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

2014年情報セキュリティアンケート調査結果

2014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

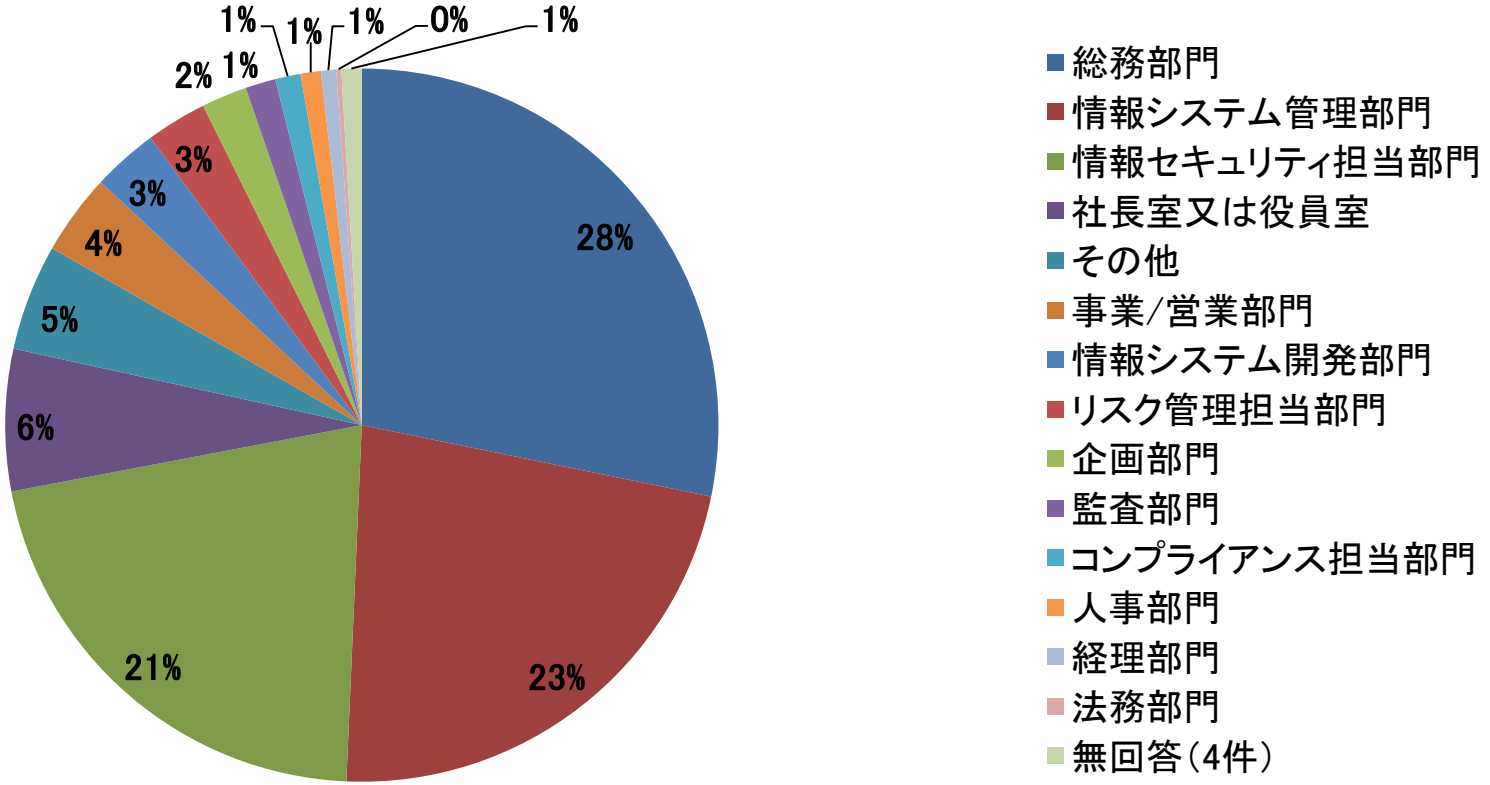
- アンケート実施期間
  2014年7月29日～8月22日
- アンケート対象
  Pマーク取得企業、ISMS認証取得企業、官公庁、教育機関(以下「組織」という。)など4,500組織の情報セキュリティ・システム担当者
- アンケート内容
  情報セキュリティマネジメントの取組状況、人的要因に関する情報セキュリティへの取組、情報セキュリティの人材育成と教育、個人の行動履歴データの取扱いなど
- 調査方法
  郵送による
- 回答状況
  437件（送達確認できた4,374組織に対して9.9%）

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．ご記入者の所属(N=437)

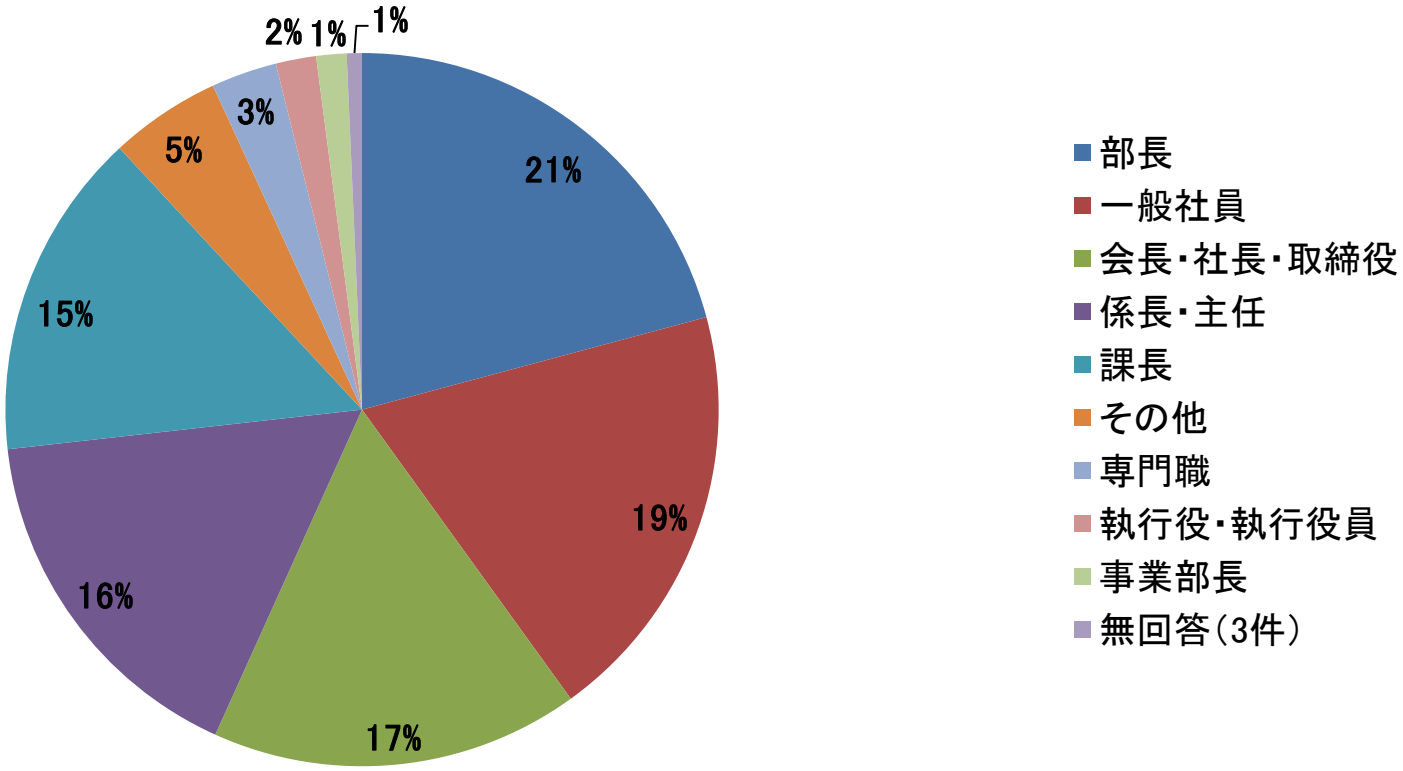


所属は、総務部門、情報システム管理部門、
情報セキュリティ担当部門順に多い。

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2. ご記入者の役職(N=437)

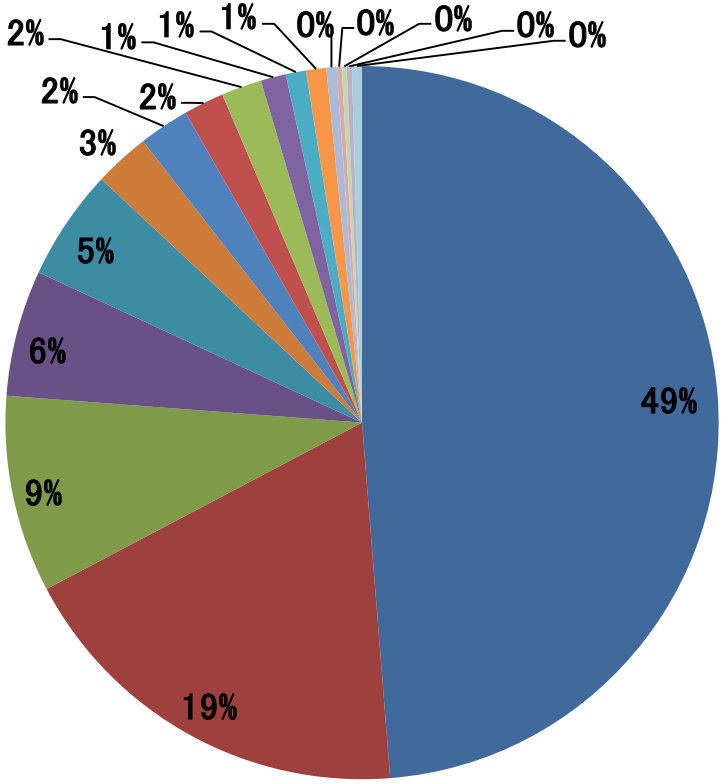


回答者の役職は、部長、一般社員、会長・社長・取締役、
係長・主任、課長の順に多い。

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3. 貴社の業種(N=437)



- 情報通信業
- 大学
- サービス業
- 公務
- 製造業
- 学術研究、専門・技術サービス業
- 運輸業、郵便業
- 建設業
- 教育、学習支援業
- 卸売業、小売業
- 金融業、保険業
- その他
- 医療、福祉
- 電気・ガス・熱供給・水道業
- 不動産業、物品賃貸業
- 生活関連サービス業、娯楽業
- 無回答（2件）

※1.農業、林業、漁業、鉱業、10. 宿泊業、飲食サービス業、17. 複合サービス事業(郵便局、協同組合)は該当なし

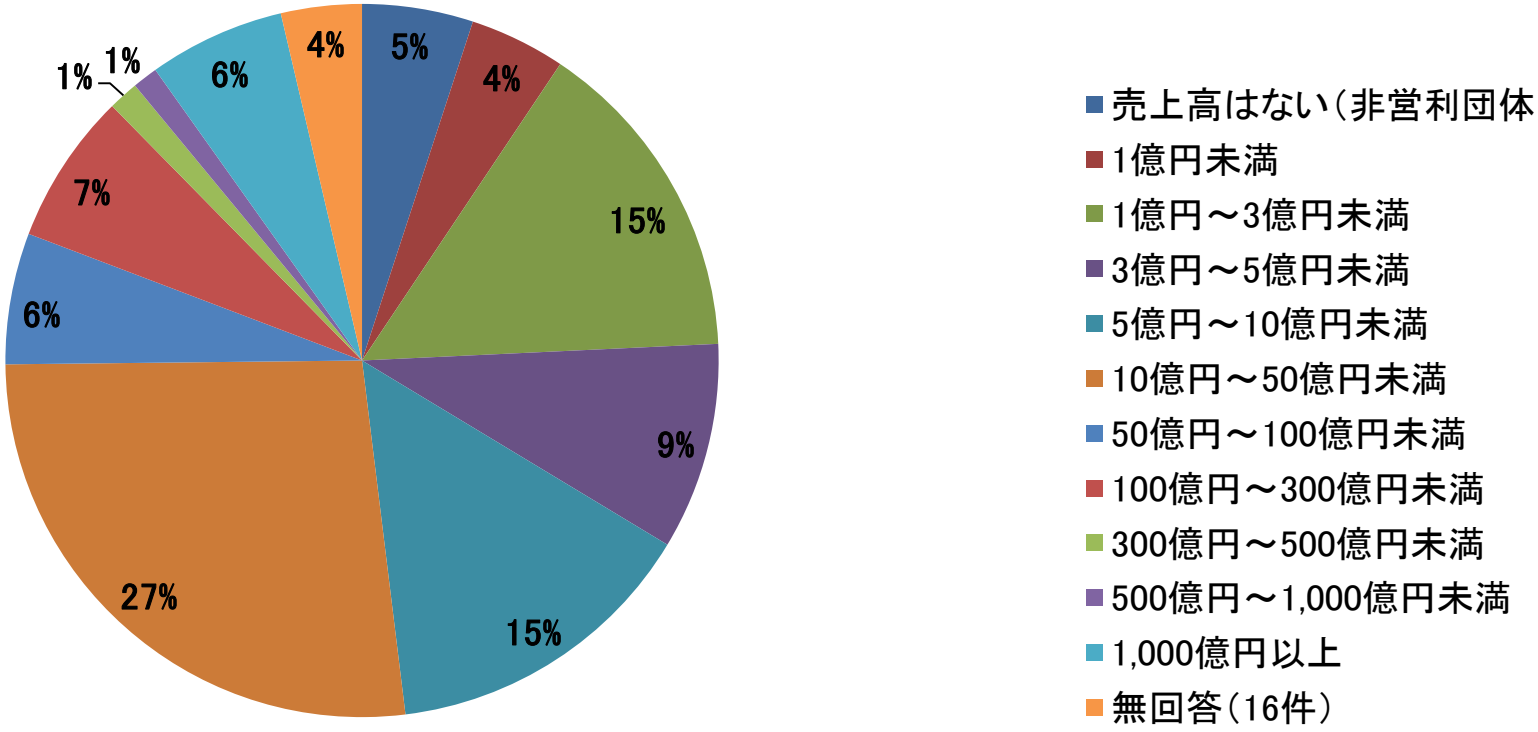
情報通信業が49%と半数近い割合となっている。

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=437）

※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、証券は営業収益高で算出

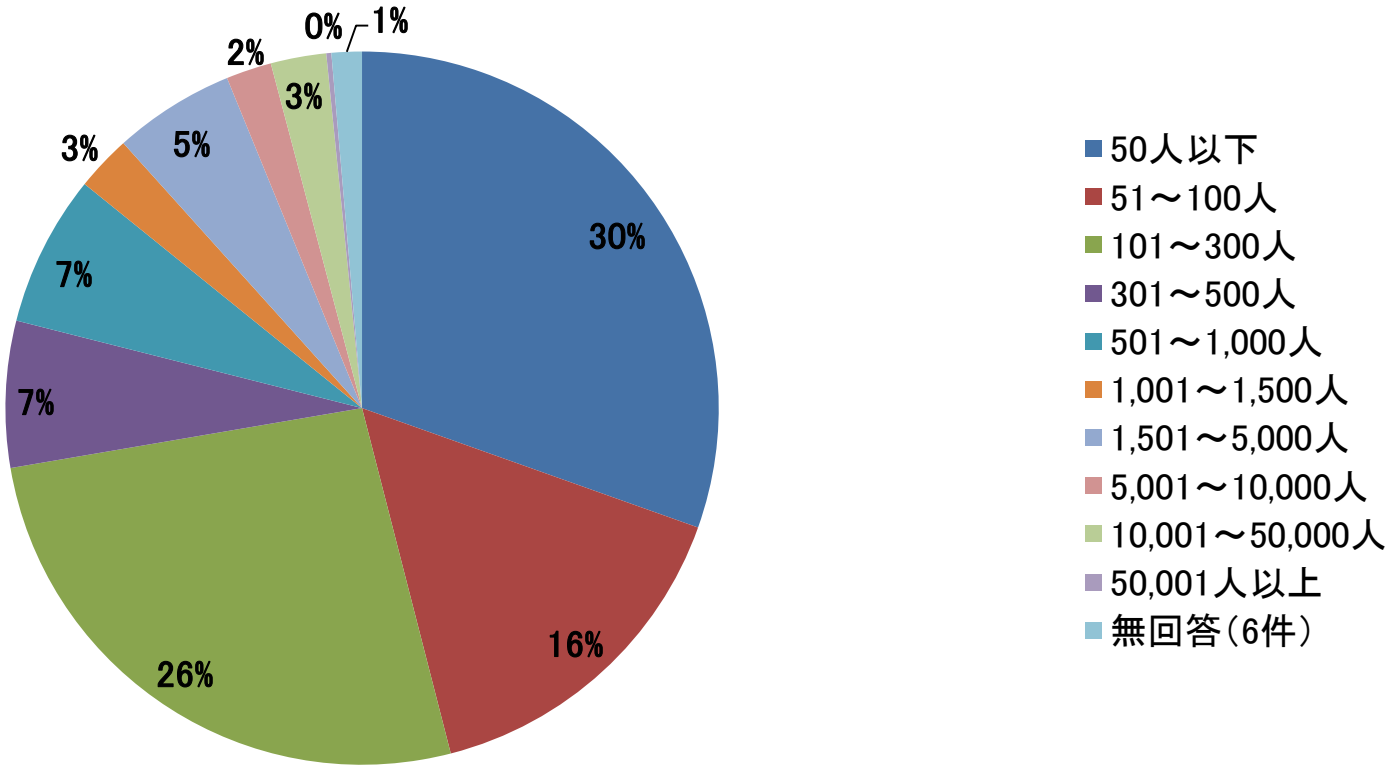


昨年同様に、売上高10億円から50億円の組織が一番多い。
また、売上高50億円未満の組織で7割を占める。

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5. 全従業員数(N=437)

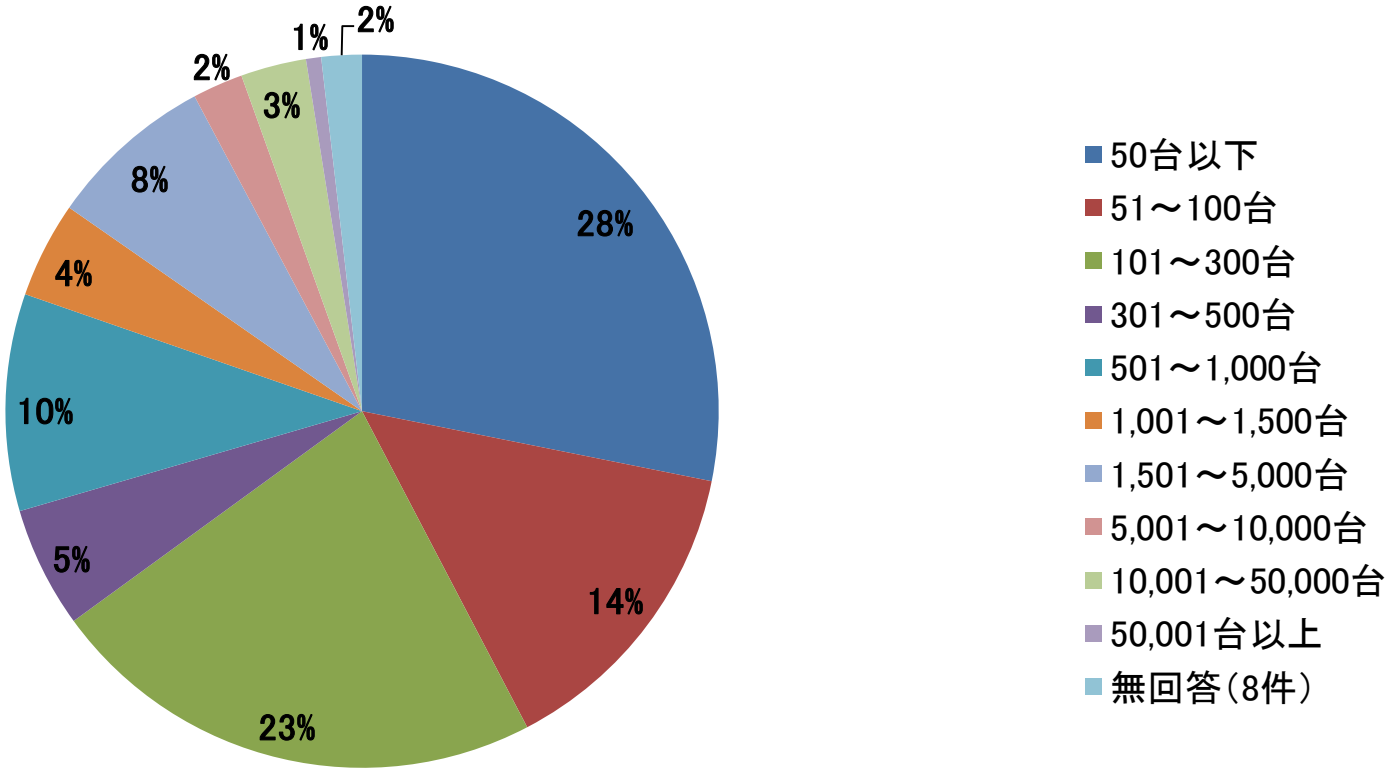


従業員数50人以下の組織が最も多い。

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. PC数（単独）(N=437)

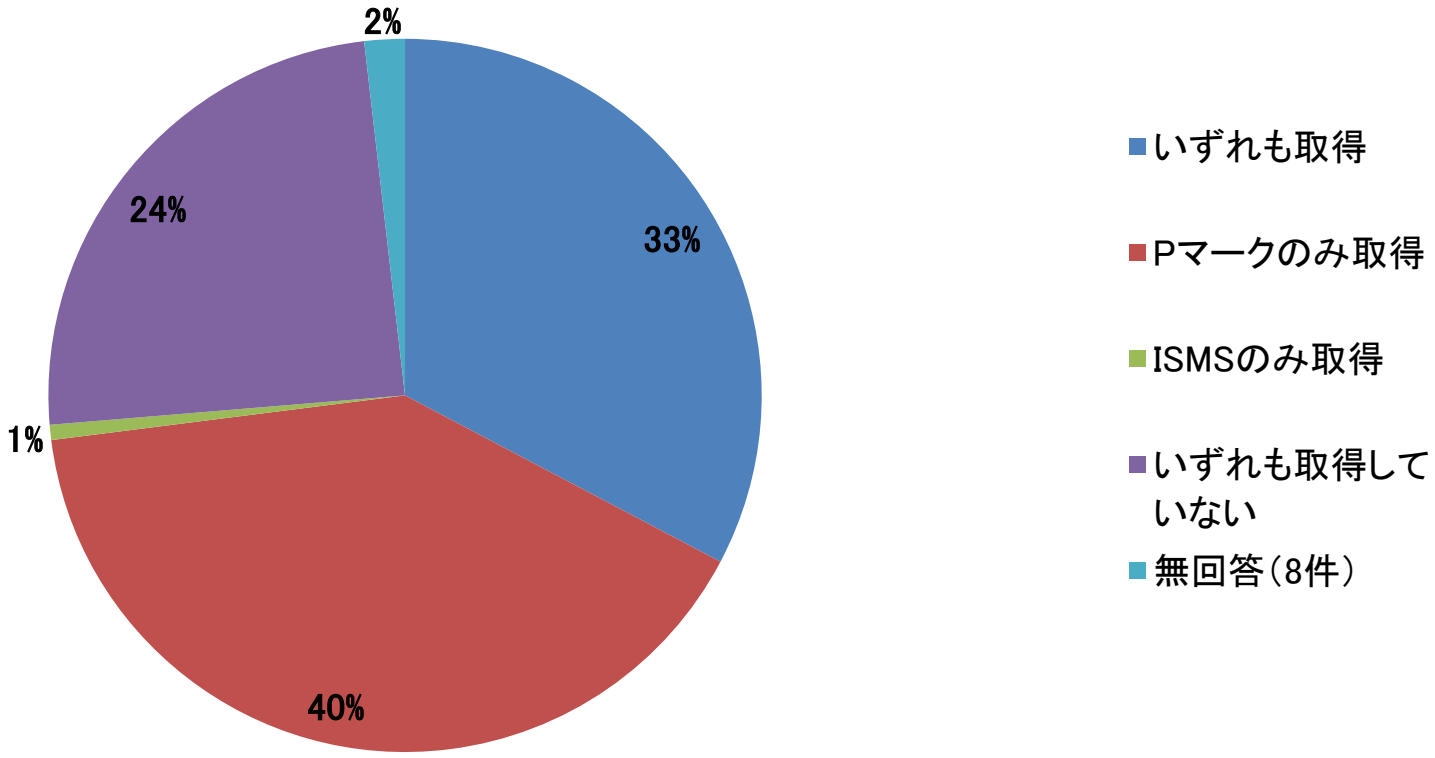


PC数300台以下の組織が65%を占める。

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．プライバシーマーク、ISMSの取得状況(N=437)

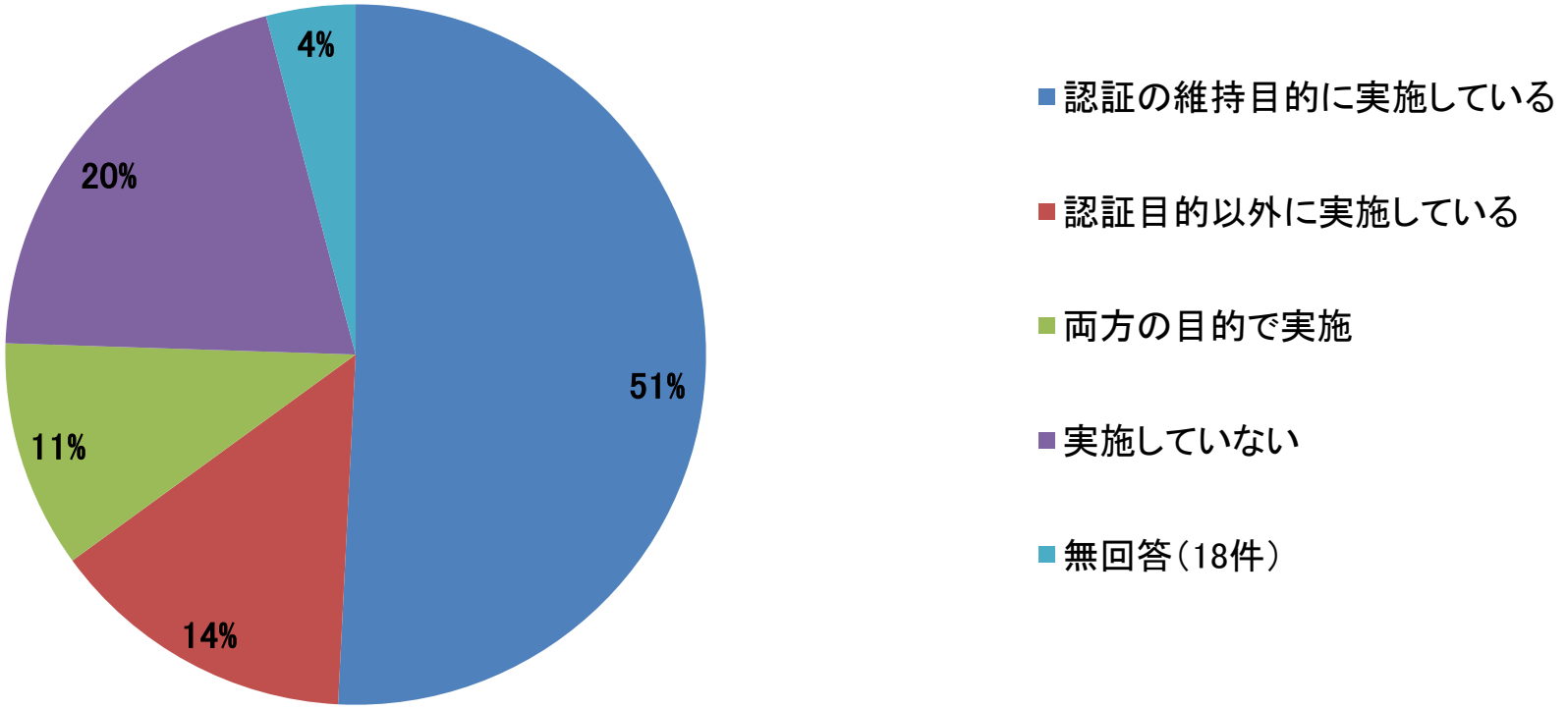


ISMSを取得している組織は、34%。Pマークは、73%。

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8. 情報セキュリティ監査の実施状況(N=437)



