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33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［2022年度］

令和５年６月２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

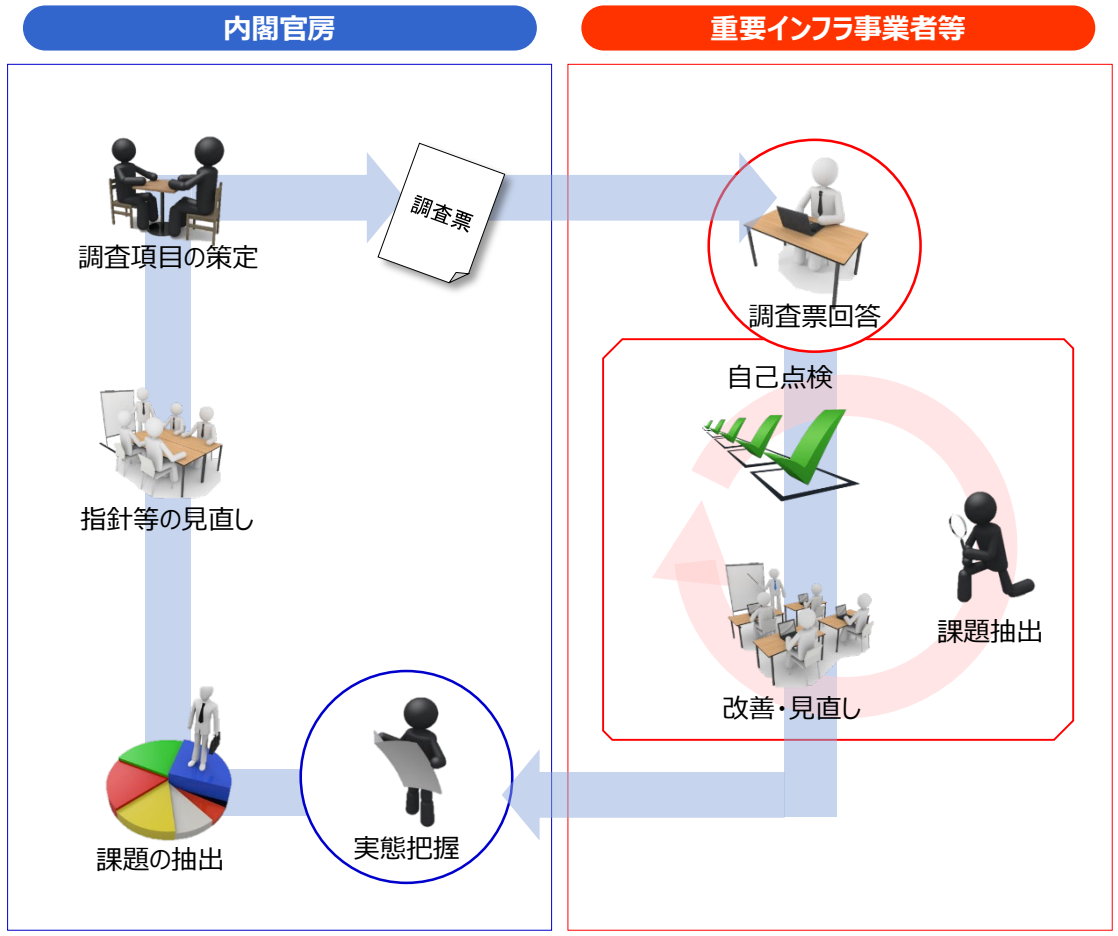
- 「重要インフラのサイバーセキュリティに係る行動計画」（以下「行動計画」という。）に基づき、**各重要インフラ分野に共通して求められるセキュリティ対策を「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）」**（以下「指針」という。）**として取りまとめ**ている。
- 重要インフラ事業者等における安全基準等（※）の浸透状況を把握するため、**重要インフラ事業者等に対しセキュリティ対策の実施状況について調査を実施**した。

（※）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：2022年３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2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）



調査対象及び回答状況

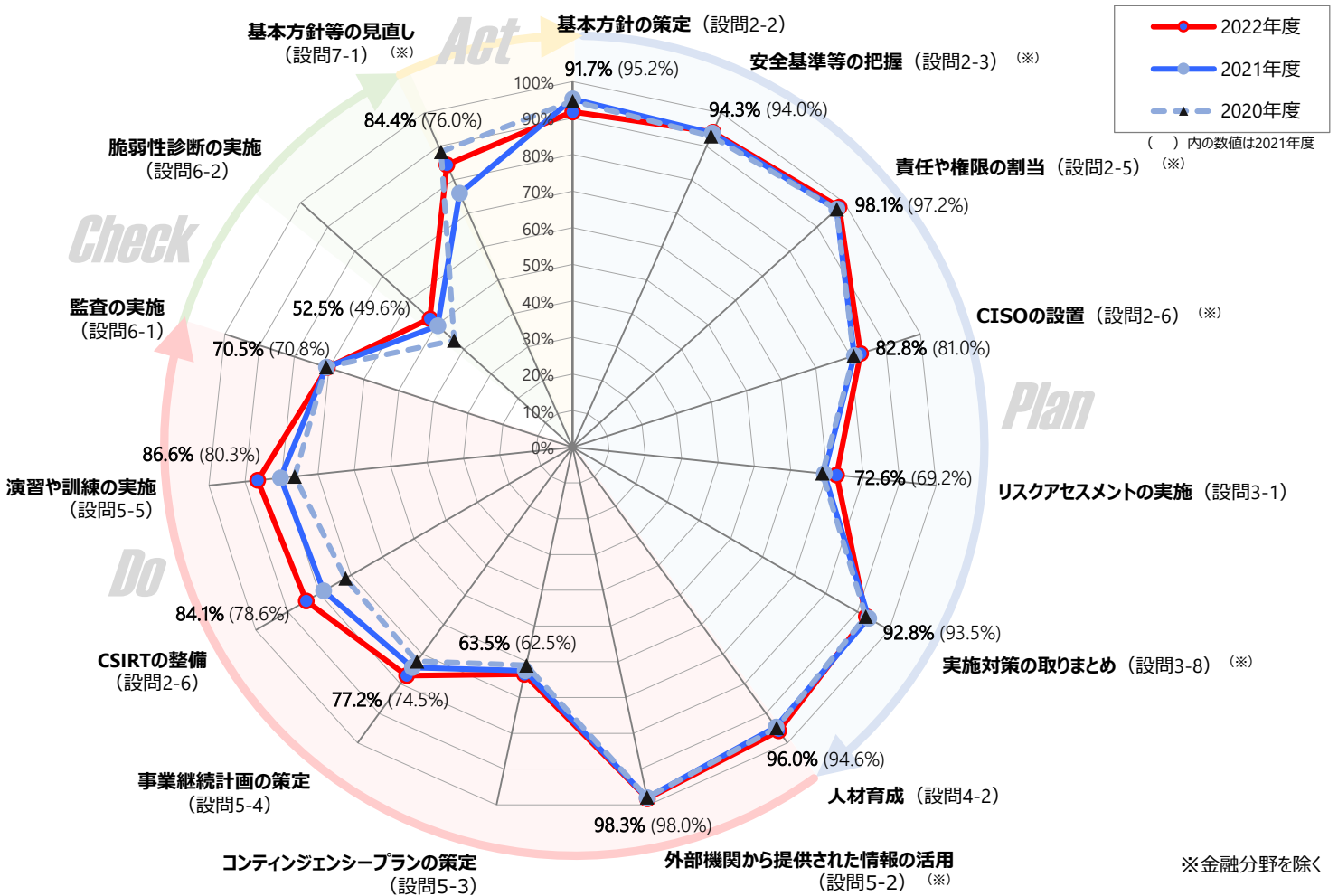
- 2022年度は、**重要インフラ分野（計14分野）の事業者等を対象に調査を実施し、1,910事業者から回答**（回答率50.5%）を得た。

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	20	NISC調査
	放送	主要な地上基幹放送事業者	103	
	ケーブルテレビ	主要なケーブルテレビ事業者	67	
金融※		銀行等、生命保険、損害保険、証券会社	652	外部調査※
航空		主たる定期航空運送事業者	4	NISC調査
空港		主要な空港・空港ビル事業者	7	
鉄道		ＪＲ各社及び大手民間鉄道事業者の主要な鉄道事業者	22	
電力		一般送配電事業者、主要な発電事業者	13	
ガス		主要なガス事業者	12	
政府・行政サービス		都道府県及び市区町村	859	
医療		医療情報システムを導入している医療機関等の中からランダムで選定した事業者	17	
水道		現在給水人口30万人以上の水道事業者及び水道用水供給事業者	91	
物流		大手物流事業者	9	
化学		主要な石油化学事業者	6	
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	22	
石油		主要な石油精製・元売事業者	6	
全分野合計		－－－	**1,910 (1,258)**※	

※1　金融分野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、金融分野を除いた合計数。

調査結果概要（総評）

- **<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、**<u>安全基準等は浸透しつつある</u>**と一定の評価ができる。
- 「事業継続計画の策定」「CSIRTの整備」「演習や訓練の実施」といった**<u>Do（実行）に係る項目の実施状況について改善</u>**が見られ、重要インフラサービス障害の発生に備えた対処体制の整備は着実に進展している。
- **<u>他方、「リスクアセスメントの実施」「コンティンジェンシープランの策定」や、Check（評価）に係る項目である「監査の実施」「脆弱性診断の実施」の実施状況は相対的に低い</u>**ことから、これらを改善していくことが今後の課題である。
  - リスクアセスメントや監査・セキュリティ評価については、組織統治の一部として実施されるよう促進していくことが重要と考えられる。
  - コンティンジェンシープランを策定していない理由として、事業継続計画をコンティンジェンシープランの代替としている場合がある。こうした事業者においては、障害発生等への初動対応に関する方針、手順、態勢等が十分かの視点から計画を確認することが重要と考えられる。

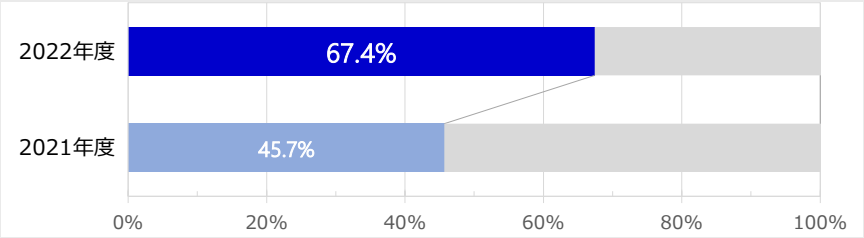


※金融分野を除く

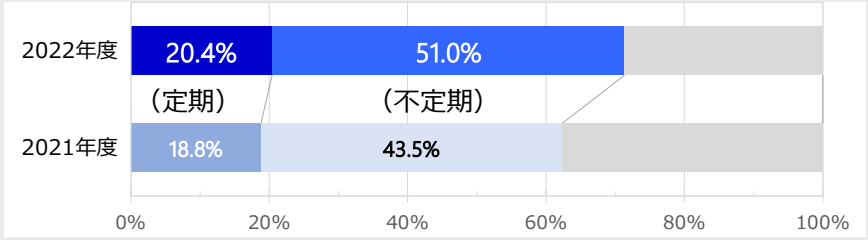
- **「セキュリティ方針の策定への経営層の関与」及び「経営層との対話の機会」について実施状況が改善**した。他方、情報開示の基準を策定している組織は比較的少数で推移している。**サイバーセキュリティを組織統治の一部として組み入れるよう促進**することが必要と考えられる。
- セキュリティに関する予算・人材の配分について適切と感じている割合は3割以下で推移しており、**予算・人材不足が課題**と考えられる。**リスクアセスメントを踏まえた適切な予算・人材の配分の促進や、分野ごとの特性に応じた予算・人材確保に関する対応の検討**が必要と考えられる。

► **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2-1）

※金融分野を除く

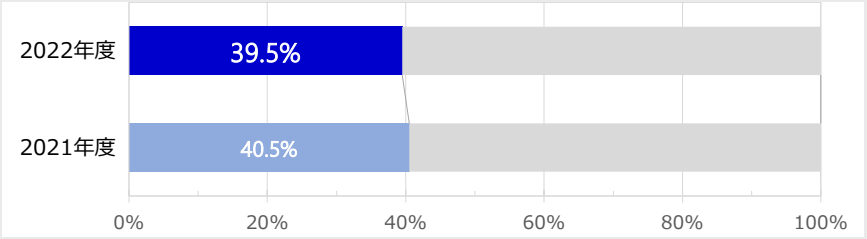


► **経営層とレポーティング・対話の場が設けられている**（設問2-7）※金融分野を除く



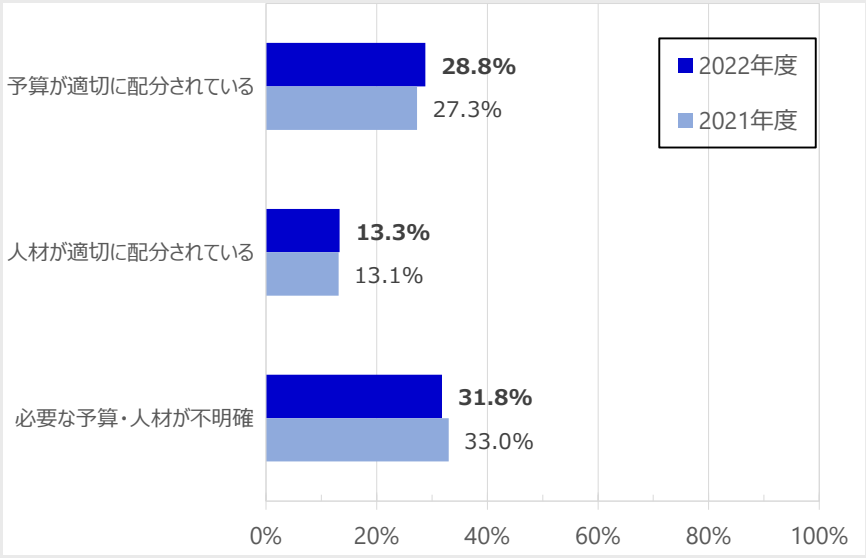
► **サイバーセキュリティに関する事件・事故が発生した場合の情報開示の基準を策定している**（設問3-11）

※金融分野を除く



► **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4-1）

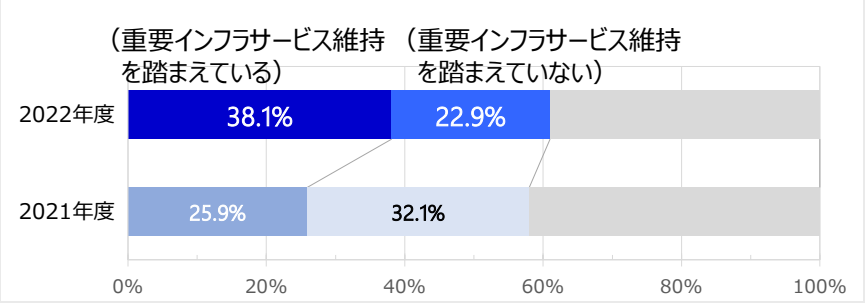
※金融分野を除く



浸透状況と課題 － リスクアセスメント、サプライチェーン

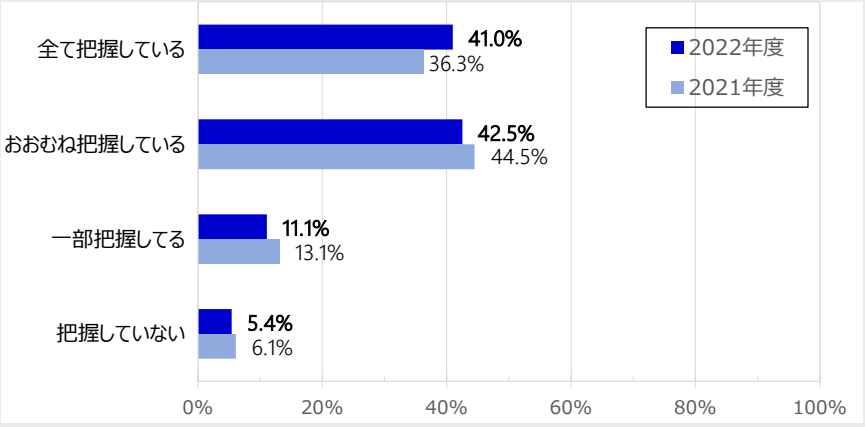
- **重要インフラサービス維持を目的としたリスクアセスメントの実施状況は改善**した。任務保証の考え方の浸透など、**引き続きの改善に向けた取組が必要**である。
- 「自組織のサプライチェーンを全て把握している」又は「おおむね把握している」状況が高い水準で推移しており、自組織のサプライチェーンの把握について着実に意識付けされている。他方、サプライチェーンに関する「責任分界点の明確化」、「インシデント発生時の報告」といった対策の実施状況は５割以下で推移しており、**必要な対策が網羅的に実施されるよう促進することが必要**である。

