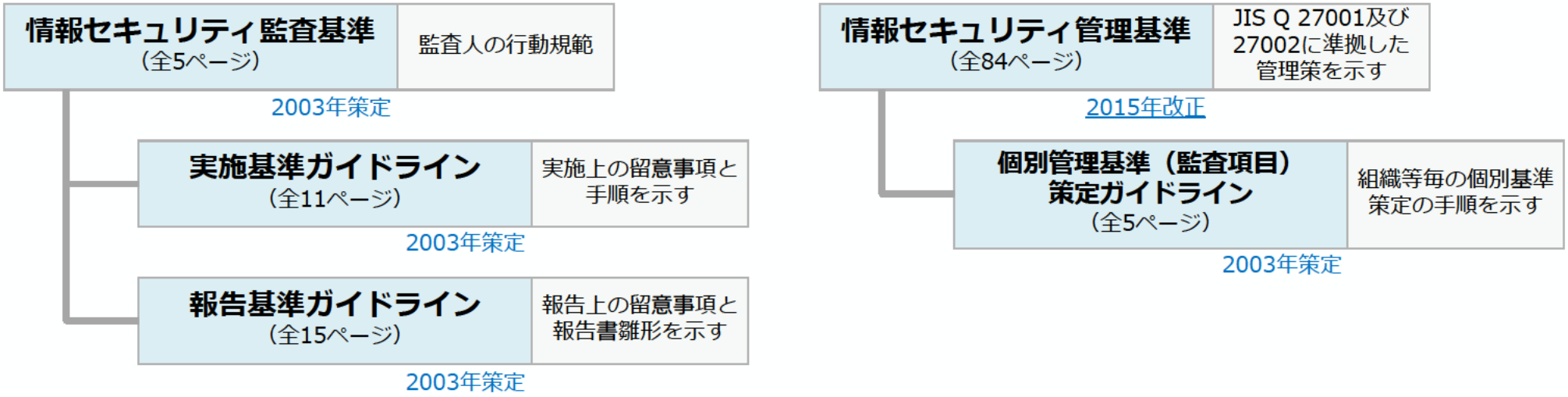
情報セキュリティ監査基準等
改正の概要

情報セキュリティ監査基準等改正の背景

- 2022年に情報セキュリティマネジメントに関する国際規格ISO/IEC 27001及び27002が改訂され、対応するJIS規格（JIS Q 27001及び27002）も2023年～2024年に改訂された。
- 情報セキュリティ監査制度で用いられる基準等文書のうち、上記規格に準拠している情報セキュリティ管理基準を除く各文書は2003年の制度創設以来改正されておらず、現在の監査実務におけるリスクベース監査の普及等の動向が反映されていない。

情報セキュリティ監査制度で用いられる基準等文書の構成と策定及び改正時期



改正にあたり設置した有識者検討会の概要

情報セキュリティ監査制度関連基準等改訂に関する検討会

- 情報セキュリティ監査基準等の改正等に関する検討を行うことを目的とした有識者検討会を設置し、下表のとおり３回の会合を開催した。

会議	開催日	主な議題
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 ●議論すべき論点の確認 ●改正方針に関する審議
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

検討会委員

- 情報セキュリティ監査制度関連基準等改訂に関する検討会の委員は下表のとおり。

	氏名（敬称略）	所　属
委員長	手塚 悟	慶應義塾大学 グローバルリサーチインスティテュート 特任教授
委員	大木 榮二郎	工学院大学 名誉教授
	加藤 俊直	PwC Japan有限責任監査法人 パートナー
	神田 雅透	独立行政法人情報処理推進機構（IPA） セキュリティセンター 技術評価部長
	島田 裕次	東洋大学 工業技術研究所 客員研究員 / システム監査学会 会長
	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
	寺尾 淳子	ISACA大阪支部 理事
	中尾 康二	国立研究開発法人情報通信研究機構（NICT） サイバーセキュリティ研究所 主管研究員
	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
	堀江 正之	日本大学商学部会計学科 特任教授
	間形 文彦	NTTコミュニケーションズ株式会社 情報セキュリティ部

