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

2013年情報セキュリティアンケート調査結果

2013年12月25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

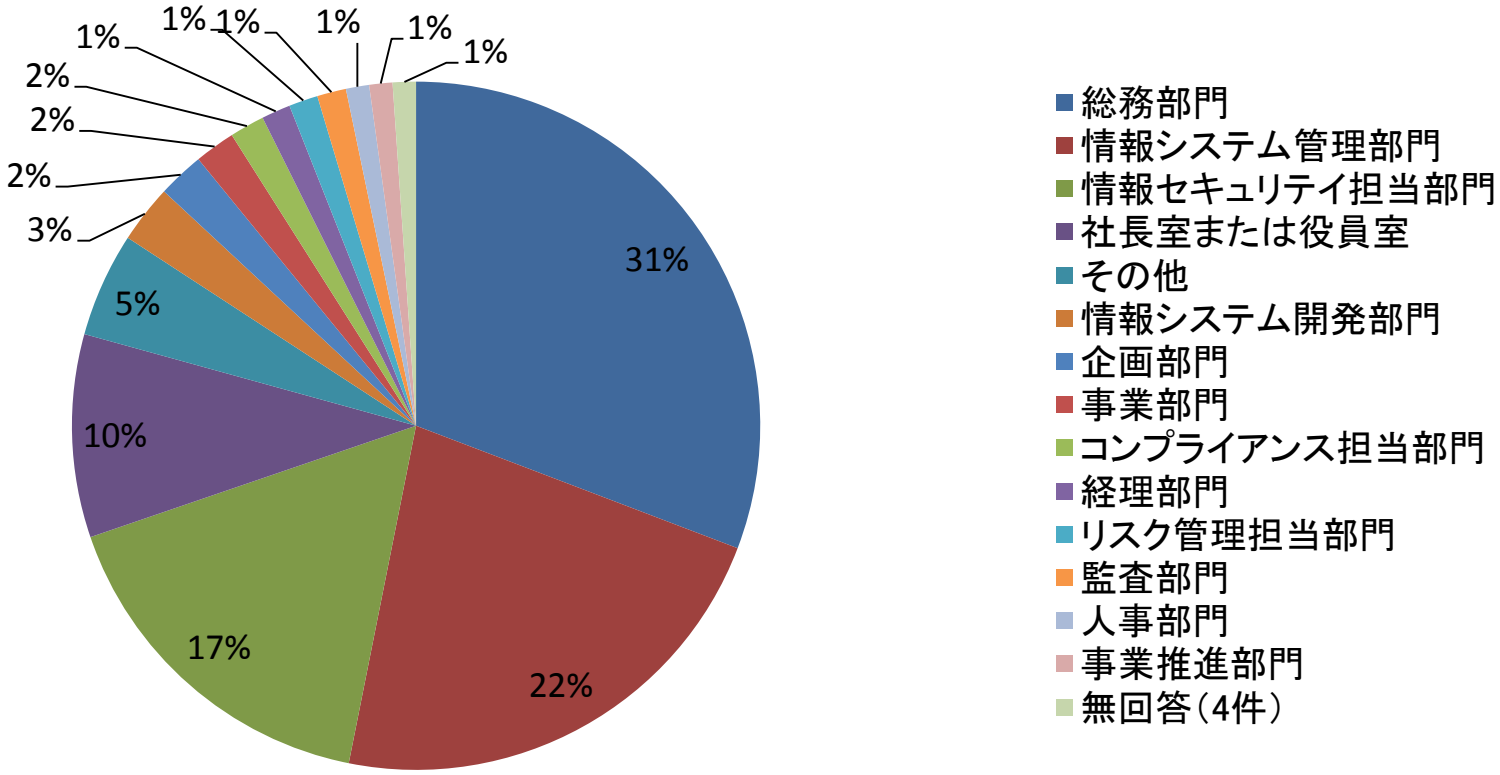
- アンケート実施期間
  2013年7月29日～8月23日
- アンケート対象
  Pマーク取得企業、ISMS認証取得企業、官公庁、教育機関など
  4,500組織の情報セキュリティ・システム担当者
- アンケート内容
  情報セキュリティマネジメントの取組み状況、情報セキュリティ管理体制と人材育成、情報セキュリティのガバナンス、営業秘密の管理、クラウド・コンピューティング、事業継続計画など
- 調査方法
  郵送による
- 回答状況
  367件（送達確認できた4,378組織に対して8.4%）

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=367)

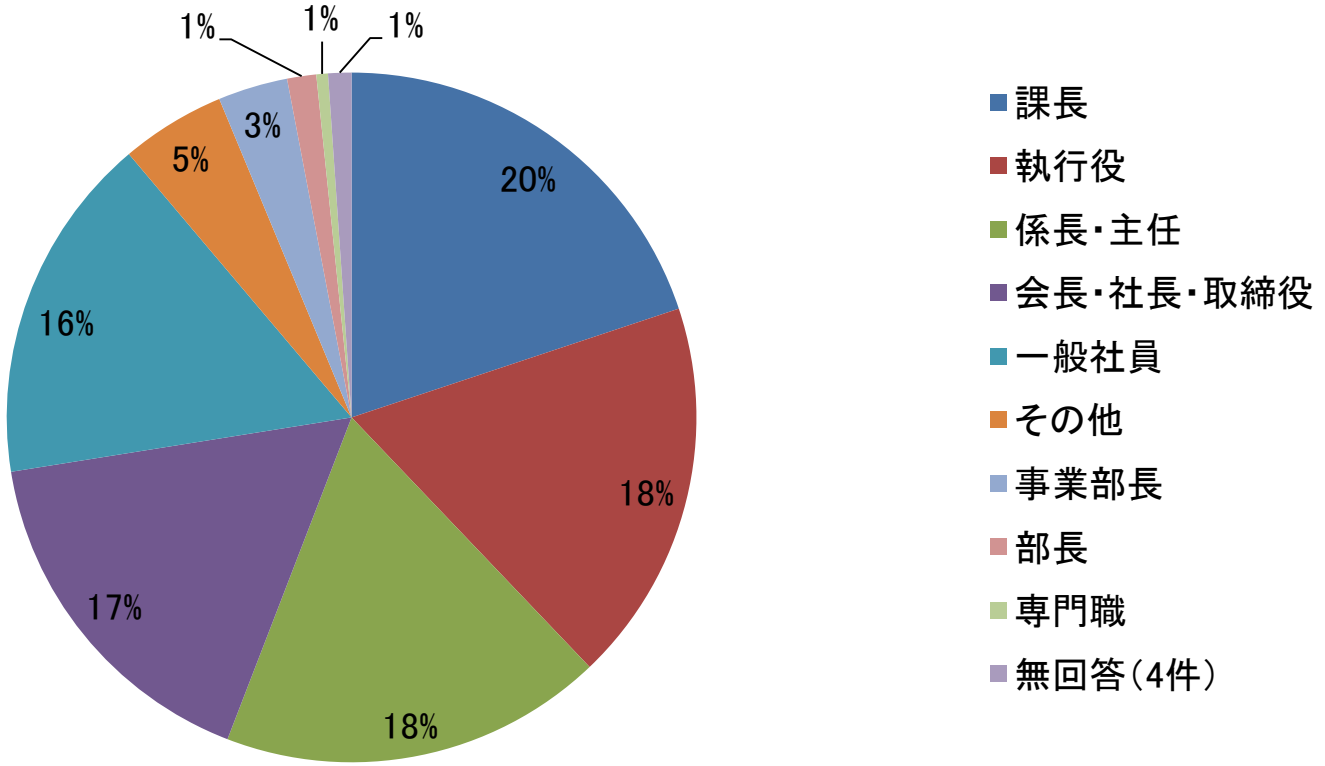


所属は、総務部門、情報システム管理部門、
情報セキュリティ担当部門順に多い。

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=367)

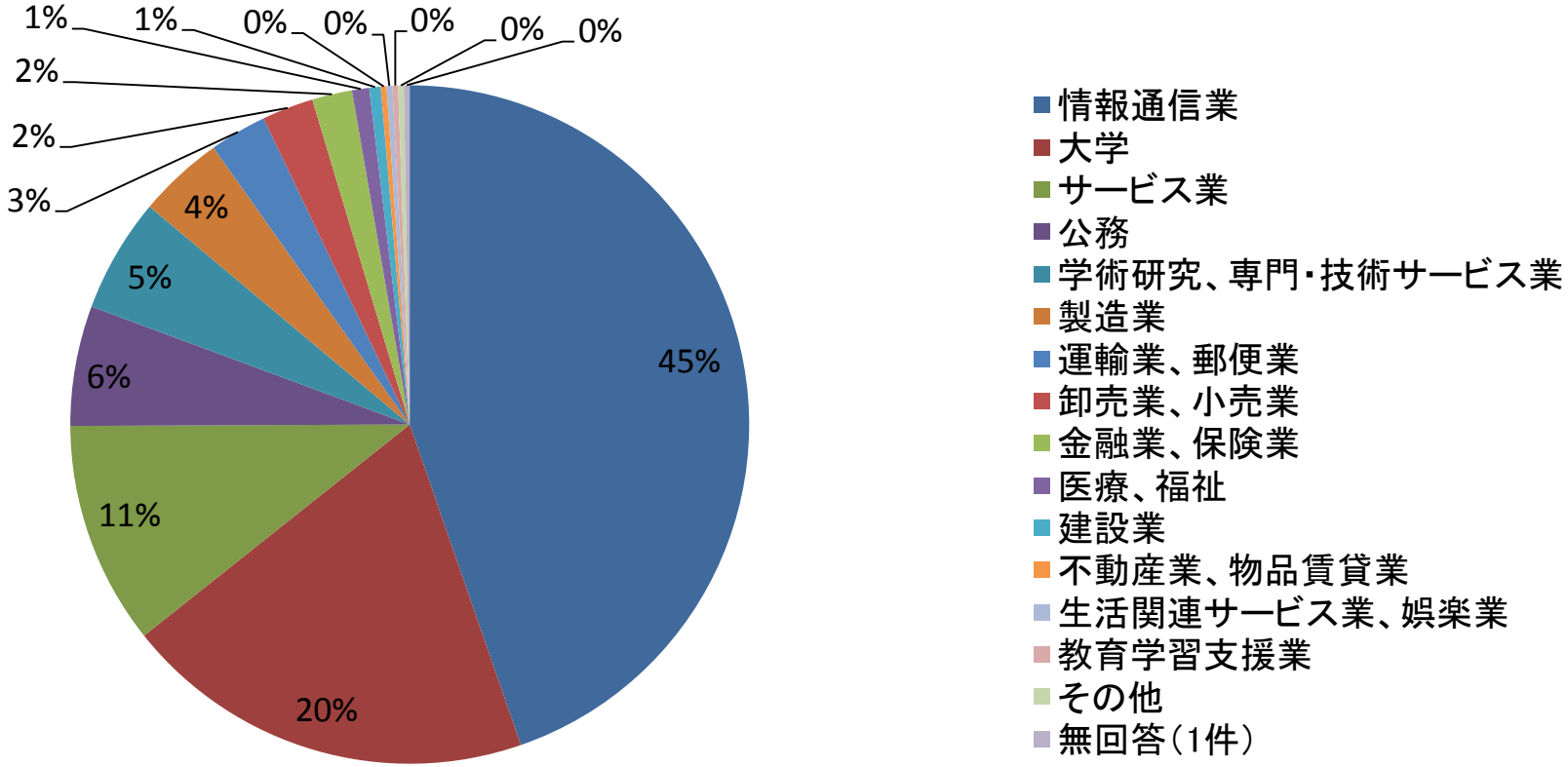


回答者の役職は、課長、執行役、係長・主任、
会長・社長・取締役、一般社員の順に多い。

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．業種※日本産業分類による(N=367)



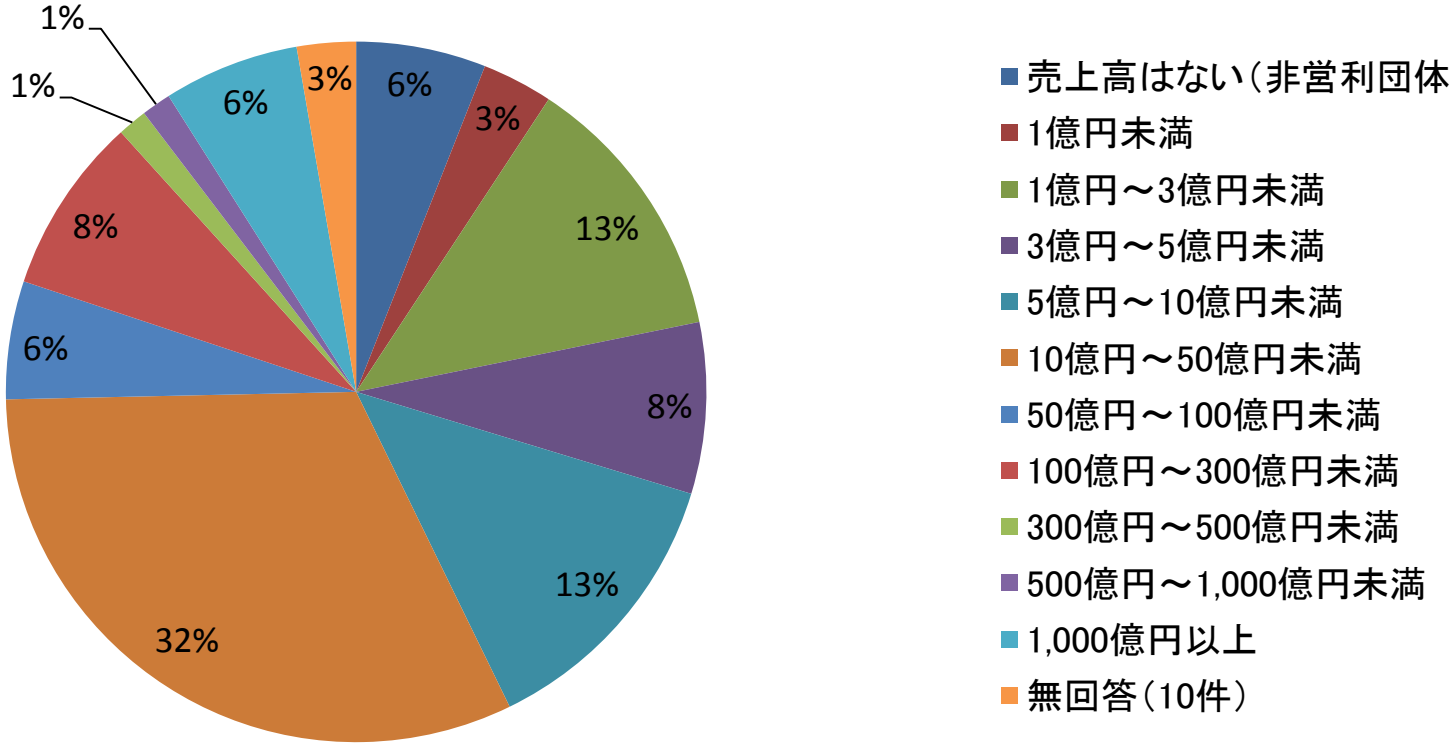
情報通信業が45%と半数近い割合となっている。

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=367）

※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

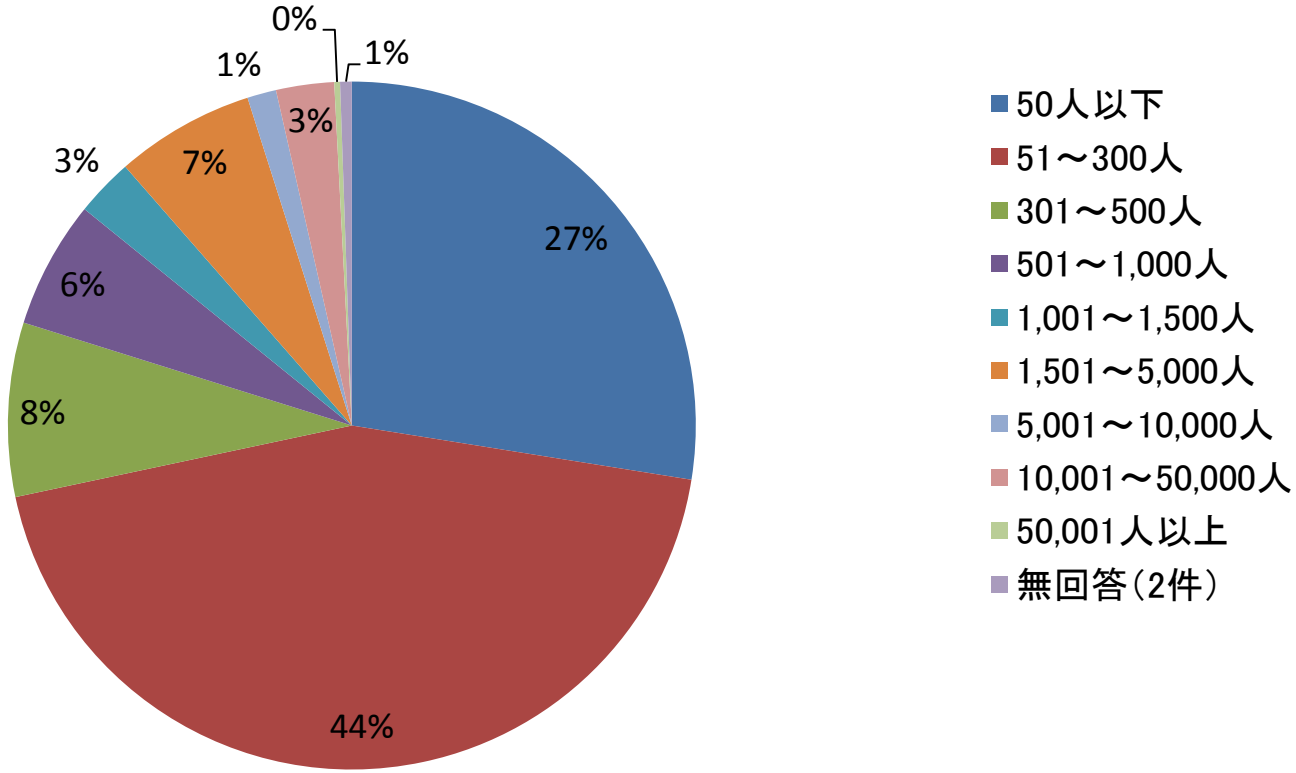


昨年同様に、売上高10億円から50億円の企業が一番多い。
また、売上高50億円以下の企業で7割を占める。

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

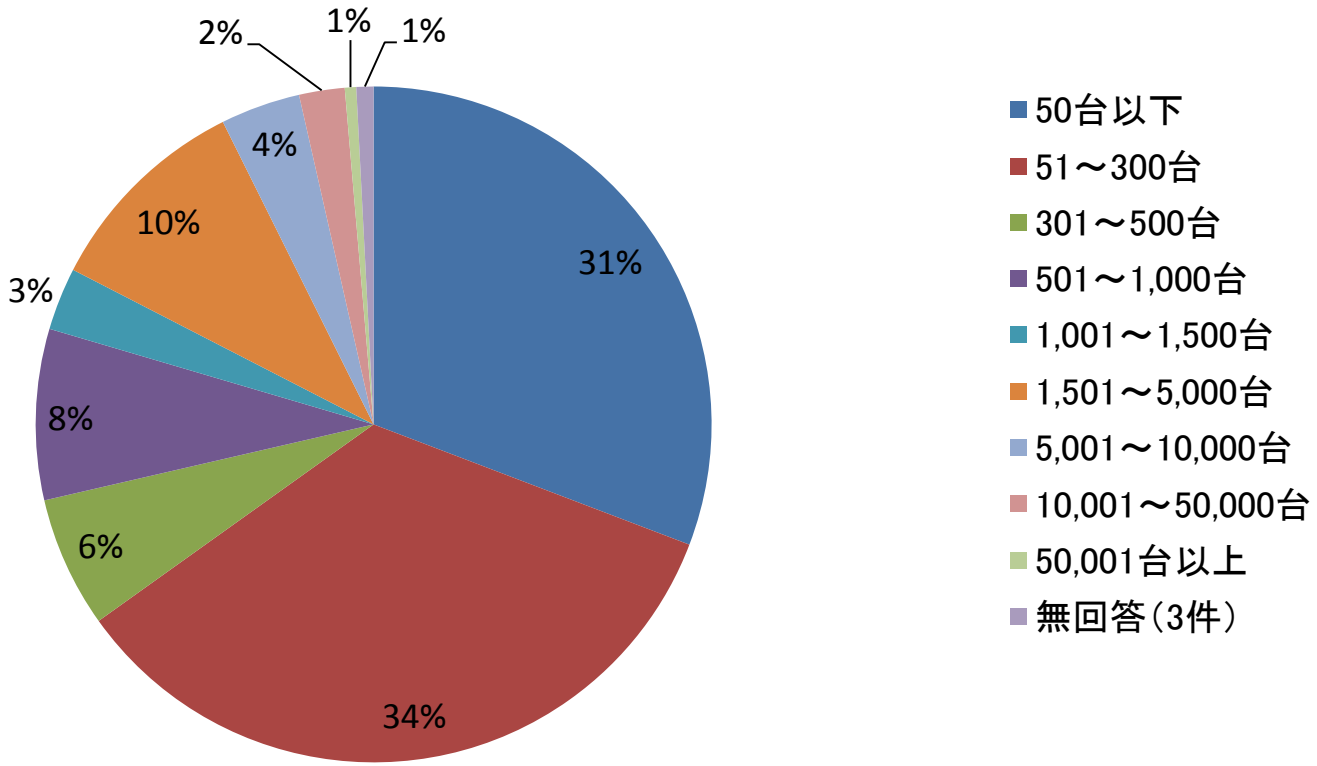
設問5. 全従業員数(N=367)



従業員数5人～300人以下の企業が最も多く、昨年同様の結果である。

第1章　概要（回答者の基本データ等）

設問6. PC数（単独）(N=367)

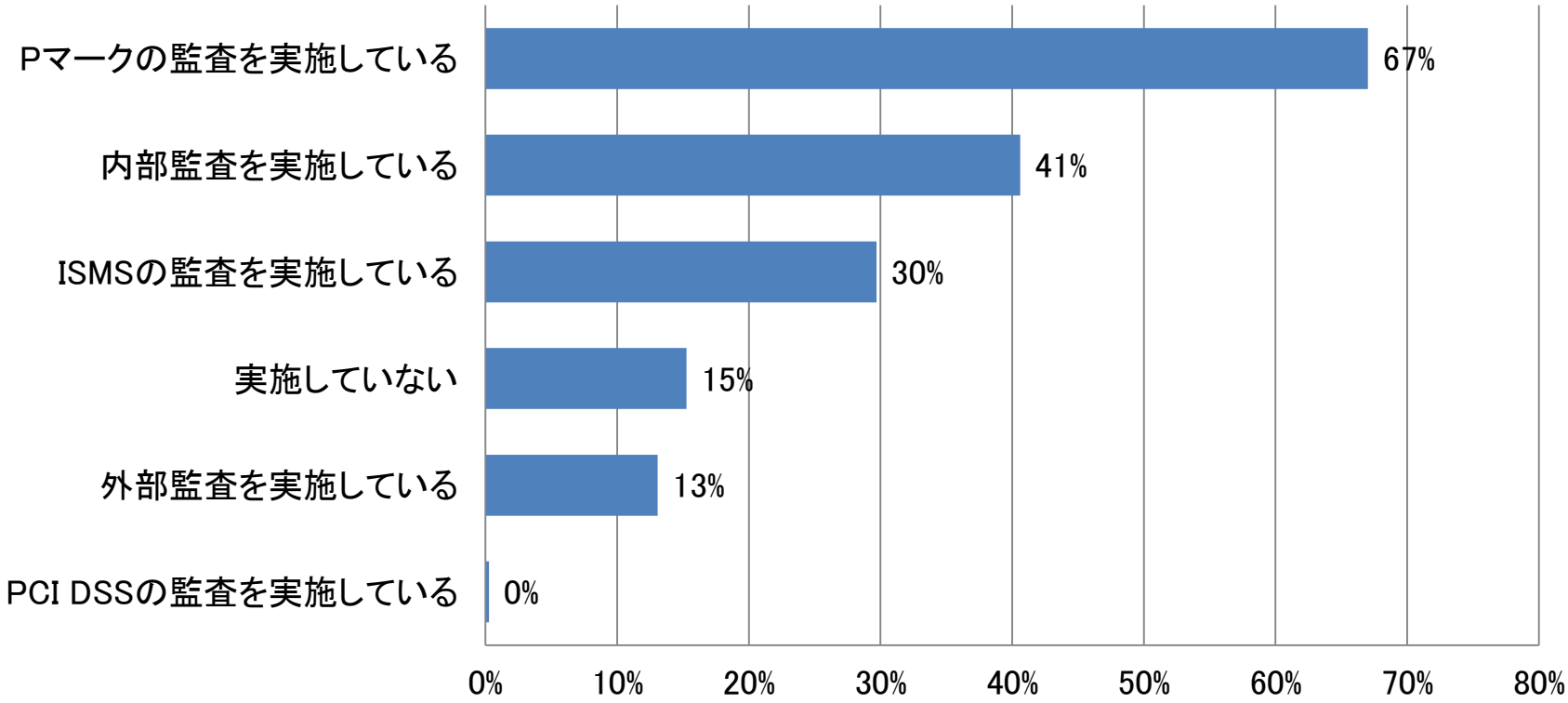


PC数300台以下の企業が65%を占める。

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．情報セキュリティ監査の実施(N=367)



