令和４年度サプライチェーン・サイバーセキュリティ対策促進事業
（サイバーセキュリティ経営に関する調査）

調査報告書

2023年3月

みずほリサーチ＆テクノロジーズ株式会社

目 次

1. 調査実施の目的、実施内容等

(1) 調査目的

- 様々なビジネスの現場において、ITの利活用は企業の収益性向上に不可欠なものとなっている一方で、企業が保有する顧客の個人情報や重要な技術情報等を狙うサイバー攻撃は増加傾向にあり、その手口は巧妙化している。
- そこで、経済産業省では、独立行政法人情報処理推進機構（IPA）とともに、大企業及び中小企業（小規模事業者を除く。）のうち、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の経営者を対象に、経営者のリーダーシップの下で、サイバーセキュリティ対策を推進するため、「サイバーセキュリティ経営ガイドライン」（以下「経営ガイドライン」という。）を策定し、公表している。また、セキュリティ人材の不足に悩む企業においては、外部の情報セキュリティサービスの利用を含めてセキュリティ対策を検討する必要があることから、情報セキュリティサービスの普及を促進し、企業が情報セキュリティサービスを安心して活用することができる環境を醸成するため、「情報セキュリティサービス基準」、「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示」及び「情報セキュリティサービスに関する審査登録機関基準」を公表している。
- 本事業は、ITの利活用、サイバー攻撃等の動向を踏まえ、経営ガイドラインの改訂事項に係る調査及び改訂案の作成を実施するものであり、これにより実情に即した経営ガイドラインが策定され、当該ガイドラインに基づいたサイバーセキュリティ経営が実現されること、及び情報セキュリティサービスの普及促進に向けた調査を実施し、情報セキュリティサービスが活用されることを目的とするものである。
- なお、経営ガイドラインについては、直近では平成29年に改訂を行ったところであるが、サイバーセキュリティ経営を取り巻く状況の変化等に伴い、新たな概念等を盛り込んだ更なる改訂が必要な状況となっており、経営ガイドラインの改訂にあたって、経済産業省とIPAにおいて「サイバーセキュリティ経営ガイドライン改訂に関する研究会」（以下「経営ガイドライン研究会」という。）を計4回開催し、検討を実施した。
- これらの取組を一体的に進めていくため、本事業では以下の事項についての調査を実施した。
  - サイバーセキュリティ経営ガイドラインの改訂に向けた調査と改訂案の作成
  - 情報セキュリティサービス普及促進・活用に関する調査

1. 調査実施の目的、実施内容等

(2) 調査の実施方針

- 前ページに示した調査目的を踏まえ、主にユーザ企業における適切なサイバーセキュリティ対策の実現を支援するため、受託者（みずほリサーチ＆テクノロジーズ株式会社）及び再委託先がこれまで関連事業の実践を通じて得た知見やネットワークを活用しつつ、本事業における２種類の調査を効率的かつ実効的に実施することで、最大限の事業成果を得て、WG2/3における今後の取組に資するように努めた。
- さらに、サイバーセキュリティ分野を取り巻く最新の動向に、随時対応できるように努めた。

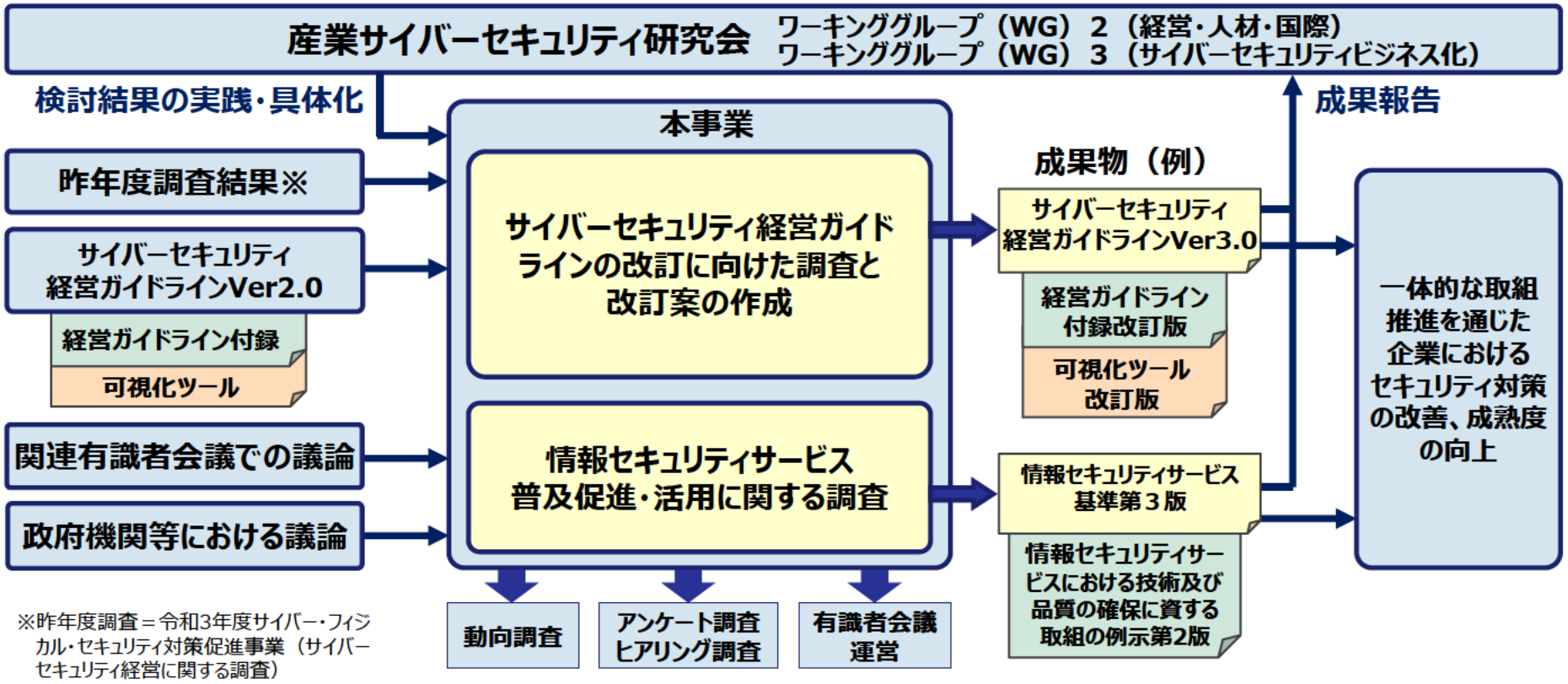

図1.1　調査の実施方針

1. 調査実施の目的、実施内容等

(3) 実施内容

- (1)(2)を踏まえ、本事業で実施した調査は次表の通りである。調査結果の詳細を本報告書第2章以降で示す。

表1.1　調査実施内容

調査項目（大項目）	調査項目（小項目）	実施内容
1. サイバーセキュリティ経営ガイドラインの改訂に向けた調査と改訂案の作成	1.1 サイバーセキュリティ経営ガイドラインの改訂に向けた動向調査と改訂案の作成	● 経済産業省との協議のもと、以下の調査対象についての最新動向に関する調査を実施した。 ➢ サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の公表 ➢ 企業におけるサプライチェーンの位置付け等の変化 ➢ 企業の経営層がコミュニケーションを行うべき「関係者」の実態 ➢ 企業におけるクラウド等最新技術の利用動向 ➢ 制御系の情報システムにおいて考慮すべき事項 ● 調査結果及び次項の有識者会議における審議結果をもとに、次の３種類の改訂作業を実施した。 ➢ サイバーセキュリティ経営ガイドラインVer2.0本編 ➢ サイバーセキュリティ経営ガイドラインVer2.0付録 ➢ サイバーセキュリティ経営可視化ツール
	1.2 有識者会議の開催	● 企業におけるコーポレートガバナンス、エンタープライズリスクマネジメント及びサイバーセキュリティ対策に知見を有する10名の有識者による研究会を設置し、4回にわたる開催にあたっての事務局運営を担当した。
	1.3 政府機関等における議論の把握	● 以下の会合における議論及び成果物をもとに議論の把握を行った。 ➢ 産業サイバーセキュリティ研究会 ➢ サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会 ● 前項と並行して経済安全保障に関する政策動向の把握を行った。