► リスクアセスメントを実施している（設問3-1） ※金融分野を除く

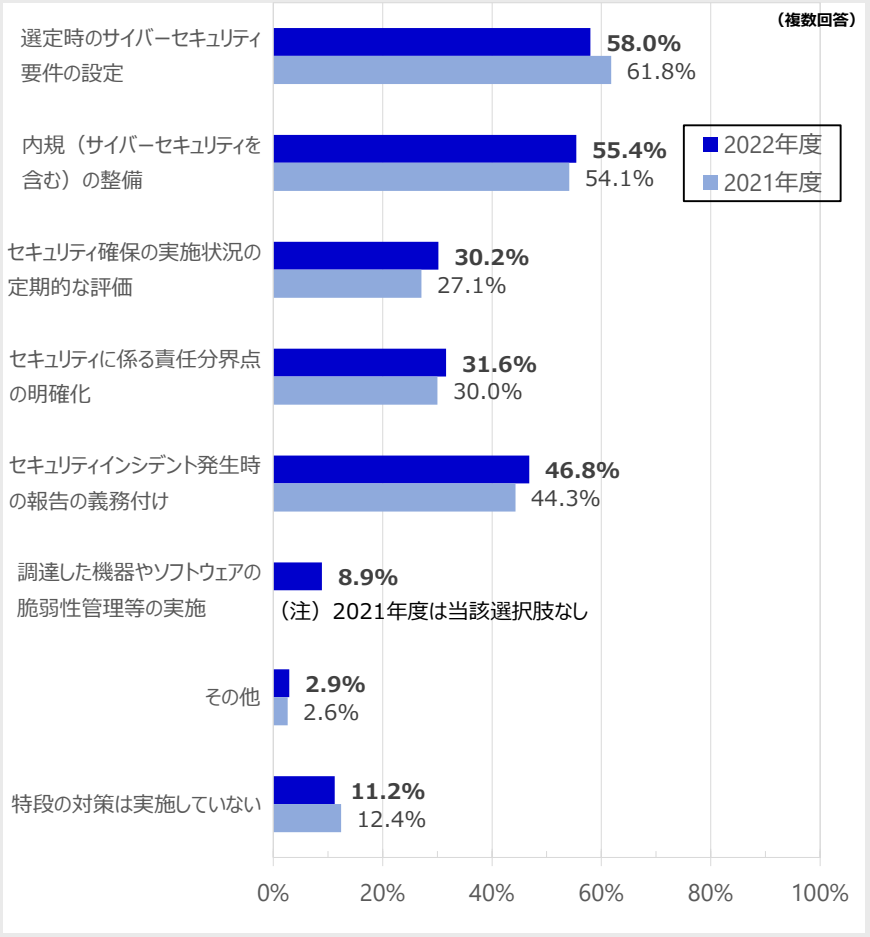


（注）2021年度の設問は「機能保証の考え方を取り入れたリスクアセスメントを実施している」

► 自組織のサプライチェーンを把握している（設問1-3） ※金融分野を除く



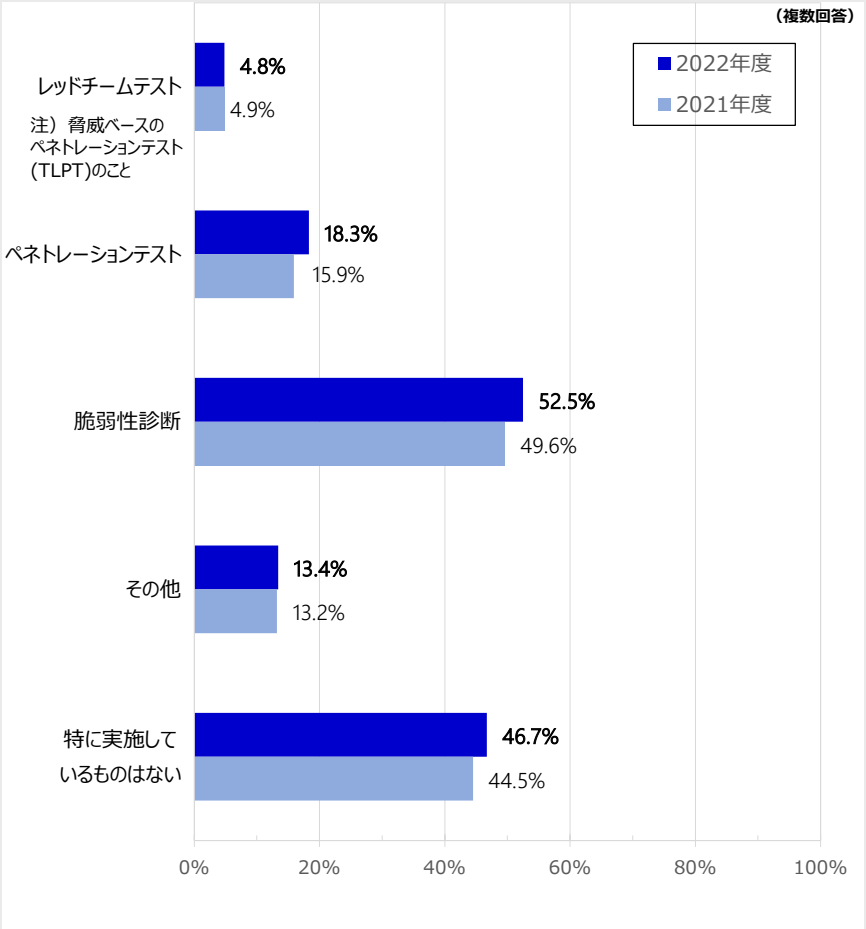
► サプライチェーン・リスク対策の実施状況（設問1-5） ※金融分野を除く



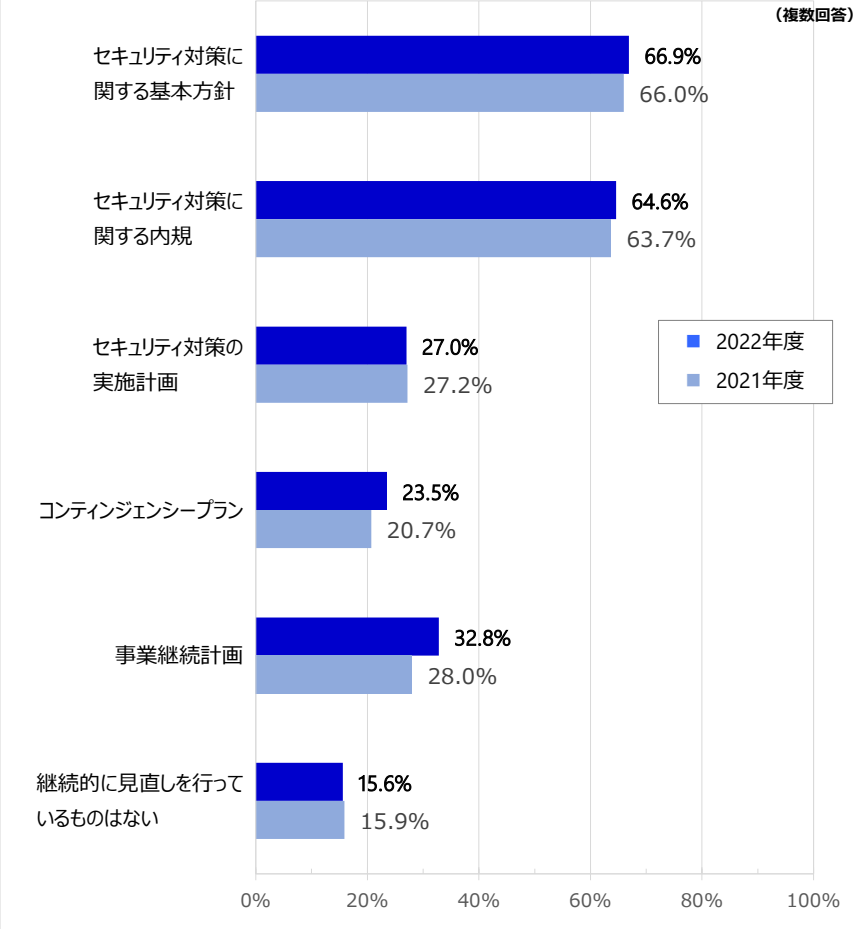
浸透状況と課題　－　評価、改善

- **ペネトレーションテスト、脆弱性診断等のセキュリティ評価に関する実施状況は改善**傾向にあり、更なる改善に取り組む必要がある。
- 「セキュリティ対策の実施計画」を見直したとの回答は３割程度。**サイバー攻撃に関する新たな脅威の発生等の環境変化に応じてセキュリティ対策が素早く見直されるよう促進することが必要**である。

► セキュリティ評価の実施状況（設問6-2）



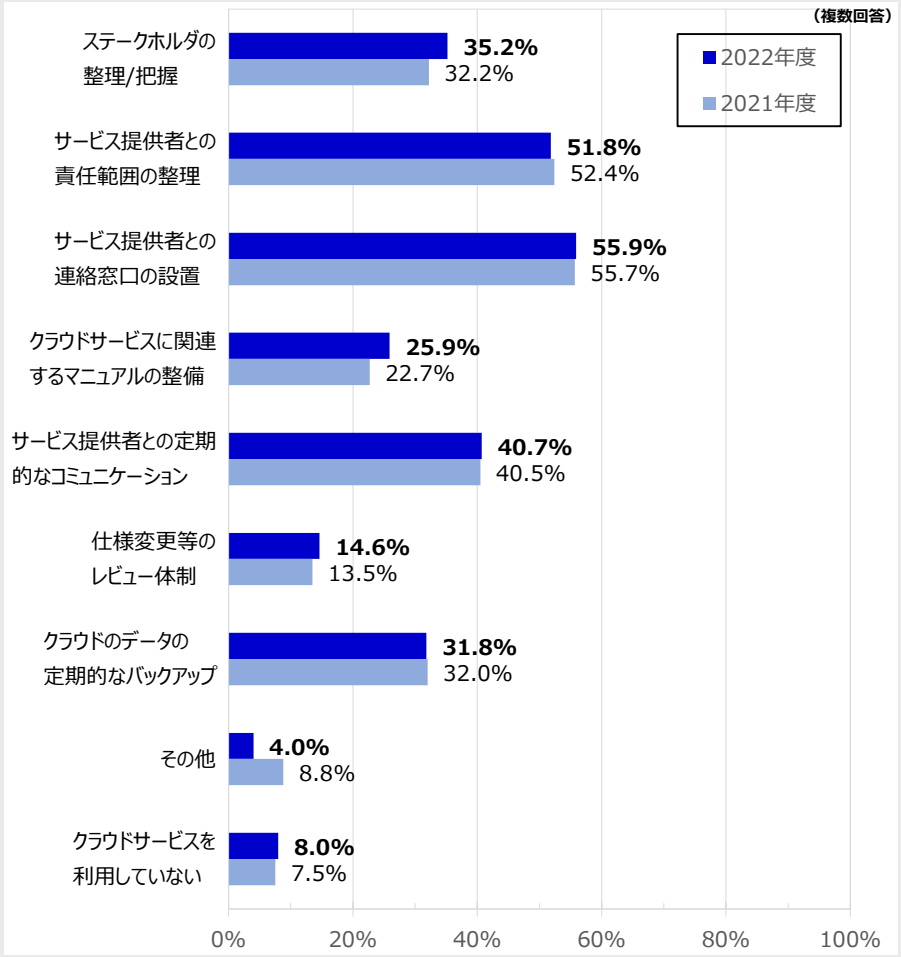
► 見直しの実施状況（設問7-1）※金融分野を除く



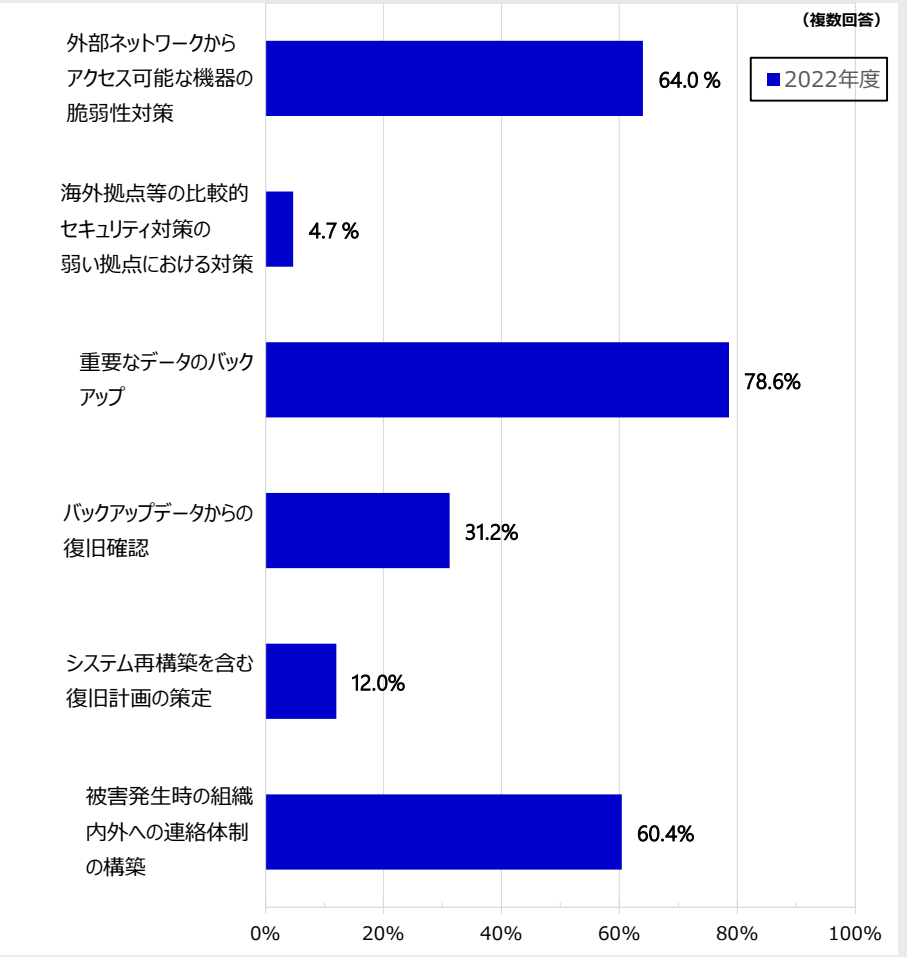
浸透状況と課題 － クラウドサービスの利用、ランサムウェア対策

- クラウドサービスを利用していないとの回答は１割以下であり、クラウドサービスは重要インフラに浸透している。対策の実施状況は2021年度から大きな変化はなく、**「クラウドを利用したシステム運用に関するガイダンス(NISC,2022年4月)」等の広報活動等により、対策を促進する必要**がある。
- ランサムウェア対策として、バックアップの実施のみならず、**バックアップデータからの復旧確認、復旧計画の策定について課題**。また、今後、**バックアップデータを物理的・論理的にシステムから切り離して保存**しているのか確認するとともに、適切なバックアップ方法を推進する必要がある。

► クラウドサービスの利用に係る対策の実施状況（設問8-2） ※金融分野を除く



► ランサムウェア対策の実施状況（抜粋） （設問10-3） ※金融分野を除く



（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。**

安全基準等に関する体系を図 2に示す。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。

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
（2022年度）

調査票の構成（設問一覧）

□ Plan［計画］

- **組織の状況の観点**
  設問1-1. 外部環境・内部環境の整理
  設問1-2. 関係主体からの要求事項の整理
  設問1-3. サプライチェーンの把握
  設問1-4. 自組織で認識しているサプライチェーンリスク
  設問1-5. 実施しているサプライチェーンリスク軽減策

- **リーダーシップの観点**
  設問2-1. サイバーセキュリティリスクに対する認識
  設問2-2. 基本方針の策定・公表
  設問2-3. 安全基準等の把握
  設問2-4. 基本方針策定に当たり参考としている基準等
  設問2-5. サイバーセキュリティ担当に対する責任及び権限の割当
  設問2-6. 自組織で設置しているサイバーセキュリティに係る役職等
  設問2-7. 経営層とのレポーティング・対話の機会

- **計画の観点**
  設問3-1. リスクアセスメントの実施
  設問3-2. リスクアセスメントの実施主体
  設問3-3. 実施しているリスクセスメントの方法
  設問3-4. リスクアセスメントの実施周期
  設問3-5. 重要システムの特定
  設問3-6. サイバーセキュリティの確保に当たり参考としている基準等
  設問3-7. 実施しているサイバーセキュリティ確保の取組
  設問3-8. セキュリティ確保の取組の内規としての取りまとめ
  設問3-9. 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
  設問3-10. リスク対応計画未策定の理由
  設問3-11. 事件・事故が発生した場合の情報開示基準の策定

