資料３－１

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39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について

［2024年度］

令和７年６月
内閣サイバーセキュリティセンター
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：2024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（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）

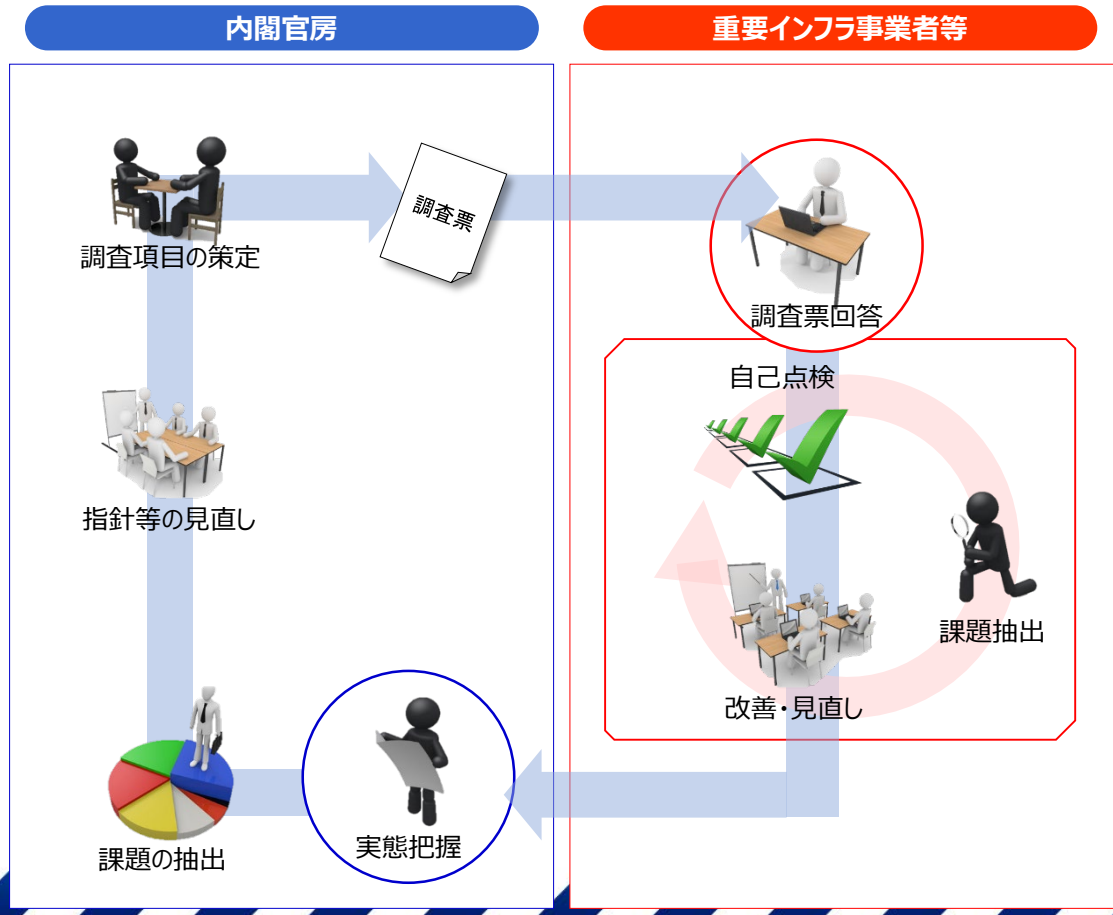
【参考：本調査の実施背景】

○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）



2024年度調査対象及び回答状況

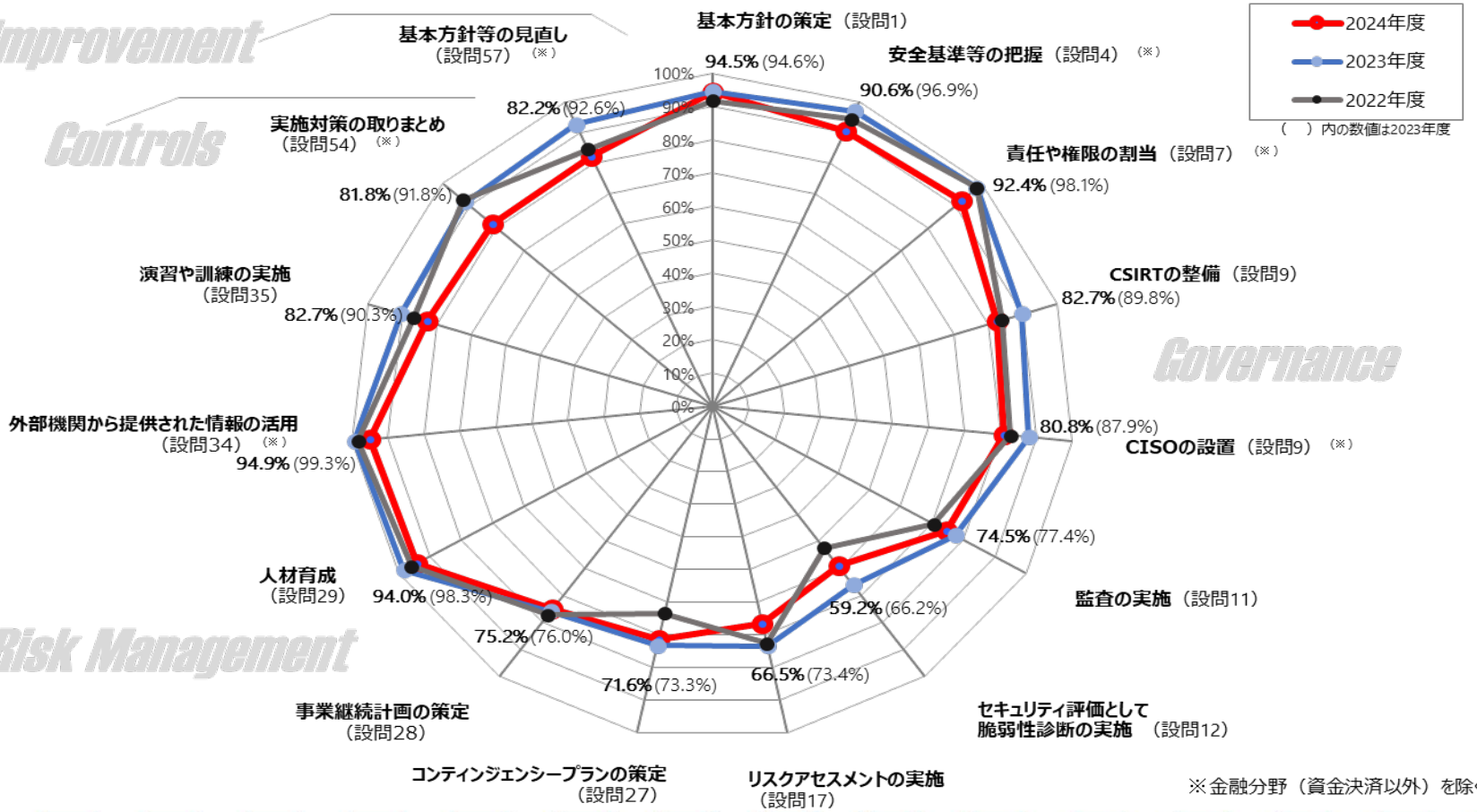
- 2024年度は、**重要インフラ分野（計15分野）の事業者等を対象に調査を実施し、合計2,099事業者から回答**（回答率53.9%）を得た。
（【参考】2023年度は、1,862事業者）

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	13
	放送	主要な地上基幹放送事業者	195	98
	ケーブルテレビ	主要なケーブルテレビ事業者	305	113
金融※1		銀行等、生命保険、損害保険、証券会社	765	670
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	171	66
航空		主たる定期航空運送事業者	15	10
空港		主要な空港・空港ビル事業者	8	4
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	17
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	13
政府・行政サービス		地方公共団体	1788	737
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	22	22
水道		大臣認可水道事業者	442	246
物流		大手物流事業者	15	14
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	19
石油		主要な石油精製・元売事業者	10	6
港湾		主要な港湾運送事業者・港湾管理者等	46	19
全分野合計		－－－	**3894 (3,129)**※2	**2,099 (1,429)**※2

※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>今年度の調査では、一部分野での中小規模事業者等への調査対象拡大（2023年度：主要な事業者⇒2024年度：中小規模を含めた全国の事業者）等があり、全体的に実施率が若干低下している。</u>**
- **<u>「基本方針の策定」、「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高い水準で推移</u>**している。
- しかし、**<u>「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」、「コンティンジェンシープランの策定」、「事業継続計画の策定」といった対策は依然として相対的に低位な実施率</u>**となっており、これらを改善していくことが継続課題である。
  - 「リスクアセスメントの実施」、「脆弱性診断の実施」については、セキュリティ人材の不足や、予算の確保が難しさが実施できていない理由の一つと考えられるが、「人材育成」についての取組は９割強と高位であるため、人材育成が進むにつれ漸次向上していくものと思われる。

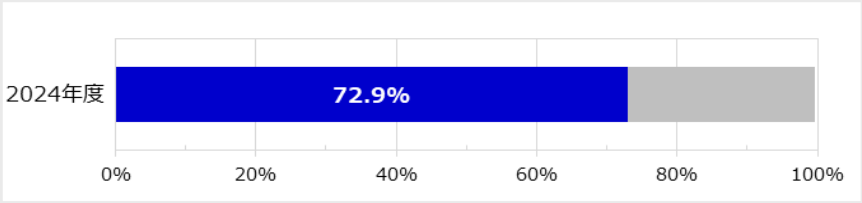


※金融分野（資金決済以外）を除く

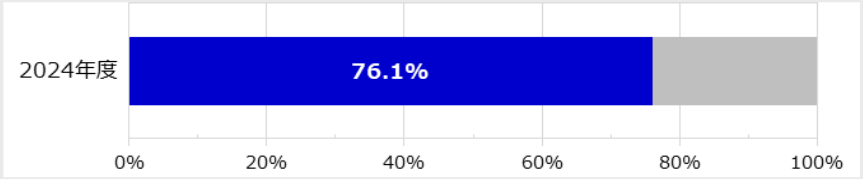
浸透状況と課題 ― 組織統治

- **「定期的なコミュニケーションの実施」及び「セキュリティ方針の策定への経営層の関与」**は７割を超える水準である。他方、情報開示の基準を策定している組織は５割を下回っている。情報開示を促進する観点から、**事件・事故が発生した場合の情報開示の基準・ルールの策定を推進**することが必要と考えられる。
- セキュリティに関する**予算または人材の配分について十分であると感じている割合は４割弱**となっており、**セキュリティに関するリソースが十分でない**実態がうかがえる。また、**必要な人材・予算が不明確との事業者等が4分の１程度**あり、**サイバーセキュリティ人材像、必要なセキュリティ対策を明確化し**、**事業者等の取組を推進していく**ことが必要と考えられる。

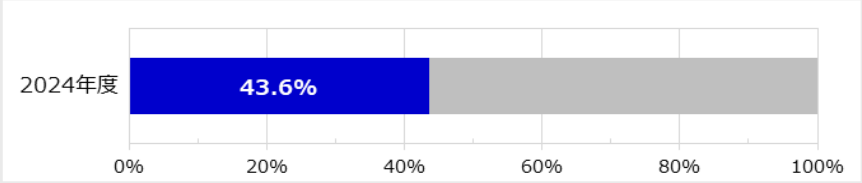
► **サイバーセキュリティリスク、インシデント等の情報について定期的なコミュニケーションを実施している**（設問5）
※金融分野（資金決済以外）を除く
※3.2.組織内外のコミュニケーション
（複数回答）



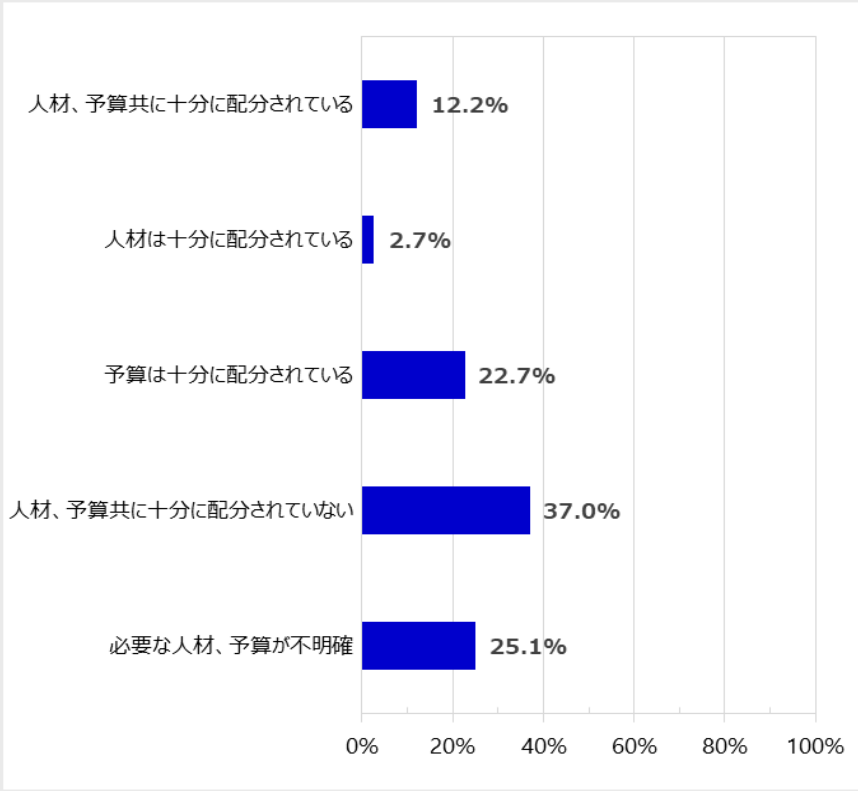
► **サイバーセキュリティリスクが経営リスクと認識され、セキュリティ方針の策定に経営層が関与している**（設問6）
※金融分野（資金決済以外）を除く
※3.3.経営リスクとしてのサイバーセキュリティリスクの管理



► **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13）
※金融分野（資金決済以外）を除く
3.7.情報開示



► **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10）
※金融分野（資金決済以外）を除く
※3.5.資源の確保

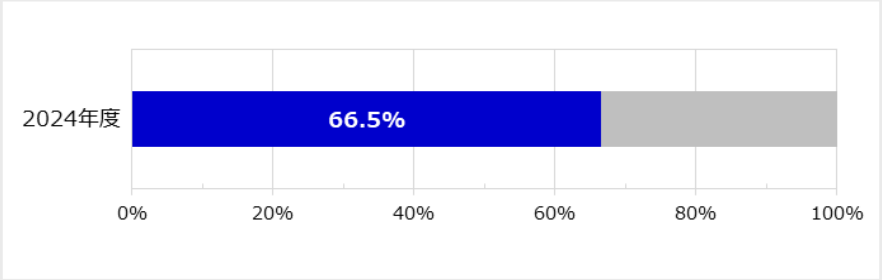


※設問に対応する「指針」の節等を記載

浸透状況と課題　－　リスクアセスメント、サプライチェーン

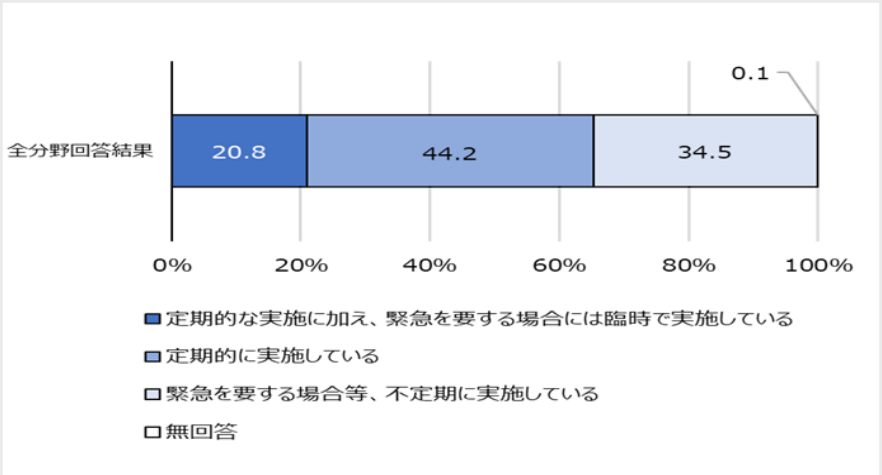
- **リスクアセスメントの実施状況は７割弱**となっている。また、リスクアセスメントを実施していると回答した事業者等のうち、**定期的に実施している割合は６割強**であった。事業者等による自主的かつ継続的なリスクアセスメントの実施を促進するために、**リスクアセスメント普及啓発セミナーの開催及びそのコンテンツの充実化などの継続的な改善取組**が必要である。
- 「自組織のサプライチェーンの把握」については**８割強が取組んでおり、サプライチェーンリスクに対する意識は高まっていると考えられる**。

► **リスクアセスメントを実施している**（設問17）　※4.2.リスクアセスメント



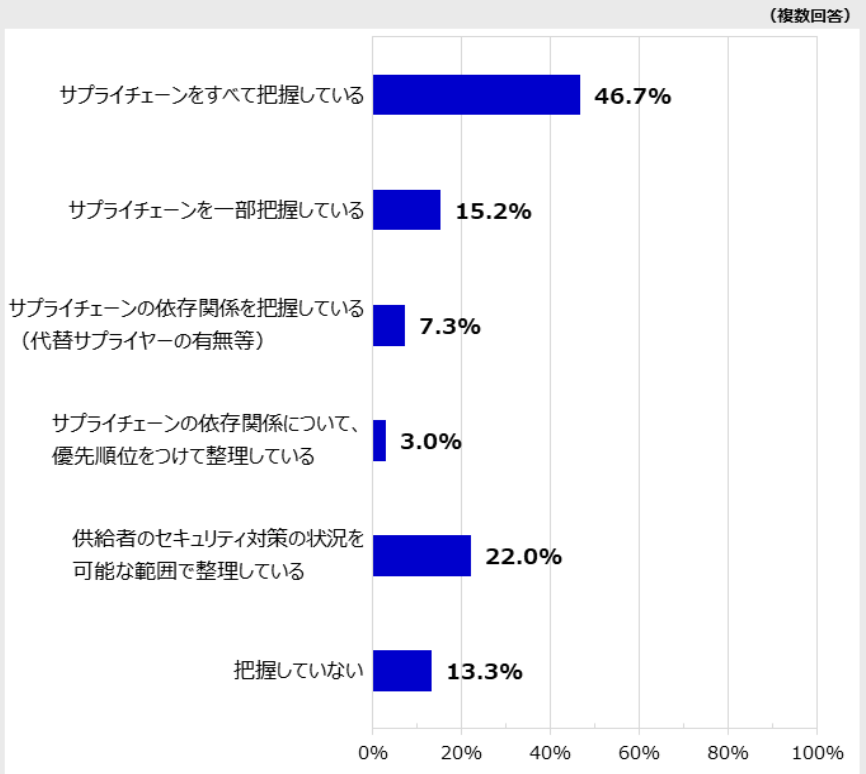
► **リスクアセスメントの実施状況**（設問20）　※4.2.リスクアセスメント

※金融分野（資金決済以外）を除く



► **自組織のサプライチェーン（一次取引先）を把握している**（設問23）

※金融分野（資金決済以外）を除く　※4.4.サプライチェーン・リスクマネジメント

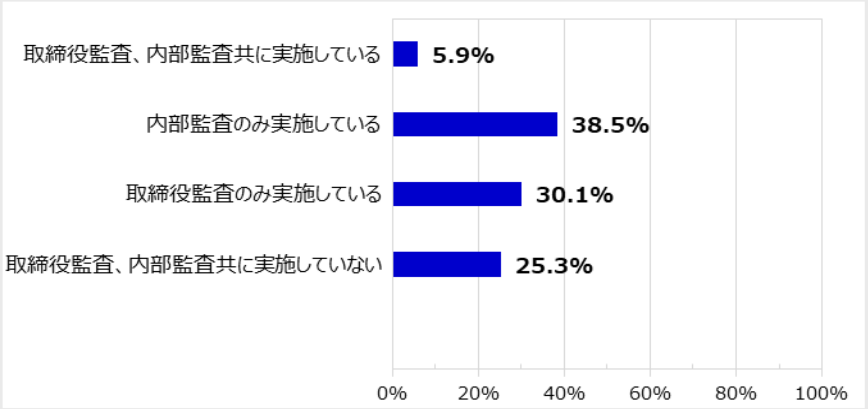


※設問に対応する「指針」の節等を記載

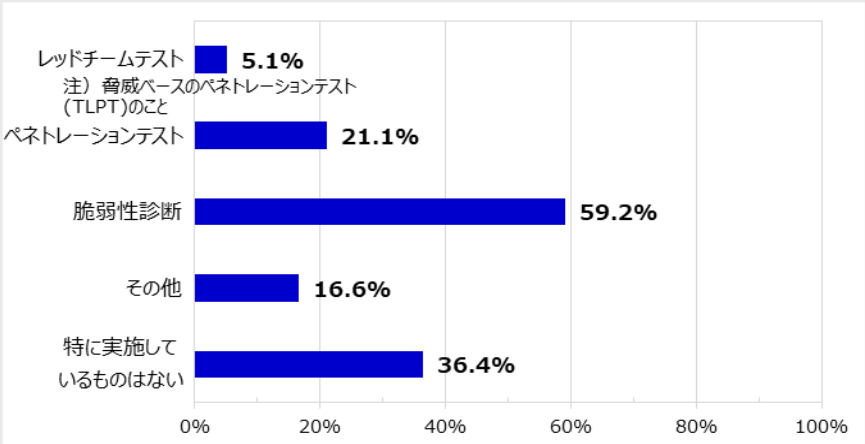
浸透状況と課題 － 評価、改善

- サイバーセキュリティ確保のための**監査の実施は、８割強の事業者等が行っており、監査については重要インフラ事業者等に浸透**している。
- **セキュリティ評価については、６割強の事業者等が実施**しているが、予算等が必要な対策であるので、主に中小規模の事業者等に対しては、取組**促進の支援策が必要**と思われる。
- 継続的な見直しについては、**８割以上の事業者が内規等の見直し**を行っている。引き続き、継続的な取組を実施していくことが重要と考える。

