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

2017年情報セキュリティアンケート調査結果

2017年12月30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

  2017年7月22日～10月31日
  （2010年より毎年実施　8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，官公庁，教育機関（以下「組織」という）など

- 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，

  個人情報保護法の改正影響，情報セキュリティガバナンス体制，Webアプリケーションセキュリティ管理の状況，人工知能技術，緊急時対応の実効性，情報セキュリティ人材に関して調査　他

- 調査方法：郵送による
- 回答状況：429件（送付総数に対して9.1%）

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　個人情報保護法の改正による影響
4章　情報セキュリティガバナンス体制
5章　Webアプリケーションセキュリティ管理の状況
6章　組織における人工知能(AI)技術の導入
7章　緊急時対応の実効性
8章　情報セキュリティ人材に関する状況
9章　その他　過去の事例・事故・用語の認知度

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）

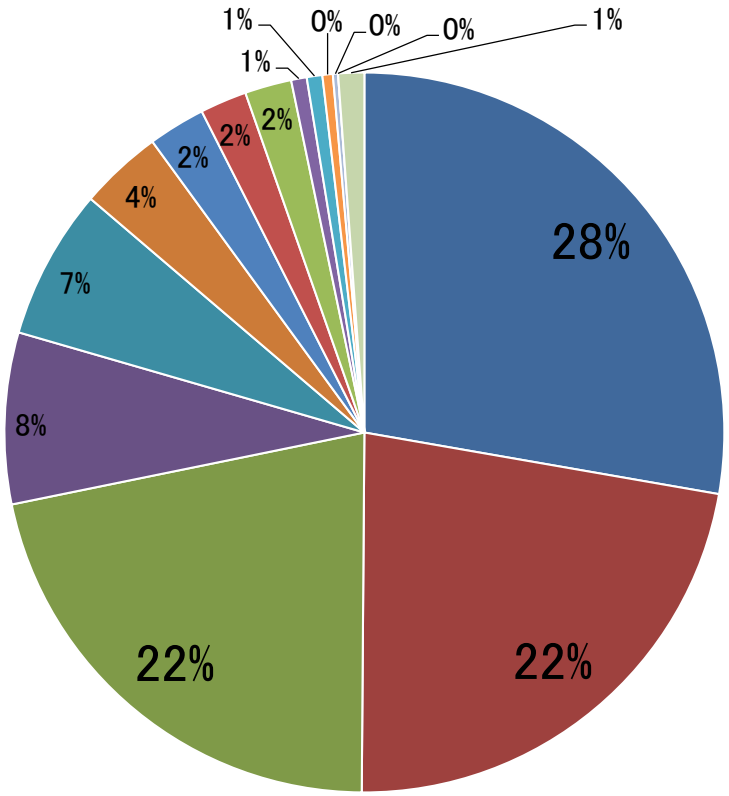
調査結果：

- 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
  - 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22%と最も多い
  - 従業員数50人以下の組織が28%と最も多い
  - また，従業員数300人未満の組織が64%を占めている
  - 民間企業61%，政府・自治体・大学34%となっているまた，民間企業の74%が中小企業が占めている
  - 41%の組織がPマークを，47%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1　回答者の所属（N=429）



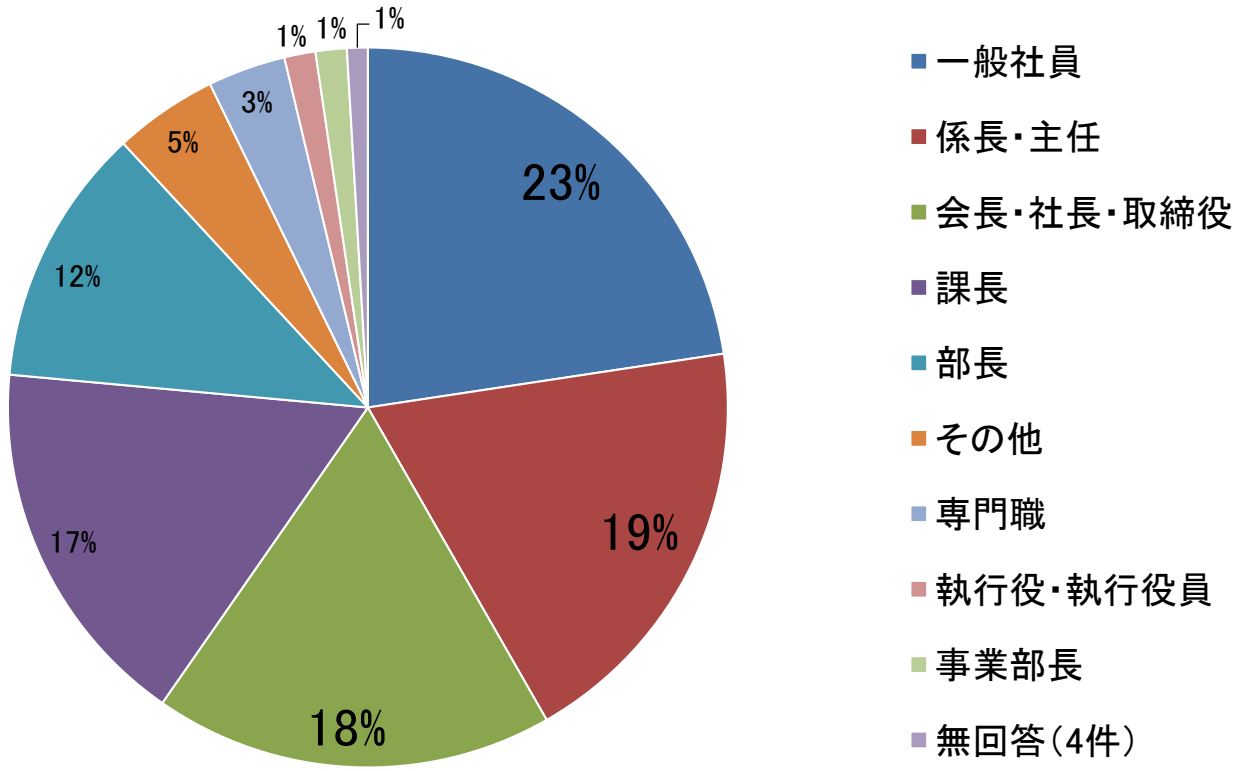
- 情報システム管理部門
- 総務部門
- 情報セキュリティ担当部門
- 社長室又は役員室
- その他
- 情報システム開発部門
- 事業/営業部門
- 経理部門
- 企画部門
- 人事部門
- リスク管理担当部門
- 監査部門
- コンプライアンス担当部門
- 法務部門
- 無回答（5件）

所属部門は「情報システム管理部門」，「総務部門」，
「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=429）

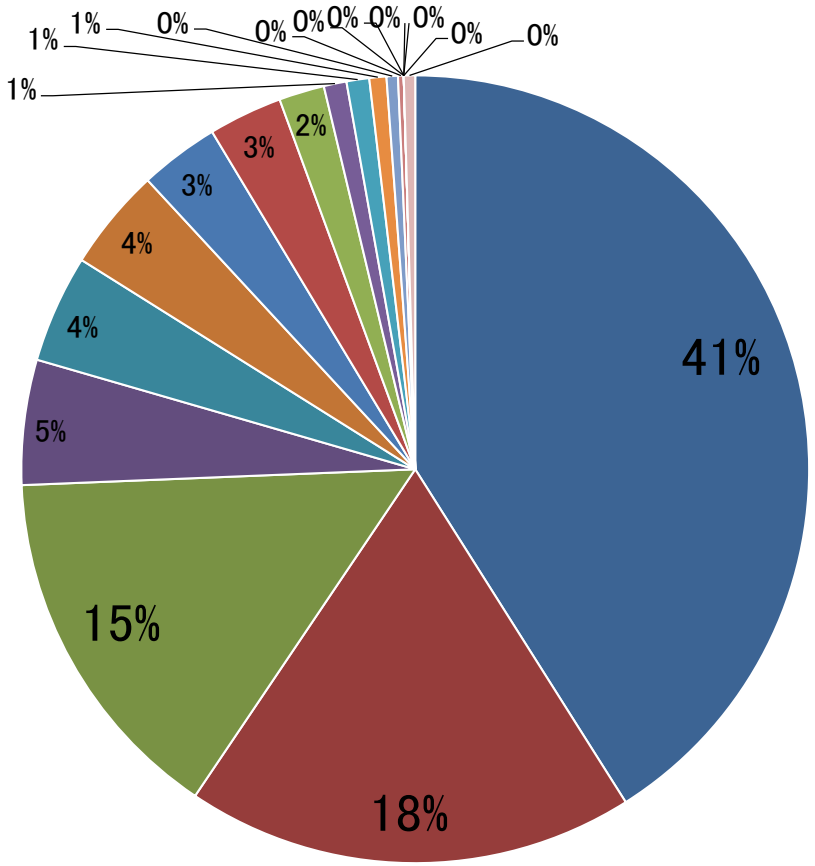


回答者は「一般社員」が最も多く（昨年度と同様），
「係長・主任」，「会長・社長・取締役」と続く

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=429）



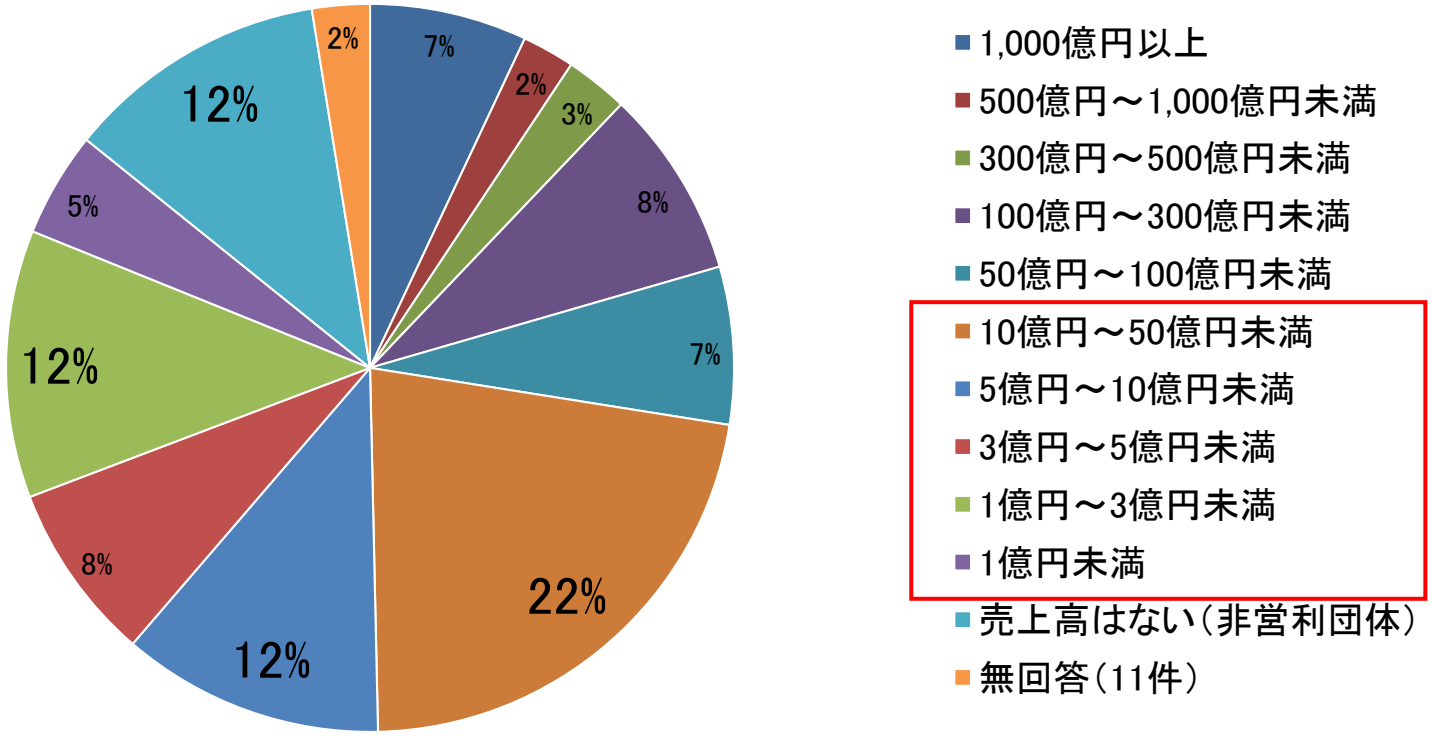
- 情報通信業
- 公務（政府・自治体）
- 大学
- サービス業
- 製造業
- 学術研究、専門・技術サービス業
- 卸売業、小売業
- その他
- 建設業
- 金融業、保険業
- 医療、福祉
- 運輸業、郵便業
- 教育、学習支援業
- 不動産業、物品賃貸業
- 農業、林業、漁業、鉱業
- 電気・ガス・熱供給・水道業
- 宿泊業、飲食サービス業
- 生活関連サービス業、娯楽業
- 複合サービス事業（郵便局、協同組合）
- 無回答（2件）

「情報通信業」は昨年と同様で41%と4割を占めている

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4　年間売上高（N=429）

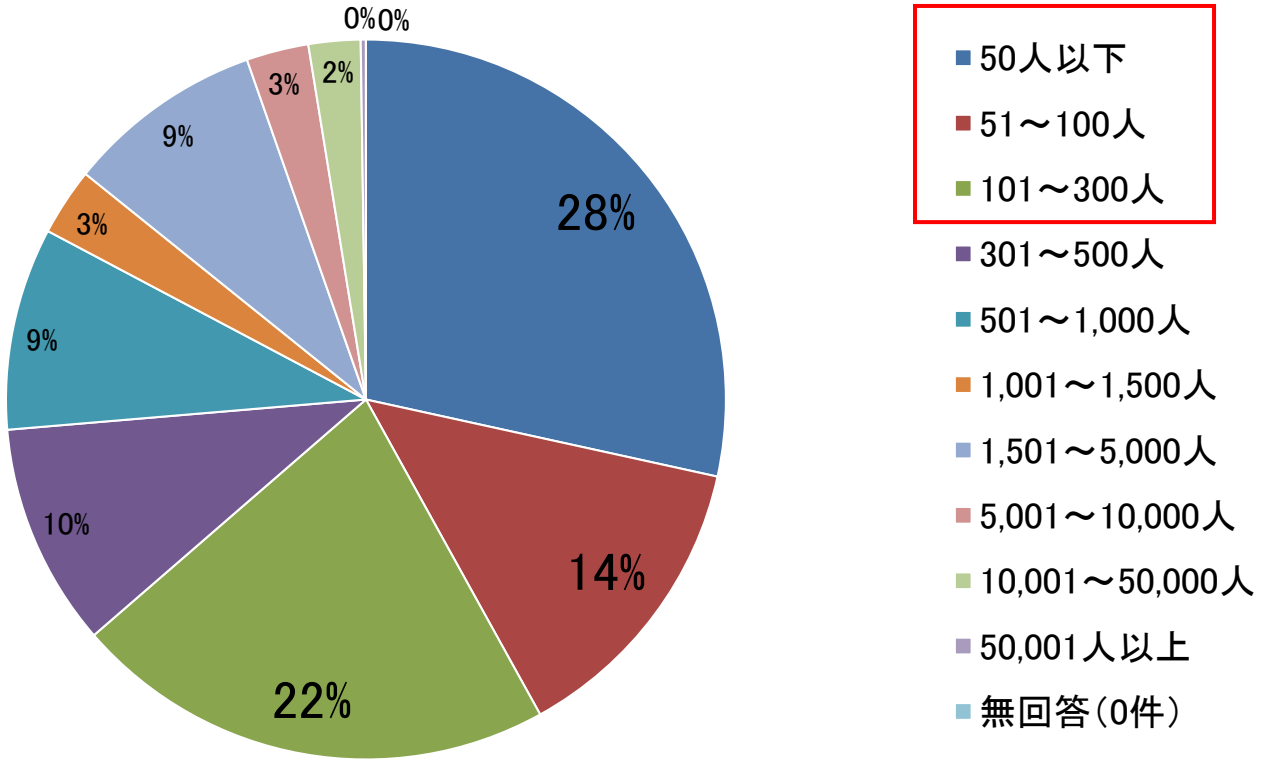


売上高「10億円～50億円」の組織が22%で最も多い
また，売上高50億円未満の組織で71%を占めている

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=429）

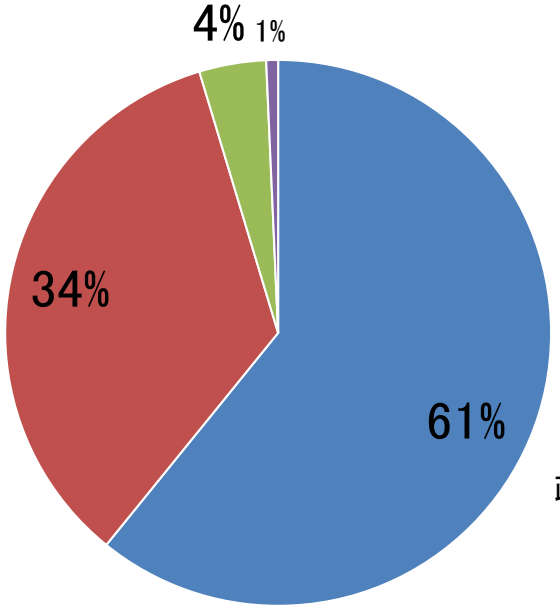


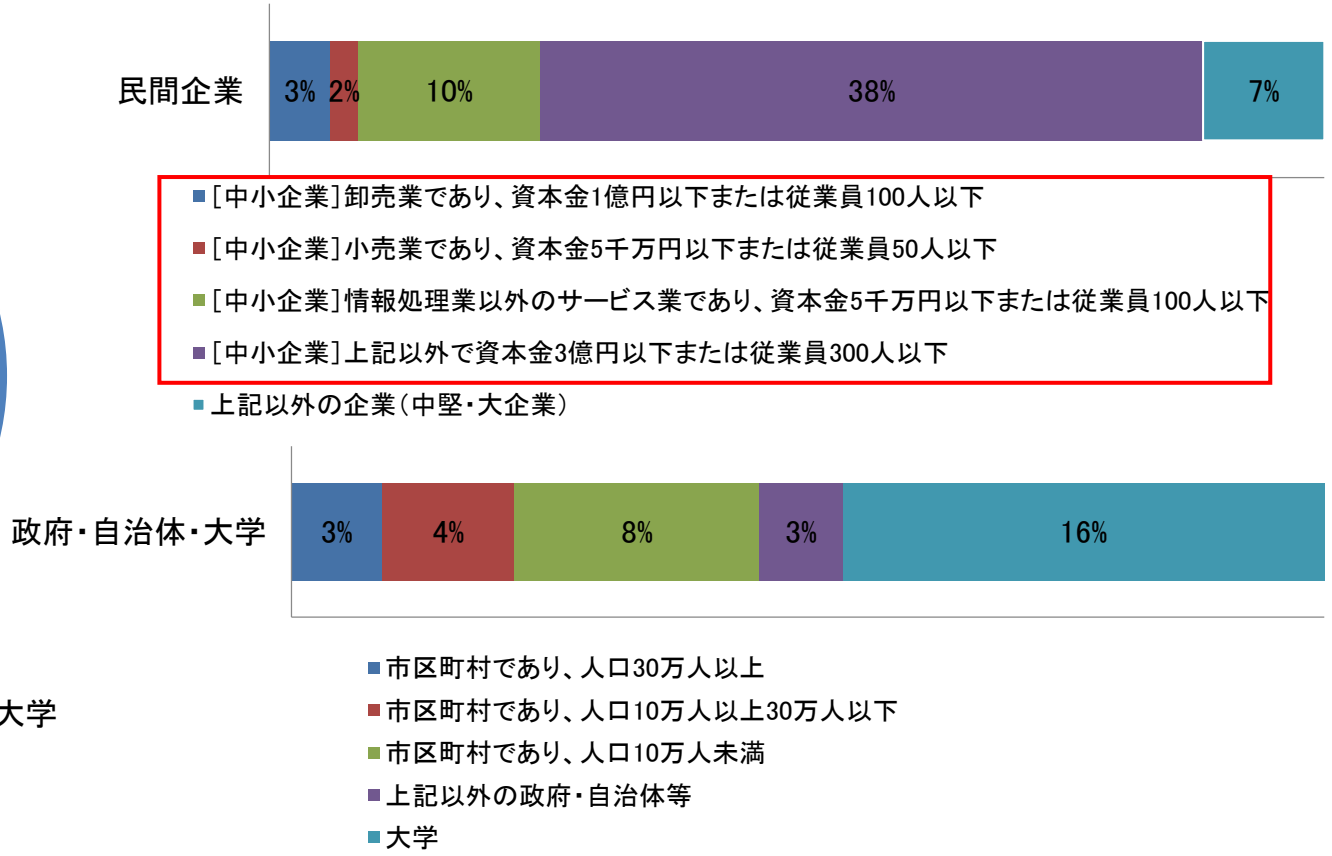
従業員数「50人以下」の組織が28%で最も多い
また，従業員300人以下の組織で64%を占めている