1. 調査実施の目的、実施内容等

(3) 実施内容（続き）

調査項目（大項目）	調査項目（小項目）	実施内容
2. 情報セキュリティサービス活用・普及に関する調査	2.1 有識者会議の開催	● 情報セキュリティサービスに関する有識者10名で構成される検討会を設置し、3回にわたって情報セキュリティサービス審査登録制度の活用・普及に関する議論を行うにあたっての事務局運営を担当した。 ● 本調査の期間中に実施した情報セキュリティサービス基準等の改訂に関する審議及びパブリックコメントに寄せられた意見に対する審議についての事務局運営を担当した。
	2.2 情報セキュリティサービス基準等の改訂支援	● 有識者会議における議論をもとに、情報セキュリティサービス基準の改訂案、並びに情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示案をとりまとめた。
	2.3 有識者会議の議論を受けた調査の実施	● 有識者会議での議論をもとに、情報セキュリティサービス審査登録制度において今後追加することが想定される候補として挙げられたサービスの提供ベンダーへのアンケート及びヒアリング調査を実施し、その結果を有識者会議にて報告した。
	2.4 情報セキュリティサービスユーザへのアンケート調査の実施	● 情報セキュリティサービスの利用者に関する最新の実態把握を目的として、企業等で情報セキュリティサービスの調達に携わるモニターを対象とする、情報セキュリティサービス利用の実態、制度の認知状況及び制度へのニーズに関するウェブアンケート調査を実施し、その結果を有識者会議にて報告した。
3. 報告書の作成	報告書の作成	● 1～2の調査結果をもとに、本報告書を作成した。

2. サイバーセキュリティ経営ガイドラインの改訂に向けた調査と改訂案の作成

2.1 サイバーセキュリティ経営ガイドラインの改訂に向けた動向調査と改訂方針案の作成

2.1.1 動向調査

- 経済産業省との協議のもと、以下の調査対象についての最新動向に関する調査を実施した。
  - サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の公表
  - 企業におけるサプライチェーンの位置付け等の変化
  - 企業の経営層がコミュニケーションを行うべき「関係者」の実態
  - 企業におけるクラウド等最新技術の利用動向
  - 制御系の情報システムにおいて考慮すべき事項
- これらの調査結果については、以降のページに示す内容を資料にとりまとめ、2.2に示す有識者会議にて報告した。

2.1.1 動向調査

(1) サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の公表

- 2019年4月に公表された「サイバー・フィジカル・セキュリティ対策フレームワーク」（CPSF）では、サイバー空間とフィジカル空間が融合することで新たな価値を産む「Society5.0」における産業社会における新たなリスクに対応する必要があるとの問題意識をもとに対応の指針を示しており、経営者においても自社のリスクマネジメントの検討にあたってこのようなリスクを認識する必要がある。
- 一方、CPSFは右図のように、「サイバー空間」と「フィジカル空間」の３層でのつながりを、従来のサプライチェーンが発展した新たな企業等間のつながりの形態としてバリュークリエイションプロセスと定義するなど、これまでの経営ガイドラインの読者にとってはなじみのない表現が用いられている。そのため、サイバーセキュリティ経営ガイドラインの改訂にあたってCPSFの内容を抜粋して記載するだけでは十分な理解が得られない可能性が高い。記述にあたっては読者が容易に理解できるように用語の選定等に工夫を図る必要がある。

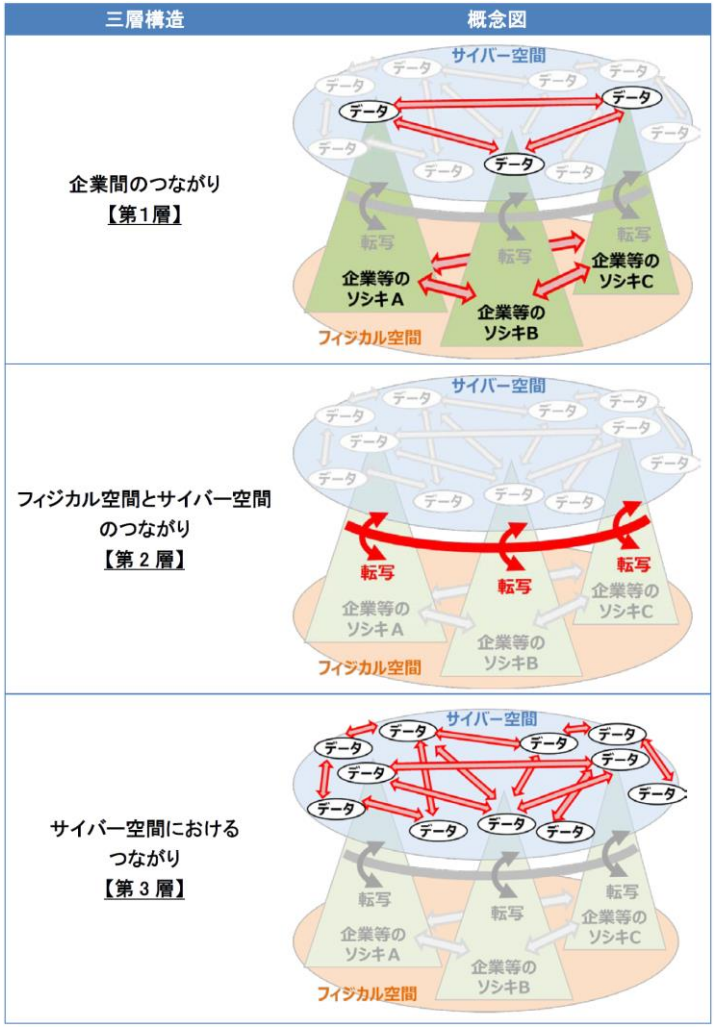

図2.1　バリュークリエイションプロセスが展開する産業社会の三層構造

（資料）『サイバー・フィジカル・セキュリティ対策フレームワーク Version1.0』（経済産業省, 2019年4月）

2.1.1 動向調査

(2) 企業におけるサプライチェーンの位置付け等の変化

- 2022年2月以降、国内企業におけるランサムウェア被害が拡大し、同年3月には部品製造企業１社における感染により、当該企業を調達先としていた大手の自動車製造企業の製造が止まるなど、サプライチェーンにおけるサイバーセキュリティ対策の実践状況が、国内産業に大きな影響を及ぼすに至っている。
- 経済産業省及び独立行政法人情報処理推進機構（IPA）では以前よりこのような状況を踏まえ、産業界が一体となって中小企業を含むサプライチェーン全体でのサイバーセキュリティ対策の推進運動を進めていくことを目的として、2020年11月に「サプライチェーン・サイバーセキュリティ・コンソーシアム」（SC3）の発足を支援しており、経営ガイドラインでもサプライチェーン対策の必要性をさらに強調していく必要がある。
- 一方、現行の経営ガイドラインは５年前の策定であることもあって、サプライチェーンにおけるサイバーセキュリティ対策の必要性は記載されているものの、部品調達や下請構造など従来典型的であったサプライチェーンをイメージさせる記述にとどまっており、前ページのCPSFで説明されているような、企業等間での多様なつながりで構成されるバリュークリエイションプロセスを想定することが困難である。また、サプライチェーンの定義やスコープについての説明は、付録Eの用語定義を含めてなされていない。これらを踏まえ、経営者が現在のサプライチェーンの置かれている状況を認識できる内容に改訂することが求められる。

(3) 企業の経営層がコミュニケーションを行うべき「関係者」の実態

- 経営ガイドラインでは、現状版（Ver2.0）において経営者に対し、「平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、関係者との適切なコミュニケーションが必要」としてコミュニケーションの重要性を説いているが、このコミュニケーションの対象としてはステークホルダー（顧客や株主など）を示しているのみである。
- サイバーセキュリティインシデント発生時には、平時からコミュニケーションを確保しておくことで、緊急時に適切な意思疎通や対応をとれるとされ、経営者には社外のみならず社内の関係者、かつ、CISO等のセキュリティ担当者のみならずセキュリティ対策を実施すべき担当者と広くコミュニケーションをとっておくことが求められ、ガイドラインにもこれを反映した内容を記載することが適切である。

2.1.1 動向調査

(4) 企業におけるクラウド等最新技術の利用動向

- 2020年のコロナ禍以降、企業におけるテレワーク利用が急速に普及するとともに、企業のIT環境についてもテレワークにおけるセキュリティ確保に対応する形で、境界防御型モデルからゼロトラストモデルへの移行やクラウド環境への移行などが進展した。一方で経営ガイドラインVer2.0は2017年に改訂されたため、このような動向を反映しておらず、境界防御型モデルを前提とした対策を示している。
- 今後も同様の技術革新や働き方の変化が生じることが見込まれることを踏まえ、経営ガイドラインの改訂に際しては、現在の企業における最新技術の利用動向にそぐわない記載が無いかを確認するとともに、特定の技術に依存しないような記述とすることについて検討することが考えられる。

