令和６年度産業サイバーセキュリティ強靱化事業
（システムやサービスに係る制度の普及促進等に関する調査）

調査報告書

2025年3月

みずほリサーチ＆テクノロジーズ株式会社

1. 事業の目的、実施内容等

(1) 事業の目的

- 近年、サイバー攻撃の脅威は顕在化し、デジタル社会を担うソフトウェアとそのサプライチェーン上の潜在的なあらゆる脆弱性を狙う攻撃が相次いでいる。デジタル社会の活動は様々な情報・通信システムやサービスを構成するあらゆるソフトウェアに深く依存しているため、ソフトウェアは経済活動や社会生活に根源的な製品と言える。将来的にもDX、IoT、５G・６G、AI、量子コンピュータとソフトウェアへの依存度は深まる一方である。そのためサイバー攻撃による被害発生時は、重要インフラを含め国民生活・経済活動に甚大な被害をもたらしデジタル社会の信頼性を損なうことになる。デジタル社会全体のレジリエンス向上のため、良質で信頼性の高いシステムやサービスを持続的に提供できるような制度の検討や企業等における情報セキュリティ対策の状況を把握するための監査制度の更なる活用等を検討する必要がある。
- 本件は、以下に示す２つの事業の実施を通じて、信頼性の高いシステムやサービスを提供する事業者に関する調査やガイドライン作成、求められるセキュリティ水準の検討等を実施することにより、デジタル社会全体のレジリエンス向上及び情報セキュリティの確保等を目的とするものである。

①情報セキュリティサービス審査登録制度の普及促進及び更なる利活用に向けた調査、検討

我が国では様々な企業がセキュリティサービスを提供している一方で、企業によって提供するサービスの品質にばらつきが生じている。品質の低いサービスが提供されていることは望ましい状況ではなく、費用対効果の高いセキュリティ投資を促すために、一定の品質を備えたセキュリティサービスを認定する制度として、平成２７年に「情報セキュリティサービス審査登録制度(以下「本制度」という。)」が設立された。本制度は提供企業ごとに異なる内容が提供されるセキュリティサービスにおいて、サービスの内容に対して基準を設けて認定することは困難であり、また、サイバーセキュリティを取り巻く状況の変化も早いことから、サービスを提供する企業のサービス品質を保つための取組を確認することで認定を得られる制度とした経緯があり、現在は、サービス事業者の信頼性を可視化する最低限の要件として、技術要件と品質管理要件を基準に示し、それに合致する事業者をリストで公開している。本制度はサービスを審査登録する制度であるが、サービスの審査登録にあたっては、サービス提供事業者自身の信頼性を確認する必要があるのではないかとの考えもある。また、現在は対象を情報セキュリティサービスに限った制度であるが、その対象を広げることについても検討すべきとの意見もある。

1. 事業の目的、実施内容等

（前ページからの続き）

これらを踏まえ、本事業では技術要件と品質管理要件を世の中の状況に合わせた最新の状態に更新すること及びサービス提供事業者の信頼性を示すことについての検討、並びに本制度が対象とする項目を広げることについての調査、検討を実施し、本制度の基準の改定内容を策定するとともに、本制度の基準を満たすサービスが市場で認知される様、本制度の普及策の検討・策定を行い、対象を広げるにあたっての整理及び検討を行うことを目的とするものである。

②情報セキュリティ監査制度の更なる利活用に向けた検討

経済産業省では、企業等が効率的に情報セキュリティマネジメント体制の構築と、適切な管理策の整備と運用を行えるように、情報セキュリティ監査業務の品質を確保し、有効かつ効率的に監査を実施することを目的とした監査人の行為規範である「情報セキュリティ監査基準」（平成１５年経済産業告示第１１４号。以下「監査基準」という。）、情報セキュリティマネジメントの基本的な枠組みと具体的な管理項目を規定した「情報セキュリティ管理基準」（以下、「管理基準」という。）を策定し、公表している。

他方、監査基準及び管理基準については、前回の改訂から数年経過しようとしているところ、前回の改訂後に公開された国際、国内基準等に対応できていない状態となっており、また、企業等における有効かつ効率的な情報セキュリティ監査の実施につなげるためには、それらの国際、国内基準等の反映が必要な状況となっている。

これらを踏まえ、本事業においては、監査基準及び管理基準の改訂及び情報セキュリティ監査制度の活用のあり方に関する検討会を開催し、当該検討会での議論等を踏まえた改訂案を作成するとともに、情報セキュリティ監査制度の活用のあり方について、検討を行うことにより、より実情に即した質の高い情報セキュリティ監査制度を普及実現させることを目的とするものである。

