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

2016年情報セキュリティ アンケート調査結果

2016年12月28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

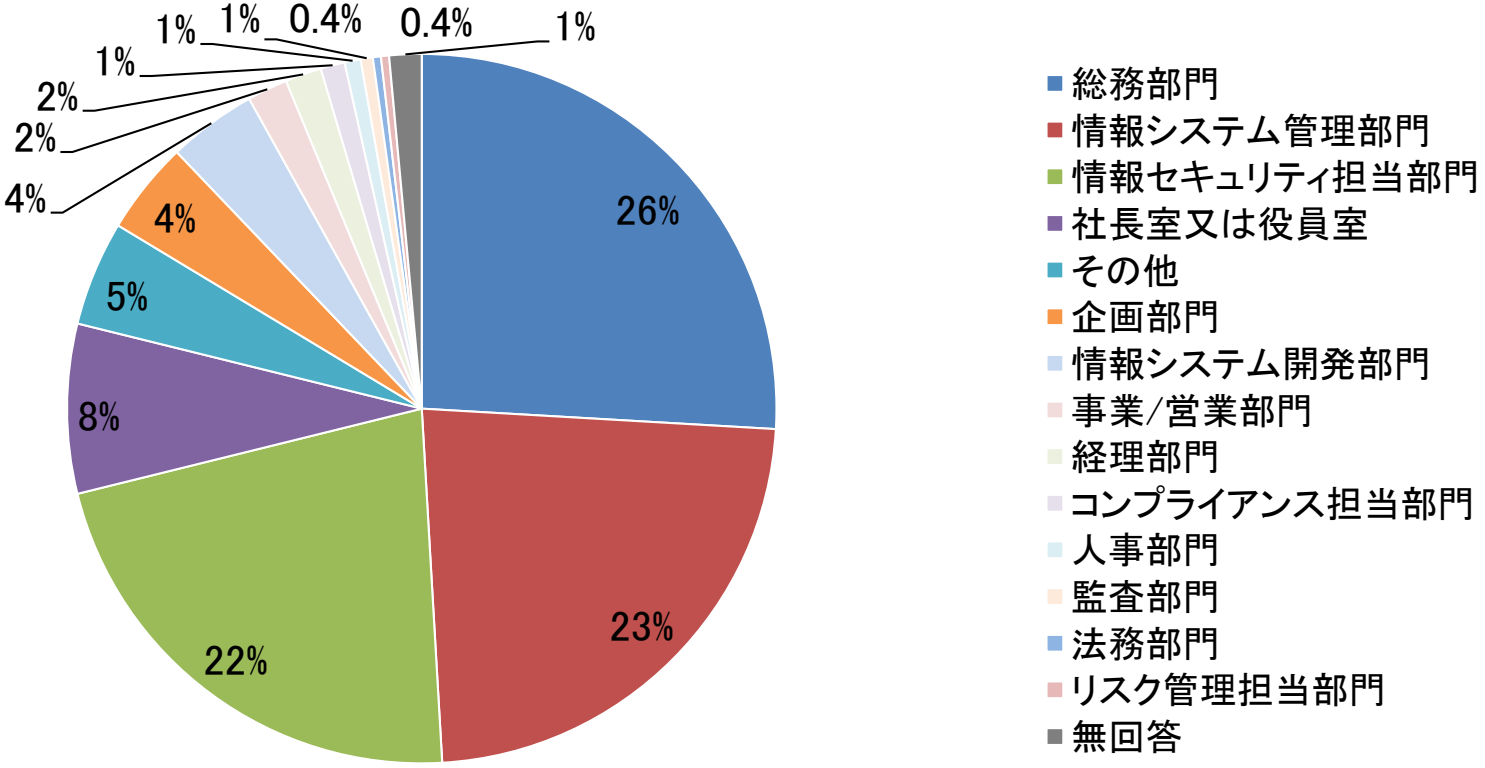
- アンケート実施期間
  2016年8月10日～10月31日
- アンケート対象
  日本国内のプライバシーマーク（以下「Pマーク」という）取得企業、ISMS認証取得企業、官公庁、教育機関(以下「組織」という)など4,800組織の情報セキュリティ関係者
- アンケート内容
  情報セキュリティマネジメントの取組状況（インシデント対応と人材育成等）、IT資産の利用・管理体制、アプリケーションセキュリティのリスク管理、クラウド利用状況および課題、マイナンバーの取り組み、過去の事例・事故や用語の認知度について
- 調査方法
  郵送による
- 回答状況
  544件（送達確認できた4,704組織に対して11.6%）

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=544）

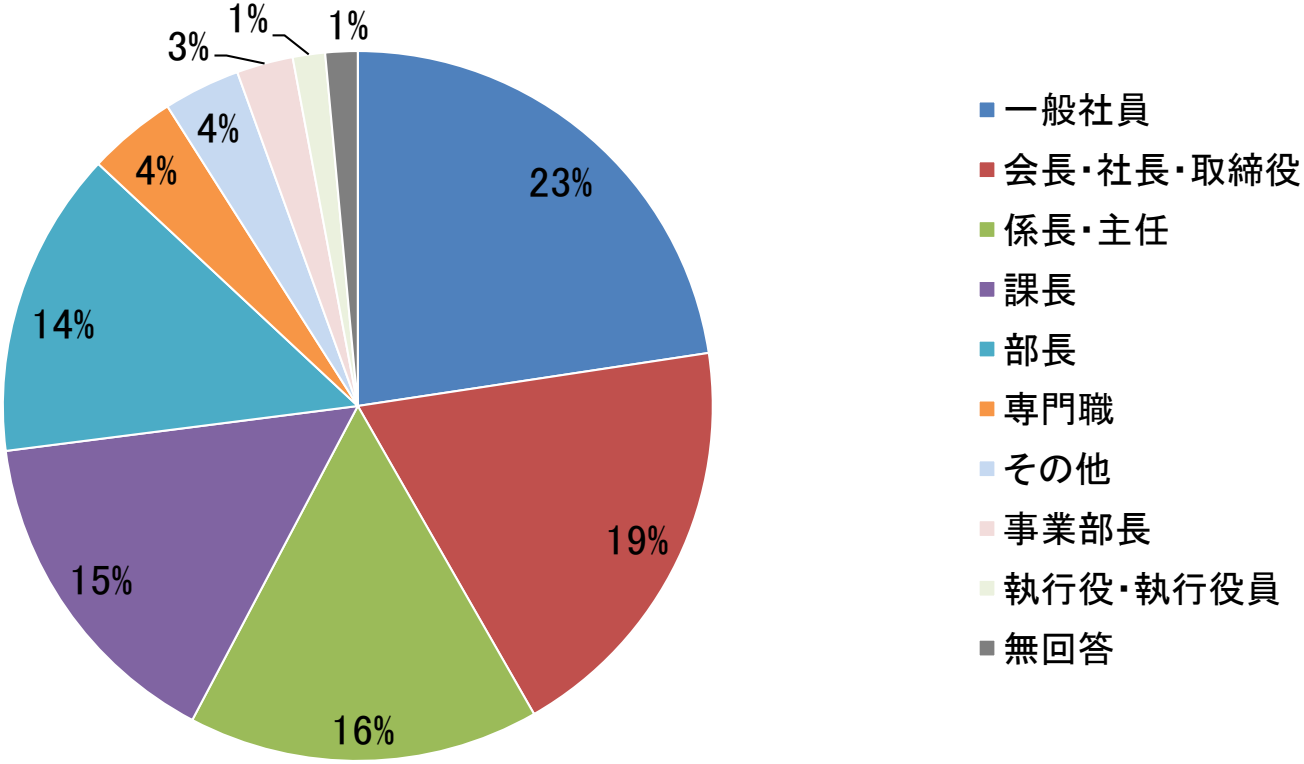


所属部門は、総務部門、情報システム管理部門、
情報セキュリティ担当部門の順に多かった。

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=544）

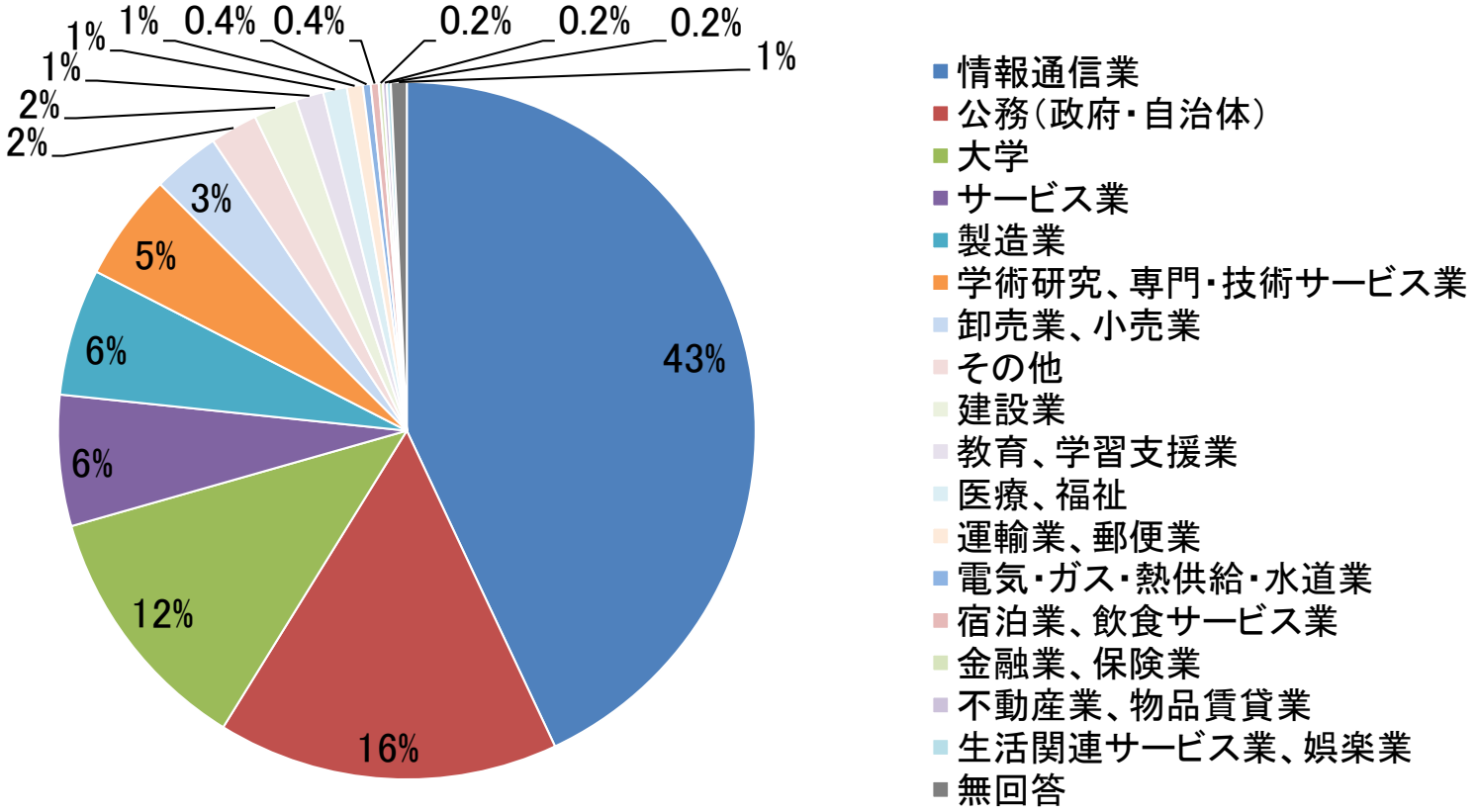


回答者は、一般社員が最も多く、会長・社長・取締役、
係長・主任、課長と続く。

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=544）



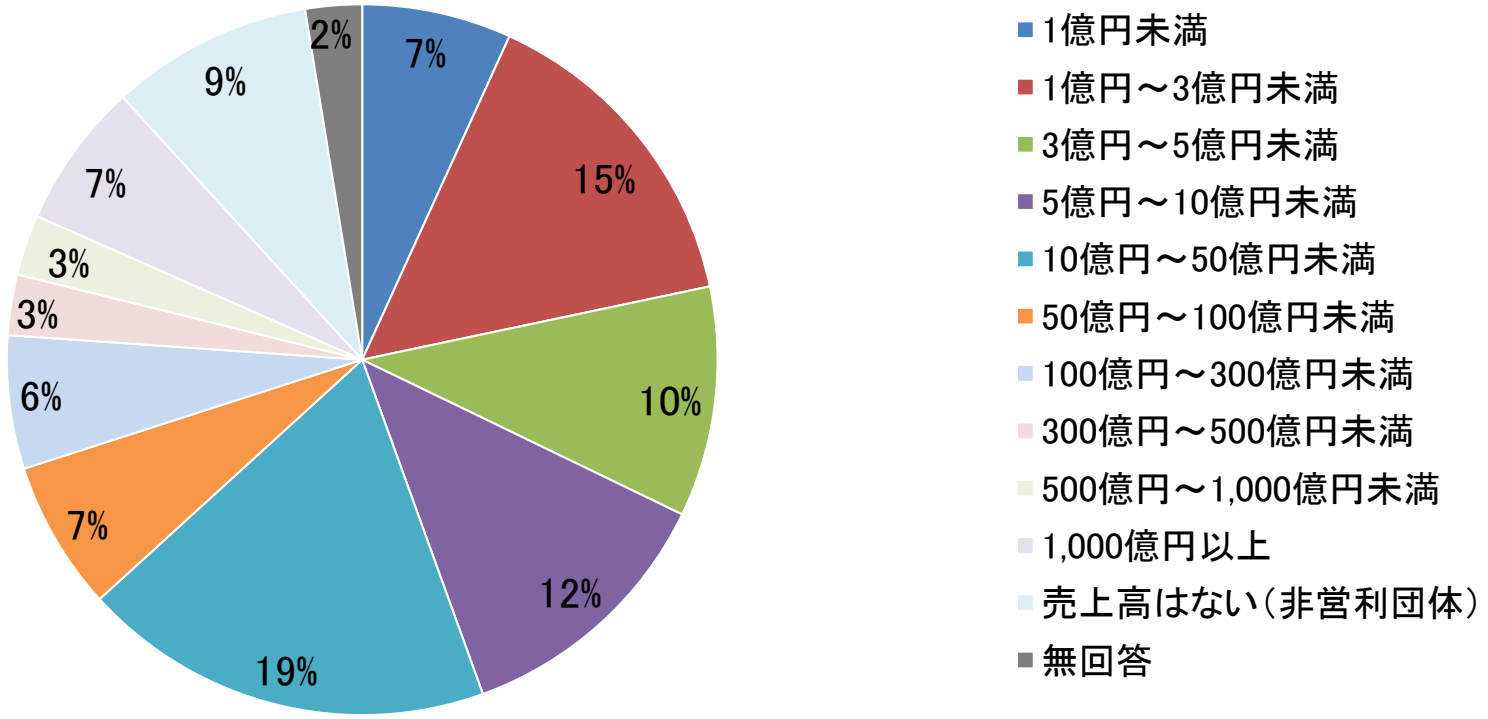
情報通信業が43%と4割を占めている。

※業種は総務省「日本標準産業分類（2013年10月改定）」をベースとして使用。

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（N=544）

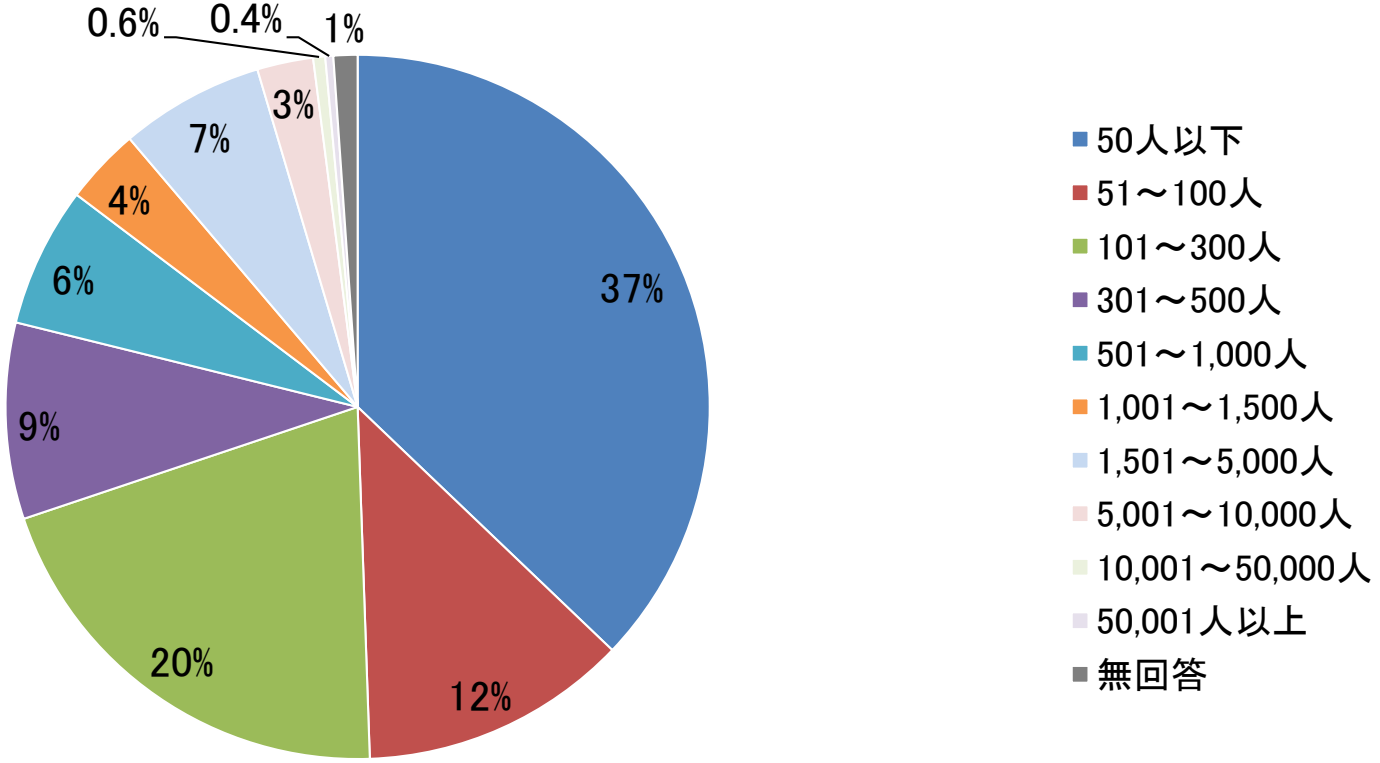


売上高10億円から50億円の組織が最も多い。
また、売上高50億円以下の組織で63%を占めている。

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5. 従業員数（N=544）

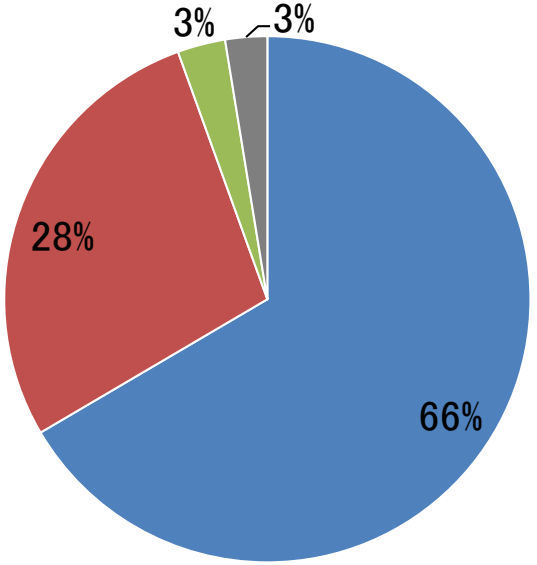


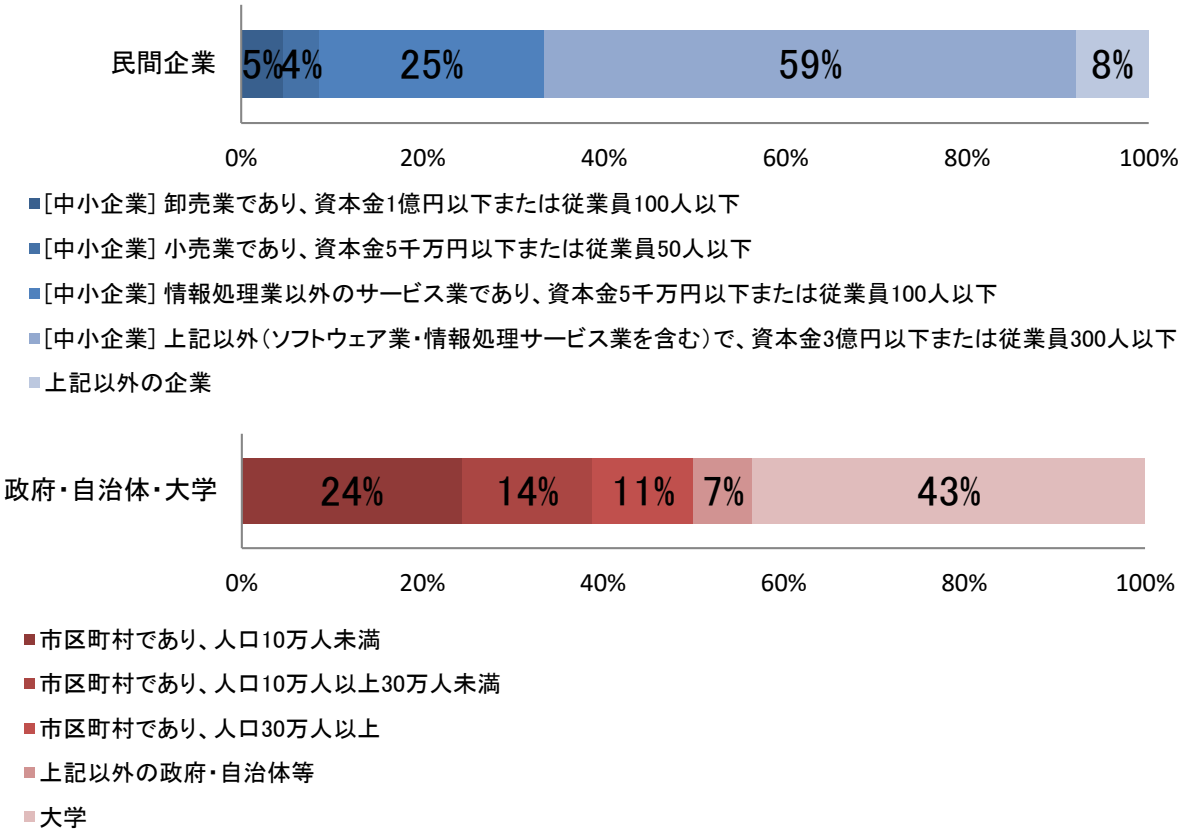
従業員数50人以下の組織が最も多い。
また、従業員数300人以下の組織で70%を占めている。

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6. 組織の種別及び規模（N=544）



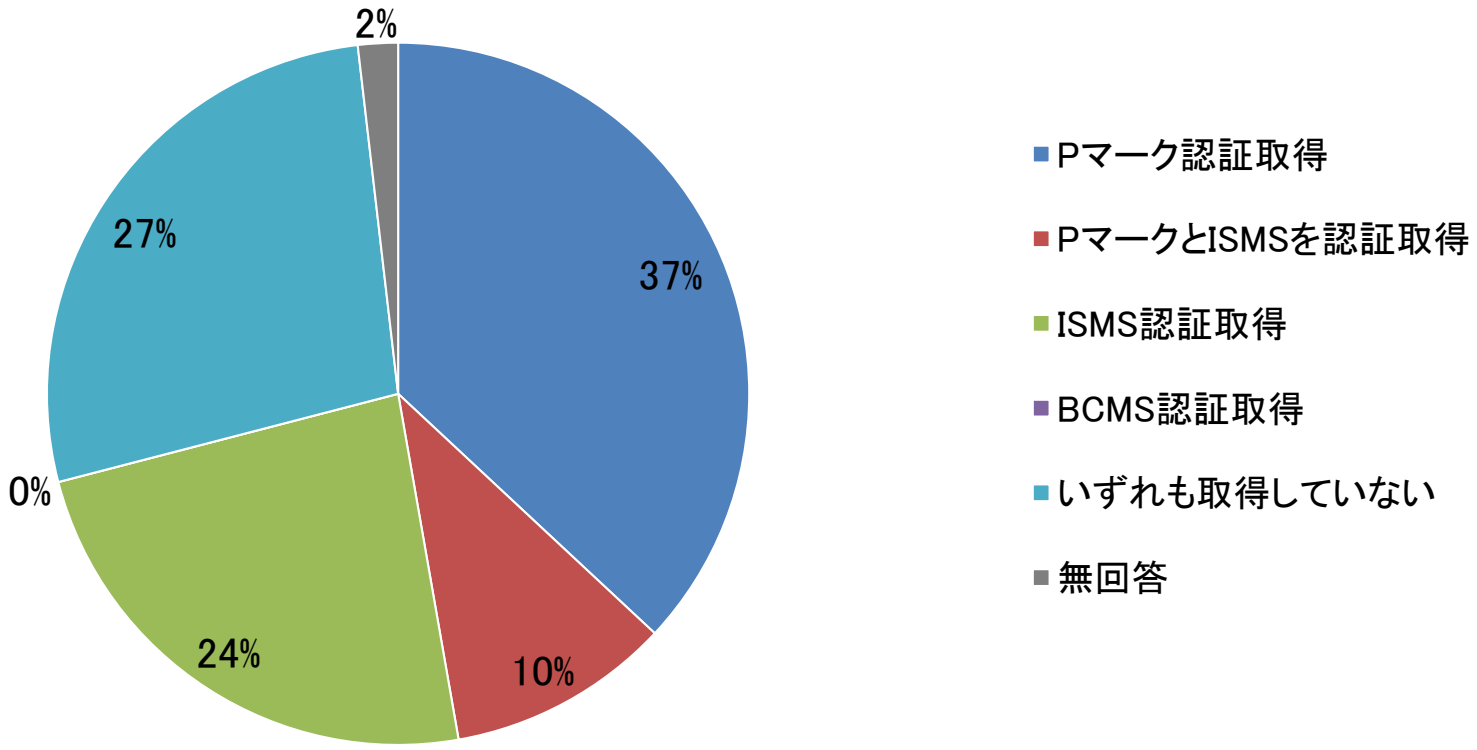


民間企業66%、政府・自治体・大学28%となっている。
中小企業が民間企業の92%を占めている。

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. プライバシーマーク、ISMS、BCMSの取得状況（N=544）