(5) 制御系の情報システムにおいて考慮すべき事項

- (2)に示した企業におけるランサムウェア被害の拡大は、制御系の情報システムを扱う製造業等においても生じている。これまで制御系システムはいわゆるIT系とは物理的に分離して運用されることで影響は限定的と考えられることもあったが、コロナ禍以降で普及した遠隔監視、遠隔操作等のサービスは工場等の製造設備等でも用いられるようになり、それらの通信に用いられるネットワークを通じてのサイバー攻撃の影響を受ける可能性が高まっており、企業においては攻撃で被害が発生することを前提に、インシデント対応や復旧に関する演習の実施等を通じてこれに備える必要がある。
- 内閣サイバーセキュリティセンターでは、2022年6月に「重要インフラのサイバーセキュリティに係る行動計画」を改訂し、重要インフラを取り巻く脅威の変化に対応するため、将来の環境変化を先取りし、サプライチェーンを含めてリスクを明確化し対応するとともに、事業者における障害対応体制の有効性を検証する目的での分野横断的演習の推進を求めている。
- 経営ガイドラインVer2.0では制御系を対象としておらず、読者が演習の対象をIT系のみでよいと誤認する恐れがあることから、制御系を対象とする演習の必要性を明記する必要がある。

2.1.2 サイバーセキュリティ経営ガイドライン改訂方針案の作成

(1) サイバーセキュリティ経営ガイドラインVer2.0本編の改訂

- 前述の動向調査をもとに、2.2に示す有識者会議での審議の結果、経営ガイドラインVer2.0の本編に関しては、次の方針で改訂を行うことで合意がなされた。
  - 内容の中核となる「経営者が認識すべき３原則」及び「サイバーセキュリティ経営の重要10項目」の構成については、企業等において幅広く利用されている実態を踏まえて維持する。
  - 経営者を直接的な読者として想定している「サイバーセキュリティ経営ガイドライン・概要」の内容を見直し、エンタープライズリスクマネジメントの一部としてサイバーセキュリティ対策の必要性やサイバーセキュリティ対策における経営者の責務などを記載するとともに、単に「指示」すればよいという誤解を与えないための説明を追記する。
  - サイバーセキュリティに関する投資は、いわゆる直接的なリターンを求めるものではなく、将来の事業活動・成長に必須の費用であることを示す。
  - 前項の通り全体構成に大きな変化がないことで読者が「大きな改訂ではない」と誤解することのないよう、改訂後のバージョンは3.0とする。
- 「経営者が認識すべき３原則」については、主に以下の改訂・見直しを行うこととなった。
  - 対策の実施を通じてサイバーセキュリティに関する残留リスクを許容水準まで低減することは、経営者の責務である旨を記載する。
  - サプライチェーン構造の複雑化に伴い、サプライチェーン全体を俯瞰し、総合的なセキュリティを徹底することの必要性等を記載する。
  - 関係者とのコミュニケーションについて、社外のみならず、社内関係者とも積極的にコミュニケーションをとることが有効である旨を記載する。

(1) サイバーセキュリティ経営ガイドラインVer2.0本編の改訂

（前ページからの続き）

- 「CISO等に対して指示すべき１０の重要項目」については、主に以下の改訂・見直しを行うこととなった。
  - 指示３について、セキュリティ業務に従事する従業員のみならず、全ての従業員が自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できるスキル向上の取組が必要である旨を記載する。
  - 指示４について、リスクアセスメントの対象を自社のデジタル環境だけでなく、自社製品にも拡大するとともに、テレワーク等の働き方の変化の影響に関する検討の必要性を記載する。
  - 指示６について、PDCAサイクルを通じた改善プロセスにおける経営者の関与の必要性を記載する。
  - 指示７について、インシデント対応体制の構築にあたっては、サプライチェーンを通じたつながりを考慮する必要があること、及び制御系を含めた演習の必要性等について記載する。
  - 指示８について、事業継続の観点から、制御系も含めた業務の復旧プロセスと整合性のとれた復旧計画・体制の整備の必要性や対象をIT系・社内・インシデントに限定せず、サプライチェーンも含めた実践的な演習の実施等について記載する。
  - 指示９について、自社へのリスク波及を防ぐ観点からサプライチェーン全体での対策が必要であること、委託先に一方的な対策を強いるのでなく、方策の実効性を高めることを記載する。
  - 指示１０について、有益な情報を得るためには適切な情報を提供することも必要であることを強調しつつ、被害の報告・公表への備えをすることやステークホルダーへの情報開示について記載する。
  - その他、全体的に対策を怠った場合のシナリオや対策例の追記、「サイバー攻撃被害に係る情報の共有・公表ガイダンス」の活用に関する記載を行う。
- コーポレートガバナンス及びエンタープライズリスクマネジメントに関する経済産業省、関連府省庁及び国際的な取組等と本ガイドラインとの関係性、ならびに関連ツール等との関係性の体系をわかりやすく伝えるため、次ページ図2.2に示す「サイバーセキュリティ経営ガイドラインの体系」を記載することとする。

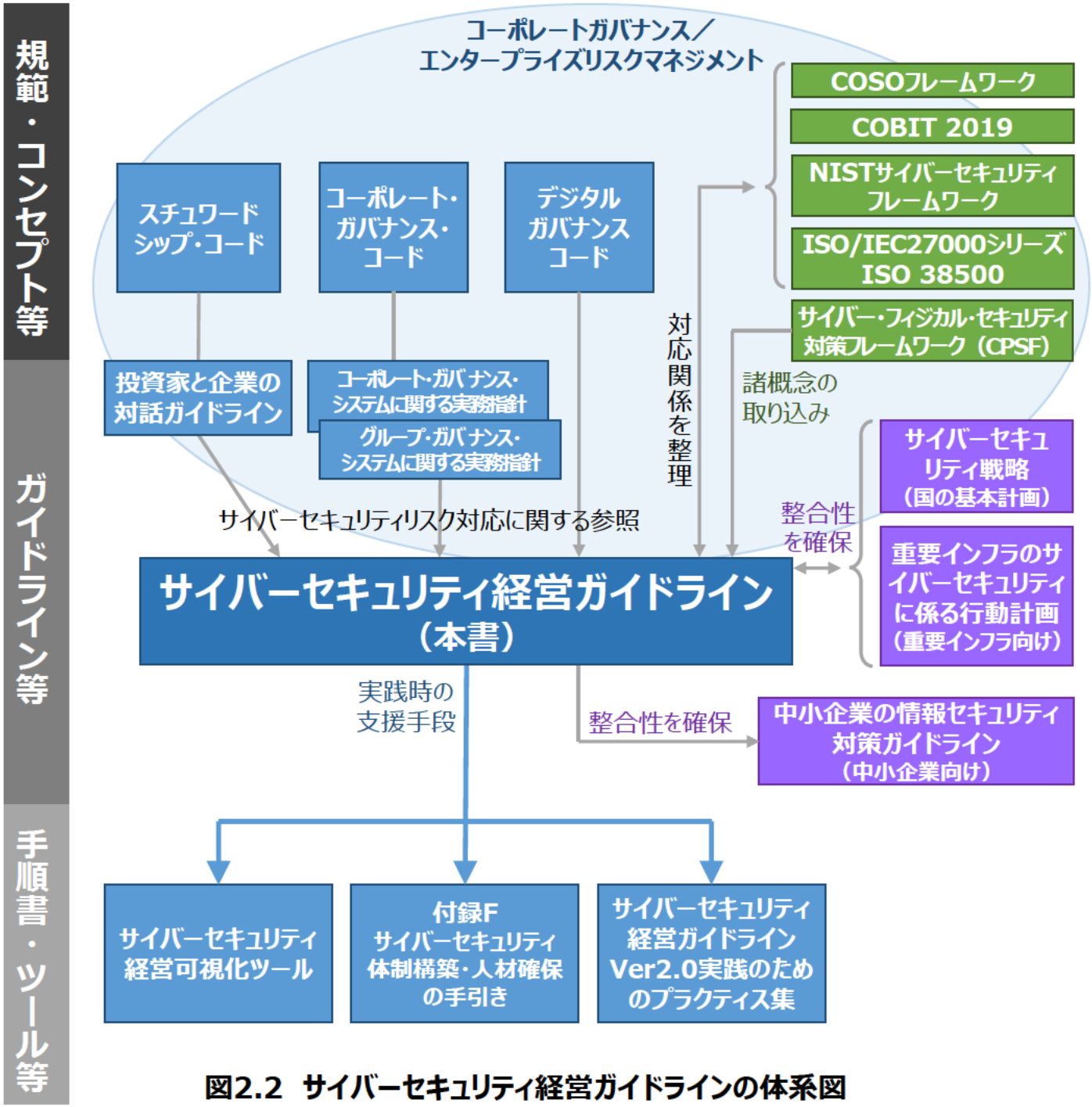

図2.2　サイバーセキュリティ経営ガイドラインの体系図

2.1.2 サイバーセキュリティ経営ガイドライン改訂方針案の作成

(2) サイバーセキュリティ経営ガイドラインVer2.0付録の改訂

- 2.2に示す有識者会議での審議の結果、経営ガイドラインVer3.0の付録の構成はVer2.0の構成を維持しつつ、以下の改訂を行うとともに、各付録の利用主体、及び経営者としてどのように関わるべきかの説明を追記することとなった。
  - 付録A及び付録Cに経営者向けの内容を追加
  - 付録B及び付録Eについて、経営ガイドライン本編の改訂に対応する情報源や用語を追加
  - 付録Dについて、規格の改訂に対応するとともに、NISTサイバーセキュリティフレームワーク、CIS Controls等を追加

