2018年情報セキュリティアンケート調査結果

公開：2018年12月20日　更新：2019年1月16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

- アンケート実施期間

  2018年8月1日～8月31日
  （2010年より毎年実施　9回目）

- アンケート対象

  4500組織の情報セキュリティ関係者
  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，ISO 9001認証取得企業，CSMS認証取得企業，官公庁，教育機関（以下「組織」という）など

- 調査方法：郵送による
- 回答状況：402件（送付総数(4233件)に対して9.5%）
- 回答の未記入及び択一問題における重複回答等の無効回答は，無回答として計上

情報セキュリティ調査について

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

調査項目

1章　概要（回答者の基本データ等）
2章　情報セキュリティマネジメントの取り組み
3章　情報セキュリティ対応体制・人材に関する状況
4章　制御システムにおける情報セキュリティに関する課題
5章　匿名加工情報
6章　情報セキュリティマネジメントの「例外措置」
7章　職場での人工知能(AI)や自律型ロボットの導入
8章　グループ企業における情報セキュリティポリシーについて
9章　EU一般データ保護規則(GDPR)への対応
10章　過去の事例・事故の認知度

設問は，Q1～Q51まで（フリーコメントを含む）

第1章
概要（回答者の基本データ等）

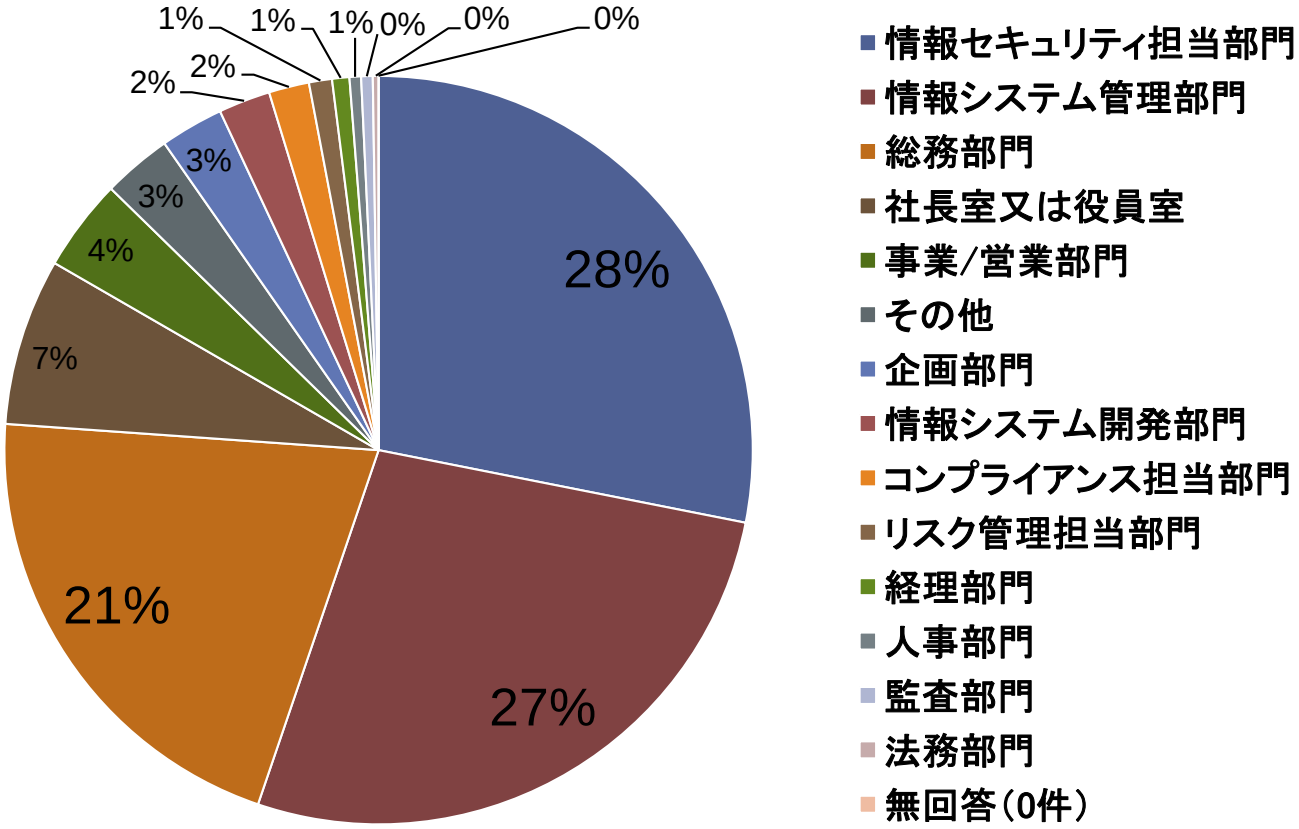
調査概要：

回答者の所属，業種，組織の規模，
従業員数 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=402）

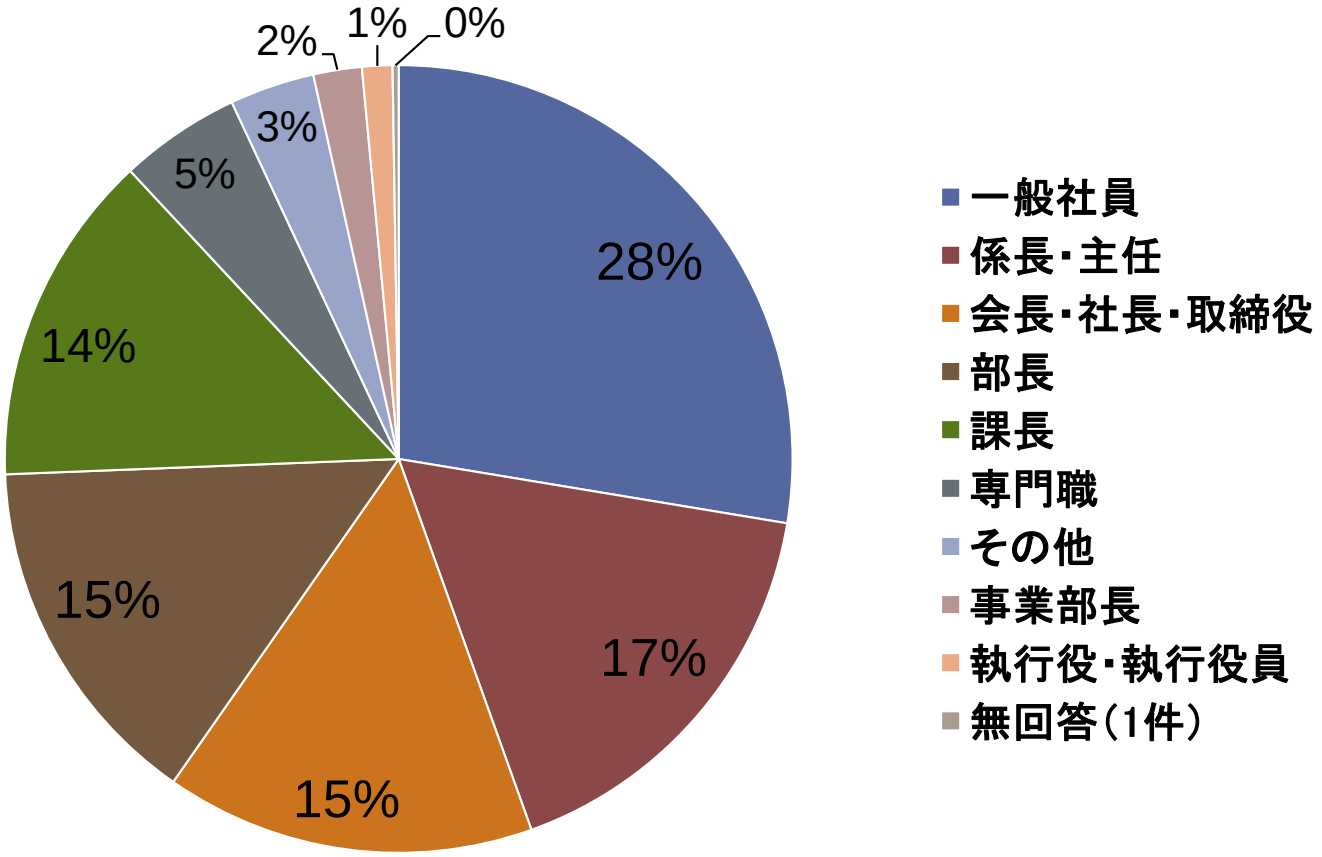


所属部門は「情報セキュリティ担当部門」
「情報システム管理部門」、「総務部門」の順に多かった。

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=402）

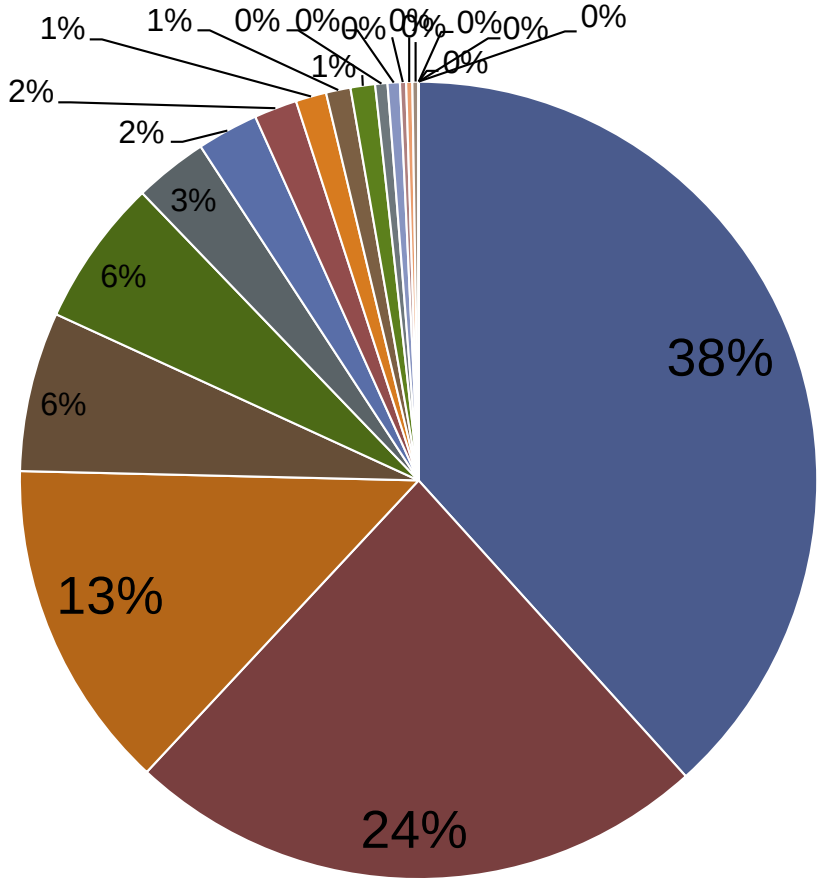


回答者は「一般社員」が最も多く（昨年度と同様）、
「係長・主任」、「会長・社長・取締役」と続く

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=402）



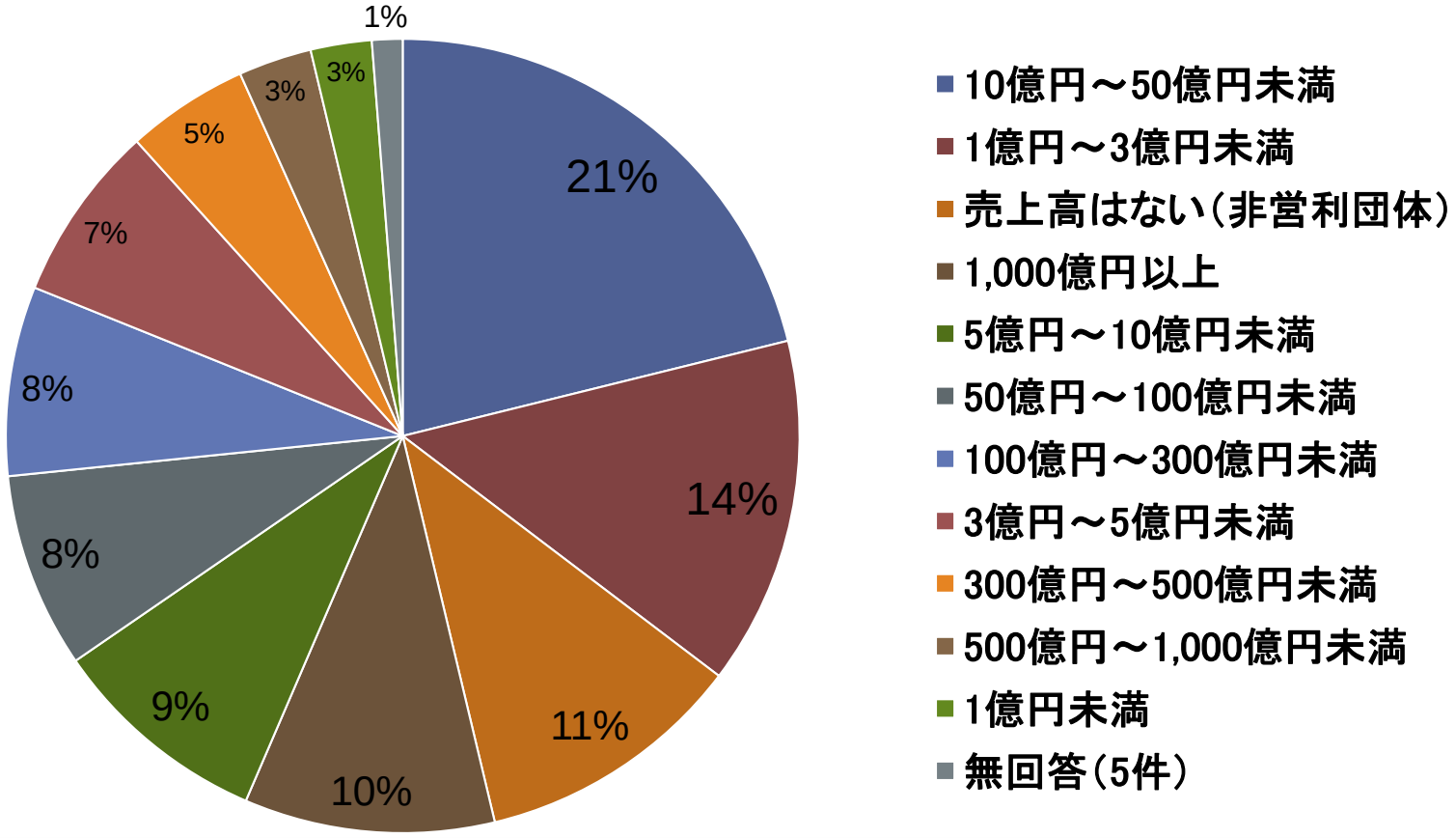
- 情報通信業
- 公務（政府・自治体）
- 大学
- サービス業
- 製造業
- その他
- 卸売業、小売業
- 学術研究、専門・技術サービス業
- 建設業
- 金融業、保険業
- 運輸業、郵便業
- 教育、学習支援業
- 生活関連サービス業、娯楽業
- 医療、福祉
- 不動産業、物品賃貸業
- 複合サービス事業（郵便局、協同組合）
- 農業、林業、漁業、鉱業
- 電気・ガス・熱供給・水道業
- 宿泊業、飲食サービス業
- 無回答（0件）

「情報通信業」が38%と4割近くを占めている（昨年と同様）

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=402）

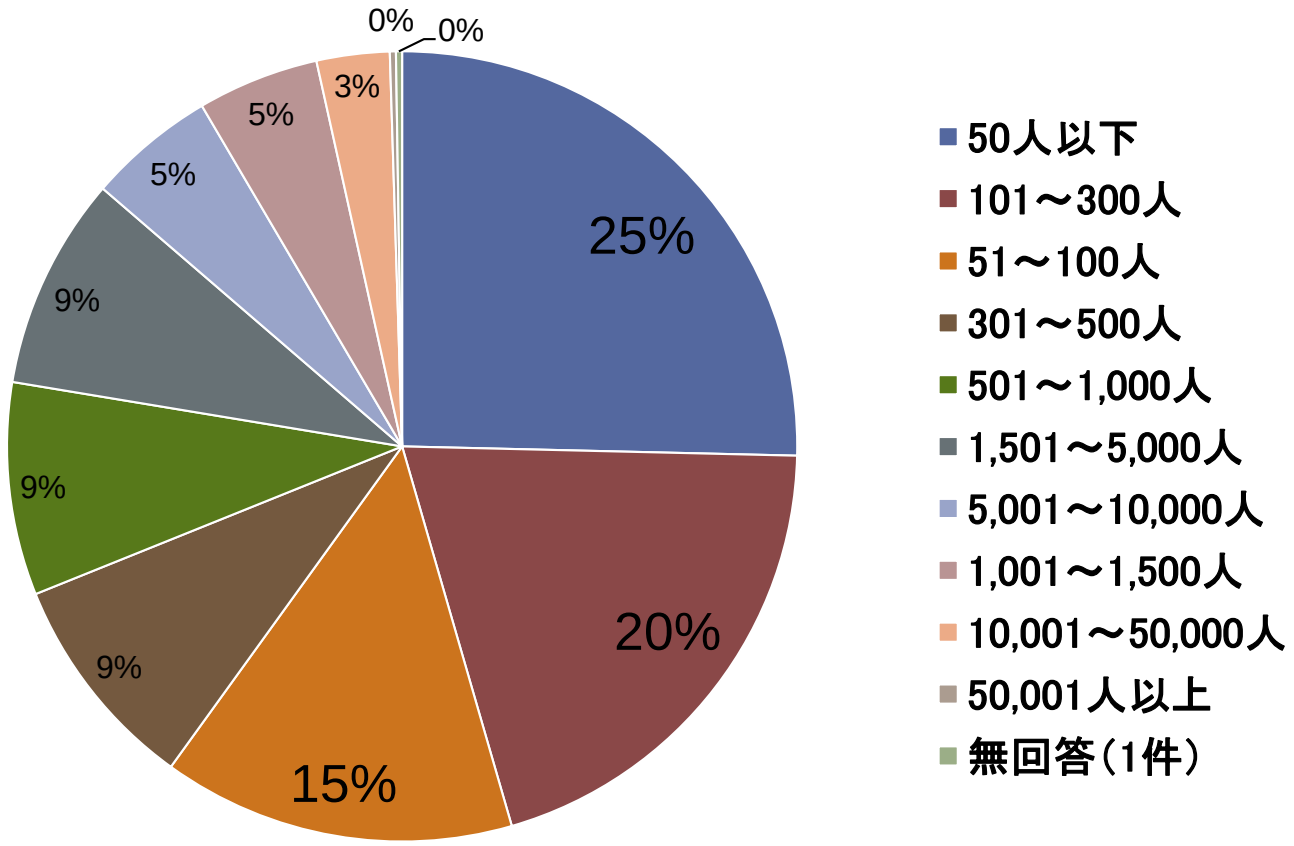


売上高10億円～50億円の組織が最も多い。
また、売上高50億円以下の組織で54%を占めている。

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=402）

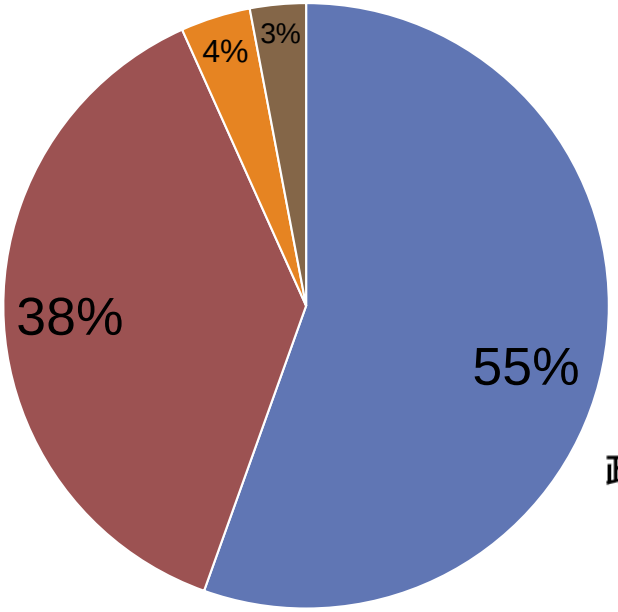


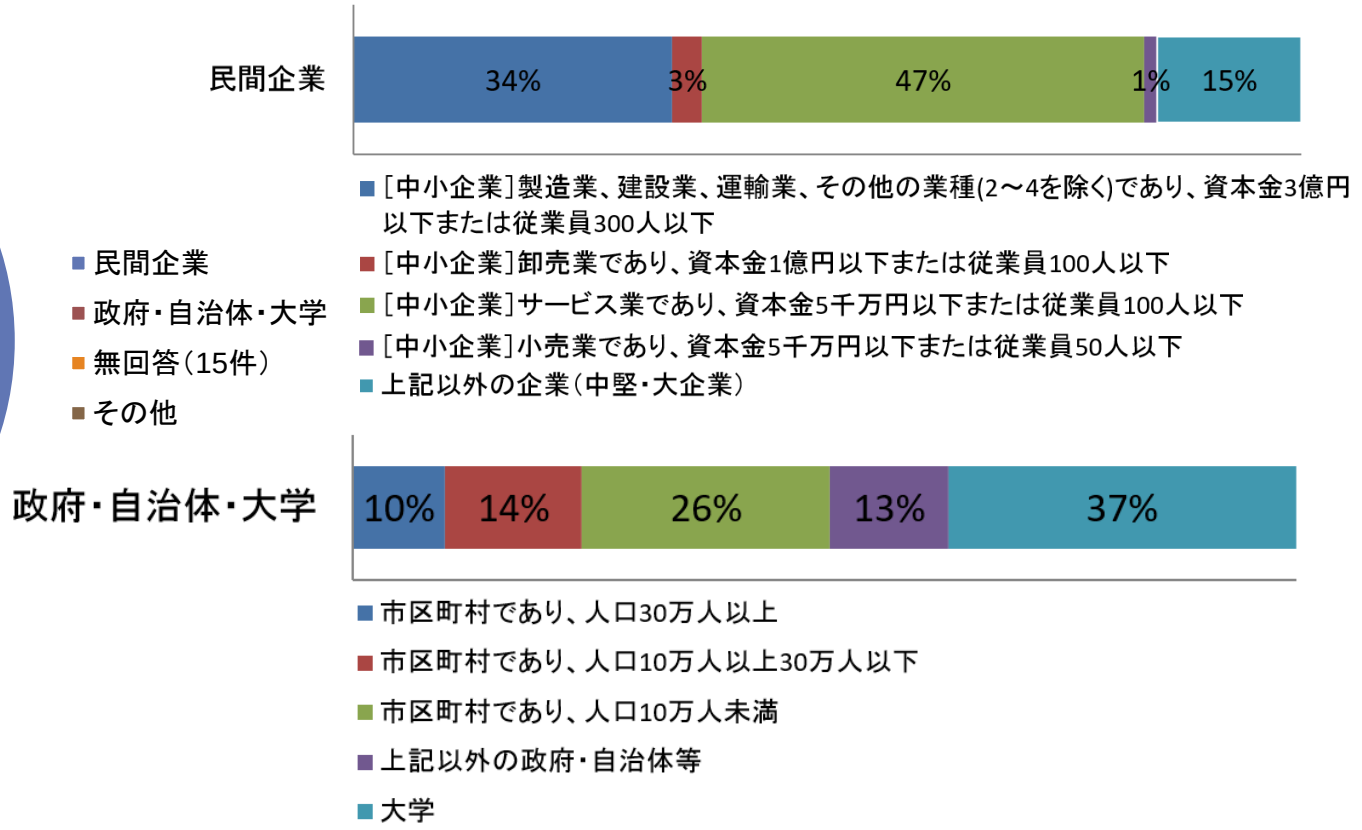
従業員数50人以下の組織が最も多い。
また、従業員300人以下の組織で60%を占めている。