以降の記述において、前述の略称のほか、次の略称を用いることとする。
「情報セキュリティサービス審査登録制度」　→　「審査登録制度」
「情報セキュリティ監査制度」　→　「監査制度」
「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」　→　「例示」
「情報セキュリティサービス基準適合サービスリスト」　→　「リスト」

1. 事業の目的、実施内容等

(2) 事業の目的

① 情報セキュリティサービス審査登録制度の普及促進及び更なる利活用に向けた調査、検討

- (1)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章にて示す。

表1.1　事業実施内容（情報セキュリティサービス審査登録制度関連）

実施項目	実施内容
ア　情報セキュリティサービス審査登録制度に関する検討会の開催	● 専門的な視点からの検討、分析及び助言を得るために、本事業に関係する民間企業、業界団体、関係機関、学識者等10名の有識者からなる検討会を設置し、期間中２回の開催にあたっての事務局運営を担当した。
イ　改訂案の作成、編集作業	● 審査登録制度に対する社会的な期待等を踏まえて情報セキュリティサービス基準及びその例示等に関する改訂案を作成し、アの検討会による承認を得た。
ウ　情報セキュリティサービス審査登録制度の更なる普及促進の検討	● 情報セキュリティサービスの利用者側の関係団体との意見交換を実施した。 ● 意見交換及び前年度までの検討結果を踏まえつつ、審査登録制度の更なる普及に向けて実施すべき取組等についての検討を実施し、アの検討会において審議を実施した。
エ　本制度の対象を拡張するための調査	● 今後の制度拡張として、審査登録対象サービスの追加候補となり得る情報セキュリティサービスについて、審査対象とする場合の検討課題等について整理した。

1. 事業の目的、実施内容等

(2) 事業の目的

② 情報セキュリティ監査制度の更なる利活用に向けた検討

- (1)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3章にて示す。

表1.2　事業実施内容（情報セキュリティ監査制度関連）

実施項目	実施内容
ア　情報セキュリティ監査に関する検討会の開催	● 専門的な視点からの検討、分析及び助言を得るために、本事業に関係する民間企業、業界団体、関係機関、学識者等11名の有識者からなる検討会を設置し、期間中3回の開催にあたっての事務局運営を担当した。
イ　改訂案の作成、編集作業	● 監査制度を取り巻く環境の変化、制度に対する社会的な期待及び監査制度関係者を対象とするアンケート調査結果をもとに、情報セキュリティ監査基準、情報セキュリティ管理基準及び関連ガイドライン等に関する改訂案を作成し、アの検討会による承認を得た。 ● 検討会にて承認された改訂案をもとに実施されたパブリックコメントに寄せられたコメントをもとに改訂案の編集・校正作業を実施し、アの検討会による審議を経て、改訂に関する最終案をとりまとめた。
ウ　情報セキュリティ監査制度の更なる活用策の検討	● 企業等におけるセキュリティ対策に関する監査への現況及びアの検討会における審議内容をもとに、監査制度とサイバーセキュリティ経営ガイドラインを連携させることで、企業におけるサイバーセキュリティ対策状況の可視化、リスクベースの管理及び監査の実施、並びに信頼性の高い情報開示につなげるための方策についての検討を実施した。

2. 情報セキュリティサービス審査登録制度の普及促進及び更なる利活用に向けた調査、検討

(1) 情報セキュリティサービス審査登録制度に関する検討会の開催

① 有識者の選定

- 事業趣旨を踏まえ、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。

表2.1 「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
委員長	土居 範久	慶應義塾大学 名誉教授
委員	阿部 恭一	ANAシステムズ株式会社 セキュリティマネジメント部 エグゼクティブマネージャー 株式会社レオンテクノロジー 相談役
	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）（2024年12月まで）
	佐藤 元彦	伊藤忠商事株式会社 IT・デジタル戦略部 技術統括室 ITCCERT 上級サイバーセキュリティ分析官 兼　伊藤忠サイバー＆インテリジェンス株式会社 CTO　主席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
	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
	萩原 健太	一般社団法人ソフトウェア協会（SAJ）（2025年1月以降）
	藤岡 友樹	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
	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：　独立行政法人情報処理推進機構（IPA）		

2. 情報セキュリティサービス審査登録制度の普及促進及び更なる利活用に向けた調査、検討

(1) 情報セキュリティサービス審査登録制度に関する検討会の開催

② 有識者会議の開催状況

- ①に示した構成員のもと、次の検討内容について次表の要領にて事業期間中２回の会合を開催した。
  - 情報セキュリティサービス審査登録制度で用いる基準等の改訂に関する検討
  - 情報セキュリティサービス審査登録制度の普及促進に関する検討
  - その他

表2.2 「情報セキュリティサービス普及促進に関する検討会」2024年度開催状況

会議	開催日	おもな議題
第1回	2024年8月30日	● 令和６年度の検討課題について
第2回	2025年2月13日	● 情報セキュリティサービス基準等の見直しについて ● 今後の制度普及促進の在り方について ● 今後の制度拡張について　他