Pマークの監査実施が67%。ISMSの監査実施が30%となっている。

考察(第1章　概要(回答者の基本データ等))

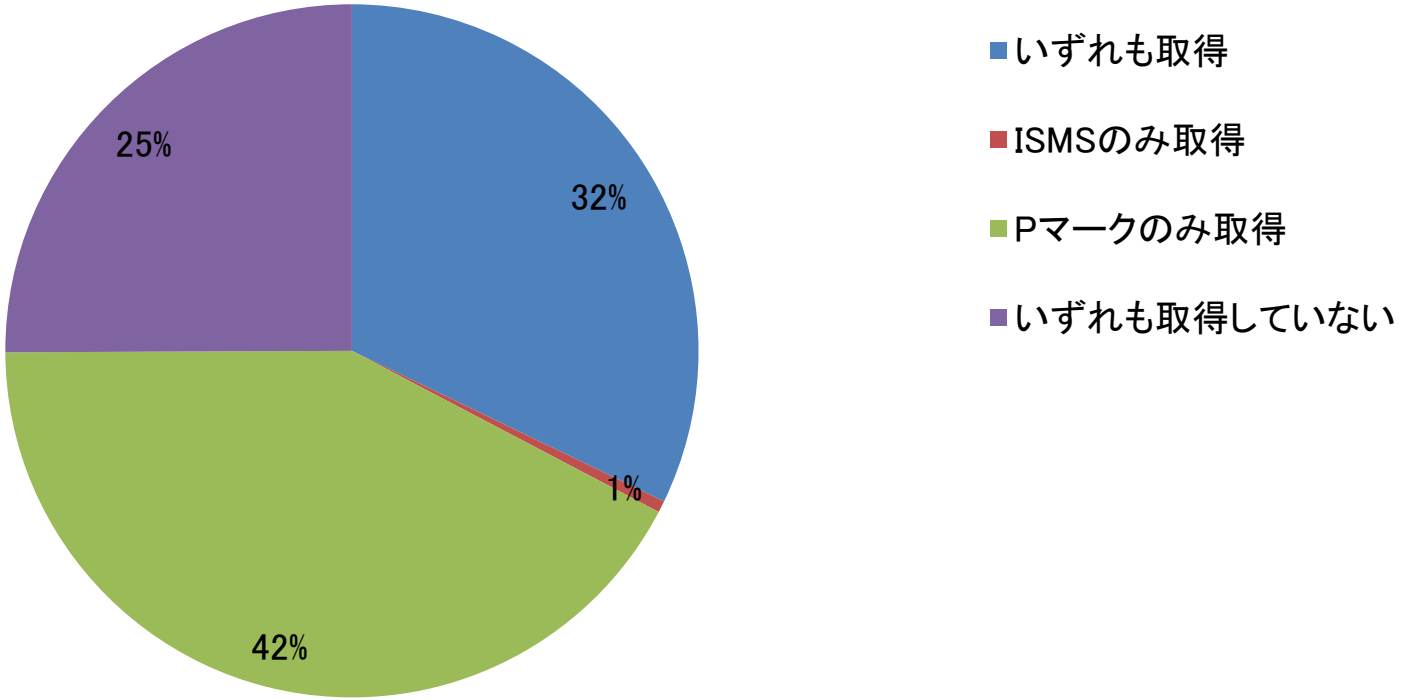
- アンケートに回答いただいた組織の傾向としては、従業員数300名以下が70%となり、中小規模の組織が多くなっている。

- 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

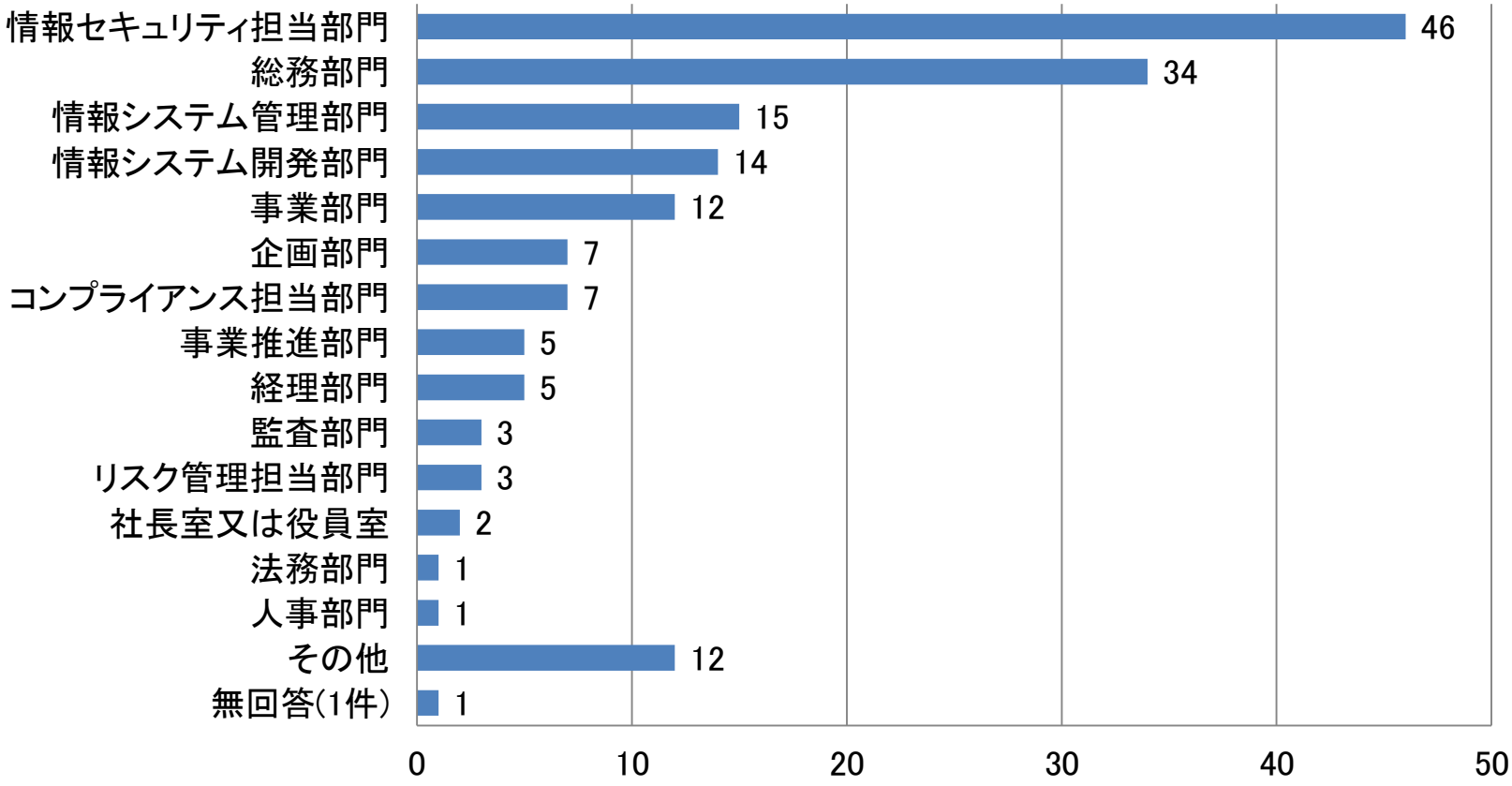
設問8．貴社ではプライバシーマーク（Pマーク）またはISMSを取得していますか。
（N=367）



ISMSを取得している組織は、33%。Pマークは、74%。

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．ISMSを管理している部門をお答えください。(複数選択可)(N=120)



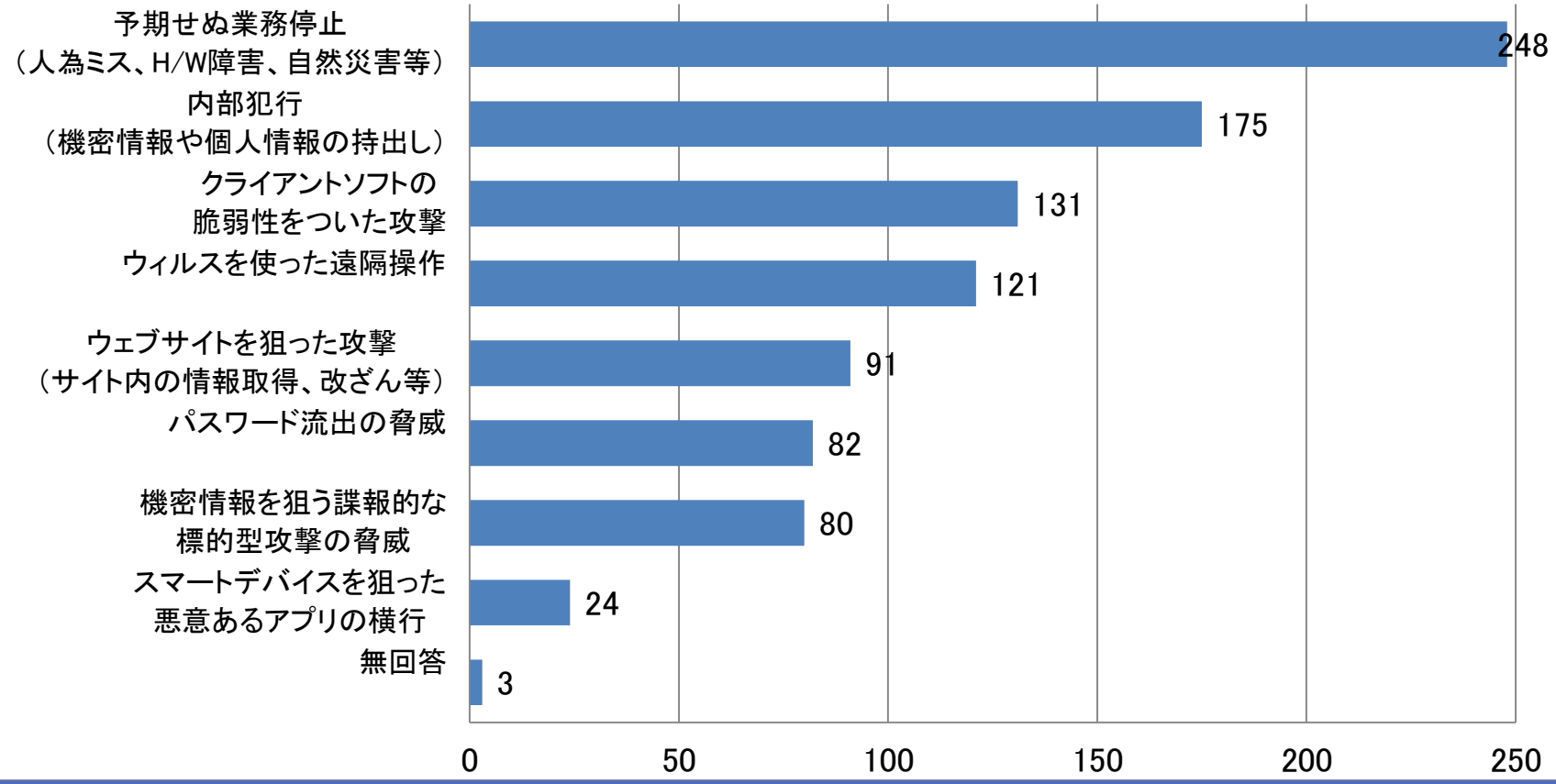
※設問8.で**「いずれも取得」**又は**「ISMSのみ取得」**と回答した組織のみ

情報セキュリティ担当部門が多い。

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10. 情報セキュリティ上の脅威のうち、現時点で重視するものはどれですか。
（〇印は3つまで）（N=367）

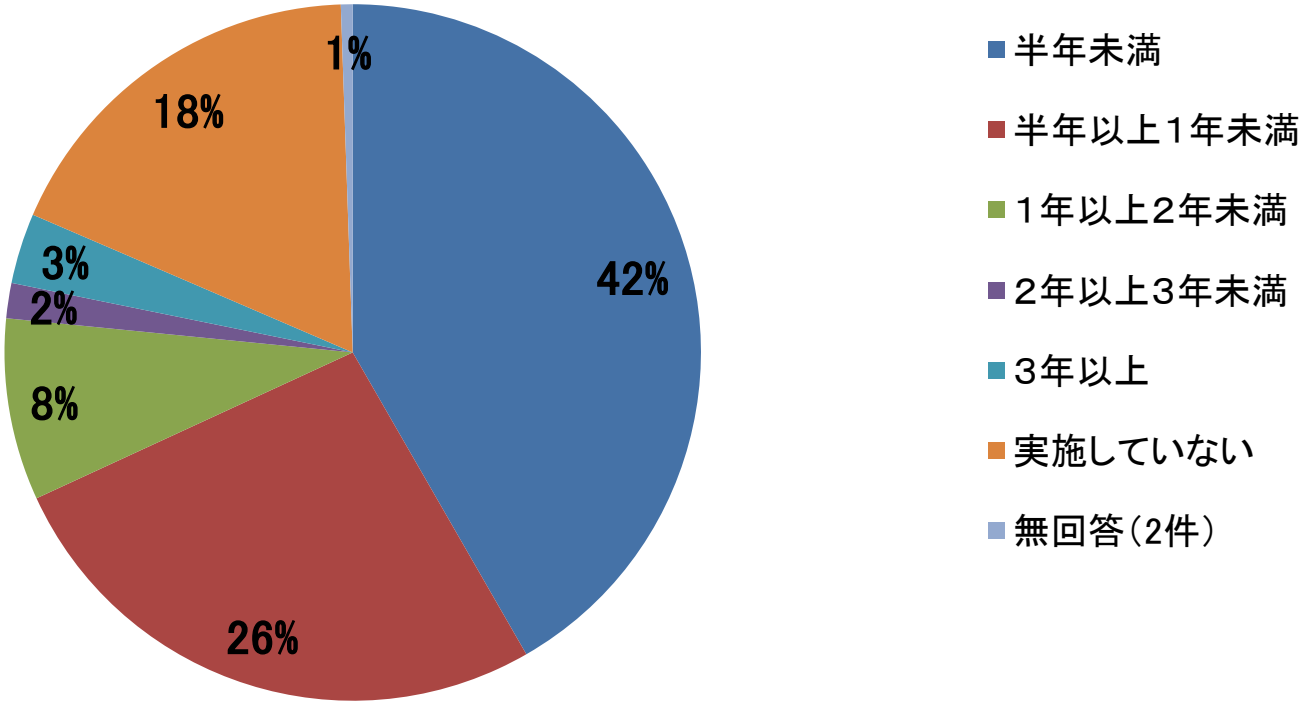


ミスや障害、災害による業務停止に対する意識が高い。

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11. 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いつですか。
（N=367）

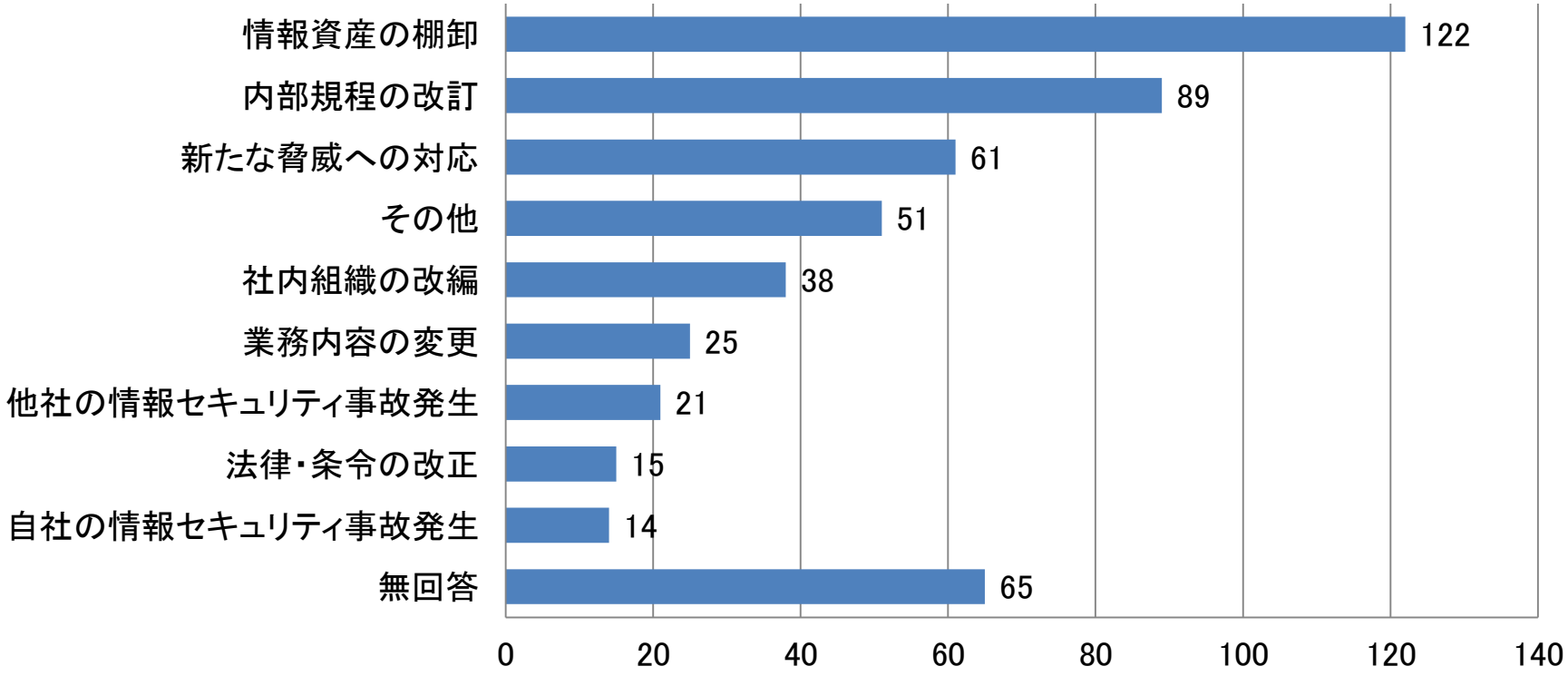


70%近くの組織が、1年以内に実施している。
一方、20%弱はリスク分析を実施していない。

第2章　情報セキュリティマネジメントの取組み状況

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

設問12. リスク分析を実施した理由として当てはまるものはどれですか。
（複数選択可）(N=367)

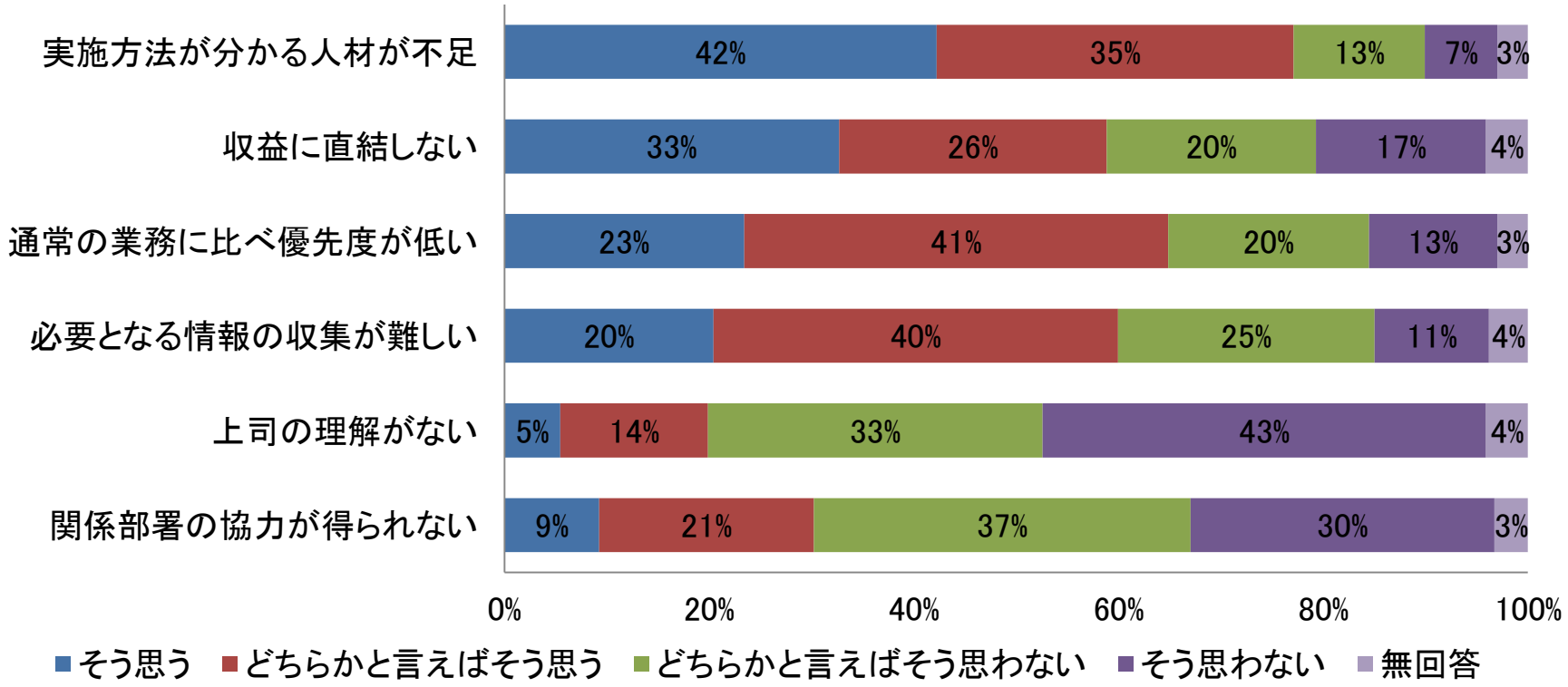


情報資産の棚卸が最も多く、内部規程の改訂、新たな脅威への対応が続く。

第2章　情報セキュリティマネジメントの取組み状況

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

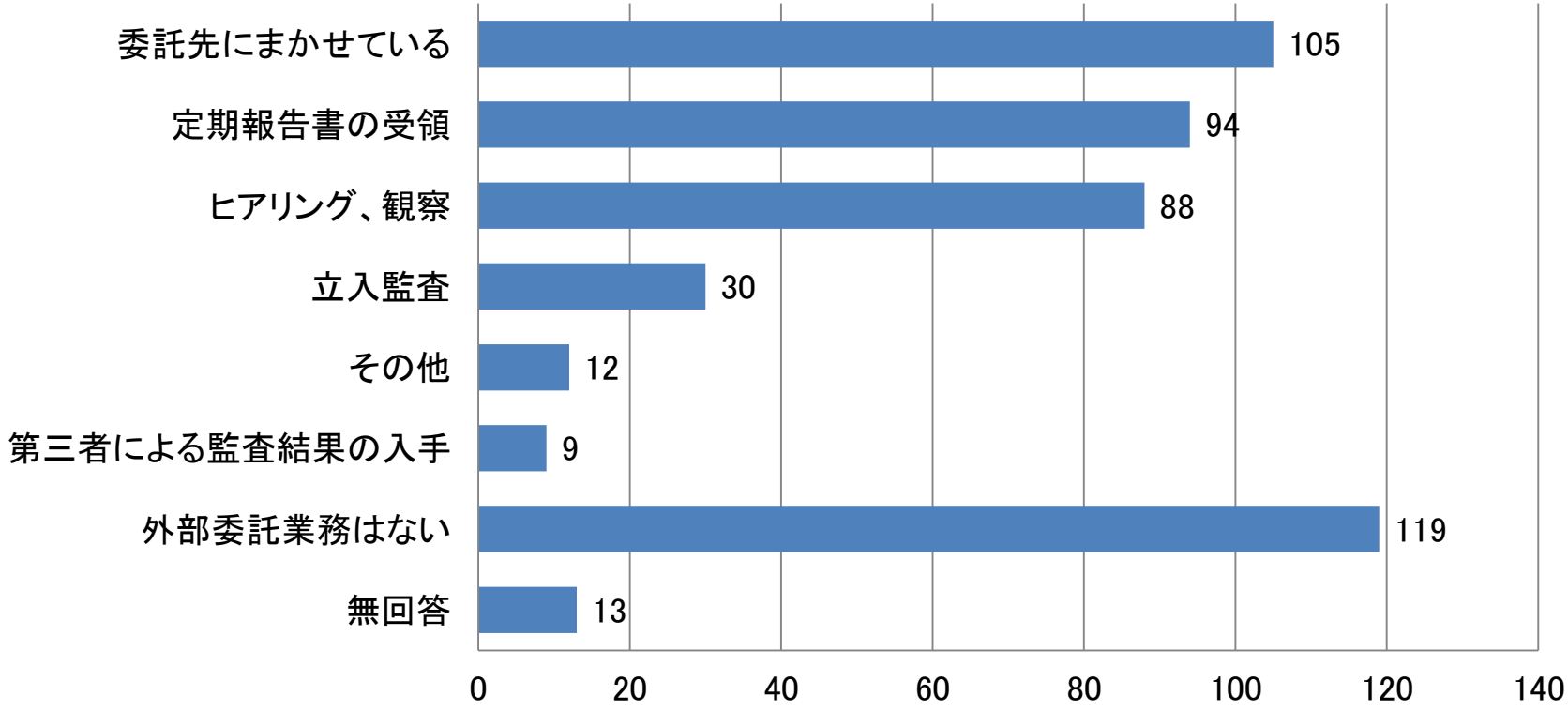
設問13. リスク分析を行う際の問題点について、最も近い番号にひとつずつ〇印を付けてください。（N=367）



