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

2012年情報セキュリティ
アンケート調査結果

2012年12月14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
  2012年7月24日～8月20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
  スマートフォンとクラウド、標的型攻撃への対応、アクセス制御と証跡（ログ）管理、個人情報漏えい事故のお詫び金、リスク分析の実施状況など
- 調査方法
  郵送による
- 回答状況
  335件（送達確認できた4,229組織に対して7.9%）

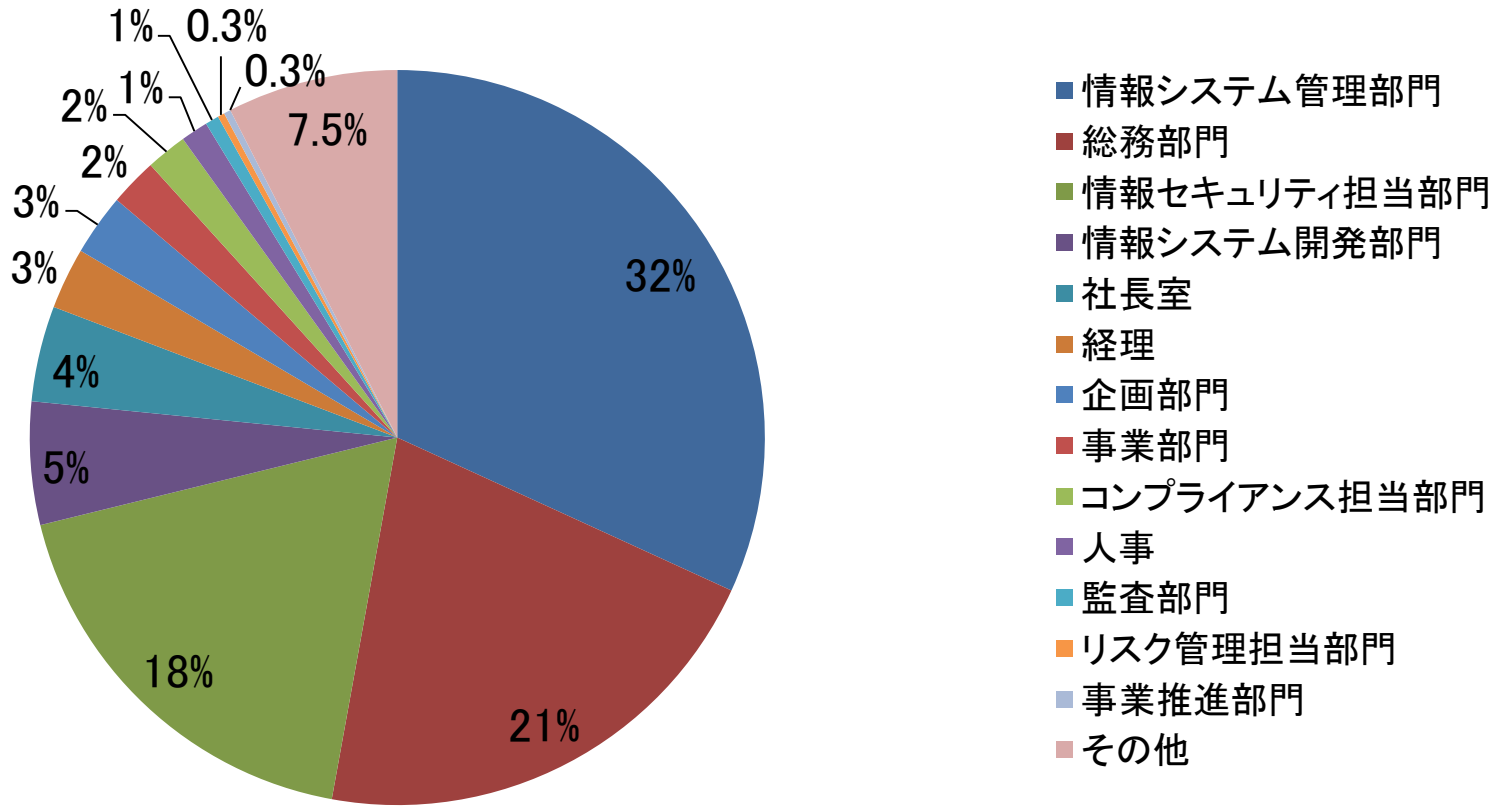
第1章

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

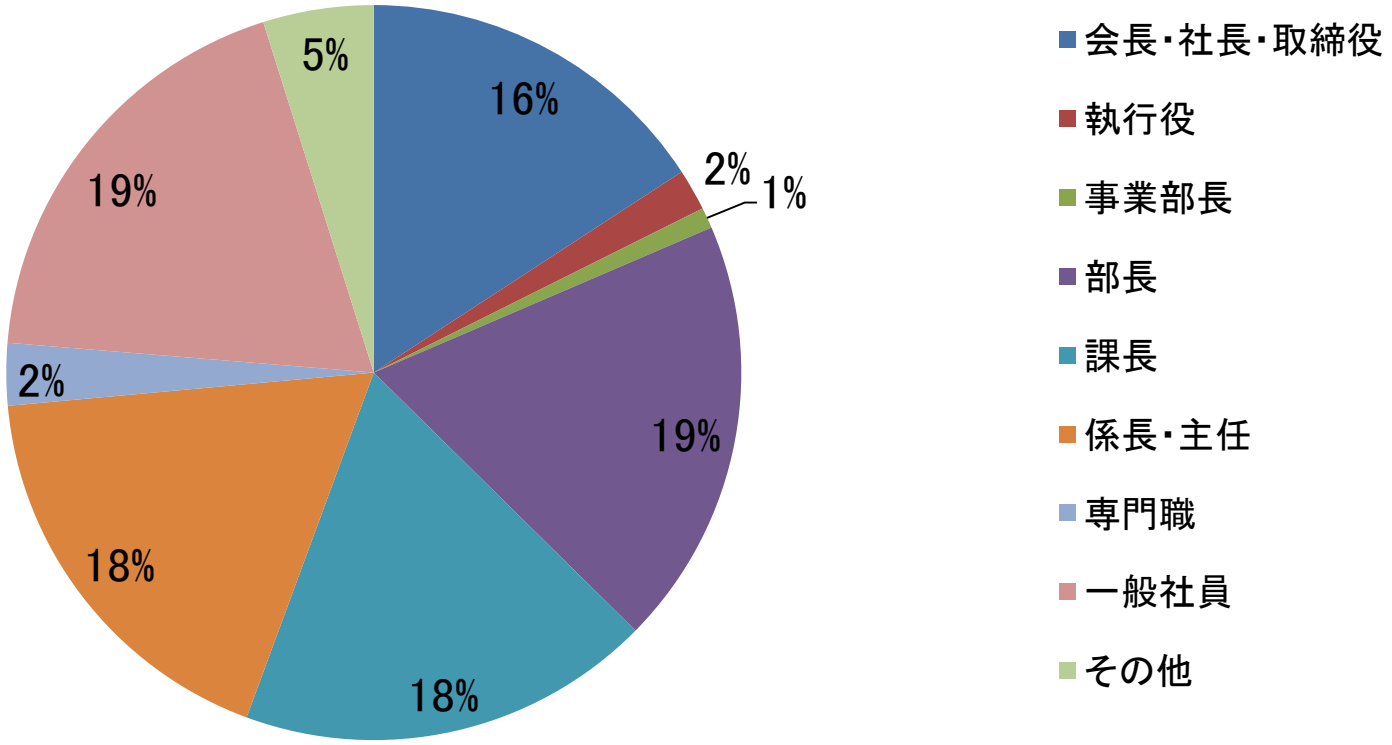
設問1.記入者の所属　（N=333）



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

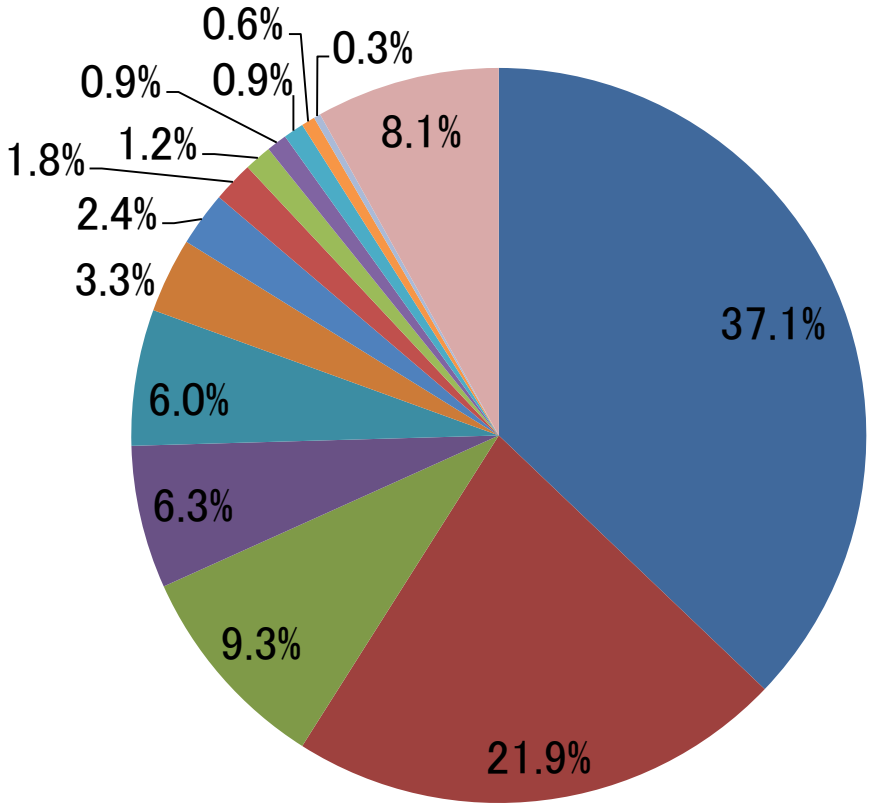
設問2.記入者の役職　（N=329）



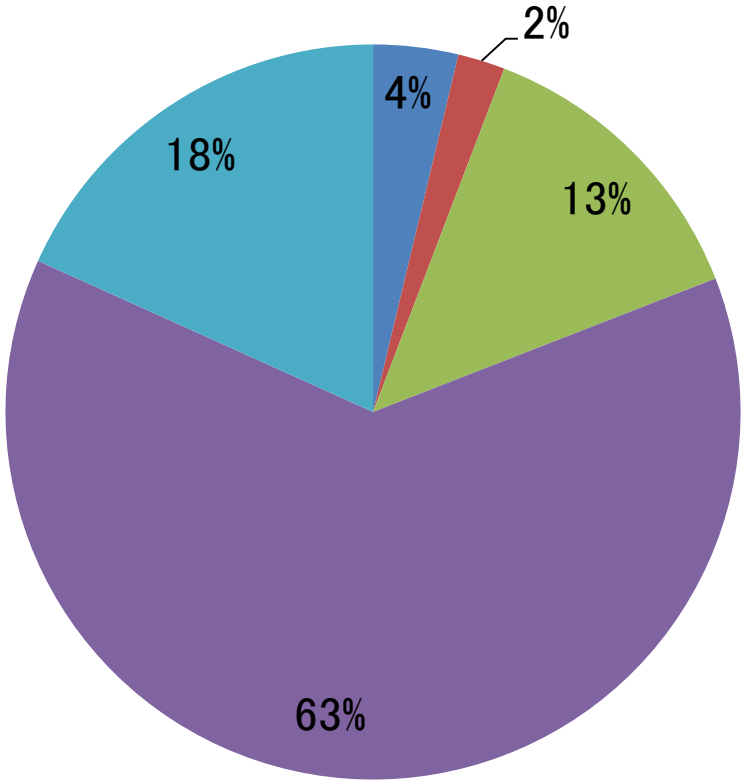
第1章　概要（回答者の基本データ等）

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=334）



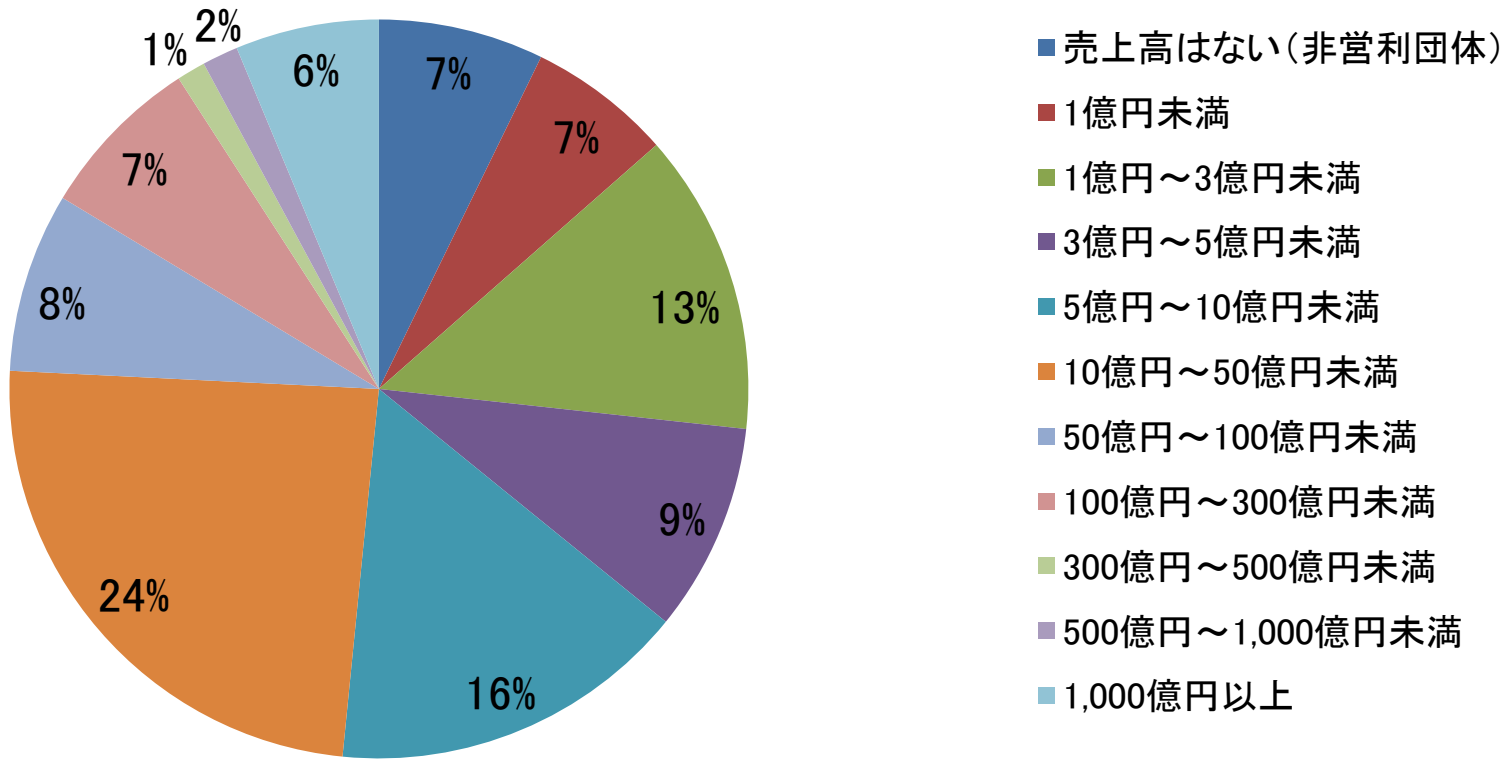
設問4.組織規模　（N=241）



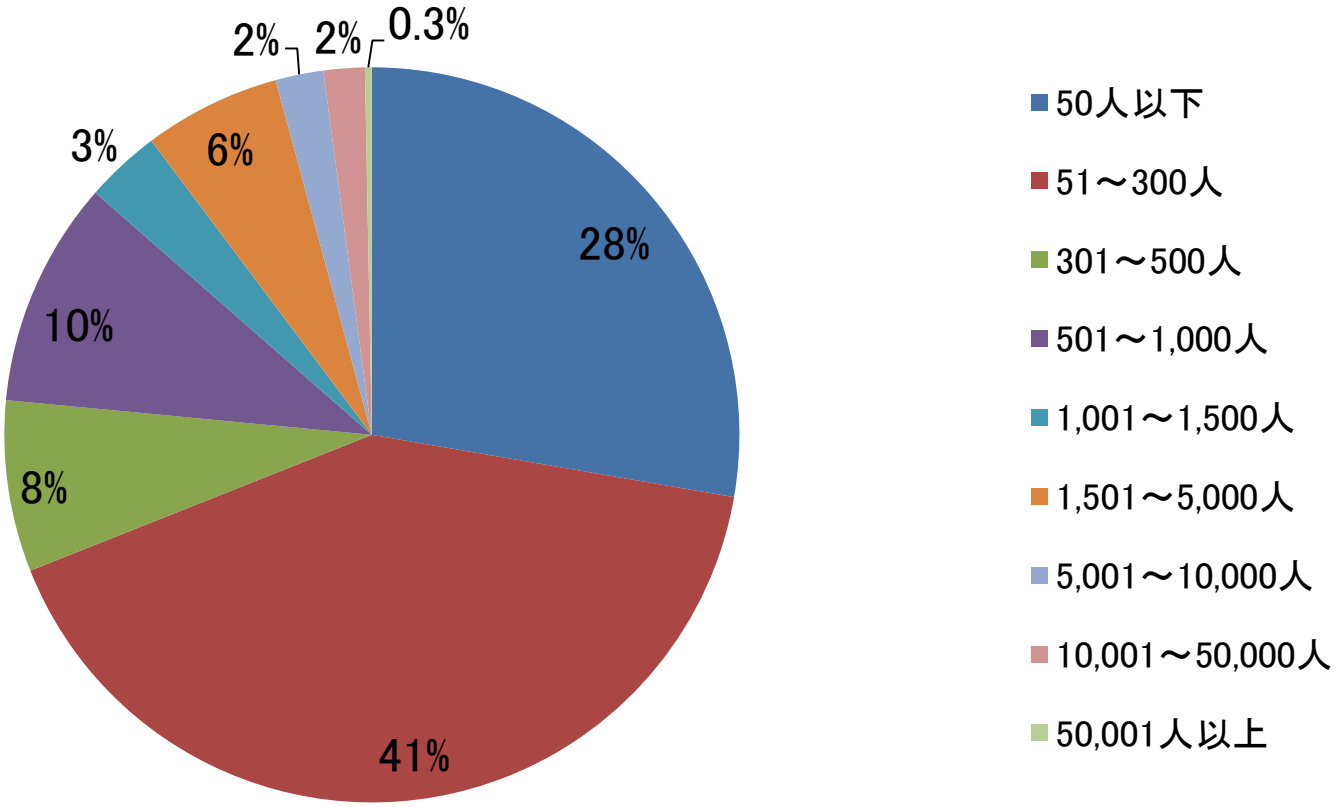
- 卸売業であり、資本金1億円以下または従業員100人以下。
- 小売業であり、資本金5千万円以下または従業員50人以下。
- 情報処理業以外のサービス業であり、資本金5千万円以下または従業員100人以下。
- 上記以外（ソフトウェア業・情報処理サービス業を含む）で、資本金3 億円以下または従業員300 人以下。
- 全てに当てはまらない。

設問5.年間売上高(単独)　(N=318)

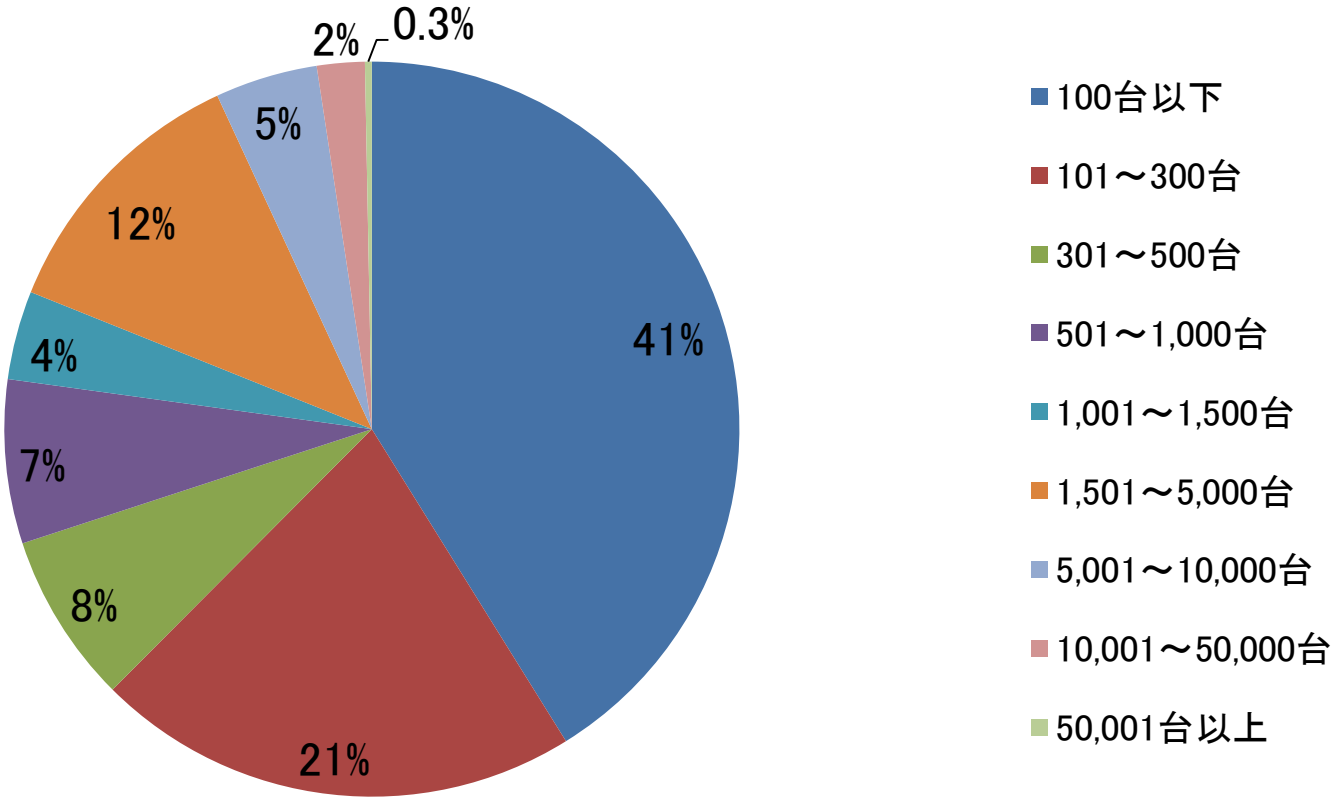
※大学・公務等は予算額、銀行は経常収益高、保険は収入保険料または正味保険料、証券は営業収入高で算出



設問6.全従業員数(単独）（N=332）



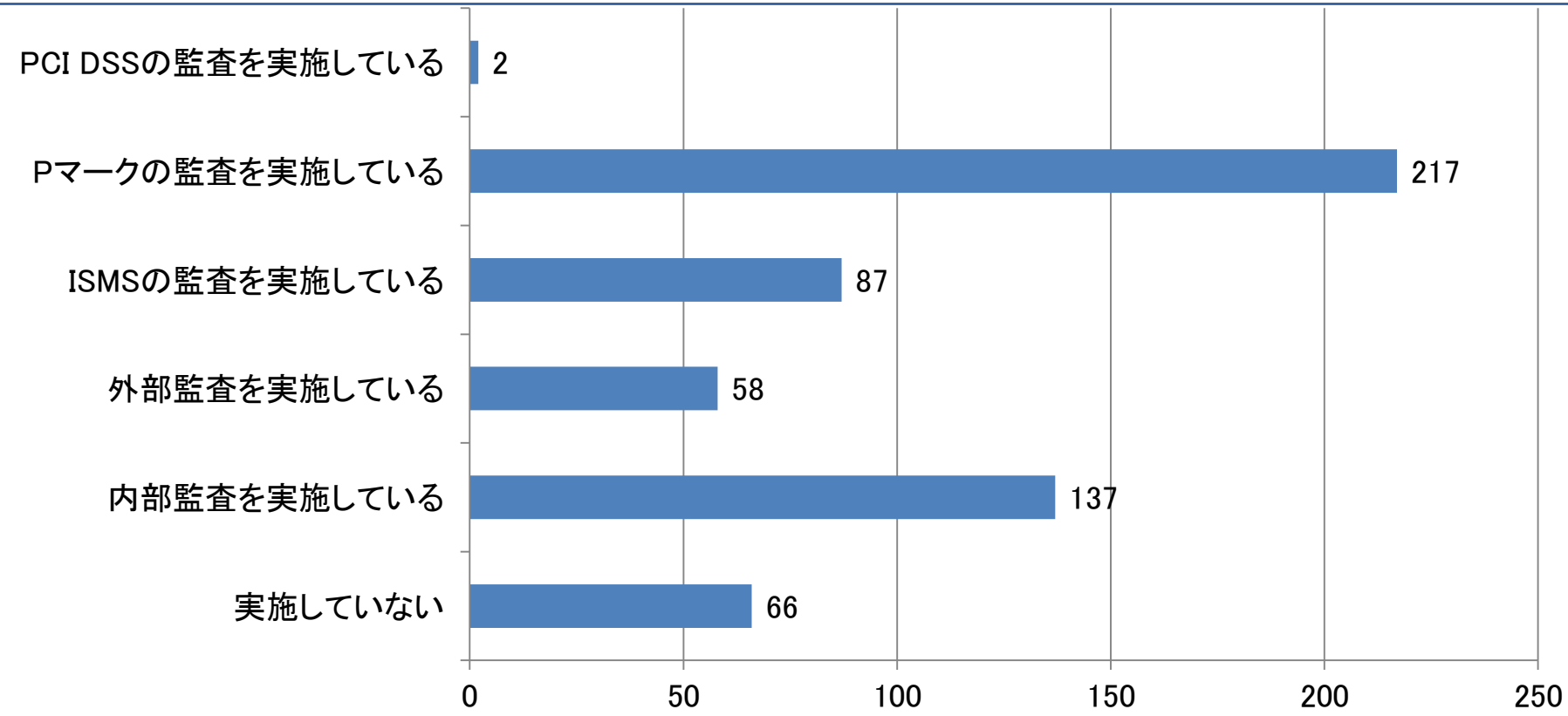
設問7.PC数(単独）（N=333）



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を実施していますか。（複数回答）（N=332）



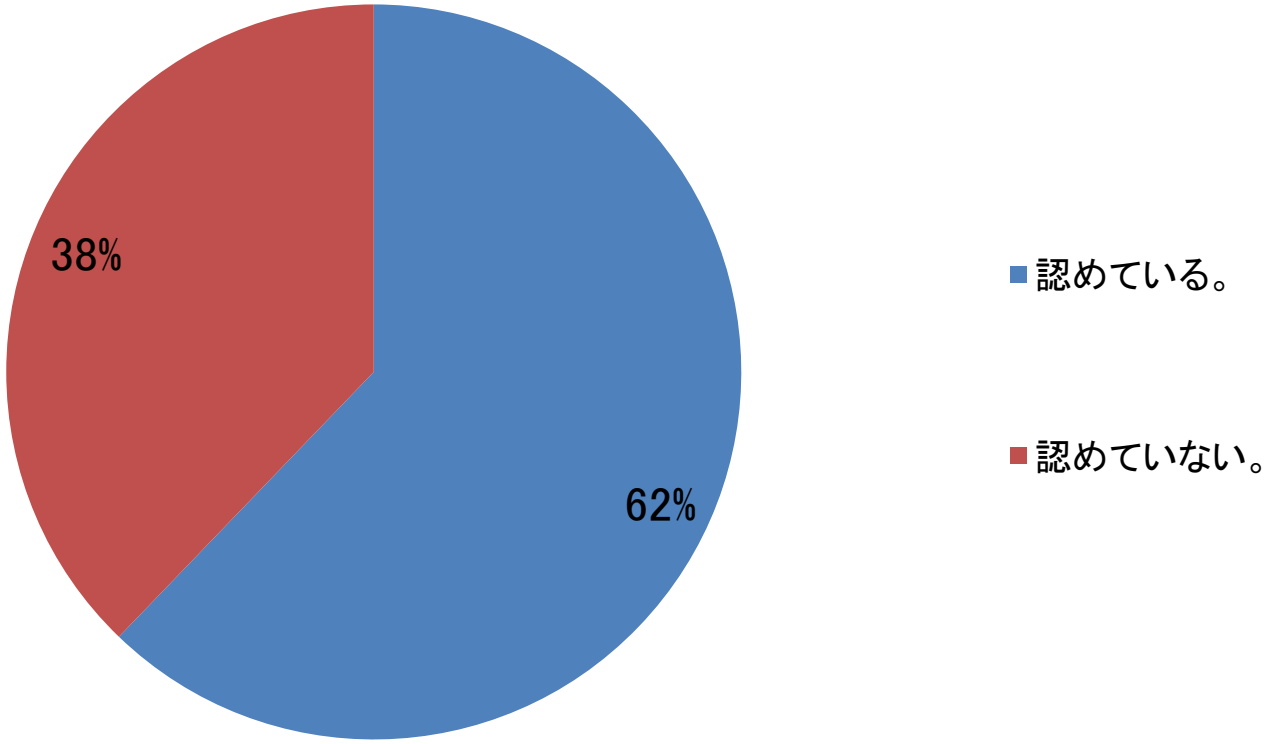
第2章

スマートデバイスの利用について

第2章　スマートデバイスの利用について

設問9.スマートデバイスの業務利用を認めていますか。(N=328)

