【参考】ISMAP管理基準の改定について（案）

令和７年９月18日（木）
国家サイバー統括室、デジタル庁、総務省、経済産業省

ISMAP管理基準改定のポイント

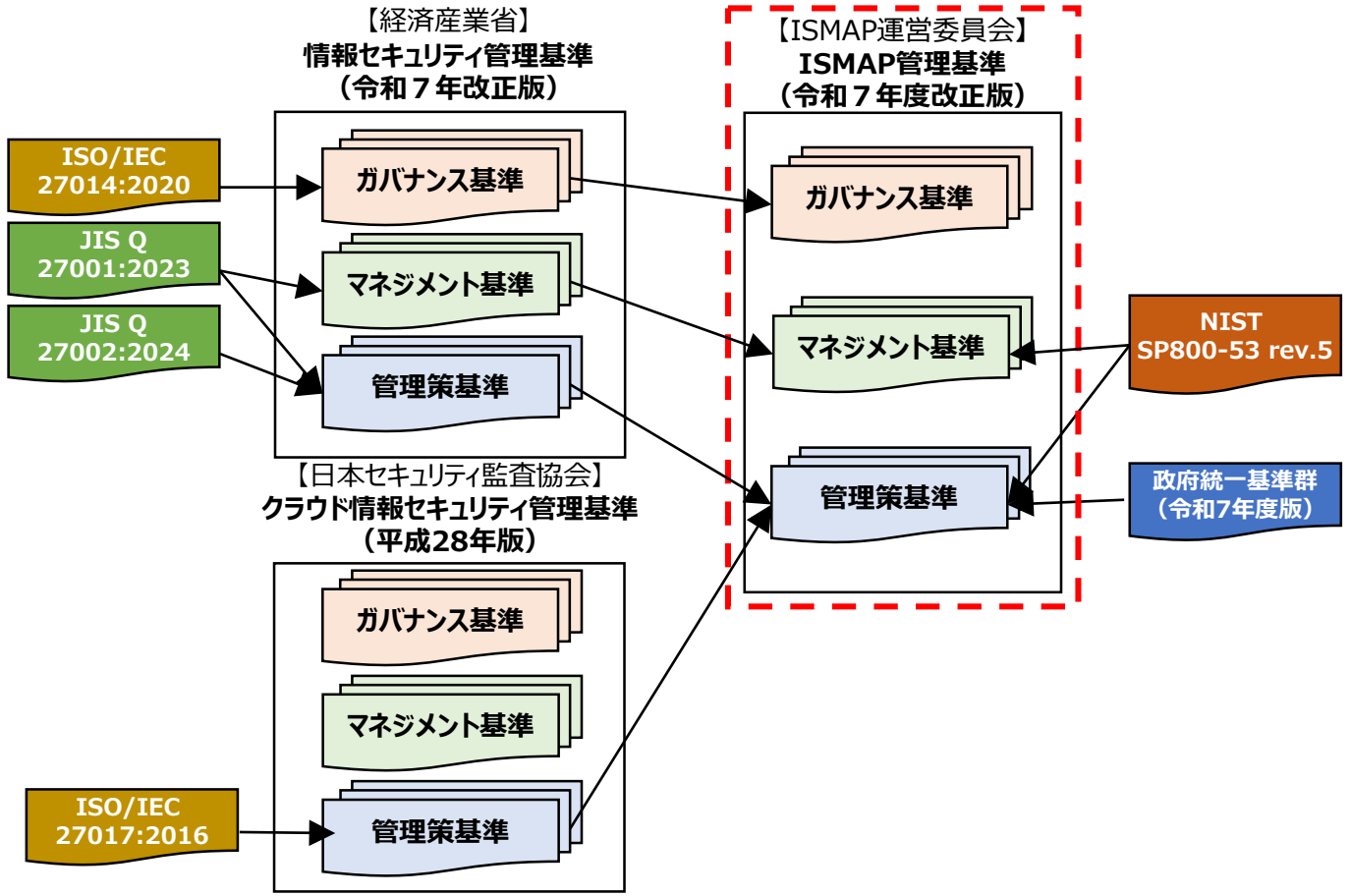
- 国際規格等の最新動向の反映、及びクラウドサービス事業者にとっての課題への対応を行うために、ISMAP管理基準を改定する。
- また、クラウドサービス事業者がISMAP管理基準に基づき実効性のある統制構築を行うために必要な「ガイドライン（仮）」の策定等を検討している。

