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29回）

重要インフラにおける安全基準等の浸透状況等に関する調査について［2021年度］

令和４年5月30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

目次

目次

安全基準等の浸透状況等に関する調査

- 「重要インフラの情報セキュリティ対策に係る第４次行動計画」（以下「行動計画」という。）では、**各重要インフラ分野に共通して求められる情報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**、重要インフラサービスの安全かつ持続的な提供の実現を図る観点から**「安全基準等」**（注）**で規定されることが望ましい項目を整理**している。
- 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浸透状況等を把握するため、**重要インフラ事業者等に対し、情報セキュリティ対策の実施状況について「アンケート調査」及び「往訪調査」を実施**している。

（注）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。

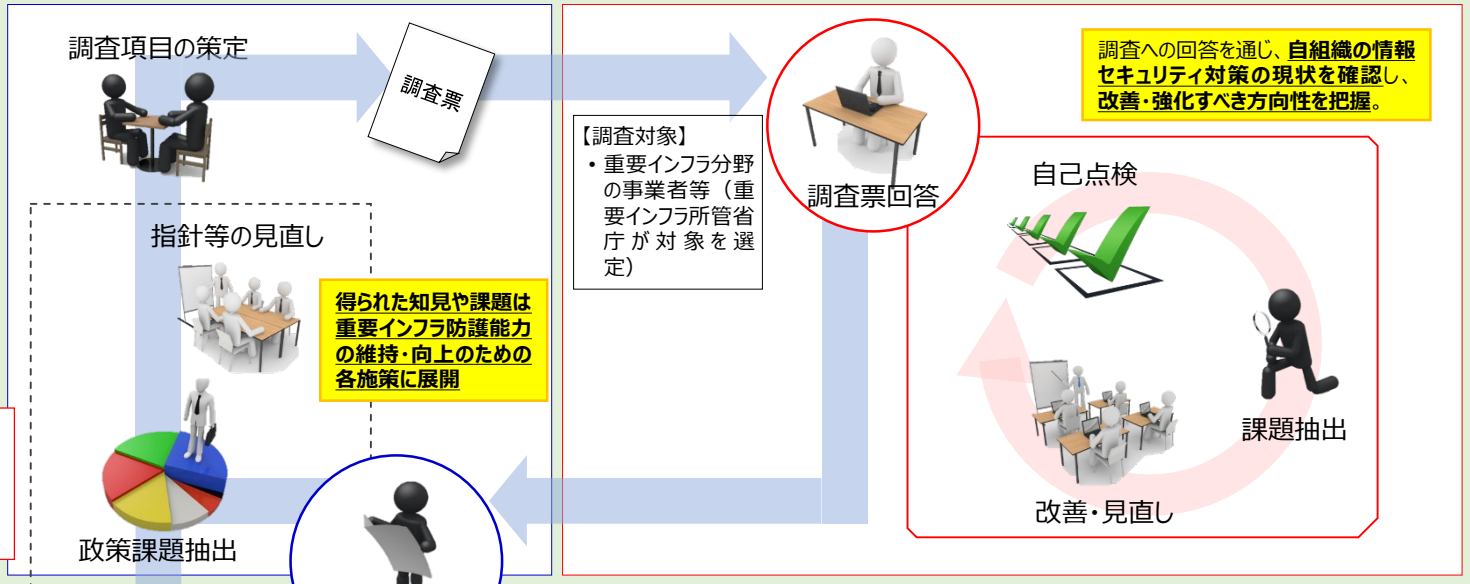
各調査の目的・内容	調査の流れ（イメージ） 内閣官房	重要インフラ事業者等

アンケート調査

【目的】
- 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**し、行動計画の検証や指針等の見直しに活用。

【内容】
- 重要インフラ事業者等の**情報セキュリティ対策の実施状況を書面で調査**。

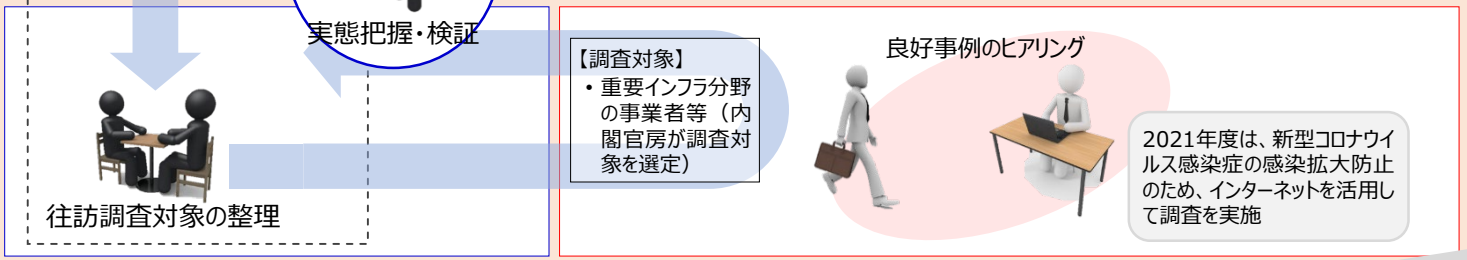
行動計画の検証のための指標
①ベースラインとなる情報セキュリティ対策に取り組んでいる重要インフラ事業者等の割合
②先導的な情報セキュリティ対策に取り組んでいる重要インフラ事業者等の割合



往訪調査

【目的】
- 情報セキュリティ対策の**良好事例の収集**等。

【内容】
- 重要インフラ事業者等に対し、ヒアリング等を実施。



（参考）調査の位置付け

「重要インフラの情報セキュリティ対策に係る第４次行動計画」

（サイバーセキュリティ戦略本部 平成29年４月18日決定、令和２年１月30日最終改定 ）

Ⅲ．計画期間内に取り組む情報セキュリティ対策

１．安全基準等の整備及び浸透

各重要インフラ分野に共通して求められる情報セキュリティ対策を「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」として策定し、必要に応じた改定を行っており、同指針を受けた形で、各重要インフラ分野におけるガイドライン等の見直し、そして重要インフラ事業者等の内規等の見直しが進められ、全体として必要な安全基準等の整備が図られている。

さらに、各重要インフラ事業者等において、安全基準等が情報セキュリティ対策の規範として浸透することにより、重要インフラサービスの安全かつ持続的な提供に必要な取組の推進が図られている。

本行動計画期間においては、**内閣官房は、重要インフラ防護能力の維持・向上を目的に、指針改定及び安全基準等の**継続的改善や**浸透状況の調査**を行う。

また、重要インフラ事業者等は、情報セキュリティ対策の重要性に鑑み、PDCAサイクルに沿った継続的かつ着実な実施に取り組む。

１.３ 安全基準等の浸透

重要インフラ事業者等における安全基準等の浸透状況のより精緻な把握を目的に、内閣官房は、毎年、重要インフラ事業者等の対策状況についてのアンケート調査及び往訪調査を実施する。アンケート調査については、重要インフラ事業者等における安全基準等の浸透及び取組の改善につながるよう、随時調査項目の見直しを行う。

具体的には、対策状況をより詳細かつ精緻に確認するための調査項目を追加するとともに、各施策によって、理想とする将来像へどの程度到達したかを把握するための調査項目を追加する。さらに、調査への回答を通じて、重要インフラ事業者等がセルフチェックを行い、自らの情報セキュリティ対策の充足度や課題点、解決策等を認識可能となるように調査票等を構成する。

また、**アンケート調査結果から得られた仮説の検証及び良好事例の収集を目的に、重要インフラ事業者等へ往訪調査を行う**。

なお、アンケート調査及び往訪調査によって得られた調査結果については、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。

Ⅴ．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

本行動計画の各施策は、いずれも重要インフラ事業者等による情報セキュリティ対策の効果を高めるため政府が支援を行うものである。施策の結果検証は、重要インフラ事業者等による情報セキュリティ対策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。なお、具体的な指標 については、前記「本行動計画の目標」を踏まえ、以下のとおり設定するものとする。

(1) 「安全基準等の整備及び浸透」に係る指標

- ○ **安全基準等の浸透状況等の調査により把握したベースラインとなる情報セキュリティ 対策に取り組んでいる重要インフラ事業者等の割合**
- ○ **安全基準等の浸透状況等の調査により把握した先導的な情報セキュリティ 対策に取り組んでいる重要インフラ事業者等の割合**

目次

浸透状況調査（アンケート調査）の概要

- 浸透状況調査（アンケート調査）は、重要インフラ事業者等における安全基準等の浸透状況等を把握するため、重要インフラの各分野における情報セキュリティ対策の実施状況について調査するものであり、2020年度に引き続き、**2021年度は、指針が「『安全基準等』において規定が望まれる」として提示している情報セキュリティ（対策項目）（注）の実施状況等について調査**を行った。
- 本調査の結果から得られた知見や課題については、必要に応じて各施策へと展開するとともに、行動計画の検証や評価に活用することとする。

（注）これらの対策項目の実施の有無が当該事業者における情報セキュリティ対策のレベルを直ちに示すものではないことに留意する必要がある。指針においても、対策項目は「重要インフラ事業者等が採否を検討する」ものとされている。

調査の概要

調査内容	**指針が「『安全基準等』において規定が望まれる」として提示している対策項目の実施状況を確認** ［ 調査基準日：2021年３月31日 ］
調査対象	**各重要インフラ分野の事業者等** ※具体的な調査対象は、各重要インフラ分野を所管する重要インフラ所管省庁が選定（ ⇒ 調査対象は7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」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

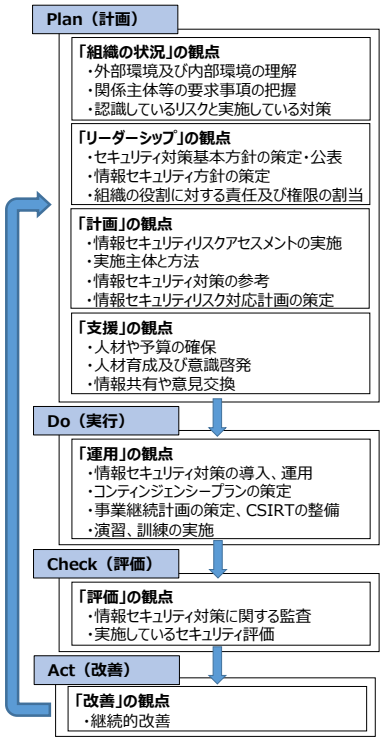
【内閣官房】
- 得られた知見や課題は必要に応じて各施策へと展開
- **行動計画の検証や評価に活用**

【重要インフラ事業者等】
- 調査への回答を通じ、**自組織の情報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**

調査票の構成

- 調査票では、これらの対策項目の実施状況が確認できるよう、指針の構成に沿って調査項目を設けることとした。

指針の構成



調査票の構成

Plan［計画］
設問１：組織の状況の観点
設問２：セキュリティポリシーの観点
設問３：情報セキュリティ対策の観点
設問４：支援の観点

Do［実行］
設問５：運用の観点

Check［評価］
設問６：評価の観点

Act［改善］
設問７：改善の観点

その他
設問８～設問11：その他の観点

調査票

- 情報セキュリティ対策のPDCAサイクルでは、通常、Planで分析結果を踏まえ対策を導出した上、Doで実行に移し、一定期間経過後、Checkで対策の見直しの必要性を評価し、Actで改善を実施するという流れになる。
- なお、実運用においては、Doでの監視・検知の結果次第では、緊急で対策内容を見直す等の動的な対応が必要となる場合がある。

調査対象及び回答状況

- 2021年度は、**全重要インフラ分野（計14分野）の事業者等を対象に調査を実施し、2,130事業者から回答**（回答率55.6%）を得た。

重要インフラ分野		調査対象事業者	回答数	調査方法
情報通信	電気通信	T-CEPTOAR構成各社、電気通信事業者協会正会員各社	26	NISC調査
	放送	日本放送協会（NHK）、地上系民間基幹放送事業者（多重単営社及びコミュニティ放送事業者を除く。）	115	
	ケーブルテレビ	ケーブルテレビセプターに加盟する全事業者	84	
金融		銀行等、証券会社、生命保険会社、損害保険会社	658	外部調査※1
航空		主たる定期航空運送事業者	7	NISC調査
空港		主要な空港・空港ビル事業者	8	
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	20	
電力		一般送配電事業者、主要な発電事業者	13	
ガス		大手事業者	10	
政府・行政サービス		都道府県及び市区町村	1,043	
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	
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	86	
物流		大手物流事業者	9	
化学		石油化学工業協会に加盟する事業者のうち主にエチレンセンターを運営する企業	4	
クレジット		重要インフラ事業者として定めている全事業者	18	
石油		石油連盟に加盟する石油精製・元売の全事業者	7	
全分野合計		－－－	**2,130 (1,472)**※	

※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リスク
  - 設問1-5. 実施している対策

- **リーダーシップの観点**
  - 設問2-1. 基本方針の策定・公表
  - 設問2-2. 安全基準等の把握
  - 設問2-3. 基本方針策定に当たり参考としている基準等
  - 設問2-4. 情報セキュリティ対策に関する責任・権限の割当
  - 設問2-5. 自組織で設置している情報セキュリティに係る役職等

- **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定期実施
  - 設問3-5. 重要インフラサービスに与える影響の度合いの特定
  - 設問3-6. 情報セキュリティ対策の実施に当たり参考としている基準等
  - 設問3-7. 実施している情報セキュリティ対策
  - 設問3-8. 情報セキュリティ対策の取りまとめ
  - 設問3-9. 情報セキュリティ対策の導入・実施に関する計画の策定
  - 設問3-10. 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. 資源（人材・予算）の明確化、適切な配分
  - 設問4-2. 必要としている情報セキュリティ人材
  - 設問4-3. 情報セキュリティに係る人材育成や意識啓発に関する取組
  - 設問4-4. 情報処理安全確保支援士の活用
  - 設問4-5. 情報共有や意見交換を行っている関係主体
  - 設問4-6. 情報共有の範囲

□ Do［実行］

設問5-1. 情報セキュリティ対策の導入・運用段階における取組
設問5-2. 外部機関から共有・提供された情報の自組織での活用
設問5-3. コンティンジェンシープランの策定
設問5-4. 事業継続計画の策定
設問5-5. 実施・参加している演習・訓練

□ Check［評価］

設問6-1. 情報セキュリティ対策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］

設問7-1. 情報セキュリティ対策の改善に向けた継続的な見直し
設問7-2. 情報セキュリティ対策の見直しの契機

□ その他

- **経営層のコミットメント**
  - 設問8-1. 経営層の関与
  - 設問8-2. 経営層とのコミュニケーション
  - 設問8-3. 経営会議での情報セキュリティリスクの扱い

- **クラウドサービスの利用について**
  - 設問9-1. 確認しているクラウドサービス提供事業者の情報セキュリティ
  - 設問9-2. クラウドサービス利用に関する運用対策や情報セキュリティ対策

- **テレワークを活用した働き方について**
  - 設問10-1. テレワークで実施しているセキュリティ対策

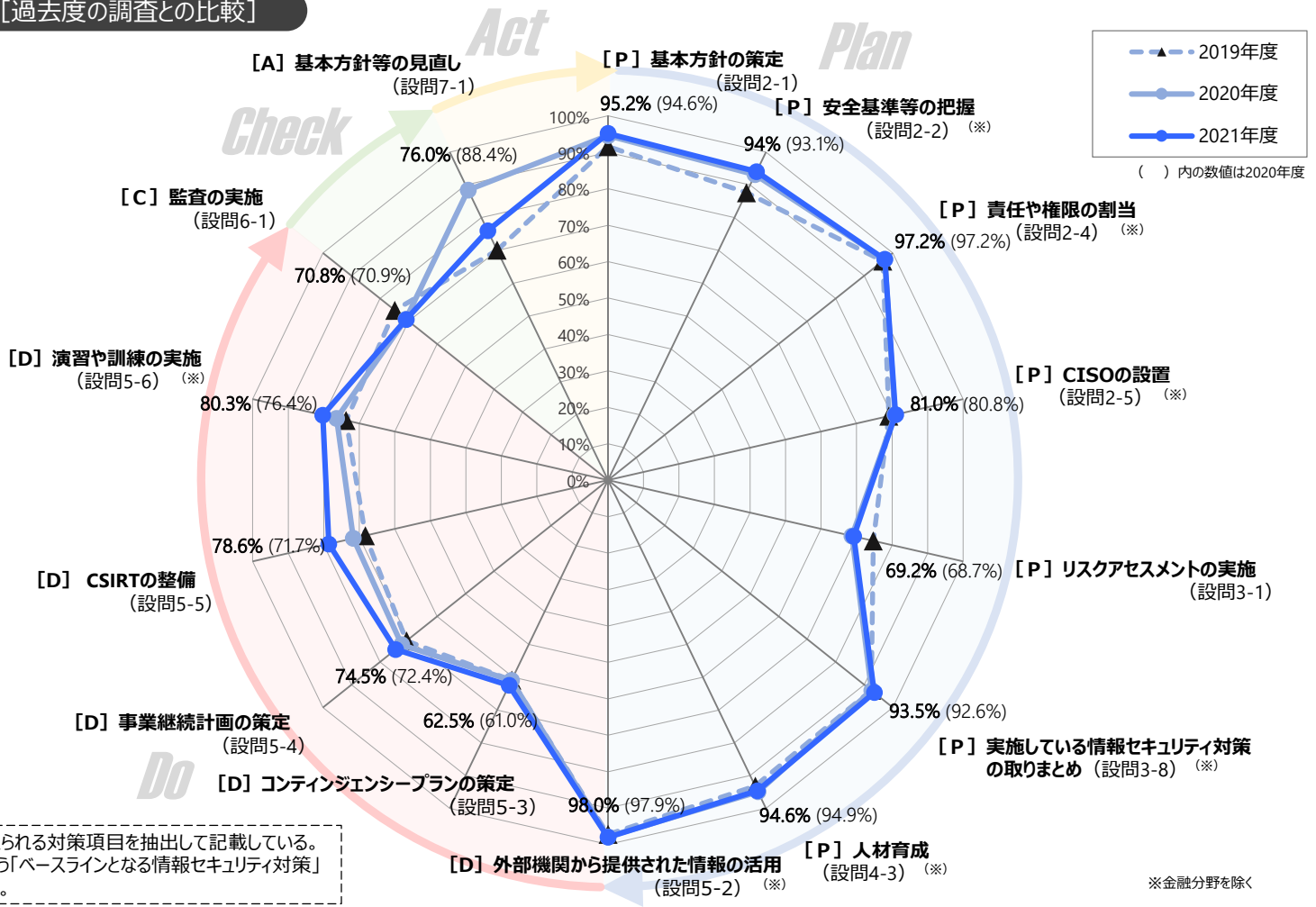
- **昨今のインシデント等を受けて**
  - 設問11-1. 代替サービス利用の対策
  - 設問11-2. 制御系システムのセキュリティ対策
  - 設問11-3. サイバー保険の加入有無
  - 設問11-4. ランサムウェア攻撃への対策、運用体制

- **重要インフラ分野の依存関係について**
  - 設問11-5. 依存している重要インフラ分野、外部サービス［非公開］

アンケート調査結果概要（総評）　－　ベースラインとなる情報セキュリティ対策

- 重要インフラの各分野における**情報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**しており、**安全基準等は浸透しつつある**と一定の評価ができる。一方で、項目によって実施状況に差があり、**Plan（計画）に係る項目として比較して、Do（実行）、Check（評価）に係る項目の実施状況は相対的に低い**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。
- 複雑化・巧妙化する情報セキュリティ上の脅威に対処していくためには、環境の変化にあわせて対策の見直しと改善を行っていく必要がある。重要インフラ事業者等においては、**PDCAサイクルを構築し、着実に情報セキュリティの確保に向けた取組を進めていくことが期待**される。

各取組の実施状況［過去度の調査との比較］



※金融分野を除く

設問の中から基礎的な取組と考えられる対策項目を抽出して記載している。これらの対策項目を行動計画でいう「ベースラインとなる情報セキュリティ対策」とみなし、評価に活用することとする。

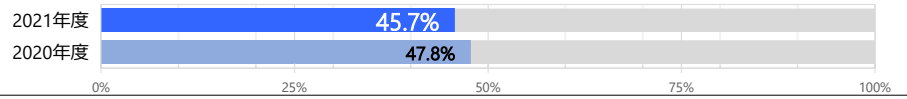
アンケート調査結果概要（総評）　－　先導的な情報セキュリティ対策（1/2）

- 行動計画では、**行動計画に基づく取組によって実現が期待される将来像を「理想とする将来像」として提示**している。これらの将来像に関連すると考えられる対策項目を「先導的な情報セキュリティ対策」とみなして本調査結果を整理したところ、**2020年度と同様の水準で推移**しており、**関係主体との情報共有等が多くの組織で実施されている**と評価できる。
- 一方で、「経営層との定期的なレポーティング・対話」、「機能保証の考え方を取り入れたリスクアセスメント」等、**2020年度と同様に2021年度調査でも実施状況が低い項目が見受けられる**ことから、行動計画が示す理想とする将来像の実現に向けては、これらの改善を図っていく必要がある。

将来像①：「情報セキュリティガバナンス」に関する次の事項が重要インフラ事業者等の間で十分に浸透している。

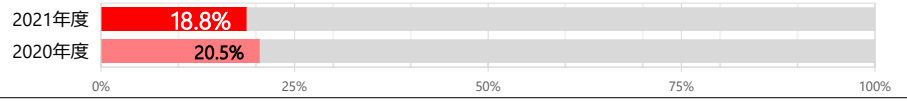
情報セキュリティ対策が単に情報システムの構築・運用の観点だけでなく、**企業経営の観点からも検討**されていること。

- 経営層からの関与がある（設問8-1）（※）　※金融分野を除く



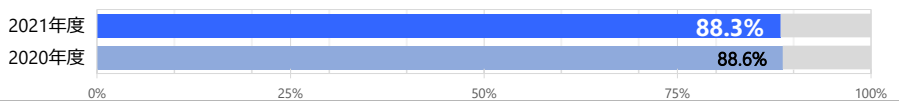
システムの構築・運用及び企業経営の**各責任者が定期的に、適切に相互関与する体制が整備**されていること。

- 経営層と定期的なレポーティング・対話の場が設けられている（設問8-2）（※）

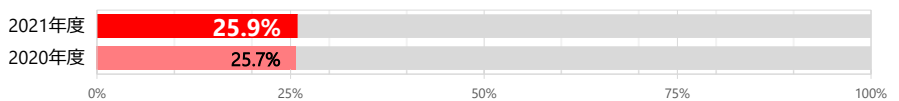


守るべき重要インフラサービス及びサービス維持レベルを踏まえ、**自らがなすべき必要な対策が理解**されていること。

- 関係主体からの要求事項を整理している（設問1-2）（※）

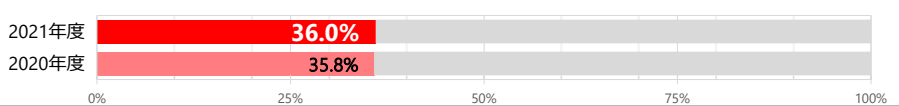


- 機能保証の考え方を取り入れたリスクアセスメントを実施している（設問3-1）（※）



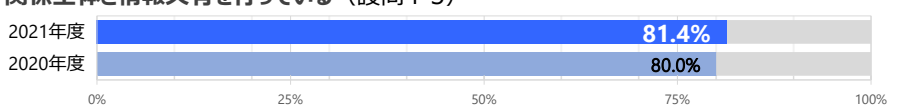
平時における情報セキュリティ対策に対する姿勢やインシデント発生時の対応に関する**情報の開示などが取り組まれている**こと。

- 基本方針を策定し外部に公表している（設問2-1）（※）



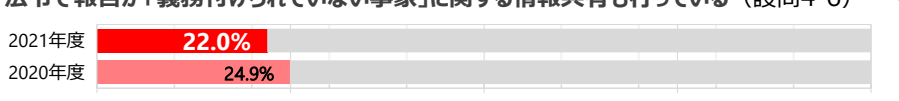
情報セキュリティ対策の水準の向上のためには可能な限り**情報共有を行うという姿勢が積極的に評価される価値観が醸成**されていること。

