内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

資料３

サイバーセキュリティ戦略本部 重要インフラ専門調査会（第37回）

重要インフラにおける安全基準等の浸透状況に関する調査について［2023年度］

令和６年６月７日

内閣サイバーセキュリティセンター
重要インフラグループ

安全基準等の浸透状況に関する調査

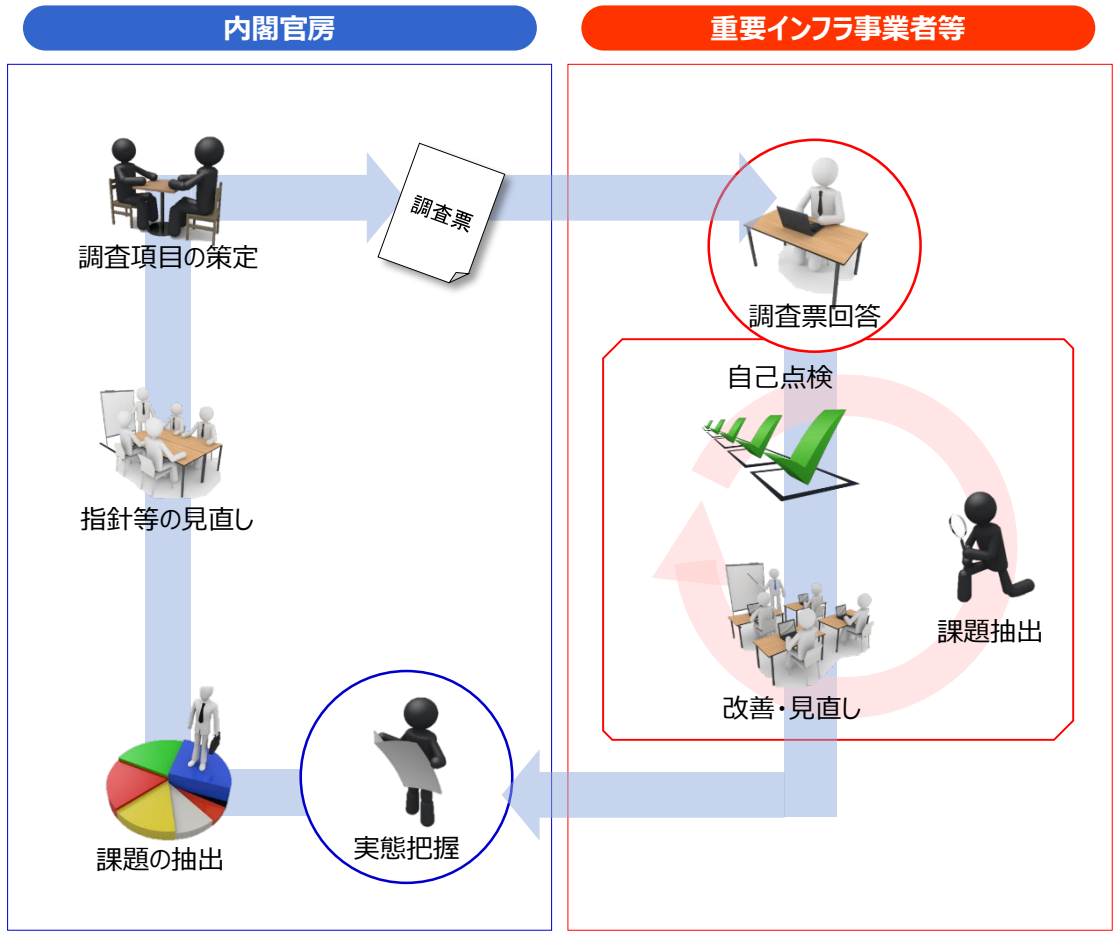
- 「重要インフラのサイバーセキュリティに係る行動計画」（以下「行動計画」という。）に基づき、**各重要インフラ分野に共通して求められるセキュリティ対策を「重要インフラのサイバーセキュリティに係る安全基準等策定指針」**（以下「指針」という。）**として取りまとめ**ている。
- 重要インフラ事業者等における安全基準等（※）の浸透状況を把握するため、**重要インフラ事業者等に対しセキュリティ対策の実施状況について調査を実施**した。

（※）各重要インフラ事業者等の判断や行為の基準となる基準又は参考となる文書類であり、関係法令に基づき国が定める「強制基準」、関係法令に準じて国が定める「推奨基準」及び「ガイドライン」、関係法令や国民からの期待に応えるべく業界団体等が定める業界横断的な「業界標準」及び「ガイドライン」、関係法令や国民・利用者等からの期待に応えるべく事業者等が自ら定める「内規」等が含まれる。

調査の概要

調査内容	**指針に記載された対策項目の実施状況を確認** ［調査基準日：2023年10月31日 ］
調査対象	**各重要インフラ分野の事業者等** ※調査対象は３ページに記載
調査方法	次の方法で書面による調査を実施 **調査方法①：NISC調査** 内閣官房が作成した「調査票」を配布し、内閣官房において集計（金融分野（資金決済以外）を除く重要インフラ分野） **調査方法②：外部調査** 他の組織が実施した調査結果を、内閣官房が作成した「調査票」の結果に読み替え（金融分野（資金決済以外）のみ）
調査結果の活用	**【内閣官房】** • 得られた知見や課題を各施策へと展開 • 行動計画の検証や評価に活用 **【重要インフラ事業者等】** • 調査への回答を通じ、自組織のセキュリティ対策の現状を確認し、改善・強化すべき方向性を把握

調査の流れ（イメージ）



（参考）調査の位置付け

「重要インフラのサイバーセキュリティに係る行動計画」

（サイバーセキュリティ戦略本部 令和４年６月17日決定 ）

Ⅳ．計画期間内の取組

２．安全基準等の整備及び浸透

重要インフラを取り巻く環境の変化や脅威の多様化を踏まえ、重要インフラ事業者等が自組織の抱えるリスクを把握し、自組織に最適な防護対策を実施できる状況を実現することが必要である。そのため、**関係主体は、安全基準等の整備及び浸透に取り組むことが期待される。**

具体的には、内閣官房は、重要インフラ所管省庁の協力のもとに、各重要インフラ分野に共通して求められるサイバーセキュリティの確保に向けた取組を「重要インフラ分野における情報セキュリティ確保に係る安全基準等策定指針」(以下「安全基準等策定指針」という。)として策定している。さらに、安全基準等策定指針で定めた手順等を具体的に示すための手引書（以下「手引書」という。） 及び個別の対処方法、留意点等を示すガイダンス等の関連文書を策定している。安全基準等策定指針、手引書等を踏まえ、関係法令に基づき国が定める「強制基準」、関係法令に準じて国が定める「推奨基準」及び「ガイドライン」、関係法令や国民からの期待に応えるべく業界団体等が定める業界横断的な「業界標準」及び「ガイドライン」、関係法令や国民・利用者等からの期待に応えるべく重要インフラ事業者等が自ら定める「内規」等(以下「安全基準等」という。)が策定されている。

２.３ 安全基準等の浸透

重要インフラ事業者等において有効な障害対応体制の構築がなされているかを精緻に把握することを目的に、**内閣官房は、重要インフラ事業者等における安全基準等の整備状況及びサイバーセキュリティ確保に向けた取組・手段について調査分析する。**結果については、原則、年度ごとに公表するとともに、本行動計画の各施策の改善に活用する。

重要インフラ分野・組織ごとのリスクの多様化・複雑化に伴い、組織に応じた対策状況や、経営層の関与状況等の実態をより正確に把握することが重要になってきている。そのため、重要インフラ事業者等における自主的な取組を促進できる調査方法へ変更する必要がある。内閣官房は、新たな調査方法について重要インフラ所管省庁と協議し、重要インフラ事業者等による自主的な取組を促進する最適な手法を検討し、2023年度中を目処に具現化する。

具体的には、重要インフラ事業者等において、①サイバーセキュリティの現状に係る自己評価、②自組織における本来あるべき状況や要件との差異の分析、③分析結果を踏まえた自組織に不足している対策の優先順位付け、④具体的な対策の実施、を繰り返すことで、サイバーセキュリティの確保に資する継続的な改善を図ることができる合理的・効果的な調査手法を検討する。

Ⅵ．評価・検証

２．本行動計画の検証

2.３「政府機関等による施策」の検証

本行動計画の政府機関等による各施策は、いずれも重要インフラ事業者等におけるサイバーセキュリティに関し、自主的な取組の促進その他の必要な施策を講ずるものである。

施策の結果検証は、重要インフラ事業者等によるサイバーセキュリティの確保に対する本行動計画の各施策による寄与の状況を検証することとする。

調査対象及び回答状況

- 2023年度は、**重要インフラ分野（計14分野）の事業者等を対象に調査を実施し、1,862事業者から回答**（回答率47.1%）を得た。

重要インフラ分野		調査対象	回答数	調査方法
情報通信	電気通信	主要な電気通信事業者	24	NISC調査
	放送	主要な地上基幹放送事業者	97	
	ケーブルテレビ	主要なケーブルテレビ事業者	105	
金融(資金決済以外)		銀行等、生命保険、損害保険、証券会社	658	外部調査※1
金融（資金決済）		主要な資金決済事業者	54	NISC調査
航空		主たる定期航空運送事業者	7	
空港		主要な空港・空港ビル事業者	8	
鉄道		大手民間鉄道事業者の主要な鉄道事業者	19	
電力		一般送配電事業者、主要な発電事業者	24	
ガス		主要なガス事業者	13	
政府・行政サービス		都道府県及び市区町村	713	
医療		医療情報システムを導入している主要な事業者	21	
水道		主要な水道事業者及び水道用水供給事業者	71	
物流		大手物流事業者	11	
化学		主要な石油化学事業者	8	
クレジット		主要なクレジットカード会社、主要な決済代行業者、指定信用情報機関等	23	
石油		主要な石油精製・元売事業者	6	
全分野合計		－－－	**1,862 (1,204)**※2	

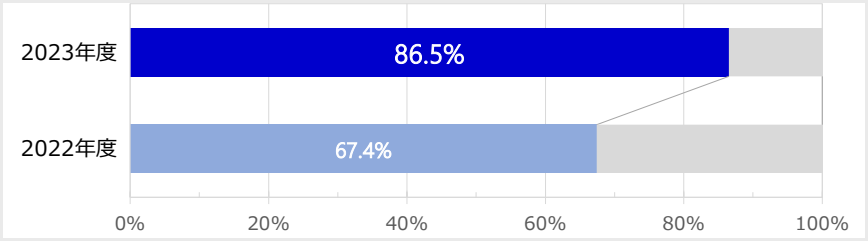
※1　金融（資金決済以外）については、外部調査にて実施したものをNISC調査の結果に読み替えて集計。
※2　全分野合計の（　）内の数値は、金融分野（資金決済以外）を除いた合計数。

浸透状況と課題 － 組織統治に関する取組

- **「セキュリティ方針の策定への経営層の関与」、「定期的なコミュニケーション」及び「サイバーセキュリティに関する事件・事故発生時の情報開示基準の策定」は、昨年度から実施状況が改善**しており、サイバーセキュリティリスクを経営リスクと見なす認識が浸透していると考えられる。
- **「セキュリティに関する予算・人材が不明確である」と回答した割合が減少**し、**予算配分、人材配分ともに向上**しており、重要インフラ事業者等のセキュリティ投資への意識が醸成されてきていると考えられる。一方で、「予算が適切に配分されている」と回答した割合の伸び率に対し、「人材が適切に配分されている」と回答した割合の伸び率が少なく、**セキュリティ人材の確保に苦慮している事業者等が多い**と思われる。

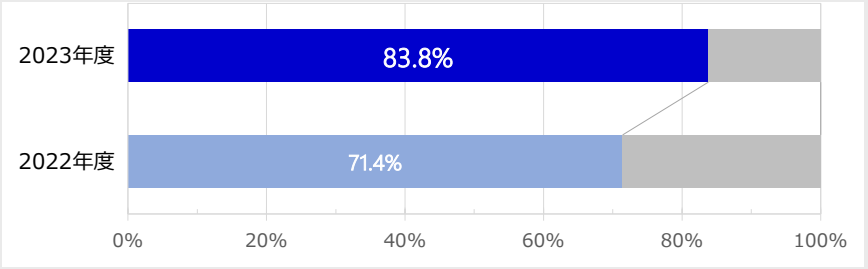
► **サイバーセキュリティリスクが経営リスクと認識され、セキュリティ方針の策定に経営層が関与している**（設問19）

※金融分野（資金決済以外）を除く



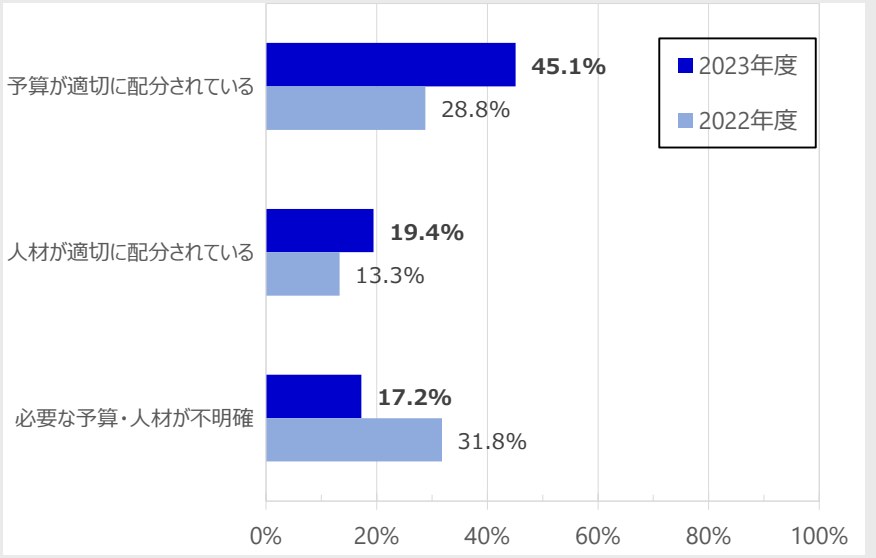
► **サイバーセキュリティリスク、インシデント等の情報について定期的なコミュニケーションを実施している**（設問17）

※金融分野（資金決済以外）を除く



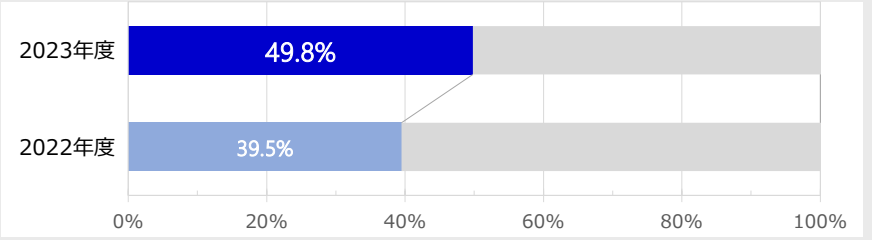
► **セキュリティ予算・人材が適切に配分されていると感じる**（設問27）

※金融分野（資金決済以外）を除く



► **サイバーセキュリティに関する事件・事故が発生した場合の情報開示の基準を策定している**（設問34）

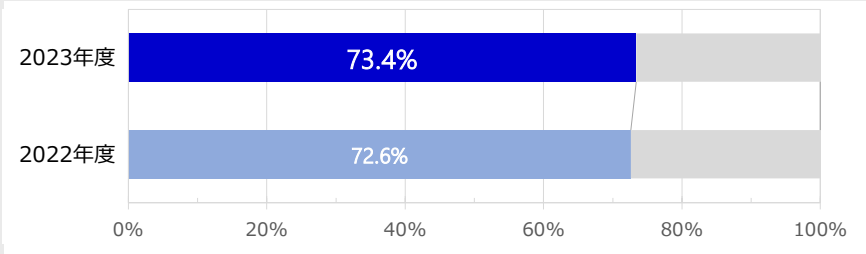
※金融分野（資金決済以外）を除く



浸透状況と課題 － リスクアセスメント、サプライチェーン

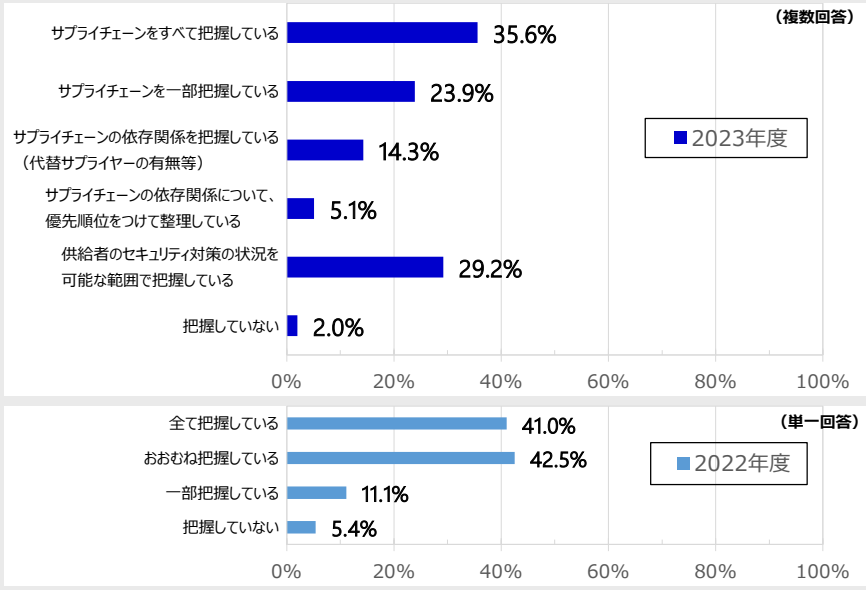
- **リスクアセスメントの実施状況は昨年度より改善**しているが、**４分の１が未実施**であるので引き続き改善に向けた取組が必要と考えられる。
- 昨年度より「サプライチェーンを把握していない」と回答した割合が減少しており、**自組織のサプライチェーンの把握については着実に意識付けされている**と思われる。サプライチェーンの把握に対する意識向上により、サプライチェーンリスクの低減や、復旧作業における業務効率の向上が期待できる。
  他方、サプライチェーンに関する**「セキュリティ確保の定期的評価」「責任分界点の明確化」「インシデント発生時の報告」「機器等の脆弱性管理」といった対策の実施状況は５割以下で推移**しており、必要な対策が実施されるよう引き続き促進することが必要と考えられる。

► リスクアセスメントを実施している（設問42）



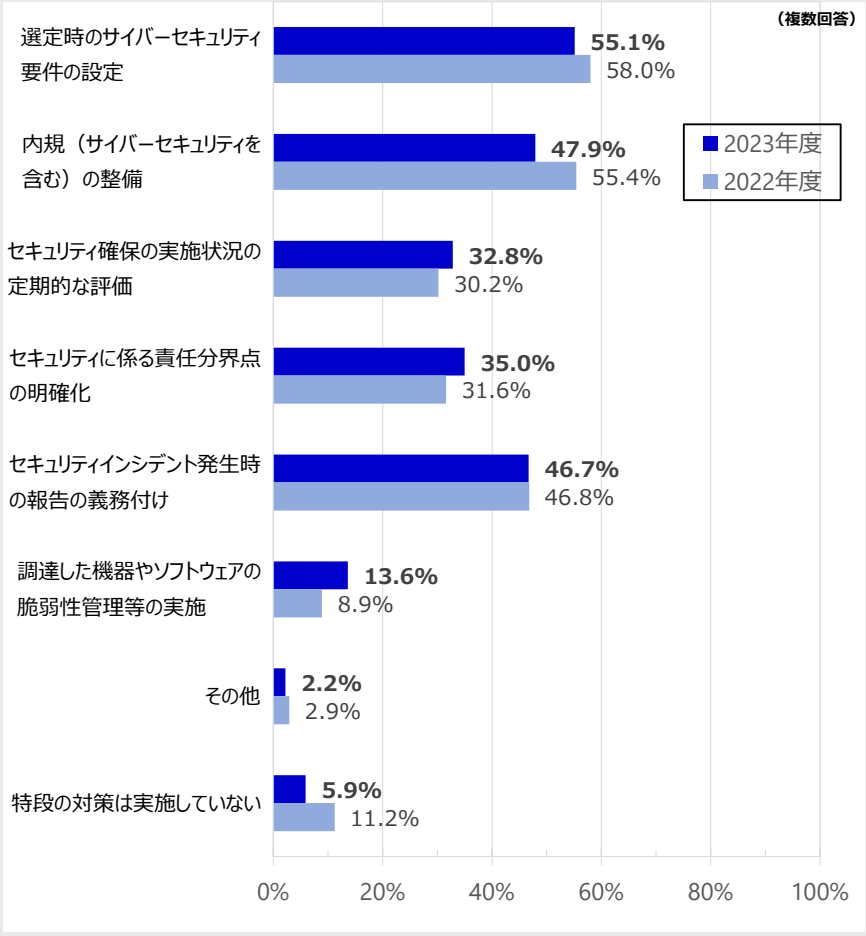
► 自組織のサプライチェーンを把握している（設問56）

※金融分野（資金決済以外）を除く



► サプライチェーン・リスク対策の実施状況（設問61）

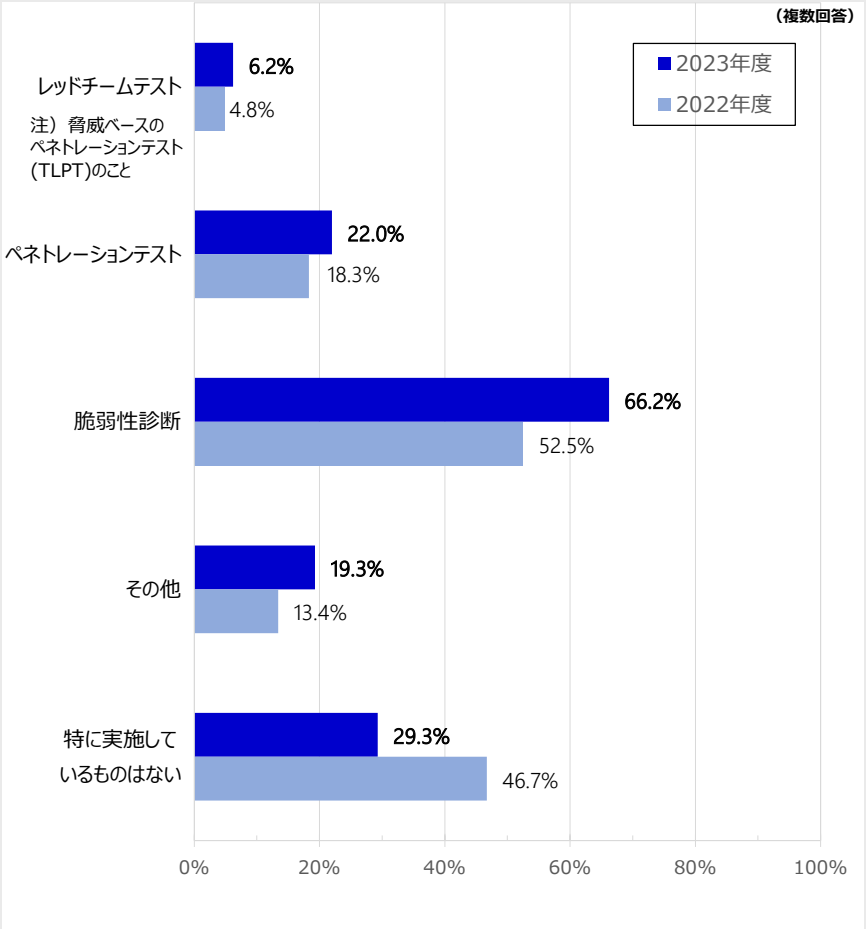
※金融分野（資金決済以外）を除く



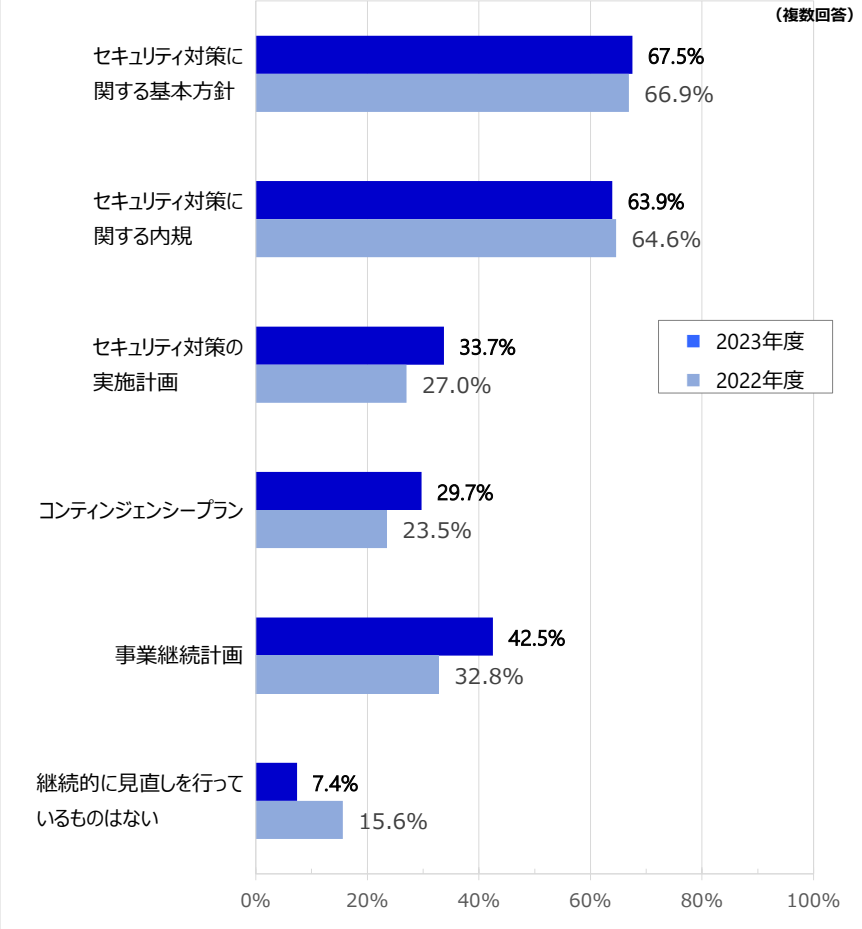
浸透状況と課題 － 評価、改善

- **セキュリティ評価に関する実施状況は未実施の割合が減少し、全体として改善**傾向にある。特に、**脆弱性診断は重要インフラ事業者において浸透**してきていると考えられる。
- **基本方針や内規の見直しの実施は横ばい**であったが、**コンティンジェンシープラン及び事業継続計画の見直しの実施率が向上**している。サイバーセキュリティインシデントの発生を前提とした、事業継続の意識が浸透しつつあると考えられる。

