| 連番 | 提出意見／電子ファイル | 御意見に対する回答 | 提出者 |
|---|---|---|---|
| 1 | 1. 前提<br>ISMAPは政府機関が利用するクラウドサービスに一定のセキュリティ水準を担保させる制度であり、国民の個人情報や行政サービスの安全性を確保するうえで重要な役割を果たすものであると理解しています。<br>一方で、その運用方法によってはクラウド事業者の負担が増大し、そのコストが利用料に転嫁され、最終的に国民負担の増加につながることを強く懸念します。<br>---<br>2. 懸念点<br>1. **監査コストの過大化**<br>＊「言明書」「経営者確認書」の提出や監査頻度の増加は、特に中小のクラウド事業者にとって高負担であり、結果として参入障壁となるおそれがあります。<br>＊ 大手数社に市場が集中すれば、サービス選択肢が減り、長期的には行政コストの増大や競争力の低下を招きます。<br>2. **除外ルールの不明確さ**<br>＊「合理的に適用できない場合の除外」が規定されているものの、その判断基準が監査人や運用主体の裁量に大きく依存しており、実務上はすべて必須化される懸念があります。<br>＊ 不透明な裁量が残ることは利権的構造を生む温床にもなり得ます。<br>---<br>3. 改善提案<br>国民負担を抑えつつ、セキュリティを確保するために以下の改善策を提案します。<br>1. **国際認証のクロス認証活用**<br>＊ ISO/IEC 27001, SOC2, FedRAMP 等の既存認証を積極的に認め、ISMAP独自の監査は追加部分に限定すべきです。<br>＊ これにより二重監査を避け、コストを大幅に削減できます。<br>2. **リスクベース監査の導入**<br>＊ 高リスクのシステム（基幹系、個人情報大量処理など）は年次監査、<br>低リスクのシステムは数年に一度、あるいはセルフアセスメント＋抜取監査に留めるなど、リスクに応じた柔軟な仕組みが必要です。<br>3. **監査の自動化・標準化**<br>＊ 政府が「ISMAPチェック自動化ツール」を標準提供し、各CSPが同一のツールでセルフチェックできる仕組みを整備してください。<br>＊ 大手クラウドが既に持つセキュリティダッシュボードをISMAP基準にマッピングする形で利用すれば、効率性が高まります。<br>4. **監査機関の多様化と共同監査**<br>＊ 特定の監査法人に依存せず、IT専門の監査会社や中小機関の参入を認めることで、価格競争を促してください。<br>＊ また、複数省庁が同一クラウドを利用する場合は共同監査を導入し、重複コストを避けるべきです。<br>---<br>4. 結論<br>ISMAPの趣旨そのものには賛同しますが、現行案のままでは「監査のための監査」になりかねず、結果として国民の利益を損なう恐れがあります。<br>国際的な整合性を活かしつつ、自動化・効率化・透明性を重視した制度設計に改めていただきたいと考えます。 | 御意見に記載の項目毎に以下のとおり回答いたします。<br>（「1. 前提」について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承ります。<br><br>（「2. 懸念点」1.について）<br>監査コストの過大化に関しまして、ISMAP管理基準改定案において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することによって、詳細管理策の数を削減しているほか、想定されるリスクに応じて統制目標に対応する詳細管理策を選択するのではなく実態としてそれ以上に詳細管理策を選択すること等への対応を行っています。<br>また、ISMAP制度の抜本的な見直しとして、SaaS事業者を対象とする負担を軽減した新たな枠組みを検討中です。<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、登録申請に関する手続きやISMAP制度の監査につきましては、検討中であるところ、御意見として承ります。<br><br>（「2. 懸念点」2.について）<br>御懸念への対応として、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しています。<br>また、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しています。<br>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、現状の課題である監査・審査対応の負担増(想定されるリスクに応じて統制目標に対応する詳細管理策を選択するのではなく実態としてそれ以上に詳細管理策を選択すること等によるもの)や追加監査等の手戻りに対応することとし、御懸念の点が起きないように検討を進めて参ります。<br><br>（「3. 改善提案」1.について）<br>現行制度において、他の認証制度の活用については、他の認証制度における統制内容と共通する部分が一定程度あるものの、準拠している基準、監査・審査の手続き、監査人の要件等が異なり、ISMAPが求めるセキュリティ水準を満たしていることを客観的に担保することが難しいなど、困難な面がございますが、御意見を踏まえ、引き続き検討を進めて参ります。<br>また、ISMAP制度の抜本的な見直しとして、SaaS事業者を対象に、他の認証制度の活用等を通じてクラウドサービス事業者の負担を軽減する新たな枠組みを検討中です。<br><br>（「3. 改善提案」2.について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、ISMAP制度の監査につきましては、検討中であるところ、御意見として承ります。<br><br>（「3. 改善提案」3.について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、ISMAP制度の監査につきましては、検討中であるところ、御意見として承ります。<br><br>（「3. 改善提案」4.について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、ISMAP制度の監査につきましては、検討中であるところ、御意見として承ります。<br><br>（「4. 結論」について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、ISMAP制度の監査につきましては、検討中であるところ、御意見として承ります。 | 個人 |
| 2 | 管理策の数を減らす方向性には賛同いたします。ただし、安全性および信頼性を確保することが最優先であるため、形式的な削減ではなく、実効性の低い重複策の整理にとどめるべきと考えます。 | ISMAP管理基準改定案において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することとしております。詳細管理策の粒度を大きくすることにより、詳細管理策の数を減らしているものの、セキュリティ対策を実施すべき範囲は大きく変わっていないため、安全性及び信頼性は確保できると考えています。 | 個人 |
| 3 | そもそもISMAP原則利用を見直してほしい。ISMAP等クラウドサービスリストに登録されている数が少ないため、選択肢が絞られる。 | 今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承ります。 | 個人 |
| 4 | 「ISMAP制度」ということばは、ISMAP自体が「政府情報システムのためのセキュリティ評価制度」と定義されており、制度ということばが含まれているため、重言ではないか。 | 単にISMAPのみとした場合、制度そのものを指していることが伝わりにくいため、敢えて「ISMAP制度」という表現を用いておりますので、御理解ください。 | 個人 |
| 5 | 第3者認証との重複監査による工数・費用負担の課題は今回の改訂で解決したといえるのか。 | ISMAP制度の抜本的な見直しとして、SaaS事業者を対象とする負担を軽減した新たな枠組みを検討中です。当該枠組みにて他の認証制度の活用を検討しています。 | 個人 |
| 6 | 参考情報として、ISMAP未登録クラウドサービスだが、政府機関等がISMAPと同等以上のセキュリティ要件を満たしたと承認したクラウドサービスのリストを公開してほしい | 今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承ります。 | 個人 |
| 7 | 現行のISMAP管理基準（以下、「現行版」という。）では、セキュリティ管理策の数が多く、クラウドサービス事業者にとって負担となっているため、セキュリティ管理策の数を減らす見直しを実施したISMAP管理基準改定案（以下、「改定案」という。）を出したとあるが、中身をみると単純に現行版の複数ある詳細管理策を改定案の定型管理策のなかに 1 つにまとめただけではないか。本当に負担軽減となっているのか。 | ISMAP管理基準改定案において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することによって、詳細管理策の数を削減しているほか、想定されるリスクに応じて統制目標に対応する詳細管理策を選択するのではなく実態としてそれ以上に詳細管理策を選択すること等への対応を行っています。これにより、一定程度の負担軽減は図れるものと考えています。<br>また、ISMAP制度の抜本的な見直しとして、SaaS事業者を対象とする負担を軽減した新たな枠組みを検討中です。 | 個人 |
| 8 | FedRAMPに比べて登録されているサービスの数が少なすぎる。このことから、ISMAP原則利用を緩和すべきだ。ISMAP自体の制度はいいが、原則利用を強いられてCSP、政府機関等は困惑・混乱しており、制度自体が批判されている。緩和が無理であるなら、他の認証取得等でISMAPと同様のセキュリティ要件を満たすことを承認すべきである。 | 今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承ります。 | 個人 |

| 連番 | 提出意見／電子ファイル | 御意見に対する回答 | 提出者 |
|---|---|---|---|
| 9 | ご担当者様、<br>「ISMAP管理基準改定概要資料」の4ページにつきまして、コメントさせていただきます。<br>先日の説明会で管理基準の改定により、詳細管理策の数は1163→322と減るとご説明がございましたが、4ページのサンプルによりますと、実際には、現在の6.1.4.xの詳細管理策を新しい詳細管理策5.6.1のa)～f)にまとめて含めているだけで、実質何も変わっていないように見えます。そのため、CSPの負担軽減にならないのではないかと思っております。<br>また、手引きを参考とのことですが、採用にするためにa)～f)をすべて満たす必要があるのかどうかの基準もよく分からず、また、監査手続きはa)～f)のすべてに対して実施するのかどうかもよく分かっておりません。<br><br>手引き、ガイドラインの内容を確認しなければ、対応の方法がイメージできないため、早い段階での手引き、ガイドラインの準備をお願いしたく思っています。<br><br>よろしくお願い致します。 | ISMAP管理基準改定案において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することによって、詳細管理策の数を削減しているほか、想定されるリスクに応じて統制目標に対応する詳細管理策を選択するのではなく実態としてそれ以上に詳細管理策を選択すること等への対応を行っています。これにより、一定程度の負担軽減は図れるものと考えています。<br>「ガイドライン」につきましては、例示いただいた御不明点が明らかになるよう、クラウドサービス事業者、監査機関等、関係者の御意見を踏まえながら、内容を検討して参ります。 | 個人 |
| 10 | ■ 問題点1：SaaS活用の妨げとなる制度運用<br>現状：ISMAP未登録のクラウドサービスは、政府調達の対象外と誤解されることが多く、SaaSの柔軟な活用が阻害されている。<br>影響：業務効率化やDX推進に有効なSaaSの導入が進まず、結果としてレガシーなシステム運用が温存される。<br>※ある省庁では、担当者変更に伴い、従来利用許可されていたSaaSサービスがISMAP未登録のSaaSサービスは利用禁止と判断されるなど、ISMAPがSaaS活用の妨げとなっている事例が見受けられます。<br>■ 提言1：ISMAP未登録SaaSの利用に関する明確なガイドラインの整備<br>ISMAP未登録であっても、リスク評価と補完的なセキュリティ対策を講じることで利用可能であることを明文化。<br>SaaS導入時の判断基準や責任分界点を明確にした「SaaS利用判断フレームワーク」の策定。<br><br>■ 問題点2：審査・維持にかかるコストと負担の大きさ<br>現状：ISMAP取得には数千万円、数ヶ月 - 1年超の期間が必要。中小SaaSベンダーにとっては大きな参入障壁。<br>影響：ISMAP登録済みの大手クラウドベンダーに選択肢が偏り、イノベーションや多様性が損なわれる。<br>■ 提言2：SaaS事業者向けのISMAP簡易版（ISMAP-LIU）の運用改善<br>ISO27001/27017/27018取得済みの事業者に対して、ISMAPの一部審査項目を簡略化。<br>中小ベンダー向けに、段階的な登録制度（ステージ制）を導入し、初期登録のハードルを下げる。<br><br>■ 問題点3：制度の硬直性とクラウドの進化との乖離<br>現状：ISMAPの評価基準は年1回の更新で、クラウドサービスの進化スピードに追いついていない。<br>影響：最新のセキュリティ技術や運用モデル（例：ゼロトラスト、DevSecOps）が制度に反映されにくい。<br>■ 提言3：ISMAP評価基準の柔軟化と更新頻度の見直し<br>クラウド技術の進化に即応できるよう、評価基準の半期ごとの見直しを検討。<br>新技術・新運用モデルに対応した「技術別補足ガイドライン」の整備。<br><br>■ 問題点4：国際認証との整合性の不在<br>現状：ISO27001/27017/27018などの国際認証がISMAPの代替として認められていない。<br>影響：すでに認証を取得済みの多くのクラウドベンダーにとって、ISMAPは重複対応となり、非効率。<br>■ 提言4：国際認証とのマッピングと審査簡略化の仕組み導入<br>ISO認証取得済みの事業者に対して、ISMAPの該当項目をマッピングにより自動適合とする制度を導入。<br>FedRAMP（米国）やC5（ドイツ）など、他国の制度との相互認証の可能性を検討。<br><br>■ 問題点5：国外リージョンのみのクラウドサービスに対する制度的な制約<br>現状：ISMAP制度では、クラウドサービスのデータ保管先が国外にある場合、政府調達における利用が事実上困難となるケースが多い。<br>背景：政府の基本方針では「国内法の適用が担保される国内データセンターの利用」が原則とされており、国外リージョンの利用には高いハードルがある。<br>影響：グローバルに展開するクラウドベンダーの多くが日本国内にデータセンターを持たない、または限定的なサービスしか提供していないため、有用なクラウドサービスの選択肢が狭まる。<br>国外リージョンにしか存在しない先進的なSaaSやAIサービスの活用が制限され、政府のDX推進に逆行する可能性がある。<br><br>■提言5：国外リージョン利用に関するリスクベースの柔軟な運用指針の整備<br>国外データ保管を一律に排除するのではなく、リスク評価に基づく柔軟な判断を可能とする制度設計を行う。<br>具体的には以下のような対応を提案：<br>国外保管が許容される条件の明文化（例：暗号化、アクセス制御、契約上の準拠法・裁判管轄の明記など）。<br>国外リージョン利用時のリスク評価テンプレートの提供と、評価結果に基づく利用可否判断の標準化。<br>国外リージョンの利用に関する透明性の確保（例：データの所在、移転先、アクセスログの開示など）。<br>※GitHubのような欧米諸国の政府機関でも活用されている世界標準のクラウドサービスが利用できず、ガバクラ上の仮想サーバにインストールして利用するなど管理面・コスト面で負担を強いられている状況と認識しています。<br><br>■ 総括<br>ISMAP制度は政府情報システムのセキュリティ確保に重要な役割を果たしていますが、現行制度のままではSaaS活用やクラウドの柔軟性を阻害するリスクがあります。<br>制度の信頼性を維持しつつ、実効性と現場適用性を高めるための制度改革が急務と考えます。 | 御意見に記載の項目毎に以下のとおり回答いたします。<br>（■ 提言1について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承ります。<br>なお、ISMAP制度の抜本的な見直しとして、SaaS事業者を対象に、他の認証制度の活用等を通じてクラウドサービス事業者の負担を軽減する新たな枠組みを検討中です。<br><br>（■ 提言2について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、登録申請に関する手続きやISMAP制度の監査につきましては、検討中であるところ、御意見として承ります。<br>なお、ISMAP制度の抜本的な見直しとして、SaaS事業者を対象に、他の認証制度の活用等を通じてクラウドサービス事業者の負担を軽減する新たな枠組みを検討中です。<br><br>（■ 提言3について）<br>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しています。「ガイドライン」の見直しのタイミング等、御意見として承ります。<br><br>（■ 提言4について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承ります。<br>なお、ISMAP制度の抜本的な見直しとして、SaaS事業者を対象に、他の認証制度の活用等を通じてクラウドサービス事業者の負担を軽減する新たな枠組みを検討中です。<br><br>（■ 提言5について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承ります。<br><br>（■ 総括について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承ります。 | 個人 |
| 11 | 今回の改定は、これからISMAPに登録しようとするCSPにとっては歓迎的な改定ではあるかもしれない。しかしながら、既にISMAPクラウドサービスリストに登録済みのCSPにとっては、現行の約1,000個超の管理策で引き続き対応をするほうが、既に対応済みであるので、改定対応するよりも容易（説明会でCSPから異口同音にコメントがあった、個別管理策の抽象化による弊害を受けたくない）ということも考えられる。一律に制度改定ではなく、新規のCSPに対しては、新たな枠組みで対応し、登録済みのCSPに対しては、既存または新たな枠組みの選択制（一時的な経過措置ではなく、より長い期間で）を検討しては如何か。 | 御意見の内容は新基準適用のタイミングや経過措置について、重要な観点と認識しております。既にISMAP等クラウドサービスリストに登録されているクラウドサービス事業者、新規で登録を予定されているクラウドサービス事業者、監査機関等、関係者の御意見を踏まえながら慎重に検討を進めて参ります。 | 個人 |
| 12 | ISMAP廃止！ | 今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承ります。 | 個人 |

| 連番 | 提出意見／電子ファイル | 御意見に対する回答 | 提出者 |
|---|---|---|---|
| 13 | 本意見は、令和7年度版「ISMAP管理基準改定案」に対し、クラウドサービス事業者（以下CSP）の実務負担軽減および制度の実効性確保の観点から提出するものです。<br><br>1. 詳細管理策の削減に関する実効性について<br>改定案では、詳細管理策の数を1,163項目から322項目へ削減するとされていますが、実質的には従来の4桁レベルの要求事項を3桁レベルに集約した構造的な整理に留まっているように見受けられます。仮に「手引き」から旧制度における詳細レベル相当の管理策選定や、合理的理由付け・制度側との事前相談を必要とする運用となる場合、実務上は従来と同等の工数が発生し、負担軽減の効果が限定的となる懸念があります。したがって、形式的な項目削減に留まらず、実務工数削減の観点から、制度全体での運用をルール化し明文化して頂ければ幸いです。<br><br>2. リスクベースによる非採用の事前承認制について<br>改定案における「リスク分析の結果、実施不要と判断した」場合の事前承認枠組みについては、効果的かつCSPの実務に側した運用設計が不可欠と考えます。詳細管理策単位で精緻なリスク分析やエビデンス提示を求め、更にIPAから追加質問が多発するような運用となれば現行方式よりも工数が増大するという矛盾が生じる懸念があります。この制度の導入に際しては、以下の点を考慮いただきたいと考えます。<br>明確な判断基準と合理的理由付けの要件をガイドライン上で明示的に文書化する<br>様式等を準備し、画一的な審査内容の基準を設けること<br>監査機関の意見書等を添付する機会を提供し、監査機関による職業的判断を尊重し、制度側（IPA）からの過度な再確認を回避する運用こと<br><br>3.「手引き」の解釈と運用範囲の明確化について<br>改定案では「詳細管理策の具体的実施方法を『手引き』に記載」とされていますが、これまでの経験的なIPAの審査の実情を鑑みると、旧制度の詳細管理策が実質的に手引きに移行することにより、手引きの内容が事実上の必須要件化する懸念があります。<br>事業者が統制目標を達成する代替的な方法を柔軟に適用できるよう、以下の点を明文化することを要望します。<br>手引きに記載された内容は「参考」・「例示」であり、全ての内容の実施を要件としないことを明文化すること<br>手引きに記載された個別の事項（旧４桁レベル）が全て充足されていない場合であっても、統制目標の達成が合理的に説明できる場合問題がないとする旨を明文化すること<br>手引きに記載された個別の事項（旧４桁レベル）の非選択については事前承認が不要であることを明文化すること<br><br>4. IPAの運用への懸念<br>現行制度における運用では、IPAへの事前相談制度を活用しても、以下のような課題が生じています。事前で合意済みの内容が、本申請後のIPAからの問い合わせで覆される、または全く別の観点から再三質問を受ける事例がある。IPAからの問い合わせが数十件規模に及ぶこともあり、またIPAからの個別の返信を受領するのに数週間を要するケースがあるこれにより、登録審査期間が長期化し、結果としてCSP・審査機関（IPA）双方の負担増に繋がっています。つきましては、制度運用上の改善として以下を要望します。<br>IPAの審査体制強化及びリソース拡充<br>CSPからの回答に対するIPAの返信にサービスレベル（SLA）を設定する<br><br>5. 他クラウドサービス利用に関する確認事項の明確化<br>他クラウドサービス等の利用確認に関しては、ルール化されていないにも関わらず実質的に必須書類化しています。本申請後もしくは事前相談において、CSPが利用中の他クラウドサービス全てに対してI使用方法やデータの取り扱い等、統制に踏み込んだ詳細な質問がIPAからなされます。ISMAPの管理策において、ベンダー管理に関する統制や契約に関する統制等、当該書類で提供する内容を含む統制は既に評価済であるにも関わらず、実質的に本申請後にIPAが更にCSPを監査している現状があることをご理解ください。上記の通り、質問が実質的な統制やプロセスに踏み込んだ詳細なものであるため、IPAからの追加質問が多発し易く、登録までのリードタイム増加に繋がっています。<br>近年は端末やアプリケーション利用環境が多様化していること、関連統制は既にISMAPの詳細監理策で評価済であること、ルール上必要書類とされていないという点を鑑み、以下の改善を要望いたします。<br>ルール上明確に要求されていない書類については、CSPに提出を求めないこと。<br>審査にあたり確認が必要な点は、ポータルの直接的なメッセージで完了するレベルに留め、具体的な統制やプロセスに踏み込んだ監査レベルまで求めないこと。<br>上記に関わらず当該書類の提出が必要であると判断する場合は、必須である旨を明文化し周知すること。またその場合出会っても、軽微なクラウドサービス利用にまで対象を拡張しないよう、重要性・リスクに基づいた適用範囲を定義すること。<br><br>6. 監査工数およびコスト負担軽減について<br>現状、ISMAP認証監査を実施できる監査法人は限定的であり、監査機関間での競争原理が十分に働かず、監査費用が高止まりしています。その結果、ISMAP取得が困難な事業者は未だ多く、制度の普及拡大を妨げる要因となっています。そのため、以下を提案します。<br>認証監査を実施可能な監査機関の拡充<br>CSPの詳細監理策の実施度合いに応じたISMAP準拠レベルの導入<br><br>以上<br>ISMAPの信頼性確保と普及促進の両立を図るため、制度の実効性向上と実務負荷軽減の両面から改定案の再検討をお願いしたく存じます。 | 御意見に記載の項目毎に以下のとおり回答いたします。<br>（1. 詳細管理策の削減に関する実効性について）<br>御意見としていただいた制度全体でのルール化及び明文化に関しては、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しています。<br>また、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しています。<br>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、現状の課題である監査・審査対応の負担増(想定されるリスクに応じて統制目標に対応する詳細管理策を選択するのではなく実態としてそれ以上に詳細管理策を選択すること等によるもの)や追加監査等の手戻りに対応することとし、御懸念の点が起きないように検討を進めて参ります。<br><br>（2. リスクベースによる非採用の事前承認制について）<br>「リスク分析の結果、実施不要と判断した」場合の事前承認の枠組みについて、審査においてクラウドサービス事業者のリスク分析の結果を確認する必要があると考えているところ、御意見も踏まえ、クラウドサービス事業者における対応工数の増大といった状況が生じることのないよう検討を進めて参ります。<br><br>（3.「手引き」の解釈と運用範囲の明確化について）<br>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しているところ、御意見も踏まえ、検討を進めて参ります。<br>なお、ガイドライン策定の際は、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であるほか、パブリック・コメント前にも関係者向けの説明会等で丁寧に説明して参りたいと考えています。<br><br>（4. IPAの運用への懸念について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承ります。<br><br>（5. 他クラウドサービス利用に関する確認事項の明確化について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、登録申請に関する手続きにつきましては、検討中であるところ、御意見として承ります。<br><br>（6. 監査工数およびコスト負担軽減について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、ISMAP制度の監査につきましては、検討中であるところ、御意見として承ります。<br>なお、ISMAP制度の抜本的な見直しとして、SaaS事業者を対象とする負担を軽減した新たな枠組みを検討中です。 | 企業 |