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=429）



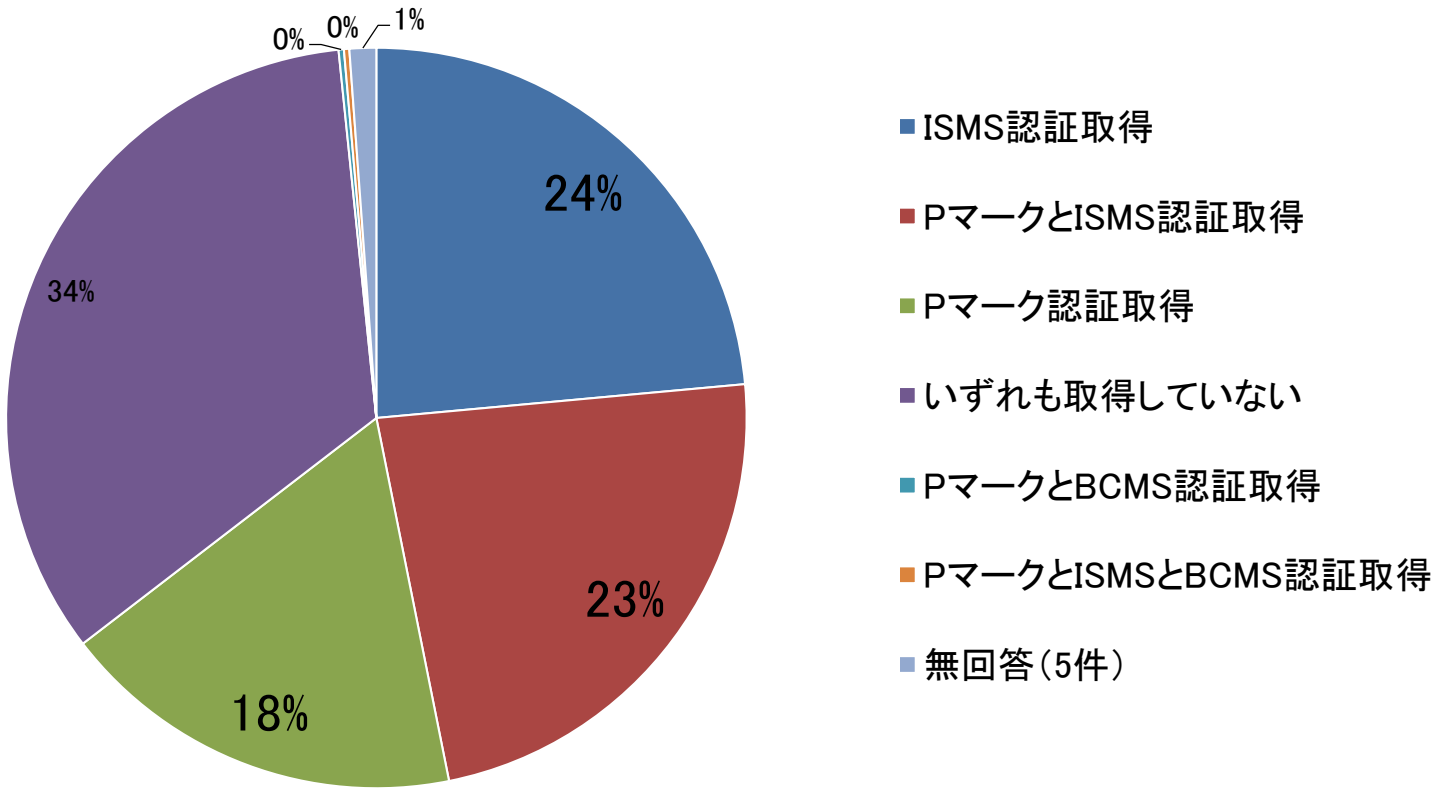


「民間企業」61%，「政府・自治体・大学」34%となっている
民間企業の中，中小企業が53%を占めている

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=429）



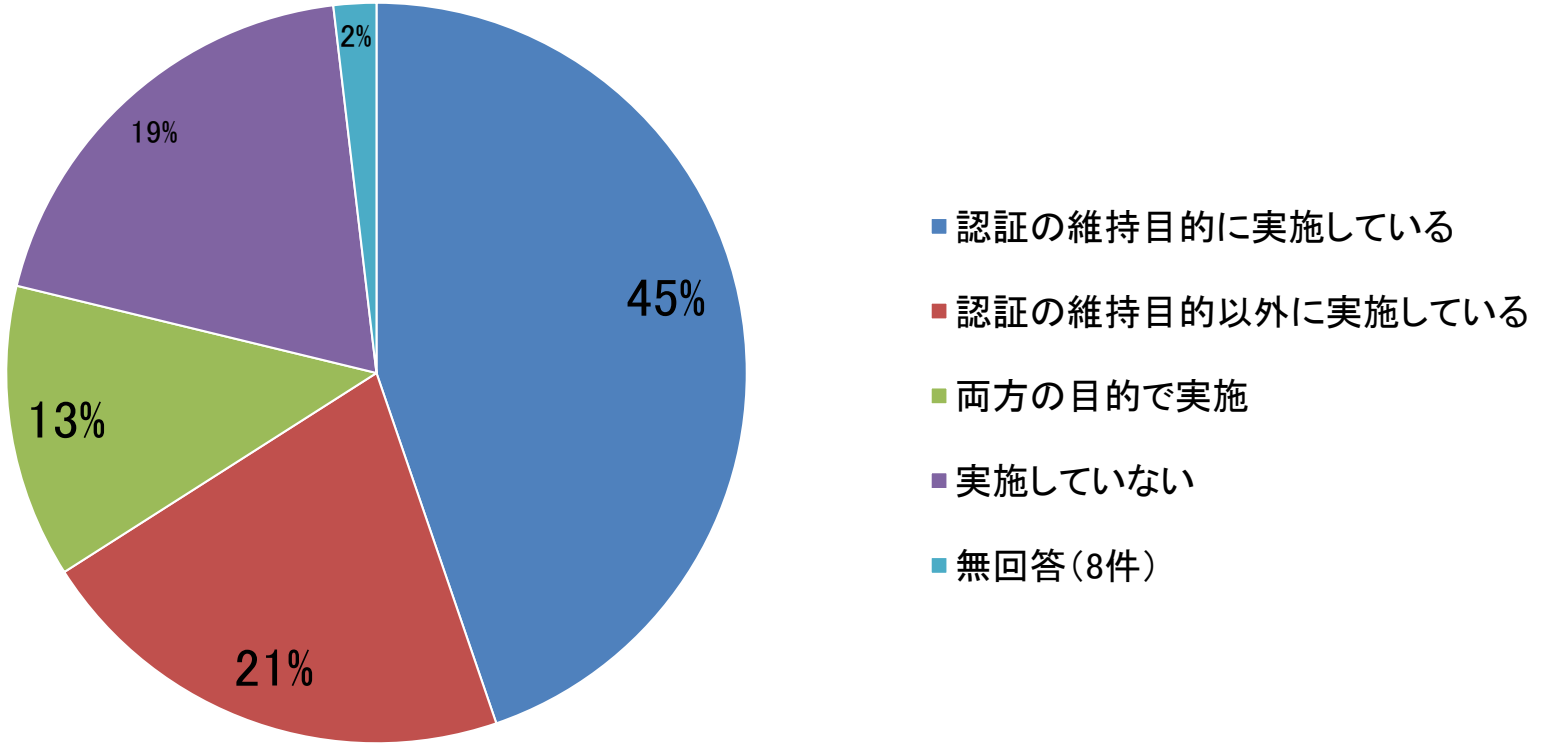
47%の組織がISMSを，41%の組織がPマークを取得している
また，23%の組織がPマークとISMSの両方を取得している

※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=429）



45%の組織が認証の維持目的，21%の組織が認証の維持目的以外，13%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2章
情報セキュリティマネジメントの取り組み

調査結果(1/2):

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(69%)は変わらない
- 問題点は，「実施方法が分かる人材の不足」(66%)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(84%)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(30%)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)」(39%)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」の認証対応が多いが，今年は「個人情報保護法　改正の対応」，「事件・事故対応」が多くなった
- 対策推進上の難しさは，「実施人材確保」，「効果を測定」が多い

調査結果(2/2):

情報セキュリティに関する支出

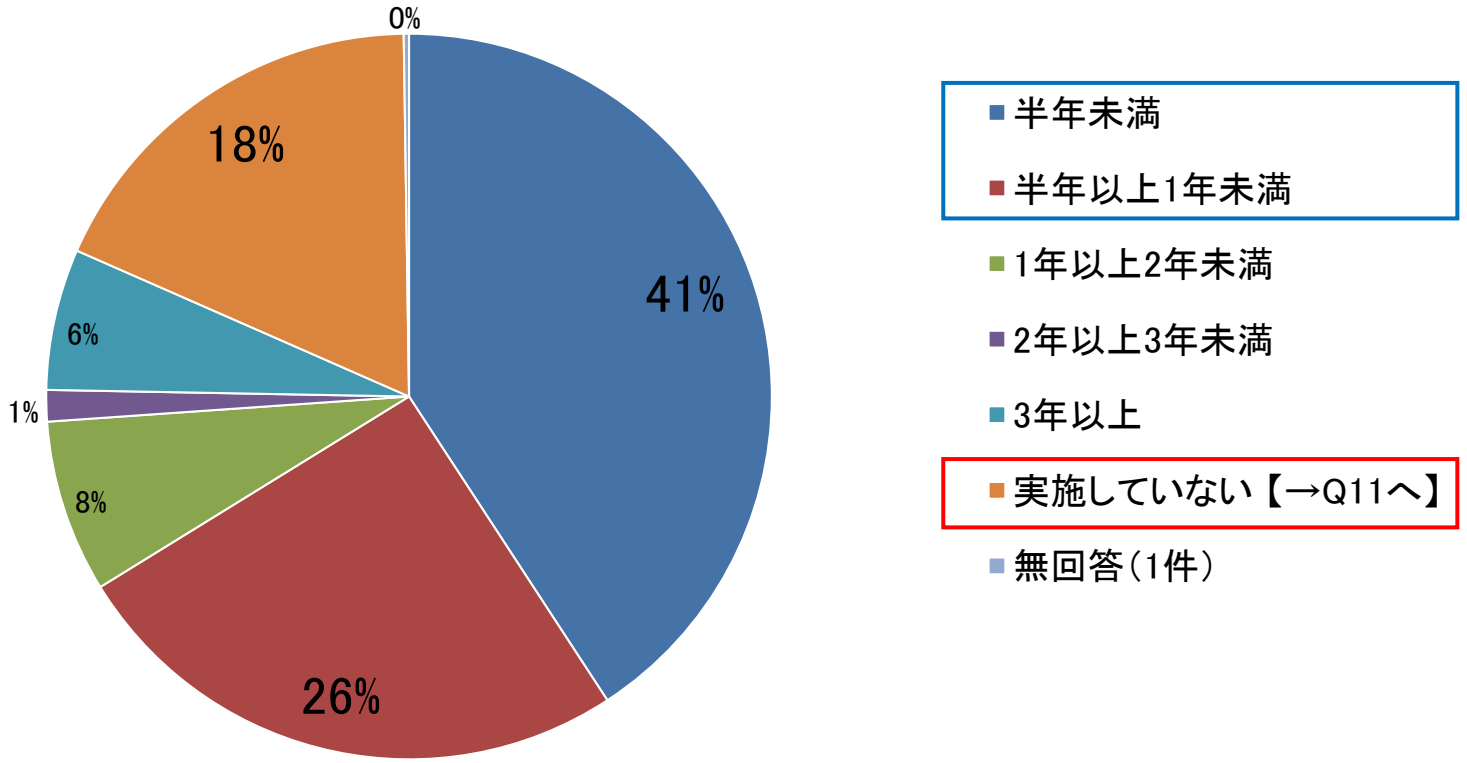
- 情報セキュリティに関する支出は，売上や予算の0.1%未満(51%)が多い認識していない組織(21%)も多い
- 情報セキュリティ支出は「前期と今期の比較」，「今後の変化」，「組織の全売上(予算)動向」のいずれも「ほぼ横ばい」が約50%から60%であった
- 「著しく増加と増加」計が「前期と今期比較」と「全売上(予算)動向」で22%超になった

情報セキュリティ政策(ガイドライン)の認知度

- 「情報セキュリティ管理基準，監査基準」が上位だが50%前後である

逆に「監査企業台帳」や「対策ビデオ」等は20%以下で認知されていない

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=429）

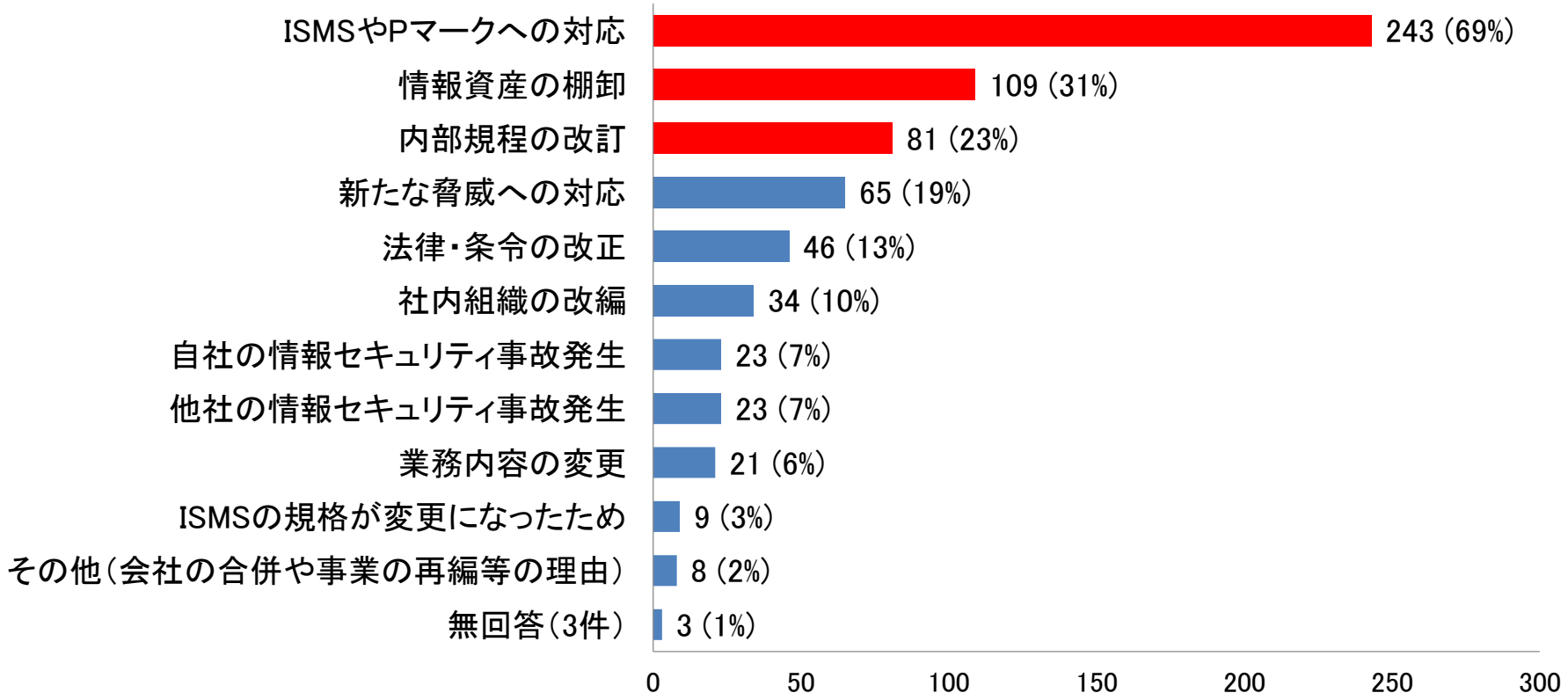


67%（284）の組織が，1年以内にリスク分析を実施している
一方，18%（78）の組織はリスク分析を実施していない

第2章 情報セキュリティマネジメントの取り組み

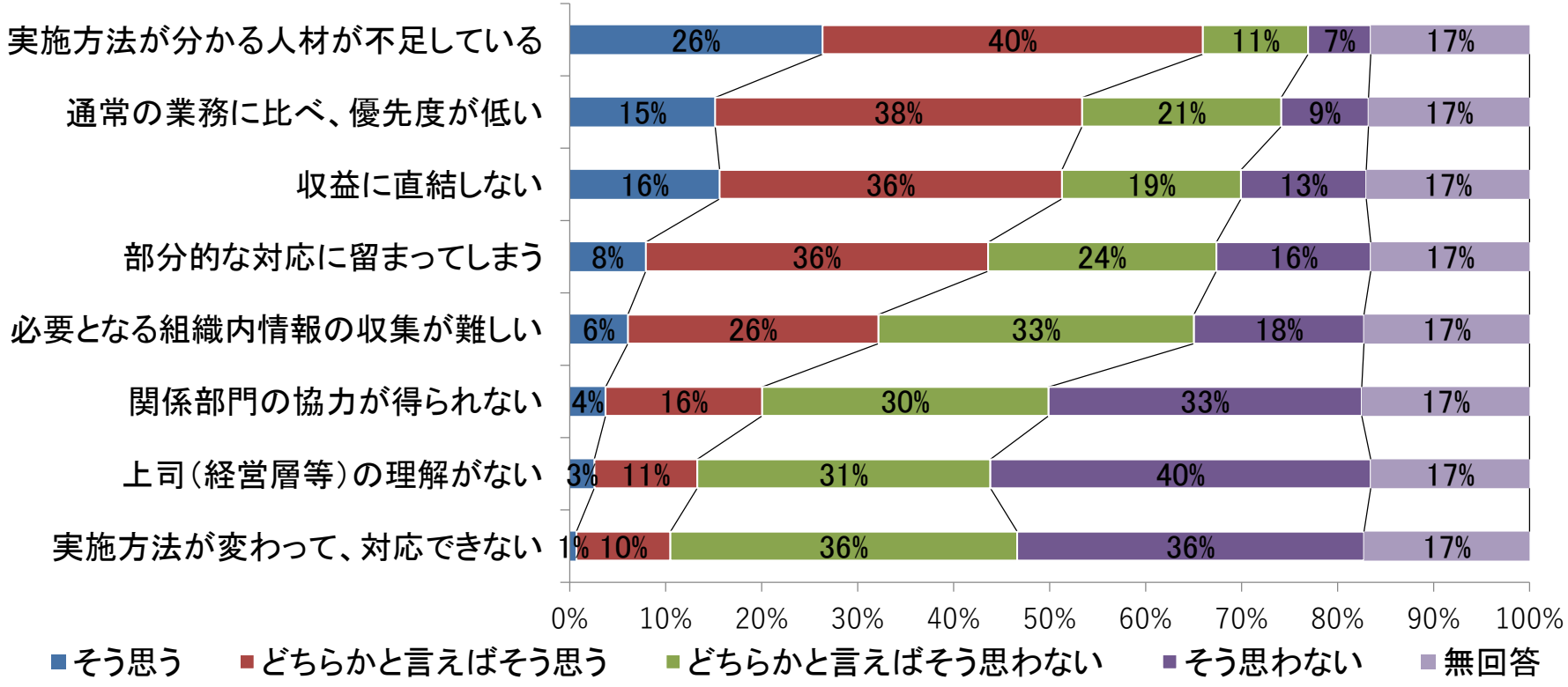
設問10　リスク分析の実施理由（複数回答，N=351）

※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243件（69%），「情報資産の棚卸」が109件（31%），「内部規程の改訂」81件と，「新たな脅威への対応」が65件で続いている

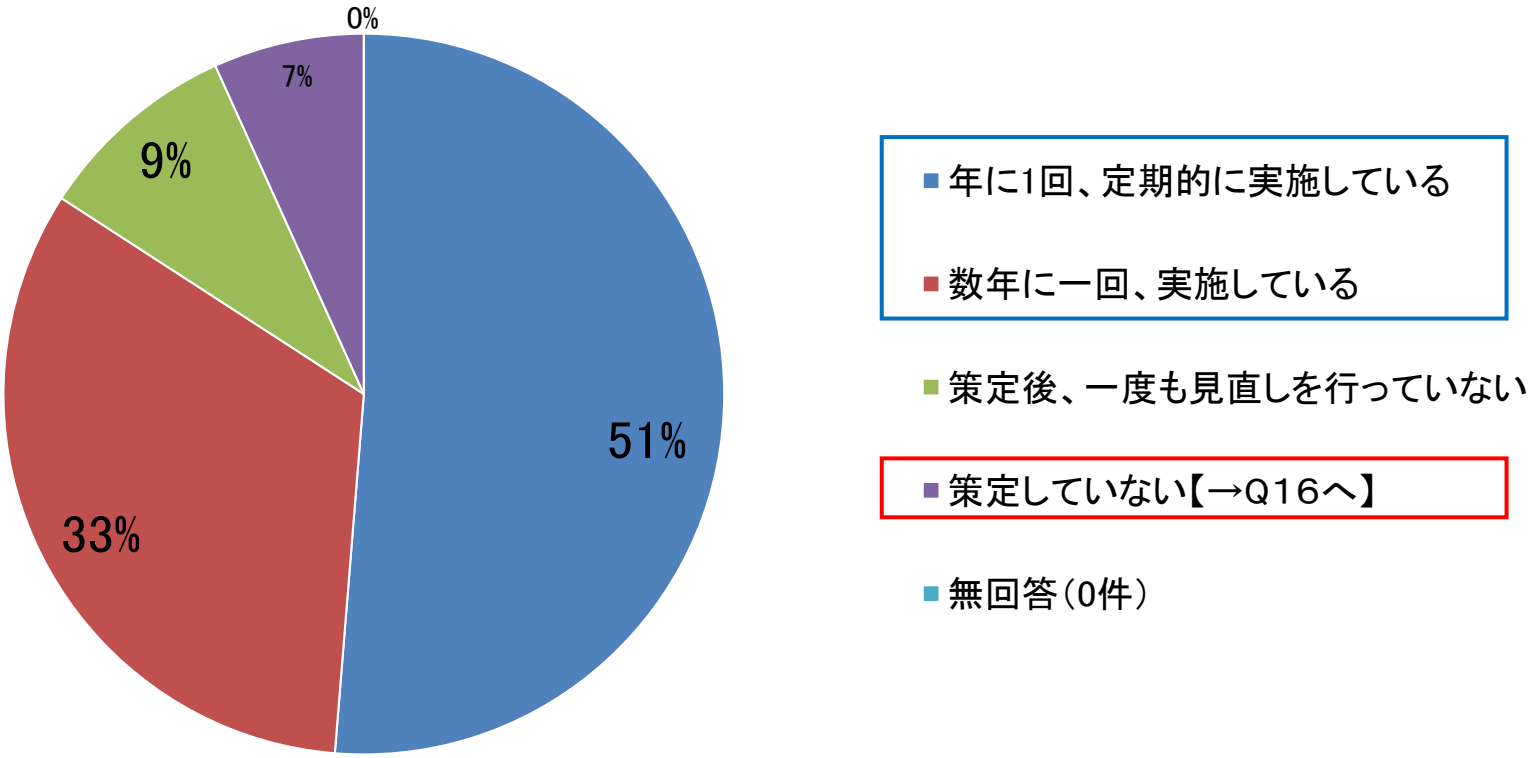
設問11　リスク分析を行う際の問題点（N=429）



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（66%），「通常業務に比べ，優先度が低い」（53%），収益に直結しない（52%）の順である，部分的な対応に留まるは44%と高く，「実施方法が変わって対応できない」は11%と低かった

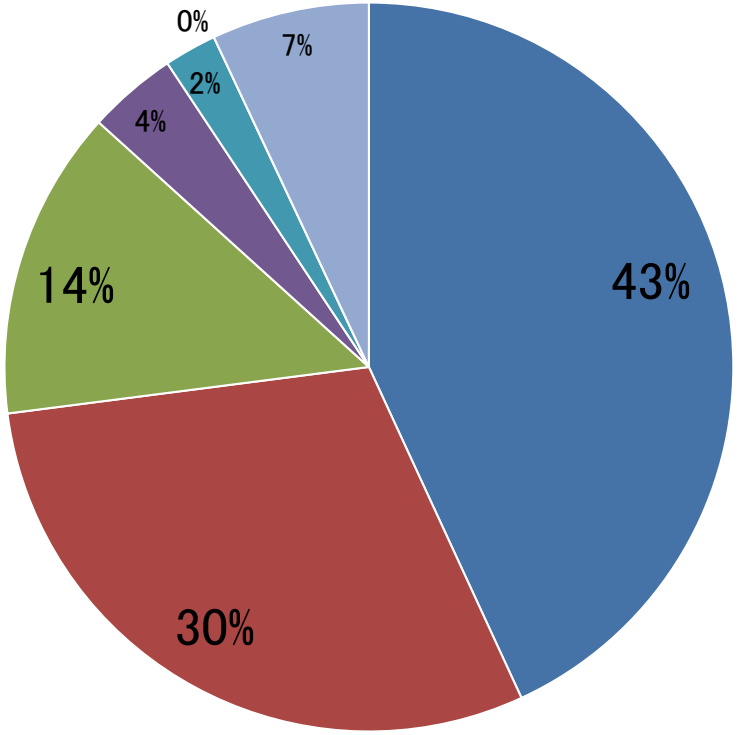
設問12　情報セキュリティポリシー（方針・対策基準）の策定と見直し状況（N=429）



84%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，
9%が策定後見直しておらず，29組織（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