► セキュリティ評価の実施状況（設問31）



► 見直しの実施状況（設問113） ※金融分野（資金決済以外）を除く

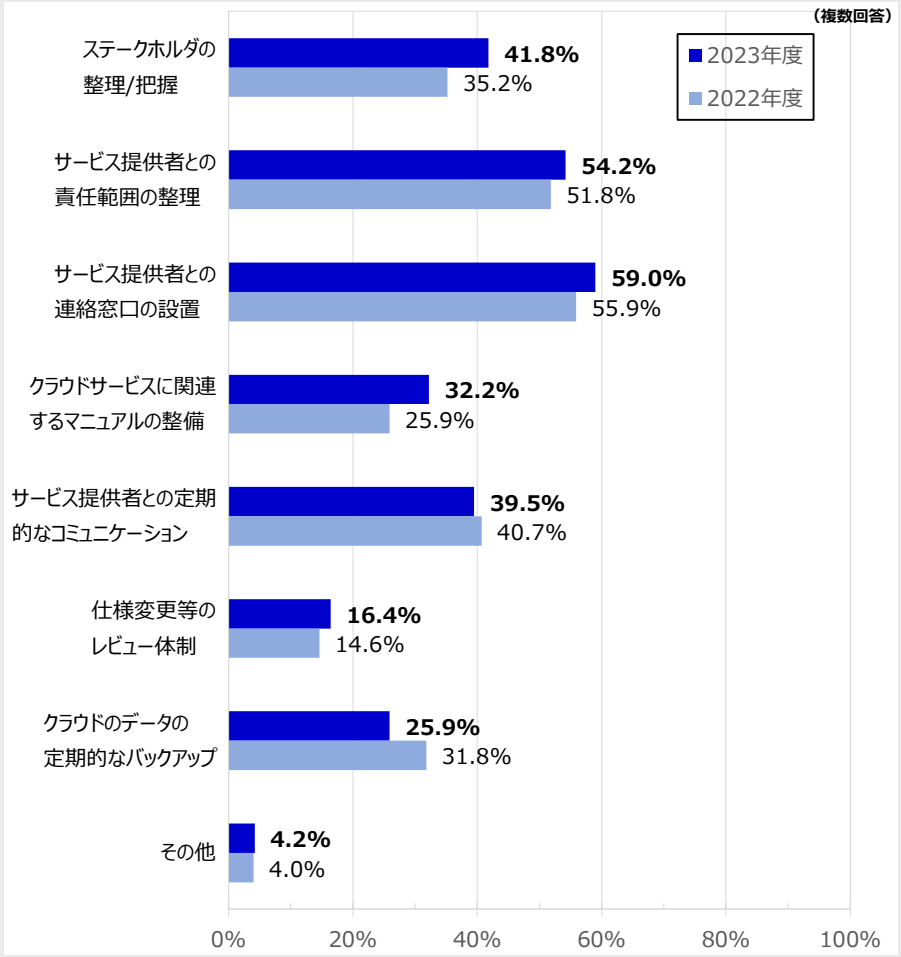


浸透状況と課題 － クラウドサービスの利用、ランサムウェア対策

- **クラウドサービスの利用に係る対策の実施状況は昨年度から大きな変化はなく**、「重要インフラのサイバーセキュリティに係る安全基準等策定指針(2023年７月4日サイバーセキュリティ戦略本部決定)」の「 5.5.2. クラウドサービス利用時の対策」等を参考に、対策を促進する必要がある。
- ランサムウェア対策については、**「バックアップデータからの復旧確認」「システム再構築を含む復旧計画の策定」「海外拠点等の比較的セキュリティ対策の弱い拠点における対策」が引き続き低位で**あり、これらの改善が今後の課題であると考えられる。

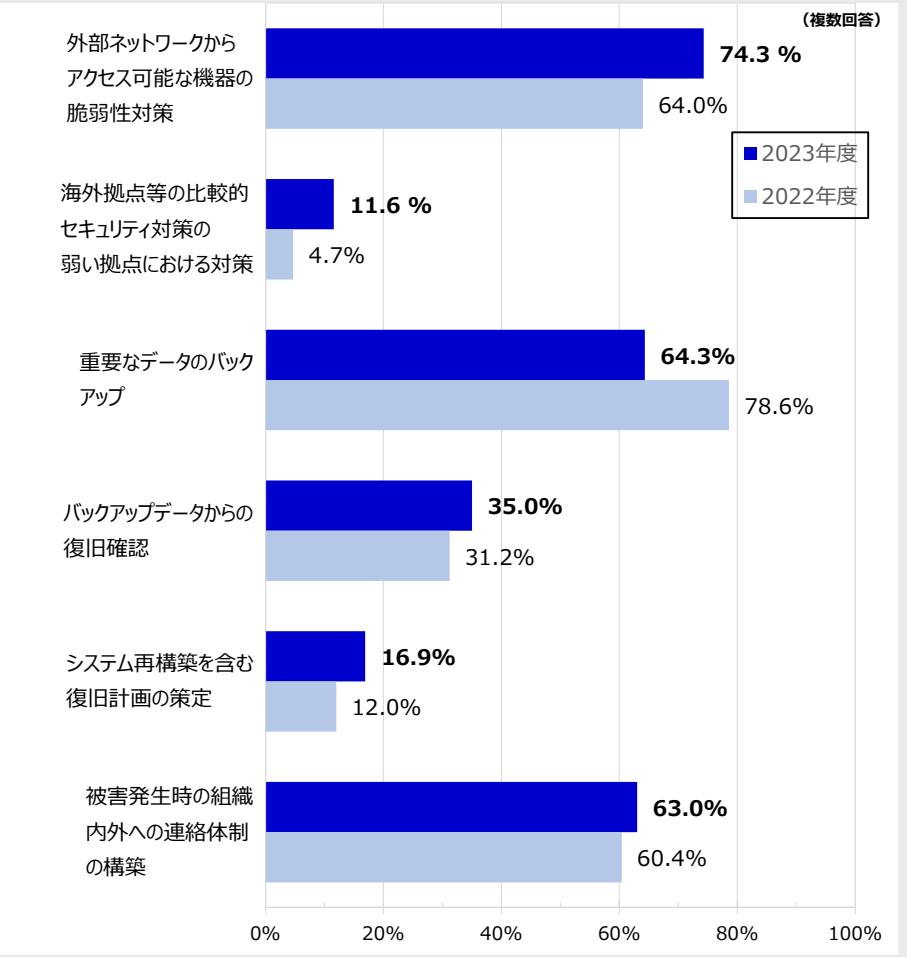
► クラウドサービスの利用に係る対策の実施状況（設問111）

※金融分野（資金決済以外）を除く



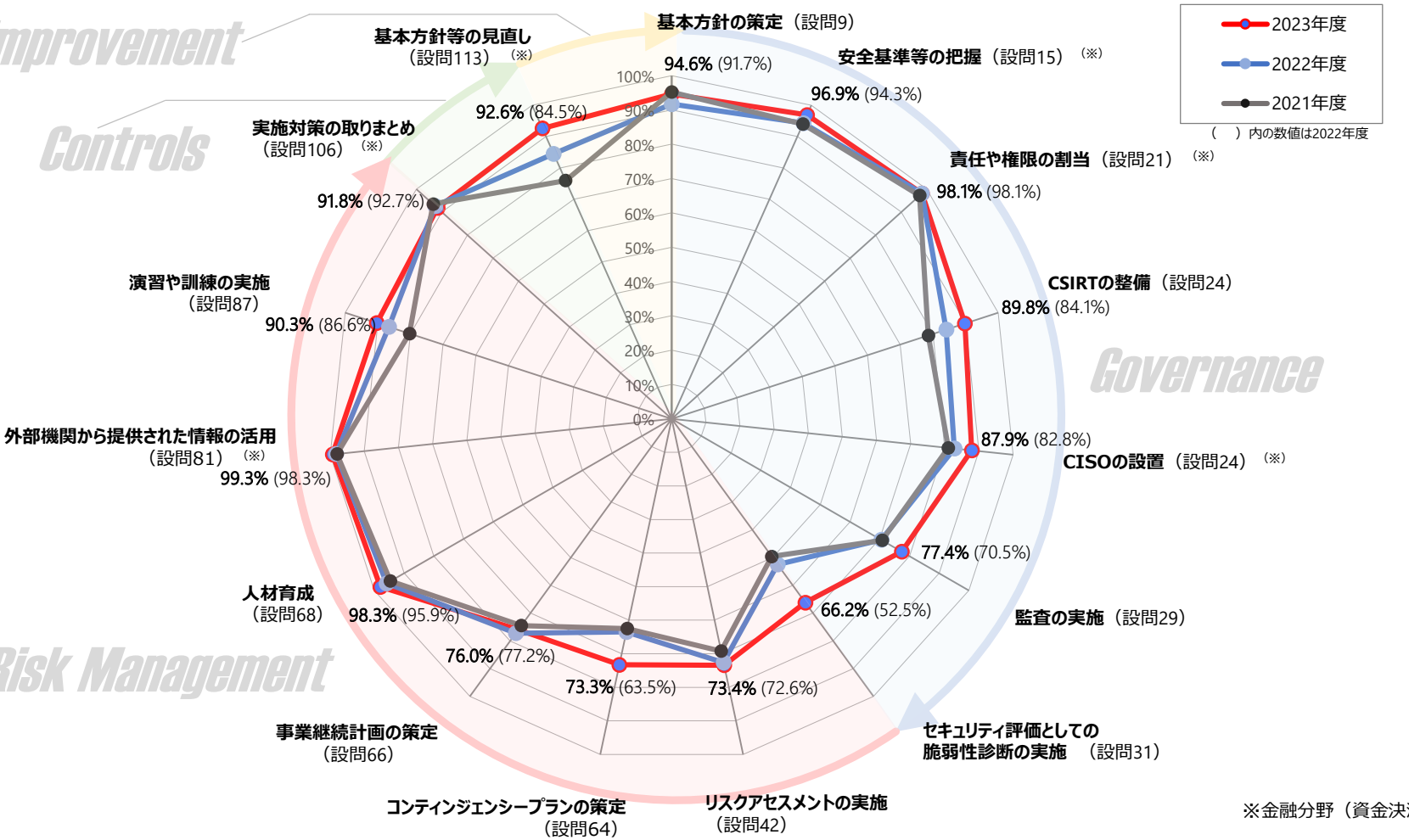
► ランサムウェア対策の実施状況（抜粋）（設問108）

※金融分野（資金決済以外）を除く



（参考）調査結果の経年比較

- **<u>セキュリティ対策の実施状況は多くの項目において高い水準で推移</u>**しており、安全基準等は浸透しつつあると評価できる。
- 「CSIRTの整備」「CISOの設置」「監査の実施」「脆弱性診断の実施」といった**<u>組織統治に関する項目の実施率について改善</u>**が見られ、 経営層の責務において実施すべき取組に進展が見られる。
- 「コンティンジェンシープランの策定」「基本方針等の見直し」といった**<u>リスクマネジメント及び改善における取組の実施率に向上</u>**が見られ、レジリエンス向上への取組の進展が見られる。
- しかし、 リスクマネジメントに係る項目である**<u>「脆弱性診断の実施」「リスクアセスメントの実施」「事業継続計画の策定」等の実施率は、７割前後</u>**であり、これらを改善していくことが今後の課題である。



※金融分野（資金決済以外）を除く

内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

資料３　別冊

サイバーセキュリティ戦略本部 重要インフラ専門調査会（第37回）

重要インフラにおける安全基準等の浸透状況に関する調査結果詳細［2023年度］

令和６年６月７日

内閣サイバーセキュリティセンター
重要インフラグループ

2023年度調査設問の構成（設問一覧）

□ 組織統治

設問9　組織方針とサイバーセキュリティ
設問11　サイバーセキュリティ方針への記載事項
設問13　要求事項の文書化
設問15　安全基準等の把握
設問17　定期的なコミュニケーション
設問19　経営リスクとしてのサイバーセキュリティ
設問21　責任・権限の割当
設問24　役職・担当者の設置
設問27　人材や予算の配分
設問29　監査の実施
設問31　サイバーセキュリティ評価の実施
設問34　情報開示の基準
設問36　サイバーセキュリティ確保の取組の見直しの契機

□ リスクマネジメント

設問38　外部環境・内部環境の整理
設問40　任務保証を踏まえた自組織の特性把握
設問42　リスクアセスメントの実施
設問44　実施しているリスクセスメントの方法
設問46　定期的なリスクアセスメントの実施
設問48　制御システムのセキュリティ確保
設問50　セキュリティ対策検討の際の取組
設問52　個々のセキュリティ対策の対応状況
設問54　リスク対応計画
設問56　サプライチェーンの把握
設問59　認識しているサプライチェーンリスク
設問61　実施しているサプライチェーンリスク軽減策
設問64　コンティンジェンシープランの策定
設問66　事業継続計画の策定
設問68　人材育成・意識啓発
設問72　情報処理安全確保支援士取得の推進
設問74　リスク対応計画の実施状況
設問76　情報共有や意見交換を行っている関係主体
設問79　情報共有の範囲
設問81　活用している情報提供元
設問83　実践している情報共有
設問85　危機管理体制
設問87　演習・訓練

□ 組織的対策

設問90　資産・情報・データ等の管理
設問91　供給者管理
設問92　運用時のセキュリティ管理
設問93　マルウェアからの保護
設問94　バックアップ
設問95　ログ管理
設問96　運用ソフトウェアの管理
設問97　脆弱性管理
設問98　システムの取得・開発及び保守
設問99　インシデント管理

□ 人的対策

設問100　人的資源及び外部委託

□ 物理的対策

設問101　物理的及び環境的セキュリティ

□ 技術的対策

設問102　アカウント管理
設問103　アクセス制御
設問104　暗号技術
設問105　通信のセキュリティ

設問106　各対策項目で実践しているセキュリティ管理策を内規として整備

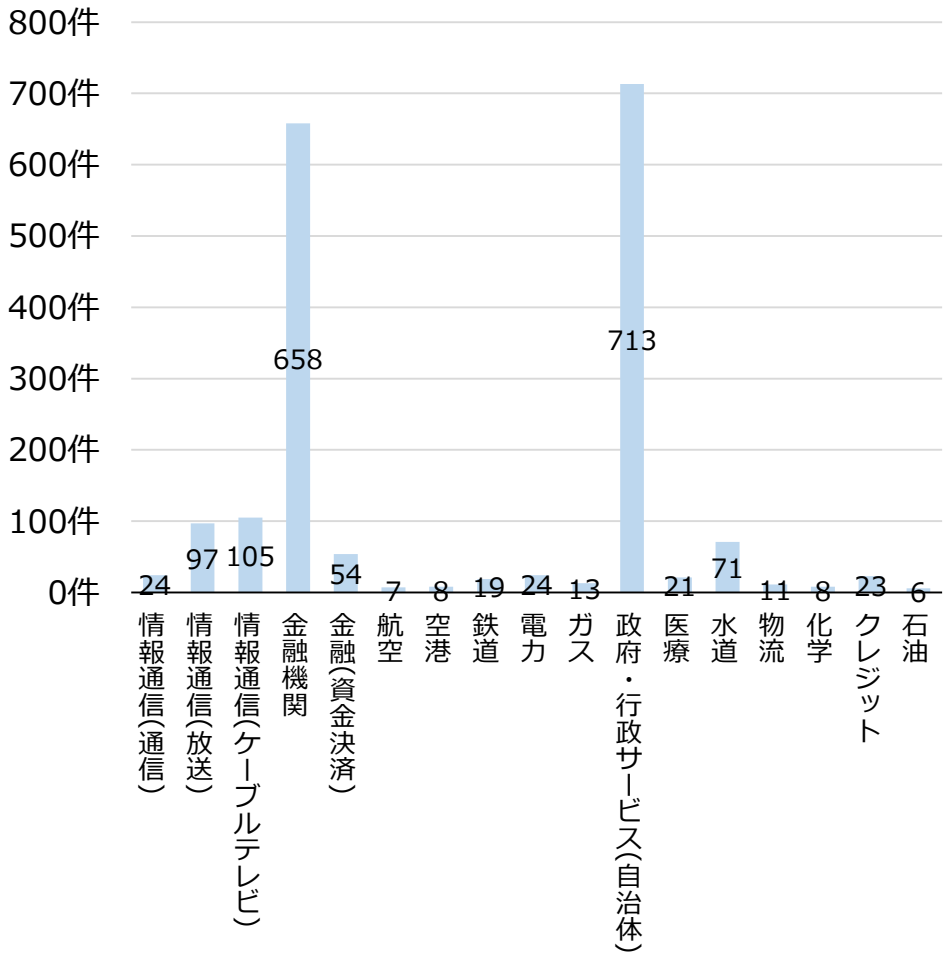
□ 動向を踏まえた対策

設問108　ランサムウェア攻撃への対策、運用体制
設問109　クラウドサービス提供事業者への確認事項
設問111　クラウドサービス利用に関する運用対策

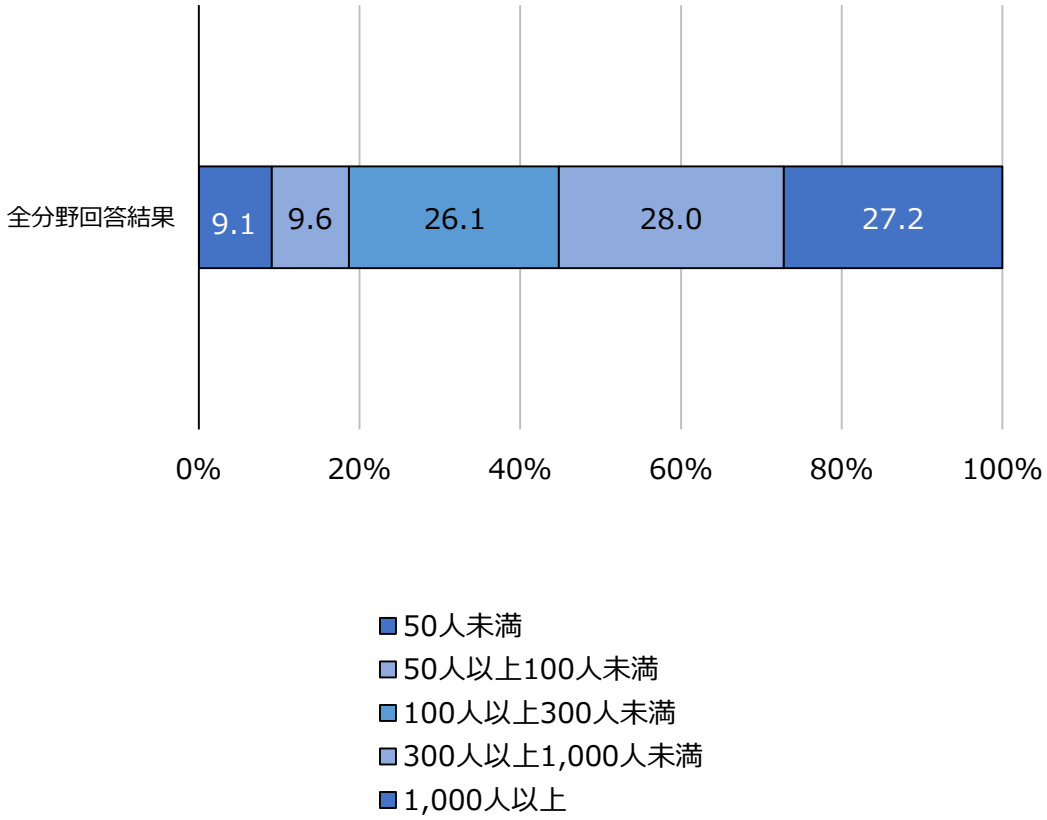
設問113　自組織で実践しているセキュリティ管理策の継続的な見直し

※設問番号の欠番は基礎情報（分野名、従業員数）及び、
各設問に付記した自由記述による回答

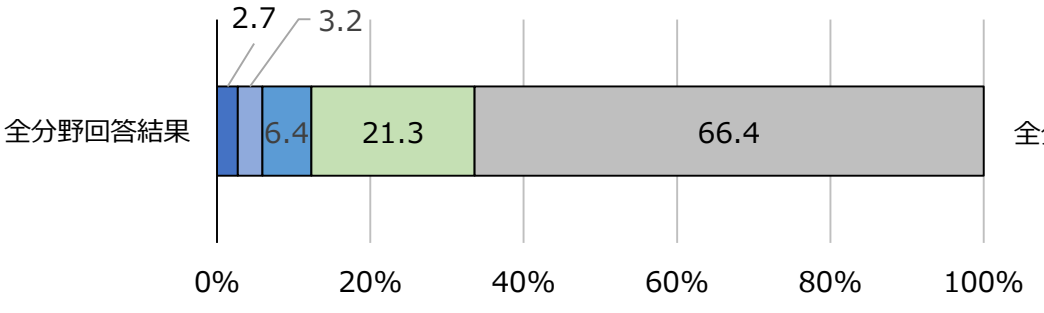
設問１．【単一回答】
貴社（又は貴団体）が属する重要インフラ分野



設問６．【単一回答】
貴社（又は貴団体）の従業員数



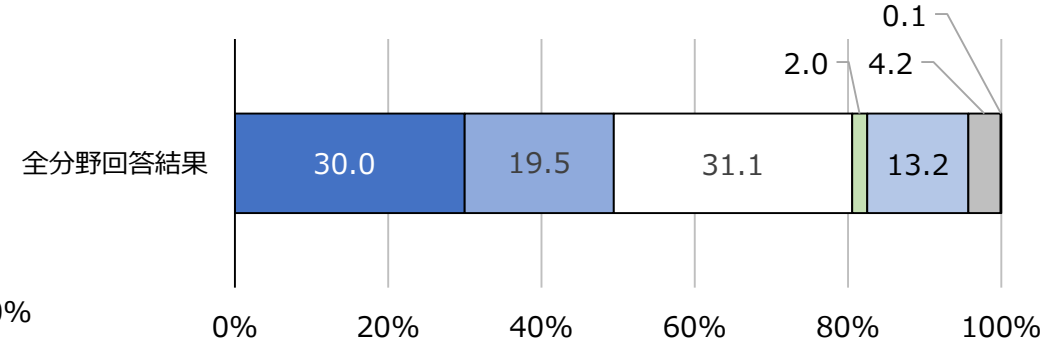
設問７．【単一回答】
貴社の資本金
（※地方公共団体の場合は、５：いずれも該当しない を選択）