| 連番 | 提出意見／電子ファイル | 御意見に対する回答 | 提出者 |
|---|---|---|---|
| 14 | ご検討ありがとうございます。以下4点を提出いたします。<br>1)要求内容は減ることがなく、集約されているだけのため、１つの項目に対しての要求事項が増えるため、楽になっていないように見受けられます。<br>2)リスク評価や事前相談の方針及びやり方を記載したガイドラインに対して、今回のように事前の意見公開・パブリックコメント募集の手順を踏む必要があると思われます。<br>3)事前確認会が任意とはいえ、リスク評価の妥当性を確認する場であるとすると、ISMAP運営委員会、および監査法人と2回の審査を受けることとなると推察される。その場合の負荷が非常に高いため、負荷軽減の策を立てて頂くことを希望します<br>4)リスク分析の事前確認会で検討した内容を、クラウドサービス事業者が合意した場合、公開して欲しい | 御意見に記載の項目毎に以下のとおり回答いたします。<br>（1について）<br>御意見の要求内容に関しまして、ISMAP管理基準改定案において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することによって、詳細管理策の数を削減しているほか、想定されるリスクに応じて統制目標に対応する詳細管理策を選択するのではなく実態としてそれ以上に詳細管理策を選択すること等への対応を行っています。これにより、一定程度の負担軽減は図れるものと考えています。<br>また、ISMAP制度の抜本的な見直しとして、SaaS事業者を対象とする負担を軽減した新たな枠組みを検討中です。<br><br>（2について）<br>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です。<br><br>（3について）<br>事前確認の枠組みは、手戻りや、想定されるリスクに応じて統制目標に対応する詳細管理策を選択するのではなく実態としてそれ以上に詳細管理策を選択すること等を抑止するために検討しています。目的に照らし事前確認による負荷が増加することがないよう、御指摘いただいた点を踏まえ、事前確認の枠組みの検討を進めて参ります。<br><br>（4について）<br>事前確認による確認事項は機密性の高い情報を含むため、公開については慎重に検討を進めて参ります。 | 個人 |
| 15 | コメント対象箇所：ISMAP管理基準(案)の2.1、2.2及び、参考2の管理策基準における定型管理策及び手引き(案)及び、ISMAP管理基準改定概要資料のp5「ISMAP管理基準改定案の全体像」<br>コメント内容：<br>ISMAP管理基準の2.1,2.2などにおける「管理策基準」で、リスク分析の結果、リスク対応方針に従って管理策を実施する際の選択肢を与える、あるいは、対象外とすることができるなどの説明があり、従来と同じくリスクベースで管理策の選択する旨が説明されている一方、ISMAP管理基準改定概要資料p5「ISMAP管理基準改定案の全体像」で、「詳細管理策(253個)：抜本的な見直し」「基本言明要件＞ 管理策基準：また詳細管理策も原則として実施するべきものである」という説明から受ける、詳細管理策253項目だけを一律実施すればよいという印象から、初見の読者等にとっては、「リスク分析による選択」の重要性の認識が薄くなる可能性があるのではと懸念している。<br>特に、改定後は、詳細管理策から、具体的な実施手段等に相当する内容を手引きにグルーピングしていることから、リスク分析等の結果により、手引き相当の具体的な実施手段・内容まで選択・決定することの認識が薄れるのではないか、<br>ISMAP監査時における監査精度は改定前と同様で、具体的な手段・内容を記載した規程・ルールやその実施記録を証跡として評価されると想定されるが、上記の認識が薄くなることによって、証跡も不十分なものになるのではないか、と懸念している。<br>リスクベースのアプローチと具体的な手段・内容の決定、実施等の重要性を、改めて周知、啓発する必要があると考えているが、周知・啓発イベントあるいは、管理策ガイドやマニュアル等での強調など、何らかの施策を制度側で検討するべきでは。 | 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しています。<br>クラウドサービス事業者に過度の負担が生じることのないよう、ガイドラインの整備ほか必要な対策について検討を進めて参ります。 | 企業 |
| 16 | コメント箇所：ISMAP管理基準(案)の2.1本管理基準の構成、2.2(3)管理策基準、及び参考2「管理策基準における定型管理策及び手引き(案)」<br>コメント内容：<br>【ISMAP管理基準(案)2.1の末尾4行の引用：「管理策基準」は、組織における情報セキュリティマネジメントの確立段階において、リスク対応方針に従って管理策を実施する際の選択肢を与えるものである。<br>なお、「管理策基準」における 詳細管理策を実施する ための参考情報（例示） として 、 手引きを定めている。】<br>2.1末尾4行における、「リスク対応の方針に従って管理策の実施する際の選択肢」として何を指すかが、本文章からは分かりません。<br>選択肢とは、次の行にある、「参考情報(例示)として、手引きを定めている」の、参考2の「手引き」欄に記載されている、具体的な手段相当の各文章のこと指しますか（*1)。<br>現状の記載では、「詳細管理策の実施するための参考情報」であり、選択肢であるというようには読み取れません。<br>仮に、(*1)「手引き」欄の各文章＝選択肢であり、リスクアセスメント等に基づき具体的にどのように行う内容を決めるのであれば、その旨が分かるように、表現の修正をお願いしたい。<br>(*1)が、「手引き」＝選択肢ではない場合、何を選択肢としているか補足説明をしていただきたい。<br><br>【ISMAP管理基準(案)2.1(3)の最初の2行の引用：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 。】<br>特に、2.1(3)の最初の行に、「管理策について、原則として実施」「詳細管理策 （ X.X.X ） も原則として実施」と記載してあるため、2.1末尾4行にある、「選択肢」が何をさすのか分かりにくい。あるいは、2.1(3)の「原則として実施」という文言のインパクトから、リスクアセスメント等の結果、何等かの対策・手段を選択・決定するという行為が省略され、一律同管理策の実施などの印象を持たれてしまうのではとも考える。<br><br>また、本改定案の参考2を見るに、管理策基準の詳細管理策(X.X.X）には、必要最低限の要件相当のみを規定しているように思える。<br>(例)5.1.1情報セキュリティ方針を策定し、トップマネジメントが承認する。<br>上記のみを満たすのであれば、例えば、「社としてセキュリティに取り組む」などの端的な姿勢を記載し、経営陣の署名のみがあることを外部監査で確認できればよいことになる、と解釈される可能性がある。<br>が、対象クラウドサービスのセキュリティリスク等を考慮することや5.1に規定されている「目的」を満たすことを考慮すれば、例えば「手引き」欄に示される方針に含めるべき記載をどのように定め、具体的に含んでいるかなども外部監査で確認する必要があると想定する。<br>上記のような解釈のどちらが正しいかを示すことも含め、「手引き」や、「手引き」と「詳細管理策」、「管理策を実施する際の選択肢」に関する説明をしていただきたい。<br><br>また、必要に応じて、リスクアセスメント・リスク対応、その結果への外部監査での確認等について周知・啓発等もして頂きたい。 | 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しています。<br>クラウドサービス事業者に過度の負担が生じることのないよう、ガイドラインの整備ほか必要な対策について検討を進めて参ります。 | 企業 |

| 連番 | 提出意見／電子ファイル | 御意見に対する回答 | 提出者 |
|---|---|---|---|
| 17 | コメント箇所：ISMAP管理基準(案)の旧2.2言明書に記載すべき内容～2.2.3システムと内部統制の全体像、2.2.6後発事象　の削除<br>コメント内容：<br>旧2.2言明書に記載すべき内容が、全て削除されているが、これは、ISMAP登録規則3.8に言明書に記載すべき内容（項目レベル）が記載されているため、あるいは、ISMAP登録規則・様式1言明書等に旧記載相当を記載する予定のため、削除しているのか。 | 「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管理基準改定案」からは削除し、「ISMAPクラウドサービス登録規則」等に移すことを検討しています。 | 企業 |
| 18 | コメント箇所：ISMAP管理基準(案)の旧2.2.5監査の対象となる期間　の削除<br>コメント内容：<br>ISMAP管理基準(案)の旧2.2.5監査の対象となる期間　は、ISMAP登録規則に、同様の記載はない（監査対象期間が3ヶ月以上であることの記載はあるが、最大1年という記載はない）が、ISMAP登録規則等に旧記載相当を記載する予定のため、削除しているのか？<br>または、「監査の対象期間は最大１年」とするルールを廃止する予定か？<br>上記のいずれでもないならば、どこかに、監査の対象期間が最大1年であることの記載が必要と考える。 | 「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管理基準改定案」からは削除し、「ISMAPクラウドサービス登録規則」等に移すことを検討しています。 | 企業 |
| 19 | コメント箇所：ISMAP管理基準(案)の旧2.3経営者確認書に記載すべき内容　の削除<br>コメント内容：<br>ISMAP管理基準(案)の旧2.3経営者確認書に記載すべき内容　は、ISMAP登録規則に、同様の記載はない（経営者確認書への言及はある）が、ISMAP登録規則・様式2経営者確認書等に旧記載相当を記載する予定のため、削除しているのか？<br>上記のいずれでもないならば、どこかに、旧2.3経営者確認書相当の記載が必要と考える。 | 「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管理基準改定案」からは削除し、「ISMAPクラウドサービス登録規則」等に移すことを検討しています。 | 企業 |
| 20 | コメント箇所：ISMAP管理基準(案)の3.2情報セキュリティガバナンスの目的<br>コメント内容：<br>ISMAP管理基準(案)の「2.2(1)ガバナンス基準」で、「全て実施しなければならない」とあるが、「3.2情報セキュリティガバナンスの目的」の「…目的を設定する」ことも、統制目標として、整備・運用すべき事項にあたるのか？<br>ISMAP管理基準(案)の「3.1情報セキュリティガバナンスの概要」は、概要としての説明であり、整備・運用事項ではない、また、「3.3情報セキュリティガバナンスのプロセス」で、「ガバナンス基準における統制目標及び詳細管理策は、別表1 のとおりとする。」とあるため、3章ガバナンス基準の整備・運用すべき統制目標及び詳細管理策は、別表1のみの内容であり、3.2は、ガバナンスのあり方の説明とも読める。<br>3.2はどのような扱いになるのか？<br><br>あるいは、3.3指示（3.3.3.1や3.3.3.2）で規定している、「目的の設定」等が、3.2の具体的な管理策内容にあたると解釈するのか？ | ガバナンス基準、マネジメント基準は現行と大きく変更はなく、統制目標及び詳細管理策が言明対象です。ISMAP管理基準改定案に「ガバナンス基準における統制目標及び詳細管理策は、別表1 のとおりとする。」と規定しておりますため、3.2のような別表に規定されていない2桁は言明対象ではございません。なお言明書を含む「ISMAPクラウドサービス登録規則」等についても今後、改定することを検討しています。 | 企業 |
| 21 | コメント箇所：ISMAP管理基準(案)の別表の構成<br>コメント内容：<br>今回の改正では、以下に相当する別表は提示されない予定か？<br>・別表4.マッピング(管理策基準vs統一基準)<br>・別表5.マッピング(統一基準vs管理基準)<br>・別表6. マッピング 管理基準 vs SP800 53)<br>・別表7. マッピング(SP800 53 vs 管理基準)<br>・別表8. 個別管理策の実施頻度の例 | マッピング等については、今回の意見募集の対象であるISMAP管理基準改定案を公表した後、作成し公開することを予定しています。<br>「別表8.個別管理策の実施頻度の例」についてはガイドラインに規定することを予定しています。 | 企業 |
| 22 | コメント箇所：ISMAP管理基準(案)の7.4物理的セキュリティ監視<br>コメント内容：<br>SaaSなどでは、物理的筐体等をもたないとして、物理的な管理策を適用除外とするケースがあるようである。<br>が、SaaSの開発・保守業務を行う上で、物理的な居室や装置の利用はあり、それらにたいする最低限の監視は必要と思われる。<br>IaaSでサーバやストレージ等を格納するデータセンタ等での監視対策の内容と、SaaSの業務を行う上での居室の監視対策の内容は、リスクアセスメント等の結果により当然異なり、その具体的な内容は、言明書の個別管理策等で提示され、評価される認識でよいか。 | 御認識のとおり、一律に個別管理策の内容を決定するものではなく、リスクアセスメントの結果に応じて個別管理策を検討いただく必要があります。<br>なお、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しています。<br>また、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しています。<br>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、現状の課題である監査・審査対応の負担増(想定されるリスクに応じて統制目標に対応する詳細管理策を選択するのではなく実態としてそれ以上に詳細管理策を選択すること等によるもの)や追加監査等の手戻りに対応することとし、御懸念の点が起きないように検討を進めて参ります。 | 企業 |
| 23 | コメント箇所：ISMAP管理基準(案)の8.23ウェブフィルタリング<br>コメント内容：<br>ウェブフィルタリングについて、外部のウェブフィルタリングサービス等を利用している場合、当該外部サービス事業者もISMAP取得している必要があるか？<br>あるいは、申請者であるクラウドサービス事業者が、外部サービス事業者の管理策の整備・運用内容を直接確認することで、本管理策を採用とすることが可能か。<br>あるいは、クラウドサービスを提供する上で必要不可欠なサービスではないとして、申請者であるクラウドサービス事業者が、上記のような直接確認をせずとも、セキュリティレベルを確保した契約を締結し、契約通りにサービスが提供されていることを確認していれば、採用とすることが可能か。 | 具体的な管理策について継続して検討を進めて参りますが、外部サービスの利用については、外部サービス事業者がISMAPを取得していることの確認や、現行の13.1.2のような、ネットワークサービスの提供者と合意の合意、監視、監査をクラウドサービス事業者が実施する等といった対応が考えられます。 | 企業 |
| 24 | 1. 依拠する基準の見直し<br>JISQ27000群を参照しているが、政府機関のセキュリティ基準である政府統一基準群を必ず満足するとは限らない点が現状の課題と考える。解決案として、政府統一基準群を参照するよう変更することで、NIST SP800-53/171とFedRAMPとの関係のような垂直統合が図れるのではないか。<br><br>2. 詳細管理策の公開<br>JISQ27000群を参照しているためにISOのライセンスによる管理策の公開制限を受ける点に対し、公開されている基準、例えば上で挙げた政府統一基準群、または情報セキュリティ管理基準を参照することでライセンスの問題を解決できないか。<br><br>3. pdf以外の形式での共有<br>言明書がpdfのみで提供されており、プロバイダでの利活用に支障がある。情報セキュリティ管理基準が今回の改定でExcel等での公開を予定しており、同様の対応を期待したい。<br><br>4. 言明書に記載されるべき項目の見直し<br>言明書を見ても管理策番号だけでは採用した管理策の詳細内容が把握できない問題がある。言明書のフォーマットについては、前述したライセンスの制約が解決することを前提に、管理策の文面を合わせて公開できるのではないか。 | 御意見に記載の項目毎に以下のとおり回答いたします。<br>（1. 依拠する基準の見直しについて）<br>政府機関等のサイバーセキュリティ対策のための統一基準群 (以下「政府統一基準」という。)も参照しており、一定の抽象度のレベルにおいて、JISQ27000群においてカバーされていない政府統一基準の部分については、ISMAP管理基準改定案に取り入れております。<br><br>（2. 詳細管理策の公開について）<br>改定案は御意見に記載の情報セキュリティ管理基準や政府統一基準を基に作成しています。民間において実施されている情報システムに関するセキュリティ監査により、既に一定程度の知見が集積していること、一定の評価水準を確保することが可能なこと、運用後の継続的な確認が可能であることといった観点から、国際規格であるISO/IEC 27017に基づいた「クラウド情報セキュリティ管理基準」を基に管理策を作成しているところ、ライセンスについては御理解を賜りたく存じます。<br><br>（3. pdf以外の形式での共有について）<br>御指摘いただいた点については、継続的に検討を進めて参ります。<br><br>（4. 言明書に記載されるべき項目の見直しについて）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、登録申請に関する手続きにつきましては、検討中であるところ、御意見として承ります。 | 個人 |

| 連番 | 提出意見／電子ファイル | 御意見に対する回答 | 提出者 |
|---|---|---|---|
| 25 | 情報セキュリティマネジメントに関わる国際規格の改正を踏まえたISMAP管理基準ついては、情報セキュリティを取り巻く環境の変化を踏まえた所要の見直し、それを踏まえたガイドラインの策定・公表が重要と考えております。今回の改正は、令和7年8月改正の「情報セキュリティ監査基準改正案等」を踏まえたもので、誠に時宜を得たものであり、弊社として賛同申し上げます。 | 御意見ありがとうございます。継続してより良い制度になるよう検討を進めて参ります。 | 企業 |
| 26 | 今回の変更で詳細管理策数が1,163項目から322項目に減らしたということが大きく取り上げられてますが、ISMAP管理基準改定概要資料の右下P3の吹き出しで、「なお、監査においては手引きを参考に監査を実施」と記載があります。手引きを参考に監査が実施されるのであれば、手引きの項目も含まれるため、実質的な項目数の削減とは言えないのではないでしょうか。P3の管理策 5.6.1も対照表を確認しても削減されたようには見えません。また、審査費用にもあまり影響がないような気がします。審査費用が高額という課題もあったと思いますので、何らかの対策が必要かと思われます。 | ISMAP管理基準改定案において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することによって、詳細管理策の数を削減しているほか、想定されるリスクに応じて統制目標に対応する詳細管理策を選択するのではなく実態としてそれ以上に詳細管理策を選択すること等への対応を行っています。これにより、項目数及び監査費用に関する課題に関して、一定程度の負担軽減は図れるものと考えています。<br>また、ISMAP制度の抜本的な見直しとして、SaaS事業者を対象とする負担を軽減した新たな枠組みを検討中です。 | 企業 |
| 27 | 意見１<br>今回意見募集対象となった管理基準では、詳細管理策の数は既存の管理基準における１１６３個から３２２個まで数が減少し、抽象度が増しました。改正の趣旨が、ＣＳＰの統制やリスク判断を尊重することによりセキュリティ水準を確保しつつ審査負担を軽減するという趣旨であれば、改正の趣旨には感謝し賛同いたします。<br>他方で、既存の詳細管理策は基本的には同じく意見募集対象である手引き案に移行されています。実際の運用におけるこの手引き記載の位置付け如何によっては、単純に詳細を手引きに移管しただけで実質的な変化の無い改正にとどまってしまうおそれもあります。<br>今回の改正によりセキュリティ水準を確保しつつ審査負担を軽減するという意図が達成されるか否かは、ガイドラインを始めとする今後の詳細の制度設計次第と考えられます。詳細制度設計においては、ＣＳＰにおけるセキュリティ確保や内部監査の現行の実務を踏まえた検討が肝要であり、ＣＳＰとしてもこれまで以上に議論に貢献させていただければありがたく存じます。<br>現時点では、今後のガイドラインの検討において考慮いただきたい点として、以下２点を提出致します。<br>（１）ガイドラインは、ＣＳＰが個別の統制に応じて柔軟に適切な管理策を選択できるよう、唯一の選択肢として記載されるのではなく、あくまでも考え方や事例を示すものとしていただきたくことを要望します。<br>（２）管理基準第３章と４章のガバナンス基準において「を考慮して決定／定義する」といった解釈の難しい表現が多く見受けられます。こういった解釈の難しい表現について、ガイドラインにおける解釈の明確化がなされることを要望します。 | 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しているところ、御意見も踏まえ、検討を進めて参ります。<br>また、クラウドサービス事業者、監査機関等、関係者の御意見を踏まえながら、内容を検討して参ります。 | 企業 |
| 28 | 意見２<br>管理基準改定案の「２．２基本言明要件」「（３）管理策基準」基準において、「詳細管理策を原則として実施すべきものとする。」としています。<br>一方で、「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。」としています。<br>一定のセキュリティ水準を担保しつつ登録負担を軽減するという改正の趣旨を実現するためには、この対象外の判断がＣＳＰのリスク分析を尊重するリスクベース・アプローチで実施されることが肝要です。非採用理由である「適用不可能」や、「リスク分析の結果、実施不要」との判断は、ＣＳＰがリスクアプローチに基づいて実施するものであり、審査機関はその判断を尊重すべきであることを管理規定及びガイドラインにて明確化・強調していただくよう要望します。 | 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しています。<br>また、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しています。<br>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、現状の課題である監査・審査対応の負担増(想定されるリスクに応じて統制目標に対応する詳細管理策を選択するのではなく実態としてそれ以上に詳細管理策を選択すること等によるもの)や追加監査等の手戻りに対応することとし、御懸念の点が起きないように検討を進めて参ります。御意見も踏まえ、利用者が政府機関等であるという前提ではありますが、できる限りクラウドサービス事業者の判断を尊重できるよう、ガイドラインの内容について検討を進めて参ります。 | 企業 |
| 29 | 意見３<br>今回の管理基準改定は、セキュリティ水準を維持しつつ、サービス登録における政府とＣＳＰの過度な負担を軽減するため、内部監査、外部監査、審査の一連の流れにおける関係機関の協働関係を改善、効率化することが目的とされていると理解しております。<br>この目的を達成するには、今後のガイドライン等の検討が、（１）ＩＳＭＡＰにおけるリスクベース・アプローチ実績が乏しいことに鑑み、幅広いステークホルダーの知見を持ち寄り実施されること、（２）ステークホルダーの共通認識及び相互理解を促進しながら実施されること、（３）審査基準・監査基準の最新の検討と有機的に連動し制度全体の円滑な運用を目指して実施されることなどが不可欠です。そのための具体的な検討方法として、以下３点をご提案させていただきます。<br><br>（ア）　マルチステークホルダーによる協議の場の設置<br>制度官庁が個別に行うヒアリングではなく、ＣＳＰ、監査機関、審査機関の実務者、各基準の改定担当者、利用官庁側代表者も交えた、実務者レベルで双方向で議論できる協議の場を設けること。<br>（イ）具体的で実践的なガイドラインの作成<br>上記協議の場を活用し、監査・審査の趣旨や観点、満たすべき基準を具体的にガイドラインへ盛り込むことで、解釈の齟齬による手戻りを防ぐなど真に価値のあるガイドラインとすること。<br>（ウ）官民連携の枠組みの恒久化<br>この協議の場を恒常的な官民の意見交換の枠組みとし、継続的に知見を蓄積する。これにより、関係者間の共通認識を醸成し、「念のため言明」や再監査といった不必要な負担を軽減すること。 | 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しています。<br>御意見も踏まえ、関係者の御意見を踏まえながら、ガイドラインの内容について検討を進めて参ります。 | 企業 |
| 30 | 意見４<br>「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中」との点について、この制度の利用が任意であり必要に応じて利用可能である場合は有意義な枠組みと考えられます。しかし利用が実質的に必須となる場合は、審査機関にとっても、ＣＳＰにとっても過度な負担となり審査コスト・期間の増大に繋がるリスクがあります。<br>これまでのご説明により利用は任意と理解しておりますが、その旨を文書上に明記していただけますよう要望します。 | 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しています。<br>御意見も踏まえ、事前確認による負荷が増加することがないよう、事前確認の枠組みの検討を進めて参ります。 | 企業 |

