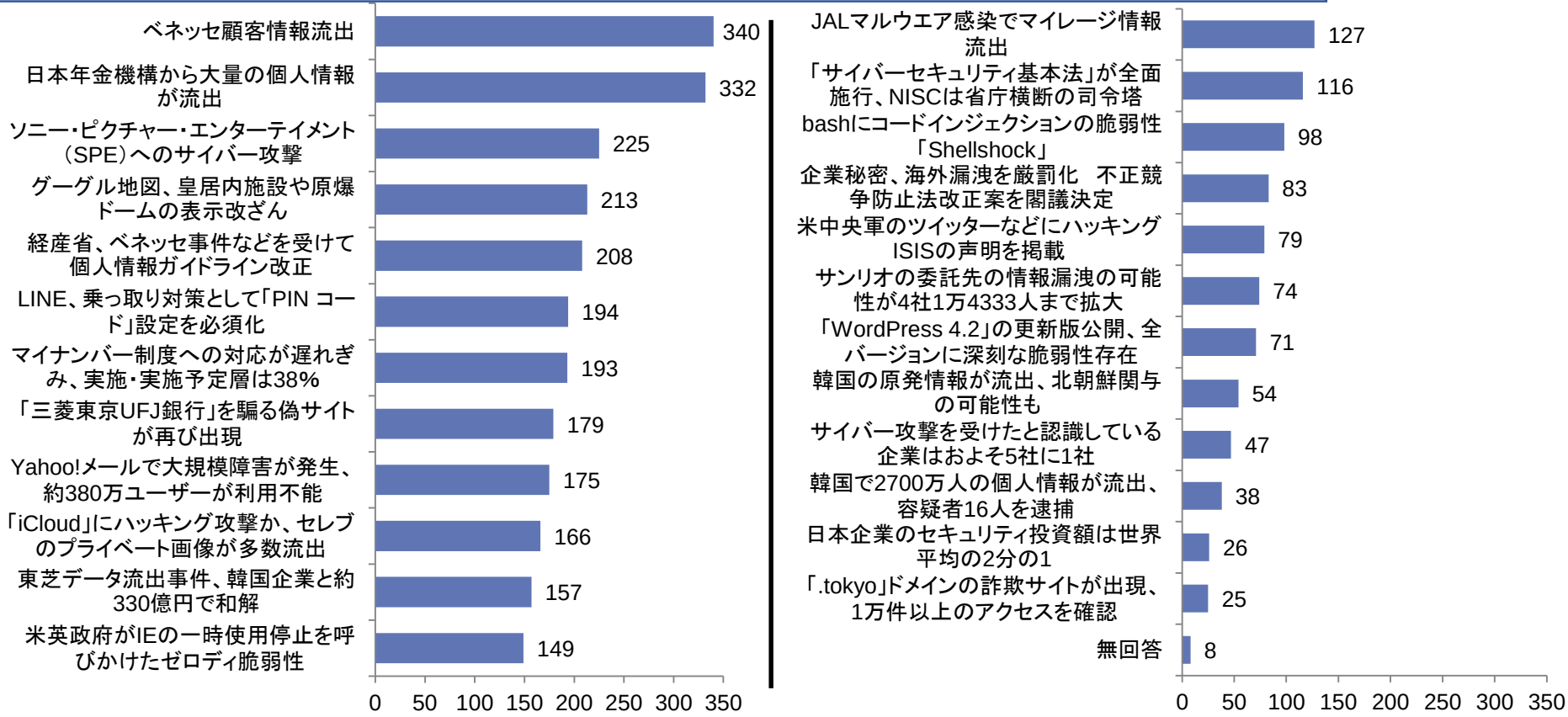
考察（第10章　日本年金機構の個人情報流出事案に関連する事項）

- 日本年金機構の事案を受けて実施する施策としては「現状のまま変更なし」（157組織・44.6%）が一番多かった。
- 237組織（68%）では、日本年金機構の事案前から不審メールに対するルール・通報体制が整備されていた。