- 5,000万円未満
- 5,000万円以上１億円未満
- １億円以上３億円未満
- ３億円以上
- いずれも該当しない

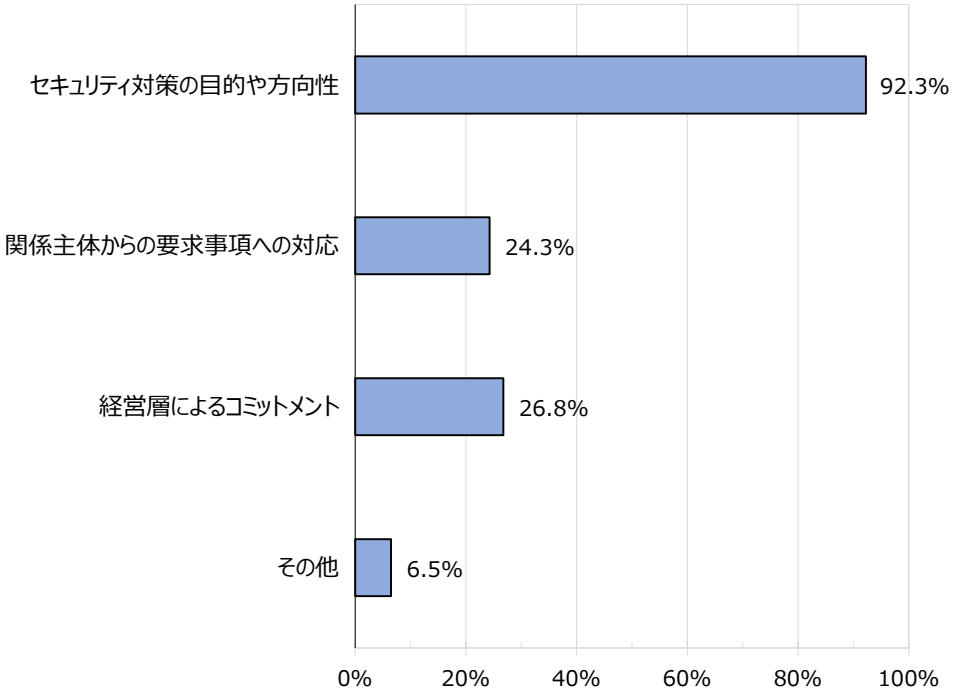
設問９．【単一回答】
組織方針（経営方針、リスクマネジメント方針等）にあたる文書に、重要インフラのサイバーセキュリティ確保に関する事項※を組み入れていますか。

※　例）「サイバーセキュリティに対する脅威からの被害がサービス提供を阻害するリスクの一つである」
「リスクマネジメントの対象としてサイバーセキュリティに関する事項を含める」

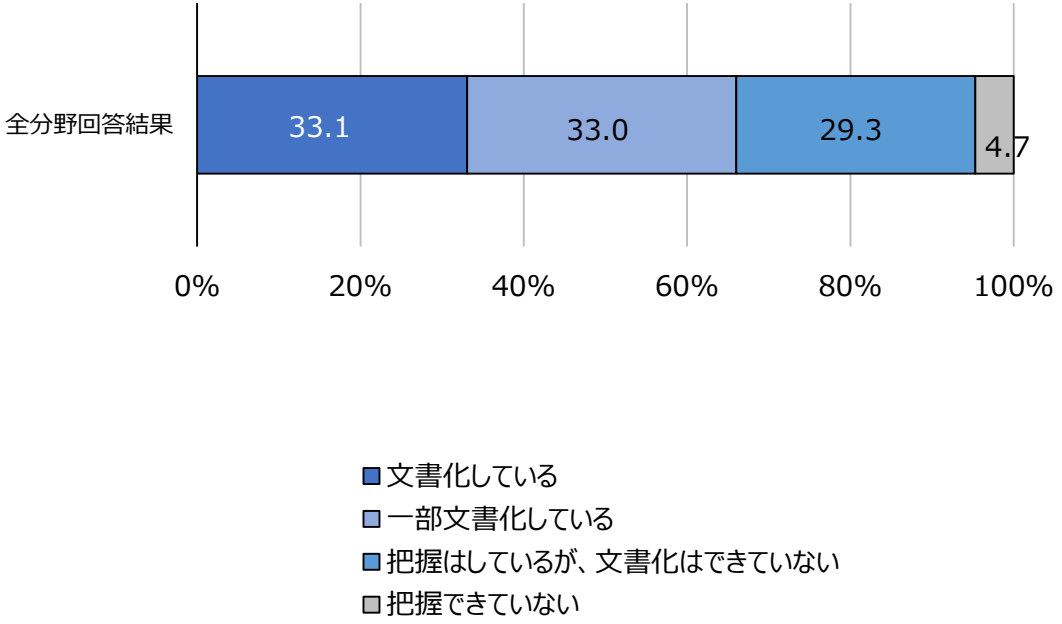


- 組織方針にあたる文書に組み入れ、サービス範囲・水準を示している。
- 組織方針にあたる文書に組み入れているが、サービス範囲・水準は示していない。
- 組織方針にあたる文書に組み入れてはいないが、サイバーセキュリティ確保に関する事項を基本方針等に定めている。
- 現在組み入れ中である
- 今後組み入れる予定である
- 組み入れる予定はない
- 無回答

設問11.【複数回答】
組織方針を踏まえて策定するサイバーセキュリティ方針に記載されている内容を選択してください。



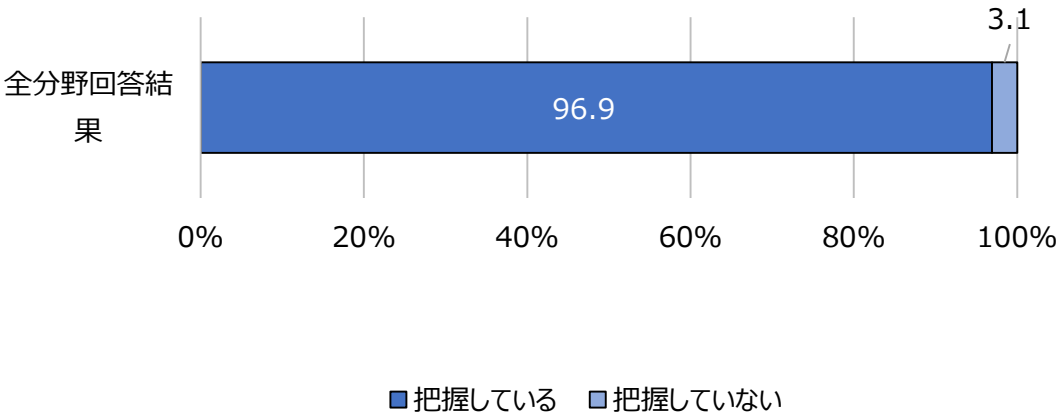
設問13.【単一回答】
関係省庁、顧客、サプライヤー、委託先等からの、サイバーセキュリティに関する自組織への要求事項※を文書化していますか。



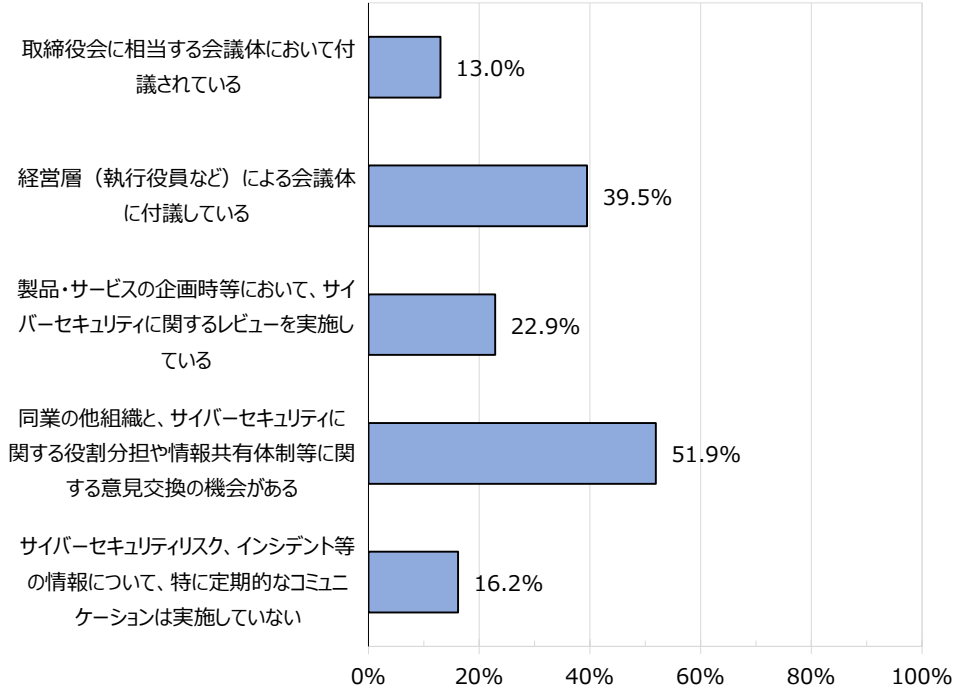
アンケート調査結果

設問15.【単一回答】
自組織に関係する安全基準等※を把握していますか

※関係法令に基づき国が定める「強制基準」、関係法令に準じて国が定める「推奨基準」及び「ガイドライン」、業界団体等が定める業界横断的な「業界標準」及び「ガイドライン」等

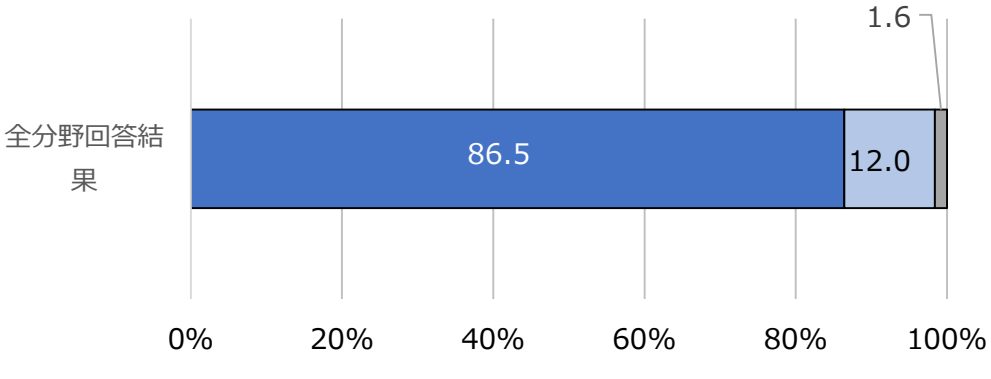


設問17.【複数回答】
サイバーセキュリティリスク、インシデント等の情報について定期的なコミュニケーションを実施していますか。



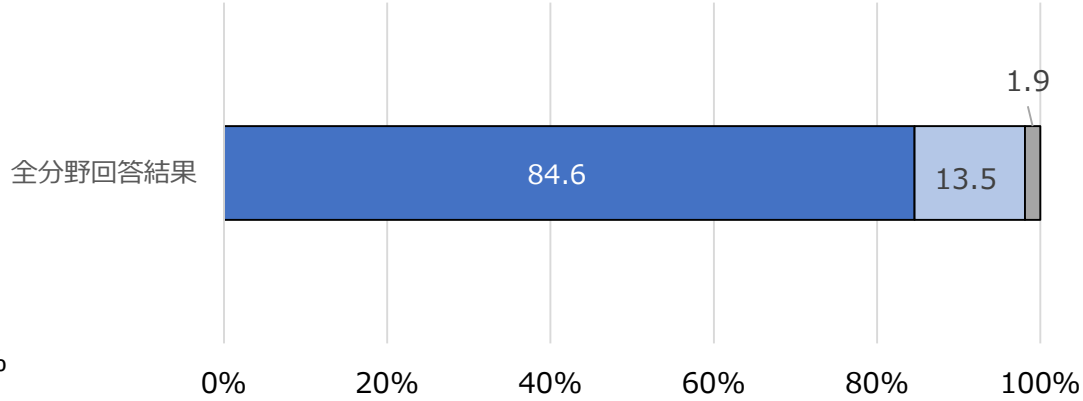
設問19.【単一回答】
サイバーセキュリティリスク（※1）が経営リスク（※2）と認識されていますか。

※1 重要インフラサービス提供に必要な情報システムや、ITを用いた制御システム等の運用を不確かにするもの
※2 自然災害や感染症等、達成するべき経営目標を阻害する可能性があるもの



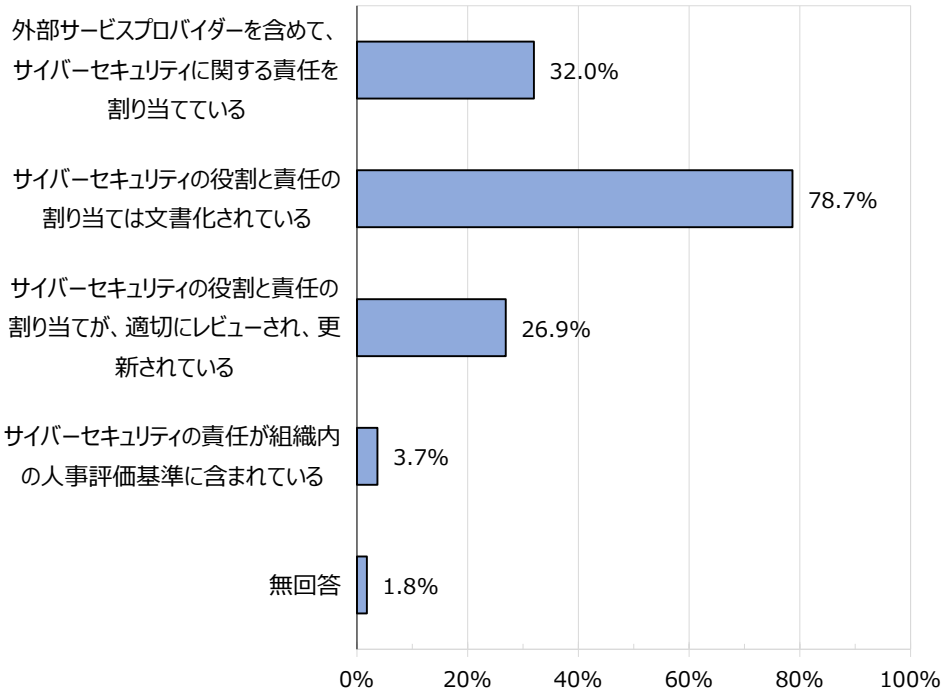
- 経営リスクと認識され、セキュリティ方針の策定に経営層が関与している
- 経営リスクと認識されているが、方針を策定するための具体的な体制が整備されていない
- サイバーセキュリティリスクは経営リスクとして認識されていない

設問21.【単一回答】
自組織のサイバーセキュリティを担当する部署及び従業員を決定するとともに責任及び権限を割り当てていますか。

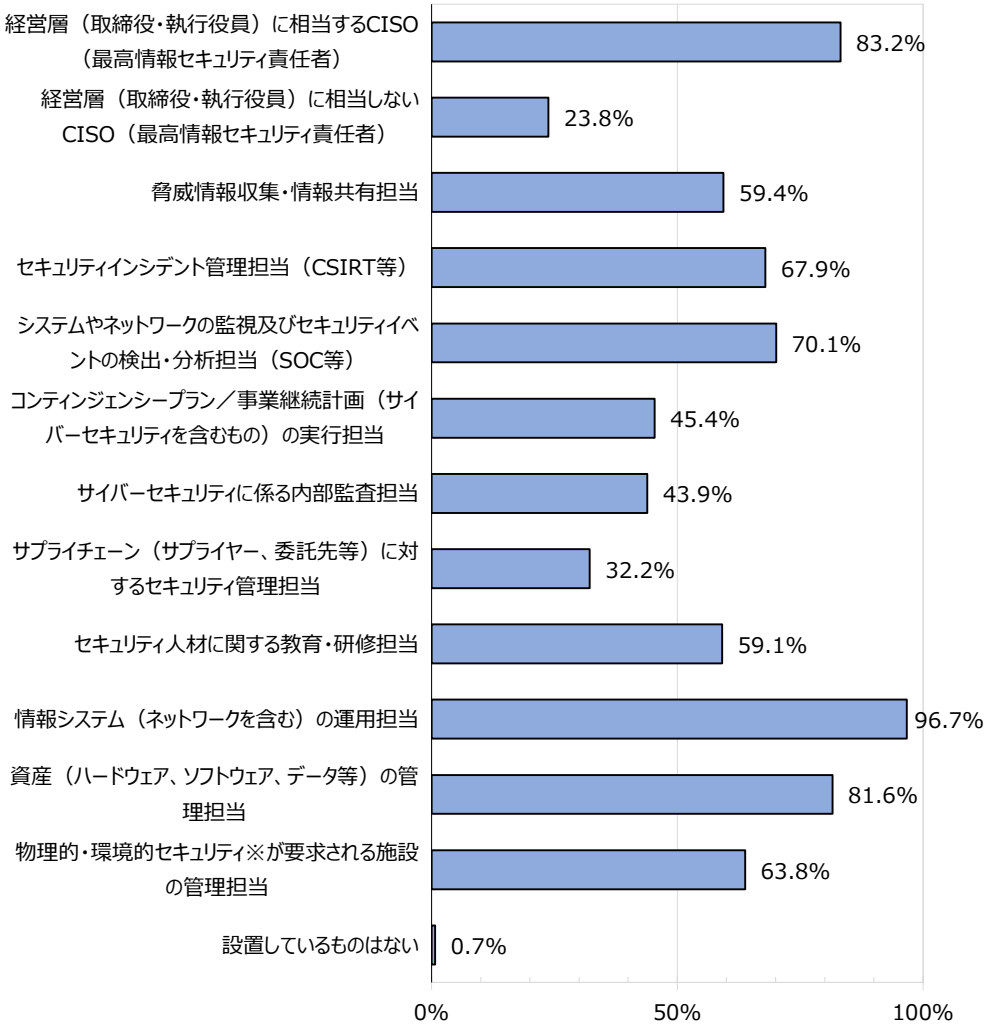


- サイバーセキュリティを担当する部署及び従業員が決められており、責任及び権限も明確である
- サイバーセキュリティを担当する部署及び従業員は決められているが、責任及び権限は明確ではない
- サイバーセキュリティを担当する部署及び従業員は決められていない

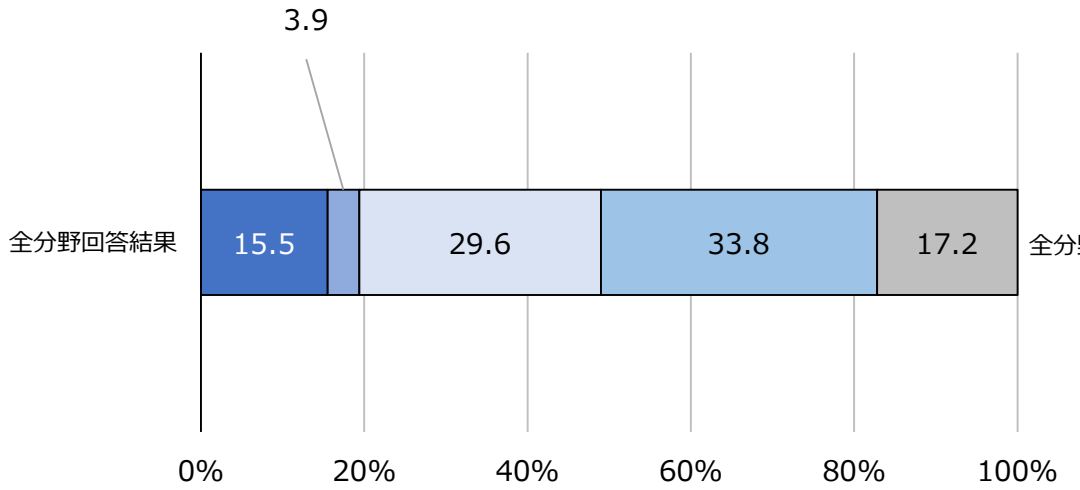
設問23.【複数回答】
サイバーセキュリティにおける責任及び権限の割り当てに関して、実施している取組を選択してください。