62%の組織が認証維持目的、25%が認証維持目的以外、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))

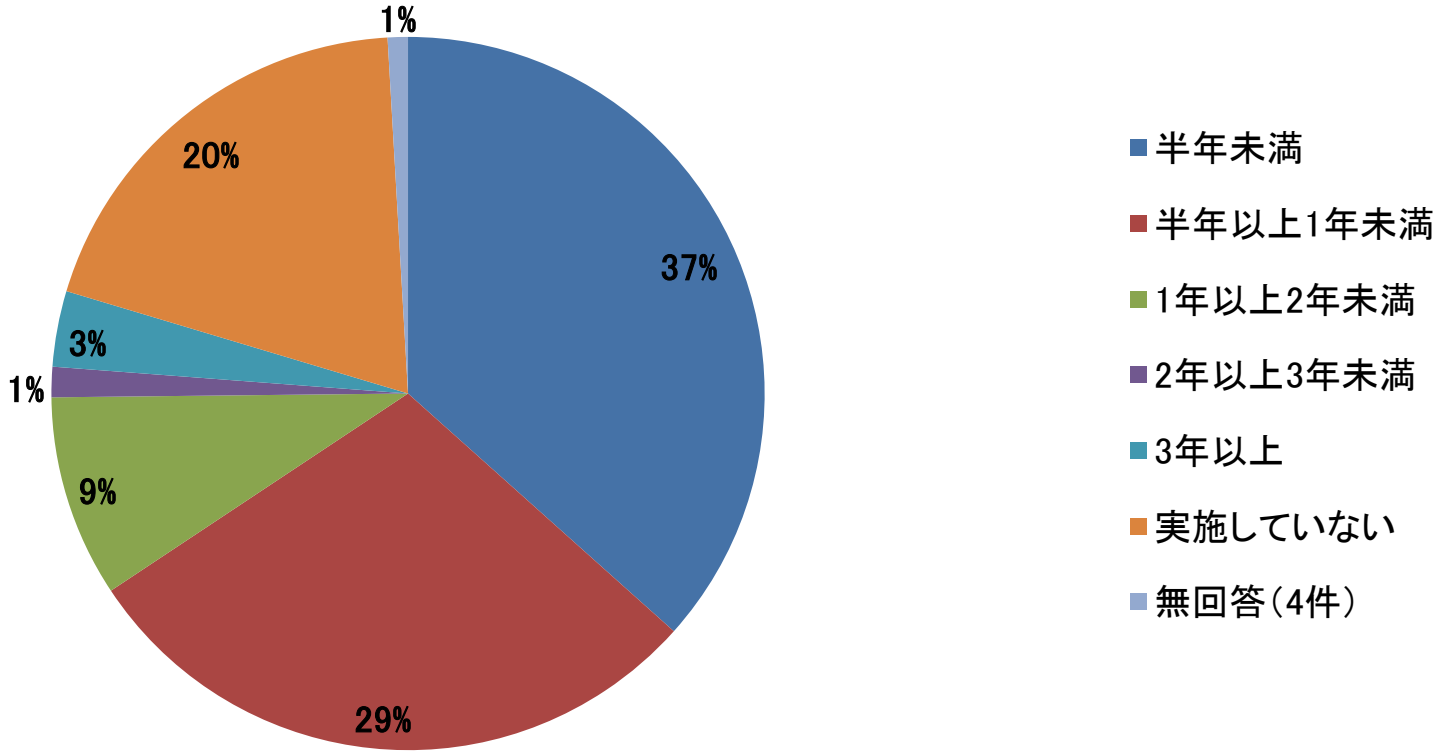
- アンケートに回答いただいた組織の傾向としては、従業員数300名以下の組織が72%となっている。

- 情報通信業が半数に近い割合を占めている。

第２章
情報セキュリティマネジメント
の取組み状況

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9．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時期(N=437)



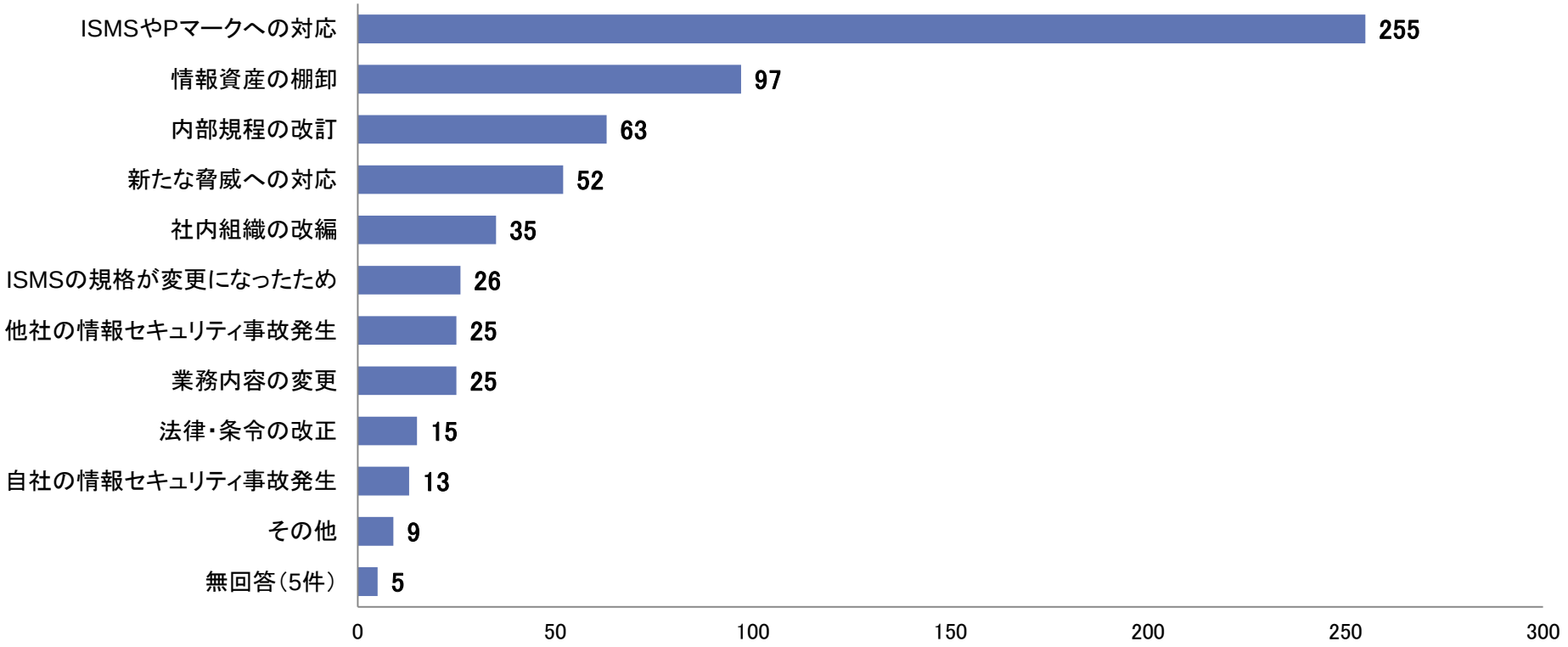
66%の組織が、1年未満の期間に実施している。
一方、20%の組織がリスク分析を実施していない。

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9.で「**6.実施していない**」と回答した組織を除く

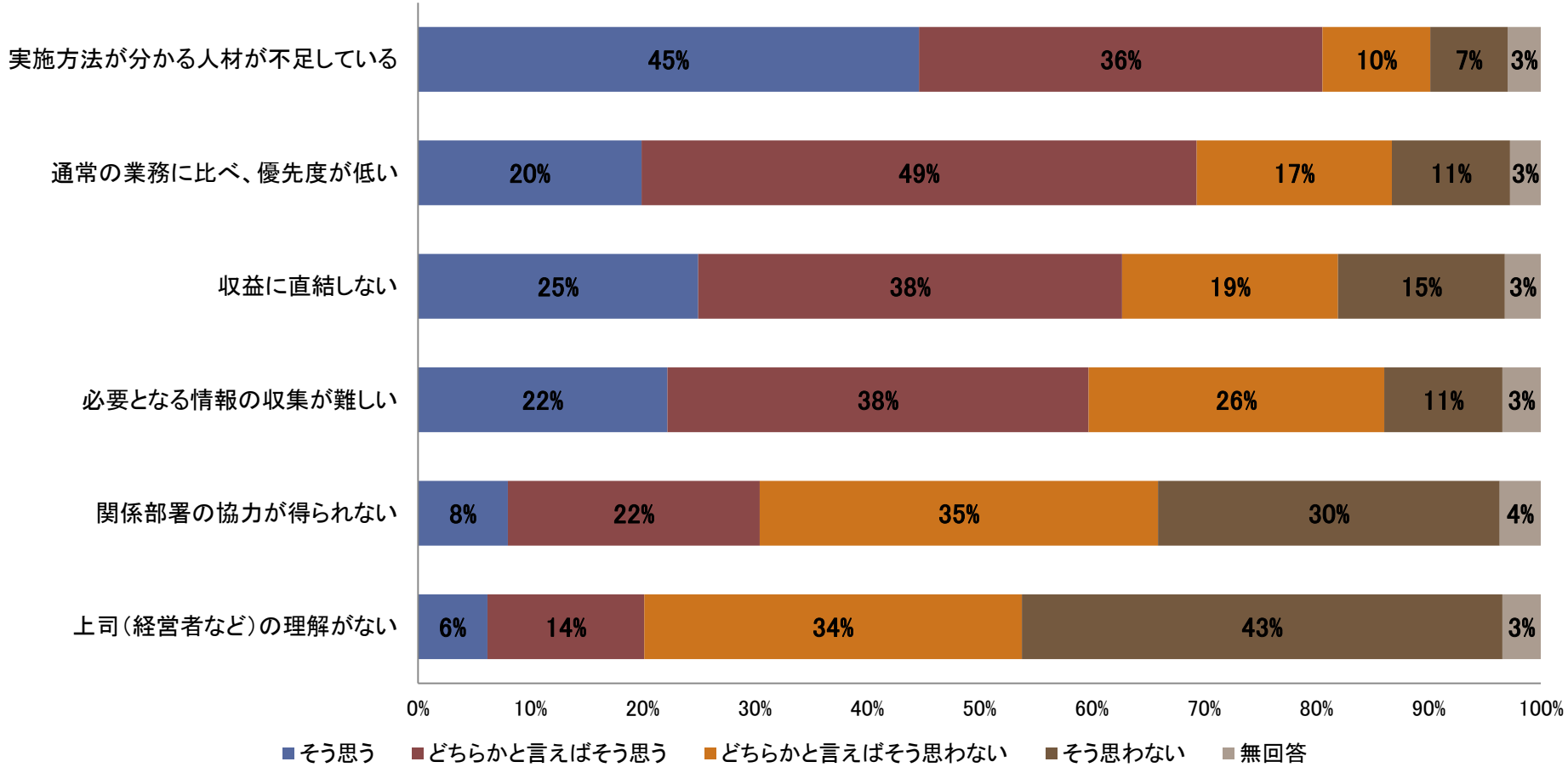
設問10. リスク分析を実施した理由(N=352)



ISMSやPマークへの対応が最も多く、情報資産の棚卸、内部規程の改訂が続く。

第2章　情報セキュリティマネジメントの取組み状況

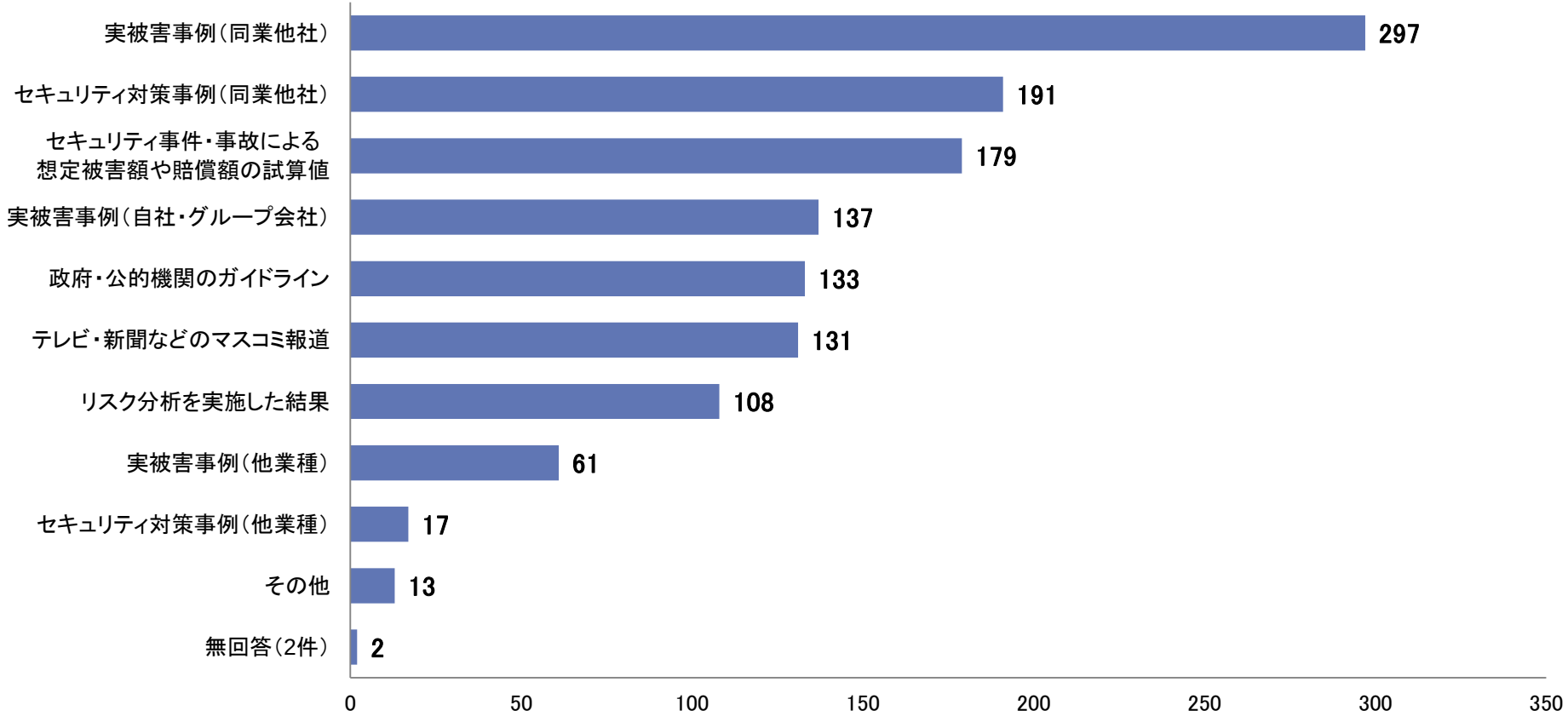
設問11．リスク分析を行う際の問題点(N=437)



人材の不足を感じる組織が81%。

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12．セキュリティ対策を進める上で経営者(責任者)に対する説得材料として有用と思うもの(N=437)

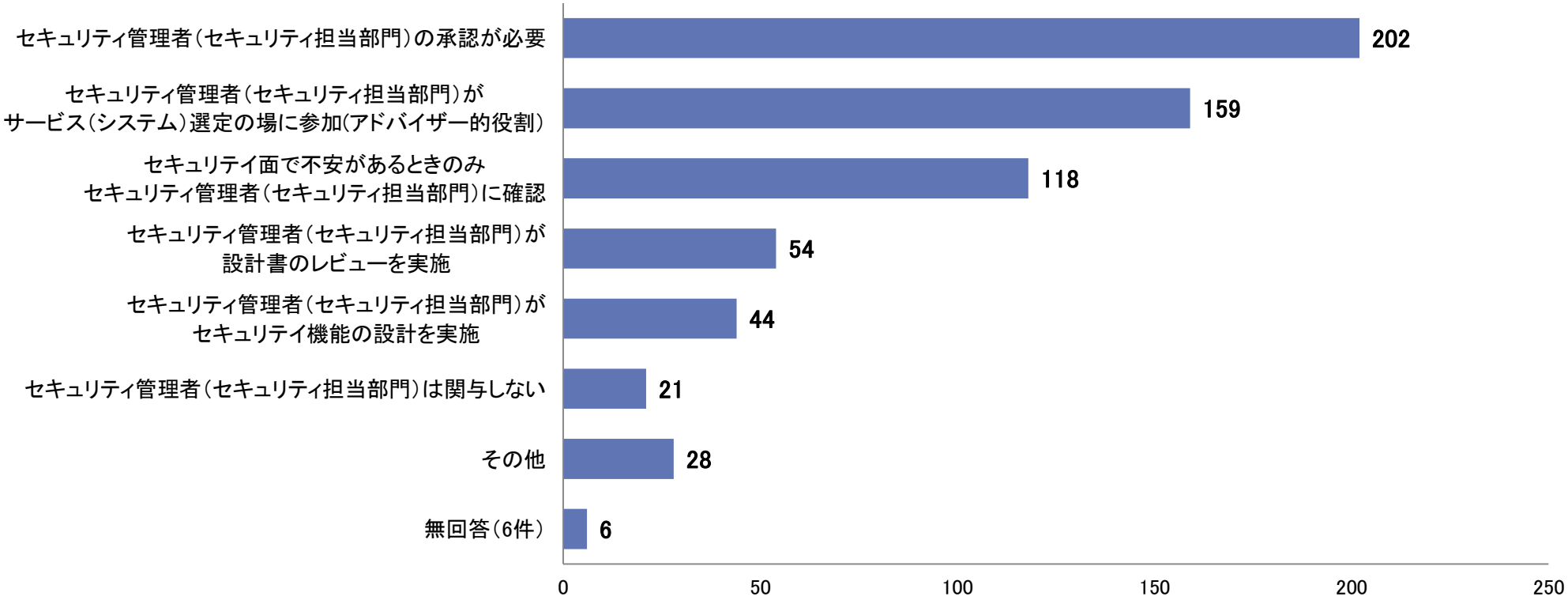


同業他社の事例が有用と回答した組織が多い。

第2章　情報セキュリティマネジメントの取組み状況

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

設問13．社内(組織内)にサービス(システム)を新たに導入する場合のセキュリティ管理者(セキュリティ担当部門)の関与の仕方(N=437)

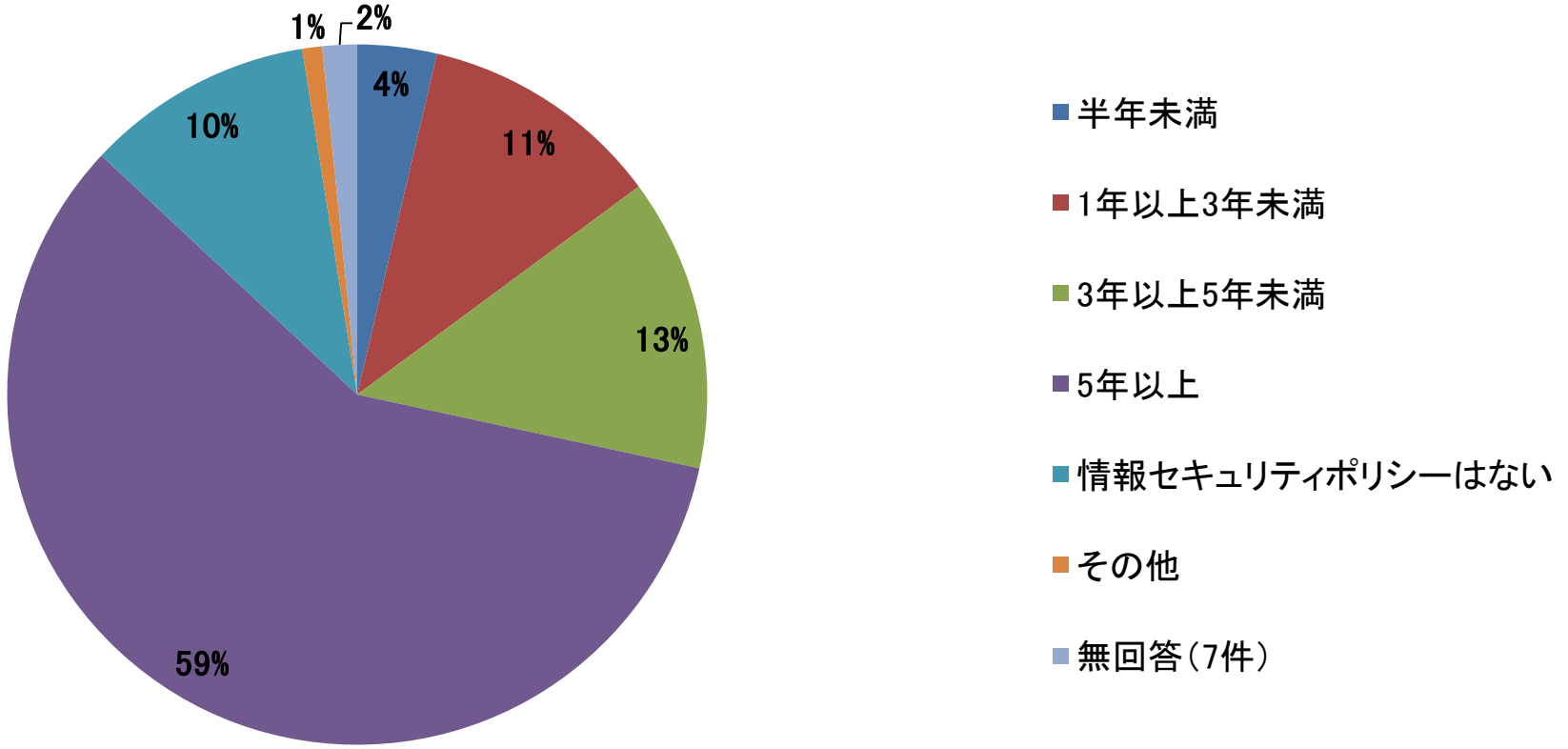


セキュリティ管理者（セキュリティ担当部門）は新サービス（システム）導入の承認や選定において関与する組織が多い。

第2章　情報セキュリティマネジメントの取組み状況

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

設問14－1．情報セキュリティポリシーを制定した時期(N=437)



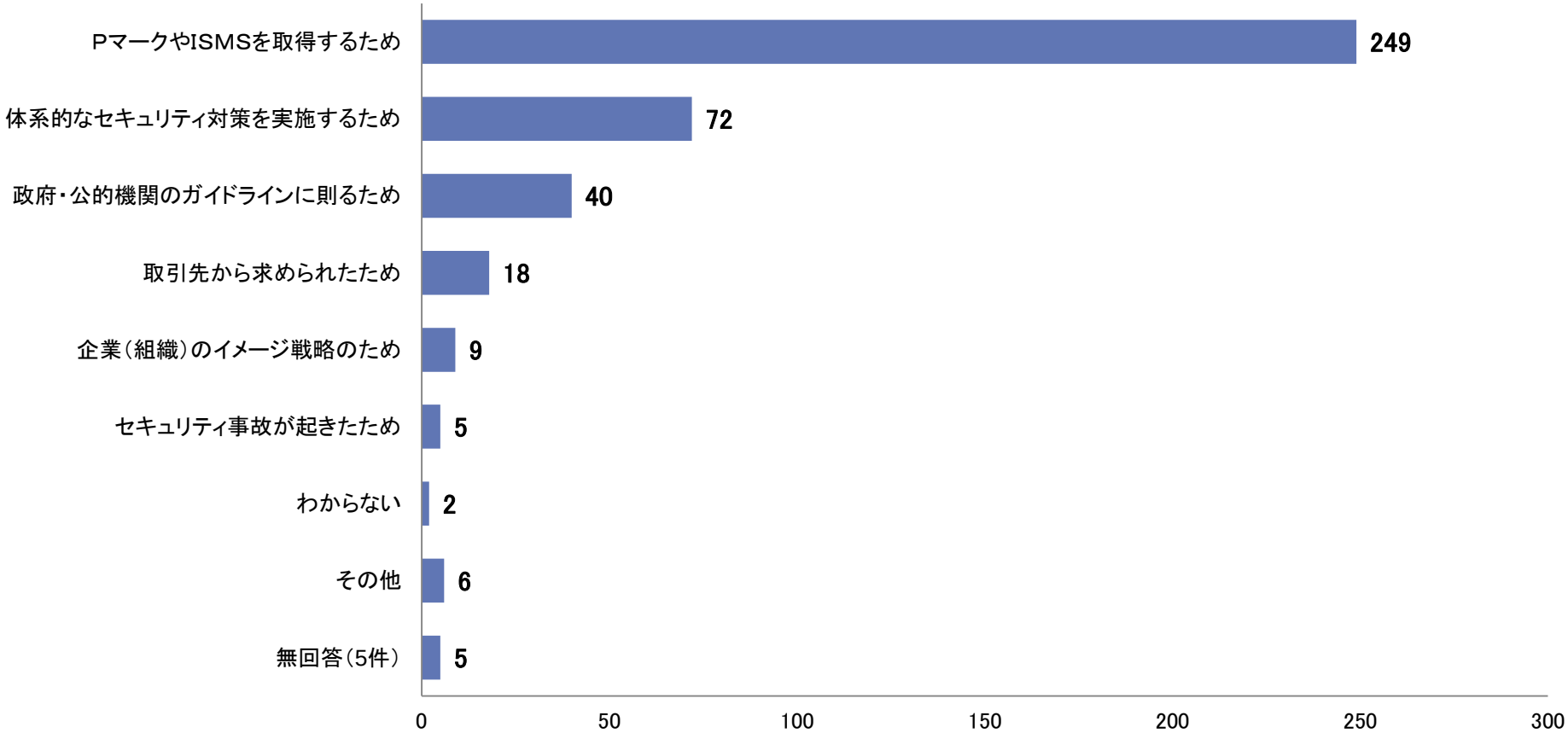
59%の組織が、情報セキュリティポリシー制定から5年以上経過している。

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14－1.で「**5.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14－2. 情報セキュリティポリシー制定のきっかけ(N=391)