※業務利用：業務上の情報を取り扱うケース（メールやスケジュール等も含む）



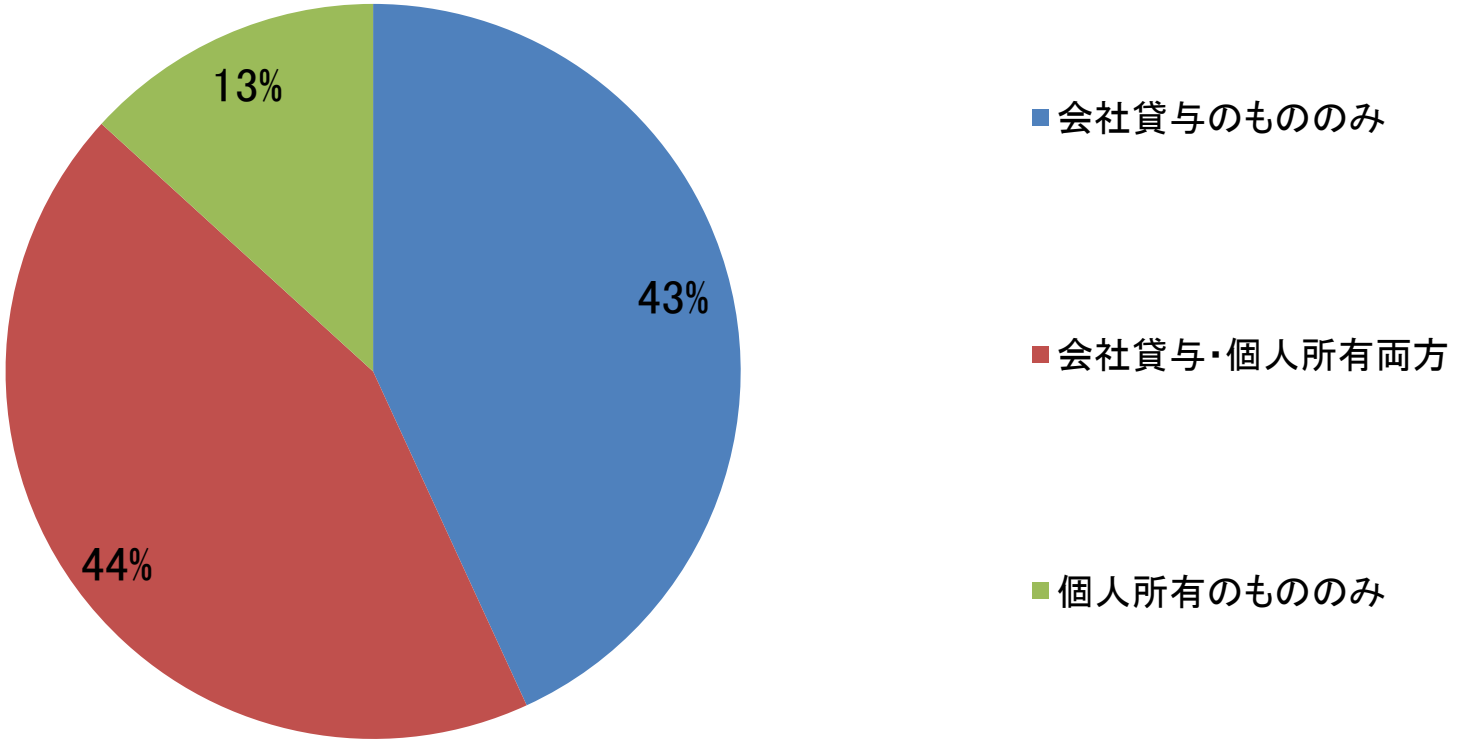
スマートデバイスの業務利用を認めている方が多い。

第2章　スマートデバイスの利用について

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

※設問9で「**認めている**」と回答した組織のみ

設問10.認めているスマートデバイスは以下のうち、どれにあてはまりますか。（N=204）

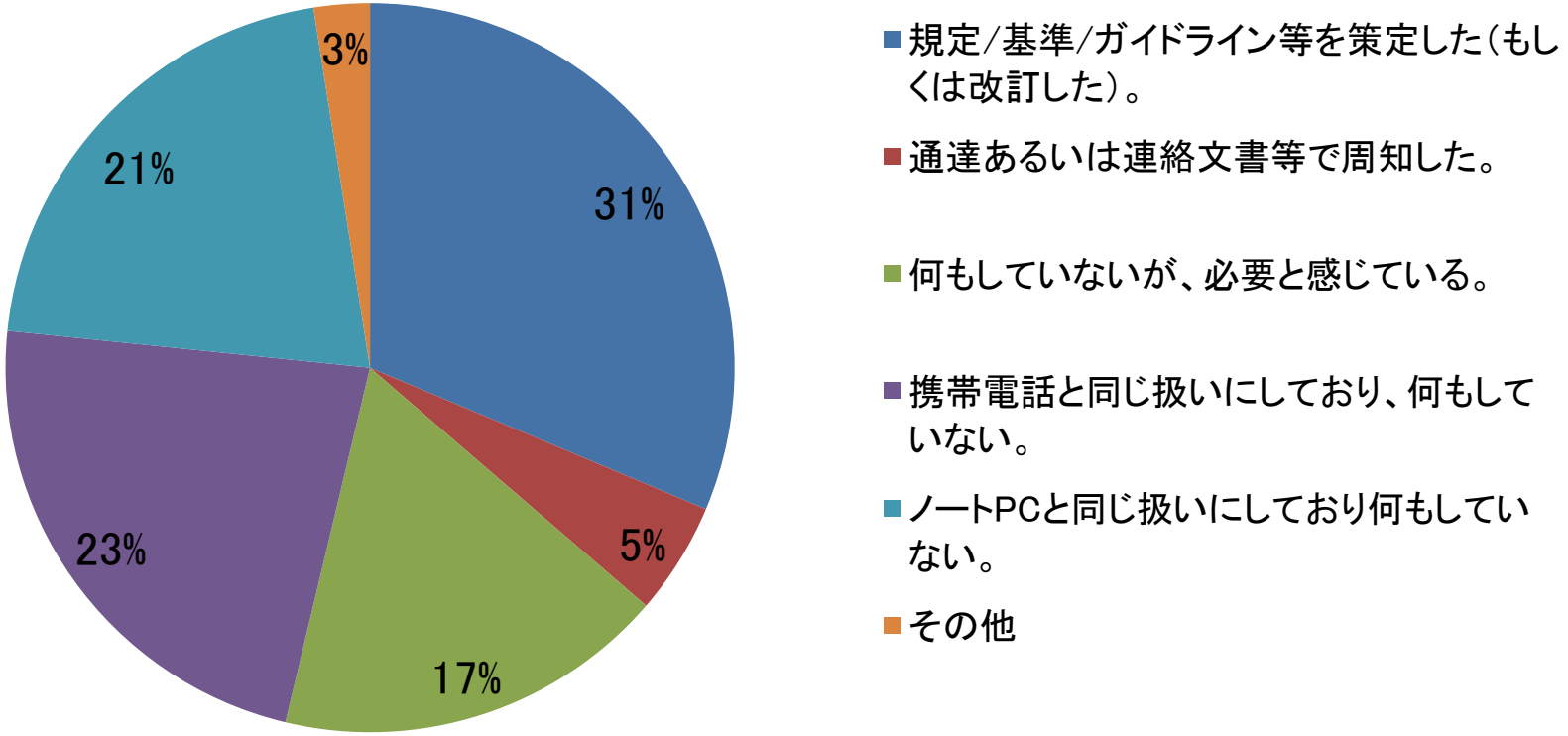


個人所有のスマートデバイスを認めているケースが半数以上。

第2章　スマートデバイスの利用について

※設問9で「**認めている**」と回答した組織のみ

設問11.業務利用を認めるにあたって利用ルールを定めていますか。(N=201)

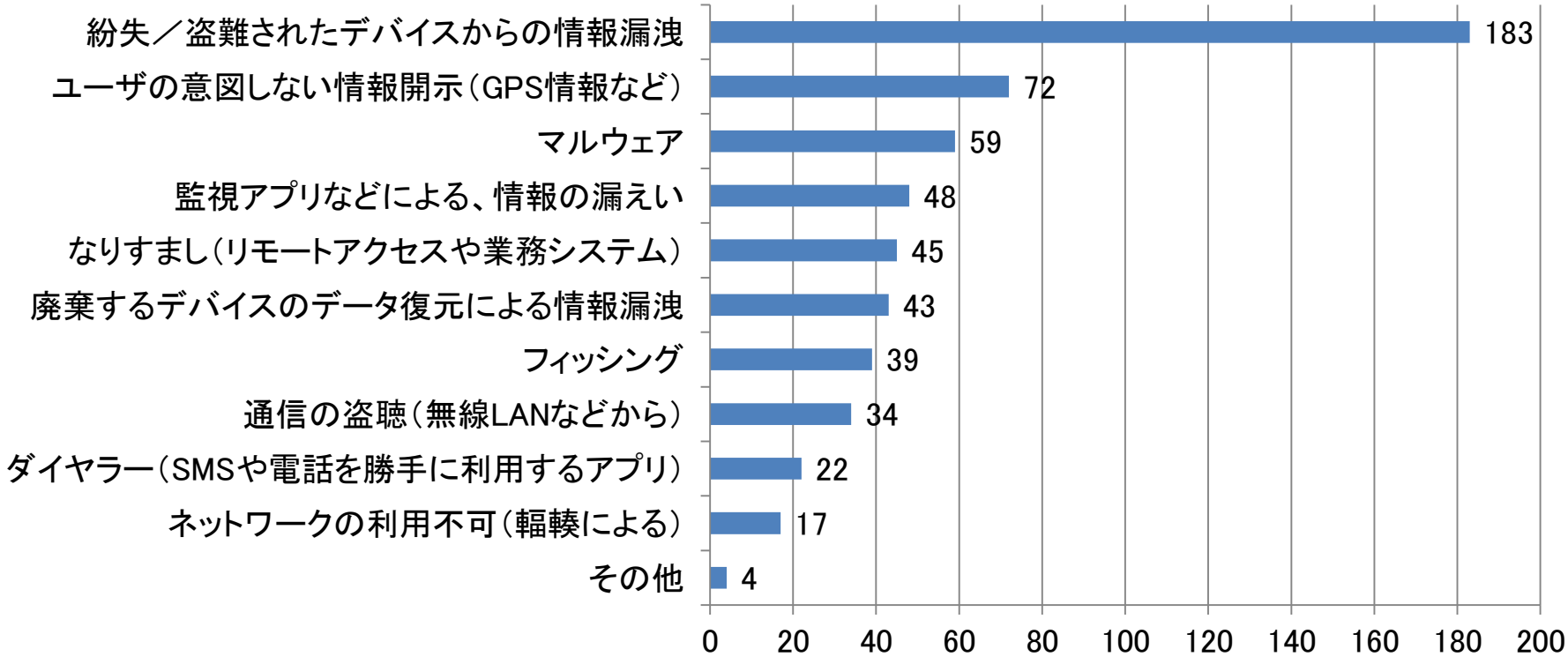


スマートデバイスに特化したルールを制定しているのは36%のみ。

第2章　スマートデバイスの利用について

※設問9で「**認めている**」と回答した組織のみ

設問12.セキュリティ上、どのようなことが懸念されますか。（複数回答）（N=201）



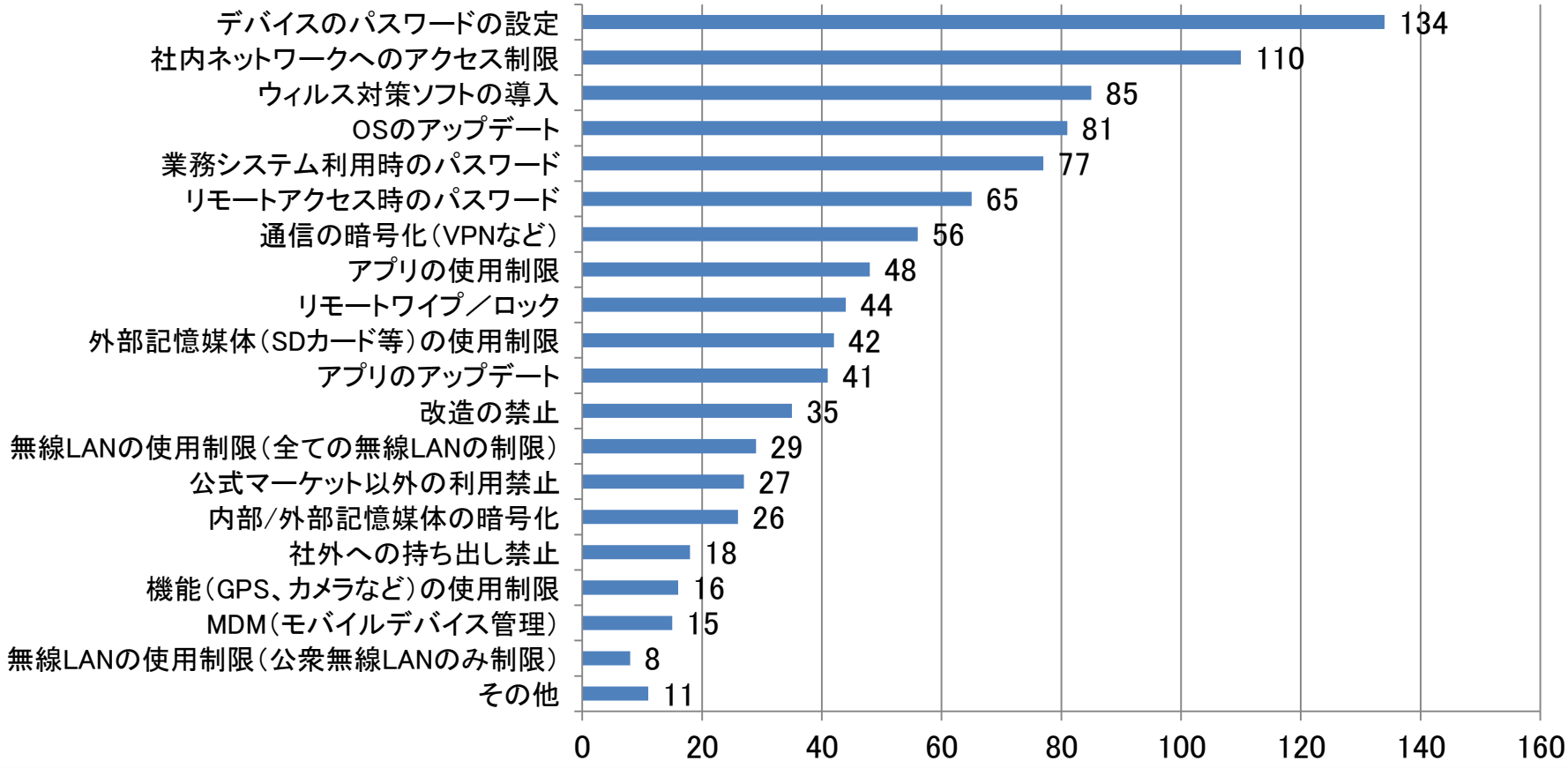
紛失／盗難に対する懸念が特に多い。

第2章　スマートデバイスの利用について

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

※設問9で「**認めている**」と回答した組織のみ

設問13.どのようなセキュリティ対策をしていますか。（複数回答）（N=195）

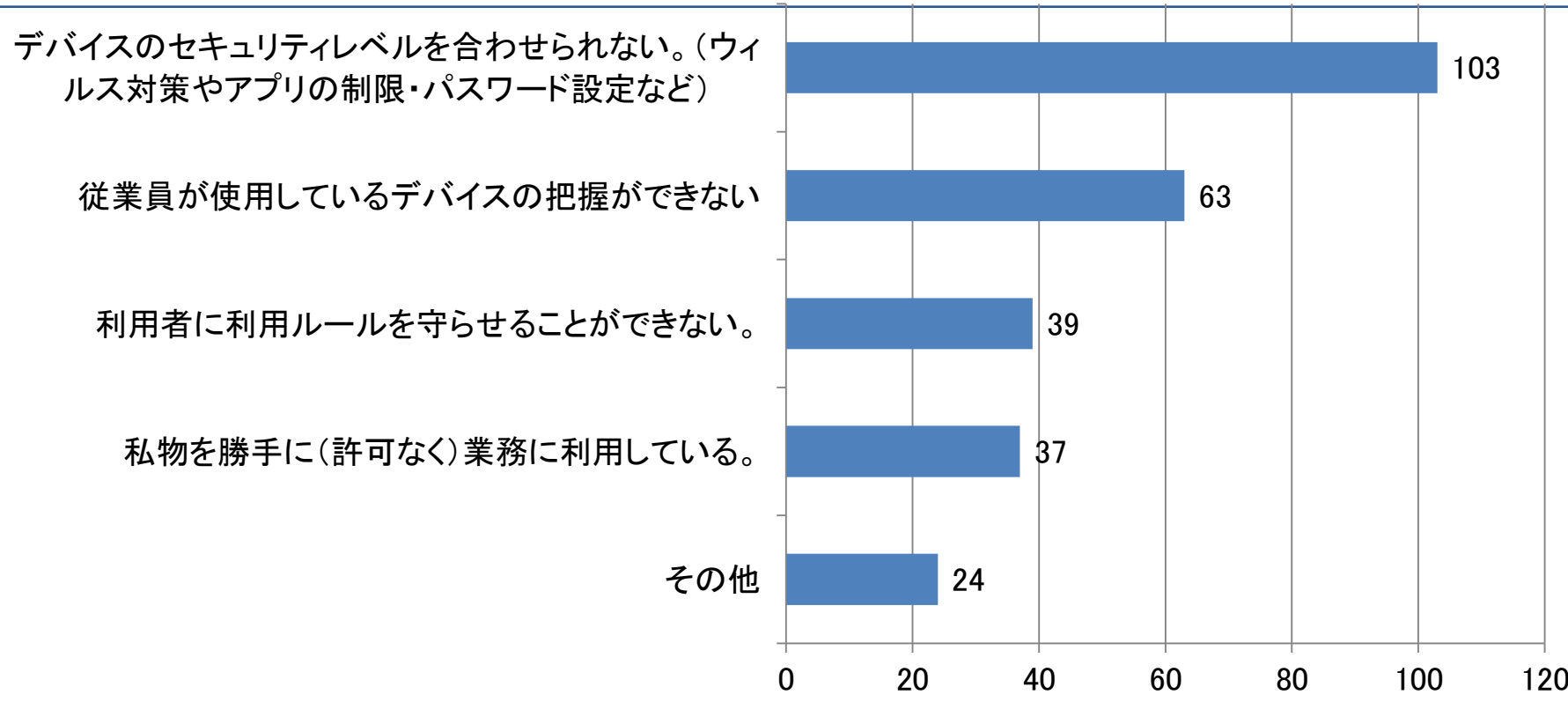


パスワード設定や社内へのアクセス制限などの対策が多い

第2章　スマートデバイスの利用について

※設問9で「**認めている**」と回答した組織のみ

設問14.運用上、どのようなことが課題になっていますか。（複数回答）（N=178）

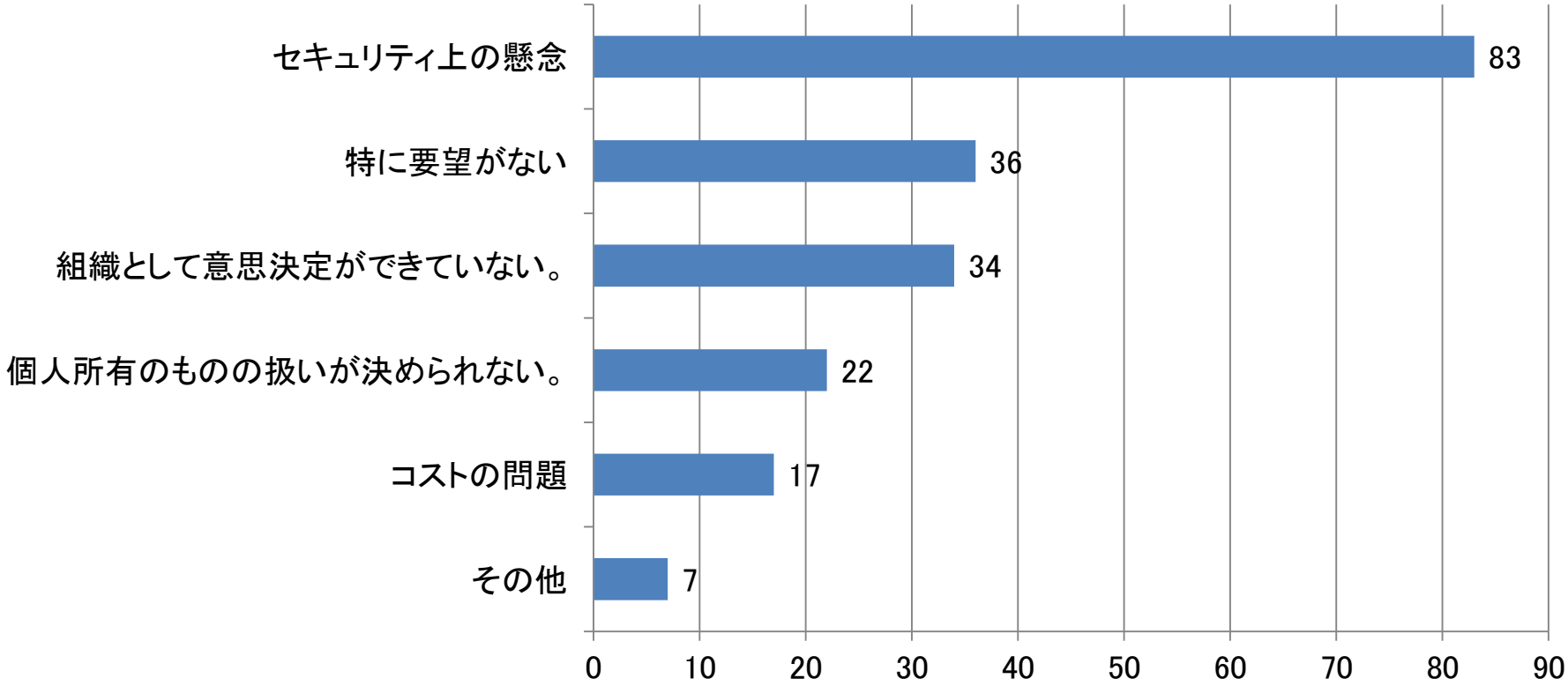


スマートデバイス特有の課題が多く挙げられている。

第2章　スマートデバイスの利用について

※設問9で「**認めていない**」と回答した組織のみ

設問15.スマートデバイスの業務利用を認めない理由は何ですか。（複数回答）（N=123）



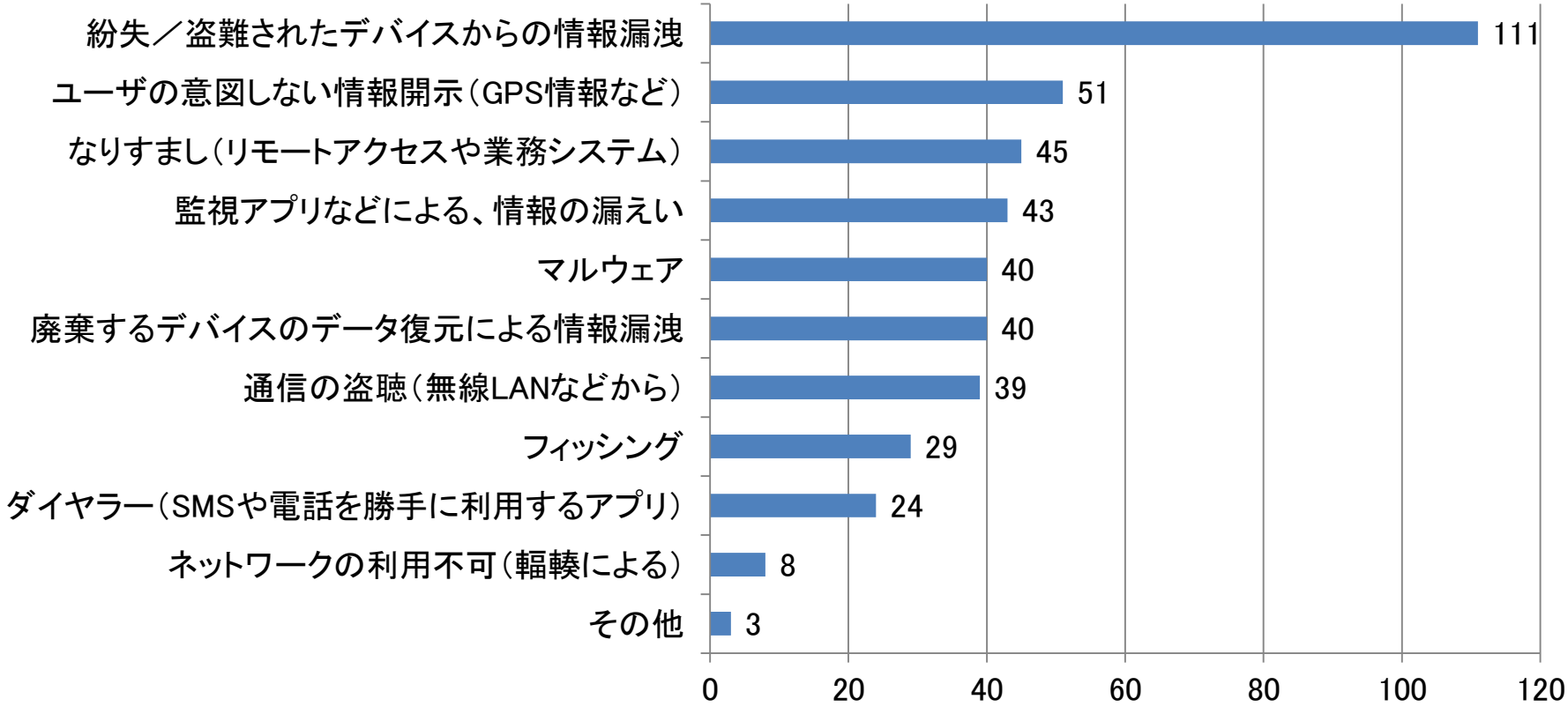
セキュリティ上の懸念が強く、業務利用されていない。

第2章　スマートデバイスの利用について

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

※設問9で「**認めていない**」と回答した組織のみ

設問16.セキュリティ上、どのようなことが懸念されますか。（複数回答）（N=117）

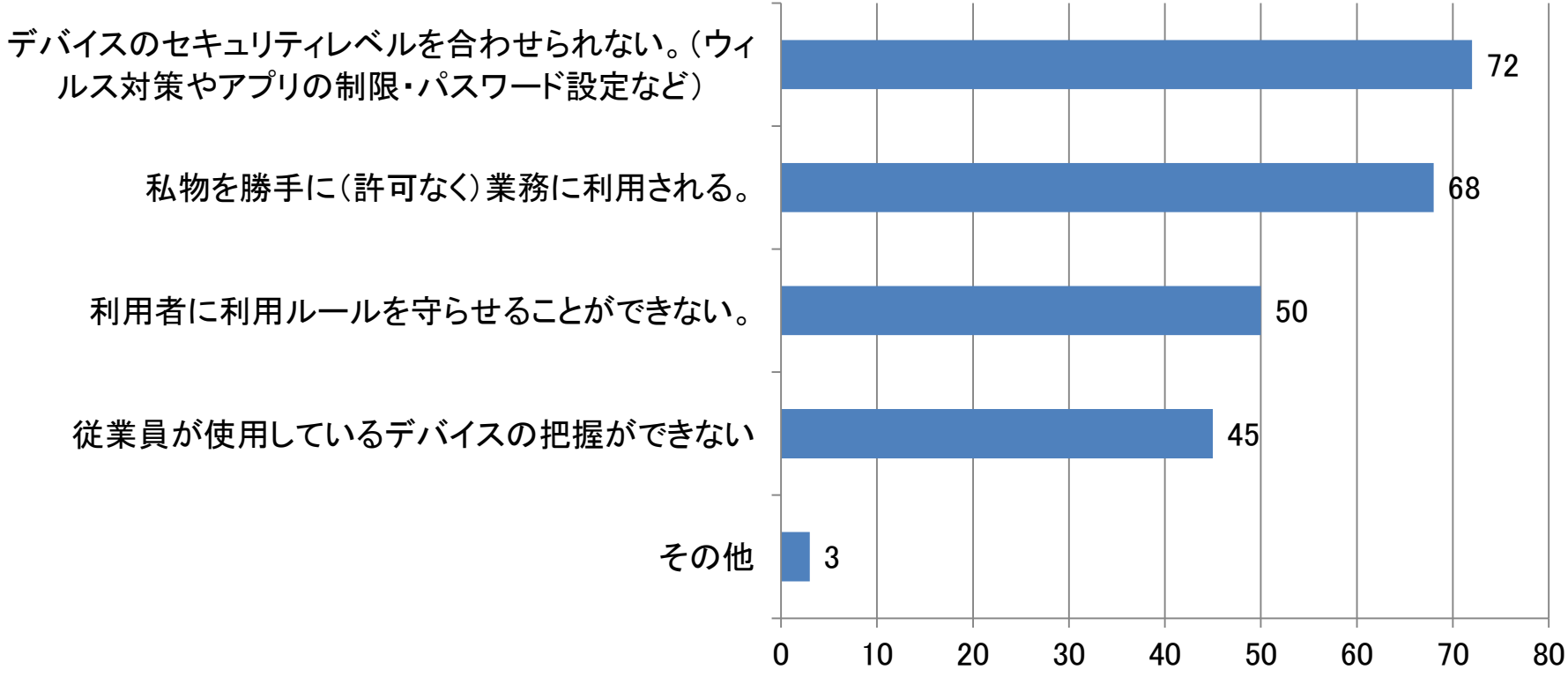


紛失／盗難されたデバイスからの情報漏えいが特に懸念されている。

第2章　スマートデバイスの利用について

※設問9で「**認めていない**」と回答した組織のみ

設問17.運用上、どのようなことが課題になると予想されますか。（複数回答）(N=111)