(3) サイバーセキュリティ経営可視化ツールの改訂

- (1)(2)の検討を踏まえ、情報処理推進機構にて検討の結果、サイバーセキュリティ経営可視化ツールは以下の方針で改訂を行うこととなった。
  - 現行の成熟度モデルに基づくセルフチェックの方法を踏襲（レベル定義は一部見直し）
  - 経営ガイドラインVer3.0の改訂に合わせ、チェック項目や回答のヒントの内容を更新
  - プラス・セキュリティに関するチェック項目を追加
  - セルフチェックを行いやすくするための回答のヒントの追記

2.2 有識者会議の開催

(1) 有識者会議の設置

- 以下の各点について議論を行うための有識者会議として、次表のメンバーで構成される「サイバーセキュリティ経営ガイドライン改訂に関する研究会」を設置した。
  - サイバーセキュリティ経営ガイドラインVer2.0及び付録文書の改訂
  - 改訂したサイバーセキュリティ経営ガイドラインの活用及び普及方策の検討
  - その他

表2.x 「サイバーセキュリティ経営ガイドライン改訂に関する研究会」構成員

氏名（敬称略）	所属・役職
稲垣 隆一	稲垣隆一法律事務所　弁護士
小松 文子	長崎県立大学 情報システム学部 情報セキュリティ学科　教授
佐々木 良一	東京電機大学　名誉教授 兼 サイバーセキュリティ研究所　客員教授
佐藤　亘	一般社団法人日本情報システム・ユーザー協会　事務局長
比留間 貴士	特定非営利活動法人ITコーディネータ協会　常務理事・事務局長
丸山 司郎	株式会社FFRIセキュリティ　セキュリティサービス本部長
丸山 満彦	PwCコンサルティング合同会社 テクノロジーコンサルティング　パートナー
三輪 信雄	S&J株式会社　代表取締役社長
山本 純也	株式会社OTデザイン研究所　代表取締役
湯淺 墾道	明治大学 公共政策大学院 ガバナンス研究科　教授
オブザーバ	内閣サイバーセキュリティセンター、独立行政法人情報処理推進機構

2.2 有識者会議の開催

(2) 有識者会議の開催状況

- (1)に示したメンバーにて、以下の計４回の検討を実施した。

表2.2 「サイバーセキュリティ経営ガイドライン改訂に関する研究会」2022年度開催状況

会議	開催日	おもな議題
第1回	2022年7月8日	● サイバーセキュリティ経営ガイドライン改訂に関する要望と改訂案について ● サイバーセキュリティ経営ガイドライン改訂スケジュールについて
第2回	2022年9月26日	● サイバーセキュリティ経営ガイドライン（本編）改訂案について ● サイバーセキュリティ経営ガイドライン（付録）改訂方針について
第3回	2023年1月11日	● パブリックコメント結果を踏まえたサイバーセキュリティ経営ガイドライン（本編）の改訂案について ● サイバーセキュリティ経営ガイドライン（付録）及びサイバーセキュリティ経営可視化ツールの改訂方針について
第4回	2023年3月8日	● サイバーセキュリティ経営ガイドライン（付録）の改訂案について ● 今後のサイバーセキュリティ経営ガイドライン（付録）の在り方と見直しの方向性について

2.2 有識者会議の開催

(3) 有識者会議におけるおもな合意事項

- 「サイバーセキュリティ経営ガイドライン改訂に関する研究会」において、次の各項についての審議を実施した。

① サイバーセキュリティ経営ガイドラインVer2.0の改訂に関する検討

- 2.1.2(1)に記載の通り、サイバーセキュリティ経営ガイドラインVer2.0の本編の改訂方針について審議し、検討に基づく成果物をVer3.0のパブリックコメント案として合意した。
- 2.1.2(2)に記載の通り、サイバーセキュリティ経営ガイドラインVer2.0の付録の改訂方針について審議し、Ver3.0の付録とすべき内容をとりまとめるとともに、今後の付録の在り方についての審議を実施した。

② パブリックコメント対応について

- 2022年10月26日から同年12月5日にかけてパブリックコメントを実施し、得られたコメントの内容を踏まえた経営ガイドラインVer3.0案の見直しに関する審議を行った。

2.3 政府会議等における議論の把握

- 本調査の実施にあたり、下記に示す政府会議等の公表情報（配付資料、議事録、報告書等）をもとに、有識者による議論を把握し、本事業の調査内容において整合を諮るとともに、調査結果の分析や報告書の作成に反映した。
  - 経済産業省「産業サイバーセキュリティ研究会」
    - WG2 第8回会合（2022年3月23日開催）
    - WG3 第7回会合（2022年4月6日開催）
    - WG3 IoT製品に対するセキュリティ適合性評価制度構築に向けた検討会 第1回会合（2022年11月1日開催）
    - WG3 IoT製品に対するセキュリティ適合性評価制度構築に向けた検討会 第2回会合（2023年2月6日開催）
  - 内閣サイバーセキュリティセンター「サイバーセキュリティ戦略本部」
    - 第33回会合（2022年5月30日開催）
    - 第34回会合（2022年6月17日開催）
    - 普及啓発・人材育成専門調査会 第17回会合（2022年6月10日開催）
    - 普及啓発・人材育成専門調査会 第18回会合（2022年9月1日開催）
    - 普及啓発・人材育成専門調査会 第19回会合（2022年10月31日開催）
  - サイバーセキュリティ協議会運営委員会
    - サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会（2022年3月16日に『サイバー攻撃被害に係る情報の共有・公表ガイダンス』を公表）
  - 経済安全保障法制に関する有識者会議
    - 第1回会合（2022年7月25日開催）、第2回会合（2022年9月12日開催）、第3回会合（2022年10月6日開催）、第4回会合（2022年11月16日開催）、第2回会合（2023年2月8日開催）

3. 情報セキュリティサービス活用・普及に関する調査

3.1 有識者会議の開催

(1) 有識者の選定

- 調査趣旨を踏まえ、以下の目的を中心とする検討を行うため、下表に示す有識者で構成される「情報セキュリティサービス普及促進に関する検討会」を設置した。
  - 情報セキュリティサービス基準（附則を含む）において見直しが必要な事項
  - 情報セキュリティサービス審査登録制度の普及促進における課題と取組の検討

表3.1 「情報セキュリティサービス普及促進に関する検討会」構成員

氏名（敬称略）	所 属
阿部 恭一	ANAシステムズ株式会社 品質・セキュリティ監理室エグゼクティブマネージャ
川口 洋	株式会社川口設計 代表取締役
小屋 晋吾	一般社団法人ソフトウェア協会（SAJ）セキュリティ委員会副委員長
佐藤 健志	日本商工会議所 情報化推進部 部長
佐藤 元彦	伊藤忠商事株式会社IT企画部技術統括室ITCCERT上級サイバーセキュリティ分析官
佐藤 芳紀	森ビル株式会社 IT推進部 セキュリティグループ 課長
下村 正洋	特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）事務局長
土居 範久	慶應義塾大学 名誉教授
永宮 直史	特定非営利活動法人日本セキュリティ監査協会（JASA）エグゼクティブフェロー
宮下 清	一般社団法人日本情報システム・ユーザ協会（JUAS）主席研究員
オブザーバー： 内閣サイバーセキュリティセンター（NISC）、総務省、独立行政法人情報処理推進機構（IPA）	

