2020 年度 サイバーセキュリティ経営ガイドライン
実践のためのプラクティスの在り方に関する調査

－ 調査報告書 －

2021年3月26日

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

エグゼクティブサマリー

背景と調査概要

経済産業省と独立行政法人情報処理推進機構（以下「IPA」と略記する）が、2017 年に共同で発行したサイバーセキュリティ経営ガイドライン Ver2.0 では、経営者がサイバーセキュリティ対策を実施する上での責任者となる担当幹部に対して指示すべき重要 10 項目が示されている。IPA では、企業がこのガイドラインにある内容を実践する上で参考となる情報、取組事例、取り組む際の考え方、ヒントその他を記載したサイバーセキュリティ経営ガイドライン Ver 2.0 実践のためのプラクティス集（以下「プラクティス集」と略記する）を、2019 年より一般に公表している。

プラクティス集は、公表から 10,000 以上の企業ユーザーがダウンロードするなど一定の評価を得ているが、更なる改善のためにはプラクティス利用の実態を把握する必要がある。

上記の背景を踏まえ、プラクティス集の利用実態を把握するとともに、今後の内容の見直しや、作成・共有のプロセスを含めたプラクティス集自体の在り方の検討を目的に、企業におけるプラクティス集の利活用の実態やプラクティスに求める要望等の調査を実施した。

調査結果

本調査を通じて、企業のサイバーセキュリティ推進における課題とともに、プラクティス集の利用実態やニーズ、またそれらを踏まえたプラクティス集の望ましい在り方が明らかとなった。

（文献調査）

文献調査では、国内外のサイバーセキュリティや IT に関する事例集を 5 文献、国内のダイバーシティ経営に関する事例集を 1 文献対象として調査した。調査の結果、作成目的の設定から主題の検討、内容の作成に至るまで、多様な考え方を背景に、様々な手法が採られていることがわかった。また、構成・内容面においても、読者による利用場面を想定して様々な工夫が講じられていた。調査を通じ、プラクティス集の在り方に関し、主に以下のような示唆が得られた。

- プラクティス集作成の目的を達成するためには、想定される企業像に適した事例を提供することが重要
- 主題の選定においては、品質の担保のため、専門家の知見や、企業における実際の取組みや悩み等を盛り込むことが重要
- 作成においては、発行主体が有識者や企業から情報を収集して編集する方法が一般的ではあるが、企業ニーズに対応した質の高いコンテンツを機動的に提供する観点から、企業のメンバーやセキュリティ専門家がより深く作成に関与することも考えられる

- 記載方法に関しては、リスト形式で対策の具体的な実施方法を列挙する方法や、架空の会社での取組みをストーリーとして紹介する形式等、利用場面や目的に応じて様々な在り方が考えられる

（アンケート調査）

文献調査の結果も踏まえ、プラクティス集について、「認知」「利用」「内容」「作成・共有」の観点から、企業における利用実態やニーズ、またその背景となるサイバーセキュリティへの取組みの実態・課題をアンケート調査にて確認した。

アンケート調査の結果、プラクティス集の利用のきっかけや利用目的として、「自社でインシデントが発生した際」や「DX・テレワーク等の環境変化や新たな IT 投資を行った際」等、企業を取り巻く環境に何らかの変化が生じた場面で利用される実態が把握できた。また、プラクティスの提供媒体や全体構成については、「検索性の高い Web 形式での提供」、「自社の状況や課題に応じて参照すべきプラクティスがわかる工夫」が、プラクティス個別の構成・内容については、「プラクティスの優先順位がわかる工夫」「実現に向けたコストの提示」等のニーズが高いことがわかった。プラクティスの作成・共有については、自社においてプラクティスの元となるサイバーセキュリティ対策はある程度進んでいるものの、対策内容を文書化して企業（グループ）内で共有するレベルにまでは至っていない企業が多いことが把握できた。また、サプライチェーン対策や演習・訓練といったテーマは、対策そのものがあまり進んでいない実態も明らかとなった。なお、プラクティスを企業間で共有する取組みや、プラクティスを共同で作成する取組みについて、情報共有や人材育成のメリットから、その必要性を認識する企業が多いことがわかった。

これらの結果を踏まえ、IT 依存度（事業・サービスの継続において、IT がどの程度重要であるかの指標）の観点から企業を 3 つのカテゴリーに分類し、サイバーセキュリティ推進における課題やプラクティス集へのニーズの傾向を整理した。

- 各カテゴリーに共通する課題及びプラクティスに対するニーズ
  - ✓ 管理体制の強化や経営層への報告に課題を有している（管理体制の強化に向けた検討や経営層への報告にプラクティスが活用される）
  - ✓ 組織全体の方針の策定やリソース（予算・人材等）の確保に課題を要している（組織全体の方針の策定やリソース確保に関するプラクティスを充実してほしい）
  - ✓ サイバーセキュリティに関する様々な対策について、実施する優先順位や順番を知りたい（プラクティスの優先順位や実施する順番を知りたい）
  - ✓ 自社の状況・課題に応じたプラクティスの利用方法や、参照すべきプラクティスの解説を充実してほしい
  - ✓ 検索性の高い Web コンテンツとしてプラクティスを提供してほしい
  - ✓ 1 年に 1 回程度の頻度でプラクティスを更新してほしい
  - ✓ プラクティスの実現に必要なコストを提示してほしい

- IT 依存度が低い組織（サイバーセキュリティの取組みが進んでいない組織）の課題及びプラクティスに対するニーズの傾向
  - ✓ サイバーセキュリティ対策全般の「はじめの一歩」を知りたい（「はじめの一歩」としてプラクティスを活用したい）
  - ✓ 経営層や従業員のセキュリティ認識に課題を有している（経営層や従業員のセキュリティ認識を向上させるためのプラクティスを充実してほしい）
  - ✓ サイバーセキュリティが経営課題である理由の解説をしてほしい
  - ✓ プラクティスの記載方法として、実施方法をストーリー形式で紹介する方法よりも、手順をリストとして掲載する方法、または対応のヒントとなる事例（Tips）を掲載する方法を求める

- IT 依存度が中程度の組織（サイバーセキュリティの取組みがある程度進んでいる組織）の課題及びプラクティスに対するニーズの傾向
  - ✓ 対策が遅れているテーマの「はじめの一歩」を知りたい（対策が遅れているテーマの「はじめの一歩」としてプラクティスを活用したい）
  - ✓ プラクティスの記載方法として、実施方法をストーリー形式で紹介する方法や手順をリストとして掲載する方法を求める

- IT 依存度が高い組織（サイバーセキュリティの取組みが進んでいる組織）の課題及びプラクティスに対するニーズの傾向
  - ✓ IT やセキュリティに関連する新たな取組みに際しての管理体制強化に課題を有している（DX 等の新たな取組みに際してプラクティスを活用したい）
  - ✓ リソース（予算・人材等）の確保に課題を要している（リソースの確保に関するプラクティスを充実してほしい）
  - ✓ 自社の状況や課題に応じたプラクティスを求める傾向が強い
  - ✓ プラクティスの記載方法として、実施方法をストーリー形式で紹介する方法や手順をリストとして掲載する方法を求める
  - ✓ 自社におけるプラクティスの蓄積が図られている

（有識者調査・企業調査）

また、サイバーセキュリティ経営の豊富な知見を有する国内の有識者、および、プラクティスの想定ユーザーである国内企業のセキュリティ部門等の役職員から、企業におけるサイバーセキュリティの課題や、現在のプラクティス集の課題、およびプラクティス集の今後の在り方等に関する意見をヒアリングするため、インタビュー調査を実施した。

インタビュー調査により、企業におけるプラクティス集の想定される利用場面やニーズ、またそれを踏まえたプラクティス集の認知・利用促進方法、構成・内容面での改善の方向性、および、今後の作成・共有の在り方まで、様々な見解が得られた。

- 想定される利用場面を踏まえた認知の在り方
  - ✓ プラクティスを認知し活用するための動機付けとして、インシデントの事例を掲載する等、対策が必要な理由が伝わるような工夫が必要
  - ✓ 業界団体を通じた周知や Web コンテンツ化による利便性の向上が必要

- ニーズを踏まえた構成・内容の在り方
  - ✓ 企業は自社の課題に応じたプラクティスを求めているため、業種やシチュエーション、企業規模ごとの事例が充実化するとより活用しやすい
  - ✓ 自社が参照すべきプラクティスがわからないといった課題が想定されるため、セキュリティ成熟度等と組み合わせて参照すべきプラクティスがわかるような工夫が必要
  - ✓ テレワーク・クラウド利用・DX 等最近のトレンドとなっているテーマについても一定程度内容の議論・標準化が進んだ段階でテーマとして取扱うことが必要
  - ✓ 対策が不十分な企業を念頭に教材的な位置づけとする場合、「利用方法の解説」や「成熟度に応じたプラクティスの提示」「絵柄を多用して視覚に訴える」等の工夫が有効
  - ✓ 他方で、既に対策が一定程度進んでおり、特定の課題認識を有する企業を念頭にした場合は、プラクティスや事例(Tips)そのものの拡充を図る必要

- 企業の実態を踏まえた作成・共有の在り方
  - ✓ サイバーセキュリティ対策が進んでいる企業では、プラクティスの素材となる知見の蓄積が進んでいる
  - ✓ プラクティスを共同で検討する在り方については、様々な情報や考え方・バックグラウンドを有するメンバーが集まり知見を活かすことで、プラクティスの充実化につながるとともに、参加する人材のモチベーション向上につながる
  - ✓ プラクティスを共同で検討する在り方については、企業の立場から必要性が理解できる一方で、検討リソースをどのように確保するかが課題
  - ✓ 社内のプラクティスを外部に提供することには一定のリスクが存在するため、情報共有のためのルールの構築や、情報の選別・加工・抽象化等の対応が必要

以上の調査結果を踏まえ、プラクティス集の今後の在り方として、以下の 3 つの方向性に整理した。

Ⅰ．企業の課題に応じてプラクティスが参照できる Web コンテンツとしての提供

調査において、企業は「自社の状況・課題に応じた内容のプラクティスを参照したい」「自社の状況・課題から参照すべきプラクティスがわかるようにしてほしい」というニーズを強く有していることがわかった。このニーズに対応するプラクティス集の在り方として、「サイバーセキュリティ経営ガイドライン実践状況の可視化ツール[1]（以下、可視化ツール）」との連携が考えられる。可視化ツールとは、サイバーセキュリティ経営ガイドラインの実践状況を、企業が自己診断できるツールである。この可視化ツールとプラクティス集が連携することで、企業がプラクティス集の参照にあたり、「まずは可視化ツールで自社の対策状況や弱点を把握し、それに対応したプラクティスをプラクティス集で確認する」といった利用方法が想定される。なお、プラクティス集の提供媒体に関して、検索性の高い Web コンテンツでの提供が望まれている点も踏まえ、この利用方法を効果的に実現するためにはプラクティス集ならびに可視化ツールを Web コンテンツとして提供し、相互のコンテンツ間をシームレスに移動・参照できるような工夫が必要となる。

またこの対応により、Web コンテンツの参照ログから、可視化ツールの診断結果と各プラクティスの参照傾向の関係性や、アンケート機能の実装によるニーズの把握等が可能となり、更なる構成・内容の改善に生かすことが可能となる。

Ⅱ．企業ニーズを踏まえた各プラクティスの構成・内容の拡充

各プラクティスの構成・内容の拡充についても、企業のニーズを踏まえ、様々な企業の状況や課題に対応してプラクティスを充実化していくことが求められる。但し、各テーマに対応するプラクティスを、業種や規模その他の組み合わせに応じて全てのパターンを作成・提供することは困難である。そのため、各テーマに関するスタンダードな内容をベースのプラクティスとして提示し、業種や規模その他に応じた補足情報や読み替えの事例等をアドオンの情報として掲載する方法が考えられる。なお、この情報の充実化においては、「サイバーセキュリティ対策のための資源（予算・人材等）の確保」等のニーズの高いテーマや、「インシデントによる被害に備えた復旧体制の整備」等の業種や規模等に特化したプラクティスが求められるテーマを優先する。

また、プラクティスの構成要素として、高いニーズが確認できた「プラクティス実現に向けたコスト（効果）」や「プラクティスの実施体制（役割・スキル）」、「関連するインシデントの事例」等の情報を現行のプラクティスをベースに追補・補強することが求められる。この対応については、比較的テーマ選定や記載内容の観点から自由度の高い現行の第 3 章（セキュリティ担当者の悩みと取組に関するプラクティス）をベースに、構成・内容の拡充を先行し、その過程で蓄積した知見・情報を踏まえて、現行の第 2 章（「サイバーセキュリティ

[1] IPA,https://www.ipa.go.jp/security/economics/checktool/index.html

経営ガイドライン Ver2.0」の「重要 10 項目」に関するプラクティス）の拡充を行う方向性が想定される。

Ⅲ．企業間でのプラクティスの作成・共有

現在、プラクティス集は、その作成において、企業のニーズ調査やインタビューを通じたプラクティスの収集、有識者の査閲等を実施し、実用性と品質を確保している。一方で、こうした作成の方法では、企業のニーズを機動的にとらえ、随時見直し・公表を図るという点で課題があると言える。

今後、企業の関心の高いテーマについて、質の高いプラクティスを機動的に作成・提供するための手法や体制の検討が求められる。調査では、サイバーセキュリティの取組みが進んでいる企業を中心に、プラクティスの元となるサイバーセキュリティ対策の推進・文書化を進めている実態が確認できた。こうした、企業に蓄積するノウハウや、また現場の課題認識をくみ取りプラクティスに反映していく方法として、例えば、プラクティスの作成に、企業の有志を募り、IPA と共同でプラクティスを作成するといった方法が考えられる。また、企業間で、プラクティスを共同で検討・作成し共有するような枠組みを IPA が主体となって運営するといった方法も考えられる。調査でも、情報共有や人材育成等のメリットから、多くの企業でそのような枠組みの必要性・有用性が理解されていることがわかった。一方で、このような共同検討には、企業のリソース面の課題や、内部情報を外部に共有する際のルール設定の必要性等、課題・乗り越えるべきハードルも確認できた。

今後、こうした方向性も視野にいれ、プラクティスの構成・内容の検討と並行し、作成・共有の在り方についても検討を進めていく。

目次

別冊資料

アンケート調査結果 単純集計

1 はじめに

1.1 調査背景・目的

経済産業省と独立行政法人情報処理推進機構（本報告書では、以下「IPA」と略記する）が、2017 年に共同で発行したサイバーセキュリティ経営ガイドライン Ver2.0 では、経営者がサイバーセキュリティ対策を実施する上での責任者となる担当幹部に対して指示すべき重要 10 項目が示されている。企業がこのガイドラインにある内容を実践する上で、より具体的なガイドブック等を求める意見が聞こえたことから、IPA では 2019 年 3 月にサイバーセキュリティ経営ガイドライン Ver 2.0 実践のためのプラクティス集（本報告書では、以下「プラクティス集」と略記する）第 1 版を、2020 年 6 月には内容を大きく刷新した第 2 版を発行した。（ここで、プラクティスとは、企業ユーザーがサイバーセキュリティの実践に取り組む際に参考となる情報、具体的には企業の取組事例、取り組む際の考え方、ヒントその他を言う。）

プラクティス集は、第 1 版の発行から 10,000 以上の企業ユーザーがダウンロードするなど一定の評価を得ているが、更なる改善のためにはプラクティス利用の実態を把握する必要がある。具体的には、記載したプラクティスが企業ユーザーのニーズに合致しているのか、プラクティスの素材の収集や作成の方式、記述の粒度が適切であるのかなど、企業が使いやすいプラクティスの在り方を明確にする必要がある。

上記の背景を踏まえ、プラクティス集の利用実態を把握するとともに、今後の内容の見直しや、作成・共有のプロセスを含めたプラクティス集自体の在り方の検討を目的に、企業におけるプラクティス集の利活用の実態やプラクティスに求める要望等の調査を実施した。

1.2 本調査の実施概要・本報告書の構成

本調査では、プラクティス集の利用実態の把握や、今後の在り方の検討を目途に、文献調査、アンケート調査、有識者・企業インタビュー調査を実施した。

本報告書の構成は、本章を含め 7 章構成である。各章の関係性を以下に記載する。文献調査を通じて構築したプラクティス集の認知、利活用、作成・共有に関する仮説に対して、アンケート調査やインタビュー調査を通じて検証を行った。その結果を踏まえ、今後のプラクティス集の在り方について検討を実施した。

- 第 2 章：類似のプラクティスに関する文献調査
  国内外の類似のプラクティスを対象に、1. 作成の目的、2. 主題の設定、3. 素材の収集、4. 作成、5. 実情把握による査閲、6. 公開等による共有、7. 読者の利用、の 7 つの観点に基づいて文献調査を実施した。
- 第 3 章：アンケート調査
  「文献調査」の結果を踏まえ、プラクティス集の利活用の実態を把握するために、企業を対象としたアンケート調査を実施した。

- 第 4 章：有識者インタビュー調査
  プラクティスの在り方に関する意見や、現在のプラクティスの課題を収集するため、プラクティスに知見を有する者を対象にインタビュー調査を実施した。
- 第 5 章：企業インタビュー調査
  プラクティスの在り方に関する意見や、現在のプラクティスの課題を収集するため、プラクティスの想定利用者である企業を対象としてインタビュー調査を実施した。
- 第 6 章：調査結果のまとめ
  「文献調査」、「アンケート調査」、「有識者・企業インタビュー調査」の結果から、プラクティス集の利用実態や、プラクティス集の課題についての示唆をとりまとめた。
- 第 7 章：データ集
  参考資料として、文献調査の結果およびアンケート調査の集計結果を記載した。

2　類似のプラクティスに関する文献調査

2.1 調査概要

IPA は、2020 年 6 月に「サイバーセキュリティ経営ガイドライン Ver 2.0 実践のためのプラクティス集　第 2 版」（以下、プラクティス集）を公表しているが、発行機関によるプラクティス集の作成から公開、さらに読者によるプラクティス集の利用までのプロセス（図 1）は、①主題の選定、②素材の収集、③作成、④実状把握による査閲、⑤公開等による共有、⑥読者による利用というステップに分解することができる。本文献調査では、現状のプラクティス集の各ステップの実態・その特徴と、プラクティス集と類似した文献（事例集）との比較分析を実施し、プラクティス集の改善点について明らかにした。調査対象とした 6 つの文献を表 2-1 に記載する。

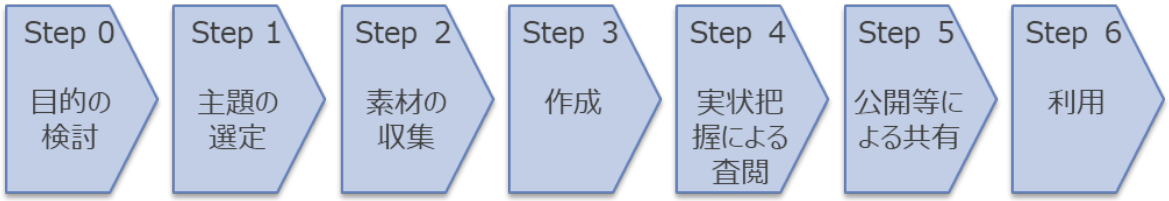


図 1　プラクティスの作成から利用に至るまでのプロセス

表 2-1　調査文献一覧

文献番号	文献名	発行機関
文献 1	CIS Controls　V7.1	CIS（米国非営利団体）
文献 2	ITIL4	AXELOS(英国内閣府による合弁会社)
文献 3	Auto-ISAC Governance Best Practice Guide	Auto-ISAC（米国自動車業界の情報共有組織）
文献 4	ENISA Good Practices for Security of IoT in the context of Smart Manufacturing	ENISA（欧州ネットワーク・情報セキュリティ機関）
文献 5	METI ユーザー企業におけるセキュリティ人材・体制の確保に関するプラクティス集	METI
文献 6	METI　新・ダイバーシティ経営ベストプラクティス	METI

2.2 調査結果

2.2.1 Step1：目的の検討

本ステップの文献調査における調査観点として、文献の目的（作成の目的や、プラクティス集の必要性）と想定読者を定義して、各文献の調査を行った。なお、現状のプラクティス集は、目的を「ファーストステップとなる事例の提供」と明確に定めているため、取り上げた事例と合致した課題を抱えている読者に対しては有効的である。その一方で、想定読者となる「今後サイバーセキュリティやインシデント対策を実施する層(初心者)」以外の読者のニーズを捉えることが課題と考えられる。

文献調査の結果（表 2-2)、各文献の目的と想定読者は表裏一体の関係であることが確認できた。その観点では、現状のプラクティス集においても、目的と想定読者に大きなズレはない。想定読者を現状の初心者から拡大し、幅広いニーズに対応することを目指す場合は、文献 1 のように、想定読者の組織を網羅的にグループ分けした上で、それぞれのグループにおける事例を提供していくことが、読者によるプラクティス集の分かりやすさ・使いやすさの観点から有効と考えられる。

表 2-2　Step1：目的の検討の調査結果

文献	調査観点	
	文献の目的	想定読者
プラクティス集	・企業がサイバーセキュリティ経営ガイドラインの内容を実践する際の考え方、ヒントを提供 ・ファーストステップとなり得る事例を提供	・情報セキュリティの取組はある程度進めてきたが、サイバーセキュリティ対策やインシデント対応について何から始めるべきかと考えている読者
文献 1	・様々なセキュリティ対策における、「膨大な選択肢による混沌（Fog of More)」を解決すること ・現在発生している、および今後の発生が予測されるサイバー攻撃に対する具体的な対策を提供	・サイバーセキュリティ対策に取り組む組織の担当者 ・想定読者の組織をサイバーセキュリティに関するリソースと経験の観点で三段階に分類している ①リソースと経験が限定的な組織 ②適度なリソースと経験を有する組織 ③十分なリソースと経験を有する組織
文献 2	・ITIL の IT サービスマネジメントの手法に関するガイダンスを提供し、個人・組織がそれを導入することを支援すること（リファレンスガイドとなること）	・学生から経験豊富な専門家までの幅広い読者

文献	調査観点	
	文献の目的	想定読者
文献 3	・自動車業界に向けてセキュリティリスクをもたらす可能性のあるサイバー脅威に対処する方法を提供すること	・自動車業界のメーカー、サプライヤー、商用車会社（フリート、運送業者など）のセキュリティ担当者
文献 4	・産業界における IIoT に関するセキュリティを確保すること	・インダストリー4.0 およびスマートマニュファクチャリング組織等の IIoT 機器およびソリューションを採用または採用する予定の組織とそのセキュリティ担当者
文献 5	・人材・体制の確保の面からセキュリティ対応力を高めるための情報を提供すること	・様々な規模・業種・成熟度のユーザー企業の経営者 ・自社のセキュリティポリシー及び体制などの企画担当者
文献 6	・ダイバーシティ経営に取り組む企業のすそ野拡大	・ダイバーシティ経営を推進する担当者や企業経営者

2.2.2 Step2：主題の選定

本ステップの文献調査における調査観点として、主題の選定の際に準拠する枠組みやその他に重視する視点と業種や業務への特化の有無を定義して、各文献の調査を行った。なお、現状のプラクティス集は、我が国の企業が広く参照する公的なガイドライン（サイバーセキュリティ経営ガイドライン）に準拠しており、主題選定の合理性を担保している。また、企業等へのインタビューを通じて収集した企業のサイバーセキュリティに関する悩みや取組みを記載しているため、事例のリアリティを確保できている。一方で、サイバーセキュリティ経営ガイドラインの指示項目ごとにプラクティスのファーストステップを 2 つに絞り込むことに加え、幅広い業種・業務を対象としている反面、特定の業種や業務に特徴的な課題を対象とすることができていない。

文献調査の結果（表 2-3）、文献 2 を除く調査対象のすべての文献が、政府機関や標準化団体等によって作成された枠組みや標準等に準拠した上で作成されており、その骨組みに対して、セキュリティの専門家の知見やグッドプラクティスとして取り上げるべき実際の企業の先進的な取組みやその悩みを盛り込んでいることが明らかになった。また、自動車や製造業に特化した文献も確認されたが、その他の文献では特定の業種や業務に主題は限定されていなかった。

表 2-3　Step2：主題の選定

文献	調査観点		
	準拠する枠組み	左記以外に重視する視点	業種や業務への特化
プラクティス集	・サイバーセキュリティ経営ガイドラインの指示項目	・セキュリティに関する、企業の実際の悩みや取組み	（特定の業種や業務へ特化していない）
文献 1	・米国政府や NIST のセキュリティ要件	・キュリティ対策の実務を担う専門家の知見	（特定の業種や業務へ特化していない）
文献 2	（準拠しているものは確認できないが、本文献自体が IT サービスマネジメント業界のスタンダードとして世界中で認知されている）	・セキュリティの専門家の知見	（特定の業種や業務へ特化していない）
文献 3	・NIST、ISO、その他の組織によって作成された標準およびフレームワーク	・リスクベースのアプローチでプラクティスを整理	・自動車業界（自動車メーカー等）に特化
文献 4	・ENISA「Baseline SecurityRecommendations for IoT（IoT のベースラインセキュリティ に関する提言）」	・セキュリティの専門家の知見	・IIoT を使用する産業界（製造業のスマートマニュファクチャリング等）
文献 5	・サイバーセキュリティ経営ガイドライン（人材と体制に特化）	・セキュリティに関する、企業の実際の悩みや取組み	（特定の業種や業務へ特化していない）
文献 6	・ダイバーシティ 2.0 行動ガイドライン	（公知情報では確認できない）	（特定の業種や業務へ特化していない）

2.2.3 Step3：素材の収集

本ステップの文献調査における調査観点として、記載する情報の素材を収集する際の、収集主体と頻度、収集方法を定義して、各文献の調査を行った。なお、現状のプラクティス集については、IPA およびその委託先事業者が、プラクティス集を改定するタイミング（1-2 年に一度）ごとに、有識者や先進的なセキュリティ対策を進めている企業の協力のもと、ヒアリングを通じて実際の取組みや課題を緻密に収集している。その一方で、ヒアリングによる素材収集の負担を軽減することと、プラクティス集の情報の鮮度を保つことが課題である。

文献調査の結果（表 2-4)、収集主体や頻度は、IPA の取組みとほぼ同様であることが明らかになった。また、収集方法についても IPA の取組みと同様に、有識者や企業へのヒアリングが主なアプローチとなっているが、文献 1 や文献 6 のような、企業が自組織の取組みをベストプラクティスとして推薦し、発行主体に提案する枠組みは、発行主体が事前に収集したい情報を定義する必要はあるものの、効果的・効率的に情報を収集することが可能であると考えられる。特に、文献 6 では、応募企業から先駆的な取組を行っている企業を選定・表彰する仕組みを採用しており、企業による積極的な情報提供を促すことが可能となっている。

表 2-4　Step3：素材の収集

文献	調査観点		
	収集主体	頻度	収集方法
プラクティス集	・IPA(および委託先事業者)	・改定のタイミング(1～2 年に一度)	・有識者や企業へのヒアリングから、実際の取組みや課題を収集
文献 1	・CIS	（公知情報では確認できない）	・企業等へアプローチすることによる情報収集 ・企業等が共同で素材を出し合う枠組み
文献 2	・AXELOS 社	（公知情報では確認できない）	・有識者や企業へのヒアリングから、実際の取組みや課題を収集
文献 3	・Auto-ISAC（Auto-ISAC ベストプラクティス常任委員会）	（公知情報では確認できない）	・自動車メーカー、電装品メーカーなど自動車業界の企業が幅広く参加するベストプラクティスワーキンググループからの情報収集
文献 4	・ENISA	（公知情報では確認できない）	・文献調査 ・有識者や企業へのヒアリングから、実際の取組みや課題を収集
文献 5	・METI(および委託先事業者)	（公知情報では確認できない）	・様々な業種・成熟度の企業におけるセキュリティ人材・組織体制についてヒアリングを実施
文献 6	・METI(および委託先事業者)	・年に一度	・企業からの応募を募集し、書類審査(一次)、プレゼン審査（二次）を経て選定

2.2.4 Step4：作成

本ステップの文献調査における調査観点として、作成主体と作成プロセスを定義して、各文献の調査を行った。なお、現状のプラクティス集は、IPA および IPA の管理の元その委託先事業者が、ヒアリングを通じて情報を収集し、それをとりまとめることで作成されている。Step3：素材の収集と同様に、作成の負担が大きいこととプラクティス集の情報の鮮度の問題に加え、プラクティス集を作成するための知見の蓄積が課題である。

文献調査の結果（表 2-5)、各文献においても、IPA の取組みと同様に、発行主体においてプラクティス集を作成するための担当者が任命され、有識者や企業等が収集した情報を取り纏め、プラクティス集を作成している。また、文献 1 では、セキュリティの専門家からの無償の協力・貢献を活用してプラクティスを作成している事例が確認された。文献 6 のように、作成の際に精査する必要があるが、プラクティス集に掲載することを念頭において所定のフォーマットを作成し、そのフォーマットに各企業が情報を記載するという方式は、限られた作成時間の中で幅広いニーズに対応したプラクティス集を作成するために有効な方法と考えられる。