| 連番 | 提出意見／電子ファイル | 御意見に対する回答 | 提出者 |
|---|---|---|---|
| 31 | 意見５<br>ＩＳＭＡＰ管理基準の別表１から３（案）に記載された一部のＪＩＳ規格を参照して作成した詳細管理策が非表示となっています。原規格の著作権の関係で一般公開ができないという理由は理解できますが、原規格を所有している者にはマスキングを解除した新旧対照表を共有するなど、ステークホルダーへの情報公開と何らかの意見聴取の機会を別途調整していただくよう要望します。 | ISMAP管理基準改定案及び新旧対照表は、ISMAPポータルの請求フォームから資料請求できるページを、年内に公開予定です。<br>なお、請求に当たり以下のJIS規格の購入が必要です。<br>JIS Q 27017:2016 (ISO/IEC 27017:2015)<br>JIS Q 27014:2015 (ISO/IEC 27014:2013) | 企業 |
| 32 | 意見６<br>ガイドライン、その他の規程の公開・改定スケジュールは検討中とのことですが、改定後のＩＳＭＡＰ管理基準の適用開始時期含め大まかなスケジュール感をご教示いただくよう希望します。なお、審査機関、監査機関、ＣＳＰの相互の議論や各組織の適用準備のため相応の準備期間が必要であり、管理基準、手引き、ガイドライン、並びに関連規程の公開から改定後の管理基準の適用開始まで２年間の準備猶予期間が望ましいと考えます。<br><br>意見７<br>規制改革推進会議答申も踏まえ、政府とＣＳＰの負担軽減、ひいてはサービス利用者の便益のため、ＣＳＰ事業者が取得したＩＳＯ２７０００シリーズやＳＯＣ２等の証跡流用の進め方について、官民実務者級での議論が実施されることを要望します。また、今回の管理基準改定を契機としたＩＳＭＡＰ登録制度におけるリスクベース・アプローチの導入においては、これらの国際規格の監査における同アプローチ導入の前例が参考にされることを期待します。 | 御意見に記載の項目毎に以下のとおり回答いたします。<br>（意見6について）<br>御意見の内容は新基準適用のタイミングや経過措置について、重要な観点と認識しております。既にISMAP等クラウドサービスリストに登録されているクラウドサービス事業者、新規で登録を予定されているクラウドサービス事業者、監査機関等、関係者の御意見を踏まえながら慎重に検討を進めて参ります。<br><br>（意見7について）<br>現行制度において、他の認証制度の活用については、他の認証制度における統制内容と共通する部分が一定程度あるものの、準拠している基準、監査・審査の手続き、監査人の要件等が異なり、ISMAPが求めるセキュリティ水準を満たしていることを客観的に担保することが難しいなど、困難な面がございますが、御意見を踏まえ、引き続き検討を進めて参ります。<br>また、ISMAP制度の抜本的な見直しとして、SaaS事業者を対象に、他の認証制度の活用等を通じてクラウドサービス事業者の負担を軽減する新たな枠組みを検討中です。 | 企業 |
| 33 | １．文書について<br>4.6.2.1 組織は、以下を決定し、その結果の証拠として文書化した情報を利用可能な状態とするとともに、情報セキュリティパフォーマンス及び情報セキュリティマネジメントの有効性を継続的に評価する。[27001-9.1]<br>4.6.2.7 組織は、監査プログラムの実施及び監査結果の証拠として、文書化した情報を利用可能な状態にする。[27001-9.2.2]<br>4.6.3.4 組織は、マネジメントレビューの結果の証拠として文書化した情報を利用可能な状態にする。[27001-9.3]<br>・マネジメントレビューの結果は次回のマネジメントレビューに活用されるため、実施内容と結果が分かるように具体的に記録する。<br><br>4.7.1.7 組織は、是正処置の証跡として、以下の文書化した情報を利用可能な状態にする。[27001-10.2f) / 10.2g)]<br>・不適合の性質及びそれに対して講じたあらゆる処置<br>・是正処置の結果<br>意見：誰がどういう方法で利用可能にするかが不明確<br>利用＝閲覧？参照？<br>4.8.2 に沿っていると記述したほうが良い。<br>なお、文書を明確にデジタル化するように記載したほうがいいのではないか？<br>－－－－－－－－－－－－－－－－－<br>２．利害関係者の定義<br>4.6.3.2 トップマネジメントは、マネジメントレビューにおいて、以下を考慮する。[27001-9.3.2]<br>・前回までのマネジメントレビューの結果講じた処置の状況<br>・情報セキュリティマネジメントに関連する外部及び内部の課題の変化<br>・情報セキュリティマネジメントに関連する利害関係者のニーズ及び期待の変化<br>意見：利害関係者とは？<br>顧客、自社のサプライチェーンなど、定義可能ではないか？<br>－－－－－－－－－－－－－－－－－－－－－－<br>３．ガイドライン策定について（全般）<br>ガイドラインの策定、事前確認の枠組みの導入〕<br>・ 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<br>・対象外とした統制目標及び詳細管理策、手引き<br>意見：従来は当事者以外にISMAPの管理策がどのような内容か不明であり、政府情報システム関係者とクラウド事業者間のクローズドになっていた。実際に各事業者がどのような詳細管理策をとっているかは、非公開で良いと思うが管理基準そのままでなくともガイドラインとして公開することは、日本企業の情報セキュリティ監査の底上げを図る目的では有効と思う。 | 御意見に記載の項目毎に以下のとおり回答いたします。<br>（１．文書について）<br>御意見の内容につきましては、情報セキュリティ管理基準における記載内容に準拠していることによるものであり、ISMAP管理基準改定案の策定方針に従って原案のとおりとします。御指摘いただいている懸念事項につきましてはガイドライン等にて説明することを検討しています。<br><br>（２．利害関係者の定義について）<br>御意見の内容につきましては、情報セキュリティ管理基準における記載内容に準拠していることによるものであり、ISMAP管理基準改定案の策定方針に従って原案のとおりとします。御指摘いただいている懸念事項につきましてはガイドライン等にて説明することを検討しています。<br><br>（３．ガイドライン策定について（全般）について）<br>各事業者の詳細管理策は機密性の高い情報を含むため、公開については慎重に検討を進めて参ります。 | 企業 |
| 34 | [コメント-1]<br>精緻な資料、特に”【新→旧】管理策基準”についてはCSP側の今後の対応に非常に有益です。ありがとうございます。<br>一方、この対照表だけですと、本制度改正の目的の一つである、工数の削減にはつなげるのがCSPにとって困難とも捉えられることもあり、予定されているガイドラインが非常に重要になります。<br>ガイドラインにおいては、どのようにして、工数削減ができるのかを、読み取れるような、もしくはヒントとなるような記載をお願いします。CSPとしては、ガイドラインが公開されてから、実際の対応作業が開始となるかと思います。ガイドライン公開時期のスケジュールや関連情報等の、積極的な展開をお願いします。<br><br>[コメント-2]<br>ISO/IEC27002 の日本語訳となっているJIS Q 27002ですが、現在のIT業界からみると明らかに誤訳とみれる表現が散見されます。そのうちの一つとしては、ISOの原典では”identity”となっているものが、JIS Q では、”識別”とされていることです。JIS Q に対し、改善を申し入れましたが修正される見込みはなく、英語原典を参照するようにとのことでした。<br>JIS Q 27002をベースとしているISMAP管理基準ですので、管理基準の解説においてこの点の補足、それが無理であればガイドラインにおいて、”英語原典を参照すること”を記載いただけないでしょうか。誤解にもとづく解釈、監査実務が行われるのは、特に外資企業にとっては、混乱する可能性があります。 | 御意見に記載の項目毎に以下のとおり回答いたします。<br>（[コメント-1]について）<br>御意見の内容は新基準適用のタイミングや経過措置について、重要な観点と認識しております。既にISMAP等クラウドサービスリストに登録されているクラウドサービス事業者、新規で登録を予定されているクラウドサービス事業者、監査機関等、関係者の御意見を踏まえながら慎重に検討を進めて参ります。<br><br>（[コメント-2]について）<br>ISMAP管理基準改定案で用いている用語について、ガイドライン等にて公表することを検討しています。 | 企業 |

| 連番 | 提出意見／電子ファイル | 御意見に対する回答 | 提出者 |
|---|---|---|---|
| 35 | 今後のISMAP制度につきましては、以下要件を含めて頂きますようご検討をお願い申し上げます。<br><br>1．現在ISMAP制度でのクラウド事業者が受けるアセスメント実施期間のサイクルは1年おきとなっております。現状の年次評価のサイクルから3年おきに変更して頂きたいと以前弊社よりご提案させて頂いたかと存じます。ISMAP監査最終報告書の提出期限を現状の監査完了直後約2カ月以内ではなく、少なくとも6カ月間に延長すること、およびクラウド事業者が監査サイクルを柔軟に管理できる制度を導入することを改めてお願いしたいと考えております。<br><br>2. ISMAPをリスクベースのアプローチに改革し、SOC2やISO 27000シリーズなどの国際的に認知された標準に合わせること。共通の管理項目について第三者監査結果の提出を許可し、国の固有の逸脱を明確に指定すること。<br>本審査および更新審査のアセスメントにつきましては、、現在IPAの審査レビュー期間に通常6か月以上の時間がかかっております。弊社としましては、IPAの審査レビューに大変感謝しているところですが、IPAの審査レビューの期間短縮のために、弊社として協力できることとして、弊社統制関連資料の提供およびIPAの審査中にクラウド事業者と直接コンタクトできるような仕組み作りを許可していただきたいと考えています。そのようなIPAおよびクラウド事業者の相互関与および協業の頻度を増すことにより、IPAの審査レビュー期間の最適化をご検討頂きたいと考えております。<br><br>先月ISMAP新管理基準の発表の中で、事前確認制度の取り組みがございました。ISMAP関連の各種アセスメントおよび審査前に各種詳細管理策およびエビデンスについてIPA、認証監査機関、クラウド事業者が事前確認できる制度であり、こちら新制度につきましては、弊社も賛同しております。このような仕組みは、上記でも提案した審査レビューの短縮につながる制度・活動になると思います。<br>現在、来年1月以降、ISMAP新管理基準が正式に公開される予定であると認識しております。またより詳細なISMAP新管理策の手引き及び採用ルールなどを含む新しいガイドラインも発表される理解です。来年以降発表されるガイドラインにある手続き・ルールの明示化および明文化を頂く状況にもよると思いますが、弊社としましては、ISMAP新管理策を導入するための準備可能な移行期間を頂きたいと考えています。来年1月以降の正式な新管理基準およびガイドラインによっては、新管理策導入・構築に想定以上の工数・時間が発生することを鑑みて頂き、十分な移行期間を設定いただきたいと考えております。<br><br>質問1<br>先月は発表されましたISMAP新管理策および説明資料では、詳細管理策数が見た目の数字上は、大幅に削減されておりました。しかしながら、「ISMAP管理基準_別表 新旧対照表」を見た限り、各種詳細管理策に紐づく手引きの要件および対応する情報セキュリティ管理基準（令和７年版）にある管理策数を数えますと、総じて管理策要件項目の総数は、むしろ増加していると思われます。<br>その中でも、「ISMAP管理基準_別表 新旧対照表」にある新詳細管理策（3桁）の手引きに紐づく要件項目に該当する旧4桁管理策が記されているものは、理解ができますが、旧4桁管理策が記されていない要件項目については、情報が全くないため把握ができない状態です。可能でしたら、旧管理策16章分にあるセキュリティ分野のどの章・分野に該当するかをご教示頂きますようお願いいたします。<br>現在のISMAP基準の旧章に対応する管理ガイダンスからのすべての新しい項目について明確にしたいと考えています。この明確化は、CSPが主要な管理を理解し、評価中のISMAP委員会およびIPAとのコミュニケーションに役立つと信じています。<br><br>質問2<br>先月発表されたISMAP新管理基準に含まれる「ISMAP管理基準_別表 新旧対照表」には、主に9章にあるJIS Q 2017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策および手引きが一切情報公開されておりません。出来ましたら、JIS Q 2017:2016 (ISO/IEC 27017:2015)を参照して作成した管理策および手引きにつきまして、情報開示を早めにご周知頂きますようお願い申し上げます。<br>公共部門におけるクラウド導入の加速は、経済全体のDXを促進し、日本の将来の成長潜在力を解き放つために不可欠です。これに沿って日本政府に対し、ISMAPスキームの負担を軽減することにより、具体的な利益を確保するよう丁重に要請します。現在のISMAPをベストプラクティスに合わせることで改革することにより、競争を強化し、日本の国内クラウドエコシステムを深化させ、セキュリティコストを削減しながらセキュリティ成果を向上させるのに役立つでしょう。 | 御意見に記載の項目毎に以下のとおり回答いたします。<br>（項番1.について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、登録申請に関する手続きにつきましては、検討中であるところ、御意見として承ります。<br><br>（項番2.について）<br>現行制度において、他の認証制度の活用については、他の認証制度における統制内容と共通する部分が一定程度あるものの、準拠している基準、監査・審査の手続き、監査人の要件等が異なり、ISMAPが求めるセキュリティ水準を満たしていることを客観的に担保することが難しいなど、困難な面がございますが、御意見を踏まえ、引き続き検討を進めて参ります。<br>また、ISMAP制度の抜本的な見直しとして、SaaS事業者を対象に、他の認証制度の活用等を通じてクラウドサービス事業者の負担を軽減する新たな枠組みを検討中です。<br>IPAの審査レビュー期間の最適化については、今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承ります。<br><br>（IPAの審査レビュー期間について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、登録申請に関する手続きにつきましては、検討中であるところ、御意見として承ります。<br><br>（事前確認制度について）<br>事前確認の枠組みは、手戻りや、想定されるリスクに応じて統制目標に対応する詳細管理策を選択するのではなく実態としてそれ以上に詳細管理策を選択すること等を抑止するために検討しています。目的に照らし事前確認による負荷が増加することがないよう、事前確認の枠組みの検討を進めて参ります。<br><br>（移行期間について）<br>御意見の内容は新基準適用のタイミングや経過措置について、重要な観点と認識しております。既にISMAP等クラウドサービスリストに登録されているクラウドサービス事業者、新規で登録を予定されているクラウドサービス事業者、監査機関等、関係者の御意見を踏まえながら慎重に検討を進めて参ります。<br><br>（質問1について）<br>ISMAP管理基準改定案及び新旧対照表は、ISMAPポータルの請求フォームから資料請求できるページを、年内に公開予定です。<br>なお、請求に当たり以下のJIS規格の購入が必要です。<br>JIS Q 27017:2016 (ISO/IEC 27017:2015)<br>JIS Q 27014:2015 (ISO/IEC 27014:2013)<br><br>（質問2について）<br>ISMAP管理基準改定案及び新旧対照表は、ISMAPポータルの請求フォームから資料請求できるページを、年内に公開予定です。<br>なお、請求に当たり以下のJIS規格の購入が必要です。<br>JIS Q 27017:2016 (ISO/IEC 27017:2015)<br>JIS Q 27014:2015 (ISO/IEC 27014:2013)<br><br>（ISMAPスキームについて）<br>ISMAP管理基準改定案において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することによって、詳細管理策の数を削減しているほか、想定されるリスクに応じて統制目標に対応する詳細管理策を選択するのではなく実態としてそれ以上に詳細管理策を選択すること等への対応を行っています。これにより、一定程度の負担軽減は図れるものと考えています。<br>また、ISMAP制度の抜本的な見直しとして、SaaS事業者を対象とする負担を軽減した新たな枠組みを検討中です。<br>その他、負担軽減策等については、引き続き検討を進めて参ります。 | 企業 |
| 36 | 国家サイバー統括室、デジタル庁、総務省、経済産業省に対して「ISMAP管理基準（案）」（以下、「改定案」）に関する意見を提出する機会が得られたことに感謝します。<br>我々は、日本政府が行政機関全体における安全なクラウドサービスの導入を推進し、ISMAP制度改善において関係者との対話を重ね、継続的な取り組みをしていることを高く評価しています。政府が本制度の見直しに取り組む中で、以下の提言が課題の解決と公共部門におけるクラウドのさらなる導入促進に寄与することを期待しております。<br><br>[改定された詳細管理策を明確化し、理解を促進すること]<br>詳細管理策の項目数を1,163項目から322項目に削減した改定案を我々は歓迎します。この簡素化は、制度の明確性と運用効率の向上に向けた前向きな一歩です。一方で、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クラウドサービスプロバイダー（CSP）が実施すべきことを求める要件は、一定の曖昧さを生じさせる可能性があります。改定案では、詳細管理策については、「リスク分析の結果、合理的な適用が不可能もしくは不要」と判断した場合、対象外とすることができるとしています。さらに、将来的にガイドラインを策定し、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、CSPが個別管理策を手引き から選択する場合の考え方や例示等を解説すると述べています。<br>これまでISMAPにおけるリスクベース・アプローチでの審査実績が乏しいことに鑑み、ガイドラインや実際の審査における運用基準の明確な設計が不可欠であると我々は考えます。例えば、従来記載されていた項目（改定案においては省略または統合された項目）が審査時に引き続き考慮されるかどうかは不明瞭なままです。改定案では従来の項目が手引きに移され、詳細管理策が依然として監査基準として満たされる必要があるようにも見えます。（２）もしそうであれば、現行と同様の監査作業が必要となります。 今回の改定は、事業者の負担軽減を目的としていると我々は理解しております。改定の趣旨に沿い、改定案を修正し、手引きに記載された項目が監査を要する義務ではなく、参考情報であることを明記するよう求めます。<br>また、ISMAP標準監査手続　に記載されている監査における証跡サンプル提出に関する明確な運用指針を策定することを求めます。(3) これらの点を明確化することで、制度実施において一貫性が保たれ、混乱を避けることができます。 | 御意見に記載の項目毎に以下のとおり回答いたします。<br>（[改定された詳細管理策を明確化し、理解を促進すること]について）<br>ISMAP管理基準改定案において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することによって、詳細管理策の数を削減しているほか、想定されるリスクに応じて統制目標に対応する詳細管理策を選択するのではなく実態としてそれ以上に詳細管理策を選択すること等への対応を行っています。これにより、一定程度の負担軽減は図れるものと考えています。<br>監査は、クラウドサービス事業者が言明した管理策に対して行うことを想定しているところ、御意見を踏まえ、「ガイドライン」の策定及び言明した管理策への監査上の取り扱いについて検討を進めて参ります。<br><br>（監査における証跡サンプル提出について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見の内容につきましては、検討中であるところ、御意見として承ります。 | 団体 |

| 連番 | 提出意見／電子ファイル | 御意見に対する回答 | 提出者 |
|---|---|---|---|
| (36の続き) | 我々は、制度運用開始までに制度官庁、審査機関、監査機関、CSP間で集中的な議論をすることを推奨します。議論においては以下を目的とすべきです。<br>・適切なリスク判断に資する知見を共有できる仕組みの構築<br>・審査機関の能力強化<br>・運用基準を踏まえたCSPの内部体制構築の支援<br>・継続的な改善を可能とする仕組みの構築<br><br>また、ガイドラインにおいては、提示された事例が「参考例」であって「規定事項」ではないこと、ならびにCSPとその顧客がそれぞれの具体的な目的に応じて適切な管理策を柔軟に選択できることを明確にすることが重要です。さらに、現行のISMAPではAIサービスの評価体制が未整備である状況を踏まえ、今後策定されるAIサービス及びサブサービスに関する言明要件が、AIサービスの利用実態に即したものであるようにすることを推奨します。ガイドライン、その他のISMAP規程の公開時期は検討中とのことですが、改定管理基準の適用開始時期含め、大まかなスケジュールを提示することを求めます。関係者との協議、および組織内準備の時間を確保するためには、手引き・ガイドラインの最終版の公開から適用開始まで十分な準備猶予期間を設けることを推奨します。<br><br>[事前確認の枠組みを必須としないこと]<br>改定案においては、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が提案されています。この制度の利用が任意である場合は有用な枠組みとなりますが、一方で利用が実質的に必須となる場合は、審査機関やCSP双方にとって過度な負担となり、審査コスト増加と審査プロセスの長期化に繋がるリスクがあります。そのため、この枠組みの利用は任意であることを明示することを推奨します。<br><br>[国際的に認められた規格を積極的に活用すること]<br>内閣府より2025年6月に公表された「規制改革実施計画」（以下、「本計画」）　では、「他の認証制度を取得している場合には、該当の認証制度を活用し、監査項目を削減するなど、監査負担を軽減する方向で、ISMAP管理基準等を改定する」と明記されています。内閣府が既存の認証の有用性を認識していることを我々は歓迎します。既存の認証は、サービスがユーザーのリスク管理ニーズを満たすことを保証することに加え、競争を促進し、政府機関が民間のイノベーションに遅れを取らないようにする上でも役立ちます。最近開催されたISMAP制度改善の説明会においては、他の認証制度の活用については、監査枠組みにおいて反映される可能性があることが説明されました。本計画の確実な実施のためにも、ISO 27000シリーズやSOC 2等、CSPが取得した証跡の再利用の仕方に関して、関係者と十分な協議を行うことを推奨します。これらの認証を認め、重複する手続きをなくすことで、政府とCSP双方の負担が軽減されます。<br><br>クラウドセキュリティを世界的に強化する上で、同志国が適用可能な部分を相互に認め合う、相互認証制度の採用を推奨します（例：日本のISMAPと米国のFedRAMP）。このようなアプローチにより、サイバーセキュリティとレジリエンスを広く向上させ、国際協力をさらに深め、政府機関が高度かつ最も安全なサービスへアクセスすることが可能となります。<br><br>[結論]<br>我々の提言をご検討頂けることに感謝します。今後のISMAP改善に関する議論に寄与できることを我々は期待しております。今回の意見に関し、ご質問や詳細な協議のご希望があれば、ぜひお知らせください。<br><br>[注釈I]<br>（1）「手引き」に記載されている項目についての取り扱いが明確ではなく、仮に、「手引き」に記載されている項目も、監査で必須とされるのであれば、運用上は事業者の負担は軽減しないこととなります。仮に、改正前のＢ項目以外の項目も必須とされるのであれば、監査対象となる項目は増大することになります。<br>（2）４桁管理策が「手引き」に移されたことで、運用状況を評価するランダムサンプリングをどのように考えるべきなのか明確となっていません。改定後は、運用状況評価ランダムサンプリングの対象は別表３の管理策基準についてとするのか、あるいは、参考２の「手引き」に記載された項目についても対象とするのかを明確化することは、理解に役立ちます。） | （制度運用開始までの議論について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見の内容につきましては、検討中であるところ、御意見として承ります。<br><br>（ガイドラインについて）<br>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しています。<br>御意見も踏まえ、利用者が政府機関等であるという前提ではありますが、できる限りクラウドサービス事業者の判断を尊重できるよう、ガイドラインの内容について、検討を進めて参ります。<br><br>（AIサービスについて）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、登録申請に関する手続きにつきましては、検討中であるところ、御意見として承ります。<br><br>（準備猶予期間について）<br>御意見の内容は新基準適用のタイミングや経過措置について、重要な観点と認識しております。既にISMAP等クラウドサービスリストに登録されているクラウドサービス事業者、新規で登録を予定されているクラウドサービス事業者、監査機関等、関係者の御意見を踏まえながら慎重に検討を進めて参ります。<br><br>（[事前確認の枠組みを必須としないこと]について）<br>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しています。<br>事前確認による負荷が増加することがないよう、御意見も踏まえ、事前確認の枠組みの検討を進めて参ります。<br><br>（[国際的に認められた規格を積極的に活用すること]について）<br>現行制度において、他の認証制度の活用については、他の認証制度における統制内容と共通する部分が一定程度あるものの、準拠している基準、監査・審査の手続き、監査人の要件等が異なり、ISMAPが求めるセキュリティ水準を満たしていることを客観的に担保することが難しいなど、困難な面がございますが、御意見を踏まえ、引き続き検討を進めて参ります。<br>また、ISMAP制度の抜本的な見直しとして、SaaS事業者を対象に、他の認証制度の活用等を通じてクラウドサービス事業者の負担を軽減する新たな枠組みを検討中です。<br><br>（注釈(1)について）<br>ISMAP管理基準改定案において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することによって、詳細管理策の数を削減しているほか、想定されるリスクに応じて統制目標に対応する詳細管理策を選択するのではなく実態としてそれ以上に詳細管理策を選択すること等への対応を行っています。これにより、一定程度の負担軽減は図れるものと考えています。<br>監査は、クラウドサービス事業者が言明した管理策に対して行うことを想定しているところ、御意見を踏まえ、「ガイドライン」の策定及び言明した管理策への監査上の取り扱いについて検討を進めて参ります。<br><br>（注釈(2)について）<br>ISMAP管理基準改定案において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することによって、詳細管理策の数を削減しているほか、想定されるリスクに応じて統制目標に対応する詳細管理策を選択するのではなく実態としてそれ以上に詳細管理策を選択すること等への対応を行っています。これにより、一定程度の負担軽減は図れるものと考えています。<br>監査は、クラウドサービス事業者が言明した管理策に対して行うことを想定しているところ、御意見を踏まえ、「ガイドライン」の策定及び言明した管理策への監査上の取り扱いについて検討を進めて参ります。 | 団体 |
| 37 | ○パブリックコメント1<br>ISMAP管理基準（案）全般について<br>　今回の改定は、「セキュリティ管理策の数が多く、クラウドサービス事業者にとって負担となってい」たため、「セキュリティ管理策の数を減らす見直しを実施した改正案」となっており、（「「ISMAP管理基準（案）」等に対する意見公募要領」より）「詳細管理策の数を1,163項目から322項目に削減」したものである。（「【参考】ISMAP管理基準の改定について（案）」より）<br>　しかし、「【参考】ISMAP管理基準の改定について（案）」のP3では、「監査においては手引きを参考に監査を実施」とあり、手引きには詳細管理策を実施するための細かい基準がしめされているため、手引きの項目数を勘案すると実質的な詳細管理策の項目数の削減は行われていないのではないか。<br>　そこで、今回の改定による事業者の負担軽減を明確にするため、監査にかかる負荷（工数や費用等）がどれくらい軽減すると想定されるか、例示でも良いので改正前との比較を数字でお示し願いたい。 | ISMAP管理基準改定案において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することによって、詳細管理策の数を削減しているほか、想定されるリスクに応じて統制目標に対応する詳細管理策を選択するのではなく実態としてそれ以上に詳細管理策を選択すること等への対応を行っています。これにより、一定程度の負担軽減は図れるものと考えています。<br>監査は、クラウドサービス事業者が言明した管理策に対して行うことを想定しているところ、御意見を踏まえ、「ガイドライン」の策定及び言明した管理策への監査上の取り扱いについて検討を進めて参ります。<br>監査にかかる負荷（工数や費用等）については、言明した管理策に対して監査を行うためにクラウドサービス事業者と監査機関での契約により決まるものとなりますので、制度として数字でお示しすることは困難です。 | 団体 |
| 38 | ○パブリックコメント2<br>ISMAP管理基準(案）全体について<br>　ISMAPは、「政府機関等がクラウドサービスを調達する際は、原則、ISMAPクラウドサービスリスト又はISMAP-LIUクラウドサービスリスト）から調達する」ために設けられた制度であるが、地方自治体の調達などでもISMAPの取得を前提としたガイドラインが設けられるなど、実際は適用される範囲が本来の目的を超えて拡大されている。<br>【例：地方公共団体における情報セキュリティポリシーに関するガイドライン(総務省：令和７年３月版）III-31　図表23 機密性の分類、分類基準の例示　中に「ISMAP登録サービスは利用可」】<br>　政府調達と地方自治体の調達を比較すると調達額や要求される非機能要件などが大きく異なっていることから、ISMAPの適用を拡大を認めるのであれば、SaaSサービスでISMAP-LIUの制度を創設したようにIaaSやPaaSにおいても管理策基準を緩和した制度の検討をお願いしたい。（ISMAP-LIGHT(仮称））<br>　これにより、政府機関等のために設けたISMAPの制度を、セキュリティレベルが異なる地方自治体も利用することができ、公共分野においてISMAPが統一感や柔軟性をもった制度になることが期待できる。<br>　あわせて、緩和した制度の検討が難しいのであれば、「ISMAPは政府機関等のために設けた制度であり、地方自治体への適用は認めない」など、適用範囲を明確化する記述をいれるようお願いしたい。 | 今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承ります。 | 団体 |

