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

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22回）

重要インフラ分野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［2019年度］

令和２年７月13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

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**。

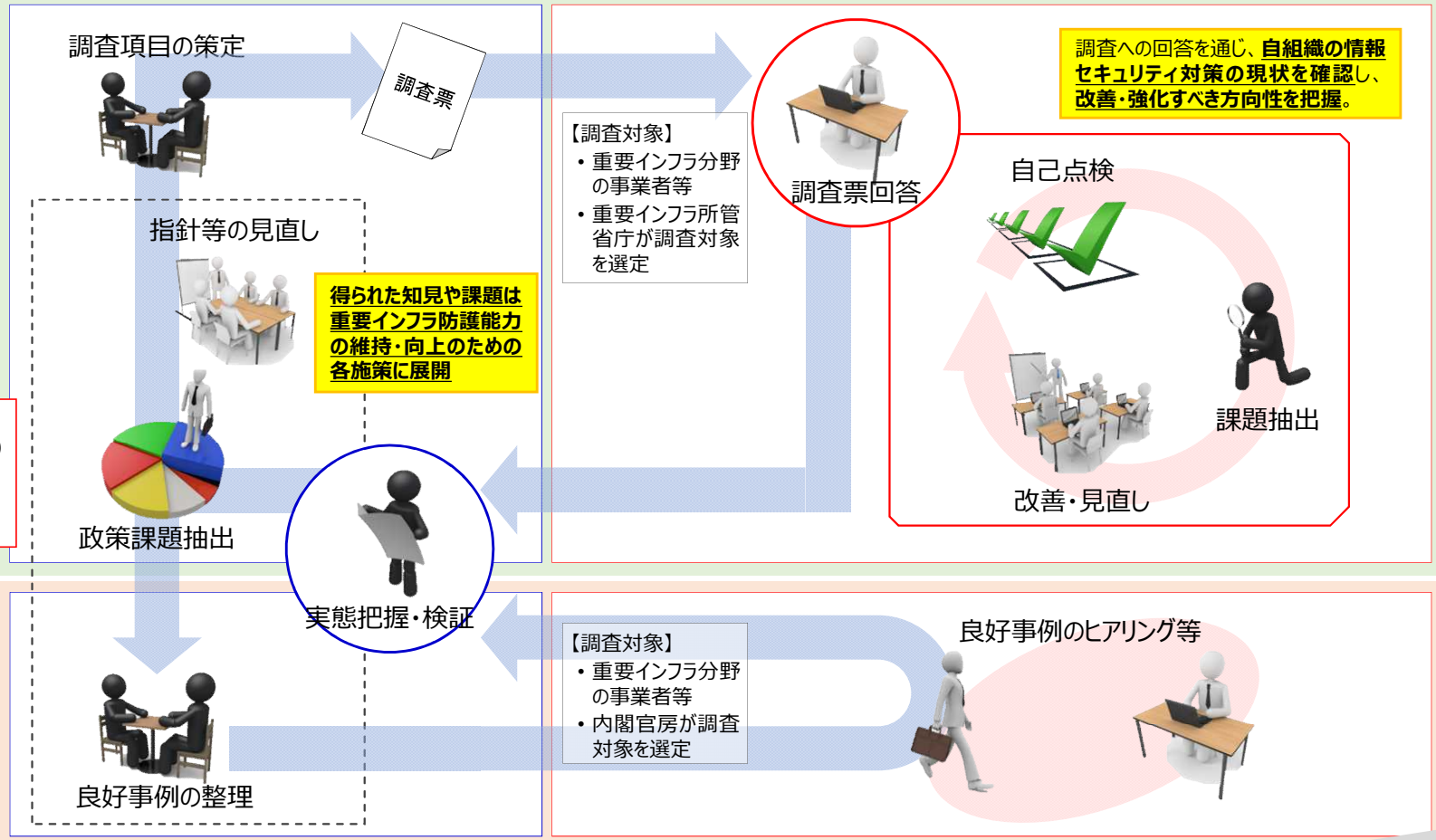
行動計画の検証のための指標
①ベースラインとなる情報セキュリティ対策に取り組んでいる重要インフラ事業者等の割合
②先導的な情報セキュリティ対策に取り組んでいる重要インフラ事業者等の割合

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。

調査の流れ（イメージ）



（参考）調査の位置付け

「重要インフラの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、**2019年度の調査では、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）の実施状況について調査**した。
- 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：2019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07ページに記載）
調査方法	次のいずれか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

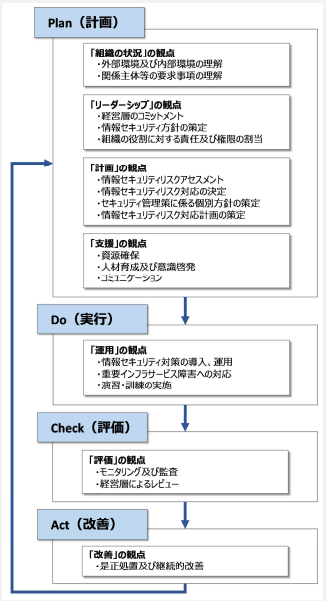
【内閣官房】
- 得られた知見や課題は必要に応じて各施策へと展開。
- **行動計画の検証や評価に活用**。

【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

- 指針は、PDCAサイクルの各段階において「安全基準等」で規定が望まれるとする情報セキュリティ対策（対策項目）を提示している。
- 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：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

- 2019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行い、**2,205事業者から回答**（回答率65.4% 前年度比＋5.3pt）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	23	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。）	122	
	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	138	
金融		銀行等、証券会社、生命保険会社、損害保険会社	（642）	外部調査※
航空		主たる定期航空運送事業者	5	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	21	
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	1,057	
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	21	
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	96	
物流		大手物流事業者	12	
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	9	
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	10	
全分野合計		－－－	**2,205**	－－－

※金融分野については、公益財団法人金融情報システムセンター（FISC）が実施した「令和元年度金融機関アンケート調査」の結果を活用。
同調査結果をNISC調査の結果に読み替えて集計。

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. サプライチェーンの把握
  設問1-3. 関係主体からの要求事項の整理

- **セキュリティポリシの観点**
  設問2-1. 基本方針の策定
  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

- **情報セキュリティ対策の観点**
  設問3-1. リスクアセスメントの実施
  設問3-2. 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3-3. 実施している情報セキュリティ対策
  設問3-4. 実施している情報セキュリティ対策の文書化
  設問3-5. 情報セキュリティ対策の導入・実施に関する計画の策定

- **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］

- **運用の観点**
  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. CSIRTの整備
  設問5-6. 実施・参加している演習・訓練

□ Check［評価］

- **評価の観点**
  設問6-1. 情報セキュリティ対策に関する監査の実施

□ Act［改善］

- **改善の観点**
  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

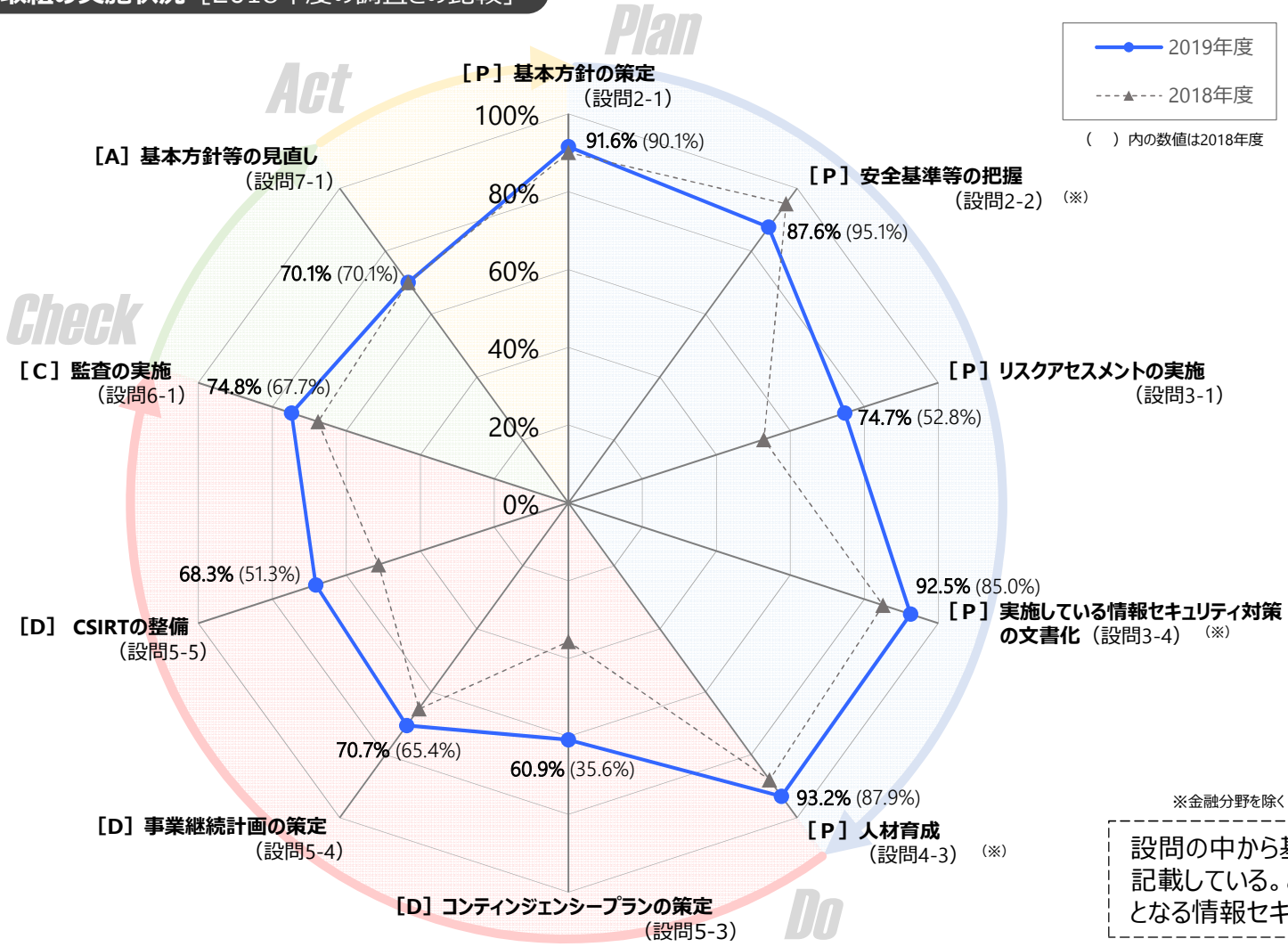
□ その他

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

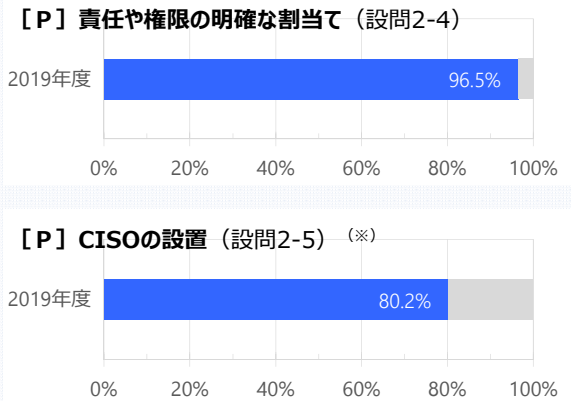
アンケート調査結果概要（総評）　－　ベースラインとなる情報セキュリティ対策

- 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おおむね向上**しており、**安全基準等の浸透は着実に進展**していると評価できる。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）、Act（改善）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。

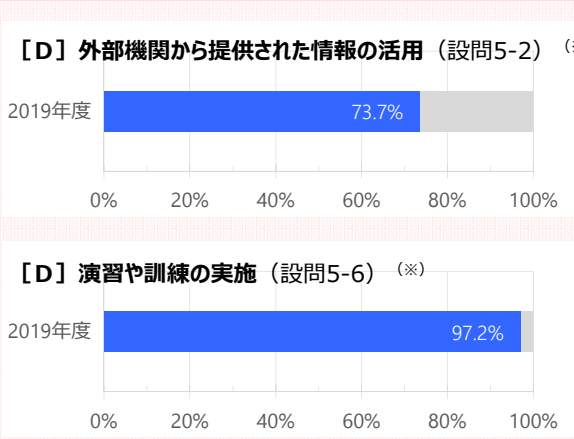
各取組の実施状況［2018年度の調査との比較］



※金融分野を除く



※金融分野を除く



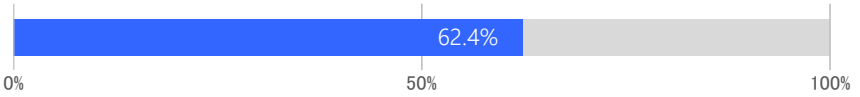
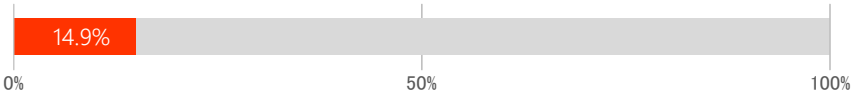
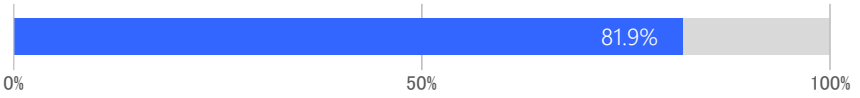
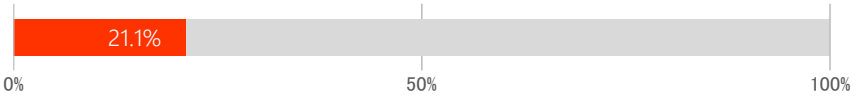
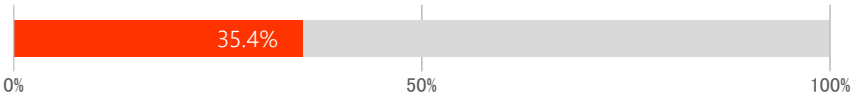
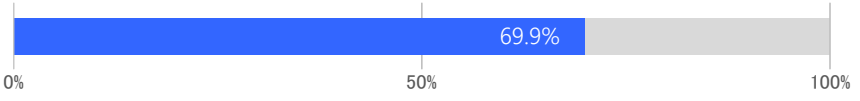
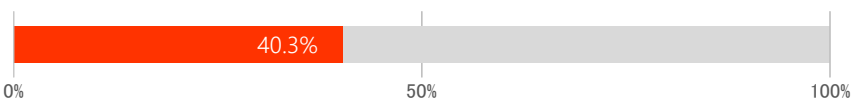
※金融分野を除く

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、**複数の項目で実施状況が５割を超えており、先導的な情報セキュリティ対策に関する取組も着実に進展**し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、実施状況が低い項目も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。

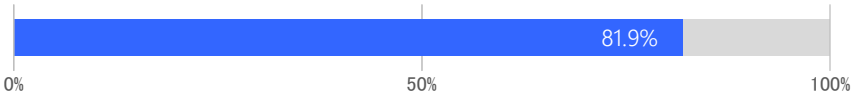
情報セキュリティ対策が単に情報システムの構築・運用の観点だけでなく、**企業経営の観点からも検討**されていること。	● **経営層からの関与がある**（設問8-1）（※）　※金融分野を除く 
システムの構築・運用及び企業経営の**各責任者が適切に相互関与する体制が整備**されていること。	● **経営層と定期的なレポーティング・対話の場が設けられている**（設問8-2）（※） 
守るべき重要インフラサービス及びサービス維持レベルを踏まえ、**自らがなすべき必要な対策が理解**されていること。	● **関係主体からの要求事項を整理している**（設問1-3）（※）  ● **機能保証の考え方を取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を行っている**（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）

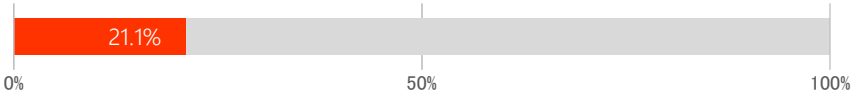
将来像②：「課題抽出」、「リスク評価」及び「対策の改善」に関する次の事項が十分に浸透している。

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1-3）（※）【再掲】　※金融分野を除く

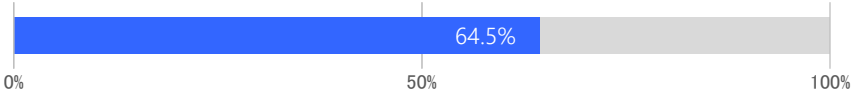


- **機能保証の考え方を取り入れたリスクアセスメントを実施している**（設問3-1）（※）【再掲】

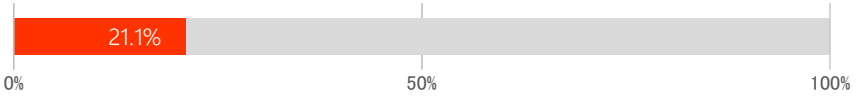


各種情報セキュリティ対策の進展や環境変化によるリスク源や重要インフラサービス障害に係る**リスクの変化を適切に察知して、各々自主的に対策を進め、また必要な調整を行うようになっている**こと。

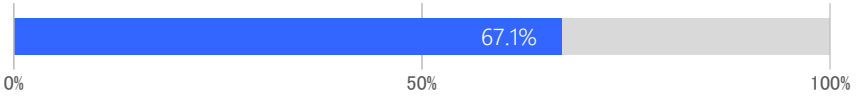
- **内部環境及び外部環境を整理している**（設問1-1）（※）



- **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】

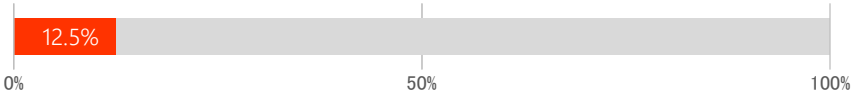


- **情報セキュリティ計画を策定している**（設問3-5）（※）



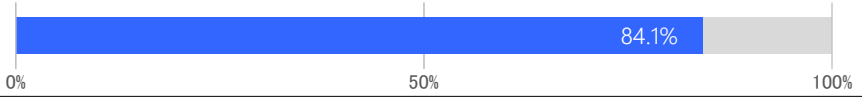
重要インフラサービス障害が発生した場合に備えた適切な対策を講じることが可能になっており、その成果として、**重要インフラサービス障害が国民生活や社会経済活動に重大な影響を与えるリスクを可能な限り低減**させることができていること。