表 2-5　Step4：作成

文献	調査観点	
	作成主体	作成プロセス
プラクティス集	・IPA(および委託先事業者)	・有識者を招聘し、検討会にて、構成や内容を検討(2018 年) ・有識者や企業へのヒアリングから、実際の取組みや課題を収集し、IPA(および委託先事業者)にて作成(2019 年)
文献 1	・CIS	・作成主体がセキュリティの専門家からの無償の協力・貢献を活用して作成
文献 2	・AXELOS 社	・AXELOS のプロジェクトチームが、IT サービスマネジメントの実務者等の有識者と共に共同で作成
文献 3	・Auto-ISAC のベストプラクティスワーキンググループ	・Auto-ISAC メンバー組織からの 140 人以上の代表者で構成されているベストプラクティスワーキンググループにおける議論を通じて作成
文献 4	・ENISA	・ENISA の専門家が、文献調査とアンケート・インタビュー調査の結果を分析し、プラクティス集の草案を作成
文献 5	・METI(および委託先事業者)	・企業のヒアリング結果を踏まえて METI(および委託先事業者)にて作成
文献 6	・METI(および委託先事業者)	・応募企業が、自社の取組みに関して作成した資料に基づく書類審査（一次)、プレゼン審査（二次）を経て評価を行い、METI(および委託先事業者)にて作成

2.2.5 Step5：実状把握による査閲

本ステップの文献調査における調査観点として、査閲主体と査閲プロセスを定義して、各文献の調査を行った。なお、現状のプラクティス集は、IPA および IPA の管理の元その委託先事業者が主体となって、有識者等に査閲の依頼をし、その意見を踏まえて修正が行われている。このステップにおいても、Step3：素材の収集、Step4：作成と同様に、有識者等からの意見のとりまとめ・プラクティス集への取り込みの負担を軽減するとともに、査閲を通じてプラクティス集の情報鮮度を保つこと課題である。

文献調査の結果（表 2-6)、各文献においても、IPA の取組みと同様に、作成主体以外の組織に属する有識者や企業の実務者が査閲を実施している事例が確認できた。また、査閲の実施方法についても、ワークショップを開催し、その場で査閲を行う事例が確認できた。

表 2-6　Step5：実状把握による査閲

文献	調査観点	
	査閲主体	査閲プロセス
プラクティス集	・有識者	・有識者や企業の実務者にレビューを依頼
文献 1	（公知情報では確認できない）	
文献 2	（公知情報では確認できない）	
文献 3	・Auto-ISAC のベストプラクティスワーキンググループ	・Auto-ISAC メンバー組織からの 140 人以上の代表者で構成されているベストプラクティスワーキンググループにおける議論を通じて査閲
文献 4	・ENISA 以外の専門家	・ENISA 以外の専門家から草案に対する意見を収集し、それをもとに作成した最終版に対して、ワークショップを開催し査閲を実施
文献 5	（公知情報では確認できない）	
文献 6	・METI(および委託先事業者)	・応募企業の情報をもとに、書類審査（一次)、プレゼン審査（二次）を実施

2.2.6 Step6：公開等による共有

本ステップの文献調査における調査観点として、公開方法と公開に伴う費用を定義して、各文献の調査を行った。なお、現状のプラクティス集は、広く企業や国民に向けて、無償でIPA の HP（ホームページ）上に公開をしている（PDF 形式）。

文献調査の結果（表 2-7)、文献 2（有償販売）を除いた調査対象のすべての文献において、IPA の取組みと同様に、作成主体の HP 上において無償で公開している事例が確認できた。これは、文献 2 以外の文献の発行機関は、政府機関（文献 3,、5、6）や非営利団体（文献 1)、情報共有組織（文献 4）であり、広くベストプラクティスを公開することを目的としていることが理由として考えられる。

表 2-7　Step6：公開等による共有

文献	調査観点	
	公開方法	費用
プラクティス集	・IPA の HP にて PDF 形式で公開	・無償
文献 1	・CIS の HP にて PDF 形式で公開 ・各プラクティスの要点をまとめた 2 分程度の動画も公開	・無償
文献 2	・書籍版、PDF 版、APP 版、ebook 版等の複数の形式で販売 ・多言語（英語版、フランス語、ドイツ語、スペイン語、日本語）に対応	・有償（日本円：約 8 千円）
文献 3	・Auto-ISAC の HP にて、ウェブページとして公開 ・下記のように段階的に公開範囲を拡大 ①発行後最初の 3 か月：TLPAmber-Auto-ISAC メンバーのみが利用可能 ②発行後 3～9 か月：TLPGreen-業界の利害関係者への要求によりリリース ③公開から 9 か月後：TLP ホワイト取締役会の確認を条件として、Web サイトを介して一般にリリースされる。	・無償
文献 4	・ENISA の HP にて PDF 形式で公開	・無償
文献 5	・METI の HP にて PDF 形式で公開	・無償
文献 6	・METI の HP にて PDF 形式で公開	・無償

2.2.7 Step7：利用

本ステップの文献調査における調査観点として、文献の「全体構成」（表 2-8）、「プラクティスの構成」（表 2-9）に加え、利用者の利便性を向上させるための「その他の工夫点」（表 2-10）を定義して、各文献の調査を行った。なお、現状のプラクティス集は、プラクティス集の目的とする「経営ガイドラインの実践」と、企業のよくある悩みの解決に資する実用的な内容のバランスをとった構成となっており、プラクティスをストーリー形式で記載し、これからセキュリティ対策を実施する企業でも理解しやすい工夫をしている。また、図表を多用するとともに、ストーリーのモデルとなる企業や人物像のディテールを記載することによって、背景の課題とその対策を結び付けて理解することが可能である（単に(「すべきこと」だけではなく、「このような状況に対してすべきこと」が整理されている)。最後に、検索性について、すべてのプラクティスが経営ガイドラインの指示項目と紐づいているため、ガイドラインの指示項目に応じた対応策を知りたいというニーズに対応することが可能である。一方で、テーマ(例:マネジメント、インシデント対応 等)に関連する対策が、テーマごとに整理・一覧化されていないため、経営ガイドラインの指示項目を意識しない読者にとっては、必ずしも検索性が高くはないことが課題として挙げられる。また、プラクティスの各ストーリーは、読者の状況に完全に合致させることが難しく、読者は自社への読み替えが必要である。そのため、ある程度の知識が読者にないと、具体的な対応内容まで理解されない可能性がある。

文献調査の結果、プラクティス集と類似し、文献の概要から始まり、背景や目的、想定読者の記載の後に、プラクティスの内容を記載するという構成が確認された。一方で、文献 1 では、特定の業種や業務に限定されない、業種や業界横断的に共通的なセキュリティに関連する、20 領域を定義し、読者にとって分かりやすいシンプルな構成をとっている。

また、プラクティスの構成について、文献内のプラクティスにおいて、共通的な要素を用いて、読者の分かりやすさを促す工夫をしている文献が多く確認された。一方で、プラクティスのまとめ方については、ストーリー形式（文献 2、5、6）とリスト形式（文献 1、3、4）を採用する文献が同数確認された。具体的なセキュリティ対策を実施する際や自社のセキュリティ対策の取組み状況を確認する等の場合では、リスト形式のプラクティスが活用しやすいと考えられる。そのため、読者の利用用途に合わせてプラクティスのまとめ方を検討する必要があると考えられる。

最後に、その他の工夫点について、プラクティス集と同様に文字だけでなく図表を駆使し、読者の理解度の向上を促す工夫が確認されたとともに、文献 1 では専用の Web ページ[2]を構築し、セキュリティ対策の成熟度・予算に応じてレベル分けされた企業のグループごとに、

[2] CIS 「 CIS Controls Navigator 」 https://www.cisecurity.org/controls/cis-controls-implementation-groups/

実施すべき具体的な対策を検索・抽出可能な機能を導入する等の検索性の工夫も確認することができた。

表 2-8　Step7：利用（全体構成）

文献	調査観点
	全体構成
プラクティス集	・第 1 章：背景、目的 ・第 2 章：ガイドラインの指示項目に対応したプラクティス ・第 3 章：悩みと取組みのプラクティス(第 2 章で不足する視点や、担当者の実践的な観点を補足)
文献 1	・全 20 領域の対策を優先度の高い順に記載 Controls1～6：基本的予防策(Basic) Controls7～16：基盤的対策(Foundational) Controls17～20：組織的対策(Organizational)
文献 2	・第 1 章：ITIL4 の概要、目的、想定読者、架空の会社のペルソナの低意義、ITIL４のフレームワークの構造と利点について記載 ・第 2 章：サービスマネジメントの概念の概説 ・第 3 章：サービスマネジメントの 4 つの構成要素についての概説 ・第 4 章：ITIL サービスバリューシステムについての概説 ・第 5 章：ITIL の管理プラクティスを、「一般的な管理プラクティス」、「サービスマネジメントのプラクティス」、「技術的なマネジメントのプラクティス」の 3 分類で記載
文献 3	・エグゼクティブサマリーと 7 つのプラクティスで構成 ・エグゼクティブサマリーでは、目的やスコープ、想定読者、ベストプラクティスの概要について記載
文献 4	・第 1 章：調査の目的、範囲、背景、対象読者、方法論および文書の構成に関する序論的情報 ・第 2 章：インダストリー4.0 とそのコンポーネントの定義。ここでは、説明した概念と関連するセキュリティ上の課題について概説 ・第 3 章：脅威の分類とインダストリー4.0 /スマートマニュファクチャリングの攻撃シナリオの例を含む脅威とリスクの分析 ・第 4 章：セキュリティ対策とグッドプラクティスを記載
文献 5	・第 1 章：本プラクティス集の概要：目的、実施内容、整理軸 ・第 2 章：活用の仕方とインデックス：活用の仕方、体制に関するプラクティス（A）インデックス、人材に関するプラクティス（B)インデックス

文献	調査観点
	全体構成
	・第 3 章.プラクティス：(A)体制、(B)人材
文献 6	・100 選プライム 最初に実施概要や審査スケジュールなどを掲載し、その後にプラクティスを掲載（章立て：実施概要、審査スケジュール、応募総数・選定企業数、令和元年度 100 選プライム　選定企業　一覧、各選定企業の事例紹介（プラクティス）） ・新 100 選 最初に実施概要や審査スケジュールなどを掲載し、その後にプラクティスを掲載（章立て：実施概要、審査スケジュール、応募総数・選定企業数、令和元年度 100 選プライム　選定企業　一覧、各選定企業の事例紹介（プラクティス））

表 2-9　Step7：利用（プラクティスの構成）

文献	調査観点	
	プラクティスの構成要素	プラクティスのまとめ方の工夫
プラクティス集	第 2 章 ・指示内容 ・実践に向けたファーストステップ(2～3 項目) ・想定される企業の状況(2～3 項目) ・〇社の実践のステップ(2～3 項目) ・〇社の実践内容 第 3 章(悩みと取組みのプラクティス) ・〇社の基本情報(状況,業種,規模等) ・セキュリティ担当者の悩み ・解決に向けたアプローチ ・得られた知見	・これからセキュリティ対策を実施する企業でも理解しやすいよう架空の企業や人物が登場するストーリー形式
文献 1	・以下の 4 要素で構成 ①対策の概要 ②対策が必要な根拠 ③対策の具体的な実施方法（リスト形式） ④文章および、図を用いた③の自動化の実現に向けた補足説明（手続きや使用ツール）	・20 領域の対策において、具体的な実施方法をリスト形式で記載
文献 2	・以下の 4 要素で構成 ①主要メッセージ：プラクティスの概要を 5 行程度の文章で説明	・ITIL の概念を実際の組織活動にどのように適用させるかを示すために、架空の会社（Axle Car

文献	調査観点	
	プラクティスの構成要素	プラクティスのまとめ方の工夫
	②詳細な説明文：プラクティスに関する言葉の説明や、そのプラクティスを実施する際の重要なポイントが文章で記載 ③ITIL サービスバリューチェーンへの貢献度：そのプラクティスがサービスバリューチェーンへ与える影響を図で説明 ④架空会社のストーリー：一部のプラクティスでは、架空会社にそのプラクティスを当てはめたときの状況をサンプルとして記載	Hire）とその従業員（4 名）の設定を文献共通的に定義して、文書による説明とストーリー（一部のプラクティスのみ）を組み合わせてプラクティスを記載
文献 3	・具体的な対策を記載	・7 つの各プラクティス領域において、具体的な実施方法をリスト形式で記載
文献 4	・グッドプラクティスを「ポリシー」、「組織的対策」、「技術的対策」の 3 カテゴリー（各 4～10 個）に分類した上で、サブカテゴリーごとに具体的なプラクティスを文章（2 行程度）で記載	・サブカテゴリーごとに、必要な対策をリスト形式で記載
文献 5	以下の 4 要素で構成 ① 類型の種類 ② (匿名)企業の状況/基礎情報 ③ 取組みの概要 ④ 実効のポイント・工夫	・ストーリー形式 ・自社の組織体制やセキュリティ成熟度、人材の充足度から参照すべきプラクティスが判別可能
文献 6	・100 選プライム ①サマリー（経営課題、人材戦略、活躍推進の取組、ダイバーシティ経営による成果、企業概要、従業員の状況）、②ダイバーシティ経営推進のストーリー（ダイバーシティの道のり、受賞コメント、経営課題、人材戦略、活躍推進の取組、ダイバーシティ経営による成果）、③ダイバーシティ 2.0 行動ガイドラインと対応した取組の紹介（経営陣の取組、現場の取組、外部コミュニケーション）、④活躍している社員	・100 選プライム 経営課題、人材戦略、活躍推進の取組、ダイバーシティ経営による成果等の項目をストーリー形式で記載 ・新 100 選 具体的には、ダイバーシティ経営のきっかけとなる「経営課題」、経営課題に即して検討・策定された「人材戦略」、それらを踏まえた「活躍推進の取組」、そ

文献	調査観点	
	プラクティスの構成要素	プラクティスのまとめ方の工夫
	・新 100 選 ① 企業概要、②従業員の状況、③ダイバーシティ経営推進のストーリー（ダイバーシティ経営の背景とねらい、ダイバーシティ経営推進のための具体的取組、ダイバーシティ経営による成果)、④活躍している社員	れらの取組を実施したことで得られた「経営上の成果」を掲載

表 2-10　Step7：利用（その他の工夫点）

文献	調査観点		
	その他の工夫	検索性の工夫	付属資料
プラクティス集	・モデルとなる企業や人物像について、ある程度までディテールを記載 ・図表やピクトグラムを多用し、理解を助ける工夫	・全てのプラクティスがガイドラインの指示項目と紐づく	・関連する参考文献 ・用語集 ・情報共有コミュニティ
文献 1	・対策を具体的な実施方法までブレークダウン ・文字中心であるが、表を用いて実施方法をリスト化し、理解を促す工夫	・CIS の HP 上（CIS Controls Navigator）では、組織のグループごとに実施すべき具体的な対策を検索・抽出可能	・具体的な実施方法のリスト（Excel）
文献 2	・文字が中心であるが、具体的な内容が記載	・索引を巻末に記載	・用語集 ・索引
文献 3	・プラクティスによってその分野の展望を記載し、読者の理解を深める工夫 ・図を時折用いて、理解を促す工夫	・巻末に付属資料として用語集、参考文献、略語の説明を搭載 ・参考文献には、出典元の URL へのリンクが貼ってある。	・用語集 ・参考資料 ・略語説明
文献 4	・付録 B にて、必要な対策に対する、具体的な実施方法や推奨事項に加え、その対策に関連する脅威やリ	・サブカテゴリーに属する具体的な対策に附番がされており、付録 B における詳細な説明との紐づけが可能	・用語集 ・付録 A:ENISA「IoT のベースラインセキュリティに関する提言」との関係

文献	調査観点		
	その他の工夫	検索性の工夫	付属資料
	スクが約 60 ページにわたり掲載		・付録 B：セキュリティ対策／グッドプラクティスの詳細なリスト ・付録 C：参考文献 ・付録 D：インダストリー 4.0 セキュリティインシデントの事例
文献 5	・文字が多いが、各プラクティスにポイントとなる図表(体制図等)が挿入 ・「実行のポイント・工夫」の最後(「ここがポイント」)に、特に重要なポイントが３～4 項目に要約 ・各プラクティスともに統一された構成で、かつ 2 ページにまとめられている。	（特になし）	（特になし）
文献 6	文字主体であるが、受賞メンバーや活躍している社員、取組みの様子などを写真や図を使用	・新 100 選 各事例のページ左端に業種インデックス、上端に重点テーマのインデックスを付記	・参考資料１「新・ダイバーシティ経営企業 100 選／100 選プライム選定企業一覧（産業別／地域別）」 ・参考資料２「ダイバーシティ経営企業に関する参考情報」 ・令和元年度 新・ダイバーシティ経営企業 100 選運営委員会　委員名簿

2.3 まとめ

本文献調査では、プラクティスの作成から利用に至るまでのプロセスを 7 ステップに分類し、そのステップごとに観点を定義し、現状のプラクティス集との比較を行った。以下に、ステップごとに、比較の結果やプラクティス集の改善に役立つ示唆を記載する。

【Step1：目的の検討】

想定読者を現状の初心者から拡大し、幅広いニーズに対応することを目的とする場合は、文献 1 のように、想定読者の組織を網羅的にグループ分けした上で、それぞれのグループにおける事例を提供していくことが求められる。

【Step2：主題の選定】

多くの文献が、プラクティス集と同様に、政府機関や標準化団体等によって作成された枠組みや標準等に準拠した上で作成されており、その骨組みに対して、セキュリティの専門家の知見やグッドプラクティスとして取り上げるべき実際の企業の先進的な取組みやその悩みを盛り込んでいることが明らかになった。

【Step3：素材の収集】

収集主体や頻度は、IPA の取組みとほぼ同様であることが明らかになった。また、収集方法についても IPA の取組みと同様に、有識者や企業へのヒアリングが主なアプローチとなっているが、文献 1 や文献 6 のような、企業が自組織の取組みをベストプラクティスとして推薦し発行主体に提案する枠組みは、発行主体が事前に収集したい情報を定義することによって、効果的・効率的に情報を収集することが可能であると考えられる。

【Step4：作成】

作成の方法は、IPA の取組みと同様に、発行主体においてプラクティス集を作成するための担当者が任命され、有識者や企業等が収集した情報を取り纏めている。また、文献 1 では、セキュリティの専門家からの無償の協力・貢献を活用してプラクティスを作成している事例が確認された。一方で、文献 6 のように、プラクティス集に掲載することを念頭において所定のフォーマットを作成し、そのフォーマットに各企業が情報を記載するという方式は、限られた作成時間の中で幅広いニーズに対応したプラクティス集を作成するために有効な方法と考えられる。

【Step5：実状把握による査閲】

IPA の取組みと同様に、作成主体以外の組織に属する有識者や企業の実務者が査閲を実施している査閲の方法が一般的であることが確認できた。上記の各企業が主体的に情報共有を行うスキームが成立すれば、査閲の負担が軽減されることが予測される。

【Step6：公開等による共有】

有償の書籍として販売されている文献 2 を除き、IPA の取組みと同様に、作成主体の HP 上において無償で公開する方法が一般的であることが確認できた。文献 1 は、文書だけでなく各プラクティスの要点をまとめた 2 分程度の動画を作成・HP 上で公開しており、様々な読者のニーズに対応できる工夫をしていることが確認できた。

【Step7：利用】

プラクティスの構成について、文献内のプラクティスにおいて、共通的な要素を定義・利用して、読者の分かりやすさを促す工夫をしている文献が多く確認された。一方で、プラクティスのまとめ方については、ストーリー形式とリスト形式を採用する文献は同数であった。ストーリー形式は企業がセキュリティ対策の背景や理由を理解するなど場合に有用であり、リスト形式は企業がセキュリティ対策の取組み状況を確認するなどの場合に有用であると考えられる。

3 アンケート調査

3.1 調査概要

文献調査の結果から、制作者によるプラクティス集作成の目的の検討から主題の設定、作成まで、多様な手法が採られていることがわかった。また、構成・内容面においても、読者による利用場面を想定して様々な工夫が講じられていた。

次に、企業におけるプラクティス集の利活用の実態や、構成・内容に関するニーズ、プラクティス集の作成・共有に関する取組みの実態や意向等を把握するため、プラクティス集の「認知（プラクティス集をどのように知ったか)」「利用（プラクティス集をどのような目的で利用するか／どのような提供媒体・構成・記載方法であれば目的にかなった利用が可能か)」「内容（どのようなテーマのプラクティスが望まれるか)」「作成・共有（プラクティスを作成しているか／今後作成に取り組む意向はあるか)」の観点から、以下の７項目の仮説を設定し、これを検証するため国内企業を対象にアンケート調査を実施した。

表 3-1　アンケート調査の仮説

分類		NO	仮説
認知		仮説 1	業種や規模により、プラクティス集の認知度や、認知のきっかけに差があるのではないか
利用	利用目的	仮説 2	プラクティス集は、環境変化を踏まえた対策の検討や、資料作成、教育・研修等、幅広い目的で利用されている(利用したいニーズがある)のではないか
	全体構成、提供媒体	仮説 3	プラクティス集は、ドキュメント全体(利用方法、付録資料等を含む)の構成について、理解の促進や情報の検索を容易にする工夫を行うことで、利用の促進が図られるのではないか
	プラクティスの構成、記載方法	仮説 4	プラクティス集は、各プラクティスの表現方法や構成要素について、理解の促進や情報の検索を容易にする工夫を行うことで、利用の促進が図られるのではないか
内容		仮説 5	プラクティスにより、幅広い企業の課題認識と合致しているものと、特定の規模や業種に偏ったものがあるのではないか(企業規模や業種に普遍のプラクティスが考えられるのではないか)
作成・共有	企業内での作成・共有	仮説 6	企業は、プラクティスの素材となるようなセキュリティ対策を推進し、文書化のうえ企業内やグループ企業間で共有されている事例もあるのではないか
	他社と共同での作成・共有	仮説 7	企業は、自社がプラクティスの作成・共有に関する取組みに参加するメリットが理解でき、また、作成・共有の体制や枠組み手順が整備されている場合に、こうした取組みに参加したいと考えるのではないか

アンケート調査は、従業員数 301 人以上かつ、情報システム部門、情報セキュリティ部門・リスク管理部門等を設置している国内企業を対象とした。調査の概要を以下に記載する。

表 3-2　アンケート調査の概要

調査目的	「文献調査」の結果を踏まえ、プラクティス集の利活用の実態を把握する
調査対象	従業員数 301 人以上かつ、情報システム部門、情報セキュリティ部門・リスク管理部門等を設置している国内企業
調査期間	2020 年 11 月 20 日～12 月 18 日
調査方法	Web アンケート調査およびアンケート票調査
回収結果	有効回答数 930 件
調査項目	● 回答企業の基本属性（業種、従業員数、事業の IT システム・IT サービスへの依存度 等） ● サイバーセキュリティ経営ガイドライン Ver2.0 の認知・利活用状況 ● プラクティス集の認知・利活用状況 ● サイバー攻撃対策やセキュリティインシデント対応に係る情報収集 ● プラクティス集の「はじめに」および「第 1 章」に関して ● プラクティス集の「第 2 章」および「第 3 章」に関して ● プラクティス集の提供方法・媒体、更新頻度、記載方法 ● より多くのプタクティスの提供を望むテーマ ● サイバーセキュリティ対策の推進や、対策内容の文書化を通じた自社・グループ企業間での共有　等　全 25 項目
データ精査	回答データに関して、下記の方針で精査し、該当したデータは、 回答内容に不備や矛盾があり、信頼性に問題があると判断し、除外した ● 回答時間が 180 秒未満の回答 ● 10 問以上連続して同じ記号の選択肢を回答する不正な回答 ● 設問 25 まで回答がなされていない回答 ● 設問間で矛盾がある回答 ● 同一企業による重複回答

3.2 調査結果

3.2.1 分析軸

今回の調査では、企業がサイバーセキュリティを経営・事業的リスクと捉えるかどうかは、各企業の事業がどの程度 IT を活用しているかに依存すると仮定し、「IT 依存度」という軸を設定して分析を実施した。「IT 依存度」は、アンケート調査 Q5「事業の IT システム・IT サービスへの依存度」[図 3-1] の回答をもとに、以下の通りに、カテゴリー1 とカテゴリー2、

カテゴリー3、カテゴリー4 に分類した。「カテゴリー1 が最も IT 依存度が高く、カテゴリー4 が最も低い」と定義した。

表 3-3　IT 依存度のカテゴリー

分類	アンケート調査 Q5 の選択肢
カテゴリー1	IT システム・IT サービスが事業上 **必要不可欠な要素** であり、その停止は **事業全体または重要な事業の停止に繋がる**（金融、通販、ネット通販等）
カテゴリー2	顧客へのサービス提供や生産活動の **一部で IT システム・IT サービスを利用** しており、その停止は **事業の一部に大きく影響する**（重要インフラ業種等）
カテゴリー3	顧客へのサービス提供や生産活動の一部で IT システム・IT サービスを利用しているが、IT に依存しない代替手段等があるため、**一時的な停止であれば事業への影響は小さい**
カテゴリー4	IT システム・IT サービスは主に社内業務等に利用するのみで、その停止は **事業にあまり影響しない**

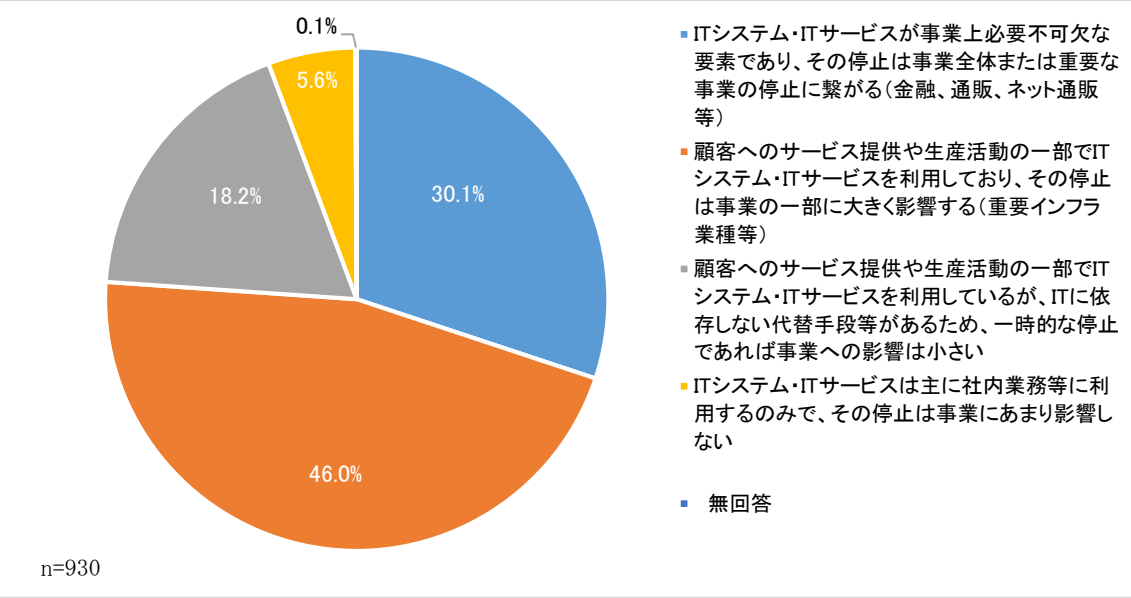


図 3-1　IT 依存度

3.2.2 調査結果

仮説 1～7 に対応する検証結果、または関連する特徴的な結果を整理する。なお、ここでは、先述した「IT 依存度」の軸で分析したアンケート項目の中でも有意な示唆につながる結果が確認できたものを記載し、他の項目を含むアンケート調査結果の全体は、第 7 章のデータ集にまとめて記載した。

3.2.2.1 プラクティス集の「認知」

（仮説 1）業種や規模により、プラクティス集の認知度や、認知のきっかけに差があるのではないか

（プラクティス集の認知度）

プラクティス集が企業にどの程度認知・活用されているかを確認したところ、「知っており、活用している（活用したことがある）」「知っており、まだ活用していないが今後の活用を検討している」「知っているが、まだ活用しておらず、今後の活用も未定」の合計が 43.0%と、アンケート回答企業の約 4 割が認知していることがわかった。一方で、「知っているが、まだ活用しておらず、今後の活用も未定」と回答した企業が全体の 23.4%と、認知している企業の半数以上を占めた。認知した企業が活用したいと思うコンテンツとするために、企業のニーズを把握し、ニーズに即した内容・構成・提供媒体等の工夫が必要であることがわかった（アンケート調査 Q7［図 3-2］）。