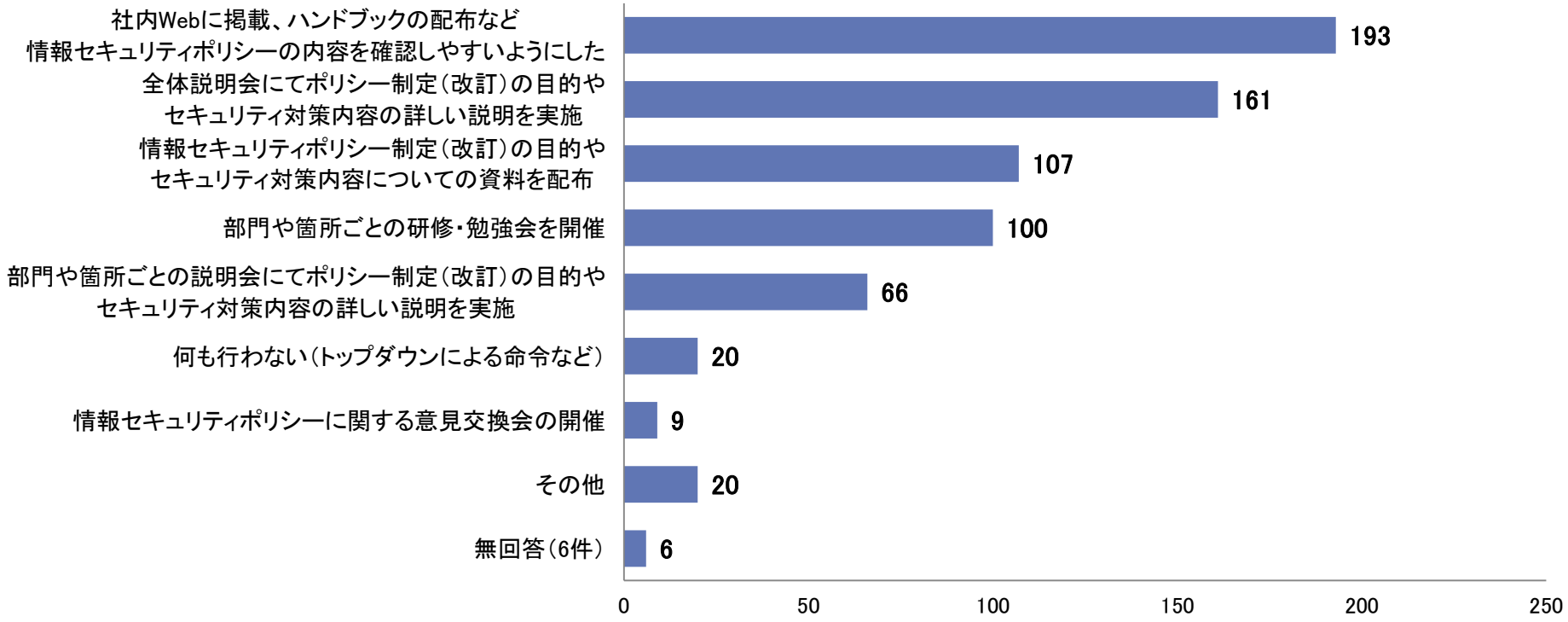
PマークやISMSを取得するためという組織が多い。

第2章　情報セキュリティマネジメントの取組み状況

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

※設問14－1.で「**5.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14－3. 情報セキュリティポリシーが従業員に定着しやすいように工夫していること(N=391)



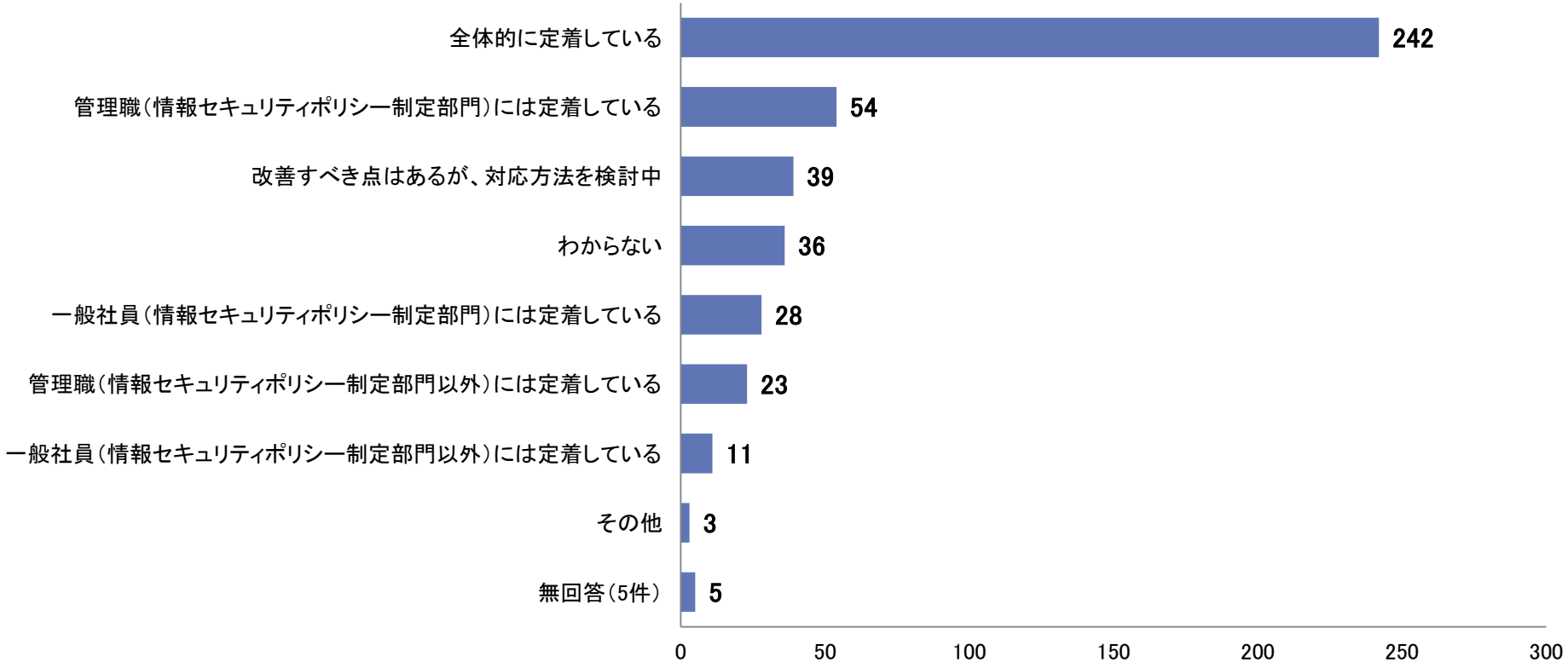
社内Webに掲載、ハンドブックの配布など情報セキュリティポリシーの内容を確認しやすいようにしている組織が多い。

第2章　情報セキュリティマネジメントの取組み状況

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

※設問14－1.で「**5.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14－4. 情報セキュリティポリシーは従業員に定着していると思うか(N=391)



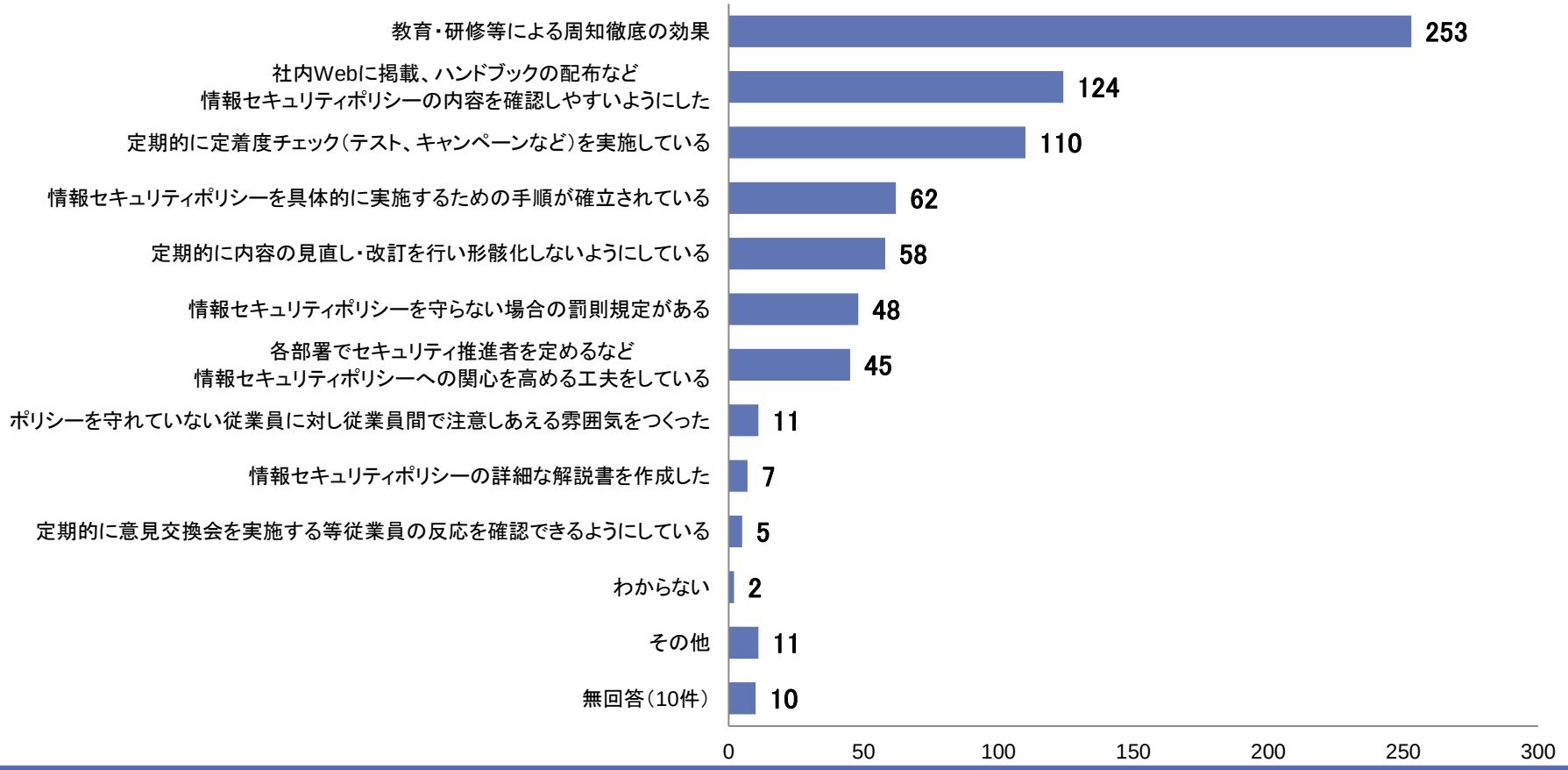
情報セキュリティポリシーは全体的に定着している
と考えている組織が多い。

第2章　情報セキュリティマネジメントの取組み状況

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

※設問14－1.で「**5.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14－5. 情報セキュリティポリシーが定着している理由(N=316)



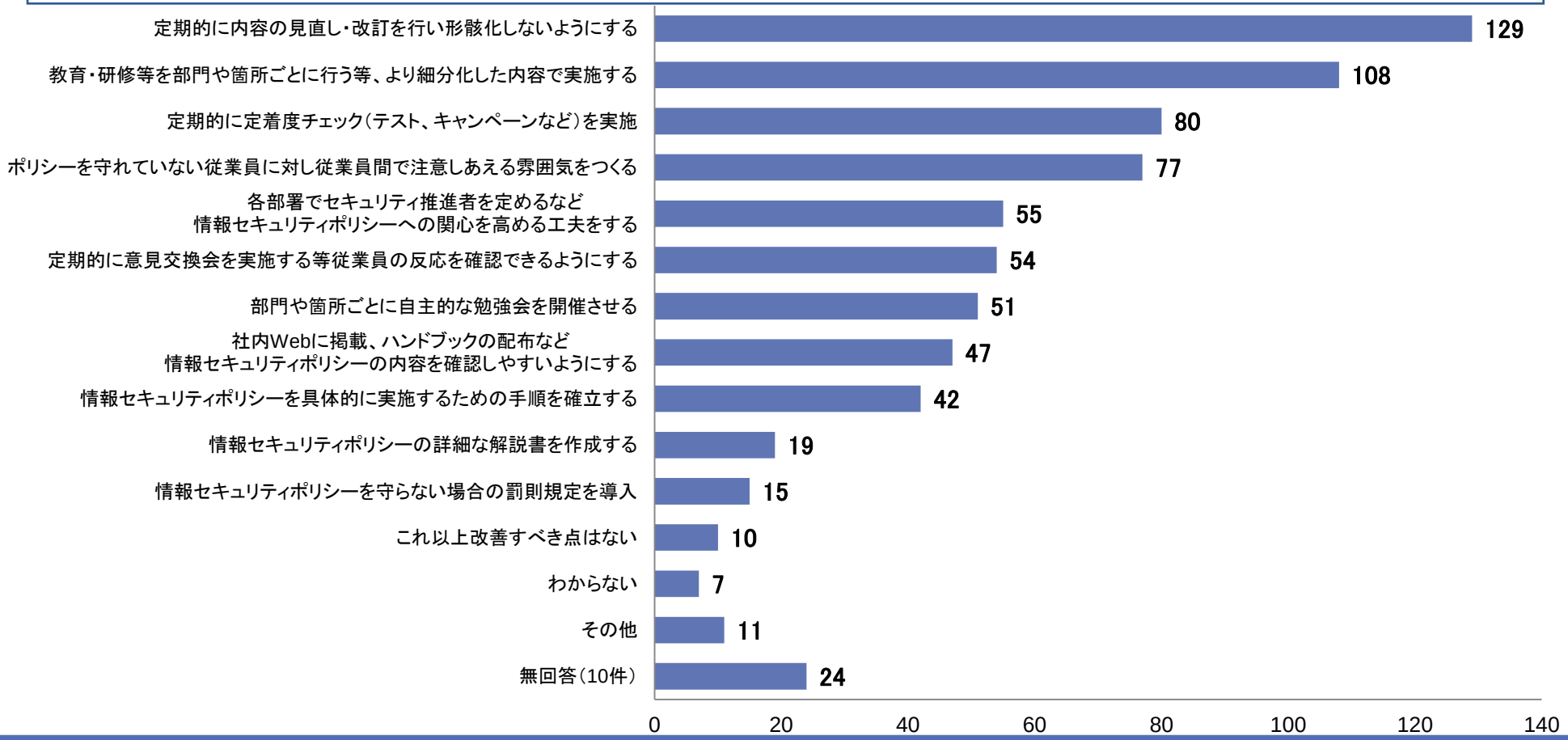
教育・研修等による周知徹底の効果が出ていると考えている組織が多い。

第2章　情報セキュリティマネジメントの取組み状況

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

※設問14－1.で「**5.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14－6. 情報セキュリティポリシーをさらに定着させるために改善すべき点(N=316)



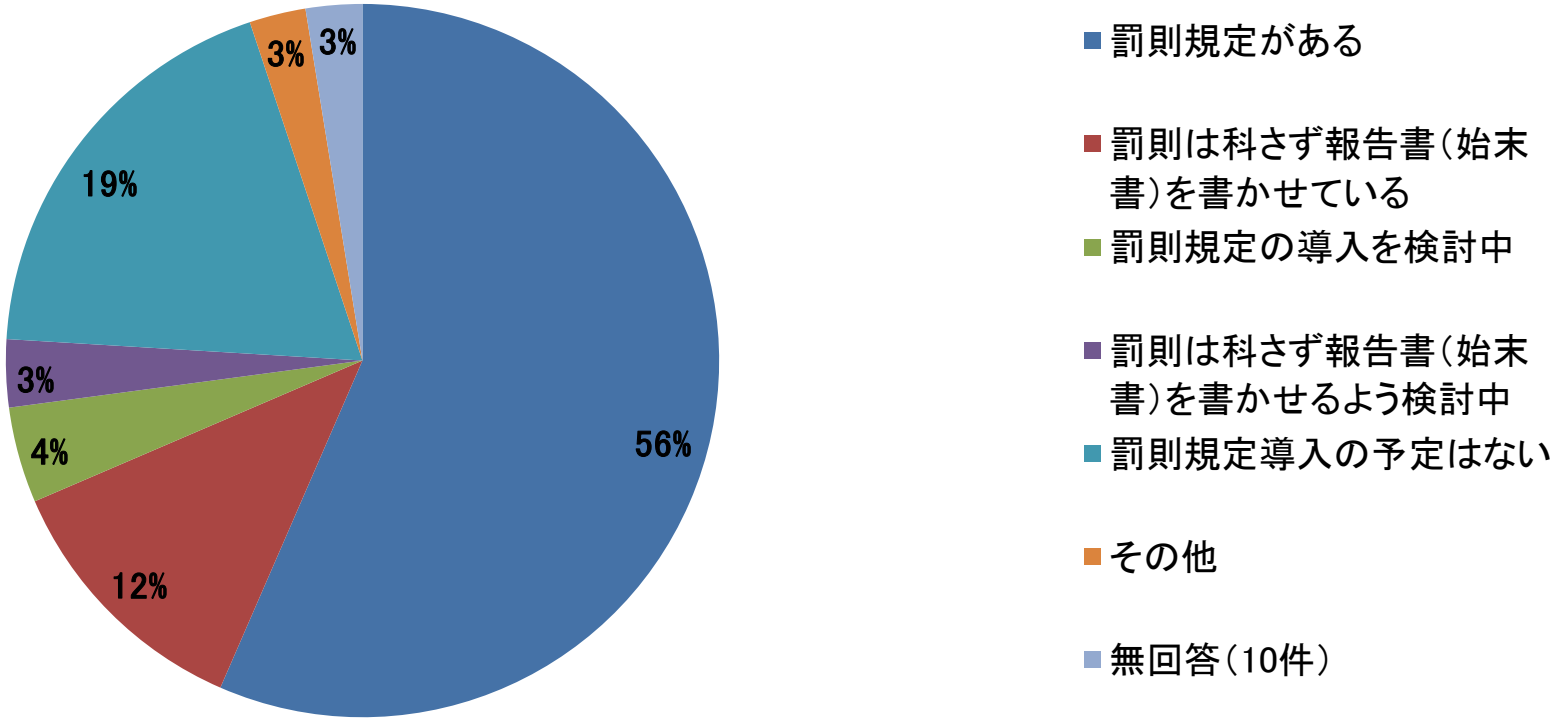
定期的な内容の見直しや教育・研修の細分化をあげる組織が多い。

第2章　情報セキュリティマネジメントの取組み状況

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

※設問14-1.で「**5.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15. 情報セキュリティポリシー違反に対する罰則規定の有無(N=391)



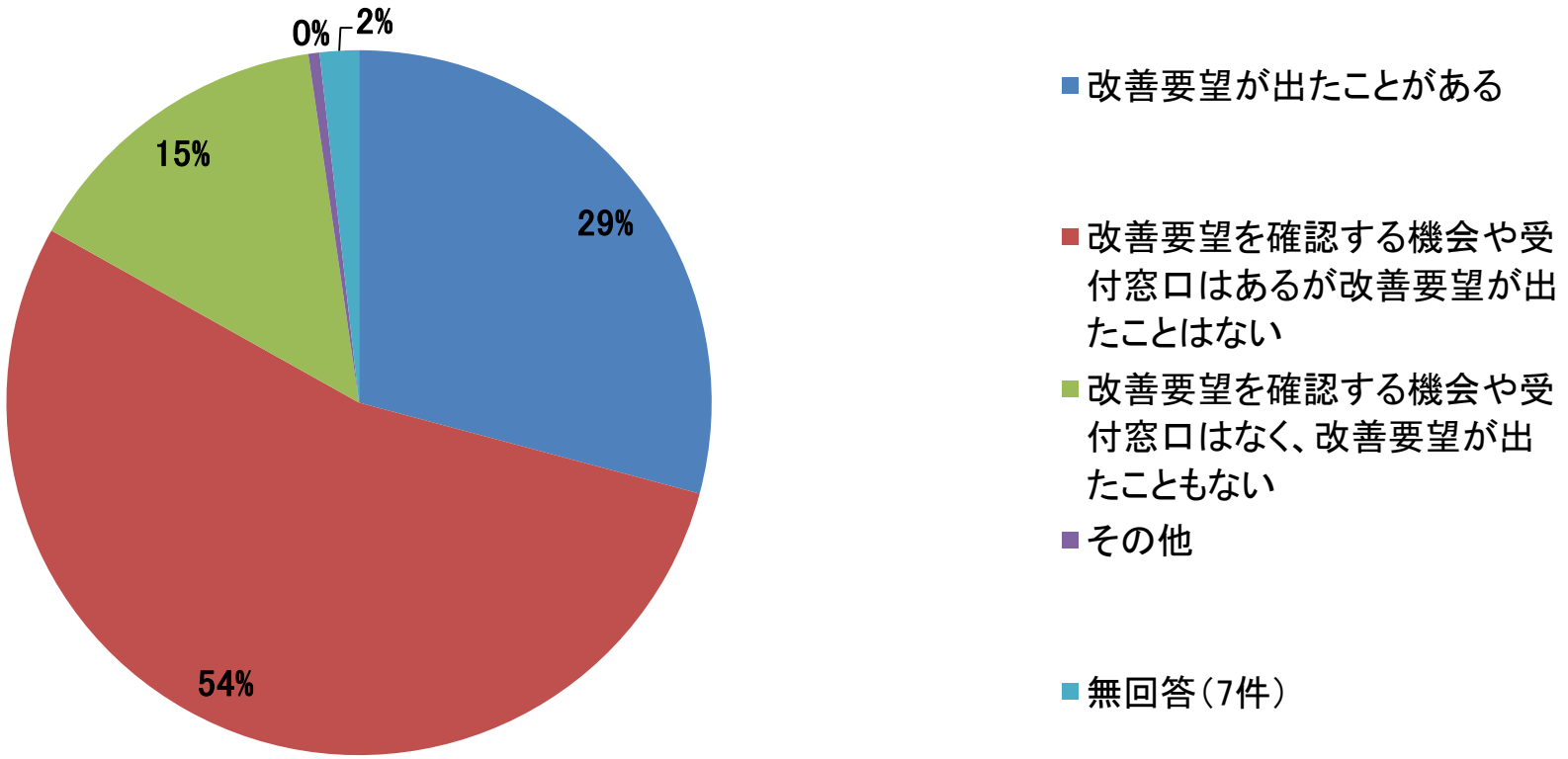
56%の組織に、情報セキュリティポリシーを守らなかった場合の罰則規定がある。

第2章　情報セキュリティマネジメントの取組み状況

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

※設問14-1.で「**5.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16－1．社内(組織内)からの改善要望の有無(N=391)



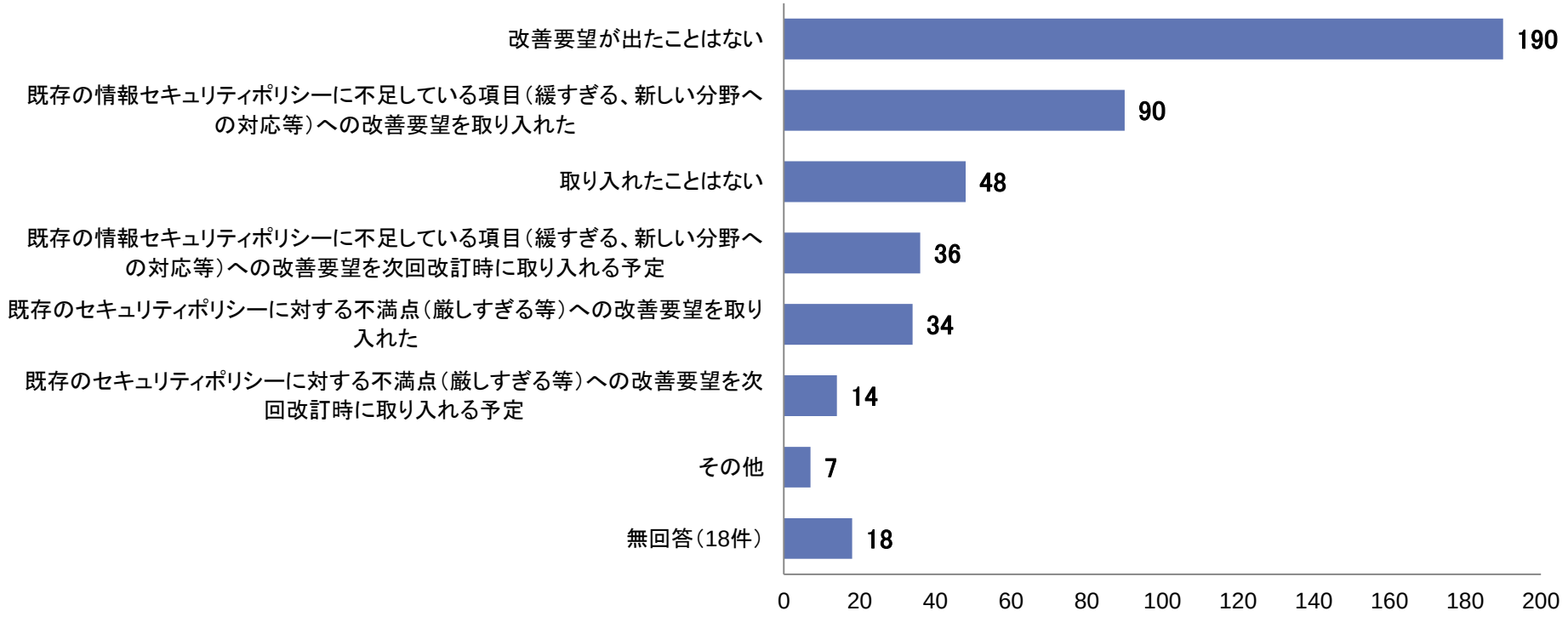
69%の組織では改善要望が出たことがない。

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14-1.で「**5.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16－2. 改善要望を情報セキュリティポリシーに取り入れたことはあるか（N=391）