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=429）



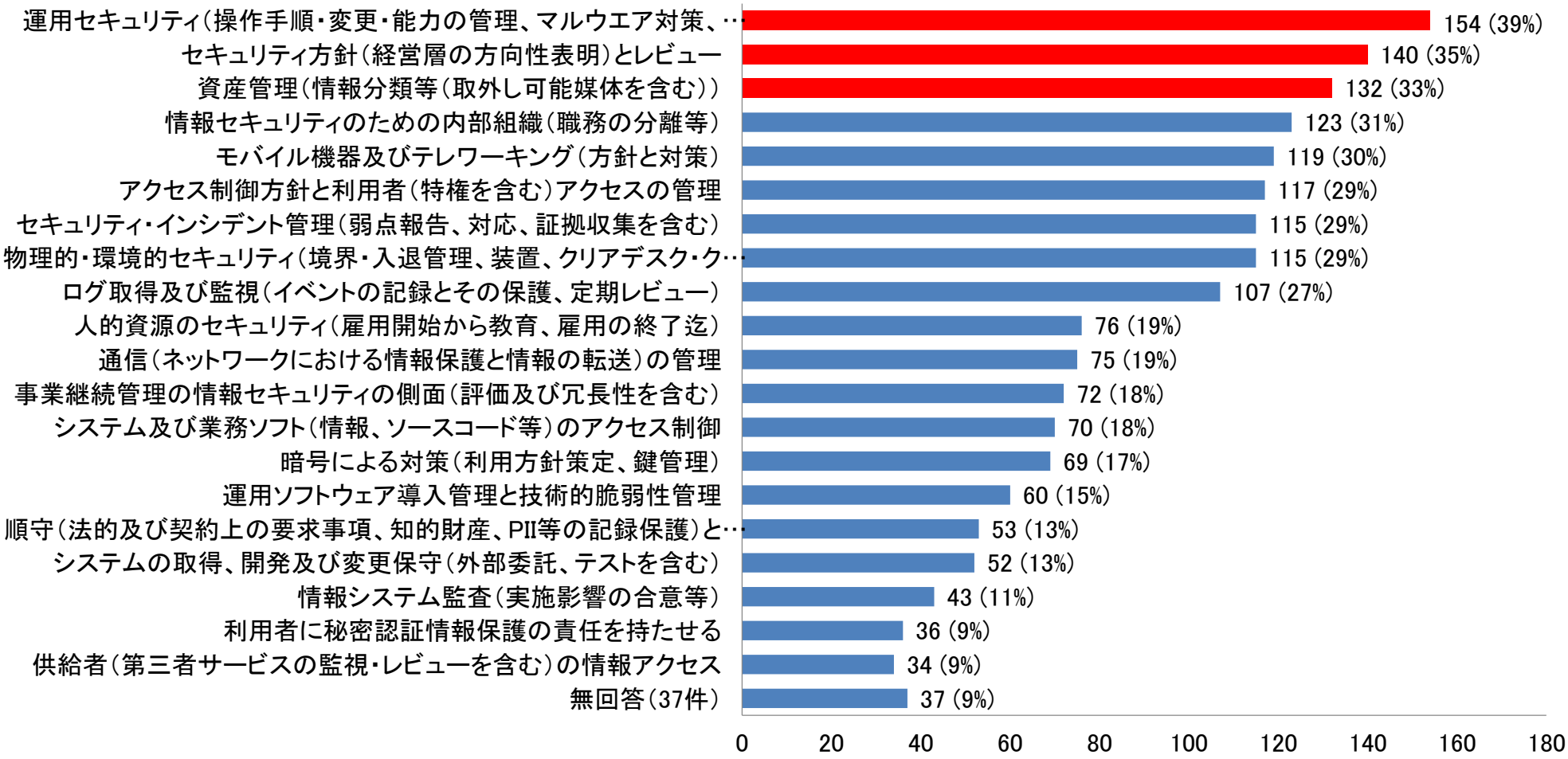
- 情報システム部門・情報セキュリティ部門が策定・見直しをしている
- 委員会組織で見直し、代表者が手続きを行っている
- 経営層（取締役以上）が策定・見直しをしている
- 情報システム部門・情報セキュリティ部門「以外」の部門が策定・見直しをしている
- その他
- 情報セキュリティポリシーはない
- 無回答（30件）

“情報システム部門・情報セキュリティ部門”が43%，
“委員会組織”が30%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

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=400）

※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

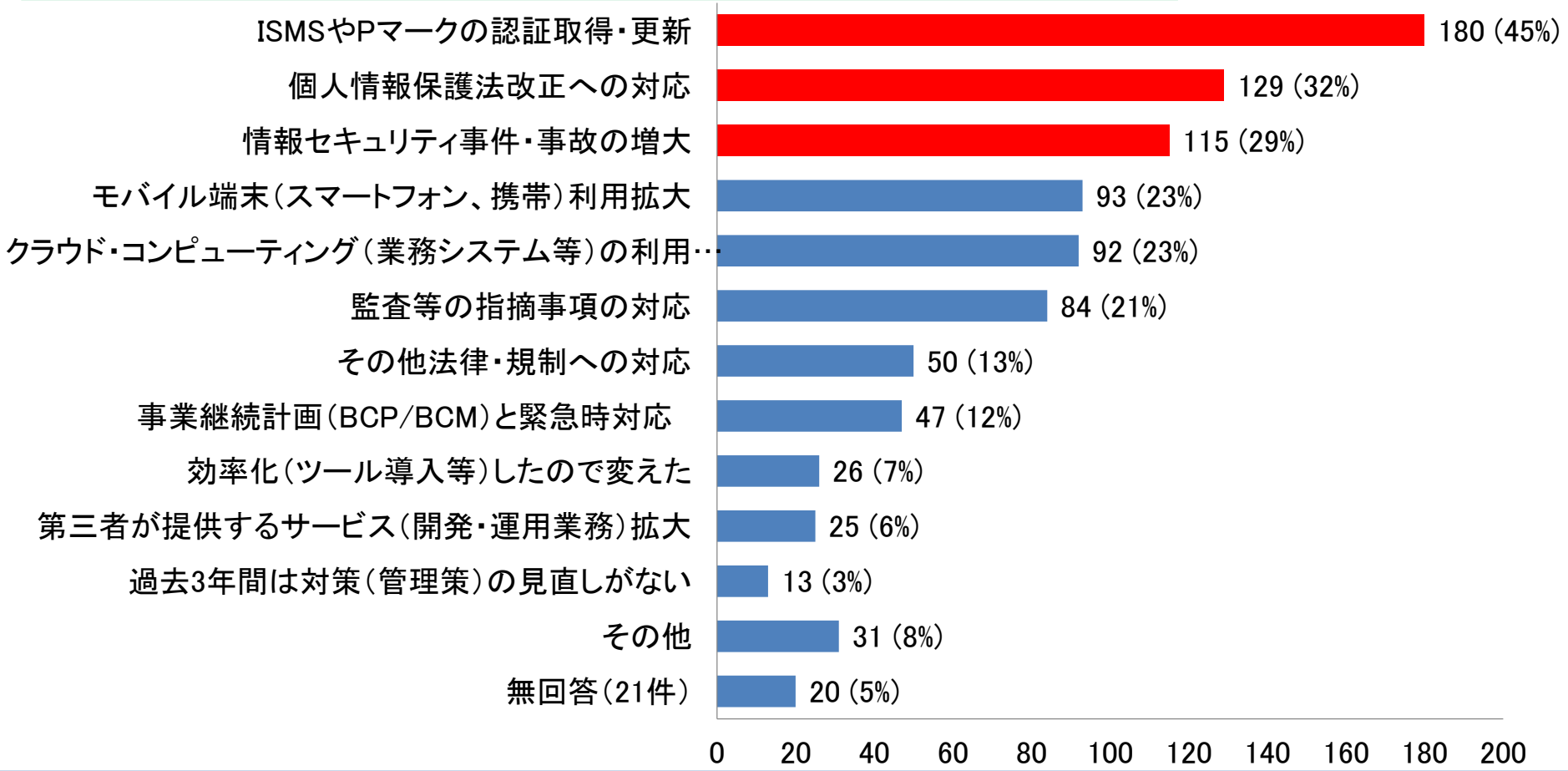


見直した管理策は，“運用セキュリティ”，“セキュリティ方針とレビュー”の順で多い
“資産管理”，“ログ取得及び監視”等の管理策が100件をこえている

第2章 情報セキュリティマネジメントの取り組み

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=400）

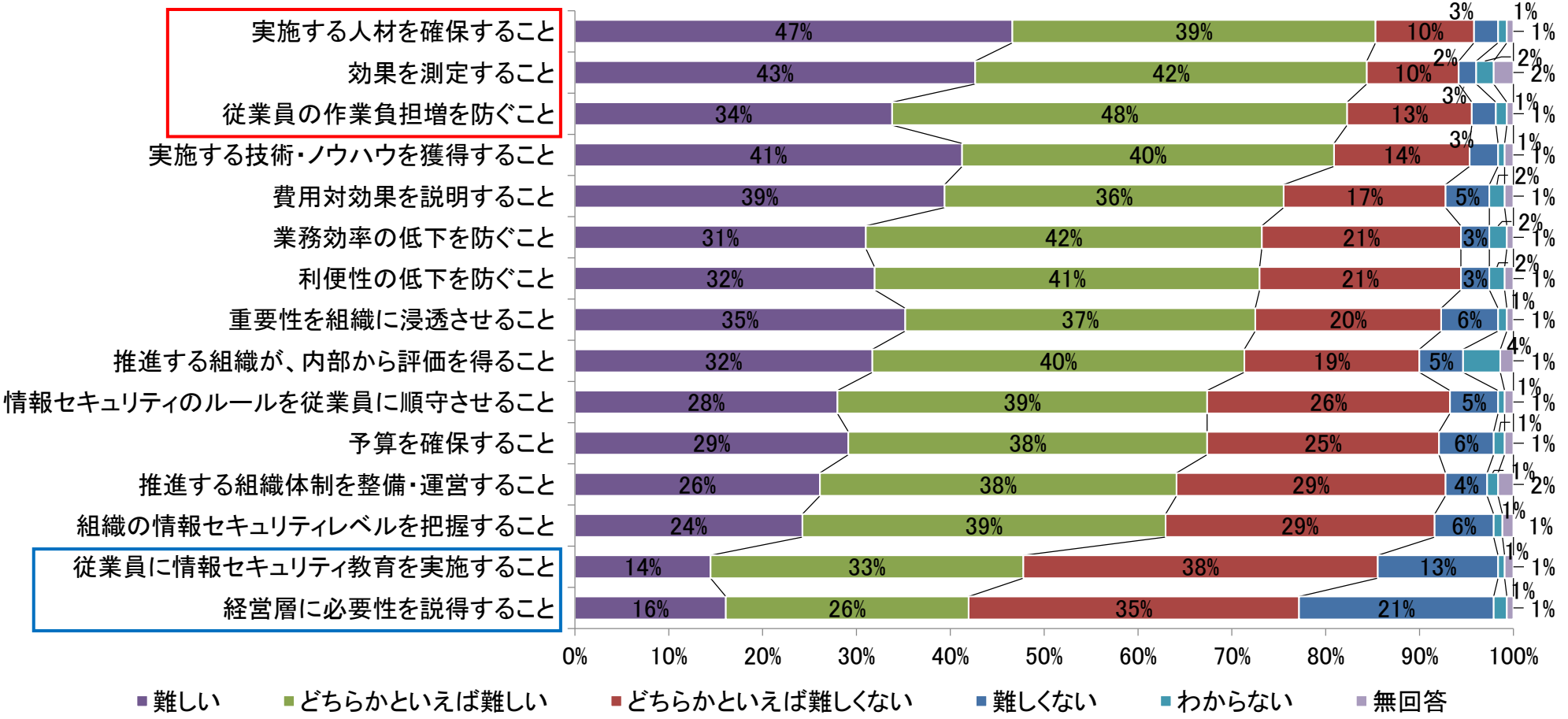
※設問 12で「**情報セキュリティポリシーはない（29件）**」以外を選択した組織を対象



「ISMSやPマーク取得・更新」が従来通り多いが，今年は
「個人情報保護法改正への対応」，「事件・事故の増大」が多かった

第2章 情報セキュリティマネジメントの取り組み

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=429）

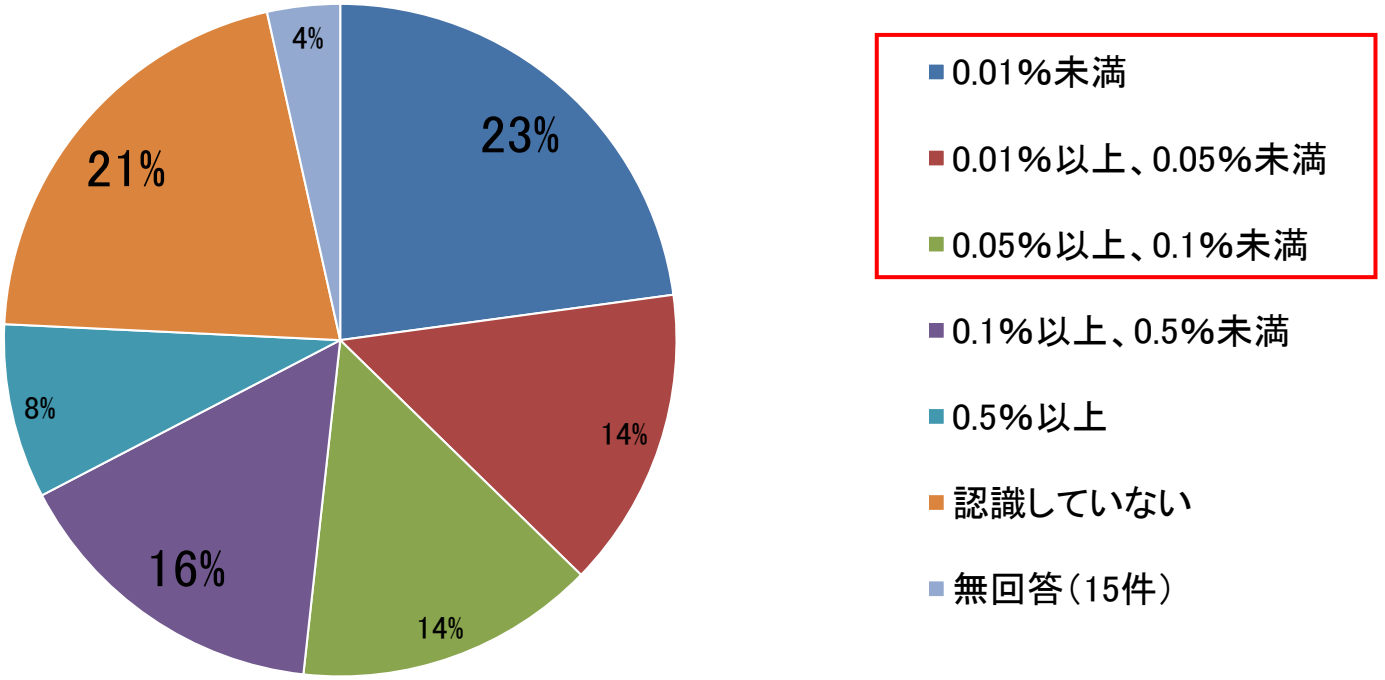


注：　＜難しい・どちらかと言えば難しい＞の多い順に表示

「実施人材を確保」,「効果測定」,「作業負担増を防ぐ」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

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（注）の割合　（N=429）

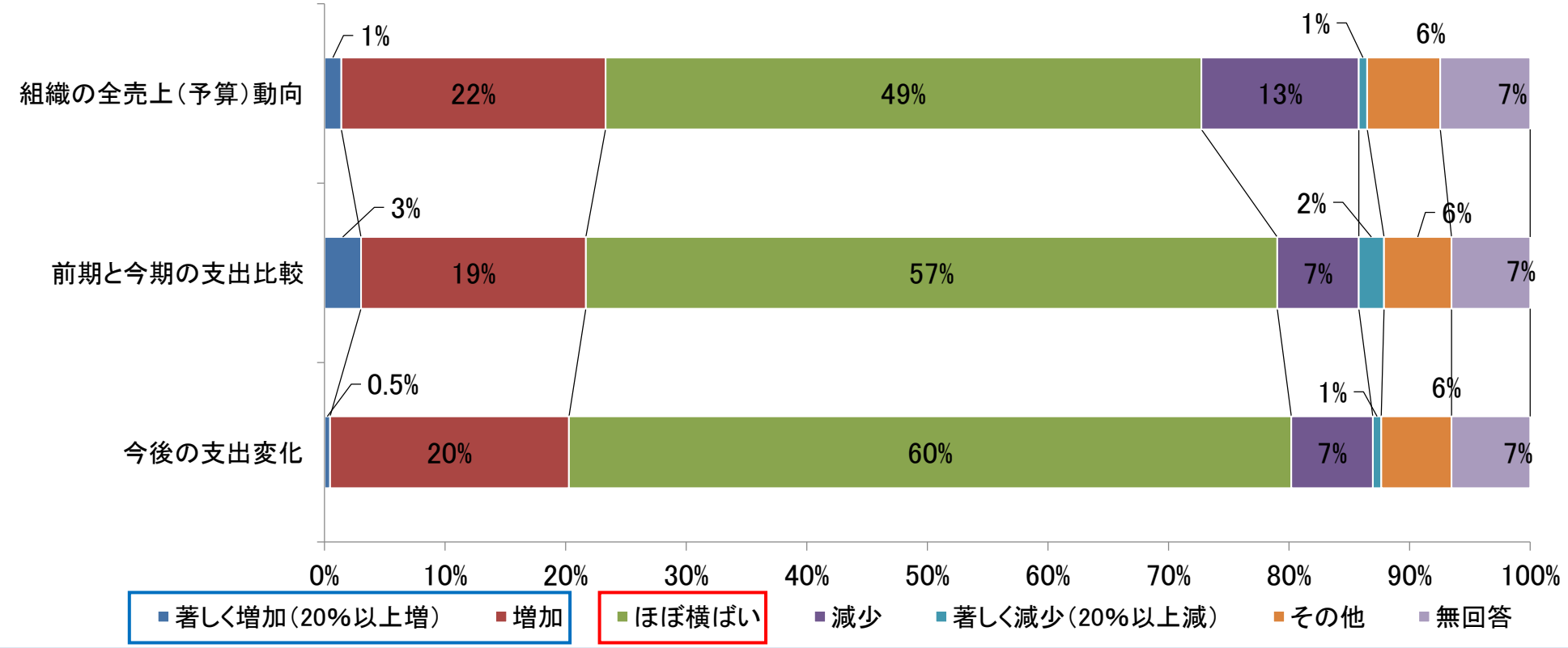


注：セキュリティ関連システム開発，運用，ライセンス等外部への支出総計

情報セキュリティ支出は，売上・予算の0.1%未満が51%であった．最多は，「0.01%未満」で23%（98件），また，「認識していない」が21%（89件）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

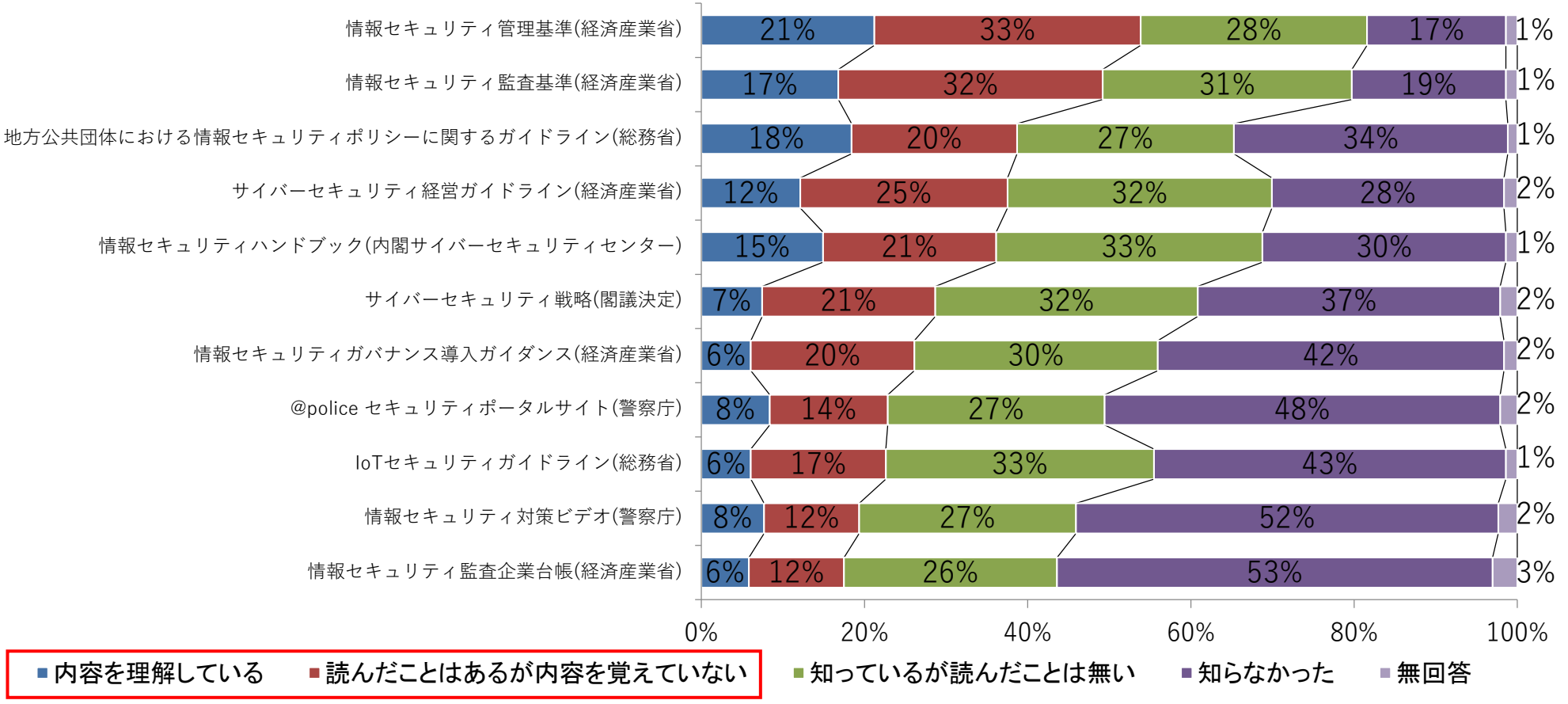
設問17-2　売上（政府・自治体・大学等は予算）に対する情報セキュリティに関する支出の傾向（N=429）



いずれも「ほぼ横ばい」が50%から60%を占めた「著しく増加と増加」計が「前期と今期比較」と「全売上（予算）動向」で22%超になった

第2章 情報セキュリティマネジメントの取り組み

設問18　情報セキュリティ政策（ガイドライン）の認知度　（N=429）



注：　＜内容理解している，読んだことが有る＞の多い順に表示

「情報セキュリティ管理基準，監査基準」が上位だが50%前後である
逆に，「監査企業台帳」や「対策ビデオ」等は20%以下で認知されてない

第3章
個人情報保護法の改正による影響

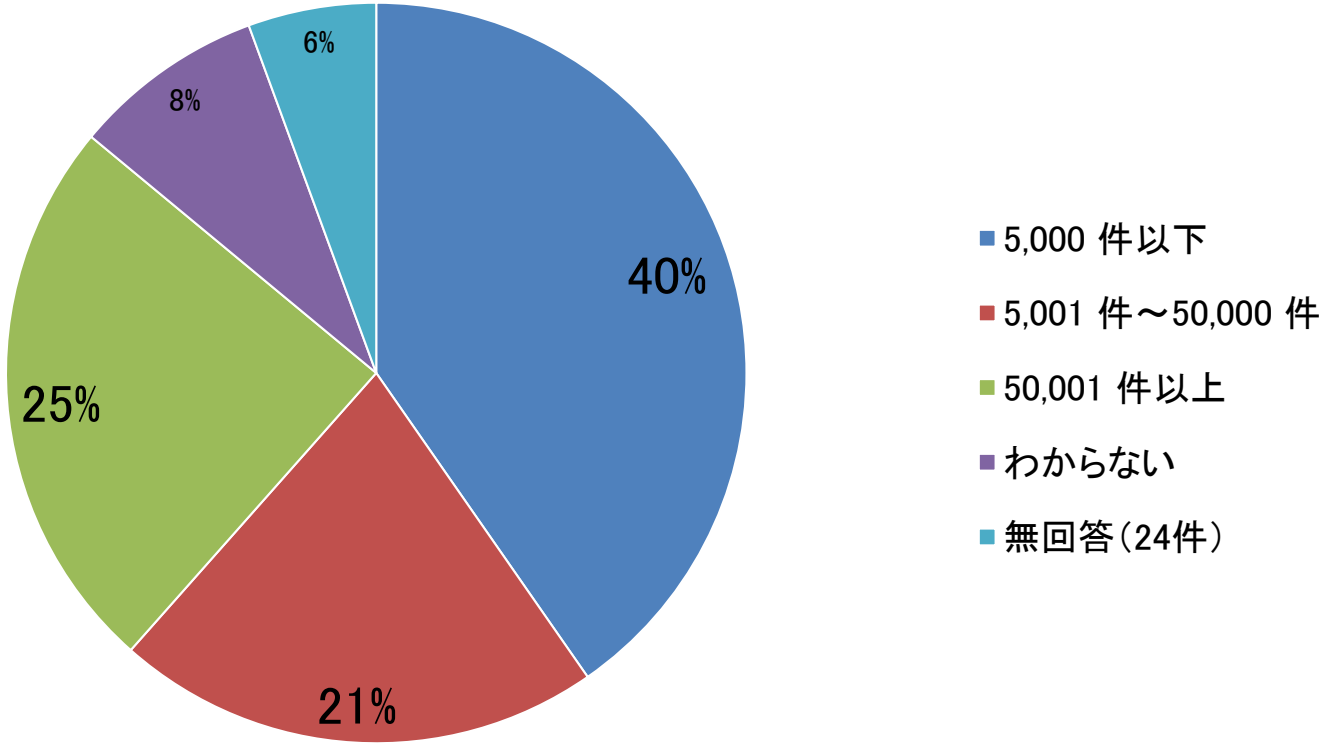
第3章　個人情報保護法の改正による影響

調査結果：

- 保有個人データの保有件数
  - 保有件数「5,000件以下」が最も多く40%であり，「5,001件～50,000件」が21%，「50,001件以上」が25%であった
  - 「わからない」が8%であった
- 改正個人情報保護法への理解度
  - 「十分理解している」「およそ理解している」の合計では「個人識別符号」が最も多く，72%であった
  - 「外国にある第三者への提供」は最も少なく，40%であった
  - 「十分理解している」のみでは「特例の廃止」が最も多く，39%であった
- 実施した施策
  - 「個人情報保護方針・規定類の見直し」（53%），「従業員教育」（39%）が多い
  - 「外国にある第三者への提供の見直し」（1%）が最も少ない
  - 「特に施策は実施していない」は21%であった