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=402）



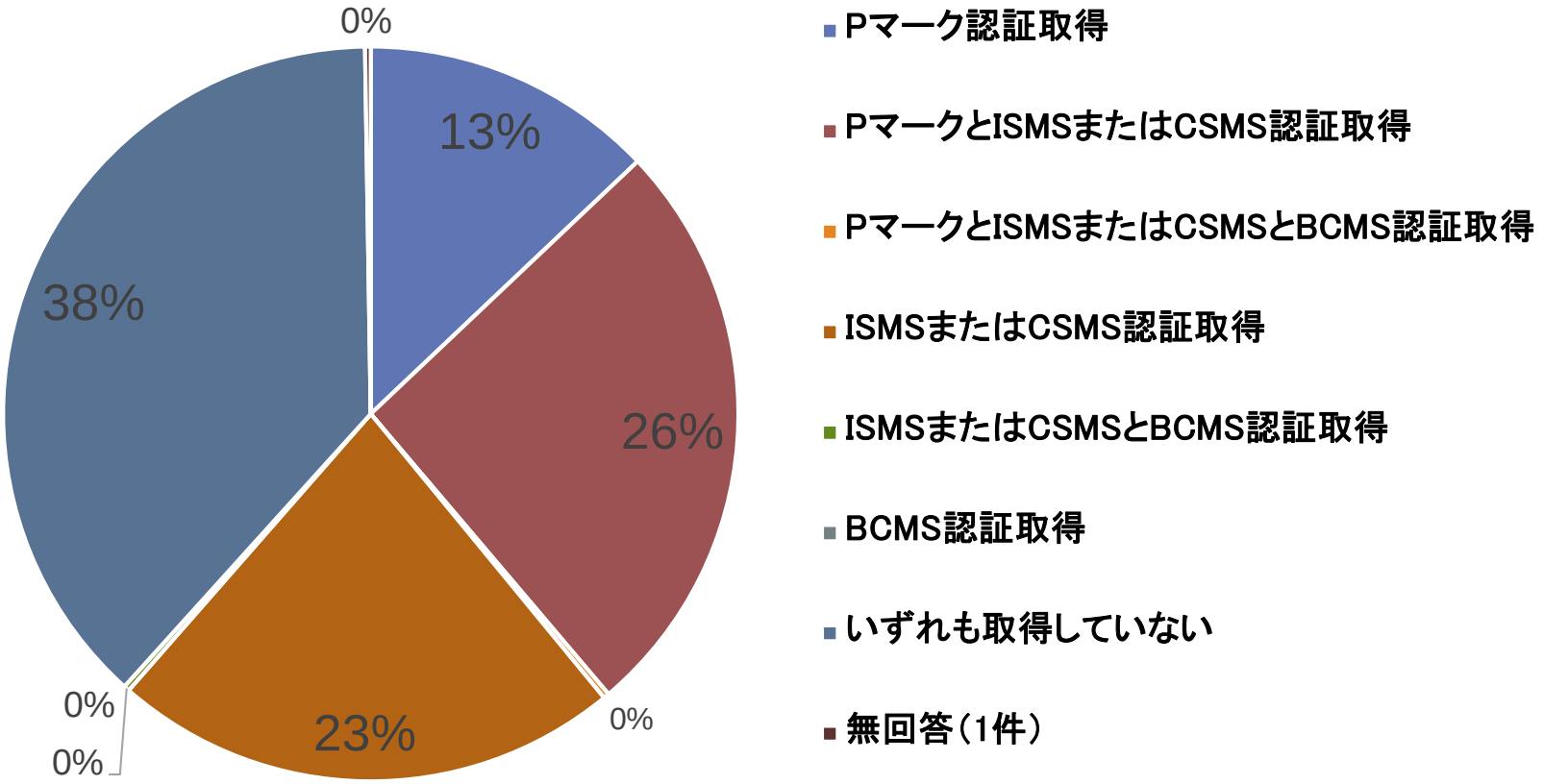


民間企業55%、政府・自治体・大学38%となっている。
中小企業が民間企業の85%を占めている。

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またはCSMS、BCMSの取得状況（N=402）

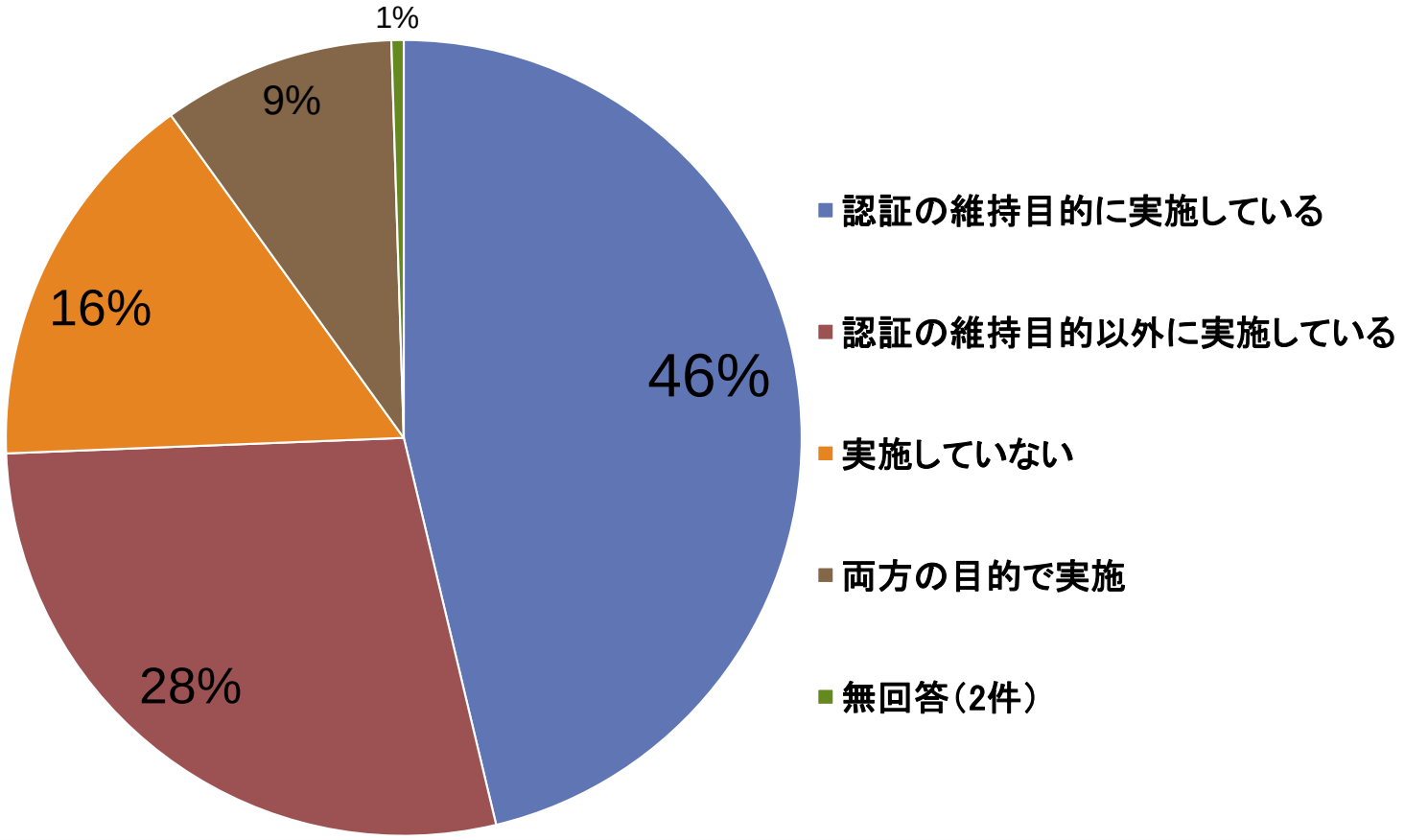


39%の組織がPマークを、49%の組織がISMSを取得している。
また、26%の組織がPマークとISMSの両方を取得している。

※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）

設問8　情報セキュリティ監査の実施状況（N=402）



46%の組織が認証の維持目的、28%の組織が認証の維持目的以外、9%の組織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。

第1章　概要（回答者の基本データ等）

回答者の業種、年間売上高、従業員数等の基本データは昨年度と比較して大きな変化はなく、概ね同様な傾向となっている。

調査結果：

- 情報通信業が回答者の4割近くを占めている。
- 売上高10億円から50億円の組織が21%と最も多い。
- 従業員数50人以下の組織が25%と最も多い。
  また、従業員数300人未満の組織が60%を占めている。
- 民間企業55%、政府・自治体・大学38%となっている。また、民間企業の85%が中小企業が占めている。
- 39%の組織がPマークを、49%の組織がISMSを取得している。
  また、23%の組織がPマークとISMSの両方を取得しており、昨年と同様である。

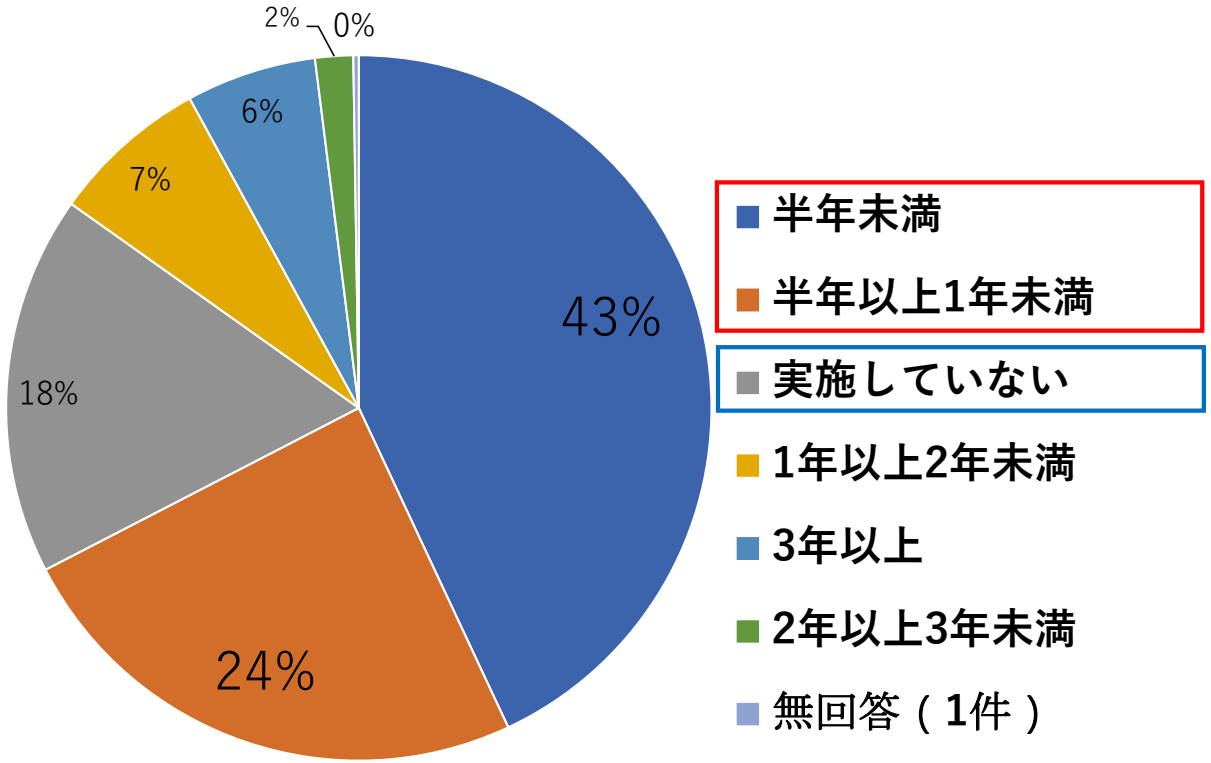
第2章
情報セキュリティマネジメントの取り組み

調査概要：

リスク分析の実施状況，情報セキュリティポリシーの策定・見直し状況，支出動向 等

第2章　情報セキュリティマネジメントの取り組み状況

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=402）

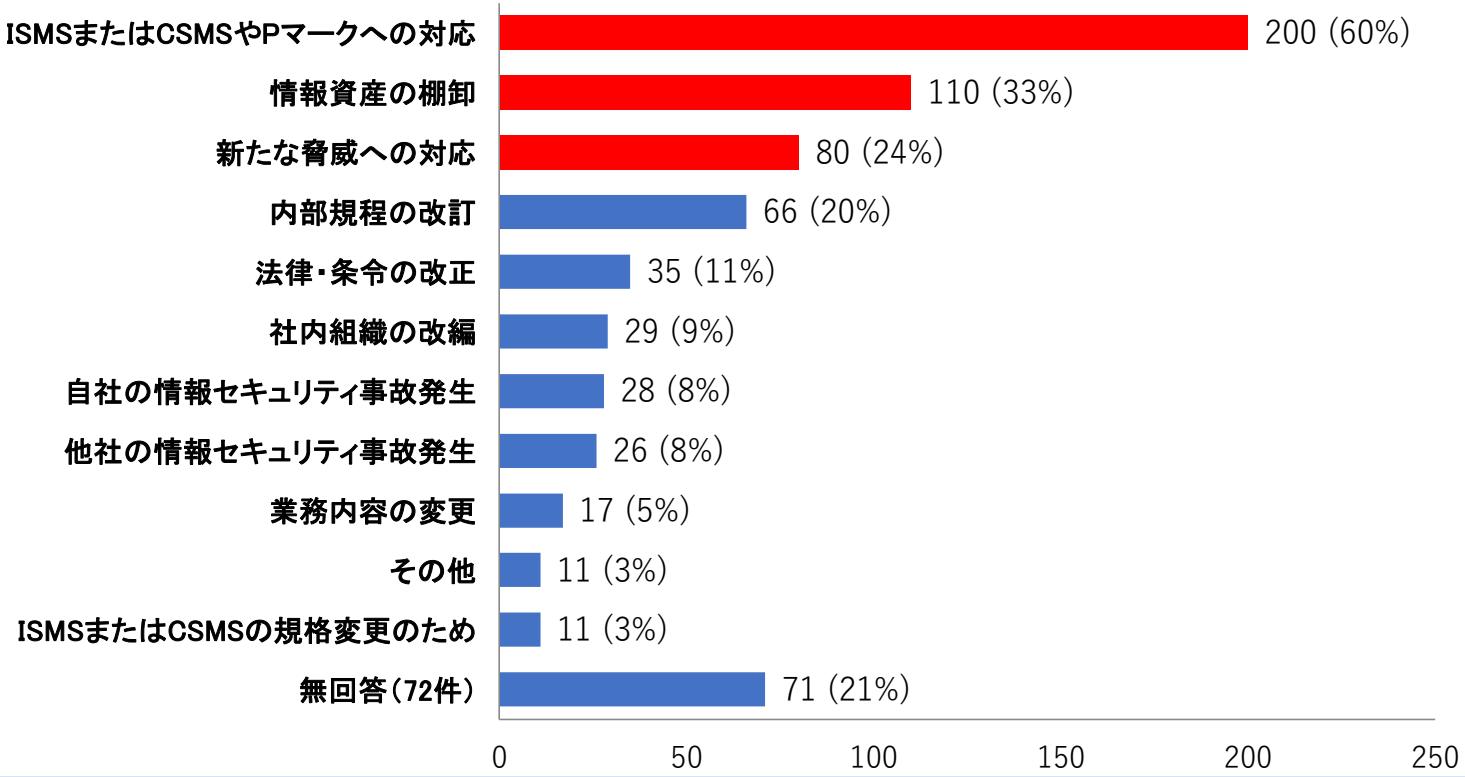


67%（271）の組織が、1年以内にリスク分析を実施している。
一方、18%（70）の組織はリスク分析を実施していない。

第2章　情報セキュリティマネジメントの取り組み状況

設問10. リスク分析の実施理由（複数回答）（N=332）

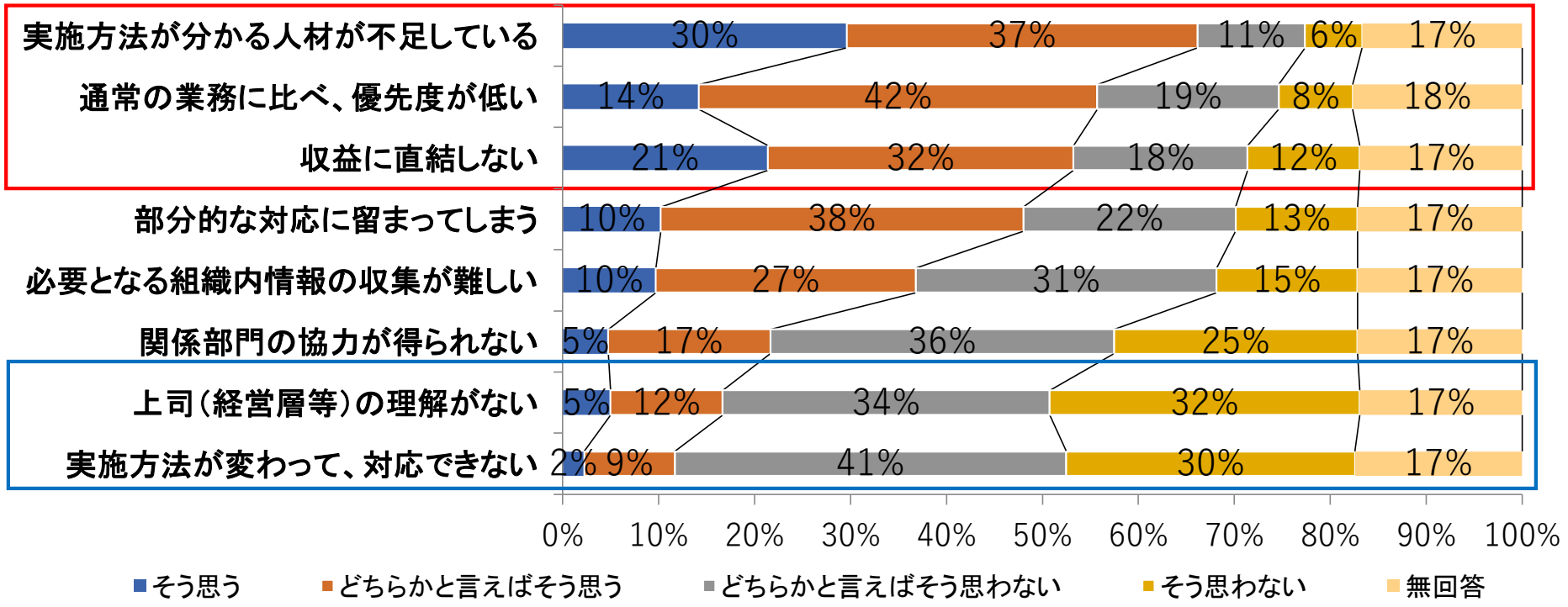
※設問9で「情報セキュリティリスク分析は実施してない」以外を回答した組織を対象



ISMSまたはCSMSやPマークへの対応がリスク分析を実施した332組織中200で60% である。情報資産の棚卸、新たな脅威への対応と続いている。

第2章　情報セキュリティマネジメントの取り組み状況

設問11. リスク分析を行う際の問題点（N=402）

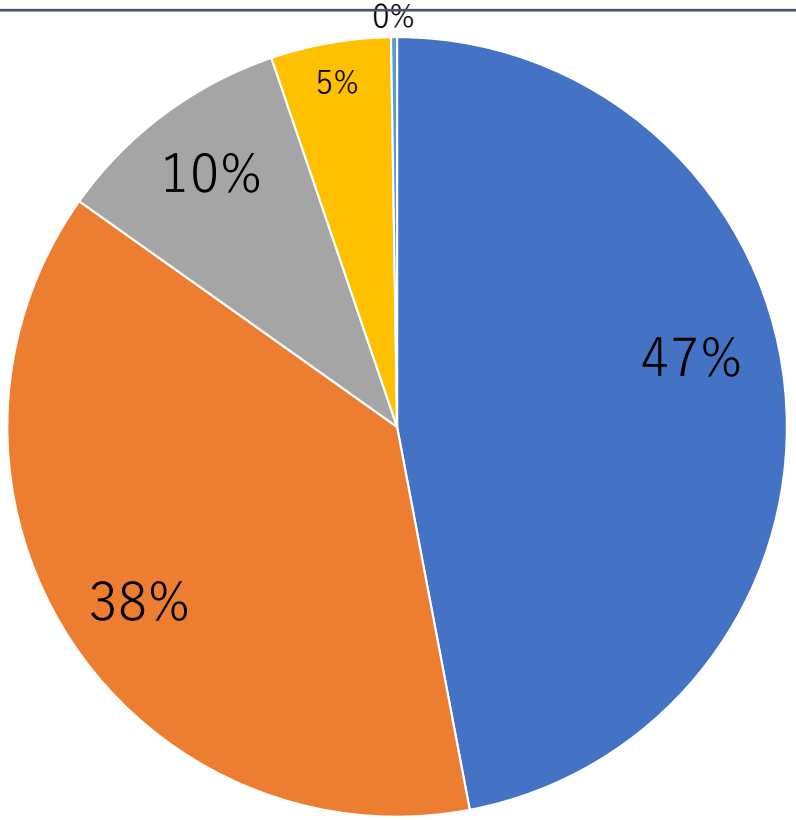


注：　＜そう思う＋どちらかと言えばそう思う＞の多い順に表示

人材の不足を感じる（67%）、通常業務に比べ、優先度が低い（56%）、収益に直結しない（53%）の順である。上司（経営層等）の理解がないは17%実施方法が変わって対応できないは11%と低かった。

第2章　情報セキュリティマネジメントの取り組み状況

設問12. 情報セキュリティポリシー（方針・対策基準）の策定と見直し状況（N=402）

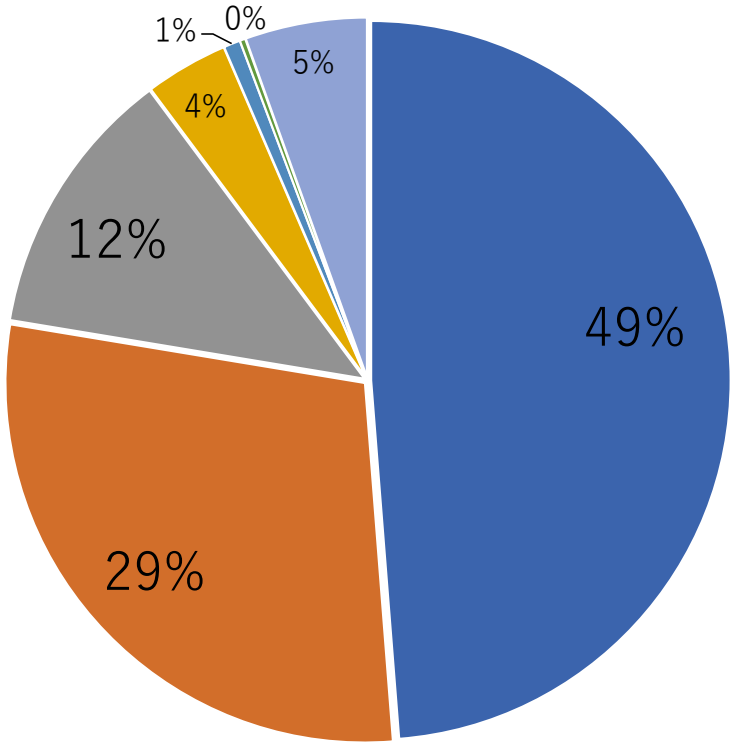


- 年に1回、定期的に実施している
- 数年に一回、実施している
- 策定後、一度も見直しを行っていない
- 策定していない
- 無回答（1件）

85%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、10%が策定後見直しておらず、20組織（5%）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

設問13. 情報セキュリティポリシー（方針・対策基準）の策定・見直しを行う部門（N=402）



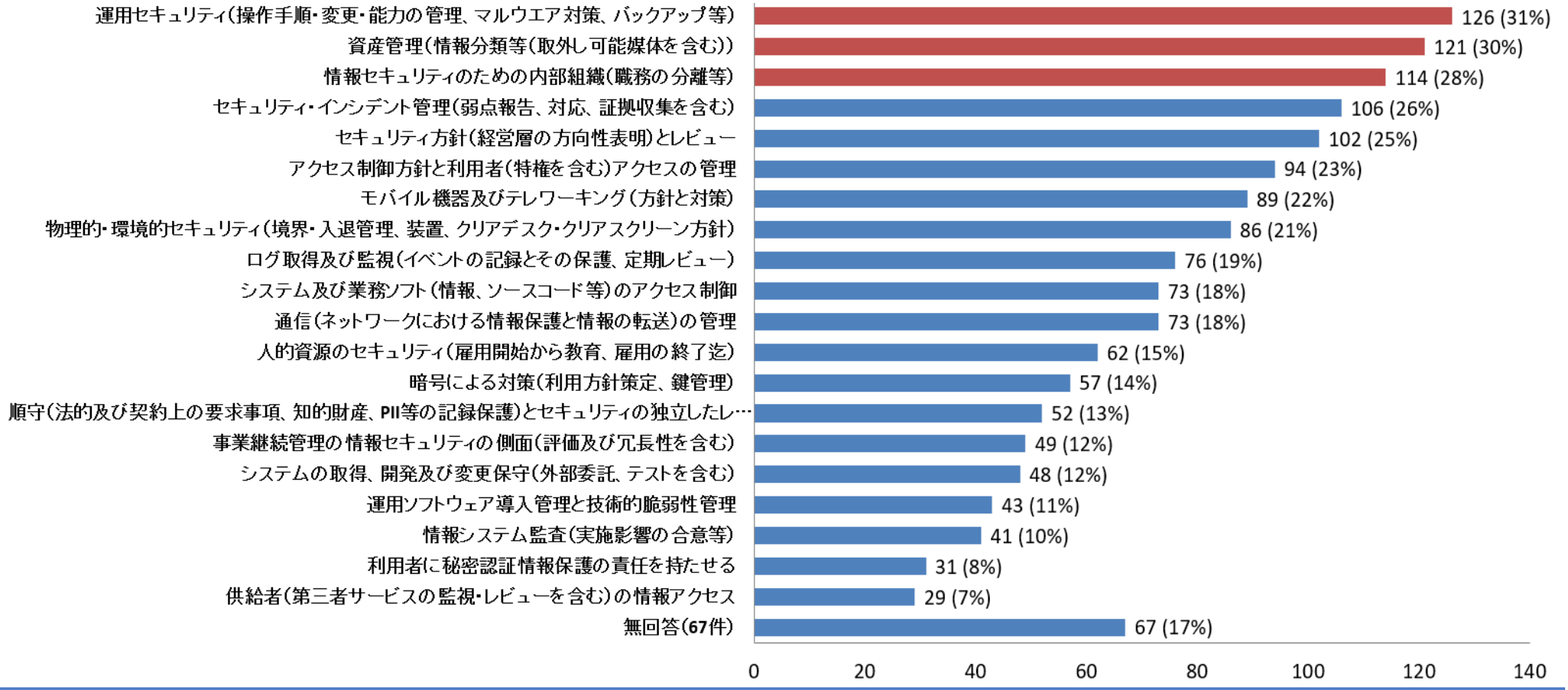
- 情報システム部門・情報セキュリティ部門が策定・見直しをしている
- 委員会組織で見直し、代表者が手続きを行っている
- 経営層（取締役以上）が策定・見直しをしている
- 情報システム部門・情報セキュリティ部門「以外」の部門が策定・見直しをしている
- その他
- 情報セキュリティポリシーはない
- 無回答（22件）