- **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。

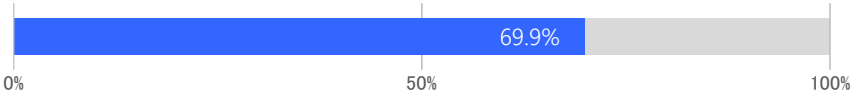
- **基本方針等の継続的な見直しを行っている**（設問7-1）（※）



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

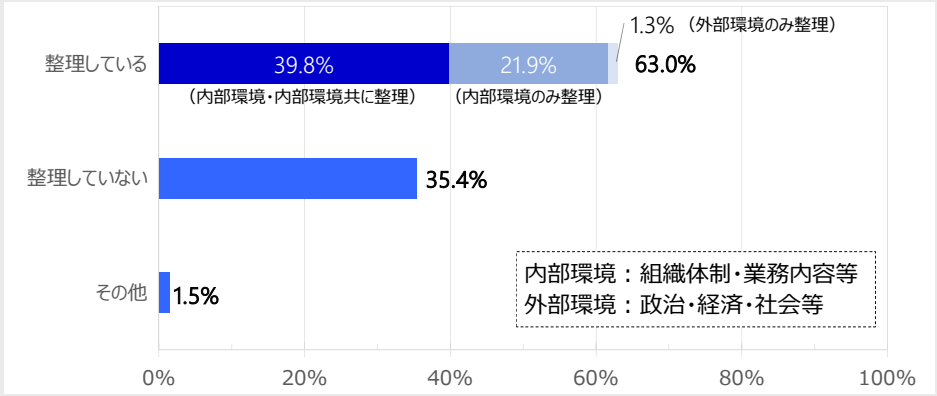


アンケート調査結果概要 － Plan［計画］（1/3）

- 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やリスクアセスメントは半数以上の組織が実施**しており、自組織を取り巻く状況の把握は進んでいる。しかしながら、**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の実施は一部にとどまっている**状況にあることから、今後はこれらの取組の着実に実施するとともに、質的な向上を図っていくことが課題であると考えられる。
- また、情報セキュリティ対策の基盤となる**人材や予算に関しては約７割の組織が十分に配分されていないと回答**していることから、各組織で自主的な努力が行われることを前提としつつ、必要に応じ、関係主体において人材育成等を支援していくことも重要であると考えられる。

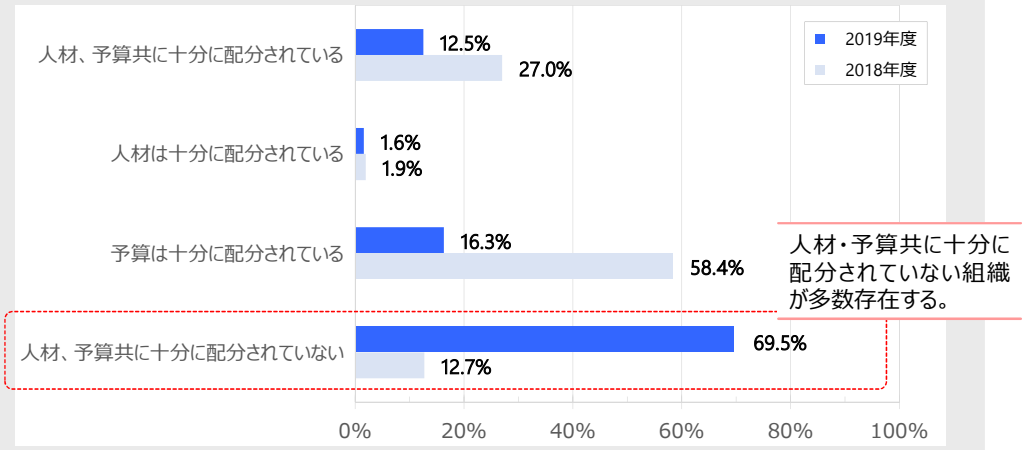
組織の状況の観点

► 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



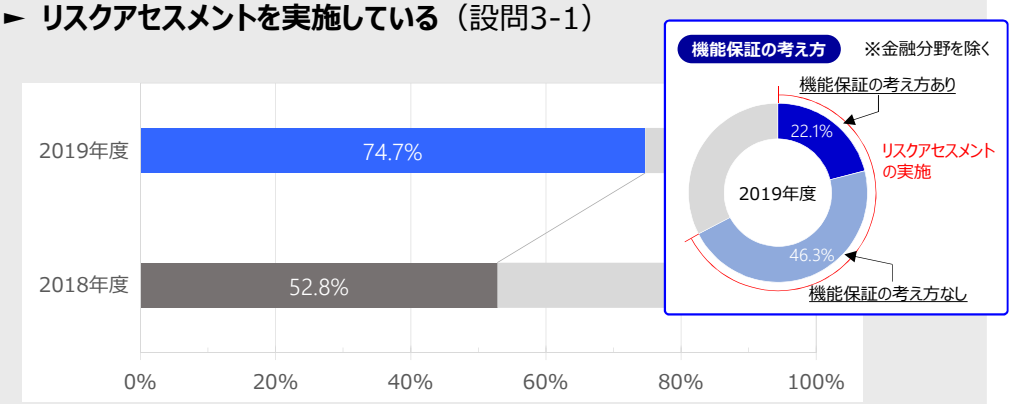
支援の観点

► 必要な人材や予算が適切に配分されている（設問4-1） ※金融分野を除く



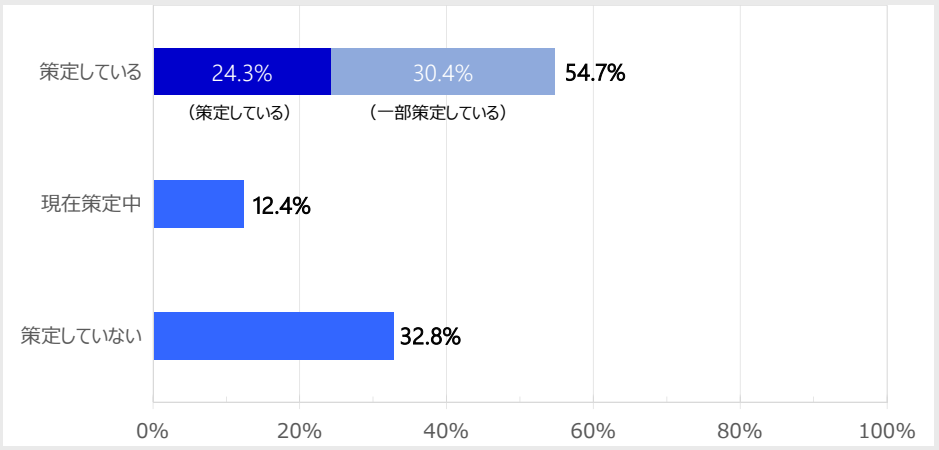
情報セキュリティ対策の観点

► 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

► 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）を策定している（設問3-5） ※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、②情報セキュリティ対策基準、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2018年度と比較して増加しており、**情報セキュリティに係る方針や基準の整備は着実に進展**している。一方で、①情報セキュリティ基本方針の策定済みの組織が約９割に達するのに対し、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や③情報セキュリティ対策実施手順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、自分野の安全基準等を把握していない組織が一部存在することから、**重要インフラ所管省庁等が主体となって安全基準等を積極的に周知していく必要**があると考えられる。

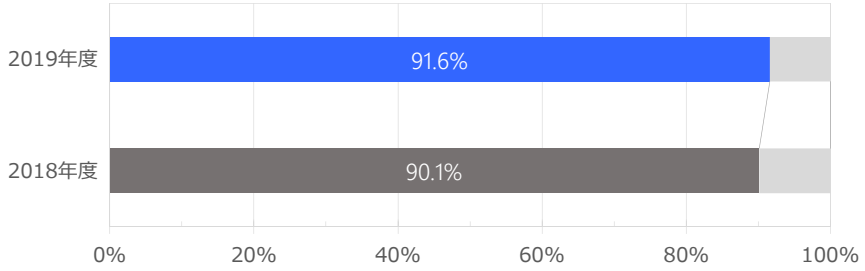
セキュリティポリシの観点／情報セキュリティ対策の観点

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

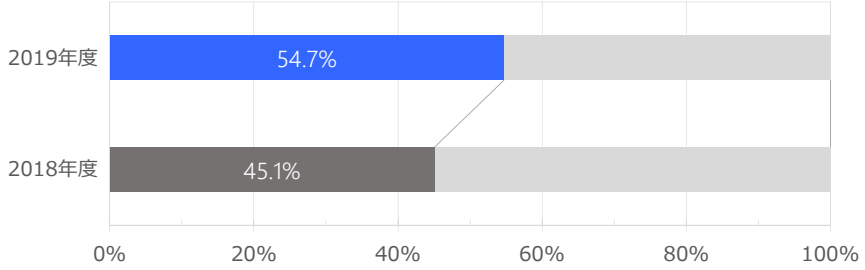
► **情報セキュリティ基本方針を策定している**（設問2-1）



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3-5）※金融分野を除く

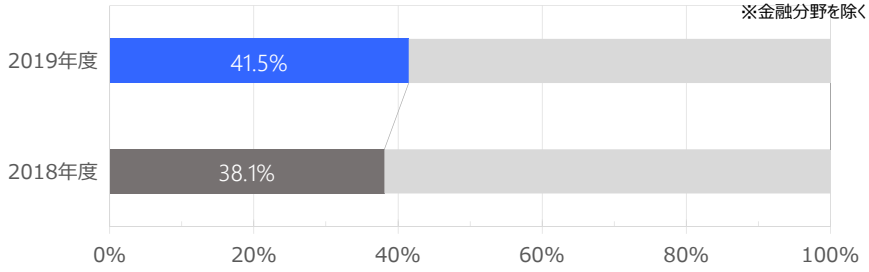


③情報セキュリティ対策実施手順

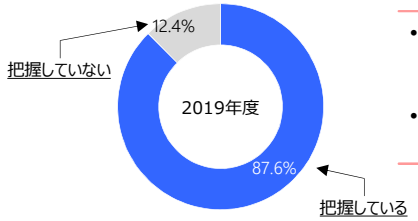
情報セキュリティ対策を実施するための詳細な手続・手順（マニュアル等）

► **情報セキュリティ対策実施手順を策定している**（設問3-4）

※金融分野を除く

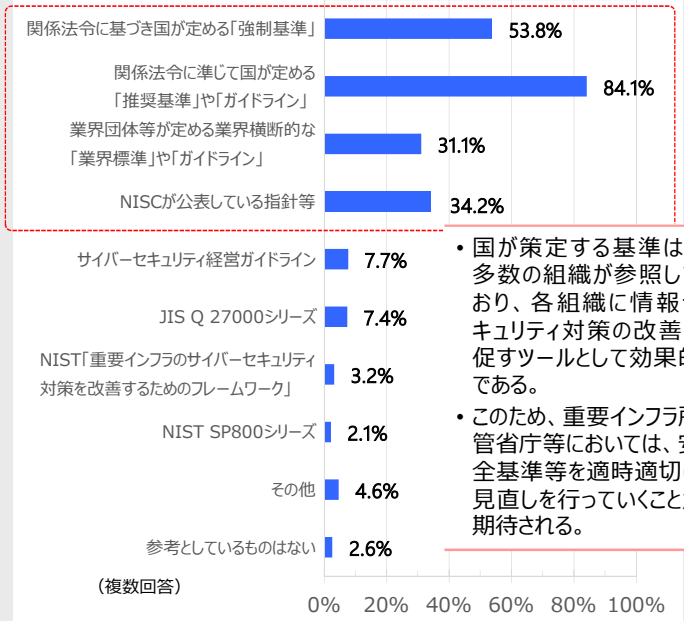


► **自分野に関係する安全基準等を把握している**（設問2-2）※金融分野を除く



- 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



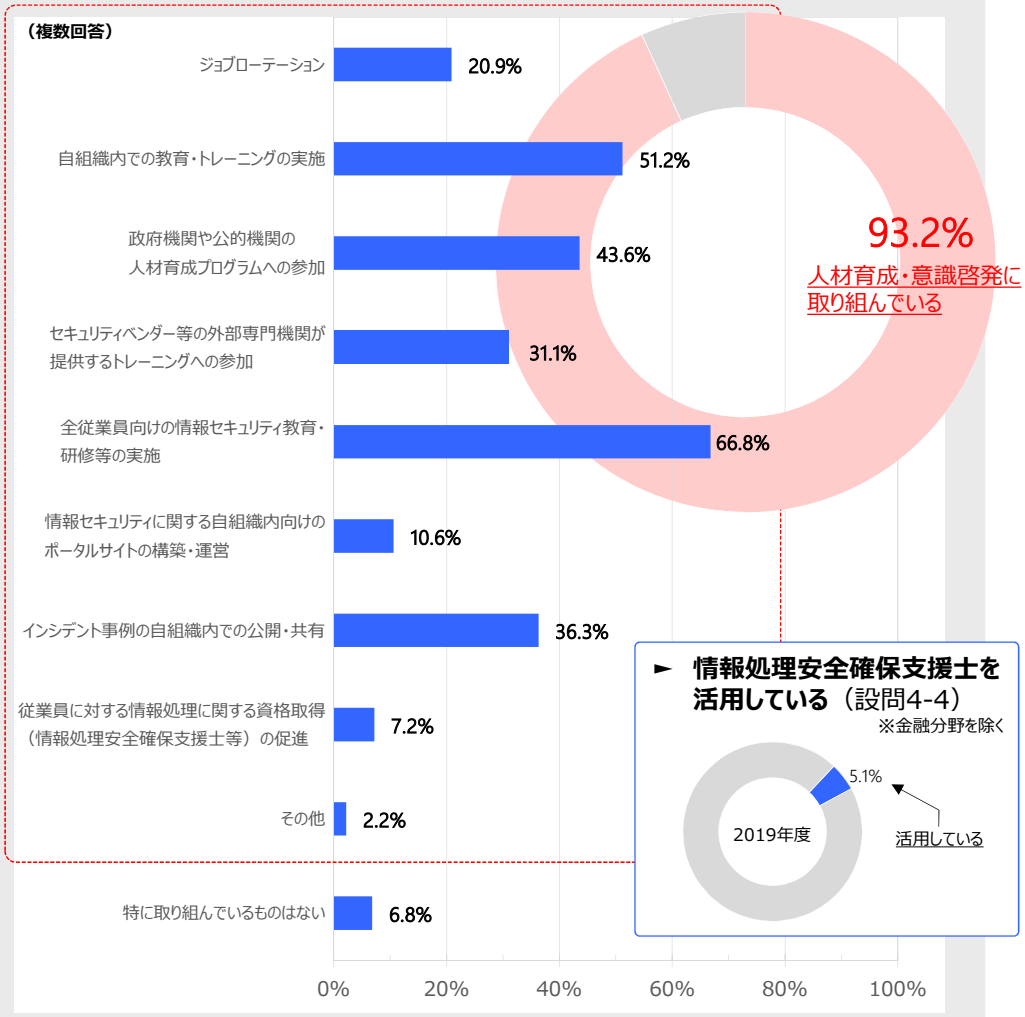
- 国が策定する基準は、多数の組織が参照しており、各組織に情報セキュリティ対策の改善を促すツールとして効果的である。
- このため、重要インフラ所管省庁等においては、安全基準等を適時適切に見直しを行っていくことが期待される。

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2018年度の調査から半減して２割を下回っている**状況にあり、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の不足が深刻化**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現場の従事者を中心に多岐にわたっており、**人材の育成・確保が多くの組織の課題**であるといえる。

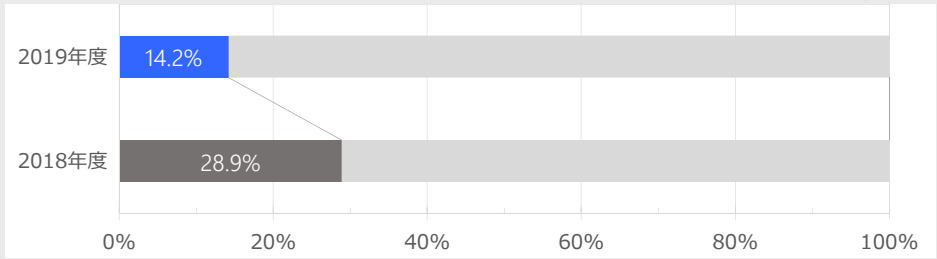
支援の観点

► 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

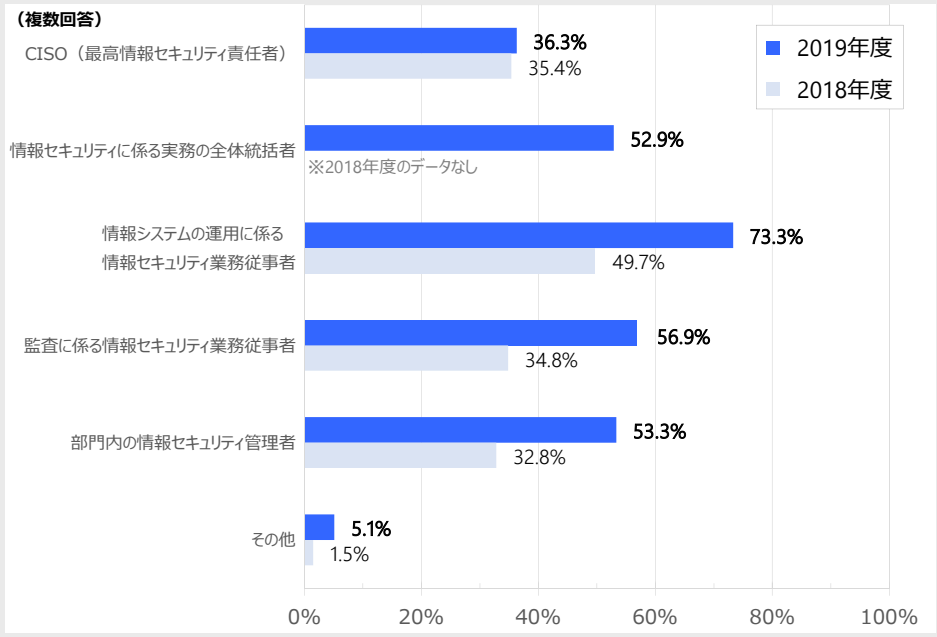


► 情報処理安全確保支援士を活用している（設問4-4）※金融分野を除く

► 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



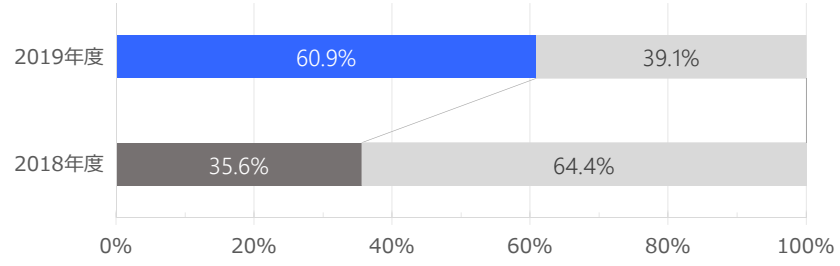
アンケート調査結果概要　－　Do［実行］

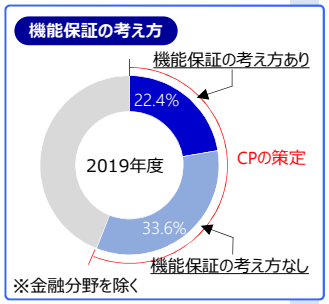
- コンティンジェンシープランや事業継続計画の策定、CSIRTの整備は多くの組織で進められており、**重要インフラサービスの障害の発生に備えた対処態勢の整備は着実に進展**している。一方で、機能保証の考え方は取り入れは一部にとどまっていることから、引き続きの課題である。
- また、多数の組織が演習・訓練の実施・参加や外部機関から共有・提供された情報の活用を通じ、サイバー攻撃等に対する自組織の対処能力の向上に努めていることが確認できる。ただし、**約３割の組織は演習・訓練を実施していない**ことから、我が国全体の対処能力を向上させるためにも、それらの組織に対しては**政府機関や公的機関が提供する演習等への参加を促していくことが一つの方策**として考えられる。