人材の不足を感じる組織が77%。

第2章　情報セキュリティマネジメントの取組み状況

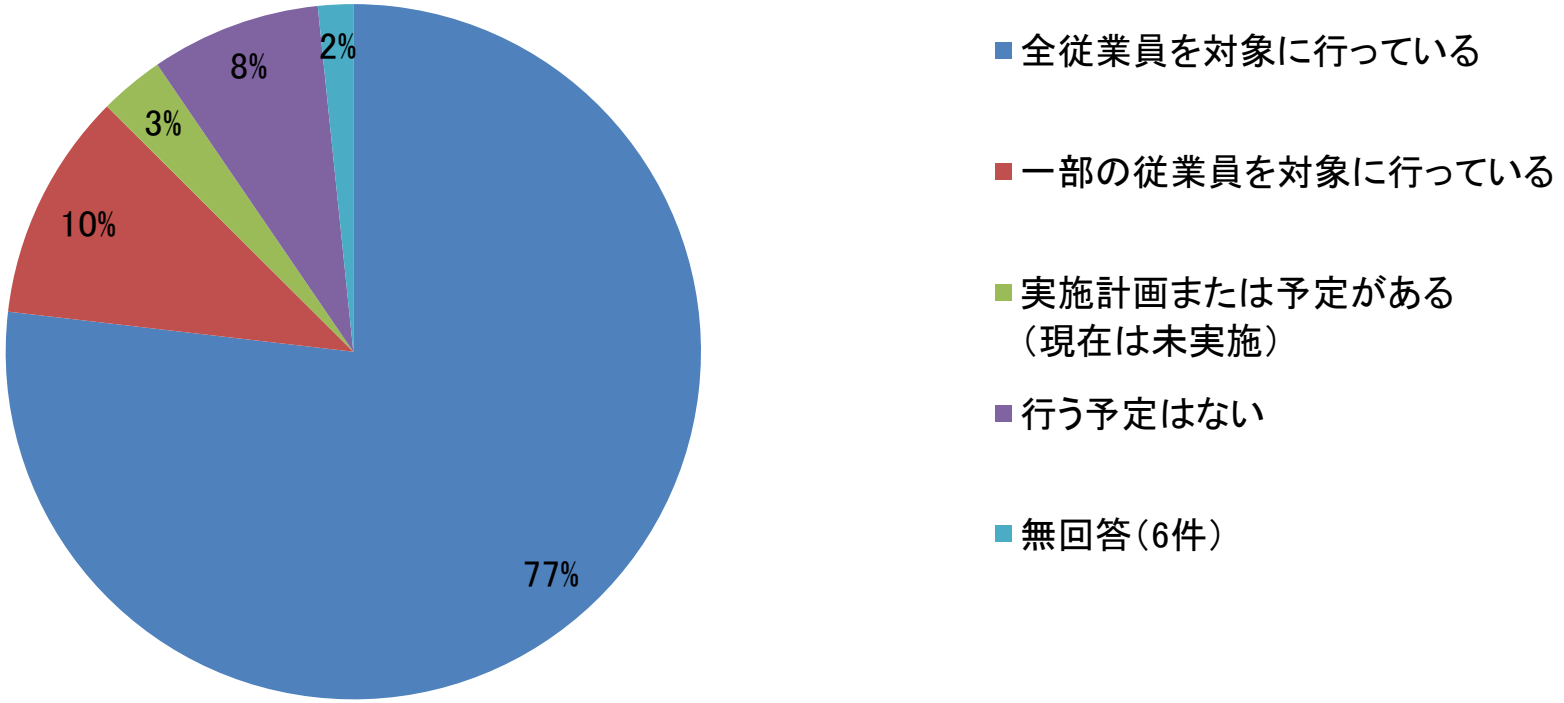
設問14. 外部委託している運用中のシステムのセキュリティ管理は、どのような手法を用いていますか。（複数選択可）（N=367）



報告書の受領やヒアリング・観察が大半、委託先まかせの組織も多い。

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15. システム部門以外の従業員に対して、情報セキュリティ教育を行っていますか。(N=367)



87%の組織で実施されているが、11%で未実施。

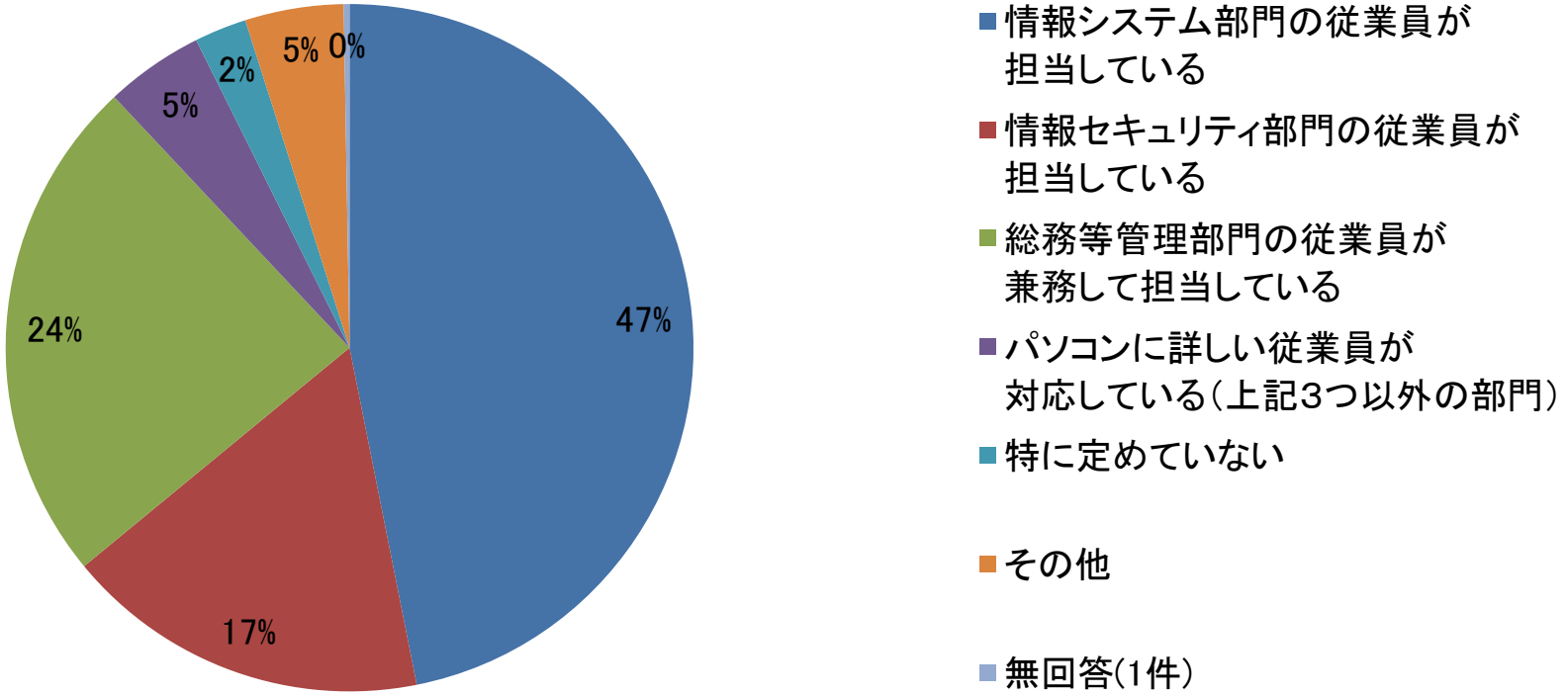
考察（第2章　情報セキュリティマネジメントの取組み状況）

- ISMS取得組織は33%で、その多くでPマークも取得されており、ISMSの単独取得は少ない。また、ISMSの管理部門は情報セキュリティ担当部門であることが多い。Pマークの取得組織は74%で、2012年度の調査と同水準である。
- 標的型攻撃などの新たな攻撃手法よりも、ミスや障害、災害による業務停止や内部犯行など、従来からの脅威を重視する組織が多い。
- リスク分析では、実施できる人材の不足を感じている組織が多い。一方で、上司の理解や関係部署の協力が得られないと感じている組織は少なく、リスク分析に組織一体で取組む枠組みは備わっていることが推測される。リスク分析のタイミングについては、情報資産の棚卸や規程改訂など、受動的なものが多い。
- 委託先の情報セキュリティ管理手法は、報告書の受領やヒアリング・観察が大半であり、完全に委託先任せとなっている組織も多い。立入監査や第三者による監査結果など、監査の手法を取り入れている組織は少ない。

第３章
情報セキュリティ管理体制、人材育成及び情報セキュリティ教育

第3章　情報セキュリティ管理体制、人材育成及び情報セキュリティ教育

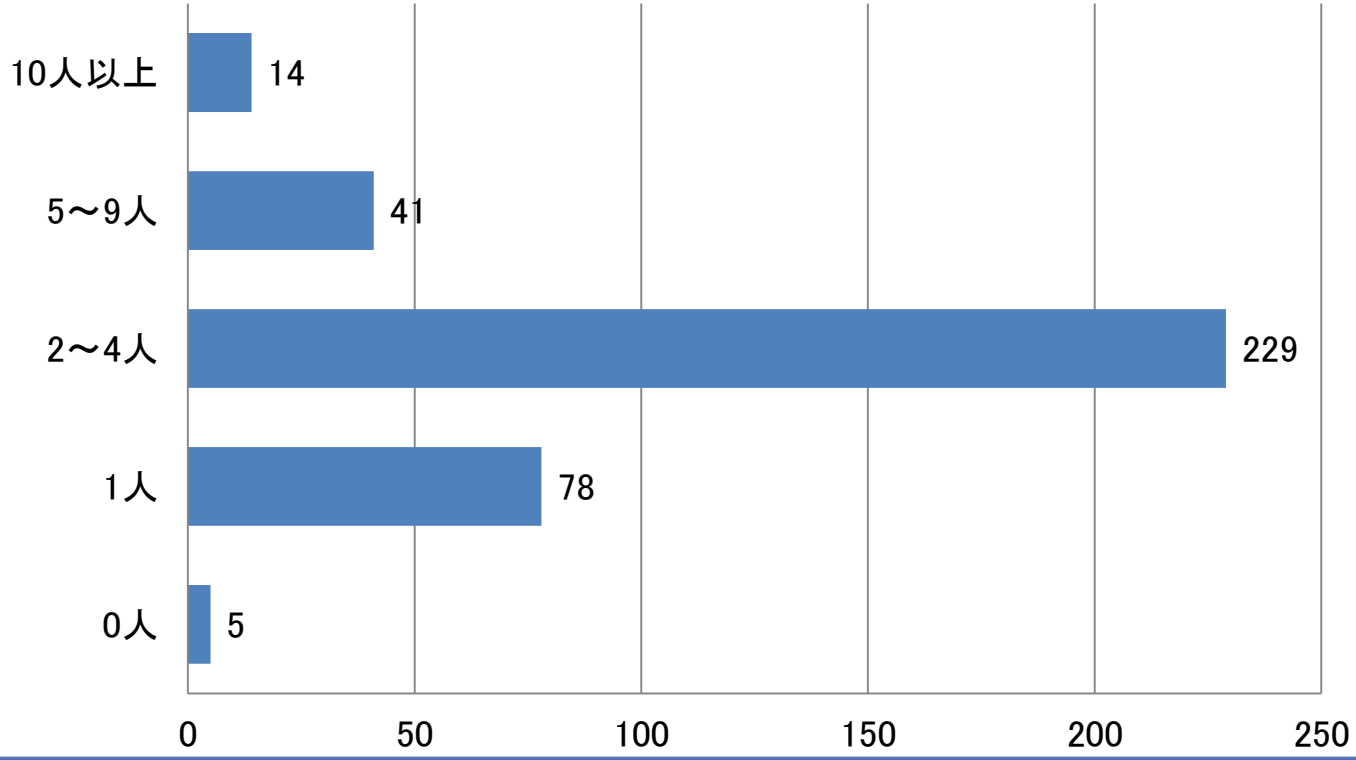
設問16-1. 情報セキュリティを主に管理されているのは、どなたですか。(N=367)



情報システム部門は47%、情報セキュリティ部門は17%、
他部門が兼務は24%であった。

第3章　情報セキュリティ管理体制、人材育成及び情報セキュリティ教育

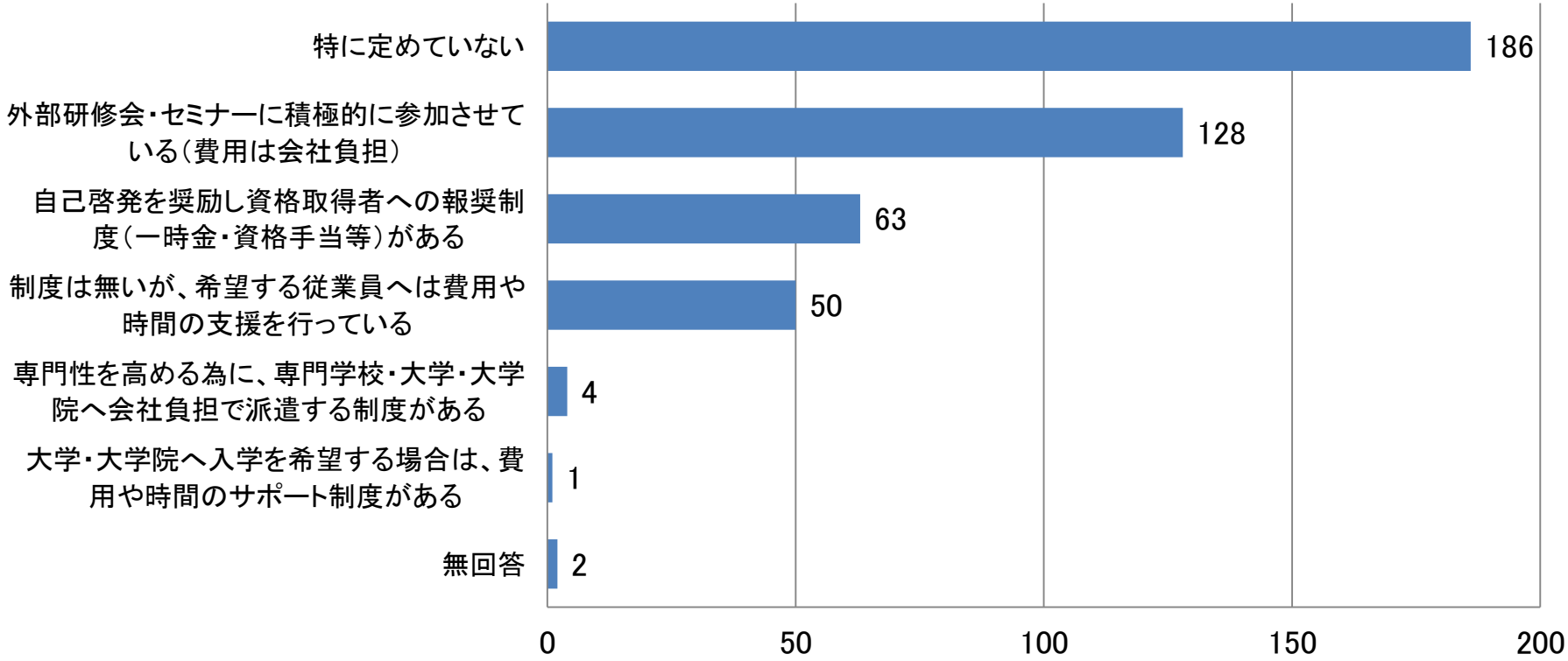
設問16-2. 情報セキュリティの管理を担当されている方は何名いますか。(N=367)



2～4人の組織が過半数である。
管理者が10人以上の組織もある一方、全くいない組織も存在する。

第3章　情報セキュリティ管理体制、人材育成及び情報セキュリティ教育

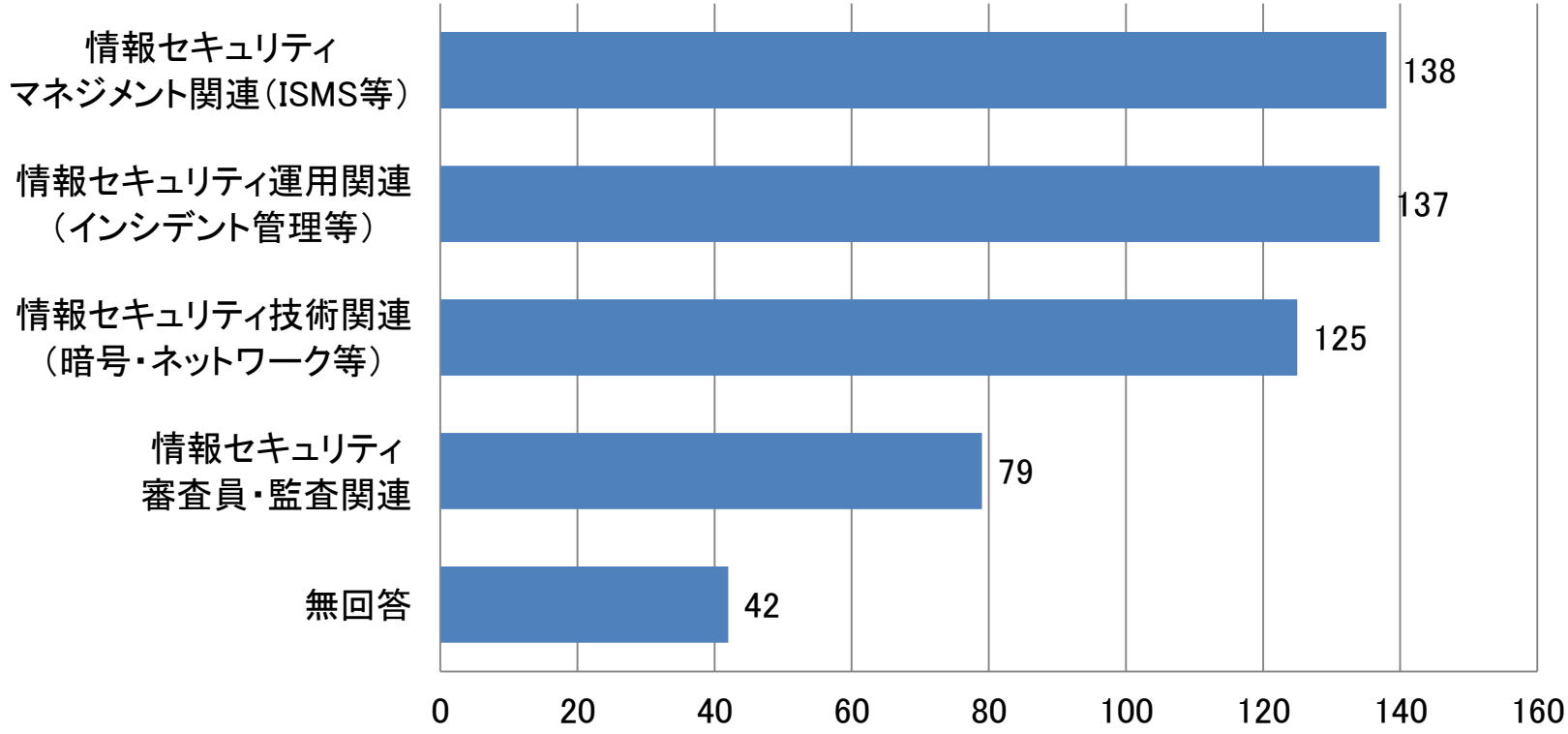
設問17. 情報セキュリティの推進者の人材育成に関してどのような制度等がありますか。（複数選択可）（N=367）



