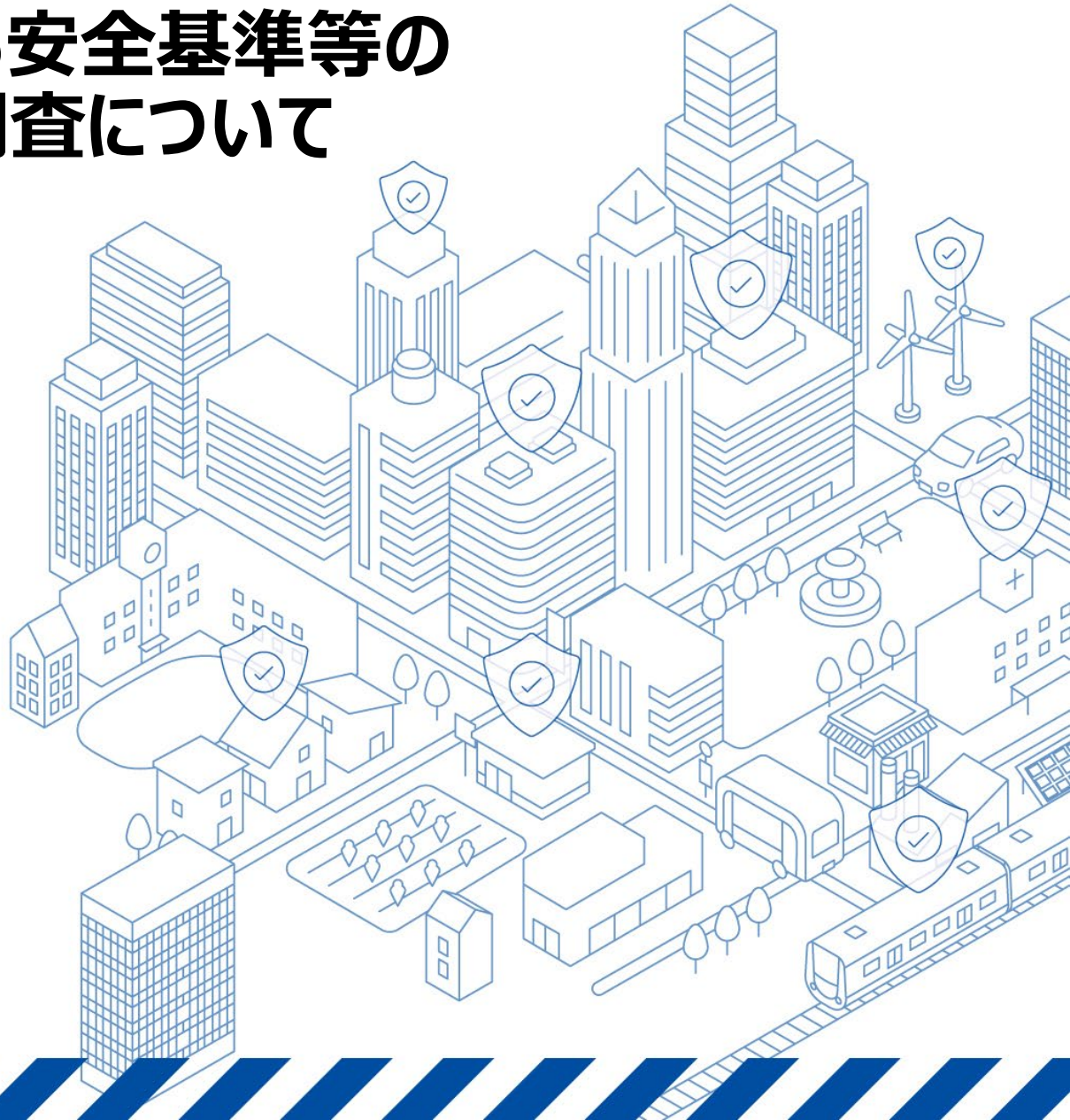
重要インフラにおける安全基準等の浸透状況に関する調査について

［2025年度］



令和８年７月
内閣官房 国家サイバー統括室
制度総括班

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。

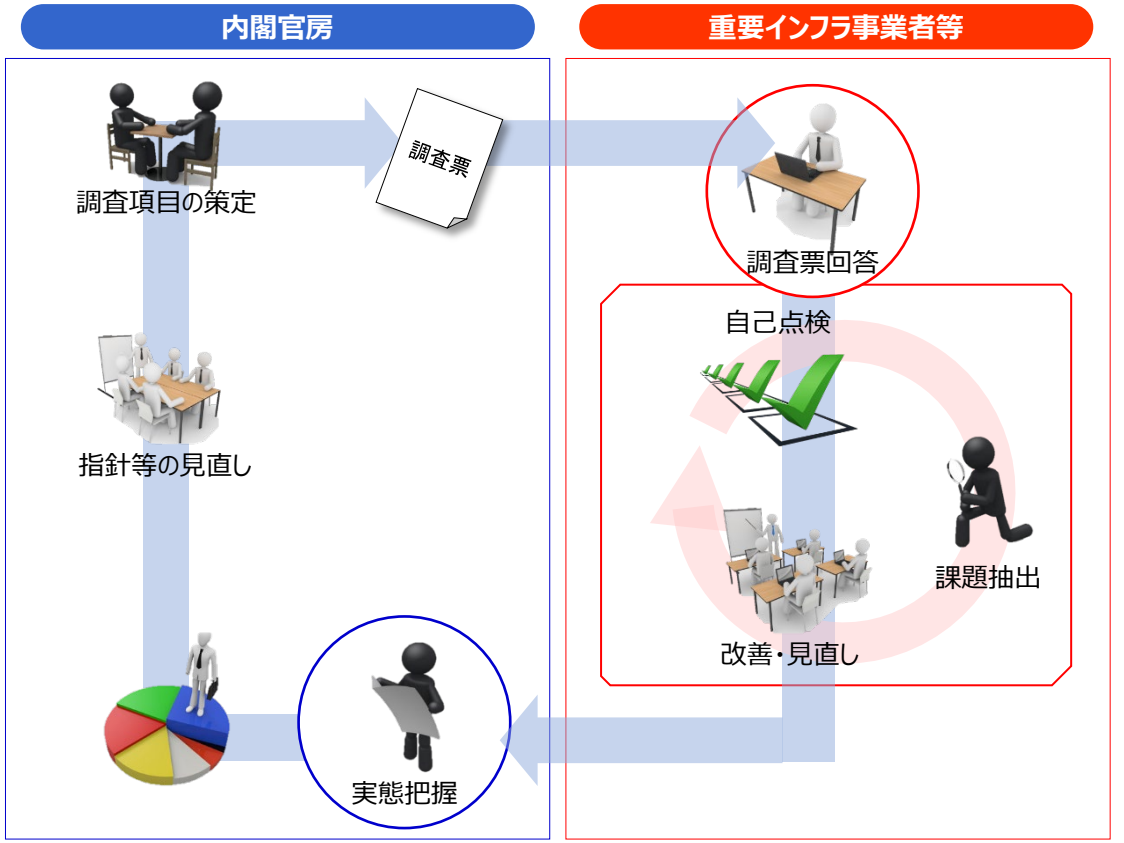
調査の概要

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：2025年9月30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	次の方法で調査を実施 **調査方法①：NCO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（資金決済以外の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（資金決済を除く金融分野のみ）

【参考：本調査の実施背景】
○重要インフラのサイバーセキュリティに係る行動計画

Ⅳ.2.3 安全基準等の浸透
（略）**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。

調査の流れ（イメージ）



2025年度調査対象及び回答状況

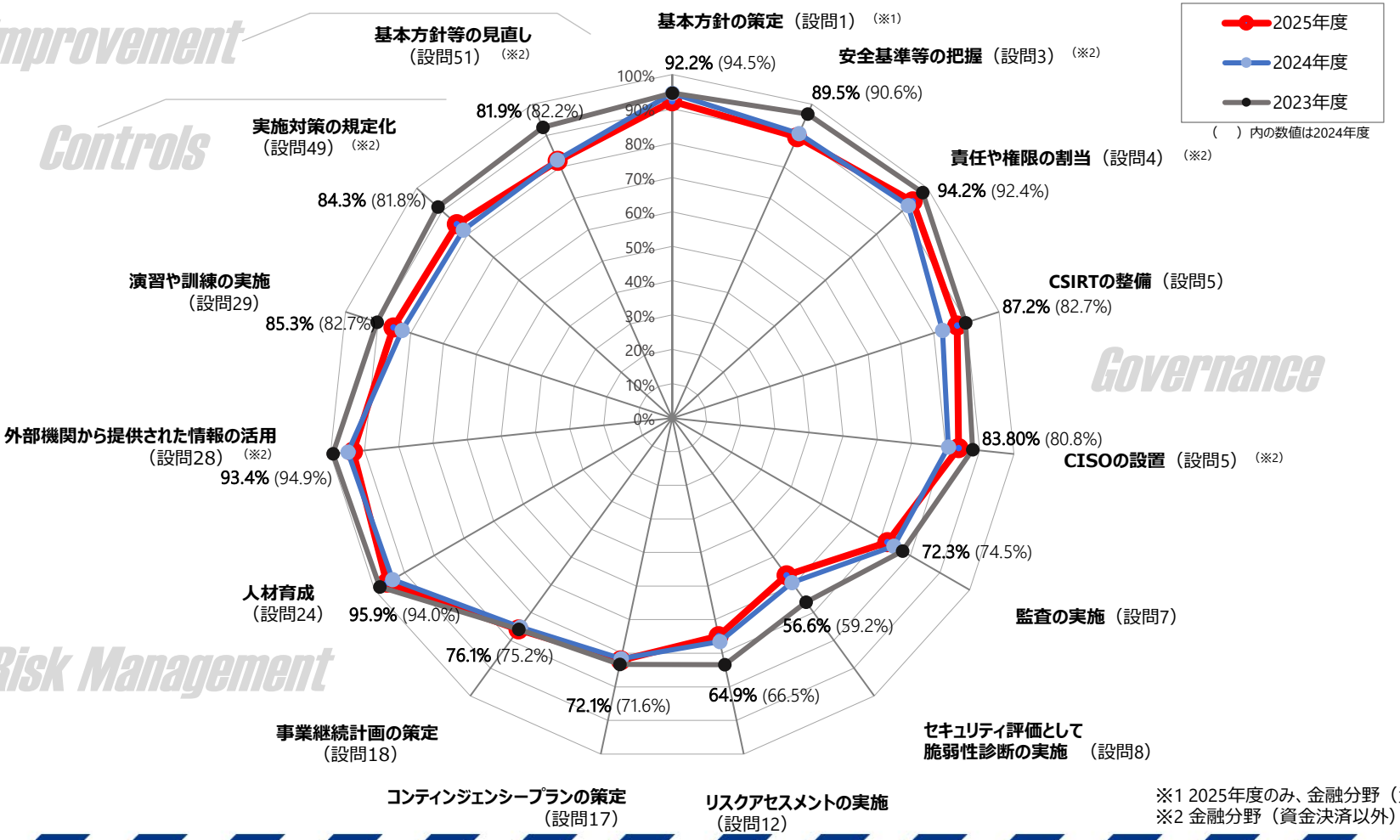
- 2025年度は、**重要インフラ分野（計15分野）の事業者等を対象に調査を実施し、合計2,103事業者から回答**（回答率54.2%）を得た。
（【参考】2024年度は、2,099事業者）

重要インフラ分野		調査対象	配布数	回答数
情報通信	電気通信	主要な電気通信事業者	20	15
	放送	主要な地上基幹放送事業者	195	91
	ケーブルテレビ	主要なケーブルテレビ事業者	300	130
金融※1		銀行等、生命保険、損害保険、証券会社	759※1	668※1
金融（資金決済）		主要な資金移動業者 主要な前払式支払手段（第三者型）発行者	170	87
航空		主たる定期航空運送事業者	15	13
空港		主要な空港・空港ビル事業者	8	8
鉄道		ＪＲ各社及び大手民間鉄道事業者等の主要な鉄道事業者	22	22
電力		一般送配電事業者、主要な発電事業者等	24	24
ガス		主要なガス事業者	13	12
政府・行政サービス		地方公共団体	1,788	652
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	30	26
水道		2025年度大臣認可水道事業者	438	297
物流		大手物流事業者	15	9
化学		主要な石油化学事業者	12	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	21	17
石油		主要な石油精製・元売事業者	6	6
港湾		主要な港湾運送事業者・港湾管理者等	46	18
全分野合計		－－－	**3,882 (3,123)**※2	**2,103 (1,435)**※2

※1　金融分野については外部調査にて実施したものを、NCO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）

- **「基本方針の策定」や、「責任や権限の割当」、「情報の活用」、「人材育成」といった対策については比較的高い水準で推移**している。加えて、**「CSIRTの整備」および「CISOの設置」は昨年度と比較して改善**が見られ、体制整備の面での前進が確認できる。
- 一方、**「監査の実施」、「脆弱性診断の実施」、「リスクアセスメントの実施」といった対策の実施率は、相対的に低い**状況である。コスト負担や必要な知識の不足がより進んでいることが主な要因と推察される。今後は、着手のハードルを下げることを目的とした支援策等を推進することが重要である。　※2024年度より、一部分野において中小規模を含めた全国の事業者等を調査対象に加えており、全体的に実施率が低下している。



※1 2025年度のみ、金融分野（資金決済以外）を除く
※2 金融分野（資金決済以外）を除く

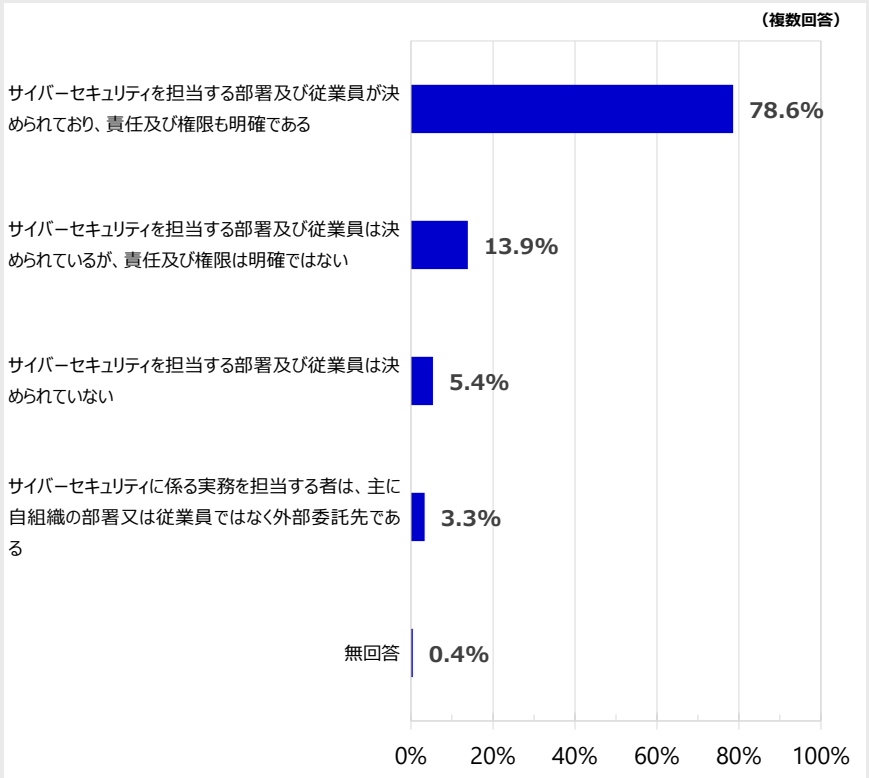
浸透状況と課題 － 組織統治に関する取組

- サイバーセキュリティの担当部署・従業員の決定や、責任・権限の明確化については、8割弱（78.6%）が実施済みであり、**体制面の整備は概ね進んでいる。**
- 人材・予算の観点では、**「共に十分に配分されている」とする事業者は1割強（11.6%）**であり、**いずれかが十分な場合も2割強（22.3%）**に留まる。
- 体制が整っている事業者を含め、**多くの事業者が人材や予算の不足、それらの必要量の不明確さを課題としており**、体制整備に加えて、必要な人員・予算の明確化や配分の見直し、外部サービスの活用等を進めることが必要と考えられる。

► サイバーセキュリティを担当する部署及び従業員の決定と、責任及び権限の割当て状況（設問４）

※３.４.責任及び権限の割当て

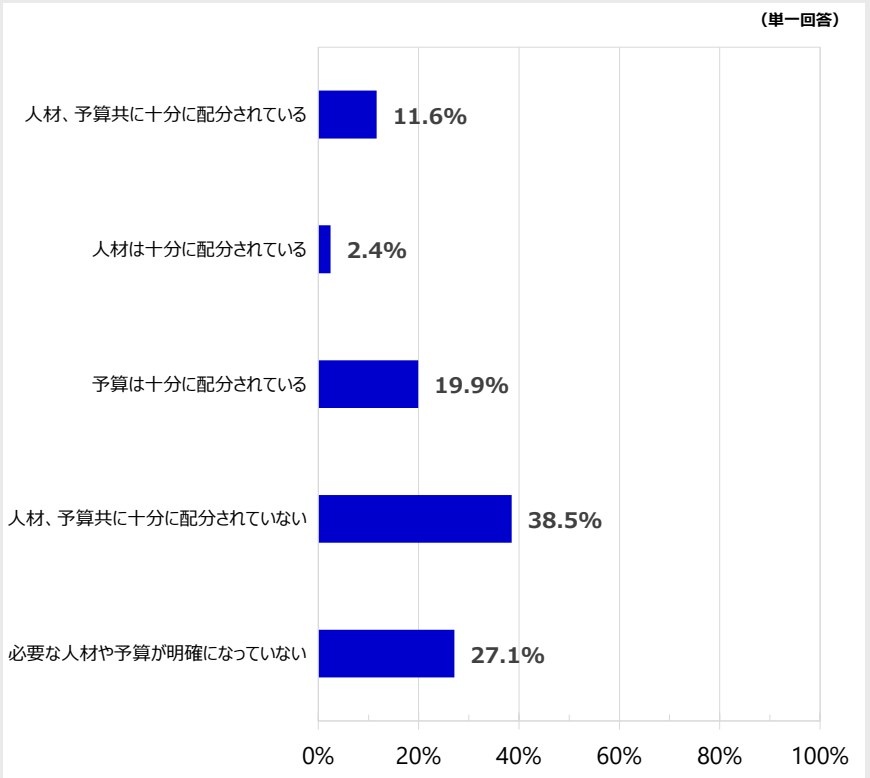
※金融分野（資金決済以外）を除く



► サイバーセキュリティの確保に必要となる人材や予算の明確化、組織内への配分状況（設問６）

※３.５.資源の確保

※金融分野（資金決済以外）を除く



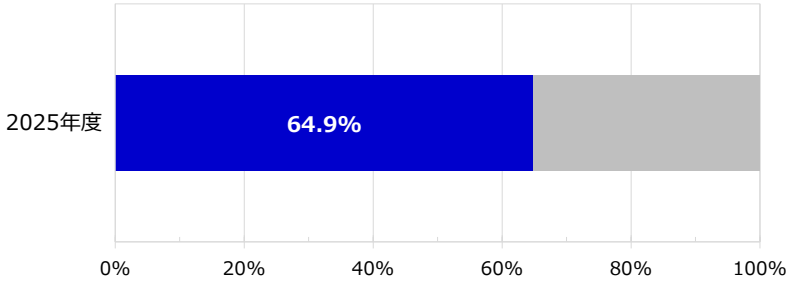
※設問に対応する「指針」の節等を記載

浸透状況と課題 － リスクマネジメントに関する取組

- **<u>リスクアセスメントの実施状況は６割強（64.9%）</u>**にとどまる。**<u>評価対象の範囲や粒度の整理が難しく着手しづらい点、また、専門人材等の実施リソースの不足が、実施率の低さの主な要因として推察される。</u>**任務保証の考え方の浸透等、**<u>引き続きの改善に向けた取組が必要</u>**である。
- サプライチェーンリスクへの認識が広まる一方で、**<u>対策の実施率は相対的に低水準</u>**である。特に、対策の起点となる「契約事項の合意」（16.9%）や「責任分界点の明確化」（19.9%）は、いずれも2割を切る低い水準に留まっている。リスクとして認識しつつも、実効性を担保するための契約締結やルール整備が追いついていないことが推察される。今後は、単なる現状把握のフェーズから、実効性のあるリスク管理体制への移行が必要と思われる。

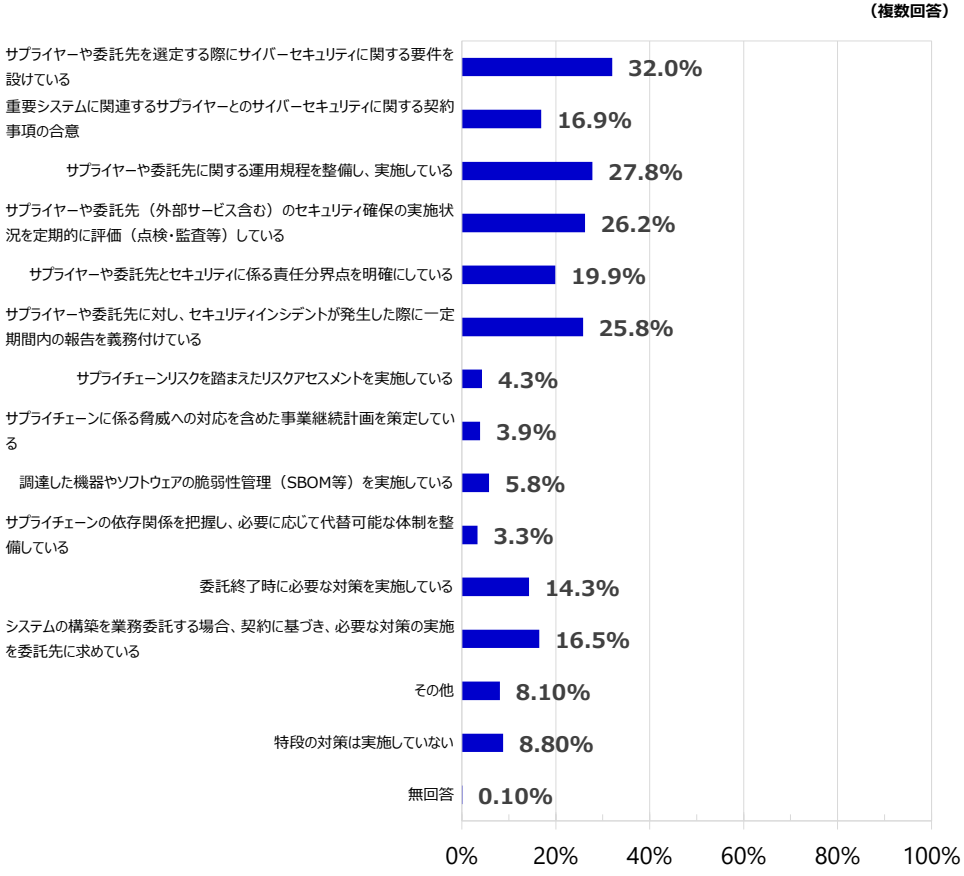
► リスクアセスメントを実施している（設問12）

※４.２.リスクアセスメント



► 自組織のサプライチェーンに関して実施しているリスク軽減策（設問16）

※４.４.サプライチェーン・リスクマネジメント

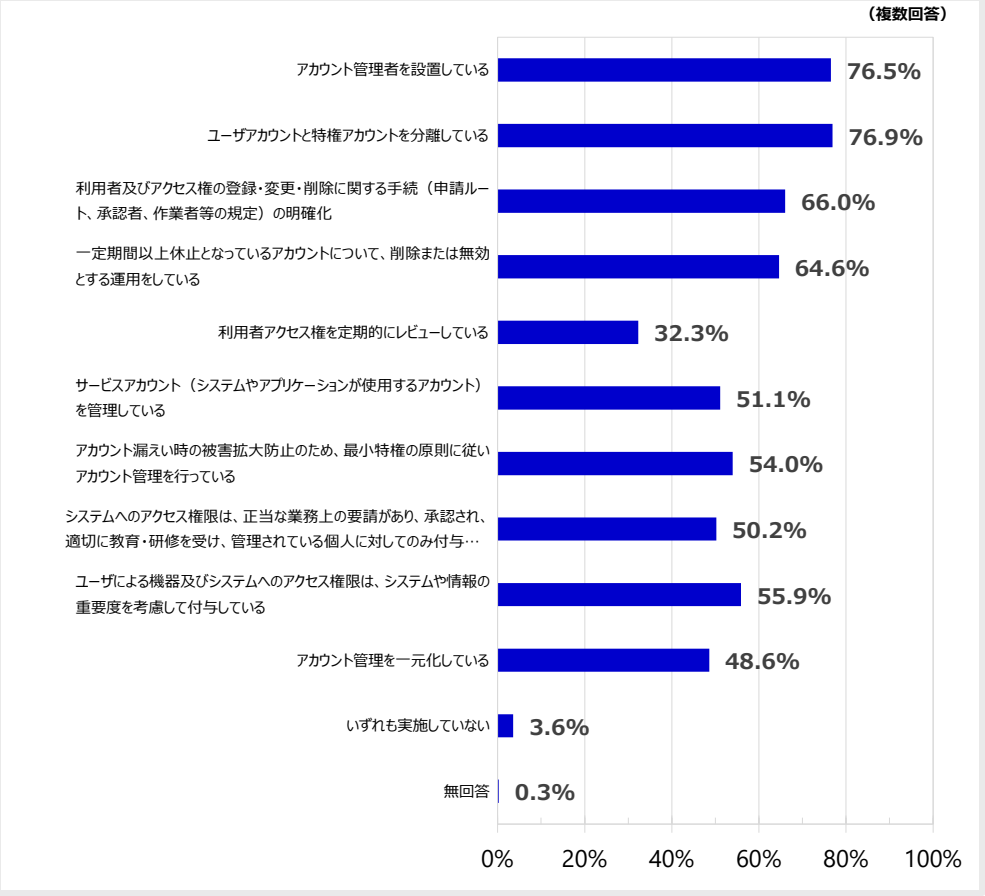


※設問に対応する「指針」の節等を記載

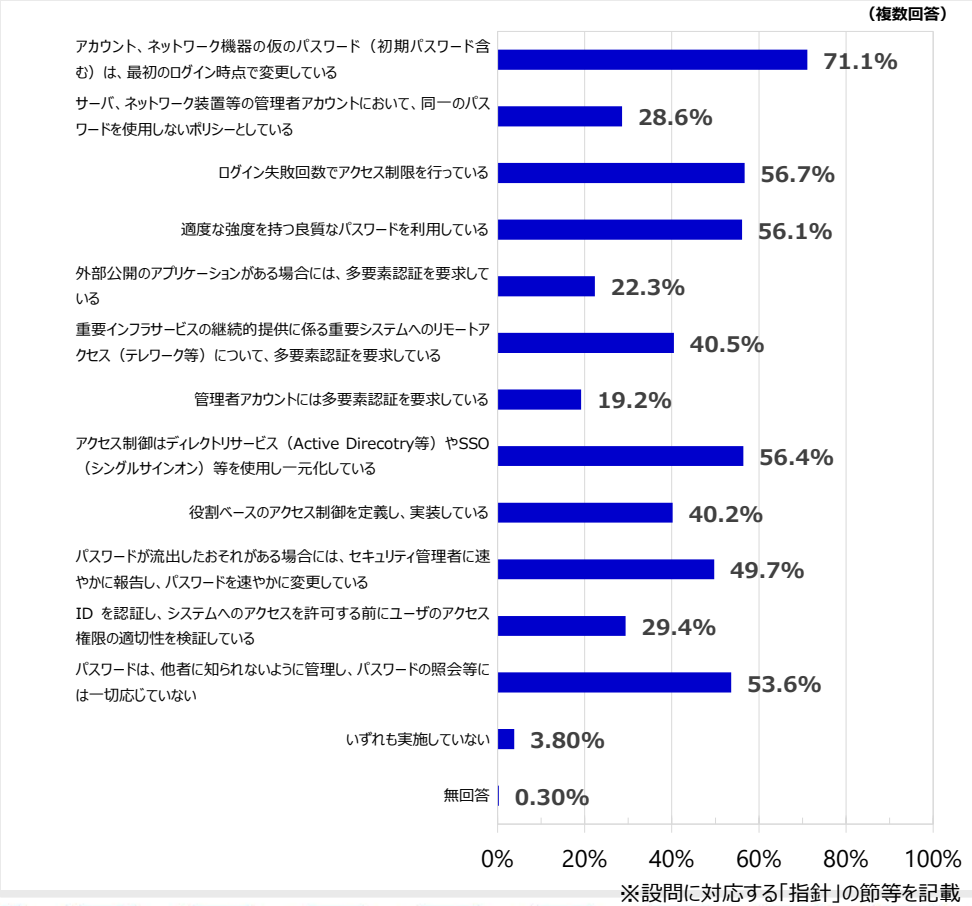
浸透状況と課題 － 技術的対策に関する取組

- アカウント管理については、権限の妥当性を継続的に確認する**「利用者アクセス権の定期的なレビュー」の実施率は約３割**にとどまり、継続的な運用サイクルが十分に機能していないおそれがある。レビューの不徹底や形骸化は、不要な権限の残存を招き、深刻なインシデントの引き金にもなり得るため、引き続き、事業者等に対して取組徹底の促進を行っていく必要がある。
- アクセス制御については、**「外部公開アプリケーションへの多要素認証」や「管理者アカウントへの多要素認証」の実施率がいずれも約２割**にとどまり、認証強度の不足が課題となっている。特権IDの奪取は致命的な被害に直結するため、重要システムや管理者アカウントに対する多要素認証の実装など、引き続き、事業者等に対して取組の促進を行っていく必要がある。