運用の観点

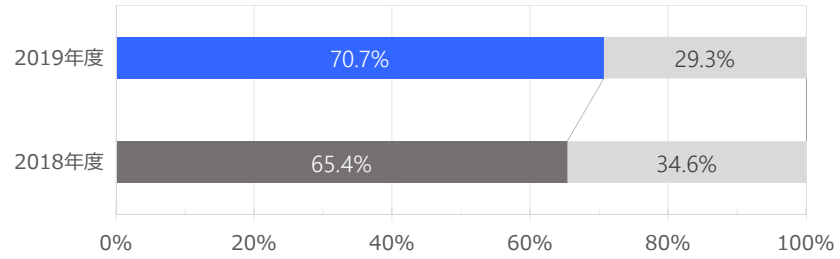
重要インフラサービス障害の発生に備えた対処態勢の整備

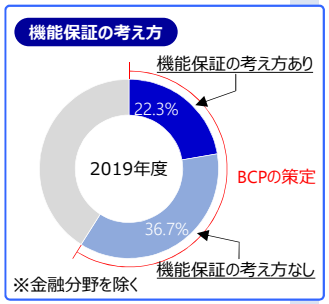
► **コンティンジェンシープラン（CP）を策定している**（設問5-3）



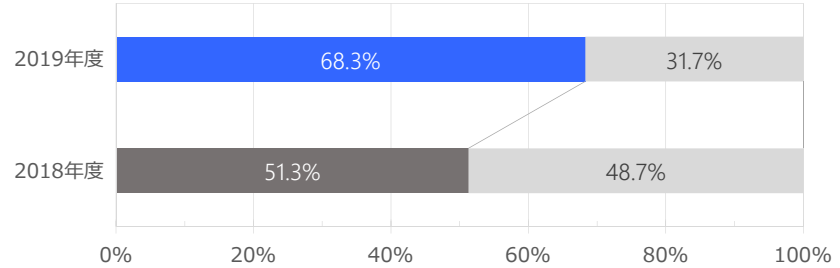


► **事業継続計画（BCP）を策定している**（設問5-4）

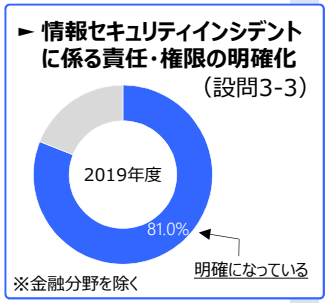




► **CSIRTを整備（注）している**（設問5-5）（注）同等の機能を持つ組織を含む。

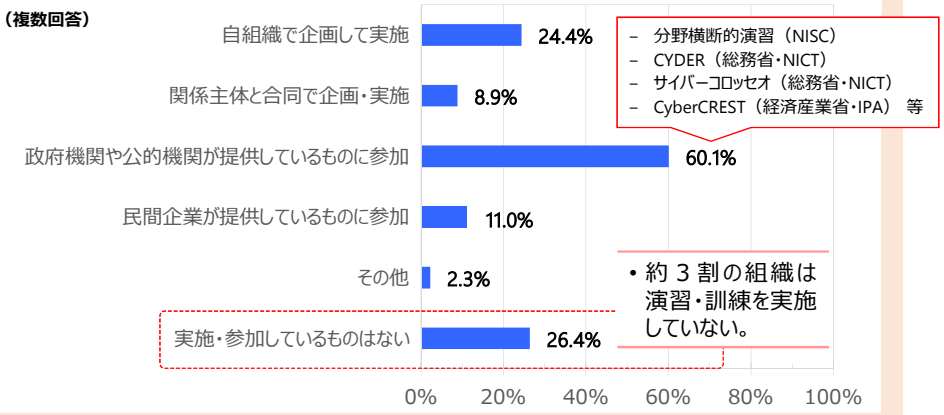


► **情報セキュリティインシデントに係る責任・権限の明確化**（設問3-3）

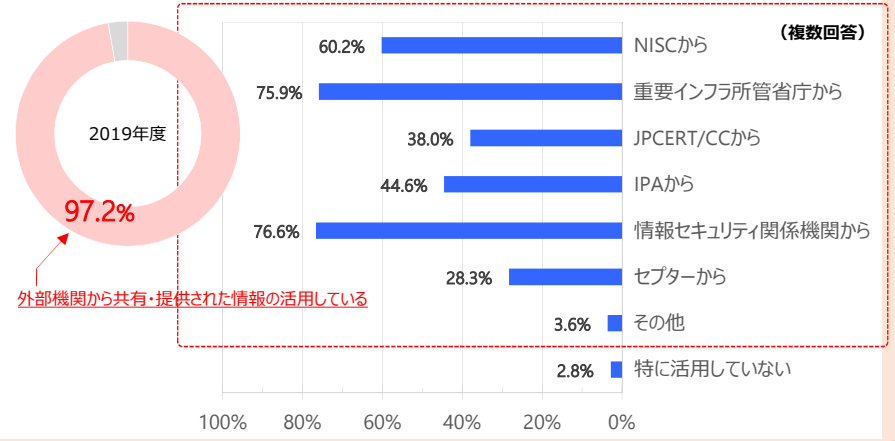


演習・訓練及び情報活用による対処能力の向上

► **実施・参加している演習・訓練**（設問5-6）※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

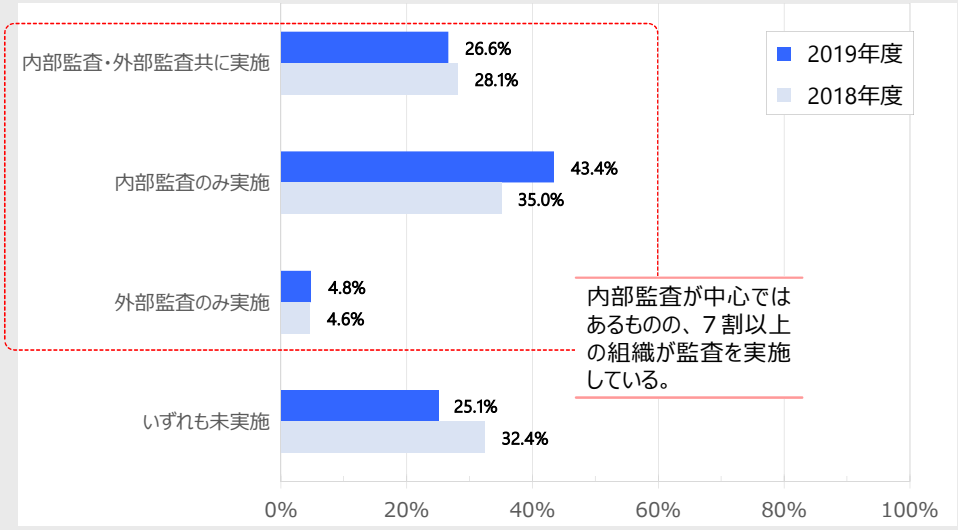


アンケート調査結果概要　－　Check［評価］／ Act［改善］

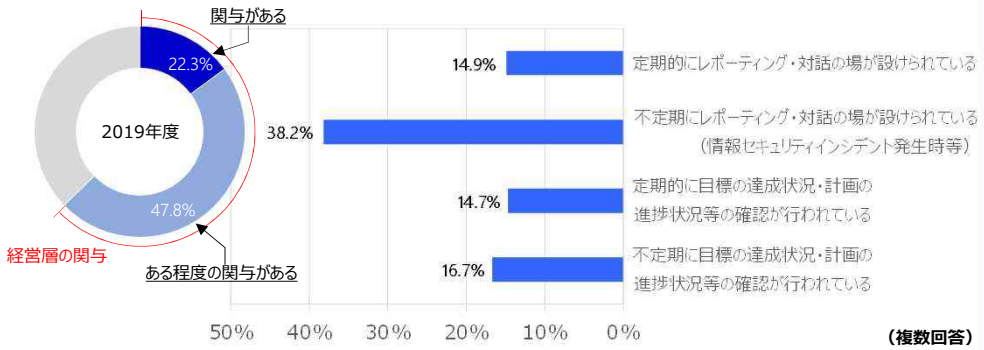
- 多くの組織で**内部監査を中心に情報セキュリティ対策に関する監査が実施**されており、**「評価」の枠組みは一定程度構築**されていると考えられるが、監査結果を基にした見直しの実施は約２割にとどまっている。情報セキュリティ対策を適切なものとしていくためには、現状を評価し、適時に改善していくことが必要不可欠であることから、**「評価」を「改善」につなげていく体制を構築していくことが今後の課題**であるといえる。
- また、情報セキュリティ対策に経営層が関与する組織は７割を超えているものの、定期的なレポーティング・対話の場が設けられているのは２割に満たないことから、各組織においては**経営層との密なコミュニケーションを図っていくことが期待**される。

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

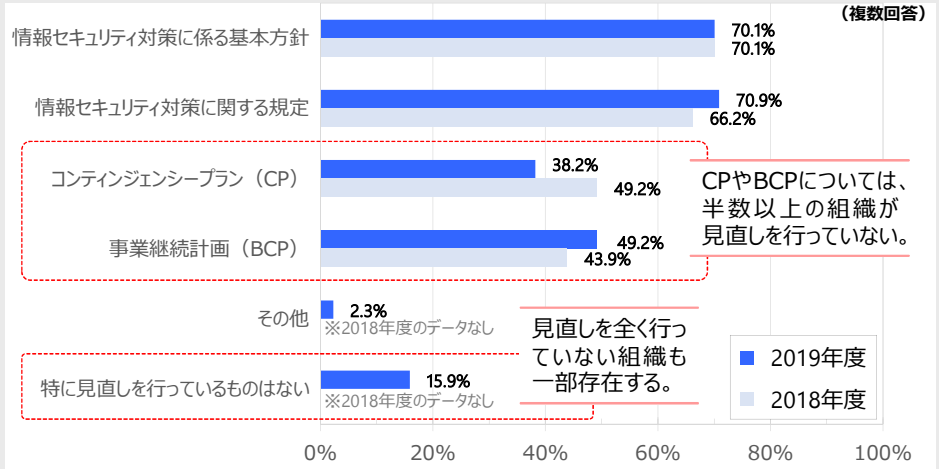


► 情報セキュリティ対策に経営層が関与している（設問8-1, 8-2）※金融分野を除く

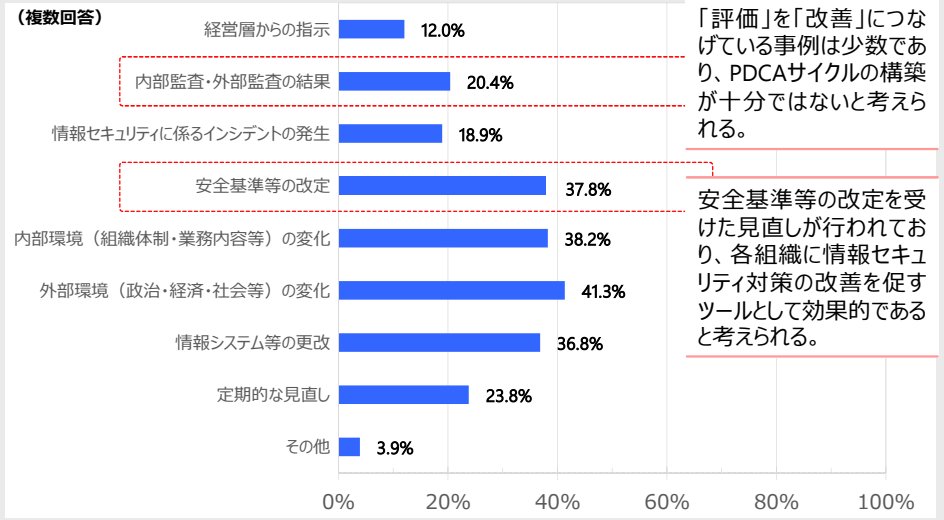


改善の観点

► 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



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。
- 2019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、**サイバー攻撃等の事案発生時の対処態勢、教育・人材育成等に関する事例の調査を実施**した。

【調査対象（2019年度）】 情報通信分野、金融分野、政府・行政サービス分野、物流分野、クレジット分野等の重要インフラ事業者等

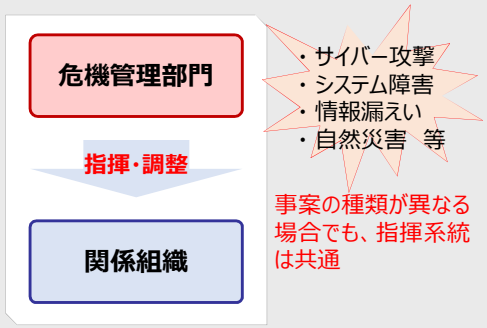
往訪調査結果概要

事例① サイバー攻撃等の対処態勢について

- サイバー攻撃、システム障害、情報漏えい、自然災害等の**事案発生時における対応組織や対応要領を共通化**

✓ **関係組織間の迅速かつ適切な連携・意思決定**の実現

● **事案発生時の対応要領等の共通化**

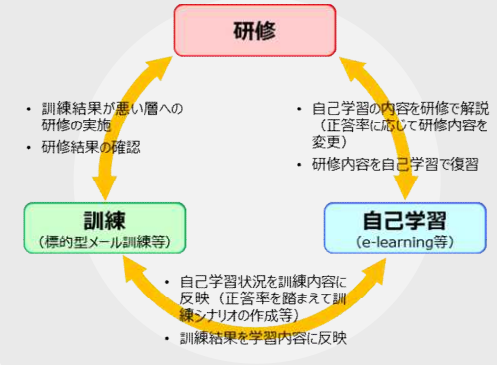


事例② 従業員等へのセキュリティ教育について

- **早期からの継続的なセキュリティ教育の実施**
- 従業員等の**セキュリティ習熟度の体系的な管理**

✓ **統一的なセキュリティ水準の確保**
✓ セキュリティ意識の向上

● **継続的なセキュリティ教育**



事例③ サイバーセキュリティに係る対処能力の評価・検証について

- システムの脆弱性だけではなく、**人や業務プロセスを含む組織的な対応能力を検証**

✓ **組織的な対応能力を把握**
✓ 自組織の**セキュリティ対策の有効性を評価**

● **レッドチームテストによる評価・検証**

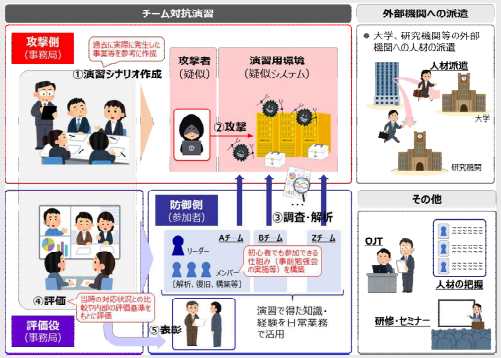
（参考）	概要	対象
レッドチームテスト	システムのセキュリティに加え、人的、物理セキュリティの脆弱性を突いた攻撃を行い、組織全体を包括的に評価する。	人、システム、業務プロセス
ペネトレーションテスト	攻撃者等が実際に用いる手法でシステムに対して攻撃を行い、システム内部への侵入を試みることでシステム全体の脆弱性を特定する。	システム
脆弱性診断	システムに存在する脆弱性やセキュリティ的な不備を網羅的に検査する。	システム

事例④ サイバー演習を通じた人材育成・発掘について

- 過去に**自組織で実際に発生した事案を基に演習を実施**
- 演習の参加者を幅広く募る仕組みの構築

✓ **セキュリティ人材の自給**
✓ 技術・知識や関心がある**人材の発掘**

● **演習等を通じた人材育成・発掘**



事例①　－　サイバー攻撃等の対処態勢について

事例の概要

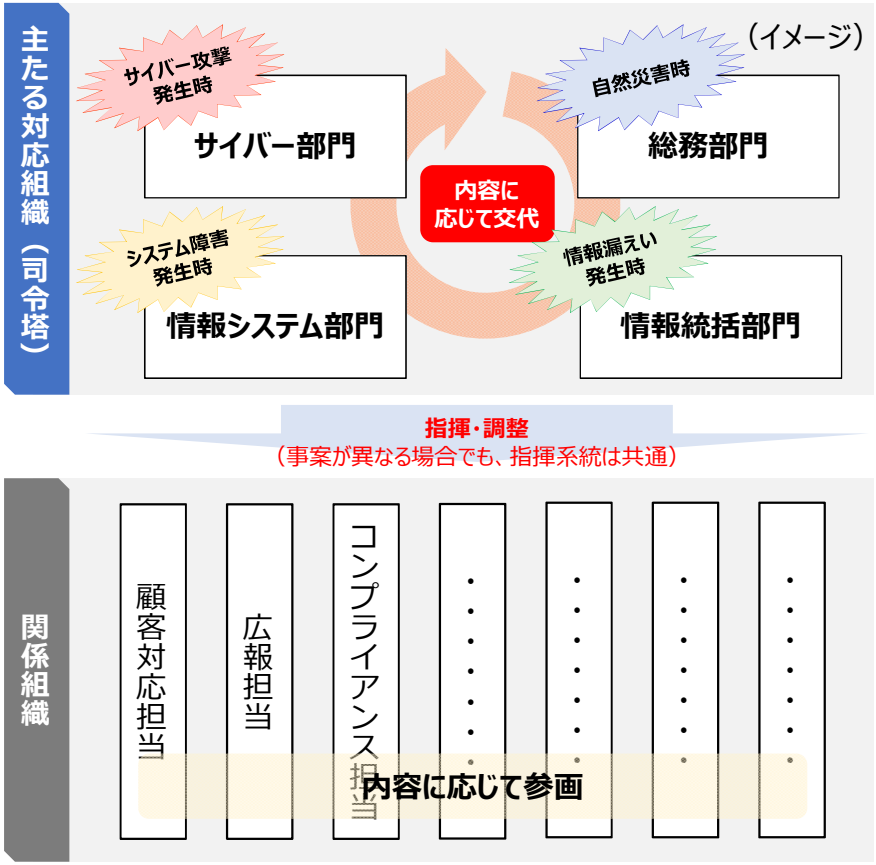
- サイバー攻撃、自然災害、情報漏えい、システム障害等の事案の種類や内容に応じて専門の対処態勢を整備するのではなく、**事案発生時における対応組織や対応要領の共通化**を図り、**同一の指揮系統で事案に対処**している。
- また、リモートで対応できること（情報収集等）を切り出し、事案対処への早期の着手を実現している。
- これらにより、様々な事案に対して**迅速な対処を可能**とするとともに、事案対応の積み重ねによって**関係者の熟練度を高め、対処能力の向上**につなげている。

a. 対応組織・対応要領を共通とする場合

➢ 事案の種類や内容にかかわらず、対応組織と対応要領を共通とする。

b. 対応要領のみを共通とする場合

➢ 事案の種類や内容に応じて対応組織の入替えを行うものの、対応要領は共通とし、指揮系統や関係部門の役割は同一とする。



本事例のポイント

- ✓ サイバー攻撃、システム障害、情報漏えい、自然災害等の**事案発生時における対応組織や対応要領を共通化**。
- ✓ 事案の種類や内容に応じた専門の態勢は設けずに、**同一の指揮系統で様々な事案に対処**。
- ✓ 現場で対応することとリモートで対応することとの切り分け。