		方針の具体化	
ISMAP管理基準※1	• ISO/IEC 27002等の国際規格の改定内容の取り込み • 情報セキュリティ管理基準の改定との連携		〔改定のポイント① 最新の国際規格等の取り込み〕 • 国際規格の改定が反映された情報セキュリティ管理基準（令和７年改正版）におけるガバナンス基準、マネジメント基準、管理策基準の内容の取り込み
	• 統制目標と詳細管理策の位置付けの明確化 • 管理策数を数百まで削減		〔改定のポイント② 詳細管理策の粒度の変更及び手引きの新設〕 • 詳細管理策は統制目標を実現するために満たすべき必要最小限の内容の記述に絞り、詳細管理策を具体的に実施するための参考情報は手引きに記述 • 詳細管理策の数を1,163項目から322項目に削減 〔改定のポイント③ 基本言明要件の定義の見直し〕 • 詳細管理策の記載粒度の変更(抽象化)に伴い、全ての詳細管理策については原則として実施すべきものと定義
その他の規程※2	• 実効性のある統制構築の促進		〔ガイドラインの策定、事前確認の枠組みの導入〕 • 統制目標及び詳細管理策を対象外とできる理由の考え方、詳細管理策の実施に当たって手引きから選択等する場合の考え方等を定めた「ガイドライン」を規程として、策定・公表することを検討 • 対象外とした統制目標及び詳細管理策、手引きから選択等した管理策の妥当性について制度（審査）の確認を受けることができる枠組みの検討

※1）ISMAP管理基準改定案をパブリック・コメントによる意見募集対象とし、今後開催予定のISMAP運営委員会での決定後、公表を予定。
※2）その他の規程（ISMAPクラウドサービス登録規則、標準監査手続等）やガイドラインは鋭意作成中であり、公開・改定スケジュール含め検討中。

ポイント① 最新の国際規格の取り込み

- ISO/IEC 27000シリーズの改定が反映された**「情報セキュリティ管理基準（令和７年度版）」より、ガバナンス基準、マネジメント基準、管理策基準を取り込む形で改定。**
- 「クラウド情報セキュリティ管理基準（平成28年版）」よりクラウドサービス固有の管理策を追加し、「政府統一基準群」及び「NIST SP800-53 rev.5」より必要な管理策を追加。



ポイント② 詳細管理策の粒度の変更及び手引きの新設

- 管理策基準における**詳細管理策は統制目標を実現するために満たすべき必要最小限の内容の記述に絞り、詳細管理策を具体的に実施するための参考情報は手引きに記述。**
- 詳細管理策の数を1,163項目から322項目に削減。