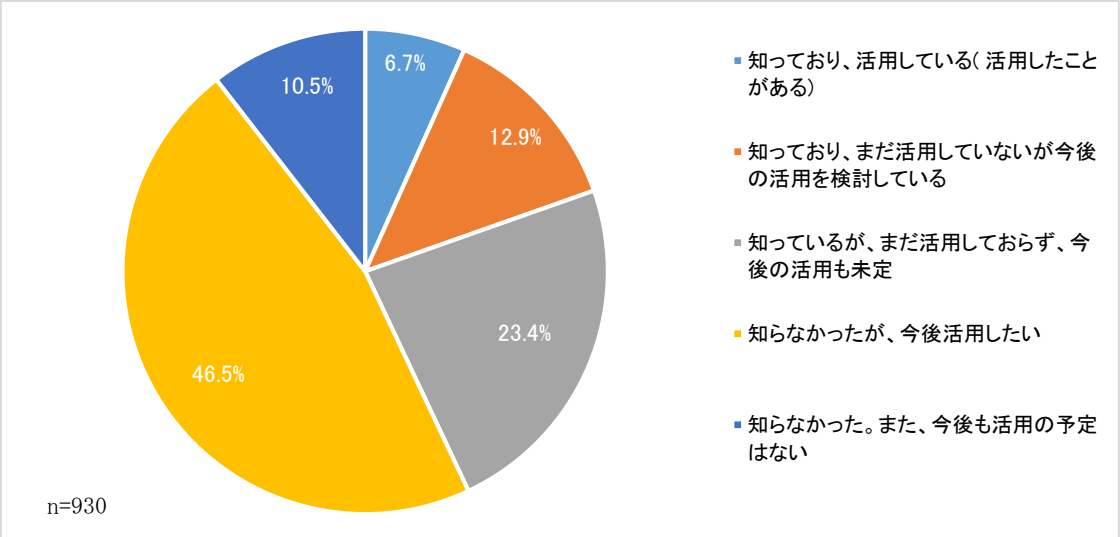


図 3-2　プラクティス集の認知、利活用

また、プラクティス集を認知している企業（43.0%）と認知していない企業（57.0%）において、従業員数（企業規模）や IT 依存度の観点でどの程度傾向に差があるかを確認したところ、プラクティス集を認知している企業は比較的従業員数が多い企業や IT 依存度の高い企業（業種）の割合が高く、認知していない企業は従業員数が少ない企業や IT 依存度の低い企業（業種）が多いことがわかった（アンケート調査 Q1［図 3-3］、Q5［図 3-4］）。

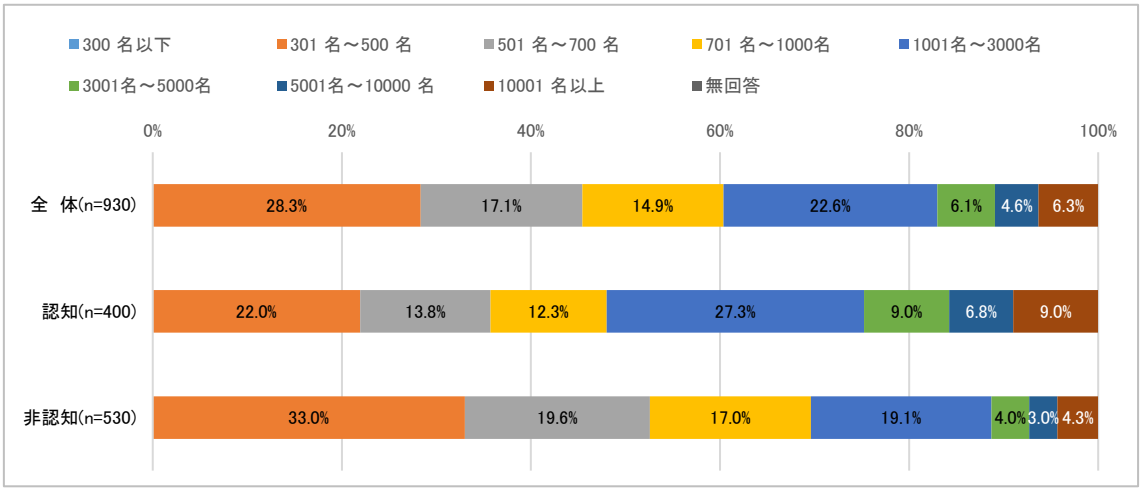


図 3-3　プラクティス集の認知／非認知ごとの従業員数

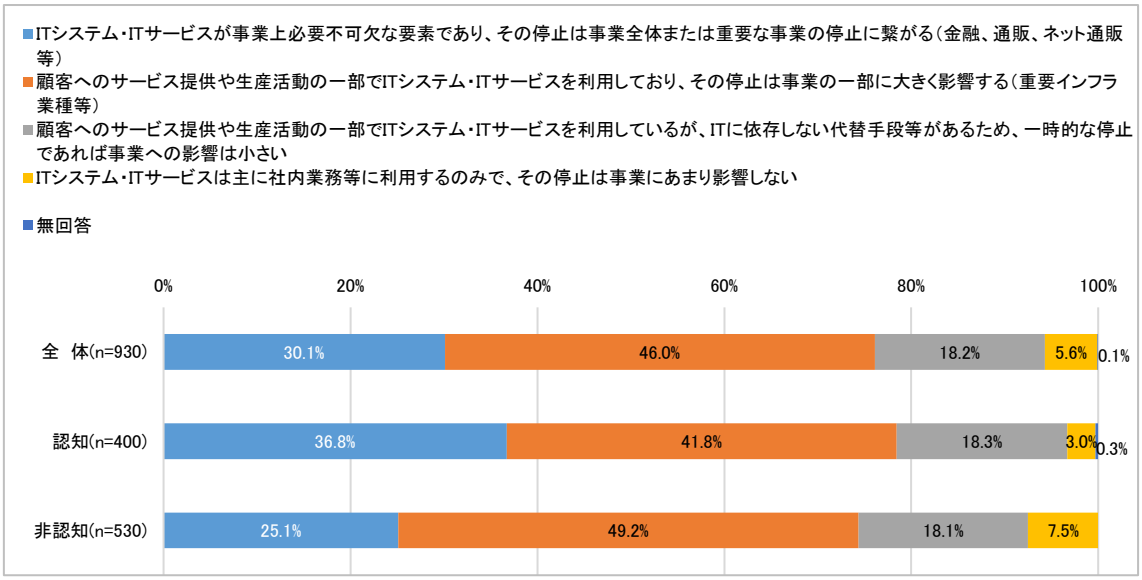


図 3-4　プラクティス集の認知／非認知ごとの IT 依存度

（プラクティス集の利活用のきっかけ）

プラクティス集を利活用したきっかけ（または、今後利活用するきっかけとして想定されるもの）は、全体として、「自社でインシデントが発生し、セキュリティ対策の強化が必要となったとき」（52.1%）が最も多く、次いで「DX・テレワーク等、IT システムの刷新や新たな利用を開始するとき」（47.6%）であった。この 2 項目の回答割合が、3 番目の「監督官庁や業界団体、取引先からサイバーセキュリティへの強化について、指導や要請があったとき」（30.9%）よりも 10Pt 以上回答の割合が高く、この傾向は IT 依存度のいずれのカテゴリーについても同様であった。また、「異動等により、自己研鑽の必要性が生じたとき」（2.9%）とする回答は少なかった。

この結果より、プラクティス集は、IT 依存度の高低に関わらず、新たな IT システムの利活用やそれに伴う体制の変化、自社におけるインシデントの発生等、IT システムに関連する何らかの課題が顕在化した場合に、組織として利活用される場合が多いことが窺える。

なお、IT 依存度が特に高い企業（カテゴリー1）を除くカテゴリー2、3、4 の各カテゴリーでは、いずれも「自社でインシデントが発生し、セキュリティ対策の強化が必要となったとき」が最も多く、次いで「DX・テレワーク等、IT システムの刷新や新たな利用を開始するとき」であった。一方で、IT 依存度の特に高い企業（カテゴリー1）は、「DX・テレワーク等、IT システムの刷新や新たな利用を開始するとき」（47.0%）が最も多く、次いで「自社でインシデントが発生し、セキュリティ対策の強化が必要となったとき」（46.5%）であった。IT 依存度が特に高い企業では、インシデントを契機とした守りのセキュリティ対策は一通り実施しており、新たな IT 戦略・投資に係る攻めのセキュリティ対策について確認したいといったニーズも想定される（アンケート調査 Q9［図 3-5］）。

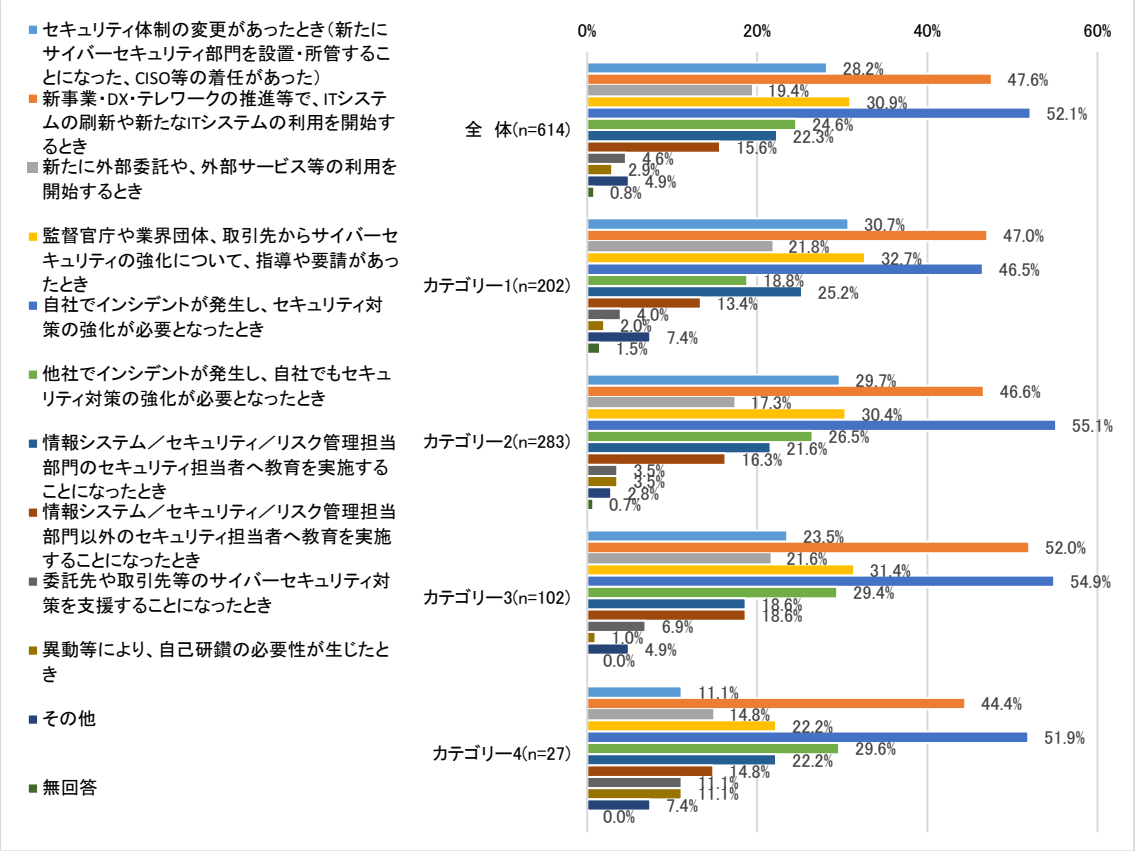


図 3-5　プラクティス集を活用するきっかけ、タイミング

なお、企業において、サイバー攻撃への対策やインシデント対応の強化等の取組みを新たに行う際に、どのような方法で外部より情報収集を行っているかを問う設問に対して、IT 依存度の低い企業（カテゴリー４）は、他のカテゴリーと比較し、「IPA や JPCERT/CC が公

開している情報をホームページ等で確認する」（51.9%）との回答少なく、「委託先の等の IT ベンダーに相談する」（48.1%）の回答が多い結果であった（アンケート調査 Q11［図 3-6］）。

IT 依存度が低い企業は、IPA や JP／CERRT が公表している各種情報へ能動的にアクセスしている傾向が少ないことから、現在の IPA のホームページを通じたプラクティス集の周知方法では、当該層へ十分にアプローチできていない実態が窺える。IT 依存度の低い企業（カテゴリー4）が情報取得の方法として回答した割合の高い「委託先等の IT ベンダーへの相談する」（48.1%）に着目し、IT ベンダーにおける顧客企業とのコミュニケーション場面での活用等を想定したプロモーションの必要性が想定される（アンケート調査 Q11［図 3-6］）。

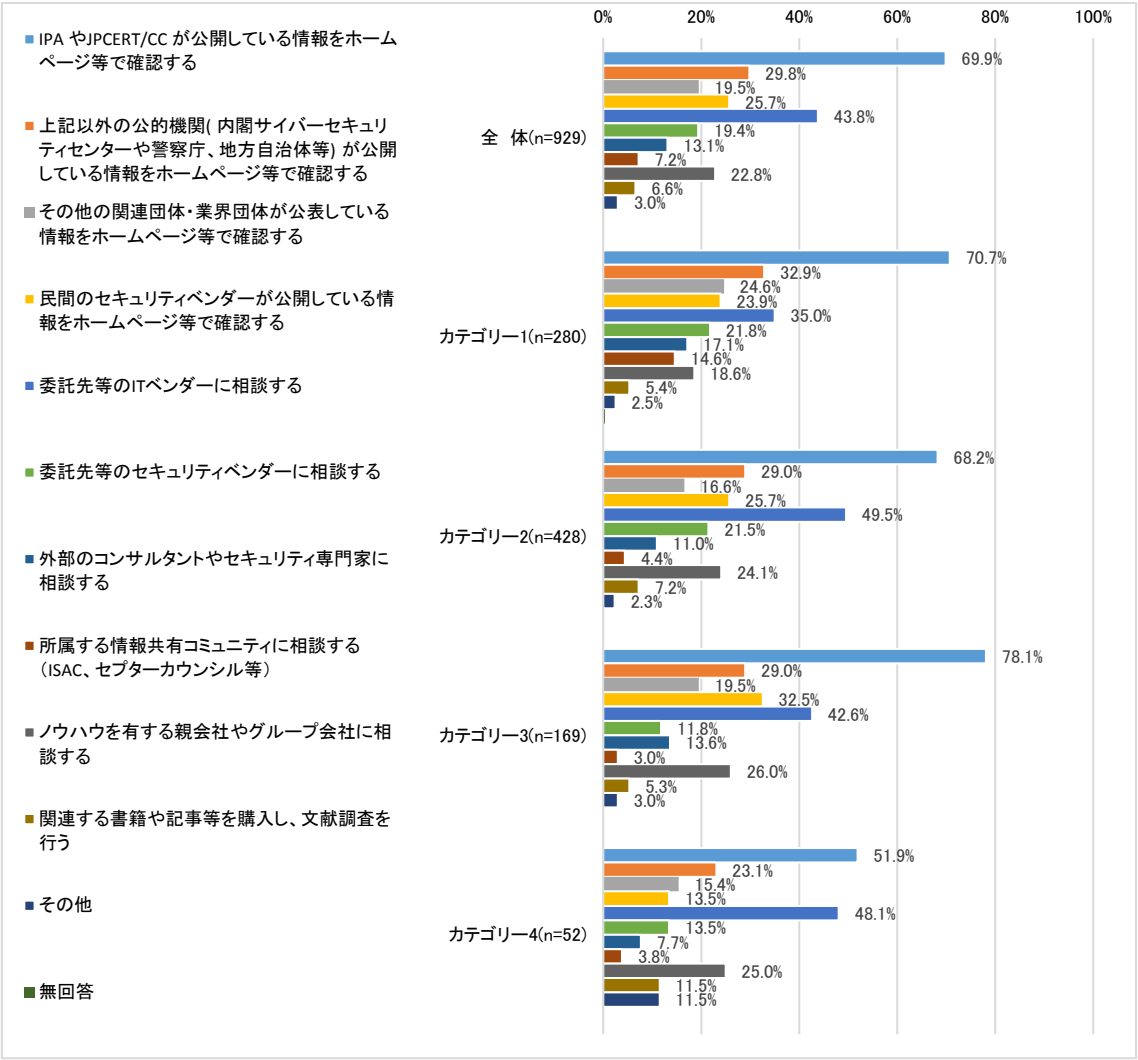


図 3-6　サイバーセキュリティ対策に関する情報収集方法

3.2.2.2 プラクティス集の「利用(利用目的)」

（仮説 2）プラクティス集は、環境変化を踏まえた対策の検討や、資料作成、教育・研修等、幅広い目的で利用されている(利用したいニーズがある)のではないか

プラクティス集を利活用する目的（または、今後利活用する目的として想定されるもの）は、全体として、「サイバーセキュリティ対策のうち、対策が遅れている（対策の必要性が新たに生じた）テーマに関する「はじめの一歩」として、具体的な対策を確認・検討するため」（44.1%）が最も多く、次いで「インシデント発生時の緊急対応体制や復旧体制の整備等、緊急時の体制強化を念頭においたサイバーセキュリティ対策の検討に活用するため」（43.3%）、「セキュリティ対策を経営層へ報告する際や、その報告資料の作成に活用するため」（39.4%）、「管理体制の構築や PDCA サイクルの実施等の、通常時の体制強化を念頭においたサイバーセキュリティ対策の検討に活用するため」（39.1%）をあげる企業が多かった。また、「自己のサイバーセキュリティ知識・能力向上を目的として研鑽に役立てるため」（13.0%）や、「セキュリティ対策を従業員や外部委託先等に連絡する際や、その連絡資料の作成に活用するため」（6.9%）は、相対的に回答が少なかった。

なお、IT 依存度の特に高い企業（カテゴリー1）では、「管理体制の構築や PDCA サイクルの実施等の、通常時の体制強化を念頭においたサイバーセキュリティ対策の検討に活用するため」（44.1%）が最も多く、次いで「サイバーセキュリティ対策のうち、対策が遅れている（対策の必要性が新たに生じた）テーマに関する「はじめの一歩」として、具体的な対策を確認・検討するため」（42.6%）であった。一方、IT 依存度の低い企業（カテゴリー4）では、「サイバーセキュリティ対策全般の「はじめの一歩」として、対策すべきテーマを確認・検討するため」（40.7%）が最も多く、次いで「サイバーセキュリティ対策のうち、対策が遅れている（対策の必要性が新たに生じた）テーマに関する「はじめの一歩」として、具体的な対策を確認・検討するため」（37.0%）であった。また、当該カテゴリーは、「管理体制の構築や PDCA サイクルの実施等の、通常時の体制強化を念頭においたサイバーセキュリティ対策の検討に活用するため」（25.9%）と回答した割合が、その他のカテゴリーと比較して低位であった。

全体として、IT 依存度の高い企業は、現在の体制で不足する観点や対応内容の確認、IT に関連する新たな取組みに際しての更なる体制面の強化を目的に、IT 依存度の低い企業は、サイバーセキュリティ体制の「はじめの一歩」としての活用のニーズが高いことが窺えた（アンケート調査 Q10［図 3-7］）。

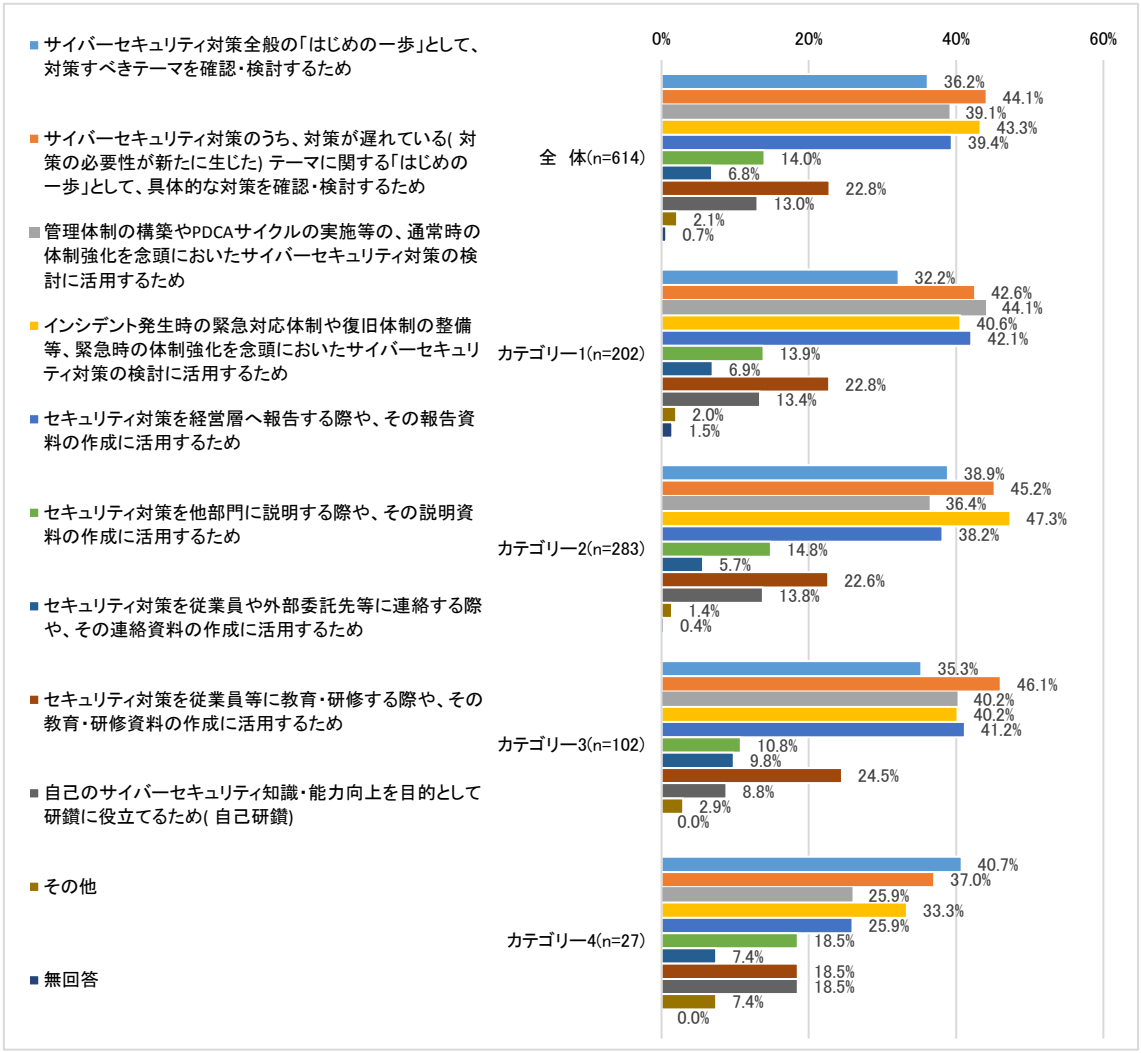


図 3-7　プラクティス集を活用する目的

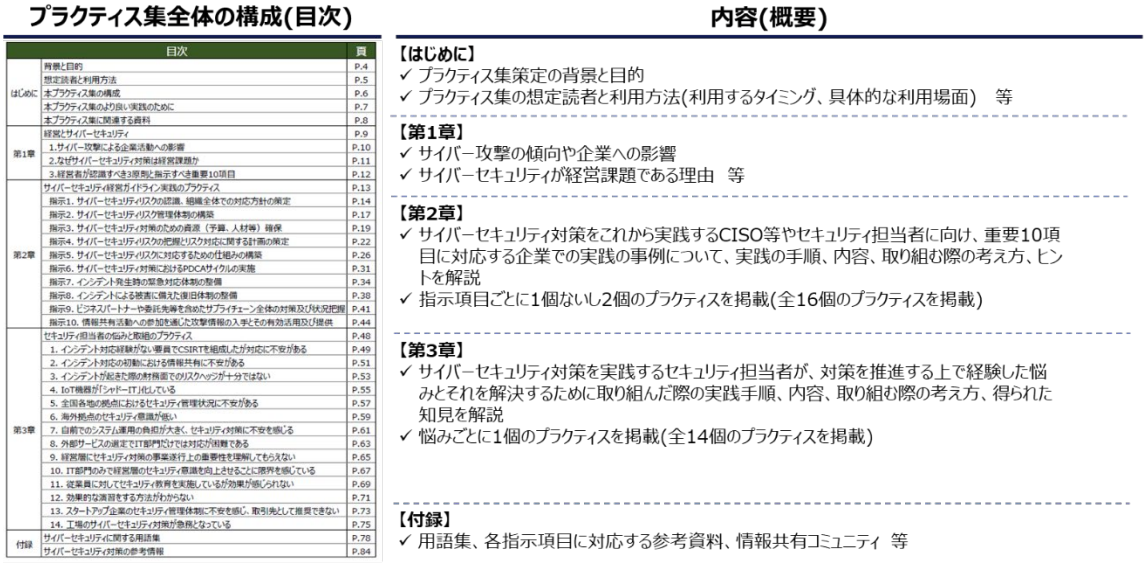
3.2.2.3 プラクティス集の「利用(全体構成、提供媒体)」

（仮説 3）プラクティス集は、ドキュメント全体(利用方法、付録資料等を含む)の構成について、理解の促進や情報の検索を容易にする工夫を行うことで、利用の促進が図られるのではないか

（導入部の構成・内容）

現在のプラクティス集は、プラクティス集提供の背景や目的、想定読者と利用方法等記載した「はじめに」、サイバー攻撃の傾向や企業への影響、サイバーセキュリティが経営課題である理由等を記載した「第 1 章」、サイバーセキュリティ対策をこれから実践する CISO 等やセキュリティ担当者に向けて、重要 10 項目に対応する企業での実践の事例について記載した「第 2 章」、サイバーセキュリティ対策を実践するセキュリティ担当者が、対策を

推進する上で経験した悩みとそれを解決するために取り組んだ際の実践手順等を記載した「第 3 章」、用語集や参考情報を記載した「付録」から構成されている（[図 3-8]）。



プラクティス集全体の構成(目次)

	目次	頁
はじめに	背景と目的	P.4
	想定読者と利用方法	P.5
	本プラクティス集の構成	P.6
	本プラクティス集のより良い実践のために	P.7
	本プラクティス集に関連する資料	P.8
第1章	経営とサイバーセキュリティ	P.9
	1.サイバー攻撃による企業活動への影響	P.10
	2.なぜサイバーセキュリティ対策は経営課題か	P.11
	3.経営者が認識すべき3原則と指示すべき重要10項目	P.12
第2章	サイバーセキュリティ経営ガイドライン実践のプラクティス	P.13
	指示1. サイバーセキュリティリスクの認識、組織全体での対応方針の策定	P.14
	指示2. サイバーセキュリティリスク管理体制の構築	P.17
	指示3. サイバーセキュリティ対策のための資源（予算、人材等）確保	P.19
	指示4. サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	P.22
	指示5. サイバーセキュリティリスクに対応するための仕組みの構築	P.26
	指示6. サイバーセキュリティ対策におけるPDCAサイクルの実施	P.31
	指示7. インシデント発生時の緊急対応体制の整備	P.34
	指示8. インシデントによる被害に備えた復旧体制の整備	P.38
	指示9. ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握	P.41
	指示10. 情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	P.44
第3章	セキュリティ担当者の悩みと取組のプラクティス	P.48
	1. インシデント対応経験がない要員でCSIRTを組成したが対応に不安がある	P.49
	2. インシデント対応の初動における情報共有に不安がある	P.51
	3. インシデントが起きた際の財務面でのリスクヘッジが十分ではない	P.53
	4. IoT機器が「シャドーIT」化している	P.55
	5. 全国各地の拠点におけるセキュリティ管理状況に不安がある	P.57
	6. 海外拠点のセキュリティ環境が低い	P.59
	7. 自前でのシステム運用の負担が大きく、セキュリティ対策に不安を感じる	P.61
	8. 外部サービスの選定でIT部門だけでは対応が困難である	P.63
	9. 経営層にセキュリティ対策の事業遂行上の重要性を理解してもらえない	P.65
	10. IT部門のみで経営層のセキュリティ環境を向上させることに限界を感じている	P.67
	11. 従業員に対してセキュリティ教育を実施しているが効果が感じられない	P.69
	12. 効果的な演習をする方法がわからない	P.71
	13. スタートアップ企業のセキュリティ管理体制に不安を感じ、取引先として推奨できない	P.73
	14. 工場のサイバーセキュリティ対策が急務となっている	P.75
付録	サイバーセキュリティに関する用語集	P.78
	サイバーセキュリティ対策の参考情報	P.84

内容(概要)

【はじめに】
- ✓ プラクティス集策定の背景と目的
- ✓ プラクティス集の想定読者と利用方法(利用するタイミング、具体的な利用場面)　等

【第1章】
- ✓ サイバー攻撃の傾向や企業への影響
- ✓ サイバーセキュリティが経営課題である理由　等

【第2章】
- ✓ サイバーセキュリティ対策をこれから実践するCISO等やセキュリティ担当者に向け、重要10項目に対応する企業での実践の事例について、実践の手順、内容、取り組む際の考え方、ヒントを解説
- ✓ 指示項目ごとに1個ないし2個のプラクティスを掲載(全16個のプラクティスを掲載)

【第3章】
- ✓ サイバーセキュリティ対策を実践するセキュリティ担当者が、対策を推進する上で経験した悩みとそれを解決するために取り組んだ際の実践手順、内容、取り組む際の考え方、得られた知見を解説
- ✓ 悩みごとに1個のプラクティスを掲載(全14個のプラクティスを掲載)