2. 情報セキュリティサービス審査登録制度の普及促進及び更なる利活用に向けた調査、検討

(2) 改訂案の作成、編集作業

- 本事業においては、審査登録制度に対する利用者の期待に応えるため、現状において審査登録機関において実施している事業者自身が反社会的勢力に該当しないことや反社会的勢力への便益の供与又はそれに類する行為を行っていないこと等に関する確認を情報セキュリティサービス基準における要件として明示する観点での修正を実施することとした。この案を表2.3に示す。
- また、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（以下、「例示」という。）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に誤記または記載漏れが生じていることから、表2.4及び表2.5の要領にて修正を行う。
- このほか、昨年度に実施したパブリックコメントにおいて、情報セキュリティサービス基準と例示の版番号が異なりわかりにくいとの意見が示されていたことから、今回の改訂で見直しを行う。この案を表2.6に示す。
- 以上の改訂案について、2.(1)に示した有識者検討会での審議の結果、改訂内容は審査に大きな影響を与えるものではないことから、パブリックコメントの手続きを経ずに改訂結果を公表することが承認された。

表2.3　情報セキュリティサービス基準（第4.1版）改訂案（追加部分）

第１章　総則

２　定義

（９）反社会的勢力等

次のいずれかの条件を満たす者をいう。

ア　日本の法令に基づき、社会の安全を脅かす集団として指定を受け又は活動を制限された団体。

イ　情報システム又は通信回線を用いて日本の法令に反する行為を実施若しくは企図する個人又は団体。

第２章　情報セキュリティサービス提供事業者に関する事項

１　情報セキュリティサービス提供事業者に係る審査基準

情報セキュリティサービスを提供しようとする者は、次に掲げるすべての条件を満たすものであること。

ア　反社会的勢力等に該当しないこと。

イ　反社会的勢力等への便益の供与又はそれに類する行為を行っておらず、将来にわたっても行わないこと。

ウ　本基準の要件への適合性に関して疑義が生じた場合に、当該事項に関する調査を受け入れること。

表2.4　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における修正箇所（赤字部分）

４－２－１	脆弱性診断サービスの提供において用いる右に例示する内容相当の基準等及びその明示方法の例示	【Webアプリケーション脆弱性診断において、次に示す内容相当の診断を行う旨の提示】 ・OWASPの定めるASVS（Application Security Verification Standard）レベル１以上 ・独立行政法人情報処理推進機構による「ウェブ健康診断仕様」が定める診断内容 ・OWASPが定める「Security Testing Guideline」 ・日本セキュリティオペレーション事業者協議会及びOWASPによる脆弱性診断士スキルマッププロジェクトが定める「脆弱性診断ガイドライン」 【Webアプリケーション脆弱性診断において、次に示すツールを使用して診断を行う旨の提示】 ・Burp Suite ・HCL AppScan ・InsightAppsec/Appspider　←現在InsishtAppsec/Appspiderと誤っていたものを修正 ・OWASP ZAP ・Vulnerability Explorer（VEX） 【プラットフォーム脆弱性診断において、次に示すツールを使用して診断を行う旨の提示】 ・insightVM/Nexpose ・Nessus ・OpenVAS ・QualysGuard ・Tripwire IP360
４－２－２	ペネトレーションテスト（侵入試験）サービスの提供において用いる右に例示する内容相当の基準等及びその明示方法の例示	・NIST SP800-115（Technical Guide to Information Security Testing and Assessment - Recommendations of the National Institute of Standards and Technology） ・Penetration Testing Execution Standard (PTES) ・MITRE ATT&CKに示されている攻撃手法や技術

表2.5　情報セキュリティサービスに関する審査登録機関基準における修正箇所（赤字部分）

第２ 用語及び定義

この規格で用いる主な用語及び定義は，次による。

(1) 審査登録機関

申請者からの申請に基づき情報セキュリティサービス基準に関する適合性の審査及び登録（以下「審査・登録」という。）を行う機関をいう。

(2) 申請者

審査登録機関に対して，自らが行う情報セキュリティサービスに対する審査・登録を申請する者をいう。

(3) 情報セキュリティサービス基準

経済産業省が定めた情報セキュリティサービス基準をいう。

(4) 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

経済産業省が定めた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をいう。

(5) 情報セキュリティサービス

情報セキュリティ監査サービス，脆弱性診断サービス，ペネトレーションテスト（侵入試験）サービス，デジタルフォレンジックサービス，セキュリティ監視・運用サービス及び機器検証サービスのいずれか又は全てを行うサービス業をいう。