3.1 有識者会議の開催

(2) 有識者会議の開催状況

- (1)に示したメンバーにて、以下の計3回の検討を実施した。

表3.2 「情報セキュリティサービス普及促進に関する検討会」2022年度開催状況

会議	開催日	おもな議題
第1回	2022年7月28日	● 「情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示」の見直しについて ● 情報セキュリティサービス基準適合サービスリストの様式見直しについて ● 「情報セキュリティサービス基準」における情報セキュリティサービスの追加について ● その他今年度検討すべき事項について
第2回	2022年12月23日	● 機器検証サービスの追加に関する情報セキュリティサービス基準等の改訂について ● 例示の改訂に関する検討について ● サービス追加に関する調査結果について
第3回	2023年3月3日	● パブリックコメント結果を踏まえた情報セキュリティサービス基準等の改訂案について ● リスト利用者向け掲載事項について ● リスト利用者へのアンケート結果について

3.2 有識者会議の開催

(3) 有識者会議におけるおもな合意事項

- 「情報セキュリティサービス普及促進に関する検討会」において、次の各項についての審議を実施した。

① 情報セキュリティサービス基準における情報セキュリティサービスの追加に関する検討

- 経済産業省における事業成果及び昨年度実施したパブリックコメントへの対応の観点からサービスの追加についての審議を行った結果、「機器検証サービス」について追加が適切との判断となり、後述の③に示すように当該サービスを追加する形で情報セキュリティサービス基準を改訂し、そのためのパブリックコメントを実施することとなった。

② 情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示の見直しについて

- 情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示の見直しの必要性についての審議を実施した結果、①で追加することとなった機器検証サービスに関連する例示以外の追加は不要との結論で合意された。

③ パブリックコメント対応について

- ①の審議結果をもとに、機器検証サービスを追加した情報セキュリティサービス基準等の改訂案を作成し、同案について2023年1月16日から同年2月17日にかけてパブリックコメントを実施した。得られたコメントの内容を踏まえ、情報セキュリティサービス基準案及び情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示案の見直しに関する審議を行った。
- パブリックコメントを反映した情報セキュリティサービス基準（第３版）及び情報セキュリティサービスにおける技術及び品質の確保に資する取組の例示（第２版）は2023年3月末に経済産業省より公表予定である。

3.3 有識者会議の議論を受けた調査の実施

- 有識者会議において、ペネトレーションテストサービス及びインシデントレスポンスサービスを将来的に制度の対象とすべきかどうかの検討にあたり、サービス提供事業者における意向やサービスの定義状況等を把握すべきとの意見が出たことを踏まえ、下表の要領にてアンケート調査及びヒアリング調査を実施し、結果を有識者会議にて報告した。

表3.3 ペネトレーションテストサービスに関するアンケート調査概要

調査目的	● 情報セキュリティ審査登録制度において、脆弱性診断サービスとは別にペネトレーションテストサービスを追加することの適切性についての審議に資するため、サービス提供事業者におけるサービスの提供状況及びサービスを追加することへの関心の状況を把握する。 ● サービス提供事業者によって異なるとされるペネトレーションテストの定義の実態を把握する。
調査対象	2022年11月1日時点で脆弱性診断サービスに登録されている事業者のうち33事業者
調査項目例	● ペネトレーションテストサービスの提供状況 ● ペネトレーションテストサービスの定義 ● ペネトレーションテストサービスが登録対象に追加されることは有益か、費用負担意向はあるか

表3.4 インシデントレスポンスサービスに関するヒアリング調査概要

調査目的	● 情報セキュリティ審査登録制度において、デジタルフォレンジックサービスとは別にインシデントレスポンスサービスを追加することの適切性についての審議に資するため、サービス提供事業者におけるサービスの提供状況及びサービスを追加することへの関心の状況を把握する。
調査対象	2022年11月1日時点で以下の両方を満たす４事業者 ● 情報セキュリティサービス基準適合サービスリスト（デジタルフォレンジックサービス）に掲載 ● NPO日本ネットワークセキュリティ協会(JNSA)の『サイバーインシデント緊急対応企業一覧』に掲載
調査項目例	● 自社で考えるインシデントレスポンスサービスの定義（どのような作業が含まれるのか） ● インシデントレスポンスサービスの品質を確保するために重視している事項は何か ● インシデントレスポンスサービスが登録対象に追加されることは有益か、費用負担意向はあるか

3.3 有識者会議の議論を受けた調査の実施

＜調査結果抜粋：ペネトレーションテストサービスの品質確保のために必要なこと＞

- ペネトレーションテストサービスの品質を確保するために必要なことと考えている内容について尋ねた結果を示す。
- すべての回答者がサービス品質を向上させるための知見の共有・更新が必要と考えているほか、要員のスキル向上についても１サンプルを除いて必要と考えている。

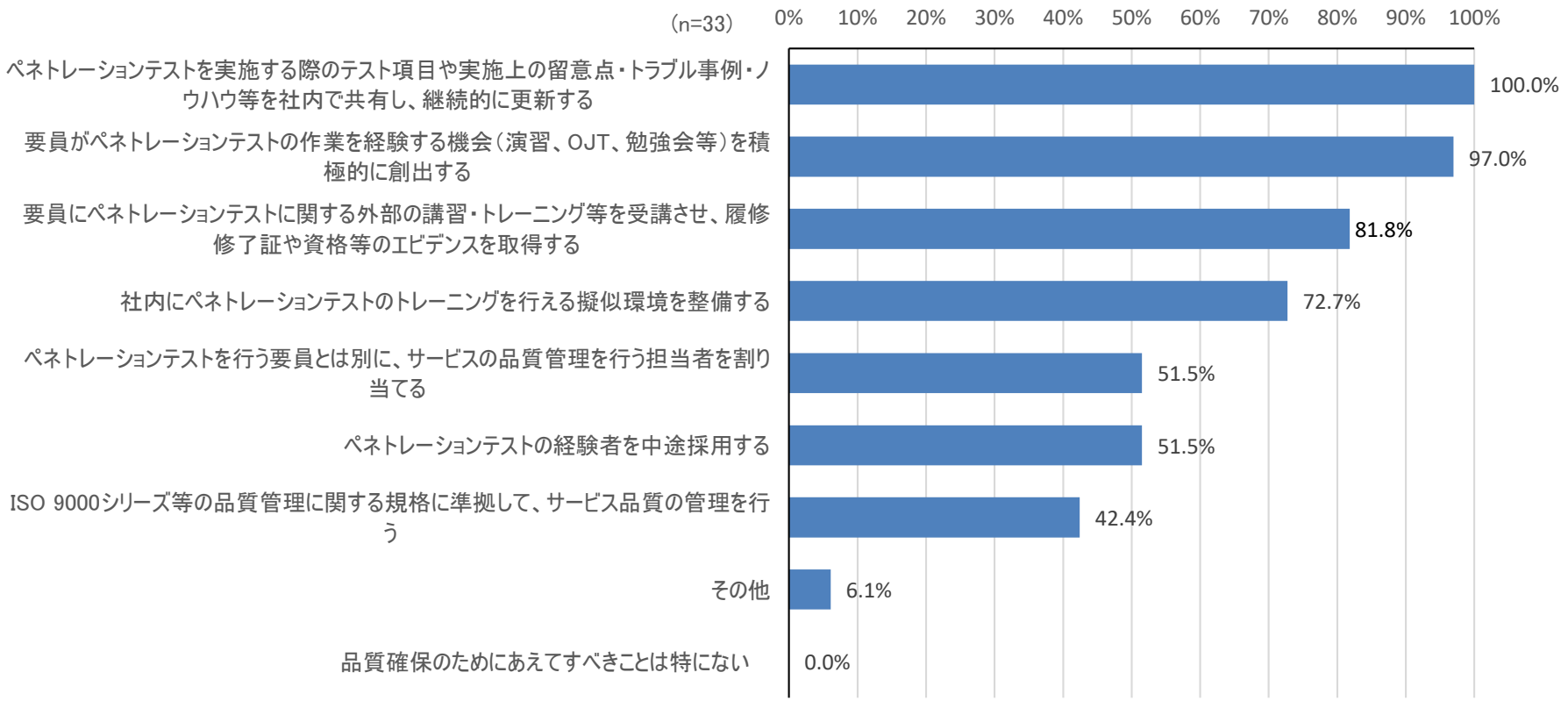

図3.1 ペネトレーションテストサービスの品質確保のために必要なこと

3.4 情報セキュリティサービスユーザへのアンケート調査の実施

3.4.1 調査概要

- 情報セキュリティサービスの普及促進・活用に向け、利用者側がどのようにサービスの選定を行うか、より詳細な実態把握を行う観点から、企業等で情報セキュリティサービスの調達に携わるモニターを対象とする、情報セキュリティサービス利用の実態、制度の認知状況及び制度へのニーズに関するウェブアンケート調査を下表の要領にて実施した。