専門検討会の開催

- 主に情報セキュリティ管理基準の改正及び個別管理基準（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、検討会とは別に、専門検討会を４回開催し、検討結果を第２回検討会にて報告。

検討会	開催日時	主な議題
第１回専門検討会	2024年10月15日	●キックオフ ●情報セキュリティ管理基準の改正方針に関する審議 ●個別管理基準（監査項目）策定ガイドラインの改訂方針に関する審議
臨時専門検討会	2024年11月5日	●第1回専門検討会の継続審議 ・管理策の分類について ・管理策／詳細管理策の構造化について ・「情報セキュリティ管理基準活用ガイドライン」の内容について
第２回専門検討会	2024年11月28日	●情報セキュリティ管理基準改正案への事前ご意見の審議 ●情報セキュリティ管理基準活用ガイドライン案への事前ご意見の審議 ●残検討項目に対する審議
第３回専門検討会	2024年12月13日	●情報セキュリティ管理基準改正案の事前指摘の審議

改正の概要

改訂の対象文書と主な改正の概要

- 改訂の対象文書及び改訂のポイントは下表のとおり。

改訂対象文書名	改訂のポイント
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。 ● 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。 ● アシュアランス型監査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。
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ひな形を、「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）に変更。 ● 上記の変更を踏まえ、ひな形に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。 ● 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。
個別管理基準（監査項目）策定ガイドライン	● 名称を「情報セキュリティ管理基準活用ガイドライン」に変更 ● 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。

情報セキュリティ監査基準の改正

- 情報セキュリティ監査基準の改正のポイントは以下のとおり。

- 「監査人の行動規範」としての位置付けを変えず、すべての監査に共通する内容を記載することとした。
  - 前文にて以下２点について追記：
    - 本基準で扱う「情報セキュリティ」には、サイバーセキュリティの文脈で扱われるサイバー空間としてのITインフラストラクチャー及び漏えいした場合にプライバシーの侵害となるようなプライバシーに関する情報を含む。（JISの名称が「情報セキュリティ、サイバーセキュリティ及びプライバシー保護」になったことを踏まえる）
    - 監査の目的として示されている「保証の付与」について、「セキュリティインシデントが発生しないことを保証する」という文脈における保証（英語のguaranteeに相当）として誤解される事例があることを踏まえ、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」と表記を改める。
  - 文書内構成は現状維持。
  - 品質管理の観点から以下２点について追加：
    - 監査の目的によっては品質を確保するための専門的能力と実務経験を有する品質管理担当者を設定する。
    - 監査の実効性を高める観点から、被監査主体におけるリスクの特徴を考慮した監査（リスクベース監査）を行わなければならない。
  - 「指導」に関する記載事項は、監査人が行うべきことではないことから削除。

（参考）改正情報セキュリティ監査基準の構成

構成	項番	見出し（赤字は主要改訂項目）	改訂事項
		前文	サイバーセキュリティ及びプライバシー保護も対象である旨を追記するとともに、アシュアランスとアドバイザリーへの変更について説明。
		情報セキュリティ監査の目的	アシュアランスとアドバイザリーを定義。[意見」と「助言」の使い分けを明確化。
一般基準	1.	目的、権限と責任	監査の目的と対象が監査依頼者の要請に応じたものであるべきことを追加。
	2.	独立性、客観性と職業倫理	
	2.1	外観上の独立性	目的に応じた独立性に関して「身分上」を「身分上・経済上」に変更。
	2.2	精神上の独立性	
	2.3	職業倫理と誠実性	
	3.	専門能力	「知識及び技能の保持」を「継続的かつ」「維持・向上」に変更。
	4.	業務上の義務	
	4.1	注意義務	
	4.2	守秘義務	
	5.	品質管理	
	5.1	情報セキュリティ監査の品質管理	品質管理者の設定について追加。
	5.2	被監査主体におけるリスクの特徴の考慮	実効性向上のため、被監査主体におけるリスクの特徴を考慮した監査を行う必要性を示す。
実施基準	1.	監査計画の立案	
	2.	監査の実施	
	2.1	監査証拠の入手と評価	
	2.2	監査調書の作成と保存	
	3.	監査業務の体制	
	4.	他の専門職の利用	
報告基準	1.	監査報告書の提出と開示	
	2.	監査報告の根拠	
	3.	監査報告書の記載事項	
	4.	監査報告についての責任	
	~~5.~~	~~監査報告に基づく改善指導~~	監査人が行うべきことではないことから削除。