表2.6　基準等の版番号の見直し案

文書名	今回の改訂に伴う版番号変更案
情報セキュリティサービス基準	第４版 → 第4.1版
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３版 → 令和７年３月版
情報セキュリティサービスに関する審査登録機関基準	第２版 → 第2.1版

2. 情報セキュリティサービス審査登録制度の普及促進及び更なる利活用に向けた調査、検討

(3) 情報セキュリティサービス審査登録制度の更なる普及促進の検討

- 国内での制度活用を促進する観点から、利用者の裾野を拡げるためには中小企業や地方機関等が情報セキュリティサービス基準適合サービスリスト掲載のサービス事業者を使う機会を増やすことが肝要との観点から、以下の目標を実現するためのアクション案を検討した。
  - 企業経営者における認知度の向上
  - 調達担当者、セキュリティ担当者における認知度の向上
  - 中小企業向けに情報システムやサービスを提供するシステムインテグレーター（SIer）のプロジェクトリーダー等における認知度の向上
- 普及方策を検討する上での参考として、情報セキュリティサービスを利用する企業等を会員とする２団体との意見交換を実施し、会員企業における情報セキュリティサービスの選定や利用に関する実態について調査を行った。
- 有識者会議において、審査登録制度の普及に向けて、覚えやすい通称名を設けてはどうかとの提案があり、本事業においては通称名の決定には至らなかったが、継続して検討することとなった。

2. 情報セキュリティサービス審査登録制度の普及促進及び更なる利活用に向けた調査、検討

(4) 本制度の対象を拡張するための調査

- 今後、審査登録対象サービスの追加候補となり得る情報セキュリティサービスとして、以下の7サービスを対象に審査対象とする場合の検討課題等について整理した。
  - マネージドSOCサービス
  - インシデント対応支援サービス
  - CSIRT・PSIRTサービス
  - セキュアインテグレーションサービス
  - セキュアコンサルティングサービス
  - セキュリティアセスメントサービス
  - セキュリティ人材育成支援サービス

3. 情報セキュリティ監査制度の更なる利活用に向けた検討

(1) 情報セキュリティ監査に関する検討会の開催

- 本事業に関係する民間企業、業界団体、関係機関、学識者等11名の有識者からなる検討会を設置し、次の検討内容について次表の要領にて事業期間中３回の会合を開催した。
  - 情報セキュリティ監査制度関連基準等の改訂に関する検討
  - 情報セキュリティ監査制度の更なる活用に関する検討
  - その他
- このほか、情報セキュリティ管理基準及び個別管理基準（監査項目）策定ガイドラインの改訂に関して専門的な観点からの審議を行うことを目的として専門検討会を事業期間中４回開催し、審議結果を有識者会議の第2回会合にて報告した。

表3.2　有識者会議の開催状況

会議	開催日	おもな議題
第1回	2024年9月20日	●情報セキュリティ監査制度に関連する調査結果の報告 ●今年度に議論すべき論点の確認 ●改訂方針に関する審議
第2回	2025年1月20日	●パブリックコメント案について ●今後のスケジュールについて
第3回	2025年3月17日	●パブリックコメント結果と対応について ●情報セキュリティ監査制度の活用方策について

3. 情報セキュリティ監査制度の更なる利活用に向けた検討

(2) 改訂案の作成、編集作業

① 改訂対象文書

- 情報セキュリティ監査制度で用いられる基準等文書の一覧を下図左側に示す。本事業の開始時点において、情報セキュリティ管理基準（2015年改訂）を除き、2003年の制度策定時の基準等が維持されていた。

図3.1　情報セキュリティ監査制度で用いられる基準等と策定時期

3. 情報セキュリティ監査制度の更なる利活用に向けた検討

(2) 改訂案の作成、編集作業

② 改訂の考え方

- 本事業の開始に先立ち、令和５年度中に経済産業省において整理されていた情報セキュリティ監査制度関連基準等の改訂の考え方は次の通りであり、本事業ではこの考え方に基づいて検討を行った。

表3.4　情報セキュリティ監査制度関連基準等の改訂の考え方（令和５年度中の整理）

○　情報セキュリティ監査基準、管理基準については、情報セキュリティマネジメントに関する国際規格であるISO27001、27002を参照として前回（平成28年）改訂がされたところ、令和４年度、令和５年度においてISO27001、27002の改訂及びJISQ27001、27002の改訂が実施されている。

○　当該改訂を踏まえ、情報セキュリティ監査基準、管理基準の改訂を行う。具体的には、今回の国際規格改定は管理策の追加が主であるため、ISO27002の改定を踏まえた管理策の追加が想定される。

○　情報セキュリティ監査基準、管理基準の下位文書（実施基準ガイドライン、報告基準ガイドライン及び個別管理基準（監査項目）策定ガイドライン。）についての整理が必要。