- 関係主体と情報共有を行っている（設問4-5）（※）



事業における重要インフラサービス障害の発生について、これを隠すべきものではなく、重要インフラ事業者等内の情報セキュリティ対策に取り組む**関係者間で共有すべきものであるという認識が醸成**されていること。

- 法令で報告が「義務付けられていない事象」に関する情報共有も行っている（設問4-6）（※）

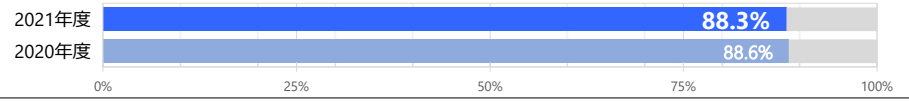


アンケート調査結果概要（総評）　－　先導的な情報セキュリティ対策（2/2）

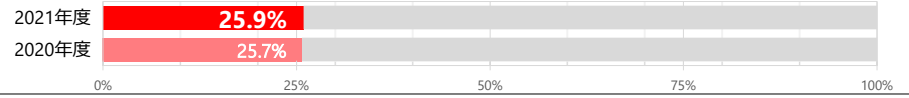
将来像②：「課題抽出」、「リスク評価」及び「対策の改善」に関する次の事項が十分に浸透している。

本行動計画に基づき、関係主体が連携して重要インフラ防護に関する情報セキュリティ対策に取り組むことによって、**自らの情報セキュリティ対策の程度及び残存するリスクが認識**されていること。

- **関係主体からの要求事項を整理している**（設問1-2）（※）【再掲】　※金融分野を除く

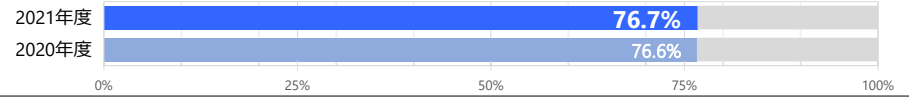


- **機能保証の考え方を取り入れたリスクアセスメントを実施している**（設問3-1）（※）【再掲】

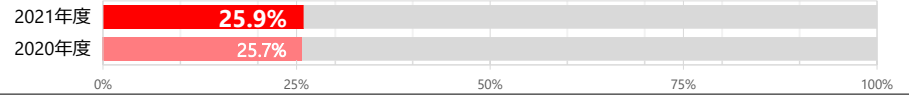


各種情報セキュリティ対策の進展や環境変化によるリスク源や重要インフラサービス障害に係る**リスクの変化を適切に察知して、各々自主的に対策を進め、また必要な調整を行うようになっている**こと。

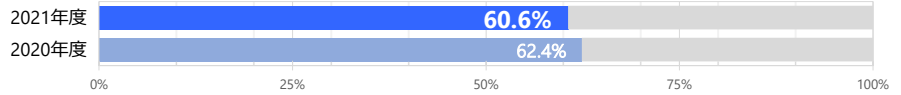
- **内部環境や外部環境を整理している**（設問1-1）（※）



- **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**（設問3-1）（※）【再掲】

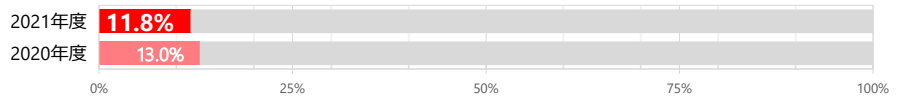


- **情報セキュリティ計画を策定している（策定中を含む）**（設問3-9）（※）



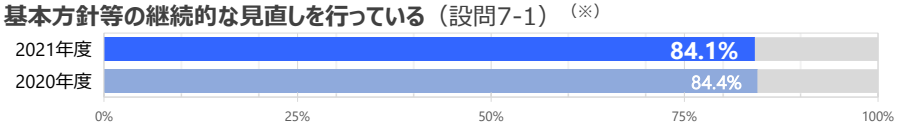
重要インフラサービス障害が発生した場合に備えた適切な対策を講じることが可能になっており、その成果として、**重要インフラサービス障害が国民生活や社会経済活動に重大な影響を与えるリスクを可能な限り低減**させることができていること。

- **情報セキュリティ対策のために適切に十分な資産（人材＋予算）配分を行っている**（設問4-1）（※）



これらの取組が**対策の継続的な改善の原動力の一つとなっている**こと。

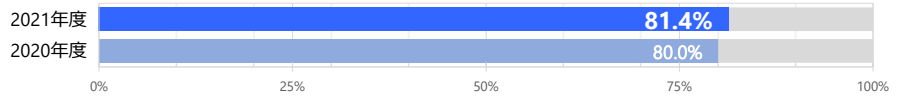
- **基本方針等の継続的な見直しを行っている**（設問7-1）（※）



将来像③：「情報共有」に関する次の事項が十分に浸透している。

重要インフラサービス障害の発生状況等に関する情報の把握ができており、必要に応じて当該情報が各分野のセプターやセプターカウンシルを通じて**外部の関係主体と共有され、公式又は非公式の連携が行われている**こと。

- **関係主体と情報共有を行っている**（設問4-5）（※）【再掲】　※金融分野を除く

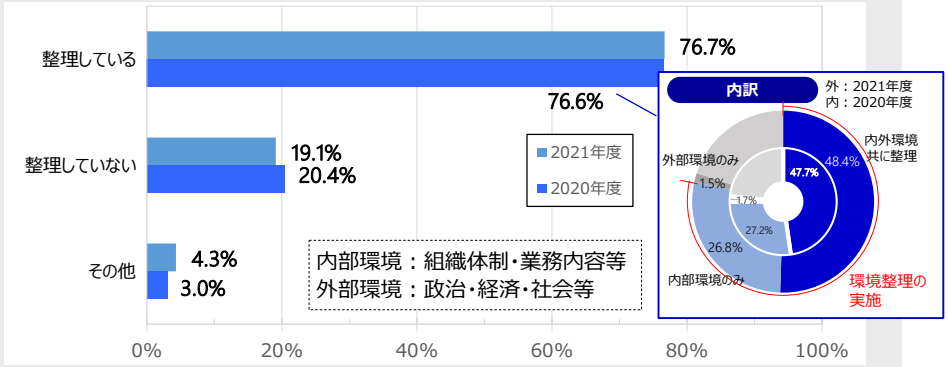


アンケート調査結果概要　－　Plan［計画］（1/3）

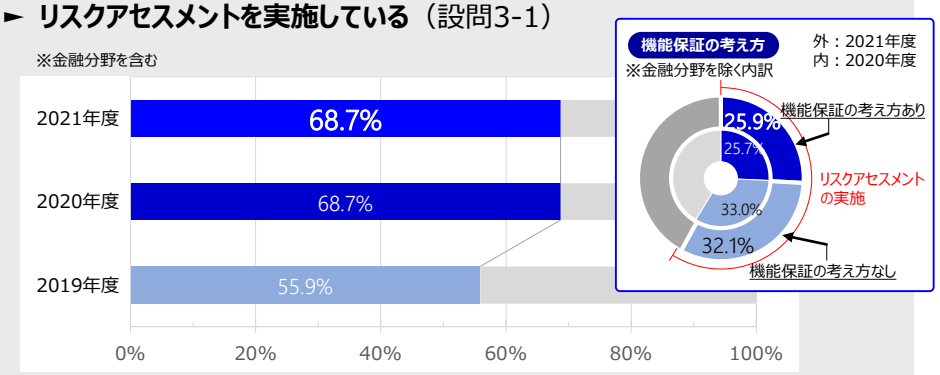
- 自組織の**重要インフラサービスに影響を与えるおそれがある環境の整理は多くの組織で実施**されており、自組織を取り巻く状況の把握は進んでいる。また、**リスクアセスメントについても着実に進展**してはいるものの、**外部環境を含めた環境の整理や機能保証の考え方の取り入れたリスクアセスメントは一部にとどまっており**、サイバー攻撃の高度化・多様化に伴うリスクの複雑化という観点からも、**今後も引き続きの取組が必要**である。
- 自組織のサプライチェーンの把握については重要インフラ事業者等において着実に意識付けされている。個別の対策についても、**必要な取組が網羅的に実施されるよう促進することが必要**である。

組織の状況の観点／情報セキュリティ対策の観点

► 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内部環境・外部環境を整理している（設問1-1）　※金融分野を除く



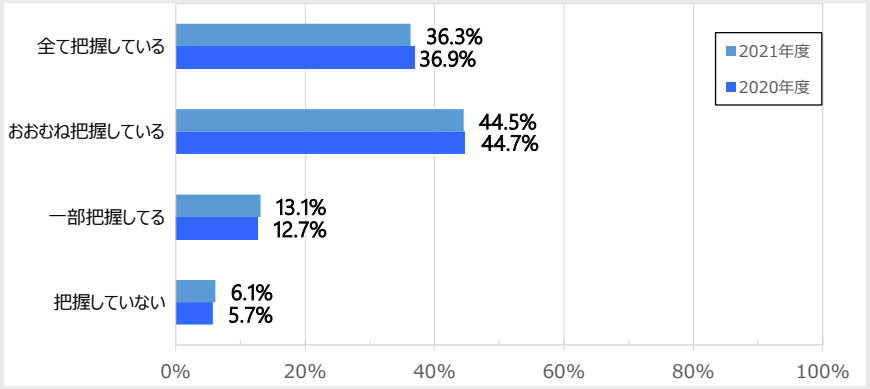
► リスクアセスメントを実施している（設問3-1）



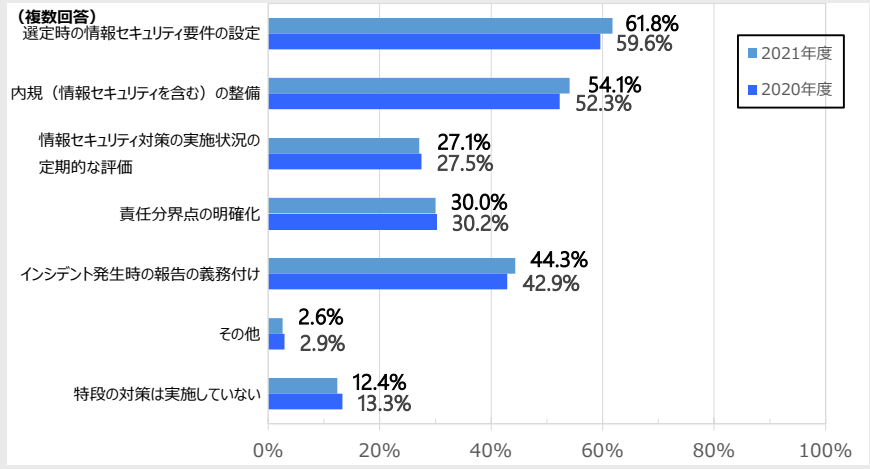
機能保証：重要インフラサービスを安全かつ持続的に提供するため、関係主体が情報セキュリティ対策に関する必要な努力を適切に払うことを求める考え方

組織の状況の観点

► 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について実施している対策（設問1-5）　※金融分野を除く



アンケート調査結果概要 － Plan［計画］（2/3）

- ①情報セキュリティ基本方針、③情報セキュリティ対策実施手順等を策定している組織は2020年度から横ばいであり、**情報セキュリティに係る方針や基準の整備について一定の浸透が図られている**。一方、具体的な基準や計画を規定する**②情報セキュリティ対策基準を策定済みの組織は比較的少数にとどまっている**。情報セキュリティ対策の実効性を確保するためにも、今後、各組織において策定されることが期待される。
- また、重要インフラ事業者等において、自分野の関係法令及び安全基準等は情報セキュリティポリシを改善していく上で把握、参考とされていることから、策定主体において**今後も適切な見直しを行っていくことが期待**される。

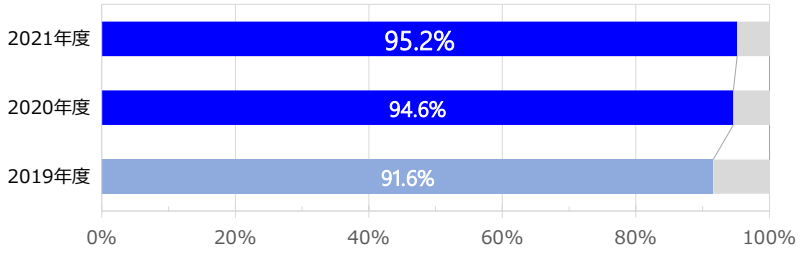
セキュリティポリシの観点／情報セキュリティ対策の観点

情報セキュリティに係る方針や基準の整備

①情報セキュリティ基本方針

情報セキュリティに対する組織としての統一的かつ基本的な考え方や方針

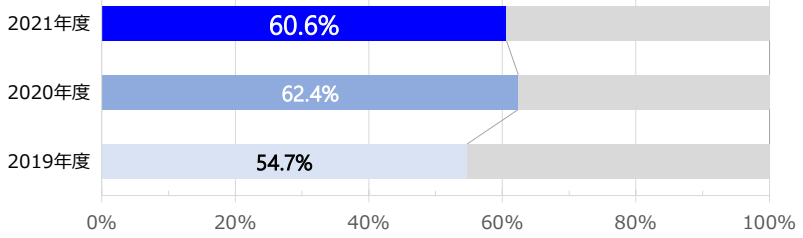
► **情報セキュリティ基本方針を策定している**（設問2-1）



②情報セキュリティ対策基準

情報セキュリティ基本方針を実践し、適切な情報セキュリティレベルを確保・維持するための具体的な遵守事項や基準

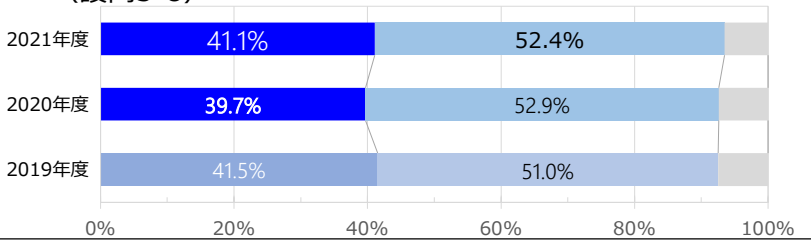
► **情報セキュリティ対策基準を策定している**（設問3-9）※金融分野を除く



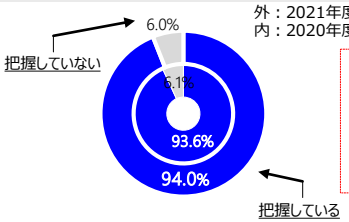
③情報セキュリティ対策実施手順

情報セキュリティ対策を実施するための詳細な手続・手順（マニュアル等）

► **情報セキュリティ対策実施手順を全てもしくは一部策定している**（設問3-8）

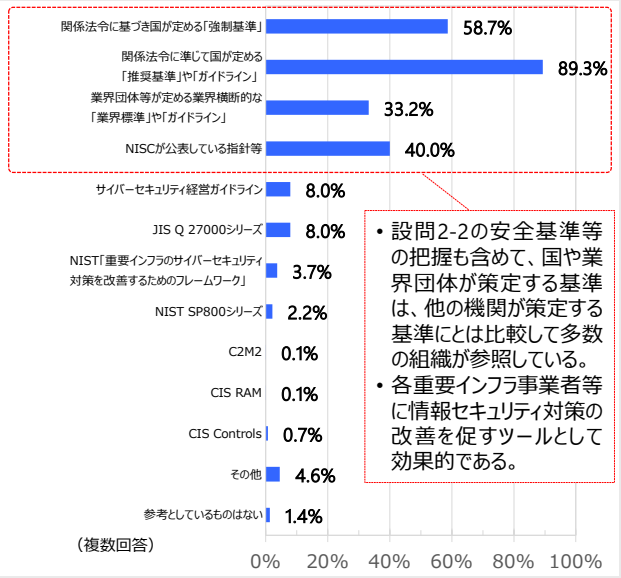


► **自分野に関係する安全基準等を把握している**（設問2-2）※金融分野を除く



- 一部の組織は自分野の安全基準等を把握できていない。
- 周知に向けた取組が必要。

► **情報セキュリティに係る方針の策定に当たって参考としている基準等**（設問2-3）※金融分野を除く



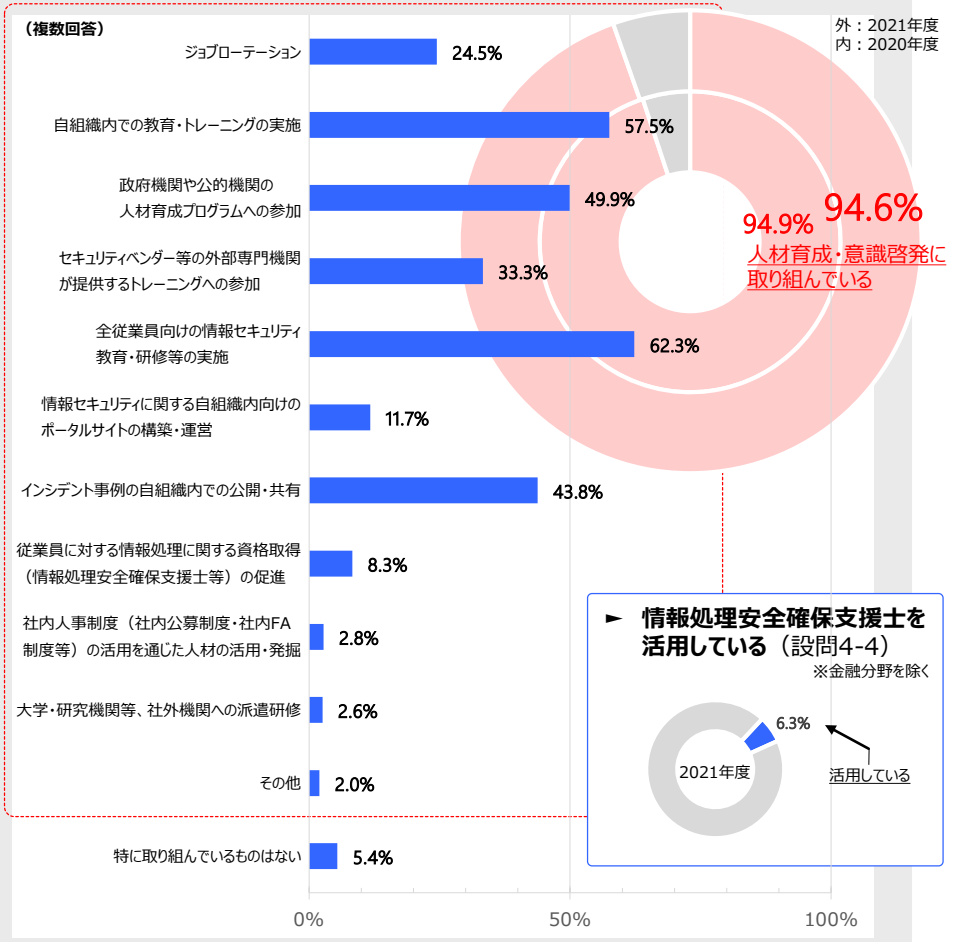
- 設問2-2の安全基準等の把握も含めて、国や業界団体が策定する基準は、他の機関が策定する基準にとは比較して多数の組織が参照している。
- 各重要インフラ事業者等に情報セキュリティ対策の改善を促すツールとして効果的である。

アンケート調査結果概要　－　Plan［計画］（3/3）

- 情報セキュリティに係る人材育成や意識啓発については9割以上の組織が何らかの取組を実施しており、**ほぼ全ての組織で研修や訓練を通じた人材育成等が行われている**。
- 一方で、**自組織において人的資産が適切に配分されていると回答した組織は若干低下**しており、人材育成・意識啓発に関する取組は積極的に進められているものの、**情報セキュリティに係る人材が深刻化**していることが確認できる。また、自組織で必要としている人材も管理者から現場の従事者まで多岐にわたっており、今後も**人材の育成・確保が多くの組織の課題**であるといえる。

支援の観点

► 情報セキュリティに係る人材育成・意識啓発の取組（設問4-3）※金融分野を除く

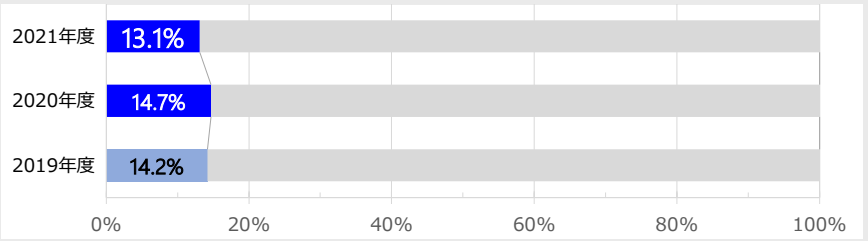


► 情報処理安全確保支援士を活用している（設問4-4）

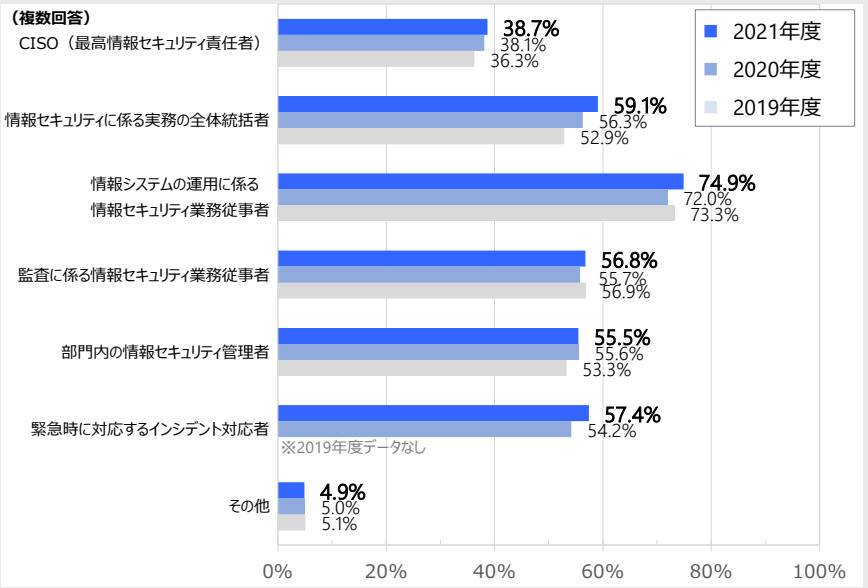
※金融分野を除く

► 情報セキュリティに係る人的資産が適切に配分されている（設問4-1）

※金融分野を除く



► 自組織で必要としている情報セキュリティ人材（設問4-2）※金融分野を除く



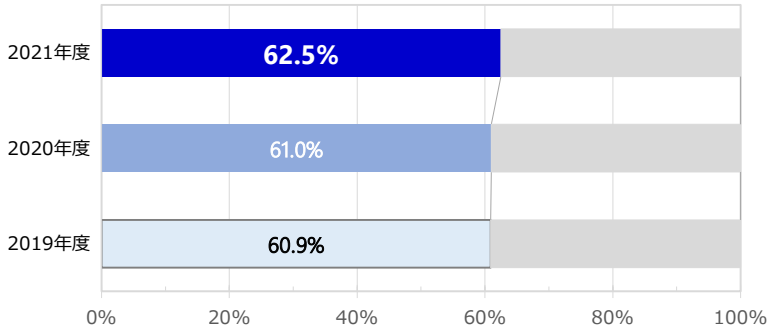
アンケート調査結果概要　－　Do［実行］

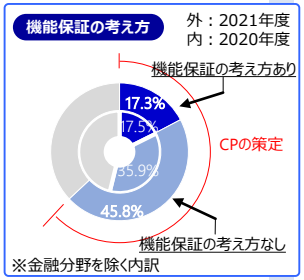
- コンティンジェンシープランや事業継続計画の策定、CSIRTの整備は多くの組織で進められ、その実施状況は2018年度から大きく向上しており、**重要インフラサービスの障害の発生に備えた対処態勢の整備は着実に進展**している。
- また、演習・訓練の実施・参加、外部機関から共有・提供された情報の活用の状況から、重要インフラ事業者等が**自組織の対処能力の向上に努めていることが確認**できる。ただし、一部の組織は演習・訓練に参加していないことから、我が国全体の対処能力を向上させるためにも、それらの組織に対して**政府機関や公的機関が提供する演習等への参加を引き続き促していくことが必要**であると考えられる。