第3章　個人情報保護法の改正による影響

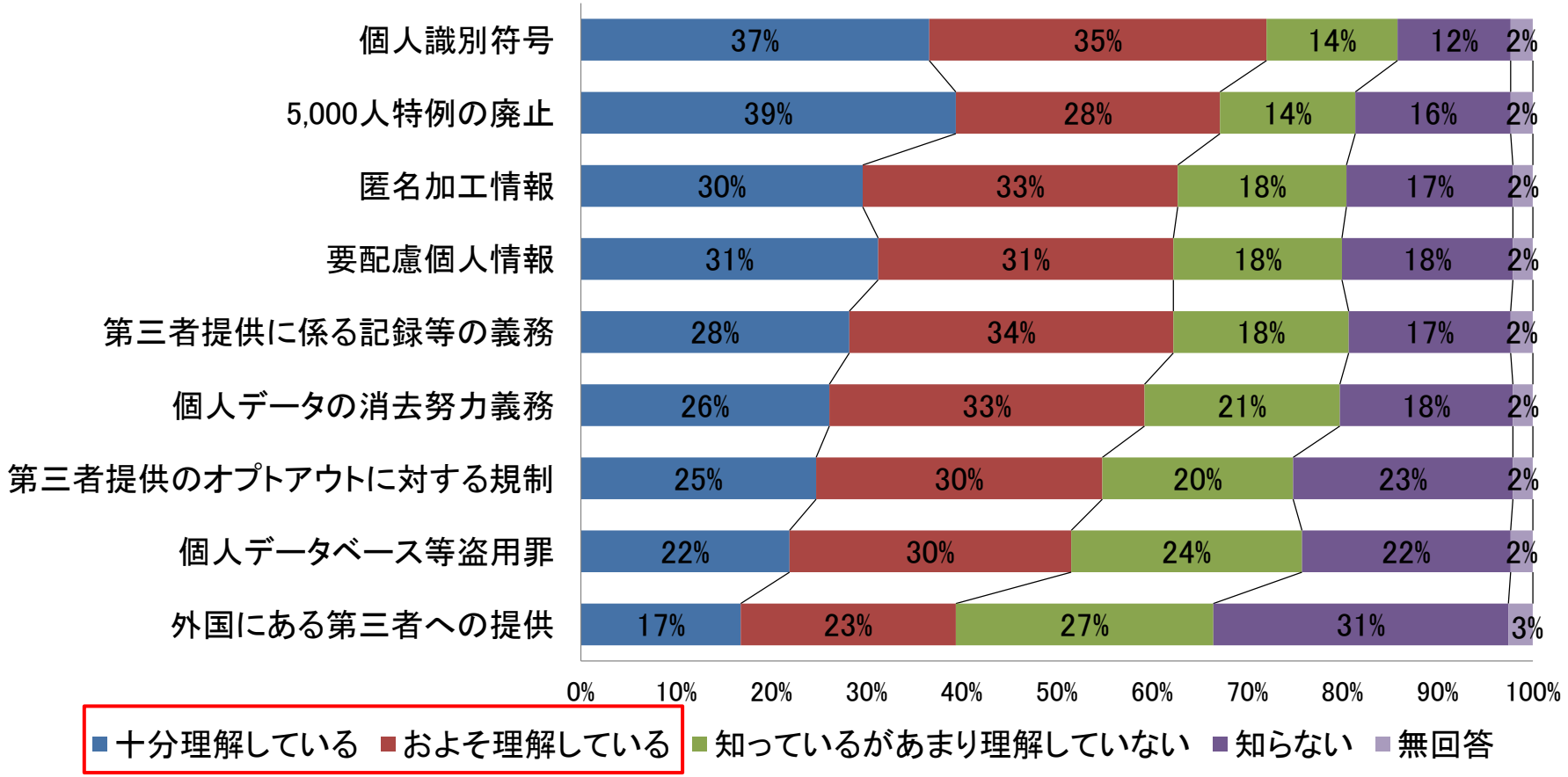
設問19　保有個人データの保有件数（N=429）



保有件数「5,000件以下」が40%で最も多く，「5,001件～50,000件」が21%，
「50,001件以上」が25%であり，「わからない」は8%であった

第3章　個人情報保護法の改正による影響

設問20　改正個人情報保護法への理解度（N=429）

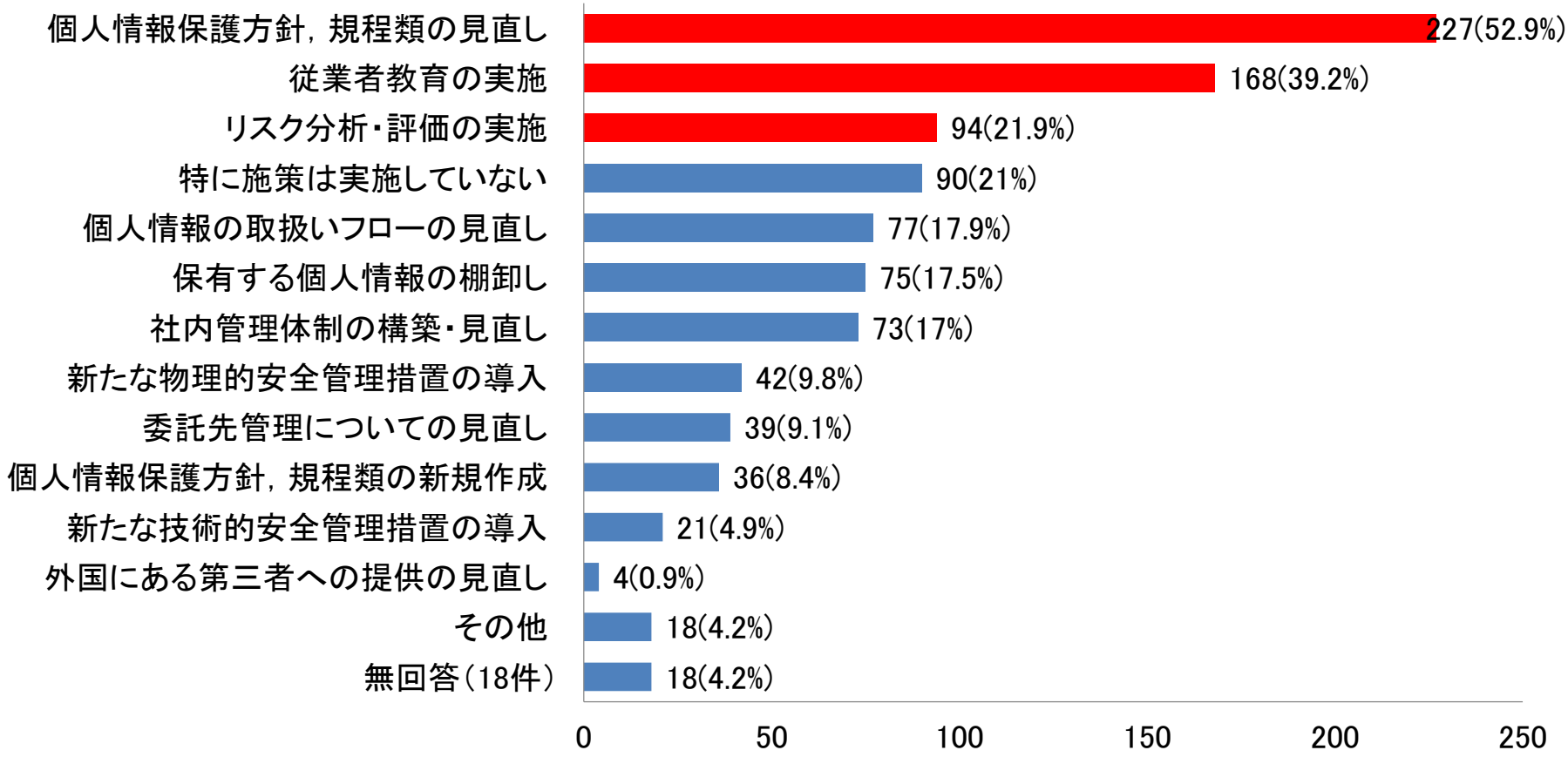


「十分理解している」「およそ理解している」の合計では「個人識別符号」が72%で最も多く，「外国にある第三者への提供」は40%で最も少なかった，「十分理解している」のみでは「特例の廃止」が39%で最も多かった

第3章　個人情報保護法の改正による影響

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

設問21　個人情報保護法改正に対する対応のため実施した施策（複数回答，N=429）



「個人情報保護方針・規定類の見直し」（53%），「従業員教育」（39%）が多い
「外国にある第三者への提供の見直し」（1%）が最も少ない

第4章
情報セキュリティガバナンス体制

第4章　情報セキュリティガバナンス体制

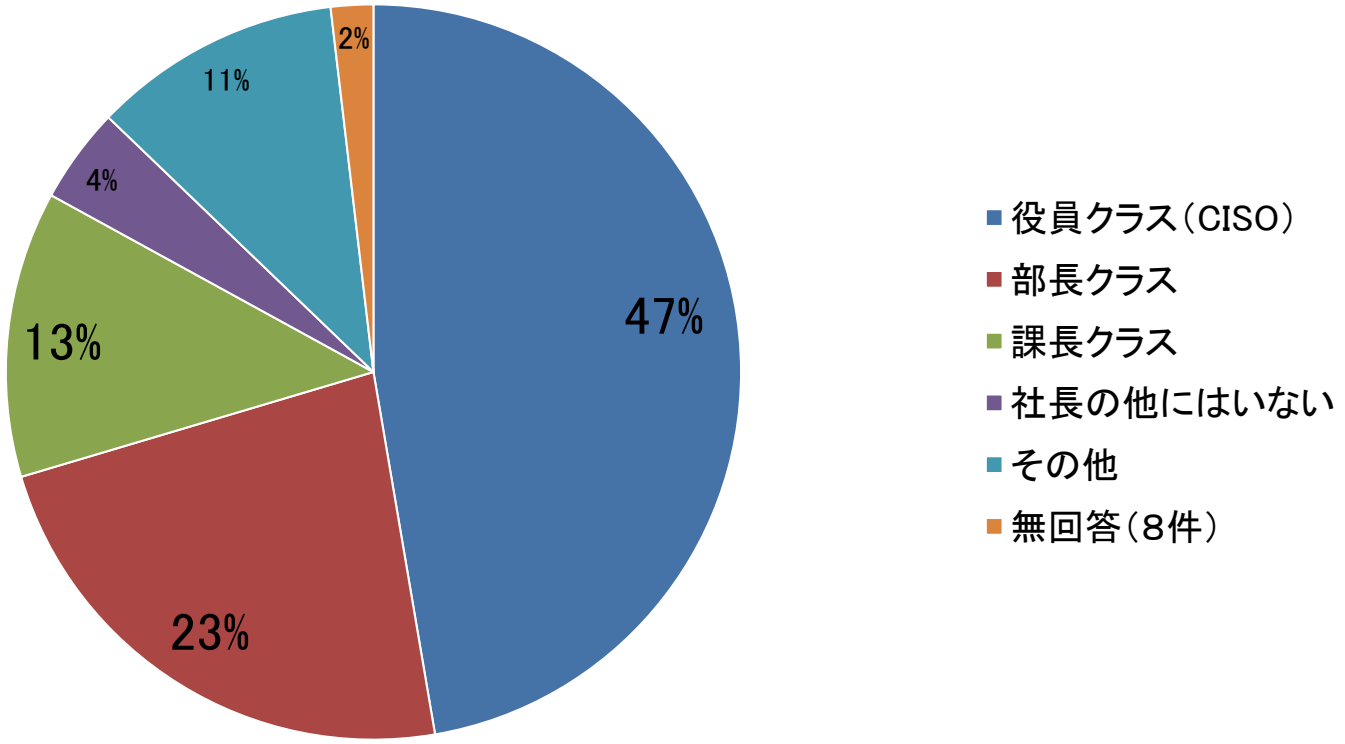
調査結果：

- 情報セキュリティ責任者は，役員・部長クラスなど上位職が担当
  情報セキュリティ内部統制，投資やリスク受容の経営判断を期待
- 情報セキュリティ専任部署があるのは15%とまだ少数派
  情報システム部門が担当は20%で牽制に懸念も
- 情報システム部門に情報セキュリティを実施してもらうには，「経営者のリーダーシップ」が重要
- 情報セキュリティ部門が情報システム部門から独立すべきかどうかは「わからない」が最多回答（44%）
  独立させない理由（分けているのは非効率との意見：139件）と
  独立させる理由（使命が違う，情報システムへの牽制：96件）が，
  1位，2位を占める

第4章　情報セキュリティガバナンス体制

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

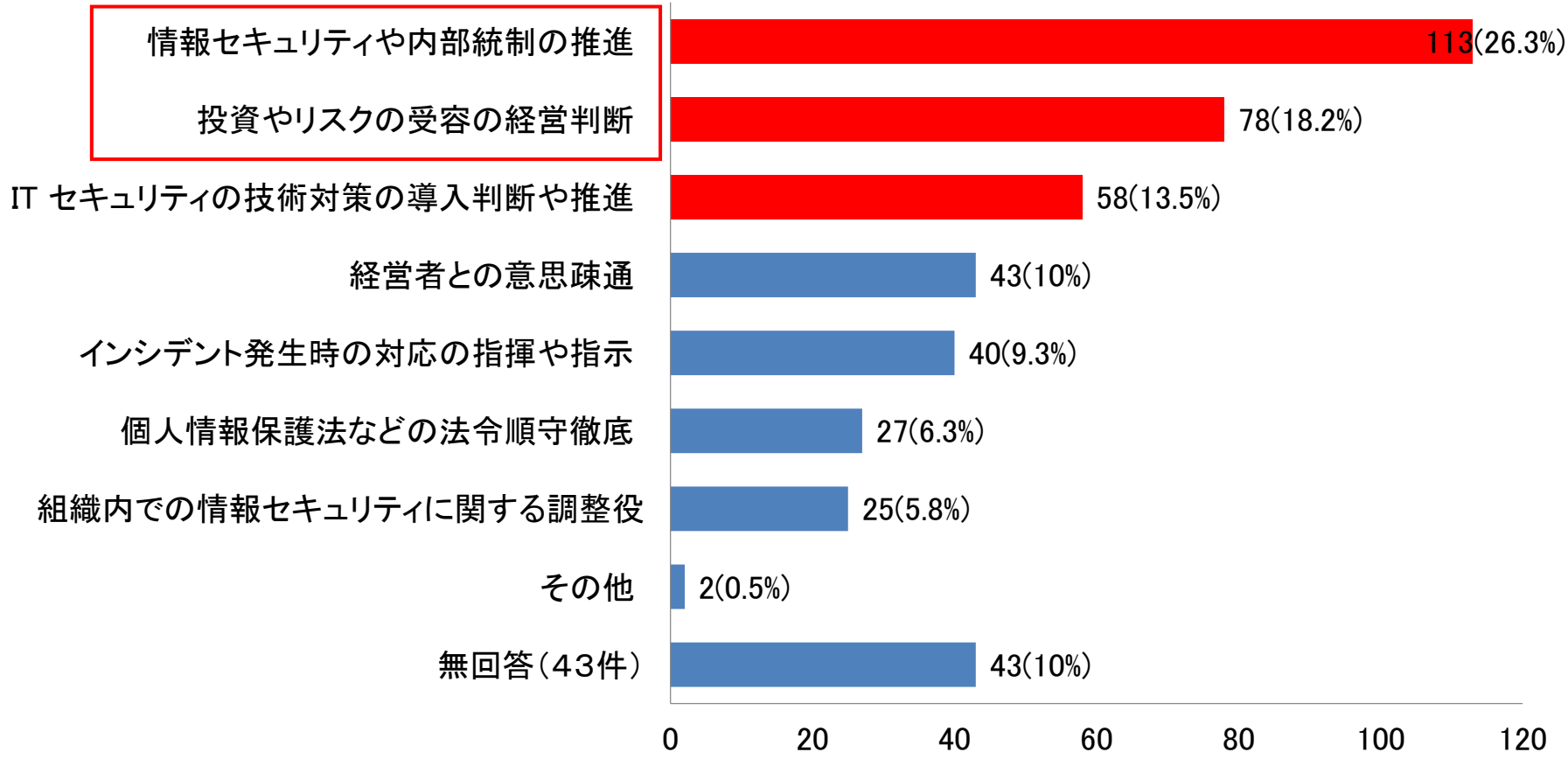
設問22　情報セキュリティ責任者の職位（N=429）



ほぼ半数（47%）が「役員クラス」，23%が「部長クラス」であり，
上位職が情報セキュリティ責任者となっている
一方，その他には，一般社員にも11%ある

第4章　情報セキュリティガバナンス体制

設問23　情報セキュリティ責任者に最も期待する役割（複数回答，N=429）



「情報セキュリティや内部統制の推進」（113件）や
「投資やリスク受容の経営判断」（78件）を望む回答が多い

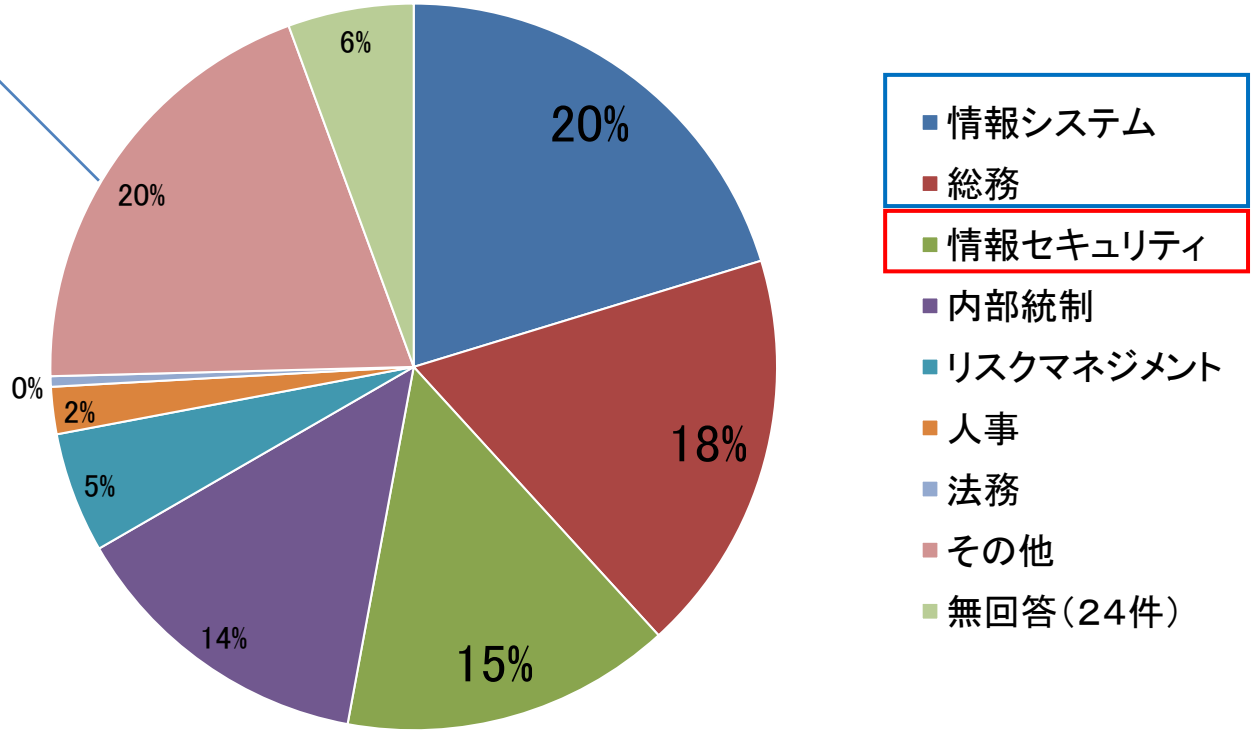
第4章　情報セキュリティガバナンス体制

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

設問24　情報セキュリティ責任者の専任・兼任と兼任の場合の主務（N=429）

その他（記述57件）

経営系	20件
営業系	12件
IT系	7件
管理系	6件
教員・開発	6件



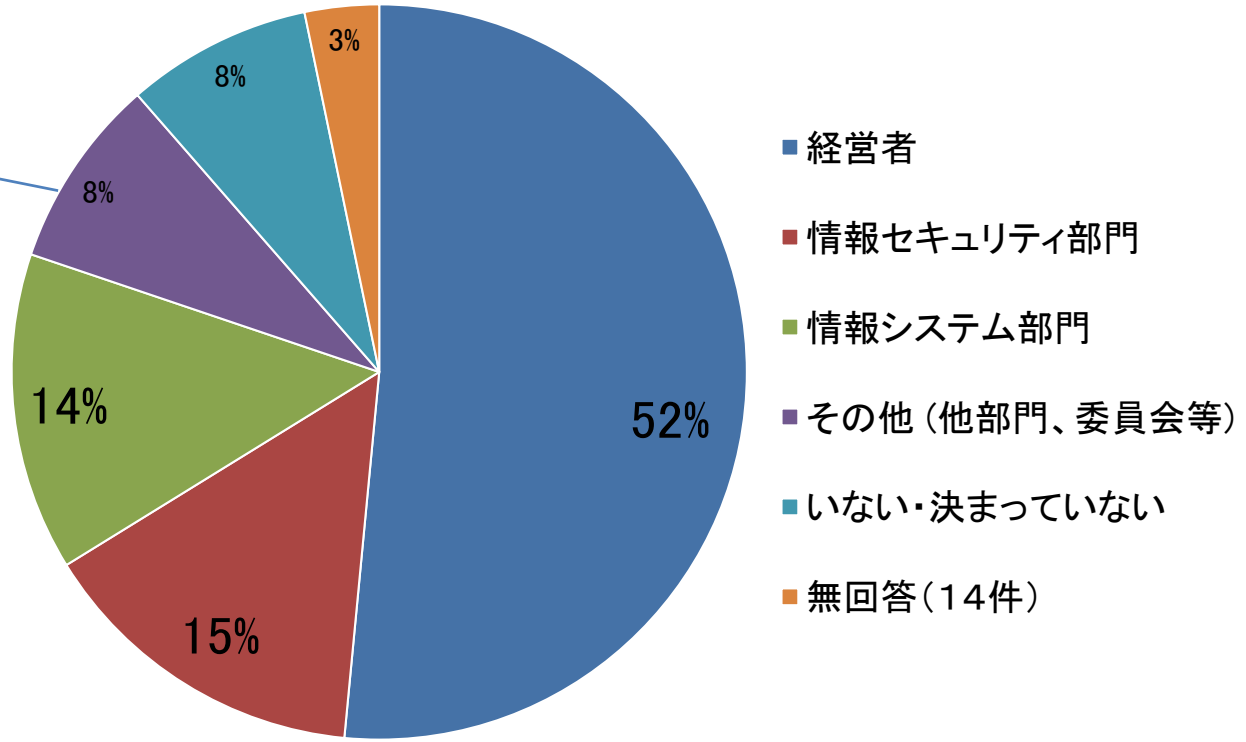
「情報セキュリティ」専任は63件（15%）で　第3位，兼務の場合の主務は，「情報システム」が87件（20%），「総務」が77件（18%），その他では，経営系，営業系が多い