- **支援の観点**
  設問4-1. 人材・予算の配分状況
  設問4-2. セキュリティ人材育成や意識啓発に関する取組
  設問4-3. 情報処理安全確保支援士の活用
  設問4-4. 情報共有や意見交換を行っている関係主体
  設問4-5. システム不具合時の情報共有範囲

□ Do［実行］

- **運用の観点**
  設問5-1. 導入・運用時におけるサイバーセキュリティ確保の取組
  設問5-2. 自組織で活用している情報の提供元
  設問5-3. コンティンジェンシープランの策定
  設問5-4. 事業継続計画・事業復旧計画の策定
  設問5-5. 実施・参加している演習・訓練

□ Check［評価］

- **評価の観点**
  設問6-1. サイバーセキュリティ確保の取組に関する監査の実施
  設問6-2. 実施しているセキュリティ評価

□ Act［改善］

- **改善の観点**
  設問7-1. サイバーセキュリティ確保の取組の改善に向けた継続的な見直し
  設問7-2. サイバーセキュリティ対策の見直しの契機

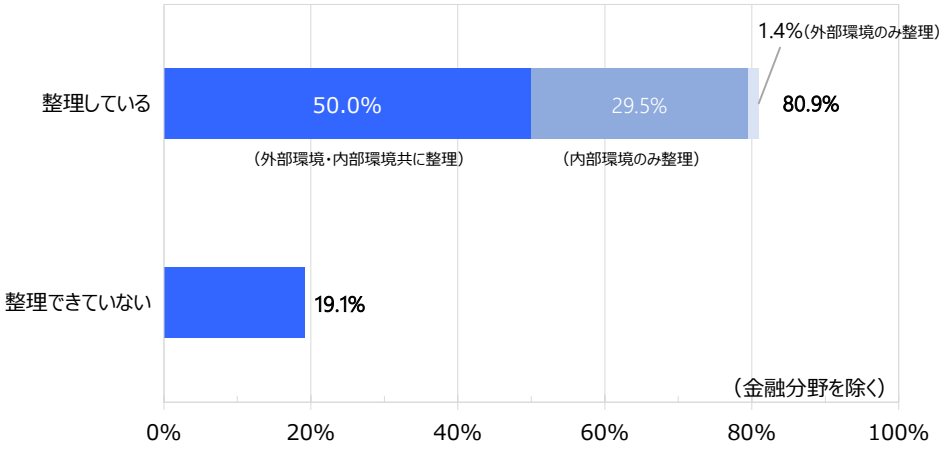
□ その他

- **クラウドサービスの利用について**
  設問8-1. クラウドサービス提供事業者への確認事項
  設問8-2. クラウドサービス利用時に自組織で行っている運用対策

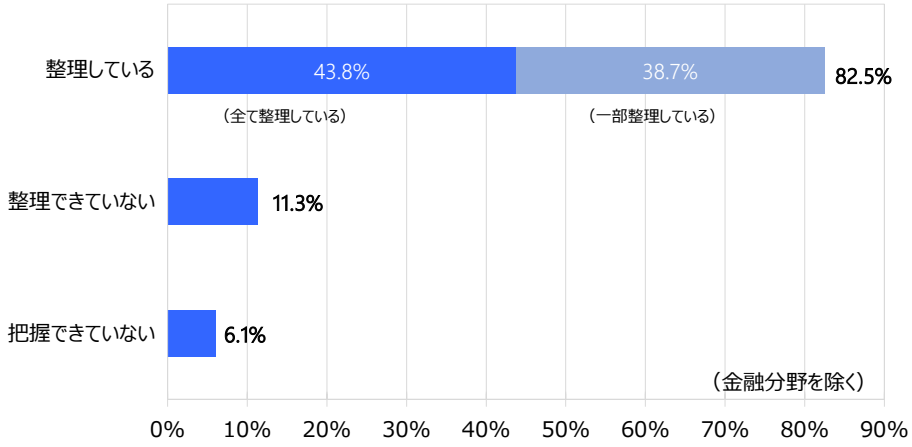
- **テレワークを活用した働き方について**
  設問9. テレワークで実施しているセキュリティ確保の取組

- **昨今のインシデント等を受けて**
  設問10-1. 制御システムのセキュリティ確保における参考文献等
  設問10-2. サイバー保険の加入有無
  設問10-3. ランサムウェア攻撃への対策、運用体制

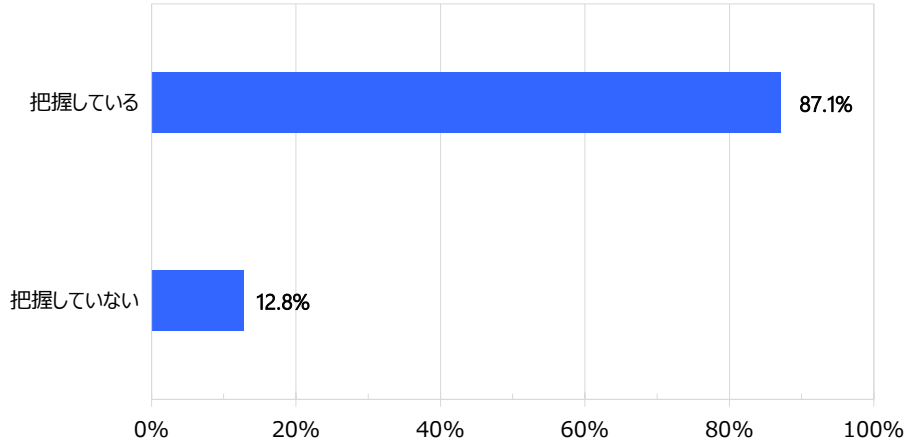
設問１－１．【単一回答】
自組織の重要インフラサービスの安定的かつ継続的な提供に影響を与えるおそれがある外部環境や内部環境について、近い将来の状況を含めて整理していますか。

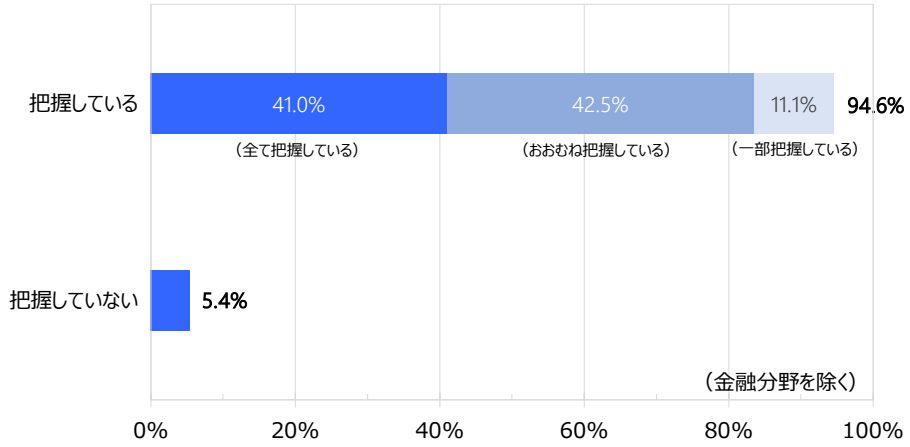


設問１－２．【単一回答】
関係省庁、顧客、サプライヤー、委託先等からの、サイバーセキュリティに関する自組織への要求事項を整理していますか。



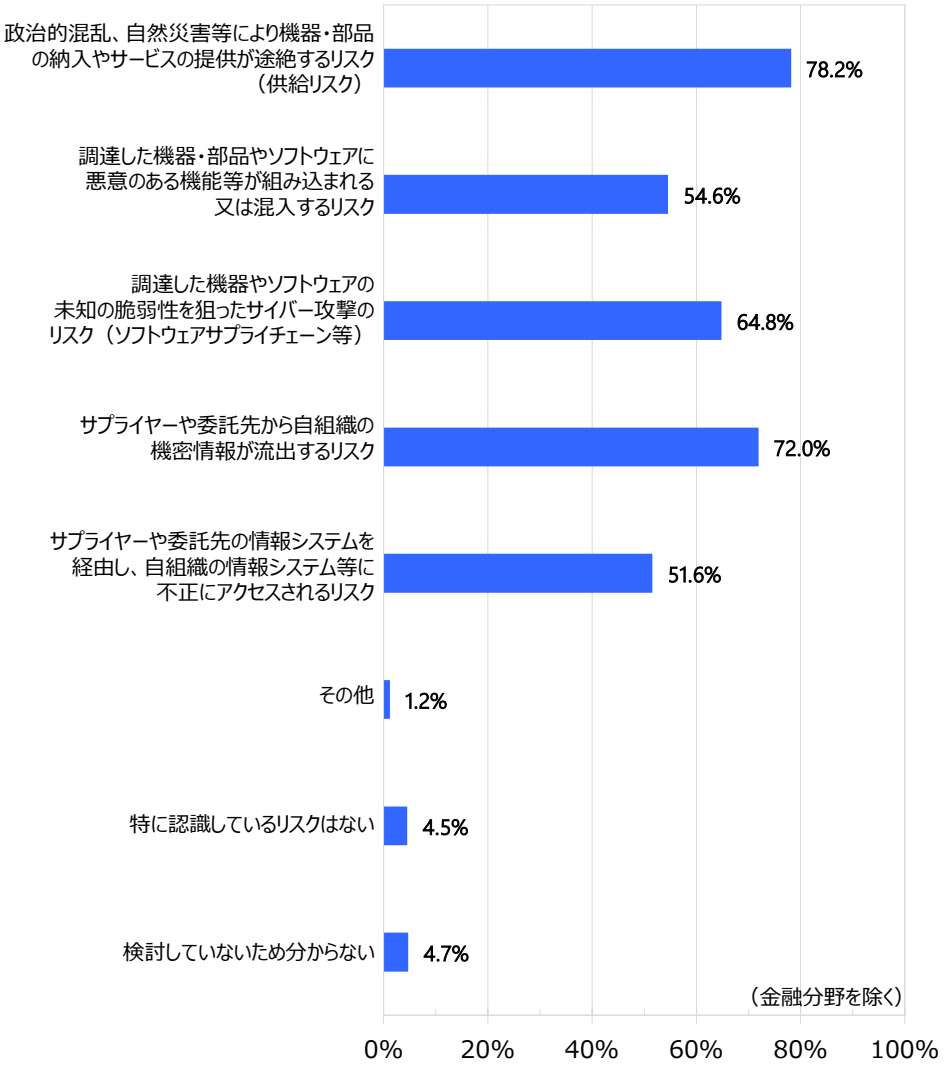
設問１－３．【単一回答】
自組織のサプライチェーン（サプライヤー、委託先等）を把握していますか。
（上段：対象の全分野　下段：金融分野を除いた内訳）



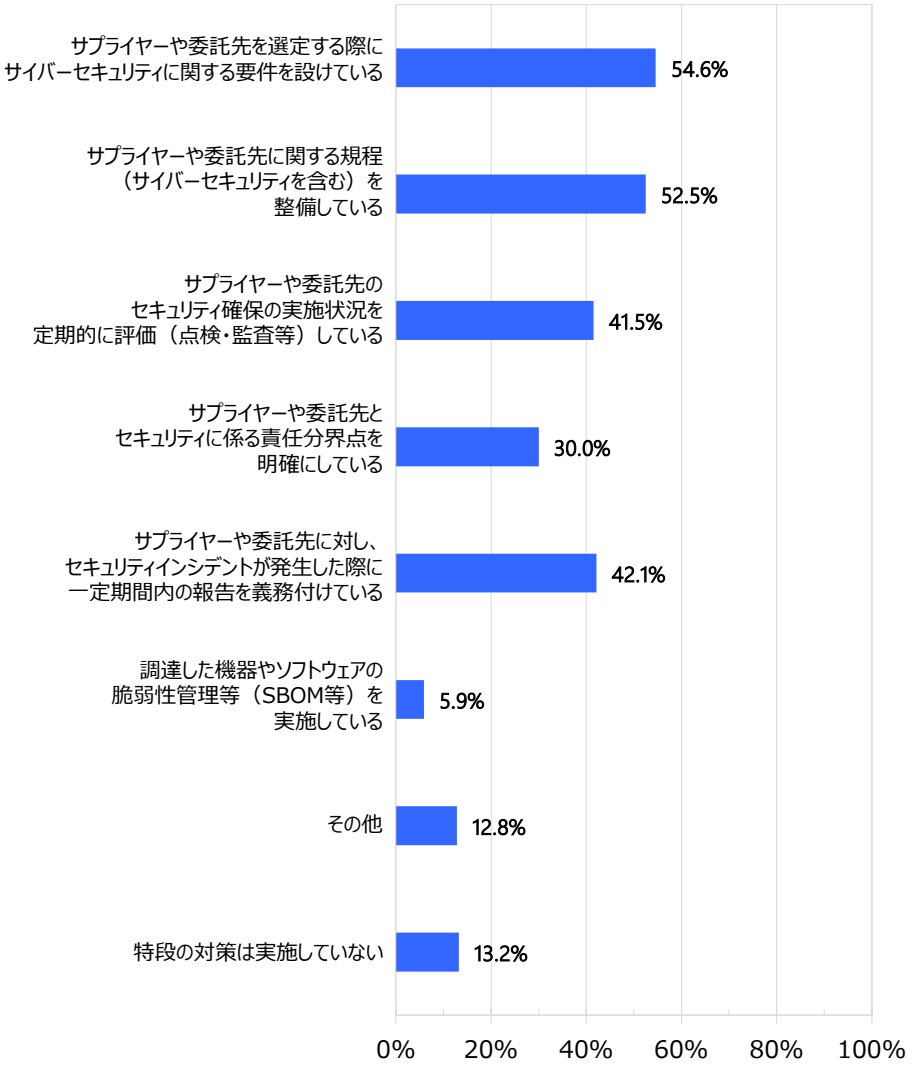


●数値は小数点以下第2位を四捨五入しています。

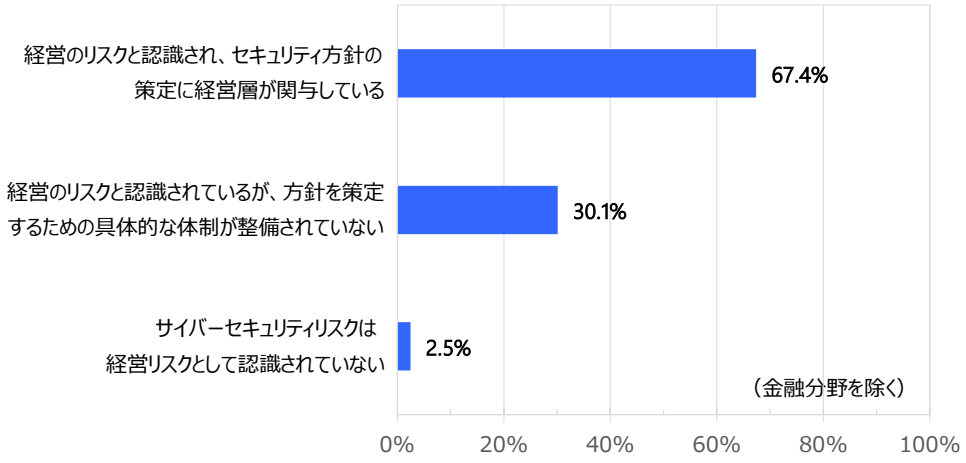
設問１－４．【複数回答】
サプライチェーンについて、自組織で認識しているリスクを全て選択してください。



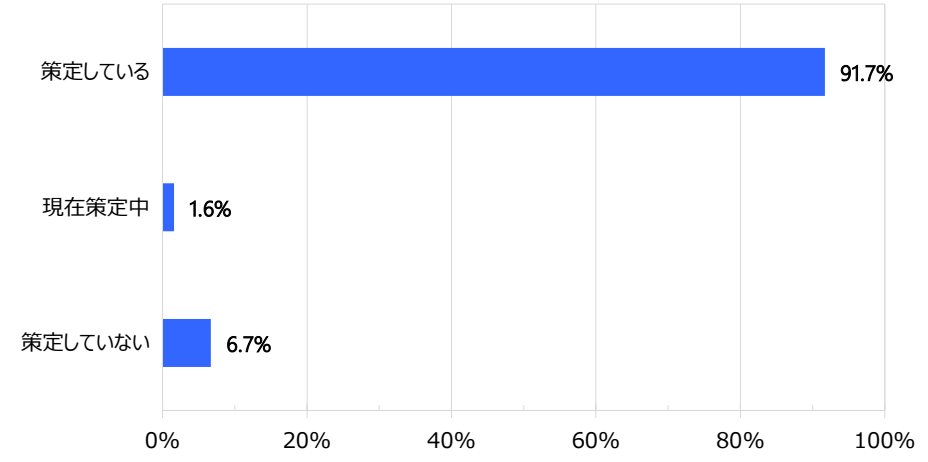
設問１－５．【複数回答】
自組織のサプライチェーンに関するリスクについて、実施しているリスク軽減策を全て選択してください。