本事例の利点

- ✓ **関係組織間の迅速かつ適切な連携・意思決定**の実現。
- ✓ 事案対応の積み重ねによる**関係者の熟練や対処能力の向上**。
- ✓ 対応要領だけではなく、対応組織まで共通化している場合は、事案の原因が不明な状況においても、事象の切り分けを待たずに**早期の態勢の立上げが可能**。
- ✓ 一部をリモートで対処することにより、**迅速な初動対応**を実現。

事例②　－　従業員等へのセキュリティ教育について

事例の概要

- セキュリティ教育は単体の取組では効果に限界があるため、研修、訓練（標的型メール訓練等）、自己学習（e-learning等）等の**各種取組を相互に活用して連携**させることにより、教育効果の向上につなげている。
- また、**セキュリティに関する事案発生時の対応方法や連絡先を従業員に常時携帯**させ、セキュリティに関する意識の向上を図っている。

日頃からのセキュリティ意識の醸成

- **研修・訓練・自己学習を連携させたセキュリティ教育の推進**

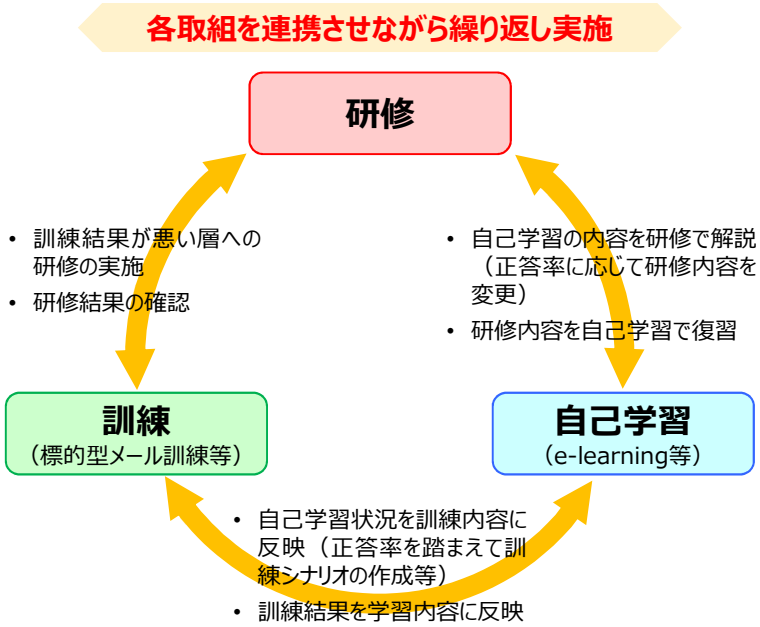
（取組の例）

研修　新人研修時から情報セキュリティに関する研修の実施**（入社時からの意識の植え付け）**。

訓練　【標的型メール訓練】
「開封率」の把握だけではなく、**「運営窓口への報告」**までを訓練として実施

自己学習　【e-learning】
一定の水準に達するまで継続的に繰り返して実施。

（イメージ）



事案発生時の対処

- セキュリティに関する**事案発生時の対応方法や連絡先を明記したカードを従業員に配布**。
- 従業員証等と同様に常時携帯させることにより、**些細なことでもセキュリティ部門へ連絡がなされるよう意識付け**。

（イメージ）

セキュリティ事故対処カード

以下の場合は情報セキュリティインシデント発生の可能性が非常に高いと考えられますので、すぐに情報セキュリティ部門（内線○○○○）に連絡してください。

- **○○○したとき**
- **○○○したとき（注意：すぐに○○すること）**
- **○○○したとき**

本事例のポイント

- ✓ **早期からの継続的なセキュリティ教育の実施**。
- ✓ 従業員等の**セキュリティ習熟度の体系的な管理**。
- ✓ セキュリティに関する**事案発生時の対応方法や連絡先の明確化**。

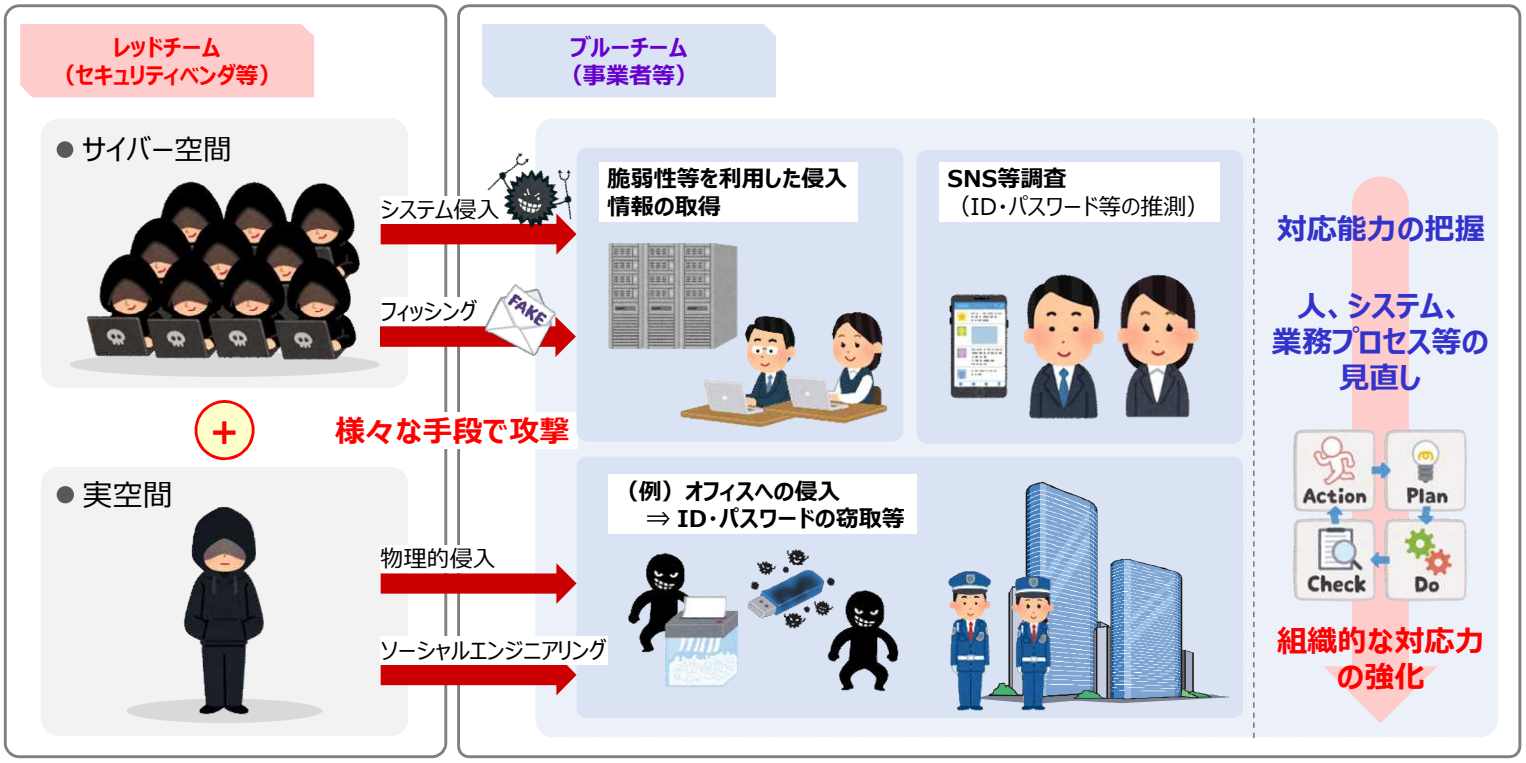
本事例の利点

- ✓ 早期からのセキュリティ教育の実施及び継続的な取組により、**従業員の統一的なセキュリティ水準の確保**。
- ✓ カード等でセキュリティに関する事案を具体的に提示し、**従業員のセキュリティに関する意識の向上**。また、これにより、**セキュリティ部門への積極的な連絡**、異常の早期発見に寄与。

事例③　－　サイバーセキュリティに係る対応能力の評価・検証について

事例の概要

- サイバーセキュリティに関する事案への組織的な対応能力の検証のため、**自組織の関係部署に対して様々な手段で攻撃への対応を行うテスト（レッドチーム）を実施**している。
- システムの脆弱性等のサイバー空間におけるセキュリティだけではなく、**事案発生時の人、業務プロセスといった実空間におけるセキュリティも対象**としており、**セキュリティ対策全般の有効性や組織的な対応能力を検証**している。



本事例のポイント

- ✓ 情報システム、通信ネットワーク等のサイバー空間だけではなく、**人、業務プロセスといった実空間におけるセキュリティも検証の対象**。
- ✓ システムの脆弱性だけではなく、**事案発生時の人や業務プロセスを含む組織的な対応能力を検証**。

本事例の利点

- ✓ 事案発生時における**組織的な対処能力を把握**。
- ✓ 自組織の**セキュリティ対策の有効性を包括的に評価**。
- ✓ 検証を通じた対処能力の養成。

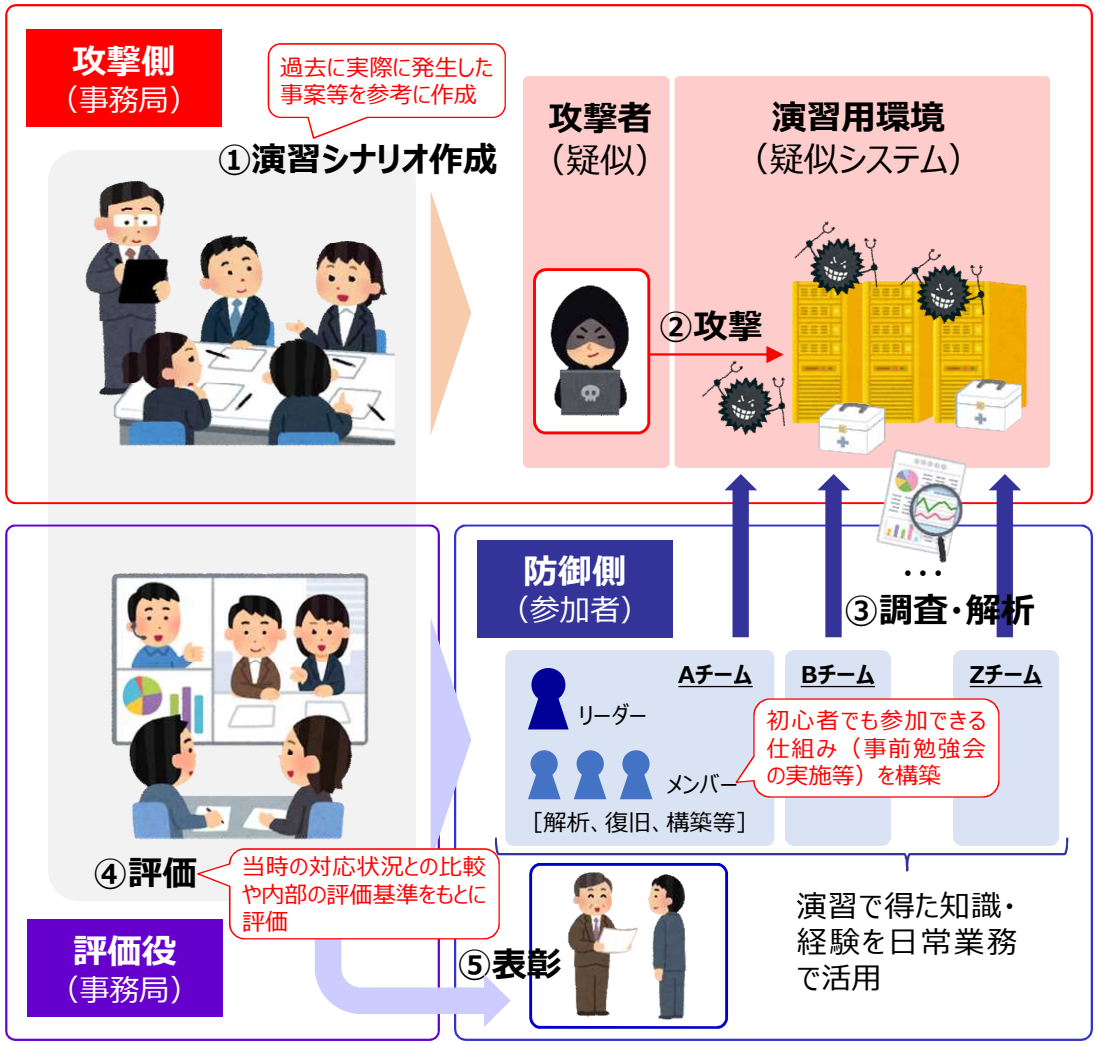
（参考）	概要	対象
レッドチームテスト	システムのセキュリティに加え、人的、物理セキュリティの脆弱性を突いた攻撃を行い、組織全体を包括的に評価する。	人、システム、業務プロセス
ペネトレーションテスト	攻撃者等が実際に用いる手法でシステムに対して攻撃を行い、システム内部への侵入を試みることでシステム全体の脆弱性を特定する。	システム
脆弱性診断	システムに存在する脆弱性やセキュリティ的な不備を網羅的に検査する。	システム

事例④　－　サイバー演習を通じた人材育成・発掘について

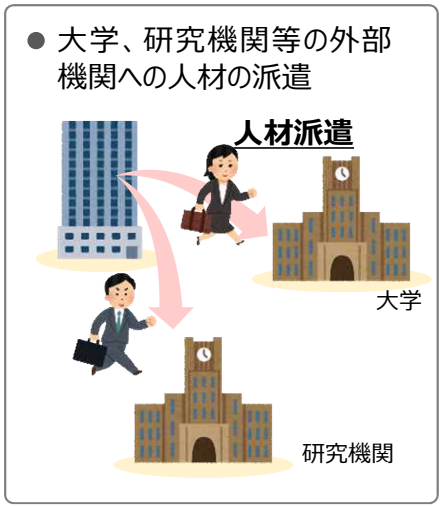
事例の概要

- サイバーセキュリティに関心を有する従業員を対象に、**演習用環境下における疑似的なサイバー攻撃に対する調査、対応、報告までを行うサイバー演習（チーム対抗演習）を実施**している。これにより、**演習参加者のスキルアップを通じて組織としての対処能力の強化**を図るとともに、**人材の発掘**を図っている。
- 加えて、OJTや研修・セミナーを通じて人材の育成を進めているほか、一定のスキルを有する人材については、大学等の外部機関へ派遣し、更なる能力の向上を図っている。

チーム対抗演習



外部機関への派遣



その他

本事例のポイント

- ✓ 演習の**目的・対象を明確化**。
- ✓ 過去に**自組織で実際に発生した事案を基に演習シナリオを策定**。
- ✓ 初心者コースの設定、見学の積極的な受入れ等、演習の**参加者を幅広く募る仕組みの構築**。
- ✓ 積極的な姿勢での参加を促すため、**事前の勉強会（ツールの使い方等）を実施**。
- ✓ 発掘した人材をOJT、研修・セミナー、外部機関（大学等）への派遣等を通じて育成。

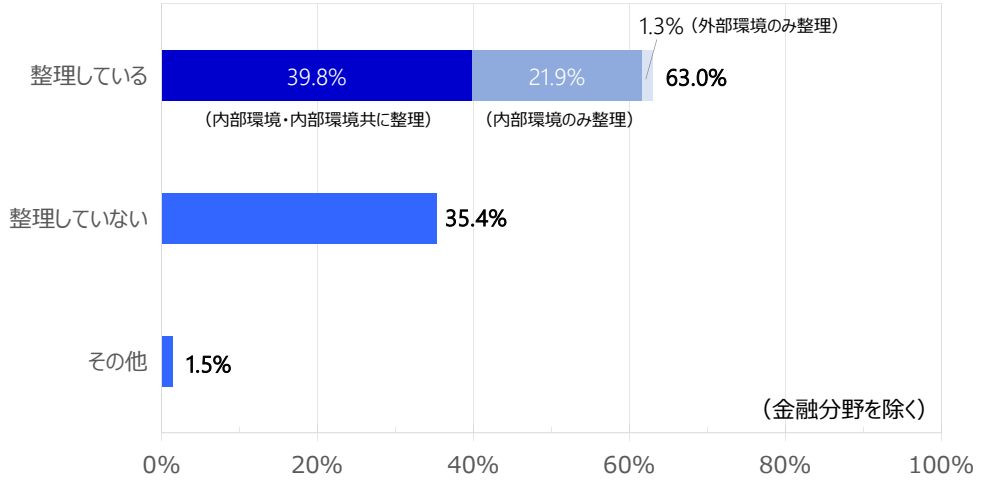
本事例の利点

- ✓ セキュリティ事案に対応できる内部人材の育成（**人材の自給**）。
- ✓ セキュリティの技術・知識を有する社員の把握、関心が高い**人材の発掘**。
- ✓ 過去に実際に自組織で発生した事案を体験することで、日常業務への活用が期待でき、効果的・効率的に**組織の対応能力を強化**。