第4章　情報セキュリティガバナンス体制

設問25-1　情報システム上の要請との対立時の判断部門（N=429）

その他（記述27件）

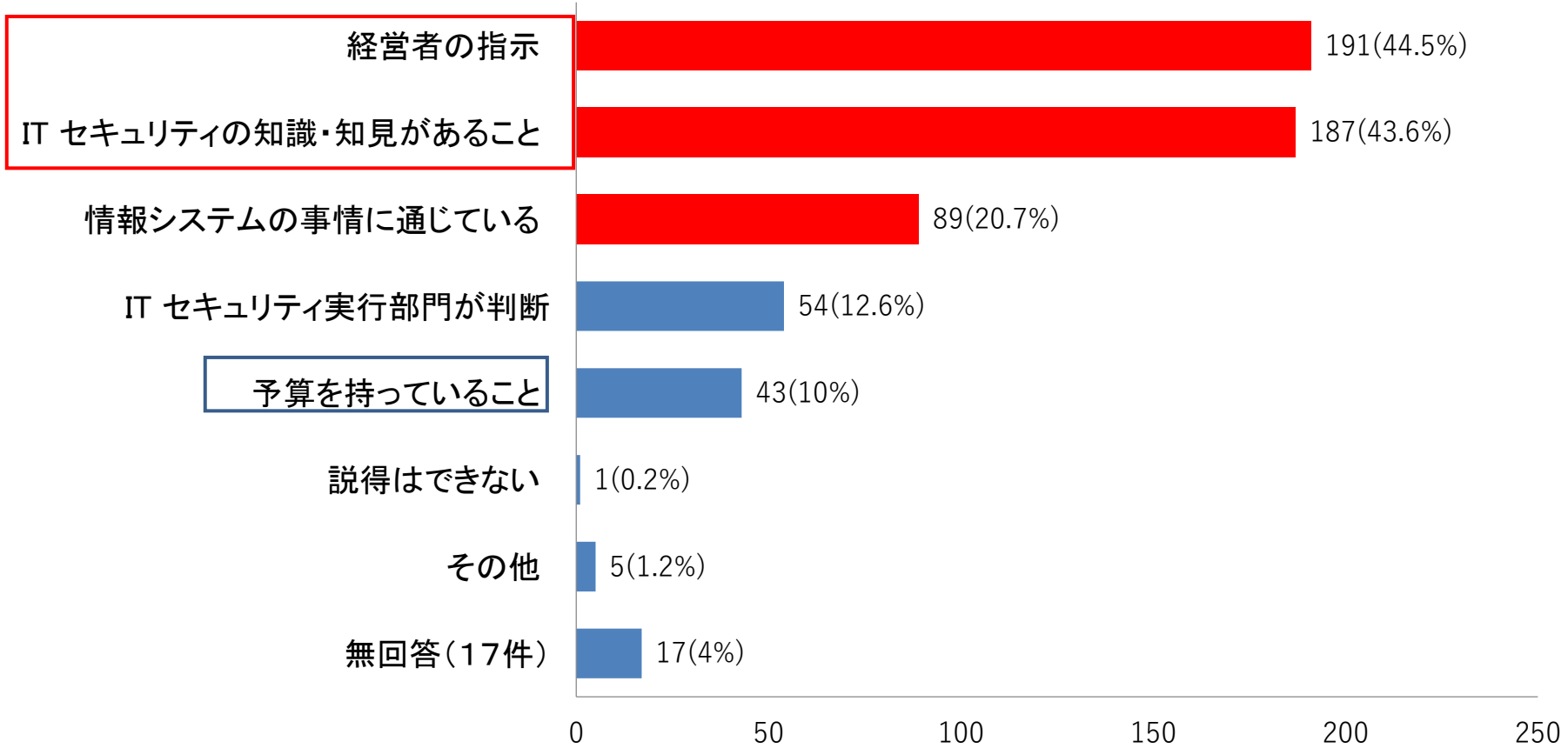
委員会・事務局　20件



過半数（52%）が「経営者」が判断している回答が最も多く，
「情報セキュリティ部門」が判断は15%，
「情報システム部門」が判断は14%であった

第4章　情報セキュリティガバナンス体制

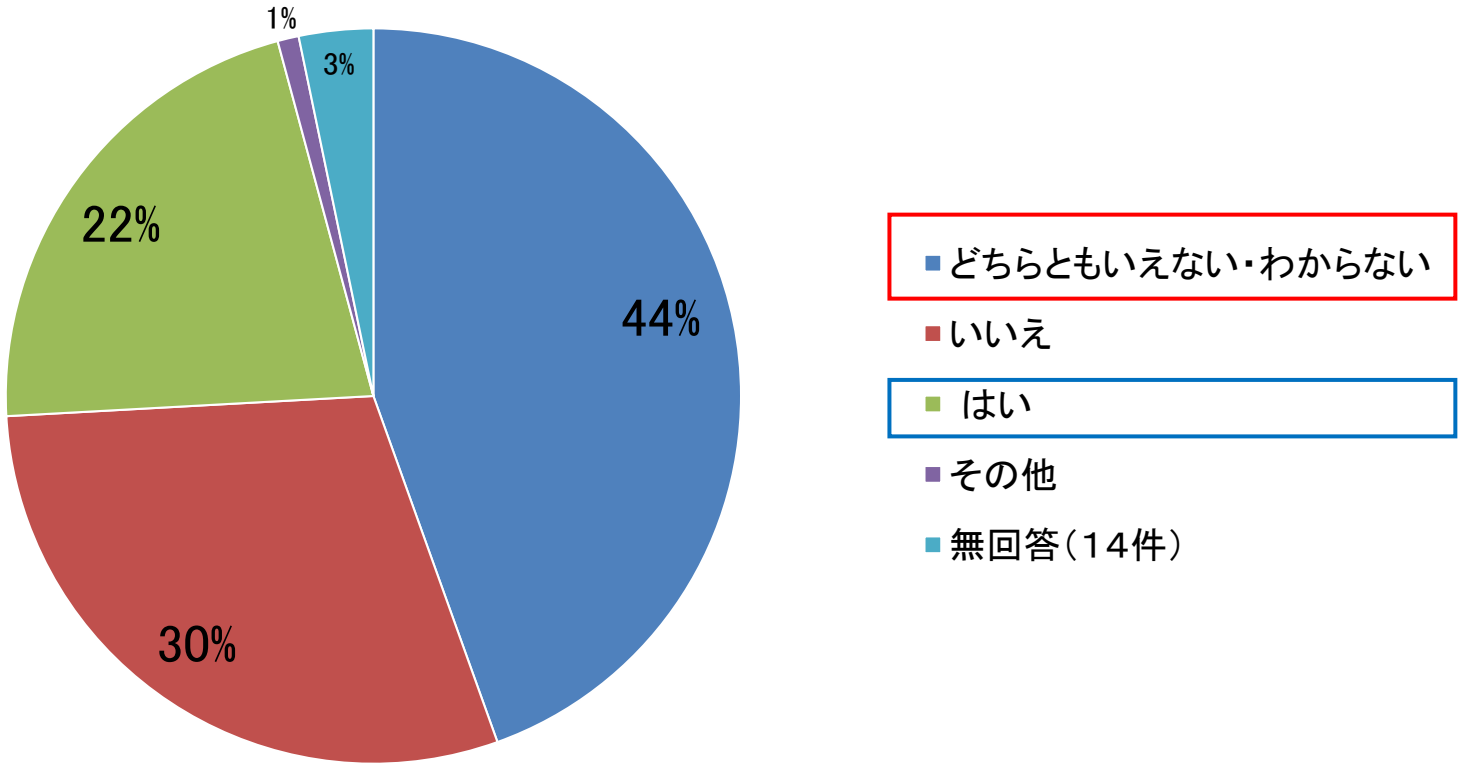
設問25-2　ITセキュリティ実行部門への説得に必要なこと（複数回答，N=429）



「経営者の指示」（191件）と「ITセキュリティの知識・知見があること」（187件）が実施部門の説得に必要が多く，「予算を持っていること」は案外少ない

第4章　情報セキュリティガバナンス体制

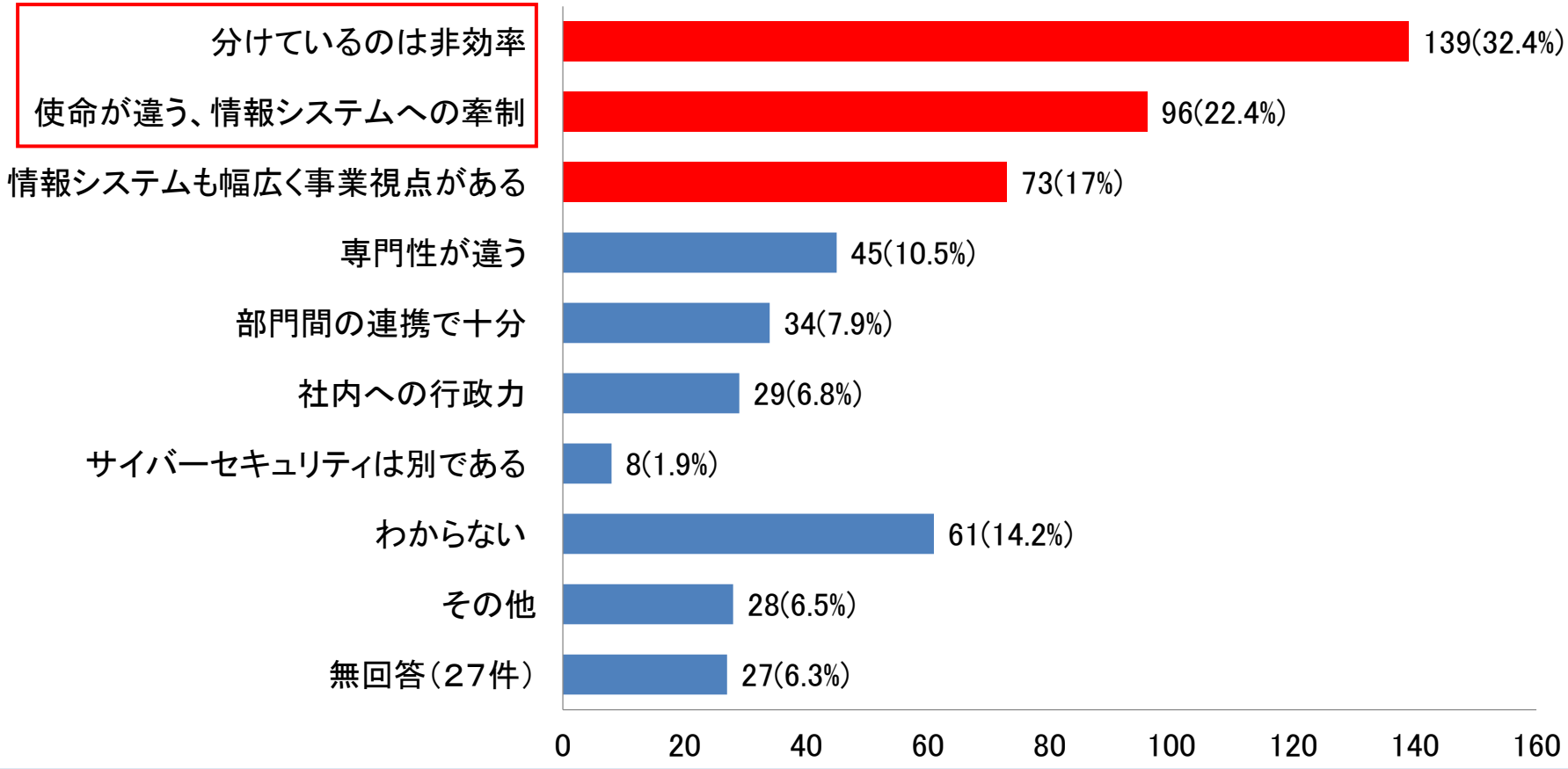
設問26-1　情報セキュリティ部門は情報システム部門から独立すべきか（N=429）



情報セキュリティ部門は独立すべきかについてはわからないが44%で最多，
独立すべきは22%を占め，
30%が情報システムが兼務すべきとの意見である

第4章　情報セキュリティガバナンス体制

設問26-2　情報セキュリティは独立すべきか否か，の理由（複数回答，N=429）



「分けているのは非効率」（139件）が最多で，
「使命が違う，情報システムへの牽制」（96件）が2位である

第5章
Webアプリケーションセキュリティ管理の状況

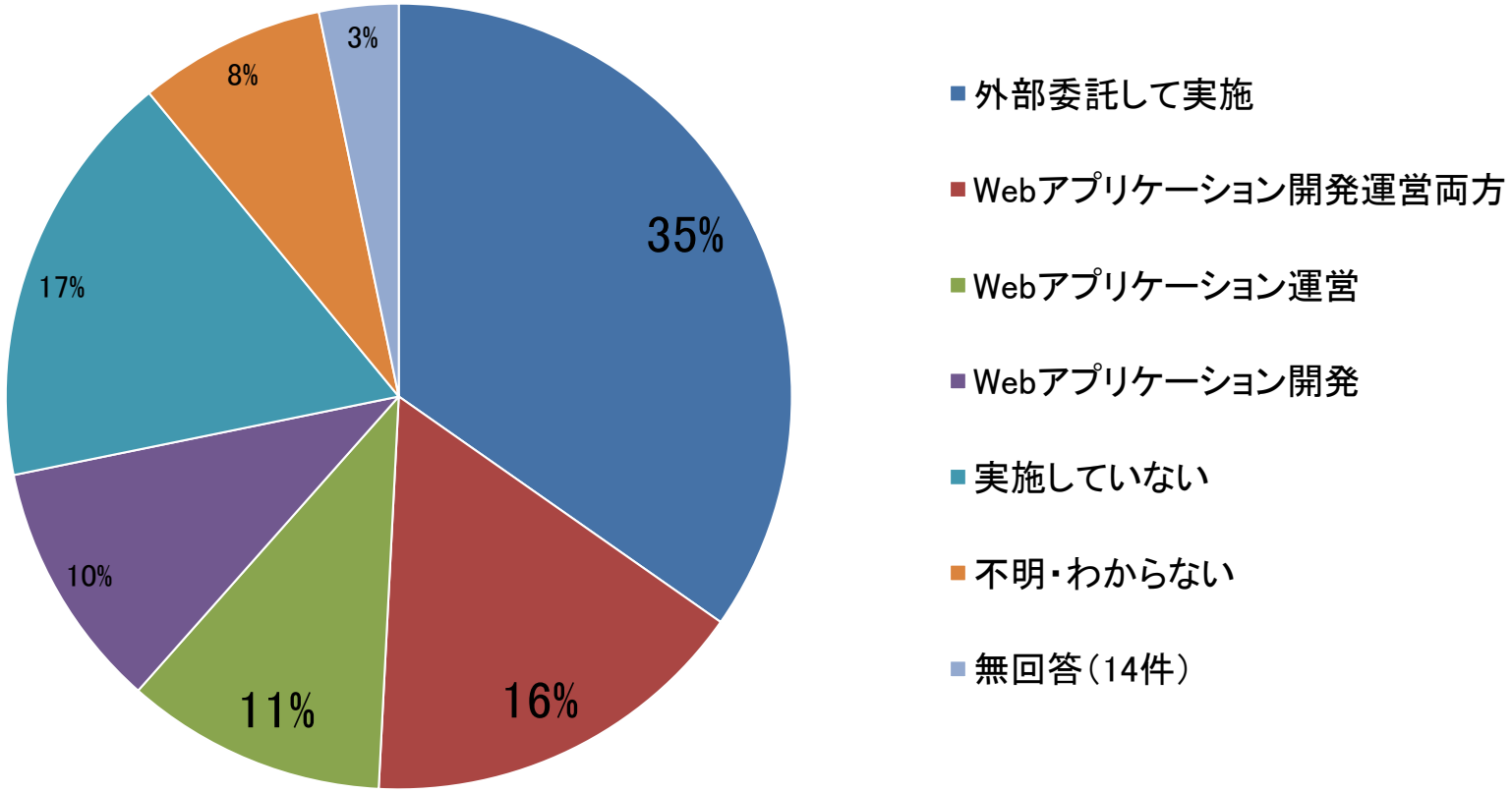
第5章　Webアプリケーションセキュリティ管理の状況

調査結果：

- 調査対象の35%の組織は，アプリケーションのセキュリティ管理を　外部に委託している
- 組織では“攻撃を受けたことがない”回答が最も多い，マルウェアに　よる攻撃の認知度が最も多い
- 開発段階の活動は“開発者向けのセキュアコーディング教育を実施”，“脅威の評価”を行っている
- 運用段階の活動は“ISMSなどの認証取得”，“ツールによる脆弱性診断”を行っている回答が最も多い
- アプリケーションセキュリティのリスク管理ができない理由として“専門知識の不足”と思われている
- 脆弱性発見時のレポートの手順がある組織は22%である