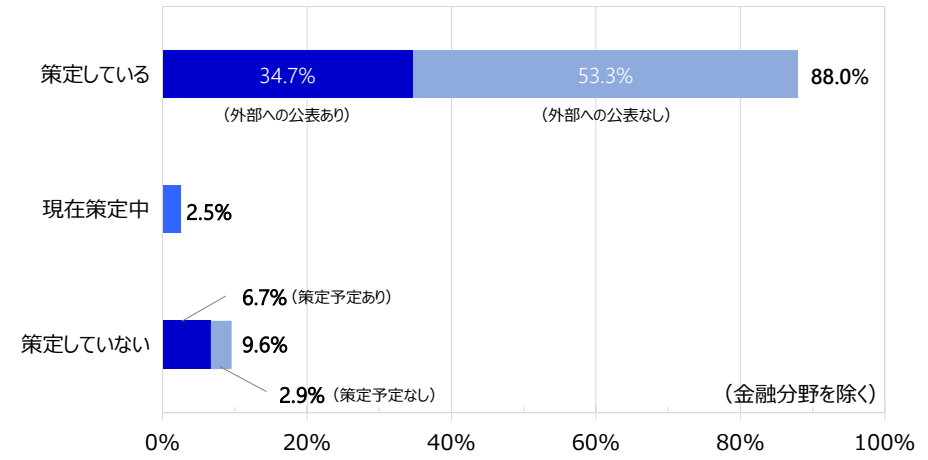


設問２－1.【単一回答】
サイバーセキュリティリスクが経営リスクと認識されていますか。

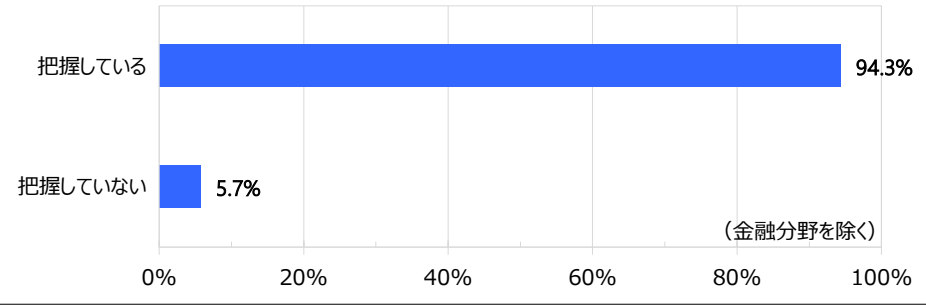


設問２－2.【単一回答】
自組織がサイバーセキュリティ確保に取り組む目的、方向性等を示したサイバーセキュリティに関する基本方針を策定・公表していますか。
（上段：対象の全分野　下段：金融分野を除いた内訳）

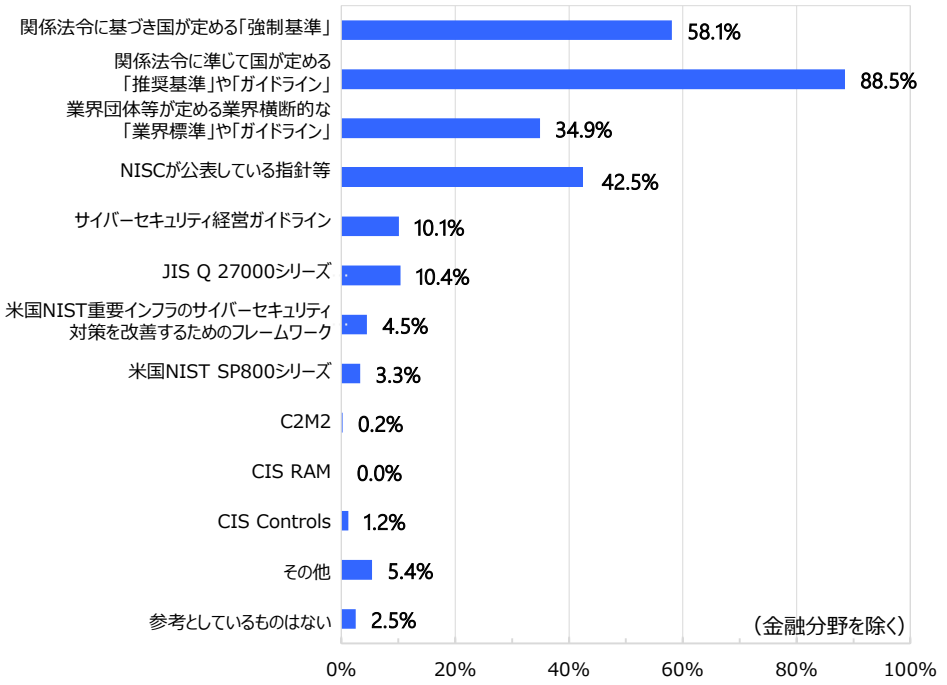




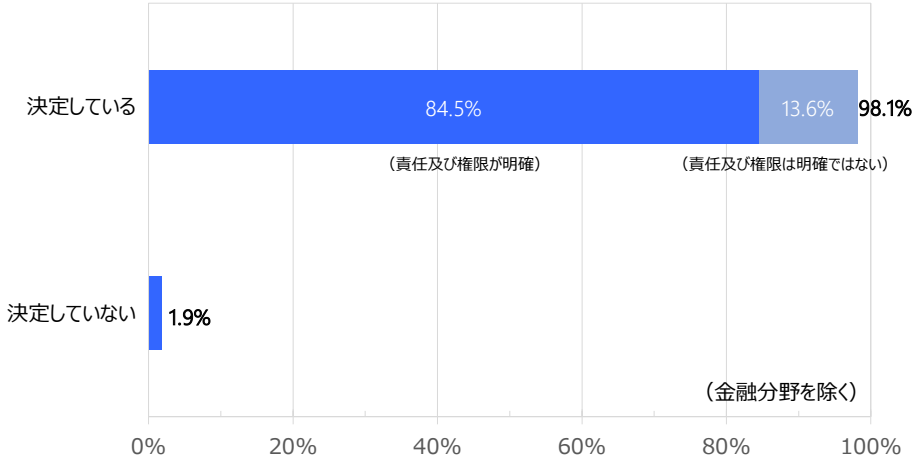
設問２－３．【単一回答】
自組織に関係する安全基準等を把握していますか。



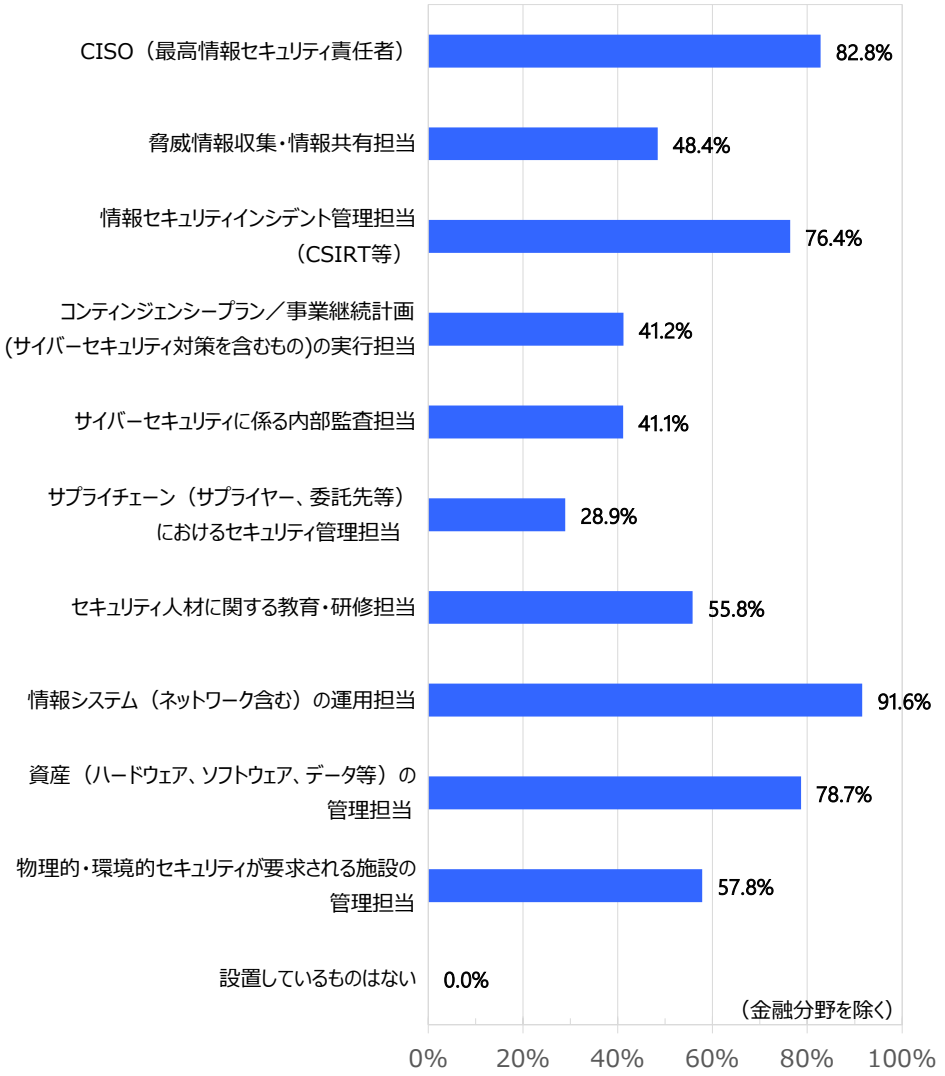
設問２－４．【複数回答】
サイバーセキュリティに関する方針の策定に当たって参考としているものを全て選択してください。



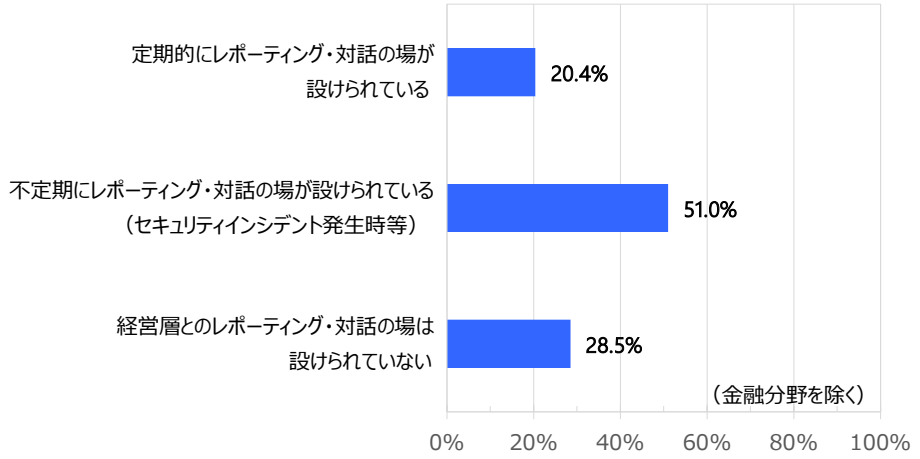
設問２－５．【単一回答】
自組織のサイバーセキュリティを担当する部署及び従業員を決定するとともに責任及び権限を割り当てていますか。



設問２－６．【複数回答】
自組織で設置しているものを全て選択ください。

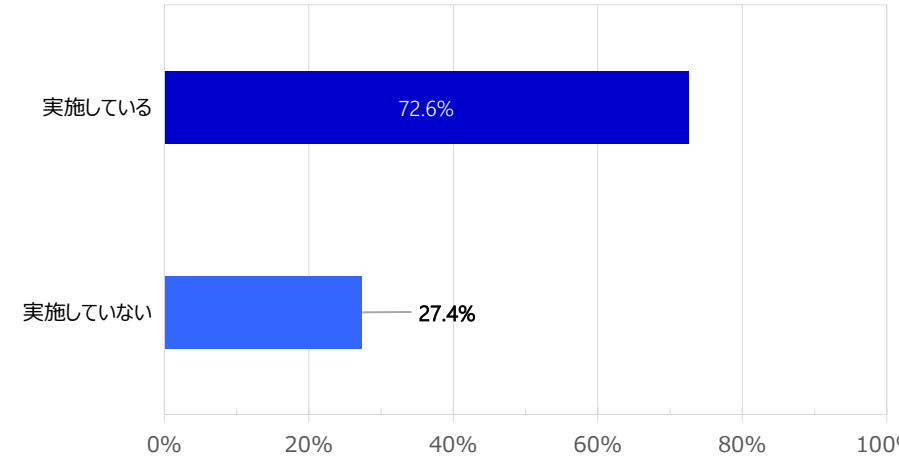


設問２－７．【単一回答】
サイバーセキュリティリスクの対処に当たり、経営層とのレポーティング・対話の場が設けられていますか。

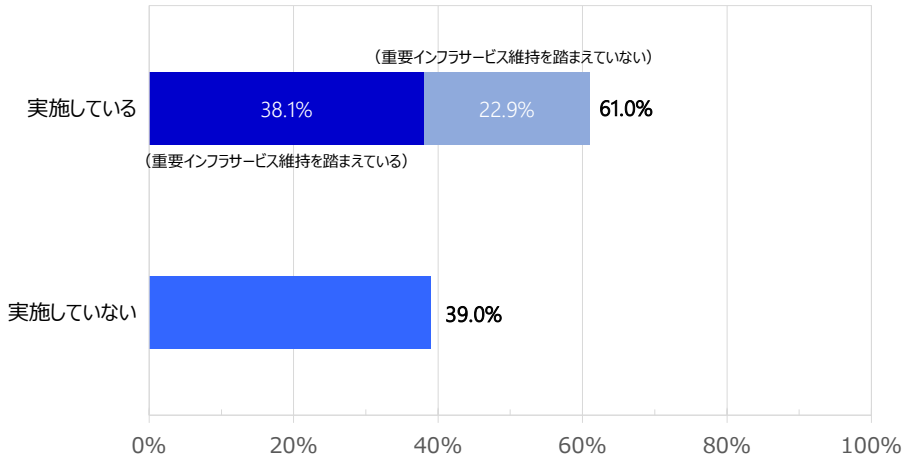


設問３－１．【単一回答】
サイバーセキュリティ確保の取組実施に当たり、情報の保護だけでなく、重要インフラサービス維持（事業継続）を目的としたリスクアセスメント（リスクの特定・分析・評価）を実施していますか。

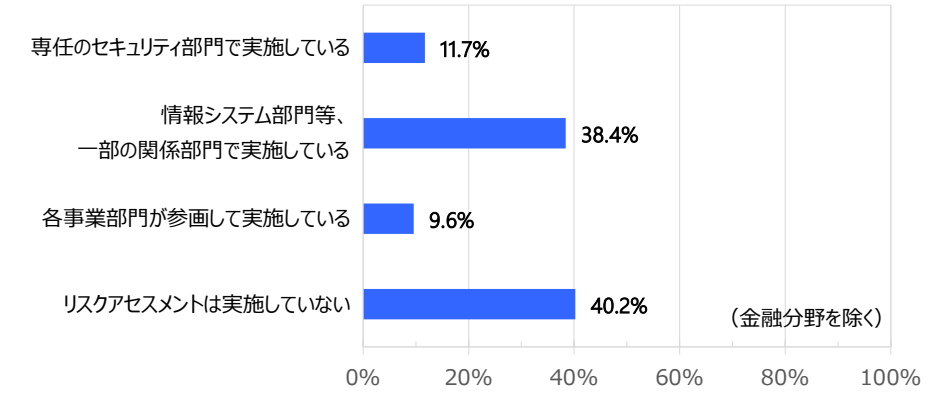
（金融を含む全分野）



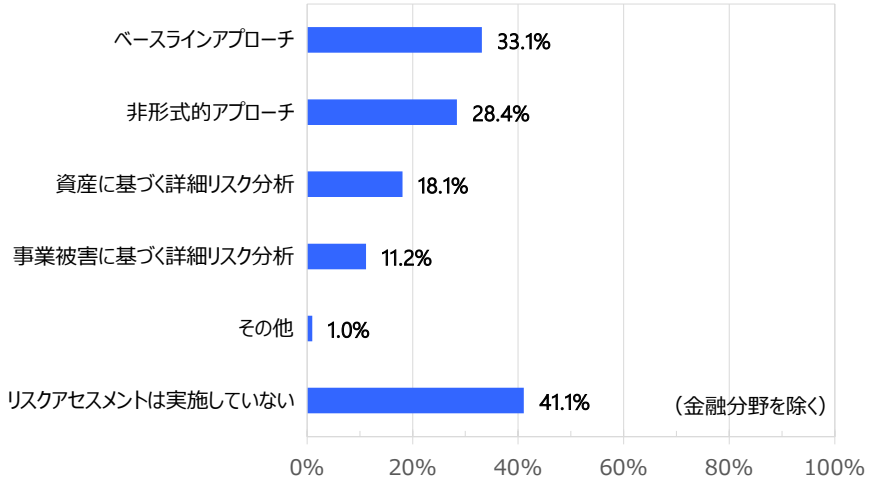
（金融分野を除いた場合）



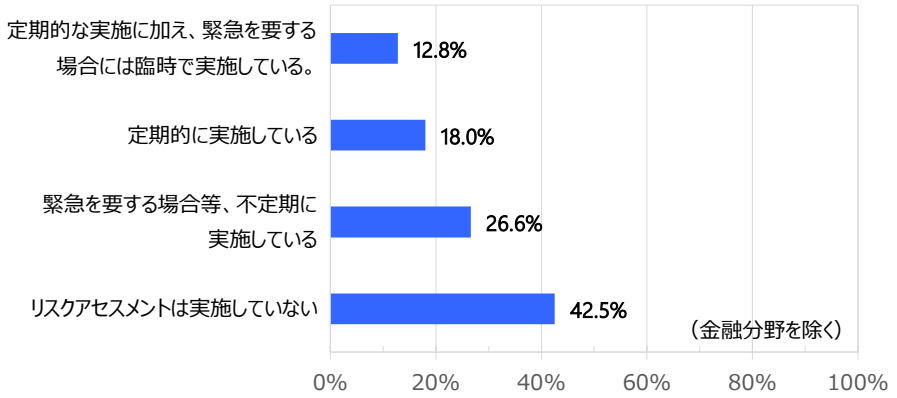
設問３－２．【単一回答】
サイバーセキュリティに関するリスクアセスメントの実施主体を選択してください。