設問24.【複数回答】
自組織で設置しているものを全て選択してください。
（※「セキュリティインシデント管理担当（CSIRT等）」のみ全金融分野を含む）

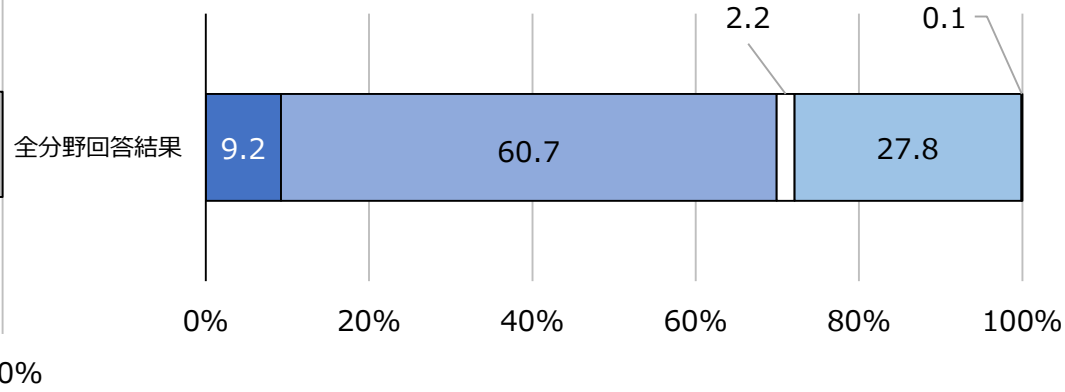


設問27.【単一回答】
サイバーセキュリティの確保に必要となる人材や予算が明確化され、組織内に適切に配分されていると感じますか。



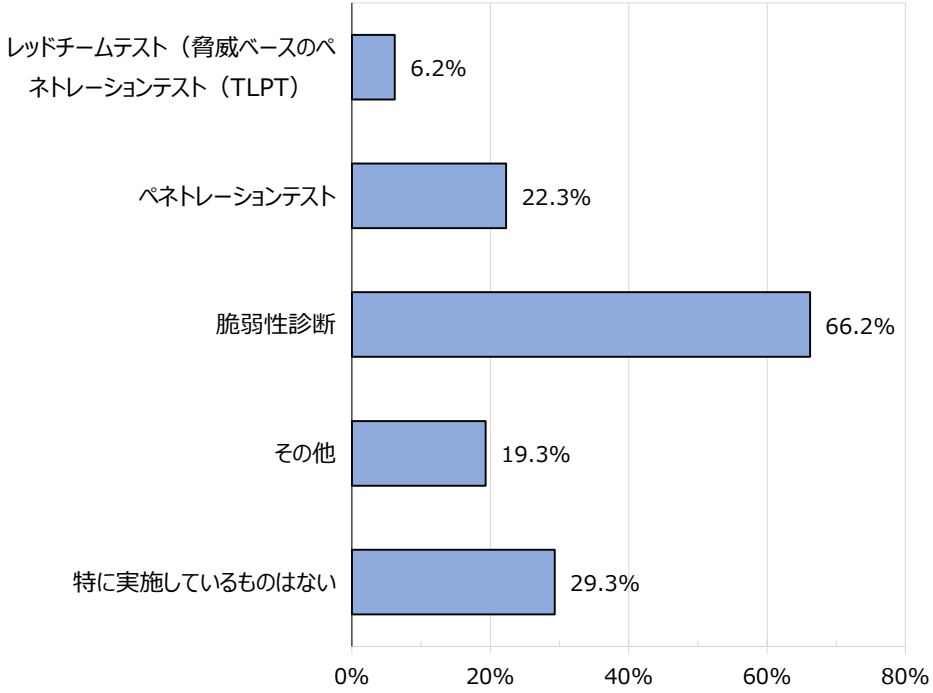
- 人材、予算共に十分に配分されている
- 人材は十分に配分されている
- 予算は十分に配分されている
- 人材、予算共に十分に配分されていない
- 必要な人材や予算が明確になっていない

設問29.【単一回答】
自組織のサイバーセキュリティ確保の取組について、監査を実施していますか。

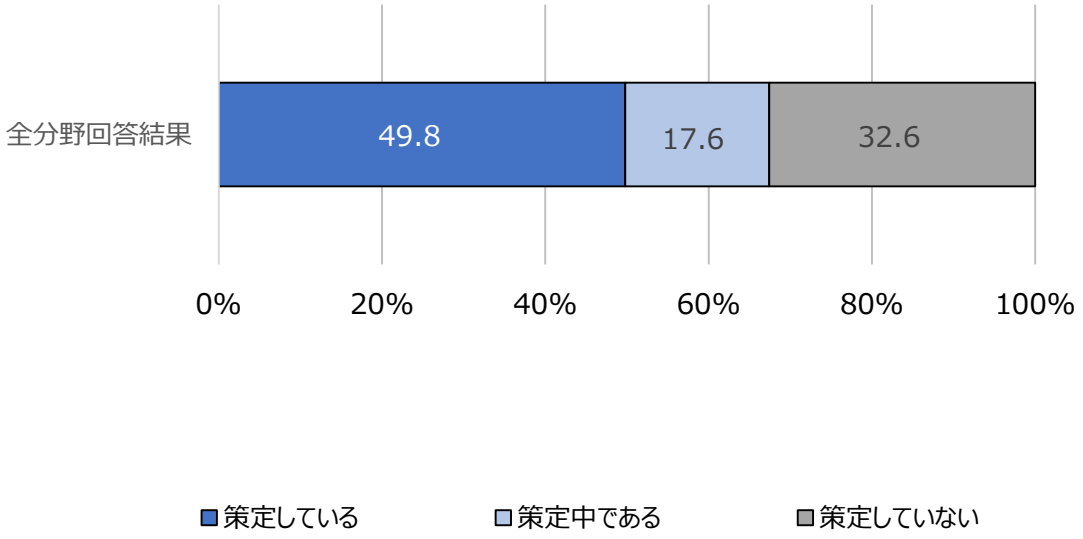


- 取締役監査、内部監査共に実施している
- 内部監査のみ実施している
- 取締役監査のみ実施している
- 取締役監査、内部監査共に実施していない
- 無回答

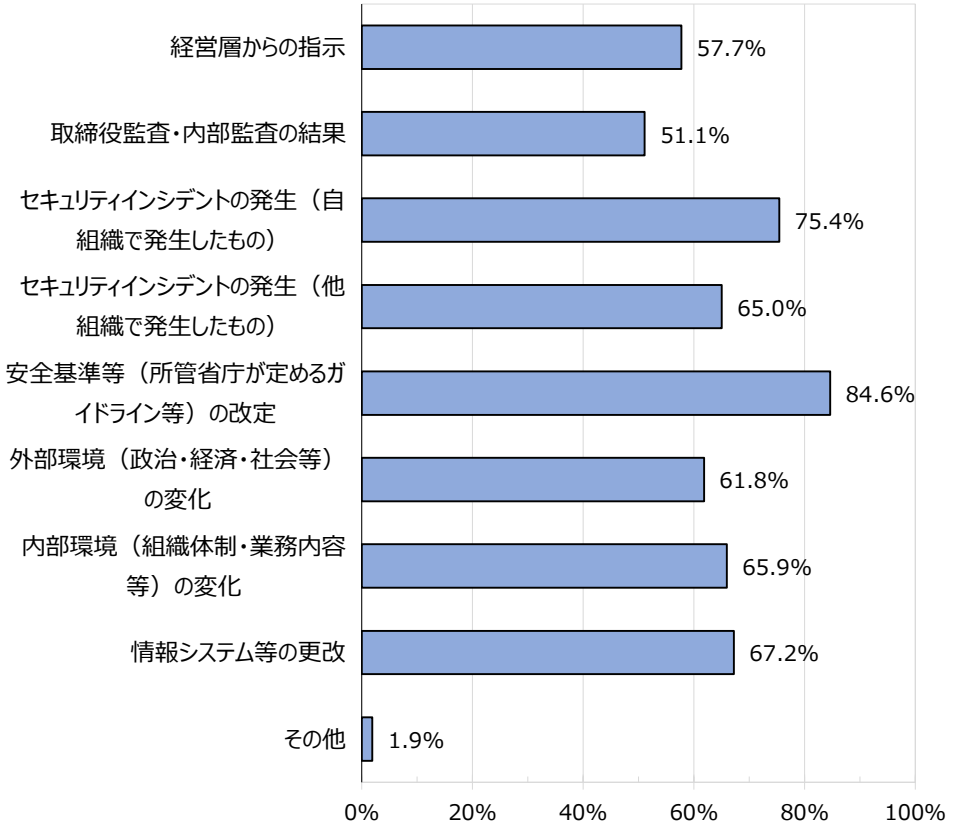
設問31.【複数回答】
自組織にて実施しているセキュリティ評価を全て選択してください。
（※全金融分野を含む）



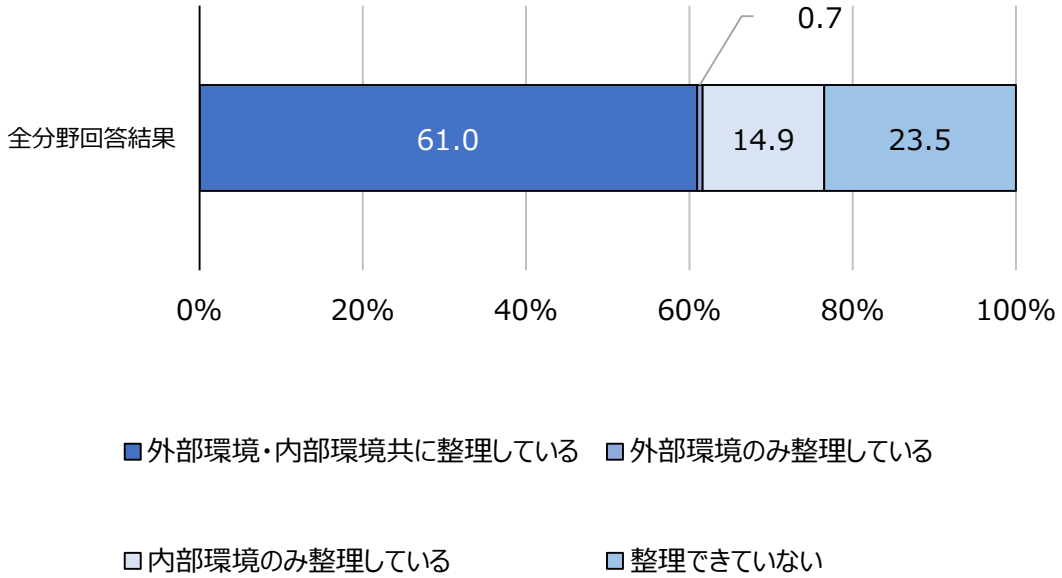
設問34.【単一回答】
サイバーセキュリティに関する事件・事故（サービス停止、情報漏えい、改ざん等）が発生した場合の情報開示の基準を策定していますか。



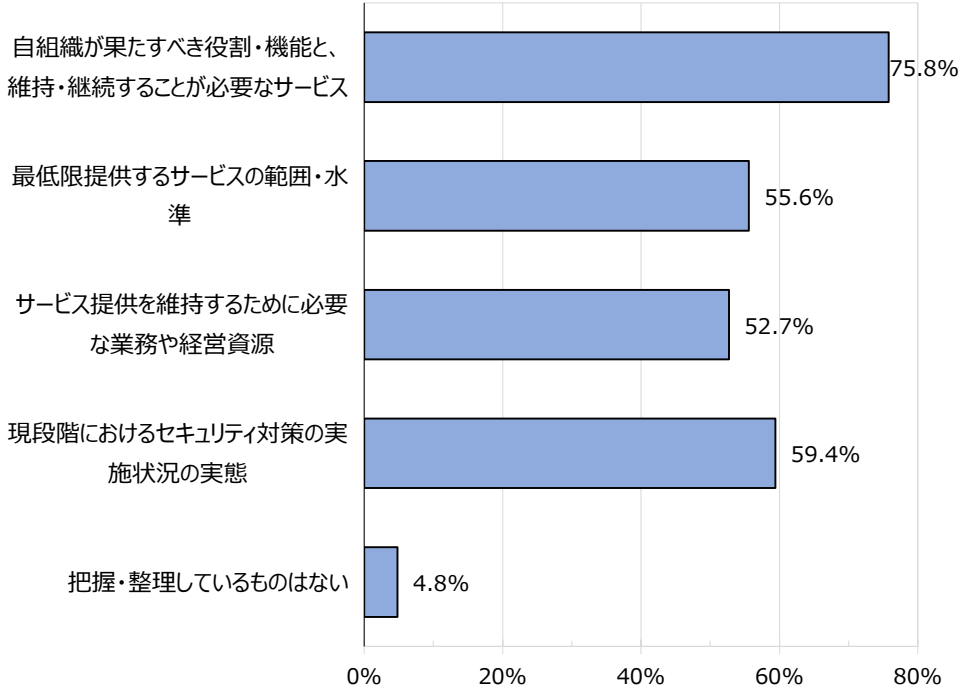
設問36.【複数回答】
サイバーセキュリティ確保の取組の見直しの契機となるものを全て選択してください。



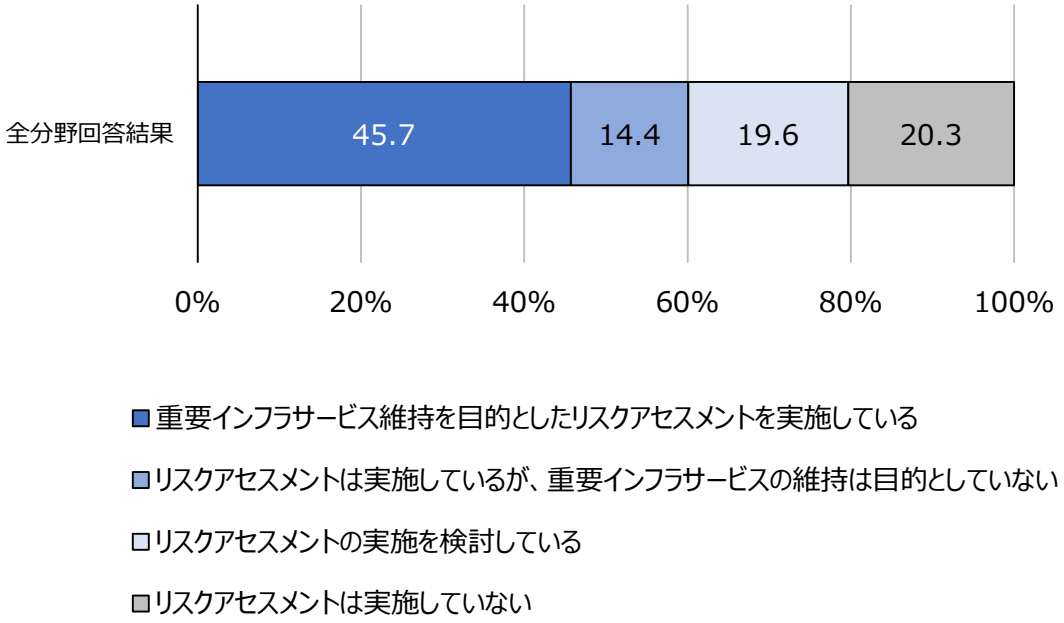
設問38.【単一回答】
自組織の重要インフラサービスに関する外部環境及び内部環境について、近い将来の状況も含めて整理していますか。



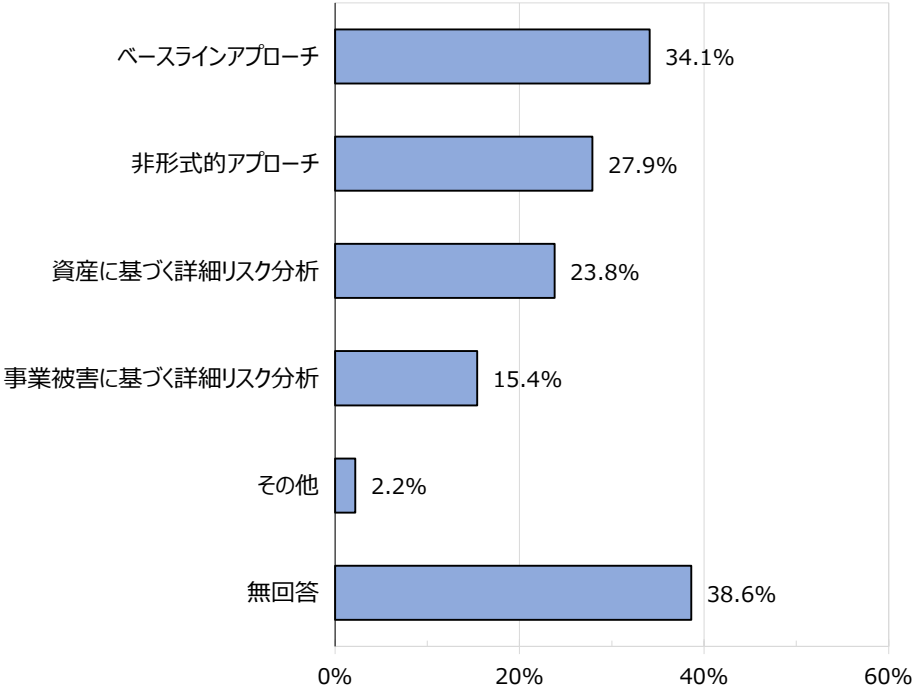
設問40.【複数回答】
任務保証の観点から、以下の自組織の特性について整理し、把握しているものを選択してください。



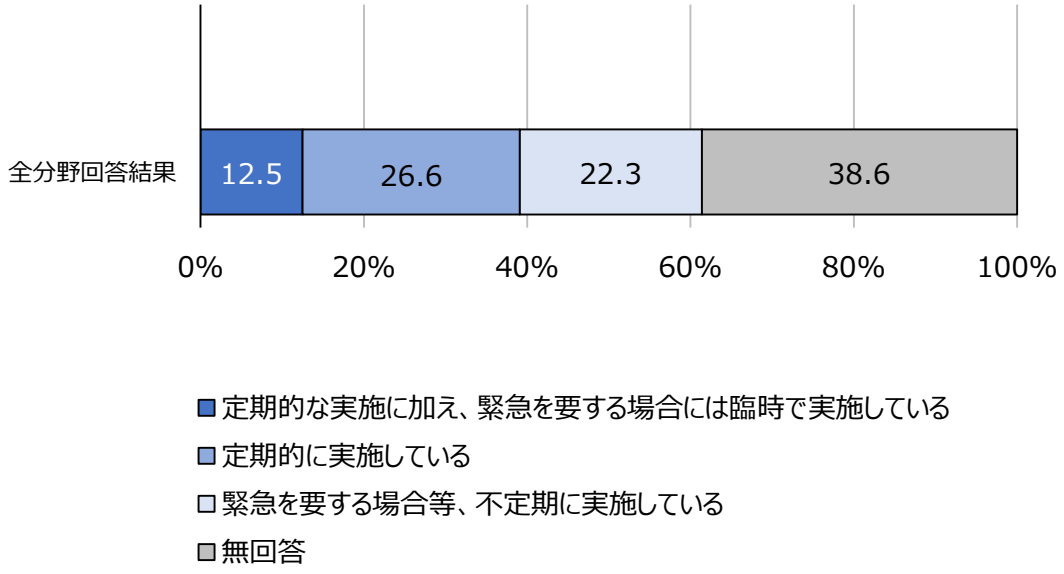
設問42.【単一回答】
サイバーセキュリティ確保の取組実施に当たって、情報の保護だけでなく、重要インフラサービス維持（事業継続）を目的としたリスクアセスメント（リスクの特定・分析・評価）を実施していますか。



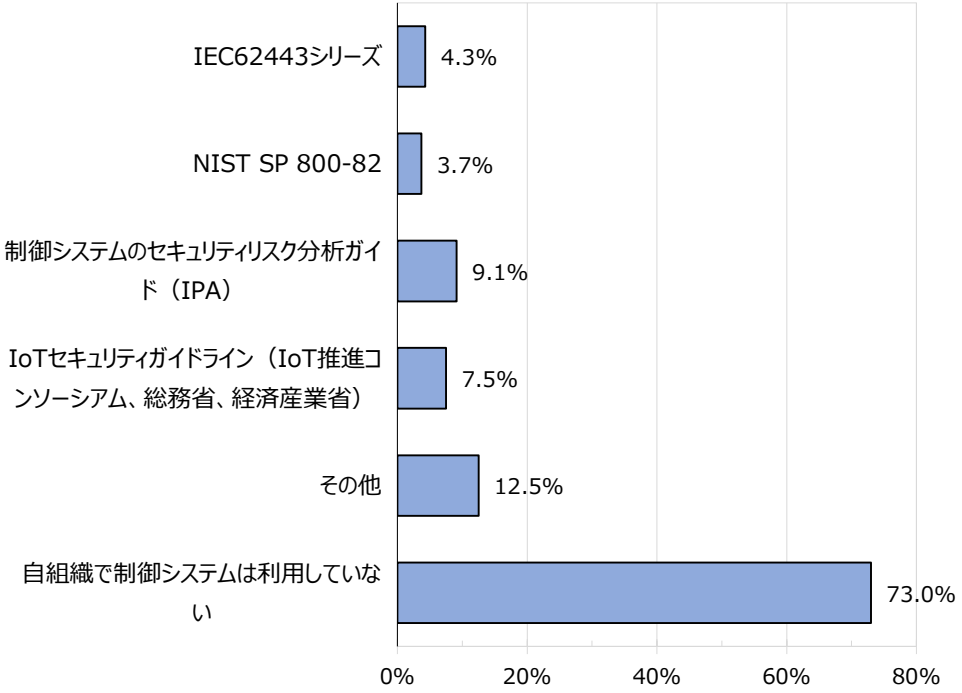
設問44.【複数回答】
自組織で実施しているリスクアセスメントの方法を全て選択してください。



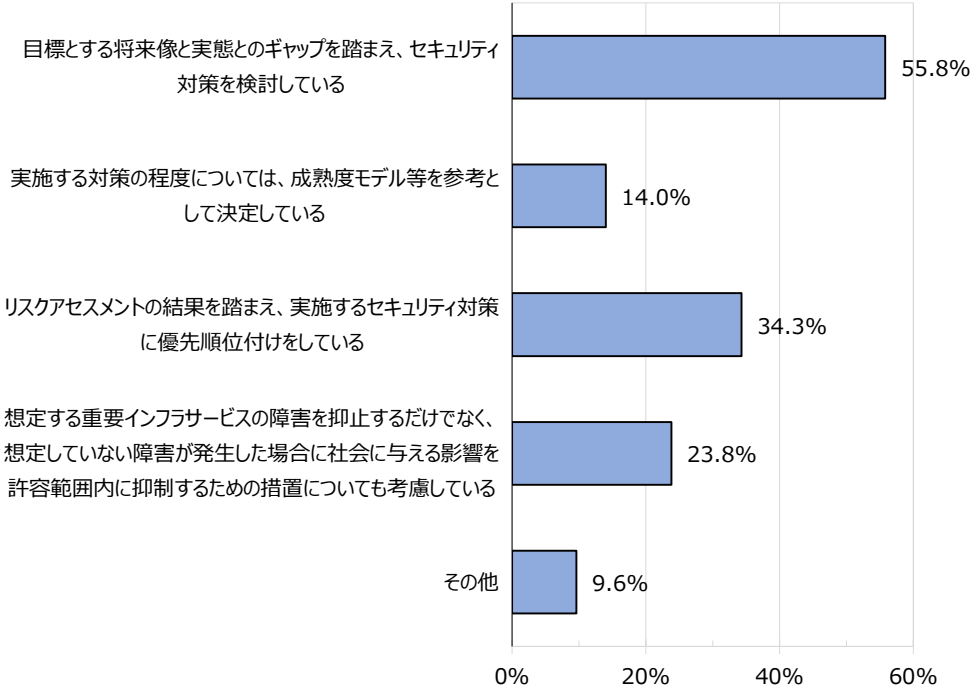
設問46.【単一回答】
サイバーセキュリティに係るリスクアセスメントを定期的に実施していますか。