【付録】
- ✓ 用語集、各指示項目に対応する参考資料、情報共有コミュニティ　等

図 3-8　プラクティス集全体の構成（目次）と記載の概要

このうち、まずは、プラクティス集全体の構成や活用方法を解説しているプラクティス集の導入部である「はじめに」と「第 1 章」について企業のニーズを確認した。

導入部の構成・内容についての要望としては、全体として、「企業の状況や課題に応じた利用方法、参照すべきプラクティスについて、具体的に解説する」（25.1%）ニーズが最も高く、次いで「サイバー攻撃が経営課題である理由について、具体的に解説する」（20.7%）であった。なお、「企業の状況や課題に応じた利用方法、参照すべきプラクティスについて、具体的に解説する」ニーズは IT 依存度が特に高い企業（カテゴリー1）で最も強く、IT 依存度が低い企業（カテゴリー4）では比較的低い傾向が把握できた。また、IT 依存度が低い企業（カテゴリー4）は、その他のカテゴリーと異なり、「サイバー攻撃が経営課題である理由について、具体的に解説する」（26.9%）ニーズが最も高かった。先述の「はじめの一歩」としての活用のニーズも踏まえると、当該カテゴリーの企業は、サイバーセキュリティへの取組みを始めるにあたり、経営層や社内の説得・意識醸成から着手する必要があり、こうした場面でサイバーセキュリティ対策の必要性を訴求できる資料を必要としている可能性がある（アンケート調査 Q12［図 3-9］）。

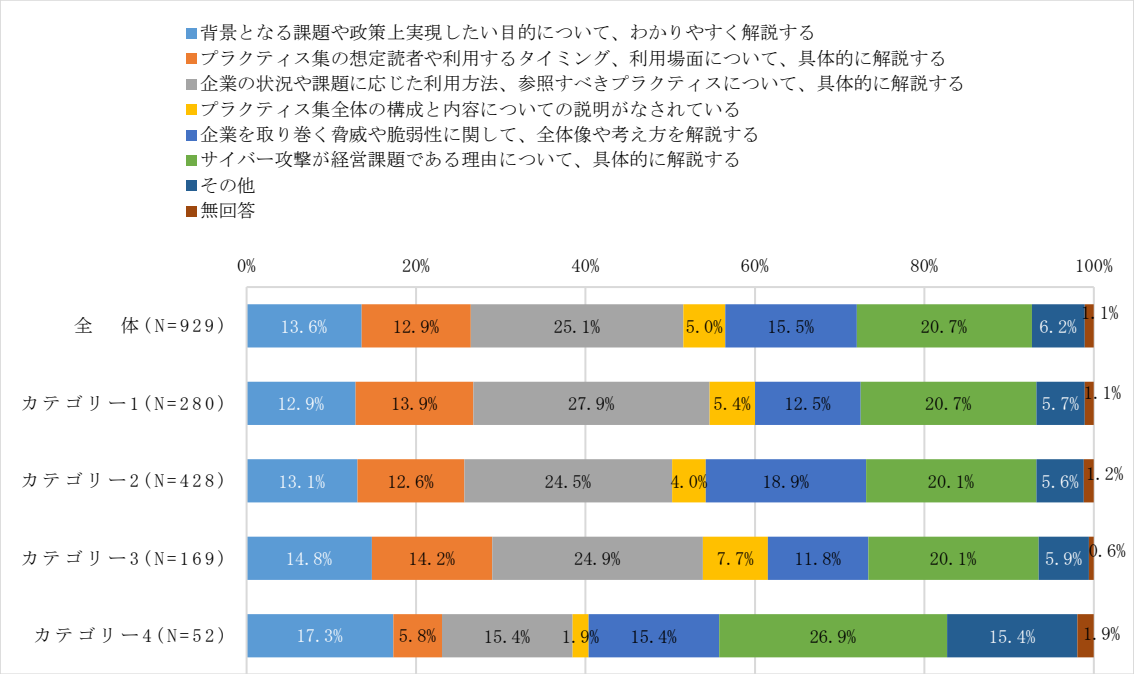


図 3-9　「導入部」の構成・内容についての要望

（提供方法・媒体、更新頻度）

プラクティス集は現在､IPA のホームページに PDF 形式で公開する方法を採っているが、このようなプラクティス集の提供方法や提供媒体についてのニーズを確認した。

IT 依存度の高低に関わらず、「検索性の高い Web コンテンツとしての提供」（44.2%）のニーズが高いことがわかった。「プラクティ内容の情報の検索性を高める」（16.1%）と合わせると、アンケート回答企業全体の約 6 割が検索性の向上を求めていることが確認できた。また、「図表やピクトグラム、写真等視覚的な理解を助ける工夫」（17.0%）や「Web サイト(IPA 公式サイトや SNS 等)を設置してコミュニケーションができるようにする」（10.7%）についても、一定のニーズが確認できた。とりわけ、IT 依存度が低い企業（カテゴリー4）は「Web サイト(IPA 公式サイトや SNS 等)を設置してコミュニケーションができるようにする」（19.2%）ニーズが高く、プラクティス集の内容を消化し具体的な取組みに着手するにあたり、フォローを必要としている実態が窺えた（アンケート調査 Q15［図 3-10］）。

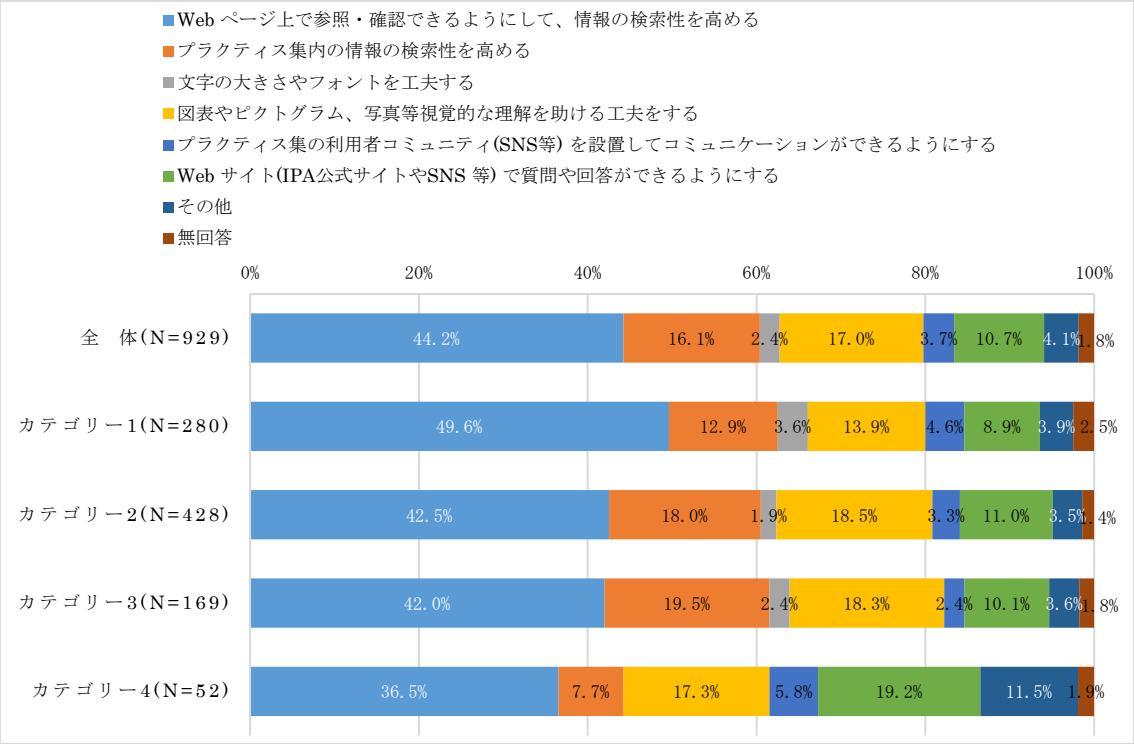


図 3-10　プラクティスの提供方法・媒体

また、プラクティス集の更新の頻度については、IT 依存度に関わらず「1 年に 1 回」を希望する回答が最も多かった。（アンケート調査 Q16［図 3-11］）

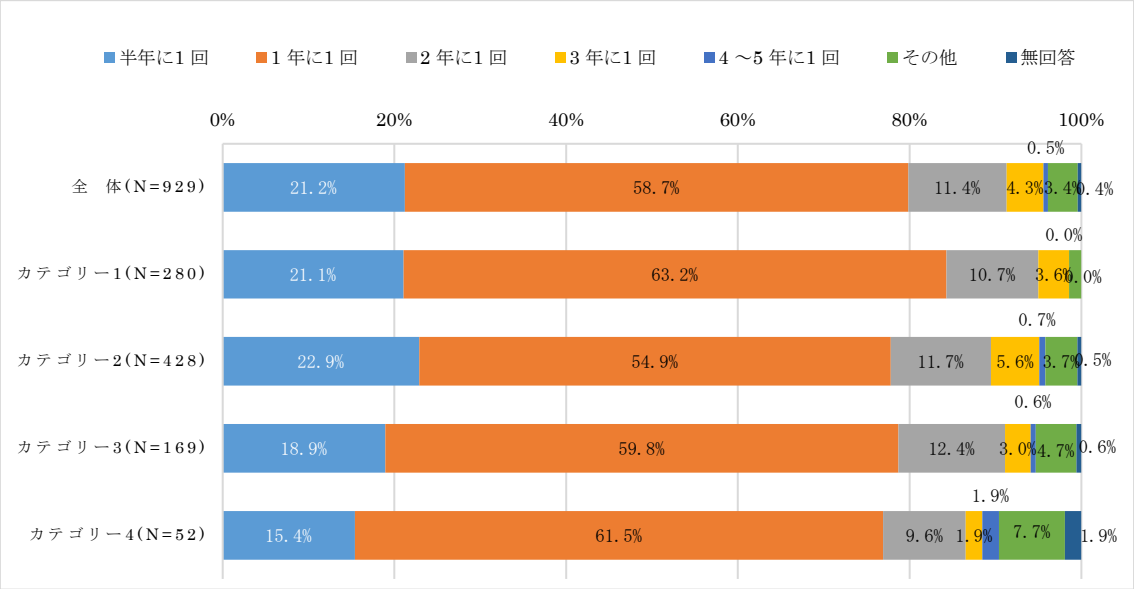


図 3-11　プラクティスの更新頻度

3.2.2.4 プラクティス集の「利用（プラクティスの構成、記載方法）」

（仮説 4）プラクティス集は、各プラクティスの表現方法や構成要素について、理解の促進や情報の検索を容易にする工夫を行うことで、利用の促進が図られるのではないか

（第 2 章の構成）

先述の通り、現在のプラクティス集では、第 2 章と第 3 章で個別のプラクティスを掲載している。このうち第 2 章は、「サイバーセキュリティ経営ガイドライン実践のプラクティス」として、サイバーセキュリティ対策をこれから実践する CISO 等やセキュリティ担当者に向け、重要 10 項目に対応する企業での実践の事例について、実践の手順、内容、取り組む際の考え方、ヒントを解説している（[図 3-12]）。

図 3-12　第 2 章の構成

この第 2 章の構成について、企業のニーズを確認した。

全体として、「企業の状況（業種、規模、組織体制等）に応じて、対応すべきプラクティスがわかるようにする」（39.3%）や、「プラクティスを実施するために必要なコストや費用対効果についての説明を充実させる」（39.9%）、「プラクティスの優先順位や、対策を実施すべき順番がわかるようにする」ニーズが高いことがわかった。一方で、「プラクティスに関連するソリューションやサービスの事例を紹介する」（9.6%）、「関連する省令、ガイドライン、書籍、用語等の参考情報を充実させる」（8.6%）、「プラクティスと参考情報との紐づけがわかるようにする」（5.4%）ニーズは低位であった。なお、IT 依存度が低い企業群（カテゴリー4）では、「企業の状況（業種、規模、組織体制等）に応じて、対応すべきプラクティスがわかるようにする」（23.1%）との回答が、その他のカテゴリーと比較して低位であり、「プラクティスの優先順位や、対策を実施すべき順番がわかるようにする」（34.6%）との回答が多

く、「はじめの一歩」として何から手を付けるべきかを示してほしい（わかるようにしてほしい）ニーズが強いものと想定される（アンケート調査 Q13［図 3-13］）。

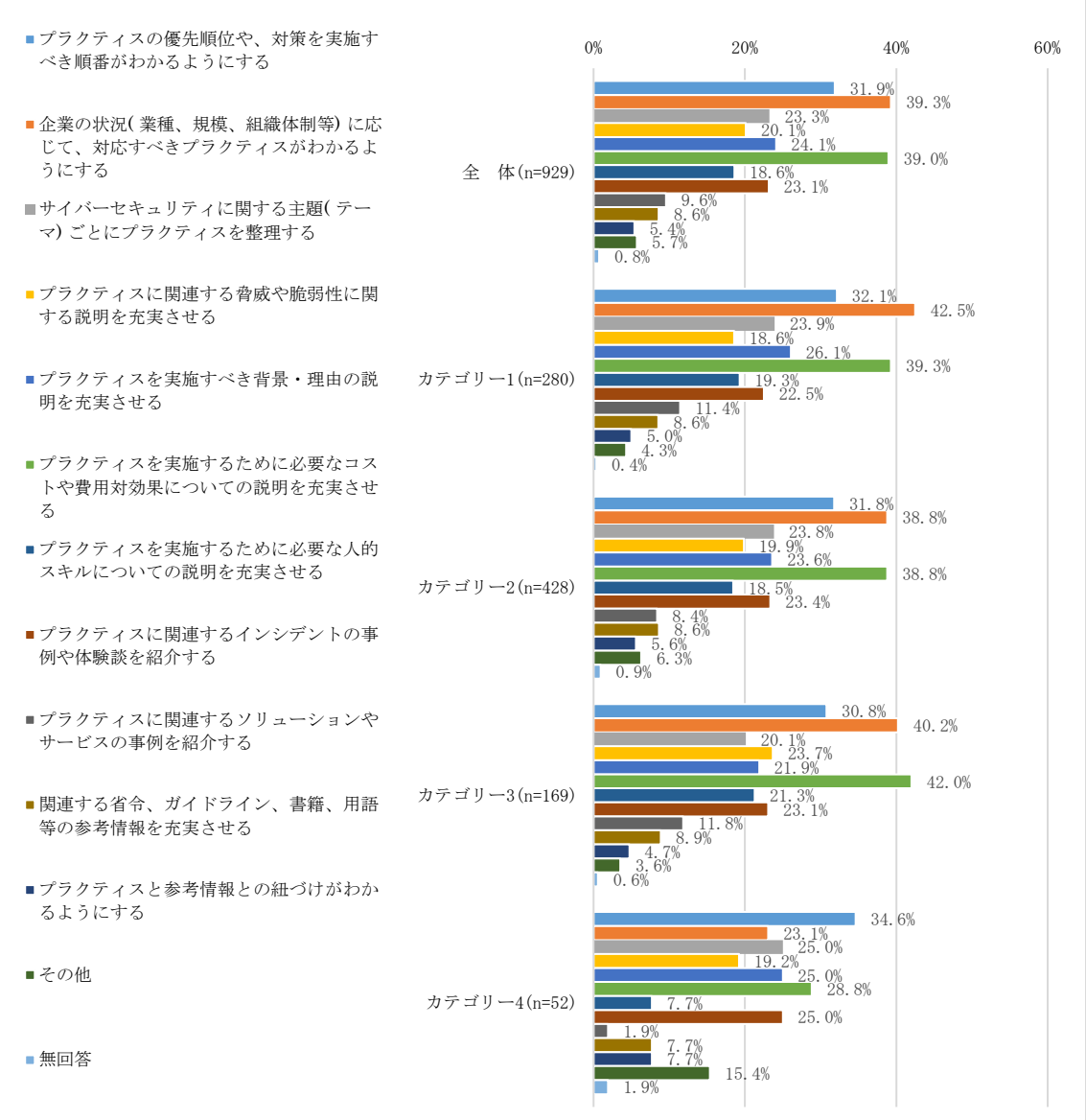


図 3-13　第 2 章の構成についての改善点

（第 3 章の構成）

第 3 章は、「セキュリティ担当者の悩みと取組のプラクティス」として、サイバーセキュリティ対策を実践するセキュリティ担当者が、対策を推進する上で経験した悩みとそれを解決するために取り組んだ際の実践手順、内容、取り組む際の考え方、得られた知見を解説している（[図 3-14]）。

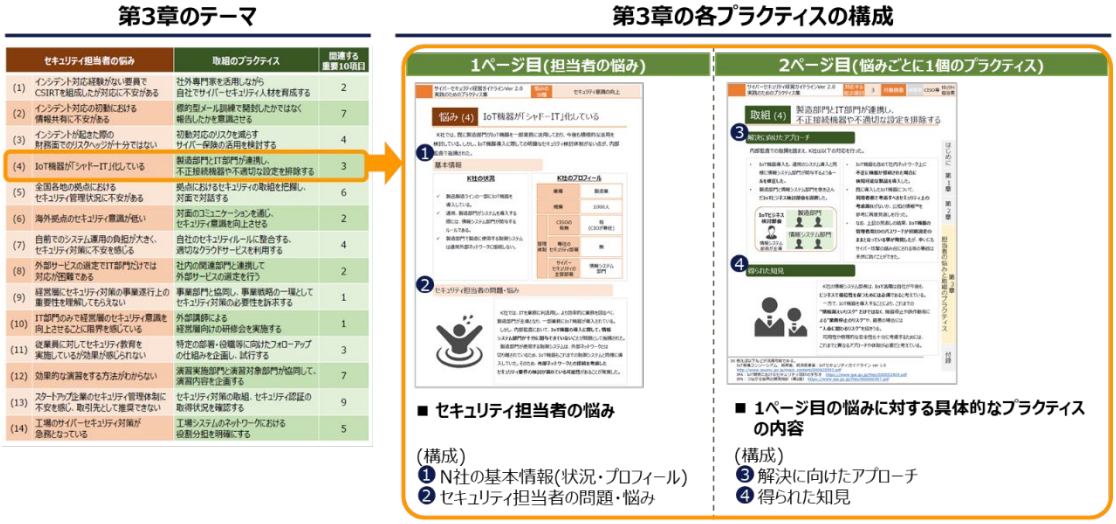


図 3-14　第 3 章の構成

この第 3 章についても、第 2 章と同様に「プラクティスを実施するために必要なコストや費用対効果についての説明を充実させる」（35.5%）や、「企業の状況（業種、規模、組織体制等）に応じて、対応すべきプラクティスがわかるようにする」（33.8%）、「プラクティスの優先順位や、対策を実施すべき順番がわかるようにする」ニーズが高いことがわかった。また、「プラクティスに関連するソリューションやサービスの事例を紹介する」（14.1%）、「関連する省令、ガイドライン、書籍、用語等の参考情報を充実させる」（7.8%）、「プラクティスと参考情報との紐づけがわかるようにする」（6.1%）ニーズが低位である点、IT 依存度が低い企業群（カテゴリー4）では、「プラクティスの優先順位や、対策を実施すべき順番がわかるようにする」（40.4%）ニーズが高い点も第 2 章と同様であった（アンケート調査 Q14［図 3-15］）。

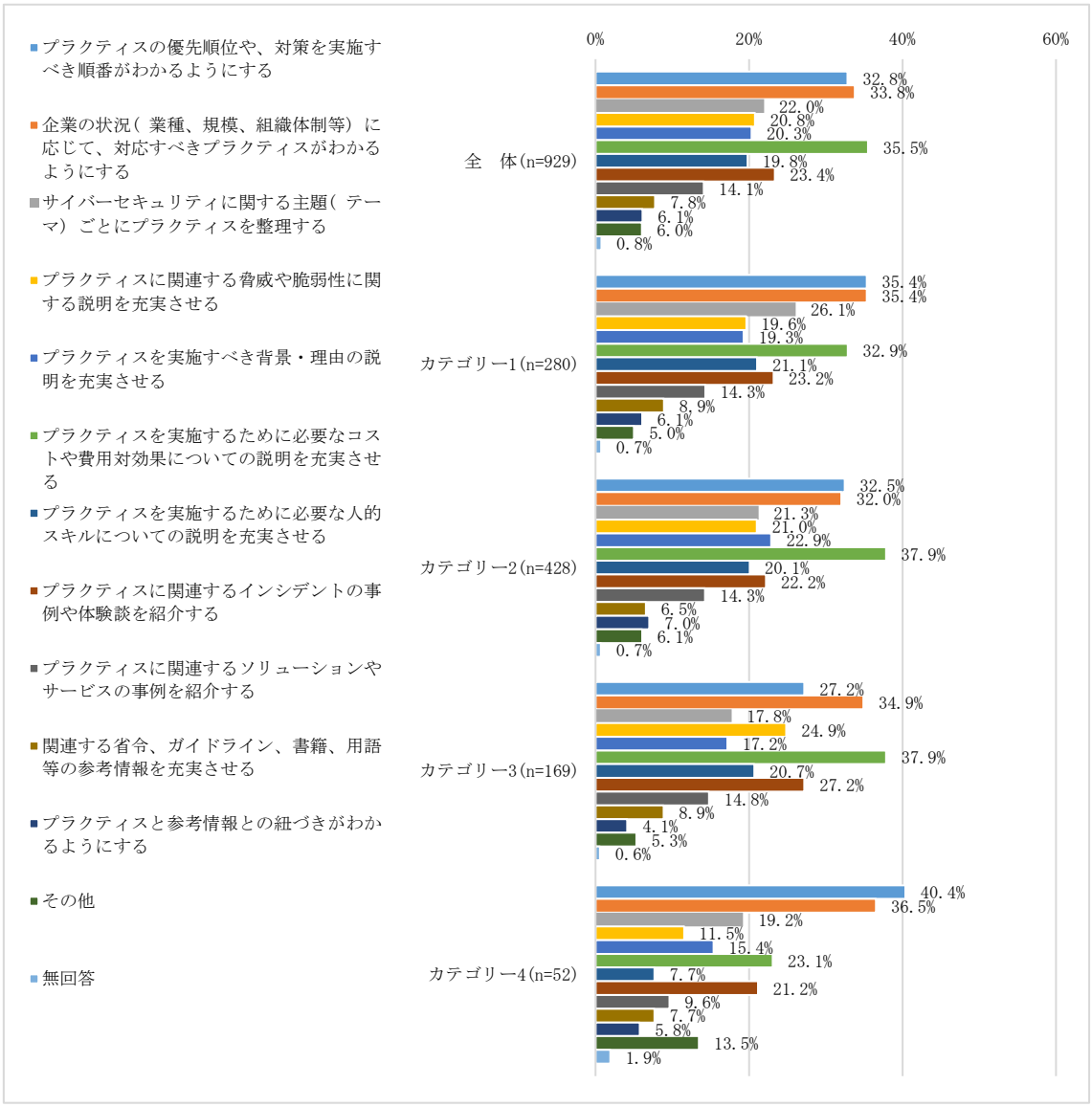


図 3-15　第 3 章の構成・内容についての改善点

（プラクティスの記載方法）

現在のプラクティス集は、第 2 章および第 3 章のいずれのプラクティスについても、実際の企業の取組みをモデルに、企業を取り巻く環境や担当者の問題意識等も描きながら、「ストーリー形式」で課題や対応手順を紹介している。一方で、文献調査にて確認した通り、プラクティスの記載方法としては、その他にも、「企業が対応すべき事項や対応手順に関する確認事項について、一覧表やリストとして整理して紹介する方法（一覧表やリスト形式など）」や「取組みのヒントとなるような、様々な対応事例(Tips)を羅列して紹介する方法（Tips 集など）」等が想定される。

このプラクティスの記載方法については、全体として、背景や理由とセットで取組み内容を紹介するストーリー形式と、対応事項や手順を一覧表やリストで紹介する方法が、それぞれ 30%代後半の回答率であり、取組みのヒントとなる対応事例を紹介する Tips 形式が 20%前半と他の 2 つと比較してやや低い結果であった。また、IT 依存度が低い企業（カテゴリー４）においては、ストーリー形式による背景や理由の説明の説明よりも、Tis 集による取組みのヒントへのニーズが高いことが窺えた（アンケート調査 Q17［図 3-16］）。

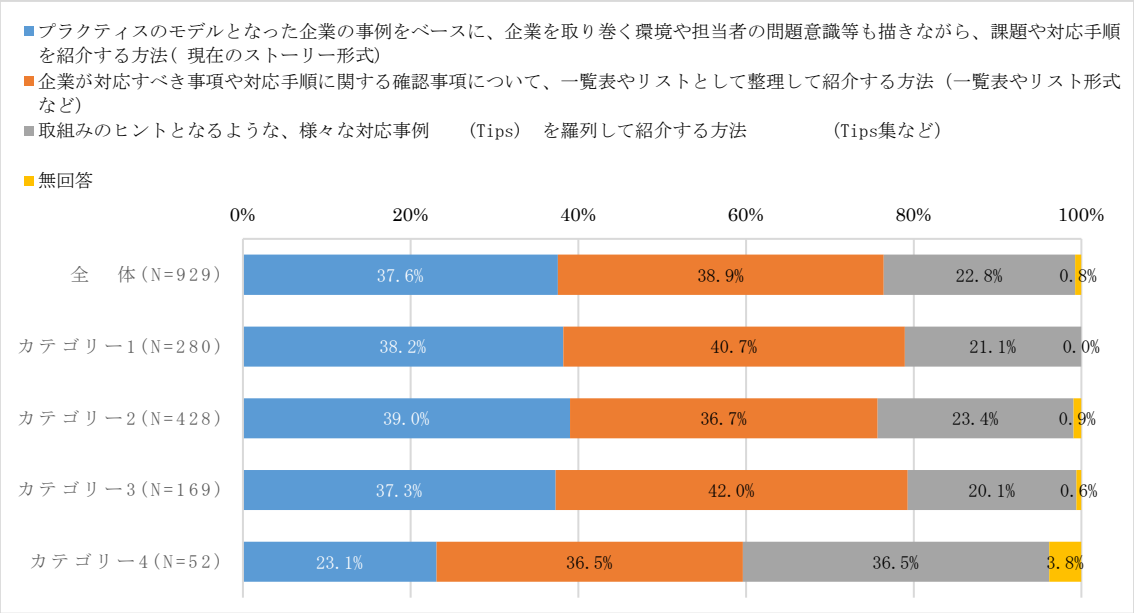


図 3-16 プラクティスの記載方法

3.2.2.5 プラクティス集の「内容」

（仮説 5）プラクティスにより、幅広い企業の課題認識と合致しているものと、特定の規模や業種に偏ったものがあるのではないか(企業規模や業種に普遍のプラクティスが考えられるのではないか)

（プラクティスの提供を望むテーマ）

先述の通り、現在のプラクティス集では、第 2 章において、サイバーセキュリティ経営ガイドラインの指示項目 1～10 に対応したサイバーセキュリティ体制の構築・強化に関連するテーマのプラクティスを、第 3 章において、セキュリティ担当者の悩みと取組として、「インシデント対応」「シャドーIT 対策」「従業員教育」「演習実施」等の個別テーマに関する対策や取組みを紹介している。

現在取り上げているテーマについて、企業のニーズに合致しているか、またテーマにより、業種や規模等の観点から個別性の強いプラクティスが求められるもの、スタンダードとして共通的なプラクティスが求められるものがそれぞれ存在するのではないかと想定し、今後プラクティス集で取り上げる（提供を望む）テーマについて企業のニーズを確認した。

今後より多くのプラクティスの提供を望むテーマについては、全体として、「サイバーセキュリティリスクの認識、組織全体の対応方針の策定」（19.4%）や「サイバーセキュリティ対策のための資源（予算・人材等）の確保」（15.9%）、「経営層や従業員のセキュリティ認識に関する悩み」（11.5%）が多くあげられた。一方で、「情報共有活動への参加を通じた攻撃情報の入手とその有効活用」（0.2%）や「演習や訓練の実施に関する悩み」（1.1%）とする回答は低位であった。なお、「サイバーセキュリティ対策のための資源（予算・人材等）の確保」については、IT 依存度が高い企業ほど強いニーズを有しており、また、IT 依存度が低い企業（カテゴリー4）は、「経営層や従業員のセキュリティ認識に関する悩み」についてのニーズが高いことがわかった。先述のプラクティス集の利用のニーズを踏まえると、IT 依存度が高い企業では、IT を活用した新たな取組みや環境の変化を踏まえた体制の強化に際し、資源（予算、人材等）の確保に向けた社内調整や採用・育成等に課題を有しており、IT 依存度が低い企業は、サイバーセキュリティ対策の「はじめの一歩」を推進するにあたり、経営層や従業員のセキュリティ認識の醸成の必要性を感じていることが窺える（アンケート調査 Q19［図 3-17-1］）。