► **サイバーセキュリティに関する監査の実施状況**（設問11） ※3.6.監査・モニタリング

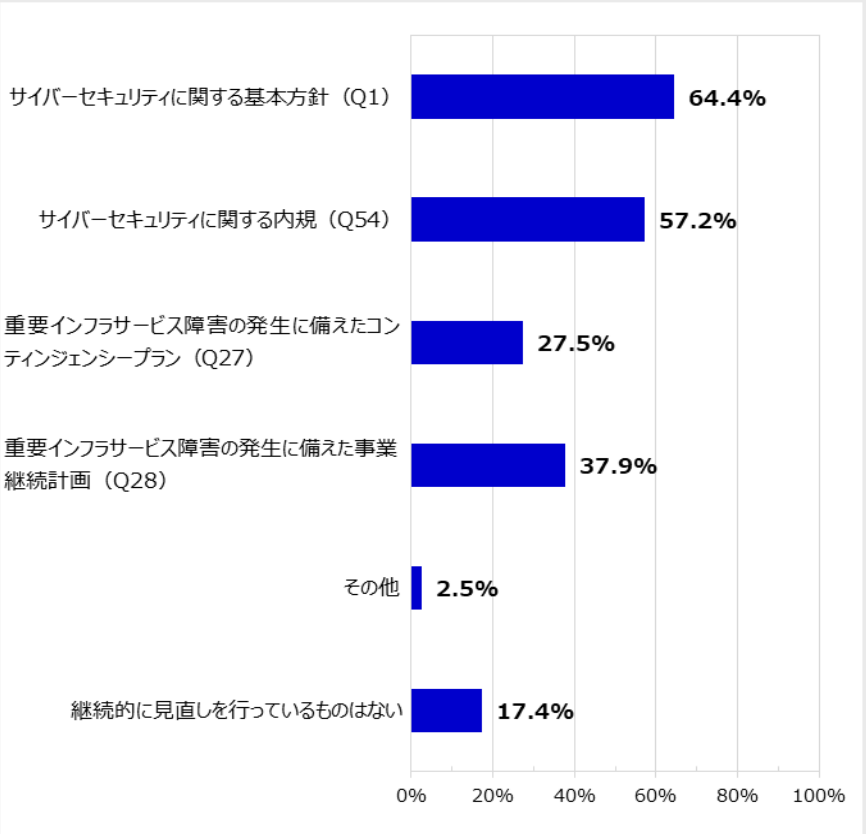


► **セキュリティ評価の実施状況**（設問12） ※3.6.監査・モニタリング （複数回答）



► **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**（設問57）

※金融分野（資金決済以外）を除く （複数回答）



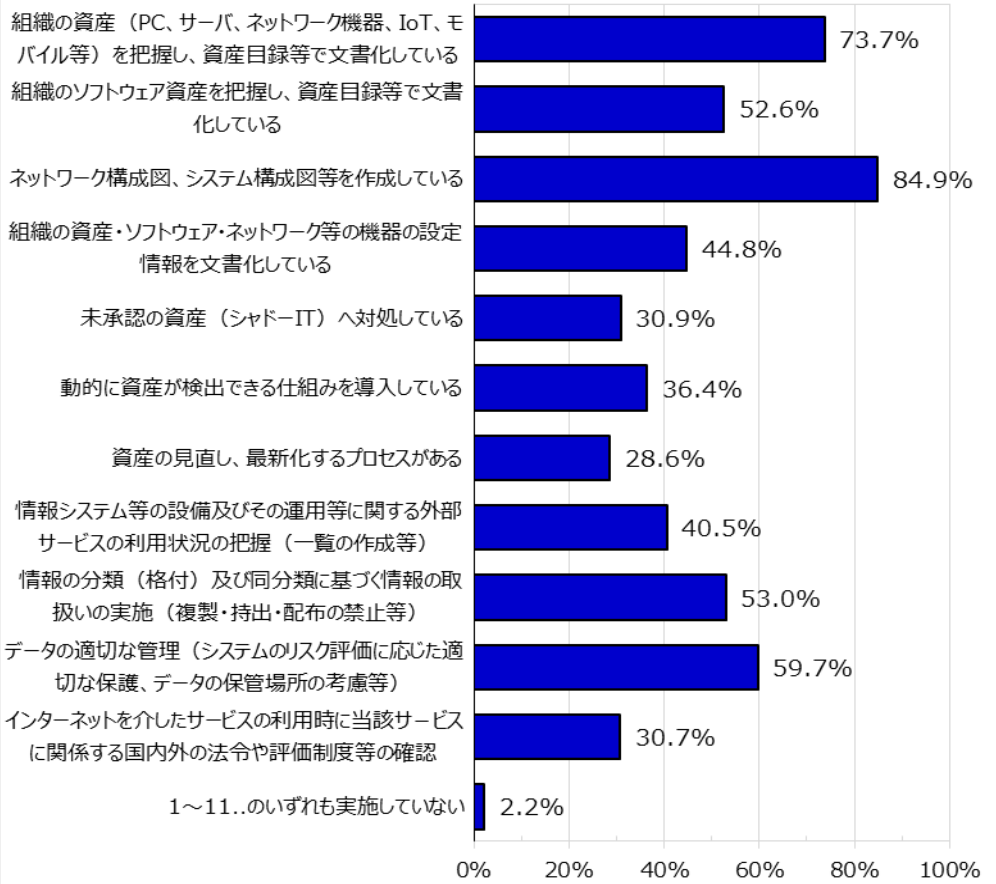
※設問に対応する「指針」の節等を記載

浸透状況と課題　－　技術的対策

- **資産管理については、ほぼ100%の事業者等が何らかの取組を実施**している。リスクアセスメントの元となる情報であるので、**基本的な対策として、引き続き事業者等に対して取組の推進を行っていく必要**がある。
- **脆弱性管理は、約85%の事業者等が実施**している。サイバー攻撃を防御するための基本的な対策であるため、脆弱性管理についても、**基本的な対策として、事業者等に対して取組の推進を行っていく必要**がある。

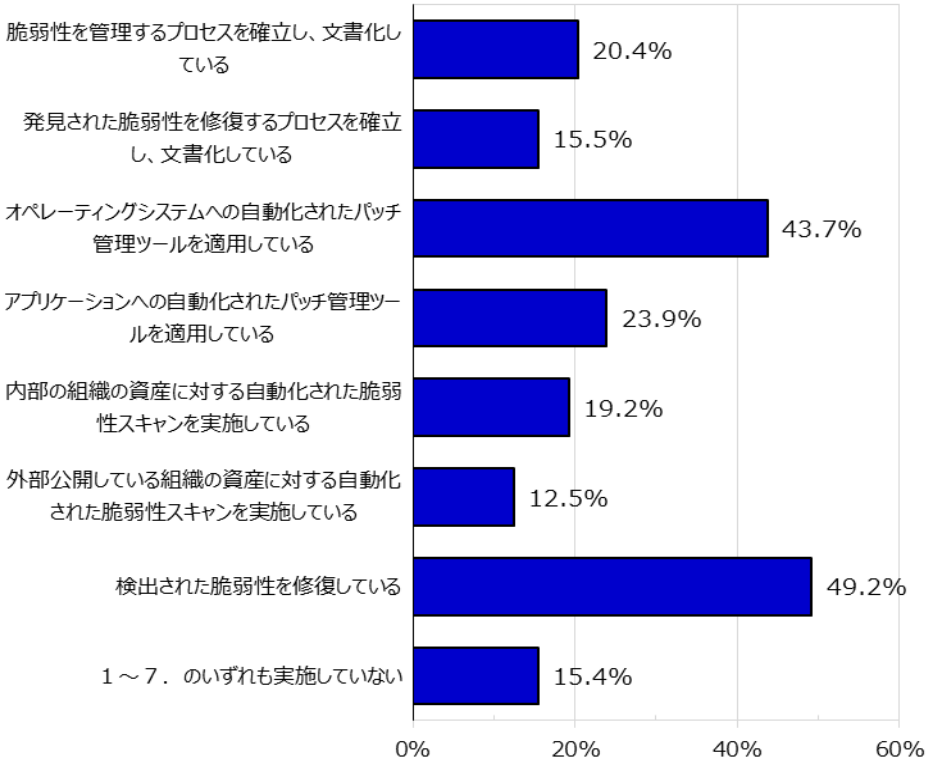
► 資産管理について実施している取組（設問37）

※金融分野（資金決済以外）を除く　※5.1.組織的対策　（複数回答）



► 脆弱性管理について実施している取組（設問43）

※金融分野（資金決済以外）を除く　※5.1.組織的対策　（複数回答）



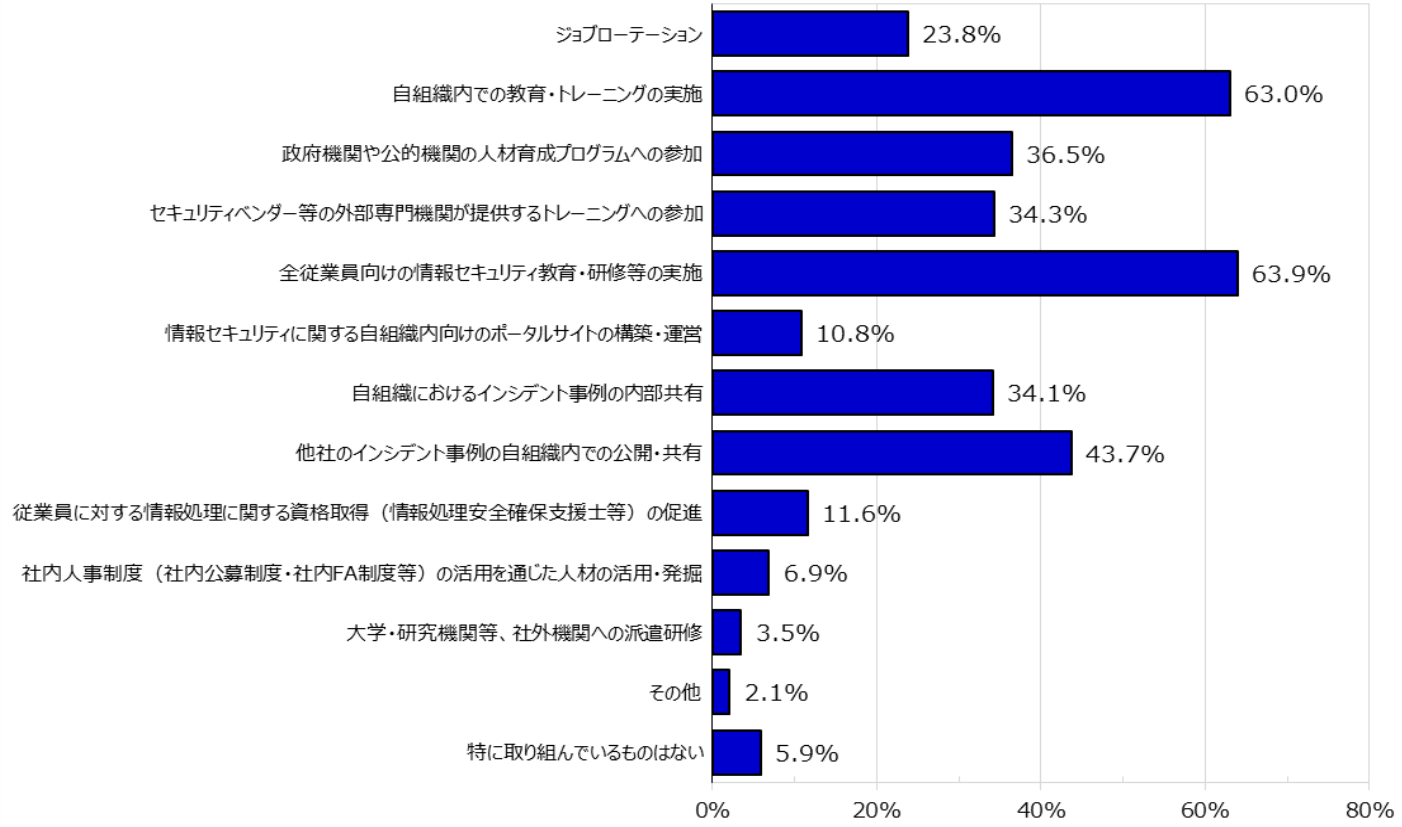
※設問に対応する「指針」の節等を記載

- **人材育成への取組は９割強の事業者等が実施**しており、事業者等に浸透していると考えられる。
- 制御システム・OTについて、**重要インフラ事業者等の３割強程度が、OT資産を保有・運用**している状況である。実施しているセキュリティ取組については、インターネットに面しない領域への制御システム・OTの設置が最も多いが、昨今の攻撃事例を考慮すると、**システム監視等のためのITとの接続や保守業者による外部記憶媒体を使ったメンテナンス等の機会があるとの認識で、今一度システム構成等の確認が必要**と思われる。

► 人材育成の取組（設問29）

※5.5.動向を踏まえた対策

（複数回答）

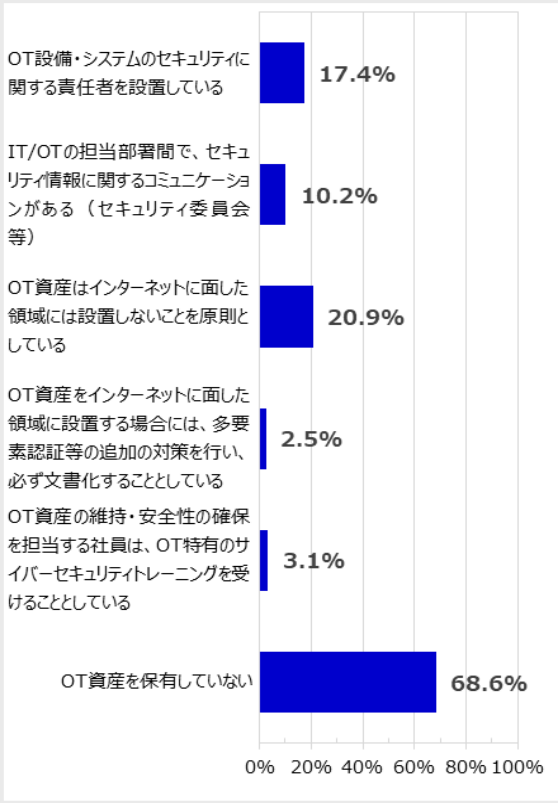


► 制御システムを保有している場合、実施している取組（設問53）

※該当なし

※金融分野（資金決済以外）を除く

（複数回答）



※設問に対応する「指針」の節等を記載

自由意見①

- セキュリティ対策を実践できない理由、及びセキュリティ取組において苦慮している点としては、**人材不足がもっとも多く、続いて、知識・予算の不足**があげられた。（設問61、63）
- 有効であると感じられる対策としては、**教育・訓練の実施、組織・体制の整備、技術的対策の実施**をあげる事業者等が多かった。（設問62）

設問61.【自由記述】
選択肢の中で、セキュリティ対策を実践できていない、と回答いただいた設問において、その理由を記載してください。

記載：230件

（※１社で複数回答は別々に集計）
（※「特に無し」は除く、
代表的な意見のみ集計）

内容	件数
人材不足のため	74 件
セキュリティに関する専門知識を持つ人材がいない、または知識不足のため	37 件
予算不足のため	28 件
組織体制の不備による（例：担当する部署がない）	20 件
セキュリティ対策の優先順位が低いため	12 件
システム環境による（例：外部ネットワークに接続していない）	10 件
AI関連の理由（例：AIの利用に関するルールが未整備）	9 件
規定・ルールの不備のため	8 件
セキュリティを外部委託しており、自組織での対応ができない等	6 件
その他	26 件

■代表的な意見（抜粋）

○その他
・インシデントが発生していないので、現時点では必要性を感じていない
・業務が多忙で、セキュリティ対策に手が回らない
・必要性は分かっているが、対策の方法がわからないため先送りになっている

自由意見②

設問62.【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。

記載：88件

（※１社で複数回答は別々に集計）
（※「特に無し」は除く、
代表的な意見のみ集計）

内容	件数
教育・訓練について	16 件
組織・体制について	13 件
技術的対策について	12 件
監査・評価について	9 件
ルール・ガイドラインについて	8 件
その他	12 件

■代表的な意見（抜粋）

○教育・訓練について
・外部からの攻撃メールを装った訓練メールを送付し、開いた職員に研修を実施
・eラーニング教材によるDX・ICTリテラシー研修への参加

○組織・体制について
・各組織ごとに「デジタルリーダー」を配置
・何かシステムに異変を感じたら、どんな些細なことであっても（自身の勘違いであっても）、気軽に担当者へ連絡しても構わないという意識付け、環境の構築

○技術的対策について
・EDRの導入を計画している

○ルール・ガイドラインについて
・業務よりも、セキュリティを優先する運用ポリシーとしている

○その他
・毎日の声掛け

自由意見③

設問63.【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。

記載：219件

（※１社で複数回答は別々に集計）
（※「特に無し」は除く、
代表的な意見のみ集計）

内容	件数
人材不足（専門知識を持つ人材の不足、育成の困難さ、採用の難しさ）	54 件
中小企業・地方自治体の困難さ（リソース不足、大企業との格差、地域による格差）	35 件
知識・意識不足（職員のセキュリティ意識が低い、リテラシー向上が困難、研修の効果が低い）	32 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）	31 件
技術的な課題（高度な技術への対応が困難、システム運用に関するノウハウ不足、外部委託先の管理）	26 件
組織的な課題（経営層の理解不足、組織内での優先度の低さ、担当部署の不在）	23 件
情報収集の困難さ（最新情報への追随が困難、他組織の事例が不明、ガイドラインの理解不足）	21 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）	14 件
業務との両立の難しさ（利便性との両立が困難、業務フロー変更への抵抗、業務負担の増加）	12 件
外部への依存（海外製品への依存、ベンダーへの依存）	6 件

■代表的な意見（抜粋）
・サイバーセキュリティ対策強化はどの程度まで実施すれば良いか、基準が難しい
・特にセキュリティ意識が低い方へのフォロー、より分かりやすい平易な言葉で書かれたセキュリティ対策に係る資料提供をお願いしたい
・本アンケートの他社動向を把握したいと考えているため、実施結果や分野における分布などの開示をお願いしたい

資料３－２

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39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について（別冊）［2024年度］

令和７年６月
内閣サイバーセキュリティセンター
制度総括班

2024年度調査設問の構成（設問一覧）

□ 組織統治におけるサイバーセキュリティ

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　要求事項の文書化
設問４　安全基準等の把握
設問５　定期的なコミュニケーション
設問６　経営リスクとしてのサイバーセキュリティ
設問７　責任・権限の割当
設問８　責任・権限の割当に対する取組
設問９　役職・担当者の設置
設問10　人材や予算の配分
設問11　監査の実施
設問12　サイバーセキュリティ評価の実施
設問13　情報開示の基準
設問14　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の活用と危機管理

設問15　外部環境・内部環境の整理
設問16　任務保証を踏まえた自組織の特性把握
設問17　リスクアセスメントの実施
設問18　実施しているリスクアセスメントの方法
設問20　定期的なリスクアセスメントの実施
設問21　制御システムのセキュリティ確保
設問22　セキュリティ対策検討の際の対応状況
設問23　サプライチェーンの把握
設問25　認識しているサプライチェーンリスク
設問26　実施しているサプライチェーンリスク軽減策
設問27　コンティンジェンシープランの策定
設問28　事業継続計画の策定
設問29　人材育成・意識啓発
設問31　リスク対応計画の実施状況
設問32　情報共有や意見交換を行っている関係主体
設問34　活用している情報提供元
設問35　演習・訓練

□ 組織的対策

設問37　資産・情報・データ等の管理
設問38　供給者管理
設問39　マルウェアからの保護
設問40　バックアップ
設問41　ログ管理
設問42　運用ソフトウェアの管理
設問43　脆弱性管理
設問44　システムの取得・開発及び保守
設問45　インシデント管理

□ 人的対策

設問46　人的資源及び外部委託

□ 物理的対策

設問47　物理的及び環境的セキュリティ

□ 技術的対策

設問48　アカウント管理
設問49　アクセス制御
設問50　暗号技術
設問51　通信のセキュリティ
設問52　電子メールの対策
設問53　制御システムに関する取組

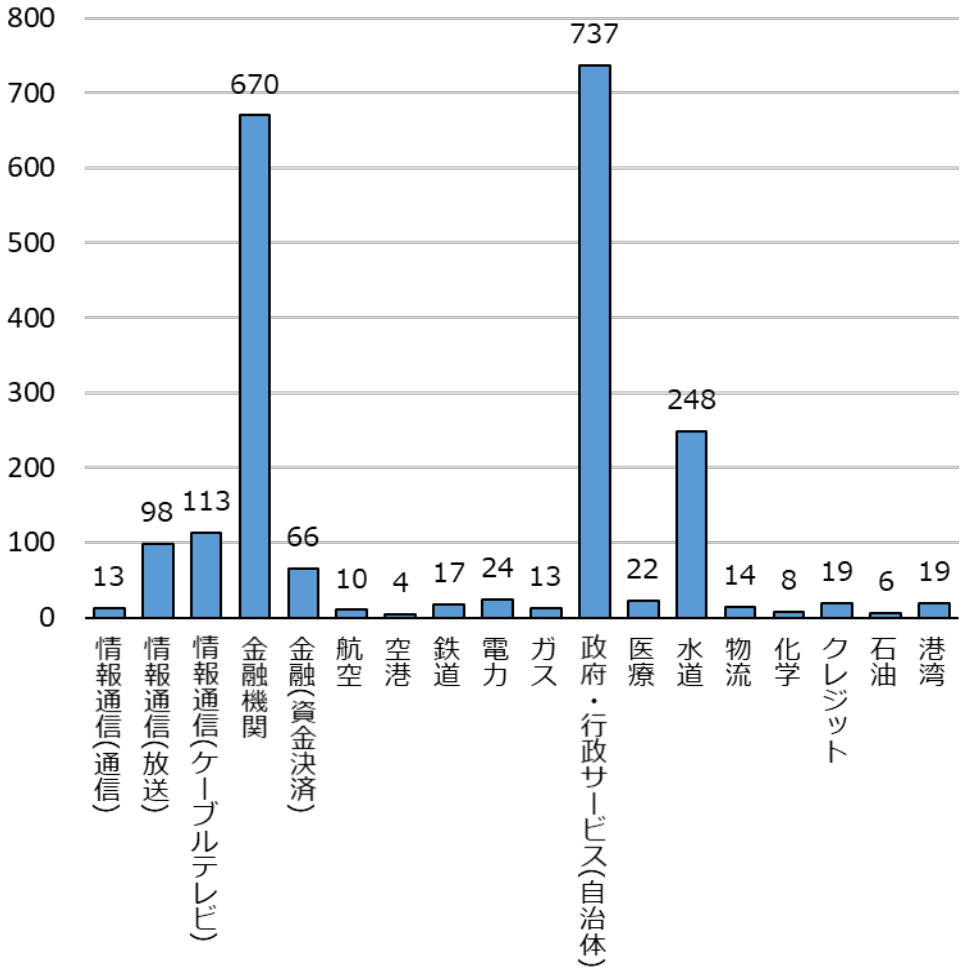
設問54　各対策項目で実践しているセキュリティ管理策を内規として整備

設問55　クラウドサービス提供事業者への確認事項
設問56　クラウドサービス利用に関する運用対策
設問57　取組改善に向けた、継続的な見直し項目

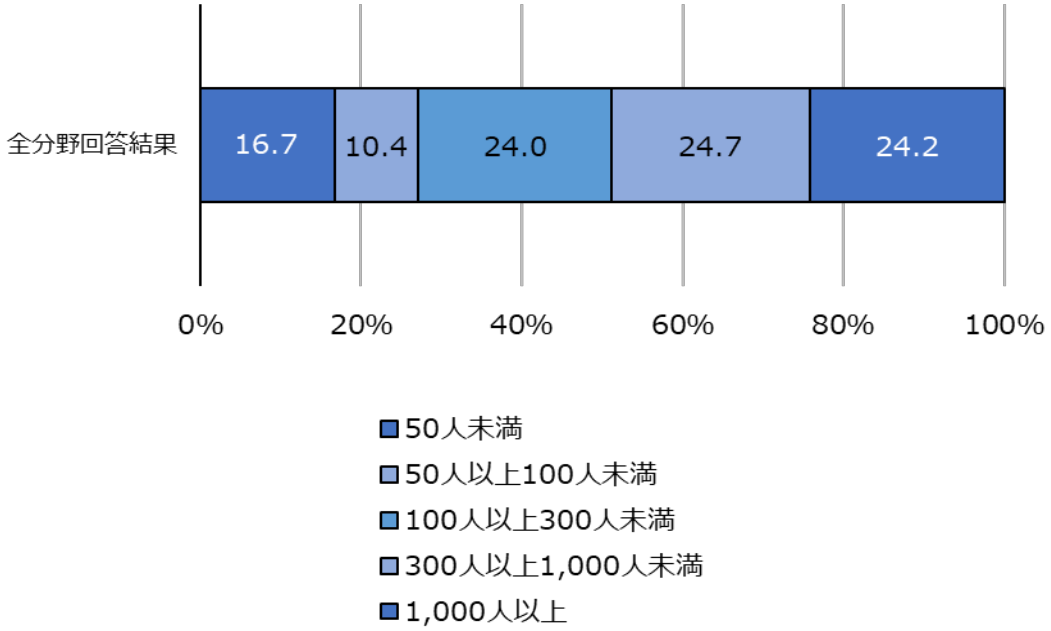
※設問番号の欠番は基礎情報（分野名、従業員数）及び、
各設問に付記した自由記述による回答