「情報システム部門・情報セキュリティ部門」が49%
「委員会組織」が29%で、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

設問14. 過去3年間で見直した情報セキュリティポリシーの管理策（複数回答）（N=401）

※設問 12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

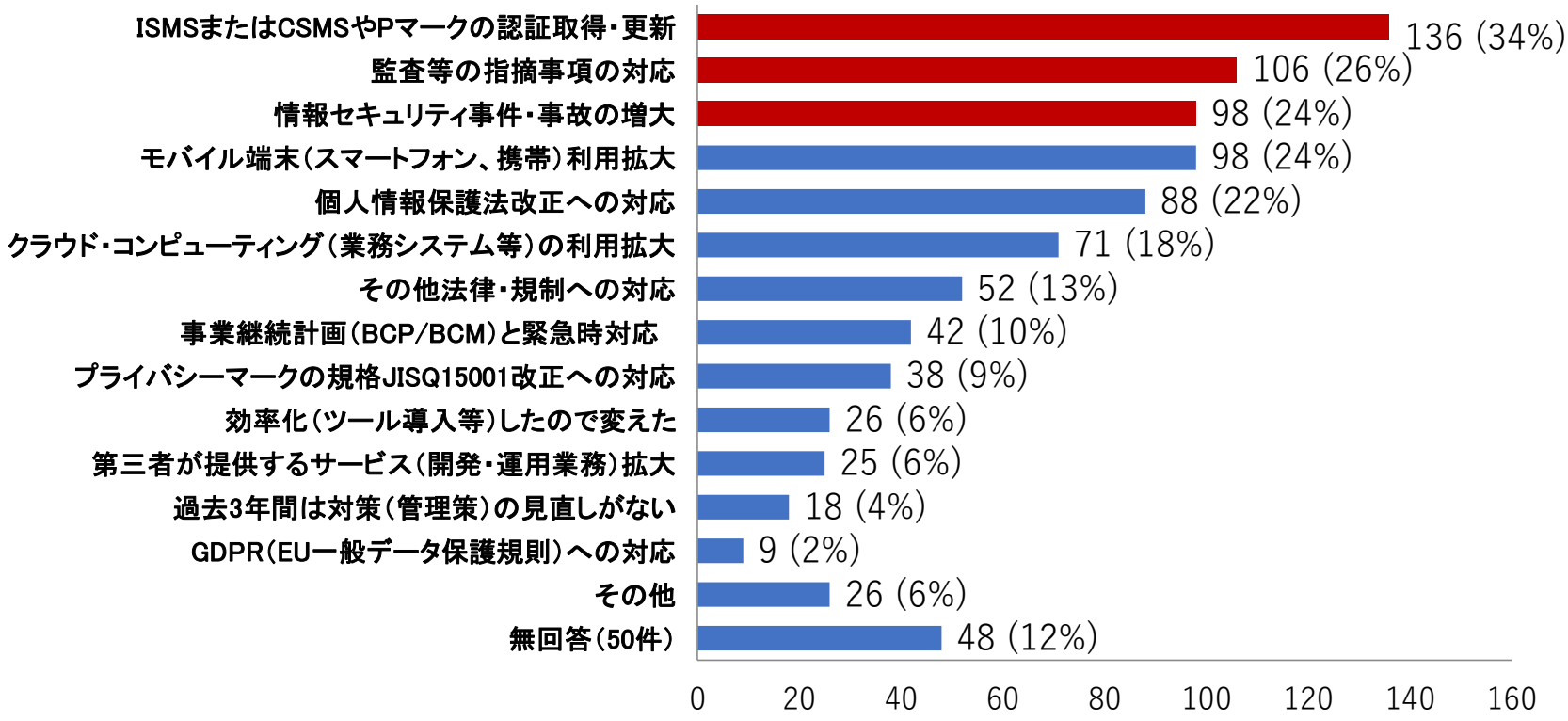


見直した管理策は、「運用セキュリティ」、「資産管理」の順で30%を超えて多い。
次いで「情報セキュリティのための内部組織」の管理策が多い

第2章　情報セキュリティマネジメントの取り組み状況

設問15. 情報セキュリティ管理策を新規導入・見直しした理由（複数回答）（N=401）

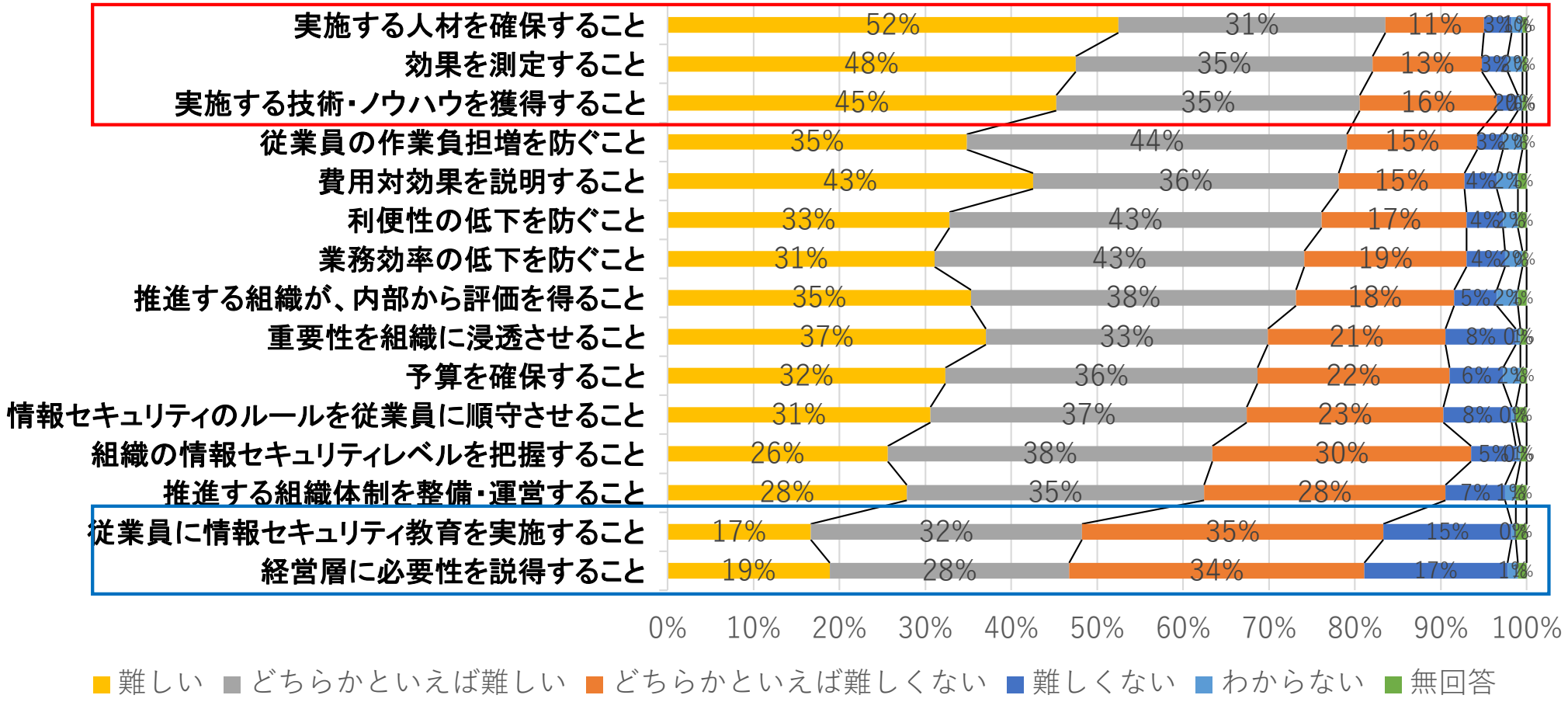
※設問 12で「情報セキュリティポリシーはない」以外を選択した組織を対象



「ISMSまたはCSMSやPマーク取得・更新」が136組織の34%と昨年同様最も多かった。「GDPRへの対応」はわずか9組織の2%であった。

第2章　情報セキュリティマネジメントの取り組み状況

設問16. 情報セキュリティ対策推進上の難しさを感じたのは？（N=402）

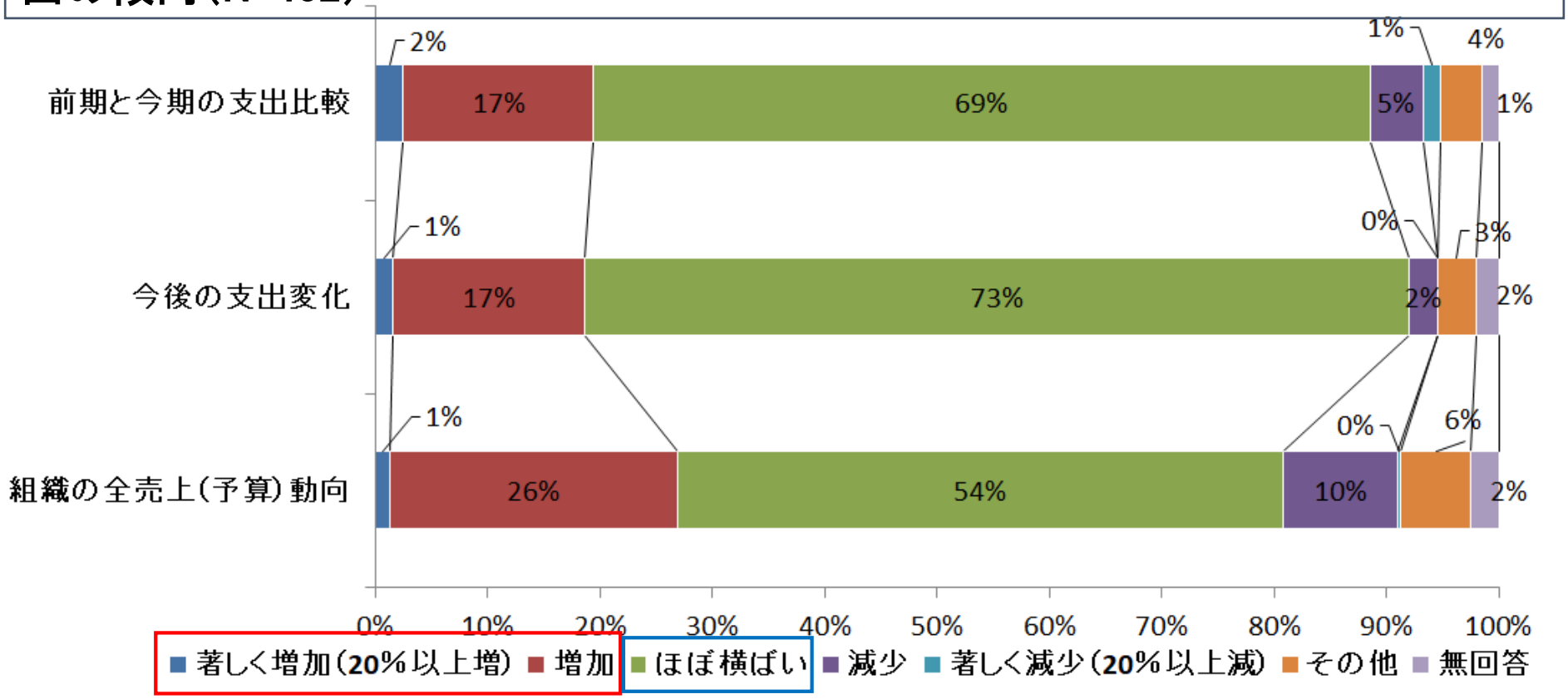


注：　＜難しい・どちらかと言えば難しい＞の多い順に表示

「実施人材を確保」、「効果測定」、「実施する技術・ノウハウを獲得すること」等が80%超で多い。逆に、「経営層に必要性を説得」、「従業員教育を実施」等は少ない。

第2章　情報セキュリティマネジメントの取り組み状況

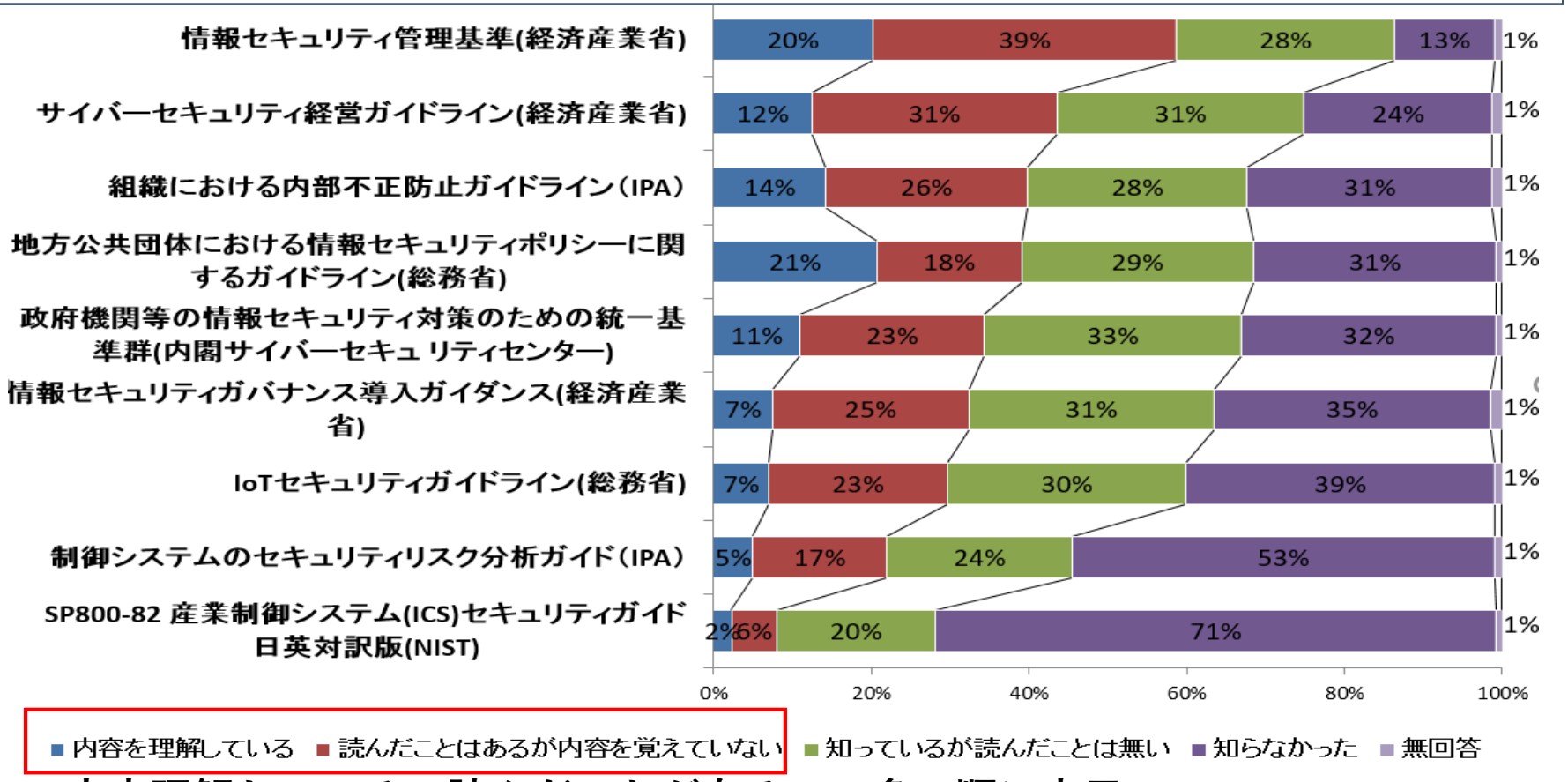
設問17. 売上（政府・自治体・大学等は予算）に対する情報セキュリティに関する支出の傾向（N=402）



いずれも「ほぼ横ばい」が50%以上を占めた。「著しく増加と増加」計が「全売上（予算）動向」で27%になった。

第2章　情報セキュリティマネジメントの取り組み状況

設問18. 情報セキュリティ政策（ガイドライン）の認知度　（N=402）



注：　＜内容理解している、読んだことが有る＞の多い順に表示

理解している・読んだことがある計で「情報セキュリティ管理基準」が236(59%)、「サイバーセキュリティ経営ガイドライン」が175(43%)と認知度が半数近くあるが、逆に制御・IoT向けのガイドライン等の認知度は低い。

第2章　情報セキュリティマネジメントの取り組み状況

調査結果：＜リスク分析＞

- 67%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（60%）は変わらない。
- 問題点は、「実施方法が分かる人材の不足」（67%）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（85%）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(49%)、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）」（31%）など具体的な項目が多くなった。見直し理由は、「ISMSやPマークの取得・更新」の認証対応が昨年同様最も多かった。
- 対策推進上の難しさは、「実施人材確保」、「効果を測定」が多く、「経営層に必要性を説得」、「従業員教育を実施」は半数以上が課題としていない。

第2章　情報セキュリティマネジメントの取り組み状況

調査結果：＜情報セキュリティに関する支出＞

- いずれも「ほぼ横ばい」が50%以上を占めた。「著しく増加と増加」計が「全売上（予算）動向」で27%になった。

＜情報セキュリティ政策（ガイドライン）の認知度＞

- 理解している・読んだことがある計で「情報セキュリティ管理基準」が236(59%)、「サイバーセキュリティ経営ガイドライン」が175(43%)と認知度が半数近くあるが、逆に制御・IoT向けのガイドライン等の認知度は低くかった。

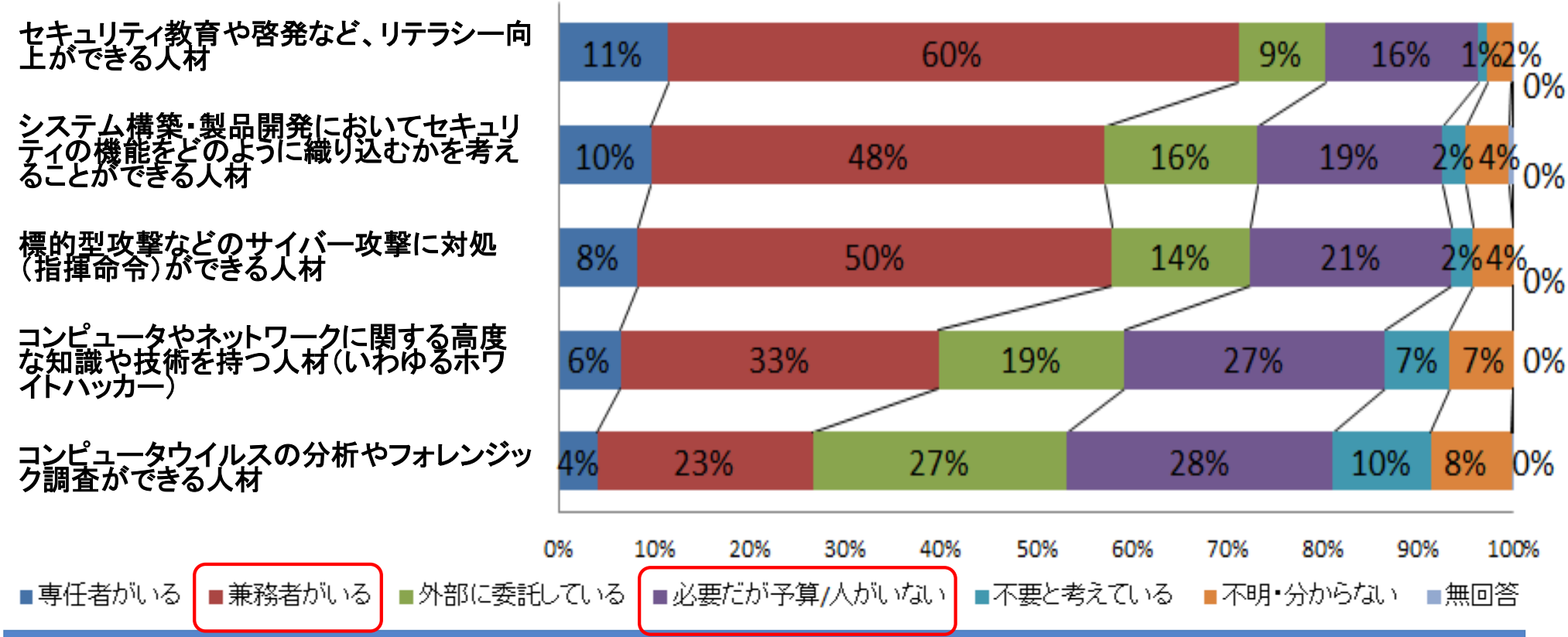
第3章
情報セキュリティ対応体制・人材に関する状況

調査概要：

情報セキュリティ対策に関わる人材の有無、
橋渡し人材の必要性など

第3章　情報セキュリティ対応体制・人材に関する状況

設問19　自組織のセキュリティ対策に関わる人材の有無（N=402）

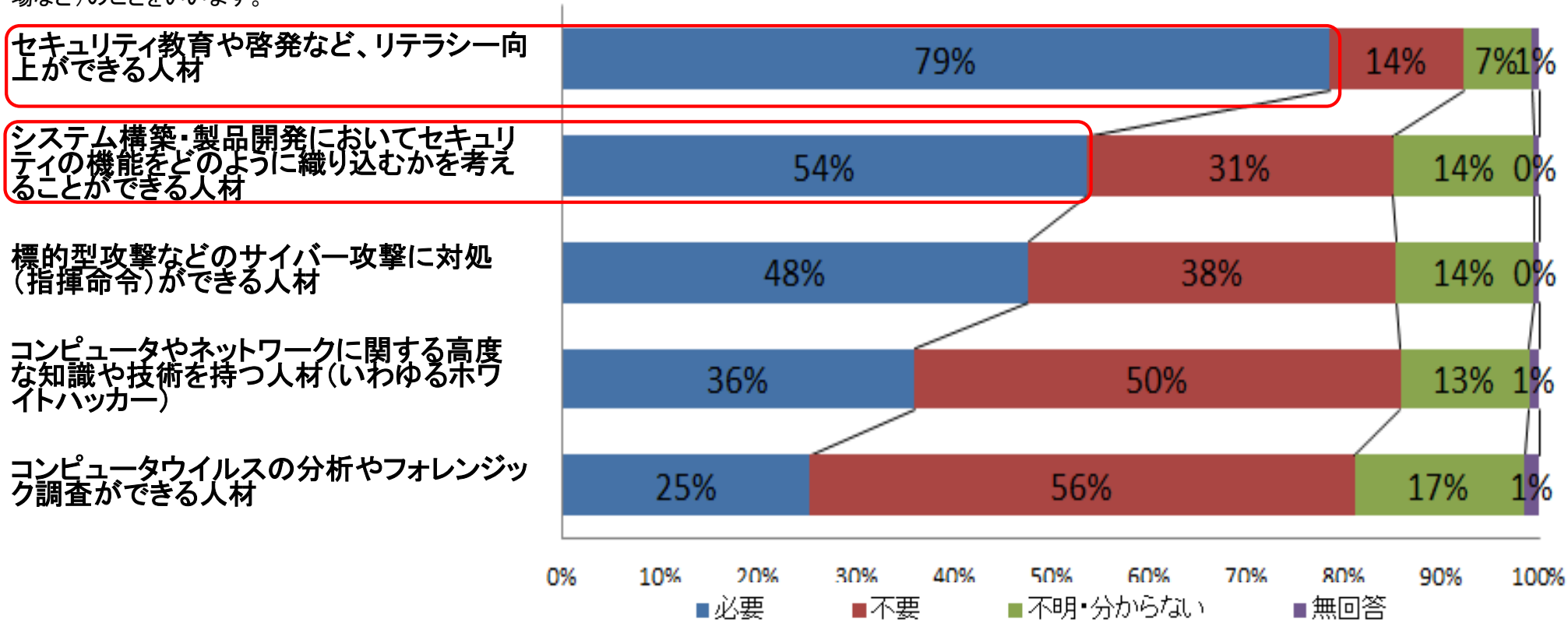


- 情報セキュリティインシデントに関わる技術者は、組織の中において、専任に従事しているより、ほかの業務との兼務することが多い。
- ホワイトハッカーやフォレンジック調査などができる高度技術者人材が不足している。外部委託もふくめて確保が難しい