運用の観点

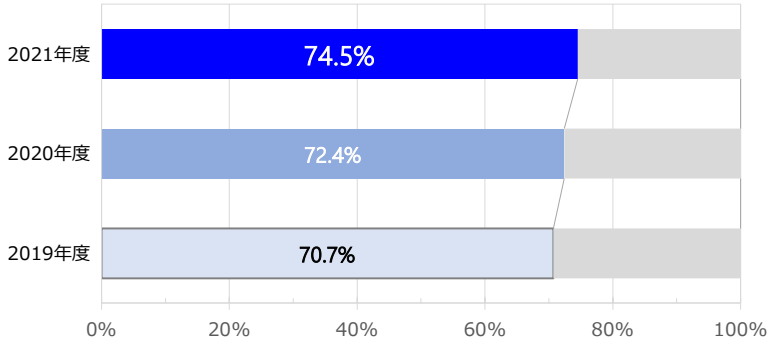
重要インフラサービス障害の発生に備えた対処態勢の整備

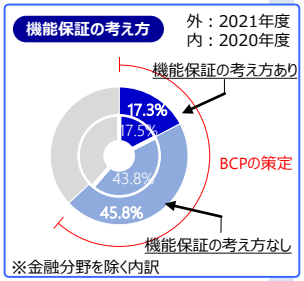
► **コンティンジェンシープラン（CP）を策定している**（設問5-3）





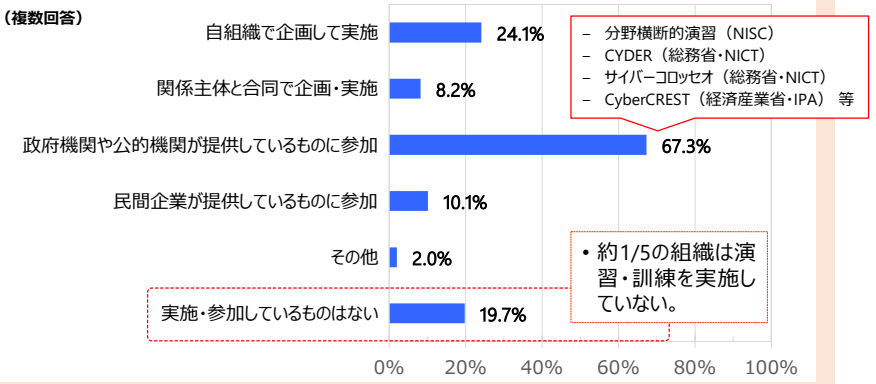
► **事業継続計画（BCP）を策定している**（設問5-4）



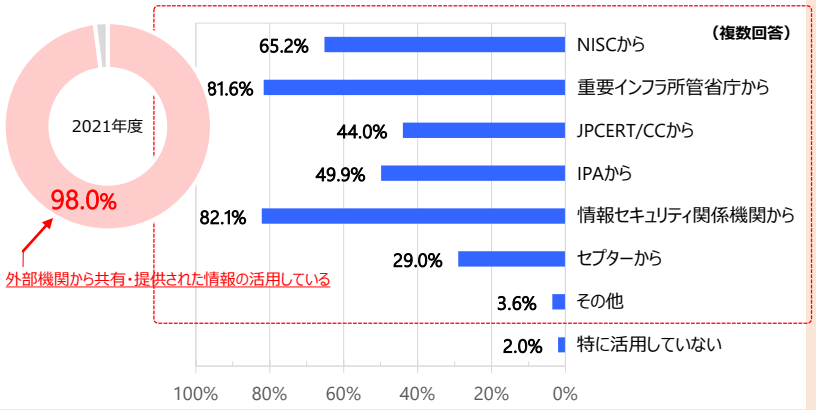


演習・訓練及び情報活用による対処能力の向上

► **実施・参加している演習・訓練**（設問5-5）※金融分野を除く



► **外部機関から共有・提供された情報の活用**（設問5-2）※金融分野を除く

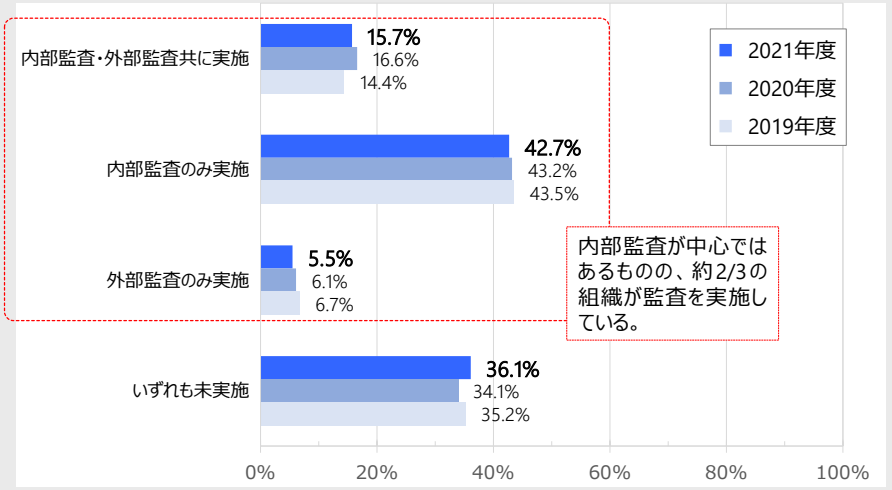


アンケート調査結果概要　－　Check［評価］／ Act［改善］

- 約2/3の組織で**内部監査を中心に情報セキュリティ対策に関する監査が実施**されており、**「評価」の枠組みは一定程度構築**されていると考えられるが、監査結果を基にした見直しの実施は少数にとどまっている。環境が変化していく中で適切に情報セキュリティを確保していくためには、現状を評価し、適時に改善していくことが必要不可欠であることから、**「評価」を「改善」につなげていく体制を構築していくことが引き続きの課題**であるといえる。
- また、情報セキュリティ対策に経営層が関与する組織は４割を超えているものの、定期的なレポーティング・対話の場が設けられているのは２割弱にとどまっていることから、**経営層との密なコミュニケーションを図っていくことが重要**であると考えられる。

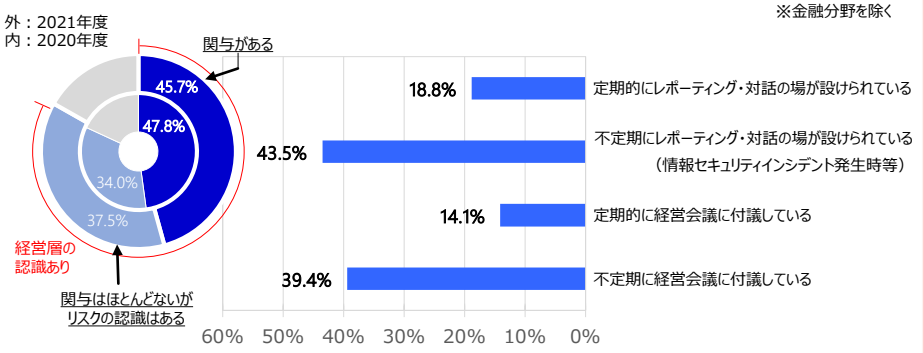
評価の観点

► 情報セキュリティ対策に関する監査を実施している（設問6-1）※金融分野を除く



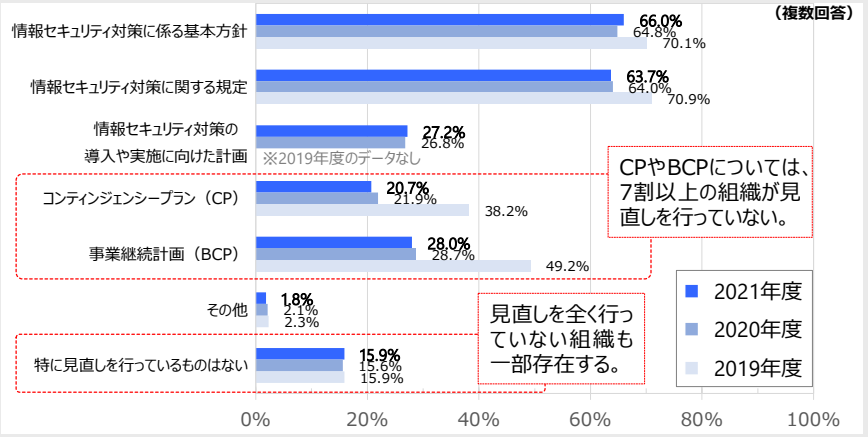
► 情報セキュリティ対策に経営層が関与している（設問8-1, 8-2, 8-3）

※金融分野を除く

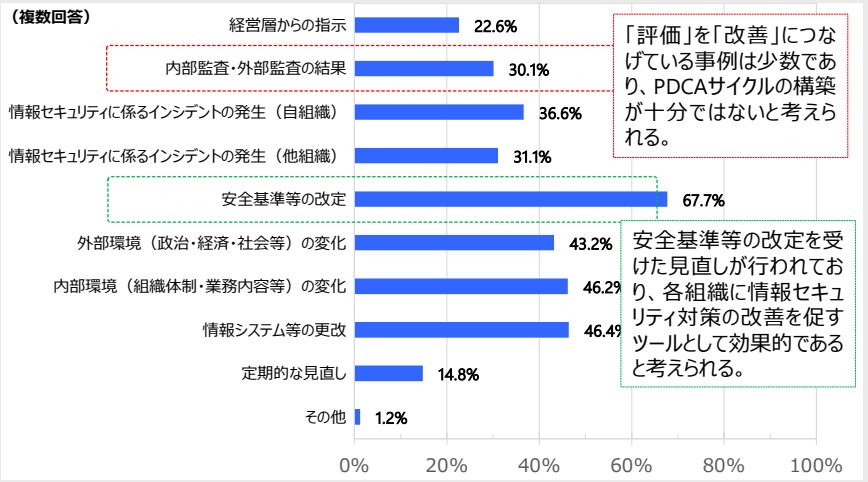


改善の観点

► 継続的に見直しを行っている（設問7-1）※金融分野を除く



► 情報セキュリティ対策の見直しの契機（設問7-2）※金融分野を除く



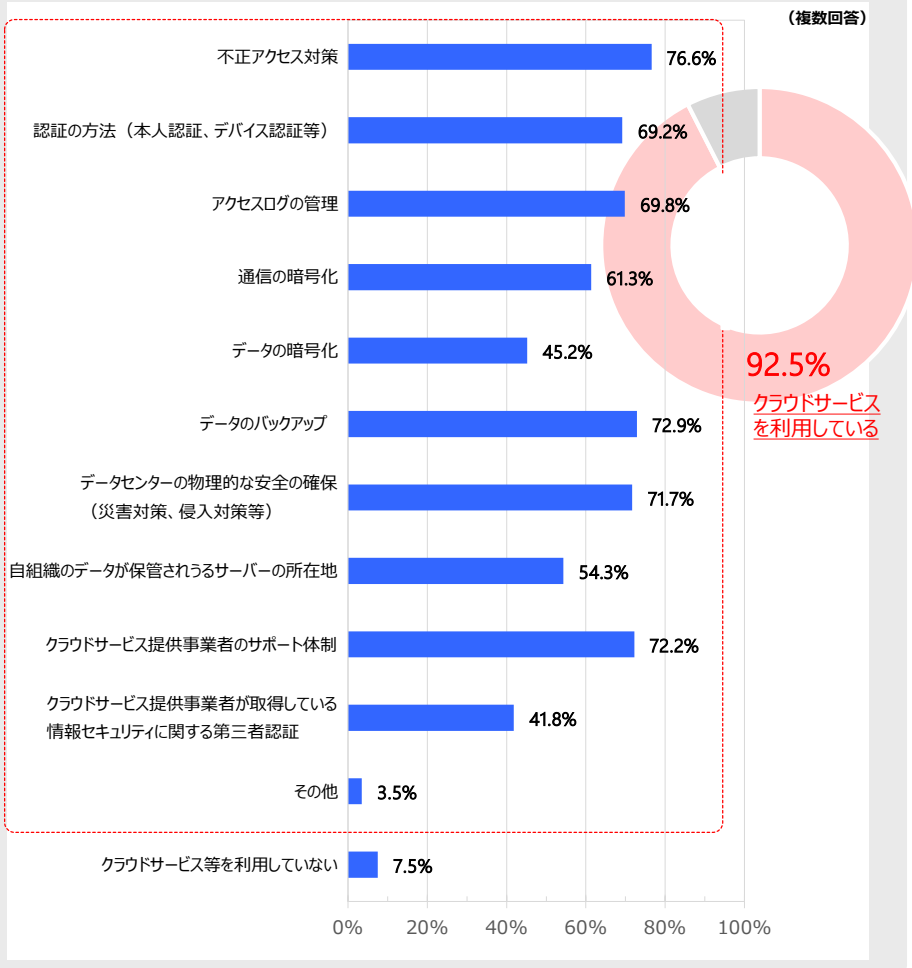
アンケート調査結果概要　－　その他（クラウドサービスの利用）

- 現在、**多くの重要インフラ事業者等においてクラウドサービスが利用**されており、クラウドサービス提供者側の情報セキュリティ対策として、不正アクセス対策や認証の方法の整備、アクセスログの管理、通信の暗号化等をはじめとするセキュリティ対策が実施されている。
- **責任範囲の整理、連絡窓口の設置については半数以上の組織で実施**されている。**マニュアルの整備、アップデートの際のレビューなどの比較的実施率の低い取組についても実施を推進**することが重要と思われる。

クラウドサービスの利用について

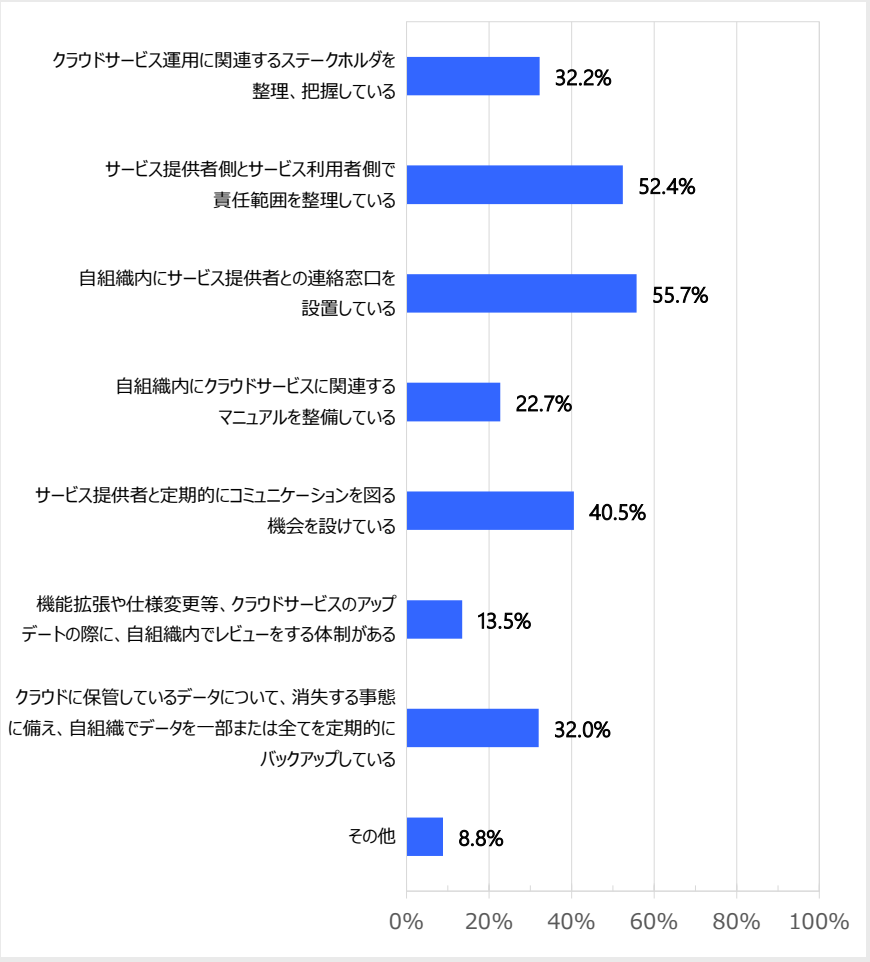
► 自組織がクラウドサービスを利用する際に確認している クラウドサービス提供事業者側の情報セキュリティ対策（設問9-1）

※金融分野を除く



► クラウドサービス利用に関する運用対策や情報セキュリティ対策（設問9-2）

※金融分野を除く



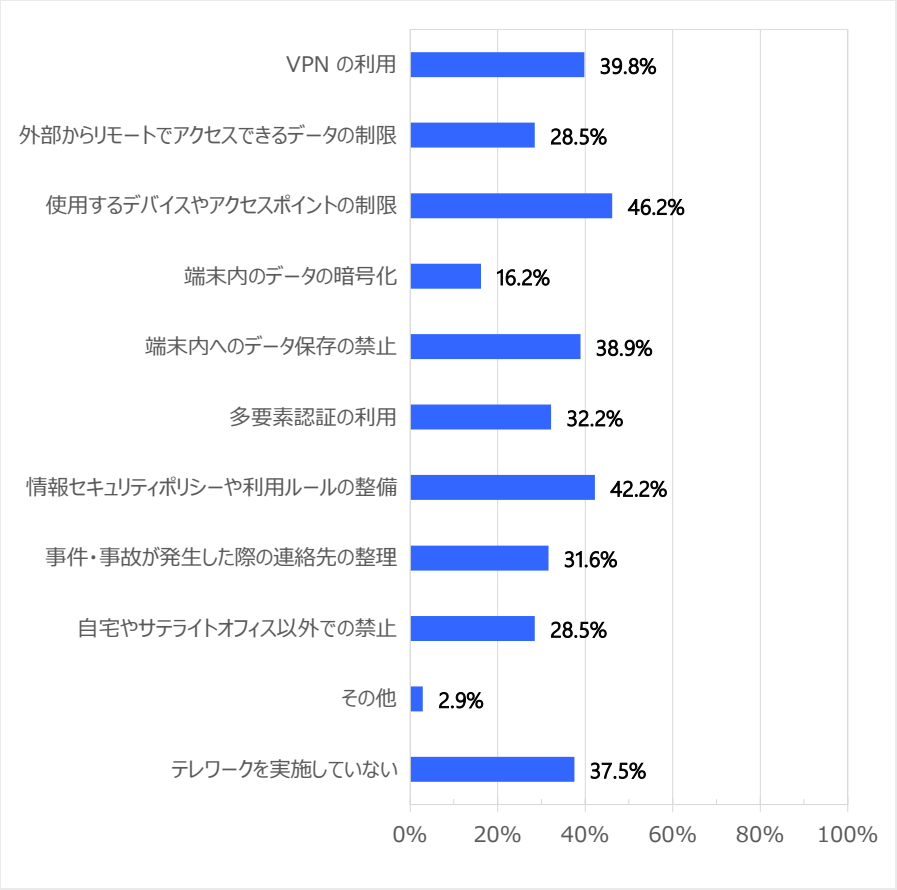
アンケート調査結果概要　－　その他（テレワーク等）

- 新型コロナウイルス感染症の拡大を契機に多くの組織でもテレワークが実施されたが、**重要インフラ事業者等においても6割以上の組織でテレワークが実施**されている。テレワークにおいては、一般にセキュリティ上の脅威が高まるため、適切にセキュリティ対策を実施していく必要がある。
- 外部サービスが利用不可能になった場合の対策としては、**「サービス提供者とSLAを締結」との回答が4割以上**あったものの、**それを上回る事業者から「特に対策を取っていない」という回答**が得られた。

新型コロナウイルスの取組について

► テレワークのセキュリティ対策（設問10）

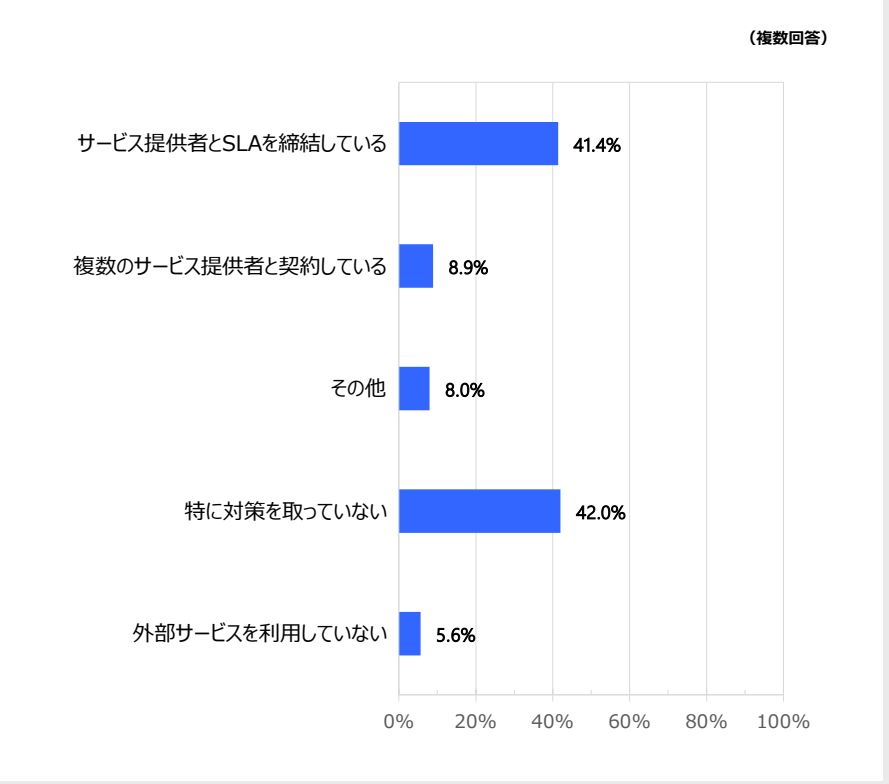
※金融分野を除く



代替対策について

► 外部サービスが利用不可になった場合の代替対策（設問11-1）

※金融分野を除く



SLA（Service Level Agreement）：サービス提供者と顧客の間で結ばれるサービス水準に関する合意である。契約で合意されたとおりにサービスを顧客に提供する。

目次

浸透状況調査（往訪調査）の概要

- 内閣官房では、重要インフラ分野における情報セキュリティ対策の良好事例を収集するため、書面による安全基準等の浸透状況の調査に加えて、**重要インフラ事業者等に対して個別に調査（往訪調査）を実施**している。
- 2021年度の往訪調査においては、サイバー攻撃が複雑化・巧妙化し、その適切な対応が課題となっている昨今の状況を踏まえ、**リスクマネジメント、人材育成等に関する調査を実施**した。