| 連番 | 提出意見／電子ファイル | 御意見に対する回答 | 提出者 |
|---|---|---|---|
| 39 | ○パブリックコメント3<br>ISMAP管理基準(案）全体について<br>　今回の見直しは、「セキュリティ管理策の数が多く、クラウドサービス事業者にとって負担となってい」たため、「セキュリティ管理策の数を減らす見直しを実施した改正案」となっており、（「「ISMAP管理基準（案）」等に対する意見公募要領」より）「詳細管理策の数を1,163項目から322項目に削減」したものである。（「【参考】ISMAP管理基準の改定について（案）」より）<br>　この見直しは、内閣府の「規制改革推進に関する中間答申（令和６年12月25日：規制改革推進会議）」の中の「イ 政府が調達するクラウドサービスにおけるスタートアップ等の参入促進（セキュリティ評価制度（ＩＳＭＡＰ）等の見直し）」にある「監査に係る項目が約1,200項目と多数に上ることによって、クラウドサービス事業者（以下「事業者」という。）によるＩＳＭＡＰ登録・更新申請に係る監査費用（以下「監査費用」という。）が高額となり、登録までの期間も長期化しているとの指摘」（Ｐ３６）に答えたものであり一定の評価ができる。<br>　しかし、今回の改定案では同答申中の「国際標準化機構（ＩＳＯ）/国際電気標準会議（ＩＥＣ）２７０００シリーズ等、他の認証制度を取得している場合には、該当の認証制度を活用」して、「監査負担を軽減する方向で、「ＩＳＭＡＰ管理基準」（令和２年６月３日ＩＳＭＡＰ運営委員会）等を改訂」（同：Ｐ３６）については全く触れられていない。<br>　そこで、ISO27000シリーズ等の活用として、当該制度の証跡流用に関する明確な記述をお示し願いたい。<br>　また、検討中であれば今後のスケジュールをお示し願いしたい。 | 現行制度において、他の認証制度の活用については、他の認証制度における統制内容と共通する部分が一定程度あるものの、準拠している基準、監査・審査の手続き、監査人の要件等が異なり、ISMAPが求めるセキュリティ水準を満たしていることを客観的に担保することが難しいなど、困難な面がございますが、御意見を踏まえ、引き続き検討を進めて参ります。<br>また、ISMAP制度の抜本的な見直しとして、SaaS事業者を対象に、他の認証制度の活用等を通じてクラウドサービス事業者の負担を軽減する新たな枠組みをスケジュールも含め検討中です。 | 団体 |
| 40 | 2.2.2 言明の対象範囲に関して、<br>”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。”とある。<br><br>用語として、クラウドサービスとそのサービス以下のサービスが混在するため、基準として名称及び位置付けを区別（慣習的にはサブサービス、と言う用語を使用されていると認識している）してはどうか。<br><br>また、現時点の記述では、”言明の対象外となるサービス”の指す意味が、対象事業者が提供するサービス（例えばAWSと言うサービスの中で提供されるAmazon EC2）と基盤としての他サービスを利用（例えばSaaSが基盤としてAWSを利用）が混在するようにも受け取れるのでこちらも明確に区別することが良いのではないか。<br><br>質問の背景として、サービスの粒度はCSPにより異なり、また、クラウドサービスの特性として従来のサービスに比べて多くのサービスが発展的にアップデート、追加されることになる。従来のISMAPの課題として、こうしたサービスの追加が年次の監査および登録更新を経なければ顧客が実質的に選択できないという点がある。（例えばセキュリティの向上に資するサービスが年次監査の終了時に発表されても、ISMAP登録外を理由に利用者が選択を取りやめるケースがあるのは、制度の期待する目的に沿わないと考えられる）<br>ISMAPにおけるサービスはあくまでも個々の上記で言うところのサブサービスではなく、統制の同質性を前提とした登録サービス全体であり、サブサービスは監査において確認した範囲となる。顧客が統制の同質性をCSPが適切に説明責任を果たすことを前提に、新たなサービスを時宜を逸せず不都合なく選択できる制度に改善することを期待している。 | ISMAP管理基準改定案で用いている用語について、ガイドライン等にて公表することを検討しています。<br>なお、言明の対象外となるサービスの意味につきまして、統制を引き継げることを目的として規定をしており、統制の引継ぎについては現行のISMAP管理基準及びISMAP管理基準ガイドブック等にて解説がされております。また、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について「ガイドライン」を規程として、策定・公表することを検討しておりますため、ガイドライン策定時に検討を進めることとし、原案のとおりとします。<br>その他御意見につきましては、今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承ります。 | 企業 |
| 41 | コメント(1)<br>各管理策の採否について回答する際に、採否に加え第三の選択肢として、いわゆる「N/A」すなわち「該当しない」も項目に応じ選択できるよう、検討をお願いいたします。<br>例として<br>・14.2.7 組織は、外部委託したシステム開発活動を監督し、監視する。<br>といった管理策をあげます。<br>外部委託したシステム開発活動がない組織では外部委託がないので、監督や監視を行いません。これによって採否を否にしますと、「基本言明要件のうち実施している統制目標の管理策」で統制を実施していないものと扱われます。<br>とはいえ、「していないことを実施したとして」採にすることも、論理上・実務上できません。このような成り行きでISMAPの監査で時間・手間を要することがございました。<br><br>- パブリッククラウドに基盤を置く事業者/自社DCに基盤を置く事業者<br>- 各サービス提供者の対象とする事業の性格（基盤寄りかサービス寄りか）<br>によって、主観ですが、当社と異なる構成・事業の性格を主な対象にしたものであろうと想像する管理策もございます。<br><br>サービスを利用される官公庁様、審査される監査法人、サービスを提供する事業者、いずれにとっても「該当しない」がないことは負担であると存じます。このことから採否に加え「該当しない」の選択肢も設けていただくよう、お願いいたします。<br>（「該当しない」が本当にそうであるかは、監査の過程で検証される事項と存じます）<br><br>コメント(2)<br>※ISMAP管理基準、とは別の事柄かもしれませんが、事業者から申し上げることのできる機会ですので記載いたします。<br>現状、官公庁にクラウドサービスを提供する際<br>- ISMAP（ISMAP-LIU含む）<br>- 政府機関等のサイバーセキュリティ対策のための統一基準群（以下、統一基準群）<br>両方への準拠が求められていると理解しています。クラウドサービス事業者が類似・重複する制度の両方へ対応するコストについて、削減方途を検討いただきたいと存じます。<br>当社が官公庁へのクラウドサービス提供を進める際、片方への対応をしていると提示した際に、もう一方の判断基準を満たしていないと指摘を受けるケースがありました。<br><br>ISMAPは「統一基準群」を外部クラウド事業者にも適用できるように発展させた制度と捉えております。上記のような指摘を受けるケースがある現状では、クラウドサービス提供者は同一の事項について、双方の制度を個別に準拠しているかどうか判断する二度手間が発生しています。<br><br>このようなことはできる限り避けたく、制度の有効活用、例えば、ISMAPのある管理策を採用としている場合、統一基準群のある基準は満たしていると見なす、など二度手間が減るよう基準の運用を検討いただきたいと存じます。 | 御意見に記載の項目毎に以下のとおり回答いたします。<br>（コメント(1)について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見の内容につきましては、検討中であるところ、今後の改定における参考とさせていただきます。<br><br>（コメント(2)について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承ります。 | 企業 |

| 連番 | 提出意見／電子ファイル | 御意見に対する回答 | 提出者 |
|---|---|---|---|
| 42 | 「ISMAP管理基準」<br>＜別表2 マネジメント基準＞<br>・JIS Q 27001：2023を基にしているのであれば、JIS Q 27001：2023に新たに追加された「6.3 変更の計画策定」もISMAP管理基準に含めたほうが良いのではないでしょうか。たとえば、4.5.4.3 に追加する等が考えられるかと思います。<br>＜別表3 管理策基準＞<br>5.31.3<br>・「国内法以外の法令及び規制」は「国外の法令・規制」で良いのではないでしょうか。<br>・「外部委託先を選定し」の「外部委託先」は唐突感があり何を指しているかが不明瞭です。外部のプロバイダー、外部のベンダー等の表現が良いのではないでしょうか。<br>・5.31.3の手引きの内容は、管理策の内容を繰り返しているだけでクラウドサービス事業者にとって参考情報にしがたいものだと感じましたので、以下のように具体化してはいかがでしょうか。<br>（手引き案）<br>当該事業者が提供するサービス上で取り扱われる情報に対して、国外の法令及び規制が適用され、意図しないアクセスや処理が行われるリスクを管理するため、次の事項を考慮する。<br>a)サービスがどの国の外部プロバイダーを利用しているかを明示<br>b)外部プロバイダーのデータセンター所在地、準拠法など、法的リスクに関する評価結果を要約して顧客へ提供<br>c)顧客のデータが保管・処理されるデータセンターの国、地域、および都市を公開<br>d)サービス利用規約や契約書に、契約の準拠法と裁判管轄を明記し、法的紛争の解決方法を明確化<br>・以下の管理策基準について、手引きが「特になし」となっていますが、管理策基準のみではクラウドサービス事業者が対応方針や具体的な対策の検討をする際に、管理策の理解に認識齟齬が生まれる可能性があると考えますので、以下に一部、手引き案を提示します。<br>5.3.2、5.12.2、5.19.1、5.32.2、8.13.5、8.22.3、8.24.3、8.24.4、8.24.5、8.26.2、9.1.1、9.2.1、9.2.3、9.3.1、9.3.2、9.3.3、9.3.4、9.5.1、9.6.2、9.6.3、9.6.4、9.7.1、9.7.2<br>---------<br>5.3.2<br>（手引き案）<br>情報セキュリティを確保するため、以下の原則に従い役割を分離する。<br>a)自己承認の禁止<br>b)承認フローの確立<br>c)監査の独立性を確保<br>自身で申請した内容（アカウント作成、権限変更、システム設定変更など）は、申請者とは別の責任者や管理者（例: 部門長、情報システム担当者）が申請内容を客観的に評価し許可する。<br>また、自身が担当する業務やシステムを自分で監査できないようにする。監査は、実際の業務担当部署から独立した部門（例: 監査部）または外部の専門家が行う。<br>5.12.2<br>（手引き案）情報分類を常に最新に保つため、システムやサービス上で取り扱われる情報資産について、その価値や重要性の変化に応じて、定期的なレビュープロセスを確立し、新しい法令が施行された場合など、特定の事象が発生した際には、分類基準を見直す。<br>5.19.1<br>（手引き案）クラウドサービス事業者の提供するサービス品質とセキュリティを維持するため、次の事項を考慮する。<br>a)サービスを構成する外部の製品やサービス（IaaS、PaaS、SaaSなど）を選定する際のセキュリティ要件を定義<br>b)外部の製品やサービスとの契約書に、情報セキュリティに関する具体的な義務を明記<br>c)策定した方針は、社内外の関連するすべての利害関係者（営業、開発、法務、供給者）へ伝達<br>8.13.5<br>（手引き案）クラウドサービス利用者の資産（バックアップを含む）を保護するため、BYOK機能を提供する場合、次の事項を考慮する。<br>a)クラウドサービス利用者が生成・管理する暗号鍵をサービスに持ち込める機能の提供<br>b)クラウドサービス利用者が自社で鍵の生成、保管、ローテーション、消去を行えるような技術的なインターフェースやAPIの整備<br>c)サービス利用規約において、暗号鍵の管理責任がクラウドサービス利用者にあることを明確に記載<br><br>BYOK機能の提供が難しい場合、クラウドサービス利用者が独自で暗号化と鍵管理を実装できるよう、次の事項を考慮し、必要な情報を提供する。<br>a)クラウドサービス利用者がデータをアップロードする前に、自社で暗号化を行えるよう、暗号化アルゴリズムやプロトコルに関する技術仕様を公開<br>b)顧客がスムーズに暗号化機能を実装できるよう、詳細な開発者向けドキュメントやSDK（ソフトウェア開発キット）を提供<br><br>8.24.3<br>（手引き案）クラウドサービス事業者が暗号や電子署名を利用する場合、あるいはシステムの新規構築や更新に伴い、暗号化又は電子署名を導入する場合において、システムで使用するアルゴリズム及び鍵長並びにそれらを利用した安全なプロトコルを、「電子政府推奨暗号リスト」に基づき定める。 | 御意見に記載の項目毎に以下のとおり回答いたします。<br>（JIS Q 27001:2023の6.3について）<br>情報セキュリティ管理基準（令和7年改正版）を構成するマネジメント基準において、6.3に相当する内容が明示的に規定されていないことからISMAP管理基準改定案においてもこれに準拠しております。御意見の内容は今後の改定における参考とさせていただきます。<br><br>（管理策基準5.31.3について）<br>御意見で御指摘いただいているいずれの表記とも、政府統一基準に由来するものであり、政府統一基準にて遵守を求めている事項であることから、原案のとおりとします。<br><br>（管理策基準5.31.3の手引きの内容について）<br>御意見の内容につきましては、情報セキュリティ管理基準における記載内容に準拠していることによるものであり、ISMAP管理基準改定案の策定方針に従って原案のとおりとします。<br><br>（手引きが「特になし」となっている項目について）<br>詳細管理策の採用にあたっての手引きに記載内容への対応方法については、管理基準のみでは判断しかねる部分もあるかと存じますので、今後管理基準の規定内容を補足するガイドラインの策定を進めていく予定です。御提案いただいた手引き案はガイドライン策定の際の参考とさせていただきます。 | 企業 |

| 連番 | 提出意見／電子ファイル | 御意見に対する回答 | 提出者 |
|---|---|---|---|
| 43 | ISMAPパブリックコメント<br>この度は『ISMAP管理基準』の改正に際し、パブリックコメントの機会を設けていただき、ありがとうございます。<br>パブリックコメントの意見募集サイトに公開されております資料を拝見し、以下のとおり、コメントさせていただきます。<br><br>１．統制目標とその詳細管理策の記載について-その１-<br>全般的に、従前より分かりやすくなったと思います。従前のように、区分としての ３桁管理策以下に、個々の４桁管理策として独立していた状態より、２桁番号の統制目標における３桁番号での詳細管理策の要求内容は、“参考(手引き)”と組み合わせることで、より理解しやすくなったと思います。これにより、特に新規にISMAP認定を目指すCSPには、対応の整備が実施しやすくなると思われます。また、一部ではありますが、従前は、４桁管理策単体でみた場合、その必要合理性が疑問だった項目も、今回の改正で改善していると認識しました。<br><br>２．統制目標とその詳細管理策の記載について-その２-<br>従前より、ISMAP制度が求める管理策の項目量が非常に多く、且つ、原則として全項目を網羅する」ことが求められており、CSP側には大きな負担となっているものと思います。<br>今回の改正では、名言はされておりませんが、資料『【参考】ISMAP管理基準の改定について（案）』のP5において、詳細管理策数の大幅削減をアピールされていることからも、量的負担の軽減も、今回改正の目的の一つかと思料いたします。しかし、実態・実質としては、管理策基準の構成が変更され、従前４桁管理策としてあった要件が、3桁番号の詳細管理策の“参考(手引き)”に集約されている状態であり、量的負担の軽減にはなっていないと思います。したがって、資料中にある詳細管理策数の大幅削減を示すことは、量的負担軽減のミスリードに感じます。<br>また、資料『【参考】ISMAP管理基準の改定について（案）』のP7において、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旨記載がございますが、<br>同資料P4に「・・・細管理策の抽象度が上がったことから・・・」を踏まえますと、逆にCSP側における解釈の余地が拡大することから、制度側の意向に沿わず、申請後の指摘による修正・再監査等の手戻りとなることを懸念いたします。<br><br>３．個別管理策に対応する資料名記載について<br>今回、言明書の最新版が開示されておりませんので具体的詳細は不明ですが、先日の説明会において「文書名は別枠で記載する」旨の説明（口頭）があったと存じます。<br>各採用管理策に関して、その根拠・証跡となる資料は、各企業における内部統制により作成・命名されます。従って、各企業における内部統制の状況変化に応じて、適宜変更される場合があります。このような、各企業独自の要件であり、且つ、変更されることが当然発生するもの（資料名）を、（おそらく）「言明書_別添２」の記載項目とすることは、記載の手間のみならず、更新手続き時にも全量の点検・見直しを要することになるため、「言明書_別添２」の作成・維持の負荷の増加となります。<br>また、ISMAPの認定に際しては、指定機関による監査受審を必須とされており、各採用管理基準（管理策）の規程・証跡の妥当性は、監査時に確認され、監査結果報告書にて確認可能だと承知しております。したがって、「言明書_別添２」の作成・維持に対する作業負荷が増加するにもかかわらず、資料名の記載が本当に必要かについて疑問を感じます。<br><br>４．ISO/IEC規格との直接的関連性強化の希望<br>資料『【参考】ISMAP管理基準の改定について（案）』のP2において、国際規格の取り込み構成を示されています。これを踏まえ、それら認証を取得済の場合、「言明書_別添２」に示される各管理基準において、ISO認証での依拠を可能とし、「言明書_別添２」への記載、及びISMAP申請に際しての監査確認事項からの免除を希望します。<br>一方、ISMAP管理基準が、 ISO27001/27002/27017等を基礎としていながらも、それら認証に依拠できない場合、そこにISMAPとしての重視観点があるものと推察します。<br>ISMAPとしての重視観点を明確、且つ具体的に示されることにより、クラウドサービス事業者として確認・構築すべき管理策を整備することが容易になることが期待できると思います。<br><br>----------<br>※以下は、今回のパブリックコメント対象資料には直接反映されてはいないと見受けられますが、かねてより要望させていただいており、今回の改正で是非、再考・お取込みいただきたく、コメントさせていただきます。<br><br>５．用語定義の充実化について<br>従前より、制度説明会や、その際の“意見フォーム”等にて要望させていただいておりますが、ISMAP制度における各種用語の定義化の充実を希望します。一部の単語・用語ではありますが、一見“一般的用語”と思われるものでも、これまでの経験上、制度側との認識・見解が相違する場合があると実感しております。実際に、過去に単語・用語の認識相違により、申請提出後に指摘を受け、当該項目に関する管理策の見直しが必要となった状況がございます。制度として認識・見解の相違が許容できないものであれば、あらかじめ“定義”を明確に示されることを求めます。<br>現状で“用語の定義”として掲載されているものは、固有名詞的な単語であり、掲載量も少ないと考えます。<br>（例） “アプリケーション” や “アプリケーションサービス” は、クラウドサービス形態区分の IaaS/PaaS/SaaSにおいては、 SaaSが該当すると考えますが、<br>ISMAPでは、サービス形態区分によらず、全般的に要求されています。この場合、IaaSやPaaSサービスにおける“アプリケーション” や “アプリケーションサービス”とは何か、定義が必要と存じます。<br><br>６．制度関連資料の活用（再利用）性改善の希望<br>ISMAP制度関連では、様々な資料がご提供されておりますが、その多くは、PDF形式ファイルが多いと認識しております。内容次第では、Excel形式での“表”や“一覧”でご提供いただけると、CSP側におけるISMAP対応作業（統制整備）に際し、利活用・再利用の利便性向上が期待できると考え、これを希望いたします。 | 御意見に記載の項目毎に以下のとおり回答いたします。<br>（１．統制目標とその詳細管理策の記載について-その１-について）<br>御意見ありがとうございます。継続してより良い制度になるよう検討を進めて参ります。<br><br>（２．統制目標とその詳細管理策の記載について-その２-について）<br>ISMAP管理基準改定案において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することによって、詳細管理策の数を削減しているほか、想定されるリスクに応じて統制目標に対応する詳細管理策を選択するのではなく実態としてそれ以上に詳細管理策を選択すること等への対応を行っています。これにより、一定程度の負担軽減は図れるものと考えています。<br>また、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、さらにISMAP制度の抜本的な見直しとして、SaaS事業者を対象とする負担を軽減した新たな枠組みを検討中です。<br>その他、負担軽減策等については、引き続き検討を進めて参ります。<br><br>（３．個別管理策に対応する資料名記載について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承ります。<br><br>（４．ISO/IEC規格との直接的関連性強化の希望について）<br>現行制度において、他の認証制度の活用については、他の認証制度における統制内容と共通する部分が一定程度あるものの、準拠している基準、監査・審査の手続き、監査人の要件等が異なり、ISMAPが求めるセキュリティ水準を満たしていることを客観的に担保することが難しいなど、困難な面がございますが、御意見を踏まえ、引き続き検討を進めて参ります。<br>また、ISMAP制度の抜本的な見直しとして、SaaS事業者を対象に、他の認証制度の活用等を通じてクラウドサービス事業者の負担を軽減する新たな枠組みを検討中です。<br><br>（５．用語定義の充実化について）<br>ISMAP管理基準改定案で用いている用語について、ガイドライン等にて公表することを検討しています。<br><br>（６．制度関連資料の活用（再利用）性改善の希望について）<br>御指摘いただいた点については、継続的に検討を進めて参ります。 | 企業 |