第3章　情報セキュリティ対応体制・人材に関する状況

設問20　自組織の非IT部門でも必要と思うセキュリティ人材について（N=402）

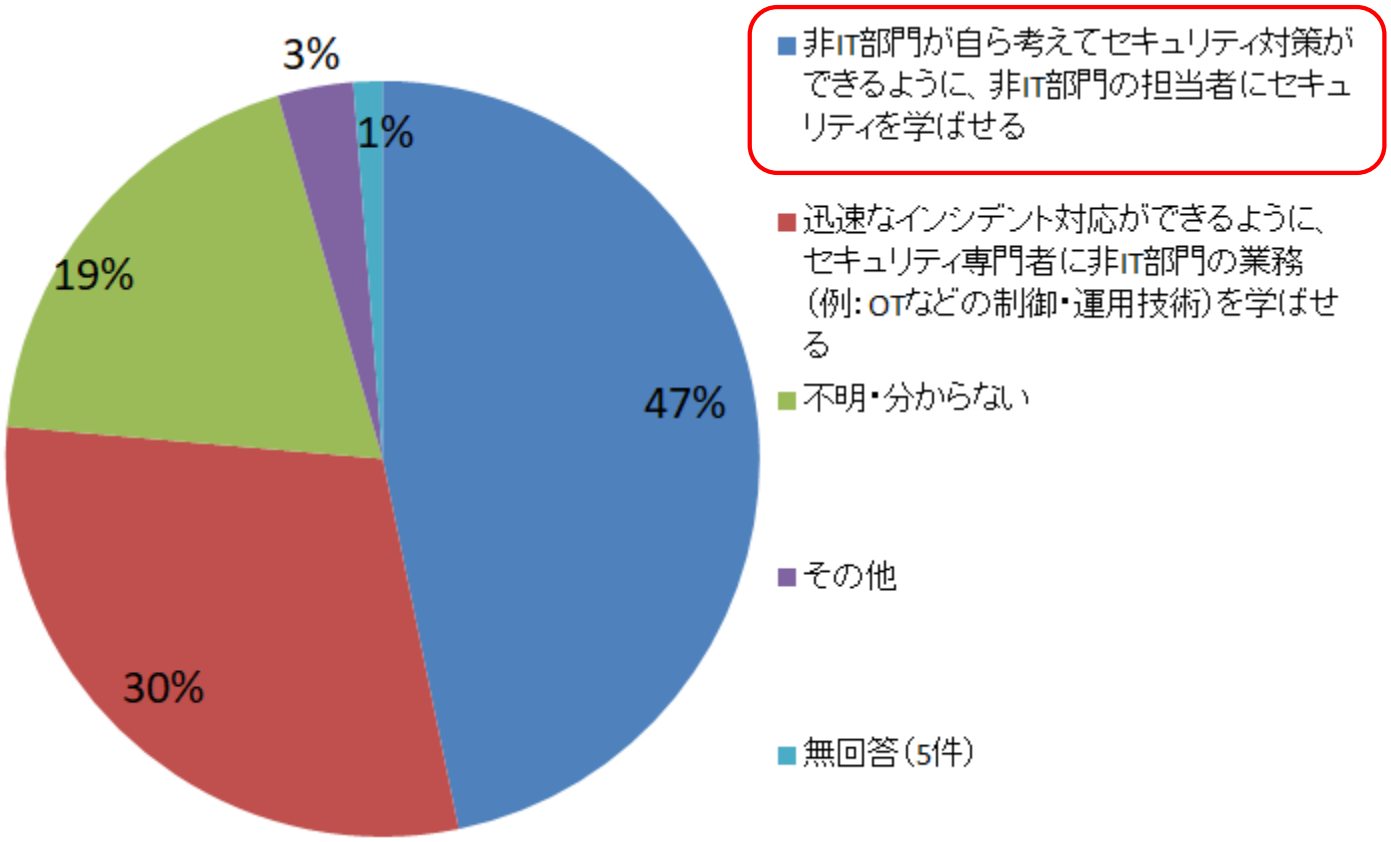
※本設問における「非IT部門」とは、会社の情報システムの企画・開発・運用・委託といった業務を主として実施していない部門（事業部門、営業部門、製造現場など）のことをいいます。



- 非IT部門においても、セキュリティ教育・啓発できる人材や、セキュリティを自部門にどのように織り込むかを考えることができる人材を必要としていることが分かった。

第3章　情報セキュリティ対応体制・人材に関する状況

設問21　自組織のセキュリティ人材育成を行うための仕組み作りについて（N=402）

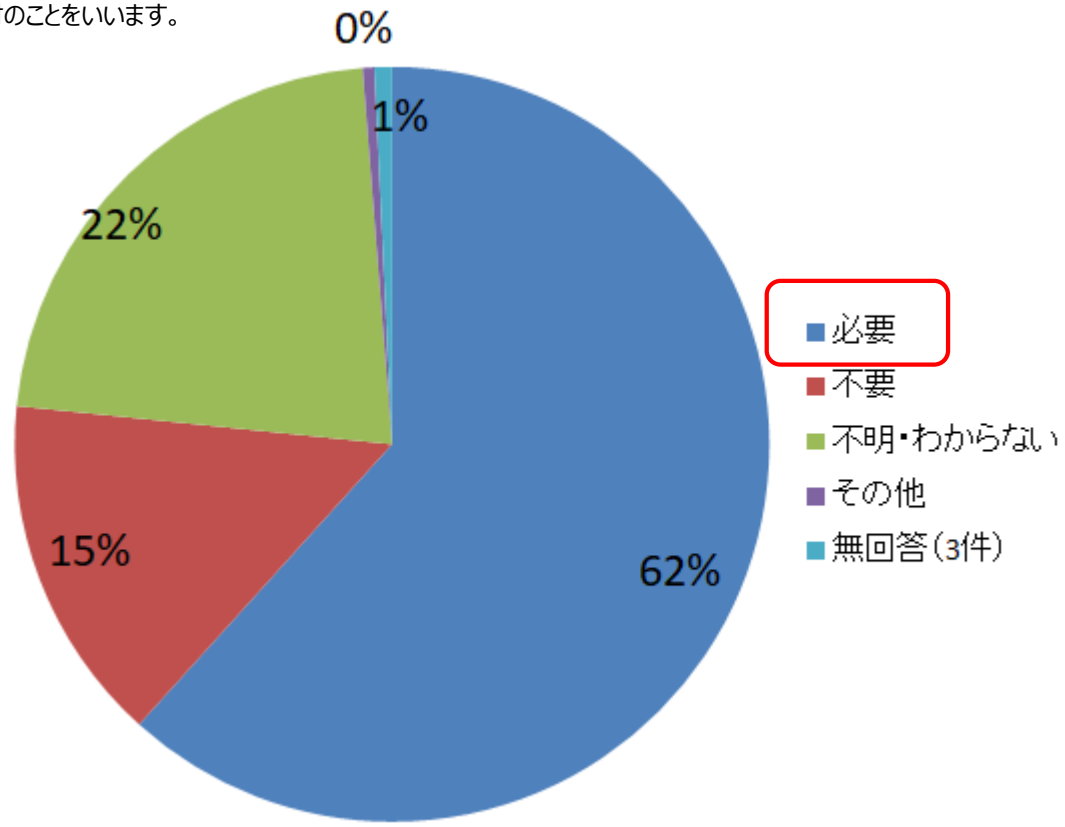


- 非IT部門が自ら考えてセキュリティ対策ができるようにしたいと考えている組織が47%で最も多い。

第3章　情報セキュリティ対応体制・人材に関する状況

設問22　自組織の情報キュリティ対策における橋渡し人材の必要性（N=402）

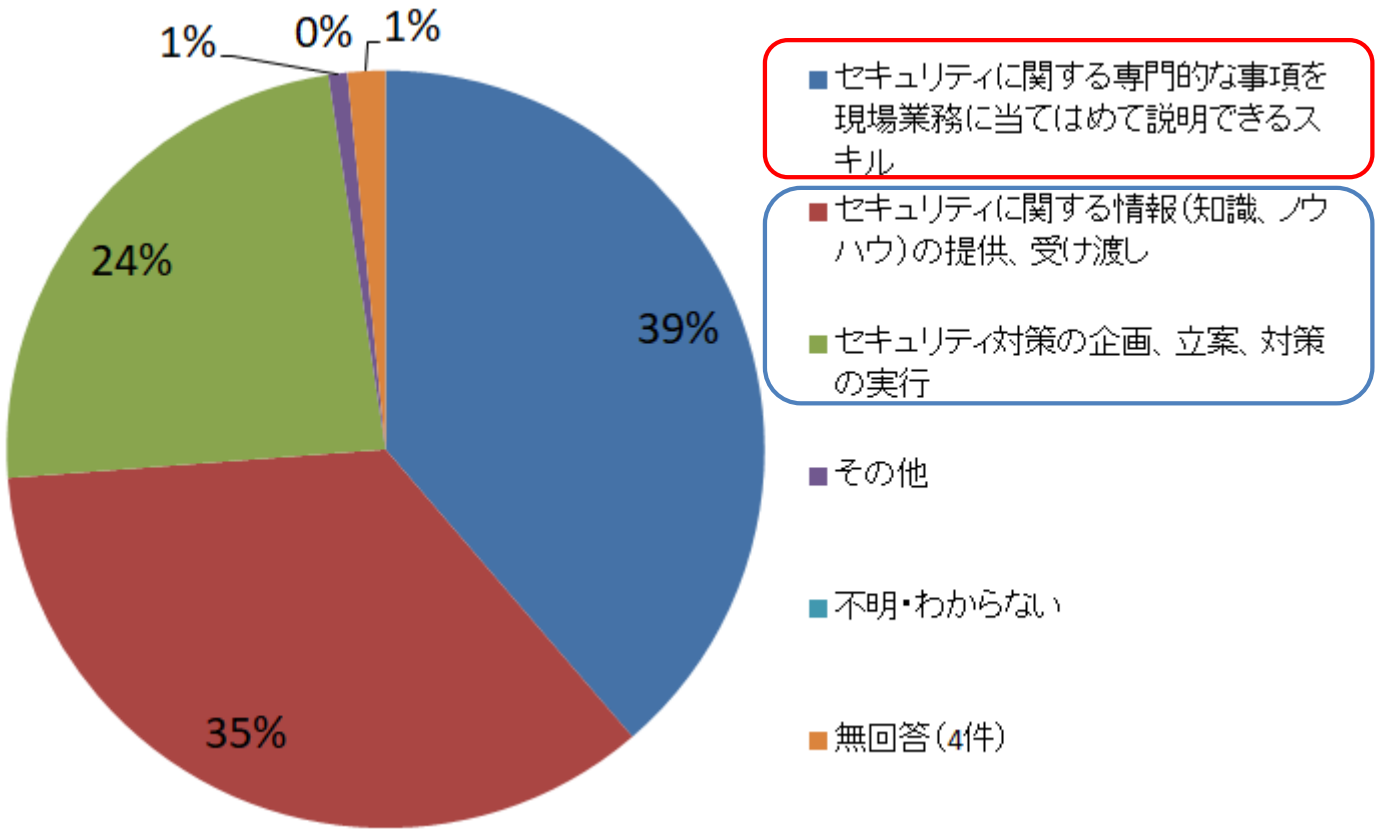
※本設問における「橋渡し人材」とは、情報セキュリティに関する知識を有し、経営層や非IT部門など会社の幅広いに部門を対象として、サイバーセキュリティ方策の企画、立案、教育などのサポートができる人材のことをいいます。



- 橋渡し人材を必要としている組織が62%と多いことが分かったが、不明・分からないと回答している組織も22%あり、「橋渡し人材」のより明確な定義が必要と考える。

第3章　情報セキュリティ対応体制・人材に関する状況

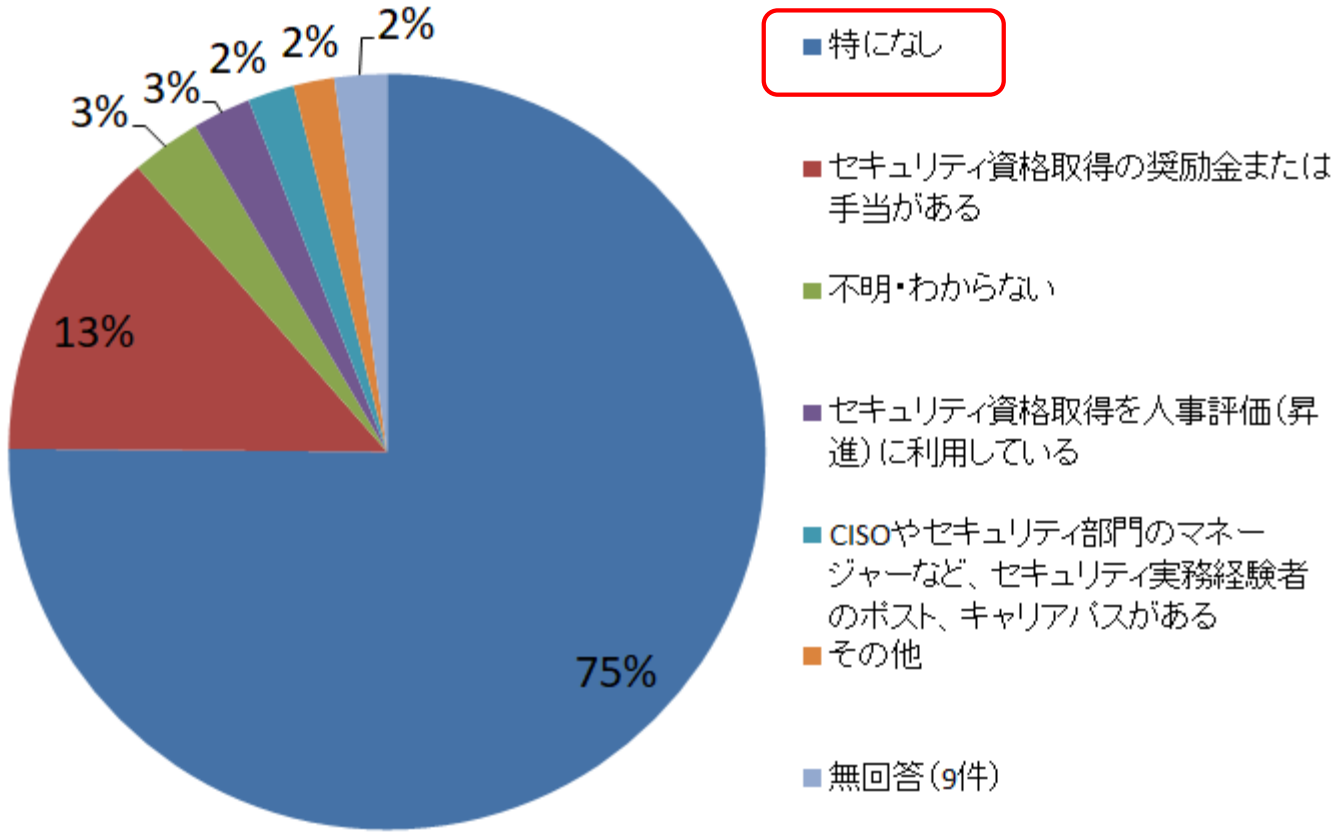
設問23　橋渡し人材に一番期待する役割（N=248：設問22で「必要」と答えた方）



- 「セキュリティに関する専門的な事項を現場業務に当てはめて説明できるスキル」が39%で最も多いが、「セキュリティに関する情報（知識、ノウハウ）の提供」35%、「セキュリティ対策の企画、立案、対策実行」24%と続いており、現場が求める橋渡し人材のニーズも分かれていると考えられる。

第3章　情報セキュリティ対応体制・人材に関する状況

設問24　自組織のセキュリティ人材に対するインセンティブの有無（N=402）



- 「特になし」が75%最も多く、多くの企業・組織においてインセンティブは一般的ではないことが分かった。

第3章　情報セキュリティ対応体制・人材に関する状況

調査結果：

- 自組織の情報セキュリティ対策に関わる人材は、組織の中において、専任に従事しているより、他の業務と兼務することが多い。また、ホワイトハッカーやフォレンジック調査などができる高度技術者人材が不足している。外部委託もふくめて確保が難しい。
- 非IT部門においても、セキュリティ教育・啓発や、セキュリティを自部門にどのように織り込むかを考えることができる人材を必要としていることが分かった。
- 自組織のセキュリティ人材育成を行うための仕組み作りについては、セキュリティ専門者に非IT部門の業務を学ばせるよりも、非IT部門が自ら考えてセキュリティ対策ができるようにしたいと考えている組織が47%で最も多い。
- 橋渡し人材を必要としている組織が62%あり、必要性が高いことが分かったが、現場が求める橋渡し人材のニーズは一つではなく、(1)専門的な事項を現場業務に当てはめて説明できるスキル、(2)知識・ノウハウの提供、(3)企画、立案、対策実行、の3つに分かれる結果となった
- セキュリティ人材に関するインセンティブは、「特になし」が75%最も多く、多くの企業・組織においてインセンティブは一般的ではないことが分かった。