【調査対象（2021年度）】 情報通信分野、航空分野、空港分野、鉄道分野、水道分野等の重要インフラ事業者等

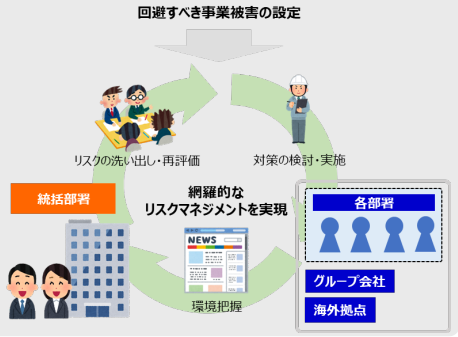
往訪調査結果概要

事例① リスクマネジメントについて

- **回避すべき事業被害**を事前に設定
- **海外拠点及びグループ会社を含めて**リスクアセスメント、対策検討

✓ **網羅的なリスクマネジメント**を実現

● 網羅的なリスクマネジメント



事例② 人材育成について

- **経営層を含めたセキュリティ勉強会**、**体験型セキュリティ教育**、**インシデント訓練**等の実施

✓ **組織全体のセキュリティ意識**の醸成
✓ **実践的な障害対処能力**の育成

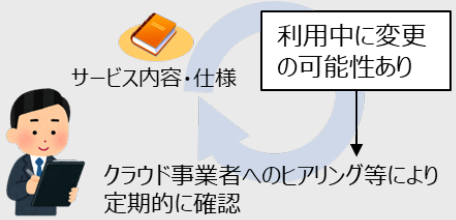
● 職員が自作したゲーム形式の体験型セキュリティ教育の実施

事例③ クラウドサービス利用に係る対策について

- **クラウド利用の内規**の整備
- クラウドサービスに係る設定不備、脆弱性、仕様変更等の確認

✓ **外部サービスも含めたセキュリティ確保**の実現

● 定期的なサービス内容や仕様変更の確認

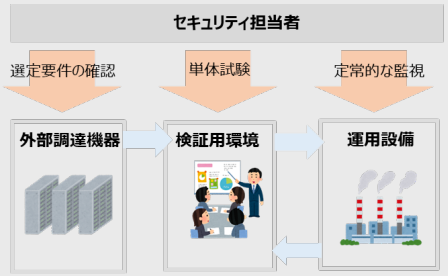


事例④ 外部調達機器のセキュリティ対策について

- 運用環境への導入前に**独立した検証用環境で試験**
- 導入後も**定常的なログ監視**等を実施

✓ **機器のライフサイクル全体にわたりリスク軽減**を実現

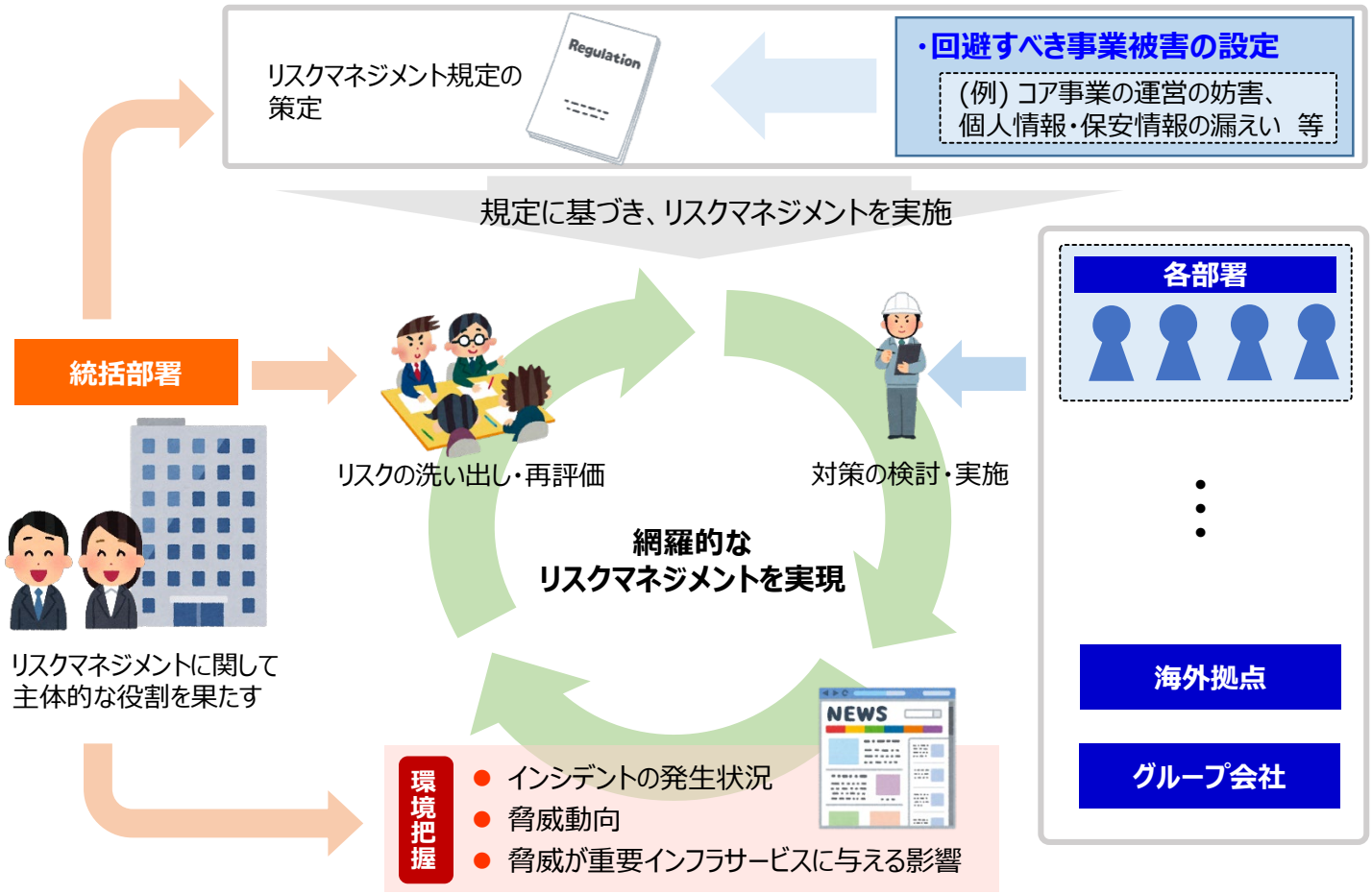
● ライフサイクル全体にわたるリスク軽減



事例① － リスクマネジメントについて

事例の概要

- 複雑化・巧妙化するサイバーセキュリティ上の脅威に対応するため、統括部署において**回避すべき事業被害を設定**した上で、**リスクマネジメント規定を策定**している。
- 規定に基づき、**海外拠点及びグループ会社を含めて組織全体を対象に毎年リスクアセスメントを実施**している。リスクアセスメントにあたっては、**インシデントの発生頻度、影響度、直近の傾向等を考慮**している。
- リスクアセスメント結果に基づき、対策が必要とされるリスクを抽出し、対象部署にて実施対策を検討している。



本事例のポイント

- ✓ 統括部署において**回避すべき事業被害を設定した上で、リスクマネジメント規定を策定**。
- ✓ **海外拠点及びグループ会社を含めて定期的にリスク評価を実施。**リスク評価に基づき、対策が必要なリスクを抽出し、実施対策を検討。

本事例の利点

- ✓ 海外拠点及びグループ会社を含め、**組織全体でのリスク管理を実現**。
- ✓ 定期的なリスクアセスメントにより、環境変化等に伴う**リスク変動に対応**。

事例② － 人材育成について

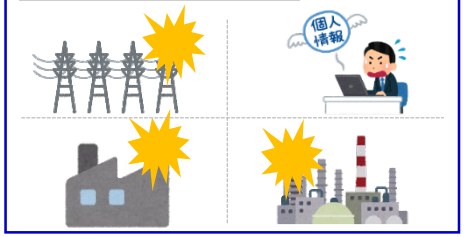
事例の概要

- 国内外で発生しているサイバーインシデント被害事例と対策の重要性を社内に展開し、**経営層を含めた組織全体でのサイバーセキュリティへの意識の浸透**を図っている。
- **セキュリティ人材の階層**（技術者層、一般従業員）**に応じた人材育成**を実施している。
- 実践的な障害対処能力を育成するため、毎年テーマを定めて、**重要インフラの機能保証のための訓練**を実施している。

◆ 組織全体でのサイバーセキュリティへの意識の浸透・底上げ

組織全体向け

サイバーインシデント事例・対策をケーススタディとして、**経営層を含めた勉強会を開催**



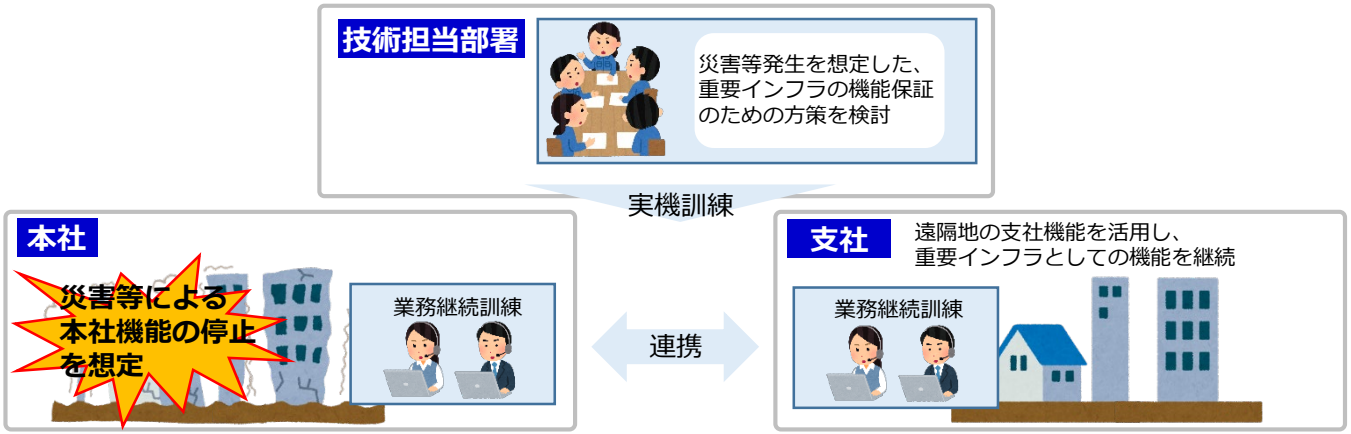
技術担当向け

外部機関の人材育成プログラムへ担当を派遣

一般職員向け

職員が自作したゲーム形式の体験型セキュリティ教育の実施

◆ 実機訓練を通じた実践的な障害対処能力の育成



本事例のポイント

- ✓ 国内外のサイバーインシデント被害事例を組織内に展開することにより、**組織全体を通じたサイバーセキュリティへの意識の浸透及び底上げ**を実現。
- ✓ 重要インフラサービスが停止する規模の災害を想定し、有事の際の**機能保証のための方策の検討及び効果確認の訓練**を実施。

本事例の利点

- ✓ 様々な役割や能力を持つ人材が組織横断的に連携し、**サイバーセキュリティの確保を可能とする体制の構築**に寄与。
- ✓ 机上訓練ではなく冗長系設備等による**実機訓練を通じた実践的な障害対処能力の育成**を実現。

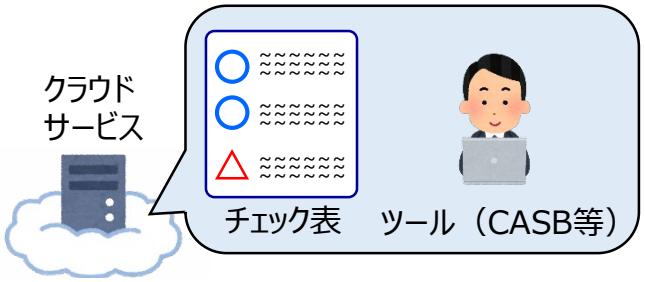
事例③　－　クラウドサービスの利用に係る対策について

事例の概要

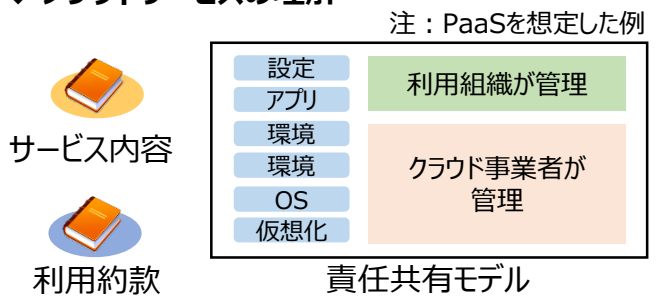
- **クラウドサービスの利用に関する内部規則を制定**し、サービス利用前にチェック表、CASB（※）等を利用することで、**設定不備や脆弱性等に係るセキュリティチェックを実施**している。
- 情報共有ツールを利用し、**クラウド事業者と密なコミュニケーション**が可能な体制を構築している。
- 定期的に、**サービス内容や仕様変更を確認**している。
- クラウド事業者に委託し設定変更等の作業を実施する際には、サービスを利用する関係者にも周知した上で、監視下のもと作業を実施している。

クラウドサービスの利用に関し、①利用申請手続き、②利用開始前のセキュリティチェック、③利用開始後の定期的な確認等の運用フローをまとめた内部規則を制定。

◆ 設定不備や脆弱性等に係る診断

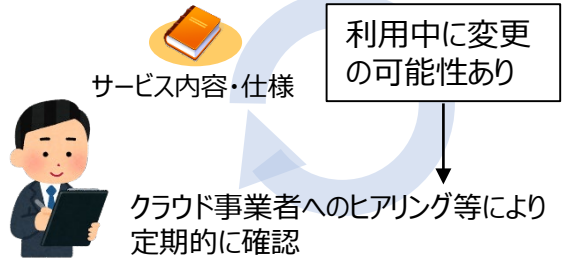


◆ クラウドサービスの理解



◆ クラウド事業者との連携体制の構築

◆ 定期的なサービス内容や仕様変更の確認



本事例のポイント

- ✓ クラウド利用のための**内部規則を制定**。
- ✓ サービス利用前に**チェック表、ツール等を利用しセキュリティチェック**を実施。
- ✓ 情報共有ツールを利用し、**クラウド事業者との連携体制を構築**、及び**クラウドサービスへの利用者理解を向上**。
- ✓ 定期的に**サービス内容や仕様変更について確認**。

本事例の利点

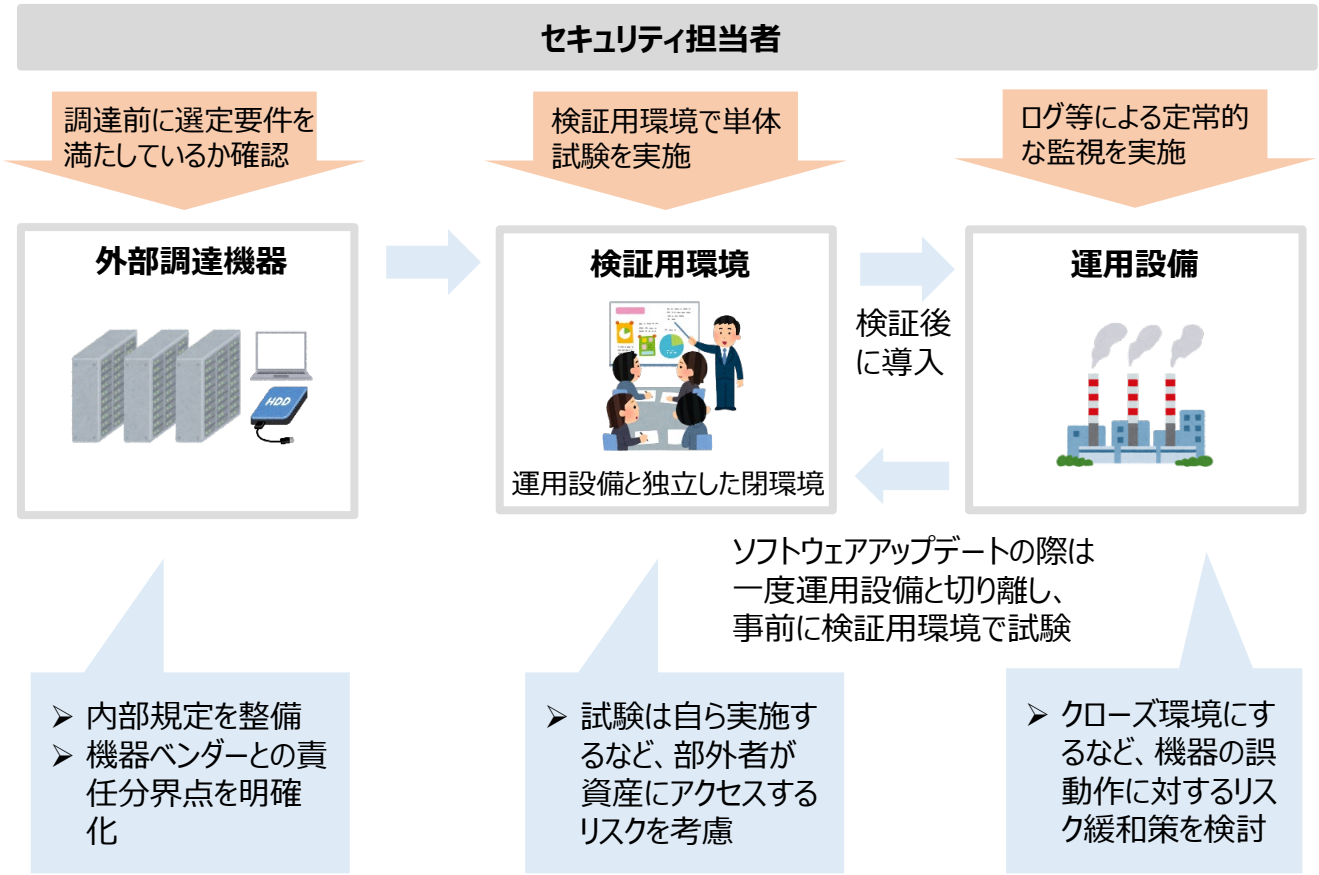
- ✓ クラウドサービスに係る設定不備、脆弱性、仕様変更等による**インシデントの発生を抑止**。
- ✓ クラウド事業者等のステークホルダーと密に連携し**インシデント発生時の被害を抑制**。

※　CASB（Cloud Access Security Broker）：クラウドサービスの利用状況を可視化・制御することで一括管理すること。

事例④　－　外部調達機器のセキュリティ対策について

事例の概要

- 機器を調達するにあたり、機器ベンダーの選定要件等を記載した**内部規定の整備及び機器供給者との責任分界点の明確化**を行っている。
- 調達機器を重要インフラ設備と接続するにあたっては、**接続前に単体試験を実施**している。また、ソフトウェアをバージョンアップする際には、検証用の環境を用意し、**運用設備とは切り離された環境でバージョンアップ試験**を行い、問題がないことを確認した後に適用する措置をとっている。
- ログ管理を行い、**追跡調査を行える体制を構築**している。



本事例のポイント

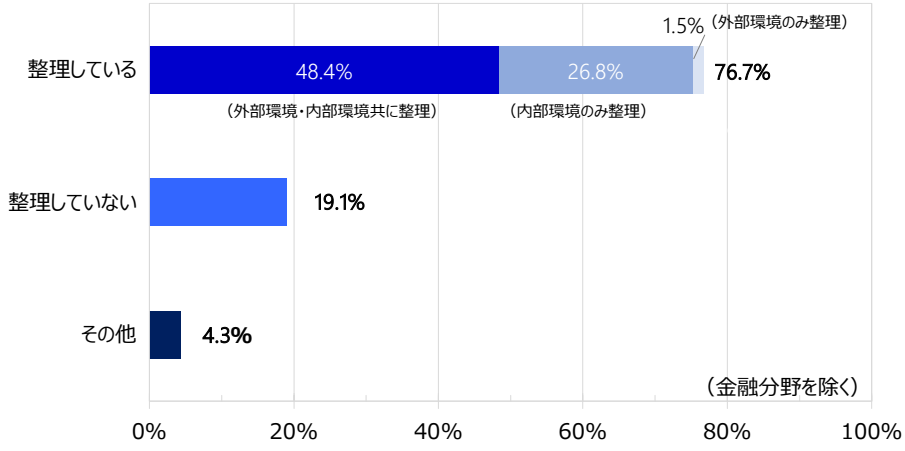
- ✓ **機器調達に関する内部規定の整備**及び**機器供給者との責任分界点の明確化**を実施。
- ✓ 重要インフラ設備に**接続する前に検証用環境で試験**を実施。
- ✓ 導入後、**運用設備とは切り離された環境でソフトウェアのバージョンアップ試験**を実施。

本事例の利点

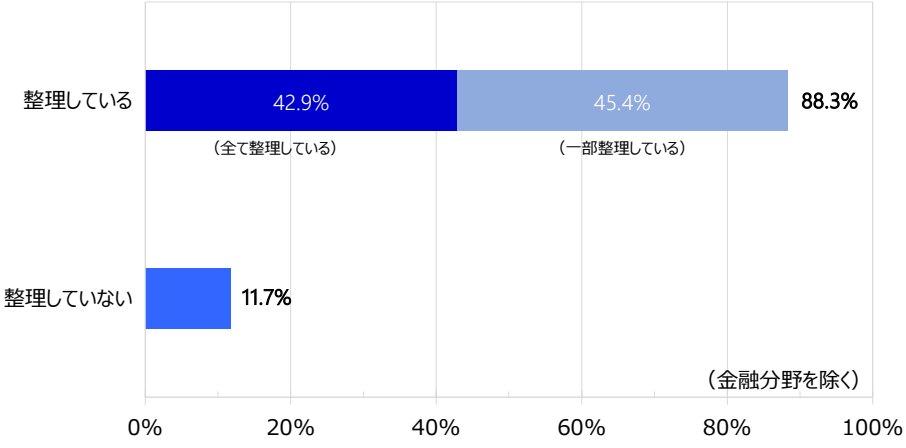
- ✓ 外部調達機器に対して**意図しない変更が加えられる等のリスク**に対し、**機器のライフサイクル全体にわたりリスク軽減**を実現。

目次

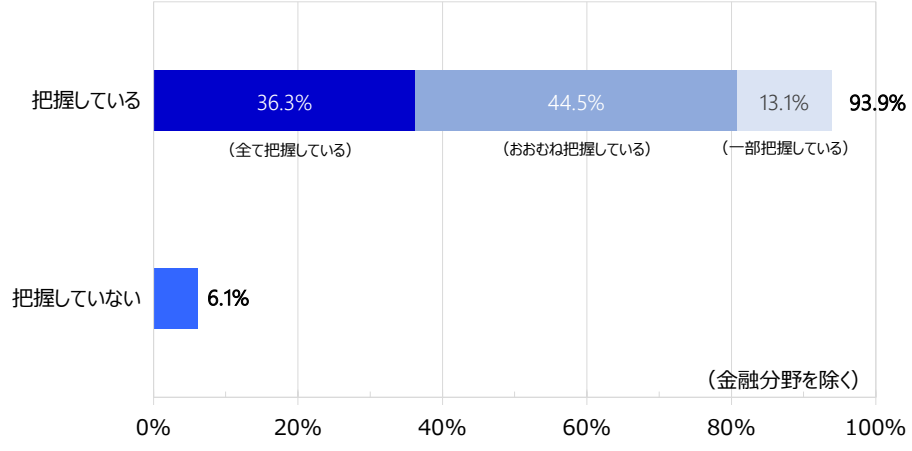
設問１－１．【単一回答】
自組織の重要インフラサービスの安定的かつ継続的な提供に影響を与えるおそれがある外部環境（政治・経済・社会等）や内部環境（組織体制・業務内容等）について、近い将来の状況を含めて整理していますか。