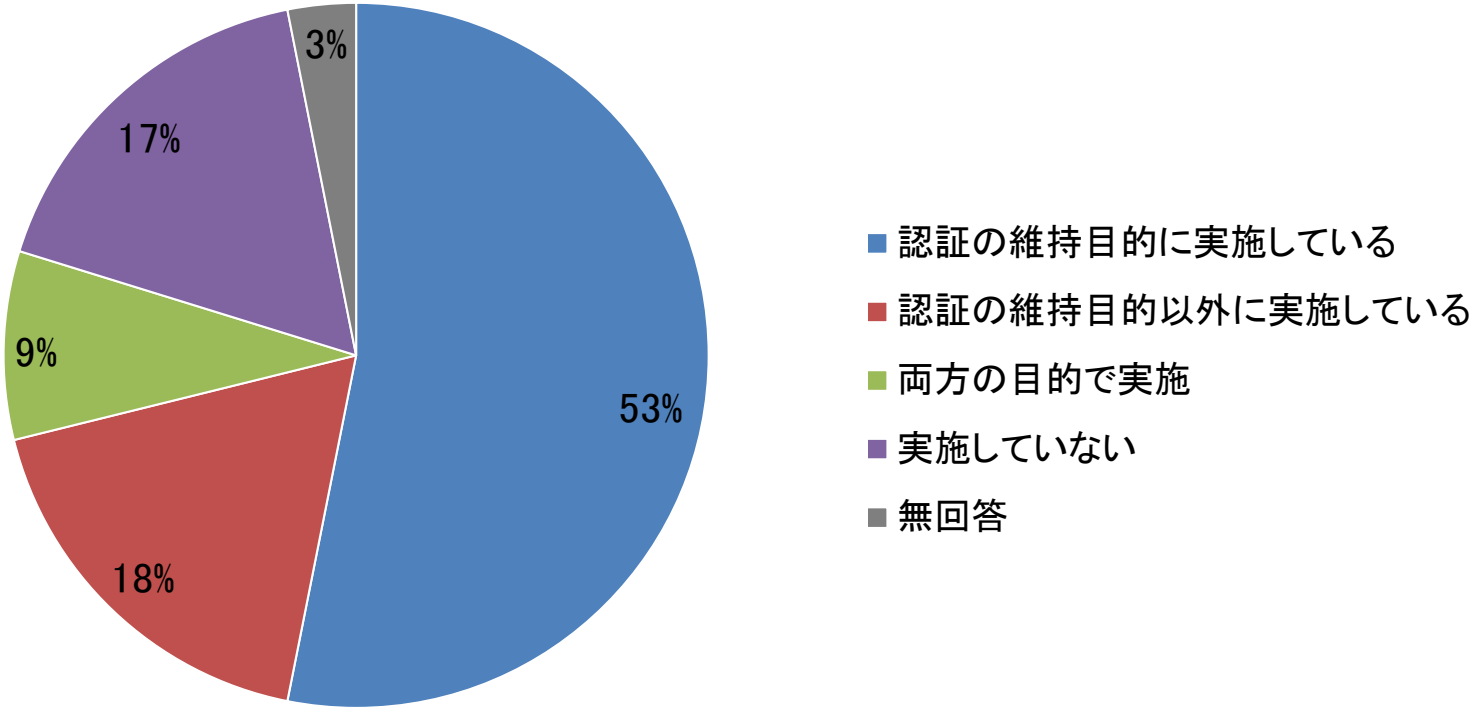
47%の組織がPマークを、34%の組織がISMSを取得している。
また、10%の組織がPマークとISMSの両方を取得している。

※複数選択の回答を択一回答になるように処理。

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=544）



53%の組織が認証の維持目的、18%が認証の維持目的以外、
9%が両方の目的で情報セキュリティ監査を実施している。

※複数選択の回答を択一回答になるように処理。

考察(第1章　概要(回答者の基本データ等))

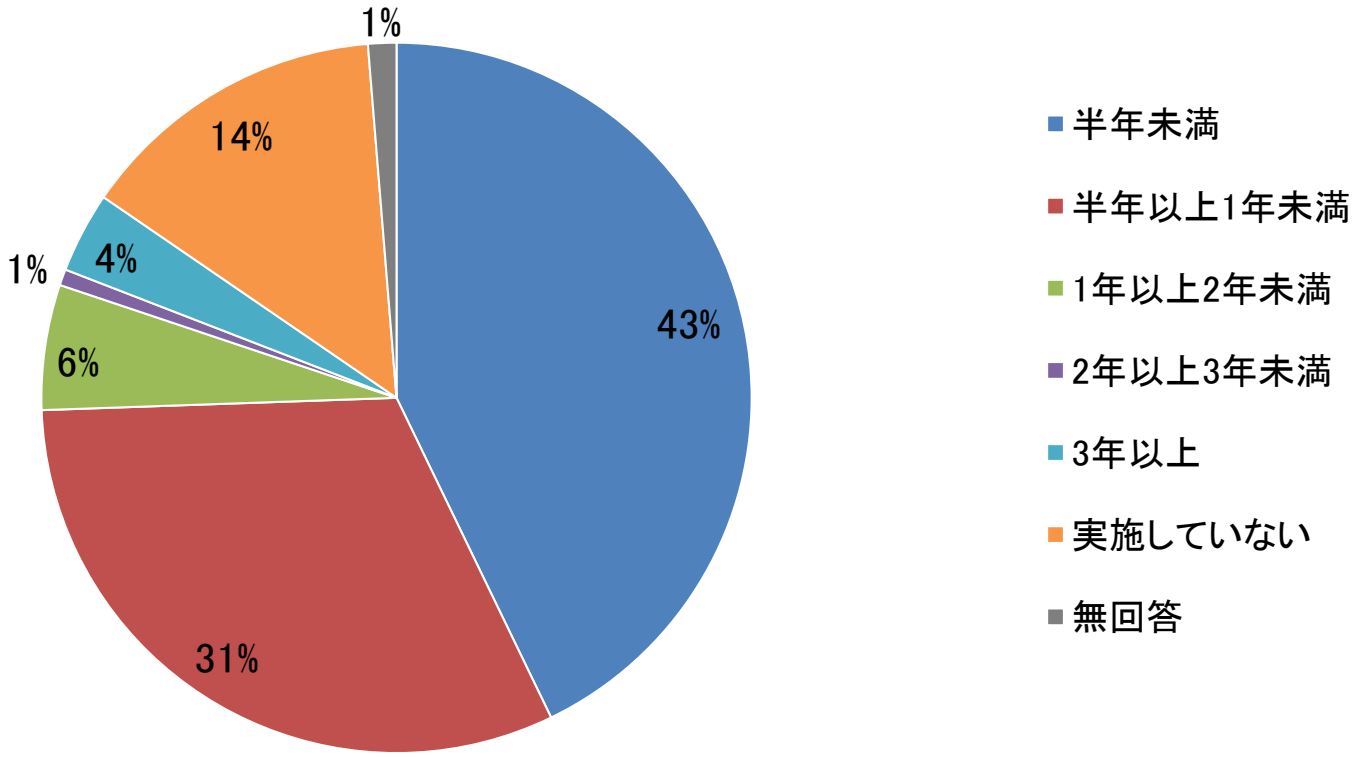
- 情報通信業が回答者の4割を占めている。
- 売上高10億円から50億円の組織が19%と最も多い。
  また、売上高50億円以下の組織で63%を占めている。
- 従業員数50人以下の組織が37%と最も多い。
  また、従業員数300人未満の組織が70%を占めている。
  これは昨年とほぼ同様の結果である。
- 民間企業66%、政府・自治体・大学28%となっている。また、民間企業の92%を中小企業が占めている。
- 2016年は送付先の内訳を変更した(公務(政府・自治体)、大学を増やし、ISMSのみ取得の組織を追加した)。
  回答者のうち、Pマーク、ISMSのいずれかを認証取得している組織は71%で、昨年より少なくなっている。

第2章
情報セキュリティマネジメントの取り組み

第2章　情報セキュリティマネジメントの取り組み状況

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

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=544）



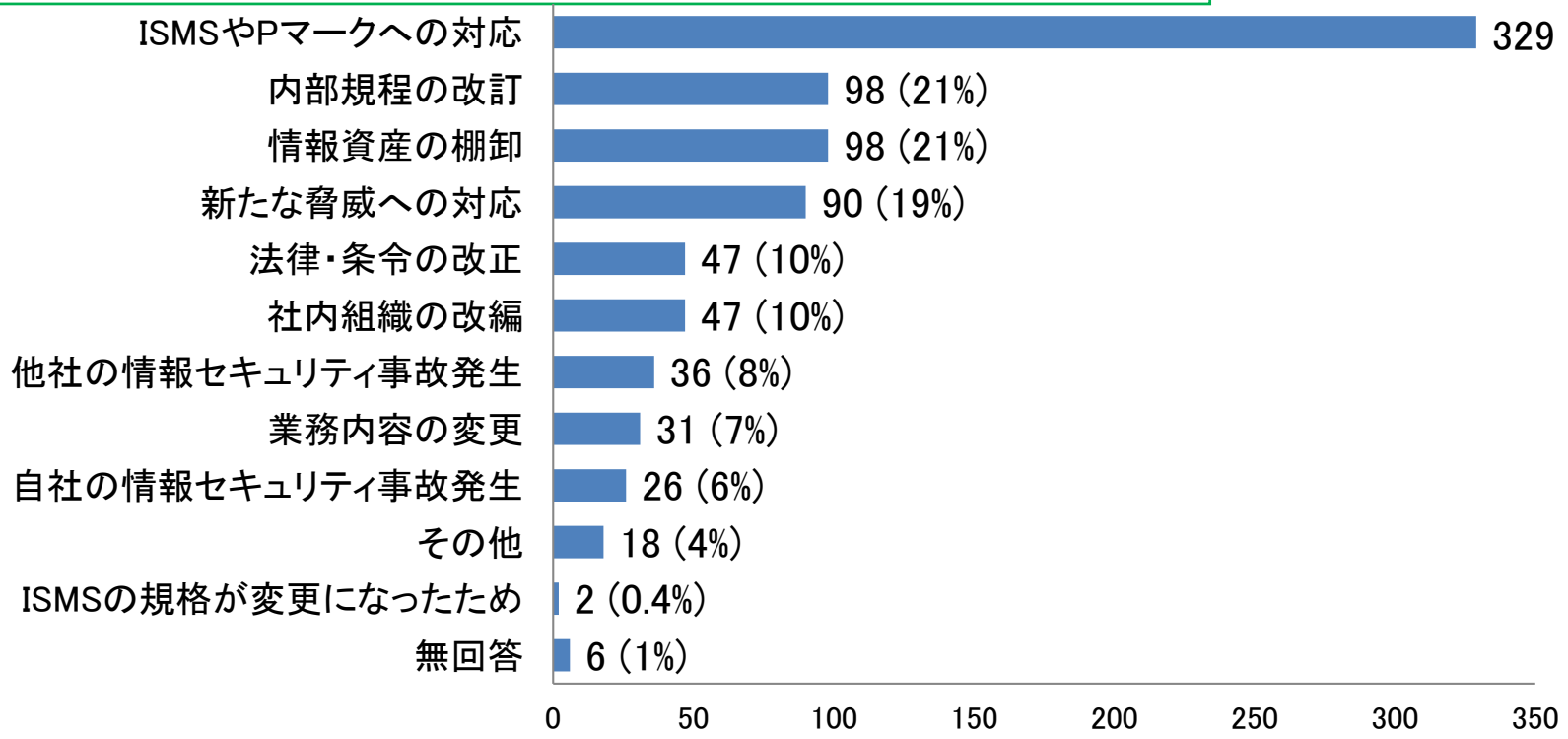
74%の組織が1年以内にリスク分析を実施している。
一方、14%の組織はリスク分析を実施していない。

第2章　情報セキュリティマネジメントの取り組み状況

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

設問10. リスク分析の実施理由（複数回答）（N=467）

※設問9で「**情報セキュリティリスク分析は実施してない**」以外を回答した組織を対象

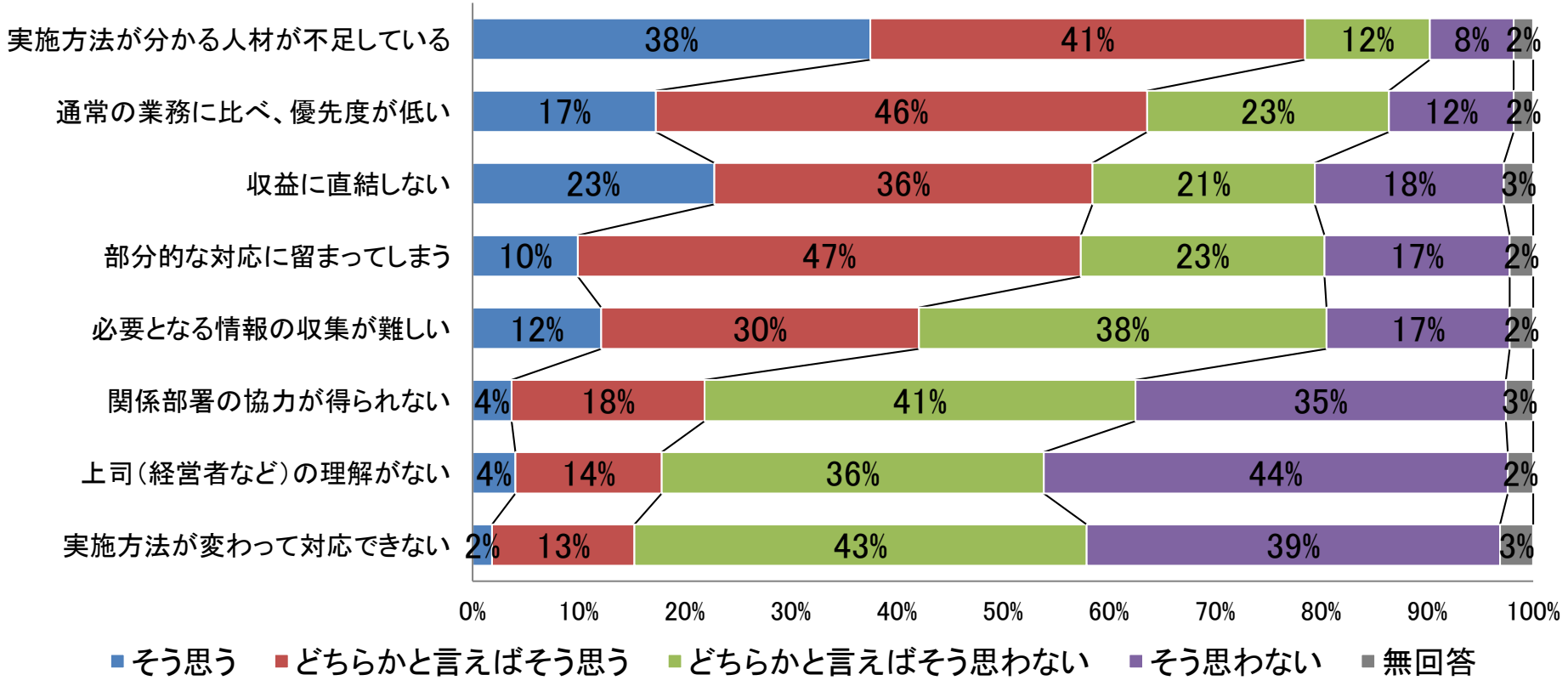


ISMSやPマークへの対応が329件（70%）、内部規程の改訂と情報資産の棚卸が98件（21%）、新たな脅威への対応が90件（19%）で続いている。

第2章　情報セキュリティマネジメントの取り組み状況

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

設問11. リスク分析を行う際の問題点（N=544）

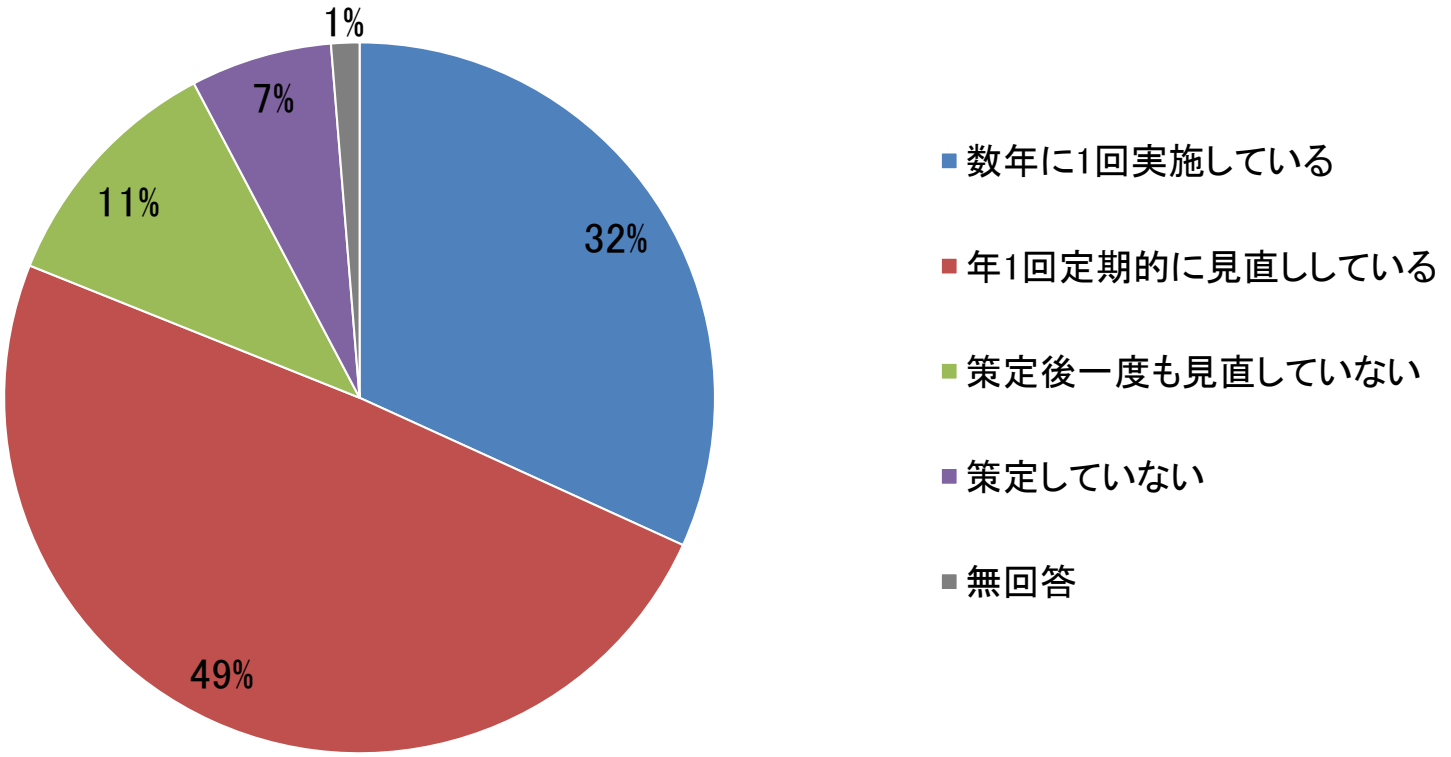


『そう思う』『どちらかといえばそう思う』の合計は、人材の不足（79%）、通常業務に比べ優先度が低い（63%）、収益に直結しない（59%）の順である。

第2章　情報セキュリティマネジメントの取り組み状況

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

設問12. 情報セキュリティポリシーの策定と見直し状況（N=544）

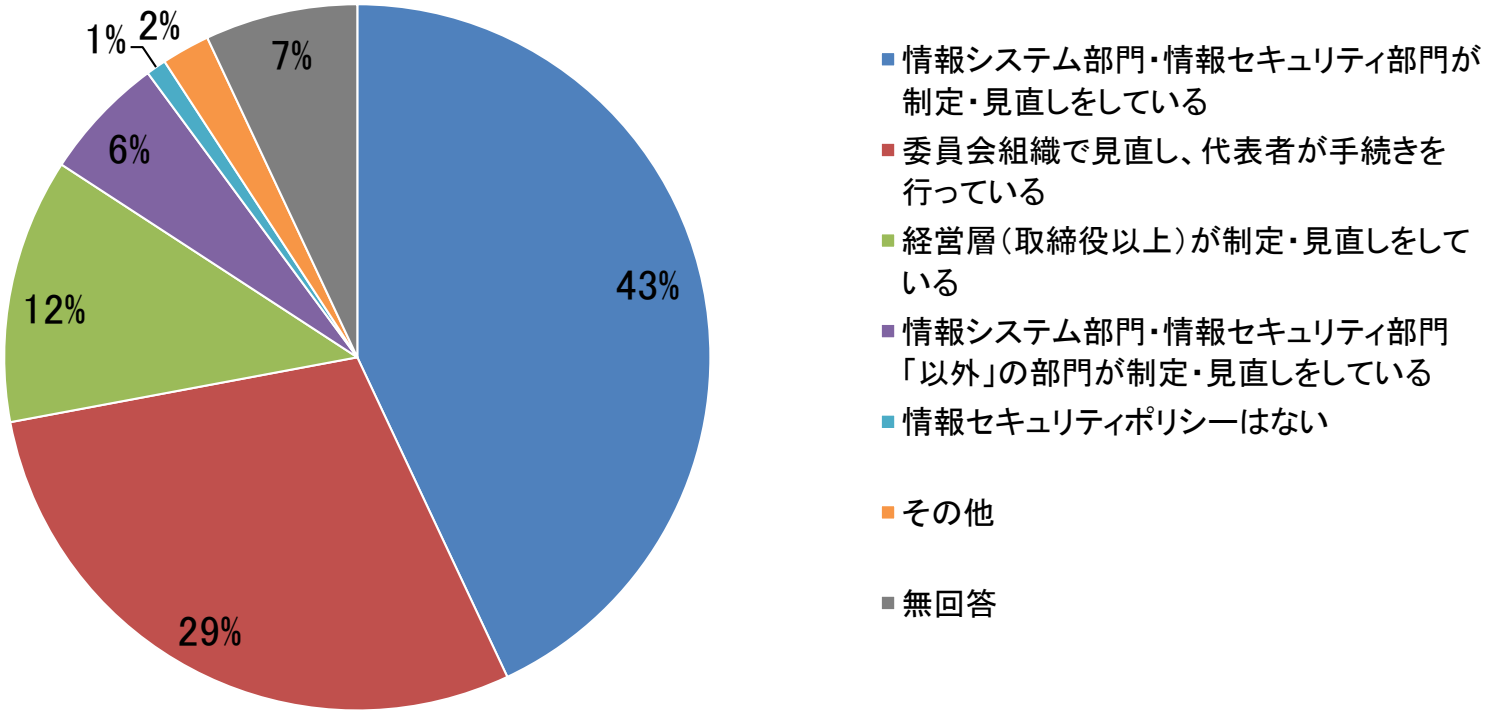


81%の組織が毎年ないし数年に一度見直しを実施している。
一方、11%が策定後見直しておらず、7%はポリシーを策定していない。

第2章　情報セキュリティマネジメントの取り組み状況

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

設問13. 情報セキュリティポリシーの策定・見直しを行う部門（N=544）



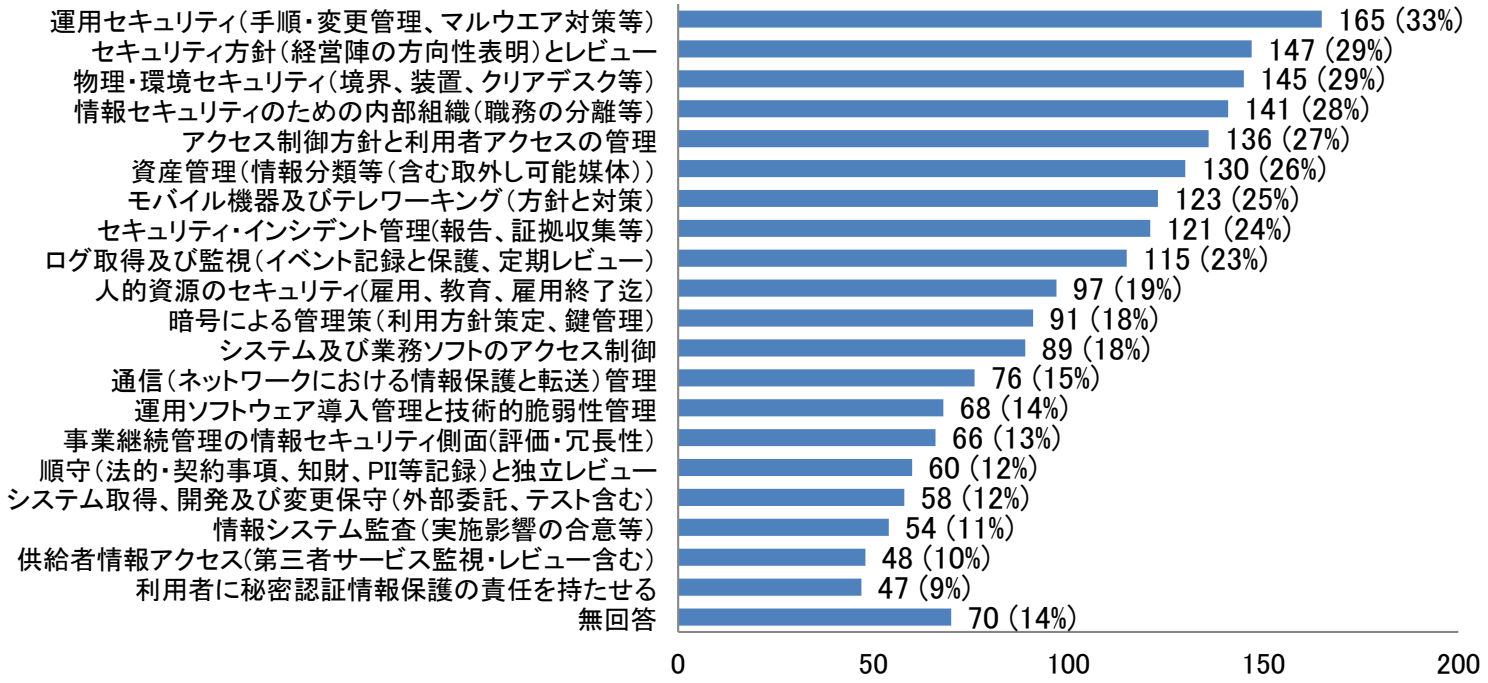
43%の組織で「情報システム部門・情報セキュリティ部門」が、29%の組織で「委員会組織」がポリシーの策定・見直しを実施している。