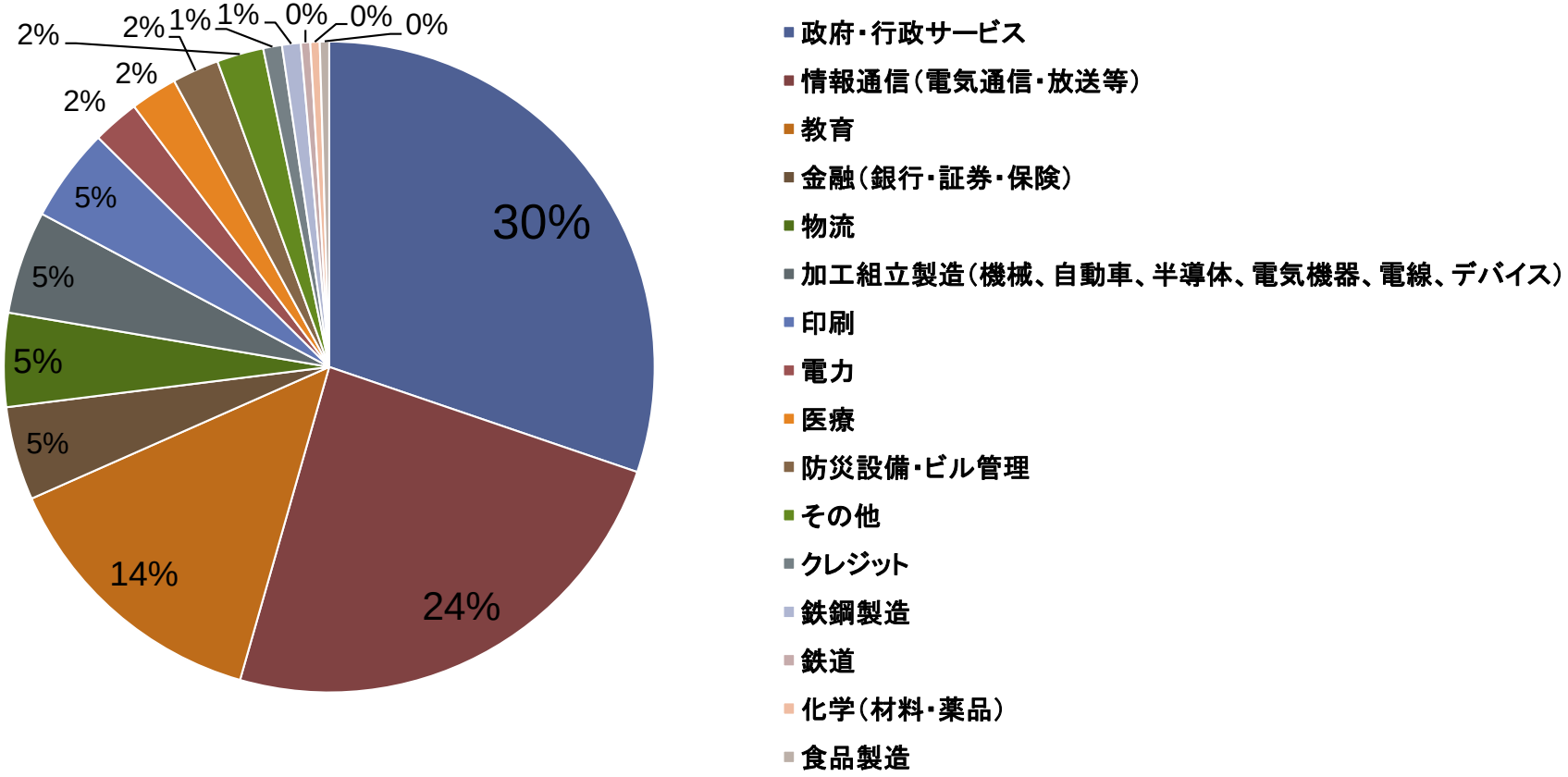
第4章
制御システムにおける
情報セキュリティに関する課題

調査概要：

制御システムにおけるセキュリティ管理状況、セキュリティ課題等

第4章　制御システムにおける情報セキュリティに関する課題

設問25　制御システムの分野(N=215)※

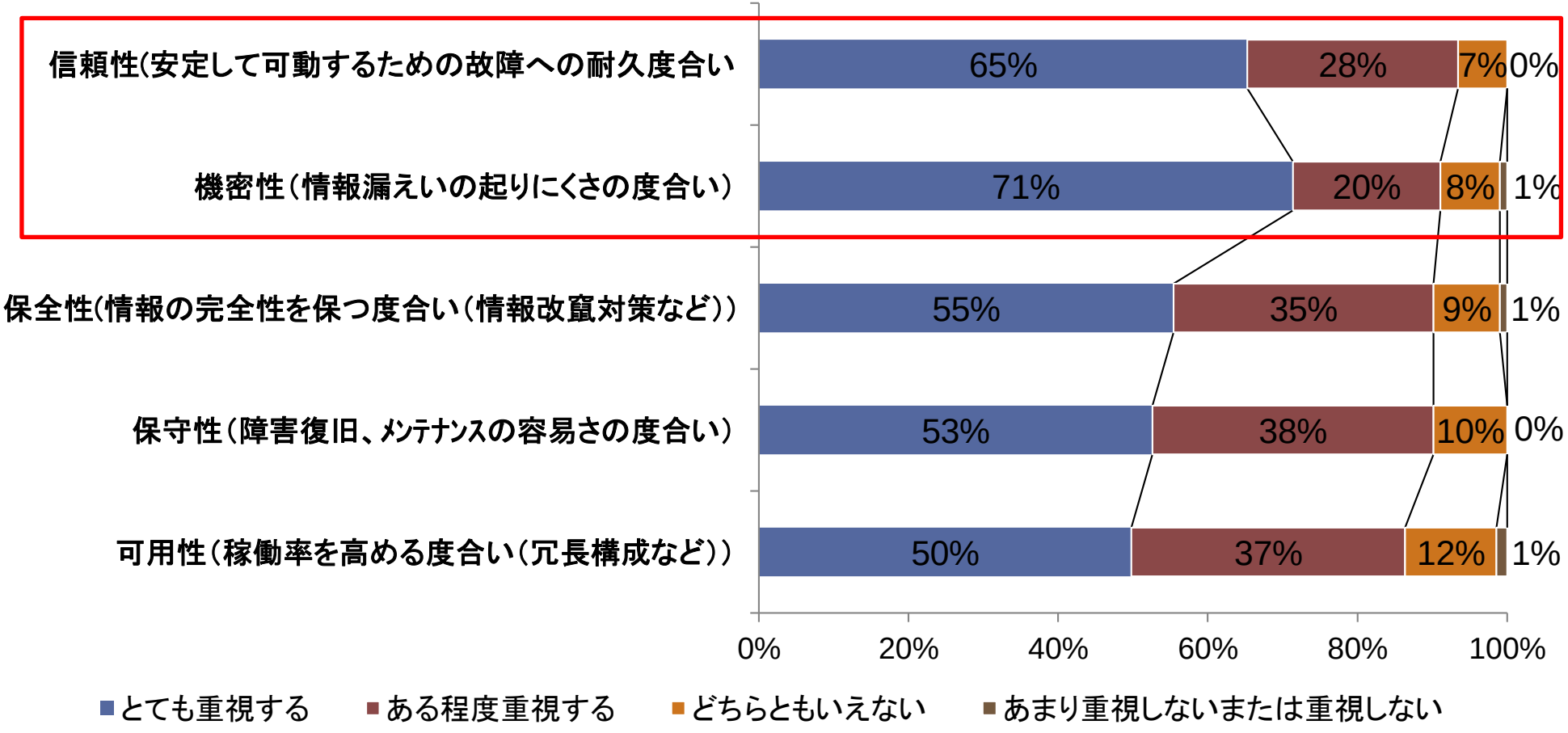


※「制御システムを持っていない」の回答(187)以外を集計

「政府行政サービス」が30%で最も多く、「情報通信（電気通信・放送等」が24%と次いで多かった。

第4章　制御システムにおける情報セキュリティに関する課題

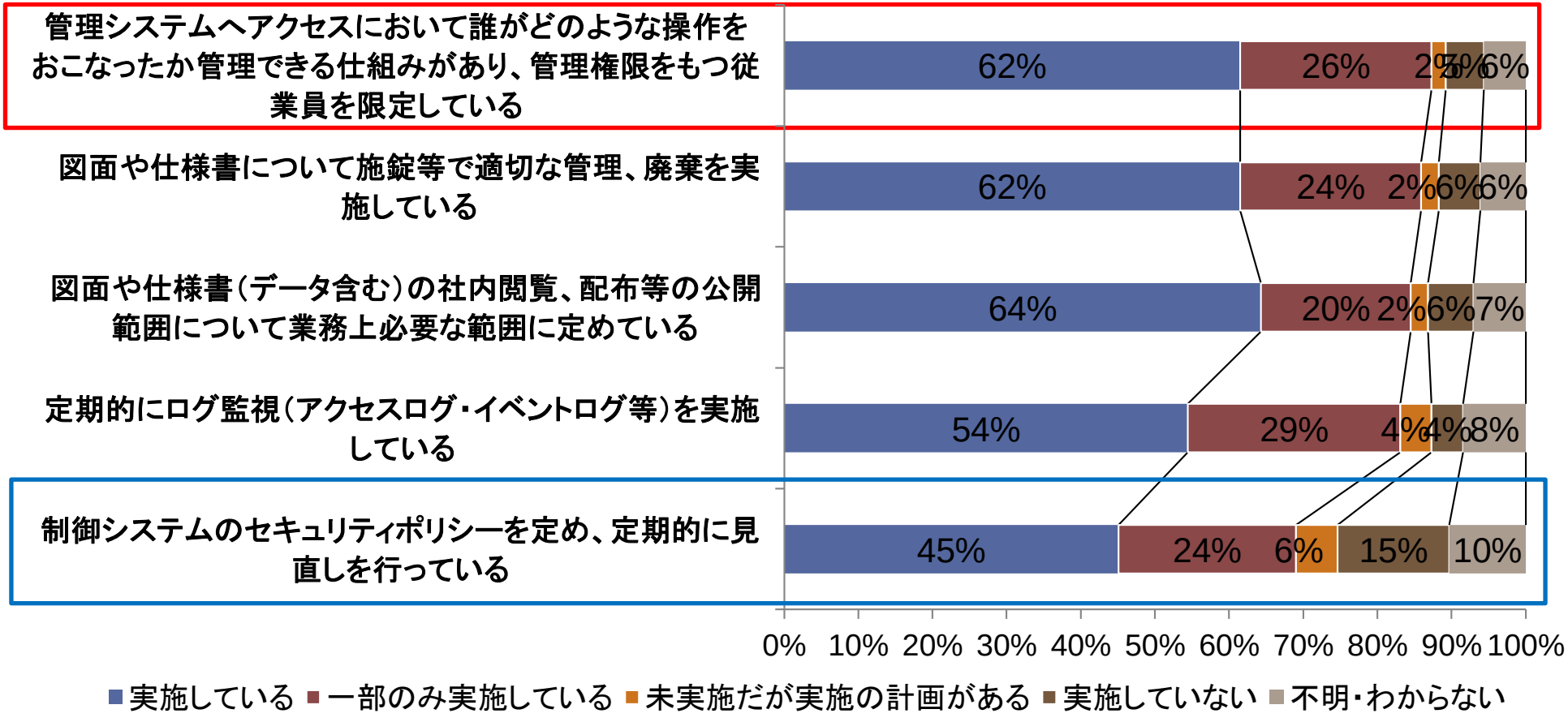
設問26　制御システムのRASIS重要性（N=213）



「とても重視する」を最も選んだのは機密性であるが、「とても重視する」と「ある程度重視する」計では信頼性が最も高い。

第4章　制御システムにおける情報セキュリティに関する課題

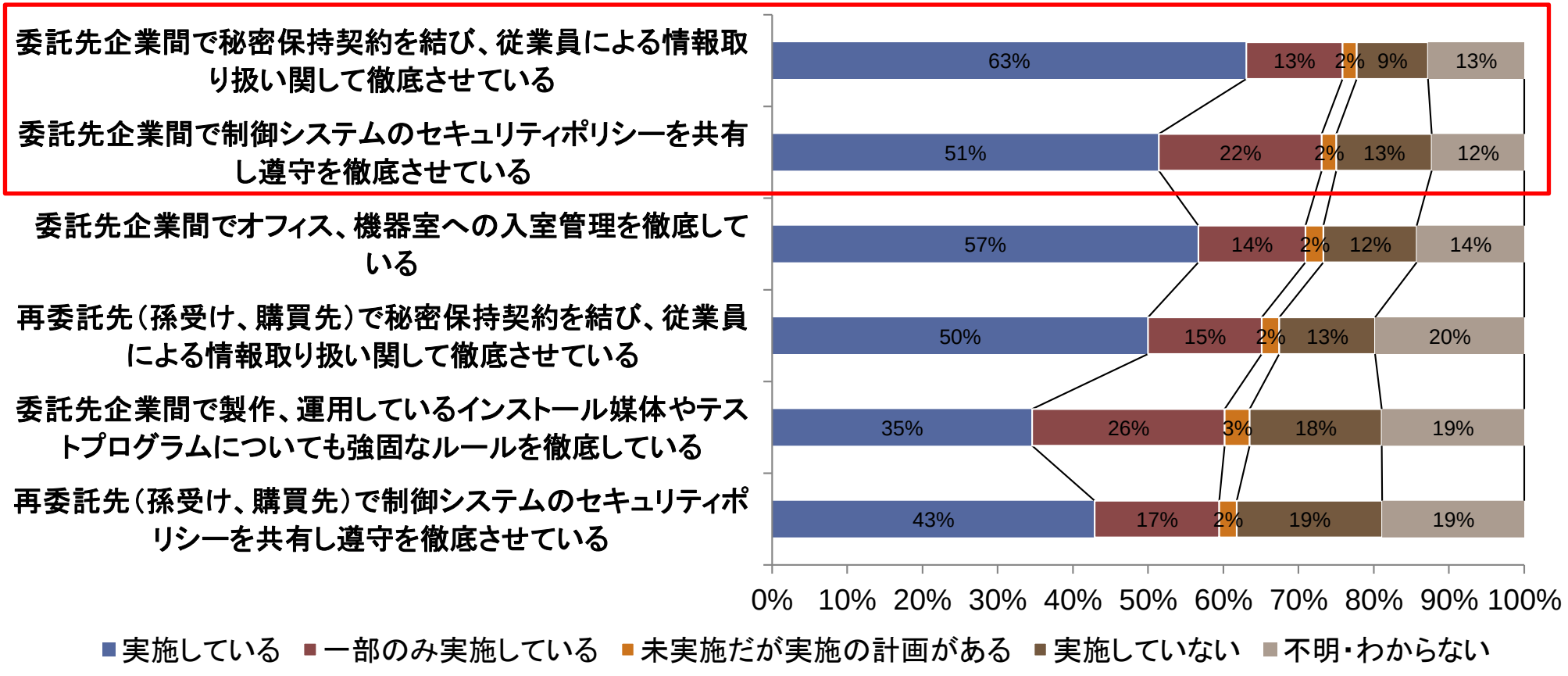
設問27　制御システムの管理状況（N=213）



実施対策で最も高かったのは「管理システムへのアクセス管理の仕組みがあり、管理権限を限定している」の88%で、「制御システムのセキュリティポリシーを定め、定期的に見直しを行っている」が最も低い69%であった。

第4章　制御システムにおける情報セキュリティに関する課題

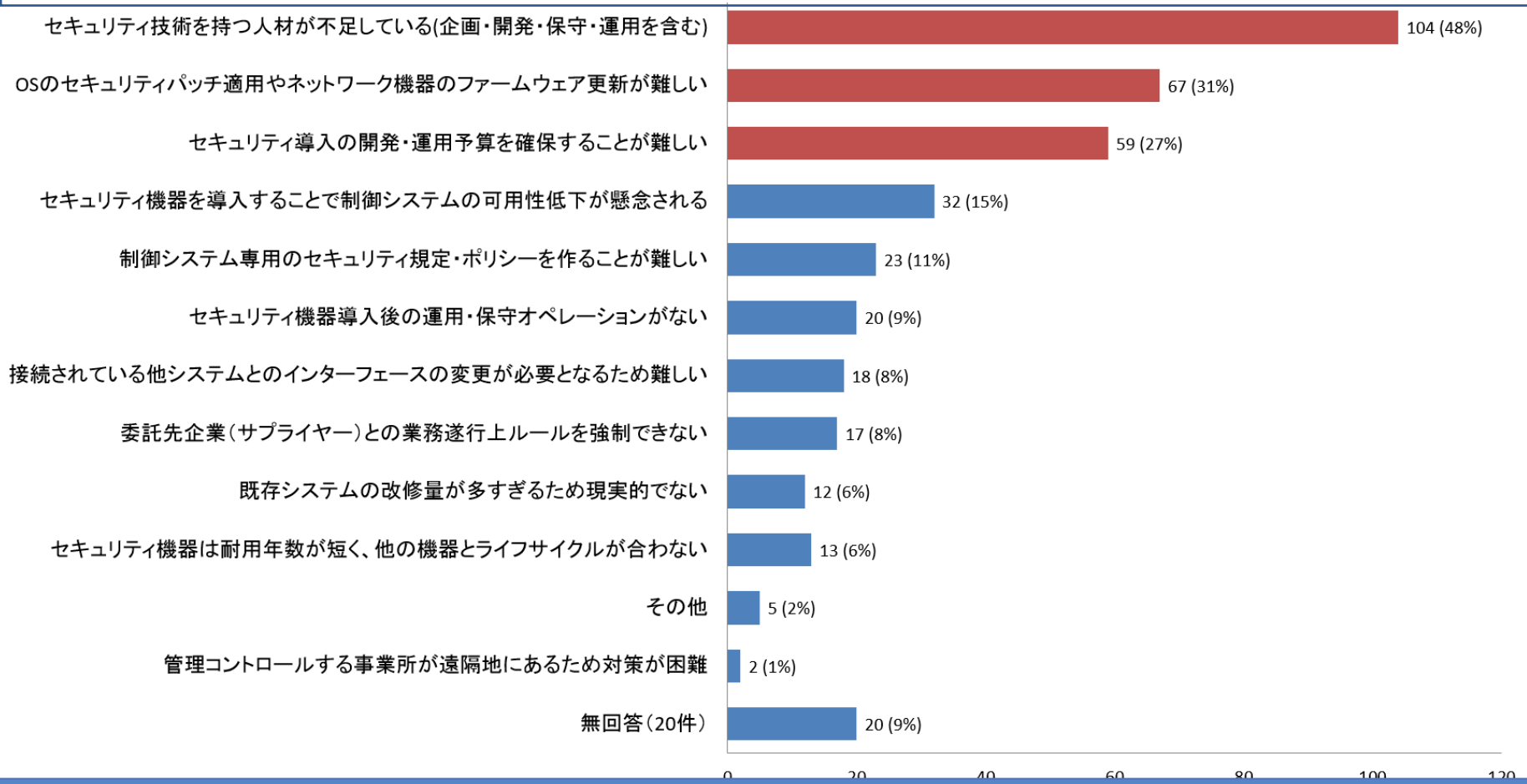
設問28　制御システムにおける委託先のセキュリティマネジメント（N=212）



実施している対策で最も高かったのは「委託先企業間で秘密保持契約を結び、情報取扱を徹底させている」の76%で、「委託先企業間で制御システムのセキュリティポリシーを共有し遵守させている」が次いで多い73%であった。

第4章　制御システムにおける情報セキュリティに関する課題

設問29　制御システムのセキュリティ対策を困難とさせている課題(N=195)



困難となる課題で最も高かったのは「セキュリティ技術を持つ人材が不足している」の48%で、「OSのセキュリティパッチ適用やネットワーク機器のファームウェア更新が難しい」が次いで多い31%であった。

第4章　制御システムにおける情報セキュリティに関する課題

調査結果：

- RASISの重要度で、「とても重視する」を最も選んだのは機密性であるが、「とても重視する」と「ある程度重視する」計では信頼性が最も高い。
- セキュリティ対策の実施状況で最も高かったのは「管理システムへのアクセス管理の仕組みがあり、管理権限を限定している」の88%で、「制御システムのセキュリティポリシーを定め、定期的に見直しを行っている」が最も低い69%であった。
- 委託先のセキュリティマネジメントで、最も高かったのは「委託先企業間で秘密保持契約を結び、情報取扱を徹底させている」の76%で、「委託先企業間で制御システムのセキュリティポリシーを共有し遵守させている」が次いで多い73%であった。
- 対策を困難とさせている課題で最も高かったのは「セキュリティ技術を持つ人材が不足している」の53%で、「OSのセキュリティパッチ適用やネットワーク機器のファームウェア更新が難しい」が次いで多い34%であった。

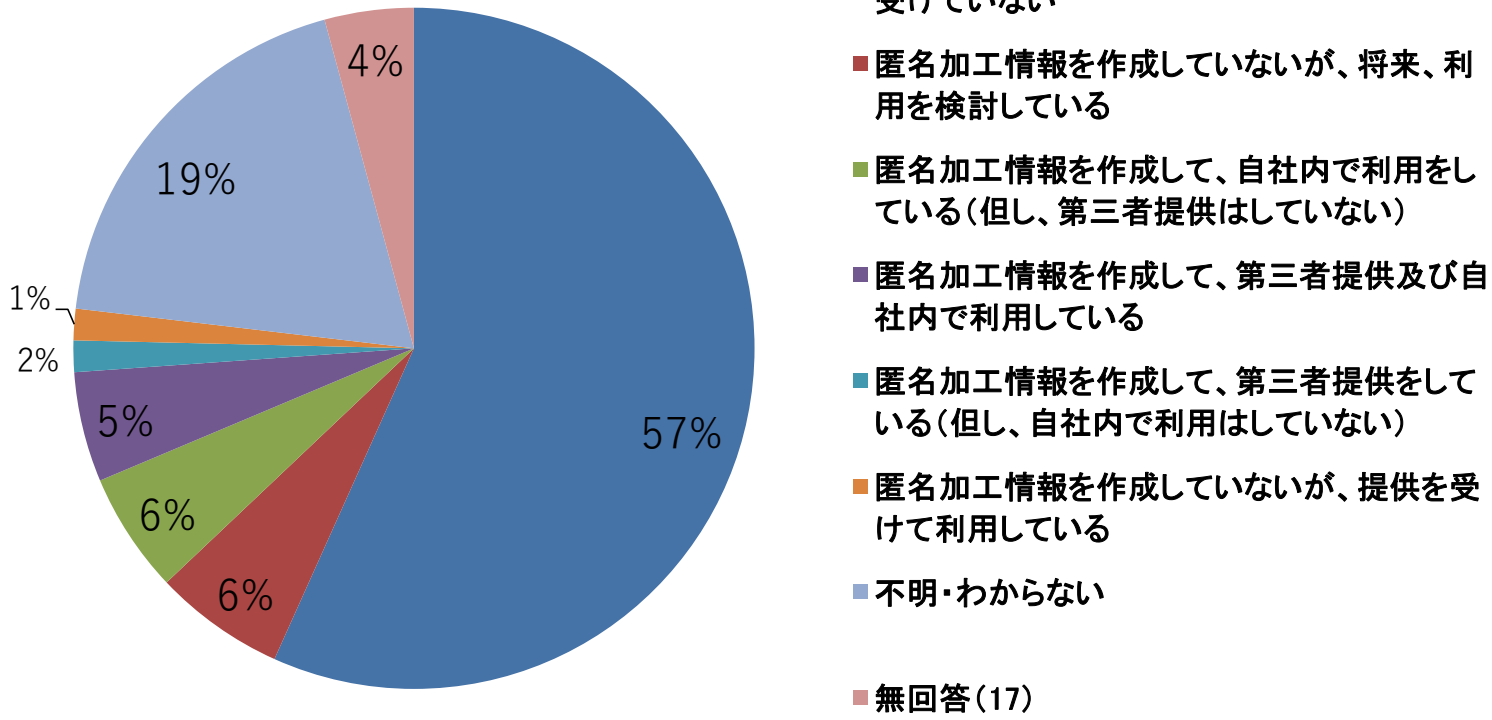
第5章
匿名加工情報の取扱い

調査概要：

匿名加工情報の利活用状況、利活用しているデータ等

第5章　匿名加工情報の取扱い

設問30　匿名加工情報の作成・利用をおこなっているか（N=402）

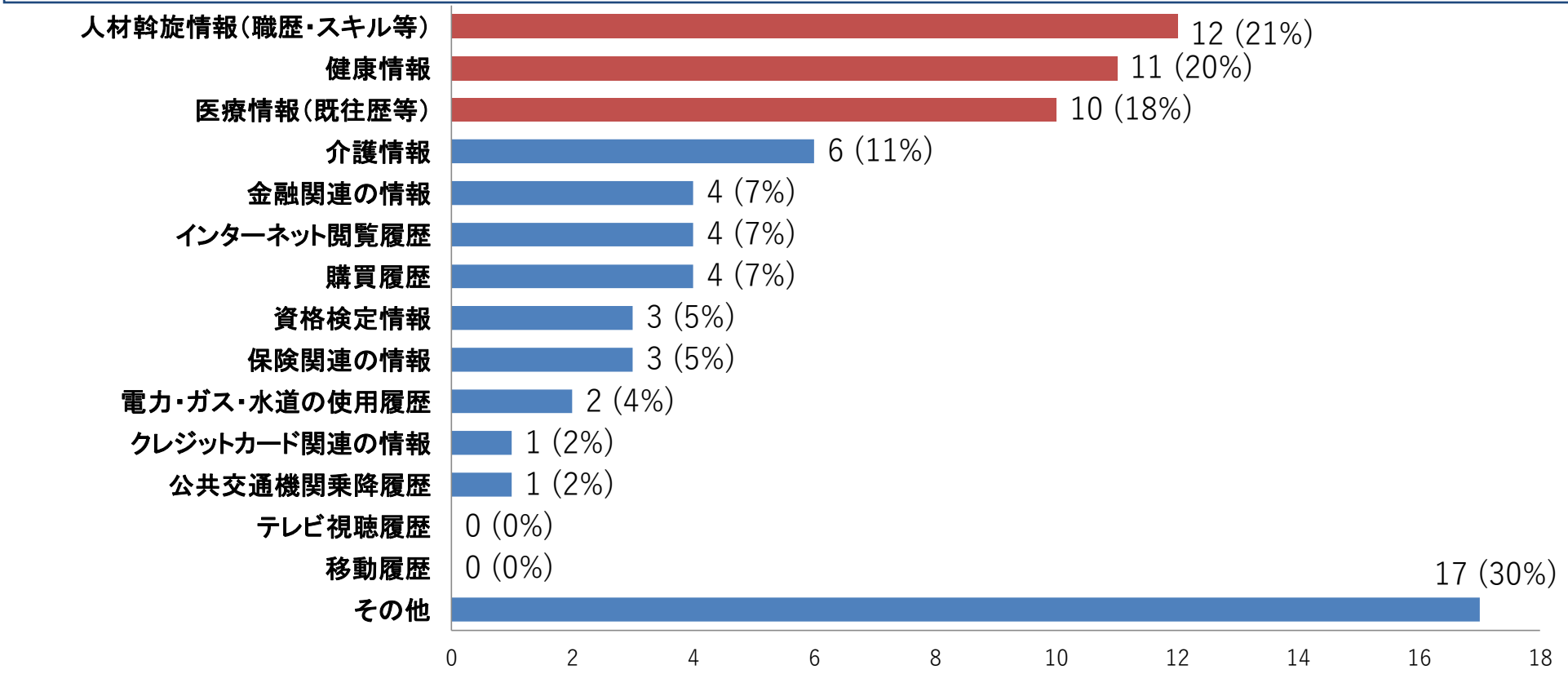


- 「作成していない、かつ提供を受けていない」が57%
- 「将来利用を検討している」が6%、「現在作成もしくは提供を受けている」は14%であり、合わせると20%
- 「不明・分からない」が19%

第5章　匿名加工情報の取扱い

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

設問31　作成・利用している匿名加工情報（N=56 ※Q30で匿名加工情報利用の回答母数のみ抽出）

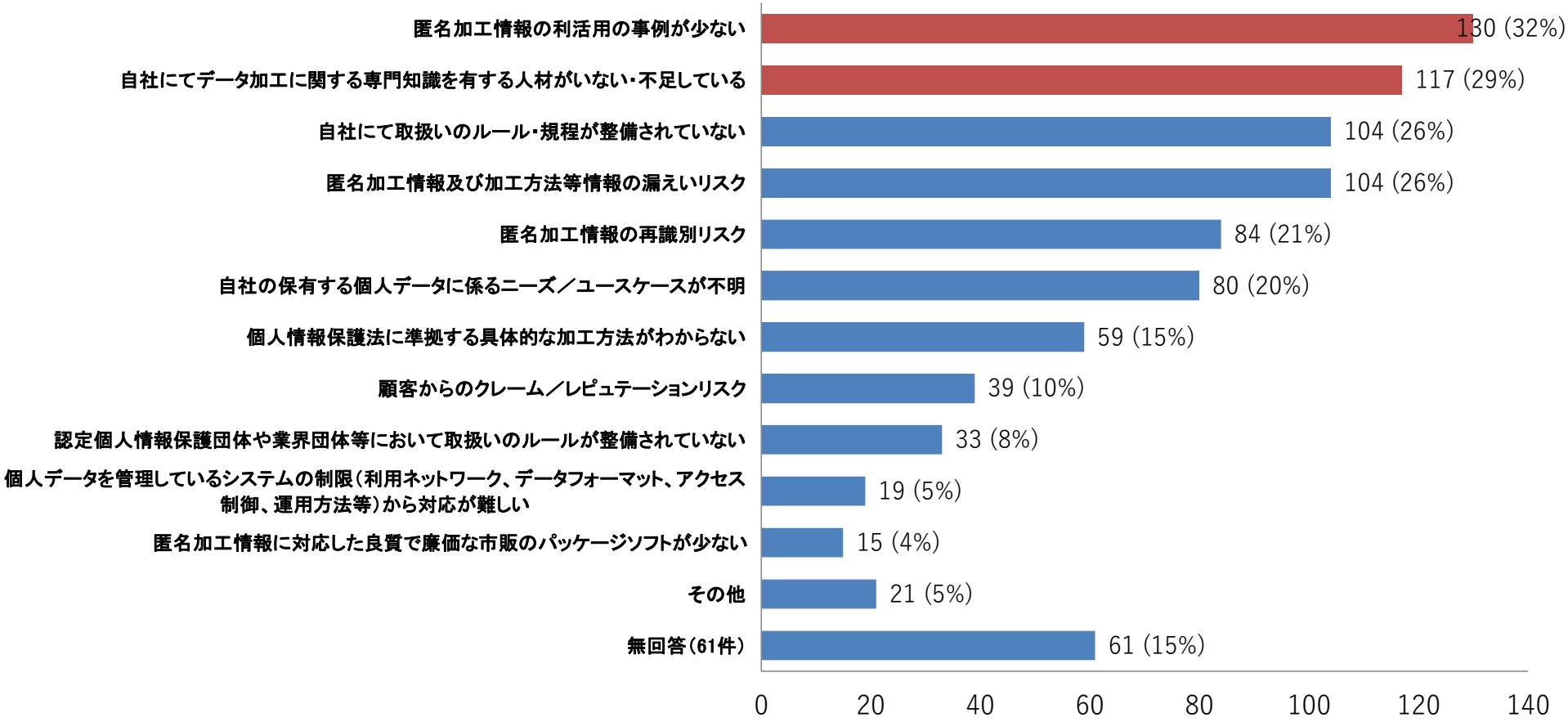


- 人材斡旋情報（職歴・スキル等）が12件と最も多く、次に医療情報（既往歴等）が11件、介護情報が10件
- その他として、学籍情報、授業履歴、成績情報、研究データ、住所、特定個人情報、履歴書、セミナー来場者情報、応対履歴等がある

第5章　匿名加工情報の取扱い

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

設問32　匿名加工情報作成時に感じる阻害要因、普及が進まない阻害要因（N=402）

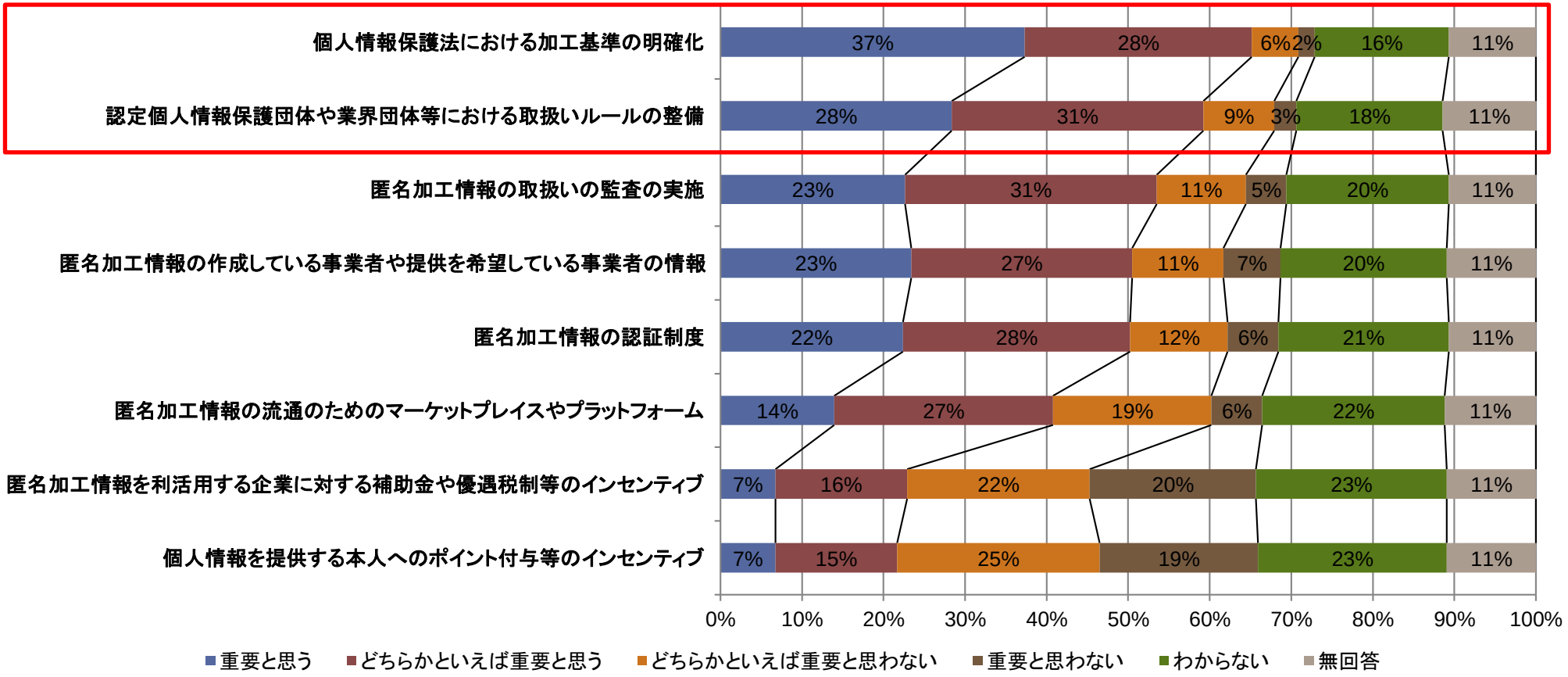


- 1位は「匿名加工情報の利活用の事例が少ない」、2位は「自社にてデータ加工に関する専門知識を有する人材がいない・不足している」その他としては、「必要がない」「予定がない」等である。