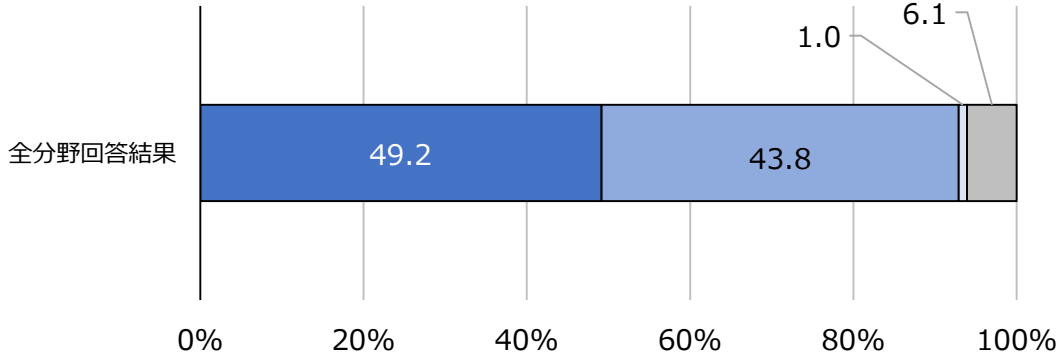
設問48.【複数回答】
制御システムのセキュリティ確保に当たって参考としているものを全て選択してください。



設問50.【複数回答】
セキュリティ対策の検討にあたり、自組織の対応状況を選択してください



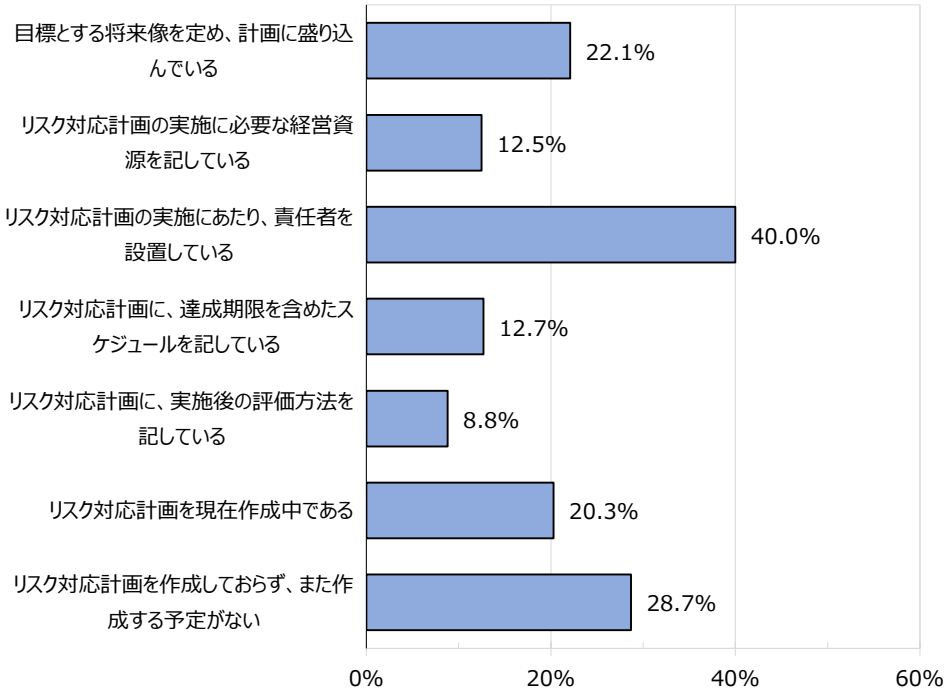
設問52.【単一回答】
個々のセキュリティ対策について、自組織の対応状況を回答してください



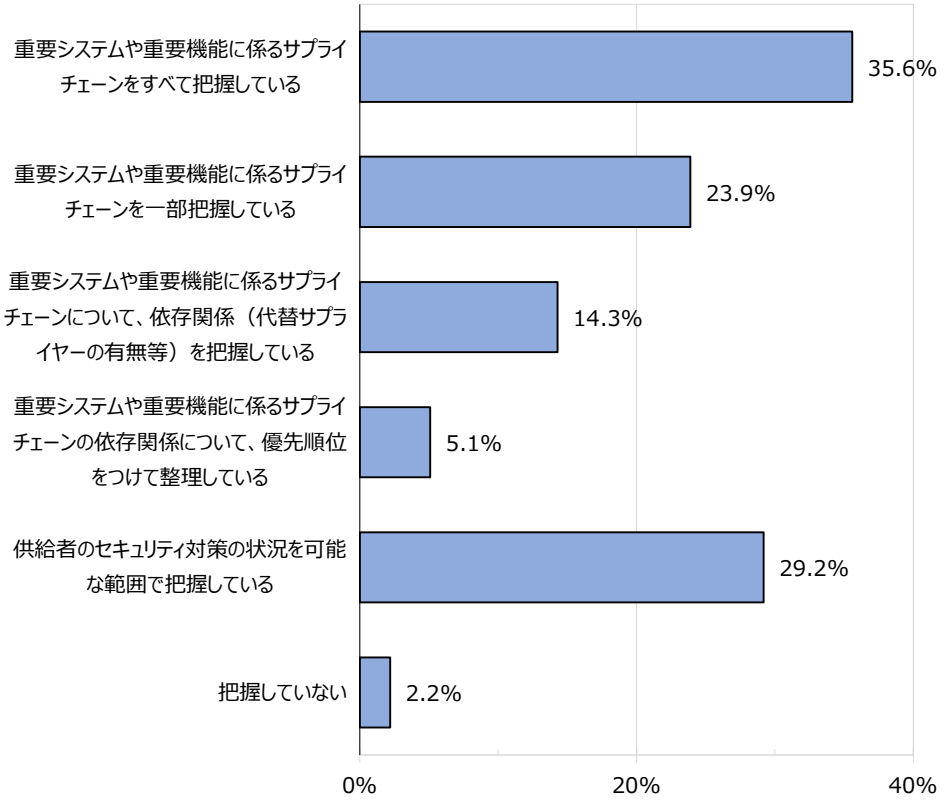
■セキュリティ対策において遵守すべき行為や判断基準を、個別方針として取り決め、組織内へ伝達している
■１に加え、必要に応じて委託先に対しても伝達し、遵守を求めている

□セキュリティ対策において遵守すべき行為や判断基準を、個別方針として取り決めているが、組織の内外へは伝達していない
□個々の対策ごとに個別方針は定めていない

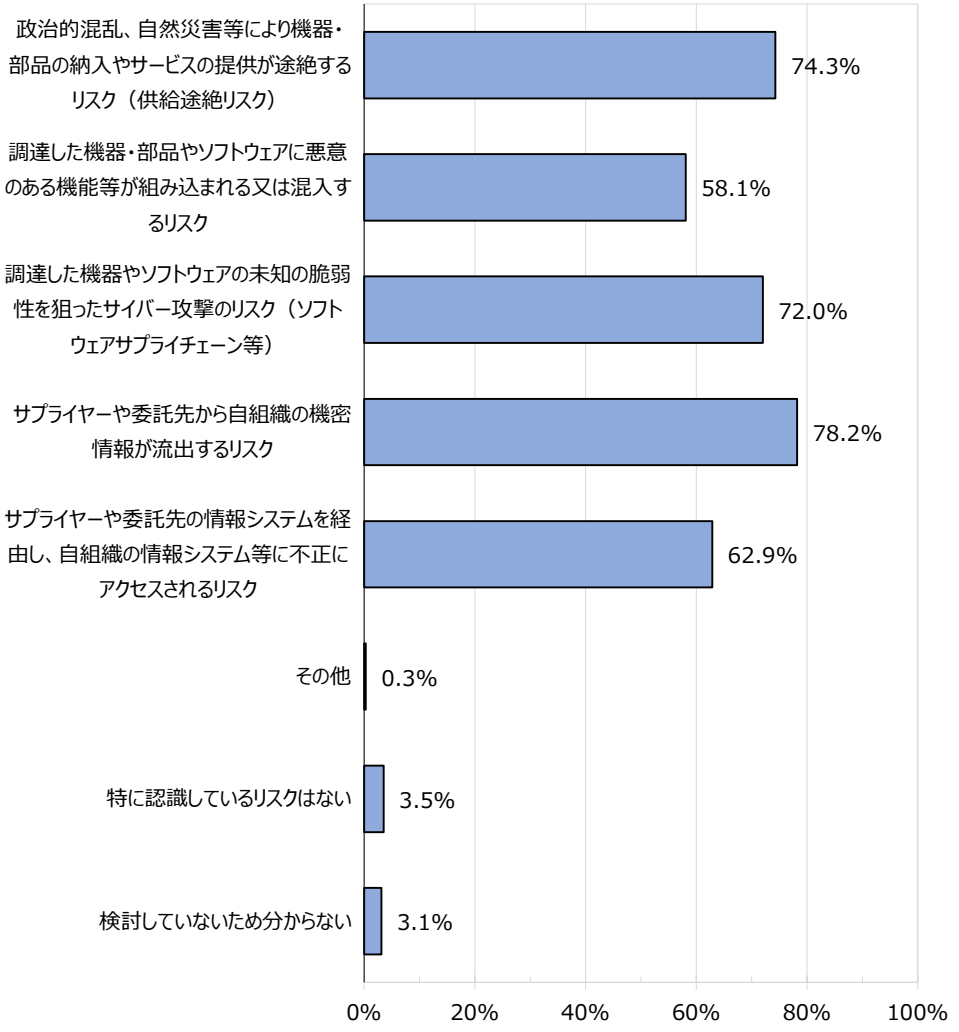
設問54.【複数回答】
サイバーセキュリティ確保の取組に向けたリスク対応計画について回答してください。



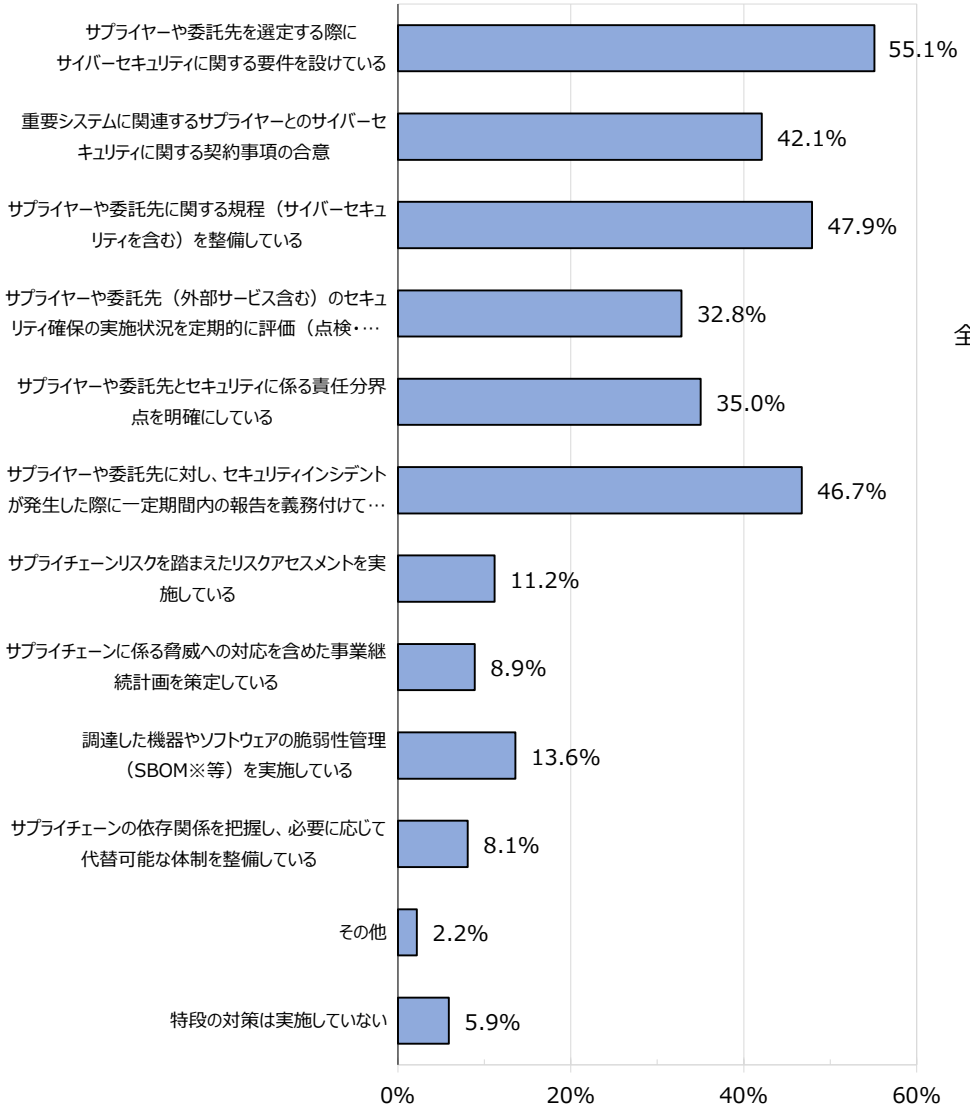
設問56.【複数回答】
自組織の重要システムや重要機能に係るサプライチェーンに関して現在の状況を回答してください。



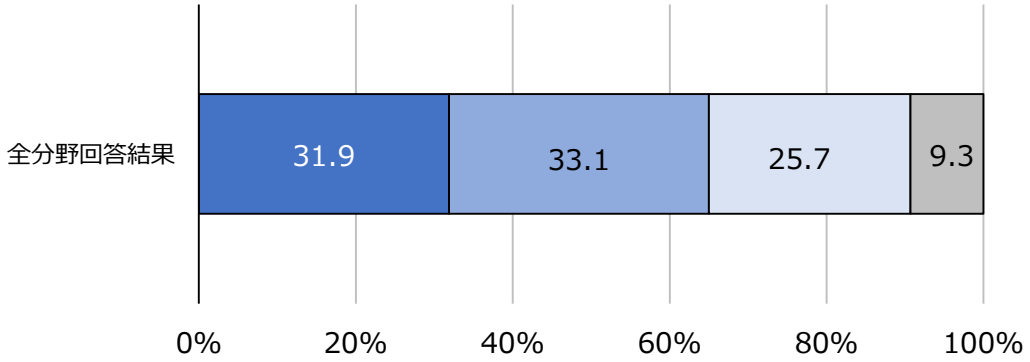
設問59.【複数回答】
サプライチェーンについて、自組織で認識しているリスクを全て選択してください。



設問61.【複数回答】
自組織のサプライチェーンに関するリスクについて、実施しているリスク軽減策を全て選択してください。

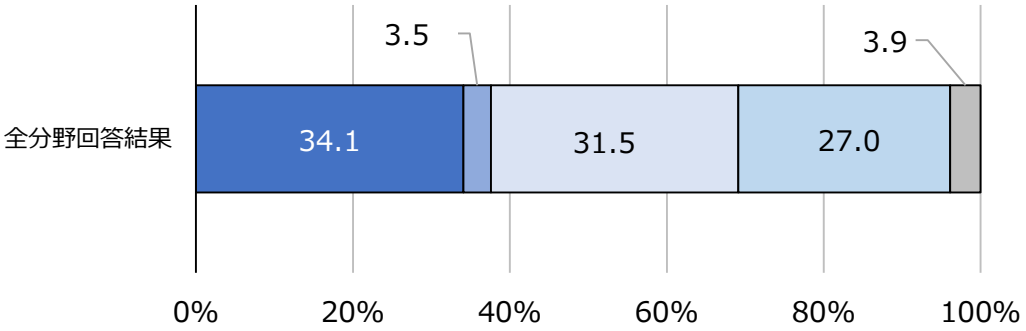


設問64.【単一回答】
重要インフラサービス障害の発生に備えたコンティンジェンシープランを策定していますか。



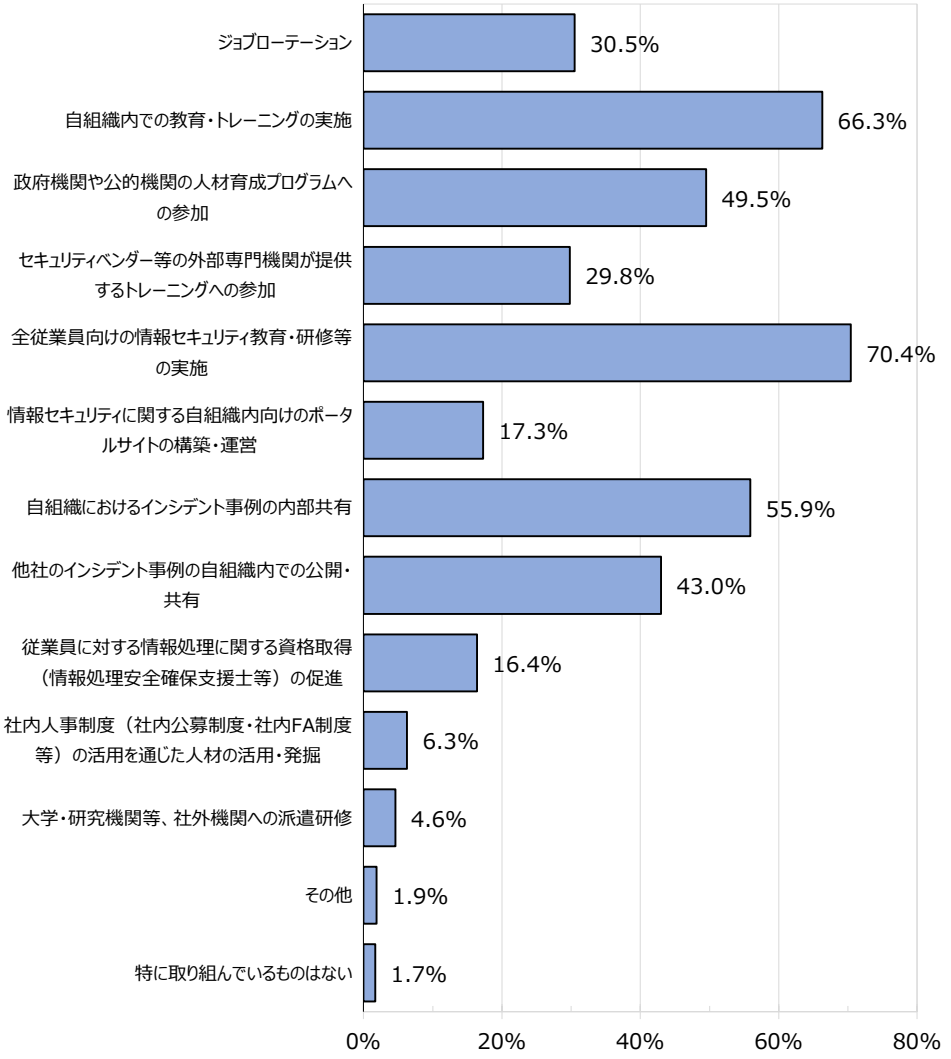
- サイバー攻撃への備えも取り入れたコンティンジェンシープランを策定している
- コンティンジェンシープランは策定しているが、サイバー攻撃への備えを目的とした要素は取り入れられていない
- コンティンジェンシープランの策定を検討している
- コンティンジェンシープランを策定する予定はない

設問66.【単一回答】
重要インフラサービス障害の発生に備えた事業継続計画を策定していますか。また、事業復旧計画を策定していますか。

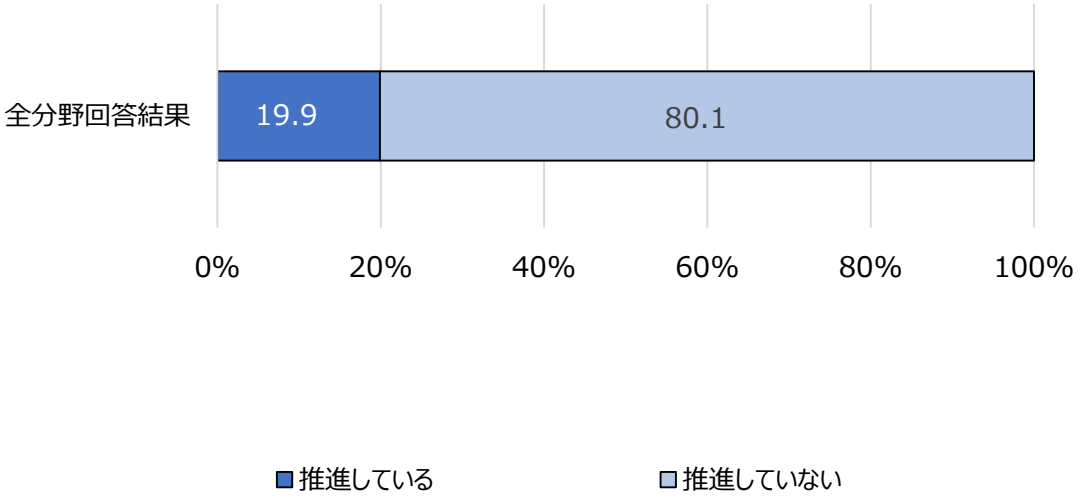


- 事業継続計画及び事業復旧計画を策定している。
- 事業継続計画は策定しており、事業復旧計画を策定中である。
- 事業継続計画は策定しているが、事業復旧計画は策定していない。
- 事業継続計画の策定を検討している、もしくは作成中である
- 事業継続計画を策定する予定はない

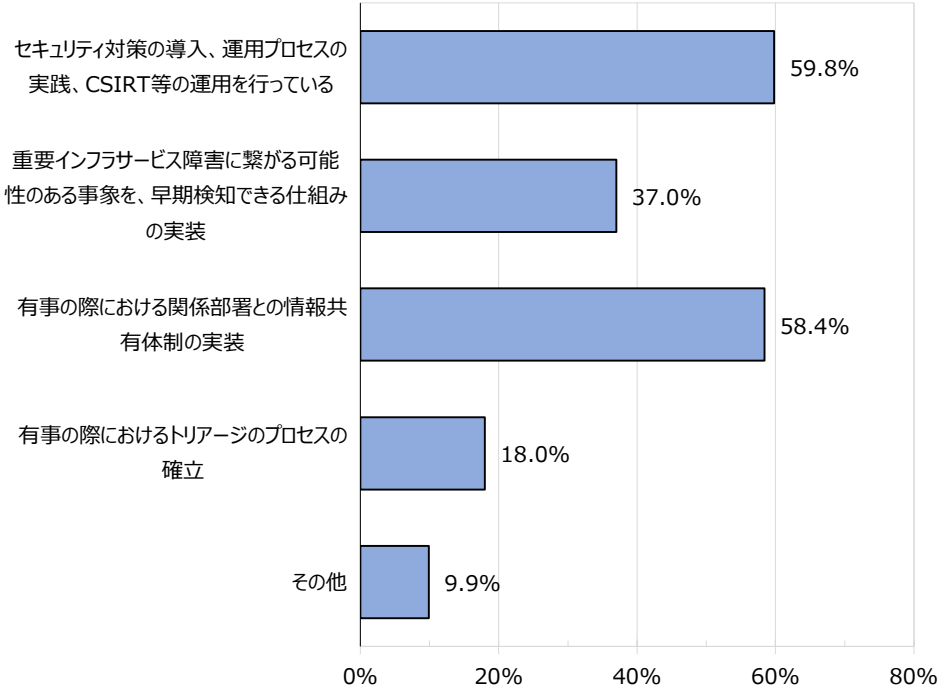
設問68.【複数回答】
セキュリティ人材の育成や従業員の意識啓発について、自組織で取り組んでいるものを全て選択してください。