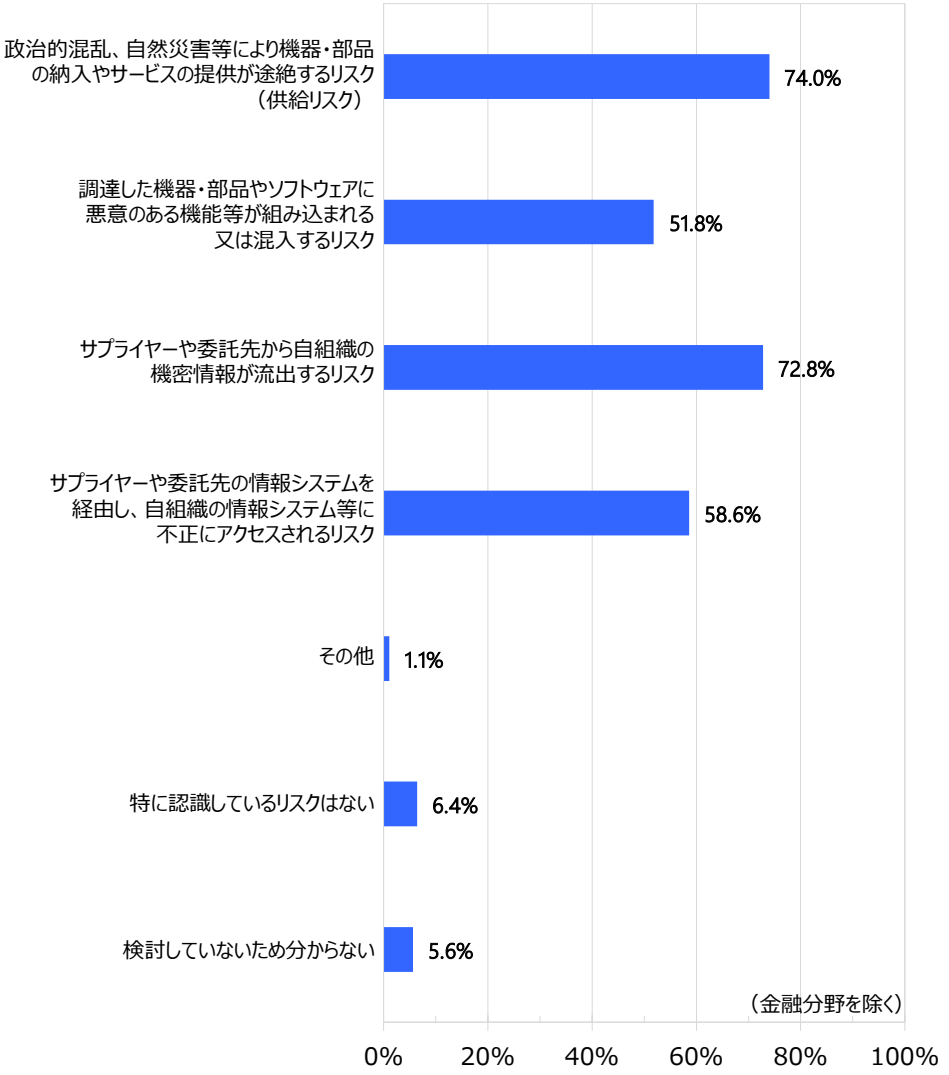
設問１－２．【単一回答】
関係省庁、顧客、サプライヤー、委託先等からの、情報セキュリティに関する自組織への要求事項（各事業分野の関係法令や契約等に規定された義務、サプライヤーや委託先が提示する制限事項等）を把握して整理していますか。



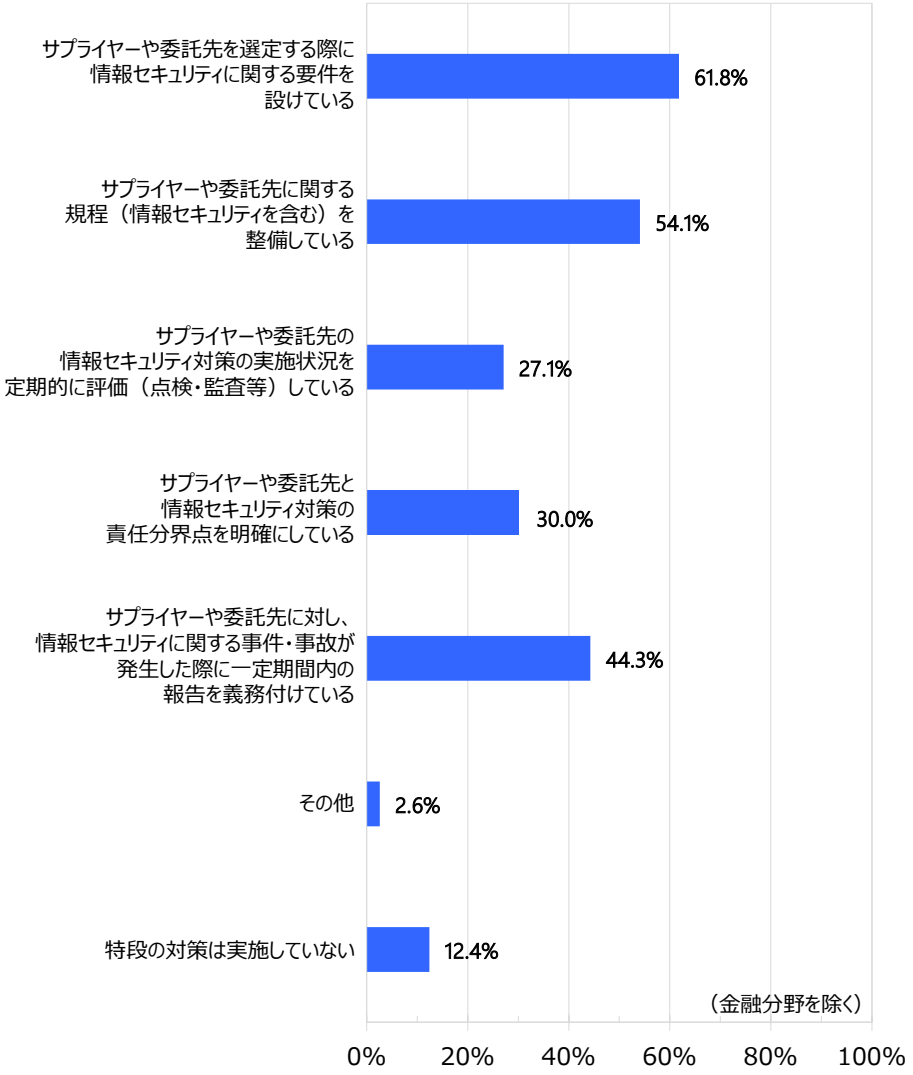
設問１－３．【単一回答】
自組織のサプライチェーン（サプライヤー、委託先等）を把握していますか。



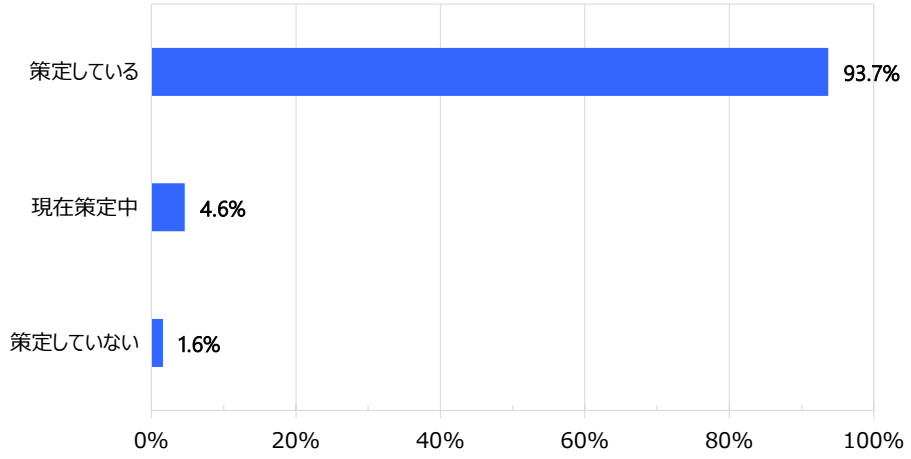
設問１－４．【複数回答】
サプライチェーンについて、自組織で認識しているリスクを全て選択してください。



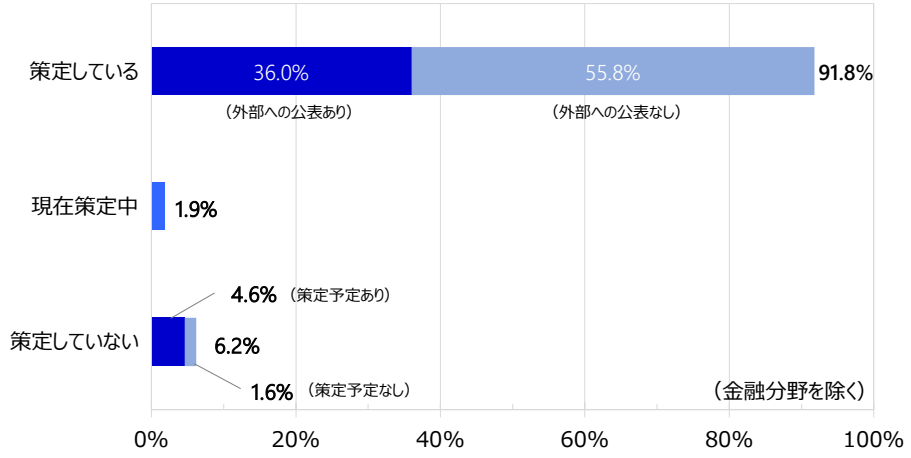
設問１－５．【複数回答】
自組織のサプライチェーンに関するリスクについて、実施している対策を全て選択してください。



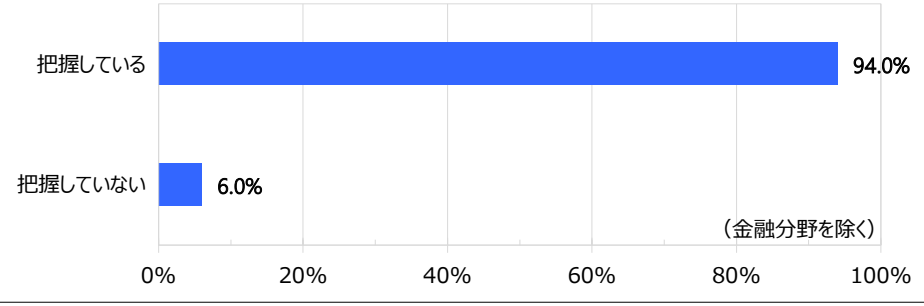
設問２－１．【単一回答】
自組織が情報セキュリティ対策に取り組む目的、方向性等を示した情報セキュリティ対策に関する基本方針を策定・公表していますか。
（上段：対象の全分野　下段：金融分野を除いた内訳）



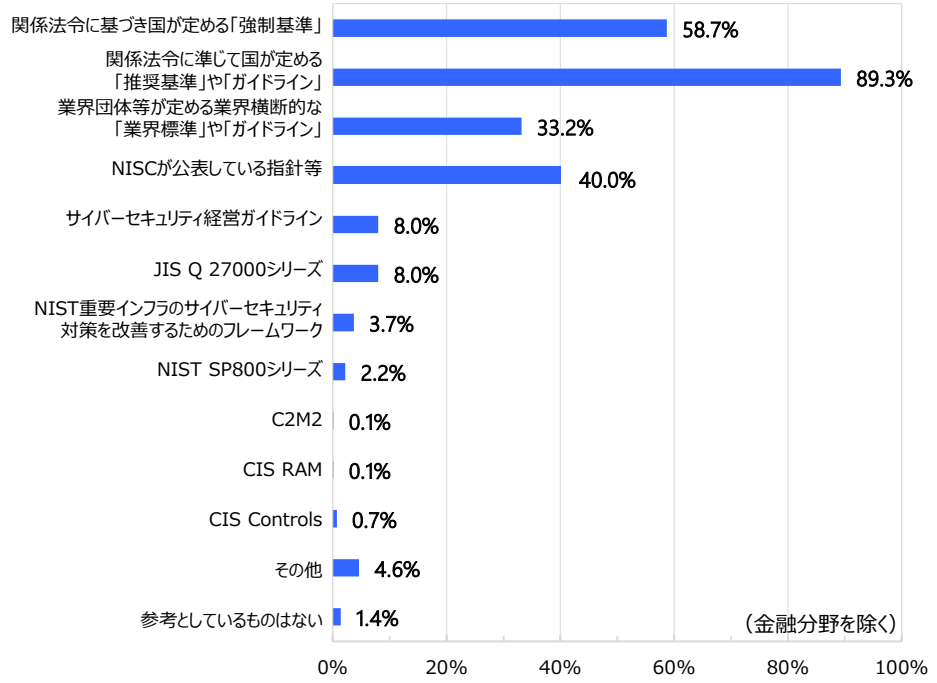
（内訳）



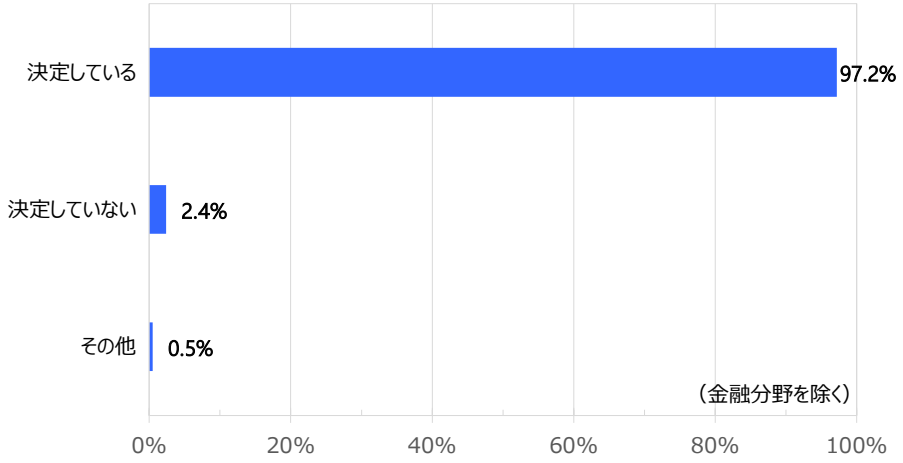
設問２－２．【単一回答】
自組織に関係する安全基準等を把握していますか。



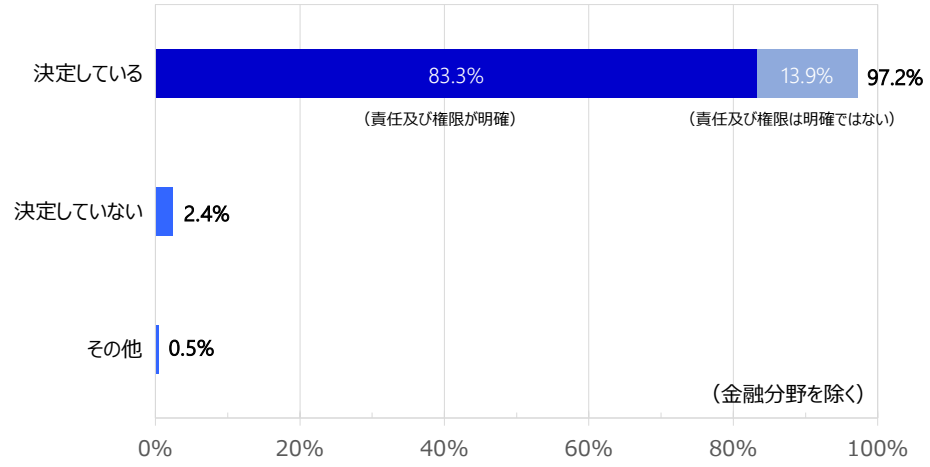
設問２－３．【複数回答】
情報セキュリティに関する方針の策定に当たって参考としているものを全て選択してください。



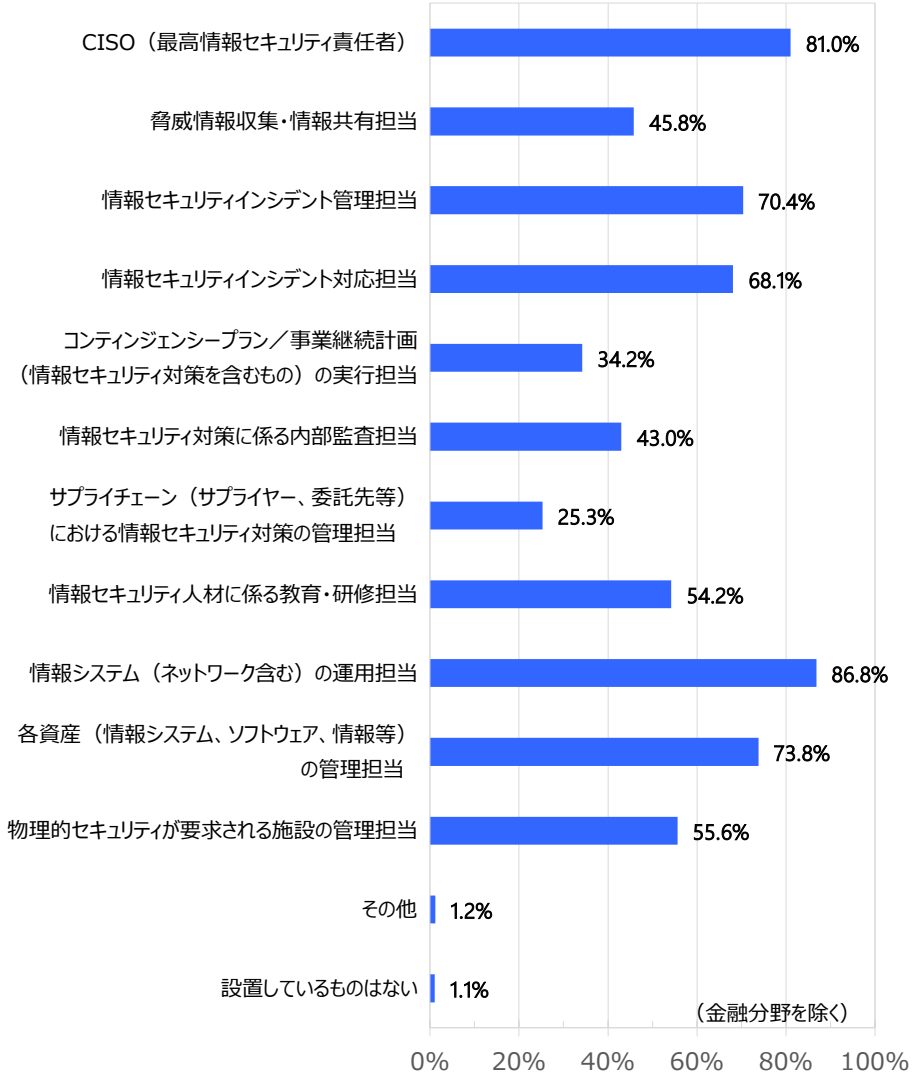
設問２－４．【単一回答】
自組織の情報セキュリティ対策を担当する部署及び従業員を決定するとともに、それらの責任及び権限が明確になっていますか。



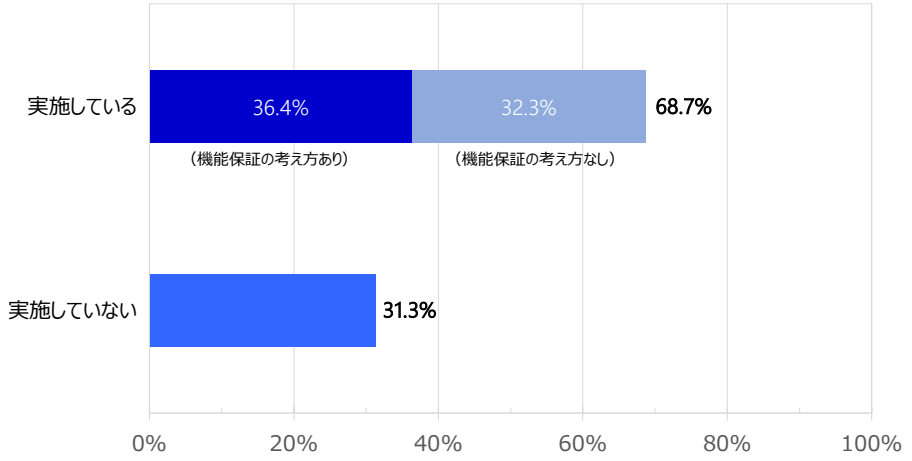
（内訳）

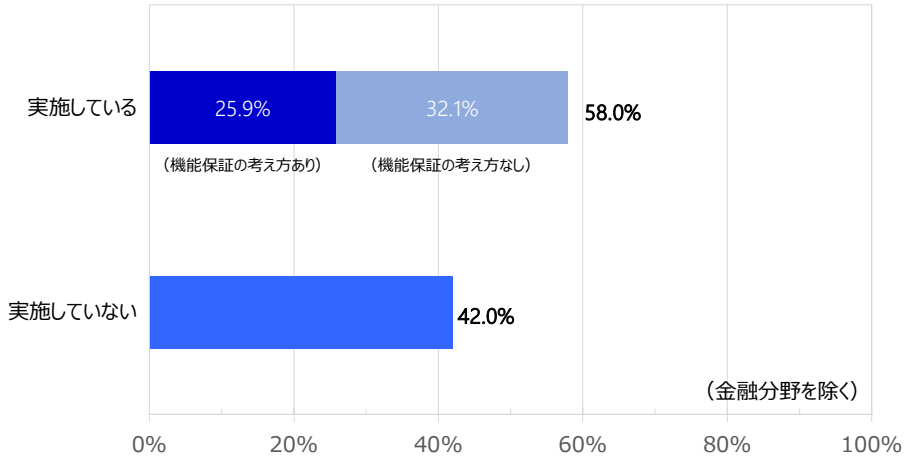


設問２－５．【複数回答】
自組織で設置しているものを全て選択ください。

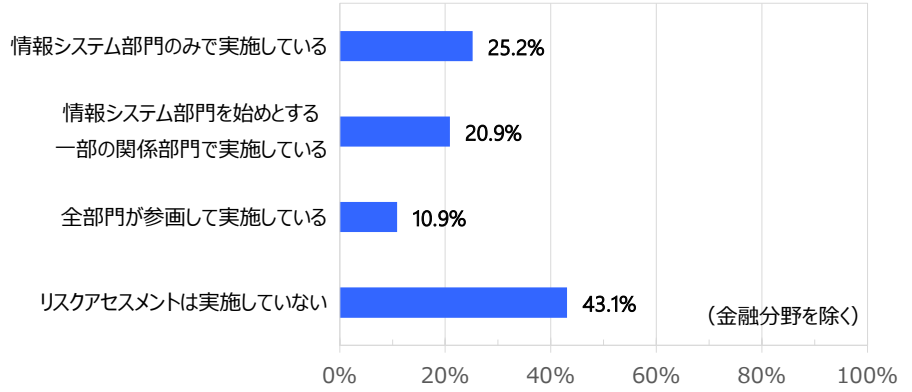


設問３－１．【単一回答】
情報セキュリティ対策の実施に当たって、自組織でリスクアセスメント（リスクの特定・分析・評価）を実施していますか。また、機能保証の考え方を取り入れていますか。
（上段：対象の全分野　下段：金融分野を除いた場合）