| 連番 | 提出意見／電子ファイル | 御意見に対する回答 | 提出者 |
|---|---|---|---|
| (43の続き) | ７．ISMAP申請の条件とされる監査の関連・位置づけ改善の希望<br>ISMAPでは、認定の取得・継続に際し、指定機関による監査受審のうえ、監査結果報告書を制度側に提出することが定められています。しかしながら、事後、制度側より、監査結果に対し“質問”され“是正（含 再監査）”が求められる場合があります。監査会社は制度側に定められた監査基準に準じて監査を実施されていると承知しておりますが、その結果に対して“質問”にとどまらず、追加監査や再監査を求められる状況は、ISMAPにおける監査の位置づけと、その有効性について疑問を感じる場合がございます。＃CSP側には、再監査により発生する内部稼働や、監査機関支払い等の負担も増加します。<br><br><最後に><br>私どもは、ISMAP制度開始時から、本制度にご登録いただいており、これまで、制度側におかれましても、様々な改善を実施いただいているものと承知しております。<br>今回のパブリック・コメントにおきましては、様々と勝手を申し上げさせていただきましたが、今後もISMSP制度対応を安定して継続していくことを目的に、コメントいたしました。<br>ご容赦の程お願い申し上げます。<br>ISMAP認定制度の、より一層の充実と、ISMAPを要する市場拡大に、少しでも寄与できればと存じます。 | （７．ISMAP申請の条件とされる監査の関連・位置づけ改善の希望について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、ISMAP制度の監査につきましては、検討中であるところ、御意見として承ります。<br><br>（<最後に>について）<br>御意見ありがとうございます。継続してより良い制度になるよう検討を進めて参ります。 | 企業 |
| 44 | 【はじめに】<br>当社は改定案を支持しつつ、ISMAP 認証プロセスのセキュリティ成果と整合性を損なうことなく、監査人および提供者間の一貫性をさらに高めうる観点から、以下のとおり提言を申し上げます。<br><br>【ベストプラクティスの原則】<br>各国の要件を、広く採用されている国際規格に整合させることは、法域間の相互運用性を高めるうえで有益です。セキュリティ認証スキームにおけるベストプラクティスは、政府要件のコントロールの意図・成果が一致する場合に、広く採用され、かつ公的に認定された第三者審査（例: NIST SP 800-53、ISO/IEC 27001、27017、27018）による既存の認証を有効な証憑として受け入れることです。これは、ISMAP の物理セキュリティ要素において特に重要です。多くのクラウド提供者は、SaaS 事業体に該当しない施設（データセンター等）を活用しており、当該施設が追加的かつ負担の大きい監査の対象となり得るためです。<br>このアプローチを採用することで、ISMAP 認証プロセスにおける監査・評価の対象は、既存の監査でカバーされない新規要件や日本独自要件のみに限定（差分監査）されます。ばらつきと重複を低減しつつ高い保証水準を維持でき、政府機関による先進的なクラウド技術の安全な採用を加速できます。<br><br>【改定案の積極的評価点】<br>以下の点は、ISMAP の近代化に向けた先見的な姿勢を示すものです。<br>・近代化と整合性: 更新された国際規格とコントロール群を整合的に基礎に据えることで、国際的な標準策定への投資を活用し、独自解釈を減らし、既存証跡の再利用を可能にします。<br>・コントロールの精選: リスクベースで簡潔なコントロールに集約することで、堅固なセキュリティ態勢を保ちながら監査負荷を軽減できます。<br>・事前審査の導入: 監査前にスコープやリスクベース除外を検証する正式な仕組みは、ISMAP 監査プロセスの効率を実質的に高めます。<br>・統制の継承: ISMAP に掲載された基盤サービスおよびインフラからの証跡継承を認めることは、重複検証を避け、現代的な共有責任モデルを反映します。<br>・証跡収集頻度と監査期間の明確化: 例示の提示や期間の連続性の明確化は、継続的なコンプライアンスの予見可能性を高めます。<br>・暗号化消去の明確化: 暗号化消去（cryptographic erasure）の明示的受入れは、クラウドネイティブなデータ消去の実務に整合します。<br><br>【提言（明確性・予見可能性・効率性の向上）】<br>文書階層の明示: ISMAP 標準を必須文書と位置づけ、ガイドラインおよびハンドブックは実装支援（同等コントロールの許容を含む）である旨を明確化してください。<br>機械可読なコントロール一覧とクロスウォークの提供: 地域・スコープ注記・版情報を含む ISMAP コントロール一覧（API/CSV）と、旧 ISMAP コントロール、統合標準、NIST SP 800-53 へのマッピング（JSON/CSV）をご提供ください。<br>非公開部分に関する変更点一覧（差分サマリー）の公表: 例として ISO/IEC 27017 や 27014 の該当箇所について、著作権保護のある原文を開示せずとも変更点を把握できるようにしてください。<br>各コントロール・ファミリー毎の具体的な除外例の提示。<br>事前審査の標準化（枠組みおよび最短処理期間の設定例: 10 営業日）。<br>継続評価・更新におけるコントロール単位の変更履歴項目例の提示。<br>コントロール継承に関するガイダンスの精緻化: 継承範囲と残存責任を明確に伝える様式・例示の整備。<br>ISMAP 標準監査手続書の調整（グローバル実務の明確化）: 合理的保証、重要性、リスクベースのサンプリングを採用可能とし、セキュリティ成果に影響しない軽微な文書上の相違は指摘事項としない旨を明示。<br>監査期間ルールの具体例（更新、短縮期間、後発事象など）の提示。<br>暗号化消去に関する受理可能な証跡の明確化: 鍵破棄ログ、承認記録、検証結果出力、承認済みプロセスなど。<br>重要用語の二言語（日本語・英語）対訳用語集の公表。 | 御意見に記載の項目毎に以下のとおり回答いたします。<br>（【ベストプラクティスの原則】について）<br>現行制度において、他の認証制度の活用については、他の認証制度における統制内容と共通する部分が一定程度あるものの、準拠している基準、監査・審査の手続き、監査人の要件等が異なり、ISMAPが求めるセキュリティ水準を満たしていることを客観的に担保することが難しいなど、困難な面がございますが、御意見を踏まえ、引き続き検討を進めて参ります。<br>また、ISMAP制度の抜本的な見直しとして、SaaS事業者を対象に、他の認証制度の活用等を通じてクラウドサービス事業者の負担を軽減する新たな枠組みを検討中です。<br><br>（【改定案の積極的評価点】について）<br>御意見ありがとうございます。継続してより良い制度になるよう検討を進めて参ります。<br><br>（文書階層の明示について）<br>ガイドラインは規程として定義する予定で検討を進めております。<br><br>（機械可読なコントロール一覧とクロスウォークの提供について）<br>マッピング等については、今回の意見募集の対象であるISMAP管理基準改定案を公表した後、作成し公開することを予定しています。<br><br>（非公開部分に関する変更点一覧（差分サマリー）の公表について）<br>ISMAP管理基準改定案及び新旧対照表は、ISMAPポータルの請求フォームから資料請求できるページを、年内に公開予定です。<br>なお、請求に当たり以下のJIS規格の購入が必要です。<br>JIS Q 27017:2016 (ISO/IEC 27017:2015)<br>JIS Q 27014:2015 (ISO/IEC 27014:2013)<br><br>（各コントロール・ファミリー毎の具体的な除外例の提示について）<br>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しています。<br><br>（事前審査の標準化について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承ります。<br><br>（継続評価・更新について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承ります。<br><br>（コントロール継承に関するガイダンスの精緻化について）<br>御意見の内容は新基準適用のタイミングや経過措置について、重要な観点と認識しております。既にISMAP等クラウドサービスリストに登録されているクラウドサービス事業者、新規で登録を予定されているクラウドサービス事業者、監査機関等、関係者の御意見を踏まえながら慎重に検討を進めて参ります。<br><br>（ISMAP標準監査手続書の調整について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、ISMAP制度の監査につきましては、検討中であるところ、御意見として承ります。<br><br>（監査期間ルールの具体例について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、ISMAP制度の監査につきましては、検討中であるところ、御意見として承ります。<br><br>（暗号化消去に関する受理可能な証跡の明確化について）<br>監査対応における証跡の例示等については、現行はISMAP管理基準ガイドブックにおいて示しているところ、今後も示す必要があると考えており、「ガイドライン」等において示すことを検討しています。<br><br>（重要用語の二言語（日本語・英語）対訳用語集について）<br>御指摘いただいた点については、継続的に検討を進めて参ります。 | 企業 |

| 連番 | 提出意見／電子ファイル | 御意見に対する回答 | 提出者 |
|---|---|---|---|
| (44の続き) | 【追加提言（長期的な一貫性の確保）】<br>・差分監査による更新: 各コントロールに実質的変更がない場合の更新時差分監査の適用。<br>・文書群の公表日・施行日の同期と移行期間（6 か月）の設定。<br>・共有責任モデルの形式化（IaaS、PaaS、SaaS）: ダイアグラムおよび証跡分担例の提示。<br>・マルチリージョンのスコープと継承のモデル化: 高可用構成等の多地域展開を想定したスコープ記述例の提示。<br><br>【結び】<br>上記の提言は、改定案の趣旨（コントロールの精選、原則実装、効果的な事前審査、監査手続の実効性向上、継承の明確化）を維持しつつ、運用の一貫性と実効性を高めるものです。これらが採用されれば、ばらつき、再作業、不必要なコストが減少し、日本政府機関における信頼できるクラウドサービスへの移行が一層加速すると考えます。ISMAP の近代化を主導される日本政府のご尽力に敬意を表し、標準および手続の最終化に向け、引き続き建設的な対話を歓迎いたします | （差分監査による更新について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、ISMAP制度の監査につきましては、検討中であるところ、御意見として承ります。<br><br>（文書群の公表日・施行日と移行期間について）<br>御意見の内容は新基準適用のタイミングや経過措置について、重要な観点と認識しております。既にISMAP等クラウドサービスリストに登録されているクラウドサービス事業者、新規で登録を予定されているクラウドサービス事業者、監査機関等、関係者の御意見を踏まえながら慎重に検討を進めて参ります。<br><br>（共有責任モデルの形式化について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承ります。<br><br>（マルチリージョンのスコープと継承のモデル化について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承ります。 | 企業 |
| 45 | 9つの意見を提出いたします。<br><br>意見1)<br>「（新）管理策基準」により管理策数が減少する一方で、「（参考）手引き」では、情報セキュリティ管理基準（令和７年版）に則った形で、a)～といった遵守すべき項目が列挙されております。そのため、実質的な負荷軽減のイメージが掴みにくい状況でございます。<br>セキュリティ品質の向上には一定の効果が期待できるものの、ISMAPにおける費用対効果の観点では、移行作業に伴う工数が増加する可能性があり、現時点ではやや懸念を抱いております。<br>つきましては、ISMAPの費用対効果の観点から、負荷軽減策や移行支援に関する具体的な内容をご提示いただけますと幸いです。<br>意見2)<br>新たに導入される事前確認につきまして、既存の事前相談では、細かなQAのやり取りにより長期化するケースが見受けられます。事前確認においては、そうしたリードタイムを軽減するための措置や、もう少し具体的なプロセスや目安をご提示いただけますと幸いです。<br>意見3)<br>「手引き」とISMAP取得済サービスの現行統制にギャップがある場合、新管理策基準への移行に際して、現行統制が優先されるのか、あるいは「手引き」への移行にあたって緩和措置が講じられるのかといった制度設計について、より明確にご説明いただけますと幸いです。<br>意見4)<br>詳細管理策が1163項目から322項目にグルーピングされる点は、負担軽減の観点からありがたく感じております。一方で、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」に基準があるとされており、説明会ではこの「手引き」に対応することで、現在のISMAP監査と比較して負荷は大きく変わらないとのご説明があったと認識しております。もしこの認識に相違がなければ、制度改定後も負荷が変わらない要因について、資料に反映していただけますと幸いです。<br>意見5)<br>ガバナンス基準およびマネジメント基準が「原則としてすべて」から「すべて」へと変更されておりますが、変更による負担の増加を評価するため、具体的な事例をご教示いただけますと幸いです。<br>意見6)<br>制度の移行期間につきまして、可能であれば早めにご案内いただけますと幸いです。<br>意見7)<br>現行のガイドブックを拝見すると、要求事項には明記されていないものの、遵守が求められる内容が追加的に記載されているケースがあるように見受けられます。今回も同様の対応が想定される場合には、可能であればその内容をあらかじめ要求事項に反映していただけますと幸いです。<br>意見8)<br>ISO/IEC 270xx、情報セキュリティ管理基準、統一基準、NISTなど、複数の基準が寄せ集められており、それぞれの表現がそのまま使用されているため、ISMAPとしての管理基準において表現の統一が図られておらず、内容の理解が難しいと感じております。<br>つきましては、管理基準としての一貫性を高めるためにも、表現の統一をご検討いただけますと幸いです。<br>意見9)<br>ISO/IEC 27001や27017など、他の認証制度の積極的な活用をご検討いただけますと幸いです。<br>また、申請クラウドサービスが利用しているピアクラウドサービスに関しても、SOC2、FedRAMP、NISTなどの認証制度を活用することが可能ではないかと考えております。 | 御意見に記載の項目毎に以下のとおり回答いたします。<br>（意見1について）<br>ISMAP管理基準改定案において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することによって、詳細管理策の数を削減しているほか、想定されるリスクに応じて統制目標に対応する詳細管理策を選択するのではなく実態としてそれ以上に詳細管理策を選択すること等への対応を行っています。これにより、一定程度の負担軽減は図れるものと考えています。<br>また、ISMAP制度の抜本的な見直しとして、SaaS事業者を対象とする負担を軽減した新たな枠組みを検討中です。その他、負担軽減策等については、引き続き検討を進めて参ります。<br><br>（意見2について）<br>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しています。<br>事前確認による負荷が増加することがないよう、御意見も踏まえ、事前確認の枠組みの検討を進めて参ります。<br><br>（意見3について）<br>御意見の内容は新基準適用のタイミングや経過措置について、重要な観点と認識しております。既にISMAP等クラウドサービスリストに登録されているクラウドサービス事業者、新規で登録を予定されているクラウドサービス事業者、監査機関等、関係者の御意見を踏まえながら慎重に検討を進めて参ります。<br><br>（意見4について）<br>ISMAP管理基準改定案において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することによって、詳細管理策の数を削減しているほか、想定されるリスクに応じて統制目標に対応する詳細管理策を選択するのではなく実態としてそれ以上に詳細管理策を選択すること等への対応を行っています。これにより、一定程度の負担軽減は図れるものと考えています。<br>また、ISMAP制度の抜本的な見直しとして、SaaS事業者を対象とする負担を軽減した新たな枠組みを検討中です。その他、負担軽減策等については、引き続き検討を進めて参ります。<br><br>（意見5について）<br>ガバナンス基準、マネジメント基準については、現行では「原則として全て実施しなければならない」としておりましたが、実施しない例外ケースが存在しないことから、「原則として」を削除しました。削除に伴う影響は、ないものと考えています。<br><br>（意見6について）<br>御意見の内容は新基準適用のタイミングや経過措置について、重要な観点と認識しております。既にISMAP等クラウドサービスリストに登録されているクラウドサービス事業者、新規で登録を予定されているクラウドサービス事業者、監査機関等、関係者の御意見を踏まえながら慎重に検討を進めて参ります。<br><br>（意見7について）<br>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しています。<br><br>（意見8について）<br>現状では、表現に関して変更を行うと、参照している規程との整合性が図られなくなる恐れがあると考えています。<br>表現の統一につきましては、今後の改善検討の参考とさせていただきます。<br><br>（意見9について）<br>現行制度において、他の認証制度の活用については、他の認証制度における統制内容と共通する部分が一定程度あるものの、準拠している基準、監査・審査の手続き、監査人の要件等が異なり、ISMAPが求めるセキュリティ水準を満たしていることを客観的に担保することが難しいなど、困難な面がございますが、御意見を踏まえ、引き続き検討を進めて参ります。<br>また、ISMAP制度の抜本的な見直しとして、SaaS事業者を対象に、他の認証制度の活用等を通じてクラウドサービス事業者の負担を軽減する新たな枠組みを検討中です。 | 企業 |

| 連番 | 提出意見／電子ファイル | 御意見に対する回答 | 提出者 |
|---|---|---|---|
| 46 | 日本政府が「安全なデジタルトランスフォーメーション（DX）」の推進を目的として、政府情報システムのためのセキュリティー評価制度（ISMAP）の改革を進めていることを踏まえ、この取組みに関するパブリックコンサルテーションに意見を提出する機会を歓迎します。この改革には、クラウドサービスプロバイダー（CSP）の参入障壁を低減し、ISMAPの既存の第三者認証の仕組みを拡張し、クラウドの機密性・完全性・可用性を保証するための手段を適正な規模に収めること、また、国際的に認められた認証制度との互換性を強化することなどが含まれています。<br><br>ISMAPの改革には以下を含めるべきです。<br>1. セキュリティ監査のサイクルを年次から3年に一度に変更し、監査内容の提出期限を監査完了後6ヶ月に延長するとともに、サービスプロバイダーがグローバルな監査サイクルを柔軟に管理できる制度を導入すること。<br>2. ISMAPをリスクベースのアプローチに改革し、SOC2やISO27000シリーズなどの国際的に認められた標準と整合させること。共通管理項目については第三者監査結果の提出を認め、日本独自の例外事項を明確に規定すること。<br><br>改正案草案に関連し、事前確認プロセスを導入することで、評価・審査の前に潜在的な課題を軽減し、正式なレビューを通じて提案された統制を事前に検証することが可能となります。<br>CSPが、評価・審査開始前に、新ガイドラインに基づく除外対象管理目標および詳細管理措置の有効性、並びにガイダンスから選択した管理措置の適切性について審査を受けられる事前確認プロセスの導入を支持します。この仕組みは、評価準備段階における情報処理推進機構(IPA)とCSP間のコミュニケーション体制の改善に寄与します。<br><br>新たな管理基準が2026年1月から2月の間に公表される予定であると認識しています。詳細ガイドラインの明確さと指示レベルに応じて、CSPが新たな管理基準を調整・適用するための猶予期間が必要となります。そのため、CSPが個々の新管理基準に対する準備・適応に十分な時間を確保できるよう、新たな管理基準発効前に移行期間を設けることを提言します。2026年に公表される新管理基準の性質によっては、実施に向けた長期の移行期間が必要となる可能性があります。<br><br>さらに、評価過程においてサービスプロバイダーがIPAと直接連携できるよう、概要説明やその他の仕組みを導入し、審査プロセスに要する時間を最適化するよう要請します。<br><br>質問1:<br>9月18日に発表された新たな管理措置とガイダンスでは、現行の管理措置と比較して詳細な管理措置の数は減少したものの、ガイダンスに記載された新規則が監査対象となる場合には、全体の項目数は増加する見込みです。この点については、来年1月に新たなガイドラインで公表される新規則において詳しく説明されるものと理解しています。<br>現行ISMAP基準の各章に対応する新規管理項目のすべてについて、明確化を求めます。これによりCSPが主要管理項目を理解し、ISMAP委員会およびIPAとの評価に関するコミュニケーションが円滑化されると考えます。<br><br>質問2:<br>9月18日に発表された新たな管理基準に含まれる新規管理項目およびガイダンスには、JIS Q 2017:2016（ISO/IEC 27017:2015）に関するガイダンスの具体的な記載がありません。JIS Q 2017:2016（ISO/IEC 27017:2015）に関するガイダンスの明確化を求めます。<br><br>公共部門でのクラウド導入を加速することは、経済全体のDXを促進し、日本の将来における成長の可能性を引き出すうえで極めて重要です。これに鑑み、ISMAPスキームの負担軽減により具体的なメリットを確保するよう、政府に要望します。現行のISMAPを国際的なベストプラクティスに整合させる改革は、競争の促進、日本の国内クラウドエコシステムの深化、セキュリティコストの削減と並行したセキュリティ成果の向上に寄与すると考えます。 | 御意見に記載の項目毎に以下のとおり回答いたします。<br>（セキュリティ監査のサイクルについて）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、ISMAP制度の監査につきましては、検討中であるところ、御意見として承ります。<br><br>（リスクベースのアプローチに関する他の認証ついて）<br>現行制度において、他の認証制度の活用については、他の認証制度における統制内容と共通する部分が一定程度あるものの、準拠している基準、監査・審査の手続き、監査人の要件等が異なり、ISMAPが求めるセキュリティ水準を満たしていることを客観的に担保することが難しいなど、困難な面がございますが、御意見を踏まえ、引き続き検討を進めて参ります。<br>また、ISMAP制度の抜本的な見直しとして、SaaS事業者を対象に、他の認証制度の活用等を通じてクラウドサービス事業者の負担を軽減する新たな枠組みを検討中です。<br><br>（事前確認プロセスについて）<br>御意見ありがとうございます。継続してより良い制度になるよう検討を進めて参ります。<br><br>（猶予期間について）<br>御意見の内容は新基準適用のタイミングや経過措置について、重要な観点と認識しております。既にISMAP等クラウドサービスリストに登録されているクラウドサービス事業者、新規で登録を予定されているクラウドサービス事業者、監査機関等、関係者の御意見を踏まえながら慎重に検討を進めて参ります。<br><br>（審査プロセスに要する時間について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承ります。<br><br>（質問1について）<br>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しています。ガイドラインにより、できる限り御不明な点が解消されるよう、明確化して参ります。<br>また、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しています。<br>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、現状の課題である監査・審査対応の負担増(想定されるリスクに応じて統制目標に対応する詳細管理策を選択するのではなく実態としてそれ以上に詳細管理策を選択すること等によるもの)や追加監査等の手戻りに対応することとし、御懸念の点が起きないように検討を進めて参ります。<br><br>（質問2について）<br>ISMAP管理基準改定案及び新旧対照表は、ISMAPポータルの請求フォームから資料請求できるページを、年内に公開予定です。<br>なお、請求に当たり以下のJIS規格の購入が必要です。<br>JIS Q 27017:2016 (ISO/IEC 27017:2015)<br>JIS Q 27014:2015 (ISO/IEC 27014:2013) | 団体 |
| 47 | ISMAP管理基準改定案に関する意見<br>当組織は、ISMAPフレームワークの継続的な改善努力と、高いセキュリティ水準を維持する取り組みに対し、深く感謝申し上げます。グローバルなクラウドサービスプロバイダー（CSP）による改定基準のスムーズかつ効率的な導入、および不必要な監査コストの発生を避けるため、以下の意見を提出いたします。<br>1. 国際的な調和と国内基準の統一<br>改定基準が世界的な相互運用性を最大化し、冗長な対応を最小限に抑えるため、管理基準の文言を国際および国内の主要なフレームワークと調和させることを提案いたします。<br>管理基準の文言統一：改定後の管理基準の最終版が、根拠となる最新の国際および国内規格、特に JIS Q 27001、ISO/IEC 27002:2022、および NIST SP 800-53 リビジョン5 で使用されている正確な文言と、可能な限り調和・対応するよう強く要望いたします。専門用語や意図のわずかな変更は、グローバルなCSPにとって解釈、実装、および監査において多大なコスト増を招くためです。<br><br>2. 認定済みインフラストラクチャにおける管理策の合理化<br>継承される管理策への対応プロセスが、不必要な重複作業を生じさせています。<br>継承管理策の自動的な適用除外の許可：CSPが、既に ISMAP認定済みである 基盤となるサードパーティIaaSサービス（例：AWS、GCP、MS Azureなど）を利用している場合、物理的セキュリティ、環境管理策、およびコアインフラストラクチャ管理に関連する管理策について、個別の徹底的なリスク評価を行うことなく、その管理策を継承し、適用を除外することを明確に許可するよう要望いたします。これにより、既存の認定の取り組みを有効活用し、CSPおよび監査機関双方の冗長な作業負荷を軽減できます。<br><br>3.「リスクベースアプローチ」導入の趣旨の明確化<br>「リスクベースアプローチ」の導入が、一部の監査法人によって、通常のコンプライアンス活動における管理工数およびコスト増加の根拠として利用される事例が見受けられます。これは、制度導入の本来の趣旨に反するものです。<br>簡素化の原則の徹底：「リスクベースアプローチ」は、監査プロセス全体の簡素化を促進し、CSPの管理上の負担を軽減するために活用されるべきであるという原則を明確化する指針を公開することを、運営委員会に強く要請いたします。監査対象となる管理策の記述の検証や、前回監査期間から軽微な変更しかなされていない管理策の評価において、監査工数を増加させるのではなく、高リスクで非継承の管理策に焦点を絞ることが目的であることを再確認してください。<br><br>4. 新技術管理策に関する指針および質疑応答集の提供<br>AI/MLサービス関連の管理策など、新しく追加される技術分野の管理策については、効果的な導入のために明確性が不可欠です。<br>ガイダンスとFAQの早期提供：ISMAP運営委員会に対し、全ての新しい技術管理策について、十分かつ包括的なガイダンス（手引書）と質疑応答集（FAQ）を、CSPおよび認定された監査機関向けに施行日よりも十分早く提供することを要望いたします。<br>SaaSにおける責任分界点の明確化：JIS Q 27001に則り、SaaSサービスモデルにおいて、データマスキングの方針や顧客定義のデータ保持設定など、本質的に顧客の責任となる管理策について、監査時の曖昧さを避けるため、責任分界点を明確にする定義済みの指針を確立することを要望いたします。 | 御意見に記載の項目毎に以下のとおり回答いたします。<br>（1. 国際的な調和と国内基準の統一について）<br>ISMAP管理基準改定案では、根拠となる最新の国際及び国内規格で使用されている文言と、できるだけ調和するように工夫しております。今後の改定等に当たり、政府統一基準とのバランスも考慮しながら、引き続き検討を進めて参ります。<br><br>（2. 認定済みインフラストラクチャにおける管理策の合理化について）<br>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しています。<br>御意見も踏まえ、「ガイドライン」の内容を検討して参ります。<br><br>（3.「リスクベースアプローチ」導入の趣旨の明確化について）<br>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しています。<br>御意見も踏まえ、「ガイドライン」の内容を検討して参ります。<br><br>（4. 新技術管理策に関する指針および質疑応答集の提供について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承ります。 | 企業 |