約半数の組織が、情報セキュリティの推進者の人材育成に関する制度を定めていない。

第3章　情報セキュリティ管理体制、人材育成及び情報セキュリティ教育

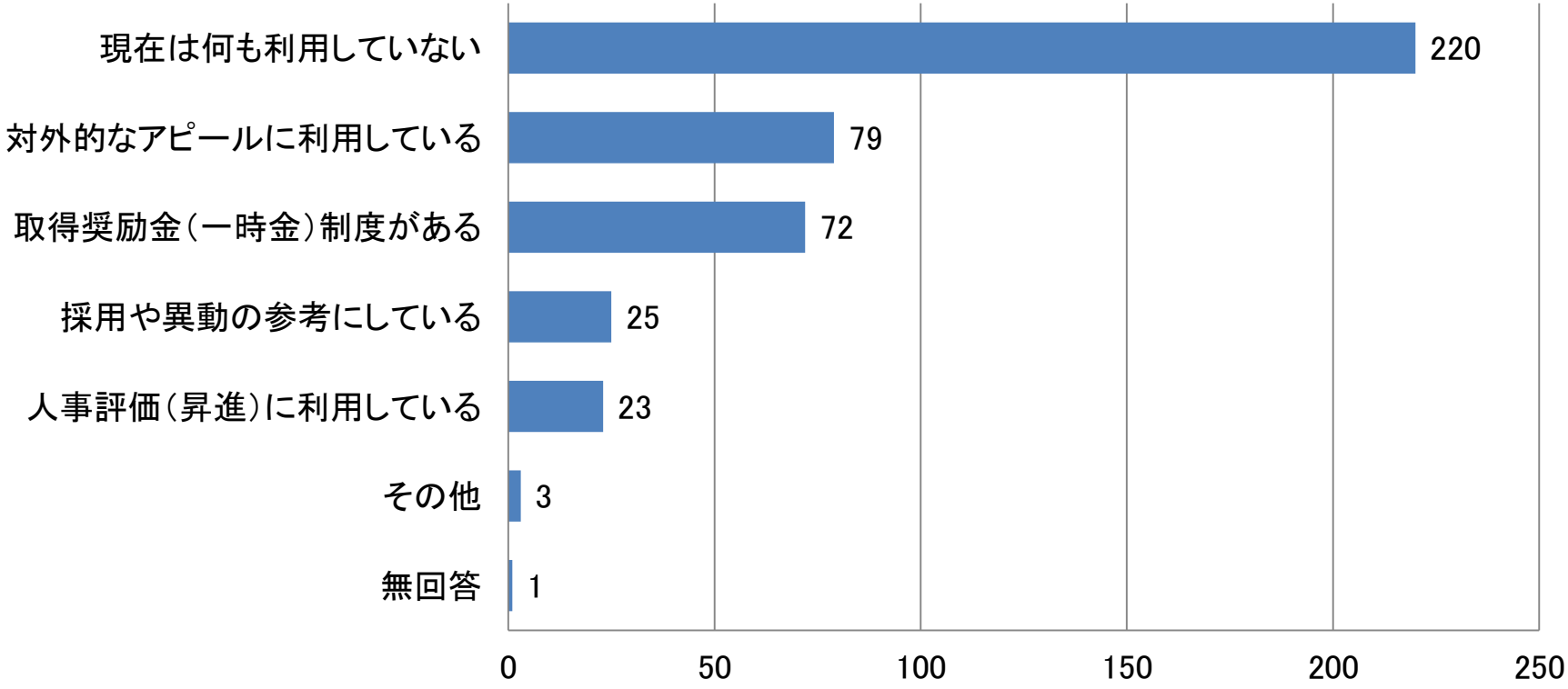
設問18. 貴社で今後必要と思われる情報セキュリティ関連の資格は何ですか。（複数選択可）（N=367）



技術・マネジメント関連資格の必要性は高いが、監査関連の資格は低い。

第3章　情報セキュリティ管理体制、人材育成及び情報セキュリティ教育

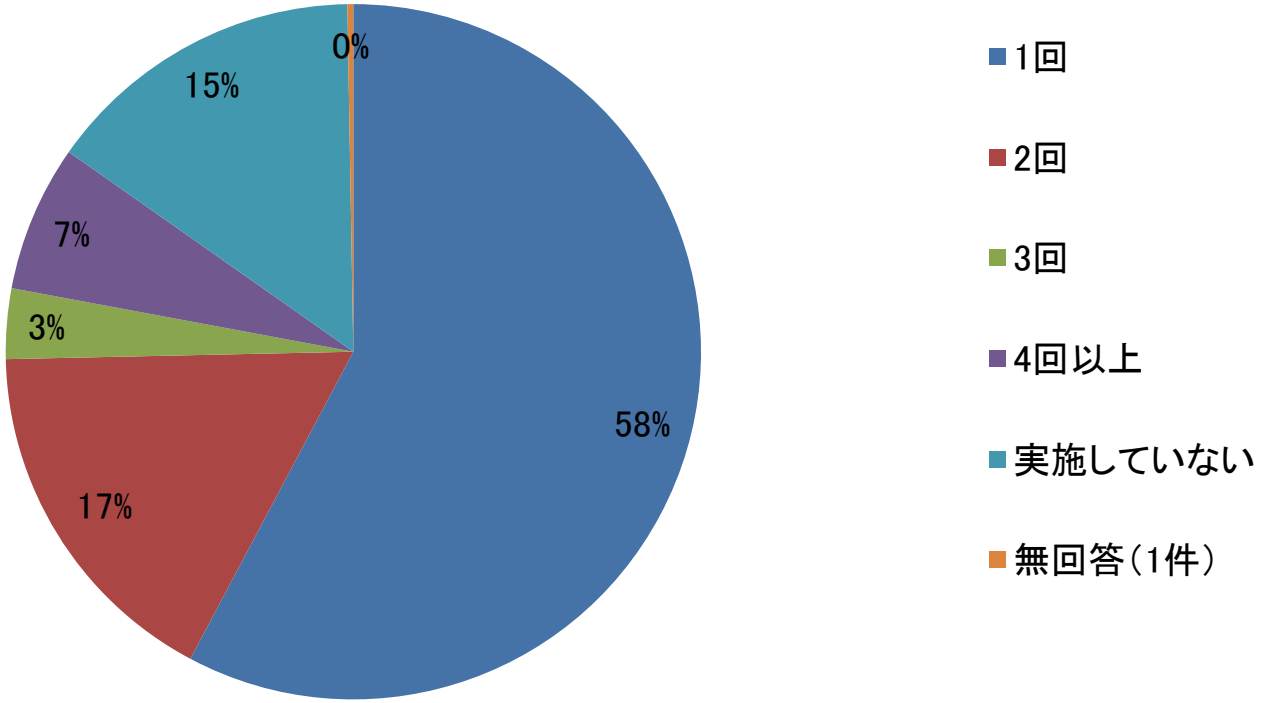
設問19. 情報セキュリティ関連の資格保有を組織の活動に利用していますか。（複数選択可）（N=367）



あまり活用されていないのが現状である。

第3章　情報セキュリティ管理体制、人材育成及び情報セキュリティ教育

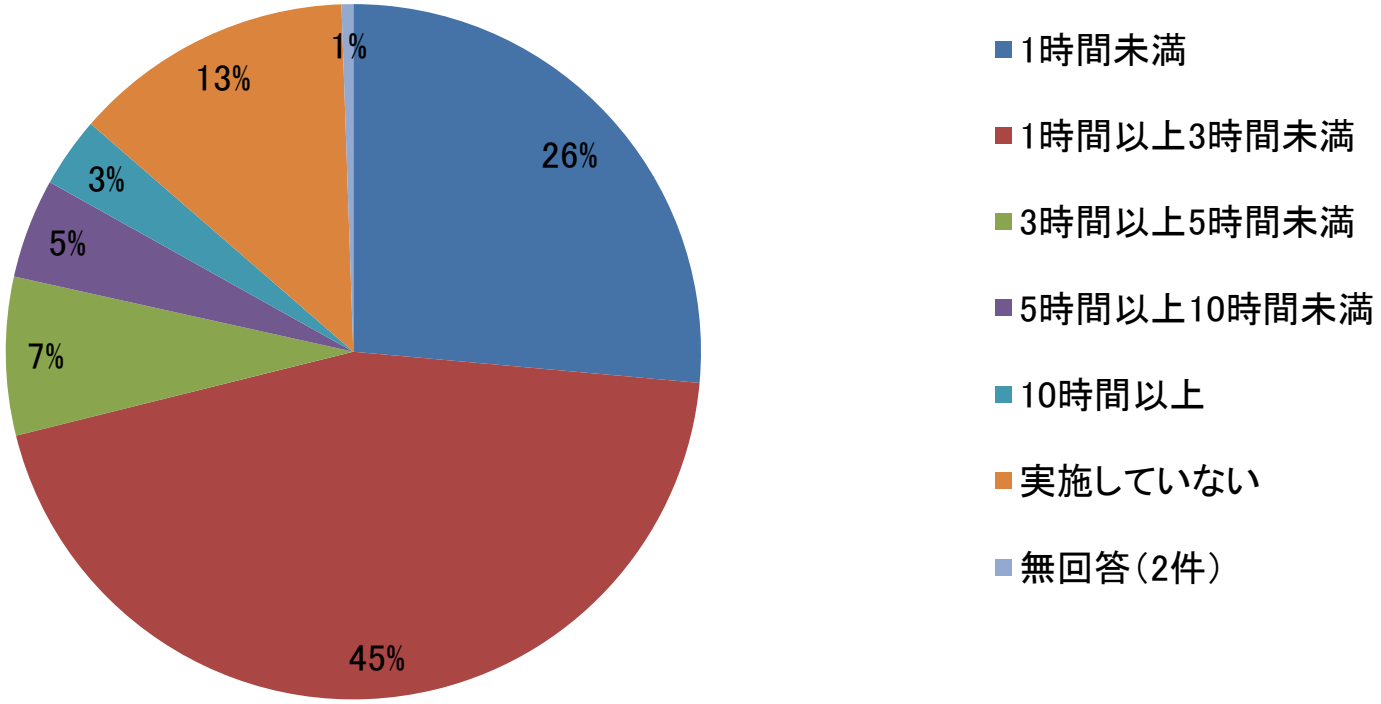
設問20−1. 情報セキュリティに関する従業員への教育（集合研修・Eラーニング等）に関してお伺いします。
従業員への教育は年間何回位実施していますか。（N=367）



80%の組織が年に1回以上情報セキュリティ教育を行っている。

第3章　情報セキュリティ管理体制、人材育成及び情報セキュリティ教育

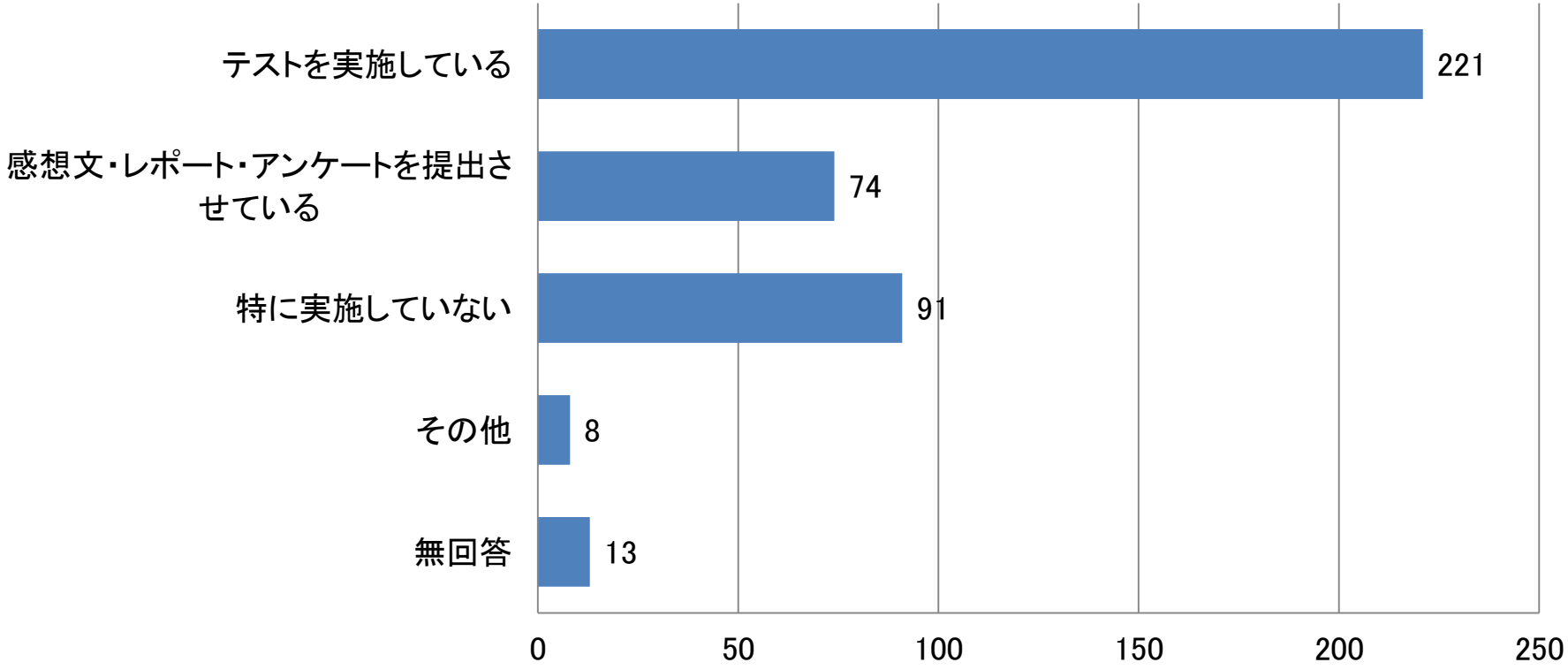
設問20-2. 情報セキュリティに関する従業員への教育（集合研修・Eラーニング等）に関してお伺いします。
従業員への教育は年間延べ何時間位実施していますか。（N=367）



80%の組織が年に1回以上情報セキュリティ教育を行っている。

第3章　情報セキュリティ管理体制、人材育成及び情報セキュリティ教育

設問20-3. 情報セキュリティに関する従業員への教育（集合研修・Eラーニング等）に関してお伺いします。
上記従業員への教育の効果を確認していますか。（複数選択可）(N=367)



教育の効果の確認にテスト等を実施する組織が多い。

考察（第３章　情報セキュリティ管理体制、人材育成及び情報セキュリティ教育）

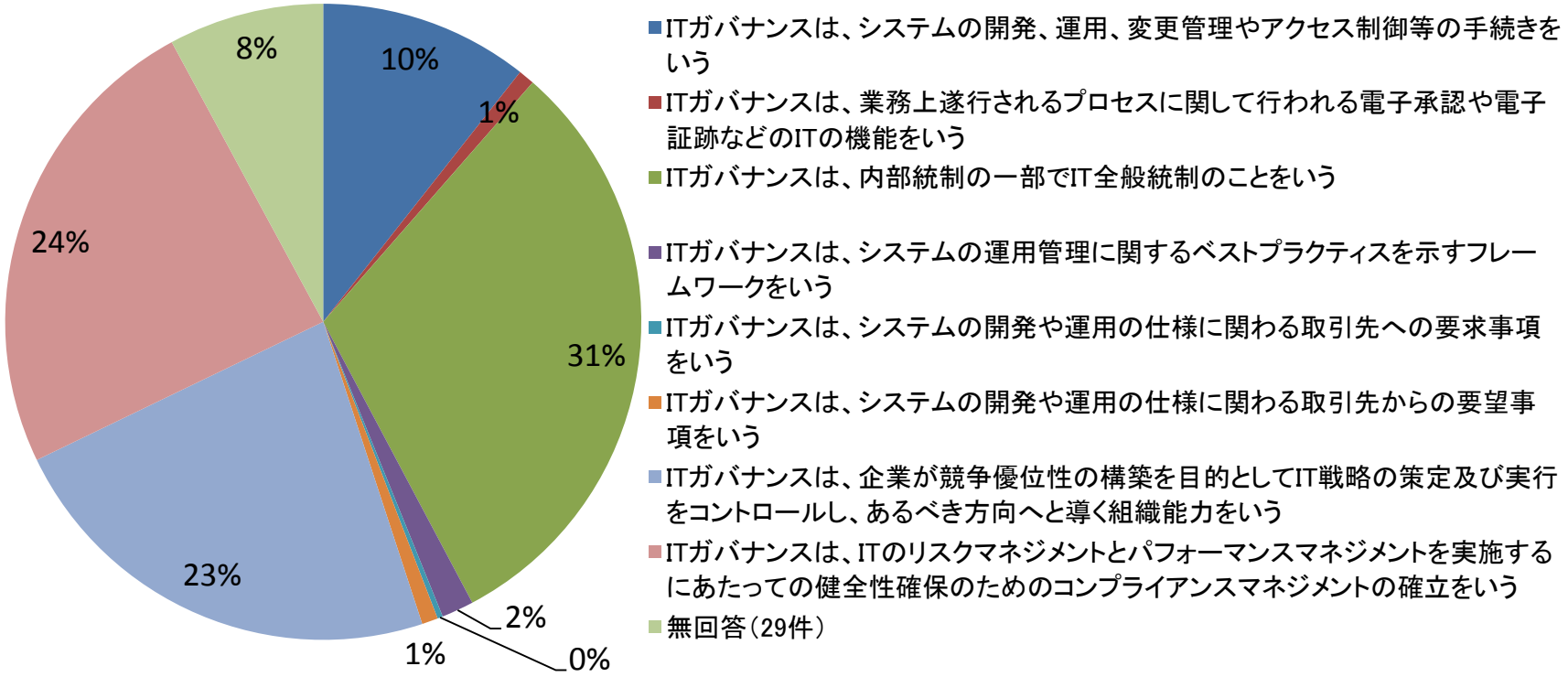
- 約半数の組織が情報セキュリティの推進者の人材育成に関する制度を定めていない。セミナー等の短期間の教育については制度を定めている組織が1/3程度ある一方、教育機関への派遣等、長期間の育成に関する制度を定めている企業は少数である。
- マネジメント、運用、技術など組織の実務に必要な資格について関心は高いが、審査・監査の関連資格については関心が低い。
- 情報セキュリティ関連の資格を、対外的アピール、採用・異動・昇進等の人事に活用している組織は少数だが存在する。しかしながら、多くの組織において、情報セキュリティ関係の資格を活用していない。
- 80%の組織が年１回以上情報セキュリティの教育を行っている。教育を行っている大半の組織が年に１回の教育である。

第4章
情報セキュリティのガバナンス

第4章　情報セキュリティのガバナンス

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

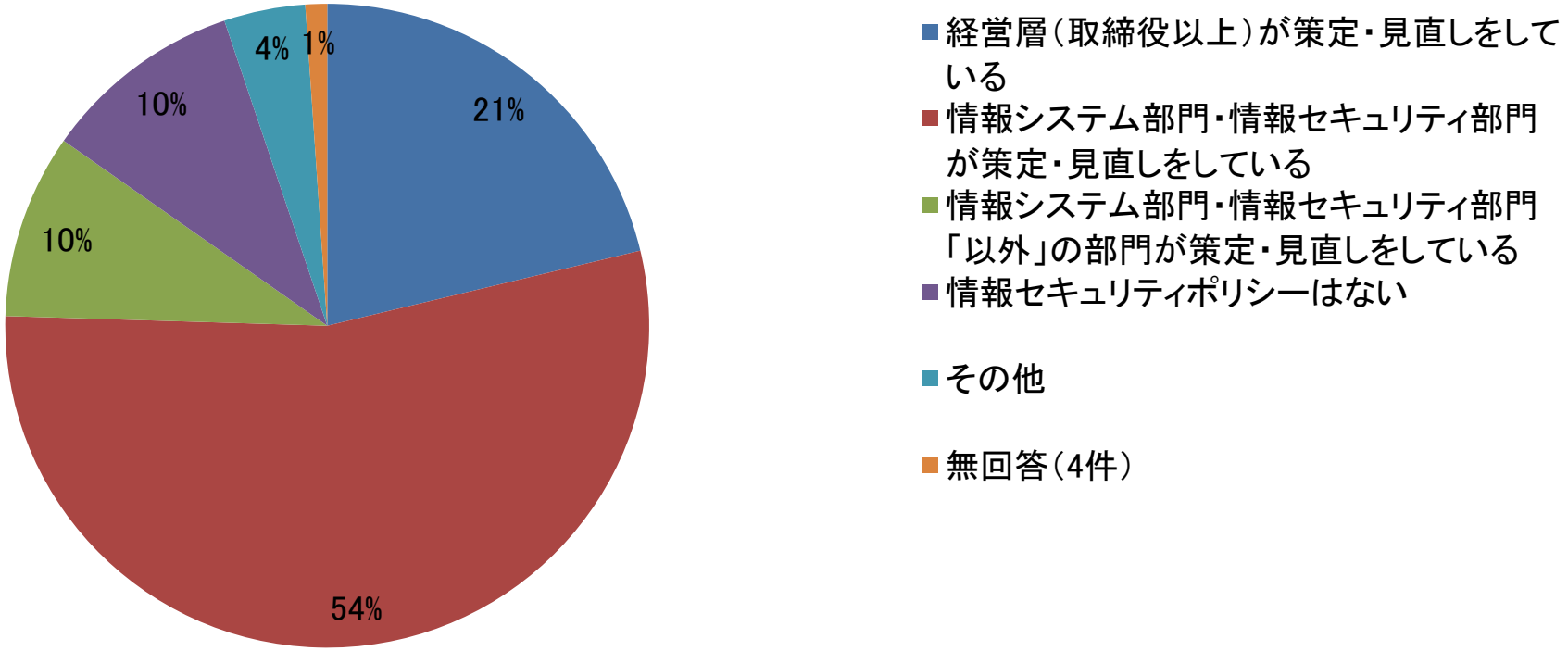
設問21. ITガバナンスの定義について次のうちから自分の考えに近いものを選んでください。（N=367）



ITガバナンスの定義に関して、さまざまな理解がある。

第4章　情報セキュリティのガバナンス

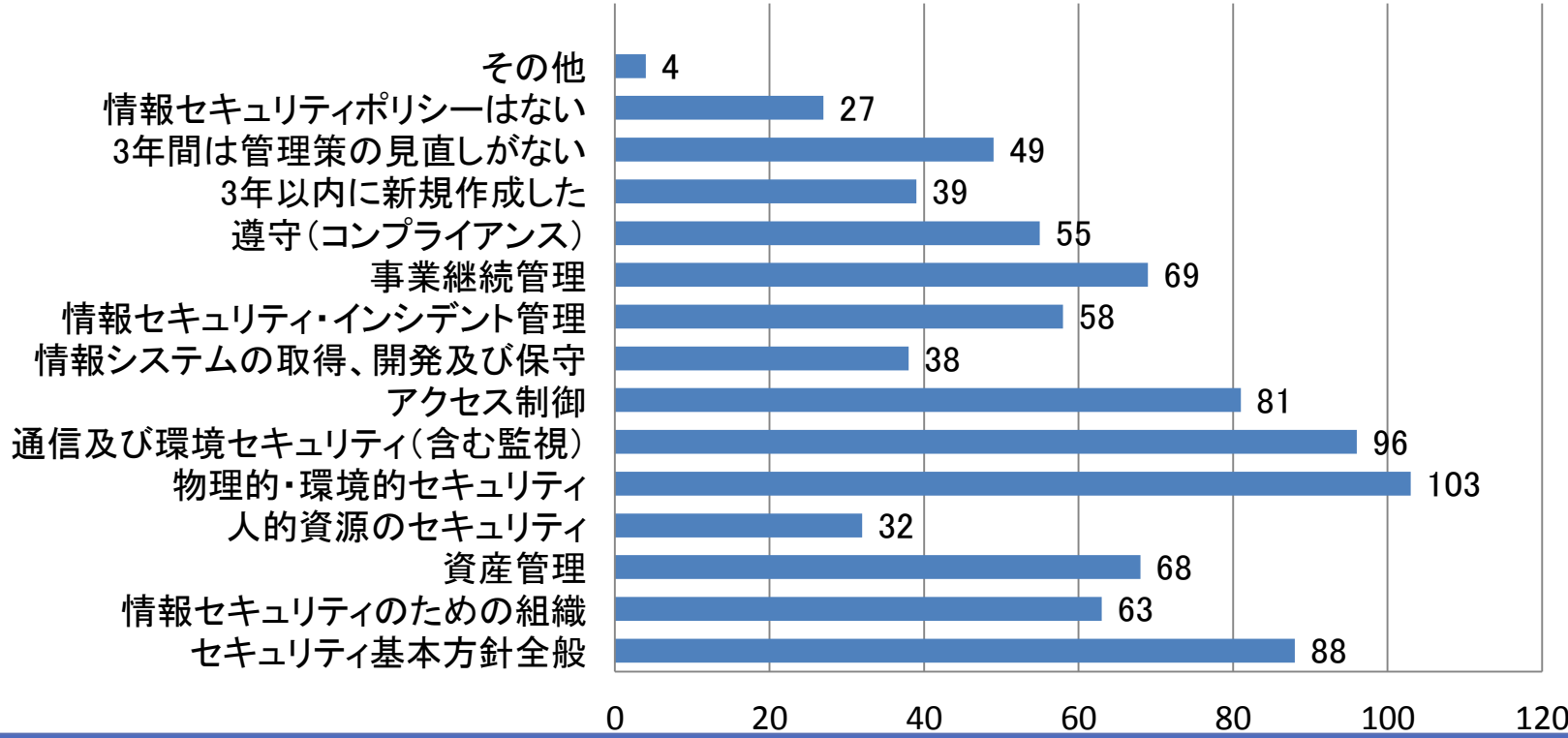
設問22. 情報セキュリティポリシー(全体)の策定・見直しの手続きについてお伺いします。手続きを行っているのはどの部門ですか。(N=367)