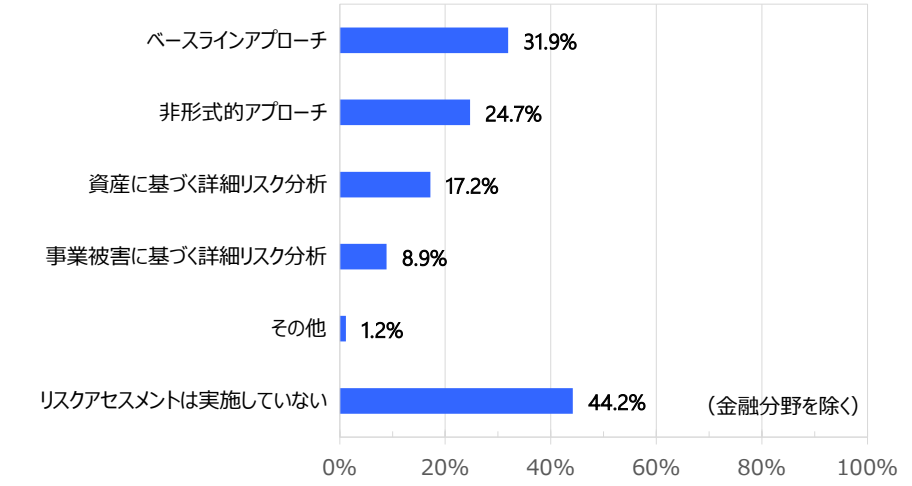




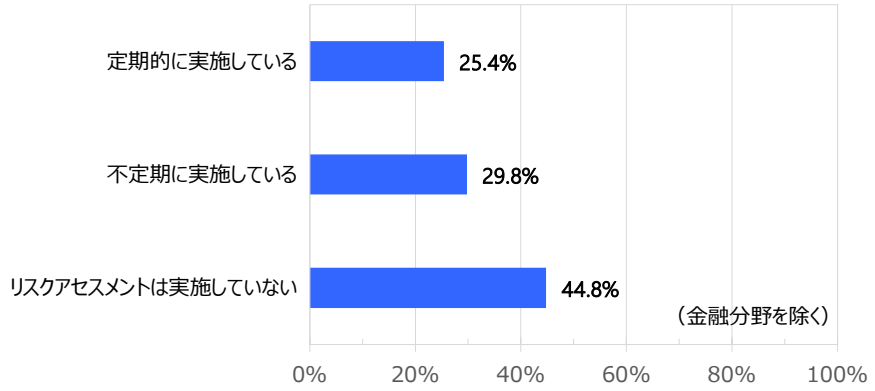
設問３－２．【単一回答】
情報セキュリティに関するリスクアセスメントの実施主体を選択してください。
（設問３－１で選択肢３を選択した場合は、選択肢４を選択してください。）



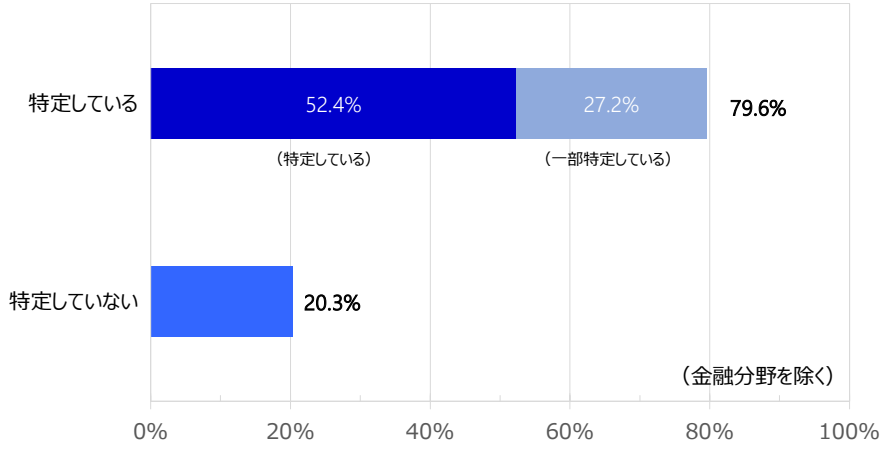
設問３－３．【複数回答】
自組織で実施しているリスクアセスメントの方法を全て選択してください。
（設問３－１で選択肢３を選択した場合は、選択肢６を選択してください。）



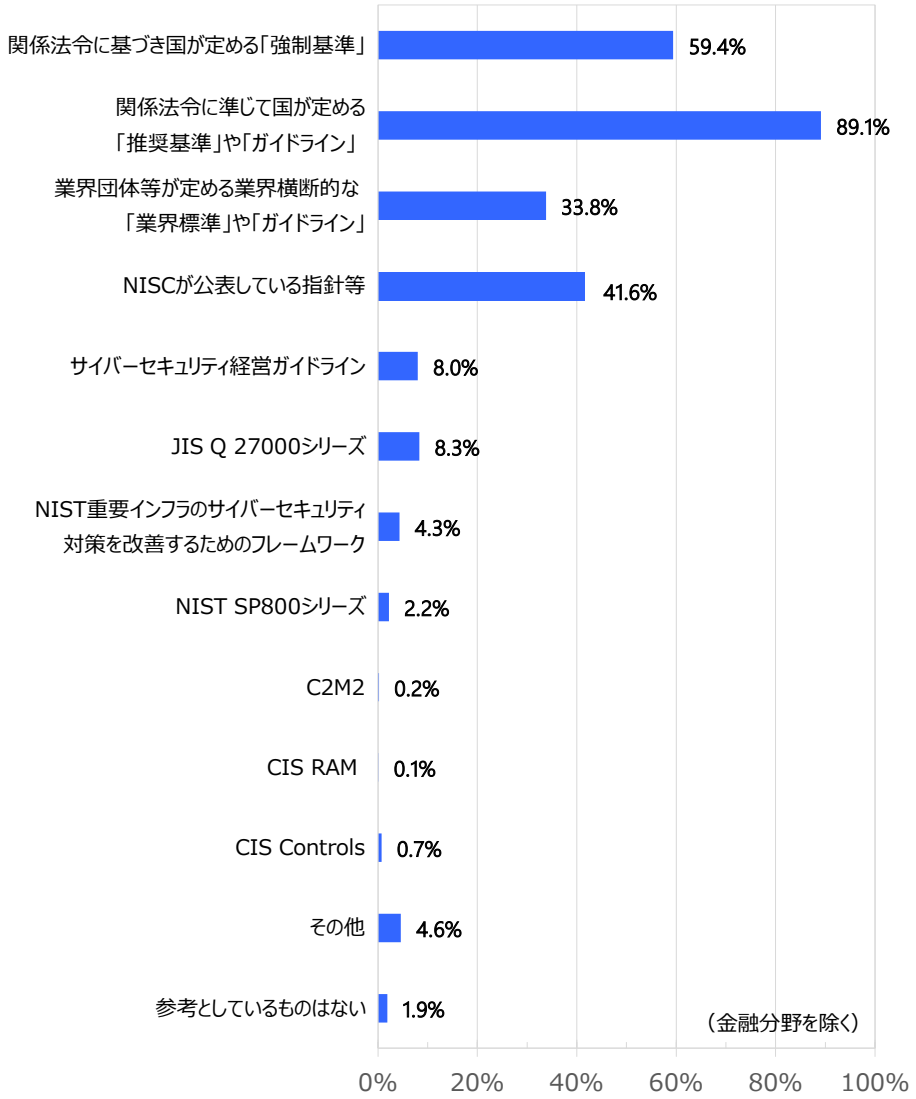
設問３－４．【単一回答】
情報セキュリティに関するリスクアセスメントを定期的に実施していますか。
（設問３－１で選択肢３を選択した場合は、選択肢３を選択してください。）



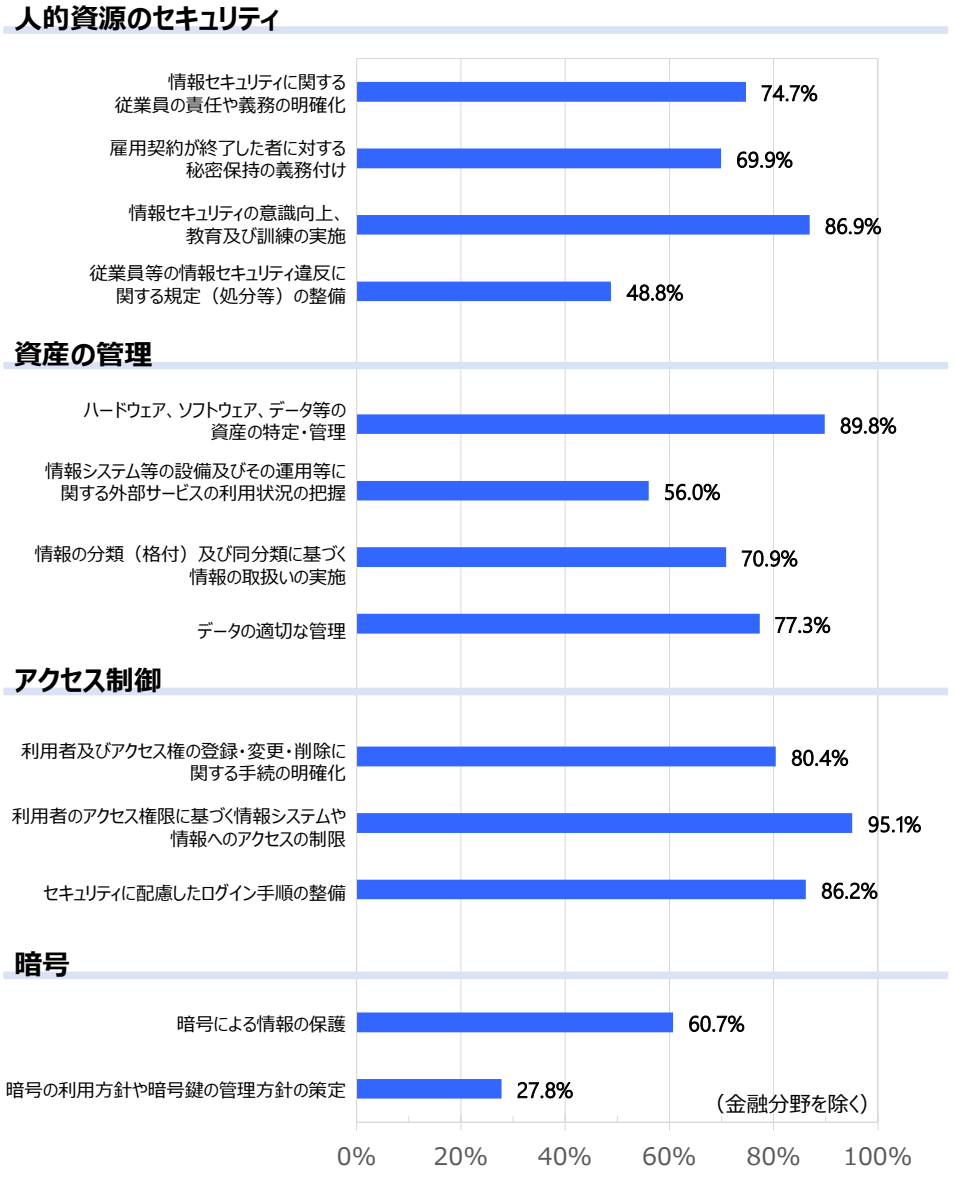
設問３－５．【単一回答】
自組織が重要インフラサービスを提供するために必要な情報システム（＝重要システム）を、重要インフラサービスに与える影響の度合いを踏まえて特定していますか。

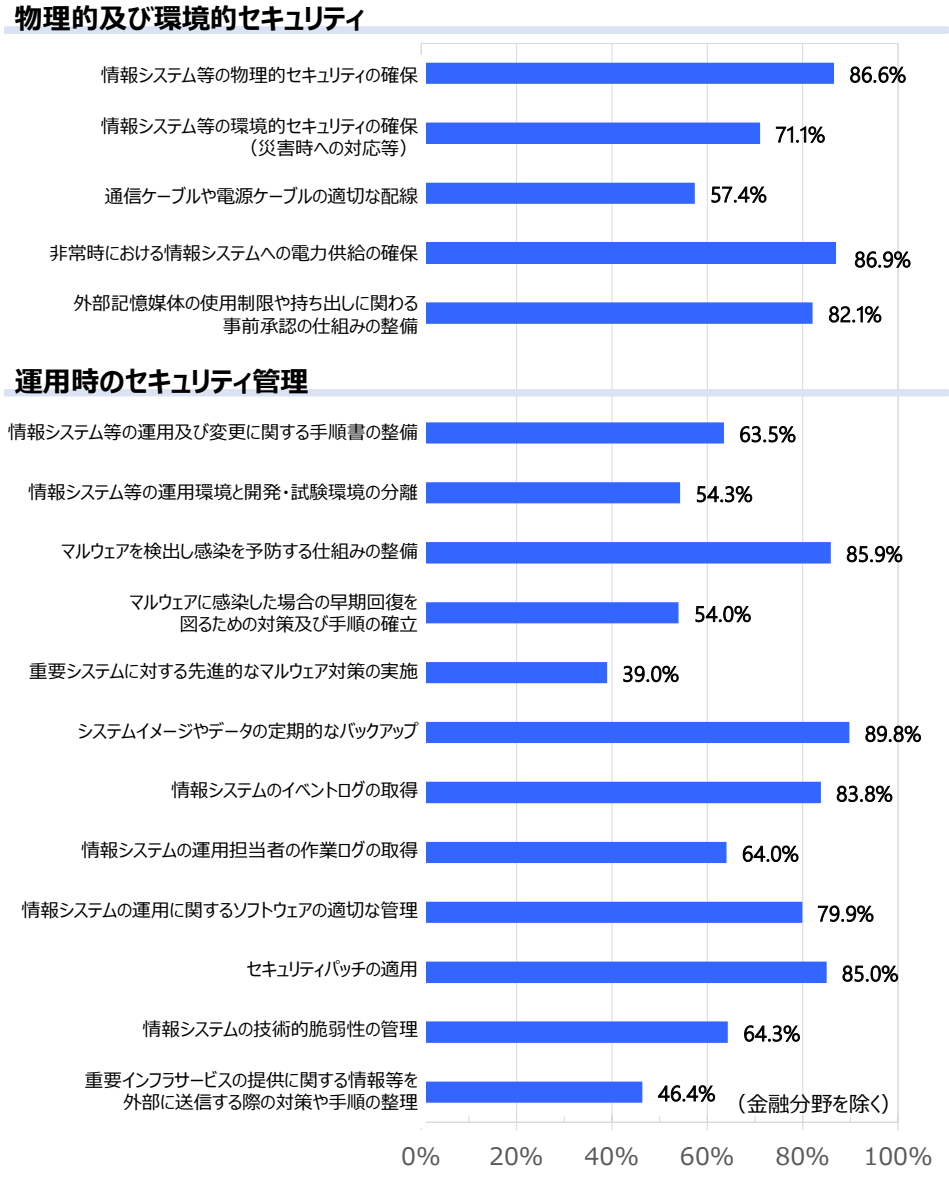


設問３－６．【複数回答】
情報セキュリティ対策の実施に当たって、参考としているものを全て選択してください。

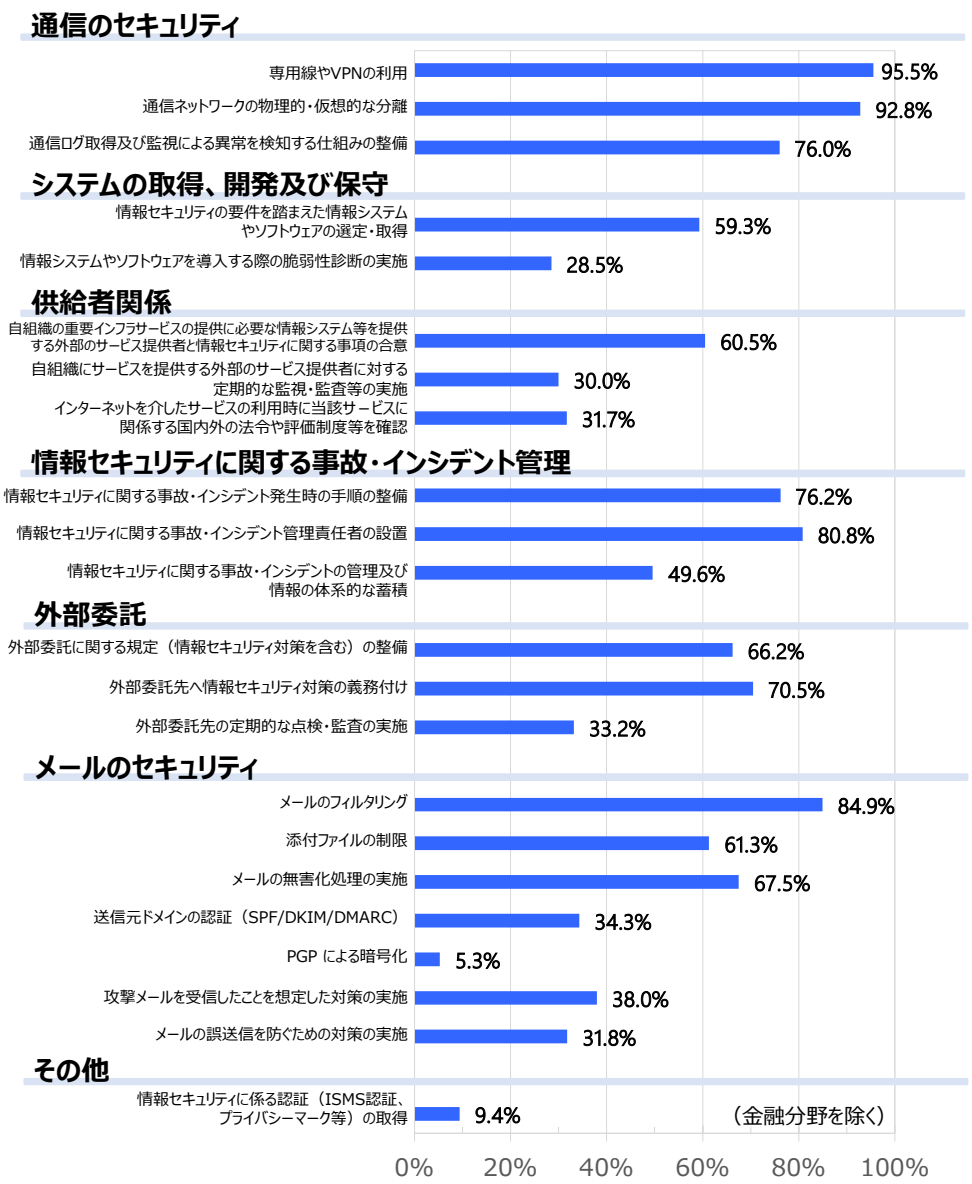


設問３－７．【複数回答】
自組織で実施している情報セキュリティ対策を全て選択してください。

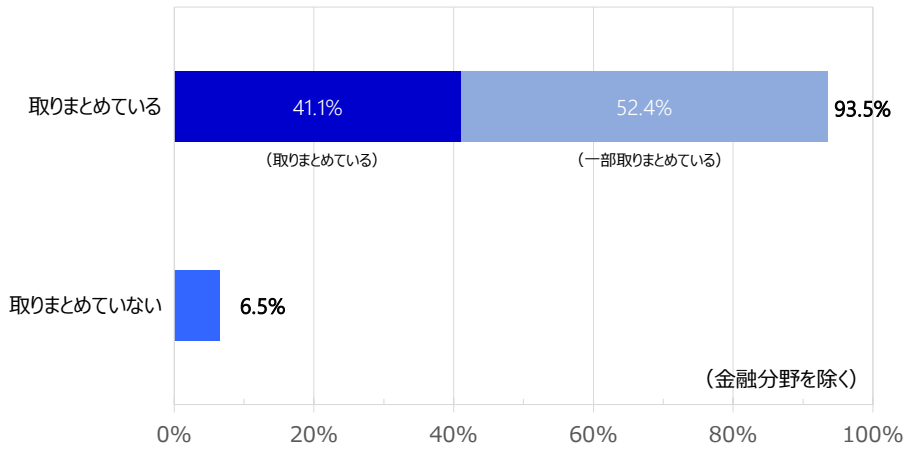




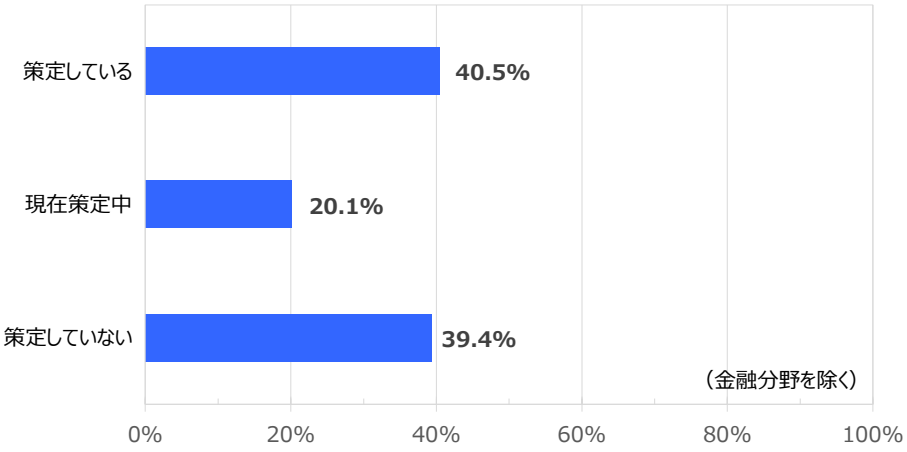
設問３－７．【複数回答】
自組織で実施している情報セキュリティ対策を全て選択してください。（続き）



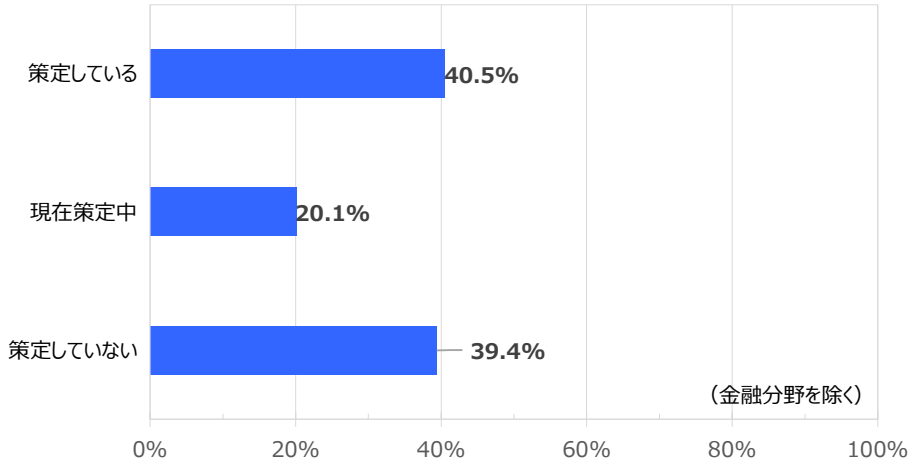
設問３－８．【単一回答】
設問３－７で実施しているとした情報セキュリティ対策を内規（実施手順・マニュアル等）として取りまとめていますか。



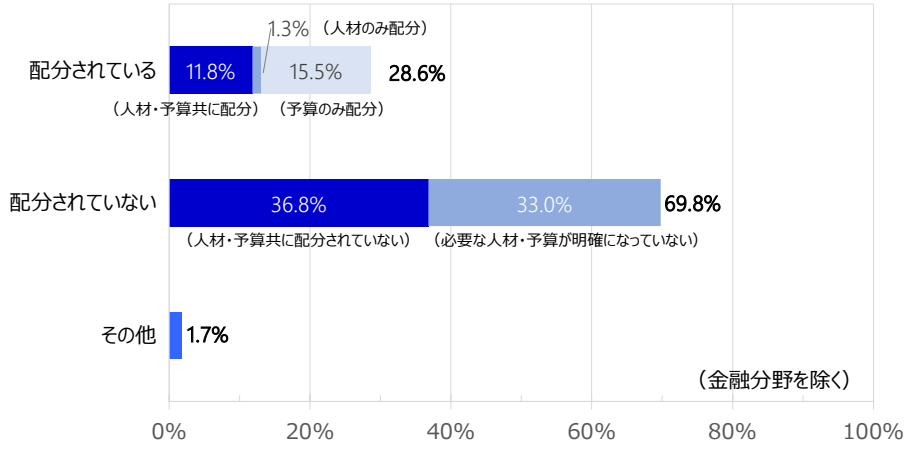
設問３－９．【単一回答】
情報セキュリティ対策の導入や実施に向けた計画（目標・達成度・スケジュール等）を策定していますか。