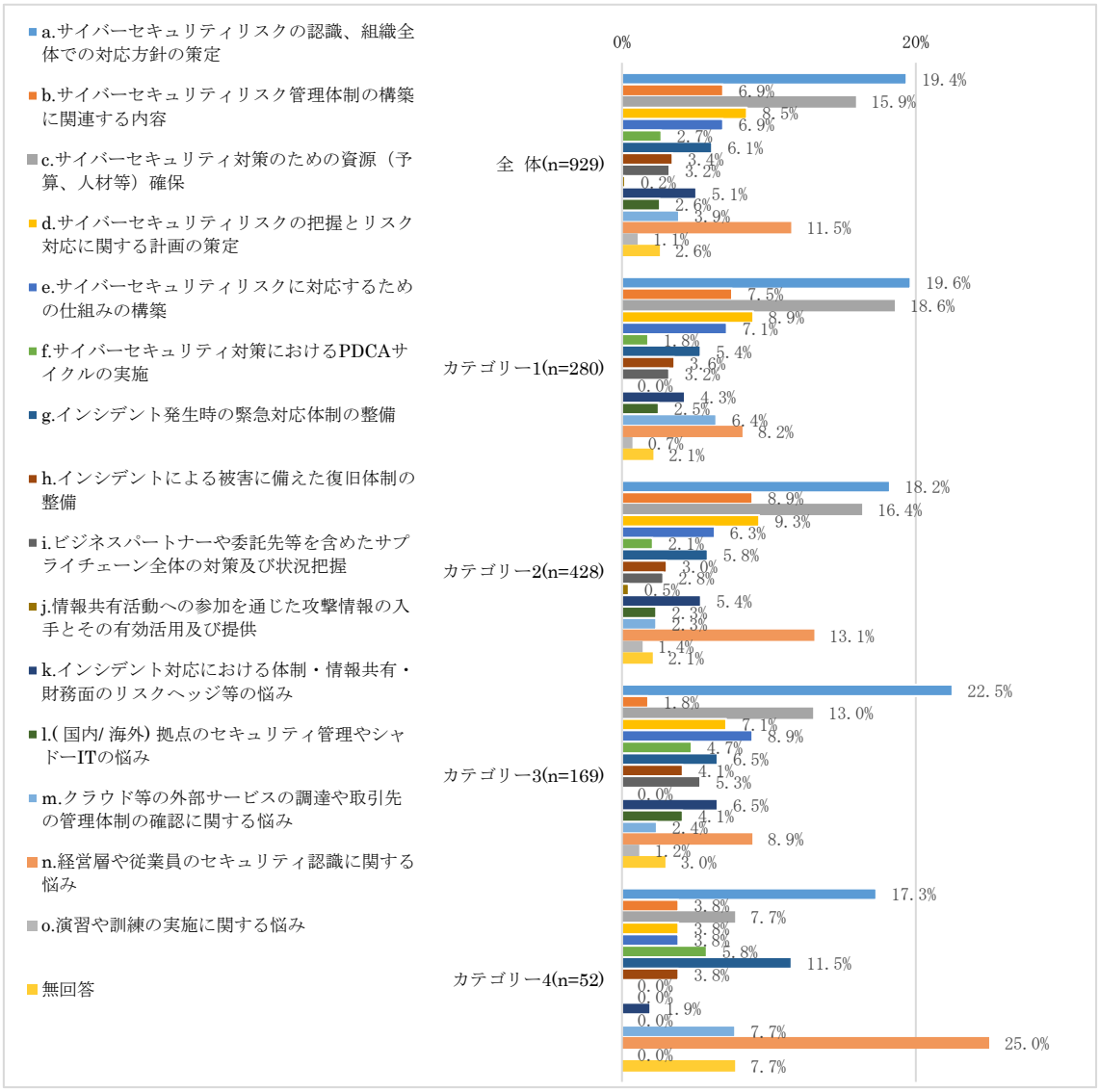


図 3-17-1　今後より多くのプラクティスの提供を望むテーマ（最も強く望むテーマ）

また、業種別の傾向では、全体平均よりも回答が多いテーマとして、建設業で「経営層や従業員のセキュリティ認識に関する悩み」や「ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握」、電気・ガス・熱供給・水道業で「サイバーセキュリティリスクの把握とリスク対応に関する計画の策定」や「インシデント対応における体制・情報共有・財務面のリスクヘッジ等の悩み」、情報通信業で「サイバーセキュリティ対策のための資源（予算、人材等）確保」、医療福祉で「サイバーセキュリティリスクの認識、組織全体での対応方針」等が確認できた。また、全体平均よりも回答が少ないテーマとして、建設業や電気・ガス・熱供給・水道業、金融・保険業で「サイバーセキュリティリスクの認識、組織全体での対応方針」、情報通信業や金融・保険業で「経営層や従業員のセキュリテ

ィ認識に関する悩み」等が確認できた。業種の違いによりテーマに対するニーズに相違がみられることから、各テーマに対する取組みの状況も業種により差があることが窺える。

	n	a.サイバーセキュリティリスクの認識、組織全体での対応方針の策定	b.サイバーセキュリティリスク管理体制の構築に関連する内容	c.サイバーセキュリティ対策のための資源（予算、人材等）確保	d.サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	e.サイバーセキュリティリスクに対応するための仕組みの構築	f.サイバーセキュリティ対策におけるPDCAサイクルの実施	g.インシデント発生時の緊急対応体制の整備	h.インシデントによる被害に備えた復旧体制の整備	i.ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握	j.情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	k.インシデント対応における体制・情報共有・財務面のリスクヘッジ等の悩み	l.（国内/海外）拠点のセキュリティ管理やシャドーITの悩み	m.クラウド等の外部サービスの調達や取引先の管理体制の確認に関する悩み	n.経営層や従業員のセキュリティ認識に関する悩み	o.演習や訓練の実施に関する悩み	無回答
建設業(n=70)	70	10.0	5.7	18.6	5.7	7.1	7.1	4.3	1.4	**8.6**	0.0	8.6	0.0	1.4	**18.6**	1.4	1.4
製造業(n=255)	255	18.8	8.6	13.3	7.5	8.6	2.7	7.1	3.5	4.7	0.0	4.7	5.5	2.7	9.4	0.8	2.0
電気・ガス・熱供給・水道業(n=17)	17	11.8	0.0	17.6	**29.4**	0.0	5.9	5.9	0.0	5.9	0.0	**11.8**	0.0	5.9	5.9	0.0	0.0
情報通信業(n=68)	68	20.6	4.4	**22.1**	**14.7**	4.4	2.9	1.5	4.4	2.9	0.0	5.9	2.9	5.9	1.5	4.4	1.5
運輸業、郵便業(n=66)	66	15.2	10.6	15.2	7.6	6.1	1.5	7.6	3.0	1.5	1.5	3.0	0.0	4.5	**18.2**	1.5	3.0
卸売業、小売業(n=111)	111	23.4	9.0	16.2	7.2	3.6	3.6	8.1	3.6	1.8	0.0	3.6	0.0	1.8	15.3	0.0	2.7
金融業、保険業(n=73)	73	13.7	5.5	20.5	12.3	9.6	2.7	4.1	2.7	4.1	0.0	4.1	4.1	8.2	5.5	2.7	0.0
不動産業、物品賃貸業(n=11)	11	0.0	18.2	18.2	9.1	**18.2**	0.0	9.1	**9.1**	0.0	0.0	9.1	0.0	**9.1**	0.0	0.0	0.0
学術研究、専門・技術サービス業(n=9)	9	**44.4**	0.0	**22.2**	0.0	11.1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	**22.2**	0.0	0.0
宿泊業、飲食サービス業(n=18)	18	**27.8**	5.6	16.7	11.1	5.6	0.0	**11.1**	0.0	0.0	0.0	5.6	0.0	5.6	11.1	0.0	0.0
生活関連サービス業務、娯楽業(n=5)	5	20.0	0.0	0.0	0.0	**20.0**	0.0	0.0	0.0	**20.0**	0.0	0.0	0.0	**20.0**	**20.0**	0.0	0.0
教育、学習支援業(n=2)	2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	**100.0**	0.0	0.0
医療、福祉(n=96)	96	**29.2**	7.3	13.5	5.2	3.1	1.0	5.2	3.1	0.0	1.0	4.2	3.1	2.1	14.6	0.0	7.3
サービス業（他に分類されないもの）(n=112)	112	21.4	3.6	13.4	9.8	8.0	2.7	7.1	5.4	1.8	0.0	6.3	1.8	5.4	9.8	0.9	2.7
その他(n=17)	17	5.9	0.0	**29.4**	0.0	11.8	0.0	5.9	5.9	0.0	0.0	5.9	0.0	5.9	**17.6**	0.0	11.8
全体(n=930)	930	19.4	6.9	15.9	8.5	6.9	2.8	6.1	3.4	3.2	0.2	5.1	2.6	3.9	11.5	1.1	2.6

※（単位：%）全体平均よりも 5pt 以上高い項目を網掛/白抜き、5pt 以上低い項目を網掛で表示

図 3-17-2　今後より多くのプラクティスの提供を望むテーマ（最も強く望むテーマ）

（業種・規模等に共通的なプラクティスを望むテーマと、業種・規模等に特化したプラクティスを望むテーマ）

サイバーセキュリティに関するテーマのうち、「業種・規模・セキュリティへの取組み状況等に関わらず共通的な内容のプラクティスの提供が望まれるもの」と「業種・規模・セキュリティへの取組み状況等に応じて、それらの状況に特化した内容のプラクティスが望まれるもの」が考えられる。現在プラクティ集が取り扱っている各テーマに対し、それぞれどちらの内容のプラクティスが望まれるかを確認した。

「共通的な内容のプラクティスの提供がより望まれるもの」としては、「サイバーセキュリティリスクの認識、組織全体での対応方針の策定」（72.3%）、「情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供」（61.4%）が、それぞれ 6 割を超えるニーズとして確認できた。一方で、「状況に特化した内容のプラクティスの提供がより望まれるもの」としては、「サイバーセキュリティ対策のための資源（予算・人材等）確保」（53.5%）および「インシデントによる被害に備えた復旧体制の整備」（52.4%）の２つのテーマのニーズがやや高い傾向であったものの、6 割を超える企業が選択したテーマは見られなかった（アンケート調査 Q21［図 3-18-1］）。

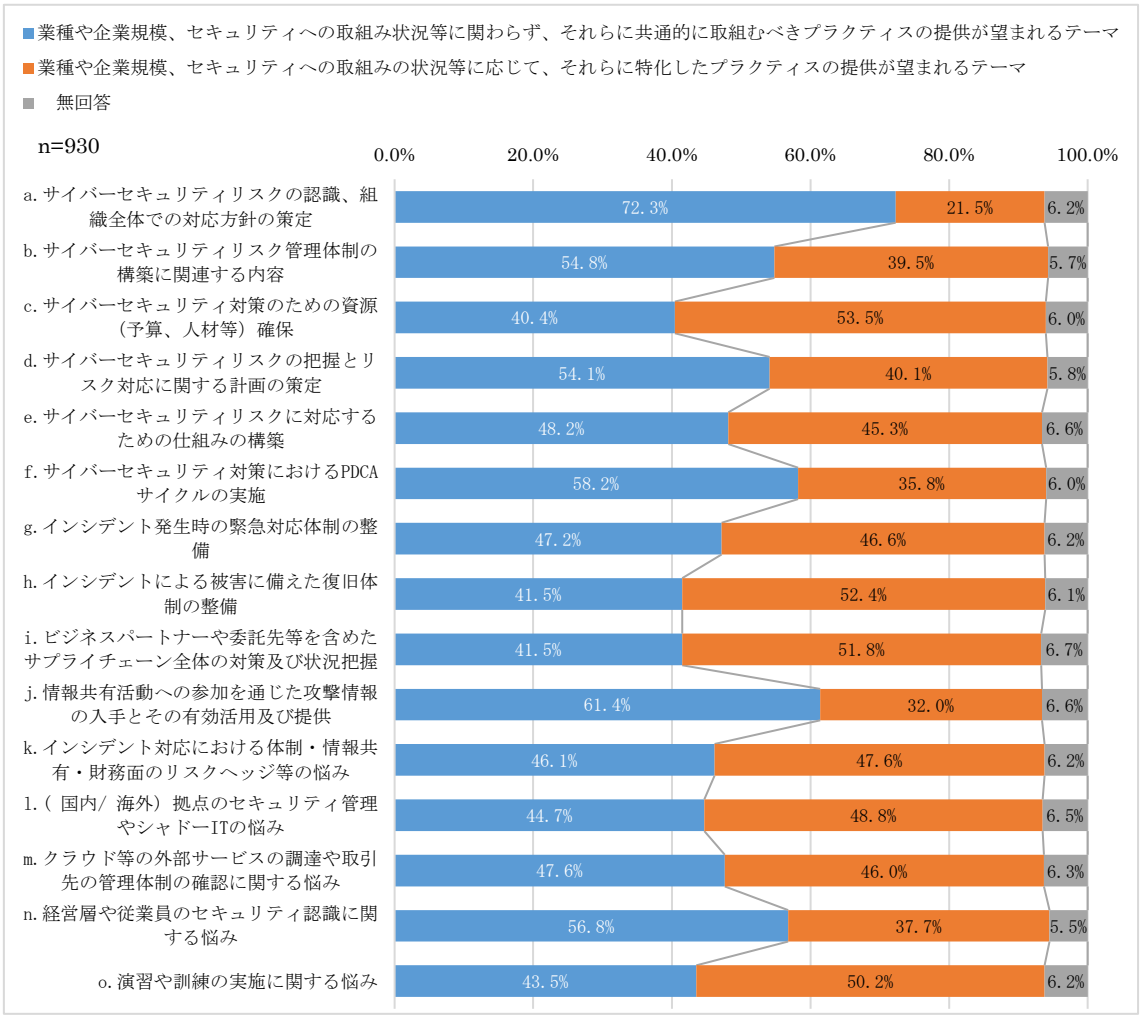


図 3-18-1　共通的なプラクティスを望むテーマと、業種・規模・セキュリティへの取組み状況に特化したプラクティスを望むテーマ

また、業種別の傾向では、全体平均よりも「業種や企業規模、セキュリティへの取組みの状況等に応じて、それらに特化したプラクティスの提供が望まれるテーマ」の回答が多い業種とテーマの組み合わせとして、金融・保険業と「g.インシデント発生時の緊急対応体制の整備」（［図 3-18-2］）、建設業や医療福祉と「h.インシデントによる被害に備えた復旧体制の整備」（［図 3-18-3］）、建設業や金融・保険業と「i.ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握」（［図 3-18-4］）等が確認できた。業種の違いにより、テーマごとに内容のニーズに相違がみられることから、テーマによっては、業種特有の課題があり、独自のアプローチ方法が求められるものも想定される。

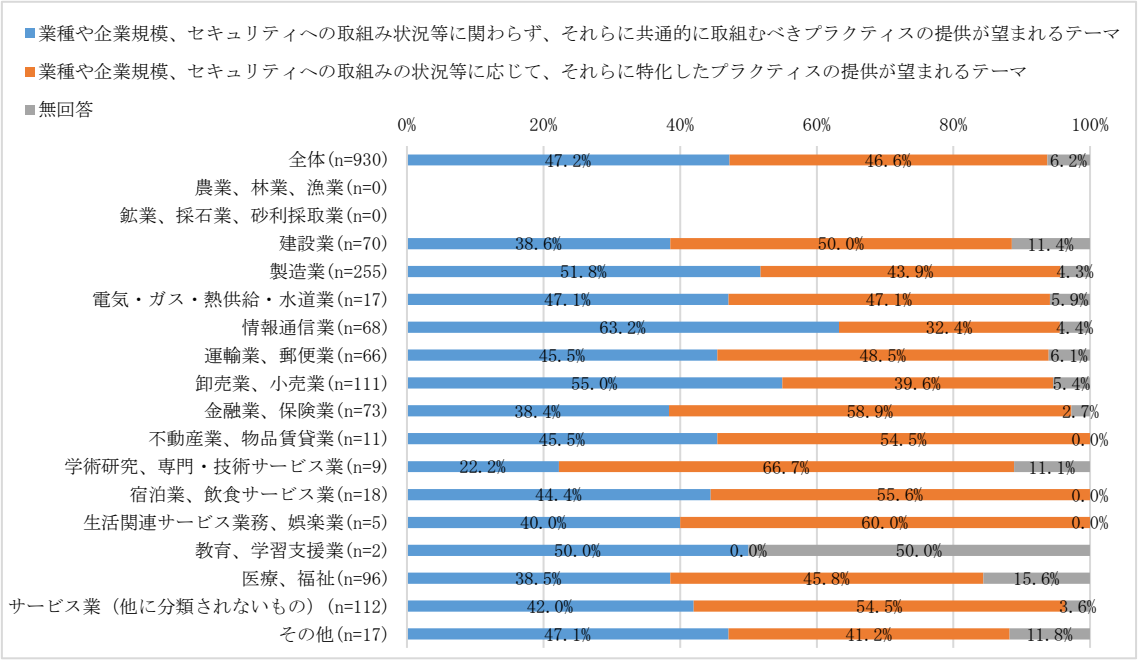


図 3-18-2　共通的なプラクティスを望むテーマと、業種・規模・セキュリティへの取組み状況に特化したプラクティスを望むテーマ（g.インシデント発生時の緊急対応体制の整備）

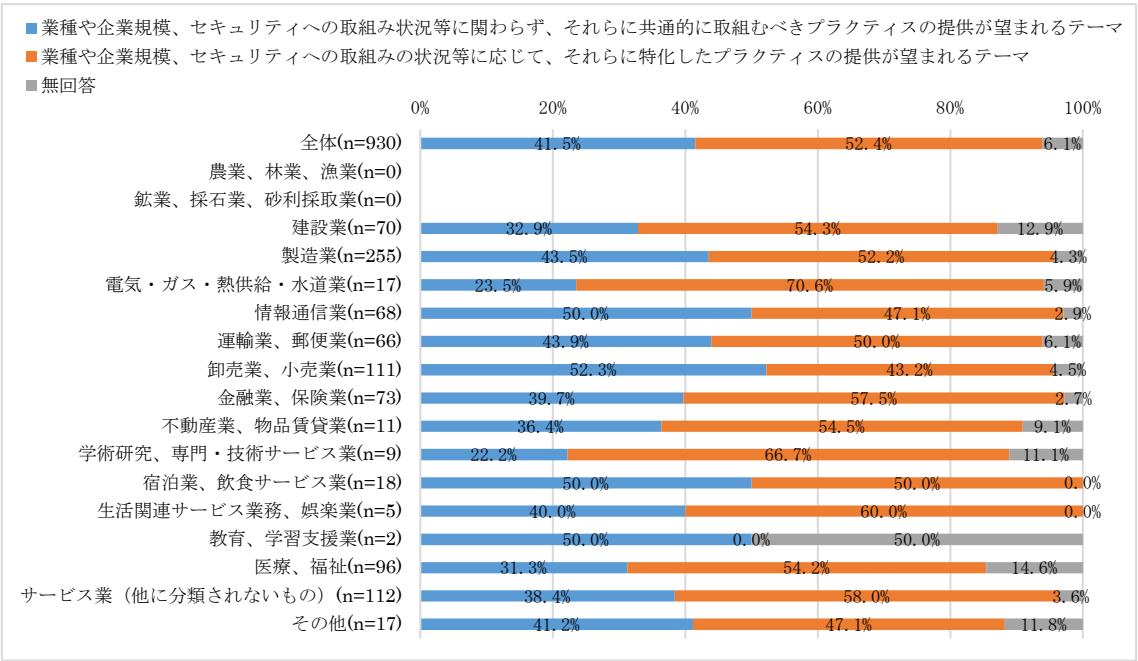


図 3-18-3　共通的なプラクティスを望むテーマと、業種・規模・セキュリティへの取組み状況に特化したプラクティスを望むテーマ（h.インシデントによる被害に備えた復旧体制の整備）

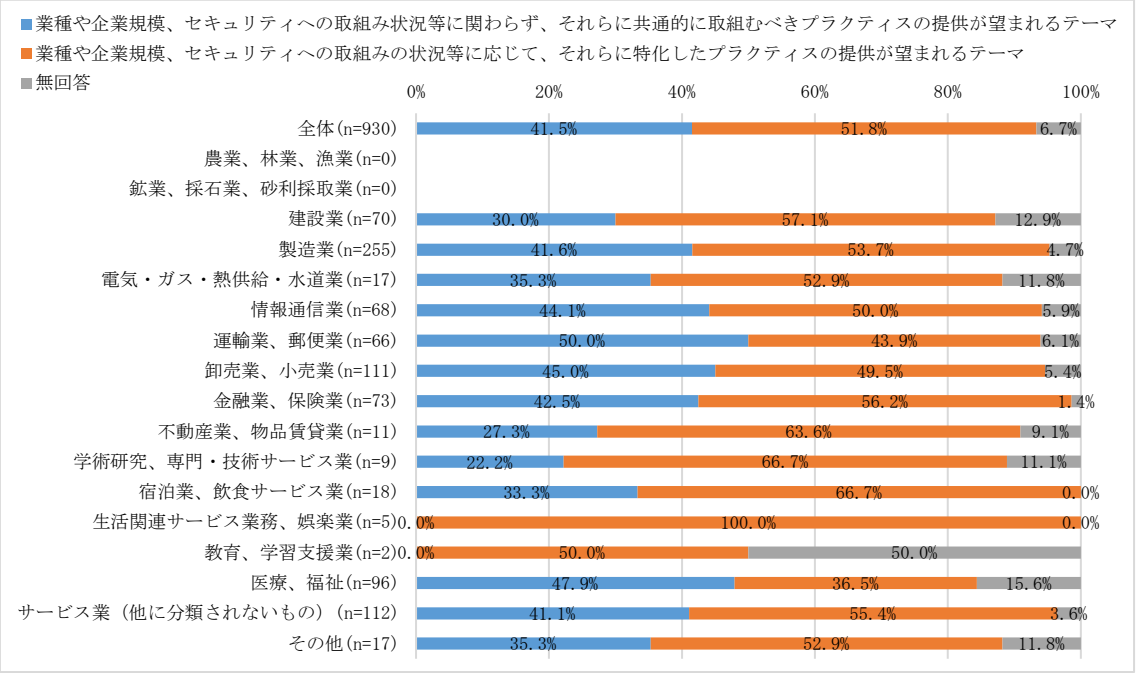


図 3-18-4　共通的なプラクティスを望むテーマと、業種・規模・セキュリティへの取組み状況に特化したプラクティスを望むテーマ（i.ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握）

3.2.2.6 プラクティス集の「作成・共有(企業内での作成・共有)」

（仮説 6）企業は、プラクティスの素材となるようなセキュリティ対策を推進し、文書化のうえ企業内やグループ企業間で共有されている事例もあるのではないか

（企業でのセキュリティ対策の推進・文書化・共有の実態）

現在、プラクティス集は、その作成において、企業のニーズ調査や、インタビューを通じたプラクティスの収集、有識者の査閲等を実施しており、内容について一定の品質が確保できる一方で、機動的な見直しや公表といった観点で課題を有している。

この点を踏まえ、将来的に、企業の関心が高いテーマについて、質の高いプラクティスを機動的に作成・共有できる仕組みの構築を検討する必要がある。その方法として、文献調査の文献 6「METI　新・ダイバーシティ経営ベストプラクティス」にように、企業からプラクティスの応募を募集し選定を経て公表する方法や、複数の企業が共同でプラクティスを作成・共有する枠組みを構築すること等が考えられる。

こうした背景から、今後のプラクティス集の作成・共有の在り方を検討するため、企業におけるサイバーセキュリティ対策の状況、マニュアルや研修教材等への対策内容の文書化、自社内またはグループ企業間での共有の実態について確認した。

サイバーセキュリティに関する各テーマのうち、「対策ができていない」と回答した企業が多いテーマは、「ビジネスパートナーや委託先を含めたサプライチェーン全体の対策」

（64.2%）、「サイバーセキュリティ演習/訓練の実施」（50.4%）、「サイバーセキュリティ管理の内部レビューや監査」（47.2%）であった。一方、「対策の内容や手順をマニュアル・研修教材等に文書化できている」及び「文書化したものを企業内またはグループ企業間で共有している」と答えた企業が多いテーマは、「サイバーセキュリティ関係規程類の策定・見直し」（37.4%）、「サイバーセキュリティリスク管理体制の構築」（34.4%）であった。

管理体制の構築や規程類の策定・見直しといった、サイバーセキュリティ体制の根幹に係る内容については、文書化や社内（グループ内）での共有が進んでいる一方で、資源（予算、人材等）確保やサプライチェーン対策、内部レビューといった発展的なテーマや抽象度が高いテーマについては、文書化や共有化が進んでおらず、ノウハウの蓄積が十分でない実態が窺えた（アンケート調査 Q22［図 3-19］）。

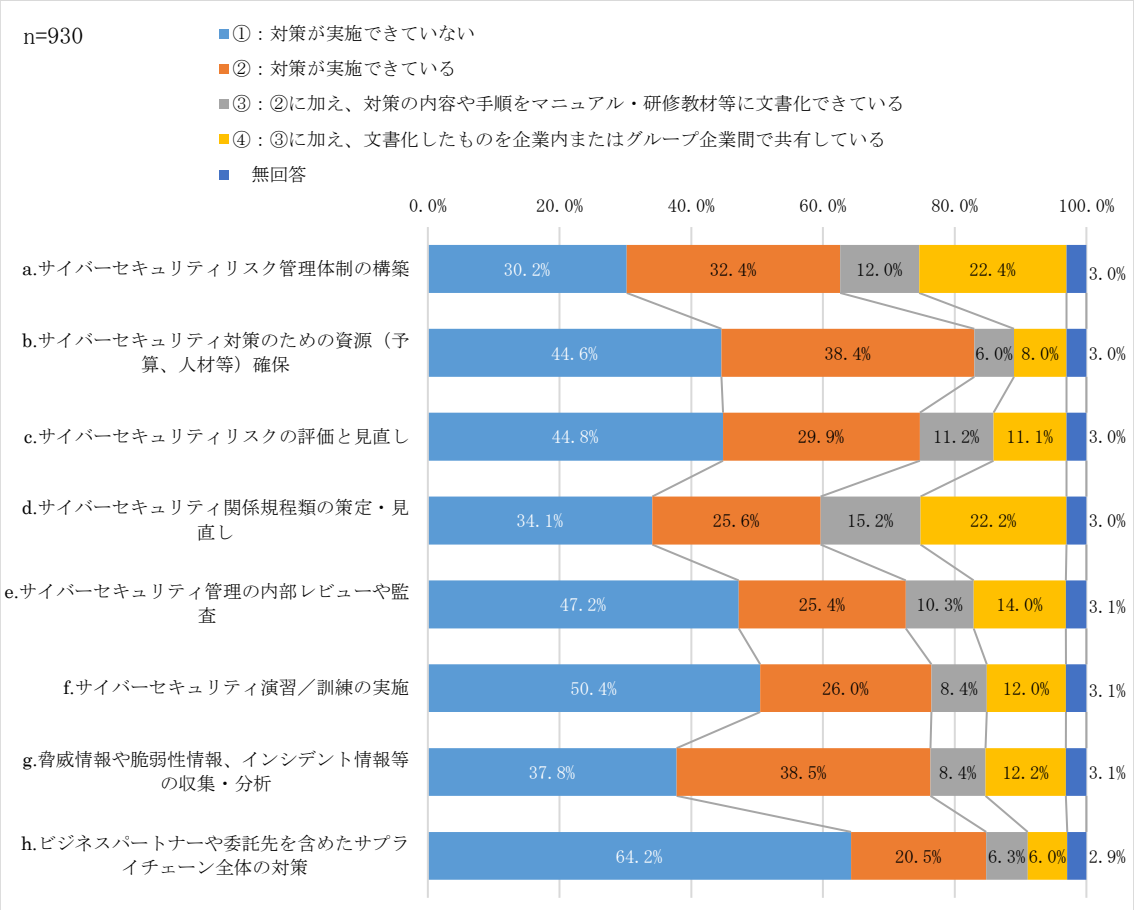


図 3-19　サイバーセキュリティ対策の状況

3.2.2.7 プラクティス集の「作成・共有(他社と共同での作成・共有)」

（仮説 7）企業は、自社がプラクティスの作成・共有に関する取組みに参加するメリットが理解でき、また、作成・共有の体制や枠組み手順が整備されている場合に、こうした取組みに参加したいと考えるのではないか

今後、プラクティス集を複数の企業で、共同で作成・共有する枠組みが構築された場合、その枠組みに自社として参加する意向があるかどうか、またその理由を確認した。

全体として、「必要であり、積極的に協力したいと思う」（10.2%）と「必要であり、機会があれば協力したいと思う」（55.7%）の合計が 6 割を超え、プラクティス集の作成・共有に前向きな企業が多いことがわかった。なお、IT 依存度が高いほど、「必要であり、積極的に協力したいと思う」と「必要であり、機会があれば協力したいと思う」と回答した企業の合計の割合が高い結果であった（アンケート調査 Q23［図 3-20］）。