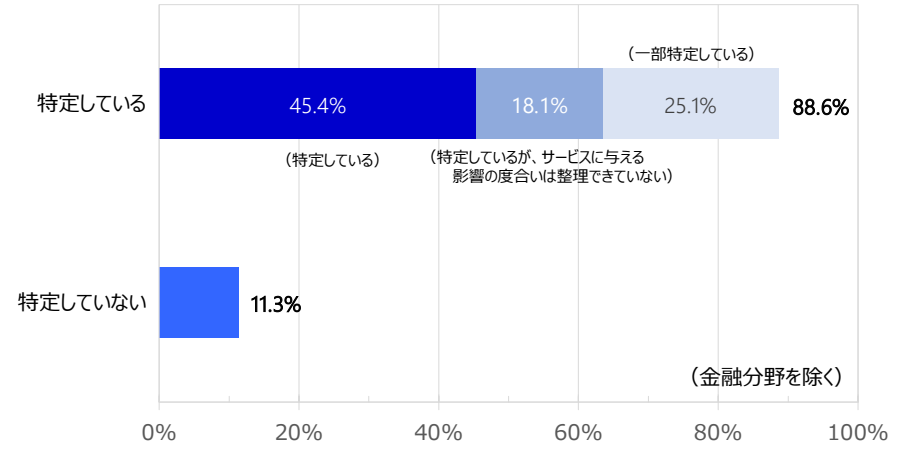
設問３－３．【複数回答】
自組織で実施しているリスクアセスメントの方法を全て選択してください。



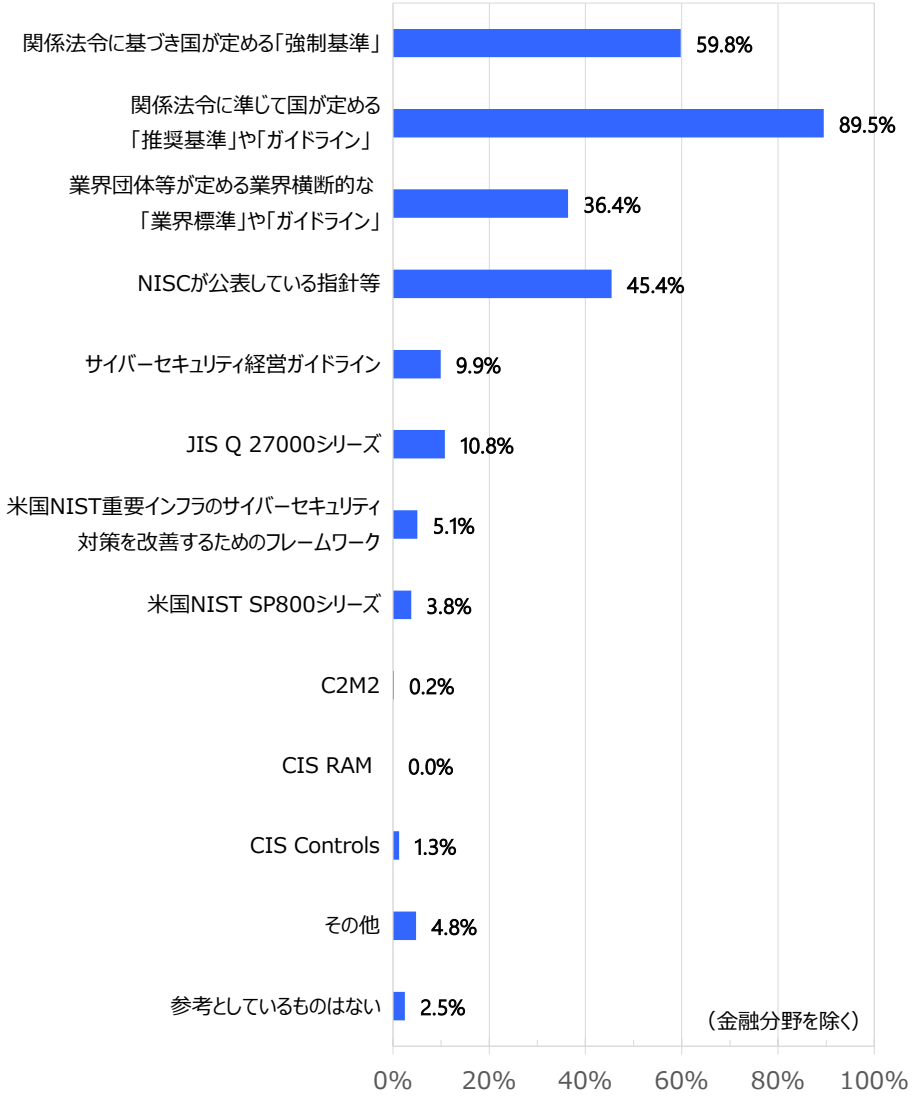
設問３－４．【単一回答】
サイバーセキュリティに関するリスクアセスメントを定期的に実施していますか。



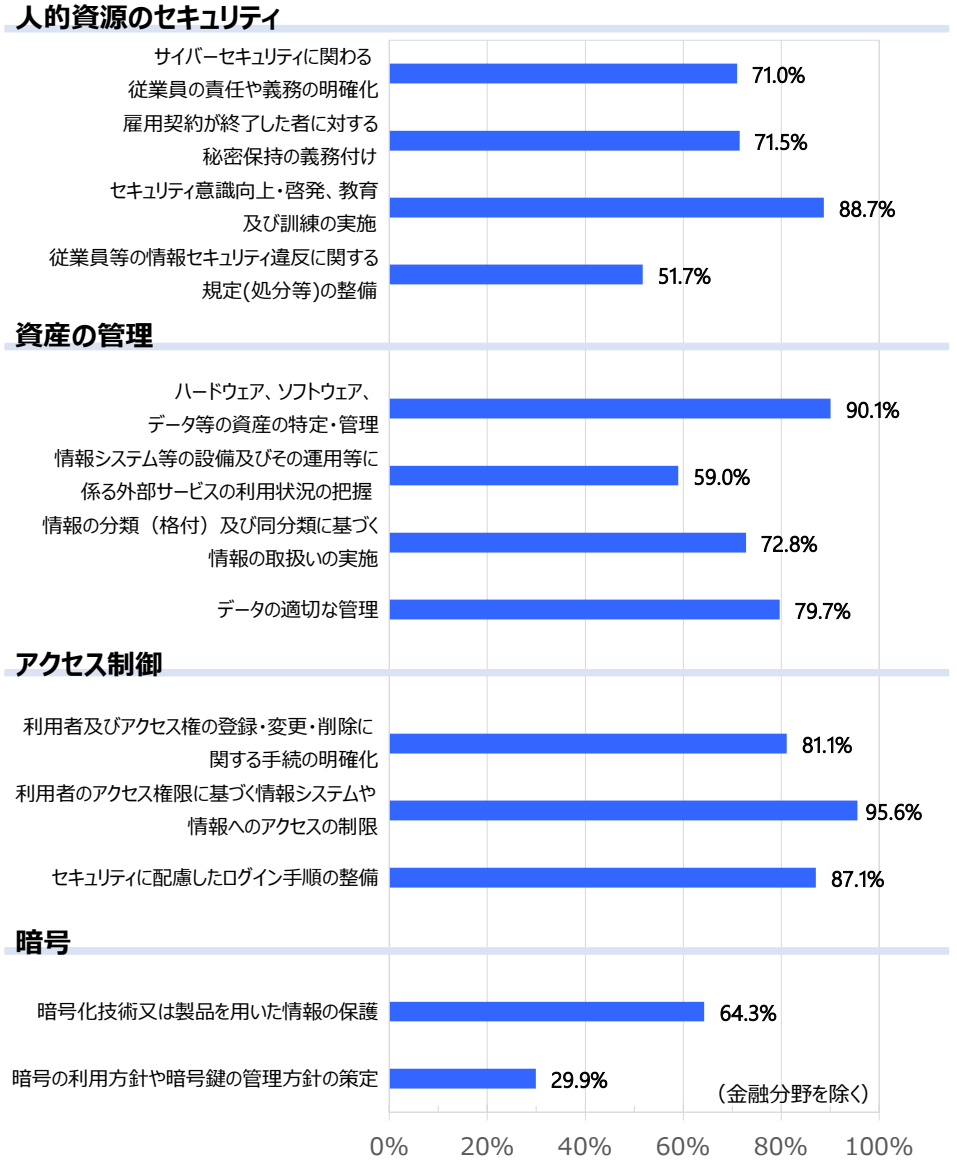
設問３－５．【単一回答】
重要システムを、重要インフラサービスに与える影響の度合いを踏まえて特定していますか。



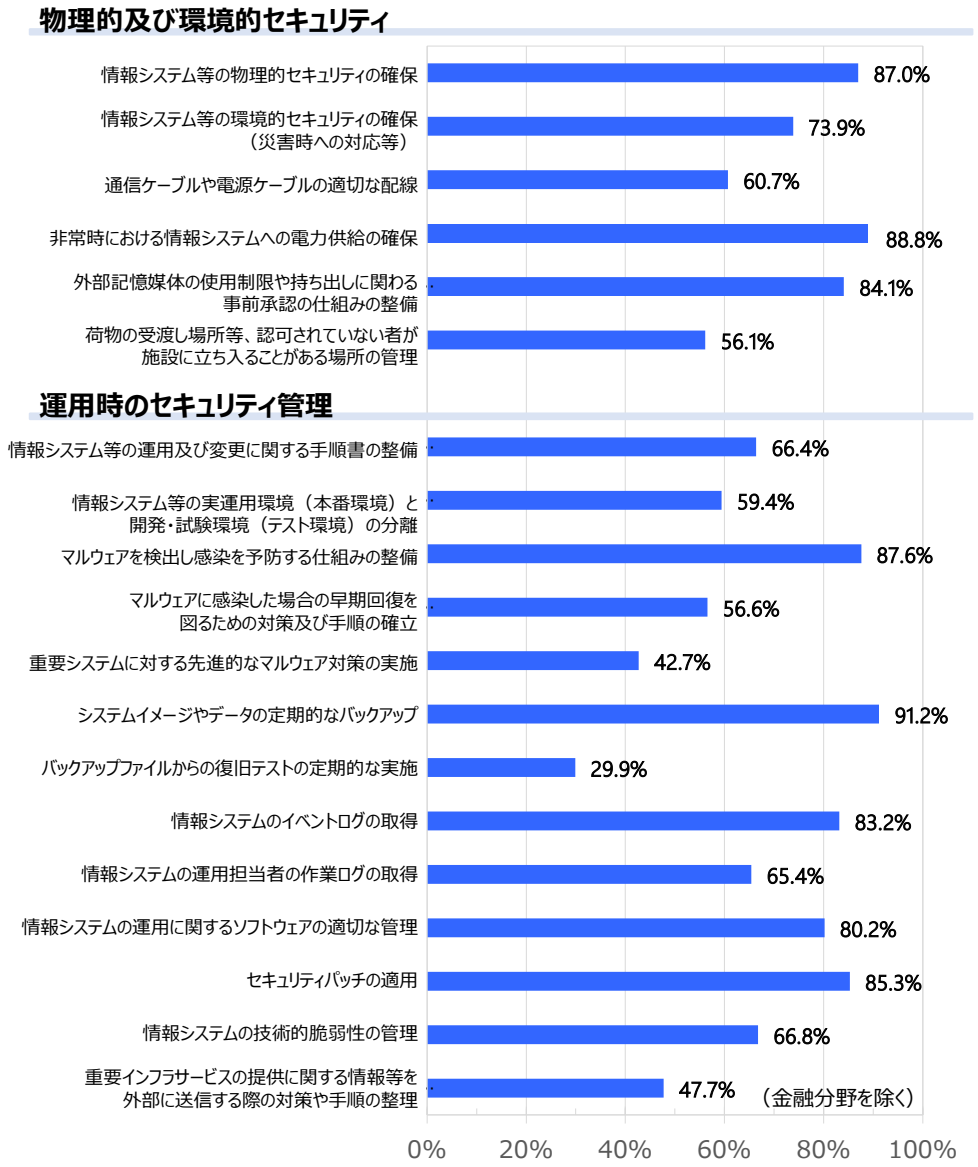
設問３－６．【複数回答】
サイバーセキュリティの確保に当たって、参考としているものを全て選択してください。