（参考）「アシュアランス」と「アドバイザリー」の定義

- 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」にて定義を明確化した。

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。

情報セキュリティ監査基準実施基準ガイドラインの改訂

- 情報セキュリティ監査基準実施基準ガイドラインの改訂のポイントは以下のとおり。

  - 以下のとおり情報セキュリティ監査制度策定後の実践状況を反映した。
    - 「情報セキュリティ管理基準」による監査についての説明内容を、同基準の改正に合わせたものに修正：
      - ガバナンス基準についての説明を追加
      - 詳細管理策の取捨選択の必要性について、より明確化
    - 文中にあった「コントロール」「サブコントロール」の用語を、それぞれ「管理策」「詳細管理策」に統一。
    - 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。
    - リスクアセスメントに関する説明において、３種類の監査リスクについて説明。
      - 固有リスク：統制がない状態における情報セキュリティリスク
      - 統制リスク：組織の統制が効かないことにより生じるリスク
      - 発見リスク：統制の有効性を正しく発見できないことにより生じるリスク
    - アシュアランス型監査の説明のうち、外部監査の場合について言明型監査に基づく形に変更。
    - アシュアランス型監査の目標設定において、「社会的合意方式」と「利用者合意方式」における考慮事項について追加。
    - 成熟度に応じた監査に関する説明について、記載内容が現在求められている内容と異なるため削除。
    - リモート監査、自動収集した情報等の扱いについて追記。

（参考）改訂実施基準ガイドラインの構成

項番	見出し（赤字は主要改訂項目）	改訂事項
Ⅰ.	情報セキュリティ監査実施上の前提事項	
1.	情報セキュリティ監査における準拠規範	● 情報セキュリティ管理基準へのガバナンス基準の追加に対応。 ● 詳細管理策の取捨選択の必要性について、より明確化。 ● 紹介する規格・基準等を最新のものに更新。
2.	情報セキュリティ監査の目的設定	● 外部監査の場合について言明型監査に基づく形に変更。 ● アシュアランスの意味する内容についての説明を詳細化。 ● 監査方法の選定に関する内容を削除。
~~3.~~	~~情報セキュリティ監査における成熟度モデルの利用~~	● 記載内容が現在求められている内容と異なるため削除。
3.	リスクの特徴に基づく監査目標設定の考え方	● 監査種類ごとのリスクの適切な取扱いについての説明を追加。
Ⅱ.	情報セキュリティ監査の実施手順	
1.	監査実施のフレームワーク	● フレームワークの説明図において古くなった内容を更新。
2.	監査計画の立案	● ３種類の監査リスクについて説明。
3.	監査手続の実施（監査証拠の入手と評価）	● リモート監査、自動収集した情報等の扱いについて追記。
4.	監査調書の作成と保存	● 監査調書に関する監査人の責任についての表現を見直し。
5.	適切な監査業務の体制整備	● 監査リスクに応じた体制整備について追記。
6.	監査の品質管理システム	● 監査の品質管理に関する考慮事項として追加。