| 連番 | 提出意見／電子ファイル | 御意見に対する回答 | 提出者 |
|---|---|---|---|
| 48 | 1-「ISMAP管理基準改定概要資料」のp.3の「-なお、監査においては手引きを参考に監査を実施」について<br>「参考に監査」との記載がありますが、標準監査手続が不明確な状況において「参考」という表現を用いると、手引きの重要性が過小評価される懸念があります。その結果、監査機関が手引きを基に指摘や質問を行った際に、CSP側が「参考に過ぎない」との認識を持つことで、不満や混乱を招く可能性があります。こうした事態を避けるためにも、表現の見直しをご検討ください。<br>2-「ISMAP管理基準改定概要資料」のp.3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」について<br>今回の変更により、各管理策における「主たる監査対象」がどのように設定されるかが不明であり、また、運用状況評価の対象をどのように識別するかについても明示されていません。これらは、監査機関が行う監査の品質を一定に保つ上で重要なのはもちろんのこと、CSPが準備を進める上でも極めて重要な要素ですので、ガイドラインに明記する予定なのか、他の文書にて周知する予定なのか等の方針を早急に明らかにする必要があると思料します。<br>3-「ISMAP管理基準改定概要資料」のp.4の「-「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」について<br>「ガイドラインにて解説予定」との記載がありますが、当該内容は今回の改定において特に重要なポイントであると認識しております。そのため、ガイドラインが未提示の現時点では、今回の変更の妥当性を適切に判断することは困難です。関係者の意見がガイドラインに十分に反映され、詳しい説明がなされるのでなければ、制度に対する不満が再燃するおそれがあるため、慎重かつ丁寧な対応をお願い致します。<br>4-「ISMAP管理基準改定概要資料」のp.7の「ガイドラインの策定、事前確認の枠組みの導入」について<br>標準監査手続の検討もガイドラインと連動して進める必要があると考えますが、ガイドラインの策定や事前確認の枠組み導入に関する具体的なスケジュールが示されておらず、標準監査手続の検討スケジュールも明らかではありません。そのため、ISMAP管理基準が改定された後すぐに新管理基準へ移行することは現実的ではないと考えます。各施策のスケジュールを改めて明確にお示しください。<br>5-「ISMAP管理基準改定概要資料」のp.7の「ガイドラインの策定、事前確認の枠組みの導入」について<br>具体的な移行期間等が明示されておりませんが、現行のISMAP管理基準に基づいてISMAPクラウドサービスリストへの登録を目指して取り組んでいるCSPも存在するので、ISMAPクラウドサービスリストに登録済みのCSPでけでなく、ISMAPクラウドサービスリストにまだ登録されていないCSPについても移行期間が考慮されるべきと考えます。<br>また、ISMAP管理基準改定等のスケジュールが明示されないため、ISMAPへの取り組みに二の足を踏むCSPもございます。このようなCSPのために、まだ具体的なスケジュールを公表できない段階であっても、いつまでにどのように進めれば取り組みが無駄にはならないこと等の情報を発信していく必要があると考えます。<br>6-「ISMAP管理基準_別表１-３（案）」の「全体」について<br>ISMAPでは、CSPに対してISMAP管理基準の文言どおりの活動を求めてきました(規程類の字句が少々異なろうと、詳細管理策に書かれた観点が存在することは求めてきました。ISMAP監査機関に対するモニタリングでは、観点の確認漏れがないかが厳しく調べられました)。ISMAP創設から5年が経ち、CSPの中には社内規程をISMAP管理基準の文言に寄せたり、ISMAP管理基準を一つの拠り所として規程類を整備したケースがあります。そのようなCSPでは、ISMAP情報セキュリティ監査を受ける際にISMAP管理基準の詳細管理策に該当する社内規程等を提示するのが容易であり、監査対応に要する負担の軽減を図れていました。<br>この度の改定によりISMAP管理基準の文言が変わることで、これらのCSPは社内規程等のあり方を再考せざるを得なくなると思料します。制度側は、ISMAP管理基準改定を踏まえた最適化をCSPにどこまで求めるのか、そのスタンスを示す必要があろうと考えます。<br>例えば、新管理基準の3.3.2.1には「事業に取り組む際の関連するリスク及び機会の確実な考慮」という文言があります。これは現管理基準の「経営陣は、事業の取組みにおいて情報セキュリティ問題を考慮することを確実にする。」に関連するものと思料します。CSPが既存の社内規程に「経営陣は、事業の取組みにおいて情報セキュリティ問題を考慮することを確実にする。」と記載していた場合、これまでであれば、ISMAP管理基準に沿ったルールの整備を容易に示せました。しかし、改定後は、新管理基準中の「リスク及び機会の考慮」を示す文言がCSPの規程内に明瞭に記載されていないと、ISMAP管理基準に沿ったルールが整備されているとはいえなくなるでしょうか。それとも、現管理基準に沿った「情報セキュリティ問題を考慮」という文言が新管理基準の「リスク及び機会の考慮」に相当するものであるとCSPが主張すれば、それは「リスク及び機会の考慮」の存在が認められたことになるでしょうか。制度側から、新管理基準の「リスク及び機会の考慮」は現管理基準の「情報セキュリティ問題を考慮」に相当するとの見解を公表してくださると、現場の混乱は小さくなると考えますが、いかがでしょうか。それだと、新しい管理基準の趣旨が反映されたとは言えず、管理基準の改定をないがしろにしたことになってしまいますでしょうか。<br>このような点について、早い段階で制度側がスタンスを明らかにしてくださることで、CSPの負担の多寡が大きく変わってくると思料します。ご検討のほどよろしくお願いいたします。<br>7-「ISMAP管理基準_別表１-３（案）」の「全体」について<br>例えば、3.3.2.1には「事業に取り組む際の関連するリスク及び機会の確実な考慮」という文言の中に”考慮”が出てきます。しかし、CSPが「一瞬でも考えた」と主張すれば「考慮すること」は満たせてしまうため(考慮していないと立証することは不可能)、基準としては不適切な用語であると思料します。<br>3.3.2.1を含む「考慮」が出てくる管理策では、”考慮”ではなく、例えば”検討した上でその記録を残す”といった表現にするなど、行動に落とし込みやすく、客観的な評価もしやすい表現に見直すべきと考えます。<br>8-「ISMAP管理基準_別表１-３（案）」の「全体」について<br>過去、”伝達”に関連してISMAP運用支援機関に代替手続を照会したところ、社内ポータルへの掲示のみでは伝達には資さないとの返答がありました。<br>ISMAP管理基準の改定を経ても同様の考え方を継続するのであれば、制度が期待する伝達とは何のことか明確に伝わるように記述すべきです。<br>※伝達が求められる全ての管理策においても同様です。<br>＜参考情報：過去の代替手続照会に対するISMAP運用支援機関からの回答(CS0003833)＞<br>本管理策の標準監査手続では、「ログオフするよう」伝達を実施した履歴が記録されていることの確認が求められておりますが、代替手続で確認される内容を見ると、「社内サイトに掲載していること」の確認に留まり、利用者への伝達が実施されていることの確認に資さないように思われます。社内サイト等に掲示する以外に、能動的な伝達（例：研修実施や、社内ポータルに掲載した旨の周知メールを行う等）は何か実施されていないのでしょうか。<br>9-「ISMAP管理基準_別表１-３（案）」の「3.3.4.2」について<br>「情報セキュリティの実績に関する結果のフィードバックを組織体の経営陣に提供」や「情報リスク及び情報セキュリティに影響する新規の開発についての、組織体の経営陣への注意喚起」が記載されておりますが、”経営陣”と” ガバナンス主体”は別の役職を指しているのでしょうか？同一の役職であれば、表現は統一すべきと考えます。<br>10-「ISMAP管理基準_別表１-３（案）」の「3.3.5.1」について<br>「情報セキュリティの優先度決定を支援するために採用すべき詳細な対象」という文言において、”対象”が何を指しているのか不明です。より具体的に説明したり、具体例を加筆することが望ましいと思料します。<br>また、「スタッフ及びその他の人々を対象とする」という文言がありますが、スタッフは他の箇所で使われておらず、未定義の用語です。読み手に趣旨が伝わらないおそれがあります。<br>その他の人々も、どのような人をどの範囲まで指すのか曖昧な表現です。<br>詳細管理策が意図する対象者を明確に記載すべきです。<br>11-「ISMAP管理基準_別表１-３（案）」の「4章以降全体」について<br>ガバナンス基準では「”top management”の呼び方を、”管理者”から”情報セキュリティマネジメントシステムの責任者”に変更。」となりました。<br>しかしながら、マネジメント基準、管理策基準にはトップマネジメントという語が登場しております。<br>ガバナンス基準と他の基準における、用語の整合性(特に同一の人物-職階を指す場合の表記揺れ)について、検討が必要ではないでしょうか。 | 御意見に記載の項目毎に以下のとおり回答いたします。<br>（1-「ISMAP管理基準改定概要資料」のp.3の「-なお、監査においては手引きを参考に監査を実施」について）<br>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しています。<br>御意見も踏まえ、クラウドサービス事業者と監査機関において御意見のような認識相違が発生しないよう、「ガイドライン」の内容を検討して参ります。<br><br>（2-「ISMAP管理基準改定概要資料」のp.3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」について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、ISMAP制度の監査につきましては、検討中であるところ、御意見として承ります。<br><br>（3-「ISMAP管理基準改定概要資料」のp.4の「-「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」について）<br>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しています。<br>ガイドライン策定の際は、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であるほか、パブリック・コメント前にも関係者向けの説明会等で丁寧に説明して参りたいと考えています。<br><br>（4-「ISMAP管理基準改定概要資料」のp.7の「ガイドラインの策定、事前確認の枠組みの導入」について）<br>御意見の内容は新基準適用のタイミングや経過措置について、重要な観点と認識しております。既にISMAP等クラウドサービスリストに登録されているクラウドサービス事業者、新規で登録を予定されているクラウドサービス事業者、監査機関等、関係者の御意見を踏まえながら慎重に検討を進めて参ります。<br><br>（5-「ISMAP管理基準改定概要資料」のp.7の「ガイドラインの策定、事前確認の枠組みの導入」について）<br>御意見の内容は新基準適用のタイミングや経過措置について、重要な観点と認識しております。既にISMAP等クラウドサービスリストに登録されているクラウドサービス事業者、新規で登録を予定されているクラウドサービス事業者、監査機関等、関係者の御意見を踏まえながら慎重に検討を進めて参ります。<br><br>（6-「ISMAP管理基準_別表１-３（案）」の「全体」について）<br>御意見の内容は新基準適用のタイミングや経過措置について、重要な観点と認識しております。既にISMAP等クラウドサービスリストに登録されているクラウドサービス事業者、新規で登録を予定されているクラウドサービス事業者、監査機関等、関係者の御意見を踏まえながら慎重に検討を進めて参ります。<br><br>（7-「ISMAP管理基準_別表１-３（案）」の「全体」について）<br>御意見の内容につきましては、情報セキュリティ管理基準における記載内容に準拠していることによるものであり、ISMAP管理基準改定案の策定方針に従って原案のとおりとします。<br><br>（8-「ISMAP管理基準_別表１-３（案）」の「全体」について）<br>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しています。<br>クラウドサービス事業者とISMAP運用支援機関において御意見のような認識相違が発生しないよう、御意見も踏まえ、「ガイドライン」の内容を検討して参ります。<br><br>（9-「ISMAP管理基準_別表１-３（案）」の「3.3.4.2」について）<br>御意見の内容につきましては、情報セキュリティ管理基準における記載内容に準拠していることによるものであり、ISMAP管理基準改定案の策定方針に従って原案のとおりといたしますが、今後の改定において御意見を参考とさせていただきます。<br><br>（10-「ISMAP管理基準_別表１-３（案）」の「3.3.5.1」について）<br>御意見の内容につきましては、情報セキュリティ管理基準における記載内容に準拠していることによるものであり、ISMAP管理基準改定案の策定方針に従って原案のとおりといたしますが、今後の改定において御意見を参考とさせていただきます。<br><br>（11-「ISMAP管理基準_別表１-３（案）」の「4章以降全体」について）<br>クラウドサービスを提供する事業者におけるガバナンスや組織形態はその規模や事業内容に応じて多様であることから、改定案ではその多様性に対応可能なように主体を示す用語の使い分けを行っております。一方で御意見のような疑問が生じることのないよう、必要に応じて「ガイドライン」における解説を検討いたします。 | 監査企業 |

| 連番 | 提出意見／電子ファイル | 御意見に対する回答 | 提出者 |
|---|---|---|---|
| (48の続き) | 12-「ISMAP管理基準_別表１-３（案）」の「4.4.1.2」や「4.4.2.1」について<br>「責任-権限の例を以下に示す。」や「以下に例示するものが含まれ得る。」と記載されておりますが、今回の改訂のポイントで解説しているとおり、例示はガイドラインにて示す方針になった認識です。<br>上記の方針であれば、当該例示もガイドラインに記載すべきではないでしょうか？<br>13-「ISMAP管理基準_別表１-３（案）」の「4.4.3.1」について<br>「以下を決定する」という管理策にて列挙している中に、「-利害関係者の要求事項には、法的及び規制の要求事項並びに契約上の義務を含める場合もあるが、利害関係者には、以下に例示する人又は組織が含まれ得る。」と列挙しているものに関する説明のような文章が記載されており、求めているものが不明瞭です。<br>解説であれば、ガイドラインに記載すべきであり、管理基準_別表には、管理策として決定すべきと求めている事項のみを記載すべきです。<br>14-「ISMAP管理基準_別表１-３（案）」の「4.4.4.1」について<br>詳細管理策において、「適用範囲を決定する」行動を求めているのか、それ以上のことを求めているのかが分かりにくいです。<br>例えば、「情報セキュリティマネジメントの目的や目標は、組織の特徴によって異なる。」では、情報セキュリティマネジメントの目的や目標を定めることもこの詳細管理策の範疇なのか、単に留意事項を書き添えただけなのか、どちらにも読めるために分かりにくいです。<br>また、「組織は以下の点を考慮して適用範囲及び境界を定義する。」や「情報セキュリティマネジメントに対する要求事項はそれぞれの組織の事業によって、外部状況、内部状況の双方があり、これらを考慮して適用範囲を定義する。」に関しても、適用範囲を決定する際のヒントを書いただけで遵守を求めるものではないのか、いずれの点も考慮することが必須で、考慮したことの証拠を残すことまでを求めているのか、分かりにくいです。<br>CSPが自らの管理策を整備する上で誤解が生じないように、また監査機関が評価する際に発見事項か否かを明確に識別できるように、含みを持たせた言い回しは管理基準から排除してくださるようお願いします。<br>15-「ISMAP管理基準_別表１-３（案）」の「4.4.5.1」について<br>「また、情報セキュリティ方針は情報セキュリティマネジメントにおける判断の基盤となる考え方を記載したものであり、組織の戦略に従って慎重に作成する。」に関し、具体的に何を求めているかがわかりにくいです。「慎重」という言葉は主観的で、CSPに順守させる基準や、監査機関が行う評価の物差しとしては不適切です。<br>単なる作成にあっての留意点であり、具体的な要求事項ではないのであれば、ガイドラインに記載すべきです。<br>16-「ISMAP管理基準_別表１-３（案）」の「4.4.5.3」について<br>「これらはトップマネジメントの責任を明確にするために実施する。」に関し、具体的に何を求めているかがわかりにくいです。<br>単なる補足説明であり、具体的な要求事項ではないのであれば、ガイドラインに記載すべきであり、管理策として不適切であるように見受けられます。<br>17-「ISMAP管理基準_別表１-３（案）」の「4.4.7.3」について<br>「なお、リスク分析は、状況に応じて、定性的、半定量的、定量的、又はそれらを組み合わせた手法で行うことが可能である。」に関し、具体的に何を求めているかがわかりにくいです。<br>単なる留意点であり、具体的な要求事項ではないのであれば、ガイドラインに記載すべきであり、管理策として不適切であるように見受けられます。<br>18-「ISMAP管理基準_別表１-３（案）」の「4.4.7.1」について<br>「なお、情報セキュリティマネジメントにおけるリスクアセスメント手法には、定番といえるものがなく、それぞれの組織に適合したものを選択している場合が多いことから、必要に応じてツールを利用することなどが必要になる。」に関し、具体的に何を求めているかがわかりにくいです。<br>単なる留意点であり、具体的な要求事項ではないのであれば、ガイドラインに記載すべきであり、管理策として不適切であるように見受けられます。 | （12-「ISMAP管理基準_別表１-３（案）」の「4.4.1.2」や「4.4.2.1」について）<br>今回の改定において、情報セキュリティ管理基準のマネジメント基準に示されている例示相当の内容については、情報セキュリティ基準におけるマネジメント基準の改定内容が比較的軽微であり、登録事業者における改定対応の便宜等も考慮して現行の管理基準同様に記載することとしております。<br><br>（13-「ISMAP管理基準_別表１-３（案）」の「4.4.3.1」について）<br>今回の改定において、情報セキュリティ管理基準のマネジメント基準に示されている解説相当の内容については、情報セキュリティ基準におけるマネジメント基準の改定内容が比較的軽微であり、登録事業者における改定対応の便宜等も考慮して現行の管理基準同様に記載することとしております。<br><br>（14-「ISMAP管理基準_別表１-３（案）」の「4.4.4.1」について）<br>御意見の対象の詳細管理策4.4.4.1は情報セキュリティ管理基準の改定内容に準拠した内容としております。当該管理策に記載のとおり、情報セキュリティマネジメントの目的や目標は組織の特徴に応じて多様となることに対応した内容であることが望ましいことから、原案のとおりとします。<br><br>（15-「ISMAP管理基準_別表１-３（案）」の「4.4.5.1」について）<br>準拠している情報セキュリティ管理基準において組織の情報セキュリティマネジメントの担当者が考慮すべき事項を示す観点で規定しているものであり、監査を行う上で支障となるものではないと考えられることから、原案のとおりとします。<br><br>（16-「ISMAP管理基準_別表１-３（案）」の「4.4.5.3」について）<br>「これらはトップマネジメントの責任を明確にするために実施する。」は補足説明に相当する内容ですが、準拠している情報セキュリティ管理基準において組織の情報セキュリティマネジメントの担当者が考慮すべき事項を示す観点で規定しているものであり、監査を行う上で支障となるものではないと考えられることから、原案のとおりとします。<br><br>（17-「ISMAP管理基準_別表１-３（案）」の「4.4.7.3」について）<br>「なお、リスク分析は、状況に応じて、定性的、半定量的、定量的、又はそれらを組み合わせた手法で行うことが可能である。」は補足説明に相当する内容ですが、準拠している情報セキュリティ管理基準において組織の情報セキュリティマネジメントの担当者が考慮すべき事項を示す観点で規定しているものであり、監査を行う上で支障となるものではないと考えられることから、原案のとおりとします。<br><br>（18-「ISMAP管理基準_別表１-３（案）」の「4.4.7.1」について）<br>「なお、情報セキュリティマネジメントにおけるリスクアセスメント手法には、定番といえるものがなく、それぞれの組織に適合したものを選択している場合が多いことから、必要に応じてツールを利用することなどが必要になる。」は補足説明に相当する内容ですが、準拠している情報セキュリティ管理基準において組織の情報セキュリティマネジメントの担当者が考慮すべき事項を示す観点で規定しているものであり、監査を行う上で支障となるものではないと考えられることから、原案のとおりとします。 | 監査企業 |
| 49 | 19-「ISMAP管理基準_別表１-３（案）」の「4.4.8.2」について<br>以下を考慮しつつ、”と記載されておりますが、”考慮しつつ”が具体的に何をすることを指すのか読み手には分かりません。箇条書で挙げられたものはあくまでヒントであって遵守を求めるものではないのか、いずれの点も考慮することが必須で、考慮したことの証拠を残すことまでを求めているのか、分かりにくいです。CSPに順守させる基準や、監査機関が行う評価の物差しとしては不適切な文言であると考えます。<br>20-「ISMAP管理基準_別表１-３（案）」の「4.5.2.6、4.5.2.7、4.5.2.8」について<br>-「組織の管理下で働く人々」の定義がありません。詳細管理策が想定する範囲が不明瞭です。<br>-「組織の管理下で働く人々は、～～を認識する。」と書かれており、「組織の管理下で働く人々」が行動の主体になっております。しかし、「組織の管理下で働く人々」に要求事項を突き付けるのはマネジメント基準の趣旨に反すると思われますので、トップマネジメントが行動の主体になるように主語を書くのがよろしいと存じます。また、述語を”認識させる。”に変える等、マネジメント基準に相応しい表現に見直したほうがよいと考えます。<br>21-「ISMAP管理基準_別表１-３（案）」の「4.5.3.1」について<br>「内部及び外部のコミュニケーションを実施する必要性を決定する。…内部及び外部のコミュニケーションを実施する際は、以下を考慮することとする。」とありますが、本管理策で求められるのは、コミュニケーションを実施する必要性を決定したことを示す証拠なのか、必要性を決定する過程で4つの箇条を考慮したことを示す証拠が求められるのか、いずれにも解釈できそうです。<br>また、２つ目と３つ目の中黒(-)ではコミュニケーションの実施を求めており、”コミュニケーションを実施する必要性を決定する。”という詳細管理策の趣旨を逸脱しています。コミュニケーションに関する”実施”を求めているのか”必要性の決定”を求めているのか分かりにくいです。<br>以上のことから、このままでは基準として十分には機能しないと思われます。<br>22-「ISMAP管理基準_別表１-３（案）」の「4.5.4.1」について<br>前半では”次に示す事項の実施によって”と記載され、文の下に2つの箇条が挙げられていますが、後半ではその箇条の実施を求めることなく”必要なプロセスを計画し、実施し、かつ管理する”と記載されており、この詳細管理策が求めている具体的な活動が大変分かりにくいです。<br>23-「ISMAP管理基準_別表１-３（案）」の「4.6.2.3」について<br>”考慮する”と記載されておりますが、詳細管理策の中での”…考慮する”という文の位置付けが不明確です。この詳細管理策が求めているのは「監査プログラムを計画、確立、実施及び維持する」のほうなのか、”…考慮する”という文に沿って考慮した記録として残し、第三者評価の際には示せるようにすることまで求めているのか分からないです。 | （19-「ISMAP管理基準_別表１-３（案）」の「4.4.8.2」について）<br>御意見の対象箇所は、情報セキュリティ対応の選択肢の選定にあたって実施すべき内容を規定しており、基準としての参照において支障が無いと判断されることから、原案のとおりとします。<br><br>（20-「ISMAP管理基準_別表１-３（案）」の「4.5.2.6、4.5.2.7、4.5.2.8」について）<br>「ガイドライン」において用語の定義を記載することを検討しています。御意見も踏まえ、「ガイドライン」の内容を検討して参ります。<br>「認識する」の表現については、情報セキュリティ管理基準が準拠しているJIS Q 27001:2023及びISO/IEC 27001:2022においても「認識させる」に相当する内容となっていないこともあり、原案のとおりとします。<br><br>（21-「ISMAP管理基準_別表１-３（案）」の「4.5.3.1」について）<br>御意見の対象である4.5.3.1の詳細管理策で要求しているコミュニケーション実施の必要性に関する決定については、組織の特徴に応じて適切な内容は異なると見込まれることから、考慮事項や例を示しております。これらをもとに決定される実施すべきコミュニケーションについての監査は可能と判断されることから、原案のとおりとします。<br><br>（22-「ISMAP管理基準_別表１-３（案）」の「4.5.4.1」について）<br>御意見の対象である4.5.4.1の詳細管理策内の箇条について、要求事項を満たすための手段として解釈可能と判断されることから、原案のとおりとします。<br><br>（23-「ISMAP管理基準_別表１-３（案）」の「4.6.2.3」について）<br>御意見の対象である4.6.2.3の詳細管理策における「考慮する」の対象はプロセスの重要性と監査の結果であると解釈可能と判断されることから、原案のとおりとします。 | 監査企業 |