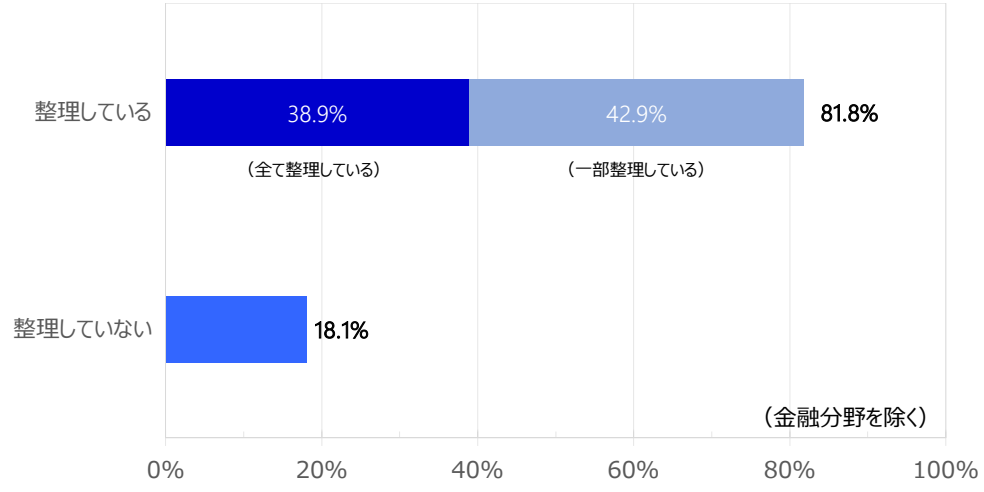
目次

アンケート調査結果　－　Plan［計画］（1/8）

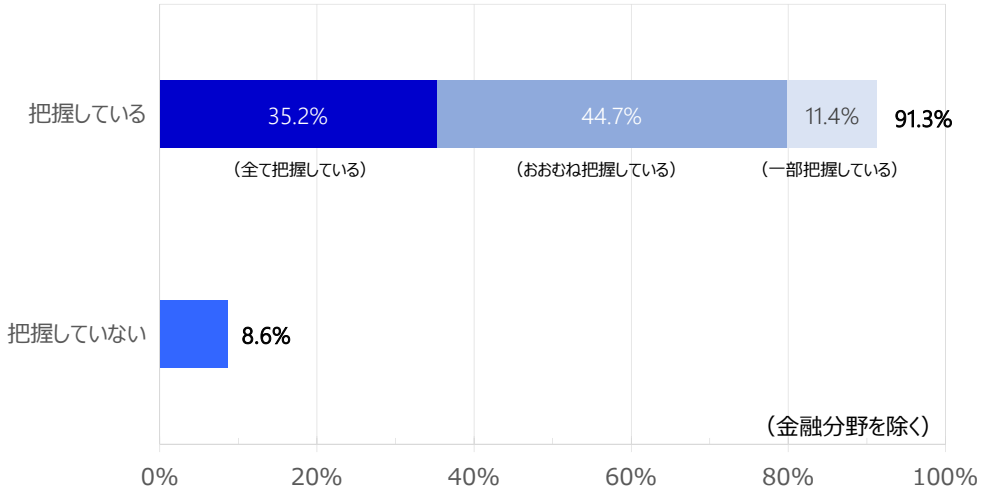
設問１－１．【単一回答】
自組織の重要インフラサービスの安定的かつ継続的な提供に影響を与えるおそれがある内部環境（組織体制・業務内容等）や外部環境（政治・経済・社会等）について、近い将来の状況を含めて整理していますか。



設問１－３．【単一回答】
関係主体、顧客、サプライヤー、委託先からの情報セキュリティ対策の取組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）を整理していますか。

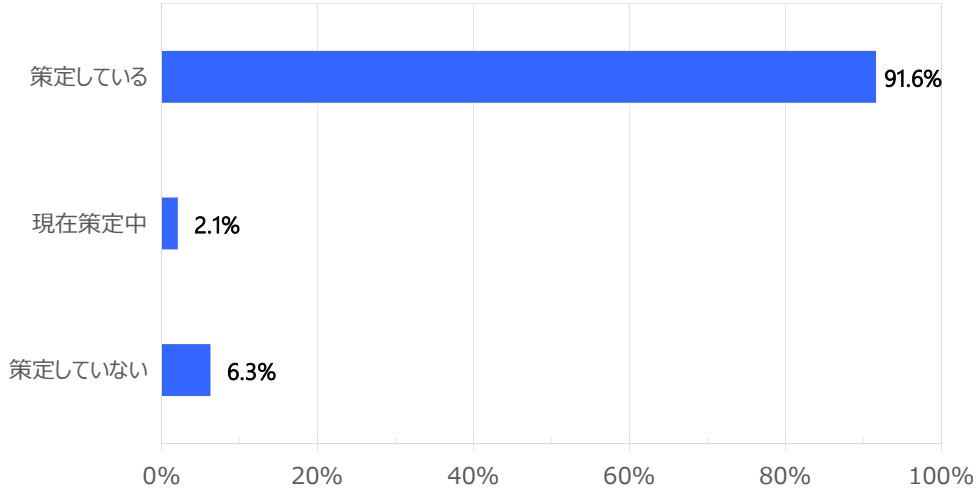


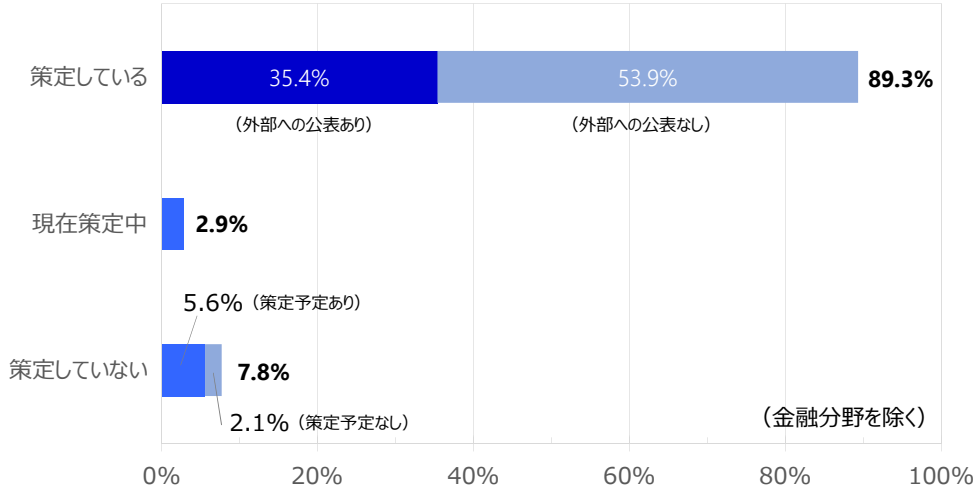
設問１－２．【単一回答】
自組織のサプライチェーン（サプライヤー、委託先等）を把握していますか。



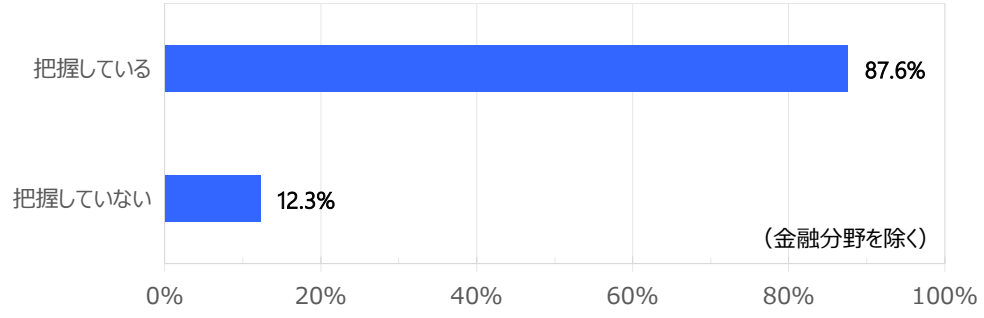
アンケート調査結果　－　Plan［計画］（2/8）

設問２－１．【単一回答】
情報セキュリティ対策に取り組む目的、方向性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。