情報セキュリティ監査基準報告基準ガイドラインの改訂

- 情報セキュリティ監査基準報告基準ガイドラインの改訂のポイントは以下のとおり。

- 以下のように情報セキュリティ監査制度策定後の実践状況を反映した。
  - 「アシュアランス型」「アドバイザリー型」の名称変更への対応。
  - アシュアランス報告書のひな形として、「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）に関するものに変更（下表参照）。
  - また、上記変更を踏まえ、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。
  - アドバイザリー報告書に関して「厳密性は必要とされない」という表現の削除。
  - アシュアランス報告書に関する注釈として、日本公認会計士協会による実務指針及びSOC2/SOC3の規定内容を考慮すべき旨を追記。

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した様式
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

（参考）改訂報告基準ガイドラインの構成

項番	見出し（赤字は主要改訂項目）	改訂事項案
Ⅰ.	監査報告書の意味と記載事項	
1.	監査報告書の定義	
2.	監査報告書の記載事項	
3.	監査報告書の種別	
Ⅱ.	アドバイザリー報告書作成上の留意事項	
1.	アドバイザリーの表明方法	
2.	助言記載上の留意事項	実施基準ガイドラインと同様、成熟度モデルに関する記載を削除。
Ⅲ.	アドバイザリー報告書の雛形	
1.	助言を記載する場合の雛型	厳密性は必要とされない旨の表現を削除。
Ⅳ.	アシュアランス報告書作成上の留意事項	
1.	アシュアランス意見の表明方法	言明方式に基づく記述に変更。
2.	アシュアランス意見の類別	言明方式に基づく記述に変更。
3.	アシュアランス意見記載上の留意事項	実施基準ガイドラインと同様、成熟度モデルに関する記載を削除。
4.	内部監査におけるアシュアランス報告書	雛形を言明方式に変更にしたことを踏まえて追加。
V.	アシュアランス報告書の雛型	
1.	社会的合意方式のアシュアランス型情報セキュリティ監査報告書【様式１】の雛型	現行版公表以降のアシュアランス型監査に関する検討結果を反映。
2.	社会的合意方式のアシュアランス型情報セキュリティ監査報告書【様式２】の雛型	現行版公表以降のアシュアランス型監査に関する検討結果を反映。
3.	利用者合意方式のアシュアランス型情報セキュリティ監査報告書【様式１】の雛型	現行版公表以降のアシュアランス型監査に関する検討結果を反映。
4.	利用者合意方式のアシュアランス型情報セキュリティ監査報告書【様式２】の雛型	現行版公表以降のアシュアランス型監査に関する検討結果を反映。

情報セキュリティ管理基準の改正

- 情報セキュリティ管理基準の改正のポイントは以下のとおり。

- JIS Q 27002:2024における大規模な構成変更を踏まえ、管理策基準を大幅に改訂した。
  - JIS Q 27001/27002の改訂内容を反映：
    - マネジメント基準：JIS Q 27001:2023における改訂内容をもとに変更差分を更新。
    - 管理策基準：管理策の番号体系及び詳細管理策の選定方針を含めて大幅な改訂を実施。
    - JIS Q 27002:2024で追加された管理策の属性情報を追加。
  - 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。
  - 情報セキュリティ管理基準をそのまま使うのではなく、監査で用いる基準として十分と判断される程度に具体化させた管理策を個別管理基準としてとりまとめるべき旨の説明を追加。
  - 利用者の便宜向上の観点から、目次と用語集を追加。