► アカウント管理に関して実施している取組（設問43）※５.４.１.利用者アクセスの管理



► アクセス制御に関して実施している取組（設問44）※５.４.２.情報システム等のアクセス制御

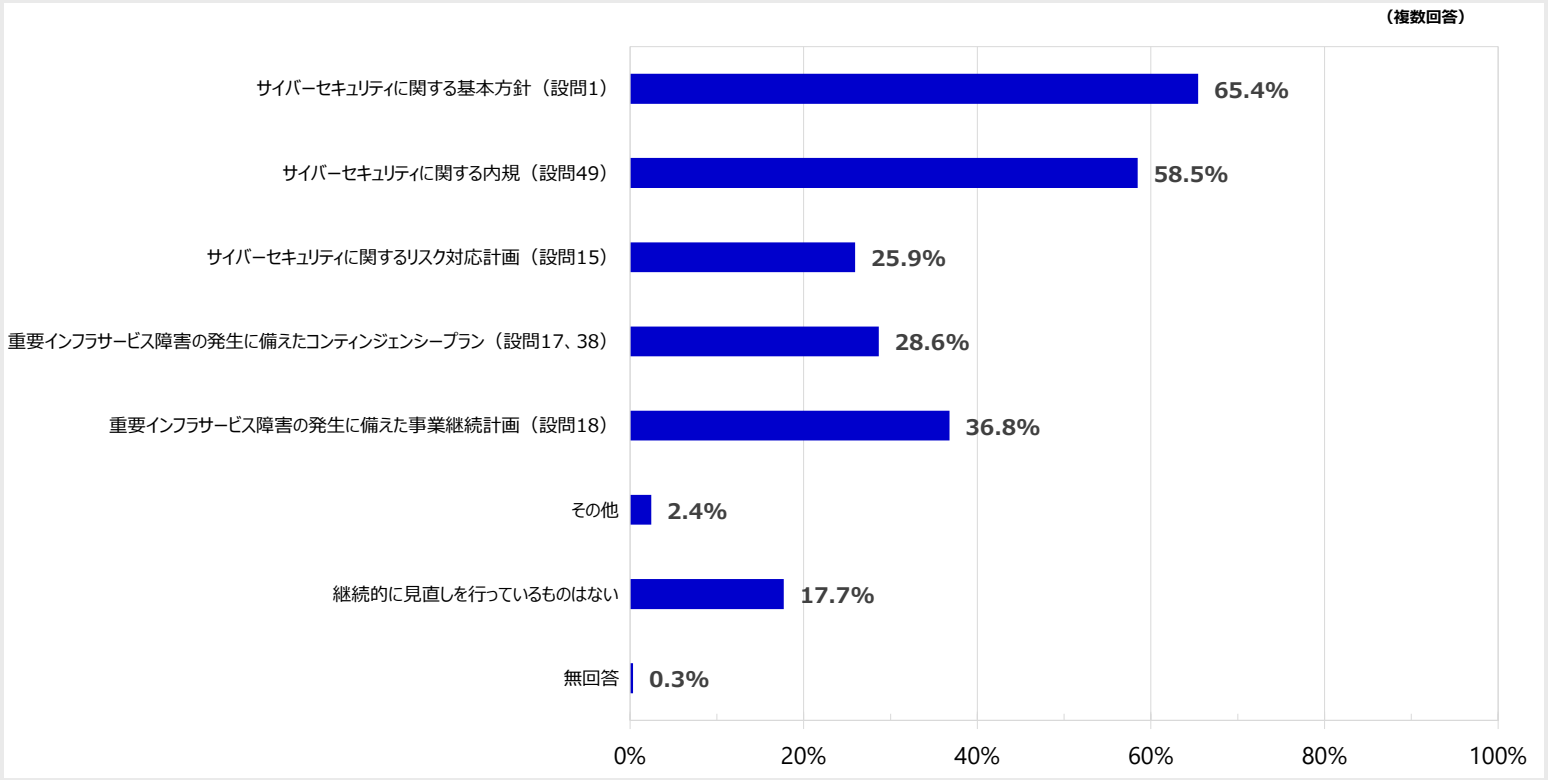


※設問に対応する「指針」の節等を記載

- 継続的な見直しについては、**８割強（82%）の事業者が基本方針等の見直し**を行っている。
- 一方、見直しの中心は基本方針（65.4%）や内規（58.5%）に偏り、**リスク対応計画（25.9%）、コンティンジェンシープラン（28.6%）、事業継続計画（36.8%）は相対的に低水準**である。重要インフラの任務保証の観点からも、リスク対応計画、コンティンジェンシープラン、事業継続計画等の定期的・継続的な見直しの推進が必要と考えられる。

► **サイバーセキュリティ確保の取組の改善に向け、継続的に見直しているもの**（設問51）　※3.8.継続的改善

※金融分野（資金決済以外）を除く



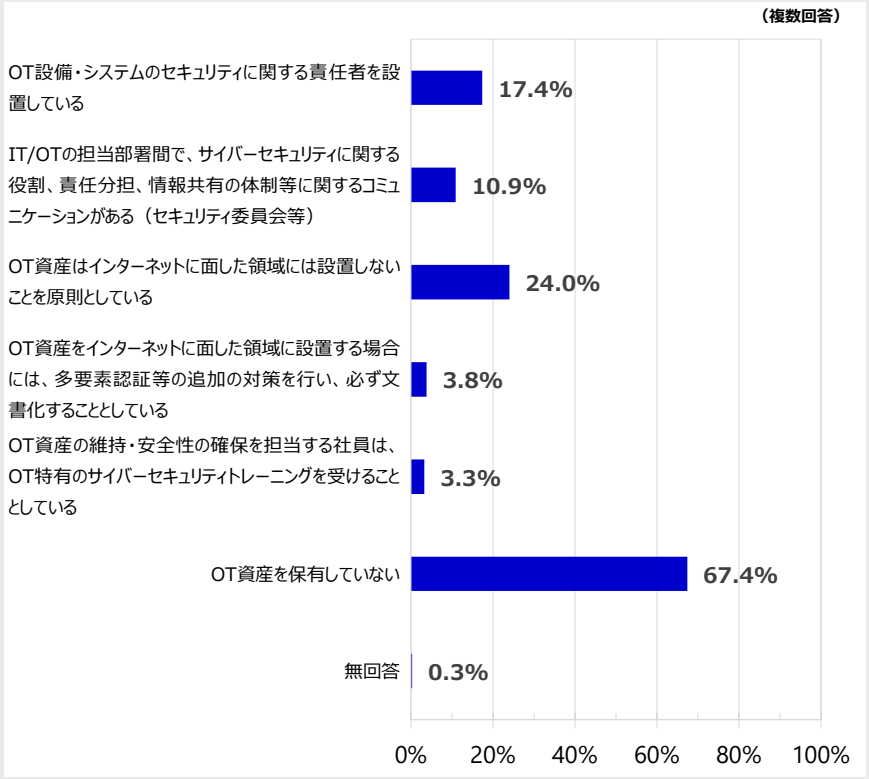
※設問に対応する「指針」の節等を記載

浸透状況と課題 － 制御システム・クラウドサービスに関する取組

- **３割強（32.4% ※無回答は除外）が制御システム（OT資産）を保有**している状況である。保有組織においては、「インターネット非接続の原則対応」は進む一方、**責任者設置は約半数にとどまり、IT/OTの担当者間のコミュニケーションや、OT特有の訓練の実施は相対的に低水準**である。
- **９割弱（89.9% ※無回答は除外）がクラウドサービス等を利用**している状況である。利用組織においては、**対策の起点となる「責任範囲の整理」が約半数にとどまるほか、アップデート時の社内レビュー体制（16.6%）やデータ消失に備えた自組織でのバックアップ（24.4%）、選定・運用時の規程整備（26～28%程度）が相対的に低水準**である。

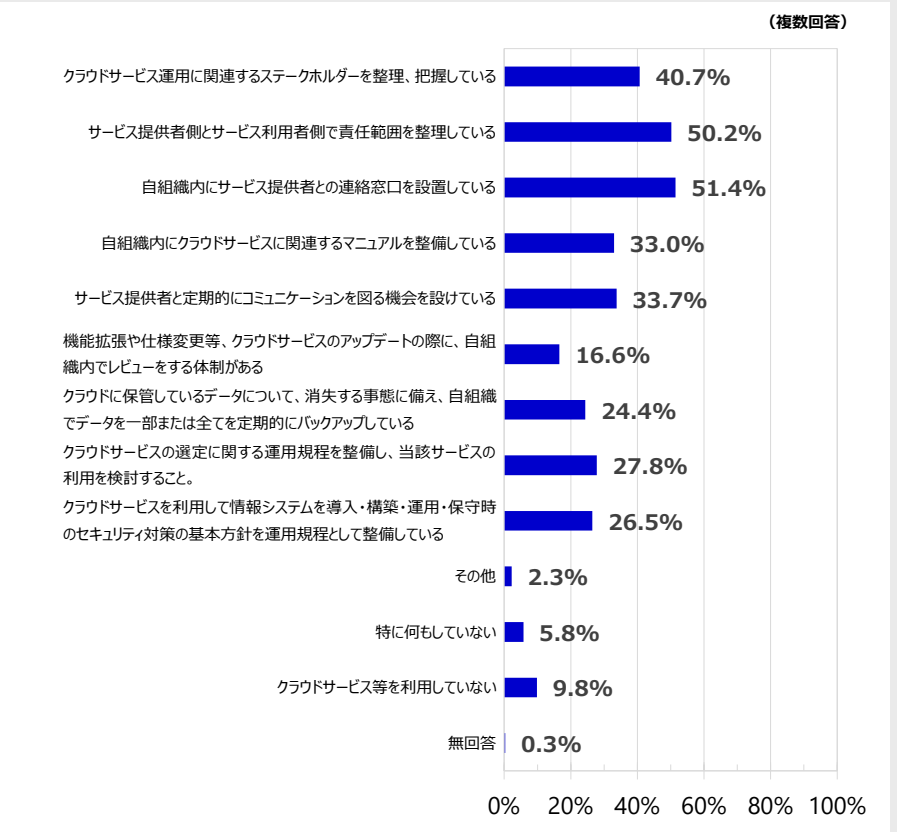
► 制御システム（OT資産）を保有している場合、実施している取組（設問48）

※金融分野（資金決済以外）を除く　※該当なし



► クラウドサービスの利用に当たり、実施している運用対策（設問50）

※金融分野（資金決済以外）を除く　※５.５.２.クラウドサービス利用時の対策



※設問に対応する「指針」の節等を記載

自由意見①

- 有効と考える独自のセキュリティ対策としては、ゼロトラストアーキテクチャの導入やネットワーク分離等、**技術的対策の実施**をあげる事業者が多かった。(設問58)
- セキュリティの取り組みにおいて苦慮している点としては、**人材とコストの両面で**多くの課題があがっている状況であった。(設問59)

設問58.【自由記述】
設問に回答いただいた以外でサイバーセキュリティに係る取組全体を通して有効であると感じられる独自取組があれば自由に記載してください。

回答記載件数：35件

(1社で複数回答は別々に集計)

■主な内容（一部抜粋）

1．教育・訓練について（回答件数：5件）
・経営者層を含むセキュリティ教育の実施
・外部の専門家を招いたセキュリティ教育の実施
・静的なマニュアルだけではなく、動的なコンテンツによる教育実施

2．組織・体制について（回答件数：3件）
・親子会社間での体制共有
・各部門毎にデジタルマネージャー、リーダーを１人以上配置
・IT部門と工場システム部門が融合した組織

3．情報共有について（回答件数：6件）
・部門間、親子会社、委託先、同業他社との情報共有

4．技術的対策について（回答件数：13件）
・ゼロトラストアーキテクチャを採用
・重要システムと非重要システム間でのネットワークセグメントの分離

5．その他（回答件数：8件）
・外部専門家を利用した監査、セキュリティポリシーの作成
・セキュアな外部クラウドサービスの利用

内容	件数
教育・訓練について	5件
組織・体制について	3件
情報共有について	6件
技術的対策について	13件
その他	8件

自由意見②

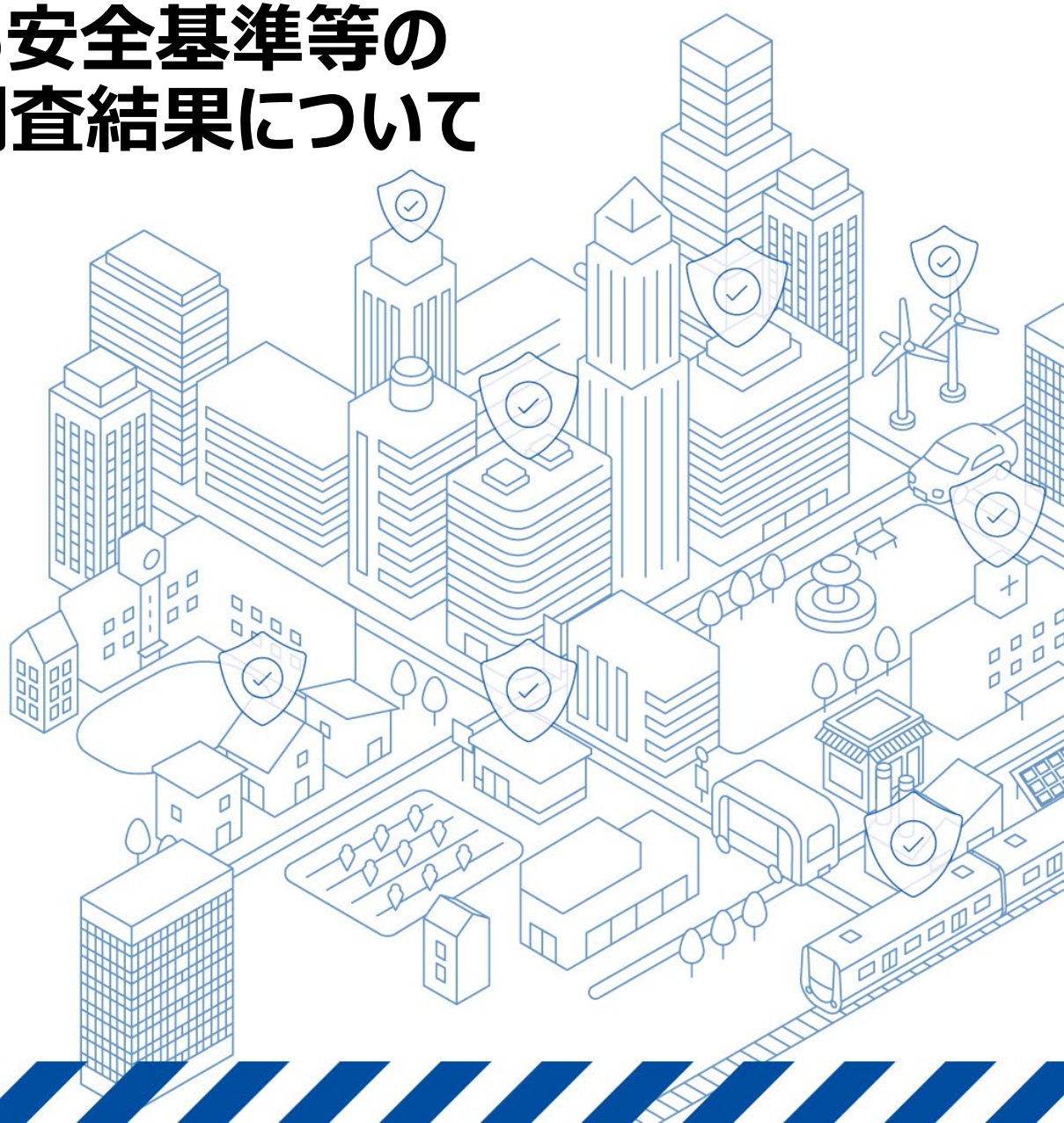
設問59.【自由記述】
サイバーセキュリティに係る取組全体を通して苦慮している点及び要望があれば自由に記載してください。

回答記載件数：248件
（1社で複数回答は別々に集計）

内容	件数
人材不足（専任者の欠如、知識を持つ人材の不足、育成の困難さ、採用の難しさ）	107 件
予算不足（対策費用が高い、財政措置が不十分、コストと効果のバランスが不明確）	55 件
知識・意識不足(職員・従業員のセキュリティ意識が低い、セキュリティ教育に課題がある）	36 件
基準・指針の不明確さ（どこまで対策すべきかの判断が困難、基準の曖昧さ、ガイドラインの複雑化）	13 件
技術的な課題（技術的な対応に課題がある）	12 件
組織的な課題（経営者層の理解の不足、組織内での優先度の低さ、担当部署の不在）	12 件
情報収集の困難さ（最新情報の追随が困難、他組織の事例が不明）	5 件
業務との両立の難しさ（利便性との両立が困難)	4 件
外部への依存（海外事業者への依存、ベンダーへの依存）	4 件

■主な内容（一部抜粋）
・サイバーセキュリティ人材の確保、育成に苦慮している
・セキュリティ機器の導入、運用（保守費用等）に多額の費用が必要である
・サイバーセキュリティ対策について、世の中に数多のサービスがあるため、自社の規模に適した対策がどこまでかということが分かりづらい

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について（別冊）［2025年度］



令和８年７月
内閣官房 国家サイバー統括室
制度総括班

2025年度調査設問の構成（設問一覧）

□ 組織統治

設問1　組織方針とサイバーセキュリティ
設問2　サイバーセキュリティ方針への記載事項
設問3　安全基準等の把握
設問4　責任・権限の割当
設問5　役職・担当者の設置
設問6　予算の配分
設問7　監査の実施
設問8　サイバーセキュリティ評価の実施
設問9　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10　外部環境・内部環境の整理
設問11　任務保証を踏まえた自組織の特性把握
設問12　リスクアセスメントの実施
設問13　リスクアセスメント結果の活用先
設問14　制御システムセキュリティの参考文書
設問15　セキュリティ対策検討の際の取組
設問16　実施しているサプライチェーンリスク軽減策
設問17　コンティンジェンシープランの策定
設問18　事業継続計画の策定
設問19~23　セキュリティ人材の体制
設問24･25　人材育成・意識啓発
設問26　リスク対応計画の実施状況
設問27　情報共有や意見交換を行っている関係主体
設問28　活用している情報提供元
設問29･30　演習・訓練

□ 組織的対策

設問31　資産・情報・データ等の管理
設問32　マルウェアからの保護
設問33　バックアップ
設問34　ログ管理
設問35　運用ソフトウェアの管理
設問36　脆弱性管理
設問37　システムの取得・開発及び保守
設問38　インシデント管理
設問39　私物端末の業務利用（BYOD）管理
設問40　システムの監視

□ 人的対策

設問41　人的資源及び外部委託

□ 物理的対策

設問42　物理的及び環境的セキュリティ

□ 技術的対策

設問43　アカウント管理
設問44　アクセス制御
設問45　暗号
設問46　通信のセキュリティ
設問47　メールのセキュリティ

□ 制御システム

設問48　制御システムに関する取り組み

設問49　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

設問50　クラウドサービス利用に関する運用対策
設問51　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

□ セキュリティ・バイデザイン

設問54･55　セキュリティ・バイデザインに関する取組み

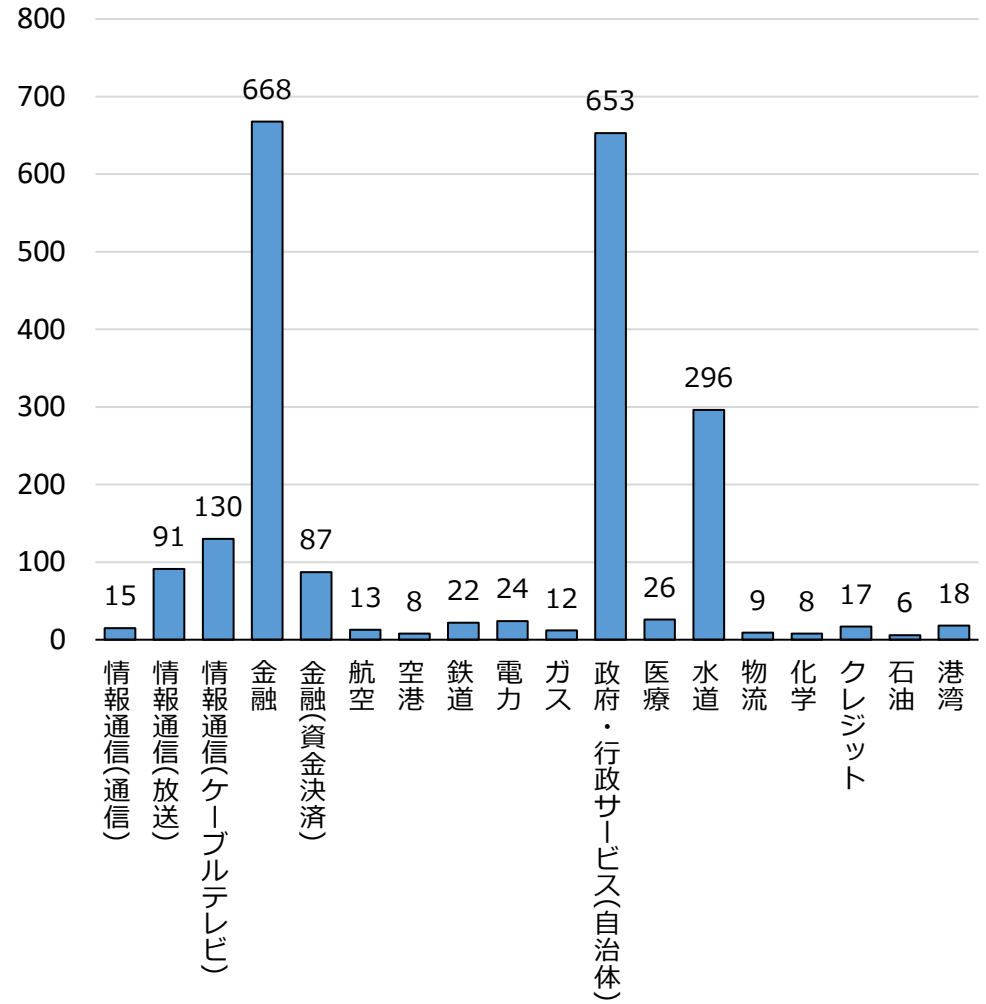
□ その他

設問56~57　サイバーセキュリティに係る取組み全体を通した課題・要望等

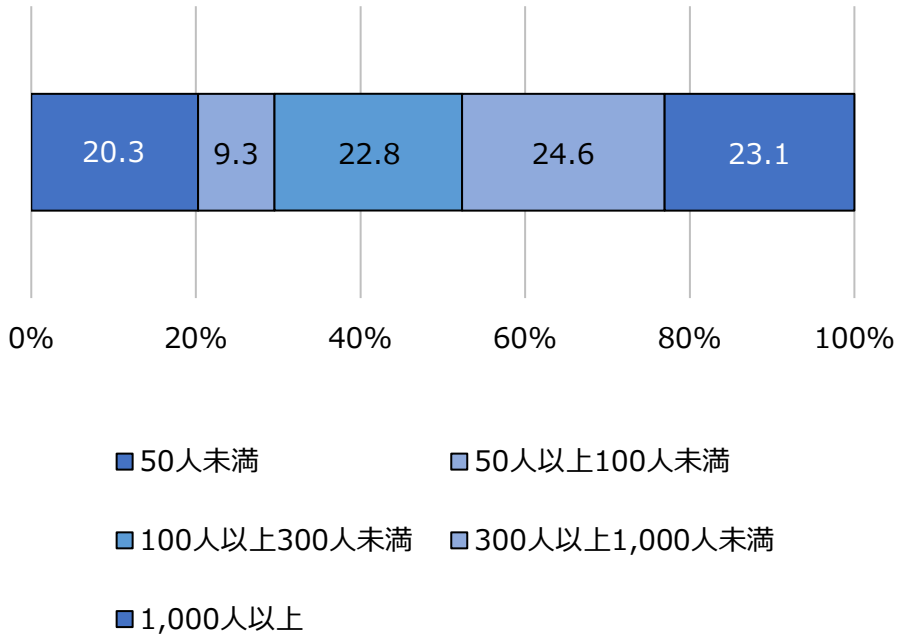
※設問番号の欠番は基礎情報（分野名、従業員数）及び、
各設問に付記した自由記述による回答

アンケート調査結果

Ⅰ.【単一回答】
貴社（又は貴団体）が属する重要インフラ分野（回答の件数）

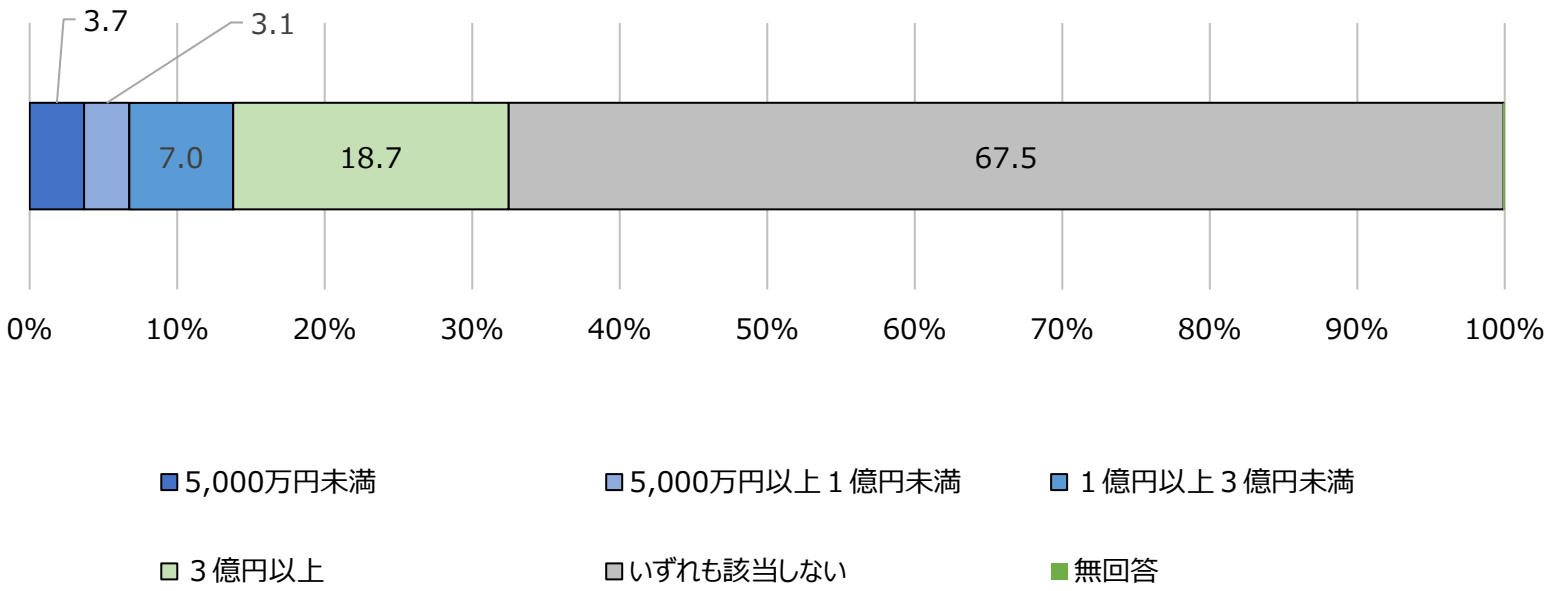


Ⅰ.【単一回答】
貴社（又は貴団体）の従業員数



アンケート調査結果

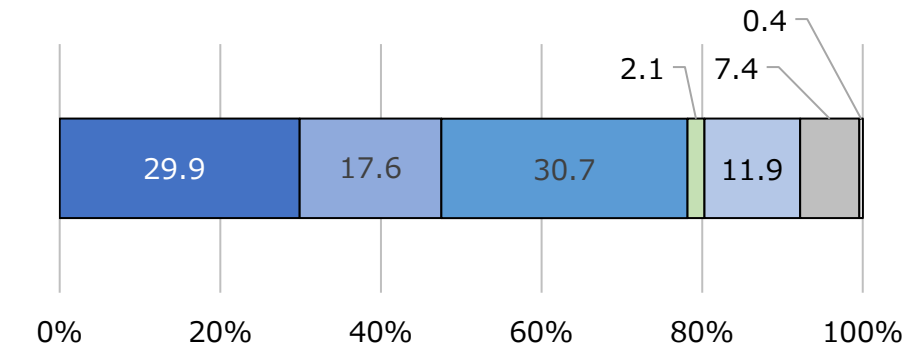
Ⅰ.【単一回答】
貴社の資本金
（※地方公共団体の場合は、５：いずれも該当しないを選択）



アンケート調査結果

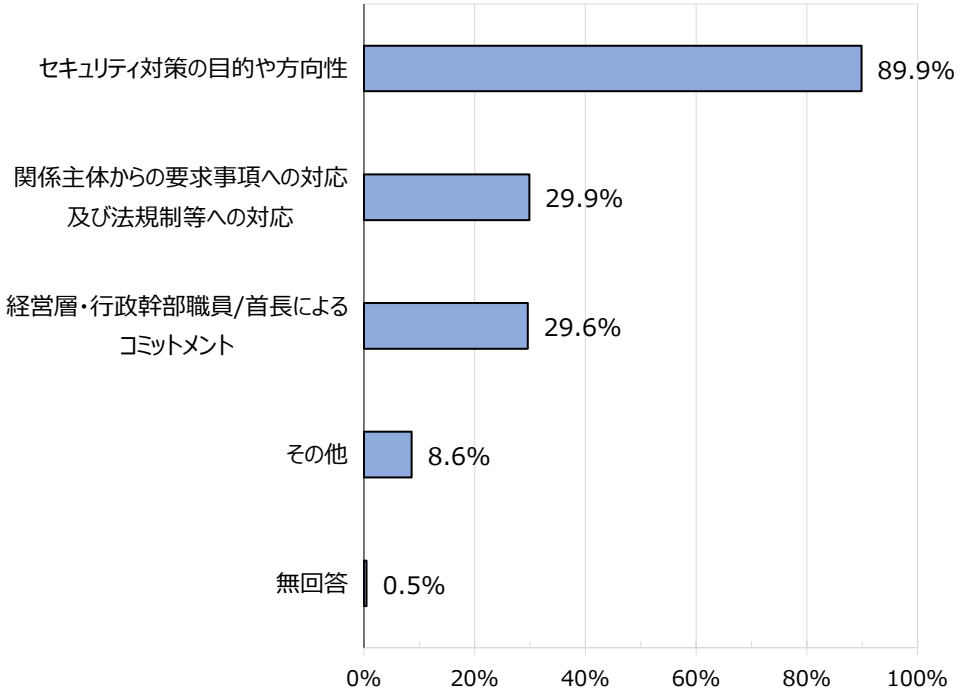
設問１．【単一回答】
組織方針（経営方針、行政運営方針、リスクマネジメント方針等）にあたる文書に、重要インフラのサイバーセキュリティ確保に関する事項（※）を組み入れていますか。
また、維持するサービス範囲・水準を示していますか。

※ 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２．【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全て選択してください。

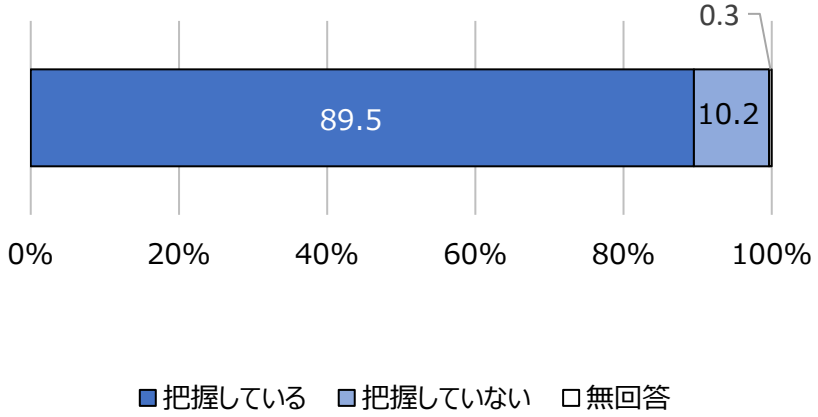


■「その他」（一部抜粋）
・対象とする脅威、職員の遵守義務、組織体制、情報セキュリティ対策、監査等
・情報セキュリティの管理方針を定めている。具体的には、CEOやCISOの役割や報告、委員会の設置、教育等を定義している。
・情報資産の保護、情報システム、システムリスク管理体制、全社員の参加と義務、外部委託等々の項目に関する事項
・サイバーセキュリティ方針は未整備