| 連番 | 提出意見／電子ファイル | 御意見に対する回答 | 提出者 |
|---|---|---|---|
| (49の続き) | 24-「ISMAP管理基準_別表１-３（案）」の「4.6.3.2」について<br>“考慮する”と記載されておりますが、詳細管理策の中での””…考慮する””という文の位置付けが不明確です。この詳細管理策が求めているのはマネジメントレビューをすることなのか、””…考慮する””という文の下の箇条それぞれについて考慮した記録として残し、第三者評価の際には示せるようにすることまで求めているのか分からないです。”<br>25-「ISMAP管理基準_別表１-３（案）」の「4.7.1.1」について<br>「不適合は以下の活動によって検出される。」とありますが、検出の機会について言及しているだけで、具体的な行動は何も求めていないように読めます。<br>-「不適合を手順どおりに検出するために、以下について文書化する。」の部分は文書化の話となっており、「不適合は以下の活動によって検出される。」の配下に続く内容として正しくないように見受けられます。<br>-「不適合を手順どおりに検出するために、以下について文書化する。」という文は、文書化すると不適合を検出できるように読めます。不適合の検出に係る活動と、文書化に関する活動が一つの文の中に混在し、趣旨を分かりにくくしています。”<br>26-「ISMAP管理基準_別表１-３（案）」の「4.7.1.6」について<br>「組織は、是正処置は、検出された不適合のもつ影響に応じたものとする。 」に関し、具体的に何を求めているかがわかりにくいです。一つの文の中に主語が二つあり、日本語として成立していないことが、分かりにくさを助長しています。<br>単なる留意点であり、具体的な要求事項ではないのであれば、ガイドラインに記載すべきであり、管理策として不適切であるように見受けられます。”<br>27-「ISMAP管理基準_参考１、２（案）」の「5.3.2」について<br>「情報セキュリティ対策の運用」の範囲が非常に広いため、監査手続を実施する際に混乱を招くおそれがあるかと存じます。<br>標準監査手続において、規程類を確認するか、実運用に供された文書-記録を確認するかで変わってきますが、文書-記録によって実運用を確認する場合、「情報セキュリティ対策の運用」という漠然とした範囲を対象にすると評価のボリュームが膨大になることが考えられます。制度として、「情報セキュリティ対策の運用」のどこに着目したいのか、焦点を絞った基準にすべきと思料します。”<br>28-「ISMAP管理基準_参考１、２（案）」の「5.7」など現管理基準にない管理策について<br>現管理基準には定めがない管理策は、CSP内に管理策が存在しない可能性がございます。管理基準の改定に当たって、現管理基準に定めがない管理策については一層の猶予期間を設け、ISMAPクラウドサービスリストに登録済みのサービスがこれを原因として登録取り消しになるようなことがないように配慮することが望まれます。”<br>29-「ISMAP管理基準_参考１、２（案）」の「5.8.1」について<br>手引きの「早い段階」という表現は、抽象度が高く、具体的に何を求めているのか不明瞭です。”<br>30-「ISMAP管理基準_参考１、２（案）」の「5.9.2」について<br>「を」が繰り返し出現しており、文法的におかしいです。”<br>31-「ISMAP管理基準_参考１、２（案）」の「5.11」について<br>「その他の利害関係者」という概念は、CSPが混乱しがちなものなので、「その他の利害関係者」として何が想定されるかを手引きに記載することが望ましいです。”<br>32-「ISMAP管理基準_参考１、２（案）」の「5.18」全般について<br>物理的セキュリティと論理的セキュリティが並列で記載されておりますが、一般的に物理的セキュリティと論理的セキュリティでは個別管理策の内容が異なることから、これを一つの詳細管理策とすることは個別管理策を煩雑-複雑にさせるおそれがあります。また、物理的セキュリティと論理的セキュリティとでは監査対象や母集団が異なることが多いと考えられ、ISMAP情報セキュリティ監査の効率-効果を低下させるおそれがあります。<br>物理的セキュリティと論理的セキュリティは分別する、又は物理的セキュリティは7章で詳細管理策を手厚く設定しているので5.18では論理的セキュリティに主眼をおく等の対策を講じることが望ましいと思料します。<br>33-「ISMAP管理基準_参考１、２（案）」の「6.8.1 」、「6.8.2」について<br>「全ての利用者」と記載されておりますが、統制目標や目的においては、「要員」との表現があります。統制目標や目的の表現にあわせて「要員」と表現すべきと考えます。”<br>34-「ISMAP管理基準_参考１、２（案）」の「7.4.2」について<br>「の機密性を維持する。」とありますが、CSPに対してはルールとして定めることを要求しているのか、それとも何かしらの記録を残すことを意図しているのかが分かるような管理策とするのが望ましいです。”<br>35-「ISMAP管理基準_参考１、２（案）」の「8.5.1」について<br>「認証技術及び手順は、」という主語に対し、「実施する。」という述語が不適当であり、何を要求しているのかが不明瞭です。”<br>36-「ISMAP管理基準_参考１、２（案）」の「8.21」について<br>「ネットワークサービス」が指し示す内容がわかりにくいように見受けられます。ガイドラインでも結構ですので、「ネットワークサービス」の解説や例を示すべきと考えます。”<br>37-「ISMAP管理基準_参考１、２（案）」の「8.21.2」について<br>「ネットワークサービスに必要なセキュリティ対策を実装する。」と要求されていますが、目的(ネットワークサービスの利用におけるセキュリティを確実にするため。)を考慮すると、CSPがネットワークサービスを利用する際に必要な対策を実装することを求めている内容でしょうか？<br>上記の趣旨の場合、そのことが明確になる表現とすべきと考えられます。”<br>38-「ISMAP管理基準_参考１、２（案）」の「8.23.1」について<br>「維持する」と記載されておりますが、何を維持することを求めているのかが不明瞭です。” | （24-「ISMAP管理基準_別表１-３（案）」の「4.6.3.2」について）<br>御意見の対象となっている4.6.3.2の詳細管理策における「トップマネジメントは、マネジメントレビューにおいて、以下を考慮する。」はマネジメントレビューで確認すべき内容を規定していると解釈可能であるため、原案のとおりとします。<br><br>（25-「ISMAP管理基準_別表１-３（案）」の「4.7.1.1」について）<br>御意見の対象となっている4.7.1.1の詳細管理策における「不適合は以下の活動によって検出される。」は不適合の検出方法を規定する内容を構成しているものであるため、原案のとおりとします。<br><br>（26-「ISMAP管理基準_別表１-３（案）」の「4.7.1.6」について）<br>御意見の対象となっている4.7.1.6の詳細管理策は是正措置が満たすべき要件を規定するものであるため、原案のとおりとします。<br><br>（27-「ISMAP管理基準_参考１、２（案）」の「5.3.2」について）<br>各管理策に対する標準監査手続については、検討中です。御意見も踏まえ、検討を進めて参ります。<br><br>（28-「ISMAP管理基準_参考１、２（案）」の「5.7」など現管理基準にない管理策について）<br>御意見の内容は新基準適用のタイミングや経過措置について、重要な観点と認識しております。既にISMAP等クラウドサービスリストに登録されているクラウドサービス事業者、新規で登録を予定されているクラウドサービス事業者、監査機関等、関係者の御意見を踏まえながら慎重に検討を進めて参ります。<br><br>（29-「ISMAP管理基準_参考１、２（案）」の「5.8.1」について）<br>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しています。御意見も踏まえ、「ガイドライン」の内容を検討して参ります。<br><br>（30-「ISMAP管理基準_参考１、２（案）」の「5.9.2」について）<br>御意見を踏まえ、5.9.2の詳細管理策の内容を次のように修正いたします。<br>「情報及びその他の関連資産の管理責任を明確にし、個人又はグループに割り当てる。」<br><br>（31-「ISMAP管理基準_参考１、２（案）」の「5.11」について）<br>ISMAP管理基準で用いている用語について、ガイドライン等にて公表することを検討しています。<br><br>（32-「ISMAP管理基準_参考１、２（案）」の「5.18」全般について）<br>御意見の対象となっている5.18では物理的及び論理的なアクセス権の扱いについて規定するものであり、準拠している情報セキュリティ管理基準及びJIS Q 27002:2024においても同様の規定となっています。<br>アクセス権の扱いに関する具体的な内容は多様となることが想定されますが、個別管理策の策定にあたり状況に応じて複数のプロセスを整備することを否定するものではありませんので、5.18の内容は原案のとおりとし、必要に応じてガイドライン等で補足説明を行うことを検討いたします。<br><br>（33-「ISMAP管理基準_参考１、２（案）」の「6.8.1 」、「6.8.2」について）<br>ISMAP管理基準改定案で用いている用語について、ガイドライン等にて公表することを検討しています。<br><br>（34-「ISMAP管理基準_参考１、２（案）」の「7.4.2」について）<br>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しています。ガイドラインで補足説明を実施し、できる限り御不明な点が解消されるよう、明確化して参ります。<br><br>（35-「ISMAP管理基準_参考１、２（案）」の「8.5.1」について）<br>御意見を踏まえ、8.5.1の詳細管理策の内容を次のように修正いたします。<br>「情報へのアクセス制限及びアクセス制御に関する方針に基づいて、セキュリティを保った認証技術及び手順を実施する。」<br><br>（36-「ISMAP管理基準_参考１、２（案）」の「8.21」について）<br>ISMAP管理基準改定案で用いている用語や管理策基準の適用範囲・対象範囲について、ガイドライン等にて公表し、クラウドサービス事業者と制度側とで共通理解の醸成を図る予定です。<br><br>（37-「ISMAP管理基準_参考１、２（案）」の「8.21.2」について）<br>情報セキュリティ管理基準においても、”ネットワークサービスに必要なセキュリティ対策”と書かれており、意味に齟齬はないため、原案のとおりとします。御指摘の点についてはガイドラインを策定する際の参考とさせていただきます。<br><br>（38-「ISMAP管理基準_参考１、２（案）」の「8.23.1」について）<br>御意見を踏まえ、8.23.1の詳細管理策の内容を次のように修正いたします。また、ガイドラインで補足説明を実施し、できる限り御不明な点が解消されるよう、明確化して参ります。<br>「外部ウェブサイトのアクセスに関する規則を整備し、外部ウェブサイトへのアクセスを管理する。」 | 監査企業 |

| 連番 | 提出意見／電子ファイル | 御意見に対する回答 | 提出者 |
|---|---|---|---|
| 50 | 詳細管理策の中に、複数の観点が含まれる管理策がある場合に、詳細管理策単位で一意に定型管理策を特定できない場合があるように思われます。<br>例えば、8.1.3.5では、以下のように、二つの観点が含まれているようですが、（a）は定型管理策２に、（b）は定型管理策３に該当するように思われます。<br>全てを洗い出すことができずに恐縮ですが、この様に、一意に特定できない詳細管理策については、定型管理策側の定義を分けて記載するようご検討をお願いします。<br><br>◇8.1.3.5<br>クラウドサービス利用者に対し、当該利用者の資産(バックアップを含む)を管理するため、次のいずれかを提供する。<br>a)当該利用者の管理する資産を、記録媒体に記録する(バックアップを含む)前に暗号化し、当該利用者が暗号鍵を管理し消去する機能<br>b)当該利用者が、当該利用者の管理する資産を記録媒体に記録する(バックアップを含む)前に暗号化し、暗号鍵を管理し消去する機能を実装するために必要となる情報 | 御意見を踏まえ、項目に応じて類型が異なる管理策について、以下に示すように両方を記載するよう修正いたします。<br>a)定型管理策2<br>b)定型管理策3 | 監査企業 |
| 51 | [1] 監査項目の減少と実質的な負担軽減の実現<br>「ISMAP管理基準改定概要資料 (参考ISMAP管理基準の改定について(案)」のp.1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、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」との記載がございます。この「ガイドライン」を策定されるにあたり、令和7年6月13日閣議決定された「規制改革実施計画」の2実施要項-3．投資大国-(4)デジタル・AI-No.1-C)に記載の通り、「国際標準化機構(ISO)/国際電気標準会議(IEC)27000 シリーズ等、他の認証制度を取得 している場合には、該当の認証制度を活用 し、監査項目を削減する」ことが可能となるよう明記されることが監査負担軽減に寄与するものと考えますため、確実に実施いただくことを要望いたします。また、ここには「国際標準化機構(ISO)/国際電気標準会議(IEC)27000 シリーズ等」と記載されておりますが、FedRAMPやSOC2など他の規格や基準が活用できる項目がある場合は同様に監査項目を削減可能とできると、さらに監査負担の軽減に寄与するものと考えますため、活用可能な認証制度の柔軟な拡大をご検討いただくことを提案いたします。これらを通じて監査項目の減少が、監査工数や費用の実質的な削減につながることを要望いたします。<br><br>[2] クラウドの定義の明確化 (その1)<br>「ISMAP管理基準(案) 1.3.2クラウドコンピューティング」では「共有化されたコンピュータリソース (サーバ、ストレージ、アプリケーション等) について、利用者の要求に応じて適宜、適切に配分し、ネットワークを通じて提供することを可能とする情報処理形態」と定義されています。現在、クラウドの形態は多岐に渡ります。ISMAPの対象をより明確に示すために、市場の実態に即し、本定義に下記の文言を追記いただくことを提案します。<br>「実装モデルとして、プライベートクラウド、コミュニティクラウド、パブリッククラウド及びハイブリッドクラウドがある。」<br>この文言は総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」にも記載されており、標準的な理解に基づくものです。<br><br>[3] クラウドの定義の明確化 (その2)<br>「ISMAP管理基準(案) 1.3.3 クラウドサービス」では「クラウドコンピューティングを提供するサービス。」と定義されています。現行定義ではクラウドサービスの形態 (パブリックやプライベートなど)に関する記載がなく、ISMAPがどの形態を対象としているかが不明確です。政府各省庁においては、パブリッククラウドとプライベートクラウドを組み合わせて利用する方針が示されており、クラウドサービスを一括りにするのではなく、本管理基準令がどのクラウド形態を対象としているかを明確にすることが重要と考えます。本定義に下記の文言を追記いただくことを提案します。<br>「本管理基準令におけるクラウドサービスはパブリッククラウドを対象とする。」<br>以下に、関連する政府方針を示します。[a] デジタル庁「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針」政府が取り扱う情報の機密性等に応じて、パブリッククラウドとプライベートクラウドを組み合わせて利用する。[b]「クラウド・バイ・デフォルト原則」政府情報システムは原則としてクラウドを第一候補とし、機密性やセキュリティ要件に応じてパブリッククラウド、プライベートクラウド、オンプレミスを適切に選択する。[c] デジタル社会の実現に向けた重点計画 (令和4年6月7日 閣議決定) 政府が取り扱う情報の機密性等に応じて、パブリッククラウドとプライベートクラウドを組み合わせて利用する「ハイブリッドクラウド」の利用を促進する。[d] 内閣府「経済安全保障重要技術育成プログラム」サイバーセキュリティや機器の信頼性を確保しつつ、クラウドサービスの活用を進めるため、ハイブリッドクラウドの利用が促進されている。<br><br>[4] ISMAPの対象となるクラウドサービスの明確化および相談窓口の整備<br>ISMAPの取得が必要となるクラウドサービスの範囲を明確にするガイドラインの策定と、相談窓口の明確化を要望いたします。具体的には、パブリッククラウド、プライベートクラウド、ハイブリッドクラウドなどのうち、どのクラウドサービスが対象となるか否か、また、ISMAPまたはISMAP-LIUのどちらを取得すべきかについて、明示するガイドライン、適切な相談窓口を整備いただくことを提案します。IPA、ISMAP運営委員会、認定監査法人がある現行の組織体系が複雑ですが、これがより簡素化されて、各組織の役割がより明確になり、相談窓口から明確な回答が得られることを期待いたします。<br><br>[5] ISMAP取得に向けた提出資料の英語対応<br>一部の提出資料が日本語のみと許可されている点は、海外企業にとって翻訳精度や翻訳に関する責任の所在が取得障壁となっています。すべての提出資料において英語による提出が可能となることを要望いたします。 | 御意見に記載の項目毎に以下のとおり回答いたします。<br>（[1] 監査項目の減少と実質的な負担軽減の実現について）<br>現行制度において、他の認証制度の活用については、他の認証制度における統制内容と共通する部分が一定程度あるものの、準拠している基準、監査・審査の手続き、監査人の要件等が異なり、ISMAPが求めるセキュリティ水準を満たしていることを客観的に担保することが難しいなど、困難な面がございますが、御意見を踏まえ、引き続き検討を進めて参ります。<br>また、ISMAP制度の抜本的な見直しとして、SaaS事業者を対象に、他の認証制度の活用等を通じてクラウドサービス事業者の負担を軽減する新たな枠組みを検討中です。<br><br>（[2] クラウドの定義の明確化 (その1)について）<br>ISMAP管理基準改定案で用いている用語について、ガイドライン等にて公表することを検討しています。<br><br>（[3] クラウドの定義の明確化 (その2)について）<br>ISMAP管理基準で用いている用語について、ガイドライン等にて公表することを検討しています。<br><br>（[4] ISMAPの対象となるクラウドサービスの明確化および相談窓口の整備について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承りました。<br>なお、クラウドサービスについては、政府統一基準にて定義がされております。<br>また、制度所管省庁の役割分担を公表しているほか、制度の総合窓口も設け公表しております。加えてISMAPポータルからISMAPに関するお問合せを受け付けるためのフォームも用意されております。<br><br>（[5] ISMAP取得に向けた提出資料の英語対応について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承ります。 | 企業 |

| 連番 | 提出意見／電子ファイル | 御意見に対する回答 | 提出者 |
|---|---|---|---|
| 52 | （全体関連）<br>【意見1-１】<br>別表３の管理策基準について、現行で４桁管理策とされていたものが、改正後は別表３からは削除され、（参考）手引きに移されたが、（参考）手引きに記載されている項目についての取り扱いが明確でない。仮に、（参考）手引きに記載されている項目も、監査で必須とされるのであれば、運用上は事業者の負担は軽減しないこととなる（仮に、改正前の末尾にBが付された詳細管理策以外の項目も、必須とされるのであれば、むしろ増大することになる。）。<br>IEC/ISO規格では、ISO27002は必須項目ではなく、ISO27001を満たすための参考資料との位置づけとされており、（参考）手引きに記載されている項目は、ISO27002に相当するものである。<br>今回の改正は、クラウドサービス事業者の負担の軽減を目的としたものと認識しているが、（参考）手引きに記載されている項目について、今回の改正の趣旨を踏まえた、監査上の取り扱いを明確にされたい。<br><br>【意見１-２】<br>リスクに基づく取組（リスクベースアプローチ）への移行が示され、現行で４桁管理策とされていた詳細な項目が別表３から削除されることとされたが、（参考）手引きに記載された詳細な項目をチェックボックスとして運用されるのであれば、実質的にはリスクベースアプローチへ移行されるとはいえないと考えられる。<br>リスクベースアプローチの本来の趣旨に沿った運用の見直しを要望する。<br><br>（個別の技術要件関連）<br>【意見２】管理策6.1.4関連<br>リスク軽減のための対策の例として、（参考）手引きに「企業資産の利用を遅らせる」といった記述があるが、資産の提供をしていないなど何かをしていないことを証明することは、悪魔の証明であり極めて困難である。<br>監査において、候補者の確認の完了前の企業資産の未提供など、リスク軽減のための対策の実施について証明を求めることとなるのであれば、その具体的な証明手段やその評価指針の明確化を要望する。<br><br>（その他）<br>【意見３】運用状況評価ランダムサンプリングについて<br>別表３の管理策基準について、現行で４桁管理策とされていたものについて、公表されているISMAP監査基準では明記はされていないが、監査実務においては25件の運用状況評価ランダムサンプリングが求められている。今回の改正で、現行で４桁管理策とされていたものが、改正後は別表３からは削除され、（参考）手引きに移されたが、運用状況評価ランダムサンプリングの対象が明確とされていない。<br>運用状況評価ランダムサンプリングは、実務上事業者の非常に大きな負担となっており、公表されているISMAP監査基準では明記されていないため対応に困難が生じているところである。改正後は、運用状況評価ランダムサンプリングの対象は別表３の管理策基準についてとするのか、あるいは、（参考）手引きに記載された項目についても対象とするのか、仮に、（参考）手引きに記載された項目についても対象とするのであれば、どの項目を対象とするのかなど、運用状況評価ランダムサンプリングの対象について明確化されたい。 | 御意見に記載の項目毎に以下のとおり回答いたします。<br>（【意見1-１】について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、ISMAP制度の監査につきましては、検討中であるところ、御意見として承ります。<br><br>（【意見１-２】について）<br>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しています。<br>御意見も踏まえ、「ガイドライン」の内容を検討して参ります。<br><br>（【意見２】管理策6.1.4関連について）<br>監査は、クラウドサービス事業者が言明した管理策に対して行うことを想定しているところ、御意見を踏まえ、「ガイドライン」の策定及び言明した管理策への監査上の取り扱いについて検討を進めて参ります。<br><br>（【意見３】運用状況評価ランダムサンプリングについて）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、ISMAP制度の監査につきましては、検討中であるところ、御意見として承ります。 | 企業 |
| 53 | FedRampでは監査・評価の自動化が進んでおり（https://www.fedramp.gov/20x/goals/）、海外のクラウド事業者ではそれを踏まえて自動化への対応を進めている。国内の事業者も監査・評価の自動化への準備を進めているところも…xx」などの何をもって適切・慎重・十分と判断すべきか迷いが生じるような表現を減らしていくことが必要だと考えられる。<br>逆に、「xxが記載されていること」「例としてxxを含むこと」といった判断が明確な記述を増やしていくことが適切だと思われる。なお、ガバナンス基準、マネジメント基準、管理策基準案では「適切」という箇所が６５箇所ある。これらは具体的に次のように変更できる。<br><br>3.3.2.2 各情報セキュリティマネジメントシステムの責任者は、以下を実行する。<br>・組織体の目的を適切に支援し、維持するような情報セキュリティの確立<br>→・組織体の目的の達成を支援し、維持するような情報セキュリティの確立<br>3.3.3.2 各情報セキュリティマネジメントシステムの責任者は、以下を実行する。<br>・適切な投資及び資源の配分の実施<br>→・投資及び資源の配分の実施（「適切な」は不要。適切であるのは当然であり、他のBulletに記載されていないことから統一することが望ましい。）<br><br>6.3.2 特定の技能及び専門知識を必要とする役割をもつ技術チームに対して、適切な訓練計画を策定し、定期的に実施する。<br>→ 特定の技能及び専門知識を必要とする役割をもつ技術チームに対して、専門知識を有していることを実証可能な訓練計画を策定し、定期的に実施する。（文脈から専門知識を有していることの確認がポイント）<br><br>単語そのものに意味の幅があるものは「例えばxxのような」など、具体的な活動を示唆することで人もAIも解釈に一定の方向性が与えられ、認識の齟齬が減るものと考えられる。<br>例えば以下が考えられる。<br>5.7.3 脅威インテリジェンス活動を実施する<br>→ 他社におけるインシデント情報の収集や、それが自社環境で発生しうるかどうかの分析などの脅威インテリジェンス活動を実施する（幅広い活動である脅威インテリジェンスの具体例を示した方がよいのでは）<br>5.35.1 情報セキュリティの定期的な独立したレビューを計画し、実施する。→ 情報セキュリティの定期的な牽制が効く利害関係のない立場からの独立したレビューを計画し、実施する。（「独立した」という言葉の求める意味を明示すべき）<br>8.1.2 エンドポイント機器を保護するための対策を実施する。→ エンドポイント機器を保護するためのアンチウイルスソフトの導入や生体認証の導入などの対策を実施する（多岐に渡るので例示が必要ではないか）<br>8.4 プログラムソースコード及びプログラムソースライブラリへの読取り及び書込みのアクセスを管理する。<br>→ プログラムソースコード及びプログラムソースライブラリへの読取り及び書込みのアクセスを定期的に監視し、必要に応じて用途の確認を行うなどの管理を行う。（「管理」の意味が曖昧であるため、求める管理の内容を例示すべき）<br>8.27.1 セキュリティに配慮したシステム構築の原則を整備する<br>→セキュリティに配慮したシステム構築の際に常に参照され、判断の共通認識・規範・立ち戻るための原点としての原則を整備する（「原則」という単語に求められるニュアンスはシステム構築においては一般的な原理原則という内容より狭義であると考えられるため、求められる要素を明示すべきでは） | 御意見に記載の項目毎に以下のとおり回答いたします。<br>（迷いが生じるような表現について）<br>ISMAP管理基準改定案では、根拠となる最新の国際及び国内規格で使用されている文言や情報セキュリティ管理基準と、できるだけ調和するように工夫しておりますが、ISMAP管理基準の表現に関する御意見として、今後の制度運用における参考とさせていただきます。<br><br>御意見の内容につきましては、情報セキュリティ管理基準における記載内容に準拠していることによるものであり、ISMAP管理基準改定案の策定方針に従って原案のとおりといたしますが、今後の改定において御意見を参考とさせていただきます。<br><br>（具体的な活動を示唆することについて）<br>ガイドラインでは個別の管理策について、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です。<br>今後のガイドライン策定における参考とさせていただきます。 | 監査企業 |