（参考）改正情報セキュリティ管理基準の構成

平成28年改正版		令和7年改正版		
Ⅰ．主旨	情報セキュリティ管理基準の策定意図と改訂経緯について説明。	Ⅰ．概要	1.1 主旨	情報セキュリティ管理基準の策定意図と改訂経緯について説明。
Ⅱ．本管理基準の位置づけ	組織体の情報セキュリティマネジメントの確立における本基準の位置づけについて説明。		1.2 本管理基準の位置づけ	そのまま使うのではなく、監査で用いる基準として十分と判断される程度に具体化させた管理策を個別管理基準としてとりまとめるべき旨の説明を追加。
Ⅲ．構成	本基準の項目の構成根拠及び実施要否等について説明。	Ⅱ．構成		本基準の項目における構造化及びその根拠、並びに実施要否等について説明。
		Ⅲ．ガバナンス基準		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ついて示す基準として、ISO/IEC 27014:2020を参考に作成。
Ⅳ．マネジメント基準	JIS Q 27001:2014準拠	Ⅳ．マネジメント基準		JIS Q 27001:2023準拠 項番の構成を維持しつつ、JIS改訂における差分内容を旧マネジメント基準に反映することで更新。
Ⅴ．管理策基準	JIS Q 27002:2014準拠	Ⅴ．管理策基準		JIS Q 27002:2024準拠 JIS改訂において章構成が大幅に変更になり、管理策毎に目的が追加されたことから、最新のJISの構成及び記載内容をもとに新たな様式にて作成。
－	－	用語集		JIS Q 27002:2024及びJIS Q 27000:2019等をもとに新規作成。

（参考）ガバナンス基準の構成

- 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している。

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。

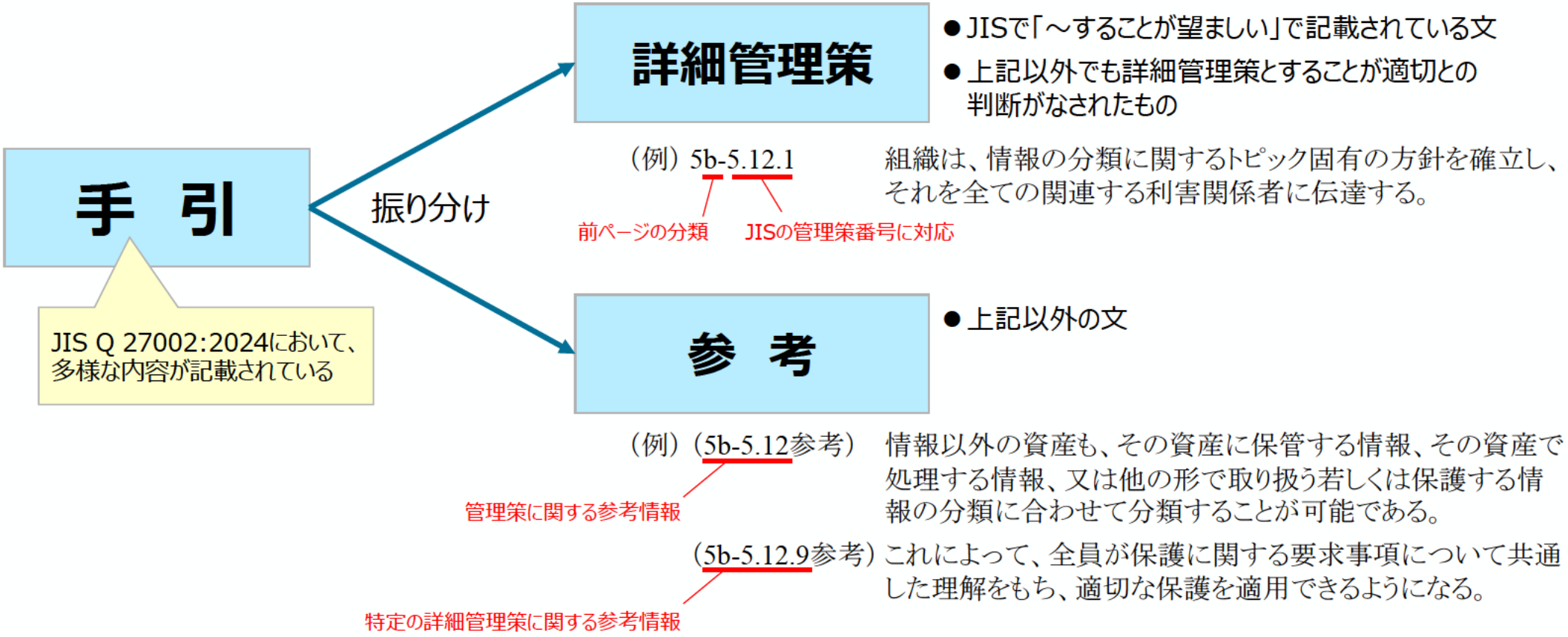
（参考）管理策基準における新たな構造化

- 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した。

大分類	小分類	説明	管理策数
5. 組織的管理策	**a 組織的管理**	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	6
	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	13
	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	5
	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