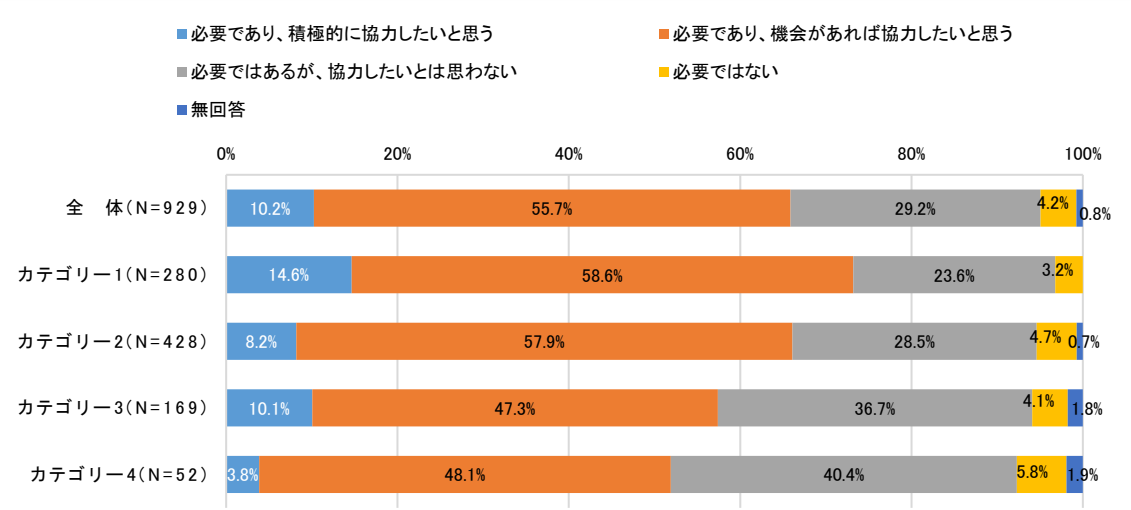


図 3-20　プラクティを共同で作成・共有する枠組みについて

また、「必要であり、積極的に協力したいと思う」または「必要であり、機会があれば協力したいと思う」理由としては、「自社のセキュリティ意識の醸成や対策レベルの向上に寄与すると考えるため」（50.0%）との回答が最も多く、次いで「他社との情報交換ができるため」（32.2%）であった（アンケート調査 Q24［図 3-21］）。

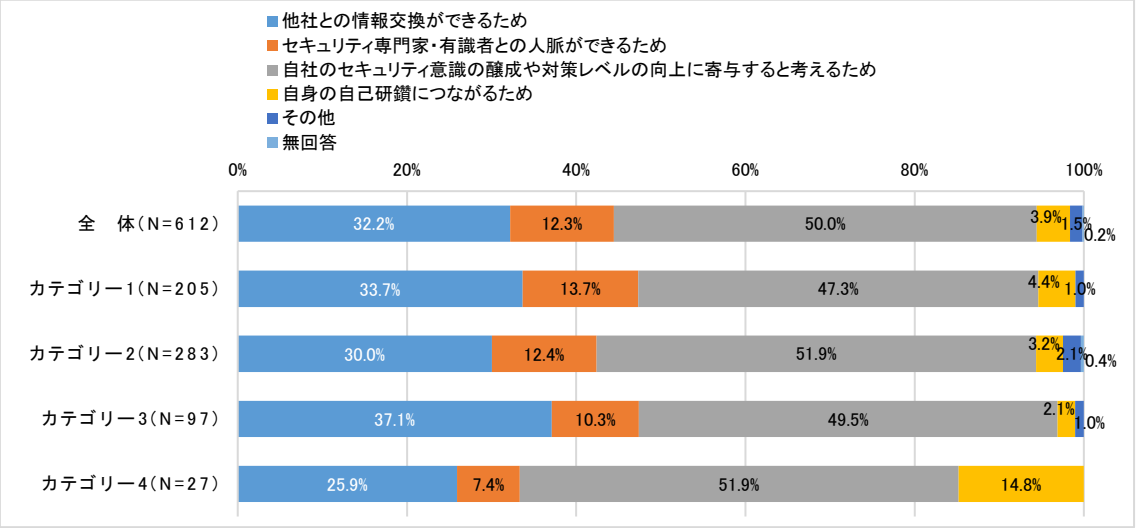


図 3-21　プラクティスを共同で作成・共有する枠組みに協力したいと思う理由

また、「必要ではあるが、協力したいとは思わない」または「必要ではない」と回答した理由については、「取組みに参加する時間がないため」（34.8%）とした回答が最も多く、次いで「プラクティスの素材となるような事例やノウハウの蓄積がないため」（19.4%）であった（アンケート調査 Q25［図 3-22］）。

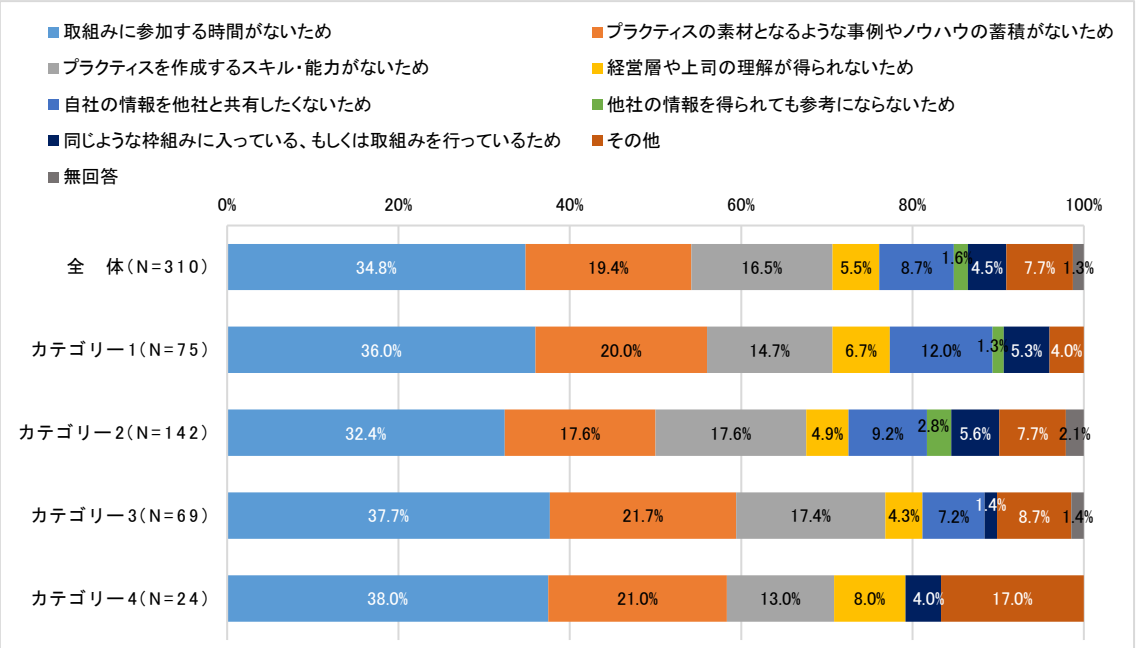


図 3-22　プラクティスを共同で作成・共有する枠組みに協力したいと思わない理由

3.3まとめ

本アンケート調査では、プラクティス集の「認知」「利用」「内容」「作成・共有」のそれぞれの観点から、企業の利用実態やニーズを確認し、IT 依存度を軸に分析を行った。それぞれの観点において、IT 依存度に依らない利用実態やニーズが窺えるとともに、利用目的や全体構成、個々のプラクティスの構成等、IT 依存度により特徴が見られるものもあった。IT 依存度の各カテゴリーに共通する利用実態やニーズの傾向、および IT 依存度のカテゴリーごとの傾向の特徴をまとめると以下の表 3-4 の通りとなる。また、アンケートにおいて設定した仮説の検証結果を表 3-5 に整理した。

プラクティス集の高度化に向けては、企業ユーザーの全体的なニーズを踏まえるとともに、IT 依存度等のプラクティスの利用目的や活用方法に影響を与える要素に着目して企業ユーザーを類型化し、各類型の利用実態やニーズに対応した、構成・内容等の工夫が必要となる。

表 3-4　アンケート調査の結果（IT 依存度ごとの利活用の実態・ニーズの特徴）

分類		IT 依存度の各カテゴリーに共通する傾向	IT 依存度ごとの特徴		
			カテゴリー1 (IT システムが事業上必要不可欠)	カテゴリー2,3 (顧客へのサービス提供や生産活動の一部で IT システムを利用)	カテゴリー4 (IT システムは主に社内業務等に利用)
認知		●「自社でのインシデントの発生」や「DX・テレワーク等の環境変化や IT 投資」をきっかけに認知されるケースが多い	●プラクティス集を既に認知していることが多い ●「DX・テレワーク等の環境変化や IT 投資」をきっかけに認知することが多い	●カテゴリー1 と 4 の中間 ●「自社でのインシデント発生」を契機に認知することが多い	●プラクティス集をまだ認知していないことが多い ●「自社でのインシデント発生」を契機に認知することが多い
利用	利用目的	●「平時の管理体制強化の検討」、「経営層への報告」等の用途に利用されている	●特に「平時の管理体制強化の検討」に活用	●特に「対策が遅れている(新たに対策の必要性が生じた)テーマのはじめの一歩」に活用	●特に「対策全般のはじめの一歩」に活用
	全体構成、提供媒体	●「企業の状況・課題に応じた利用方法、参照すべきプラクティスの解説」や「サイバーセキュリティが経営課題である理由の解説」についてのニーズが高い ●「Web コンテンツとしての提供」を求める	●特に「企業の状況や課題に応じた利用方法、参照すべきプラクティスの解説」を求める	●特に「企業の状況や課題に応じた利用方法、参照すべきプラクティスの解説」を求める	●特に「サイバーセキュリティが経営課題である理由の解説」を求める

分類		IT 依存度の各カテゴリーに共通する傾向	IT 依存度ごとの特徴		
			カテゴリー1 (IT システムが事業上必要不可欠)	カテゴリー2,3 (顧客へのサービス提供や生産活動の一部で IT システムを利用)	カテゴリー4 (IT システムは主に社内業務等に利用)
プラクティスの構成、記載方法		●「企業の状況・課題に応じたプラクティス」や「実現に向けたコストの提示」「プラクティスの優先順位や対策の順番」へのニーズが高い	●特に「企業の状況や課題に応じたプラクティス」を求める ●「リスト形式」または「ストーリー形式」を求める	●特に「実現に向けたコストの提示」を求める ●「リスト形式」または「ストーリー形式」を求める	●特に「プラクティスの優先順位や対策の順番」を求める ●「リスト形式」または「Tips 集」を求める(ストーリー形式は具体的な対応内容がわからない)
内容		●「組織全体の方針策定」や「予算・人材の確保」といったテーマの提供が望まれている	●特に「サイバーセキュリティ対策のための資源確保」のプラクティスを求める	●特に「組織全体の方針策定」のプラクティスを求める	●特に「経営層や従業員のセキュリティ認識に関する悩み」のプラクティスを求める
作成・共有	企業内での作成・共有	●「サプライチェーン対策」や「演習/訓練」「内部監査」等のテーマは、対策ができていない企業が多い	●セキュリティ対策の推進・文書化・共有が進んでいる	●カテゴリー1 と 4 の中間	●セキュリティ対策の推進・文書化・共有が進んでいない
	他社と共同での作成・共有	●「自社の対策強化」や「他社との情報交換の機会」と捉え、プラクティスの作成・共有に前向きな企業が多い ●但し、時間の確保がネックとなる	●どちらかというと、プラクティスの作成・共有の枠組みへの協力に前向き	●カテゴリー1 と 4 の中間	●どちらかというと、プラクティスの作成・共有の枠組みへの協力に後ろ向き

表 3-5　アンケート調査の結果（仮説の検証結果）

分類		N0	仮説	検証結果
認知		仮説1	業種や規模により、プラクティス集の認知度や、認知のきっかけに差があるのではないか	●企業規模や、業種に関連性の高いIT依存度の観点で、プラクティス集の認知に差が見られた ●規模の大きい企業やIT依存度の高い企業ほどプラクティス集の認知が高い(規模や小さい企業やIT依存度の低い企業には十分に認知されていない) （アンケート調査Q1［図3-3］、Q5［図3-4］）
利用	利用目的	仮説2	プラクティス集は、環境変化を踏まえた対策の検討や、資料作成、教育・研修等、幅広い目的で利用されている(利用したいニーズがある)のではないか	●体制構築に向けた「はじめの一歩」から、緊急時の体制構築、通常時の管理体制の強化、経営層への報告等、多様な目的で利用される ●自己研鑽での利用は比較的少ない （アンケート調査Q9［図3-5］、Q10［図3-7］）
	全体構成、提供媒体	仮説3	プラクティス集は、ドキュメント全体(利用方法、付録資料等を含む)の構成について、理解の促進や情報の検索を容易にする工夫を行うことで、利用の促進が図られるのではないか	●企業の状況や課題に応じ参照すべきプラクティスがわかるような構成上の工夫が求められる ●検索性の高いWebコンテンツとしての提供が求められる （アンケート調査Q12［図3-9］、Q15［図3-10］）
	プラクティスの構成、記載方法	仮説4	プラクティス集は、各プラクティスの表現方法や構成要素について、理解の促進や情報の検索を容易にする工夫を行うことで、利用の促進が図られるのではないか	●企業の状況や課題に応じた内容のプラクティスの提供が求められる ●構成要素として、プラクティスを実施するためのコストや費用対効果、対策の優先順位・実施する順番についてのニーズが高い （アンケート調査Q13［図3-13］、Q14［図3-15］）
内容		仮説5	プラクティスにより、幅広い企業の課題認識と合致しているものと、特定の規模や業種に偏ったものがあるのではないか(企業規模や業種に普遍のプラクティスが考えられるのではないか)	●IT依存度や業種によりプラクティスの提供を望むテーマについて、傾向の差が見られた ●組織全体での対応方針の策定等抽象度の高いテーマは規模や業種に共通のプラクティスの提供が望まれる傾向にあり、資源(予算、人材)の確保やインシデント時の体制整備といった個別性の強いテーマは、業種や企業規模に特化したプラクティスの提供が望まれる傾向がやや高い （アンケート調査Q19［図3-17］、Q21［図3-18］）
作成・共有	企業内での作成・共有	仮説6	企業は、プラクティスの素材となるようなセキュリティ対策を推進し、文書化のうえ企業内やグループ企業間で共有されている事例もあるのではないか	●管理体制の構築や規程類の策定等のサイバーセキュリティ体制の根幹に係る内容については、文書化や社内やグループ内での共有が進んでいる ●一方、資源(予算、人材等)確保やサプライチェーン対策等のテーマは、文書化や共有化が進んでおらず、ノウハウの蓄積が十分でない （アンケート調査Q22［図3-19］）
	他社と共同での作成・共有	仮説7	企業は、自社がプラクティスの作成・共有に関する取組みに参加するメリットが理解でき、また、作成・共有の体制や枠組み手順が整備されている場合に、こうした取組みに参加したいと考えるのではないか	●情報共有や従業員の意識醸成等のメリットから、多くの企業で、その必要性・有用性が理解されている ●一方で、共同検討に係る企業のリソース面の課題や、内部情報を外部に共有する際のルール設定の必要性等、課題・乗り越えるべきハードルも存在する （アンケート調査Q23［図3-20］、Q24［図3-21］、Q25［図3-22］）

4 有識者調査

4.1 調査概要

サイバーセキュリティ経営の豊富な知見を有する国内の有識者から、プラクティスの在り方に関する意見や、現在のプラクティスの課題についてインタビュー調査を実施した。有識者インタビュー調査の概要を以下に記載する。

表 4-1　有識者インタビュー調査の概要

調査対象	● 国内有識者　4 名 ➢ 情報セキュリティ関連団体に属する有識者 2 名 ➢ セキュリティベンダー、ユーザー系 IT 企業経営者　1 名 ➢ 航空/情報通信系企業のセキュリティ担当者　1 名
調査期間	2020 年 11 月 30 日～12 月 23 日
主な質問事項	① プラクティス集の「認知」に関して ● プラクティス集の周知方法について
	② プラクティス集の「利活用」に関して ● プラクティスの利活用の目的と、プラクティス集の構成・内容との整合性
	③ プラクティス集の「作成・共有」に関して ● セキュリティ推進の取組みと、情報共有・活用

4.2 調査結果

4.2.1 プラクティス集の「認知」に関して

プラクティス集の認知向上のためには、企業での活用場面を想定のうえ、活用場面のニーズに沿って内容や構成を工夫する必要があるとの見解が得られた。また、プラクティス集は対策が不十分な企業における組織的な活用の促進を図るべきであるが、対策が不十分な企業は自組織の課題を十分把握できていない可能性があるため、セキュリティ成熟度等の評価結果[3]から参照すべきプラクティスがわかるような構成上の工夫が求められるとの示唆も得られた。更に、経営層にプラクティス集を読んでもらうためには、インシデント事例を掲載するなどのインパクトが求められるとの示唆も得られた。加えて、プラクティス集の認知向上に際してセキュリティベンダーに協力を仰ぐためには、プラクティス集に記載されている内容と、セキュリティベンダーのソリューションとを紐づけできるかどうかが重要であるとの見解も得られた。

有識者の主な見解を以下に記載する。

---

[3] サイバーセキュリティの実践状況を企業自身が可視化ツールでセルフチェックした結果のこと

表 4-2 「認知」に関する有識者の主な見解

#	分類	仮説	有識者の主な見解
1	認知	業種や規模により、プラクティス集の認知度や、認知のきっかけに差があるのではないか	（全般的な課題） ● プラクティス集は、担当者個人の読み物として読まれているという印象であり、組織的な活用を促進する必要がある （対策が不十分な企業を想定した工夫） ● プラクティス集は、対策が不十分な企業での活用の促進を目指し、提供方法や内容の工夫、効果的な周知方法を検討していくべきだ ● プラクティス集が活用できる領域や自社で対策が不足している領域が明らかにならないと、組織としての利活用には至らない ● 利活用を促進する手段として、セキュリティ成熟度等の評価結果を示したうえで、評価結果の低い領域について、対策を強化するためのプラクティスを提示するという方法が想定される （セキュリティ担当者を想定した工夫） ● プラクティス集は必ずしも経営層自身に読んでもらう必要はなく、セキュリティの必要性を経営層に説明する際の参考資料(武器)として、セキュリティ担当者が使用するのが有効な使い方であるため、セキュリティ担当者が利用しやすい内容・構成とすべきだ （経営層を想定した工夫） ● 世の中に大きく取り上げられたインシデントの事例を掲載する等、インパクトが重要 （セキュリティベンダーに協力を仰ぐための工夫） ● プラクティス集を効果的に周知・アピールするにあたって、セキュリティベンダーに協力を仰ぐためには、プラクティス集に記載されている内容と、セキュリティベンダーのソリューションとを紐づけできるかどうかが重要である。セキュリティベンダーにとっての営業活動的なメリットがなければ、協力を得るのは難しいと思われる

4.2.2 プラクティス集の「利用」に関して

＜利用目的＞

現在のプラクティス集の第 2 章は、対策が不十分な企業の体制構築のための「模範」「教材」としての活用に適しているとの見解が得られた。一方で、体制構築が一定程度進んだ企業を念頭にした場合、実践的な対策内容を確認したいというニーズが想定されるが、現状の第 2 章および第 3 章はそのニーズには十分対応できていないとの意見もあった。第 3 章を中心とした実践的な対策内容の充実化と、プラクティス集全体を通じた「対策が必要な理由」が伝わるような構成・内容とする工夫が求められると想定される。

有識者の主な見解を以下に記載する。

表 4-3　「利用目的」に関する有識者の主な見解

#	分類	仮説	有識者の主な見解
2	利用	プラクティス集は、環境変化を踏まえた対策の検討や、資料作成、教育・研修等、幅広い目的で利用されている（利用したいニーズがある）のではないか	（体制構築のはじめの一歩としての活用） ● セキュリティにこれから取り組む組織(読者)にとっては、2 章のように体系的に方法論が記載されていると、教材として取組みやすい ● 体制面として「どうあるべきか」が整理されているので、規定を作成したり、何らかのスタンダードを作成したりする用途では利用しやすい （実践的な対策事例としての活用） ● 問題や対処の切り口が体制論であるため、想定される脅威や攻撃に対し、現場レベルでの実践的な対策を検討する場合には利用しにくい ● 事例集としての活用を想定した場合、より多くのプラクティスや参考事例(Tips)を掲載する必要がある （経営層や他部門への報告場面での活用） ● セキュリティの必要性を経営層に説明する際の参考資料(武器)として、セキュリティ担当者が使用するのが有効な使い方である ● 対策の必要性が経営層やセキュリティを知らない事業部門の担当者に上手く伝わらないことがあるが、そのような場合に、プラクティス集を用いて、「他社ではこのような対策を行っている」という説明ができるとよい

＜全体構成、提供媒体＞

対策が不十分な企業を念頭に教材的な位置づけとする場合、「利用方法の解説」や「成熟度に応じたプラクティスの提示」「絵柄を多用して視覚に訴える」等の工夫が有効であるとの示唆が得られた。他方、既に対策が一定程度進んでおり、特定の課題認識を有する企業を念頭にした場合は、プラクティスや事例(Tips)そのものの拡充を図る必要があるとの意見もあった。

有識者の主な見解を以下に記載する。

表 4-4 「全体構成、提供媒体」に関する有識者の主な見解

#	分類	仮説	有識者の主な見解
3	利用	プラクティス集は、ドキュメント全体(利用方法、付録資料等を含む)の構成について、理解の促進や情報の検索を容易にする工夫を行うことで、利用の促進が図られるのではないか	（体制構築のはじめの一歩としての活用） ● 中小企業等がこれから何をやるのかを確認する趣旨で活用する場合、現在の 2 章のような形式がよい ● プラクティス集を教科書的なものとして使用する場合、できるだけ文字は少なくし、視覚的に訴えかけるような絵柄を多く盛り込む必要がある ● どこから手をつけてよいかわからない企業にとっては、プラクティス集の活用方法の解説や、活用事例の紹介は有効 （実践的な対策事例としての活用） ● 事例集としてのニーズを満たす点では、利用方法の解説や実施手順のリストを作るのではなく、プラクティスそのものを充実させることが重要 ● 特定の課題認識を有する組織が、その課題を解決するために、ピンポイントで必要な箇所を読むという形式を志向すべき （その他提供媒体に関する工夫） ● 企業側からの質問や情報の追補機能等、双方向でコミュニケーションが取れるような工夫が求められるのではないか

＜プラクティスの構成、記載方法＞

対策が必要な理由が伝わるような工夫が必要であり、例えば他社でのインシデントの事例を掲載することが考えられるとの見解が得られた。プラクティスの記載方法については、具体的な対策内容をイメージしやすい方法として、Tips 形式や対策項目のリストアップが有効であるとの意見があった。ただし、企業の状況や課題の違いを踏まえた具体化・細分化には限界があるため、基本的な対策内容はストーリー形式で記載し、リスト化できない部分は行間を読み取ってもらうような工夫が必要であると想定される。

有識者の主な見解を以下に記載する。

表 4-5 「プラクティスの構成、記載方法」に関する有識者の主な見解

#	分類	仮説	有識者の主な見解
4	利用	プラクティス集は、各プラクティスの表現方法や構成要素について、理解の促進や情報の検索を容易にする工夫を行うことで、利用の促進が図られるのではないか	（読者の理解度を向上させるための構成面での工夫） ● 読者に内容を印象付けるための工夫として、取組みのメリットや、取組みを行わない場合のリスクを記載する ● 後者の例として、他社でのインシデント事例の掲載が有効 ● 記載の順番として、指示項目や悩みから解説を行うよりも、インシデントの事例から関連する指示内容や悩みのプラクティスを解説した方が読者の印象に残りやすい （記載方法について） ● ストーリー形式は、読み物としては有効だが、何らかの具体的な対策を検討する場合、自社の状況に当てはめて考えるのが難しく使い勝手が悪い ● Tips 形式で、具体的な対策のイメージを記載したほうが使いやすい ● 中小企業と大企業で同じ対策手順を参考にするのは無理がある ● リストに明文化できない部分(所謂“行間”の部分)については、シナリオベースのプラクティスで読み取ってもらうのが有効。また、絶対的な正解として示してしまうと、担当者の思考停止に繋がりかねない

4.2.3 プラクティス集の「内容」に関して

企業が現実に直面している課題とその対処方法について、理解しやすいように構成や内容面を工夫して取扱う必要があるとの見解が得られた。また、テレワーク・クラウド利用・DX など最近のトレンドとなっているテーマについても、一定程度、対策内容の議論・標準化が進んで段階において、テーマとしての取扱いを検討することが求められるとの意見もあった。加えて、取り扱うテーマの内容が現在の企業の課題にマッチしていないという意見もあった。

有識者の主な見解を以下に記載する。

表 4-6　「内容」に関する有識者の主な見解

#	分類	仮説	有識者の主な見解
5	内容	プラクティスにより、幅広い企業の課題認識と合致しているものと、特定の規模や業種に偏ったものがあるのではないか(企業規模や業種に普遍のプラクティスが考えられるのではないか)	（プラクティスが取り扱うテーマについて） ● 企業が現実的に直面している課題やデファクト・スタンダードとなった脅威について、その対処方法が豊富に掲載されているべきである ● テレワークやクラウド利用・DX 推進における“攻めのセキュリティ”など、最近のトレンドを盛り込む必要がある ● 問題の切り方が ISMS なのが実践的ではない。(規定や体制整備自体が進んでいない) 2005 年ぐらいの状況にマッチする資料のイメージであり、2020 年現在の課題に適合していない （読者の理解度を向上させるための構成・内容面での工夫) ● 読者に内容を印象付けるための工夫として、取組みのメリットや、取組みを行わない場合のリスクを記載する ● 後者の例として、他社でのインシデント事例の掲載が有効

4.2.4 プラクティス集の「作成・共有」に関して

＜作成・共有（企業・グループ内）＞

サイバーセキュリティ対策が進んでいる企業では、インシデントの事例等から独自にプラクティスを作成し、自社・グループ間で共有を行っている事例があるとの見解が得られた。こうした企業は、対外的に公表を行っていないが、プラクティスの作成・共有に関する何らかのノウハウを有している可能性がある。

有識者の主な見解を以下に記載する。

表 4-7 「作成・共有（企業・グループ内)」に関する有識者の主な見解

#	分類	仮説	有識者の主な見解
6	作成・共有	企業は、プラクティスの素材となるようなセキュリティ対策を推進し、文書化のうえ企業内やグループ企業間で共有されている事例もあるのではないか	（プラクティスの作成および自社・グループ間での共有について） ● 自社では、プラクティスの作成・共有を実施しており、特定の領域についてのノウハウが体系化されている ● 自社では、インシデントの発生事例からプラクティスを作成・共有している ● プラクティスを作成している企業はそれほど多くはないと想定される ● 対外的に発表を行っていないケースでも、セキュリティに関する独自の知見・ノウハウを蓄積している企業はあると想定される

＜作成・共有（他社）＞

様々な情報や考え方・バックグラウンドを有するメンバーが集まり、知見を活かすことで、プラクティスの内容の充実化が図られるとともに、参加するサイバーセキュリティ人材のモチベーション向上につながるとの示唆が得られた。一方で、情報を社外に提供することには一定のリスクが存在するため、情報共有ルールの構築や、情報の選別・加工・抽象化等の対策が必要であるとの意見もあった。

有識者の主な見解を以下に記載する。

表 4-8 「作成・共有（他社)」に関する有識者の主な見解

#	分類	仮説	有識者の主な見解
7	作成・共有	企業は、自社がプラクティスの作成・共有に関する取組みに参加するメリットが理解でき、また、作成・共有の体制や枠組み手順が整備されている場合に、こうした取組みに参加したいと考えるのではないか	（プラクティスを他社と共同作成するうえでのハードル） ● プラクティスの素材を社外に公表することには一定のリスクがあるが、情報共有のルールや匿名化等の措置を講じることで、安全性が保障されればハードルは解消可能 ● 社外に公表するためには、情報を一定程度、選別・加工・抽象化することが必要である （プラクティスを他社と共同作成するメリット） ● 様々な参加者の知見を活かすことができるため、内容の深化が図られる ● セキュリティに関わる人材に社内にとどまらない活躍の場を提供することができ、モチベーションの向上につながる （企業がプラクティスを作成・共有する場合のフォーマット） ● OSS 化してみるのが手である。読者が自由にコメントできて、エディターが最終責任を持つという形がよい。様々な参加者の知見が最終的にドキュメントとして纏まっていくのが理想的である

4.3 有識者調査結果のまとめ

有識者調査では、プラクティス集の「認知」、「利活用」、「作成・共有」の観点から、プラクティス集の改善に繋がる幅広い意見を収集した。

有識者調査から得られたプラクティス集の改善のポイントを以下に記載する。

- プラクティス集の「認知」に関して
  - ✓ プラクティス集の認知向上のためには、企業での活用場面を想定のうえ、活用場面のニーズに沿って内容や構成を工夫する必要がある
  - ✓ 対策が不十分な企業向けには、セキュリティ成熟度等の評価結果から参照すべきプラクティスがわかるような構成上の工夫が求められる
- プラクティス集の「利活用」に関して
  - ✓ 可視化ツールとプラクティス集を連携することで、可視化ツールでの診断結果と、その診断結果に対応するプラクティスを、一連の流れで確認できれば有効である
  - ✓ 体制構築が一定程度進んだ企業を念頭にした場合、実践的な対策内容を確認したいというニーズが想定されるが、現状の第 2 章および第 3 章はそのニーズには十分対応できておらず、第 3 章を中心とした実践的な対策内容の充実化と、プラクティス集全体を通じた「対策が必要な理由」が伝わるような構成・内容とする工夫が求められる
  - ✓ 対策が不十分な企業を念頭に教材的な位置づけとする場合、「利用方法の解説」や「成熟度に応じたプラクティスの提示」「絵柄を多用して視覚に訴える」等の工夫が有効である。他方、既に対策が一定程度進んでおり、特定の課題認識を有する企業を念頭にした場合は、プラクティスや事例(Tips)そのものの拡充を図る必要がある
  - ✓ 対策が必要な理由が伝わるような工夫が必要であり、例えば他社でのインシデントの事例を掲載することが考えられる
  - ✓ 具体的な対策内容をイメージしやすい方法として、Tips 形式や対策項目のリストアップが有効である。ただし、企業の状況や課題の違いを踏まえた具体化・細分化には限界があるため、基本的な対策内容はストーリー形式で記載し、リスト化できない部分は行間を読み取ってもらうような工夫が必要である
  - ✓ 企業が現実に直面している課題とその対処方法について、理解しやすいように構成や内容面を工夫して取扱う必要がある。また、テレワーク・クラウド利用・DX など最近のトレンドとなっているテーマについても、一定程度、対策内容の議論・標準化が進んで段階において、テーマとしての取扱いを検討することが求められる
- プラクティス集の「作成・共有」に関して
  - ✓ サイバーセキュリティ対策が進んでいる企業では、インシデントの事例等から独自にプラクティスを作成し、自社・グループ間で共有を行っている事例がある