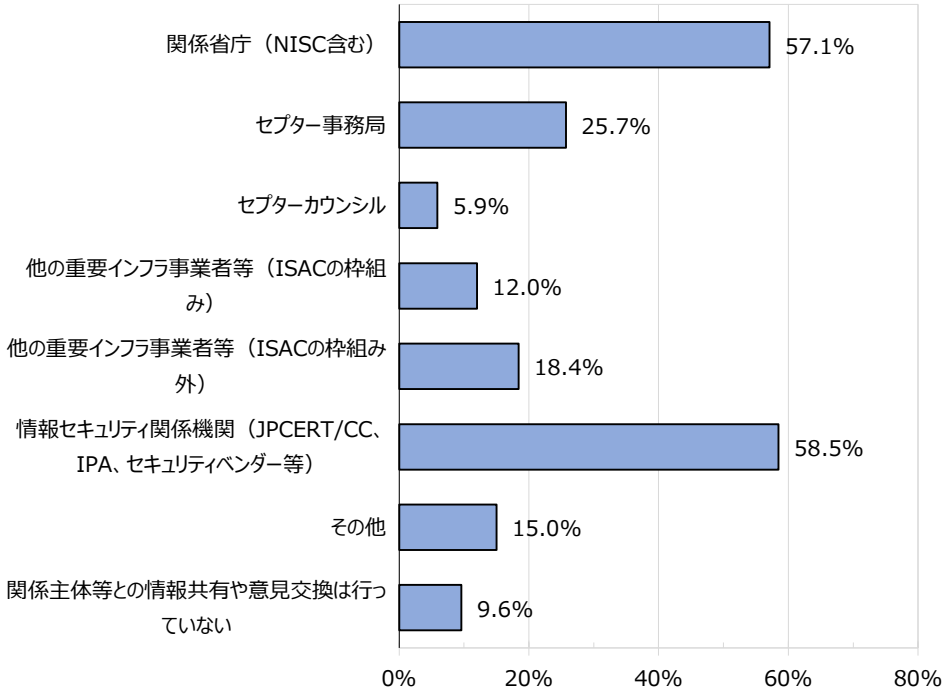
設問72.【単一回答】
自組織において、セキュリティ対策業務に従事する人材に対して、情報処理安全確保支援士の資格取得を推進していますか。



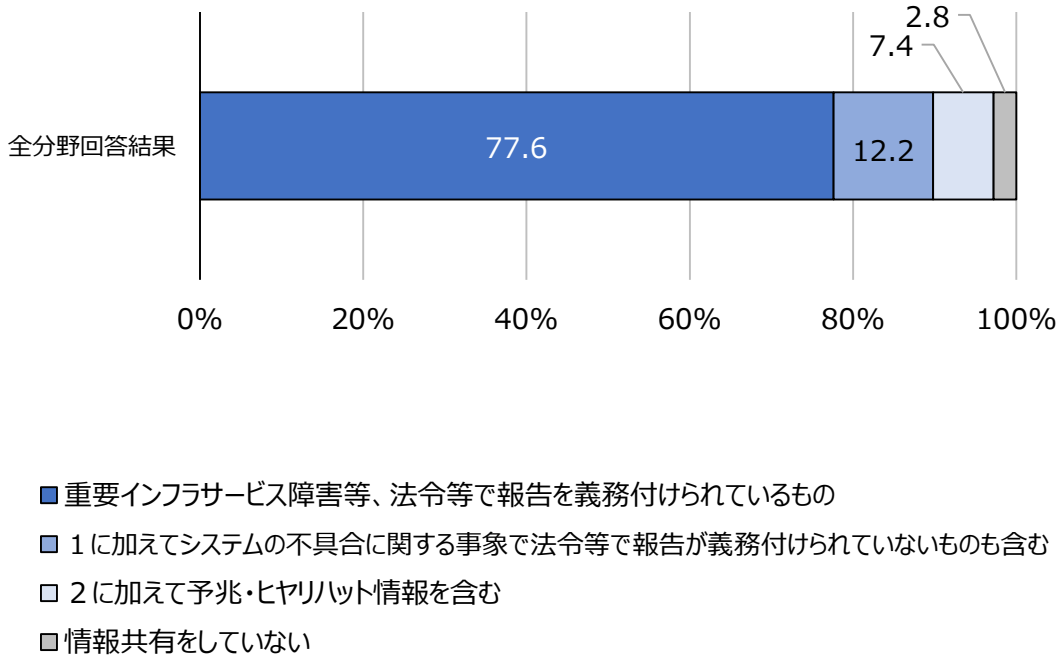
設問74.【複数回答】
リスク対応計画の実施について、状況を選択してください



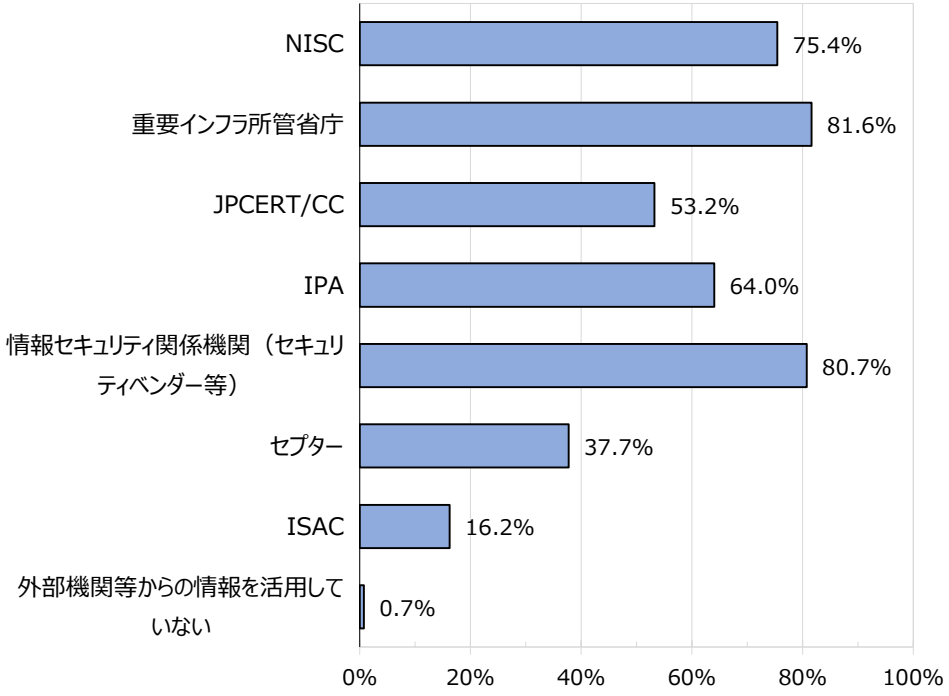
設問76.【複数回答】
重要インフラサービスの安全かつ持続的な提供を実現するという観点から、情報共有や意見交換を行っている関係主体を全て選択してください。



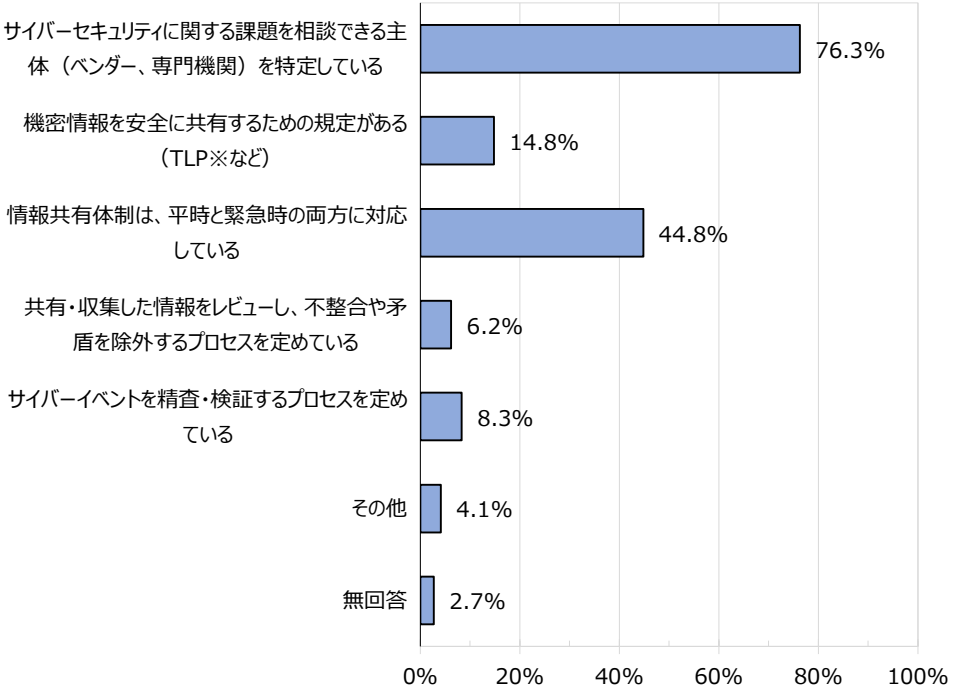
設問79.【単一回答】
自組織の情報システムの不具合について、重要インフラ所管省庁等との情報共有の対象範囲を選択してください。



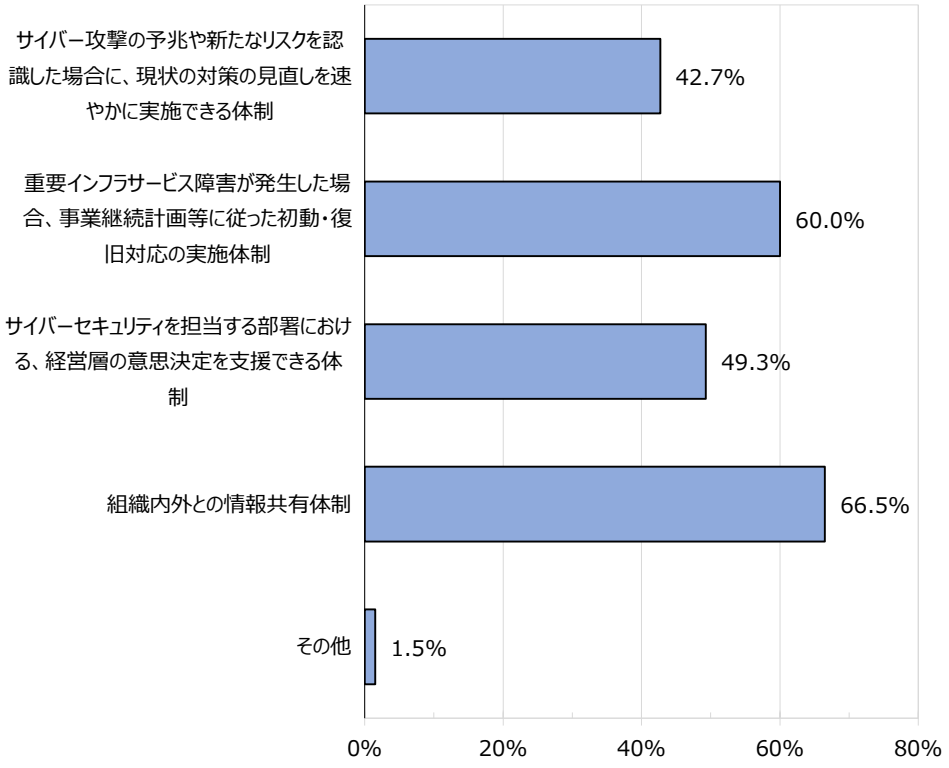
設問81.【複数回答】
自組織で活用している情報の提供元を全て選択してください。



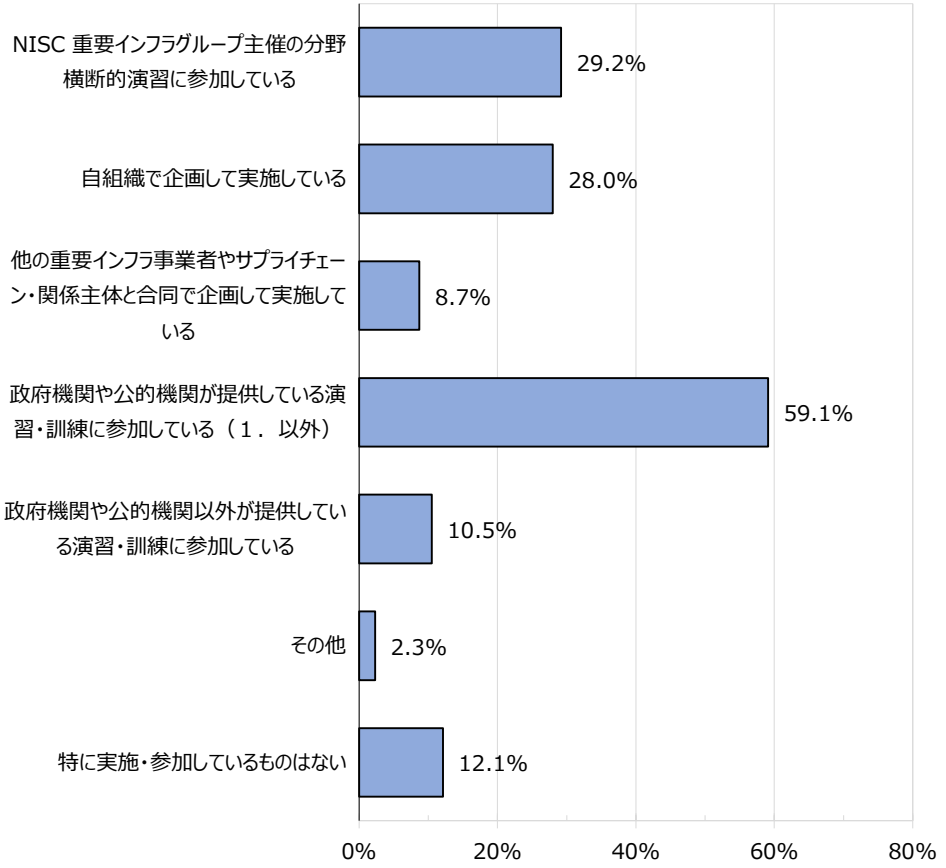
設問83.【複数回答】
情報共有において、自組織で実践しているものを選択してください



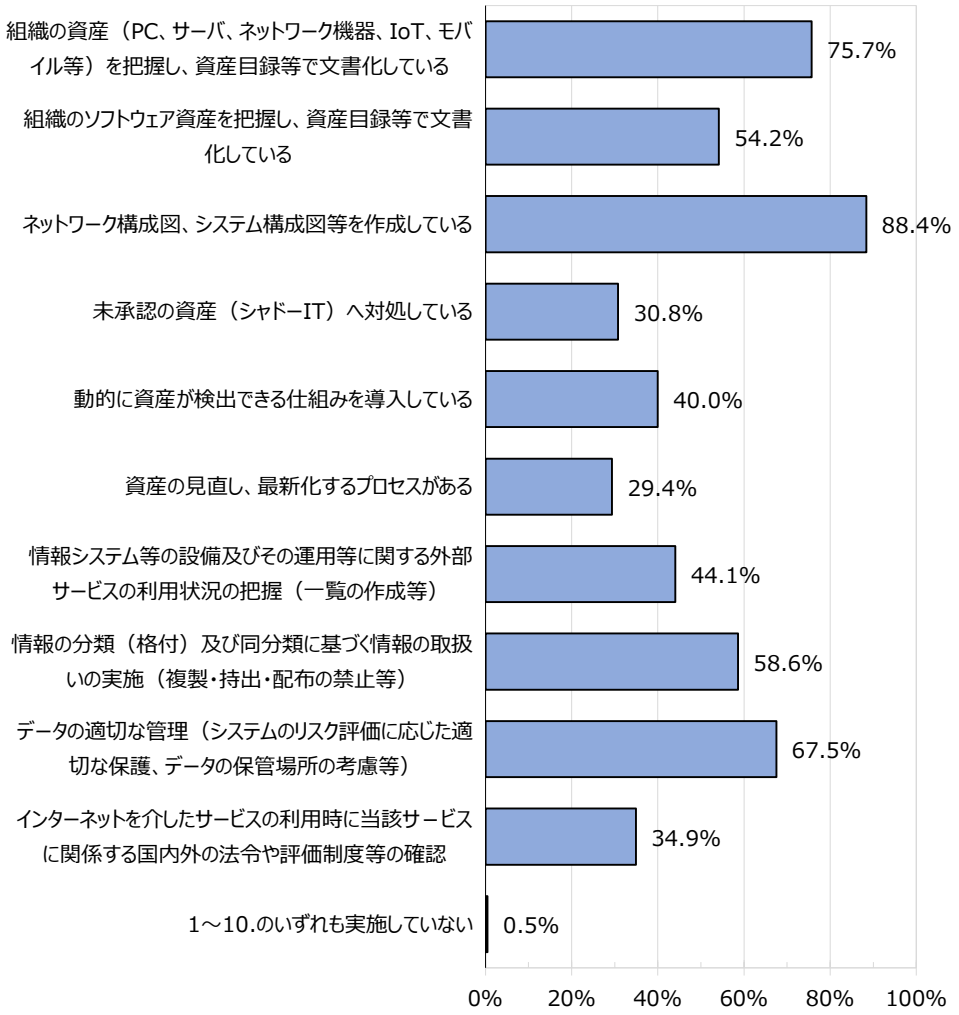
設問85.【複数回答】
危機管理体制において、自組織の状況を回答してください



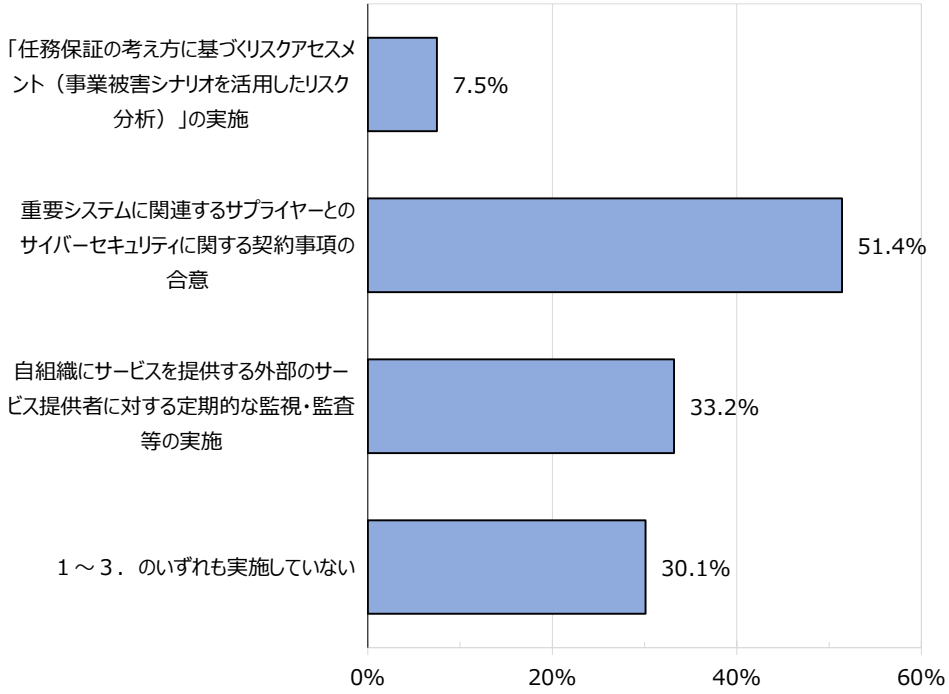
設問87.【複数回答】
サイバーセキュリティ確保に関する演習・訓練について実施・参加しているものを全て選択してください。



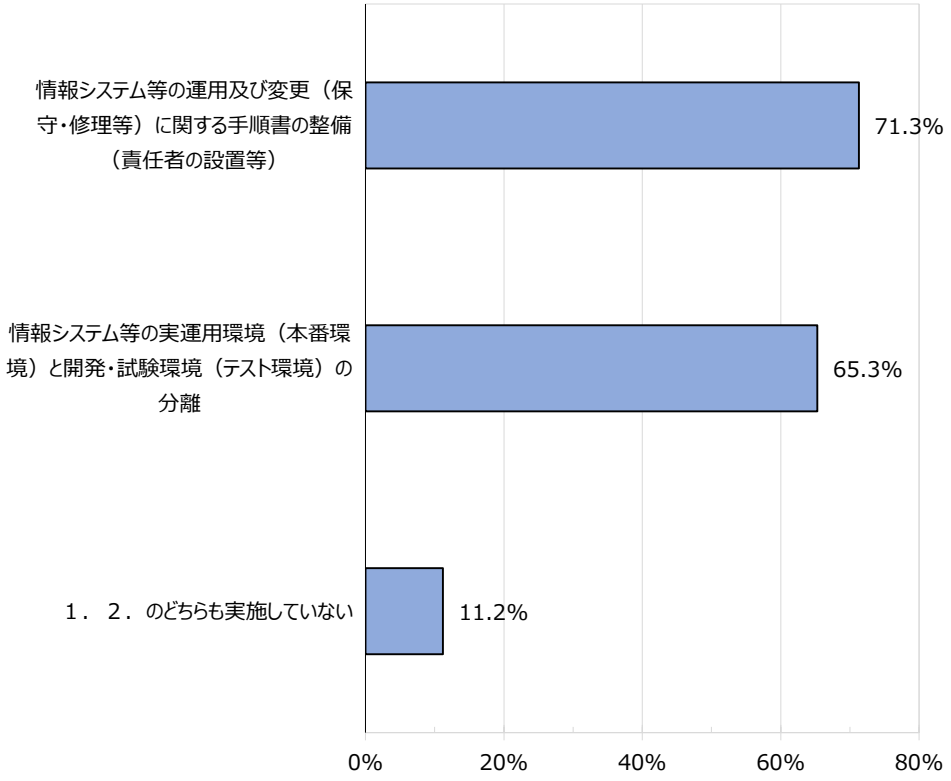
設問90.【複数回答】
資産・情報・データ等の管理に関して、実施している取組を選択してください。