（参考）詳細管理策と参考情報の振り分けと採番体系

- 詳細管理策とすべきでない手引は「参考」としてカッコ付きで記載
- 振り分けに関する判断はISMSの専門家によるレビュー及び合議をもとに実施



情報セキュリティ管理基準活用ガイドラインの策定

- 情報セキュリティ管理基準活用ガイドラインの策定のポイントは以下のとおり。

- 個別管理基準（監査項目）策定ガイドラインが認知・活用されていないとの指摘を踏まえ、構成及び内容を大幅に見直した。
  - 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」
  - 個別管理基準等の策定の必要性の認知度が低いことを踏まえ、「はじめに」において情報セキュリティ管理基準をもとに個別管理基準等を策定する必要性について説明。
  - 情報セキュリティ監査基準でリスクベース監査を扱っていることと整合をとるため、「はじめに」において個別管理基準をリスクベースで活用する方法について説明。
  - 個別管理基準の策定手順について、マネジメント基準との関係等、現行ガイドライン策定時からの変化を反映。
  - ガバナンスの評価に関する内容を追加。
  - 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。

（参考）情報セキュリティ管理基準活用ガイドラインの構成

項番		旧ガイドラインからの変更内容	変更理由
Ⅰ．はじめに	**1．本ガイドラインの位置付け**	本ガイドラインの位置付けについて説明。想定読者についての説明を追加し、サンプルへの言及を削除。	サンプルの内容が古くなったため。
	2．個別管理基準と業種・業態別管理基準	情報セキュリティ管理基準をもとに個別管理基準等を策定する必要性について説明。	（新規）
	3．個別管理基準をリスクベースで活用するには	リスクベースの考え方について説明。	（新規）
Ⅱ．個別管理基準の策定手順	**（前書き）**	個別管理基準策定に関する全体の流れについて説明。情報資産という表現を見直すとともに項目の変更に伴い図を修正。	各項番における変更の反映のため。
	1．情報セキュリティ管理基準の参照・項目の抽出	必要項目の抽出と表現の修正方法について説明。当該業種・業態向けに提供されているセキュリティ管理基準やガイドライン等の参照に関する記述を追加。	業種・業態向けの基準やガイドライン等の活用促進のため。
	2．関連法規制及び考慮すべき事項の明確化	考慮すべき法令を記述することの効果について説明。一部表現を修正。	実施順の見直し及びわかりやすさの改善のため。
	3．他の規定の参照	情報セキュリティ管理基準の対象とならない管理策の検討方法について説明。最新の基準等を参照するように内容を更新。	考慮すべき規定等における前回策定時点からの変化の反映のため。
	4．当該組織体に必要とされる項目の追加	追加すべき項目の選定方法と表現について説明。一部表現を修正。	実施順の見直し及びわかりやすさの改善のため。
	5．組織内規定との整合性を図る	既存の組織内規定との整合の確保について説明。一部表現を修正。	実施順の見直し及びわかりやすさの改善のため。
	6．管理策の選定	リスク管理目標への影響度に応じて必須・推奨を区分する方法について説明。	リスクベースアプローチへの対応のため。
	7．技術的検証項目の策定	外部の専門家への委託による実施等の対応が必要な項目の識別について説明。	技術的な検証を行う項目の増加を踏まえて位置付けを見直したため。
Ⅲ．管理基準のさらなる活用	**1．ガバナンスの評価（有効性評価）の考え方**	ガバナンスに関する管理策の有効性評価の方法について説明。	（新規）
	2．管理策に関する属性情報の活用	JIS Q 27002:2024にて新たに追加された属性情報の活用案と活用例について説明。	（新規）