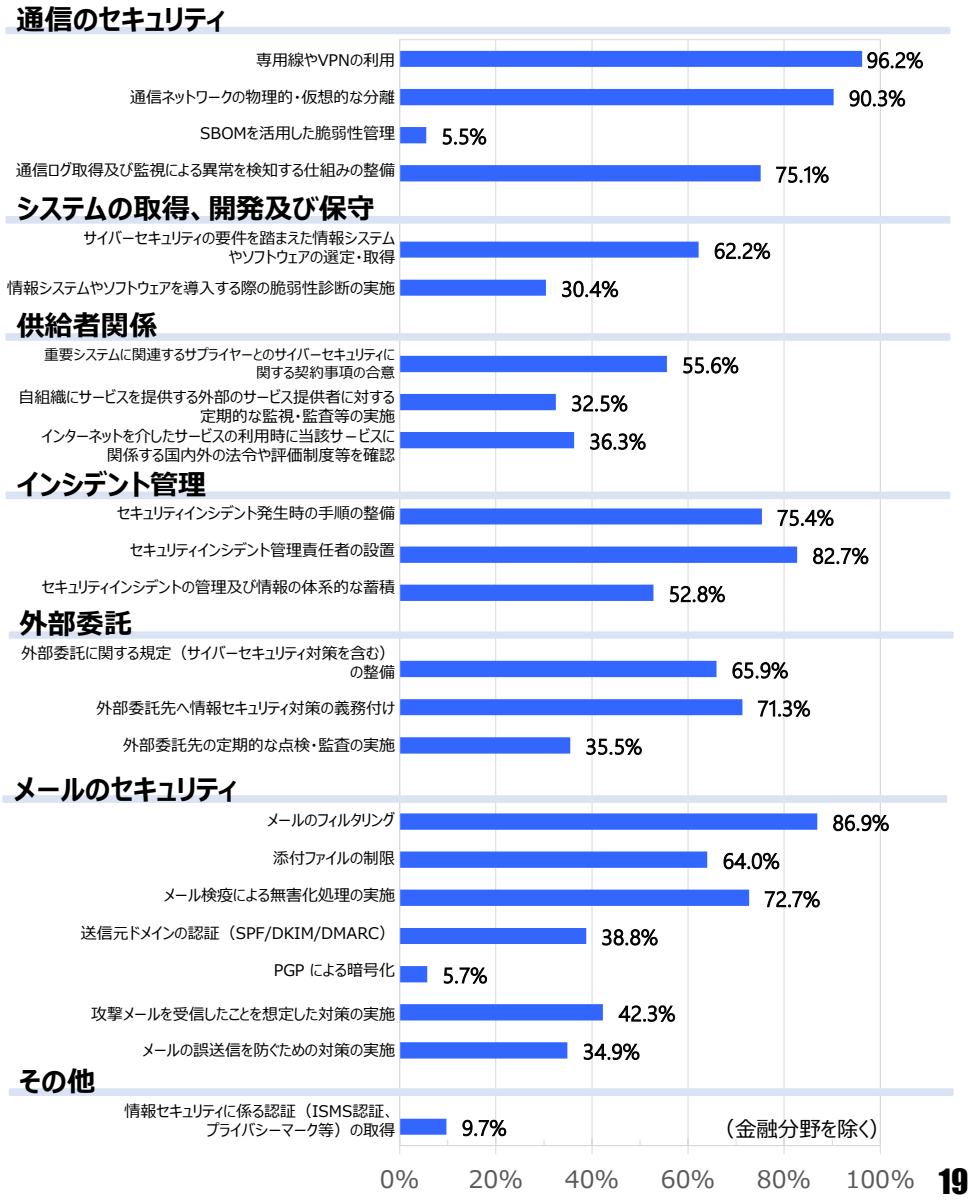


設問３－７．【複数回答】
自組織で実施しているサイバーセキュリティ確保の取組を全て選択してください。

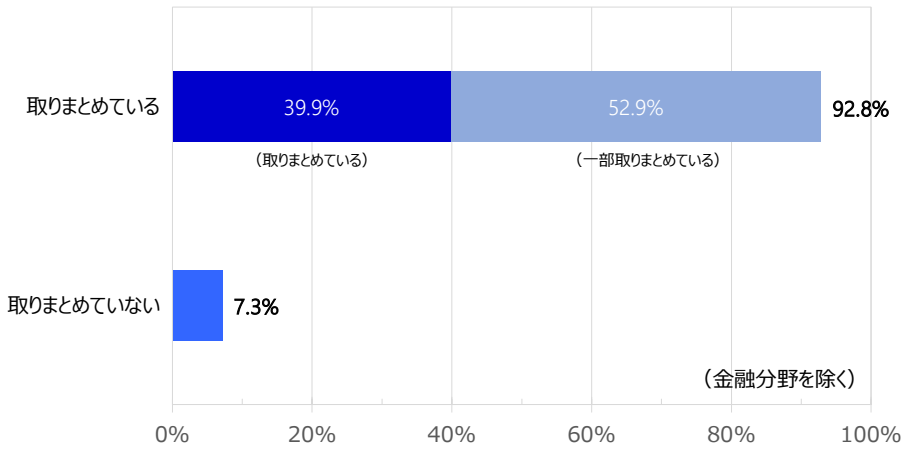


設問３－７．【複数回答】
自組織で実施している情報セキュリティ対策を全て選択してください。（続き）

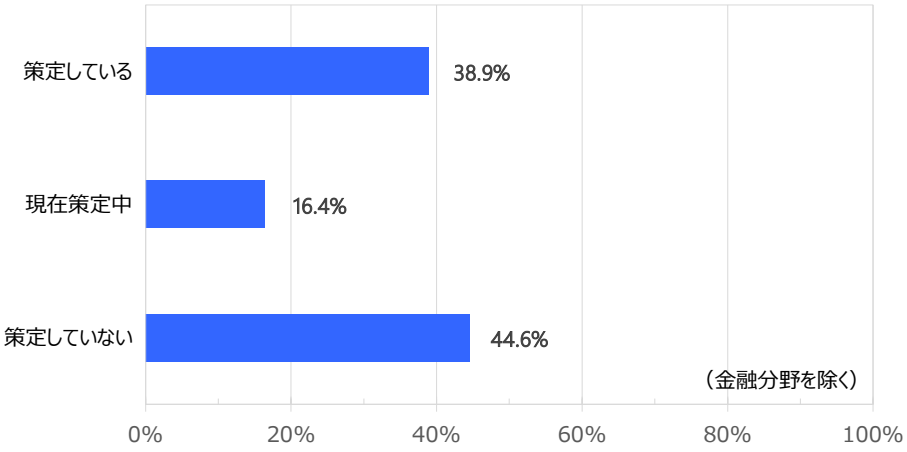




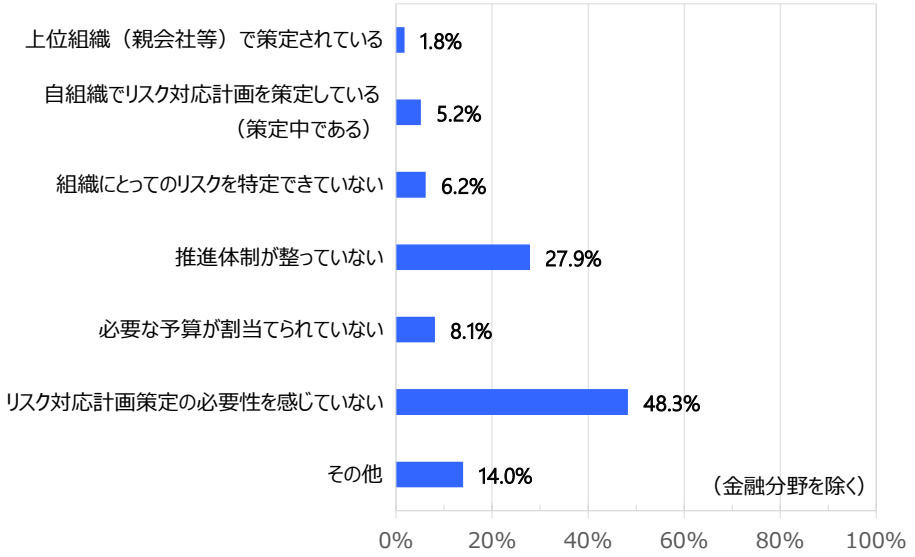
設問３－８．【単一回答】
設問３－７で実施しているとしたサイバーセキュリティ確保の取組を内規（実施手順・マニュアル等）として取りまとめていますか。



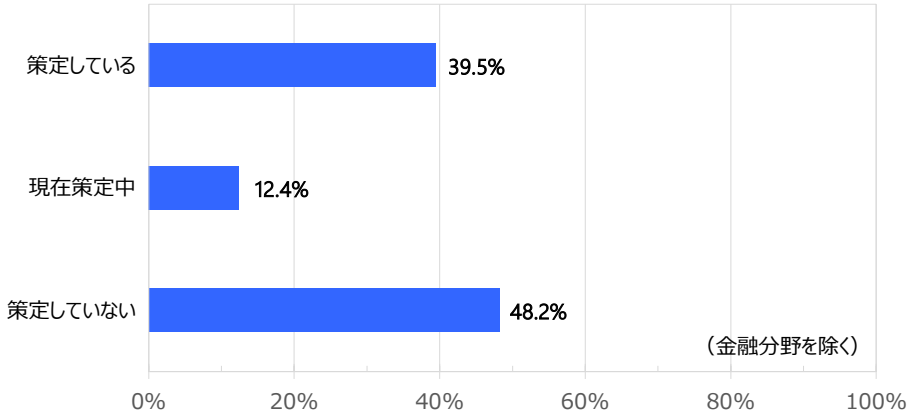
設問３－９．【単一回答】
サイバーセキュリティ確保の取組に向けたリスク対応計画（目標・達成度・スケジュール等）を策定していますか。



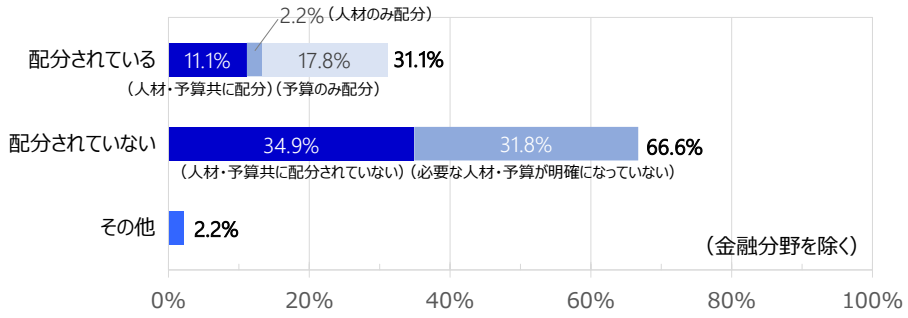
設問３－10．【複数回答】
設問3-9で「策定していない」を選択した場合には、その理由を選択してください。



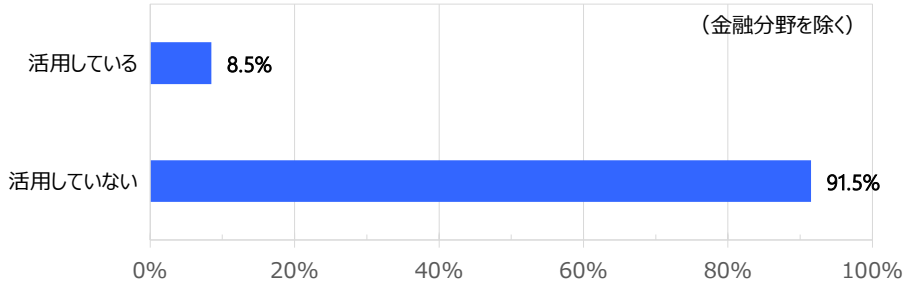
設問３－11．【単一回答】
サイバーセキュリティに関する事件・事故（サービス停止、情報漏えい、改ざん等）が発生した場合の情報開示の基準を策定していますか。



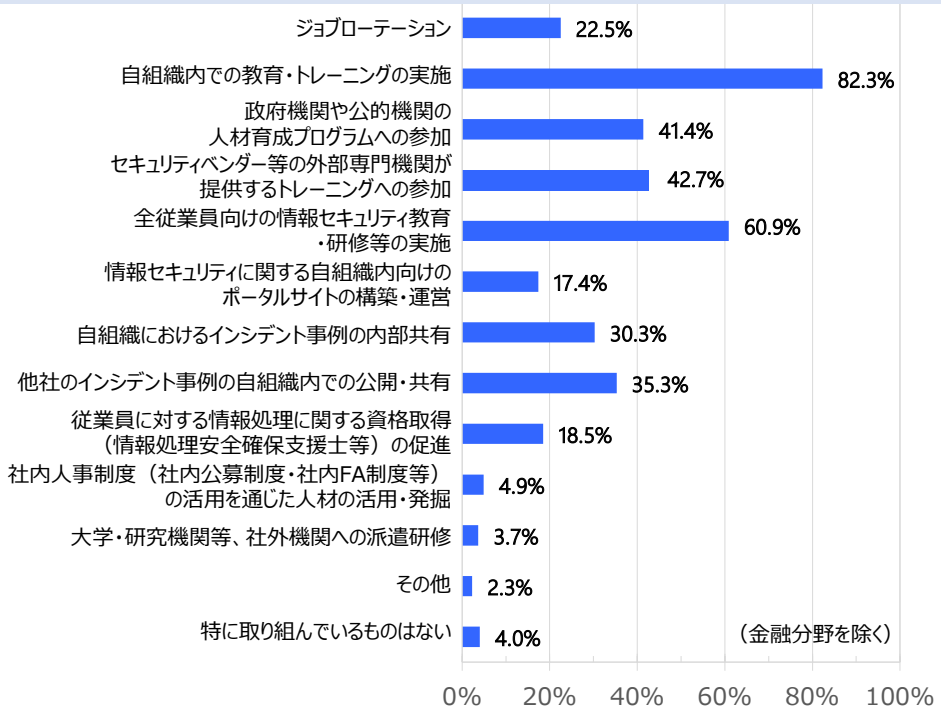
設問４－１．【単一回答】
サイバーセキュリティの確保に必要となる人材や予算が明確化され、組織内に適切に配分されていると感じますか。



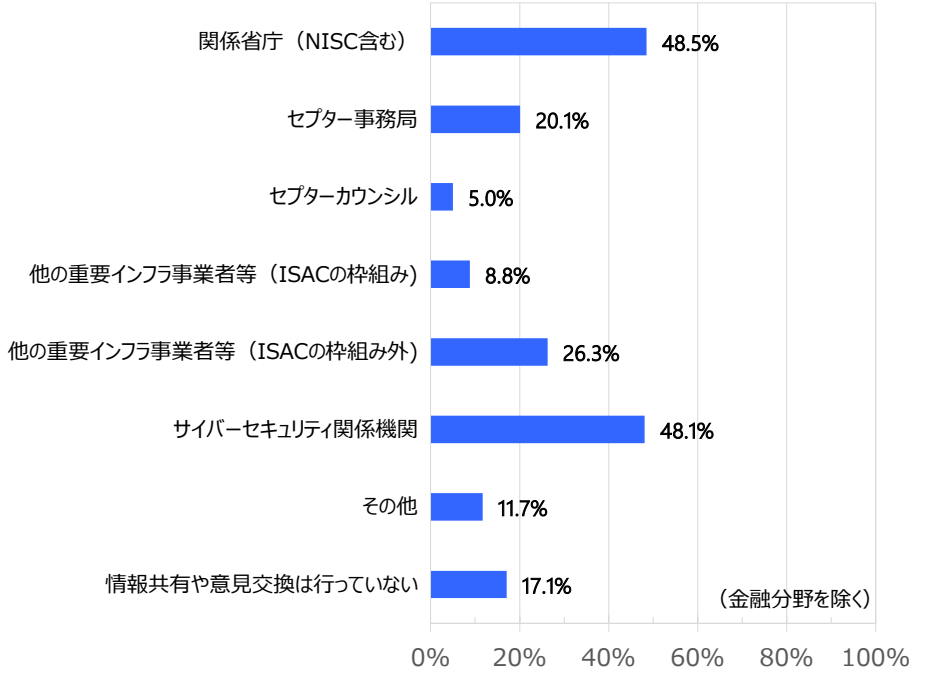
設問４－３．【単一回答】
自組織において、情報処理安全確保支援士資格取得者を活用していますか。



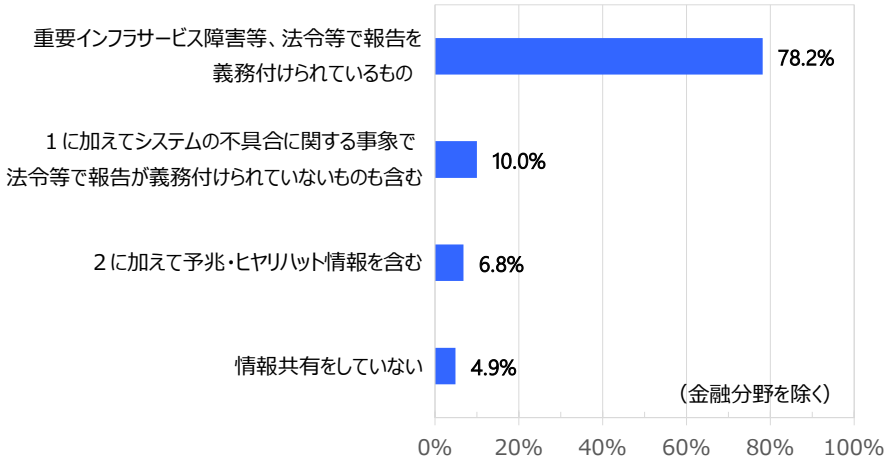
設問４－２.【複数回答】
情報セキュリティ人材の育成や従業員の情報セキュリティに関する意識啓発について、自組織で取り組んでいるものを全て選択してください。



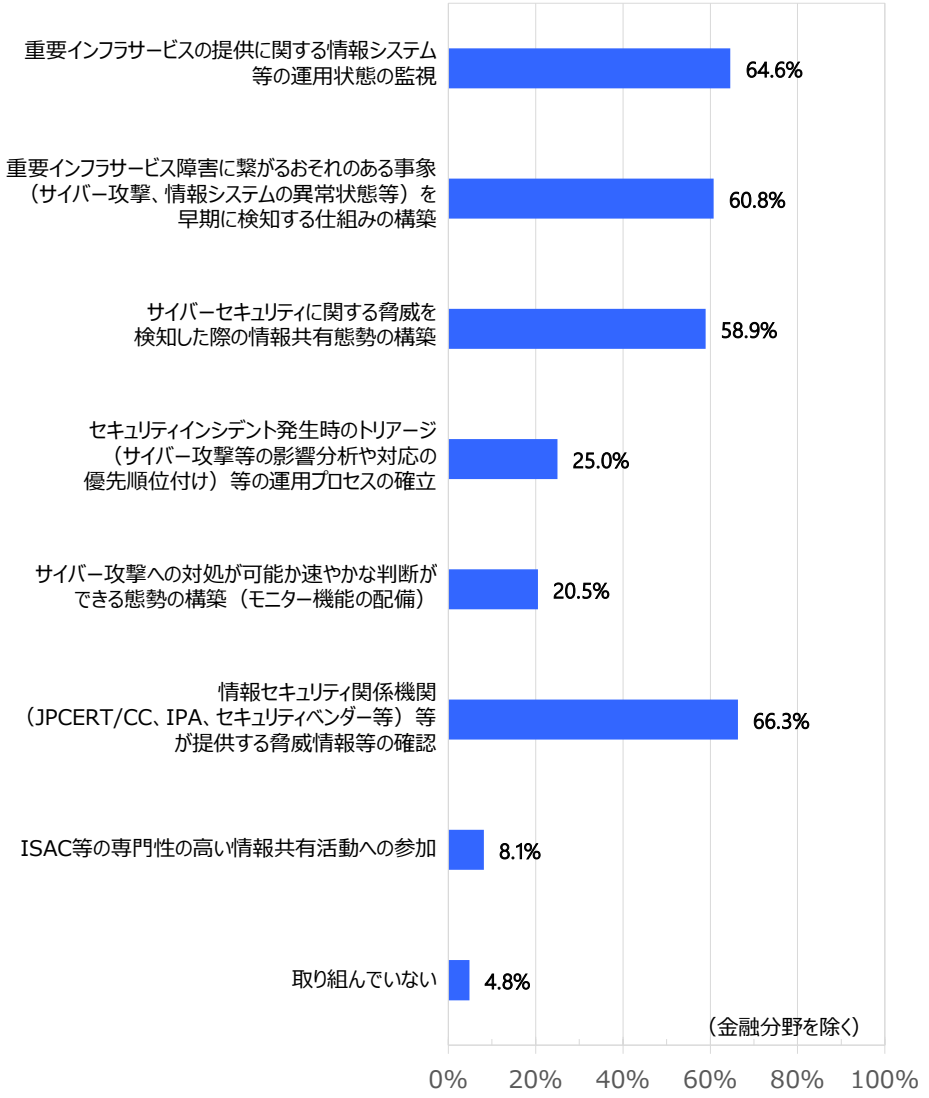
設問４－４．【複数回答】
重要インフラサービスの安全かつ持続的な提供を実現するという観点から、情報共有や意見交換を行っている関係主体を全て選択してください。