セキュリティ対策とともに、許可なく私物が利用されることへの懸念がある。

考察（第2章　スマートデバイスの利用について）

- 半数以上の組織でスマートデバイスが業務に利用されているが、スマートデバイスに特化した利用ルールを定めている組織は約1／3にとどまり、対応が追いついていない状況が読み取れる。

- 利用を認めている組織のうち、半数以上が個人所有のデバイスの業務利用を認めているが、その一方で、従業員が使用しているデバイスの把握ができないことが運用上の課題となっている。

- 紛失／盗難に対する懸念が強いが、リモートロック／ワイプや内部／外部記憶媒体の暗号化の対策を実施している組織は少ないという結果になっており、十分なセキュリティ対策が実施されている状況ではないと言える。

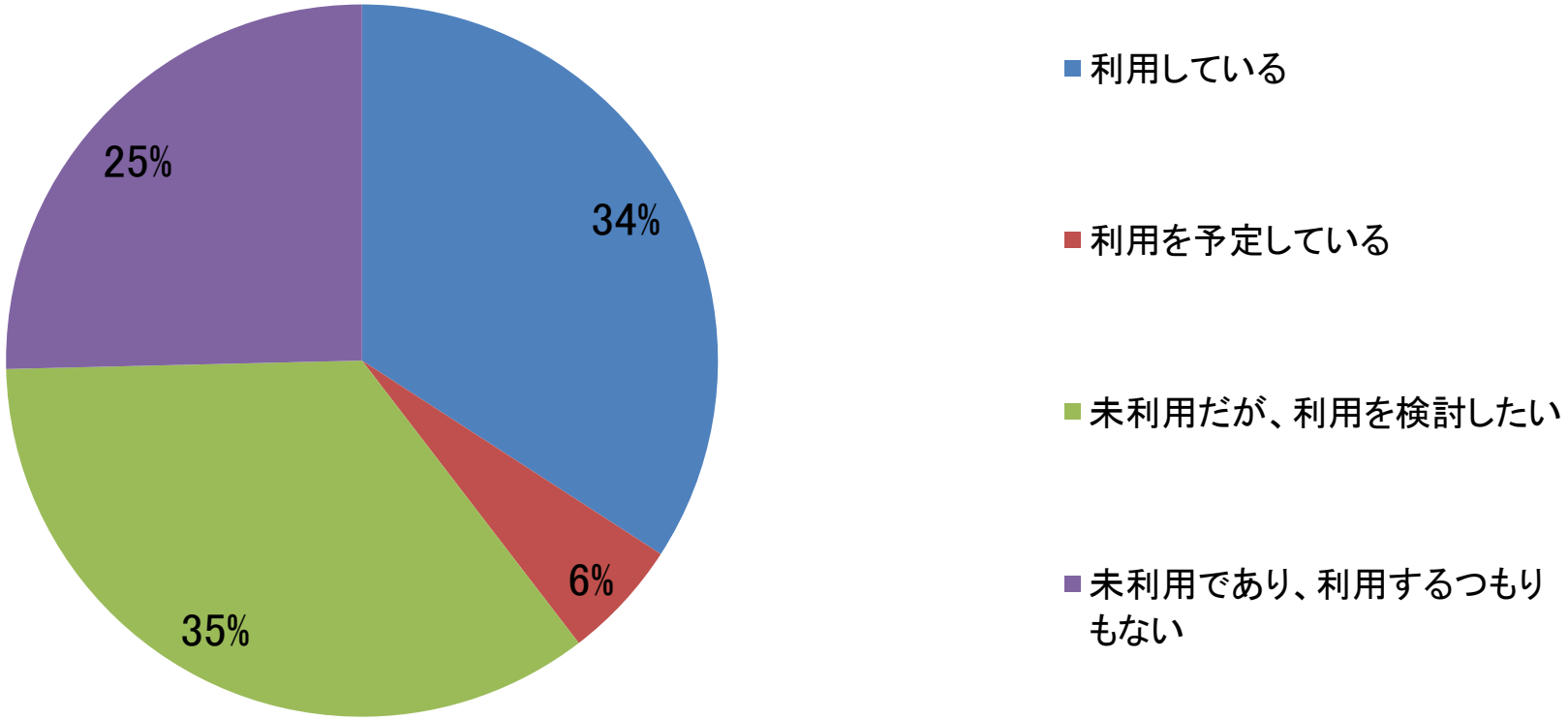
- 管理のためのノウハウが蓄積されているPCと違い、従業員の使用するスマートデバイスのセキュリティレベルを合わせられないことが、スマートデバイス独自の運用上の課題となっていると考えられる。

- 利用を認めていない理由として、紛失／盗難をはじめとしたセキュリティ上のリスクとともに、許可なく私物が利用されることへの懸念が挙げられている。

第3章

クラウド・コンピューティング（クラウド）について

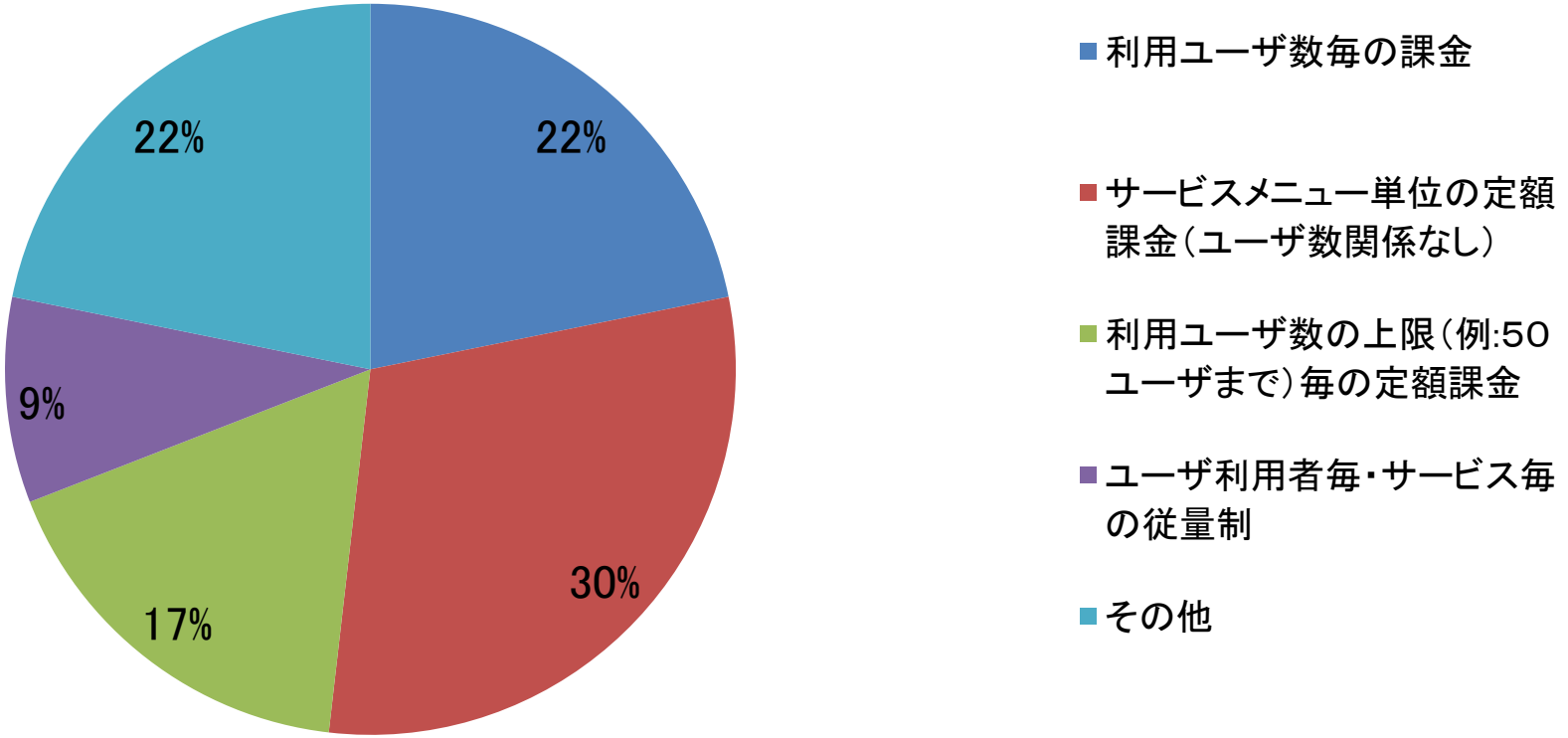
設問18.クラウド・コンピューティングを利用していますか。(N=321)



現在は、未利用のほうが多いが、検討中の組織が多い。

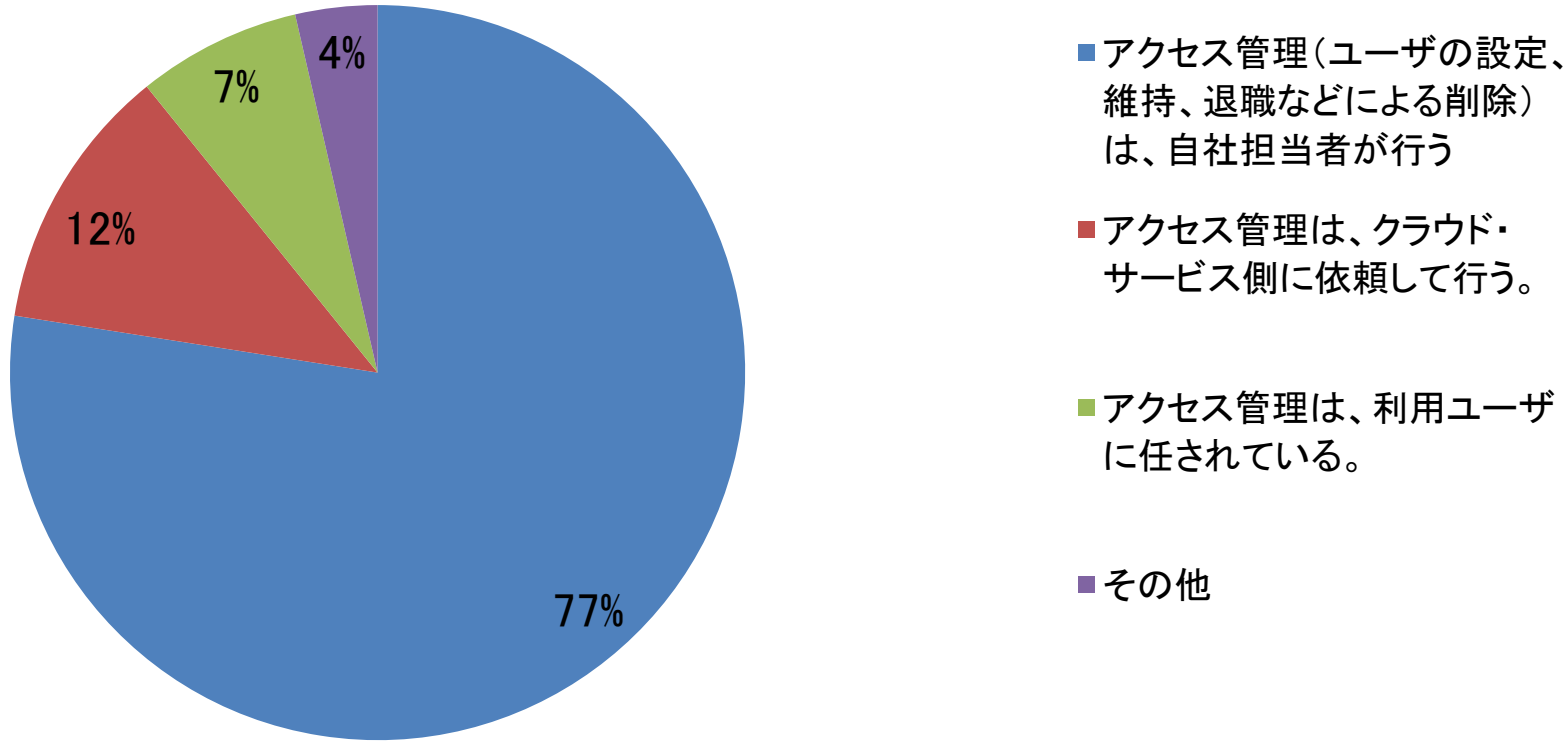
第3章　クラウド・コンピューティングについて

設問19.クラウド・コンピューティング（複数ある場合は最大のサービス）の利用料金形態は以下のいずれでしょうか。（N=110）



利用料金は、多様な形態に分かれている。

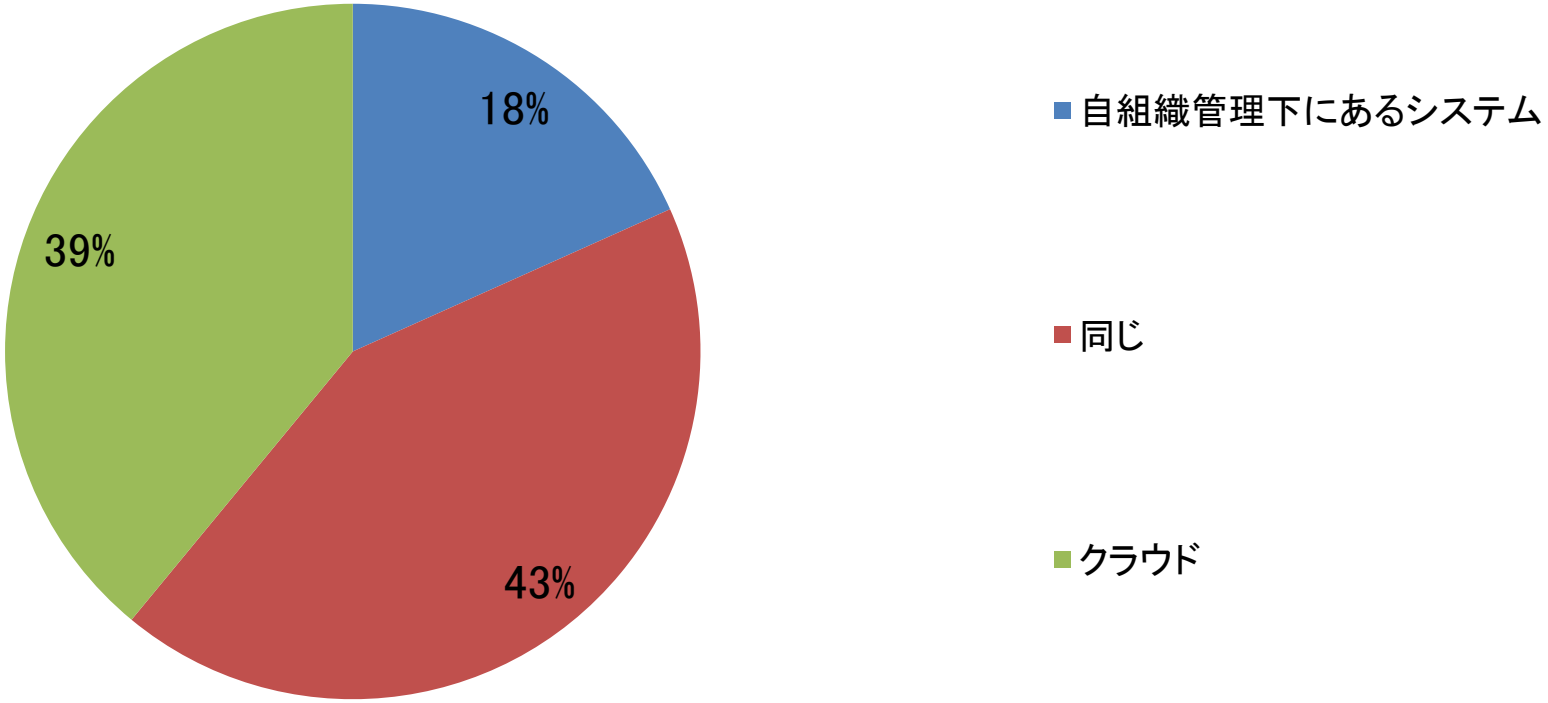
設問20.クラウド・コンピューティング（複数ある場合は最大のサービス）の利用者登録の形態は以下のいずれでしょうか。(N=111)



アクセス管理は、自組織の担当者が行うことが多い。

第3章　クラウド・コンピューティングについて

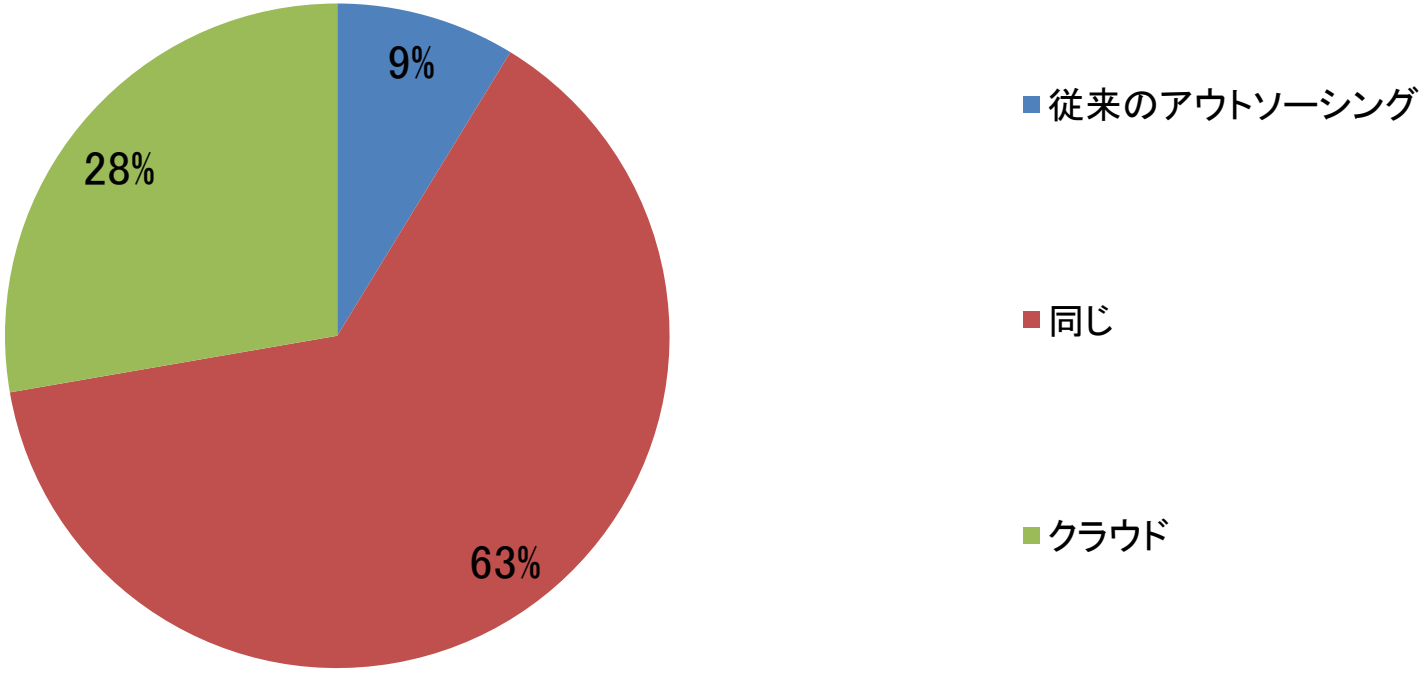
設問21.自組織管理下にあるシステムに対するセキュリティ上の脅威と、クラウド・コンピューティングに対するセキュリティ上の脅威とで、どちらの脅威が大きいと感じますか。(N=328)



自組織管理よりクラウドの方が脅威が大きいと感じている組織が多い。

第3章　クラウド・コンピューティングについて

設問22.従来のアウトソーシング（ホスティング）に対するセキュリティ上の脅威と、クラウド・コンピューティングに対するセキュリティ上の脅威とで、どちらの脅威が大きいと感じますか。（N=321）



同じが最も多い(63%)が、クラウドとアウトソーシングを比較すると
クラウドの方が脅威が大きいと感じている組織が多い。

考察（第3章　クラウドコンピューティングについて）

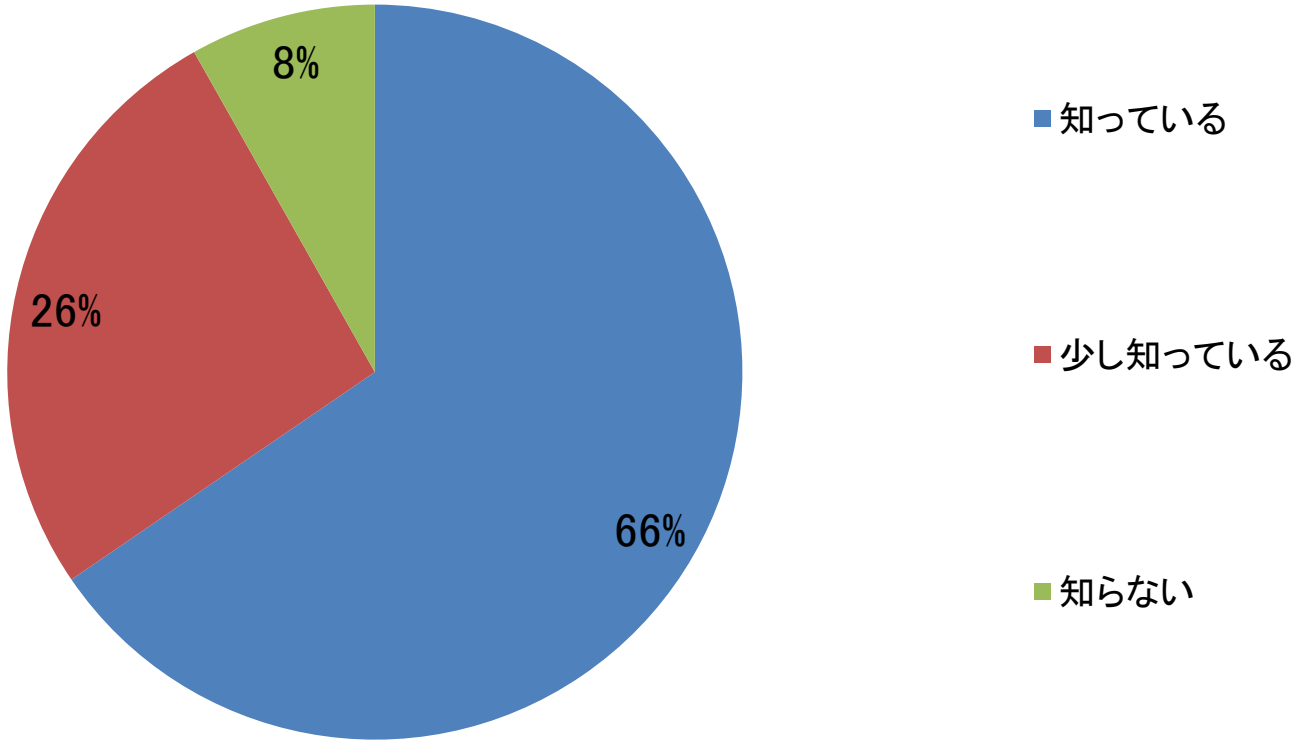
- クラウド・コンピューティングを利用している組織が34%、利用予定、検討したいを含めると75%となり関心は高い。（平成22年度は20%、67%）
- クラウドコンピューティングの利用料金は、従量課金の他に定額制もあり、多様な形態に分かれている。
- クラウドコンピューティングの利用者登録は、自組織担当者が行うことが多い。
- クラウドのセキュリティ上の脅威を自組織管理と比較した設問の回答を、平成22年度に実施した当研究室による調査結果と比較すると、クラウド(36%⇒39%)、同じ(41%⇒43%)、自社管理下(23%⇒18%)となった。
- 同様に、クラウドのセキュリティ上の脅威を従来のアウトソーシングと比較した設問の回答を、平成22年度の調査結果と比較すると、クラウド(27%⇒28%)、同じ(60%⇒63%)、従来のアウトソーシング(13%⇒9%)となった。
- クラウドコンピューティングを利用するユーザは増えている一方で、セキュリティへの懸念は2年前からあまり変化していないと考えられる。

第4章

標的型攻撃の対応について

第4章　標的型攻撃の対応について

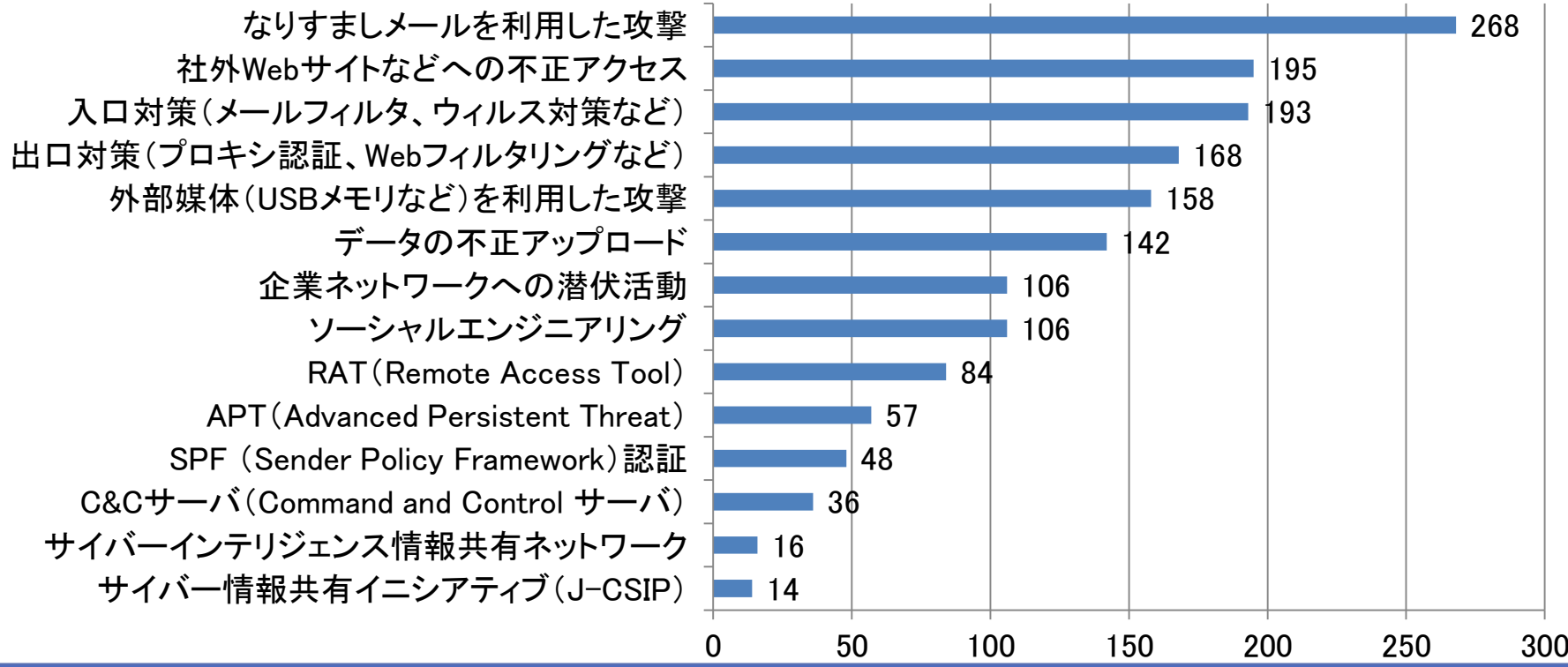
設問23.「標的型攻撃」という言葉を知っていますか。（N=330）



標的型攻撃という言葉自体の認知度は高い。

第4章　標的型攻撃の対応について

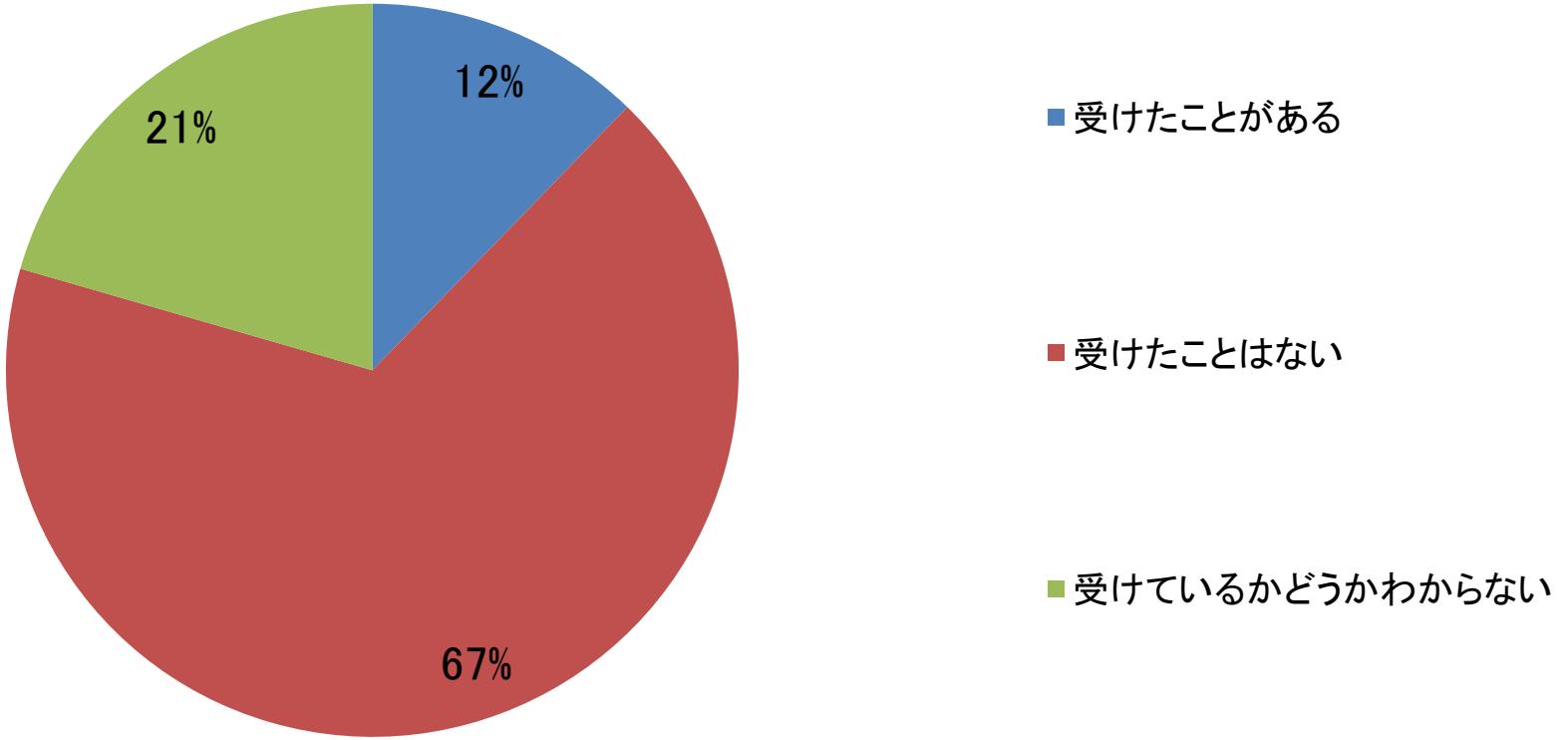
設問24.標的型攻撃に関連するキーワードで知っているものを教えてください。（複数回答）（N=302）