情報システム・情報セキュリティ部門が
策定・更新を行っているケースが多い。

第4章　情報セキュリティのガバナンス

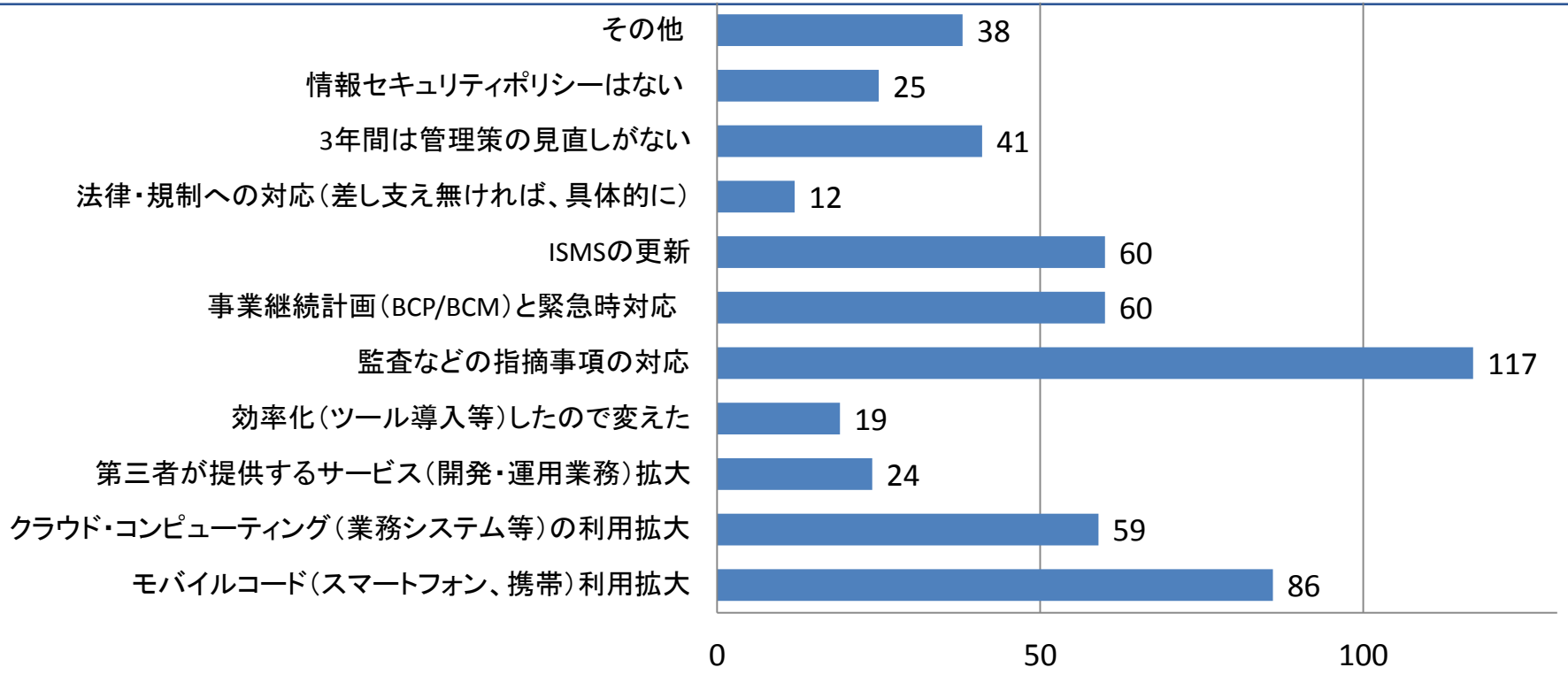
設問23. 情報セキュリティポリシー(全体)についてお伺いします。過去3年(2010年以降)でどの’管理策の項目’を見直しましたか。(複数選択可) (N=367)



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4章　情報セキュリティのガバナンス

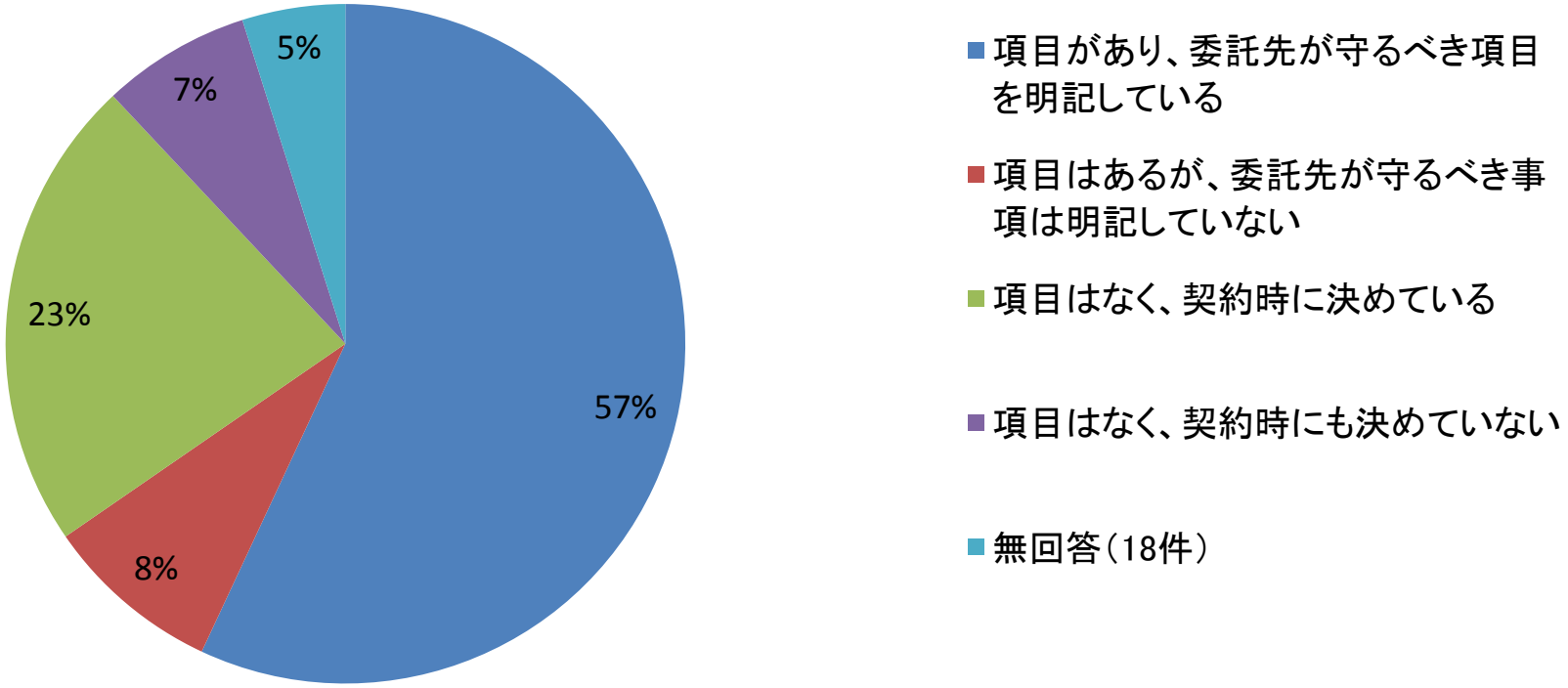
設問24. 過去3年で情報セキュリティポリシーを見直した理由として当てはまるものはどれですか。(複数選択可) (N=367)



監査指摘の対応やモバイル・クラウドへの対応
また、事業継続計画の見直により情報セキュリティポリシーを改定している。

第4章　情報セキュリティのガバナンス

設問25. 情報セキュリティポリシーの中で委託先に関する項目はありますか。
（N=367）

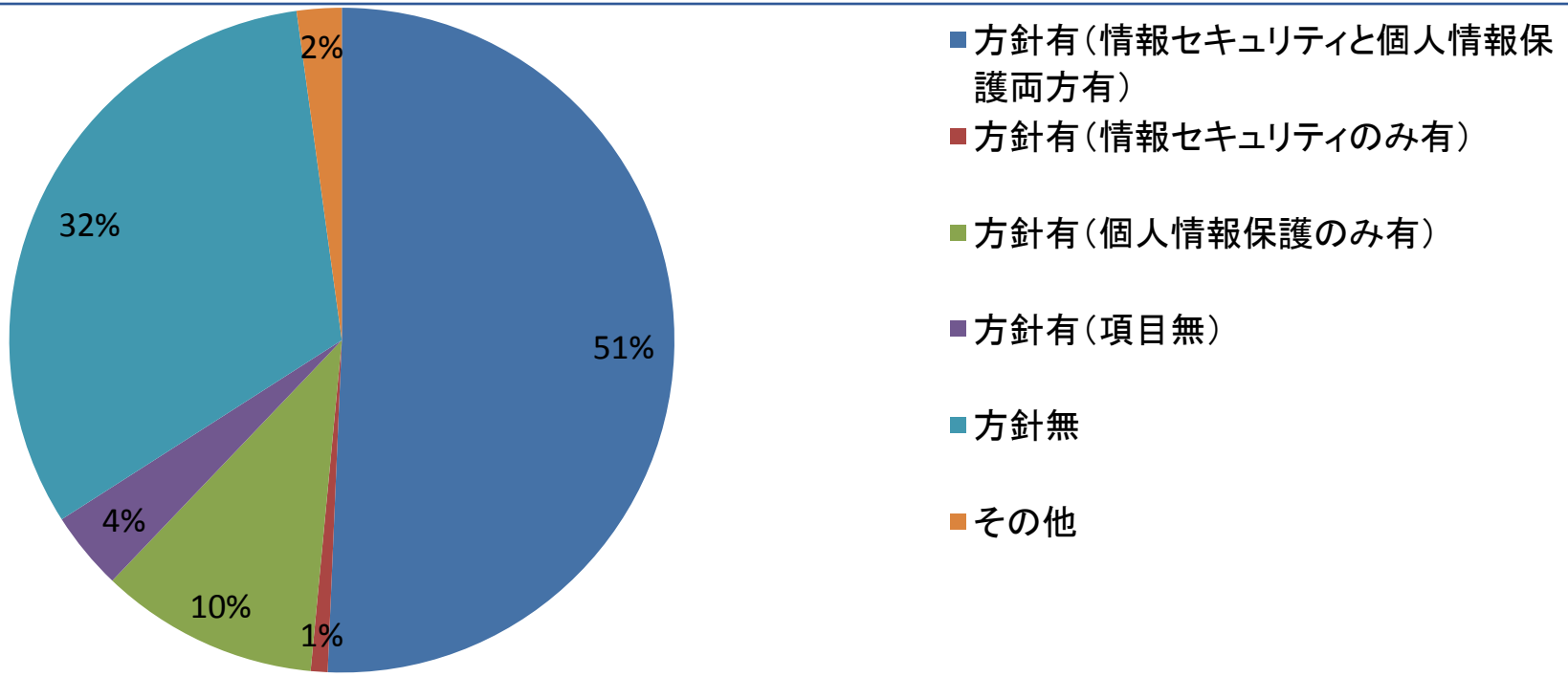


委託先の情報セキュリティに関して、
80%以上がポリシーもしくは契約で何らかの取り決めを定めている。

第4章　情報セキュリティのガバナンス

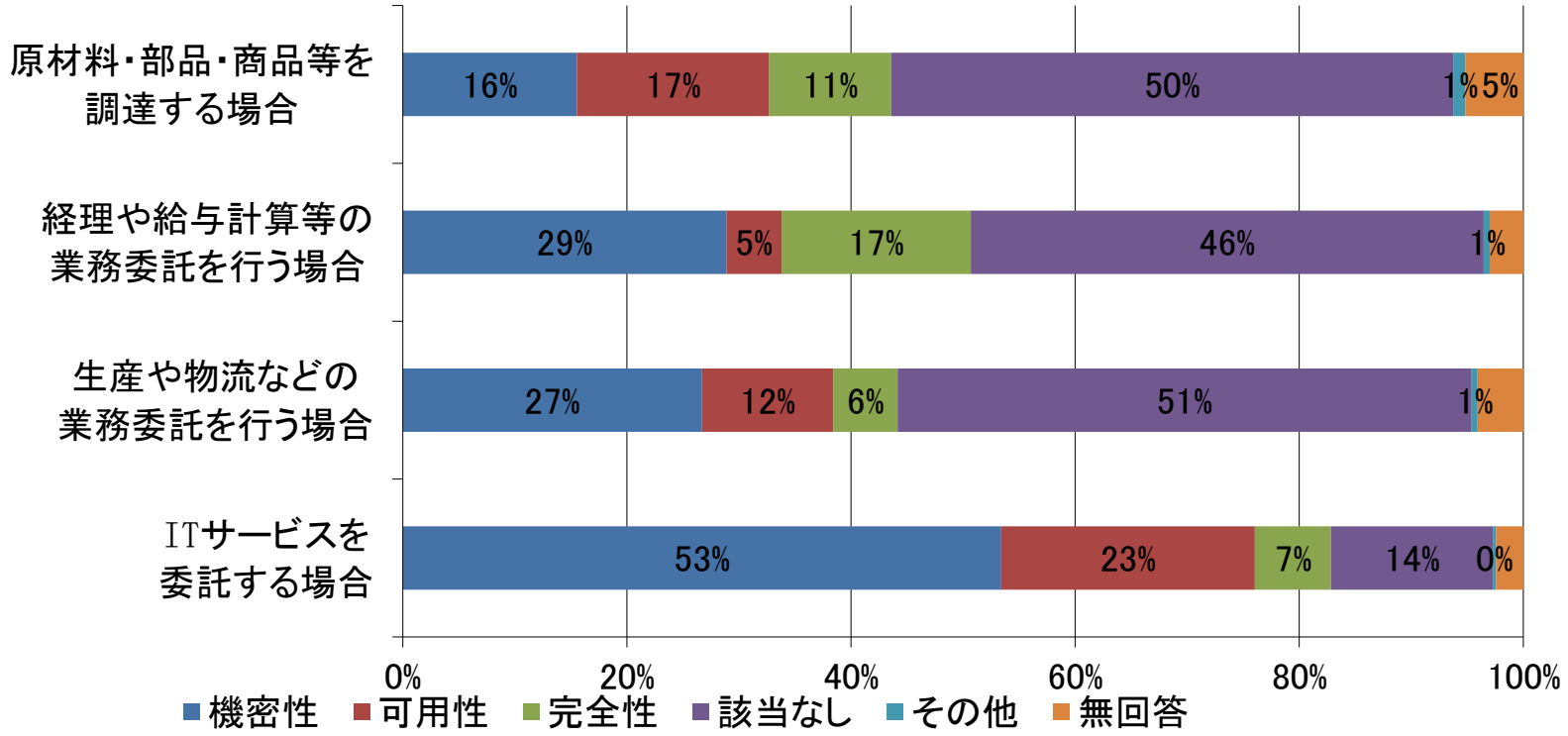
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

設問26. 顧客の立場として、購買方針や調達方針（IT委託、業務委託を含む）が策定されていますか。策定されている場合、個人情報保護および情報セキュリティに関する項目が含まれていますか。（各項目について○印はひとつだけ）（N=367）



購買・調達方針における情報セキュリティに関連した項目は60%強に記載があるが、個人情報保護が若干多い。

設問27. 顧客の立場として委託先・調達先を選定する際、情報セキュリティの観点から最も重要な項目はどれですか。　（各項目について〇印はひとつだけ）(N=367)

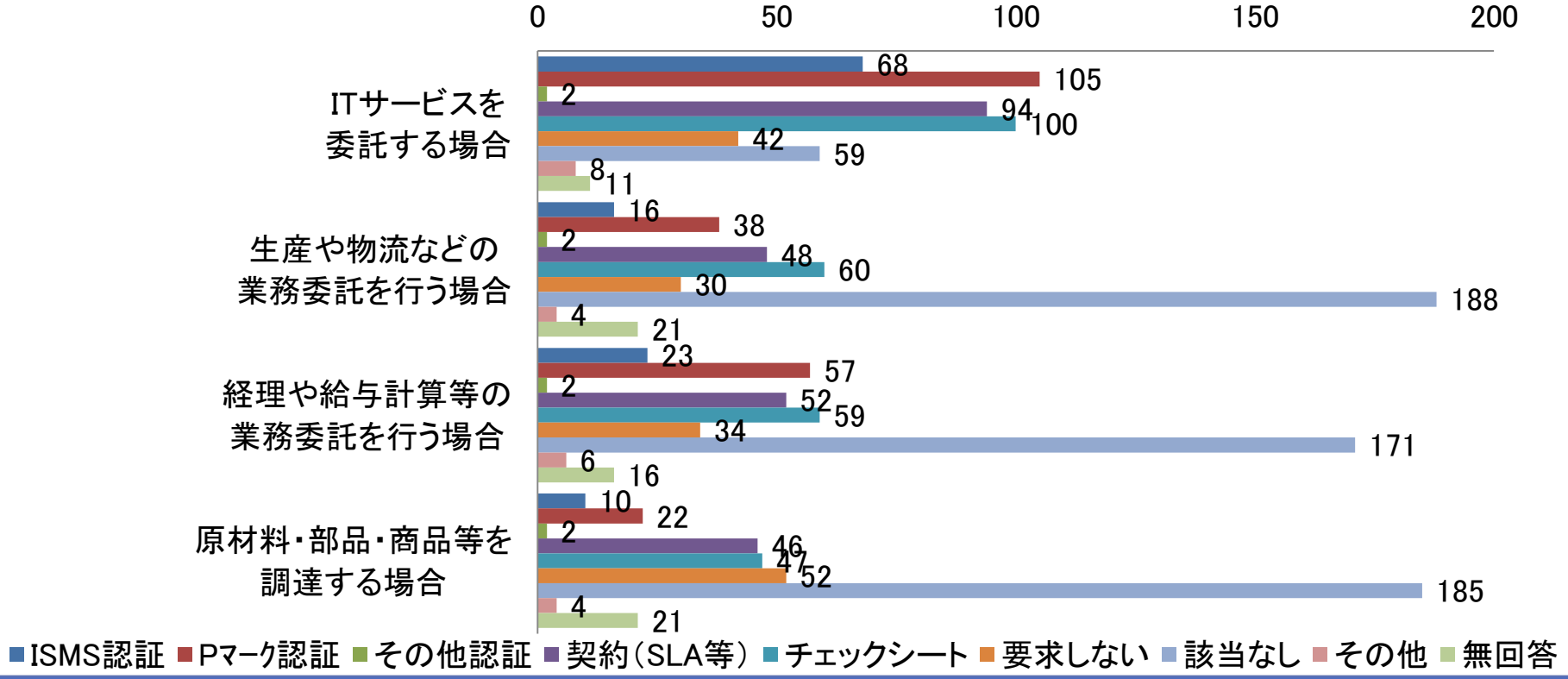


全ての業務で機密性を重視している。
可用性や完全性を重視している業務も多い。

第4章　情報セキュリティのガバナンス

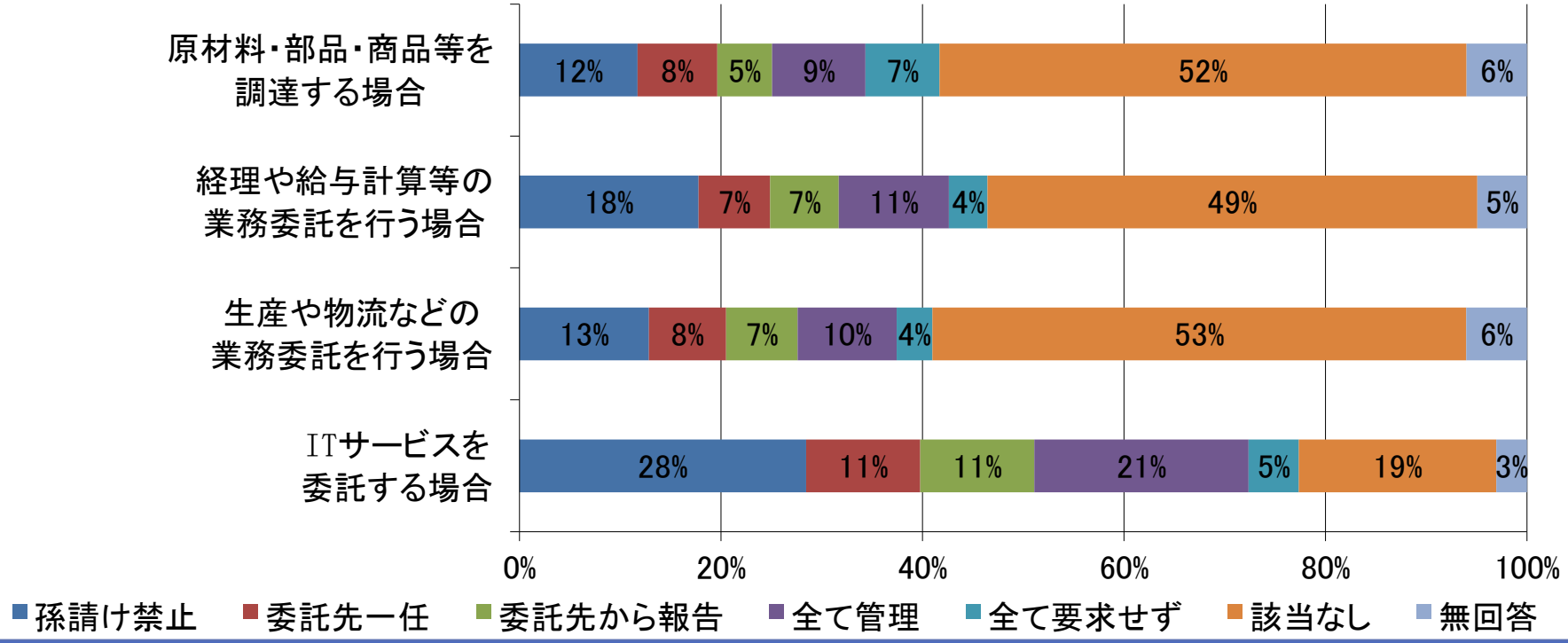
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

設問28. 顧客の立場として委託先を選定する際に、情報セキュリティのリスク対応として要求している事項はどれですか。（各項目について複数選択可）（N=367）



契約やチェックシートといった独自のスペックを定めたものが使われることが多い。第三者認証としてはPマークが比較的多い。

設問29. 顧客の立場として委託先・調達先を選定する際に、下請けになる二次、三次といった委託先・調達先に情報セキュリティ管理（個人情報保護を除く）を要求していますか。該当するものを一つ選んでください。（各項目について○印はひとつだけ）（N=367）