第2章　情報セキュリティマネジメントの取り組み状況

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

設問14. 過去3年間（2013年10月以降）で見直した管理策（複数回答）（N=501）

※設問 12、13で「**情報セキュリティポリシーはない**」以外を選択した組織を対象



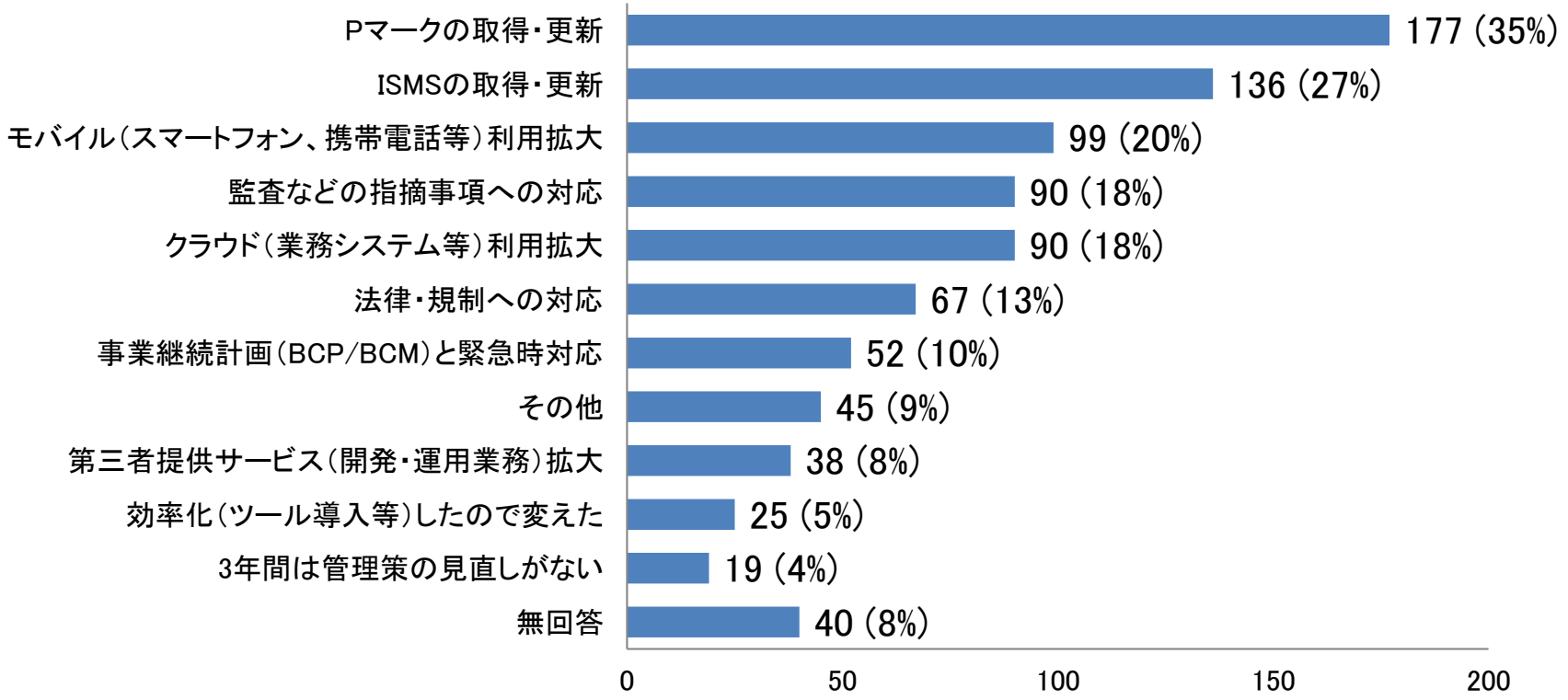
見直した管理策は、「運用セキュリティ」、「セキュリティ方針とレビュー」、「物理・環境セキュリティ」が多い。「情報セキュリティのための内部組織」、「アクセス制御・利用者アクセス管理」等も多い。

第2章　情報セキュリティマネジメントの取り組み状況

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

設問15. 管理策を新規導入・見直しした理由（複数回答）（N=501）

※設問 12、13で「**情報セキュリティポリシーはない**」以外を選択した組織を対象

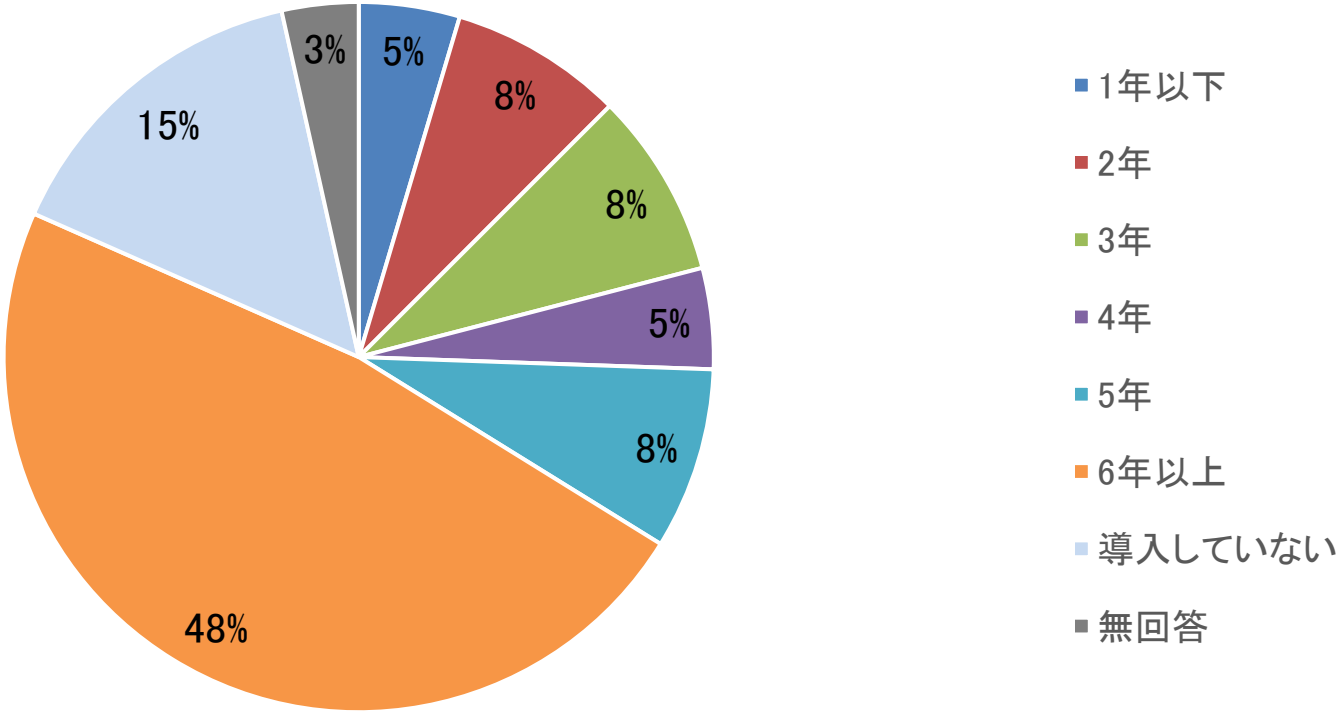


管理策の導入・見直し理由は、「Pマーク取得・更新」、「ISMSの取得・更新」、「モバイル（スマートフォン、携帯電話等）利用拡大」の順である。

第2章　情報セキュリティマネジメントの取り組み状況

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

設問16. 情報セキュリティマネジメント導入後の運用期間（N=544）

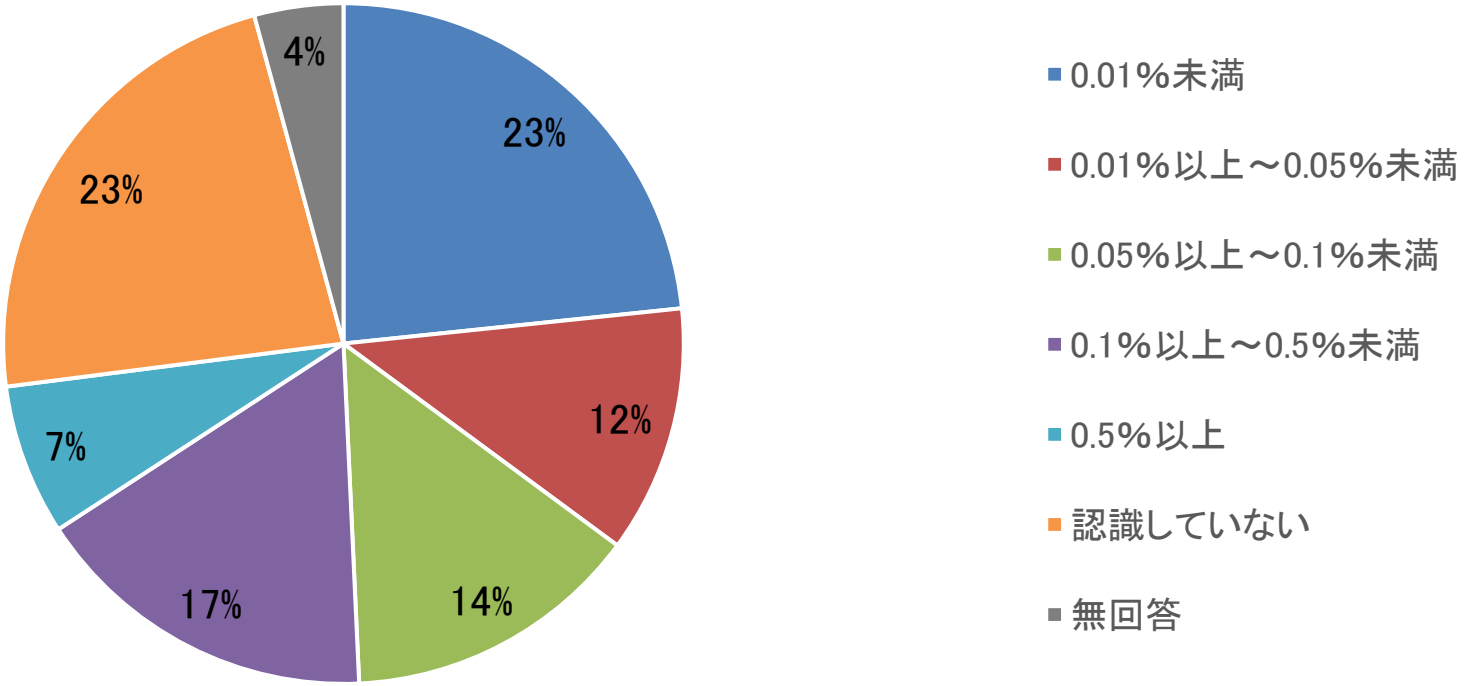


情報セキュリティマネジメントを導入後6年以上経過している組織が48%、5年以上の組織が56%を占めている。一方で導入していない組織も15%ある。

第2章　情報セキュリティマネジメントの取り組み状況

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

設問17-1. 売上（政府・自治体・大学等は予算）に対する情報セキュリティに関する支出の割合（前期実績）（N=544）

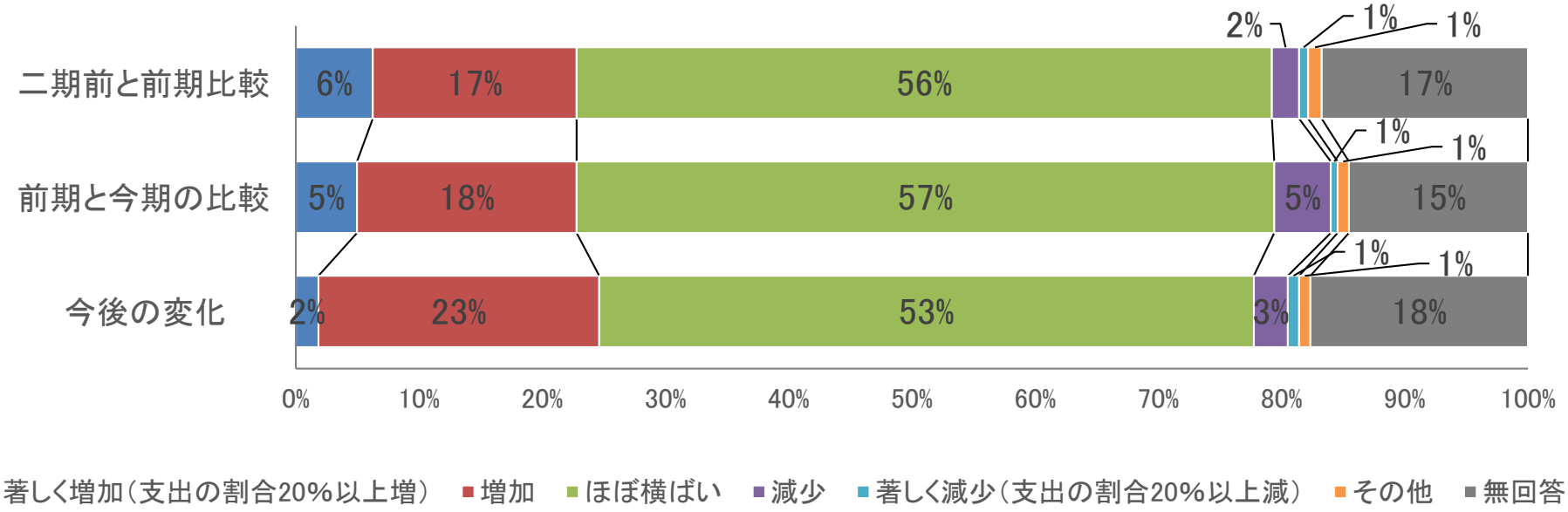


情報セキュリティに関する支出は売上・予算の0.1%未満の組織が49%だった。
最も多かったのは、0.01%未満の組織で23%だった。
また、「認識していない」組織も23%あった。

第2章　情報セキュリティマネジメントの取り組み状況

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

設問17-2. 売上（政府・自治体・大学等は予算）に対する情報セキュリティに関する支出の傾向（N=544）



「二期前と前期比較」、「前期と今期の比較」、「今後の変化」のいずれも「ほぼ横ばい」が50%を占めた。
「今後の変化」では、他と比べて「著しく増加」と「増加」の合計が大きい。

考察（第2章　情報セキュリティマネジメントの取り組み状況）(1/2)

＜リスク分析＞

- 74%の組織が1年以内にリスク分析を実施し、定着傾向にある。
- 認証審査への対応がきっかけである状況（70%）は変わらない。
- 問題点は、「実施方法が分かる人材の不足」（79%）が最も多い。

＜情報セキュリティポリシーの策定と見直し＞

- 毎年ないし数年に一度、セキュリティポリシーの見直しを実施する組織（81%）が最も多い。見直しは情報システム部門・情報セキュリティ部門(43%)、次いで委員会組織(29%)が担当している。
- 見直した管理策項目は「運用セキュリティ（含むマルウエア対策等）」（33%）など具体的・技術的な項目が多くなった。見直し理由は、「PマークやISMSの取得・更新」といった認証対応が多い。

考察（第2章　情報セキュリティマネジメントの取り組み状況）(2/2)

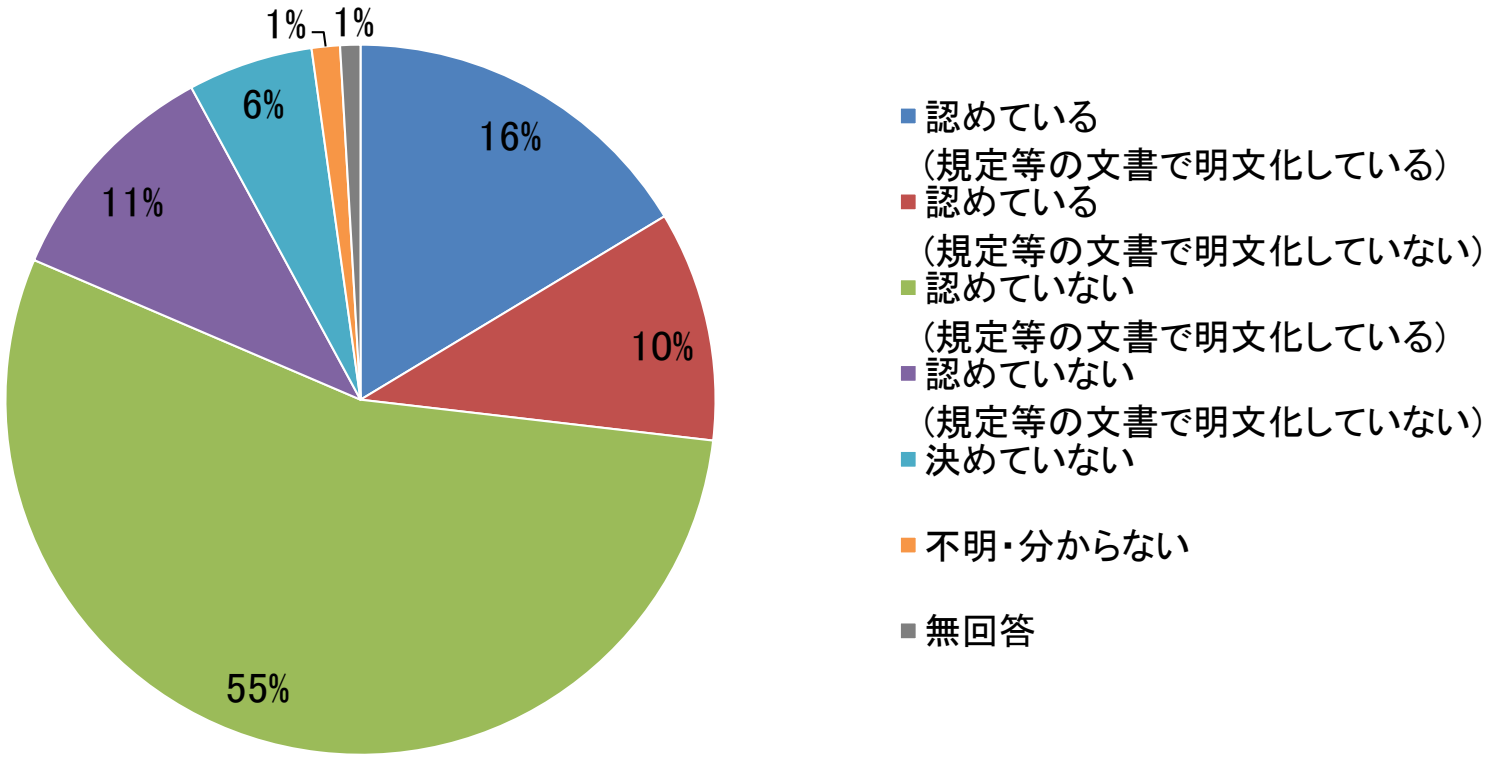
＜情報セキュリティに関する支出＞

- 情報セキュリティに関する支出の割合は、売上・予算の0.1%未満の組織（49%）が多い。一方で、認識していない組織（23%）も多い。
- 情報セキュリティに関する支出の傾向は、「二期前と前期比較」、「前期と今期の比較」、「今後の変化」のいずれも「ほぼ横ばい」が50%を占めていた。
- 「今後の変化」では、「二期前と前期比較」、「前期と今期の比較」と比べて、「著しく増加」と「増加」の合計が23%から25%に増加していた。