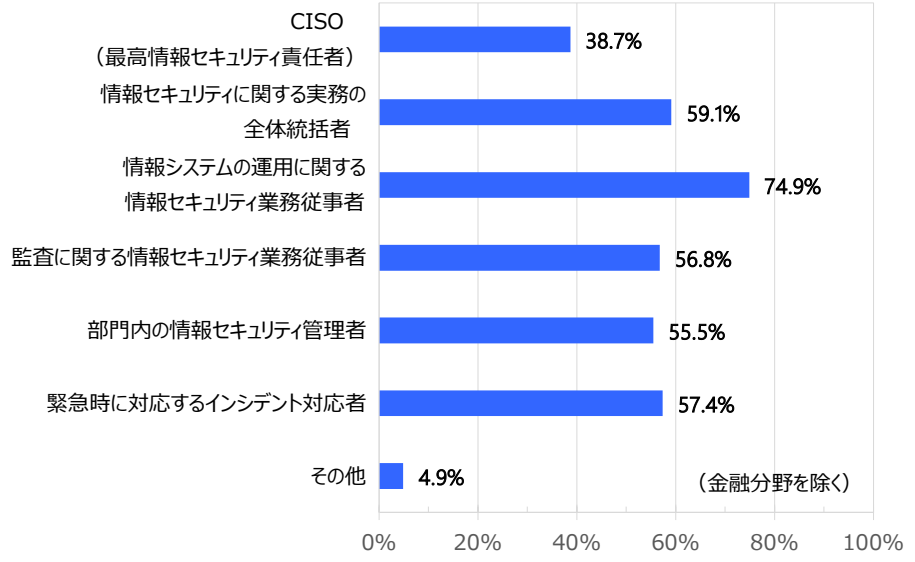
設問３－10．【単一回答】
情報セキュリティに関する事件・事故（サービス停止、情報漏えい、改ざん等）が発生した場合の情報開示の基準を策定していますか。



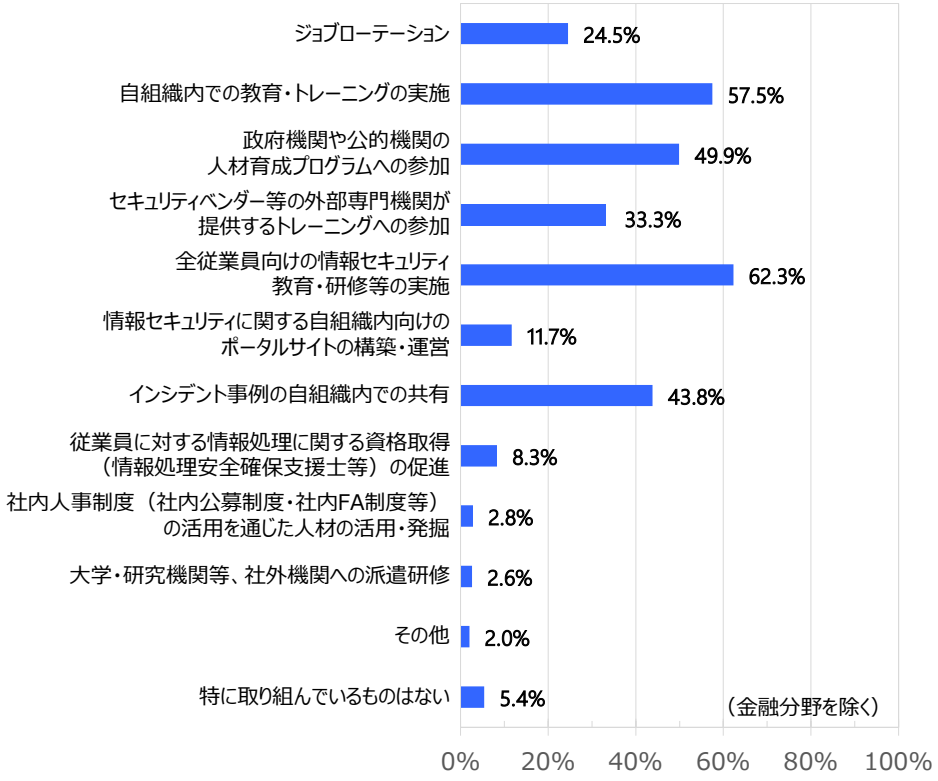
設問４－１．【単一回答】
情報セキュリティ対策の実施に必要となる人材や予算が明確化され、組織内に適切に配分されていますか。



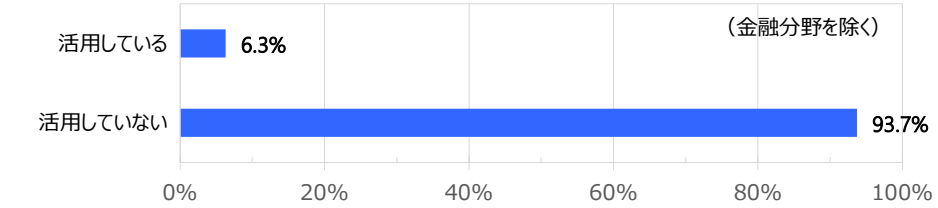
設問４－２．【複数回答】
自組織において、必要としている情報セキュリティ人材を全て選択してください。



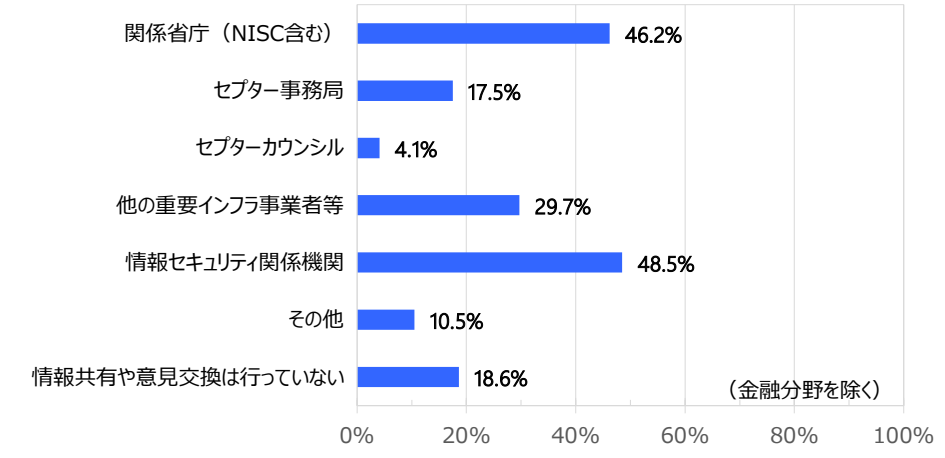
設問４－３．【複数回答】
情報セキュリティ人材の育成や従業員の情報セキュリティに関する意識啓発について、自組織で取り組んでいるものを全て選択してください。



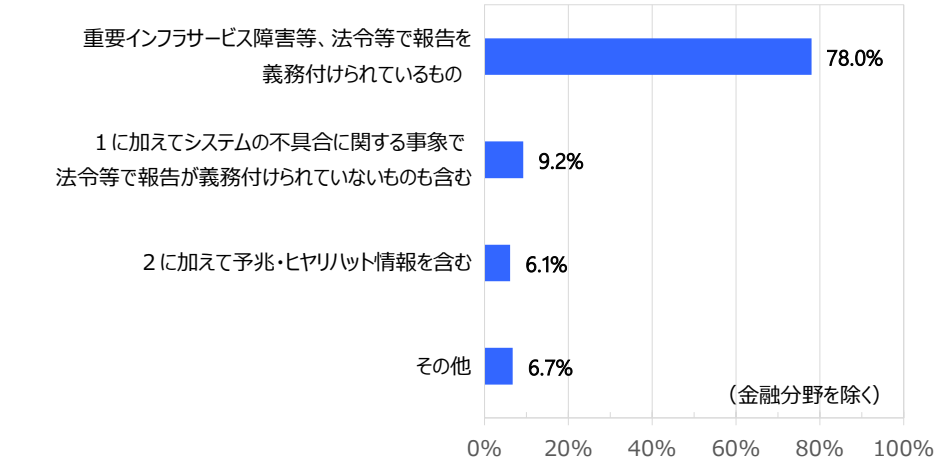
設問４－４．【単一回答】
自組織において、情報処理安全確保支援士資格取得者を活用していますか。



設問４－５．【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。

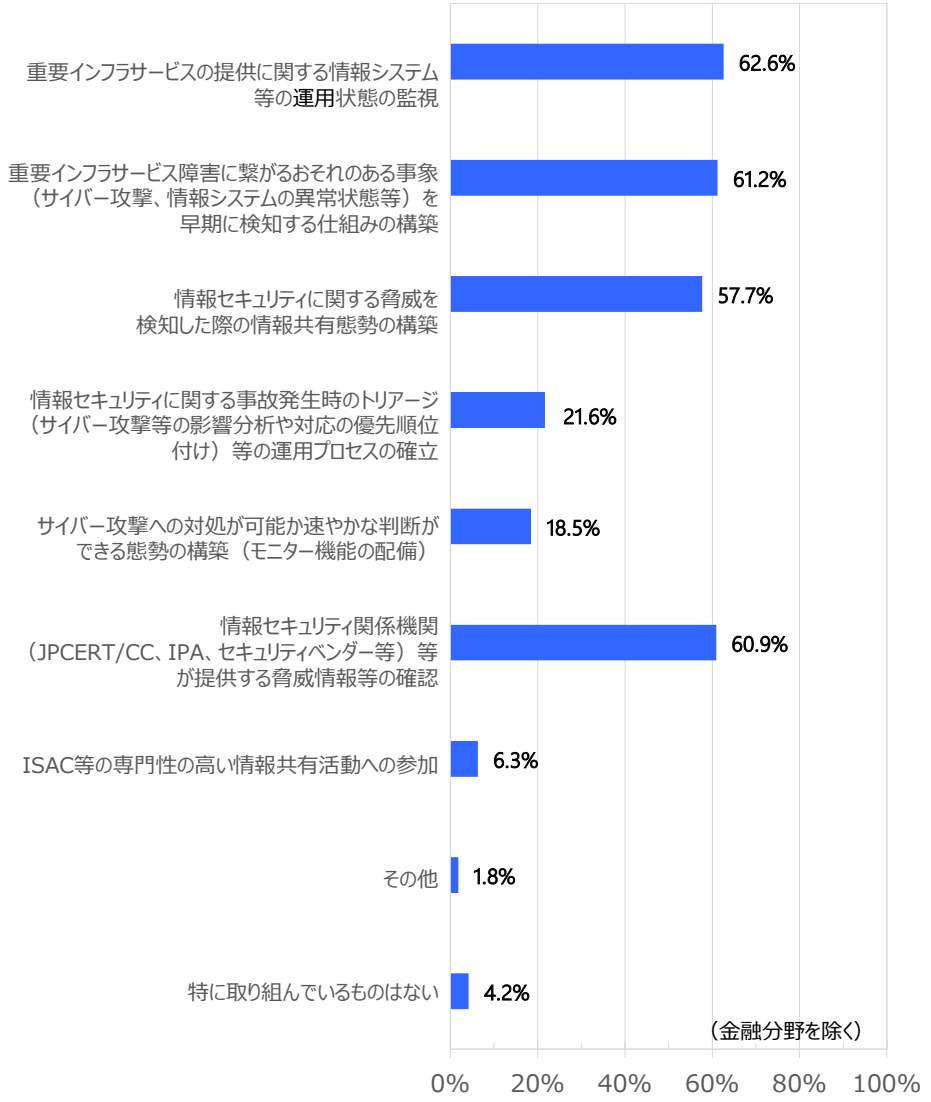


設問４－６．【単一回答】
自組織の情報システムの不具合について、重要インフラ所管省庁等との情報共有の対象範囲を選択してください。

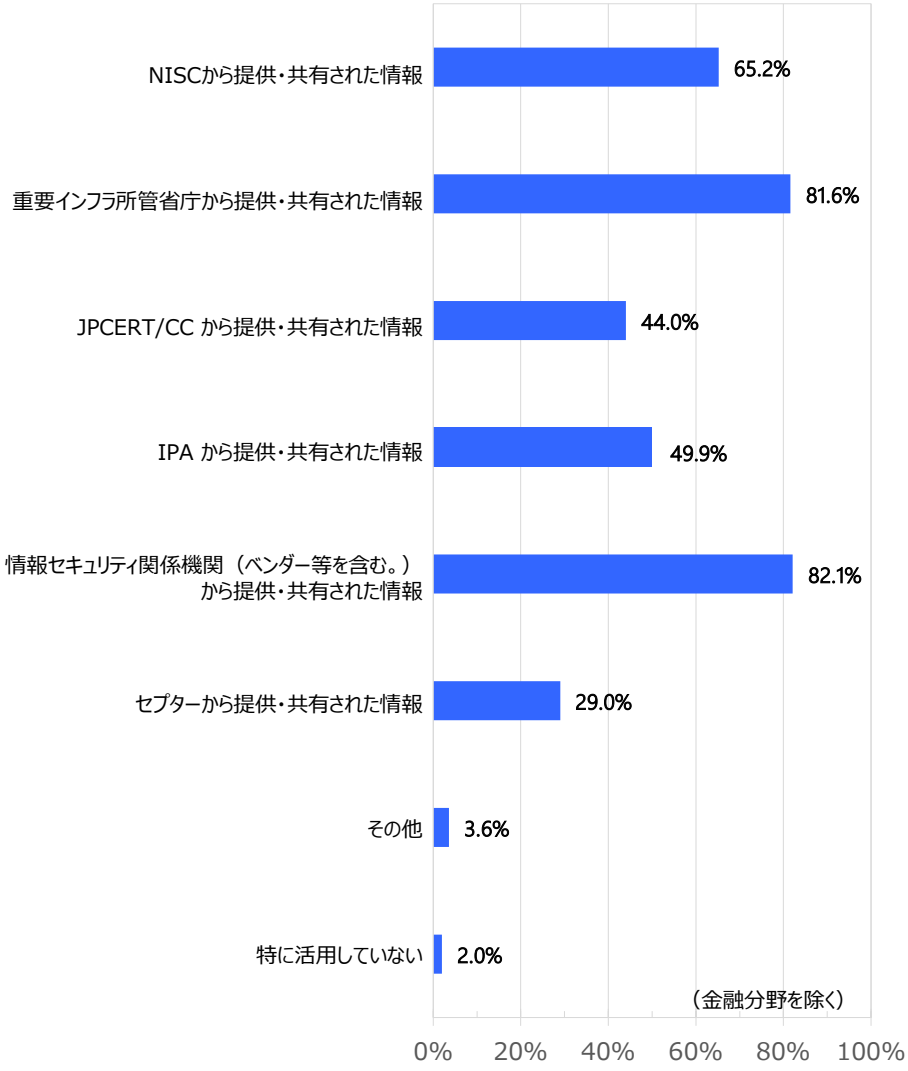


アンケート調査結果 － Do［実行］（1/3）

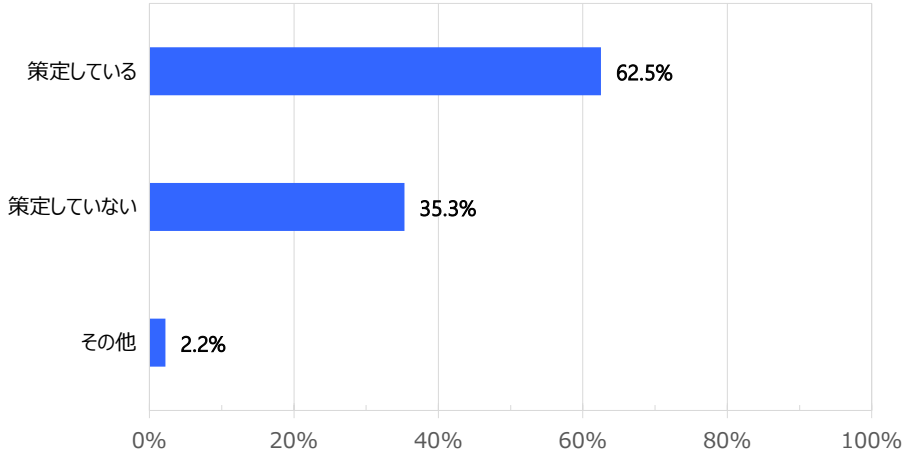
設問５－１．【複数回答】
情報システムの導入・運用時の情報セキュリティ対策を全て選択してください。



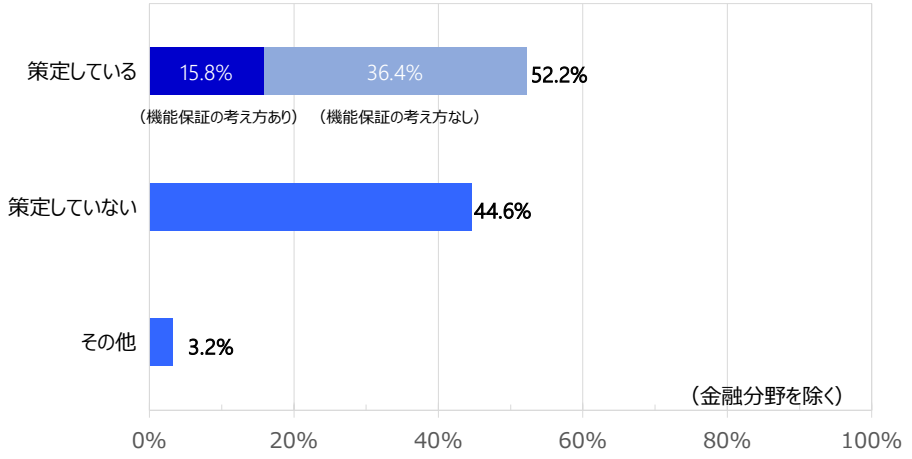
設問５－２．【複数回答】
外部機関から共有・提供された情報について、自組織で活用しているものを全て選択してください。



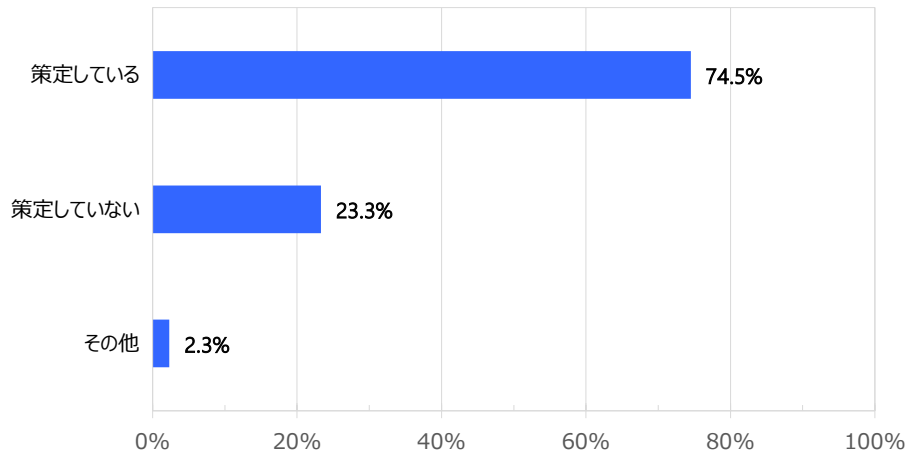
設問５－３．【単一回答】
重要インフラサービス障害の発生に備えたコンティンジェンシープランを策定していますか。また、機能保証の考え方を取り入れていますか。
（上段：対象の全分野　下段：金融分野を除いた内訳）



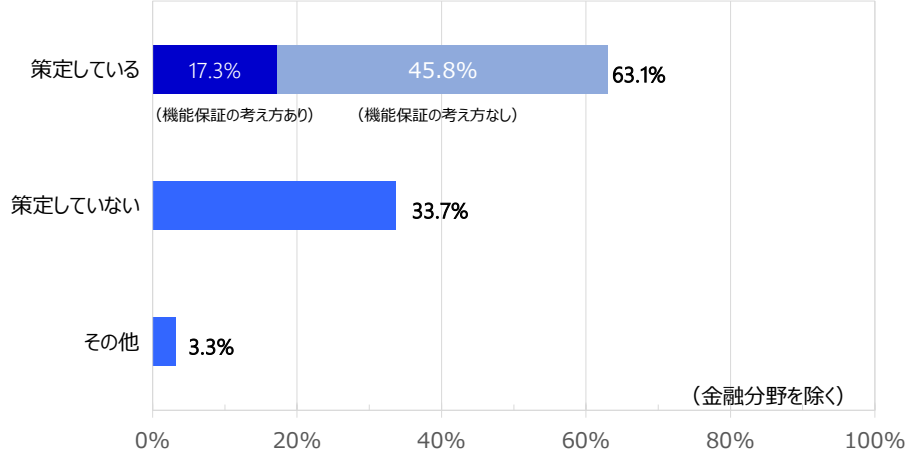
（内訳）



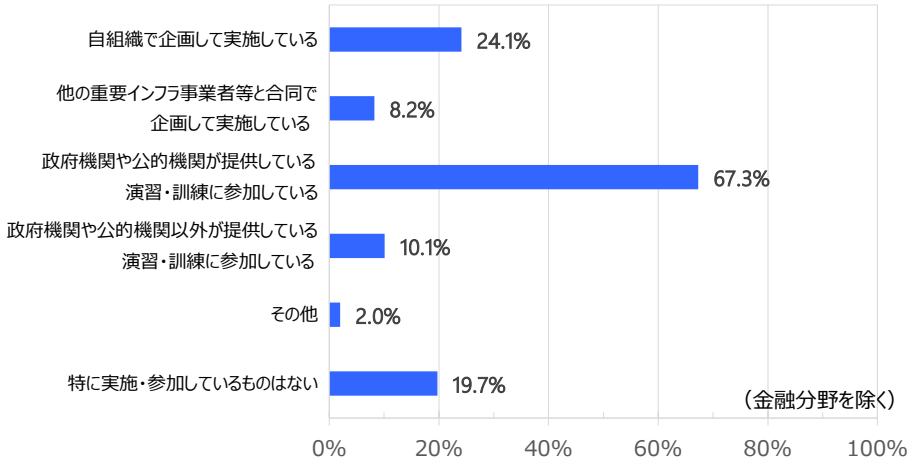
設問５－４．【単一回答】
重要インフラサービス障害の発生に備えた事業継続計画を策定していますか。また、機能保証の考え方を取り入れていますか。
（上段：対象の全分野　下段：金融分野を除いた内訳）