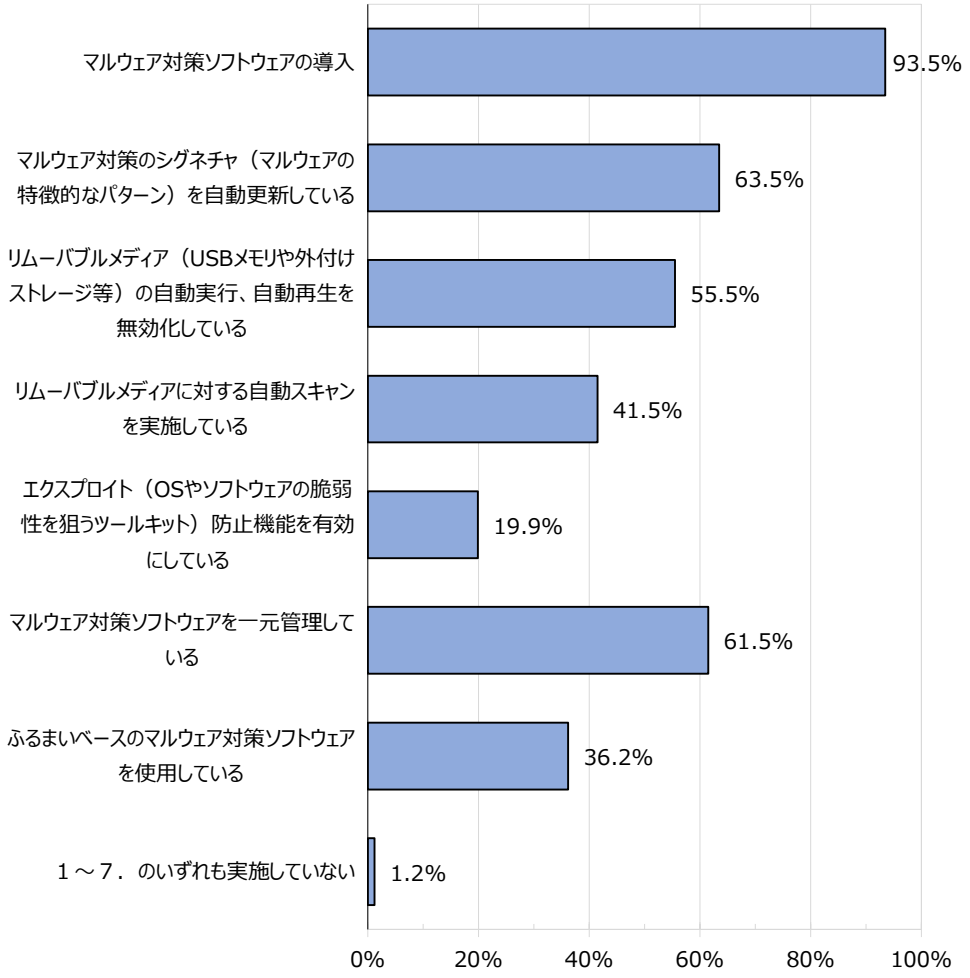
設問91.【複数回答】
供給者管理に関して、実施している取組を選択してください。



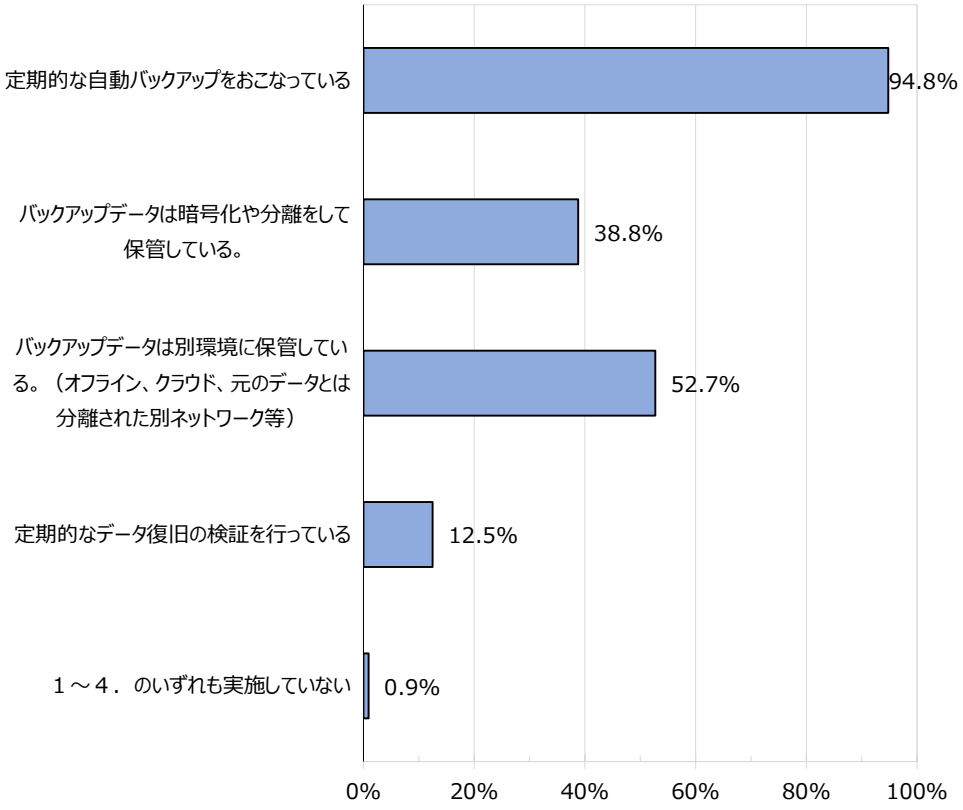
設問92.【複数回答】
運用時のセキュリティ管理に関して、実施している取組を選択してください。



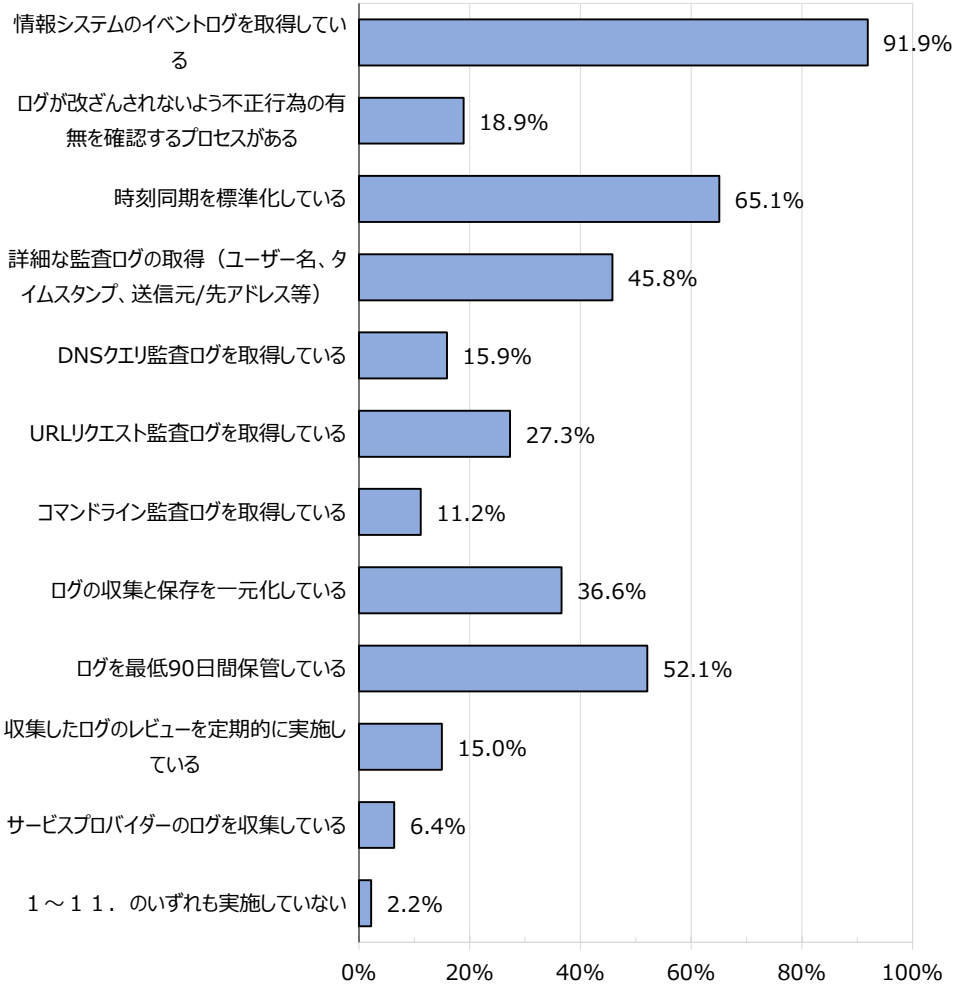
設問93.【複数回答】
マルウェアからの防御のため、実施している取組を選択してください。



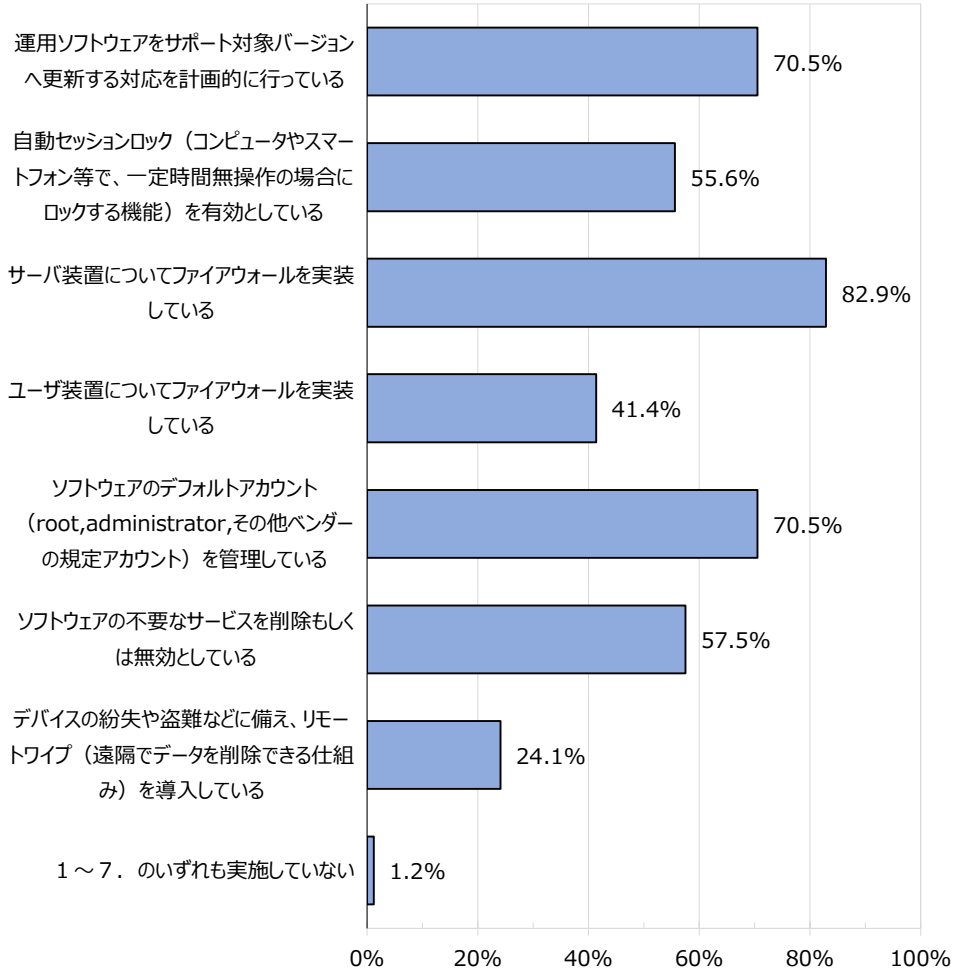
設問94.【複数回答】
バックアップに関して実施している取組を選択してください。



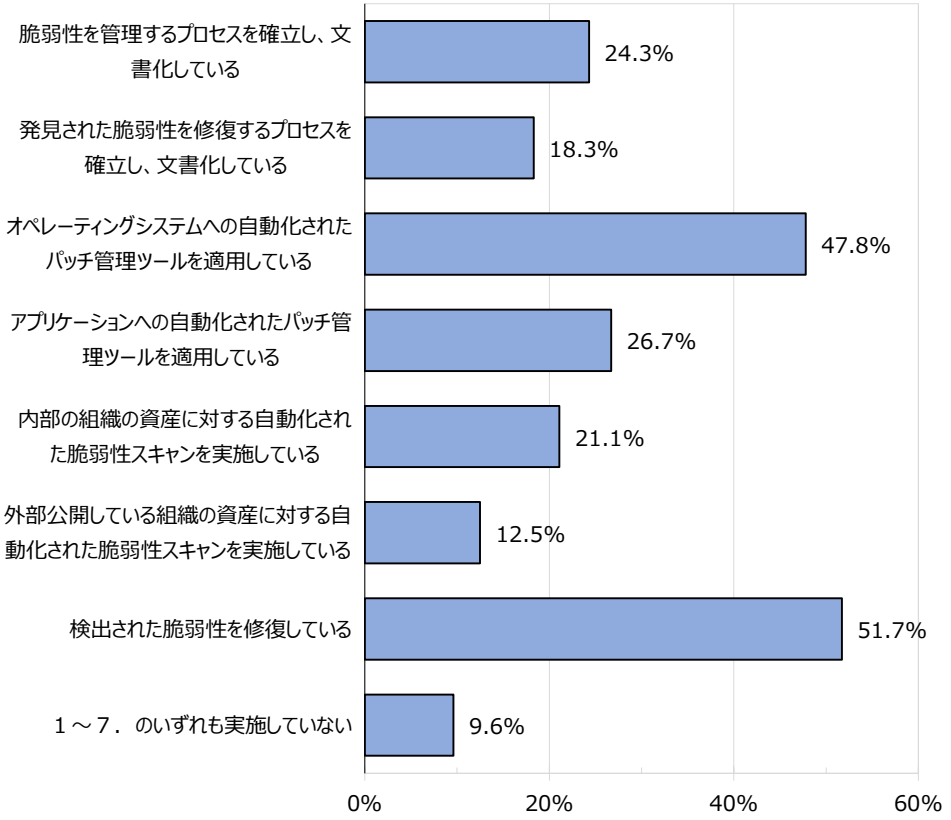
設問95.【複数回答】
ログ管理に関して実施している取組を選択してください。



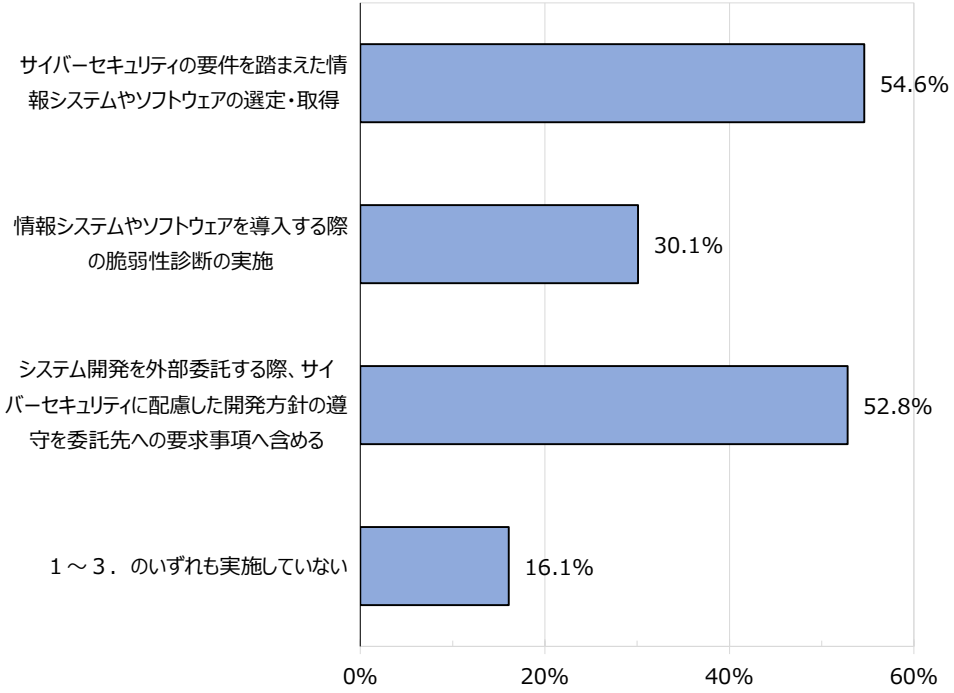
設問96.【複数回答】
運用ソフトウェアの管理について実施している取組を選択してください。



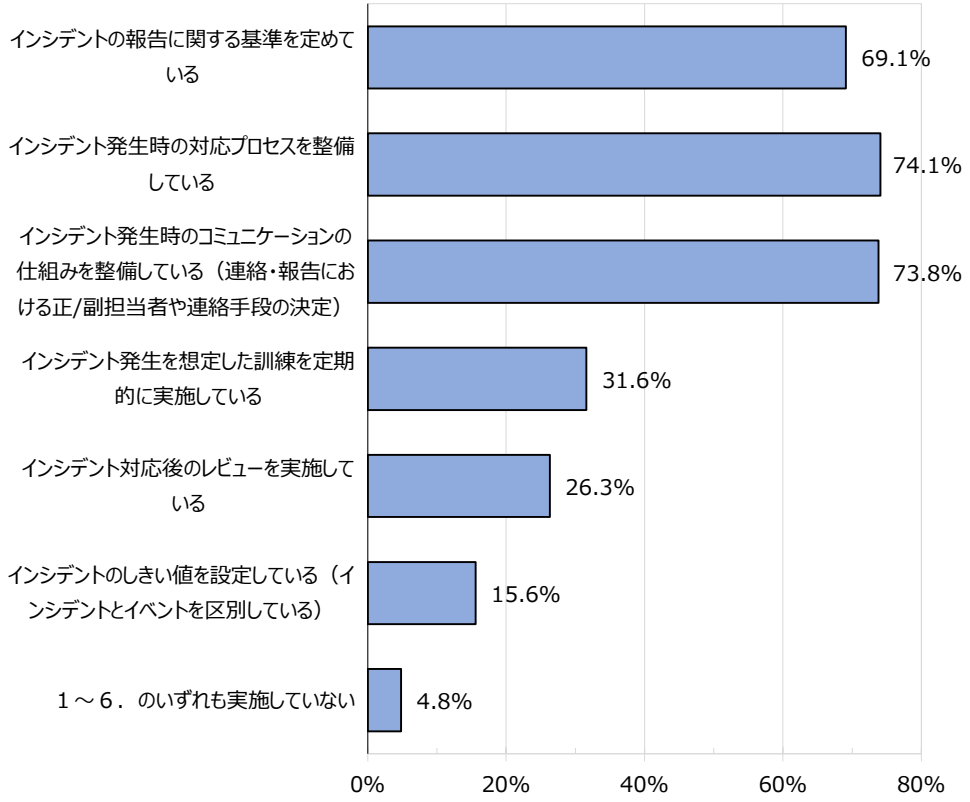
設問97.【複数回答】
脆弱性管理について実施している取組を選択してください。



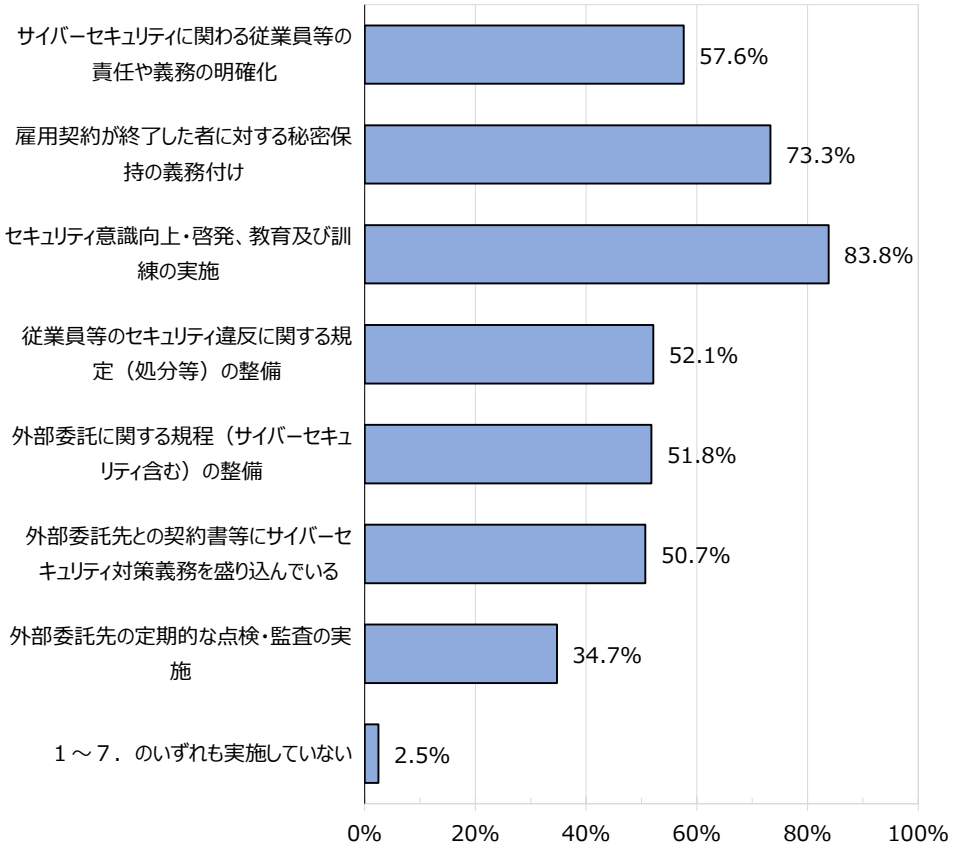
設問98.【複数回答】
システムの取得・開発及び保守に関して、実施している取組を選択してください。



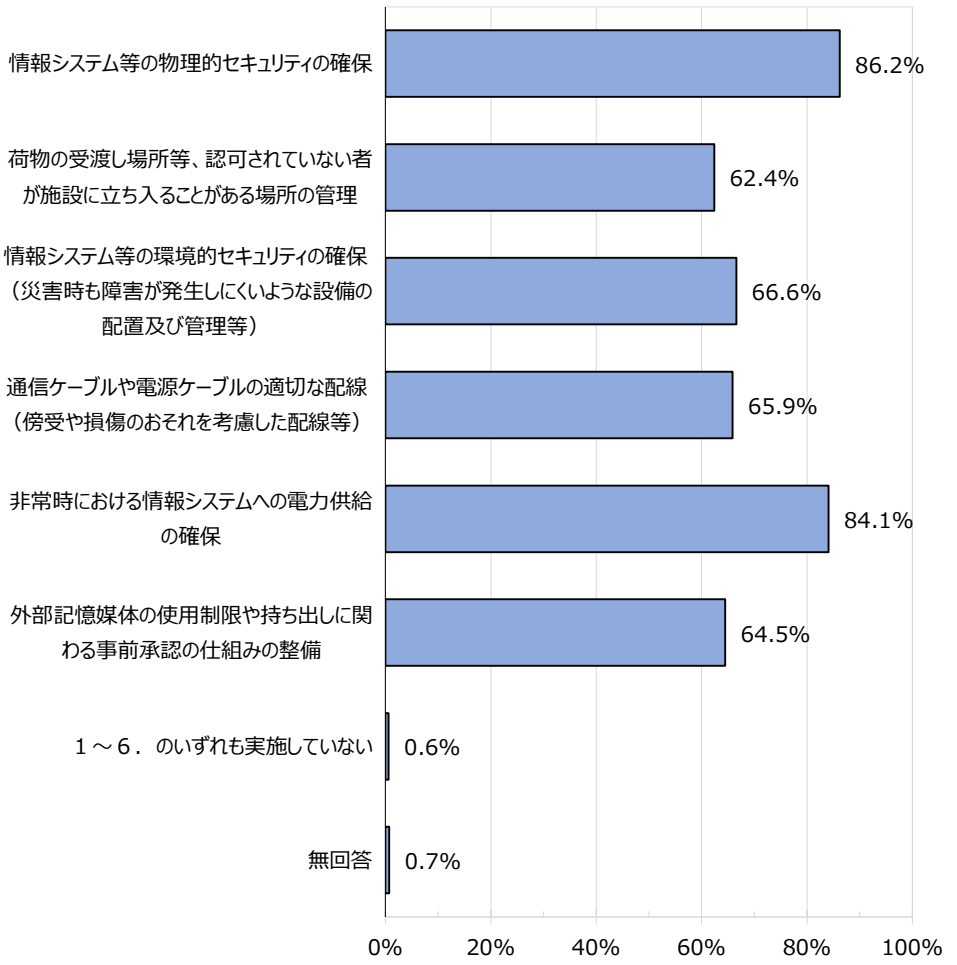
設問99.【複数回答】
インシデント管理について実施している取組を選択してください。