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）

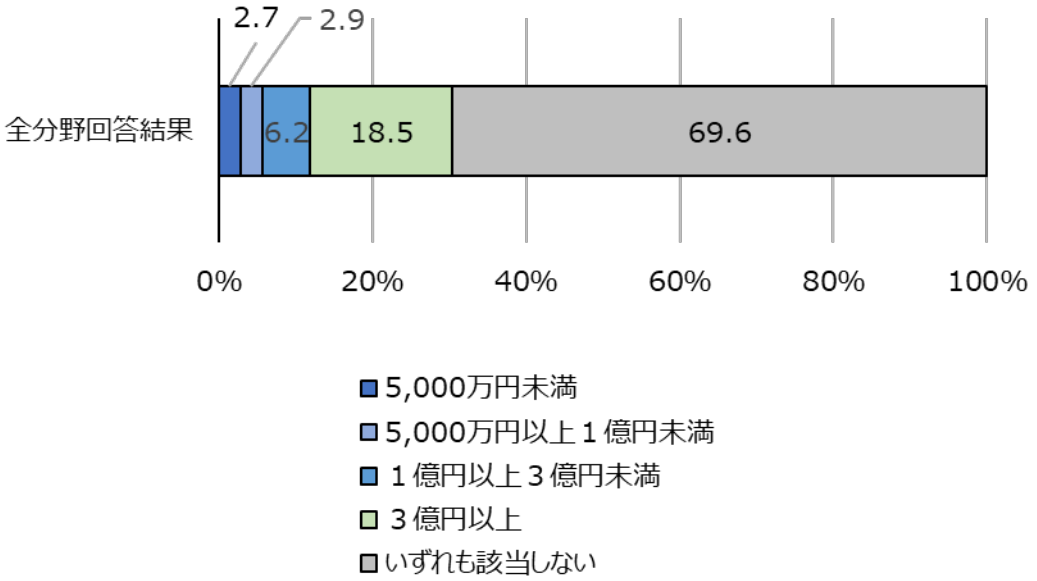


Ⅰ.【単一回答】
貴社（又は貴団体）の従業員数



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）

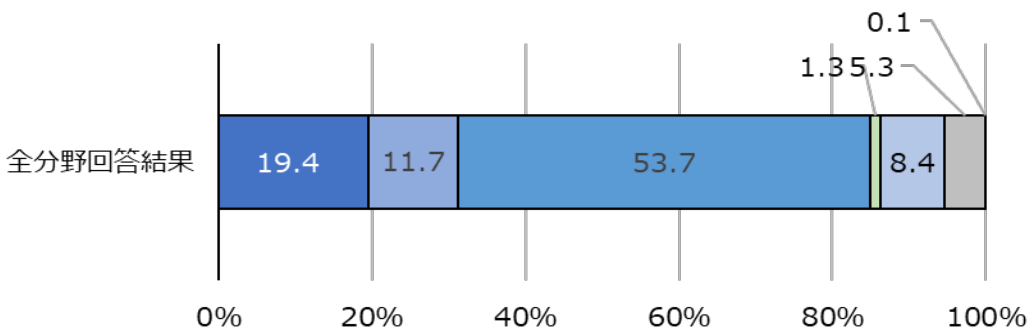


アンケート調査結果

設問１．【単一回答】
組織方針（経営方針、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。

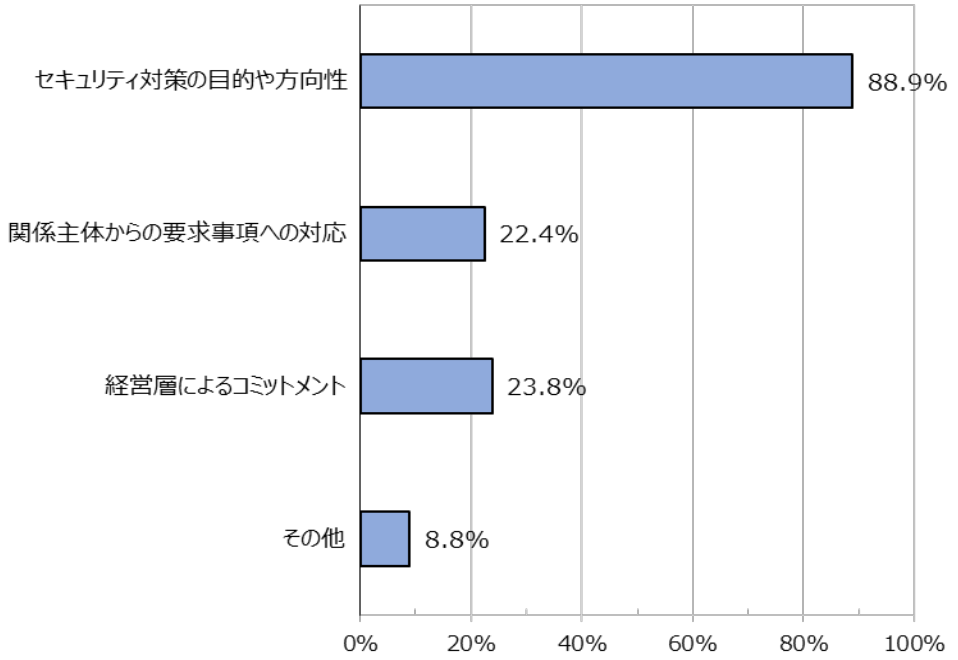
※ 例）「サイバーセキュリティに対する脅威からの被害がサービス提供を阻害するリスクの一つである」
「リスクマネジメントの対象としてサイバーセキュリティに関する事項を含める」

※金融を含む



- 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２．【単一回答】
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。

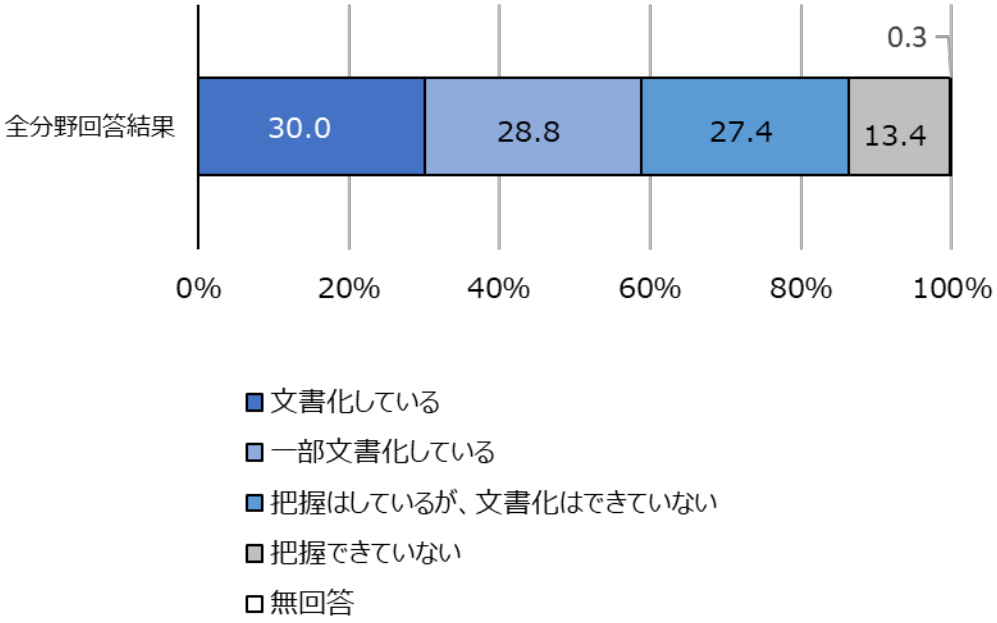


■「その他」（一部抜粋）
・対象とする脅威、職員の遵守義務、組織体制、情報セキュリティ対策、監査等
・サイバーセキュリティ方針自体を策定していない
・セキュリティマニュアルが未整備
・具体的な内容を現在策定中

アンケート調査結果

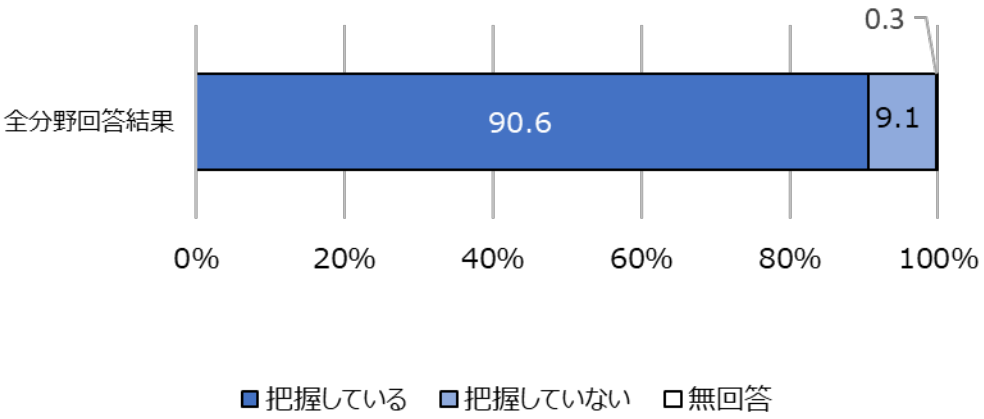
設問３．【単一回答】
関係省庁、顧客、サプライヤー、委託先等からの、サイバーセキュリティに関する自組織への要求事項※を文書化していますか。

※各事業分野の関係法令、ステークホルダーとの契約等に規定された義務、サプライヤーや委託先が提示する制限事項等



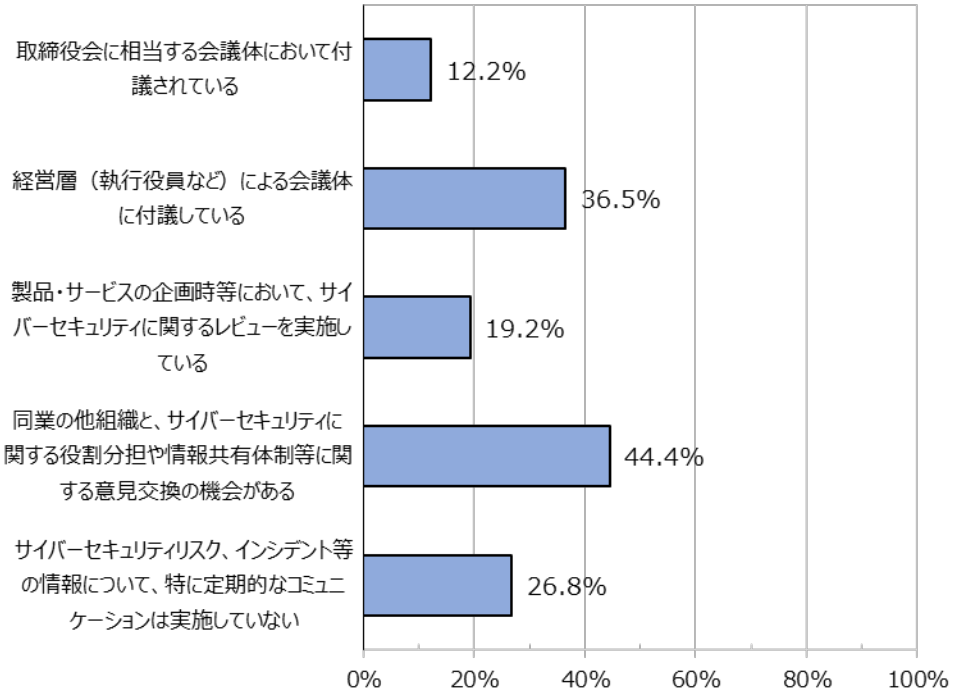
設問４．【単一回答】
自組織に関係する安全基準等※を把握していますか。

※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



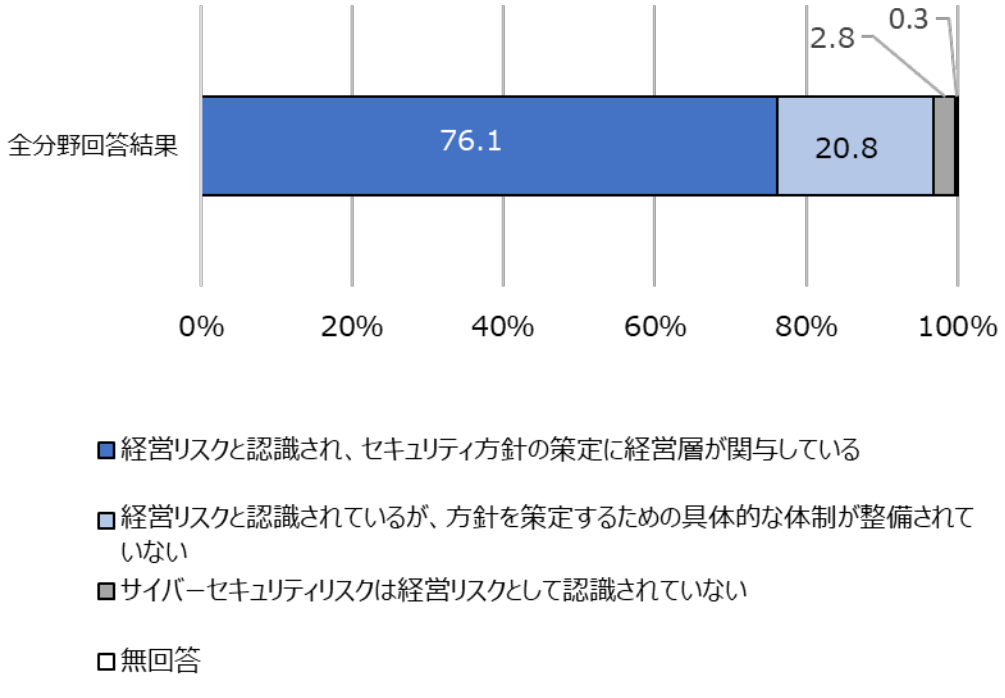
アンケート調査結果

設問５．【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。



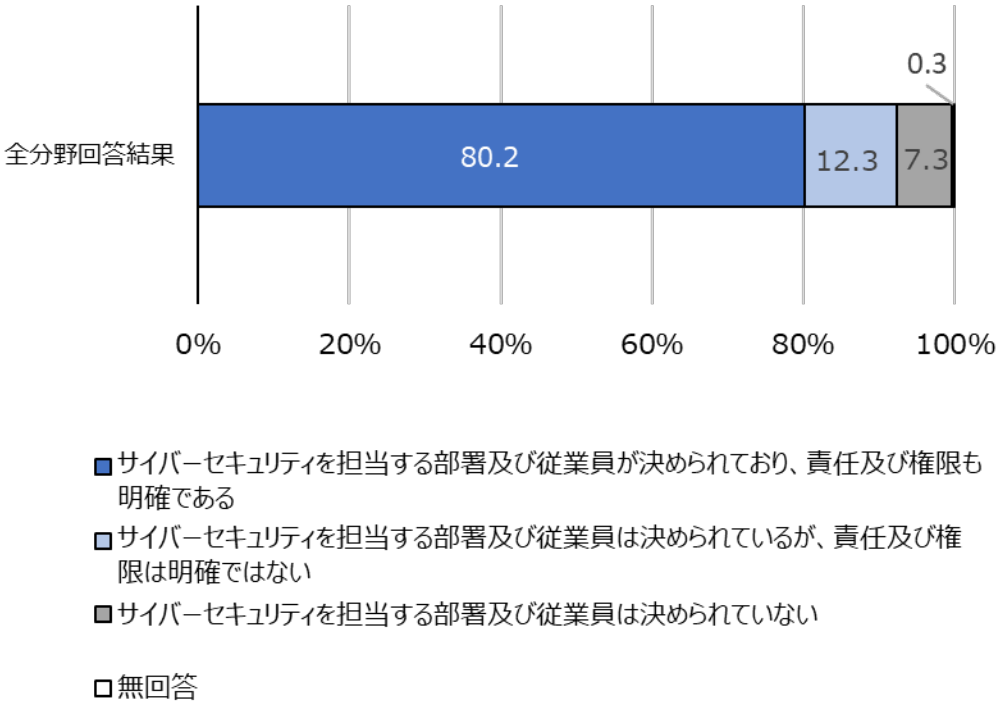
設問６．【単一回答】
サイバーセキュリティリスク（※1）が経営リスク（※2）と認識されていますか

※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

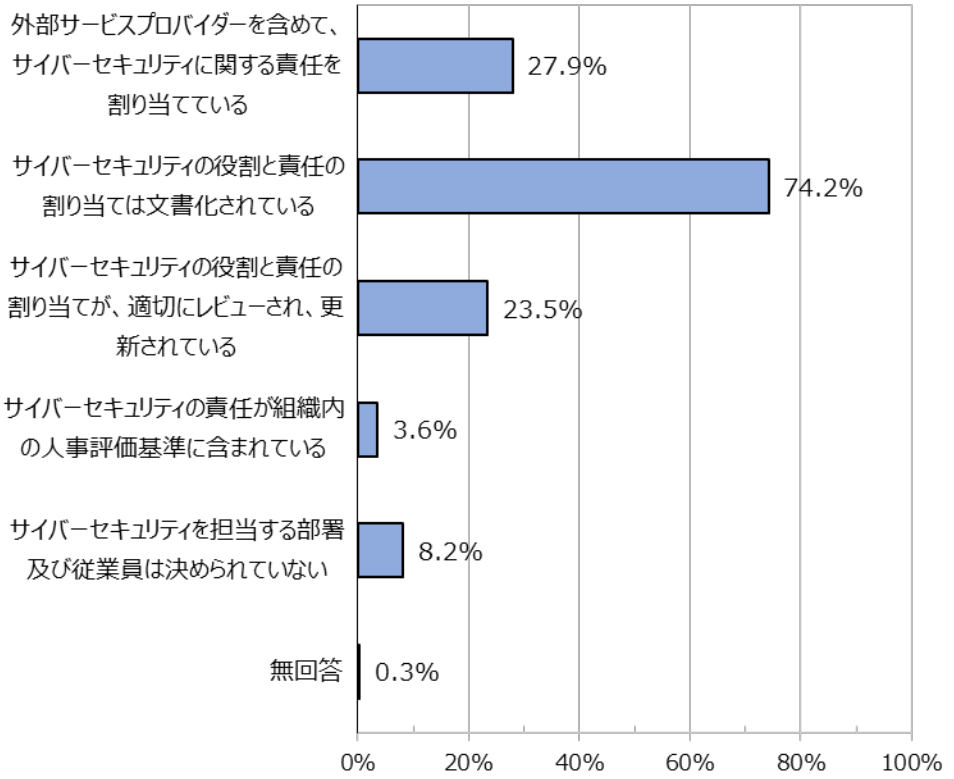


アンケート調査結果

設問７．【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。

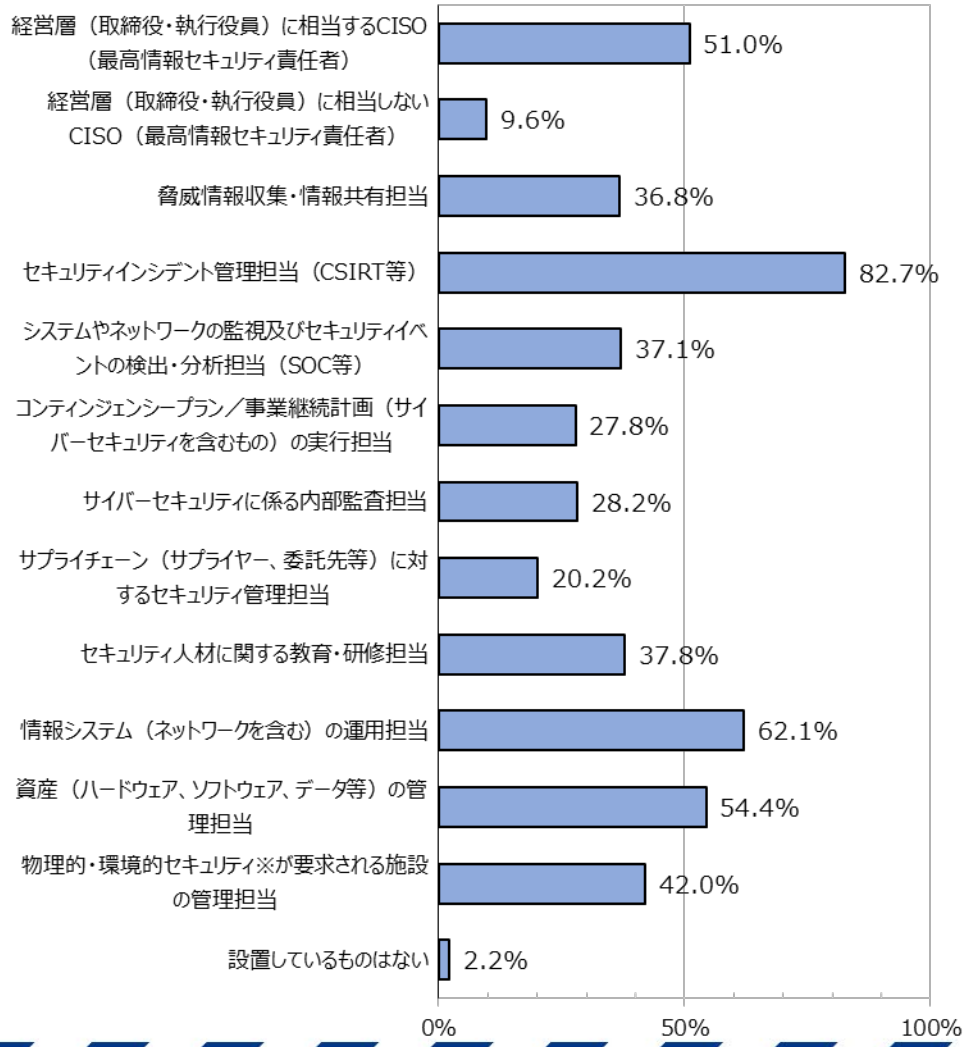


設問８．【複数回答】
サイバーセキュリティにおける責任及び権限の割り当てに関して、実施している取組を選択してください。

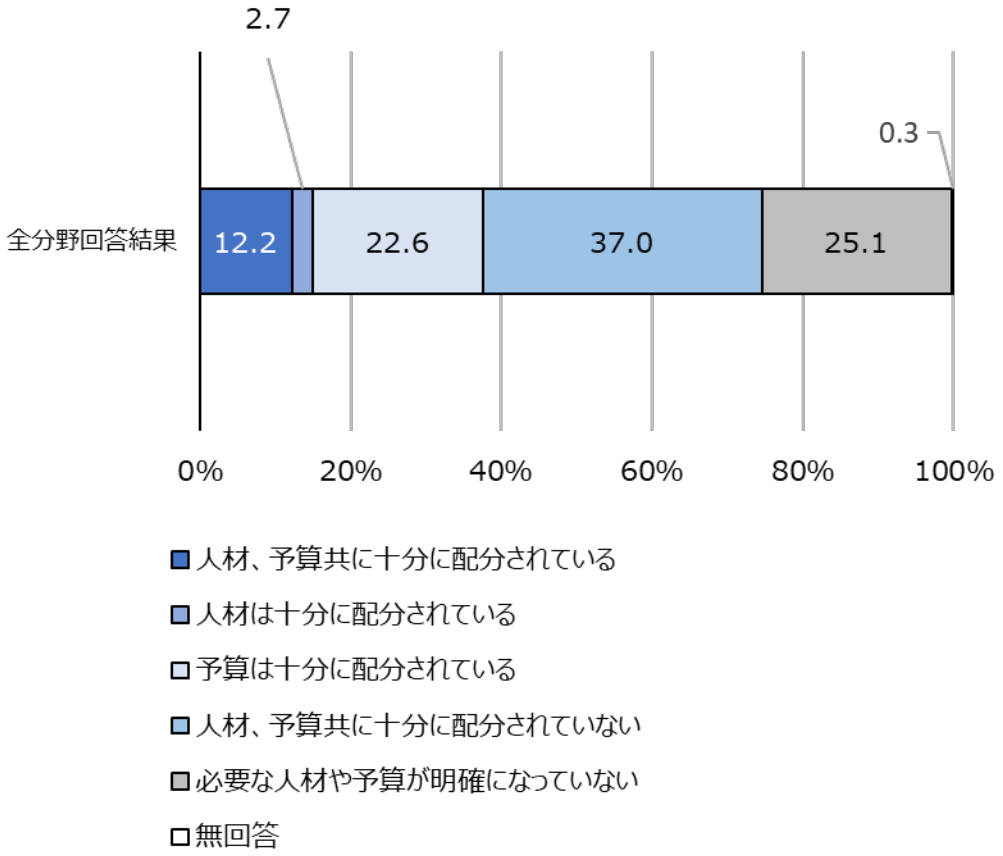


アンケート調査結果

設問９．【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）



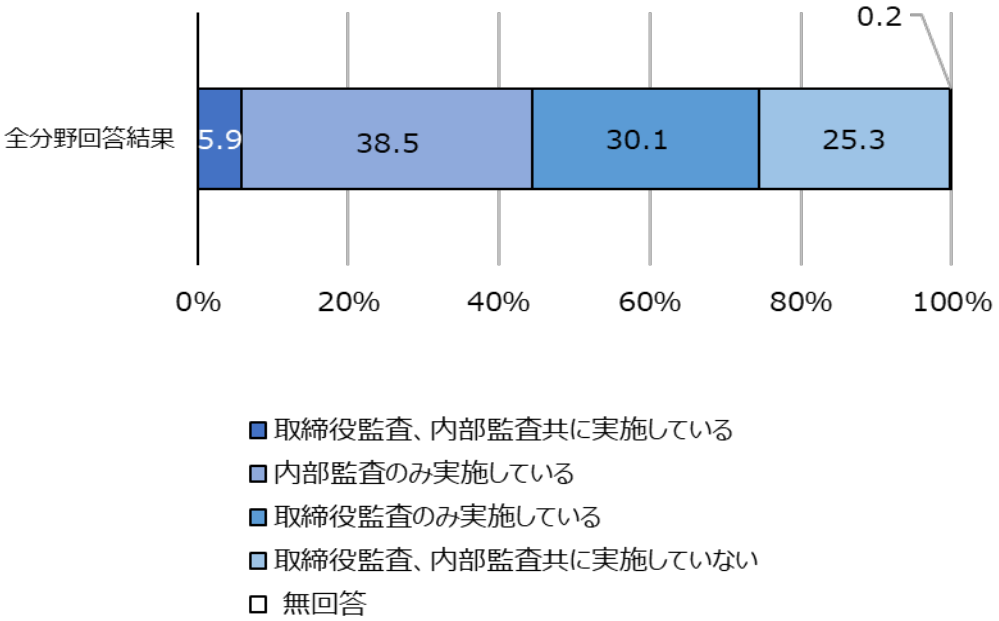
設問10.【単一回答】
サイバーセキュリティの確保に必要となる人材や予算が明確化され、組織内に適切に配分されていると感じますか。