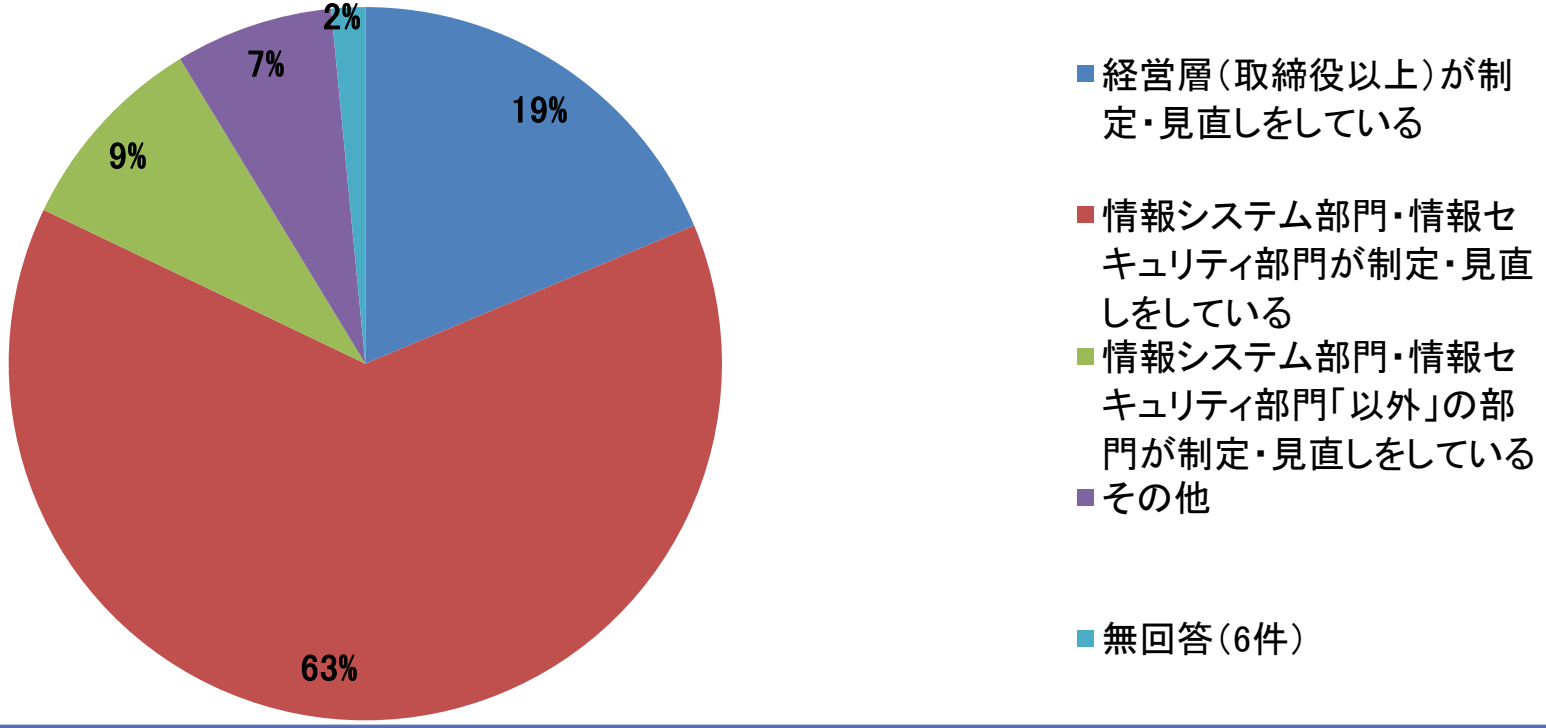
改善要望を取り入れる場合は、既存の情報セキュリティポリシーに不足している項目（緩すぎる、新しい分野への対応等）への対応が多い。

第2章　情報セキュリティマネジメントの取組み状況

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

※設問14-1.で「5.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17. 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(N=391)



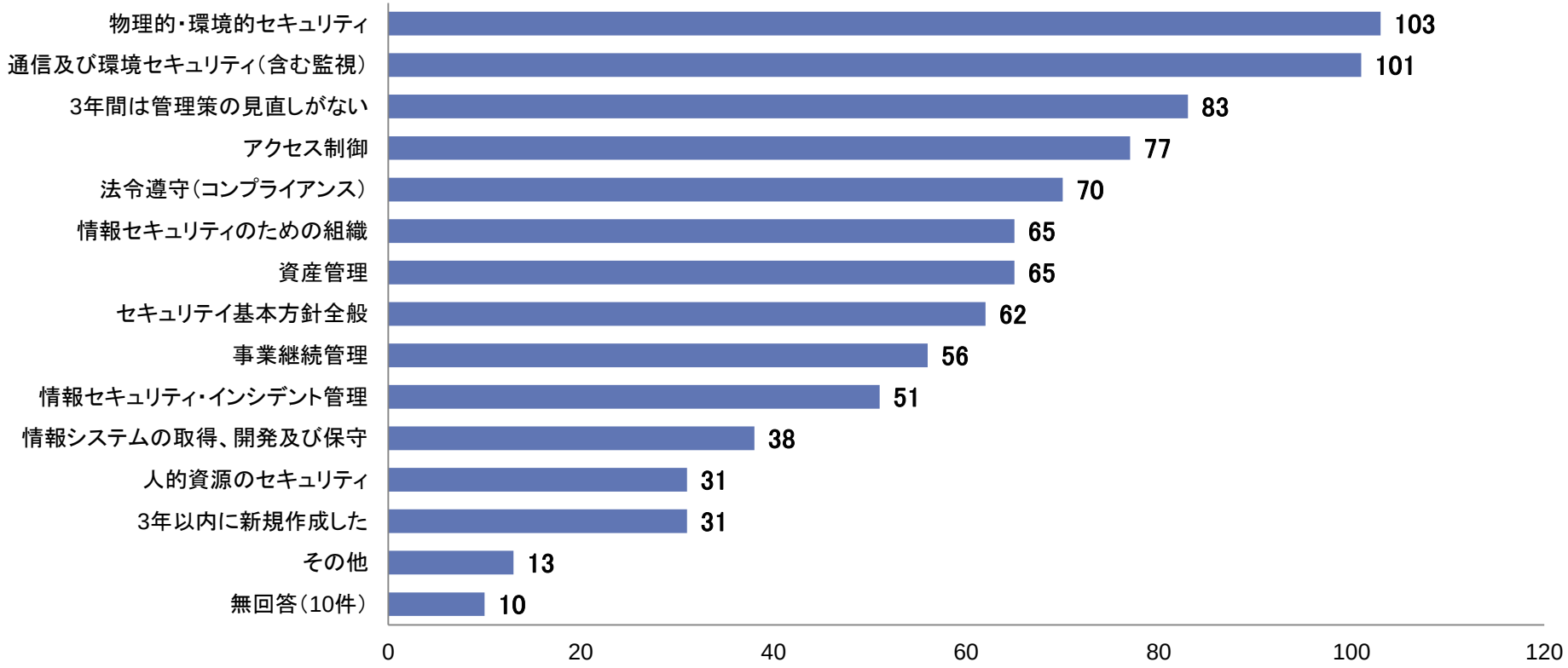
63%の組織において情報システム部門・情報セキュリティ部門が制定・見直しをしている。

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14-1.で「**5.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18. 過去3年（2012年1月以降）で見直した管理策(N=391)



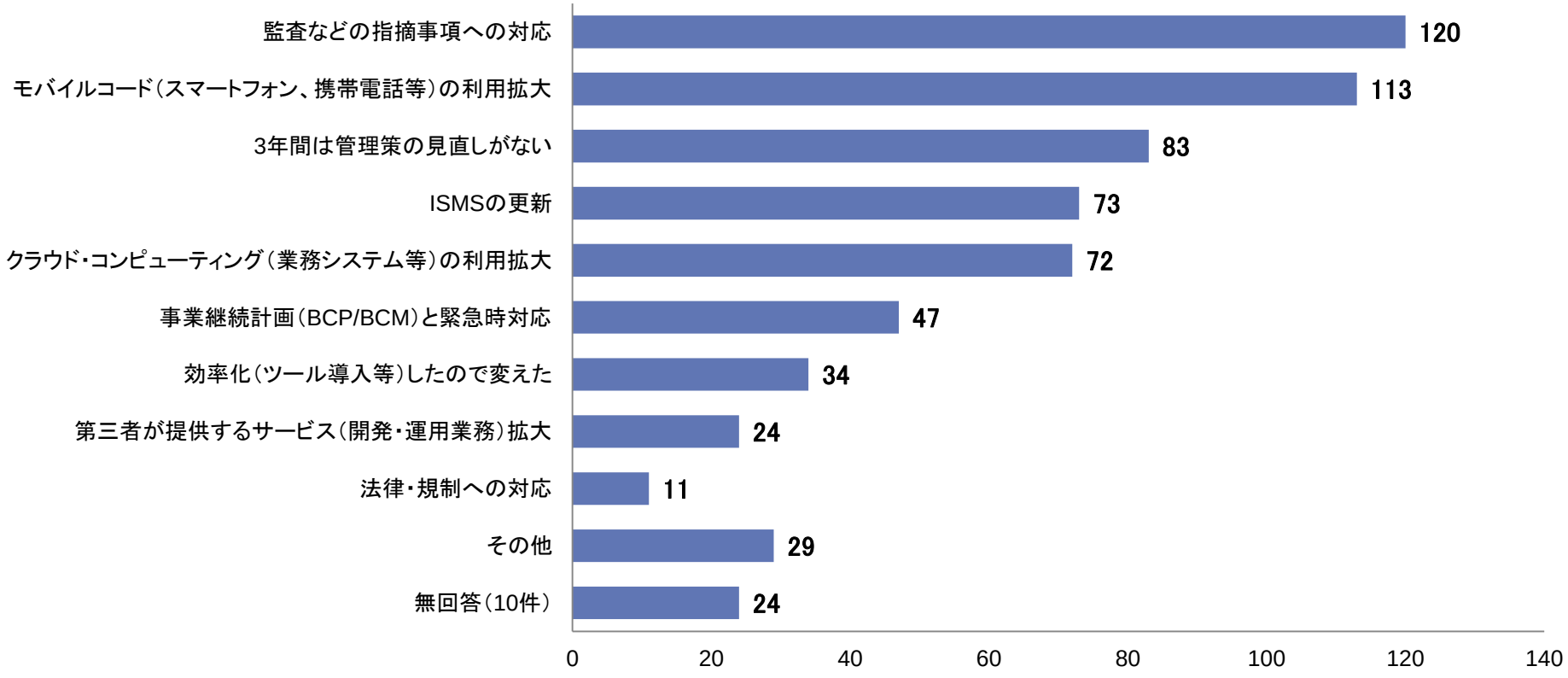
物理的・環境的セキュリティ及び通信に関するセキュリティポリシーの見直しを行っている組織が多い。

第2章　情報セキュリティマネジメントの取組み状況

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

※設問14-1.で「**5.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19．過去3年で情報セキュリティポリシー（全体）を見直した理由(N=391)



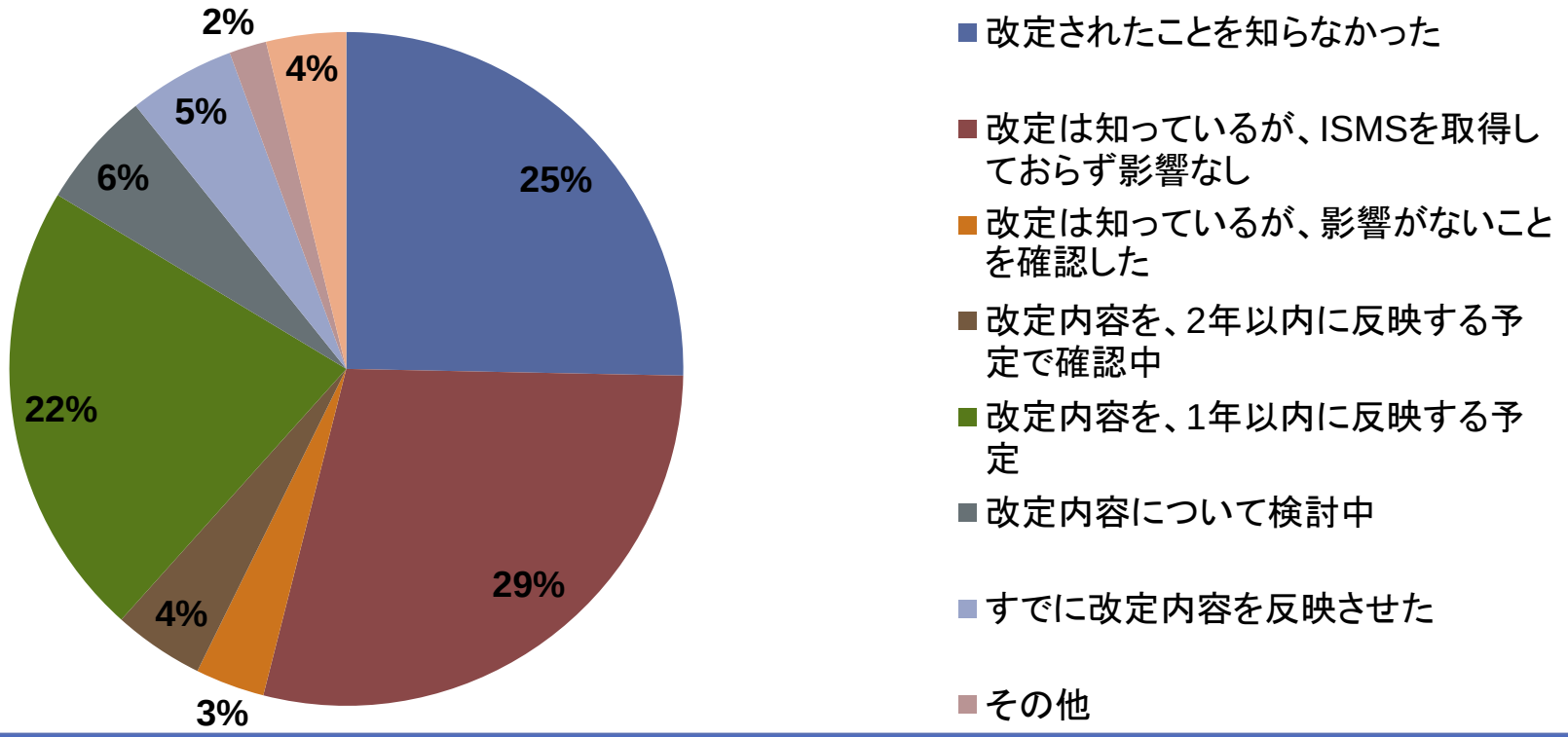
監査の指摘事項やモバイルコード利用拡大への対応のために情報セキュリティポリシーを見直している。

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14-1.で「**5.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20. ISO/IEC27001および27002の改定の影響(N=391)



25%の組織では改定されたことを知らなかった。
22%の組織では改定内容を1年以内に反映する予定。

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）

- 情報セキュリティのリスク分析を66%の組織が、1年未満の期間に実施している。リスク分析の実施理由は、ISMSやPマークへの対応が最も多く、情報資産の棚卸、内部規程の改訂が続く。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」と感じる組織が81%で一番多い。
- 過去3年間で情報セキュリティポリシー（全体）を見直した理由として多いのは、監査の指摘事項やモバイルコード利用拡大への対応である。3年間は管理策の見直しがない組織も多い。2013年秋に行われたISMSの基本基準であるISO/IEC27001および27002の改定については情報セキュリティポリシーがあると回答した391組織の内25%の組織では改定されたことを知らなかった。22%の組織において改定内容を1年以内に反映する予定。6%の組織では改定内容を検討中、5%の組織ではすでに改定内容を反映させている。

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）

- 情報セキュリティポリシーは全体的に定着していると考えている組織が多い。定着した理由として一番多いのは、教育・研修等による周知徹底の効果である。情報セキュリティポリシー制定時や改訂時に従業員に定着しやすいように工夫している点としては「社内Webに掲載、ハンドブックの配布など情報セキュリティポリシーの内容を確認しやすいようにしている」という回答が一番多い。両設問において異なる結果となっているのは、教育・研修の中で社内Webへの掲載やハンドブックについても従業員に再認識させられる点も関係していると考えられる。
- 56%の組織に情報セキュリティポリシーを守らなかった場合の罰則規定がある。12%の組織では罰則規定はないが、報告書（始末書）を書かせている。罰則導入の予定がないのは19%のみである。一方、情報セキュリティポリシーが従業員に定着した理由として「罰則規定がある」と回答したのは48件（延べ回答数750件のうち約6%）と少数であった。

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）

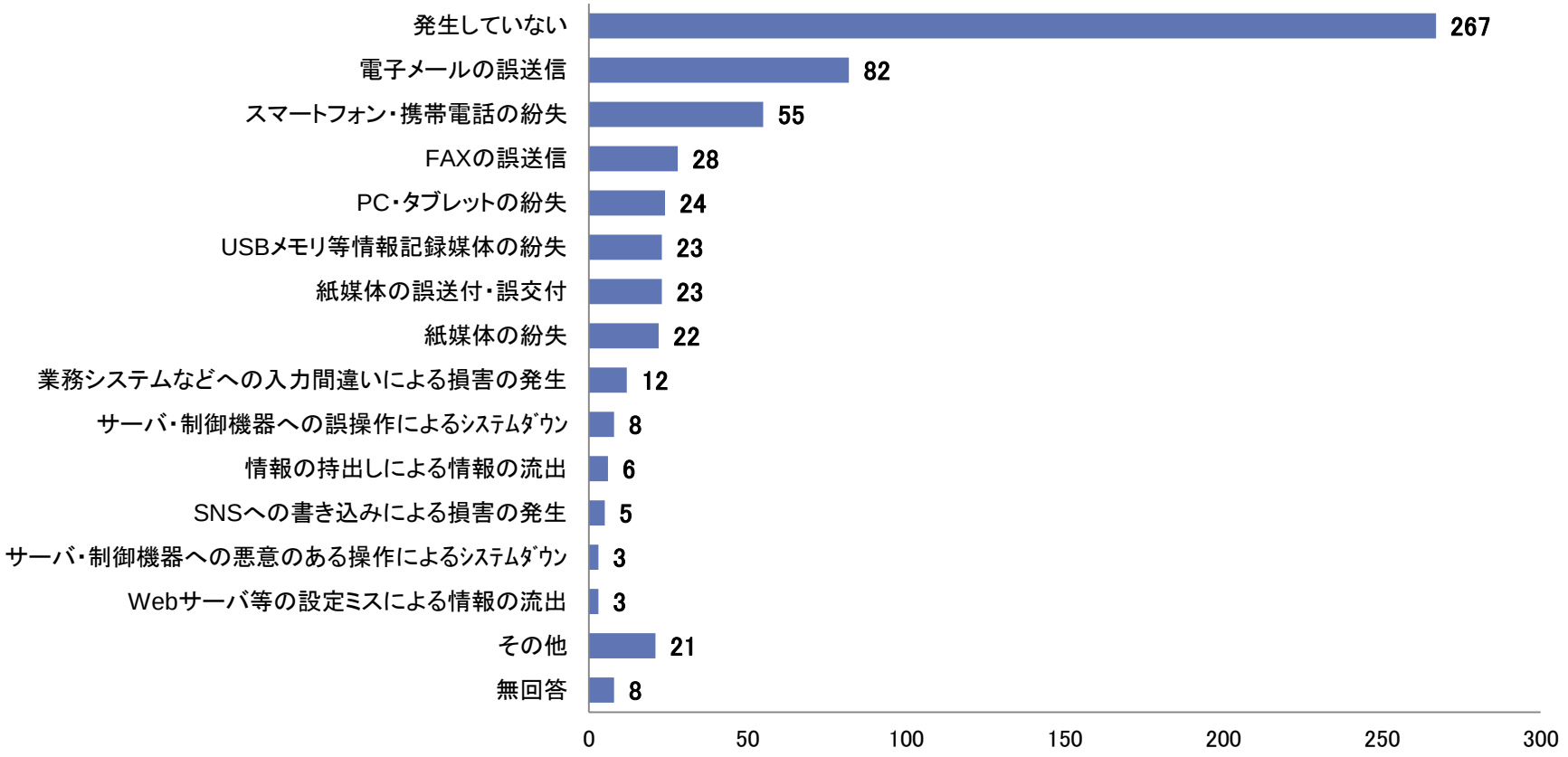
- 情報セキュリティポリシーに対する改善要望が出たことがあるのは29%のみ。改善要望を取り入れた、もしくは取り入れる予定の内容については、既存の情報セキュリティポリシーの緩和への対応よりも、不足している項目（緩すぎる、新しい分野への対応等）への対応という回答の方が多い。

第３章
人的要因に関する
情報セキュリティへの取組み

第3章　人的要因に関する情報セキュリティへの取組み

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

設問21．人的要因による事故・トラブル発生状況(N=437)

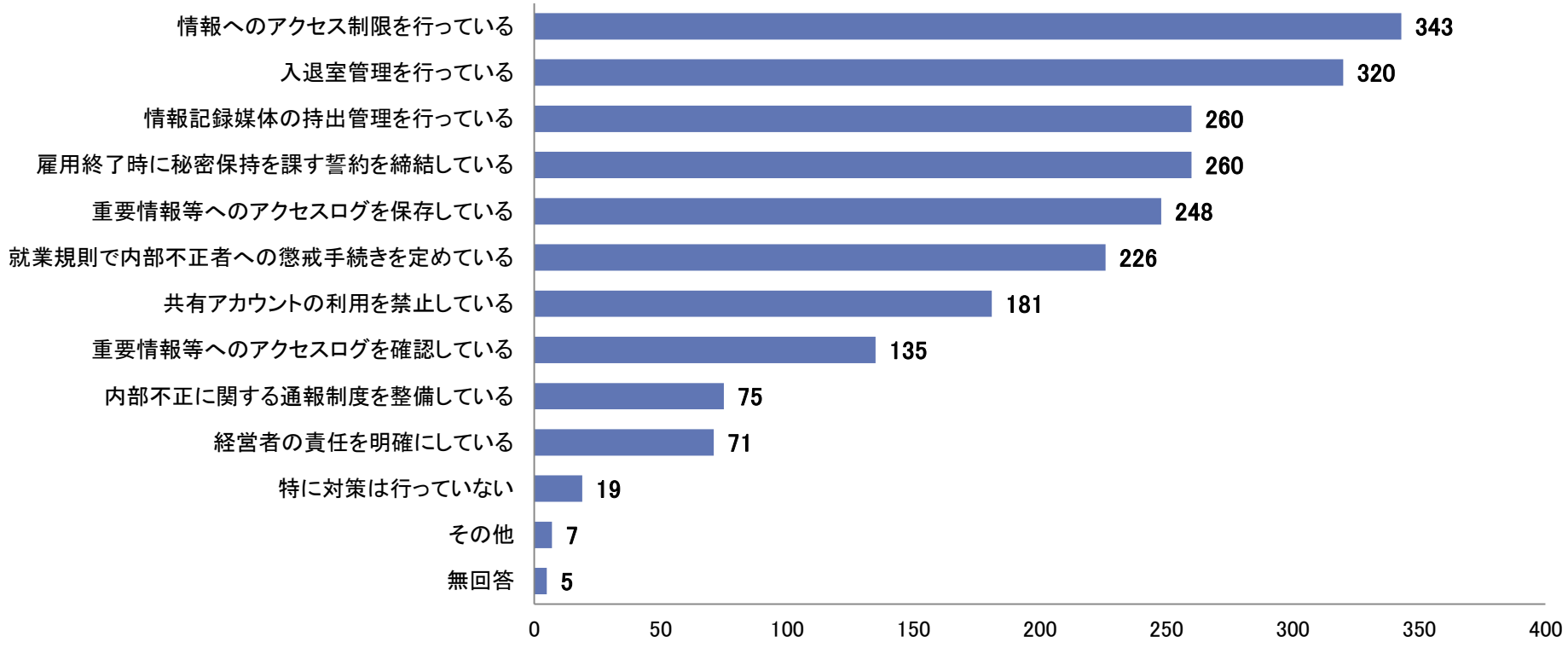


約61%の組織で、人的要因による事故・トラブルは発生していない。
約1%の組織において、情報の持出しによる情報の流出が発生している。

第3章　人的要因に関する情報セキュリティへの取組み

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

設問22. 不正行為防止のための対策状況(N=437)