○　情報セキュリティ管理基準の管理基準策などはISMAP等でも引用されているところ、ISMAPについても改訂が検討されていることからISMAPとの連携も必要。

○　また、検討事項として、情報セキュリティ監査基準、管理基準の更なる活用策について検討する。

3. 情報セキュリティ監査制度の更なる利活用に向けた検討

(2) 改訂案の作成、編集作業

③ 監査人アンケート調査の実施

- 情報セキュリティ監査制度関連基準等の改訂にあたって、監査実務に携わる方からの意見・要望を把握することを目的として、事業期間中２回にわたり下表のアンケート調査を実施し、回答結果を改訂案に反映した。

表3.5　監査人アンケート調査の実施概要

	アンケート調査（第１回）	アンケート調査（第２回）
調査目的	情報セキュリティ監査制度関連基準等の改訂にあたって、監査実務に携わる方からの意見・要望の把握	情報セキュリティ監査制度関連基準等のパブリックコメント案に関する事前意見把握
調査対象	情報セキュリティ監査制度に関連する資格保有者（1,999名）	
実施時期	2024年9月2日～17日	2024年12月26日～2025年1月10日
回答数	111件	4件
質問事項	● 現行の情報セキュリティ監査基準等において見直しや追加が必要と感じる事項 ● 情報セキュリティ監査の活用・普及における課題 ほか	以下２文書のパブコメ案についてのご意見 ● 情報セキュリティ管理基準 ● 情報セキュリティ管理基準活用ガイドライン

3. 情報セキュリティ監査制度の更なる利活用に向けた検討

(2) 改訂案の作成、編集作業

④ 改訂案の作成

- 有識者会議第1回会合及び専門検討会における審議内容及びアンケート調査等の内容を踏まえ、本事業において実施した改訂のポイントを下表に示す。

表3.6 各文書における改訂案のポイント

改訂対象文書名	改訂案のポイント
情報セキュリティ監査基準	● これまで「保証」及び「助言」と記載していた箇所について、それぞれ「アシュアランス」及び「アドバイザリー」と表記を変更。（表3.7参照） ● リスクベース監査を行うべきことを明記。
情報セキュリティ監査基準実施基準ガイドライン	● 監査目標設定に関する説明を、リスクベース監査を前提としたものに変更。（図3.2参照） ● アシュアランス型監査についての説明のうち、外部監査の場合について言明型監査に基づく形に変更し、「社会的合意方式」と「利用者合意方式」に関する考慮事項を追加。（表3.8参照）
情報セキュリティ監査基準報告基準ガイドライン	● アシュアランス報告書の雛形として、「社会的合意方式」及び「利用者合意方式」の言明型監査に基づく報告書（各２種類、計４例）に関するものに置換。（表3.9参照） ● 前項の置換を踏まえ、内部監査におけるアシュアランス報告書の活用について追記。
情報セキュリティ管理基準	● JIS Q 27001/27002の改訂内容を反映。（表3.10、表3.11、図3.3参照） ● 従来のマネジメント基準、管理策基準に加え、ガバナンス基準を追加。（表3.12参照）
個別管理基準（監査項目）策定ガイドライン	● 名称を変更：「個別管理基準（監査項目）策定ガイドライン」→「情報セキュリティ管理基準活用ガイドライン」 ● 情報セキュリティ管理基準における属性の追加を踏まえ、その活用方法に関する説明を追加。

表3.7 「アシュアランス」と「アドバイザリー」の定義

保証 ⇒	**アシュアランス**	評価に対して証拠等の客観的な検証を根拠とした事実認定に基づき信頼性についての意見表明をすること。
助言 ⇒	**アドバイザリー**	評価に対して証拠等の客観的な検証を根拠とした基準不適合の事項に対する改善のための助言を行うこと。

現行の基準と意味を変えず、「情報セキュリティ監査の目的」にて上表のように定義を明確化した。

会計監査

- 長年の蓄積をもとに、監査リスクの大きさを（売上額等を基準として）定量的に評価することが可能。
- 監査におけるリスクアプローチではこのような評価結果から最適な監査手続を設計できる。

情報セキュリティ監査

- 対象とするリスクの大小比較が可能な場合はあっても、その数量的な把握や比較が困難な場合が多い。
- リスクに関する定量的なモデル等をもとに、最適な監査手続を設計することが難しい。
- 情報セキュリティ監査におけるリスクベース監査の考え方：
  - **アドバイザリー型監査：**被監査主体のリスクの特徴に基づき、重大と判断されるリスクに対応した管理策の有効性評価に監査資源を集中することで、限られた期間と資源でより的確な監査結果が得られるような、リスクベース監査を実施することが可能。
  - **アシュアランス型監査：**アドバイザリー型と同様のアプローチを取ろうとすると、被監査主体が実施したリスク評価及びそれに基づく管理策の選定のプロセスについて、外部の監査人が有効であるとの意見を述べるには、相当の監査資源を投入する必要が生じるため、現実的ではない。むしろ、比較的リスクが大きいと被監査主体と合意できる範囲を監査対象として限定し、管理策の有効性について意見表明を行うことが望ましい。
- このほか、適切な監査を実施するには、監査計画立案段階において、被監査主体によるリスクアセスメントの実施状況を評価することが望ましい。