〔現行ISMAP管理基準〕

統制目標 / 詳細管理策

番号	管理策基準	定型管理策種別
6.1.4	情報セキュリティに関する研究会又は会議、及び情報セキュリティの専門家による協会・団体との適切な連絡体制を維持する。	
6.1.4.1	最適な慣行に関する認識を改善し、関係するセキュリティ情報を最新に保つ手段として、情報セキュリティに関する研究会又は会議へ参加する。	定型管理策１
6.1.4.2	情報セキュリティ環境の理解が最新かつ完全であることを確実にする手段として、情報セキュリティに関する研究会又は会議へ参加する。	定型管理策１
6.1.4.3	攻撃及びぜい弱性に関連する早期警戒警報、勧告及びパッチを受理する手段として、情報セキュリティに関する研究会又は会議へ参加する。	定型管理策１
6.1.4.4	専門家から情報セキュリティの助言を得る手段として、情報セキュリティに関する研究会又は会議へ参加する。	定型管理策１
6.1.4.5	新しい技術、製品、脅威又はぜい弱性に関する情報を共用し、交換する手段として、情報セキュリティに関する研究会又は会議へ参加する。	定型管理策１
6.1.4.6	情報セキュリティインシデントを扱う場合の、適切な連絡窓口を提供する手段として、情報セキュリティに関する研究会又は会議へ参加する。	定型管理策１

〔ISMAP管理基準改定案〕

統制目標

番号	統制目標	番号	詳細管理策	(参考)定型管理策	(参考)手引き
5.6	専門組織との連絡 統制目標：組織は、情報セキュリティに関する研究会又は会議、及び情報セキュリティの専門家による協会・団体との連絡体制を確立し、維持する。 目的：情報セキュリティに関して適切な情報流通が行われることを確実にするため。				
		5.6.1	情報セキュリティに関して、適切な情報の流通が行われることを確実にするために、専門組織との連絡体制を確立し、維持する。	定型管理策１	次の事項を達成する手段として、専門組織（情報セキュリティに関する研究会又は会議及び情報セキュリティの専門家による協会・団体）との連絡体制を確立し、維持する。 a) 最適な慣行に関する知識を改善し、関係するセキュリティ情報に追随する。 b) 情報セキュリティ環境の理解が最新であることを確実にする。 c) 攻撃及びぜい弱性に関する早期警戒警報、勧告及びパッチを受理する。 d) 専門家から情報セキュリティの助言を得る。 e) 新しい技術、製品、サービス、脅威又はぜい弱性に関する情報を共有し、交換する。 f) 情報セキュリティインシデントを扱う場合の、適切な連絡窓口を提供する（5.24～5.28参照）。

詳細管理策

・クラウドサービス事業者は詳細管理策毎に個別管理策を策定
・手引きは詳細管理策を実施するための例示であり参考情報
・個別管理策の策定における、手引きからの選択または独自の統制構築における考え方や例示をガイドラインにて解説予定
・なお、監査においては手引きを参考に監査を実施

ポイント③ 基本言明要件の定義の見直し

- **詳細管理策は統制目標を実現するために満たすべき必要最小限の内容の記述に絞ったことにより、詳細管理策の抽象度が上がったことから、すべての詳細管理策については原則として実施すべきものとしている。**そのため、「.B」及び「.PB」の管理策は存在しない。
- 他方、**「リスク分析の結果、実施不要と判断した」場合であっても対象外とすることが出来る点を明確化。**

〔現行ISMAP管理基準〕

2.2.4 基本言明要件

言明の対象となる管理策として、以下の内容を実施しなければならない。なお、言明の対象となるクラウドサービスの基盤に言明の対象外となるサービスを利用している場合において、当該対象外のサービスがISMAP クラウドサービスリストに登録されている場合には、当該対象外のサービスが実施している統制を引き継ぐことで当該統制に係る監査の手続を省略することができる。

（1） ガバナンス基準

原則としてすべて実施しなければならない。

（2） マネジメント基準

原則としてすべて実施しなければならない。

（3） 管理策基準

全ての統制目標としての管理策について、原則として実施しなければならない。また、末尾にBが付された詳細管理策（X.X.X.X.B及びX.X.X.X.PB）も原則として実施すべきものとする。