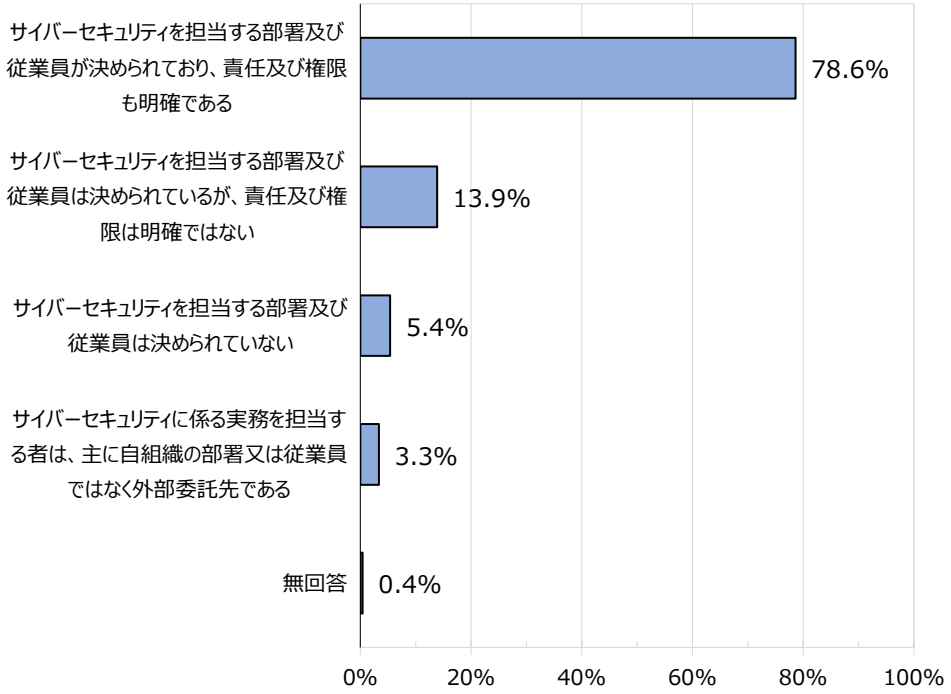
アンケート調査結果

設問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。

※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

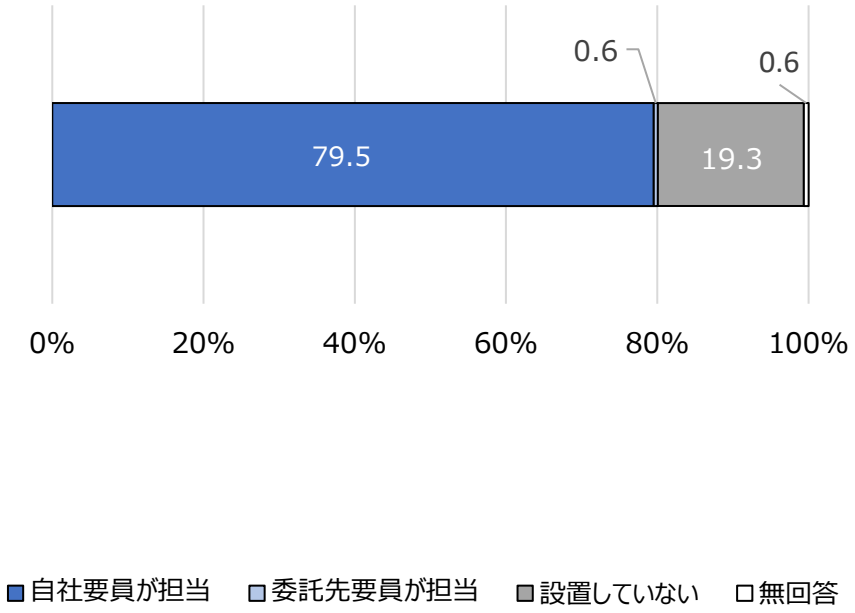


設問４．【複数回答】
自組織のサイバーセキュリティを担当する部署及び従業員を決定するとともに責任及び権限を割り当てていますか。全て選択してください。

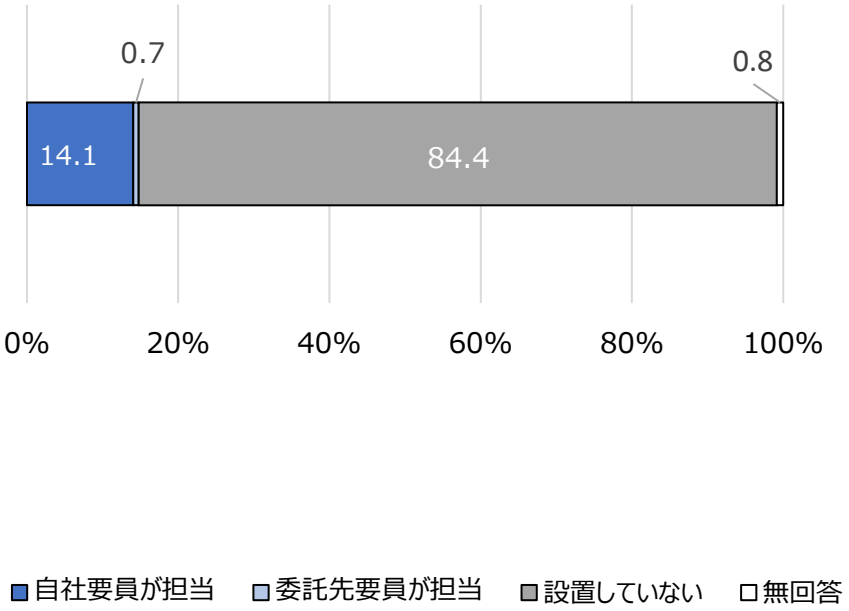


アンケート調査結果

設問５．【単一回答】
[１．経営層（取締役・執行役員）・行政幹部職員に相当するCISO（最高情報セキュリティ責任者）について]
自組織で設置しているものを全て選択してください。
専任者だけでなく、兼務で担当を割り当てている場合も含みます。

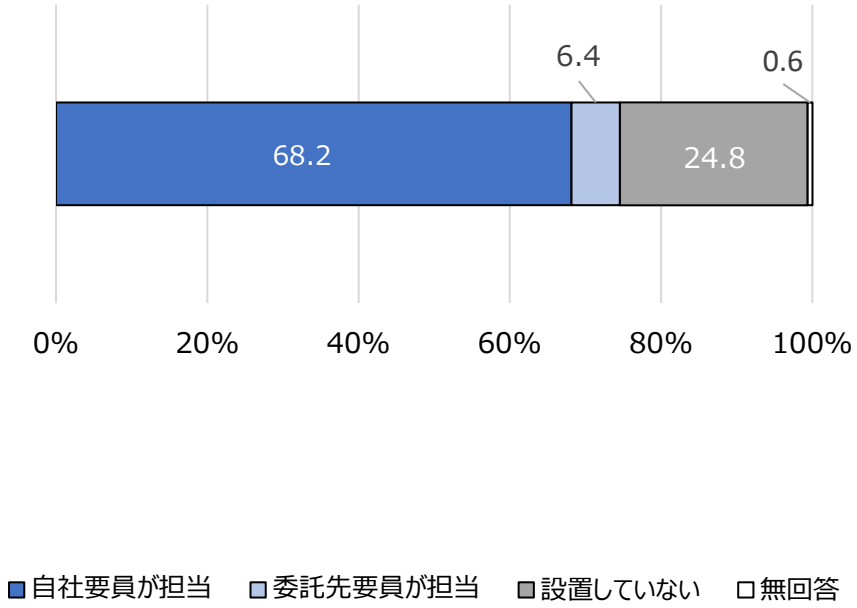


設問５．【単一回答】
[２．経営層（取締役・執行役員）・行政幹部職員に相当しないCISO（最高情報セキュリティ責任者）について]
自組織で設置しているものを全て選択してください。
専任者だけでなく、兼務で担当を割り当てている場合も含みます。

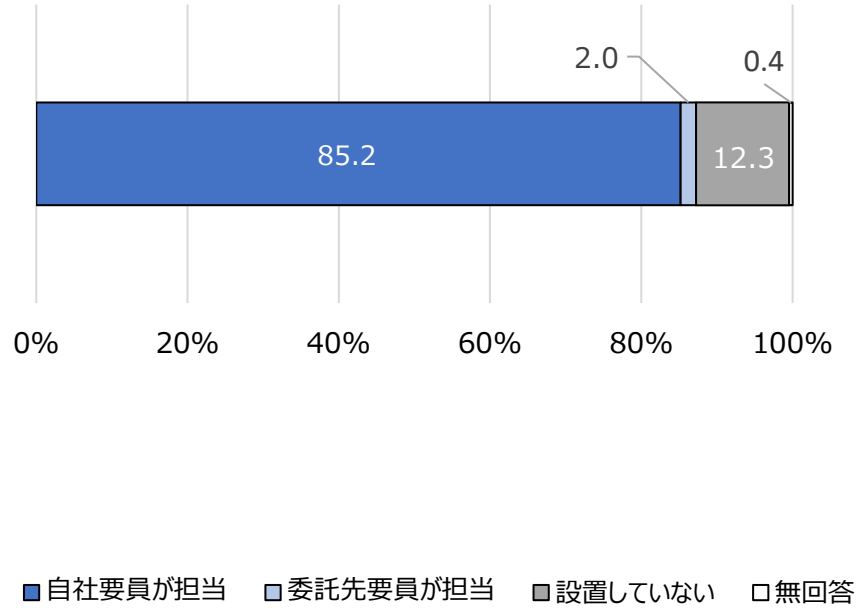


アンケート調査結果

設問５．【単一回答】
[３．脅威情報収集・情報共有担当について]
自組織で設置しているものを全て選択してください。
専任者だけでなく、兼務で担当を割り当てている場合も含みます。

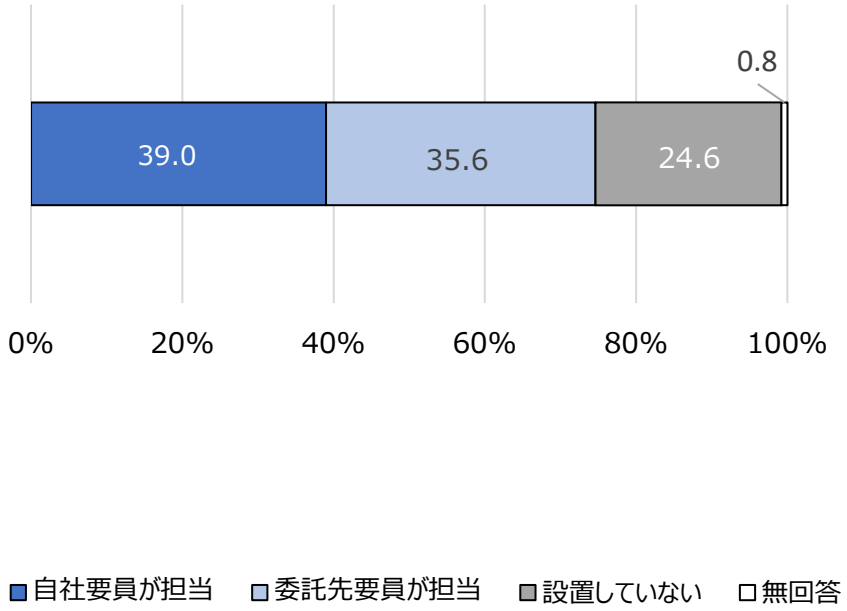


設問５．【単一回答】
[４．セキュリティインシデント管理担当（CSIRT等）について]
自組織で設置しているものを全て選択してください。
専任者だけでなく、兼務で担当を割り当てている場合も含みます。
（※金融分野を含む）

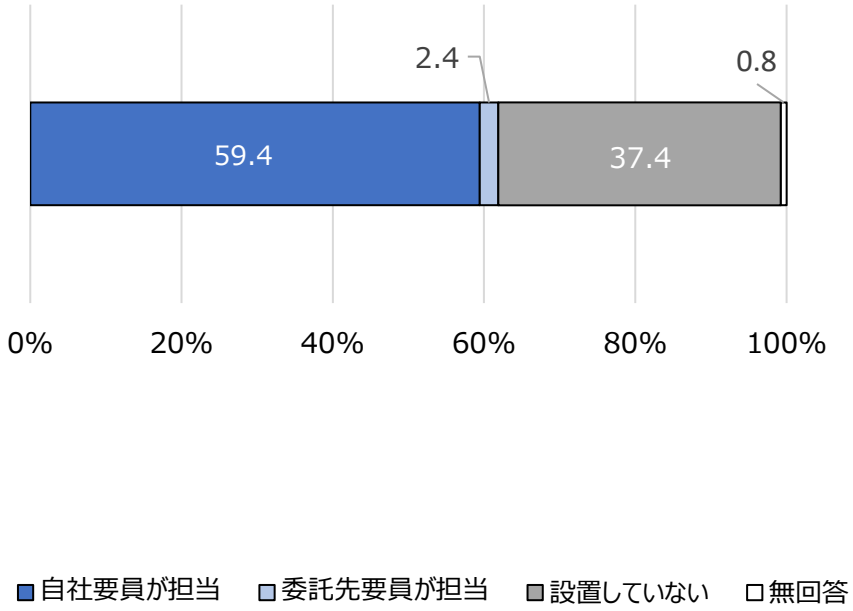


アンケート調査結果

設問５．【単一回答】
[５．システムやネットワークの監視及びセキュリティイベントの検出・分析担当（SOC等）について]
自組織で設置しているものを全て選択してください。
専任者だけでなく、兼務で担当を割り当てている場合も含みます。

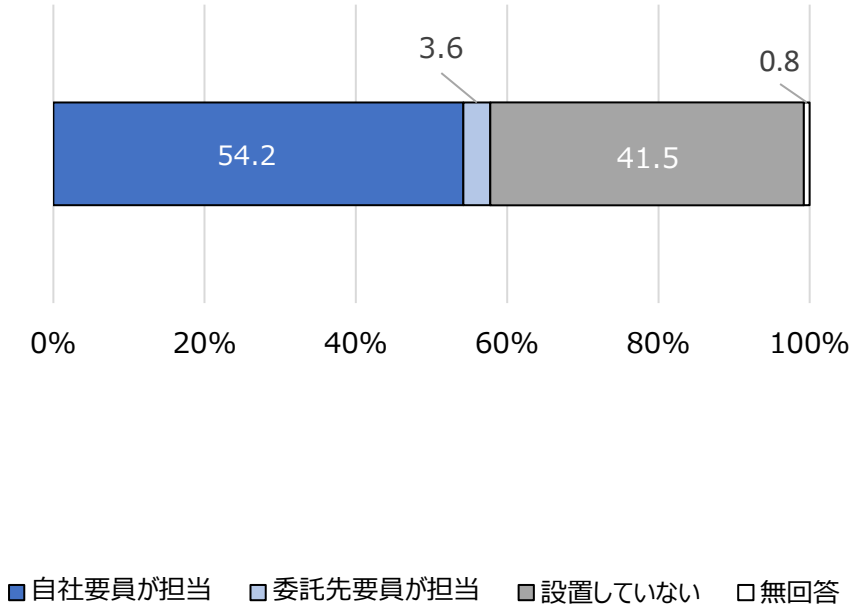


設問５．【単一回答】
[６．コンティンジェンシープラン／事業継続計画（サイバーセキュリティを含むもの）の実行担当について]
自組織で設置しているものを全て選択してください。
専任者だけでなく、兼務で担当を割り当てている場合も含みます。

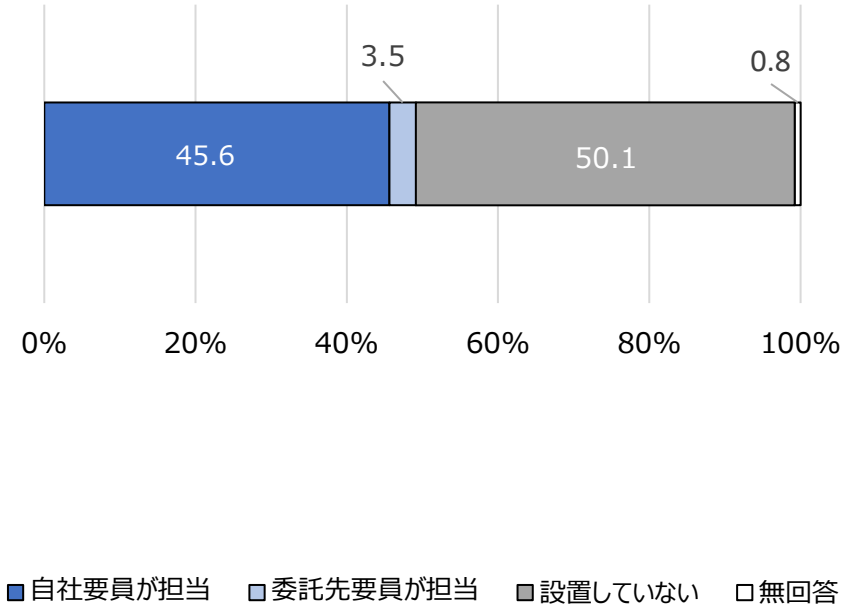


アンケート調査結果

設問５．【単一回答】
[７．サイバーセキュリティに係る内部監査担当について]
自組織で設置しているものを全て選択してください。
専任者だけでなく、兼務で担当を割り当てている場合も含みます。

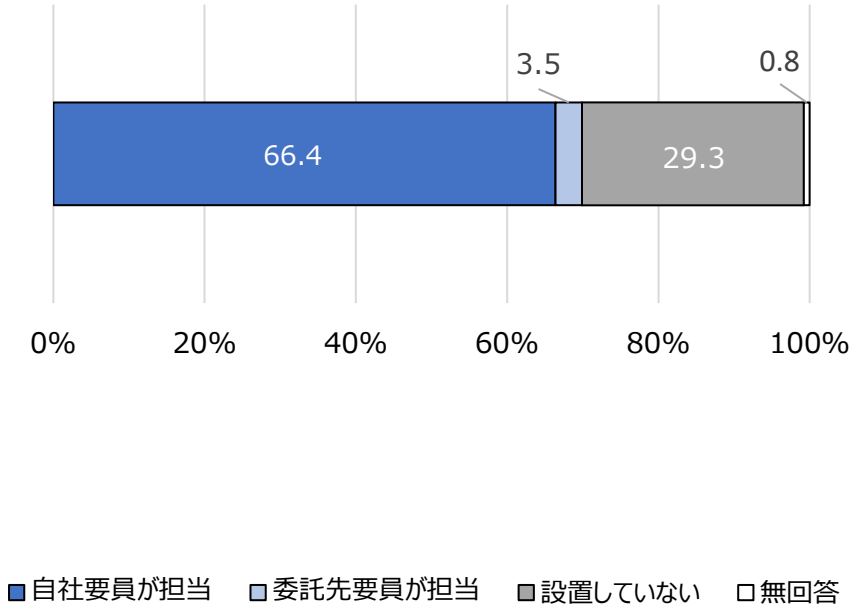


設問５．【単一回答】
[８．サプライチェーン（サプライヤー、委託先等）に対するセキュリティ管理担当について]
自組織で設置しているものを全て選択してください。
専任者だけでなく、兼務で担当を割り当てている場合も含みます。

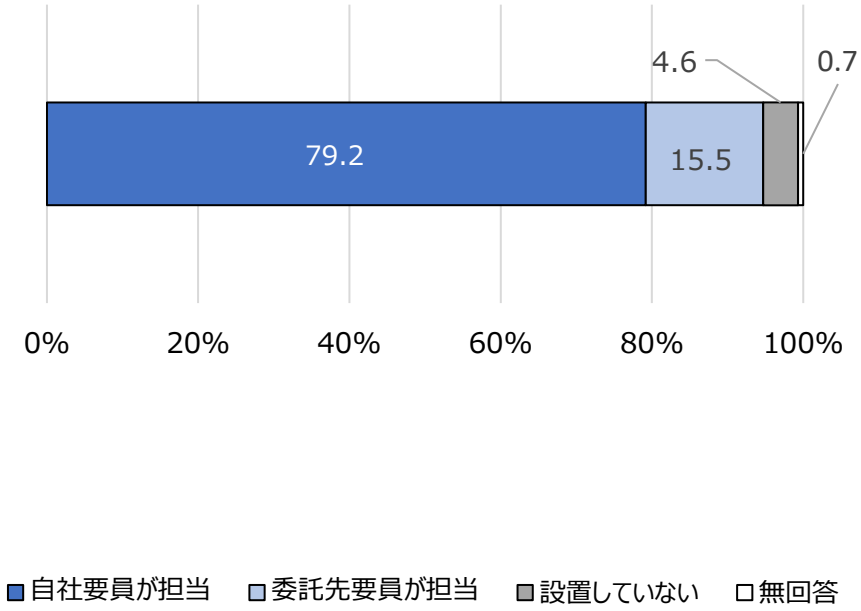


アンケート調査結果

設問５．【単一回答】
[９．セキュリティ人材に関する教育・研修担当について]
自組織で設置しているものを全て選択してください。
専任者だけでなく、兼務で担当を割り当てている場合も含みます。

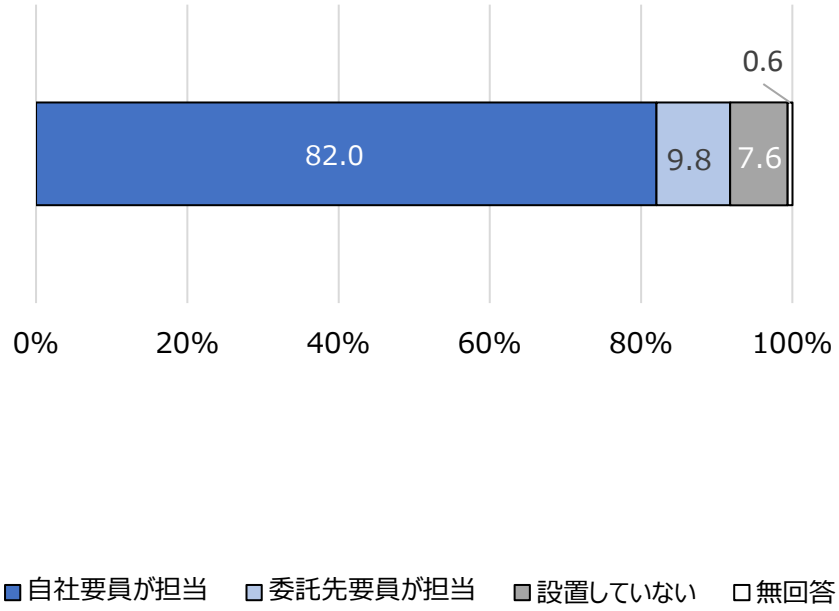


設問５．【単一回答】
[10．情報システム（ネットワークを含む）の運用担当について]
自組織で設置しているものを全て選択してください。
専任者だけでなく、兼務で担当を割り当てている場合も含みます。

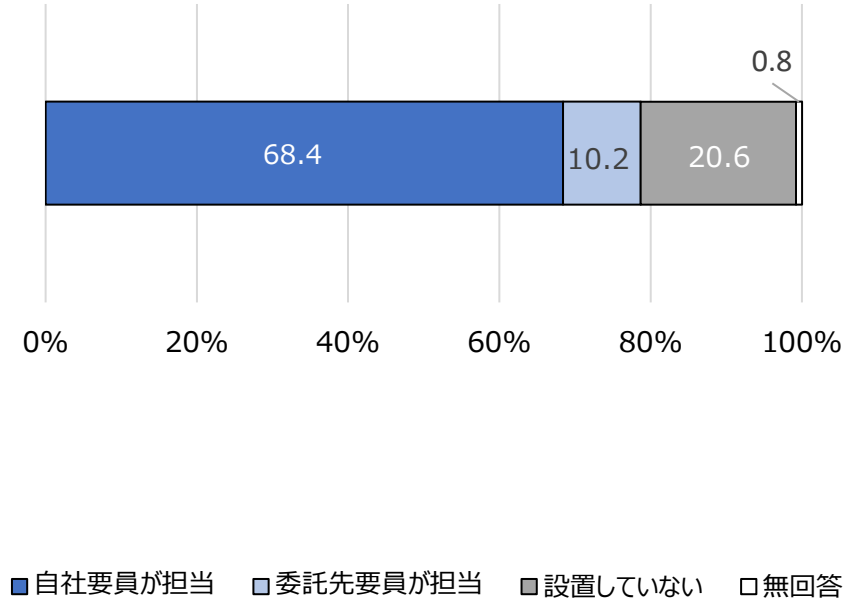


アンケート調査結果

設問５．【単一回答】
[11．資産（ハードウェア、ソフトウェア、データ等）の管理担当について]
自組織で設置しているものを全て選択してください。
専任者だけでなく、兼務で担当を割り当てている場合も含みます。

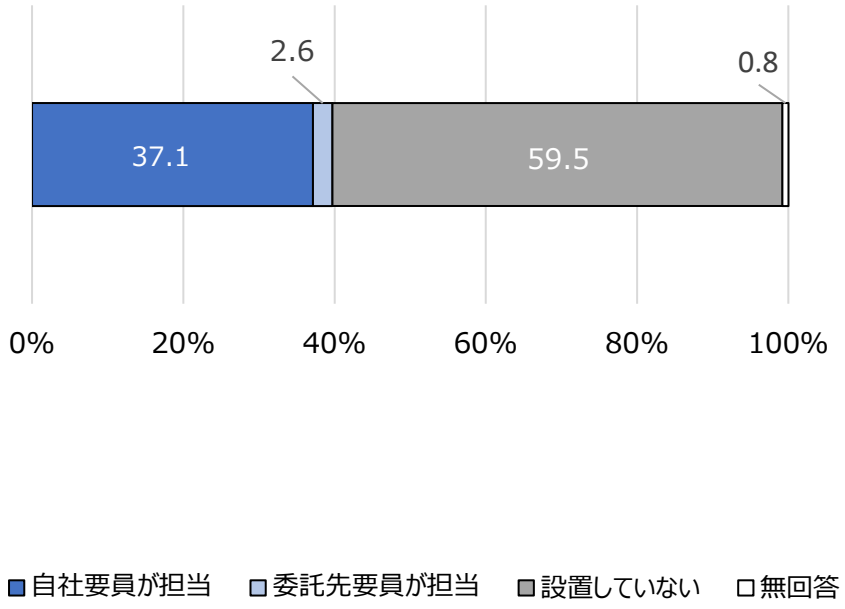


設問５．【単一回答】
[12．物理的・環境的セキュリティが要求される施設の管理担当について]
自組織で設置しているものを全て選択してください。
専任者だけでなく、兼務で担当を割り当てている場合も含みます。

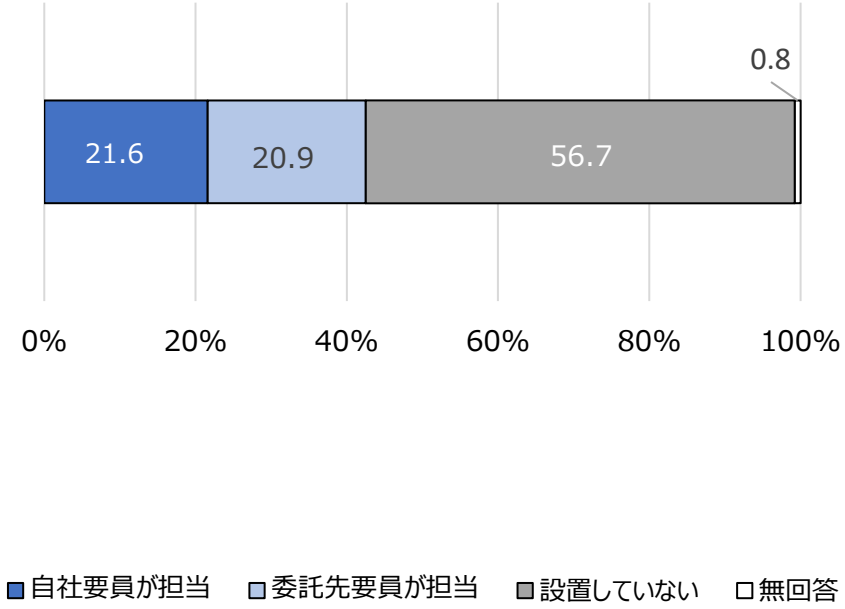


アンケート調査結果

設問５．【単一回答】
[13．サイバーセキュリティに係る法務担当について]
自組織で設置しているものを全て選択してください。
専任者だけでなく、兼務で担当を割り当てている場合も含みます。

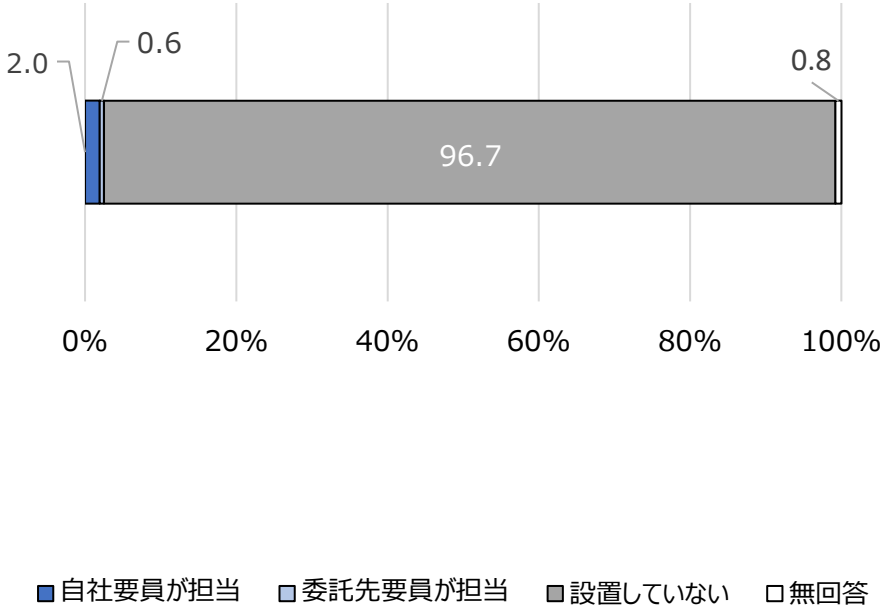


設問５．【単一回答】
[14．セキュリティを考慮したシステム開発担当について]
自組織で設置しているものを全て選択してください。
専任者だけでなく、兼務で担当を割り当てている場合も含みます。



アンケート調査結果

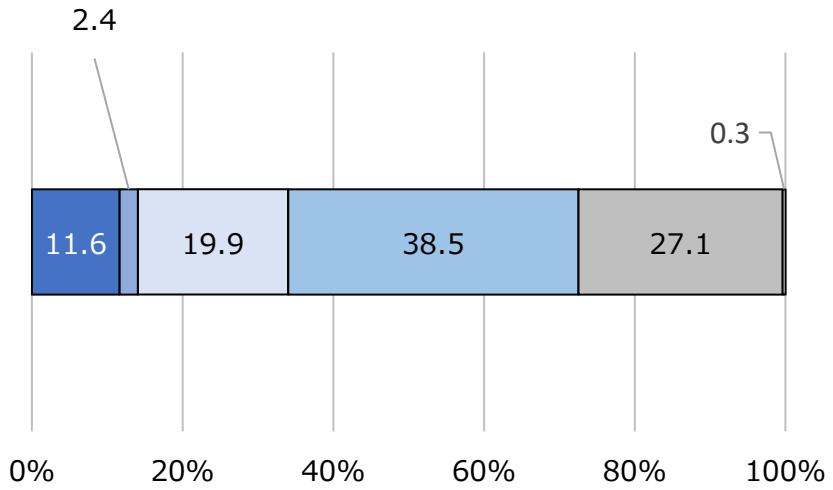
設問５．【単一回答】
[15．その他について]
自組織で設置しているものを全て選択してください。
専任者だけでなく、兼務で担当を割り当てている場合も含みます。



■「その他」（一部抜粋）
・自社内でセキュリティ委員会を設置し総合的に対応
・サイバー事故発生時のフォレンジック業務を外部委託
・部門、部署ごとの情報セキュリティ責任者