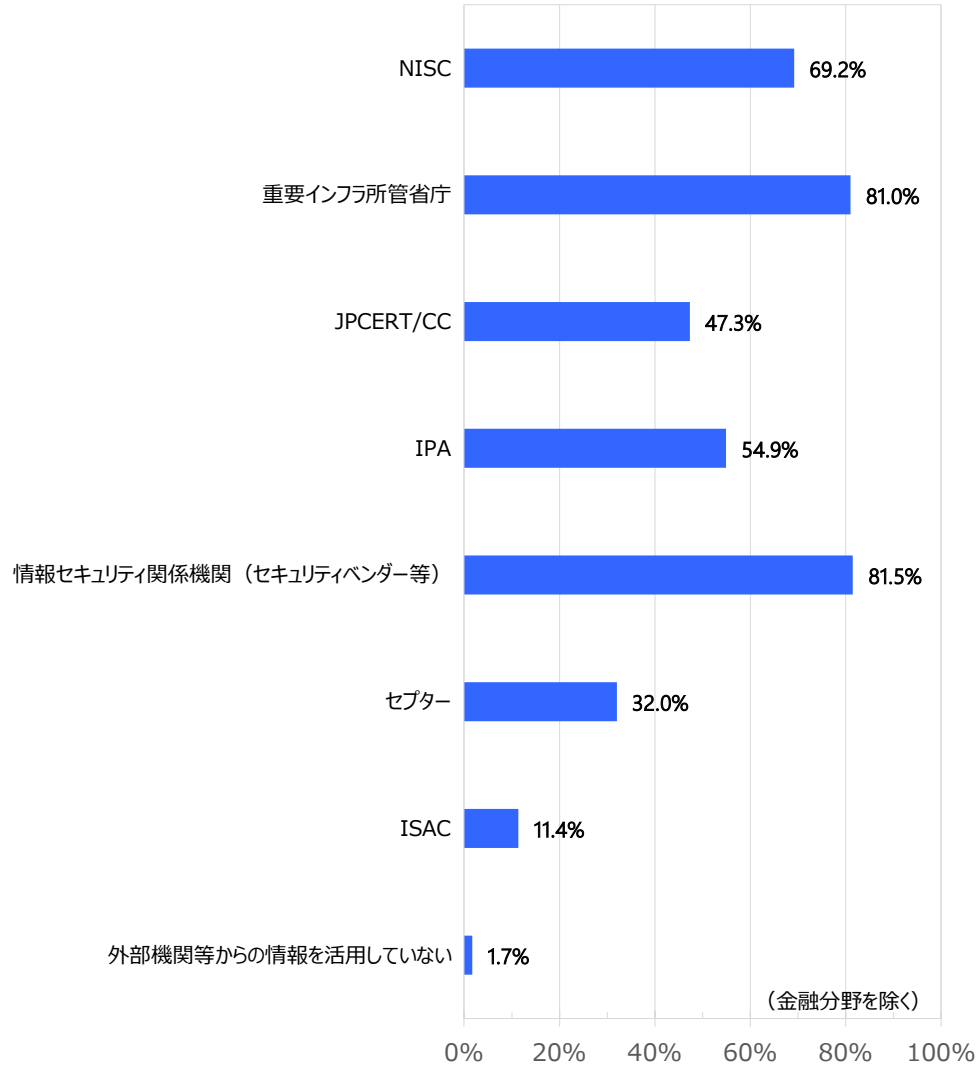
設問４－５．【単一回答】
自組織の情報システムの不具合について、重要インフラ所管省庁等との情報共有の対象範囲を選択してください。



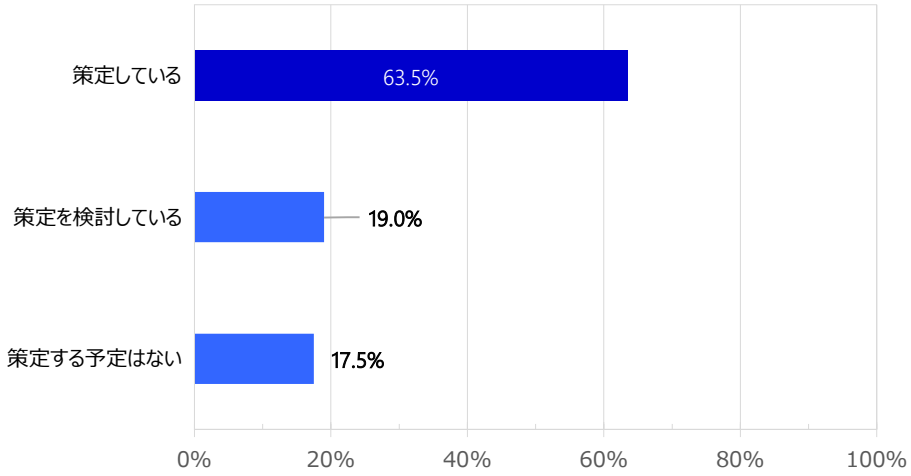
設問５－１．【複数回答】
情報システムの導入・運用時におけるサイバーセキュリティ確保の取組を全て選択してください。

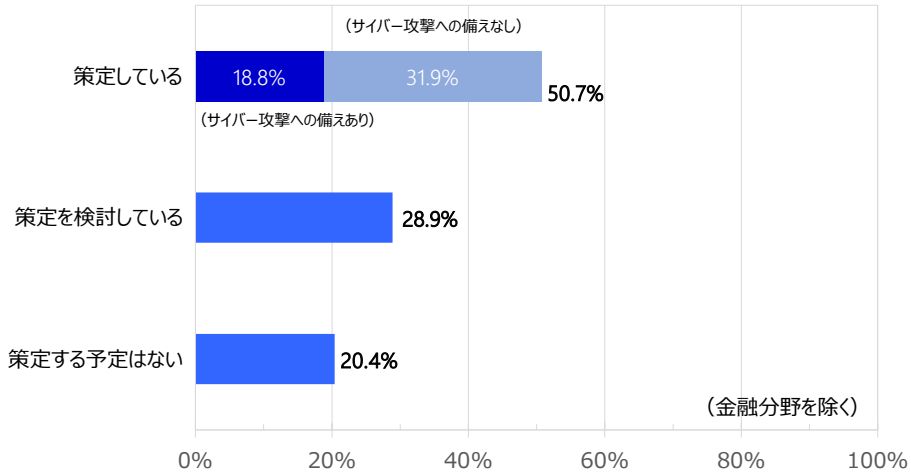


設問５－２．【複数回答】
自組織で活用している情報の提供元を全て選択してください。

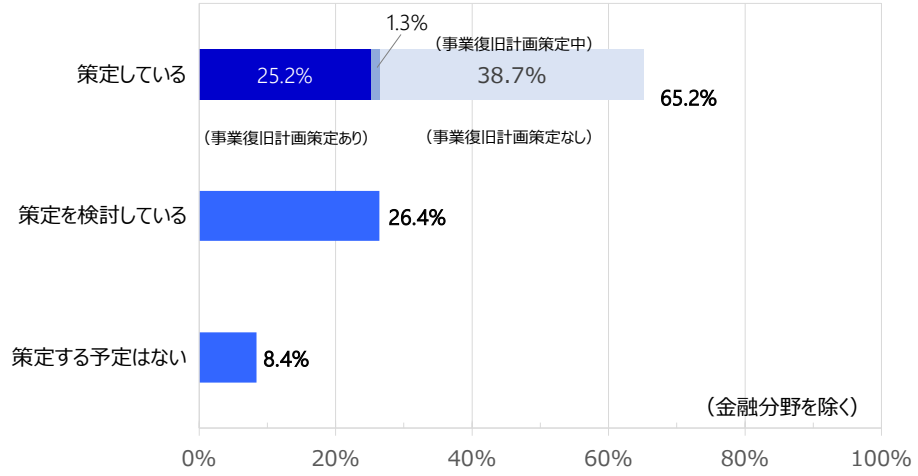


設問５－３．【単一回答】
重要インフラサービス障害の発生に備えたコンティンジェンシープランを策定していますか。
また、サイバー攻撃への備えを取り入れたものとしていますか。
（上段：対象の全分野　下段：金融分野を除いた内訳）

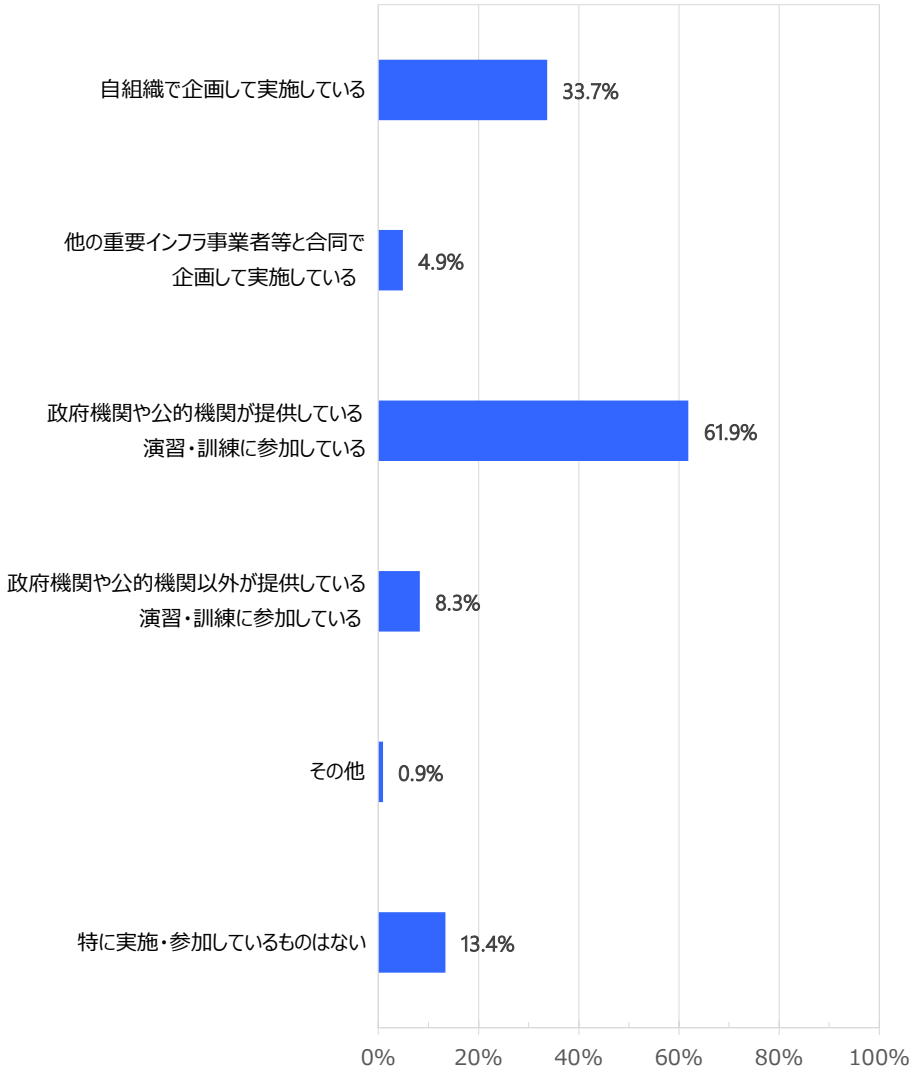




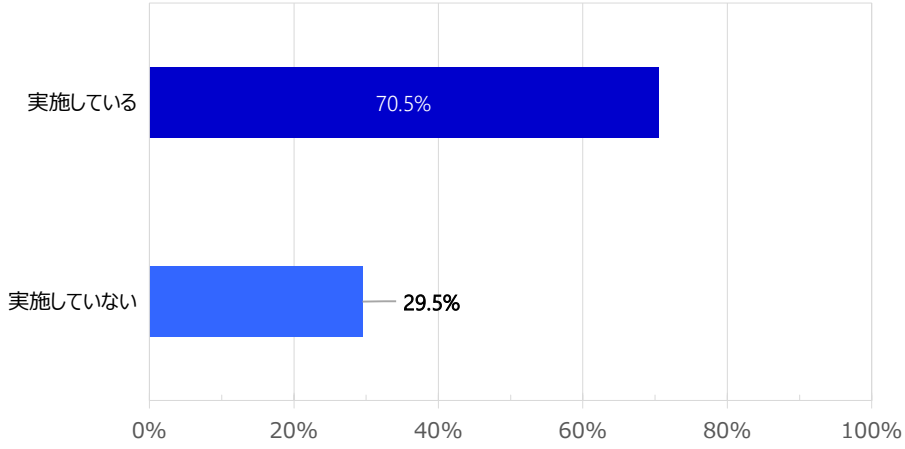
設問５－４．【単一回答】
重要インフラサービス障害の発生に備えた事業継続計画を策定していますか。
また、事業復旧計画を策定していますか。