入口/出口対策、なりすましメールの認知度が高いが
情報共有に関連する取り組みの認知度は低い。

第4章　標的型攻撃の対応について

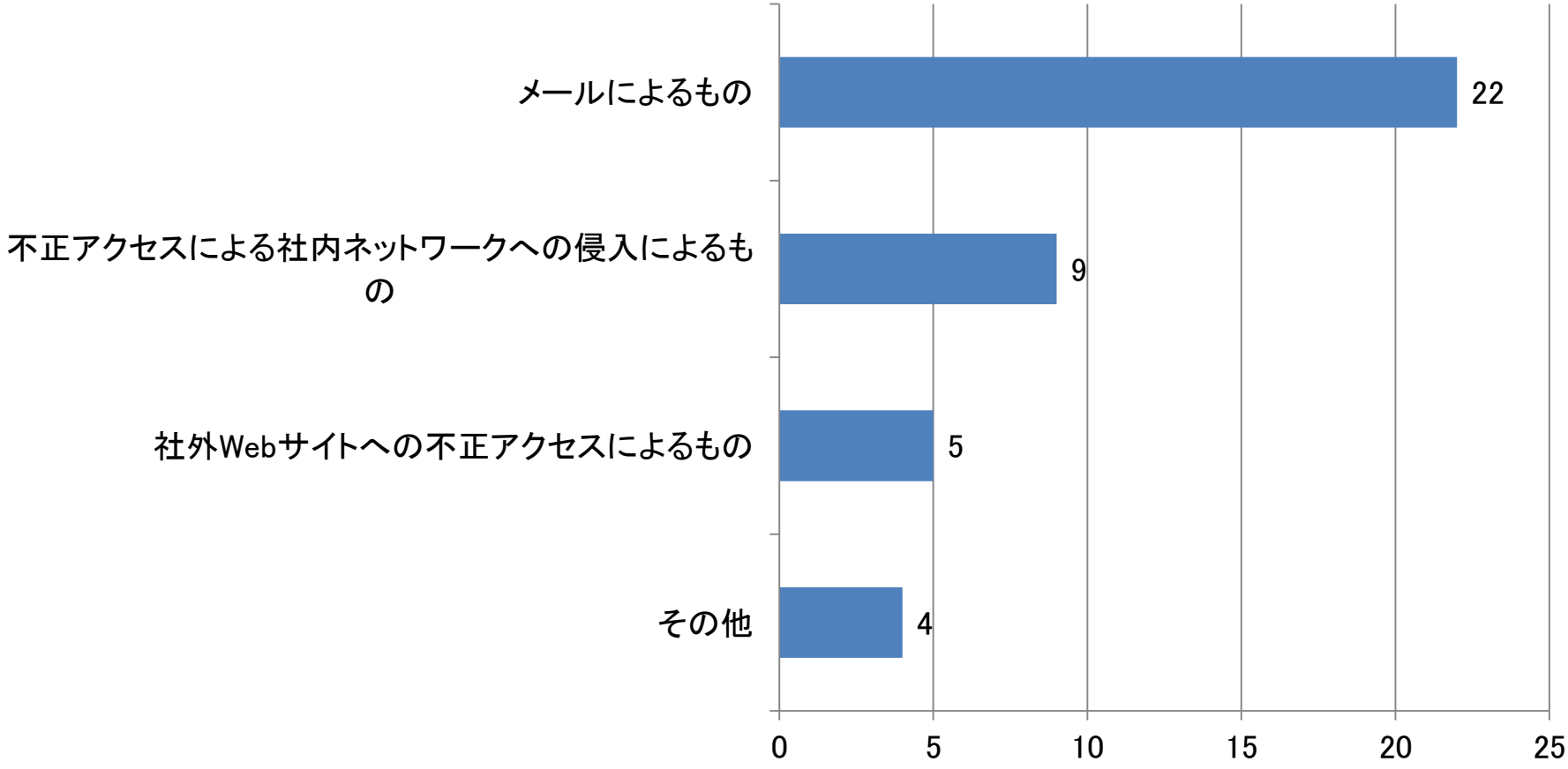
設問25.標的型攻撃若しくは標的型攻撃と思われる攻撃を受けた経験はありますか。(N=302)



実際に攻撃を受けたことがあると回答した組織は少ない。

第4章　標的型攻撃の対応について

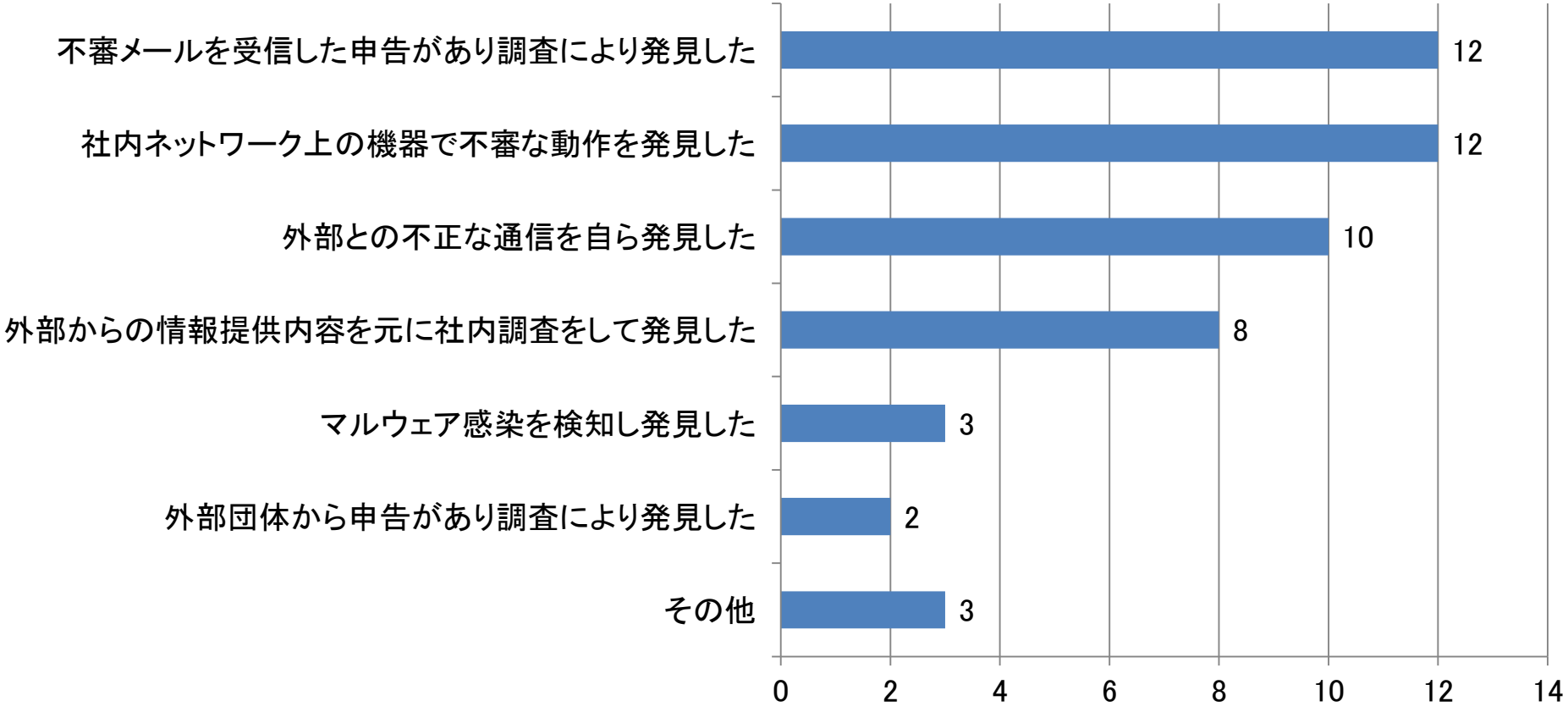
設問26.それはどのような攻撃手法でしたか。（複数回答）（N=37）



メールによるものが多数を占める。

第4章　標的型攻撃の対応について

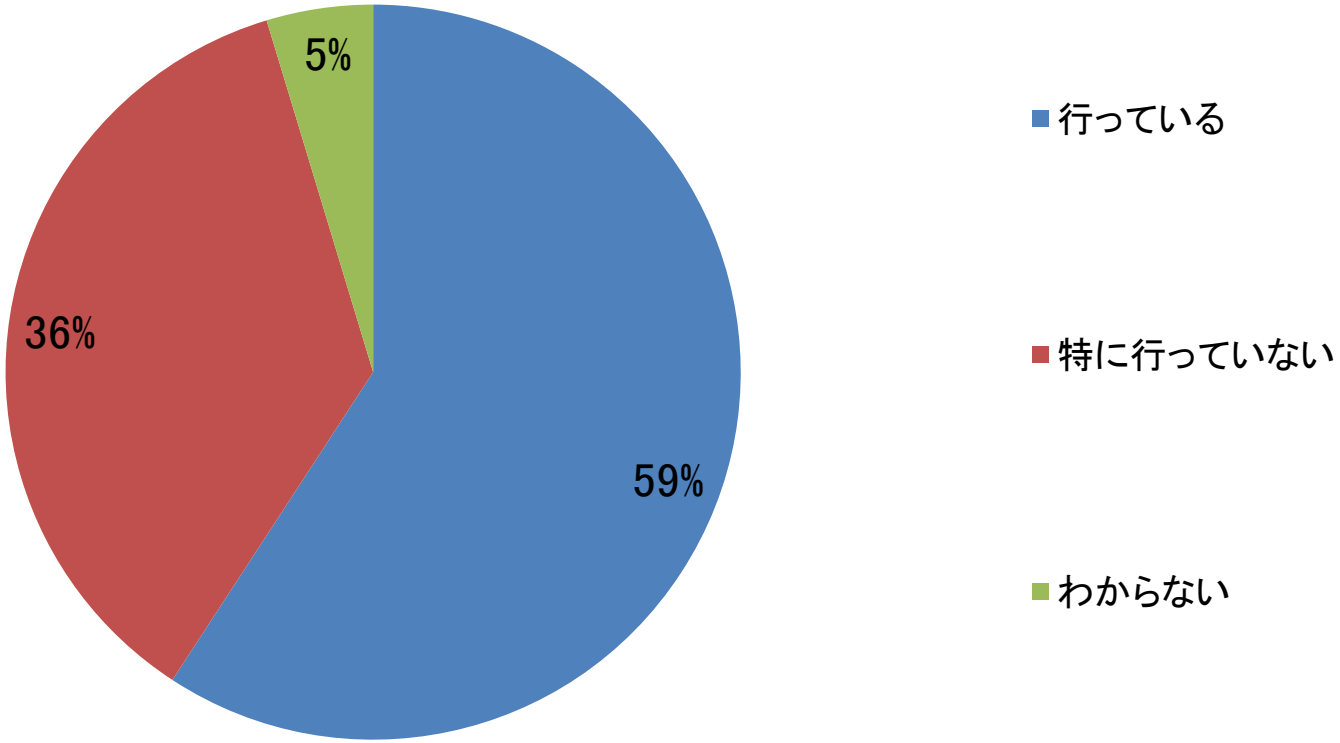
設問27.その攻撃をどうやって発見しましたか。（複数回答）（N=37）



ネットワークや機器や通信の監視で発見したケースに加え、
不審メール受信申告による発見が多い。

第4章　標的型攻撃の対応について

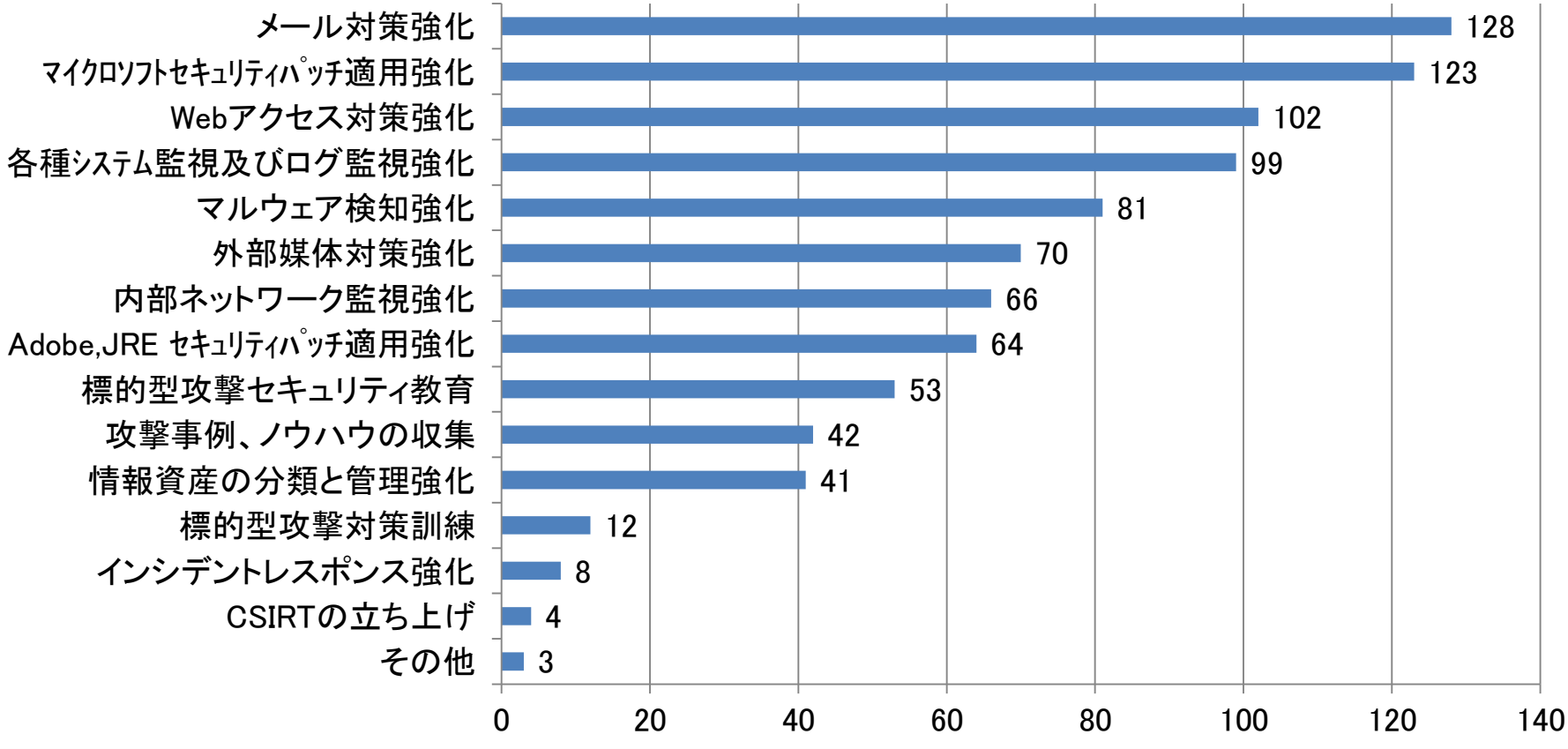
設問28.標的型攻撃対策を行っていますか。（N=293）



対策を実施している割合が半数を超えている。(59%)

第4章　標的型攻撃の対応について

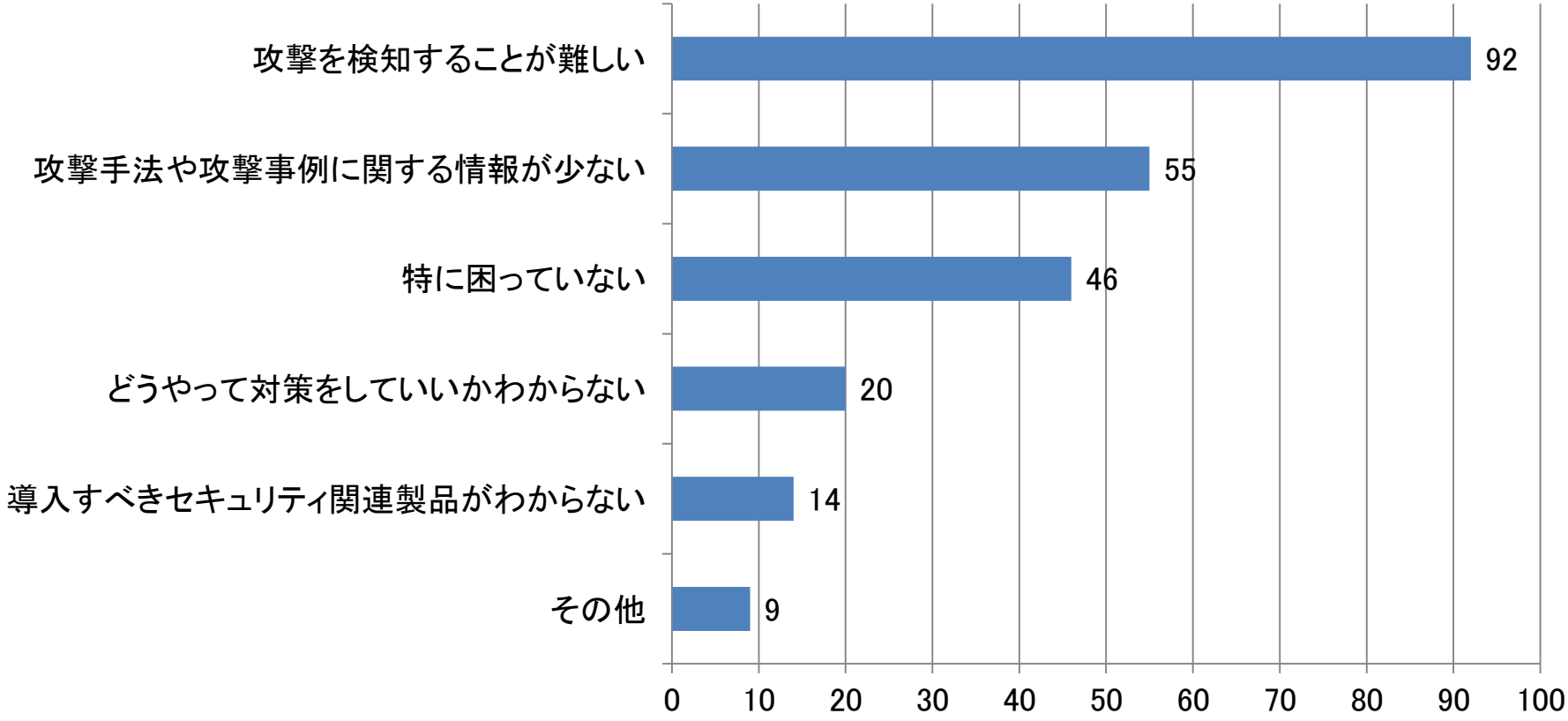
設問29.どのような対策を行っていますか。（複数回答）（N=174）



入口/出口対策、ログ監視などの予防策の強化率が高いが、
インシデントレスポンスやCSIRT立ち上げなどの事後対応の強化率が低い。

第4章　標的型攻撃の対応について

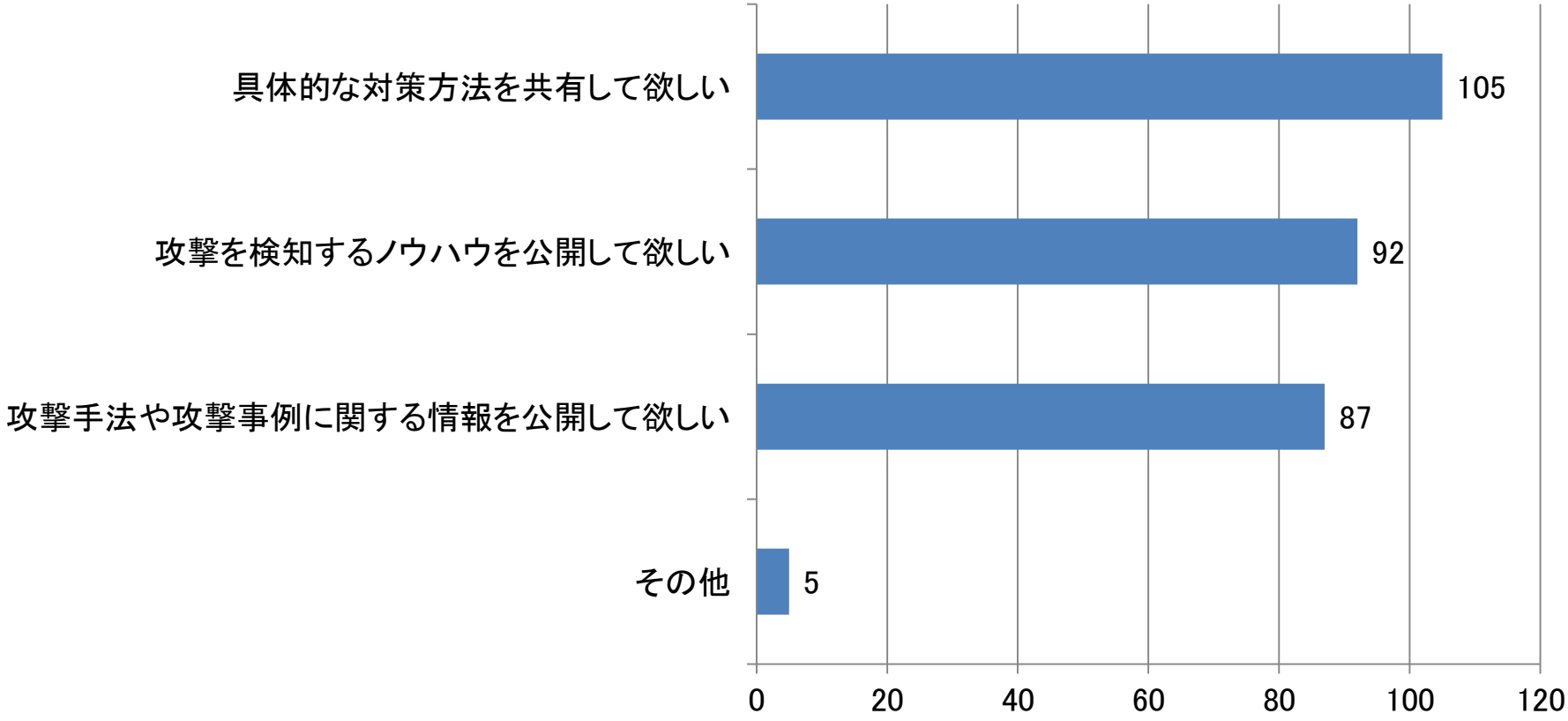
設問30.標的型攻撃の対策を行う上で困ったことがあれば教えてください。（複数回答）（N=168）



検知の難しさ、事例の少なさが課題として多く挙げられている。

第4章　標的型攻撃の対応について

設問31.困っている方へ、今後必要と思う事を教えてください。（複数回答）（N=156）

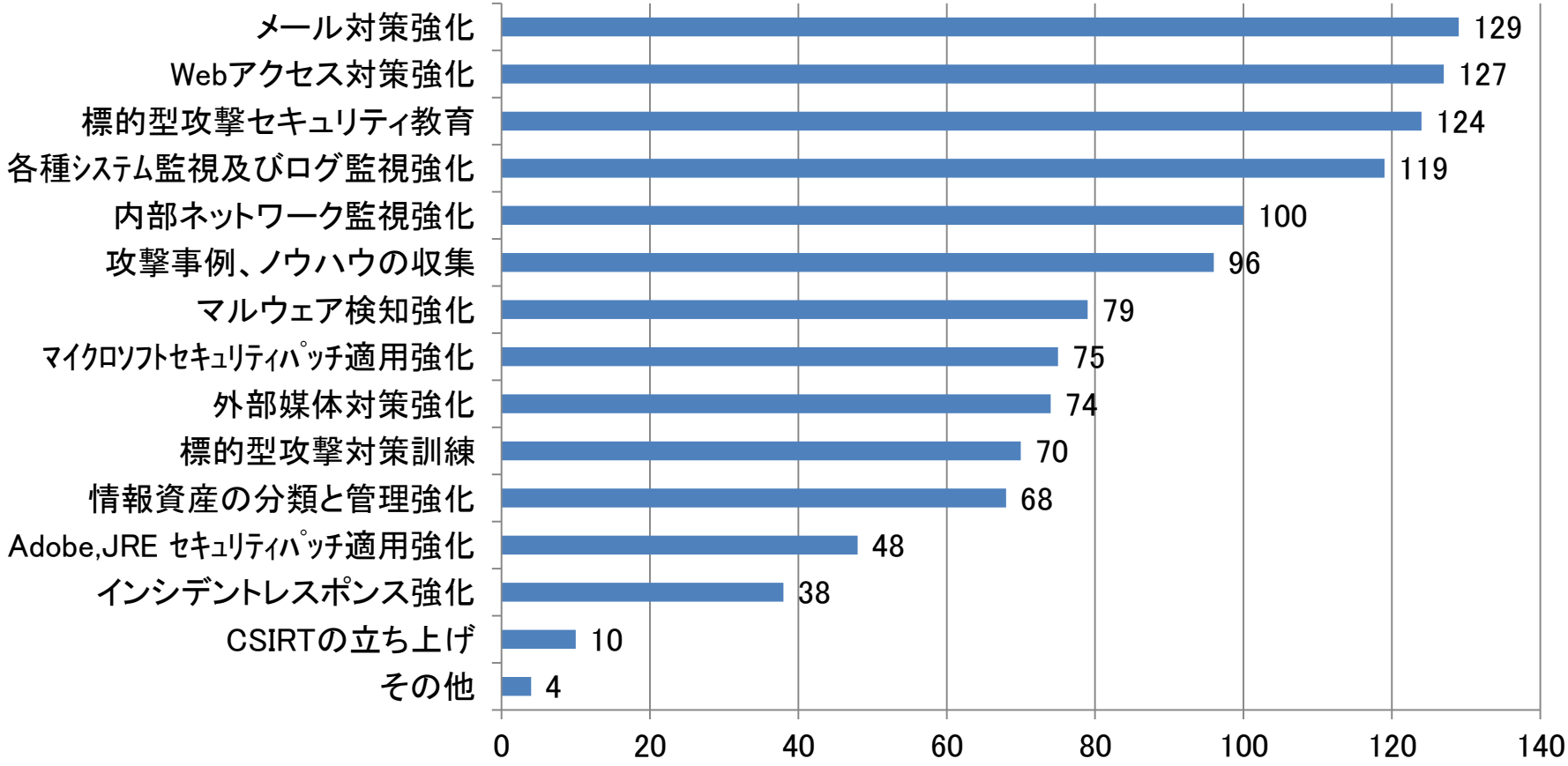


検知ノウハウ、対策方法などの情報共有への期待が高い。

第4章　標的型攻撃の対応について

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

設問32.今後どのような対策が必要と思いますか。(複数回答)　(N=283)