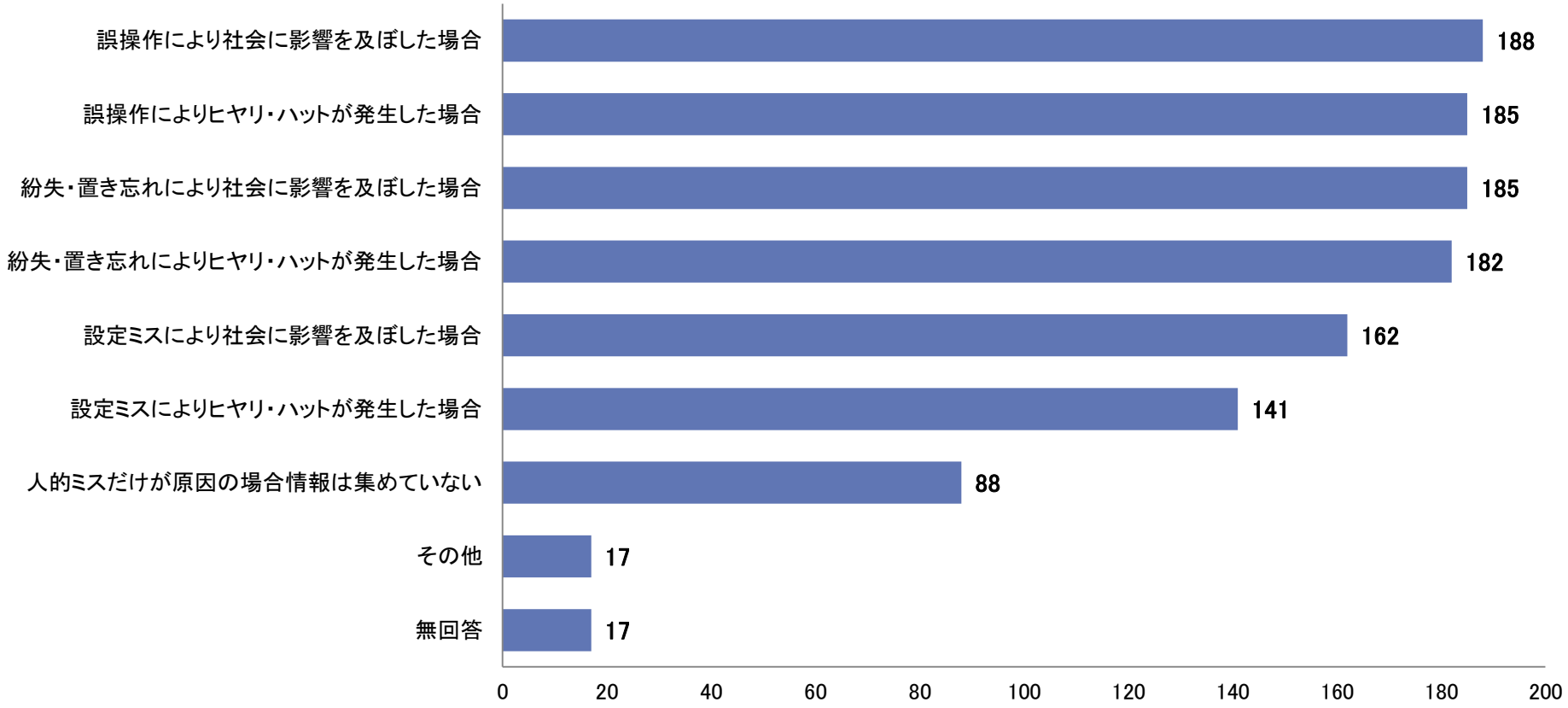


情報へのアクセス制限、入退室管理は70%以上の組織が行っている。
アクセスログは約57%の組織が保存しているが、
確認している組織は約31%である。

第3章　人的要因に関する情報セキュリティへの取組み

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

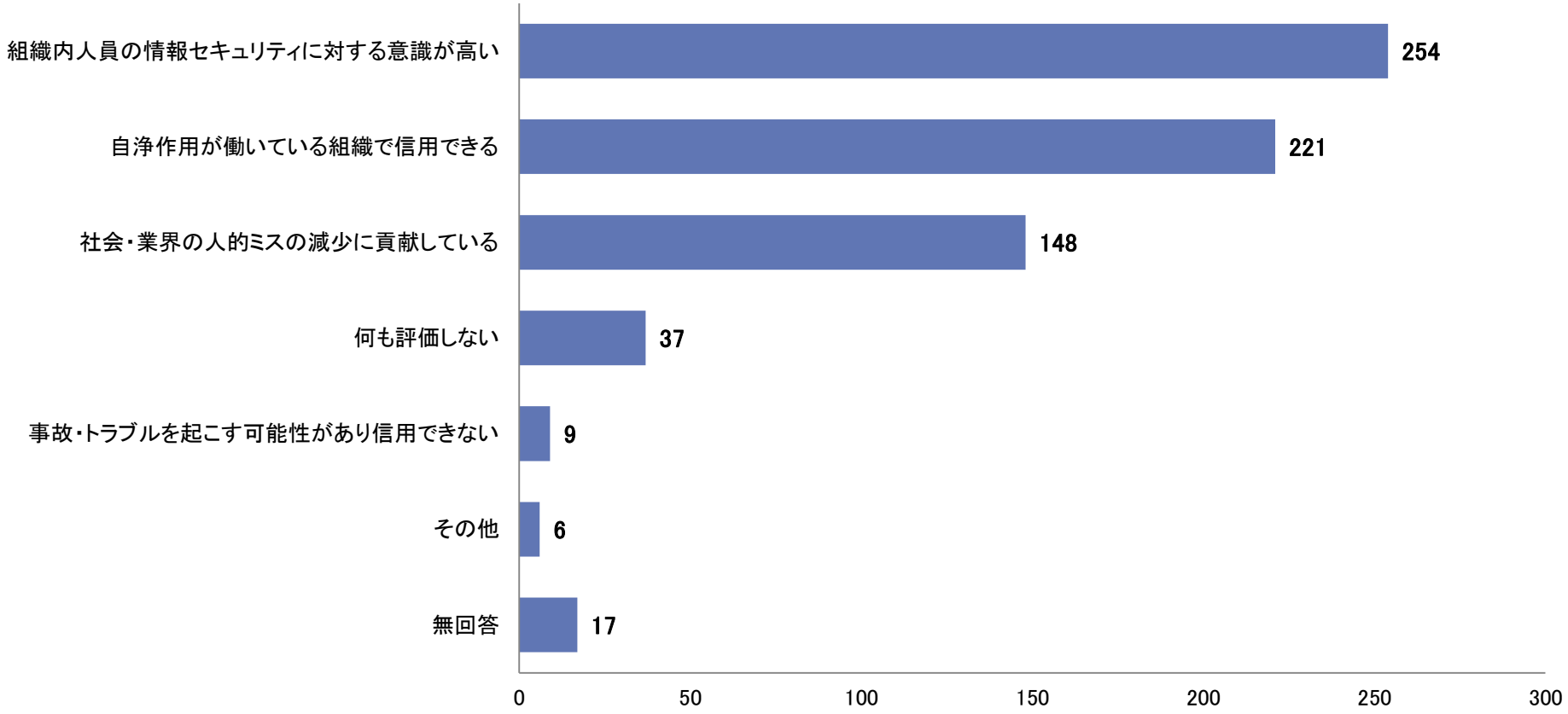
設問23．組織内における人的ミスによる事故・トラブルの収集状況(N=437)



誤操作、紛失・置き忘れについての事故・トラブルの情報を集める組織は40%強存在する。

第3章　人的要因に関する情報セキュリティへの取組み

設問24. ヒヤリ・ハット事例情報を公表している組織に対する評価(N=437)

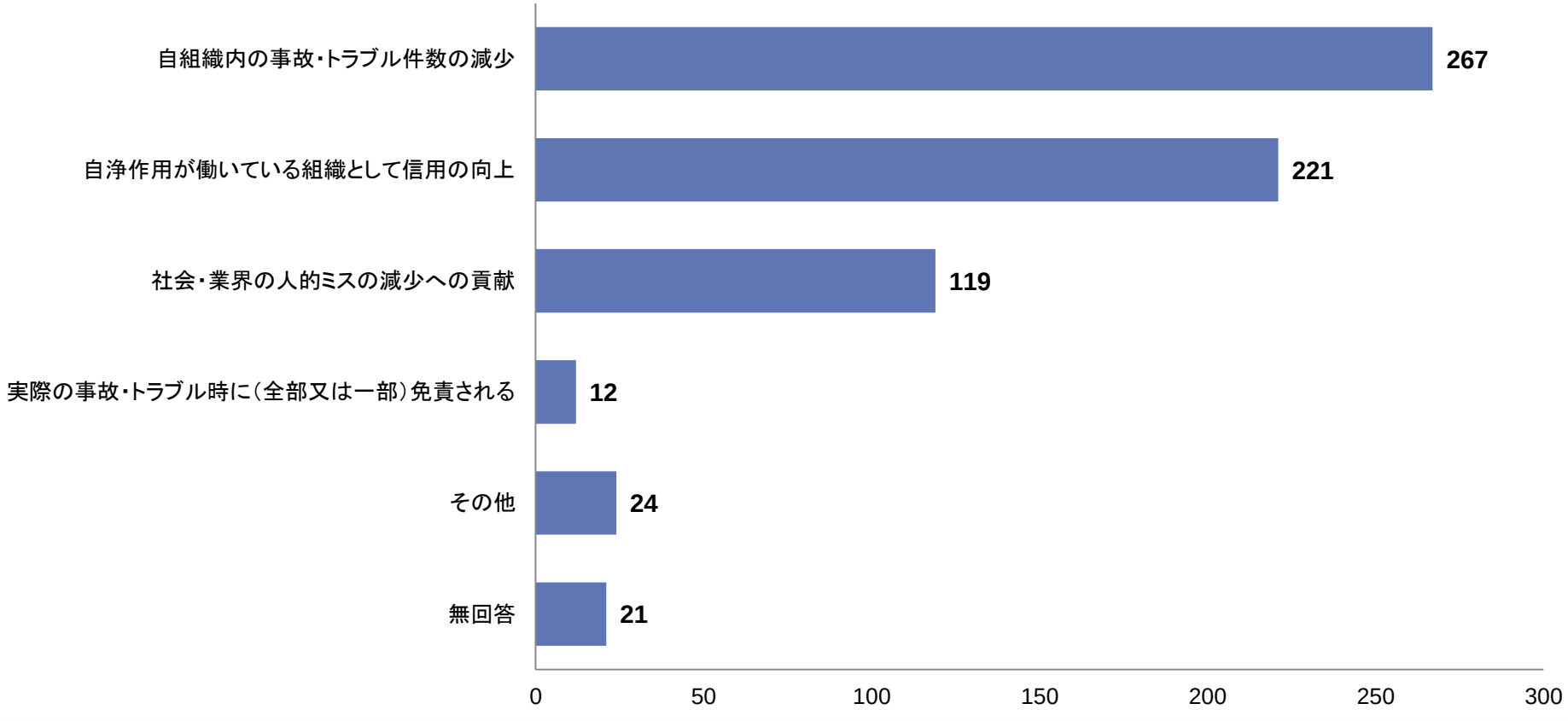


組織内人員の情報セキュリティに対する意識が高いと評価している組織は、約58%である。信用できないとした組織は約2%である。

第3章　人的要因に関する情報セキュリティへの取組み

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

設問25. ヒヤリ・ハット事例情報を公表している組織の外部への期待(N=437)

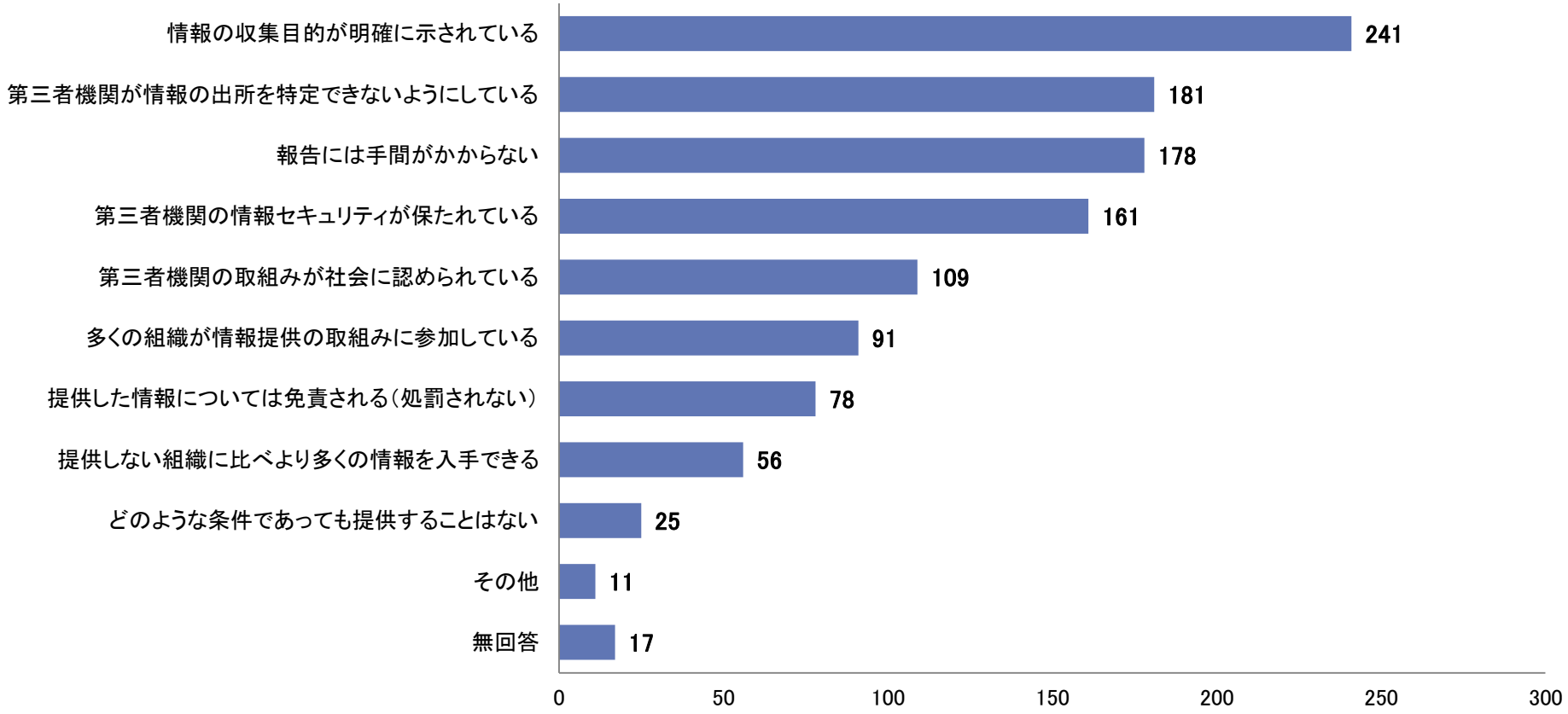


自組織内の事故・トラブル件数の減少を期待する組織は約61%存在。
事故・トラブル時に免責されることを期待した組織は約3%存在。

第3章　人的要因に関する情報セキュリティへの取組み

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

設問26. 第三者機関へのヒヤリ・ハット事例情報提供の条件(N=437)



提供要素として一番多いのは情報の収集目的が明確に示されているであった。
どのような条件であっても提供しないとした組織は約6%。

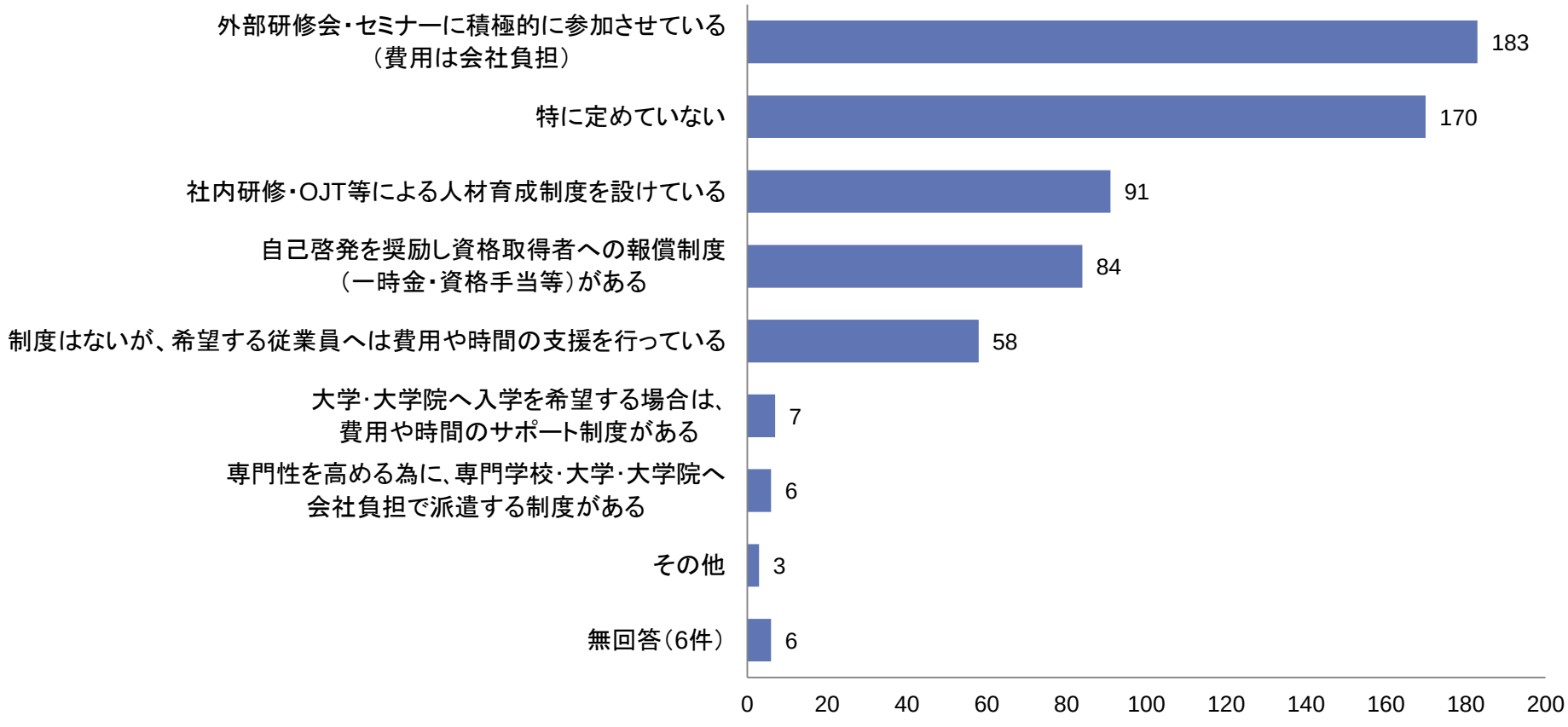
考察（第3章　人的要因に関する情報セキュリティへの取組み）

- 内部不正を防ぐ対策の一つとしてアクセスログの保存・確認が挙げられるが、保存している組織は約57%、確認をしている組織は約31%という結果であった。
- 情報セキュリティの事故・トラブルの情報のうち、誤操作、紛失・置き忘れについては40%強の組織が収集している。また、情報セキュリティのヒヤリ・ハット事例情報を第三者機関に提供する場合の要件としては情報の収集目的が明確に示されていることが一番多く求められている。一方、どのような条件であっても提供しないとした組織は約6%しか存在しない。

第４章
情報セキュリティの人材育成と教育に関して

第4章　情報セキュリティの人材育成と教育に関して

設問27. 情報セキュリティの推進者の人材育成に関する制度(N=437)

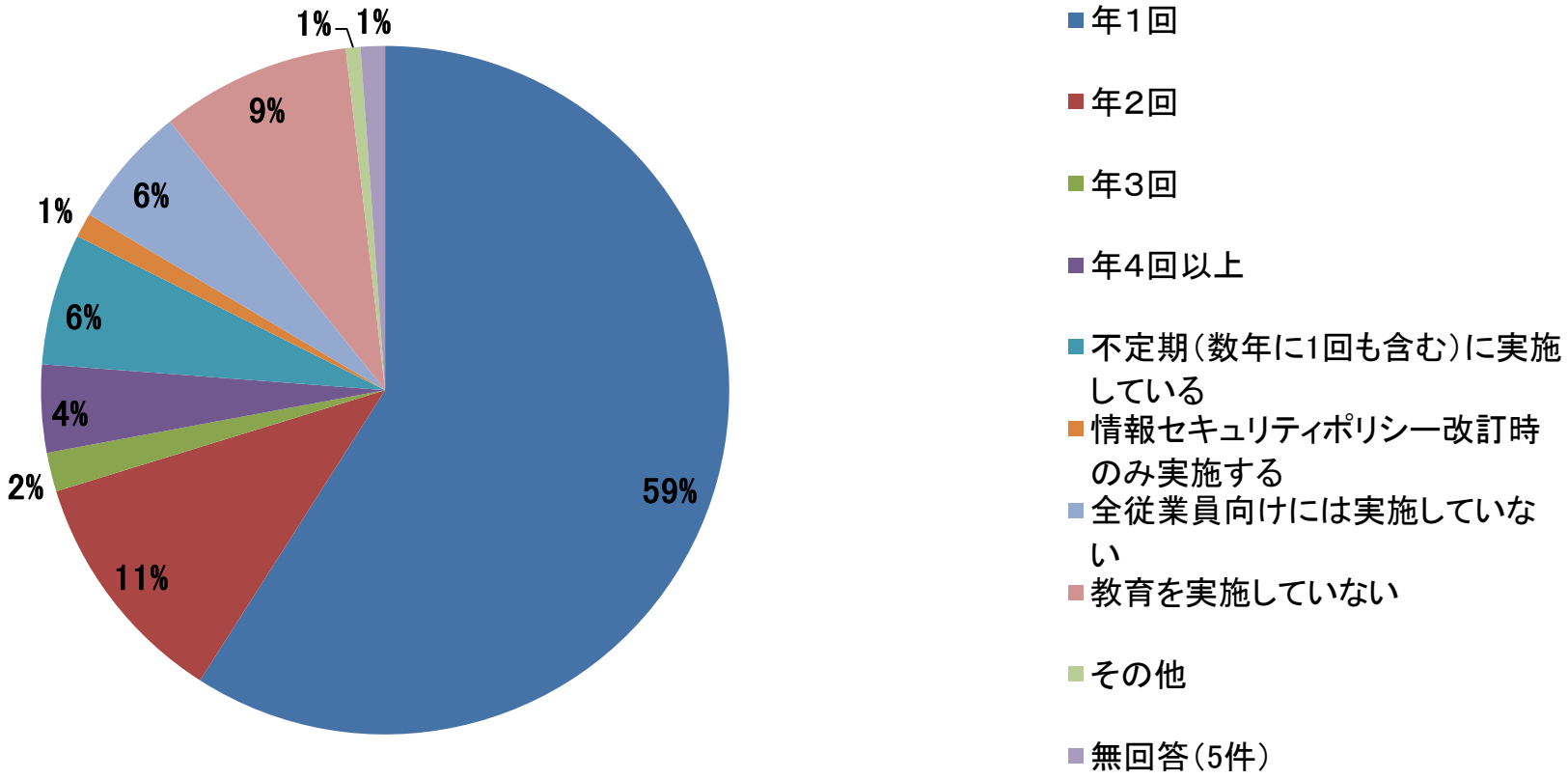


外部研修会・セミナーに積極的に参加させている組織、特に定めていない組織が共に多い。

第4章　情報セキュリティの人材育成と教育に関して

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

設問28－1．全従業員向けの教育実施回数(N=437)



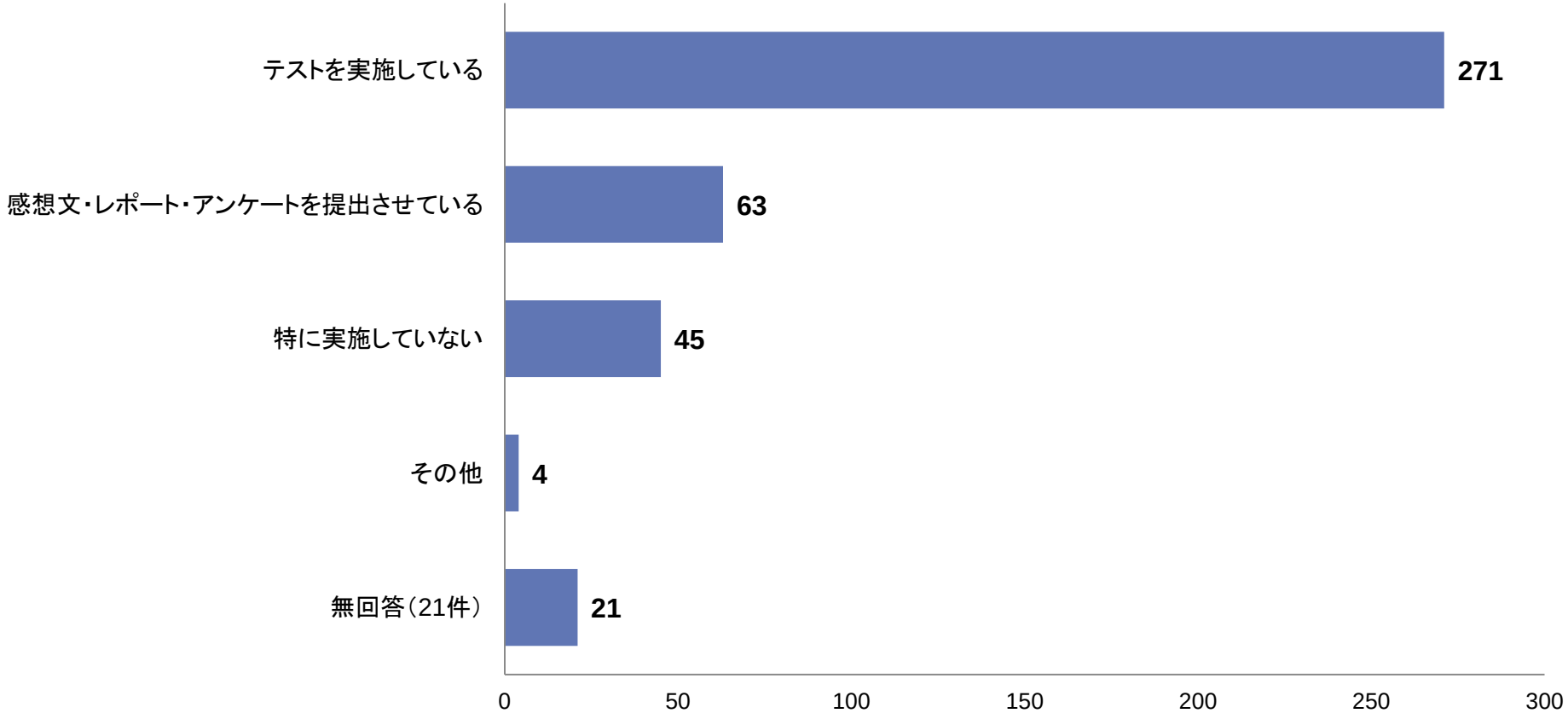
76%の組織が年1回以上全従業員向けの定期的な教育を実施している。

第4章　情報セキュリティの人材育成と教育に関して

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

※設問28－1.で「**1～6(教育を実施している)**」と選択した組織のみ

設問28－2. 従業員への教育の効果確認方法(N=365)



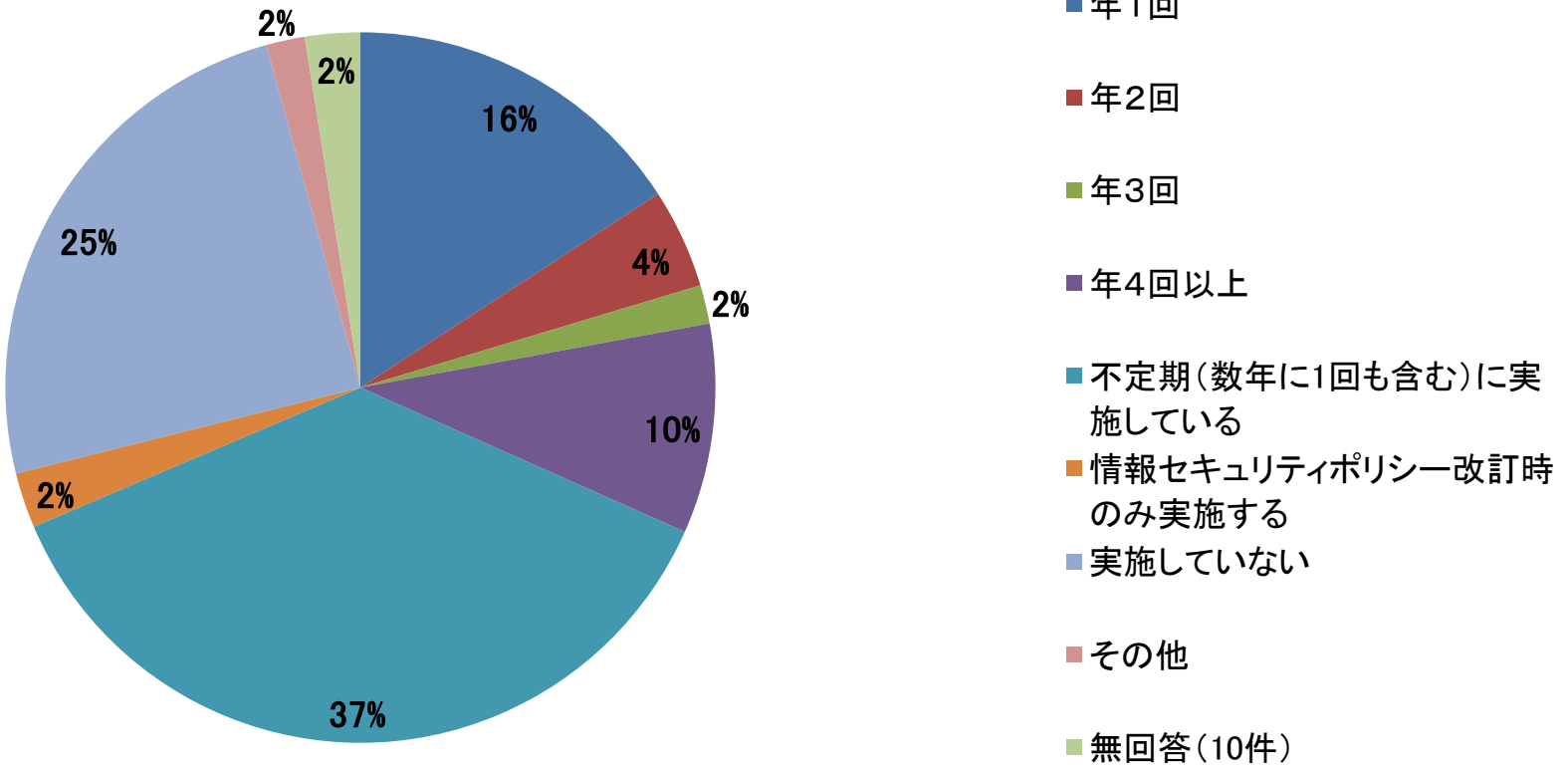
教育の効果の確認にテストを実施する組織が多い。

第4章　情報セキュリティの人材育成と教育に関して

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

※設問28-1.で「8. **教育を実施していない**」と回答した組織を除く

設問28－3. 特定の従業員が対象の教育実施回数(N=398)