情報セキュリティ監査において、そのリスクを考慮した効果的な監査ができるかどうかは、監査の種類や被監査主体における対応状況などに依存するため、情報セキュリティ監査基準実施基準ガイドラインでその旨を説明。

図3.2 リスクベース監査に関する考え方

表3.8　アシュアランス監査における合意形態

合意形態の種類	定義	ガイドラインにおける説明内容
社会的合意方式	監査人があらかじめ社会的に合意された監査手続を行う	● 監査人は実施する監査手続が社会的に合意されていることを確認し、監査目標を設定 ● 監査報告書は一般に公開
利用者合意方式	監査人が監査報告書利用者と明示的に、あるいは暗黙に監査手続について合意する	● 監査報告書のリスクを監査人と報告書利用者が共有 ● 監査報告書の配付・閲覧をリスクを理解している者に制限
被監査主体合意方式	監査人と被監査主体が合意した監査手続について、監査報告書の利用者が確認する	（利用されていないため記載せず）

情報セキュリティ監査基準実施基準ガイドラインでは、アシュアランス型監査における３種類の合意形態のうち、現在用いられている２種類における目標設定の考え方を説明。

表3.9　アシュアランス報告書の雛形における様式の種類

様式１	情報セキュリティ監査のための意見表明方式として、訴訟等で用いられる鑑定意見書等の様式を参考に作成
様式２	これまでの会計監査等で用いられてきた保証業務等の意見表明方式との整合性を考慮した様式

被監査主体の要望を踏まえて選択可能な２種類の様式毎に雛形を提示。

表3.10 JIS Q 27001/27002の主な改訂内容

	分類	おもな改訂内容
JIS Q 27001	（全体）	● マネジメントシステムの共通テキストへの整合 ● 附属書Aの内容をISO/IEC 27002:2022の管理策に合わせて差し替え
JIS Q 27002	管理策の追加	● 以下の内容に関する管理策を追加（カッコ内はJIS Q 27002:2024における項番）： ➢ 脅威インテリジェンス（5.7） ➢ クラウドサービスの利用における情報セキュリティ（5.23） ➢ 事業継続のためのICTの備え（5.30） ➢ 物理的セキュリティの監視（7.4） ➢ 構成管理（8.9） ➢ 情報の削除（8.10） ➢ データマスキング（8.11） ➢ データ漏えい防止（8.12） ➢ 監視活動（8.16） ➢ ウェブフィルタリング（8.23） ➢ セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則（8.27）　←ゼロトラストの概念の追加等 ➢ セキュリティに配慮したコーディング（8.28）
	管理策の再構成	● 管理策を４分類93項目に再構成
	手引きの充実	● 管理策毎の記載内容強化、表現の改善、小見出しの設置等
	その他様式等の変更	● 箇条構成を変更（１階層減） ● 管理策群の分類手段として、属性及び属性値を記載した属性表を導入

表3.11　情報セキュリティ管理基準の管理策基準における新たな構造化

大分類	小分類	説明	管理策数
5. 組織的管理策	**a 情報セキュリティのための経営陣の方向性**	情報セキュリティのための方針、役割、責任、連絡及びインテリジェンス等に関する管理策	8
	b 資産管理	情報及びその他の関連資産についての目録、利用、分類、転送等に関する管理策	6
	c アクセス権管理	アクセス権及び識別情報の管理、アクセス制御並びに認証等に関する管理策	4
	d 供給者管理	クラウドサービス利用を含む供給者との関係における情報セキュリティに関する管理策	5
	e インシデント管理	情報セキュリティインシデントへの対応及び管理に関する管理策	5
	f 事業継続における情報セキュリティ管理	事業継続管理及び事業中断・阻害時の情報セキュリティに関する管理策	2
	g コンプライアンス管理	法規制及び契約等の遵守並びに知財権、プライバシー及びPII保護等に関する管理策	7
6. 人的管理策	**a 人的管理**	要員等の雇用、教育及び遵守すべき事項等に関する管理策	8
7. 物理的管理策	**a 物理的領域の管理**	オフィス、部屋及び施設の物理的セキュリティの確保に関する管理策	7
	b 装置の管理	装置、記憶媒体及び配線等の運用・保守におけるセキュリティの確保に関する管理策	7
8. 技術的管理策	**a 情報アクセスの管理**	利用者等による情報へのアクセスの管理に関する管理策	5
	b 情報資産運用に関する管理	構成管理、脆弱性対応、情報の漏えい防止及びバックアップ等に関する管理策	9
	c 情報システムの適正利用の管理	ログ取得、監視、ソフトウェア利用、ネットワーク構成及び暗号利用等に関する管理策	10
	d 情報システム開発/導入の管理	ソフトウェア開発のライフサイクルを通じたセキュリティの確保に関する管理策	10