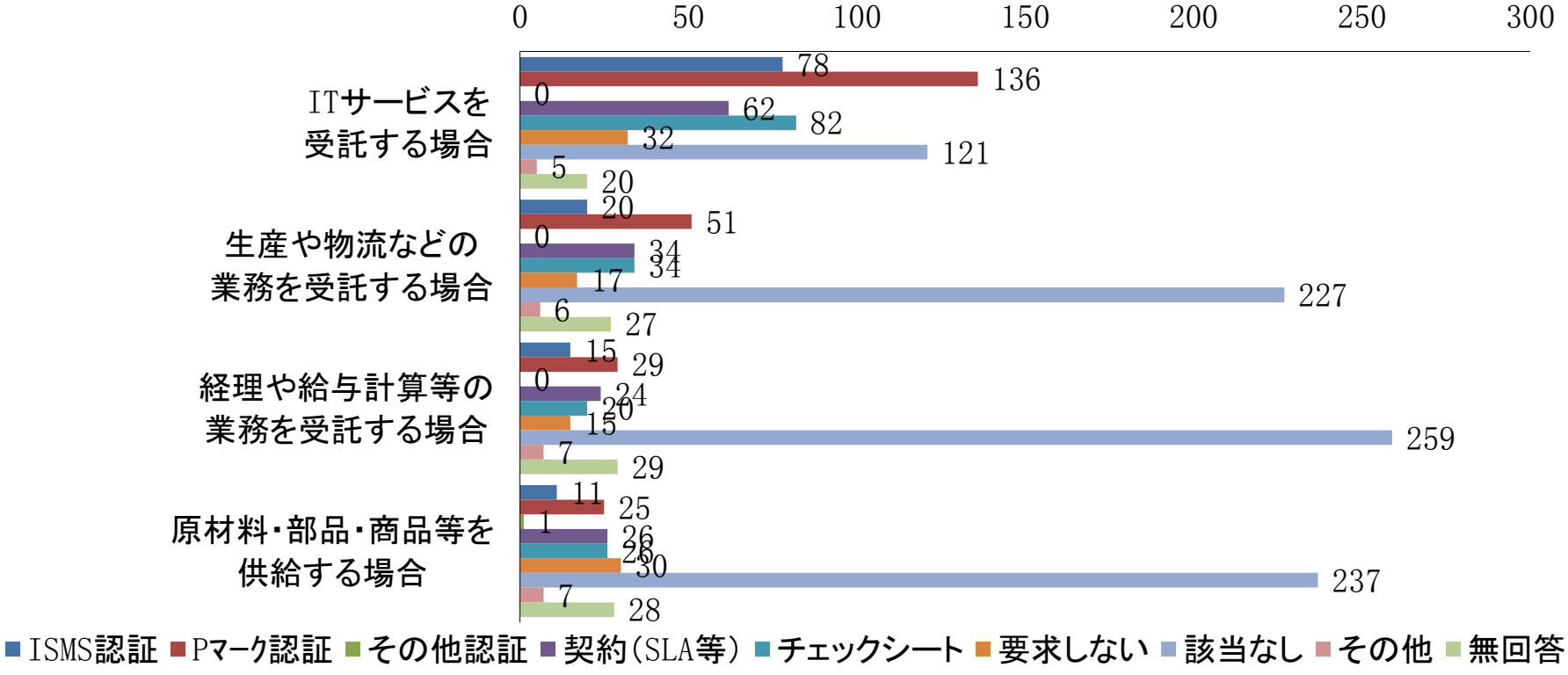


孫請け禁止や全て管理という場合が多いが、生産・物流や
原材料・部品・商品の調達では一次委託先に管理を任せていることも多い。

第4章　情報セキュリティのガバナンス

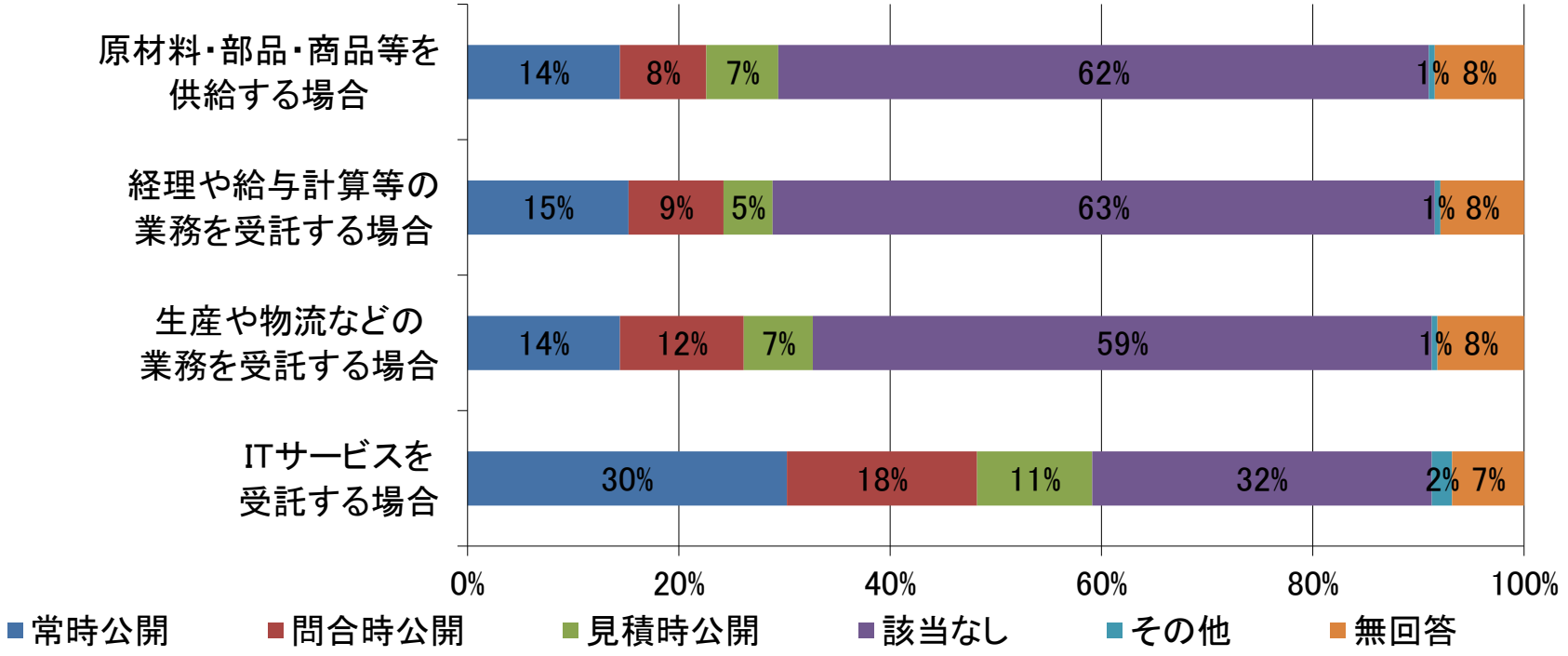
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

設問30. 受託者・供給者の立場として、顧客から情報セキュリティのリスク対応を要求されていますか。(各項目について複数選択可) (N=367)



業務を受託する場合には、Pマークが利用されることが多いが、契約やチェックシートも使われる。

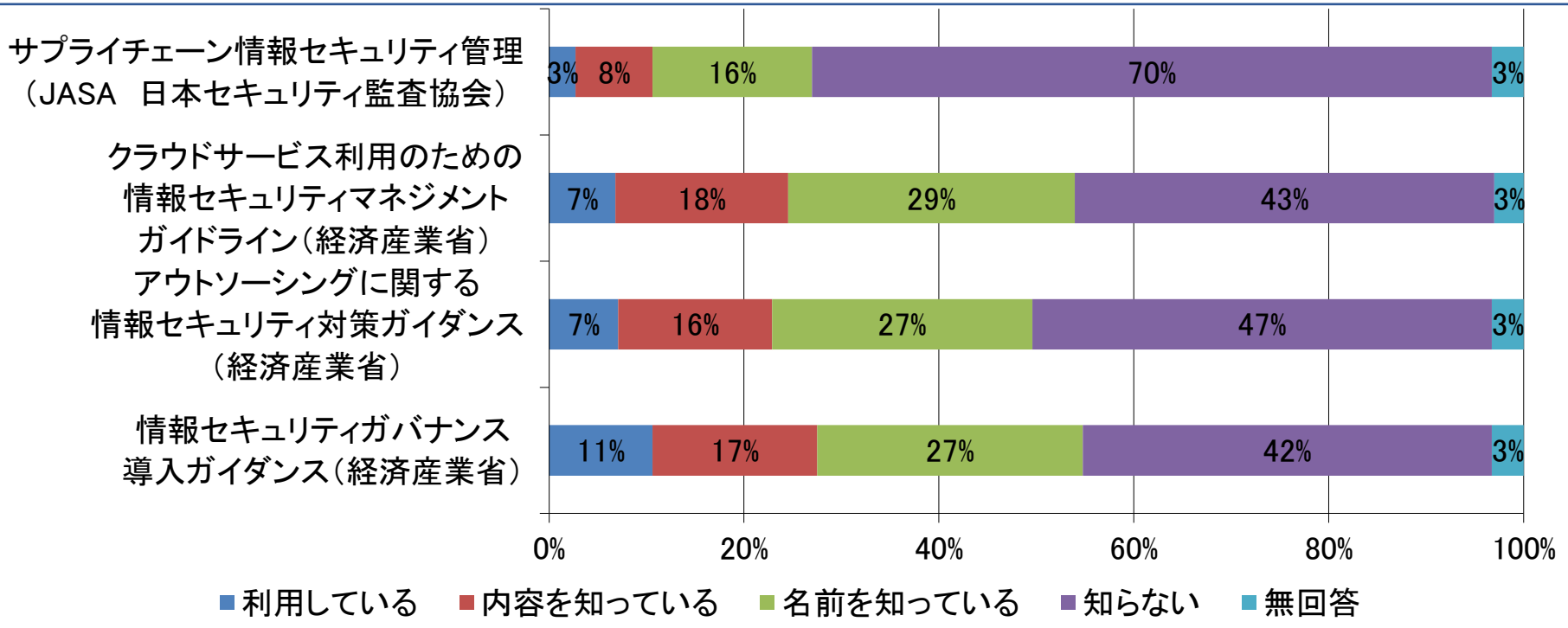
設問31. 受託者・供給者の立場として、顧客に対して調達方針や情報セキュリティ方針において情報セキュリティ上の遵守事項の公開を望みますか。
（各項目について〇印はひとつだけ）（N=367）



ITサービスを受託する場合においては、
情報セキュリティの遵守事項の開示を要望する声が強い。

第4章　情報セキュリティのガバナンス

設問32. 外部との委託先・調達先に対する情報セキュリティガバナンスに関する下記のガイドライン、ツールについてご存知ですか。
（各項目について○印はひとつだけ）（N=367）



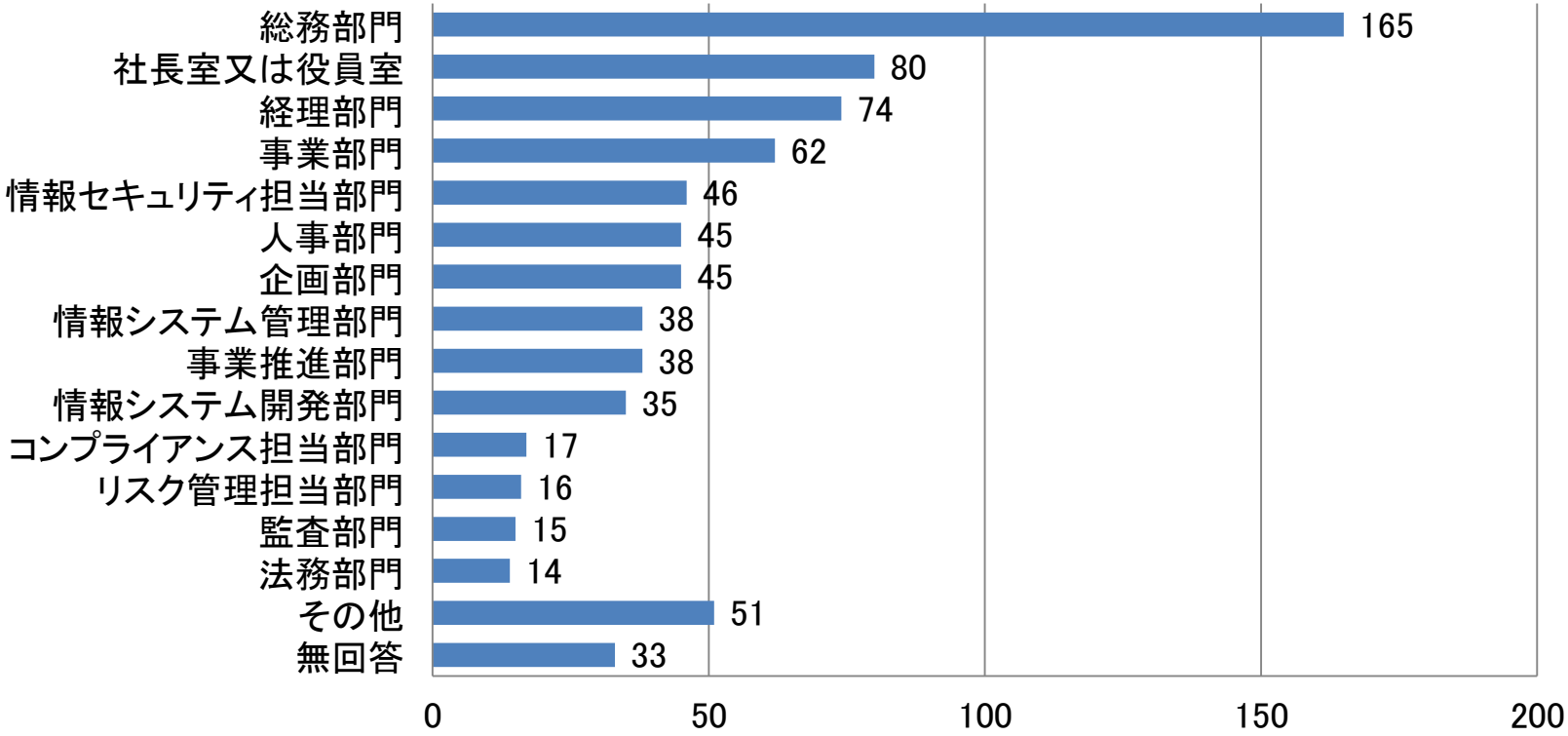
外部委託における情報セキュリティのガイドライン・ツールについて、周知は十分でなく、実際に活用されている例は少ない。

考察（第4章　情報セキュリティのガバナンス）

- 業務の外部委託・受託においては機密性が重視される中で、Pマークの利用が多く、また、自組織の要求事項が反映される契約やチェックシートが使われることも多い。国際的な相互認証の可能なISMSの利用は少なく、コスト面の理由が大きいと考えられる。

第5章
営業秘密の管理

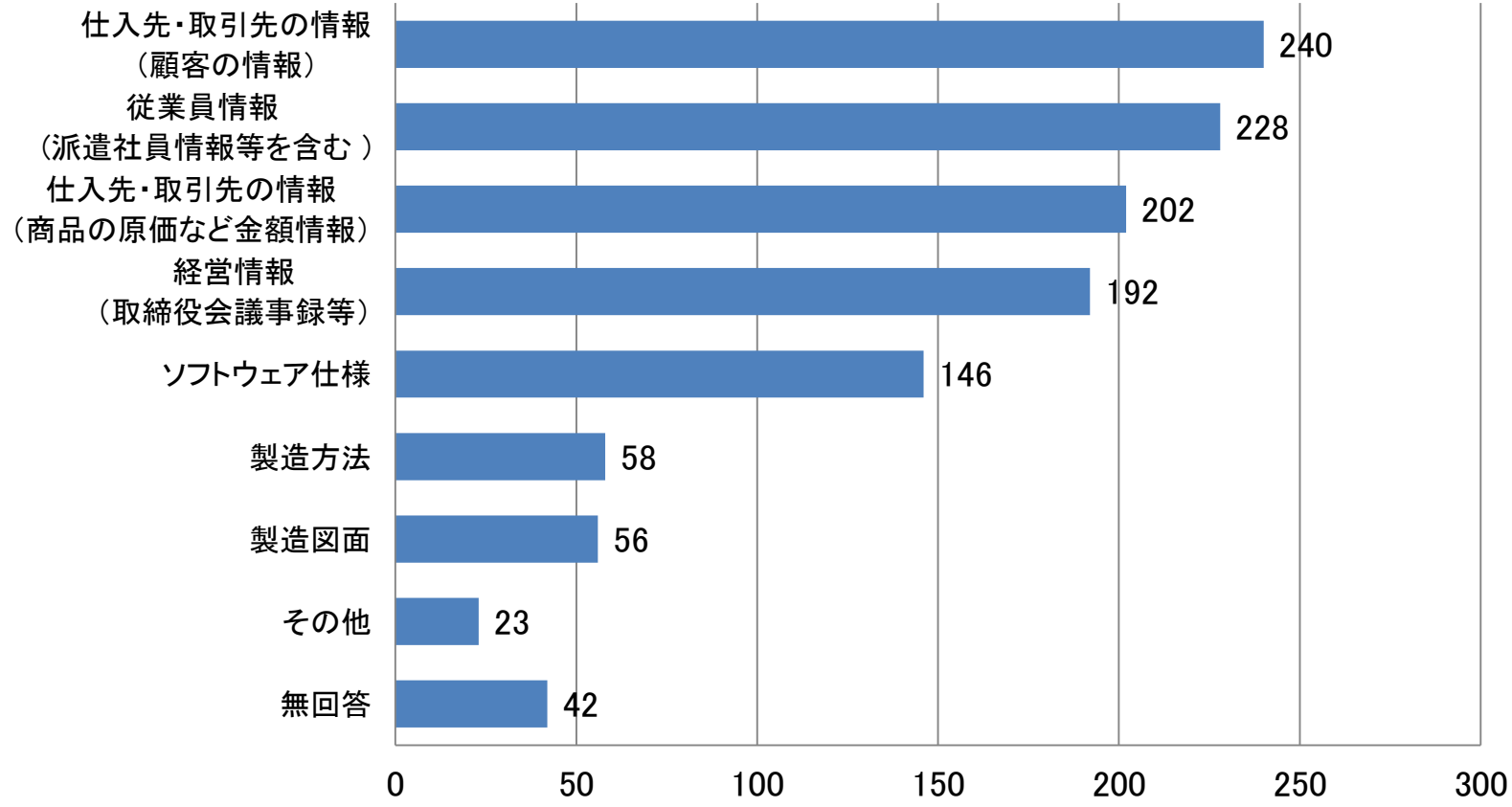
設問33. 営業秘密の管理している部門をお答えください。(N=367)



総務部門が165件であり、最も多い。

第5章　営業秘密の管理

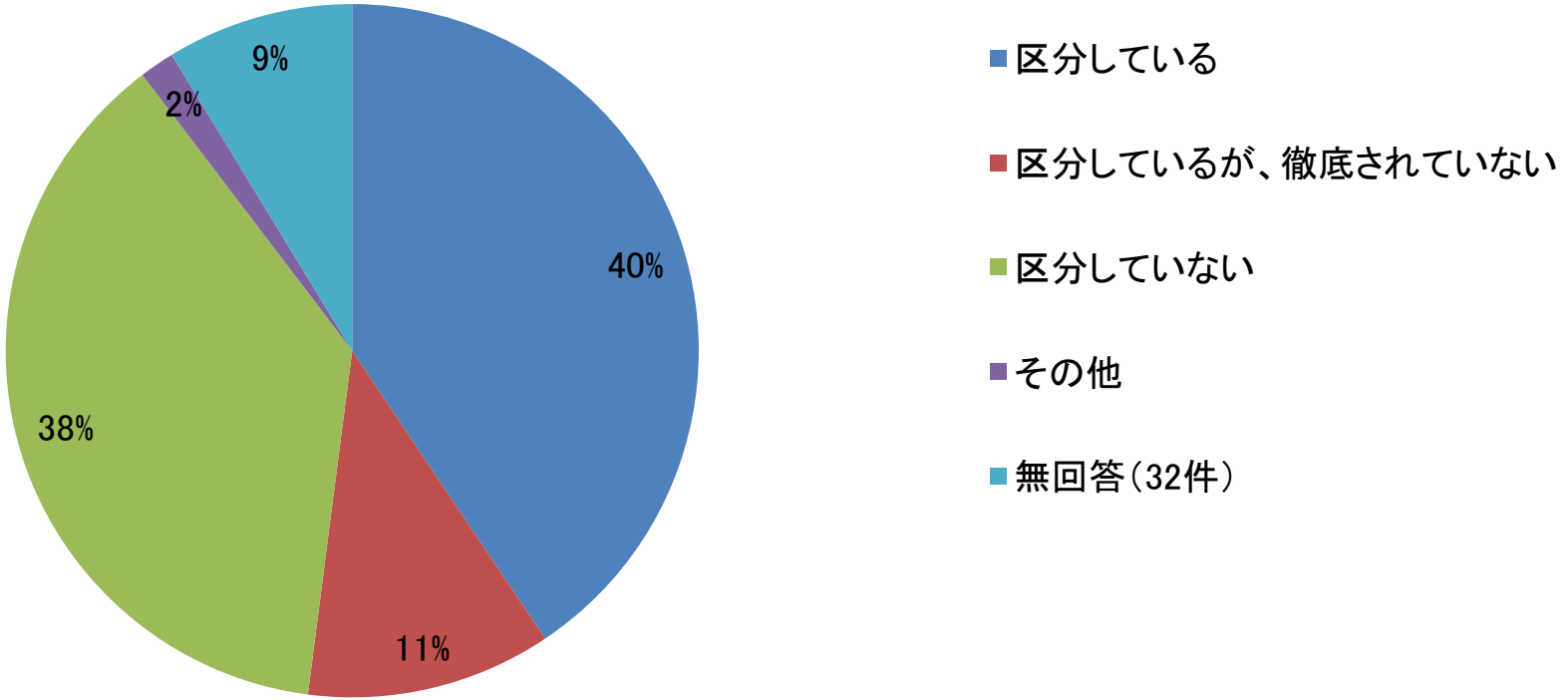
設問34. 以下にあげる情報を営業秘密として扱っていますか。(複数選択可)(N=367)



顧客情報、従業員情報、経営情報の回答が多い。

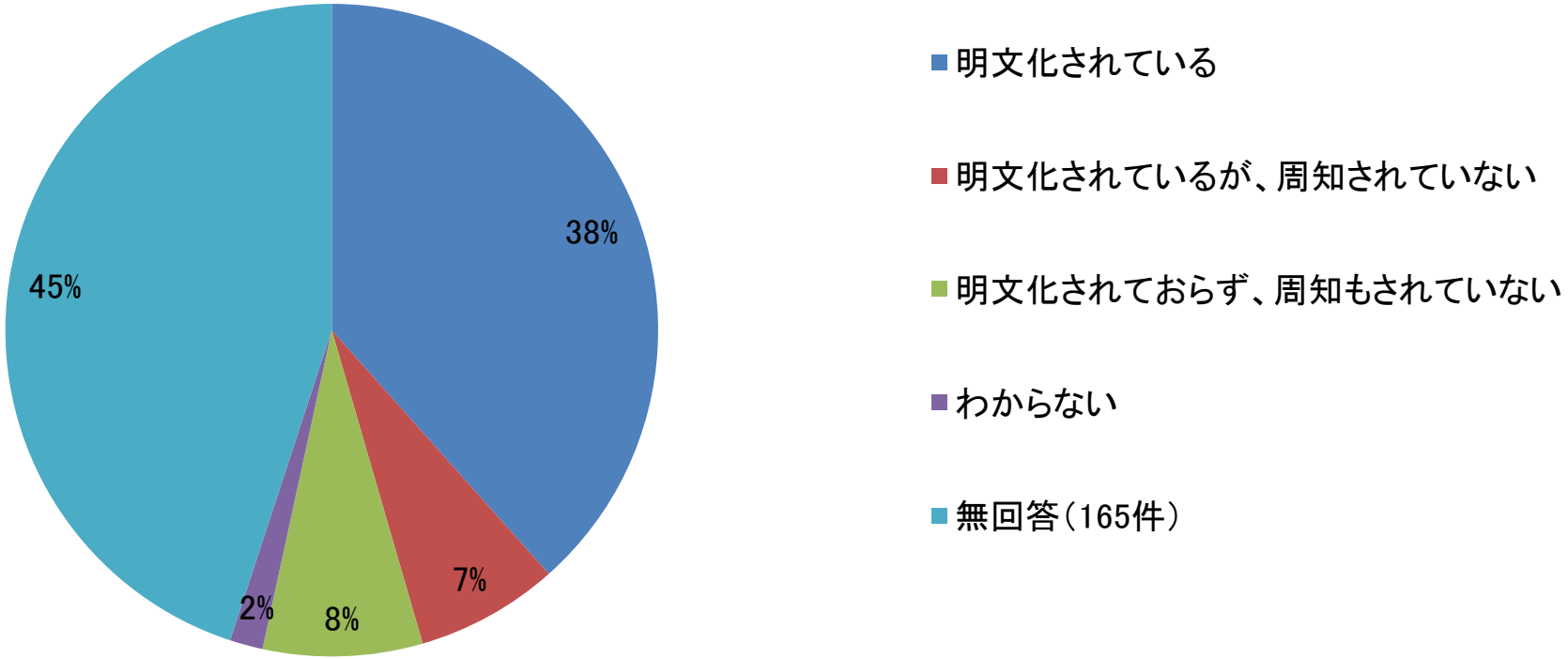
第5章　営業秘密の管理

設問35. 営業秘密を秘密度に応じて区分(極秘、秘、社外秘等)していますか。
(N=367)