その他の詳細管理策は、言明の対象となるサービスにおける組織・環境・技術等に応じて必要とする事項を選択する（選択制）。

他方、クラウドサービス事業者は自身の提供するサービスと照らし、合理的な適用が不可能な統制目標としての管理策については、その理由を示すことで対象外とすることができる。この場合、対象外とした統制目標としての管理策に含まれる詳細管理策のうち末尾にBが付された詳細管理策も対象外にすることができる。また、詳細管理策については、前述のとおり選択制であるが、選択しない詳細管理策についてはその理由を記載する。ただし、選択しない理由については監査の対象外である。

選択制の詳細管理策の項目については、別表３を参照すること。また、詳細管理策の選択及びその運用に当たっては、別紙１の内容に留意すること。

〔ISMAP管理基準改定案〕

2.2 基本言明要件

クラウドサービス事業者は、言明の対象となる管理策として、以下の内容を実施し、書面にて言明を行わなければならない。また、特に変更の言明が行われていない限りにおいて、その言明はクラウドサービス事業者が責任を負うものとして有効であると見なされる。なお、言明の対象となるクラウドサービスの基盤に言明の対象外となるサービスを利用している場合において、当該対象外のサービスがISMAPクラウドサービスリストに登録されている場合には、当該対象外のサービスが実施している統制を引き継ぐことで当該統制に係る監査の手続を省略することができる。

⑴ ガバナンス基準

全て実施しなければならない。

⑵ マネジメント基準

全て実施しなければならない。

⑶ 管理策基準

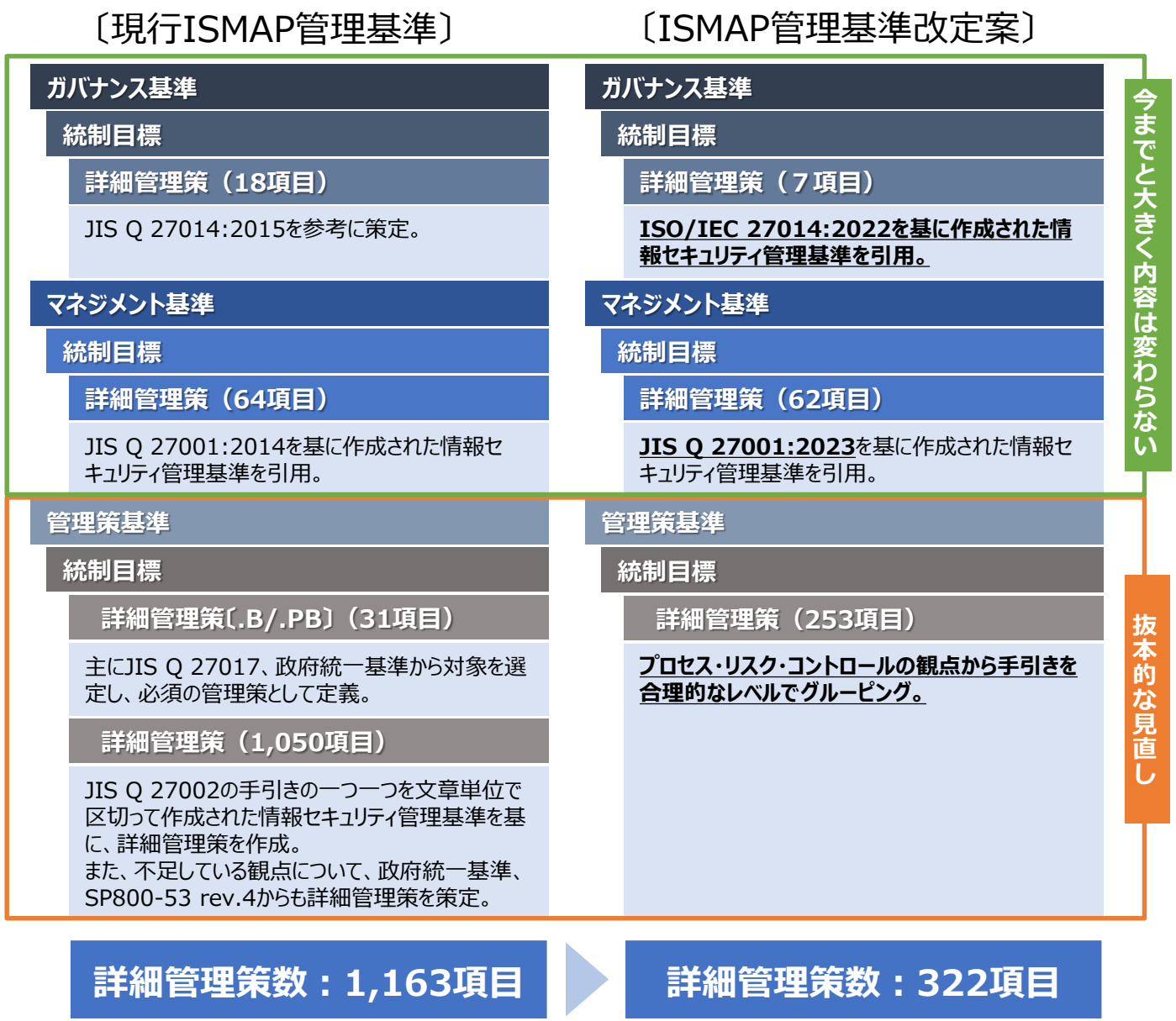
全ての統制目標としての管理策について、原則として実施しなければならない。また、詳細管理策（X.X.X）も原則として実施すべきものとする。