第5章　匿名加工情報の取扱い

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

設問33　匿名加工情報の普及にあたり重要と思うもの（N=402）



- 「重要と思う」・「どちらかと言えば重要と思う」の多い順で、1位は「個人情報保護法における加工基準の明確化」、2位は「認定個人情報保護団体や業界団体等における取扱いルールの整備」である。

第5章　匿名加工情報の取扱い

調査結果：

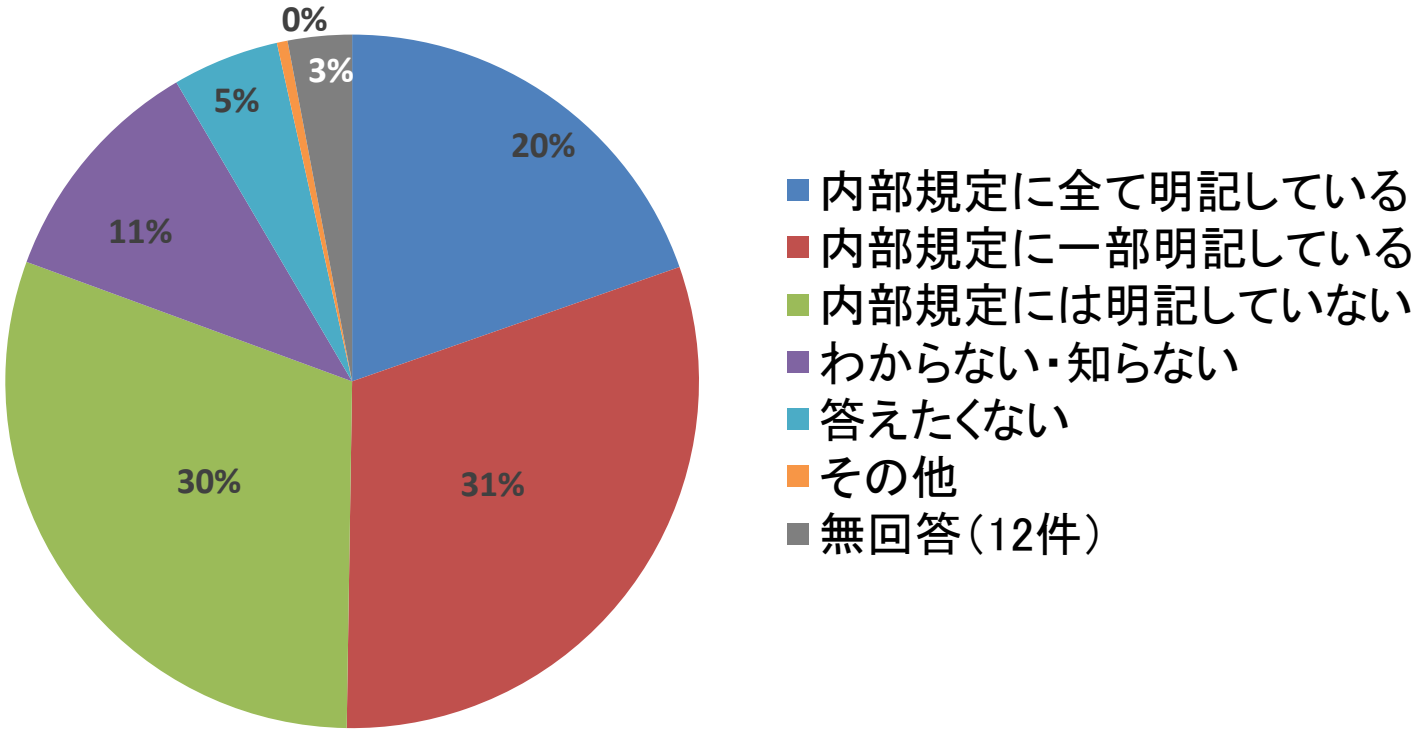
- 匿名加工情報の利活用について、「作成していない、かつ提供を受けていない」が57%。「将来利用を検討している」が6%、「現在作成もしくは提供を受けている」は14%であり、合わせると20%、「不明・分からない」が19%。
- 作成・利用の対象情報は、人材斡旋情報（職歴・スキル等）が12件と最も多く、次に医療情報（既往歴等）が11件、介護情報が10件。その他として、学籍情報、授業履歴、成績情報、研究データ、住所、特定個人情報、履歴書、セミナー来場者情報、応対履歴等がある。
- 利活用の阻害要因としては、1位は「匿名加工情報の利活用の事例が少ない」、2位は「自社にてデータ加工に関する専門知識を有する人材がいない・不足している」、3位は「自社にて取扱いのルール・規程が整備されていない」・「匿名加工情報及び加工方法等情報の漏えいリスク」である。その他としては、「必要がない」「予定がない」等がある。
- 今後の普及にあたり重要なのは、1位は「個人情報保護法における加工基準の明確化」、2位は「認定個人情報保護団体や業界団体等における取扱いルールの整備」である。

第6章
情報セキュリティマネジメントの「例外措置」

調査概要：例外措置の有無、策定部門の傾向、現場でのカスタマイズ程度、見直し頻度、具体的な管理策での通常規定／例外措置の策定傾向

第6章　情報セキュリティマネジメントの「例外措置」

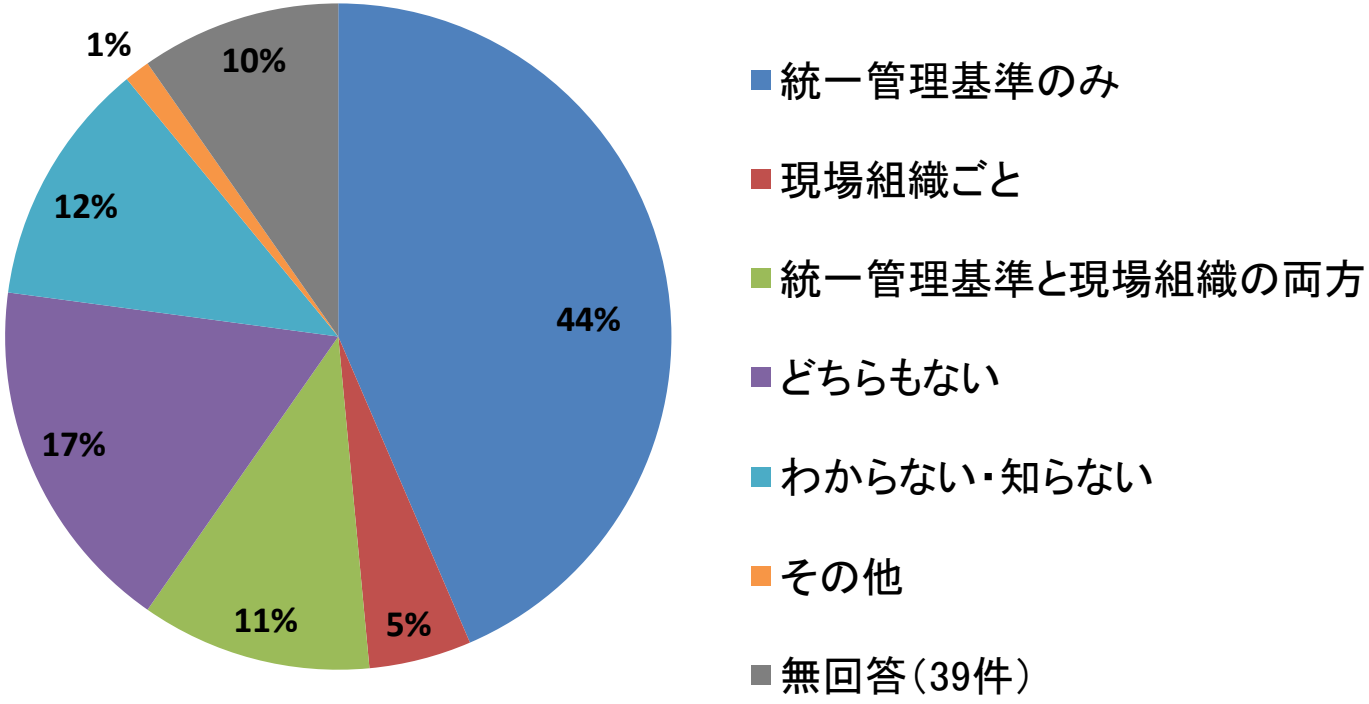
設問34. 情報セキュリティに関わる内部規定全般においての「例外規定」の有無
(N=402)



- 例外措置の策定が内部規定に記載されている割合はされていない割合より21ポイント高い。

第6章　情報セキュリティマネジメントの「例外措置」

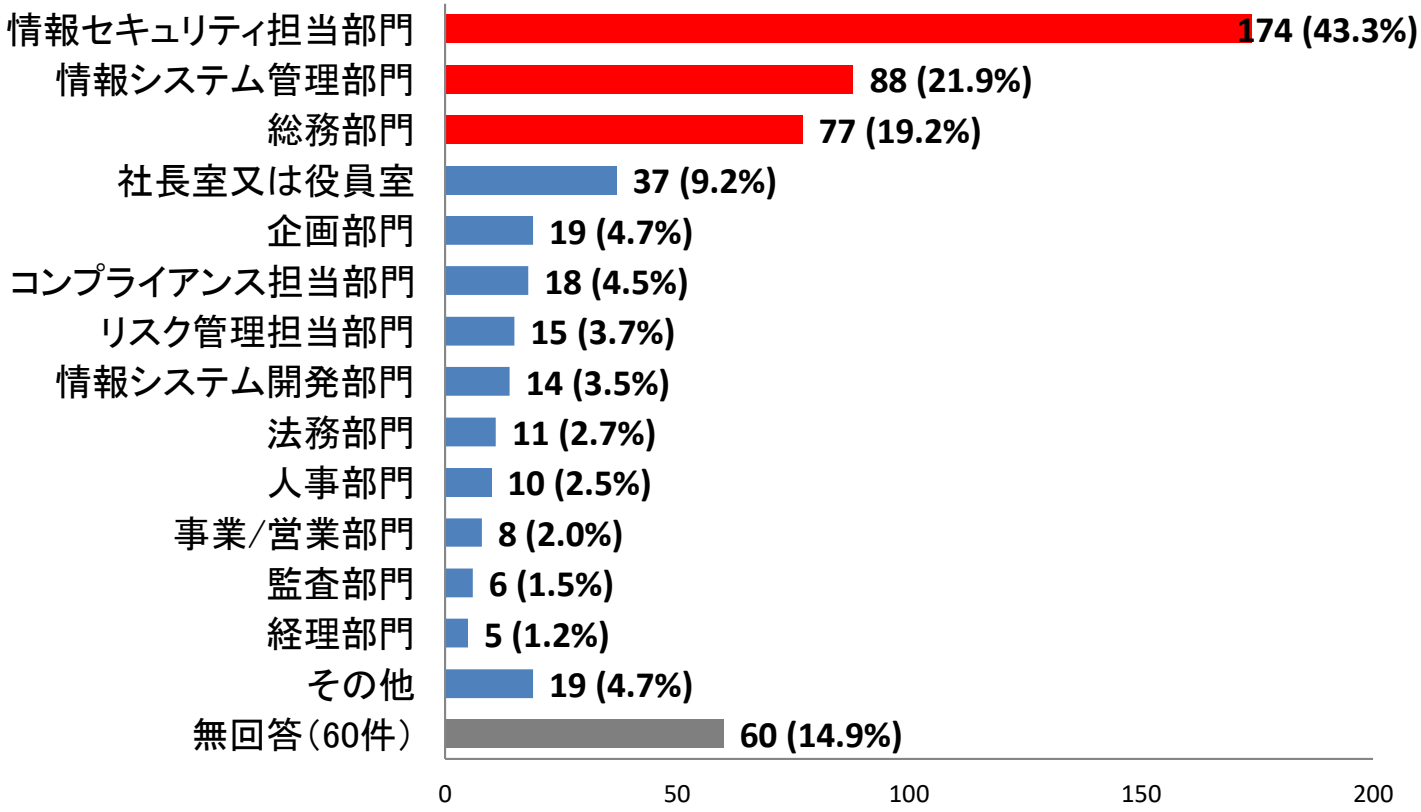
設問35. 例外規定は、全体で統一された内部規定のみか、現場組織ごとにも規定されているか(N=402)



例外措置の策定は統一基準のみで策定・措置されている組織が4割を超え、現場組織での策定は1割程度にとどまる

第6章　情報セキュリティマネジメントの「例外措置」

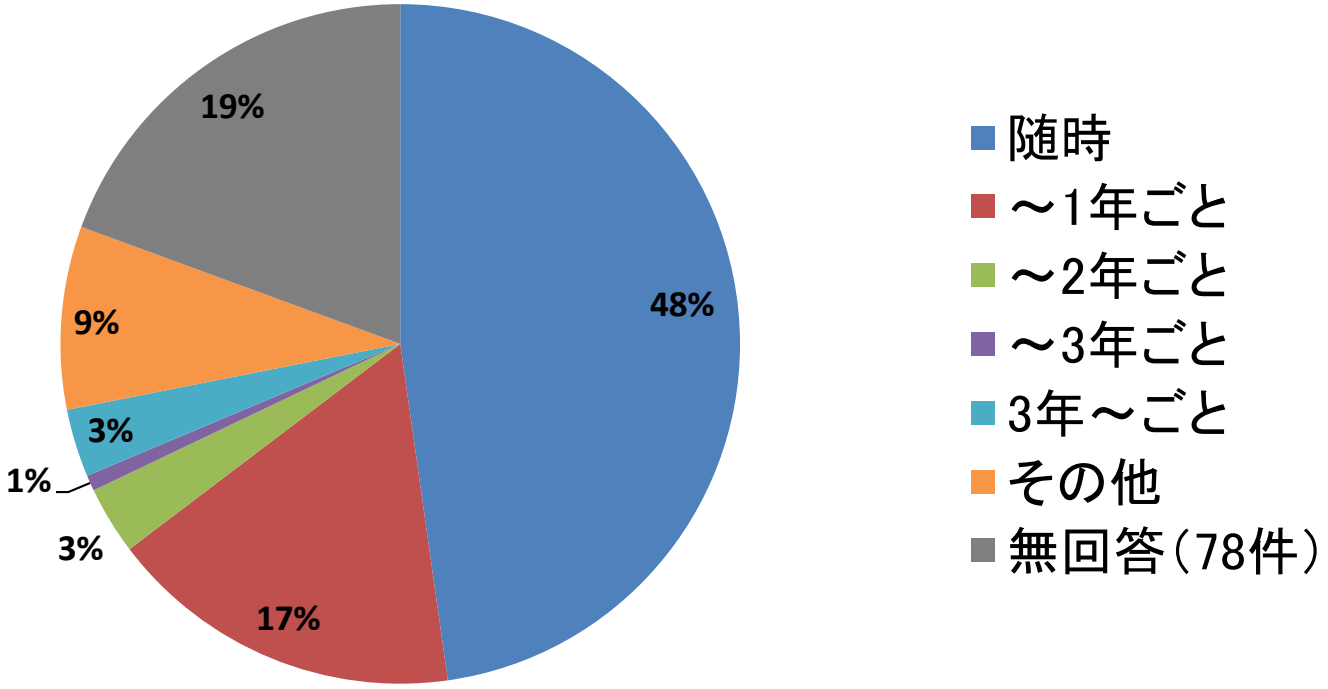
設問36. 例外規定を策定するにあたり、規程の策定と管理の事務処理をする主体部門(N=402)



策定する組織は主に情報システム系を取り扱い部門で占める。

第6章　情報セキュリティマネジメントの「例外措置」

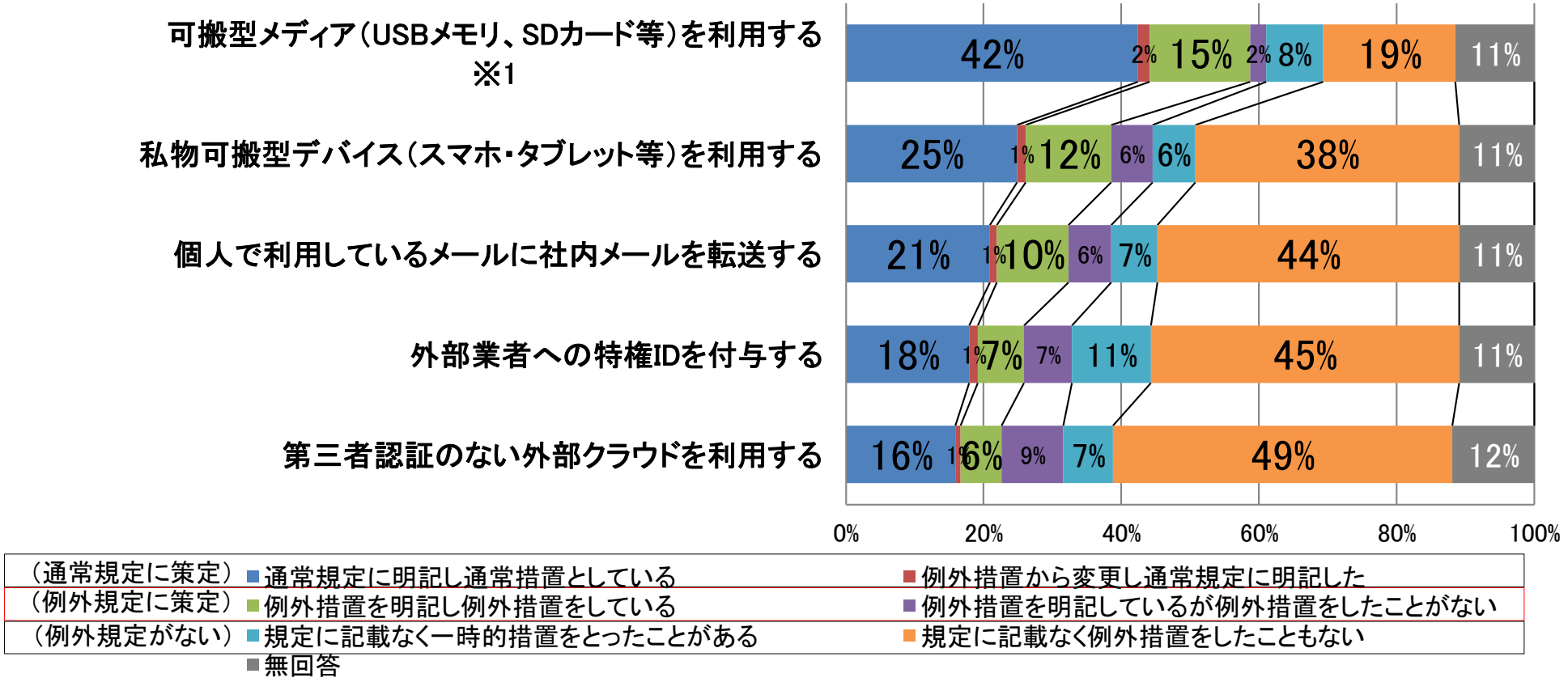
設問37．例外規定の見直し頻度(N=402)



例外措置の見直し頻度は、特に定期的に実施しておらず、案件が発生し実施した後に見直している組織が多い

第6章　情報セキュリティマネジメントの「例外措置」

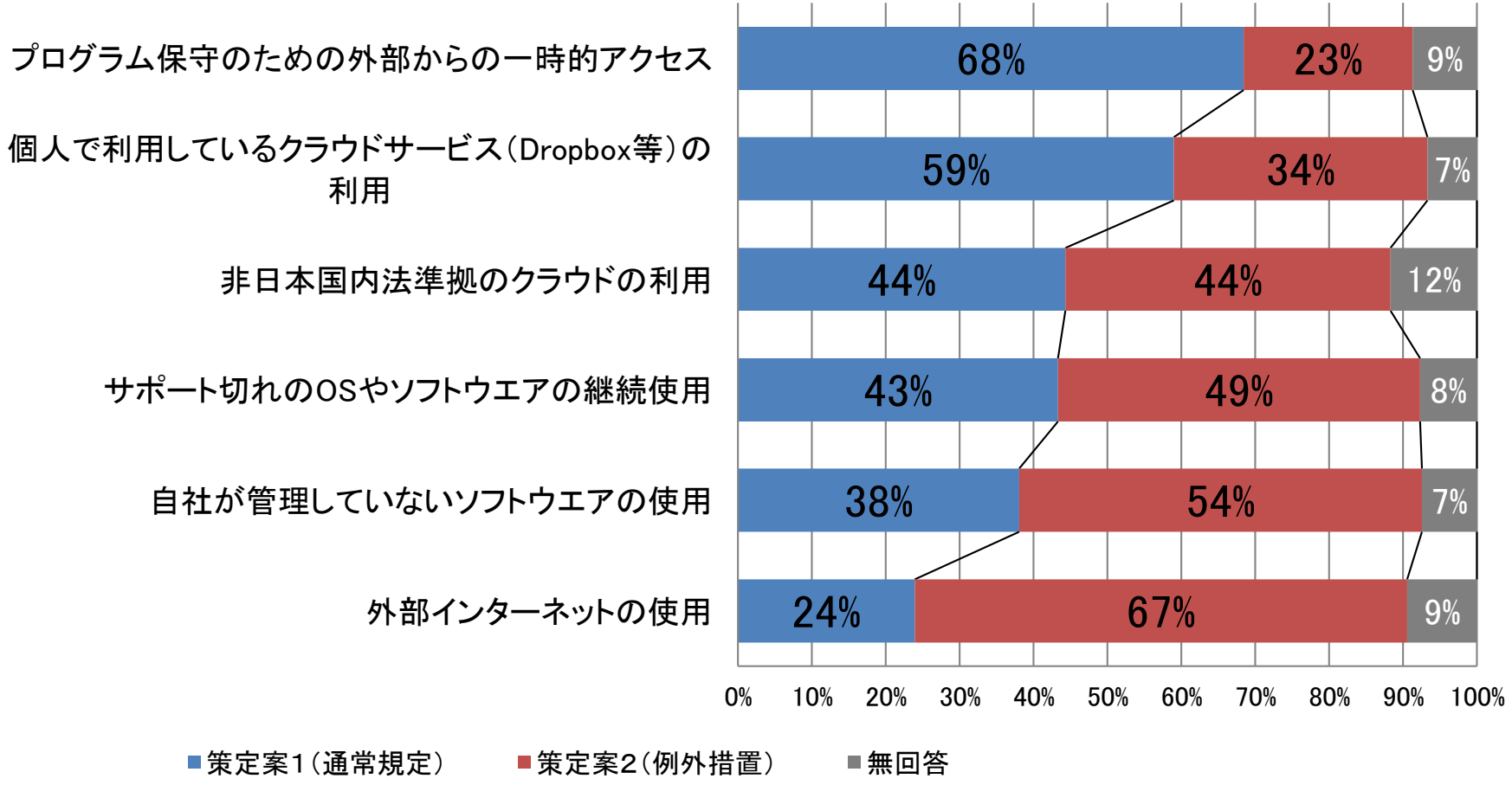
設問38．具体的な業務上の事象における例外措置の策定の有無
(N=402，※1はN=349)



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「可搬型メディアの利用」が目立っている

第6章　情報セキュリティマネジメントの「例外措置」

設問39．具体的な業務上の事象における通常規定か例外措置への選択(N=402)



個々の具体的な管理策において、通常規定が多いもの、例外措置が多いもの、あるいは双方均衡しているものなど、特徴が表れている。

第6章　情報セキュリティマネジメントの「例外措置」

調査結果：

- 例外措置の策定が内部規定に記載されている割合はされていない割合より21ポイント高い。
- 例外措置の策定は統一基準のみで策定・措置されている組織が4割を超え、現場組織での策定は1割程度にとどまる。
- 例外措置を策定する部門は主に情報システム系を取扱う部門で占める。
- 例外措置の見直し頻度は、特に定期的に実施しておらず、案件が発生し実施した後に見直している組織が多い。
- 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「可搬型メディアの利用」が目立っている。
- 具体的に通常規定例、例外措置例で選択してもらうと、通常規定で措置するもの、例外措置をとるもの、あるいは双方均衡しているものなど、個々の具体的な管理策において特徴が表れている。