メール/Webアクセス対策/ログ監視は必要性が高く、攻撃事例やノウハウの収集/教育/訓練は、対策の必要性は感じている。CSIRT立ち上げやインシデントレスポンスの必要性は低いと認識されている。

考察（第4章　標的型攻撃の対応について）

- 標的型攻撃という言葉の認知率は92%と高く、そのキーワードとしては、なりすましメールを利用した攻撃、入口/出口対策が認知率が高い。

- 実際に攻撃を受けていると認識している組織は少ない（12%）。実際の攻撃被害としては、なりすましメールによるものが多く、ネットワークや機器の監視による発見に加え、従業員からの不審メール報告により発見されているものが多い。

- 対策の実施率は半数を超えており（59%）、予防対策である基礎的な対策（パッチ適用）に加えて、入口/出口対策、ログ監視の強化率が高い。その反面、CSIRT設置、インシデントレポンス強化等の事後対応への取り組み率が低い。

- 対策実施にあたっては、検知の難しさ、事例の少なさが課題として多く、検知ノウハウ、事例、対策方法の共有など標的型攻撃への情報共有に期待が多い。これは、今後必要な対策に関しても同様の傾向にある。また、CSIRT設置、インシデントレポンス強化の事後対策への取り組みは、対策実施済みの状況と同様に必要性も低い。

第5章

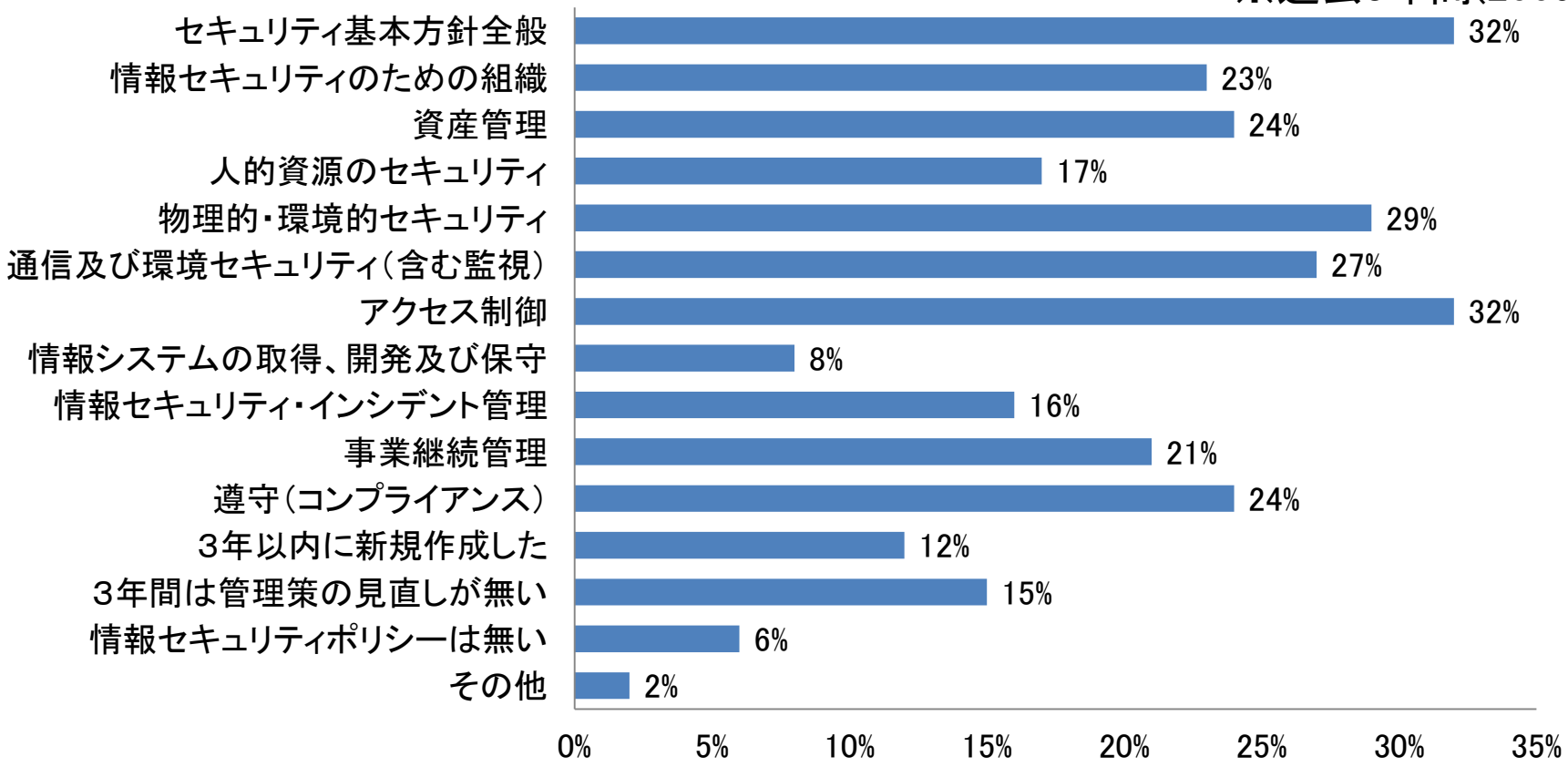
アクセス制御と証跡(ログ)管理について

第5章　アクセス制御と証跡(ログ)管理

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

設問33.情報セキュリティポリシー見直し項目(複数回答)(N=322)

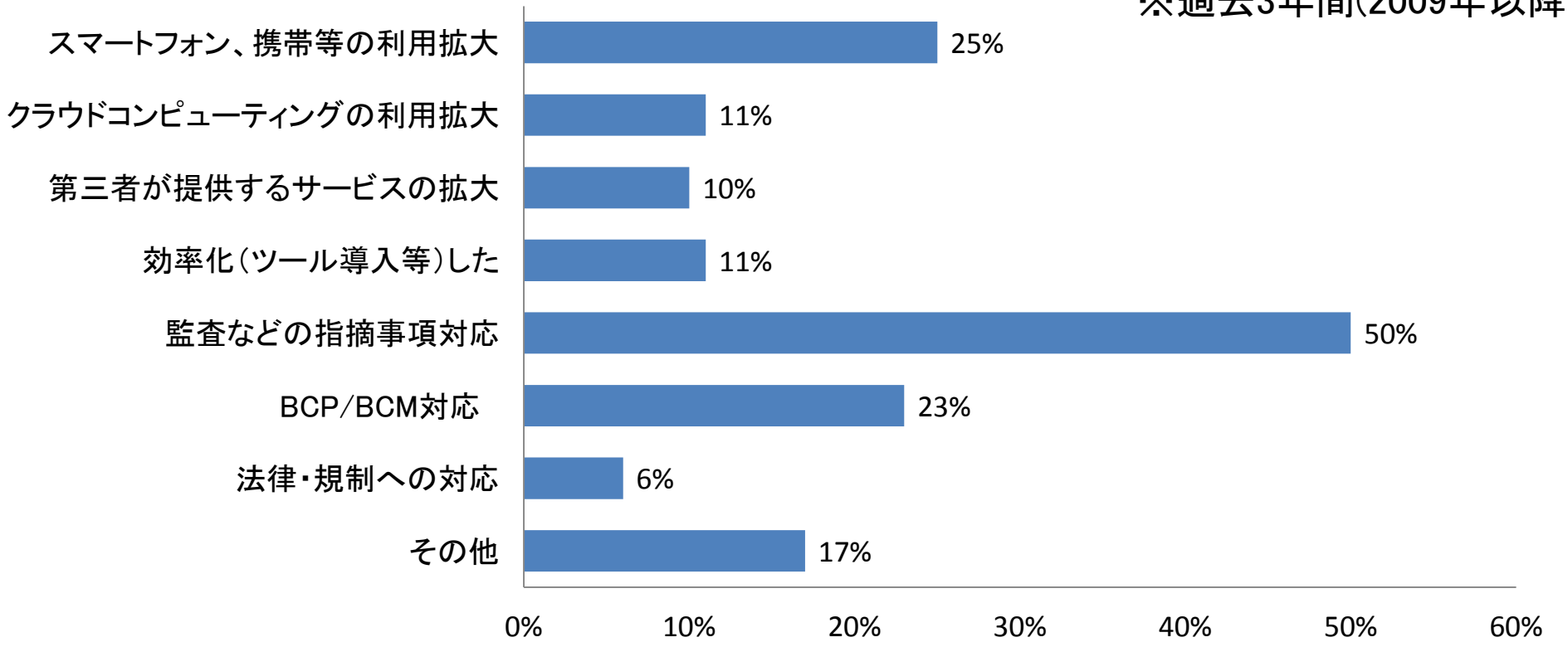
※過去3年間(2009年以降)



セキュリティ基本方針全般とアクセス制御に対する見直しが多かった。

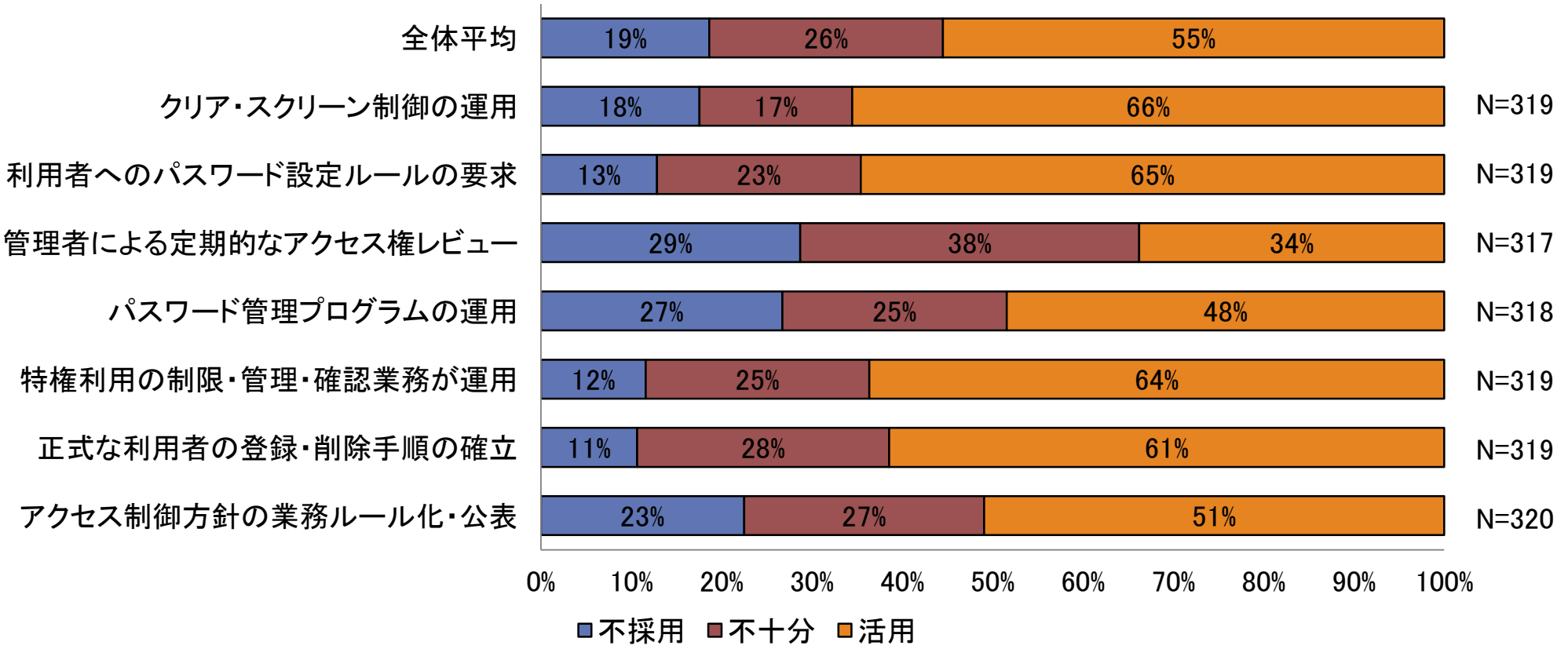
設問34.情報セキュリティポリシー見直しの理由（複数回答）（N=242）

※過去3年間(2009年以降)



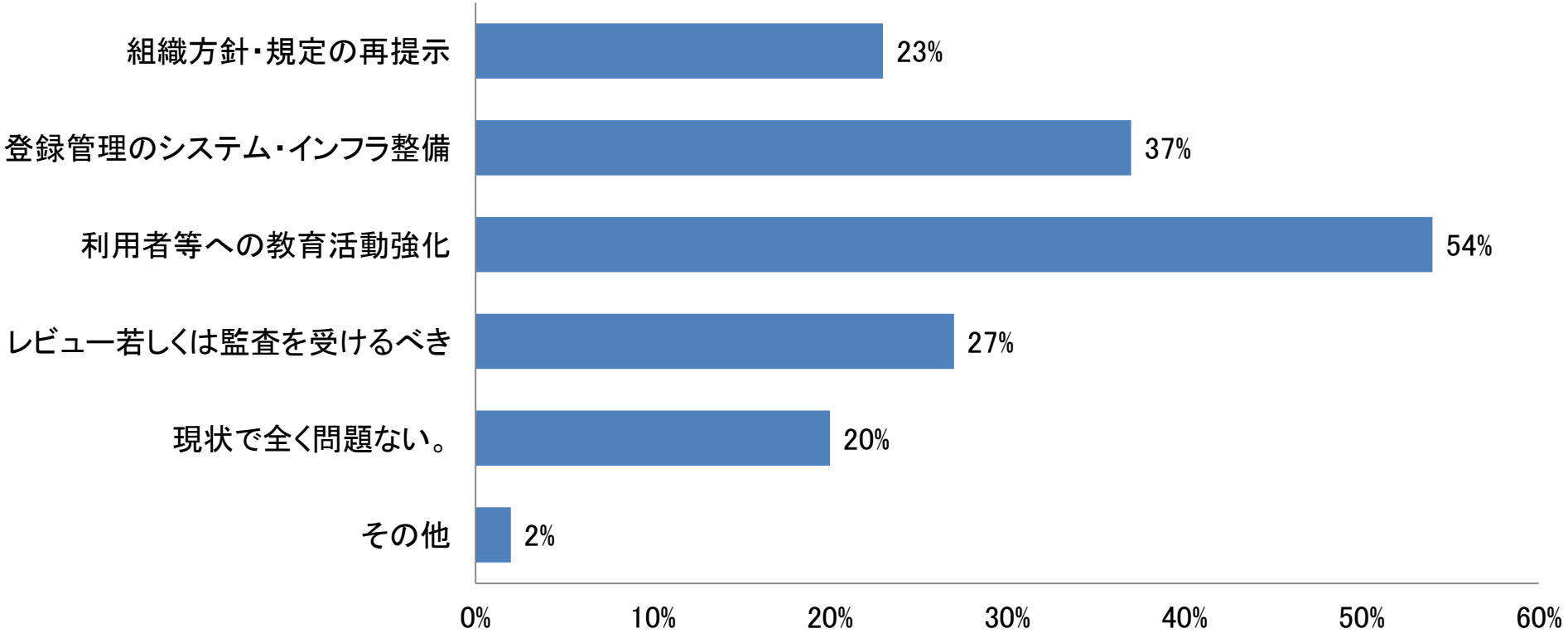
**Pマークや監査の指摘事項対応が50%と多く、
スマートフォン、携帯の利用拡大、BCP/BCM対応が続いた。**