第5章　Webアプリケーションセキュリティ管理の状況

設問27　Webアプリケーションセキュリティの管理の組織の役割（N=429）

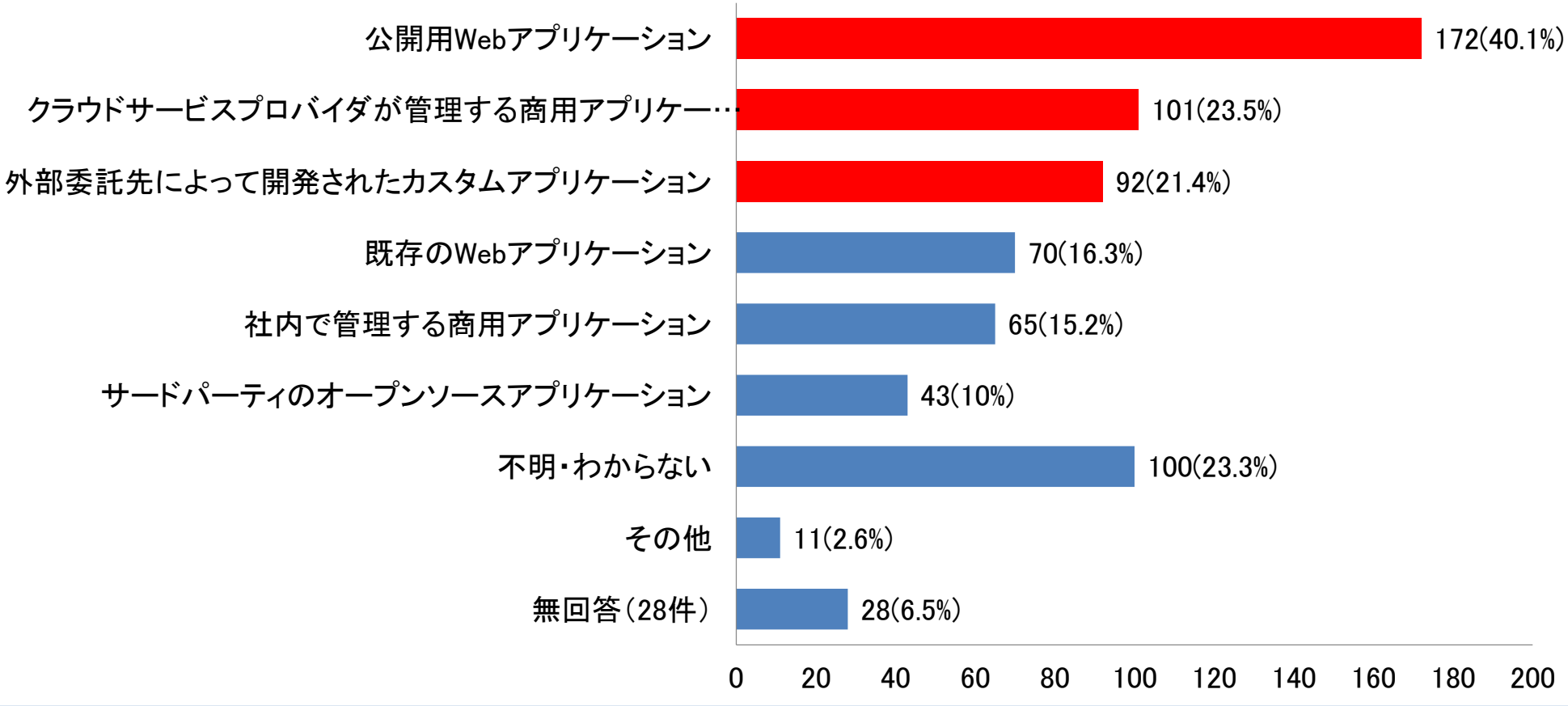


35%の組織は，アプリケーションのセキュリティ管理を外部に委託している

第5章　Webアプリケーションセキュリティ管理の状況

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

設問28　セキュリティ対策を適用しているWebアプリケーション（複数回答，N=429）

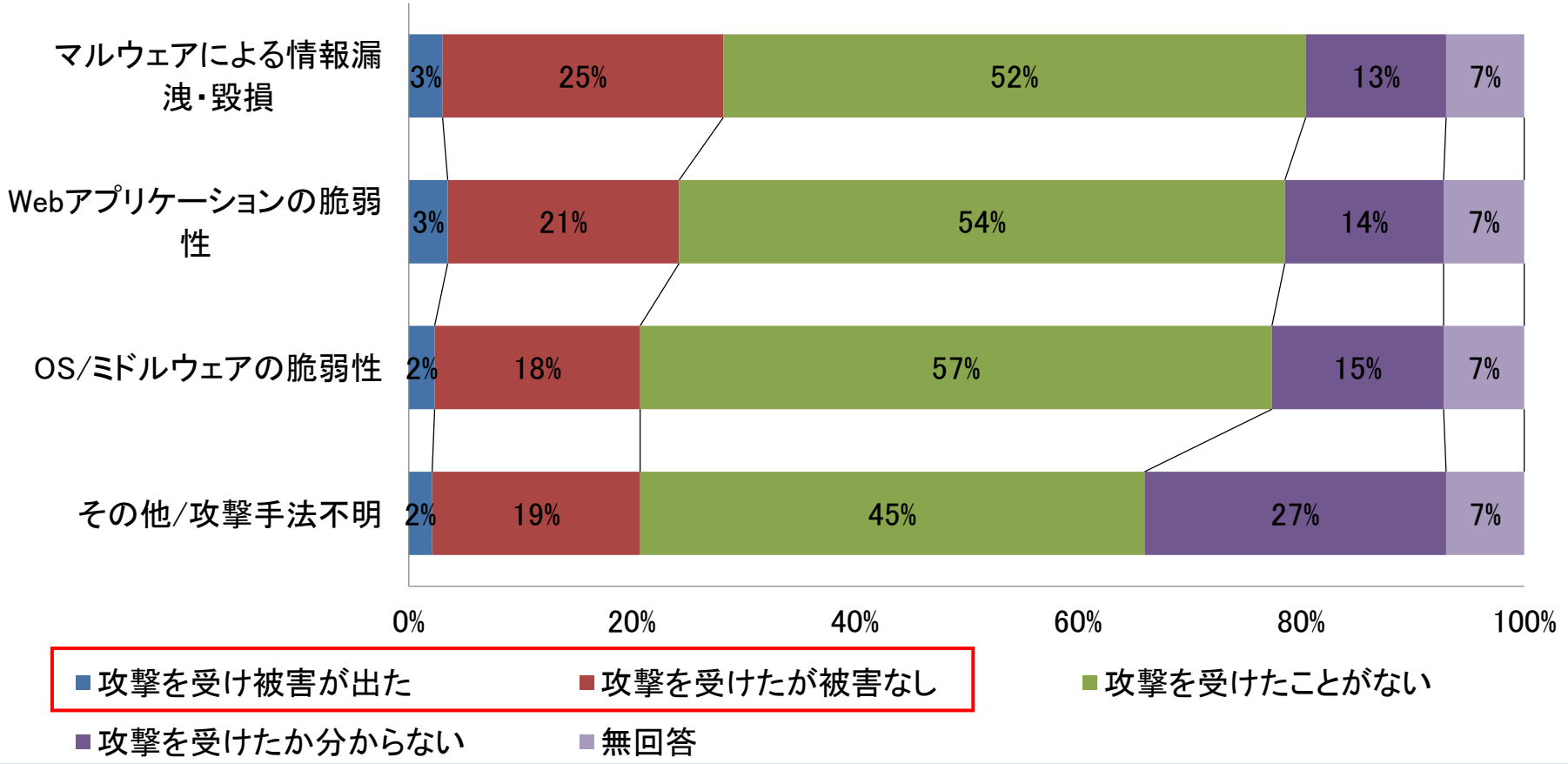


「公開用Webアプリケーション」のセキュリティ対策を適用している組織は172件で最も多く，クラウドサービスプロバイダ（101件），外部委託（92件）の順

第5章　Webアプリケーションセキュリティ管理の状況

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

設問29　攻撃と被害に対する認知度（N=429）

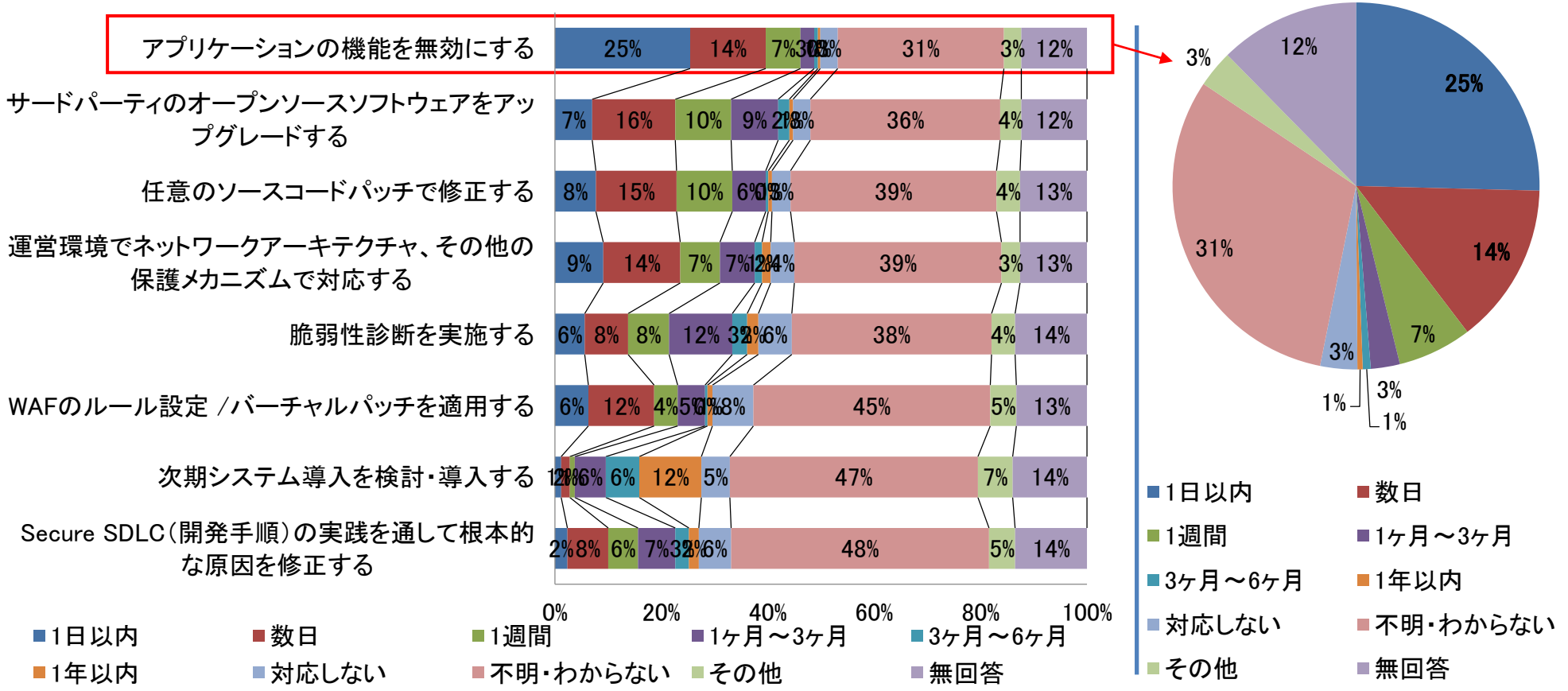


“攻撃を受けたことがない”回答が最も多い，マルウェアによる攻撃の認知度が一番高い回答である

第5章　Webアプリケーションセキュリティ管理の状況

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

設問30　セキュリティ対策と対処の平均所与時間（N=429）

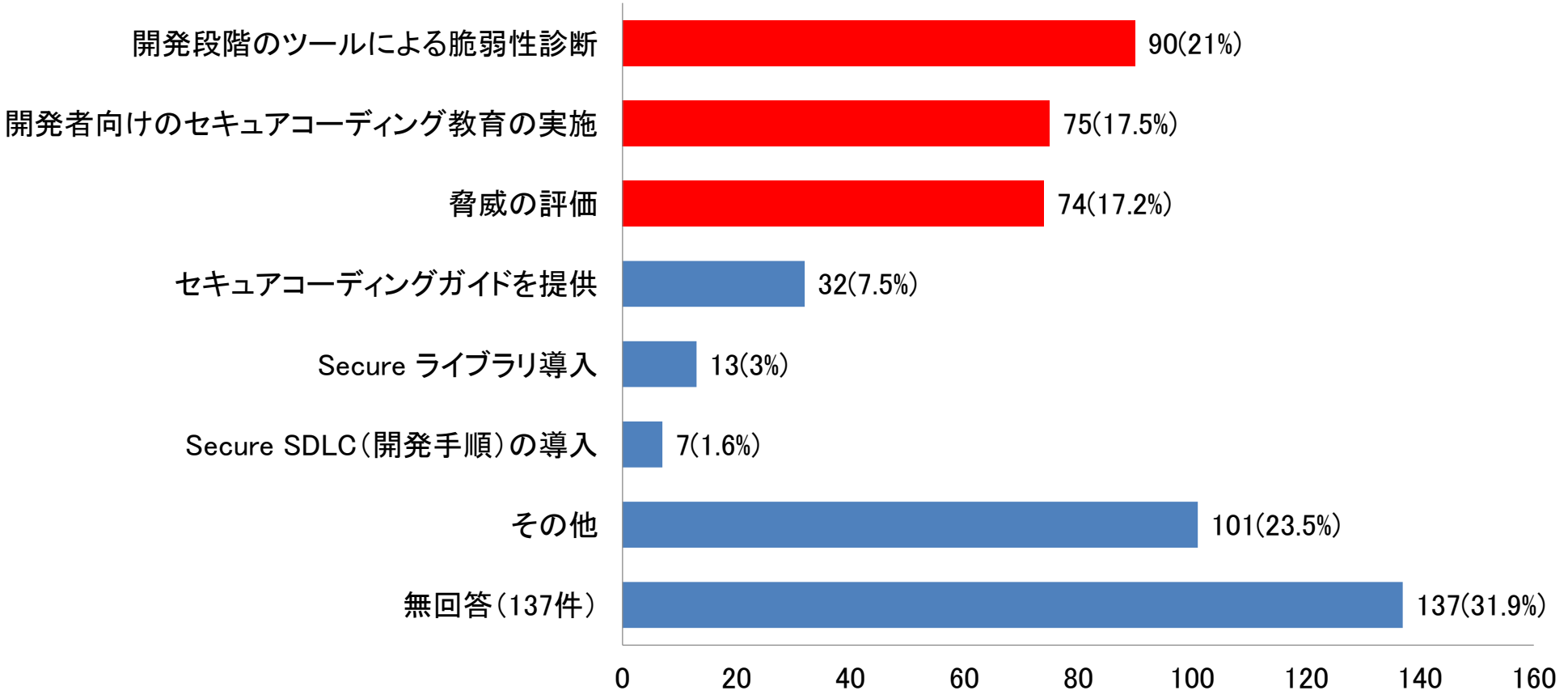


脆弱性が発見された場合に，“アプリケーションの機能を無効にする”という回答が最も多くその場合1日以内対応できることが25%ある

第5章　Webアプリケーションセキュリティ管理の状況

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

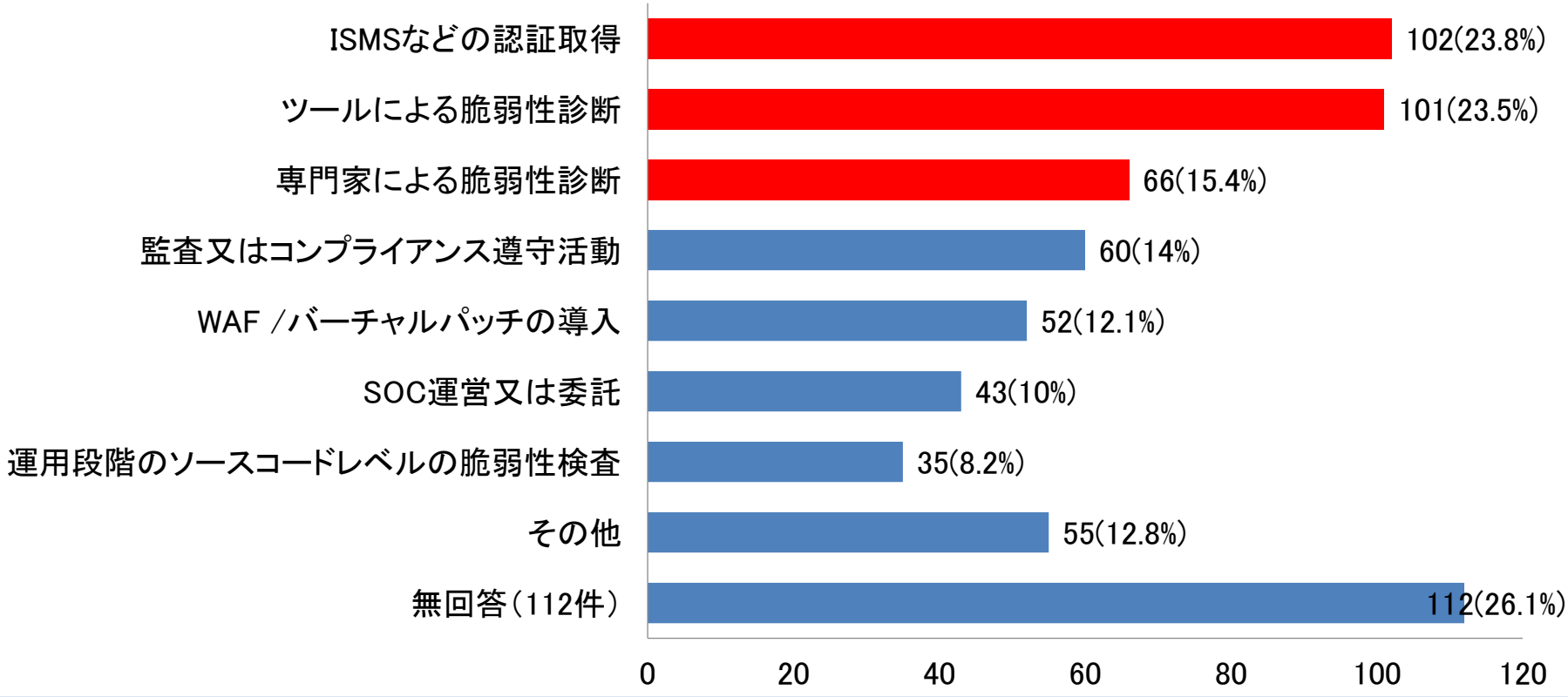
設問31　開発面の脆弱性のあるWebアプリケーションのリスク対策（複数回答，N=429）



開発段階の活動は「開発段階のツールによる脆弱性診断」「開発者向けのセキュアコーディング教育を実施」，「脅威の評価」を行っている

第5章　Webアプリケーションセキュリティ管理の状況

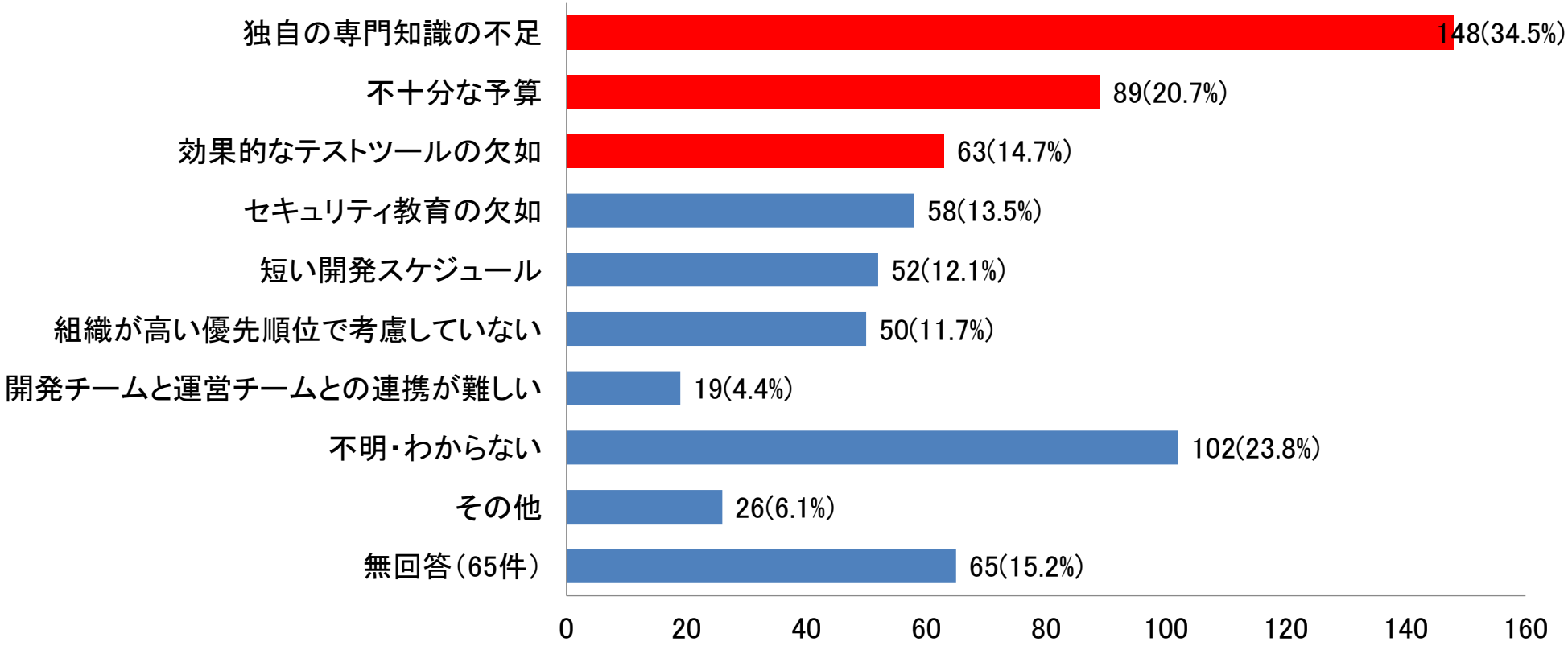
設問31　運用面の脆弱性のあるWebアプリケーションのリスク対策（複数回答，N=429）



運用段階の活動は，「ISMSなどの認証取得」，「ツールによる脆弱性診断」，「専門家による脆弱性診断」を行っている

第5章　Webアプリケーションセキュリティ管理の状況

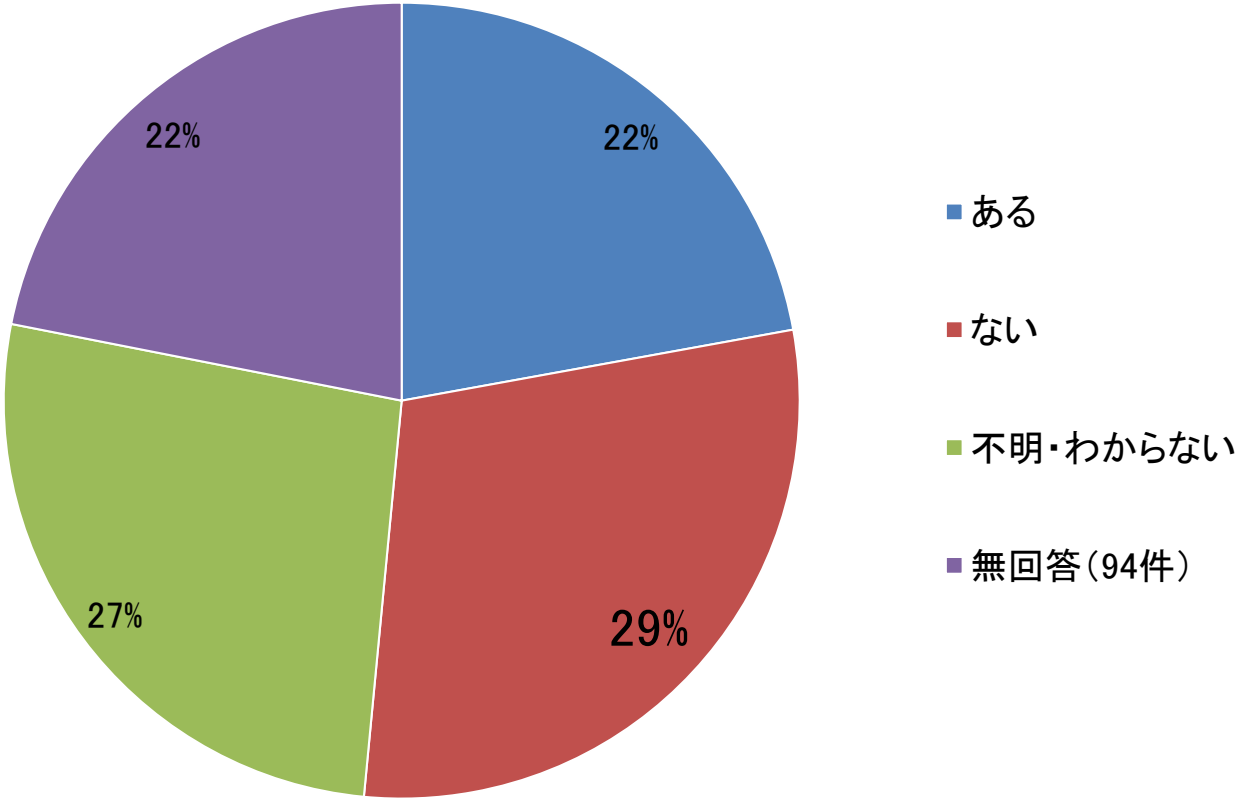
設問32　Webアプリケーションのセキュリティのリスク管理されてない理由（複数回答，N=429）



管理ができない理由として「専門知識の不足」（148件）と回答が最も多く，「十分な予算」（89件），「効果的なテストツールの欠如」（63件）の問題が挙げられている

管理の状況

設問33　脆弱性発見時の報告の手順の有無（N=429）



脆弱性発見時のレポートの手順がある組織は22%である

第6章
組織における人工知能（AI）技術の導入

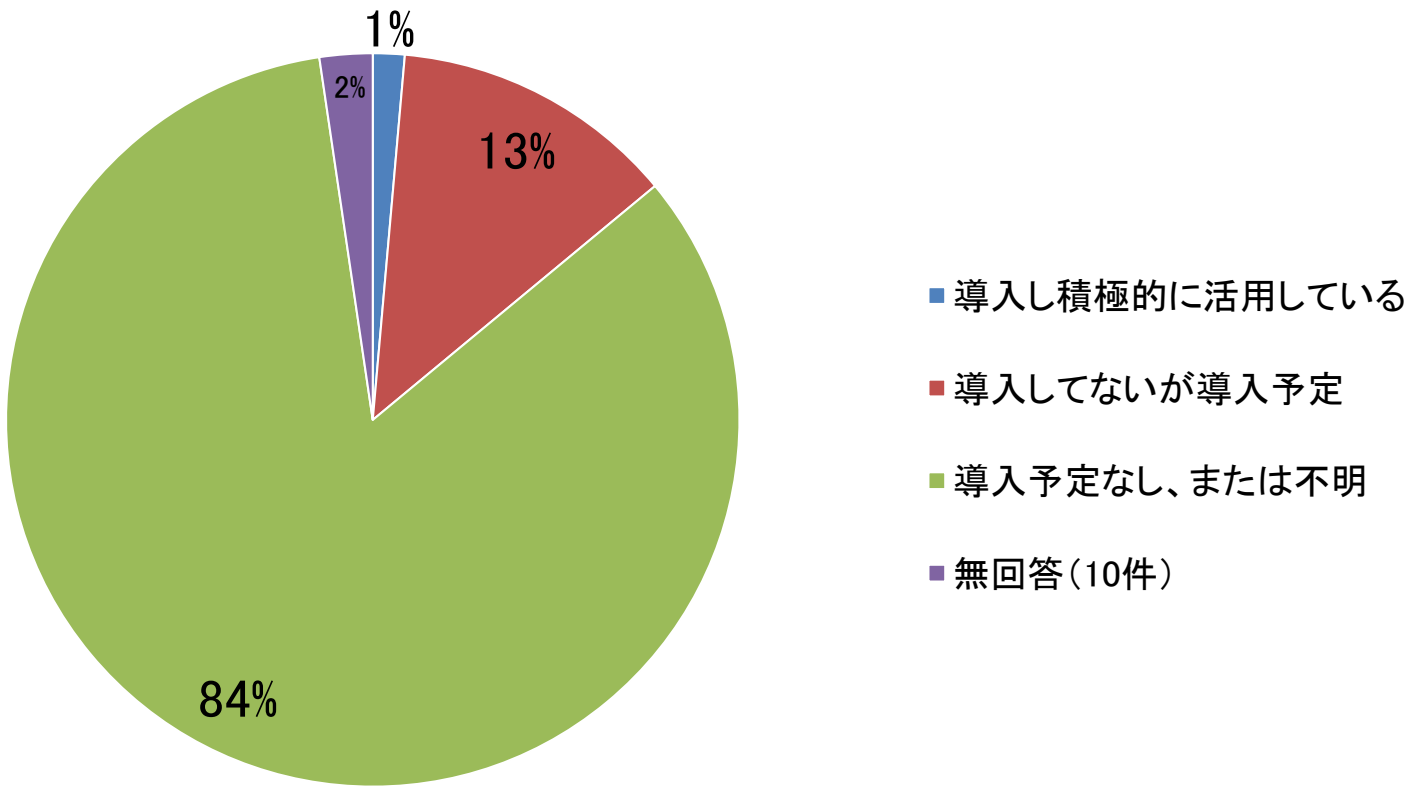
第6章　組織におけるAI技術の導入

調査結果：

- AI技術の導入状況については，導入予定がないもしくは不明と回答したものが圧倒的に多く，実際にはまだ導入している組織は少ない.
- AI技術を導入した利点としては，業務の自動化・効率化への回答が突出して多かったが，よくわからないとした回答も多いことから，AIの特徴がまだ明らかでない実態がわかる.
- AI技術の導入の具体的なリスクとしては，企業秘密の流出などの回答が多かったが，よくわからないと回答したものが圧倒的に多かった.
- AI技術の導入について，活用すべきとの回答よりも，よくわからないとの回答が上回り，AIに関する理解がまだ低いことが明らかになった.