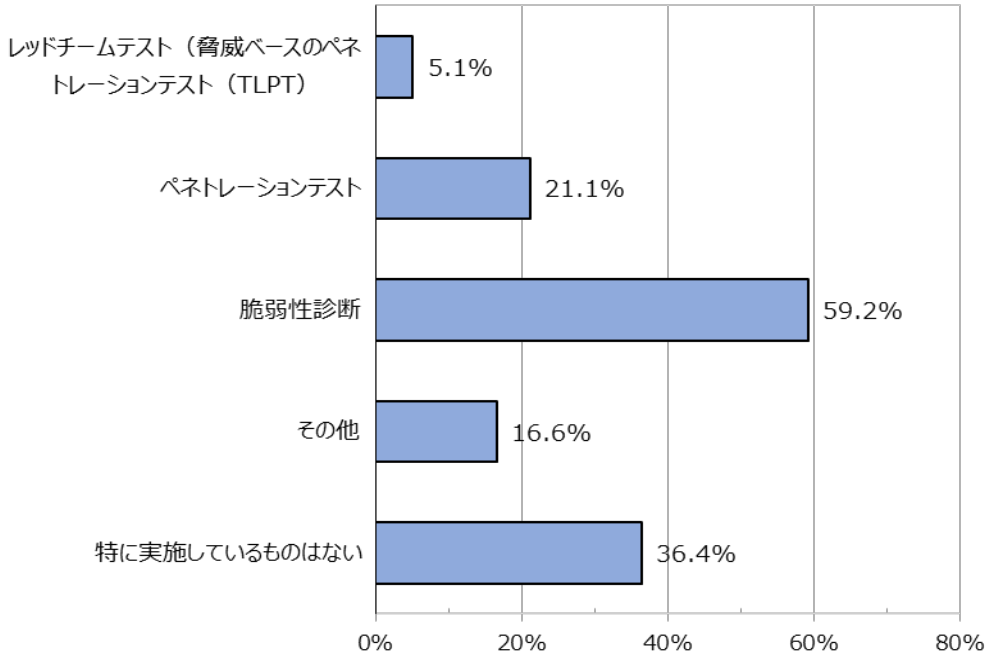
アンケート調査結果

設問11.【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。
（※全金融分野を含む）

※セキュリティ目標達成状況や、計画の進歩のほか、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



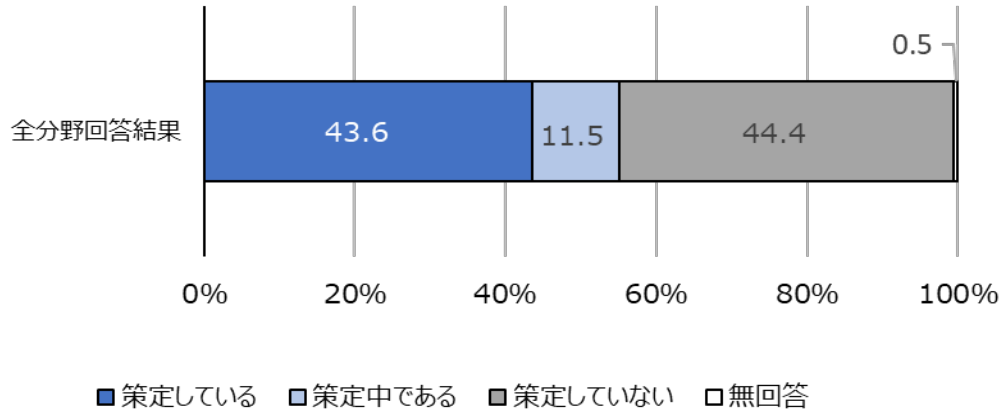
設問12.【複数回答】
自組織にて実施しているセキュリティ評価を全て選択してください。
（※全金融分野を含む）



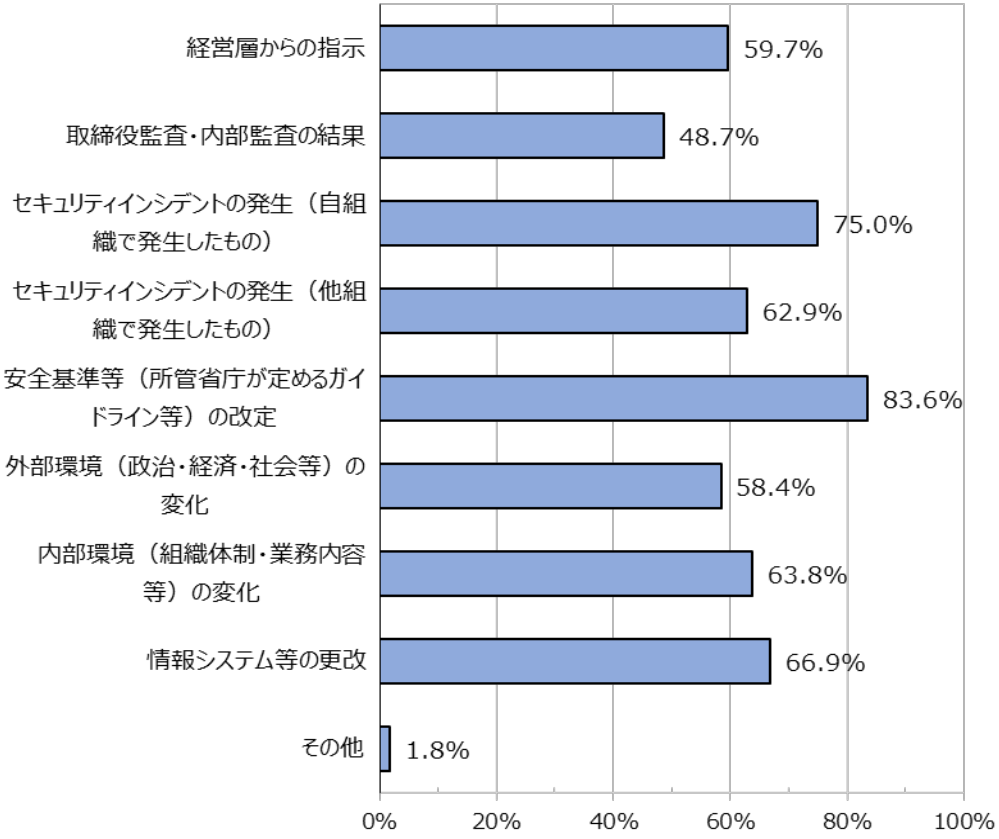
■「その他」（一部抜粋）
・標的型攻撃メール訓練
・独自に作成したチェックリスト
・資格をもった外部の監査人による監査や、内部職員で実施する監査を実施
・全職員を対象とした情報セキュリティ研修（テスト）を実施
・自治体で定めるセキュリティ内部監査基準
・組織内において、セキュリティ監査及び自己点検を実施

アンケート調査結果

設問13.【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。



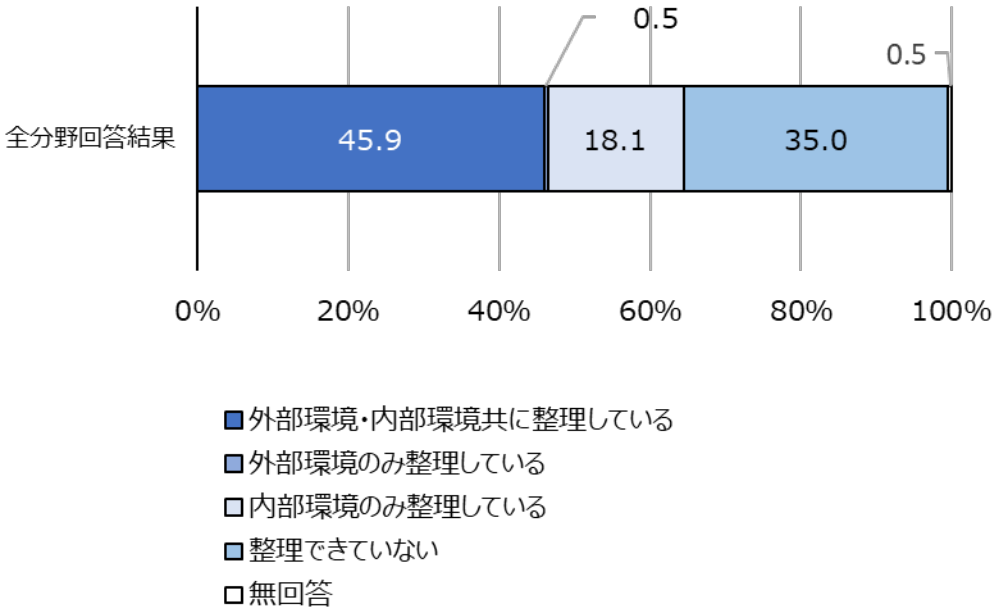
設問14.【複数回答】
サイバーセキュリティ確保の取組の見直しの契機となるものを全て選択してください。



■「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
・親会社の基準に基づく指示

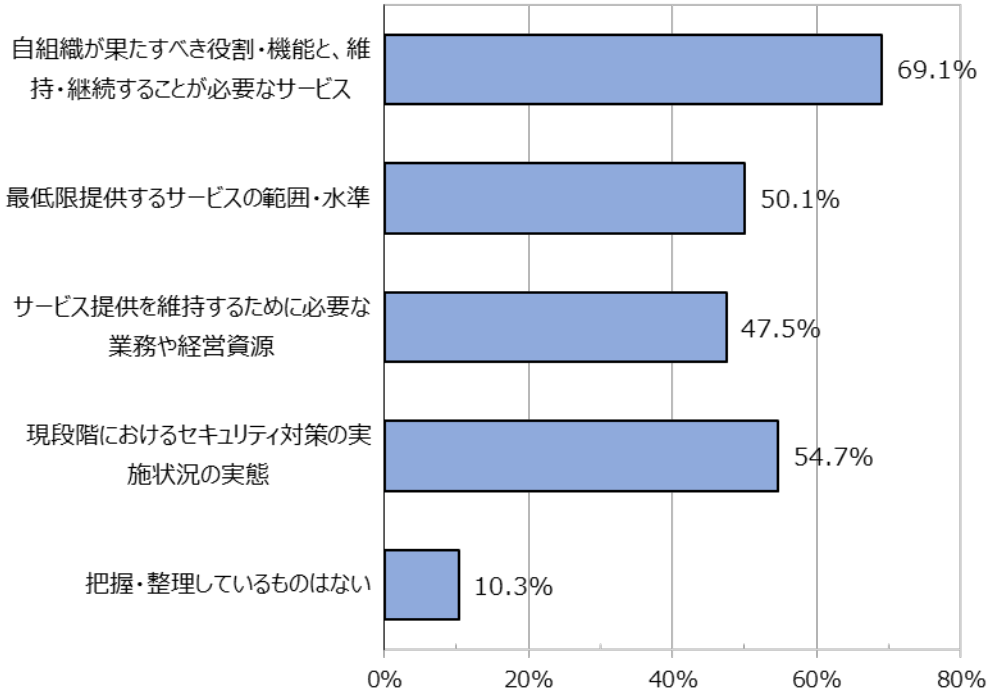
アンケート調査結果

設問15.【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。



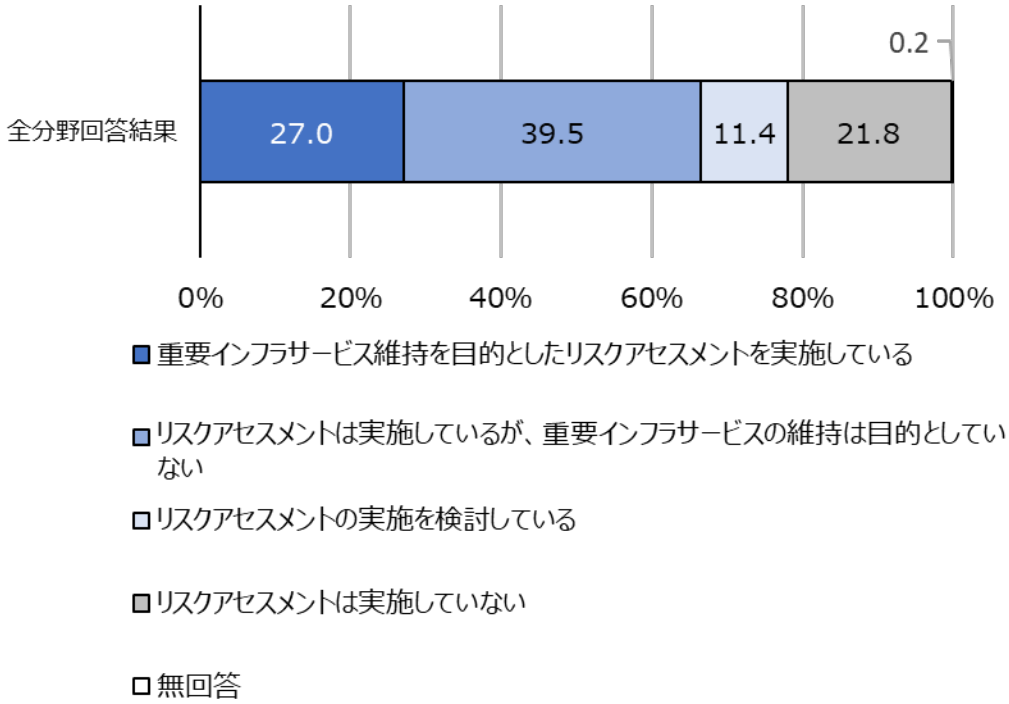
設問16.【複数回答】
任務保証※の観点から、以下の自組織の特性について整理し、把握しているものを選択してください。

※「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。」

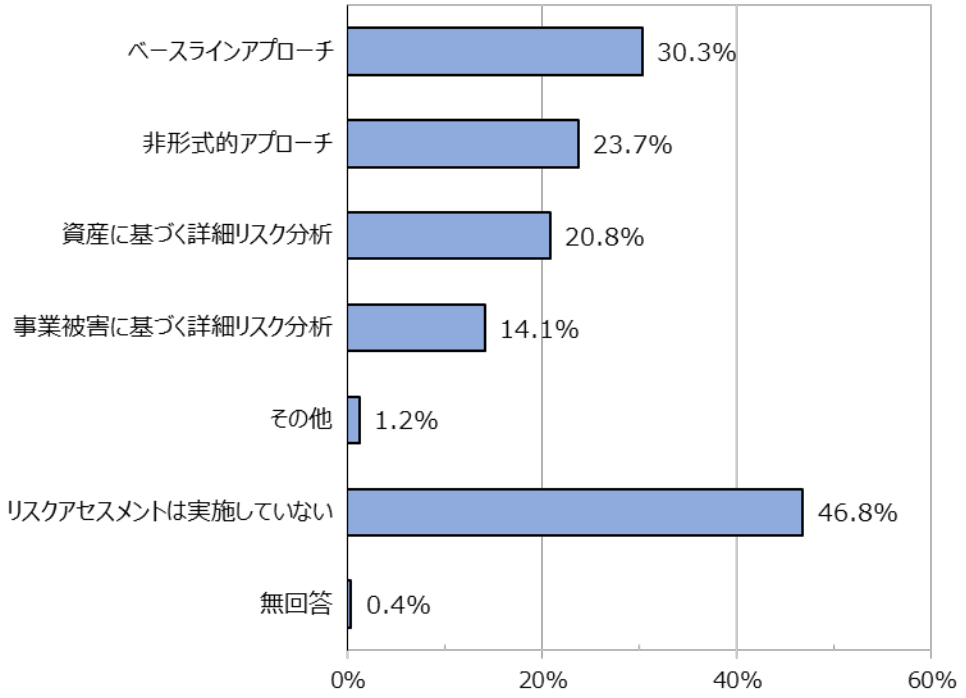


アンケート調査結果

設問17.【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。**（※全金融分野を含む）**



設問18.【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。



アンケート調査結果

設問19.【自由記述】
アセスメント手法や、実施する際に参考としてしてガイドライン等があれば記載してください。

記載：145件

■代表的な意見（抜粋）

・個人情報の保護に関する法律についてのガイドライン（通則編）、電気通信事業における個人情報等の保護に関するガイドライン、放送受信者等の個人情報保護に関するガイドライン

・ISO27001、ISO27002、ISO27005

・総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」

・特定個人情報の適正な取扱いに関するガイドライン特定個人情報保護評価指針

・IPA／制御システムのセキュリティリスク分析ガイド 第2版

・内閣サイバーセキュリティセンター「機能保証のためのリスクアセスメント・ガイドライン」

・金融機関等コンピュータシステムの安全対策基準・解説書（第12版）

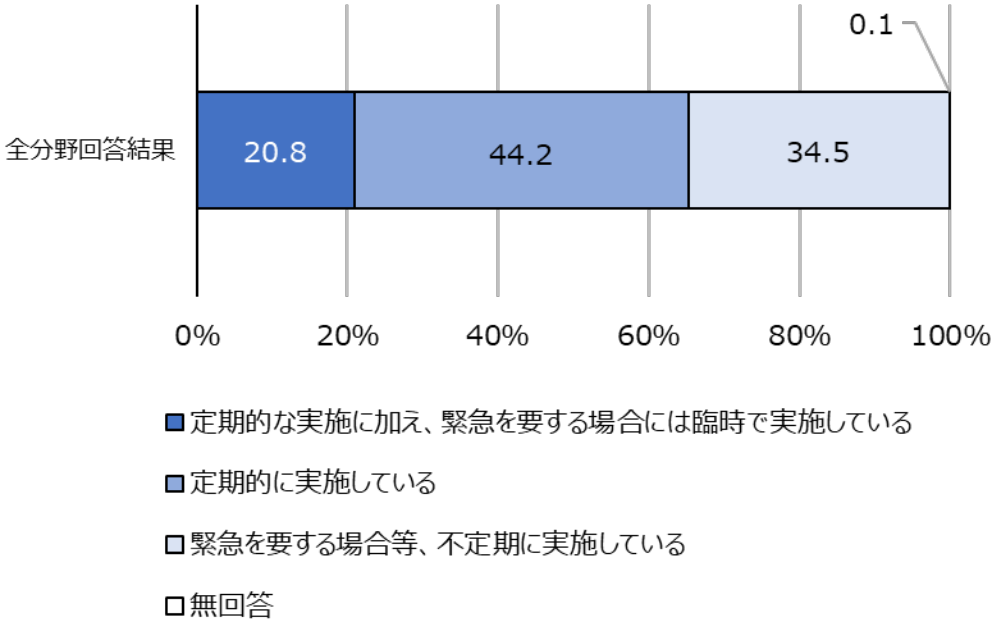
・水道分野における情報セキュリティガイドライン（第４版）

・都市ガス製造・供給に係る監視・制御系システムのセキュリティ対策要領及び同解説

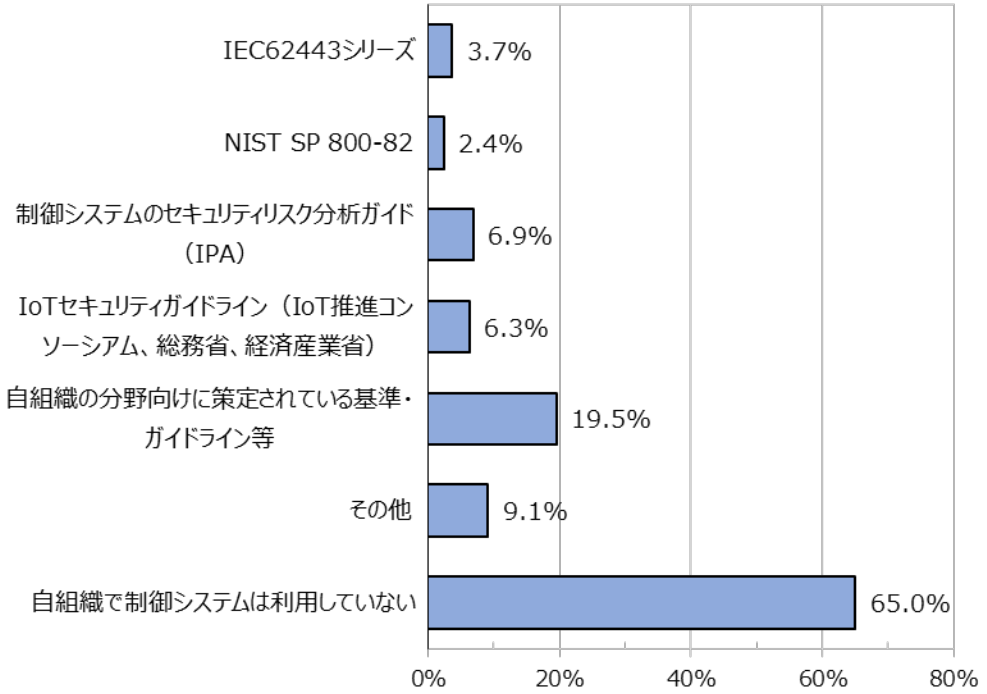
・CRI Profile

アンケート調査結果

設問20.【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21.【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。