第3章
IT資産の管理・運用体制

第3章　IT資産の管理・運用体制

設問18. 従業員の私有IT資産の業務利用（BYOD）の許可状況（N=544）

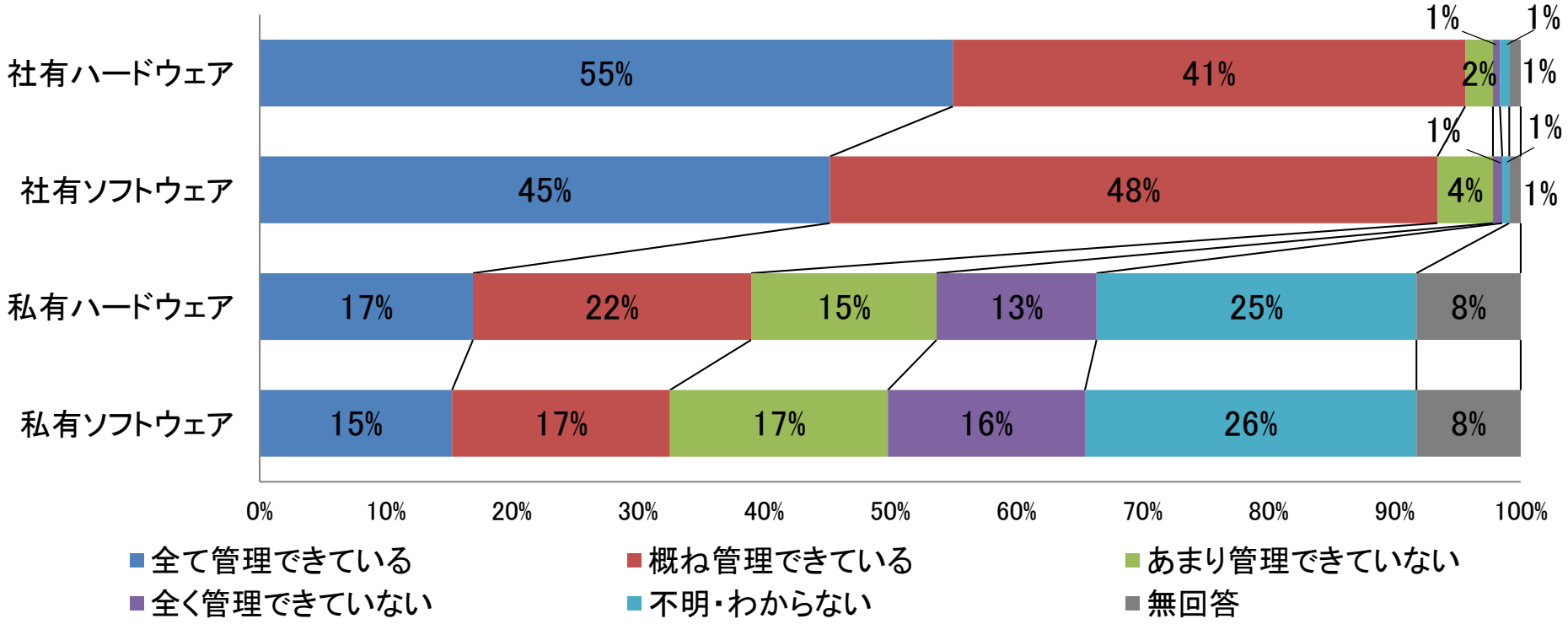


従業員の私有IT資産の業務利用(BYOD)は26%の組織が認めているが、66%の組織で認めていなかった。

第3章　IT資産の管理・運用体制

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

設問19. 業務利用するIT資産の管理状況（N=544）

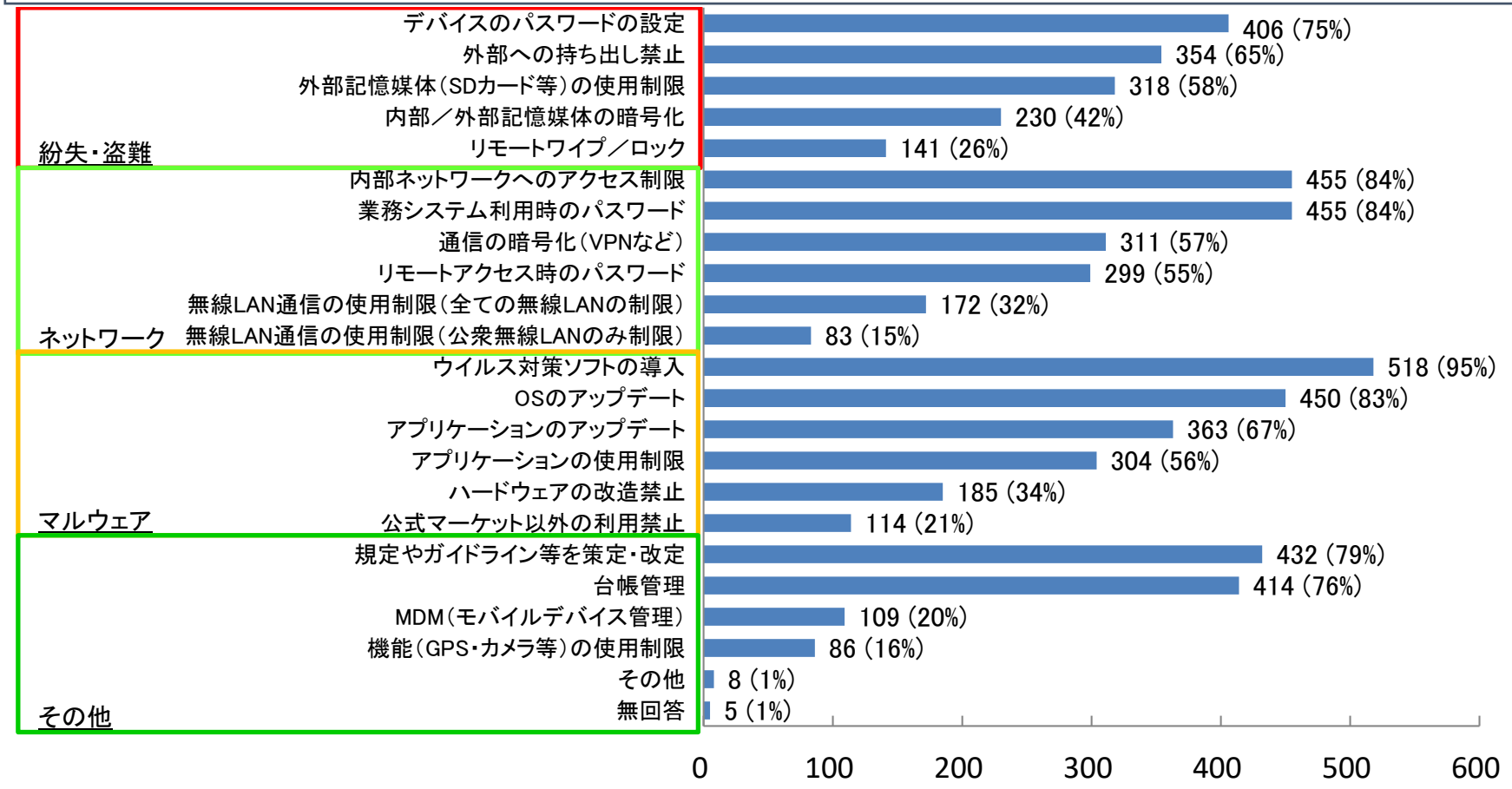


社有IT資産は、90%以上の組織で管理できている
（『全て管理できている』『概ね管理できている』の合計）という認識である。
一方、私有IT資産を管理できている組織は、40%未満にとどまっている。

第3章　IT資産の管理・運用体制

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

設問20. 業務で利用しているIT資産のセキュリティ対策状況（複数回答）（N=544）

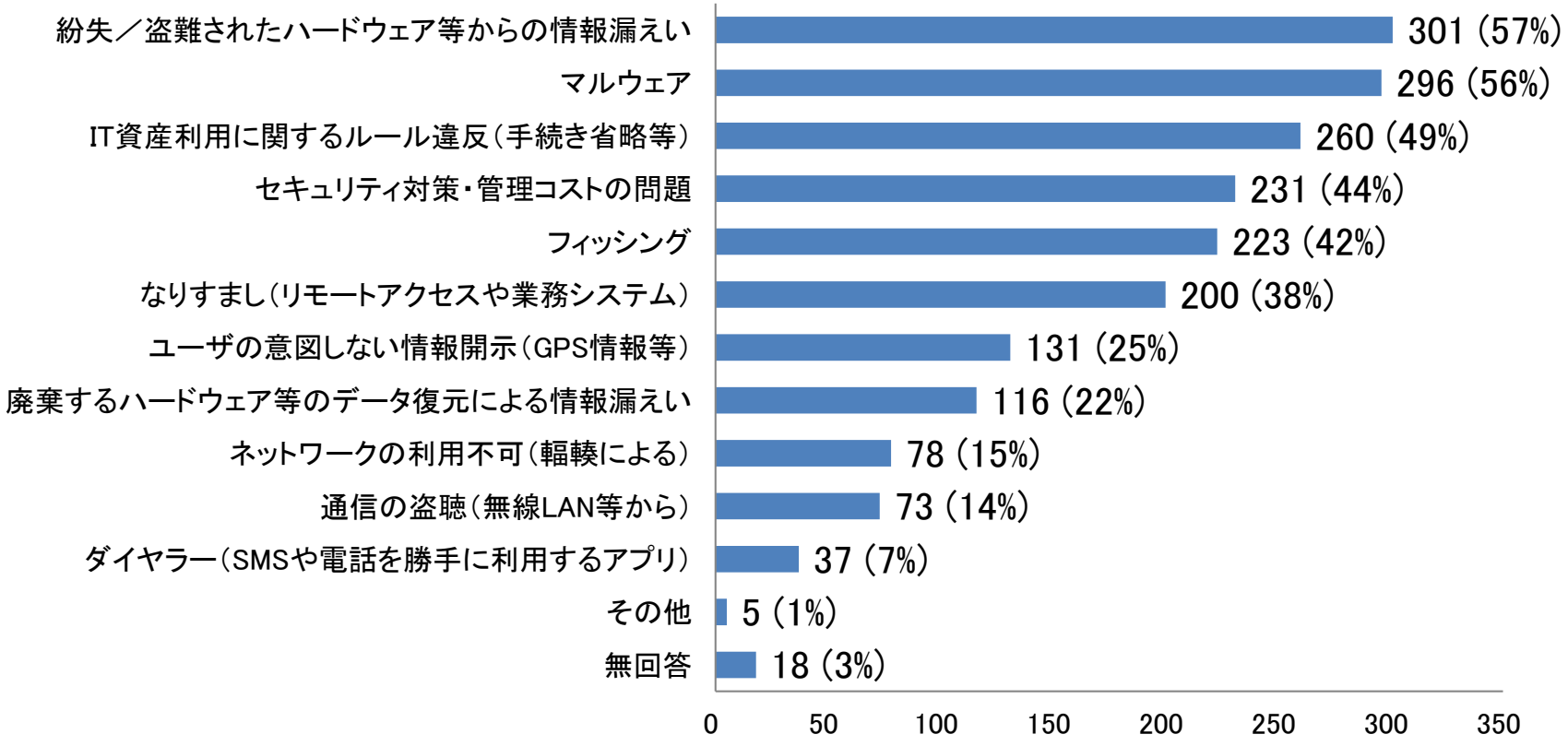


IT資産のセキュリティ対策は「ウイルス対策ソフトの導入」(95%)が最も多い。

第3章　IT資産の管理・運用体制

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

設問21. IT資産管理・運用に関するセキュリティ課題・懸念（複数回答）（N=544）

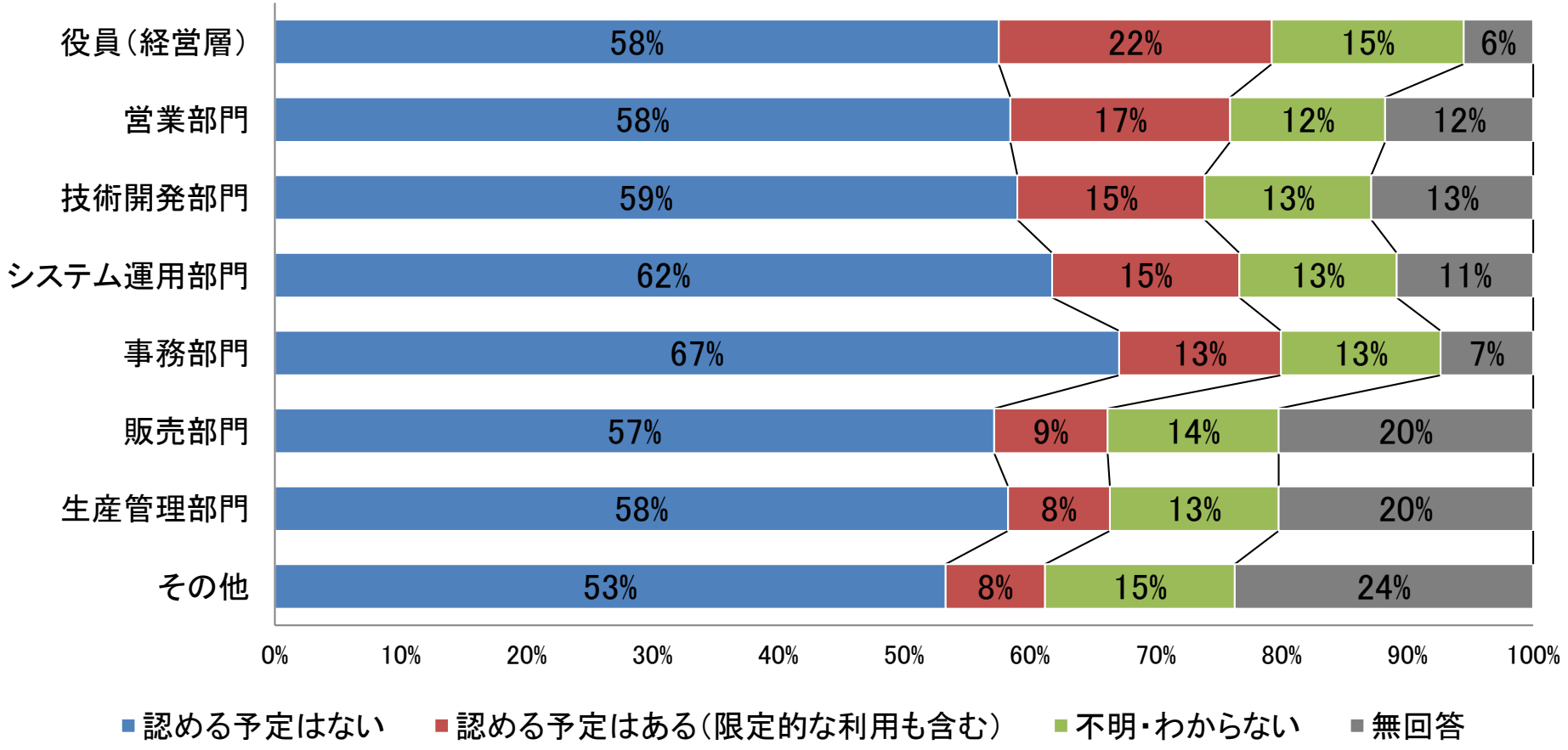


50%以上の組織が、「紛失／盗難による情報漏えい」や「マルウェア感染」に対してセキュリティ課題の意識を持っている。

第3章　IT資産の管理・運用体制

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

設問22. 将来的な私有IT資産の業務利用（BYOD）の方針（N=544）



50%以上の組織で、いずれの部門でも私有IT資産の業務利用予定はない。

考察(第3章　IT資産の管理・運用体制)

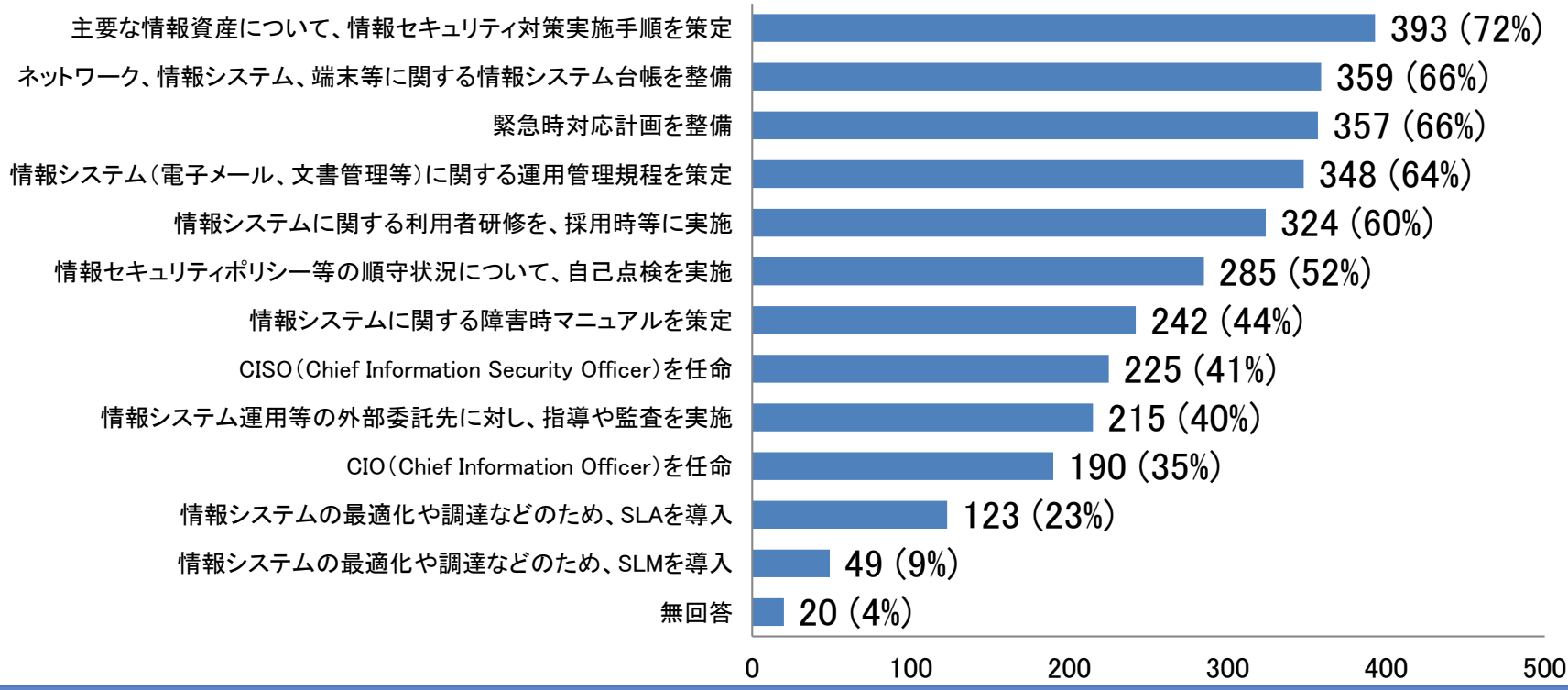
- 従業員の私有IT資産の業務利用(BYOD)を認める組織は、26%にとどまっており、66%の組織では認めていない。
- 2012年調査[1]では私有IT資産の業務利用(BYOD)を認める組織が約35%あり、以前よりも認めない方針が強まっている。
- 将来的に私有IT資産の業務利用(BYOD)を認める方針の組織も20%前後にとどまっている。
- 「紛失／盗難による情報漏えい」や「マルウェア感染」に対して、50%以上の組織がセキュリティ課題の意識を持っている。
- 「紛失／盗難」「ネットワーク」「マルウェア」「その他」でそれぞれ対策が取られている。しかし、「リモートワイプ／ロック」や「無線LANの制限」などを実施している組織は30%程度にとどまっている。

[1] 2012年情報セキュリティ調査 http://lab.iisec.ac.jp/~harada_lab/survey/2012.html

第4章
情報セキュリティ対策

第4章　情報セキュリティ対策

設問23. 情報セキュリティ対策の実施状況（複数回答）（N=544）

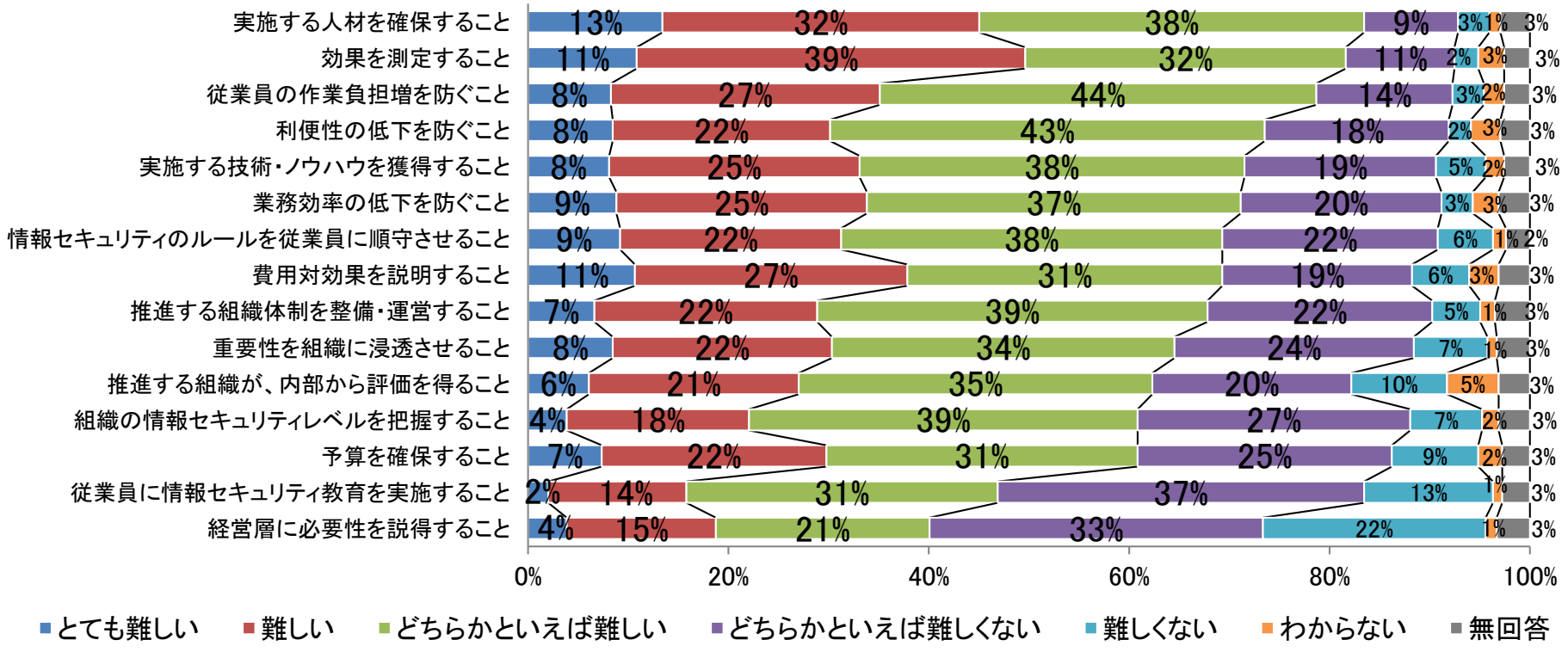


60%以上の組織が「実施手順を策定」「情報システム台帳を整備」
「緊急時対応計画を整備」「運用管理規程を策定」
「利用者研修」を実施している。

第4章　情報セキュリティ対策

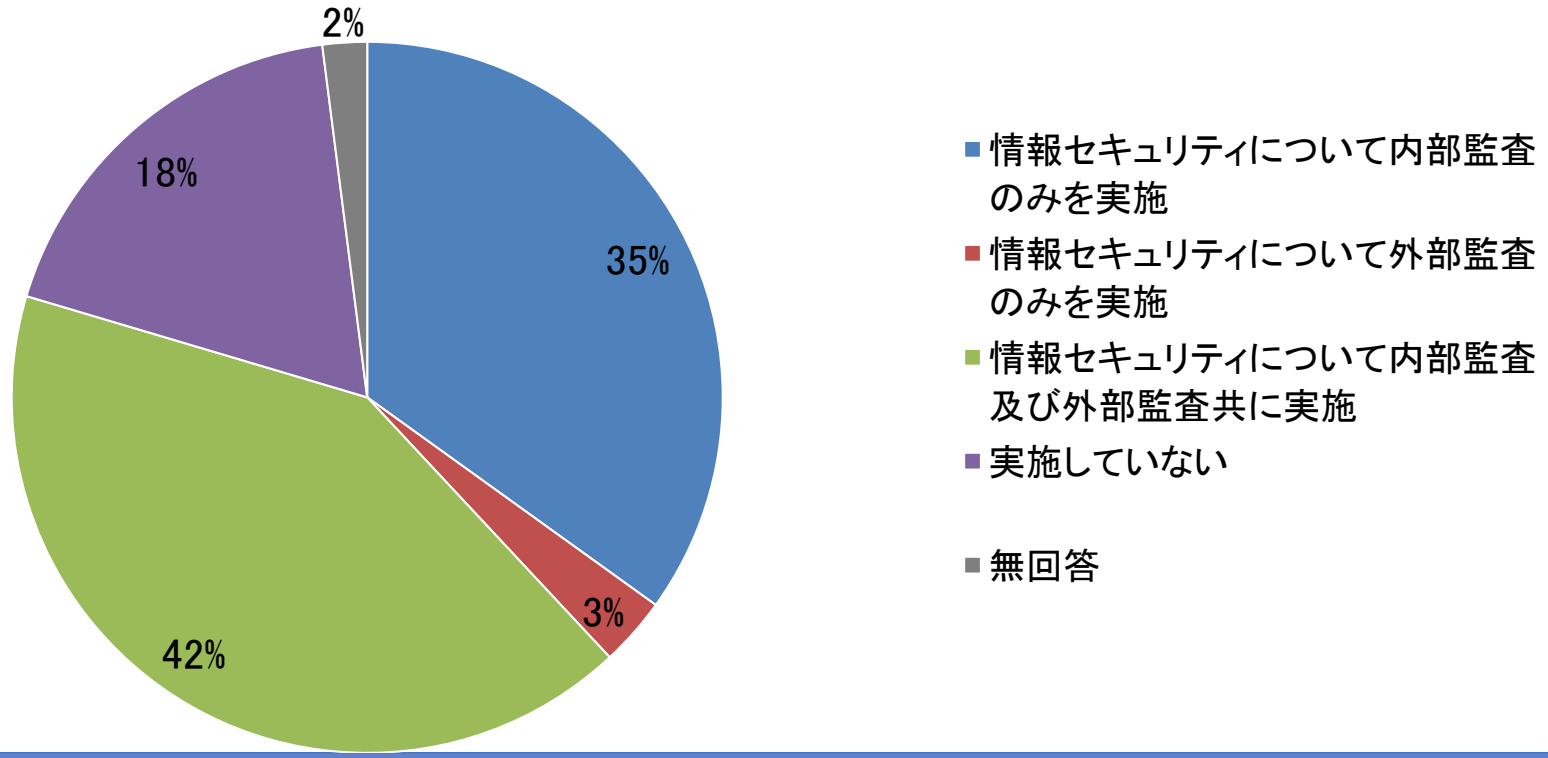
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