- ✓ 様々な情報や考え方・バックグラウンドを有するメンバーが集まり、知見を活かすことで、プラクティスの内容の充実化が図られるとともに、参加するサイバーセキュリティ人材のモチベーション向上につながる
- ✓ 情報を社外に提供することには一定のリスクが存在するため、情報共有ルールの構築や、情報の選別・加工・抽象化等の対策が必要である

5 企業調査

5.1 調査概要

プラクティスの想定利用者である国内企業から、プラクティスの在り方に関する意見や、現在のプラクティスの課題について、インタビュー調査を実施した。企業インタビュー調査の概要を以下に記載する。

表 5-1　企業インタビュー調査の概要

調査対象	プラクティスの想定利用者である国内企業　6 社
調査期間	2020 年 12 月 16 日～2021 年 2 月 17 日
主な質問事項	① プラクティス集の「認知」に関して ● プラクティス集の周知方法について
	② プラクティス集の「利活用」に関して ● プラクティスの利活用の目的と、プラクティス集の構成・内容との整合性
	③ プラクティス集の「作成・共有」に関して ● セキュリティ推進の取組みと、情報共有・活用

5.2 調査結果

5.2.1 プラクティス集の「認知」に関して

プラクティス集の認知向上のためには、企業での活用場面を想定のうえ、活用場面のニーズに沿って内容や構成を工夫する必要があるとの見解が得られた。また、業界団体へのアプローチや、Web コンテンツでの提供とセットでの SEO 対策、想定読者を意識した内容の拡充等が必要であるとの意見もあった。

企業の主な見解を以下に記載する。

表 5-2　「認知」に関する企業の主な見解

#	分類	仮説	企業の主な見解
1	認知	業種や規模により、経営ガイドライン実践のためのプラクティス集の認知度や、認知のきっかけに差があるのではないか	（想定読者を念頭においたアプローチ） ● 総務や情シス等のセキュリティ担当者が想定読者と考えられるが、テレワークやシャドーIT 等、課題が山積みである一方で、専任人材が不足しているケースが多く想定される。こうした課題に応える内容であれば認知や利活用が進むのではないか ● セキュリティに関する情報共有機関や業界団体にアプローチする方法が考えられる ● 経営層に対しては、経営層が集まる場(経団連など)でプラクティス集の存在をアナウンスするなど、セキュリティ担当者向けとは違ったアプローチが考えられる （その他） ● Web コンテンツとして提供し、SEO 対策を行う

5.2.2 プラクティス集の「利用」に関して

＜利用目的＞

プラクティス集は、情報システム部門や総務部門等のセキュリティ担当者が、経営層や他部門へセキュリティ対策が必要な理由等を説明する際に活用すると想定されるとの見解が得られた。また、上記のような説明の場面では、他社の対策状況や自社の立ち位置がわかるような構成上の工夫があれば活用しやすいとの意見があった。

企業の主な見解を以下に記載する。

表 5-3　「利用目的」に関する企業の主な見解

#	分類	仮説	企業の主な見解
2	利用	プラクティス集は、環境変化を踏まえた対策の検討や、資料作成、教育・研修等、幅広い目的で利用されている(利用したいニーズがある)のではないか	(利用目的) ● 総務や情シス等のセキュリティ担当者が想定読者と考えられるが、テレワークやシャドーIT 等、課題が山積みである一方で、専任人材が不足しているケースが多く想定される。こうした課題に応える内容であれば認知や利活用が進むのではないか ● 経営層は他社の対策状況について関心が高い。経営層への説明を念頭に、他社の対策状況や自社の立ち位置が伺い知れるような内容が提供できれば、利活用が促進されるのではないか

＜全体構成、提供媒体＞

セキュリティ成熟度や企業規模、業態等により目指すべき対策のレベルや実現のステップが異なるため、自社の状況や課題を診断し、その結果に応じて参照すべきプラクティスがわかるような工夫が求められるとの見解が得られた。また、可視化ツールとの連携に際しての意見も得られた。

企業の主な見解を以下に記載する。

表 5-4 「全体構成、提供媒体」に関する企業の主な見解

#	分類	仮説	企業の主な見解
3	利用	プラクティス集は、ドキュメント全体(利用方法、付録資料等を含む)の構成について、理解の促進や情報の検索を容易にする工夫を行うことで、利用の促進が図られるのではないか	（全体構成） ● 自社の課題を診断でき、その課題に応じて参照すべきプラクティスがわかるような構成がよい ● 業種等の観点から他社との比較ができるとよい ● これらが Web コンテンツとしてオンラインで参照できるとよい ● セキュリティは、企業規模や業態によってどこまで対策できるのかが変わってくる。早見表のような形式で、企業規模や業態別にプラクティスが整理されていればよい ● オンラインで質問に答える（オンラインでの脆弱性診断）と、プラクティス集の該当箇所に導かれるというような形式はいかがか （可視化ツールとの連携に際しての工夫） ● 可視化ツールとプラクティス集を連携することで、可視化ツールでの診断結果と、その診断結果に対応するプラクティスを、一連の流れで確認できれば有効である ● 現場が取り組みを行っているにもかかわらず、セキュリティレベルがなかなか向上しない場合、現場のモチベーション低下にも繋がりかねない。可視化の仕組みを検討する際に留意すべき点である

＜プラクティスの構成、記載方法＞

企業は自社の課題に応じたプラクティスを求めているため、業種やシチュエーションごとの事例が充実化するとより活用しやすいとの見解が得られた。また、経営層への報告場面においては、他社のインシデント事例が有効であるとの意見もあった。

企業の主な見解を以下に記載する。

表 5-5 「プラクティスの構成、記載方法」に関する企業の主な見解

#	分類	仮説	企業の主な見解
4	利用	プラクティス集は、各プラクティスの表現方法や構成要素について、理解の促進や情報の検索を容易にする工夫を行うことで、利用の促進が図られるのではないか	（読者の理解度を向上させるための構成面での工夫） ● プラクティスを自社の課題としてとらえるためには、自社に近しい業種の事例や、自社のシチュエーションに合致した事例の紹介が有効 ● 読者に内容を印象付けるための工夫として、他社でのインシデント事例の掲載が有効 ● 記載の順番として、これから対策を進める企業には、指示項目や悩みから解説を行い、ある程度対策が進んだ企業にはインシデントの事例をから関連する指示内容や悩みのプラクティスを解説する方が読者の印象に残りやすい （記載方法について） ● 目的によりストーリー形式が適している場合と、リスト形式や Tips 形式が適している場合の両方が想定される

5.2.3 プラクティス集の「内容」に関して

企業が現実に直面している課題とその対処方法について、理解しやすいように構成や内容面を工夫して取扱う必要があるとの見解が得られた。また、テレワーク・クラウド利用・DX など最近のトレンドとなっているテーマについても、一定程度、対策内容の議論・標準化が進んで段階において、テーマとしての取扱いを検討することが求められるとの意見もあった。

企業の主な見解を以下に記載する。

表 5-6　「内容」に関する企業の主な見解

#	分類	仮説	企業の主な見解
5	内容	プラクティスにより、幅広い企業の課題認識と合致しているものと、特定の規模や業種に偏ったものがあるのではないか(企業規模や業種に普遍のプラクティスが考えられるのではないか)	（プラクティスが取り扱うテーマについて） ● 企業が現実的に直面している課題や脅威について、その対処に有用なコンテンツが提供されるとよい ● テレワークやクラウド利用・DX 推進・ランサムウェア感染への対処等、最近のトレンドを盛り込む必要がある ● 同一規模の企業が経営環境の変化にどう対応しているかを知りたい ● インシデント対応の具体例が欲しい ● 当社は事業が非常に幅広いため、必ずしも実態にそぐわないプラクティスがあり、事業ごとに読み替えが必要であると認識している （読者の理解度を向上させるための構成・内容面での工夫） ● 人材育成や技術的対処等のテーマは、業種や企業規模に特有の課題があるため、業種や企業規模の違いによる内容を補足説明した方がよい ● 読者の関心を惹起するためには、取り組みを進めていくうえで苦労したことなど、もう少し生の声を記載すると有効かもしれない

5.2.4 プラクティス集の「作成・共有」に関して

＜作成・共有（企業・グループ内）＞

サイバーセキュリティ対策が進んでいる企業では、プラクティスの素材となる知見の蓄積が図られている。また、内外のインシデント対応の記録をベースに、社内教材や演習のシナリオ検討に生かしている事例も存在する。

企業の主な見解を以下に記載する。

表 5-7 「作成・共有（企業・グループ内)」に関する企業の主な見解

#	分類	仮説	企業の主な見解
6	作成・共有	企業は、プラクティスの素材となるようなセキュリティ対策を推進し、文書化のうえ企業内やグループ企業間で共有されている事例もあるのではないか	（プラクティスの作成および自社・グループ間での共有について） ● 自社では、インシデント対応の事例から定期的に社内教材を策定し、全社員を対象に受講させている ● 自社では、毎年の BCP 訓練において独自のシナリオを策定して実施している

＜作成・共有（他社）＞

プラクティスを他社と共同作成する取組みの必要性について、企業の立場から理解が示された一方で、リソース面での課題が提起された。また、情報を社外に提供することには一定のリスクが存在するため、情報共有ルールの構築や、情報の選別・加工・抽象化等の対策が必要であるとの意見もあった。加えて、何らかのフォーマットを指定し、そこに企業がプラクティスを記載する場合、実態を記載するのは難しいのではないかとの見解も得られた。

企業の主な見解を以下に記載する。

表 5-8 「作成・共有（他社)」に関する企業の主な見解

#	分類	仮説	企業の主な見解
7	作成・共有	企業は、自社がプラクティスの作成・共有に関する取組みに参加するメリットが理解でき、また、作成・共有の体制や枠組み手順が整備されている場合に、こうした取組みに参加したいと考えるのではないか	（プラクティスを他社と共同作成するうえでのハードル） ● プラクティスの素材を社外に公表することには一定のリスクがあるが、情報共有のルールや匿名化等の措置を講じることで、安全性が保障されればハードルは解消可能 ● 社外に公表するためには、情報を一定程度、選別・加工・抽象化することが必要である ● リソース面での課題を念頭にすると、テーマ選定のみ関与し、コンテンツの作成自体は事務局で対応するといった方法が想定される （企業がプラクティスを作成・共有する場合のフォーマット） ● 何らかのフォーマットを指定してプラクティスを記載してもらう場合、実態をそのまま記載いただくことは難しいのではないか （情報共有に際しての工夫） ● 情報共有に関しては、お互いの信頼関係があることが前提となる。当社では、情報共有ではなく情報“共感”という言い方をしている。単に情報を共有するのではなく、内容に共感いただくことが重要である ● IPA の人材育成プログラムの卒業生の中で情報共有するのは有効だと思われる。お互いに信頼関係が出来ているため、生の情報を共有することが出来る

5.3 企業調査結果のまとめ

企業調査では、プラクティス集の「認知」、「利活用」、「作成・共有」の観点から、プラクティス集の改善に繋がる幅広い意見を収集した。

企業調査から得られたプラクティス集の改善のポイントを以下に記載する。

- プラクティス集の「認知」に関して
  - ✓ プラクティス集の認知向上のためには、企業での活用場面を想定のうえ、活用場面のニーズに沿って内容や構成を工夫する必要がある
  - ✓ 業界団体へのアプローチや、Web コンテンツでの提供とセットでの SEO 対策、想定読者を意識した内容の拡充等が必要である
- プラクティス集の「利活用」に関して
  - ✓ 可視化ツールとプラクティス集を連携することで、可視化ツールでの診断結果と、その診断結果に対応するプラクティスを、一連の流れで確認できれば有効である
  - ✓ プラクティス集は、情報システム部門や総務部門等のセキュリティ担当者が、経営層や他部門へセキュリティ対策が必要な理由等を説明する際に活用すると想定されるが、このような説明の場面では、他社の対策状況や自社の立ち位置がわかるような構成上の工夫があれば活用しやすい
  - ✓ セキュリティ成熟度や企業規模、業態等により目指すべき対策のレベルや実現のステップが異なるため、自社の状況や課題を診断し、その結果に応じて参照すべきプラクティスがわかるような工夫が求められる
  - ✓ 企業は自社の課題に応じたプラクティスを求めているため、業種やシチュエーションごとの事例が充実化するとより活用しやすい
  - ✓ 企業が現実に直面している課題とその対処方法について、理解しやすいように構成や内容面を工夫して取扱う必要がある。また、テレワーク・クラウド利用・DX など最近のトレンドとなっているテーマについても、一定程度、対策内容の議論・標準化が進んで段階において、テーマとしての取扱いを検討することが求められる
- プラクティス集の「作成・共有」に関して
  - ✓ サイバーセキュリティ対策が進んでいる企業では、プラクティスの素材となる知見の蓄積が図られている
  - ✓ 内外のインシデント対応の記録をベースに、社内教材や演習のシナリオ検討に生かしている事例も存在する
  - ✓ プラクティスを他社と共同作成する取組みの必要性について、企業の立場から理解が示された一方で、リソース面での課題を克服する必要がある
  - ✓ 情報を社外に提供することには一定のリスクが存在するため、情報共有ルールの構築や、情報の選別・加工・抽象化等の対策が必要である

6 まとめ・今後のプラクティス集の在り方

6.1 調査結果のまとめ

本調査では、文献調査により、サイバーセキュリティやIT、その他テーマに関するプラクティスの作成プロセスや、構成・内容面の工夫の事例を確認したうえで、アンケート調査により、現在のプラクティス集の利用実態やニーズを、IT 依存度を軸に定量的に分析した。加えて、有識者調査および企業調査にて、専門的な見地や企業実務における経験から、プラクティスの利用ニーズや内容・構成面の課題や改善の方向性について、個別具体的に見解をヒアリングした。

本章では、これらの結果を踏まえ、プラクティス集の今後の内容の見直しや、作成・共有を含めた在り方について取りまとめる。

6.1.1 企業像に応じたプラクティスへのニーズ

一連の調査結果より、プラクティス集を活用する企業は大きく以下の 3 類型に分類できると考えられる（[図 6-1]）。まずは、この企業像ごとに、プラクティス集の利用実態やニーズを以下に整理する。

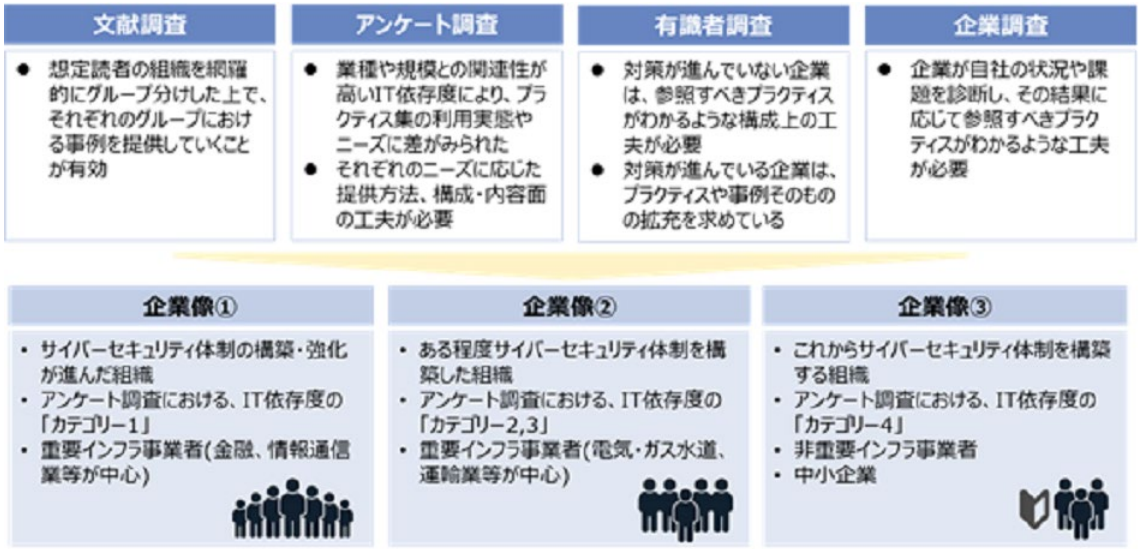


図 6-1 各調査結果を踏まえたプラクティス集の活用企業像

企業像①：サイバーセキュリティの取組みが進んでいる企業

当該の企業像は、アンケート調査における IT 依存度の「カテゴリー1」に該当する企業、すなわち、すなわち「IT システム・IT サービスが事業上必要不可欠な要素であり、その停止は事業全体または重要な事業の停止に繋がる（金融、通販、ネット通販等）」企業を想定している。なお、

IT 依存度のカテゴリー1 に該当する企業は、他のカテゴリーの企業と比較して、事業規模の観点では大企業が、業種の観点では重要インフラ事業者とりわけ金融業や情報通信業が多い。

当該の企業像は、サイバーセキュリティの取組みが進んでおり、自社の課題や取組みが必要な領域・テーマについて把握できている。このため、プラクティス集の利用は、「新たに取組みが必要なテーマの体制強化」「セキュリティ対策の経営層への報告」等が主な目的となる。これを踏まえると、当該層に有効なプラクティス集の形態としては、IT に関連する新たな取組みを実施する際に、管理体制の構築や PDCA サイクルの実施をどのように図るかといった観点から現在の第 2 章の形態が、加えて、企業像②と同様、直近の IT やセキュリティトレンドも加味した新たなテーマに関する対策の確認を想定した第 3 章の形態、この両方が必要と考えられる。

プラクティス集の全体構成・提供媒体へのニーズという観点では、その他の企業像と同様に、「自社の状況や課題に応じ、参照すべきプラクティスがわかる」「自社の状況や課題に応じたプラクティスが掲載されている」等に強いニーズがある。なお、その他の企業像よりも、上記（自社の状況や課題に応じたプラクティス）のニーズが強い。また、個別のプラクティスの構成についても、概ねその他の企業像と同様、「プラクティス実現に向けたコストや費用対効果・人的スキル」「プラクティスの優先有順位や対策を実施する順番」「対策が必要な理由の説明(他社でのインシデント事例等)」「業種ごとの特徴を踏まえたプラクティス」へのニーズが高い。なお、プラクティスの記載方法については、企業像②と同様に、ストーリー形式またはリスト形式のニーズが強い。また、有識者より、対策が進んでおり明確な課題認識を有する企業は、プラクティスの活用方法について丁寧な解説は求めておらず、むしろ様々なテーマに関して具体的な対応事例が豊富に掲載されていることが重要との見解もあげられた。企業調査においても、CSIRT 等で実務にあたるメンバーとしては、事例が豊富に掲載されていることや、業種・事業規模・システムの特性等に応じたプラクティスが掲載されていることについてのニーズが把握できた。

企業像②：サイバーセキュリティの取組みがある程度進んでいる企業

当該の企業像は、アンケート調査における IT 依存度の「カテゴリー2 または 3」に該当する企業、すなわち「顧客へのサービス提供や生産活動の一部で IT システム・IT サービスを利用しており、その停止は事業の一部に大きく影響する（重要インフラ業種等）」企業（カテゴリー2）、または「顧客へのサービス提供や生産活動の一部で IT システム・IT サービスを利用しているが、IT に依存しない代替手段等があるため、一時的な停止であれば事業への影響は小さい」企業（カテゴリー3）を想定している（アンケート調査において、カテゴリー2 と 3 には利用実態やニーズの観点で大きな傾向の差は見られなかった）。なお、IT 依存度のカテゴリー2 または 3 に該当する企業は、他のカテゴリーの企業と比較して、事業規模の観点では中堅企業が、業種の観点では重要インフラ事業者が多い。

当該の企業像は、サイバーセキュリティの取組みはある程度進んでおり、自社の課題や取組みが必要な領域・テーマもある程度把握できている。このため、プラクティス集の利用は、「取組みが遅れているテーマの体制強化」や「新たに取組みが必要なテーマに関する対策の確認」「セキュリ

ティ対策の経営層への報告」等が主な目的となる。(アンケート調査 Q10)。これを踏まえると、当該層に有効なプラクティス集の形態としては、体制面で取組みが遅れている論点の確認を想定した現在の第 2 章に加え、直近の IT やセキュリティのトレンドも加味した新たなテーマに関する対策の確認を想定した第 3 章の形態、両方が必要と考えられる。

プラクティス集の全体構成・提供媒体という観点では、その他の企業像と同様、「自社の状況や課題に応じ、参照すべきプラクティスがわかる」「自社の状況や課題に応じたプラクティスが掲載されている」等に強いニーズがある。また、個別のプラクティスの構成についても、概ねその他の企業像と同様に、「プラクティス実現に向けたコストや費用対効果・人的スキル」「プラクティスの優先有順位や対策を実施する順番」「対策が必要な理由の説明(他社でのインシデント事例等)」「業種ごとの特徴を踏まえたプラクティス」へのニーズが高い。なお、プラクティスの記載方法については、企業像③と比較してストーリー形式を求める傾向が強い。これは、ストーリー形式であっても対策のポイントを把握できる、すなわち「行間を読む」ことができるためと考えられる。なお、企業調査において、記載方法に関し、リスト形式では多様な状況・課題を有する全ての企業にマッチした記載は困難であるため、ストーリー形式としてある程度自社の課題に合わせて「行間を読む」ことを求める必要があるとの見解も得られた。

企業像③：サイバーセキュリティの取組みが進んでいない企業

当該の企業像は、アンケート調査における IT 依存度のカテゴリー4 に該当する企業、すなわち、「IT システム・IT サービスは主に社内業務等に利用するのみで、その停止は事業にあまり影響しない企業」を想定している。なお、IT 依存度のカテゴリー4 に該当する企業は、他のカテゴリーの企業と比較して、事業規模の観点では中小企業が、業種の観点では非重要インフラ事業者が多い。

当該の企業像は、サイバーセキュリティの取組みはあまり進んでおらず、自社の課題や取組みが必要な領域・テーマが把握できていない。このため、プラクティス集の利用目的は、サイバーセキュリティ体制構築のための「はじめの一歩」、すなわち、サイバーセキュリティ体制構築のために必要な対応内容の外観をつかみ、最初に手を付けるべき課題を理解することが第一と考えている。これを踏まえると、当該の企業像に有効なプラクティス集の形態は、現在の第 3 章のような個別テーマに関するプラクティスを提示する形態ではなく、サイバーセキュリティ体制の構築に必要な各論点とその実現のためのファーストステップを一通り解説した現在の第 2 章のような形態が合致すると考えられる。また、当該の企業像は、その他の企業像よりも、プラクティスの優先順位や対策を実施する順番を示してほしいというニーズを強く認識しているが、現在の第 2 章は具体的にどのテーマから手を付けるべきかについては、十分に把握・理解できる構成となっていない。なお、自社が取り組むべきプラクティスがわかるような構成面の工夫や診断機能の必要性については、複数の有識者や企業からも見解として示された。また、当該の企業像は、経営層や従業員のセキュリティ認識が十分ではないと考えられ、「サイバー攻撃が経営課題である理由」についての解説を充実化することで利活用が進む可能性がある。

個別のプラクティスに関しては、「対策が必要な理由の説明(他社でのインシデント事例等)」や「プラクティス実現に向けたコストや費用対効果・人的スキル」「業種ごとの特徴を踏まえたプラクティスの提示」等が強いニーズとして確認できた。また、プラクティスの記載方法の観点では、対応すべき内容がわかりにくいという理由から「ストーリー形式」は利用しにくいと考えている企業もみられ、当該層に対しては、ストーリー形式のプラクティスを読みこなすための「ガイド」や「解説」が必要かもしれない。

プラクティスの内容の理解促進や記憶への定着のために「絵柄を多用すべき」という見解が有識者より得られたが、特にサイバーセキュリティに関する基本的な知見・ノウハウが不足している企業に対しては、絵柄を活用して文書の説明を補足する観点は、理解を助ける有効な手段となると考えられる。

なお、より多くの提供が望まれるプラクティスのテーマ・内容については、いずれのカテゴリーも概ね同様の傾向であり、「組織全体での対応方針作成のプラクティス」「資源(予算、人材等)確保のプラクティス」「経営層や従業員のセキュリティ認識向上のプラクティス」「DX 推進・テレワーク導入等、タイムリーな環境変化を踏まえたプラクティス」、「サプライチェーン対策、演習・訓練、監査等のプラクティス」 等があげられた。

また、プラクティス集の提供媒体としては、検索性の高い Web コンテンツとしての提供、プラクティス集の更新頻度としては、1 年に 1 回程度が各カテゴリーに共通するニーズの傾向であった。

6.1.2 プラクティス集の提供媒体と全体構成の在り方

6.1.1 で整理した各企業像の利用実態やニーズを踏まえ、プラクティス集の提供媒体や全体構成の在り方、各企業像のユースケース等を整理する。

プラクティス集の提供媒体に関しては、各カテゴリーに共通するニーズとして、検索性の高い Web コンテンツとして提供のニーズが、また、全体構成については自社の業種や規模、セキュリティへの取組み状況等に応じて参照すべきプラクティスがわかることへのニーズが高いことが把握できた。まず、提供媒体の点で、現在のプラクティス集は PDF 形式での提供であり、ドキュメント内で該当の箇所へワンタッチで画面遷移するといった機能はなく、また検索は PDF ファイルの閲覧ソフトの機能を利用する方法に限定される等、情報の検索性については課題があると言える。また、読者は自社に関係するテーマや関心のあるテーマを自社の課題認識を踏まえ、自ら探し出して参照することが前提となっており、企業の状況を踏まえ参照すべきプラクティスがわかる仕組みにはなっていない。これらに関しては、PDF 形式から Web コンテンツへ転換を図ることと合わせ、「サイバーセキュリティ経営ガイドライン実践状況可視化ツール[4] (以下、「可視化ツール」)」との連携を図ることで、ニ

[4] IPA,https://www.ipa.go.jp/security/economics/checktool/index.html

ーズに合致したコンテンツとして提供できる可能性がある。可視化ツールとは、現在 IPA がホームページで提供している経営ガイドラインの実践状況を企業が自己診断できるツールである。執筆時点ではβ版としてエクセル形式での提供となっているが、これを Web コンテンツとして提供し、その診断結果からプラクティス集において参照すべきプラクティスを提示し Web 画面から簡単に遷移できるようにすることで、活用を促進することが可能となる。

また、Web コンテンツ化することで、ワンタッチでの画面遷移やキーワードでの検索が容易になり、「関連するプラクティスをすぐに参照できる」「プラクティス内の専門用語のリンクから用語集へ画面遷移する」といった利用が可能となる。なお、Web コンテンツ化は、読者側のメリットだけではなく、制作側のメリットとして、ページの区切りやレイアウト等の制約を受けにくく、記載の自由度が高まり、コンテンツを機動的に拡充しやすくなるといった利点もあげられる。

この Web コンテンツ化および可視化ツールとの連携を念頭に、各企業像のユースケースを整理する。

企業像①：サイバーセキュリティの取組みが進んでいる企業

当該カテゴリーに属する企業は、サイバーセキュリティ対策を進めてきており、基本的な体制の構築は既に図られている。一方で、DX やテレワークの推進等、IT やセキュリティに関連する新たな取組みに際し、更なる体制強化の必要性を認識する機会もあり、このような機会に可視化ツールを参照して体制面で不足する領域を把握し、ピンポイントで対処するといった利用方法が想定される。また、当該カテゴリーの企業は、自社の課題や対策が必要な領域が明確であることから、可視化ツールによる診断を経ずに直接第 2 章の内容を参照することも想定される。また、体制面の構築は既に図られていると考える企業が多いため、より具体性の高いテーマを取り扱う第 3 章のプラクティスから参照するといった利用方法も、企業像②のカテゴリーに属する企業以上にニーズが高いと想定される。なお、有識者調査においても、対策が進んでいる企業での活用を念頭に「(現状の体制論を切り口としたプラクティスでは) 想定される脅威や攻撃に対し、現場レベルでの実践的な対策を検討する場合には利用しにくい」「より多くの参考事例を掲載すべきである」との見解も得られている。このようなニーズも踏まえ、具体性の高いテーマを扱う第 3 章においては、より実践的かつ具体的な対策を盛り込む (プラクティスに紐づけて情報を追加していく) 必要があると言える。