Q：臨時もしくは不定期に実施する際の起点となるものは？【自由記述】
（記載419件）
・「インシデントが発生したとき」が突出して多く（269件）、その他では、

・当社にも当てはまる重大な事故が発生した場合
・オリンピックやG７など、大きなイベントが開催される時
・CSIRTメンバーの変更時　など

アンケート調査結果

設問21.【自由記述】
設問21で、「その他」を選択した場合の理由

記載：127件

■代表的な意見（抜粋）　※個社名や個社の製品名が記載された意見は除く

・ネットワークの冗長構成。その他外部サービスのハードウェア冗長構成等

・セキュリティベンダーからの情報提供等

・全庁的なセキュリティポリシーや業務継続計画など

・電力制御システムセキュリティガイドライン

・納入業者独自で、必要と思われる対策（VPN接続サービス利用及び施設の施錠管理）を行っているのみ

・NERC-C1P、ISO27000シリーズ

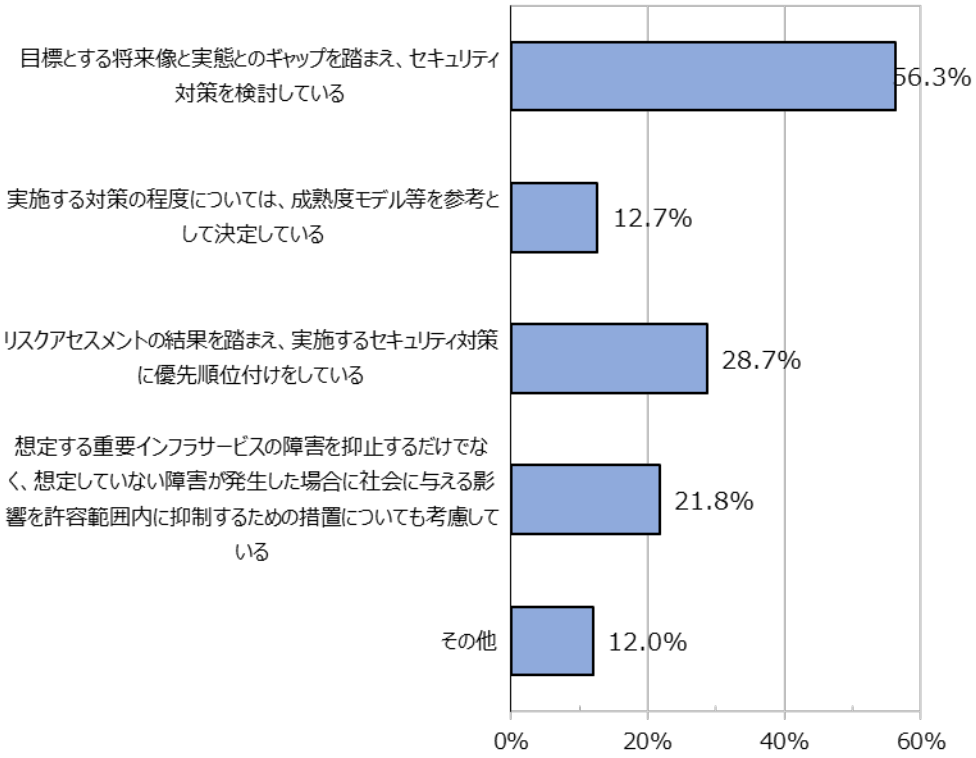
・NIST CSF 1.1、工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン

・NERC-CIP、ISMS、CSMS、ISA

・参考としているものはない（制御システムは、外部から隔離されたネットワーク環境）

アンケート調査結果

設問22.【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22.【自由記述】
設問22で、「その他」を選択した場合の理由

記載：167件
※金融を含む

■代表的な意見（抜粋）

・ガイドラインに則した対応の検討、セキュリティーポリシーの見直しを実施

・情報セキュリティポリシーに基づき、対策ハンドブックの作成を予定している

・電力制御システムセキュリティガイドライン、スマートメーターシステムセキュリティガイドラインへの準拠

・費用対効果を検討し予算確保が可能か否かで決定している

・総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」を参考

・「政府機関等のサイバーセキュリティ対策のための統一基準群」に準拠した規程等の整備

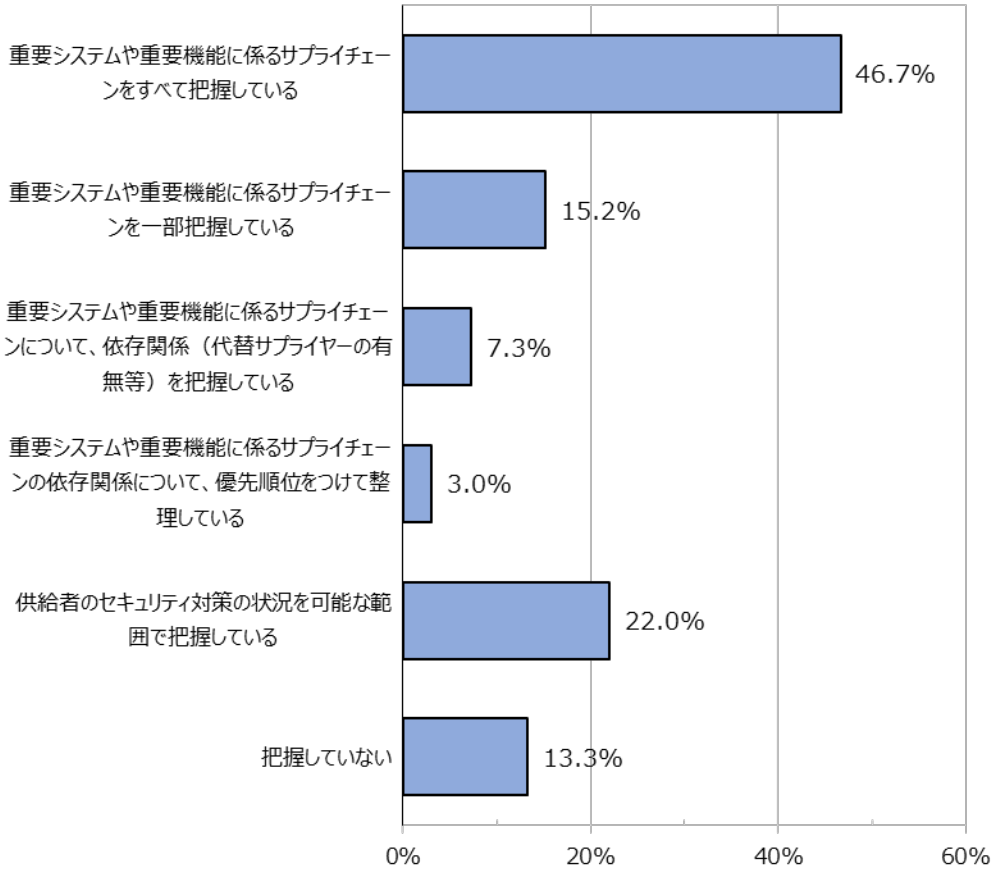
・同業他社や関係事業者が実施する対策をモデルに対策を検討

・外部に接続していないため、基本的にセキュリティ対策は行っていない。

アンケート調査結果

設問23.【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（供給者、委託先等※）に関して現在の状況を回答してください。

※サプライチェーンの範囲は１次取引先とします。



設問24.【自由記述】
設問23で、「サプライチェーンをすべて（一部）把握している」を選択した場合、サプライチェーンの把握の方法や粒度を記載してください。

記載：700件

■代表的な意見（抜粋）

・契約書情報の一元把握。一部の要求事項を「情報資産に係る外部委託管理規則」に規定

・保守委託業者に定期報告を受けている

・契約時の仕様書・作業責任者報告書などでの把握

・業務継続計画に記載されているサプライチェーンに変更がないか年1回確認を行っている

・契約時に保守体制や連絡体制の提出を求めることで把握

・各管理部署による

・ISMS文書内緊急連絡先一覧にて、社内担当者、業務内容、連絡先を一覧管理

・一次取引先からの聞き取り

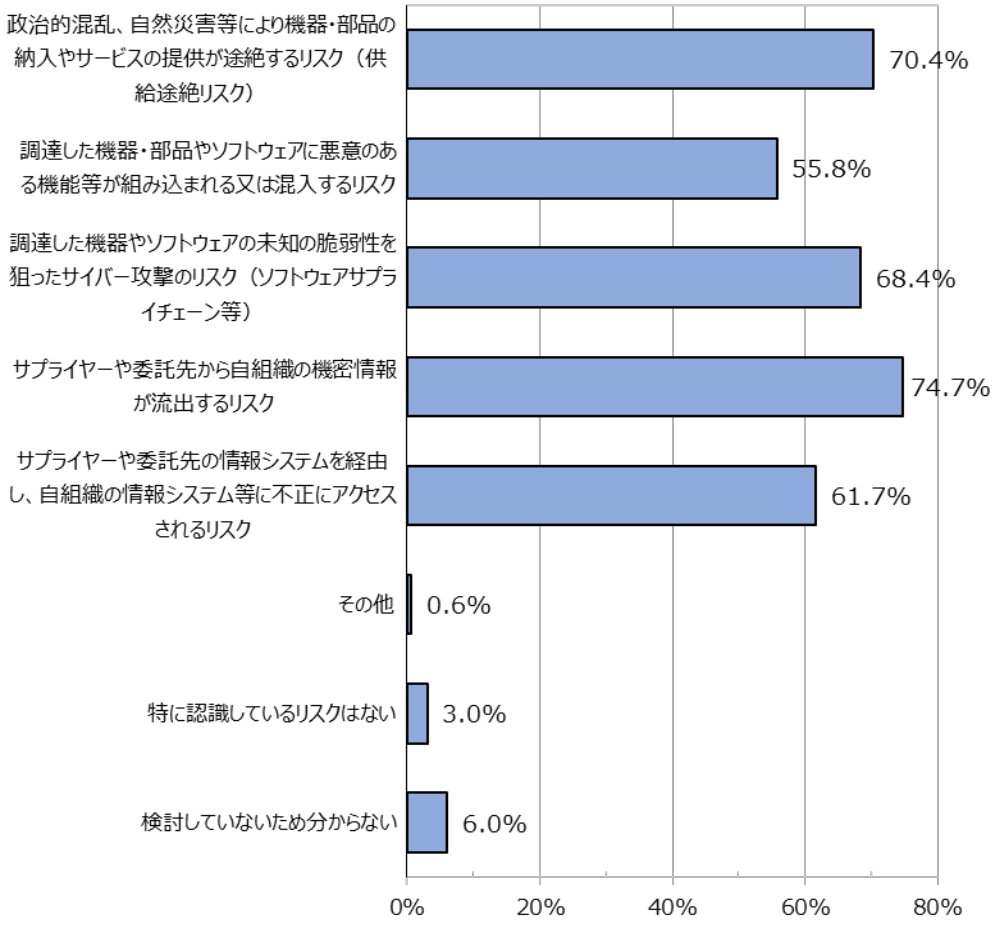
・契約書にて業務単位で把握

・委託先へのヒアリングや資料要求などによる

・毎年度、各システムの現況調査を実施し把握

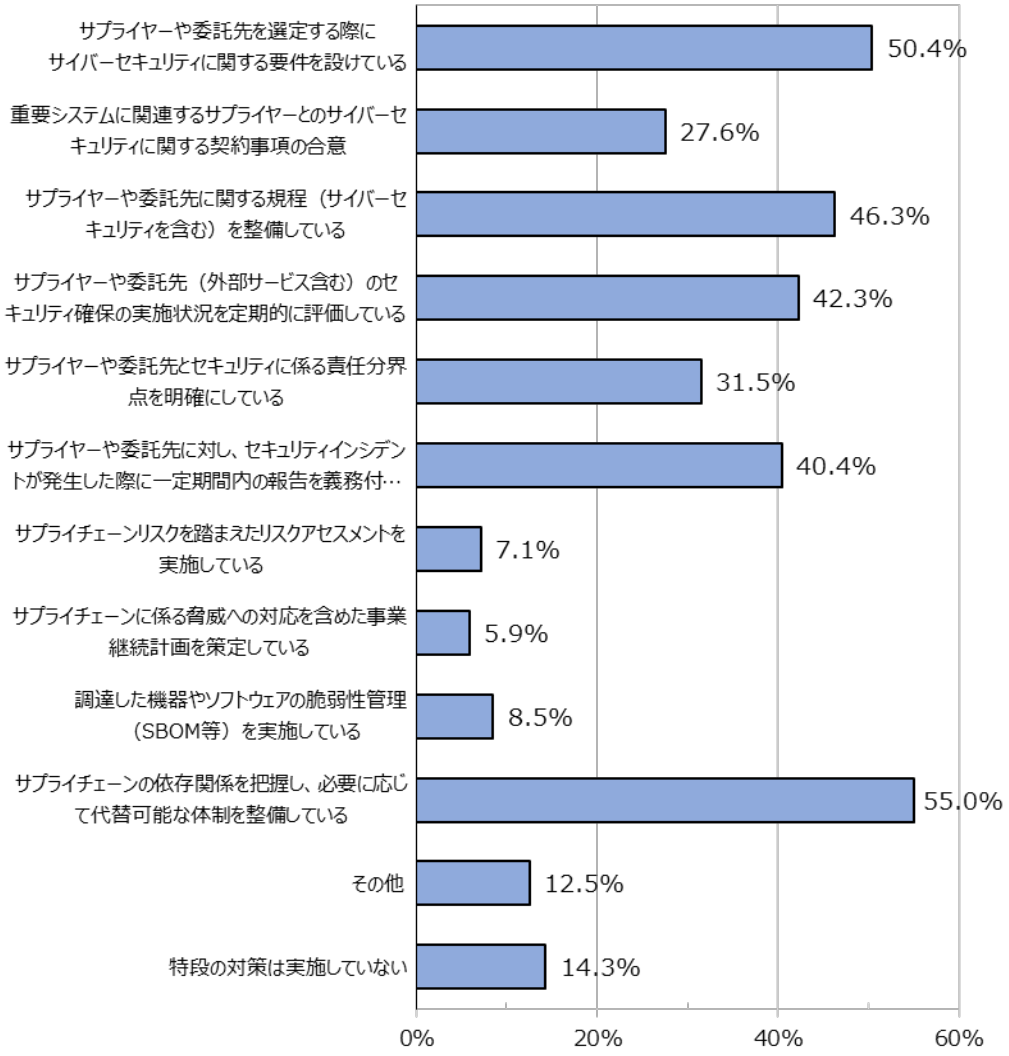
アンケート調査結果

設問25.【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。



■「その他」（一部抜粋）
・再委託先がサイバー攻撃を受けたり、機密情報の漏洩を生じさせるリスク

設問26.【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。**（※全金融分野を含む）**



アンケート調査結果

設問26.【自由記述】
設問26で、「その他」を選択した場合の理由

記載：33件

■代表的な意見（抜粋）

・重要システムに関連するサプライヤーとのセキュリティに関する契約事項の合意

・契約時に情報セキュリティポリシーの遵守を義務付けている

・インシデント発生時には、関係先に状況報告を要請する

・情報の取り扱いについて個別事項で契約している

・個人情報を取り扱う委託先については「委託先評価チェックリスト」で評価、又は「個人情報保護に関する覚書」を締結し、責任の明確化や安全管理に関する事項を定めている

・ISMSクラウドセキュリティ認証取得組織や、ISO/IEC 27001等の認証を受けた業者を委託の必要条件としている

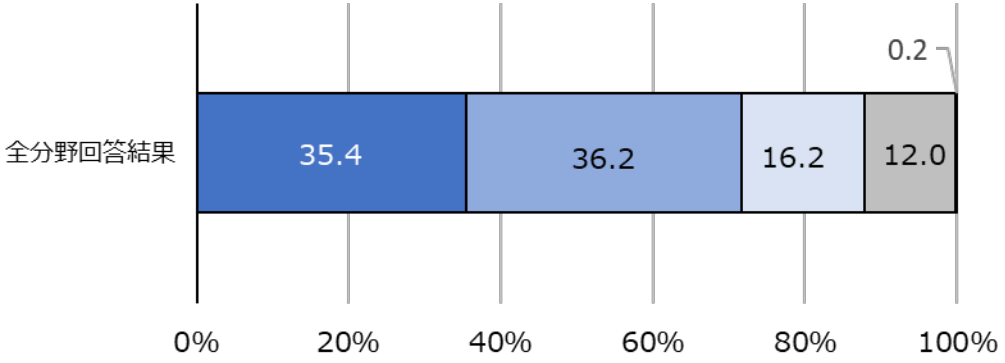
・SASEソリューションやゼロトラスト型のセキュリティソフトを導入することでネットワーク上にかかわるものやクライアントについてリスク軽減をおこなっている

・委託契約書に個人情報の取り扱いについて明記している。使用している機器等についてソフトウエア等のアップデータがある場合は、影響を確認したうえで、できるたけ速やかに適用している

アンケート調査結果

設問27.【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。**（※全金融分野を含む）**

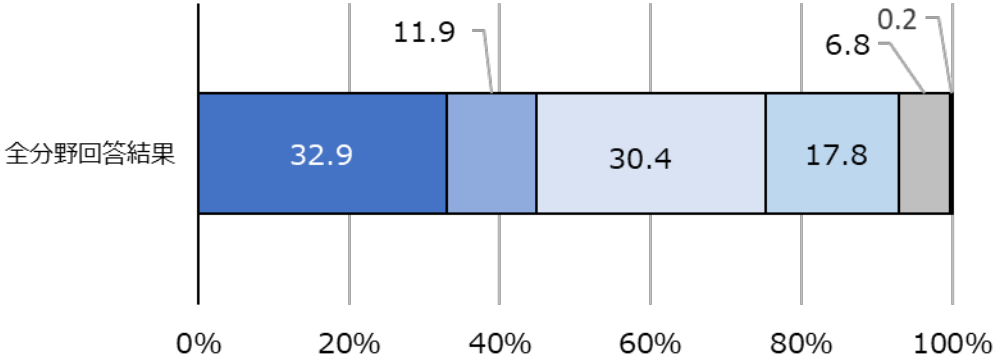
※重要インフラ事業者等が重要インフラサービス障害の発生又はそのおそれがあることを認識した後に経営層や職員等が行うべき初動対応(緊急時対応)に関する方針、手順、態勢等をあらかじめ定めたもの。



- 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28.【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。**（※全金融分野を含む）**

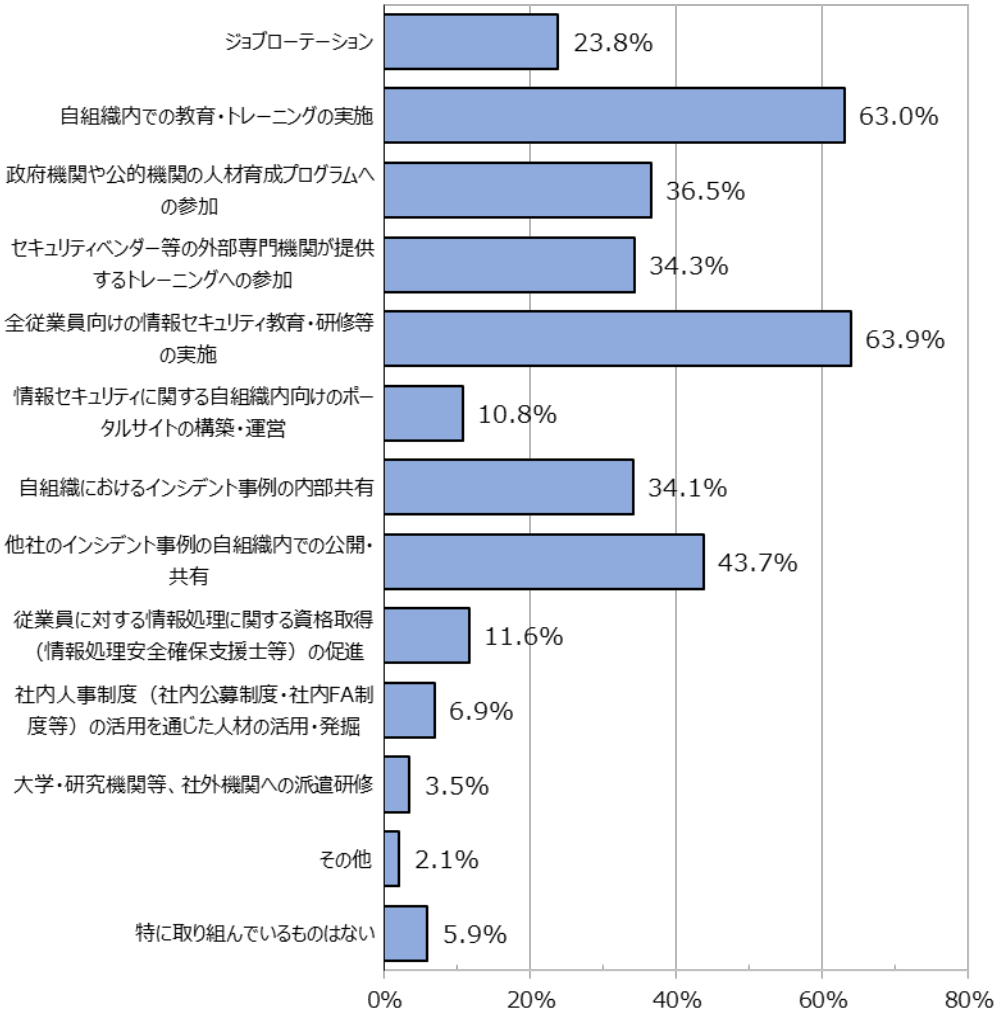
※1 重要インフラ事業者等が重要インフラサービス障害により影響を受けた重要インフラサービスを許容可能な時間内に許容可能な水準(目標復旧水準)まで復旧させることを目的として、その復旧に向けた目標水準、優先順位その他の方針、手順、態勢等をあらかじめ定めたもの。
※2 目標復旧水準から、平時のサービス水準まで完全復旧させることを目的としたもの。



- 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29.【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。**（※全金融分野を含む）**



設問29.【自由回答】
設問29で、「政府機関や公的機関の人材育成プログラムへの参加」を選択した場合、具体的なプログラム名を記載ください。

記載：588件

（※１社で複数回答は別々に集計）
（※「特に無し」は除く）

内容	件数
CYDER（実践的サイバー防御演習）	347 件
J-LIS（地方公共団体情報システム機構）主催の研修	144 件
IPA（情報処理推進機構）主催の研修	44 件
分野横断的演習	33 件
省庁関連の演習	31 件
自治体CSIRT協議会主催の研修や訓練	25 件
CSIRT研修・訓練	21 件
都道府県・県警主催の研修	17 件
金融ISAC	4 件
その他公的機関の研修（地方自治体アカデミーなど）	41 件

アンケート調査結果

設問29.【自由回答】
設問29で、「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への参加」を選択した場合、具体的なトレーニング名を記載ください。

記載：180件

（※「特に無し」は除く）

■代表的な意見（抜粋）　※個社名や個社の製品名が記載された意見は除く

・産業サイバーセキュリティセンター 中核人材育成プログラム
・標的型攻撃メール訓練及びセキュリティ対策研修インシデント対応訓練
・九州自治体情報システム協議会主催の多岐にわたるプログラム
・電力ISACのトレーニングなど
・日本経営協会「情報システム担当者の基本実務」
・ネットワーク保守委託業者による研修
・日本ガス協会：情報連絡訓練
・ベンダーの実施する自治体向けのオンライントレーニング
・毎年参加するものではない

アンケート調査結果

設問30.【自由記述】
設問30で、「取り組んでいる」ものを回答した場合、自組織において必要としているセキュリティ人材や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。