設問24. 情報セキュリティ対策を実施する上での難しさ（N=544）



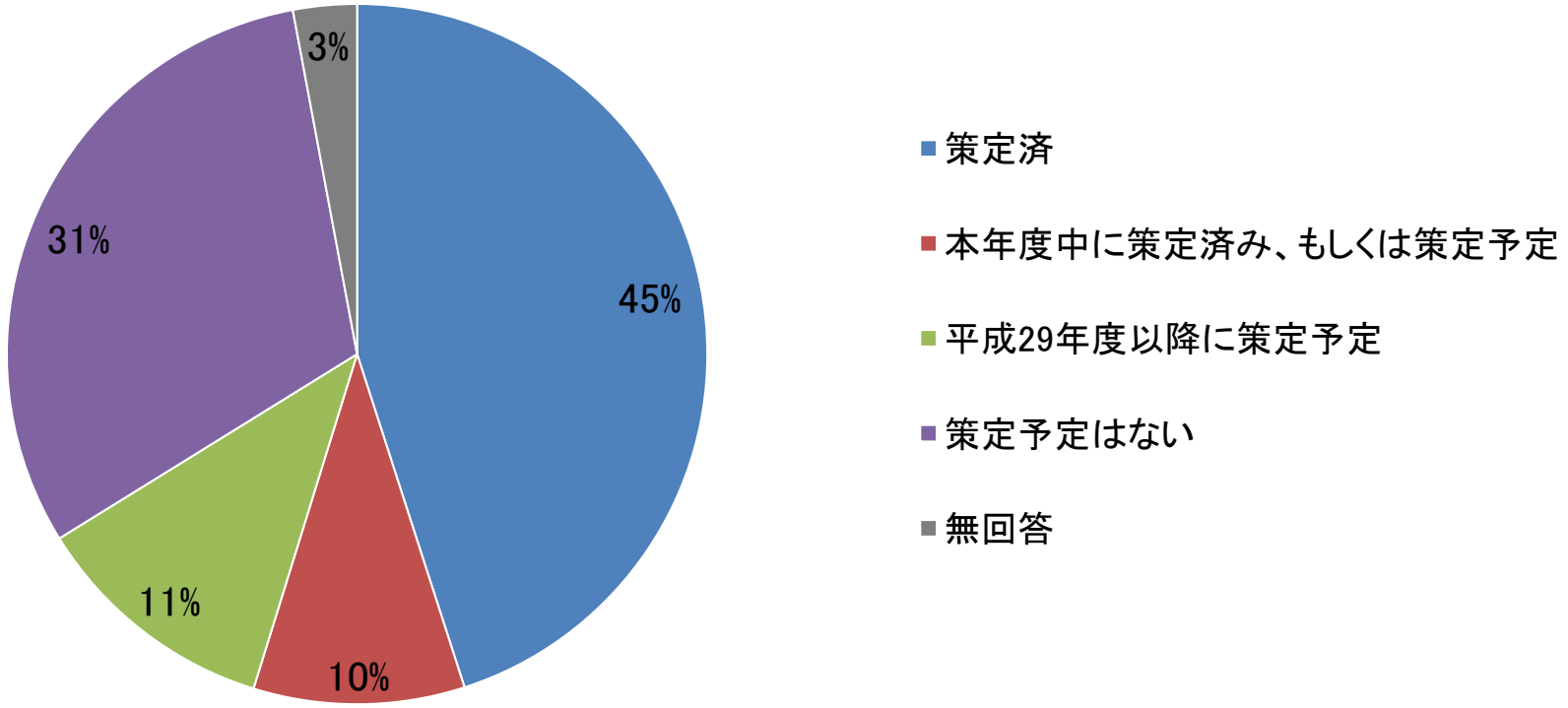
『難しい』の回答（『とても難しい』～『どちらかといえば難しい』の合計）は、「人材を確保すること」や「効果を測定すること」で80%を超えている。
一方、「経営層に必要性を説得すること」では40%であった。

設問25. 情報セキュリティ監査（審査を含む）の実施状況（過去1年間）(N=544)



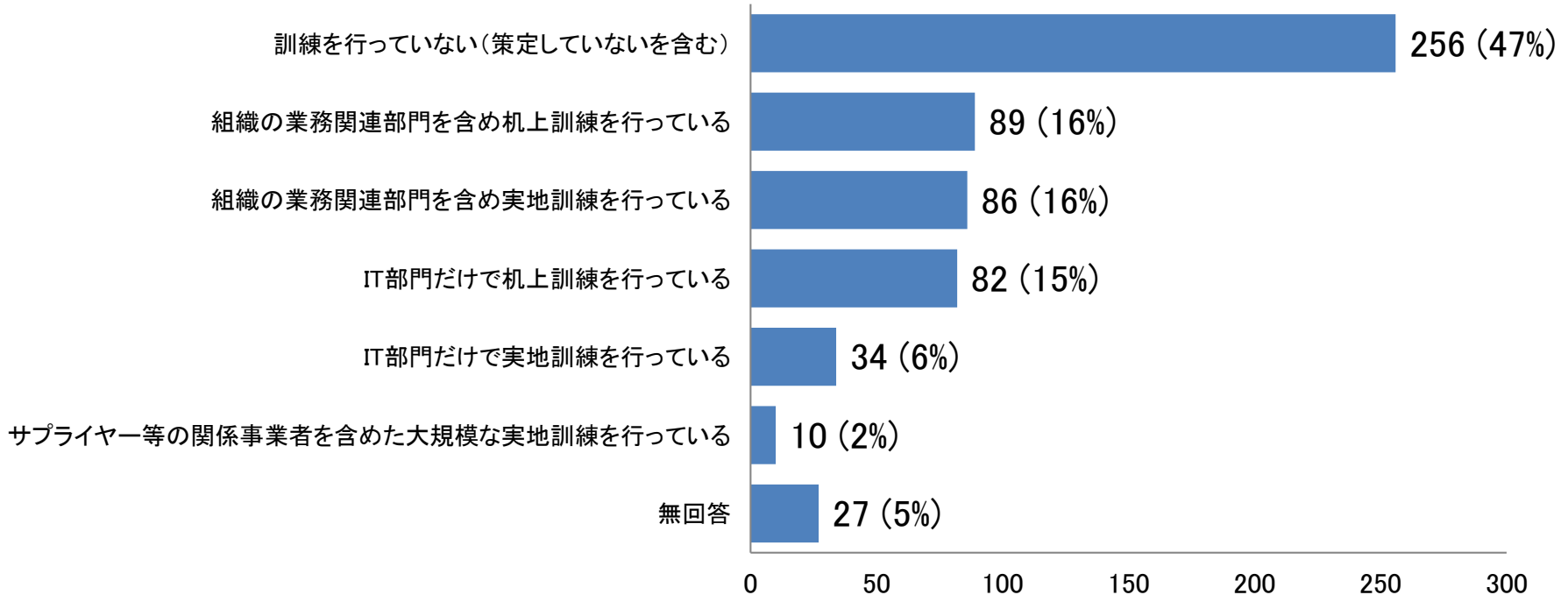
過去1年間に80%の組織が監査を実施しており、
42%の組織が内部監査及び外部監査共に実施している。
一方、18%の組織は監査を実施していない。

設問26-1. 事業継続計画（BCP）の策定状況(N=544)



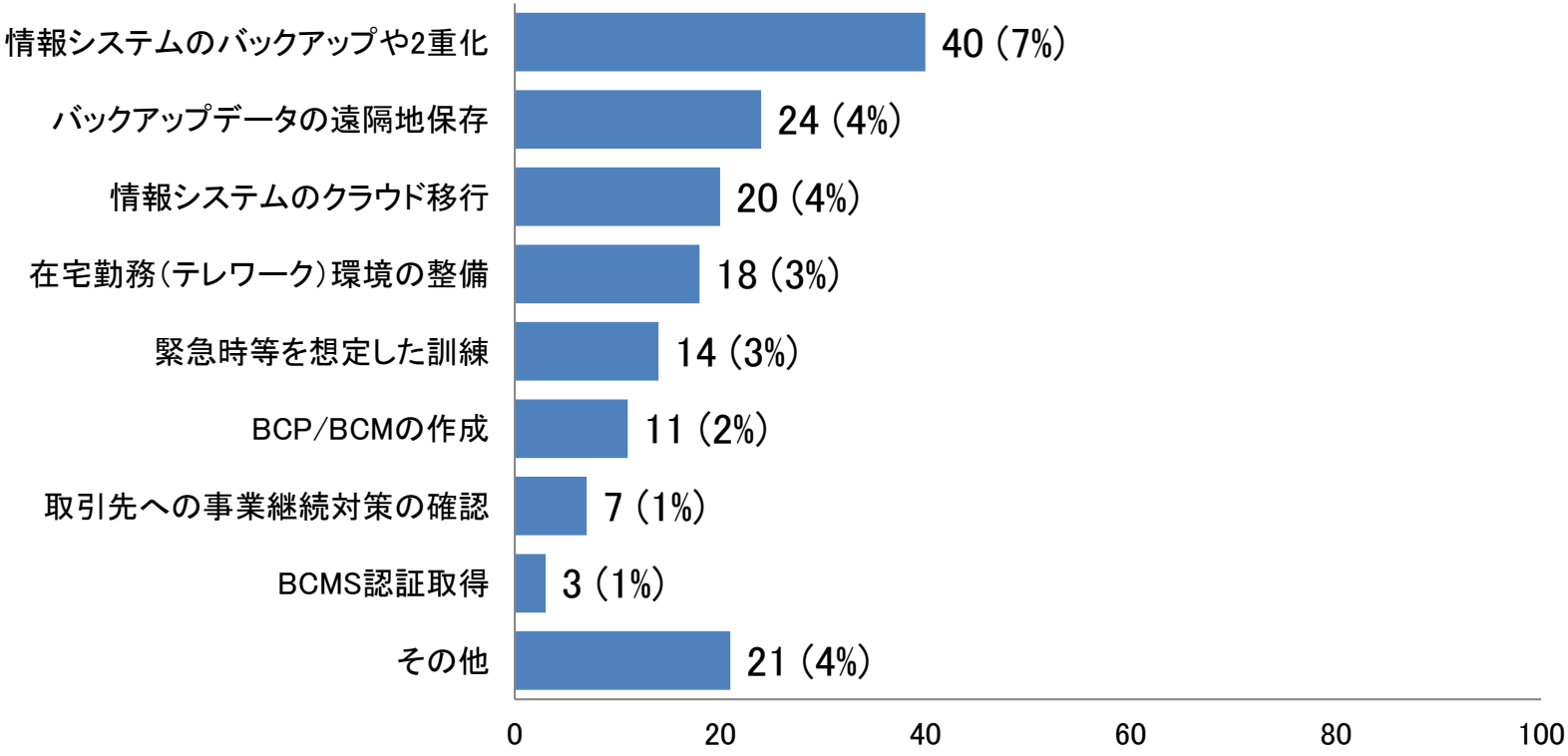
「策定済」の組織が45%で、「策定予定」の組織と合わせると66%となる。
一方、「策定予定はない」組織は31%であった。

設問26-2. 事業継続訓練の実施状況（複数回答）(N=544)



「訓練を行っていない（策定していないを含む）」組織は47%であった。
「業務関連部門を含めた訓練（実地・机上）」「IT部門だけの訓練（実地・机上）」を実施している組織は15%程度にとどまった。

設問27. 過去に実施した後、止めた事業継続の取り組み（複数回答）(N=544)



事業継続に関する取り組みで止めたものは、最も多いものでも「情報システムのバックアップや2重化」の7%であった

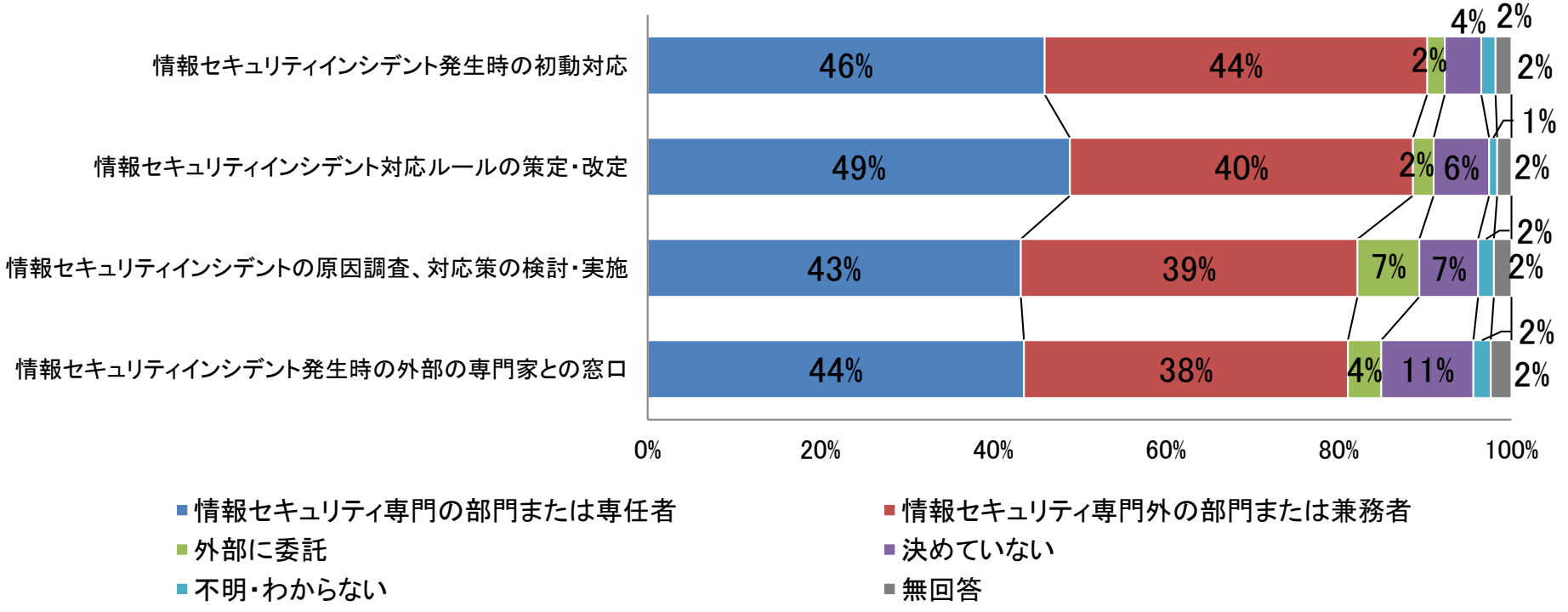
考察（第4章　情報セキュリティ対策）

- 情報セキュリティ対策の実施状況では、実施手順書や計画等の規程類の整備は進んでいる。
- 情報セキュリティ監査は80%が実施しており、45%は外部監査を活用していた。
- 情報セキュリティ対策を推進する上では、「効果の測定」や「人材の確保」が難しいと回答した組織が多かった。一方で、「経営層への説得」や「情報セキュリティ教育の実施」については、比較的難しくないと回答した組織が多かった。
- 事業継続計画は45%が策定済みであったが、策定の予定なしが31%あった。
- 事業継続訓練は、47%で実施していなかった。
- 事業継続に関する取り組みで止めたものは、最も多いものでも「情報システムのバックアップや2重化」の7%だった。

第5章
情報セキュリティインシデント対応の体制と人材育成

第5章　情報セキュリティインシデント対応の体制と人材育成

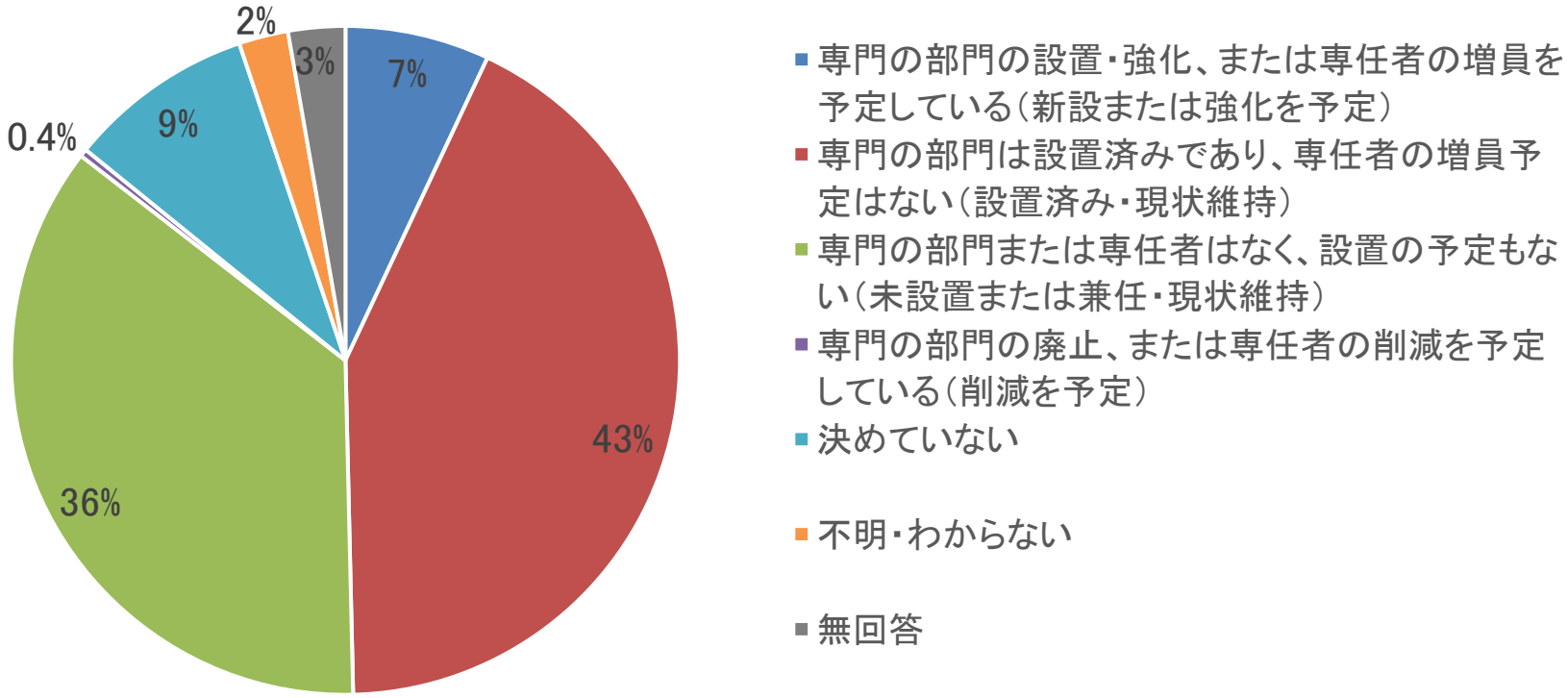
設問28. 情報セキュリティインシデントに関わる業務の担当（N=544）



80%以上の組織で業務の担当を決定している。
「原因調査、対応策の検討・実施」は外部委託の割合が他業務より大きい。
「外部の専門家との窓口」を決めていない組織が11%ある。

第5章　情報セキュリティインシデント対応の体制と人材育成

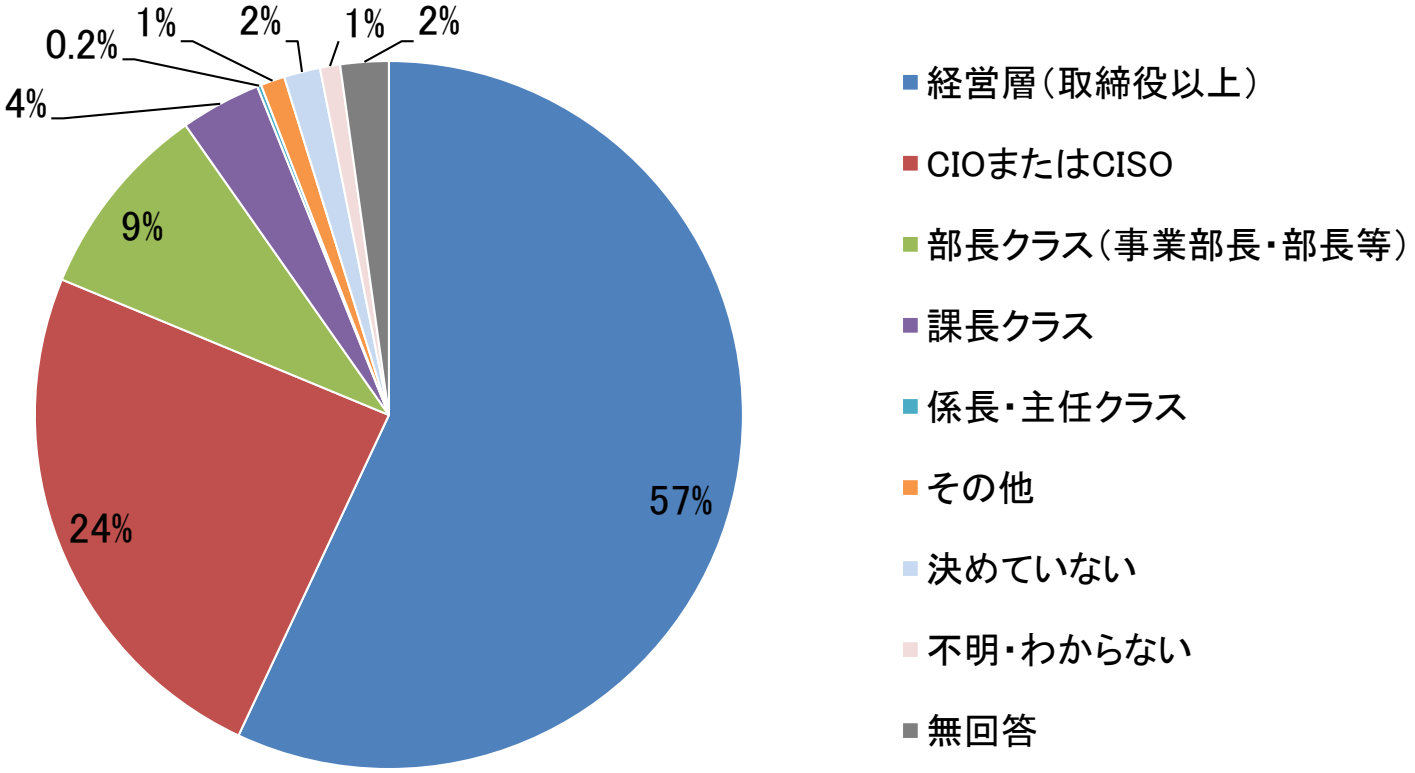
設問29. 情報セキュリティインシデント対応の担当部門・専任者の設置（N=544）



現状維持の組織が79%を占めている。
強化を予定している組織は7%で、方針を決めていない組織が9%ある。

第5章　情報セキュリティインシデント対応の体制と人材育成

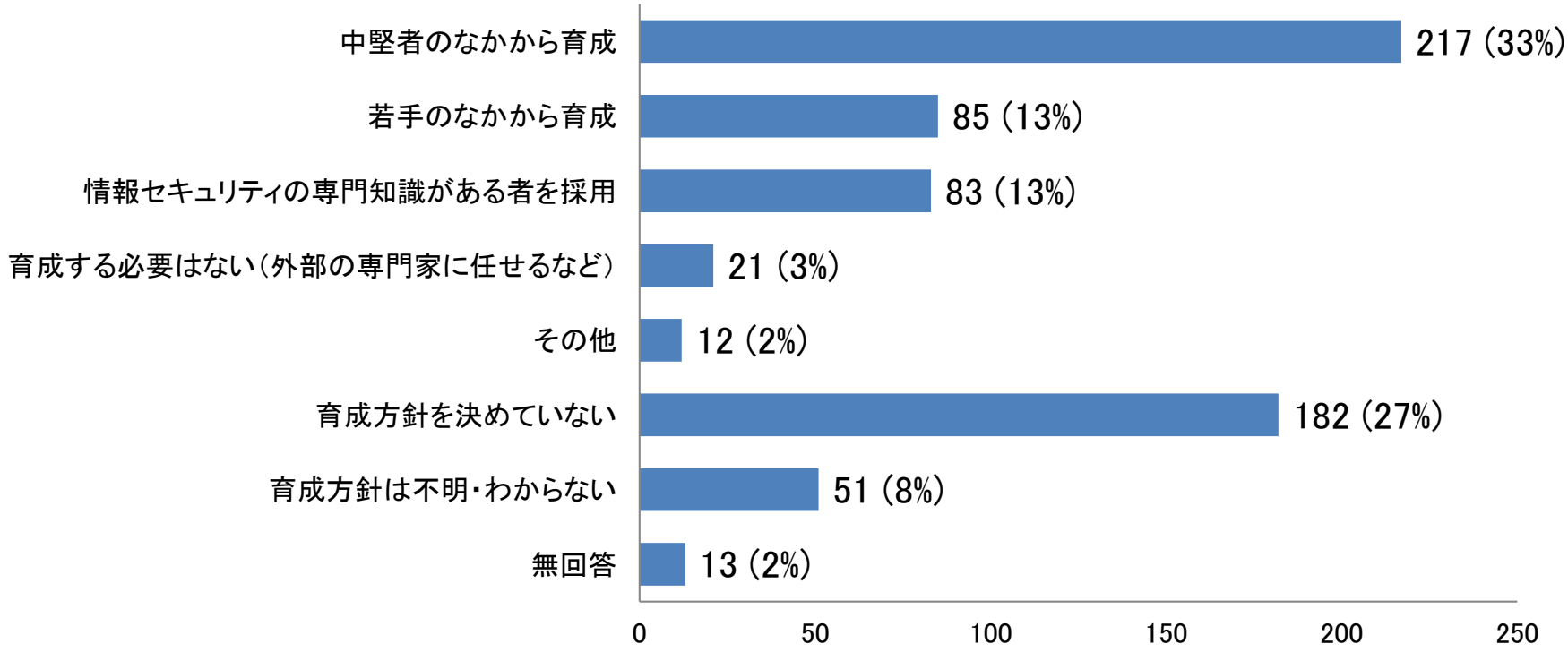
設問30. 情報セキュリティインシデント対応の最終的な指示・決定者（N=544）