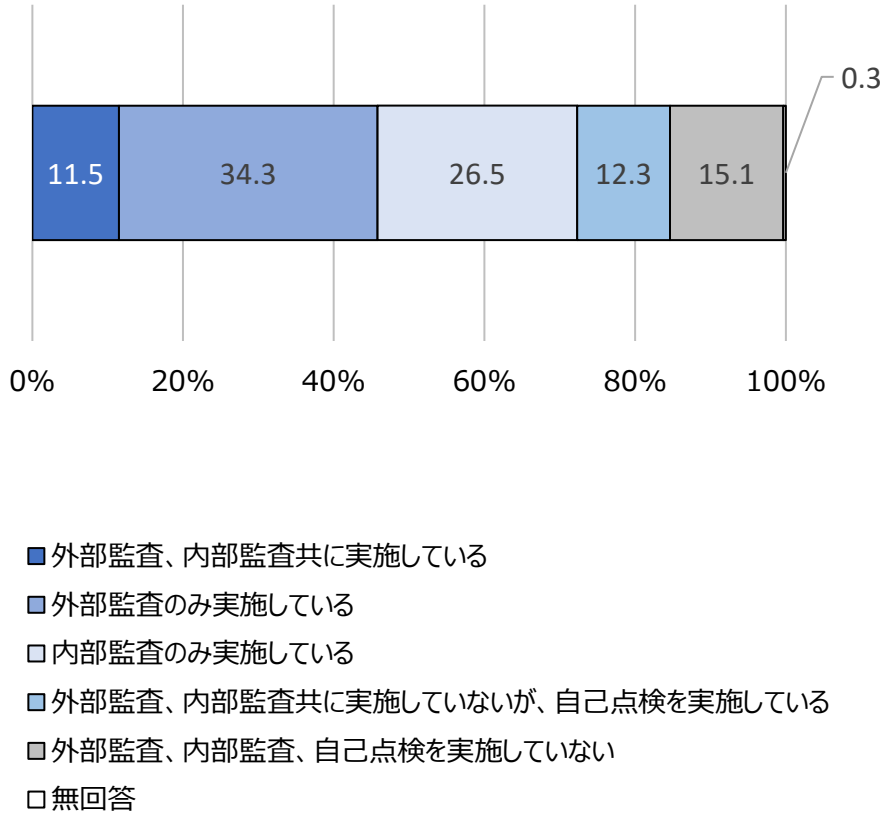
アンケート調査結果

設問６．【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。



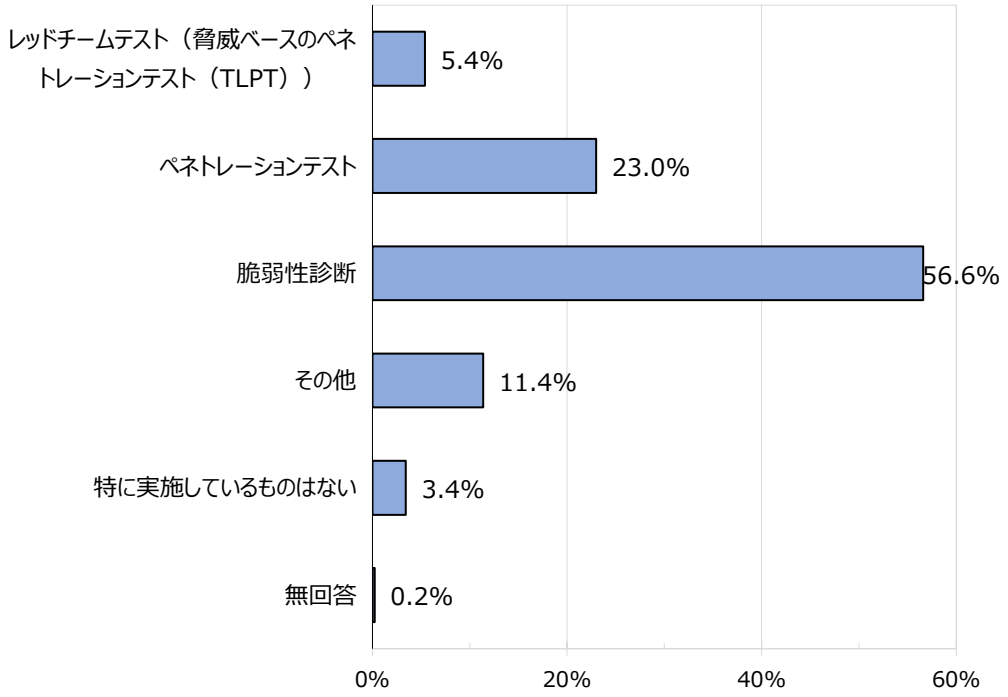
設問７．【単一回答】
自組織のサイバーセキュリティ確保の取組について、監査（※）を実施していますか。
（※金融分野を含む）

※セキュリティ目標達成状況や、計画の進捗のほか、ガバナンスプロセス、リスクマネジメントの遂行状況等について客観的な評価を実施すること



アンケート調査結果

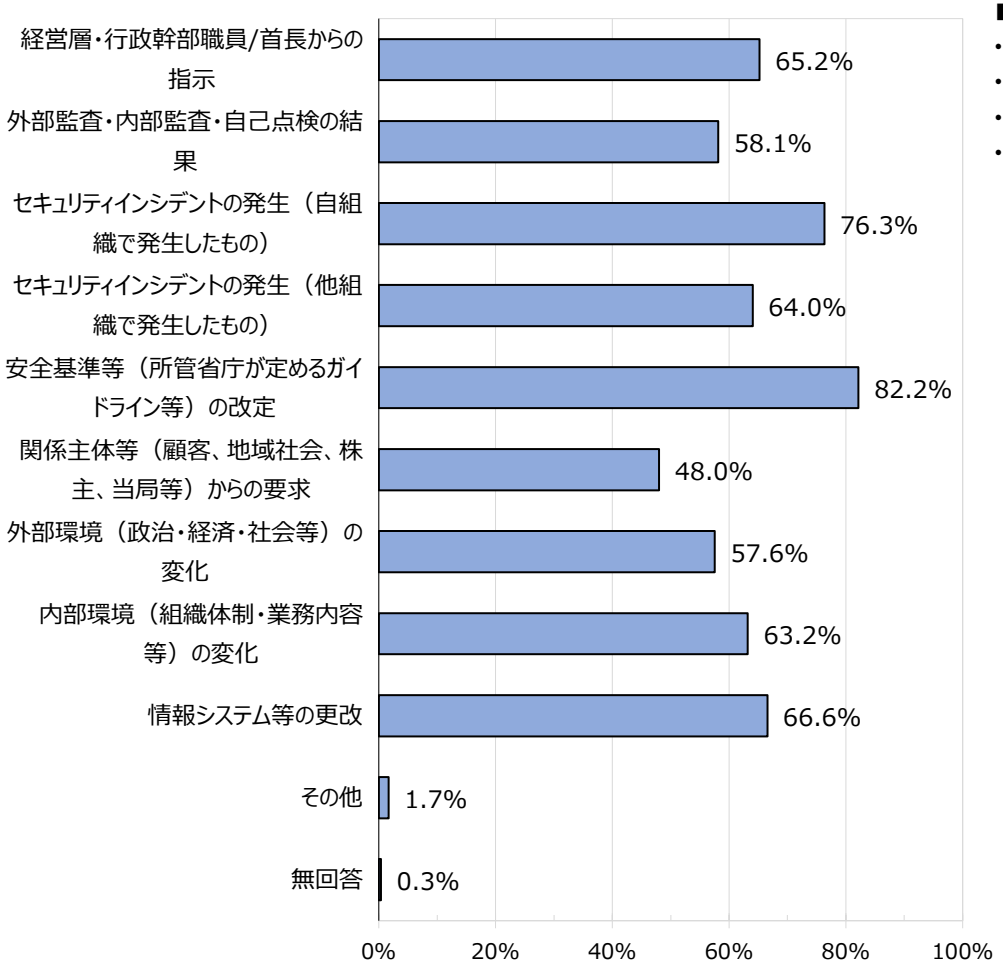
設問８．【複数回答】
自組織にて実施しているセキュリティ評価を全て選択してください。
（※金融分野を含む）



■「その他」（一部抜粋）
・標的型メール訓練
・セキュリティ外部監査
・内部監査を実施している
・自組織で作成したチェックシートに対する達成度評価を実施
・サイバー攻撃対象領域調査（ASM）
・現地調査やヒアリングによる物理的対策、人的対策及び技術・運用における対策の確認
・ISMSのグローバル基準をもとにしたリスクアセスメント
・社外の第三者によるセキュリティ評価の実施(NIST CSF2.0ベース)及び、制御システムのセキュリティリスクアセスメント(IPAガイドベース)の実施
・情報セキュリティ管理基準に基づき、各システム所管部署へアンケート（予備調査・現地調査）

アンケート調査結果

設問９．【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。

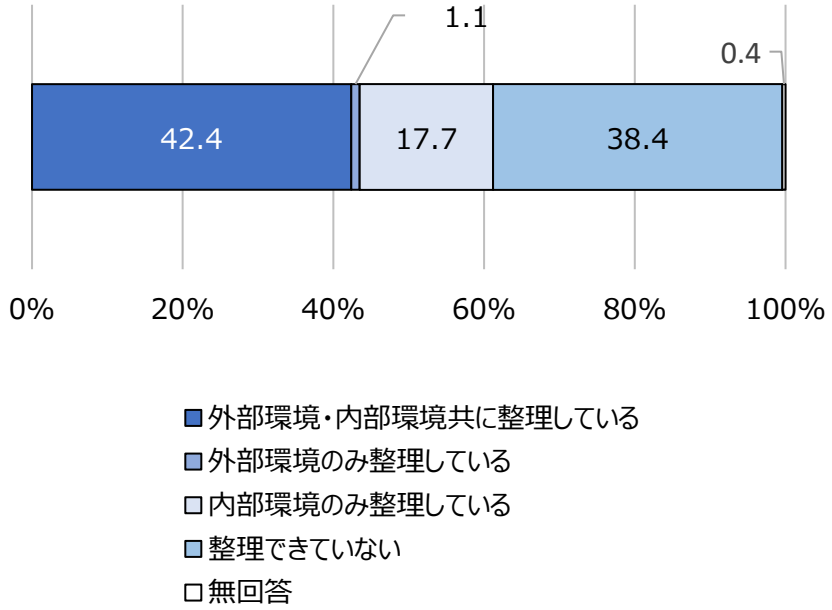


■「その他」（一部抜粋）
・外部・内部要因に関わらず、継続的に見直しを行っている
・経営計画やIT戦略、サイバーセキュリティ戦略の策定
・セキュリティベンダーからの情報
・組織の再編

アンケート調査結果

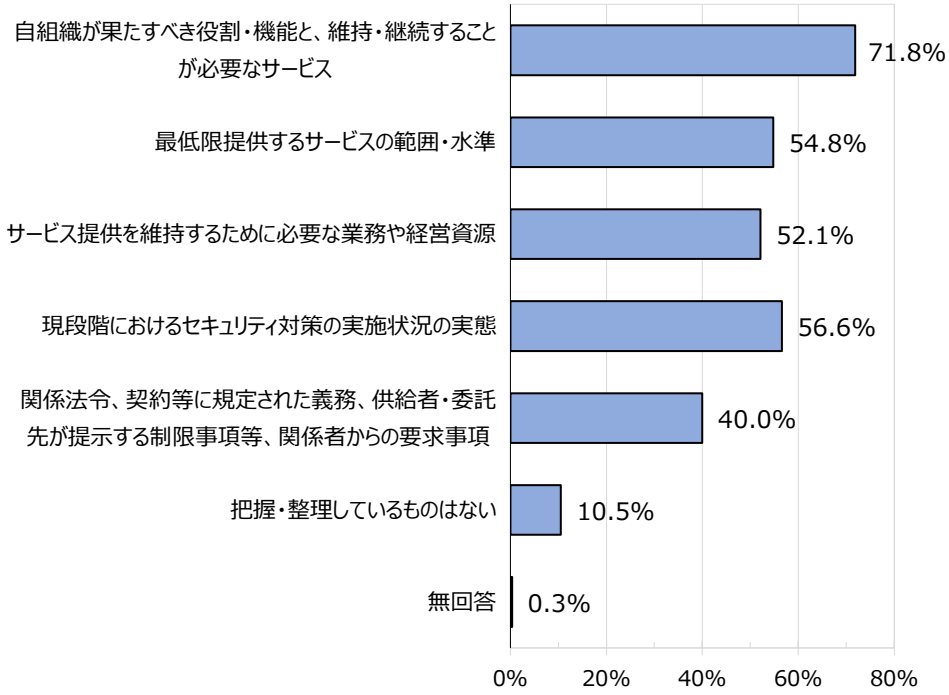
設問10.【単一回答】
自組織の重要インフラサービスに関する外部環境（※1）及び内部環境（※2）について、近い将来の状況も含めて整理していますか。

※1 外部環境：国内、国際、地方を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然及び競争の環境
※2 内部環境：統治、組織体制、役割、方針、目的を達成するために策定された戦略、情報システム、情報の流れや意志決定プロセス、内外のステークホルダ



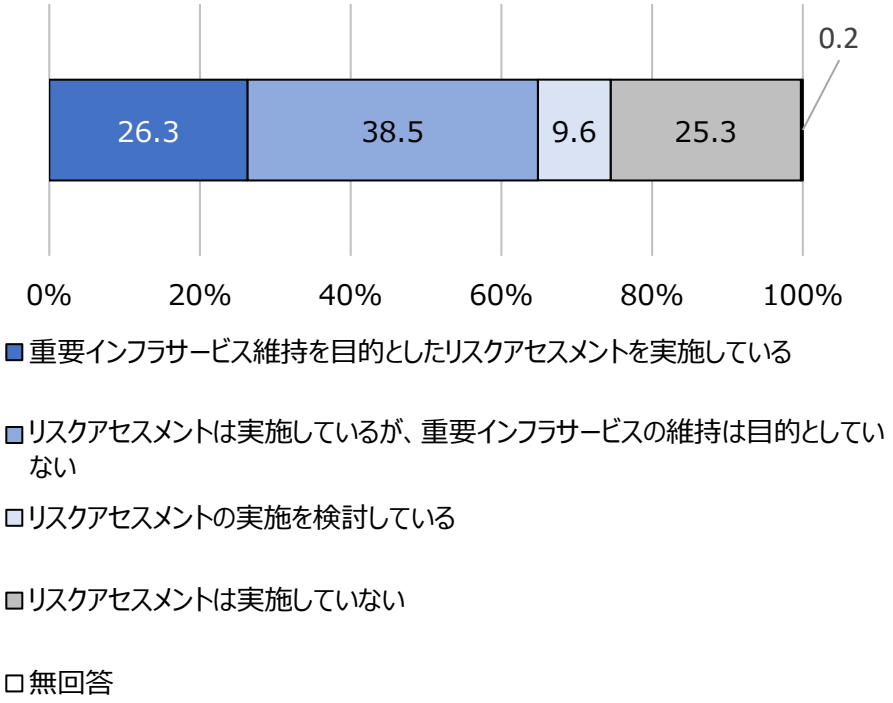
設問11.【複数回答】
任務保証（※）の観点から、以下の自組織の特性について整理し、把握しているものを全て選択してください。

※「企業、重要インフラ事業者や政府機関に代表されるあらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、係る「任務」を着実に遂行するために必要となる能力及び資産を確保すること。サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供に関する責任を全うするという考え方。」

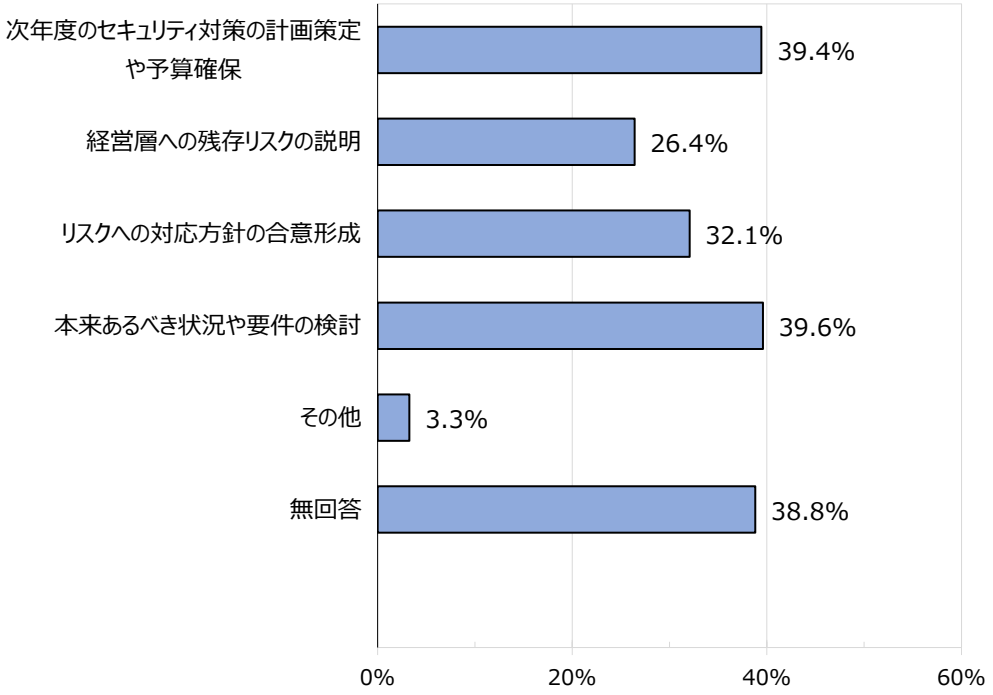


アンケート調査結果

設問12.【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。
（※金融分野を含む）



設問13.【複数回答】
リスクアセスメントの結果の活用先を全て選択してください。

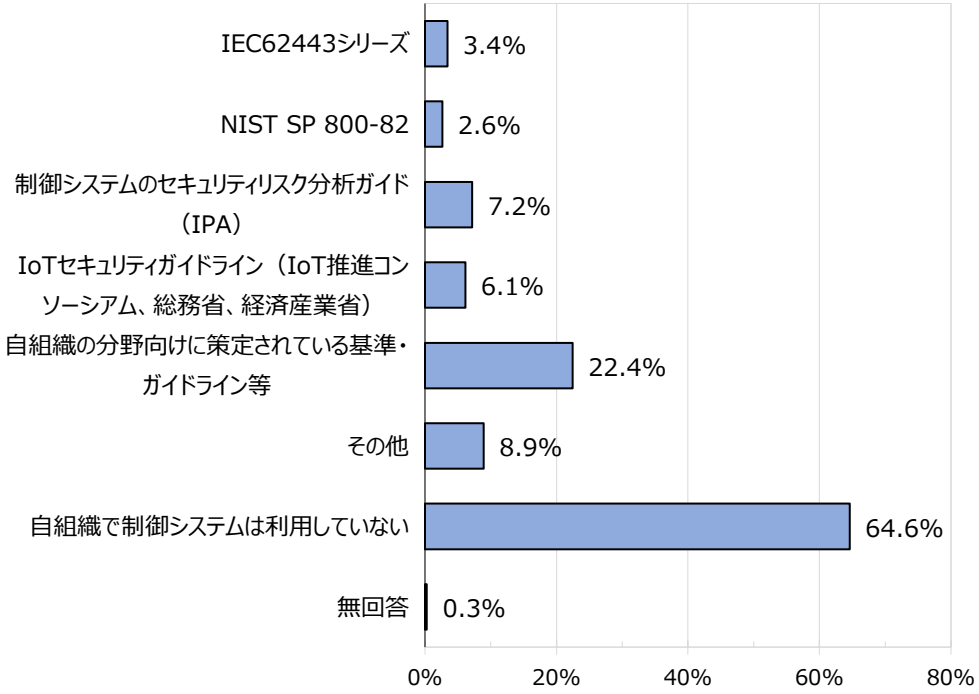


■「その他」（一部抜粋）
・研修
・事例の共有
・緊急度に応じた開発、対応時期とその方式の策定
・次期リプレース時のシステム構成やセキュリティ対策の見直しに活用している

アンケート調査結果

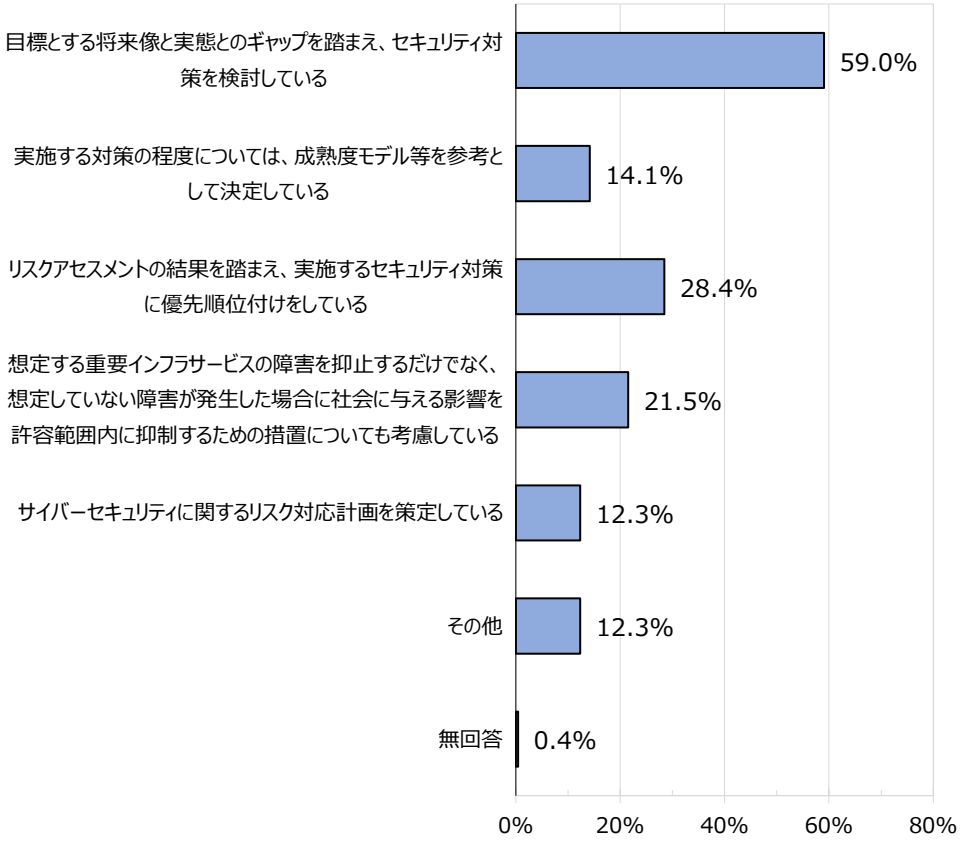
設問14.【複数回答】
制御システム（※）のセキュリティ確保に当たって参考としているものを全て選択してください。

※工場や電力、プラント等の設備で活用される、他の機器やシステムを管理、制御するためのシステム（DCS、PLC等）
※監視カメラや生体認証等は含みません。



■「その他」（一部抜粋）
・ISO/IEC 27001
・SOC2 Type 2, PCI DSS 及びNISTのような業界ベストプラクティス
・製品ベンダー等からの情報提供
・NIST CSF2.0

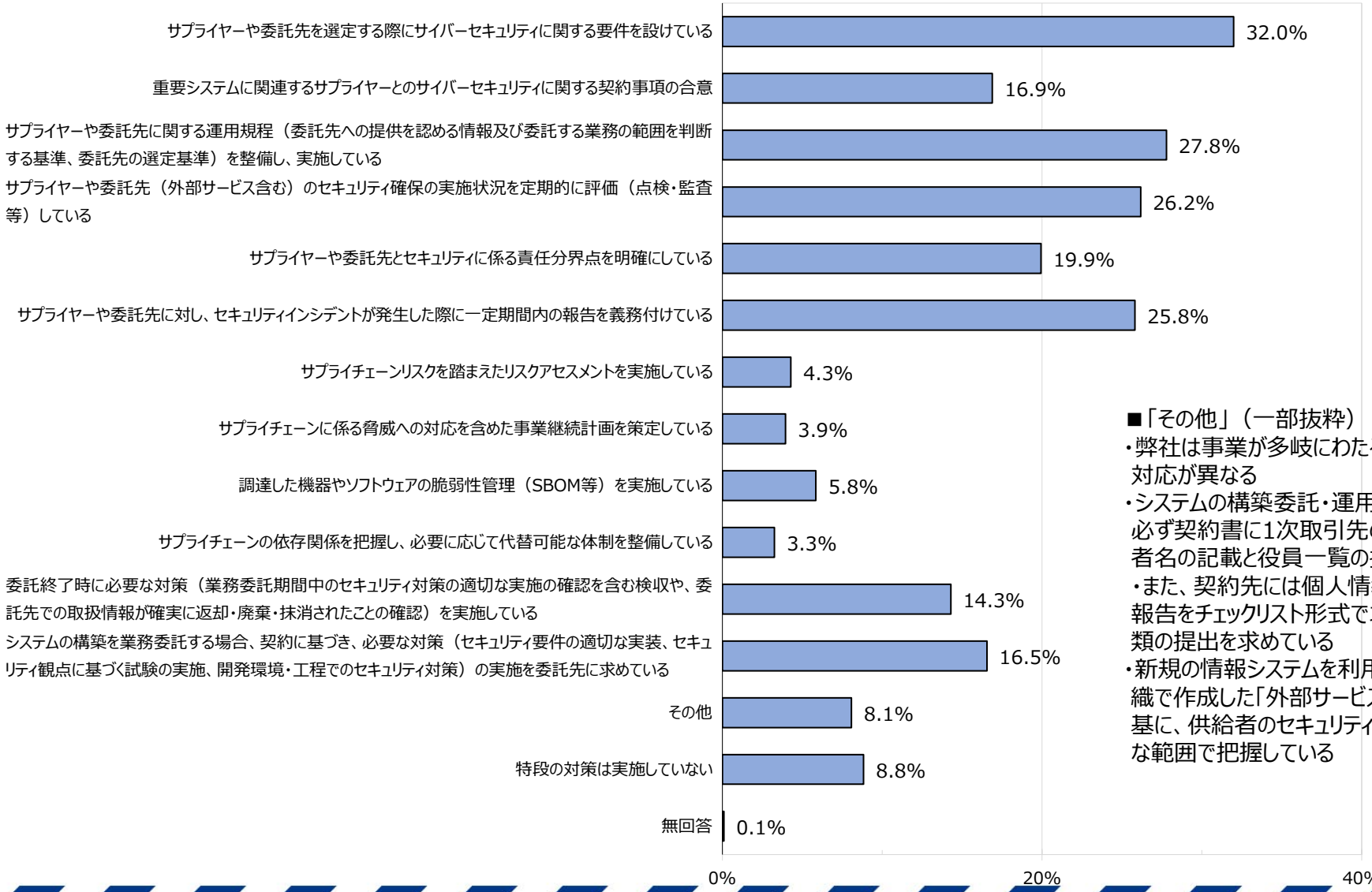
設問15.【複数回答】
セキュリティ対策の検討にあたり、自組織の対応状況を全て選択してください。



■「その他」（一部抜粋）
・委託ベンダーに任せきりになっている
・対応が必要となった場合に都度対応
・起こりうる可能性が高い事案が確認された場合に対策を検討する

アンケート調査結果

設問16.【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。**（※金融分野を含む）**

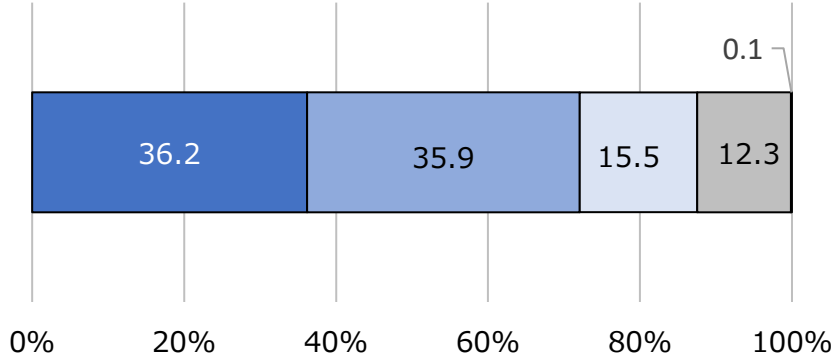


■「その他」（一部抜粋）
・弊社は事業が多岐にわたるため、事業により対応が異なる
・システムの構築委託・運用委託をする場合、必ず契約書に1次取引先の社名及び代表者名の記載と役員一覧の提出を求めている
・また、契約先には個人情報の取扱いに関する報告をチェックリスト形式で求めるとともに、規程類の提出を求めている
・新規の情報システムを利用する場合は、自組織で作成した「外部サービス選定チェック表」を基に、供給者のセキュリティ対策の状況を可能な範囲で把握している

アンケート調査結果

設問17.【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。（事業継続計画の中に初動対応に関する方針・手順・態勢等が含まれていれば「策定している」とします。）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。**（※金融分野を含む）**

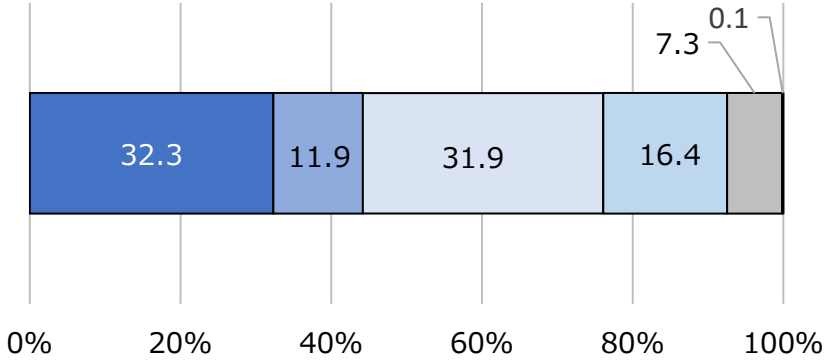
※重要インフラ事業者等が重要インフラサービス障害の発生又はそのおそれがあることを認識した後に経営層・行政幹部職員/首長や職員等が行うべき初動対応(緊急時対応)に関する方針、手順、態勢等をあらかじめ定めたもの。



- 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
- 無回答

設問18.【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（※1）を策定していますか。また、事業復旧計画（※2）を策定していますか。
（※金融分野を含む）

※1 重要インフラ事業者等が重要インフラサービス障害により影響を受けた重要インフラサービスを許容可能な時間内に許容可能な水準(目標復旧水準)まで復旧させることを目的として、その復旧に向けた目標水準、優先順位その他の方針、手順、態勢等をあらかじめ定めたもの。
※2 目標復旧水準から、平時のサービス水準まで完全復旧させることを目的としたもの。