JIS Q 27002:2024で大分類数が減ったことを踏まえ、下表で定める小分類を設定し、管理策番号にて識別可能とする。

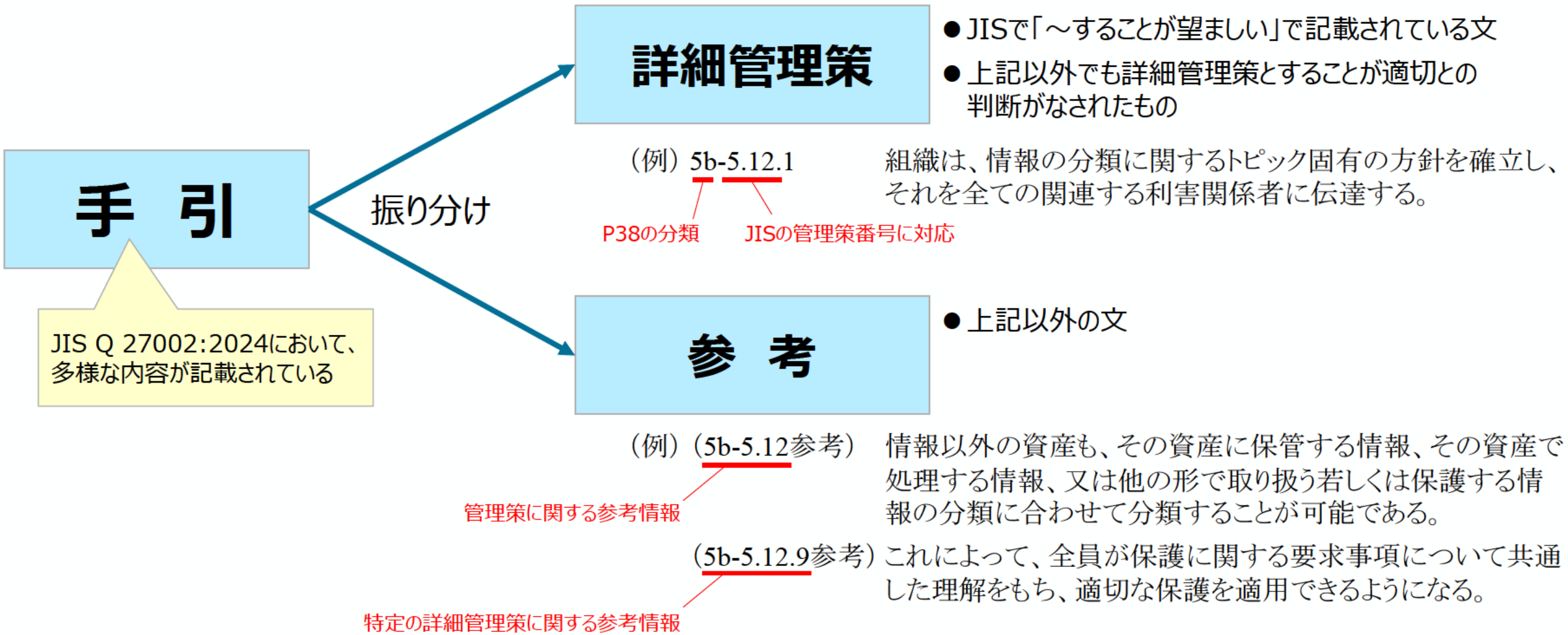

図3.3　情報セキュリティ管理基準の管理策基準における詳細管理策と参考情報の振り分けと採番体系

表3.12　情報セキュリティ管理基準におけるガバナンス基準の構成

項目	おもな内容
3.1 **情報セキュリティガバナンスの概要**	情報セキュリティに関するガバナンスモデルの策定にあたって考慮すべき事項について説明。
3.2 **情報セキュリティガバナンスの目的**	組織体における情報セキュリティガバナンスの目的として以下を提示： 目的１：組織体全体の統合された包括的情報セキュリティを確立する 目的２：リスクに基づく取組を採用して意思決定を行う 目的３：投資の方向性を設定する 目的４：内部及び外部の要求事項との適合性を確実にする 目的５：セキュリティに積極的な文化を醸成する 目的６：セキュリティのパフォーマンスが現在及び将来の組織体の要求事項を満たすことを確実にする
3.3 **情報セキュリティガバナンスのプロセス**	「評価」、「指示」、「モニタ」及び「コミュニケーション」の各プロセスにおいて、ガバナンス主体及び各情報セキュリティマネジメントシステムの責任者 が実行する内容を提示。