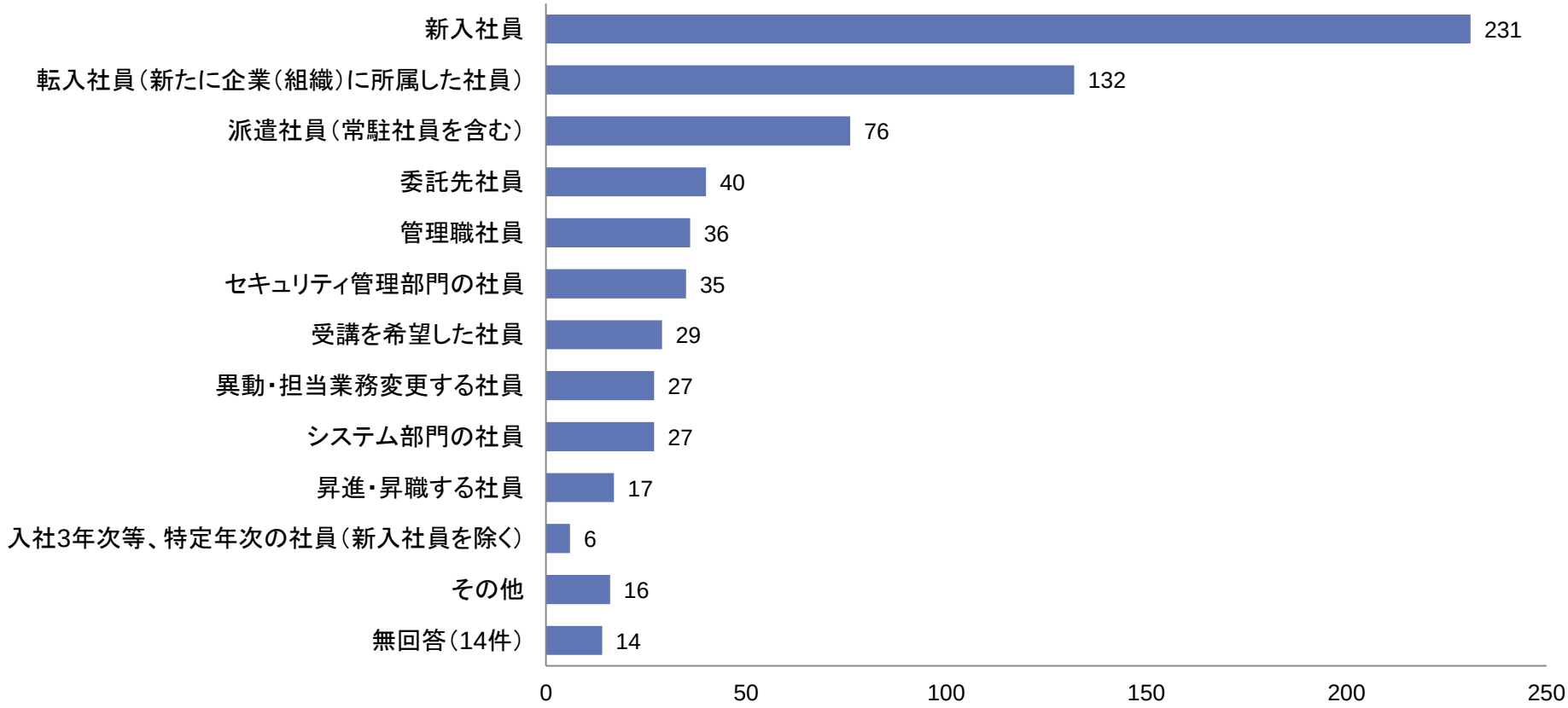


32%の組織が特定の従業員向けの教育を年1回以上実施している。

第4章　情報セキュリティの人材育成と教育に関して

※設問28－3.で「**1～6(教育を実施している)**」と選択した組織のみ

設問28－4. 特定の教育の対象となる従業員(N=283)



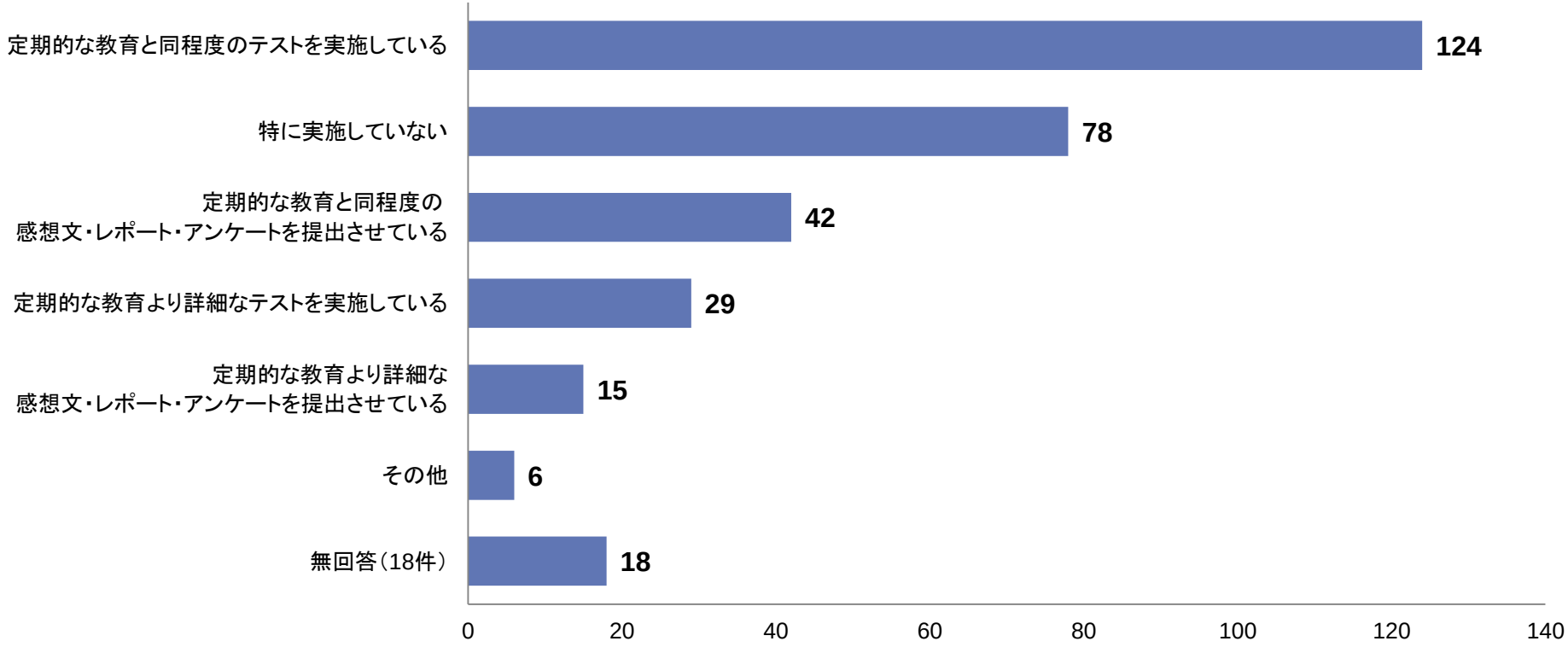
新入社員・転入社員に対して教育を行っている組織が多い。

第4章　情報セキュリティの人材育成と教育に関して

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

※設問28－3.で「**1～6(教育を実施している)**」と選択した組織のみ

設問28－5. 特定の従業員向け教育の効果確認方法(N=283)



教育の効果の確認に全従業員向けの定期的な教育と同程度のテストを実施する組織が多い。

考察（第4章　情報セキュリティの人材育成と教育に関して）

- 情報セキュリティの推進者の人材育成に関して、外部研修会・セミナーに積極的に参加させている組織が40%超で一番多いが、特に定めていない組織も40%近くと多く存在する。
- 76%の組織が年1回以上全従業員向けの情報セキュリティの教育を行っており、教育の効果の確認にはテストを実施する組織が多い。
- 71%の組織が特定の従業員向けの教育を実施しており、新入社員・転入社員を対象としている組織が多い。教育の効果の確認にはテストを実施する組織が多いが全従業員向けと比較すると教育効果の確認を特に実施しない組織が多い。
- 全従業員向けの定期的な教育以外の特定の従業員を対象にした教育の対象となるのは、新入社員・転入社員であると回答した組織が多く、次いで、派遣社員・委託先社員であった。

考察（第４章　情報セキュリティの人材育成と教育に関して）

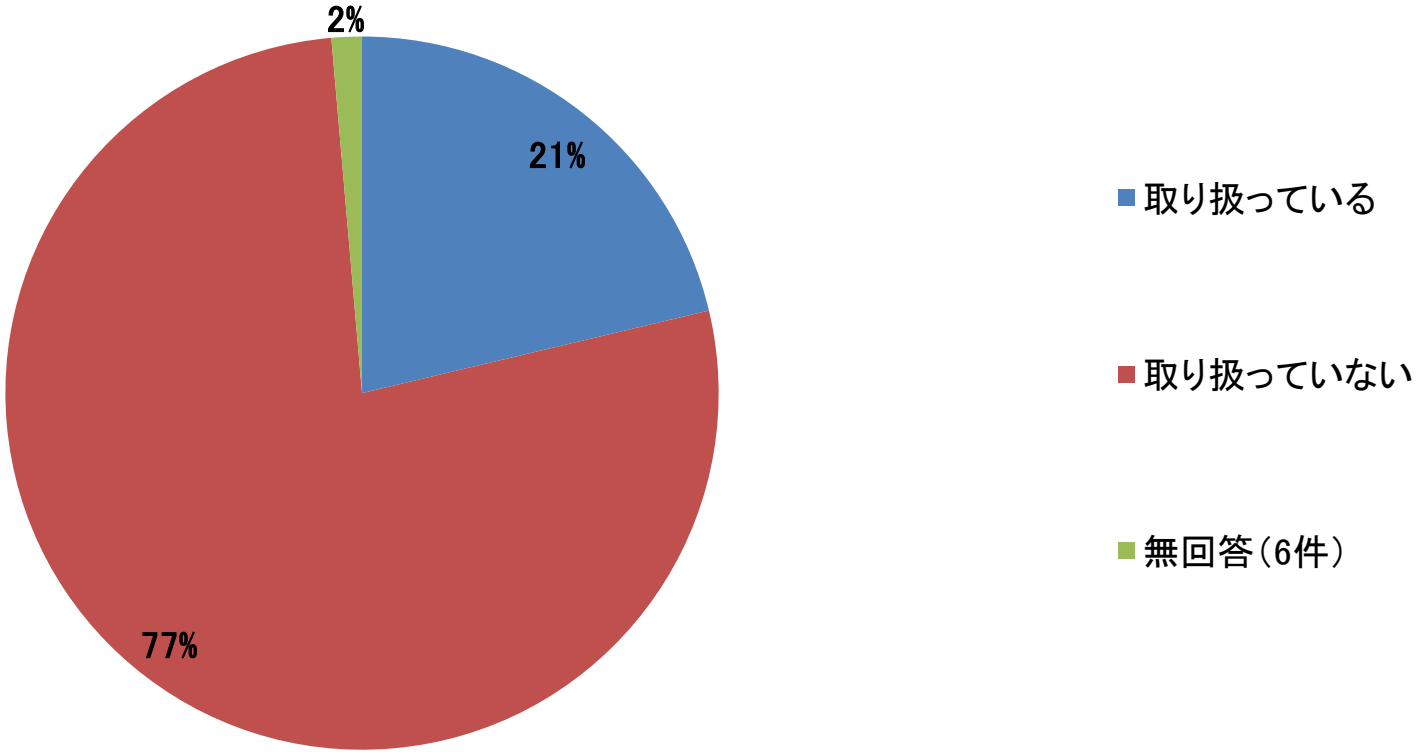
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 少数回答ではあったが、テストの成績の悪い社員や長期休暇・出向から復帰した社員に対して教育を行うなど、フォローアップをしている組織が見られた。

第５章
「個人の行動履歴データ」の取扱い

第5章　個人の行動履歴データの取扱い

設問29.「個人の行動履歴データ」の業務での取り扱い(N=437)



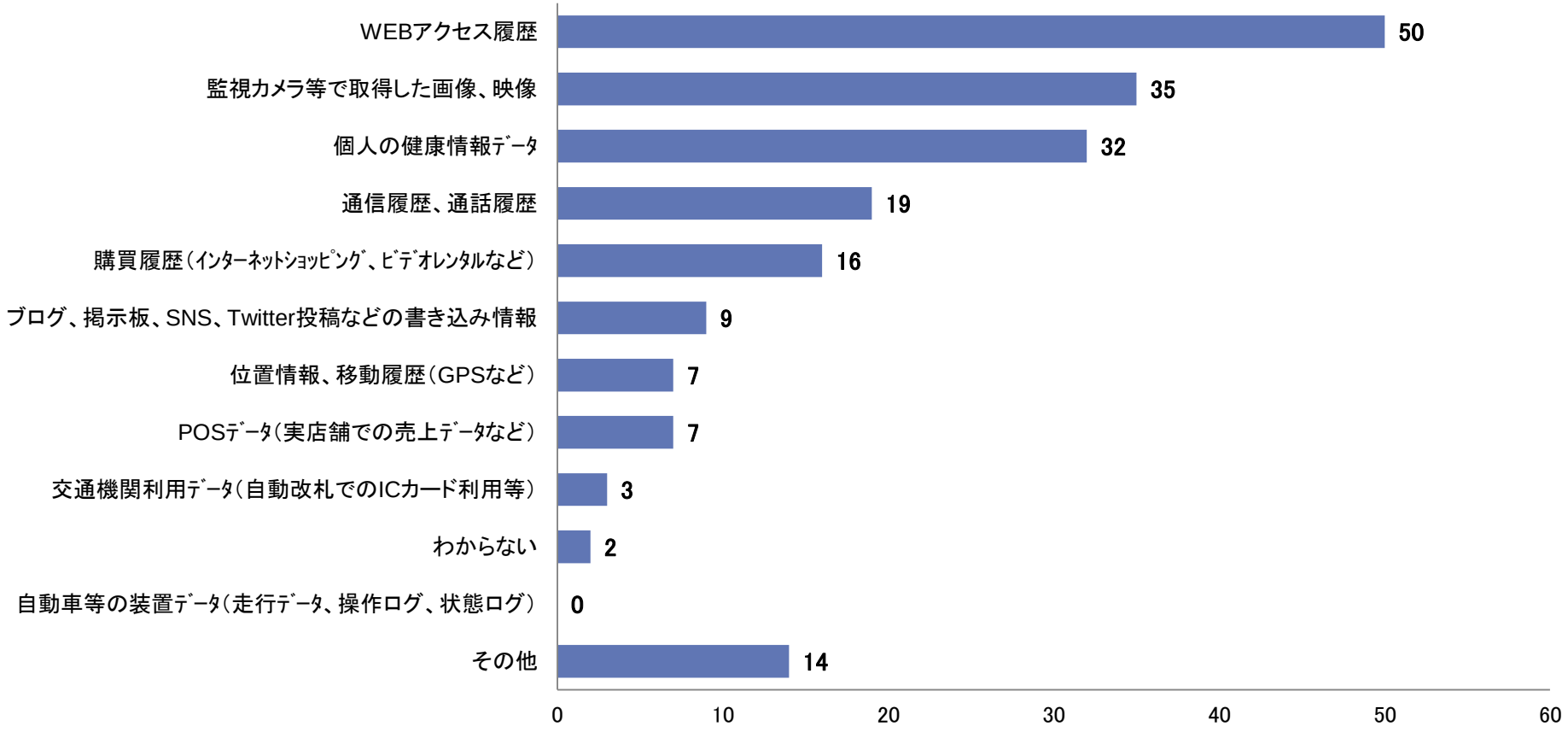
アンケート回答組織の内、個人の行動履歴データを取り扱っている組織が21%（93組織）。

第5章　個人の行動履歴データの取扱い

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

※設問29.で「1. **取り扱っている**」と選択した組織のみ

設問30. 取り扱っている「個人の行動履歴データ」の種類(N=93)



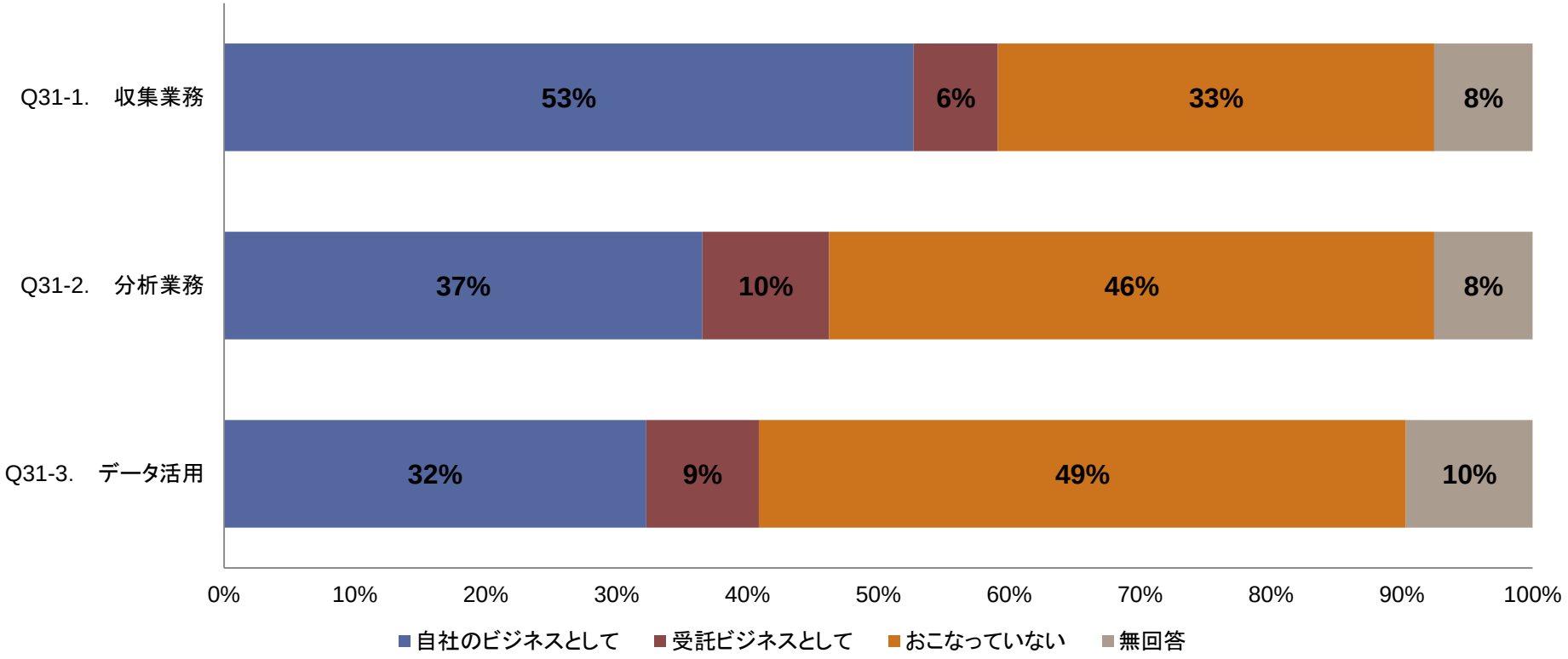
WEBアクセス履歴が1番多く、50件の回答数であった。

第5章　個人の行動履歴データの取扱い

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

※設問29.で「1. **取り扱っている**」と選択した組織のみ

設問31.「個人の行動履歴データ」に関する業務内容(N=93)

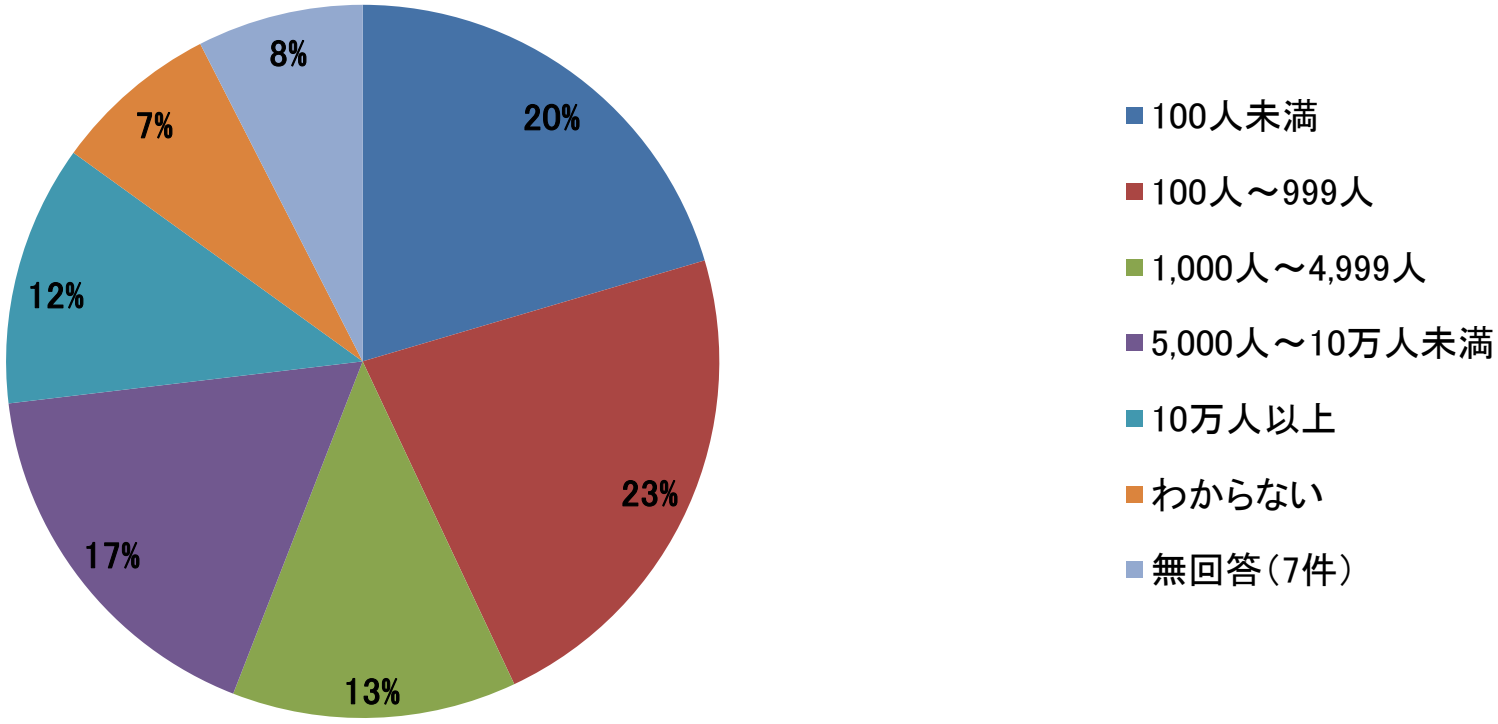


個人の行動履歴データの収集業務を自社のビジネスとして行っている組織が50%強であった。

第5章　個人の行動履歴データの取扱い

※設問29.で「1. **取り扱っている**」と選択した組織のみ

設問32. 取り扱っている「個人の行動履歴データ」の対象人数(N=93)