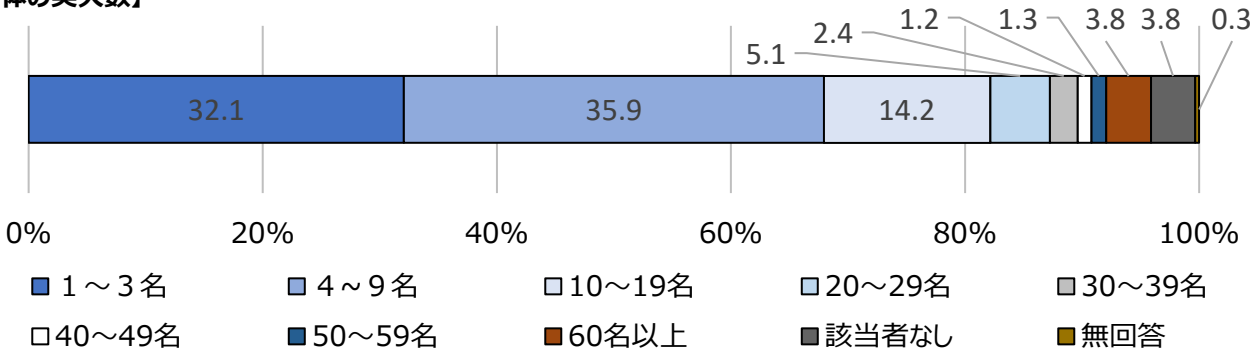
- 事業継続計画及び事業復旧計画を策定している
- 事業継続計画は策定しており、事業復旧計画を策定中である
- 事業継続計画は策定しているが、事業復旧計画は策定していない
- 事業継続計画の策定を検討している、もしくは作成中である
- 事業継続計画を策定する予定はない
- 無回答

アンケート調査結果

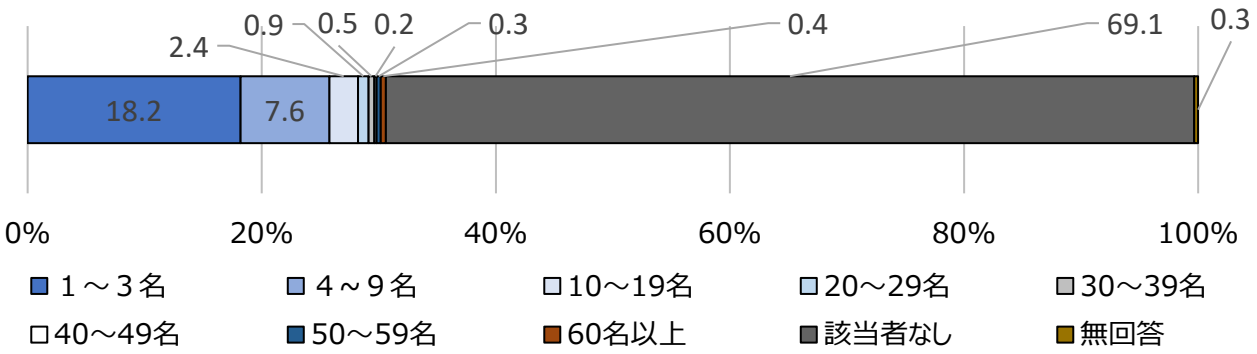
設問19.【単一回答】
本調査時点において、以下に示す「セキュリティ業務」の従事者について、全体の実人数（重複を計上せず）と、そのうちセキュリティ専任者（いる場合）の実人数を全て選択してください。なお、外部委託する業務の人数は含まず、内製化する業務従事者のみを対象としてください。また、総数の5%程度の誤差が含まれていても構いません。

（セキュリティ業務）
- 経営層（取締役・執行役員）・行政幹部職員に相当するCISO（最高情報セキュリティ責任者）
- 経営層（取締役・執行役員）・行政幹部職員に相当しないCISO（最高情報セキュリティ責任者）
- 脅威情報収集・情報共有担当
- セキュリティインシデント管理担当（CSIRT等）
- システムやネットワークの監視及びセキュリティイベントの検出・分析担当（SOC等）
- コンティンジェンシープラン／事業継続計画（サイバーセキュリティを含むもの）の実行担当
- サイバーセキュリティに係る内部監査担当
- サプライチェーン（サプライヤー、委託先等）に対するセキュリティ管理担当
- セキュリティに関する教育・研修担当
- 情報システム（ネットワークを含む）の運用担当
- 資産（ハードウェア、ソフトウェア、データ等）の管理担当
- 物理的・環境的セキュリティが要求される施設の管理担当
- サイバーセキュリティに係る法務担当
- セキュリティを考慮したシステム開発担当
- その他

【全体の実人数】

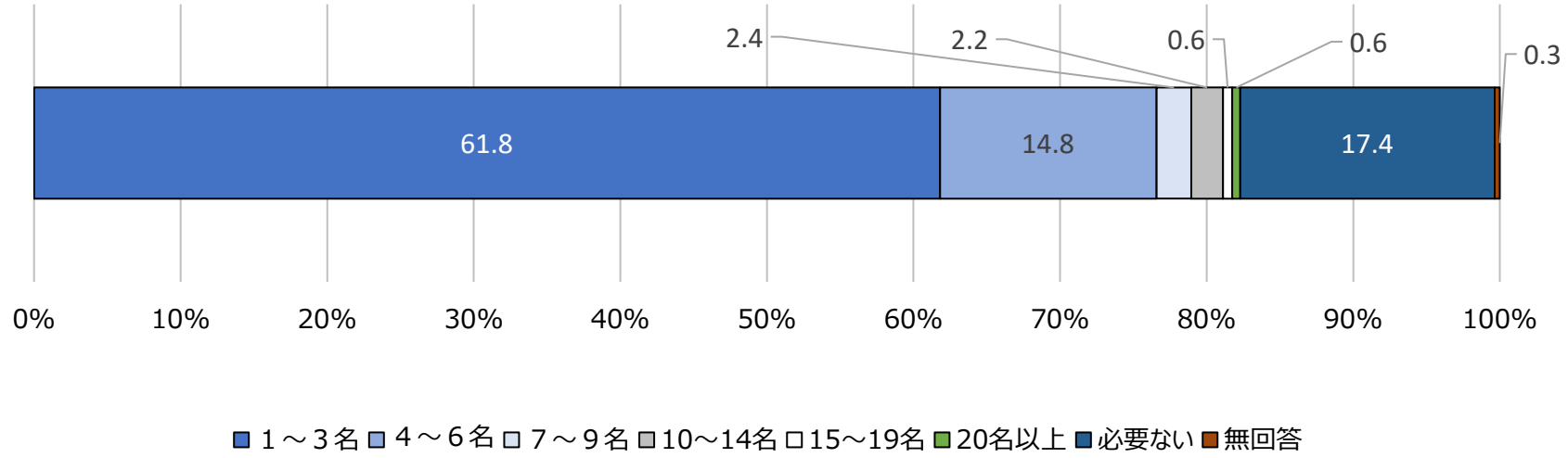


【うち専任者数】



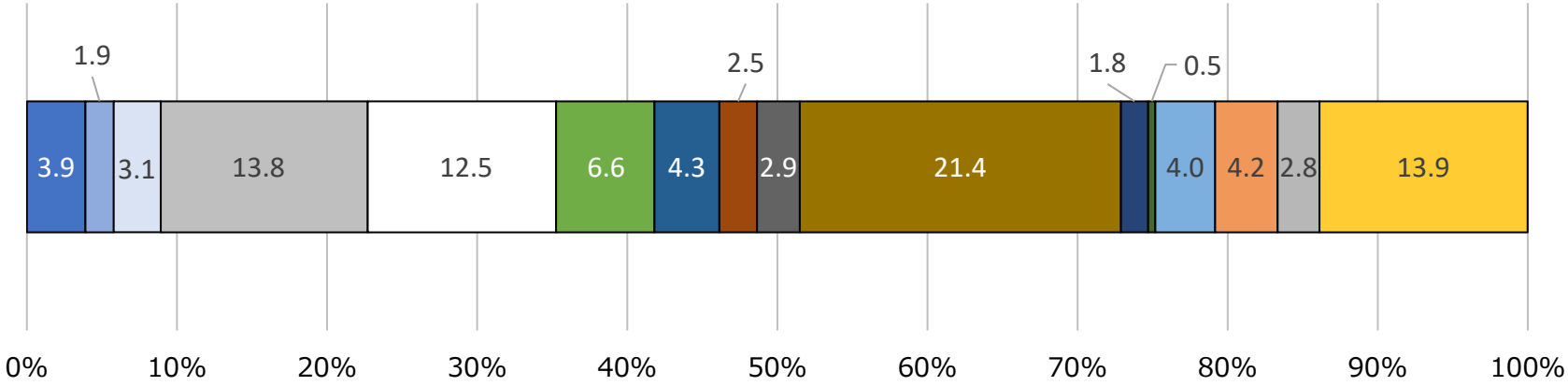
アンケート調査結果

設問20.【単一回答】
（設問19に関連）現在の体制を踏まえ、追加で必要と考える人数（外部委託の人数は含まず、自組織で確保すべき従業員に限定）を選択してください。



アンケート調査結果

設問21.【単一回答】
（設問20に関連）人材不足が最も深刻と感じる人材のタイプを１つだけ選択してください。

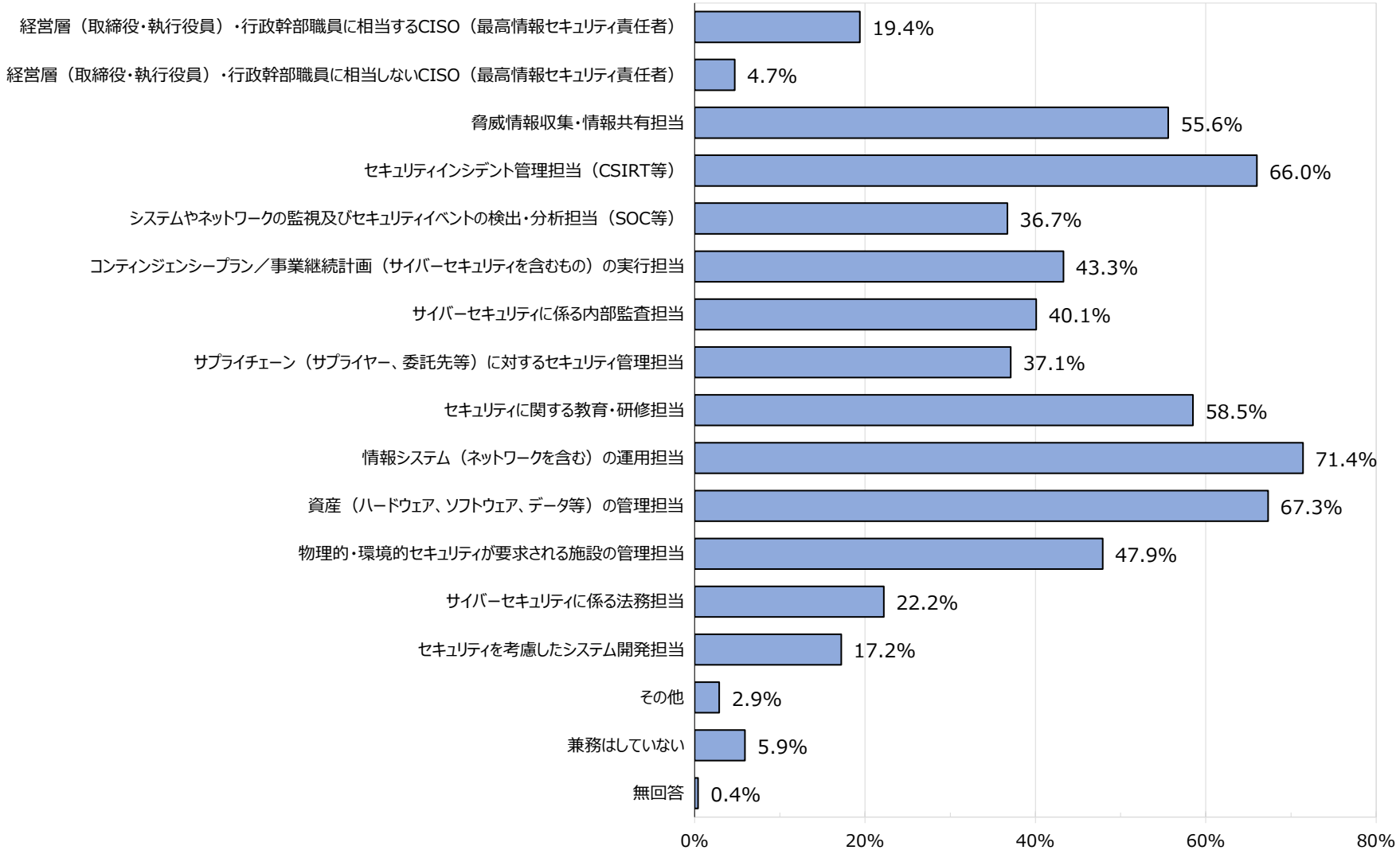


- 経営層（取締役・執行役員）・行政幹部職員に相当するCISO（最高情報セキュリティ責任者）
- 経営層（取締役・執行役員）・行政幹部職員に相当しないCISO（最高情報セキュリティ責任者）
- 脅威情報収集・情報共有担当
- セキュリティインシデント管理担当（CSIRT等）
- システムやネットワークの監視及びセキュリティイベントの検出・分析担当（SOC等）
- コンティンジェンシープラン／事業継続計画（サイバーセキュリティを含むもの）の実行担当
- サイバーセキュリティに係る内部監査担当
- サプライチェーン（サプライヤー、委託先等）に対するセキュリティ管理担当
- セキュリティに関する教育・研修担当
- 情報システム（ネットワークを含む）の運用担当
- 資産（ハードウェア、ソフトウェア、データ等）の管理担当
- 物理的・環境的セキュリティが要求される施設の管理担当
- サイバーセキュリティに係る法務担当
- セキュリティを考慮したシステム開発担当
- その他
- 無回答

■「その他」（一部抜粋）
・すべてのタイプにおいて、その役割に必要な能力や知識を持つ人材が不足している
・少人数の体制のため、特定の担当者ではなくオールラウンドプレーヤーが必要となっている
・少人数の組織であるため、技能を全て兼ね備える人材が必要
・特定の領域に限らず、セキュリティ全般を管理および推進していく役割
・情報セキュリティポリシーの策定・見直し担当
・情報セキュリティに関するガバナンスの強化担当

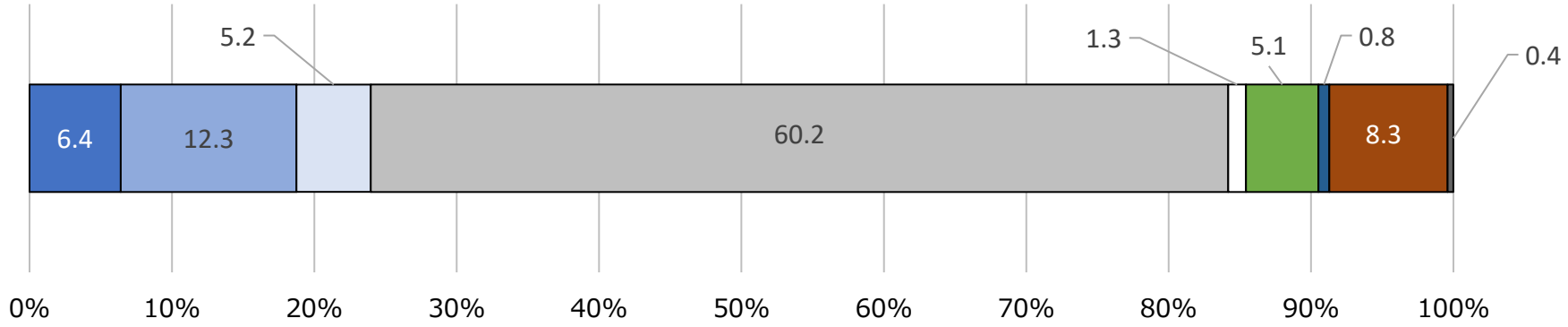
アンケート調査結果

設問22.【複数回答】
（設問５に関連）自社要員が担当と回答したセキュリティ業務（内製化業務）について、1人の従業員又は複数の従業員が兼務して担う場合、兼務しているセキュリティ業務（主たる業務）を全て選択してください。



アンケート調査結果

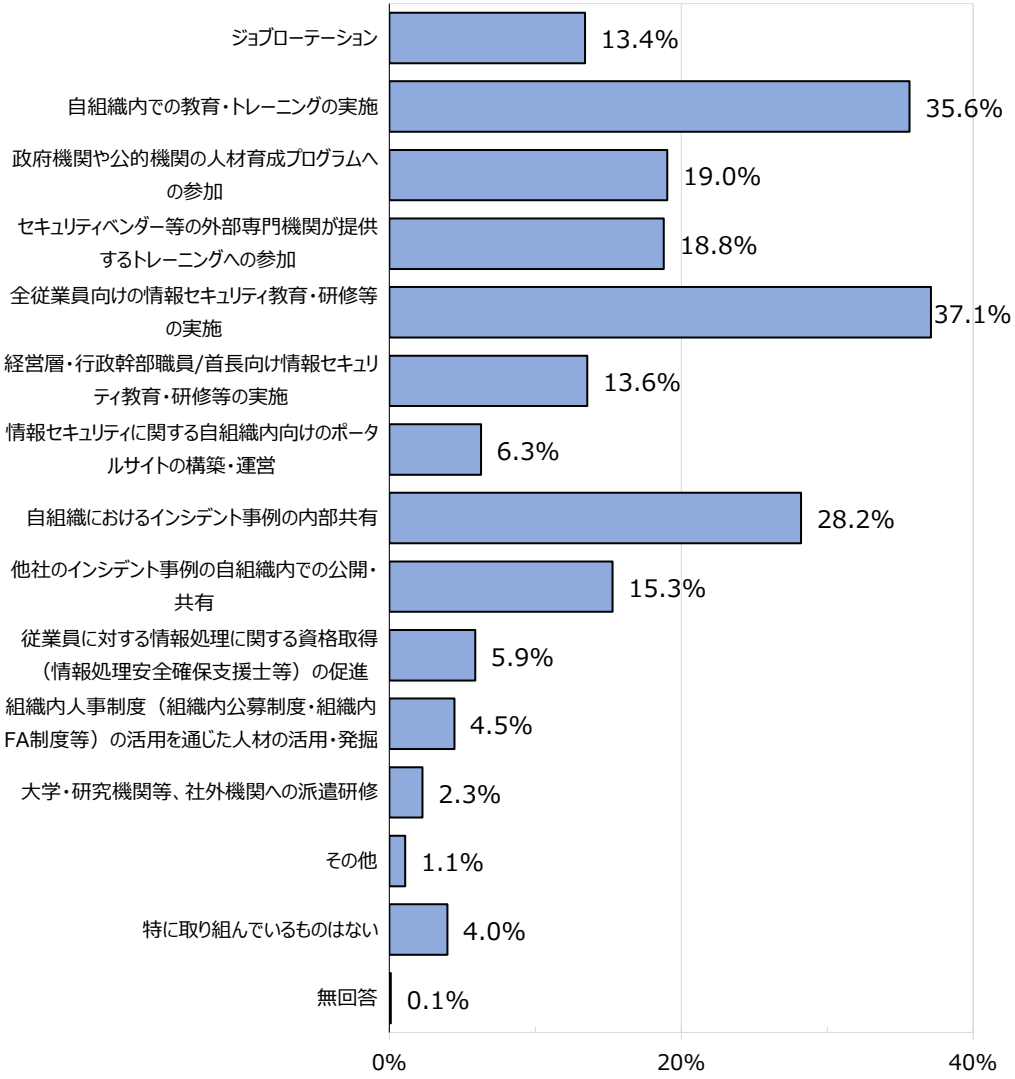
設問23.【単一回答】
（設問19に関連）平時、非セキュリティ業務も兼務する従業員が担当している本来業務について、主たるものを選択してください。



- 組織経営（役員等）
- 組織管理（いわゆるコーポレート部門の業務）
- 情報システムの設計開発、サービス企画開発等
- 情報システムの運用・保守
- 品質管理
- リスクマネジメント、事業継続管理、設備保安
- 監査
- 兼務はしていない
- 無回答

アンケート調査結果

設問24.【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。**（※金融分野を含む）**



■「政府機関や公的機関の人材育成プログラム」の具体的記載（一部抜粋）
・実践的サイバー防御演習（CYDER） [主催：総務省、NICT]
・リモートラーニングによるデジタル人材育成のための基礎研修 [主催：J-LIS]
・インシデント発生時CSIRT対応訓練 [主催：J-LIS]
・全分野一斉演習（旧・分野横断的演習）[主催：NCO]
・中核人材育成プログラム（ICSCoE）[主催：IPA]
・官民共同サイバー攻撃対策技能訓練 [主催：警視庁]
・eラーニングによる情報連携に向けた研修 [主催：総務省]
・サイバーセキュリティ企画演習（CyberSPEX）[主催：IPA]
・制御システム向けサイバーセキュリティ演習（CyberSTIX）[主催：IPA]
・業界別サイバーレジリエンス強化演習（CyberREX）[主催：IPA]
・金融業界横断的なサイバーセキュリティ演習（Delta Wall）[主催：金融庁]
・サイバーインシデント演習（自治体CSIRT向け）[主催：NCO、J-LIS]

■「セキュリティベンダー等の外部専門機関が提供するトレーニング」の具体的記載（一部抜粋）
・ラックセキュリティアカデミー
・キヤノンマーケティングジャパン サイバーセキュリティセミナー
・富士通ラーニングメディア（セキュリティ研修・サイバー攻撃対策基礎講座）
・NTTドコモビジネス主催 ビジネスセミナー（最新のサイバー攻撃の脅威と対策）
・日立アカデミー
・IIJ（攻撃技術理解・防御APT対策基礎コース）
・Microsoft セキュリティ オペレーション アナリスト (SC-200T00)
・SANSトレーニング（CISSP CBK、Certified SOC Analystなど）
・Trend Micro「ランサムウェア対応・防御トレーニング」
・NRIセキュアテクノロジーズ セキュアEggs研修
・JUAS（情報セキュリティマネジメント研修など）
・SmartLearning（NEC）
・Udemy（セキュリティ関連コース）
・PCI SSC認定 PCI内部監査人(ISA)資格研修
・Zscalerトレーニング（EDU-200、EDU-220、EDU-230、EDU-280）
・電力ISAC関連ハンズオン演習（ベンダー開催）

アンケート調査結果

設問25.【自由記述】
設問24で、「特に取り組んでいるものはない」以外を選んだ場合、人材育成における具体的な取組や認識している課題を記載してください。

■「人材育成における具体的な取組」の主な記載

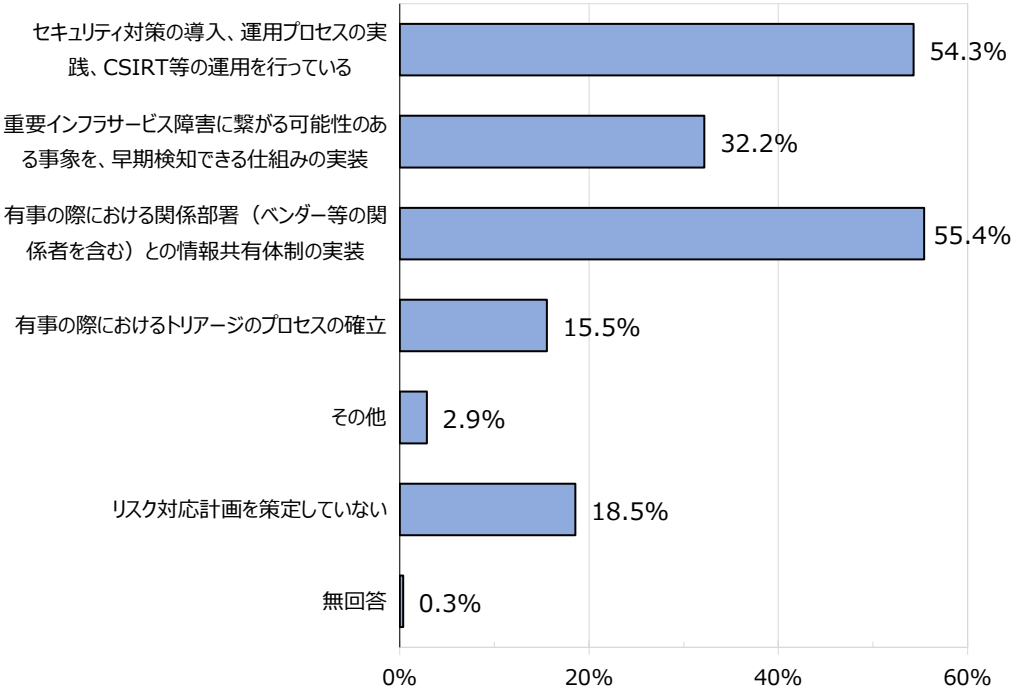
・全職員向けの情報セキュリティ研修を毎年実施
・eラーニングやリモートラーニングの活用（J-LIS提供など）
・新規採用職員向けセキュリティ研修の必須化
・標的型攻撃メール訓練の定期実施
・外部講師によるセキュリティ研修や講演会の開催
・インシデント事例の社内共有による啓発活動
・資格取得支援制度の導入（情報処理安全確保支援士など）
・ジョブローテーションによる情報部門職員の知識継承
・外部専門機関やベンダー研修への参加
・DX推進リーダーや情報化推進担当者の育成
・管理職・経営層向けのセキュリティ研修の実施
・セキュリティスキルマップに基づく教育制度の構築
・実践的サイバー防御演習（CYDER）やCSIRT訓練への参加
・社内ポータルやチャットツールでの啓発活動
・標的型メール訓練後のフィードバック教育
・外部セミナーやハンズオン研修への積極参加
・ITパスポートや情報処理試験取得の推奨
・部署ごとのセキュリティ責任者育成
・グループ会社や関連企業との合同研修
・セキュリティ教育コンテンツの内製化と定期更新

■「人材育成において認識している課題」の主な記載

・専門知識を有する人材の不足
・人事異動によるノウハウ継承の困難
・研修を受ける時間や人的リソースの不足
・教育効果の定量化が難しい
・セキュリティ人材の採用・定着が困難
・予算不足による外部研修や専門教育の制約
・職員のセキュリティ意識の低さ・当事者意識の欠如
・研修が形骸化し、知識定着が不十分
・最新の脅威や技術への対応が遅れる
・兼務によるセキュリティ業務への時間不足
・組織全体でのセキュリティ文化の醸成が不十分
・育成に長期間を要し、異動でリセットされる構造的課題
・高度な専門知識を持つ指導者の不足
・クラウドやDX対応に必要なスキル不足
・教育後の人材流出による再育成の負担
・職員間のリテラシー格差が大きい
・実務と研修内容の乖離
・外部研修の費用負担が大きい
・セキュリティ人材のキャリアパスが不明確
・業務優先で研修が後回しになる傾向

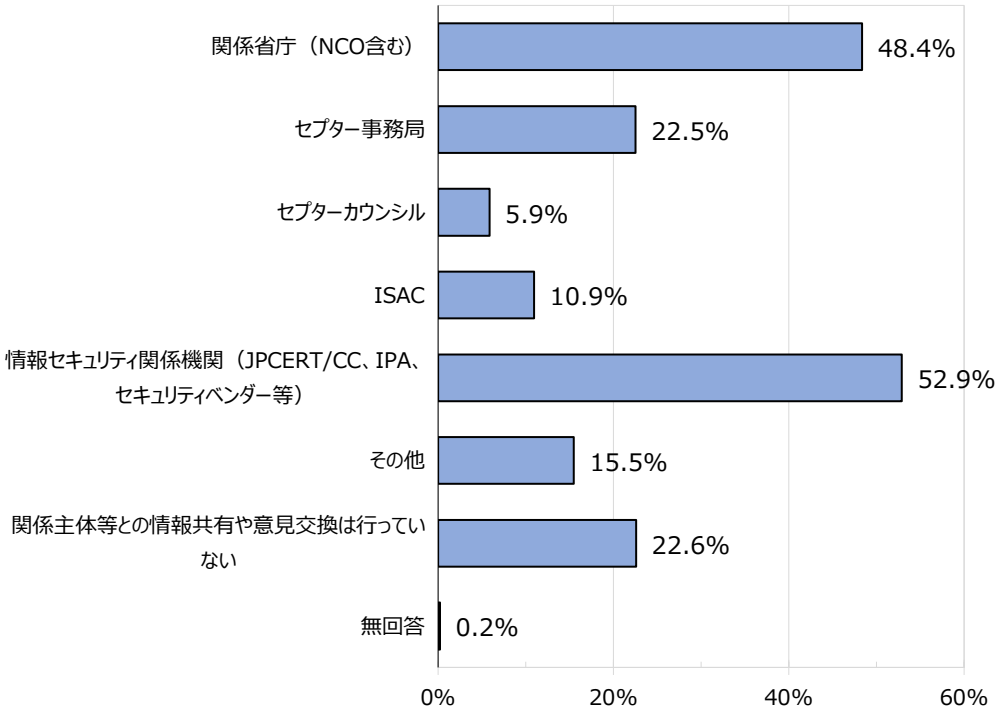
アンケート調査結果

設問26.【複数回答】
リスク対応計画の実施について、状況を全て選択してください。



■「その他」（一部抜粋）
・リスク対応計画についての推進体制が整っていない
・リスク対応計画の策定に向けて協議中

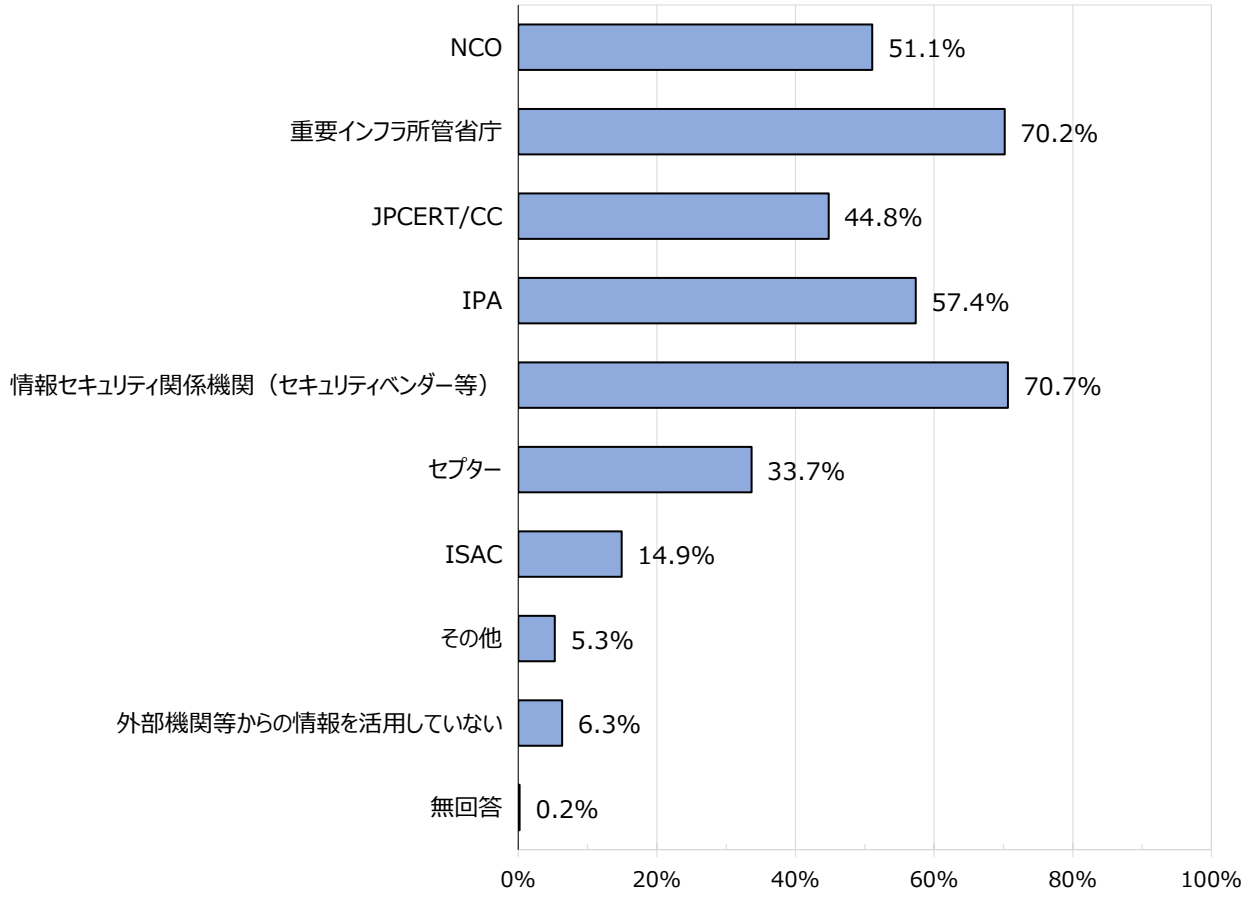
設問27.【複数回答】
重要インフラサービスの安全かつ持続的な提供を実現するという観点から、情報共有や意見交換を行っている関係主体を全て選択してください。