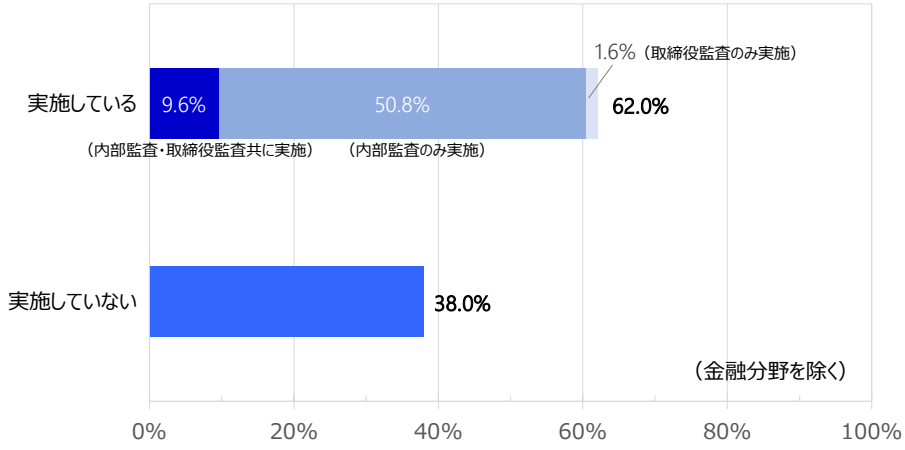


設問５－５．【複数回答】
サイバーセキュリティ確保に関する演習・訓練について、自組織で実施・参加しているものを全て選択してください。

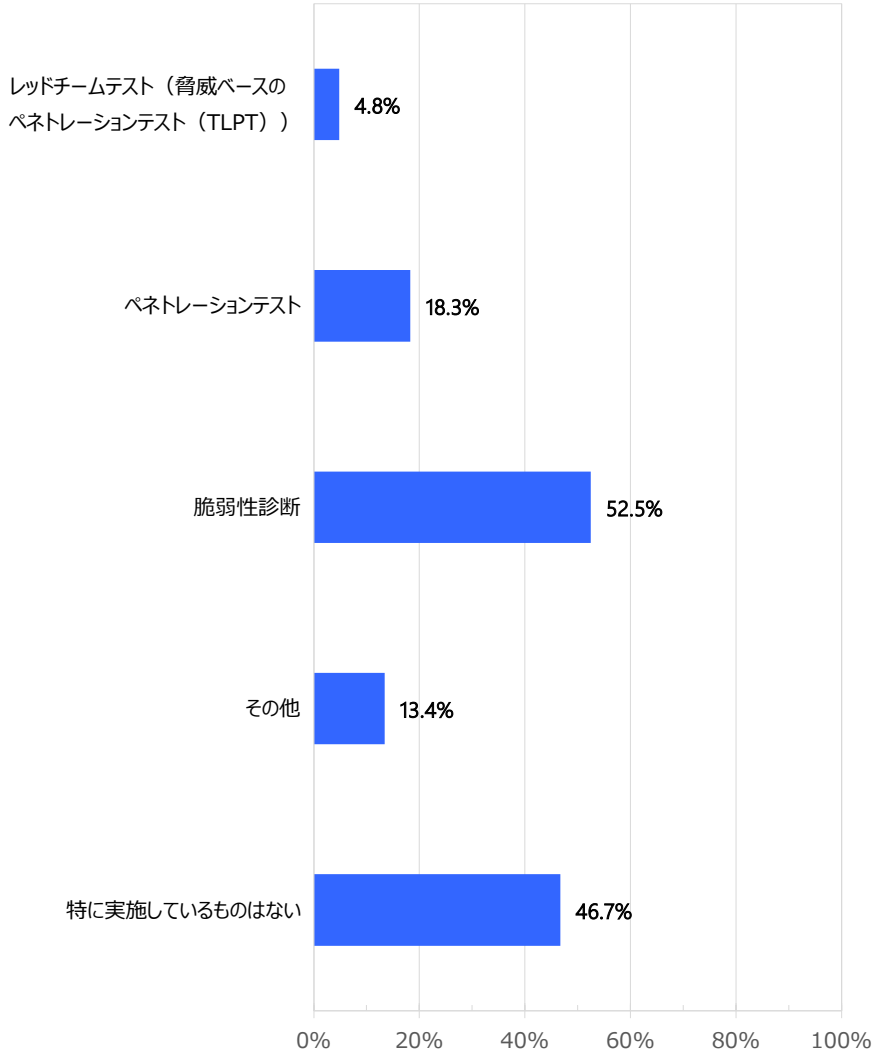


設問６－１．【単一回答】
自組織のサイバーセキュリティ確保の取組について、監査を実施していますか。
（上段：対象の全分野　下段：金融分野を除いた内訳）

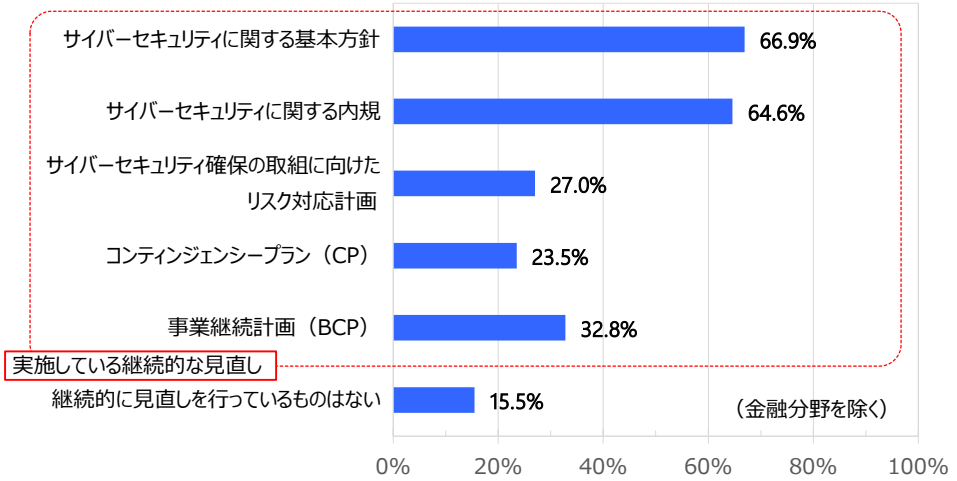




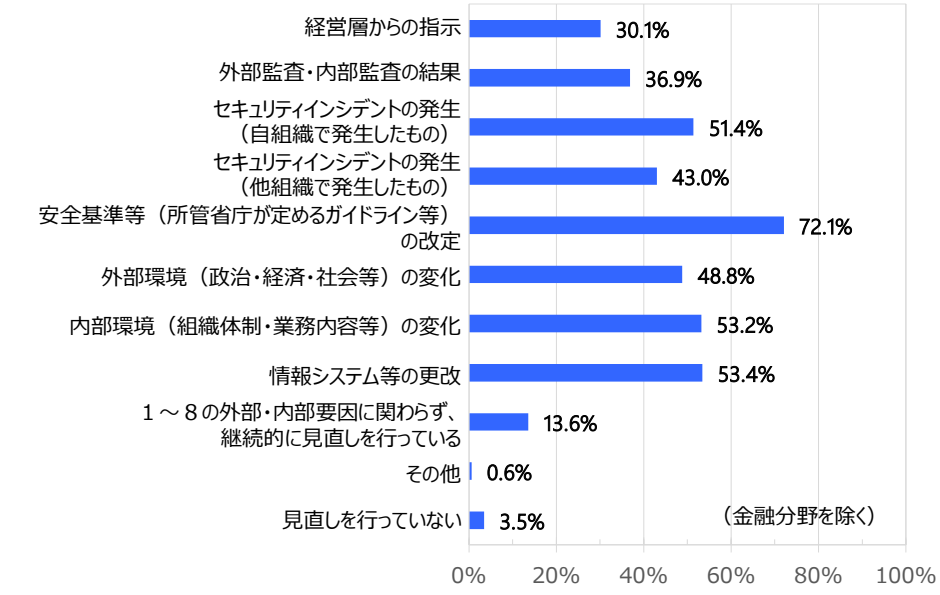
設問６－２．【複数回答】
自組織にて実施しているセキュリティ評価を全て選択してください。



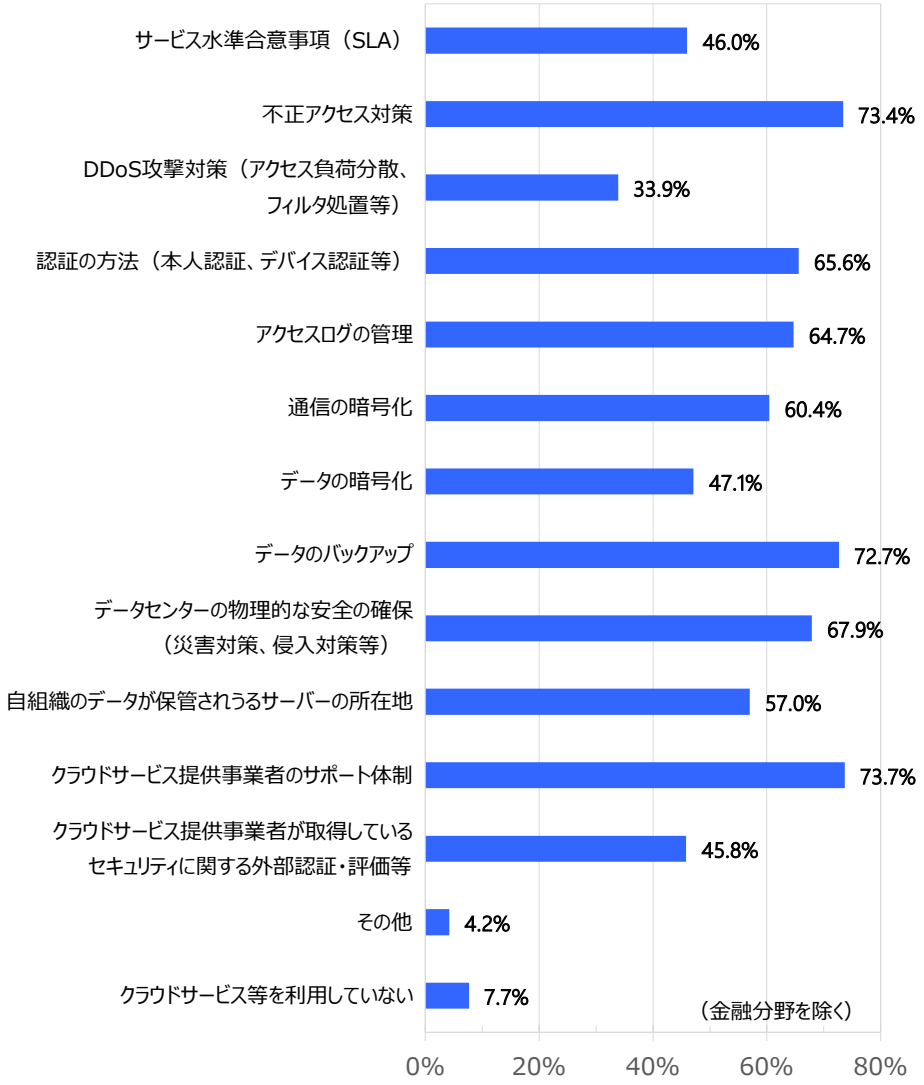
設問７－１．【複数回答】
サイバーセキュリティ確保の取組の改善に向け、継続的に見直しを行っているものを全て選択してください。



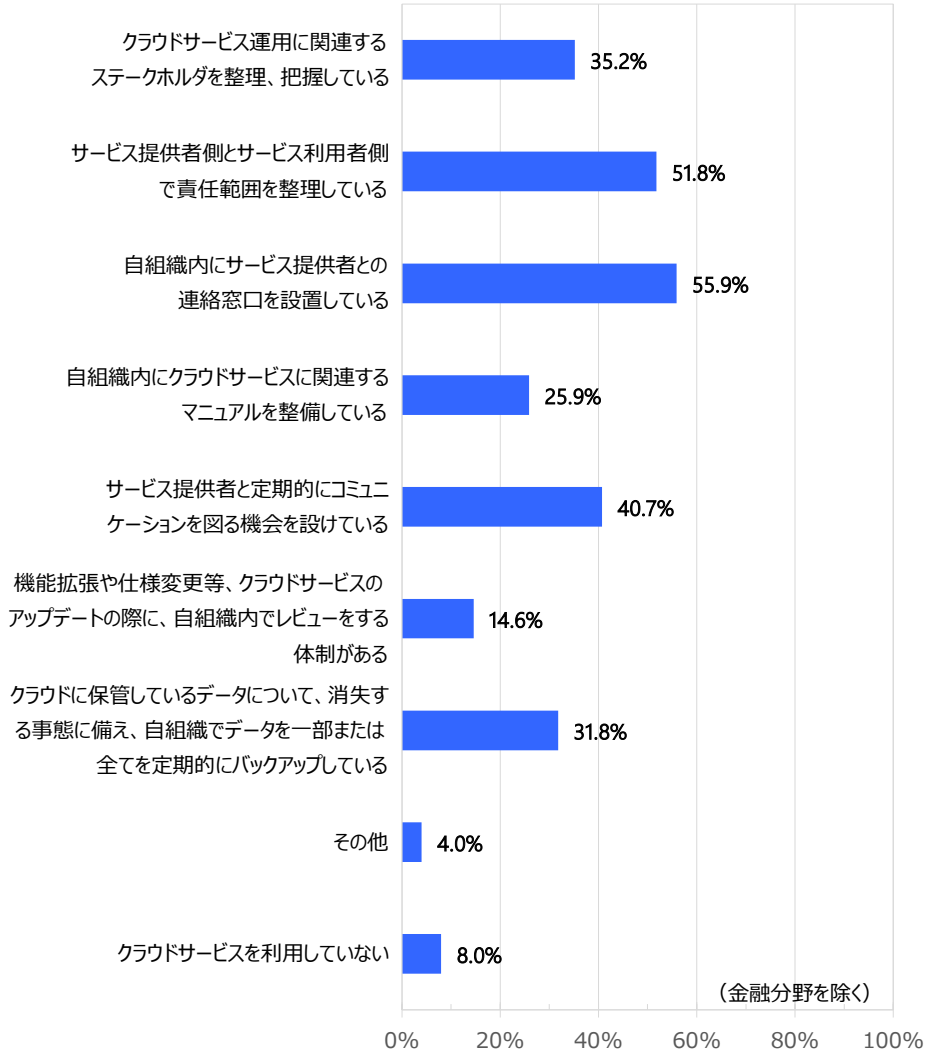
設問７－２．【複数回答】
サイバーセキュリティ確保の取組の見直しの契機となるものを全て選択してください。



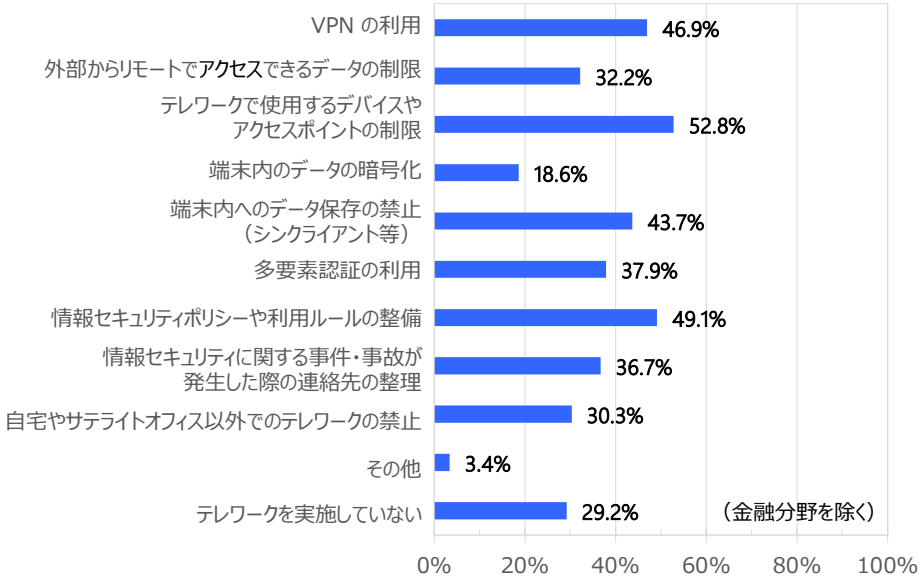
設問８－１．【複数回答】
自組織がクラウドサービスを利用する際に、クラウドサービス提供事業者側へ確認している事項を全て選択してください。



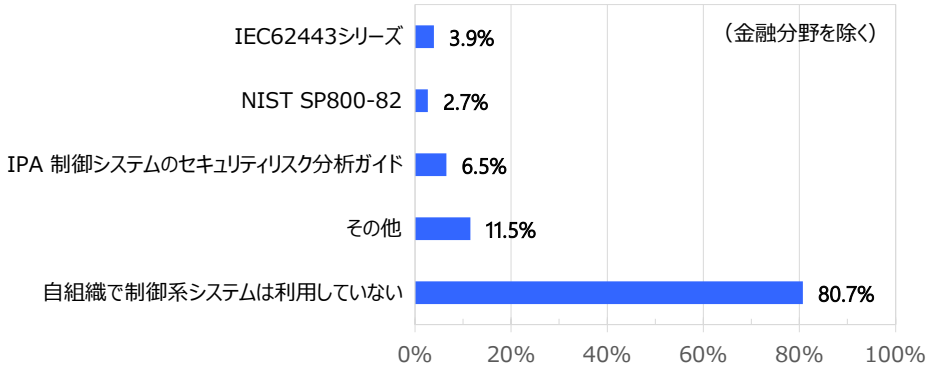
設問８－２．【複数回答】
クラウドサービスを利用するに当たり、自組織で行っている運用対策を選択してください。



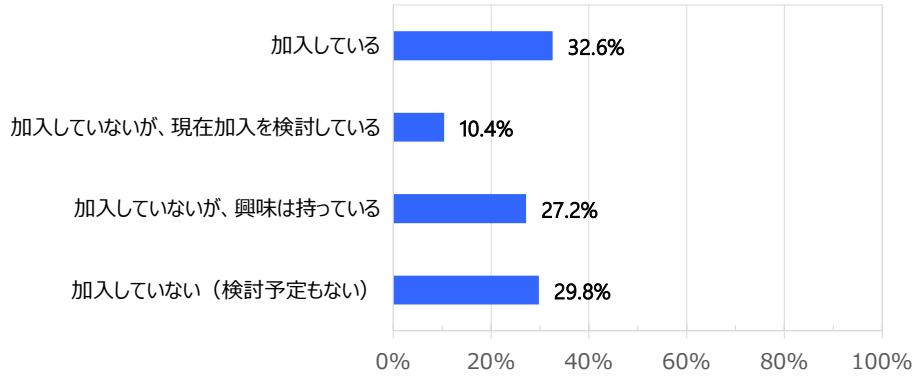
設問９．【複数回答】
テレワークの際に実施しているセキュリティ確保の取組を全て選択してください。



設問10－１．【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10－２．【単一回答】
自組織でサイバー保険に加入していますか。



設問10－３．【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。