第6章　組織におけるAI技術の導入

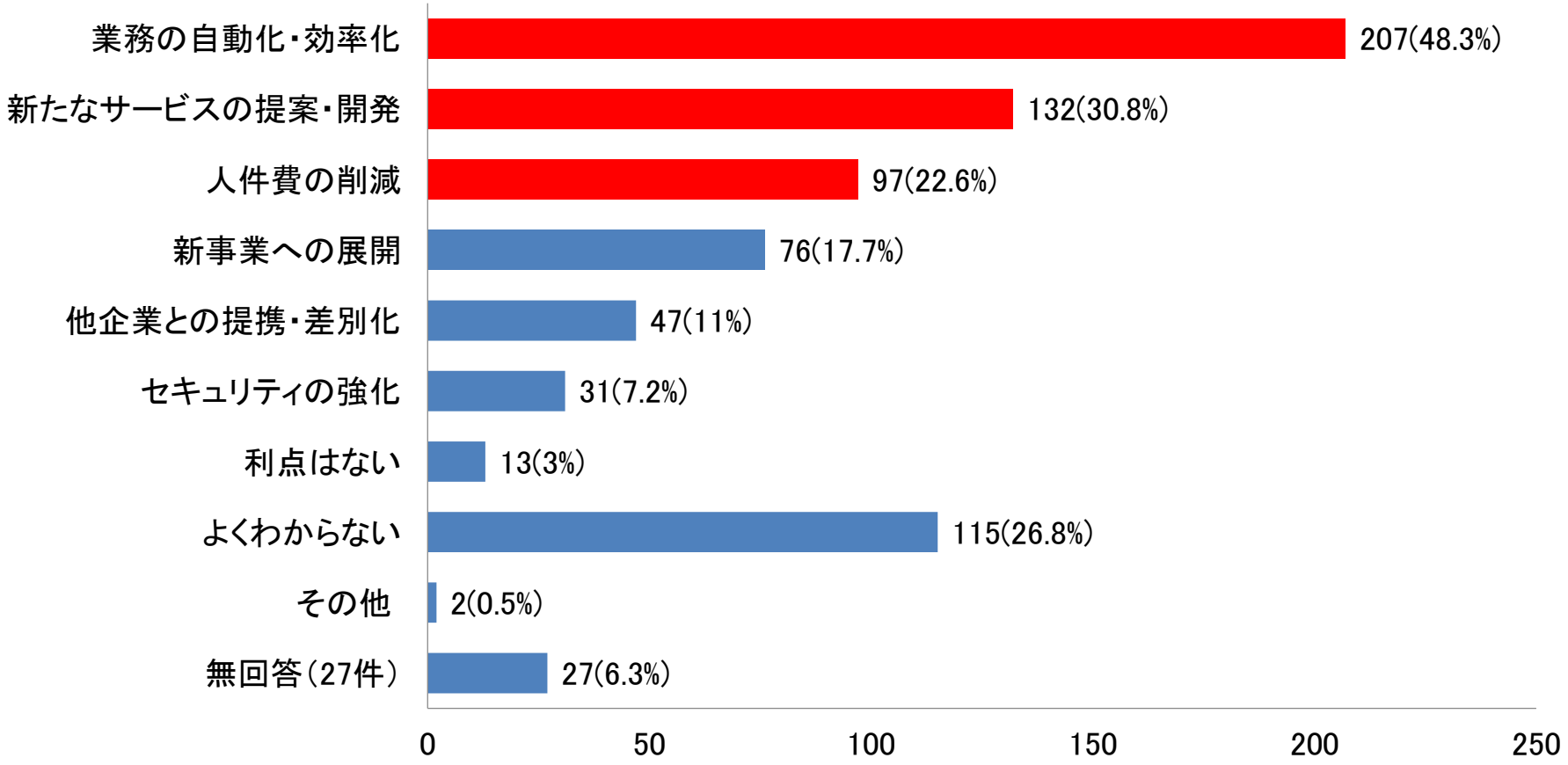
設問34　AI 技術の導入状況（N=429）



「導入予定がない，または不明」と回答したものが84%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6章　組織におけるAI技術の導入

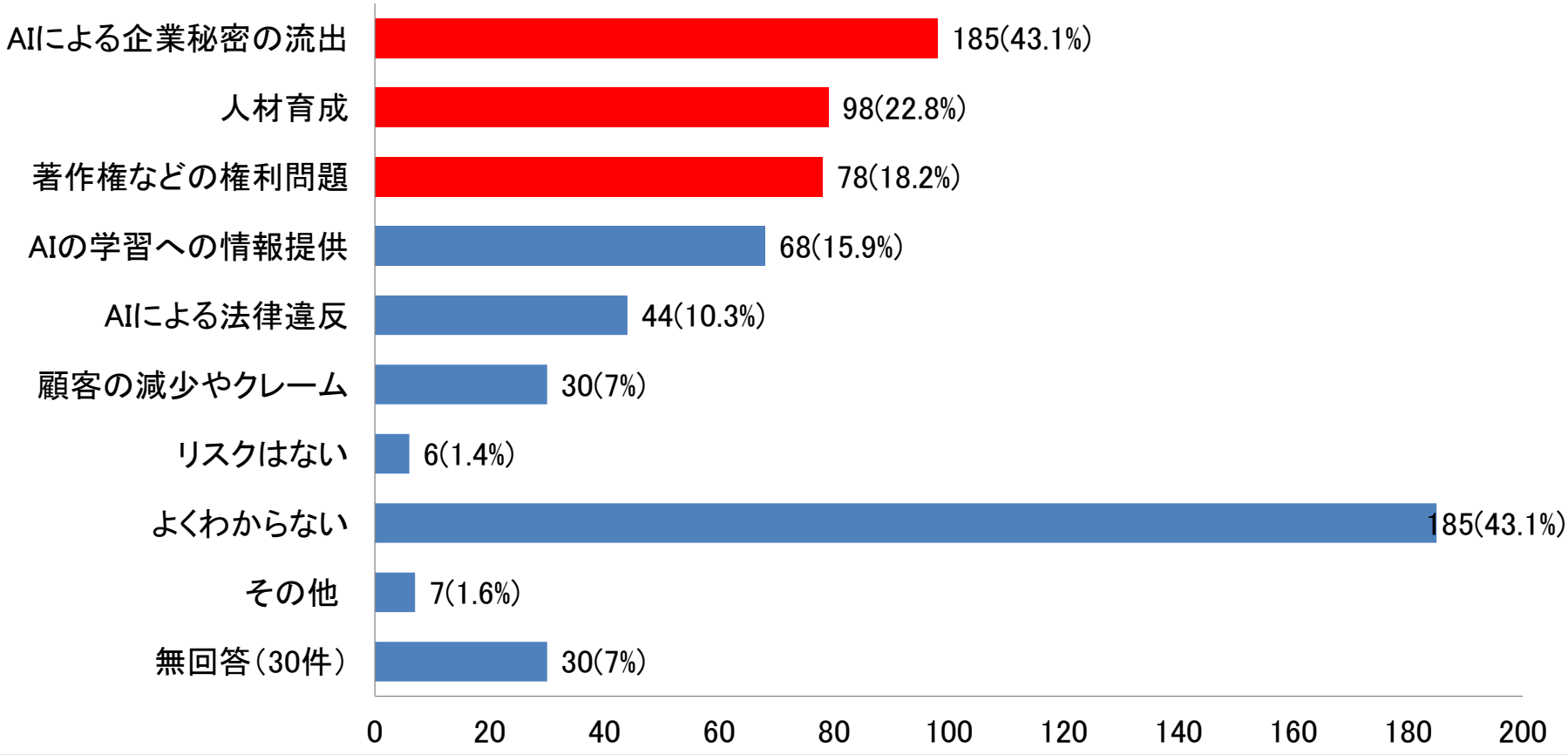
設問35　AI 技術を業務で導入した際の利点（複数回答，N=429）



「業務の自動化・効率化」（207件）と回答が最も多く，次いで「新たなサービスの提案・開発」（132件）「人件費の削減」（97件）が多い

第6章　組織におけるAI技術の導入

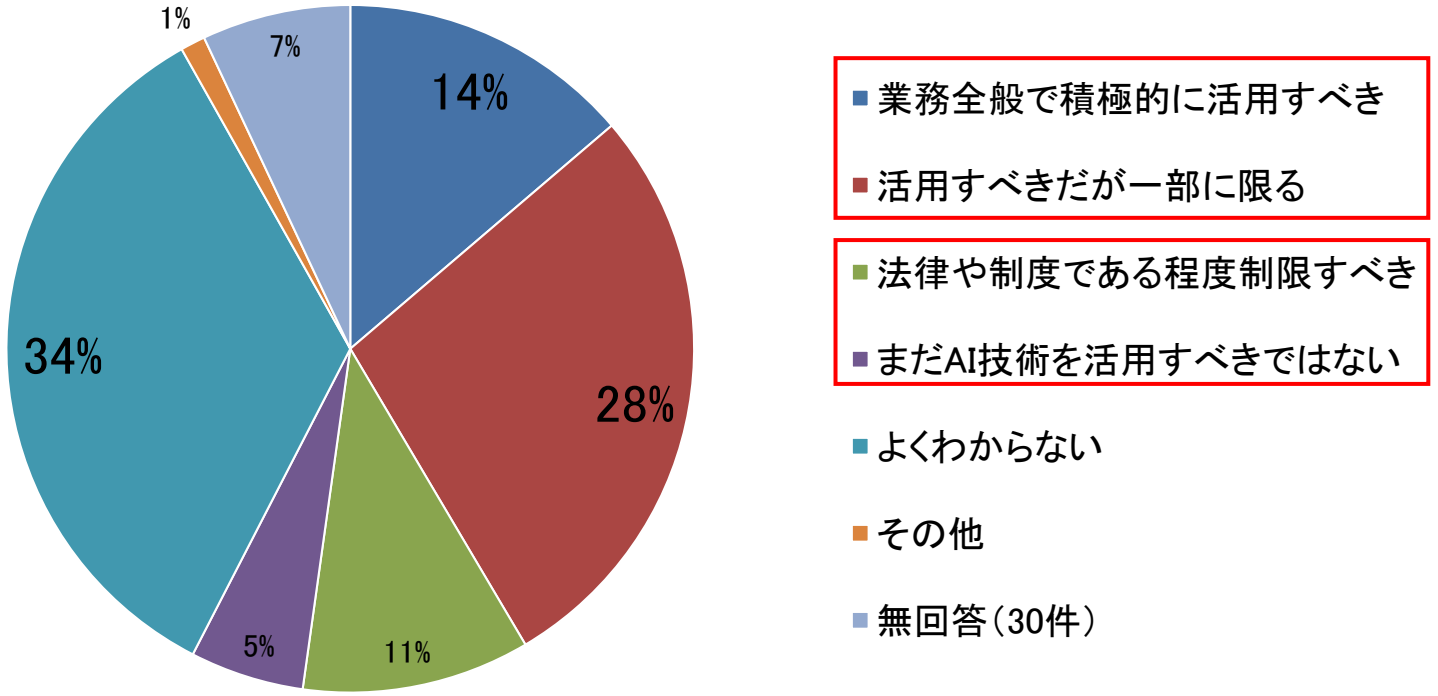
設問36　AI 技術を業務や他企業との提携で導入した際のリスク（複数回答，N=429）



「よくわからない」と回答したものが185件と圧倒的に多かった
具体的なリスクとしては「企業秘密の流出」（98件）が最も多かった

第6章　組織におけるAI技術の導入

設問37　AI 技術を業務に導入理由（N=429）



「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42%あり，「法律や制度である程度制限すべき」「まだAI技術を活用すべきではない」を合わせた回答16%で，AIを活用していく考えが多い
よくわからない（34%）との回答も多いことからAI活用への理解がまだ低い

第7章
緊急時対応の実効性

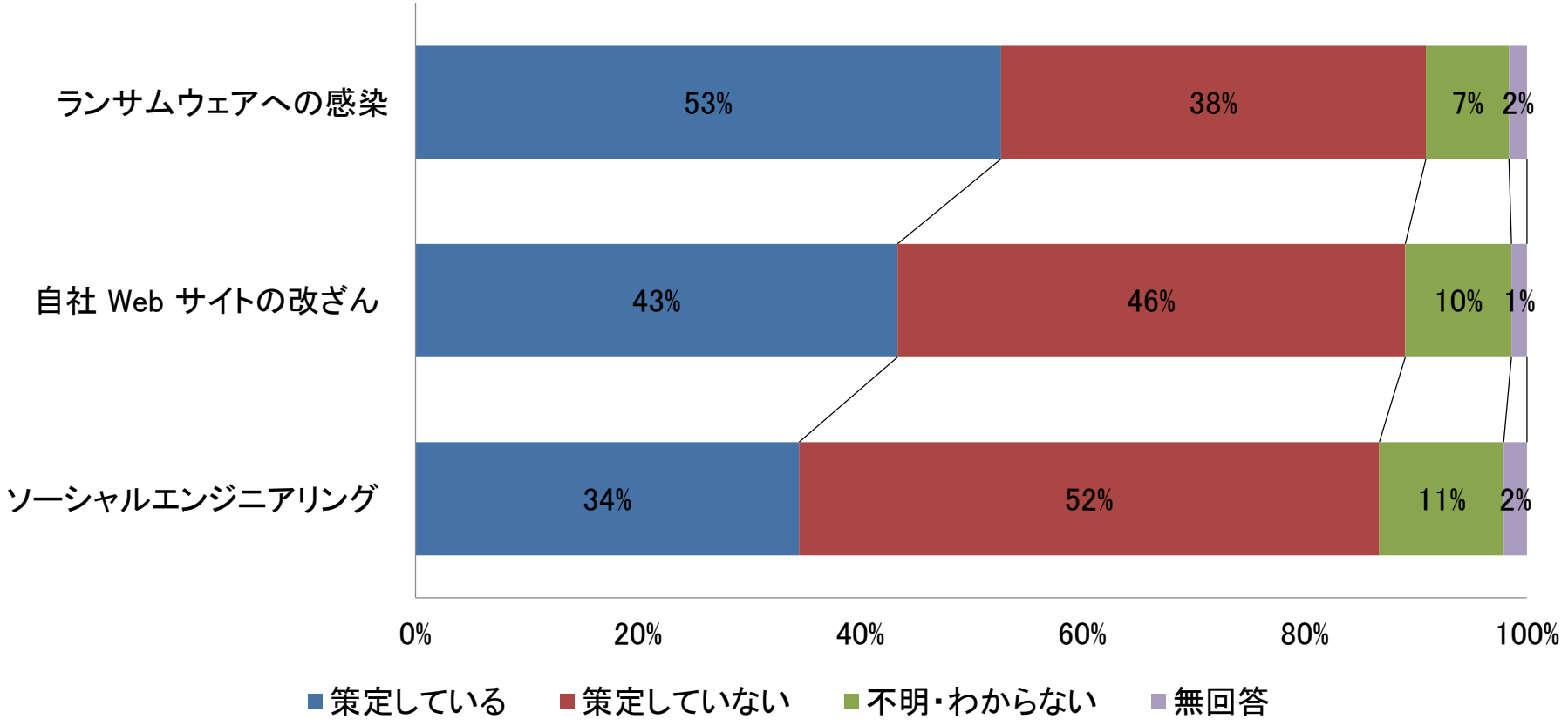
第7章　緊急時対応の実効性

調査結果：

- 自社 Web サイトの改ざん
  - 自社 Web サイトが不正に改ざんされていることを発見した
- ランサムウェアへの感染
  - 自分の PC がコンピュータウィルスに感染した全てのファイルが暗号化され操作不能となり，画面には「身代金」を要求するメッセージが表示されている
- ソーシャルエンジニアリング
  - 警察を名乗る男から「貴社のメールサーバーがハッカーに乗っ取られているので，セキュリティ担当者の氏名と連絡先を教えてほしい」と要請された（電話の相手が本物か確認できない）

第7章　緊急時対応の実効性

設問38　各状況を想定した／適用可能な文書（手順書等）は策定状況（N=429）

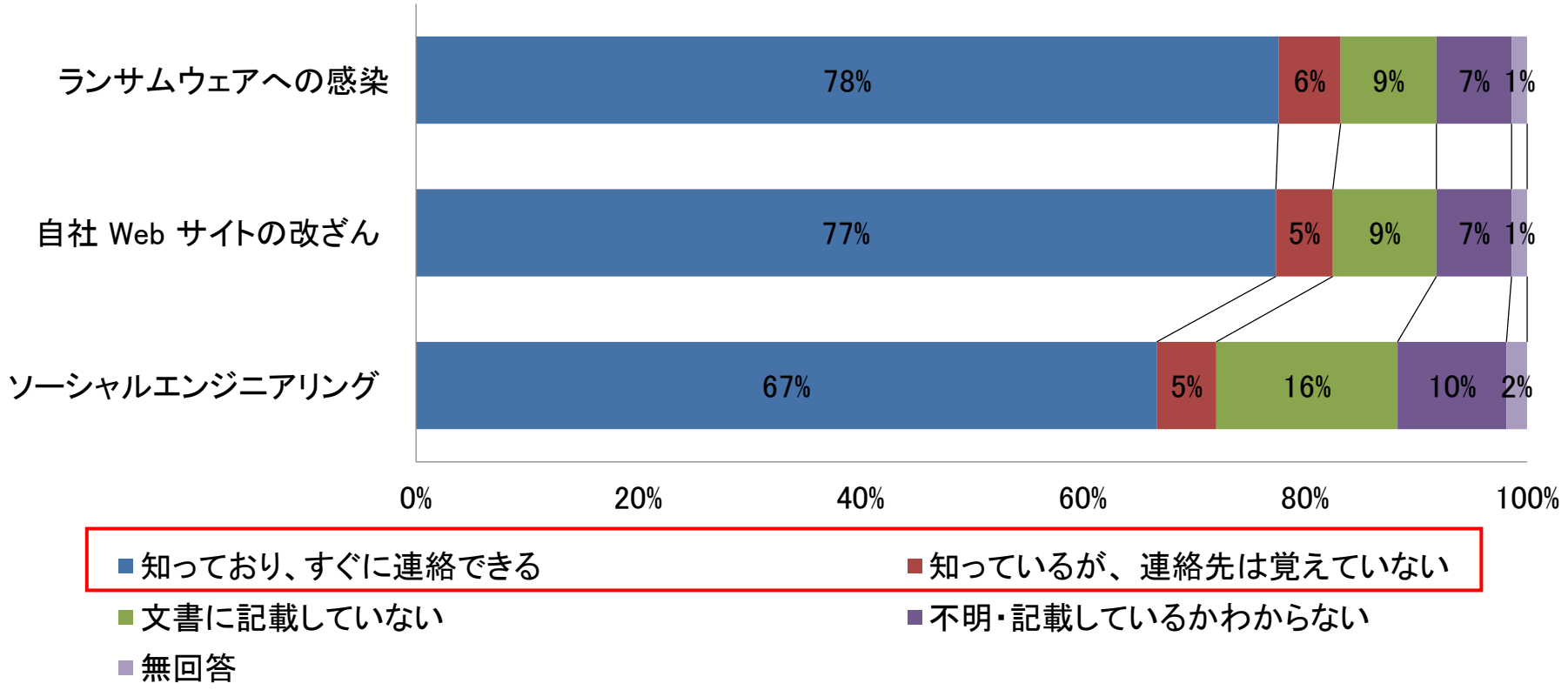


53%組織が，「ランサムウェアへの感染」に適用可能な文書を策定している
「ソーシャルエンジニアリング」でも34%以上の組織が文書を策定している

第7章　緊急時対応の実効性

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

設問39　緊急時対応の連絡先（N=429）

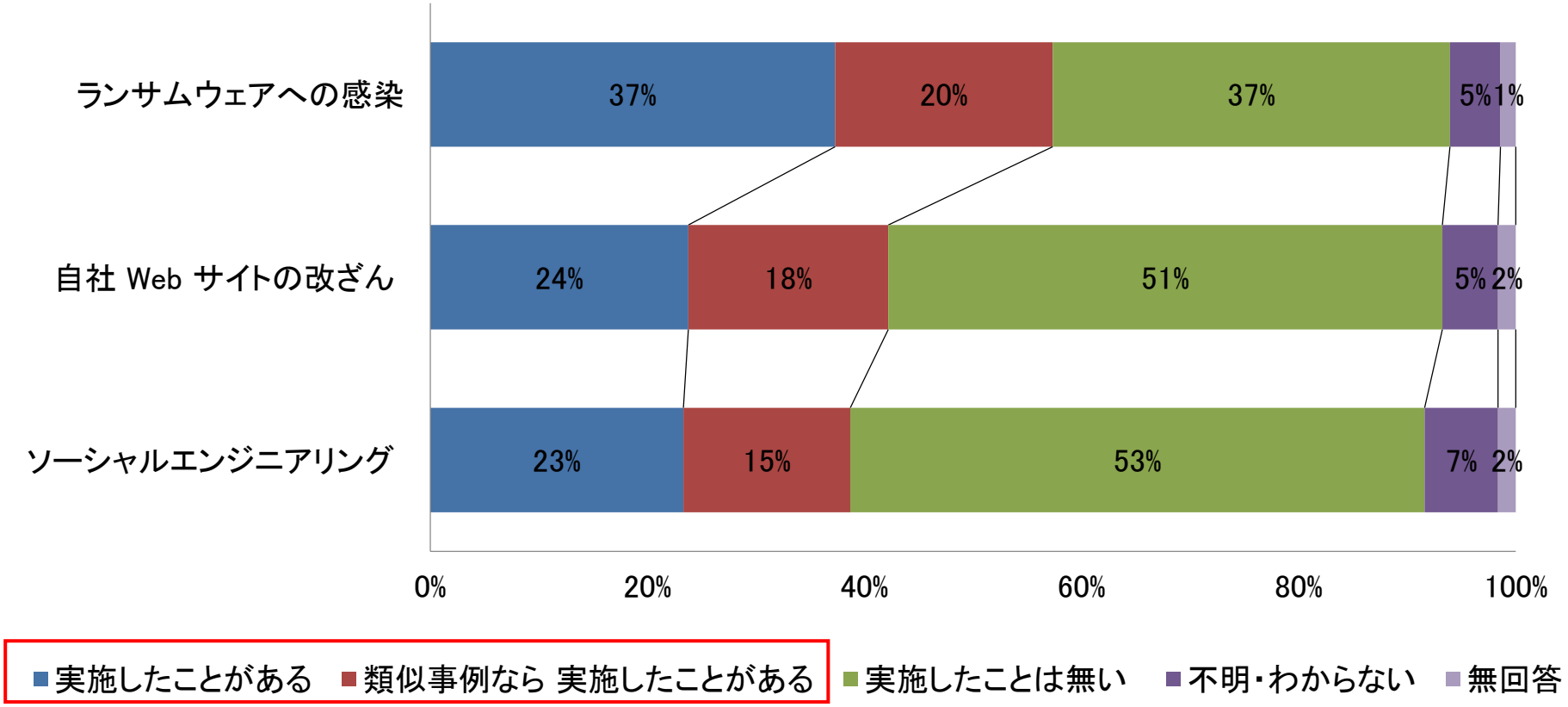


「ランサムウェアへの感染」，「自社Webサイトの改ざん」に関して，約8割以上の組織で連絡体制が構築されている．「ソーシャルエンジニアリング」についても，67%の組織で連絡体制が構築されている