■「その他」（一部抜粋）
・警察
・親会社やグループ会社
・同業他社

アンケート調査結果

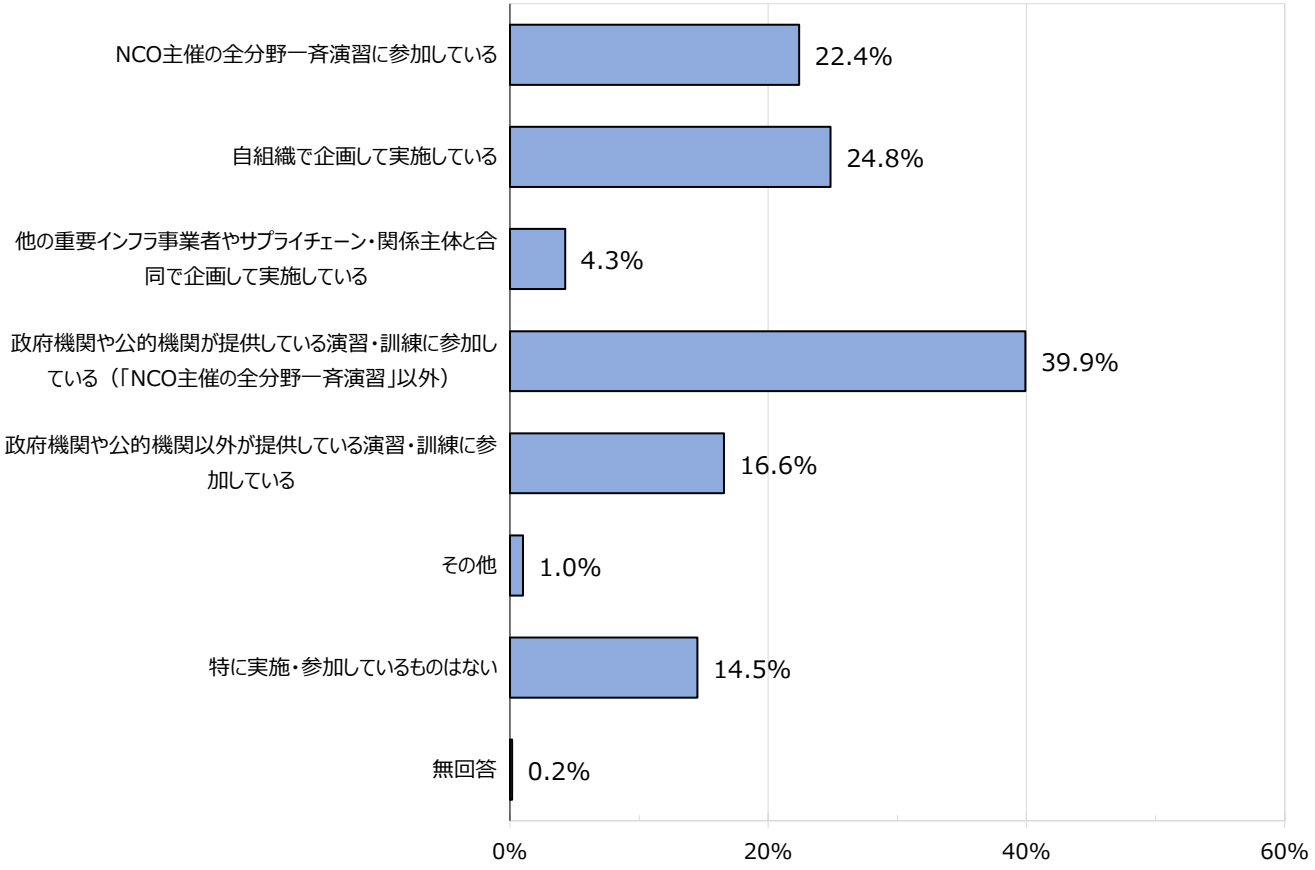
設問28.【複数回答】
自組織で活用している情報の提供元を全て選択してください。



■「その他」（一部抜粋）
・警察
・ニュース
・顧客
・外部コンサル会社
・地域情報化推進アドバイザー
・親会社やグループ会社

アンケート調査結果

設問29.【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。
（※金融分野を含む）



■「その他」（一部抜粋）
・グループ本体が行うサイバーセキュリティ研修に全社員参加
・親会社によるeラーニング
・専門性ある人間を常駐させて適時アドバイスを受けている

アンケート調査結果

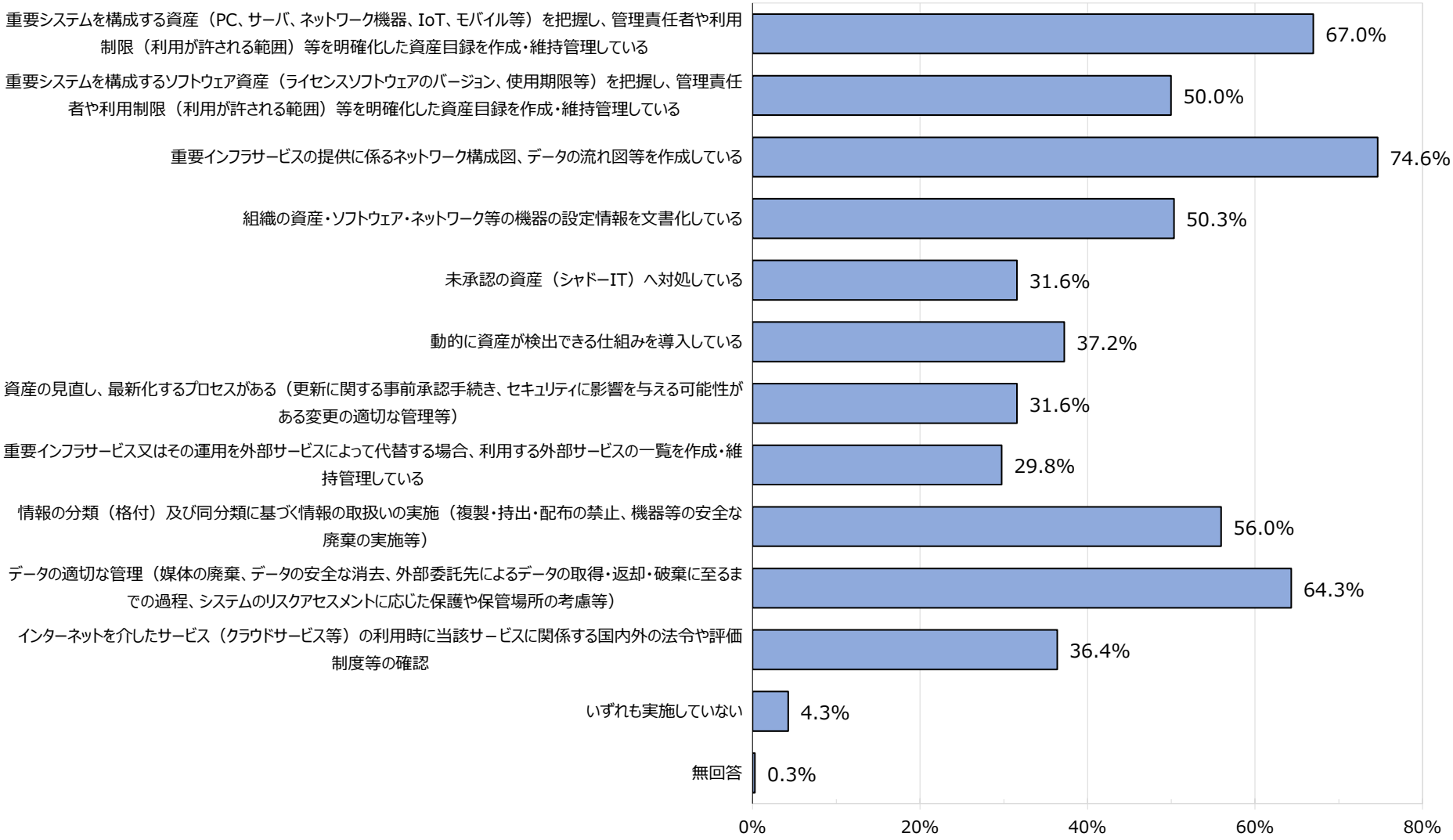
設問30.【自由記述】
設問29で、「特に実施・参加しているものはない」以外を選んだ場合、実施、参加している演習、訓練について、実施主体、内容、形式、規模等を具体的に記載してください。また、演習・訓練の実施・参加の目的（対処能力の向上、自組織の情報セキュリティ対策の効果の検証、改善点の検証等）を記載してください。

■主な記載

演習・訓練名	実施主体	内容	形式	規模	参加目的
実践的サイバー防御演習（CYDER）	総務省・NICT	インシデント対応に必要となる知識・スキルの習得	実機演習	全国規模	インシデント対応能力の向上
プレCYDER	総務省・NICT	CYDER入門、基礎知識習得	オンライン	全国規模	新任担当者教育
標的型攻撃メール対応訓練	自治体・県警等	擬似メール送信による対応確認	メール配信	数十名～全職員	セキュリティ意識向上
インシデント発生時CSIRT対応訓練	J-LIS	シナリオに基づくCSIRT対応	オンライン	数十名規模	CSIRT対応力強化
全分野一斉演習	NCO	重要インフラ含む障害対応体制検証	机上演習・オンライン	部門横断	対応体制検証
セプター訓練	NCO・CEPTOAR事務局	緊急時の情報疎通確認	メール連絡	全国規模	情報共有体制強化
金融業界横断演習（Delta Wall）	金融庁	金融業界でのサイバー攻撃対応演習	机上演習・オンライン	業界横断	対処能力向上
金融ISAC演習（FIRE）	金融ISAC	マルウェア感染等を想定した対応	実機演習・机上演習	業界横断	インシデント対応力強化
個人情報インシデント対応訓練	個人情報保護委員会	個人情報漏えい時の対応手順確認	オンライン	自治体・関係部門	個人情報保護対応力向上
制御システム演習（CSSC演習）	CSSC・電力ISAC等	制御系対象のハンズオン演習	実機演習	業界単位	重要インフラ防護能力強化