表3.5 アンケート調査概要

調査目的	● 情報セキュリティサービスを利用する企業における制度の認知状況及び活用に関する実態を、可能な限り正確に把握する ● 2020年に実施した同様の調査との経験比較により、普及活動の効果とサービス提供事業者の増加による影響について分析する
調査対象	全国のユーザー企業でサイバーセキュリティ対策関連業務に従事するアンケート回答モニター　400名 （企業に勤務するモニター50,000名を対象とするスクリーニング調査をもとに抽出）
調査方法	アンケート事業者のアンケートシステムを用いたウェブアンケート
実施時期	2023年2月27日～28日
質問事項	● 勤務先企業におけるIT利活用とセキュリティサービス利用状況 ● 情報セキュリティサービス審査登録制度の認知と活用状況 ● 登録サービスの利用経験とその結果 ● 情報セキュリティサービス利用の課題 ● 情報セキュリティサービス審査登録制度への要望

3.4.2 アンケート調査結果

(1) 情報セキュリティサービス審査登録制度の認知度

- 回答者における情報セキュリティサービス審査登録制度の認知状況を示す。
- 前回調査と比較すると、わずかながら制度の認知度が低下している。ただし、「名前は聞いたことがある」まで含めるとほぼ前回調査と同様である。

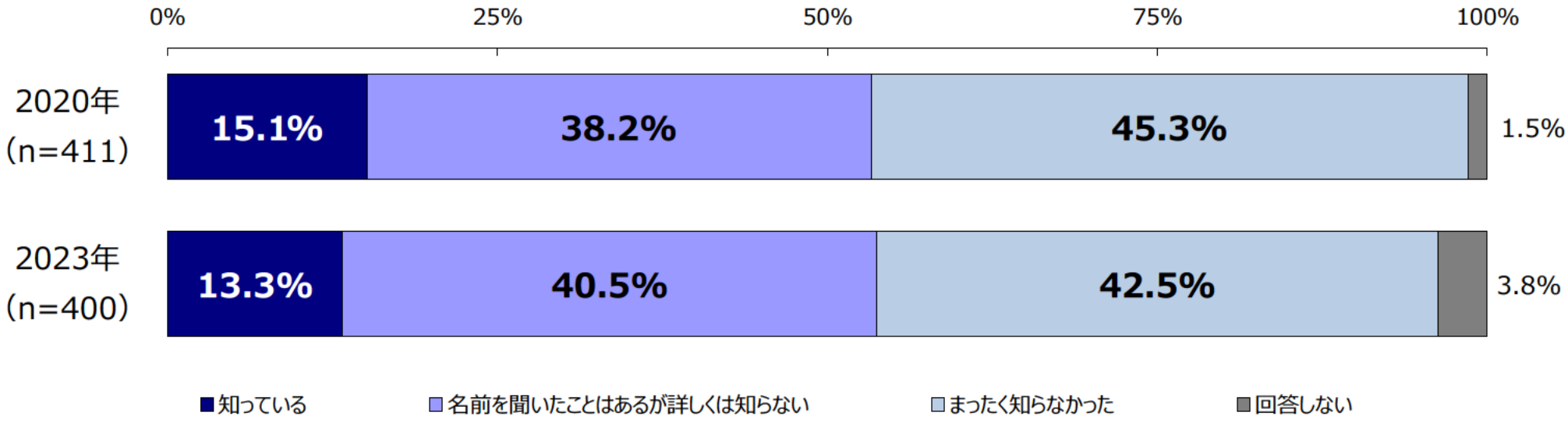

図3.2　情報セキュリティサービス審査登録制度の認知度

3.4.2 アンケート調査結果

(2) 情報セキュリティサービス審査登録制度の利用経験

- (1)で「知っている」を選択した回答者に、情報セキュリティサービス審査登録制度を用いてサービスを選定した経験があるかどうかを尋ねた結果を示す。
- 前回調査と比較すると、リストを知っているだけで活用していない回答者が減少し、実際に発注した経験をもつ回答者の比率が増えている。

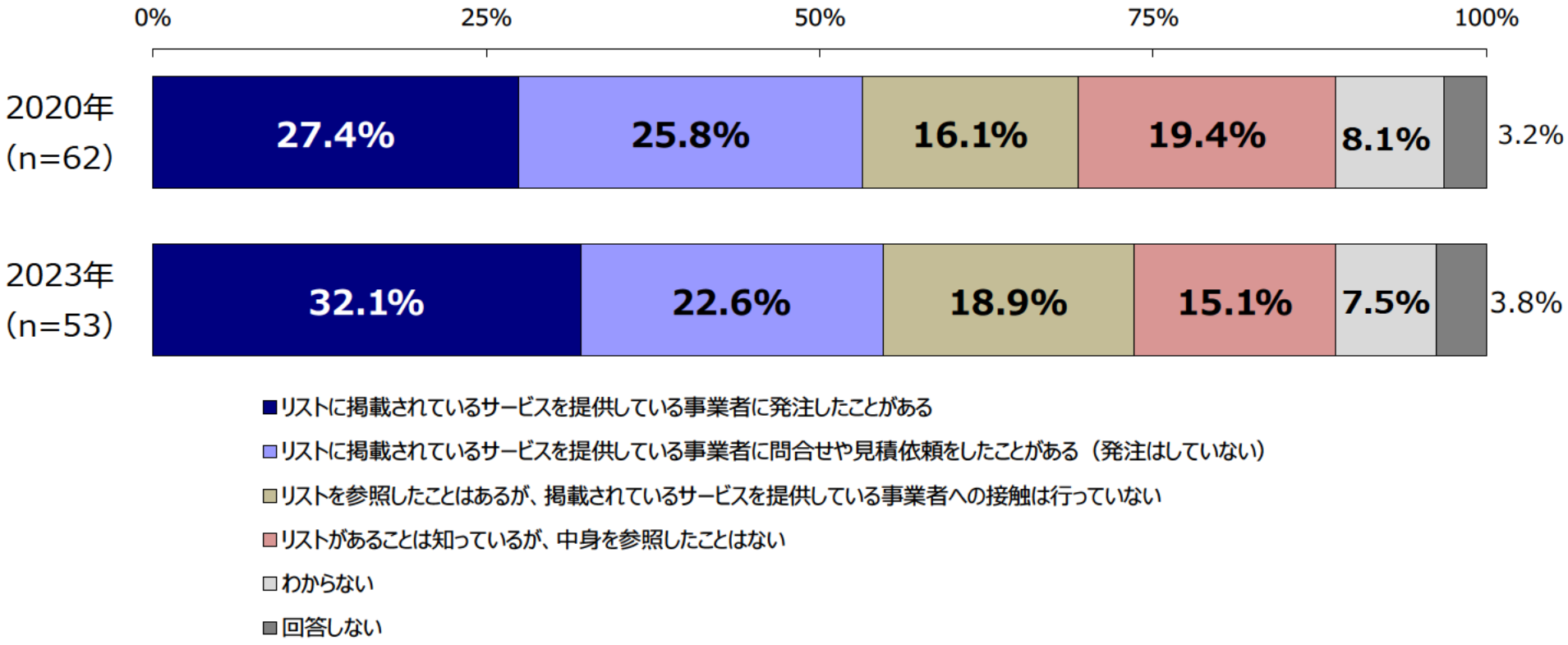

図3.3　情報セキュリティサービス審査登録制度の利用経験

3.4.2 アンケート調査結果

(3) 情報セキュリティサービス審査登録制度への要望

- (1)で「知っている」を選択した回答者に、情報セキュリティサービス基準適合サービスリストを自社で活用しようとするために期待したい要望について尋ねた結果を示す。
- 本設問については前回調査と選択肢の構成を大きく変更しているため、経年比較は困難であるが、登録数を増やすことへの要望が最多であるという傾向は前回と変わっていない。