記載：1,161件

（※１社で複数回答は別々に集計）
（※代表的な意見のみ集計、また「特に無し」は除く）

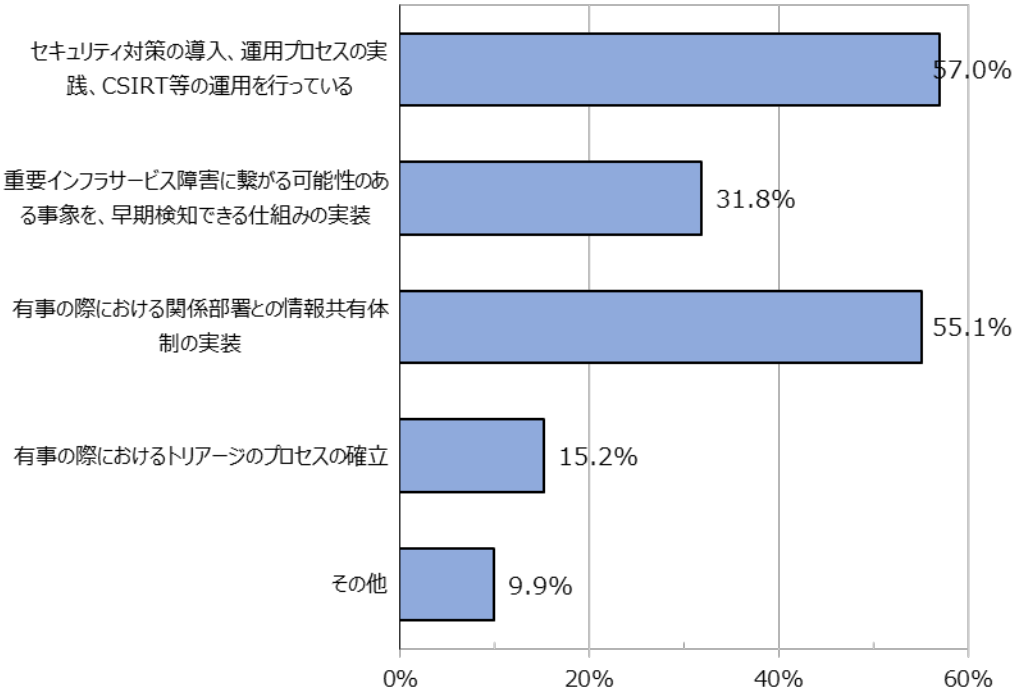
内容	件数
育成・研修の不足（時間や体制、ノウハウが不足。また研修の効果も低い）	387 件
専門知識・スキル不足（専門知識やスキルを持つ人材が不足）	304 件
人材不足・人員不足（そもそも人手が不足している）	261 件
人材育成の難しさ（専門用語の理解や習得が大変、人事異動で定着しない、体系的な育成ができない）	212 件
ITリテラシー不足（職員全体のITリテラシーが低い）	112 件
組織体制の課題（セキュリティ専門の部署がない）	110 件
実践的な対応力不足（実践的な訓練の機会が少ない）	64 件
最新技術への対応課題（セキュリティ技術の更新が早過ぎる）	16 件

■代表的な意見（抜粋）

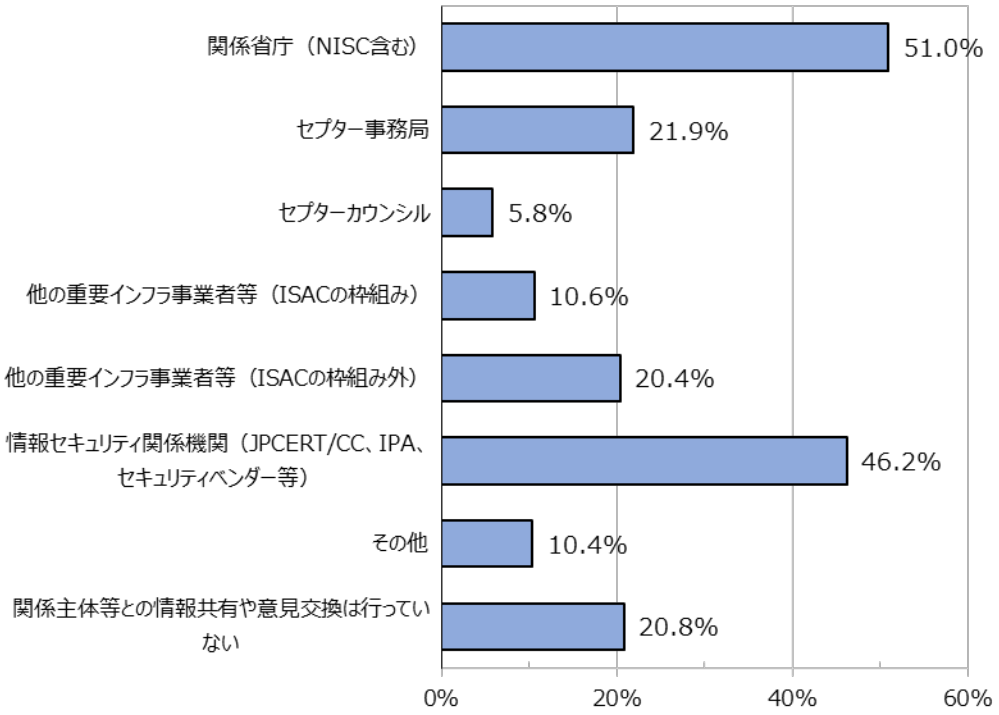
・資格取得や教育、外部研修の導入を取り組んでいる
・自組織内の職員によっては、セキュリティ知識や認識に差がある
・内部統制に充分な人材を割り当てることができない。組織内で、セキュリティに係る教育・研修を体系的かつ一元的に実施できていない
・職員が多忙なため、研修を受講することも困難
・人事異動が多く、セキュリティの専門家が育ちにくい環境にある
・予算や人員が限られ、情報システムの運用以外の対応を行う余力が無い。情報セキュリティの推進に対応可能な人材が属人化している
・情報システムなど専任者がおらず、兼任が多く、人材のみならずそもそもの人員が不足
・セキュリティは日々高度化しており、他の業務との兼任ではなく専門人材が必要
・セキュリティに比較的関係性の高い部署からメンバーを寄せ集め、手探りで「兼任」で取り組んでいるが、求められる知識経験も多岐に渡り、兼任では着手できず実態は機能できていない

アンケート調査結果

設問31.【単一回答】
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32.【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」（主な意見を抜粋）
実施していない / 計画自体策定していない / 現在検討中

アンケート調査結果

設問33.【自由記述】
設問32で、「情報共有や意見交換を行っている」と回答した場合、対話や情報共有の内容、頻度等を記載してください。

記載：1,031件

（※１社で複数回答は別々に集計）
（※代表的な意見のみ集計、また「特に無し」は除く）

頻度は、適宜 / 定期的 / 不定期と様々

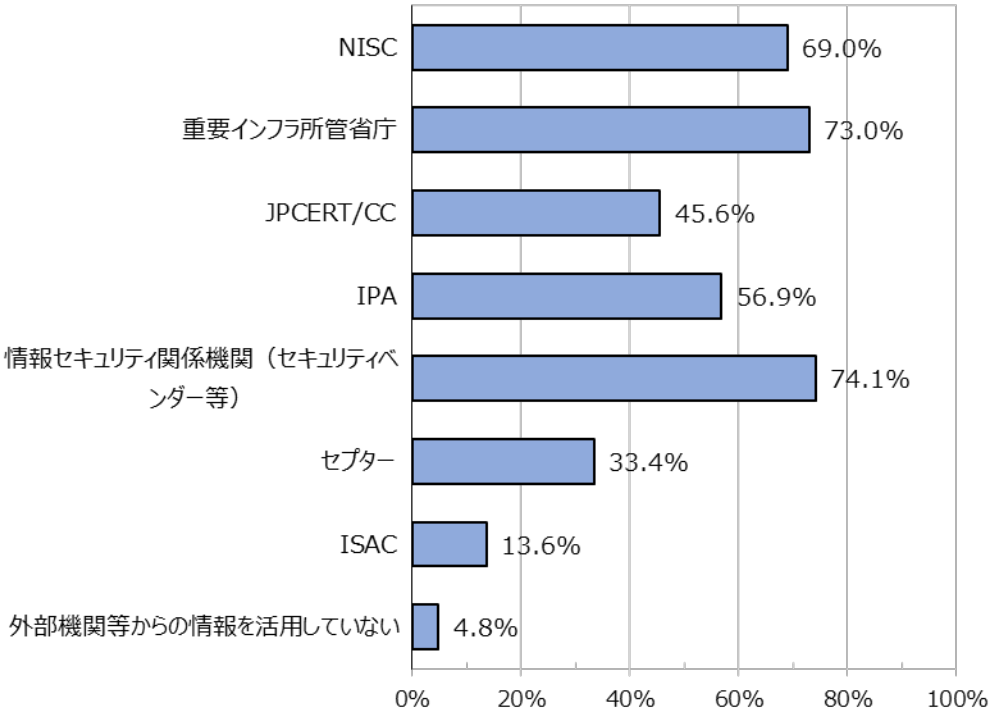
内容	件数
業界団体等との情報共有	87 件
インシデント情報の共有	82 件
セキュリティベンダーとの情報共有	66 件
システム・ネットワーク保守業者との情報共有	65 件
地方自治体・関連団体との情報共有	57 件
個別事業者やグループ会社	50 件
関係省庁からの情報共有	47 件
メールマガジン等による情報提供	42 件

■代表的な意見（抜粋）

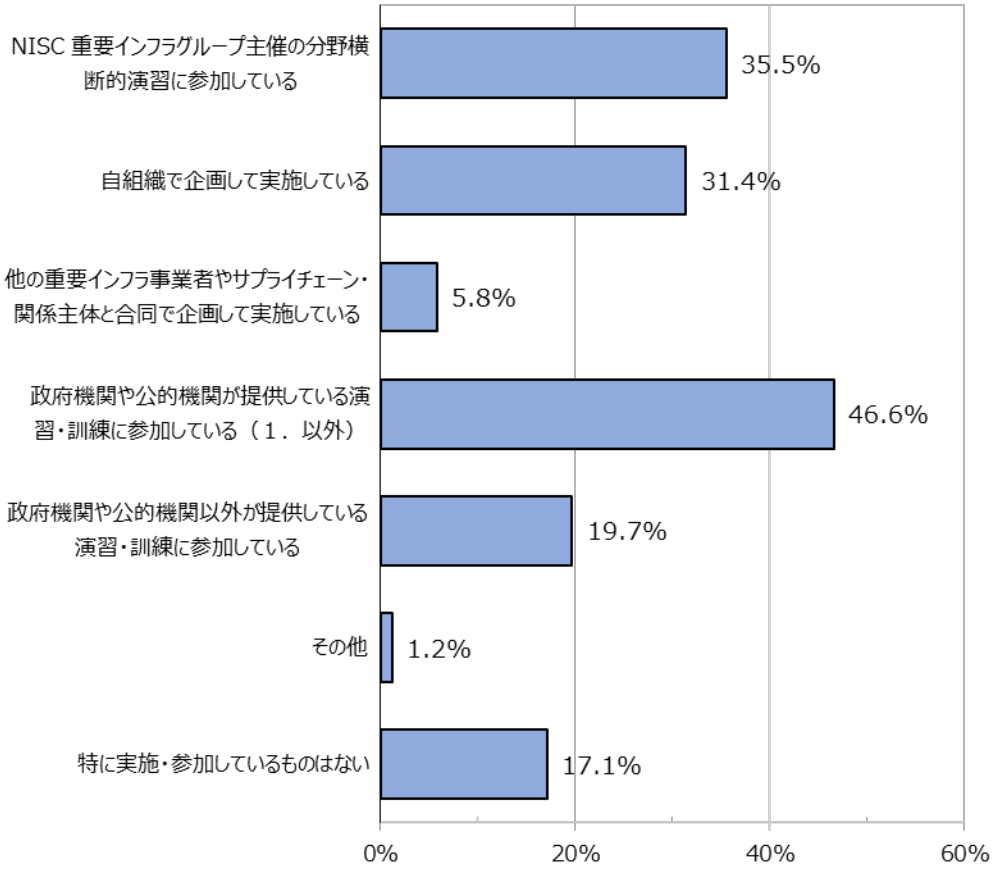
・某協議会に参加しいくつかのワーキンググループに参画している。また、JPCERT/CC、IPA、セキュリティベンダーからのアラート情報を受け取っている
・NISCからのお知らせや他団体からの情報共有（不定期）
・サイバーテロに関する対策等の情報共有
・1ヶ月に4,5回程度、他組織におけるインシデント情報及びセキュリティリスクのある製品情報等を取得
・年１回、県サイバーテロ対策協議会総会に出席し、サイバー攻撃等について情報共有している
・ベンダーとは、毎月1回定例会を実施
・月1回以上、グループ会社間のCSIRT検討や脆弱性診断の合同実施
・同業者と不定期での対話

アンケート調査結果

設問34.【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35.【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。**（※全金融分野を含む）**



アンケート調査結果

設問36.【自由記述】
設問35で、「実施・参加している」と回答した場合、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。また実施参加の目的を記載してください。

記載：1,008件

■代表的な意見（抜粋）

○NICT（情報通信研究機構）主催のCYDER（実践的サイバー防御演習）
・インシデントの対処能力向上のため、実践的サイバー防御演習「CYDER」へ参加している
・実施主体：情報通信研究機構・総務省、内容：分野的横断的演習（ＣＹＤＥＲ）、形式：集合演習、規模：５０名程度

○ NISC（内閣サイバーセキュリティセンター）主催の分野横断的演習
・2023年度分野横断的演習に参加自社内コンティンジェンシープランの実効性確認、従業員のセキュリティ対策、有事対応の意識向上の為
・ NISC主催の全分野一斉演習に毎年参加している
・分野一斉演習の疑似体験プログラムに参加している

○標的型攻撃メール訓練
・実施主体：市町村振興協会 内容：標的型攻撃メール訓練 規模：各室の代表者１名を対象に標的型攻撃メールを模したメールを送り、メールを開いたか否かを確認し、セキュリティ意識を確認している。

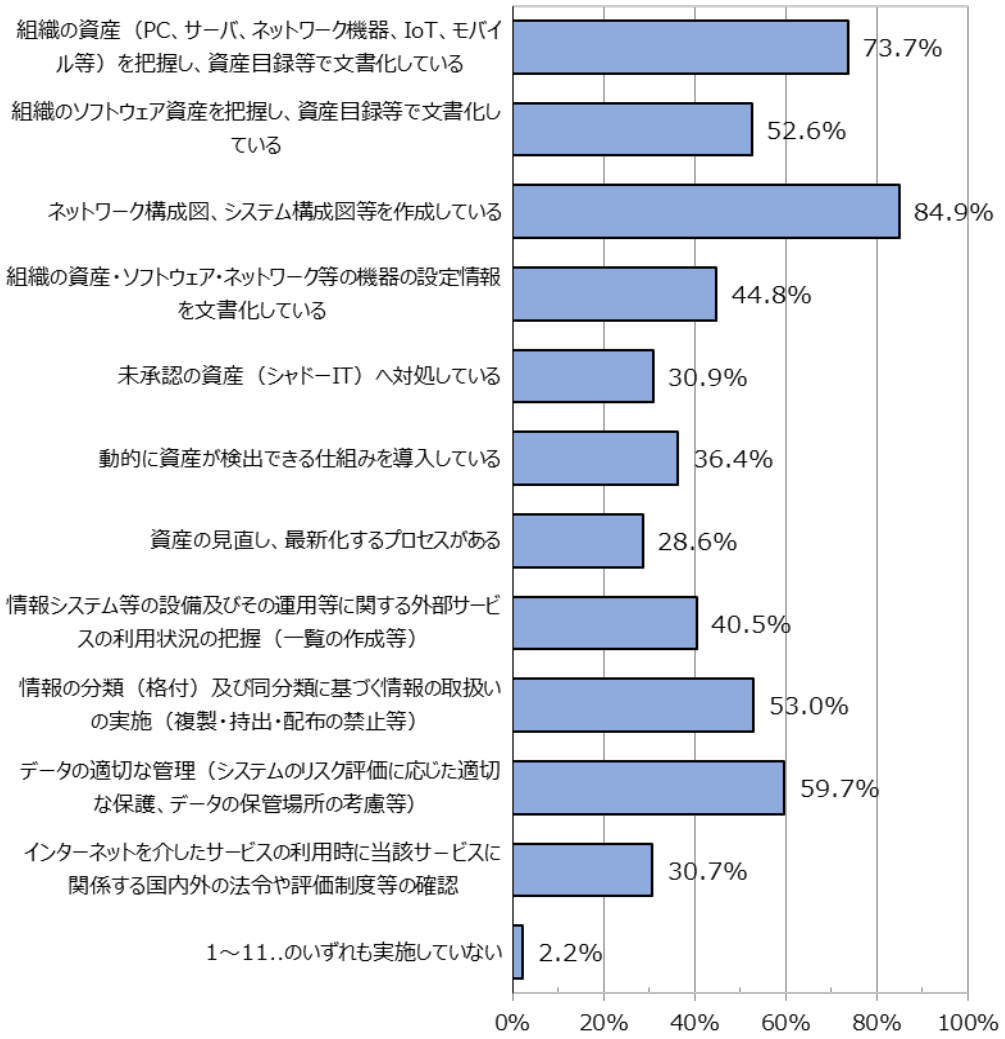
○ J-LIS（地方公共団体情報システム機構）主催の研修・訓練
・J-LIS主催のインシデント発生時CSIRT対応訓練への参加（市CSIRTの対応力向上のため）