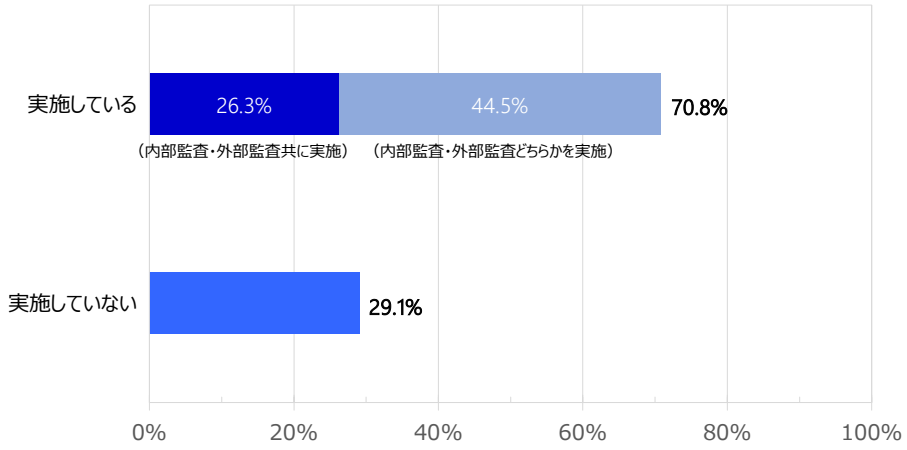
（内訳）

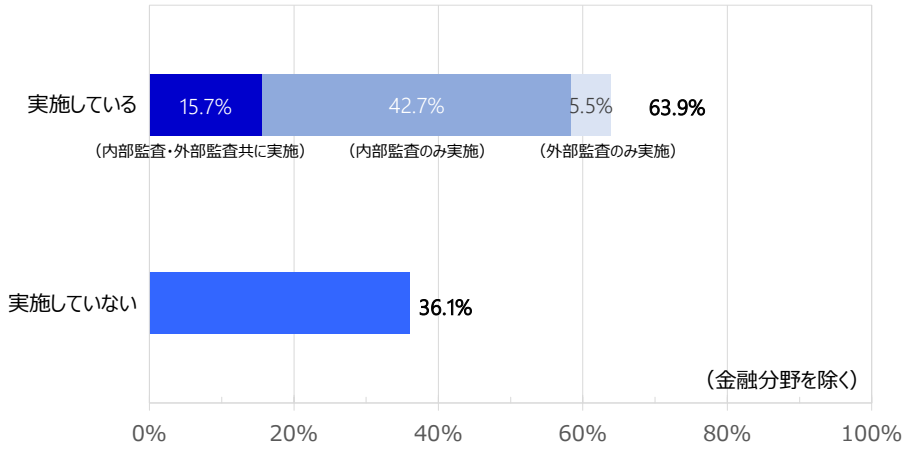


設問５－５．【複数回答】
情報セキュリティ対策に関する演習・訓練について、自組織で実施・参加しているものを全て選択してください。

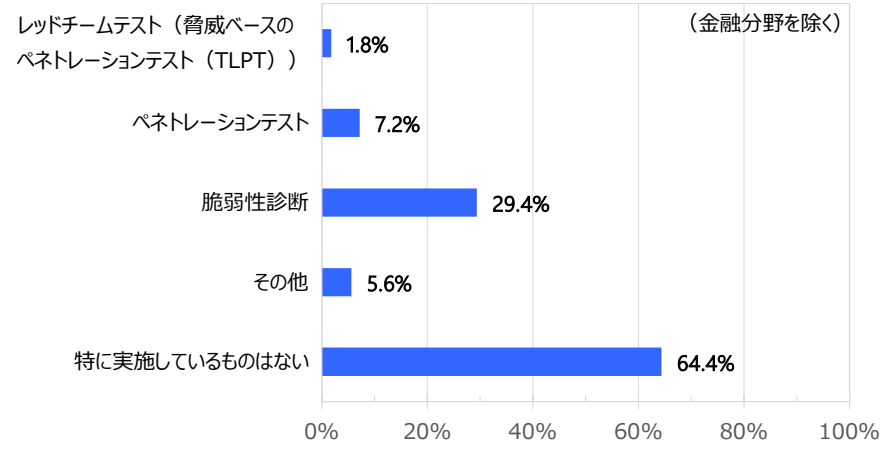


設問６－１．【単一回答】
自組織の情報セキュリティ対策に関する目標の達成状況、計画の進捗状況等について、監査を実施していますか。（上段：対象の全分野　下段：金融分野を除いた場合）

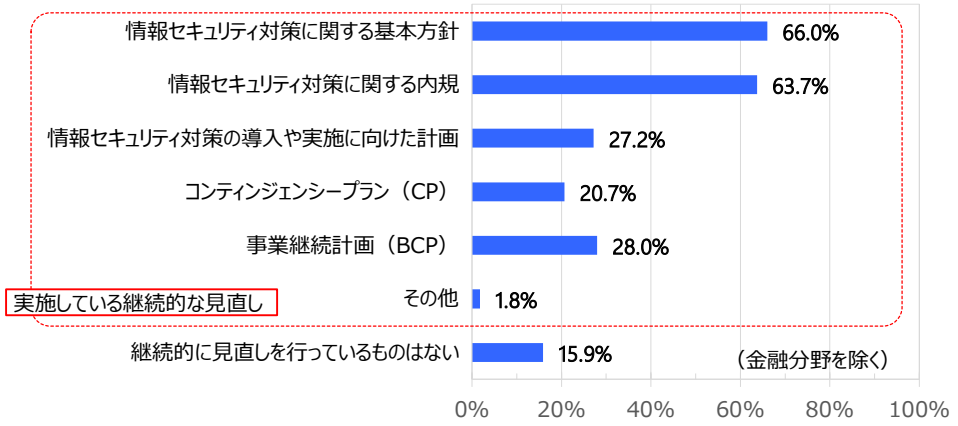




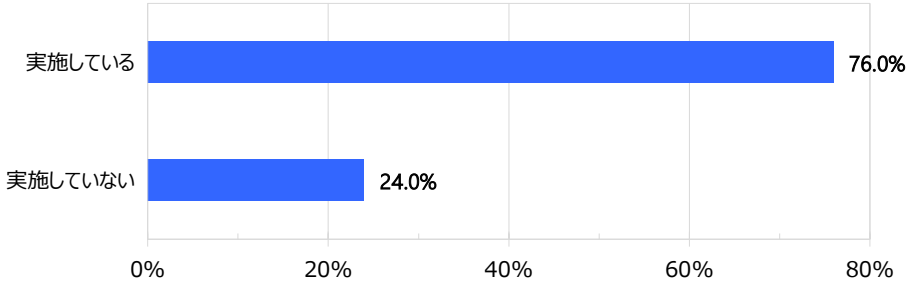
設問６－２．【複数回答】
自組織にて実施しているセキュリティ評価を全て選択してください。
（設問６－１で選択肢４を選択した場合は、選択肢５を選択してください。）



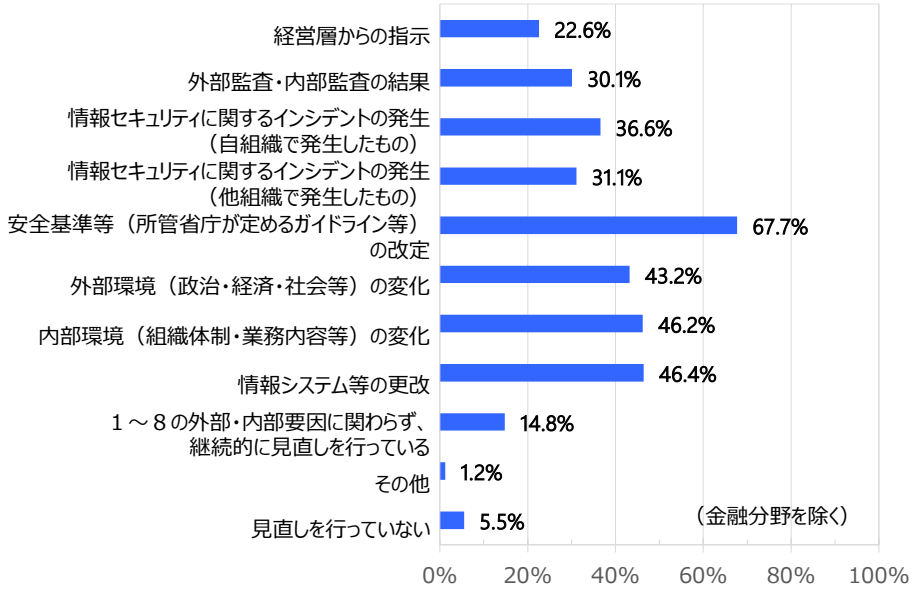
設問７－１．【複数回答】
情報セキュリティ対策の改善に向け、継続的に見直しを行っているものを全て選択してください。



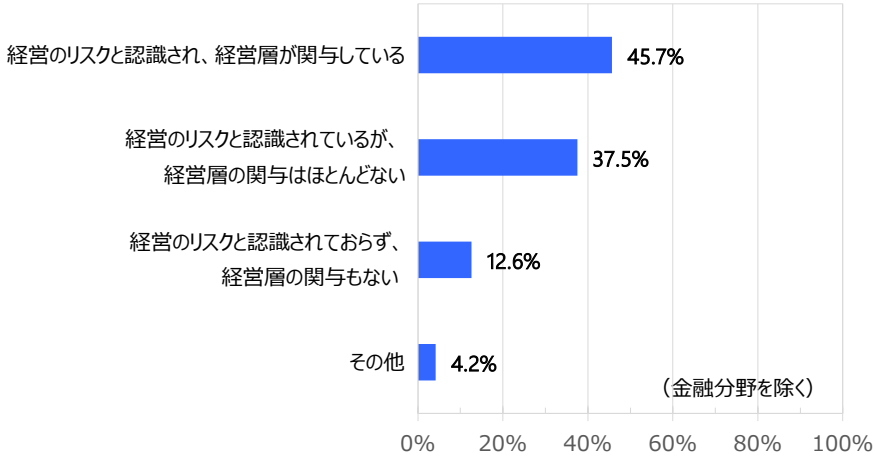
※継続的な見直し（金融分野を含む）



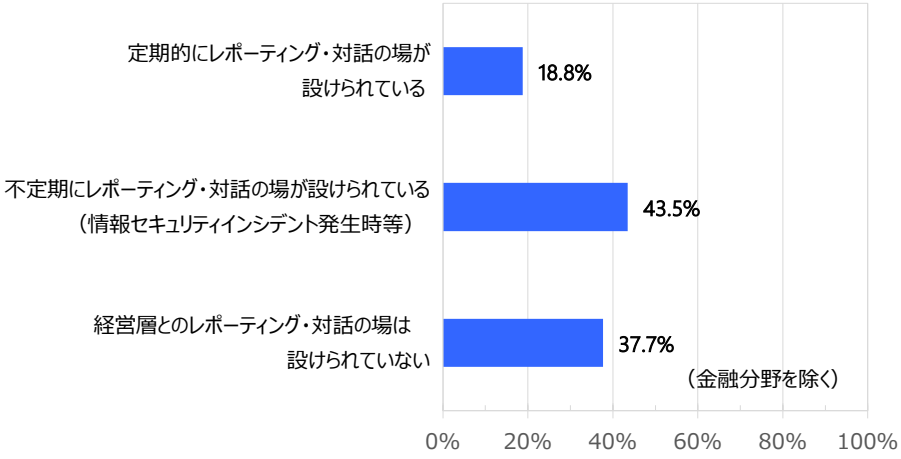
設問７－２．【複数回答】
情報セキュリティ対策の見直しの契機となったものを全て選択してください。



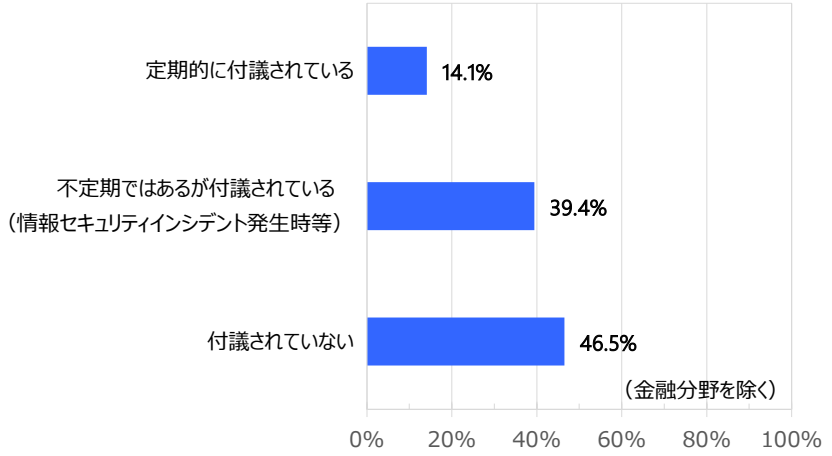
設問８－１．【単一回答】
情報セキュリティリスクが経営のリスクと認識され、その対応方針の策定に経営層が関与していますか。



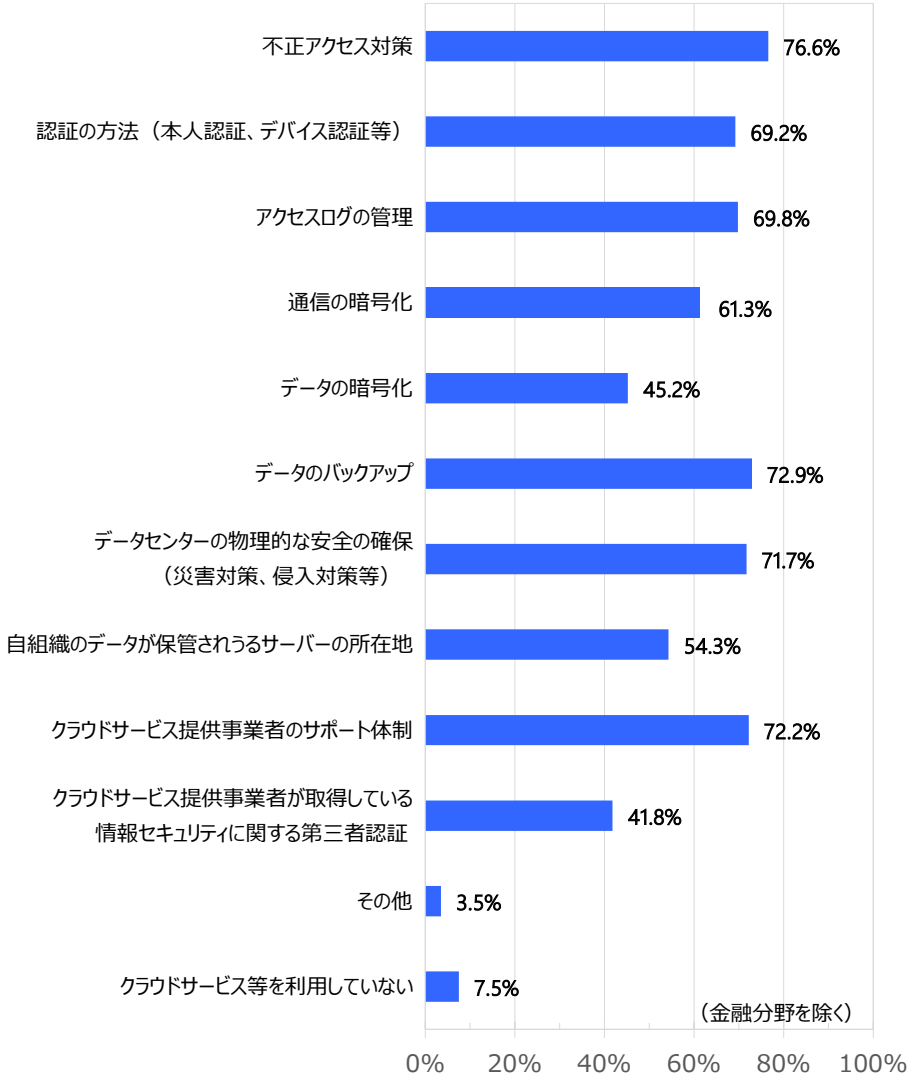
設問８－２．【単一回答】
情報セキュリティリスクの対処に当たり、経営層とのレポーティング・対話の場が設けられていますか。



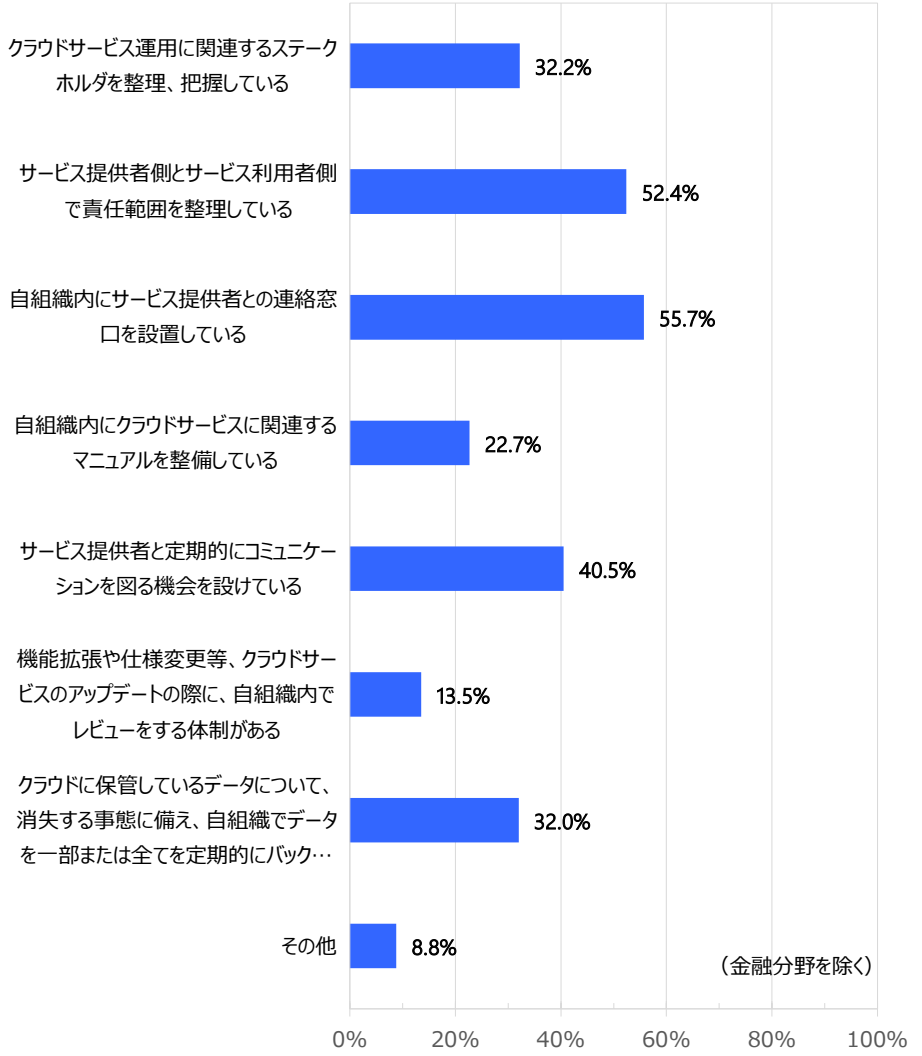
設問８－３．【単一回答】
情報セキュリティリスクが経営会議（経営層が一同に参加する会議）等に付議されていますか。



設問９－１．【複数回答】
自組織がクラウドサービスを利用する際に、確認しているクラウドサービス提供事業者側の情報セキュリティ対策等を全て選択してください。

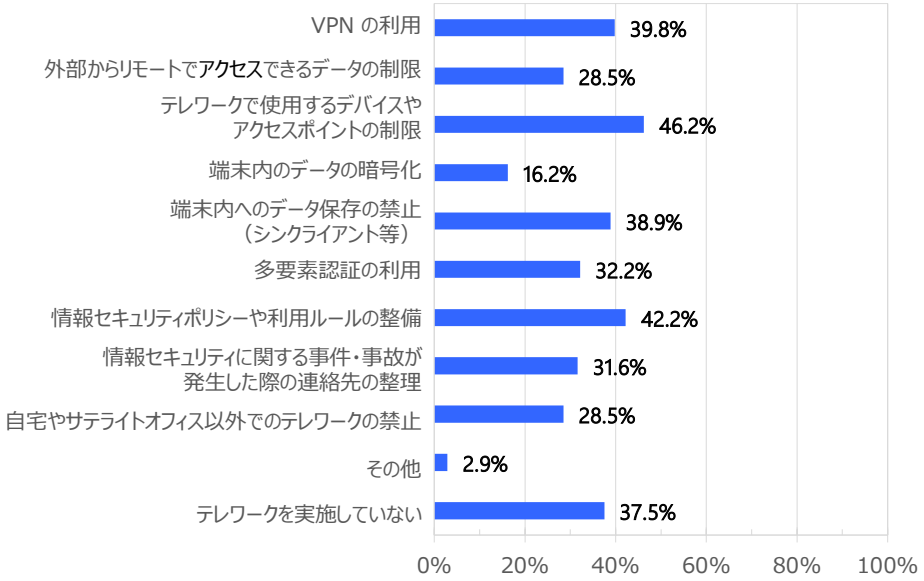


設問９－２．【複数回答】
行っている運用対策や情報セキュリティ対策。

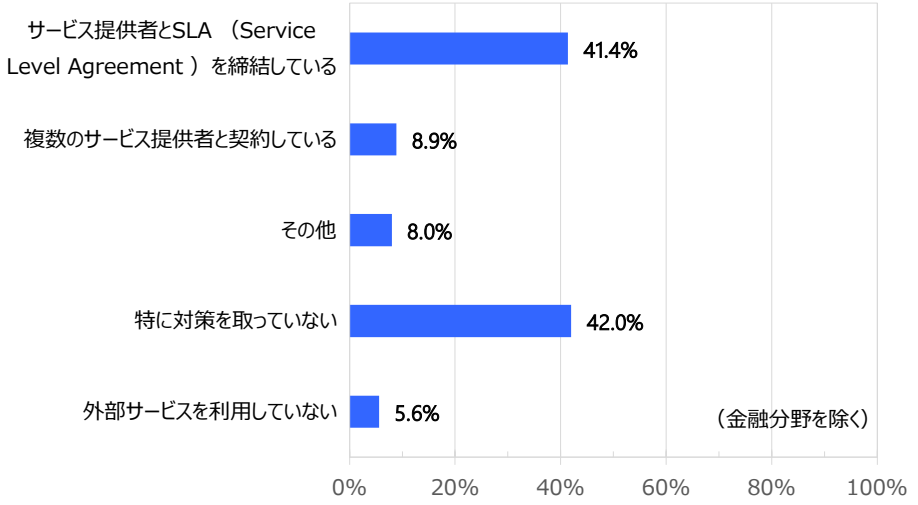


設問10.【複数回答】
テレワークの際に実施している情報セキュリティ対策を全て選択してください。

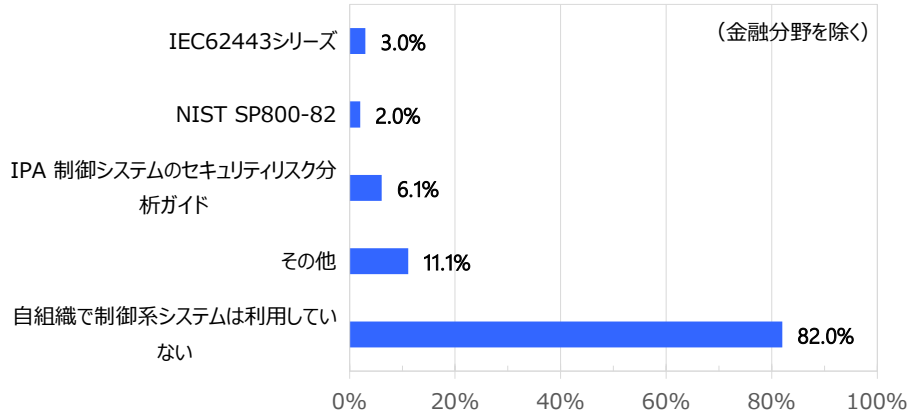
（金融分野を除く）



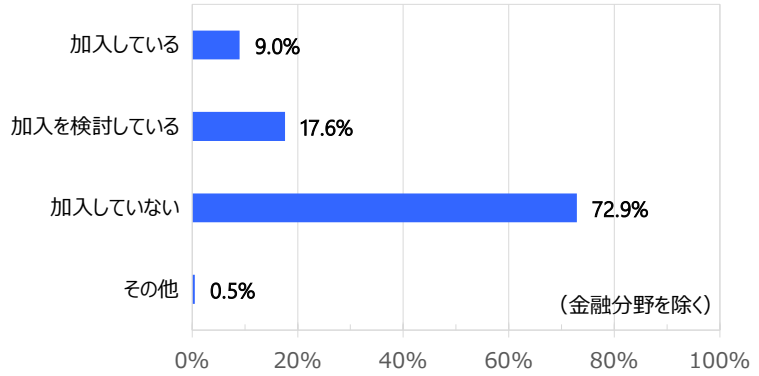
設問11－1.【複数回答】
他組織が提供するサービス（外部サービス）が何らかの事由によって利用不可能となった場合に備えて行っている対策を全て選択してください。



設問11－2.【複数回答】
制御系システムのセキュリティ対策。



設問11－３．【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11－４．【複数回答】
ランサムウェア対策の攻撃、運用体制。