設問35.アクセス制御（利用者）管理策の活用



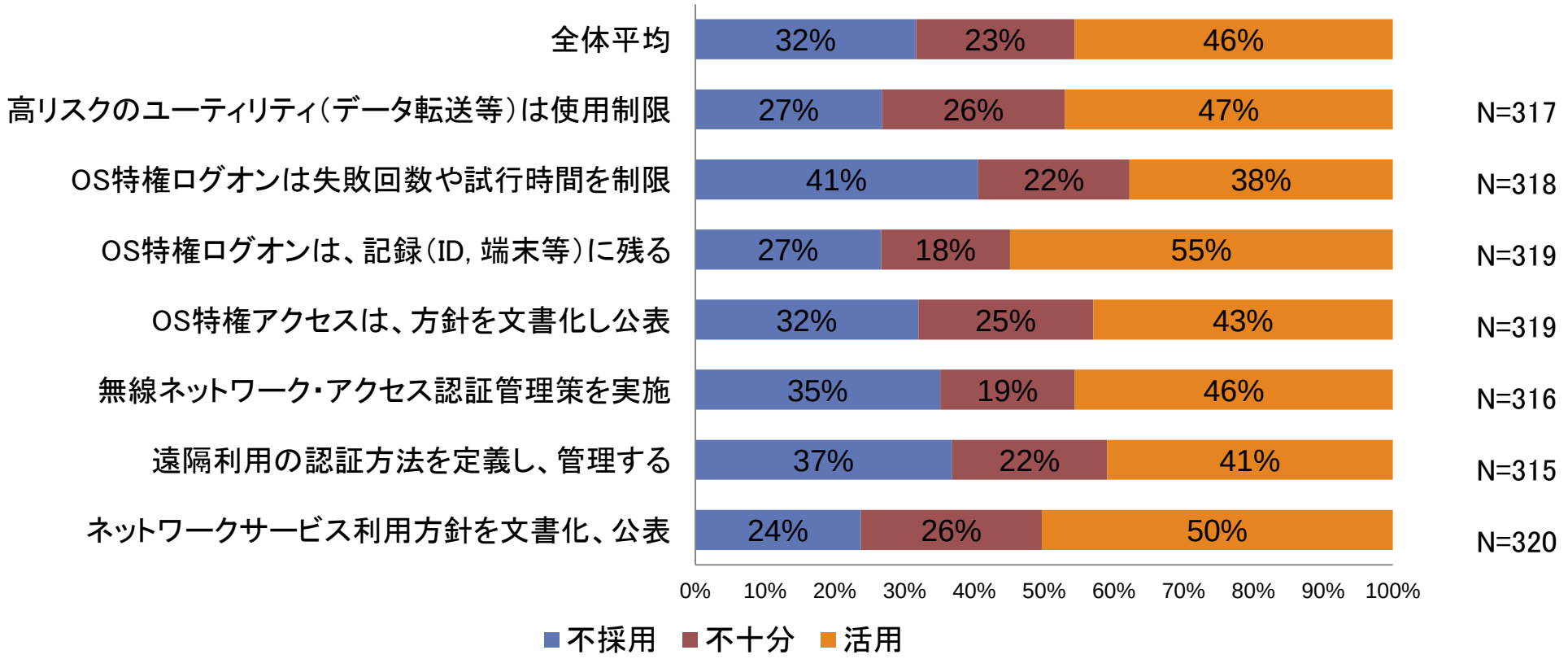
管理者による定期的な利用者アクセス権レビューの活用が少ない。

設問36.アクセス制御（利用者）管理策の強化方策（複数回答）（N=302）



利用者等への教育活動強化が多く、
登録管理のシステム・インフラ整備が続いた。

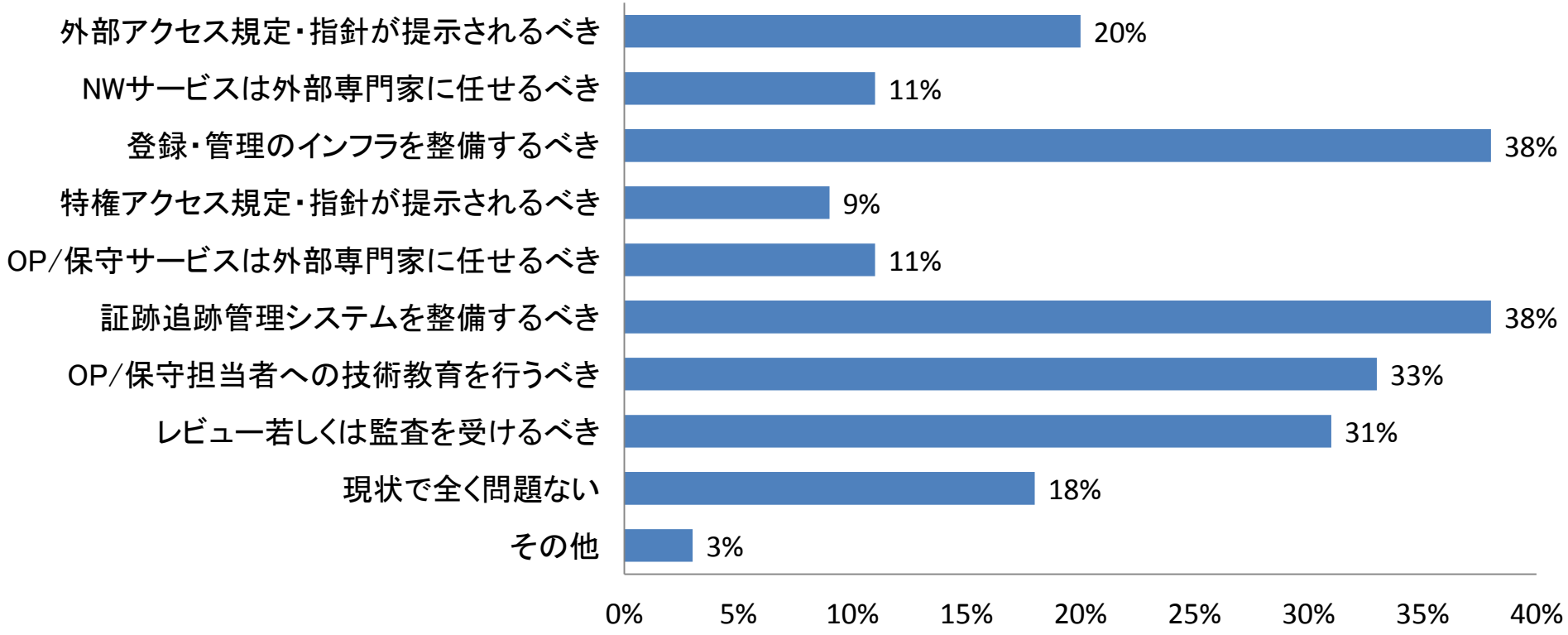
設問37.アクセス制御（ネットワーク・OS）管理策の活用



OS特権ログオンの失敗回数や試行時間の制限活用が少ない。

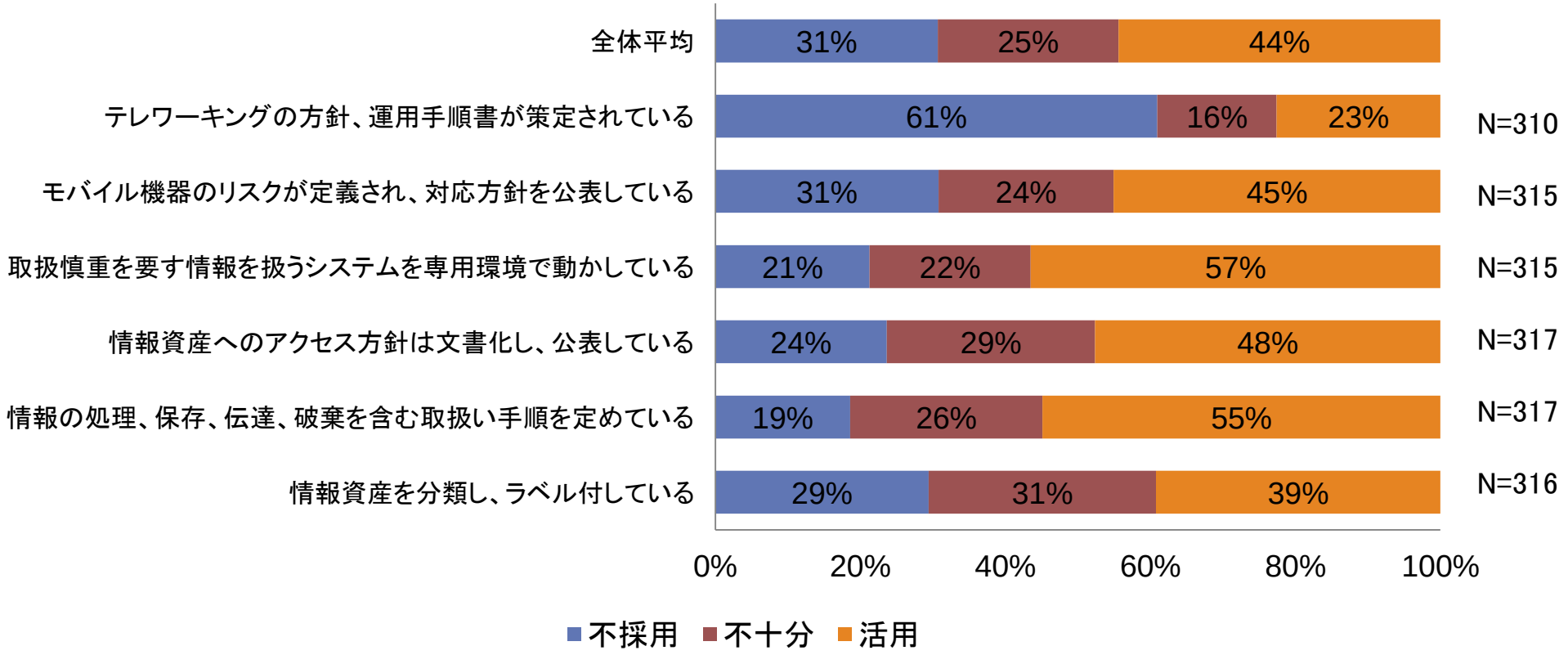
第5章　アクセス制御と証跡(ログ)管理

設問38.アクセス制御（NW/OS）管理策の強化方策（複数回答）（N=308）



登録管理インフラと認証追跡管理システムを整備が多く、担当者への技術教育が続いた。

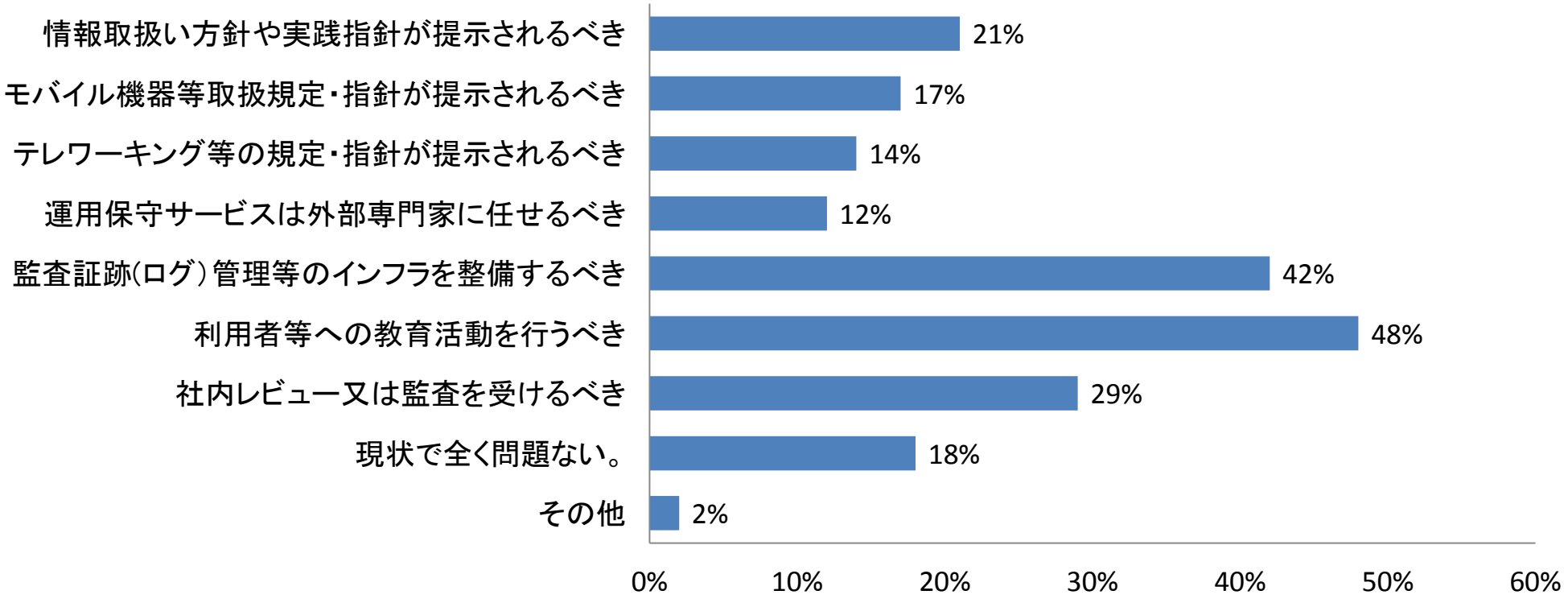
設問39.アクセス制御（情報・業務プログラム）管理策の活用



重要情報を扱うシステムの分離や情報取扱い手順確立は活用が多いが、テレワーキングの方針・運用は活用が低く、不採用が多い。

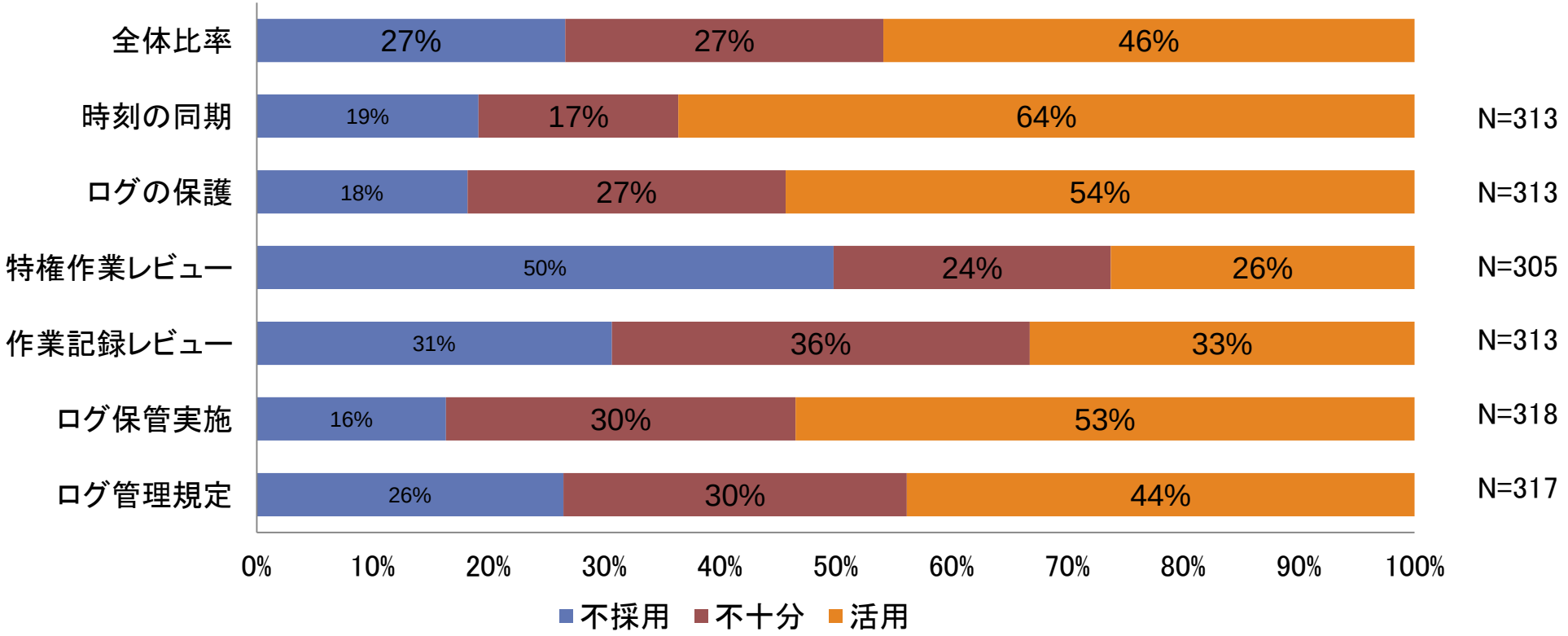
第5章　アクセス制御と証跡(ログ)管理

設問40.アクセス制御（情報・業務）管理策の強化方策（複数回答）（N=301）



利用者等への教育活動が多く、
監査証跡(ログ）管理等のインフラ整備が続いた。

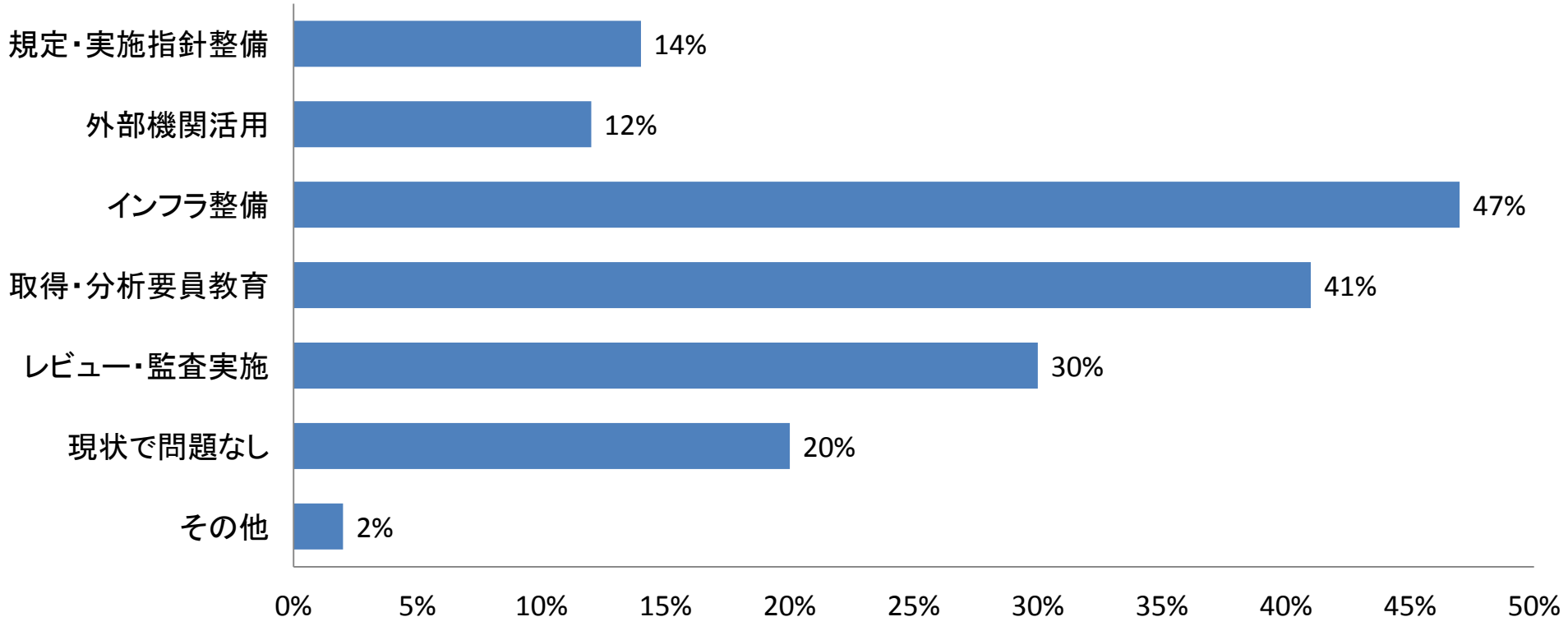
設問41.アクセス制御(ログ管理)管理策の活用



時刻の同期、ログの保護、保管実施は活用が多いが、特権作業および作業記録レビューが少ない。

第5章　アクセス制御と証跡(ログ)管理

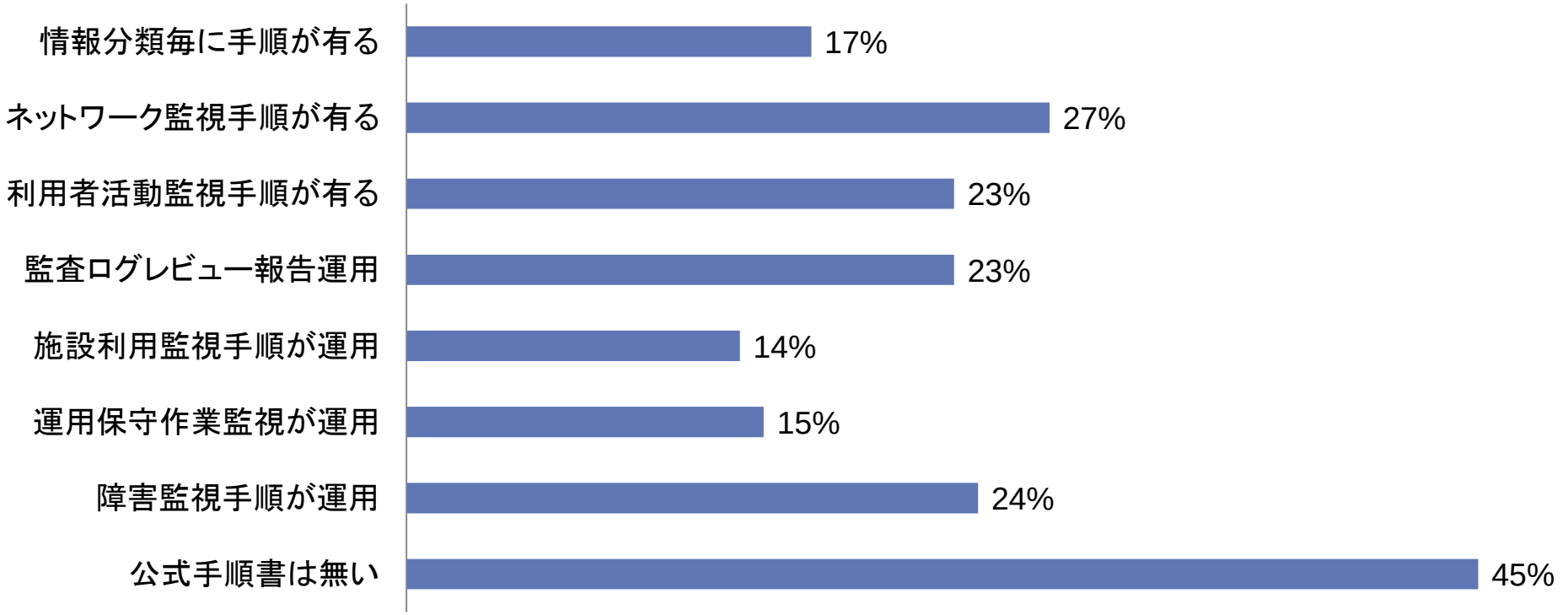
設問42.アクセス制御（ログ管理）管理策の強化方策（複数回答）（N=305）



インフラ整備が多く、取得・分析要員教育が続いた。

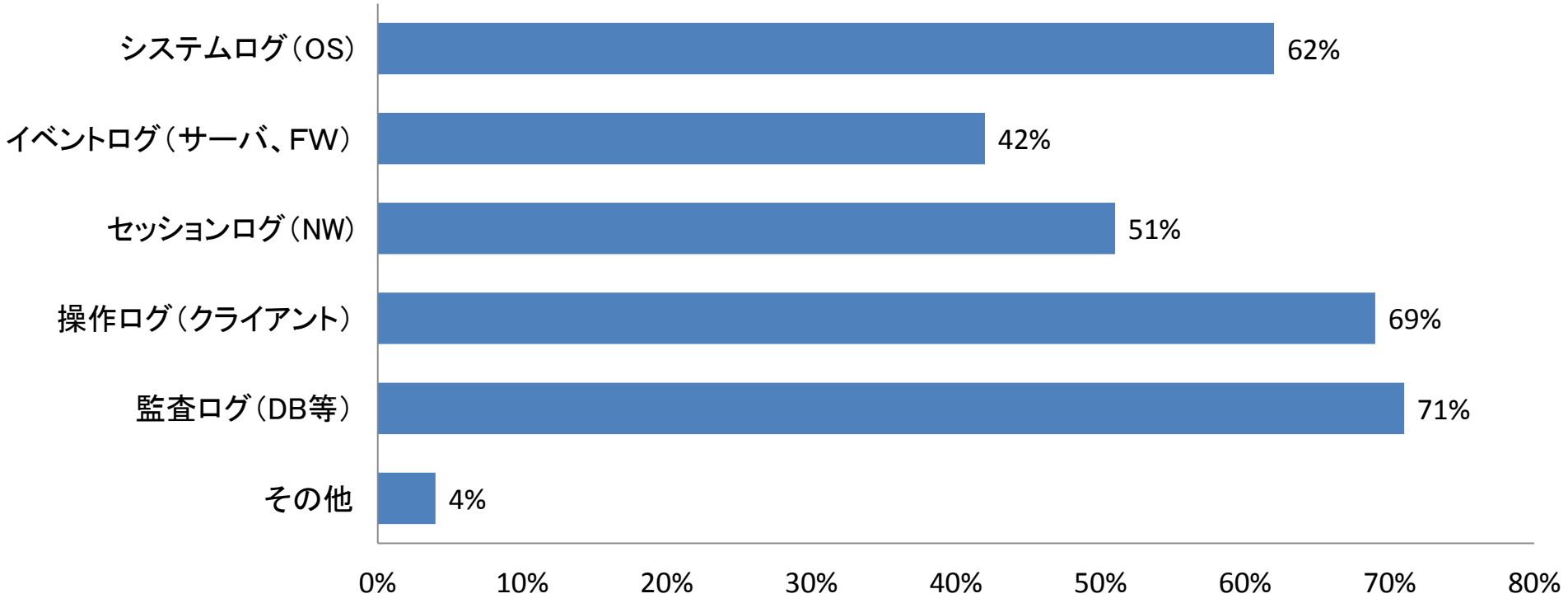
第5章　アクセス制御と証跡(ログ)管理

設問43.ログ管理手順書の作成・運用　（複数回答）（N=320）



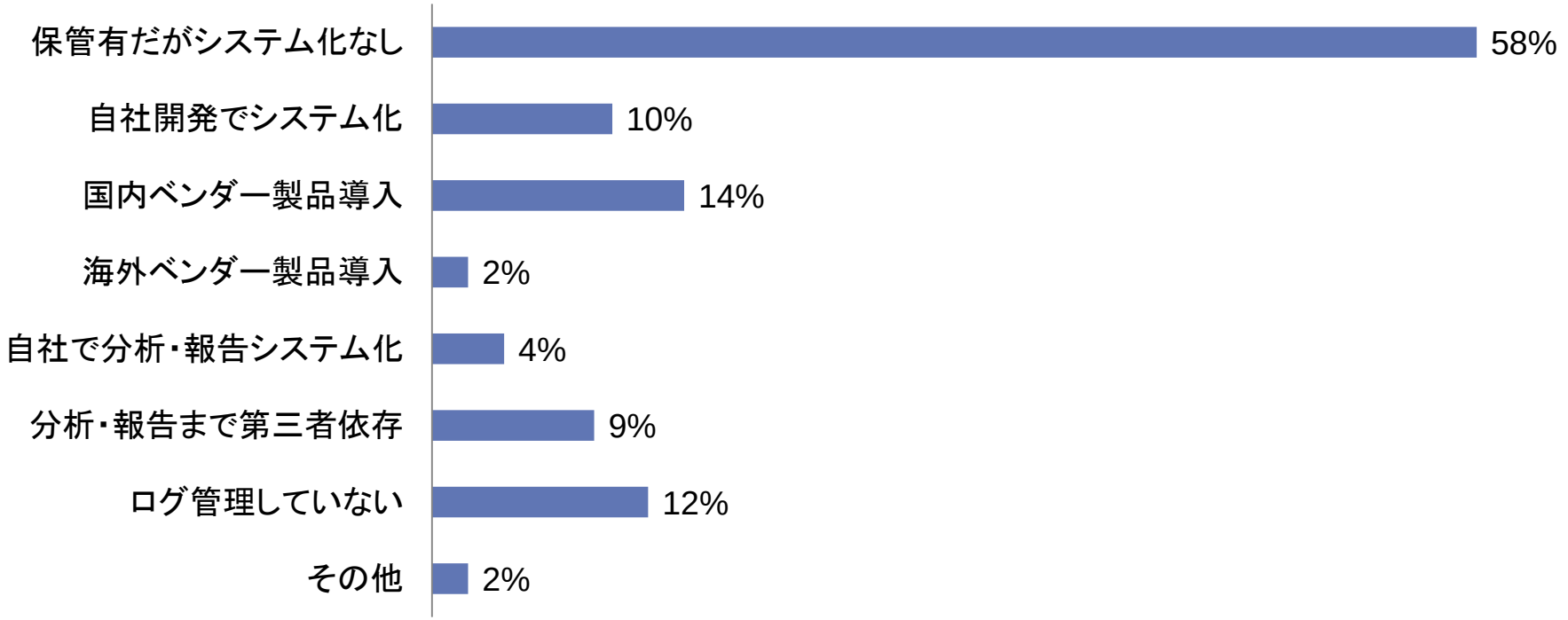
公式の手順書はない組織が45%と最も多い。
手順書のある組織は25%前後で、手順が運用されている組織は更に少ない。

設問44.取得・分析を行っているログ種類 （複数回答）（N=304）



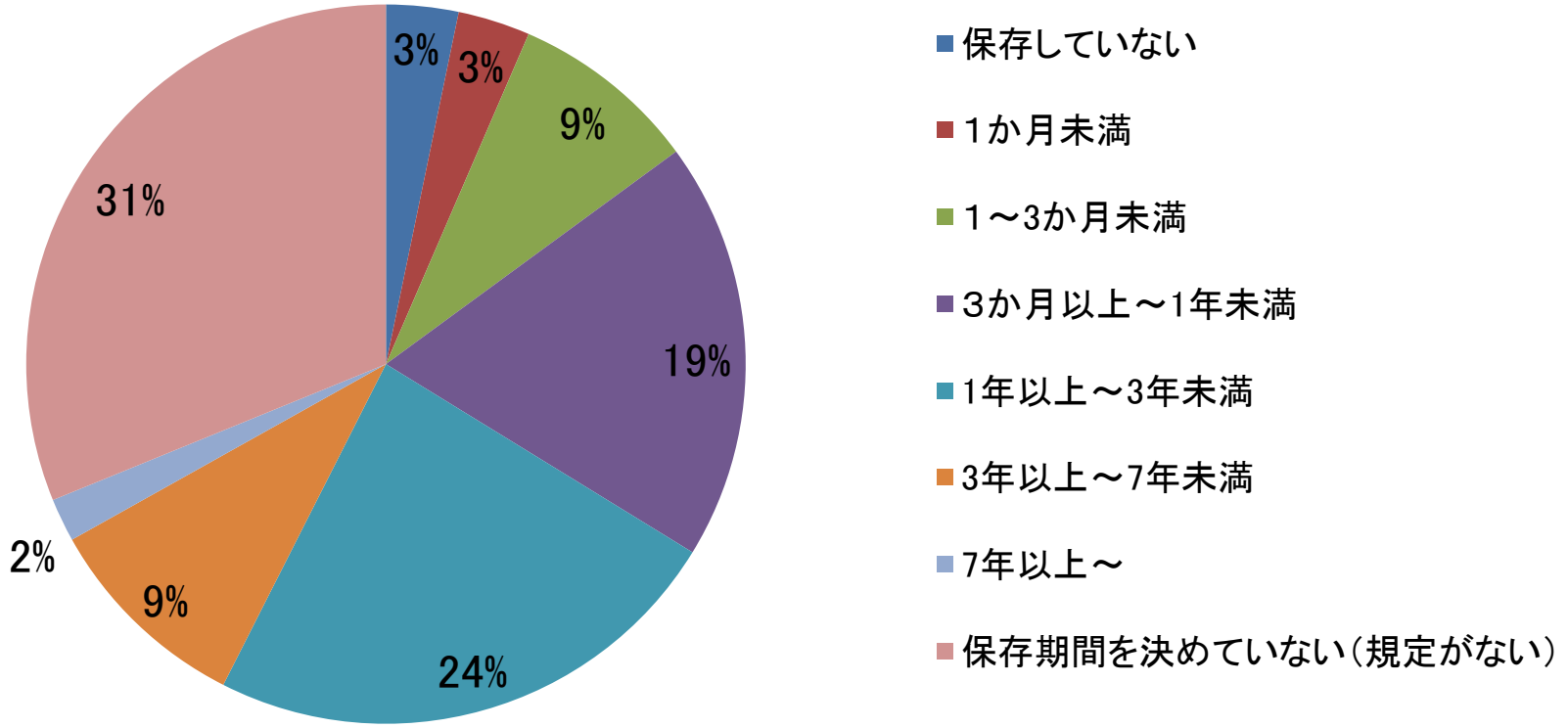
監査ログ、操作ログ、システムログの順で多く、イベントログは少ない。

設問45.ログ効率化の為の自動化ツール使用　（複数回答）（N=312）



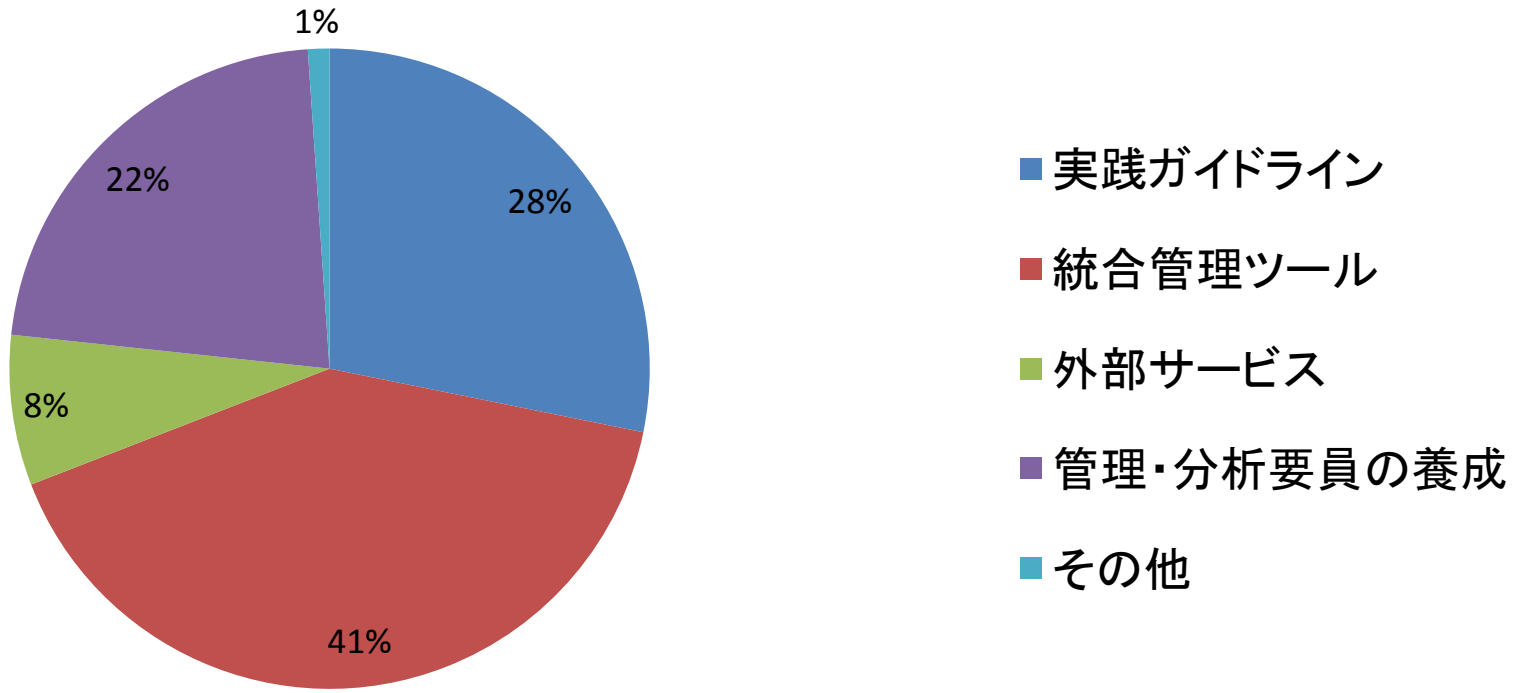
ログを保管しているが、システム化していない組織が58%と多く、
ログ管理していない組織も12%ある。

設問46.ログ保管期間の規定　（N=308）



ログ保管期間の規定が無いが31%、ログ保存していないが3%ある。
保管期間は1年から3年、3カ月以上1年未満が多い。

設問47.ログ管理を効率化するには何が必要か　（N=311）



統合管理ツールが41%、実践ガイドラインが28%、
管理・分析要員の養成が22%で続く。

考察（第5章 アクセス制御と証跡(ログ)管理）

- 過去3年間に情報セキュリティポリシーを見直した項目としては、アクセス制御、セキュリティ基本方針全般が多かった。見直しの理由としては、監査などの指摘事項対応が50%の組織で挙げられた。

- アクセス制御管理策の活用は、利用者管理(55%)、ネットワーク・OS(46%)、ログ管理(46%)、情報・モバイル活用(44%)の順で有った。

- 活用が出来ていない管理策として、管理者による定期的な利用者アクセス権レビュー(66 %)、OS特権ログオン制御(62%)、特権作業レビュー(74%)、作業記録レビュー(67%)が各組織で挙げられた。

- 管理策強化には、利用者管理、情報・業務管理では教育活動強化、他の分野ではインフラ整備、要員教育、レビュー・監査への要請が多かった。

- ログ管理については、ログの保護、保管実施は活用が多いが、特権作業および作業記録のレビューが少ない。管理策としてのログ保管手順書が無いが45%、保管はしているがシステム化なしが58%あり、保管後のログの取り扱いに苦慮している組織が多いと考えられる。

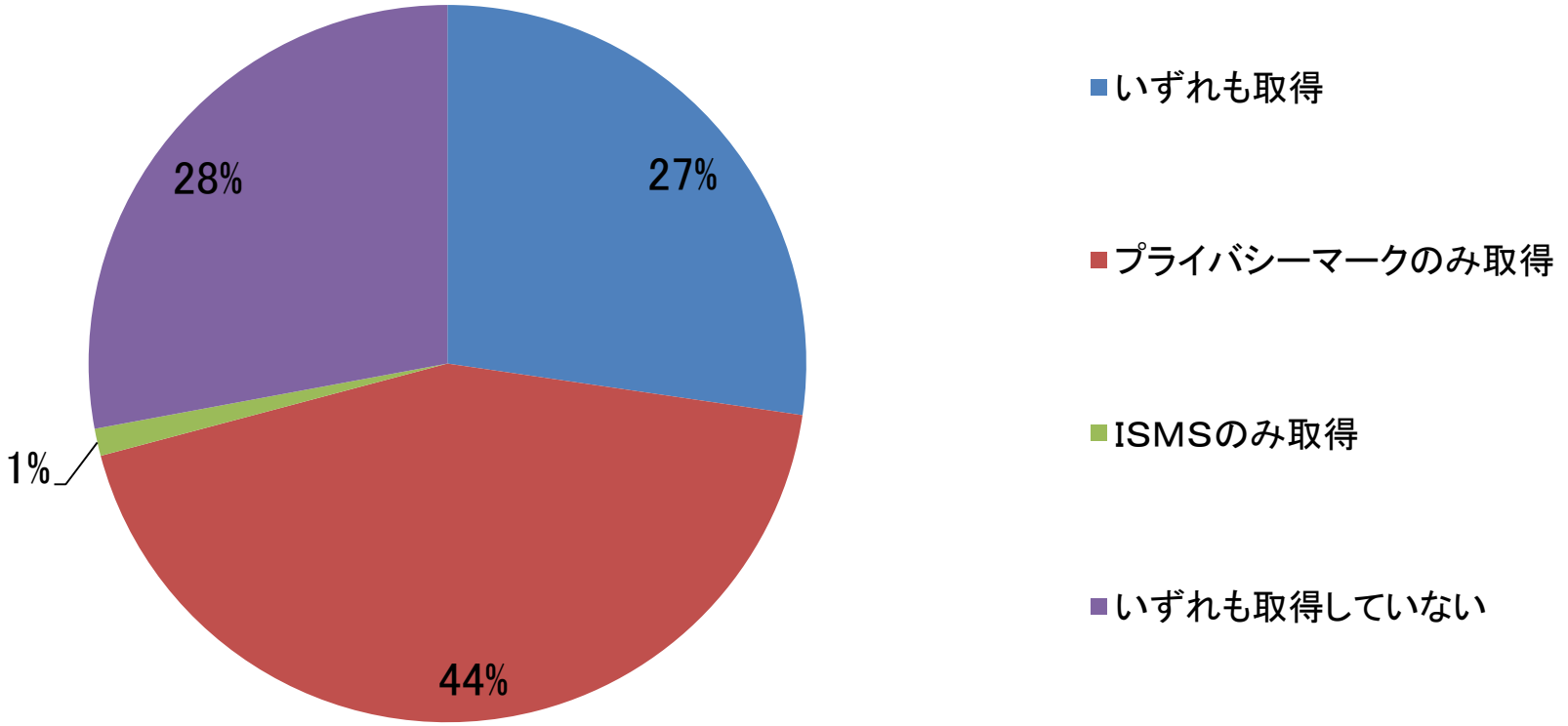
- ログ管理を効率化するには、統合ログ管理ツールとその活用ノウハウへの期待が41%であった。保管期間は1年から3年が24%、3カ月以上1年未満が19%の順である。