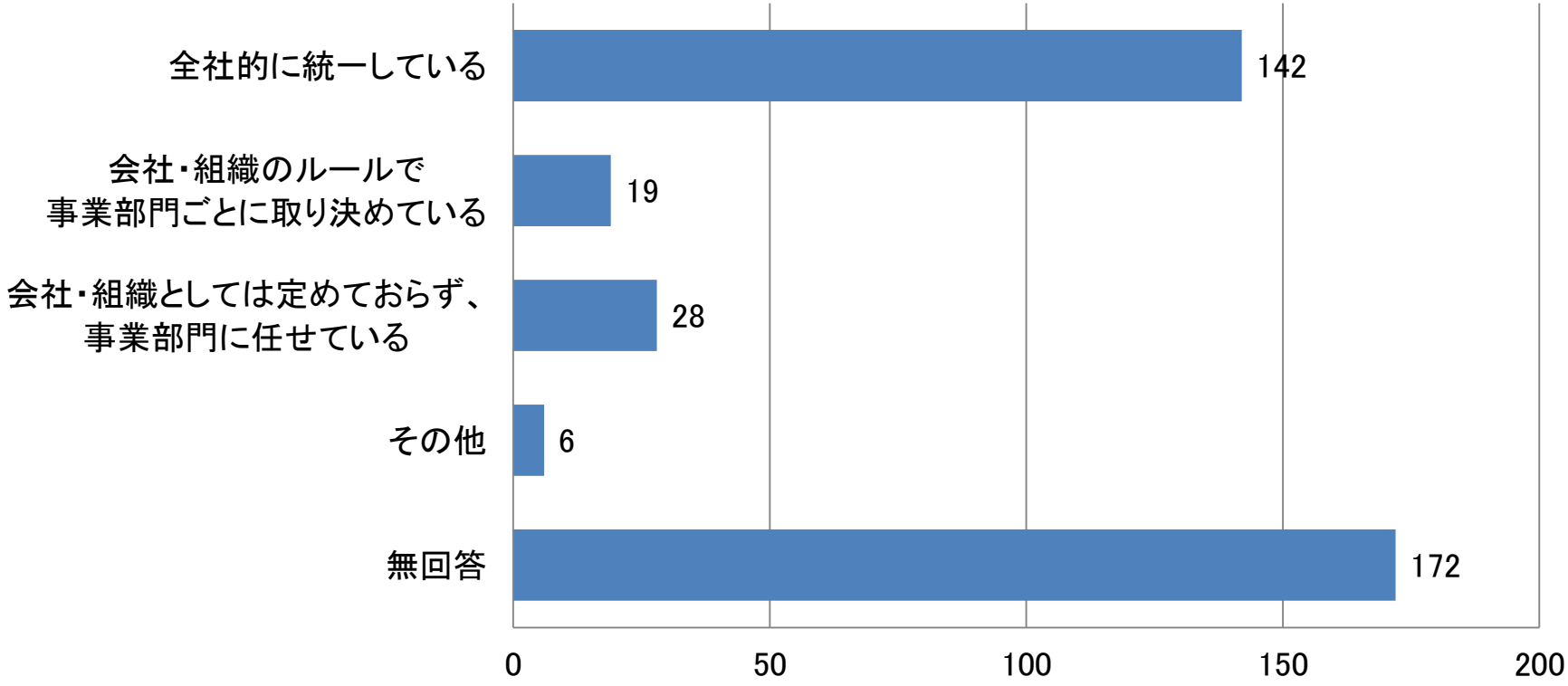
区分している企業が51%、区分していない企業が38%である。

設問36. 営業秘密を秘密度に応じて区分するための基準について明文化されていますか。(N=367)



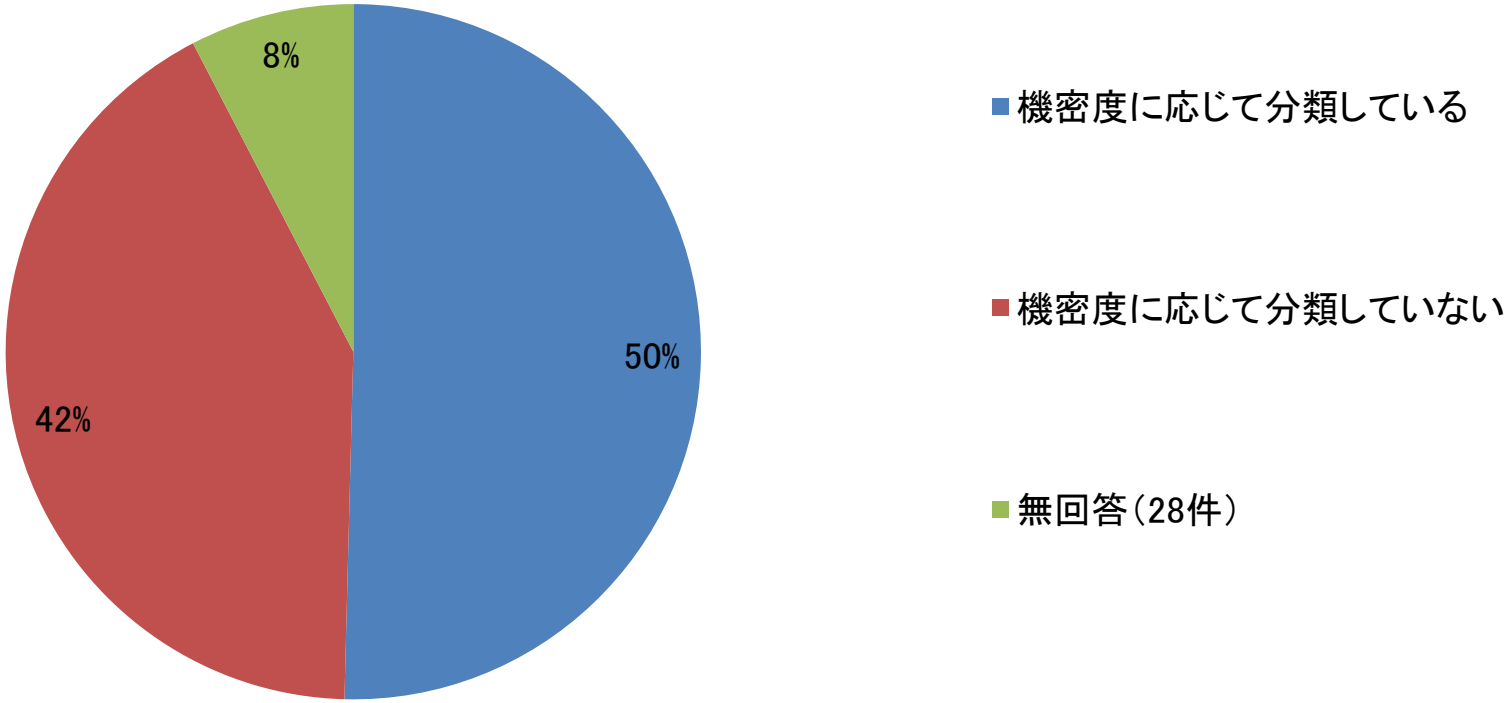
明文化している企業が45%である。

設問37. 秘密度に応じて区分した営業秘密の適応範囲を教えてください。(N=367)



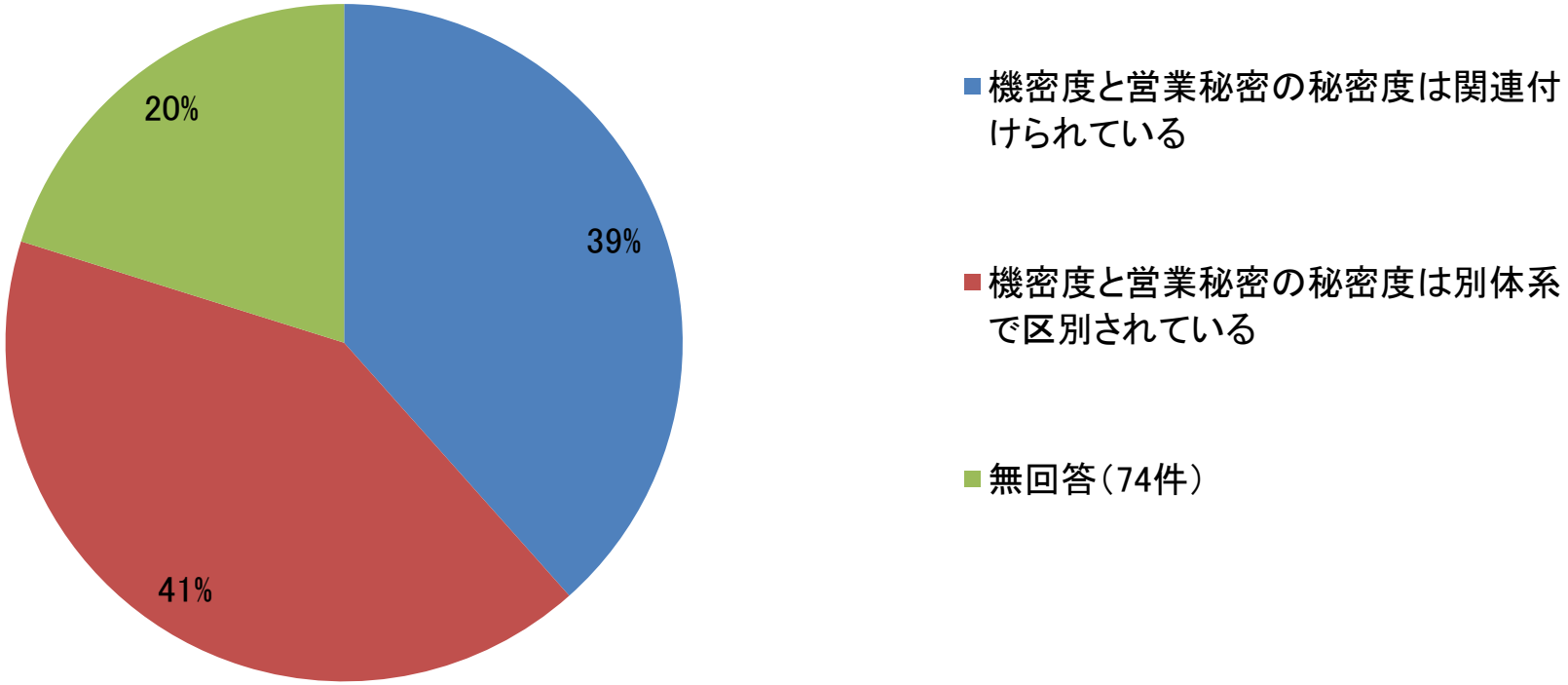
全社的に統一している組織が多い。

設問38. 情報資産を機密度に応じて分類していますか。(N=367)



分類している企業は50%、分類していない企業が42%である。

設問39. 情報資産の機密度と営業秘密の秘密度は関連付けられていますか、それとも区別されていますか。(N=367)

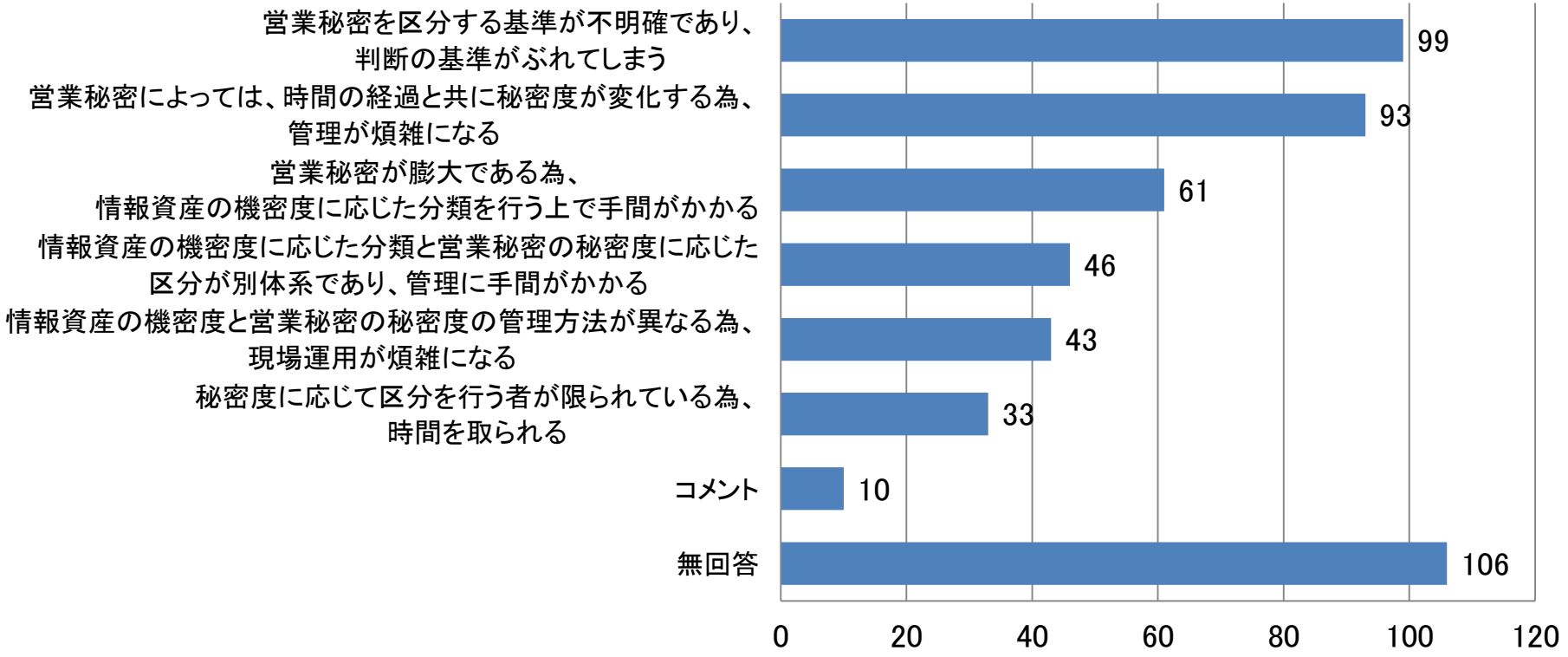


39%の組織で、機密度と営業秘密の秘密度が関連付けられている。

第5章　営業秘密の管理

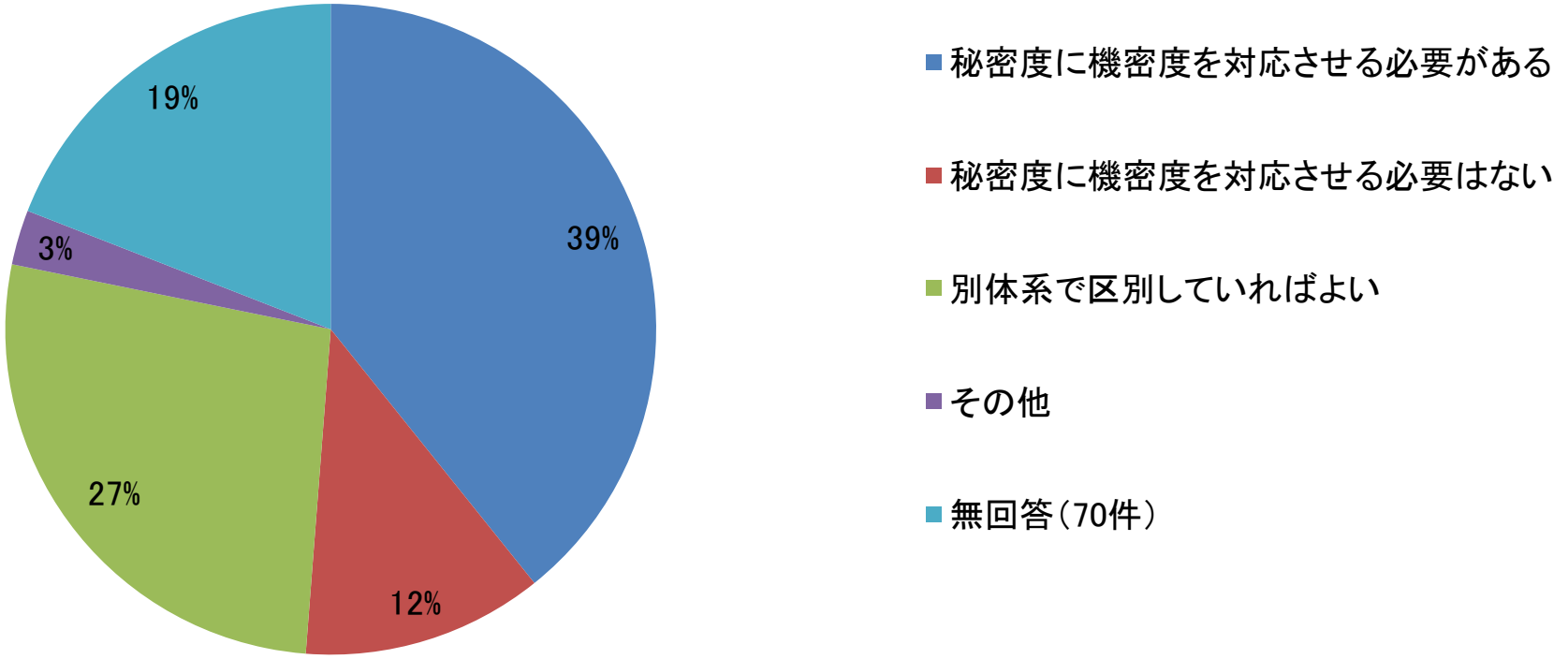
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

設問40. 営業秘密の管理について、以下の中からお困りの点を選択してください。
また、その他にお困りの点がありましたらコメント欄にご記入ください。
（複数選択可）（N=367）



管理が煩雑になることや、判断の基準がぶれてしまうことについての回答が多い。

設問41. 情報資産の機密度と営業秘密の秘密度との対応関係について、どのような考えをお持ちですか。(N=367)



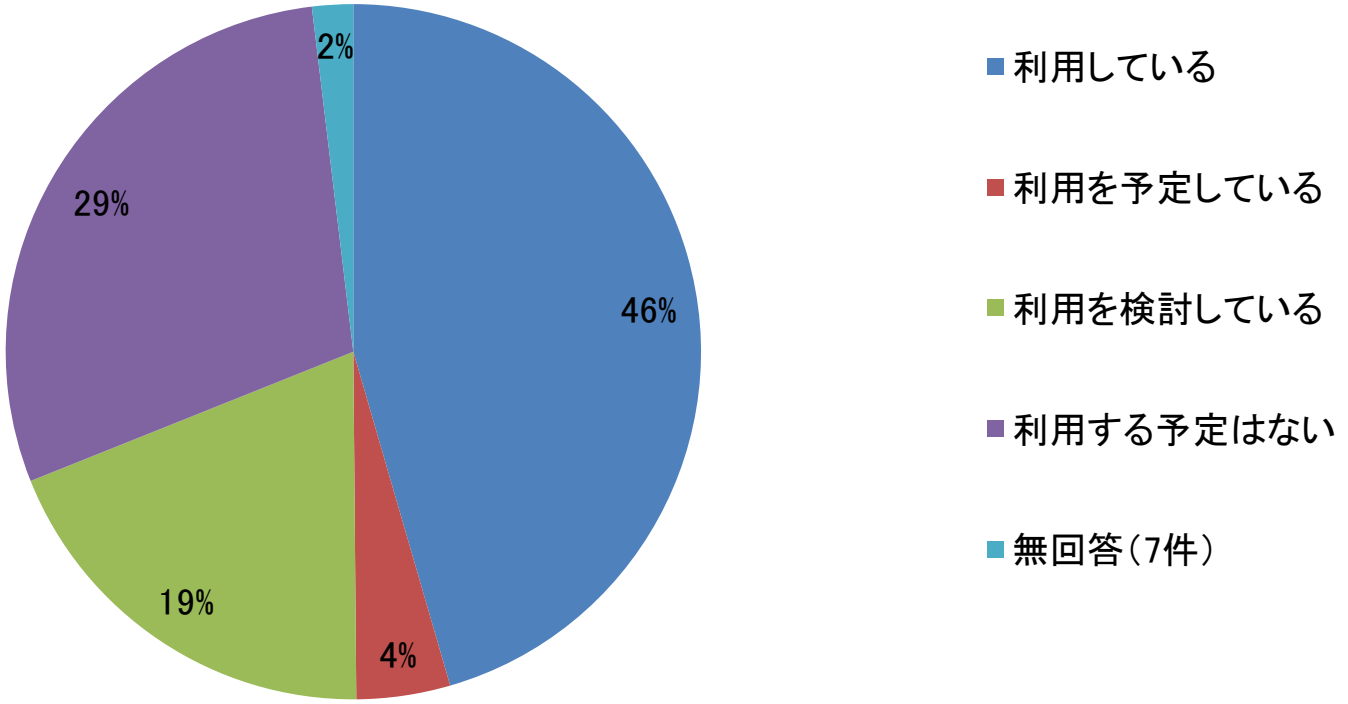
対応させる必要があると答えた企業が39%であり、最も多い。

考察（第5章　営業秘密の管理）

- 営業秘密としているのは、顧客情報、従業員情報、経営情報が多い。
- 本章は、他の章に比べ無回答が多い。

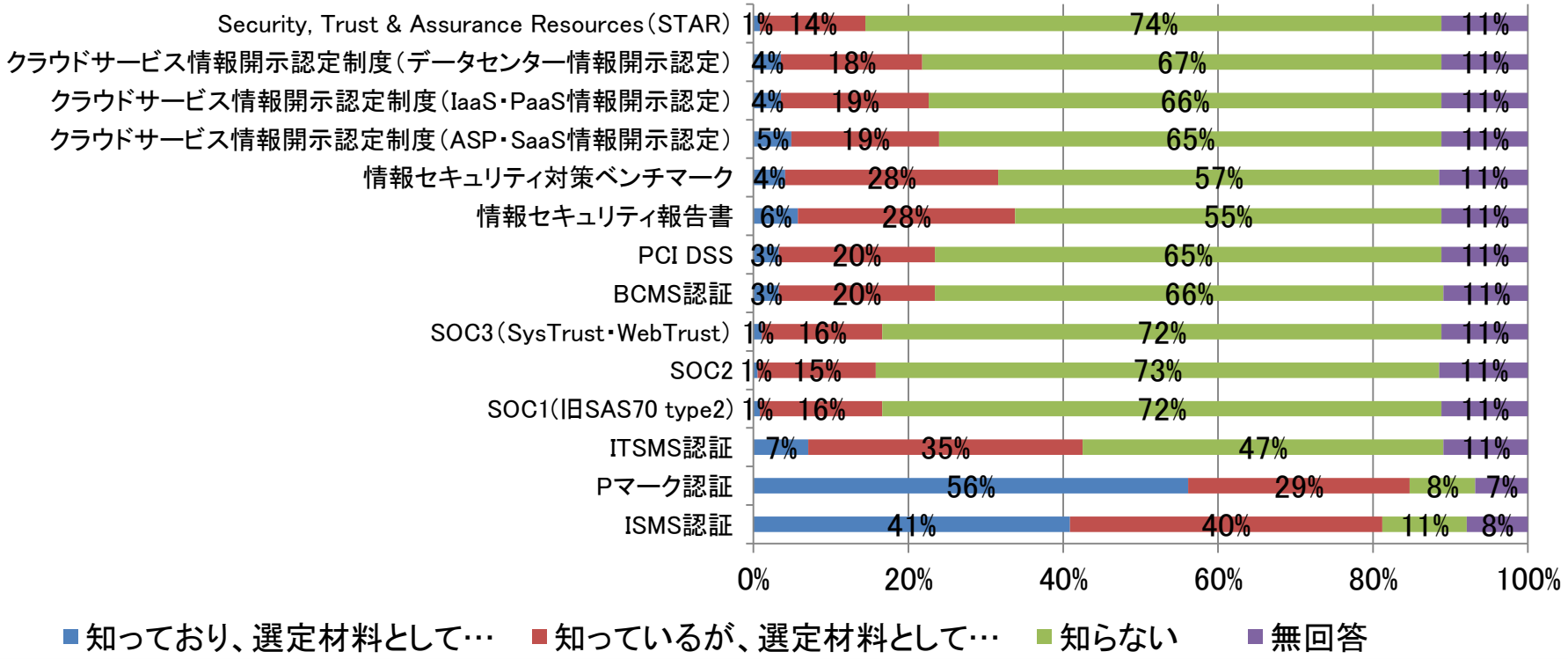
第６章
クラウド・コンピューティング（クラウド）

設問42. 貴社では、クラウドを利用していますか。（N=367）



クラウドを利用する組織は増加傾向にある。（昨年34%から本年46%）

設問43. 以下の情報セキュリティの第三者認証制度または情報公開制度を知っていますか。知っている場合、クラウドサービスの選定材料として利用または利用を予定していますか。（N=367）