インシデント対応の最終的な指示・決定には組織の上層部が関与している。

第5章　情報セキュリティインシデント対応の体制と人材育成

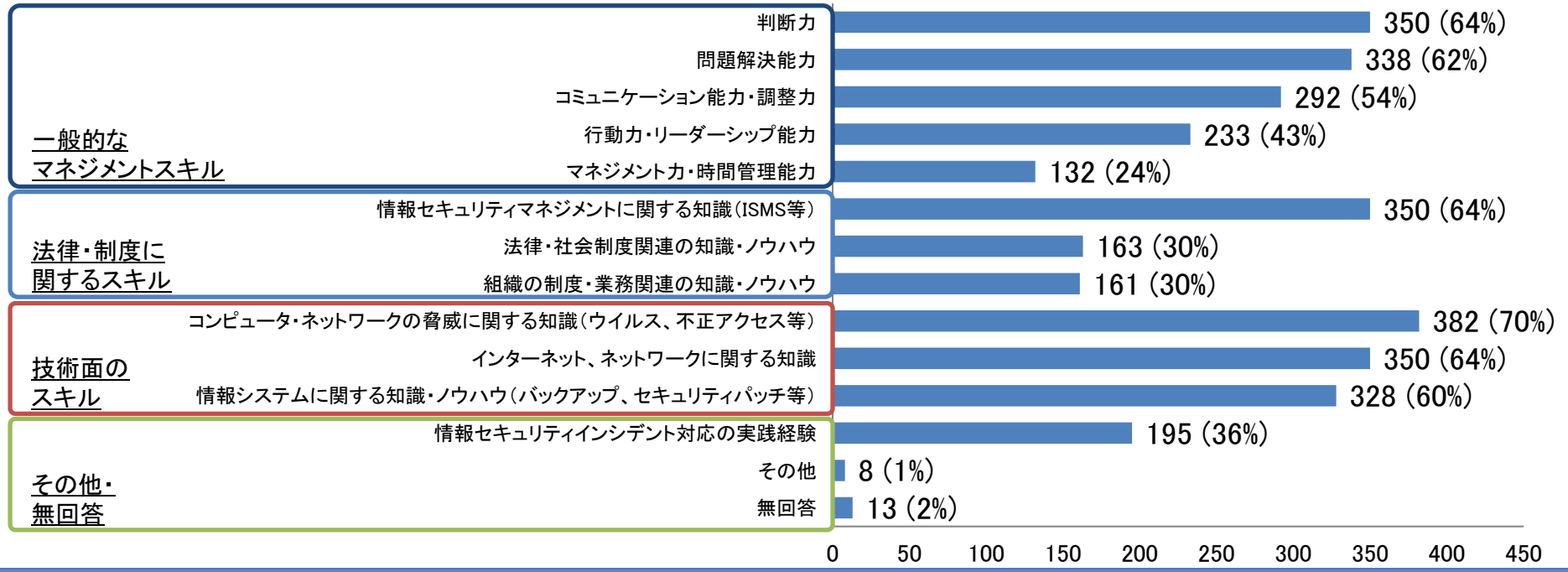
設問31. 情報セキュリティインシデント対応の専任者の育成方針（複数回答）
（N=544）



多くの組織が自組織で専任者を育成・採用する方針である。
育成方針を決めていない組織が27%ある。

第5章　情報セキュリティインシデント対応の体制と人材育成

設問32. 情報セキュリティインシデント対応の専任者に求めるスキル（複数回答）
（N=544）



技術面のスキルに対する要求は総じて高く、
法律・制度に関するスキルに対する要求はあまり高くない。
一般的なマネジメントスキルに対する要求も高いが項目により差がある。

考察（第5章　情報セキュリティインシデント対応の体制と人材育成）

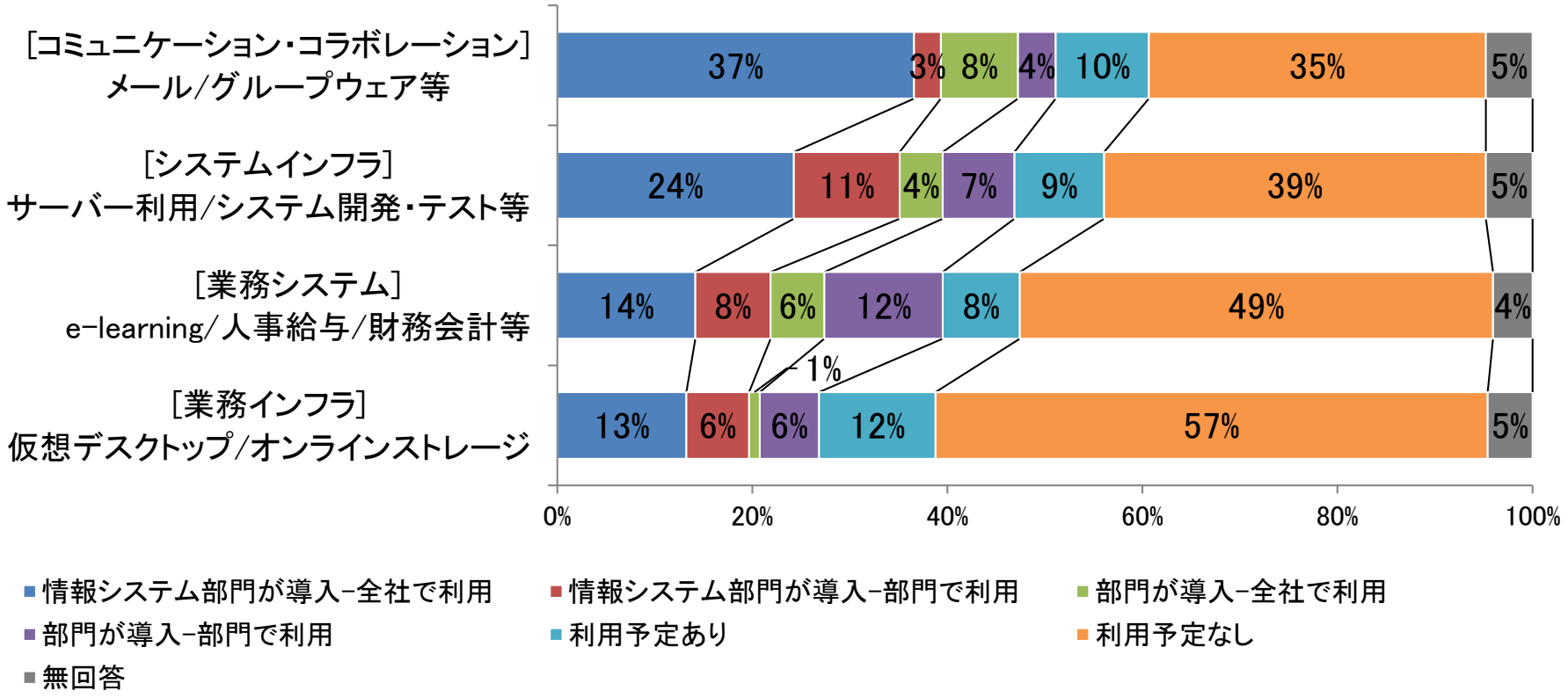
- インシデント対応において必要とされる「外部の専門家との窓口」について、未決定の組織が11%あり、他のインシデント対応に関する業務と比べ割合が高くなっている。「原因調査、対策の検討・実施」は外部委託の割合が他業務より大きい。
- インシデント対応の専任者の育成は、自組織で育成・採用する組織と育成方針を決めていない組織に二極化している。自組織での育成方針は、中堅者を育成、若手を育成、採用等外部から受け入れの順となっている。
- インシデント対応の担当者に対しては、技術面のスキルの要求が高く、法律・制度に関するスキルの要求は低い。一般的なマネジメントスキルのうち、コミュニケーション能力・調整力、行動力・リーダーシップの要求は低い傾向にある。
- インシデント対応における最終的な指示・決定には組織の上層部が関与している。特に「経営層」が多く、6割近くを占めている。