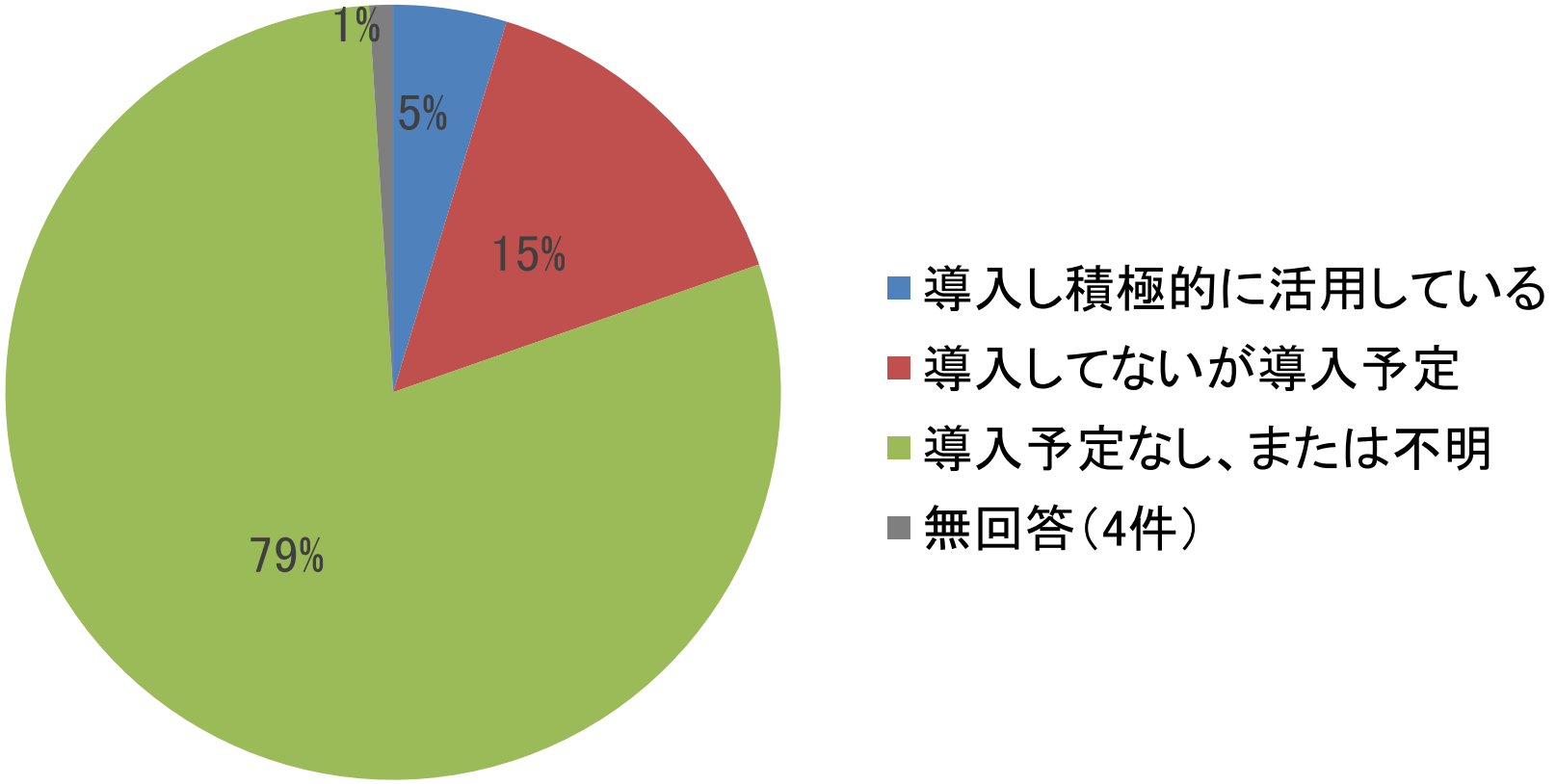
第7章
職場での人工知能(AI)や自律型ロボットの導入

調査概要：

AI 技術の導入状況，導入した際の利点，導入した際のリスク，導入理由

第7章　職場での人工知能(AI)や自律型ロボットの導入

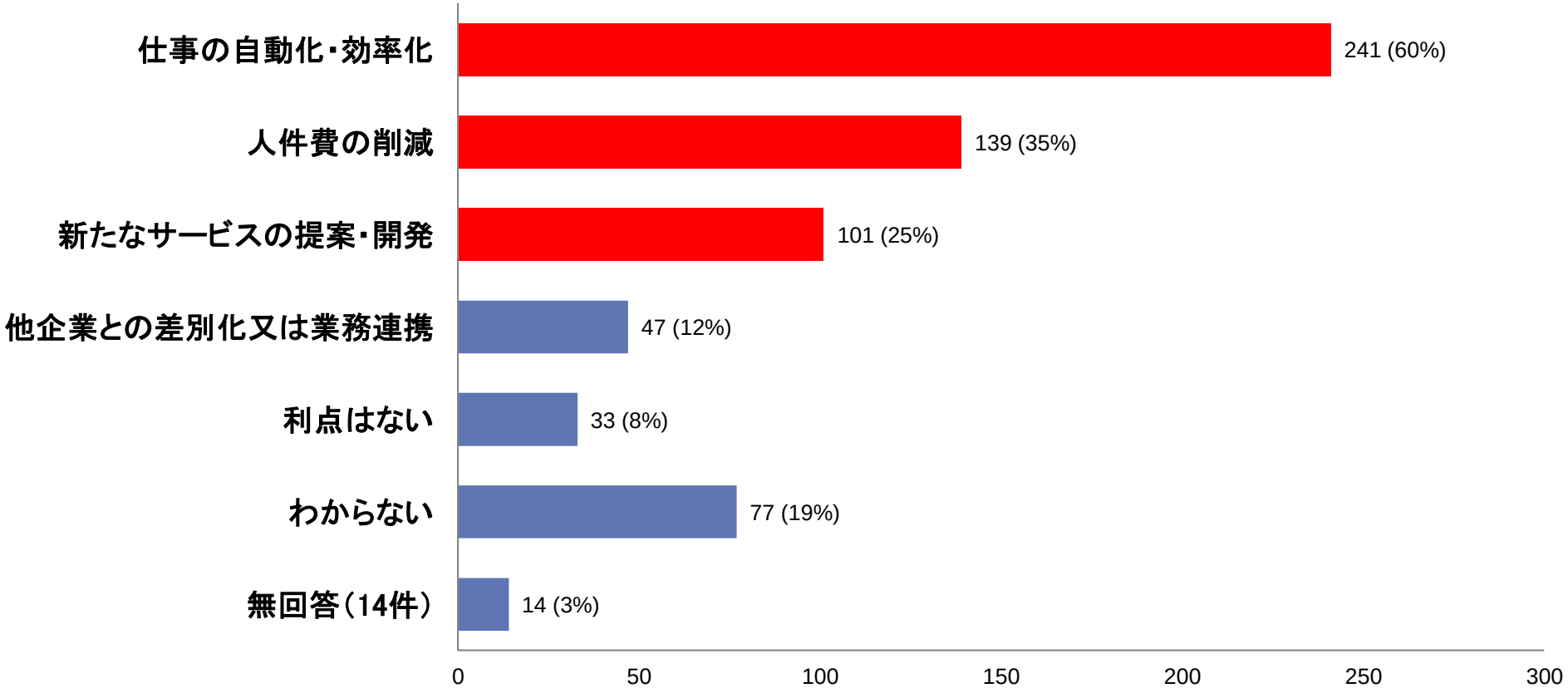
設問40　AIや自律型ロボットの導入状況（N=402）



「導入予定がない，または不明」と回答したものが79%と圧倒的に多く，実際にはまだ導入している組織は少ない

第7章　職場での人工知能(AI)や自律型ロボットの導入

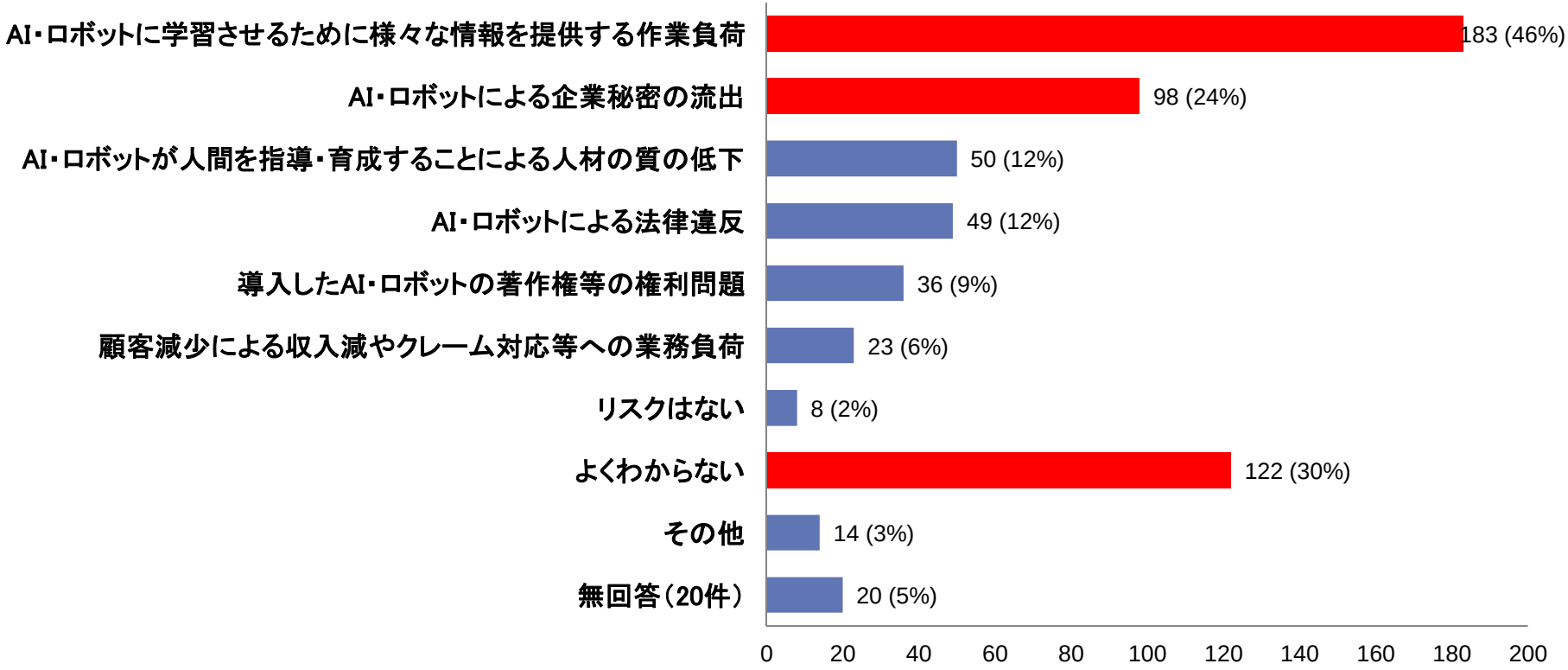
設問41　AIや自律型ロボットを業務で導入した際の利点（複数回答，N=402）



「仕事の自動化・効率化」60%（241件）と回答が最も多く、次いで「人件費の削減」35%（139件）、「新たなサービスの提案・開発」25%(101件)が多い

第7章　職場での人工知能(AI)や自律型ロボットの導入

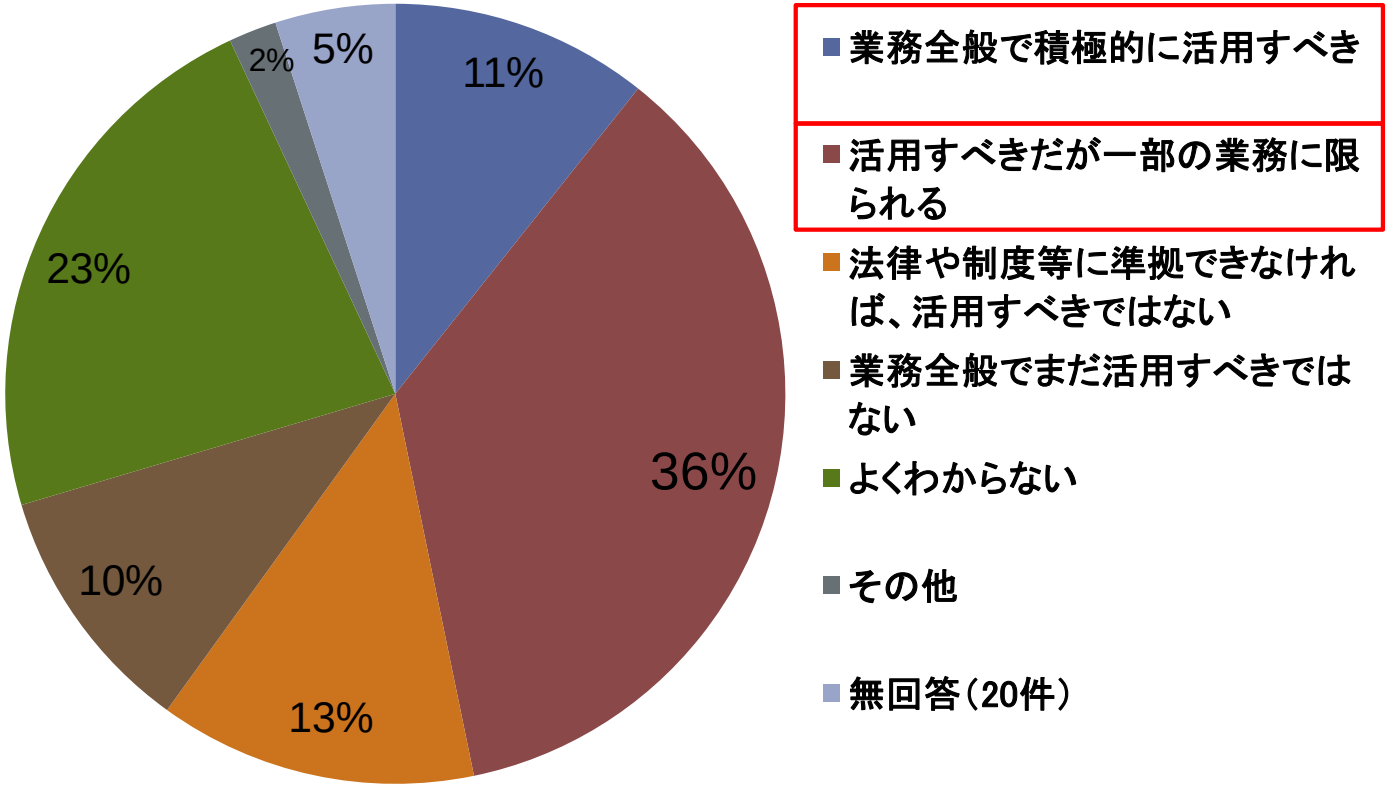
設問42　AIや自律型ロボットを業務や他企業との提携で導入した際のリスク（複数回答，N=402）



具体的なリスクとしては「学習させるために様々な情報を提供する作業負荷」46%（183件）と最も多く、次いで「企業秘密の流出」24%（98件）が最も多かった。一方、「よくわからない」と回答したものも30%(122件)と多かった。

第7章　職場での人工知能(AI)や自律型ロボットの導入

設問43　AIや自律型ロボットを業務に導入することについて（N=402）



「業務全般で積極的に活用すべき」「活用すべきだが一部に限る」を合わせ、全体の半数近くに及ぶ。
一方、「法律や制度で制限すべき」「活用すべきではない」を合わせた回答23%、よくわからない（23%）との回答もある程度占める。

第7章　職場での人工知能(AI)や自律型ロボットの導入

調査結果：

- AIや自律型ロボットの導入状況については，「導入予定がない，または不明」と回答したものが79%と圧倒的に多く，実際にはまだ導入している組織は少ない。
- AIや自律型ロボットを導入した利点としては，「仕事の自動化・効率化」と回答が最も多く，次いで「人件費の削減」「新たなサービスの提案・開発」 が多い。
- AIや自律型ロボット導入への具体的なリスクとしては「学習させるために様々な情報を提供する作業負荷」と最も多く、次いで「企業秘密の流出」）が多い。
- AIや自律型ロボット導入へのリスクについて，「よくわからない」と回答したものも30%(122件)と多かった。
- AIや自律型ロボットを活用すべきと回答したものが全体の半数近くに及ぶ一方、活用すべきではないとの回答も23%とある程度占める。また、よくわからないとの回答23%もあり、AI活用への理解がまだ低いこともわかった。

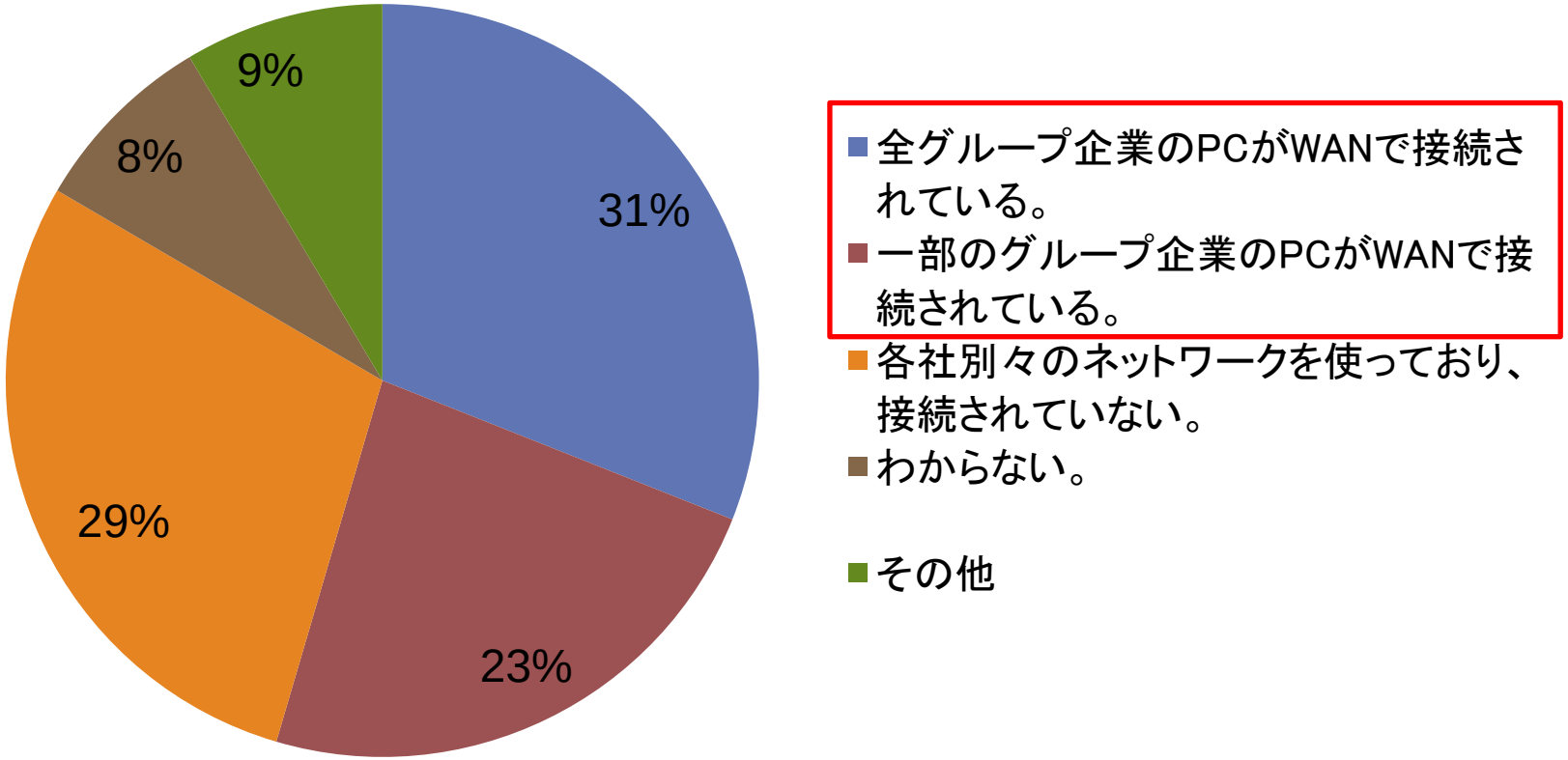
第8章
グループ企業における
情報セキュリティポリシーについて

調査概要：

グループ企業におけるセキュリティポリシーの整備状況、ポリシー整備・遵守の課題

第8章　グループ企業における情報セキュリティポリシーの整備・遵守

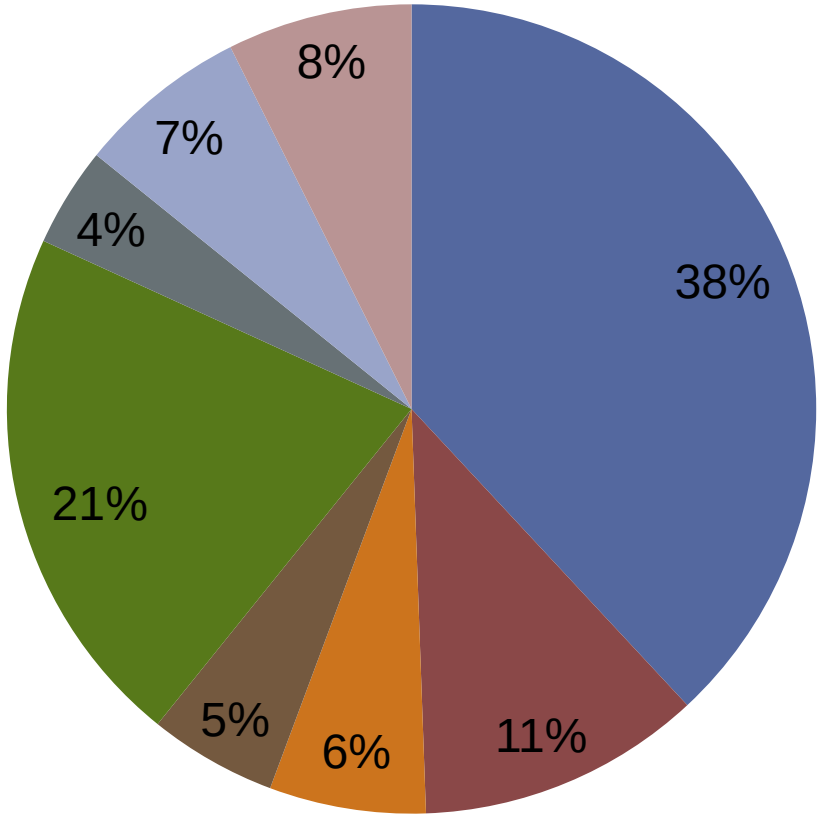
設問44　グループ企業間のネットワーク接続状況（N=187）



グループ企業において、PC環境をWANで接続している企業は、「全グループ企業を接続している」、「一部グループ企業を接続している」を合わせると、54%となっている。

第8章　グループ企業における情報セキュリティポリシーの整備・遵守

設問45　グループ企業のセキュリティポリシー整備状況（N=176）

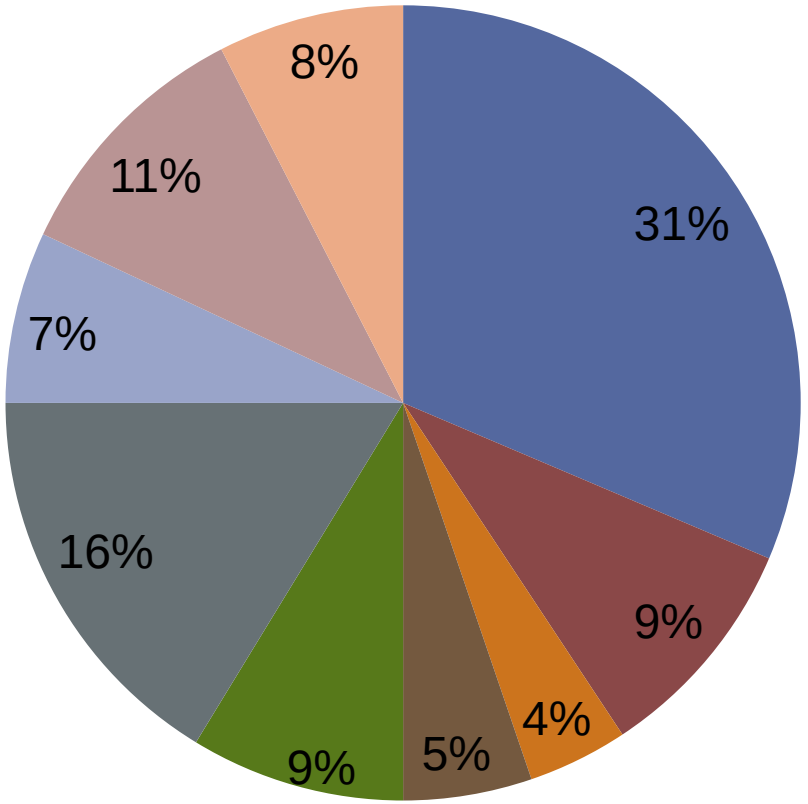


- 全グループ企業に、親会社と共通のポリシーを適用している。
- 全グループ企業に、親会社のポリシーを一部変更して適用している。
- 一部のグループ企業に、親会社と共通のポリシーを適用している。
- 一部のグループ企業に、親会社のポリシーを一部変更して適用している。
- 共通のポリシーはなく、各社個別のポリシーを作成している。
- 情報セキュリティポリシーは特に定めていない。
- わからない
- その他