他方、クラウドサービス事業者は自身の提供するサービスと照らし、合理的な適用が不可能、若しくは、リスク分析の結果、実施不要と適切に判断した統制目標としての管理策及び詳細管理策については、その理由を示すことで対象外とすることができる。

・「合理的な適用が不可能、若しくは、リスク分析の結果、実施不要」と判断した場合の考え方や理由記載例について、ガイドラインにて解説予定
・監査・審査前に、クラウドサービス事業者はガイドラインをベースに対象外とした統制目標及び詳細管理策、手引きから選択等した管理策の妥当性について制度（審査）の確認を受けることができる枠組みの検討

※改定箇所を下線で明示、そのうちポイントとなる箇所を赤字で明示

ISMAP管理基準改定案の全体像（イメージ図）



ISMAP管理基準改定案　基本言明要件

・ガバナンス基準
　全て実施しなければならない。

・マネジメント基準
　全て実施しなければならない。

・管理策基準
　全ての統制目標としての管理策について、原則として実施しなければならない。**また、詳細管理策も原則として実施すべきものとする。**
　他方、クラウドサービス事業者は自身の提供するサービスと照らし、合理的な適用が不可能**若しくはリスク分析の結果、実施不要と適切に判断した**統制目標としての管理策**及び詳細管理策**については、その理由を示すことで対象外とすることができる。

その他の形式面での修正

- **「2.2 言明書に記載すべき内容」、「2.3 経営者確認書に記載すべき内容」**について、クラウドサービスの登録に係る手続きの一部であり、ISMAP管理基準の性質とは異なるものであることから、**「ISMAPクラウドサービス登録規則」に移すことを前提に、「ISMAP管理基準」からは削除。**
- ただし、「2.2 言明書に記載すべき内容」内に定義されている**「2.2.4 基本言明要件」については、ISMAP管理基準として定める内容であるため、ISMAP管理基準内に記載。**

〔現行ISMAP管理基準〕

2.2 言明書に記載すべき内容
クラウドサービス事業者は、言明に際しては「ISMAPクラウドサービス登録規則」若しくは「ISMAP-LIUクラウドサービス登録規則」で定める様式に従って、以下の内容について書面にて言明を行わなければならない。また、特に変更の言明が行われていない限りにおいて、その言明はクラウドサービス事業者が責任を負うものとして有効であると見なされる。
なお、以下項目のうち、「クラウドサービスの名称」、「言明の対象範囲」、「基本言明要件」のうち実施している統制目標としての管理策、「監査対象期間」、「後発事象」については、ISMAP等クラウドサービスリストにおいて一般に公開することとする。