第7章　緊急時対応の実効性

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

設問40　各状況を想定した教育・研修を実施（N=429）

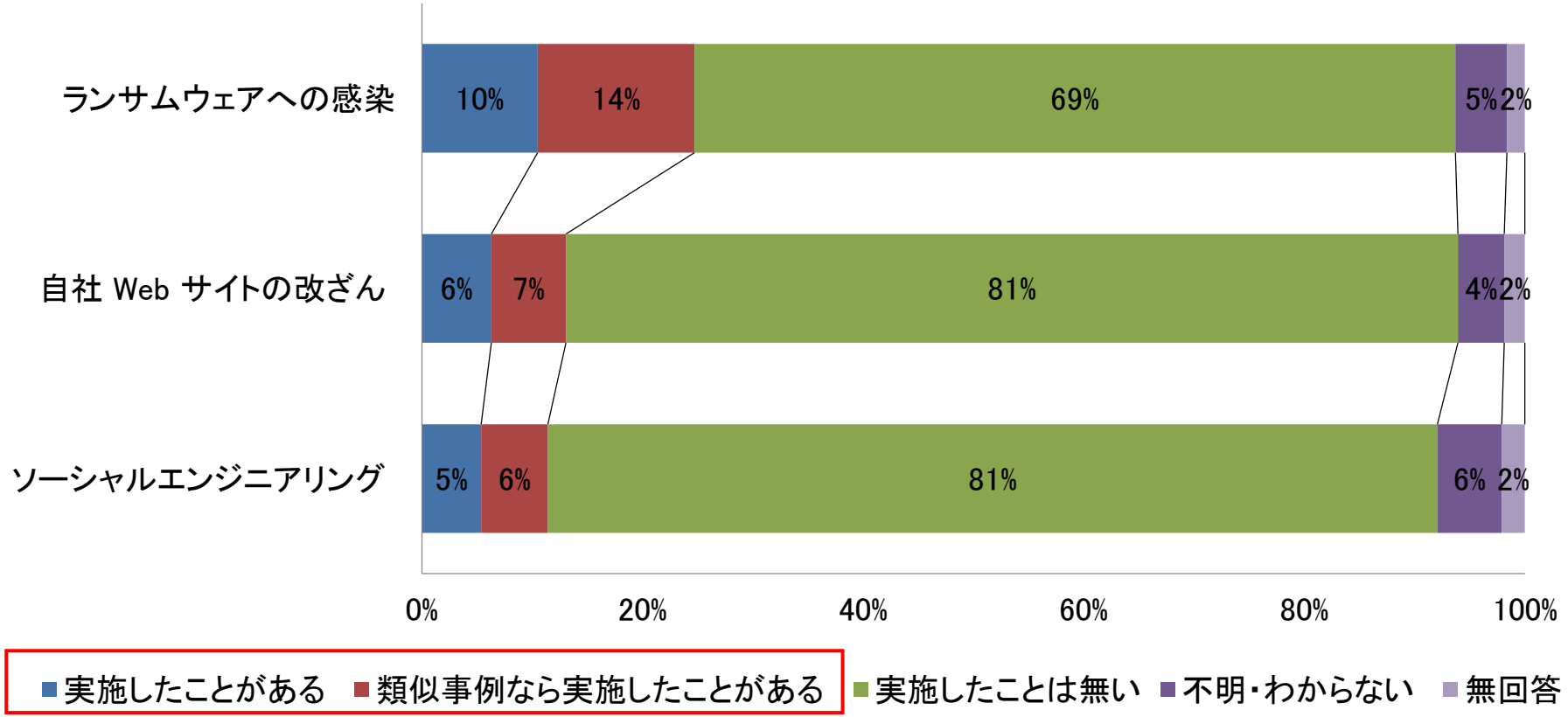


「ランサムウェアへの感染」については，57%の組織が教育・研修を実施している.「自社Webサイトの改ざん」,「ソーシャルエンジニアリング」についても38%の組織で教育・研修を実施している

第7章　緊急時対応の実効性

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

設問41　各状況を想定した訓練を実施状況（N=429）



ランサムウェアへの感染でも24%の組織しか訓練を実施していていない

第8章
情報セキュリティ人材に関する状況

第8章　情報セキュリティ人材に関する状況

調査結果：

情報セキュリティ技術者の有無

- 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技術者の必要性は認識していても，予算／人の確保が困難な状況であった

技術者育成ためのキャリアパス

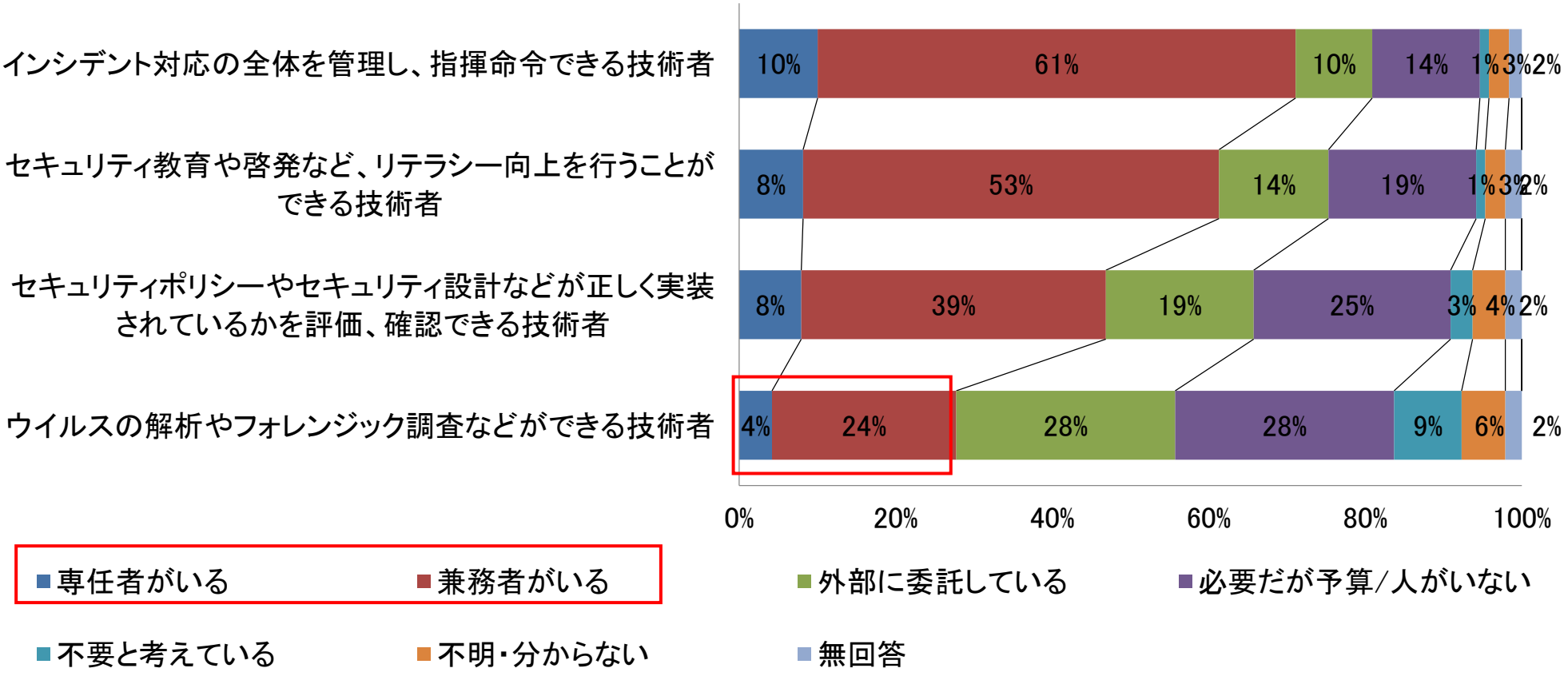
- 「決めていない」が74%で最も多く，「不明・わからない」の回答と合わせ92%を占めていたキャリアパスの必要性について認識が低い状況であった

必要と考えるスキル（知識・ノウハウ）

- 「情報セキュリティマネジメントに関する知識（ISMS 等）」が最も多く，”知識”の必要性を意識した回答が上位であった が最も多く，”知識”の必要性を意識した回答が上位であった

第8章　情報セキュリティ人材に関する状況

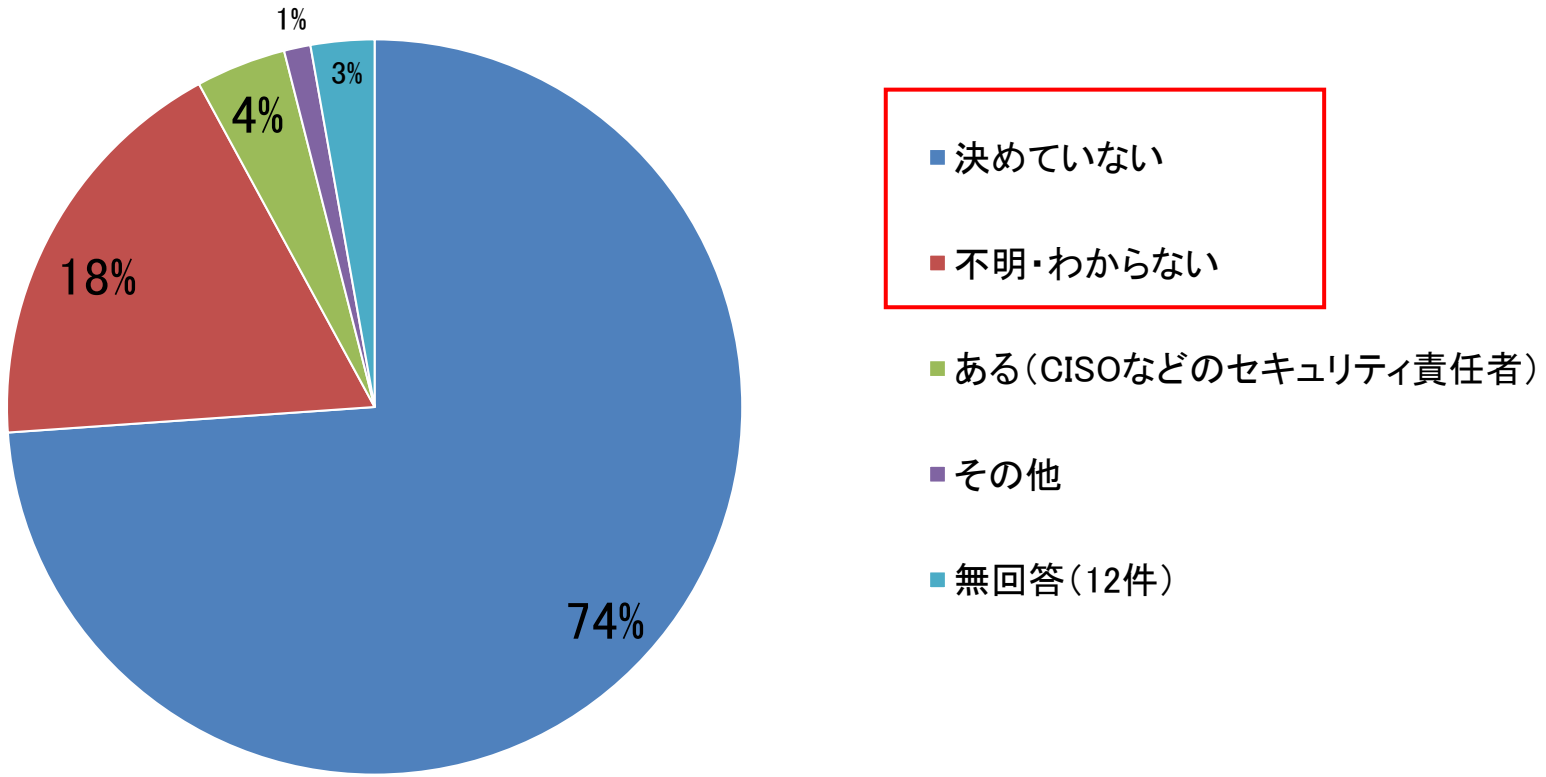
設問42　情報セキュリティインシデントに関わる業務の担当者（N=429）



「インシデント対応の全体を管理し，指揮命令ができる技術者」は専任または兼務者が多く，「ウイルスの解析やフォレンジック調査などができる技術者」専任または兼務者は少ない

第8章　情報セキュリティ人材に関する状況

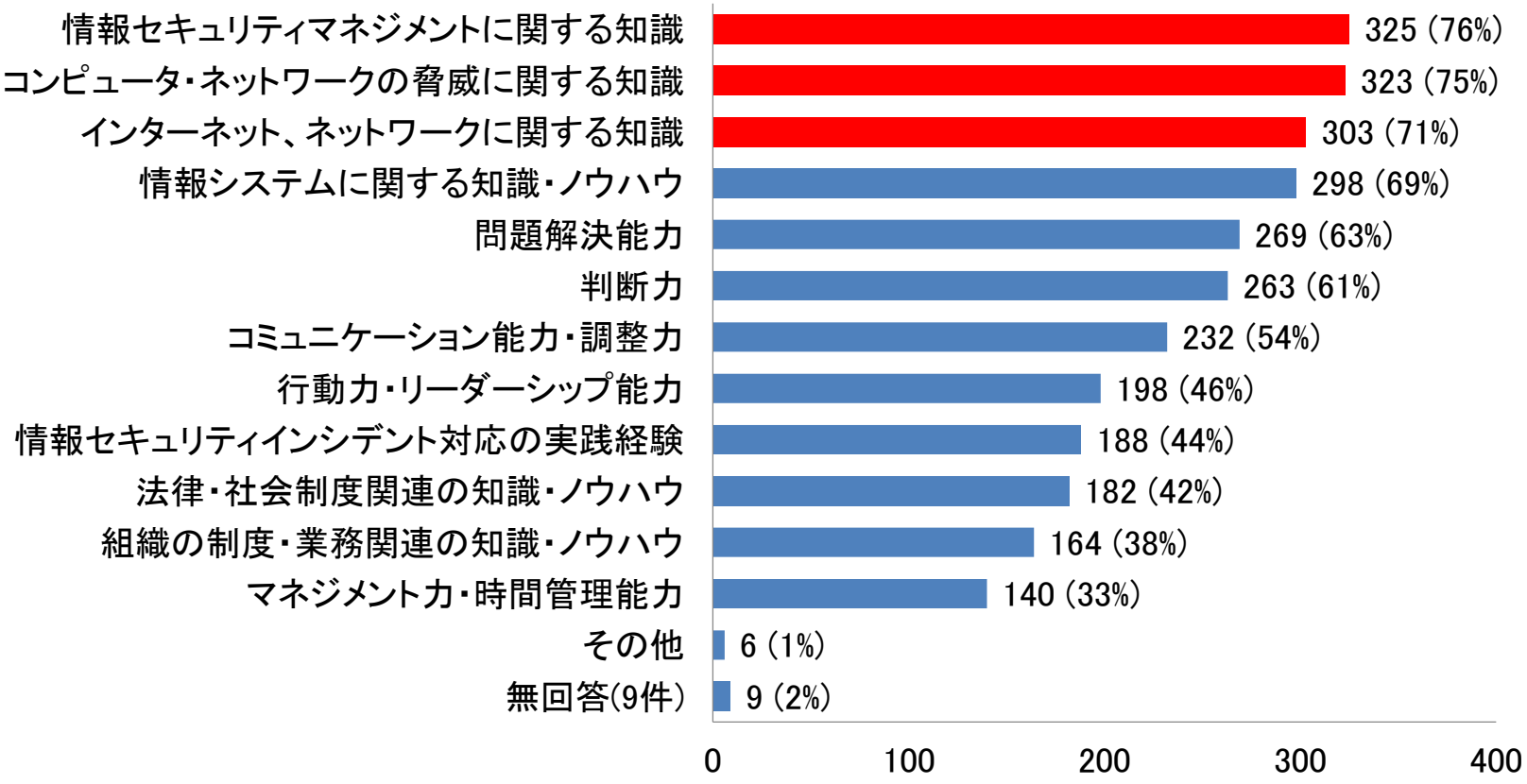
設問43　情報セキュリティ担当者を育成するためのキャリアパス（N=429）



「決めていない」が74%で最も多く，「不明・わからない」の回答と合わせ92%を占めている

第8章　情報セキュリティ人材に関する状況

設問44　情報セキュリティ業務の担当者に必要なスキル（複数回答，N=429）



必要なスキルとして情報セキュリティマネジメントコンピュータ・ネットワークの脅威，インターネット・ネットワークに関する知識の順である

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

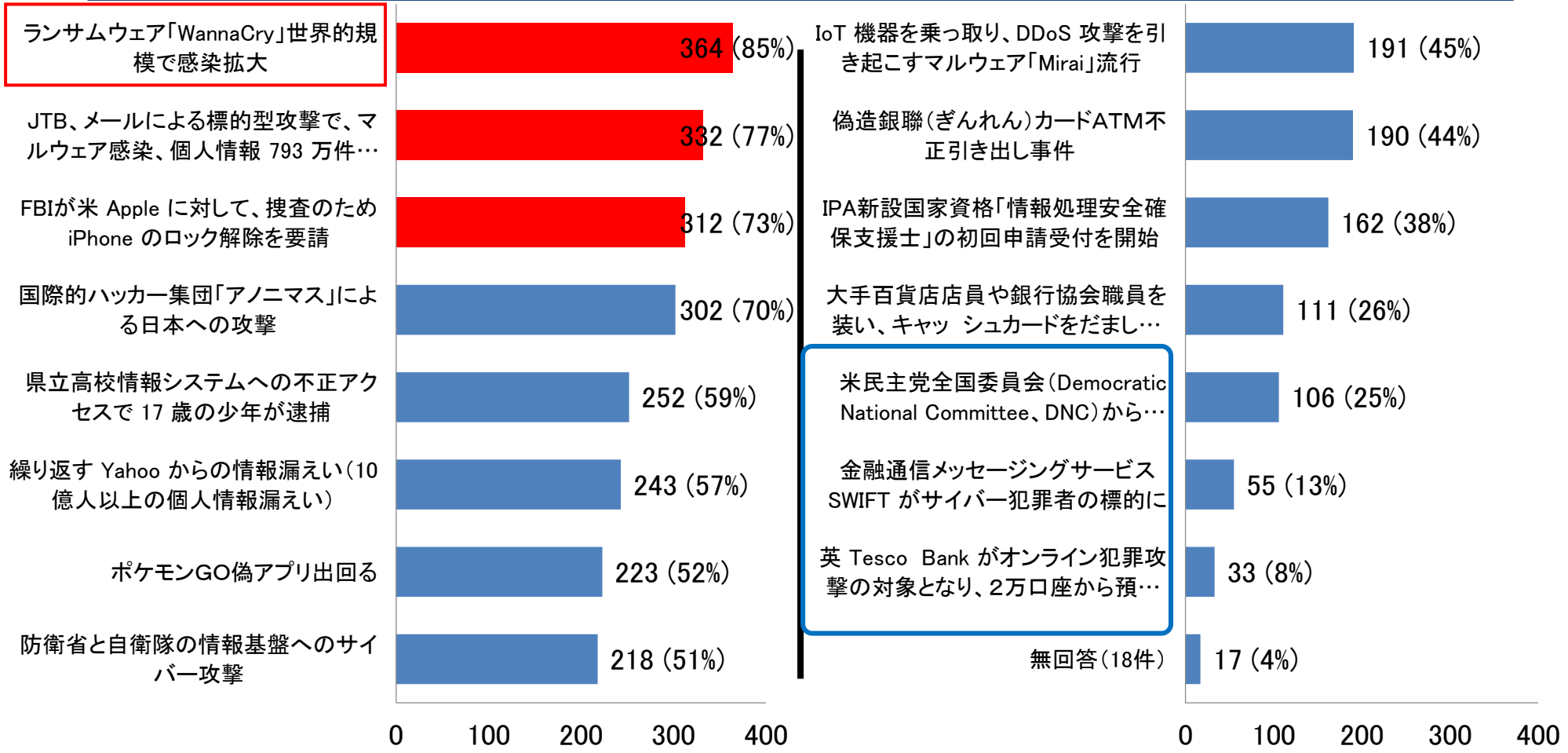
調査結果：

- 過去の事例、事故
  - アンケート調査前に猛威を振るったランサムウェア「WannaCry」が１位。約９割の組織で「知っている」と回答。
  - 海外の出来事については、世界的には大規模で大被害を被った事件でも、認知度は低かった。
  - 個人情報流出やスマートフォンのロック解除といった、個人情報やプライバシーに関する事件・事故が、上位にランクイン。
- 用語
  - 今回は「匿名加工情報」が認知度第１位(55%)
  - 「ディープラーニング」（前回は「機械学習」は9位) が2位となる
  - 前回は認知度7位だった「WAF(Web Application Firewall)」も3位(45%)となる。
  - 過去の事件、事故では「ランサムウェアWannaCry」の事件が１位であったが、その原因である「SMB V1の脆弱性」については、認知度は今一つ。認知度12位（12%）となる。

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=429）

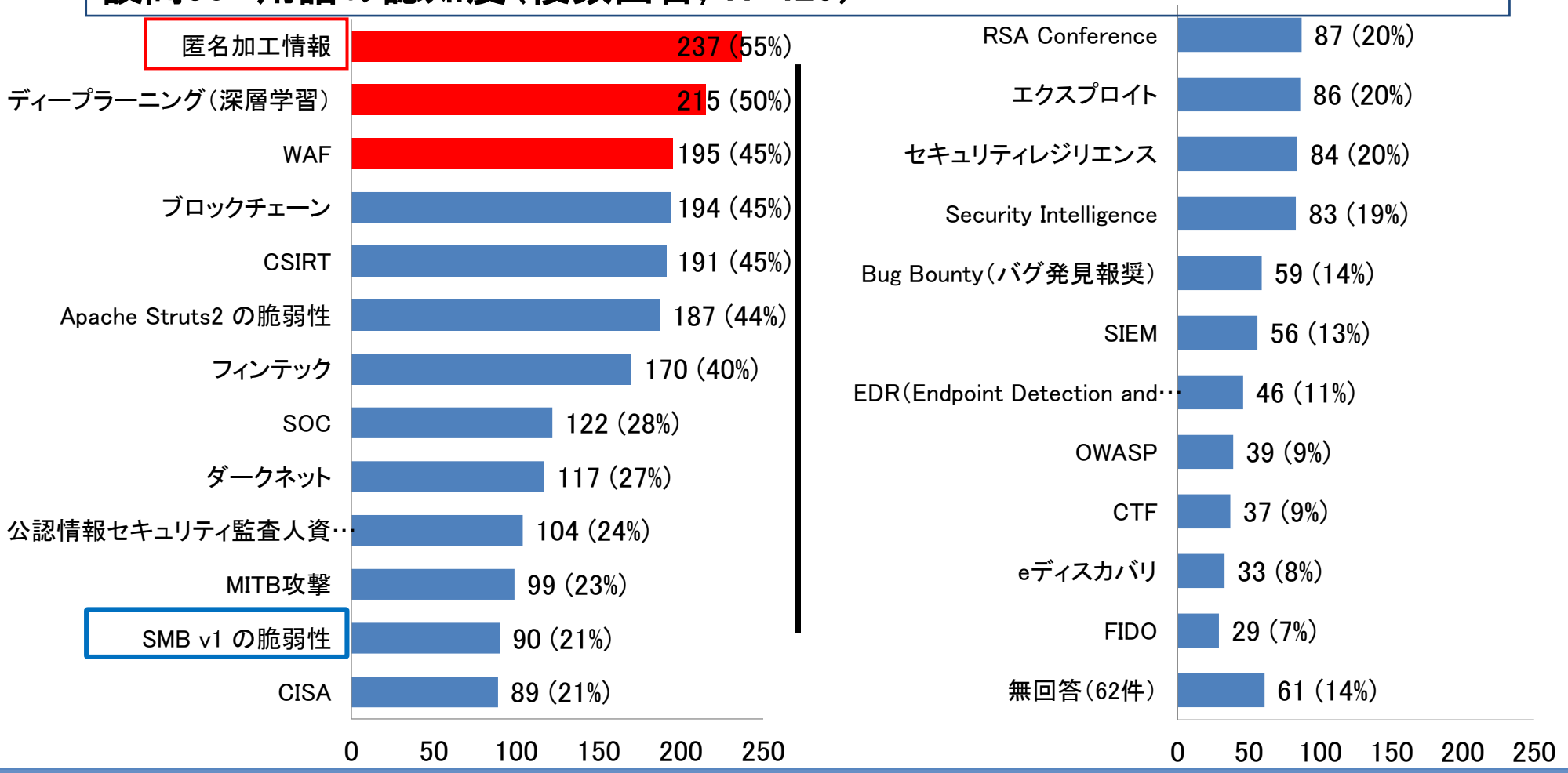


ランサムウェアWannaCryが1位。
海外の出来事は、大規模でも認知度が低い結果に。

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=429）



匿名加工情報が1位。出来事では1位のWannaCry、しかし原因であるSMB v1の脆弱性の認知度は中位に。

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
  - 神奈川県立鶴見養護学校　岸根分教室
  - 神奈川県立麻生養護学校　元石川分教室

  他3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