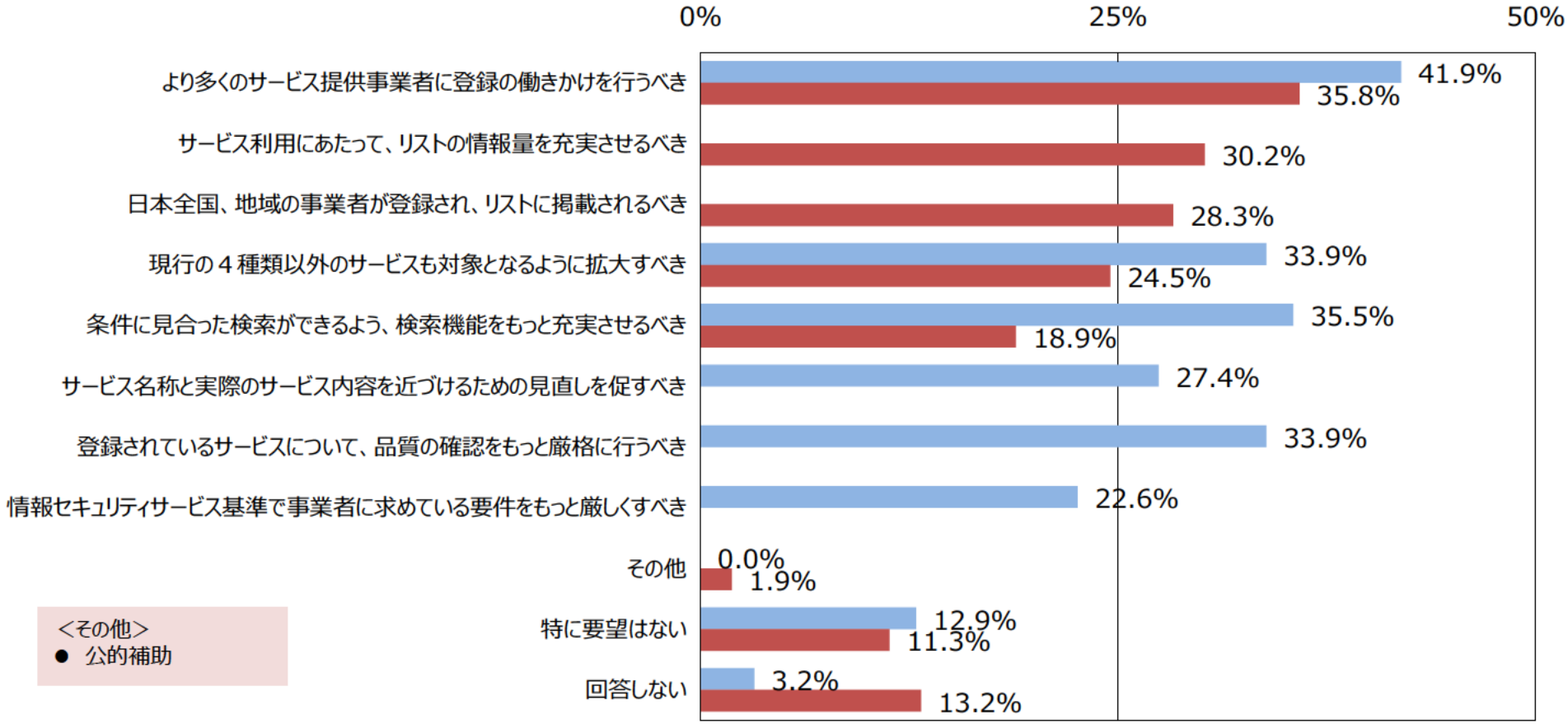

図3.4　情報セキュリティサービス審査登録制度への要望

3.4.2 アンケート調査結果

(4) 今後制度の対象とすべき情報セキュリティサービス

- (3)で「現行の４種類以外のサービスも対象となるように拡大すべき」を選択した回答者に、追加すべき具体的サービスについて尋ねた結果を示す。なお、今回調査の実施は機器検証サービスの追加に関するパブリックコメントの実施直後であったため、調査時にはその旨の補足を行っている。また、本設問は今回のみ調査を行っている。
- 最多はコンサルティングサービスであり、機器検証サービスもそれに続く第２位の結果となっている。本報告書3.4.2に示したペネトレーションテストサービス及びインシデントレスポンスサービスについては、現行のサービスでもある程度対応可能なこともあるためか比率は高くならなかった。

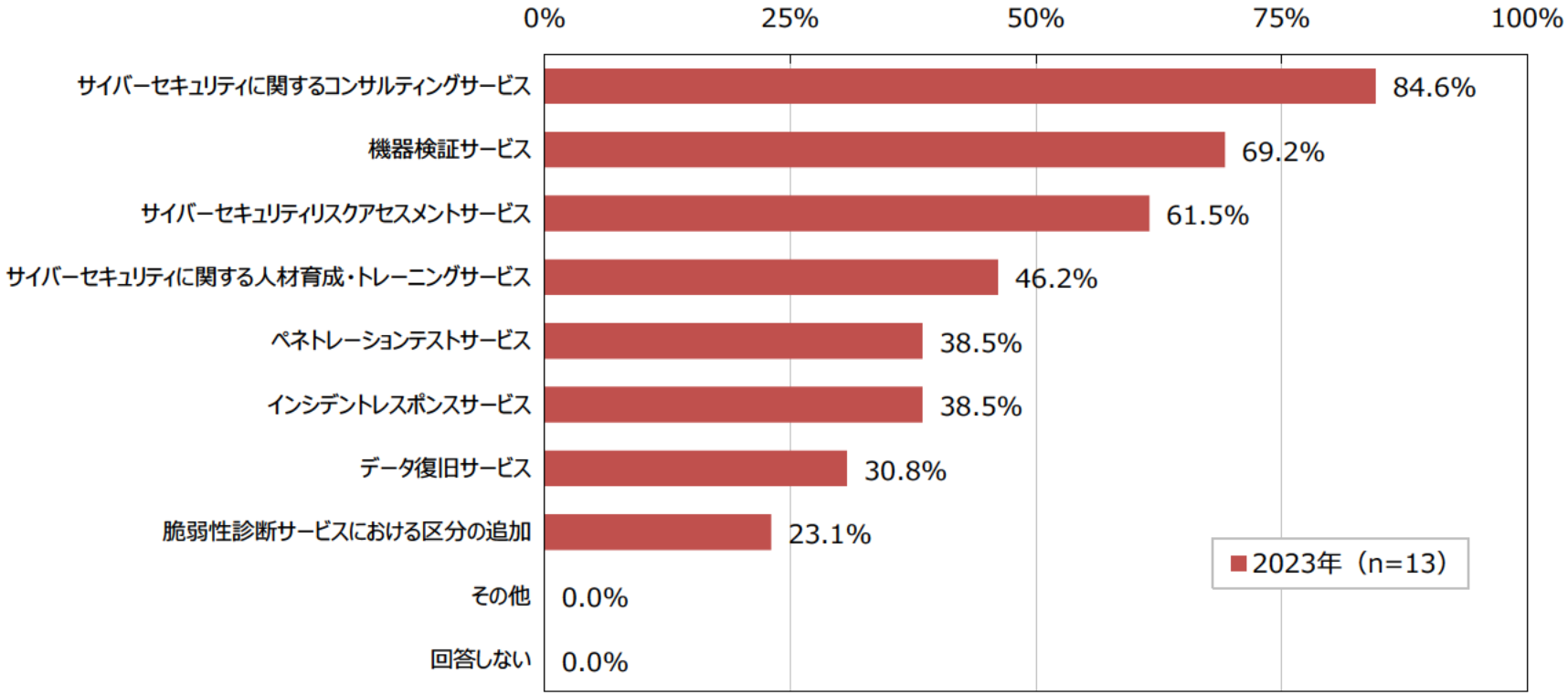

図3.5　今後制度の対象とすべき情報セキュリティサービス

3.4.2 アンケート調査結果

(5) サービスや提供事業者への要望

- (1)で「知っている」を選択した回答者に、今後リストを自社で活用するために、リストに掲載されるサービスやサービスを提供する事業者に関する要望について尋ねた結果を示す。本設問は今回のみ調査を行っている。
- 「品質の確認をもっと厳格に行うべき」との回答が最多であり、サービス利用企業において現状のサービス品質に満足していない実態が推察される。なお、厳格化の具体的内容としては、「品質に関するKPIやKRIの記載」「できていることとの差の明確化」「ケーススタディを示す」等が挙げられている。