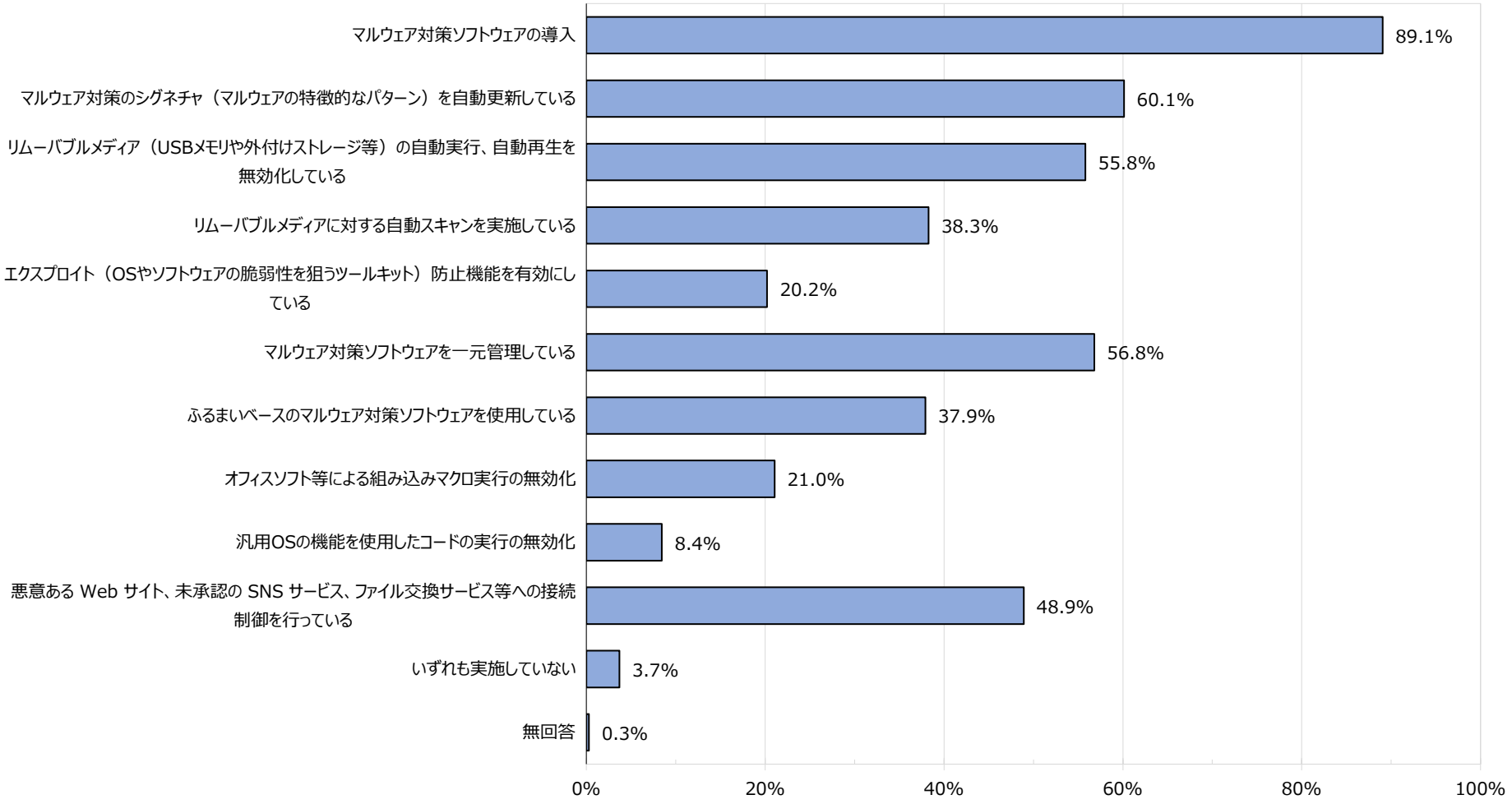
アンケート調査結果

設問31.【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全て選択してください。



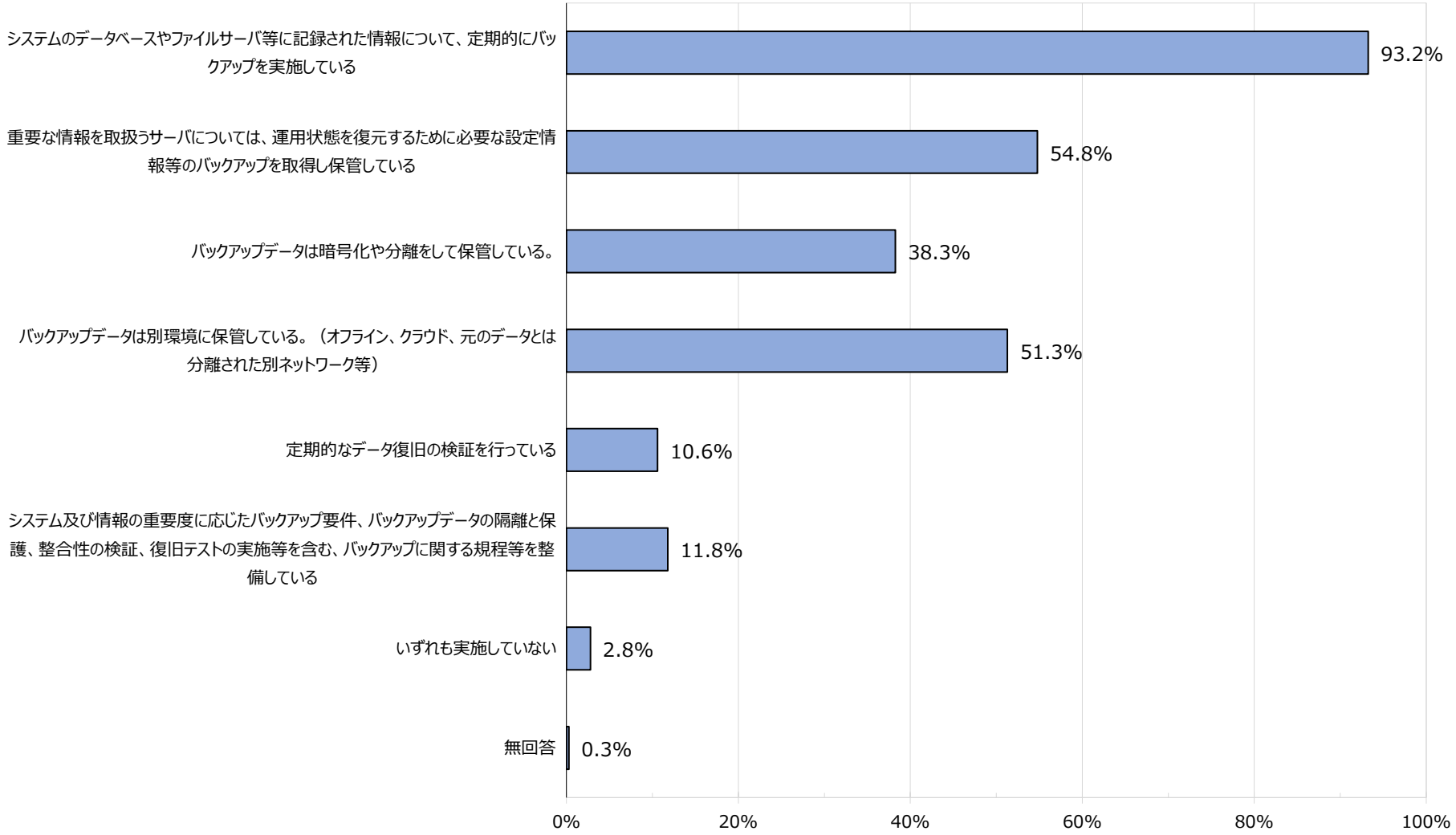
アンケート調査結果

設問32.【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全て選択してください。

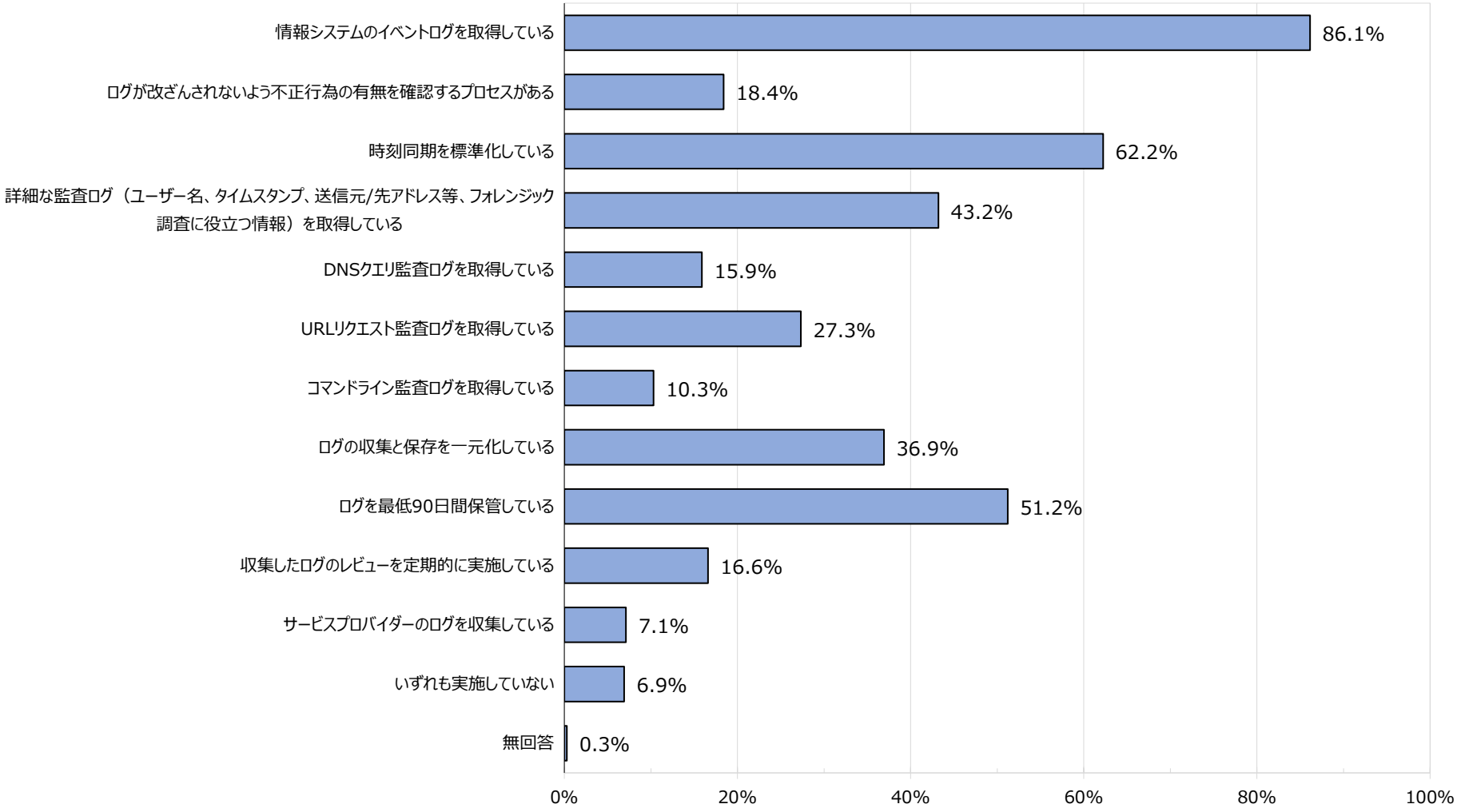


アンケート調査結果

設問33.【複数回答】
バックアップに関して実施している取組を全て選択してください。

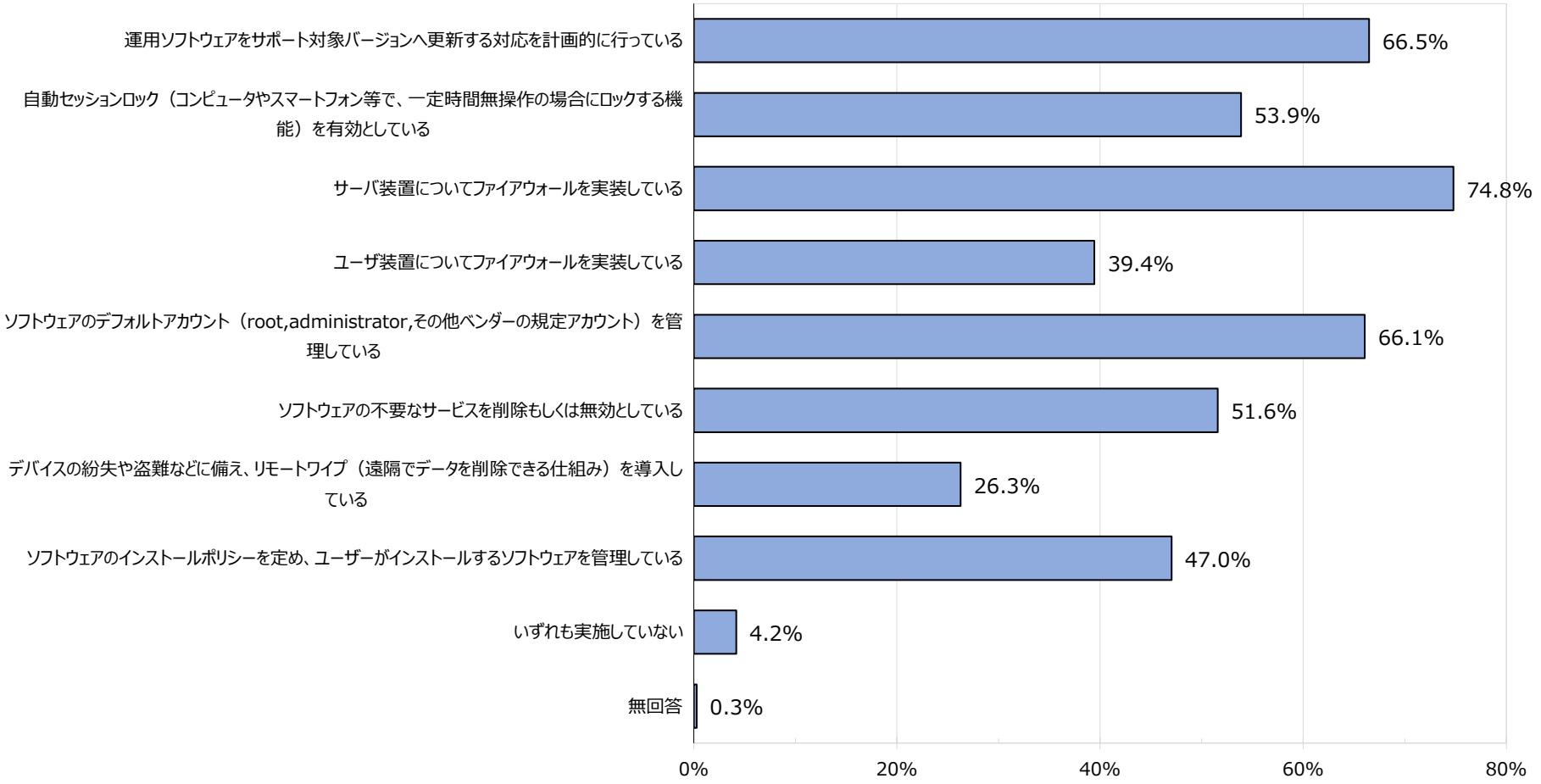


設問34.【複数回答】
ログ管理に関して実施している取組を全て選択してください。



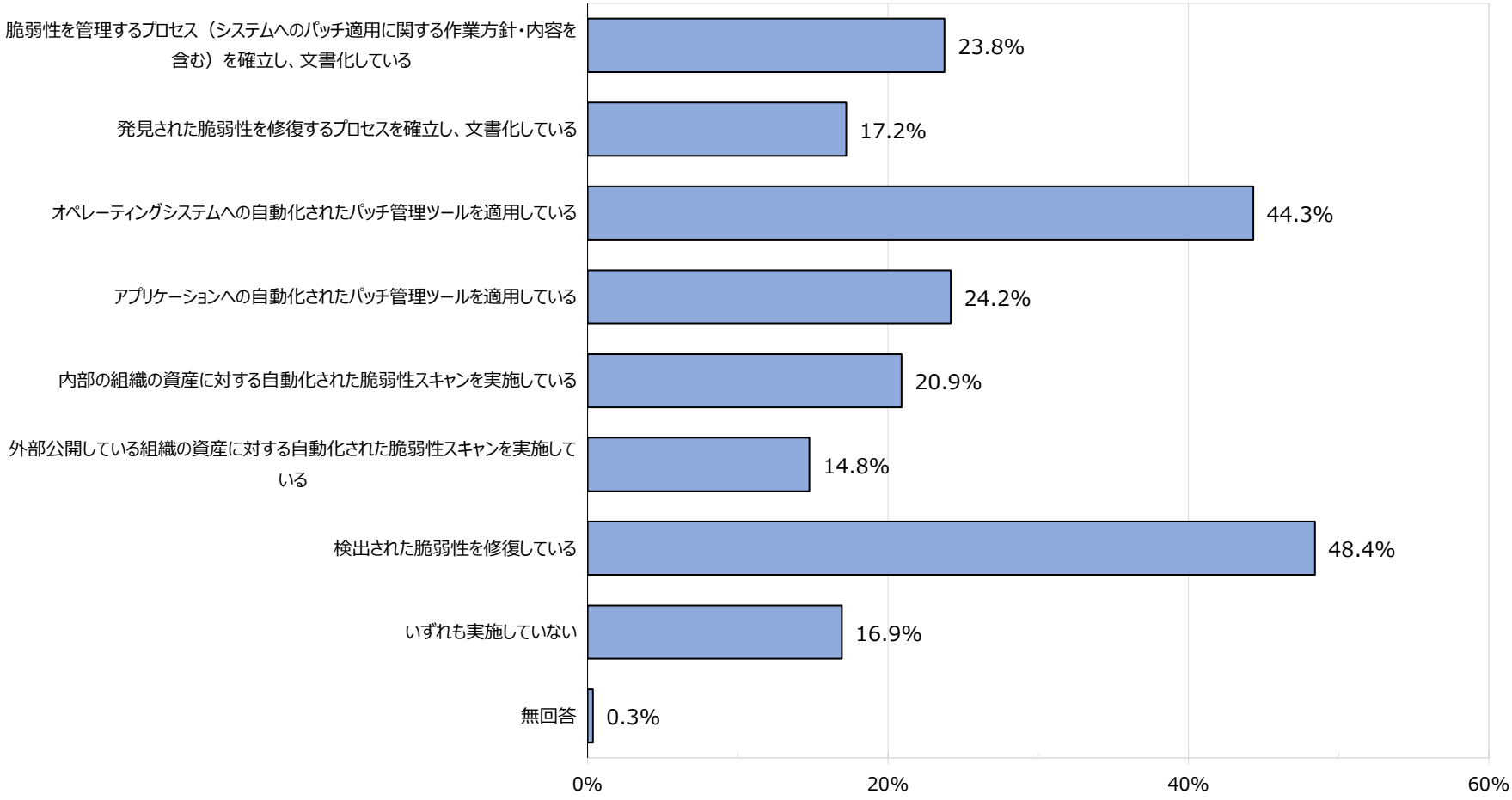
アンケート調査結果

設問35.【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全て選択してください。



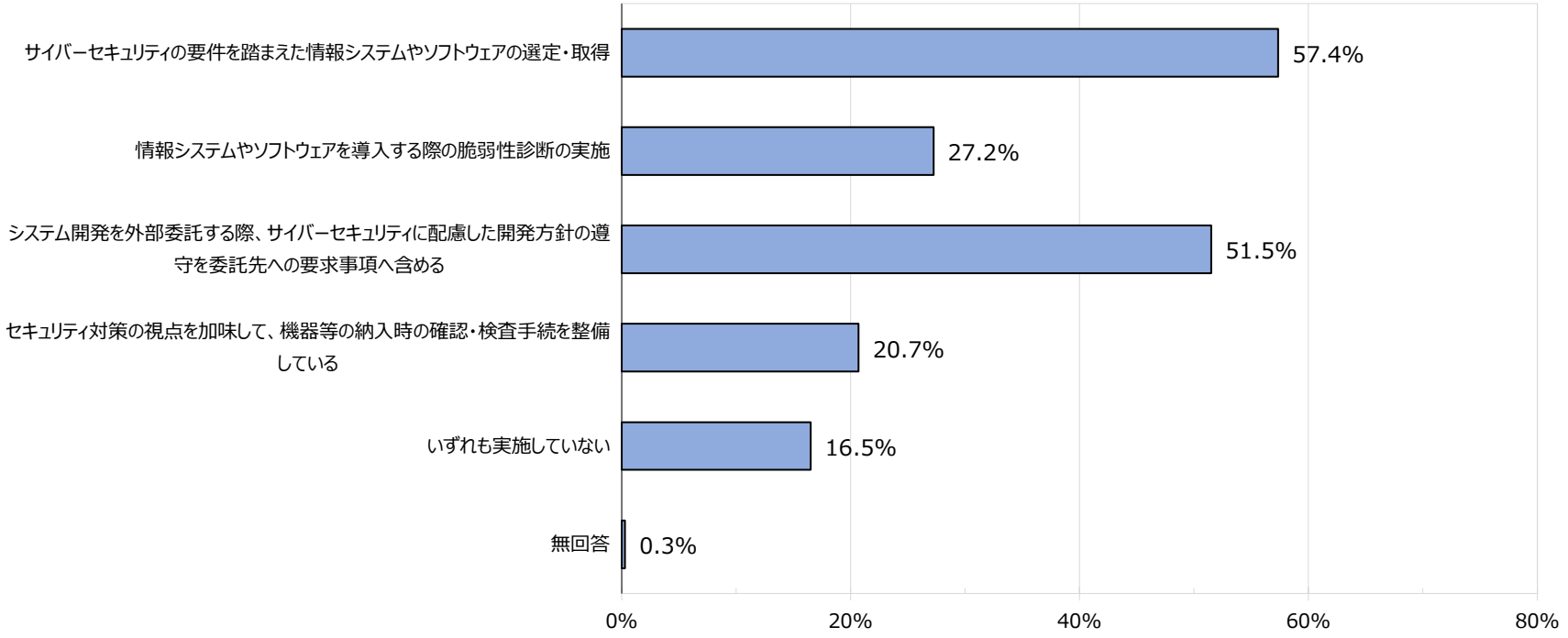
アンケート調査結果

設問36.【複数回答】
脆弱性管理について実施している取組を全て選択してください。



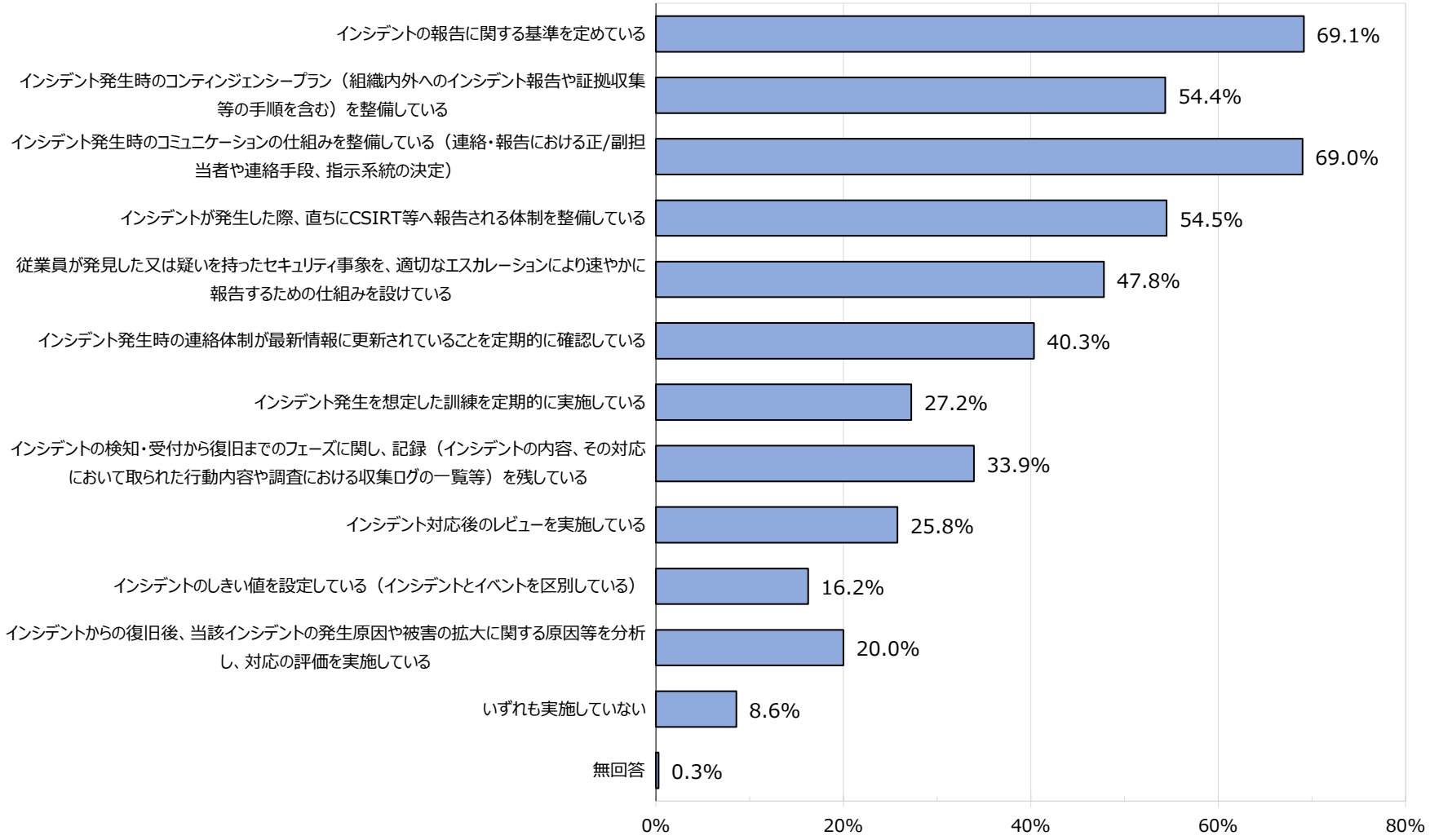
アンケート調査結果

設問37.【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全て選択してください。



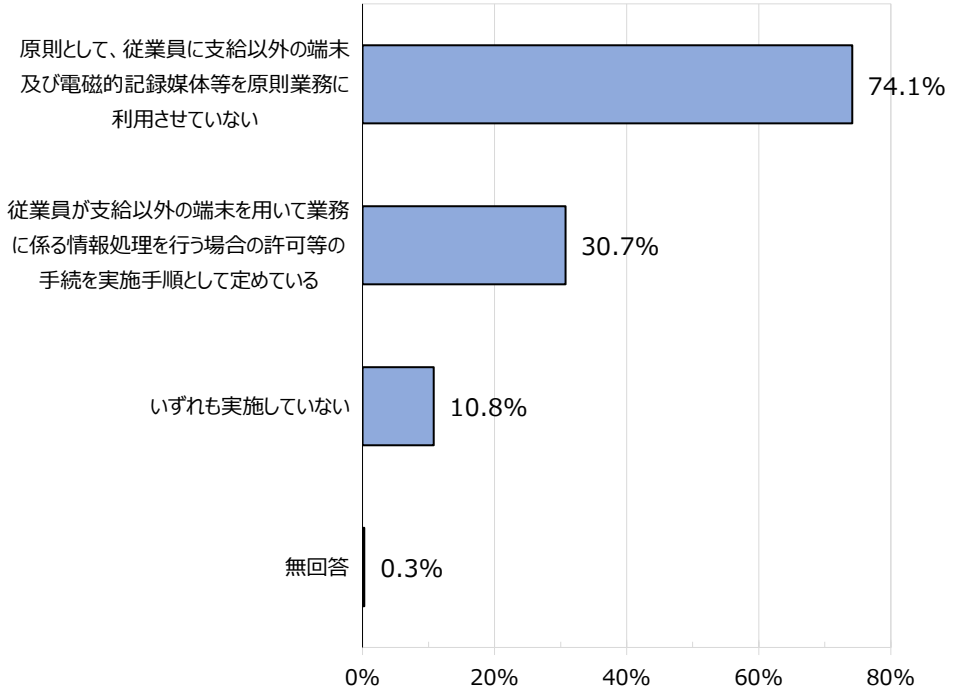
アンケート調査結果

設問38.【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全て選択してください。

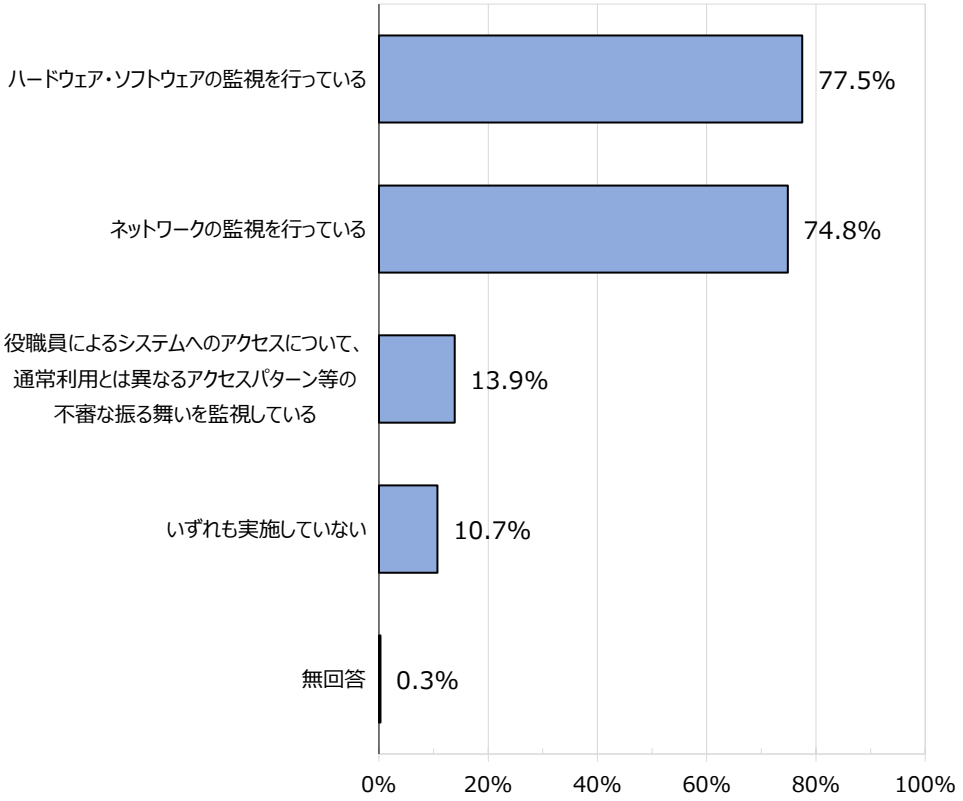


アンケート調査結果

設問39.【複数回答】
私物端末の業務利用（BYOD）管理について実施している取組を全て選択してください。

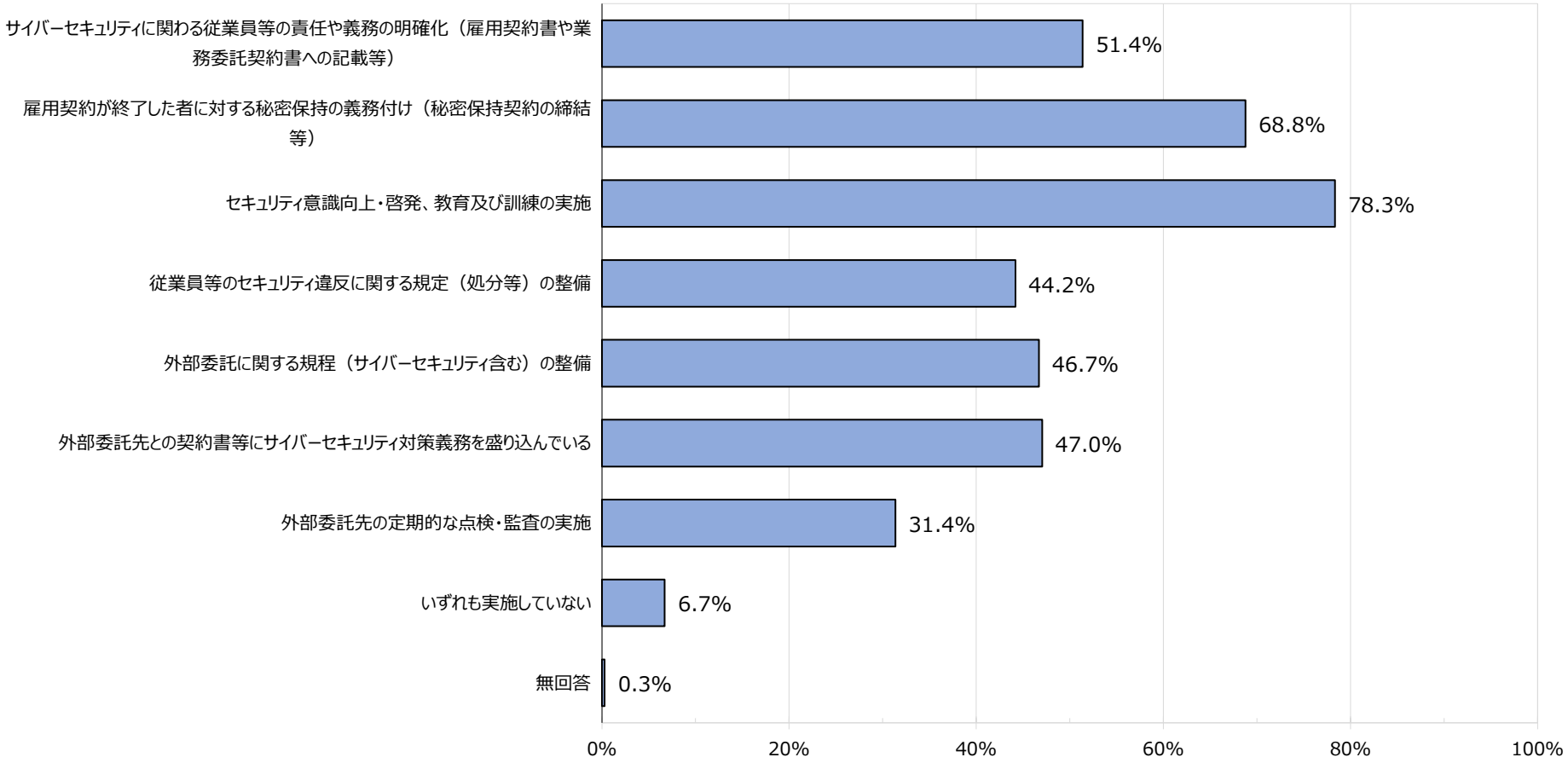


設問40.【複数回答】
システムの監視について実施している取組を全て選択してください。



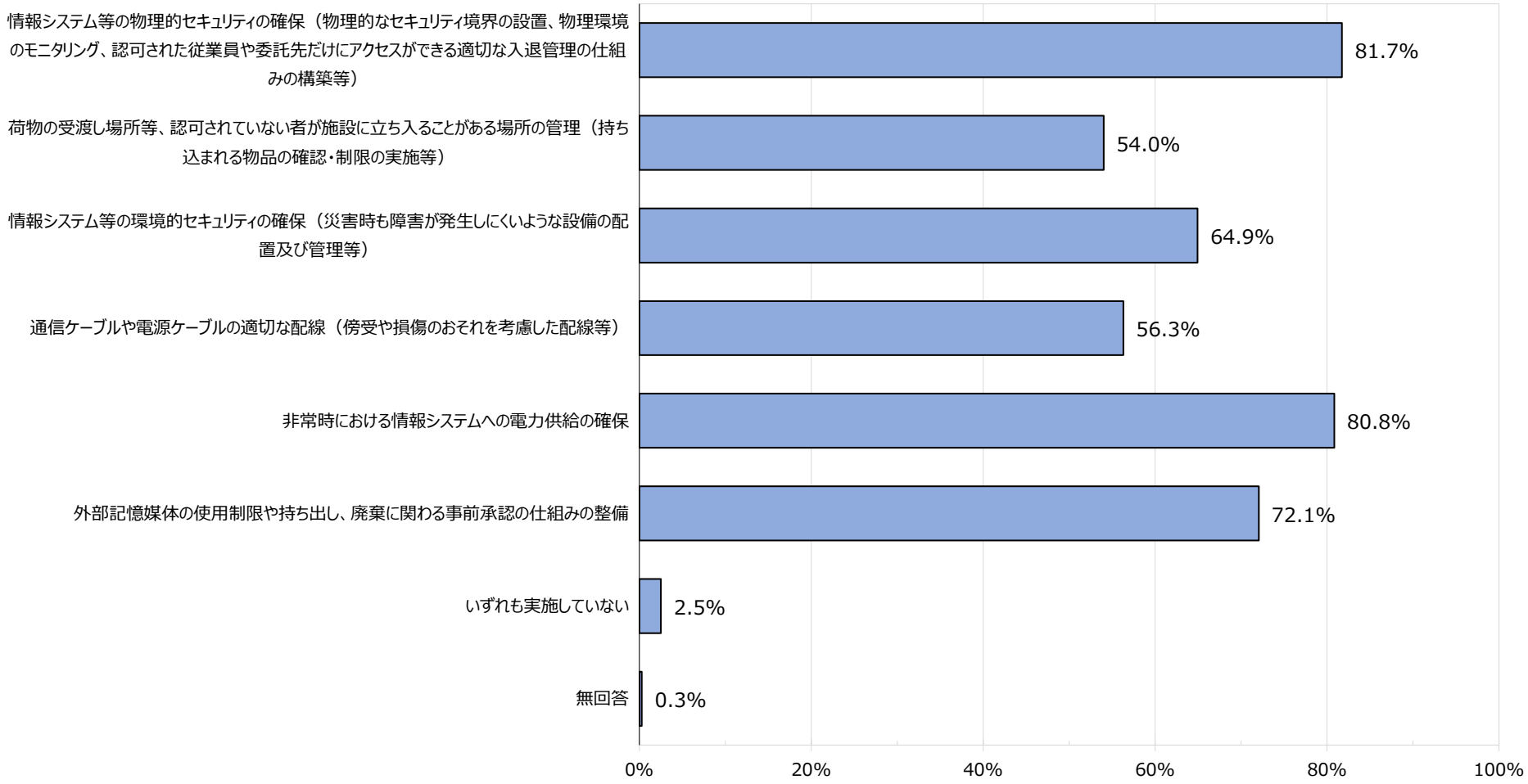
アンケート調査結果

設問41.【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全て選択してください。



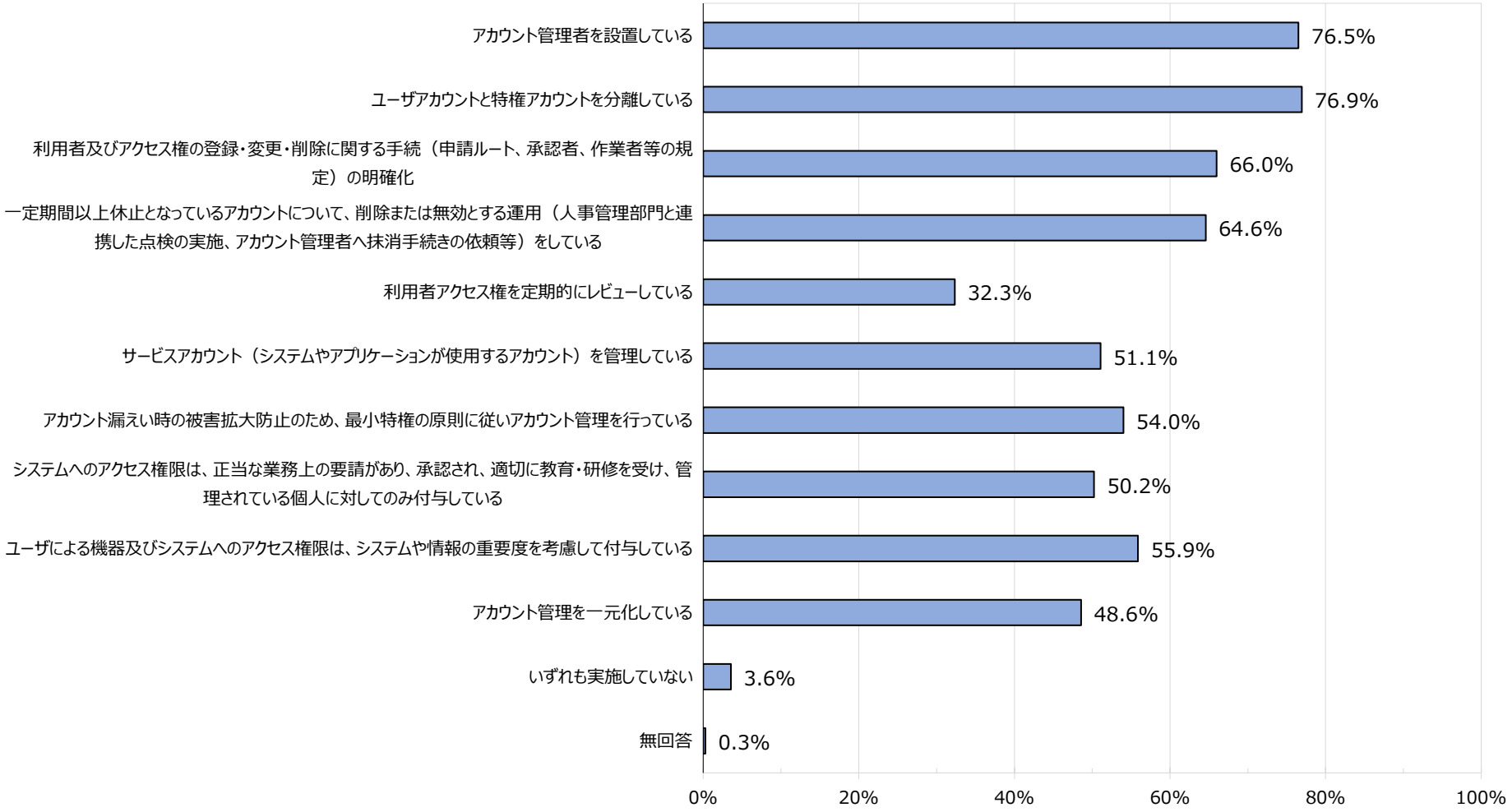
アンケート調査結果

設問42.【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全て選択してください。



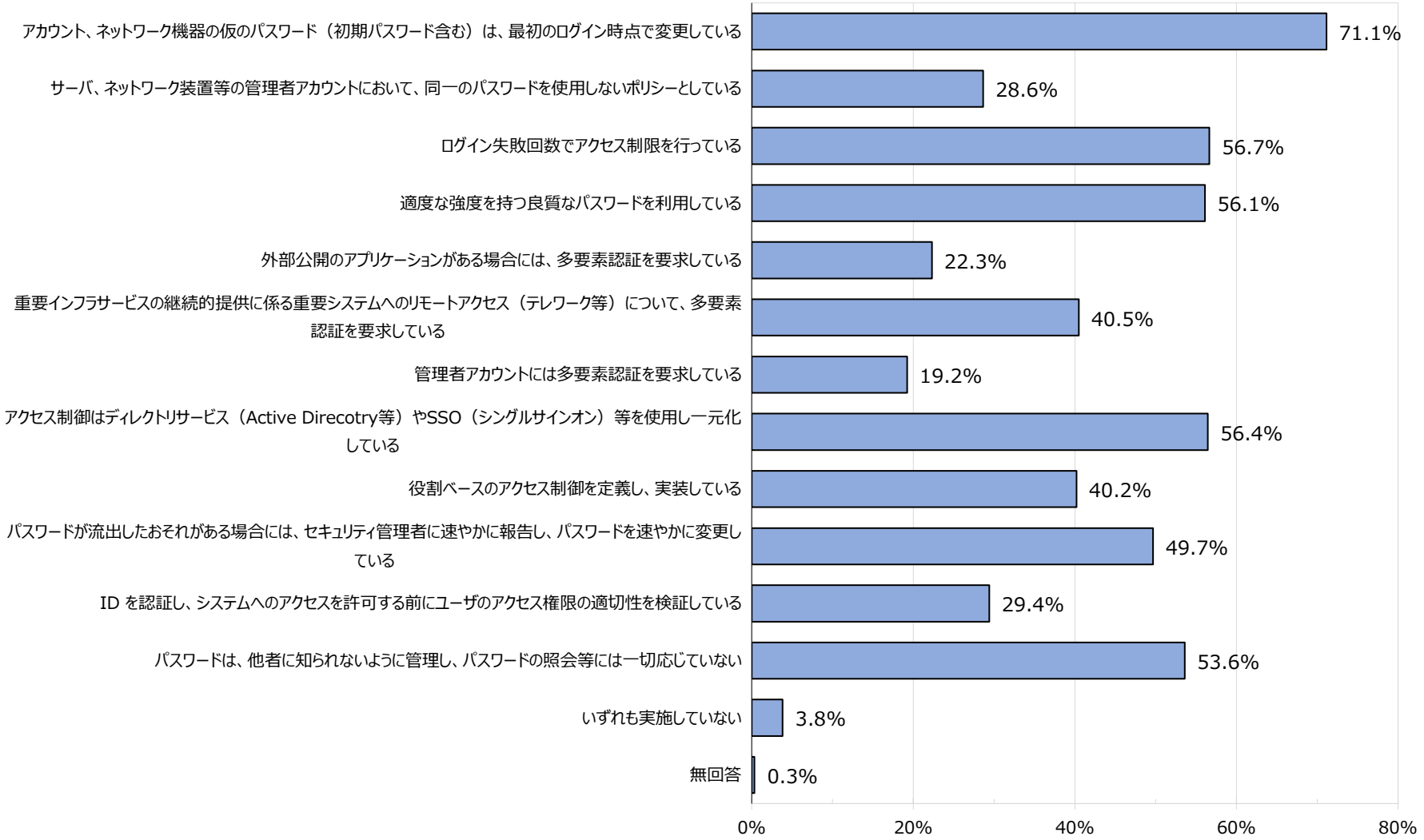
アンケート調査結果

設問43.【複数回答】
アカウント管理に関して、実施している取組を全て選択してください。



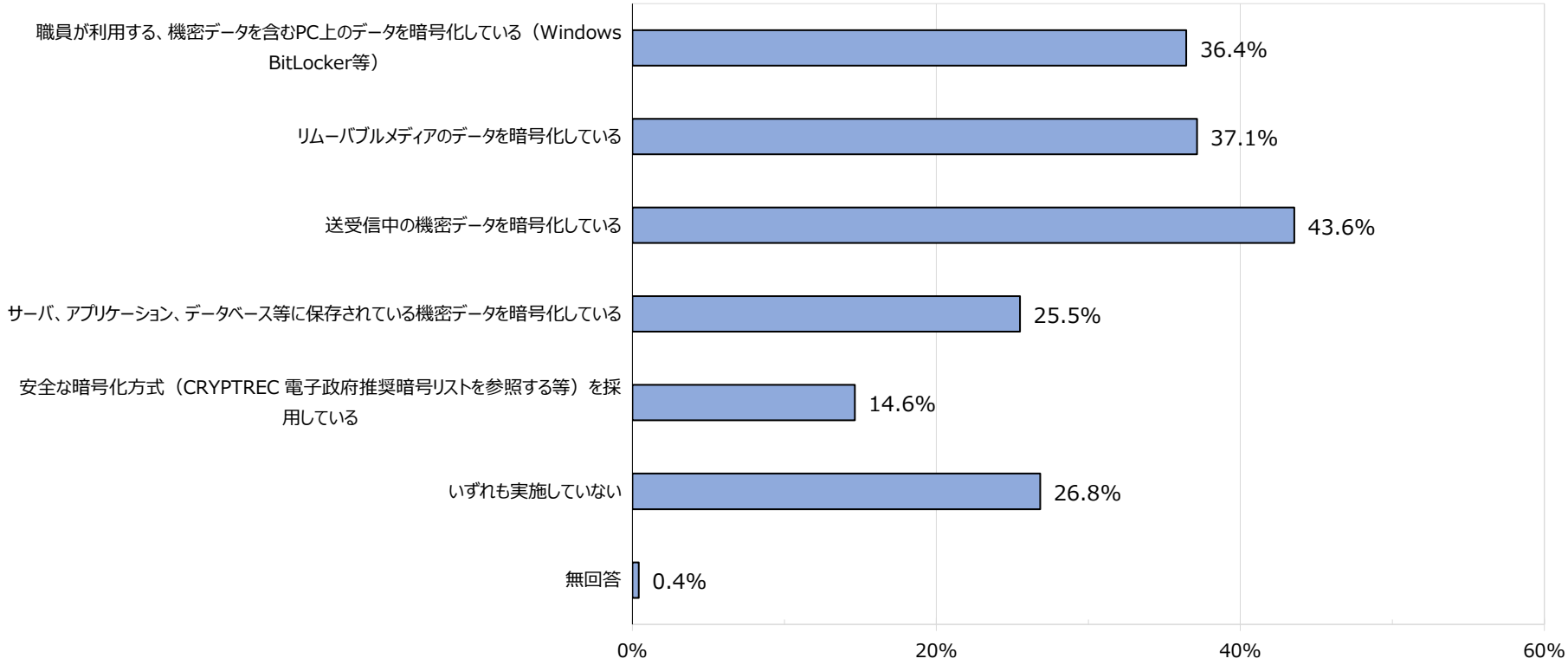
アンケート調査結果

設問44.【複数回答】
アクセス制御に関して、実施している取組を全て選択してください。



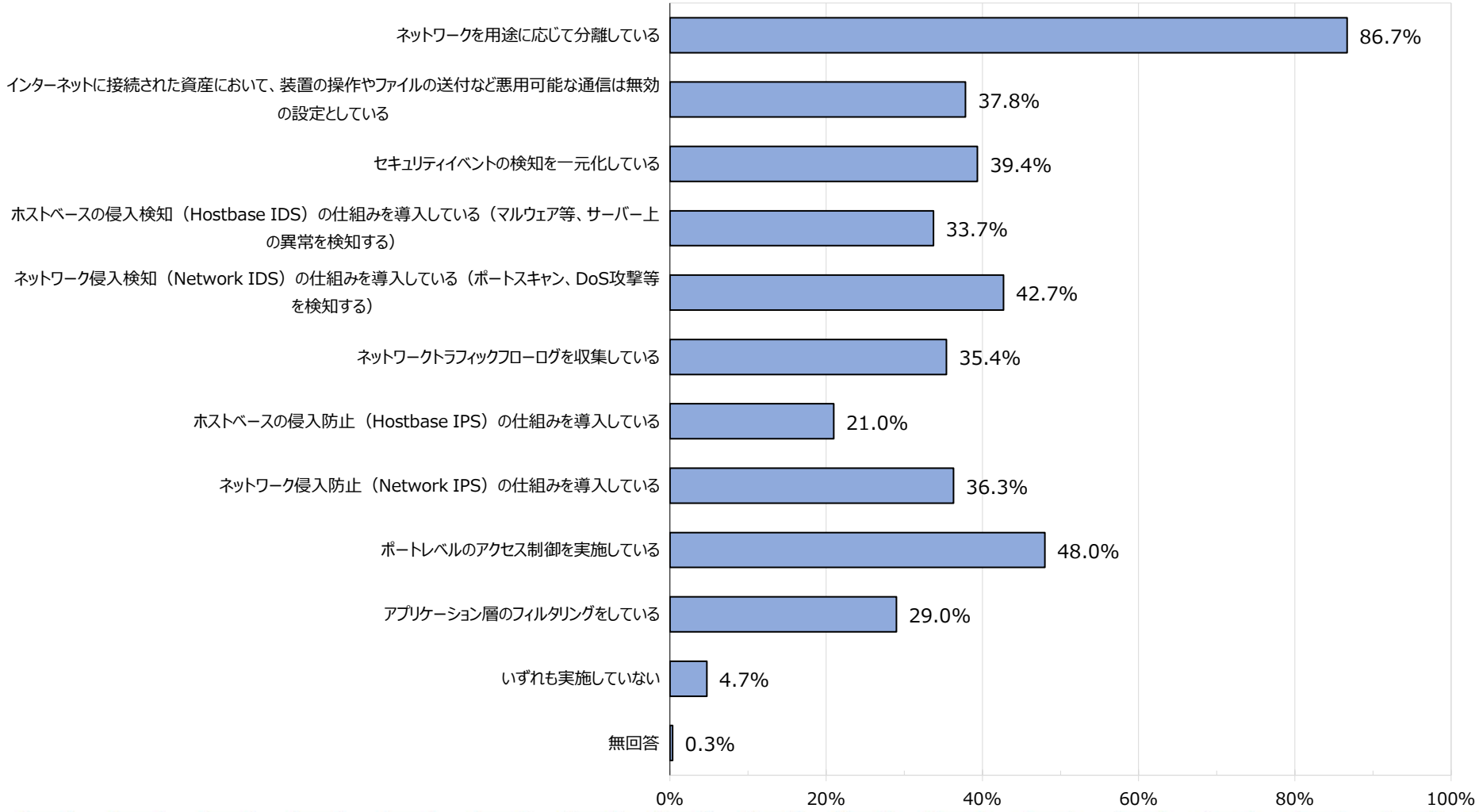
アンケート調査結果

設問45.【複数回答】
暗号に関して、実施している取組を全て選択してください。



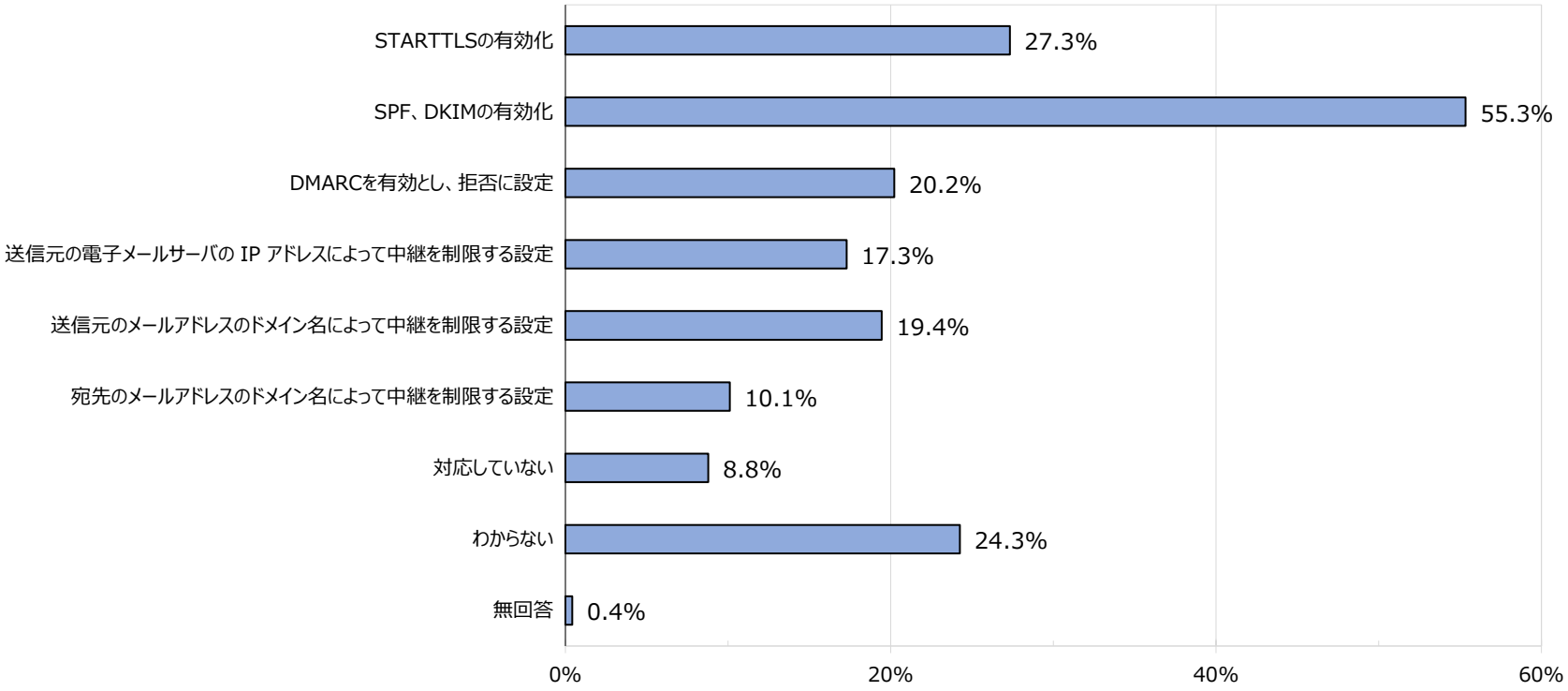
アンケート調査結果

設問46.【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全て選択してください。



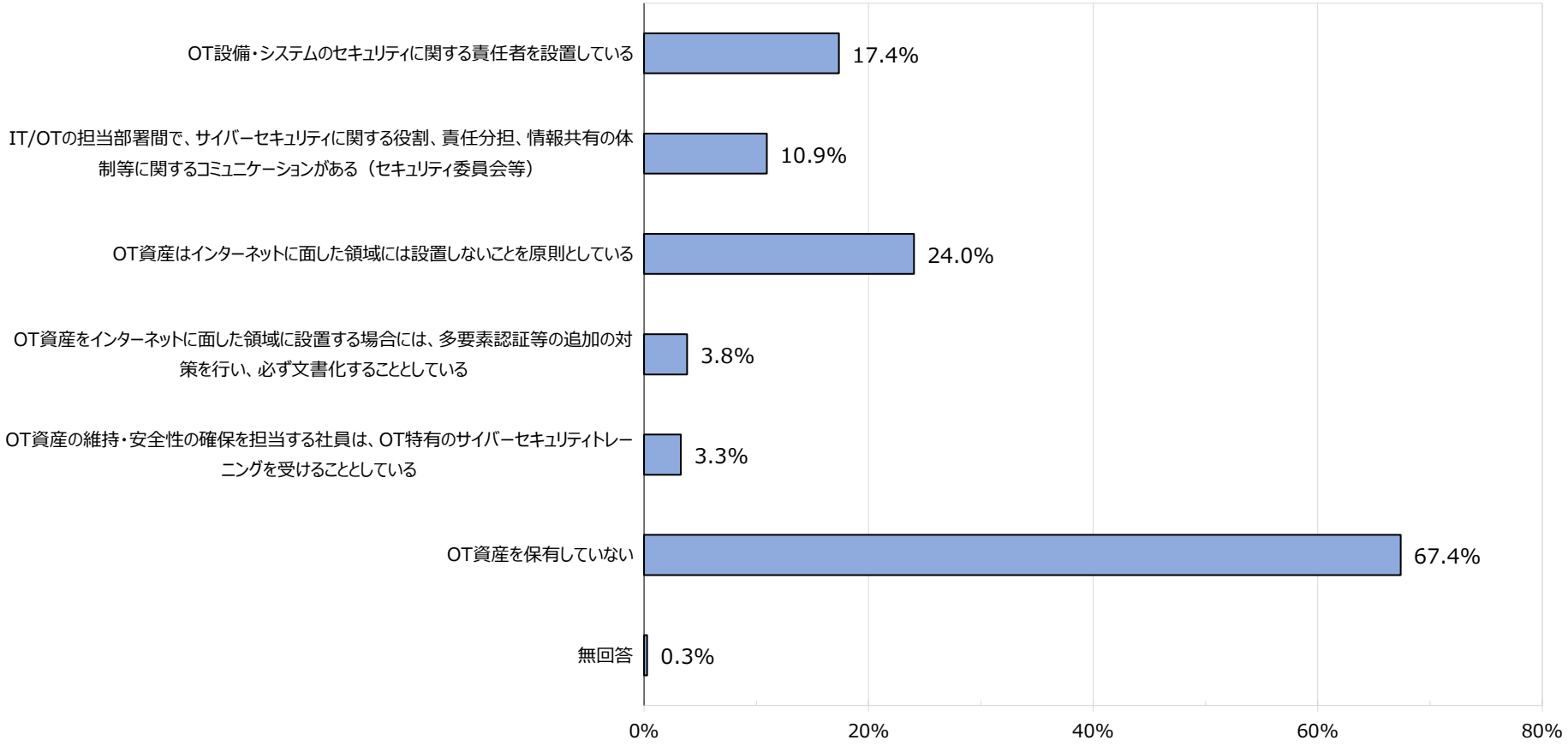
アンケート調査結果

設問47.【複数回答】
電子メールを使用した一般的なサイバー脅威リスクを低減するため、導入している対策を全て選択してください。

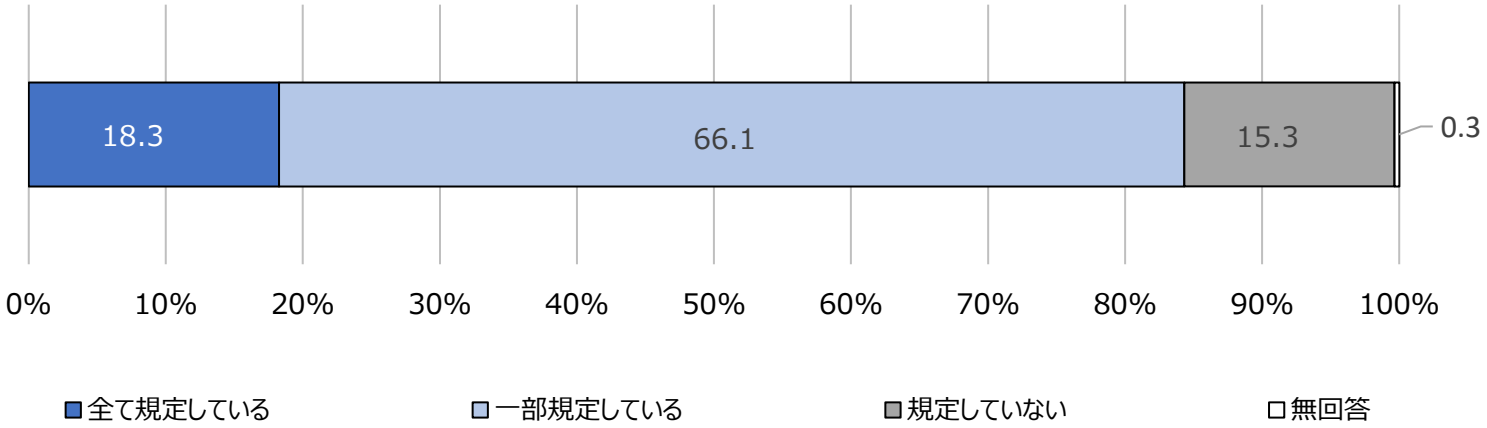


アンケート調査結果

設問48.【複数回答】
制御システム（OT資産）を保有している場合に、実施している取り組みを全て選択してください。

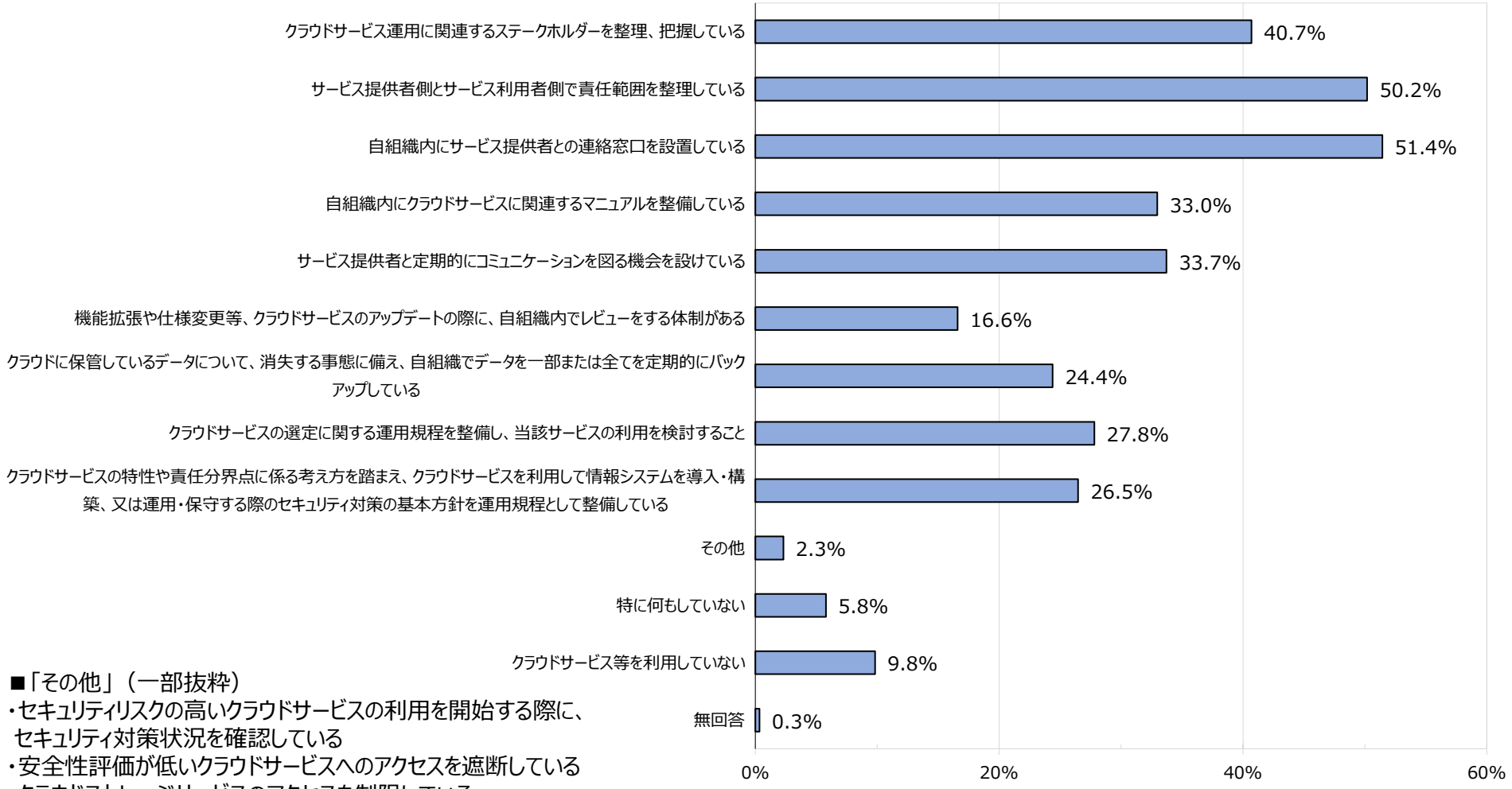


設問49.【単一回答】