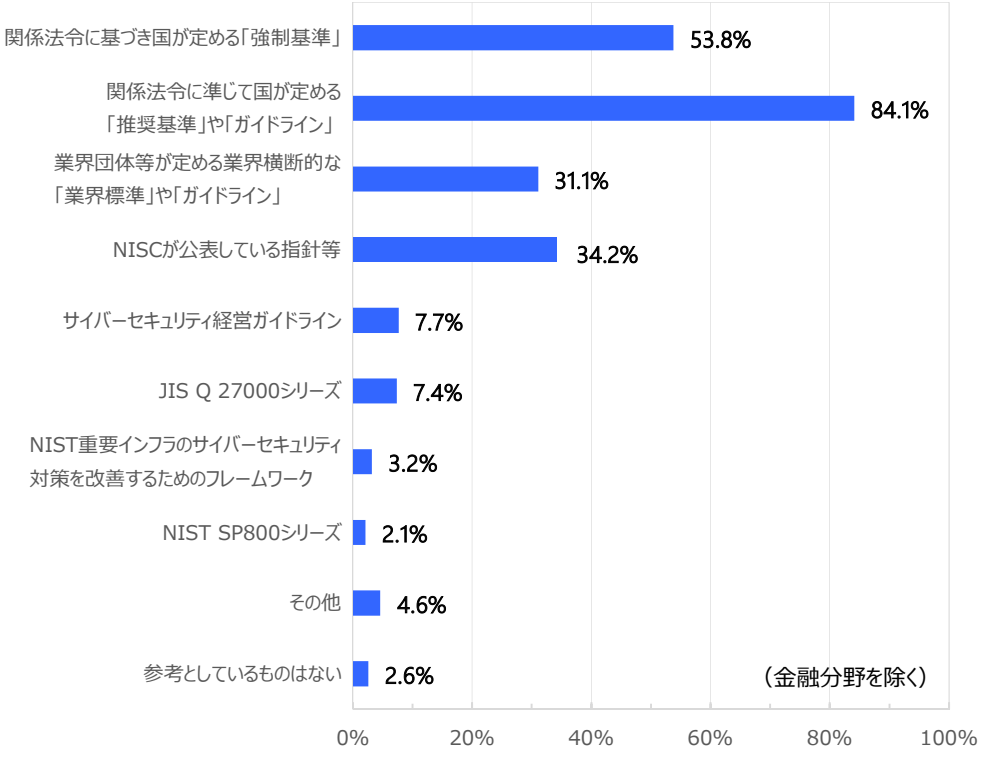




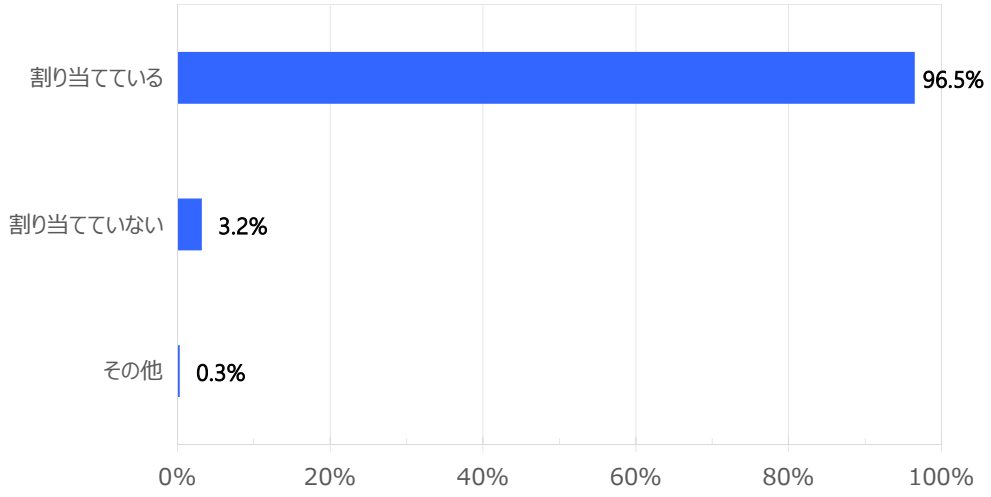
設問２－２．【単一回答】
自組織に関係する安全基準等を把握していますか。

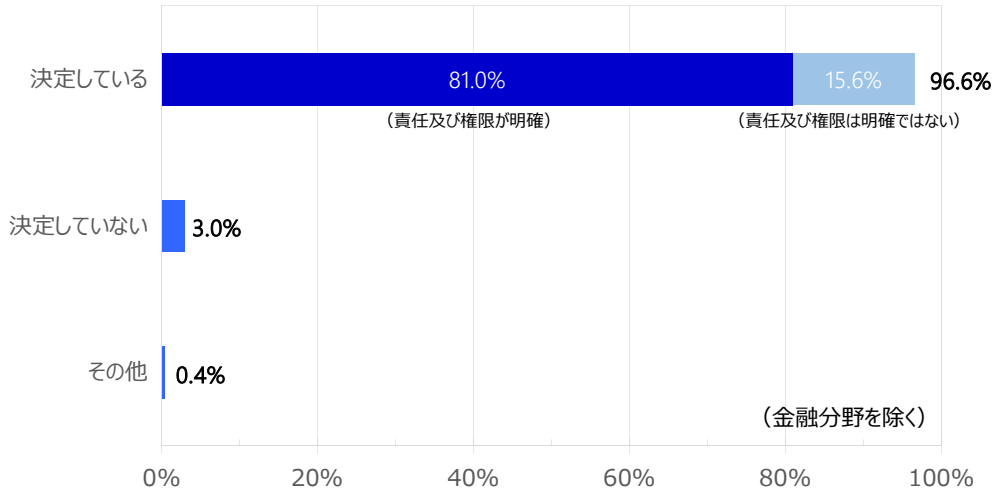


設問２－３．【複数回答】
情報セキュリティに係る方針の策定に当たって参考としているものを全て選択してください。

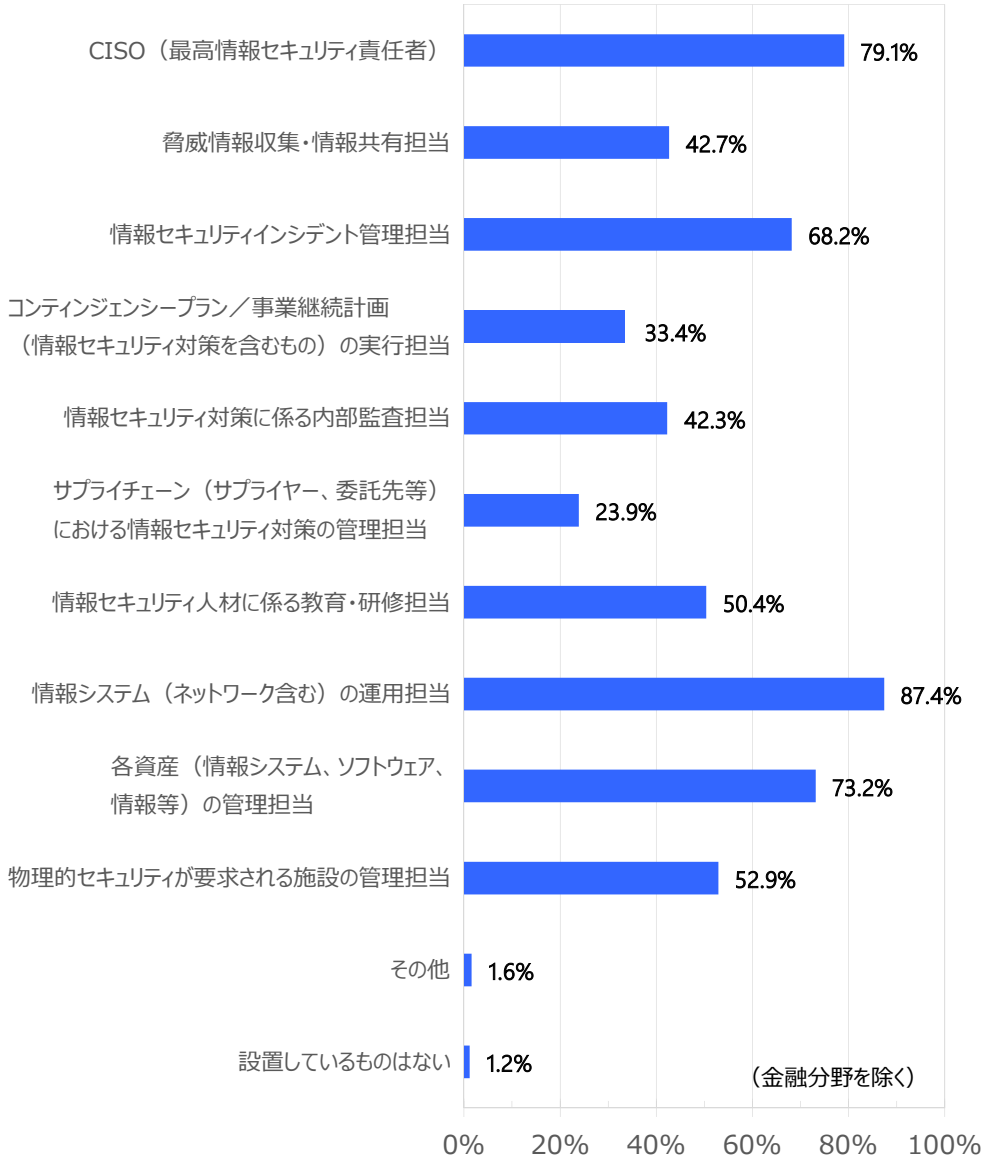


設問２－４．【単一回答】
自組織の情報セキュリティ対策を担当する部署及び従業員を決定するとともに、それらに対して責任及び権限を割り当てていますか。



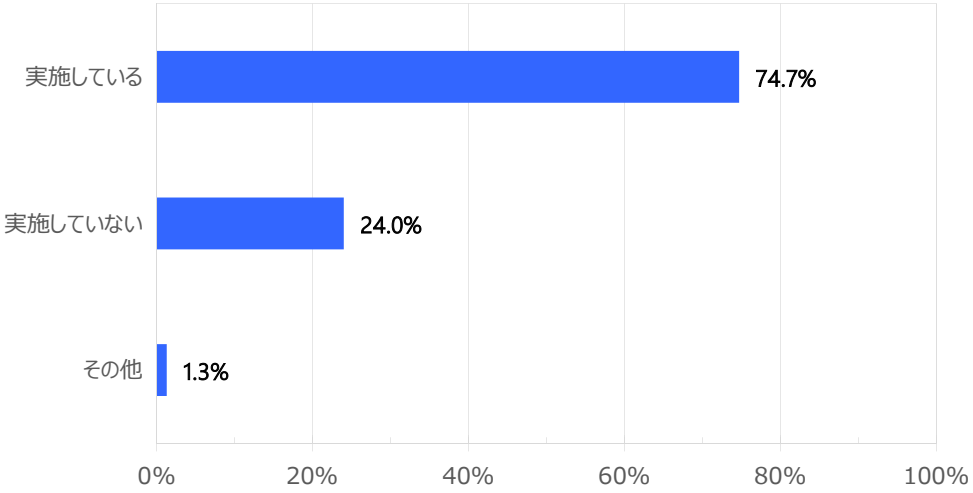


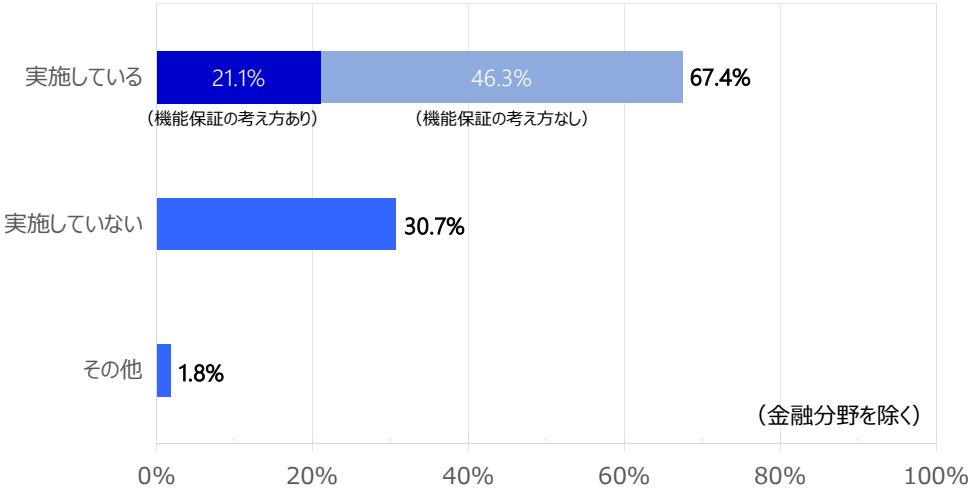
設問２－５．【複数回答】
自組織で設置しているものを全て選択ください。



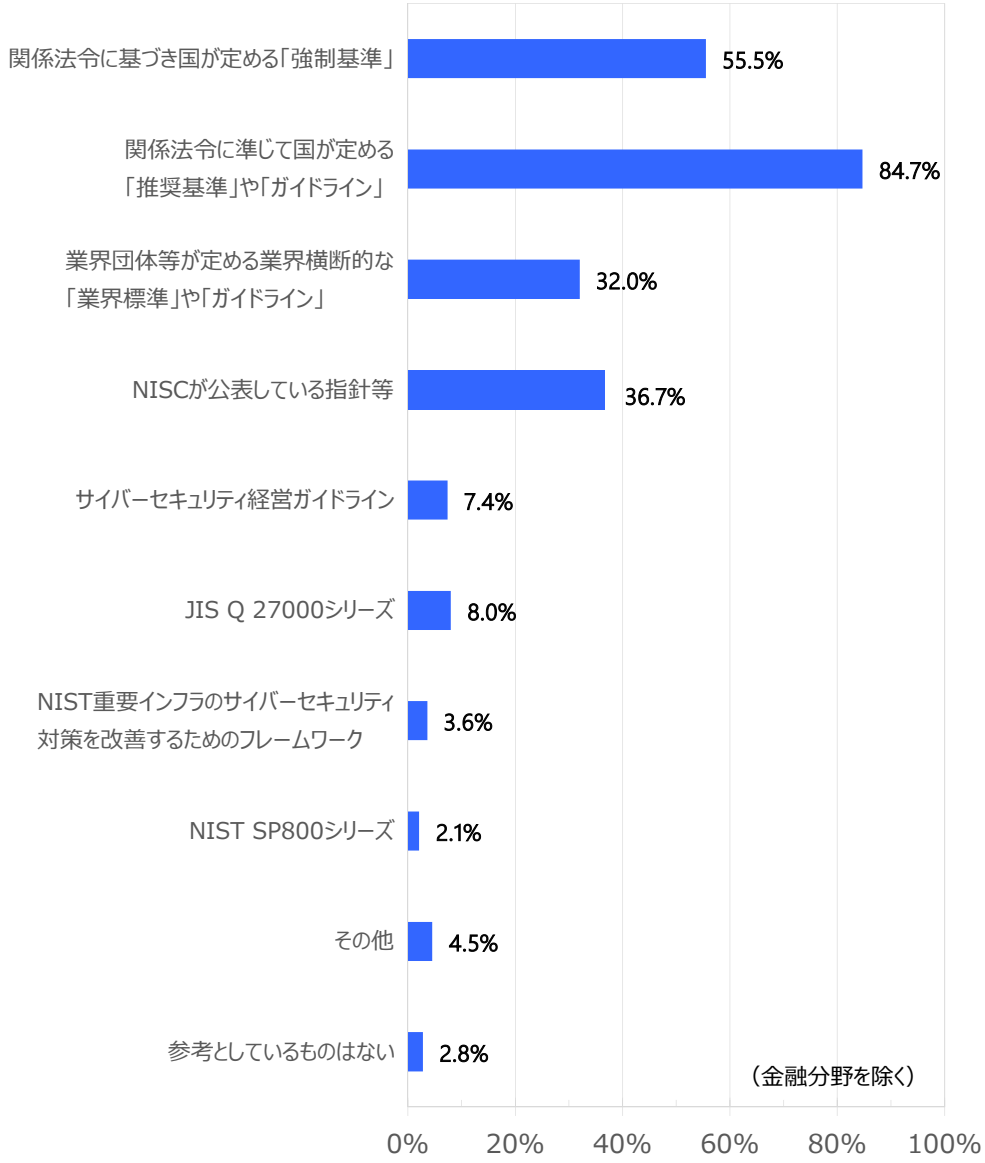
アンケート調査結果　－　Plan［計画］（4/8）

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、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。



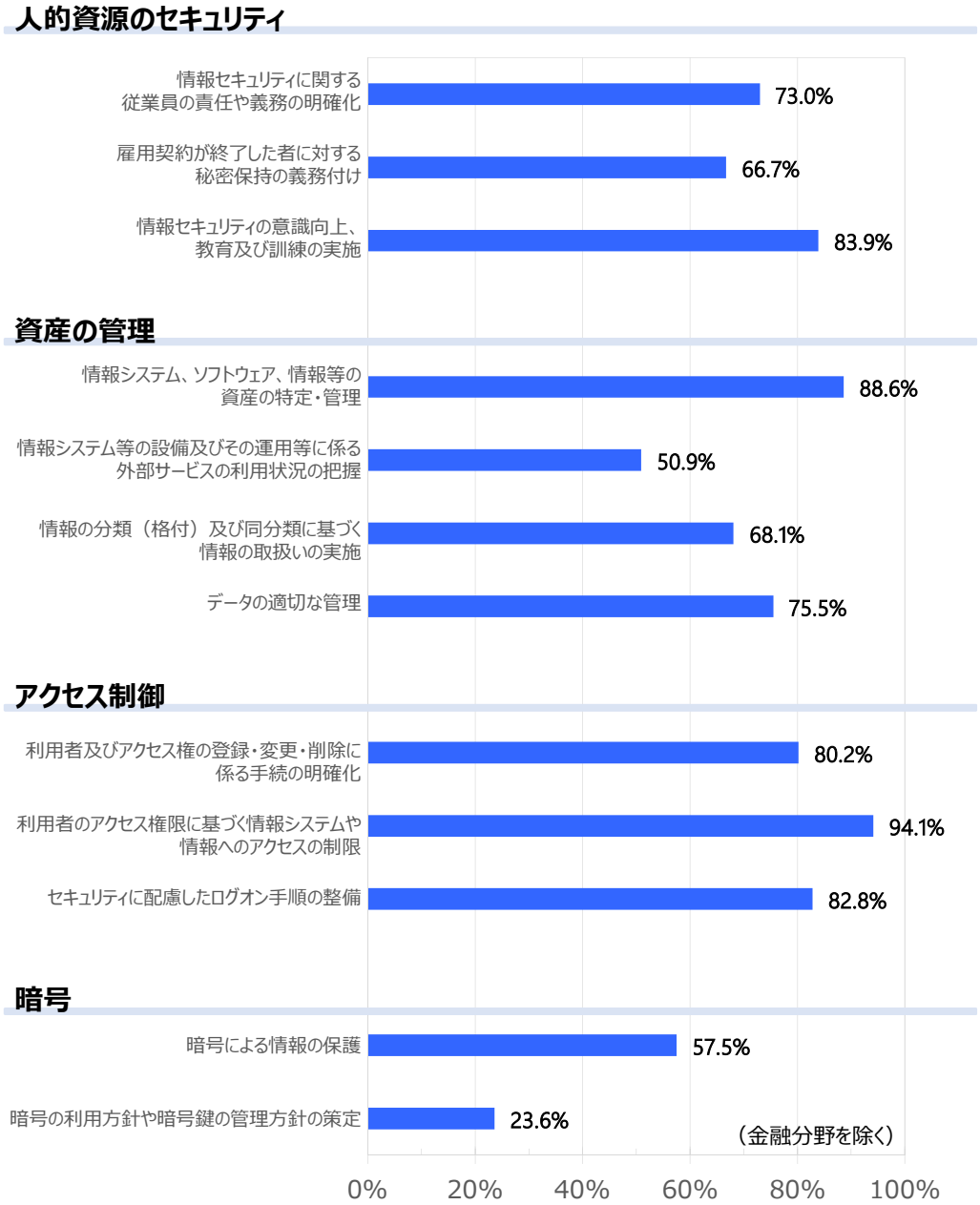


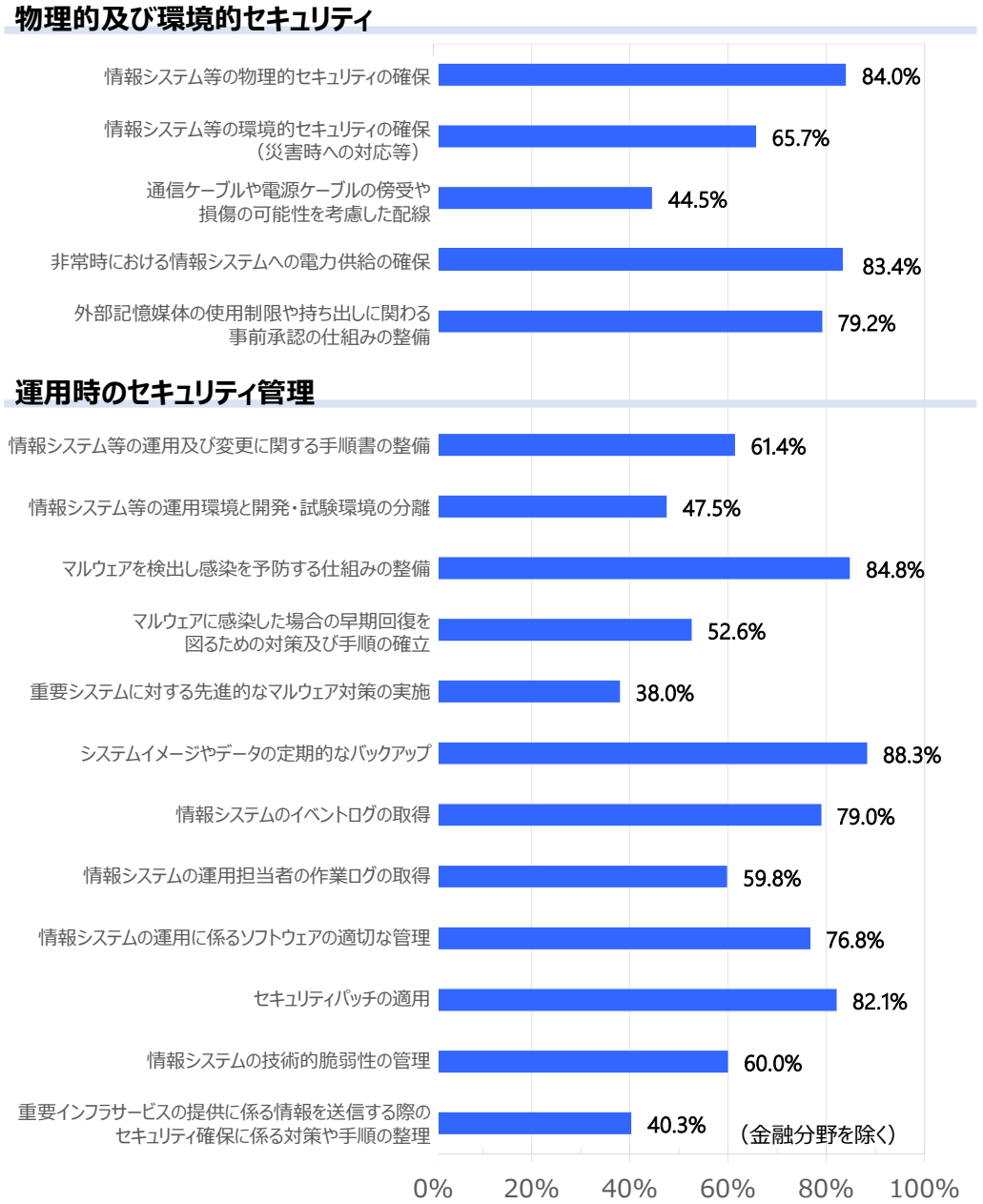
設問３－２．【複数回答】
情報セキュリティ対策の実施に当たって、参考としているものを全て選択してください。



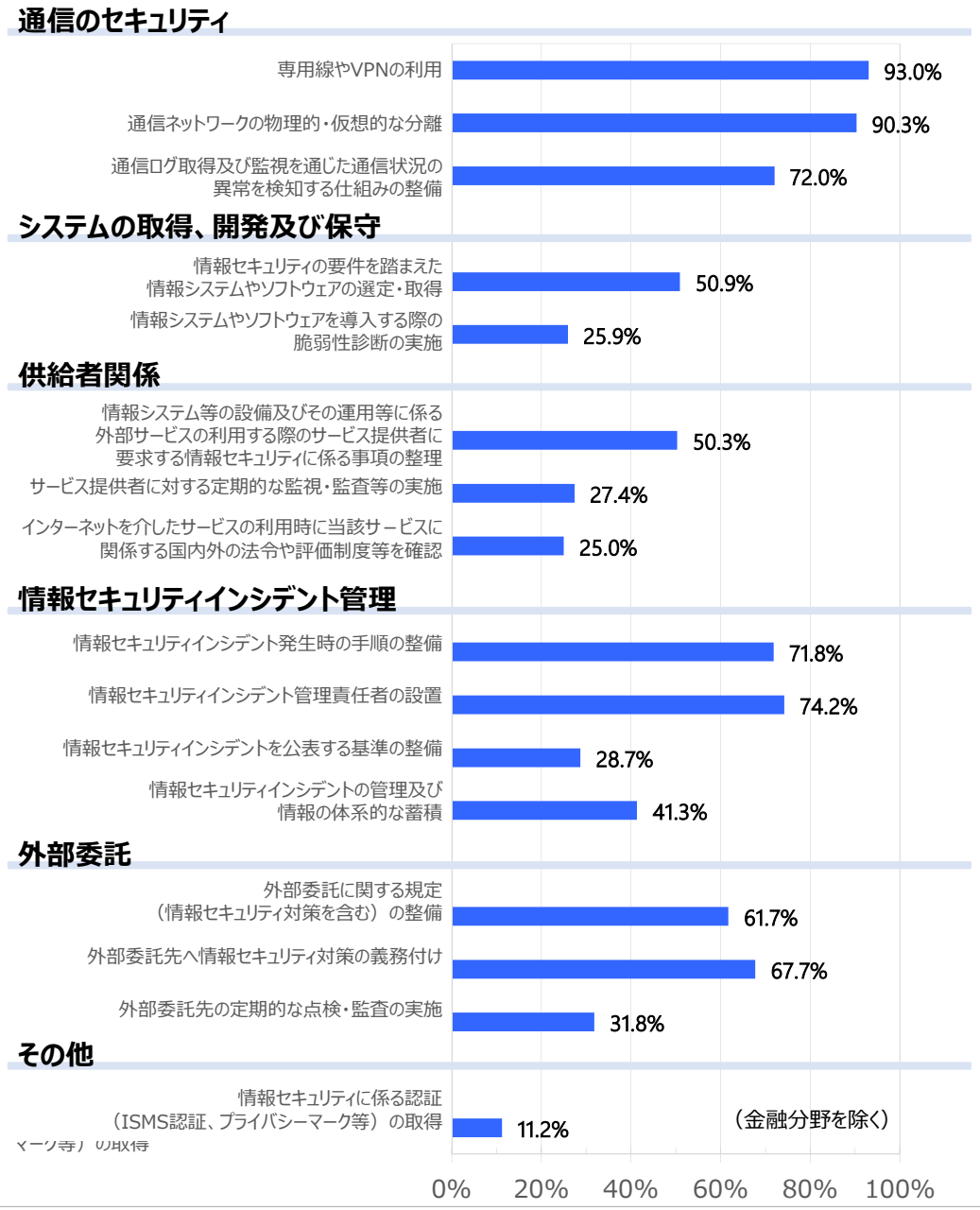
アンケート調査結果　－　Plan［計画］（5/8）

設問３－３．【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。

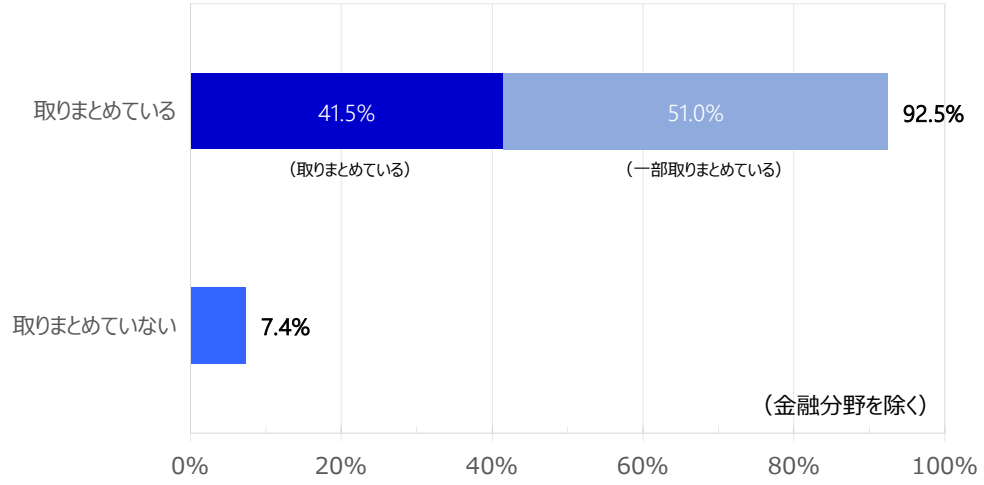




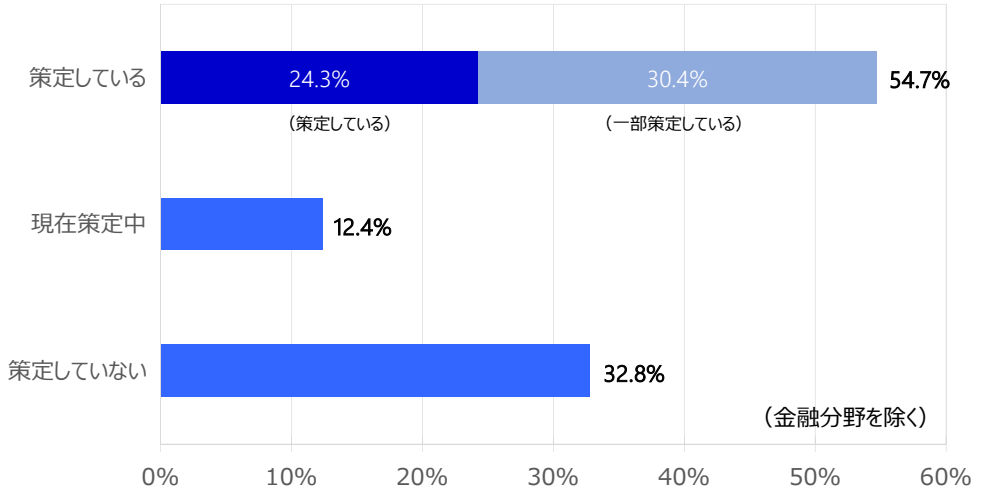
設問３－３．【複数回答】
自組織で実施している情報セキュリティ対策を全て選択してください。（続き）