ISO/IEC 27014:2020をもとに、組織体のガバナンスのうち、情報セキュリティガバナンスを確立するための目的及びプロセスに関する管理策を示す。

3. 情報セキュリティ監査制度の更なる利活用に向けた検討

(2) 改訂案の作成、編集作業

⑤ パブリックコメントへの対応

- 2025年2月3日19時～3月5日19時にわたってパブリックコメントを実施し、期間中に48件（複数のコメントを含むものを1件と数えると10件）のコメントが寄せられた。
- それぞれのコメントについて回答案及び基準等文書の修正案を作成し、有識者会議の第3回会合での審議を経て承認された。

⑥ 誤記修正・校正の実施

- 改訂最終案のとりまとめに先立ち、パブリックコメントに寄せられた誤記の指摘への対応を行うとともに、パブリックコメント案について網羅的な校正を行い、発見したの誤記等についての修正を実施した。

3. 情報セキュリティ監査制度の更なる利活用に向けた検討

(3) 情報セキュリティ監査制度の更なる活用策の検討

- 監査制度の更なる活用策の検討にあたり、経済産業省との協議のもと、『サイバーセキュリティ経営ガイドライン』との連携を行うことで有識者会議にて審議を行った。審議にて示された意見をもとに、サイバーセキュリティ経営ガイドラインに基づいてセキュリティ対策の改善に取り組む企業を対象に、情報セキュリティ管理基準（業種別管理基準を含む）を活用する各種の手段を当該企業のセキュリティ成熟度に応じて次のようにステップアップ的に提供することで支援する形の活用案を検討した。
  - 成熟度低：業界団体が策定した個別管理基準を用いて、重要10項目毎に自社の対策実施状況を可視化して改善につなげる
  - 成熟度中：重要10項目のうち、指示4（リスク把握・対応）、指示5（仕組み構築）、指示6（継続的改善）について、内部監査担当の協力のもとリスクベース監査を行うことで改善を実現する
  - 成熟度高：情報セキュリティ管理基準に準拠した個別管理基準に基づく言明書を経営者名で公表し、アシュアランス型の監査を実施することでセキュリティ情報開示に関する信頼性を向上させる

４．まとめ

- 本事業では、デジタル社会全体のレジリエンス向上及び情報セキュリティの確保等を目的として、情報セキュリティサービス審査登録制度及び情報セキュリティ監査制度の２つの制度で用いる基準等の改訂案作成を中心とする各種の取り組みを実施した。
- 情報セキュリティサービス審査登録制度の普及促進及び更なる利活用に向けた調査、検討については、審査登録制度に登録する事業者がそのサービス提供を通じて反社会的勢力への便益供与を行わないことを確実にするための情報セキュリティサービス基準の改訂案の作成を行い、有識者会議による審議を経て確定された。また、審査登録制度の更なる普及に向けた取組として、中小企業等及び地方機関等による活用を促進するためのアクション案についての検討を行った。さらに、審査登録制度の対象を拡張するための検討として、これまでのアンケート調査や経済産業省における検討等をもとに追加の対象となり得るサービスについて、審査対象サービスとする場合に検討すべき事項について整理した。
- 情報セキュリティ監査制度の更なる利活用に向けた検討については、改訂対象となる基準等にこれまで20年以上にわたって改訂がなされていないものも含まれることから、現在の情報セキュリティ監査の実態を踏まえた改訂の方針案を検討するとともに、情報セキュリティ監査に携わる関係者を対象とするアンケート調査結果等も参考として、情報セキュリティ監査基準・情報セキュリティ管理基準及びこれらに関連するガイドラインを対象とする改訂案を作成し、有識者検討会にて審議した結果をもとにパブリックコメント案を作成した。さらに、パブリックコメントで得られた意見をもとに改訂案の見直し及び校正作業を実施し、最終的な改訂案としてとりまとめた。このほか、情報セキュリティ監査制度の更なる活用策の検討として、監査制度とサイバーセキュリティ経営ガイドラインを連携させるにより、企業がサイバーセキュリティ経営ガイドラインをより実践できるようにするための方策について検討した。
- 今後、審査登録制度、監査制度のそれぞれで基準等の改訂が行われることを通じて、社会におけるサイバーセキュリティに関するリスクの実態により即した制度運用が可能となり、情報セキュリティ監査を含む情報セキュリティサービスの利用又は内部監査の実践等を通じて冒頭に示した本事業の目的が達成に向けて進展していくことが期待される。