組織的対策、人的、物理的、技術的対策にて、「実施している」としたサイバーセキュリティ確保の取組を内規（実施手順・マニュアル等）として規定しているか。



アンケート調査結果

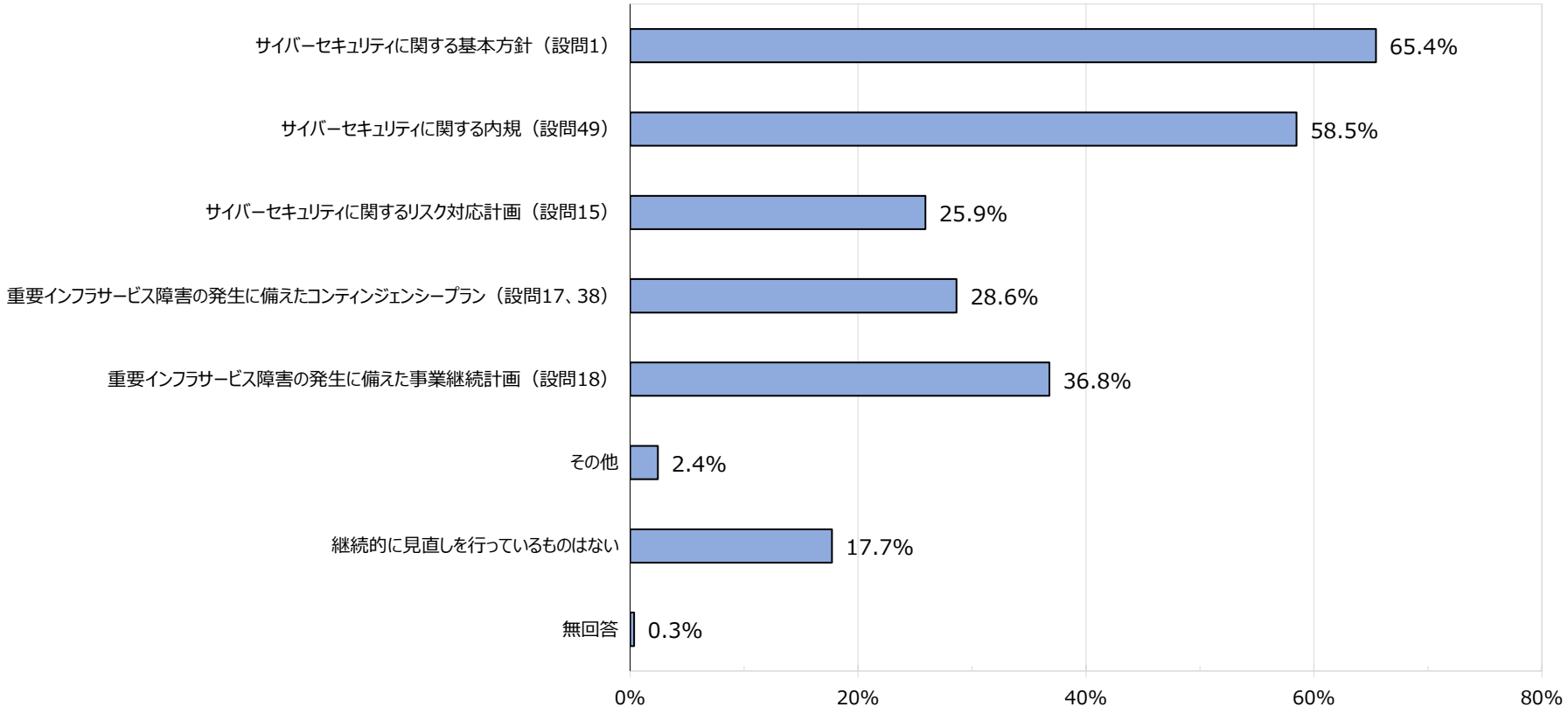
設問50.【複数回答】
クラウドサービスを利用するに当たり、自組織で行っている運用対策を全て選択してください。



■「その他」（一部抜粋）
・セキュリティリスクの高いクラウドサービスの利用を開始する際に、セキュリティ対策状況を確認している
・安全性評価が低いクラウドサービスへのアクセスを遮断している
・クラウドストレージサービスのアクセスを制限している
・ISMAPやISMS等、サービスや提供事業者の認証取得状況を確認している

アンケート調査結果

設問51.【複数回答】
ご回答いただいた内容について、見直し・改善に関する設問です。
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。

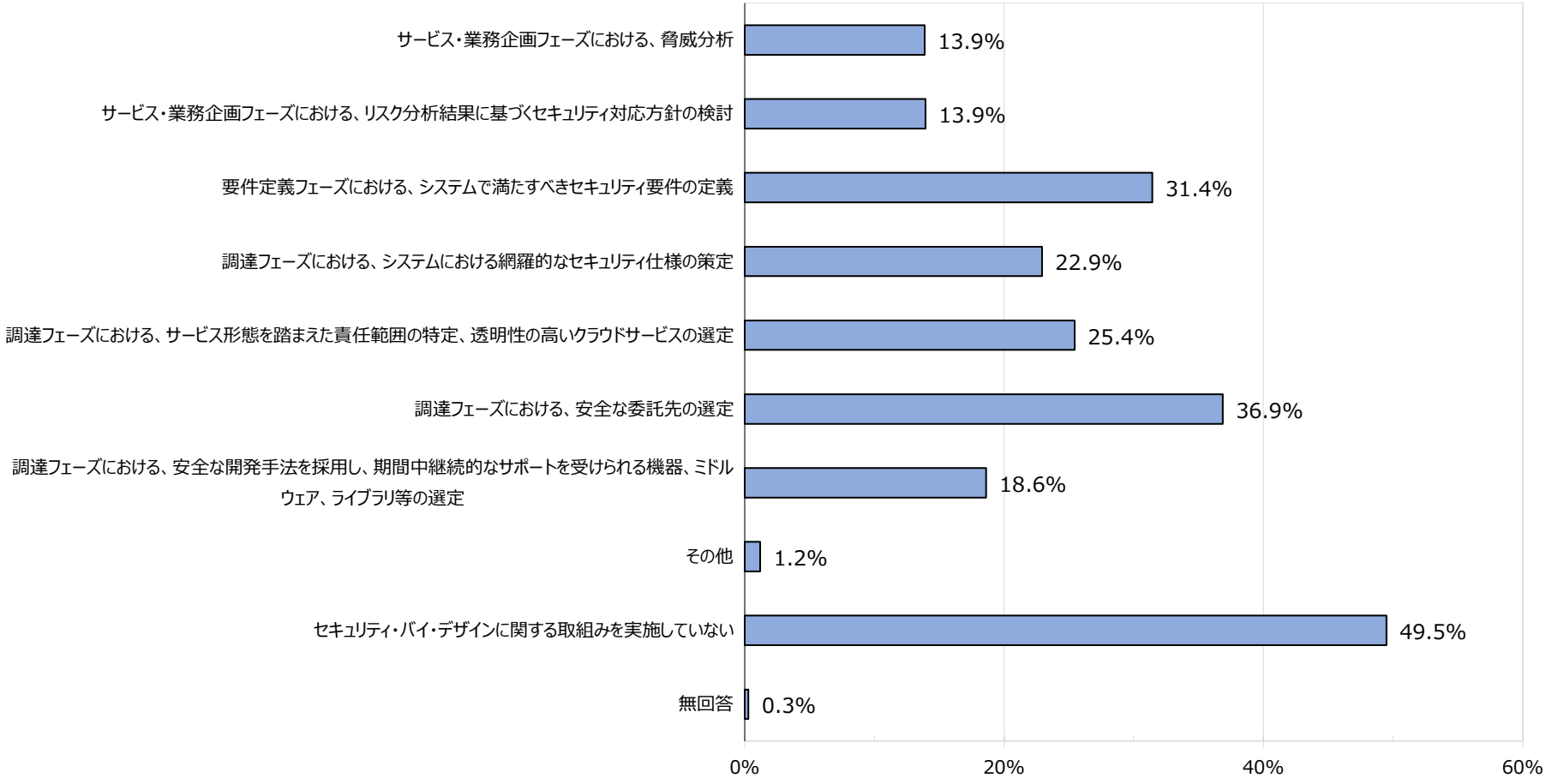


■「その他」（一部抜粋）
・サイバーセキュリティに関する基本方針を策定中である
・不定期に見直しを行っている
・セキュリティ確保のため具体的な対策

アンケート調査結果

設問54.【複数回答】
セキュリティ・バイ・デザイン（※）について実施している取組を全て選択してください。

※システムのライフサイクルにおける企画段階からサイバーセキュリティの観点を意識し、システム仕様にセキュリティ要件を適切に組み込むこと。



設問55.【自由記述】
設問54において「セキュリティ・バイ・デザインに関する取組みを実施していない」以外を選択した場合、選択した取組みの具体的な内容について記載してください。

■選択した取組みの具体的内容（一部抜粋）

1．サービス・業務企画フェーズ
・調達フェーズでは遅いので、弊社ではセキュリティ・バイ・デザインとして企画段階から調達対象のセキュリティ審査も実施してます
・ベンダ選定を含めて、システムの企画・開発プロセスに関わるガイドラインを策定し、ポリシー遵守
・サプライチェーンリスクに対する対応方針の検討など
・予算要求前に情報システム部門による審査を実施している
・サービスの企画フェーズにおいて、リスクアセスメントを行うプロセスを整備しており、当該プロセスの中でセキュリティリスクの評価を行なっている
・企画段階で脅威・リスク分析を行い、対応方針を策定

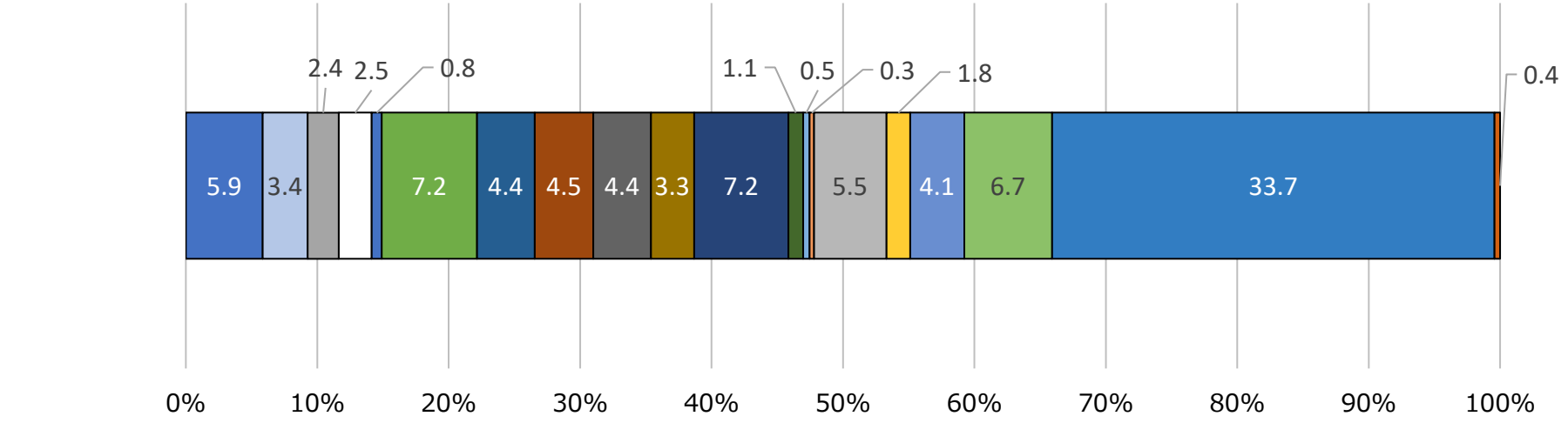
2．要件定義フェーズ
・要件定義でセキュリティ要件を明確化
・セキュリティ要件についてはポリシーとして整備している
・情報セキュリティポリシー上に必要な項目を定義し、システム担当部署及び委託事業者による調達支援により適切なサービス選定を行っている

3．調達フェーズ
・外部委託や外部サービスを利用する際の評価基準及び評価プロセスを定めており、当該プロセス内にてリスク評価を行なっている
・調達段階では、詳細なセキュリティ仕様の作成、安全な委託先の選定、透明性の高いクラウドサービスの評価を実施
・情報セキュリティポリシー上に必要な項目を定義し、システム担当部署及び委託事業者による調達支援により適切なサービス選定を行っている
・継続的サポートが受けられる機器やソフトウェアを選定し、開発手法にもセキュリティを組み込みます
・調達フェーズにおける非機能要件の評価

4．その他
・安全な開発手法と継続的サポートを確保する

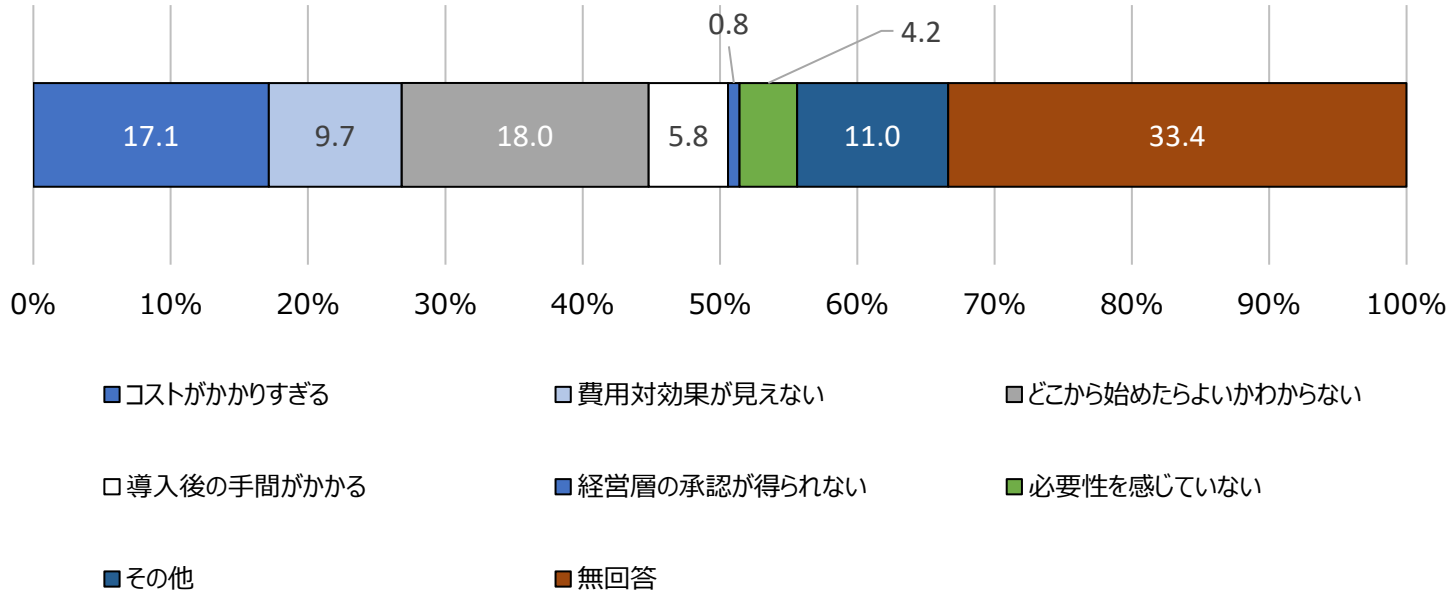
アンケート調査結果

設問56.【単一回答】
設問31～48において「実施していない」旨を回答した対策・取組みのうち、実施にあたって特に課題があると考えている対策・取組みを１つだけ選択してください。



アンケート調査結果

設問57.【単一回答】
設問56において、選択した対策・取組みの実施する際の課題を選択してください。



■「その他」（一部抜粋）
・職員が業務過多で実施・参加できない
・少ない職員が兼務で業務を行っており、時間のかかるシステムにかかるセキュリティ対策に時間をかけることが困難
・セキュリティに関する専門知識を持つ人材がいない
・情報システム担当の人的リソースが不足している上、担当課においても人事異動等によりシステムやソフトウェアの詳細を把握しきれていないケースがある
・バックアップテストのリストアテストを定期的に実施したいが、コストや本番環境下（本番環境を再現した環境含む）でのテストが難しい
・情報システム部門が把握・管理していない機器(私物や部署独自で導入したもの)などが多い
・どこに線を引くべきかわからない
・グローバル・グループとして国をまたがる多数のエンティティを管理しているため、完全な一元化に時間を要する事がネックとなっている