| 連番 | 提出意見／電子ファイル | 御意見に対する回答 | 提出者 |
|---|---|---|---|
| (53の続き) | ・管理策基準においてはシステムの設計値・設定値をレビューすることで要件の充足が判断できる部分が多分にあると考えられる。パラメータシートを提出させ利用されているコンポーネントの設定値から各要件の充足度を自動的に判断する仕組みを導入することにより、文書作成や文書レビューの工数が大幅に削減されることが期待される。また各要件を満たすための設計集・設定集を共有することで、IaaS/PaaSを利用して基盤を構築しサービスを提供するSaaSベンダーは設計の手間や工数が大幅に削減され、競争力の高いサービスの検討と維持にリソースを割くことができるため、スタートアップ含む中小ベンダーへの有効な支援策となるのではないかと考えられる。<br>今後の施策としてこうした設計値・設定値のレビューにも取り組んで頂きたい<br><br>例えば<br>8.15.2 ログ情報の完全性を確実にするための対策を実施する。8.16.2 リアルタイム又は定期的な間隔で監視を行う。8.17.1 クロックは、組織が採用した時刻源と同期させる。<br>→OSの該当する設定値や対策ソリューション及びその設定値を提出させることで監査可能だと考えられる。 | （設計値・設定値のレビューについて）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承ります。いただいた御意見は、今後の制度改善に関する検討の参考とさせていただきます。 | 監査企業 |
| 54 | 本パブリックコメントは「ISMAP管理基準（案）」等に関するものとなりますが、「ISMAP管理基準（案）」等に関するものは別で提出させていただきましたので、こちらISMAP制度全般に関するパブリックコメントを提出させていただきます。<br><br>■英語サイト・英語文書について<br>英語サイトは長期間更新されていないように思いますので、特に外資系CSP向けにもう少し情報の充実化を図って頂きたく、また英語文書につきましてもタイムリーに公開していただきたいです。<br><br>■更新時の提案<br>ISMAPを更新するCSPについては、現状のその他の認証(ISOやSOC等)）の確認や、プロダクトのアップデート、管理手法の変更があったか否か等について、「ISMAP更新ポータルサイト」のようなものから、自動的に行うことが望ましいと考えております(毎回、監査法人、CSP担当者、IPA担当者が実作業で文書を作成・確認するのではなく)<br><br>■監査法人<br>これまで複数の監査法人に監査をお願いしてきましたが、監査法人間で監査手続きの厳格さに差異があるように見受けられますので、監査手続きの厳格さに一貫性を確保してもらいたい。また、これに加え、監査法人の質＆量(人員)の担保、監査で自動化出来る部分の自動化(既に取得している認証や明らかに不要な再監査など)<br><br>■他の認証制度の活用<br>他の認証制度(ISO27001、SOC2)を活用した外部監査の一部省略化につきましては、あまり進捗がないように見えますので、なんらかのアップデートをしていただきたい。<br><br>■IPA担当者<br>審査時においてIPA担当者ごとに厳格さに差異があるように感じられますので、このあたり人依存でないようにしてほしいです。<br><br>■セキュリティインシデント報告<br>セキュリティインシデント報告義務において、「影響のある”利用者”」と「”重大な影響”」の定義が広く、かつ曖昧であるため、もう少し明確化してほしい(CSP側で報告すべきインシデントかどうかの判断が難しいため) | 御意見に記載の項目毎に以下のとおり回答いたします。<br>（■英語サイト・英語文書について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承ります。いただいた御意見は、今後の制度改善に関する検討の参考とさせていただきます。<br><br>（■更新時の提案について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承ります。いただいた御意見は、今後の制度改善に関する検討の参考とさせていただきます。<br><br>（■監査法人について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、ISMAP制度の監査につきましては、検討中であるところ、御意見として承ります。いただいた御意見は、今後の制度改善に関する検討の参考とさせていただきます。<br><br>（■他の認証制度の活用について）<br>現行制度において、他の認証制度の活用については、他の認証制度における統制内容と共通する部分が一定程度あるものの、準拠している基準、監査・審査の手続き、監査人の要件等が異なり、ISMAPが求めるセキュリティ水準を満たしていることを客観的に担保することが難しいなど、困難な面がございますが、御意見を踏まえ、引き続き検討を進めて参ります。<br>また、ISMAP制度の抜本的な見直しとして、SaaS事業者を対象に、他の認証制度の活用等を通じてクラウドサービス事業者の負担を軽減する新たな枠組みを検討中です。<br><br>（■IPA担当者 について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承ります。いただいた御意見は、今後の制度改善に関する検討の参考とさせていただきます。<br><br>（■セキュリティインシデント報告について）<br>今回の意見募集の対象（ISMAP管理基準の改定等）に対する直接の御意見ではないと理解しますが、御意見として承ります。いただいた御意見は、今後の制度改善に関する検討の参考とさせていただきます。 | 個人 |
| 55 | 貴重な機会をありがとうございます。3点コメントさせていただきます。<br>１）<br>ISMAP管理基準改定概要資料 のP3にて<br>「・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」とあるので参考情報になったとのことですが「・なお、監査においては手引きを参考に監査を実施」ともあり、結局手引きを参考した監査を実施されるのであれば”項目数を削減”といえ、結局1つの管理策にてこれまでの管理策内容が箇条書きに集約されただけで対応者側からすると呼応状態の確認など、より煩雑な対応をせざるを得ないと感じます。<br><br>２）<br>「ガイドライン」にて管理策や証跡など解説予定とのことですが、今回の改定の肝がその手引きやガイドラインにあると思います。それも一緒に拝見しないことには今回の改定へのコメントが難しく、今回の改定の進め方に疑問を覚えます。今回のパブコメなども踏まえたガイドラインや手引きを用意されること、またガイドライン公開タイミング後十分な確認期間を確保したうえでのISMAP改定施行日が設定されることを望みます。<br><br>３）<br>マルチテナントでサービス提供しているSaaS事業者の場合、解約時の暗号化消去は現実的ではないと考えます。暗号鍵の抹消は復元不可となる分かりやすい手段だとは思うのですが、それ以外の許容されうる手法をガイドラインで例示いただきたいです。（事前相談の枠が用意されるとのことではありますが、ベースとなる考え方や手法を現行より詳細に提示いただけると事前相談前の準備がしやすくありがたいです）<br>以上です。よろしくお願いいたします。 | 御意見に記載の項目毎に以下のとおり回答いたします。<br>（1について）<br>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しています。<br>御意見も踏まえ、これまで以上に負荷がかかることのないよう、ガイドラインの内容について検討を進めて参ります。<br><br>（2について）<br>新基準適用のタイミングや経過措置については、クラウドサービス事業者、監査機関等、関係者の御意見を踏まえながら慎重に検討を進めて参ります。<br>なお、ガイドライン策定の際は、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であるほか、パブリック・コメント前にも関係者向けの説明会等で丁寧に説明して参りたいと考えています。<br><br>（3について）<br>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しています。<br>御意見も踏まえ、ガイドラインの内容や事前確認の枠組みについても、検討を進めて参ります。 | 個人 |

| 連番 | 提出意見／電子ファイル | 御意見に対する回答 | 提出者 |
|---|---|---|---|
| 56 | 以下の通り、７つの意見を提出します。<br>(1)利用者による暗号鍵管理機能に関する管理策の削除<br>8.13.5，8.24.5 及び 10.1.2.20.PB の利用者による暗号鍵管理機能を要求する管理策の削除、もしくはIaaSのみに適用される管理策として位置づけを変更するようお願いします。<br><br>理由：日本のクラウドサービスベンダーにおいて、利用者鍵管理機能の実装のハードルは高くまた、クラウドサービスの利用者において、鍵を管理すること自体もハードルが高く、実際に利用者が鍵を管理する機能を提供しても、政府機関が一般的に利用することはまだまだ困難な状況であるにも関わらず、実装を強制されていて、ISMAPの監査におけるハードルをあげるものとなっています。<br>利用者鍵管理をしてデータを保護する必要があるのは、機密性がかなり高い水準にあるもので、少なくともISMAP-LIUが想定する情報を利用者鍵管理で保護する必要性は低いと考えられますが、LIUを取得しようとするクラウドベンダーに対しても、機能が求められている状況です.ISMAPの制度趣旨は、クラウドベンダーのセキュリティ対策を実施していることを確認する制度であり、実装されているセキュリティ機能を確認する制度ではないと認識しています。セキュリティ機能は、その機能を利用する利用者自身で確認が可能なので、利用者鍵管理機能を利用する予定がない利用者に対しても門戸を閉じてしまっていることに違和感があります。<br><br>(2)デセプション設置に関する管理策の削除<br>8.12.1 に「敵対者の決定を混乱させる方策を講じる。」とあり、デセプションの設置を要件として設定しているようですが、デセプションの設置はまだ一般的なセキュリティ対策として広がっているわけではなく、必ずしも必須のセキュリティ対策とは言えないと思われます。<br>(3)侵害されたパスワードの利用検知に関する項目の削除<br>5.17.3 に「f) 一般的に使われるパスワード、並びにハッキングされたシステムで侵害された利用者名及びパスワードの組合せの使用を防止する。」という項目がありますが、パスワードの管理は利用者の責任で実施されるべきものであり、侵害されたパスワードの検知は、利用者が導入すべきパスワード管理ツールなどで実施すべきものと考えられ、必ずしもクラウドサービスの機能として導入が必須ではないと思われます。<br>(4)目立たないオフィスに関する管理策の削除<br>11.1.3.2 に「オフィス…セキュリティを保つために、建物を目立たせず…」とした管理策がありますが、「目立つ」かどうかは主観的な評価であり、監査項目として適切ではないと思われます。<br>(5)管理策が採用された理由の明確化<br>管理策の説明において、8.13.5の説明に「統一基準由来」と記載されている箇所がありますが、ISO由来なのか、NIST由来なのか、どちらでも無ければどのような経緯で管理策に追加されたのか、解説をしていただけませんでしょうか。ISMAP審査にあたって、管理策の解釈が明示されているほうが審査側と申請側の相互理解が進みやすいと考えております。<br>(6)ISAMP-LIUを早期に取得できるようにする仕組みの提案<br>ISMAP-LIUは、インパクトの低い情報を扱うサービスに関する制度であるが、監査のハードルが高く制度の運用開始から期間が経過しても現状2件の登録があるのみとなっています。ISAMP-LIU活性化のため、参考となる認証制度を紹介させていただきます。<br>・TX-RAMP<br>https://dir.texas.gov/information-security/texas-risk-and-authorization-management-program-tx-ramp<br><br>テキサス州の州政府が利用するクラウドサービスは、TX-RAMPの認証を取得する必要があります。TX-RAMPには、Fast Track という制度があり、特定の認証監査を受けているサービスについて、Fast Trackを利用することができます。<br>SOC2監査を受けている場合は、SOC2監査レポートをテキサス州に提出することで、18ヶ月の暫定ステータスを得ることができます。暫定ステータスの間、州政府は当該クラウドサービスに発注をすることができ、18ヶ月の間に、テキサス州からのセキュリティ対策に関する質問を受け、ベンダーが対応することで、正式なTX-RAMPの認証を得ることができる、という制度です。Fast Trackの仕組みの利用は、無償となっており、ベンダーに対して優しい制度となっています。日本では、ISO/IEC 27017 を取得しているサービスが普及していることから、この認証を取得しているサービスは、ISAMP-LIUのFast Trackを利用して、認証を受けていることを証明、およびIPAからのセキュリティ対策に関する質問に答えることで、ISMAP-LIUに登録できるような仕組みを検討いただければと思います。<br><br>(7)ISMAP-LIUの負担軽減<br>現行ISMAP管理基準では、ISMAP-LIUは対象となる管理策基準を「一部の重要な管理策（サービス基盤やサービス構成に直接的な影響を及ぼし得る管理策）」とする事が明記されていました。しかし改定案では「全ての詳細管理策については原則として実施」となり、またISMAP-LIUに関する特別の言及が無いことから、ISMAPとISMAP-LIU取得における負担の差は、事実上変わらなくなってしまったように感じられます。ISMAP-LIUという枠組みを有効に活用するためにも、ISMAPとISMAP-LIUの違いを明示いただきたいと思います。<br>以上、よろしくお願いします。 | 御意見に記載の項目毎に以下のとおり回答いたします。<br>（(1)利用者による暗号鍵管理機能に関する管理策の削除について）<br>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しています。<br>御意見も踏まえ、ガイドラインの内容について検討を進めて参ります。<br><br>（(2)デセプション設置に関する管理策の削除について）<br>一律に個別管理策の内容を決定するものではなく、リスクアセスメントの結果に応じて個別管理策を検討いただく必要があります。<br>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しています。<br>御意見も踏まえ、ガイドラインの内容について検討を進めて参ります。<br><br>（(3)侵害されたパスワードの利用検知に関する項目の削除について）<br>一律に個別管理策の内容を決定するものではなく、リスクアセスメントの結果に応じて個別管理策を検討いただく必要があります。<br>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しています。<br>御意見も踏まえ、ガイドラインの内容について検討を進めて参ります。<br><br>（(4)目立たないオフィスに関する管理策の削除について）<br>御指摘いただいた点は、手引きの内容であり、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しています。<br>御意見も踏まえ、ガイドラインの内容について検討を進めて参ります。<br><br>（(5)管理策が採用された理由の明確化について）<br>8.13.5の説明において、政府統一基準由来との記載が見受けられないため回答は差し控えさせていただきます。<br>なお、各管理策の由来については新旧対照表を公表予定です。<br><br>（(6)ISAMP-LIUを早期に取得できるようにする仕組みの提案について）<br>現行制度において、他の認証制度の活用については、他の認証制度における統制内容と共通する部分が一定程度あるものの、準拠している基準、監査・審査の手続き、監査人の要件等が異なり、ISMAPが求めるセキュリティ水準を満たしていることを客観的に担保することが難しいなど、困難な面がございますが、御意見を踏まえ、引き続き検討を進めて参ります。<br>また、ISMAP制度の抜本的な見直しとして、SaaS事業者を対象に、他の認証制度の活用等を通じてクラウドサービス事業者の負担を軽減する新たな枠組みを検討中です。<br><br>（(7)ISMAP-LIUの負担軽減について）<br>現行ISMAP管理基準の本文に、御意見で記載いただいた文言の記載はありません。ISMAP-LIUに関連した内容は、「ISMAP-LIUクラウドサービス登録規則」等に規定しておりますので、改定後も同規則等にて規定をすることを検討しています。<br>なお、ISMAP制度の抜本的な見直しとして、SaaS事業者を対象とする負担を軽減した新たな枠組みを検討中です。 | 団体 |

| 連番 | 提出意見／電子ファイル | 御意見に対する回答 | 提出者 |
|---|---|---|---|
| 57 | 社内での意見を取りまとめましたので、ご確認のほどよろしくお願いいたします。<br>■全体<br>- これまで４桁レベルで統制内容を記載が必要でしたが、今回の改訂においては、３桁レベルの統制内容を書くということにとどめ、「手引き」ごとに記載を求めるような運用にならないよう、検討をお願いします。「手引き」がこれまでの４桁項目よりも詳細になっており、増えていることを鑑みると、「手引き」レベルでの記載を求められるとこれまで以上に負荷がかかると想定されます。<br>- 旧管理基準にない項目が手引きとして４００項目以上追加されることになったことも鑑みて、実際の監査時には、「手引き」がそのまま「監査テスト項目」にならないよう、監査手続きに明確にあくまでも「手引き」であることを明示するようお願いしたい<br>- ISMAP管理基準改訂概要資料にもある通り「手引き」から選択できるとあるが、選択しなかった手引きの内容に１つ１つ理由を提出し、ISMAP運営委員会などが承認する、というような運用にすると、手引きの数の多さから、必要以上に時間がかかる、煩雑になる、議論が求められることが考えられるため、手引きの選択においてはビジネスリスク判断に委ねる形にしていただくことを強く希望します。<br>- ISMAP管理基準改訂概要資料にもある通り、「リスク分析の結果、実施不要」と判断することが認められるとのことだが、リスク分析の結果の判断は、クラウドサービス提供側の判断ではあるものの、ビジネスをする以上、お客様への悪影響を及ぼすような判断は通常しないことはお分かりかと思います(CSPにだけ都合の良い判断をしたら、そもそもお客様からの信頼や評価が下がるのでビジネス判断としてすることはない）。したがって、その適切なプロセスを経て行われたビジネスリスク判断はそもそもそのまま認められるべきものとは思いますが、リスク判断の「理由」について、たとえばIPA担当者が納得できない、などの理由で却下されることがあることを懸念しております。そのようなことがないような運用の徹底をお願いしたいと思います。<br>■ガバナンス基準<br>- 3.3.2.1にあるリスクおよび機械の確実な考慮と、リスク選好の決定について、ほぼ同じ監査テストがなされることが想定されるため、重複のない管理策にしていただきたい。<br>- 3.3.2.2に内包されることも考えられるが、3.3.3.2として分離している理由は何でしょうか。理由がない場合は、別途管理策を設ける必要はないのではないでしょうか。<br>■管理策基準<br>- 5.1.3 (5a-5.1参考1～3)： これをわざわざ含めることで何らかのリスクを追加で回避できるとは考えにくいため、省いても良いのではと思います。<br>- 5.1.4： ISMAPはそもそもクラウドサービスの登録のための制度であるため、当然「情報セキュリティ方針」というとクラウドサービスの提供の立場からのセキュリティ方針であるため、この項目をわざわざ別に出すことによる意味がわからない。（一般的な情報セキュリティの考えとしてクラウドサービスに特化したものを含めるのであれば納得はいくがISMAPとしては別に項目を設ける必要はないのでは）<br>- 5.3.1(5a-5.3.6)： 役割を「慎重に定義し付与」について、何の証跡が監査として適切かが不明なので、もしこれを含める場合は、明確な監査証跡の例を明示してほしい。<br>- 5.5.1 (5a-5.5.2): この項目をどう監査するのか、明確な監査証跡について例示をいただきたい。<br>- 5.9.1 (5b-5.9.6): 資産の目録の粒度のレベルがニーズに適しているかどうかを、監査時にどう判断するのでしょうか。明確な監査手続きや証跡の例を明示していただきたい。<br>- 5.9.1 (5b-5.9.6参考): これは監査項目となるのでしょうか、それとも単なる注記の扱いでしょうか。手引きに書く以上、監査の視点にフォーカスしていただくか、わかりやすく注記なら注記としておくようお願いします。<br>- 5.20.2 (5d-5.20.2)： ここでいう「登録簿」がいわゆる表のようなリストでない、システム上の登録（契約の管理システムなど）であっても監査証跡として認められるよう配慮していただきたいと思います。<br>- 7.2.1 (7a-7.2.3)： どのような対策が具体的に監査視点で合格となるのか明確な例示をいただきたい。<br>- 8.21.4 (8c-8.21.4)： 旧管理策基準の13.1.2.1に対応していると思われるが、対応項なし、となっている。何か別のことが求められているのか教えていただきたい。<br>- 8.27.1 (8d-8.27.4): e)最新の優れた慣行　が主観的であり、監査対象としては不十分であることから、こちらは考慮に入れること自体は問題ないとしても監査対象とすべきではないのではないでしょうか。監査対象となる場合は、何をもって「最新の優れた慣行」となるかを明示してほしい。<br>- 8.28.5 (8d-8.28.13)： d) の「実証された定評のある供給元」は主観的であり、これを監査の項目にするのは難しい。もし監査項目にする場合は、何をもとに定評があるとするのかを明示していただきたい。<br>- 8.31.3 (8d-8.31.5): 「通常と異なる状況」とはどういった状況を想定しているのか明示していただきたい。 | 御意見に記載の項目毎に以下のとおり回答いたします。<br>（統制内容について）<br>クラウドサービス事業者が詳細管理策の採用にあ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しています。<br>御意見も踏まえ、これまで以上に負荷がかかることのないよう、ガイドラインの内容について検討を進めて参ります。<br><br>（監査手続きについて）<br>監査については、手引きを全て対象にするのではなく現行と同様に、クラウドサービス事業者が言明した管理策に対して監査を行います。<br>クラウドサービス事業者が詳細管理策の採用にあたっての手引きに記載内容への対応方法については、管理基準のみでは判断しかねる部分もあるかと存じますので、今後管理基準の規定内容を補足するガイドラインの策定及び言明した管理策への監査上の取り扱いについて検討を進めて参ります。<br><br>（手引きの選択について）<br>クラウドサービス事業者が詳細管理策の採用にあたって手引きの記載内容への対応方法については、管理基準のみでは判断しかねる部分もあるかと存じますので、今後管理基準の規定内容を補足するガイドラインの策定を進めていく予定です。<br>手引きは参考であり、１つ１つ選択について理由を求めない想定です。クラウドサービス事業者が詳細管理策の採用にあたっての手引きに記載内容への対応方法については、管理基準のみでは判断しかねる部分もあるかと存じますので、今後管理基準の規定内容を補足するガイドラインの策定及び言明した管理策への監査上の取り扱いについて検討を進めて参ります。<br>クラウドサービス事業者のビジネスリスク判断については一定程度許容するものの、利用者である政府の考える脅威・リスクを踏まえた管理策を構築いただく必要があります。<br>また、手戻りや、想定されるリスクに応じて統制目標に対応する詳細管理策を選択するのではなく実態としてそれ以上に詳細管理策を選択すること等を抑止するために制度（審査）による事前確認を受けることができる枠組みの検討を進めていく予定です。<br><br>（リスク分析の結果の判断について）<br>事前確認の枠組みは、手戻りや、想定されるリスクに応じて統制目標に対応する詳細管理策を選択するのではなく実態としてそれ以上に詳細管理策を選択すること等を抑止するために検討しています。目的に照らし事前確認による負荷が増加することがないよう、御指摘いただいた点を踏まえ、事前確認の枠組みの検討を進めて参ります。<br><br>（3.3.2.1について）<br>御意見いただいた点を踏まえ、標準監査手続の検討を進めて参ります。<br><br>（3.3.2.2について）<br>御意見の対象となるガバナンス基準の構成は、情報セキュリティ管理基準及びその根拠となっているISO/IEC 27014:2020の構成に合わせており、これらの基準に基づいたガバナンスを実践している事業者において利便性が高いものと考えております。<br><br>（5.1.3(5a-5.1参考1～3)について）<br>詳細管理策の採用にあたっての手引きに記載内容への対応方法については、管理基準のみでは判断しかねる部分もあるかと存じますので、今後管理基準の規定内容を補足するガイドラインの策定を進めて参ります。<br><br>（5.1.4について）<br>当管理策では、クラウドサービスの提供及び利用に言及した情報セキュリティ方針の策定にあたり、含めるべき観点を手引きにて定義しております。パブリック・コメント用の資料では著作権の関係でマスキングをしておりますため、その判断しかねる部分があるかと存じます。<br>マスキングされていない管理基準案及び新旧対照表は、ISMAPポータルの請求フォームから資料請求できるページを、年内に公開予定です。なお、請求に当たり以下のJIS規格の購入が必要です。<br>JIS Q 27017:2016 (ISO/IEC 27017:2015)<br>JIS Q 27014:2015 (ISO/IEC 27014:2013)<br><br>（5.3.1(5a-5.3.6)、5.5.1 (5a-5.5.2)、5.9.1 (5b-5.9.6)、5.9.1 (5b-5.9.6参考)、5.20.2 (5d-5.20.2)、7.2.1 (7a-7.2.3)について）<br>ISMAP管理基準ガイドブックにて、監査対応における証跡等の例示を提供しております。管理基準の改定後も同様に、監査対応における証跡の例示等をガイドライン等にて示すことを検討しています。<br><br>（8.21.4 (8c-8.21.4)について）<br>本管理策は、情報セキュリティ管理基準を参照に記載しております。<br>なお、各管理策で求められる事項についてはガイドラインで示す予定です。<br><br>（8.27.1 (8d-8.27.4)、8.28.5 (8d-8.28.13)、8.31.3 (8d-8.31.5)について）<br>ガイドラインでは個別の管理策について、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です。 | 企業 |

| 連番 | 提出意見／電子ファイル | 御意見に対する回答 | 提出者 |
|---|---|---|---|
| 58 | 【意見1】<br>今後、監査自動化の流れは一層加速すると考えられます。すでに米国のFedRAMPでは、OSCALなどの技術を活用した自動化プログラムが推進されており、ISMAPも同様の方向性を取るべきだと考えてます。<br><br>この流れを妨げないためには、ISMAP管理基準を機械可読な形式で提供することが不可欠です。現在の「ISMAP管理基準_別表1-3（案）」はPDF形式で公開されており、表計算ソフトのセル結合も多用されているため、人間には読みやすい一方で、機械にとっての可読性が低い状態です。<br><br>将来的に日本でも監査自動化の概念や技術が普及した際に、ISMAP管理基準が障壁とならないよう、以下を提案します。<br><br>・「ISMAP管理基準_別表1-3」をPDFではなく、ExcelまたはCSV形式で公開すること。<br>・セル結合の使用を避け、機械可読性を確保した構造で発行すること。<br><br>なお、機械可読性の参考としては、総務省の「統計表における機械判読可能なデータ作成に関する表記方法について」が有用だと考えています。<br>https://www.soumu.go.jp/main_content/000723626.pdf<br><br>【意見2】<br>今後、監査自動化の流れは一層加速すると考えられます。すでに米国のFedRAMPでは、OSCALなどの技術を活用した自動化プログラムが推進されており、ISMAPも同様の方向性を取るべきだと考えてます。<br><br>この流れを妨げないためには、ISMAP管理基準を機械可読な形式で提供することが不可欠です。そのため、現行の「ISMAP管理基準_別表1-3（案）」を、NIST OSCALのCatalog Model形式で公開することを提案します。<br><br>すでにデジタル庁では「政府機関等のサイバーセキュリティ対策のための統一基準群」をOSCALフォーマットで公開しており、ISMAPもこの取り組みに追従すべきと考えます。<br><br>なお、OSCALフォーマットでの公開が技術的・運用的に困難な場合には、代替策として各詳細管理策にUUIDを付与することを提案します。UUIDの付与は既存の監査プロセスに影響を与えることなく、監査自動化に取り組む事業者に大きな利便性をもたらすものであり、実質的なデメリットはないと考えます。 | 御意見の【意見1】【意見2】のいずれとも、ISMAP管理基準の活用における効率化に関する御意見として、今後の制度運用における参考とさせていただきます。 | 企業 |
| 59 | 情報セキュリティ管理基準では、「3.3 情報セキュリティガバナンスのプロセス」（10頁）の脚注でガバナンス主体を「～組織における経営者又は取締役会が該当する」と説明している。基準案では、「1..3 用語及び定義」の項で、「準じる」としているが、ガバナンス主体の認識は重要なポイントであり、主体が誰かを明確化するために（）書き、あるいは脚注で同様の文言を入れた方が良い。 | ISMAP管理基準改定案で用いている用語について、ガイドライン等にて公表することを検討しています。 | 団体 |
| 60 | ガバナンス主体、責任者について明確にする。情報セキュリティ管理基準では、「3.3 情報セキュリティガバナンスのプロセス」（10頁）の脚注3でガバナンス主体を「～組織における経営者又は取締役会が該当する」、脚注5で責任者を、「～運用の責任を担う個人またはグループ」と解説して明確化を図っているのでそれと平仄を図るべきと思料する。 | ISMAP管理基準改定案で用いている用語について、ガイドライン等にて公表することを検討しています。 | 団体 |