第6章
クラウドサービスの利用状況と阻害要因

第6章　クラウドサービスの利用状況と阻害要因

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

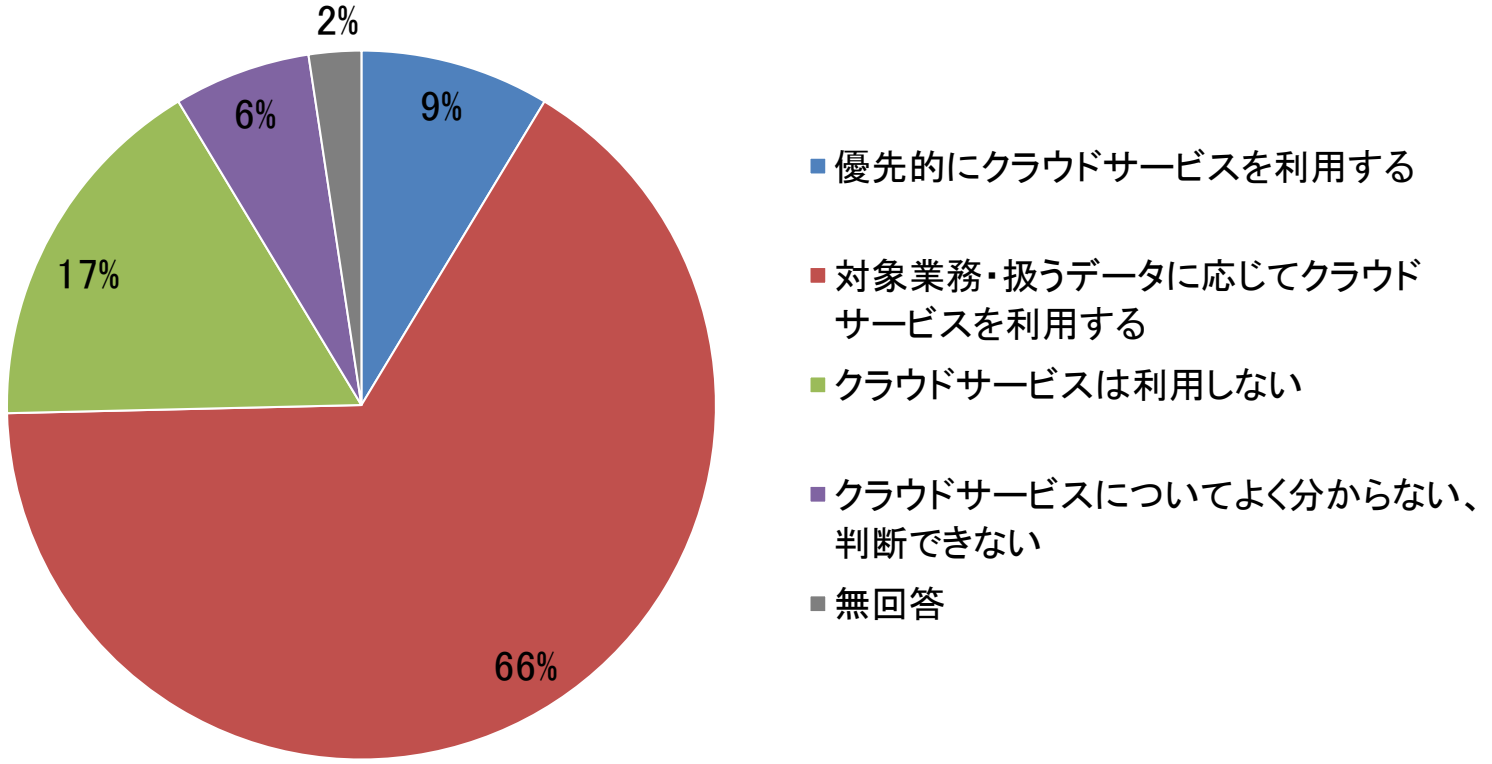
設問33. クラウドサービスの利用状況（N=544）



コミュニケーション・コラボレーションサービスの利用率は52%と最も高い。一方、「利用予定なし」は業務インフラ（57%）、業務システム（49%）で高い。

第6章　クラウドサービスの利用状況と阻害要因

設問34. クラウドサービスに対する組織の方針（N=544）

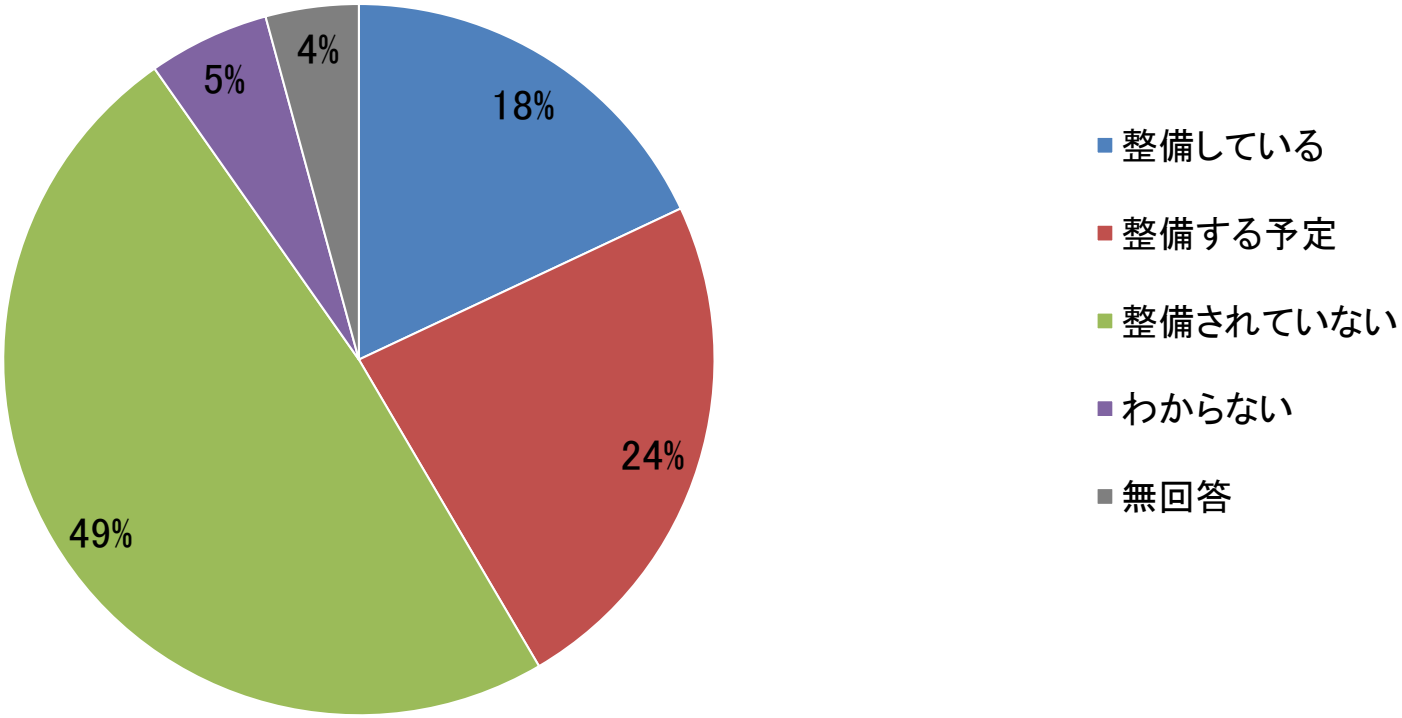


9%の組織が優先的にクラウドサービスを利用する方針であり、
66%の組織は対象業務・扱うデータに応じて利用する方針である。

第6章　クラウドサービスの利用状況と阻害要因

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

設問35. クラウドサービス利用における規定やガイドラインの整備状況（N=544）

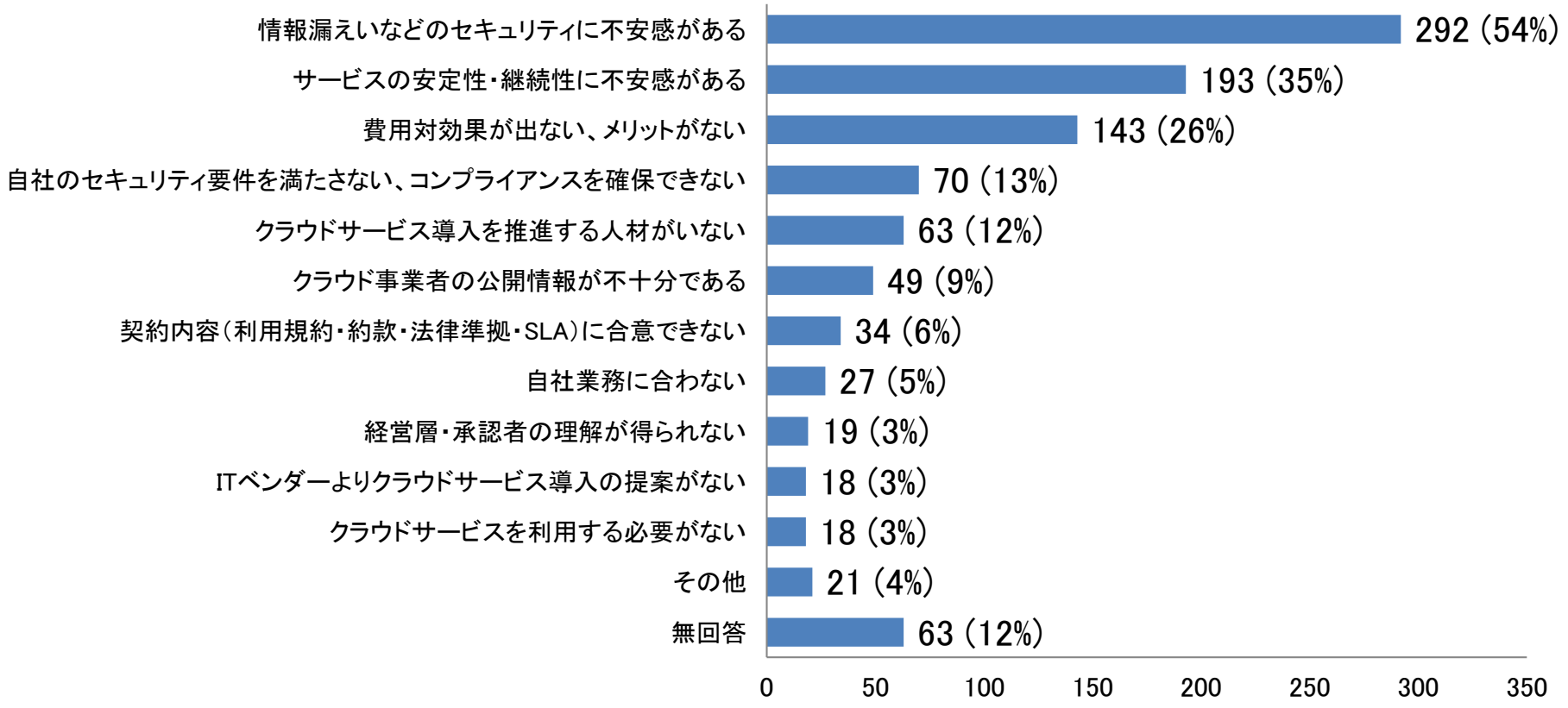


42%の組織が規定やガイドラインを整備済み、整備予定となっている。
一方、半数の組織では整備されていない。

第6章　クラウドサービスの利用状況と阻害要因

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

設問36. クラウドサービス利用の阻害要因および懸念事項（複数回答）（N=544）

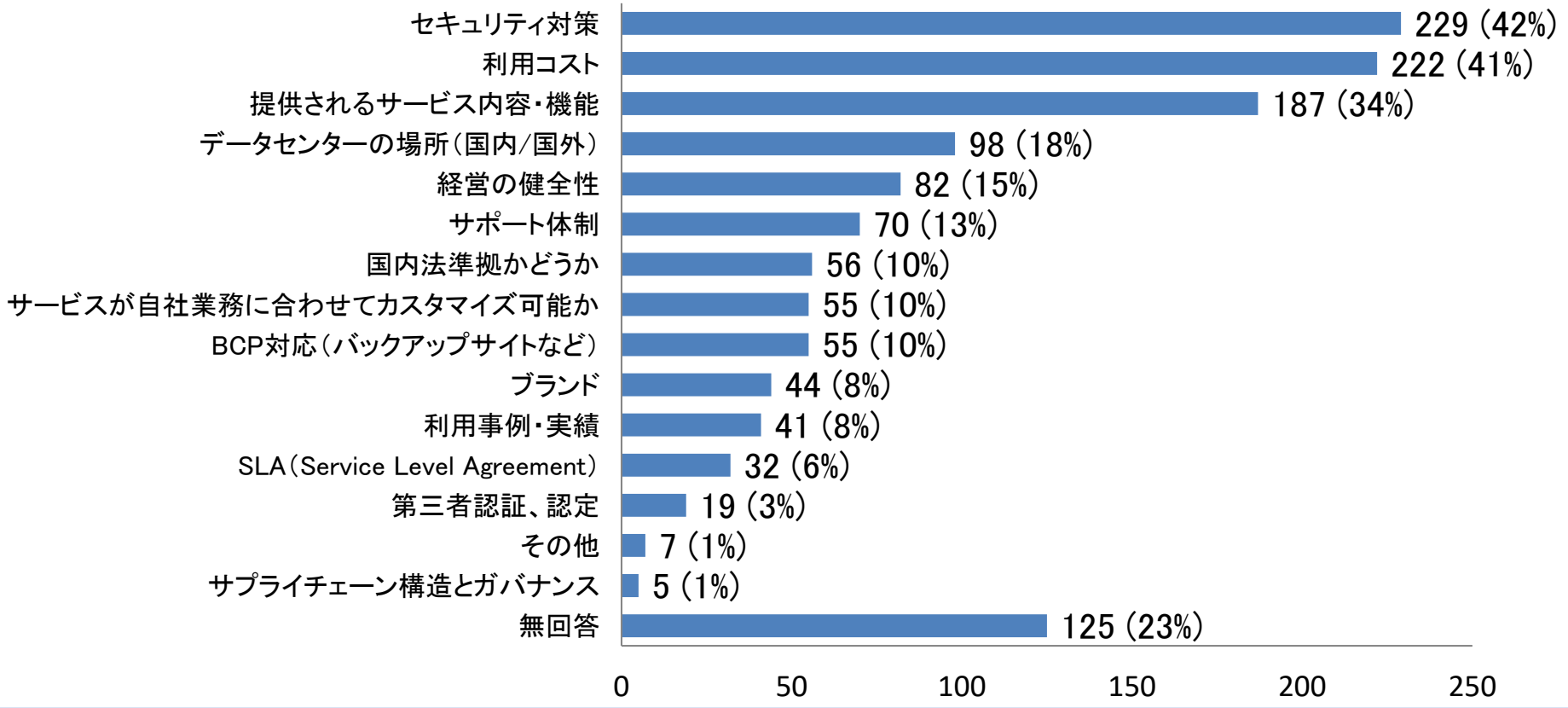


阻害要因の上位は、「セキュリティへの不安感」（54%）、「安定性・継続性への不安感」（35%）、「費用対効果が出ない、メリットがない」（26%）であった。

第6章　クラウドサービスの利用状況と阻害要因

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

設問37. クラウド事業者の選定において重視する点（複数回答）（N=544）

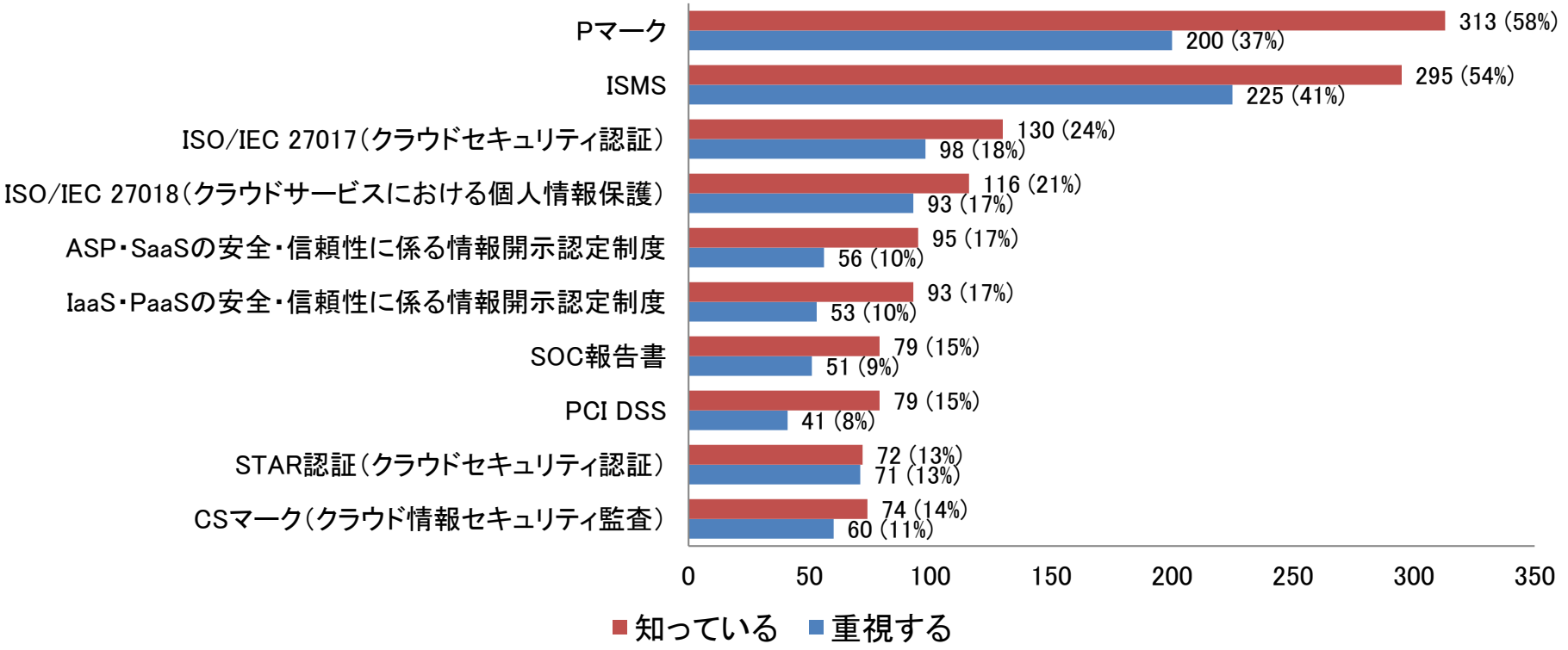


40%以上の組織が「セキュリティ対策」、「利用コスト」を重視している。
また、34%の組織が「提供されるサービス内容・機能」を重視している。

第6章　クラウドサービスの利用状況と阻害要因

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

設問38. クラウドサービスに対応した認証制度の認知度および重視度（個別回答）
（N=544）



認知度および重視度は、PマークとISMSが高い。
一方、専門的な認証制度の認知度・重視度は全体的に低い。

考察（第6章　クラウドサービスの利用状況と阻害要因）

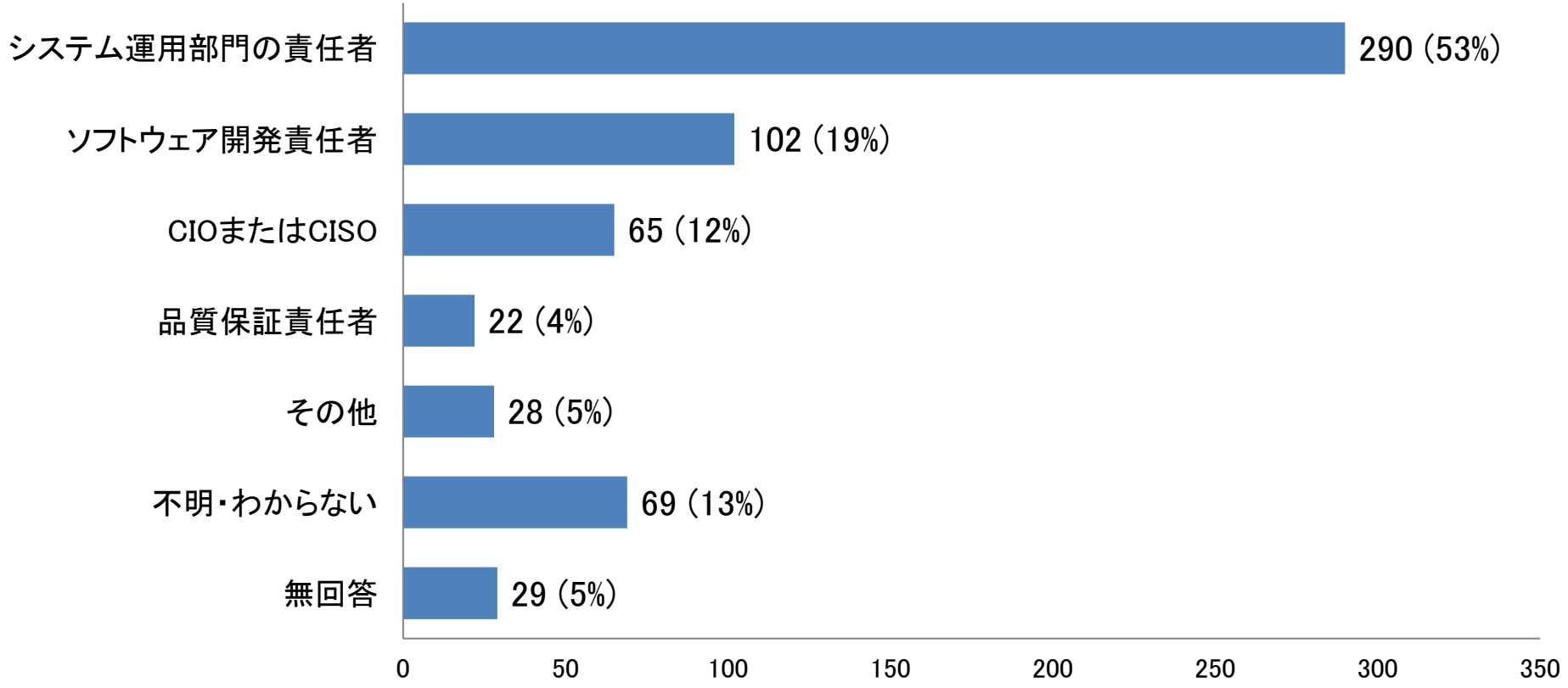
- クラウドサービスの利用状況は、コミュニケーション・コラボレーションサービスの利用率は52%と最も高い。一方、「利用予定なし」は業務インフラ（57%）や業務システム（49%）で高い。
- クラウドサービス利用の阻害要因は、セキュリティ面への不安感が上位となっている。
- 事業者選定時に重視する要素として、セキュリティ対策(42%)、利用コスト(41%)、サービス内容・機能(34%)が上位になっている。
- 第三者認証の中ではISMSとPマークの認知度・重視度が高い。