設問３－４．【単一回答】
設問３－３で実施しているとした情報セキュリティ対策を文書として体系的に取りまとめていますか。

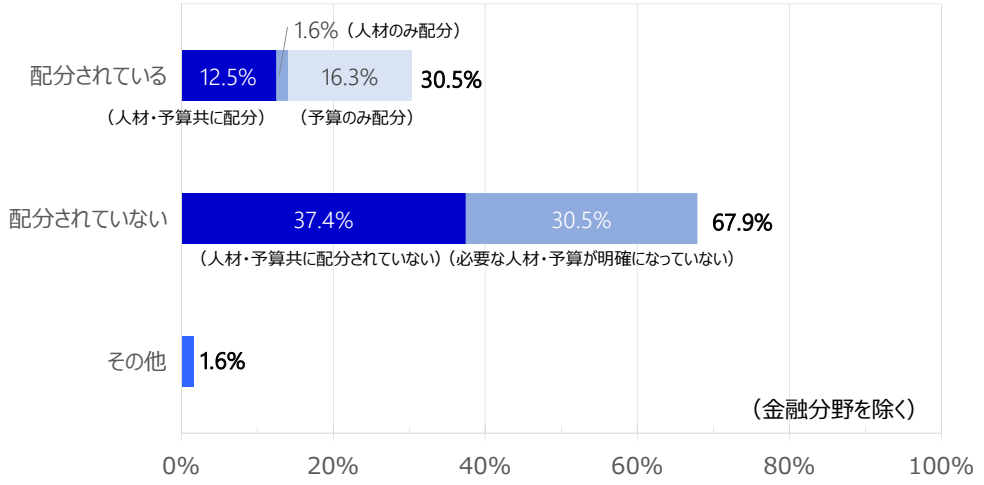


設問３－５．【単一回答】
情報セキュリティ対策の導入や実施に向けた計画（目標・達成度・スケジュール等）を策定していますか。

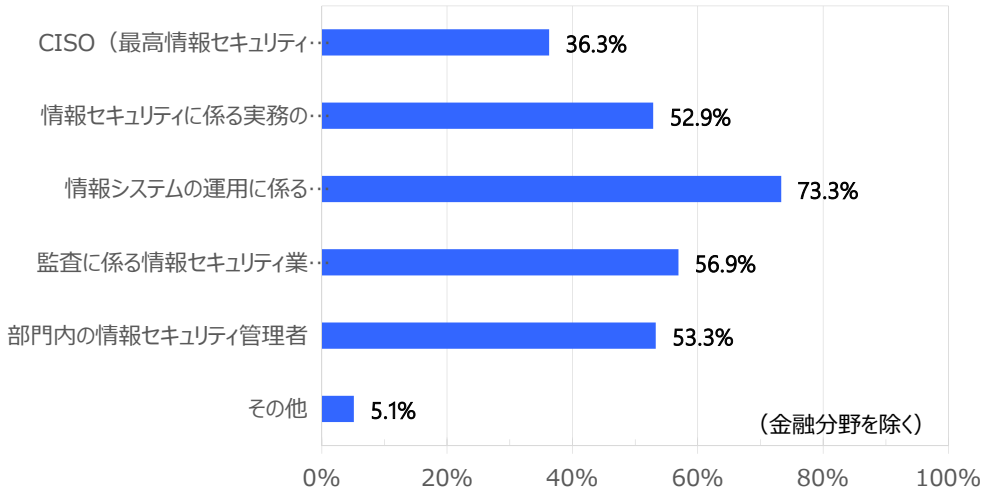


アンケート調査結果　－　Plan［計画］（7/8）

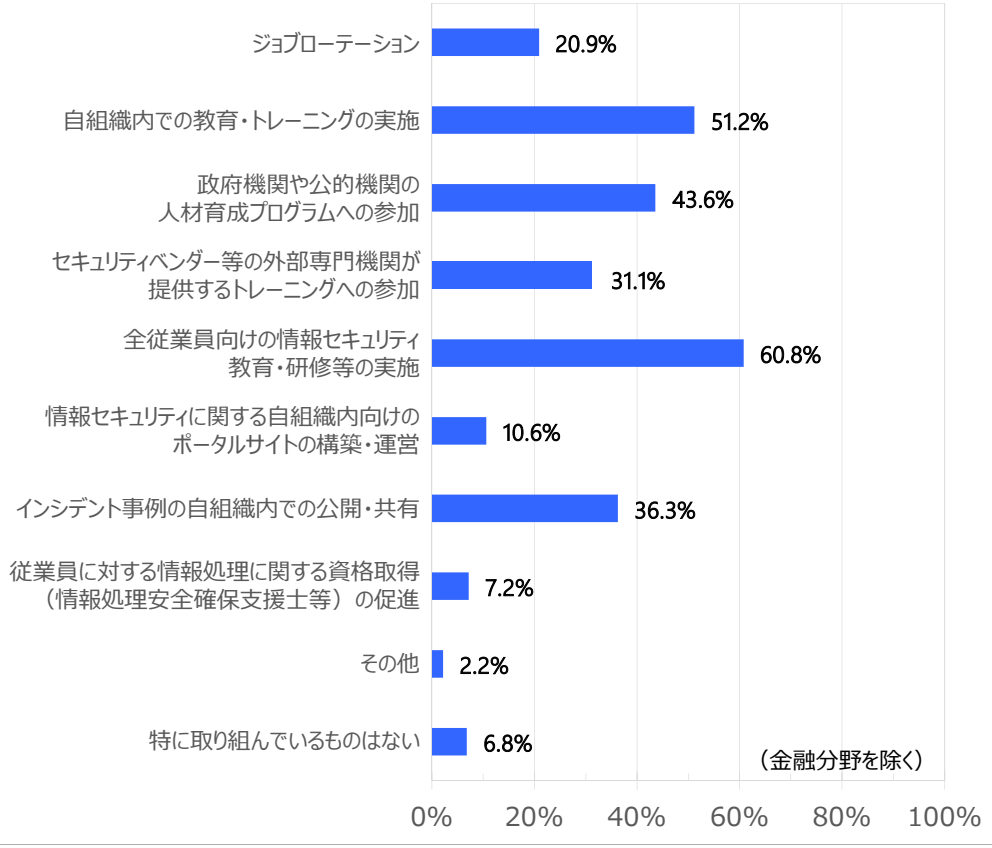
設問４－１．【単一回答】
情報セキュリティ対策の実施に必要となる人材や予算が明確化され、組織内に適切に配分されていますか。



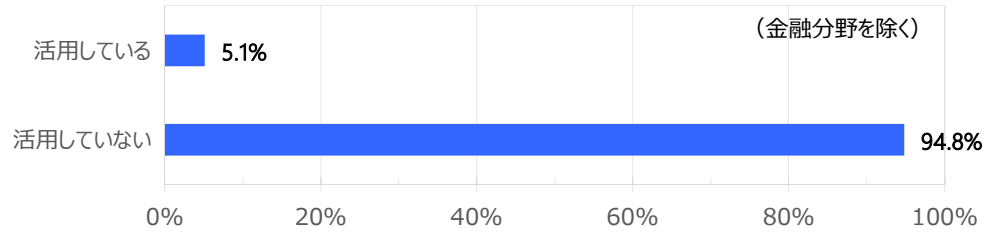
設問４－２．【複数回答】
自組織において、必要としている情報セキュリティ人材を全て選択してください。



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。

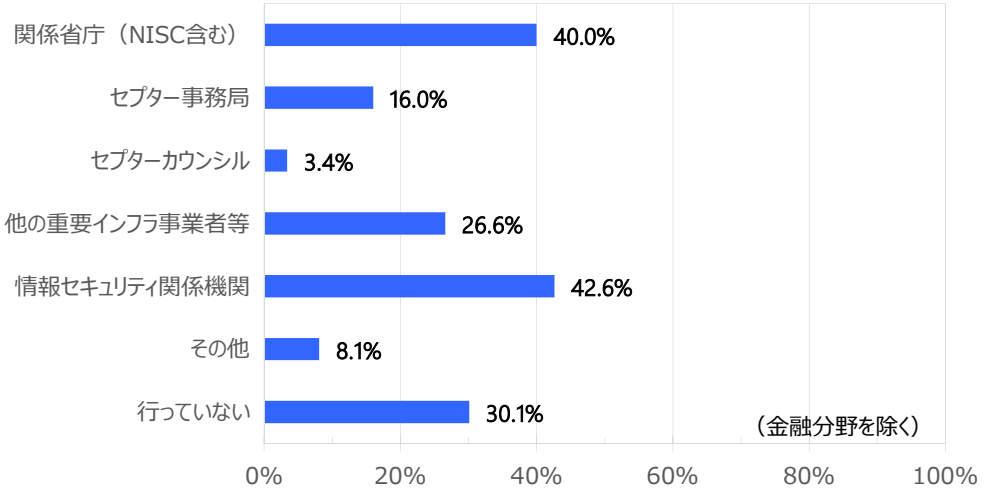


設問４－４．【単一回答】
自組織において、情報処理安全確保支援士を活用していますか。

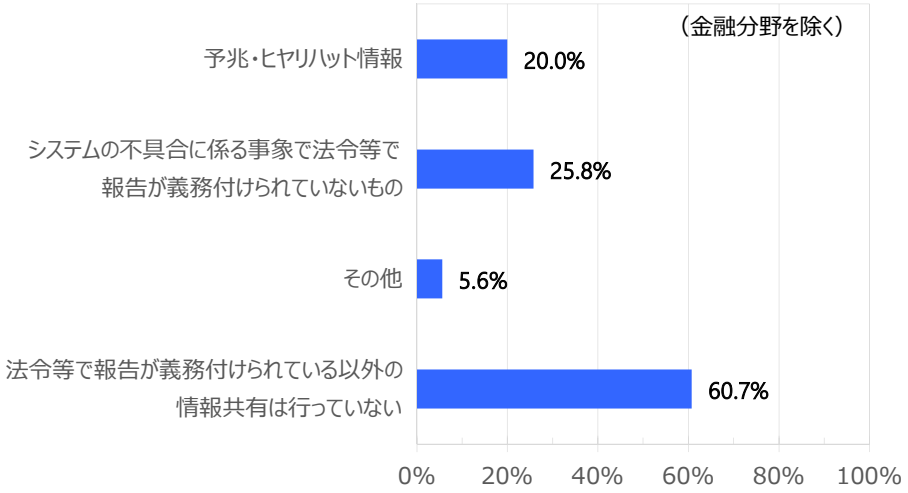


アンケート調査結果　－　Plan［計画］（8/8）

設問４－５．【複数回答】
自組織が所属する重要インフラ分野全体で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。