第6章

個人情報漏えい事故のお詫び金について

第6章　個人情報漏えい事故のお詫び金について

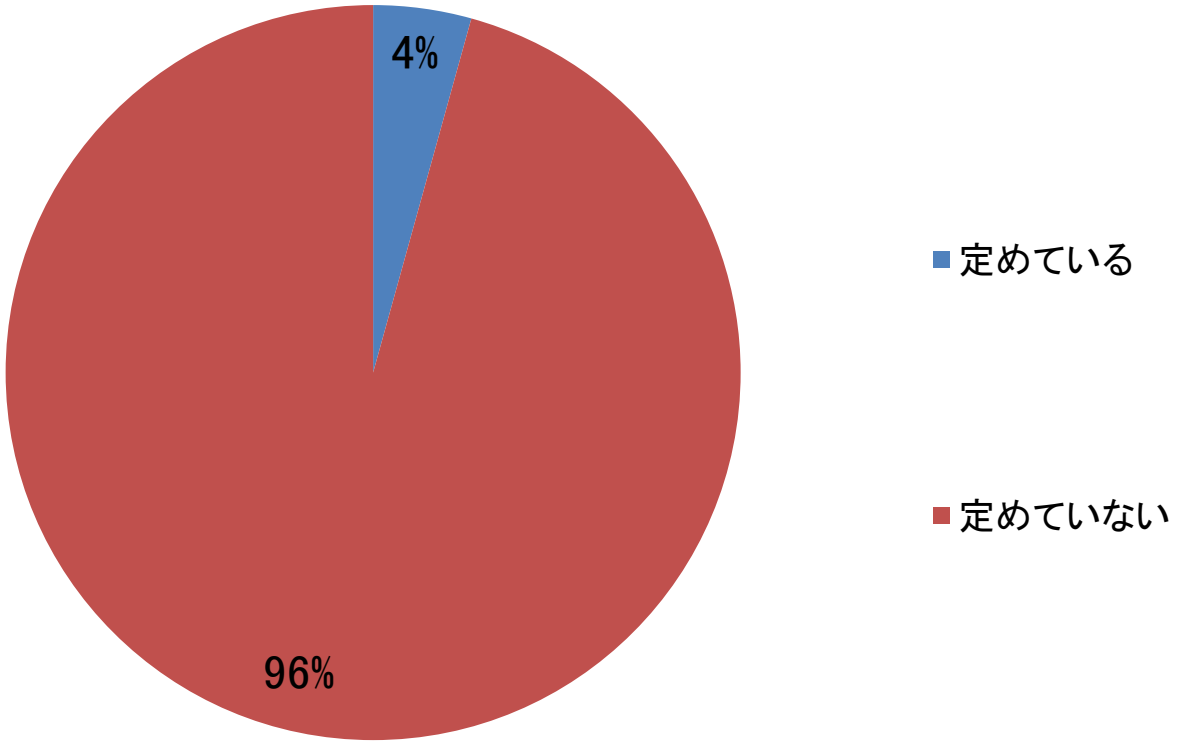
設問48.プライバシーマークまたはISMSを取得していますか。
（N=326）



プライバシーマークを取得している組織は約7割。

第6章　個人情報漏えい事故のお詫び金について

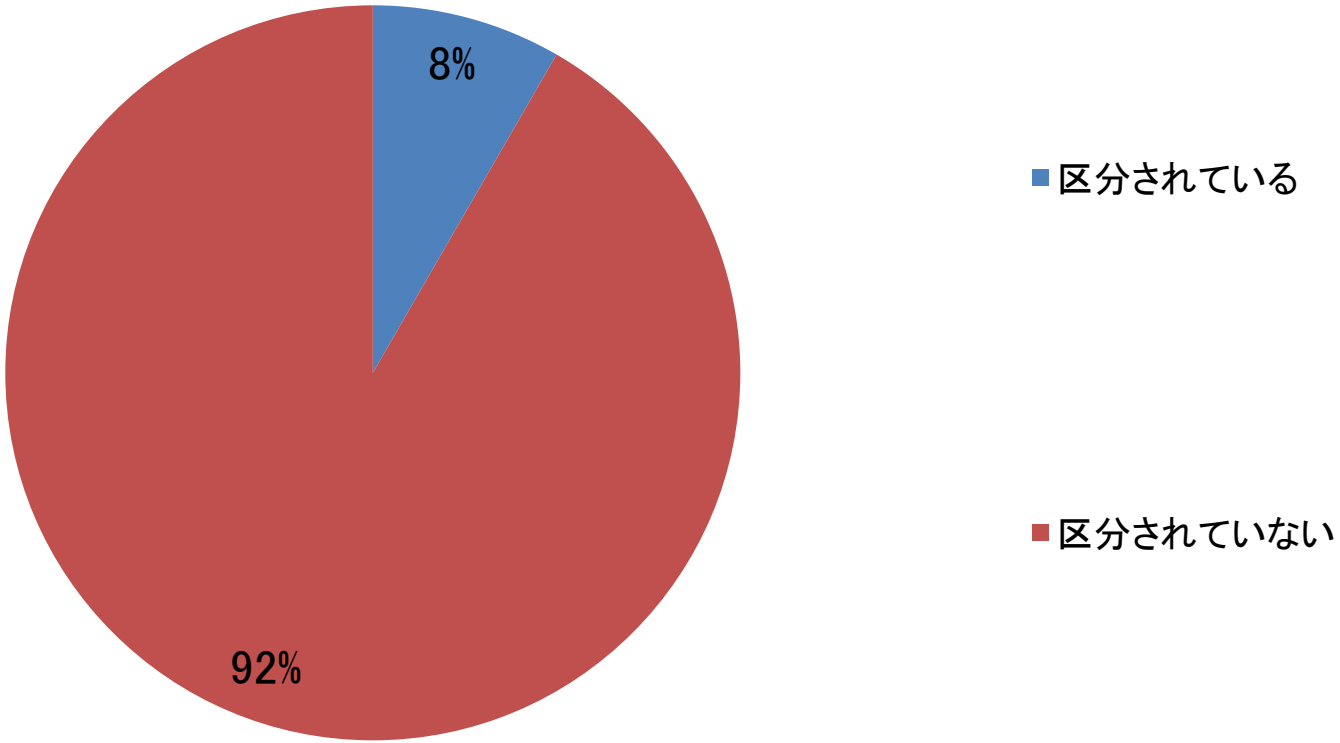
設問49.個人情報漏えい事故のお詫び金についての基準を事前に定めていますか。（N=325）



ほとんどの組織では、事前に基準を定めていない。

第6章　個人情報漏えい事故のお詫び金について

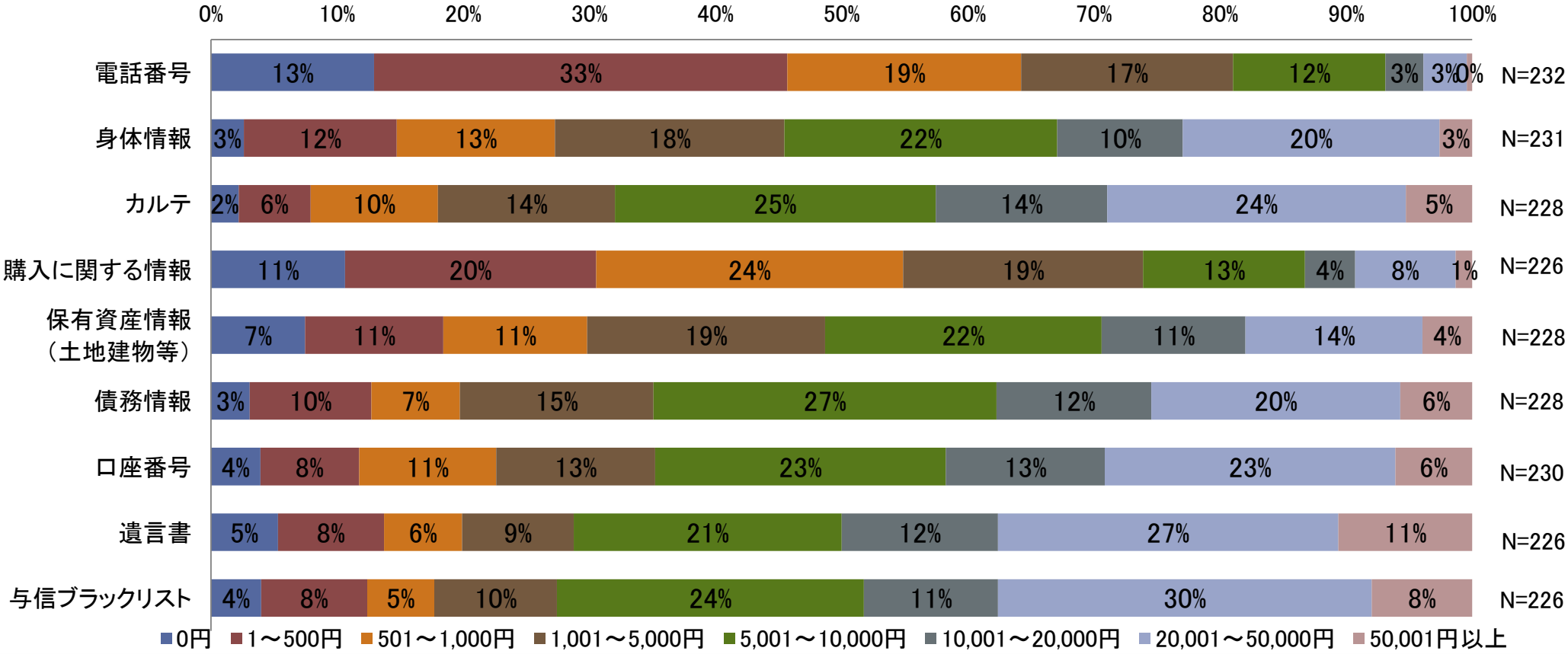
設問50.個人情報の種類（レベル）によって、お詫び金支払額が区分されていますか。（N=60）



8%の組織は個人情報の種類（レベル）で支払額を区分している。

第6章　個人情報漏えい事故のお詫び金について

設問51.個人情報が漏えいした場合、1名あたりに支払うべきお詫び金支払額はいくらが妥当であると考えますか。



「遺言書」、「与信ブラックリスト」漏えい時の想定支払額が特に高い。

考察（第6章　個人情報漏えい事故のお詫び金について）

- 個人情報漏えい事故が発生した場合を想定したお詫び金支払額について、事前に基準を定めている組織は少ない。

- 事前に基準を定めている組織のうち8%では、個人情報の種別毎にお詫び金支払額を区分している。

- 「電話番号」や「購入に関する情報」といった基本的な個人情報は1000円以内のお詫び金支払額を想定している。

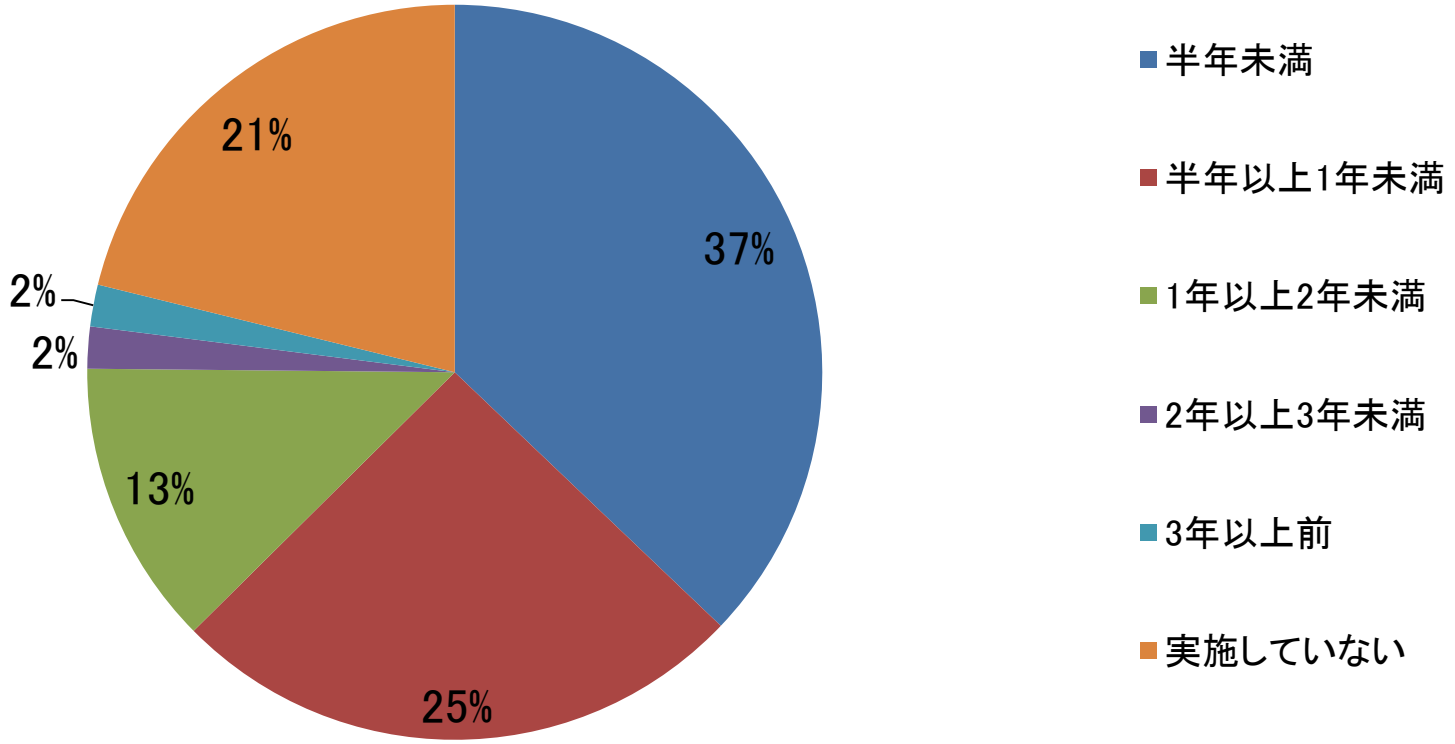
- 金銭的・精神的被害に結びつきやすい個人情報が漏えいした場合のお詫び金支払額が高く想定されている。

第7章

リスク分析の実施状況について

第7章　リスク分析の実施状況について

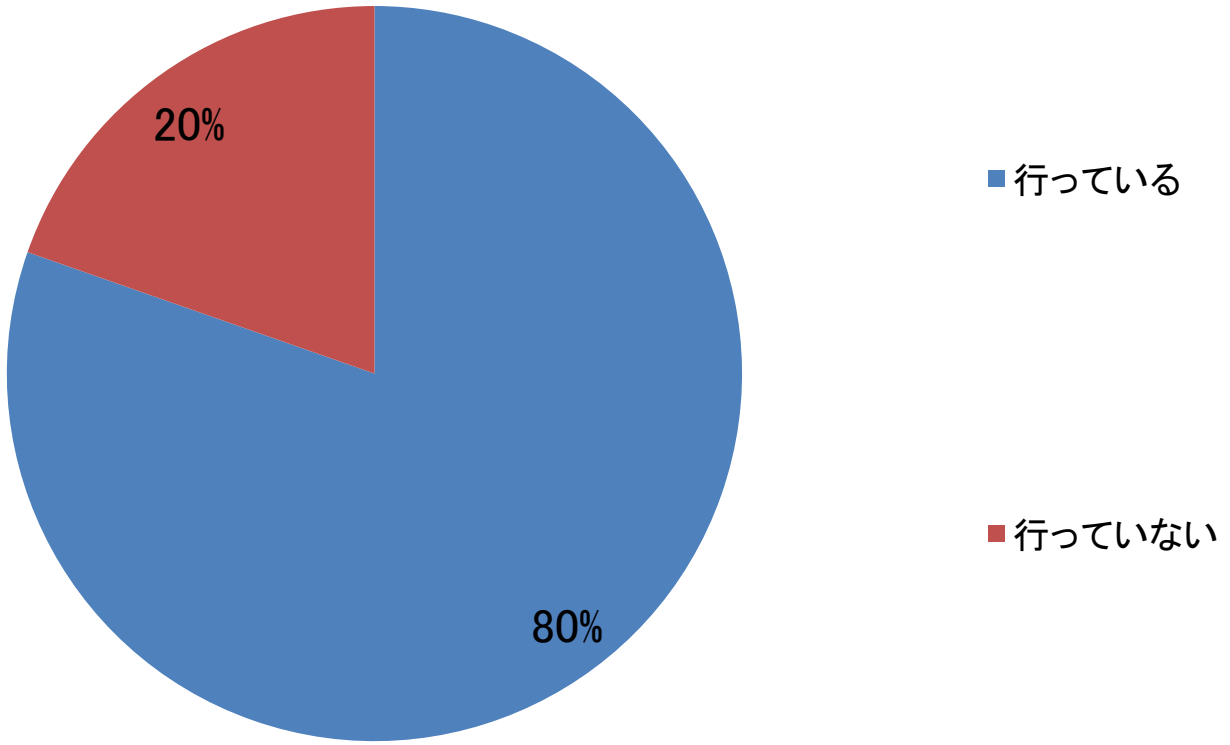
設問52.情報セキュリティに関するリスク分析を最後に実施したのはいつですか。（N=326）



6割以上の組織が1年以内に実施している一方、約2割は実施していない。

第7章　リスク分析の実施状況について

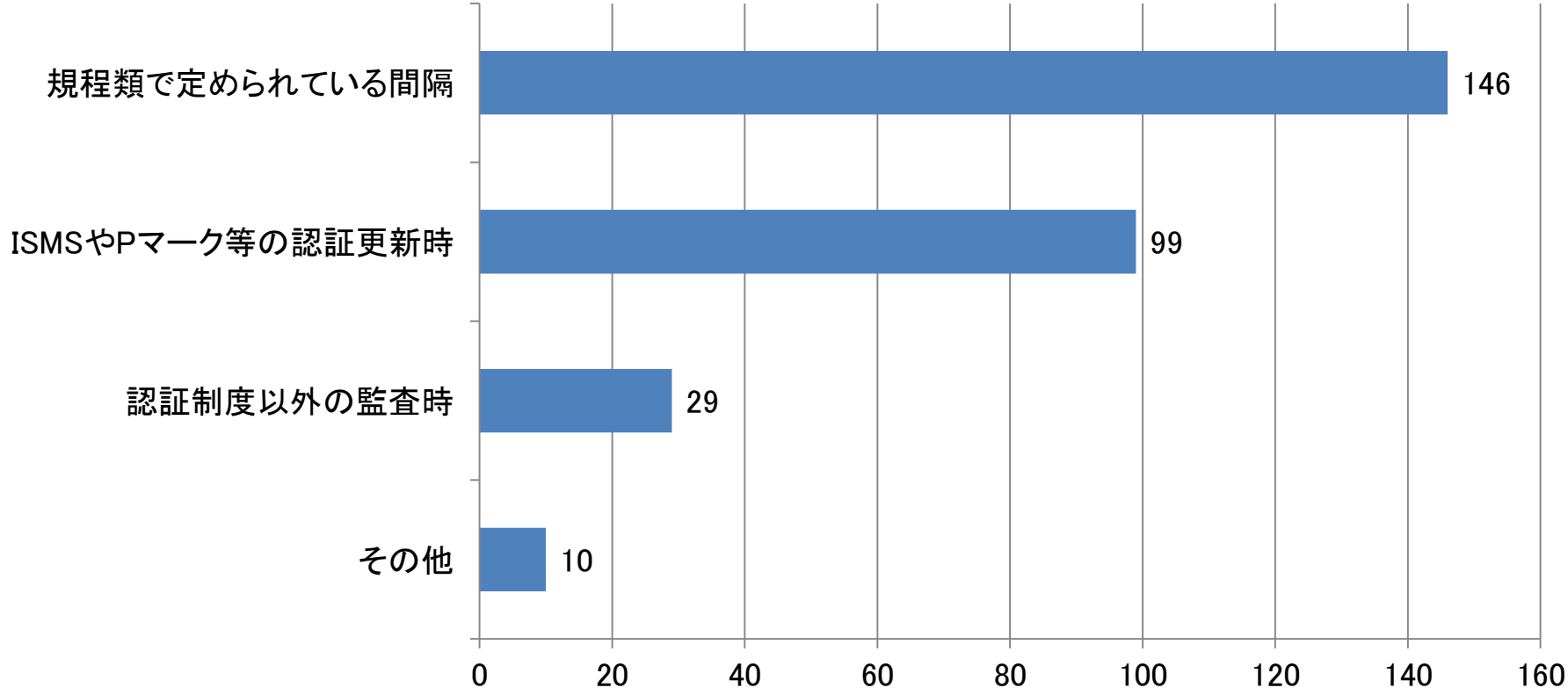
設問53.情報セキュリティに関するリスク分析を定期的に行っていますか。(N=280)



8割の組織が定期的に実施している。

第7章　リスク分析の実施状況について

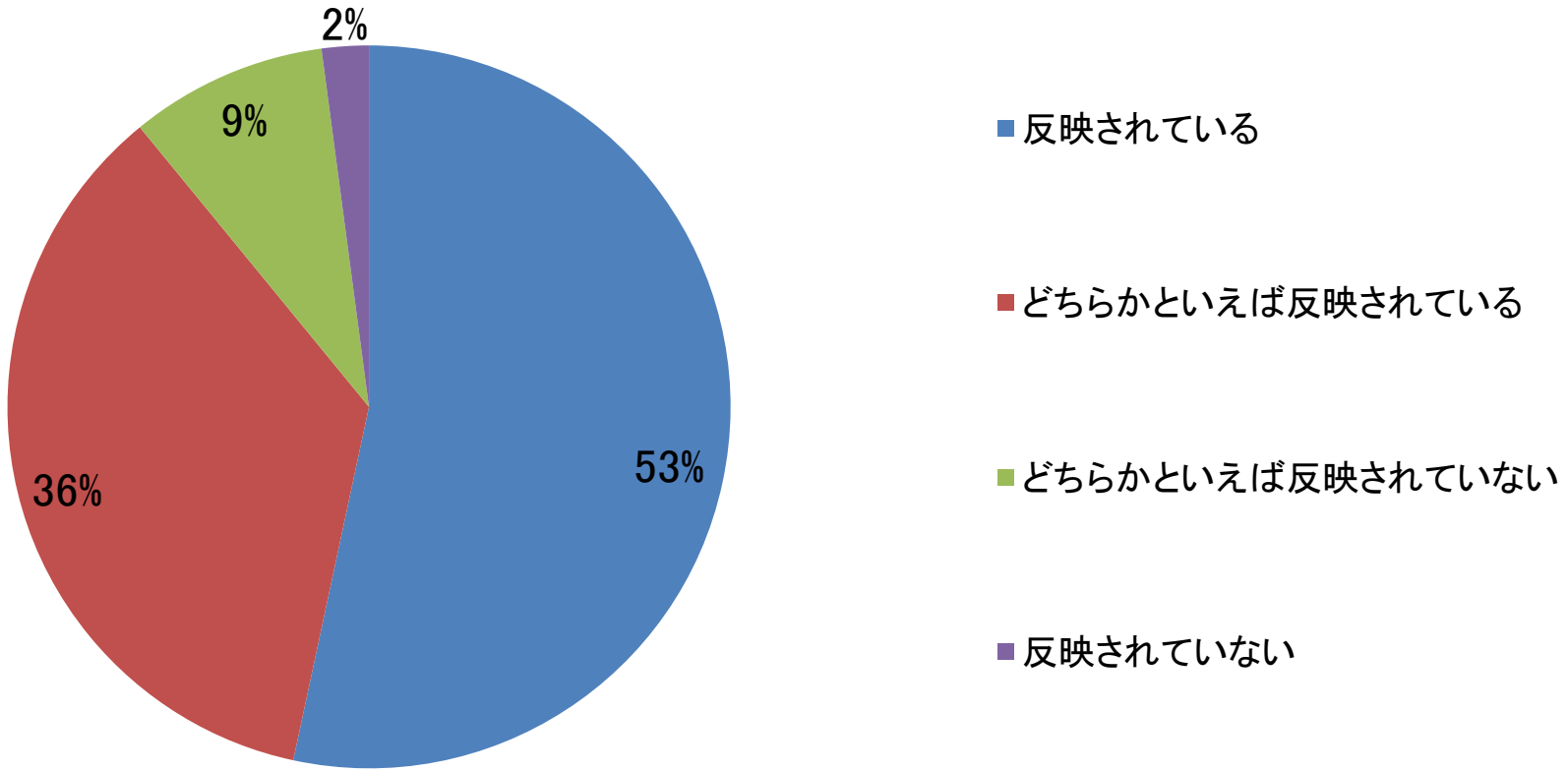
設問54.定期的な情報セキュリティに関するリスク分析を行うタイミングとしてあてはまるのはどれですか。(複数回答)(N=225)



規程類で定められた間隔や認証更新時に実施する組織が多い。

第7章　リスク分析の実施状況について

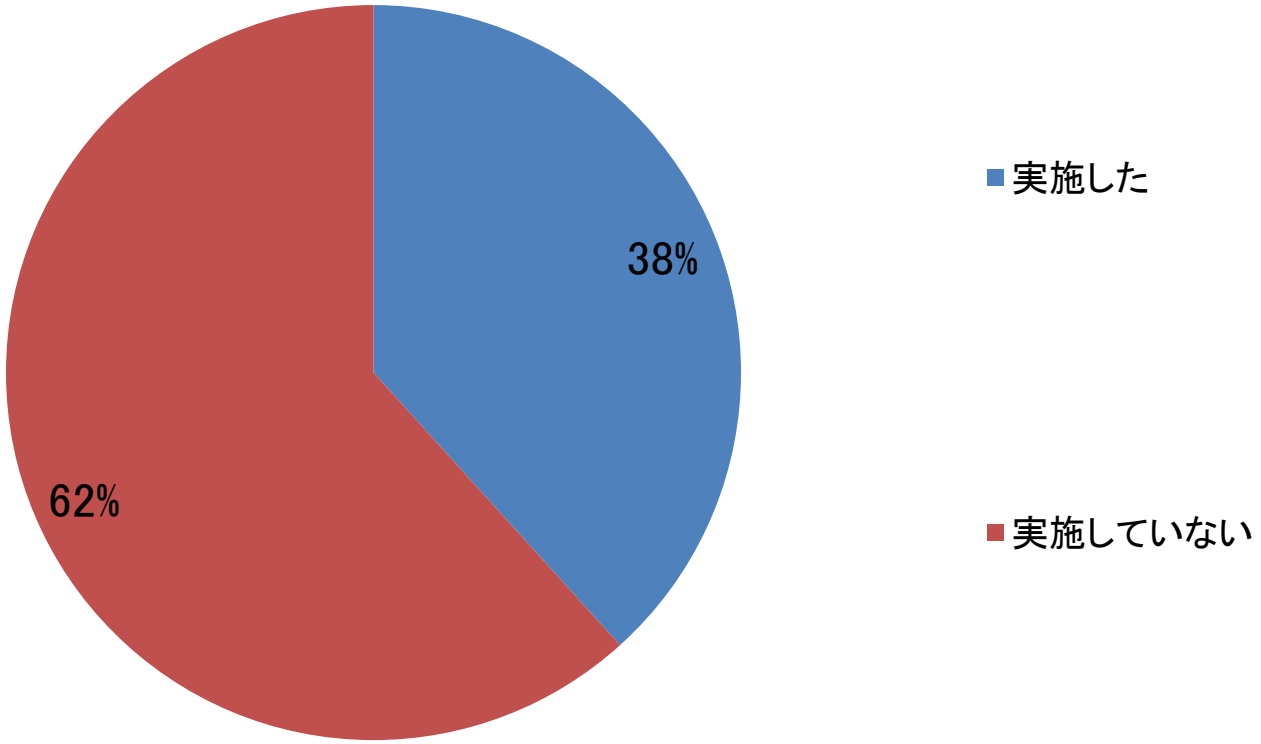
設問55.定期的な情報セキュリティに関するリスク分析の結果は、実際のセキュリティ対策に反映されていますか。（N=225）



9割近くの組織は実際のセキュリティ対策に反映している。

第7章　リスク分析の実施状況について

設問56.2年以内(2010年4月～2012年3月)に定期的でない(非定期的な)情報セキュリティに関するリスク分析を実施しましたか。(N=282)