第7章
アプリケーションセキュリティの
リスク管理状況

第7章　アプリケーションセキュリティのリスク管理状況

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

設問39. リスク管理担当（複数回答）（N=544）

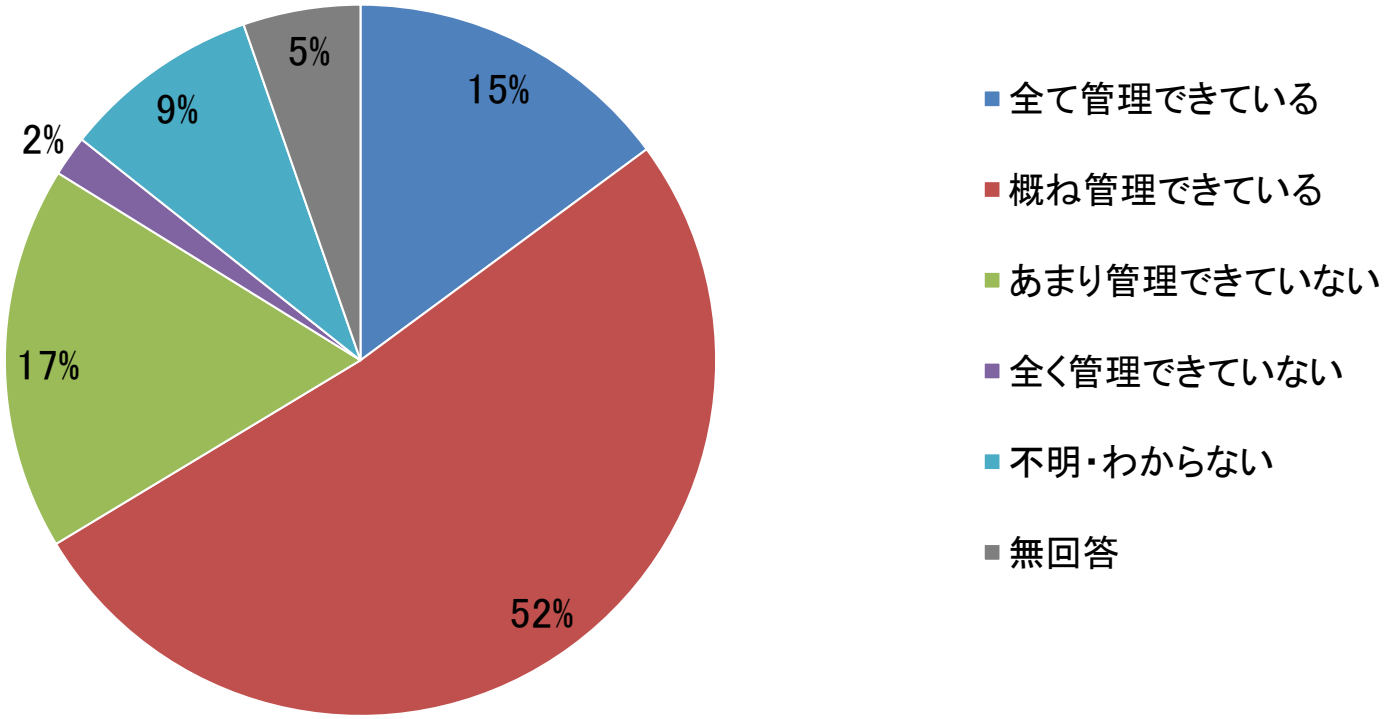


アプリケーションセキュリティのリスク管理担当は
「システム運用部門の責任者」の組織が53%を占めている。

第7章　アプリケーションセキュリティのリスク管理状況

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

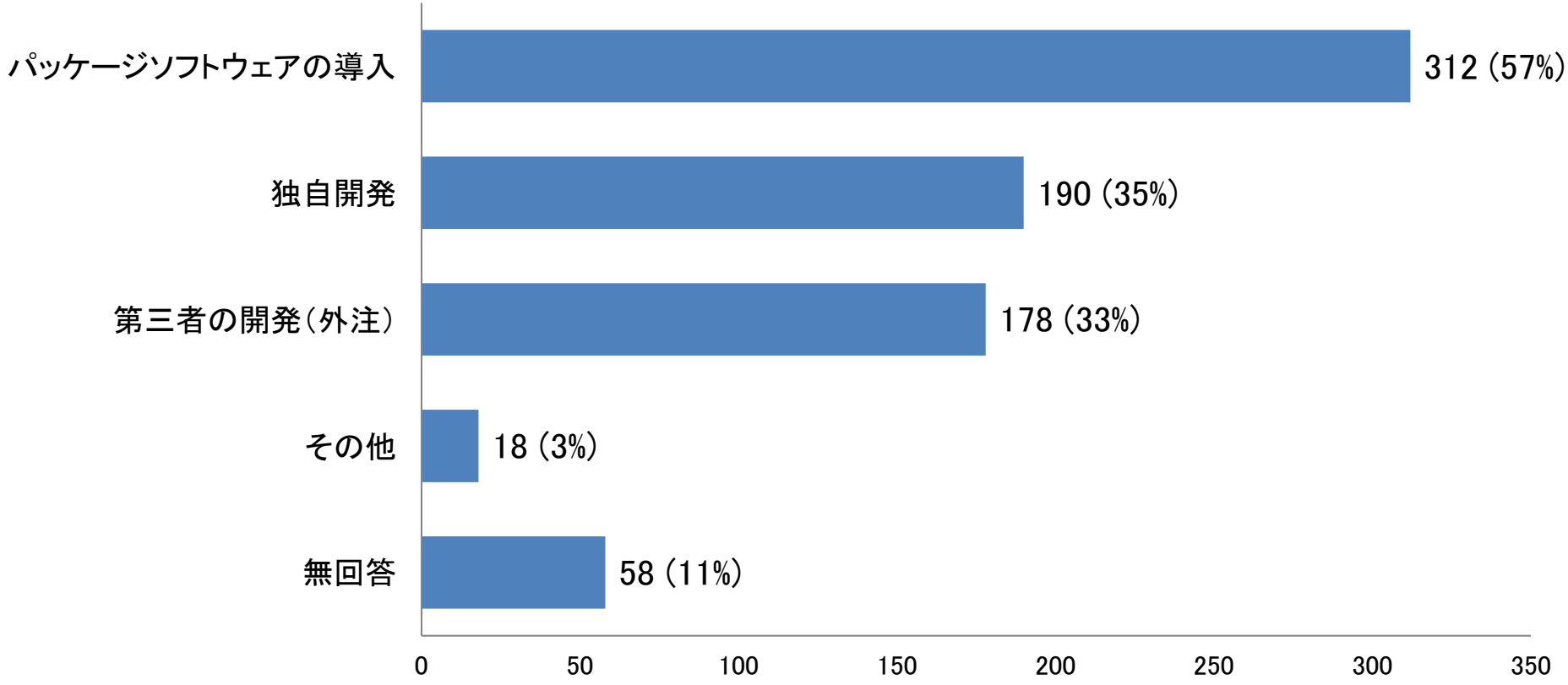
設問40. 運営中のウェブやモバイルのアプリケーションの管理状況（N=544）



ウェブやモバイルのアプリケーションは、67%の組織で管理できている（『全て管理できている』と『概ね管理できている』の合計）認識である。

第7章　アプリケーションセキュリティのリスク管理状況

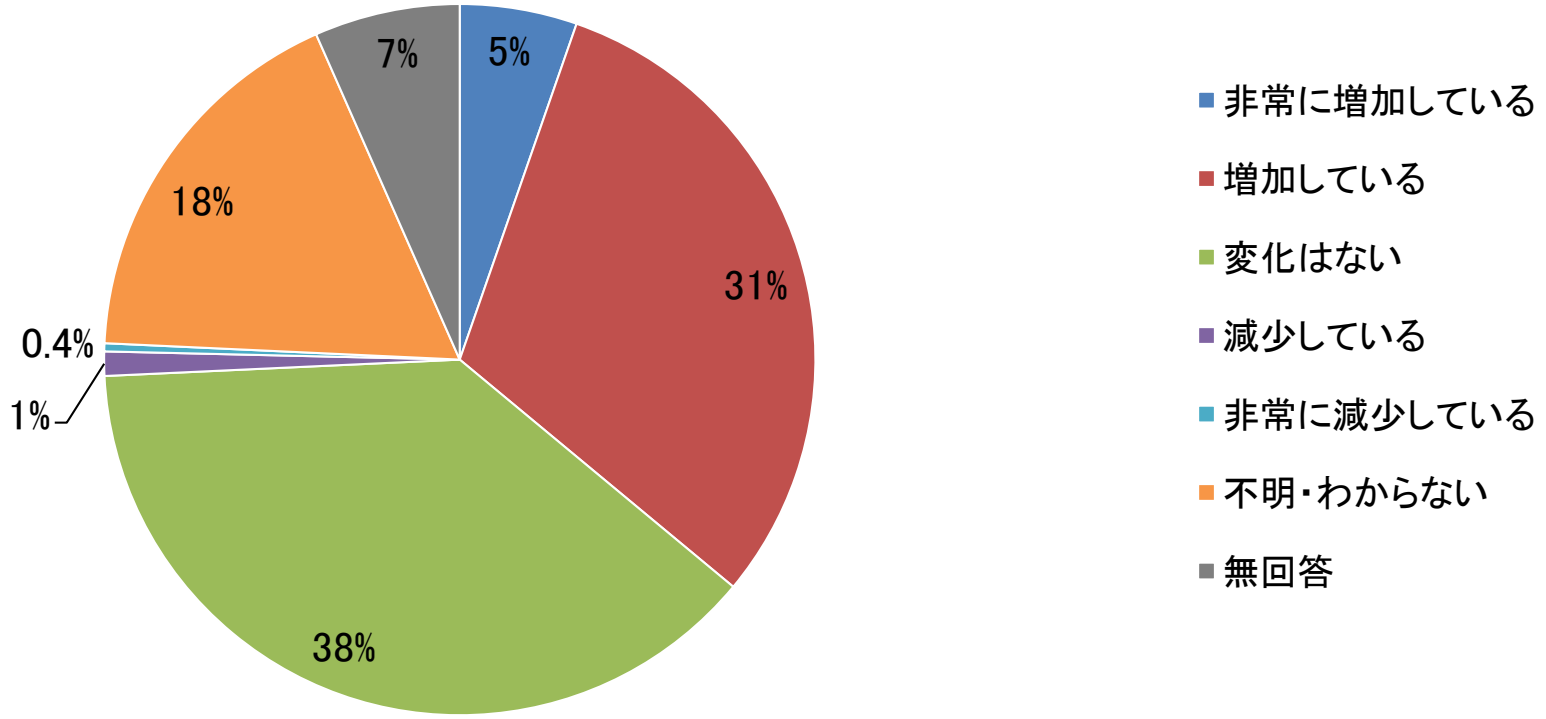
設問41. アプリケーションの開発運営形態（複数回答）（N=544）



「パッケージソフトウェアの導入」が57%であり、
「独自開発」が35%、「第三者の開発（外注）」が33%であった。

第7章　アプリケーションセキュリティのリスク管理状況

設問42. この1年間のアプリケーションのリスクの変化に対する認識（N=544）

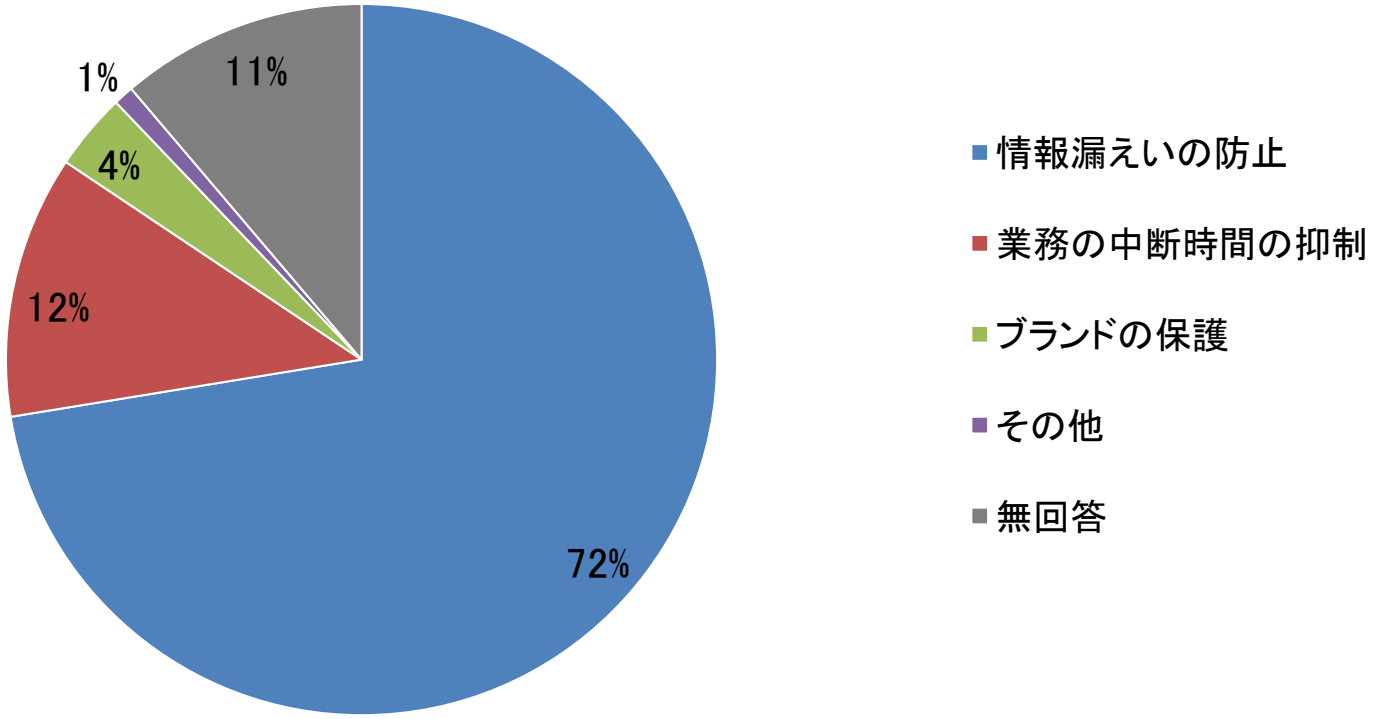


この1年間のリスクの変化に対する認識は『変化はない』が38%、
『増加』（『非常に増加している』と『増加している』の合計）が36%を占めてい

第7章　アプリケーションセキュリティのリスク管理状況

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

設問43. アプリケーションのリスク管理の目的で一番重視しているもの（N=544）

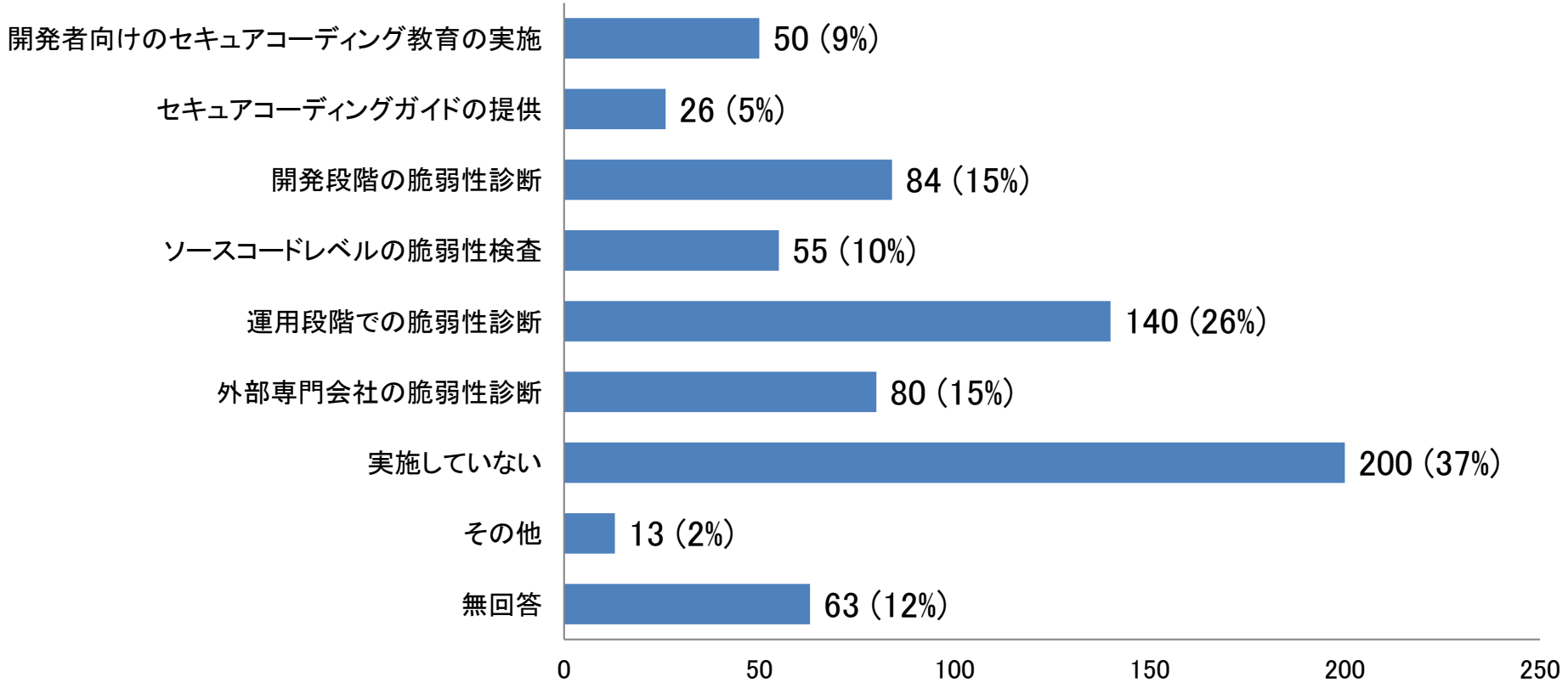


リスク管理の目的で一番重視しているものは、
「情報漏えいの防止」が72%を占めた。

第7章　アプリケーションセキュリティのリスク管理状況

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

設問44. アプリケーションのリスク対策状況（複数回答）（N=544）

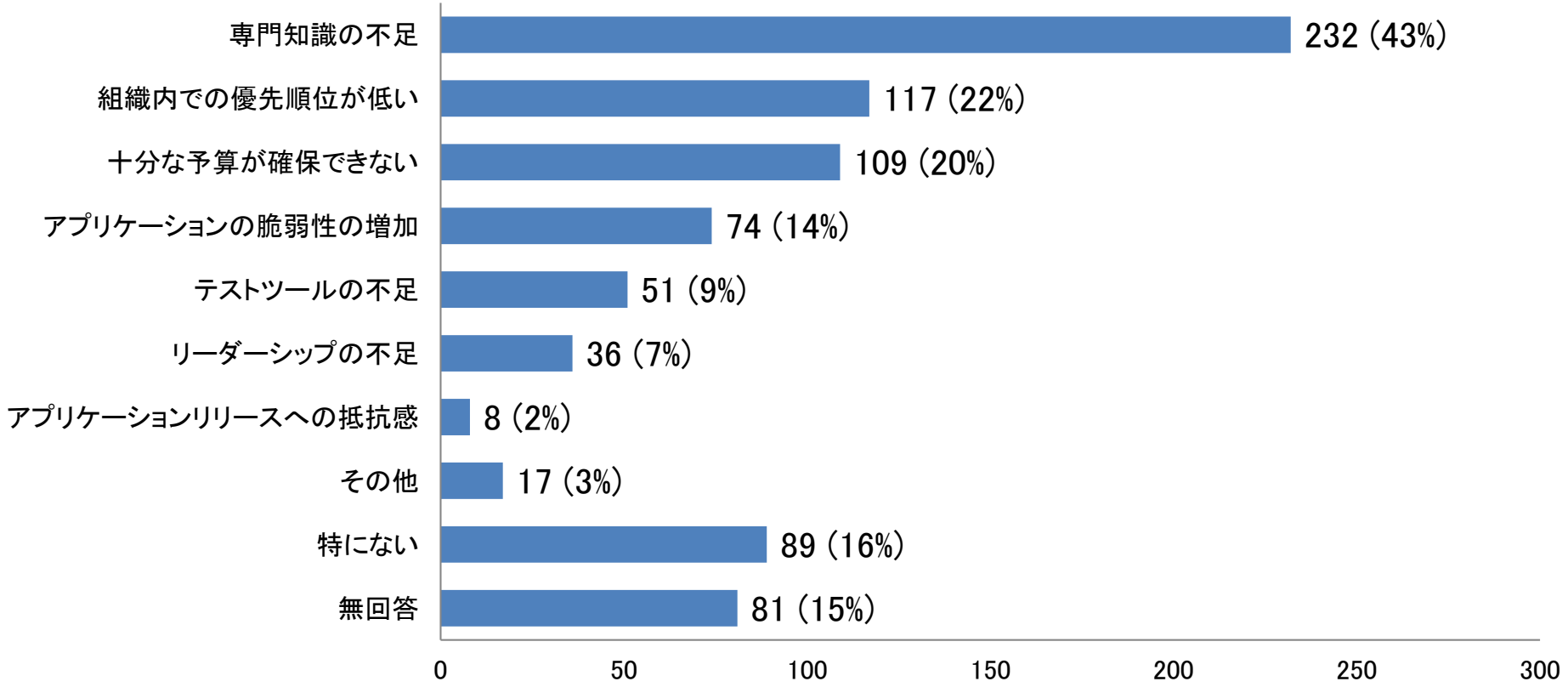


開発段階から運用段階におけるアプリケーションのリスク対策は、「実施していない」が37%、「運用段階での脆弱性診断」が26%であった。

第7章　アプリケーションセキュリティのリスク管理状況

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

設問45. アプリケーションのリスク管理ができない理由（複数回答）（N=544）



リスク管理ができない理由は、「専門知識の不足」（43%）、「組織内での優先順位が低い」（22%）、「十分な予算が確保できない」（20%）が上位であった。

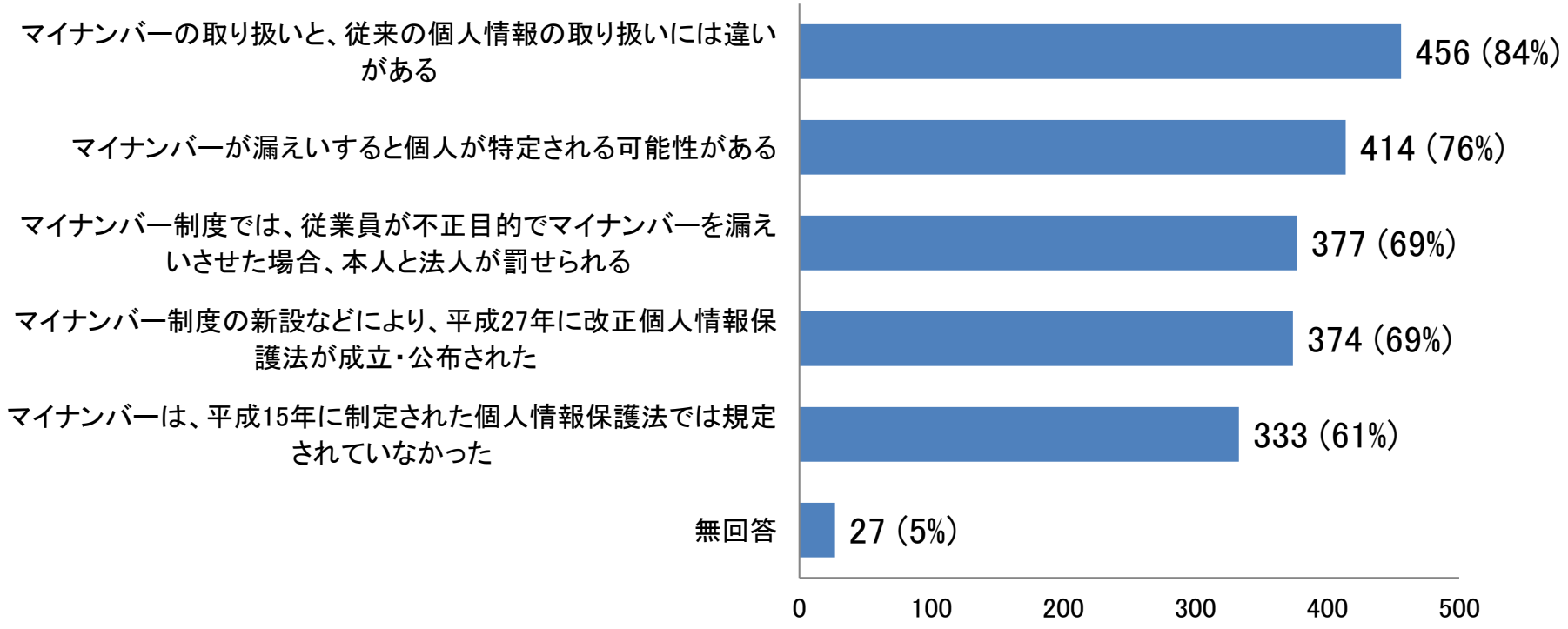
考察（第7章　アプリケーションセキュリティのリスク管理状況）

- ウェブやモバイルのアプリケーションは、67%の組織で管理できている（『全て管理できている』と『概ね管理できている』の合計）認識であった。
- この1年間のリスクの変化に対する認識は『変化はない』が38%、『増加』（『非常に増加している』と『増加している』の合計）が36%を占めている。
- アプリケーションのリスク管理の目的で一番重視しているものは、「情報漏えいの防止」が72%を占めている。
- 開発段階から運用段階におけるアプリケーションのリスク対策は、「実施していない」が37%を占める。
  リスク対策を「実施していない」理由は、「専門知識の不足」（43%）が最も多い。

第8章
マイナンバーの取り組み状況

第8章　マイナンバーの取り組み状況

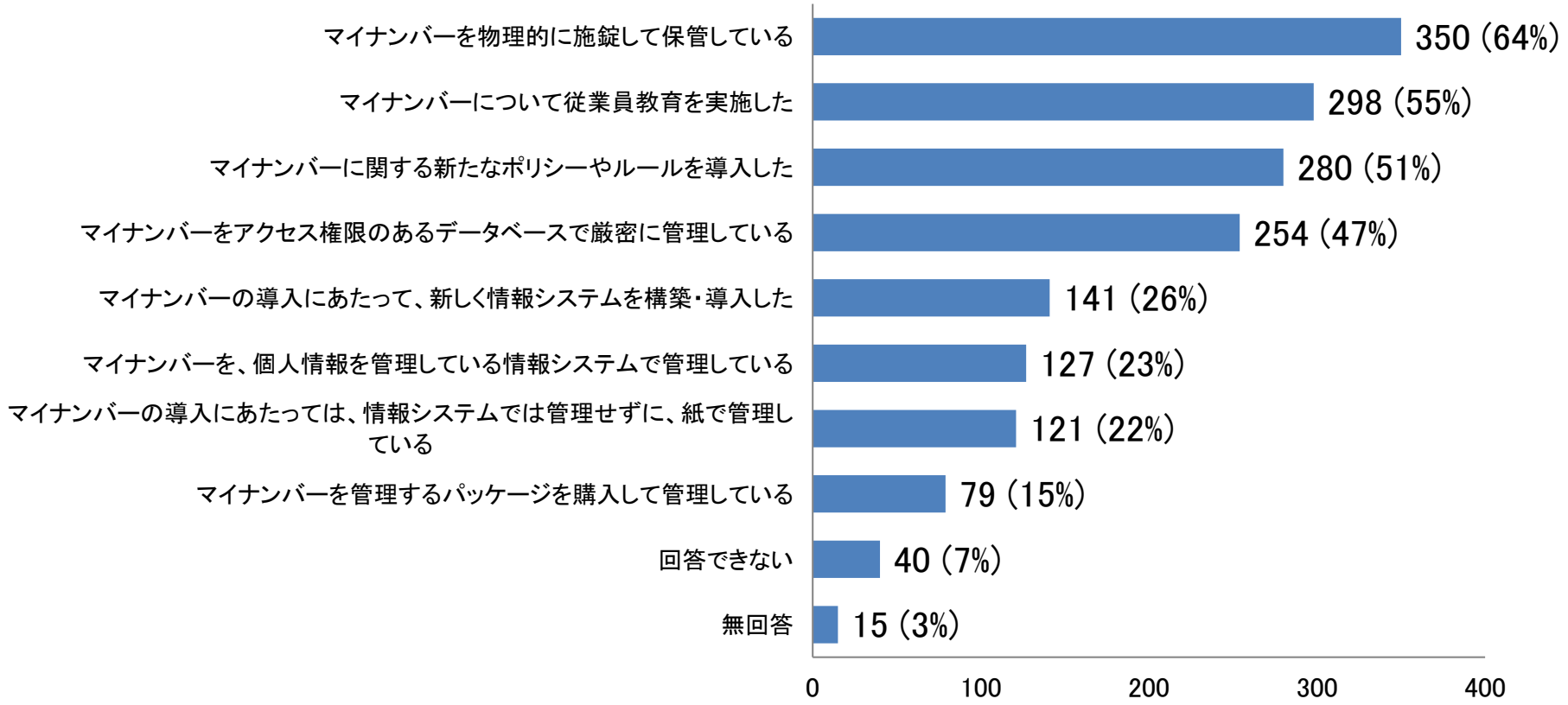
設問46. マイナンバー制度の内容の認知度（個別回答）（N=544）



84%の組織が、「マイナンバーの取り扱いと従来の個人情報の取り扱いには違いがある」ことを認知していた。
60%以上の組織が、いずれの内容についても認知していた。

第8章　マイナンバーの取り組み状況

設問47. マイナンバーの取り扱い内容（複数回答）（N=544）

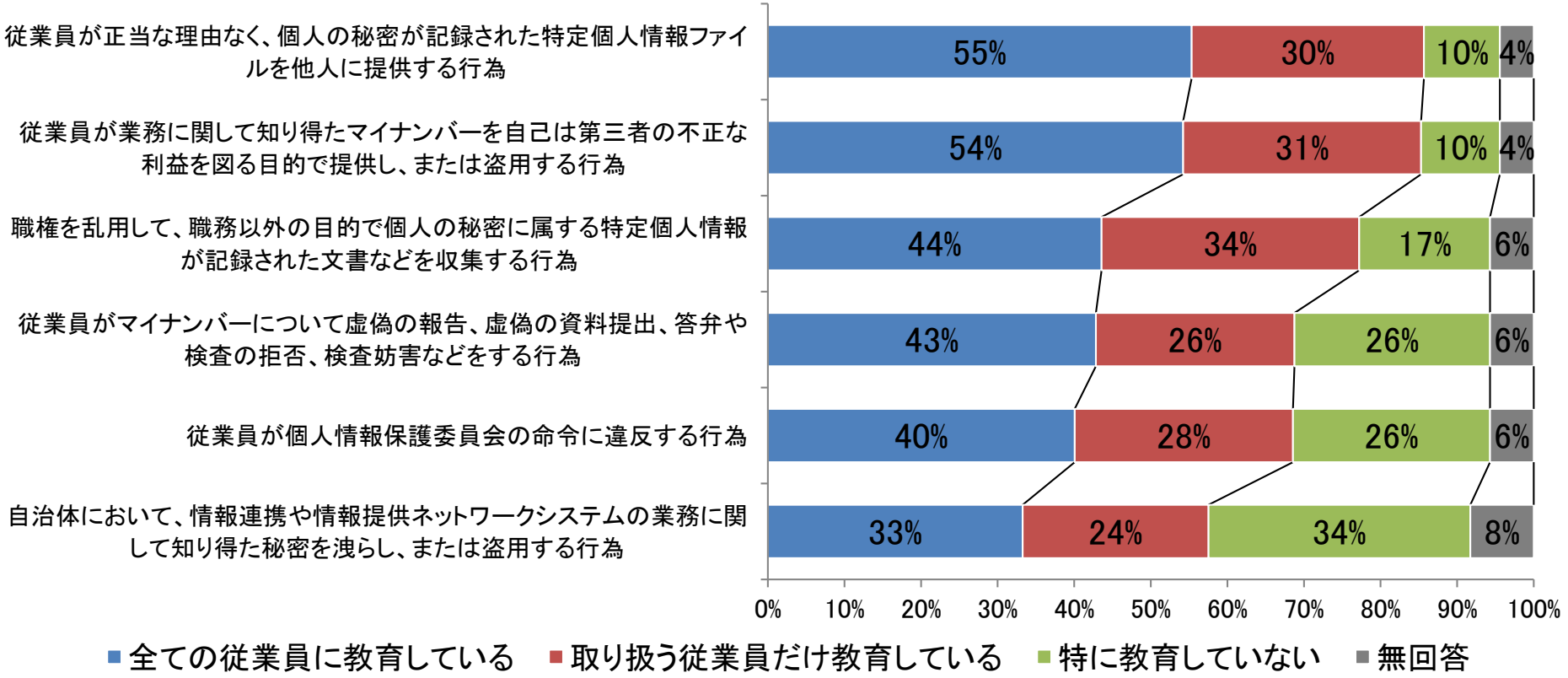


50%以上の組織で、「マイナンバーの施錠保管」、「従業員教育」、「ポリシーやルールの導入」を実施している。

第8章　マイナンバーの取り組み状況

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

設問48. マイナンバーに関する違法行為についての教育状況（N=544）



85%の組織で、「特定個人情報の他人への提供」や
「マイナンバーの不正な提供・盗用」の教育が行われている。

考察（第8章　マイナンバーの取り組み状況）

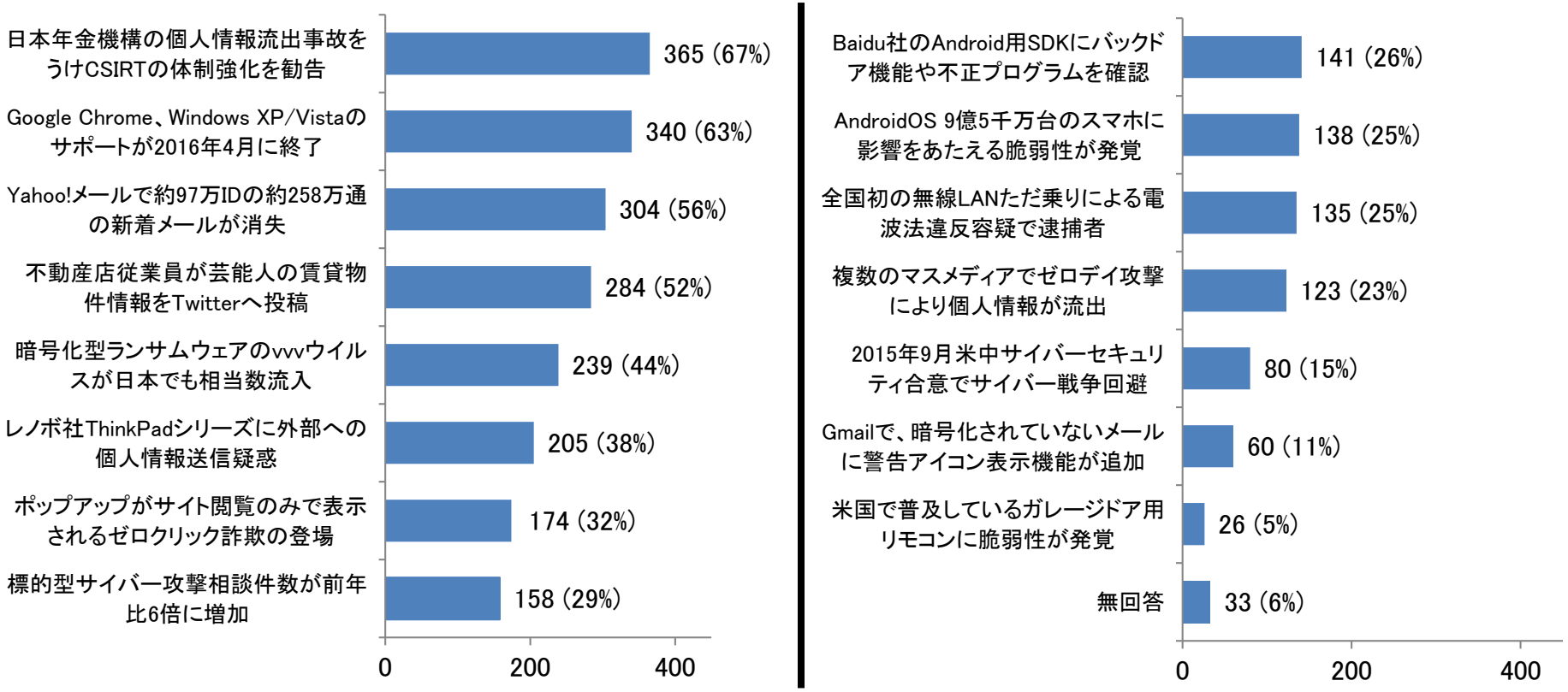
- マイナンバー制度の内容については、84%の組織が「マイナンバーの取り扱いと従来の個人情報の取り扱いには違いがある」ことを認知していた。また、60%以上の組織がいずれの内容についても認知していた。
- マイナンバーの取り組み内容については、50%以上の組織で「マイナンバーの施錠保管」、「従業員教育」、「ポリシーやルールの導入」を実施している。
- マイナンバーに関する違法行為の教育については、85%の組織で「特定個人情報の他人への提供」や「マイナンバーの不正な提供・盗用」の教育が行われている。

第9章
その他　過去の事例・事故・用語の認知度

第9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49. 出来事（事例・事故の認知度）（複数回答）（N=544）

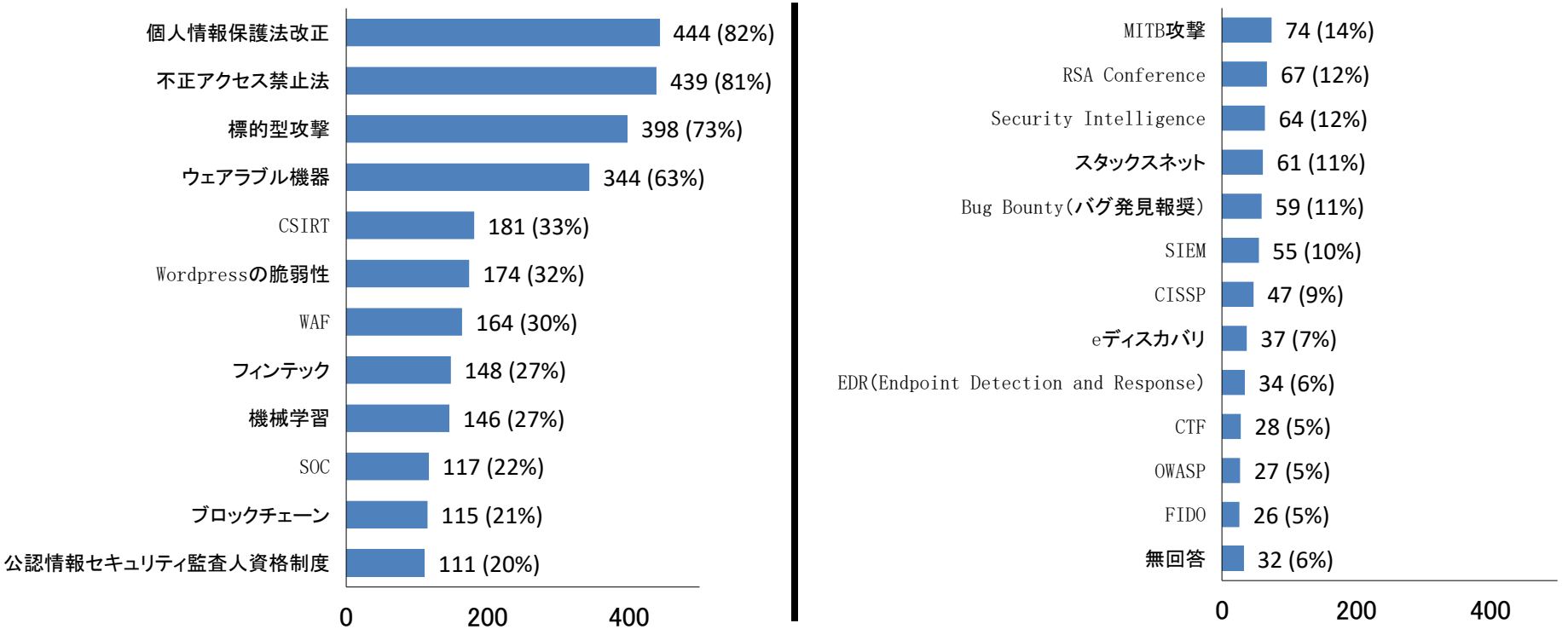


マスメディアで取りあげられた事件・事故への認知度が高い。
一方、海外事故や専門的なものについては認知度が高くない。

第9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50. 用語の認知度（複数回答）（N=544）



「個人情報保護法改正」、「不正アクセス禁止法」の認知度が80%を超えた。
「標的型攻撃」、「ウェアラブル機器」も60～70%程度で認知度が高かった。
「CSIRT」等は30%程度にとどまり、専門的な用語の認知度は低かった。

考察（第9章　その他（過去の事例・事故・用語の認知度））

- 事例・事故の認知度は、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・事故では高い傾向にあった。例えば、「日本年金機構の個人情報流出をうけたCSIRTの体制強化勧告」や「Google ChromeがWindows XP/Vistaのサポート終了」は60%を越えた。一方で、「Baidu社のAndroid用SDKにバックドア機能や不正プログラム確認」や「米国で普及しているガレージドア用リモコンの脆弱性」などの専門的な事例では低い結果となった。
- 用語の認知度は、「個人情報保護法改正」、「不正アクセス禁止法」といった法律関連用語では高い。「標的型攻撃」、「ウェアラブル機器」では60～70%程度で高い結果となったが、「CSIRT」や「フィンテック」などの専門的な用語では低い結果となった。
- 特に「CSIRT」は、最も認知度の高かった事例・事故に含まれているにも関わらず、用語としての認知度が低いという結果となり、詳しい内容が知られていないことがうかがえる。

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企業や団体、組織の皆さまに感謝いたします。
- 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
  - 神奈川県立相模原養護学校
  - 神奈川県立相模原養護学校　橋本分教室
  - 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
  - 神奈川県立中原養護学校
  - 神奈川県立みどり養護学校　新栄分教室
  - 川崎市立田島支援養護学校

（五十音順）

の皆さまに感謝いたします。

情報セキュリティ大学院大学
原田研究室　一同