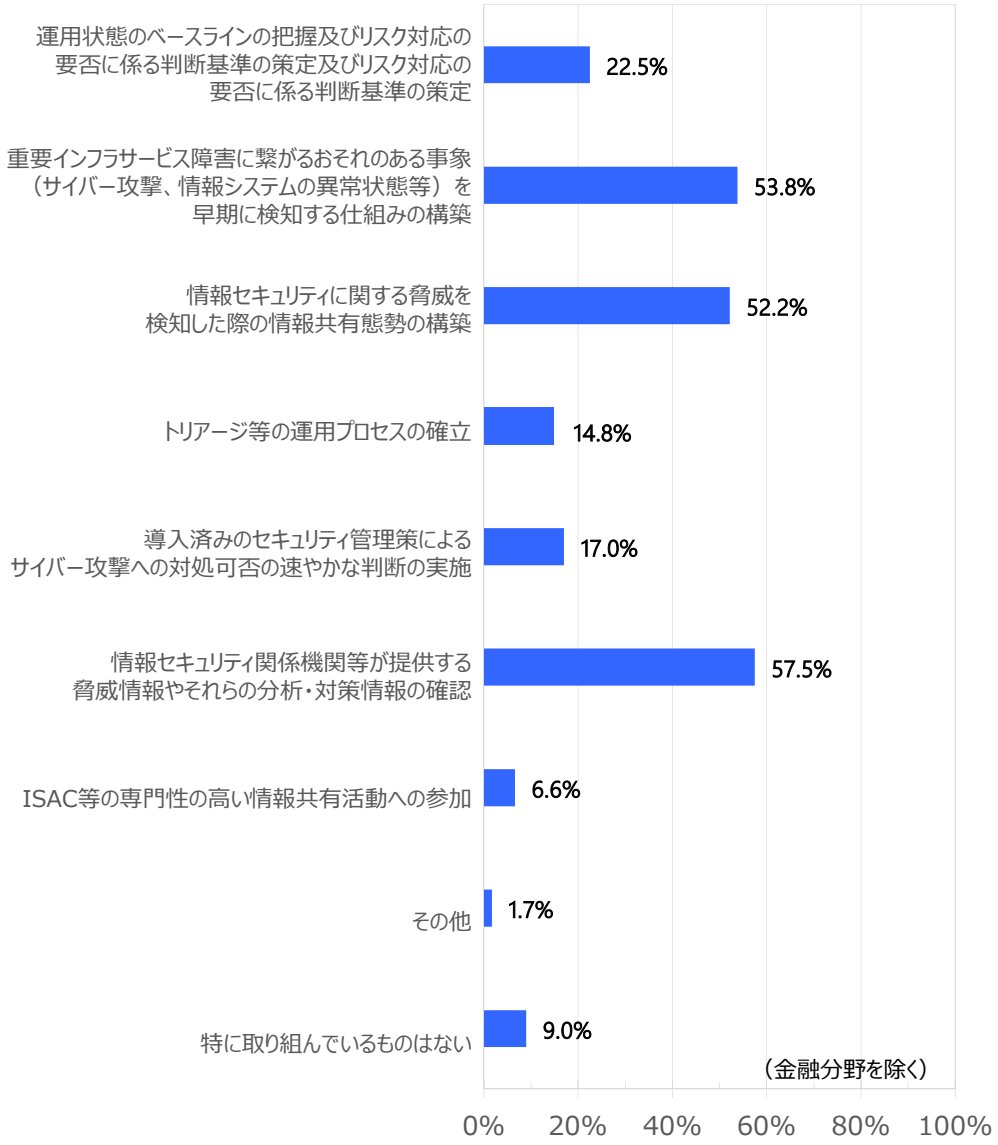


設問４－６．【複数回答】
自組織における重要インフラ所管省庁とのシステムの不具合に関する情報共有の対象範囲を全て選択してください。

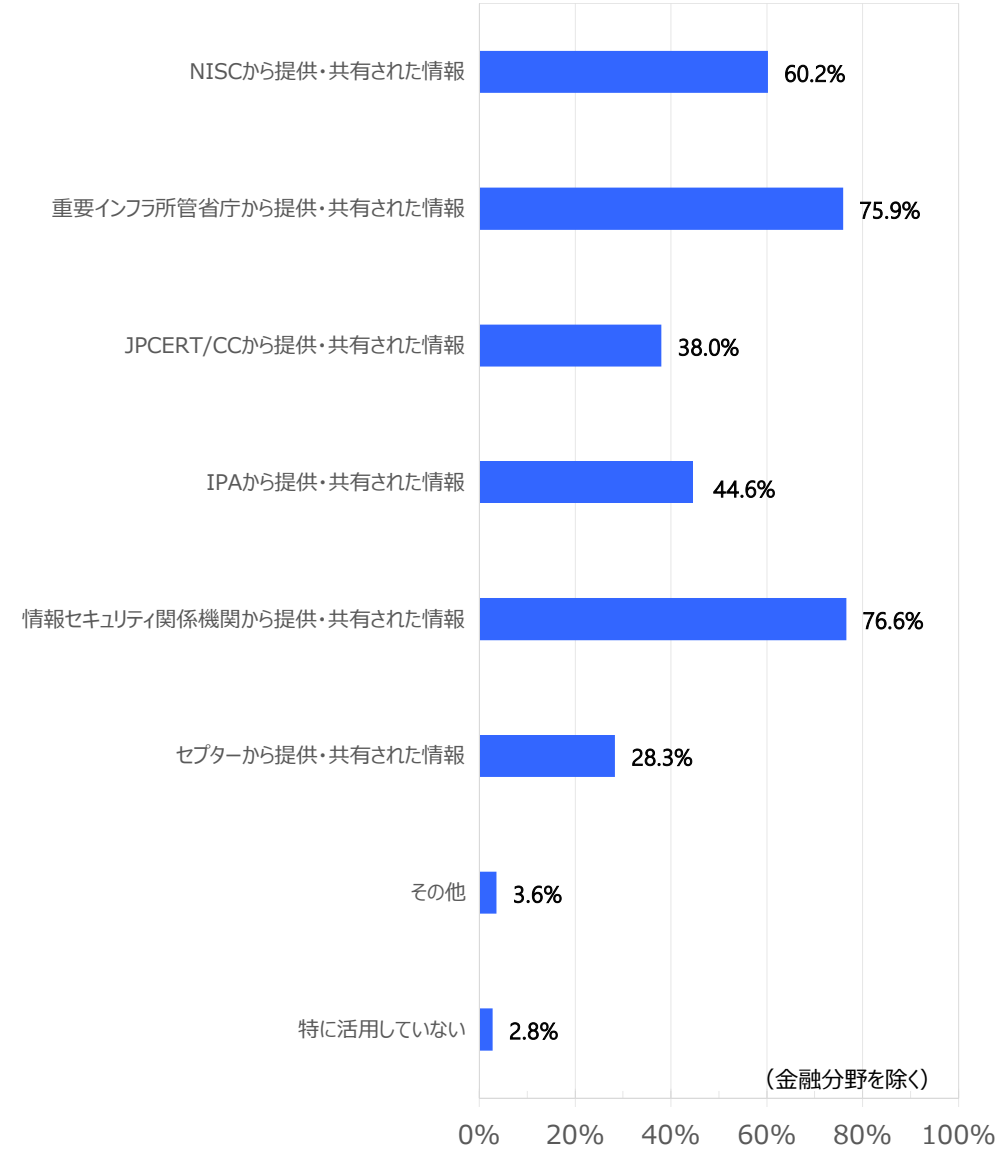


アンケート調査結果　－　Do［実行］（1/3）

設問５－１．【複数回答】
情報セキュリティ対策の導入・運用段階において取り組んでいるものを全て選択してください。

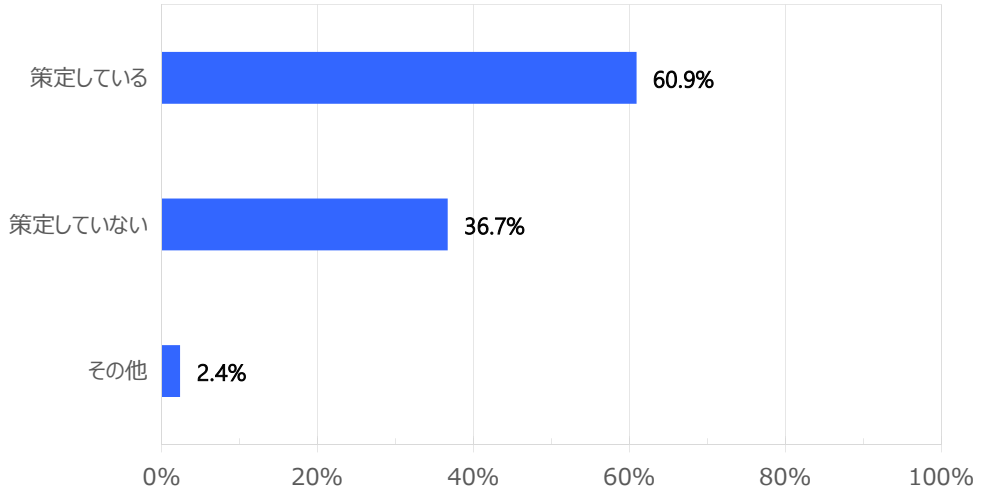


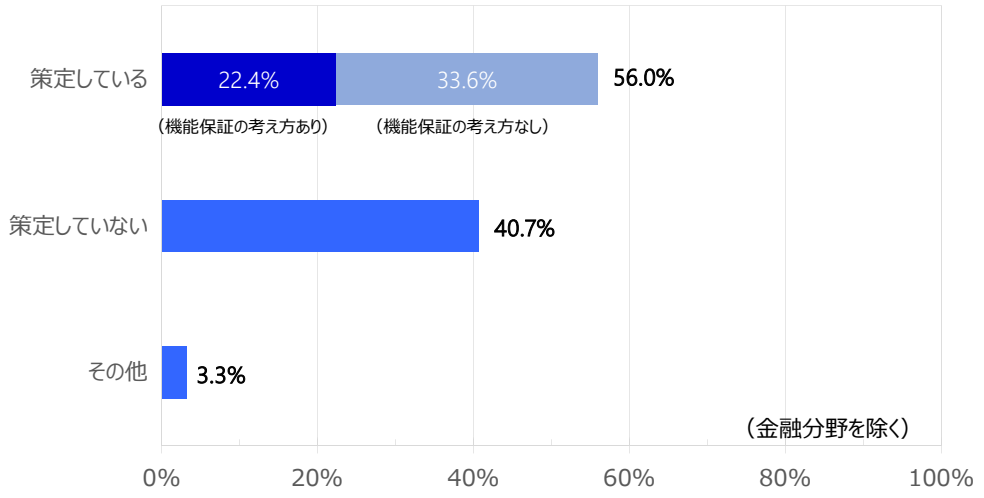
設問５－２．【複数回答】
外部機関から共有・提供された情報について、自組織で活用しているものを全て選択してください。



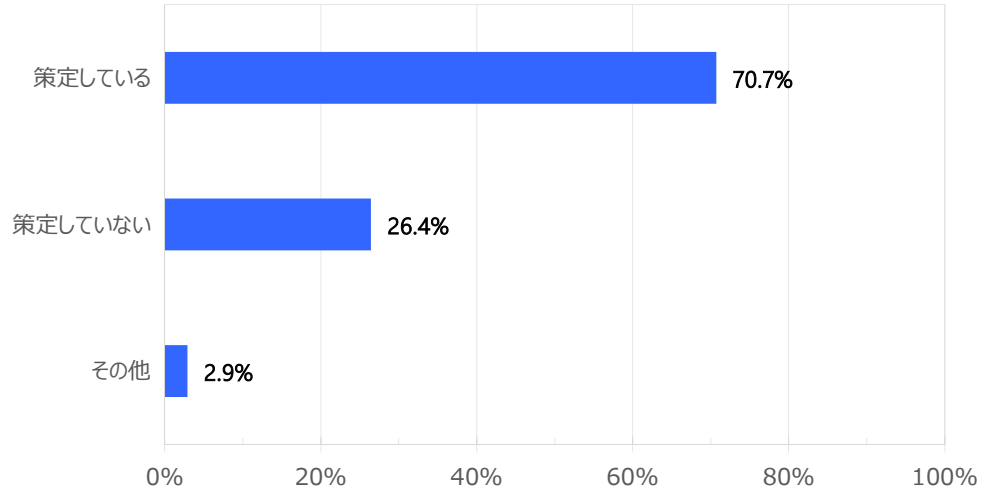
アンケート調査結果　－　Do［実行］（2/3）

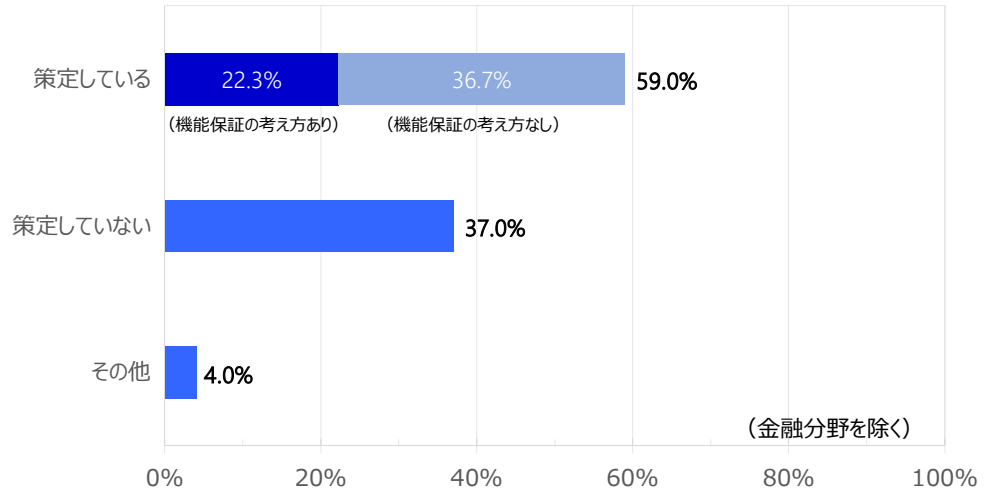
設問５－３．【単一回答】
重要インフラサービス障害の発生に備えたコンティンジェンシープランを策定していますか。また、機能保証の考え方を取り入れていますか。





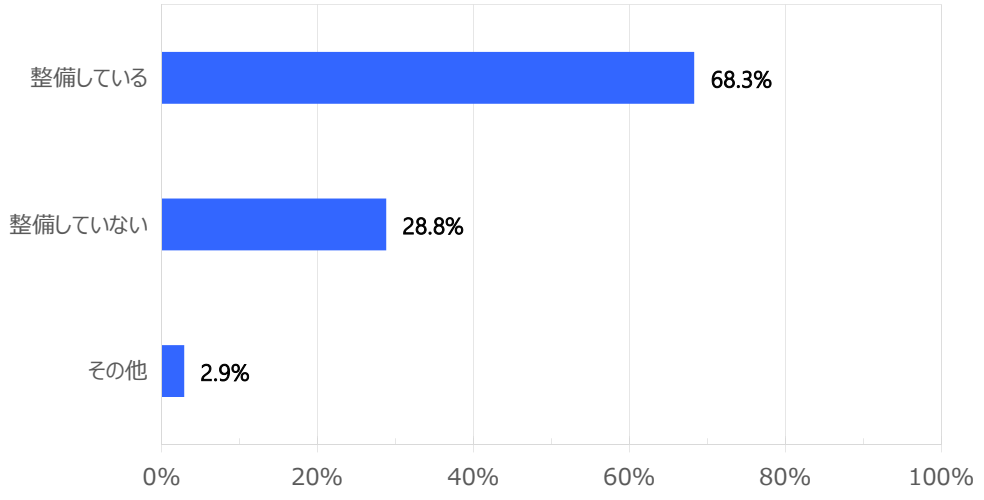
設問５－４．【単一回答】
重要インフラサービス障害の発生に備えた事業継続計画を策定していますか。また、機能保証の考え方を取り入れていますか。



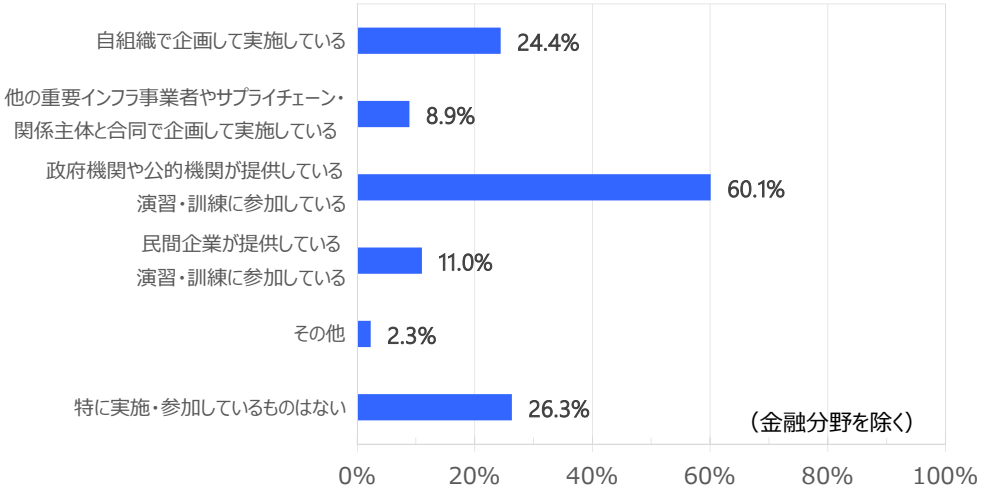


アンケート調査結果　－　Do［実行］（3/3）

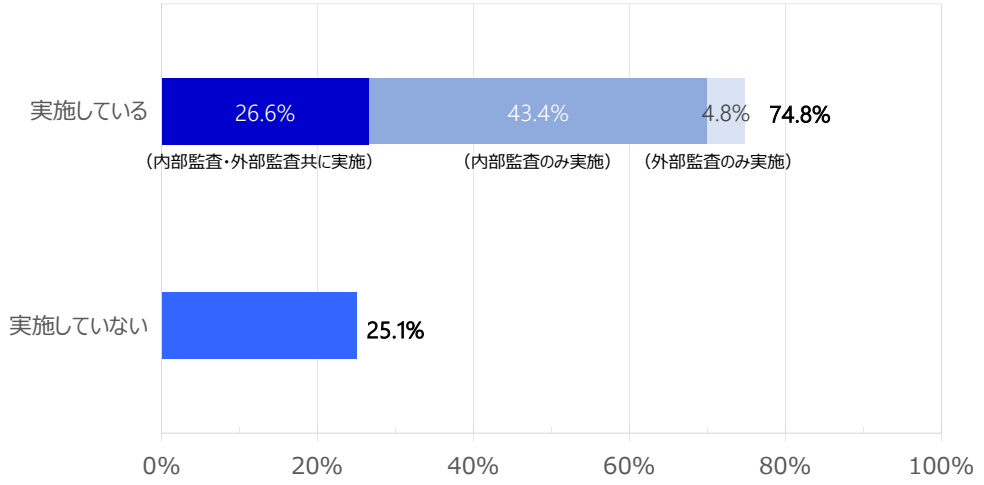
設問５－５．【単一回答】
自組織にCSIRT（又は同等機能を持つ組織）を整備していますか。



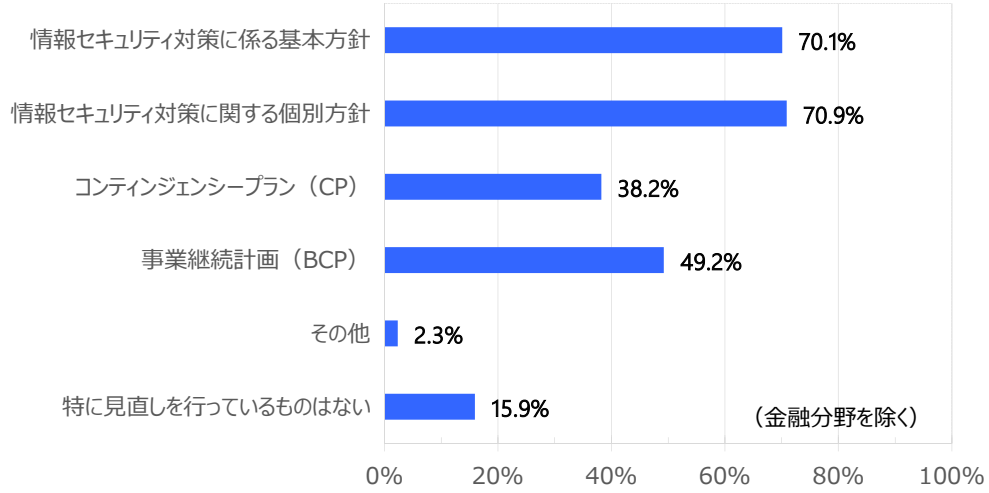
設問５－６．【複数回答】
情報セキュリティ対策に関する演習・訓練について実施・参加しているものを全て選択してください。



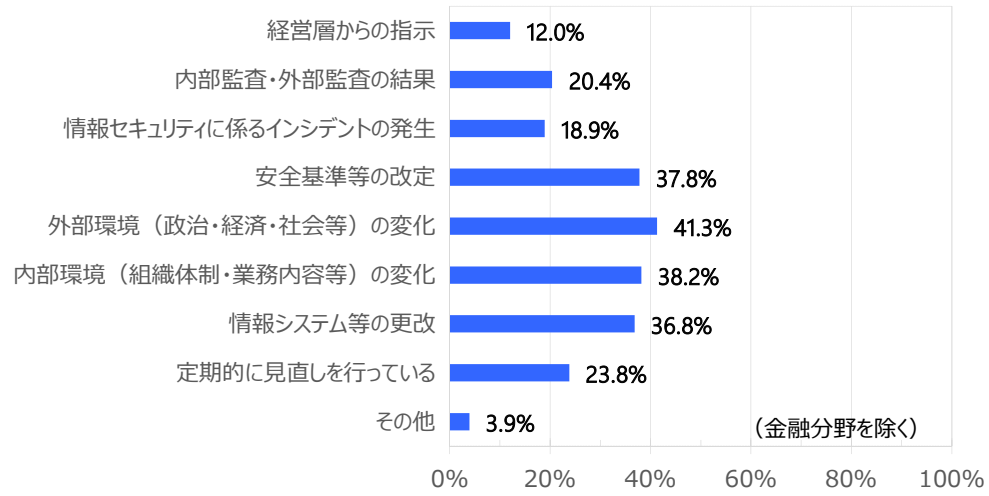
設問６－１．【単一回答】
自組織の情報セキュリティ対策に係る目標の達成状況・計画の進捗状況について、監査を実施していますか。



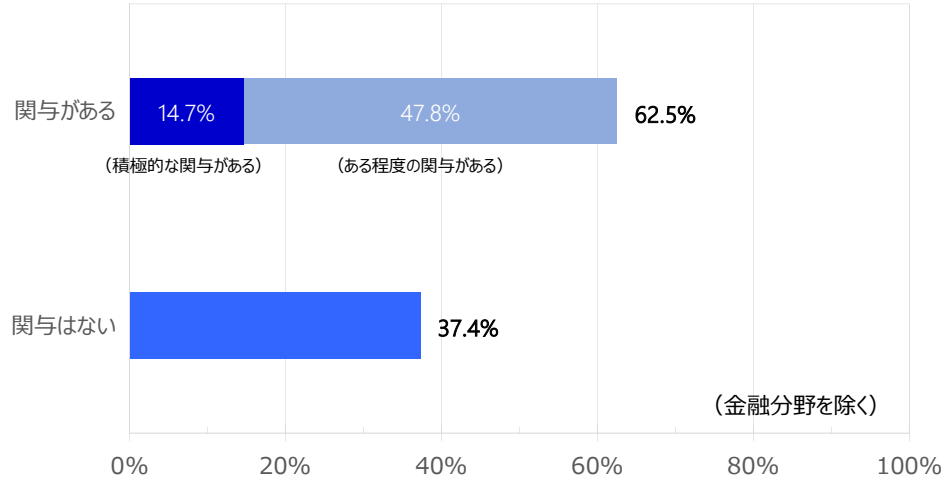
設問７－１．【複数回答】
情報セキュリティ対策の改善に向け、継続的に見直しを行っているものを全て選択してください。



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の対処にあたり、経営層の積極的な関与がありますか。



設問８－２．【複数回答】
経営層の関与のうち、該当するものを以下より選択ください。