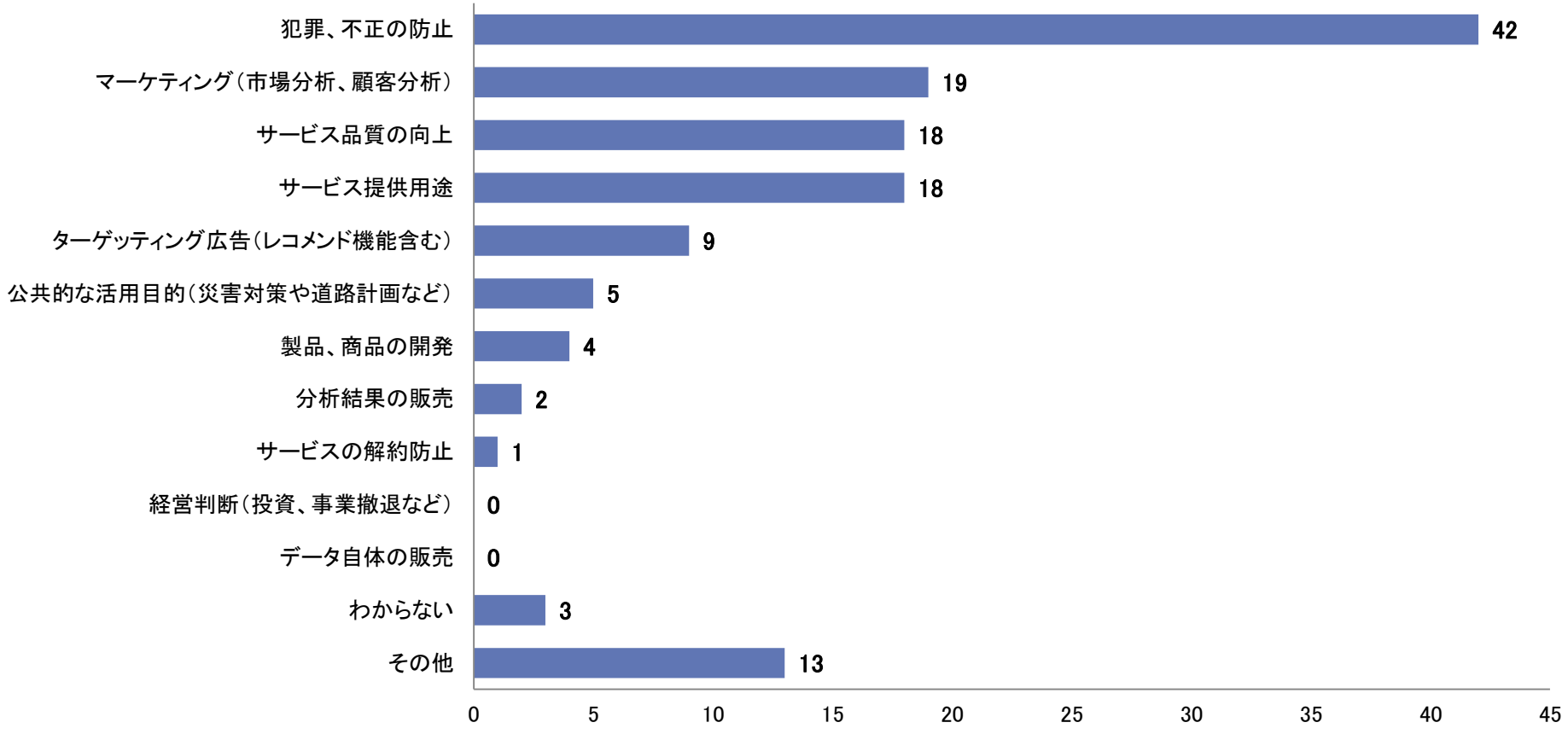
個人の行動履歴データの対象人数が、個人情報保護法対象となる5,000人以上の組織は、約29%。

第5章　個人の行動履歴データの取扱い

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

※設問29.で「1. **取り扱っている**」と選択した組織のみ

設問33.「個人の行動履歴データ」を取り扱い業務の目的(N=93)



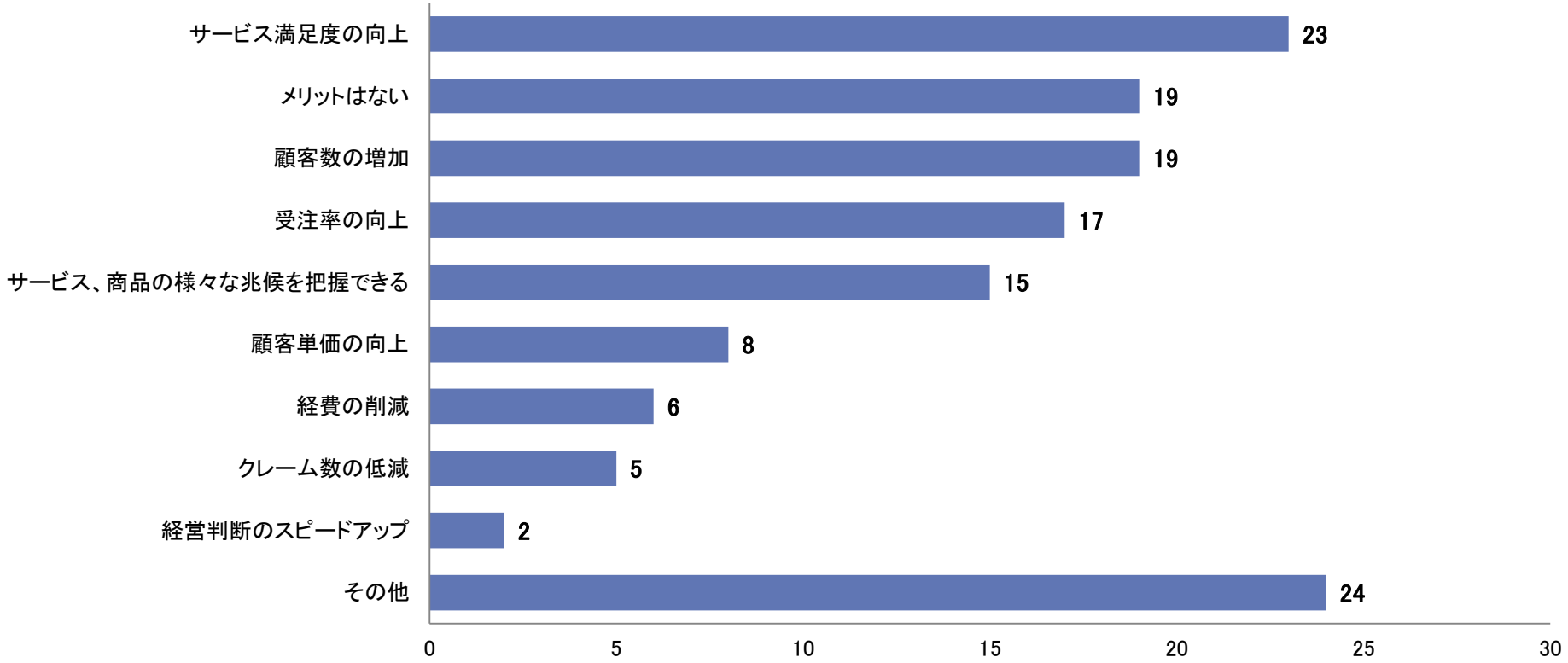
犯罪、不正の防止が圧倒的に多く、42件(93件中)という回答数であった。

第5章　個人の行動履歴データの取扱い

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

※設問29.で「1. **取り扱っている**」と選択した組織のみ

設問34.「個人の行動履歴データ」取り扱い業務を行うメリット(N=93)



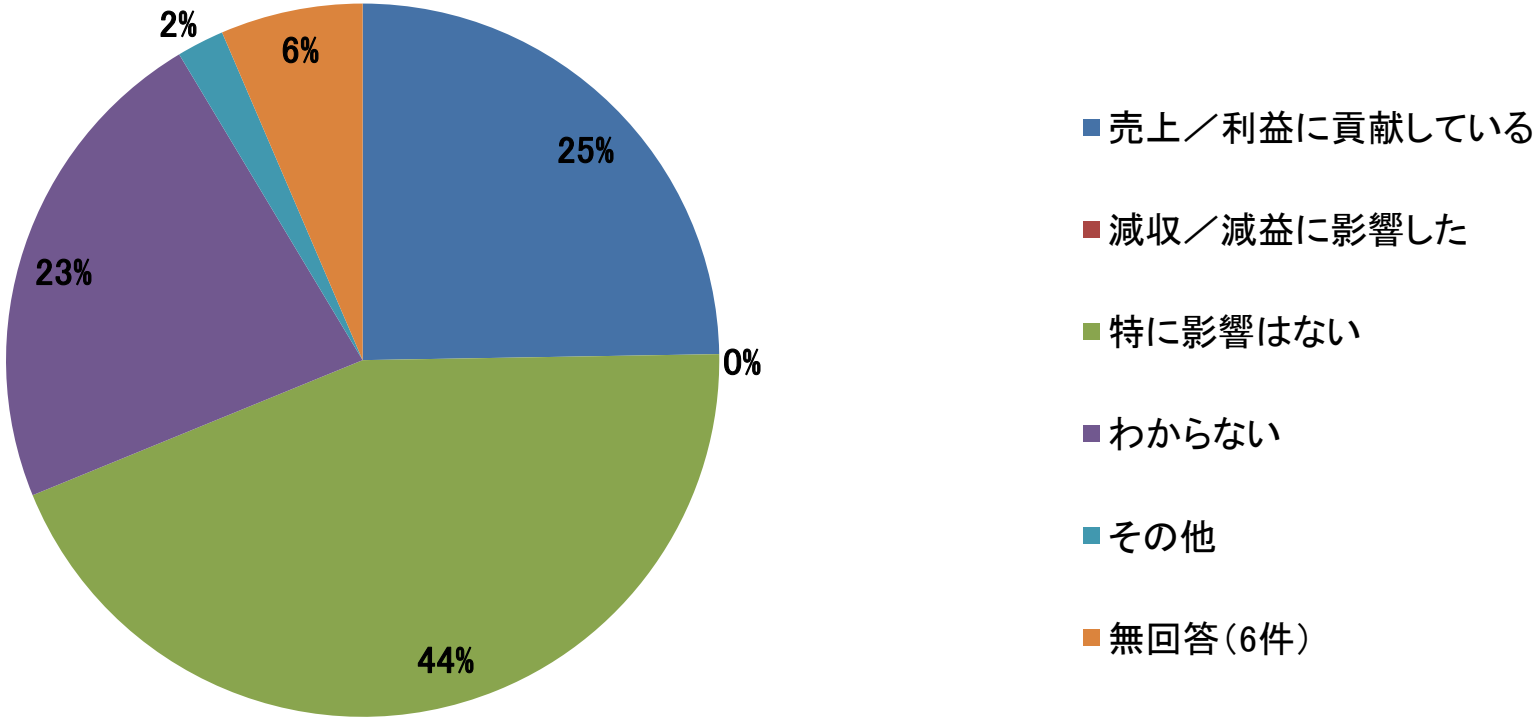
その他が一番多かったが、その中身としては、犯罪、不正の防止に関するメリットの記述が多く見られた。

第5章　個人の行動履歴データの取扱い

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

※設問29.で「1. **取り扱っている**」と選択した組織のみ

設問35.「個人の行動履歴データ」取り扱い業務による売上／利益への影響(N=93)

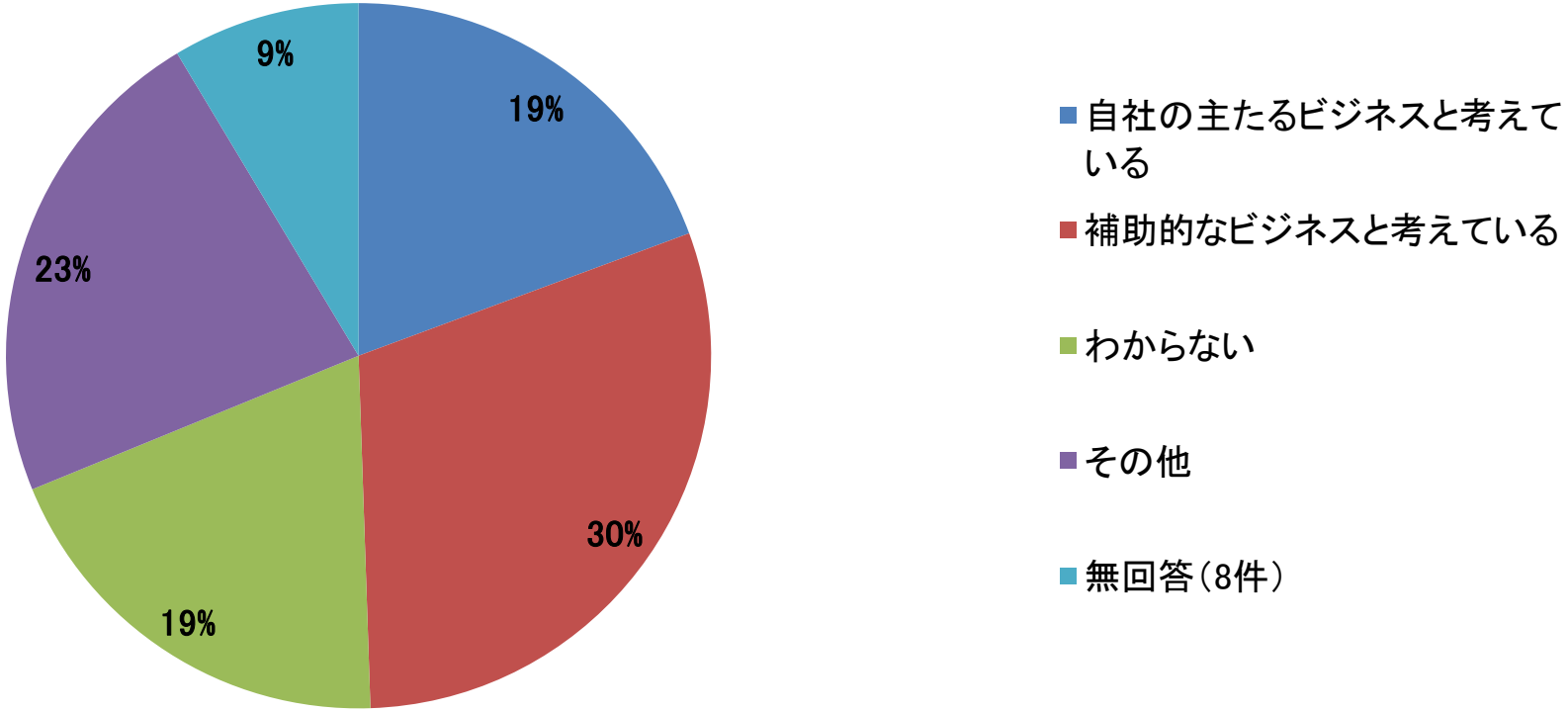


個人の行動履歴データの取り扱いが、特に売上／利益に影響はないと回答した組織が一番多く、約44%であった。

第5章　個人の行動履歴データの取扱い

※設問29.で「1. **取り扱っている**」と選択した組織のみ

設問36.「個人の行動履歴データ」を取り扱う業務の位置付け(N=93)



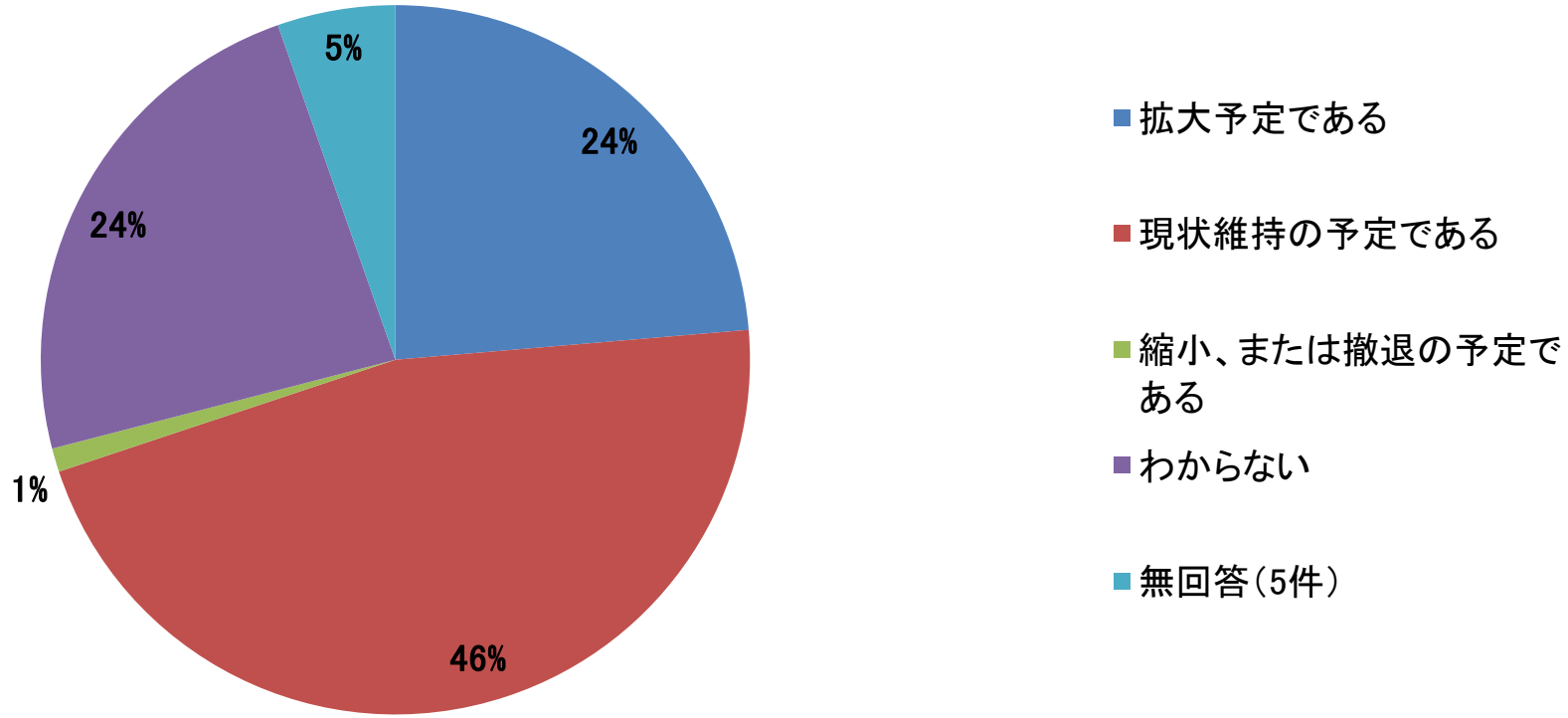
個人の行動履歴データの取り扱いが、自社の主たるビジネス、もしくは補助的なビジネスと考えている組織が約50%であった。

第5章　個人の行動履歴データの取扱い

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

※設問29.で「1. **取り扱っている**」と選択した組織のみ

設問37.「個人の行動履歴データ」取り扱い業務の拡大予定(N=93)



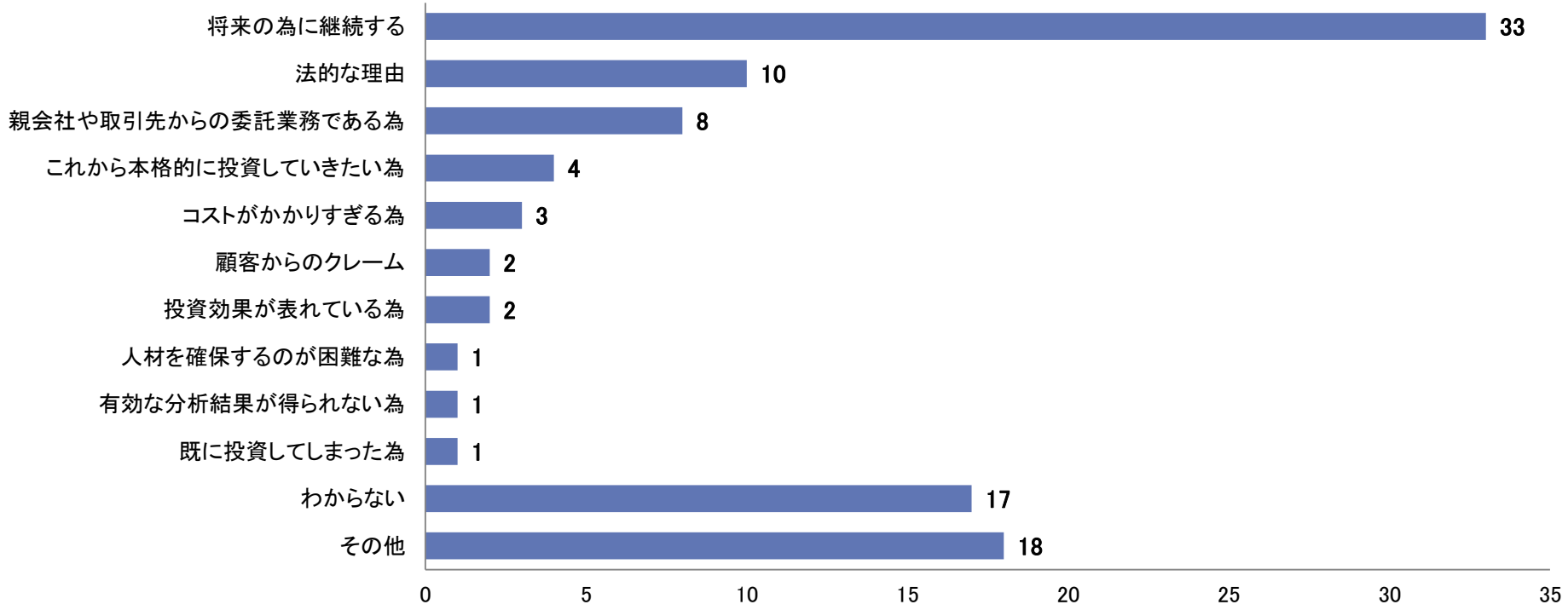
個人の行動履歴データの取り扱い業務について、
現状維持の予定であると回答した組織が一番多く、約46%であった。

第5章　個人の行動履歴データの取扱い

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

※設問29.で「1. **取り扱っている**」と選択した組織のみ

設問38.「個人の行動履歴データ」取り扱いの、拡大、縮小/撤退、現状維持の理由(N=93)



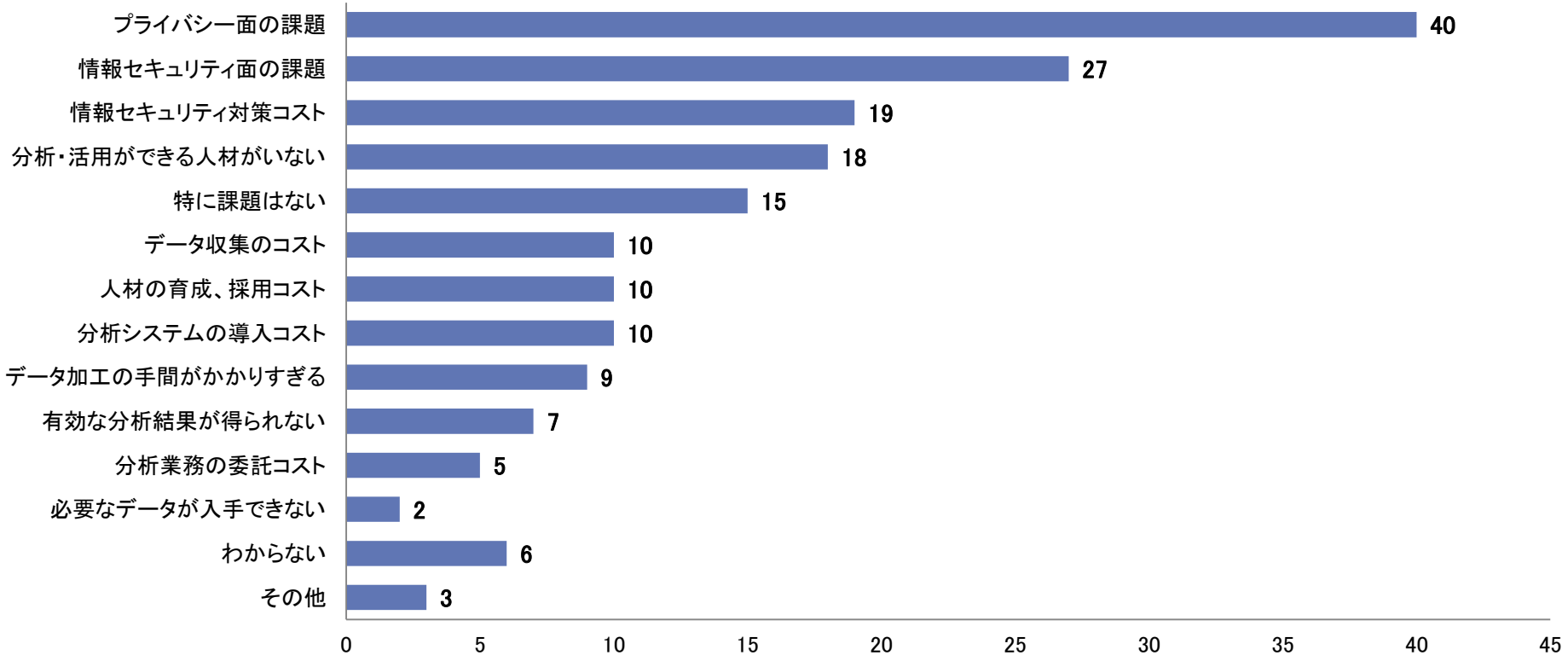
個人の行動履歴データの取り扱い業務の拡大、縮小、撤退については、将来の為に継続するという回答が1番多かった。

第5章　個人の行動履歴データの取扱い

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

※設問29.で「1. **取り扱っている**」と選択した組織のみ

設問39.「個人の行動履歴データ」の取り扱いにあたっての主な課題(N=93)



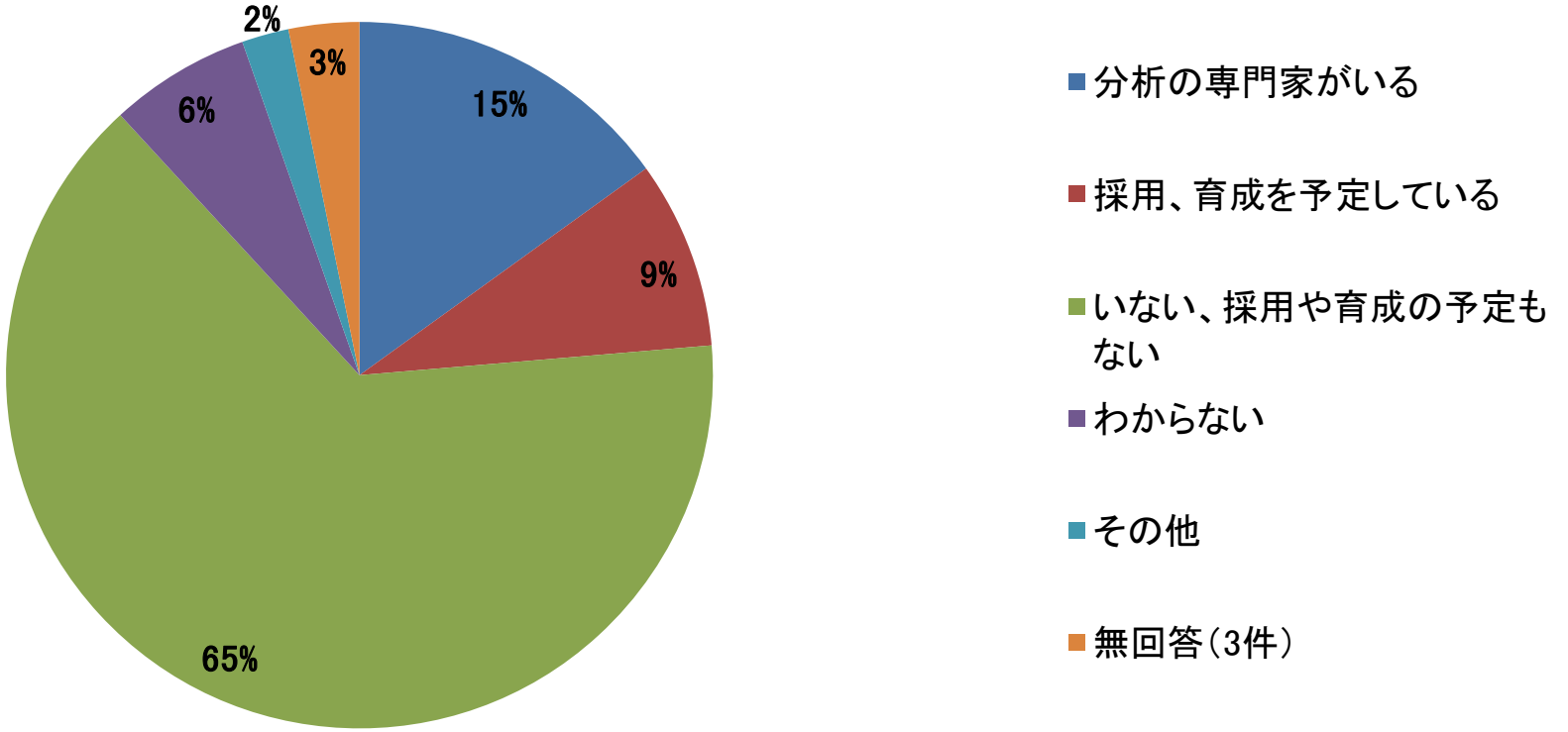
個人の行動履歴データの取り扱いにおける主な課題で1番多かったのが、プライバシー面の課題で40件の回答数であった。