第11章　その他
過去の事例･事故･用語の認知度

第11章　過去の事例・事故・用語の認知度

設問58. 出来事（事件・事故）の認知度（複数回答可）（N=352）

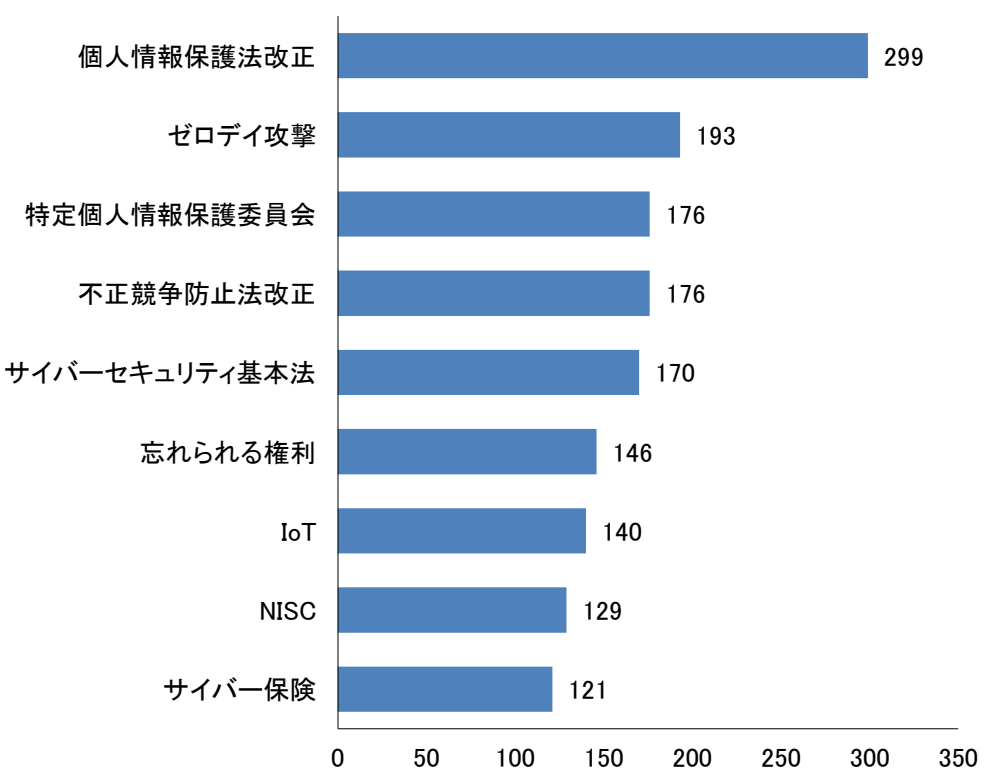


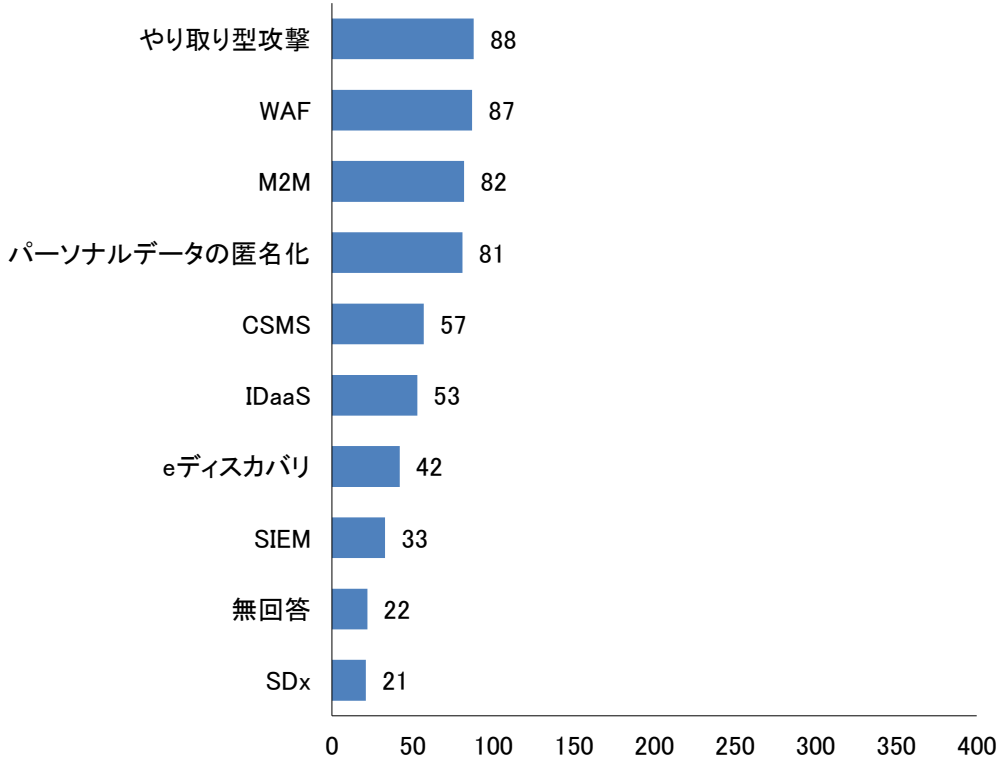
マスメディアで取り上げられた事件・事故への認知度が高く、あまり取り挙げられない海外事故や専門的なものについては認知度が高くない。「ベネッセ顧客情報流出」や、「年金機構から大量の個人情報が流出」の認知度は95%前後となっている。

第11章　過去の事例・事故・用語の認知度

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

設問59. 用語の認知度（複数回答可）（N=352）





個人情報保護法改正などの法律関連用語は、認知度が高い。
IoTは40%程度であったが、関連するM2MやCSMSは低い結果となった。
専門的な用語は、認知度が低い。

考察（第11章　その他（過去の事例・事故・用語の認知度））

- 例年の傾向とおり、マスメディアなどで取り上げられた事例・事故の認知度が高い。例えば、「ベネッセ顧客情報流出」や、「年金機構から大量の個人情報が流出」の認知度は95%前後となっている。一方、「米中央軍へのハッキング」や「韓国の情報流出」などの海外事例、「bash」や「Word Press」などの専門的な認知度は低い結果となっている。
- 個人情報保護法改正などの法律関連用語は、認知度が高い。IoTは40%程度であったが、関連するM2MやCSMSは低い結果となった。専門的な用語は、認知度が低い。

謝辞

本アンケート調査を実施するにあたり、

- アンケートへの回答にご協力を頂きました組織の皆様に感謝いたします。
- アンケートの封入、データ入力に多大なご協力を頂きました
  - 神奈川県立麻生養護学校　元石川分教室
  - 神奈川県立高津養護学校　川崎北分教室
  - 神奈川県立鶴見養護学校　岸根分教室
  - 神奈川県立みどり養護学校　新栄分教室
  - 川崎市立中央支援学校
  - 他1校の神奈川県内の特別支援学校（五十音順）

の皆様に感謝いたします。

情報セキュリティ大学院大学
原田研究室　一同