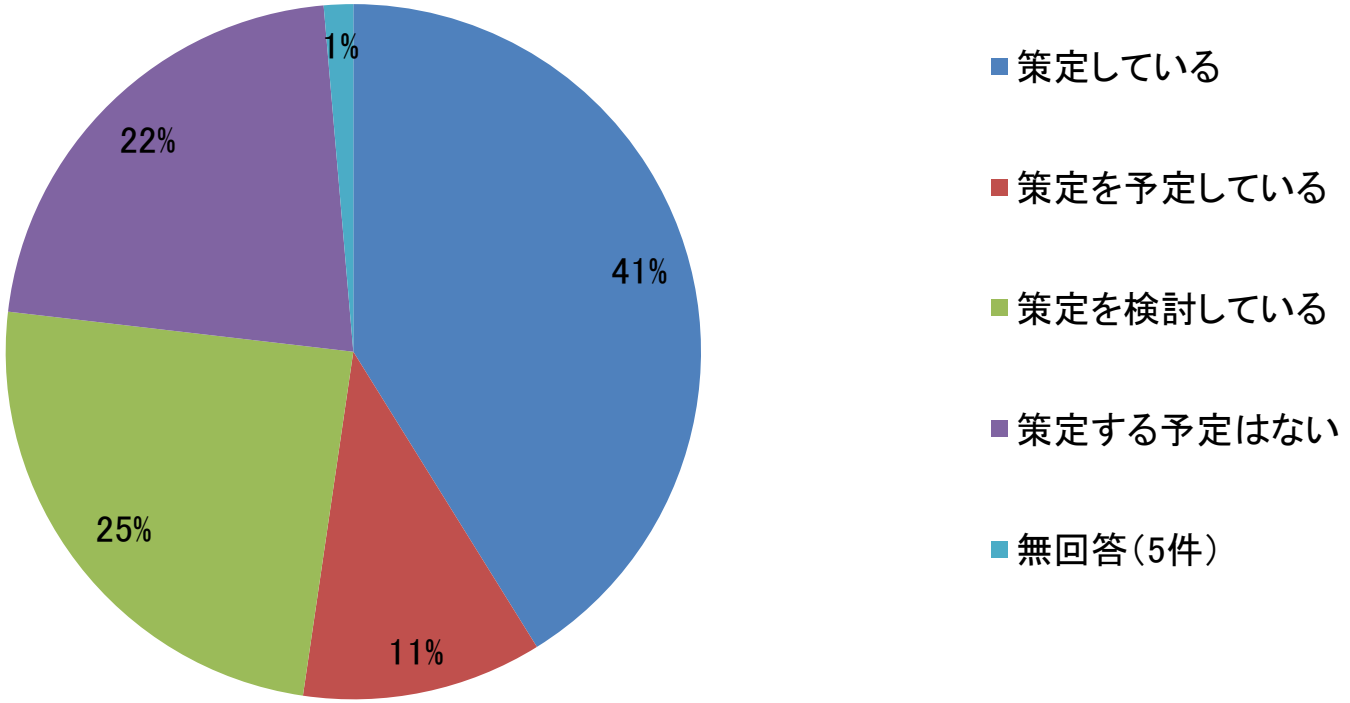
ISMS認証・Pマーク認証以外の制度の認知度は低く、利用されていない。

考察（第６章　クラウド・コンピューティング（クラウド））

- クラウドを利用する組織は増加傾向にある（昨年34%から本年46%）が、利用する予定がないと答えた組織も微増（昨年25%から本年29%）している。
- ISMS認証・Pマーク認証・ITSMS認証以外の制度の認知度は高くなく（40%以下）、選定材料としての利用度はさらに低い（10%未満）。

第7章
事業継続計画

設問44. 貴社では事業継続計画(BCP)を策定していますか。(N=367)

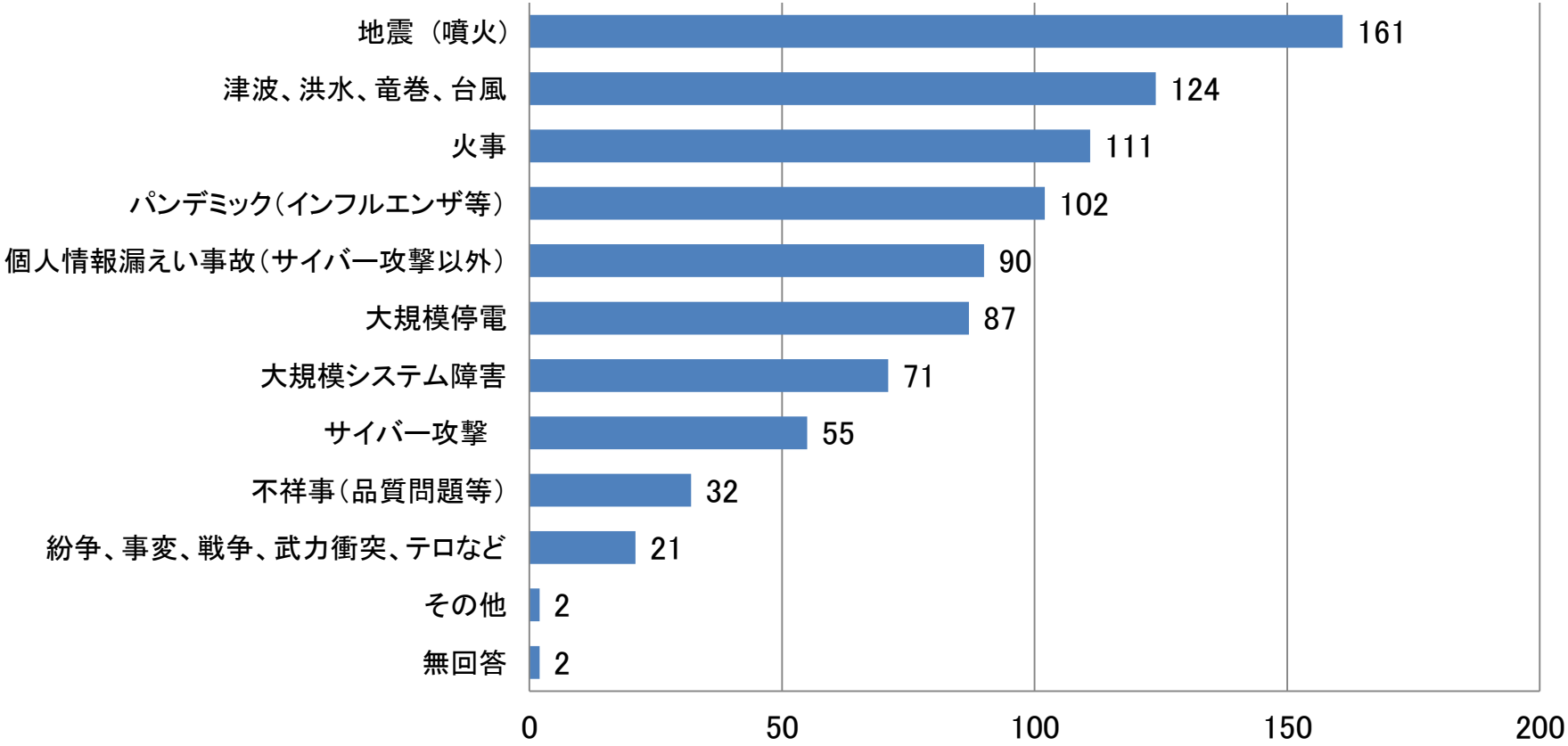


策定している組織が41%であった。策定予定をしている組織を含めると半数を超えた。一方、策定予定がない組織も22%あった。

第7章　事業継続計画

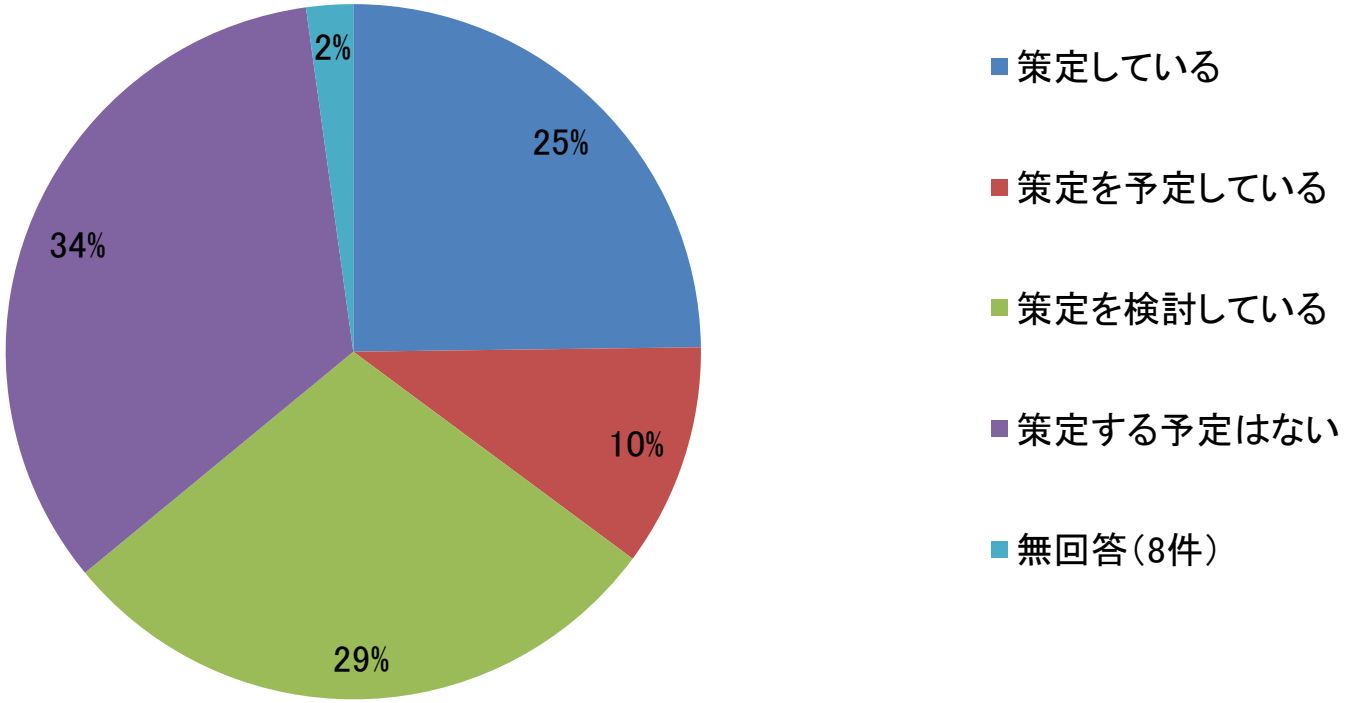
※設問44.で「策定している」又は「策定を予定している」と回答した組織のみ

設問45. 想定する脅威は何ですか。（複数選択可）（N=192）



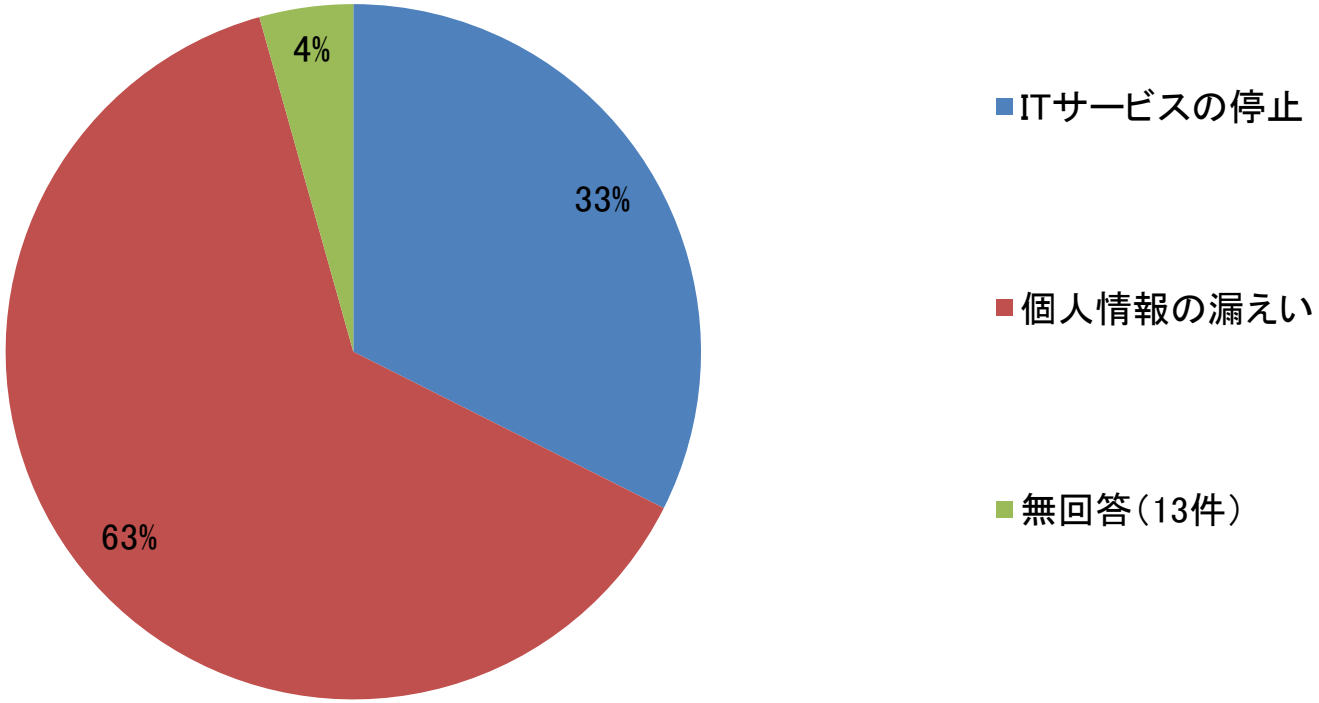
自然災害（地震、津波、火事等）に係る脅威が上位を占めた。
また、情報漏えい事故では、個人情報漏えい事故を脅威とする組織が多かった。

設問46. 貴社ではITサービス継続に係る事業継続計画(IT-BCP)を策定していますか。(N=367)



ITサービス継続に係る事業継続計画を策定している組織が25%であった。
一方、策定予定がない組織も34%あった。

設問47. 貴社において事業インパクトが大きいのはどちらですか。(N=367)



ITサービスの停止を選択した組織は33%であり、
個人情報の漏えいを選択した組織は63%であった。

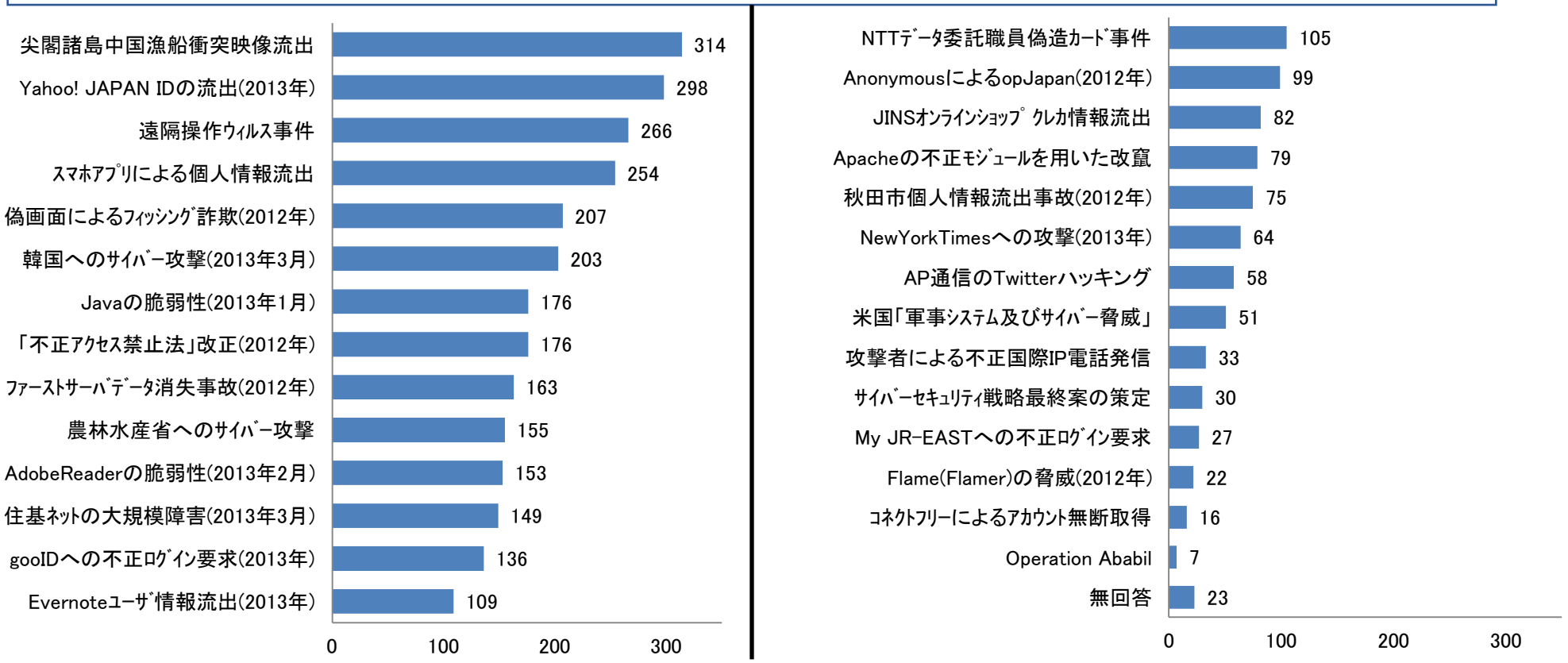
考察（第7章　事業継続計画）

- 事業継続計画の策定状況は41%であった。
- ITサービスの停止と比べ、個人情報の漏えいの方が
  事業インパクトが大きいとの認識する組織が約2倍であった。

第8章
その他

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

設問48. 次の出来事について、ご存知なものをご選択ください。（複数選択可）（N=367）



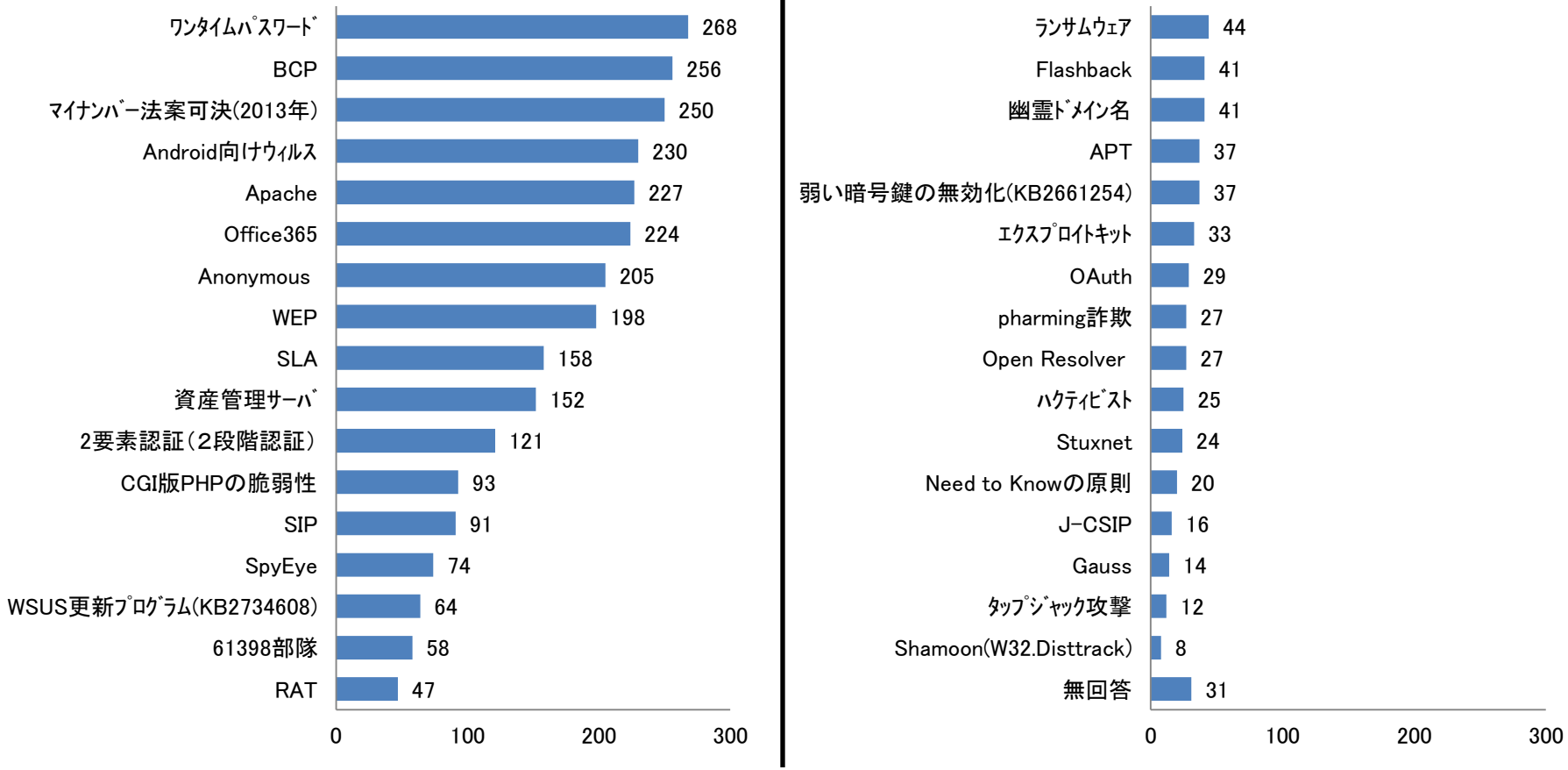
マスメディアで取り上げられた事件・事故、用語への認知度が高く、専門的なものについては認知度が高くない。

「米国「軍事ｼｽﾃﾑ及びｻｲﾊﾞｰ脅威」」は、アンケート調査において
「米国報告書「弾力的軍事ｼｽﾃﾑ及び先進的ｻｲﾊﾞｰ脅威」の発表(2013年3月)」と記載している。

第8章　その他

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

設問49. 次の用語ついて、ご存知なものをご選択ください。（複数選択可）（N=367）



BCPやマイナンバー法案などの時事的なものへの認知度が高い。

考察（第8章　その他）

- 過去3年間と同様に、マスメディアで取り上げられた事件・事故、用語への認知度が高く、専門的なものについては認知度が高くない。（Yahoo事件、遠隔操作ウィルス、スマホアプリによる個人情報漏えい、偽画面によるフィッシングなどはマスメディアで広く取り上げられた。）
- 機密性に関する出来事が多い中、可用性の観点では、2012年のファーストサーバ事件や住基ネットの事件が認知されている。
- 用語では、上位8位までと、それ以下との認知度の差が大きい。BCPやマイナンバー法案などの時事的なものへの関心が高い。昨年・一昨年と比較すると、BCPの認知度が上がっている、一方APT、Anonymous の認知度が下がっている。

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
  - 神奈川県立鶴見養護学校
  - 神奈川県立保土ケ谷養護学校
  - 川崎市立田島養護学校　　（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