第5章　個人の行動履歴データの取扱い

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

※設問29.で「1. **取り扱っている**」と選択した組織のみ

設問40. データ分析の専門家の有無(N=93)



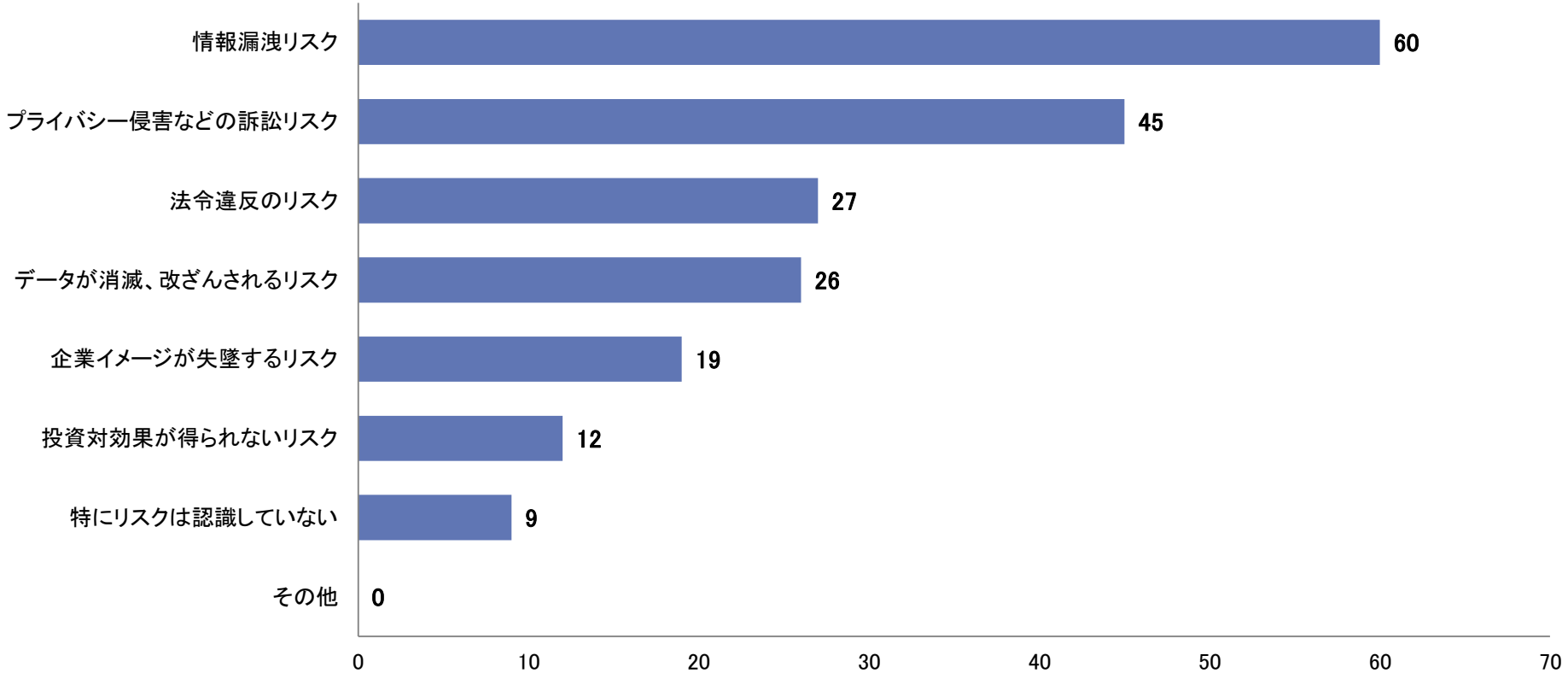
いない、採用や育成の予定もないと回答した組織が一番多く、約65%であった。

第5章　個人の行動履歴データの取扱い

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

※設問29.で「1. **取り扱っている**」と選択した組織のみ

設問41.「個人の行動履歴データ」の収集・分析・活用業務を取り扱いにあたり認識しているリスク(N=93)



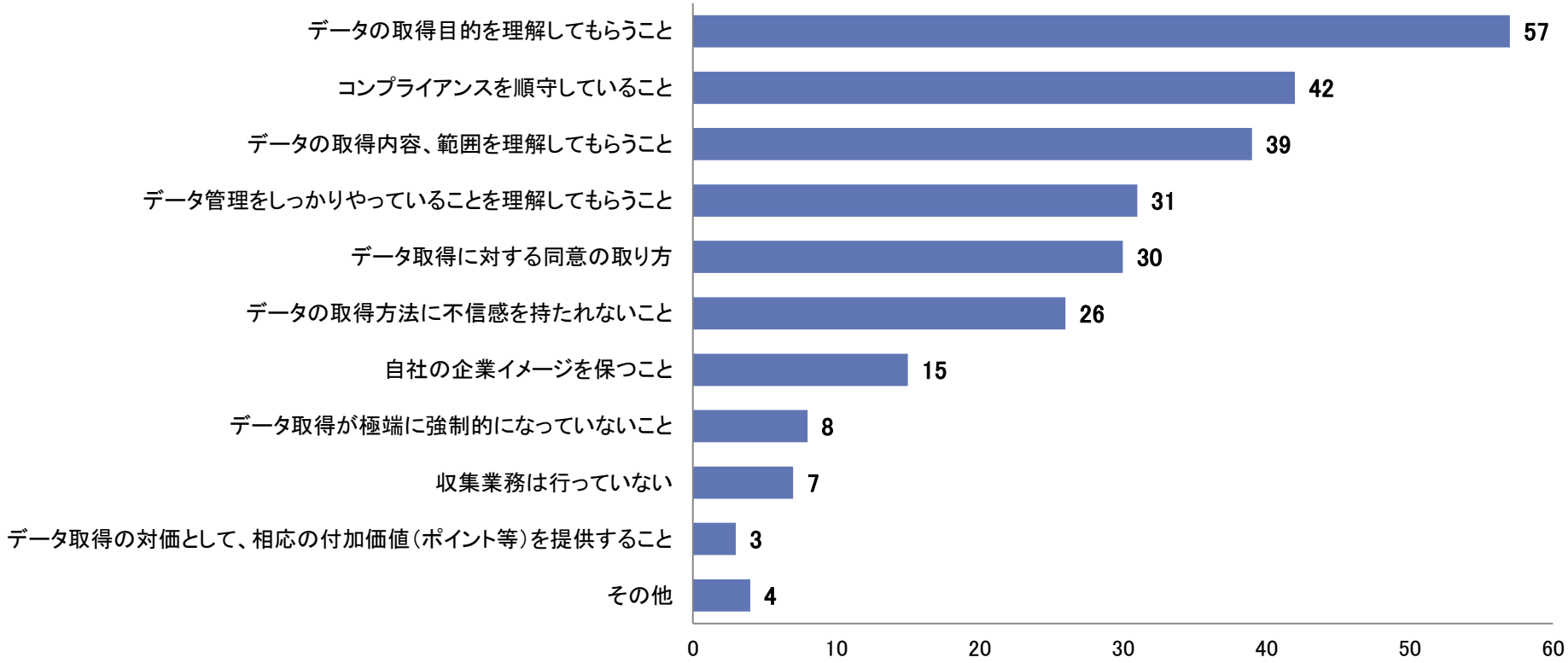
情報漏洩のリスクが一番多く、60件の回答数であった。

第5章　個人の行動履歴データの取扱い

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

※設問29.で「1. **取り扱っている**」と選択した組織のみ

設問42.「個人の行動履歴データ」を収集するにあたっての考慮点(N=93)



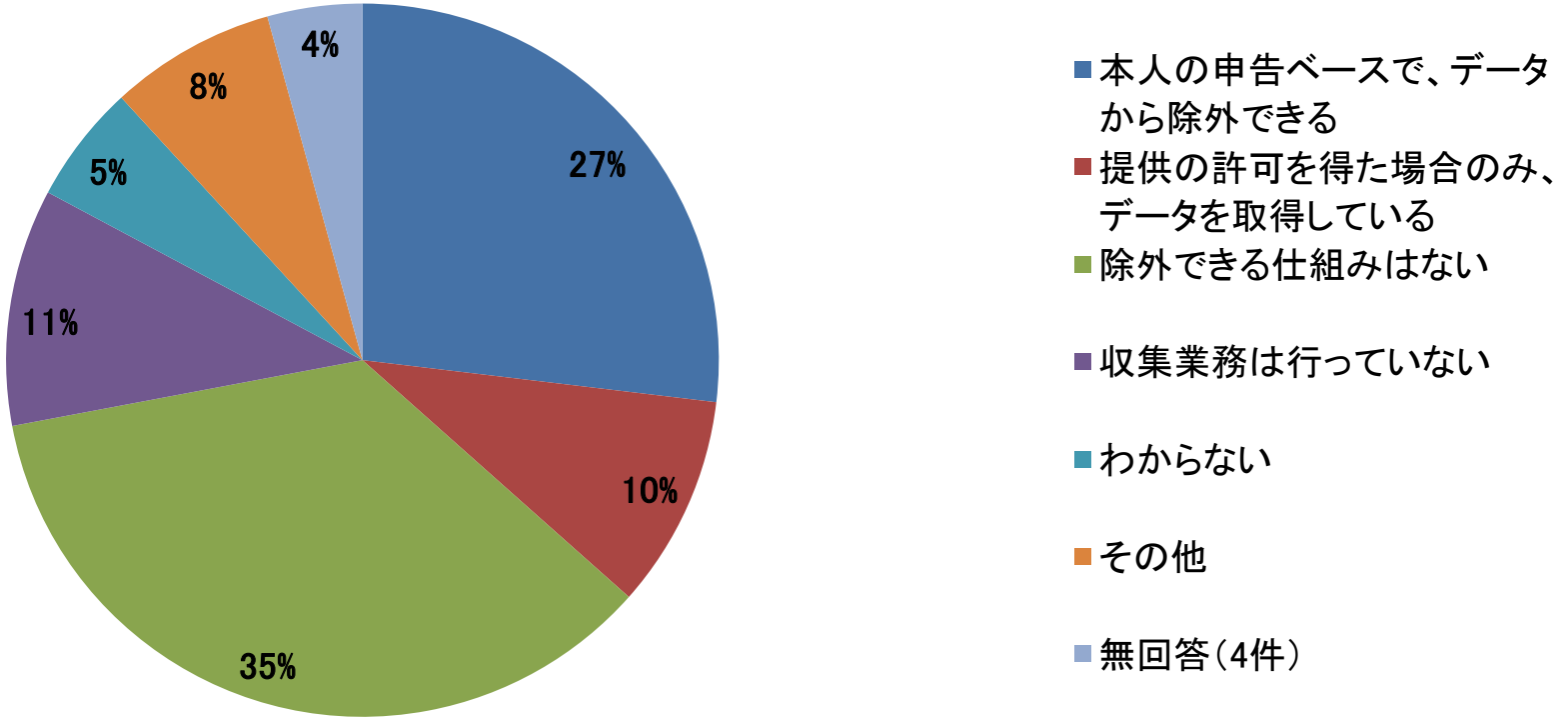
一番多かったのはデータの取得目的を理解してもらうことで、約57件の回答数であった。これは回答総数(N=93)に対し、60%強の回答率となる。

第5章　個人の行動履歴データの取扱い

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

※設問29.で「1. **取り扱っている**」と選択した組織のみ

設問43.「個人の行動履歴データ」からの本人の希望によるデータからの除外(N=93)



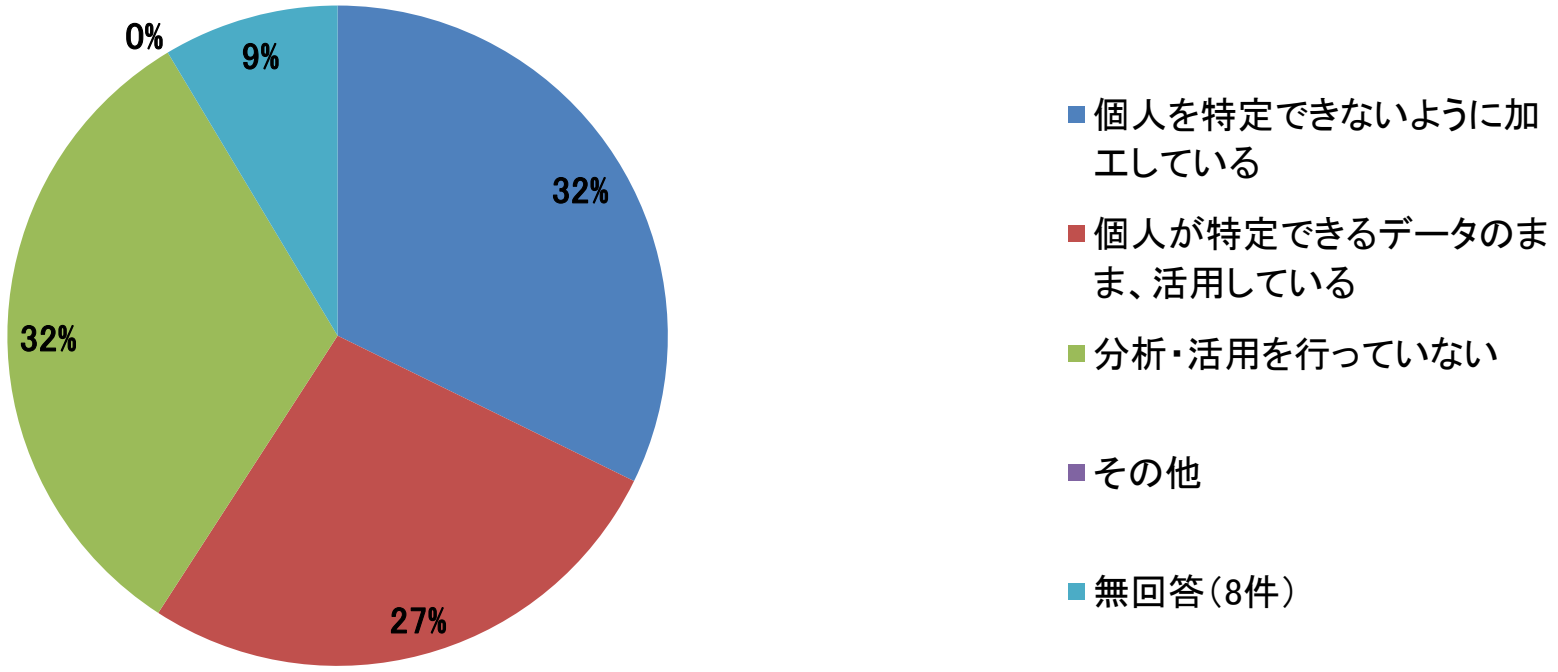
本人の希望により個人の行動履歴データから除外出来る仕組みが無いと回答した組織が1番多く、約35%であった。

第5章　個人の行動履歴データの取扱い

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

※設問29.で「1. **取り扱っている**」と選択した組織のみ

設問44「個人の行動履歴データ」を分析・活用する際の個人特定性(N=93)



個人の行動履歴データの分析・活用を行うにあたり、個人を特定できないように加工している組織が約32%で1番多かった。

考察（第5章　個人の行動履歴データの取扱い）

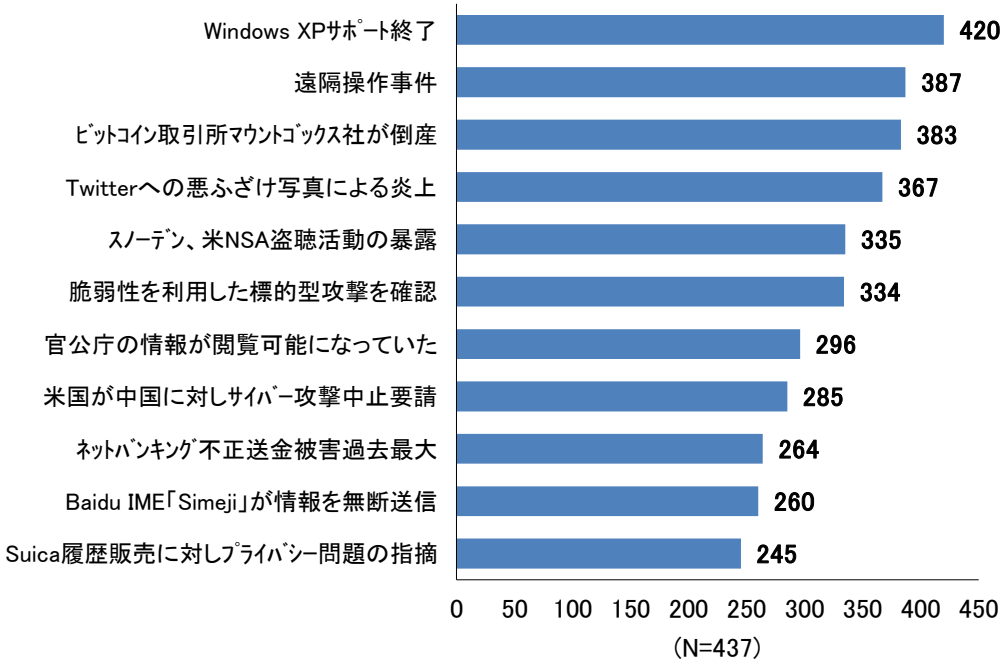
- 個人の行動履歴データの利活用目的で1番多かったのは、犯罪／不正の防止であった。個人の行動履歴の利活用については、マーケティングやターゲッティング広告のように売上／利益に繋がるものもあるが、今回調査した母集団におけるアンケート結果では、売上／利益よりも、犯罪、不正の防止目的の方が多く活用されている。

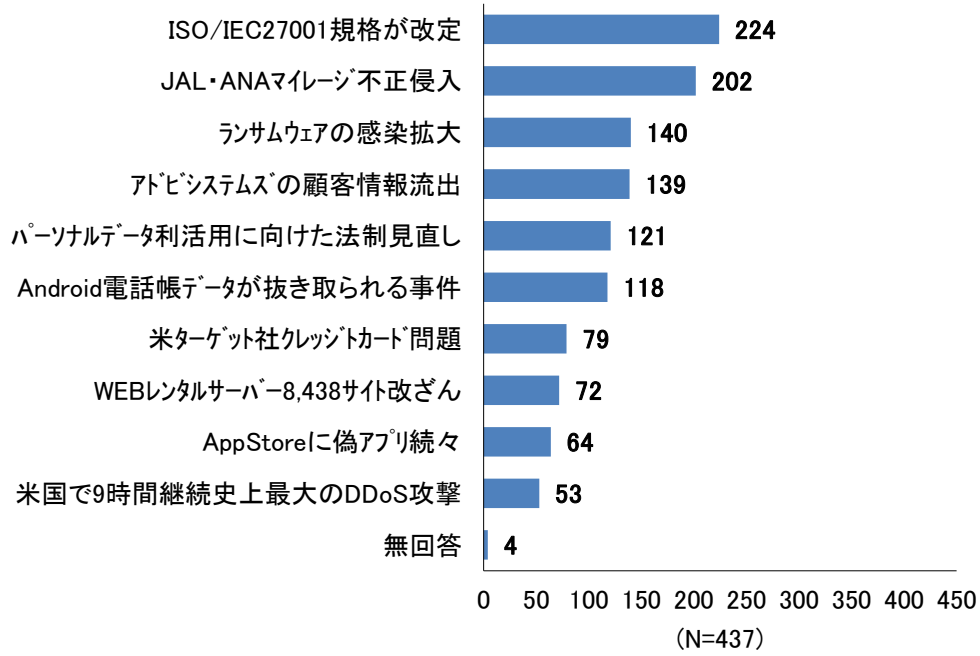
第6章
過去の事例・事故・用語の認知度

第6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45. 過去の事例・事故の認知度(N=437)

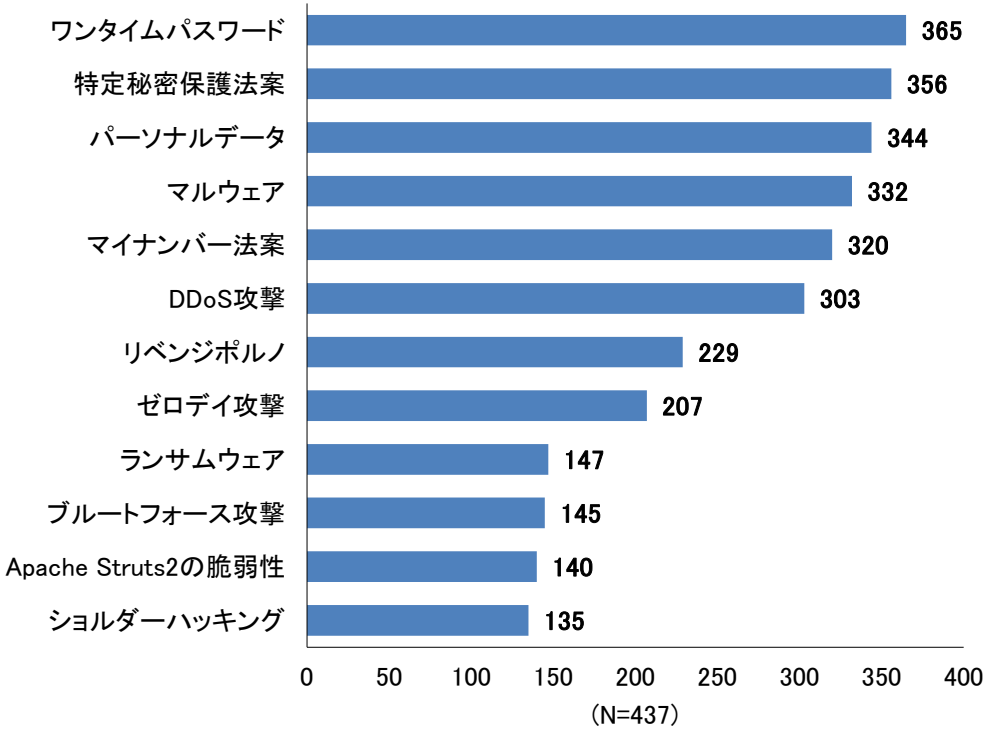


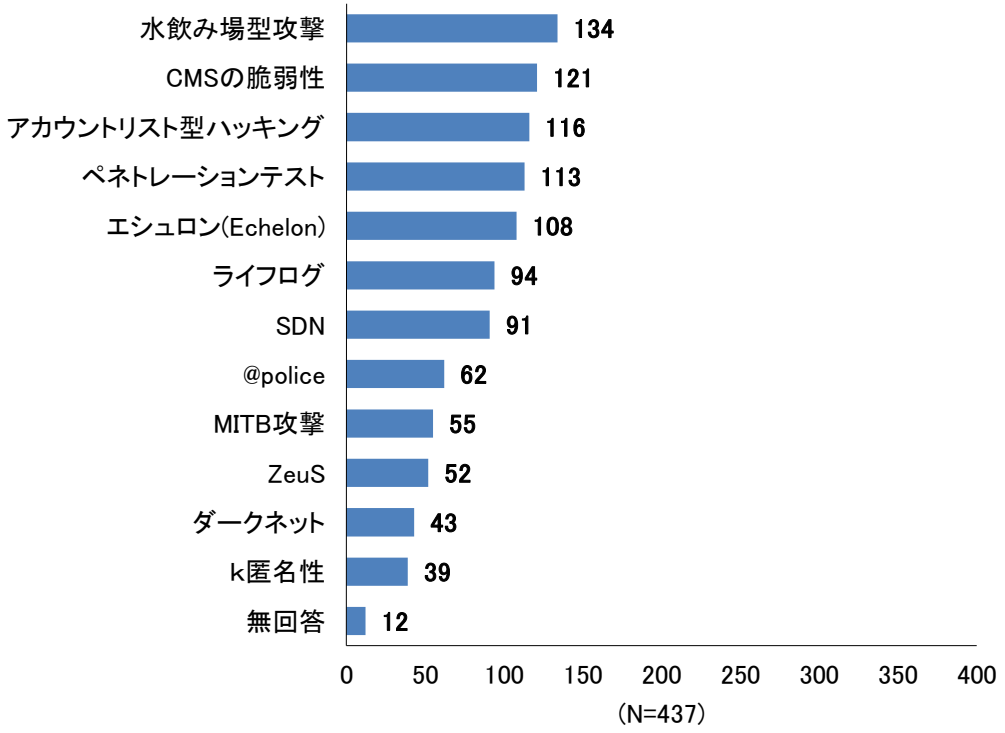


マスメディアで取り上げられた事件・事故への認知度が高く、あまり取り挙げられない海外事故など専門的なものについては認知度が高くない。ISMS既取得組織が対応する必要がある「ISO/IEC27001規格が改定」の認知度が51%となっている。

第6章　過去の事例・事故・用語の認知度

設問46. 用語の認知度(N=437)





マスメディアやセキュリティ関連組織で頻繁に取り上げている用語についての認知度は高い傾向となっている。反面、攻撃手法や一般化されていない専門用語(ライフログやダークネットなど)の認識度が低い。

考察（第6章　過去の事例・事故・用語の認知度）

- 例年の傾向通り、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、遠隔操作事件、ビットコイン取引所マウントゴックス社が倒産、Twitterへの悪ふざけ投稿、スノーデン、米NSA盗聴活動の暴露などである。反面、海外での事故・攻撃手法など専門的なものについては高くない傾向が見て取れる。
- 出来事では、ISMS認証基準である「ISO/IEC27001規格が改定」の認知度が51%であり、想定より低かった。既取得組織は2015年10月までにこの改定に対応する必要がある。
- パーソナルデータについては、用語は認知度が高いが、出来事に挙げられた法制の見直しについての認知度は低い結果となった。社会の動きとの結びつけがされていない一例である。

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　生田東分教室
  - 神奈川県立高津養護学校　川崎北分教室
  - 神奈川県立中原養護学校
  - 神奈川県立横浜ひなたやま支援学校
  - 川崎市立田島支援学校
  - 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