企業像②：サイバーセキュリティの取組みがある程度進んでいる企業

当該カテゴリーに属する企業は、ある程度サイバーセキュリティ対策を行ってきたが、体制面での弱点の強化や、新たな取組みに際しての更なる体制強化の必要性を感じている。こうした悩みを有する企業についても、可視化ツールで自社の状況を把握するとともに、対策

を補強するプラクティスをレコメンドする機能は有効に活用されると考えられる。また、当該カテゴリーの企業のうち、体制面の強化は一定程度図られていると考える企業については、より具体性の高いテーマを取り扱う第 3 章のプラクティスから参照する利用方法も想定される。なお、第 3 章のプラクティスについても、それを実行するにおいては、第 2 章が取り扱う体制面の強化と無関係ではないため、必要に応じて第 2 章の内容を確認し、体制面で不足している対応がないかを確認する必要がある。例えば、現在の第 3 章（3）「インシデントが起きた際の財務面でのリスクヘッジが十分ではない悩みに対し、初動対応のリスクを減らすサイバー保険の活用を検討する」プラクティスについては、その実現のために、指示 4 の「リスクの把握と対応計画の策定」を踏まえた自社のリスクの特定・評価が必要である。また、（6）「海外拠点のセキュリティ意識が低い悩みに対し、対面コミュニケーションを通じセキュリティ意識を向上させる」プラクティスについては、指示 2 の「管理体制の構築」を踏まえた組織設計が必要となる（[表 6-1]）。このように、第 3 章の具体性の高いテーマから、体制面の弱点の強化や更なる改善の必要性を認識して第 2 章を参照する流れを想定し、第 3 章のプラクティスにおいても第 2 章の内容にも言及し、リンクからワンタッチで画面遷移できるような機能が求められる。

表 6-1 現在の第 3 章の内容と関連する指示項目(重要 10 項目)

セキュリティ担当者の悩み		取組みのプラクティス	関連する 重要10項目
(1)	インシデント対応経験がない要員でCSIRTを組成したが対応に不安がある	社外専門家を活用しながら自社で サイバーセキュリティ人材を育成する	指示2：管理体制の構築
(2)	インシデント対応の初動における情報共有に不安がある	標的型メール訓練で開封したかではなく 報告したかを意識させる	指示7：緊急対応体制の整備
(3)	インシデントが起きた際の 財務面でのリスクヘッジが十分ではない	初動対応のリスクを減らすサイバー保険の 活用を検討する	指示4：リスクの把握と対応計画の策定
(4)	IoT機器が「シャドーIT」化している	製造部門とIT部門が連携し、不正接続 機器や不適切な設定を排除する	指示3：資源（予算、人材等）確保
(5)	全国各地の拠点におけるセキュリティ管理 状況に不安がある	拠点におけるセキュリティの取組みを把握し、対面で対話する	指示6：PDCAサイクルの実施
(6)	海外拠点のセキュリティ意識が低い	対面コミュニケーションを通じ、 セキュリティ意識を向上させる	指示2：管理体制の構築
(7)	自前でのシステム運用の負担が大きく、 セキュリティ対策に不安を感じる	自社のセキュリティルールに整合する、 適切なクラウドサービスを利用する	指示4：リスクの把握と対応計画の策定
(8)	外部サービスの選定でIT部門だけでは 対応が困難である	社内の関連部門と連携して 外部サービスの選定を行う	指示2：管理体制の構築
(9)	経営層にセキュリティ対策の事業遂行上の重要性を理解してもらえない	事業部門と共同し、事業戦略の一環として セキュリティ対策の必要性を訴求する	指示1：組織全体での対応方針の策定
(10)	IT部門のみで経営層のセキュリティ意識を 向上させることに限界を感じている	外部講師による経営層向けの研修会を 実施する	指示1：組織全体での対応方針の策定
(11)	従業員に対してセキュリティ教育を実施しているが効果が感じられない	特定の部署・役職等に向けたフォローアップの仕組みを企画し、試行する	指示3：資源（予算、人材等）確保
(12)	効果的な演習をする方法がわからない	演習実施部門と演習対象部門が共同して、 演習内容を企画する	指示7：緊急対応体制の整備
(13)	スタートアップ企業のセキュリティ管理体制に不安を感じ、取引先として推奨できない	セキュリティ対策の取組み、セキュリティ認証の取得状況を確認する	指示9：サプライチェーン対策
(14)	工場のサイバーセキュリティ対策が 急務となっている	工場システムのネットワークにおける 役割分担を明確にする	指示5：リスク対応の仕組みの構築

企業像③：サイバーセキュリティの取組みが進んでいない企業

当該カテゴリーに属する企業は、サイバーセキュリティ対策を何から始めればよいかわからないという悩みを抱えているため、まずは体制構築の「はじめの一歩」として、プラクティス集の第 2 章の全体を読み込んで必要な対策の全体像を把握し、次に、自社の課題から優先的に取組むべきポイントを把握して実際の対策に取り込むといった利用方法が想定される。その際、前述の可視化ツールにおいて、経営ガイドラインの重要 10 項目で対策が不

足する指示内容を把握し、これに対応する個別のプラクティスを参照するといった活用方法が有効となる。また、第 2 章の体制強化のプラクティスの内容と関連する第 3 章のプラクティスを紹介し、ワンタッチで遷移できる機能を設けることで、体制に関する「はじめの一歩」の理解から、個別テーマへの関心や、取組みの必要性の気づきを促進することができる。

以上を踏まえ、各企業像とプラクティス集および可視化ツールの関係を図 6-2 に整理する。

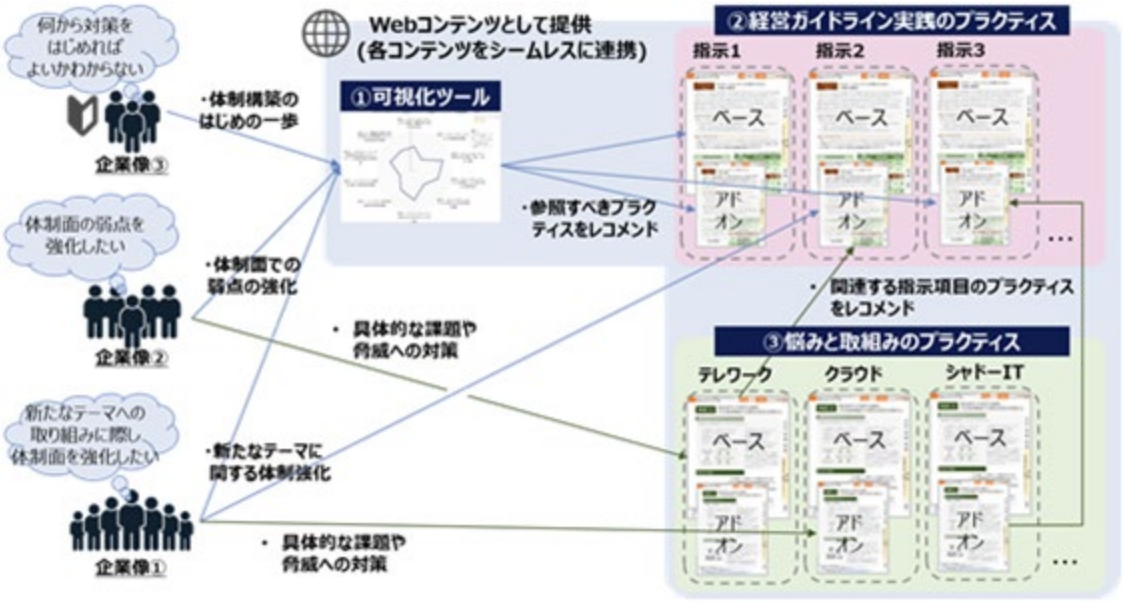


図 6-2 プラクティス集の提供媒体と全体構成

6.1.3 個別のプラクティスの構成・内容の在り方

次に、第 2 章および第 3 章の個々のプラクティスの構成・内容について、今後の在り方を整理する。

まず、第 2 章および第 3 章に共通して強いニーズとしてあげられたものが「企業の状況（業種、規模、組織体制等）に応じて、対応すべきプラクティスがわかるようにする」ことである。なお、IT 依存度の高いカテゴリーに属する企業ほど、自社の状況や課題に応じたプラクティスを求める傾向が強いことが傾向として把握できた。また、企業調査においても、自社の業種に特有の内容が掲載されていれば、プラクティスの内容を「自分事」すなわち自社に関係の強い内容として捉えやすいため、活用が進むのではないかといった見解や、企業規模によりリソースの観点から対応できる内容が異なるため、大企業と中堅企業、中小企業でプラクティスを分けて記載すべきといった見解が得られた。

この点に関しては、6.1.2 で整理したように、全体構成の観点から、可視化ツールとの連携により参照すべきプラクティスをレコメンドするという方向性に加えて、様々な企業の状

況に対応するプラクティスの数を充実化していくことが考えられる。但し、各テーマに対応するプラクティスを業種や規模の類型その他の組み合わせに応じ、全てのパターンを作成することは現実的に不可能である。また、プラクティス集が準拠する「サイバーセキュリティ経営ガイドライン」は、業種や規模等に関わらず、IT に関するシステムやサービス等を供給する企業及び経営戦略上 IT の利活用が不可欠である企業であれば対策が必要となる「指針」を示したものであり、これに対応するプラクティス集も、この「指針」を実施するためのファーストステップとして、スタンダードな内容をまずは提示すべきと考えられる。これらの観点を踏まえると、各テ―マに対するスタンダードなプラクティスを「ベース」のプラクティスとして定義し、業種や規模その他システムの特性等に応じた補足情報や読み替えの事例等を「アドオン」の情報として掲載する方法が考えられる。

また、プラクティスの構成要素として、「プラクティス実現に向けたコスト（効果）」や「プラクティスの実施体制（役割・スキル）」の記載が各カテゴリーに共通するニーズとして確認できた。企業調査においても、経営層への報告の際にコストやリソースについて明示されていると、「一般的には（他社では）この程度のコストやリソースを投下しているため、当社も同程度の対応が必要である」といった説得が可能となり、活用しやすいという見解も得られた。なお、経営層の説得という観点では、有識者より、他社でのインシデントの事例と各プラクティスが紐づいていると有効であるとの見解も得られた。

また、第 3 章については、先述の通り、対策が進んでいる企業を想定し、より実践的かつ具体的な対策内容を盛り込んでいく必要がある。加えて、IT やセキュリティのトレンドや脅威の変化等に応じ、取り扱うテーマ、プラクティスの機動的な拡充が求められる。この点は、有識者調査や企業調査でも共通した見解として得られた。具体的なテーマの例としては、コロナ禍を踏まえたテレワークの進展に対応するプラクティスや昨今増加している企業を狙ったランサムウェアによる脅迫への対応、DX の推進に伴うクラウド利用の増加等が想定される。なお、このような第 3 章が取り扱うテーマについて、現在は、「セキュリティ担当者の悩み」という幅広い観点から、実際の企業の取組みや有識者の課題認識をヒアリングして掲載するテーマを決定している。この方法は、テーマ選定の自由度が高い一方で、サイバーセキュリティ対策の全体像を踏まえたフレームワーク等に準拠しないため、IPA やヒアリングを行った企業、有識者等の課題認識にテーマが寄ってしまう可能性や、掲載が不足する（または、「多すぎる」「掲載が漏れている」）テーマが生じやすいといった課題が想定される。この点に関しては、今後も幅広く意見集約を行いながら検討を進めていく。

以上について、第 2 章、第 3 章それぞれの現在の構成・内容との対比で、以下の図 6-3 および 6-4 に整理した。

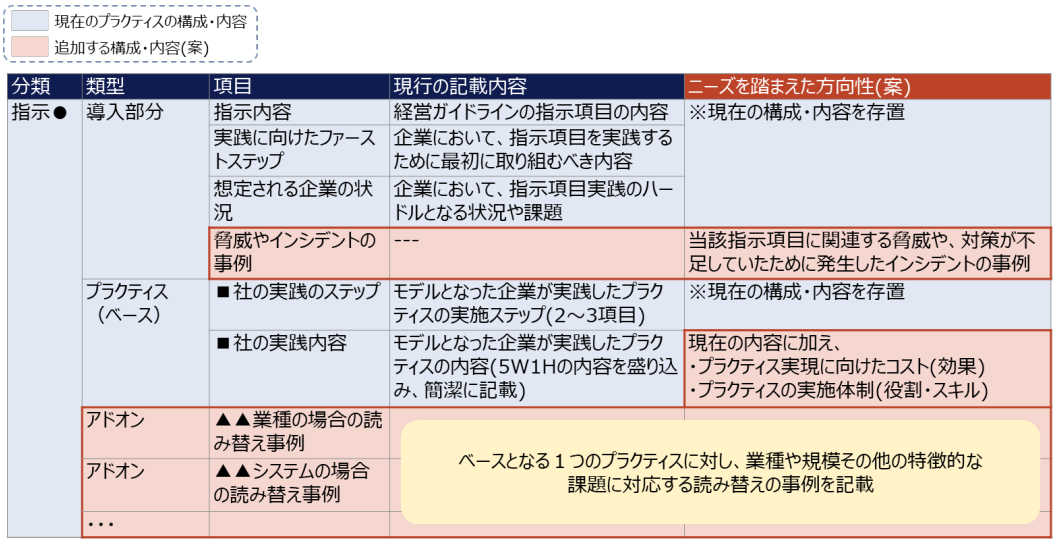


図 6-3 第 2 章の改訂の方向性

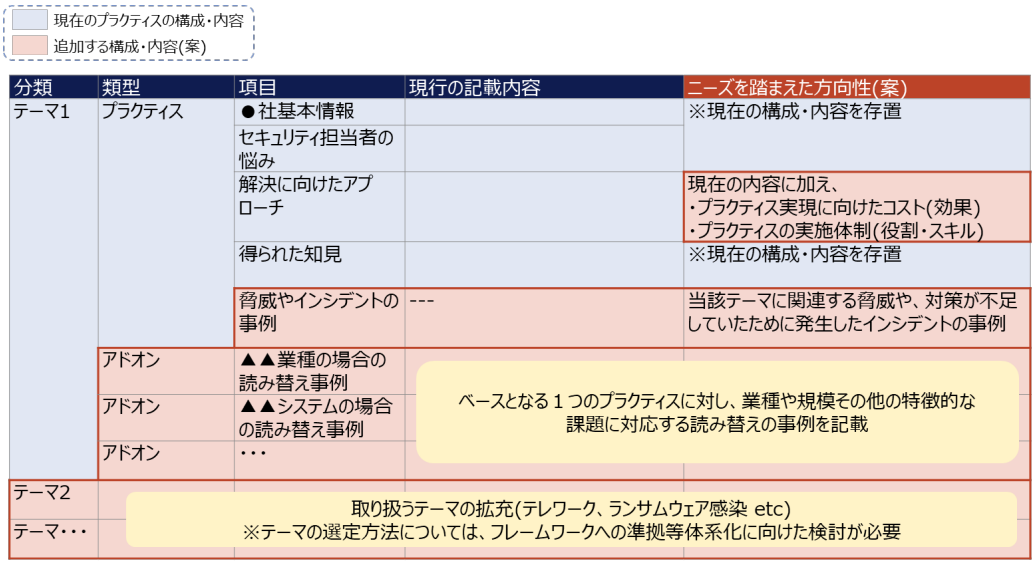


図 6-4 第 3 章の改訂の方向性

6.2 プラクティス集の在り方について

調査結果を踏まえ、プラクティス集の今後の在り方として、以下の 3 つの方向性に整理した。

Ⅰ. 企業の課題に応じたプラクティスが参照できる Web コンテンツとしての提供

アンケート調査や企業調査において、企業は「自社の状況・課題に応じた内容のプラクティスを参照したい」「自社の状況・課題から参照すべきプラクティスがわかるようにしてほしい」というニーズを強く有していることがわかった。こうしたニーズへ対応するため、可視化ツールとの連携や Web コンテンツ化を通じて実現することが考えられる。これを実現することで、企業による可視化ツールの診断結果とプラクティスの参照・活用方法に関するデータが蓄積され、業種や規模等で平均的な指示項目の対策状況やそれに応じて参照されるプラクティスの傾向、コンテンツ内で検索されることが多い用語等の分析が可能となる。また、Web コンテンツ内にアンケート機能を設けることで、改善要望や取り上げてほしいテーマ等の意見を比較的容易に収集できる。このような、企業による活用実態やニーズの把握により、将来的には、企業像と必要なコンテンツとの関係が精緻化され、よりきめ細かなニーズに即したコンテンツが提供できる（[図 6-5]）。

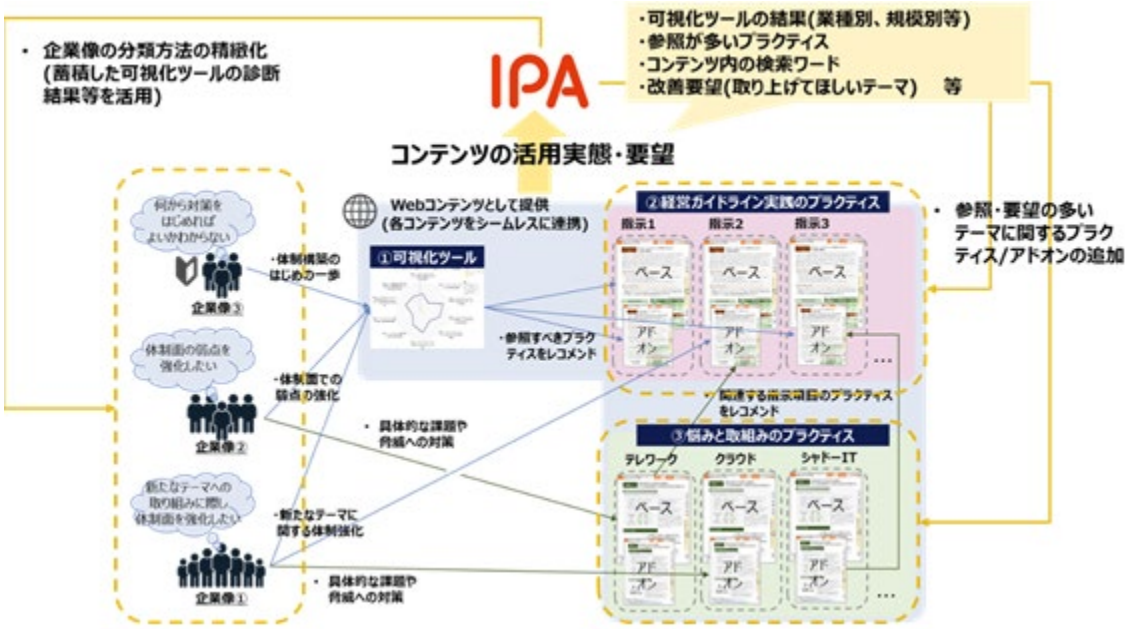


図 6-5　可視化ツールとの連携・Web コンテンツ化による活用実態の把握と改善

加えて、Web コンテンツ化により紙面（レイアウト）の制約を受けにくくなるため、視覚的に理解を助ける工夫をしやすいといったメリットも考えられる。アンケート調査でも、図表やピクトグラム、写真等の視覚的な理解を助ける工夫についてのニーズが確認できた。また、将来的には Q&A 機能や掲示板機能等の動的なコンテンツを導入し、取組みが進んでいない企業へはフォローの充実化の仕組みとして、対策が進んでいる企業へは新たな対策の事例を収集・発信・共有しやすくする仕組みとして提供することも考えられる。

なお、可視化ツールとの連携については、「具体的にどの診断結果に対してどのプラクティスを紐づけるか」「各診断結果に対応するプラクティスが現在のプラクティスで充足して

いるか」等、議論すべき論点が多く存在するため、改訂に向けたグランドデザインを描きながら、段階的に検討していく。

また、これらの検討に並行して、コンテンツをより多くの企業に活用してもらうための取組み、すなわち、コンテンツ自体の認知度を向上する取組みが必要となる。具体的には業界団体・IT ベンダーとの連携、SEO 対策等が想定される。

Ⅱ．企業ニーズを踏まえた各プラクティスの構成・内容の拡充

各プラクティスの構成・内容の拡充について、様々な企業の状況や課題に対応してプラクティスを充実化していくことが求められている。但し、各テーマに対応するプラクティスを業種や規模その他の組み合わせに応じて全てのパターンを網羅することは困難である。そのため、各テーマに関するスタンダードな内容をベースのプラクティスとして提示し、業種や規模その他に応じた補足情報や読み替えの事例等をアドオンの情報として掲載する方法が考えられる。なお、この情報の充実化においては、ニーズの高いテーマや、業種や規模等に特化したプラクティスが求められるテーマを優先する。調査より、全般的にニーズの高いテーマとして、「サイバーセキュリティリスクの認識、組織全体の対応方針の策定」「サイバーセキュリティ対策のための資源（予算・人材等）の確保」「経営層や従業員のセキュリティ認識に関する悩み」が、業種や規模等に特化したプラクティスの提供が望まれるテーマとして、「サイバーセキュリティ対策のための資源（予算・人材等）の確保」「インシデントによる被害に備えた復旧体制の整備」「ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握」等が確認できた。これらのテーマに関しては、企業の取組みが相対的に遅れている、もしくは取り組み方に悩みを抱えている企業が多いと想定され、優先的に情報を充実化することが必要となる。

また、プラクティスの構成要素として、高いニーズが確認できた「プラクティス実現に向けたコスト（効果）」や「プラクティスの実施体制（役割・スキル）」、「関連するインシデントの事例」等の情報を現行のプラクティスをベースに追補・補強することが必要となる。なお、この点については、比較的テーマ選定や記載内容の観点から自由度の高い現行の第 3 章（セキュリティ担当者の悩みと取組に関するプラクティス）をベースに、構成・内容の拡充を先行し、その過程で蓄積した知見・情報を踏まえて、現行の第 2 章（「サイバーセキュリティ経営ガイドライン Ver2.0」の「重要 10 項目」に関するプラクティス）の拡充を行う方向性が想定される。なお、第 3 章については、IT やセキュリティのトレンド、脅威の変化等に応じ、テレワーク、クラウド利用等の新たなテーマに関するプラクティスを積極的に拡充していくことも重要となる（[図 6-6]）。

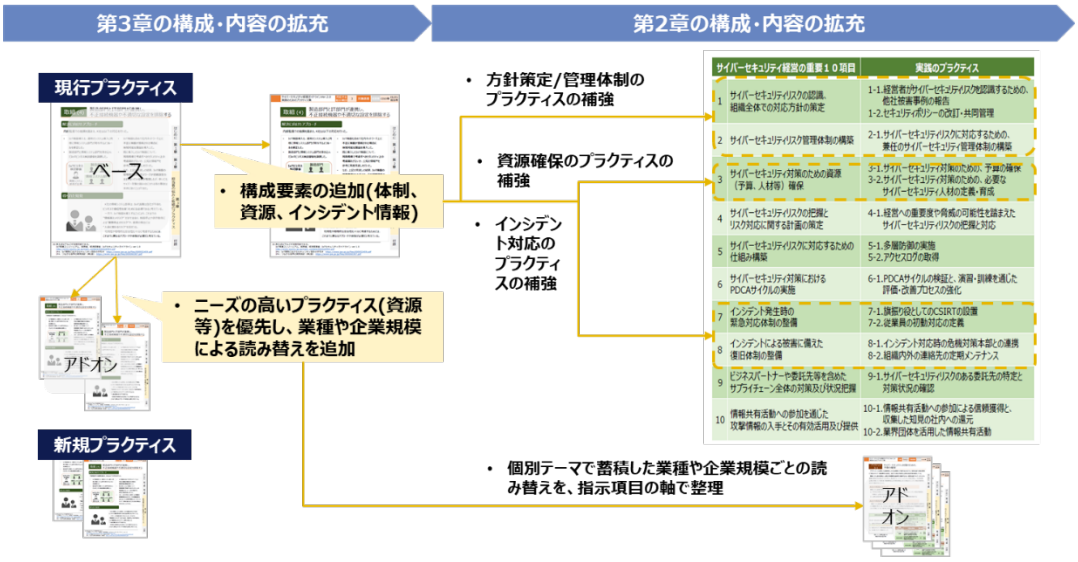


図 6-6 プラクティスの構成・内容の拡充のステップ

Ⅲ. 企業間でのプラクティスの作成・共有

現在プラクティス集は、IPA が外部機関に調査を委託して作成をしている。作成においては、企業のニーズ調査やインタビューを通じたプラクティスの収集、有識者の査閲等を実施し、実用性と品質を確保している。一方で、こうした作成・共有の方法では、企業のニーズを機動的にとらえ、迅速に見直し・公表を図るという点では限界があると言える。

この点を踏まえ、今後、企業の関心の高いテーマについて、質の高いプラクティスを機動的に作成・提供するための手法や体制の検討が求められる。調査では、サイバーセキュリティの取組みが進んでいる企業を中心に、プラクティスの元となるサイバーセキュリティ対策の推進・文書化を進めている実態が確認できた。こうした、企業に蓄積するノウハウや、また現場の課題認識をくみ取りプラクティスに反映していく方法として、例えば、プラクティスの作成に、企業の有志を募り、IPA と共同でプラクティスを作成するといった方法が考えられる。また、企業間で、プラクティスを共同で検討・作成し共有するような枠組みを IPA が主体となって運営するといった方法も考えられる。調査でも、情報共有や人材育成等のメリットから、多くの企業でそのような枠組みの必要性・有用性が理解されていることがわかった。なお一方で、このような共同検討には、企業のリソース面の課題や、内部情報を外部に共有する際のルール設定の必要性等、課題・乗り越えるべきハードルも確認できた。

今後、プラクティスの構成・内容の検討と並行し、作成・共有に在り方についても検討を進めていく。

最後に、以上の３つの方向性を踏まえた今後の検討イメージを参考として記載する（[図 6-7]）。なお、各ステップの順序は、企業のニーズが強いもの（Web コンテンツ化、自社の状況や課題に応じ、参照すべきプラクティスがわかる構成）や、先行して取り組むことで後段の取組みに有効な知見が得られるもの（Web コンテンツ化、第 3 項の構成要素の充実化）を前半に、取組みに向けて準備や検討に時間を要するもの（企業間での作成・共有の枠組みの構築）を後半にプロットしている。

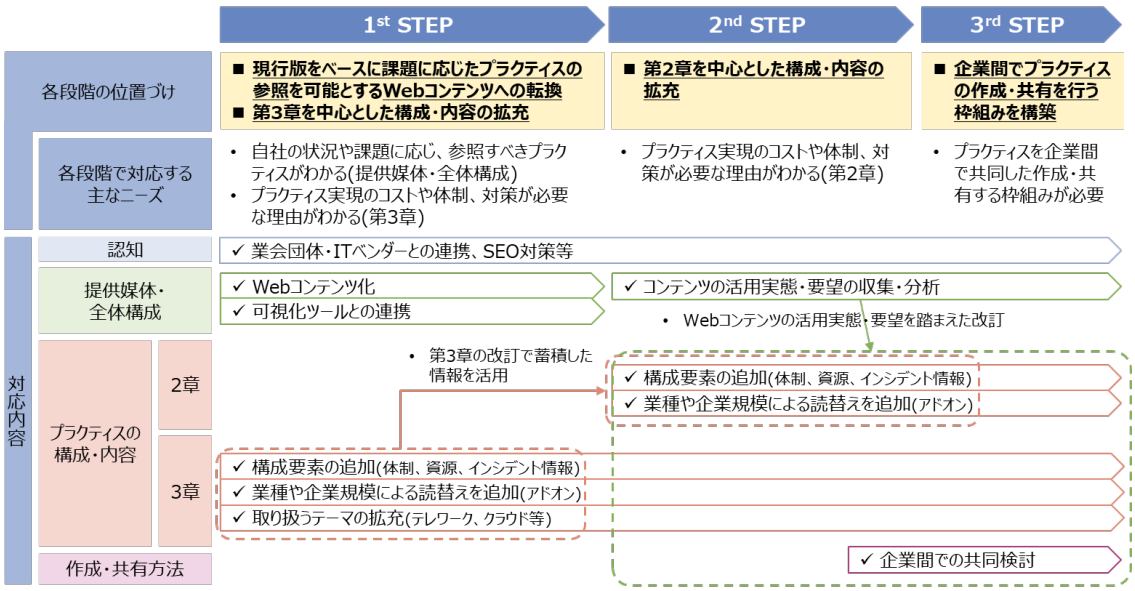


図 6-7 （参考）今後の在り方を踏まえた検討イメージ

企業活動のデジタルトランスフォーメーションの動きが活発になるとともにサイバー攻撃の脅威が拡大する中、企業におけるサイバーセキュリティの確保はますます重要となっている。また、こうした状況は、新型コロナウイルスの影響による消費行動や労働環境の変化等をうけ今後も加速することが見込まれる。こうした環境変化をうけ、プラクティス集が必要とされる機会は増加し、多様なニーズへの対応も必要となる。また、環境変化のスピードに応じて、これまで以上に機動的な見直しを図っていくことが必要となる。