何らかの形で親会社と共通のポリシーを適用している組織が、60%に上っている。

第8章　グループ企業における情報セキュリティポリシーの整備・遵守

設問46　グループ企業のセキュリティポリシー遵守状況の確認方法（N=172）

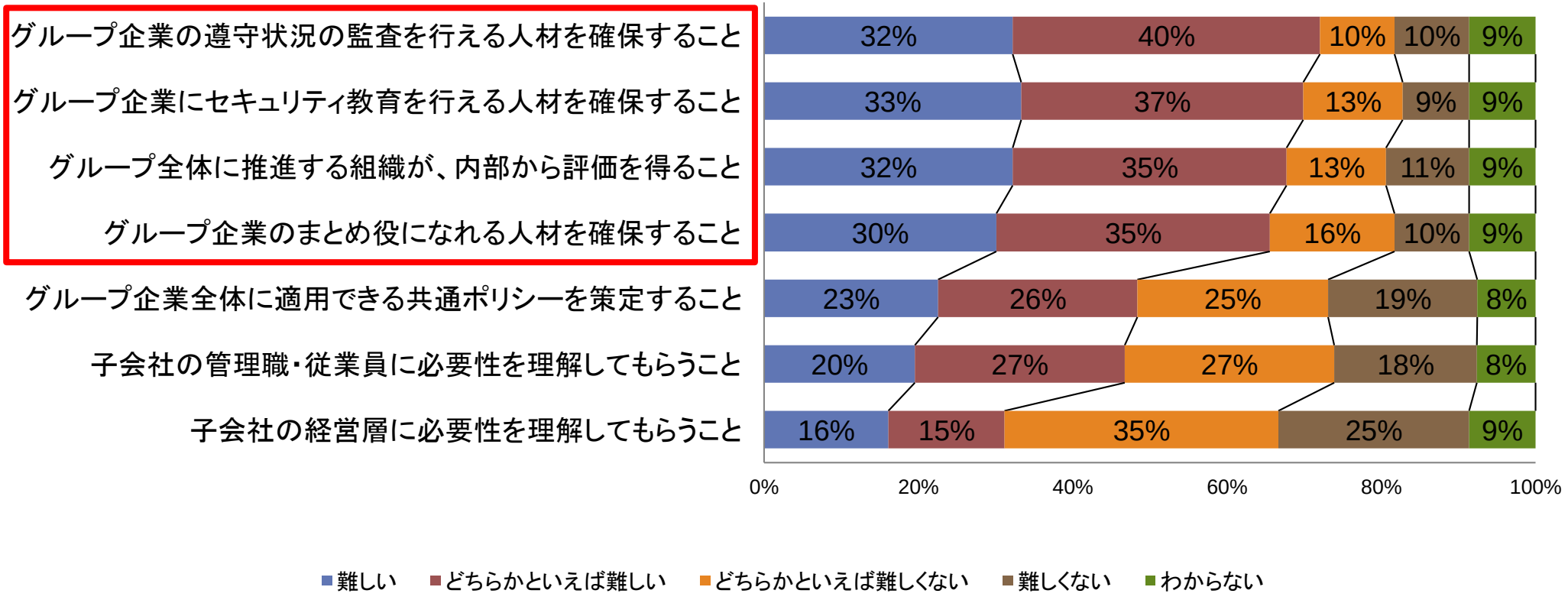


- 全グループ企業に、共通の評価基準で、親会社の監査担当部門などによる確認を定期的に実施している。
- 全グループ企業に、親会社の評価基準を一部変更して、親会社の監査担当部門などによる確認を定期的に実施している。
- 一部のグループ企業に、共通の評価基準で、親会社の監査担当部門などによる確認を定期的に実施している。
- 一部のグループ企業に、親会社の評価基準を一部変更して、親会社の監査担当部門などによる確認を定期的に実施している。
- 各社で、共通の評価基準による自己点検を定期的に実施している。
- 各社で、各自で作成した評価基準による自己点検を定期的に実施している。
- 親会社のセキュリティ担当部門などによる確認や、自己点検は実施していない。
- わからない
- その他

親会社の監査担当部門などによる確認を定期的に実施している組織が約半数の49%となっている。また共通の基準で自己点検を実施している組織を合わせると約6割となる。

第8章　グループ企業における情報セキュリティポリシーの整備・遵守

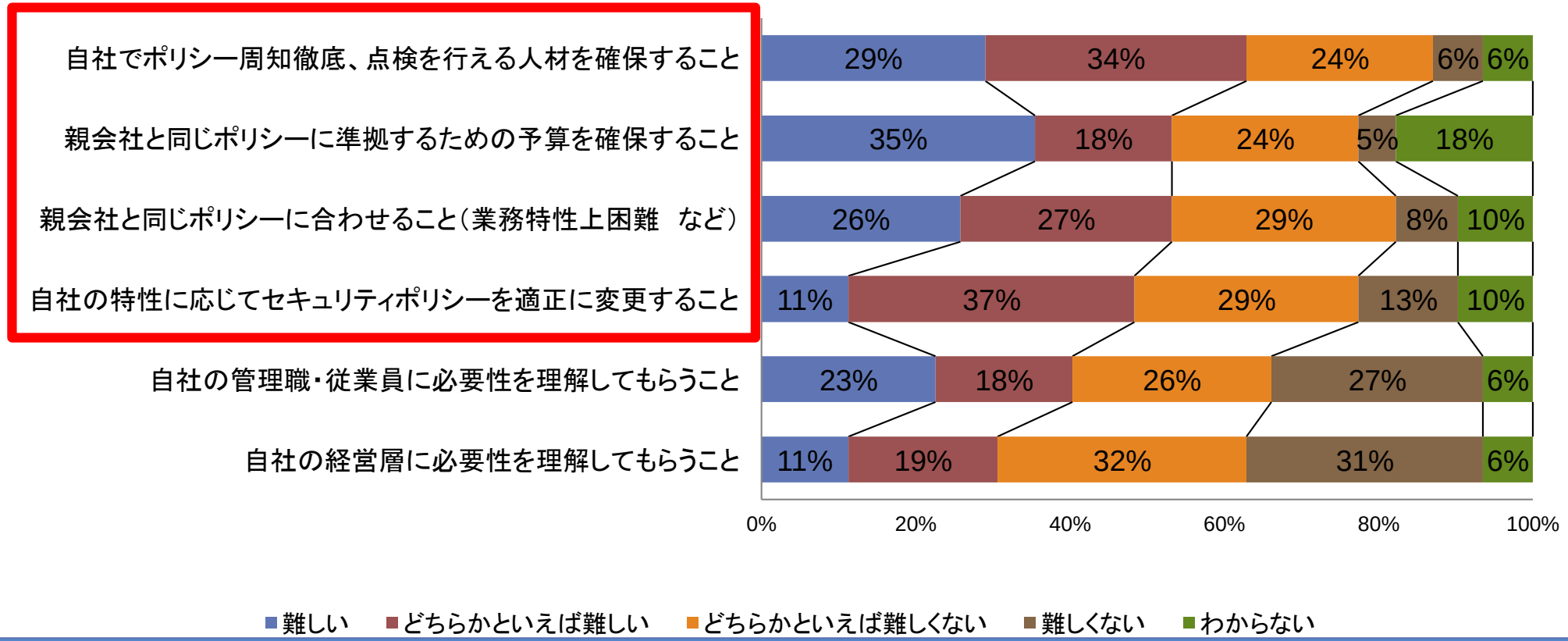
設問47　グループ企業全体でセキュリティポリシー遵守を徹底する上での難しさ
①グループ企業にポリシーを守るよう働きかける親会社の立場（N=93）



親会社の立場では、必要性を理解してもらうことや、共通ポリシーを策定することよりも、人材の確保と、内部から評価を得ることの方が「難しい」、「どちらかといえば難しい」と　回答している割合が高く、いずれも65%を超えている。

第8章　グループ企業における情報セキュリティポリシーの整備・遵守

設問47　グループ企業全体でセキュリティポリシー遵守を徹底する上での難しさ
②ポリシーを守る子会社の立場（N=74）



子会社の立場でも、人材の確保が「難しい」、「どちらかといえば難しい」と回答している組織が多く、63%に及ぶ。次いで、予算の確保、親会社とポリシーを合わせること、適正に変更することが難しいがそれぞれ約半数ある。

第8章　グループ企業における情報セキュリティポリシーの整備・遵守

調査結果：

- グループ企業のPC環境をWANで接続している企業は、「全グループ企業を接続している」、「一部グループ企業を接続している」を合わせると、54%であった。
- グループ企業で情報セキュリティポリシーを共通化している企業も、「親会社と共通のポリシーを適用している」、「親会社のポリシーを一部変更して適用している」、「一部のグループ企業に親会社と共通のポリシーを適用している」を合わせると、60%に及ぶ。
- 共通の基準を用いて、親会社の監査担当部門による監査や、自己点検を行っている企業も合わせると約6割である。
- 親会社の立場では、人材の確保と、情報セキュリティを推進する組織が内部から評価を得ることが「難しい」、「どちらかといえば難しい」と回答している割合が高く、いずれの項目でも65%を超えている。
- 子会社の立場でも、人材の確保が「難しい」、「どちらかといえば難しい」と回答している組織が多く、約6割に及ぶ。次いで、予算の確保、親会社とポリシーを合わせること、親会社のポリシーを適正に変更することが難しいとの回答が約半数ある。

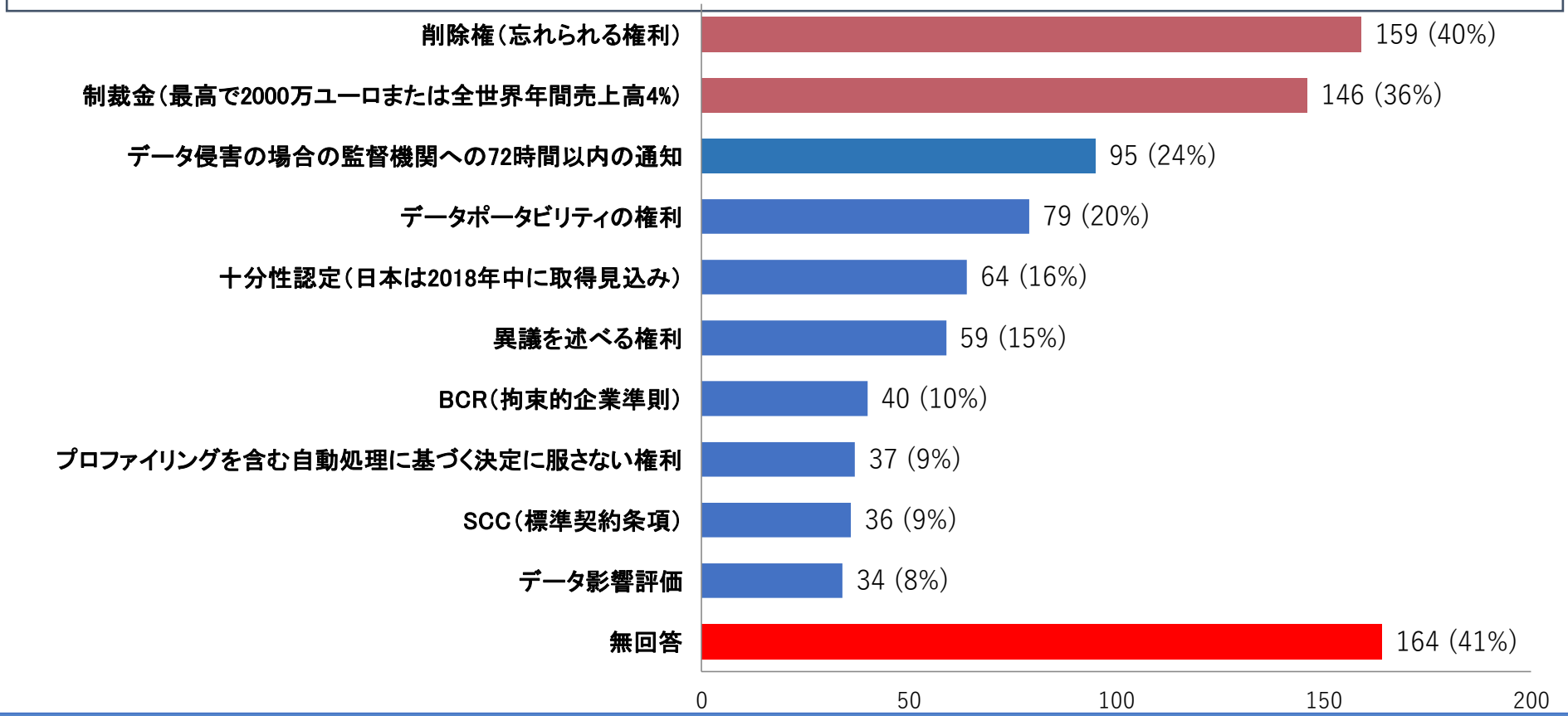
第9章
EU一般データ保護規則(GDPR)への対応

調査概要：

GDPRに対する認知度、また対応状況等

第9章　EU一般データ保護規則(GDPR)への対応状況

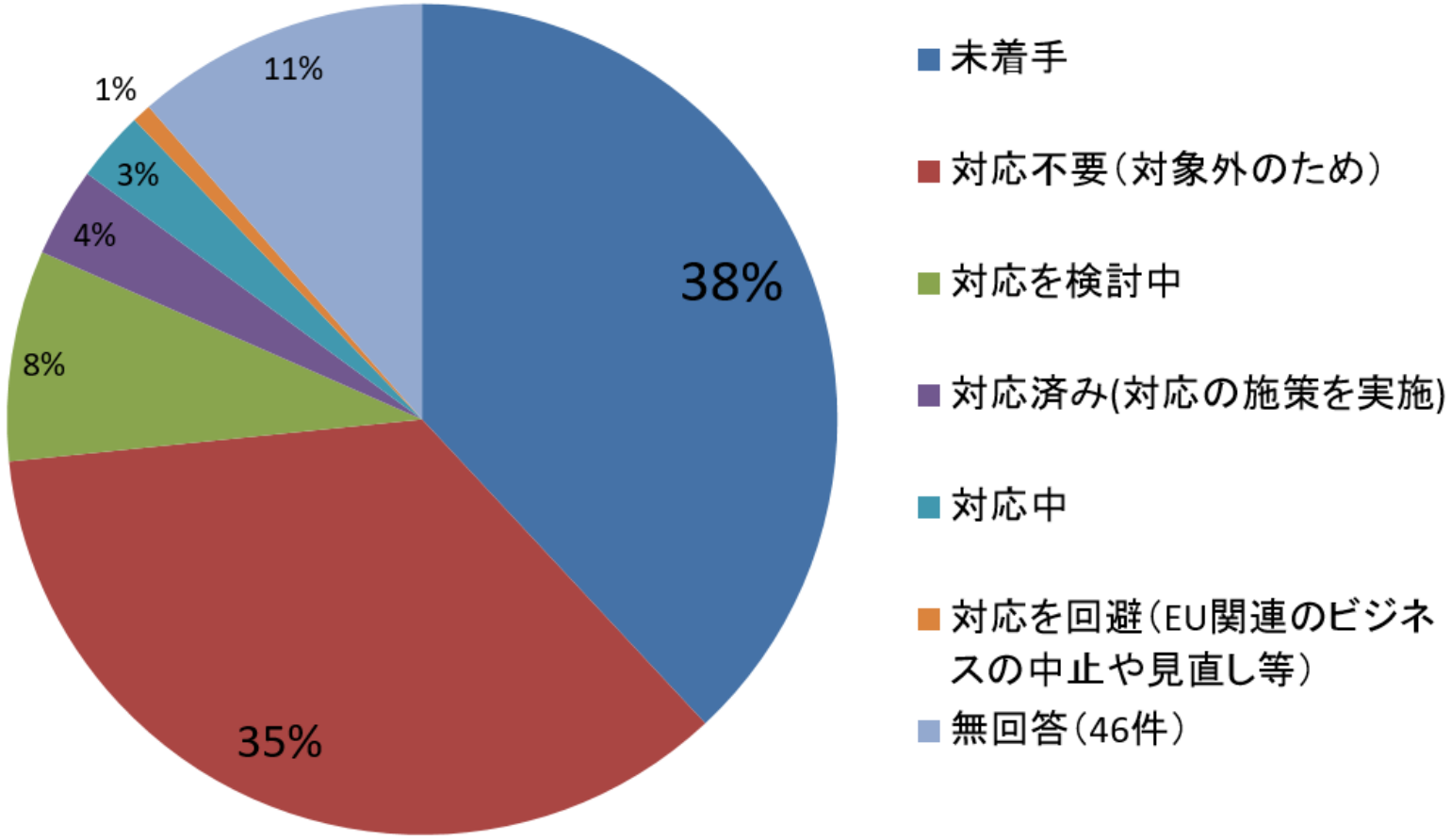
設問48. GDPRに関する事項の認知度（複数回答）（N=402）



「削除権」が最も多く40%、次に「制裁金」が36%と多い。
「無回答」が402組織のうち41%であった。

第9章　EU一般データ保護規則(GDPR)への対応状況

設問49. GDPRへの対応状況（N=402）



「未実施」が38%と最も多く、次に「対応不要」が35%であった。
「対応済み」・「対応中」・「対応を検討中」を合わせて15%であった。

第9章　EU一般データ保護規則(GDPR)への対応状況

調査結果：＜GDPRに関する事項の認知度＞

- 「削除権」が最も多く40%、次に「制裁金」が36%と多い。
- 「無回答」が402組織の41%であった。

＜GDPRへの対応状況＞

- 未実施（153組織）が38%と最も多く、次に対応不要（142組織）が35%と多い。
- 対応済み（14組織）・対応中（11組織）・対応を検討中（33組織）を合わせて15%であった。

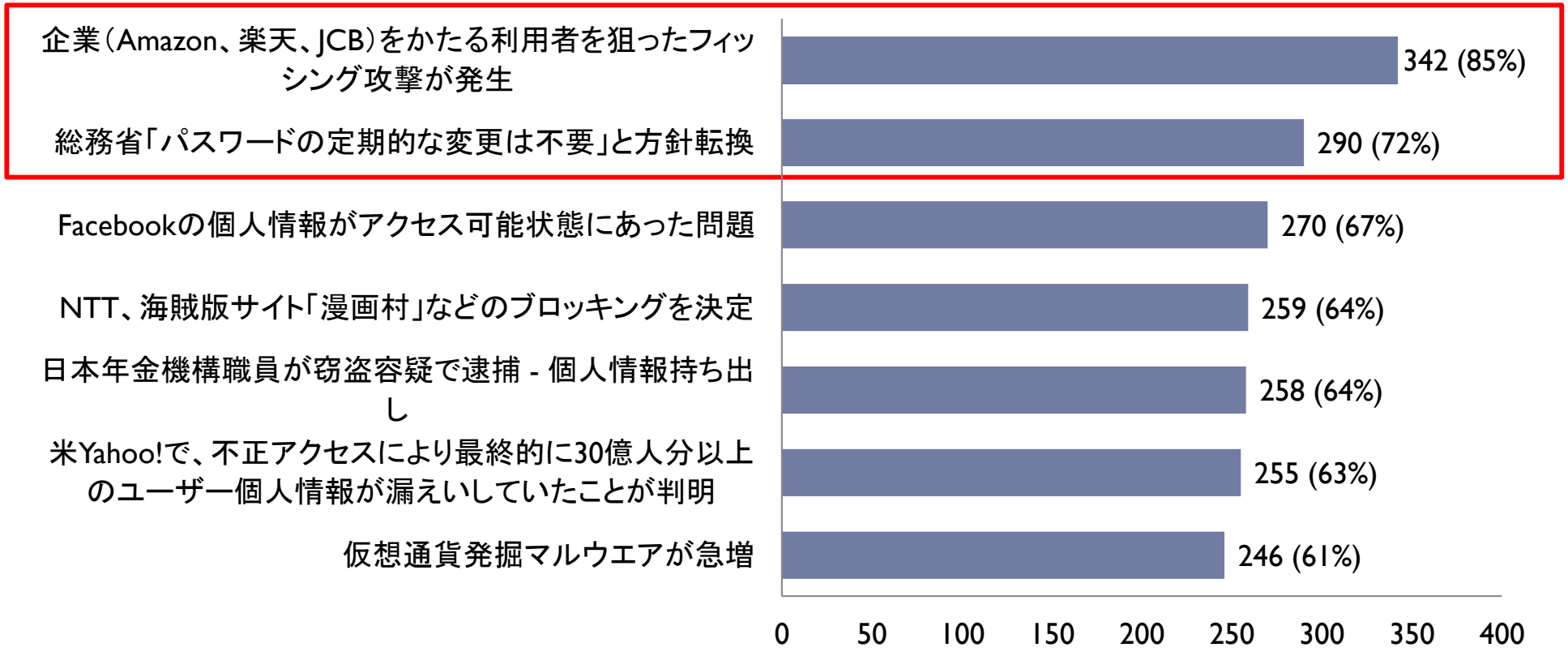
第10章
その他　過去の事例・事故の認知度

調査概要：

2018年6月までに起きた主要な情報セキュリティに関する事件・事故についての組織の認知度

第10章　過去の事例・事故・用語の認知度

設問50　出来事（事例・事故の認知度）（複数回答，N=402）

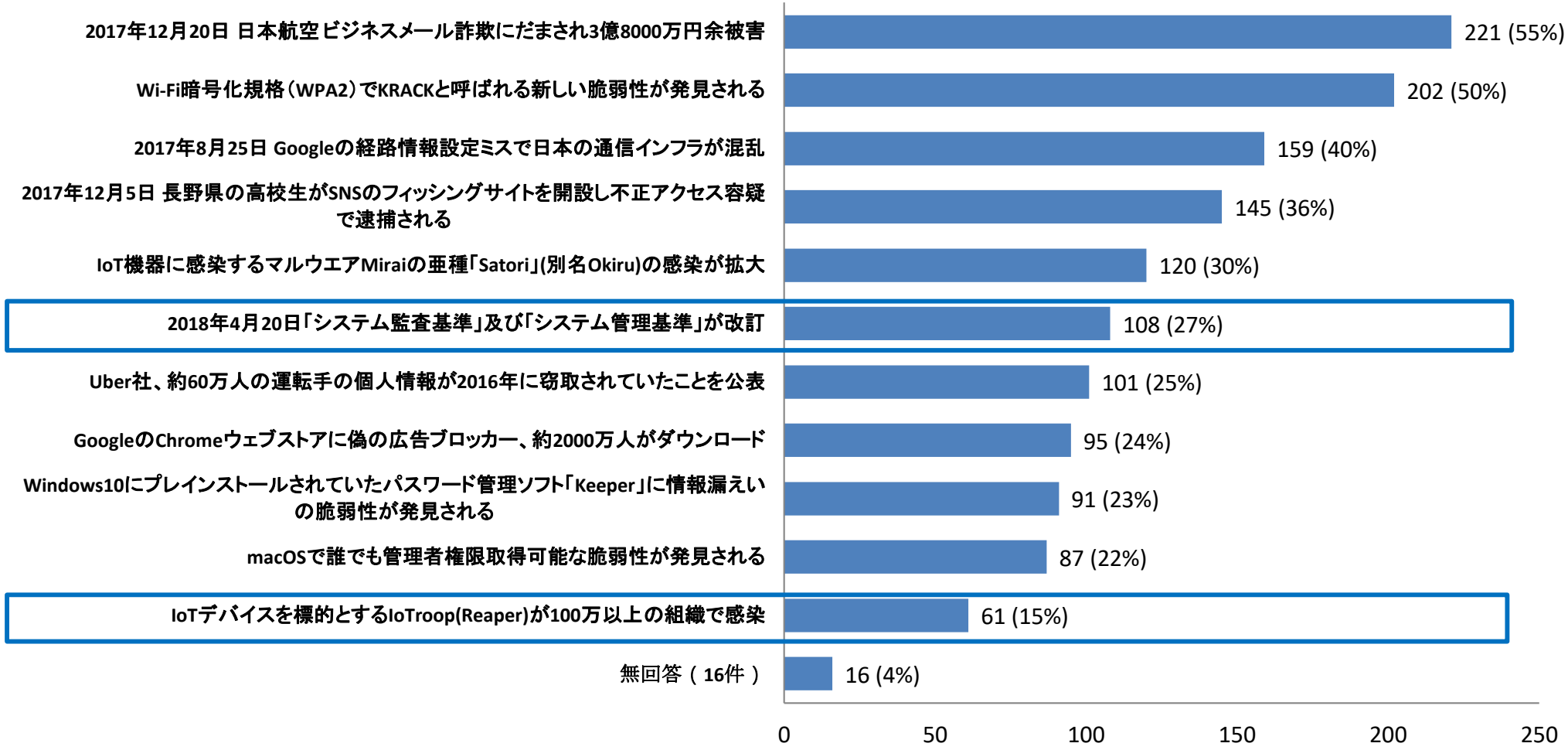


[1～7位]企業を語る利用者を狙ったフィッシング攻撃が発生が85%で最も認知度が高かった。
他に総務省「パスワードの定期的な変更は不要」と方向転換も72%と認知度が高い。

第10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　出来事（事例・事故の認知度）（複数回答，N=402）



[8～18位]IoTデバイスを標的とするIoTroop(Reaper)が100万以上の組織で感染などの事例の認知度が最も低く、システム監査基準、管理基準の改定も比較的低い。

調査結果：

過去の事例、事故

- 企業を語る利用者を狙ったフィッシング攻撃が発生が85%で最も認知度が高かった。他に総務省「パスワードの定期的な変更は不要」と方向転換も72%と認知度が高い。
- IoTデバイスを標的とするIoTroop(Reaper)が100万以上の組織で感染などの事例の認知度が最も低く、システム監査基準、管理基準の改定も比較的低い。

まとめ

- 今回の単純集計とその分析結果から，日本の組織の情報セキュリティの現状をより深く把握することが出来た。
- 2018年における日本の情報セキュリティの断面であり，今後の調査や研究活動の参考となる。
- さらにいくつかの章については，今後詳細な分析を進め，学会研究会等で発表する予定。

- 本研究が，実務担当者の理解と対策を進める一助になればと考える。

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
  - 神奈川県立みどり養護学校新栄分教室
  - 神奈川県立麻生養護学校　元石川分教室

    他1校

  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