○自組織内でのインシデント対応訓練・演習
・自団体で新人職員向けの研修を行っている。国が提供するeラーニングへの参加を行っている

○業界団体・協議会等主催の訓練・演習
・電力ISAC主催のサイバー演習、電力中央研究所主催のサイバー演習

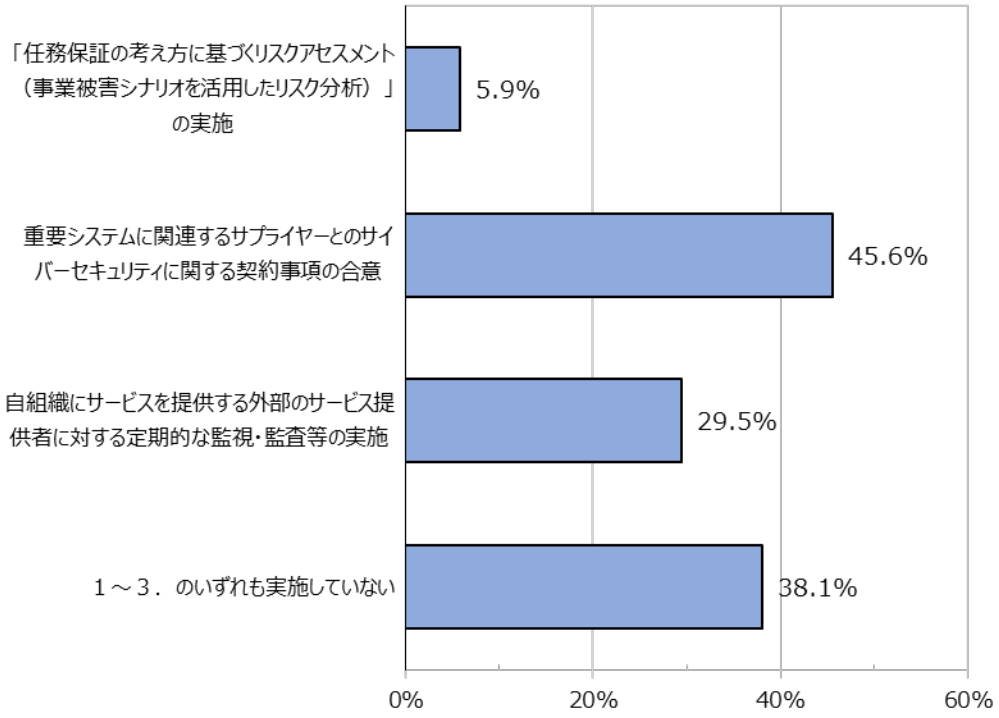
アンケート調査結果

設問37.【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。

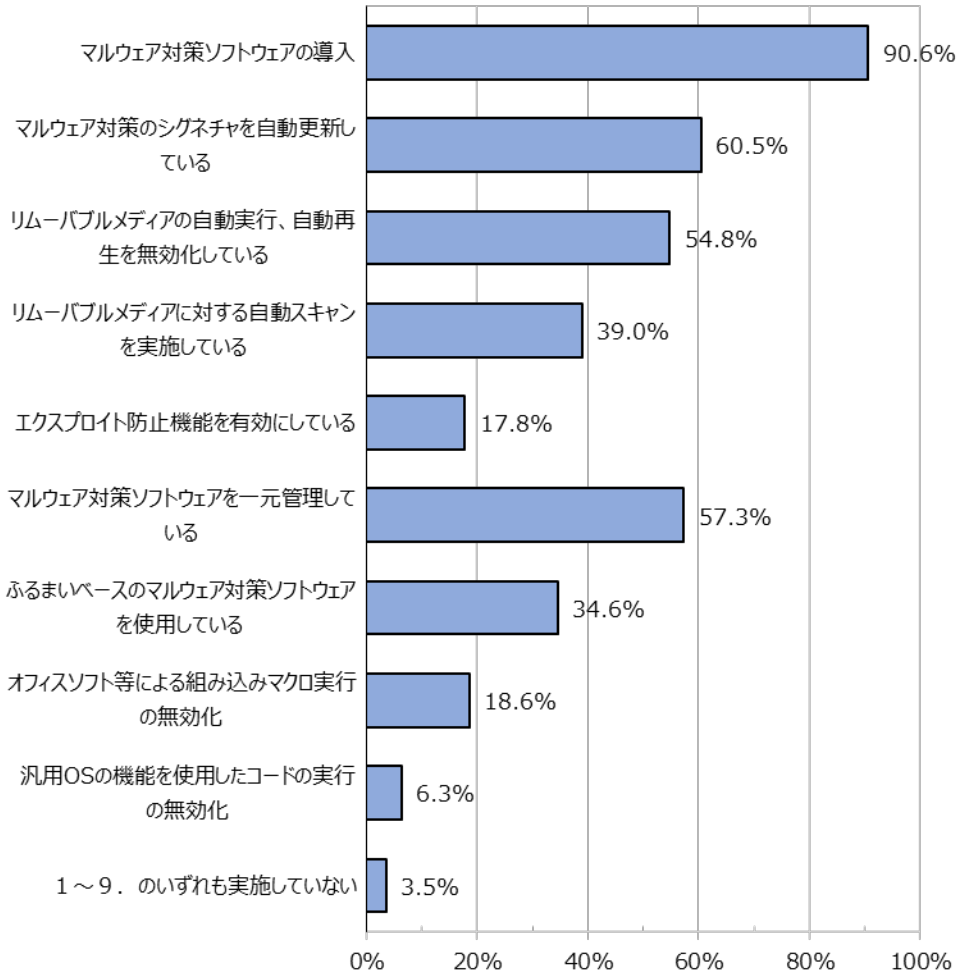


アンケート調査結果

設問38.【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。

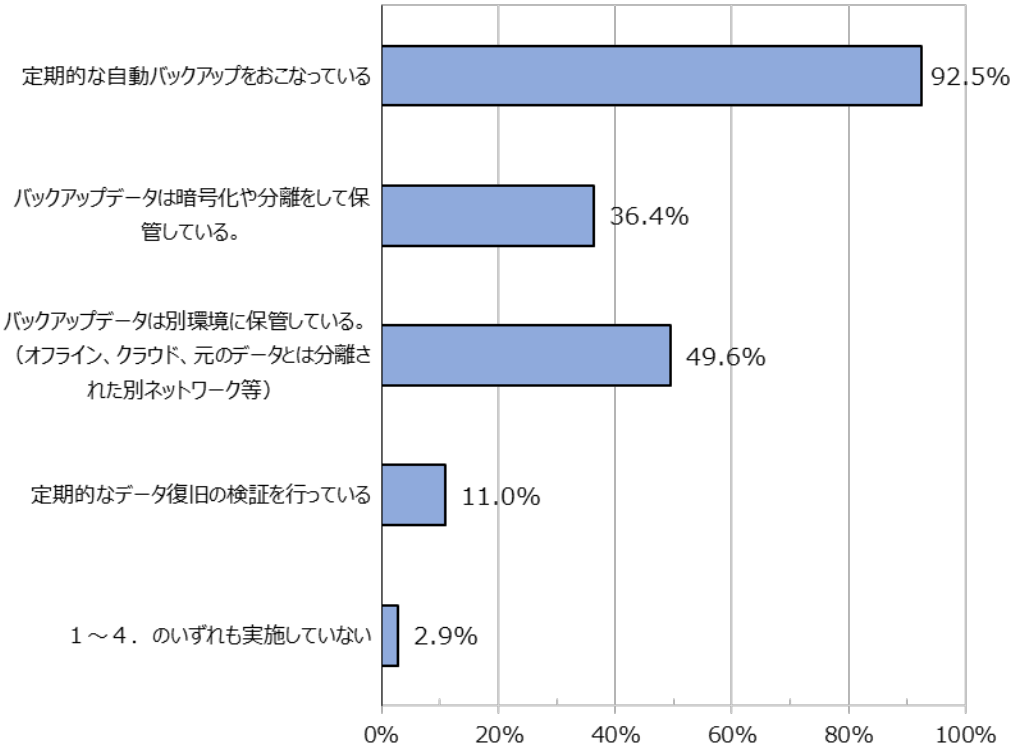


設問39.【複数回答】
マルウェアからの防御のため、実施している取組を選択してください。

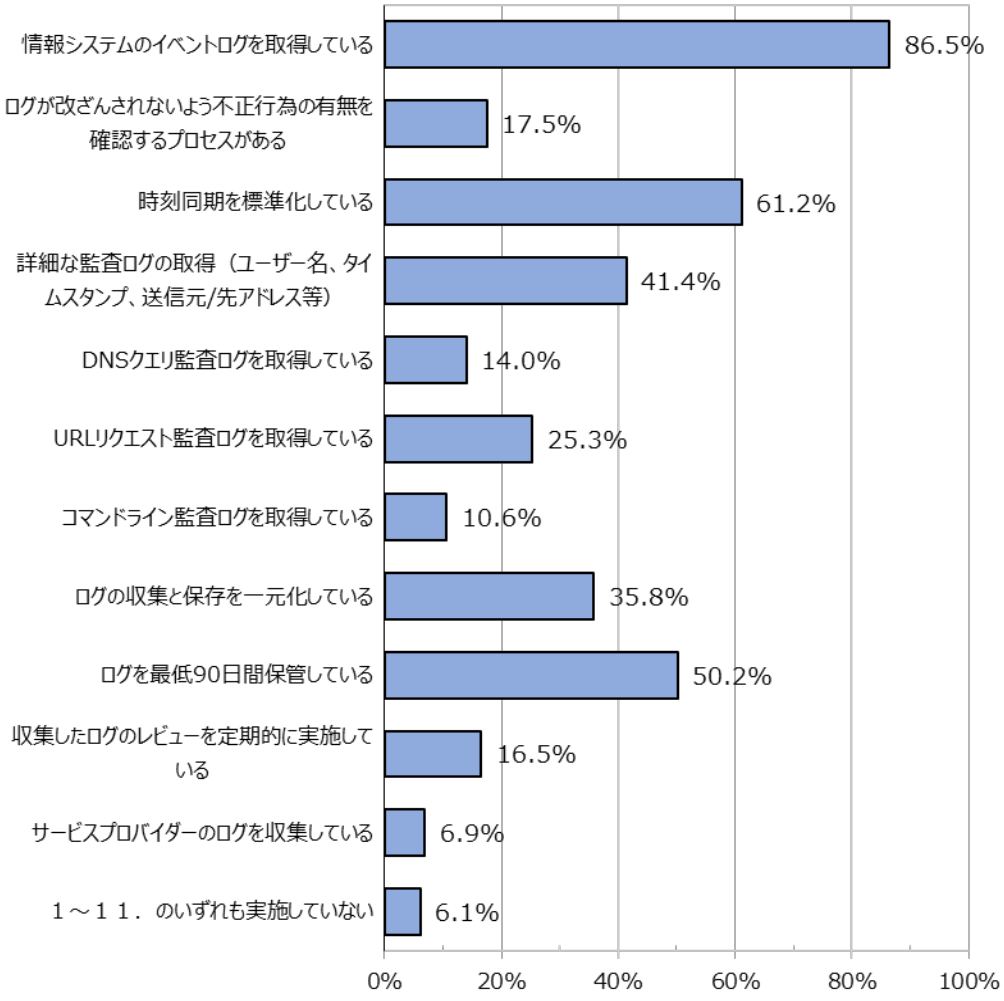


アンケート調査結果

設問40.【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。

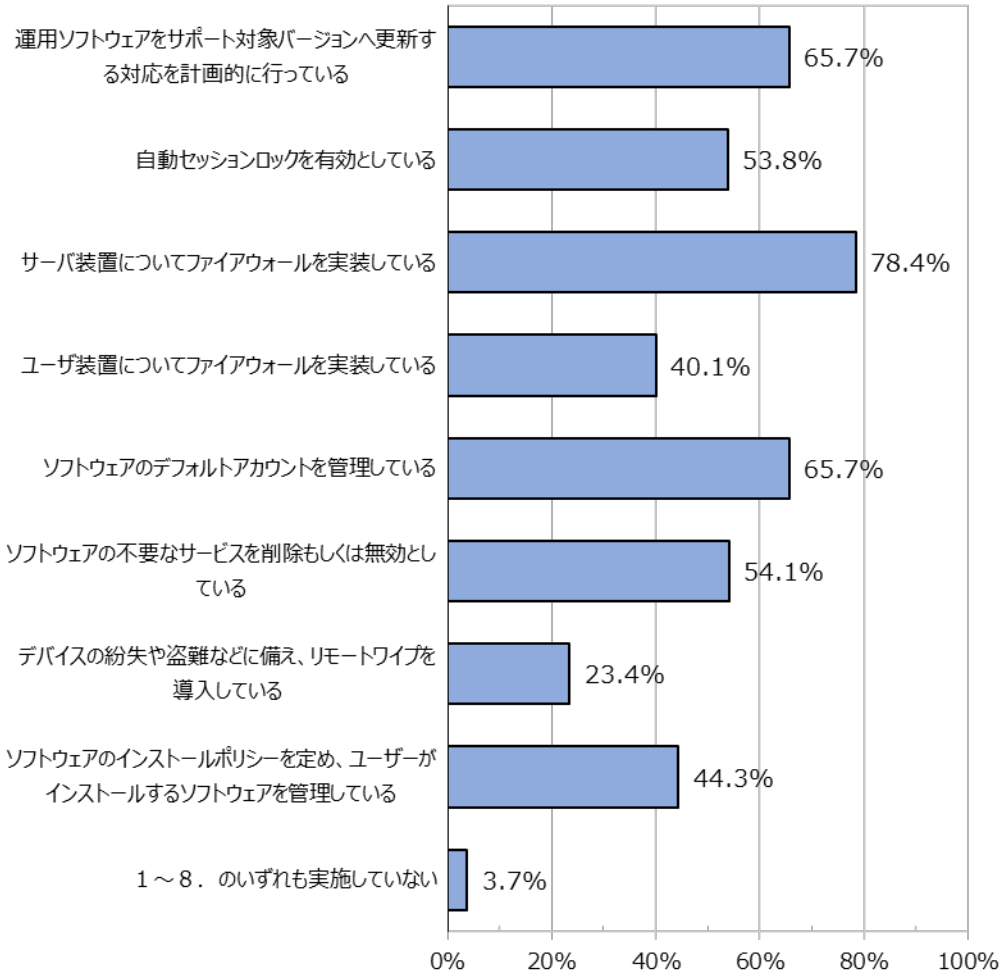


設問41.【複数回答】
ログ管理に関して実施している取組を選択してください。

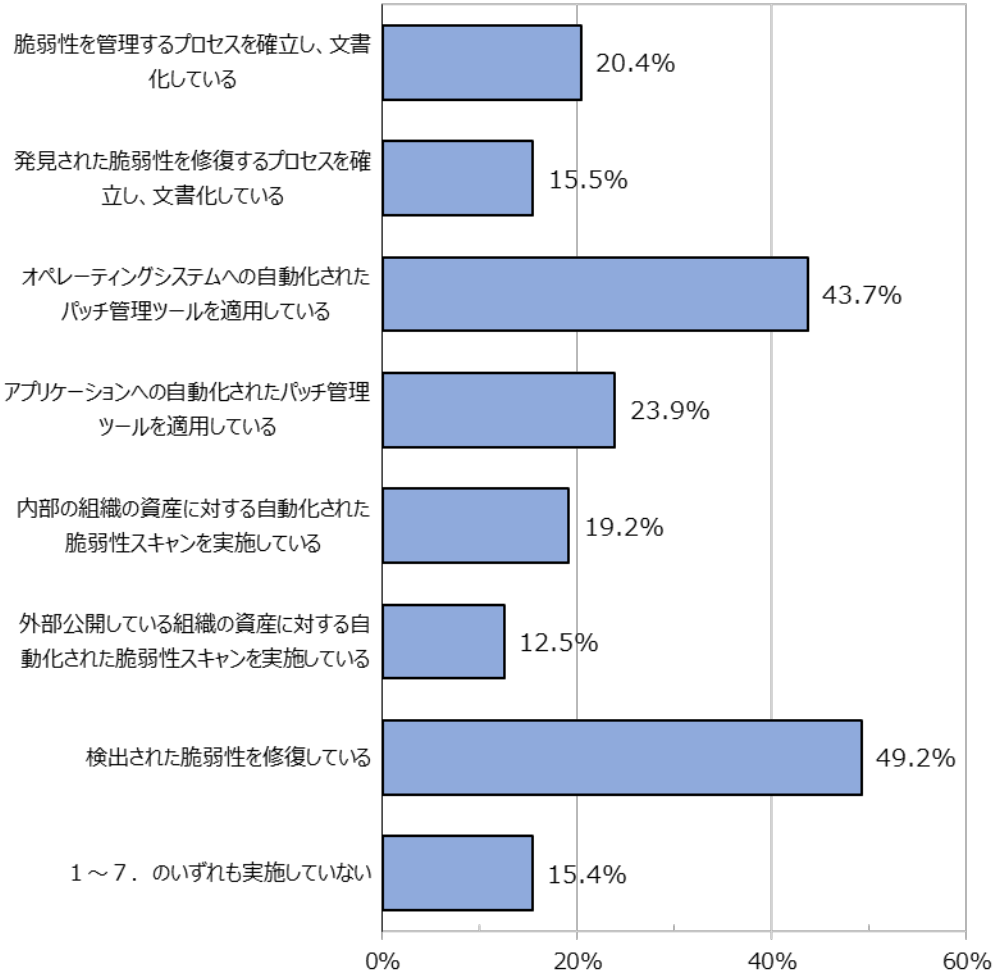


アンケート調査結果

設問42.【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。

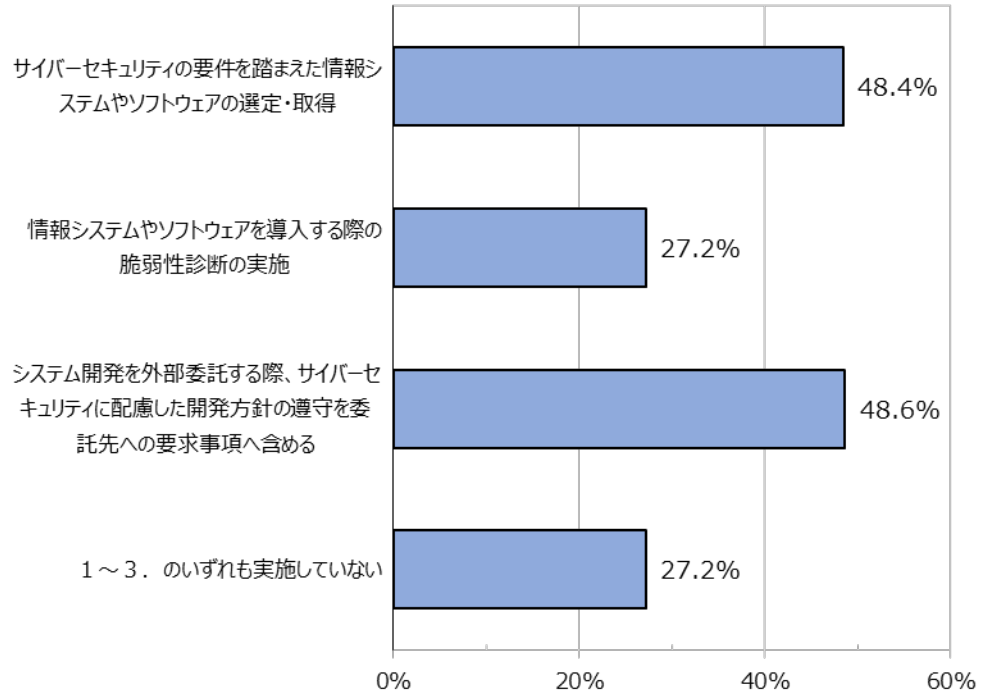


設問43.【複数回答】
脆弱性管理について実施している取組を選択してください。

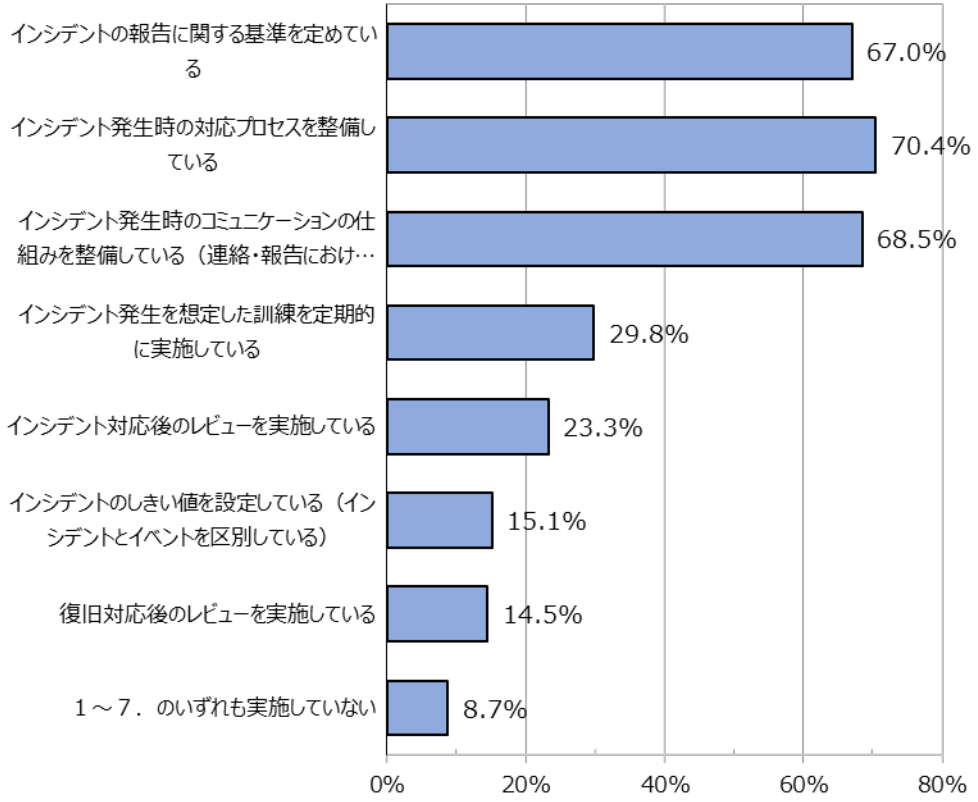


アンケート調査結果

設問44.【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。

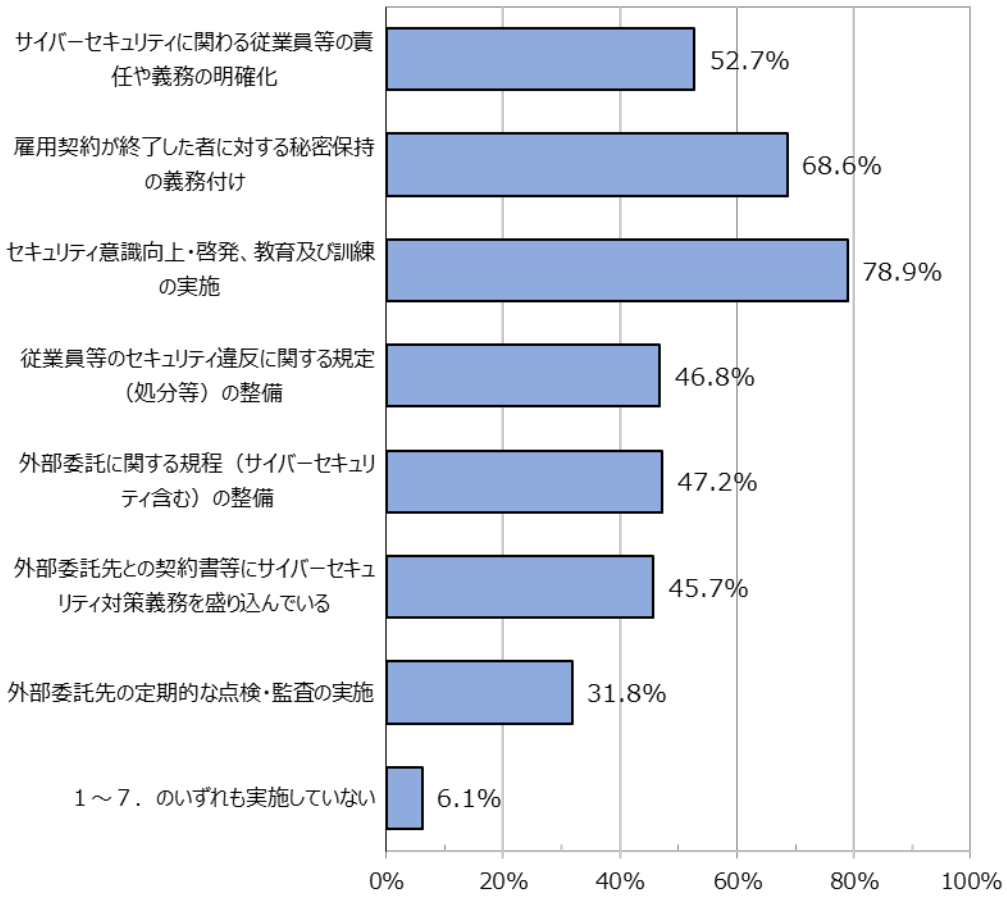


設問45.【複数回答】
インシデント管理について実施している取組を選択してください。

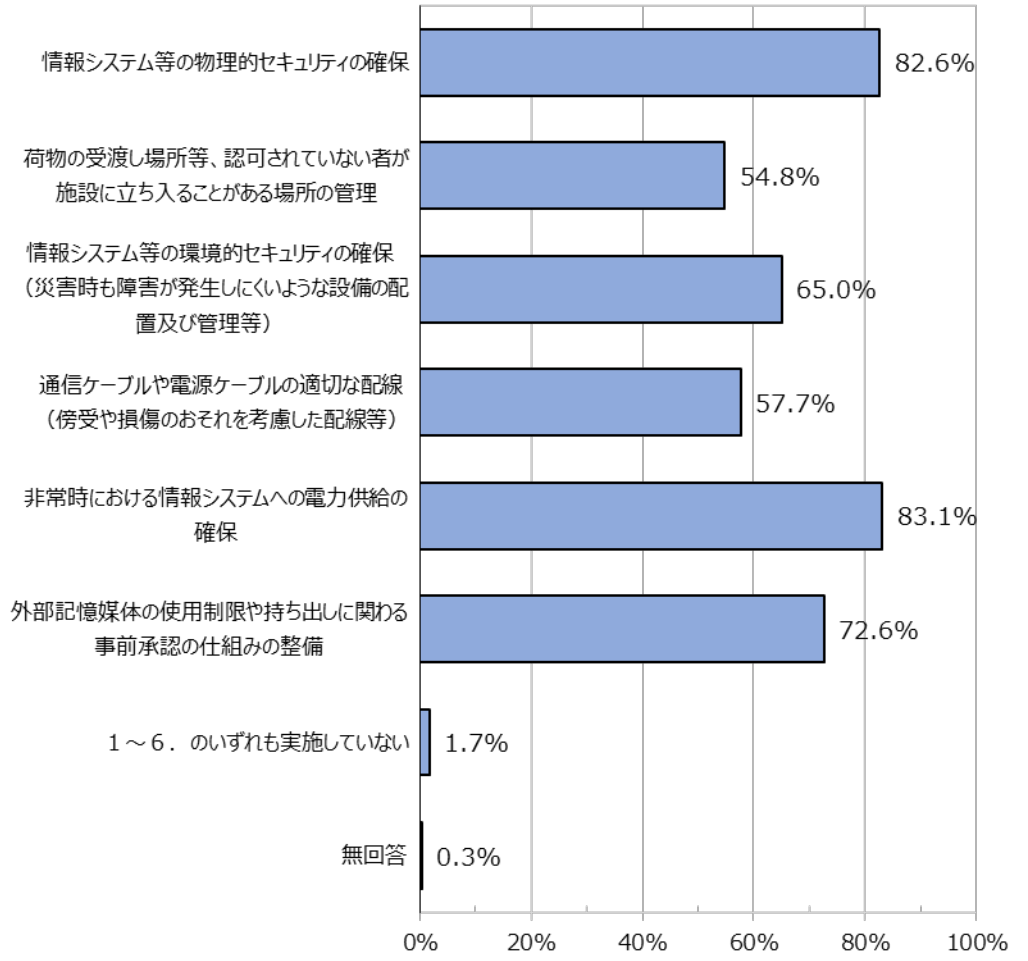


アンケート調査結果

設問46.【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。

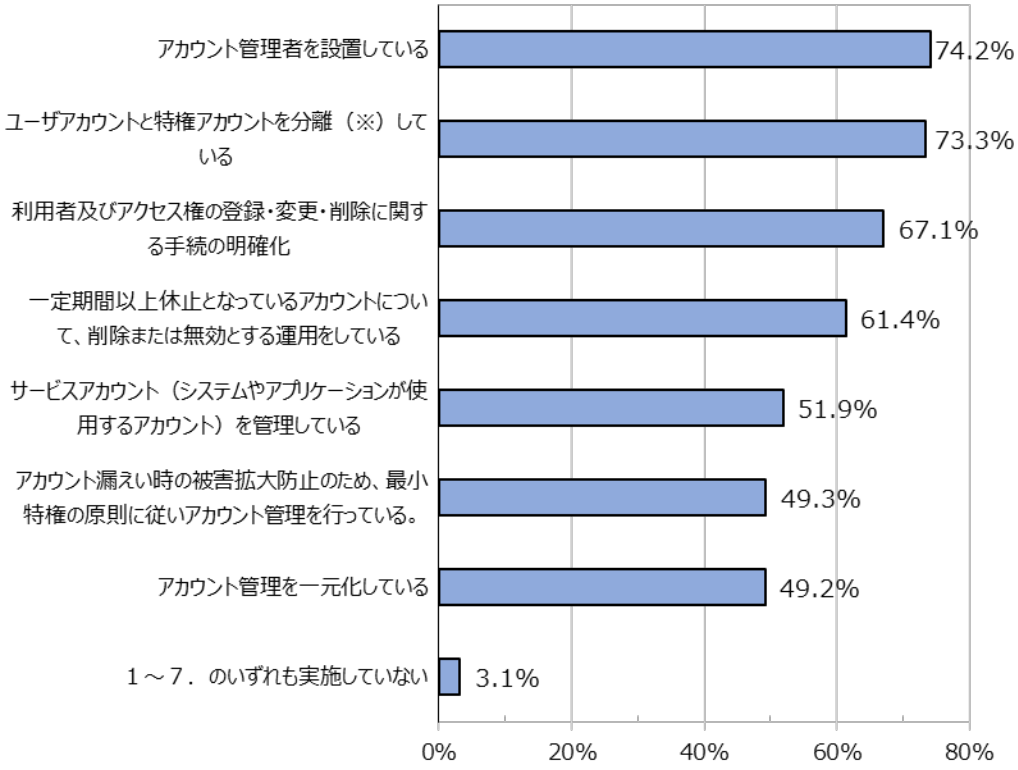


設問47.【複数回答】
物理的及び環境的セキュリティに関して、実施している取組を選択してください。

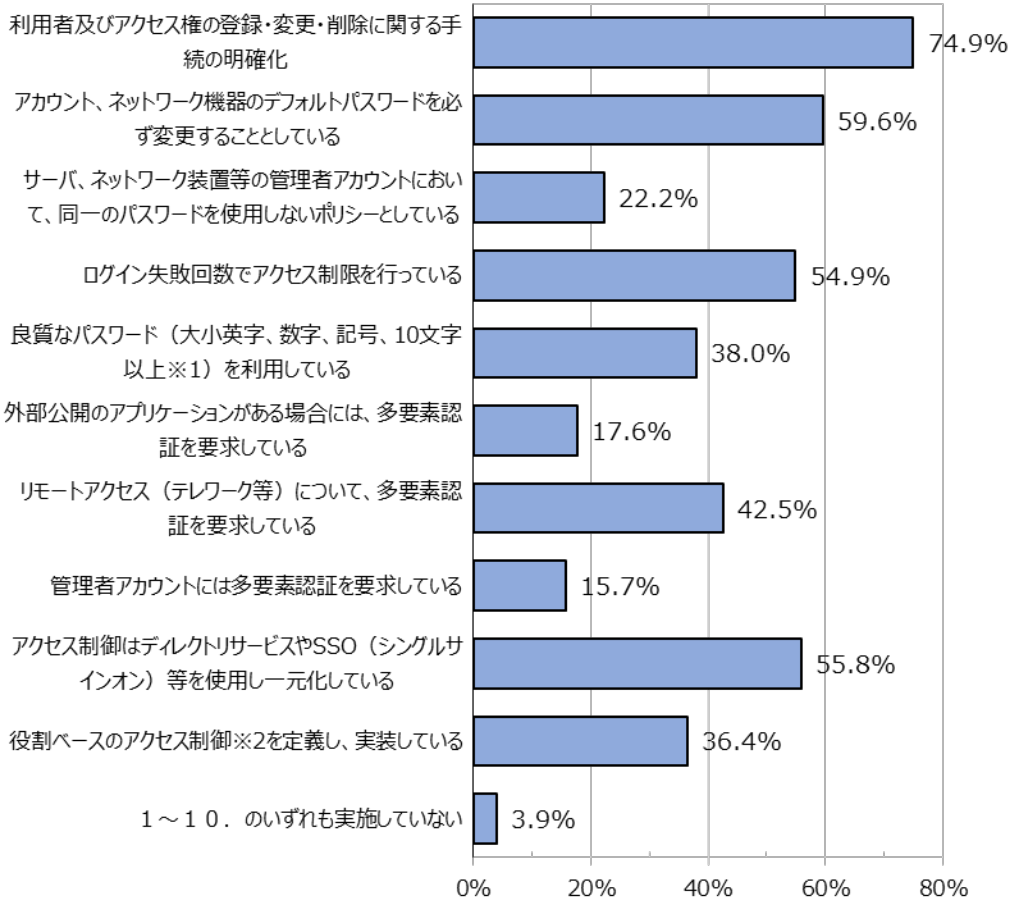