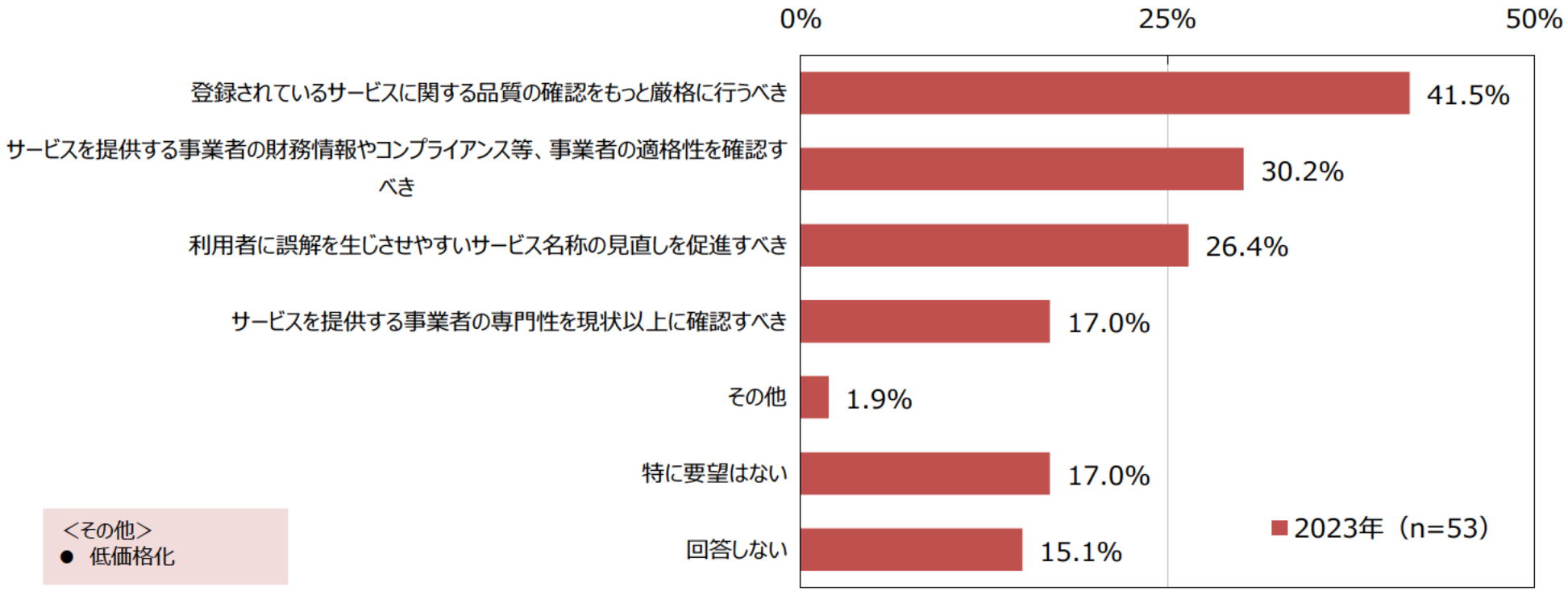

図3.6 サービスや提供事業者への要望

3.4.2 アンケート調査結果

(6) 事業者の適格性確認への要望

- (5)で事業者の適格性を確認すべき」を選択した回答者に、具体的にどのような確認が行われていると事業者を信頼でき、サービスを利用しやすくなると思うかについて尋ねた結果を示す。本設問は今回のみ調査を行っている。
- 該当する回答者の全員が、「事業者が満たすべき財務、コンプライアンス等の条件を設定し、審査によって確認」すべき旨を選択しており、事業者による自主的な開示がそれに続いている。

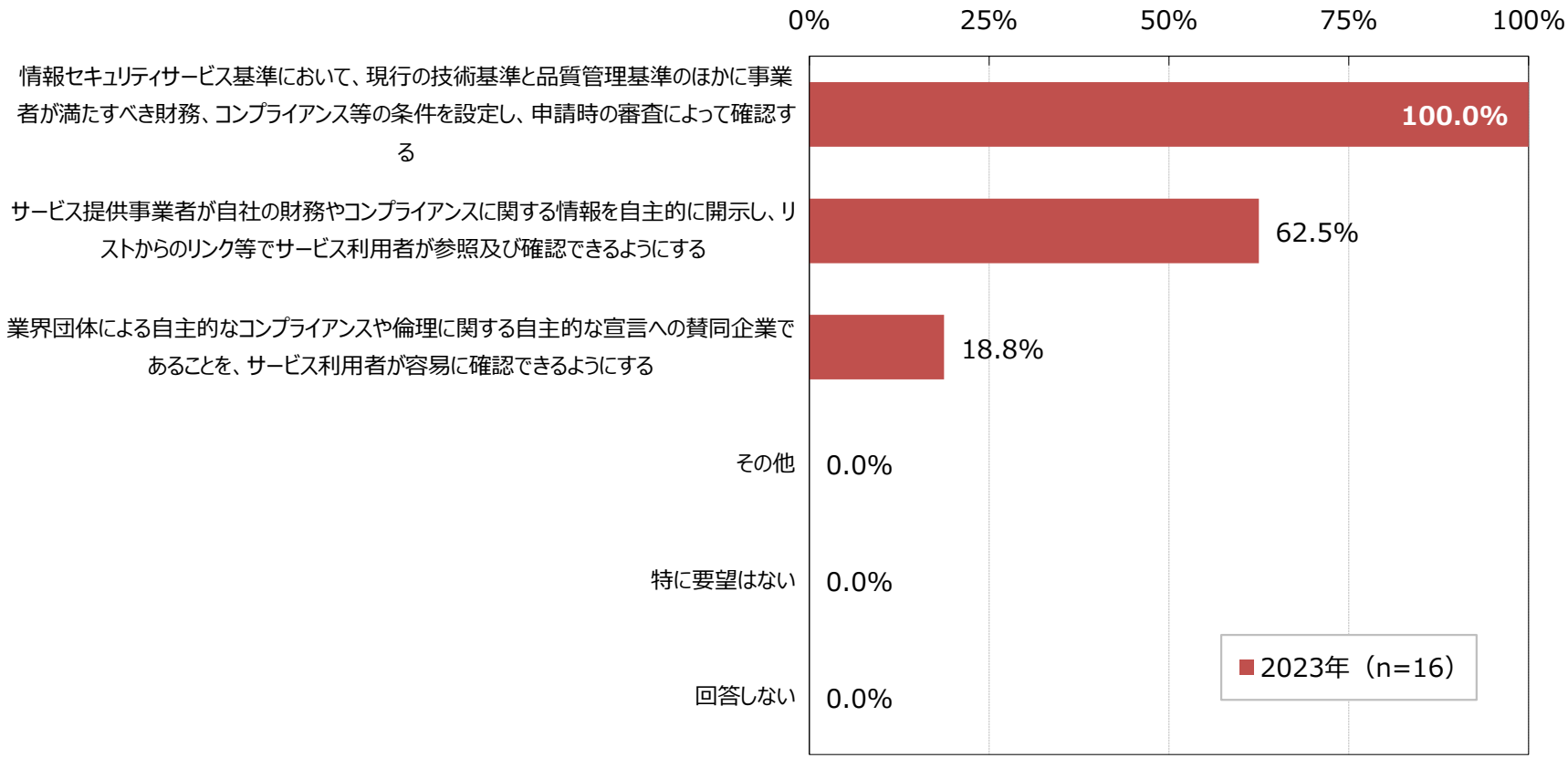

図3.7　事業者の適格性確認への要望

3.4.3 アンケート調査結果のまとめ

- アンケート調査を通じて観察される傾向は次の通りである。

(1) 制度の認知度と活用状況について

- 認知度はやや低下している。ただし「名前は聞いたことがある」まで含めるとほぼ変化がない。
- リストの活用状況はやや向上しており、制度を認知している回答者の 3 割超が発注実績を有している。

(2) サービス利用者における制度への期待について

- 最も要望が多いのはコンサルティングサービスであるが、機器検証サービスもそれに次ぐ関心を呼んでいる。
- ペネトレーションサービスやインシデントレスポンスサービスへの関心は低めとなっている。
- サービス品質の確認を厳格化することへの期待が高い。

４．まとめ

- 本調査では、本報告書2.～3.の各項において示した調査項目に基づき、企業におけるサイバーセキュリティ経営の実現を支援する取組に関する調査を実施した。
  - 企業経営層とその指示を受ける担当者を対象とするサイバーセキュリティ経営ガイドライン及び可視化ツールの改訂及び普及促進
  - 情報セキュリティサービス基準の改訂及びこれを用いて運用される情報セキュリティサービス審査登録制度の普及促進策の検討
- これらの取組は、国内企業や社会におけるデジタル活用の進展がもたらすサイバーセキュリティリスクの変化に対応するために適時に実施すべきものであり、本調査の実施期間中でも必要な見直しを実践することで国内サイバーセキュリティ分野における最新の動向に対応した。
- 本調査において改訂を行った経営ガイドライン及び情報セキュリティサービス基準は、今後も継続的に保守及び更新を行っていく必要がある。このうち経営ガイドラインについては、本編の内容は特定の技術や脅威に依存するものではなく、短期で頻繁に更新するものではないとされる一方、付録については改訂の必要に応じて適宜更新していくことが望ましいとされ、今後は両者を分けて更新していくことが想定されている。情報セキュリティサービス基準については、サービス提供ベンダー及びサービス利用者からのサービス追加への要望、ならびにサービスの品質の維持・向上のための取組への期待があることを踏まえ、サービスや品質の定義等の整備等の取組を着実に進めていくことが求められる。