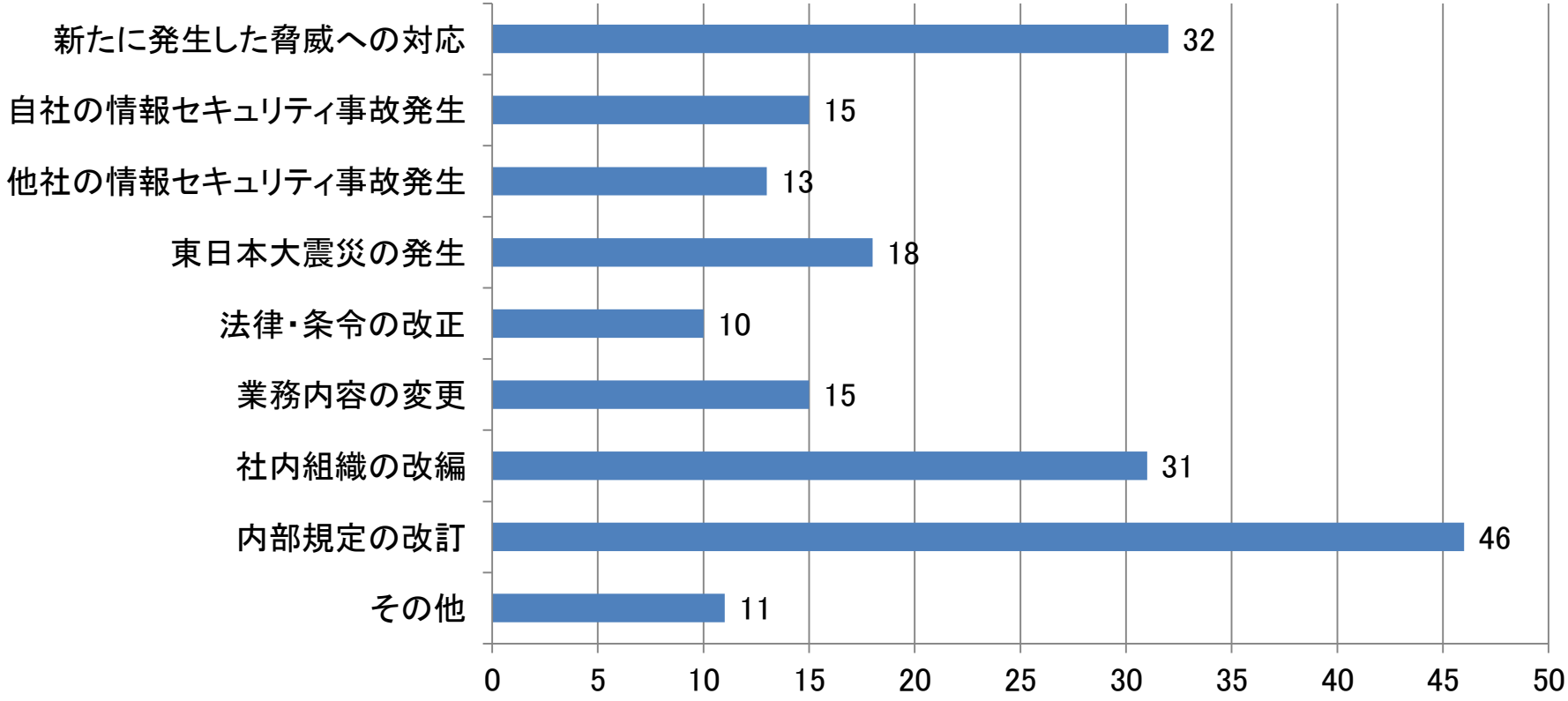


非定期的なリスク分析を実施している組織は4割未満。

第7章　リスク分析の実施状況について

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

設問57.非定期的に情報セキュリティに関するリスク分析を実施した理由としてあてはまるのはどれですか。(複数回答)(N=108)

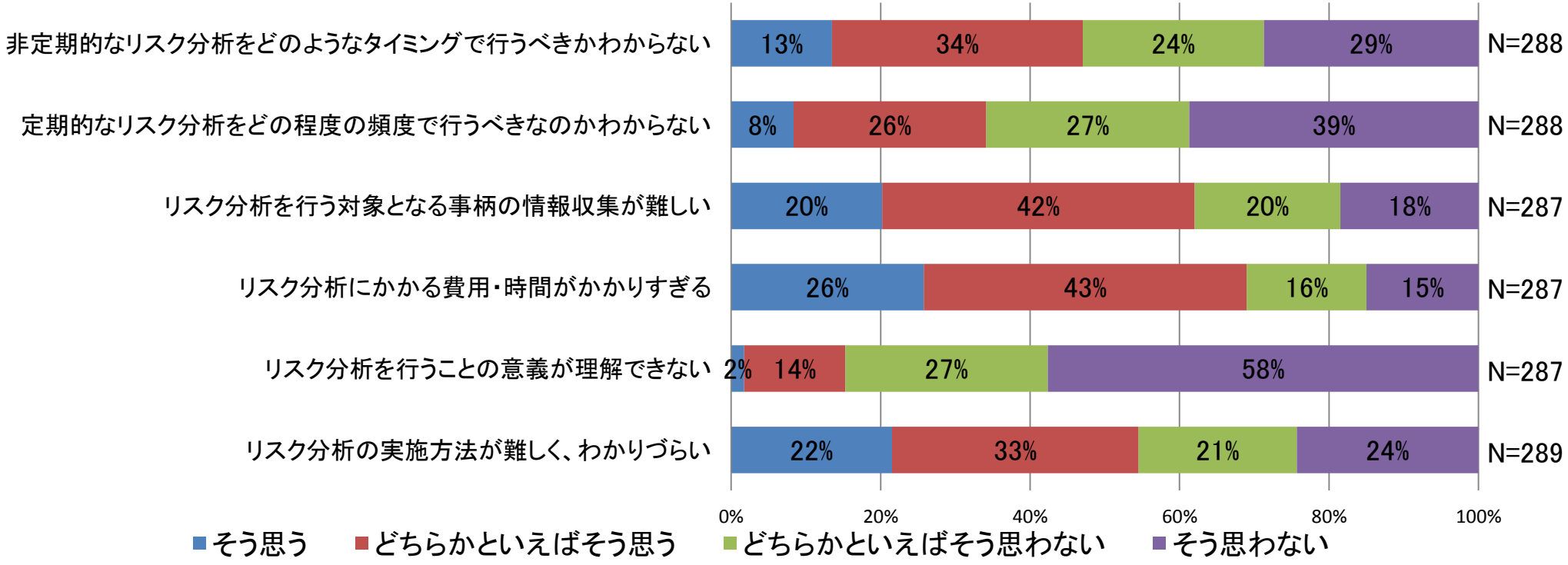


社内規定・組織変更の他、新たな脅威への対応も多く挙げられている。

第7章　リスク分析の実施状況について

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

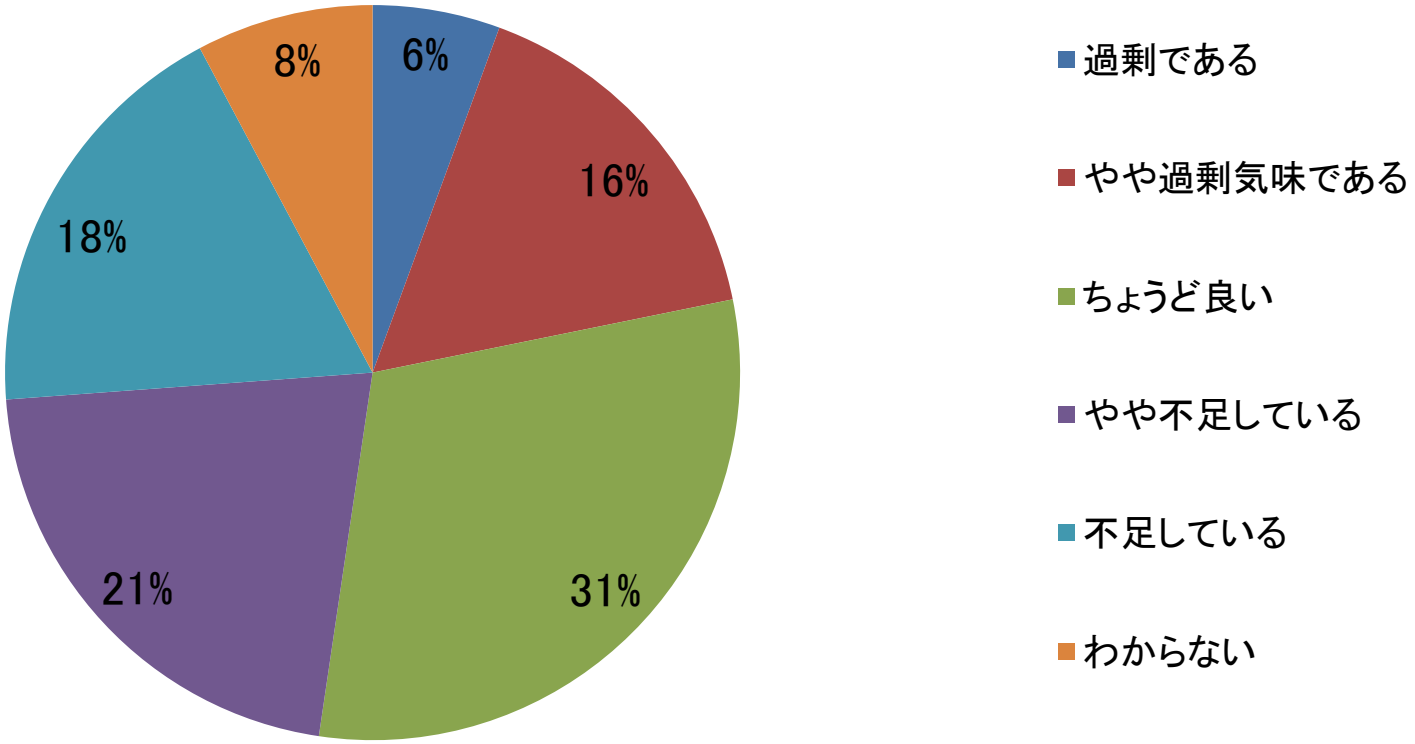
設問58.リスク分析を行わない理由、またはリスク分析を行う際の問題点



リスク分析の意義は理解されているが、
情報収集、実施方法、費用・時間などに問題がある。

第7章　リスク分析の実施状況について

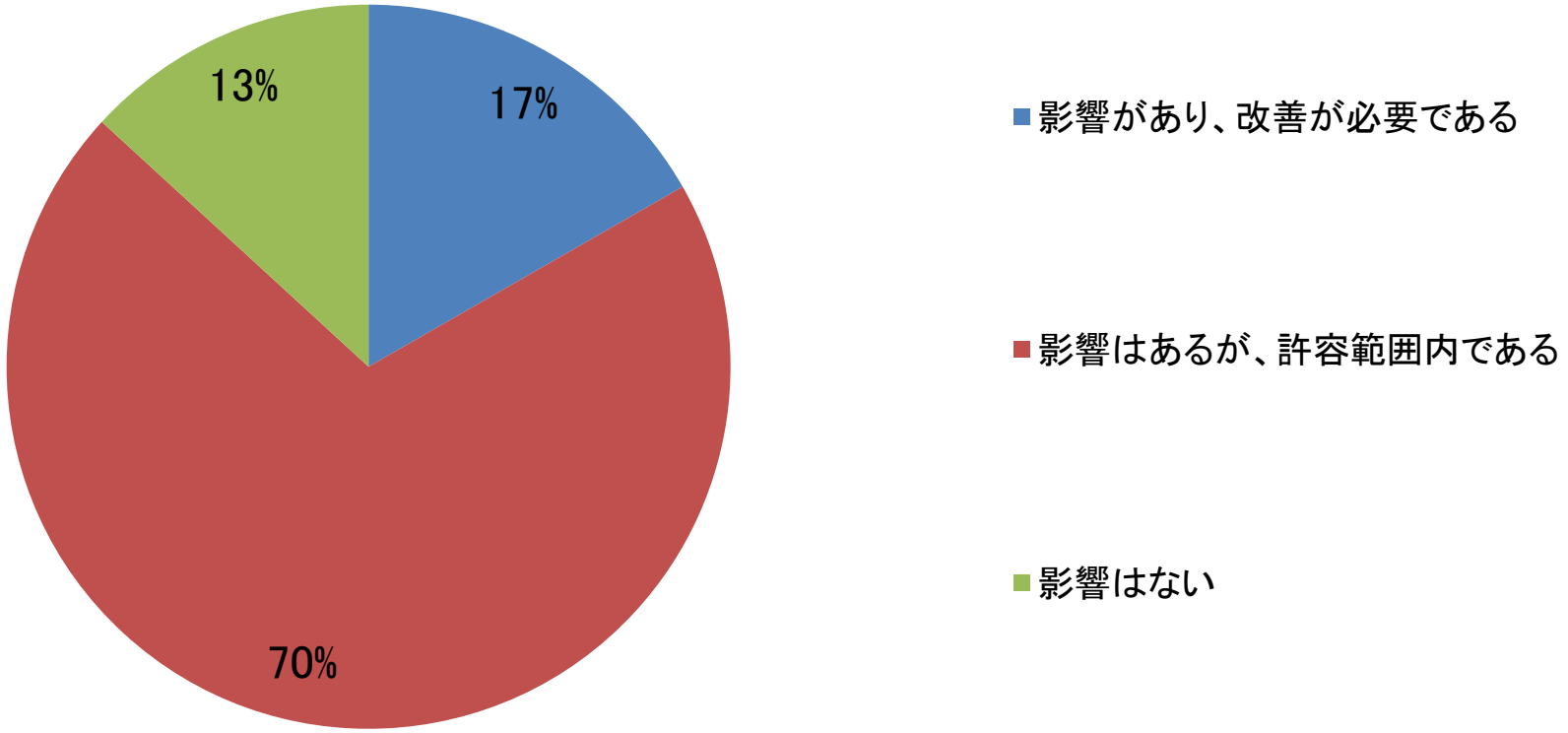
設問59.情報セキュリティリスクに対する管理策の内容についてあてはまるのはどれですか。(N=321)



39%の組織が不足と感じている一方、22%の組織が過剰であると感じている。

第7章　リスク分析の実施状況について

設問60.情報セキュリティリスクに対する管理策の実業務への影響についてあてはまるのはどれですか。(N=311)



影響を感じているものの、許容範囲であると考える組織が大半である。

考察（第7章　リスク分析の実施状況について）

- 8割の組織が、規程類や監査対応などにより定期的なリスク分析を実施しており、その結果を実際に管理策へ反映している組織が9割近くあり、定期的なリスク分析の実施は定着していると考えられる。

- 規定類や監査などに依らない非定期的なリスク分析を行っている組織は4割弱にとどまっている。実施理由は、組織や規程類の変更などに合わせた必然性の高いものが中心であるが、新たな脅威への対応など、社会情勢に合わせて実施する組織も見られた。

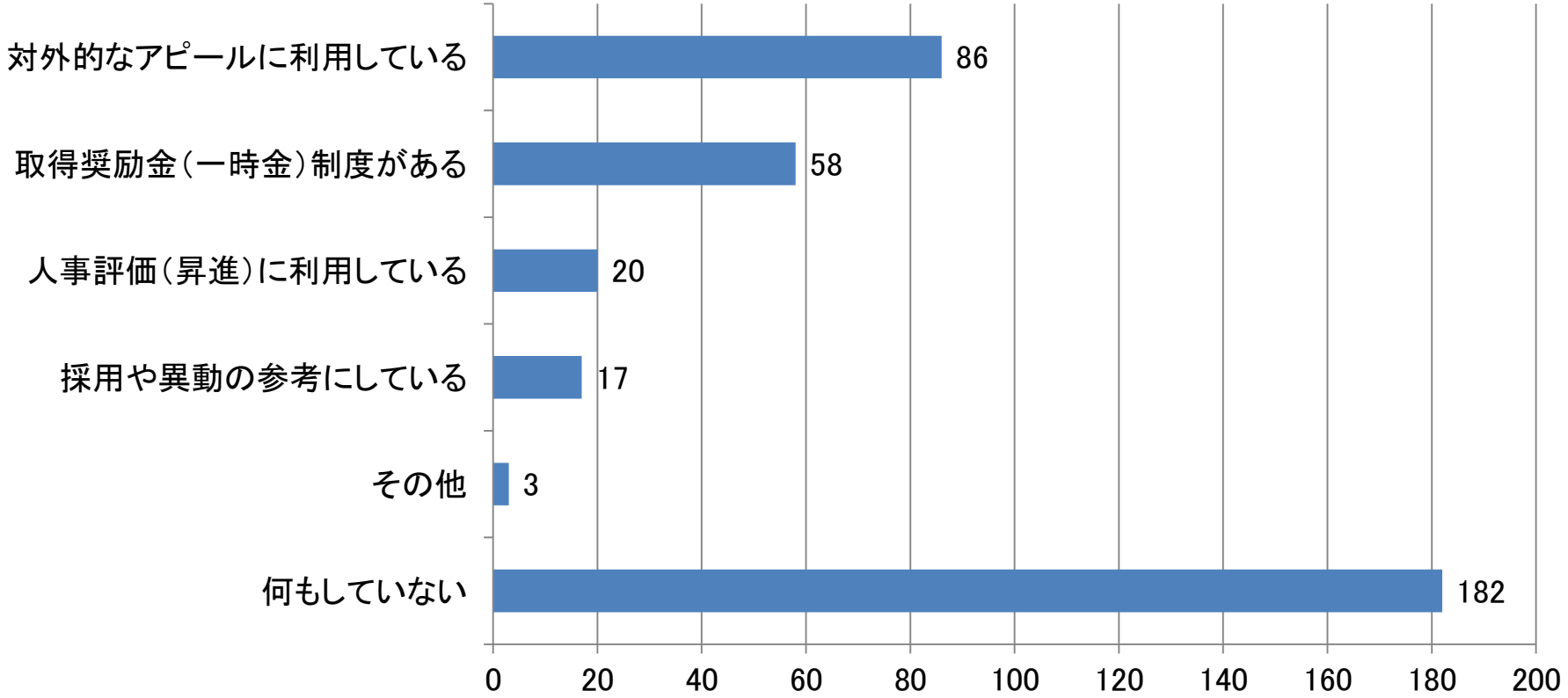
- リスク分析の意義は理解されているが、時間・費用などの問題が解決されておらず、情報収集や実施方法が確立されていないのが現状であると考えられる。

- 管理策の実業務への影響は概ね理解されていると言えるが、約4割の組織が管理策の内容が不十分であると感じているのも現状であり、両者のバランスが課題であると考えられる。

第8章

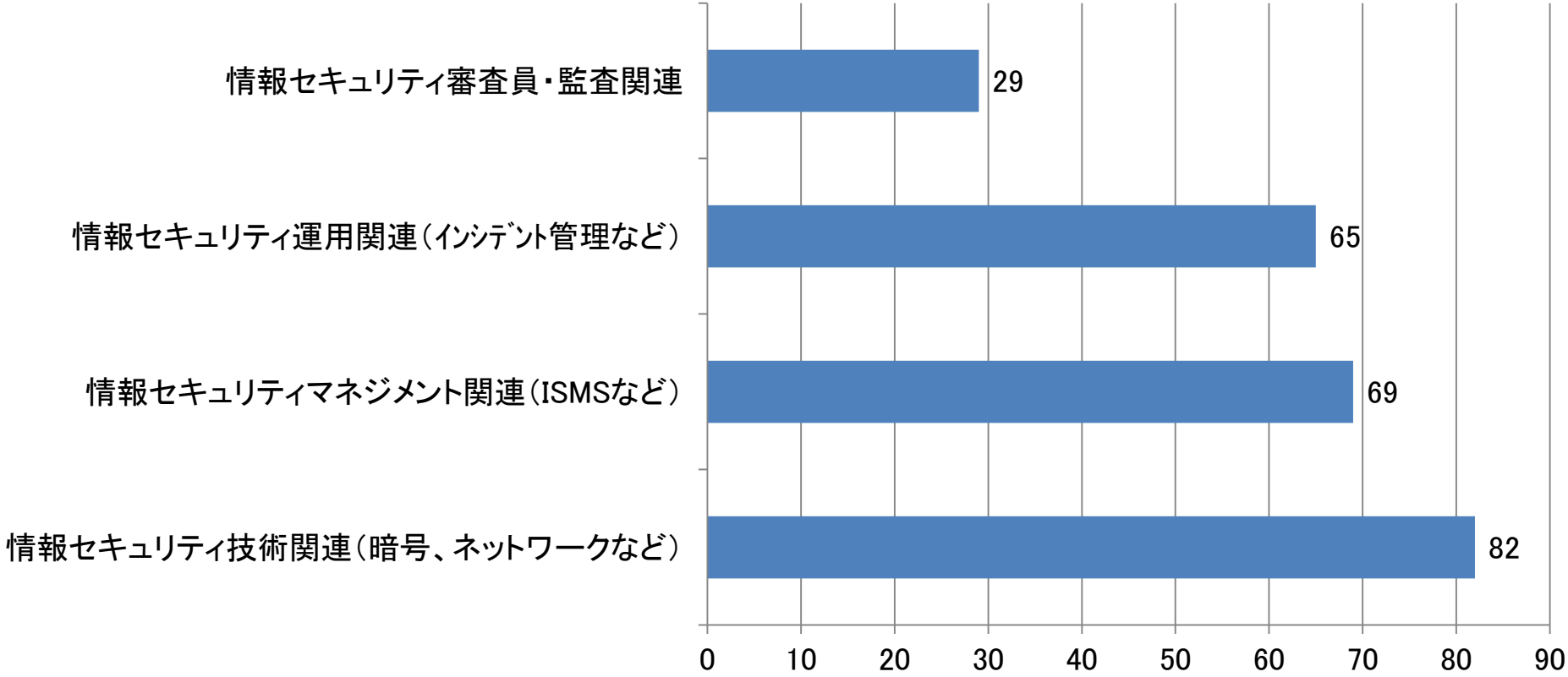
その他

設問61.貴社の情報セキュリティ関連の資格の活用について教えてください。（複数回答）（N=319）



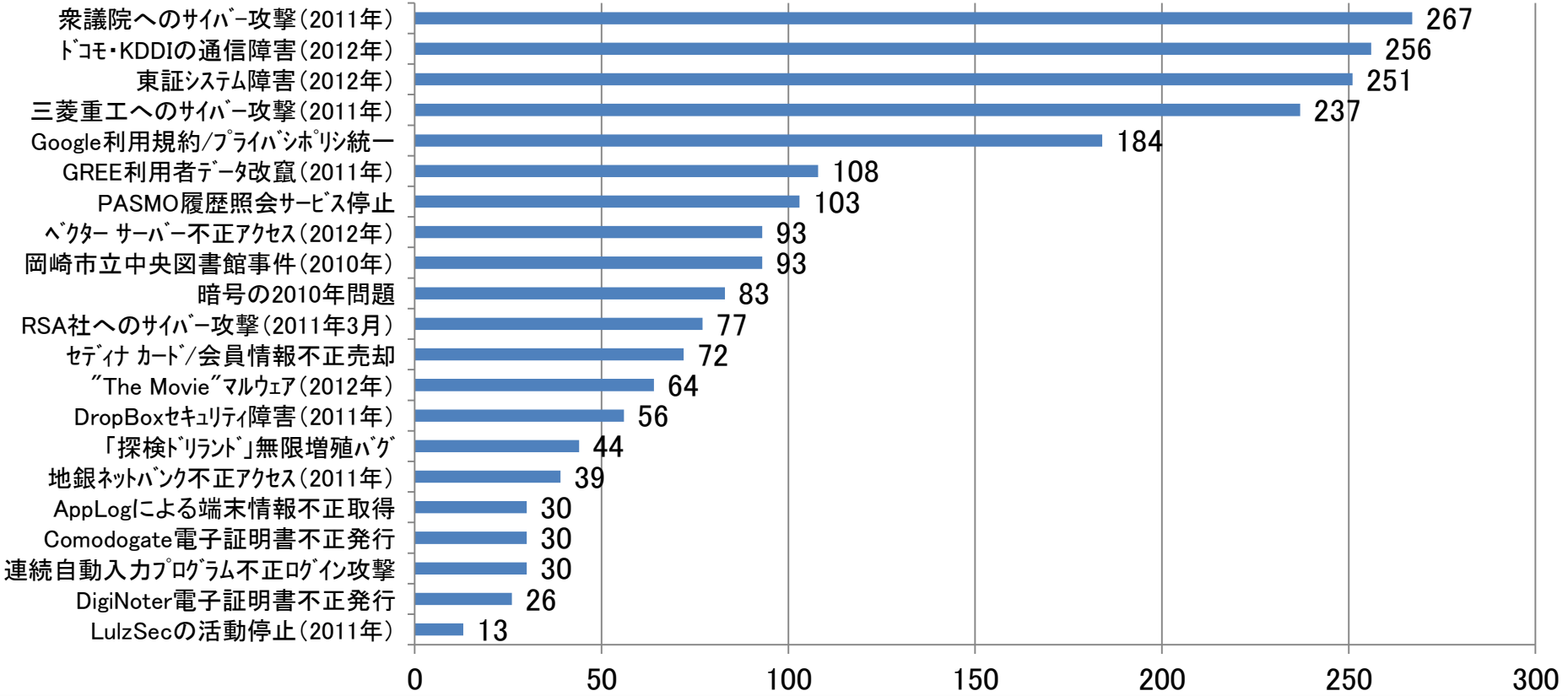
あまり活用されていないのが現状である。

設問62.貴社の今後必要と思われる情報セキュリティ関連の資格はなんですか。（複数回答）（N=152）



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。

設問63.次の出来事について、ご存知なものをご選択ください。（複数回答）（N=320）

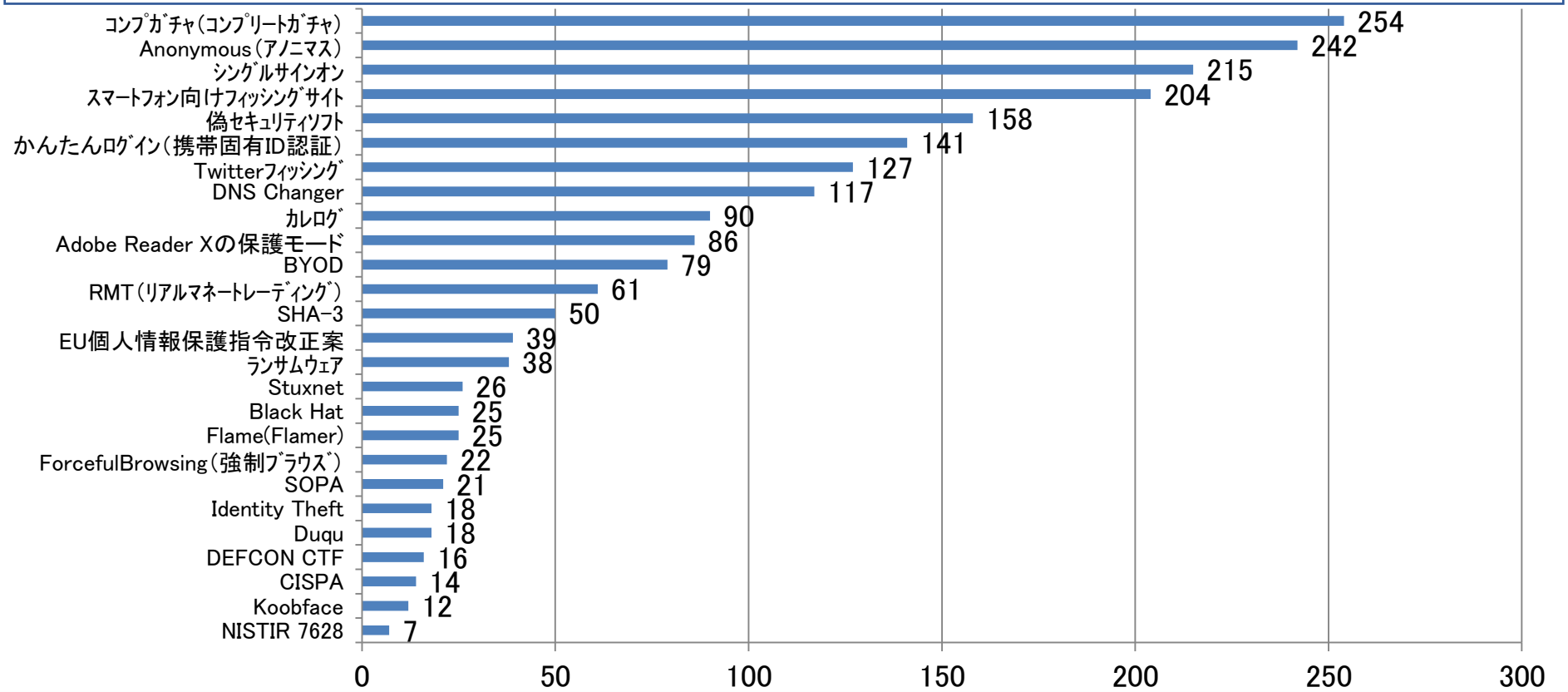


日本のテレビ・新聞で大きく報道された出来事の認知度が高い傾向にある。

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64.次の用語ついて、ご存知なものをご選択ください。（複数回答）（N=317）



日本のマスメディアで取り上げられにくい用語の認知度が低い傾向にある。

考察（第8章　その他）

- 情報セキュリティ関連の資格の活用は、「何もしていない」、「対外的なアピールに利用」が多く、従業員が資格を取得することへの直接的なインセンティブを設けている組織は多くない。

- 技術・マネジメント関連など、組織の実務に必要な資格への関心は高いが、情報セキュリティ監査関連資格への関心は低い。

- アンケート直近の6月に悪用された電子証明書を失効させる更新プログラムがMicrosoftよりリリースされたにもかかわらず、DigiNoterやComodogateの電子証明書不正発行の件(※)についての認知度が低い（10%未満）。

  ※昨年度、当該の電子証明書を失効させる更新プログラムがMicrosoftよりリリースされている。

- 「Anonymous」の高い認知度（76%）の一方で、「SOPA」や「CISPA」、「LulzSecの活動停止」については認知度が低い（10%未満）。また、「標的型攻撃」に対する高い認知度（66%、設問23参照）の一方で、「Stuxnet」や「Duqu」、「Flame」についての認知度が低い（10%未満）。こうした傾向から、総称的なキーワードは呼称として浸透した一方で、その具体的な内容については深く理解されていないと考えられる。