2.2.1 クラウドサービスの名称
対象としたクラウドサービスの名称を記載する。

2.2.2 言明の対象範囲
一つのクラウドサービスの名称であっても、その傘下に複数のサービスがある場合等、どのサービスを対象にしているのか具体的に記載する。
また、この言明の対象外となるサービスを利用してここに記載するサービスを提供している場合、その範囲及び利用しているサービスを明示し、言明書の対象外になる旨記載をする。ただし、サービスの基盤に言明の対象外となるクラウドサービスを利用している場合には、当該対象外のサービスがISMAPクラウドサービスリストに登録されていることが求められる。
また、対象となるリージョンを記載する。
（中略）

2.3 経営者確認書に記載すべき内容
クラウドサービス事業者は、「ISMAPクラウドサービス登録規則」若しくは「ISMAP-LIUクラウドサービス登録規則」で定める様式に従って、以下の事項を確認するため又は他の監査証拠を裏付けるため、経営者による陳述を書面にて監査人に対して行わなければならない。
（後略）

→ ISMAP管理基準から削除し、ISMAPクラウドサービス登録規則に記載することとする

ガイドラインの策定、事前確認の枠組みの導入

- ISMAP管理基準改定案は、以下のとおりとなっている。
  - 詳細管理策は統制目標を実現するために満たすべき必要最小限の内容の記述に絞り、詳細管理策を具体的に実施するための参考情報は手引きに記述
  - 全ての詳細管理策については原則として実施すべきもの（ただし、「リスク分析の結果、実施不要と判断した」場合も対象外と出来る。）
- クラウドサービス事業者がISMAP管理基準改定案に基づき実効性のある統制構築を行うために必要となる指標や対応を示した「ガイドライン（仮）」を規程として策定し、公表することを検討。
- ガイドラインは、脅威や管理策の重要度の指標を明確化するとともに、統制目標及び詳細管理策を対象外とできる理由の考え方や例示、詳細管理策の実施に当たって手引きから選択等する場合の考え方や例示等を示す予定。審査においては、ガイドラインに基づき統制が構築されていることも含めて確認し、監査においては、実施した詳細管理策に対して現状と同様の方法にて確認する予定。
- 更に、手戻りを防ぐために、実施しようとする管理策の妥当性について、制度（審査）による事前確認を受けることができる枠組みを検討。
- これらの対策により、クラウドサービス事業者、監査機関、制度（審査）の間で共通認識を醸成し、現状でも課題となっている、いわゆる「念のため言明」による監査・審査対応の負担増や再監査等の手戻りに対応する。
- なお、ガイドライン及び事前確認の枠組みに関連する規程改定の際は、ISMAP運営規則2.5.2に基づき、パブリック・コメントを実施する予定。

ガイドラインの内容（案）

指標の明確化	**政府機関等が特に対応が必要と考える脅威の明示** • 政府情報システムの特性を踏まえ、クラウドサービス事業者が優先的に考慮すべき脅威 **脅威を踏まえた管理策の重要度の指標化** • 各管理基準項目に対し、脅威との関連性や重要度を示す指標
対応の明確化	**統制目標または管理策の対象外判断の根拠・手順** • フレームワークを用いた管理策の実装状況の説明方法 **手引きからの選択または独自統制構築の考え方・例示** • 手引きからの選択またはクラウドサービス事業者による独自の統制構築における考え方や例示 • その際の合理的な理由付け、エビデンスの提示方法
その他	• 用語の定義 等

事前確認の枠組み（案）

- 監査・審査前に、クラウドサービス事業者はガイドラインをベースに対象外とした統制目標及び詳細管理策、手引きから選択等した管理策の妥当性について制度（審査）の確認を受けることができる枠組みの検討