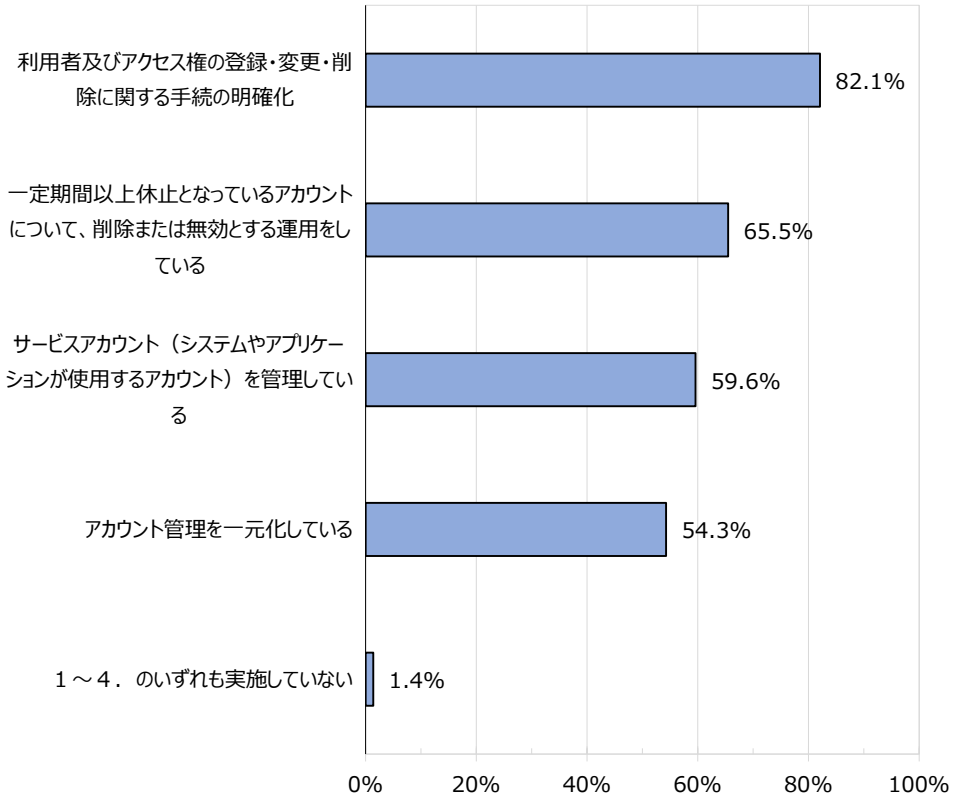
設問100.【複数回答】
人的資源及び外部委託について、実施している取組を選択してください。



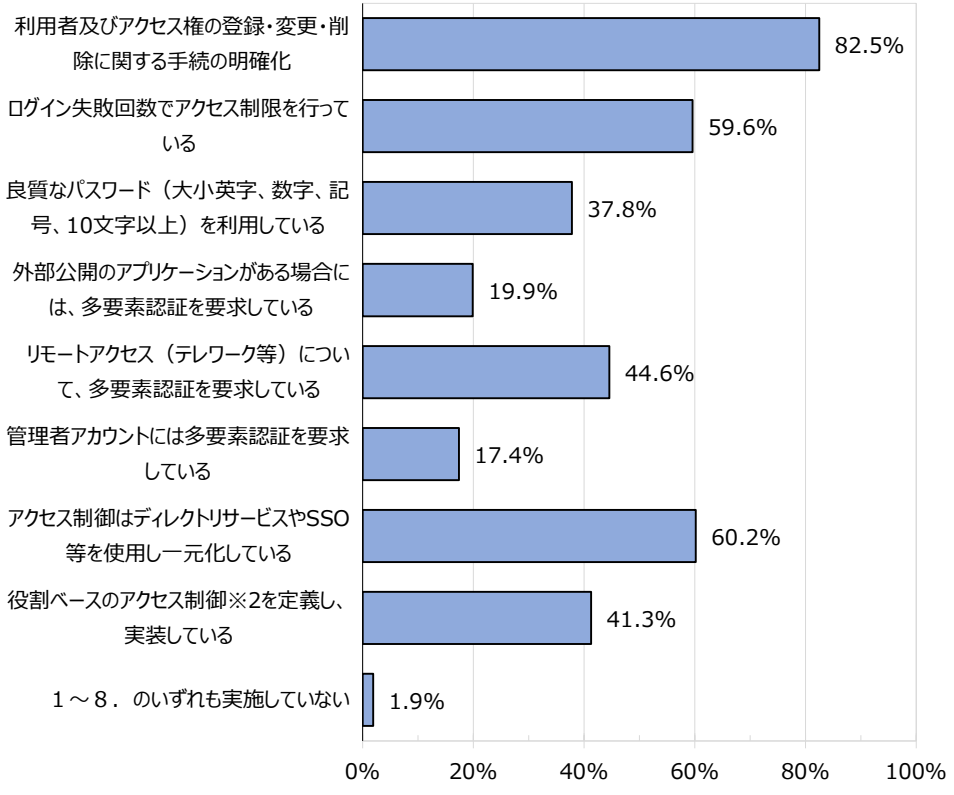
設問101.【複数回答】
物理的及び環境的セキュリティに関して、実施している取組を選択してください。



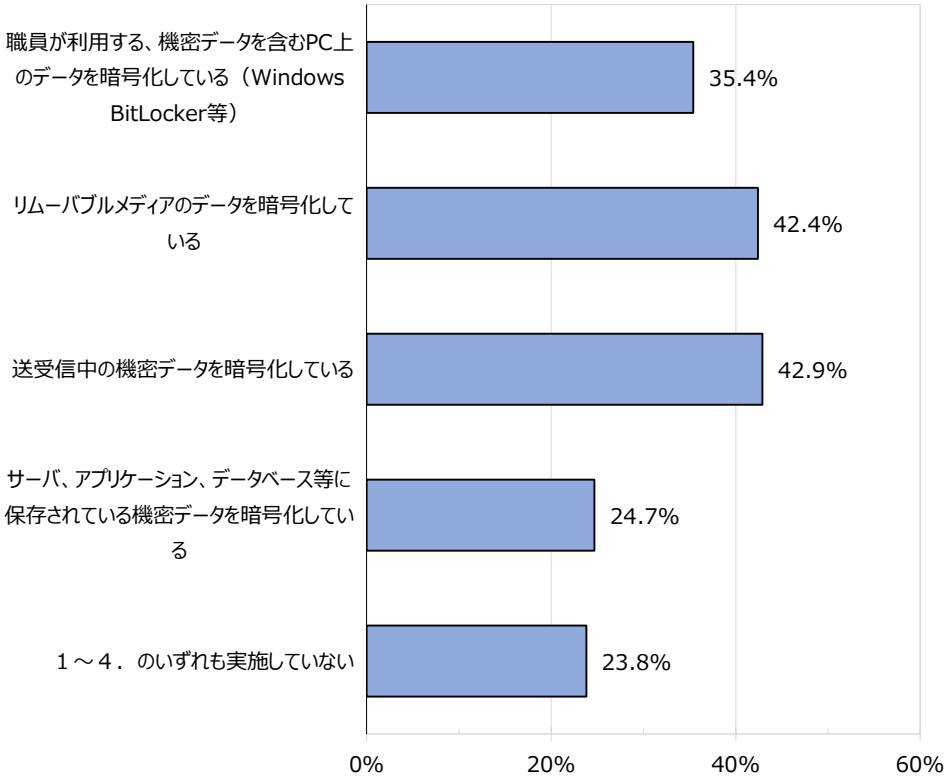
設問102.【複数回答】
アカウント管理に関して、実施している取組を選択してください。



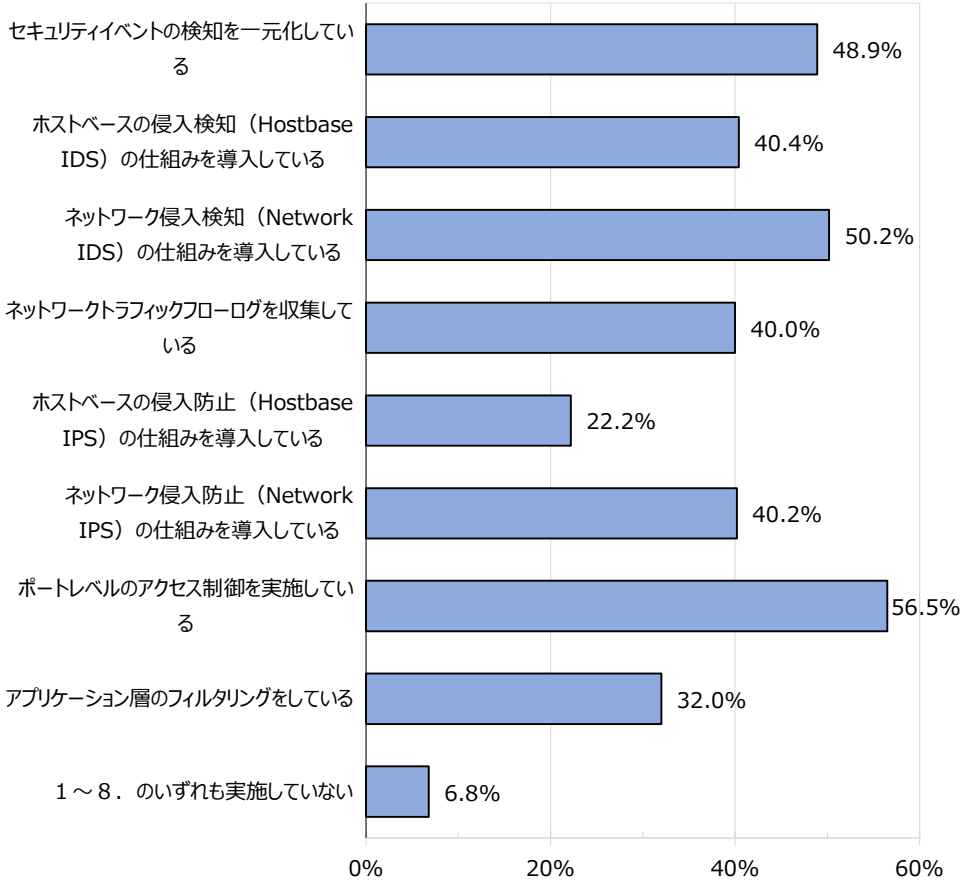
設問103.【複数回答】
アクセス制御に関して、実施している取組を選択してください。



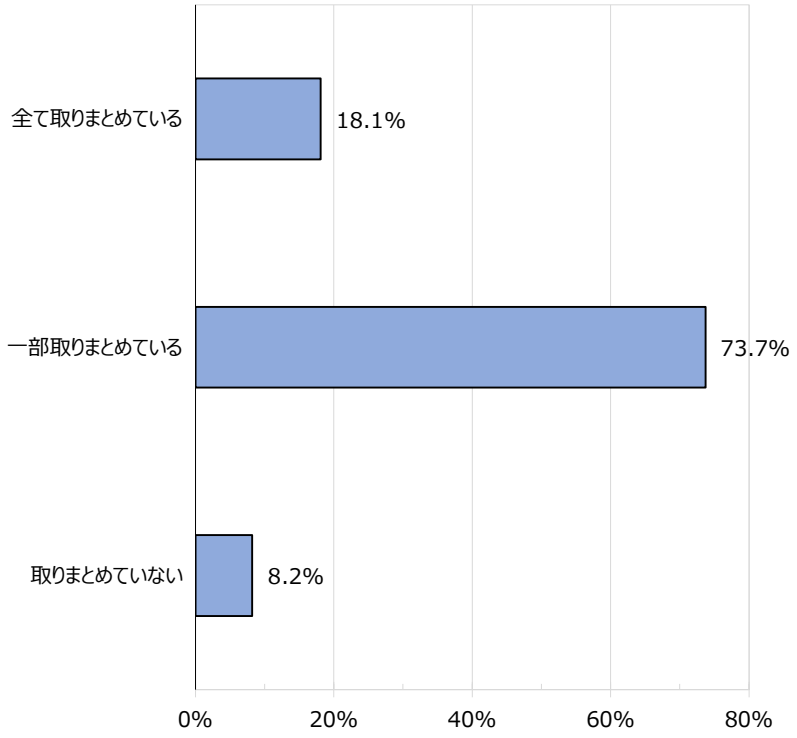
設問104.【複数回答】
暗号に関して、実施している取組を選択してください。



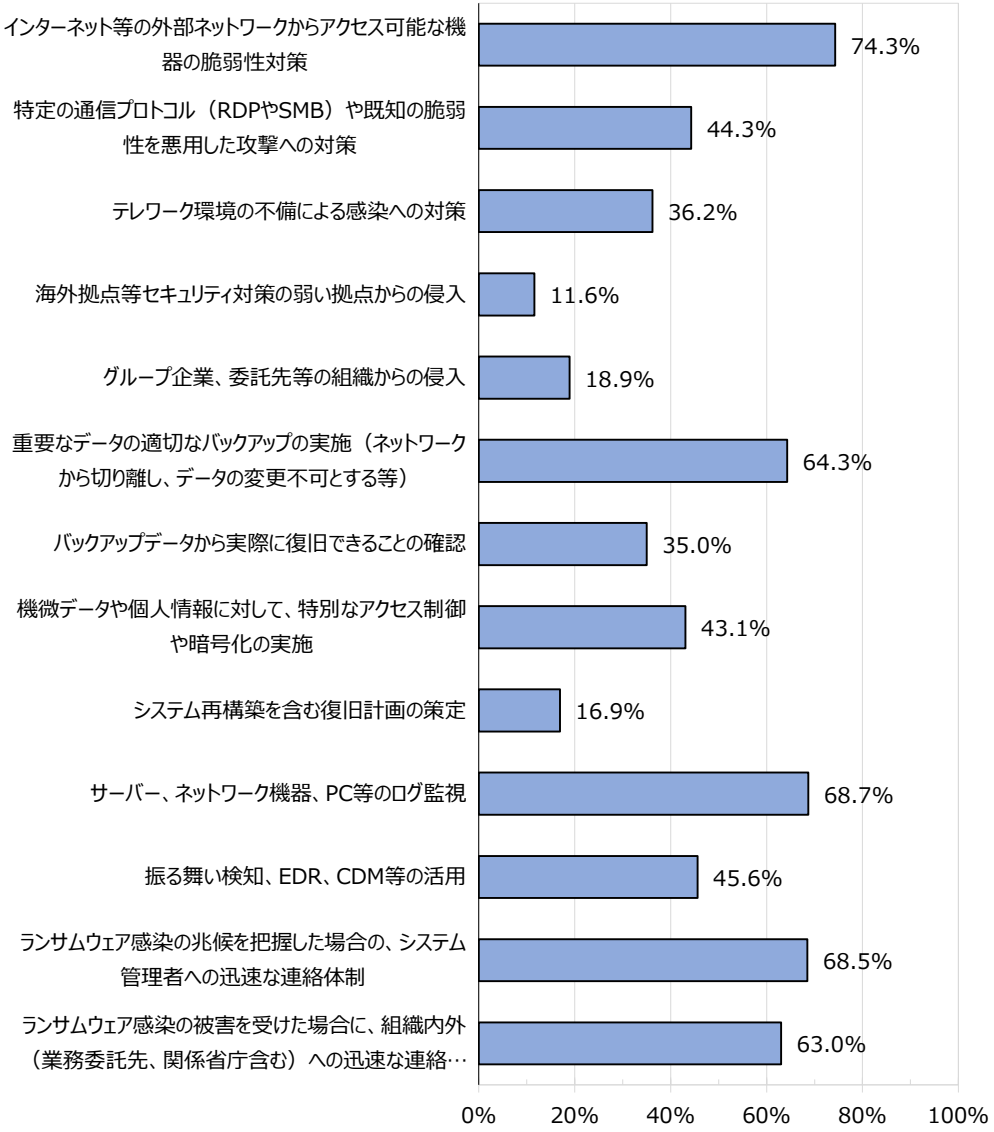
設問105.【複数回答】
通信のセキュリティに関して、実施している取組を選択してください。



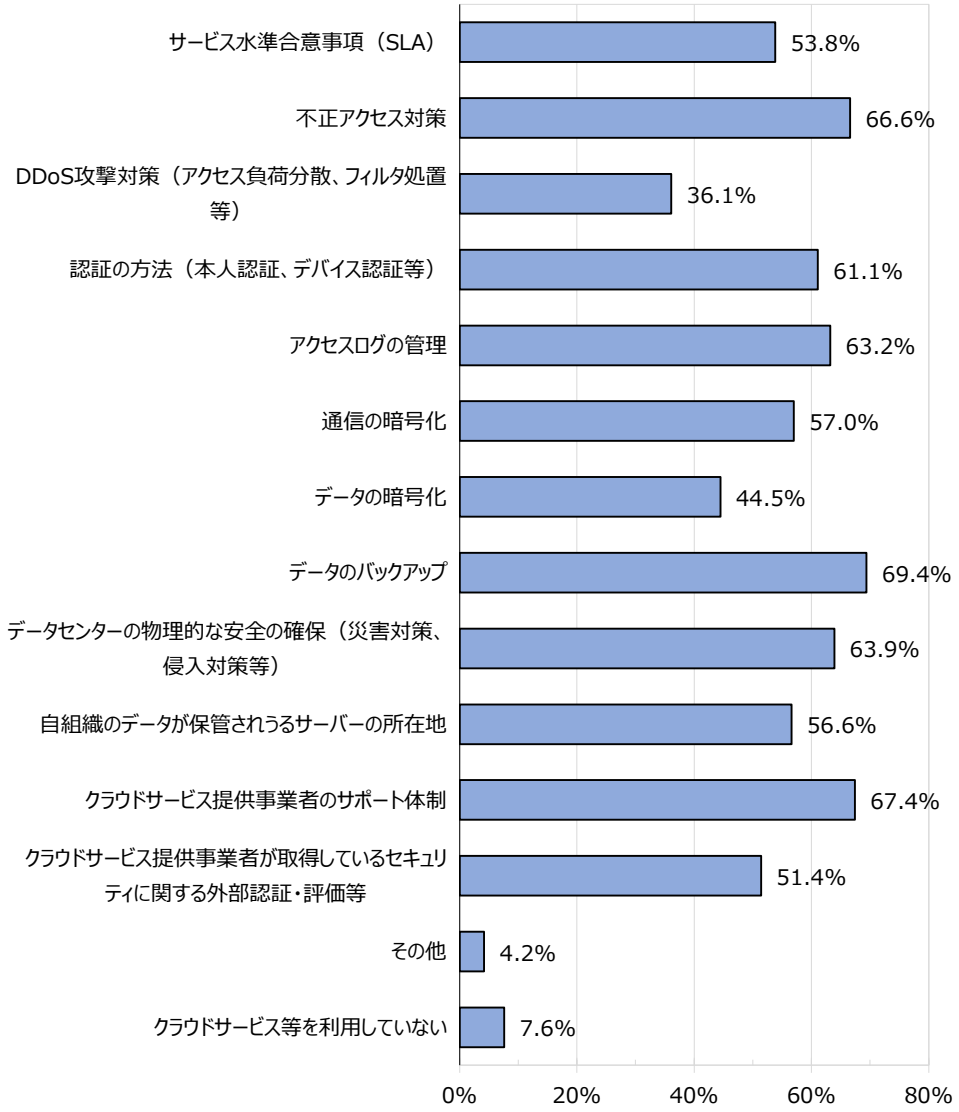
設問106. 【複数回答】
上記設問における組織的対策及び、ここの回答ページの人的、物理的、技術的対策にて、「実施している」としたサイバーセキュリティ確保の取組を内規（実施手順・マニュアル等*）として取りまとめていますか。



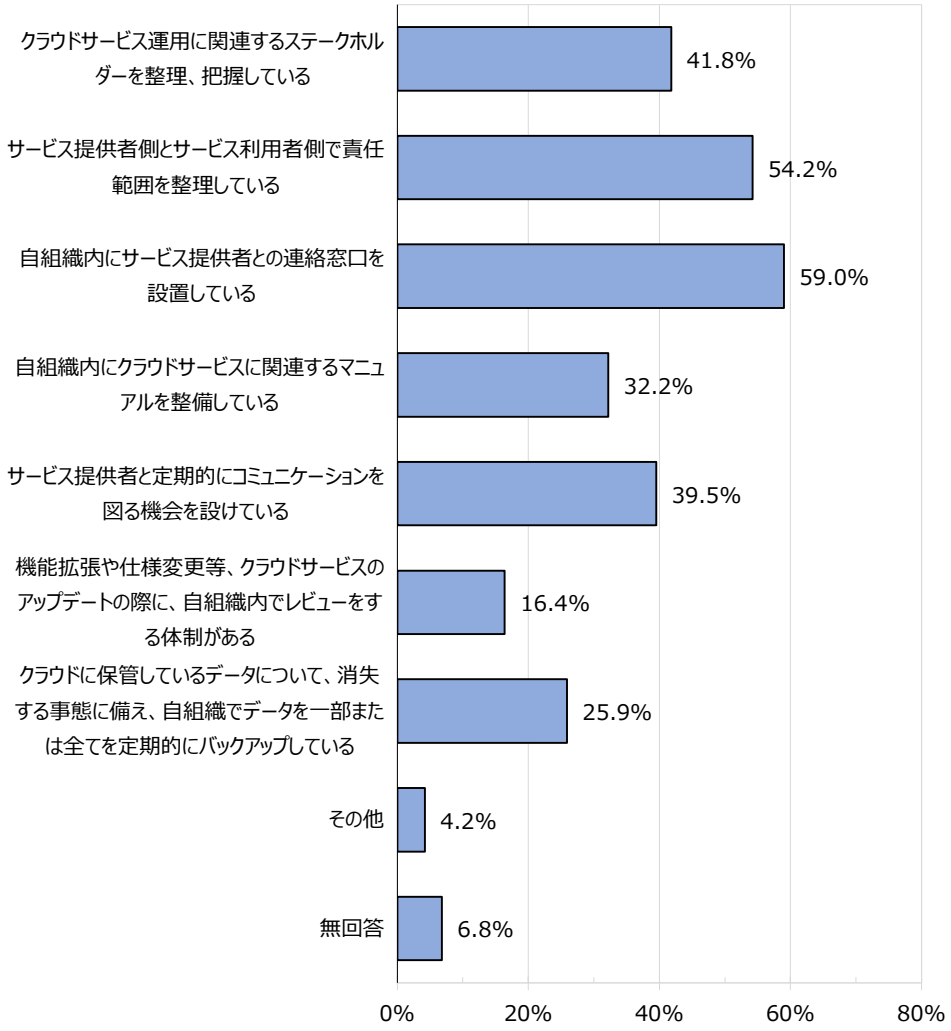
設問108.【複数回答】
ランサムウェアによるサイバー攻撃について、実施している対策、運用体制を選択してください。



設問109.【複数回答】
自組織がクラウドサービスを利用する際に、クラウドサービス提供事業者側へ確認している事項を全て選択してください。



設問111.【複数回答】
クラウドサービスを利用するに当たり、自組織で行っている運用対策を選択してください。



設問113.【複数回答】
サイバーセキュリティ確保の取組の改善に向け、継続的に見直しを行っているものを全て選択してください。