アンケート調査結果

設問48.【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。

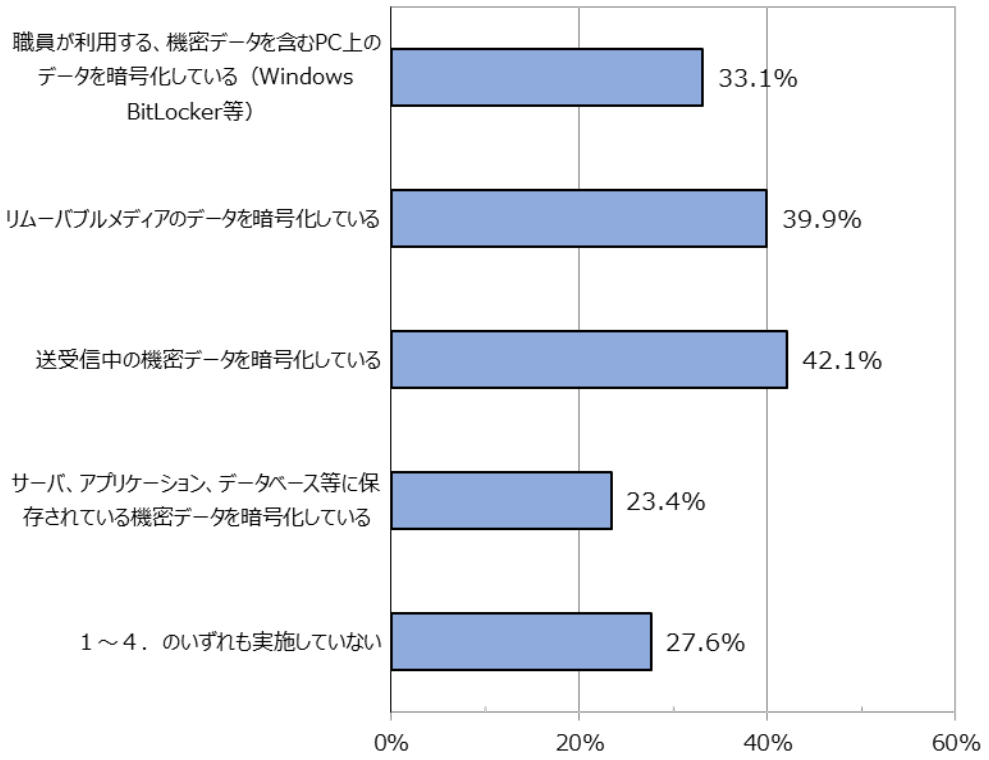


設問49.【複数回答】
アクセス制御に関して、実施している取組を選択してください。

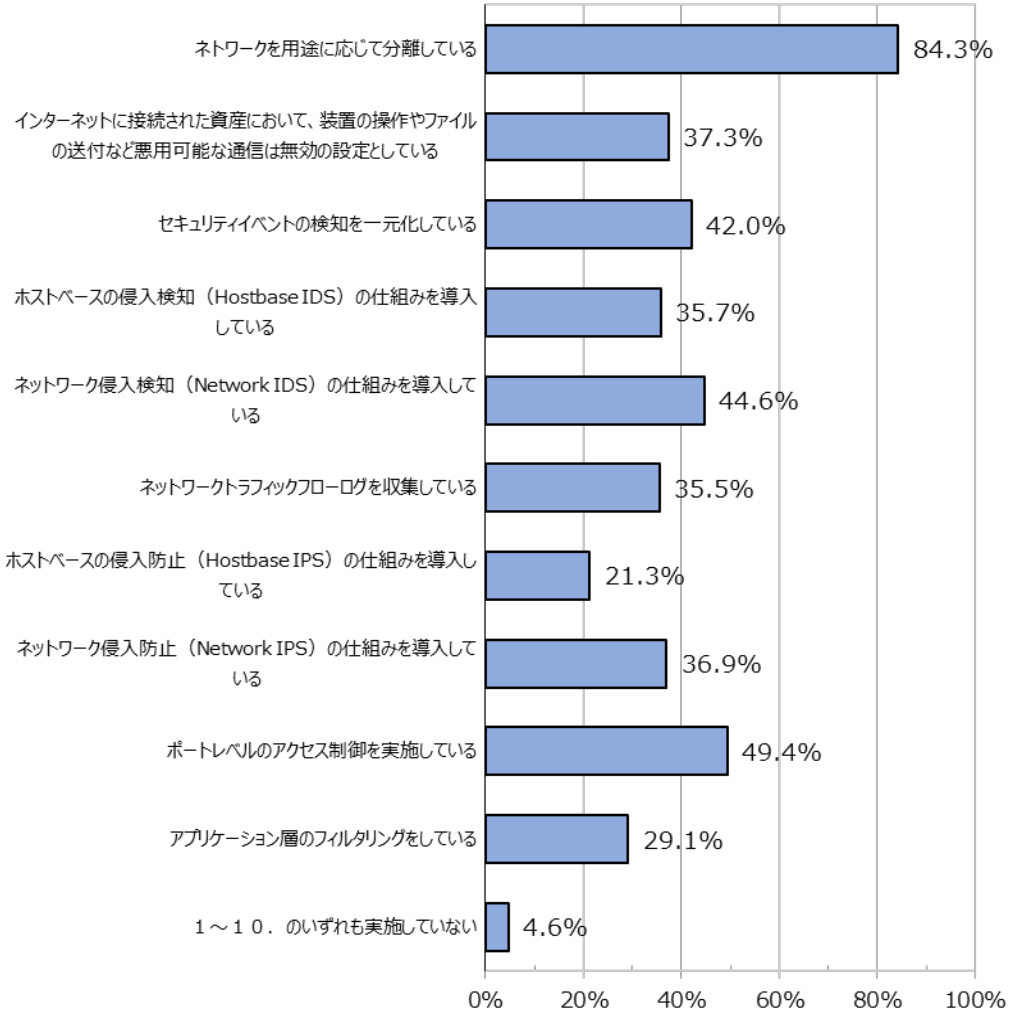


アンケート調査結果

設問50.【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。

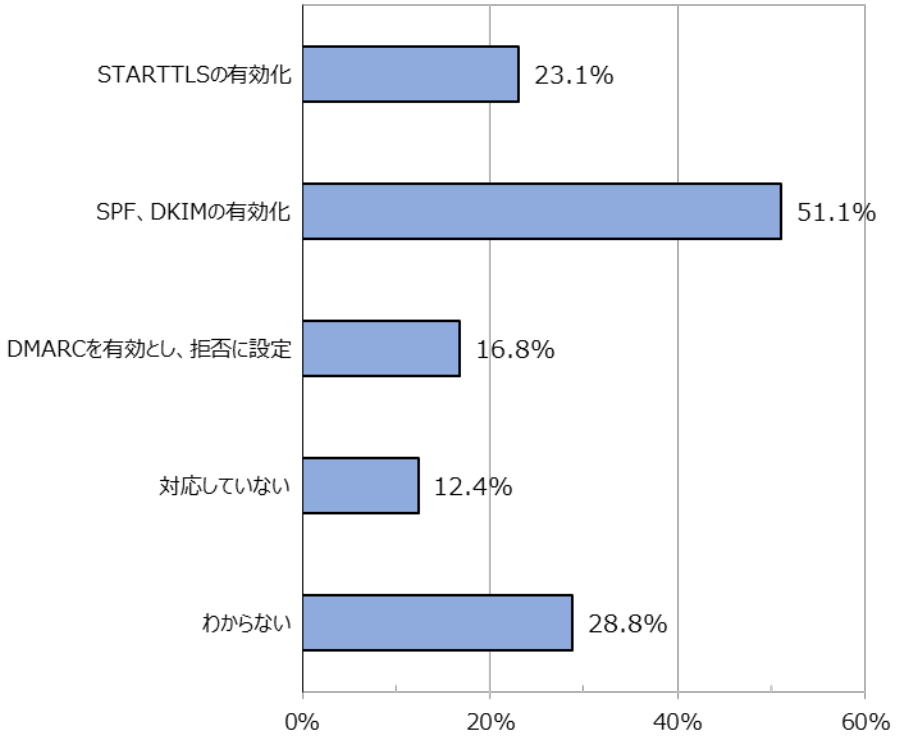


設問51.【複数回答】
通信のセキュリティに関して、実施している取組を選択してください。

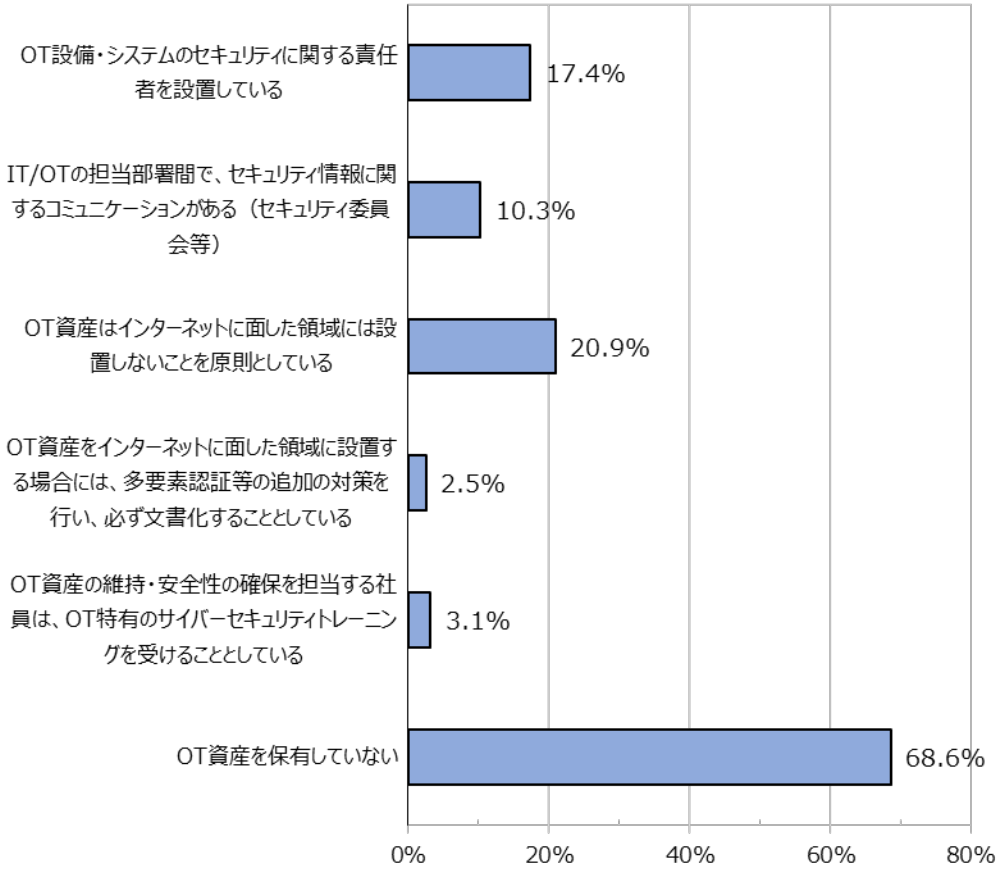


アンケート調査結果

設問52.【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選択してください。

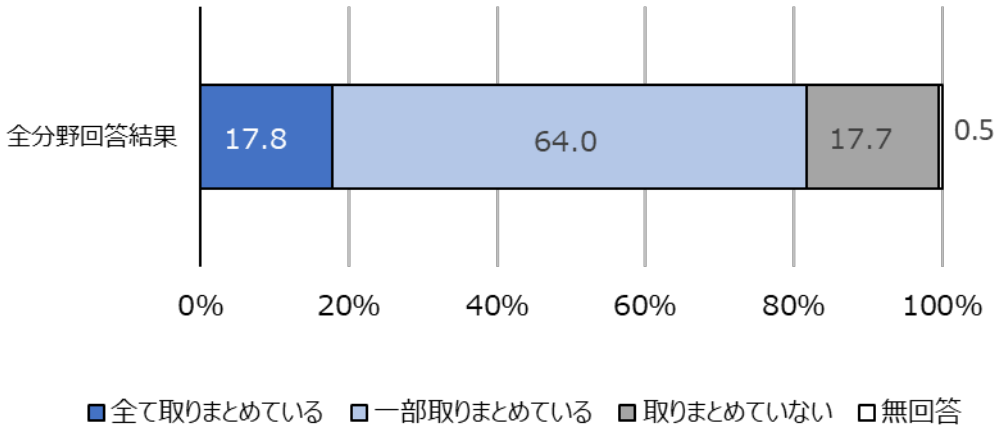


設問53.【複数回答】
制御システム（OT資産）を保有している場合、実施している取組を選択してください。



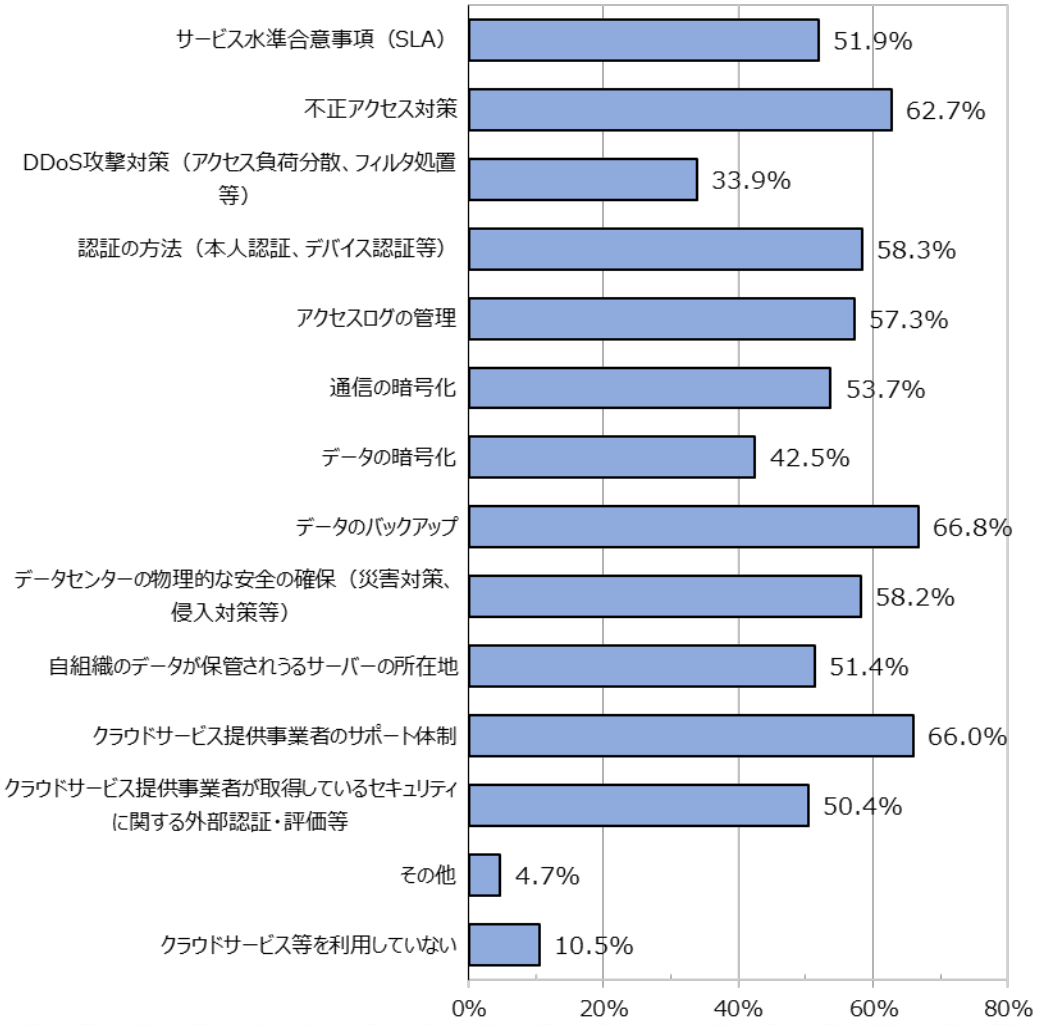
アンケート調査結果

設問54.【単一回答】
設問53までの組織的、人的、物理的、技術的対策において、「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。



アンケート調査結果

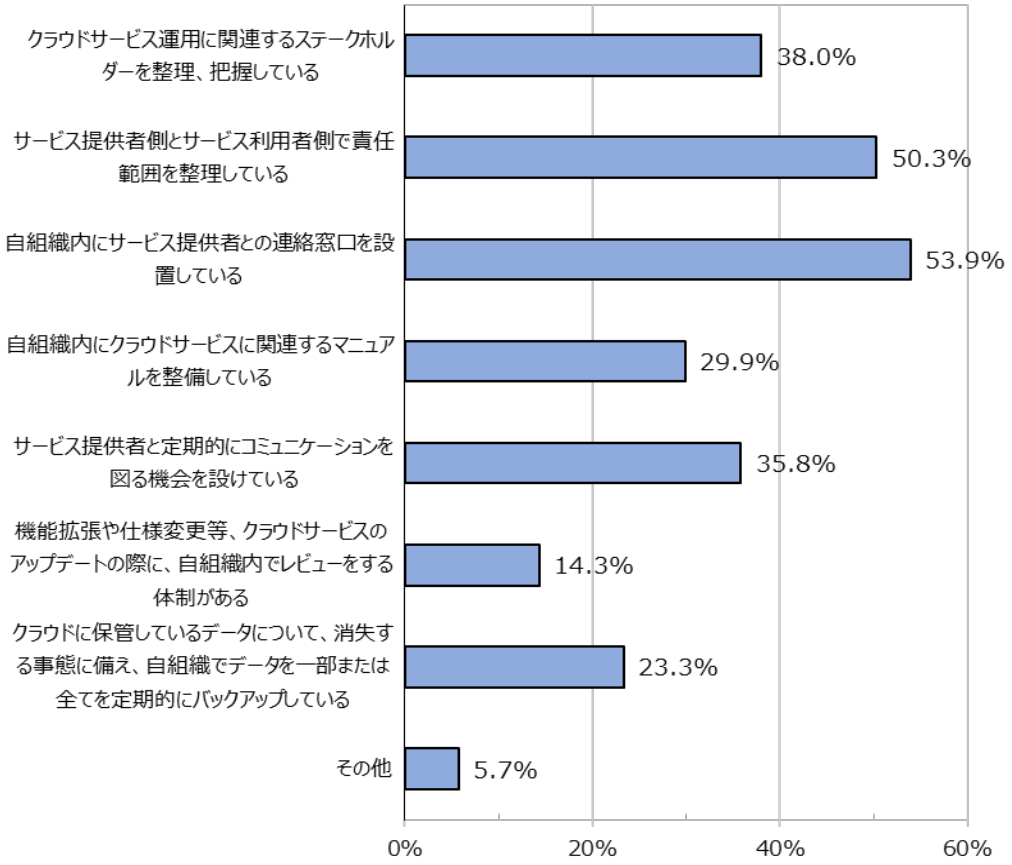
設問55.【複数回答】
自組織がクラウドサービスを利用する際に、クラウドサービス提供事業者側へ確認している事項を全て選択してください。



■「その他」（主な意見を抜粋）
・サービス使用終了時のデータの削除方法
・ISMAP登録サービスであるかどうか
・CASBによる評価
・適用法がどの国の法律であるか、解約などした際のデータの扱い、規約変更の際の連絡有無

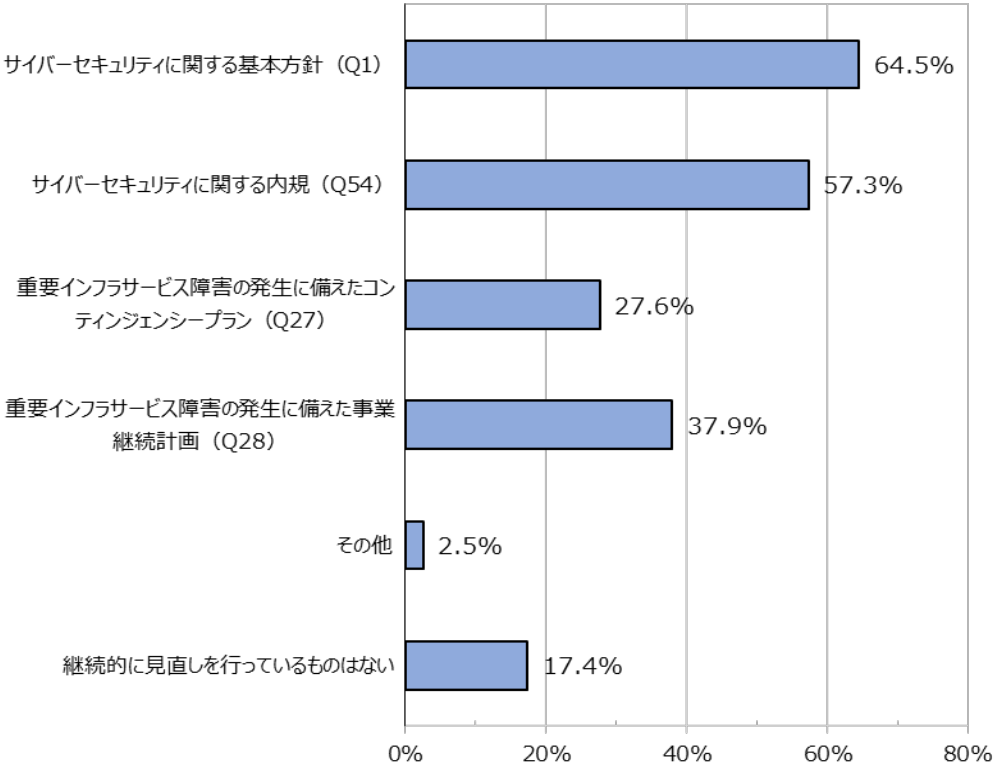
アンケート調査結果

設問56.【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。



■「その他」（主な意見を抜粋）
・取り扱う情報に留意するよう注意喚起している
・外部サービス利用規程にて、利用時の対策等について規定
・特に明文化されたものはない

設問57.【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」（主な意見を抜粋）
・検討中
・情報セキュリティポリシーを定期的に見直し
・システム管理に関する規程